IBM BladeCenter HC10 ワークステーション・ブレードのインプリメント

新しいブレード・ソリューションの概念と利点の紹介

システムを構成する製品とテクノロジーの説明

デバイスの構成方法および管理方法の説明

David Watts
Ben Karchner
Ricky Fritz
Mark Kohan

Redpaper

ibm.com/redbooks

International Technical Support Organization

IBM BladeCenter HC10
ワークステーション・ブレードのインプリメント

March 2008

SG88-4029-00

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

First Edition (March 2008)

本書は、CP20 および HC10 圧縮カード・ファームウェアのバージョン 0.17 をベースとした、IBM BladeCenter HC10、マシン・タイプ 7996 に適用されます。

2008 年 10 月現在、ファームウェアのバージョンは 1.7、ファームウェアのビルド ID は v163 です。

本書は 2008 年 3 月 19 日に作成または更新されました。

注 : 本書は GA 前のバージョンの製品に基づいており、本製品が一般出荷可能になったときには適用されない場合があります。最新情報については、製品資料または本書の後続版を参照することをお勧めします。

目次

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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。

〒 106-8711
東京都港区六本木 3-2-12
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を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

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

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

IBM は、お客様が提供するいかなる情報も、お客様に対してな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。

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。

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

著作権使用許諾 :

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

商標

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

Redbooks (ロゴ)  ®	IBM®	RETAIN®
BladeCenter®	PowerExecutive™	System x™
Calibrated Vectored Cooling™	Predictive Failure Analysis®	Tivoli®
IntelliStation®	Redbooks®	Wake on LAN®

Active Directory、ESP、Internet Explorer、Microsoft、Windows Vista、Windows、および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Intel、Intel Core、Pentium、Pentium 4、Intel ロゴ、Intel Inside ロゴ、および Intel Centrino ロゴは、Intel Corporation または子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。

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

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

前書き

IBM® BladeCenter® HC10 は、BladeCenter ファミリーの新しいブレード製品です。HC10 を使用すれば、強力なワークステーションをデスクの下で稼働させるために生じる騒音、熱、およびスペースの問題を心配せずに、高性能ユーザー・コンピューティングを利用できます。

HC10 は、ハイ・セキュリティーと管理の容易性を備えている上、グラフィックス性能に優れ、USB の互換性を備えており、ワークステーション・アプリケーション向けのサーバー・ベースのコンピューティング・テクノロジーを提供します。組み込まれた機能は、エンジニアリング・デザイン・アプリケーション、取引所などで使用される金融アプリケーション、地理情報システム・アプリケーション、遠隔コラボレーションなどに最適です。

HC10 のアーキテクチャーは、サーバー・チップ・セットではなく Intel® Core 2 Duo デスクトップ・チップ・セットをベースにしており、パワー・ユーザーに適したパフォーマンス特性を実現しています。このシステムは Microsoft® Windows® Logo Program の認定を受けており、Microsoft Windows アプリケーションとの互換性が最大限に保証されています。

本書では、IBM BladeCenter、IBM BladeCenter HC10 ワークステーション・ブレード、および IBM CP20 ワークステーション・コネクション・デバイスのテクノロジーと設計について説明します。CP20 は、モニターと USB デバイスが取り付けられ、各ユーザーのデスクに置かれます。本書では、HC10 ソリューションのインプリメントに必要な計画を段階的に説明します。本書には、CP20 から HC10 への接続を管理するコネクション・ブローカーのインプリメント方法を説明する章があります。また、構成オプションと管理インターフェースについての詳しい説明もあります。

本書は、HC10 ソリューションの導入計画の策定、導入実施手順を理解する必要があるお客様、IBM ビジネス・パートナー、および IBM 従業員を対象としています。

本書の執筆チーム

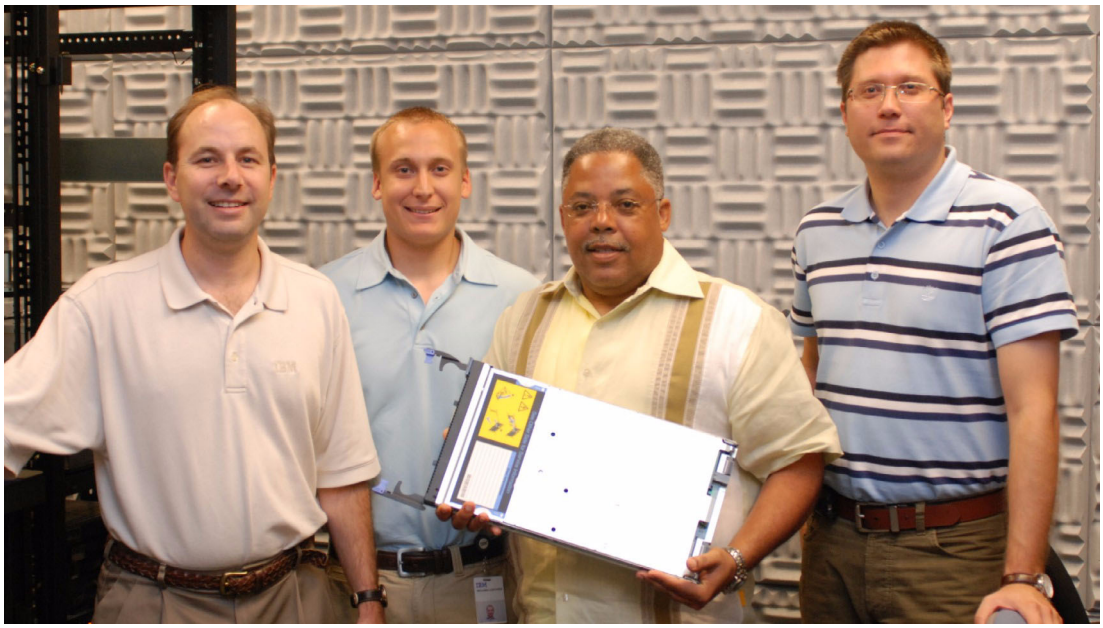
本書は、IBM International Technical Support Organization (ITSO)、ラーレー・センターに勤務する、世界中から集まった専門家のチームによって制作されました。

David Watts は、ラーレーの IBM ITSO Center に勤務するコンサルティング IT スペシャリストです。実習生を指揮して、IBM System x™ と BladeCenter サーバー、および関連クライアント・プラットフォームのハードウェアとソフトウェアに関するトピックの IBM Redbook® 出版物を制作しています。80 冊を超える Redbook、Redpaper、および技術情報の著作があります。クイーンズランド大学（オーストラリア）で工学士号を取得し、1989 年から米国とオーストラリアの両方で IBM に勤務しています。同氏は IBM が認定した IT スペシャリストです。

Ricky Fritz は、IBM System x および IBM BladeCenter の分野のエキスパートで、ジョージア州アトランタの IBM Sales and Distribution Techline 組織に勤務しています。IT 業界での経験は 20 年を超え、最初は米空軍電子セキュリティー部隊に所属し、続いて Microsoft および Ingram Micro で販売、Compaq では販売管理に携わりました。IBM での勤務は 10 年を超え、System x と BladeCenter の販売とソリューションをサポートしています。専門分野は、デジタル・メディア・ソリューション設計、仮想クライアント・インフラストラクチャー (デスクトップ) ソリューションなどです。同氏はシニア IT スペシャリストであり、IBM の System x および BladeCenter テクニカル・セールス・スペシャリストです。

Ben Karchner はペンシルベニア州立大学の学部生です。現在は、情報科学およびテクノロジー分野の理学士号取得に取り組んでいます。主に重点を置いている分野は、情報技術の統合と応用です。

Mark Kohan は、ハンガリーで IBM に勤務するフィールド技術サポート・スペシャリストです。



執筆チーム (左から右へ): David、Ben、Ricky、Mark

このプロジェクトにご協力いただいた次の方々に感謝いたします。

IBM ITSO:

- Carolyn Briscoe
- Linda Robinson
- Margaret Ticknor
- Jeanne Tucker
- Erica Wazewski
- Debbie Willmschen

IBM Corporation:

- Richard Brothers
- Markesha Farmer
- Jordan Hibbits
- Makoto Ono
- Charles Perkins
- Stephen Poe
- Junjiro Sumikawa
- Ed Suffern
- Shawn Walsh

Devon IT, Inc:

- Bill Horrocks
- Ian Geiser
- J. Adam Knudsen
- Paul Mancini

- Stephane Verdy

Leostream:

- David Crosbie

Teradici™ Corporation:

- Kurt Fennig
- Ziad Lammam
- Chris Michael
- Andrew Preston
- Ken Unger
- Brian Zingle

そのほかに、次の方から寛大なご支援をいただきました。

- Nick Pellegrene、ペンシルベニア州立大学

執筆にご協力ください

2 週間から 6 週間の実習プログラムに加わりませんか。特定の製品またはソリューションを扱う書籍の作成を手伝い、最先端のテクノロジーを実地で経験できます。IBM の技術プロフェッショナル、ビジネス・パートナー、およびお客様と、チームとして協働する機会が得られます。

ご協力いただければ、製品の認知度とお客様の満足度の向上につながります。加えて、IBM 開発研究所との連絡ネットワークが構築され、生産性と市場性が向上します。

実習プログラムの詳細は、次の URL で実習のインデックスをご覧の上、オンラインにてお申し込みください。

ibm.com/redbooks/residencies.html

コメントをお寄せください

お客様のコメントを大切にしています。

弊社では、Redpaper を可能な限り役に立つものにしていきたいと考えています。本書や他の IBM Redbooks に関するコメントを、次のいずれかの方法でお送りください。

- 次のアドレスにある「**Contact us**」をクリックして、オンラインの Redbooks レビュー・フォームにアクセスしてください。

  ibm.com/redbooks

- 次の宛先に、E メールでコメントをお寄せください。

  redbooks@us.ibm.com

- 次の宛先に、手紙でコメントをお寄せください。

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

BladeCenter の概要

この章では、IBM BladeCenter の概要について説明します。BladeCenter シャーシの機能、およびブレード・サーバー、ワークステーション、およびネットワーク・オプションの機能について解説します。また、2002 年の発表以来、ブレード市場に変革を起こした BladeCenter の柔軟で適応性のあるモジュラー設計についても説明します。

この章で説明するトピックは、次のとおりです。

1.1 BladeCenter シャーシ

ブレード・サーバーは、プロセッサー、メモリー、ストレージ、ネットワーク・コントローラー、オペレーティング・システム、およびアプリケーションを備えたサーバーです。これらのブレードは、本棚に収められた本のように、IBM BladeCenter と呼ばれる *シャーシ* に垂直に収納されます。

ブレード・サーバーは、次の主な利点を備えているため、サーバー市場では最も急速に成長している分野です。

- 格納密度

  スペースの使用効率が非常に高くなるように、格納装置 (シャーシ) 内でブレードとモジュールが配置されており、一般的には従来型のサーバーよりも高いサーバー密度を実現しています。ブレード・サーバーを使用すれば、従来型のサーバーの使用時よりも数倍高いラック密度が得られます。

- ケーブル管理

  従来型のサーバーの数が増えると、電源、管理、ネットワーキング、キーボード、ビデオ、マウスなどに必要なケーブルの数が増加の一途をたどります。標準 1U サーバーを格納する業界標準の典型的なフルラック (42U) には、数百本ものケーブルが必要になることがあります。サーバー・ブレードを格納するフルラック (42U) に必要なケーブルは数十本と少数なので、信頼性が向上し、複雑さが軽減され、コストが削減されます。

- セットアップおよび構成のコスト

  シャーシの台数と取り付け金具が少ないので、サーバー管理上問題になるいくつかの面が改善されます。例えば、サーバーのラックを組み立てて構成するために必要な時間、誤りが起こる可能性、セットアップと構成を実施するために必要なスキル・レベルの問題などです。この利点は、サプライヤーが事前構成済みのラックを提供する場合や、データ・センター内でカスタム構成を行う場合のコスト節約につながります。

- インフラストラクチャー統合

  従来型のデータ・センター・インフラストラクチャーの特徴としては、サーバー用のボックスと、ネットワーキングおよびストレージ・エリア・ネットワーク (SAN) 機器用のボックスが物理的に分離しています。サーバー・ブレード・アーキテクチャーを利用すれば、ネットワーキングと SAN スイッチをシャーシに組み込むことができます。*物理統合* が実現すれば、運用と管理を統合するプラットフォームが確立され、ネットワークとサーバー全体を通じて切れ目のないサービス品質が得られ、サーバー、ネットワーク、およびストレージのシステム管理を単一の視点で行うことができます。

- 信頼性・可用性・保守性

  従来型のラック・マウント・サーバーとは異なり、サーバー・ブレード・ノードを交換するために、工具を使用して取り付け金具を操作したり、ケーブルを取り外したりする必要はありません。サーバー・ブレードを取り外すには、シャーシ・ベゼルを開き、ロック機構を解放するだけです。また、サーバー・ブレードでは *ホット・スワップ* ・コンポーネントを容易に交換できます。多くのラック・マウント 1U フォーム・ファクター・サーバーでは、これらのコンポーネントの交換は容易ではありません。また、サーバー・ブレードの設計により、ネットワークやディスク I/O のコンポーネントが取り扱いやすくなっており、シャーシ内のスイッチの保守やアップグレードが容易です。

- コスト

  サーバー・ブレード・シャーシの内容と構造によって、ノード密度が高まるほどサーバー・ノード増設の実質的なコストを削減できます。このコスト削減は、*ノード償却* によって実現します。ノード償却とは、シャーシ・フレーム、ミッドプレーン、電源、

ファン、CD、ディスケット・ドライブ、その他の I/O が共用され、償却されていくことを意味します。また、従来型のラック・マウント・サーバーと比べて、大幅な省電力が実現します。

- 柔軟性のある機能とテクノロジー

  交換可能なプロセッサー・ブレードやその他のモジュール (ネットワーク・ルーター、SAN スイッチ、電源など) により、お客様はサーバー・システム全体を交換することなく、新しいテクノロジーや代替テクノロジーを容易に活用できます。この柔軟性によってシャーシの有用性が保たれ、陳腐化を防ぐことができます。

BladeCenter シャーシ内では、個々のブレードがリソースを共用できます。例えば、電源、ファン、スイッチ、さらにオプティカル・ドライブ、USB、シリアル・ポート、管理インターフェースなどのリソースが共用可能です。これらのリソースは、シャーシに格納されたブレードによって共用されます。シャーシ前面のブレード・ベイに、最大 14 台のブレード・サーバーまたはワークステーションを取り付けることができます (図 1-1 を参照)。このリソースの共用により、ブレード管理が容易になり、ラック密度の増加によってパフォーマンスが向上します。BladeCenter はシャーシ内で完全な冗長性を備え、ネットワークとストレージの統合を可能にします。

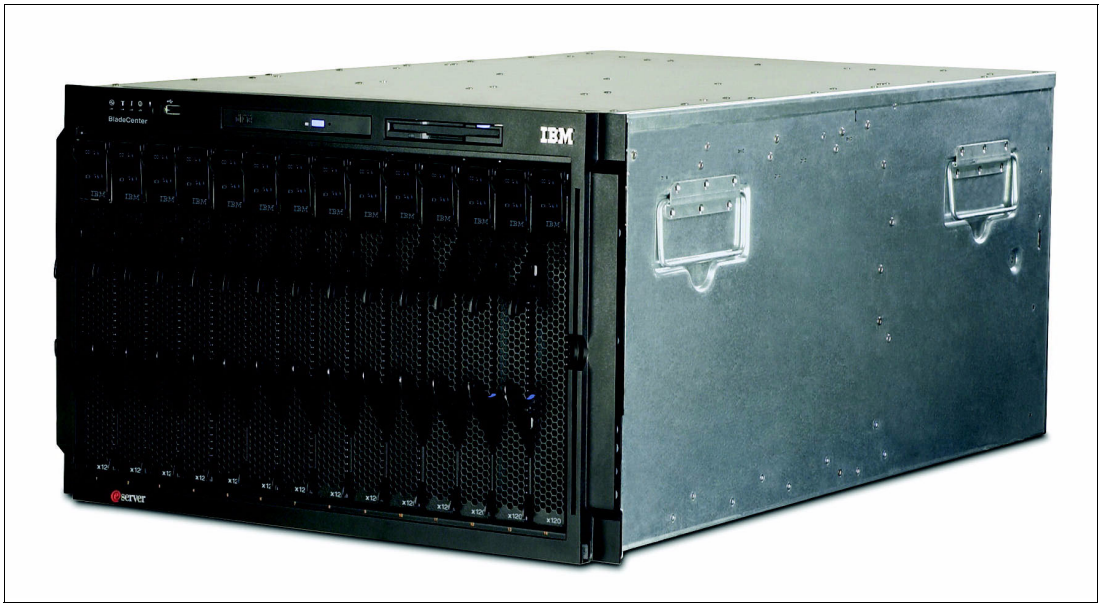


図 1-1　最大 14 台のサーバーまたはワークステーションを取り付けることができる BladeCenter E

それぞれの BladeCenter シャーシには、*アドバンスト・マネージメント・モジュール* が標準装備されています。アドバンスト・マネージメント・モジュールは、取り付けられた BladeCenter コンポーネントすべての構成および管理に使用するホット・スワップ・デバイスです。BladeCenter シャーシ内のブレードすべてに対して、システム管理機能とキーボード・ビデオ・マウス (KVM) 機能 (セレクタ式) を提供します。リモート管理アクセス用のイーサネット接続とシリアル・ポート接続を制御します。冗長化のために、第 2 のアドバンスト・マネージメント・モジュールを取り付けることもできます。

BladeCenter シャーシ用に幅広い IBM およびサード・パーティー製のスイッチが利用でき、イーサネット、ファイバー・チャネル、および InfiniBand® の各ネットワークに接続できます。

BladeCenter ファミリーには 5 種類のシャーシが存在します。

- IBM BladeCenter E。最も高密度で、共通ファブリック・サポートを提供します。
- IBM BladeCenter S。小規模から中規模のビジネス、および支社向けソリューションを利用したい大企業に最適です。
- IBM BladeCenter H。ハイパフォーマンス、最高の信頼性、最も要求の厳しい IT 環境に対応するきわめて高い柔軟性を備えています。
- IBM BladeCenter T。特に通信ネットワーク・インフラストラクチャーなどの厳しい環境に対応できるように設計されています。
- IBM BladeCenter HT。ハイパフォーマンスの柔軟な通信環境に対応できるように設計され、10G イーサネットなどの高速インターネットワーキング・テクノロジーをサポートし、次世代ネットワーク (NGN) のための堅固なプラットフォームを提供します。

5 種類のシャーシすべてが、共通のブレードと標準スイッチ・モジュールのセットを共用し、さらに BladeCenter H と HT は、Nortel 10 Gb イーサネット高速スイッチ・モジュールなどの高速スイッチ用の高速 I/O ベイを装備しています。

本書では、IBM BladeCenter E と BladeCenter S を中心に説明します。

1.1.1 IBM BladeCenter E

IBM BladeCenter E は、多様なビジネス要件に対応する、高度にモジュール化されたシャーシとして設計されています。BladeCenter E は、ブレード・サーバーとブレード・ワークステーションをサポートし、さらにお客様の既存ネットワーク環境への高速接続に対応する Gigabit Ethernet、ファイバー・チャネル、InfiniBand などの幅広いネットワーキング・モジュールをサポートします。また、BladeCenter E は包括的なシステム管理のために、管理モジュールの冗長ペアもサポートします。

BladeCenter E の優れた高密度と機能セットは、革新的なシャーシ・アーキテクチャーによって実現しています。BladeCenter E はエネルギー効率の高いコンポーネントと共用インフラストラクチャー・アーキテクチャーを使用しているので、代わりによく使われるブレード・サーバー以外の設計と比べて、お客様は電力消費量を削減できます。BladeCenter E の低電力消費量と Calibrated Vectored Cooling™ によって、より多くのサーバーやワークステーションが、厳しい電源または冷却の要件がある環境に適合するようになります。

図 1-2 に、BladeCenter E とその主要コンポーネントの正面図を示します。

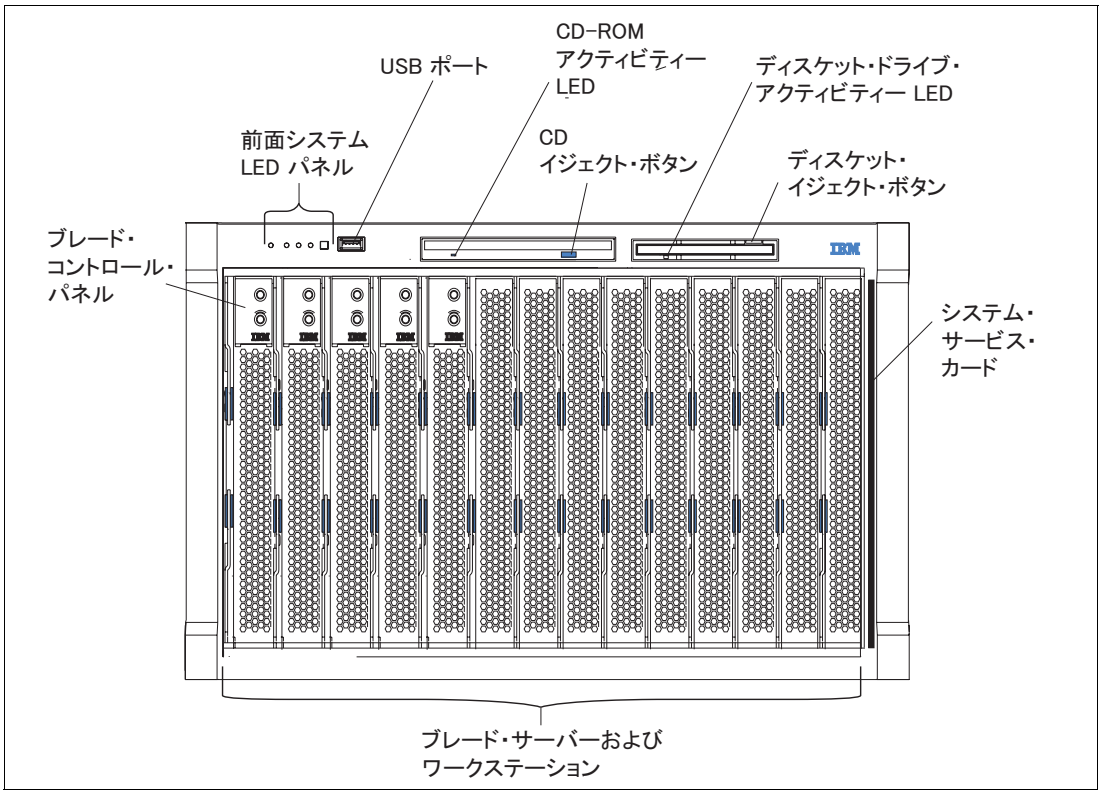


図 1-2 BladeCenter E の正面図、およびシャーシの主要な機構

図 1-3 および図 1-4 は、BladeCenter E の背面図です。

図 1-3 BladeCenter E の背面図

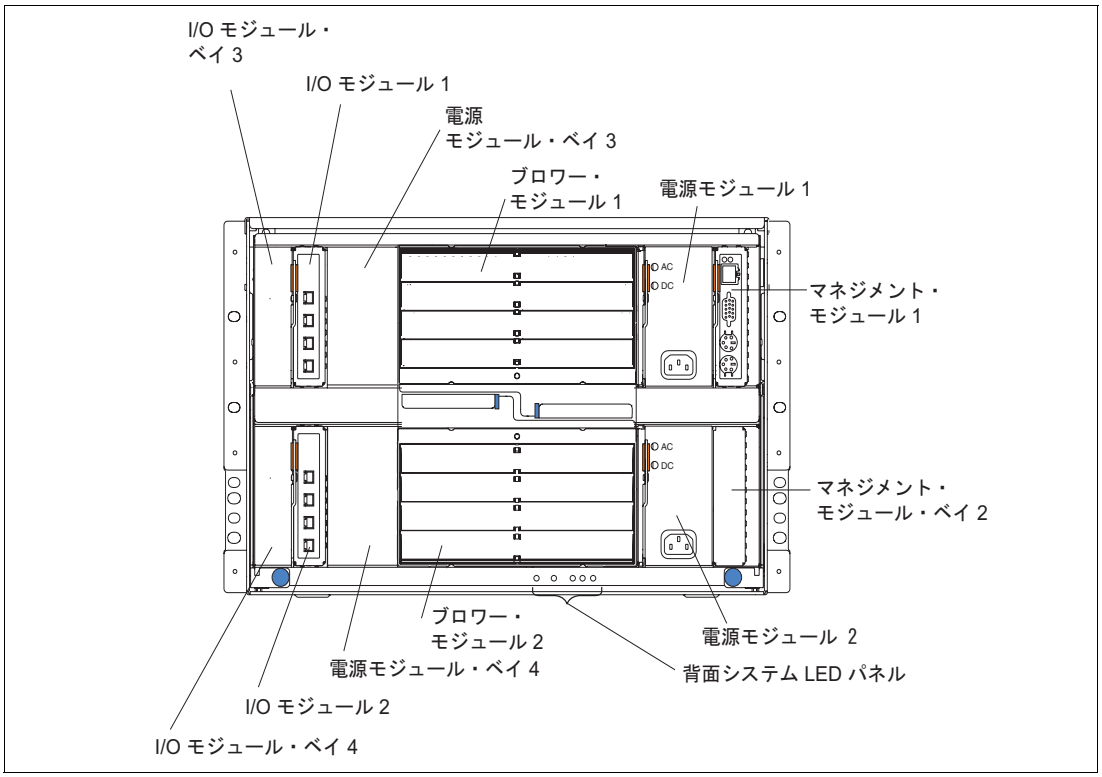


図 1-4 BladeCenter E の背面図、およびシャーシの主要な機構

BladeCenter E の背面にある主要な機構には、次のものがあります。

- ホット・スワップ I/O モジュール・ベイ 4 つ
- ホット・スワップ・マネジメント・モジュール・ベイ 2 つ (標準として 1 つのマネジメント・モジュール)
- ホット・スワップ電源モジュール・ベイ 4 つ (標準として 2 つの電源モジュール)
- ホット・スワップ・ブロワー 2 つ

BladeCenter E シャーシには、最大 14 台の単一スロット・ブレード・サーバーまたはワークステーションを取り付けることができます。電源および冷却の要件に応じて、さまざまなブレード・サーバーまたはワークステーションのモデルを 1 つのシャーシ内で組み合わせて、要件を満たすことができます。

BladeCenter E に I/O モジュールは標準装備されていません。必要な接続に応じて、これらの I/O モジュールを選択する必要があります。BladeCenter HC10 の場合は、I/O モジュール・ベイ 1 および 2 に、イーサネット・スイッチ・モジュール (ESM) が必要です。

I/O モジュール・ベイ 3 および 4 に必要な I/O モジュールは、サーバー・ブレードに取り付ける I/O 拡張カードによって異なります。ベイ 3 および 4 に取り付けられる I/O モジュールは、取り付け済みの HC10 ワークステーション・ブレードには接続されません。これは、HC10 が拡張カードの使用をサポートしないからです。

表 1-1 は、BladeCenter E シャーシの主な機構のリストです。

表 1-1 BladeCenter E の機構一覧

機構	仕様
マシン・タイプ	8677-3RU、3RX
ラックのフォーム・ファクター (H x D)	7U x 711 mm (28 インチ)
DVD/CD ドライブ (標準)	1x DVD-ROM (メディア・トレイ内)
ディスケット・ドライブ (標準)	1x 1.44 MB ディスケット・ドライブ (メディア・トレイ内)
ブレード・スロットの数	14 (30 mm ブレード・サーバーまたはワークステーション)
スイッチ・モジュール・スロットの数	ホット・スワップ 4 つ
スイッチ・モジュール (標準)	なし
パワー・サプライのサイズ (標準)	2000 ワット AC
パワー・サプライの数 (標準 / 最大)	2 / 4
ブロワーの数 (標準 / 最大)	2 / 2
寸法	高さ :305 mm (12.0 インチ) 幅 :4429 mm (17.5 インチ) 奥行き :711 mm (28.0 インチ)

1.1.2 IBM BladeCenter S

IBM BladeCenter S (マシン・タイプ 8886) は、BladeCenter ファミリーに最も新しく加わったモデルです。データ・センター外での使用に特化して設計されているという点が、BladeCenter ファミリーの中で他と異なっています。IBM は中小規模の市場からいただいたフィードバックを基に、他のモデルと同様の機能を備えながら、柔軟性とカスタマイズ性を高めたシャーシを開発しました。

このシャーシは、長年にわたる厳しいテストを経てデータ・センターで実証されたブレード・テクノロジー、110V または 220V の電源で稼働するエネルギー効率の高いパワー・サプライ、内蔵の SAS または SATA ストレージ、および最も洗練されたシステム管理機能を備えたアドバンスト・マネージメント・モジュールを搭載しています。

BladeCenter S は BladeCenter ファミリーに欠けていた部分を完全に補うもので、正式なデータ・センターの制御環境を実現できないオフィスに最適なソリューションです。

図 1-5 は、BladeCenter S シャーシの前面を示しています。前面からは、ブレード・サーバーおよびドライブを操作することができます。

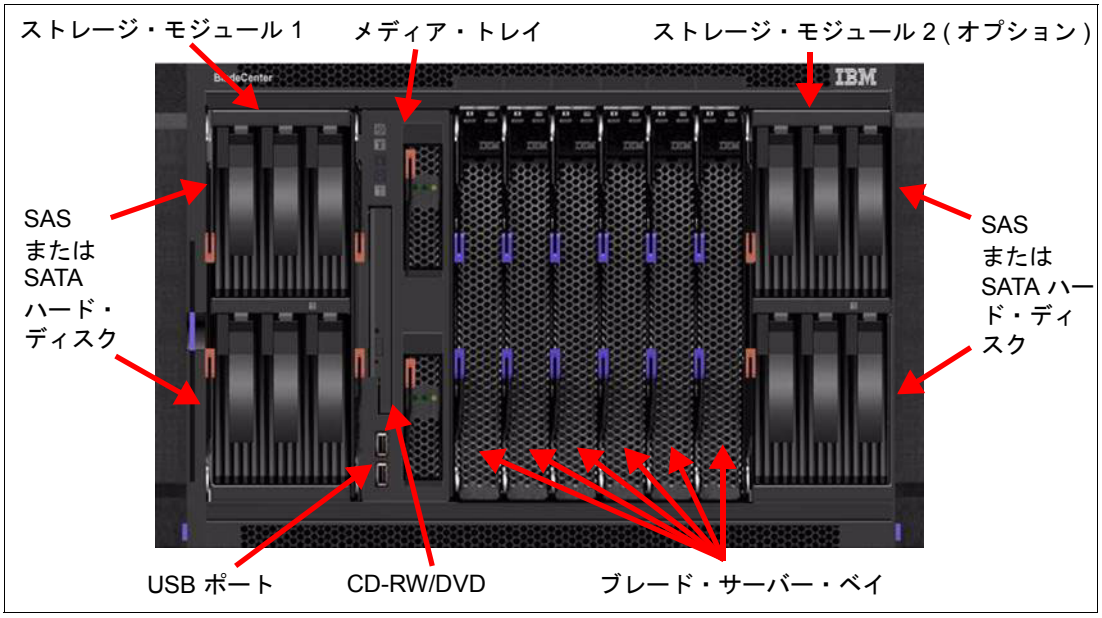


図 1-5 BladeCenter S シャーシの前面

図 1-6 は、BladeCenter S シャーシの背面を示しています。背面からは、ホット・スワップ・ファン、パワー・サプライ、および I/O モジュールを着脱することができます。

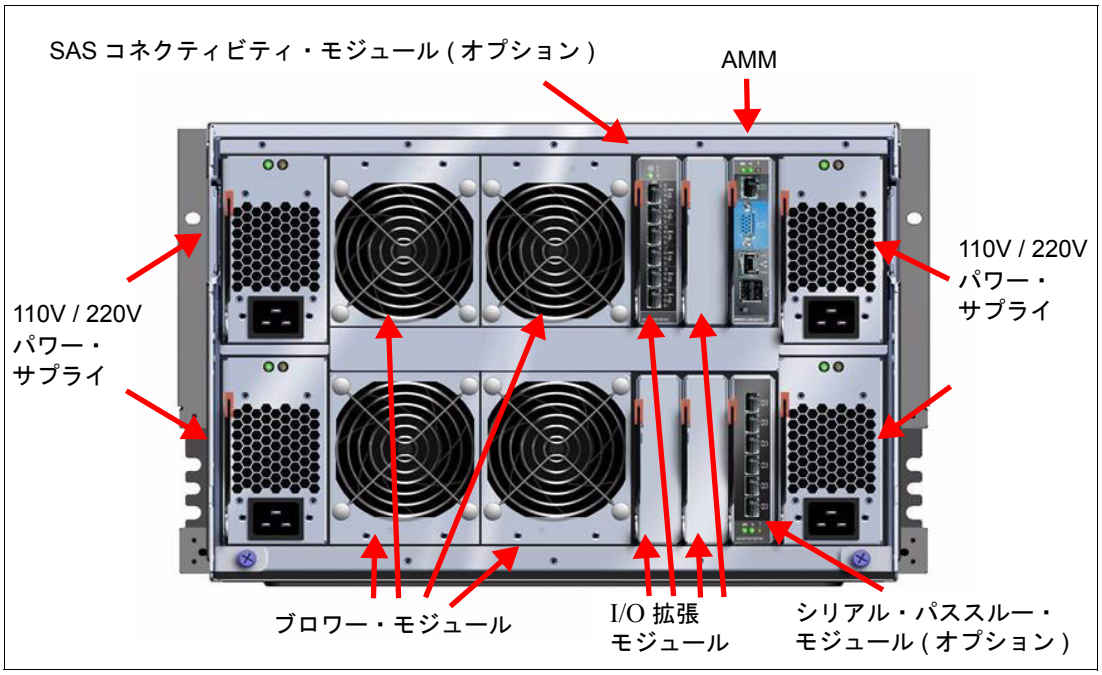


図 1-6 BladeCenter S シャーシの背面

BladeCenter S シャーシには、6 台の単一スロット・ブレード・サーバー、または 3 台の 2 スロット・ブレード・サーバーを取り付けることができます。ただし、電源と冷却の要件に応じて、モデルと幅の異なる数種類のブレード・サーバーを 1 つのシャーシに同時に組み合わせて、ほぼすべての要件をサポートできます。

表 1-2 は、BladeCenter S の主な機構を示しています。

表 1-2 BladeCenter S の機構一覧

機構	仕様
マシン・タイプ	8886-1MX、E1Y
ラックのフォーム・ファクター (H x D)	7U x 733.4 mm (28.9 インチ)
ディスク・ストレージ・モジュール (標準 / 最大)	1 / 2
DVD/CD ドライブ (標準)	1x CD-RW / DVD-ROM (メディア・トレイ内)
USB ポート (標準)	2x USB 2.0 ポート (メディア・トレイ内)
シリアル・パススルー機能	あり
ブレード・サーバー・スロットの数	6 (30 mm ブレード・サーバー)
I/O スイッチ・モジュール・ベイの数	ホット・スワップ 4 つ (1 つは予約済み)
スイッチ・モジュール (標準)	なし
パワー・サプライのサイズ (標準)	950 ワット AC (110V) または 1450 ワット AC (220V)
パワー・サプライの数 (標準 / 最大)	2 / 4
ブロワーの数 (標準 / 最大)	4 / 4
寸法	高さ :306.3 mm (12.0 インチ) 幅 :444 mm (17.5 インチ) 奥行き :733.4 mm (28.9 インチ)

1.2 システム管理

IT 管理者が、複雑な異機種混合の IT 環境を管理するという任務に直面している現在、効率的なシステム管理がこれまでにも増して重要になっています。この難題に立ち向かうお客様を支援するためには、重要な IT 作業を単純化する、必要なトレーニングの少ない直観的な自動化されたツールによって複雑さを軽減することが不可欠です。IBM BladeCenter のシステム管理コンポーネントは、IBM Director、アドバンスト・マネージメント・モジュール、および IBM Remote Deployment Manager (RDM) の組み合わせです。これらのツールを使用すれば、システム停止を減らし、IT 要員の生産性を高め、サポート・コストを削減できます。

1.2.1 IBM Director

IBM Director は、ハードウェア管理の容易性に優れたシステム管理ツールのスイートで構成されます。IBM Director は業界標準を基盤としているので、異機種混合のハードウェア・サポートが可能で、さまざまなオペレーティング・システムおよびネットワーク・プロトコルの環境で動作します。

環境でただ 1 つのシステム管理アプリケーションとして、IBM Director はハードウェア機構と設定値のインベントリーを作成し、一般的なシステム情報を取得し、事前の対策を講じたシステム管理機能を起動し、IBM のサービスおよびサポート Web ページへの直接リンクを提供する、完全な管理ソリューションを提供できます。業界標準の活用によって、他のシステム管理ツールやアプリケーションと容易に統合できます。

IBM Director が提供する機能は多岐にわたり、容易なインストールとセットアップ、自己管理型のスマート・ツール、主要なワークグループ環境やエンタープライズ・システム管理環境へのシームレス統合など、幅広い機能を備えています。IBM Director は業界標準に基づいているので、提供されているツールの多くを使用して IBM 以外のハードウェアも管理できます。

IBM Director の機能は、次のカテゴリーに分けることができます。

- インベントリー

  システム管理戦略の重要な第 1 歩は、環境にどのハードウェアが存在し、どのように構成されているか正確に把握することです。IBM Director は、検出した管理対象システムそれぞれの詳細なインベントリー・スキャンを実行します。ハードウェアとソフトウェアのデータ・ポイントが多数収集され、IBM Director データベースに格納されます。インベントリーの収集は、手動で繰り返すことも、複数の自動化プロセスによって繰り返すこともできます。

- ハードウェア状況

  IBM Director は、インストール後すぐに作動を開始し、管理対象の IBM System x サーバーに発生したハードウェアの問題をユーザーに知らせます。パワー・サプライ、ファン、電圧調節モジュール（VRM）、ネットワーク・インターフェース・カード (NIC)、またはその他のハードウェアに問題が生じた場合、IBM Director はどのような問題が発生したか、どのシステムが影響を受けているかを通知します。

- イベント管理

  すべてのシステム管理ソリューションの中心となる機能は、システムに問題が発生したときに IT スタッフにアラートを出す能力です。IBM Director は、*イベント・アクション・プラン* と呼ばれる、独自の非常に強力なアラート方式を備えています。この方式により、行われるアクションとは独立してイベント・トリガーを定義できます。その後、これら 2 種類の項目を組み合わせてカスタマイズされたアクションの計画を簡単に作成でき、個別またはグループ単位の管理対象システムに割り当てることができます。

- プロセス管理

  IBM Director のプロセス管理タスクを使用して、ご使用の環境で実行されている重要なプロセスすべてを追跡できます。IBM Director は、モニター対象のプロセスが開始した、停止した、または開始に失敗した場合に、アラートを出すことができます。サポートされる Windows オペレーティング・システムを実行する管理対象システム上で、インストールされているすべてのサービスおよびデバイス・ドライバーから状況を取得することもできます。

- リソース管理

  リソース管理は、IT 環境を常にピークの効率で稼働させるために重要な側面です。いずれかのシステムが過負荷状態になっていないか、ワークロードの需要に対応できなくなっていないか知ることは重要です。IBM Director は、多数のシステム・リソースをモニターし、これらのリソースに対して個別またはグループ単位のしきい値を設定し、リソースしきい値を超過したときにアラートを出す機能を備えています。

- リモート管理

  IBM Director には、リモート管理を実行する機能が組み込まれています。ローカル・システム上で実行できる管理タスクはすべて、ネットワーク接続が使用可能である限り、はるか遠く離れたシステム上でも実行できます。また、IBM Director のリモート制御タスクにより、管理対象環境にある管理対象システムを制御できます。

- 更新管理

  IBM Director 5.20 で新しく導入された更新マネージャーは、ネイティブ IBM Director タスクによって更新管理を実行します。更新機能には、プロファイルの作成、更新のダウンロード、プロファイル内で定義された更新とシステムとの比較、レポートの生成などがあります。

- 一括構成

  IBM Director を使用したシステム管理の利点の 1 つは、特定の構成変更を複数の管理対象システムに対して一度に実行できることです。動的ホスト構成プロトコル（DHCP）対応の環境であっても、重要なサーバーの多くは固定アドレスを使用する傾向にあります。一括構成プロファイルを使用すれば、例えばこれらの管理対象システムが 1 次 DNS サーバーの位置指定に使用する IP アドレスを変更でき、それぞれのシステムに物理的に出向く必要はありません。

- SNMP 管理

  IBM Director エージェントを実行するシステムに対して IBM Director が実行できる高度な管理機能に加えて、SNMP デバイスの検出および管理も可能です。IBM Director は、SNMP トラップを送受信し、これらのトラップを IBM Director ネイティブのアラートに変換できるので、未加工の SNMP トラップが通常提供できる情報よりさらに有用な情報が提供されます。

1.2.2 アドバンスト・マネージメント・モジュール

アドバンスト・マネージメント・モジュールは、BladeCenter シャーシ自体、取り付けられたネットワーキング・モジュール、および取り付けられたすべてのブレードを管理します。

アドバンスト・マネージメント・モジュールには内蔵 KVM スイッチ、および内蔵ネットワーク・スイッチが備わっており、イーサネット・スイッチ・モジュール (ESM)、ファイバー・チャネル・スイッチ・モジュールなど、あらゆるモジュールへの内部 IP 接続によってブレードを管理できます。アドバンスト・マネージメント・モジュールは、すべてのブレードに組み込まれたサービス・プロセッサーと通信します。

アドバンスト・マネージメント・モジュールに組み込まれた Web インターフェースを使用して、モジュールとブレードそれぞれの状況を管理および検査したり、ブレードをリモート側から制御したり、ブレードを再始動したりでき、その他さまざまなオプションがあります。12 ページの図 1-7 に、インターフェースの例を示します。左側のメニューは、実行できる主なタスクを示しています。

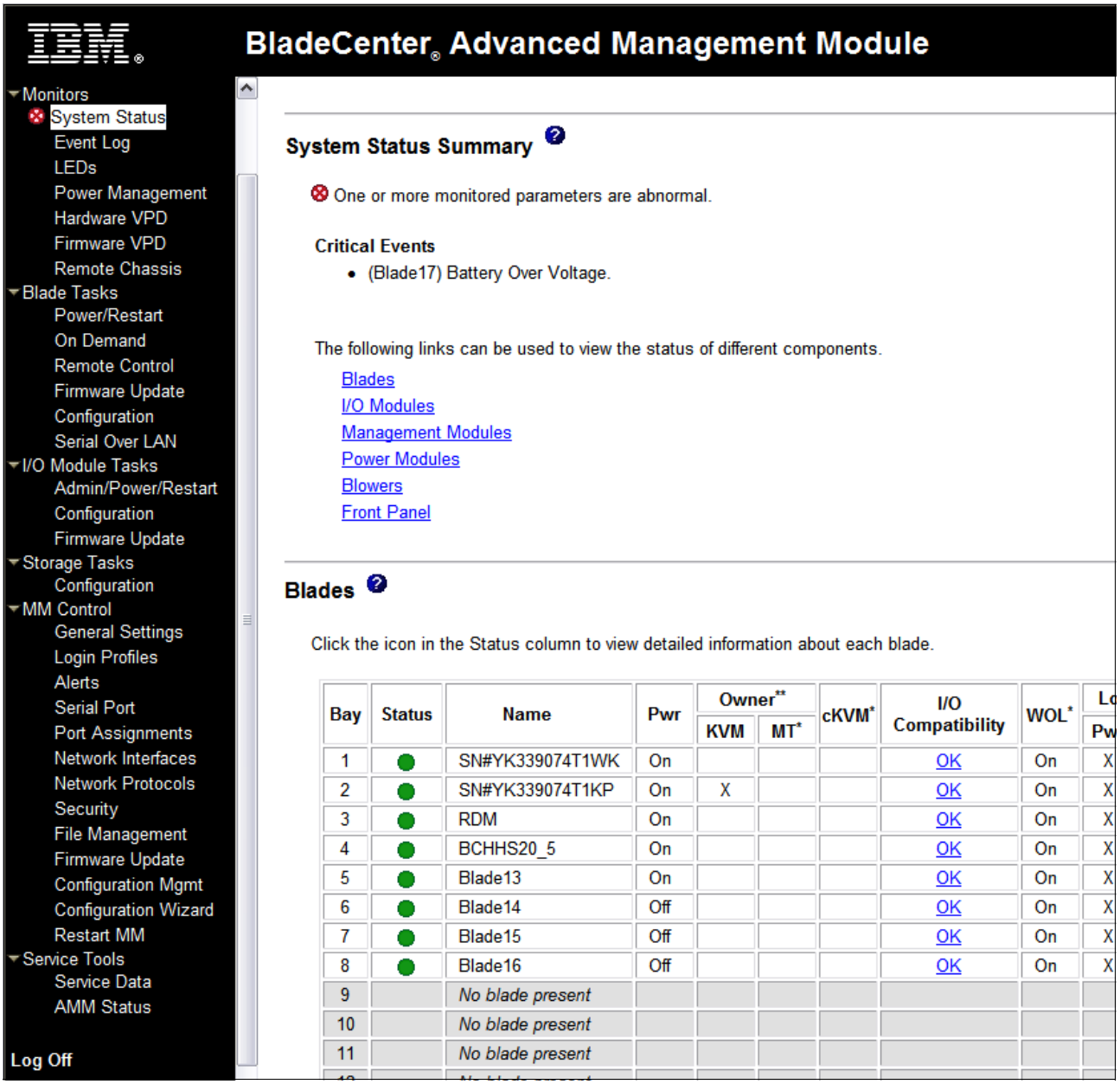


図 1-7　アドバンスト・マネージメント・モジュールの Web インターフェース

1.2.3 Remote Deployment Manager

Remote Deployment Manager (RDM) は、システム・イメージをブレード・サーバーおよびワークステーションに配布するための強力なツールです。Remote Deployment Manager は IBM Director をベースにしたツールで、サーバーおよびワークステーションの配布、更新、および構成に使用します。RDM を使用すれば、複数のプラットフォームと複数のハードウェア・ベンダーにサーバーのデプロイメント時間と TCO が削減されます。このため、新しいシステムとハードウェアのデプロイ、およびオペレーティング・システムのマイグレーションにかかるコストが少なく、複雑さが緩和されます。

RDM V4.40 を使用すれば、次のタイプのデプロイメントが可能です。

- サーバーおよびクライアントのデプロイ
- Windows および Linux® のデプロイ

> **注 :** HC10 ワークステーション・ブレードは、現時点では Linux をサポートしていません。

- Windows および Linux 上で稼働
- IBM Director からのデプロイメント・タスクおよびイメージの構成

1.3 ブレード・サーバーおよびブレード・ワークステーションの概要

ブレード・サーバーおよびブレード・ワークステーションは外観上はよく似ていますが、まったく異なります。ここでは、ブレード・サーバーとブレード・ワークステーションの概要、および利点について説明します。

1.3.1 ブレード・サーバー

IBM BladeCenter サーバーは、幅広いプロセッサー・テクノロジーとオペレーティング・システムの選択をサポートするので、お客様は単一のアーキテクチャーの中で多種多様なワークロードをすべて実行できます。ブレード・サーバーは、本棚に収められた本のように単一のシャーシに収容される、薄型のホット・スワップ可能なサーバーです。それぞれのサーバーは独立しており、専用のプロセッサー、メモリー、ストレージ、ネットワーク・コントローラー、オペレーティング・システム、およびアプリケーションを備えます。ブレード・サーバーは、シャーシ内のベイにスライドさせて挿入するだけで、ミッドプレーンまたはバックプレーンに接続し、電源、ファン、ディスケット・ドライブ、スイッチ、およびポートを他のブレード・サーバーと共用します。図 1-8 は、HS21 XM ブレード・サーバーを示しています。

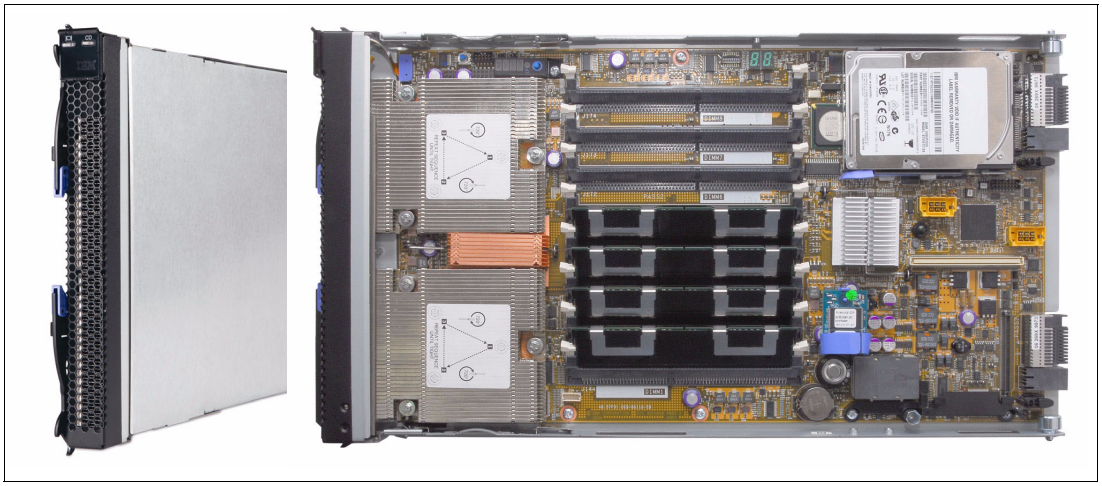


図 1-8 HS21 XM サーバー

サーバーを増設したり取り外したりするためだけに、ラックに張り巡らされた何百本ものケーブルをたぐる作業をしたことのある方なら、ブレード・アプローチの利点は明らかで

しょう。スイッチと電源装置が共用されているので、貴重なスペースが開放され、さらにブレード・サーバーによって密度の向上がきわめて容易に実現します。

1.3.2 ブレード・ワークステーション

ブレード・サーバーと同様に、IBM BladeCenter ワークステーションをベイにスライドさせて挿入し、ミッドプレーンまたはバックプレーンに接続すれば、単一のシャーシにワークステーションが収容されます。これらのワークステーションは、電源、ファン、ディスケット・ドライブ、光学式ドライブ、スイッチ、およびポートを共用します。それぞれのワークステーションは、専用のプロセッサー、メモリー、ストレージ、ネットワーク・コントローラー、オペレーティング・システム、およびアプリケーションを備えたシステムです。

ブレード・ワークステーションの概念は、デスクトップ・ワークステーションのコンピューティング・リソースと、サーバー・ベースのコンピューティング・ソリューションを組み合わせたものです。ブレードはデータ・センター内のシャーシに収容され、ユーザーのワークステーション・コネクション・デバイスと通信します。このデバイスは、通信モジュール、USB キーボード、モニター、マウス、その他の USB ユーザー・デバイス (プリンターなど) で構成されます。図 1-9 に、HC10 ブレード・ワークステーションを示します。

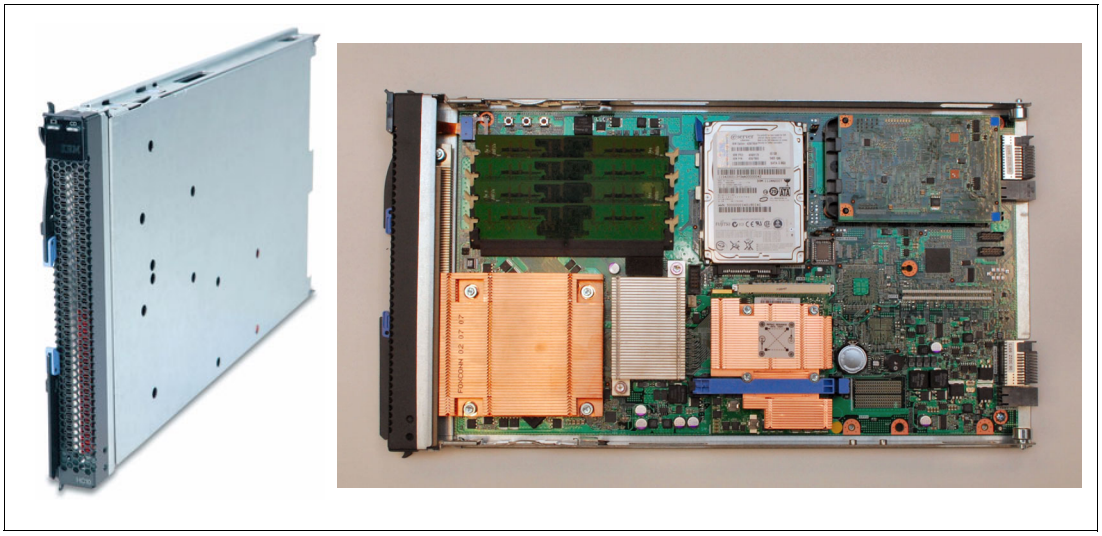


図 1-9 HC10 ブレード・ワークステーション

ブレード・ワークステーションを使用すれば、貴重な資産とデータが、ぜい弱なユーザーのワークステーションではなくデータ・センター内で保護され、管理されるので、セキュリティーとプライバシーが強化されます。PC とユーザー・データの統合、およびサポートと修理を集中管理する方式の提供によって、デスクトップの TCO は劇的に削減されます。ユーザーは、アプリケーションを閉じたり、作業環境を再設定したりせずに、さまざまな場所からブレード・ワークステーションにアクセスできます。また、ブレード・ワークステーションを使用すればオフィス内の乱雑な機器がすっきりし、オフィス内で発生する熱と騒音が低減されるので、より理想的なオフィス環境が実現します。

1.4 ネットワーク・オプション

ここでは、ネットワーク・オプションのいくつかについて説明します。互換性のあるイーサネット・スイッチ・モジュールについて概説し、IBM サーバー・コネクティビティ・モジュールについて具体的に説明します。

HC10 は、BladeCenter シャーシのベイ 1 とベイ 2 で次のタイプの I/O モジュールをサポートします (ベイ 2 は、BladeCenter S を除く、サポートされる BladeCenter シャーシすべてに装備)。

- イーサネット・スイッチ・モジュール (次に説明)
- カッパー・パススルー・モジュール (『1.4.3, IBM BladeCenter カッパー・パススルー・モジュール』(ページ 17) で説明)
- オプティカル・パススルー・モジュール (『1.4.4, IBM BladeCenter オプティカル・パススルー・モジュール』(ページ 18) で説明)

1.4.1 イーサネット・スイッチ・モジュール

さまざまなネットワーク層およびサービスをサポートする BladeCenter に対して、さまざまなタイプのイーサネット・スイッチ・モジュールが使用できます。イーサネット・スイッチ・モジュール (16 ページの図 1-10 に示す) には、いくつかの用途があります。BladeCenter 格納装置とブレードにネットワーク接続を提供し、さらにブレードと管理モジュール間の相互接続も提供します。イーサネット・スイッチ・モジュールは BladeCenter シャーシに標準装備されていませんが、HC10 のインプリメンテーションには 2 台が必要です。（BladeCenter S を除く）

注 : 他のスイッチ・モジュールには、InfiniBand スイッチ・モジュールや、ファイバー・チャネル・スイッチ・モジュールなどがあります。これらのモジュールは HC10 では使用できないので、本書ではこれらのモジュールについて特に説明しません。これらのモジュールについて詳しくは、IBM Redbooks 資料「*IBM BladeCenter Products and Technology*」(SG24-7523) を参照してください。

表 1-3 に示すように､さまざまなネットワーク層およびサービスをサポートする BladeCenter に対して、さまざまなタイプのイーサネット・スイッチ・モジュールが使用できます。

表 1-3 イーサネット・スイッチ・モジュール

部品番号	名前	外部ポート	ネットワーク層
39Y9324	IBM サーバー・コネクティビティ・モジュール	6	レイヤー 2
32R1888	Cisco Systems Fiber Intelligent Gigabit ESM	4	レイヤー 2 レイヤー 3 QoS[a]
32R1892	Cisco Systems Intelligent Gigabit ESM	4	レイヤー 2 レイヤー 3 QoS[a]
32R1860	Nortel Networks L2/3 カッパー Gigabit ESM	6	レイヤー 2 レイヤー 3
32R1861	Nortel Networks L2/3 ファイバー Gigabit ESM	6	レイヤー 2 レイヤー 3
32R1859	Nortel Networks Layer 2-7 Gigabit ESM	4	レイヤー 2 から 7

部品番号	名前	外部ポート	ネットワーク層
32R1783	Nortel 10 Gb Uplink イーサネット・スイッチ・モジュール	4[b]	レイヤー 2 レイヤー 3
39Y9267	Nortel 10 Gb イーサネット・スイッチ・モジュール	6	レイヤー 2 レイヤー 3

a. レイヤー 3 の場合、このスイッチは QoS (Quality of Service) のみをサポートします。
b. このスイッチには、10 Gb ポート 3 つと 1 Gb ポート 1 つが備わっています。

レイヤー 2 のサポートにより、イーサネット・スイッチは、MAC アドレスなどの物理アドレスを含むフレーム・ヘッダーを処理できます。レイヤー 3 の処理が可能ならば、スイッチは IP アドレスなどの論理アドレスを含むパケット・ヘッダーを検査できます。

スイッチがレイヤー 3 より上をサポートしていれば、ヘッダーのみでなくパケットの内容 (TCP ポートや、FTP、HTTP などのアプリケーション・プロトコルも) を検査できます。

1.4.2 IBM サーバー・コネクティビティ・モジュール

IBM サーバー・コネクティビティ・モジュールは、HC10 で使用できるイーサネット・スイッチ・モジュールの一例です。サーバー・コネクティビティ・モジュール (部品番号 39T9324) は、基本的なレイヤー 2 機能を備えたスイッチです。このデバイスは、ユーザーがネットワーキング・システム管理者でなくても、グラフィカル・ユーザー・インターフェース (GUI) またはコマンド・ライン・インターフェース (CLI) を使用して構成できます。図 1-10 に、IBM サーバー・コネクティビティ・モジュールを示します。

図 1-10 IBM サーバー・コネクティビティ・モジュール

IBM サーバー・コネクティビティ・モジュールは 14 個の内部全二重ギガビット・ポートを搭載しており、BladeCenter シャーシ内のブレードにそれぞれ接続します。さらに 2 つの内部全二重 100 Mbps ポートがあり、スロット 1 と 2 のマネジメント・モジュールに接続されます。標準のカテゴリー 5 拡張 (5e) 銅線ケーブル・コネクターを使用する、6 つの外部ポートが提供されています。外部ポートは、10 Mbps 全二重、100 Mbps 全二重、または 1 Gbps 全二重で接続します。銅線接続は、バックボーン、エンド・ステーション、およびサーバーへの接続手段になります。

1.4.3 IBM BladeCenter カッパー・パススルー・モジュール

IBM BladeCenter カッパー・パススルー・モジュール (CPM)、部品番号 39Y9320 は、構成の不要なネットワーク接続を提供し、BladeCenter シャーシ内のブレードがこの接続を使用して既存のネットワーク・インフラストラクチャーに接続できます。カッパー・パススルー・モジュールの構成を行う必要はありません。

CPM は、それぞれのブレードからの接続を 1 つずつ提供します。シャーシ内にある 14 台のブレードそれぞれから直接 1 つずつの RJ-45 コネクターが出て、外部スイッチ・パネルまたはパッチ・パネルに RJ-45 プラグを接続できます。CPM にはケーブルが 1 本付属しており、これはシャーシ内のブレード・サーバー 5 台分のみです。シャーシに 14 台のブレードがある場合は、追加のケーブルが 2 本必要です。これらのケーブルによって、15 個の RJ-45 コネクター (1 個は未使用のまま) が使用できます。図 1-11 に、IBM BladeCenter カッパー・パススルー・モジュールとケーブルを示します。

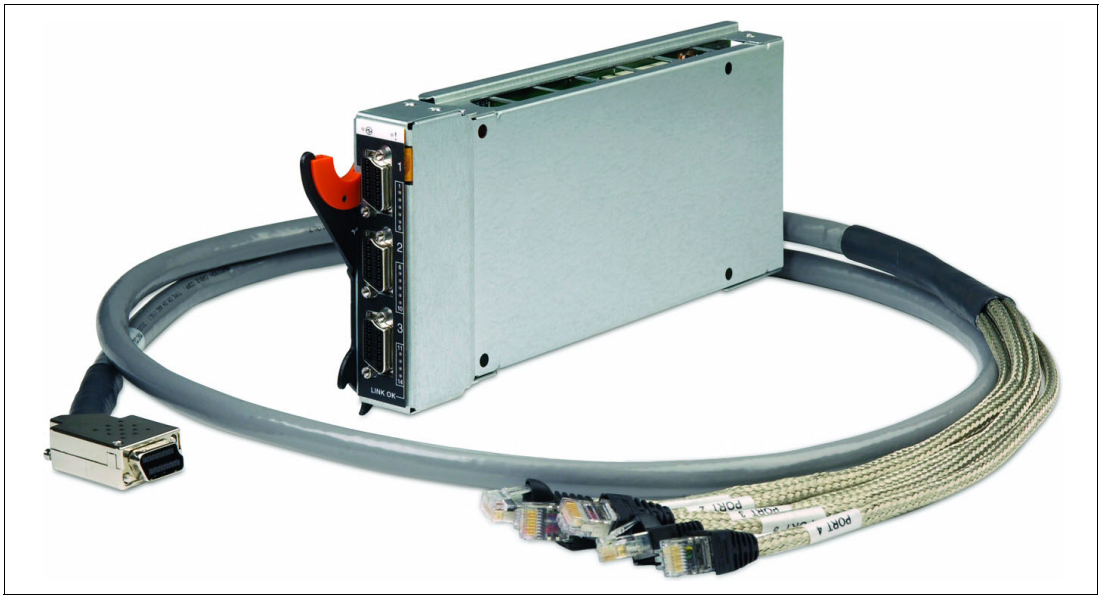


図 1-11 IBM BladeCenter カッパー・パススルー・モジュールとケーブル

3 本までのカッパー・パススルー・モジュール・ケーブルを、カッパー・パススルー・モジュールに接続できます (1 本のカッパー・パススルー・モジュール・ケーブルが付属)。カッパー・パススルー・モジュール・ケーブルは、業界標準の両方向コネクターによって終端します。

表 1-4 に、カッパー・パススルー・モジュールのオプションを示します。

表 1-4 カッパー・パススルー・モジュールのオプション

部品番号	説明
39Y9320	IBM BladeCenter カッパー・パススルー・モジュール (ケーブル 1 本付属)
39Y9170	IBM BladeCenter カッパー・パススルー・モジュール・ケーブル

カッパー・パススルー・モジュール用のケーブルは、一端にマルチポート銅線コネクター、他端に 5 つの RJ45 イーサネット・コネクターへのファンアウトを備えています。1 本の銅線パススルー・ケーブルがカッパー・パススルー・モジュールに付属し、必要な場合は 2 本の追加ケーブルを別途購入できます。

注 : カッパー・パススルー・モジュールは、1000 Mbps 接続のみをサポートする Gb イーサネットで、構成を必要としません。カッパー・パススルー・モジュールが接続する先の外部スイッチ・デバイスが、1000base-T ポートを装備していることを確認してください。

1.4.4 IBM BladeCenter オプティカル・パススルー・モジュール

IBM BladeCenter オプティカル・パススルー・モジュール (部品番号 39Y9316) は、構成の不要なネットワーク接続を提供し、BladeCenter 格納装置のブレード・サーバーがこの接続を使用して既存のネットワーク・インフラストラクチャーに接続できます。オプティカル・パススルー・モジュールの構成を行う必要はありません。図 1-12 は、IBM BladeCenter オプティカル・パススルー・モジュールと SC ケーブルを示しています。

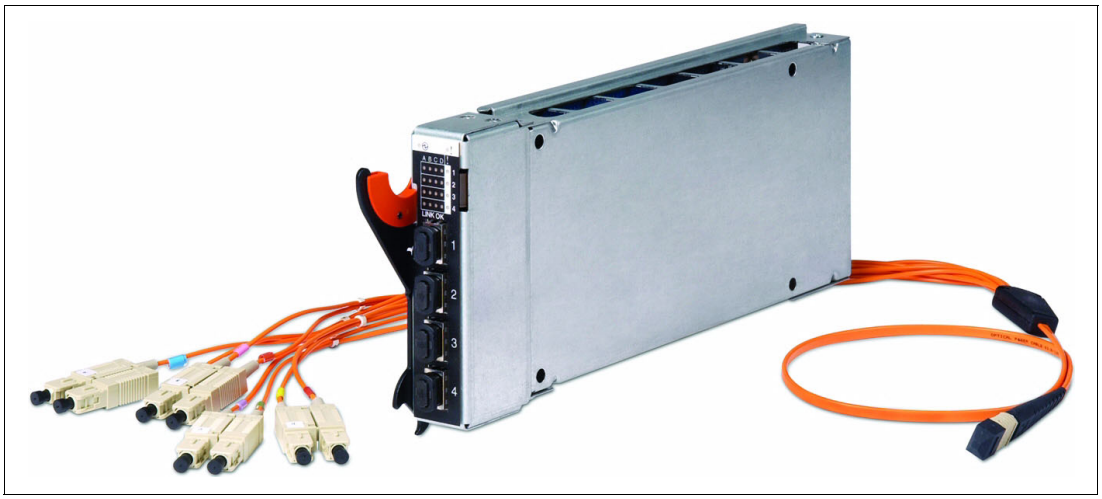


図 1-12 IBM BladeCenter オプティカル・パススルー・モジュールと SC ケーブル

4 本までのオプティカル・パススルー・モジュール・ケーブル (付属していません) を、オプティカル・パススルー・モジュールに接続できます。オプティカル・パススルー・モジュール・ケーブルは、業界標準の二重コネクターによって終端します。

表 1-5 に、オプティカル・パススルー・モジュールのオプションを示します。

表 1-5 オプティカル・パススルー・モジュールのオプション

オプション番号	説明
39Y9316	IBM BladeCenter オプティカル・パススルー・モジュール (ケーブルは付属しない)
39Y9171	IBM BladeCenter オプティカル・パススルー・モジュール SC ケーブル
39Y9172	IBM BladeCenter オプティカル・パススルー・モジュール LC ケーブル

オプティカル・パススルー・モジュール・ケーブルはオプティカル・パススルー・モジュールに付属しておらず、別途購入する必要があります。このケーブルによって、オプティカル・パススルー・モジュールと、外部のイーサネットまたはファイバー環境との間で 4 つの接続が可能です。オプティカル・パススルー・モジュール・ケーブルの長さは 1.5 メートルで、ケーブルに付属の光カプラーを使用すれば、長さを 150 メートルまで延長できます。

オプティカル・パススルー・モジュールのマルチポート光コネクターは、オプティカル・パススルー・モジュールの光ファイバー・ポートに接続され、ケーブルの他端には 4 つの SC

または LC 二重光コネクターが備わっています。これらのコネクターは、オプティカル・パススルー・モジュールの接続先のネットワーキング・デバイスに接続されます。

注 : オプティカル・パススルー・モジュールは、最高 2 Gb のファイバー・チャネル速度をサポートします。外部 4 Gb FC スイッチと内部 4 Gb FC 拡張カードをオプティカル・パススルー・モジュールで同時に使用した場合、FC ファブリックは 2 Gb で動作します。

2

ワークステーション・ブレードの概念

この章では、*ワークステーション・ブレード*の概念を紹介し、IBM IntelliStation® ワークステーションなどの従来型ワークステーション、および現在利用可能なその他のサーバー・ベースのコンピューティング・オプションと比較した、このソリューションの利点を示します。また、このソリューションの利点を生かすことができるお客様のタイプ、および IBM BladeCenter HC10 ワークステーション・ブレードの一般的な利点についても説明します。

この章で説明するトピックは、次のとおりです。

2.1 IBM IntelliStation ワークステーションの用途

IBM IntelliStation をはじめとするワークステーション PC は、大量のローカル計算能力、高度なグラフィックス処理、および一般に大規模なメモリー構成と I/O 能力を必要とするユーザーが使用するクライアント・システムです。例えば次のように、さまざまな業界で使用されます。

- 自動車、航空宇宙、防衛、エネルギー、および運輸の各業界のエンジニアと設計者
- 証券、債券、商品のトレーダー
- 地理情報システムの専門家
- ビジュアル・アーティスト
- 医用画像および科学計算の視覚化

それぞれの専門職のオフィスに置かれたワークステーションは、以前の *サーバー・スプロール* と同じような IT 問題を引き起こしています。

ワークステーション PC には主に次のような問題があります。

- セキュリティー

  ワークステーションで作成され、保管される知的財産の安全保護。特に、USB メモリー・キーなどの取り外し可能ストレージ・デバイスの使用に伴う問題。

- 環境および運用

  それぞれの専門職のデスク上、またはデスクの下に高出力ワークステーションが置かれているために生じる、電源、冷却、およびスペースの問題。狭いオフィスで仕事をしている設計者にとっては、電源と発熱は特に問題になります。

- サポート

  ユーザーのワークステーションが停止したときに、デスク・サイド・サポートに費用がかかり、生産性が失われます。

- 変更管理

  システムをユーザーのワークスペースに置くと、新規アプリケーションをロールアウトしたり、必要なときにワークステーションをオフィス間で移動したりすることが難しくなる可能性があります。お客様によっては、生産性向上のために頻繁なレイアウト変更が必要になることがあります。また、定期リースによってシステムの置き換えが頻繁に行われると、IT サポート技術員を必要とする機会が多くなります。

こうした問題に対処するために、HC10 のようなサーバー・ベースのワークステーション・ブレード・ソリューションは、次の機能を備えています。

- セキュリティー

  デスクトップ資産とデータはデータ・センターに置かれて、より安全に保護されます。USB デバイスのアクセスは制御され、許可されたデバイスのみが使用できます。(プリンター、マウス、キーボードなど)

- 環境および運用

  BladeCenter に備わっている効率的なサーバー・テクノロジーにより、全体のコストが削減されます。高出力のワークステーション・ハードウェアはデータ・センターに移されるので、消費電力が少なくなるとともに、発熱とスペースの問題も解消され、それぞれの専門職のオフィスが改善されます。

- サポート

  デスク・サイドでのサポートやリモート制御ツールを必要とせずに、データ・センター内で IT スタッフによってサポートが実施されるようになります。

- 変更管理

  データ・センター内にワークステーションを配置できるようになります。ワークスペースを移動する際には、ユーザー・デバイスは移動しますが、大きなワークステーション自体は移動せずに済みます。*フリー・シーティング*と呼ばれる新機能により、ユーザーは任意のワークステーション・コネクション・デバイスから PC に接続できるので、柔軟性が高まります。

大企業がワークステーション・ブレードに移行するきっかけとなる状況の 1 つは、従業員がシフト制で勤務していて、同時にオンラインになる従業員が全体の一部のみである場合です。この場合は、個々のユーザーごとに固有のシステムを維持する代わりに、ピーク時間にオンラインになる同時ユーザーの最大数よりわずかに多いワークステーション・ブレードの共用プールを使用できます。この方式により、リソースの使用効率が高まり、企業で購入する必要があるワークステーション・ブレードの数は、例えば従業員 1000 人に対して 750 台で済みます。これは、ワークステーション・ブレードを配置することによって実現するコスト削減の一例です。

2.2 クライアントに対するサーバー・ベース・コンピューティングの利用

図 2-1 に示すように、サーバー・ベース・コンピューティングのインプリメントには 3 つの方法があります。

- ターミナル・サーバーと Citrix タイプのソリューションが、同じオペレーティング・システム・イメージ内でアプリケーションをホストする。アプリケーションのインターオペラビリティーと互換性は重要ですが、サーバー・リソースの使用効率を最大にするために、個々のクライアントのパフォーマンス特性を犠牲にしています。
- 仮想化された独立のオペレーティング・システム・イメージを使用すれば、アプリケーション互換性の問題が解消されると同時に、複数ユーザー間でサーバー・リソースを共用する制約の中でサーバー・リソースを最大限に活用できます。
- ワークステーション・ブレード・ソリューションの特徴は、ユーザーのデスクトップとブレードの両方で専用のハードウェアを使用することによって、ユーザー・デスクトップへのデータを圧縮し、セキュリティーを確保することにあります。専用サーバー・ハードウェア (BladeCenter シャーシに収容されたワークステーション・ブレード) により、最高のユーザー・パフォーマンスが保証されます。

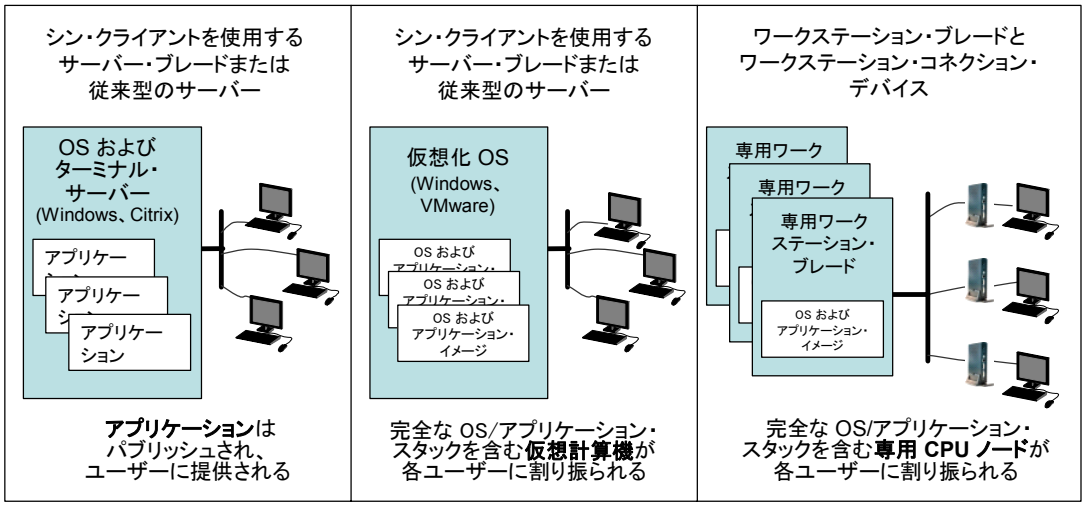


図 2-1　クライアントに対するサーバー・ベース・コンピューティングの利用を実現する 3 つの方法

ワークステーション・ブレード・ソリューションを他と区別する重要な点は、CPU、メモリー、およびグラフィックス能力の面でハイパフォーマンス特性を備えていることです。このハイパフォーマンスは、データをワークステーション・コネクション・デバイスに送信する前に圧縮する専用ハードウェアによって実現しています。

セキュリティーも主な特長です。ワークステーション・コネクション・デバイスはユーザー・データを保管せず、またワークステーション・ブレードとの接続を確立するためには、企業ネットワークへのアクセスと、有効なユーザー・ログイン資格情報が必要です。ユーザーのデータはデータ・センター内のワークステーション・ブレード上でセキュアに保持され、ユーザーが認証を受けずに機密データにアクセスする可能性はありません。

ワークステーション・コネクション・デバイスは、ローカル接続のさまざまな USB デバイスもサポートします。マウスおよびキーボードのほかに、コネクション・デバイスはプリンター、ストレージ・デバイス、および特殊なユーザー・インターフェース・デバイスをサポートします。データ・セキュリティーを確保するために、管理者は接続を特定のデバイスのみに制限できます (例えば、キーボード、マウス、およびプリンターのみ)。

仮想ソリューション (ターミナル・サービスや仮想化など) よりも強力なコンピューティング能力を必要とする専門職にとっては、ワークステーション・ブレードが最も有用です。例えば、非常に大きなグラフィカル・データとスプレッドシートを処理するために膨大な処理能力を必要とする金融トレーダーが、こうした専門職に含まれます。その他のユーザーとしては、工業分野でエントリーからミッドレンジの CAD/CAE アプリケーションを使用する場合が考えられます。

2.3 対象となるお客様

長年にわたって、サーバー・ベース・コンピューティングを支持する声は強く、今こそこのアーキテクチャーの時代が到来したと言われ続けてきました。もはや PC は最良のオプションではなく、コンピューティングを多数のエンドポイントで個々に管理するよりも、集中管理したほうが効率的だという提言がなされています。他には、セキュリティーの強化、可用性の向上 (ダウン時間の短縮) などの利点があります。

サーバー・ベース・コンピューティングには数々の利点がありますが、それでもまだ主流にはなっていません。ほとんどの組織では、まだサーバー・ベース・コンピューティングではなく PC を採用しています。何年も前から、サーバー・ベース・コンピューティングの売り上げ成長率は PC を上回っていますが、市場全体での規模にはいまだに 2 桁もの差があります。つまり、PC の全世界での出荷数は 2007 年には 2 億 5000 万台に達したとみられていますが、ワークステーション・コネクション・デバイスとシン・クライアントの出荷数見通しはわずかに 400 万ユニットでした。

以前は、リモート・コンピューティングはコール・センター、データ入力、生産性アプリケーションなどのオフィス・タスク用と見なされていました。ワークステーション・ブレードはほとんどのワークステーション・クラスのワークロードを処理できますが、デジタル・モックアップやビデオ・レンダリングなど、ハイエンドのワークステーション・タスクを実行するユーザーは、従来型のワークステーションを使用することを IBM はお勧めします。

一方、サーバー・ベース・コンピューティングではこれまで不可能だったさまざまなワークロード、例えばメインストリーム CAD、地理情報システム (GIS)、金融端末、遠距離コラボレーションなどに、BladeCenter HC10 の機能は十分に対応します。ワークステーション・ブレードは、ターゲット市場の典型的なワークロードに代表される、莫大な投資を保護するためのきわめて強固な信頼性を備えています。例えば、複雑な設計や金融モデルが消失すると、再作成に膨大なコストがかかります。

図 2-2 は、IBM ワークステーション・ブレード・ソリューションに最も適したお客様のタイプを示しています。

図 2-2　IBM BladeCenter HC10 のターゲット・ユーザー

2.4 ワークステーション・ブレードを使用する利点

図 2-3 に、IBM BladeCenter HC10 ソリューションを示します。

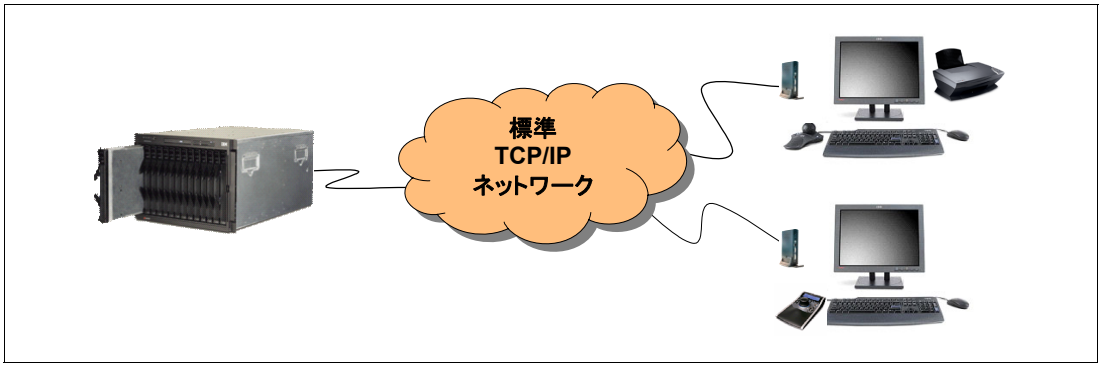


図 2-3　BladeCenter シャーシ内の HC10、および 2 台の CP20 ワークステーション・コネクション・デバイス

IBM BladeCenter HC10 には次のような利点があります。

- データ・セキュリティー

  HC10 では、データはデータ・センター内の HC10 ワークステーション・ブレードに物理的に保管され、無許可のユーザーからはアクセスできません。IBM CP20 ワークステーション・コネクション・デバイスにはストレージが存在せず、メモリー・キーなどのポータブル・ストレージ・メディアの使用を禁止するように USB 接続を構成できるので、ユーザーがアクセスするデータは画面に表示される内容のみに制限できます。さらに、HC10 と CP20 の間のデータ伝送を 128 ビット暗号によって暗号化して、データの機密性を保持できます。

- 柔軟なアクセス

  HC10 の構成方法に応じて、ネットワークに接続した CP20 が存在するどの場所からも、ユーザーはアプリケーションとデータにアクセスできます。ネットワークの帯域幅と遅延によっては、HC10 があるデータ・センターから遠く 4000 キロメートル (2500 マイル) も離れた場所に CP20 を置くこともできます。

  特定のユーザーが接続のたびに同じ HC10 に常に接続するようにソリューションを構成することもでき、また使用可能な任意の HC10 を選択し、Windows ローミング・プロファイルを利用してユーザーの Windows デスクトップをロードするように構成することもできます。CP20 と HC10 の接続を管理する適切なコネクション・ブローカー管理ソフトウェアがインストールされていれば、プーリングをインプリメントすることもできます。この場合は、ログオン資格情報に基づいて、使用可能な HC10 のサブセットから 1 つがユーザーに割り当てられます。

- 作業環境の改善

  CP20 ワークステーション・コネクション・デバイスの消費電力は 15 ワットと小さく、ディスク・ドライブ、ファンなどの可動部品は搭載していません。このため、通常のワークステーション PC と比べて CP20 の消費電力は小さく、さらにオフィス環境の冷却コストも削減されます。また、CP20 は小さなデバイスで、平均的なコンピューター関連の書籍と大きさにあまり差がないので、専門職のワークスペースが乱雑になりません。

- 容易な集中管理

  HC10 ソリューションは、プロビジョニング (リソースやサービスの提供)、保守、およびサポートの集中管理のために、資産をデータ・センターに配置します。さらに、HC10 の設計により、お客様は IBM Director や IBM Tivoli® Provisioning Manager などのミドルウェアを活用して、管理を効率化することができます。

- ワークステーション・クラスのパフォーマンス

  HC10 は、多くのプロフェッショナル・ワークステーションと同等のさまざまな機能を備えています。例えば、NVIDIA ハイパフォーマンス 2D/3D グラフィックス・コントローラー、Intel Core™ 2 Duo プロセッサー、データ・トランスポートのパフォーマンスを高める TCP/IP Offload Engine (TOE) をサポートする Gigabit Ethernet コントローラーなどを搭載しています。

- ローカル・デバイスのサポート

  HC10 および CP20 ワークステーション・コネクション・デバイスは、ローカルに接続された USB デバイスをサポートします。このサポート対象には、プリンター、ストレージ・ドライブ、Web カメラ、特殊なユーザー入力デバイスなど、ほとんどの USB デバイスが含まれます。サポートされるデバイスのタイプを管理者がカスタマイズして、例えばメモリー・ストレージ・ドライブの使用を禁止できます。

- アプリケーションの互換性

  HC10 は Microsoft Windows ロゴ・プログラムによって認定済みです。つまり、アプリケーションおよびデバイスに対してハイレベルの互換性を備えています。

3

HC10 のアーキテクチャーおよび設計

IBM BladeCenter HC10 は、BladeCenter ファミリーの新しいブレード・オファリングです。HC10 は、高いセキュリティーと管理の容易性を備えている上、グラフィックス性能に優れ、USB 機能を完備しており、ワークステーション・アプリケーション向けのサーバー・ベースのコンピューティング・テクノロジーを提供します。組み込まれた機能は、技術設計アプリケーション、取引所などで使用される金融アプリケーション、地理情報システム・アプリケーション、遠距離コラボレーションなどに最適です。HC10 のアーキテクチャーは、サーバー・チップ・セットではなく Intel Core 2 Duo デスクトップ・プラットフォームをベースにしています。

この章では、HC10 ワークステーション・ブレード・ソリューションの設計について説明し、主なコンポーネントについて技術的に詳しく解説します。また、HC10 ワークステーション・ブレードと IBM CP20 ワークステーション・コネクション・デバイスの間の通信に使用されるプロトコルについても説明します。

この章で説明するトピックは、次のとおりです。

3.1 HC10 のネットワーク

HC10 ソリューションには、図 3-1 に示すように 2 つの主なコンポーネントがあります。

- HC10 ワークステーション・ブレード。これは、データ・センター内の BladeCenter シャーシに収容されます。
- CP20 ワークステーション・コネクション・デバイス。これは、ユーザーのデスクに置かれます。

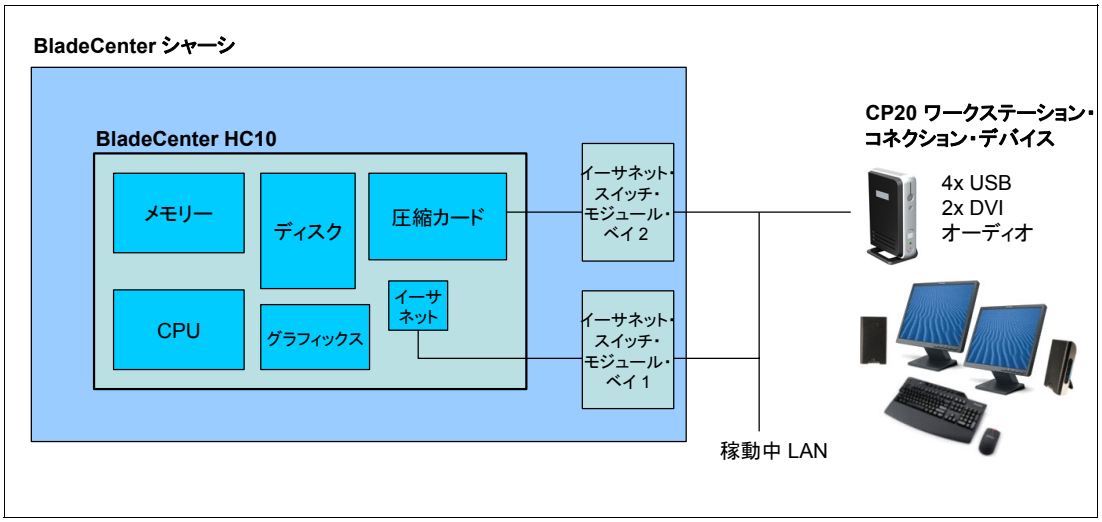


図 3-1 HC10 のレイアウトと接続 (HC10 BIOS のデフォルト設定)

HC10 は、Broadcom 5708S デュアル・ポート Gigabit Ethernet コントローラーを使用するイーサネット接続を 2 つ備えています。それぞれの接続は、BladeCenter シャーシ内のイーサネット・スイッチ・モジュールを経由して、次のように経路指定されます。

- HC10 上で稼働する Windows がデフォルトで使用するイーサネット接続は、BladeCenter シャーシのベイ 1 にあるイーサネット・スイッチ・モジュールによって提供される接続です。
- HC10 内の圧縮カード (*I/O グラフィックス伝送アダプター*とも呼ばれる) は、デフォルトで BladeCenter シャーシのベイ 2 にあるイーサネット・スイッチ・モジュールを経由して CP20 に接続されます。

  圧縮カードと CP20 の間のネットワークは、必要ならばプライベート・ネットワーク (または VLAN) にすることができ、また単にこれらの接続を稼動中 LAN に追加することもできます。どちらの場合にも、トラフィックが暗号化されるのでデータは安全です。

デフォルトのネットワーク設定は、図 3-1 に示したとおりです。使用されるイーサネット・スイッチ・モジュールは、HC10 BIOS の Advanced Settings によって変更できます。『6.2, イーサネット・スイッチ・モジュールの役割を指定』(ページ 106) を参照してください。

3.1.1 PC-over-IP プロトコル

HC10 と CP20 の間のリンクのパフォーマンスに重要な役割を果たすのが、PC-over-IP™ (*PCoIP*™ とも呼ばれる) プロトコルのインプリメンテーションです。PC-over-IP プロセッサーは、CP20 と HC10 内の圧縮カードの基礎になっています。

HC10 の PC-over-IP プロセッサーは、HC10 のユーザー・インターフェース全体 (ビデオ、USB シグナル、およびオーディオ) をリアルタイムにエンコードして暗号化し、標準 TCP/IP ネットワークを経由して、ペアを組む CP20 内の PC-over-IP プロセッサーにセキュア

なシグナルを送信します。シグナルは CP20 内でリアルタイムにデコードされ、ユーザーに提供されます。

図 3-2 に示すように、この処理によってグラフィックス・プロセッサーとユーザーのデスクトップにあるモニターの間で、遅延の短い接続が可能になります。

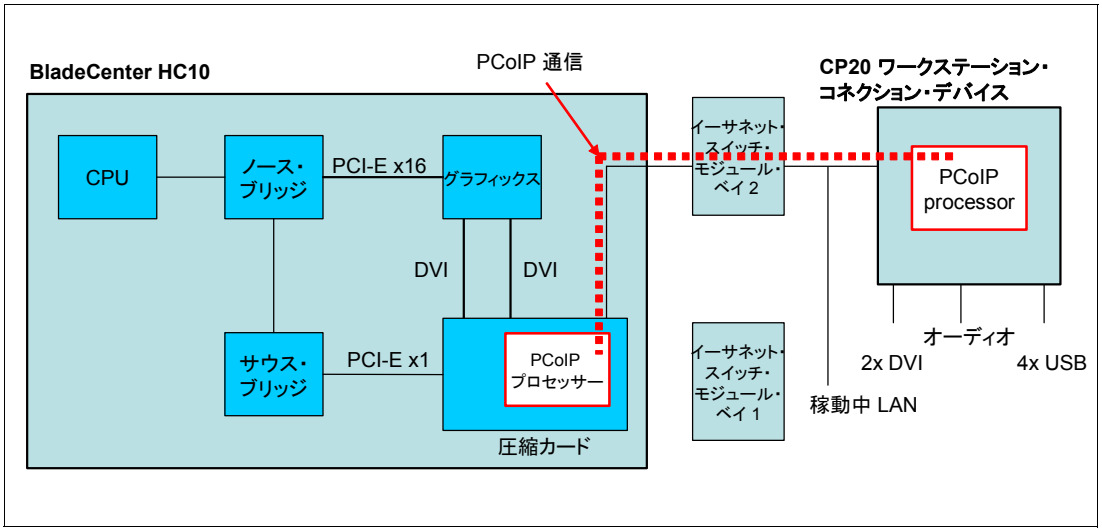


図 3-2　HC10 と CP20 間の PC-over-IP 通信

HC10 内の PC-over-IP プロセッサーは、グラフィックス・プロセッサーのデジタル・ビデオ・インターフェース、および PCI Express リンクに接続して、USB デバイスや HD オーディオ・デバイスなどの PC 周辺装置の透過ブリッジングを行います。

ネットワーク伝送の前に、HC10 内の PC-over-IP プロセッサーは、ビデオ・ストリームを圧縮し、サウス・ブリッジからの USB とオーディオのトラフィックを結合します。CP20 側では、PC-over-IP プロセッサーがデータ・ストリームの暗号化解除と圧縮解除を行い、ビデオ、オーディオ、および USB の各デバイスに配信します。

CP20 からは、マイクロホン、キーボード、マウスなどのオーディオや周辺装置の入力データがまとめられ、HC10 に送り返されます。このユーザー・デスクトップの圧縮、伝送、および再構築の処理はごく短時間に行われるので (通常は 10 ミリ秒未満)、遅延への影響はほとんどありません。

128 ビット SSL トンネルが、CP20 内の PC-over-IP プロセッサーとの非メディア通信に使用されます。SSL ハンドシェーク・プロトコルの一部として、証明書に基づいた相互デバイス認証が実行されます。メディア・トラフィックは、128 ビット IPsec ESP™ トンネルによって暗号化されます。IPsec トンネルのキーイング情報は、128 ビット SSL トンネル上でセキュアに設定されます。

また、HC10 内の PC-over-IP プロセッサーは、圧縮アルゴリズムと品質をリアルタイムに最適化し、使用可能なネットワーク帯域幅に応じて可能な限り最高のイメージ品質を実現します。この最適化によって、PC-over-IP デバイスはさまざまなタイプのネットワークとデータ転送速度で動作できます。使用可能なネットワーク帯域幅が拡大したとき、または表示イメージがあまり頻繁に変化しない場合には、圧縮イメージがオリジナル・イメージを損わない表示状態になるまで、イメージ・プロセッサーは圧縮イメージの品質を高めていきます。

イーサネット・ネットワークの特性によって、圧縮イメージ情報の一部が失われたり壊れたりする可能性がありますが、イメージ・プロセッサーはエラーを検出して回復するアルゴリズムをインプリメントしており、イメージの高品質が保証されます。

PC-over-IP テクノロジーの効果により、図 3-3 に示すように、CP20 に接続したユーザー・デバイスが実質的には HC10 にローカルに接続されます。

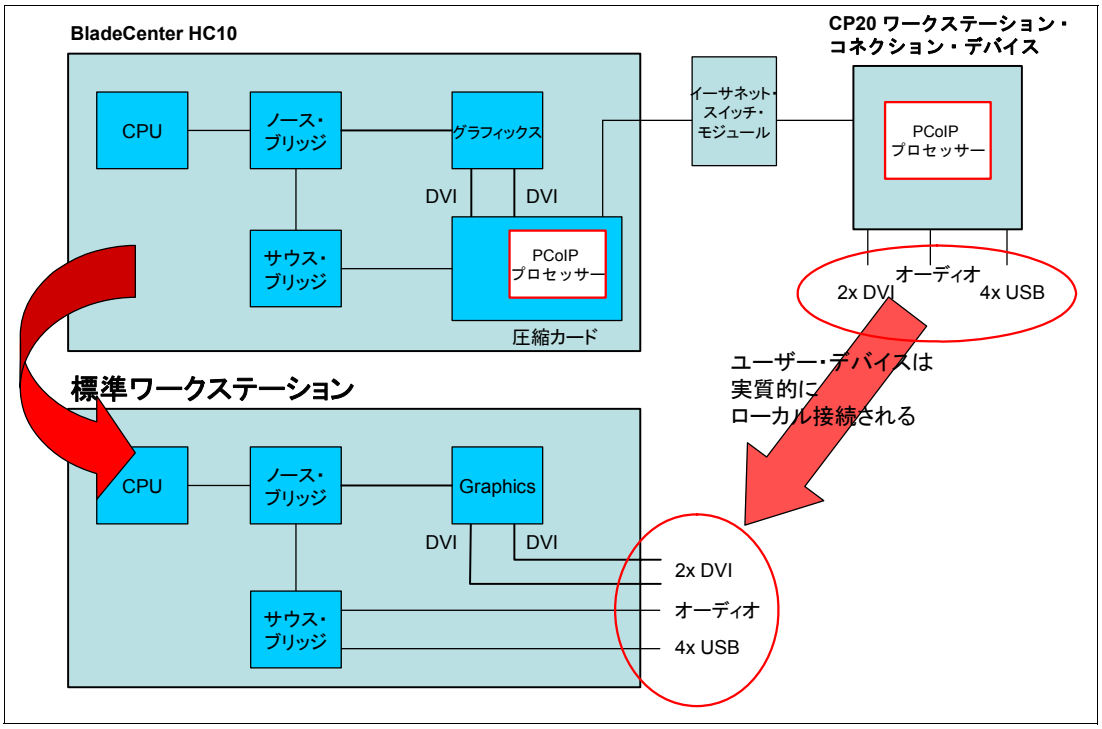


図 3-3　ユーザー・デバイスは実質的にローカルに接続される

3.1.2 USB

PC-over-IP プロセッサーがブリッジとなり、HC10 から CP20 に USB コントローラーを提供します。HC10 は、オペレーティング・システムに業界標準 USB インターフェースを提供します。つまり、特別なデバイス・ドライバーは必要ありません。バルク、割り込み、および等時性の USB 転送がサポートされるので、USB 1.1 全体との互換性があります。

注 : 現行インプリメンテーションでは、USB 2.0 デバイスは USB 1.1 の速度で動作します。

3.1.3 High Definition Audio のサポート

オーディオ・システムは、Intel High Definition Audio (HD オーディオ) 仕様をインプリメントしています。HD オーディオは、アドイン・オーディオ・カードの機能とハイエンド・パフォーマンスを提供できる、内蔵オーディオの新しい仕様です。この仕様の詳細と用途については、次の Web ページをご覧ください。

http://www.intel.com/design/chipsets/hdaudio.htm
http://www.intel.com/standards/hdaudio/

オーディオ・コントローラーは標準のデバイス・ドライバーと互換で、Microsoft の Universal Audio Architecture ドラフトに準拠しています。このドラフトは、次の Web ページに掲載されています。

http://www.microsoft.com/whdc/device/audio

オーディオ・コントローラーは、1 つのクライアント・コーデックに対して 4 つの出力オーディオ・ストリーム、および 3 つの入力オーディオ・ストリームをサポートしています。無

音抑止の実行時を除いては、PC-over-IP プロセッサーはそれぞれのオーディオ・ストリームの構成を認識しません。ストリームごとに 8 つのオーディオ・チャネルが完全にサポートされます。サポートされるサンプリング・レートは、48 k Hz および 44.1 k Hz の倍数 (最高 192 K サンプル / 秒) と約数です。

3.1.4 ネットワーク帯域幅に関する推奨事項

画面の変更や連続した画面の更新 (例えば、高解像度ビデオ) が生じているときはネットワーク帯域幅が消費されますが、ほとんどのオフィス・アプリケーションには画面が長時間変更されないという特徴があるので、ネットワーク・トラフィックはほとんど発生しません。このため、帯域幅の要件はアプリケーションと使用シナリオによって異なるので、単に画面解像度やリフレッシュ・レートのみでなく、画面内容の変更状況が要件を決める要素になります。

グラフィックスとビデオを表示するほかに、PC-over-IP プロセッサーは、ホストとユーザー・デスクトップの間で USB 周辺装置とオーディオを透過的に受け渡すブリッジにもなります。このようなタイプのメディアの帯域幅要件は、通常は厳しくありません。

ネットワーク帯域幅のプロビジョニングとは関係なく、何らかの理由でネットワークに十分なリソースがなくなった場合、HC10 と CP20 は使用可能なネットワーク帯域幅に収まるように表示圧縮を動的に調整することによって、動作を継続します。この調整は、ユーザー・エクスペリエンスの質が短期的に低下することのないように行われます。経験則として、最高負荷時のシナリオでユーザーが許容できるレベルのパフォーマンスを維持するための帯域幅は、1 ピクセル当たり 12.5 ビット / 秒にピクセルの総数を掛けることによって計算できます。

3D CAD レンダリング、ビデオ編集、アニメーションなど、ハイエンドのビジュアル・アプリケーションの場合は、ネットワーク帯域幅の計算に最低 25 ビット / ピクセル / 秒を使用してください。ユーザーごとの合計ネットワーク帯域幅要件を判別するには、USB とオーディオの帯域幅も考慮する必要があります。ほとんどのユーザーの場合は、2 から 3 Mbps の帯域幅を割り振れば、表示帯域幅リソースの使用時に瞬間的に起こる偶発性のピーク USB/ オーディオ負荷に十分対応できます。ただし、DVD の書き込みや DVD 再生など、需要の大きな USB アプリケーションをユーザーが使用する見込みがある場合は、追加の帯域幅を提供する必要があります。

表 3-1 は、アプリケーションの使用状況に応じたネットワーク帯域幅の割り振りを示しています。

表 3-1　アプリケーションの使用状況に応じたネットワーク帯域幅の割り振り

モニター解像度	1024x768	1280x1024	1680x1050	1600x1200	1920x1200
標準的な帯域幅の割り振り	10 Mbps	16 Mbps	22 Mbps	24 Mbps	29 Mbps
最大の帯域幅の割り振り	-	-	44 Mbps	48 Mbps	58 Mbps

3.2 HC10 の仕様

HC10 は、パフォーマンスとセキュリティーを高めるために、ハードウェアに基づいてグラフィックスの圧縮と暗号化を行うように設計されています。暗号化された USB シグナルは、TCP/IP ネットワーク上で透過的にワークステーション・デバイスに送信されます。グラ

フィックスや USB の情報をネットワーク上で暗号化し、送信するために、追加のソフトウェアやデバイス・ドライバーをお客様が用意する必要はありません。このワークステーション・ソリューションは、Microsoft Windows XP および Vista 用に設計されています。

このセクションで説明するトピックは、次のとおりです。

3.2.1 フィーチャー

HC10 のフィーチャーは、次のとおりです。

- デュアル・コア Intel Core 2 Duo 1 つ (最高 2.66 GHz)
- 1066 MHz フロント・サイド・バス
- 2 MB または 4 MB の L2 キャッシュ
- 最大 8 GB の DDR2 SDRAM (PC2-5300 667 MHz)
- SATA ディスク・ベイ 1 つ (80GB または 60GB ドライブが標準装備)
- 次のどちらかの NVIDIA グラフィックス・アダプター (標準)
  - Quadro NVS 120M Professional 2D グラフィックス・アダプター
  - Quadro FX 1600M Advanced 3D グラフィックス・アダプター
- 内蔵ベースボード管理コントローラー (BMC)
- Microsoft Windows Vista® Business Blade PC Edition (64 ビット) プリロード
- サポートされるオペレーティング・システム :
  - Microsoft Windows XP Professional (32 ビットおよび x64)
  - Microsoft Windows Vista Business (32 ビット /64 ビット)
  - Microsoft Windows Vista Enterprise (32 ビット /64 ビット)
  - Microsoft Windows Vista Ultimate (32 ビット /64 ビット)
- 3 年間の顧客取替可能ユニットおよびオンサイト限定保証

表 3-2 は、使用可能なモデルのリストです。モデル番号の中の文字 *x* は、国によって異なります。

表 3-2 BladeCenter HC10 モデル

モデル	Intel Core 2 Duo	速度	L2 キャッシュ	メモリー (標準 / 最大)	グラフィックス	ディスク
7996-21x	E6300	1.86 GHz	2 MB	1 GB / 8 GB	Quadro NVS 120M 2D	60 GB SATA
7996-51x	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro NVS 120M 2D	60 GB SATA
7996-5Ax	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro FX 1600M 3D	60 GB SATA
7996-5Bx	E6700	2.66 GHz	4 MB	4 GB / 8 GB	Quadro FX 1600M 3D	60 GB SATA
7996-PAQ	E6400	2.13 GHz	2 MB	1 GB / 8 GB	Quadro NVS 120M 2D	80 GB SATA
7996-PAR	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro NVS 120M 2D	80 GB SATA
7996-PAM	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro FX 1600M 3D	80 GB SATA
7996-PAL	E6700	2.66 GHz	4 MB	4 GB / 8 GB	Quadro FX 1600M 3D	80 GB SATA

モデル	Intel Core 2 Duo	速度	L2 キャッシュ	メモリー (標準 / 最大)	グラフィックス	ディスク
7996-PAT	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro FX 1600M 3D	160 GB SATA
7996-PAU	E6700	2.66 GHz	4 MB	4 GB / 8 GB	Quadro FX 1600M 3D	160 GB SATA

図 3-4 に、HC10 のレイアウトを示します。

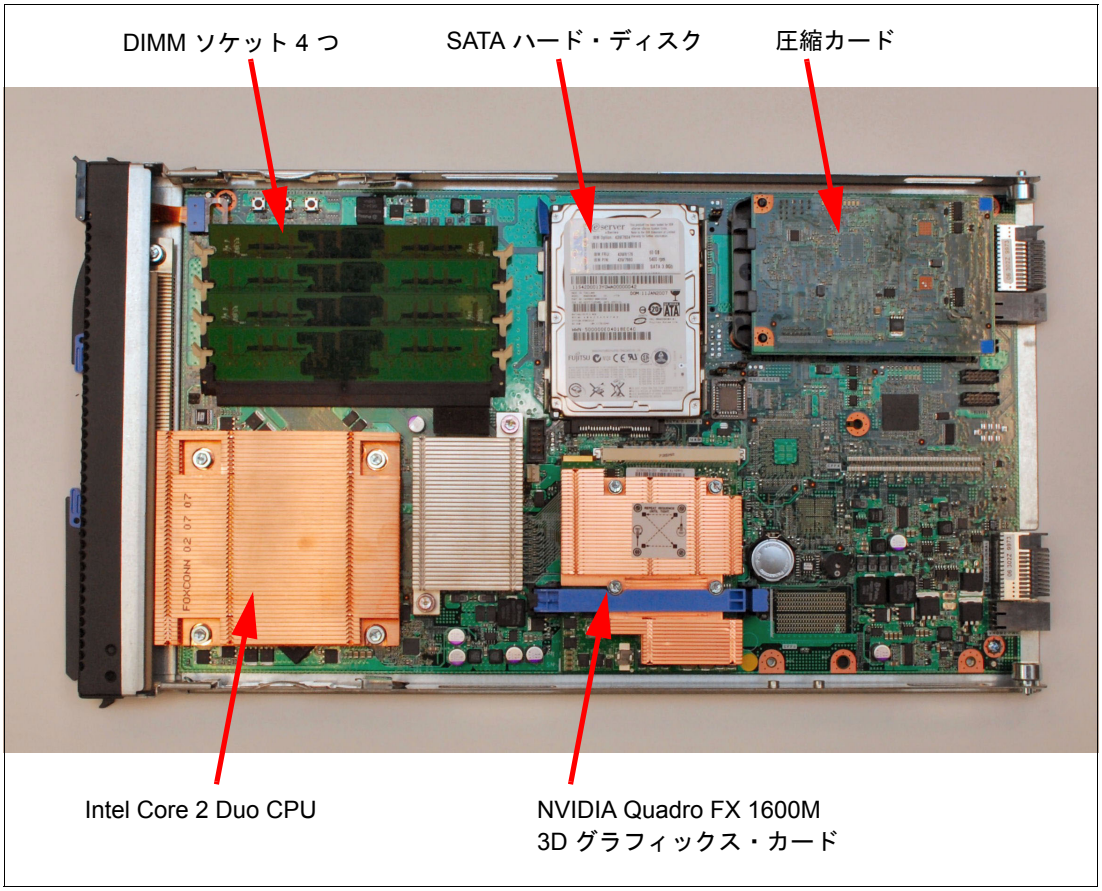


図 3-4 BladeCenter HC10

3.2.2 プロセッサー

HC10 のプロセッサーの標準および最大は 1 つです。アップグレードは利用できません。モデルによって、3 種類のプロセッサーがあります。両者の違いは、表 3-3 に示すように、内部クロック速度と L2 キャッシュのサイズのみです。

表 3-3 Intel Core 2 Duo プロセッサー間の違い

プロセッサー	クロック速度	フロント・サイド・バス	L2 キャッシュ・サイズ	CPU 電力消費量
Intel Core 2 Duo E6300	1.86 GHz	1066 MHz	2 MB	65 W
Intel Core 2 Duo E6400	2.13 GHz	1066 MHz	2 MB	65 W
Intel Core 2 Duo E6700	2.66 GHz	1066 MHz	4 MB	65 W

全プロセッサーのフィーチャーは、次のとおりです。

- 共用 L2 キャッシュを使用するデュアル・コア・アーキテクチャー
- Intel 64 アーキテクチャー (EM64T)
- 1066 MHz フロント・サイド・バス
- Intel Virtualization Technology のサポート
- 65 nm テクノロジー

3.2.3 メモリー

HC10 内で使用されているメモリーは、667 MHz で稼働するアンバッファード DDR2 SDRAM (PC2-5300) です。DIMM は non-ECC であり、対応するペアごとに取り付ける必要があります (ソケット 1 と 3、ソケット 2 と 4)。表 3-4 に、使用可能なメモリー DIMM オプションのリストを示します。

表 3-4 ブレード・サーバー HS20 タイプ 7981 のメモリー・オプション

部品番号	メモリーの説明
41Y2822	1 GB (2 x 512 MB キット) PC2-5300 CL5 DDR2 SDRAM RDIMM
41Y2825	2 GB (2 x 1 GB キット) PC2-5300 CL5 DDR2 SDRAM RDIMM
41Y2828	4 GB (2 x 2 GB キット) PC2-5300 CL5 DDR2 SDRAM RDIMM

3.2.4 ネットワーク・コントローラー

HC10 は、Broadcom 5708S デュアル・ポート Gigabit Ethernet コントローラーを使用します。このチップのフィーチャーは次のとおりです。

- PCI Express ベース
- TCP/IP Offload Engine (TOE) のサポート
- Wake on LAN®
- Serial over LAN (SOL)
- PXE 2.0 ブート・エージェント
- Alert Standard Format (ASF) 2.0

注 : Broadcom 5708S の iSCSI イニシエーターは使用できません。

2 つのイーサネット・ポートは、BIOS 内で次のように構成されています。（BladeCenter S を除く）

- シャーシのベイ 1 への接続は、HC10 のオペレーティング・システムが使用します。
- 圧縮カードおよび CP20 への接続は、シャーシのベイ 2 を経由します。

『6.2, イーサネット・スイッチ・モジュールの役割を指定』(ページ 106) で説明するように、これらは両方とも変更できます。

3.2.5 グラフィックス・アダプター

HC10 のモデルに応じて、2 種類のグラフィックス・アダプターのどちらかが標準として取り付け済みです (32 ページの表 3-2 を参照)。アダプターは、プレーナー上の MXM3 タイプのコネクターに取り付けられています。両方とも PCI Express x16 アダプターです。グラフィックス・アダプターには、次のものがあります。

- NVIDIA Quadro NVS 120M グラフィックス・ボードは、プロフェッショナル 2D ワークステーション・グラフィックス・ソリューション向けです。128 MB のオンボード・ビデオ・メモリー、および 64 ビット・インターフェースを備えています。

- NVIDIA Quadro FX 1600M グラフィックスは、3D グラフィックス機能を必要とするお客様向けです。256 MB のオンボード・ビデオ・メモリー、および 256 ビット・メモリー・インターフェースを備え、Shader Model 4.0 をサポートします。

どちらのグラフィックス・アダプターも、次のように 2 台までのモニターをサポートします。

- モニター 1 台を接続 : 最大解像度は 1920 x 1200 (75 Hz)
- モニター 2 台を接続 : 各モニターの最大解像度は 1600 x 1200 (60 Hz)

ワークステーション・コネクション・デバイスに 1 台または 2 台の CRT ディスプレイを接続した場合は、高解像度で問題が生じることがあります。詳しくは、次の RETAIN® ヒント H191783 を参照してください。

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597

3.2.6 圧縮カード

圧縮カード (*I/O グラフィックスおよび伝送アダプター*、または *IGTA* とも呼ばれる) は、PC-over-IP プロセッサー、および別個のイーサネット・コントローラーを内蔵しています。

圧縮カードは次の機能を備えています。

- アドバンスト・マネージメント・モジュールとの間で重要プロダクト・データ (VPD) 機能を提供する I^2C 回路。
- HC10 CPU とのデータ通信を提供する PCI Express インターフェース。
- CP20 ワークステーション・コネクション・デバイスへの USB コントローラー機能のルーティング。
- 業界標準のグラフィックス・カードからの DVI 入力 2 つ。
- デュアル・モニターのサポート。
- HC10 内での CP20 モニターのプラグ・アンド・プレイを実現する Microsoft WHQL のサポート。
- Lossless ビデオ圧縮。
- セキュア通信のための IPsec プロトコル。
- 表示更新時の往復回数を最小限にする機能。
- EDID 標準を使用して CP20 のモニター解像度を検出する機能。これは、圧縮チップからグラフィックス・カードへの DDC インターフェースを使用して実現できます。
- SSL、LDAP、Kerberos などの高度なセキュリティーおよび認証機能のサポート。

3.2.7 統合システム管理プロセッサー

HC10 には、次の機能を備えたベースボード管理コントローラー (BMC) が組み込まれています。

- IPMI 1.5 (Intelligent Platform Management Interface) への準拠
- Serial over LAN (SOL)
- Wake on LAN (WOL)
- 省電力機能
- KVM およびメディア・トレイの所有権
- Light path 診断のサポート
- 自動 BIOS リカバリー
- 自動サーバー再始動 (ASR)

- システム・コンポーネント (プロセッサー、メモリー、およびドライブ) 上の障害予知 (PFA)
- インベントリー
- エラー・ロギング
- 環境モニター (システム・ボード上の電圧および温度)

管理者が BMC に直接アクセスすることはできません。BMC は、BladeCenter シャーシ内のマネジメント・モジュールへのインターフェースとしてのみ使用されます。マネジメント・モジュールは、シャーシ内に含まれるサーバーおよびスイッチのコンポーネントすべてのハードウェア管理を行う、単一の制御ポイントです。

3.2.8 ローカル・ストレージ

HC10 は、次のフィーチャーを備えた 80 GB SATA または 60 GB SATA ドライブを標準として装備しています。

- 80 GB または 60 GB の容量
- 2.5 インチ SFF フォーム・ファクター
- SATA インターフェース、300 MBps
- 7200 RPM または 5400 RPM 回転速度
- 非ホット・スワップ

3.2.9 I/O 拡張オプション

BladeCenter HS21 などのブレード・サーバーとは異なり、HC10 には I/O 拡張カードをサポートする PCI-X コネクターや PCI Express コネクターはありません。

3.3 IBM CP20 ワークステーション・コネクション・デバイス

図 3-5 に示す IBM CP20 ワークステーション・コネクション・デバイス (3096-CDX) は、モニター、マウス、キーボード、スピーカー、その他の USB デバイスを接続するユーザー・デバイスです。可動部品はなく、外部電源アダプターを備えています。CP20 の寸法は、次のとおりです。

- 高さ :232 mm
- 幅 :94 mm
- 奥行き :174 mm
- 重量 1.1 Kg

図 3-5　CP20 の前面 (左側の写真) および背面 (右側の写真)

CP20 は、セキュリティーの強化と企業のサポート・コストの削減をどちらも実現するとともに、パーソナル・コンピューターまたはワークステーションのグラフィカル・ユーザー・インターフェースの完全なリモート表示、および I/O 機能を提供します。

CP20 の機能は、次のとおりです。

- HC10 から送信されたビデオ情報の表示。
- デュアル・モニターのサポート。両方の DVI コネクターをサポートし、またコンバーターの追加によって VGA アナログ・コネクターをサポートします。
- 2 つの DVI ビデオ・スプリッターの追加によるクワッド・モニターのサポート。
- USB デバイスのサポート (USB 1.1)。
- モニター解像度を検出して HC10 に送信する機能。
- 圧縮ビデオとオーディオを正しく分離するための IPsec パケットの解釈。
- ローカル構成用の EEPROM ベースのパネル。
- ブラウザー・ベース構成用の統合 Web サーバー。
- ピアツーピア接続、およびコネクション・ブローカー・ソフトウェアによる接続のサポート。

図 3-6 に、CP20 のブロック・ダイアグラムを示します。

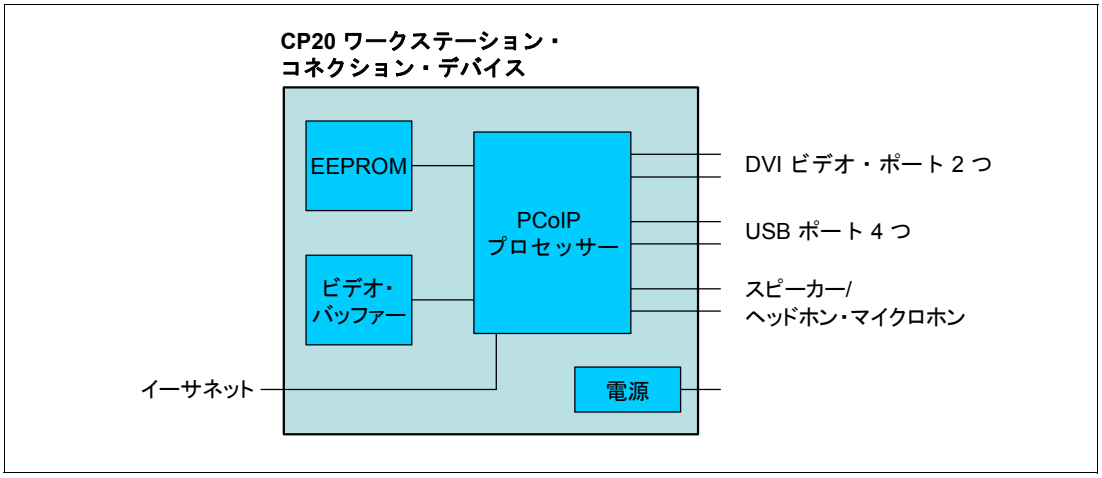


図 3-6 CP20 ブロック・ダイアグラム

3.3.1 コネクターおよびコントロール

図 3-7 は、CP20 の前面を示しています。ここには、2 つの USB コネクター、切断ボタン、リモート HC10 電源オン / オフ・ボタン、マイクロホン入力ジャック 1 つ、ヘッドホン・ジャック 1 つ、および接続状態、電源、および HC10 の電源状況を示す状況 LED があります。

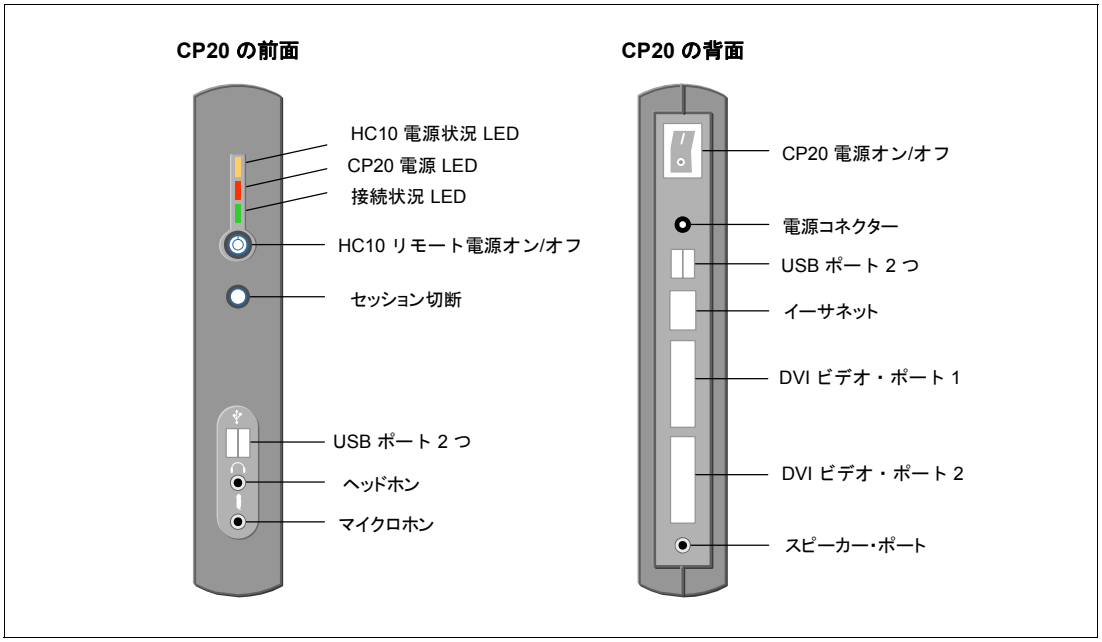


図 3-7 CP20 の前面および背面のコントロールとコネクター

HC10 の電源状況 LED の意味は、次のとおりです。

- *オン*: セッションは接続済みで、HC10 の電源がオンになっています。
- *オフ*: HC10 の電源がオフになっているか、セッションが存在しません (セッションの状態は、接続状況 LED を使用して判別します)。
- *点滅*: セッションは接続済みで、HC10 はスタンバイ / ハイバネート・モードになっています。

CP20 の背面には、RJ-45 10/100/1000 Mbps イーサネット・ポート 1 つ、デュアル DVI ビデオ・ポート、USB ポート 2 つ、スピーカー用のソケット (前面のヘッドホン・ソケットと同じ)、電源コネクター、および電源スイッチがあります。

4

HC10 の取り付けの計画

この章では、IBM BladeCenter HC10 ワークステーション・ブレード・ソリューションを計画し、インプリメントするために考慮する重要なことがらについて説明します。HC10 は、BladeCenter E シャーシの中に取り付けます。理解しておくべき重要な点として、BladeCenter 構成をインプリメントするには、ネットワーク、ストレージ、および電源の要件を考慮する必要があります。

またこの章では、ピアツーピア接続とコネクション・ブローカーを使用して、CP20 ワークステーション・コネクション・デバイスを HC10 ワークステーション・ブレードに接続する方法についても説明します。その後に続く 2 つの章では、これらの方法を実際にインプリメントする手順について説明します。

この章で説明するトピックは、次のとおりです。

4.1 IBM BladeCenter E シャーシ

1 ページの『第 1 章 BladeCenter の概要』で説明したとおり、BladeCenter E シャーシは BladeCenter HC10 を含む 14 台までのブレードをサポートします。サポートされる任意のブレード・サーバーを HC10 と組み合わせることができますが、ほとんどのお客様は多数の HC10 ワークステーション・ブレードをインプリメントし、シャーシ全体が HC10 ブレードで埋まるようになると考えられます。

図 4-1 に、IBM BladeCenter E の正面図を示します。

図 4-1 IBM BladeCenter E の正面図

BladeCenter E シャーシには、次の機構が標準装備されています。

- アドバンスト・マネージメント・モジュール 1 つ
- ホット・スワップ・パワー・サプライ・モジュール 2 つ
- ホット・スワップ・ブロワー・モジュール 2 つ
- USB v1.1 ポート 1 つ
- DVD-ROM ドライブ 1 つ
- 1.44 MB ディスケット・ドライブ 1 つ

ここでは、HC10 のロールアウトに必要なシャーシ構成のさまざまな面について説明します。

4.1.1 パワー・サプライ

BladeCenter E シャーシには次の電源入力が必要です。

- 正弦波入力 (50-60 Hz 単相)
- 入力電圧 :
  - 最小 : 200 V ac
  - 最大 : 240 V ac

IBM BladeCenter E 格納装置には、IEC 320-C19 から C20 の電源ケーブルが 2 本付属しています。それぞれのパワー・サプライに、専用の IEC 320-C20 電源コネクターが備わっています。

4 つの電源モジュールを取り付けた場合は (14 台のブレードをサポートするために必要)、4 つの電源コンセントが必要です。

4.1.2 電源モジュール

電源モジュール 2 台が IBM BladeCenter E に標準装備されており、最初の 6 台のブレード・ベイに電源を供給します。14 台のブレードをすべてサポートするには、2000 W パワー・サプライ・モジュール (部品番号 39M4675) のペアをもう 1 組取り付ける必要があります。

IBM BladeCenter E 格納装置には、IEC 320-C19 から C20 の電源ケーブルが 2 本付属しています。それぞれのパワー・サプライに、専用の IEC 320-C20 電源コネクターが備わっています。ベイ 1 および 2 のパワー・サプライは、I/O モジュールとマネジメント・モジュール、およびブレード・ベイ 1 から 6 のすべてに電源を供給します。

電源モジュールの各ペアには冗長性があります。どちらかの電源モジュールに障害が起こると、残りの電源モジュールが電源の供給を続けますが、冗長性は失われます。障害の起こった電源モジュールは、可能な限り早期に交換する必要があります。

真の冗長電源を提供するには、電源モジュール 2 および 4 とは異なる AC 給電部に電源モジュール 1 および 3 を接続する必要があります。電源モジュール 1 および 3 は、電源モジュール 2 および 4 とは異なる PDU に接続します。その後、別個の回路ブレーカーによって制御される AC 給電部 (建物の給電部、または引き込み口) に、それぞれの PDU を接続します。

注 : 以前に出荷された IBM BladeCenter E シャーシのパワー・サプライのサイズは異なる場合があります (1200 W、1400 W、1800 W、または 2000 W)。HC10 などのブレードは、2000 W パワー・サプライのみをサポートします。このため、既存の BladeCenter E シャーシに新しいブレードを取り付ける場合は、電源モジュールを 2000 W 電源モジュールに置き換える計画を立てる必要があります。

4.1.3 ブロワー・モジュール

IBM BladeCenter E シャーシには、1+1 冷却冗長性を備えた 2 つのホット・スワップ・ブロワーが付属しています (6 ページの図 1-4 を参照)。

次のように、BladeCenter E の前面周囲の温度によってブロワーの速度は異なります。

- 周囲の温度が 22 ℃ 以下の場合、BladeCenter E のブロワーは最高回転速度の 30% で稼働し、必要に応じて速度を上げて BladeCenter 内部の温度を制御します。
- 周囲の温度が 22 ℃ を超える場合、ブロワーは最高回転速度の 80% で稼働し、必要に応じて速度を上げて BladeCenter 内部の温度を制御します。

ブロワーに障害が起こると、残りのブロワーが BladeCenter E 格納装置とブレード・サーバーの冷却を続けます。冷却の冗長性を回復するために、障害の起こったブロワーは可能な限り早期に交換してください。

雑音を抑える必要がある環境では、騒音低減モジュールを使用できます (次の 4.1.4, “ 騒音低減モジュール ” を参照)。雑音レベルを低減するもう 1 つの方法は、アドバンスト・マネージメント・モジュールの *音響モード* 設定を使用することです。このモードでは、アドバンスト・マネージメント・モジュールはブレードのプロセッサー速度を抑えて、発熱を限度内に保ちます。

4.1.4 騒音低減モジュール

騒音低減モジュール (部品番号 39M4674) は、一般にマフラーとも呼ばれ、シャーシ背面のブロワー・モジュールを覆うように取り付けることによって、雑音を抑える必要がある環境でデシベル数を下げることができる BladeCenter E 用オプションです。BladeCenter E は、最高パフォーマンス・レベルで 74 デシベル (7.4 ベル) の騒音を発します。騒音低減モジュールは、T 形のバッフルを使用して、デシベル・レベルを 69 デシベルまで低減します（図 4-2 を参照）。

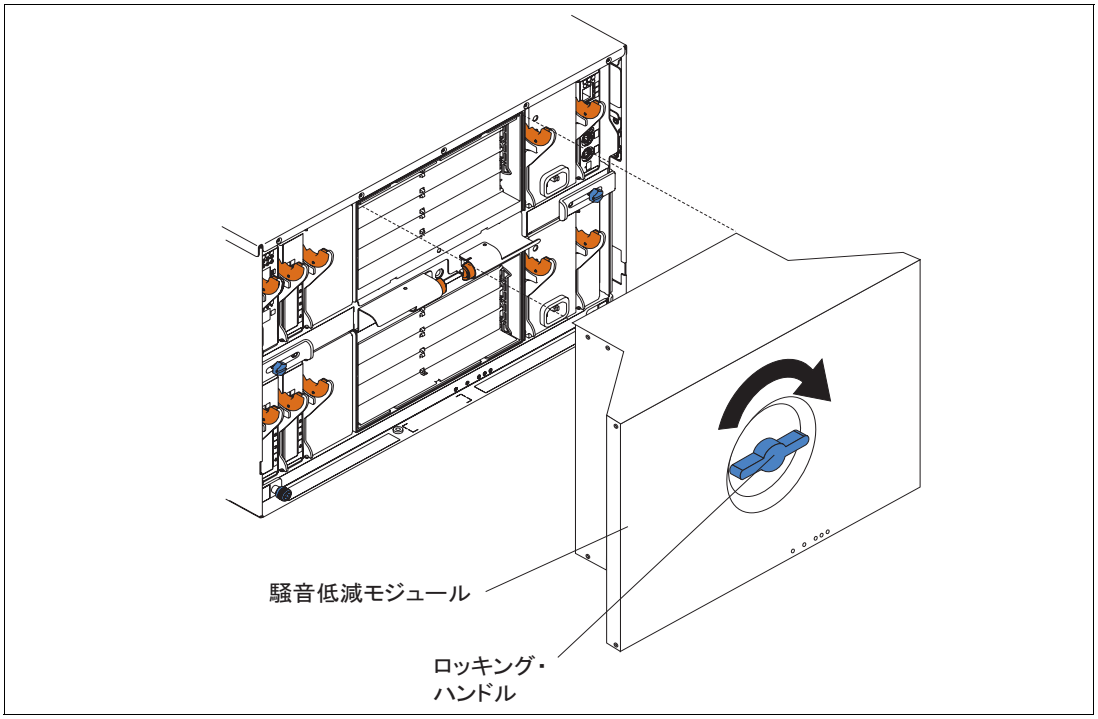


図 4-2 IBM BladeCenter E 騒音低減モジュール

4.1.5 冷却に関する考慮事項

データ・センターを計画する際には、冷却について次の点を考慮に入れてください。

- BladeCenter E の温度と湿度の許容限度は、次のとおりです。
  - 電源オン時 : 高度 0 から 914 m で 10.0 から 35.0 度 C
  - 電源オン時 : 高度 914 から 2,133 m で 10.0 から 32.0 度 C
  - 電源オフ時 : -40 から 60 度 C
  - 相対湿度 :
    - 電源オン時 : 8% から 80%
    - 電源オフ時 : 8% から 80%
  - 最大高度 : 2133 m
- 1 時間当たりの BTU 単位で表した BladeCenter E シャーシの発熱量は、最大構成で 8425 BTU/ 時 (5400 W) です。

4.1.6 アドバンスト・マネージメント・モジュール

マネジメント・モジュールは、取り付けられた BladeCenter コンポーネントすべての構成および管理に使用するホット・スワップ・デバイスです。BladeCenter 格納装置内のブレード

すべてに対して、システム管理機能とキーボード・ビデオ・マウス (KVM) 多重化を提供します。リモート管理アクセス用のイーサネット接続とシリアル・ポート接続を制御します。

BladeCenter E シャーシには、アドバンスト・マネージメント・モジュールが 1 つ標準装備されています。オプションの冗長アドバンスト・マネージメント・モジュール (部品番号 25R5778) を使用すれば、BladeCenter E の回復力が高まります。シャーシ内で、第 2 のモジュールはパッシブ・モードまたはスタンバイ・モードになります。アクティブ・モジュールまたは 1 次モジュールに障害が起こると、1 次モジュールの構成設定値をすべて使用して、第 2 のモジュールが自動的に使用可能になります。

注 : 以前の BladeCenter シャーシ (タイプ 8677) には、*アドバンスト・マネージメント・モジュール*ではなく旧型の*マネジメント・モジュール*が取り付けられていました。この旧型のデバイスは、シャーシに取り付けた HC10 ではサポートされません。

マネジメント・モジュール内のサービス・プロセッサーは、各ブレード内のサービス・プロセッサーと通信して、ブレードの電源オン要求、エラーおよびイベントの報告、KVM 要求、BladeCenter 共用メディア・トレイ (取り外し可能メディア・ドライブと USB コネクター) の使用要求などの機能をサポートします。

マネジメント・モジュールを使用して、IP アドレスなどの情報を設定することによって、BladeCenter コンポーネントを構成します。マネジメント・モジュールは、BladeCenter 格納装置内のすべてのコンポーネントと通信して、存在の有無を検出し、状況を報告し、必要ならばエラー条件に関するアラートを送信します。

アドバンスト・マネージメント・モジュールには、ローカルおよびリモート管理のためのさまざまなオプションがあります。

- 10/100 Mbps イーサネット・ポートは、Web ベース、CLI ベース、または IBM Director の管理インターフェースによるリモート管理に使用できます。
- アドバンスト・マネージメント・モジュールの前面にあるシリアル・ポートは、CLI ベースのローカル管理に使用できます。CLI ベースの管理は、無人リモート構成、およびバッチ処理に便利です。マネジメント・モジュールは、イーサネット・ポート経由のリモート管理のみをサポートします。
- アドバンスト・マネージメント・モジュールは、ローカル・キーボードおよびマウス用の USB ポート 2 つを備えています。マネジメント・モジュールは、同じ機能に PS/2 ポートを使用します。ブレードの適切なボタンを使用して、制御するブレードを選択します。
- アドバンスト・マネージメント・モジュールとマネジメント・モジュールの Web インターフェースは、どちらもマウスとキーボードのリモート制御 (リモート KVM) が可能です。

マネジメント・モジュールも電力消費モニターをサポートしていますが、アドバンスト・マネージメント・モジュールはそれに加えて、電力に上限を設ける機能などの PowerExecutive™ 拡張機能をサポートします。

アドバンスト・マネージメント・モジュールは、通信に使用する IP アドレスを 1 つ必要とします。マネジメント・モジュールと I/O モジュールの管理インターフェースには同じサブネットを使用するように計画を立ててください。アドバンスト・マネージメント・モジュールには、静的 IP アドレス (または、少なくとも DHCP の予約) を使用することをお勧めします。

4.1.7 イーサネット・スイッチ・モジュール

HC10 ワークステーション・ブレードを使用するには、シャーシのベイ 1 と 2 にイーサネット・スイッチ・モジュール 2 つを取り付ける必要があります（BladeCenter S を除く）。これらのイーサネット・スイッチ・モジュールは、14 台のブレードすべてからイーサネット・ネットワークへの接続を提供します。

- ベイ 1 のスイッチ・モジュールは、各 HC10 上のオペレーティング・システムへの接続を提供します。
- ベイ 2 のスイッチ・モジュールは、各 HC10 内の圧縮カードから、ネットワーク内の CP20 ワークステーション・コネクション・デバイスへの接続を提供します。

これらのイーサネット・スイッチ・モジュールは、冗長ではありません。

表 4-1 に、使用可能なイーサネット・スイッチ・モジュール、および適合するスイッチ・モジュールを選択する際に役に立つ一般的な選択上の考慮事項を示します。HC10 ソリューションに必要になる基本的な Gigabit Ethernet 接続の場合は、IBM サーバー・コネクティビティ・モジュールの使用をお勧めします。

注 : お使いのスイッチが、『4.3.3, TCP/IP ポート』(ページ 55) で説明する、必要なトラフィックを許容するように構成されていることを確認してください。

表 4-1 スイッチ・モジュールの選択基準

要件	適合するスイッチ・モジュール
基本的なレイヤー 2 Gigabit Ethernet スイッチング接続 (VLAN、ポート集約)	► IBM サーバー・コネクティビティ・モジュール
拡張レイヤー 2 Gigabit Ethernet スイッチング : 標準ベースの機能 (STP、QoS)	► Cisco System Intelligent Gigabit Ethernet Switch Module ► Nortel Networks L2/L3 カッパー Gb Ethernet スイッチ・モジュール
レイヤー 3 Gigabit Ethernet スイッチング (IP ルーティング、フィルタリング)	► Nortel Networks Layer 2-7 GbE スイッチ・モジュール (IBM BladeCenter 用)
レイヤー 4-7 Gigabit Ethernet スイッチング (コンテンツ・ベース・スイッチング、トラフィック検査、サーバー・ロード・バランシング)	► Nortel Networks Layer 2-7 GbE スイッチ・モジュール (IBM BladeCenter 用)

4.1.8 IBM サーバー・コネクティビティ・モジュール

IBM BladeCenter 用の IBM サーバー・コネクティビティ・モジュール (部品番号 39Y9324) は、基本的なレイヤー 2 機能を備えたスイッチです。このデバイスは、ユーザーがネットワーキング・システム管理者でなくても、グラフィカル・ユーザー・インターフェース (GUI) またはコマンド・ライン・インターフェース (CLI) を使用して構成できます。

スパンニング・ツリー冗長化、仮想ローカル・エリア・ネットワーク (VLAN)、ポート・フィルター、リンク集約、ポート・トランク、リモート・モニター (RMON) 統計などの標準的なネットワーキングの概念は、本製品の対象とするクラスの管理者は通常使用せず、習熟していないものです。

デフォルトの動作では、基礎となるネットワーキングの機能と構成はユーザーから隠されます。スパンニング・ツリー・プロトコルなど、一部の機能は必要ないので削除されています。サーバー・コネクティビティ・モジュールを構成し、制御するためにユーザーが使用できるネットワーキング・パラメーターは、少数の単純なもののみです。サーバー・コネクティビティ・モジュールの写真は、16 ページの図 1-10 を参照してください。

標準の機構および機能には、次のものがあります。

- 内部ポート
  - 内部全二重ギガビット・ポート 14 個 (BladeCenter 格納装置内の各ブレードに 1 つずつ接続される)
  - 内部全二重 100 Mbps ポート 2 つ（スロット 1 および 2 のマネジメント・モジュールに接続される）
- 外部銅線ポート
  - 6 つの外部ポートが、標準のカテゴリー 5 拡張 (5e) 銅線ケーブル・コネクターを使用して提供される
  - 10/100/1000 Mbps インターフェース : 外部ポートの接続速度は、10 Mbps 全二重、100 Mbps 全二重、または 1 Gbps 全二重
  - オートネゴシエーション機能
  - バックボーン、エンド・ステーション、およびサーバーに接続するための銅線接続
- 内部スイッチング
  - シャーシ内のブレードと管理モジュール間のパケット交換により、Serial over LAN (SOL) をサポート
- サーバー・コネクティビティ・モジュールの構成は、管理モジュール・ポートへの接続のみを経由して行い、外部スイッチ・ポートは経由しない
- タグ付き VLAN のサポート (管理者は、特定のサーバー・アプリケーション要件に一致する VLAN ID を定義できる)
- Cisco EtherChannel 互換の静的リンク集約
- 外部ポートを使用可能または使用不可に設定できる管理モジュール制御
- イーサネット・ジャンボ・フレーム・フォーマットのサポート (フレームごとに最大 9 K バイト)
- 独立した 2 つの内部 100 Mbps FDX リンクが、2 つの管理モジュールそれぞれに接続 (これらのリンクにジャンボ・フレームのサポートは不要)
- VPD およびレジスターへのアクセスを提供する管理モジュール I2C インターフェース
- 現行の業界標準と実務に適合するレベル 2 (L2) スイッチング
- 非ネットワーキング・デバイスとして認識されるので、ネットワーク管理者ではなくシステム管理者がこのデバイスを管理し、インストールすることが可能
- ポート集約 (外部ポートのみ)
- ポート・グループ・フェイルオーバー (外部ポートによって起動)
- IEEE 802.3x フロー制御
- インターネット・グループ・マルチキャスト・プロトコル (IGMP) スヌープ
- SOL、およびオプションで外部ポートのユーザー VLAN タグ付けに対応する IEEE 802.1Q のサポート
- RADIUS または TACACS+ ユーザー認証

4.2 IBM BladeCenter S シャーシ

1 ページの『第 1 章 BladeCenter の概要』で説明したとおり、BladeCenter S シャーシは BladeCenter HC10 を含む 6 台までのブレードをサポートします。サポートされる任意のブレード・サーバーを HC10 と組み合わせることができますが、ほとんどのお客様は多数の HC10 ワークステーション・ブレードをインプリメントし、シャーシ全体が HC10 ブレードで埋まるようになると考えられます。

ヒント : HC10 のお客様にとっての BladeCenter S の主な利点は、110V AC 電源で稼働できることです。

図 4-3 に、IBM BladeCenter S の正面図を示します。

図 4-3 IBM BladeCenter S の正面図

BladeCenter S シャーシには、次の機構が標準装備されています。

- 6 ベイ・ディスク・ストレージ・モジュール 1 つ
- アドバンスト・マネージメント・モジュール 1 つ
- ホット・スワップ・パワー・サプライ・モジュール 2 つ
- ホット・スワップ・ブロワー・モジュール 4 つ
- USB v2.0 ポート 2 つ
- CD-RW / DVD-ROM 1 つ

ここでは、HC10 のロールアウトに必要なシャーシ構成のさまざまな面について説明します。

4.2.1 消費電力

シャーシ・ファミリーの他のメンバーと異なる BladeCenter S シャーシ独自の機能の 1 つは、110V AC パワー・サプライからの電源で動作できることです。

BladeCenter S は、110V または 220V のどちらの AC 電源もサポートできる、最大 4 つの自動センス電源モジュールをサポートします。2 つの電源モジュールが標準で、最大 4 つがサポートされます。第 2 の電源モジュールのペアは、部品番号 43W3582 です。

第 2 の電源モジュールのペアは、次のいずれかの状態になった場合に必要です。

- 取り付けられたコンポーネント (サーバー、I/O モジュール、ディスクなど) の消費電力が、標準の電源モジュール 2 つの容量を超えた。
- 第 2 のストレージ・モジュールを取り付けた (電源モジュール 3 と 4 は、この第 2 のストレージ・モジュールを冷却するために必要なファンも備えているため)。

- 選択した電源プロファイルが、冗長性のために追加のパワー・サプライを必要としている。電源管理プロファイルの構成は、アドバンスト・マネージメント・モジュールのユーザー・インターフェース内で行い、AC 給電部の冗長性と電源モジュールの冗長性に関連したオプションを設定できます。

ご使用の構成に第 2 のパワー・サプライのペアが必要かどうか確認するには、BladeCenter Power Configurator を使用します。

http://www.ibm.com/systems/bladecenter/powerconfig

また、電力使用量と電源管理ポリシーについて詳しくは、「*BladeCenter S Planning Guide*」の第 2 章の電源に関するセクションを参照してください。

電源モジュールはホット・スワップ可能なコンポーネントで、BladeCenter の通常動作中に簡単に交換できます (アドバンスト・マネージメント・モジュールで冗長電源ポリシーが選択されていれば)。パワー・サプライに障害が起こっても、パワー・サプライ・ファンの電源はミッドプレーンから*共通の*電圧で供給されるので、パワー・サプライ内部の冷却ファンは通常の動作を継続します。パワー・サプライ・ファンは、ストレージ・モジュールに冷却用の空気の流れを供給することに注意してください。

電源モジュールは自動センスで、110V または 220V のどちらの AC 電源もサポートできます。ただし、異なる電圧の給電部を同じ BladeCenter S シャーシ内で混合してはなりません。

4.2.2 I/O モジュール・ベイ

図 4-4 に示すように、BladeCenter S には 4 つの I/O ベイがあります。

- ベイ 1 は、HC10 のイーサネット・コントローラーと、HC10 の圧縮カードをイーサネット・ネットワークに接続するために必要なイーサネット・スイッチ・モジュールを格納します。BladeCenter E とは異なり、BladeCenter S シャーシは両方のネットワークのルーティングに 1 つのベイのみを使用します。サポートされるスイッチ・モジュールのリストについては、50 ページの表 4-2 を参照してください。
- ベイ 2 は将来の使用のために予約されています。
- ベイ 3 と 4 は、SAS コネクティビティ・モジュールやその他のネットワーキング I/O モジュールなどの I/O 接続用です。これらのベイにある I/O モジュールは、ブレード・サーバーに取り付けられた拡張カードに接続します (CFFv、小型、または標準のフォーム・ファクター)。ただし、HC10 には拡張カードを取り付けるオプションがないので、シャーシに HC10 ブレードのみが取り付けられている場合、これらの I/O ベイは使用されません。

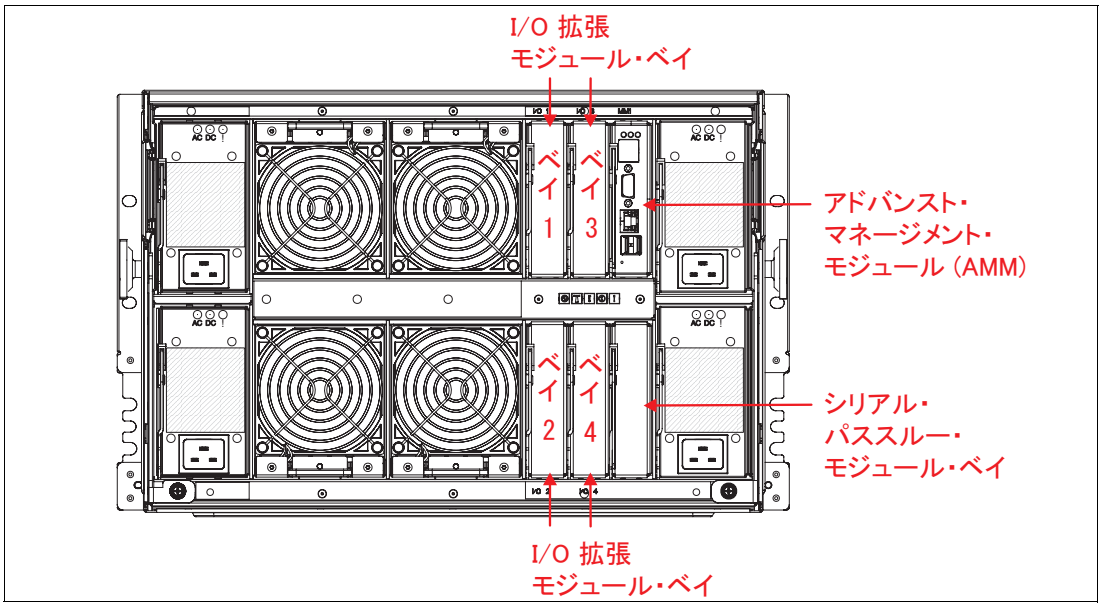


図 4-4　I/O モジュール・ベイの番号を示す BladeCenter S の背面

4.2.3 I/O 拡張モジュール・オプション

BladeCenter S に対しては、次の I/O 拡張モジュールを使用できます。

注 : HC10 は拡張カードをサポートしません。シャーシのオンボード・ストレージを使用するには、SAS 拡張カードを備えたブレード・サーバー 1 台 (例えば、HS21) をシャーシに取り付けて、ファイル・サーバーとして使用する必要があります。この場合、I/O ベイ 3 および 4 には、表 4-2 に示す SAS コネクティビティ・モジュールを取り付けてください。

表 4-2　BladeCenter S に対してサポートされる I/O 拡張モジュール

部品番号	説明	適合する I/O モジュール・ベイ
SAS I/O 拡張モジュール		
39Y9195	IBM BladeCenter SAS コネクティビティ・モジュール	3, 4
イーサネット I/O 拡張モジュール		
32R1860	Nortel Layer 2/3 カッパー Gb Ethernet スイッチ	1, 3, 4[a]
32R1861	Nortel Layer 2/3 ファイバー Gb Ethernet スイッチ	1, 3, 4[a]
39Y9324	サーバー・コネクティビティ・モジュール	1, 3, 4[a]
32R1783	Nortel 10G Uplink イーサネット・スイッチ	1, 3, 4[a]
ファイバー・チャネル I/O 拡張モジュール		
32R1813	Brocade 10 ポート - 4 Gb SAN スイッチ	3, 4[a]
43W6724	QLogic® 10 ポート - 4 Gb ファイバー・チャネル・スイッチ	3, 4[a]

部品番号	説明	適合する I/O モジュール・ベイ
43W6723	4 Gb インテリジェント・パススルー・モジュール	3, 4[a]
39Y9284	Cisco Systems 4 Gb 10 ポート・ファイバー・チャネル・スイッチ	3, 4[a]
その他の I/O 拡張モジュール		
39Y9316	オプティカル・パススルー・モジュール	1, 3, 4[a]
39Y9320	カッパー・パススルー・モジュール	1, 3, 4[a]

a. このスイッチ・モジュールをベイ 3 または 4 に取り付けるには、適合する拡張カードをブレード・サーバーに取り付ける必要があります。この場合、BladeCenter S 内部ストレージ・モジュールは使用できなくなります。

4.2.4 ストレージ・モジュール

ストレージ・モジュールは、基本的にはディスク・ドライブの集まりです。ブレード・サーバーは、ブレード内の SAS 拡張カード、およびシャーシのベイ 3 と 4 にある SAS コネクティビティ・モジュールを介して、これらのドライブにアクセスできます。

重要 : HC10 ワークステーション・ブレードは拡張カードをサポートしないので、BladeCenter S シャーシ内のストレージ・モジュールを使用できません。シャーシにサーバー・ブレードも取り付ける予定にしている場合は、これらのサーバーに SAS 拡張カードを取り付ければ、ストレージ・モジュール内のディスクにアクセスできます。

BladeCenter S シャーシには最大 2 つのストレージ・モジュールを取り付けることができ、それぞれのストレージ・モジュールには 6 つまでの 3.5 インチ・ホット・スワップ・ハード・ディスクを組み込むことができます。同じストレージ・モジュール内で SAS 方式と SATA 方式のハード・ディスクを混合して使用できます。

シャーシ内では、標準ストレージ・モジュールに 6 つまでの 3.5 インチ・ハード・ディスクを格納でき、追加のストレージ・モジュールを使用するとさらに 6 つ格納できます。組み込みの定義済み構成、またはユーザーが定義可能なカスタム構成を使用して、素早く簡単にディスクをブレードに直接割り当てることができます。

サポートされるディスク・ドライブは、次のとおりです。

- 73 GB 15 K RPM SAS ドライブ (部品番号 40K1043)
- 146 GB 15 K RPM SAS ドライブ (部品番号 40K1044)
- 300 GB 15 K RPM SAS ドライブ (部品番号 43X0802)
- 500 GB SATA ドライブ (部品番号 39M4530)
- 750 GB SATA ドライブ (部品番号 43W7576)

4.2.5 BladeCenter S Office Enablement Kit

BladeCenter S Office Enablement Kit (部品番号 2018-86X) は、雑音を抑えることが重要なオフィスで使用するために特に設計された、BladeCenter S シャーシ用の新しい格納装置です。図 4-5 に、この格納装置を示します。

図 4-5 BladeCenter S Office Enablement Kit

NetBAY11 をベースとした Office Enablement Kit は、オフィス環境に適したセキュリティー・ドアと特殊な防音機構、および空気ろ過装置を備えた 11U の格納装置です。BladeCenter S シャーシを取り付けた状態で、ほかのラック・デバイスを格納する 4U の追加スペースが残っています。

Office Enablement Kit には次のような利点があります。

- 音響モジュール

  Office Enablement Kit には、オフィス環境で BladeCenter S の騒音を抑制するとともに、BladeCenter S コンポーネントの容易な取り扱いを可能にする防音モジュールが付属しています。

- ロック式ドア

  オフィス環境ではセキュリティーが重要な考慮事項です。Office Enablement Kit には、どのような環境でもデータの安全とセキュリティーを維持するために役立つ、前面ロック式ドアが付属しています。

- 他のデバイスに使用できる 4U の追加スペース

  オフィス IT を実現するために、さまざまなビジネスでさまざまなツールが使用されています。Office Enablement Kit には、オフィスに必要な他のタイプの IT 機器に使用できる 4U の追加スペースが含まれています。このスペースに、4U 以下の標準ラック・スペースに収まる IT 機器を格納できます。

- 移動が容易

  Office Enablement Kit にはロック可能な車輪が付いており、BladeCenter S を簡単に移動できます。

- 防じんフィルター

  どのような環境にも BladeCenter S を配置できるように、Office Enablement Kit にはオプションの防じんフィルターを組み込むことができます。このフィルターは、BladeCenter S をちりやほこりから保護し、IT 機器の寿命を延ばすために役立ちます。追加のフィルターはオプションとして入手可能です。部品番号は 43X0430 で、またフィルター 4 個パックの部品番号は 43X0437 です。

格納装置の寸法は、およそ次のとおりです。

- 高さ : 611 mm (24.1 インチ)
- 幅 : 518 mm (20.4 インチ)
- 奥行き : 1156 mm (45.5 インチ)

4.2.6 BladeCenter S での HC10 ブレードの使用

HC10 ワークステーション・ブレードを取り付けたまま BladeCenter S の内部ストレージを利用するには、次のような構成をお勧めします。

- BladeCenter HS21 などのサーバー・ブレード 1 つを、シャーシ内のブレード・ベイ 6 つのいずれかに取り付けます。

  このサーバー・ブレードには、シャーシ内に取り付けられた SAS コネクティビティ・モジュールに接続する SAS 拡張カードを取り付けることができます。サーバー・ブレードはシャーシの内部 SAS ストレージすべてにアクセスできるようになり、HC10 ワークステーション・ブレードはネットワーク共有としてこのストレージにアクセスできます。

- 残り 5 つのブレード・ベイには、HC10 ワークステーション・ブレードを格納できます。

このソリューションを使用すれば、単一のポータブルなシャーシに 5 つのワークステーション・ブレードと大容量の準ローカル・ストレージが組み込まれます。

4.3 ネットワーク接続

標準的な HC10 ワークステーション・ブレード・ソリューションは、次の 3 つのコンポーネントをベースにしています。

- データ・センター内の BladeCenter シャーシに取り付けられた、いくつかの HC10 ワークステーション・ブレード。通常はユーザーごとに 1 つずつですが、従業員がシフト制で勤務している企業では、システムの共用も検討できます。
- 各ユーザーのワークスペースに配置された、いくつかの CP20 ワークステーション・コネクション・デバイス。
- CP20 から HC10 への初期接続を管理するデータ・センター内のサーバーにインストールされた、Devon IT または Leostream の接続管理ソフトウェア。このコンポーネントについては、『4.7, 接続方式』(ページ 62) で詳しく説明しています。

これらのワークステーション・ブレードは、図 4-6 に示すように、ほかのサーバーおよびストレージと一緒に稼動中のネットワークに接続できます。

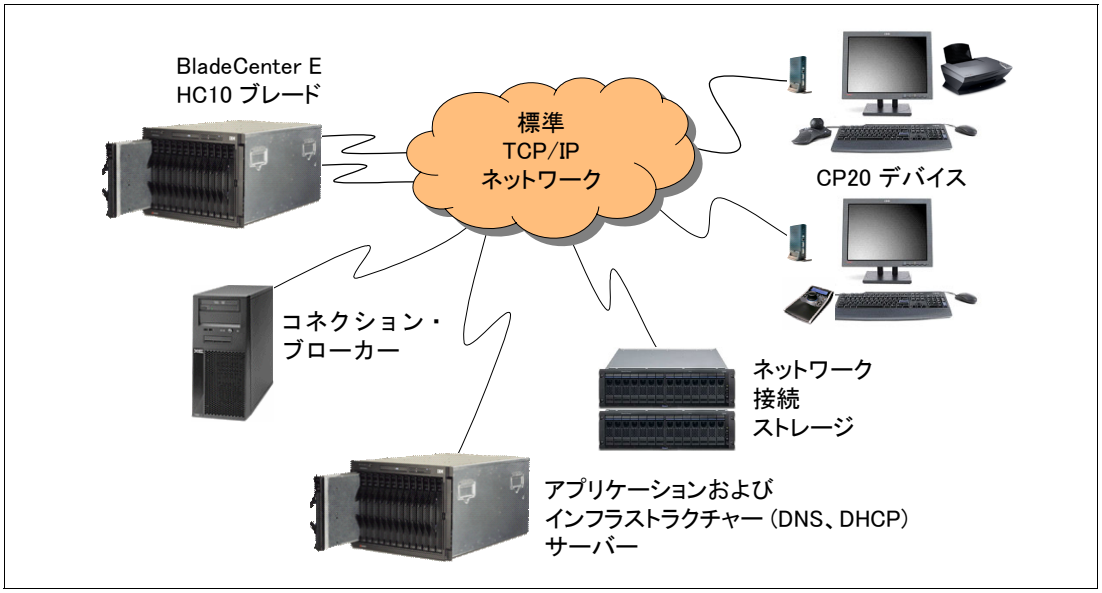


図 4-6　コネクション・ブローカーを使用する標準 HC10 構成

図 4-6 では、1 つのイーサネット・ネットワーク上で、ネットワーク内のすべてのシステムとデバイスが一緒に接続されています。このため、HC10 ブレードから CP20 ユーザー・デバイスへのデータ・トラフィックは、稼動中のシステムと同じイーサネット・ネットワークを共用しています。CP20 トラフィックは暗号化されているので、セキュリティー面でのリスクはありません。

ただし、イーサネット・ネットワークの稼動中のトラフィックの負荷に応じて、PC-over-IP プロトコルを使用して通信するデバイスを分離することも検討できます。図 4-7 に示すように、HC10 ブレードの圧縮カード、CP20 ワークステーション・コネクション・デバイス、およびコネクション・ブローカーがこれに該当します。これらのデバイスをこのように分離すれば、PC-over-IP の帯域幅要件をサポートするために十分な帯域幅が確保されます。

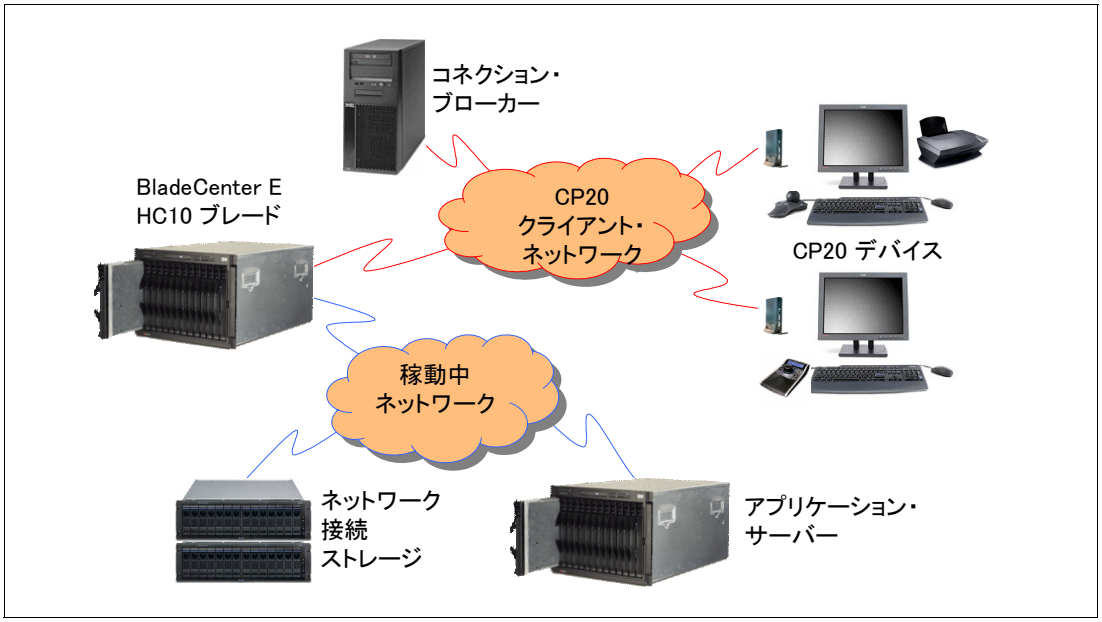


図 4-7 CP20 トラフィックとその他のネットワークの分離

CP20 と HC10 の圧縮カードのデフォルト構成では、DHCP を使用します。DHCP を使用する場合は (推奨)、DHCP サーバーに次のオプションが設定されていることを確認する必要があります。

- オプション 12
- オプション 15

これらのオプションを構成する方法、およびオプションに指定する値については、DHCP サーバーの資料を参照してください。IBM のラボ環境では、オプション 12 をネーム・サーバーの完全修飾ドメイン名 (`itsons.itso.ral.ibm.com`) に設定し、オプション 15 をドメインの DNS 接尾部 (`itso.ral.ibm.com`) に設定しています。

4.3.1 シャーシ内の I/O モジュール

HC10 ワークステーション・ブレードと CP20 ワークステーション・コネクション・デバイスにイーサネット接続を提供するには、BladeCenter シャーシに 1 つまたは 2 つの I/O モジュールを取り付ける必要があります。サポートされる I/O モジュールは、次のとおりです。

- サポートされるイーサネット・スイッチ・モジュール (『1.4.1, イーサネット・スイッチ・モジュール』(ページ 15) で説明)

- カッパー・パススルー・モジュール (『1.4.3, IBM BladeCenter カッパー・パススルー・モジュール』(ページ 17) で説明)
- オプティカル・パススルー・モジュール (『1.4.4, IBM BladeCenter オプティカル・パススルー・モジュール』(ページ 18) で説明)

HC10 はファイバー・チャネルおよび InfiniBand スイッチ・モジュールをサポートしません。これは、ファイバー・チャネルまたは InfiniBand 拡張カード用に必要な拡張スロットが HC10 に備わっていないからです。

デフォルトでは、2 つの I/O モジュールが必要です。1 つはベイ 1 に、もう 1 つはベイ 2 に取り付けます。これらの I/O モジュールは、次のように使用されます。

- シャーシのベイ 1 への接続は、HC10 のオペレーティング・システムが使用します。
- 圧縮カードおよび CP20 への接続は、シャーシのベイ 2 を経由します。(BladeCenter S を除く)

『6.2, イーサネット・スイッチ・モジュールの役割を指定』(ページ 106) で説明するように、これらのモジュールは変更できます。例えば、I/O モジュールがただ 1 つ取り付けられている (例えば、ベイ 1 に) 場合は、両方のネットワーク機能がベイ 1 を経由するように構成できます。

4.3.2 IBM サーバー・コネクティビティ・モジュールの使用

BladeCenter シャーシ内でイーサネット接続のために IBM サーバー・コネクティビティ・モジュールを使用する場合は (『1.4.2, IBM サーバー・コネクティビティ・モジュール』(ページ 16) を参照)、CP20 と HC10 の通信を可能にするために、モジュール内の IGMP スヌープを使用不可に設定する必要があります。

この方法について詳しくは、次のアドレスにある RETAIN ヒント H192042 を参照してください。

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5073011

4.3.3 TCP/IP ポート

表 4-3 に、HC10 と CP20 が使用する TCP/IP ポートの一覧を示します。CP20 と、HC10 を格納する BladeCenter シャーシの間で正しく通信が行われるように、ファイアウォールとルーター内でこれらのポートを開放する必要があります。

表 4-3 HC10 および CP20 が使用するポート

機能	プロトコル	HC10 および CP20 のポート番号
動的 IP	DHCP	UDP 67、68
ディスカバリー	DNS	TCP/UDP 53
ディスカバリー	SLP	UDP/TCP 427
Web	HTTPS (TLS/SSL)	TCP 443
Web	HTTP	TCP 80 (HTTPS にリダイレクト)
管理	HTTPS/SOAP/XML	TCP 50000
FW 更新	FTP	TCP 21 (構成可能)
メディア	IPsec-ESP	N/A (暗号化)
メディア制御	SSL	TCP 8000

機能	プロトコル	HC10 および CP20 のポート番号
セキュリティー	HTTPS/SOAP/XML	TCP 50001 (相互認証)
リモート (CP20 のみ)	RDP (PC-over-IP N/A)	TCP 3389

関連情報については、次のアドレスにある RETAIN ヒント H191730 を参照してください。

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072550

4.3.4 VLAN

VLAN はレイヤー 2 ネットワークで一般に使用されます。サポートされる VLAN の数とタイプ、管理 VLAN、サポートされる VLAN タグ付けプロトコル、およびインプリメントされる具体的な VLAN 構成プロトコル (Cisco VLAN Trunking Protocol など) を検討する必要があります。IBM BladeCenter 用のスイッチ・モジュールはすべて、VLAN タグ付けに対応する 802.1Q プロトコルをサポートしています。

4.3.5 デフォルト TCP/IP 構成

HC10 ワークステーション・ブレードには、次の 2 種類の IP アドレスがあります。

- 圧縮カードとワークステーション・コネクション・デバイス間で通信を行うための圧縮カードの IP アドレス。
- ワークステーション・ブレードの内蔵イーサネット・コントローラーの IP アドレス（ネットワーク内でのワークステーション通信用）。

ワークステーション・コネクション・デバイスにも、HC10 ワークステーション・ブレードの圧縮カードと通信するための IP アドレスがあります。これらの IP アドレスの変更について詳しくは、『6.1, 固定 IP アドレスの構成』(ページ 102) を参照してください。

HC10 と CP20 の出荷時の構成では、ホスト名 *ws-broker* のコネクション・ブローカーを使用します。CP20 と HC10 の圧縮カードの IP アドレスは、DHCP を使用するように設定されています。

4.3.6 遅延と帯域幅

遅延時間と帯域幅の 2 つのパラメーターがあります。IBM によるテストの結果では、ワークステーション上で遅れを感じずに快適に作業するには、往復遅延時間が 60 から 80 ミリ秒以下であることが必要です。企業イントラネットの場合、HC10 とワークステーション・デバイスが 4000 キロメートル（2500 マイル）離れていてもこの遅延時間内になります。必要な帯域幅は、アプリケーションによって異なります。テキストや 2D データの場合、必要なデータ転送速度は 1 から 2 Mbps です。CAD などの 3D アプリケーションには、20 から 35 Mbps が必要です。さまざまな距離での遅延時間の長さについては、表 4-4 を参照してください。

表 4-4　テスト・イントラネット上での往復遅延時間の測定

距離 (キロメートル)	理論上のファイバー遅延時間 （ミリ秒）	ping 測定値 (ミリ秒)	米国での距離
0	0	<1	ローカル
800	7	24	隣接する州
1120	12	36	隣接する州

距離 (キロメートル)	理論上のファイバー 遅延時間 (ミリ秒)	ping 測定値 (ミリ秒)	米国での距離
2400	25	50	隣接する州
4800	50	74	東海岸から 西海岸まで
4800	50	119	東海岸から 西海岸まで
11200	116	188	大陸間

4.3.7 帯域幅に関する推奨事項

複数のリモート・デスクトップ・デバイス (CP20) が、共通のイーサネット・リンクに接続されます。このリンク速度は、100 Mbps または 1000 Mbps のどちらかです。リンク速度と BladeCenter HC10 ワークステーション・ブレード内で実行されるアプリケーションが、CP20 リモート・デスクトップのユーザー・エクスペリエンスに直接影響を及ぼします。イーサネット伝送に使用できる帯域幅が十分でなければ、リモート・ビデオの品質低下がユーザーに感じられます。これは通常、ビデオのフリッカーやビデオ・イメージの画面の乱れとして現れます。

CATIA のようにビデオを集中的に使用する高解像度環境では、100 Mbps リンクの場合はユーザー数を 2 人に、1000 Mbps リンクの場合は 15 人に限定してください。

BladeCenter HC10 が動的帯域幅割り振り (デフォルト設定) を行うように構成されていることを確認してください。この構成では、現在のネットワーク状態に応じて、それぞれのユーザーに割り振られる帯域幅が最大化されます。この構成を設定するには、131 ページの『「Bandwidth」オプション』で説明するように、HC10 Web インターフェースで「Device Bandwidth Limit」を 0 に設定します。

この構成により、I/O グラフィックス伝送アダプターが伝送帯域幅を動的に設定できるようになります。ワーストケースのシナリオで、50 Mbps がネットワーク内の各ユーザーごとに割り振られます。

帯域幅に関する最新の考慮事項については、次のアドレスにある RETAIN ヒント H191818 を参照してください。

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072671

4.4 セキュリティー

HC10 ソリューションには、次のように多数のセキュリティー機能が組み込まれています。

- 管理インターフェースへのアクセス

  CP20 ローカル・インターフェース、CP20 Web インターフェース、および HC10 Web インターフェースの 3 つのインターフェースがあります。これらのインターフェースはそれぞれ、パスワードを入力しなければアクセスできません。このパスワードは、それぞれの HC10 および CP20 ごとに固有のものを設定でき、管理者がパスワードを管理できます。

- Web インターフェースのセキュリティー

  HC10 および CP20 の Web インターフェースは、SSL および https を使用して保護されます。すべての http 要求が https にリダイレクトされます。ブラウザーから証明書に関する警告が出されないように、CA ルート証明書も使用されます。

  一度に 1 ユーザーのみが Web インターフェースにログインできます。ユーザーが Web インターフェースにログインしているときに別のユーザーがログインしようとすると、2 番目のユーザーにはログイン先が使用中であることを示す警告が出されます。それでも 2 番目のユーザーがログインを選択すると、最初のユーザーのログアウトが自動的に行われます。

- ローカル・データ

  CP20 にローカル・データは保管されません。このため、機密データがユーザーのデスクに保管されることはなくなり、CP20 と HC10 の間で有効な接続が確立されなければ機密データにはアクセスできません。

- HC10 および CP20 の間の暗号化トラフィック

  128 ビット SSL トンネルが、CP20 との非メディア通信すべてに使用されます。SSL ハンドシェーク・プロトコルの一部として、証明書に基づいた相互デバイス認証が実行されます。メディア・トラフィックは、128 ビット IPsec ESP トンネルによって暗号化されます。IPsec トンネルのキーイング情報は、128 ビット SSL トンネル上でセキュアに設定されます。

- コネクション・ブローカーと、SSL によって保護されたデバイス間のトラフィック

  HC10 と CP20 の間のセッションが切断された場合、コネクション・ブローカーは許可ユーザーのみが Windows デスクトップにアクセスできるようにして HC10 を保護します。Devon IT Connection Broker を使用すると、HC10 はスタンバイ・モードに入り、ユーザーがシステムにアクセスするときに、Windows ユーザー ID とパスワードを入力するためのプロンプトが出されるようになります。

4.5 USB のコントロール

システム管理者は、ユーザーが使用できる USB デバイスを制限できます。

すべての USB デバイスを許可するか、USB デバイスを許可しないか、特定の USB デバイスのみを許可するオプションがあります。このため、管理者がユーザーにヒューマン・インターフェース・デバイス (マウス、キーボードなど) の使用のみを許可したい場合は、このタイプの制御を許可するように USB 制御を設定できます。このセキュリティー機能を使用すれば、従業員がストレージ・ドライブを使用して HC10 から機密情報を取り出すことを防止できます。

図 4-8 に示すように、CP20 Web インターフェースを使用して USB 許可を構成します。ドロップダウン・リストから、使用を許可するデバイスのタイプを選択できます。

注 : ストレージ・ドライブなど特定の USB デバイスの使用を制限する場合は、USB ハブの使用も不可にすることが非常に重要です。ユーザー識別、クラス・タイプなどに基づくデバイスの許可は、ポートごとに行われます。つまり、ハブの使用を許可すると、あらゆるタイプのデバイスが他の USB 許可に関係なくハブ経由で接続できるようになります。

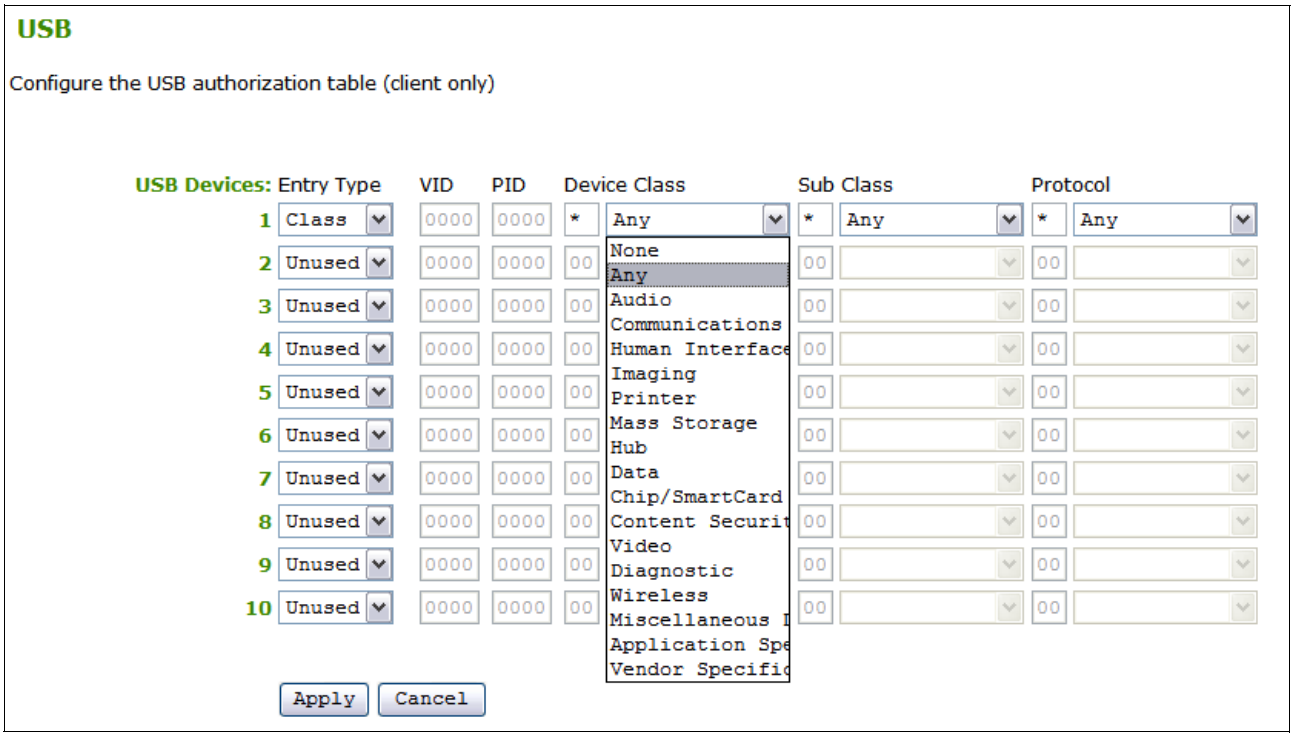


図 4-8　CP20 上での使用を許可するさまざまなタイプのデバイスを示す「USB」オプション

この制御について詳しくは、136 ページの 『USB』を参照してください。

注 : 本書の執筆時点では、複数のデバイスに対して一度に USB 許可を設定する方法はありません。デバイスの USB 許可は個別に設定する必要があります。

4.6 ビデオの接続

HC10 に使用できるビデオ・カードは、1 台または 2 台のモニターをサポートします。これらのモニターは、CP20 ワークステーション・コネクション・デバイスに接続されます。ユーザーは、CP20 の上部または下部の DVI ポートにモニターを接続するか (38 ページの 図 3-7 を参照)、両方の DVI ポートに接続するかを選択できます。

また、HC10 は BladeCenter シャーシ内に取り付けられるので、アドバンスト・マネージメント・モジュールを経由した HC10 からのビデオ表示がサポートされます。BladeCenter シャーシ・コンソールでローカルに表示することも、アドバンスト・マネージメント・モジュール Web ブラウザー・インターフェースを使用してリモート側から表示することもできます。(リモート表示を行う場合、解像度は 1024 × 768 に限定されます)

ビデオ・カードにはポートが 2 つしかないので、これら 3 つのビデオ出力 (デジタル DVI 出力 2 つ、およびアナログのアドバンスト・マネージメント・モジュール出力 1 つ) のうち、同時にアクティブにできるものは 2 つまでです。また、その時点での表示内容によっては、他にもビデオ・カードに起因する制限が生じることがあります。

表 4-5 および 61 ページの表 4-6 は、これらの制限の一覧です。これらの表では、CP20 に接続されたモニター、またはアドバンスト・マネージメント・モジュール・コンソールに表示できるビデオ・ソースが 3 つあります。

- CP20 インターフェース (CP20 ワークステーション・コネクション・デバイスの構成を実行できる)。『6.3, CP20 ローカル・インターフェース』(ページ 106) を参照してください。
- HC10 の POST メッセージ。
- オペレーティング・システムのビデオ（Microsoft Windows のブート画面とデスクトップ)。

表では、3 つの出力に接続されたモニターに表示されるビデオ・ソースを次のように示します。

- DVI ポート 1 (CP20 の背面にある上部コネクター)
- DVI ポート 2 (CP20 の下部コネクター)
- AMM コンソール (BladeCenter シャーシのローカル側、またはブラウザーを介したリモート側)

注 : DVI ポート上でモニター・エミュレーションが使用可能になっている場合 (133 ページの 『「Monitor emulation」 オプション』を参照)、これはポートに物理的に接続されたモニターと同等です。

モニター・エミュレーションは使用可能にすることをお勧めします。

表 4-5 に、2D ビデオ・カードを取り付けた HC10 のビデオ構成を示します。説明については、表の脚注を参照してください。

表 4-5 NVIDIA NVS 120M 2D ビデオ・カード

	DVI ポート 1 のビデオ	**DVI ポート 2 のビデオ**	**AMM コンソール**
DVI ポート 1 (上部ポート) にモニターがただ 1 つ接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	あり	接続されない	適用外[a]
HC10 の POST メッセージ	あり	接続されない	ビデオは表示されない[b]
オペレーティング・システムのビデオ	あり	接続されない	ビデオは表示されない[b]
DVI ポート 2 (下部ポート) にモニターがただ 1 つ接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	接続されない	あり	適用外[a]
HC10 の POST メッセージ	接続されない	あり	あり
オペレーティング・システムのビデオ	接続されない	あり	あり[c]
両方の DVI ポートにモニター 2 台が接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	あり	ビデオは表示されない	適用外[a]
HC10 の POST メッセージ	あり	あり	ビデオは表示されない
オペレーティング・システムのビデオ	あり	あり[d]	ビデオは表示されない

a. CP20 自体によって生成されるビデオなので、適用外。したがって、CP20 ローカル・インターフェースの表示に AMM コンソールを使用することはできません。

b. セキュリティー上の理由から、単一のモニターが使用されている場合に、そのモニターが DVI ポート 1 に接続されていると、AMM コンソールには画面を表示できないように設計されています。
c. AMM コンソール上でオペレーティング・システムのビデオを表示できるようにするには、NVIDIA コントロール・パネルを使用して、デジタル・モニター (DVI ポート) とアナログ・モニター (AMM コンソール) の両方にビデオをミラーリングする必要があります。
d. 両方の DVI モニターにオペレーティング・システムのビデオを表示できるようにするには、NVIDIA コントロール・パネルを使用してデュアル・ビュー・モードを使用可能にする必要があります。

表 4-6 に、2D ビデオ・カードを取り付けた HC10 のビデオ構成を示します。説明については、表の脚注を参照してください。

表 4-6 NVIDIA FX 1600M 3D ビデオ・カード

	DVI ポート 1 のビデオ	**DVI ポート 2 のビデオ**	**AMM コンソール**
DVI ポート 1 (上部ポート) にモニターがただ 1 つ接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	あり	接続されない	適用外[a]
HC10 の POST メッセージ	あり	接続されない	ビデオは表示されない[b,c]
オペレーティング・システムのビデオ	あり	接続されない	ビデオは表示されない[b]
DVI ポート 2 (下部ポート) にモニターがただ 1 つ接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	接続されない	あり	適用外[a]
HC10 の POST メッセージ	接続されない	あり	ビデオは表示されない[c]
オペレーティング・システムのビデオ	接続されない	あり	あり[d]
両方の DVI ポートにモニター 2 台が接続されている場合のビデオ出力			
CP20 ローカル・インターフェース	あり	ビデオは表示されない	適用外[a]
HC10 の POST メッセージ	あり	ビデオは表示されない[c]	ビデオは表示されない[c]
オペレーティング・システムのビデオ	あり	あり[e]	ビデオは表示されない

a. CP20 自体によって生成されるビデオなので、適用外。したがって、CP20 ローカル・インターフェースの表示に AMM コンソールを使用することはできません。
b. セキュリティー上の理由から、単一のモニターが使用されている場合に、そのモニターが DVI ポート 1 に接続されていると、AMM コンソールには画面を表示できないように設計されています。
c. FX 1600M は、POST 時には 1 台の DVI モニターへのビデオのみをサポートします (2 番目の DVI、および AMM には表示しない)。
d. AMM コンソール上でオペレーティング・システムのビデオを表示できるようにするには、NVIDIA コントロール・パネルを使用して、デジタル・モニター (DVI ポート) とアナログ・モニター (AMM コンソール) の両方にビデオをミラーリングする必要があります。
e. 両方の DVI モニターにオペレーティング・システムのビデオを表示できるようにするには、NVIDIA コントロール・パネルを使用してデュアル・ビュー・モードを使用可能にする必要があります。

4.6.1 CRT モニターの制限事項

CRT モニターが CP20 ワークステーション・コネクション・デバイスに接続されている場合は、高解像度または高リフレッシュ・レート時にビデオが壊れたり、表示されなくなったりすることがあります。

HC10 内のビデオ・カードは 2048x1536 までの解像度をサポートできますが、CP20 内のコンポーネントによってこれより低く制限されます。このコンポーネントは *Chrontel* パーツと呼ばれ、CP20 に送られるデジタル信号をアナログ信号に変換します。Chrontel パーツの最大ピクセル・クロックは 165 MHz です。POST 中に、ビデオ・カードはネイティブの解像度でビデオを表示します。C220P や P275 などの大きな CRT の場合、ネイティブ解像度は 1600x1200 (75 Hz) です。この解像度では 165 MHz より高いピクセル・クロックが使用されるので、ビデオは表示されません。

デスクトップで使用される解像度にも、同じ制限が影響を及ぼします。165 MHz より高いピクセル・クロックを必要とする解像度を使用する場合、ビデオ・ドライバーは高い解像度を削除し、パン・スキャン・モード（Windows デスクトップが画面の表示内容より大きくなる）に切り替えることによって、デスクトップをモニター自体より大きく表示します。

詳しくは、次のアドレスにある RETAIN ヒント H191783 を参照してください。

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597

4.6.2 その他のビデオに関するヒント

ビデオとモニター・エミュレーション機能に関連した RETAIN ヒントには、次のものがあります。

- ワークステーション・コネクション・デバイスにビデオが表示されない (ヒント H191777)

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596

- WCD 上で Microsoft Windows が起動するまで画面が黒くなる (ヒント H191763)

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072561

- WCD にビデオを表示するためにシャーシ側でのユーザー対話操作が必要 (ヒント H191777)

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596

- マウスまたはキーボードを使用して HC10 のスタンバイ・モードを終了できない (ヒント H191821)

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072678

4.7 接続方式

HC10 と CP20 間の接続を確立するには 2 とおりの方法があります。

- 接続管理ソフトウェア
- ピアツーピア

4.7.1 接続管理ソフトウェア

コネクション・マネージャー (*コネクション・ブローカー* とも呼ばれる) は、HC10 と CP20 の間の接続を作成、維持、および削除するためのソフトウェア・コンポーネントです。この

ソフトウェアを使用すれば、接続の集中管理により、1 人の管理者がすべての接続を制御できます。HC10 と CP20 のコンポーネントを環境に追加すると、その存在、ID、および物理トポロジーが、企業環境内で実行されているコネクション・マネージャーの 1 つ以上のインスタンスに対して通知されるか、コネクション・マネージャーによって検出されます。

ユーザーが CP20 を使用して環境へのログインを試みると、コネクション・マネージャーは特定の CP20 装置を認識して識別し、使用可能な (または既に割り当て済みの) HC10 を識別し、2 つのデバイス間のアソシエーションを作成します。

接続が確立された後、コネクション・マネージャーは接続の状態 (*接続* または *切断*) を監視してセッション管理を行う一方、接続されたエンドポイント間の通信を調整します。

HC10 と CP20 間の接続を確立するには 3 とおりの方法があります。

- 固定シーティング
- フリー・シーティング
- プーリング

ヒント : デバイスの接続方法 (フリー、固定、およびプーリング) は、コネクション・ブローカーによって制御されます。

固定シーティング

固定シーティング は、それぞれの CP20 を特定の HC10 に割り当て、この接続のみを確立できるようにする方式です。固定シーティング環境では、同じ CP20 が常に同じ HC10 に接続します。図 4-9 は、固定シーティングのダイアグラムを示しています。

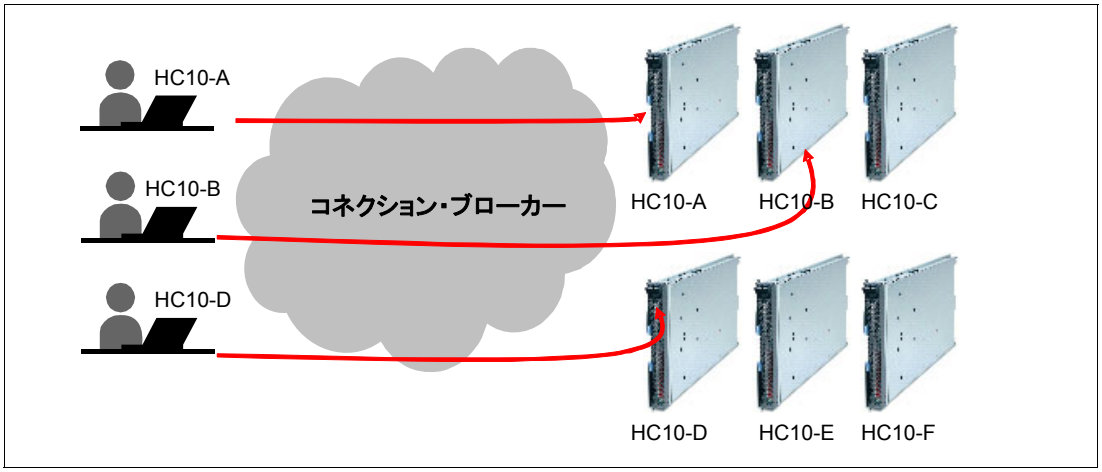


図 4-9　固定シーティング接続

図 4-9 では、HC10-A に割り当てられた CP20 の席にユーザーが座ると、その CP20 は常に HC10-A に接続します。ログオン・セキュリティーは、HC10 のオペレーティング・システムによって処理されます。

フリー・シーティング

フリー・シーティング を使用する場合、特定の HC10 に関連付けられるものは、固定シーティングのように CP20 ではなく、ユーザーです。つまり、その指定されたユーザーはどの CP20 デバイスの席に座っても構わず、ユーザー名を入力すればそのユーザーの HC10 ワークステーション・ブレードに接続されます。図 4-10 は、フリー・シーティングの例を示しています。

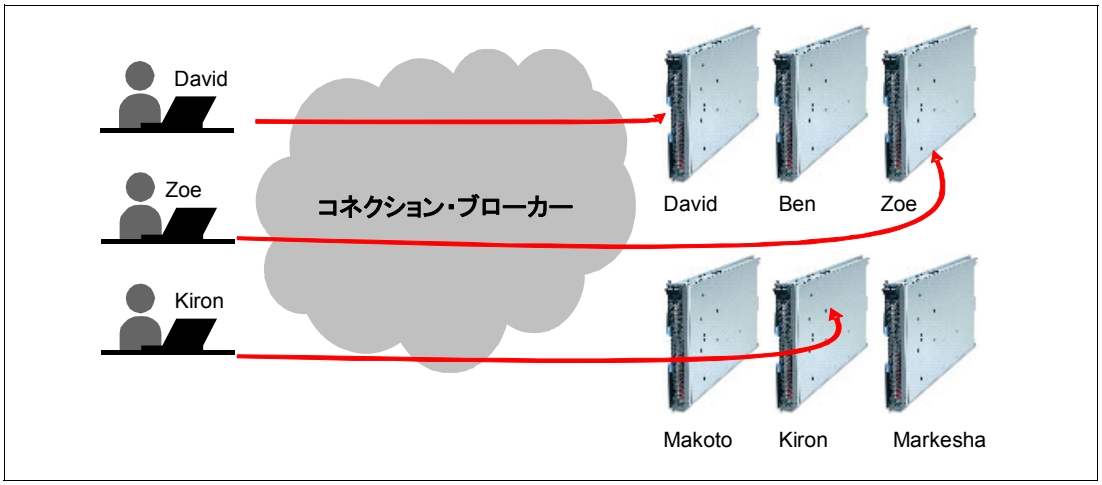


図 4-10　フリー・シーティング接続

図 4-10 では、ユーザー Zoe がオフィス内で座っている席に関係なく、ログインすれば毎回同じワークステーション・ブレードに接続します。

コネクション・ブローカーのインプリメンテーションによっては、ユーザーはユーザー名を指定するだけでパスワードは指定しません。固定シーティングの場合と同様に、ログオンのセキュリティーは HC10 のオペレーティング・システムによって処理されます。

プーリング

*プーリング*は、フリー・シーティングのスーパーセットです。フリー・シーティングの場合のように、ユーザーがただ 1 つのワークステーション・ブレードにリンクされることはなく、プーリングではそのユーザーが HC10 のプールからワークステーションに割り当てられます。

プーリングの例については、図 4-11 を参照してください。ユーザー Kiron がログインすると、Kiron が接続する資格のあるワークステーション・ブレードのプールを判別するために、認証データベースが照会されます。*プール B* が戻されます。その後、ブローカーはプール B からいずれかのワークステーション・ブレードを選択して、Kiron に割り当てます。プールのユーザー・セキュリティーを確保するために、認証と割り当ての処理が開始される前に、Kiron はユーザー ID とパスワードの両方を入力する必要があります。

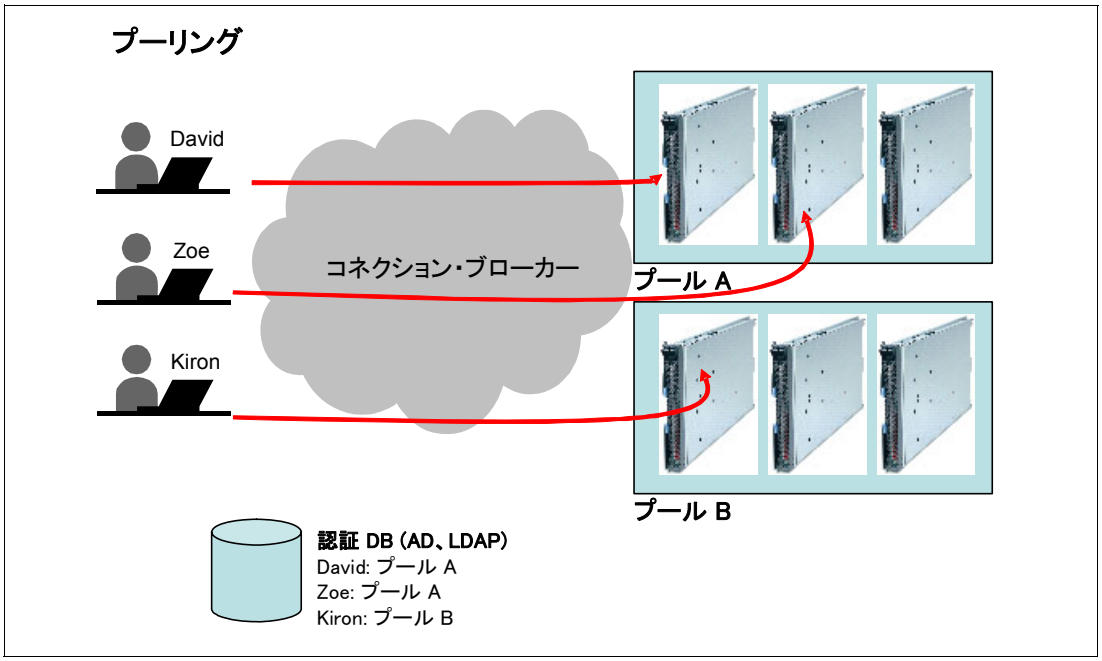


図 4-11　プーリング接続の例

次の例に示すように、プーリングはいくつかの方法でインプリメントできます。

- プール A には高度な構成のワークステーション (大きなメモリーと高速 CPU) を含め、プール B には標準構成のワークステーションを含めることができます。
- プール A のシステムには 1 つのアプリケーションのセットをインストールし、プール B には別のセットをインストールできます。
- プール A はスペイン語を話すユーザー用に構成し、プール B は英語を話すユーザー用に構成できます。

プーリングはフリー・シーティングの 1 形式で、プール・サイズをただ 1 つのシステムに設定すれば、プーリングとフリー・シーティングの結果は同じになります。

4.7.2 ピアツーピア接続

コネクション・ブローカーを使用する代わりに、ピアツーピア接続を使用して接続することもできます。*ピアツーピア接続* を使用すると、HC10 と CP20 の間で追加ソフトウェアを使用せずに接続が可能です。次のように、接続のオプションが 2 つあります。

- セッション

  セッション接続は、接続先の HC10 の IP アドレスを入力すると行われ、特定の HC10 に直接接続できます。

- 検出

  検出オプションを使用すると、使用可能な 10 台の HC10 ブレード (つまり、まだセッション中ではない) のリストが示され、ユーザーはそこから接続先を 1 つ選択できます。

図 4-12 に、これら 2 つのオプションを示します。

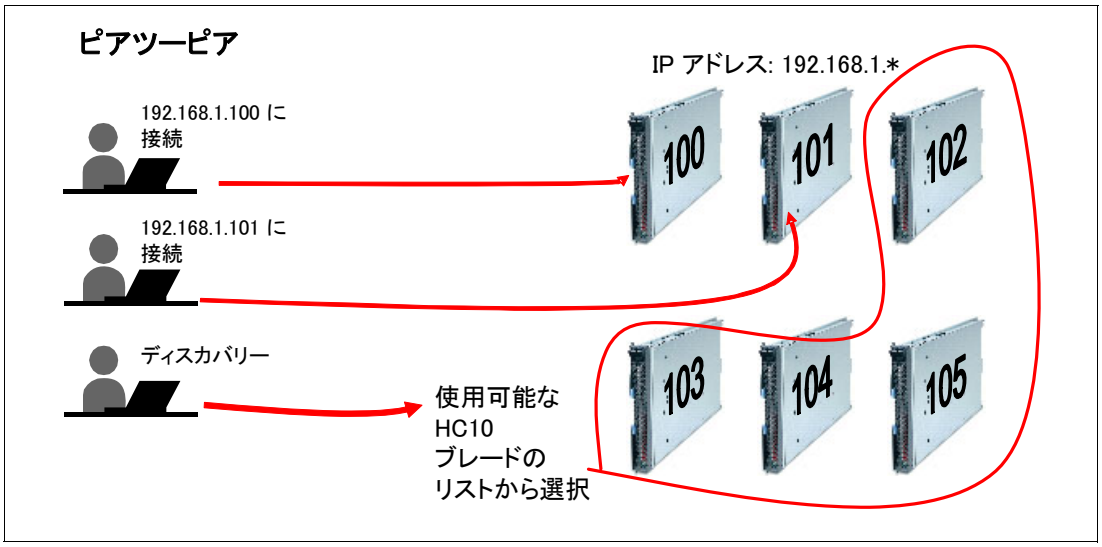


図 4-12　ピアツーピア接続

4.8 Devon IT Connection Manager

Devon IT Connection Manager は、フリー・シーティングと固定シーティングの両方をサポートします。現行バージョンでは、LDAP または Active Directory® サーバーを使用したプーリングまたは認証はサポートしていません。

Devon IT Connection Manager は、仮想計算機をベースとしたアプライアンスとしてインプリメントされます。ソフトウェアを実行する前に、VMware Player または VMware Server をダウンロードし、インストールする必要があります。VM をホストするマシンの最小システム要件は、次のとおりです。

- VMware Server 1.03 または VMware Player 1.04
- 768 MB RAM
- クロック速度 2 GHz の Pentium® 4 プロセッサー
- 40 GB のハード・ディスク・スペース

ブローカーは、静的 IP アドレス、または DHCP によって割り当てられる IP アドレスの使用をサポートしますが、静的 IP アドレスの使用をお勧めします。ホスト名は *ws-broker* にする必要があります。CP20 と HC10 の圧縮カードは、この名前を検索するように出荷時に構成されているからです。

コネクション・ブローカーは、Web ブラウザー・ベースのグラフィカル・ユーザー・インターフェース (GUI)、およびコマンド・ライン・インターフェース (CLI) の 2 種類の管理インターフェースを備えています。サポートされる Web ブラウザーは、次のとおりです。

- Firefox 1.5 以降
- Internet Explorer® 7 以降

Web ベース・インターフェースでは、ホスト名 *ws-broker* (デフォルト) のコネクション・ブローカーを検索するように構成されたネットワーク内のデバイスが、電源オンと同時に表示されます。Web インターフェースは、図 4-13 に示すように 3 つのテーブルに分かれています。

- 「Terminals」テーブルには、ブローカーと通信した CP20 デバイスがすべてリストされます。

- 「Hosts」テーブルには、ブローカーと通信した HC10 がすべてリストされます。リストされる IP アドレスは、圧縮カードのものです。
- 「Sessions」テーブルには、アクティブ・セッションがすべてリストされます。

CP20 または HC10 を左クリックすると、そのデバイスに関連したイベント・ログなど、デバイスの詳細情報が右側のペインに表示されます。また、CP20、HC10、またはセッションを右クリックすると、使用可能なアクションが表示されます。

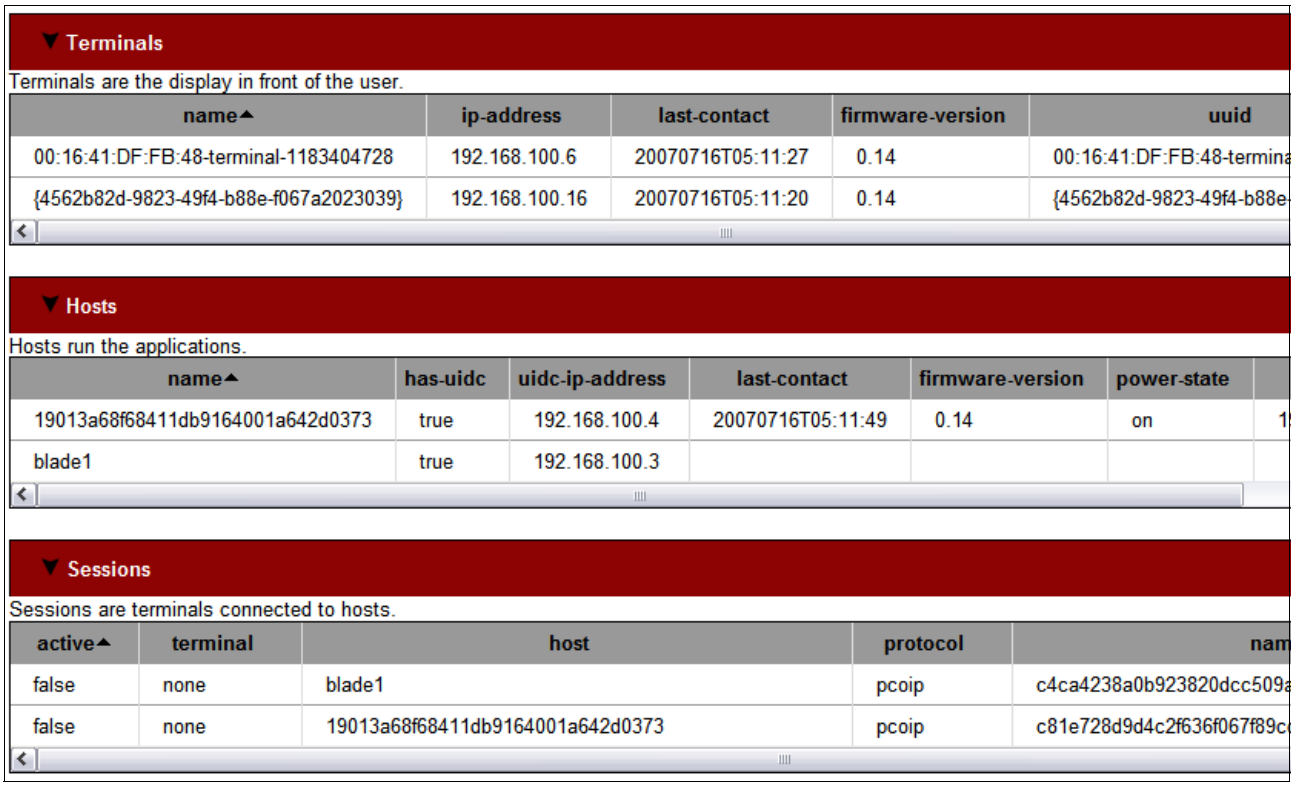


図 4-13　Devon IT Connection Broker のブラウザー・インターフェース

本書の執筆時点では、Devon IT は次の 2 とおりの接続方式をサポートしています。

- 固定シーティング

  この方式は、特定の CP20 から特定の HC10 への接続を確立するために使用されます。この方式を使用すると、ユーザーは CP20 から HC10 に自動的に接続されます。

- フリー・シーティング

  この方式も、CP20 と HC10 の間で 1 対 1 の接続を確立するために使用されますが、さらに柔軟性の高い方式です。ユーザーが接続を確立しようとすると (CP20 画面の「**Connect**」ボタンをクリックして)、プロンプトが表示され、ユーザーは接続に使用する名前を入力できます。ユーザーが接続される HC10 は、入力したユーザー名と同じ名前のものです。1 つの HC10 に接続できる CP20 は常にただ 1 つですが、フリー・シーティングを使用すればユーザーは任意の CP20 から特定のブレードにログインできます。

接続が確立されると、Web ベース・インターフェースに表示されます。このインターフェースは、接続が確立されているかどうか、どのマシン (HC10 および CP20) が接続に関係しているか、どのタイプのプロトコルが使用されているか (常に PC-over-IP) を表示します。

Connection Management ソフトウェア内の検索機能を使用すれば、大規模な CP20-HC10 環境の管理が容易になります。検索機能によって、結果が照会に基づいてフィルターに掛けられます。テーブルの見出しになっている属性に基づいて検索を適用できます。管理者がこの検

索機能を使用して多数のデバイスを容易にナビゲートでき、情報を迅速に効率よく見つけることができます。また検索機能は、同じ名前で始まる (例 : *Floor_1*) デバイスのグループの検索、または同じレベルのファームウェア (例 : *0.13*) を使用するデバイスの検索にも便利です。さまざまな検索オプションを表示するには、『5.1.4, 検索フィルター機能』(ページ 85) を参照してください。

Connection Management ソフトウェアのもう 1 つの重要なコンポーネントは、環境にあるすべてのデバイスのファームウェアを更新する機能です。ファームウェアを Connection Management ソフトウェアにアップロードしてから、すべての CP20 と HC10 にプッシュできます。

次のように、ファームウェア更新のオプションが 2 つあります。

- 即時

  即時更新は、すべての接続を自動的に切断し、新規ファームウェアをインストールして、圧縮カードをリセットします。この更新方法の欠点は、勤務時間中にはユーザーの接続が中断され、ユーザーが接続を再確立できるようになるまで数分のインストール時間がかかることです。

- バックグラウンド

  バックグラウンド更新は、接続のない状態が次回生じたときに更新をインストールします。このため、ファームウェアがプッシュされたときにデバイスが現在セッション中でなければ、そのデバイスは自動的に更新を受信するためのキューに入れられます。この方式の欠点は、ユーザーが HC10 から CP20 を切断しない限り、デバイスが更新されない点です。

ファームウェア更新の戦略としては、ファームウェアをデプロイする基本方式としてバックグラウンドを使用し、少数のシステムのみが残ったとき (例えば、1 週間ほど経った後) に即時方式を使用することをお勧めします。

Devon IT Connection Management ソフトウェアを環境に適用する方法について詳しくは、『5.1.3, ファームウェアの更新』(ページ 79) を参照してください。

4.9 Leostream Hosted Desktop Connection Broker

Leostream Hosted Desktop Connection Broker は仮想アプライアンスとして稼働し、次の最小ハードウェアを必要とします。

- Pentium 4™ (または同等品) 1.5 GHz 以上
- 1.5 GB のメモリー
- 8 GB のハード・ディスク・スペース

仮想アプライアンス・イメージを仮想化層にロードするには、VMware Converter ツールを使用する必要があります。

ソフトウェアを実行すると、図 4-14 のようなパネルが表示され、Web ベース管理者インターフェースの IP アドレスが示されます。Web ブラウザーを使用して、この IP アドレスにアクセスします。この Web インターフェースを使用して、すべての管理機能を実行できます。

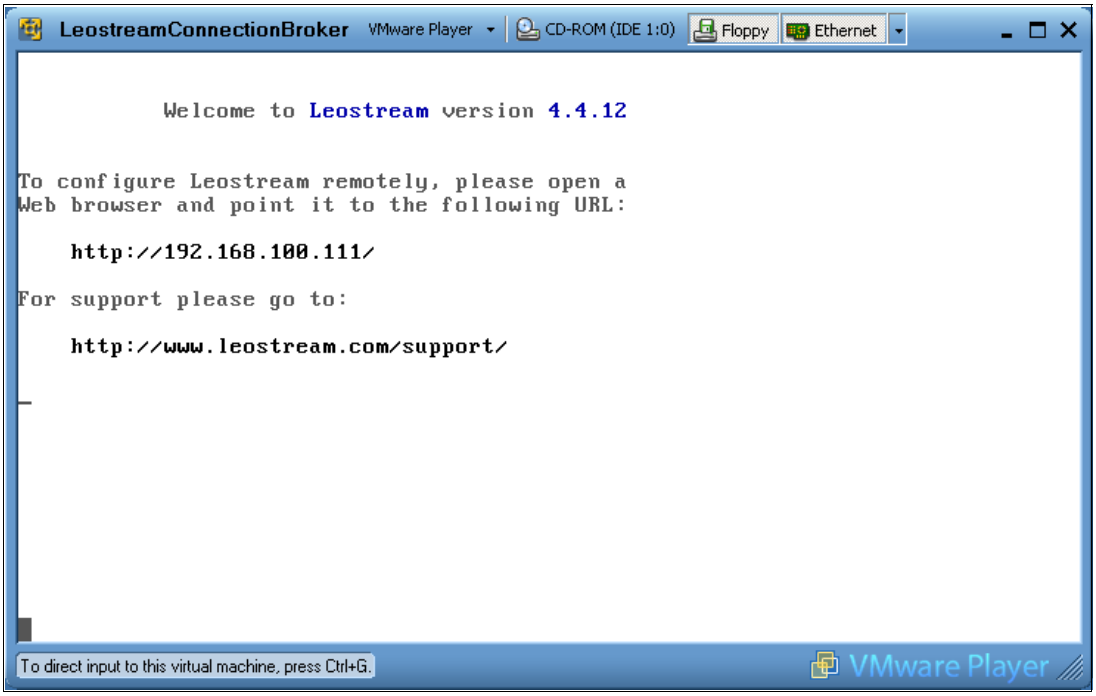


図 4-14　稼働中の Leostream 仮想アプライアンス

注 : コネクション・ブローカーの IP アドレスを変更する必要がある場合は、コンソールで Alt-F2 を押し、ユーザー名 *admin* とパスワード *leo* を指定してログインします。これで、ネットワーク設定を変更するオプションが表示されます。

Web インターフェースにログインするには、次の資格情報を使用します。

- ユーザー名 : *admin*
- パスワード : *leo*

その後、ライセンス・キーを入力し、ライセンス条項を受諾する必要があります。図 4-15 に示すように、Web ブラウザーを使用して管理インターフェースにアクセスします。

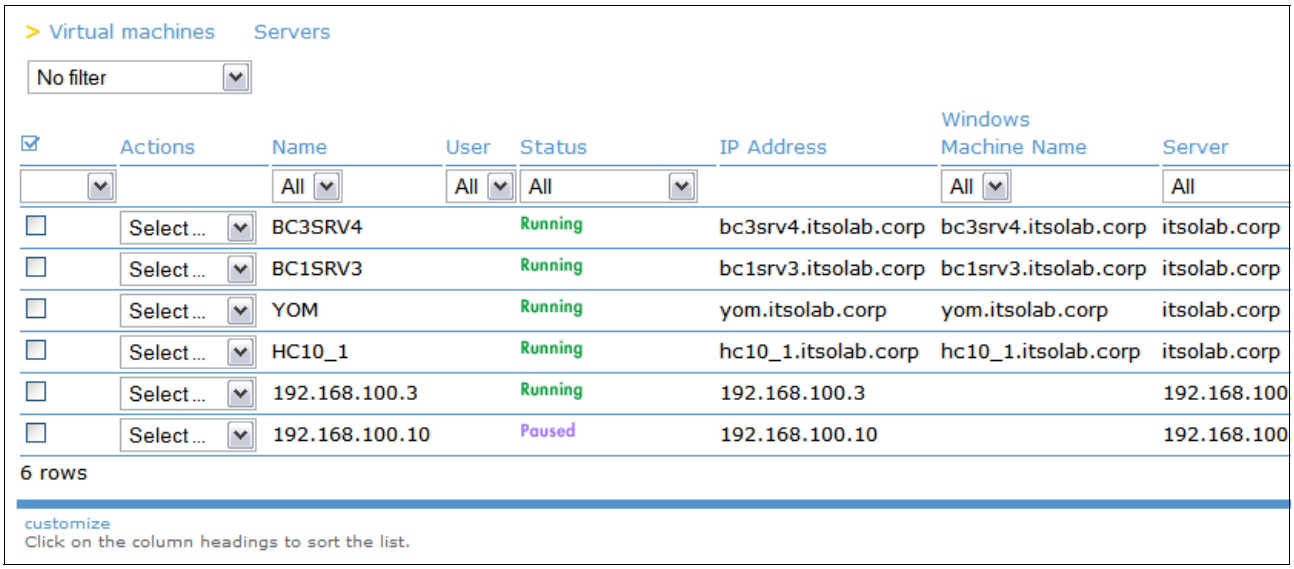


図 4-15　Leostream Connection Broker メインパネル

Leostream Hosted Desktop Connection Broker は、HC10-CP20 接続の集中管理、およびホスト・デスクトップ・セッションを実行します。このセッションは、RDP や VNC など、他のリモート・ビューアー・プロトコルを実行し、物理ハードウェアまたは仮想ハードウェアを使用します。

出荷時の構成では、HC10 と CP20 はホスト名 *ws-broker* のコネクション・ブローカーを使用します。Leostream ブローカーはデフォルトでこのように構成されているので、これ以外の構成は必要とせずにデバイスからコネクション・ブローカーへの接続を確立できます。

ブローカーに接続するためにデバイスを構成するには、さらに 2 とおりの方法があります。

- それぞれの HC10 と CP20 にコネクション・ブローカーの IP アドレスを手動で入力する
- SLP ディスカバリーを使用可能に設定し、コネクション・ブローカーに HC10-TC10 を検出させる

HC10 ブレードが検出された後、使用可能なその他のホスティッド・デスクトップ・リソースとともに、ブレードがコネクション・ブローカーに表示されます。

管理者はその後、ブレードを一連のリソース・プールに分割し、ユーザーに割り振る方法を決定できます (プールからランダムに選択するか、特定のユーザーに永続的に割り当てる)。

コネクション・ブローカー内にユーザー情報を保管することもできますが、一般的には外部認証サーバー (Microsoft Active Directory、Novell eDirectory、IBM Tivoli Directory Server、または Open LDAP) が使用されます。外部認証サーバーを使用すれば、ホスティッド・デスクトップの割り当てを認証サーバー内の既存ユーザー・プロファイルに関連付けることができます。

Hosted Desktop ソフトウェアを環境に適用する方法について詳しくは、『5.2, Leostream Hosted Desktop ソフトウェア』(ページ 87) を参照してください。

製品情報については、次のアドレスにある Leostream Hosted Desktop Connection Broker の Web ページを参照してください。

http://www.leostream.com/productVHDC.html

5

コネクション・ブローカーを使用したセットアップ

『4.7.1, 接続管理ソフトウェア』(ページ 62) で説明したとおり、コネクション・マネージャー (*コネクション・ブローカー* とも呼ばれる) は、HC10 (ホスト) と CP20 (端末) の間の接続を作成、維持、および削除するためのソフトウェア・コンポーネントです。このソフトウェアを使用すれば、接続の集中管理により、1 人の管理者がすべての接続を制御できます。

この章では、コネクション・ブローカー・ソフトウェアと組み合わせて BladeCenter HC10 ソリューションを使用する方法を説明します。Devon IT Connection Management ソフトウェアと Leostream Hosted Desktop ソフトウェアを使用して環境を構成する方法について解説し、セキュアな環境を確立するために役立つさまざまなセキュリティー・オプションについて説明します。

ほとんどのお客様が、接続を管理するためにコネクション・ブローカーを採用するものと考えられます。したがって、HC10 ソリューションは出荷時に次のようにあらかじめ構成済みです。

- CP20 と HC10 の圧縮カードは、DHCP 割り当ての IP アドレスを使用します。
- HC10 と CP20 の両方で接続管理が使用可能に設定されています。
- デバイスはホスト名 *ws-broker* のブローカーに接続するように構成されています。

テストまたは随時接続のために、CP20 と HC10 は、101 ページの『第 6 章 構成オプション』で説明するピアツーピア接続もサポートしています。

この章で説明するトピックは、次のとおりです。

- 『5.1, Devon IT Connection Broker』(ページ 72)
- 『5.2, Leostream Hosted Desktop ソフトウェア』(ページ 87)
- 『5.3, セキュリティー』(ページ 99)

5.1 Devon IT Connection Broker

HC10 と CP20 のデフォルト構成では、IP アドレスには DHCP を使用し、接続にはコネクション・ブローカーを使用します。どちらのデバイスも、接続管理ソフトウェアのホスト名として *ws-broker* を使用し、ソフトウェアがサーバーにインストールされると同時に、通信および接続の作成が可能になります。したがって、デバイスがネットワークに追加されると、デバイスはすぐに接続を確立できるようになります。

Devon IT Connection Management ソフトウェアを使用すると、*固定シーティング*または*フリー・シーティング*のどちらかを使用した接続が可能です。固定シーティングの方式では、それぞれの CP20 (クライアントまたは端末) が、常に 1 台の HC10 (ホスト) に接続できます。固定シーティングを使用すると、Connection Management ソフトウェア内でクライアントとホストの名前は同じになります。もう 1 つの接続オプションはフリー・シーティングで、ユーザーはオフィス内の任意の CP20 から特定の HC10 にログインできます。

本書では、ブローカー・ソフトウェアのインストールについては説明しないので、ソフトウェアに付属のインストール手順書のとおりに行う必要があります。ただし本書の執筆時点では、インストールに必要な作業は、仮想計算機ファイルを解凍し、VMware Player または別の VMware エンジンを実行して、プロンプトのとおりに管理者パスワード、時間帯、およびネットワーク・アドレスを構成するだけです。

Connection Management ソフトウェアをインストールした後、仮想計算機の IP アドレス（図 5-1 に示すような）を Firefox または Internet Explorer 7.0 ブラウザーに入力します。(IE 7 は各種ログの最新項目を 250 件までリストしますが、Firefox は最新項目を 2500 件までリストします。)

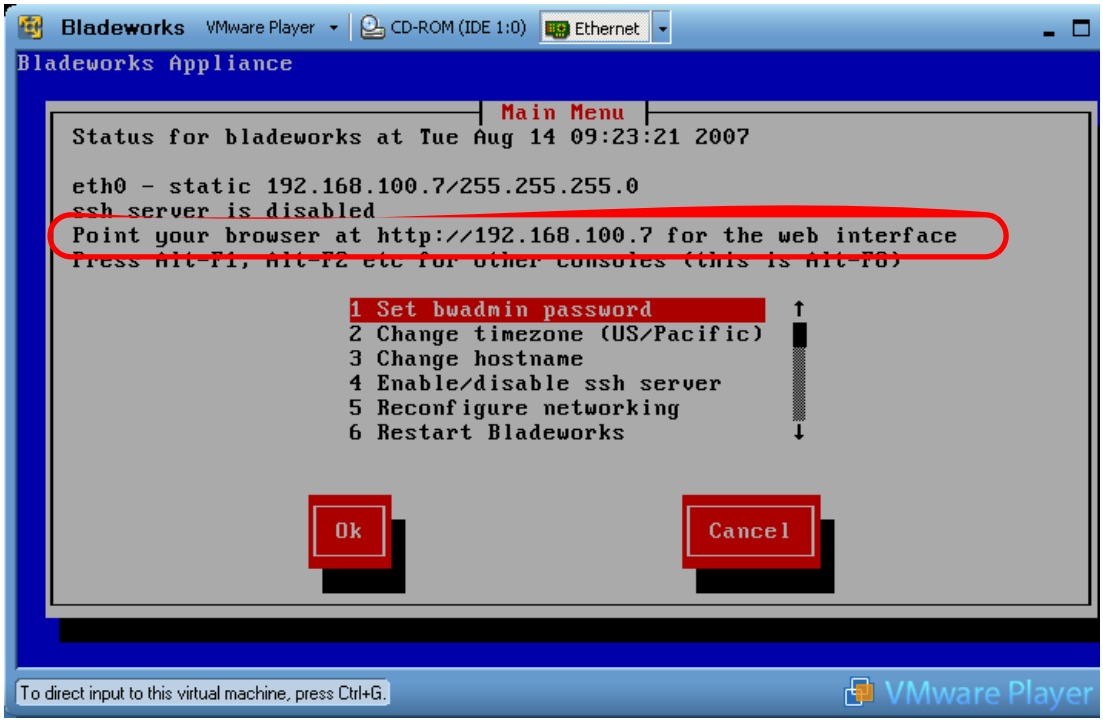


図 5-1　Devon IT Connection Management ソフトウェアの VMware 仮想イメージ

この操作によって、Connection Management ソフトウェアの Web インターフェースが開きます。このインターフェースのメインパネルには、図 5-2 に示すように 4 つのオプションがあります。

- Quick start

  「Quick start」オプションを選択すると、Connection Management ソフトウェアの使用法の説明が表示されます。

- Web browser-based administration tool

  Web ブラウザー・ベースのインターフェースを使用すると、HC10 と CP20 の環境を Web インターフェースによって管理できます。(この章の大部分で、このインターフェースについて説明します。)

- Command line based administration tool

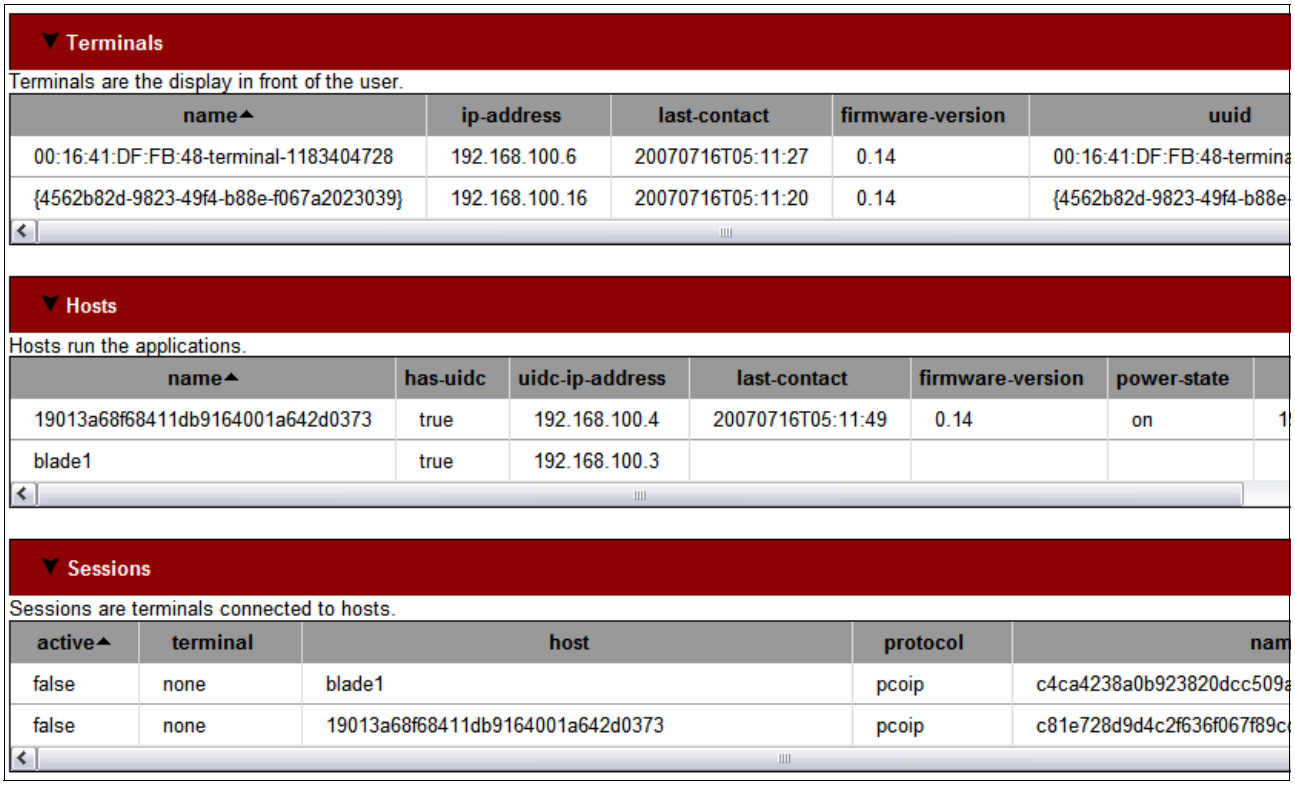
  「command line」オプションを選択すると、CLI インターフェースの使用法が表示されます。CP20 と HC10 の環境の管理は Web インターフェースから行うことができますが、コマンド行インターフェースを使用して同じ作業を行うこともできます。

- Learn more

  「learn more」オプションを選択すると、用語集、コンポーネントとその相互作用、管理ツールの使用法、サポート情報などを説明する、ドキュメンテーション全体を表示できます。環境の管理を始めるには、「Web based administration tool」をクリックします (図 5-2 を参照)。

図 5-2　Web ベース Connection Management ソフトウェアのメインウィンドウ

Web ベース管理ツールは、存在する HC10 (ホスト)、CP20 (端末)、および接続 (セッション) を表示します。図 5-3 に、アクティブ・デバイスとセッションの表示例を示します。



Terminals

Terminals are the display in front of the user.

name▲	ip-address	last-contact	firmware-version	uuid
00:16:41:DF:FB:48-terminal-1183404728	192.168.100.6	20070716T05:11:27	0.14	00:16:41:DF:FB:48-termina
{4562b82d-9823-49f4-b88e-f067a2023039}	192.168.100.16	20070716T05:11:20	0.14	{4562b82d-9823-49f4-b88e-

Hosts

Hosts run the applications.

name▲	has-uidc	uidc-ip-address	last-contact	firmware-version	power-state	
19013a68f68411db9164001a642d0373	true	192.168.100.4	20070716T05:11:49	0.14	on	1
blade1	true	192.168.100.3				

Sessions

Sessions are terminals connected to hosts.

active▲	terminal	host	protocol	nam
false	none	blade1	pcoip	c4ca4238a0b923820dcc509a
false	none	19013a68f68411db9164001a642d0373	pcoip	c81e728d9d4c2f636f067f89c

図 5-3　Web 管理ツールでのデバイスの検出

特定のデバイスに関する詳細を表示するには、そのデバイスをクリックします。ウィンドウの右側に詳細ペインが開きます。図 5-4 にこの詳細ペインの例を示します。

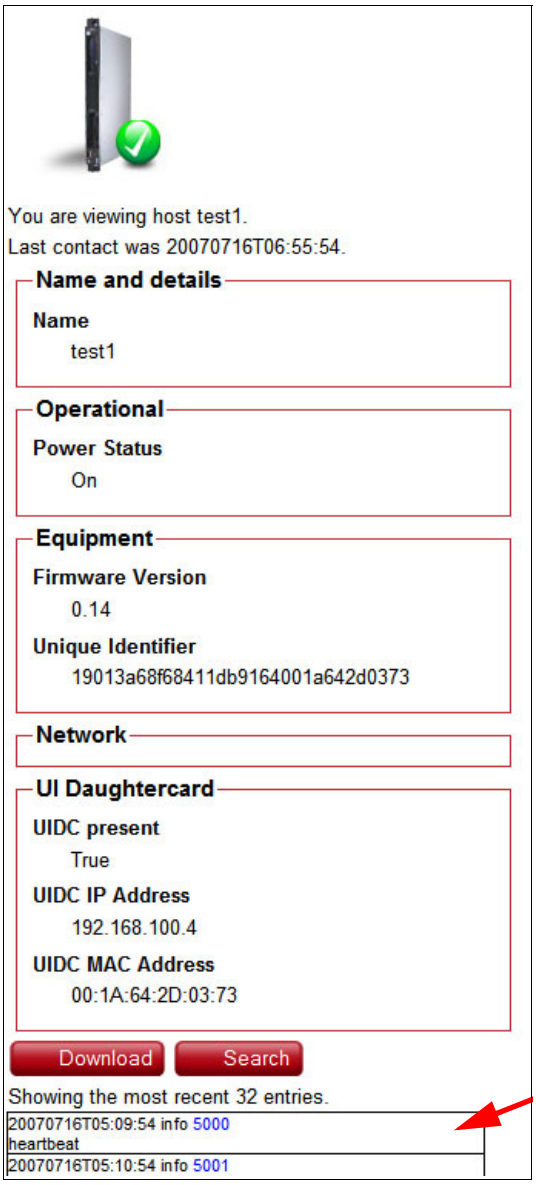


図 5-4　検出された特定のデバイスの詳細

HC10 の場合、「Network」フィールドはデフォルトでブランクになっています。必要に応じて、このフィールドを使用して、HC10 上で稼働する Windows が使用するネットワーク・コントローラーの IP アドレスを入力できます。CP20 の「Network」フィールドには、CP20 の IP アドレスと MAC アドレスが表示されます。

詳細ペインには、図 5-4 に示すように、最新のログ項目も表示されます。ただし、より簡単にこれらのログ項目を表示する方法として、**「Search」**をクリックすれば、図 5-5 に示すように大きなウィンドウにログ・メッセージが表示されます。

Logs for host 2d. 67/67

These log events are pertinent to your device.

time▲	id	type	objects	message
20070824T16:35:22	5001	info	host:2d	Deferring soft reset until host restarts, sleep, etc
20070824T16:35:22	5001	info	host:2d	Current host power state: S0
20070824T16:36:27	6007	error	host:2d	cms setPeer failed for the host due to network failure. Det
20070824T16:36:46	5016	info	host:2d	eventHostProcessorPowerStatus message. Power status:
20070824T16:36:47	6026	info	firmware:Version 15,host:2d	cms sent startFirmwareDownload to the device since the c
20070824T16:37:32	5001	info	host:2d	Firmware Build ID: v062
20070824T16:37:32	5001	info	host:2d	*** Power management post reset state: standalone ***
20070824T16:37:32	5001	info	host:2d	Previous Bootloader Build ID: , Version: 0.0
20070824T16:37:32	5001	info	host:2d	Previous Firmware Build ID: v062 , Version: 0.14
20070824T16:37:32	5001	info	host:2d	*** Power management event: PCI sleep ***
20070824T16:37:32	5001	info	host:2d	*** RESET CAUSED BY: UI ***
20070824T16:37:32	5001	info	host:2d	Firmware Version: 0.14
20070824T16:37:32	5001	info	host:2d	Teradici Corporation (c)2007
20070824T16:37:32	5001	info	host:2d	Firmware Build date: Aug 3 2007 11:02:28
20070824T16:37:32	5001	info	host:2d	Bootloader version not found
20070824T16:37:37	5001	info	host:2d	Network link UP
20070824T16:37:37	5001	info	host:2d	Renewing DHCP lease

図 5-5　HC10 のログ詳細

ログ・ビューには検索フィルター・フィールドがあり、ここで特定のログ項目を選択できます。

また、75 ページの図 5-4 に示した**「Download」**をクリックして、ログ項目をテキスト・ファイルに保存することもできます。

変更を加える対象のデバイスを右クリックして、いくつかのタスクを実行できます。右クリックすると、図 5-6 に示すように、オプション「Related」、「Edit」、「Rename」、および「Delete」を含むメニューが開きます。

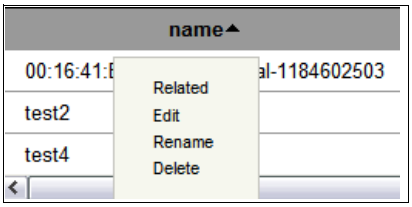


図 5-6　デバイスを右クリックすると表示されるオプション

「**Related**」をクリックすると、クリックしたものと同じ名前のデバイスが自動的に表示されます。例えば、*test2* という名前のホストと *test2* という名前の端末があり、ホストを右クリックして「**Related**」をクリックすると、次の検索照会が実行されます。

```
"+terminal:test2" OR "+name:test2"
```

検索結果には、*test2* という名前の付いたホストと端末の両方が表示されます。元のリストに戻るには、検索フィールドからテキストを消去するだけです。Connection Management の検索機能について詳しくは、『5.1.4, 検索フィルター機能』(ページ 85) を参照してください。

「**Edit**」をクリックすると、メニューが右側に表示され、デバイスの詳細を編集できます。「**Rename**」をクリックすると、デバイスの名前を変更できます。例えば、固定シーティングを実装するには CP20 と HC10 の両方に同じ名前を付ける必要があり、そのような場合にこのオプションを選択します。

「**Delete**」をクリックすると、リストからデバイスが削除されますが、後で自動的に表示されます。CP20 は 5 分以内に表示され、再起動は必要ありませんが、HC10 をリストに表示するためには、その前に HC10 内の PC-over-IP プロセッサーをリセットし、HC10 を再起動する必要があります。

また、「**Add**」→「**Terminal**」または「**Add**」→「**Host**」をクリックして、端末またはホストを手動で追加することもできます (図 5-7 を参照)。この操作を行うと、右側にメニューが表示され、そこにデバイスに関する詳細を手動で入力できます。通常は、この作業を行う必要はありません。

図 5-7　端末またはホストの手動追加

5.1.1 フリー・シーティング

フリー・シーティング接続を使用すると、任意のロケーションから特定の HC10 にアクセスできます。フリー・シーティングについての説明は、63 ページの 『フリー・シーティング』を参照してください。このタイプの接続を構成するには、次の手順で行います。

1. 名前を変更する HC10 を右クリックし、「**Rename**」をクリックします (図 5-8 を参照)。

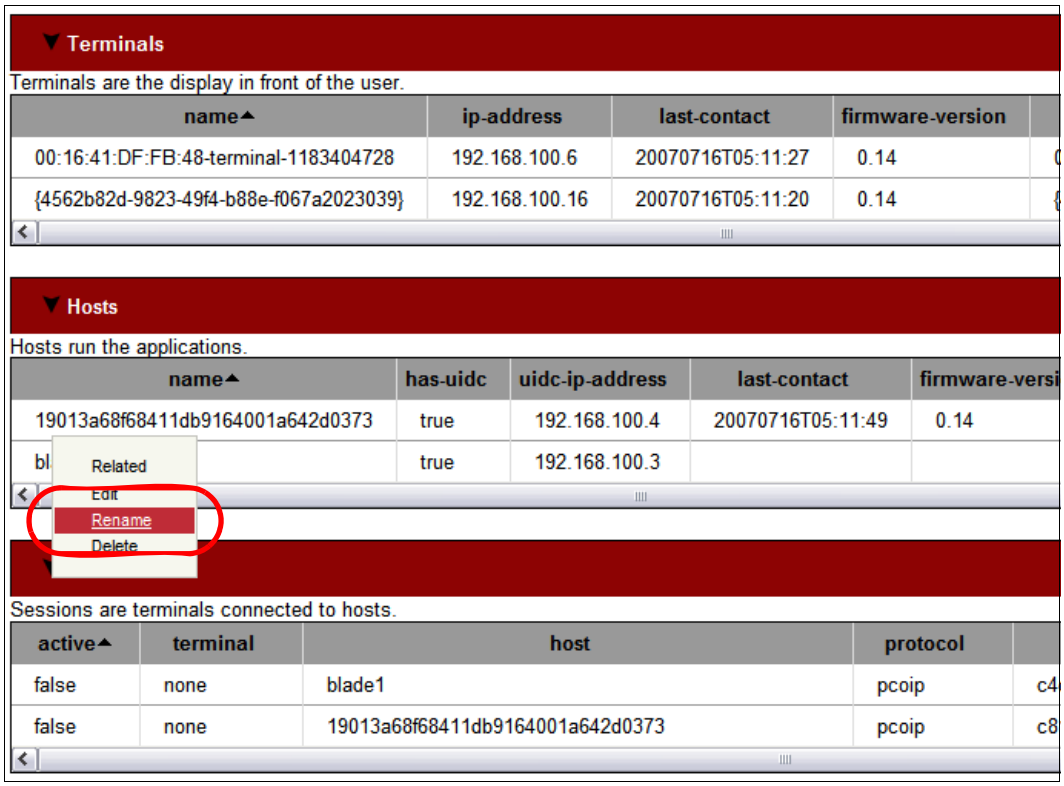


図 5-8　Connection Management でのデバイスの名前変更

2. デバイスに付ける名前を「Name」フィールドに入力し、「**OK**」をクリックします（図 5-9 を参照）。それぞれの HC10 に固有の名前を付ける必要があります。

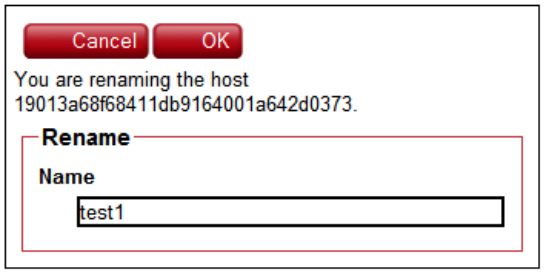


図 5-9　Connection Management でのデバイスの名前変更

3. CP20 上で「**Connect**」をクリックします。ユーザー名を入力するためのプロンプトが出されます。HC10 に割り当てた名前を入力し、「**OK**」をクリックします（図 5-10 を参照）。

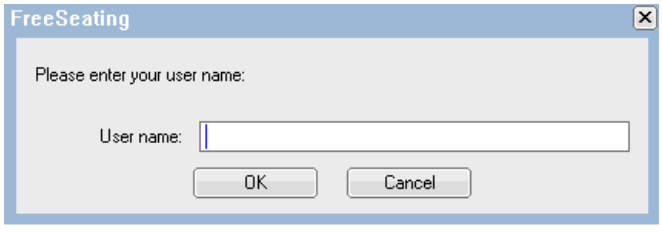


図 5-10　Connection Management を使用したフリー・シーティング接続

4. 入力した HC10 に CP20 が接続します。CP20 に接続されたモニターに、HC10 上で実行されている Windows デスクトップが表示されます。また、コネクション・ブローカーの「Sessions」テーブルに、ホストと端末の間のアクティブ・セッションが表示されます。(ブラウザー・ウィンドウを最新表示するか、セッション・テーブルの右上隅にある最新表示アイコンを押す必要が生じることがあります。)

5.1.2 固定シーティング

固定シーティング接続を確立するには (それぞれの HC10 に、特定の 1 台の CP20 がログインできる)、HC10 (ホスト) と CP20 (端末) を同じ名前に変更する必要があります。例えば、3 台の CP20 と 3 台の HC10 があって、3 台の CP20 には *User1*、*User2*、および *User3* という名前が付いているとします。接続を作成するためには、HC10 にも *User1*、*User2*、および *User3* という名前を付ける必要があります。固定シーティングについての説明は、63 ページの 『固定シーティング』を参照してください。

ヒント : ほとんどのデバイスがフリー・シーティングを使用している場合でも、テスト目的には単一の固定シーティング接続を実装することをお勧めします。

固定シーティング接続をセットアップするには、次の手順で行います。

1. すべての HC10 の名前を変更します (例については、77 ページの 『フリー・シーティング』を参照)。
2. HC10 の名前変更と同様にして、CP20 の名前を HC10 と同じ名前に変更します。
3. 名前を変更した CP20 のいずれかで「**Connect**」をクリックすると、同名の HC10 とのセッションが確立されます。「Sessions」の下に、この手順で構成したホストと端末間のアクティブ・セッションが表示されます。

5.1.3 ファームウェアの更新

Devon IT Connection Management ソフトウェアを使用して、すべてのデバイスのファームウェアを自動的に更新できます。このためには、次の手順で行います。

1. コネクション・ブローカーの Web インターフェースの上部で、「**Admin**」→「**Firmware**」をクリックします (図 5-11 を参照)。ブラウザーのタブまたはウィンドウが新しく開き、使用可能なファームウェア・バージョンが表示されます。

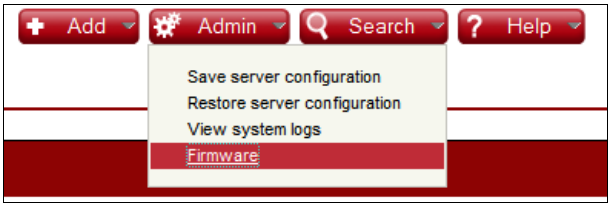


図 5-11　ファームウェアを更新できるページへのアクセス

2. 新規ファームウェア・バージョンを追加するには、「**Add**」→ 「**Firmware**」をクリックします (図 5-12 を参照)。ページの右側に詳細が表示されます。

図 5-12 Connection Management ソフトウェアによるファームウェアの追加

3. 該当する「Name」、「Description」、および「Version」の各フィールドに入力します (図 5-13 を参照)。名前は固有であることが必要で、そうでなければ新しいファームウェアが同名の古いファームウェアを上書きします。

   「Name」と「Version」の両フィールドが必須です。バージョン・フィールドの内容は、適用されるバージョンをユーザーに対して表示する目的で使用されるもので、現在インストール済みのファームウェアと比較する実際のバージョン番号として使用されることはありません。説明フィールドはオプションです。

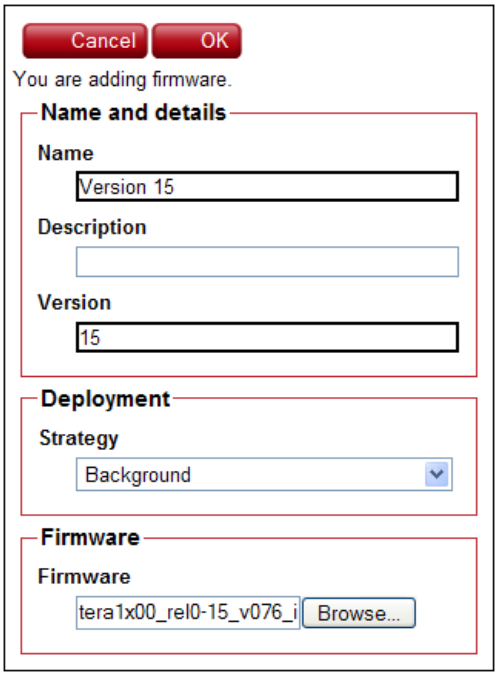


図 5-13 ファームウェアを追加する際の「Name and details」フィールド

4. 次に、デプロイメント方式を決める必要があります。方式として、**即時**または**バックグラウンド**のどちらかを選択します (図 5-14 を参照)。
   - 「**Immediate**」(即時) オプションは、アクティブ接続が存在していても、すべてのデバイスを自動的に更新します。このオプションは、すべての接続を強制的に終了してデバイスを更新します。
   - 「**Background**」(バックグラウンド) オプションは、接続が終了するまで待った後、ファームウェアを適用してデバイスをリセットします。

   これらのオプションについて詳しくは、『4.8, Devon IT Connection Manager』(ページ 66) を参照してください。

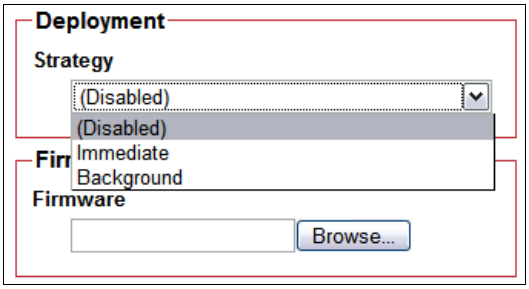


図 5-14　ファームウェア更新のデプロイメント方式の選択

5. 「Firmware」の下にある「**Browse**」をクリックします。次に、アップロードするファイルの位置を指定し (.app ファイルであることが必要)、「**Open**」をクリックします。
6. 「**OK**」をクリックしてアップロード処理を開始します。
7. ファームウェアはブローカーにアップロードされ、使用可能なファームウェア更新のリストに表示されます (図 5-15 を参照)。

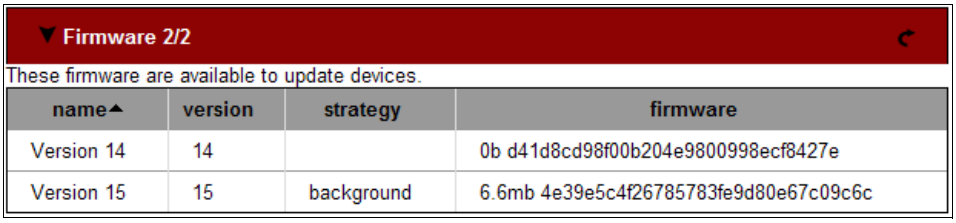


図 5-15　更新された使用可能ファームウェアのリスト

図 5-15 から、ファームウェアの 2 つのバージョンがアップロードされたことが分かります。バージョン 15 がアップロードされたとき、以前にアップロードされていたファームウェア (バージョン 14) のデプロイメント方式は自動的に使用不可に設定され、単にブランクとして表示されます。これは、一度にアクティブにすることができるファームウェアがただ 1 つであるからです。

8. これで、ファームウェアを HC10 圧縮カードと CP20 に適用する準備ができました。更新方式としてバックグラウンドを選択したので、ブローカーはデバイスを更新する前に、デバイスがセッションを終了するまで待ちます。*即時* を選択した場合は、更新処理が即時に開始され、必要な場合はセッションが強制終了されます。

リストからファームウェアを選択すると、図 5-16 に示すように、更新に関連したログが右側ペインに表示されます。

図 5-16　更新されたデバイスを示すファームウェア・ログ

ヒント：「Search」をクリックすると、ログ・メッセージをブラウザー・ウィンドウ全体に表示できます。また、**「Download」**をクリックして、ログ・メッセージをテキスト・ファイルに保存することもできます。

デバイスがファームウェア更新をコネクション・ブローカーからダウンロードすると、ログ項目が作成されます。デバイスへのダウンロードが完了すると、ログに別のメッセージが示されます。例 5-1 は、更新中の 2 つのデバイスから出されたメッセージを示しています。

ヒント：Web インターフェースに示されるログのメッセージ (図 5-16) は、最新のメッセージを先頭にして表示されます。

例 5-1　ファームウェア更新に関してブローカーに記録されたメッセージ

```
cms sent startFirmwareDownload to the device since the device's firmware version
is outdated.Device's current firmware version is:0.14 while the latest firmware
version is: 15

eventDownloadStatus message.Download status:Firmware download done successfully.
```

```
cms sent startFirmwareDownload to the device since the device's firmware version
is outdated.Device's current firmware version is:0.14 while the latest firmware
version is: 15

eventDownloadStatus message.Download status:Firmware download done successfully.
```

Web インターフェースのメインページでは、図 5-17 に示すように、それぞれのデバイスに存在するファームウェアのバージョンを確認できます。

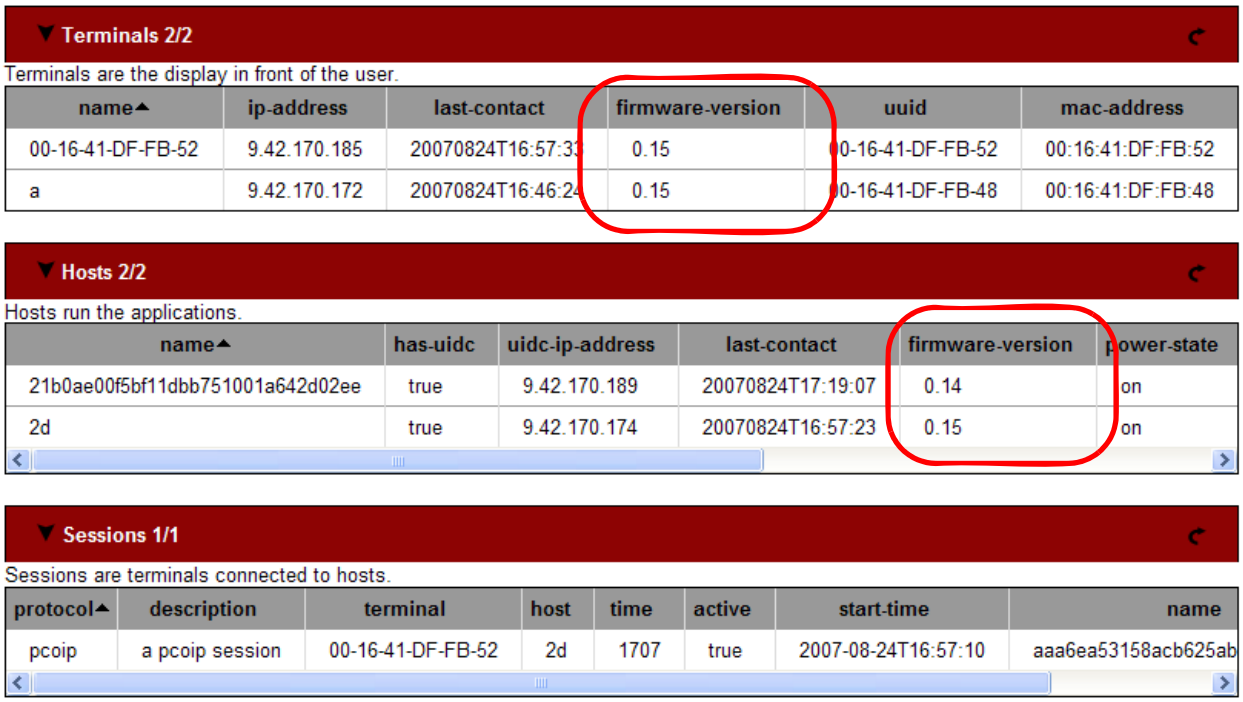


図 5-17　それぞれのデバイスのファームウェア・バージョンを示す、ブローカー・インターフェースのフロントページ

多数のデバイスがある場合は、これらすべてのスキャンを行って、最新のファームウェアが適用されていないデバイスを調べることは困難です。解決策として、検索フィルター機能を使用して、特定のバージョン (この例では 0.15) を使用していないデバイスをすべて表示できます。使用する構文は次のとおりです。

```
-firmware-version:0.15
```

検索フィールドにこの構文を入力すると、図 5-18 に示すように、バージョン 0.15 がインストールされていないデバイスのみが表示されます。

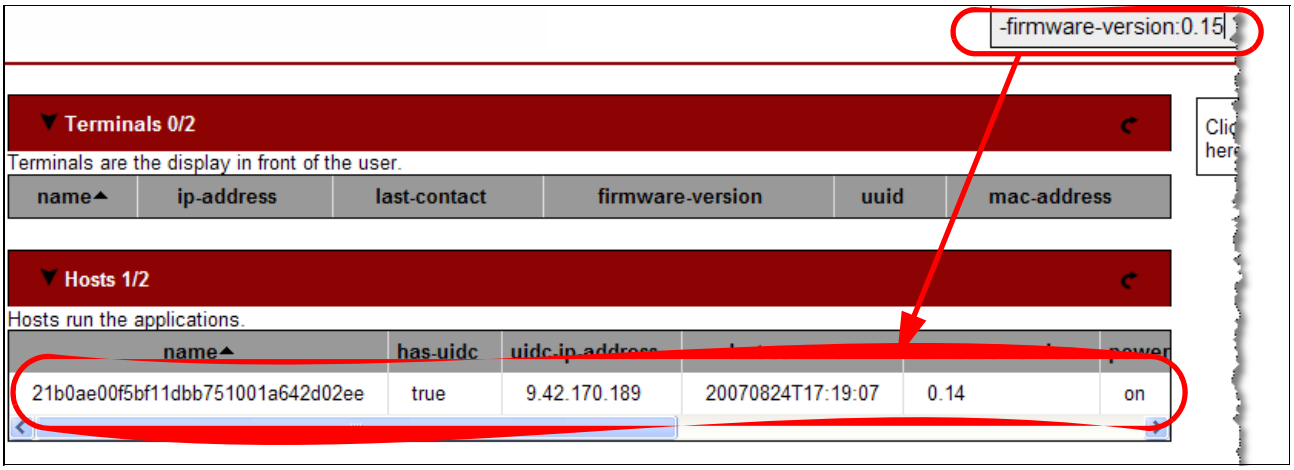


図 5-18　0.15 が適用されていないデバイスのみの表示

検索フィルターの構文について詳しくは、『5.1.4, 検索フィルター機能』(ページ 85) を参照してください。

ファームウェア更新の特性

ファームウェア更新に関する重要な点として、次のことに注意してください。

- アップロード対象として指定したファイルに対して、検査は行われません。選択したファイルが実際に有効なファームウェア・ファイルかどうかは検査されません。
- 一度にアップロードできるファームウェア・ファイルは 1 つですが、必要ならば追加のファームウェア・ファイルをアップロードできます。ただし、アクティブになるファイルはただ 1 つです (つまり、*バックグラウンド*または*即時*のどちらか)。その他のファイルにはすべて、自動的に*使用不可*のマークが付けられます。前にアップロードしたファームウェア・ファイルを編集して、方式やその他のフィールドを変更できます。使用不可のファイルをアクティブ方式に変更すると、既存のアクティブ・ファイルは非アクティブに設定されます。
- 既に存在するファームウェア名を使用すると、そのファイルは警告なく上書きされます。
- バージョン番号フィールドは必須です。これは、更新中に表示されるメッセージの中で、適用されているバージョンを示すために使用されます。ブローカーは、ファームウェアの実際のバージョン番号を判別するためにはこの値を使用しません。代わりに、アップロードしたファイルからこの情報を直接読み取ります。
- ブローカーは、現在インストール済みのファームウェアのバージョンを、アップロードしたファイルから読み取ったバージョンと比較して、特定のデバイスにファームウェアを適用するかどうかを決定します。これらの値が異なる場合、ブローカーはファームウェアの適用を試みます。この方式は、ファームウェアのアップグレードにもダウングレードにも当てはまります。
- *即時*方式を選択すると、更新はデバイスの小さなグループ単位で直ちに開始されます。デバイスが更新される時点で接続されているユーザーがいる場合は、即時に切断されます。
- *バックグラウンド*を選択した場合、ブローカーはデバイスをファームウェア更新対象と見なす前に、セッションの終了を待ちます。ユーザーがセッションを切断しなければ、CP20 と HC10 は一切更新されません。管理者は「Firmware Version」フィールドを監視し

てデバイスの状況を確認し、必要に応じて方式を*即時*に変更して更新を強制する必要があります。フィルター `-firmware-version:x.xx` を使用すると、特定のファームウェア・バージョンを使用していないデバイスをすべて表示できます。

5.1.4 検索フィルター機能

Devon IT Connection Broker には検索フィルター・オプションがあり、HC10、CP20、およびセッションのサブセットを表示できます。多数のデバイスがある大規模なインストール環境では、表示したいデバイスを見つけづらい場合があります。検索機能を使用すれば、検索フィールドにテキストを入力することにより、結果をフィルターに掛けることができます。テキストを入力するにつれて、表示されるデバイスはそのテキストに一致するもののみに絞り込まれます。

高度な検索オプションもあります。その他の検索方法には次のものがあります。

- *引用符*: スペースを含む項目は二重引用符 (“ “) で囲むことができます。また、各種文字のエスケープのためにバックスラッシュを使用できます。例を次に示します。

  ```
  "Lab Blade"
  ```

- *属性*: 突き合わせを特定の属性に限定するには、属性名 (列名) の接頭部の後にコロン (:) を付けて使用します。例えば、次の検索オプションを使用すると、IBM を製造メーカーとする項目をすべて検索できます。

  ```
  manufacturer:ibm
  ```

  すべての項目にタイプがあります。例えば、結果をホストのみに限定するには、次の検索を使用できます。

  ```
  type:host
  ```

  属性名とコロンのみを入力した場合は、そのフィールドを持つ項目と、その項目の値のみが表示されます。例えば、次の検索オプションを入力すると、IP アドレスをもつ項目がすべて表示されます。

  ```
  ip-address:
  ```

- *完全一致突き合わせ*: 通常は、検索ストリングを含むテーブル項目が検索結果に表示されます。例えば、*lab* を検索すると、*laboratory* と *collaborate* が一致します。完全一致突き合わせを使用したい場合は、入力する単語の前に正符号 (+) を入力します。例えば、次の検索オプションを指定すると、*lab* に完全に一致する結果のみが表示されます。

  ```
  +lab
  ```

  完全一致突き合わせは、大 / 小文字の区別もします。(通常、突き合わせは大 / 小文字を区別しません。) 特定の属性に対する完全一致突き合わせを指定するには、次のように属性の前に正符号 (+) を付けます。

  ```
  +name:lab
  ```

  用語を引用符で囲む必要がある場合は、検索ストリング全体を二重引用符で囲みます。

  ```
  "+name:lab 20"
  ```

- *否定*: 項目を除外するには、負符号 (-) を使用します。例えば、*John* に関連した項目をすべて除外するには、次の検索オプションを使用します。

  ```
  -john
  ```

  同様に、この構文を使用して、特定のファームウェアを使用していないデバイスをすべて表示できます。例えば、バージョン 0.15 がインストールされていないデバイスを表示するには、次の検索フィルターを使用します。

  ```
  -firmware-version:0.15
  ```

- *論理和*: 複数の単語を入力した場合、突き合わせ結果に現れる項目にはこれらの単語がすべて含まれている必要があります (考え方としては、それぞれの単語の間に AND が指定された場合と同様)。OR (大文字で入力する必要があります) を使用すると、入力した単語の少なくとも 1 つに一致する項目が結果に現れるように指定できます。例えば、次の検索オプションを入力すると、*john* または *jane* のどちらかを含む項目が検索されます。

  ```
  john OR jane
  ```

- *グループ化と複雑な照会*: 語句を丸括弧 (小括弧) で囲むと、単語をグループ化して複雑な照会を行うことができます。例を次に示します。

  ```
  (a b) OR -(c d) OR e
  ```

  表 5-1 に、グループ化の例をいくつか示します。

表 5-1 検索フィルターの例

例	意味
-description:	説明のない項目が返されます。
john OR lab	john または lab を含む項目が返されます。
(john OR jane OR tim) lab	lab を含み、john、jane、または tim のうち少なくとも 1 つを含む項目が返されます。
-(john OR jane OR tim) lab	lab を含み、john、jane、または tim のどれも含まない項目が返されます。

5.1.5 セッション切断時のセキュリティー・ロック

Devon IT Connection Broker は、パスワードを要求するプロンプトを出してユーザーを認証することはしません。代わりに、HC10 上で実行されている Windows オペレーティング・システムに依存して、権限のあるユーザーのみがログオンできるようにしています。

ユーザーが最初に HC10 に接続すると、そのユーザーには Windows からプロンプトが出され、ユーザー ID とパスワードの入力を求められます。これは、パスワードがオペレーティング・システム内で設定済みであることを前提としています。(Windows XP および Vista のどちらでも、ユーザーにパスワードを要求せずに Windows を開始できますが、ユーザー ID とパスワードを要求するようにこのオプションを変更することをお勧めします。)

単に接続が切断されるか、またはユーザーが CP20 の**セッション切断**ボタン (38 ページの図 3-7 を参照) を押すことによってセッションが終了したときに、セキュリティーを保つためには、Windows をセキュアな状態にする必要があります。Devon IT Connection Broker は、「ソフト電源オフ」コマンドのエミュレートによって Windows をセキュアな状態にします。これは、通常の PC の電源オフ・ボタンを 4 秒より短く押すことと同等な機能です。この目的は、HC10 をスタンバイ・モードにすることです。

デフォルトでは、Windows XP はソフト電源オフ・イベントへの対応としてシャットダウンを開始します。セッションの切断時に HC10 をセキュアな状態に保つために、オペレーティング・システムがシャットダウンでなくスタンバイを実行するように Windows XP を再構成することをお勧めします。この変更を行うには、HC10 で次の手順を実行します。

1. コントロール・パネルを開き、「電源オプション」アプレットを起動します。
2. 「詳細」タブをクリックします。図 5-19 に示すような「電源オプションのプロパティ」ウィンドウが開きます。

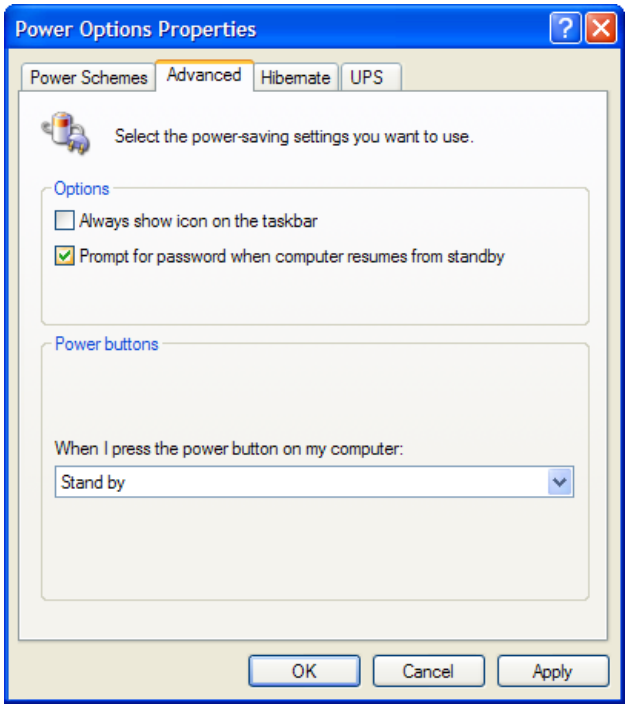


図 5-19　Windows XP の電源オプション

3. 「スタンバイから回復するときにパスワードの入力を求める」オプションが選択されていることを確認します。
4. 「電源ボタン」の下にある「コンピュータの電源ボタンを押したとき」オプションに対して、**「スタンバイ」**を選択します。(デフォルトは「シャットダウン」です。)
5. **「OK」**をクリックします。

これで、ユーザーがセッションを切断したとき、または CP20 セッションが失われたときに、HC10 が自動的にスタンバイ・モードになります。

ヒント : セッションの切断時にシステムの実行を継続したい場合は、図 5-19 の電源ボタンの設定を**「何もしない」**に変更する必要があります。こうすると、HC10 へのログインが維持され、CP20 にアクセスできるすべてのユーザーが HC10 にアクセスできるので、機密漏れが発生する可能性があります。

スクリーン・セーバー・オプションを構成して (コントロール・パネルの「画面」アプレットの「スクリーン セーバー」タブ)、例えば 5 分か 10 分後に自動的に開始するように設定し、**「パスワードによる保護」**を選択することをお勧めします。

5.2 Leostream Hosted Desktop ソフトウェア

『4.9, Leostream Hosted Desktop Connection Broker』(ページ 68) で説明したとおり、Leostream Hosted Desktop ソフトウェアを使用すると、Microsoft Active Directory などの LDAP サーバーの認証およびポリシー管理によって、HC10-CP20 接続の集中管理が可能です。ここでは、

CP20 から HC10 への認証接続を可能にするために Leostream ソフトウェアを構成する方法を説明します。Leostream ソフトウェアをインストールする方法については、「*Leostream Hosted Client User's Guide*」を参照してください。Leostream ソフトウェアは VMware 仮想計算機内で実行されます。

ソフトウェアを実行すると、図 5-20 のようなパネルが表示され、Web ベース管理者インターフェースの IP アドレスが示されます。この Web インターフェースを使用して、すべての管理機能を実行できます。

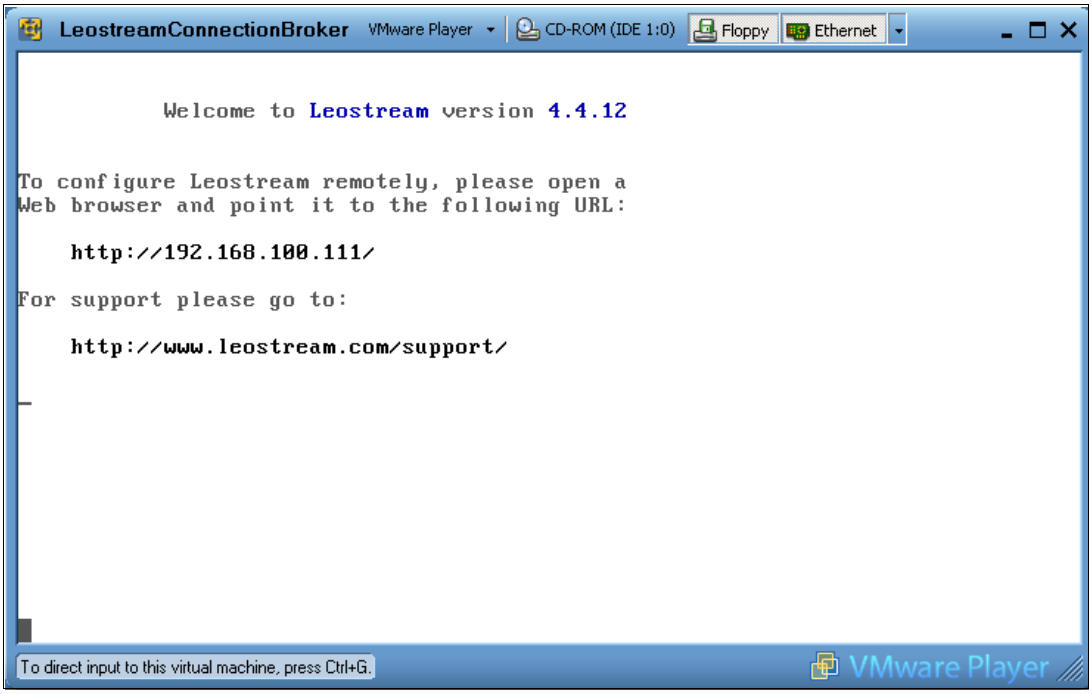


図 5-20　仮想計算機の IP アドレスの取得

Web インターフェースにログインするには、次の資格情報を使用します。

- ユーザー名 : *admin*
- パスワード : *leo*

その後、ライセンス・キーを入力し、ライセンス条項を受諾する必要があります。図 5-21 に示すように、Web ブラウザーを使用して管理インターフェースにアクセスします。

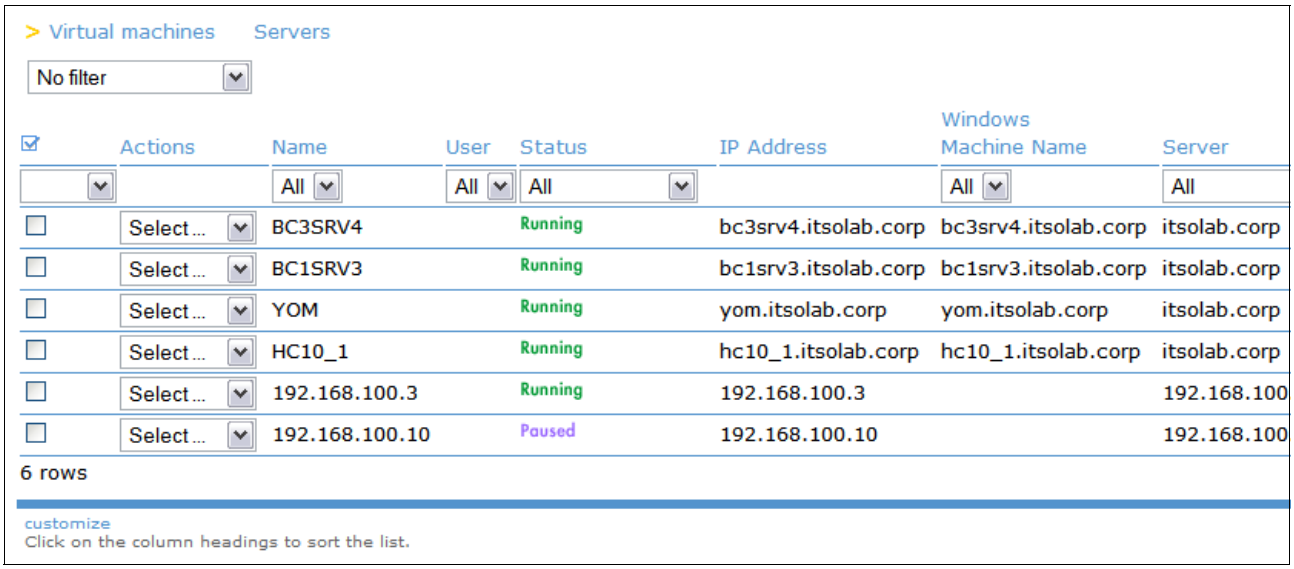


図 5-21　Leostream Connection Broker メインパネル

出荷時の構成では、HC10 と CP20 はホスト名 *ws-broker* のコネクション・ブローカーを使用します。Leostream ブローカーはデフォルトでこのように構成されているので、これ以外の構成は必要とせずにデバイスからコネクション・ブローカーへの接続を確立できます。

Leostream Hosted Desktop のユーザーは、特定の HC10 のグループに含まれる HC10 に接続することも (*プーリング*)、HC10 を固定して割り当てることもできます。このソフトウェアでは、ユーザーには特定のポリシーが割り当てられます。これらのポリシーには固有のタグが組み込まれています。それぞれの HC10 に、これら固有のタグのいずれかを割り当てることができます。つまり、タグ属性はユーザーが接続できるマシンを定義します。

接続をセットアップする前に、デバイスを検出する必要があります。このためには、次の手順で行います。

1. Hosted Desktop Web インターフェースにログインし、**「System」→「General Configuration」**を選択します。
2. 次のオプションを選択します (図 5-22 を参照)。
   - Use the Hosted Desktop configuration
   - Use Hosted Desktop agents
   - Enable SLP discovery and blade API

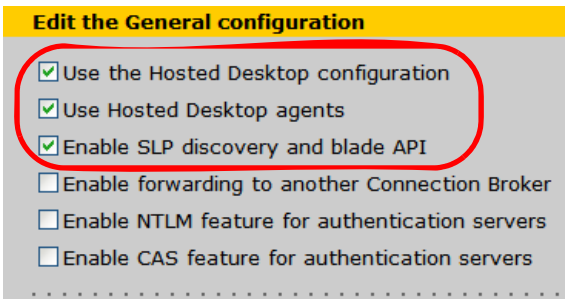


図 5-22　SLP 検出とブレード API を使用可能にする

また、次のオプションを必ず選択してください。

- Enable PCoIP support
- Enable USB passthrough control

3. 「Other」にスクロールダウンし、「**Allow URL access to the logs**」を選択します。
4. その他の設定値はすべてデフォルトのままにし、パネルの一番下にある「**Save**」をクリックします (図 5-23 を参照)。

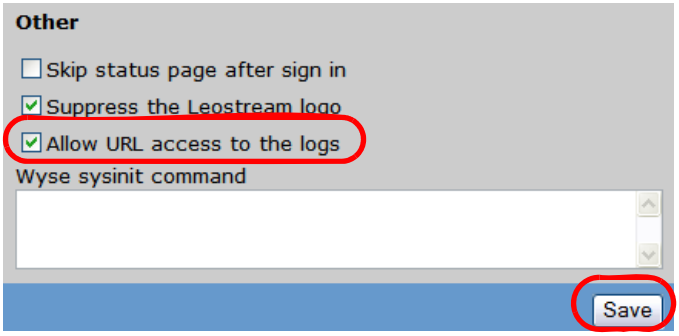


図 5-23　ログへの URL アクセスの許可

5. Hosted Desktop ソフトウェアをリブートします。

5.2.1 センターの追加

ここで重要な作業として、次の手順で PCoIP Devices を修正する必要があります。

1. 「**Machines**」→「**Centers**」→「**PCoIP Devices**」→「**Edit**」をクリックします。
2. Type は PCoIP Devices 固定です。Name と Discovery Interval (SLP) と Connection Broker の IP アドレスを確認し、「**Save**」をクリックします。

5.2.2 タグの作成

タグはマシンの属性として使用されます。次の手順で、マシンにタグを付けたり、特定のタグ・グループを指定したりすることができます。

1. 「**Users**」→ 「**Tags**」→ 「**Settings**」をクリックして、タグ・グループを作成します。
2. タグ・グループの名前を任意の名前 (例えば Language、Location など) に変更します。これらのタグ・グループは、類似したタグをまとめて編成するために使用されます (例えば、スペイン語のタグ、英語のタグ、およびフランス語のタグを、すべて *Language* (言語) タグ・グループに入れる)。
3. 「**Users**」→ 「**Tags**」→「**Create**」をクリックします。「Create a tag」ダイアログ・ボックスで、タグの名前を作成し、「Name」フィールドに入力します (図 5-24)。
4. 「タグ」グループのドロップダウン・リストからタグ・グループを選択することにより、タグの属するタグ・グループを選択します。
5. 「Auto-tag」フィールドを使用して、このタグをマシンに自動的に適用できます。まず、「**Starts with**」、「**Contains**」、または「**Ends with**」をドロップダウン・リストから選択します。その後、「Text to match」フィールドに適切なテキストを入力します。インポートした HC10 の名前がこの自動タグに一致すると、HC10 にはこのタグが付けられます。この例では、*192* で始まる名前 (IP アドレス) を持つ HC10 にタグ *Tag_test* が付けられるように、自動タグを設定しました。

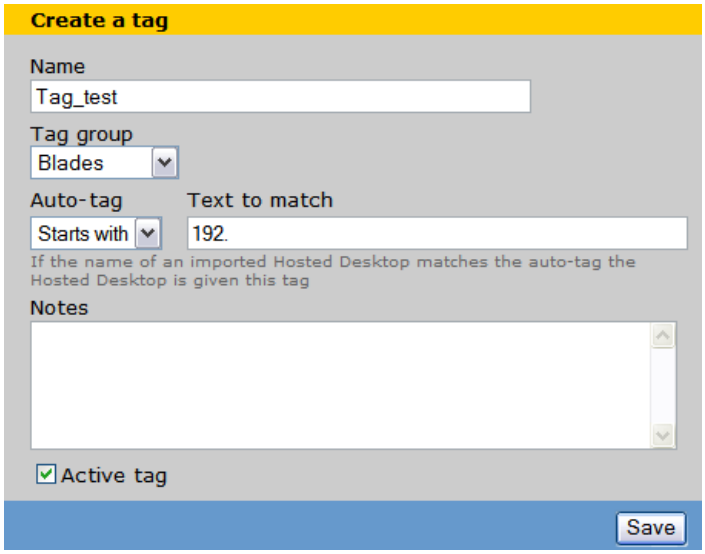


図 5-24　Leostream Hosted Desktop ソフトウェアを使用したタグの作成

6. 「Active tab」オプションは選択された状態のまま、**「Save」**をクリックします。

5.2.3 ポリシーの作成

ポリシーはユーザーによって使用され、ユーザーが接続できるマシンを決定します。ポリシーの中で適切なタグを選択することによって、プールに所属させる HC10 をいくつか選択して定義できます。次の手順で行います。

1. **「Users」→「Policies」→「Create」**をクリックします。「Create a policy」ダイアログ・ボックスの「Name」フィールドに、ポリシーの名前を入力します。
2. HC10 のプールを定義するには、「Available tags」の下にある作成済みのタグをクリックし、**「Add highlighted items」**をクリックします (図 5-25)。

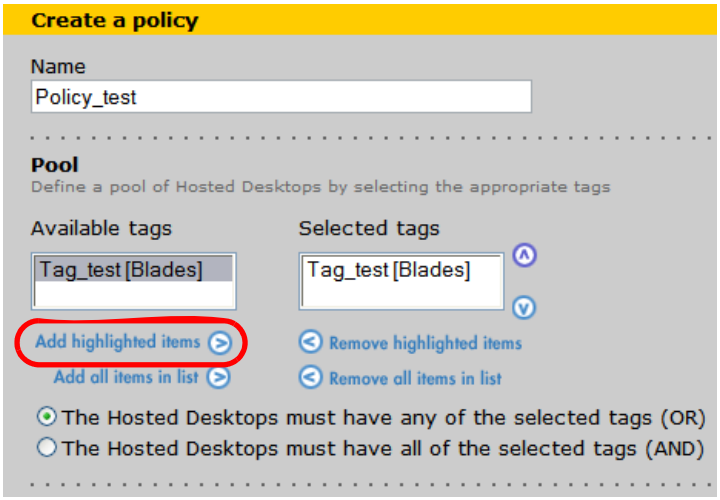


図 5-25　Leostream の Hosted Desktop ソフトウェアによるポリシーへのタグの追加

3. その他の設定値はすべてデフォルトのままにし、**「Save」**をクリックします。

5.2.4 ロールの作成

ロールは、ユーザーが実行できる操作を定義します。ロールを新しく作成するには、次の手順で行います。

注 : ロールは自動的に作成されるので、この手順を行うことは必須ではありません。

1. 「**Users**」→ 「**Roles**」→ 「**Create**」をクリックします。「Create a role」ダイアログ・ボックスの「Name」フィールドに、ロールの名前を入力します。
2. 「Permissions」の下で、このロールに設定する許可を選択します (図 5-26)。

注 : 管理者ロールはすべての機能に対して完全なアクセス権限を持っています。

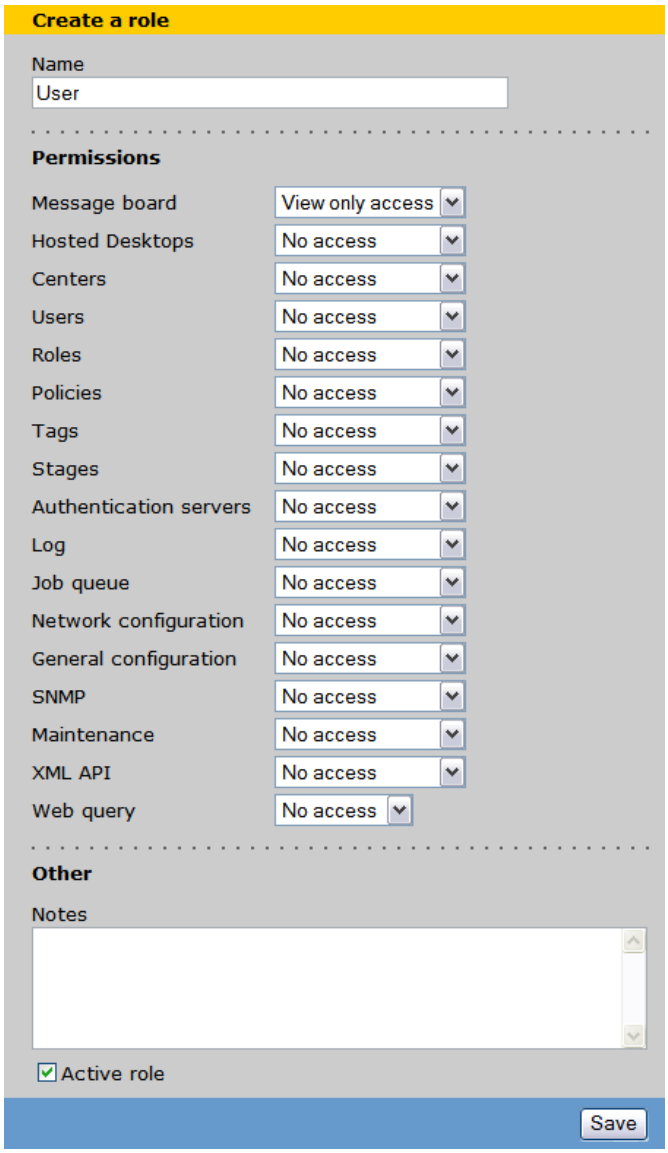


図 5-26 Leostream の Hosted Desktop ソフトウェアによるロールの作成

3. 「**Save**」をクリックします。

5.2.5 ユーザーの作成

注 : ユーザー・アカウントに対して外部認証サーバーを使用している場合は、コネクション・ブローカー内でユーザーを作成する必要はありません。このセクションは飛ばして構いません。

特定のポリシーを使用し、ログイン名とパスワードを指定して、ユーザーを作成できます。次の手順で行います。

1. **「Users」→ 「Users」→ 「Create」**をクリックします。「Create a user」ダイアログ・ボックスに、ユーザーの名前を入力します (図 5-27 を参照)。

   注 : この名前は、単なるユーザーの名前です。ログイン名ではありません。

2. 「Role」 ドロップダウン・リストから、ユーザーに指定するロールを選択します。
3. 作成済みのポリシーを「Policy」 ドロップダウン・リストから選択します。基本的には、ユーザーにこのポリシーが割り当てられると、ポリシーに含まれるタグを使用して、同じタグを持つマシンからの選択が行われるようになります。
4. ユーザーがログインに使用する名前とパスワードを入力します。

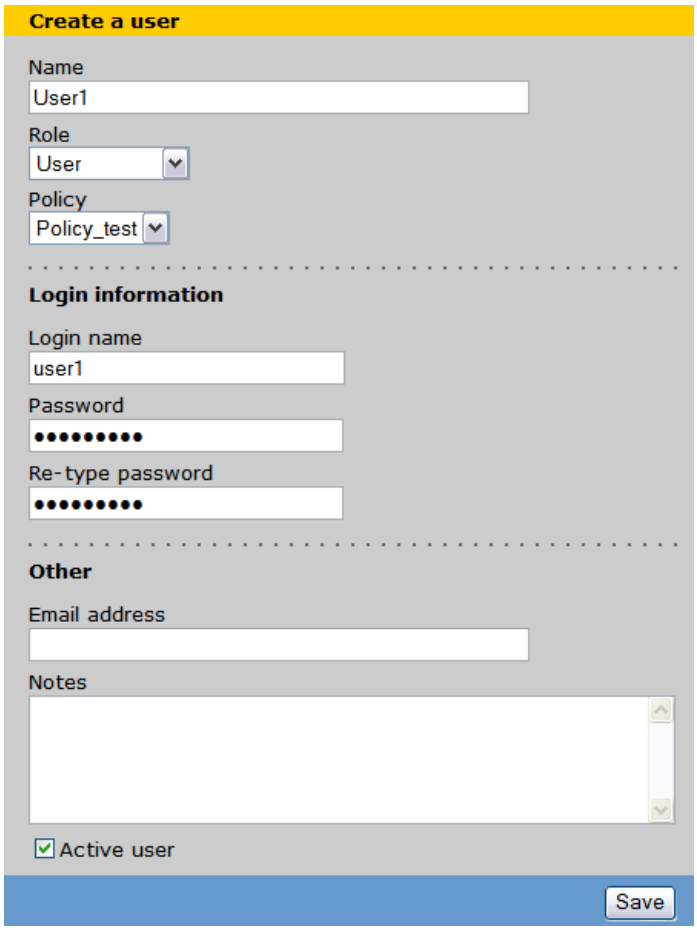


図 5-27 Leostream の Hosted Desktop ソフトウェアによるユーザーの作成

5. **「Save」**をクリックします。

5.2.6 HC10 の割り当て

ここで、ユーザーに HC10 を割り当てます。次の手順で行います。

1. 「**Machines**」→「**Hosted Desktops**」をクリックします。
2. 「Actions」列の下で、構成したい HC10 のドロップダウン・リストから「**Edit**」を選択します (図 5-28 を参照)。

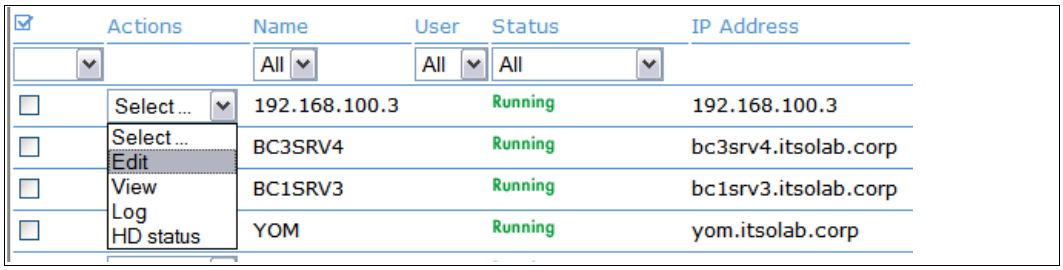


図 5-28 Hosted Desktop ソフトウェアの「Machines」メニューから行う HC10 の編集

3. ユーザーが接続できる HC10 を決定するためにポリシーを使用する場合は、「User Assignment Mode」ドロップダウン・リストから「**Policy-driven**」を選択します。その後、「Tag Editing」の下のドロップダウン・リストから、使用するポリシーを選択します (図 5-29)。

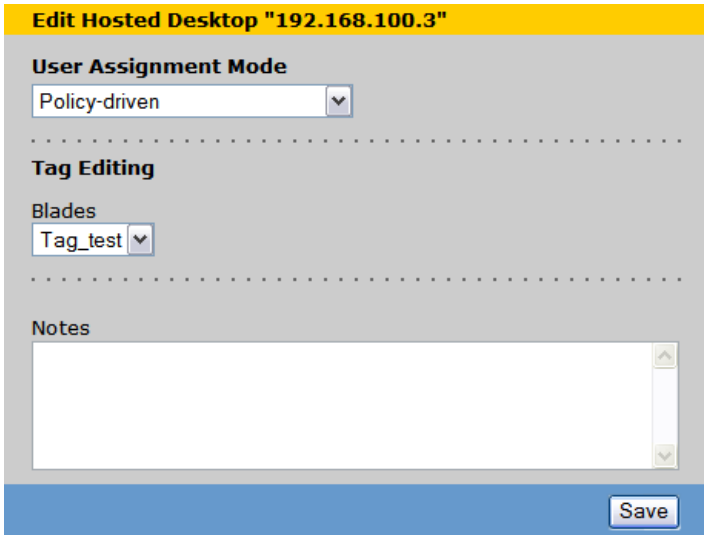


図 5-29 HC10 へのユーザーの接続にポリシー方式のユーザー割り当てモードを使用

4. 特定の HC10 に接続できるようにユーザーをハードコーディングする場合は、「**Hard-assigned to a specific user**」を選択します。「Assigned User」ドロップダウン・リストから、この特定の HC10 に接続できるようにするユーザーを選択します (図 5-30)。

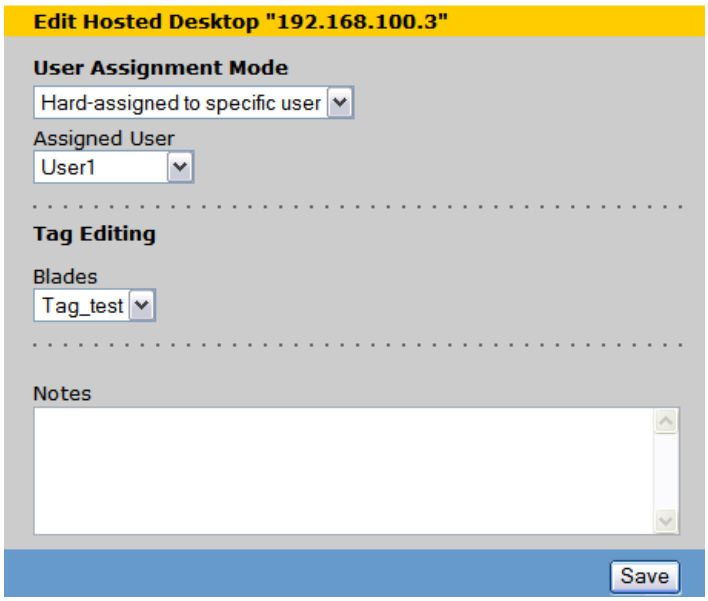


図 5-30　Hosted Desktop ソフトウェアによる HC10 へのユーザーのハード割り当て

5. また、「User Assignment Mode」ドロップダウン・リストから「**Unavailable for assignment**」を選択して、HC10 を割り当て不可にすることも選択できます (図 5-31)。

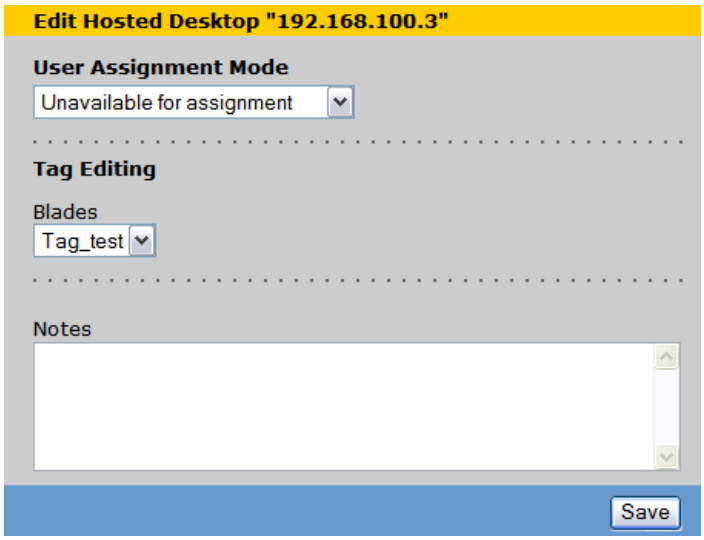


図 5-31　Hosted Desktop ソフトウェア内で HC10 を割り当て不可にする

6. 「**Save**」をクリックします。

5.2.7 CP20 から HC10 への接続

前述の手順を完了したら、Leostream の Hosted Desktop ソフトウェアを使用して、CP20 から HC10 に接続する準備ができます。接続するには次の手順で行います。

1. CP20 側で「**Connect**」をクリックします。ユーザー名とパスワードを入力するためのプロンプトが出されます。前に説明した、Hosted Desktop ソフトウェアで作成したユーザー・ログイン情報を入力します (図 5-32 を参照)。「**OK**」をクリックします。

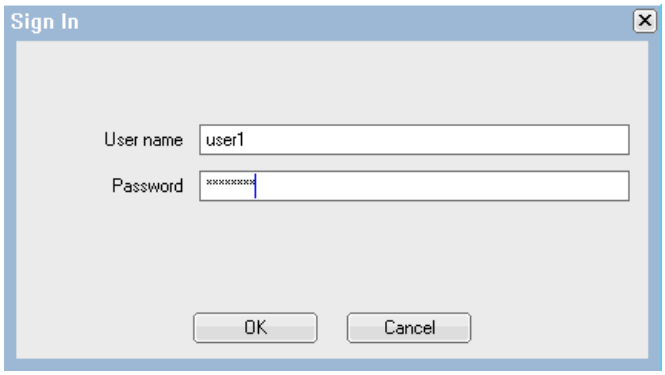


図 5-32 Hosted Desktop ソフトウェア使用時に CP20 のローカル・インターフェースに表示されるログイン・ダイアログ・ボックス

2. 接続可能な HC10 のリストが表示されます (ただし、1 つしかない場合はリストは表示されず、自動的に接続されます)。接続したい HC10 をクリックして、「**OK**」をクリックします。図 5-33 を参照してください。

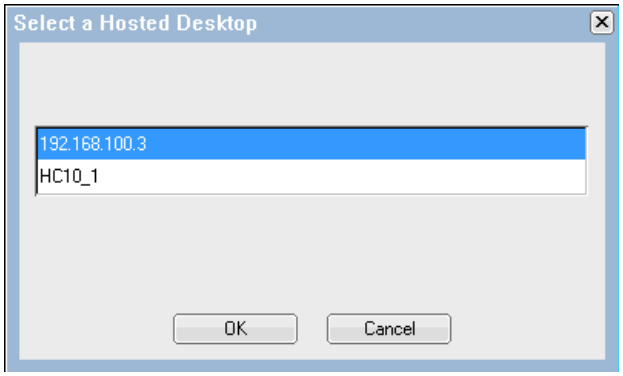


図 5-33 リストから使用可能な HC10 を選択

3. これで、HC10 に正常に接続しました (図 5-34 を参照)。

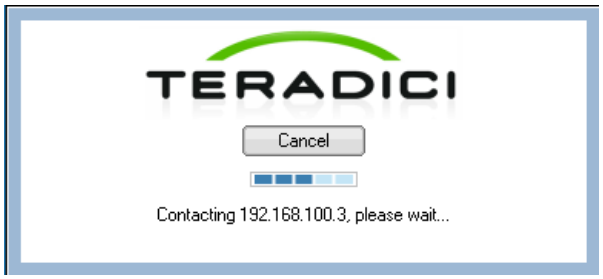


図 5-34 CP20 が HC10 に接続していることを示すメッセージ

5.2.8 認証サーバーの作成

Leostream Hosted Desktop と組み合わせて Active Directory を使用できます。これは、コネクション・ブローカー・ソフトウェアにユーザーをロードするために便利です。Active Directory などの認証サーバーを追加するには、次の手順で行います。

1. 「**Users**」→「**Authentication Servers**」→「**Create**」をクリックします。
2. フォームに入力します。具体的には、ご使用の Active Directory のタイプ、名前、および LDAP 設定を入力します (図 5-35 を参照)。

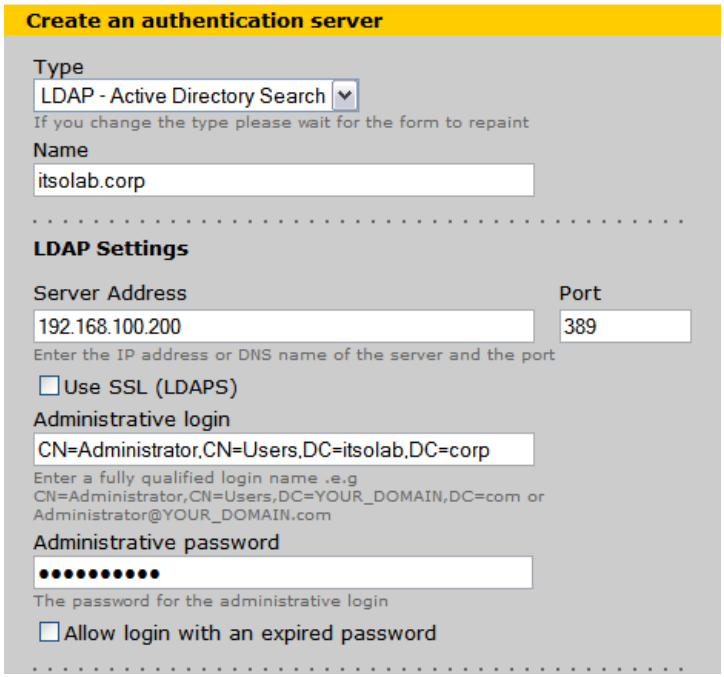


図 5-35　認証サーバーを追加するための初期設定

3. 「User Assignments」の下で、ロード時にユーザーにポリシーを自動的に割り当てる規則を指定します。図 5-36 に示すように、「Active Directory Sub-tree」と「Attribute to search」に入力します。

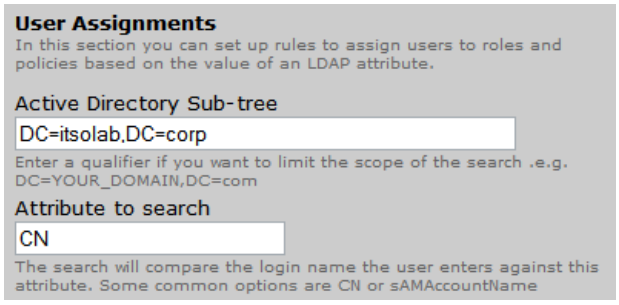


図 5-36　認証サーバーを追加する際のユーザー割り当て設定

4. 特定のポリシーに割り当てる属性および属性値を決定します。完了した後、ドロップダウン・リストを使用して、作成したポリシーを選択します (図 5-37 を参照)。複数の属性値に対して、この作業を同時に実行できます。

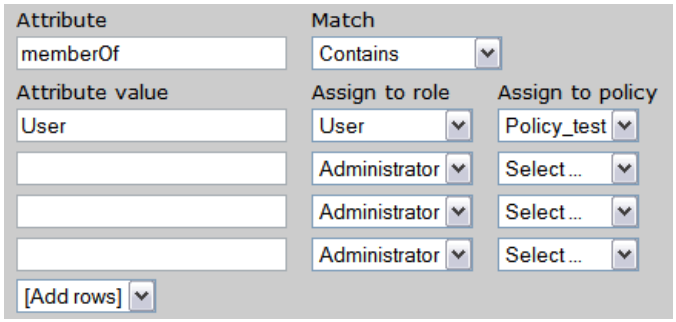


図 5-37　ユーザーへのポリシーの自動割り当て

5. また、ユーザーが従来の設定値のどれにも一致しない場合のために、デフォルト・ロールとデフォルト・ポリシーをセットアップすることもできます。すべてのユーザーをデフォルトのロールとポリシーに設定することもできます (図 5-38 を参照)。

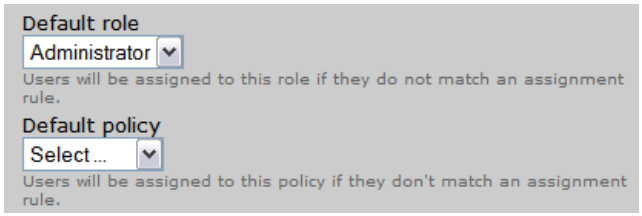


図 5-38　デフォルト・ロールとデフォルト・ポリシーの設定

6. 「**Save**」をクリックします。認証サーバーが正常に追加されました。

認証サーバーからのユーザーの認証をテストすることもできます。次の手順で行います。

1. 「**User**」→「**Authentication Servers**」をクリックします。
2. 「Actions」列のドロップダウン・リストから「**Test**」を選択します (図 5-39 を参照)。

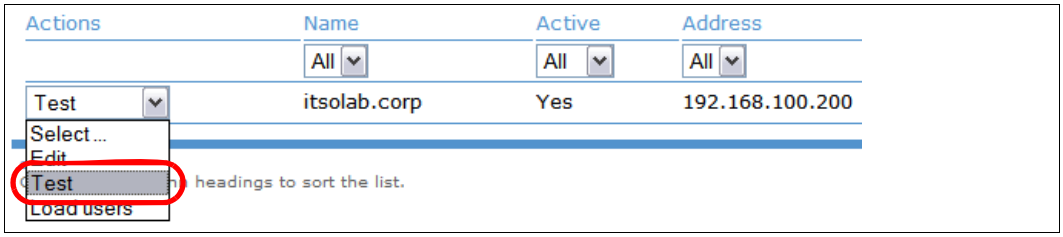


図 5-39　認証サーバーからのユーザーのテスト

3. 表示されるメニューに、ユーザー名とパスワードを入力して、「**Authenticate**」をクリックします。

5.3 セキュリティー

HC10 と CP20 の重要な機能は、重要なデータを保護する能力です。それぞれの HC10 と CP20 は、両デバイスの Web インターフェース上でも、CP20 のローカル・インターフェース上でも、パスワードによって保護されています。デフォルト・パスワードは PASSW0RD（英文字の *O* ではなくゼロを含む）に設定されており、このデフォルト・パスワードを固有のパスワードに変更することを強くお勧めします。パスワードの変更方法について詳しくは、『6.3.1, パスワードの変更』(ページ 107) を参照してください。この保護の強化により、ユーザーは構成オプションを変更できなくなります。

また、CP20 と HC10 に取り付けて使用することを許可する USB デバイスを設定することもできます。例えば、USB サム・ドライブを使用不可に設定できます。いつでも、何者かがマシンにサム・ドライブを挿入して、極秘のデータを数分で取り出してしまう恐れがあります。そこで、サム・ドライブの使用を不許可にする機能を利用すれば、このセキュリティー脅威は問題にならなくなります。そのほかにも、要件に応じてさまざまなオプションがあります。管理者は、キーボードとマウス (ヒューマン・インターフェース・デバイス) のみが動作するように環境をセットアップできます。また、プリンターやイメージ処理などを許可することもできます。USB デバイスへのアクセスの構成について詳しくは、136 ページの『USB』を参照してください。

6

構成オプション

ほとんどのお客様は、コネクション・ブローカーを使用して CP20 と HC10 の間の接続を管理します。したがって、HC10 ソリューションは次のようにあらかじめ構成済みです。

- IP アドレスは DHCP によって割り当てられます。
- HC10 と CP20 の両方で接続管理が使用可能に設定されています。
- 両方のデバイス・タイプが、ホスト名 *ws-broker* のブローカーに接続するように構成されています。

コネクション・ブローカーを使用しない場合は、ピアツーピア接続を使用できます。この章では、ピアツーピア接続の使用法について説明します。

また、追加の構成手順を行う必要が生じることもあります。この章では、HC10 と CP20 が提供する次のようなインターフェースについて説明します。

- CP20 ローカル・ファームウェア・ベース・インターフェース
- CP20 Web ブラウザー・インターフェース
- HC10 Web ブラウザー・インターフェース

これらの構成オプションそれぞれについて説明し、さらにこれらのインターフェースを使用したファームウェア更新についても解説します (『5.1.3, ファームウェアの更新』(ページ 79) で説明した Devon IT Connection Broker の使用に代わる方法)。

この章で説明するトピックは、次のとおりです。

注 : この章の図と本文は、CP20 および HC10 圧縮カード・ファームウェアのバージョン 17 に基づいています。

6.1 固定 IP アドレスの構成

HC10 と CP20 のデフォルト構成では、DHCP を使用します。ただし、DHCP を使用できない場合、または固定アドレスを使用する必要がある場合は、ブレード・ワークステーション圧縮カードと、ワークステーション・コネクション・デバイスの IP アドレスを構成して、これらが相互に通信できるようにすることが重要です。

これらのデバイスの Web インターフェースにアクセスするために、圧縮カードの IP アドレスを調べる必要があります。HC10 の場合、圧縮カードの IP アドレスは BIOS 内で確認できます。CP20 の IP アドレスは、CP20 のローカル・インターフェースを使用して確認できます。これらのアドレスを確認した後、Web インターフェースからこれらのアドレスにアクセスし、変更できます。

6.1.1 HC10 の BIOS 内での IP 構成

HC10 の圧縮カードの構成を表示および設定するには、BIOS または HC10 の Web インターフェースを使用します。BIOS を使用して IP 構成を調べ、設定するには、次の手順で行います。

1. HC10 のブート中に、F1 を押して Configuration/Setup ユーティリティーに入ります。「**Advanced Setup**」を選択し、Enter を押します (図 6-1)。

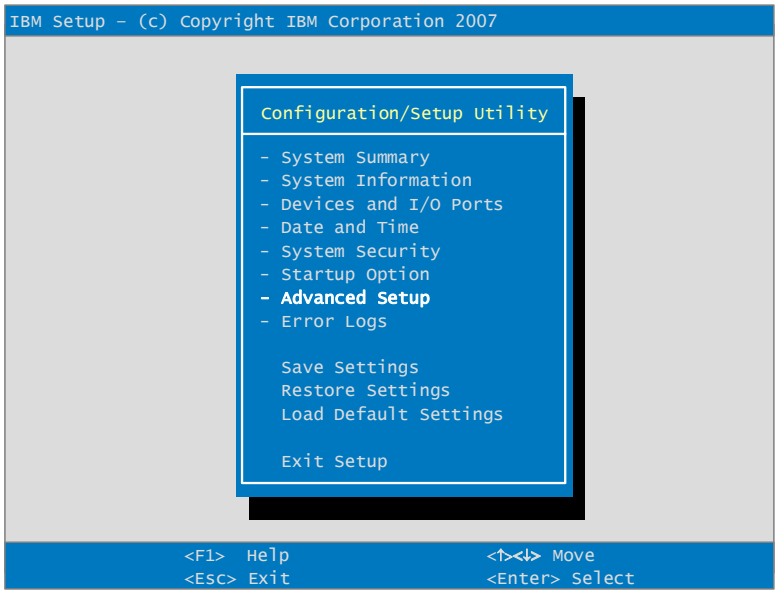


図 6-1 Configuration/Setup ユーティリティーのメインメニュー

2. 「**Compression Card Network Configuration**」を選択し、Enter を押します (図 6-2)。

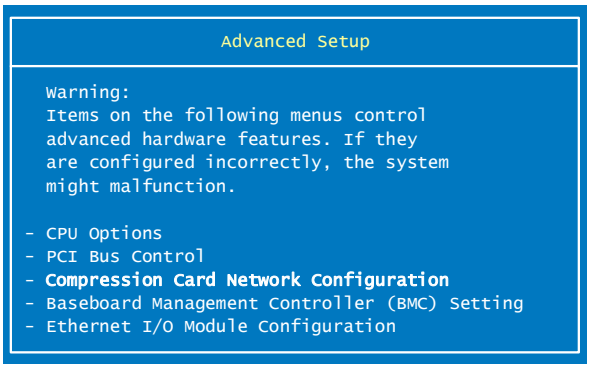


図 6-2 HC10 の BIOS の「Advanced setup」メニュー

3. メニューには、デバイスが DHCP を使用していることが示され、IP アドレスが表示されます (図 6-3)。この IP アドレスは HC10 の圧縮カードの IP アドレスで、Web インターフェースへのアクセスにはこのアドレスを使用できます。

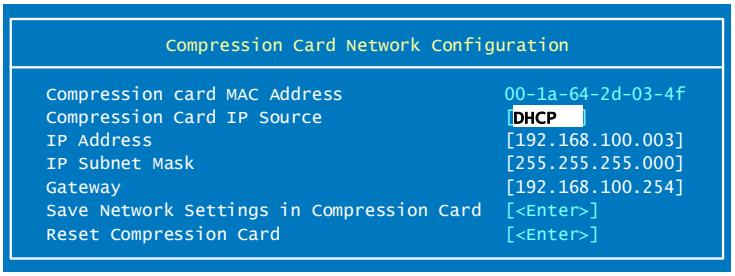


図 6-3 HC10 の圧縮カードの IP アドレス

4. 固定 IP アドレスを使用する場合は、「DHCP」を強調表示し、右矢印キーを押します。表示は「Static」に変わり、アドレス・フィールドを変更できるようになります。使用する IP アドレスを入力します。ネットワークの競合を避けるために、アドレスが固有であることを確認してください。
5. ご使用のネットワークのサブネット・マスクとゲートウェイを入力します。(Gateway 必須)
6. 「Save Network Settings in Compression Card」まで下に進み、Enter を押します。
7. Enter を再度押して、設定値が保存されたことを確認します。
8. Configuration/Setup ユーティリティーのメインメニューに戻るまで、Esc を押します。
9. セットアップ・パネルを終了します。

HC10 上で IP 設定値が構成されます。

6.1.2 ローカル・インターフェースを使用した CP20 の IP 構成

CP20 の IP 構成を表示および設定するには、CP20 のローカル・インターフェースまたは CP20 の Web インターフェースを使用します。ローカル・インターフェースを使用して IP 構成を調べ、設定するには、次の手順で行います。

1. CP20 の電源を入れて、「**Options**」→「**Configuration**」をクリックします。
2. 「**Unlock**」を選択して、パスワードを入力し、「**OK**」を押して設定をアンロックします。

> **注 :** デフォルト・パスワードは PASSW0RD (英文字の *O* ではなくゼロを含む) です。パスワードの設定方法については、『6.3.1, パスワードの変更』(ページ 107) を参照してください。

3. 「Network」タブでは、DHCP が使用されていることが示され、すべての構成ボックスが使用不可になっています。図 6-4 に示すように、ここで動的 IP アドレスを判別できます。

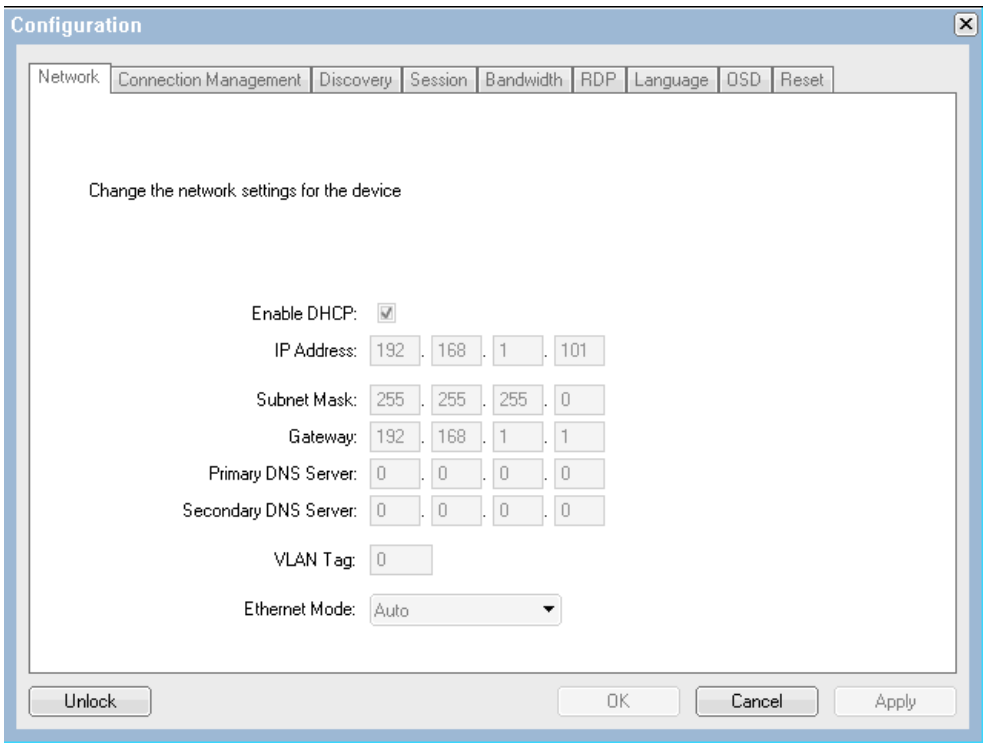


図 6-4　CP20 の動的アドレスを判別する方法

4. 固定アドレスを使用する場合は、「Enable DHCP」というラベルの付いたボックスをクリアし、CP20 に割り当てる IP アドレスを入力します。
5. ご使用のネットワークのサブネット・マスクとゲートウェイを入力します。CP20 と HC10 が通信するためには、このマスクが HC10 と同じであることが必要です (109 ページの図 6-10 を参照)。(Gateway 必須)
6. 「**Apply**」→「**OK**」をクリックして、設定を適用します。
7. 設定を有効にするには、CP20 の電源をオフにし、再びオンにする必要があります。

CP20 上で IP 設定値が構成されます。

6.1.3 Web インターフェースによる HC10 IP アドレスの構成

HC10 圧縮カードの IP アドレスが既に分かっていて、アドレスを変更する必要がある場合は、別のシステム上で稼働する Web ブラウザーから、圧縮カードの Web インターフェースを使用することもできます。次の手順で行います。

1. HC10 の電源をオンにします。
2. I/O モジュール 2 が接続されているネットワークにコンピューターを接続します。（BladeCenter S では I/O モジュール 1）
3. そのコンピューター上で Web ブラウザーを開き、ブレード・ワークステーションの IP をブラウザーのアドレス・フィールドに入力します。BIOS を使用して、HC10 の IP アドレスを調べ (『6.1.1, HC10 の BIOS 内での IP 構成』(ページ 102))、Enter を押します。
4. ブラウザー・ウィンドウ内で、メニューから「**Configuration**」→「**Network**」をクリックします。図 6-5 に示すパネルが表示されます。

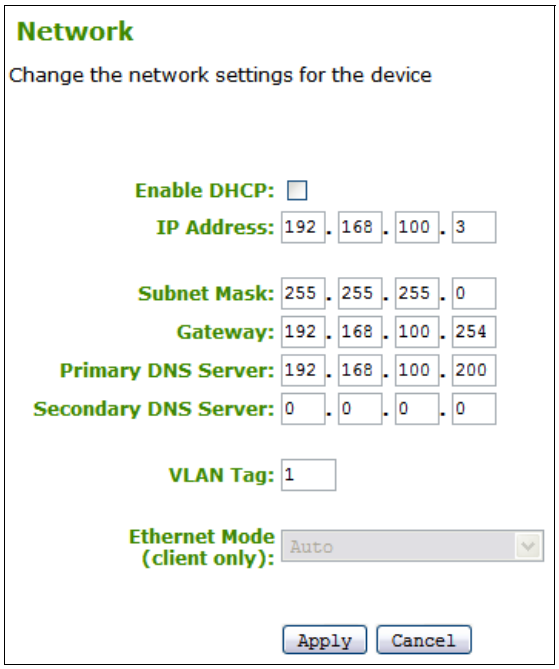


図 6-5 HC10 のネットワーク構成設定

5. HC10 の IP アドレス、サブネット・マスク、およびゲートウェイを、目的の構成に変更します。（Gateway 必須）
6. 「**Apply**」をクリックし、Web ブラウザーを閉じます。
7. 変更を有効にするには、HC10 をシャットダウンしてから、電源をオンにします。

6.1.4 Web インターフェースによる CP20 IP アドレスの構成

ブレード・ワークステーションと同じネットワーク上にある別のコンピューターを使用して、CP20 の IP 設定を構成することもできます。次の手順で行います。

1. CP20 の電源を入れます。
2. I/O モジュール 2 が接続されているネットワークにコンピューターを接続します。（BladeCenter S では I/O モジュール 1）
3. そのコンピューター上で Web ブラウザーを開き、CP20 の IP アドレスをブラウザーのア

ドレス・フィールドに入力します。CP20 のローカル・インターフェースを使用して、デバイスの IP アドレスを調べ (『6.1.2, ローカル・インターフェースを使用した CP20 の IP 構成』(ページ 104) を参照)、Enter を押します。

4. 表示されるダイアログ・ボックスで、「**Configuration**」→「**Network**」を選択します。109 ページの図 6-10 を参照してください。
5. CP20 の IP アドレス、サブネット・マスク、およびゲートウェイを、目的の構成に変更します。
6. 「**Apply**」をクリックし、Web ブラウザーを閉じます。
7. 変更を有効にするには、CP20 をシャットダウンしてから、電源をオンにします。

6.2 イーサネット・スイッチ・モジュールの役割を指定

HC10 ワークステーション・ブレードは、BladeCenter シャーシに取り付けられたイーサネット・スイッチ・モジュール (ESM) を使用して、イーサネット経由で通信します。デフォルトでは、HC10 には 2 つの ESM を取り付ける必要があります。

- BladeCenter シャーシのベイ 1 の ESM は、Windows ネットワーキング・トラフィックに使用されます。
- シャーシのベイ 2 の ESM は、HC10 の圧縮カード (I/O グラフィックス伝送アダプターとも呼ばれる) を CP20 に接続するために使用されます。(BladeCenter S を除く)

これらのデフォルトは、HC10 の BIOS 内で変更できます。BIOS の「Advanced Setup」パネルで、「**Ethernet I/O Module Configuration**」を選択します。図 6-6 に示すパネルが表示されます。

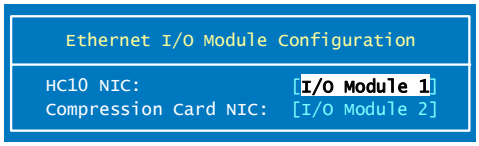


図 6-6 使用されるイーサネット・スイッチ・モジュールの選択

ここで、Windows ネットワーキングに使用するスイッチ・モジュール (図 6-6 の「HC10 NIC」)、および HC10-CP20 接続 (Compression Card NIC) を選択できます。それぞれの場合に選択する項目は、次のとおりです。

- I/O Module 1
- I/O Module 2

つまり、必要に応じて、両方とも I/O モジュール 1 を使用するように構成し、BladeCenter シャーシに ESM を 1 つだけ取り付けることもできます。この構成では、Windows トラフィックと CP20 トラフィックは 1 つの稼動中ネットワーク上に存在します。この場合にも、HC10-CP20 トラフィックは暗号化されているのでセキュアです。

6.3 CP20 ローカル・インターフェース

CP20 ローカル・インターフェースを使用して、次のことが可能です。

- IP 設定値を構成する。
- コネクション・ブローカー・ソフトウェアを使用して接続を確立する。

- HC10 の IP アドレスと MAC アドレスを手動で入力するか、検出オプションを使用して、HC10 に接続する。
- 帯域幅制限を設定する。
- RDP 固有の構成を変更する。
- 言語を選択する。
- 画面表示テキストを設定する。
- イベント・ログやセッション統計を表示したり、IP アドレスを ping したりする。
- CP20 に関する情報を表示し、設定を保護するためのパスワードを適用する。

CP20 のメインメニューにある「**Options**」には、5 つの選択項目があります（図 6-7 を参照）。

図 6-7　CP20 インターフェースの「Options」メニュー

次に、これらのメニュー・オプションについて説明します。.

- 『6.3.2, 「Configuration」パネル』(ページ 109)
- 『6.3.3, 「Diagnostics」パネル』(ページ 118)
- 『6.3.4, 「Information」パネル』(ページ 122)
- 『6.3.5, 「User Settings」パネル』(ページ 123)
- 『6.3.6, 「Password」パネル』(ページ 124)

6.3.1 パスワードの変更

CP20 の構成を変更するには、メニューをアンロックする必要があります。パスワードを設定し、構成設定値をアンロックするには、次の手順で行います。

1. 「**Options**」→「**Password**」をクリックします。
2. 「Change Password」ダイアログ・ボックスで、旧パスワードを入力します。

   注 : デフォルト・パスワードは PASSW0RD (英文字の *O* ではなくゼロを含む) です。

3. 新規パスワードを入力し、この新規パスワードを確認します。「**OK**」をクリックします。図 6-8 を参照してください。

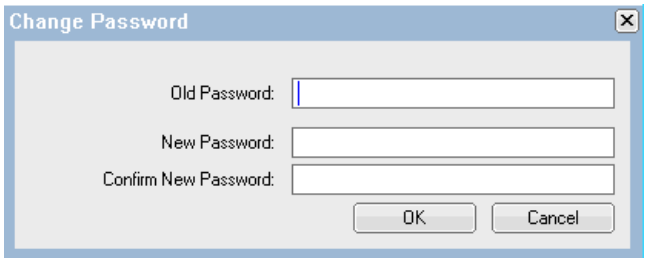


図 6-8 CP20 インターフェースの「Change password」メニュー

4. 「**Options**」→「**Configuration**」→「**Unlock**」をクリックします。
5. 作成したパスワードを入力します。新規パスワードを作成していない場合は、デフォルトの PASSW0RD (英文字の *O* ではなくゼロを含む) を入力します。図 6-9 を参照してください。「**OK**」をクリックします。

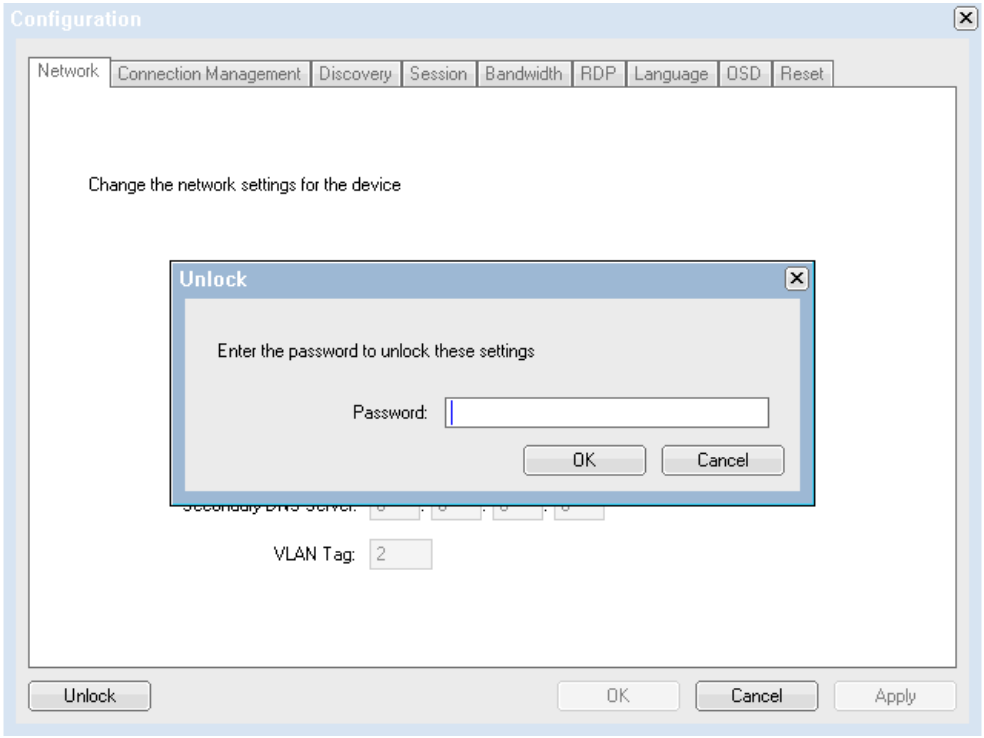


図 6-9 CP20 インターフェースの設定値のアンロック

6.3.2 「Configuration」パネル

「Configuration」パネルには、次に説明する一連のタブを含むウィンドウが表示されます。

注 : パラメーターを変更する前に、**「Unlock」**ボタンをクリックしてパスワードを入力する必要があります。デフォルト・パスワードは PASSW0RD (英文字の *O* ではなくゼロを含む) です。

「Configuration」パネルの設定値について重要なことは、状況に応じて設定値の一部が無視されることです。これについて次に説明します。

- コネクション・ブローカーを使用可能にすると (つまり、「Connection Management」タブで**「Enable Connection Management」**を選択すると)、「Discovery」タブと「Session」タブのフィールドがすべて無視されます。
- ディスカバリーを使用可能に設定すると (つまり、「Connection Management」タブで**「Enable Connection Management」**を選択せず、「Discovery」タブでは**「Enable Discovery」**を選択)、「Session」のフィールドがすべて無視されます。
- コネクション・ブローカーを使用可能にしたか、ディスカバリーを使用可能にしたか、「Session」タブでセッション・タイプとして**「PCoIP」**を選択した場合は、「RDP」タブの内容が無視されます。

「Network」タブ

接続を確立するには、図 6-10 に示すように、「Network」タブでネットワーク設定値を構成する必要があります。『6.2, イーサネット・スイッチ・モジュールの役割を指定』(ページ 106) も参照してください。

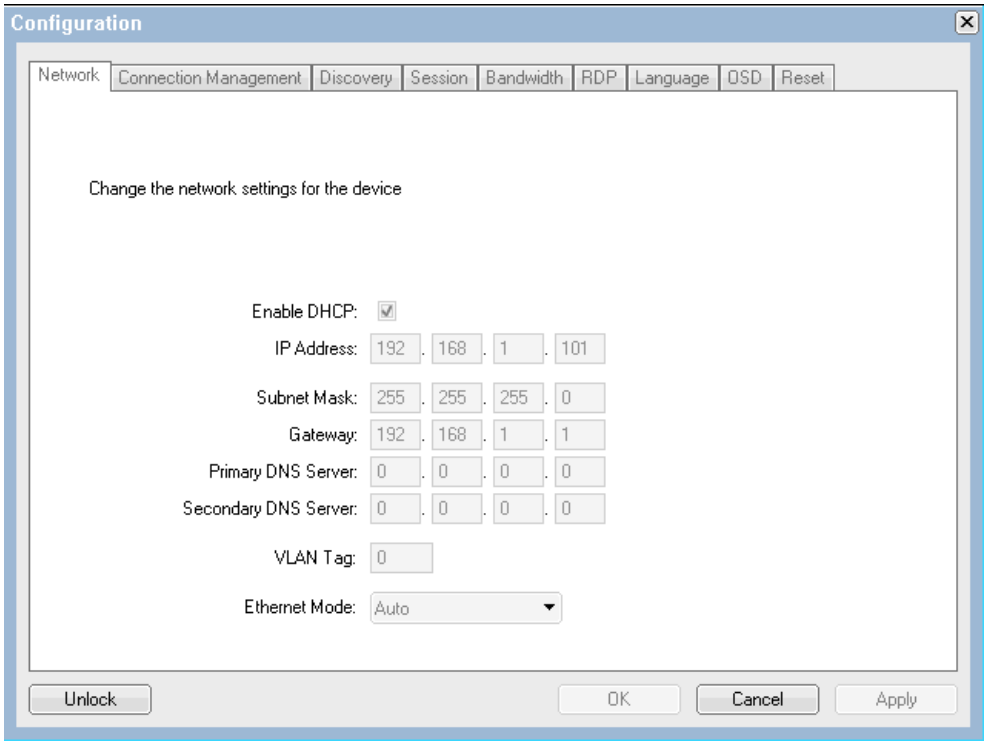


図 6-10 CP20 インターフェースの「Network」タブ

「Network」タブでは、DHCP または固定アドレスのどちらを使用するか選択できます。デフォルトは DHCP に設定されており、ボックスはすべて使用不可になります。DHCP によって現在割り当てられているアドレスは、使用不可のフィールドに示されます。

「Enable DHCP」チェック・ボックスをクリアし、IP アドレス、サブネット・マスク、ゲートウェイ、および 1 次と 2 次の DNS サーバーを入力することによって、IP アドレスを固定に変更できます。

「Connection Management」タブ

「Connection Management」タブでは、接続管理に対応するように CP20 を構成できます (図 6-11 を参照)。このタブにより、接続の管理にコネクション・ブローカー・ソフトウェアを使用するようにデバイスを構成できます。

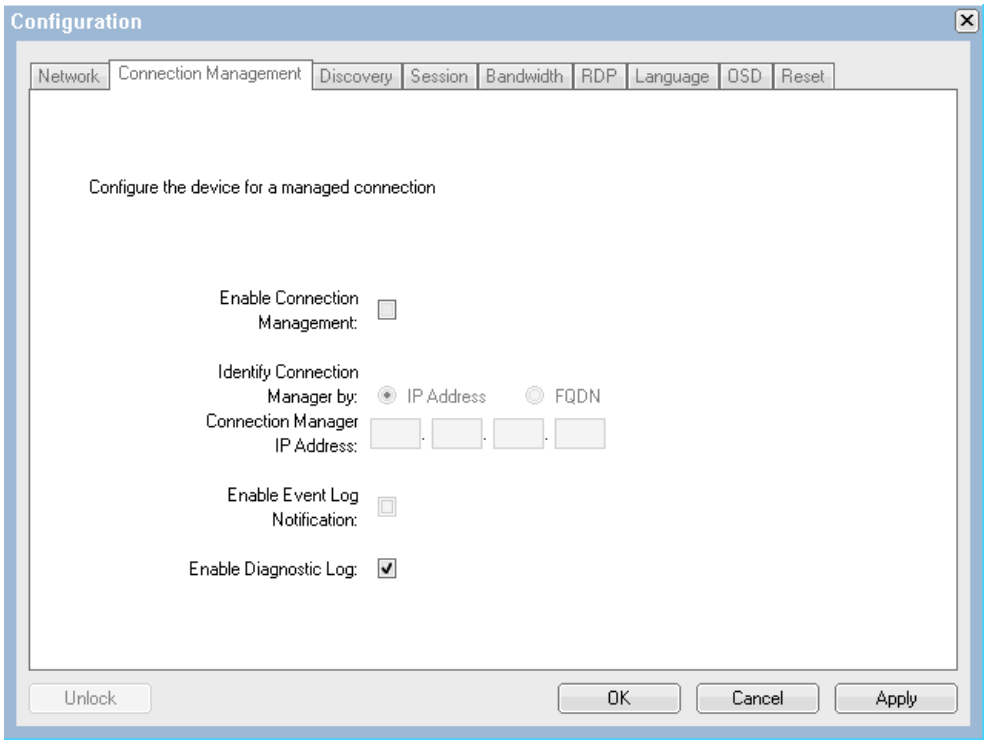


図 6-11　CP20 インターフェースの「Connection management」タブ

「**Enable Connection Management**」を選択すると、CP20 は HC10 への接続を確立するために、コネクション・ブローカー・ソフトウェアへの接続を試みます。コネクション・ブローカー・ソフトウェアを手動で構成する場合は、コネクション・ブローカーの IP アドレスを使用して接続するか、完全修飾ドメイン・ネーム (FQDN) を使用して接続するかを選択する必要があります。

IP アドレスを使用するには、「**IP Address**」を選択し、該当するフィールドに IP アドレスを入力します。FQDN の場合は、「**FQDN**」を選択して、ドメイン・ネームを入力します。

また、イベント・ログに関するオプションが 2 つあります。

- 「**Enable Event Log Notification**」を選択できます。このオプションを選択すると、デバイスはイベント・ログ・メッセージをコネクション・ブローカーに送信します。受信したメッセージがすべて送信されるまで、1 分に約 1 回、一度に 10 件までのメッセージが送信されます。デバイスの電源をオフにしてからオンにしたとき、およびリセット後は、イベント・ログが消去されます。

- 「**Enable Diagnostic Log**」は、診断目的のみに使用されます。このオプションを選択すると、コネクション・ブローカーにメッセージは送信されません。

ヒント：「Connection」タブで「**Enable Connection Management**」を選択すると、「Discovery」タブ、「Session」タブ、および「RDP」タブの内容がすべて*無視されます*。これら 3 つのタブは、ピアツーピア構成専用です。コネクション・ブローカーとピアツーピア接続の使用は相互に排他的なオプションなので、これらのパラメーターは使用されません。

「Discovery」タブ

「Discovery」タブ (図 6-12 を参照) では、ピアツーピア接続を使用可能に設定し、接続可能な HC10 を接続時に自動的に検索します。このタブと「Session」タブを使用すれば、コネクション・ブローカーを使用せずに CP20 から HC10 に直接接続できます。

ヒント：「Discovery」タブと「Session」タブは両方とも、ピアツーピア接続に関連しています。「Session」タブのパラメーターを使用すると、接続する特定の HC10 を指定できます。一方、「Discovery」タブを使用すると、使用可能な HC10 (つまり、オンラインになっているが、まだセッション中でない HC10) のリストから HC10 を選択できます。「Discovery」は、単純なコネクション・ブローカーと考えることができます。

ピアツーピア接続の使用法について詳しくは、『6.5, ピアツーピア接続のセットアップ』(ページ 145) を参照してください。

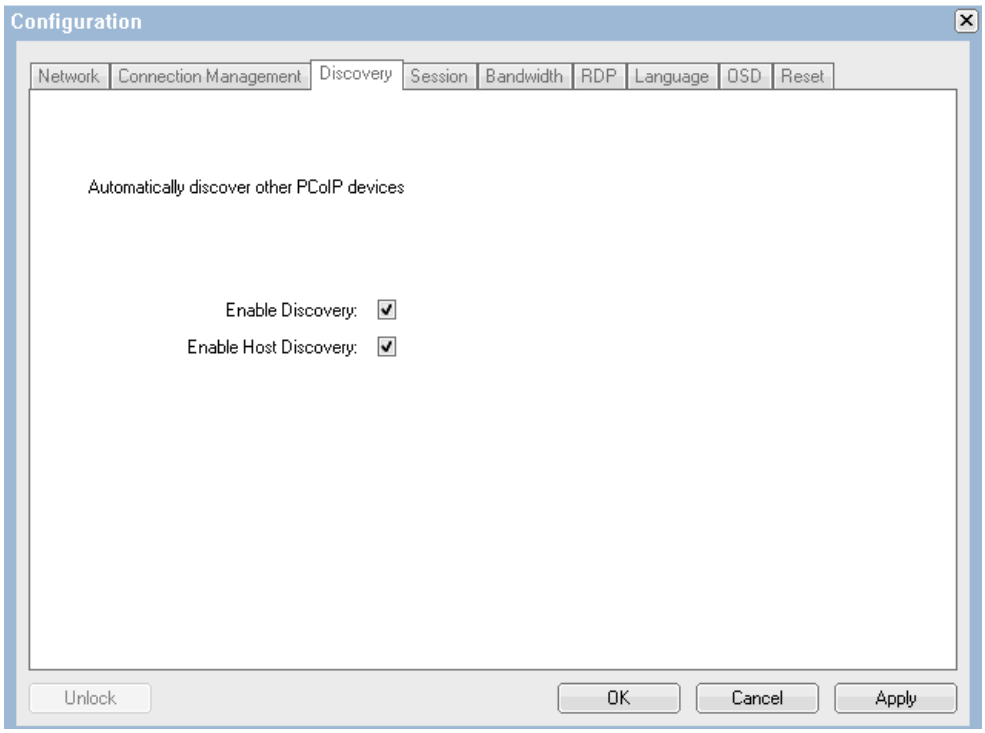


図 6-12　CP20 インターフェースの「Discovery」タブ

ディスカバリーの目的は、CP20 が接続可能な HC10 を検索することです。このタブで構成できるオプションは 2 つあります。ディスカバリー・オプションを使用するには、「**Enable Discovery**」と「**Enable Host Discovery**」の両方を選択する必要があります。これら両方のオ

プションを選択すると、接続先の HC10 を選択するオプションが表示されます。このオプションを表示する際に、CP20 は使用可能な HC10 を検出して、図 6-13 に示すように接続可能な HC10 のリストを作成します。このリストから、接続する HC10 を選択できます。

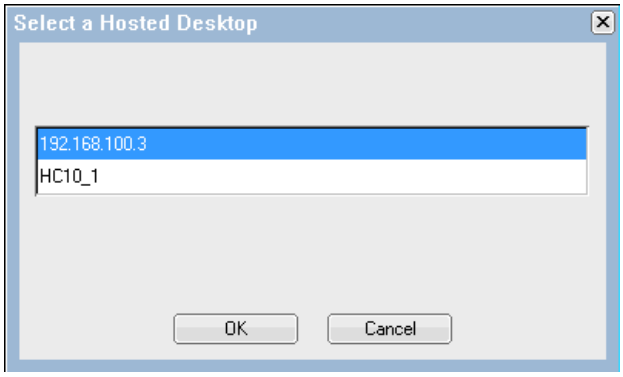


図 6-13　接続可能な HC10 のリスト

注 : 110 ページの図 6-11 に示した「Connection」タブで「**Enable Connection Management**」を選択した場合、検出機能は使用されず、このタブの設定値は無視されます。

「Session」タブ

図 6-14 に示す「Session」タブでは、この CP20 から接続したい特定の HC10 の IP アドレスと MAC アドレスを手動で指定して、ピアツーピア・セッションを構成できます。ピアツーピア接続の使用法について詳しくは、『6.5, ピアツーピア接続のセットアップ』(ページ 145)を参照してください。

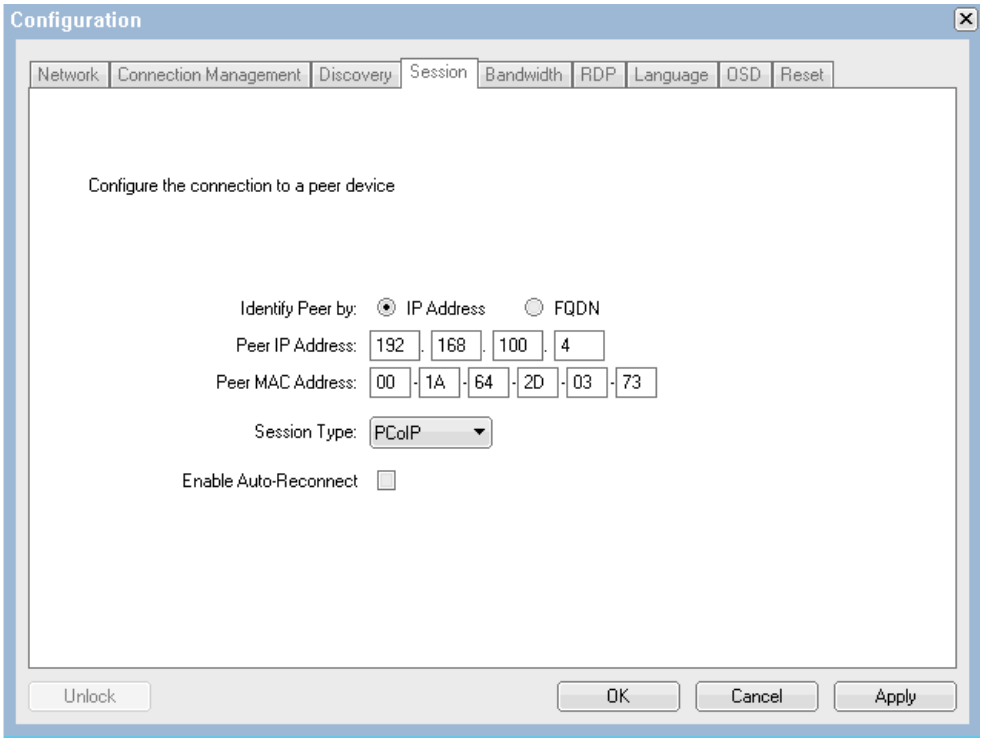


図 6-14　CP20 インターフェースの「Sessions」タブ

注 : このタブのフィールドをアクティブにするには、「Discovery」タブの「**Enable Discovery**」の選択を*解除* し、「Connection Management」タブの「**Enable Connection Management**」の選択を*解除* する必要があります。これらのどちらかのオプションが選択されていると、「Session」タブのすべてのフィールドが無視されます。

HC10 の IP アドレス、または完全修飾ドメイン・ネーム (FQDN) のどちらかが分かっていれば、ピアツーピア接続を確立できます。IP アドレスを使用するには、「**IP Address**」を選択し、HC10 圧縮カードの IP アドレスを該当するフィールドに入力します。FQDN を使用するには、「**FQDN**」を選択して、ドメイン・ネームを入力します。

HC10 の圧縮カードの MAC アドレスも入力する必要があります。MAC アドレスを判別するには、次の 2 とおりの方法があります。

- HC10 をブートし、F1 を押して BIOS に入ってから、「**Advanced Settings**」→「**Compression Card Network Configuration**」を選択します。表示されるパネルに MAC アドレスが示されます。
- 112 ページの図 6-14 に示した MAC アドレスの無効な値をそのままにして、HC10 への接続を試みます。接続は失敗し、「`Session Refused!`」というメッセージが表示されます。その後、「**Options**」→「**Diagnostics**」をクリックします。イベント・ログに 2 つの項目が示されます。1 つは無効な MAC アドレスをリストし、もう 1 つは予期されていた MAC アドレスをリストするものです。その予期されていたアドレスを、112 ページの図 6-14 に示したようにフィールドにコピーします。例えば、すべてゼロからなる仮の MAC アドレスを指定すると (`00-00-00-00-00-00`)、イベント・ログには例 6-1 に示すようなメッセージが表示されます。

例 6-1 圧縮カードの正しい MAC アドレスを示すエラー・ログ・メッセージ

```
Connecting with host (9.42.170.185, 00-00-00-00-00-00)
Peer MAC mismatch:(00-1A-64-2D-02-EE, 00-00-00-00-00-00)
```

この例での正しい MAC アドレスは、`00-1A-64-2D-02-EE` です。

注 : 将来のファームウェア更新によって、MAC アドレスの入力は不要になる可能性があります。

セッション・タイプは PCoIP または RDP のどちらかですが、HC10 に接続するにはセッション・タイプを PCoIP に設定する必要があります。

「**Enable Auto-Reconnect**」を選択すると、CP20 の電源がオンになったときに、CP20 は最後に接続した HC10 への接続を自動的に試行するように構成されます。CP20 はブート時にのみ再接続を試み、セッションの切断後は再接続しません。

「Connection Management」または「Discovery」が使用可能に設定されている場合、「Session」タブは考慮されません。設定値の構成は可能ですが、これらのオプションのどちらかが使用可能に設定されていると、このタブは無視されます。

「Bandwidth」タブ

図 6-15 に示す「Bandwidth」タブを使用すると、デバイスの帯域幅制限を Mbps 単位で設定できます。これを無制限に設定するには、単にゼロ (0) を入力するか、最大限の量を入力します。

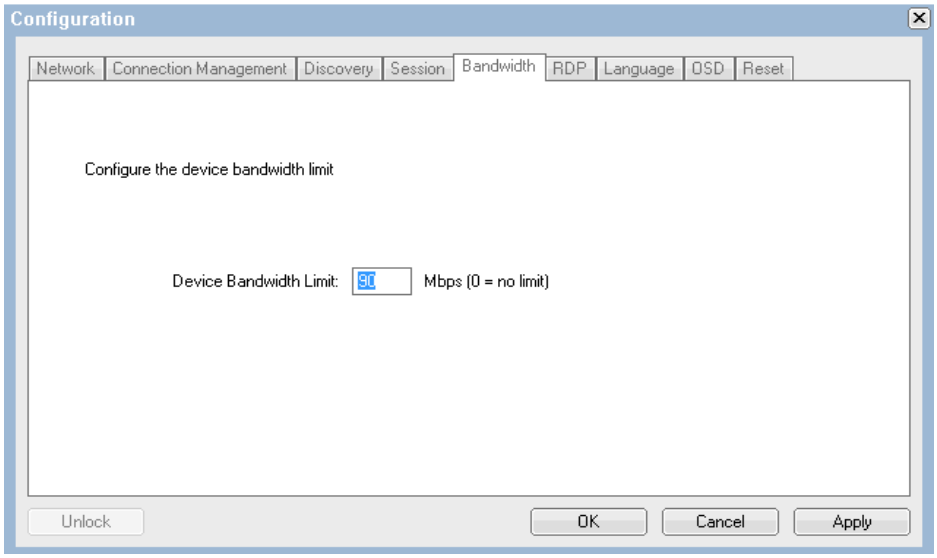


図 6-15　CP20 インターフェースの「Bandwidth」タブ

「RDP」タブ

図 6-16 に示す「RDP」タブを使用すると、RDP 接続の解像度、ビット深さ、およびターミナル・サーバー・ポートを構成できます。このタブのフィールドは、「Session」タブでセッション・タイプとして RDP を指定した場合のみ使用されます。そうでなければ、これらのフィールドは無視されます。

CP20 から HC10 に接続する構成の場合、セッション・タイプは常に PCoIP なので、「RDP」タブは使用されません。

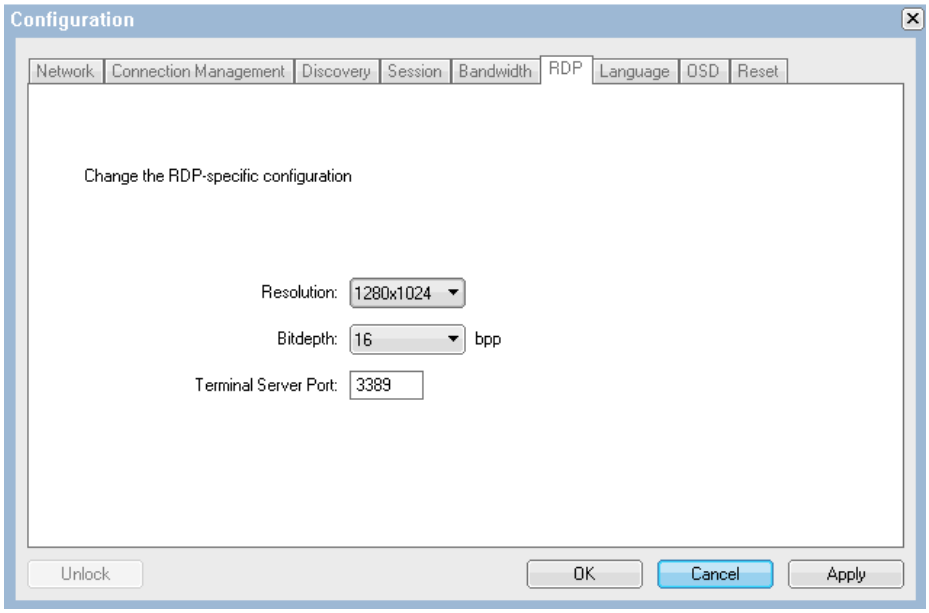


図 6-16　CP20 インターフェースの「RDP」タブ

「Language」タブ

「Language」タブを使用すると、CP20 の言語設定とキーボード・レイアウトを変更できます (図 6-17 を参照)。

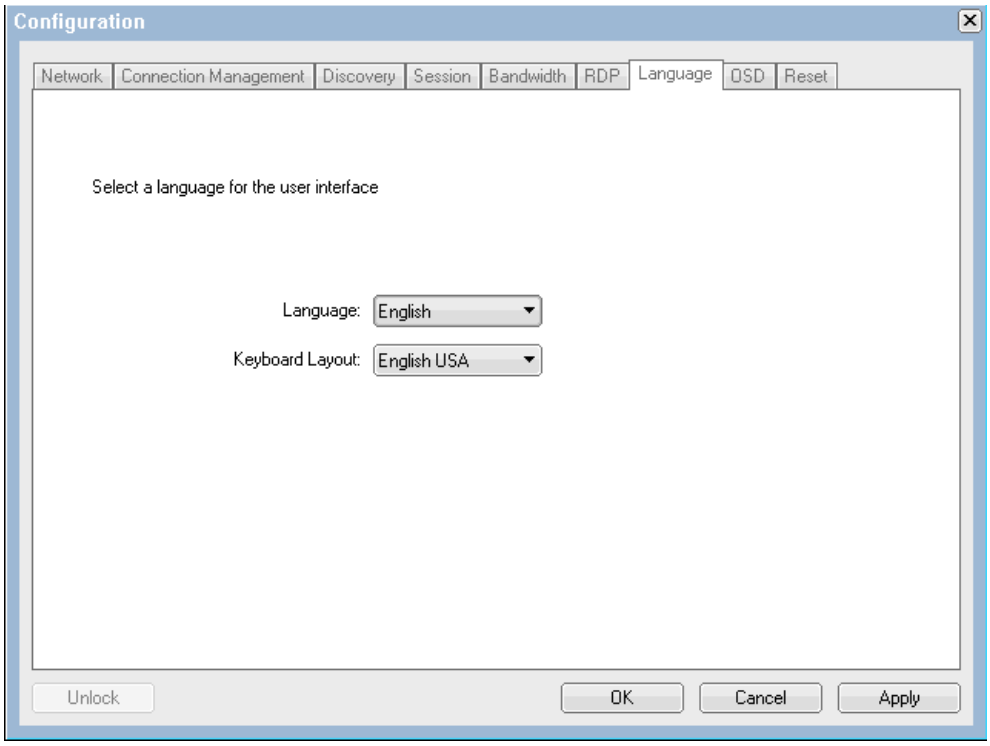


図 6-17 CP20 インターフェースの「Language」タブ

本書の執筆時点では、CP20 の言語オプションはただ 1 つ (英語) です。キーボード・レイアウトは、「English U. S.」と「French Canada」のどちらかを選択できます。

注 : 「Language」タブの設定値は、HC10 上の Windows で定義した言語設定に影響を与えません。これらの設定値の対象は、CP20 のローカル・インターフェースと Web インターフェースのみです。

「OSD」タブ

「OSD」タブを使用すると、CP20 がセッションを行っていないときのスクリーン・セーバー・テキストを設定できます (図 6-18)。デフォルトのスクリーン・セーバー・テキストは Screen Saver Text で、デフォルトのタイムアウトは 300 秒 (5 分) に設定されています。

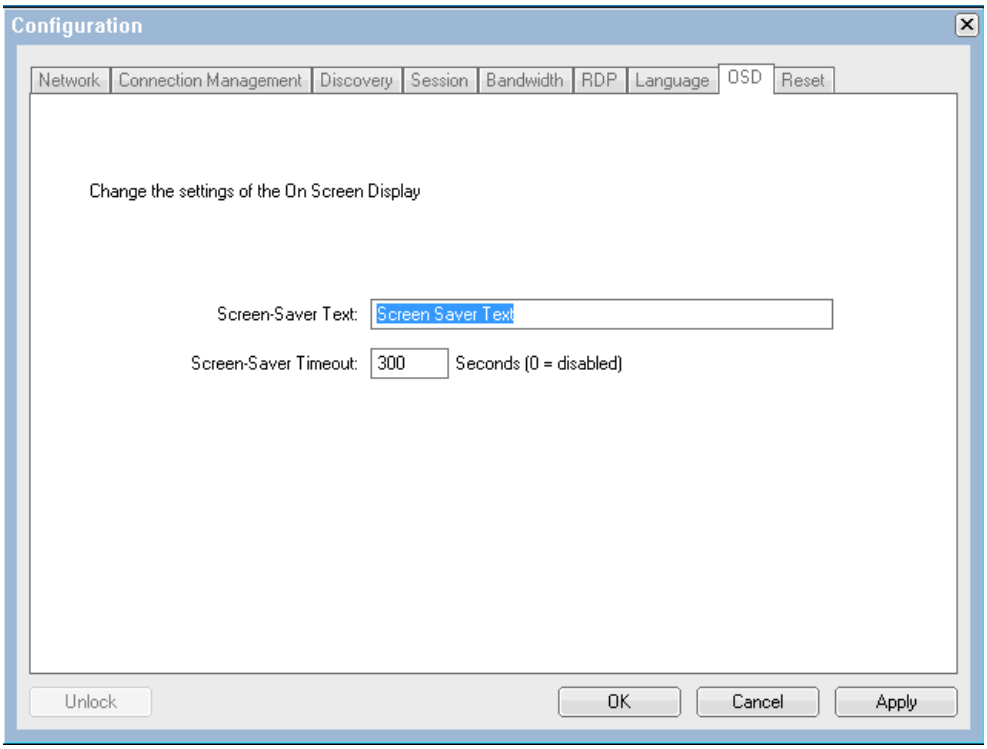


図 6-18　CP20 インターフェースの「OSD」タブ

テキストを変更するには、「Screen-Saver Text」フィールドに新しいテキストを入力します。200 文字を超えて入力できますが、テキストは折り返しません。

スクリーン・セーバーが使用されるまでの待ち時間を変更することもできます。このためには、「Screen-Saver Timeout」フィールドに新しい数値を入力します。このタイムアウト値は、秒数で入力します。ゼロ (0) を入力すると、スクリーン・セーバーが使用不可に設定されます。

実際のスクリーン・セーバーは、黒の背景に単純な白いテキストを表示するもので、テキストは画面にランダムに配置されます。このスクリーン・セーバーは、HC10 に対するアクティブ・セッションがない場合にのみ使用されます。

「Reset」タブ

「Reset」タブを使用すると、CP20 の構成をデフォルト設定にリセットできます (図 6-19)。

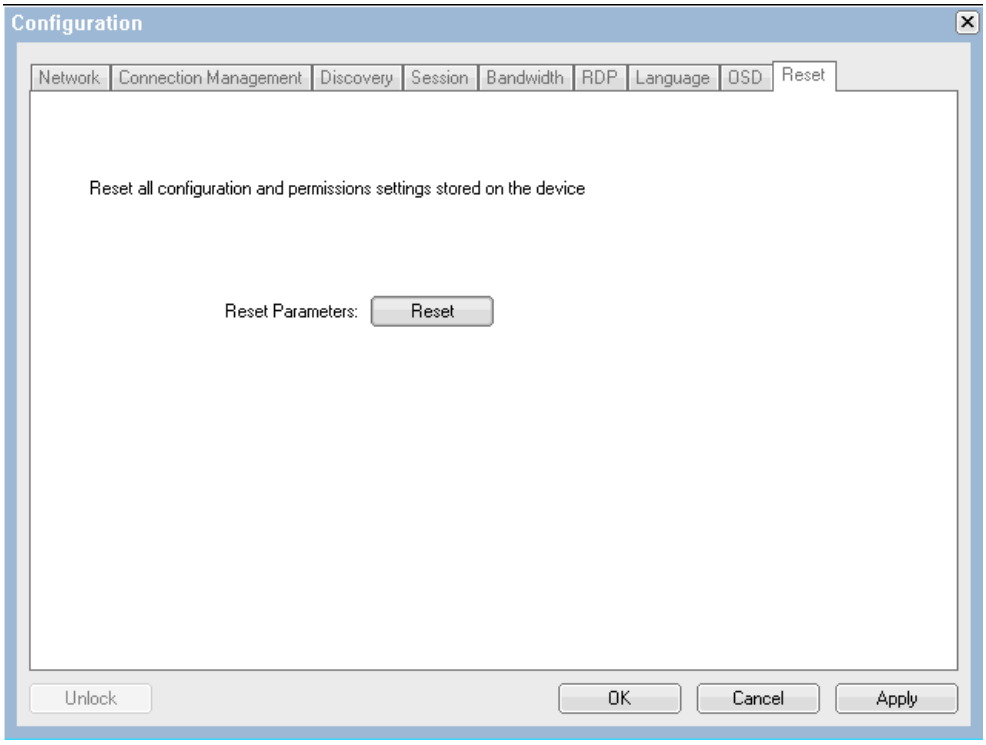


図 6-19　CP20 インターフェースの「Reset」タブ

構成をすべてリセットするには、「**Reset**」をクリックします。これにより、すべての構成がデフォルトに変更され、デバイスは DHCP とコネクション・ブローカーを使用するようになります。

注 : このリセット処理によって、ログイン・パスワードも PASSW0RD (英文字の *O* ではなくゼロを含む) にリセットされます。

6.3.3 「Diagnostics」パネル

「Diagnostic」パネルは、接続に問題がある場合に便利です。

「Event Log」タブ

図 6-20 に示す「Event Log」タブは、接続の問題のトラブルシューティングに役立ちます。

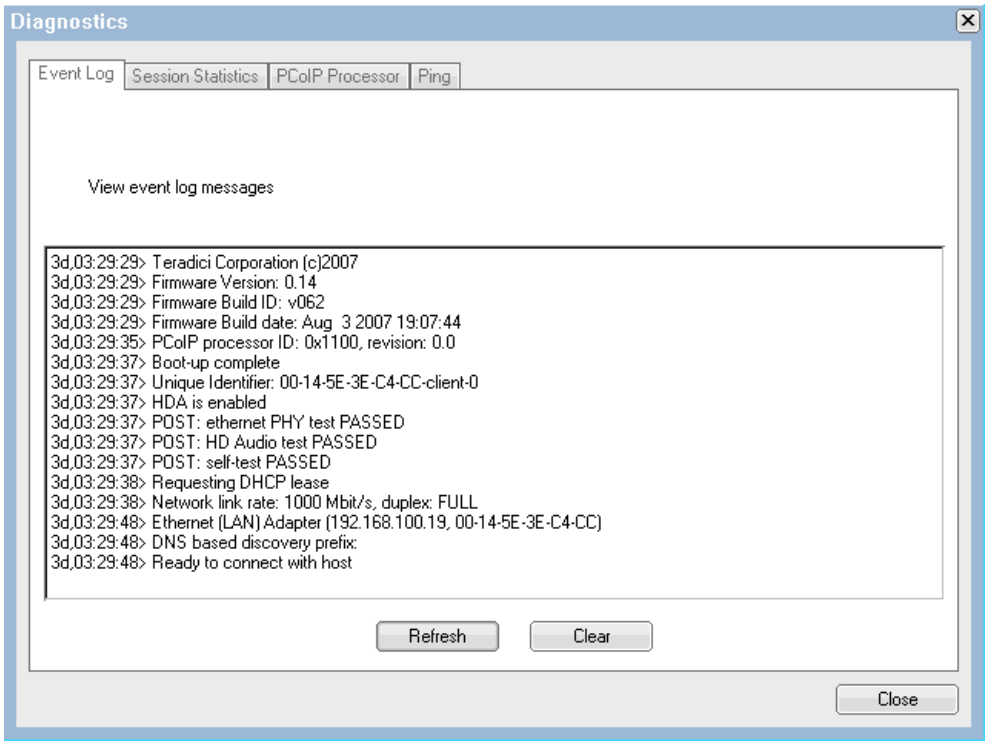


図 6-20　イベント・ログを表示する「Diagnostics」メニュー

「Event Log」タブは、発生したイベントを各イベントの発生時のタイム・スタンプとともに表示します。「Event Log」タブには、最新のイベントがログに記録されるようにする最新表示ボタンがあり、すべてのログを削除する「Clear」ボタンもあります。

「Session Statistics」タブ

「Sessions Statistics」タブでは、現行セッションに関する情報を確認できます (図 6-21)。

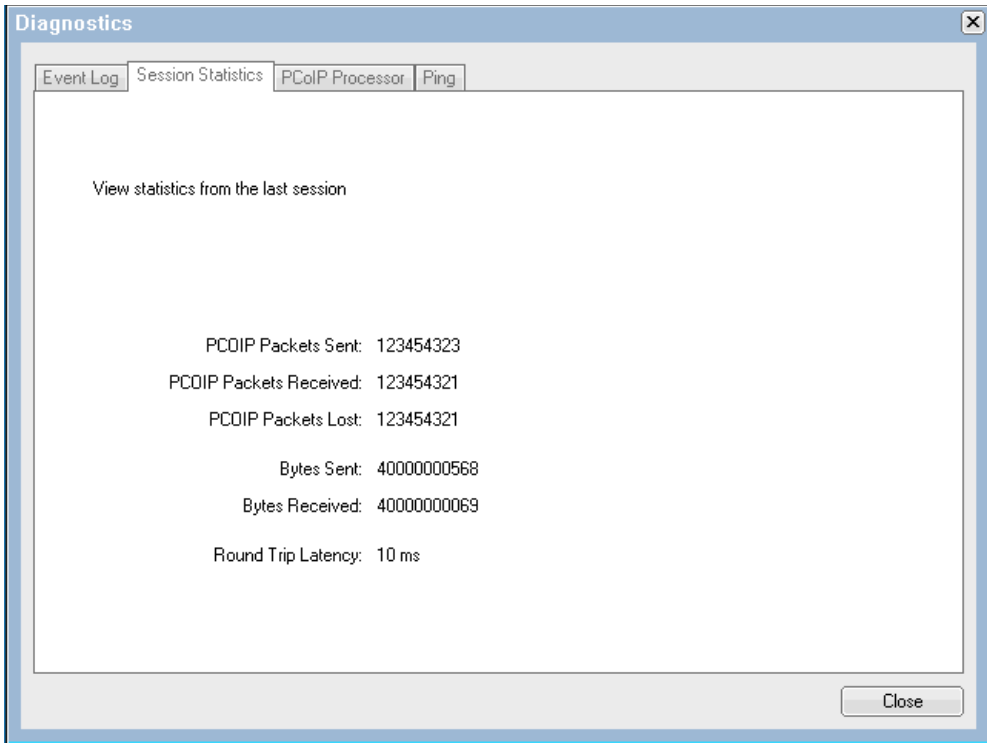


図 6-21　CP20 ローカル・インターフェースの「Sessions Statistics」タブ

このタブには、送信済み、受信済み、および破損した PC-over-IP パケットの数が表示され、送受信されたバイト数が示されます。

さらに、往復遅延 (Round Trip Latency) (ms) も表示されます。これは、CP20 内の PC-over-IP プロセッサーと、HC10 の圧縮カード内にある PC-over-IP プロセッサーとの間で、往復して通信するための遅延を示します。この値の精度は +/- 1 ms です。この値は、CP20 と HC10 の間の距離、およびネットワーク設計が実際の使用に十分適しているかどうか判断する際に有用です。

「PCoIP Processor」タブ

「PCoIP Processor」タブでは、前回のブート以降に経過した時間の長さを確認できます（図 6-22）。

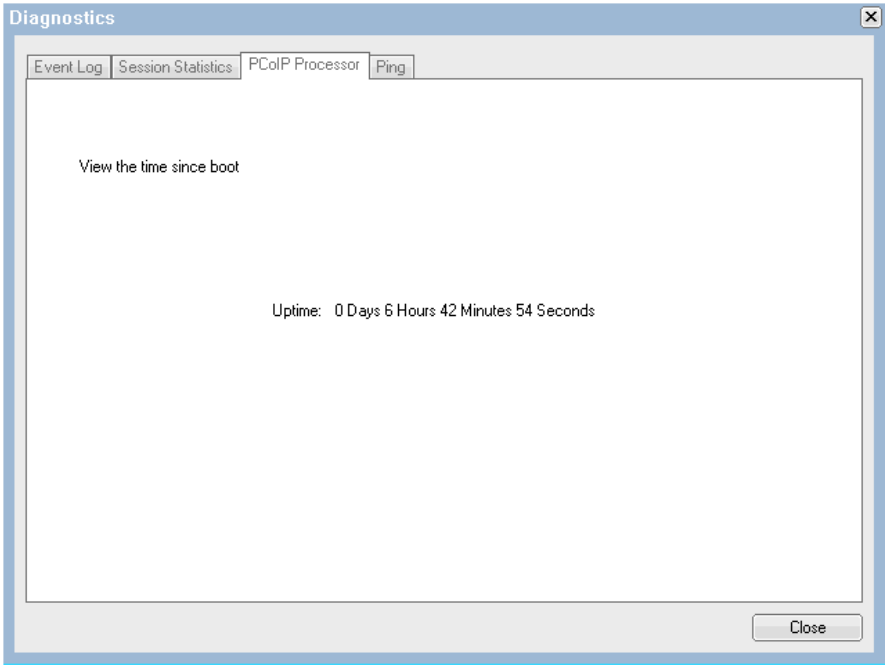


図 6-22　CP20 ローカル・インターフェースの「PCoIP Processor」タブ

「Ping」タブ

「Ping」タブでは、IP アドレスを ping できます (図 6-23)。

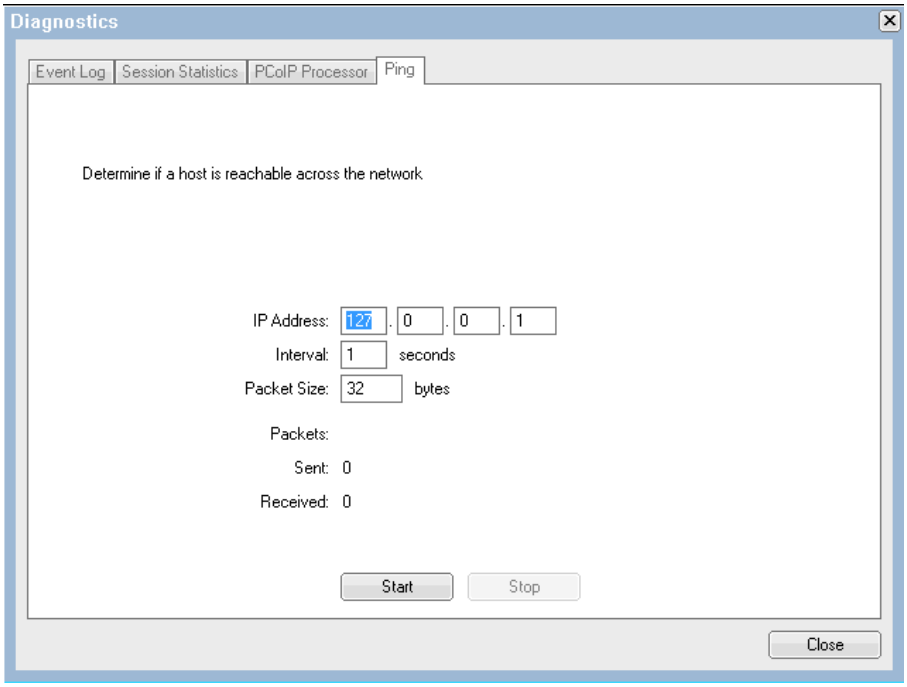


図 6-23 ping オプションを表示する「Diagnostics」メニュー

IP アドレスを ping するには、ping したい IP アドレスとともに、パケットの間隔秒数とサイズを入力します。**「Start」**をクリックすると、送受信されたパケット数が表示されます。

送信数が受信数と等しければ、IP アドレスの ping は正常に行われています。一方、パケットが受信されていない場合は、その IP アドレスを ping できないことを示しています。この機能は、特定のアドレスへの接続に問題が生じている場合に使用すると便利です。

6.3.4 「Information」パネル

「Information」パネルのタブは「Version」ただ 1 つです。「Version」タブは、CP20 のハードウェアとファームウェアの情報を詳しくリストします (図 6-24)。

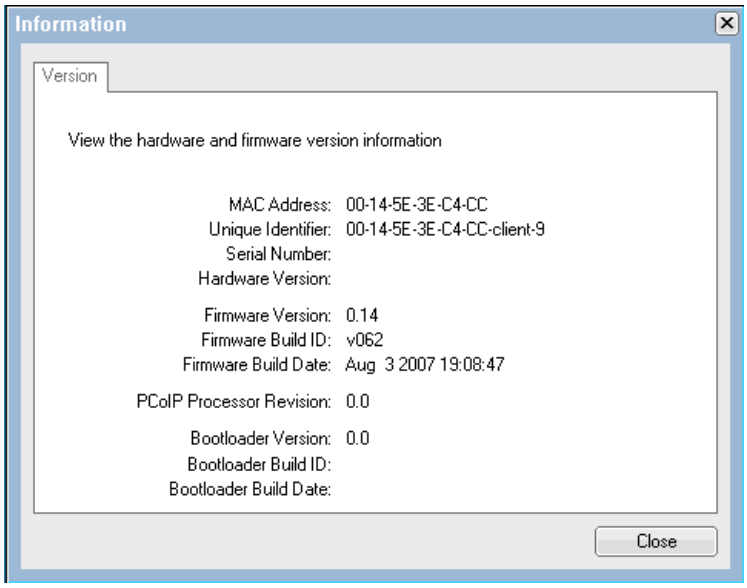


図 6-24 CP20 インターフェースの「Version」タブ

このタブを使用して、CP20 の MAC アドレス、シリアル番号、およびハードウェア・バージョンを取得できます。また、CP20 が現在使用しているファームウェア・バージョンを確認するためにも役立ちます。

ファームウェアを最新バージョンに保つことは重要です。Devon IT Connection Broker ソフトウェアを使用して、『5.1.3, ファームウェアの更新』(ページ 79) で説明したようにファームウェアをデプロイできます。

6.3.5 「User Settings」パネル

「User Setting」パネルでは、CP20 ローカル・インターフェース内でのマウスとキーボードの反応度を調整できます。

図 6-25 に示す「Mouse」タブでは、マウスの移動に対応してマウス・ポインターを動かす速度を指定できます。

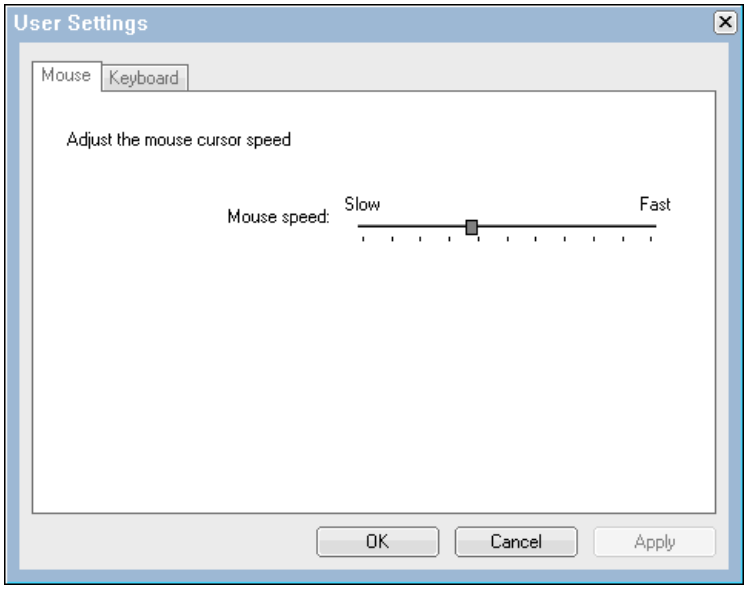


図 6-25 CP20 ローカル・インターフェースのユーザー設定の「Mouse」タブ

図 6-26 に示す「Keyboard」タブでは、キーの押下に対するキーボードの反応を制御できます。

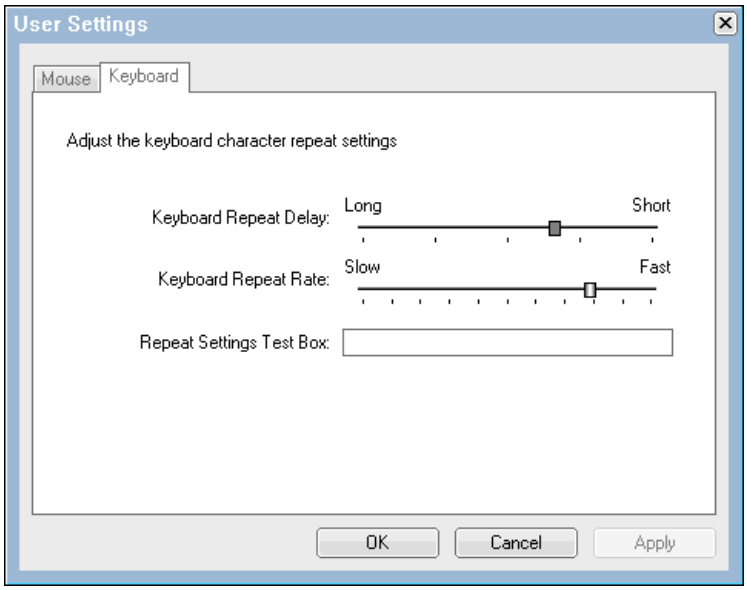


図 6-26 CP20 ローカル・インターフェースのユーザー設定の「Keyboard」タブ

6.3.6 「Password」パネル

「Password」パネル (図 6-27) を使用して、HC10 または CP20 のパスワードを設定できます。デフォルト・パスワードは PASSW0RD (英文字の *O* ではなくゼロを含む) です。セキュリティー対策として、デバイスすべてのパスワードを変更することをお勧めします。

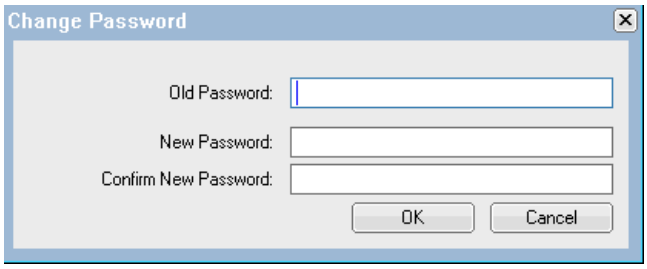


図 6-27　CP20 構成パネルのパスワードの変更

注 : ローカル CP20 を使用してパスワードを変更すると、Web インターフェース経由での接続に使用されるパスワードも変更されます。

6.4 HC10 および CP20 の Web インターフェース

HC10 および CP20 の Web インターフェースはよく似ています。同じレイアウトを使用し、同じオプションを含んでいますが、オプションによっては HC10 または CP20 のどちらかのみに適用されるものがあります。このセクションの図では、この違いを強調するために、通常は HC10 と CP20 の両インターフェースの同じダイアログを記載します。ダイアログ・ボックスが同一の場合は、一方のダイアログのみを示します。

次の手順では、Web インターフェースにアクセスする方法を説明します。

1. HC10 または CP20 (アクセスする対象のデバイス) の電源をオンにします。
2. I/O モジュール 2 が接続されているネットワークにコンピューターを接続します (または、デフォルトを変更した場合、HC10-CP20 トラフィックのルーティングのために構成したイーサネット・スイッチ・モジュール)。
3. そのコンピューター上で Web ブラウザーを開き、デバイスの IP アドレスをブラウザーのアドレス・フィールドに入力します。
4. パスワード (デフォルトは PASSW0RD、ただし英文字の *O* ではなくゼロを含みます) を入力し、アイドル時間を選択して、「**Log in**」をクリックします。図 6-28 を参照してください。

図 6-28　Web インターフェースのパスワード・パネル

一度に 1 ユーザーのみが Web インターフェースにログインできます。ユーザーが Web インターフェースにログインしているときに別のユーザーがログインしようとすると、2 番目のユーザーにはログイン先が使用中であることを示す警告が出されます。それでも 2 番目のユーザーがログインを選択すると、最初のユーザーのログアウトが自動的に行われます。ログアウトするには、ウィンドウの左上にある「**Log out**」をクリックします（図 6-29 を参照）。

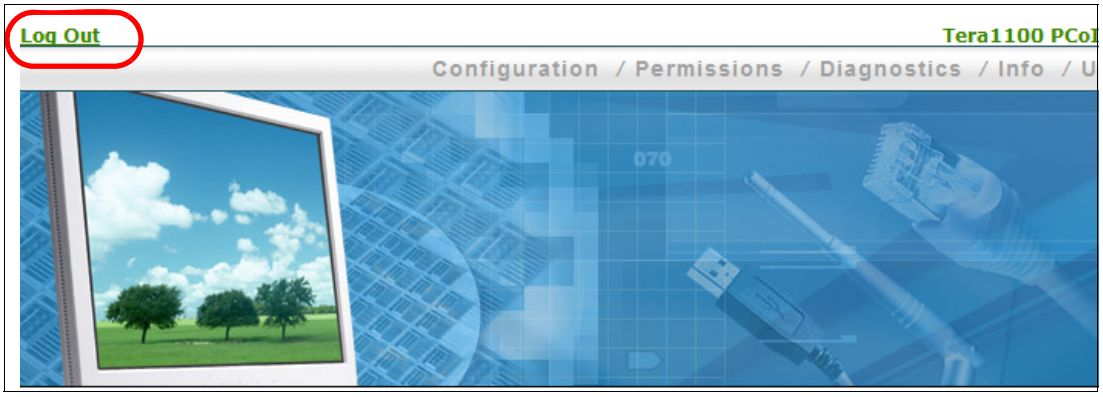


図 6-29　Web インターフェースからのログアウト

ログインすると、5 つのメニュー・オプションが表示され、それぞれにオプションのサブリストがあります。次に、これらのオプションについて説明します。

- 『6.4.1, 「Configuration」メニュー』(ページ 126)
- 『6.4.2, 「Permissions」メニュー』(ページ 136)
- 『6.4.3, 「Diagnostics」メニュー』(ページ 139)
- 『6.4.4, 「Info」メニュー』(ページ 142)
- 『6.4.5, 「Upload」メニュー』(ページ 144)

6.4.1 「Configuration」メニュー

「Configuration」メニューを使用してデバイスを構成し、接続の準備を行うことができます（図 6-30）。「Configuration」メニューは、「Password」オプションと「User Settings」オプションが追加されていることを除いては、CP20 のローカル・インターフェースと同一です。

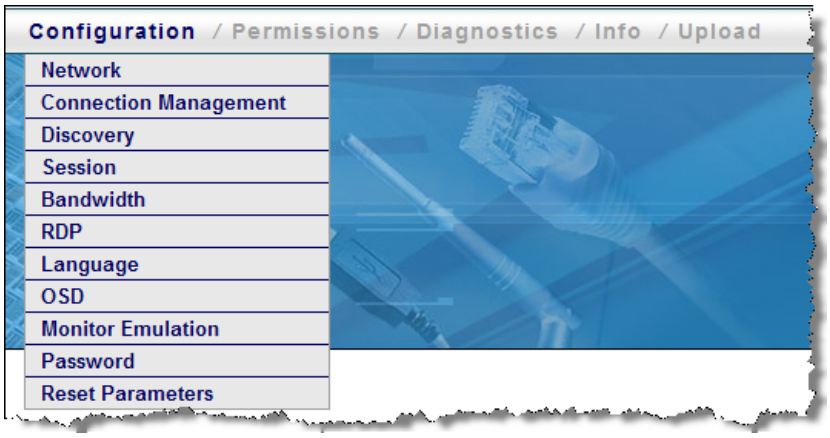


図 6-30 「Configuration」メニュー

CP20 ローカル・インターフェースと同様、「Configuration」メニューの設定値について重要なことは、次のように状況に応じて一部のサブメニュー項目のフィールドが無視されることです。

- コネクション・ブローカーを使用可能にすると (つまり、「Connection Management」ウィンドウで**「Enable Connection Management」**を選択すると)、「Discovery」ウィンドウと「Session」ウィンドウのフィールドがすべて無視されます。
- 検出を使用可能に設定すると (つまり、「Connection Management」ウィンドウで**「Enable Connection Management」**を選択せず、「Discovery」ウィンドウでは**「Enable Discovery」**を選択)、「Session」のフィールドがすべて無視されます。
- コネクション・ブローカーを使用可能にしたか、検出を使用可能にしたか、「Session」ウィンドウでセッション・タイプとして**「PCoIP」**を選択した場合は、「RDP」ウィンドウの内容が無視されます。

次に、これらの構成メニュー項目のそれぞれについて詳しく説明します。

- 127 ページの 『「Network」オプション』
- 128 ページの 『「Connection Management」オプション』
- 129 ページの 『「Discovery」オプション』
- 129 ページの 『「Session」オプション』
- 131 ページの 『「Bandwidth」オプション』
- 132 ページの 『「RDP」オプション』
- 132 ページの 『「Language」オプション』
- 133 ページの 『「OSD」オプション』
- 133 ページの 『「Monitor emulation」オプション』
- 135 ページの 『「Password」オプション』
- 135 ページの 『「Reset Parameters」オプション』

「Network」オプション

「Network」オプション (図 6-31) を使用して、デバイスの IP 設定値を構成できます。このオプションは、CP20 および HC10 の両方で同じですが、例外として CP20 の場合はイーサネット・モードを選択できます。このモードでは、「Auto」または「100 Mbps Full-Duplex」のどちらかを選択できます。

ヒント : CP20 と HC10 の Web インターフェースは同じレイアウトですが、これらのインターフェースは別々のものです。つまり、例えば IP アドレスの取得に DHCP を使用するように両方のデバイスを構成するには、*両方の* Web インターフェースで別々にこの構成を行う必要があります。

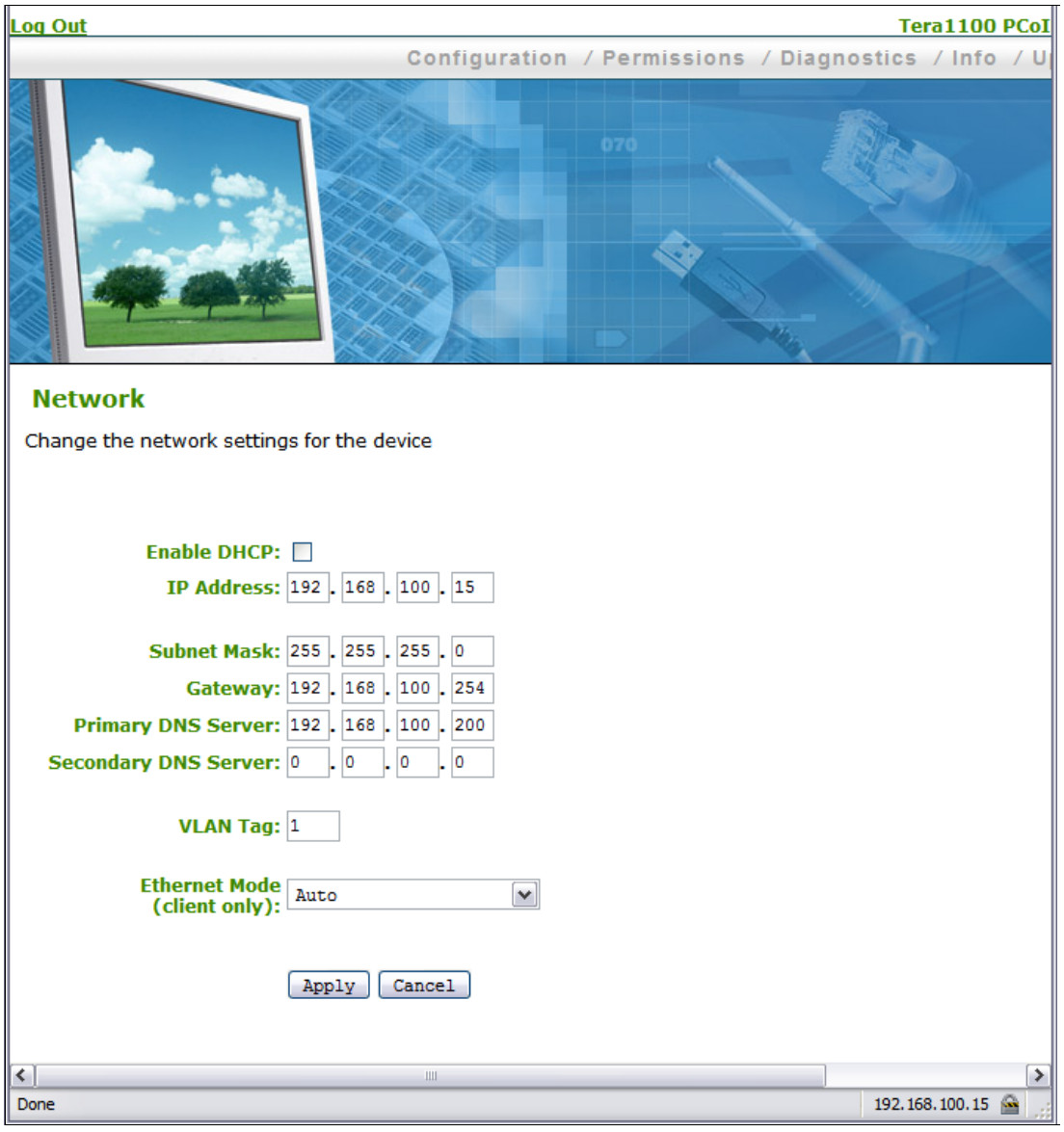


図 6-31　「Network」オプション (HC10 と CP20 の両方)

「Network」オプションによって、DHCP または固定アドレスのどちらを使用するか選択できます。デフォルトは DHCP に設定されており、ボックスはすべて使用不可になります。使用不可になっているボックスは、DHCP によって割り当てられた IP アドレスを示します。

固定アドレスを使用するようにデバイスを構成するには、「Enable DHCP」チェック・ボックスをクリアします。その後、IP アドレス、サブネット・マスク、ゲートウェイ、および 1 次と 2 次の DNS サーバーを入力できます。

「Connection Management」オプション

「Connection Management」オプション (図 6-32) を使用すると、接続管理ソフトウェアによってデバイスを構成できるようになります。

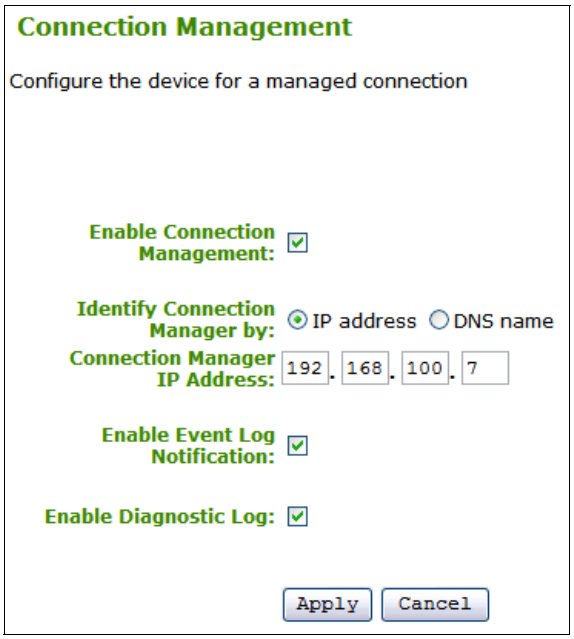


図 6-32 「Connection Management」オプション (HC10 と CP20 の両方に表示される)

「**Enable Connection Management**」を選択すると、CP20 は HC10 への接続を確立するために、コネクション・ブローカー・ソフトウェアへの接続を試みます。コネクション・ブローカー・ソフトウェアを手動で構成する場合は、コネクション・ブローカーの IP アドレスを使用して接続するか、完全修飾ドメイン・ネーム (FQDN) を使用して接続するかを選択する必要があります。

IP アドレスを使用するには、「**IP Address**」を選択し、該当するフィールドに IP アドレスを入力します。FQDN の場合は、「**DNS name**」を選択して、ドメイン・ネームを入力します。

また、イベント・ログに関するオプションが 2 つあります。

- 「**Enable Event Log Notification**」を選択できます。このオプションを選択すると、デバイスはイベント・ログ・メッセージをコネクション・ブローカーに送信します。受信したメッセージがすべて送信されるまで、1 分に約 1 回、一度に 10 件までのメッセージが送信されます。デバイスの電源をオフにしてからオンにしたとき、およびリセット後は、イベント・ログが消去されます。
- 「**Enable Diagnostic Log**」は、診断目的のみに使用されます。この場合、コネクション・ブローカーにメッセージは送信されません。

ヒント：「Connection」ウィンドウで「**Enable Connection Management**」を選択すると、「Discovery」ウィンドウ、「Session」ウィンドウ、および「RDP」ウィンドウの内容がすべて*無視されます*。これら 3 つのウィンドウは、ピアツーピア構成専用です。コネクション・ブローカーとピアツーピア接続の使用は相互に排他的なオプションなので、これらのパラメーターは使用されません。

「Discovery」オプション

「Discovery」オプションを使用すると、ピアツーピア接続を使用可能に設定して、接続可能な HC10 を接続時に自動的に検索できます (図 6-33)。このオプションと「Session」オプションを使用すれば、コネクション・ブローカーを使用せずに CP20 から HC10 に直接接続できます。

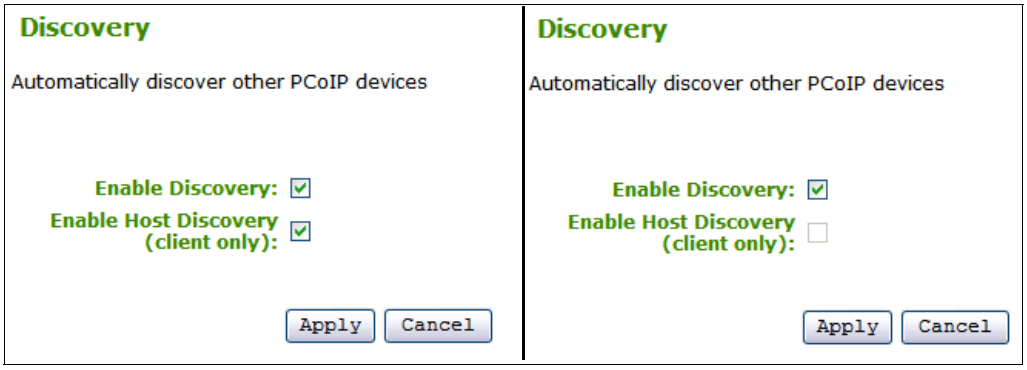


図 6-33　CP20 (左) および HC10 (右) の Web インターフェースの「Discovery」オプション

このオプションを使用して構成できるオプションは 2 つあります。ディスカバリー・オプションを使用するには、CP20 の場合は「**Enable Discovery**」と「**Enable Host Discovery**」の両方を選択し、HC10 の場合は「**Enable Discovery**」を選択する必要があります。これらのオプションを選択すると、接続先の HC10 を選択するオプションが表示されます。このオプションを表示する際に、CP20 は使用可能な HC10 を検出して、図 6-34 に示すように接続可能な HC10 のリストを作成します。このリストから、接続する HC10 を選択できます。

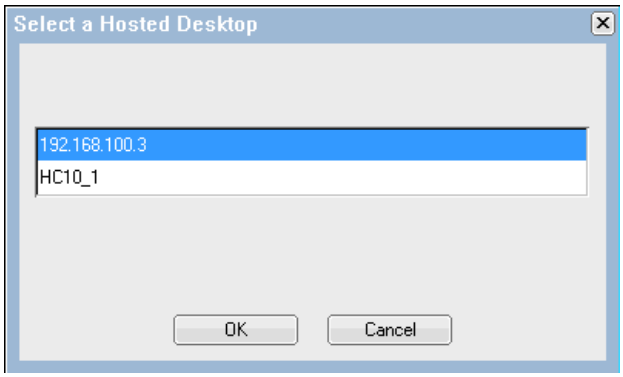


図 6-34　接続可能な HC10 のリスト

注 : 110 ページの図 6-11 に示した「Connection」タブで「**Enable Connection Management**」を選択した場合、ディスカバリー機能は使用されず、このタブの設定値は *無視されます。*

「Discovery」オプションについて詳しくは、『6.5.3, ディスカバリー・オプションを使用した HC10 への接続』(ページ 149) を参照してください。

「Session」オプション

「Session」オプション (図 6-35 に示す) では、この CP20 から接続したい特定の HC10 の IP アドレスと MAC アドレスを手動で指定して、ピアツーピア・セッションを構成できます。

ピアツーピア接続の使用法について詳しくは、『6.5, ピアツーピア接続のセットアップ』(ページ 145) を参照してください。

注 : このオプションのフィールドをアクティブにするには、「Discovery」オプションの「**Enable Discovery**」を*使用不可*に設定し、「Connection Management」オプションの「**Enable Connection Management**」を*使用不可*に設定する必要があります。これらのどちらかのオプションが使用可能に設定されていると、「Session」オプションのすべてのフィールドが*無視されます*。

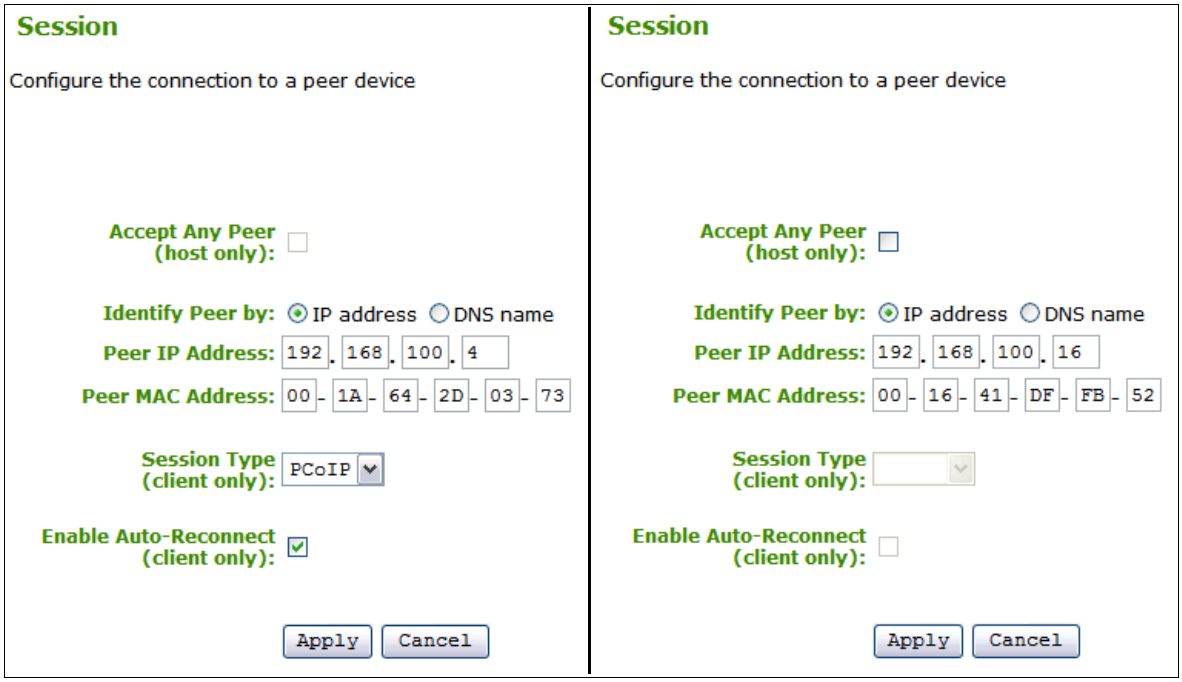


図 6-35 CP20 (左) および HC10 (右) の Web インターフェースの「Sessions」オプション

図 6-35 に示したように、HC10 (ホスト) のみに適用されるフィールドは CP20 (クライアント) 内では使用不可になり、その逆も同様です。

CP20 (図の左側) 上では、HC10 の IP アドレス、または完全修飾ドメイン・ネーム (FQDN) のどちらかが分かっていれば、ピアツーピア接続を確立できます。IP アドレスを使用するには、「**IP Address**」を選択し、HC10 圧縮カードの IP アドレスを該当するフィールドに入力します。FQDN を使用するには、「**FQDN**」を選択して、ドメイン・ネームを入力します。

HC10 の圧縮カードの MAC アドレスも入力する必要があります。圧縮カードの MAC アドレスを判別するには、次の 2 とおりの方法があります。

- HC10 をブートし、F1 を押して BIOS に入ります。次に、「**Advanced Settings**」→「**Compression Card Network Configuration**」を選択します。ダイアログ・ボックスが開き、MAC アドレスが表示されます。
- 図 6-35 に示した MAC アドレスの無効な値をそのままにして、HC10 への接続を試みます。接続は失敗し、「`Session Refused!`」というメッセージが表示されます。その後、「**Options**」→「**Diagnostics**」をクリックします。イベント・ログに 2 つの項目が示されます。1 つは無効な MAC アドレスをリストし、もう 1 つは予期されていた MAC アドレスをリストするものです。その予期されていたアドレスを図 6-35 のフィールドにコピーします。例えば、すべてゼロからなる仮の MAC アドレスを指定すると

(00-00-00-00-00-00)、イベント・ログには例 6-2 に示すようなメッセージが表示されます。

例 6-2 圧縮カードの正しい MAC アドレスを示すエラー・ログ・メッセージ

```
Connecting with host (9.42.170.185, 00-00-00-00-00-00)
Peer MAC mismatch:(00-1A-64-2D-02-EE, 00-00-00-00-00-00)
```

この例での正しい MAC アドレスは、00-1A-64-2D-02-EE です。

HC10 上では、「**Accept any Peer**」を選択することによって、すべての CP20 がこの HC10 に接続することを許可できます。また、特定の 1 つの CP20 のみを対象に接続を許可する場合は、「**Accept any Peer**」がクリアされた状態のまま、前述のとおりフィールドに入力します。「Information」パネルから、CP20 の MAC アドレスを確認できます (122 ページの図 6-24 を参照)。

注 : 将来のファームウェア更新によって、MAC アドレスの入力は不要になる可能性があります。

セッション・タイプは PCoIP または RDP のどちらかですが、HC10 に接続するにはこのオプションを PCoIP に設定する必要があります。このフィールドは、CP20 の場合のみ有効です。

「Enable Auto-Reconnect」オプションを選択すると、CP20 の電源がオンになったときに、CP20 は最後に接続した HC10 への接続を自動的に試行するように構成されます。CP20 はブート時にのみ再接続を試み、セッションの切断後は再接続しません。

このウィンドウのフィールドは、接続管理または検出が使用可能に設定されている場合は使用されません。設定値の構成は可能ですが、これらのオプションのどちらかが使用可能に設定されていると、このタブは無視されます。

「Bandwidth」オプション

「Bandwidth」オプションを使用して、デバイスの帯域幅制限を設定できます (図 6-36)。帯域幅制限を変更するには、最大 Mbps 数を入力するか、制限なしを表すゼロ (0) を入力します。

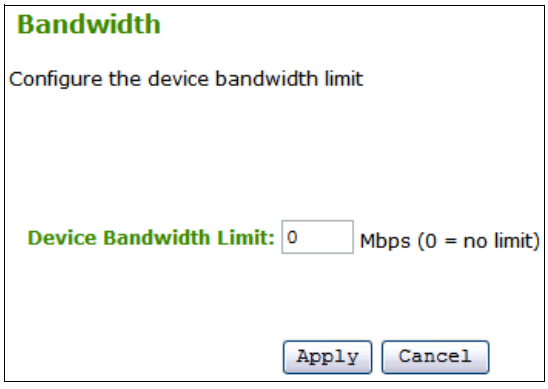


図 6-36 HC10 と CP20 の Web インターフェースの「Bandwidth」オプション

HC10 内での設定は、ダウンストリーム帯域幅を制御し、そのほとんどはビデオ・トラフィックが占めています。CP20 内での設定は、アップストリーム帯域幅を制御し、そのほ

とんどは USB トラフィックが占めています。この値は 0 のままにすることをお勧めします。このようにすれば、デバイスが必要に応じて帯域幅を動的に割り振ります。

「RDP」オプション

図 6-37 に示す「RDP」オプションを使用すると、RDP 接続の解像度、ビット深さ、およびターミナル・サーバー・ポートを構成できます。これらの変更はクライアント・サイドでのみ実行できます。

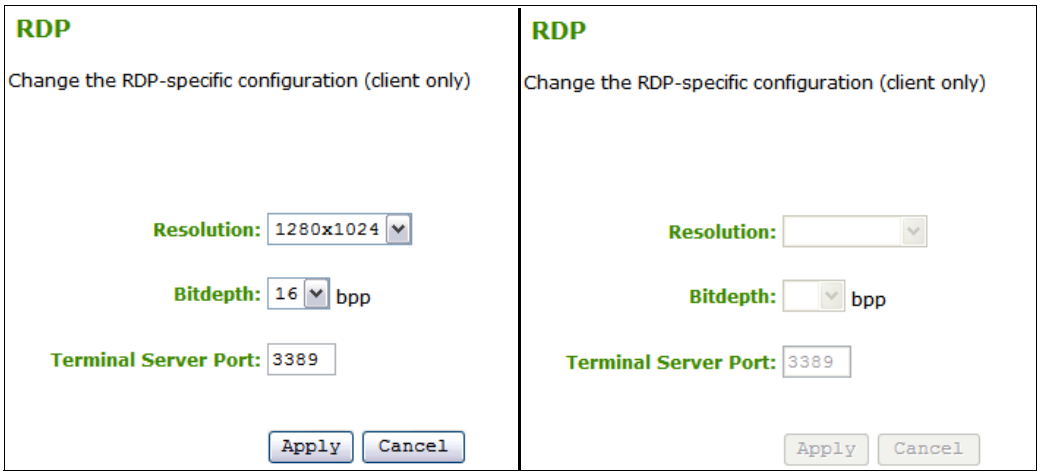


図 6-37　CP20 (左) および HC10 (右) の Web インターフェースの「RDP」オプション

このウィンドウのフィールドは、「Session」オプションでセッション・タイプとして RDP を指定しない限りは無視されます。CP20 から HC10 に接続する構成の場合、セッション・タイプは常に PCoIP なので、このタブは使用されません。

「Language」オプション

「Language」オプションを使用して、CP20 の言語を設定し、キーボード・レイアウトを設定できます (図 6-38)。言語またはキーボード・レイアウトを設定するには、ドロップダウン・メニューから該当するオプションを選択します。

図 6-38　「Language」オプション (HC10 と CP20 の両方)

このオプションは、CP20 の場合のみ有効です。本書の執筆時点では、CP20 の言語オプションはただ 1 つ (英語) です。キーボード・レイアウトは、「English U. S.」と「French Canada」のどちらかを選択できます。

注：「Language」タブの設定値は、HC10 上の Windows で定義した言語設定に影響を与えません。これらの設定値の対象は、CP20 のローカル・インターフェースと Web インターフェースのみです。

「OSD」オプション

「OSD」オプションを使用すると、スクリーン・セーバーとして表示されるメッセージを入力でき、スクリーン・セーバーのタイムアウトを設定できます。このオプションは、CP20 の場合のみ有効です。HC10 インターフェースでは、ボタンとテキスト・ボックスは使用不可になります。図 6-39 を参照してください。

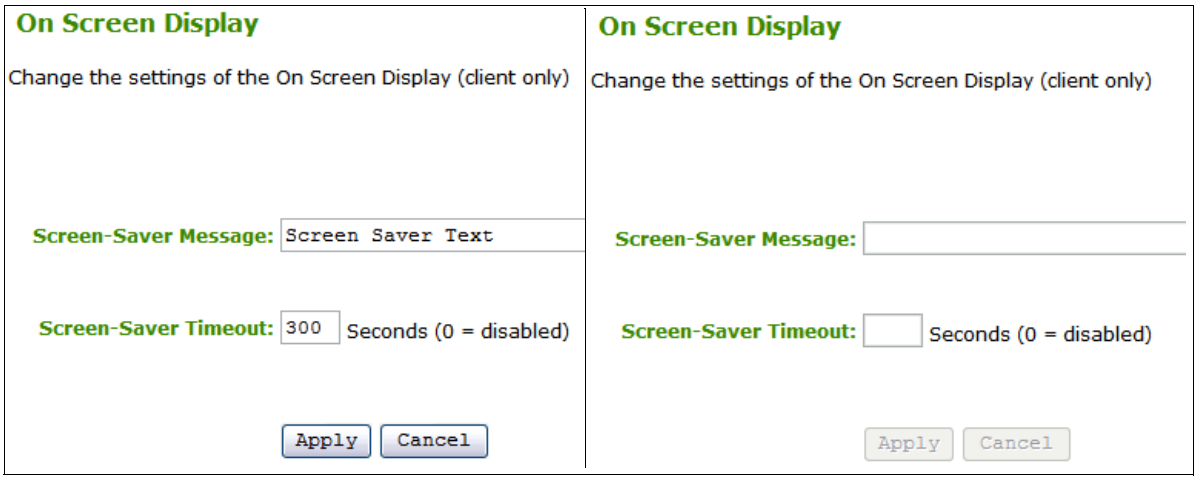


図 6-39　CP20 (左) および HC10 (右) の Web インターフェースの「OSD」オプション

デフォルトのスクリーン・セーバー・テキストは Screen Saver Text で、デフォルトのタイムアウトは 300 秒 (5 分) に設定されています。

テキストを変更するには、「**Screen-Saver Text**」フィールドに新しいテキストを入力します。スクリーン・セーバーが使用されるまでの待ち時間を変更することもできます。このためには、「**Screen-Saver Timeout**」フィールドに新しい数値を入力します。このタイムアウトは秒数で入力し、ゼロ (0) を入力するとスクリーン・セーバーが使用不可になります。

実際のスクリーン・セーバーは、黒の背景に単純な白いテキストを表示するもので、テキストは画面にランダムに配置されます。このスクリーン・セーバーは、HC10 に対するアクティブ・セッションがない場合にのみ使用されます。

「Monitor emulation」オプション

「Monitor emulation」オプションは、HC10 上で使用可能に設定できる機能です (図 6-40 を参照)。この機能を使用可能に設定すると、CP20 ワークステーション・コネクション・デバイスがセッションを行っていなくても、モニターが接続されていることが HC10 上の圧縮カードからビデオ・カードに通知されます。

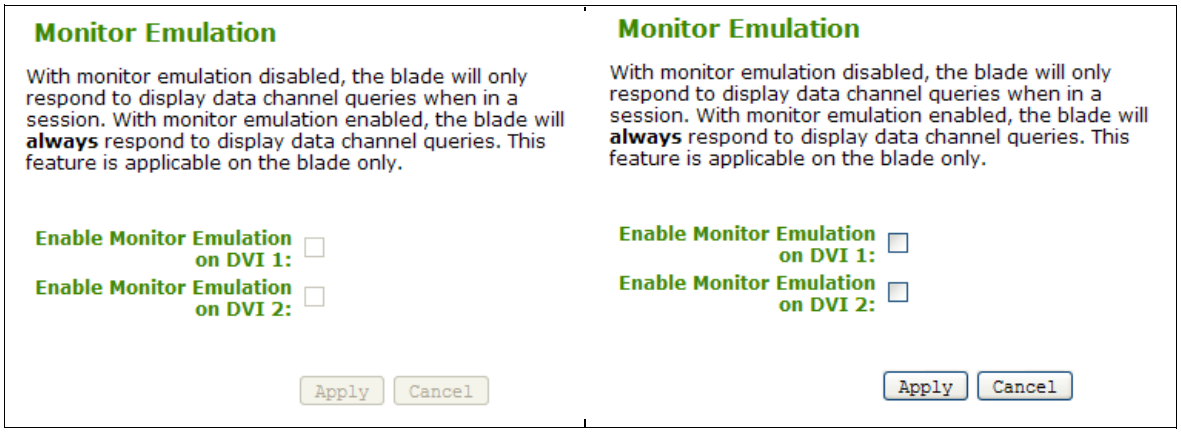


図 6-40　CP20 (左) および HC10 (右) の Web インターフェースの「Monitor Emulation」オプション

このオプションを使用可能に設定することをお勧めします。この HC10 に接続する CP20 デバイスに 2 台のモニターが接続されている場合は、図 6-40 に示したボックスを両方とも選択する必要があります。それぞれの CP20 に接続されているモニターが 1 台のみならば、そのモニターのボックスのみを選択します。

この機能は、圧縮カードに電源が供給されたときにビデオ・カードにデジタル EDID (extended display identification data) を提供することによって、モニターをエミュレートします。この機能によって、CP20 とのセッションを行う前に EDID が使用可能になるので、ビデオ・カードが EDID を受信して、CP20 に接続されたモニターにビデオを表示するタイミングを合わせるために役立ちます。デスクトップの表示後にセッションが接続されたとき、およびブレードの電源をオフにせずにセッションの切断と再接続が行われたときに、ビデオを表示できるようになります。

注 : モニター・エミュレーションを使用可能に設定した後、この機能を活動化する前に HC10 を再起動する必要があります。

構成に関する注 :

- CP20 の背面では、上部の DVI ポートが *DVI 1*、下部のポートが *DVI 2* です。38 ページの図 3-7 を参照してください。
- DVI 1 と DVI 2 の両方に対してモニター・エミュレーションを使用可能に設定した場合、DVI 2 にビデオを表示するには、その前に NVIDIA ドライバー内でも第 2 のモニターを使用可能に設定する必要があります。
- 同じ CP20 を使用して複数の HC10 ワークステーション・ブレードに接続する場合は、モニター・エミュレーションを同じ方法で使用可能に設定する必要があります。

注 :

- 両方の DVI ポート上でモニター・エミュレーションを使用可能に設定すると、BladeCenter アドバンスト・マネージメント・モジュールのローカル・コンソール、またはブラウザー・ベースのリモート・コンソールを使用して HC10 のビデオを表示できなくなります。これは、ビデオ・カードがサポートするモニターが 2 台のみで、DVI 接続が優先されるからです。
- モニターが DVI ポート 1 に接続されているときにモニター・エミュレーションを使用可能に設定した場合も、BladeCenter アドバンスト・マネージメント・モジュールのローカル・コンソール、またはブラウザー・ベースのリモート・コンソールを使用して HC10 のビデオを表示できなくなります。この機能は、セキュリティー上の理由でこのように

設計されています。AMM コンソール (ローカルまたはリモート) を使用できるようにするには、モニターを DVI 2 に接続してください。

- モニター・エミュレーションを使用可能に設定したポートが 1 つのみでも、両方のポートにモニターが接続されている場合は、NVIDIA コントロール・パネルを使用して、オペレーティング・システム内で第 2 のモニターを手動で使用可能に設定する必要があります。
- NVIDIA FX 1600M 3D ビデオ・カードが取り付けられている HC10 ブレードの場合、DVI ポート上でモニター・エミュレーションを使用可能に設定すると、POST メッセージは表示されなくなります。これは、FX 1600M が POST 中にサポートするモニターが 1 台のみであるためです。

ビデオとモニター・エミュレーション機能に関連した RETAIN ヒントのリストは、『4.6.2, その他のビデオに関するヒント』(ページ 62) を参照してください。

「Password」オプション

「Password」オプションを使用して、HC10 または CP20 のパスワードを設定できます (図 6-41)。デフォルト・パスワードは PASSW0RD (英文字の *O* ではなくゼロを含む) です。セキュリティー対策として、デバイスすべてのパスワードを変更することをお勧めします。

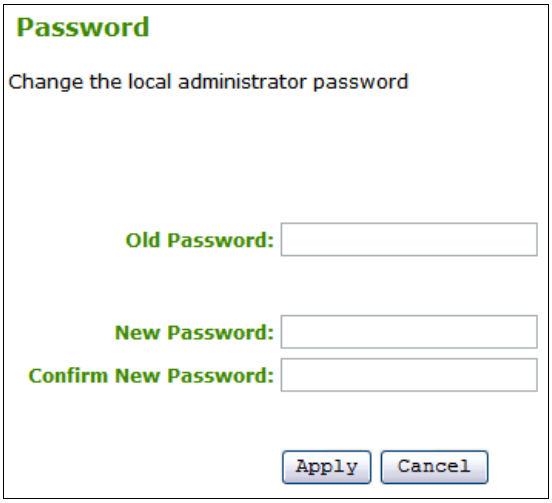


図 6-41 「Password」オプション (HC10 と CP20 の両方)

注 : ここでパスワードを変更すると、ローカル CP20 インターフェースへの接続に使用されるパスワードも変更されます。

「Reset Parameters」オプション

「Configuration」メニューの最後のオプションは、「Reset Parameters」です (図 6-42)。このオプションを使用して、すべての構成と許可をデフォルトにリセットできます。これにより、デバイスは DHCP を使用し、コネクション・ブローカーと組み合わせて使用できる状態に戻ります。パラメーターをリセットするには、**「Reset」**をクリックします。

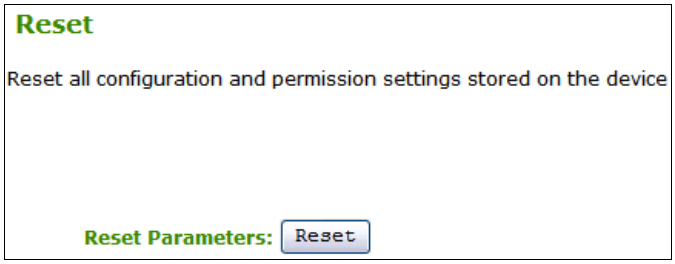


図 6-42　「Reset Parameters」オプション (HC10 と CP20 の両方)

注 : このリセット・オプションによって、ログイン・パスワードも PASSW0RD (英文字の *O* ではなくゼロを含む) にリセットされます。

6.4.2 「Permissions」メニュー

図 6-43 に示す「Permissions」メニューを使用して、次のようにさまざまな許可を設定できます。

- CP20 の USB ポートに接続できる USB デバイス
- HC10 からのオーディオを CP20 に送るかどうか
- CP20 に対する HC10 リモート電源ボタンの動作

図 6-43　HC10 と CP20 の Web インターフェースの「Permissions」メニュー

USB

「USB」ウィンドウでは、CP20 に取り付けて使用することを許可する USB デバイスを構成できます (図 6-44)。この構成オプションには、CP20 Web インターフェースからのみアクセスできます。ドロップダウン・リストから、使用を許可するデバイスのタイプを選択できます。

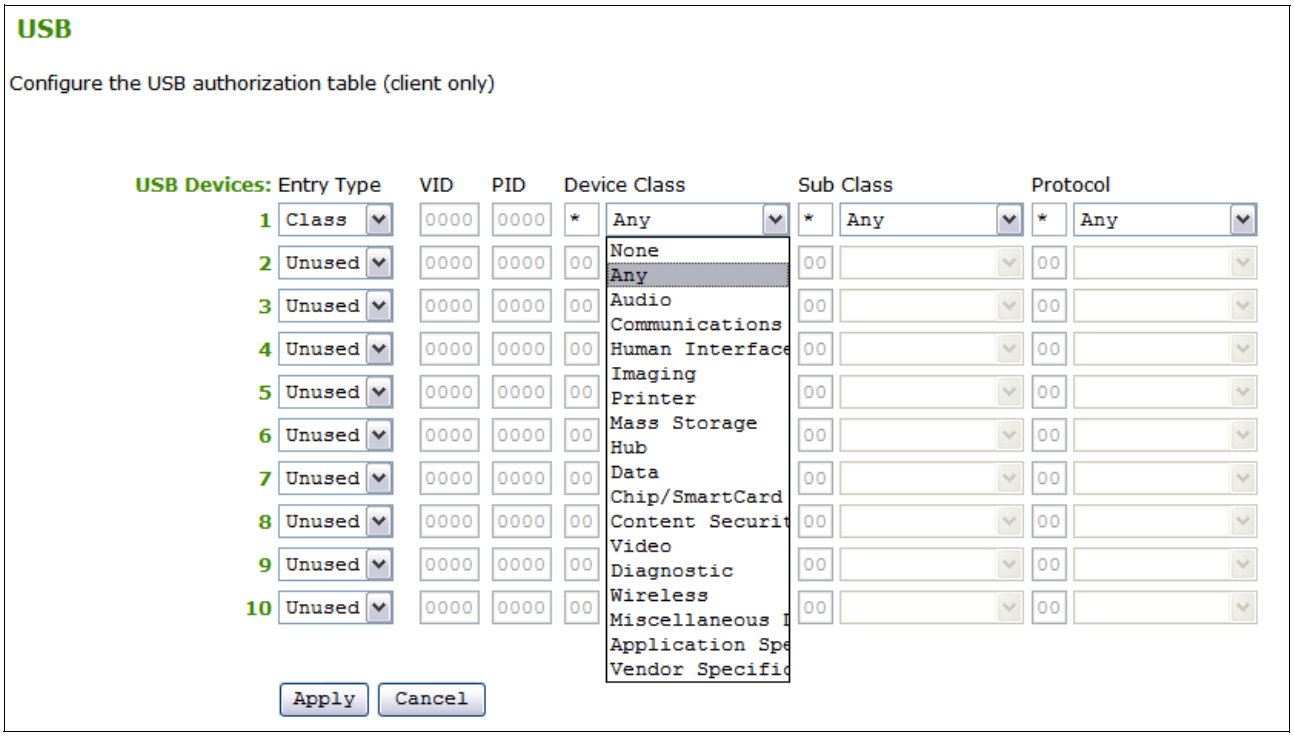


図 6-44　CP20 上での使用を許可するさまざまなタイプのデバイスを示す「USB」オプション

USB 許可テーブルは、セキュリティーや制御を強化する機能として提供されています。デフォルトではすべての USB デバイス・タイプが許可されていますが、セキュリティーのために、許可するデバイスを厳密に指定できます。許可していないその他すべての USB デバイスは、挿入されても単に無視されます。

図 6-44 に示したとおり、許可する USB デバイスのタイプは「Device Class」列で指定します。例えば、ユーザーがキーボードとマウスのみを接続できるようにするには、「Device Class」ドロップダウン・リストから**「Human Interface Devices」**を選択し、「Class」と「Protocol」は**「Any」**のままにします。10 個の行を使用して、複数のデバイスに対する許可を与えることができます。

ドロップダウン・リストの最初の列からは、3 つの項目タイプを選択できます。

- 必要ない行に対しては、**「Unused」**オプションを選択する必要があります。
- **「ID」**オプションを使用すると、許可したい特定のデバイスの VID と PID を入力できます。これらの値を確認するには、すべての USB デバイスを許可し、特定のデバイスを接続して、「Attached Devices」オプションを表示します (143 ページの 『「Attached Devices」オプション』を参照)。その後、項目タイプとして「ID」を選択し、デバイスの VID と PID の番号を該当するフィールドに入力します。
- **「Class」**項目タイプを使用すると、許可したいデバイスに対応するデバイス・クラスをリストから選択できます (137 ページの図 6-44 を参照)。デバイスが許可されていない場合は、その USB デバイスが CP20 に接続されても影響はありません。デバイスは挿入されたものと見なされません。

サム・ドライブなど特定の USB デバイスの使用を制限する場合は、USB ハブの使用も不可にすることが非常に重要です。ユーザー識別、クラス・タイプなどに基づくデバイスの許可は、ポートごとに行われます。つまり、ハブの使用を許可すると、以後ハブ経由で接続されるあらゆるタイプのデバイスが、他の USB 許可に関係なく許可されます。

「Audio」オプション

ユーザーがスピーカーとマイクロホンを使用するには、HC10 と CP20 の両方でオーディオを使用可能に設定する必要があります。

注 : オーディオはデフォルトでは使用不可に設定されています。

「Audio」オプションには、HD オーディオを使用可能に設定するためのオプションもあります (図 6-45 を参照)。

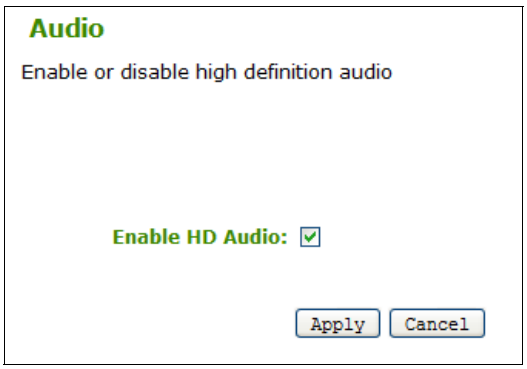


図 6-45 「Audio」オプション (CP20 と HC10 の両方)

ユーザーに対してオーディオを使用可能に設定するには、CP20 と HC10 の両方でこのパラメーターを使用可能に設定する必要があります。どちらかのオプションをクリアすると、オーディオは使用できなくなります。HC10 でこのオプションをクリアすると、オーディオ・デバイスは Windows に認識されなくなります。

HC10 でこの設定値を変更する場合 (使用可能または使用不可に設定)、この変更を有効にするには、その前に HC10 をリブートする必要があります。

「Power」オプション

図 6-46 に示す「Power」オプションは、CP20 の前面にある HC10 リモート電源ボタンが押されたときの動作を制御します (38 ページの図 3-7 を参照)。

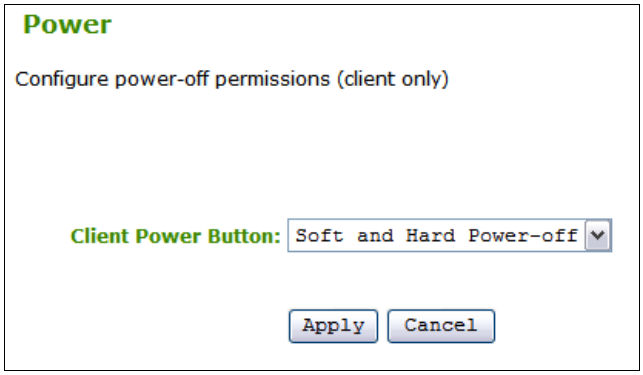


図 6-46 「Power」オプション (CP20 のみ)

「Power」オプションは次のとおりです。

- *Power-off not permitted*: CP20 のボタンを押しても何も起こりません。
- *Soft power-off only*: ボタンを押すとオペレーティング・システムのシャットダウンが実行され、その後 HC10 がオフになります。

- *Hard power-off only*: ボタンを 4 秒以上押すと、HC10 が即時にオフになり、その前にプロセスの終了やシャットダウンを待機しません。ボタンを 4 秒より短く押した場合は、何も起こりません。
- *Soft and hard power-off*: ソフト電源オフまたはハード電源オフのどちらかを実行できます。ソフト電源オフを行うには、ボタンを 4 秒より短く押す必要があります。ハード電源オフを行うには、ボタンを 4 秒より長く押す必要があります。

6.4.3 「Diagnostics」メニュー

次に、「Diagnostics」メニューのオプションについて説明します (図 6-47)。

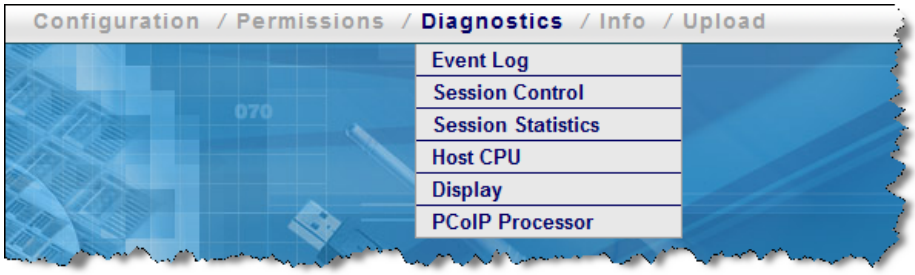


図 6-47 HC10 と CP20 の Web インターフェースの「Diagnostics」メニュー

「Event Log」オプション

「Event Log」オプションには、イベント・ログを表示または消去するためのボタンが 2 つあります (図 6-48)。

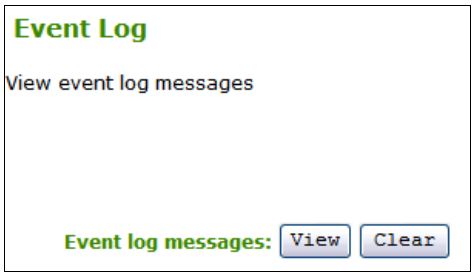


図 6-48 HC10 と CP20 の Web インターフェースの「Event Log」オプション

イベント・ログを表示するには、**「View」**をクリックします。ログ情報を表示する新規ブラウザー・ウィンドウが開きます。

イベント・ログを消去するには、**「Clear」**をクリックします。

「Session Control」オプション

「Sessions Control」オプションを選択すると、アクティブな接続の有無が示され、デバイスを接続または切断できます (図 6-49)。

図 6-49　HC10 と CP20 の Web インターフェースの「Session Control」オプション

デバイスが接続されている場合は、「**Disconnect**」をクリックしてセッションを切断できます。これは、CP20 の前面にあるセッション切断ボタンを押すことと同じです (38 ページの図 3-7 を参照)。接続が切断状態であることが示されている場合は、「**Connect**」ボタンをクリックでき、クリックすると既に構成済みの方式を使用して接続が行われます。

「Session Statistics」オプション

「Session Statistics」オプションは、現行セッションの統計を表示するか、アクティブ・セッションが存在しない場合には切断状態であることを示します (図 6-50)。

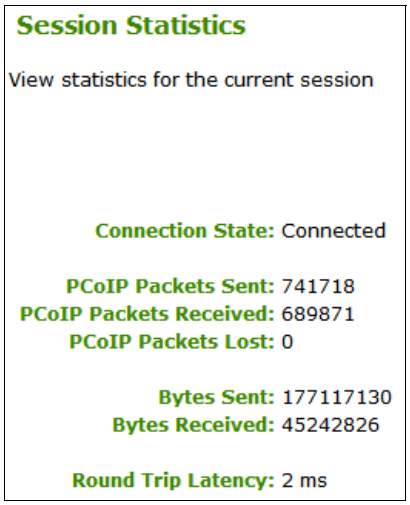


図 6-50　HC10 と CP20 の Web インターフェースの「Session Statistics」オプション

このオプションを選択すると、送信済み、受信済み、および破損した PC-over-IP パケットの数を確認できます。また、送受信されたバイト数も表示されます。さらに、往復遅延時間を ms 単位で表示します。これは、パケットが HC10 の圧縮カードから CP20 の圧縮カードまで移動し、戻ってくるまでにかかる待ち時間です。

「Host CPU」オプション

「Host CPU」オプションを選択すると、ホストの識別を確認したり、現在の電源状態を表示および変更したり、ホスト CPU をリセットしたりすることができます。これらのオプションは、HC10 の場合のみ有効です。図 6-51 を参照してください。

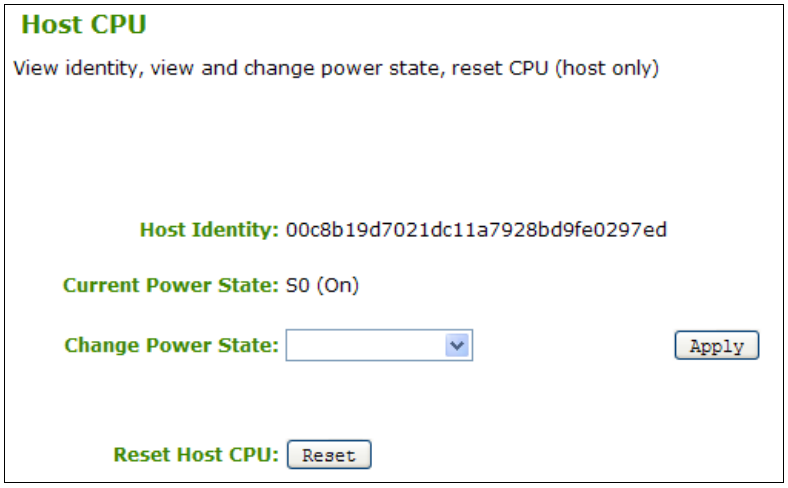


図 6-51　HC10 の Web インターフェースの「Host CPU」オプション (HC10 のみ)

「Host Identity」は、CP20 に接続された HC10 を一意的に識別します。

「Current Power State」フィールドは、HC10 の現在の状態をリストします。可能な状態は次のとおりです。

- S0 (電源オン)
- S1 (スリープ)
- S2 (スリープ)
- S3 (スタンバイ)
- S4 (ハイバネート)
- S5 (電源オフ)

「Change Power State」フィールドを使用して、ホスト・コンピューターの電源状態を変更できます。状態は次のように変更できます。

- S0 (オン): HC10 の電源をオンにします。
- S3 (ソフト・オフ): 制御された OS のシャットダウンによって HC10 のソフト電源オフを実行します。
- S3 (ハード・オフ): OS の関与なしに HC10 のハード・シャットダウンを実行します。

「Display」オプション

「Display」オプションを使用すると、CP20 の画面にテスト・パターンが表示されます。このオプションは、HC10 の場合は使用不可で、CP20 の場合のみ選択可能です。図 6-52 を参照してください。

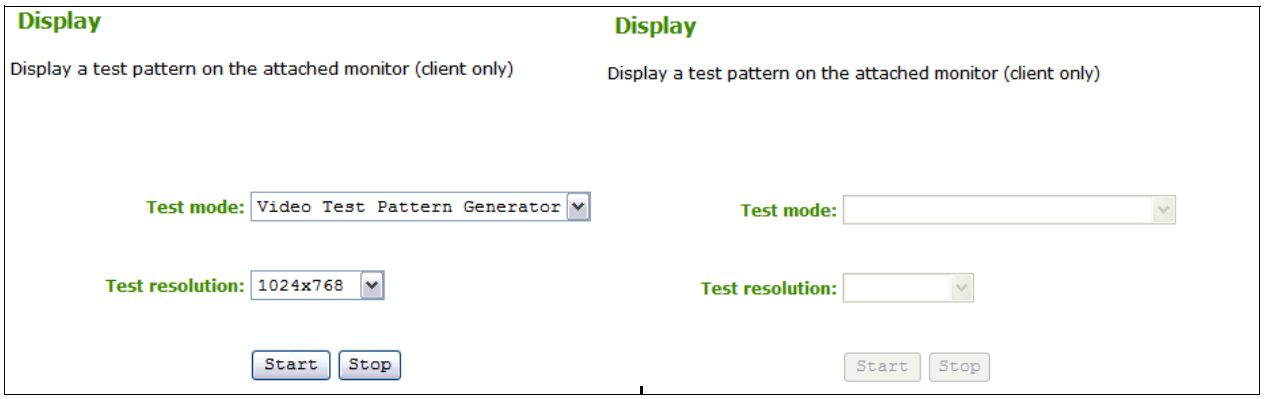


図 6-52　CP20 (左) および HC10 (右) の Web インターフェースの「Display」オプション

テスト・モードには 2 つのオプションがあり、それぞれ CP20 上でパターンを生成します。

- Video Test Pattern Generator
- Pseudo Random Bitstream

また、テスト用解像度のドロップダウン・リストもあり、次に示す解像度を選択できます。

- 1024x768
- 1280x1024
- 1600x1200
- 1920x1200

該当するテスト・モードと解像度を選択した後、「**Start**」をクリックします。CP20 のディスプレイにテストが表示されます。テストを停止するには、「**Stop**」をクリックします。

「PCoIP Processor」オプション

「PCoIP Processor」オプションを使用すると、前回のブートから経過した時間が表示され、PC-over-IP プロセッサーをリセットできます。構成作業によっては PC-over-IP プロセッサーをリセットするようにプロンプトで指示されることがあり、ここでリセットを行うことができます。プロセッサーをリセットするには、「**Reset**」をクリックします。図 6-53 を参照してください。

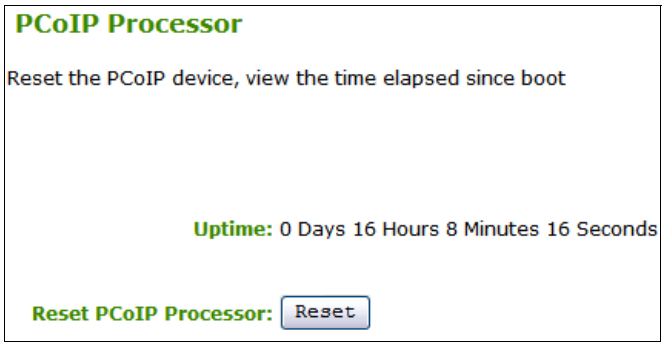


図 6-53　HC10 と CP20 の Web インターフェースの「PCoIP」オプション

リセットするデバイスが CP20 ならば、PC-over-IP プロセッサーが即時にリセット (再起動) されます。HC10 圧縮カード上の PC-over-IP プロセッサーをリセットする場合、リセットは HC10 が次にシャットダウンするか、リブートするか、スタンバイまたはハイバネーション状態になるときに行われます。

6.4.4 「Info」メニュー

次に、「Info」メニューのオプションについて説明します (図 6-54)。

図 6-54　HC10 および CP20 の Web インターフェースの「Info」メニュー

「Version」オプション

「Version」オプションを使用すると、デバイスに関する情報を表示できます (図 6-55)。

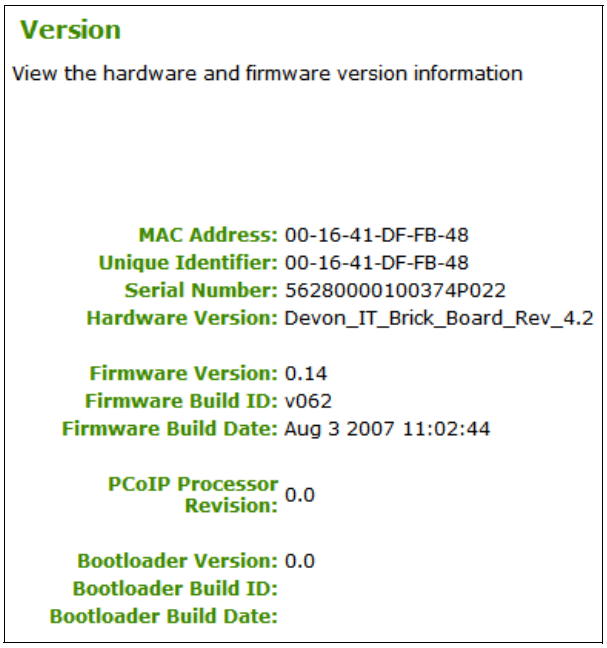


図 6-55 HC10 と CP20 の Web インターフェースの「Version」オプション

このオプションを使用して、HC10 と CP20 の MAC アドレス、シリアル番号、およびハードウェア・バージョンを取得できます。また、HC10 または CP20 が現在使用しているファームウェアのバージョンとビルドを確認するためにも役立ちます。ファームウェアを最新バージョンに保つことはきわめて重要です。さらに、使用されている PC-over-IP プロセッサー、およびブート・ローダーのバージョンに関する情報もあります。

「Attached Devices」オプション

「Attached Devices」オプションを使用すると、接続されているモニターと USB デバイスを表示できます。このオプションは、CP20 の Web インターフェース上でのみ有効です。図 6-56 を参照してください。

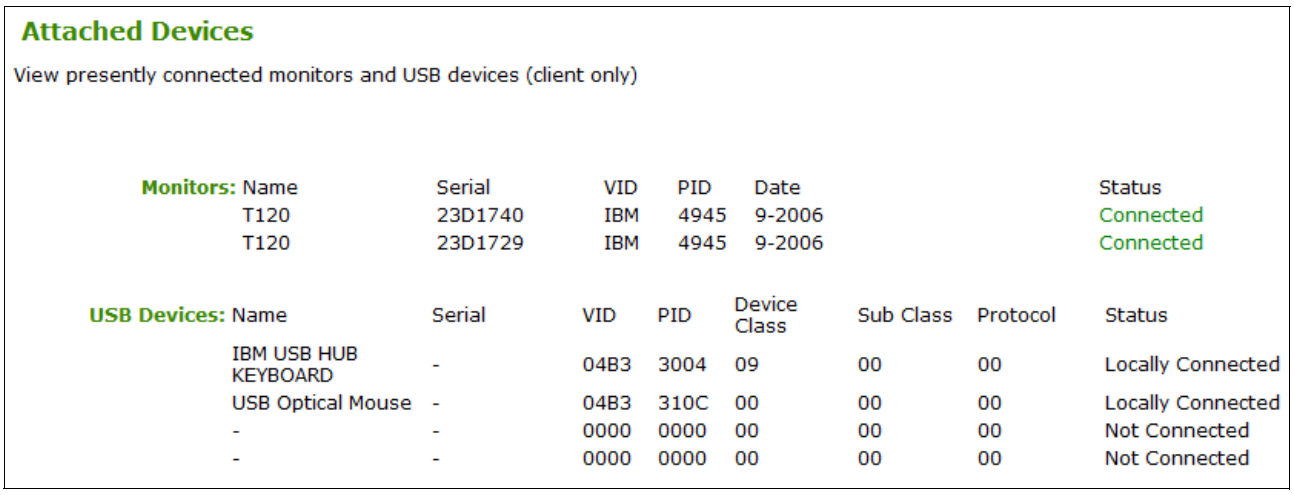


図 6-56 CP20 の Web インターフェースの「Attached Devices」オプション

このオプションは、現在 CP20 に接続されているすべてのモニターと USB デバイスを表示します。これは、USB セキュリティー機能と組み合わせて使用する VID 番号と PID 番号を判別するために非常に便利です (136 ページの 『USB』を参照)。

6.4.5 「Upload」メニュー

次に、「Upload」メニューのオプションについて説明します (図 6-57)。

図 6-57 HC10 および CP20 の Web インターフェースの「Upload」メニュー

「Firmware」オプション

「Firmware」オプションを使用して、CP20 または HC10 に新規ファームウェアをアップロードできます (図 6-58)。該当するファイルを表示して「**Upload**」をクリックします。ファームウェアの更新について詳しくは、『6.6, ファームウェアの更新』(ページ 151) を参照してください。

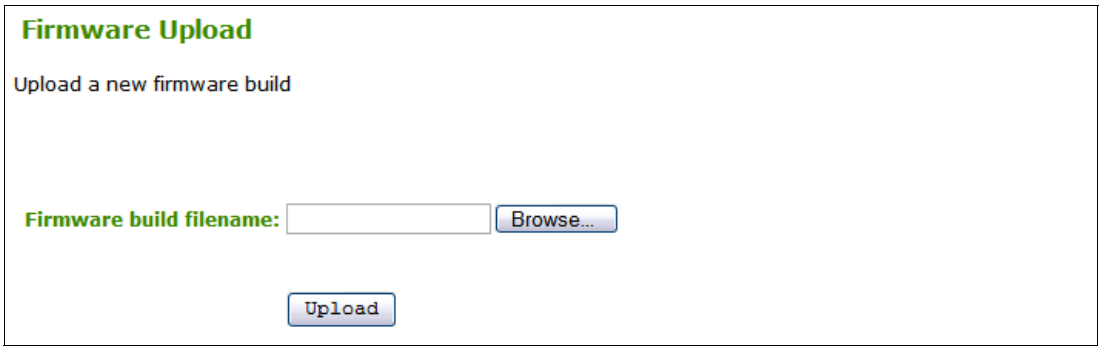


図 6-58 HC10 と CP20 の Web インターフェースの「Firmware」オプション

「Bootloader」オプション

「Bootloader」オプションを使用して、新規のブート・ローダー・ファイルをアップロードできます。ブート・ローダーは、特殊なファームウェアです。該当するファイルを表示して「**Upload**」をクリックします。図 6-59 を参照してください。

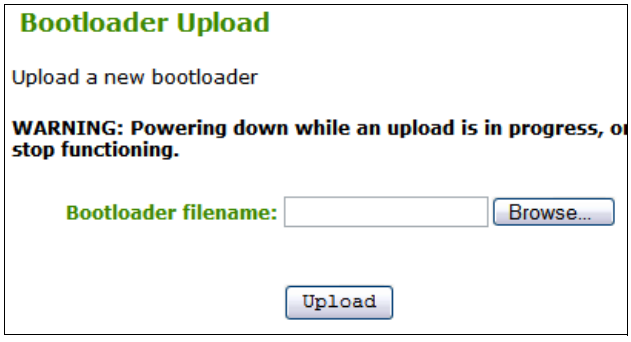


図 6-59 HC10 と CP20 の Web インターフェースの「Bootloader」オプション

「OSD Logo」オプション

「OSD Logo」オプションを使用すると、CP20 ローカル・インターフェースに表示するロゴをアップロードできます (図 6-60 を参照)。

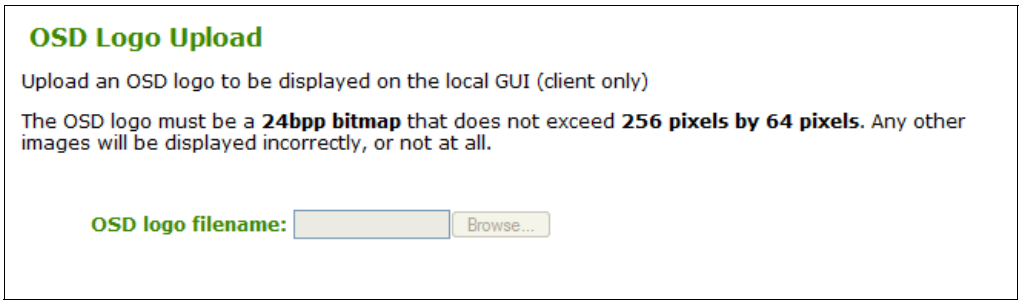


図 6-60 HC10 と CP20 の Web インターフェースの「OSD Logo」オプション

ロゴは 102 ページの図 6-1 の IBM ロゴのように表示されます。画像の要件は次のとおりです。

- 幅 256 ピクセル、高さ 64 ピクセルを超えない
- BMP フォーマット (非圧縮)
- 24 ビット / ピクセルを超えない

6.5 ピアツーピア接続のセットアップ

コネクション・ブローカーを使用せずに CP20 を HC10 に接続したい場合は、ピアツーピア接続を使用できます。HC10 へのピアツーピア接続には 2 とおりの方法があります。

- セッション

  特定の HC10 圧縮カードのホスト名または IP アドレスと、MAC アドレスを使用して接続します。セッション方式について詳しくは、『4.7.2, ピアツーピア接続』(ページ 65) を参照してください。

- ディスカバリー

  使用可能な HC10 を検索し、リストから 1 つ選択して接続します。検出方式について詳しくは、『4.7.2, ピアツーピア接続』(ページ 65) を参照してください。

ほとんどの場合は、コネクション・ブローカー・ソフトウェアの使用が想定されます。ただし、実装されている HC10 が少数 (例えば、14 台以下を収容するシャーシが 1 つ) の場合は、ピアツーピア接続の使用が適しています。

6.5.1 デバイスの IP アドレスと MAC アドレスの確認

選択する接続方式によっては、接続する前に HC10 または CP20 の IP アドレスを確認する必要が生じることがあります。HC10 圧縮カードの IP アドレスと MAC アドレスを確認するには、次の手順で行います。

1. HC10 をブートして BIOS に入ります。
2. **「Advanced Setup」→「Compression Card Network Configuration」**を選択します。
3. 図 6-61 に示すように、IP アドレスと MAC アドレスがリストされます。

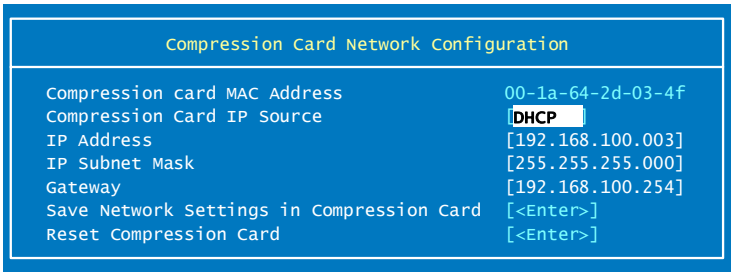


図 6-61　HC10 の圧縮カードの IP アドレス

CP20 の IP アドレスと MAC アドレスを確認するには、次の手順で行います。

1. CP20 の電源を入れます。
2. CP20 の接続パネルで、「**Options**」→「**Configuration**」をクリックします。
3. 図 6-62 のように、CP20 が使用している IP アドレス (固定または DHCP 割り当て) が「Network」タブに表示されます。

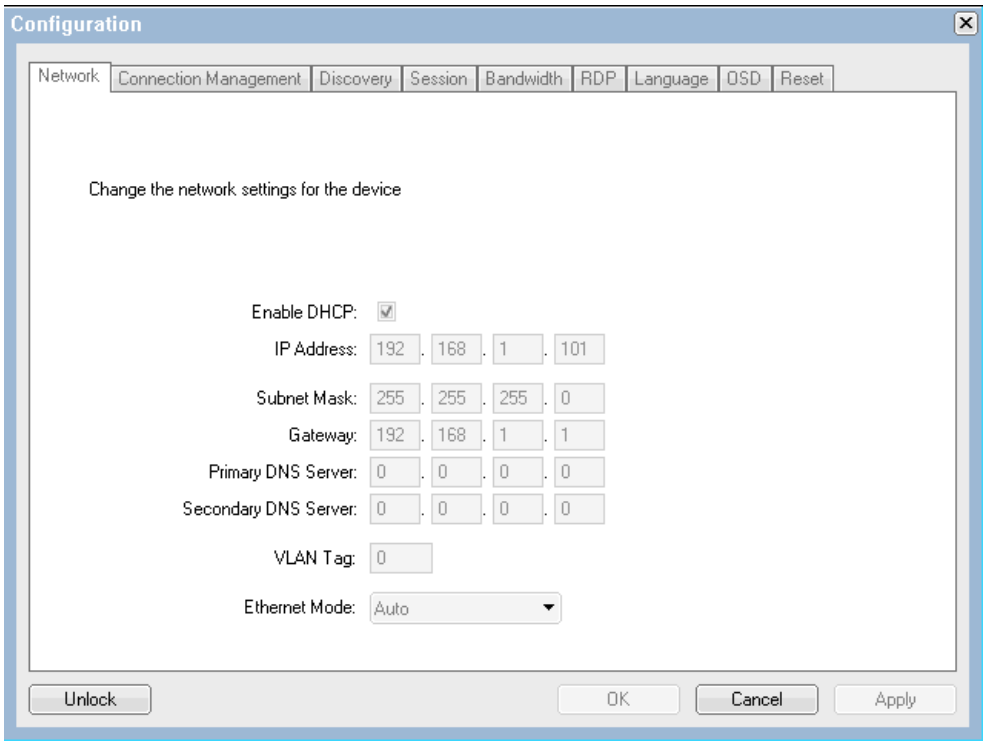


図 6-62　CP20 の IP アドレスを表示する「Network」タブ

4. CP20 の MAC アドレスを確認するには、「**Cancel**」をクリックして「Configuration」ウィンドウを閉じます。その後、「**Options**」→「**Information**」をクリックします。
5. ウィンドウが開き、図 6-63 のように MAC アドレスが示されます。

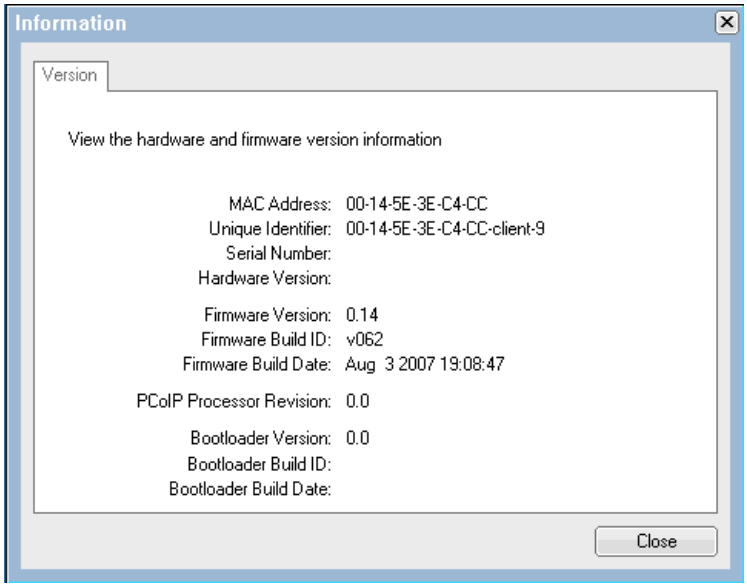


図 6-63 CP20 の MAC アドレスを表示する「Information」ウィンドウ

6.5.2 HC10 への直接接続

ここでは、CP20 と HC10 の間でコネクション・ブローカーを使用せずに直接接続できるようにするために、CP20 と HC10 を構成する方法を説明します。HC10 圧縮カードと CP20 の IP アドレスと MAC アドレスを確認する必要があります。この情報を入手するには、『6.5.1, デバイスの IP アドレスと MAC アドレスの確認』(ページ 145) の手順で行います。

CP20 を構成するには、次の手順で行います。

1. CP20 の電源を入れます。
2. CP20 の接続パネルで、「**Options**」→「**Configuration**」をクリックします。
3. 「**Unlock**」をクリックし、パスワードを入力して (デフォルト・パスワードは PASSW0RD、ただし英文字の *O* ではなくゼロを含む)、「**OK**」をクリックします。
4. 「Connection Management」タブで、「**Enable Connection Management**」が選択されていないことを確認します。
5. 「Discovery」タブで、「**Enable Discovery**」が選択されていないことを確認します。
6. 「Session」タブをクリックします (図 6-64 を参照)。
   a. IP アドレスを使用して接続する場合は、「**IP Address**」を選択し、先に調べた HC10 の IP アドレスと MAC アドレスを入力します。
   b. 完全修飾ドメイン・ネームを使用して接続する場合は、「**FQDN**」を選択し、セットアップ済みのピア FQDN を入力します。
   c. セッション・タイプは、デフォルトの「**PCoIP**」のままにします。

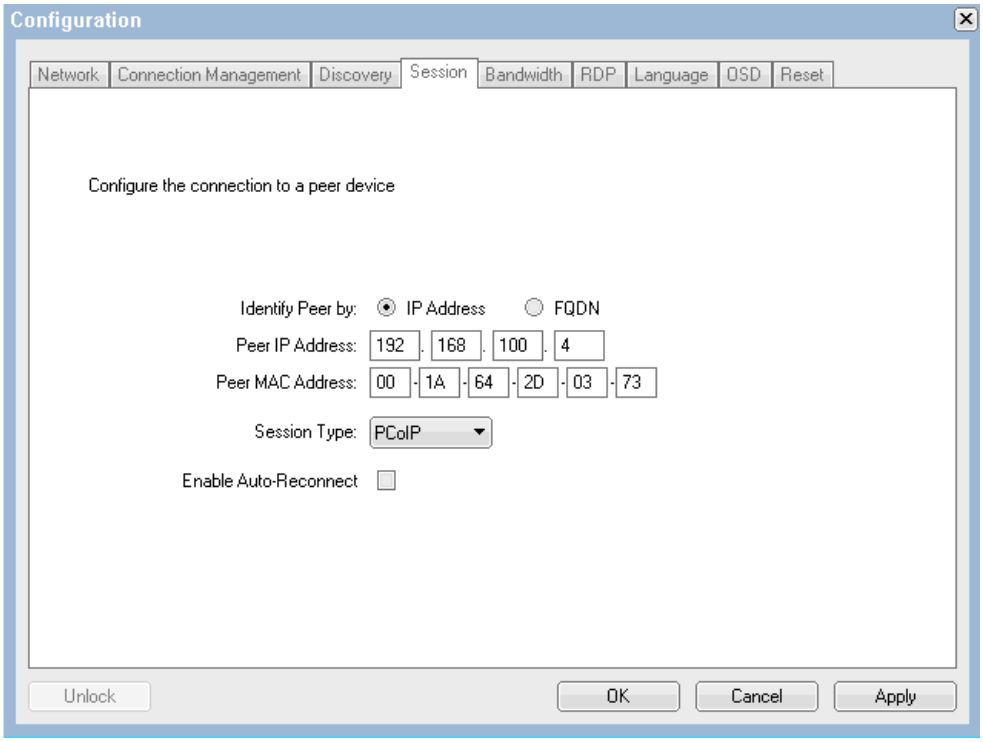


図 6-64　ローカル・インターフェースの「Session」タブ

7. 「**OK**」をクリックして変更内容を保存します。クライアント・プロセッサーを再起動するようにプロンプトで指示された場合は、装置背面にあるロッカー・スイッチを使用して CP20 の電源をオフにし、再びオンにします。

ピアツーピア接続要求を受け入れるように HC10 圧縮カードを構成するには、次の手順で行います。

1. Web ブラウザーを開きます。HC10 圧縮カードの IP アドレスをブラウザーのアドレス・フィールドに入力して、Enter を押します。
2. デバイスのパスワードを入力します (デフォルトは PASSW0RD、ただし英文字の *O* ではなくゼロを含む)。
3. 「**Configuration**」→「**Connection Management**」をクリックし、「**Enable Connection Management**」が選択されて*いない*ことを確認します。変更を行った場合は「**Apply**」をクリックします。
4. 「**Configuration**」→「**Discovery**」をクリックし、「Enable Discovery」が選択されて*いない*ことを確認します。変更を行った場合は「**Apply**」をクリックします。
5. 「**Configuration**」→;「**Session**」をクリックします。HC10 が任意の CP20 から接続を受け入れるようにする場合は、「**Accept Any Peer**」を選択します。そうでなければ、IP アドレスと MAC アドレス、または DNS ホスト名によって CP20 を指定します。変更を行った場合は「**Apply**」をクリックします。

CP20 と HC10 の構成が済んだので、CP20 接続ウィンドウで「**Connect**」をクリックして、HC10 に接続します。HC10 の電源がオフになっている場合は、ブレードの電源が自動的に入ります。

ヒント : 接続しようとしたときにエラー・メッセージ「Connection Refused!」が表示された場合は、HC10 上で接続管理がまだ使用可能に設定されているか、HC10 (CP20 構成内) または CP20 (HC10 構成内) の MAC アドレスを誤って入力したことが原因として考えられます。接続が確立されなかった理由については、「Diagnostics」メニューのイベント・ログを検討してください。

6.5.3 ディスカバリー・オプションを使用した HC10 への接続

ディスカバリー機能を使用すれば、接続先の IP アドレス、ホスト名、または MAC アドレスを指定する必要はありません。代わりに、CP20 からすべてのオンライン HC10 へのサブネットにブロードキャストが送信され、使用可能な HC10 のリストが表示されます。このリストから、接続先を選択できます。

接続する前に、デバイスをディスカバリー・モードで構成する必要があります。まず、CP20 を構成します。

1. CP20 の電源を入れます。
2. CP20 の接続ウィンドウで、**「Options」→「Configuration」**をクリックします。
3. **「Unlock」**をクリックし、パスワードを入力して (デフォルト・パスワードは PASSW0RD、ただし英文字の *O* ではなくゼロを含む)、**「OK」**をクリックします。
4. 「Connection Management」タブで、**「Enable Connection Management」**が選択されていないことを確認します。
5. 「Discovery」タブで、図 6-65 に示すように、**「Enable Discovery」**と**「Enable Host Discovery」**を選択します。

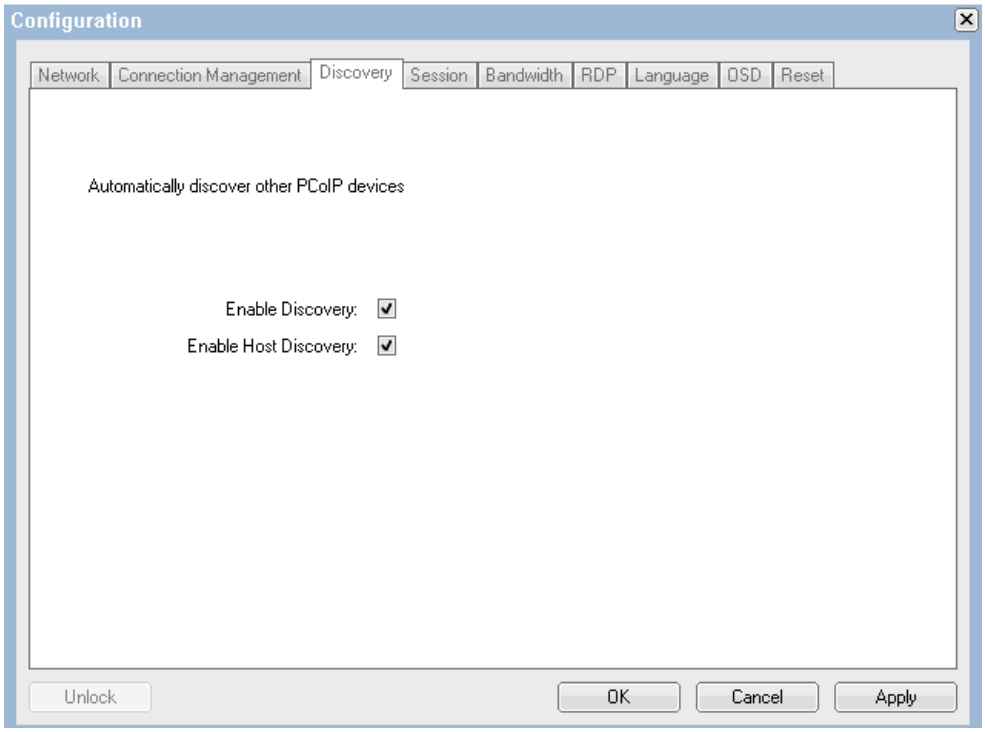


図 6-65　CP20 内での検出の構成

6. 「**OK**」をクリックして変更内容を保存します。クライアント・プロセッサーを再起動するようにプロンプトで指示された場合は、装置背面にあるロッカー・スイッチを使用して CP20 の電源をオフにし、再びオンにします。

次のステップでは、各 HC10 の圧縮カードのディスカバリーを使用可能に設定します。次のように行います。

1. 圧縮カードと CP20 が接続されているネットワークにコンピューターを接続します。
2. 圧縮カードの IP アドレスが分かっていれば、次のステップに進みます。そうでなければ、『6.5.1, デバイスの IP アドレスと MAC アドレスの確認』(ページ 145) の手順のとおりに行って、この情報を入手します。
3. Web ブラウザーを開き、HC10 圧縮カードの IP アドレスをブラウザーのアドレス・フィールドに入力して、Enter を押します。
4. プロンプトが出されたら、デバイスのパスワードを入力します (デフォルトは PASSW0RD、ただし英文字の *O* ではなくゼロを含む)。
5. 「**Configuration**」→「**Discovery**」をクリックします。
6. 図 6-66 に示すように、「**Enable Discovery**」を選択します。次に、「**Apply**」をクリックして変更内容を保存します。

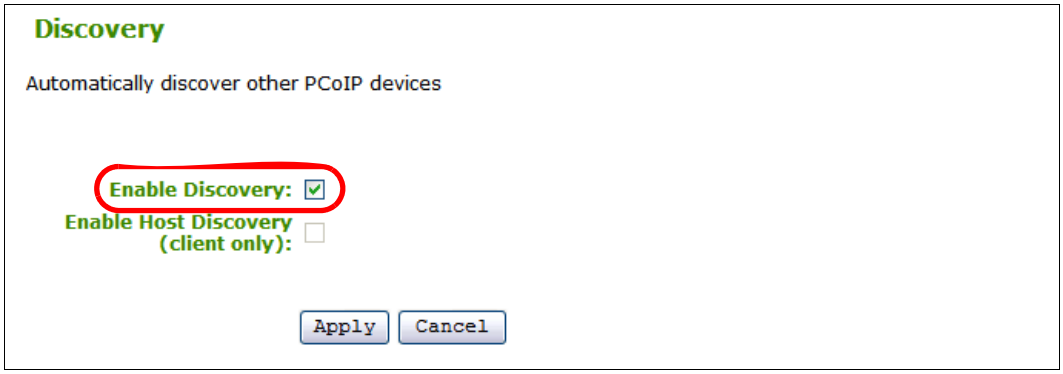


図 6-66　「Discovery」メニューによって検出を使用可能に設定

7. 「**Configuration**」→「**Connection Management**」をクリックし、「**Enable Connection Management**」が選択されていないことを確認します。変更を行った場合は「**Apply**」をクリックします。

CP20 と HC10 が検出のために構成されたので、CP20 の接続ウィンドウで「**Connect**」をクリックします。少し待つと、図 6-67 のように使用可能な HC10 のリストが表示されます。接続したい HC10 を選択して、「**OK**」をクリックします。

注 : 10 台までの HC10 が表示されます。

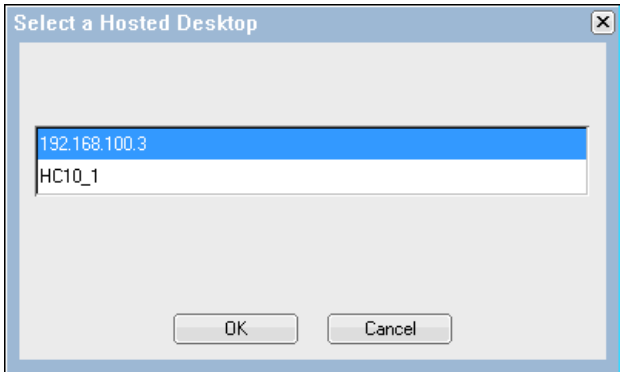


図 6-67　接続可能な HC10 のリスト

ヒント : 図 6-67 に示したウィンドウにリストされた HC10 に接続しようとして、「Connection Refused」というエラーが出された場合は、その HC10 の設定値を調べて、**「Enable Connection Management」**が選択されていないことを確認します。

6.6 ファームウェアの更新

HC10 圧縮カードと CP20 の両方にある PC-over-IP プロセッサーに、最新ファームウェアが適用されていることが重要です。Devon IT Connection Broker を使用している場合は、ファームウェアのデプロイにこのソフトウェアを使用することをお勧めします。この方法について詳しくは、『5.1.3, ファームウェアの更新』(ページ 79) を参照してください。

Devon IT Connection Broker を使用していない場合は、次のようにデバイスを手動で更新できます。

1. 次の URL から最新ファームウェアをダウンロードします。

   http://www.ibm.com/support

2. 一時ディレクトリーにファイルを解凍します。デバイスにアップロードするファームウェア・ファイルには、.app 拡張子が付いています。
3. HC10 圧縮カードおよび CP20 と同じネットワークにコンピューターを接続します。
4. HC10 または CP20 (更新する対象のデバイス) の電源をオンにします。
5. Web ブラウザーを開き、更新するデバイス (つまり、HC10 圧縮カード、または CP20) の IP アドレスを入力します。デバイスの IP アドレスが分からない場合は、『6.5.1, デバイスの IP アドレスと MAC アドレスの確認』(ページ 145) の手順どおりに行って、この情報を入手してください。
6. **「Upload」→「Firmware」**をクリックします。
7. **「Browse」**をクリックし、ダウンロードした .app ファームウェア・ファイルを表示します。このファイルを選択し、**「OK」**をクリックします。
8. **「Upload」**をクリックしてファームウェアをアップロードします。この処理には数分かかることがあります。
9. この他に更新するデバイスがあれば、ステップ 5 から 8 を繰り返します。

HC10 と CP20 のファームウェアが最新であることを確認する方法はいくつかあります。ファームウェア・バージョンは次の場所に示されています。

- HC10 または CP20 の Web インターフェースの「Information」メニュー (『6.4.4, 「Info」メニュー』(ページ 142) を参照)。
- CP20 のローカル・インターフェースの「Information」メニュー (『6.3, CP20 ローカル・インターフェース』(ページ 106) を参照)。
- Devon IT Connection Management ソフトウェアのメインパネル（74 ページの図 5-3 を参照）。

省略語および頭字語

AC 交流 (alternating current)

AMM アドバンスト・マネージメント・モジュール (Advanced Management Module)

API アプリケーション・プログラミング・インターフェース (application programming interface)

ASF Alert Standard Format

BIOS 基本 I/O システム (basic input output system)

BMC ベースボード管理コントローラー (baseboard management controller)

BMP ビットマップ (bitmap)

BS 理学士号 (Bachelor of Science)

BTU 英国熱量単位 (British thermal unit)

CA 認証局 (Certification Authority)

CAD コンピューター支援設計 (computer aided design)

CAE コンピューター支援エンジニアリング (computer aided engineering)

CD コンパクト・ディスク (compact disk)

CLI コマンド・ライン・インターフェース (command-line interface)

CPU 中央演算処理装置 (central processing unit)

CRT 陰極線管 (Cathode Ray Tube)

DDC Display Data Channel

DHCP 動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)

DIMM デュアル・インライン・メモリー・モジュール (dual inline memory module)

DNS ドメイン・ネーム・システム (Domain Name System)

DVI Digital Video Interface

EDID Extended Display Identification Data

ESM イーサネット・スイッチ・モジュール (Ethernet switch modules)

ESP カプセル化セキュリティー・ペイロード (Encapsulating Security Payload)

FDX 全二重 (full duplex)

FQDN 完全修飾ドメイン名 (fully qualified domain name)

FTP ファイル転送プロトコル (File Transfer Protocol)

GB ギガバイト (gigabyte)

GIS 地理情報システム (geographic information systems)

GUI グラフィカル・ユーザー・インターフェース (graphical user interface)

HD 高品位 (high definition)

HT Hyper-Threading

HTTP Hypertext Transfer Protocol

I/O I/O (input/output)

IBM International Business Machines

ID 識別子 (identifier)

IE Internet Explorer

IEC 国際電気標準会議 (International Electro-technical Commission)

IEEE 米国電気電子学会 (Institute of Electrical and Electronics Engineers)

IGMP Internet Group Management Protocol

IGTA I/O Graphics and Transmission Adapter

IP インターネット・プロトコル (Internet Protocol)

IPMI Intelligent Platform Management Interface

IT 情報技術 (information technology)

ITSO International Technical Support Organization

KVM キーボード・ビデオ・マウス (keyboard video mouse)

LAN ローカル・エリア・ネットワーク (local area network)

LDAP Lightweight Directory Access Protocol

LED 発光ダイオード (light emitting diode)

MAC メディア・アクセス制御 (media access control)

MB メガバイト (megabyte)

NIC ネットワーク・インターフェース・カード (network interface card)

OS オペレーティング・システム (operating system)

OSD オンスクリーン・ディスプレイ (on screen display)

PC パーソナル・コンピューター (personal computer)

PCI Peripheral Component Interconnect

PDU 電力配分装置 (power distribution unit)

PFA Predictive Failure Analysis&regi;

PID 製品 ID (Product ID)

POST 電源オン自己診断テスト (power on self test)

PXE Preboot Execution Environment

RADIUS Remote Authentication Dial In User Service

RAM ランダム・アクセス・メモリー (random access memory)

RDM Remote Deployment Manager

RDP Remote Desktop Protocol

RETAIN Remote Electronic Technical Assistance Information Network

RMON リモート・モニター (Remote Monitoring)

RPM 回転 / 分 (revolutions per minute)

SAN ストレージ・エリア・ネットワーク (storage area network)

SAS シリアル接続 SCSI (Serial Attached SCSI)

SATA シリアル ATA (Serial ATA)

SDRAM static dynamic RAM

SFF Small Form Factor

SLP Service Location Protocol

SNMP Simple Network Management Protocol

SOL Serial over LAN

SSL Secure Sockets Layer

TACACS Terminal Access Controller Access Control System

TCO 総所有コスト (total cost of ownership)

TCP 伝送制御プロトコル (Transmission Control Protocol)

TCP/IP 伝送制御プロトコル / インターネット・プロトコル (Transmission Control Protocol/Internet Protocol)

TOE TCP オフロード・エンジン (TCP offload engine)

URL Uniform Resource Locator

USB ユニバーサル・シリアル・バス (universal serial bus)

VGA Video Graphics Array

VID ベンダー ID (Vendor ID)

VLAN 仮想 LAN (virtual LAN)

VM 仮想計算機 (virtual machine)

VNC Virtual Network Computing

VPD 重要プロダクト・データ (vital product data)

VRM 電圧調節モジュール (voltage regulator module)

WCD ワークステーション・コネクション・デバイス (Workstation Connection Device)

WHQL Windows Hardware Quality Labs

WOL Wake on LAN

関連資料

ここに示す資料は、この Redpaper で説明しているトピックをより詳しく解説する資料として特に適切と考えられるものです。

IBM Redbooks の資料

Redbooks、Redpaper、技術情報、ドラフト資料、追加資料の検索、表示、またはダウンロード、およびハードコピー IBM Redbooks 資料のご注文は、次の IBM Redbooks 資料 Web サイトで行うことができます。

ibm.com/redbooks

関連する IBM Redbooks および Redpaper 資料には、次のものがあります。

- *IBM eServer xSeries および BladeCenter サーバー管理*、SG88-8550
- *IBM BladeCenter Products and Technology*, SG24-7523

その他の資料

次の資料も、詳しい情報源として関係のあるものです。次のようにしてダウンロードできます。

1. http://ibm.com/support にアクセスします。
2. 「Choose support type」プルダウンから「**BladeCenter**」を選択し、  をクリックします。
3. 「Popular links」の下にある「**Publication lookup**」をクリックします。
4. 「Product family」プルダウンから「**BladeCenter HC10**」を選択し、「**Continue**」をクリックします。

直接リンクは次のとおりです。

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/resourceselect?familyind=5353629&typeind=0&osind=0&continue.x=37&continue.y=13&brandind=5000020&oldfamily=5353629&taskind=2&pubs=Y

関連資料は次のとおりです。

- *IBM BladeCenter HC10 Installation and User's Guide*
- *IBM BladeCenter HC10 Problem Determination and Service Guide*
- *IBM CP20 Installation, Use and Troubleshooting Guide*
- *Installing Microsoft Windows Vista on the HC10*

オンライン・リソース

次の Web サイトも、詳しい情報源として関係のあるものです。

製品情報ページ

- BladeCenter HC10 および CP20 製品ページ
  http://www.ibm.com/systems/bladecenter/workstation/
- IBM BladeCenter ホーム
  http://www.ibm.com/bladecenter
- IBM BladeCenter HC10 製品の発表
  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-336
- IBM CP20 ワークステーション・コネクション・デバイス製品の発表
  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-580
- IBM BladeCenter S 製品の発表
  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-576
- Devon IT Connection Broker
  http://devonit.com/gateway/gateway_bladeworks.php
- Leostream Hosted Desktop Connection Broker
  http://www.leostream.com/productVHDC.html
- IBM BladeCenter Power Configurator
  http://www.ibm.com/systems/bladecenter/powerconfig
- SAS Connectivity Module および Expansion Card 製品の発表
  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-575
- BladeCenter に関する IBM ServerProven 互換性情報
  http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html

サポート・ページ

- IBM サポート・ホーム
  http://ibm.com/support
- IBM BladeCenter サポート・ホーム
  http://www.ibm.com/systems/bladecenter/support/
- IBM BladeCenter サポート・フォーラム
  http://www.ibm.com/developerworks/forums/dw_forum.jsp?forum=819&cat=53
- RETAIN ヒント H191783:CRT モニターのビデオが壊れている、または表示されない
  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597
- RETAIN ヒント H191730: ブレードがファイアウォールの認証を通らない
  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072550
- RETAIN ヒント H192042:IBM CP20 ワークステーション・コネクション・デバイスがサーバー・コネクティビティ・モジュールを使用して HC10 に接続できない
  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5073011

- RETAIN ヒント H191818: 帯域幅に関する推奨事項

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072671

- RETAIN ヒント H191777: ワークステーション・コネクション・デバイスにビデオが表示されない

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596

- RETAIN ヒント H191763: ワークステーション・コネクション・デバイス上で Microsoft Windows が起動するまで画面が黒くなる
- http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072561
- RETAIN ヒント H191821: マウスまたはキーボードを使用してスタンバイ・モードを終了できない

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072678

- IBM Director ダウンロード

  http://www.ibm.com/systems/management/director/downloads.html

- Windows Audio Device Technologies

  http://www.microsoft.com/whdc/device/audio

- Intel High Definition Audio

  http://www.intel.com/design/chipsets/hdaudio.htm
  http://www.intel.com/standards/hdaudio/

IBM が提供するヘルプ

IBM サポートおよびダウンロード

ibm.com/support

IBM グローバル・サービス

ibm.com/services