Power Systems

ハードウェア管理コンソールの取り付けおよび構成

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、v ページの『安全上の注意』、99 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 9 リリース 2 保守レベル 950 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

目次

安全上の注意

安全上の注意は、このガイド全体を通じて記載されています。

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

ワールド・トレードの安全上の注意

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

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

レーザーに関する安全上の注意

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

レーザーに関する準拠

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

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

電源ケーブルや電話線、通信ケーブルからの電圧および電流は危険です。 感電を避けるため、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ないでください。
- マシンの検査を実行する際は、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。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。
- 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、以下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。

  電源を切るには、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ーから取り外します。5) すべてのケーブルをデバイスから 取り外します。

  接続するには、1) すべての電源をオフにします (別に指示される場合を除く)。2) すべてのケーブルをデバイスに接続します。3) シグナル・ケーブルをコネクターに接続します。4) 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おきます。
- 地震オプションを取り付ける場合を除き、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 (提供されている場合)。
- 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。

  
- 安定度の危険:
  - ラックがひっくり返って、重傷を引き起こす可能性があります。
  - ラックを取り付け位置に広げる前に、設置手順を読んでください。
  - 取り付け位置にマウントされているスライド・レールが装着済みの装置に負荷をかけないでください。
  - スライド・レールが装着済みの装置を取り付け位置に入れたままにしないでください。
- 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 1)

(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、装置を取り付けないでください。
- 空気の流れが妨げられているラック内には、装置を取り付けないでください。 装置内で空気の流れのために使用される装置のいずれかの側面、前面、または背面で、空気の流れが妨げられたり減速されたりしないようにしてください。
- 回路の過負荷によって電源配線や過電流保護が破損しないように、 電源回路への機器の接続には十分注意してください。 ラックに正しく電源を接続するには、ラック内の機器の定格ラベルで、電源回路 の総消費電力を確認してください。
- (引き出し式ドロワーの場合。) ラック・スタビライザー・ブラケットがラックに取り付けられていない場合や、ラックが床にボルトで留められていない場合、ドロワーやフィーチャーを引き出したり、取り付けたりしないでください。一度に複数のドロワーを引き出さないでください。 一度に複数のドロワーを引き出すと、ラックが不安定になる可能性があります。

- (固定式ドロワーの場合。) このドロワーは固定ドロワーなので、製造元の 指定がない限り、保守のために動かさないでください。 ラックからドロワーの一部または全部を引き出そうとすると、ラックが不安定になったり、ドロワーがラックから落下する可能性があります。(R001 パート 2 の 2)

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

- ラック・キャビネットの上部から順に装置を取り外すことにより、ラック・キャビネットの重量を減らします。 可能な場合は、ラック・キャビネットを納品時のラック・キャビネットの構成に復元します。 この構成がわからない場合は、以下の手順を実行する必要があります。
  - 32U 位置以上にあるすべてのデバイスを取り外します。

  - 最も重いデバイスがラック・キャビネットの下部に取り付けられていることを確認します。
  - 受け取った構成で明確に許可されている場合を除き、ラック・キャビネット内で 32U 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 2083 mm (30 x 82 インチ) 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、以下の手順を実行します。
  - 4 つのレベル・パッドを下げます。
  - ラック・キャビネット上にスタビライザー・ブラケットを取り付けるか、地震環境ではラックを床にボルトで留めます。
  - 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)

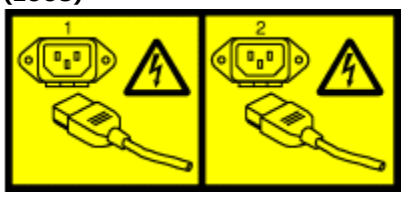
(L002)

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。 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掛かかったり、(はしごに乗って作業している場合などに) 体の位置を安定させるためにそれらの装置を使用したりしないでください。 安定度の危険:

- ラックがひっくり返って、重傷を引き起こす可能性があります。
- ラックを取り付け位置に広げる前に、設置手順を読んでください。
- 取り付け位置にマウントされているスライド・レールが装着済みの装置に負荷をかけないでください。
- スライド・レールが装着済みの装置を取り付け位置に入れたままにしないでください。

(L002)

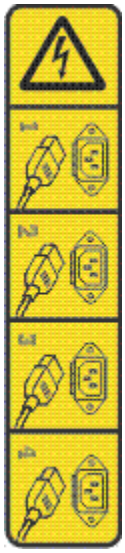
(L003)



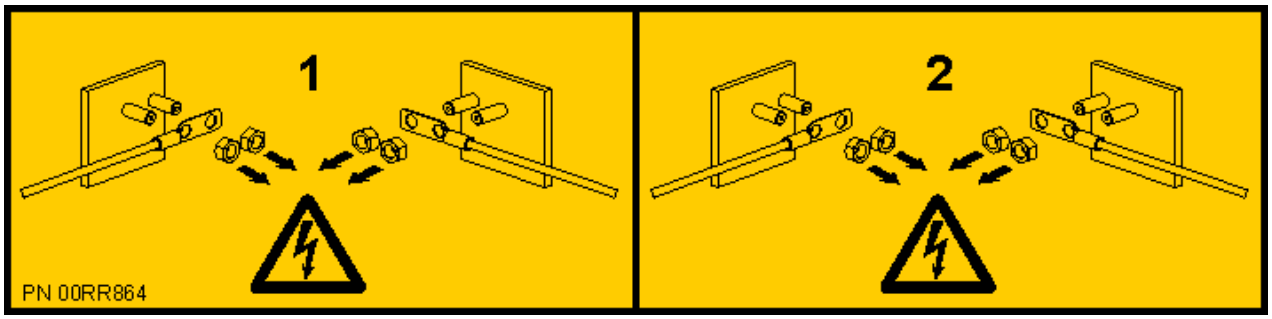
または

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。 次の情報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)

(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℃ を超えて加熱
- 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、ウォーキー、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、作業者用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。

- スタビライザー (ブレーキ・ペダル・ジャック) が完全に固定されていない限り、プラットフォーム積載棚を上下左右に動かしてはなりません。使用も移動もしていない場合は、スタビライザーのブレーキを固定したままにしてください。
- 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棚の端には、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、角度のあるユニット設置ウェッジ、その他の付属品オプションの隅に荷重をかけないでください。そのようなプラットフォーム (ライザー傾斜、ウェッジなどのオプション) は、使用する前に、提供されたハードウェアのみを使用して 4 つの位置すべて (4x またはその他のプロビジョン取り付け) にあるメイン・リフト棚または分岐点に固定します。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 (調整可能な角度プラットフォーム) オプションは、最終的な微調整 (必要な場合) を除き、常に平ら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 (このツールを使用した高さでの作業に対して認定された手順に従うものに特定のあそびが設けられている場合を除く)。
- 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、スプリンクラー、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。

- このツールは、IBM サービス担当員が使用するために、適切に維持する必要があります。IBM は、操作の前に状態を検査し、保守履歴を確認します。担当者は、不足がある場合に、このツールを使用しない権利を有します。(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。

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、トピックをまとめた前回の更新以降の、新機能または大きな変更情報をお読みください、

2021 年 4 月

- 以下のトピックが追加されました。
  - 4 ページの『ラックへの IBM Power Systems HMC (7063-CR2) の取り付け』
  - 4 ページの『ラック・マウント型 7063-CR2 システムの設置の前提条件』
  - 5 ページの『ご使用のシステム用の部品の用意』
  - 5 ページの『7063-CR2 システムを設置するラック内の位置の決定とマーク付け』
  - 7 ページの『システム・シャーシおよびラックへの調整可能レールの取り付け』
  - 8 ページの『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』
  - 10 ページの『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』
  - 10 ページの『ラック・マウント型 7063-CR2 HMC のケーブル接続』
  - 12 ページの『7063-CR2 HMC の構成』

2020 年 11 月

- 以下のトピックが更新されました。
  - 2 ページの『取り付けおよび構成のタスク』
  - 87 ページの『HMC の保護』
  - 94 ページの『HMC ポートの位置』

2020 年 7 月

- 以下のトピックが更新されました。
  - 24 ページの『HMC 仮想アプライアンスの取り付け』
  - 94 ページの『HMC ポートの位置』

2019 年 10 月

- 以下のトピックが更新されました。
  - 24 ページの『HMC 仮想アプライアンスの取り付け』
  - 87 ページの『HMC の保護』

2019 年 2 月

- 以下のトピックが追加されました。
  - 87 ページの『HMC の保護』

- 89 ページの『拡張パスワード・ポリシー』
- 91 ページの『HMC の保護における一般的な問題の解決』
- 90 ページの『セキュリティー・プロファイル: Global Data Protection Regulation (GDPR) および Payment Card Industry Data Security Standard (PCI-DSS) 』

2018 年 8 月

- 以下のトピックが更新されました。
  - 21 ページの『7063-CR1 HMC の構成』
  - 94 ページの『HMC ポートの位置』

2017 年 12 月

- POWER9 プロセッサーを搭載した 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。

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 :

- POWER9™ プロセッサー・ベースのサーバーを管理する場合、HMC はバージョン 9.1.0 以降でなければなりません。詳しくは、76 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。
- ハードウェア管理コンソールのバージョン 9.2.950 以降は、HMC 7042 マシン・タイプではサポートされません。ご使用の 7042 HMC の HMC バージョンについて詳しくは、Fix Central Web サイトにある HMC リリース・ノート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。	47 ページの『HMC 用のプリインストール構成ワークシート』 45 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。	19 ページの『ラック・マウント型 7063-CR1 HMC のケーブル接続』
4. 電源ボタンを押し、HMC の電源をオンにする。	
5. HMC Web アプリケーションにログインし、起動する。	
6. ガイド付きセットアップ・ウィザードにアクセスするかまたは HMC メニューを使用して、HMC を構成する。	54 ページの『ガイド付きセットアップ・ウィザードによる高速パスを使用した HMC の構成』 54 ページの『メニューを使用した HMC の構成』

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 *(*続き*)*	
作業	**関連情報の入手先**
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* コードの更新またはアップグレード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. アップグレードを入手する。	81 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 を追加する際に完了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、次の手順を完了します。

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完了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. 情報を収集する情報を収集し、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。	47 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。	19 ページの『ラック・マウント型 7063-CR1 HMC のケーブル接続』
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。	

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完了する必要があるタスク (続き)	
作業	**関連情報の入手先**
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。	76 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』 81 ページの『HMC ソフトウェアのアップグレード』
8. ガイド付きセットアップ・ウィザードにアクセスするかまたは HMC メニューを使用して、HMC を構成する。	54 ページの『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。	68 ページの『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』
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。

ラックへの IBM Power Systems HMC (7063-CR2) の取り付け

IBM Power Systems HMC (7063-CR2) をラックに取り付ける方法について説明します。

オンラインの設置資料を表示するか、または同じ資料の PDF バージョンを印刷できます。PDF バージョンを表示または印刷するには、「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」を参照してください。

ラック・マウント型 7063-CR2 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。

このタスクについて

注意 : この部品または装置は重量がありますが、重さは 18 kg 未満です。 この部品または装置を持ち上げ、取り外し、または取り付けるときは注意してください。 (C008)

サーバーの設置を開始する前に、以下の資料を読むことが必要になる場合があります。

- この資料の最新版は、オンラインで維持されています (『ラックへの 7063-CR2 の取り付け (Installing the 7063-CR2 into a rack)』 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm))
- サーバーの設置を計画する場合は、サイトおよびハードウェア計画を参照してください。

手順

1. 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ます。
   - サイズ 2 のプラス・ドライバー
   - マイナス・ドライバー
   - T25 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
   - 1 EIA (米国電子工業会) 単位 (1U) 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・フィーチャー』 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm)を参照してください。
- 電源機構定格は 100 V AC から 127 V AC、9 A (x2)、200 V AC から 240 V AC、4.5 A (x2); 50 または 60 Hz。

2. 5 ページの『ご使用のシステム用の部品の用意』から続行します。

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。

手順

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、部品が揃っていることを確認し、注文した部品をすべて受け取っていることを確認してください。

   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。

4. 5 ページの『7063-CR2 システムを設置するラック内の位置の決定とマーク付け』から続行します。

7063-CR2 システムを設置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設置する場所を決定する必要があります。

手順

1. 『ラックの安全上の注意』 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_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。
   - 最初に、ラックの下の方の段からシステム装置を取り付けるように計画します。
   - 計画に EIA (Electronic Industries Alliance (米国電子工業会)) の位置を記録します。
3. 必要な場合は、6 ページの図 1 に示すように、装置を設置するラック・エンクロージャー内にアクセスできるように、フィラー・パネルを取り外します。

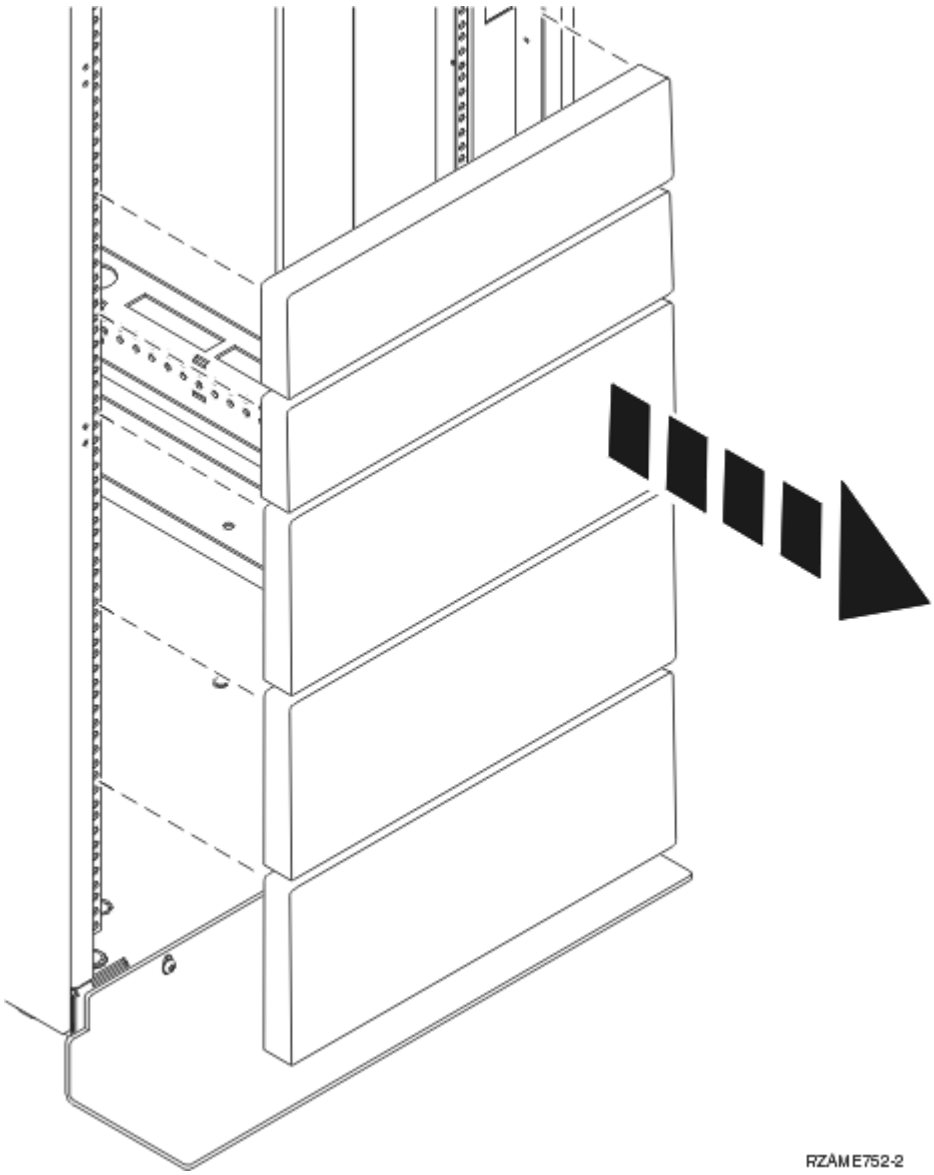


図 *1.* フィラー・パネルの取り外し

4. ラック内の、システムを設置する場所を決定します。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、マーカー、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 6 ページの『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。
11. 7 ページの『システム・シャーシおよびラックへの調整可能レールの取り付け』 に進んで、調整可能レールを取り付けるか、または 8 ページの『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』 に進んで、固定レールを取り付けます。

システム・シャーシおよびラックへの調整可能レールの取り付け

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。

このタスクについて

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またはスペーサーを使用して取り付けないでください。 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 : ラックでの 1 EIA 単位は、垂直方向への 44.45 mm (1.75 インチ) の増分で測定されます。44.45 mm (1.75 インチ) の増分を「EIA」と呼びます。国によっては、同じ増分が「U」と呼ばれることがあります。

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。

- 6.35 mm のプラスねじ 4 本
- ラックとスライド・ブラケット・レールのアセンブリー 2 個
- HMC スライド・ブラケット 2 個
- 四角の EIA 取り付け穴用のナット・クリップ 10 個
- 丸い EIA 取り付け穴用のナット・クリップ 10 個
- M5 六角フランジねじ 10 本

手順

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. HMC のラック内で 1U のスペースを識別します。
3. スライド・ブラケットを HMC に取り付けるには、以下の作業を行います。
   a. 右スライド・ブラケットを識別します。
   b. 右スライド・ブラケットの穴を、HMC の右側にあるスライド・ブラケット・ピンの位置に正しく合わせます。すべてのピンがブラケットの穴に正しく位置合わせされていることを確認します。
   c. HMC スライド・ブラケットがしっかり所定の位置に収まるまで、HMC の背面方向にスライド・ブラケットを押します。
   d. 6.35 mm のプラスねじ 2 本をねじ穴に取り付けて、右スライド・ブラケットを HMC ワークステーションの右側に固定します。
   e. ステップ 7 ページの『3.a』 から 7 ページの『3.d』 までを繰り返して、左スライド・ブラケットを HMC ワークステーションの左側に取り付けます。
4. ラックの前面に移動します。
   a. 左側で、HMC 用に指定された 1U スロット内のラックの前端にある 3 個の穴に 3 個のナット・クリップを取り付けます。

      注 : レール・キットには、四角のラック穴と丸いラック穴の両方に専用のナット・クリップが含まれています。必ず、ラックの穴に適合する正しいナット・クリップを使用してください。
   b. ラックの右側でステップ 7 ページの『4.a』 を繰り返します。
5. ラックの背面に移動します。
   a. 左側で、HMC 用に指定されている 1U スロット内のラックの前端にある上位の穴と下位の穴に 2 個のナット・クリップを取り付けます。

注 : 真ん中の穴は空にしておく必要があります。

b. ラックの右側でステップ 7 ページの『5.a』 を繰り返します。

6. HMC スライド・レールをラックに取り付けるには、以下のステップを実行します。

a. ラックの奥行きを測定します。奥行きは、558.8 mm (22 インチ) から 863.6 mm (34 インチ) までになければなりません。

b. HMC スライド・レールを平らな面に置き、事前取り付け済みのねじを確認します。

注 : スライド・レールには、ねじ穴が 4 つあります。

c. スライド・レールを容易に動かせるように、レールの事前取り付け済みのねじを緩めます。

d. ステップ 8 ページの『6.a』 で測定したラックの奥行きに基づいて、レールのねじを調整する必要があります。

i) ラックの奥行きが 558.8 mm (22 インチ) から 698.5 mm (27.5 インチ) までの場合は、最初の穴と 3 つ目の穴にねじを取り付けます。

ii) ラックの奥行きが 698.5 mm (27.5 インチ) から 863.6 mm (34 インチ) までの場合は、2 つ目の穴と 4 つ目の穴にねじを取り付けます。

注 :

- 最初の穴は、常に、スライド・レールの端に最も近い穴です。3 つ目の穴と 4 つ目の穴は、直ぐ近くにあります。
- スライド・レールをラックに取り付けるときにレールの長さをいくらか調整できるほどにねじが緩んでいるようにします。

7. ラックの前面で、以下のステップを実行して HMC スライド・レールをラックに取り付けます。

a. 左スライド・レール・アセンブリーを見つけます。

b. レール・アセンブリーの方向を、最も近いねじ穴 (最初の穴) がある端が最初にラックに入るように合わせます。ねじ頭がラックの内側に向いていることを確認します。レール・アセンブリーの開放スロットが、ラックの前面に最も近くなります。

c. ラックの左側で、2 本の M5 ねじを使用して、スライド・レールの端のフランジをラックの前端につなぎます。真ん中のねじ穴は開いたままにします。HMC を挿入できるように、ラックの前面でレール・アセンブリーが少し緩くなっているようにします。

8. ラックの背面右側で、スライド・レールの固定されていない方の端を背面方向に引っ張り、2 本の M5 ねじを使用してスライド・レールのフランジをラックに固定します。真ん中のねじ穴は開いたままにします。

9. ステップ 8 ページの『7』 とステップ 8 ページの『8』 を繰り返して、ラックの右側に右スライド・レール・アセンブリーを取り付けます。

10. ラックの前面で、以下のステップを実行して HMC ワークステーションをラックに取り付けます。

a. HMC ワークステーションを水平に保ちながら、スライド・ブラケットを、前のステップで取り付けた HMC スライド・レールに差し込みます。HMC の前面にあるフランジがラック前面の開いたねじ穴にぴったり付くまで、HMC を前方に押します。

b. M5 ねじを 1 本使用して、HMC をフレームの左側につなぎます。ラックの右側で、このステップを繰り返します。

11. 10 ページの『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』 から続行します。

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。

このタスクについて

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またはスペーサーを使用して取り付けないでください。 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 : ラックでの 1 EIA 単位は、垂直方向への 44.45 mm (1.75 インチ) の増分で測定されます。44.45 mm (1.75 インチ) の増分を「EIA」と呼びます。国によっては、同じ増分が「U」と呼ばれることがあります。

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。

- 6.35 mm のプラスねじ 4 本
- 内側レール 2 本
- HMC サポート・レール 2 本
- 四角の EIA 取り付け穴用のナット・クリップ 2 個
- 丸い EIA 取り付け穴用のナット・クリップ 2 個
- M5 六角フランジねじ 8 本

手順

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. HMC のラック内で 1U のスペースを識別します。
3. 内側レールを HMC に取り付けるには、以下の作業を行います。
   a. 右内側レールを識別します。
   b. 内側レールの穴を、HMC の右側にある内側レール・ピンの位置に正しく合わせます。すべてのピンが内側レールの穴に正しく位置合わせされていることを確認します。
   c. HMC の内側レールがしっかり所定の位置に収まるまで、HMC の前面方向に内側レールを押します。
   d. 6.35 mm のプラスねじ 2 本をねじ穴に取り付けて、右内側レールを HMC ワークステーションの右側に固定します。
   e. ステップ 3.a から 9 ページの『3.d』 までを繰り返して、左内側レールを HMC ワークステーションの左側に取り付けます。
4. ラックの前面に移動します。左側で、HMC 用に指定されている 1U スロット内のラックの前端にある穴にナット・クリップを 1 個取り付けます。

   注 : レール・キットには、四角のラック穴と丸いラック穴の両方に専用のナット・クリップが含まれています。必ず、ラックの穴に適合する正しいナット・クリップを使用してください。
5. ラックの背面に移動します。左側で、HMC 用に指定されている 1U スロット内のラックの前端にある真ん中の穴にナット・クリップを 1 個取り付けます。
6. ラックの前面で、以下のステップを実行して HMC サポート・レールをラックに取り付けます。
   a. サポート・レールのピンを、前のステップで取り付けたナット・クリップの上下に位置合わせします。
   b. ラックの右側で、上位と下位のねじ穴に 2 本の M5 ねじを使用して、サポート・レールの端のフランジをラックの前端につなぎます。真ん中のねじ穴は開いたままにします。HMC を挿入できるように、ラックの前面でレール・アセンブリーが少し緩くなっているようにします。
7. ラックの背面右側で、サポート・レールの固定されていない方の端を背面方向に引っ張り、2 本の M5 ねじを使用してサポート・レールのフランジをラックに固定します。真ん中のねじ穴は開いたままにします。
8. ステップ 9 ページの『6』 とステップ 9 ページの『7』 を繰り返して、ラックの左側に左サポート・レール・アセンブリーを取り付けます。
9. ラックの前面で、以下のステップを実行して HMC ワークステーションをラックに取り付けます。

a. HMC ワークステーションを水平に保ちながら、内側レールを、前のステップで取り付けた HMC サポート・レールに差し込みます。HMC の前面にあるフランジがラック前面の開いたねじ穴にぴったり付くまで、HMC を前方に押します。

b. M5 ねじを 1 本使用して、HMC をフレームの左側につなぎます。ラックの右側で、このステップを繰り返します。

注 : オレンジ色の配送用ブラケットがシステムの 背面に取り付けられている場合は、それを取り外し、ねじを元どおりに付け直します。

10. 10 ページの『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』から続行します。

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

システムをレール上に設置し、電源ケーブルを接続して配線します。

このタスクについて

注意 : この部品または装置は重量がありますが、重さは 18 kg 未満です。 この部品または装置を持ち上げ、取り外し、または取り付けるときは注意してください。 (C008)

手順

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. 電源コードのプラグを電源装置に差し込みます。

   注 : この時点では、電源コードのもう一方の端を電源に接続しないでください。

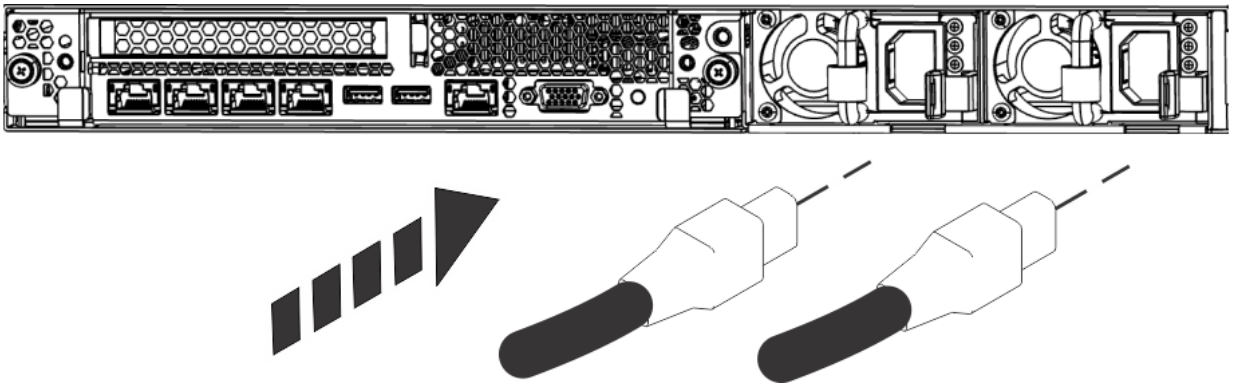


図 2. 電源装置への電源コードのプラグの差し込み

3. 面ファスナーで電源コードを固定します。
4. 10 ページの『ラック・マウント型 7063-CR2 HMC のケーブル接続』から続行します。

ラック・マウント型 7063-CR2 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。

手順

1. HMC がラックに取り付けられており、電源コードが電源装置に接続されていることを確認します。 詳しくは、10 ページの『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』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。
2. キーボード、モニター、およびマウスを接続します。

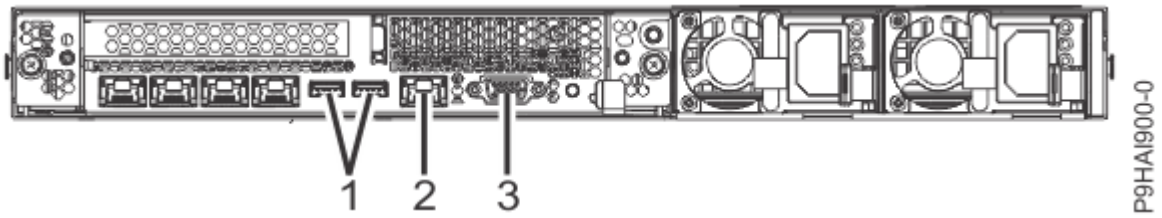


図 *3.* 背面ポート

表 *4.* 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	モニターに使用される Video Graphics Array (VGA)。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。

注 : システムには使用可能な 2 つの前面 USB ポートがあります。

3. 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

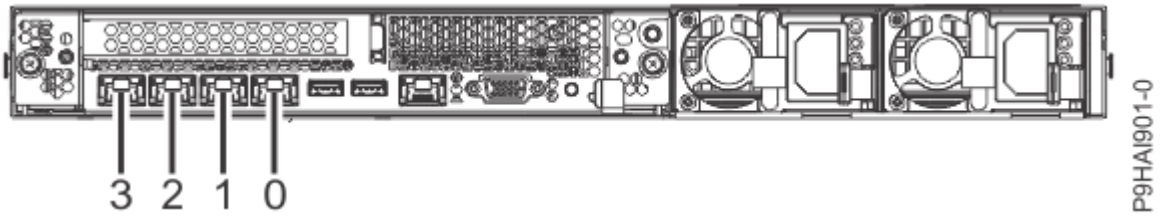


図 *4.* イーサネット・ポート

表 *5.* イーサネット・ポート	
ID	**説明**
0	共用イーサネット Intelligent Platform Management Interface (IPMI) と HMC のネットワーク接続
1、2、および 3	HMC ネットワーク接続

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、38 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。

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。詳しくは、IBM にお問い合わせください。

4. 管理対象システム (複数可) に接続するためのイーサネット・ケーブルを接続します。

注 :

- IPMI と HMC に共用接続を使用している場合、図 2 のポート 0 へのケーブルが 1 本あれば、IPMI と HMC の両方の必要を満たします。
- HMC ネットワーク接続の詳細については、37 ページの『HMC ネットワーク接続』を参照してください。

5. 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。
6. 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。
7. 電源機構 LED をインディケーターとして使用して、電源状況を確認します。詳しくは、『7063-CR2 システムの LED7063-CR2 システムの LED』を参照してください。
8. 電源ボタンを押して、システムを始動します。パワーオン表示ライトが明滅を停止して点灯したままになり、システムの電源がオンになったことを示します。

タスクの結果

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。12 ページの『7063-CR2 HMC の構成』から続行します。

7063-CR2 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。

HMC に付属の HMC バージョンを確認します。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方法については、『HMC に付属の HMC バージョンの確認』を参照してください。Fix Central Web サイトから、使用可能な最新の 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 : 以下の表では、HMC インターフェースおよび BMC インターフェースの 事前定義 (デフォルト) のログイン情報について説明します。

表 *6.*

コンソールまたはインターフェース	デフォルト ID	デフォルトのパスワード	説明
BMC (OpenBMC)	`root`	`0penBmc`	root ユーザー ID およびパスワードは、初めて BMC にログインする際に使用します。
HMC	`hscroot`	`abc123`	hscroot ユーザー ID およびパスワードは、初めて HMC にログインする際に使用します。 これらは大/小文字の区別があり、スーパー管理者のロールを持つメンバーのみが使用できます。
HMC	`root`	`passw0rd`	root ユーザー ID およびパスワードは、保守手順を実行するためにサービス・プロバイダーが使用します。 この ID やパスワードを使用して HMC にログインすることはできません。

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。

注 : 各種オペレーティング・システムでの例については、以下を参照してください。

- Windows: USB flash installation media (Windows)
- Mac: USB flash installation media (macOS)

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 ドライブが挿入されている場合、Linux コマンド `lsblk` を実行して、そのデバイス名を判別できます。
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。

   注 : USB ドライブは、少なくとも 8 GB でなければなりません。特定の USB ドライブは、幅が広すぎてシステムの背面にある USB ポートに正しく収まらない場合があります。先に進む前に、USB ドライブが適合しているかどうかテストしてください。
4. Petitboot メニューが表示されたら、「**USB**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

BMC から仮想メディアを使用しての HMC のインストール

BMC から仮想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. サポートされる Web ブラウザーを開きます。アドレス・バーに、接続する BMC の IP アドレスを入力します。 例えば、Web ブラウザーのアドレス・バーでは `https://<BMC IP>` の形式を使用できます。
2. 「**OpenBMC ログオン (OpenBMC logon)**」ウィンドウで、BMC の「**ホスト**」アドレスと、割り当てられた「**ユーザー名**」および「**パスワード**」を入力します。

   注 : デフォルトのユーザー ID は `root`、デフォルトのパスワードは `0penBmc` です。

   ファームウェア・レベル OP940.01 以降を使用する場合、root パスワードはデフォルトで有効期限切れになります。BMC にアクセスする前に、デフォルト・パスワードを変更する必要があります。有効期限が切れたデフォルトのパスワードの変更について詳しくは、『パスワードの設定』を参照してください。

   パスワードを忘れた場合は、システムを工場出荷時状態にリセットすることで、デフォルト・パスワードを復元できます。 システムをリセットするには、『工場出荷時状態へのリセットの実行』を参照してください。
3. 「**ログイン**」をクリックします。
4. 「**サーバー制御 (Server control)**」を選択します。
5. 「**仮想メディア (Virtual Media)**」を選択します。
6. 「**ファイルの選択 (Choose file)**」をクリックします。
7. HMC リカバリー・メディア ISO を見つけて、「**開く (Open)**」をクリックします。
8. 「**開始**」をクリックします。
9. システムの電源をオンにします。
10. Petitboot メニューが表示されたら、「**USB**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

外付け USB 接続 DVD ドライブを使用した HMC のインストール

外付け USB 接続 DVD ドライブを使用して HMC をインストールするには、以下の手順を実行します。

1. Fix Central Web サイトから、必要な HMC リカバリー・バージョンをダウンロードします。
2. HMC リカバリー DVD イメージを、イメージとして DVD-R DL メディアに焼き付けます。
3. HMC の電源をオフにします。
4. 外付け USB DVD ドライブを HMC に接続し、HMC リカバリー DVD を挿入します。

   注 : DVD ドライブに十分な電力を供給するために、USB DVD ドライブを外部電源に接続するか、USB Y ケーブルを使用して追加の USB ポートに接続することが必要な場合があります。
5. HMC の電源をオンにします。

   注 : 始動中は、表示モニターに信号が何も表示されないことがあります。表示モニターに何かの状況が表示されるまで、処理に 2 分か 3 分かかる場合があります。
6. Petitboot ブート・ローダーが始動したら、ナビゲートして自動ブートを停止してください。

   注 : 10 秒のタイムアウトが強制的に適用されます。10 秒以内にアクションを取らないと、システムはハード・ディスクからブートしようとします。
7. Petitboot メニューに「**CD/DVD**」デバイスが表示されるまで待ってください。

   注 : この処理には最大 1 分かかることがあります。
8. 「**CD/DVD**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

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。

オンラインの設置資料を表示するか、または同じ資料の PDF バージョンを印刷できます。PDF バージョンを表示または印刷するには、「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」を参照してください。

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。

このタスクについて

注意 :

または

または

この部品または装置の重量は 18 kg から 32 kg です。 この部品または装置を安全に持ち上げるには、2 人の人員が必要です。 (C009)

サーバーの設置を開始する前に、以下の資料を読むことが必要になる場合があります。

- この資料の最新版は、オンラインで維持されています。ラックへの 7063-CR1 の設置 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm)を参照してください。
- サーバーの設置を計画する場合は、サイトおよびハードウェア計画を参照してください。

手順

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ます。

- サイズ 2 のプラス・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
- 1 EIA (米国電子工業会) 単位 (1U) 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・フィーチャー』 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_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。

手順

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、部品が揃っていることを確認し、注文した部品をすべて受け取っていることを確認してください。

   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 システムを設置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。

手順

1. 『ラックの安全上の注意』 (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_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。
   - 最初に、ラックの下の方の段からシステム装置を取り付けるように計画します。
   - 計画に EIA (Electronic Industries Alliance (米国電子工業会)) の位置を記録します。
3. 必要な場合は、16 ページの図 5 に示すように、装置を設置するラック・エンクロージャー内にアクセスできるように、フィラー・パネルを取り外します。

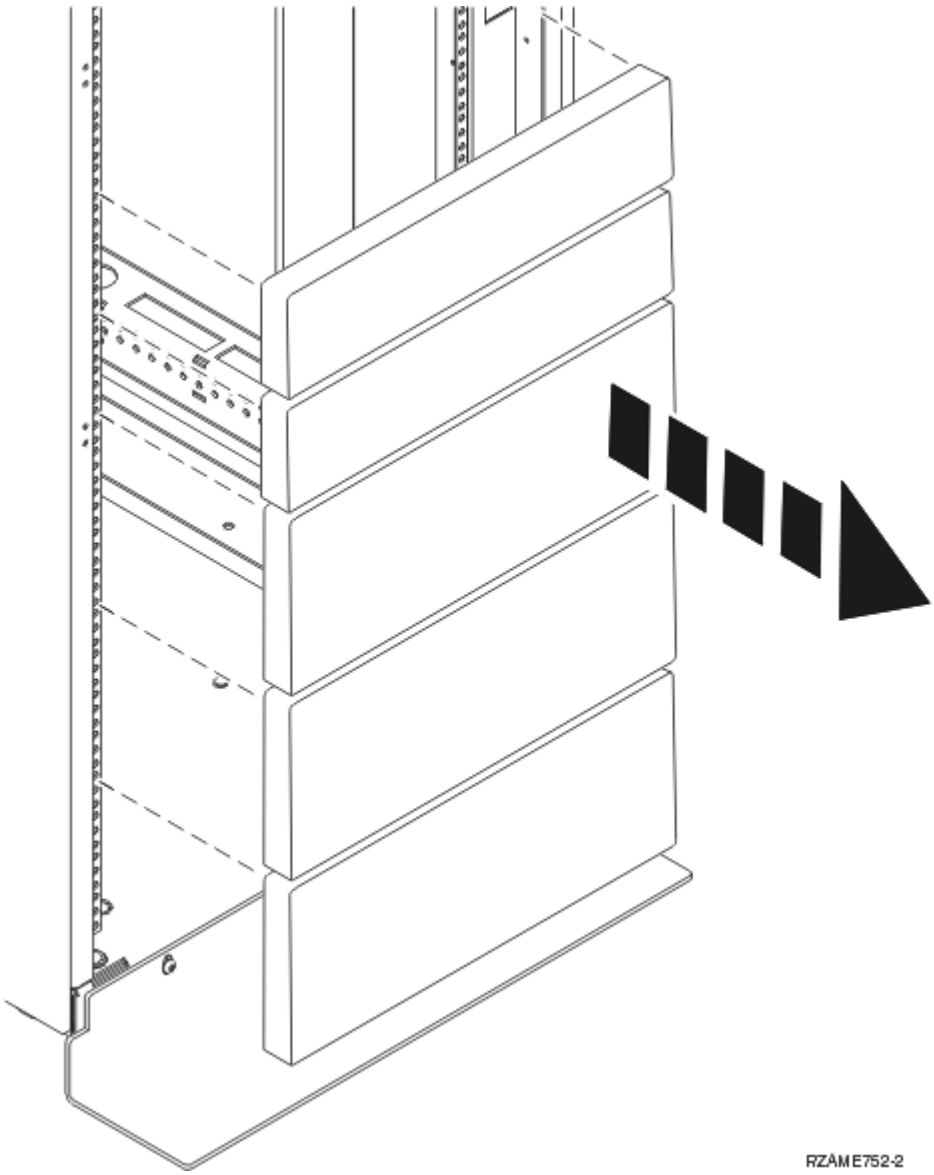


図 5. フィラー・パネルの取り外し

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、マーカー、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 16 ページの『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。

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。

このタスクについて

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またはスペーサーを使用して取り付けないでください。 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。

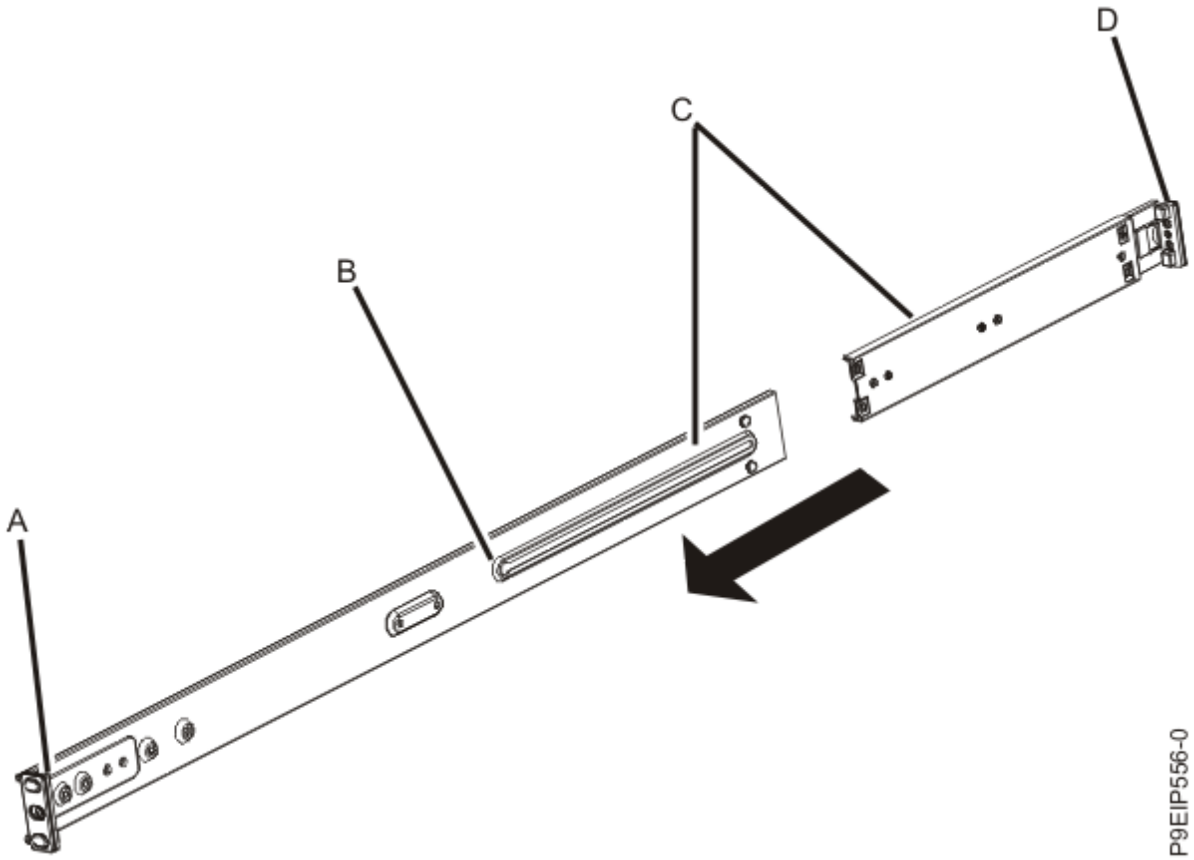
注 : システムには、1 EIA ラック単位 (1U) のスペースが必要です。

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)。

手順

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. レール・ラックの正方形のピン (**A**) および (**D**) をレール・ラックの丸いピンと交換します。
3. 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 本のスレッド・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。

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。

注 : レールのねじにアクセスしてしっかり締めるには 2U のスペースが必要な場合があります。

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。

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

システムをレール上に設置し、電源ケーブルを接続して配線します。

このタスクについて

注意 :

この部品または装置の重量は 18 kg から 32 kg です。 この部品または装置を安全に持ち上げるには、2 人の人員が必要です。 (C009)

手順

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. システムの両側に 1 人ずつ立ち、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. システムを、ラックの後部の方へ静かに押します。
5. システム・シャーシの両側にあるハンドルにワッシャー付きねじを差し込んで回し、システムをラックに固定します。

注 : ワッシャー付きねじを使用する必要があります。レール・キットに含まれている長い方の 2 本のねじ (1.5 cm (0.59 インチ)) のそれぞれにワッシャーをはめてスライドさせます。システムの前面から、左右両側にワッシャー付きねじを差し込んで回します。

6. 電源コードのプラグを電源装置に差し込みます。

   注 : この時点では、電源コードのもう一方の端を電源に接続しないでください。

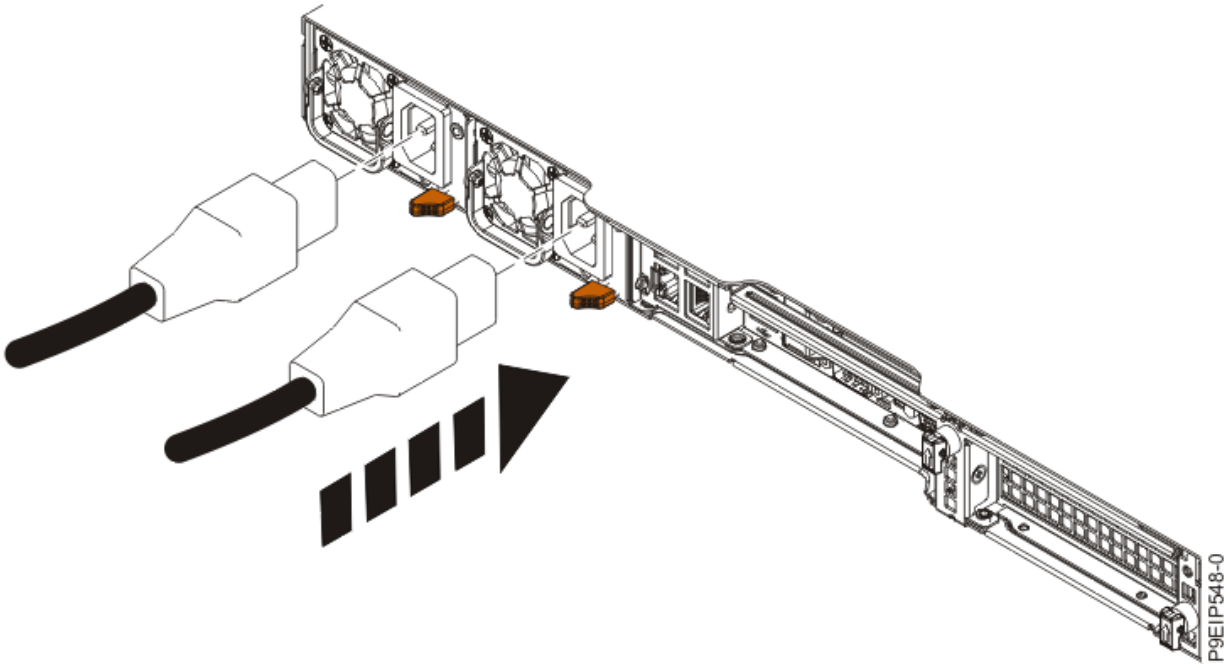


   図 6. 電源装置への電源コードのプラグの差し込み

7. 19 ページの『ラック・マウント型 7063-CR1 HMC のケーブル接続』から続行します。

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。

手順

1. HMC がラックに取り付けられており、電源コードが電源装置に接続されていることを確認します。 詳しくは、18 ページの『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』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。

   注 : システムの背面で使用する必要があるポートをプラグが覆っている場合は、そのプラグを取り外して廃棄してください。ポート・カバーがあると、初期システム IPL 時に管理対象システムで 管理者パスワードのリセットが必要であることを必ず思い出します。

2. キーボード、モニター、およびマウスを接続します。

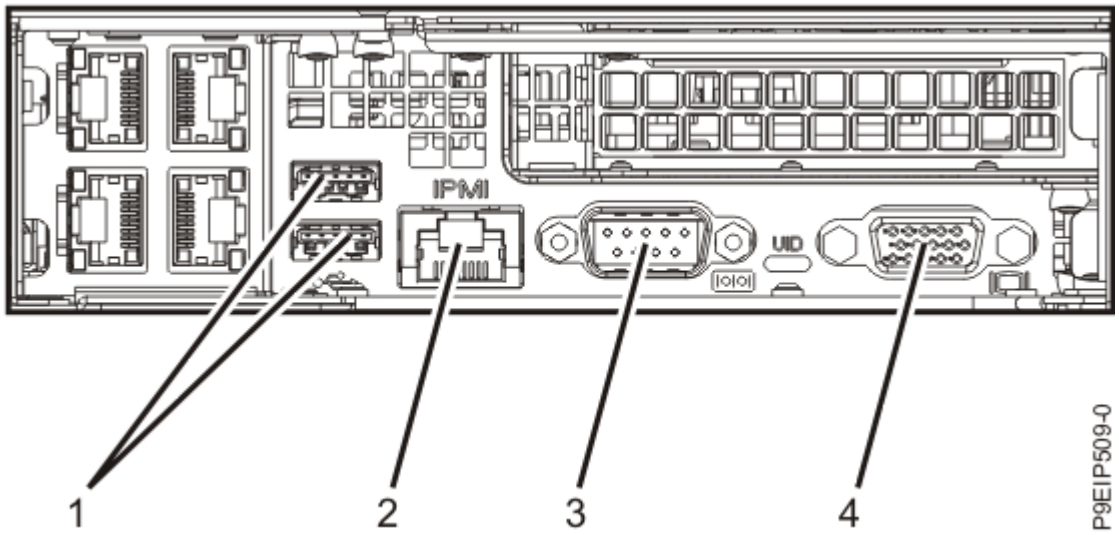


図 7. 背面ポート

表 7. 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	モニターに使用される Video Graphics Array (VGA)。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。

注 : システムには使用可能な 2 つの前面 USB ポートがあります。前面のシリアル・ポートは機能していません。

3. 管理対象システム (複数可) に接続するためのイーサネット・ケーブルを接続します。

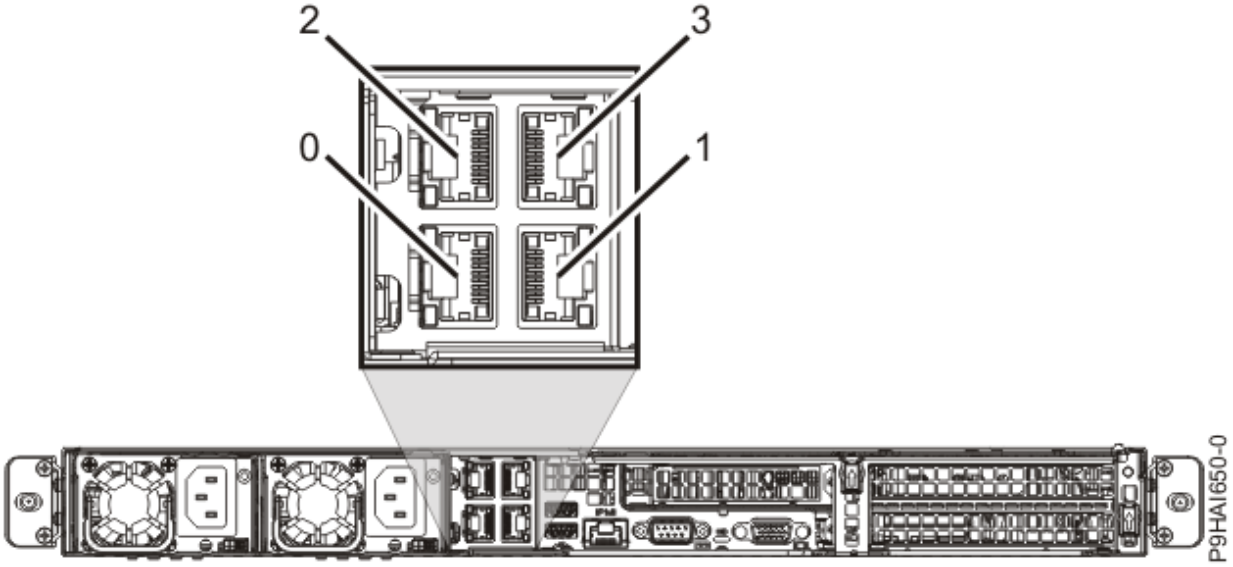


図 8. イーサネット・ポート

注 : HMC ネットワーク接続の詳細については、37 ページの『HMC ネットワーク接続』を参照してください。

4. 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。
5. 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、38 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。

6. 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。
7. 電源機構 LED をインディケーターとして使用して、電源状況を確認します。詳しくは、7063-CR1 システムの LED7063-CR1 システムの LED を参照してください。

タスクの結果

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。21 ページの『7063-CR1 HMC の構成』から続行します。

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。

HMC に付属の HMC バージョンを確認します。Fix Central Web サイトから、使用可能な最新の 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 : 以下の表では、HMC インターフェースおよび BMC インターフェースの 事前定義 (デフォルト) のログイン情報について説明します。

表 *8.*

コンソールまたはインターフェース	デフォルト ID	デフォルトのパスワード	説明
BMC	ADMIN	ADMIN	ADMIN ユーザー ID およびパスワードは、初めて BMC にログインする際に使用します。
HMC	hscroot	abc123	hscroot ユーザー ID およびパスワードは、初めて HMC にログインする際に使用します。 これらは大/小文字の区別があり、スーパー管理者のロールを持つメンバーのみが使用できます。
HMC	root	passw0rd	root ユーザー ID およびパスワードは、保守手順を実行するためにサービス・プロバイダーが使用します。 この ID やパスワードを使用して HMC にログインすることはできません。

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。

注 : 各種オペレーティング・システムでの例については、以下を参照してください。

- Windows: USB flash installation media (Windows)
- Mac: USB flash installation media (macOS)

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 ドライブが挿入されている場合、Linux コマンド `lsblk` を実行して、そのデバイス名を判別できます。
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。

   注 : USB ドライブは、少なくとも 4 GB でなければなりません。特定の USB ドライブは、幅が広すぎてシステムの背面にある USB ポートに正しく収まらない場合があります。先に進む前に、USB ドライブが適合しているかどうかテストしてください。
4. Petitboot メニューが表示されたら、「**USB**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

コンソール・ビューアーからリモート・メディアを使用しての 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。
10. Petitboot メニューが表示されたら、「**CD/DVD**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

外付け USB 接続 DVD ドライブを使用した HMC のインストール

外付け USB 接続 DVD ドライブを使用して HMC をインストールするには、以下の手順を実行します。

1. Fix Central Web サイトから、必要な HMC リカバリー・バージョンをダウンロードします。
2. HMC リカバリー DVD イメージを、イメージとして DVD-R メディアに焼き付けます。もう 1 つの方法として、DVD に入ったリカバリー・メディアを注文することもできます。
3. HMC の電源をオフにします。
4. 外付け USB DVD ドライブを HMC に接続し、HMC リカバリー DVD を挿入します。

   注 : DVD ドライブに十分な電力を供給するために、USB DVD ドライブを外部電源に接続するか、USB Y ケーブルを使用して追加の USB ポートに接続することが必要な場合があります。
5. HMC の電源をオンにします。

注 : 始動中は、表示モニターに信号が何も表示されないことがあります。表示モニターに何かの状況が表示されるまで、処理に 2 分か 3 分かかる場合があります。

6. Petitboot ブート・ローダーが始動したら、ナビゲートして自動ブートを停止してください。

   注 : 10 秒のタイムアウトが強制的に適用されます。10 秒以内にアクションを取らないと、システムはハード・ディスクからブートしようとします。

7. Petitboot メニューに「**CD/DVD**」デバイスが表示されるまで待ってください。

   注 : この処理には最大 1 分かかることがあります。

8. 「**CD/DVD**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

SMB ファイル・サーバーでホストされるリモート・メディアを使用しての HMC のインストール

Server Message Block (SMB) ファイル・サーバーでホストされるリモート・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. リカバリー ISO ファイルを SMB 準拠のファイル・サーバー上の共有ホストにコピーします。

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

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

   共有ホスト

   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。

6. 「**保管**」をクリックします。
7. 「**マウント**」をクリックします。
8. 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 6 からステップ 8 を繰り返します。

9. システムの電源をオンにします。
10. Petitboot メニューが表示されたら、「**CD/DVD**」の下にある「**ハードウェア管理コンソールのインストール (Install Hardware Management Console)**」オプションを選択します。

オプション: 組み込まれている USB メモリー・キーを使用した、HMC ファームウェア・レベルの更新

注 : 構成に USB メモリー・キーについての HMC ファームウェア更新が含まれていた場合は、以下のステップを実行して、HMC ファームウェア・レベルを更新してください。

組み込まれている USB メモリー・キーを使用して、HMC ファームウェア・レベルを更新するには、以下のステップを実行します。

1. USB メモリー・キー・ドライブを、システムの背面にある USB ポートに差し込みます。
2. システムの電源をオンにして、HMC にログオンします。
3. 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。
4. 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。
5. 「HMC 修正サービスのインストール」ウィザードで画面に示される手順に従います。

次に、HMC ソフトウェアの構成が必要です。手順については、37 ページの『HMC の構成』を参照してください。

関連概念

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 では、以下の POWER 仮想化ハイパーバイザーをサポートします。

- PowerVM®

HMC 仮想アプライアンスを稼働するための最小要件:

- 16 GB のメモリー
- 仮想プロセッサー 4 個
- ネットワーク・インターフェース 2 つ (最大 4 個可能)
- 500 GB の空きディスク・スペースを含むディスク・ドライブ 1 個

注 :

- HMC 仮想アプライアンスをホスティングするシステム 上のプロセッサーは、Intel VT-x または AMD-V ハードウェア仮想化対応プロセッサーでなければなりません。
- 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。
- 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。
- PowerVM 仮想化ハイパーバイザーは、160 GB のディスク・スペースを必要とします。ただし、500 GB のメモリーをお勧めします。
- PowerVM プロセッサーは、最小限 1.0 処理装置と上限ありの共用モードの 4 個の共用仮想プロセッサーです。専用プロセッサーの使用はお勧めしません。 PowerVM プロセッサーでは、16 GB のメモリーも必要です。

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 7.0 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。
   f. Activation Engine を使用している場合は、「**AEDISK**」を Activation Engine の仮想ディスク・イメージの名前に置き換えます。それ以外の場合は、ディスク・エレメントを除去します。
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. 定義済み VM のリストに仮想 HMC が追加されたことを確認するために、コマンド virsh list --all を実行します。
9. VM を始動するために、コマンド virsh start vHMC を実行します。
10. 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。
11. 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 がリブートされるときに、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 6.0 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。

POWER での HMC 仮想アプライアンスのインストール

仮想 POWER 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。

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。

ファームウェア・レベル FW910 以降では、HMC 仮想アプライアンス は POWER9 サーバーをサポートします。詳しくは、Supported Linux distributions for POWER8® and POWER9 Linux on Power systems (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm)を参照してください。

注 :

1. HMC 仮想アプライアンス をホストするサーバーを管理することはできません。
2. この HMC 仮想アプライアンス をホストしているサーバーを別の HMC 仮想アプライアンス が管理している場合、その HMC 仮想アプライアンス をホストしているサーバーを管理することはできません。

   例えば、HMC 仮想アプライアンス A がサーバー A で稼働しており、HMC 仮想アプライアンス B がサーバー B で稼働しているとします。このとき、HMC 仮想アプライアンス A がサーバー B を管理するのと同時に、HMC 仮想アプライアンス B がサーバー A を管理することはできません。一方の HMC 仮想アプライアンス が他方のサーバーを管理することはできますが、両方の HMC 仮想アプライアンス が相互のサーバーを同時に管理することはできません。

自動 HMC インストール・イメージの作成 (オプション)

「**HMC インストール**」ウィザードのプロンプトを出さずに、HMC 仮想アプライアンス を自動的にインストールする、自動 HMC インストール・イメージを作成することができます。

注 : PowerVM 上の HMC 仮想アプライアンス では、区画に割り当てられているアダプターのグラフィックス・アダプター・サポートを提供していません。サポートされる Web ブラウザーを使用して HMC に接続することによって、ユーザー・インターフェース ・サポートを得られます。

自動 HMC インストール・イメージを作成するには、以下のステップを実行します。

1. コマンド mkdir -p oldiso および mkdir -p newiso を実行して、ディレクトリーを 2 つ作成します。
2. コマンド sudo mount -o loop <イメージ・パス> oldiso を実行して、HMC インストール・イメージを **oldiso** ディレクトリーにマウントします。
3. コマンド cp -r oldiso/* newiso を実行して、**oldiso** ディレクトリーの内容を **newiso** ディレクトリーにコピーします。

4. コマンド `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg` を実行して、自動インストール用の Grub ファイルを編集します。
5. コマンド `sudo chown 0444 newiso/boot/grub/grub.cfg` を実行して、Grub ファイルを読み取り専用にします。
6. コマンド `mkisofs -o <新規 iso 名> -V <ISO ラベル> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso` を実行して、新規の HMC インストール ISO を作成します (ここで **ISO label** は、`HMC-8.0.870.0` など、`HMC-<hmc バージョン・リリース番号>` にする必要があります)。

注 : Activation Engine および構成ファイルのセットアップについて詳しくは、31 ページの『HMC 仮想アプライアンスに対する Activation Engine の使用』を参照してください。

論理ボリュームのセットアップ

論理ボリュームをセットアップするには、以下の手順を完了します。

1. 管理対象システムを選択します。
2. メニュー・ポッドで、「**システム・アクション**」 > 「**Power VM**」 > 「**仮想ストレージ**」を選択します。
3. 「**システム VIOS の管理 (Manage System VIOS)**」 > 「**アクション**」 > 「**仮想ストレージの管理**」を選択します。
4. 「**仮想ディスク**」タブを選択します。
5. 「**仮想ディスクの作成**」をクリックし、以下の情報を入力します。
   - 「**仮想ディスク名**」: 仮想ディスクの名前。
   - 「**ストレージ・プール名**」: ストレージ・プールの名前。
   - 「**仮想ディスク・サイズ**」: 仮想ディスクのサイズ。
   - 「**割り当て区画**」: 論理区画の名前。

   注 : 最小 160 GB のディスク・スペースが必要です (500 GB のディスク・スペースが推奨されます)。

インストール・メディアのセットアップ - メディア・ライブラリーの作成

メディア・ライブラリーを作成するには、以下の手順を実行します。

1. 管理対象システムを選択します。
2. メニュー・ポッドで、「**システム・アクション**」 > 「**Power VM**」 > 「**仮想ストレージ**」を選択します。
3. 「**システム VIOS の管理 (Manage System VIOS)**」 > 「**アクション**」 > 「**仮想ストレージの管理**」を選択します。
4. 「**光ディスク装置**」タブを選択します。
5. 「**ライブラリーの作成**」をクリックし、以下の情報を入力します。
   - 「**ストレージ・プール**」: ストレージ・プールの名前。
   - 「**メディア・ライブラリー・サイズ**」: メディア・ライブラリーのサイズ。
6. 「**了解**」をクリックします。

インストール・メディアのセットアップ - VIOS へのメディアのアップロード

メディアを Virtual I/O Server (VIOS) にアップロードするには、以下の手順を実行します。

1. VIOS にログインします。
2. VIOS ルート・モードで、コマンド `oem_setup_env` を実行します。
3. NFS 接続を許可するために、コマンド `nfso -o nfs_use_reserved_ports=1` を実行します。
4. NFS をローカル VIOS フォルダーにマウントするために、コマンド `mount <サーバー IP>:/Mountpoint <ローカル・フォルダー>` を実行します。

5. NFS マウントにご使用の HMC インストール ISO および Activation Engine 構成イメージ (オプション) が含まれていることを確認するには、コマンド `ls` を実行します。

インストール・メディアのセットアップ - メディア・ライブラリーへのメディアのリンク

メディア・ライブラリーにメディアをリンクするには、以下の手順を実行します。

1. 「**システム VIOS の管理 (Manage System VIOS)**」 > 「**アクション**」 > 「**仮想ストレージの管理**」に戻り、「**光ディスク装置**」タブを選択します。
2. 「**仮想光メディア**」セクションで、「**アクション**」メニューから「**メディアの追加**」を選択します。
3. 「**仮想メディアの追加**」ウィンドウで、「**VIOS ファイルシステムからの既存ファイルの追加**」を選択し、以下の情報を入力します。
   - 「**メディア名**」: メディアの名前 (`HMCInstall` または `AEDrive` など)。
   - 「**光メディアのファイル名**」: インストール ISO ファイルのファイル名 (`01234567-ppc64ie.iso` など)。
4. 「**了解**」をクリックします。
5. Activation Engine 構成イメージを作成した場合は、ステップ 3 から 4 を繰り返して、Activation Engine 構成イメージを追加してください。それ以外の場合は、ステップ 6 に進みます。
6. メディア名が「**仮想光メディア**」リストに表示されたかどうかを調べて、光メディアがメディア・ライブラリーにアップロードされたことを確認してください。

論理区画のセットアップ

論理区画をセットアップするには、以下の手順を完了します。

1. 管理対象システムを選択します。
2. メニュー・ポッドで、「**システム・アクション**」 > 「**区画**」 > 「**区画**」を選択します。
3. 「**区画の作成**」をクリックし、以下の情報を入力します。
   - 「**区画の名前**」: 区画の名前。
   - 「**区画 ID**」: 区画の ID。
   - 「**区画タイプ**」: 選択するオペレーティング・システム (「**AIX/Linux**」または「**IBM i**」)。
4. 「**了解**」をクリックします。
5. 区画用のプロセッサー数とメモリー容量を割り振ります。

   注 : 最小 4 個の仮想プロセッサーと 8 GB のメモリーが必要です。
6. メニュー・ポッドで、「**区画アクション**」 > 「**仮想 I/O**」 > 「**仮想ネットワーク**」を選択します。
7. jp「**仮想ネットワークの接続 (Attach Virtual Network)**」をクリックして、「**新規イーサネット・アダプターの表示および接続 (Show and attach new virtual ethernet adapters)**」チェック・ボックスを選択します。テーブルから、論理区画に接続したい仮想ネットワーク・アダプターを 選択します。

   注 : 許可される仮想ネットワーク・アダプターは最大 4 個です。
8. メニュー・ポッドで、「**区画アクション**」 > 「**仮想 I/O**」 > 「**仮想ストレージ**」を選択します。
9. 「**仮想光ディスク装置**」タブで、「**仮想光ディスク装置の追加**」をクリックします。
10. 「**デバイス名**」 (`HMCInstall` または `AEDrive` など) を入力し、必要なバーチャル I/O サーバーを表から選択します。

    注 : `AEDrive` のインストールはオプションです。
11. 「**了解**」をクリックします。
12. ステップ 10 で追加した仮想光ディスク装置が表にリストされていることを確認します。
13. 「**アクション**」メニューで、「**ロード**」をクリックします。
14. 論理区画に割り当てるメディア・ファイルを選択し、「**OK**」をクリックします。

15. ステップ 13 でロードした仮想光ディスク装置が表にリストされていることを確認します。

HMC 仮想アプライアンス の始動

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 に開始するには、以下のステップを完了します。

1. 管理対象の区画を選択します。
2. 「**アクション**」 > 「**コンソール**」 > 「**端末ウィンドウを開く**」を選択して、論理区画へのアクティブな接続を開きます。
3. 「**アクション**」 > 「**活動化**」を選択して、論理区画を活動状態にします。
4. 「**活動化 (通常)**」および「**現在の構成**」を選択します。
5. 「**完了**」をクリックします。
6. 端末ウィンドウを切り替えます。
7. 「**ブート**」メニューで、「**1 = SMS メニュー**」を選択します。
8. 「**メイン**」メニューで、「**5 = ブート・オプションの選択**」を選択します。
9. 「**マルチブート**」メニューで、「**1 = インストール/ブート・デバイスの選択**」を選択します。
10. 「**デバイス・タイプの選択**」メニューで、「**5 = すべてのデバイスのリスト**」を選択します。
11. デバイスの位置に基づいて `HMCInstall` デバイスを選択します。
12. 「**2. 通常モードのブート**」を選択します。
13. 「**1. はい**」を選択して、確定します。
14. 「**HMC インストール**」ウィザードのスクリーン内の指示に従います。

    注 : 自動 HMC インストール・イメージを使用した場合は、このステップをスキップしてください。
15. 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。
16. 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。
17. `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、セキュア・シェル (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 ethX -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>
chhmc -c remotewebui -s enable -i ethX
hmcshutdown -r -t now
```

- 「**ethX**」は、構成するネットワーク・インターフェースの 名前です。
- **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。

注 : 複数の仮想イーサネット・アダプターを 使用する場合は、各インターフェースの HMC 仮想アプライアンス で、コマンド **cat /etc/sysconfig/network-scripts/ifcfg-ethX** を実行します。メディア・アクセス制御 (MAC) アドレスを、HMC が区画の仮想ネットワークのアダプター・ビューに表示するものと比較します。仮想イーサネット・アダプターについて詳しくは、「**仮想イーサネット・アダプター設定の表示**」をクリックします。このステップは、使用する正しいインターフェースを 判別するのに役立ちます。

18. 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 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、32 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)
- キーボード・セットアップの 使用不可設定
- ディスプレイ ・セットアップの 使用不可設定
- 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
- ネットワーク・インターフェースを IPv4 DHCP サーバーとして構成
- プライベート・インターフェースおよびオープン ・インターフェースの 構成
- デフォルト・ゲートウェイ・インターフェース ・デバイスの構成

注 : vHMC-Conf.xml 構成ファイルで定義されているイーサネット・アダプターの 数は、**domain.xml**、**vHMC.cfg**、または **VMWare** のいずれかの構成ファイルで定義されているネットワーク・アダプターと 相互に関連付けられている必要があります。

Activation Engine には、XML 構成を保持する仮想ディスクが必要です。テキスト・エディターで **user_data** ファイルを編集して、以下の例に示されている XML 構成ガイドを使用することができます。

Linux 環境で Activation Engine 構成を使用して仮想 ISO ディスク・イメージを作成するには、以下の手順を実行します。

1. ディレクトリーを作成します。

```
mkdir -p config-drive/openstack/latest
```

2. 編集した **user_data** ファイルをそのディレクトリーにコピーします。

```
cp user_data config-drive/openstack/latest
```

3. Activation Engine 構成を使用して仮想ディスク・イメージを作成します。

```
mkisofs -R -V config-2 -o AEdrive.iso config-drive
```

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

以下のサンプルの構成ファイルを使用して、XML タグについて説明します。

```
<vHMC-Configuration>
   <ConfigurationVersion>2.0</ConfigurationVersion>
   <LicenseAgreement></LicenseAgreement>
   <AcceptLicense>Yes</AcceptLicense>
   <Locale>en_US.UTF-8</Locale>
   <SetupWizard>No</SetupWizard>
   <SetupCallHomeWizard>No</SetupCallHomeWizard>
   <SetupKeyboard>No</SetupKeyboard>
   <SetupDisplay>No</SetupDisplay>
   <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
      <Hostname></Hostname>
      <Domain></Domain>
      <DNSServers></DNSServers>
      <IPV4Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Netmask></Netmask>
         <Gateway></Gateway>
      </IPV4Config>
      <IPV6Config>
         <NetworkType></NetworkType>
         <IPAddress></IPAddress>
         <Gateway></Gateway>
      <IPV6Config>
      <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>
         <NTP>Disabled</NTP>
         <SNMPTraps>Disabled</SNMPTraps>
         <SNMPAgents>Disabled</SNMPAgents>
      </Firewall>
   </Ethernet>
   <NTPServers>
      <ntpparam ntpserver="" ntpversion=""/>
   </NTPServers>
</vHMC-Configuration>
```

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、以下のテーブルを使用してください。

表 *9. XML* タグ

タグ	説明	許容値	注
ConfigurationVersion	必須エレメント。使用する構成バージョンを定義します。	**2.0**	
LicenseAgreement	必須エレメント。HMC 仮想アプライアンス の「ご使用条件」を表示します。		

表 9. *XML タグ (続き)*

タグ	説明	許容値	注
AcceptLicense	必須エレメント。HMC 仮想アプライアンス の「ご使用条件」を受け入れます。	• **はい**: HMC の「ご使用条件」を受け入れます。 • **いいえ**: ユーザーに HMC の「ご使用条件」の受け入れを要求します。	無効な値が入力された場合、Activation Engine はデフォルト設定の「**いいえ**」を使用します。
Locale	必須エレメント。ロケール設定を定義します。	**en_US.UTF-8**	無効な値が入力された場合、Activation Engine はデフォルト設定の「**US**」を使用します。
SetupWizard	必須エレメント。「**HMC セットアップ**」ウィザードを有効または無効にします。	• **はい**: 「**HMC セットアップ**」ウィザードを表示します。 • **いいえ**: 「**HMC セットアップ**」ウィザードの表示を無効にします。	無効な値が入力された場合、Activation Engine はデフォルト設定の「**はい**」を使用します。
SetupCallHomeWizard	必須エレメント。「**HMC コール・ホーム**」ウィザードを有効または無効にします。	• **はい**: 「**HMC コール・ホーム**」ウィザードを表示します。 • **いいえ**: 「**HMC コール・ホーム**」ウィザードの表示を無効にします。	無効な値が入力された場合、Activation Engine はデフォルト設定の「**はい**」を使用します。
SetupKeyboard	必須エレメント。キーボード構成を定義します。	• **はい**: ユーザーにキーボード構成を要求します。 • **いいえ**: デフォルトのキーボード構成を受け入れます (US)。	無効な値が入力された場合、Activation Engine はデフォルト設定の「**はい**」を使用します。
SetupDisplay	必須エレメント。ディスプレイ構成を有効または無効にします。	• **はい**: ユーザーにディスプレイ 構成を要求します。 • **いいえ**: デフォルトのディスプレイ 構成を受け入れます。	無効な値が入力された場合、Activation Engine はデフォルト設定の「**はい**」を使用します。

表 9. *XML タグ (続き)*

タグ	説明	許容値	注
Ethernet	必須エレメント。イーサネット・アダプター構成の値を保持します。構成可能なイーサネット・アダプターは最大 4 つです。	**Enable**: • **はい**: このアダプターを 構成します。 • **いいえ**: このアダプターを 構成しません。 **DefaultGatewayDevice**: • **はい**: このアダプターをメインのネットワーク・アダプターとして構成します。 • **いいえ**: このアダプターをメインのネットワーク・アダプターとして 構成しません。 **PrivateInterface**: • **はい**: このアダプターをプライベート・インターフェースとして 構成します。インターフェースを IPv4 DHCP サーバーとして構成する場合は、「**はい**」にする必要があります。 • **いいえ**: このアダプターをプライベート・インターフェースとして 構成しません。インターフェースを IPv4 静的タイプとして構成する場合は、「**いいえ**」にする必要があります。	イーサネット・アダプター・セクションで無効な値が入力された場合、または複数の「**デフォルト・ゲートウェイ・デバイス**」が定義されている場合は、Activation Engine はデフォルトの構成を実行します。オプションのエレメントは構成から省略できます。少なくとも 1 つの IPV4 構成または IPV6 構成が必要です。IP 構成を指定しないと、Activation Engine はデフォルトの構成を使用します。
HostName	オプションのエレメント。ネットワークのホスト名を定義します。	ホスト名を示す任意の有効なストリング。	エレメントが定義されていない場合、Activation Engine はデフォルトのローカル・ホストの「**HostName**」値を使用します。
Domain	オプションのエレメント。ネットワークのドメインを定義します。	任意の有効なドメイン値 (例: **example.us.com**)。	エレメントが定義されていない場合、Activation Engine はデフォルトの空の「**ドメイン**」値を使用します。
DNSServers	オプションのエレメント。ネットワークの DNS サーバーを定義します。	DNS サーバーの値を 1 つ、あるいはコンマで区切られた有効な IPv4 アドレスまたは IPv6 アドレスを最大 3 つ指定することができます。 • 例 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • 例 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • 例 3: IPv4: 8.3.2.1,8.5.4.1,8.4.3.2 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844, ::ffff:903:201	エレメントが定義されていない場合、Activation Engine はデフォルトの空の「**DNSServers**」値を使用します。

表 9. *XML タグ (続き)*

タグ	説明	許容値	注
IP4Config	オプションのエレメント。IPv4 構成設定を定義します。	**IPType**: 必須エレメント。IPv4 構成タイプを定義します。 • **静的**: このアダプターを静的構成を使用して構成します。 • **DHCP**: このアダプターを DHCP 構成を使用して構成します。 • **DHCPServer**: このアダプターを IPv4 DHCP サーバーとして構成します (「**PrivateInterface**」を「**はい**」に設定する必要があります)。 **IPAddress**: オプションのエレメント。「**静的**」構成または「**DHCPServer**」構成を選択している場合のみ必要です。 • **静的構成**: 任意の有効な IPv4 アドレス値。 • **DHCPServer 構成**: IP 範囲内にある任意の DHCP サーバー IP。 **ネットマスク**: オプションのエレメント。「**静的**」構成を選択している場合のみ必要です。 • 任意の有効な IPv4 ネットマスク値。 **ゲートウェイ**: オプションのエレメント。「**静的**」構成を選択している場合のみ必要です。 • 任意の有効な IPv4 ネットマスク値。	
IP6Config	オプションのエレメント。IPv6 構成設定を定義します。	**IPType**: 必須エレメント。IPv6 構成タイプを定義します。 • **静的**: このアダプターを静的構成を使用して構成します。 • **DHCP**: このアダプターを DHCP 構成を使用して構成します。 **IPAddress**: これは、詳細形式または簡易形式の IPv6 フォーマットおよび詳細形式または簡易形式の IPv6 接頭部を指定できます。 • 例 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • 例 2: IPv6: 2001:4860:4860::8888 • 例 3: IPv6: 2001:4860:4860::8888/128 接頭部が指定されていない場合、Activation Engine はデフォルト設定の /64 接頭部を使用します。 **ゲートウェイ**: • 任意の有効な IPv6 アドレス値。	

表 9. *XML タグ (続き)*

タグ	説明	許容値	注
Firewall	オプションのエレメント。ファイアウォール設定を定義します。	**PEGASUS**: • **有効**: PEGASUS ポートを開くことができます。 • **無効**: PEGASUS ポートを無効にします。 **RPD**: • **有効**: RMC ポートを開くことができます。 • **無効**: RMC ポートを無効にします。 **FCS**: • **有効**: FCS ポートを開くことができます。 • **無効**: FCS ポートを無効にします。 **I5250**: • **有効**: 5250 ポートを開くことができます。 • **無効**: 5250 ポートを無効にします。 **PING**: • **有効**: Ping ポートを開くことができます。 • **無効**: Ping ポートを無効にします。 **L2TP**: • **有効**: L2TP ポートを開くことができます。 • **無効**: L2TP ポートを無効にします。 **SLP**: • **有効**: SLP ポートを開くことができます。 • **無効**: SLP ポートを無効にします。 **RSCT**: • **有効**: RSCT ポートを開くことができます。 • **無効**: RSCT ポートを無効にします。 **SECUREREMOTEACCESS**: • **有効**: セキュア・リモート・アクセス・ポートを開くことができます。 • **無効**: セキュア・リモート・アクセス・ポートを無効にします。 **SSH**: • **有効**: SSH ポートを開くことができます。 • **無効**: SSH ポートを無効にします。	

表 9. *XML タグ (続き)*

タグ	説明	許容値	注
Firewall	オプションのエレメント。ファイアウォール設定を定義します。	**NTP**: • **有効**: NTP ポートを開くことができます。 • **無効**: NTP ポートを無効にします。 **SMNPTraps**: • **有効**: SMNP トラップ・ポートを開くことができます。 • **無効**: SMNP トラップ・ポートを無効にします。 **SMNPAgents**: • **有効**: SMNP エージェント・ポートを開くことができます。 • **無効**: SMNP エージェント・ポートを無効にします。	
NTPServers	HMC 仮想アプライアンスで最大 5 つの NTP サーバーを構成したい場合は、「**NTPServers**」タグが必要です。	**NTPServers**: `<ntpparam ntpserver="server" ntpversion="version"/>` を受け入れます。 **ntpparam**: • **ntpserver**: 任意の有効な IPv4 値または IPv6 値、および有効なホスト名を受け入れます。 • **ntpversion**: 1 から 4 の数値を受け入れます。 例: `<NTPServers> <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/> <ntpparam ntpserver="192.168.34.1" ntpversion="4"/> <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/>` `</NTPServers>`	

HMC の構成

ネットワーク接続のセットアップ、HMC の構成、構成完了後のステップの実行、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。

HMC に関するネットワーク設定の選択

ハードウェア管理コンソール (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

ネットワークでハードウェア管理コンソール HMC を使用する方法について説明します。

いくつかのタイプのネットワーク接続を使用して、ご使用の HMC を管理対象システムに接続することができます。 HMC をネットワークに接続できるように構成する方法の詳細については、54 ページの『HMC

の構成』を参照してください。 ネットワーク上での HMC の使用について詳しくは、以下の情報をお読みください。

HMC ネットワーク接続のタイプ

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

HMC は、以下のタイプの論理通信をサポートします。

HMC から管理対象システムへ

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

HMC から論理区画へ

このタイプの通信は、論理区画で稼働中のオペレーティング・システムからプラットフォーム 関連の情報 (ハードウェア・エラー・イベント、ハードウェア・インベントリー) を収集したり、特定のプラットフォーム活動 (動的 LPAR、並行修復) 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。
- 仮想端末サーバーを使用して、仮想論理区画コンソールにリモート・アクセスする。

HMC からサービス・プロバイダーへ

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

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

- 1 つのネットワーク・インターフェースを 、HMC と管理対象システム間の通信に専用に使用する ことができます。つまり、HMC および管理対象システムのサービス・プロセッサーのみが そのネットワーク上に存在することになります。 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・プロセッサーのみであることを意味します。 サービス・プロセッサーへのネットワーク・インターフェースは SSL (Secure Sockets Layer) プロトコルで暗号化されており、パスワードで保護されていますが、別の専用ネットワークがあれば、これらのインターフェースに 対して、より高水準のセキュリティーを提供することができます。
- HMC と論理区画間の通信では、オープン・ネットワーク・インターフェースが 、HMC と 管理対象システム上の論理区画の間でのネットワーク接続に通常使用 されます。このオープン・ネットワーク・インターフェースを 使用して、HMC をリモートで管理することもできます。
- オプションで、3 番目のインターフェースを 使用して、論理区画に接続し、HMC をリモートで管理することができます。この 3 番目のインターフェースは 、異なるグループの論理区画 に別の HMC 接続を持たせるためにも使用することができます。例えば、すべての通常のビジネス・トランザクションを実行している LAN とは別の管理 LAN を 持つこともできます。リモート管理者は、この方式を使用して、HMC お

よび他の管理対象装置にアクセスすることもできます。場合によっては、論理区画が、おそらくはファイアウォールの背後で異なるネットワーク・セキュリティー・ドメイン内にあることがあり、これら 2 つのドメインのそれぞれに対して異なる HMC ネットワーク接続を持つこともできます。

HMC の Web ブラウザー要件

ハードウェア管理コンソール (HMC) バージョン 9.1.0 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・プロキシーを使用するように構成されている場合は、例外リストにローカル IP アドレスを指定する必要があります。例外リストについての詳細は、ネットワーク管理者にお問い合わせください。 プロキシーを使用して HMC にアクセスする必要がある場合は、「インターネット オプション」ウィンドウの「詳細設定」タブで「プロキシ接続で HTTP 1.1 を使用する」を有効にしてください。

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

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

1. 「ツール」を選択して、「インターネット オプション」をクリックします。
2. 「プライバシー」を選択して、「詳細設定」をクリックします。
3. 「常にセッション Cookie を許可する」にチェック・マークが付いていることを確認します。チェック・マークが付いていない場合は、「自動 Cookie 処理を上書きする」と「常にセッション Cookie を許可する」を選択します。
4. 「ファースト パーティの Cookie」および「サード パーティの Cookie」で「ダイアログを表示する」を選択します。
5. 「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
ハードウェア管理コンソール (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フレキシブル ・サービス・プロセッサー (FSP) 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。最大 2 つの HMC に接続可能です。

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 がないシステム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*
ハードウェア管理コンソール (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。

最初のネットワーク・インターフェースをプライベート ・ネットワークとして構成する場合は、DHCP サーバーがそのクライアントに割り当てるために IP アドレスの範囲から選択することができます。選択可能なアドレス範囲には、標準の経路指定不能な IP アドレス範囲 からのセグメントが含まれます。

これらの標準範囲に加えて、IP アドレスの特別な範囲が IP アドレス用に予約されています。この特別な範囲は、HMC 接続のオープン・ネットワーク がルーティング不能なアドレス範囲の 1 つを使用中である場合に競合を避けるために 使用できます。選択された範囲に基づいて、プライベート・ネットワーク上の HMC ネットワーク・インターフェースに、その範囲の最初の IP アドレスが自動的に割り当てられ、 サービス・プロセッサーには残りの範囲からアドレスが割り当てられます。

HMC 内の DHCP サーバーは、自動的な割り振りを行います。つまり、固有なサービス・プロセッサーの各イーサネット・インターフェースには、それが開始される たびに同じ IP アドレスが再割り当てされます。各イーサネット・インターフェースは、 組み込まれた Media Access Control (MAC) アドレスに基づいた固有 ID を持ち、これに より DHCP サーバーは同じ IP パラメーターを再割り当てすることができます。**eth0** と **eth1** の両方の HMC ポートを構成して、DHCP アドレスに対応できます。**eth0** と **eth1** の両方の HMC ポートを構成して、DHCP アドレスに対応できます。

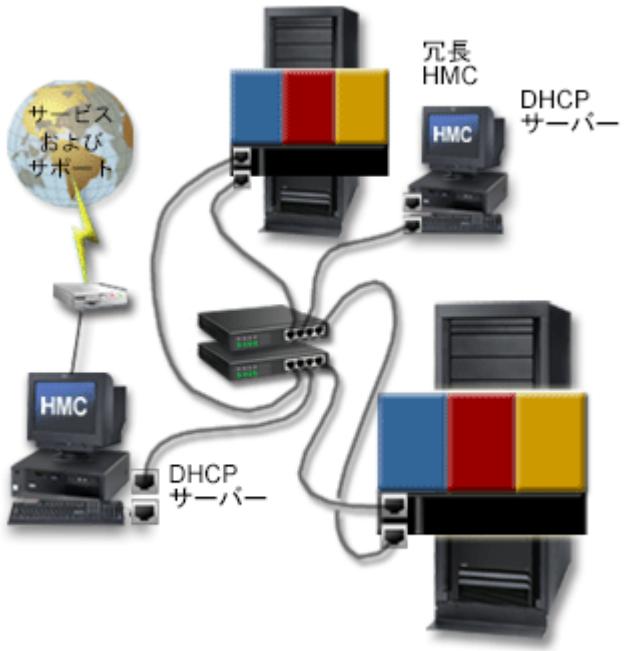
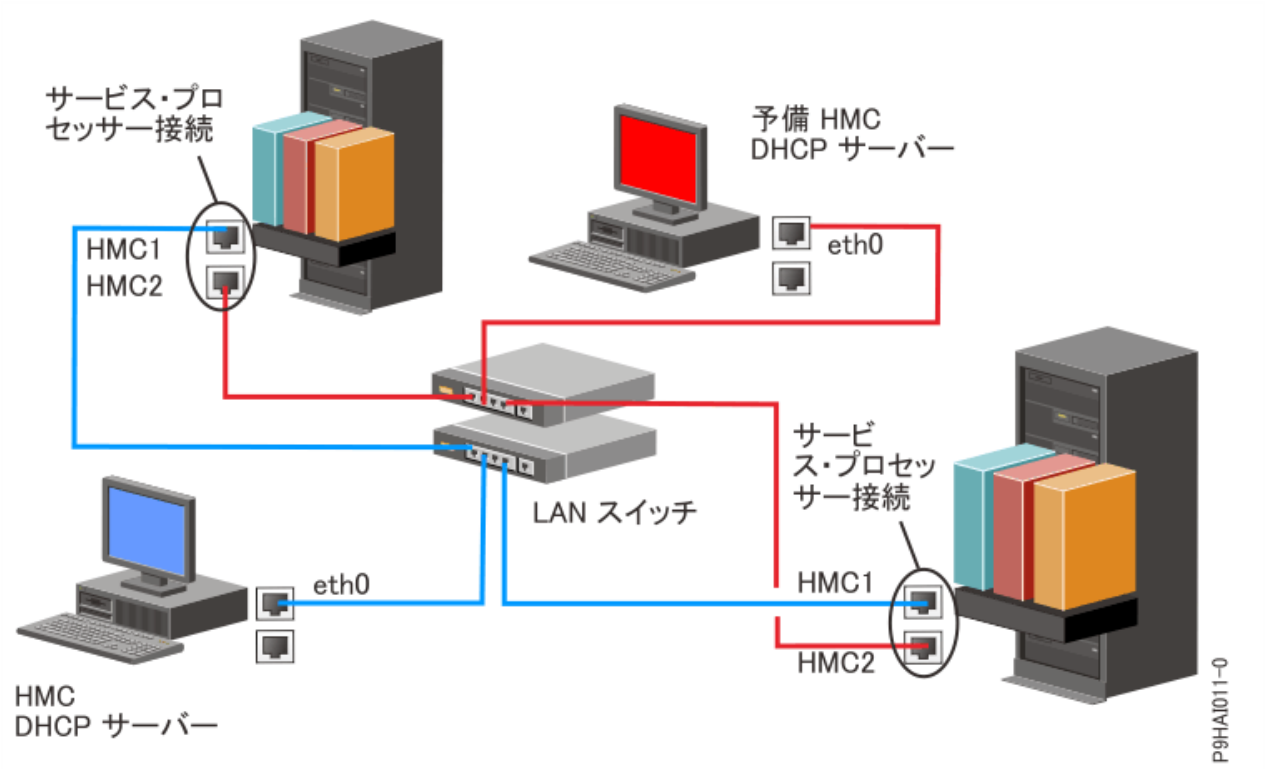


図 *9. DHCP* サーバーとしての *1* 台の *HMC* を持つプライベート・ネットワーク

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 の場合、自動ディスカバリーは使用できません。

HMC を DHCP サーバーとして構成する方法について詳しくは、62 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。

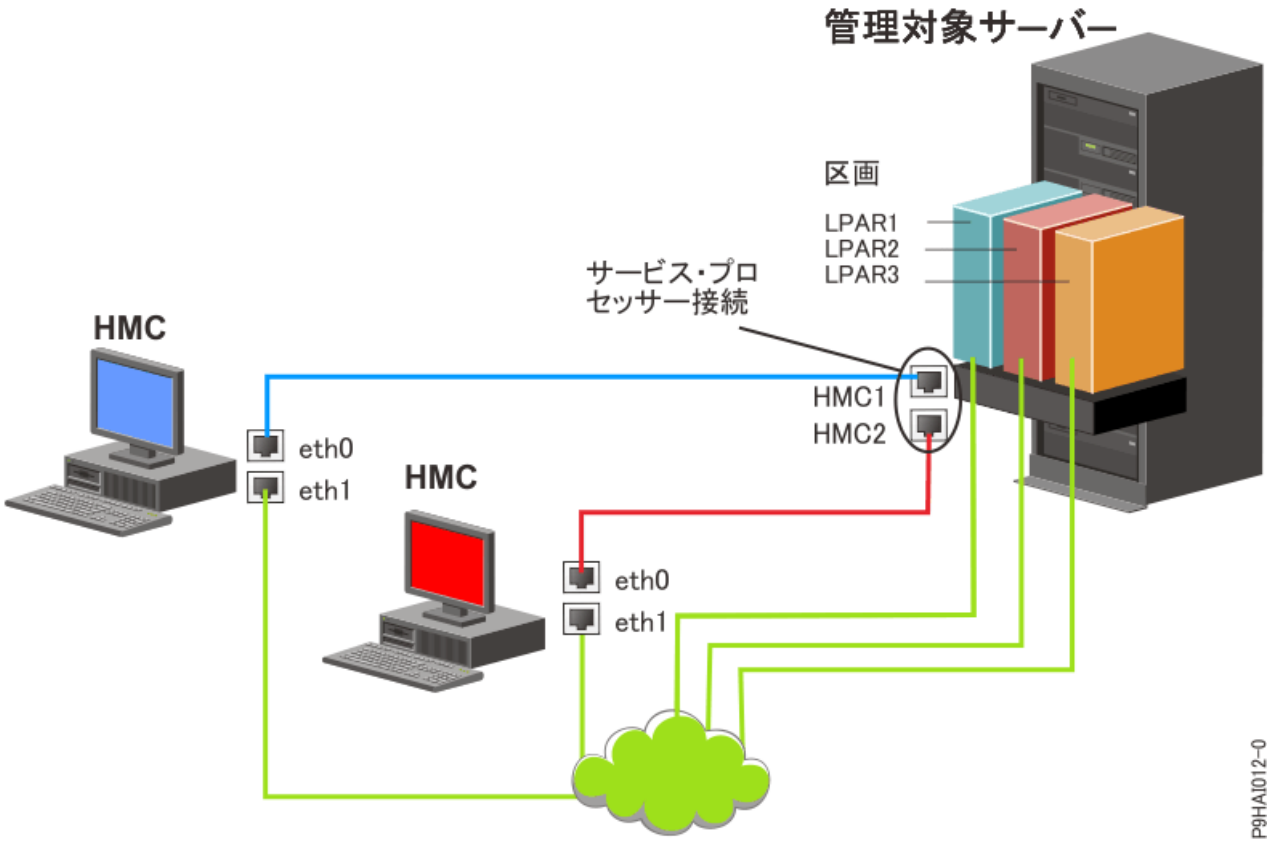


この図には、2 つの管理対象システムに接続する冗長 HMC 環境を記載してあります。最初の HMC は、各 FSP 上の最初のポートに接続され、冗長 HMC は各 HMC 上の 2 番目のポートに接続されています。各 HMC は DHCP サーバーとして構成され、異なる範囲の IP アドレスを使用しています。各接続は独立したプライベート・ネットワーク上にあります。このように、どの FSP ポートも 2 台以上の HMC に接続されていないようにすることが重要です。

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 と交差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。

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。

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

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

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、44 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。

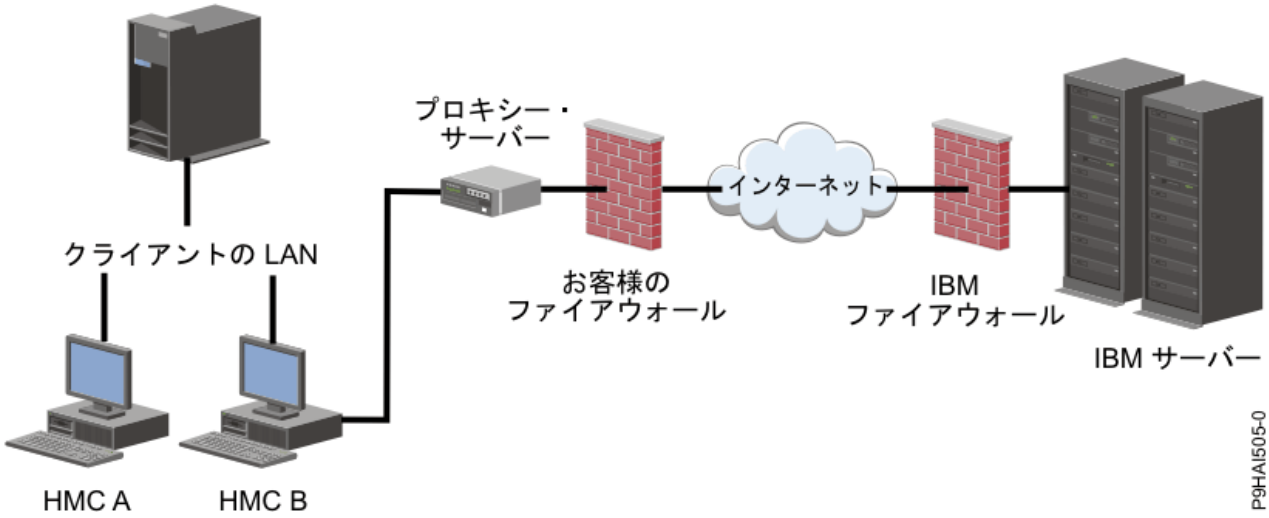
- HMC と IBM Service Support System 間で転送される全データは、高度な暗号化機能を使用して暗号化されています。データは、選択した接続方式に応じて、SSL または IPSec Encapsulating Security Payload (ESP) のいずれかを使用して暗号化されます。
- 暗号化された接続の開始時に、HMC はターゲットとなる宛先を IBM Service Support System として認証します。

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

プロキシー・サーバー経由での間接インターネット接続の使用

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

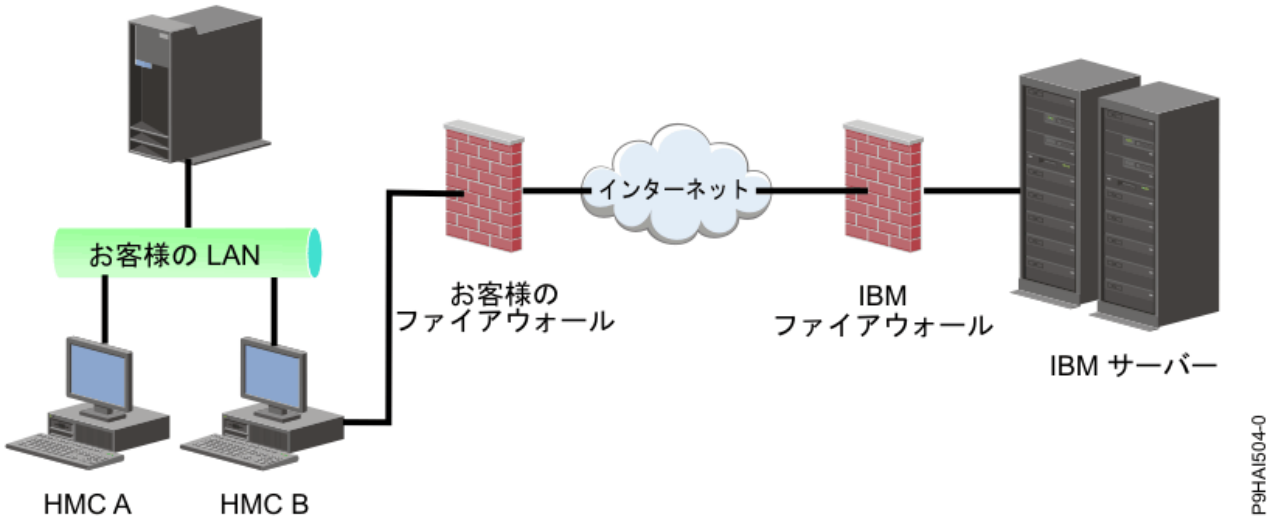
SSL ソケットをフォワードするには、そのプロキシー・サーバーは基本プロキシー・ヘッダー機能 (RFC 2616 に記載あり) と CONNECT メソッドをサポートする必要があります。オプションとして、基本プロキシー認証 (RFC 2617) を、プロキシー・サーバー経由でソケットを転送しようとする前に HMC が認証するように構成することができます。



HMC が通信を正常に行うためには、そのクライアントのプロキシー・サーバーはポート 443 に接続可能でなければなりません。プロキシー・サーバーを構成して、HMC が接続可能な IP アドレスを特定のものに限定することができます。IP アドレス・リストは、44 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 44 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、ハードウェア管理コンソール (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 (44 ページの『インターネット SSL アドレス・リスト』参照)。それによって、これらの接続を許可するように外部ファイアウォールを構成します。

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

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

インターネット・プロトコルの選択

ハードウェア管理コンソール (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、63 ページの『IPv4 アドレスの設定』および 63 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

ハードウェア管理コンソール (HMC) がインターネット SSL 接続を使用している場合に 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

複数のコール・ホーム・サーバーの使用

複数のコール・ホーム・サーバーの使用を決定した場合に、必要な事項について説明します。

Single Point of Failure を防ぐには、ハードウェア管理コンソール (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・サーバーが試行されるまで、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について説明します。

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。

ご使用の HMC を以下のロケーション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・プロセッサー
- 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)

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、61 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。
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、物理的にこのシステムに近くて、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、47 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。

HMC の改善されたパスワード・ポリシー

HMC バージョン 9.940.0 以降を備えた新たに製造されたシステムに対し、最初に使用する際に、システムの出荷時リセット後に新規パスワードを設定する必要があります。このポリシーの変更は、HMC が既知のパスワードが使用された状態のままに置かれないようにする上で役立ちます。

HMC バージョン 9.940.0 以降では、`hscroot` パスワードは期限切れになっており、変更してからでないと、HMC の機能にアクセスできません。パスワードの変更方法について詳しくは、https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm を参照してください。ただし、以前の HMC レベルまたは稼働中のインストール済み環境からアップグレードしている場合は、パスワードの変更は必要ありません。

ネットワーク設定

LAN インターフェース : 管理対象システム、論理区画、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。詳しくは、37 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
適切なイーサネット・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 *10.* イーサネット・アダプターのスピードと二重モード

特性	**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、39 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 *11.* 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

特性	**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。HMC を DHCP サーバーとして有効にする場合、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 *12. DHCP* サーバー		
特性	**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、62 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 *13. BMC* 接続	
特性	**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、57 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。

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 *14. IPv6* (静的)				
特性	**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 *15. IPv6 (DHCP* サーバー*)*				
特性	**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 16. IPv6 (IPv6 ルーター)				
特性	**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 63 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、64 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 17. IPv4				
特性	**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。				

TCP/IP 情報

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

ファイアウォール設定

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

オープン・ネットワーク・アダプターとして少なくとも 1 つのアダプターを構成する場合、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 *18.* オープン・ネットワーク・アダプター	
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。ターゲット・ステーションがソースと同じサブネット上にない場合、ゲートウェイ・アドレスは、データを送信する時点を各コンピューターまたはネットワーク・デバイスに通知します。

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

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

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

電子メール通知

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

表 *19.* 電子メール通知	
特性	**入力フィールド**
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 *20.* サービス連絡先情報	
特性	**入力フィールド**
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	
代替電話番号	
所在地住所	
所在地住所 2	
市または地域	
県	

表 *20.* サービス連絡先情報 *(*続き*)*	
特性	**入力フィールド**
郵便番号	
国または地域	
HMC の場所 (上記管理者住所と同じ場合は、「同じ」と指定)	
所在地住所	
所在地住所 2	
市または地域	
県	
郵便番号	
国または地域	

サービス権限と接続性

サービス・プロバイダーに連絡するための接続タイプを選択してください。これらの方法の詳細 (セキュリティー特性と構成要件を含む) は、70 ページの『既存のコール・ホーム・サーバーを選択して、この HMC 用のサービスおよびサポートに接続する方法』を参照してください。

表 *21.* サービス権限と接続性	
特性	**入力フィールド**
インターネット経由の Secure Sockets Layer (SSL)	_____
インターネットを介する仮想プライベート・ネットワーク (VPN)。	_____

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

表 *22. SSL*	
特性	**入力フィールド**
SSL プロキシーの使用? (はい/いいえ)	
「はい」の場合、以下の情報をリストします。	
アドレス:	
ポート:	
SSL プロキシーにより認証?	
「はい」の場合、以下の情報をリストします。	
ユーザー:	

表 *22. SSL (続き)*	
特性	**入力フィールド**
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、57 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。

___ IPv4

___ IPv6

___ IPv4 および IPv6

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 (VPN) を選択すると、お客様は他のどのオプションも選択することができません。

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、45 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 *23.* 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 *24.* マイ・システムとプレミアム・サーチ	
特性	**入力フィールド**
IBM ID のリスト	_____
追加の IBM ID のリスト	_____

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

注 : IBM はパーソナライズされた Web 機能を提供して、その機能で、IBM 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、45 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、47 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。

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、本書に収録されていないタスクの参照も含まれています。 HMC 上または Web 上の IBM Power Systems ハードウェア情報にアクセスすることができます。HMC では、タスクバーの右上隅から IBM Knowledge Center にアクセスできます。 Web では、https://www.ibm.com/support/knowledgecenter から IBM Knowledge Center にアクセスできます。

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、45 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 *25.* 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。	56 ページの『HMC の始動』
2. 日時を設定します。	

表 25. 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**
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。	57 ページの『HMC ネットワーク・タイプの構成』
6. HMC モデル 7063-CR1 の場合、ベースボード管理コントローラー (BMC) の IP アドレスを構成する必要があります。	62 ページの『BMC 接続の構成』
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、識別情報を設定します。	
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、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。	65 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』
9. 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。	66 ページの『ドメイン名サービスの構成』
10. 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。	66 ページの『ドメイン・サフィックスの構成』
11. 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。	68 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』
12. 「コール・ホーム用イベント・マネージャー」を構成します。	72 ページの『「コール・ホーム用イベント・マネージャー」の構成』
13. 管理対象システムに電源を接続します。	
14. 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。	73 ページの『管理対象システムに対するパスワードの設定』
15. 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。	
16. 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。	
17. 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。	
18. 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。	
19. 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。	
20. 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。	75 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。

このタスクについて

HMC を始動するには、以下の手順を実行します。

手順

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

   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・プロセッサーに接続する際に、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ハードウェア管理コンソール (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。

このタスクについて

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。

手順

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。

タスクの結果

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。

始める前に

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 *26.* 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。	47 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。	60 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。	61 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。	61 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。	63 ページの『IPv6 アドレスの設定』
d. ファイアウォールを設定します。	64 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。	65 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。	66 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。	74 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。

始める前に

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 27. 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。	47 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。	60 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。	62 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。	74 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

始める前に

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 28. 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。	47 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。	60 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。	61 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。	61 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。	63 ページの『IPv6 アドレスの設定』
d. ファイアウォールを設定します。	64 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。	65 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。	66 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。	74 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

始める前に

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 *29.* 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。	47 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。	60 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。	61 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。	61 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。	63 ページの『IPv6 アドレスの設定』
d. ファイアウォールを設定します。	64 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。	65 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。	66 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。	66 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

始める前に

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

表 *30. 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。	47 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。	68 ページの『ローカル・コンソールを構成してサービス・プロバイダーへエラーを報告する方法』 70 ページの『既存のコール・ホーム・サーバーを選択して、この HMC 用のサービスおよびサポートに接続する方法』
3. コール・ホーム構成が機能しているかどうかを検証します。	71 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。	71 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。	72 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であって、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る場合、eth0 として定義されるポートは、取り付けてあるイーサネット・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 *31. 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 eth0 となります。Act/link B のラベルが付いたポートは eth1 です。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、取り付けられたイーサネット・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、61 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) コネクターでのみ作動可能です。 イーサネット・ケーブルを接続する必要がある NIC コネクターを判別する必要がある場合があります。 ここでは、HMC が eth0 および eth1 として識別する NIC コネクターの判別方法について説明します。

このタスクについて
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、以下の手順を完了します。

手順
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. 「**ネットワーク設定の変更**」ウィンドウで、「**LAN アダプター**」タブをクリックします。次の例のエントリーは、このイーサネット・ポートが eth0 として識別されることを示しています。 `Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>)`
4. 結果を記録します。LAN アダプター設定を表示または変更する必要がある場合は、「**詳細**」をクリックします。
5. 「**了解**」をクリックします。

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。

始める前に
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。

手順
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 (LAN) 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、ハードウェア管理コンソール (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。

このタスクについて

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、次の手順を完了します。

手順

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。

ハードウェア管理コンソール (HMC) を DHCP サーバーとして構成するには、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、「**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 の使用可能化**」を選択するためのオプションは使用できません。
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、61 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、40 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。

手順

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。

手順

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。

手順

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 アドレスを追加して、「**OK**」をクリックします。

次のタスク
「**了解**」をクリックしたら HMC を再始動して、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。

このタスクについて

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。

手順

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できます。あるいは、1 つ以上の IP アドレスを指定することができます。
   - ある特定のアプリケーションを使用している IP アドレスは、ファイアウォールを通ることができます。
     a. 上部ボックスで、該当のアプリケーションを強調表示します。
     b. 「**着信の許可**」をクリックします。 そのアプリケーションが選択されたことを示すために、該当の下部ボックスに表示されます。
   - ファイアウォールを通ることができる IP アドレスを指定します。
     a. 上部ボックスで、アプリケーションを強調表示します。
     b. 「**IP アドレス別の着信許可**」をクリックします。

c.「許可されるホスト」ウィンドウで、IP アドレスとネットワーク・マスクを入力します。

d.「**追加**」をクリックし、「**了解**」をクリックします。

7.「**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。

このタスクについて

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、次の手順を完了します。

手順

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。

次のタスク

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
ハードウェア管理コンソール (HMC) へのリモート Web アクセスを使用可能にできます。

このタスクについて

リモート Web アクセスを使用可能にするには、次の手順を完了します。

手順

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。

次のタスク

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。 この作業は、オープン・ネットワークを使用している場合に使用できます。

始める前に

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、次の手順を完了します。

手順

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。

このタスクについて

オープン・ネットワークをセットアップする予定の場合は、ドメイン名サービスを構成してください。 ドメイン名システム (DNS) は、ホスト名およびそれらに関連するインターネット・プロトコル (IP) アドレスを管理するための分散データベース・システムです。 ドメイン名サービスの構成には、DNS の使用可能化、およびドメイン・サフィックスのサーチ順序の指定が含まれます。

手順

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・サーチ・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。

このタスクについて

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。 ただし、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る場合、`myname.mloc.mycompany.com` を解決する試みが行われます。

ドメイン・サフィックス・エントリーを構成するためには、以下の手順を完了します。

手順

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。

始める前に

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、57 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。

このタスクについて

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。

手順

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。

始める前に

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検証されます。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、57 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。

このタスクについて

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、次の手順を完了します。

手順

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、次の手順を完了します。

   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. オプションとして、サービス・キー・ファイルをこの HMC にインポートすることができます。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、次の手順を完了します。

   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。

   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、次の手順を完了します。

   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。

   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。

始める前に

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

この作業を開始する前に、以下のことを確認してください。

- ネットワーク管理者が、ネットワーク接続が可能であることを検証している。詳しくは、45 ページの『HMC 構成の準備』を参照してください。
- プロキシー・サーバー経由のインターネット・サポートを構成する場合は、以下の情報も必要です。
  - プロキシー・サーバーの IP アドレスとポート
  - プロキシー認証情報
- **eth1** として指定されたアダプター (オープン・ネットワークとして指定されるもの) が使用されます。詳しくは、37 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、次の手順を完了します。

手順

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。

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。

始める前に

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している。詳しくは、45 ページの『HMC 構成の準備』を参照してください。
- お客様連絡先情報が構成されている。連絡先情報を検証するには、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。
- プロキシー・サーバー経由のインターネット・サポートを構成する場合は、以下の情報も必要です。
  - プロキシー・サーバーの IP アドレスとポート
  - プロキシー認証情報
- 少なくとも 1 つのオープン・ネットワーク・インターフェースが構成されているかどうか。詳しくは、39 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。

このタスクについて

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、次の手順を完了します。

手順

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 プロキシーを使おうとしている場合、「**SSL プロキシーの使用 (Use SSL proxy)**」ボックスにチェック・マークを付けます。
9. SSL プロキシーを使おうとしている場合、プロキシーのアドレスとポートを入力します。この情報はネットワーク管理者から入手してください。
10. 「**SSL プロキシーの使用 (Use SSL proxy)**」にチェック・マークを付けていた場合で、かつ、このプロキシーではユーザー ID とパスワードの認証が必要となる場合は、「**SSL プロキシーを使用した認証 (Authenticate with the SSL proxy)**」ボックスにチェック・マークを付けます。ユーザー ID とパスワードを入力します。ユーザー ID およびパスワードは、ネットワーク管理者から入手してください。
11. 使用する「**インターネットに対するプロトコル (Protocol to Internet)**」を選択します。
12. 「**インターネット (Internet)**」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。

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ハードウェア管理コンソール (HMC) によって認識または検出されている既存の HMC コール・ホーム・サーバーを選択します。

始める前に

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、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、次の手順を完了します。

手順

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。

タスクの結果
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**」をクリックしてから「**OK**」をクリックします。

サービス・プロバイダーへの接続が機能しているかどうかの検証
サービスおよびサポートへの接続が機能していることを確認するために問題報告機能をテストします。

このタスクについて
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、次の手順を完了します。

手順
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 PMH イベントと PMH 番号が割り当てられていることを確認します。
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。

始める前に
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 47 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。

このタスクについて
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、次の手順を完了します。

手順
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したり、情報が定期的に送信されるようにスケジュールしたりすることができます。

始める前に

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、71 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。

このタスクについて

サービス情報を送信するには、以下の手順を実行します。

手順

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。

「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 使用方法および上記パスワードの設定方法について説明します。

始める前に

「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。

このタスクについて

「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

始める前に

サーバー・パスワードを更新するには、次の手順を完了します。

手順

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

始める前に

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、次の手順を完了します。

手順

1. HMC のナビゲーション領域で、管理対象システムを選択します。
2. 「タスク」領域で、「**操作**」をクリックします。
3. 「**拡張システム管理 (ASM)**」をクリックします。 「ASM インターフェースの 起動 (Launch ASM Interface)」ウィンドウが開きます。
4. 「サービス・プロセッサー IP アドレスの選択 (Select a Service Processor IP Address)」を選択して、「**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

始める前に

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

ネットワークに適切に接続されているかどうかを検証する方法について説明します。

このタスクについて

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、以下の手順を完了します。

手順

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。

タスクの結果

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、37 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、54 ページの『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。

管理コンソールのデータのバックアップ

これは、HMC ハード・ディスクに保存されている、HMC 操作をサポートする上で重要なデータをバックアップ (またはアーカイブ) するタスクです。

始める前に

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

このタスクについて

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 データのバックアップは、HMC または論理区画に関連する情報に変更を加えた後に行います。

HMC ハード・ディスクに保管されている HMC データは、ローカル・システム上の DVD-RAM に保管したり、HMC ファイルシステムにマウントされているリモート・システム (例えば NFS) に保管したり、ファイル転送プロトコル (FTP) を使用してリモート・サイトに送信したりすることができます。

注 : HMC モデル 7063-CR1 の場合、外付け USB DVD ドライブを接続することができます。

HMC を使用して、以下のような重要データをすべてバックアップすることができます:

- 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

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、次の手順を完了します。

手順

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 Management Console Data)**」をクリックします。
3. 「**管理コンソール・データのバックアップ**」ウィンドウから、実行するアーカイブ・オプションを選択します。
4. 「**次へ**」をクリックして、選択したオプションに応じて該当する指示に従います。
5. 「**了解**」をクリックしてバックアップ処理を続けます。

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。

注 : HMC モデル 7063-CR1 の場合、外付け USB DVD ドライブを接続することができます。

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。

このタスクについて

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、以下の手順を完了します。

手順

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。

このタスクについて

HMC 用のマシン・コード更新を入手するには、すべてのステップを実行します。

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

このタスクについて

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、以下のいずれかの接続が必要です。

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

インターネットに接続していることを確認して、次のようにします。

手順

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。

   注 : HMC モデル 7063-CR1 の場合、外付け USB DVD ドライブを接続することができます。
6. 77 ページの『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

このタスクについて

既存の HMC マシン・コード・レベルを表示するには、次の手順を完了します。

手順

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. 77 ページの『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

このタスクについて

使用可能な HMC マシン・コード・レベルを表示するには、次の手順を完了します。

手順

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. 78 ページの『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

このタスクについて

HMC マシン・コードの更新を適用するには、以下の手順を完了します。

手順

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、75 ページの『管理コンソールの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、「**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

このタスクについて

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、次の手順を完了します。

手順

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. 別のリポジトリーを使用してファームウェア更新を再試行する。
c. 問題が解決しない場合は、次のレベルのサポートに連絡する。

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

DVD または FTP サーバーを使用して ハードウェア管理コンソール (HMC) 用マシン・コード更新を入手する方法を説明します。

このタスクについて

HMC マシン・コード更新を入手するには、すべてのステップを実行します。

注 : HMC モデル 7063-CR1 の場合、外付け USB DVD ドライブを接続することができます。

ステップ *1.* 既存の *HMC* マシン・コード・レベルを表示する

始める前に

既存の HMC マシン・コード・レベルを表示するには、次の手順を完了します。

手順

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. 79 ページの『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

始める前に

使用可能な HMC マシン・コード・レベルを表示するには、次の手順を完了します。

このタスクについて

手順

1. インターネットに接続しているコンピューターまたはサーバーから、Fix Central Web サイトにアクセスします。
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. 79 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

始める前に

HMC マシン・コードの更新を適用するには、次の手順を完了します。

このタスクについて

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ているコンピューターまたはサーバーから、Fix Central Web サイトにアクセスします。
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ているコンピューターまたはサーバーから、Fix Central Web サイトにアクセスします。
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。

次のタスク

完了したら、80 ページの『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

始める前に

HMC マシン・コードの更新を適用するには、以下の手順を完了します。

手順

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、75 ページの『管理コンソールのデータのバックアップ』を参照してください。
2. 更新を収めた DVD-RAM を入手または作成した場合は、HMC の DVD ドライブにその DVD-RAM を挿入する。更新を収めた USB メモリー・デバイスを入手または作成した場合は、そのメモリー・デバイスを挿入する。
3. 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、75 ページの『管理コンソールの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。
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。

8. 81 ページの『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

始める前に

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、次の手順を完了します。

手順

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、次の手順を実行します。
   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。

このタスクについて

HMC でマシン・コードをアップグレードするには、すべてのステップを実行します。

注 : HMC モデル 7063-CR1 および 7063-CR2 の場合、外付け USB DVD ドライブを接続することができます。

ステップ *1.* アップグレードの入手

このタスクについて

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、次の手順を完了します。

手順

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、82 ページの『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

このタスクについて

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。

手順

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**」をクリックする。
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. 82 ページの『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』から続行します。

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

このタスクについて

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、次の手順を完了します。

手順

1. プロファイル・データを保管するシステムを選択します。
2. 「**アクション**」 > 「**すべてのアクションの表示**」 > 「**レガシー**」 > 「**区画データの管理**」 > 「**バックアップ**」をクリックします。
3. バックアップ・ファイル名を入力し、その情報を記録しておく。
4. 「**了解**」をクリックします。
5. 各システムごとに、これらのステップを繰り返す。
6. 82 ページの『ステップ 4. HMC データのバックアップ』から続行します。

ステップ 4. *HMC* データのバックアップ

このタスクについて

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、以下の手順を完了します。

手順

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. 83 ページの『ステップ 5. 現行 HMC 構成情報の記録』から続行します。

ステップ *5.* 現行 *HMC* 構成情報の記録

このタスクについて

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、次の手順を完了します。

手順

1. HMC 構成情報を記録する管理対象システムまたは区画を選択する。
2. メニュー・ポッドで、「**アクション**」 > 「**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。
3.「**ソート**」 > 「**オブジェクト別**」を選択する。
4. 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。

5.「**スケジュール操作のカスタマイズ**」ウィンドウを閉じる。
6. 84 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』から続行します。

ステップ 6. リモート・コマンドの状況を記録する

このタスクについて

リモート・コマンドの状況を記録するには、以下の手順を完了します。

手順

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、「**リモート・コマンド実行を有効にする**」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)**」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. 84 ページの『ステップ 7. アップグレード・データの保管』から続行します。

ステップ 7. アップグレード・データの保管

このタスクについて

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。アップグレード後に HMC 構成設定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、次の手順を完了します。

手順

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**」をクリックします。
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. 85 ページの『ステップ 8. HMC ソフトウェアのアップグレード』から続行します。

ステップ *8. HMC* ソフトウェアのアップグレード

このタスクについて
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。

手順
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 Managment 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. 85 ページの『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』から続行します。

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

このタスクについて
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、以下の手順を完了します。

手順
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。

このタスクについて

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。

手順

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、Hardware Management Console Support and downloads Web サイト (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html) にアクセスします。
2. 該当する HMC V9 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ーです。

6. HMC を再始動して、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 を再始動するには、**chhmc -c altdiskboot -s enable --mode upgrade** を実行します。
7. HMC を再始動し、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 の保護

企業セキュリティー標準に基づいてハードウェア管理コンソール (HMC) のセキュリティーを強化する方法について説明します。

HMC のデフォルト構成は、大半の企業ユーザーにとって十分なセキュリティーを提供します。ハードウェア管理コンソール (HMC) バージョン 8.4.0 以降では、企業セキュリティー標準に基づいて、HMC のセキュリティーをさらに強化することができます。HMC のセキュリティーを強化するには、HMC を少なくともレベル 1 セキュリティーに設定する必要があります。ご使用の環境および企業セキュリティー要件に応じて、レベル 2 およびレベル 3 を選択することもできます。

注 : セキュリティー・レベルを変更する前に、企業のセキュリティー・コンプライアンス・チームと確認してください。

レベル 1 セキュリティー

HMC を保護する (レベル 1 セキュリティー) には、以下の手順を実行します。

1. デフォルトの hscroot ユーザーの事前定義パスワードを変更します。パスワード・ポリシーの詳細については、89 ページの『拡張パスワード・ポリシー』を参照してください。
2. HMC が物理的に安全な環境に属していない場合は、コマンド `chhmc -c grubpasswd -s enable --passwd <new grub password>` を実行して、grub パスワードを設定します。
3. HMC 上で構成済みの統合管理モジュール (IMM) がある場合は、強固な IMM パスワードを設定してください。
4. すべてのサーバーの 管理者 ユーザーおよび一般ユーザーのための強固なパスワードを設定します。
5. 最新リリースのセキュリティー修正で HMC を更新します。セキュリティー修正について詳しくは、IBM Fix Central を参照してください。

レベル 2 セキュリティー

複数のユーザーが存在する場合は、以下の手順を実行して HMC のセキュリティーを強化します。

1. HMC 上で各ユーザーのアカウントを作成し、必要なロールとリソースをユーザーに割り当てます。HMC でのさまざまな役割について詳しくは、HMC タスク、ユーザー・ロール、ID、および関連コマンドを参照してください。

   注 : HMC で作成されたユーザーには、必要なリソースとロールのみを割り当ててください。 必要な場合は、カスタム・ロールを作成することもできます。
2. 異なるハードウェア管理コンソール間でのユーザー・データ複製を有効にします。ユーザー・データ複製は、マスター/スレーブ・モードまたはピアツーピア・モードで実行できます。 ユーザー・データ複製について詳しくは、データ複製の管理を参照してください。
3. 認証局によって署名された証明書をインポートします。

レベル 3 セキュリティー

複数のハードウェア管理コンソールとシステム管理者が存在する場合は、以下の手順を実行して HMC のセキュリティーを強化します。

1. Lightweight Directory Access Protocol (LDAP) や Kerberos など、一元管理された認証を使用します。LDAP の構成について詳しくは、How to Configure LDAP on HMC を参照してください。
2. 異なるハードウェア管理コンソール間でのユーザー・データ複製を有効にします。
3. HMC が強固な暗号のみを使用するように、HMC を NIST SP 800-131A モードにする必要があります。

4. 不要なポートをファイアウォールでブロックします。使用できる HMC ポートについては、次の表を参照してください。

表 *32. HMC* との対話でユーザーが使用するポート

ポート	説明	タイプ	プロトコル・バージョン (デフォルト・モード)	プロトコル・バージョン (NIST モード)
22	OpenSSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	SNMP エージェント	UDP	SNMP v3	SNMP v3
162	SNMP トラップ	UDP	SNMP v3	SNMP v3
427	SLP	UDP	N/A	N/A
443	HMC GUI および REST API	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (非暗号化テキスト + ハッシュおよび署名)	RSCT (非暗号化テキスト + ハッシュおよび署名)
2300	IBM i の 5250 端末	TCP	非暗号化テキスト	非暗号化テキスト
2301	IBM i の 5250 セキュア端末	TCP	TLS 1.2	TLS 1.2
5989	CIM (レガシー・ポート、無効)	TCP	無効	無効
9900	FCS: HMC-HMC ディスカバリー	UDP	FCS	FCS
9920	FCS: HMC-HMC 通信	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	GUI の VTerm アプレット	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	HMC REST API (レガシー・ポート)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	RSCT ピア・ドメイン	UDP	RSCT (非暗号化テキスト + ハッシュおよび署名)	RSCT (非暗号化テキスト + ハッシュおよび署名)
12348	RSCT ピア・ドメイン	UDP	RSCT (非暗号化テキスト + ハッシュおよび署名)	RSCT (非暗号化テキスト + ハッシュおよび署名)

注 :

- イントラネットで公表されている SSH (ポート 22)、HTTPS (ポート 443 とポート 12443)、IBM i の 5250 セキュア端末 (ポート 2301)、および VTerm (ポート 9960) のみを使用してください。 その他のポートはすべて、プライベート・ネットワークまたは分離されたネットワークで使用する必要があります。分離されたイーサネット・ポートおよび VLAN は、Resource Monitoring and Control (RMC) (ポート 657)、FCS (ポート 9900 とポート 9920)、および RSCT ピア・ドメイン (ポート 12347 とポート 12348) に使用できます。

- **netstat** コマンドにリストされているポートは、内部処理にのみ使用されます。

拡張パスワード・ポリシー

ハードウェア管理コンソール (HMC) を使用して、ローカルで認証されたユーザーにパスワード要件を設定することができます。 システム管理者は、拡張パスワード・ポリシー機能でパスワード制限を設定できます。 拡張パスワード・ポリシーは、HMC がインストールされたシステムに適用されます。

システム管理者は、拡張パスワード・ポリシーを使用して、すべてのユーザーに対する単一のパスワード・ポリシーを定義できます。 HMC は、ミディアム・セキュリティー・パスワード・ポリシーを提供します。 システム管理者はこのパスワード・ポリシーを活動化してパスワード制限を設定できます。 また、システム管理者は、このミディアム・セキュリティー・ポリシーまたは新規のユーザー定義ポリシーを活動化することもできます。 HMC ミディアム・セキュリティー・パスワード・ポリシーはシステムから除去することができません。 以下の表は、ミディアム・セキュリティー・ポリシーの属性とそのデフォルト値を示しています。

表 *33. HMC* ミディアム・セキュリティー・パスワード・ポリシーのパスワード属性

属性	説明	デフォルト値
min_pwage	パスワードをアクティブにしておく必要がある最小日数。	1
pwage	パスワードをアクティブにしておく最大日数。	180
min_length	パスワードの最小文字数。	8
hist_size	再使用できない、以前に保管されたパスワードの数。	10
warn_pwage	パスワードの有効期限切れが近づいた場合に、何日前にパスワードの有効期限が間もなく切れることユーザーに警告するか。	7
min_digits	パスワードに含める数字の最小数。	なし (None)
min_uppercase	大文字の最小数。	1
min_lowercase	小文字の最小数。	6
min_special_chars	パスワードで使用する必要がある特殊文字の最小数。	なし (None)

HMC ミディアム・セキュリティー・パスワード・ポリシーに関する以下の項目について考慮してください。

- ポリシーは、「**hscroot**」、「**hscpe**」、および「**root**」ユーザー ID には適用されません。
- ポリシーの影響を受けるのは、HMC によって管理され、ローカルで認証されるユーザーのみです。ポリシーは、LDAP や Kerberos では実施できません。
- HMC ミディアム・セキュリティー・パスワード・ポリシーまたはユーザー定義のポリシーを使用すると、システム管理者はパスワード再利用の制限を設定できます。
- HMC ミディアム・セキュリティー・パスワードは読み取り専用であり、HMC ミディアム・セキュリティー・パスワードの属性を変更することはできません。 新規にユーザー定義パスワードを作成すると、パスワードの制限を設定できます。

以下のコマンドを使用して、HMC ミディアム・セキュリティー・パスワード・ポリシーを構成できます。

mkpwdpolicy
すべてのパラメーターが含まれているファイルからパスワード・ポリシーをインポートするか、パスワード・ポリシーを作成します。

lspwdpolicy
使用可能なすべてのパスワード・ポリシー・プロファイルをリストし、個々のパラメーターを検索します。 現在アクティブなパスワード・ポリシーを表示することもできます。

rmpwdpolicy
アクティブでない既存のパスワード・ポリシーを削除します。

注 : アクティブなミディアム ・セキュリティー・ポリシーとデフォルトの読み取り専用パスワード・ポリシーは削除できません。

chpwdpolicy
アクティブでないパスワード・ポリシーのパラメーターを変更します。

セキュリティー・プロファイル: Global Data Protection Regulation (GDPR) および Payment Card Industry Data Security Standard (PCI-DSS)

ハードウェア管理コンソール (HMC) がどのようにユーザーのプライバシー情報を処理するかについて説明します。

ハードウェア管理コンソール (HMC) は、カード所有者データを保管しないクローズド・アプライアンスです。 したがって、HMC には、PCI-DSS によって定義された IT セキュリティーの一部の要件およびセキュリティー評価手順のみが適用されます。 IBM が配布する信頼できるコードのみを HMC にインストールできます。IBM PSIRT プロセス によって脆弱性が判明した場合は、暫定修正が公開されます。 要件および推奨には、以下の項目が含まれます。

GDPR 照会

表 *34. GDPR* 照会. この表には、GDPR に関連する質問についての情報が示されています。

質問	回答
HMC にはどのような種類のデータが保管されますか?	HMC には、Power ハードウェア、PowerVM 仮想化の構成情報、およびパフォーマンス・メトリック情報が保管されます。
HMC は個人データを処理しますか?	コール・ホーム機能用に連絡先情報を指定することができます。コール・ホーム機能用に連絡先情報を指定することはオプションです。
HMC のシステム管理にはどの事前定義アカウントが使用されますか?	システム管理者ユーザーは、ユーザー名 *hscroot* を使用します。
HMC 内のアカウントは特定の個人に関連付けられますか?	いいえ。
HMC での個人データの指定は必須ですか?	いいえ。個人データ情報を指定する必要はありません。しかし、この情報の指定はオプションです。
HMC ログ・ファイルに個人データ情報は含まれますか?	いいえ。
個人データを完全かつ永久に削除することは可能ですか?	はい。コール・ホーム機能を構成解除してください。

PCI-DSS 照会

表 *35. PCI-DSS* 照会. この表には、PCI-DSS に関連する質問についての情報が示されています。

質問	回答
カード所有者のデータを保護するために、どのようにファイアウォール構成をインストールおよび保守しますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。ただし、HMC にはファイアウォール構成があり、ユーザーは特定のポートを制御および有効化することができます。

表 *35. PCI-DSS* 照会. この表には、PCI-DSS に関連する質問についての情報が示されています。 *(続き)*	
質問	**回答**
システム・パスワードやその他のセキュリティー・パラメーターにベンダー提供のデフォルト値を使用することはできますか?	ネットワーク上にシステムを組み入れる前に、*hscroot* ユーザーのすべての事前定義パスワードを変更してください。
HMC は保管されているカード所有者のデータをどのように保護しますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。
カード所有者のデータがオープン・パブリック・ネットワーク間で送信される場合に、HMC はどのようにデータを暗号化しますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。
アンチウィルス・ソフトウェア・プログラムをどのように使用および定期更新しますか?	HMC はクローズド・アプライアンスです。したがって、マルウェアが HMC に感染することはありません。
セキュアなシステムやアプリケーションをどのように開発および保守しますか?	IBM Fix Central Web サイトから入手した必須パッチをご使用のシステムに手動でインストールする必要があります。IBM が配布する信頼できるコードのみを HMC にインストールできます。
HMC はカード所有者データへのアクセスを制限しますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。
コンピューターへのアクセス権限を持つ個人にどのように固有 ID を割り当てますか?	共用 ID がないことを確認し、パスワード・ポリシーに従うことで、この要件を満たすことができます。
カード所有者のデータへの物理アクセスをどのように制限しますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。
ネットワーク・リソースおよびカード所有者データへのアクセスをどのように追跡およびモニターしますか?	HMC はカード所有者データを保管することも、データにアクセスすることもありません。
HMC はシステムおよびプロセスのセキュリティーをどのようにテストしますか?	スキャン・ツールを使用して、HMC のすべてのリリース済みバージョンでセキュリティー・スキャンを実行します。スキャン・ツールには、*Qualys*、*Nessus*、*testssl*、*sslscan*、および *ASoC* があります。
従業員や請負業者の機密保護が含まれるセキュリティー・ポリシーをどのように保持しますか?	システム管理者は、リモート・ユーザー・ログインを無効にし、必要性があるときにのみユーザー・ログインを活動化して、アクセスが不要になった場合はユーザー・ログインを非活動化します。

HMC の保護における一般的な問題の解決

HMC を保護する際に発生する可能性のあるいくつかの一般的な問題を解決する方法を説明します。

ハードウェア管理コンソール (HMC) とシステムの間の接続を保護する方法

HMC は、フレキシブル・サービス・プロセッサー (FSP) を介してシステムに接続します。FSP と Power ハイパーバイザーの両方を保護するために、ネットワーク・クライアント・プロトコル (NETC) と呼ばれる専有バイナリー・プロトコルが使用されます。次の表には、HMC が使用するポートをリストしています。

表 *36. HMC* との対話に使用される *FSP* 上のポート			
FSP 上のポート	**説明**	**プロトコル・バージョン (デフォルト・モード)**	**プロトコル・バージョン (NIST モード)**
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2)。古いファームウェアをサポートするために、SSLv3 にフォールバックします。	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2)。古いファームウェアをサポートするために、SSLv3 にフォールバックします。	NETC (TLS 1.2)

HMC のロック方法

ご使用のインフラストラクチャーのセキュリティーを強化したい場合は、不正侵入防御システム (IPS) デバイスを使用するか、すべてのハードウェア管理コンソールおよび IBM Power Systems サーバーをファイアウォールで保護することができます。また、HMC をリモートで使用しない場合や HMC へのアクセスを禁止したい場合は、HMC でネットワーク・サービスを無効にすることもできます。 HMC でネットワーク・サービスを無効にするには、以下の手順を実行します。

1. SSH ポートを使用して、リモート・コマンドの実行を無効にします。
2. リモート仮想端末 (VTerm ポート) を無効にします。
3. リモート Web アクセス (HMC グラフィカル・ユーザー・インターフェースおよび REST API) を無効にします。
4. HMC ネットワーク設定を使用して、構成済みの各イーサネット・ポートについて、ファイアウォールでポートをブロックします。

NIST SP 800-131A 準拠モードで HMC を設定する方法

HMC バージョン 8.1.0 以降では、HMC を準拠モードで設定する場合、NIST SP 800-131A にリストされている強固な暗号のみがサポートされます。Transport Layer Security (TLS 1.2) をサポートしない古い Power Systems サーバー (POWER5 サーバーなど) に接続できなくなる可能性があります。 セキュリティー・モードの変更について詳しくは、HMC V8R8 NIST mode を参照してください。

HMC で使用する暗号を表示および変更する方法

HMC バージョン 8.1.0 以降では、HMC は NIST 800-131A で定義されているより安全な暗号セットをサポートします。 デフォルト・モードで使用される暗号は強固です。HMC で使用されている暗号鍵の詳細を確認するには、**lshmcencr** コマンドを実行します。企業標準によって別の暗号セットを使用する必要がある場合は、**chhmcencr** コマンドを実行して暗号鍵を変更してください。

ユーザー・パスワードを暗号化するために HMC で使用されている暗号鍵をリストするには、次のコマンドを実行します。

```
lshmcencr -c passwd -t c
```

HMC Web ユーザー・インターフェースおよび REST API で現在使用できる暗号鍵をリストするには、次のコマンドを実行します。

```
lshmcencr -c webui -t c
```

HMC SSH インターフェースで 現在使用できる暗号鍵および MAC アルゴリズムをリストするには、次のコマンドを実行します。

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

HMC 上の証明書の強度を確認する方法

HMC 上の自己署名証明書は、2048 ビット RSA 暗号化対応の SHA256 を使用します。これは強固です。CA 署名証明書を使用する場合は、1024 ビット暗号化を使用しないでください。これは脆弱です。 HMC では、以下の証明書を使用できます。

- CA 署名証明書は、HMC グラフィカル・ユーザー・インターフェースおよび REST API (ポート 443 および 12443) で使用できます。
- HMC 間通信では、ポート 9920 が使用されます。この証明書を独自の証明書に置き換えることはできません。

自己署名証明書 (デフォルト) または CA 署名証明書のどちらを使用するかを選択する方法

HMC は、インストール時に証明書を自動生成します。ただし、HMC から証明書署名要求 (CSR) を作成し、認証局によって発行された新規証明書を取得することもできます。 この証明書を HMC にインポートできます。必ず、HMC のドメイン・ネームも取得してください。 HMC での証明書の管理について詳しくは、証明書管理を参照してください。

HMC の監査方法

ハードウェア管理コンソールでの監査は、構成されている暗号と、さまざまな HMC ユーザーの使用活動にフォーカスしています。 さまざまな HMC ユーザーの使用活動を表示するには、以下のコマンドを使用します。

表 *37. HMC* で使用されている暗号

目的	**コマンド**
パスワード暗号化 (グローバル設定)	`lshmcencr -c passwd -t c`
各ユーザーのパスワード暗号化	`lshmcusr -Fname:password_encryption`
SSH 暗号	`lshmcencr -c ssh -t c`
SSH MAC	`lshmcencr -c sshmac -t c`
HMC グラフィカル・ユーザー・インターフェースおよび REST API に使用されている暗号	`lshmcencr -c webui -t c`

HMC で使用するさまざまなコンソールおよびサービス可能イベントの情報をモニターするには、以下のコマンドを使用します。

表 *38. HMC* でログオン・ユーザーとコンソールまたはサービス可能イベントの情報を表示するためのコマンド

情報	**コマンド**
GUI ユーザー	`lslogon –r webui –u`
GUI タスク	`lslogon –r webui –t`
CLI ユーザー	`lslogon –r ssh –u`
CLI タスク	`lslogon –r ssh –t`
HMC 上の操作	`lssvcevents -t console -d <number of days>`

表 38. HMC でログオン・ユーザーとコンソールまたはサービス可能イベントの情報を表示するためのコマンド (続き)	
情報	**コマンド**
システム上の操作	`lssvcevents –t hardware –m <managed system> -d <number of days>`

一元管理された HMC のイベントのモニター: 多くのハードウェア管理コンソールを使用している場合、`rsyslog` ファイルを設定してすべての使用データを収集します。

IBM が HMC セキュリティーの脆弱性を修正する方法

IBM には、IBM Product Security Incident Response Team (PSIRT) と呼ばれるセキュリティー・インシデント対応プロセスがあります。IBM 製品セキュリティー・インシデント対応チーム (PSIRT) は、IBM オファリングに関連したセキュリティーの脆弱性に関する情報の受領、検証、および内部調査を管理するグローバル・チームです。 HMC に付属のオープン・ソースおよび IBM のコンポーネントは、アクティブにモニターおよび分析されます。 サポートされるすべてのリリースの HMC について、暫定修正およびセキュリティー修正が IBM によって提供されます。

HMC に対する新規の暫定修正を追跡する方法

セキュリティー情報には、サポートされる HMC バージョンの脆弱性および暫定修正に関する情報が含まれます。 HMC に対する暫定修正を追跡するには、以下のようにします。

- 最新のセキュリティー情報を IBM Security Bulletin で検索します。
- Twitter で @IBMPowereSupp をフォローし、通知を受け取ります。
- IBM サポートで E メール通知に登録します。

HMC ポートの位置

ロケーション・コードを使用して、ポート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 5105-22E、 9008-22L、9009-22A、9009-22G、9223-22H、および 9223-22S の HMC ポート位置

以下の図と表を使用して、5105-22E、 9008-22L、9009-22A、9009-22G、9223-22H、および 9223-22S 上の HMC ポートの位置を対応させます。

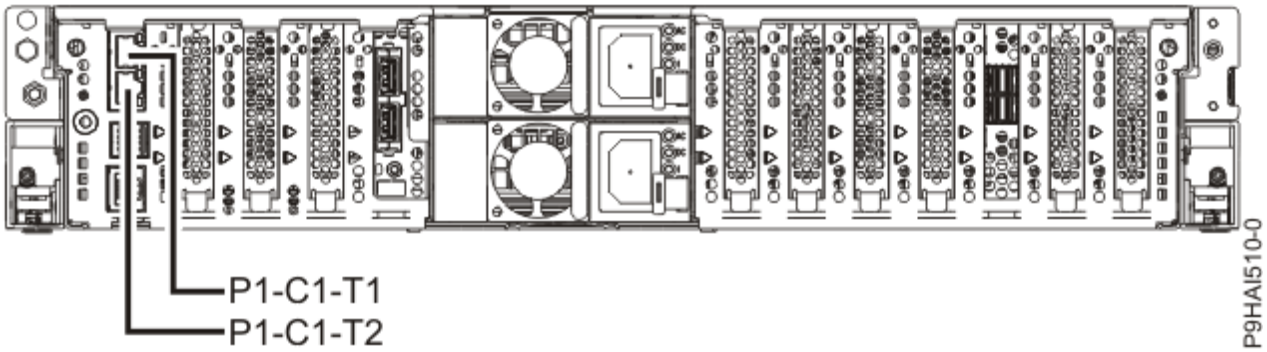


図 *10. 5105-22E、 9008-22L、9009-22A、9009-22G、9223-22H、および 9223-22S HMC* ポートの位置

表 *39. 5105-22E、 9008-22L、9009-22A、9009-22G、9223-22H、および 9223-22S HMC* ポートの位置		
ポート	**物理ロケーション・コード**	**識別 LED**
HMC ポート 1	Un-P1-C1-T1	いいえ
HMC ポート 2	Un-P1-C1-T2	いいえ
5105-22E、 9008-22L、9009-22A、9009-22G、9223-22H、または 9223-22S の HMC ポートの位置について詳しくは、9008-22L、9009-22A、9009-22G、9223-22H、または 9223-22S の部品の位置とロケーション・コードを参照してください。		

モデル 9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、および 9223-42S の HMC ポート位置

以下の図と表を使用して、9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、および 9223-42S 上の HMC ポートの位置を対応させます。

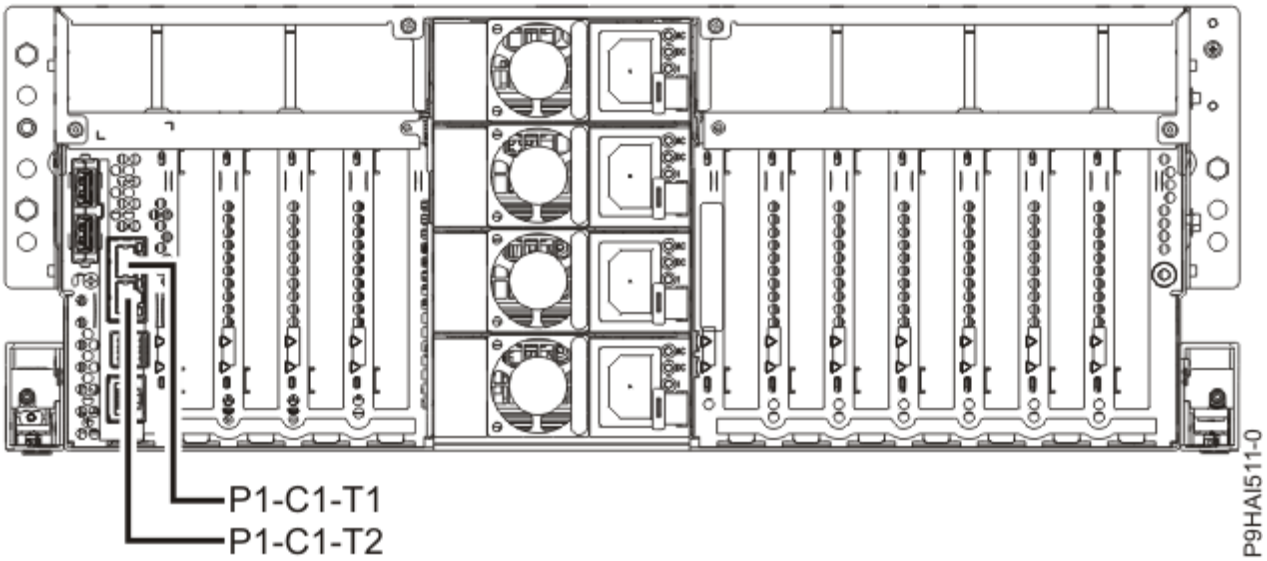


図 *11. 9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、および 9223-42S HMC* ポートの位置

表 *40. 9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、および 9223-42S HMC* ポートの位置		
ポート	**物理ロケーション・コード**	**識別 LED**
HMC ポート 1	Un-P1-C1-T1	いいえ
HMC ポート 2	Un-P1-C1-T2	いいえ
9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、または 9223-42S の HMC ポートの位置について詳しくは、9009-41A、9009-41G、9009-42A、9009-42G、9223-42H、または 9223-42S の部品の位置とロケーション・コードを参照してください。		

モデル 9040-MR9 の HMC ポート位置

以下の図と表を使用して、9040-MR9 上の HMC ポートを対応させます。

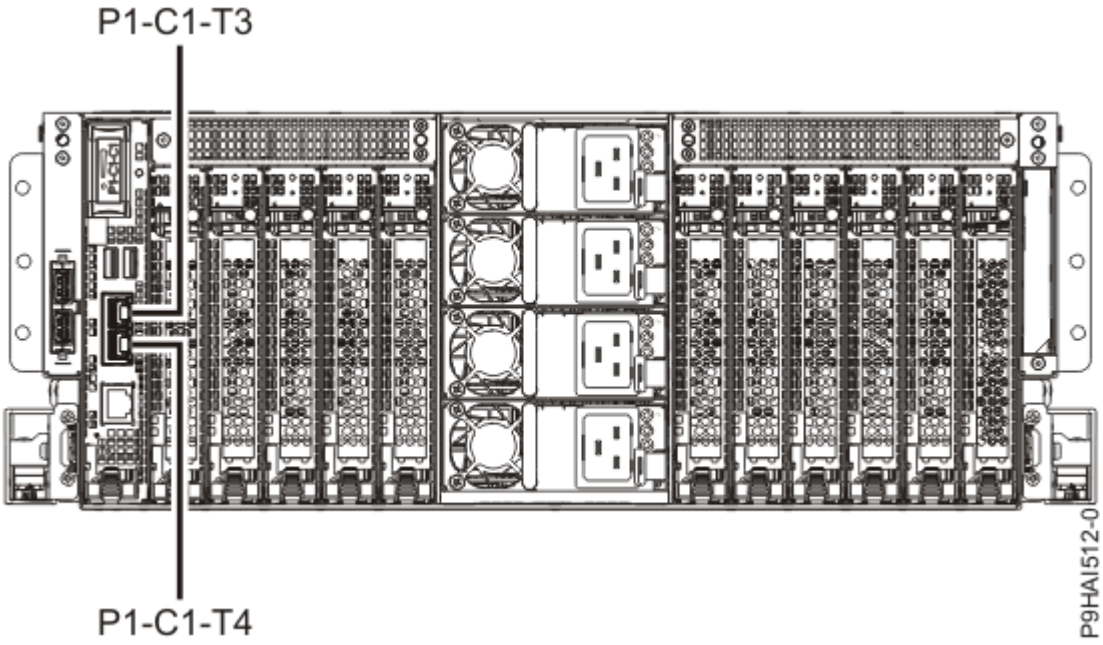


図 *12. 9040-MR9 の HMC* ポート位置

表 *41. 9040-MR9 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-C1-T3	いいえ
HMC ポート 2	Un-P1-C1-T4	いいえ
9040-MR9 の HMC ポート位置について詳しくは、部品の位置とロケーション・コードを参照してください。		

モデル 9080-M9S の HMC ポート位置

以下の図と表を使用して、9080-M9S 上の HMC ポートを対応させます。

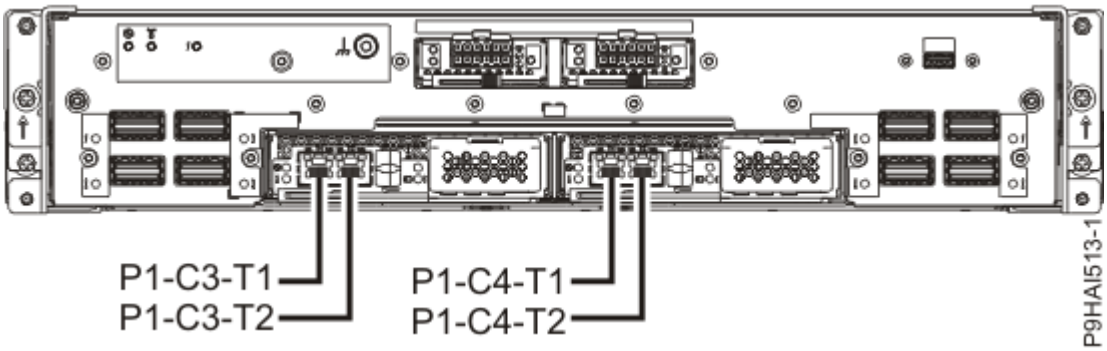


図 *13. 9080-M9S の HMC* ポート位置

表 *42. 9080-M9S の HMC* ポート位置		
ポート	**物理ポート・ロケーション**	**識別 LED**
サービス・プロセッサー・カード 1 - HMC ポート 1	Un-P1-C3-T1	いいえ
サービス・プロセッサー・カード 1 - HMC ポート 2	Un-P1-C3-T2	いいえ

表 *42. 9080-M9S の HMC* ポート位置 *(*続き*)*		
ポート	**物理ポート・ロケーション**	**識別 LED**
サービス・プロセッサー・カード 2 - HMC ポート 1	Un-P1-C4-T1	いいえ
サービス・プロセッサー・カード 2 - HMC ポート 2	Un-P1-C4-T2	いいえ
9080-M9S の HMC ポート位置について詳しくは、部品の位置とロケーション・コード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で提供し、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証できません。 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、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ー機能

アクセシビリティー機能は、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ー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。アクセシビリティー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、アクセシビリティーに対応しています。IBM Knowledge Center のアクセシビリティー機能は、IBM Knowledge Center のヘルプの『アクセシビリティー』セクション (www.ibm.com/support/knowledgecenter/help#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ー機能については、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ー情報については、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ー情報

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)

アクセシビリティーに対する IBM の取り組みについて詳しくは、IBM アクセシビリティー (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・オファリング」) 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・オファ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・オファリング」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・オファリング」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・オファリングは、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・オファリング」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 プライバシー・ステートメント』 (https://www.ibm.com/jp-ja/privacy)、およびセクション『クッキー、ウェブ・ビーコン、その他のテクノロジー』の『IBM オンライン・プライバシー・ステートメント』(https://www.ibm.com/jp-ja/privacy/details) を参照してください。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、Web 上で「Copyright and trademark information」をご覧ください。

登録商標 Linux は、世界中で商標の所有者である Linux Torvalds の独占的ライセンシーである Linux Foundation のサブライセンスに従って使用されています。

Red Hat、JBoss、OpenShift、Fedora、Hibernate、Ansible、CloudForms、RHCA、RHCE、RHCSA、Ceph、および Gluster は、米国およびその他の国で Red Hat, Inc. またはその子会社の米国およびその他の国における登録商標もしくは商標です。

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。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

電波障害規制特記事項

クラス A 表示

以下のクラス A 表示は、POWER9 プロセッサーを搭載した 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。

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。

Canada Notice

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

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization 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.

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Germany Notice

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-Mitgliedsstaatenund 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 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.

一般社団法人 電子情報技術産業協会 (JEITA) の特記事項

（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、20 A/相以下の製品に適用されます。

高調波電流規格 JIS C 61000-3-2 適合品

この表示は、20 A/相 (単相) を超える製品に適用されます。

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/相 (3 相) を超える製品に適用されます。

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

一般財団法人 VCCI 協会 (VCCI) の特記事項

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

Korea Notice

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

People's Republic of China Notice

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。

Russia Notice

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

Taiwan Notice

警告使用者：
此為甲類資訊技術設備，
於居住環境中使用時，可
能會造成射頻擾動，在此
種情況下，使用者會被要
求採取某些適當的對策。

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

United States Federal Communications Commission (FCC) Notice

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. Proper cables and connectors are available from IBM-authorized dealers.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.

Responsible Party:
International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

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。

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。

Canada Notice

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

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization 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.

German Notice

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-Mitgliedsstaatenund 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 55032 Klasse B

一般社団法人 電子情報技術産業協会 (JEITA) の特記事項

（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、20 A/相以下の製品に適用されます。

高調波電流規格 JIS C 61000-3-2 適合品

この表示は、20 A/相 (単相) を超える製品に適用されます。

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/相 (3 相) を超える製品に適用されます。

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

一般財団法人 VCCI 協会 (VCCI) の特記事項

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

Taiwan Notice

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

United States Federal Communications Commission (FCC) Notice

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 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.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

使用条件

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

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

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

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

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

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

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

IBM は、これらの資料の内容についていかなる保証もしません。 これらの資料は、特定物として現存するままの状態で 提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。