Dominion KX II

ユーザ ガイド
リリース **2.5.0**

Copyright © 2012 Raritan, Inc.
DKX2-v2.5.0-0P-J
2012 年 5 月
255-62-4023-00

この文書には、著作権で保護されている固有の情報が含まれています。無断で転載することは禁じられています。この文書のどの部分も Raritan, Inc. より事前に書面による承諾を得ることなく複写、複製、他の言語へ翻訳することを禁じます。

© Copyright 2012 Raritan, Inc. このドキュメントに記載されているすべてのサードパーティ製のソフトウェアおよびハードウェアは、それぞれの所有者の登録商標または商標であり、それぞれの所有者に帰属します。

FCC 情報

この装置は試験済みであり、FCC 規則の Part 15 に規定された Class A デジタル装置の制限に準拠していることが証明されています。これらの制限は、商業環境に設置した場合に有害な干渉を防止するために規定されています。この装置は、無線周波数を生成、利用、および放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信に対して有害な干渉を引き起こす可能性があります。この装置を居住環境で使用した場合、有害な干渉を引き起こす可能性があります。

VCCI 情報 (日本)

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

Raritan 社は、事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が関与しない範囲での使用や、通常の使用条件以外での使用による製品の故障について、一切の責任を負いません。

同梱された電源ケーブルは、本製品専用に使われるものです。

1F61
I.T.E.

ラック マウントの安全上のガイドライン

ラック マウントが必要なラリタン製品を使用する場合、以下のことに注意してください。

- 閉め切ったラック環境では、室温より高くなる場合があります。装置で指定された最高動作温度を超えないようにしてください。**仕様**を参照してください。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機械的に安定して搭載されるように注意してマウントしてください。
- 回路に過大電流が流れないよう、装置を電源に接続する際は注意してください。
- 特に、電源タップ（直接接続を除く）など電力供給をはじめとするすべての装置を分岐回路に正しく接地してください。

目次

はじめに 1

KX II の概要 2
KX II ヘルプ 4
ヘルプでの最新情報 5
関連文書 5
KX II のクライアント アプリケーション 5
仮想メディア 6
KX II デバイスの写真 7
製品の特長 9
ハードウェア 9
ソフトウェア 10
用語 11
パッケージの内容 13

インストールと設定 14

概要 14
ラック マウント 14
前向きの取り付け 14
後向きの取り付け 16
デフォルトのログイン情報 17
入門 18
手順 1: KVM ターゲット サーバの設定 18
ステップ 2: ネットワーク ファイアウォールの設定 31
手順 3: 装置の接続 32
手順 4: KX II の設定 36
手順 5: KX II リモート コンソールの起動 43
手順 6: キーボード言語の設定 (オプション) 44
手順 7: カスケード接続の設定 (オプション) 45

ターゲット サーバの使用 46

KX II インタフェース 46
KX II ローカル コンソール インタフェース: KX II デバイス 47
KX II リモート コンソール インタフェース 47
KX II リモート コンソールの起動 47
インタフェースおよび画面操作 49
KX II コンソールでの案内 52
[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ) 53

[Port Action] (ポート アクション) メニュー 57
ポートのスキャン 59
お気に入りの管理 62
ログアウト 66
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 66
Virtual KVM Client (VKC) および Active KVM Client (AKC) 68
Active KVM Client について 68
ツール バーのボタンおよびステータス バーのアイコン 70
[Connection Properties] (接続プロパティ) 74
接続情報 76
キーボードのオプション 77
ビデオのプロパティ 83
マウス オプション 89
ツール オプション 94
表示オプション 98
デジタル音声 101
スマート カード 108
ヘルプのオプション 112
Multi-Platform Client (MPC) 112
Web ブラウザからの MPC の起動 112

ラック PDU (電源タップ) のコンセントの制御 114

概要 114
コンセントの電源オン/オフの切り替えまたは電源再投入を行う 115

仮想メディア 118

概要 119
仮想メディアを使用するための条件 122
Windows XP 環境での仮想メディア 123
Linux 環境での仮想メディア 124
Mac 環境での仮想メディア 126
読み取り/書き込み可能に設定できない状況 126
仮想メディアの使用 127
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) 128
仮想メディアへの接続 130
ローカル ドライブのマウント 130
CD-ROM/DVD-ROM/ISO イメージのマウント 131

仮想メディアの切断 133

USB プロファイル 134

概要 134
CIM の互換性 135
使用できる USB プロファイル 135
KVM ポート用のプロファイルの選択 143
DCIM-VUSB で Mac OS-X USB プロファイルを使用する場合のマウス モード 144

[User Management] (ユーザ管理) 145

ユーザ グループ 145
ユーザ グループ リスト 146
ユーザとグループの関係 146
新規ユーザ グループの追加 147
既存のユーザ グループの変更 153
ユーザ 154
KX II ユーザ リストの表示 155
ポート別のユーザの表示 156
ポートからのユーザの切断 156
KX II からのユーザのログオフ (強制ログオフ) 157
新規ユーザの追加 157
既存のユーザ グループの変更 158
[Authentication Settings] (認証設定) 159
LDAP/LDAPS リモート認証の実装 160
ユーザ グループ情報を Active Directory サーバから返す 164
RADIUS リモート認証の実装 165
ユーザ グループ情報を RADIUS 経由で返す 169
RADIUS 通信交換仕様 169
ユーザ認証プロセス 171
パスワードの変更 172

デバイス管理 173

ネットワーク設定 173
ネットワーク基本設定 174
LAN インタフェース設定 178
[Device Services] (デバイス サービス) 179
SSH を有効にする 179
HTTP ポートおよび HTTPS ポートの設定 180
検出ポートを入力する 180
カスケード接続を設定および有効化する 181
URL を経由したダイレクト ポート アクセスの有効化 186

AKC ダウンロード サーバ証明書の検証の有効化 188
SNMP エージェントの設定 189
モデムを設定する 191
日付/時刻の設定 193
イベント管理 194
[Power Supply Setup] (電源設定) 205
ポートの設定 206
標準ターゲット サーバの設定 208
KVM スイッチを設定する 209
CIM ポートの設定 211
ラック PDU (電源タップ) ターゲットの設定 211
ブレード シャーシの設定 217
USB プロファイルの設定 ([Port] (ポート) ページ) 243
KX II のローカル ポートの設定 246
スクリプトの接続と切断 252
スクリプトの適用および削除 252
スクリプトの追加 253
スクリプトの変更 256
スクリプトのインポートとエクスポート 256
ポート グループ管理 258
ポート グループの作成 259
デュアル ビデオ ポート グループの作成 260
デフォルトの GUI 言語設定の変更 262

セキュリティ上の問題 263

セキュリティの設定 263
[ログイン制限] 264
[強力なパスワード] 266
[ユーザ ブロック] 267
[Encryption & Share] (暗号化および共有) 269
FIPS 140-2 の有効化 273
IP アクセス制御を設定する 275
SSL 証明書 278
セキュリティ バナー 281

保守 283

[Audit Log] (監査ログ) 283
[Device Information] (デバイス情報) 284
バックアップと復元 286
[USB Profile Management] (USB プロファイルの管理) 288
プロファイル名の競合を処理する 289

CIM アップグレード 290
[Upgrading Firmware] (ファームウェアのアップグレード) 290
アップグレード履歴 293
KX II の再起動 293
CC-SG 管理の終了 295

診断 297

[Network Interface (ネットワーク インタフェース)] ページ 298
[Network Statistics] (ネットワーク統計) ページ 299
[ホストに ping する] ページ 301
[Trace Route to Host (ホストへのルートの追跡)] ページ 301
KX II 診断 303

コマンド ライン インタフェース (CLI) 305

概要 305
CLI を使用しての KX II へのアクセス 306
KX II への SSH 接続 306
Windows PC から SSH で接続する 306
UNIX/Linux ワークステーションから SSH で接続する 307
ログイン 307
CLI の画面操作 307
コマンドのオート コンプリート 307
CLI 構文: ヒントとショートカット キー 308
すべての CLI レベルで使用できるコマンド 308
CLI を使用した初期設定 309
パラメータ値を設定する 309
ネットワーク パラメータの設定 309
CLI プロンプト 310
CLI コマンド 310
セキュリティ上の問題 311
KX II コンソール サーバ設定用コマンドを使用する 311
ネットワークを設定する 312
interface コマンド 312
name コマンド 313
ipv6 コマンド 313

KX II ローカル コンソール 314

概要 314
ユーザが同時接続可能 314
KX II ローカル コンソール インタフェース: KX II デバイス 315
セキュリティと認証 315
有効な解像度 316
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ) 317
ターゲット サーバにアクセスする 318
ポートのスキャン - ローカル コンソール 318
スキャン オプションの使用 320
ローカル コンソールのスマート カード アクセス 321
KX2 8xx デバイスでのスマート カード アクセス 322
ローカル コンソールの USB プロファイル オプション 323
ホット キーと接続キー 324
接続キーの例 324
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ 325
KX II ローカル コンソールの画面に切り替える 326
ローカル ポートの管理 326
KX II ローカル コンソールのローカル ポートの設定 327
KX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ 331
スクリプトの接続と切断 333
スクリプトの適用および削除 333
スクリプトの追加 334
スクリプトの変更 337
リセット ボタンを使用して KX II をリセットする 337

仕様 339

KX II の物理的仕様 339
サポートされているオペレーティング システム (クライアント) 342
サポートされている画面解像度 343
サポートされているターゲット サーバとビデオ 345
サポートされているブラウザ 345
サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 345
デジタル CIM ターゲット サーバのタイミングおよび画面解像度 349
サポートされている Paragon CIMS および設定 350
KX II – KX II 構成に関するガイドライン 352
KX II – Paragon II 構成に関するガイドライン 353
KX II の統合向けにサポートされている距離 355
スマート カード リーダー 355
サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー 355
スマート カードの最小システム要件 357

Dell 筐体を接続する場合のケーブル長と画面解像度 359
音声 359
サポートされている音声デバイス形式 359
音声の再生とキャプチャに関する推奨事項と要件 359
サポートされている音声/仮想メディアおよびスマート カード接続の数 361
認定モデム 361
拡張ローカル ポートでサポートされているデバイス 362
KX2 8xx 拡張ローカル ポートの推奨最大距離 362
サポートされているリモート接続 362
各言語に対してサポートされているキーボード 363
使用される TCP ポートおよび UDP ポート 364
監査ログおよび Syslog でキャプチャされるイベント 367
ネットワーク速度の設定 367

デュアル ビデオ ポート グループ 370

概要 370
デュアル ポート ビデオ グループ設定の例 371
手順 1: ターゲット サーバの画面の設定 372
手順 2: KX II へのターゲット サーバの接続 373
手順 3: マウス モードおよびポートの設定 374
手順 4: デュアル ビデオ ポート グループの作成 374
手順 5: デュアル ビデオ ポート グループを開く 375
デュアル ポート ビデオに関する推奨事項 376
サポートされているマウス モード 376
デュアル ビデオ サポートに必要な CIM 377
デュアル ポート ビデオ グループの使いやすさに関する注意事項 378
権限およびデュアル ビデオ ポート グループ アクセス 379
デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作 379
ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ 380
[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ 380

KX II を使用した Paragon II へのアクセス 381

概要 381
KX II への Paragon II の接続 382

LDAP スキーマを更新する 384

ユーザ グループ情報を返す 384
LDAP/LDAPS から返す場合 384
Microsoft Active Directory から返す場合 385

スキーマへの書き込み操作を許可するようにレジストリを設定する 385
新しい属性を作成する 386
属性をクラスに追加する 387
スキーマ キャッシュを更新する 388
ユーザ メンバの rciusergroup 属性を編集する 389

留意事項 392

概要 392
Java Runtime Environment (JRE) 392
IPv6 のサポートに関する注意事項 394
デュアル スタック ログインのパフォーマンスに関する問題 395
Mac に関する注意事項 395
Mac Mini BIOS のキー入力コマンド 395
Mac Lion クライアントでの MPC の起動 396
キーボード 397
アメリカ英語以外のキーボード 397
Macintosh キーボード 400
Fedora 400
Fedora Core のフォーカスに関する問題を解決する 400
マウス ポインタの同期 (Fedora) 401
Fedora サーバへの VKC および MPC のスマート カード接続 401
Fedora 使用時の Firefox のフリーズに関する問題の解決 401
ビデオ モードと解像度 402
SUSE と VESA のビデオ モード 402
サポートされている画面解像度が表示されない 402
音声 403
音声の再生とキャプチャに関する問題 403
Linux 環境での音声 403
Mac 環境での音声 404
Windows 環境での音声 404
USB ポートとプロファイル 404
VM-CIM および DL360 の USB ポート 404
USB プロファイルの選択に関するヘルプ 405
スマート カード リーダー使用時の USB プロファイルの変更 407
仮想メディア 408
Windows 環境での VKC および AKC を介した仮想メディア 408
ファイル追加後に仮想メディアが最新の情報に更新されない 409
アクティブ システム パーティション 409
ドライブ パーティション 409
仮想メディアの Linux ドライブが 2 回リストされる 409
Mac および Linux でマップしてロックしたドライブ 409
D2CIM-VUSB を使用して Windows 2000 サーバ上の仮想メディアにアクセスする 410
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間 410
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー 410

CIM....410
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合....410
Windows 2000 での複合 USB デバイスの動作....411
CC-SG....412
VKC のバージョンが CC-SG プロキシ モードで認識されない....412
シングル マウス モード: Firefox を使用して CC-SG の管理下にあるターゲットに VKC を介してアクセスする場合....412
プロキシ モードと MPC....412
デバイスのポート間の移動....412

FAQ **413**

一般的な FAQ....414
リモート アクセス....416
ユニバーサル仮想メディア....419
帯域幅と KVM-over-IP のパフォーマンス....423
Ethernet と IP ネットワーキング....428
IPv6 ネットワーキング....431
サーバ....433
ブレード サーバ....434
インストール....437
ローカル ポート....439
拡張ローカル ポート (Dominion KX2-832 および KX2-864 モデルのみ)....442
インテリジェント電源タップ (PDU) の管理....443
ローカル ポートの統合およびカスケード接続....445
コンピュータ インタフェース モジュール (CIM)....448
セキュリティ....450
スマート カード認証と CAC 認証....452
管理機能....453
ドキュメントおよびサポート....454
その他....455

索引 **457**

Ch 1 はじめに

この章の内容

KX II の概要 2
KX II ヘルプ 4
KX II のクライアント アプリケーション 5
仮想メディア 6
KX II デバイスの写真 7
製品の特長 9
用語 11
パッケージの内容 13

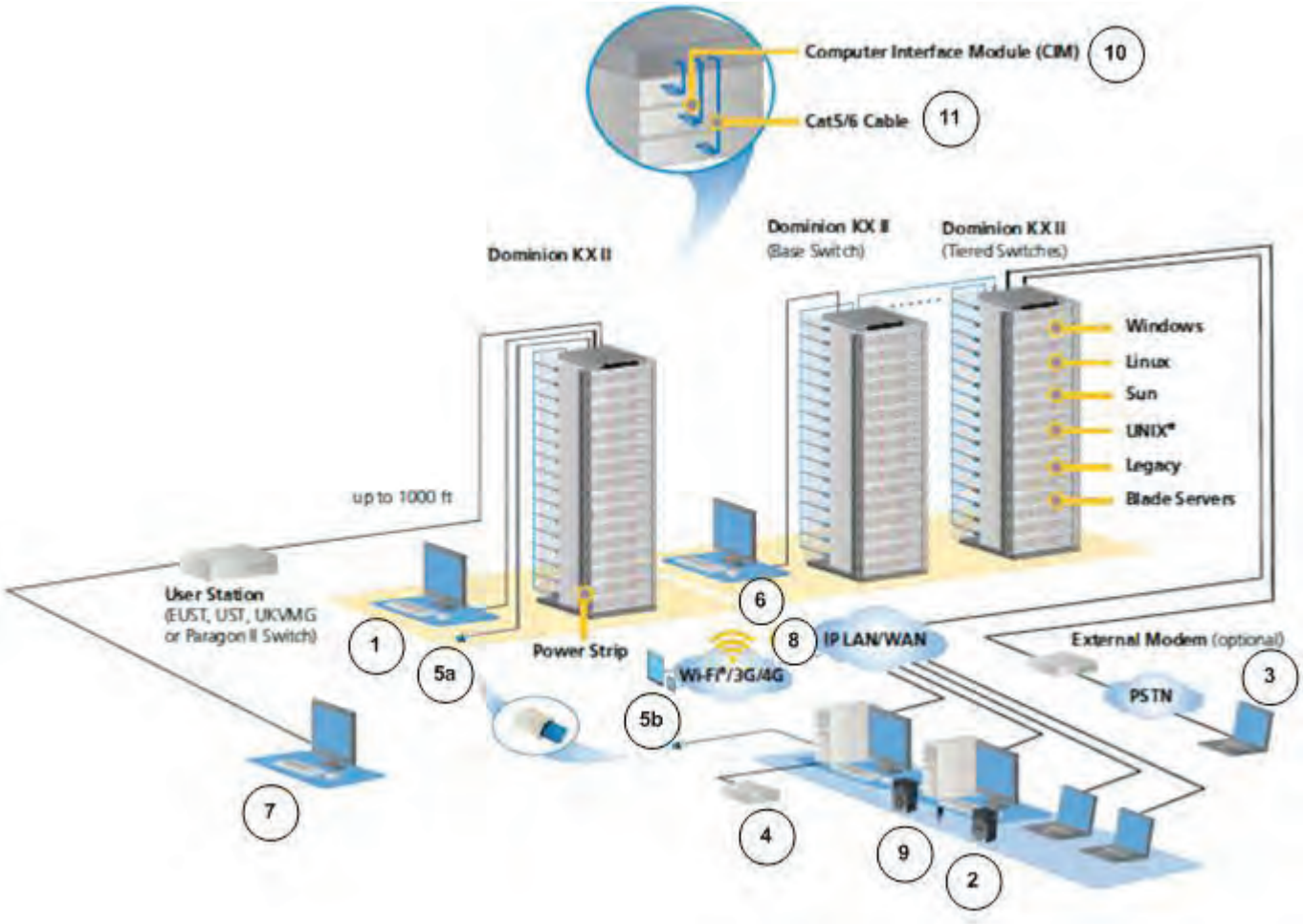
KX II の概要

Raritan の Dominion KX II は、世界中どこからでも Web ブラウザを介してサーバへの BIOS レベル以上のアクセスおよび制御を提供する、企業規模のセキュアなデジタル KVM (キーボード、ビデオ、マウス) スイッチです。標準の KX II で最大 64 台のサーバを制御できます。KX II の 8 ユーザ モデルの場合、KX2-832 では最大 32 台のサーバを、KX2-864 では最大 64 台のサーバを制御できます。スキャン機能を使用すると、最大 32 台のターゲットを検索して表示できます。ターゲットは、スライド ショーのサムネイルとして表示され、そこからユーザが各ターゲットにアクセスします。

KX II では、最大 8 つのビデオ チャネルがサポートされるため、最大 8 人の同時ユーザが任意の時点で 8 台の異なるビデオ ターゲットに接続できます。デジタル音声デバイスがサポートされているので、リモート クライアント PC の再生デバイスおよび録音デバイスをターゲット サーバに接続できます。ラック内の KX II で、1 組のキーボード、モニタ、およびマウスから、最大 64 台のサーバと IT デバイスを BIOS レベルで制御できます。また、KX II のリモート アクセス機能の統合によって、Web ブラウザを使用した同じレベルのサーバの制御が可能になっています。

KX II は、標準 UTP (Cat 5/5e/6) ケーブルを使用した配線で簡単に取り付けることができます。その高度な機能には、仮想メディア、256 ビット暗号化、二重化電源、リモート電源管理、二重化 Ethernet、LDAP、RADIUS、Active Directory®、Syslog との統合、外付けモデム機能、および Web 管理などが含まれています。KX II の 8 ユーザ モデルでは、デバイスの背面に拡張ローカル ポートも搭載されています。これらの機能により、より長い稼働時間、より優れた生産性、強固なセキュリティを、いつでも、どこからでも提供できます。

KX II 製品は、スタンドアロン装置として動作し、中央管理デバイスには依存しません。大規模なデータ センタや企業では、多数の KX II デバイス (Dominion SX デバイスをリモート シリアル コンソール アクセス用、Dominion KSX をリモート/支店管理用に併用) を、ラリタンの CommandCenter Secure Gateway (CC-SG) を使用して、1 つの論理ソリューションとして統合することが可能です。


Computer Interface Module (CIM)
10
Cat5/6 Cable
11
Dominion KX II
Dominion KX II
(Base Switch)
Dominion KX II
(Tiered Switches)
Windows
Linux
Sun
UNIX*
Legacy
Blade Servers
up to 1000 ft
User Station
(EUST, UST, UKVMG
or Paragon II Switch)
1
5a
Power Strip
6
8
IP LAN/WAN
Wi-Fi*/3G/4G
5b
External Modem (optional)
PSTN
3
7
4
9
2

図の説明			
1	ローカル ポート アクセス	6	カスケード接続
2	IP ベースのネットワーク アクセス	7	拡張ローカル ポート
3	モデム	8	CC-SG を使用する iPhone® や iPad® を介したモバイル アクセス
4	仮想メディア	9	デジタル音声
5a	ラックでのスマート カード アクセス	10	CIM
5b	リモート スマート カード アクセス	11	Cat5/6 ケーブル

KX II ヘルプ

KX II ヘルプでは、KX II のインストール、セットアップ、および設定の方法に関する情報を確認できます。また、ターゲット サーバに対するアクセス、仮想メディアの使用、ユーザおよびセキュリティの管理、KX II の保守と診断に関する情報も提供します。

現在のリリースに関する重要な情報について KX II リリースノートを参照してから、KX II を使用してください。

PDF バージョンのヘルプは、Raritan の Web サイトの [Firmware and Documentation] ページからダウンロードできます。最新のユーザ ガイドが利用できるかどうかを Raritan の Web サイトで確認することをお勧めします。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

ヘルプでの最新情報

製品やユーザ マニュアルに対する強化や変更に基づいて、以下の情報が追加されています。

- 新しい KX2-808 モデル (KVM ポート x 8、ローカル ポート x 1、拡張ローカル ポート x 1、およびネットワーク上の 8 リモート ユーザのサポート)

このアプライアンスおよびこのバージョンのヘルプに対して適用される変更の詳細は、KX II リリース ノートを参照してください。

関連文書

KX II ヘルプには、KX II クイック セットアップ ガイドが付属しています。これは、*Raritan の Web サイト『http://www.raritan.com/support/firmware-and-documentation* 参照 』の [Firmware and Documentation] ページにあります。

KX II で使用するクライアント アプリケーションのインストールの要件および手順についても、Raritan の Web サイトにある『KVM and Serial Access Clients Guide』を参照してください。該当する場合は、KX II で使用される特定のクライアント機能がこのヘルプに掲載されます。

KX II のクライアント アプリケーション

KX II で使用できるクライアント アプリケーションは以下のとおりです。

製品	使用可能				
	MPC	AKC	VKC	RSC	RRC
KX II (第 2 世代)	✓		✓		
KX II 2.2 以降	✓	✓	✓		

クライアント アプリケーションの詳細については、『KVM and Serial Access Clients User Guide』を参照してください。このガイドの「*ターゲット サーバの使用『46*p. 』」セクションも参照してください。KX II でのクライアントの使用に関する情報が記載されています。

注: MPC および VKC を使用するには、Java™ Runtime Environment (JRE™) が必要です。AKC は .NET ベースです。

仮想メディア

すべての KX II モデルにおいて仮想メディアがサポートされています。それぞれの KX II は仮想メディアを装備しているので、CD、DVD、USB、音声再生および録音デバイス、内部およびリモート ドライブ、イメージなどのいろいろなデバイスを使用したリモート管理タスクが可能です。KX II では、ハード ディスク ドライブおよびリモートにマウントされたイメージの仮想メディアにアクセスできます。

仮想メディアのセッションは、256 ビットの AES または RC4 暗号化によって保護されます。

デジタル CIM、D2CIM-VUSB CIM、および D2CIM-DVUSB CIM（コンピュータ インタフェース モジュール）では、USB 2.0 インタフェースをサポートする KVM ターゲット サーバへの仮想メディア セッションがサポートされます。これらの CIM では、ずれないマウス機能、仮想メディア、およびリモート ファームウェア アップデートもサポートされます。

注: DVUSB CIM の黒のコネクタは、キーボードとマウスに使用します。グレーのコネクタは、仮想メディアに使用します。CIM の両方のプラグをデバイスに接続したままにします。両方のプラグがターゲット サーバに接続されていない場合は、デバイスが正しく動作しないことがあります。

KX II デバイスの写真

KX II

KX2-808

KX2-832

KX2-864

製品の仕様については、「*KX II の寸法および物理的仕様 『339*p. の*″KX II の物理的仕様″*参照 *』*」を参照してください。CIM の仕様書および画像については、「*サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 『345*p. *』*」を参照してください。

製品の特長

ハードウェア

- KVM-over-IP リモート アクセスの統合
- 1U または 2U サイズ、ラックマウント対応、ブラケット付属
- フェイルオーバ対応の二重化電源 – 障害警告機能を備えた自動切換え電源
- カスケード接続がサポートされています。これにより、ベース KX II デバイスは他の複数台のティアー接続デバイスにアクセスします。ティアー接続の詳細については、「*ティアー接続を設定および有効化する* 『*181*p. の*"カスケード接続を設定および有効化する"*参照 』」を参照してください。
- マルチ ユーザ機能 (1/2/4/8 リモート ユーザ、1 ローカル ユーザ)
- UTP (Cat5/5e/6) ケーブルを使用したサーバへの配線
- フェイルオーバ対応の二重化 Ethernet ポート (10/100/1000 LAN)
- フィールド アップグレード可能
- ラック内アクセス用ローカル ユーザ ポート
  - KX2-808、KX2-832、および KX2-864 の PS/2 キーボード/マウス用ポートは USB のみ
  - サポートされる USB デバイス用の、USB 2.0 ポート (前面に 1 基、背面に 3 基)
  - リモート ユーザ アクセスと同時に操作可能
  - 管理用のローカル グラフィカル ユーザ インタフェース (GUI)
- KX2 8xx デバイス上のラック内アクセスの到達距離を延長する拡張ローカル ポート
- 中央管理されるアクセス セキュリティ
- 電源管理の統合
- 二重化電源やネットワーク アクティビティ、リモート ユーザの状況を示す LED インジケータ
- ハードウェア リセット ボタン
- 外付けモデムに接続するためのシリアル ポート
- モデルごとにサポートされているユーザ数とポート数:

[Model] (モデル)	リモート ユーザ	ポート
KX II-864	8	64
KX II-832	8	32
KX II-808	8	8
KX II-464	4	64

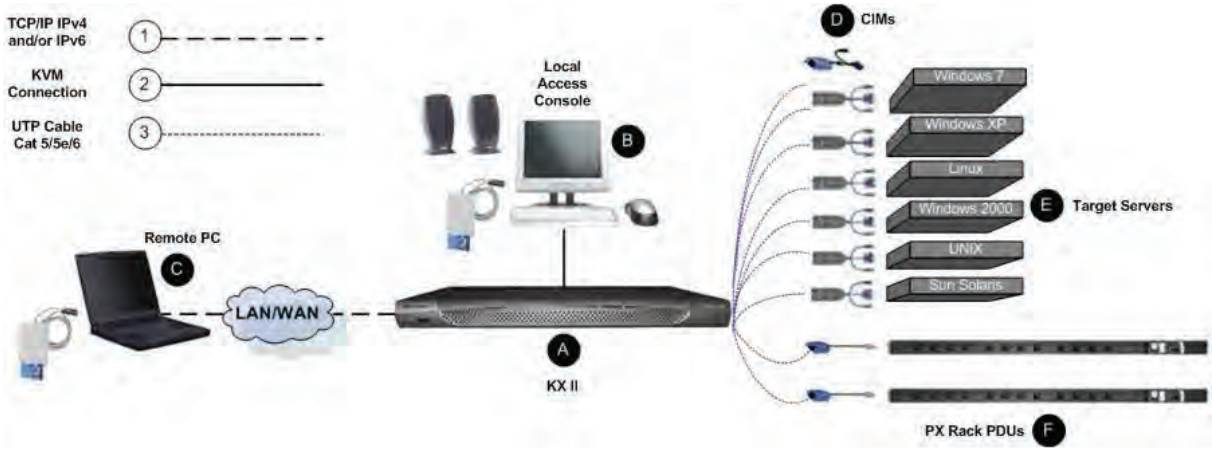
[Model] (モデル)	リモート ユーザ	ポート
KX II-432	4	32
KX II-416	4	16
KX II-232	2	32
KX II-216	2	16
KX II-132	1	32
KX II-116	1	16
KX II-108	1	8

ソフトウェア

- Windows®、Mac®、Linux® の各環境で仮想メディアをサポート (D2CIM-VUSB CIM、D2CIM-DVUSB CIM、およびデジタル CIM を使用)
- USB を介したデジタル音声をサポート
- 設定可能なスキャン セット内で最大 32 台のターゲットをポートスキャンしサムネイル表示
- ずれないマウス機能 (Absolute Mouse Synchronization) (D2CIM-VUSB CIM、D2CIM-DVUSB CIM、およびデジタル CIM を使用)
- プラグ & プレイ
- Web ベースのアクセスと管理
- わかりやすいグラフィカル ユーザ インタフェース (GUI)
- デュアル ポート ビデオ出力のサポート
- すべての KVM 信号を 256 ビット暗号化 (ビデオや仮想メディアを含む)
- LDAP、Active Directory®、RADIUS、または内部機能による認証および認可
- DHCP または静的な IP アドレスの指定
- スマート カード/CAC 認証
- SNMP、SNMP3、および Syslog 管理
- IPv4 および IPv6 のサポート
- 誤操作を防ぐためにサーバと直接関連付けられる電源管理
- Raritan の CommandCenter Secure Gateway (CC-SG) 管理本体との統合
- CC-SG の制御からデバイスを解除するための CC Unmanage 機能
- Raritan PX1 および PX2 のアプライアンスのサポート

用語

ヘルプでは、KX II の標準的なコンポーネントに次の用語を使用しています。



図の説明	
1	TCP/IP IPv4 または IPv6
2	KVM (キーボード、ビデオ、マウス)
3	UTP ケーブル (Cat5/5e/6)
A	KX II
B	ローカル アクセス コンソール ローカル ユーザ – ターゲット サーバを (ネットワーク経由ではなく直接ラック内で) 制御するために KX II に直接接続された、(キーボード、マウス、マルチシンク VGA モニタで構成される) オプションのユーザ コンソール。USB スマート カード リーダーをローカル ポートに接続してターゲット サーバにマウントすることもできます。DKX2-808、DKX2-832、DKX2-864 の各モデルには、拡張ローカル ポートも搭載されています。
C	リモート PC KX II に接続している KVM ターゲット サーバへのアクセスとその制御に使用する、ネットワークに接続したコンピュータ。USB スマート カード リーダーをリモート PC に接続したり、KX II 経由でターゲット サーバに接続したりすることもできます。
D	CIM 各ターゲット サーバまたはラック PDU (電源タップ) に接続するドングル。サポートされているすべてのオペレーティング システムに対して使用できます。
E	ターゲット サーバ KVM ターゲット サーバ – KX II を介してリモート アクセスされる、ビデオ カードとユーザ インタフェース (例: Windows®、Linux®、Solaris™) を備えたサーバ。
F	Dominion PX ラック PDU (電源タップ) KX II を介してリモート アクセスされる Raritan ラック PDU。

サポートされているオペレーティング システムと CIM の一覧については、「**サポートされている CIM およびオペレーティング システム (ターゲット サーバ)**」を、KX II によってリモート ディスプレイサポートされるオペレーティング システムの一覧については、「*サポートされているオペレーティング システム (クライアント)*『*342*p. 』」を参照してください。

パッケージの内容

KX II は、標準 1U (DKX2-864 の場合は 2U) 19 インチ ラックマウント シャーシに搭載される、完全に構成されたスタンドアロン製品として出荷されます。各 KX II デバイスは、以下の内容で出荷されます。

数量	品目
1	KX II デバイス
1	KX II クイック セットアップ ガイド
1	ラックマウント キット
2	AC 電源コード
2	Cat5 ネットワーク ケーブル
1	Cat5 ネットワーク クロス ケーブル
1	ゴム足 1 組 (4 個、デスクトップ設置用)
1	アプリケーション ノート
1	保証書

Ch 2 インストールと設定

この章の内容

概要 14
ラック マウント 14
デフォルトのログイン情報 17
入門 18

概要

このセクションでは、インストール手順の概要を説明します。それぞれの手順については、この章の後のセクションで詳しく説明します。

▶ **KX II をインストールおよび設定するには、以下の手順に従います。**

- *手順 1: KVM ターゲット サーバの設定* 『*18*p. 』
- *手順 2: ネットワーク ファイアウォールの設定* 『*31*p. の"*ステップ 2: ネットワーク ファイアウォールの設定*"参照 』
- *手順 3: 装置の接続* 『*32*p. 』
- *手順 4: KX II* 『*36*p. の"*手順 4: KX II の設定*"参照 』 の設定
- *手順 5: KX II リモート コンソールの起動* 『*43*p. 』
- *手順 6: キーボード言語の設定（オプション）*『*44*p. 』
- *手順 7: カスケード接続の設定（オプション）*『*45*p. 』

このセクションには、必要なデフォルトのログイン情報も含まれます。この情報には、特にデフォルト IP アドレス、ユーザ名、およびパスワードがあります。「*デフォルトのログイン情報* 『*17*p. 』」を参照してください。

ラック マウント

KX II は、標準の 19 インチ機器用ラックの 1U（4.4 cm、1.75 インチ）の縦方向スペースに取り付けることができます。

前向きの取り付け

注: ここに示す図で使用されている Raritan デバイスは、例として挙げているにすぎず、KX II デバイスの画像ではありません。ただし、取り付け手順は同じです。

各手順は、前面ラック マウント図に示されている番号に対応しています。

1. 付属の 2 本のネジを使用して側面ブラケットの後端にケーブル支持バーを固定します。

2. ユーザ ステーションまたは KVM スイッチを、背面パネルがケーブル支持バーに面した状態で側面ブラケットの間にはめ込み、その前面パネルを側面ブラケットの「耳」に揃えます。
3. 残りのネジ（各側面に 3 本）を使用して、ユーザ ステーションまたはスイッチを側面ブラケットに固定します。
4. アセンブリ全体をラックに取り付け、専用のネジ、ボルト、ケージ ナットなどで側面ブラケットの耳をラックの前面レールに固定します。
5. ユーザ ステーションまたはスイッチの背面のパネルにケーブルを接続する場合は、ケーブルをケーブル支持バーに掛けます。

前面ラック マウント

前面ラック マウント

後向きの取り付け

注: ここに示す図で使用されている Raritan デバイスは、例として挙げているにすぎず、KX II デバイスの画像ではありません。ただし、取り付け手順は同じです。

各手順は、背面ラック マウント図に示されている番号に対応しています。

1. 付属の 2 本のネジを使用して側面ブラケットの前端に（側面ブラケットの「耳」の近くに）ケーブル支持バーを固定します。
2. ユーザ ステーションまたは KVM スイッチを、背面パネルがケーブル支持バーに面した状態で側面ブラケットの間にはめ込み、その前面パネルを側面ブラケットの後端に揃えます。
3. 残りのネジ（各側面に 3 本）を使用して、ユーザ ステーションまたはスイッチを側面ブラケットに固定します。
4. アセンブリ全体をラックに取り付け、専用のネジ、ボルト、ケージ ナットなどで側面ブラケットの耳をラックの前面レールに固定します。
5. ユーザ ステーションまたはスイッチの背面のパネルにケーブルを接続する場合は、ケーブルをケーブル支持バーに掛けます。

後向きの取り付け

後向きの取り付け

デフォルトのログイン情報

デフォルト設定	値
ユーザ名	デフォルトのユーザ名は admin です。このユーザは、管理者特権を有します。
パスワード	デフォルトのパスワードは raritan です。 パスワードは大文字と小文字が区別されるため、大文字と小文字は作成したとおりに正確に入力する必要があります。たとえば、デフォルトのパスワード raritan は、すべて小文字で入力する必要があります。 KX II を初めて起動したときは、デフォルトのパスワードを変更する必要があります。
IP アドレス	KX II の出荷時には、デフォルトの IP アドレス (192.168.0.192) が設定されています。

重要: バックアップと事業の継続性のためには、バックアップ管理者用のユーザ名およびパスワードを作成し、その情報を安全な場所に保管しておくことを強くお勧めします。

入門

手順 1: KVM ターゲット サーバの設定

KVM ターゲット サーバとは、KX II を介してアクセスおよび制御するコンピュータのことです。最適なパフォーマンスを確保するために、KX II をインストールする前に、すべての KVM ターゲット サーバを設定します。この設定は、KVM ターゲット サーバのみに適用されます。KX II のリモート アクセスに使用されるクライアント ワークステーション（リモート PC）には適用されません。詳細については、「用語 『11p. 』」を参照してください。

デスクトップの背景

Windows®、Linux®、X-Windows、Solaris™、KDE などのグラフィカル ユーザ インタフェースを実行する KVM ターゲット サーバは、帯域幅効率とビデオ パフォーマンスを最適化するための設定が必要になる場合があります。デスクトップの背景は完全な無地にする必要はありませんが、写真や複雑な配色の背景を使用すると、パフォーマンスが低下する可能性があります。

マウスの設定

KX II は、ずれないマウス モード™、インテリジェント マウス モード、および標準マウス モードで動作します。

ずれないマウス モードの場合は、マウス パラメータを変更する必要はありません。ただし、このモードを使用するには、D2CIM-VUSB、D2CIM-DVUSB、またはデジタル CIM が必要です。標準マウス モードとインテリジェント マウス モードの場合は、マウス パラメータを特定の値に設定する必要があります。マウス設定は、ターゲットのオペレーティング システムによって異なります。詳細については、使用するオペレーティング システムのマニュアルを参照してください。

インテリジェント マウス モードは、ほとんどの Windows プラットフォームで正常に機能しますが、ターゲット上でアクティブ デスクトップが設定されている場合は、予測できない結果を生じることがあります。インテリジェント マウス モードではアニメーション カーソルは使用しないでください。 インテリジェント マウス モード設定の詳細については、「*インテリジェント マウス モード『92*p. 』」を参照してください。

ブレード筐体内に KVM スイッチを備えているサーバの場合、通常、ずれないマウス機能はサポートされません。

Windows XP、Windows 2003、および Windows 2008 の設定

▶ **Microsoft® Windows XP® オペレーティング システムを実行している KVM ターゲット サーバを設定するには、Windows 2003® オペレーティング システムまたは Windows 2008® オペレーティング システムで、以下の操作を行います。**

1. マウスの設定を行います。
   a. ［スタート］、［コントロール パネル］、［マウス］の順に選択します。
   b. ［ポインタ オプション］タブをクリックします。
   c. ［速度］グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - ［ポインタの精度を高める］チェック ボックスをオフにします。
      - ［動作］のオプションを無効にします。
      - ［OK］をクリックします。

   注: ターゲット サーバで Windows 2003 を実行している場合に、KVM を介してサーバにアクセスし、次に挙げるアクションのいずれかを実行すると、以前有効になっていたマウスの同期が失われる可能性があります。同期を再度有効にするには、クライアントで［マウス］メニューの［マウスの同期］コマンドを選択する必要があります。これが発生する可能性があるアクションを以下に示します。

   – テキスト エディタを開く。

   – Windows の［コントロール パネル］から［マウスのプロパティ］、［キーボードのプロパティ］、および［電話とモデムのオプション］にアクセスする。

2. アニメーション効果を無効にします。
   a. ［コントロール パネル］の［画面］オプションを選択します。
   b. ［デザイン］タブをクリックします。
   c. ［効果］をクリックします。
   d. ［次のアニメーション効果をメニューとヒントに使用する］オプションをオフにします。
   e. ［OK］をクリックします。
3. ［コントロール パネル］を閉じます。

注: Windows XP、Windows 2000、または Windows 2008 を実行している KVM ターゲット サーバの場合、KX II を介したリモート接続用に、専用のユーザ名を作成することが可能です。これにより、ターゲット サーバのマウス ポインタの速度や加速を KX II 接続用に遅く設定できます。

Windows XP、2000、および 2008 のログイン ページでは、マウスのパラメータが、最適な KX II パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。この結果、これらの画面ではマウスの同期は最適ではありません。

注: Windows KVM ターゲット サーバのレジストリを調整してもかまわない場合のみ、次の操作を行ってください。Windows レジストリ エディタを使って次の設定を変更することにより、ログイン ページで KX II のマウスの同期を改善することができます。
HKey_USERS¥.DEFAULT¥Control Panel¥Mouse:> MouseSpeed = 0、MouseThreshold 1=0、MouseThreshold 2=0。

Windows 7 および Windows Vista の設定

▶ Windows Vista® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. [スタート]、[設定]、[コントロール パネル]、[マウス] の順に選択します。
   b. 左側のナビゲーション パネルから [システムの詳細設定] を選択します。[システムのプロパティ] ダイアログ ボックスが表示されます。
   c. [ポインタ オプション] タブをクリックします。
   d. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [OK] をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. [コントロール パネル] の [システム] オプションを選択します。
   b. [パフォーマンス情報] を選択し、[ツール]、[詳細ツール]、[調整] の順に選択し、Windows の外観とパフォーマンスを調整します。
   c. [詳細設定] タブをクリックします。
   d. [パフォーマンス] グループの [設定] をクリックして、[パフォーマンス オプション] ダイアログ ボックスを開きます。
   e. [カスタム] オプションで、以下のチェック ボックスをオフにします。
   - アニメーション関連のオプション:

- [Windows 内のアニメーション コントロールと要素]
- [ウィンドウを最大化や最小化するときにアニメーションで表示する]

- フェード関連のオプション:
  - [メニューをフェードまたはスライドして表示する]
  - [ヒントをフェードまたはスライドで表示する]
  - [メニュー項目をクリック後にフェード アウトする]

3. [OK] をクリックして、[コントロール パネル] を閉じます。

▶ Windows 7® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[ハードウェアとサウンド]、[マウス] の順に選択します。
   b. [ポインタ オプション] タブをクリックします。
   c. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [OK] をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. [コントロール パネル]、[システムとセキュリティ] を選択します。
   b. [システム] を選択し、左側のナビゲーション パネルから [システムの詳細設定] を選択します。[システムのプロパティ] ダイアログ ボックスが表示されます。
   c. [詳細設定] タブをクリックします。
   d. [パフォーマンス] グループの [設定] ボタンをクリックして、[パフォーマンス オプション] ダイアログ ボックスを開きます。
   e. [カスタム] オプションで、以下のチェック ボックスをオフにします。
   - アニメーション関連のオプション:
     - [Windows 内のアニメーション コントロールと要素]
     - [ウィンドウを最大化や最小化するときにアニメーションで表示する]
   - フェード関連のオプション:
     - [メニューをフェードまたはスライドして表示する]
     - [ヒントをフェードまたはスライドで表示する]
     - [メニュー項目をクリック後にフェード アウトする]
3. [OK] をクリックして、[コントロール パネル] を閉じます。

Windows 2000 の設定

▶ Microsoft® Windows 2000® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. ［スタート］、［コントロール パネル］、［マウス］の順に選択します。
   b. ［Motion］（動作）タブをクリックします。
      - アクセラレーションを［なし］に設定します。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - ［OK］（OK）をクリックします。
2. アニメーション効果を無効にします。
   a. ［コントロール パネル］の［画面］オプションを選択します。
   b. ［効果］タブをクリックします。
      - ［次のアニメーション効果をメニューとヒントに使用する］オプションをオフにします。
3. ［OK］をクリックして、［コントロール パネル］を閉じます。

注: Windows XP、Windows 2000、または Windows 2008 を実行している KVM ターゲット サーバの場合、KX II を介したリモート接続用に、専用のユーザ名を作成することが可能です。これにより、ターゲット サーバのマウス ポインタの速度や加速を KX II 接続用に遅く設定できます。

Windows XP、2000、および 2008 のログイン ページでは、マウスのパラメータが、最適な KX II パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。この結果、これらの画面ではマウスの同期は最適ではありません。

注: Windows KVM ターゲット サーバのレジストリを調整してもかまわない場合のみ、次の操作を行ってください。Windows レジストリ エディタを使って次の設定を変更することにより、ログイン ページで KX II のマウスの同期を改善することができます。
HKey_USERS¥.DEFAULT¥Control Panel¥Mouse:> MouseSpeed = 0、MouseThreshold 1=0、MouseThreshold 2=0。

Linux 設定 (Red Hat 4、Red Hat 5、および Fedora 14)

注: 以下の設定は、標準マウス モード専用に最適化されています。

▶ Linux® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (グラフィカル ユーザ インタフェース)。

1. マウスの設定を行います。
   a. メイン メニュー、［Preferences］（個人設定）、［Mouse］（マウス）の順に選択します。［Mouse Preferences］（マウスの設定）ダイアログボックスが表示されます。

b. [Motion] (動作) タブをクリックします。

c. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間に設定します。

d. [Speed] (速度) グループ内で、[Sensitivity] (感度) を低く設定します。

e. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値を小に設定します。

f. [Mouse Preferences] (マウスの設定) ダイアログ ボックスを閉じます。

注: これらの手順でうまく設定できない場合は、Linux com コマンドラインの方法で説明されているように、コマンド「xset mouse 1 1」を入力します。

2. 画面解像度を設定します。

a. メイン メニュー、[System Settings] (システム設定)、[Display] (画面) の順に選択します。[Display Settings] (画面の設定) ダイアログ ボックスが表示されます。

b. [Display] (画面) タブから、KX II でサポートされている解像度を選択します。

c. [Advanced] (高度) タブから、KX II でサポートされている垂直走査周波数を確認します。

注: ターゲット サーバに接続している場合、ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ を押すと、XF86Config または /etc/X11/xorg.conf (使用中の X サーバ ディストリビューションに応じて決まります) で有効になっているすべての解像度が順にスクロールされ、ビデオ解像度が変更されます。

▶ Linux を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (コマンド ライン)。

1. マウスの加速を正確に 1 に設定し、しきい値も正確に 1 に設定します。コマンド「*xset mouse 1 1*」を入力します。このコマンドは、ログイン時の実行用に設定する必要があります。

2. Linux を実行している各ターゲット サーバが、KX II でサポートされている解像度を、標準 VESA 解像度および垂直走査周波数で使用していることを確認します。

3. さらに、各 Linux ターゲット サーバを、ブランキング時間が VESA の標準値の +/- 40% になるように設定する必要があります。

a. Xfree86 設定ファイル XF86Config を表示します。

b. テキスト エディタを使用して、KX II でサポートされていない解像度をすべて無効にします。

c. (KX II でサポートされていない) 仮想デスクトップ機能を無効にします。

d. ブランキング時間を確認します（VESA 標準の +/- 40%）。

e. コンピュータを再起動します。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログオフし、再度ログインする必要があります。

Red Hat および Fedora KVM のターゲット サーバに関する注意

USB CIM が使用されているターゲット サーバで Red Hat® を実行していて、キーボードやマウスに問題が発生した場合は、ここに説明する設定を試すことができます。

ヒント: これらの手順は、OS を新規にインストールした後でも実行する必要があります。

USB CIM が使用されている Red Hat サーバを設定するには、以下の手順に従います。

1. システムの設定ファイル（通常は /etc/modules.conf）を探します。
2. 任意のエディタを使用して、modules.conf ファイルの alias usb-controller 行を次のように設定します。

   alias usb-controller usb-uhci

   注: /etc/modules.conf ファイル内で usb-uhci が記述されている行が他に存在する場合は、その行を削除するかコメントアウトする必要があります。

   ---

3. ファイルを保存します。
4. 変更を有効にするために、システムをリブートします。

Linux 設定 (標準マウス モードの場合)

注: 以下の設定は、標準マウス モード専用に最適化されています。

Linux® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (グラフィカル ユーザ インタフェース)。

1. マウスの設定を行います。

   a. Red Hat 5 ユーザの場合は、メイン メニュー、[Preferences]（個人設定）、[Mouse]（マウス）の順に選択します。Red Hat 4 ユーザの場合は、[System]（システム）、[Preferences]（個人設定）、[Mouse]（マウス）の順に選択します。[Mouse Preferences]（マウスの設定）ダイアログ ボックスが表示されます。

   b. [Motion]（モーション）タブをクリックします。

   c. [Speed]（速度）グループ内で、[Acceleration]（加速）スライダを正確に中間に設定します。

d. [Speed]（速度）グループ内で、[Sensitivity]（感度）を低く設定します。

e. [Drag & Drop]（ドラッグ & ドロップ）グループ内で、しきい値を小に設定します。

f. [Mouse Preferences]（マウスの設定）ダイアログ ボックスを閉じます。

注: これらの手順でうまく設定できない場合は、Linux com コマンドラインの方法で説明されているように、コマンド「xset mouse 1 1」を入力します。

2. 画面解像度を設定します。

a. メイン メニュー、[System Settings]（システム設定）、[Display]（画面）の順に選択します。[Display Settings]（画面の設定）ダイアログ ボックスが表示されます。

b. [Settings]（設定）タブから、KX II でサポートされている解像度を選択します。

c. [OK]（OK）をクリックします。

注: ターゲット サーバに接続すると、ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ を押すと、XF86Config または /etc/X11/xorg.conf（使用中の X サーバ ディストリビューションに応じて決まります）で有効になっているすべての解像度が順にスクロールされ、ビデオ解像度が変更されます。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

SUSE Linux 10.1 の設定

注: SUSE Linux® ログイン プロンプトでマウスを同期しないでください。マウス カーソルを同期するには、ターゲット サーバに接続している必要があります。

▶ マウスを設定するには、以下の手順に従います。

1. **[デスクトップ] メニューの [コントロールセンター] を選択します。[Desktop Preferences]（デスクトップの設定）ダイアログ ボックスが表示されます。**
2. [Mouse]（マウス）をクリックします。[Mouse Preferences]（マウスの設定）ダイアログ ボックスが表示されます。
3. [Motion]（動作）タブを開きます。
4. [Speed]（速度）グループ内で、[Acceleration]（加速）スライダを正確に中間位置に設定します。
5. [Speed]（速度）グループ内で、[Sensitivity]（感度）スライダを低く設定します。

6. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値スライダを小に設定します。
7. [Close] (閉じる) をクリックします。

▶ **ビデオを設定するには、以下の手順に従います。**

1. [Desktop Preferences] (デスクトップの設定) の [Graphics Card and Monitor] (グラフィックカードとモニター) を選択します。[Card and Monitor Properties] (カードとモニターのプロパティ) ダイアログ ボックスが表示されます。
2. 解像度と垂直走査周波数に、KX II でサポートされている値が使用されていることを確認します。詳細は、「**サポートされている画面解像度 『343p. 』**」を参照してください。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

Linux の設定の永続化

注: この手順は、使用している Linux® のバージョンによって少し異なる場合があります。

▶ **Linux で設定を永続化するには、以下の手順に従います (プロンプト)。**

1. [System] (システム) メニュー、[Preferences] (設定)、[Personal] (個人)、[Sessions] (セッション) の順に選択します。
2. [Session Options] (セッション オプション) タブをクリックします。
3. [Prompt on log off] (ログオフ時にプロンプト) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。
4. ログアウトするときに、ダイアログで [Save current setup] (現在の設定を保存) オプションを選択します。
5. [OK] (OK) をクリックします。

ヒント: ログアウト時にプロンプトが表示されないようにするには、代わりに以下の手順に従います。

▶ **Linux で設定を永続化するには、以下の手順に従います (プロンプトなし)。**

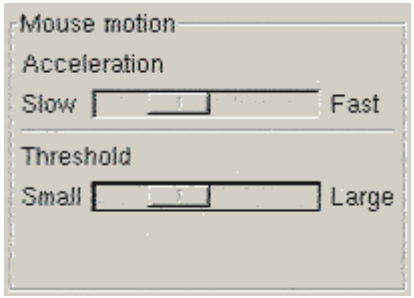
1. [Desktop] (デスクトップ)、[Control Center] (コントロールセンタ)、[System] (システム)、[Sessions] (セッション) の順にを選択します。
2. [Session Options] (セッション オプション) タブをクリックします。

3. [Prompt on the log off] (ログオフ時にプロンプト) チェックボックスをオフにします。
4. [Automatically save changes to the session] (セッションに対する変更を自動保存) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションが自動的に保存されます。

Sun Solaris の設定

▶ Sun™ Solaris™ を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定します。そのためには、以下の操作を行います。
   - グラフィカル ユーザ インタフェースを使用する場合



   - コマンド ラインを使用する場合 *xset mouse a t "a"* は加速 (acceleration)、*"t"* はしきい値 (threshold) を意味します。
2. すべての KVM ターゲット サーバは、KX II でサポートされているいずれかの表示解像度に設定する必要があります。Sun マシンで一般的にサポートされる解像度を以下に示します。

表示解像度	垂直操作周波数	縦横比
1600 x 1200	60 Hz	4:3
1280 x 1024	60、75、85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60、70、75、85 Hz	4:3
800 x 600	56、60、72、75、85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60、72、75、85 Hz	4:3

3. Solaris オペレーティング システムを実行している KVM ターゲット サーバのビデオ出力は、VGA である必要があります (コンポジット Sync ではなく H-and-V sync)。

▶ **Sun のビデオ カード出力をコンポジット Sync からデフォルト以外の VGA 出力に変更するには、以下の手順に従います。**

1. Stop+A コマンドを発行して、bootprom モードに移行します。
2. 以下のコマンドを発行して、出力解像度を変更します。*setenv output-device screen:r1024x768x70*
3. 次に、`boot` コマンドを実行して、サーバを再起動します。

別の方法として、ラリタンの代理店からビデオ出力アダプタを購入することもできます。

環境	対応するビデオ出力アダプタ
Sun 13W3、コンポジット Sync 出力	APSSUN II Guardian コンバータ
Sun HD15、コンポジット Sync 出力	HD15 から 13W3 への変換用の 1396C コンバータ、およびコンポジット Sync をサポートするための APSSUN II Guardian コンバータ
Sun HD15、独立同期出力	APKMSUN Guardian コンバータ

注: 一部の Sun サーバでは、縁が暗い標準の Sun の背景画面が正確に中央に配置されないことがあります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

マウスの設定

▶ **マウスを設定するには、以下の手順に従います (Sun Solaris 10.1)。**

1. ランチャーを選択します。アプリケーション マネージャ - デスクトップ コントロールが表示されます。
2. マウス スタイル マネージャを選択します。[Style Manager - Mouse] (スタイル マネージャ - マウス) ダイアログ ボックスが表示されます。
3. 速度のスライダを 1.0 に設定します。
4. しきい値のスライダを 1.0 に設定します。
5. [OK] (OK) をクリックします。

コマンド ラインに対するアクセス

1. 右クリックします。
2. [Tool] (ツール)、[Terminal] (ターミナル) の順に選択します。ターミナル ウィンドウが表示されます (ルートでコマンドを発行することをお勧めします)。

ビデオ設定 (POST)

Sun システムには、2 種類の解像度設定があります。POST の解像度と GUI の解像度です。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

現在の POST の解像度を確認するには、以下の手順に従います。

- 次のコマンドを root として実行します。`# eeprom output-device`

POST の解像度を変更するには、以下の手順に従います。

1. `# eeprom output-device=screen:r1024x768x75` を実行します。
2. ログアウトするか、コンピュータを再起動します。

ビデオ設定 (GUI)

GUI の解像度は、お使いのビデオ カードに応じたコマンドを使用して確認および設定できます。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

カード	解像度の確認	解像度の変更
32 ビット	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
64 ビット	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
32 ビットおよび 64 ビット	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。

IBM AIX 5.3 の設定

IBM® AIX™ 5.3 を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

▶ **マウスを設定するには、以下の手順に従います。**

1. ランチャーに移動します。
2. [Style Manager] (スタイル マネージャ) を選択します。
3. [Mouse] (マウス) をクリックします。[Style Manager – Mouse] (スタイル マネージャ – マウス) ダイアログ ボックスが表示されます。
4. スライダを使用して、[Mouse acceleration] (マウスの加速) を 1.0 に設定し、[Threshold] (しきい値) を 1.0 に設定します。
5. [OK] (OK) をクリックします。

▶ **ビデオを設定するには、以下の手順に従います。**

1. ランチャーから、[Application Manager] (アプリケーション マネージャ) を選択します。
2. [System_Admin] を選択します。
3. [Smit]、[Devices] (デバイス)、[Graphic Displays] (グラフィック表示)、[Select the Display Resolution and Refresh Rate] (表示解像度と垂直操作周波数の選択) の順に選択します。
4. お使いのビデオ カードを選択します。
5. [List] (リスト) をクリックします。表示モードの一覧が表示されます。
6. KX II でサポートされている解像度および垂直走査周波数を選択します。詳細は、「*サポートされている画面解像度* 『*343*p. 』」を参照してください。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

UNIX の設定の永続化

注: これらの手順は、お使いの UNIX® の種類 (例: Solaris™、IBM® AIX™) および特定のバージョンによって少し異なる可能性があります。

---

1. [Style Manager] (スタイル マネージャ)、[Startup] (起動) の順に選択します。[Style Manager – Startup] (スタイル マネージャ – 起動) ダイアログ ボックスが表示されます。
2. [Logout Confirmation] (ログアウトの確認) ダイアログ ボックスで、[On] (オン) オプションを選択します。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。

Apple Macintosh の設定

Apple Macintosh® オペレーティング システムを実行している KVM ターゲット サーバに対しては、D2CIM-VUSB およびずれないマウス機能を使用する方法が推奨されます。

注: [USB Profile] (USB プロファイル) メニューまたは [Port Configuration] (ポート設定) ページから USB プロファイル [Mac OS-X, version 10.4.9 and later] (MAC OS X (10.4.9 以降)) を選択する必要があります。

ステップ 2: ネットワーク ファイアウォールの設定

Multi-Platform Client を使用してネットワーク ファイアウォールを介して、または [Port Access] (ポート アクセス) ページを介して KX II にアクセスするには、TCP ポート 5000 または指定した他のポートでの通信を許可するようにファイアウォールを設定する必要があります。

KX II の機能	ファイアウォールでインバウンド通信を許可する必要があるポート
Web アクセス機能	ポート 443 – HTTPS 通信用の標準 TCP ポート
HTTP リクエストの HTTPS への自動リダイレクト (″https://xxx.xxx.xxx.xxx″ の代わりにより一般的な ″http://xxx.xxx.xxx.xxx″ を使用できるようにする機能)	ポート 80 – HTTP 通信用の標準 TCP ポート

別の検出ポートを指定する方法についての詳細は、「*ネットワーク設定* 『*173*p. 』」を参照してください。

手順 3: 装置の接続

KX II を、電源、ネットワーク、ローカル PC、ローカル ビデオ ディスプレイ、キーボード、マウス、およびターゲット サーバに接続します。図中の文字は、このセクションで接続を解説しているトピックに対応しています。

A. AC 電源:

▶ 電源を接続するには、以下の手順に従います。

1. 付属の AC 電源コードを KX II と AC 電源コンセントに接続します。
2. 二重化電源フェイルオーバ保護を実装するには、付属の 2 つ目の AC 電源コードを、1 つ目の電源コードとは別の電源コンセントに接続します。

*注: システムは自動的に 2 つの電源を検出するように設定されているので、電源コードを 1 本しか接続していない場合、KX II のフロント パネルの電源 LED が赤色で点灯します。 使用されていない電源の自動検出をオフにする方法については、「*電源設定 *『*205*p. の*"[Power Supply Setup] (電源設定)*"参照 』」を参照してください。*

B. モデム ポート (オプション)

KX II は、LAN/WAN が利用できない場合でもリモート アクセス用の専用モデムポートを搭載しています。ストレート シリアル (RS-232) ケーブルを使用して、外付けシリアル モデムを KX II の背面にある「MODEM」のラベルの付いたポートに接続します。認定済みモデムのリストについては、「*仕様 『339*p. 』」を、モデムの設定については「*モデムを設定する 『191*p. 』」を参照してください。

注: モデムは、CD (キャリア検出) 設定を有効にするように設定することをお勧めします。

C. ネットワーク ポート

KX II は、フェイルオーバ用に 2 つの Ethernet ポートを提供しています (負荷分散用ではない)。デフォルトでは LAN1 のみがアクティブで、自動フェイルオーバは無効になっています。自動フェイルオーバが有効な場合、KX II の内部ネットワーク インタフェース、またはその接続先のネットワークが使用できなくなると、同じ IP アドレスで LAN2 が利用可能になります。

注: フェイルオーバ ポートは実際にフェイルオーバが発生するまで有効にならないので、フェイル オーバ ポートを監視しないか、フェイルオーバが発生した後にのみ監視するようにすることをお勧めします。

▶ ネットワークを接続するには、以下の手順に従います。

1. (付属の) 標準 Ethernet ケーブルを、「LAN1」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
2. オプションの KX II Ethernet フェイルオーバ機能を使用するには、以下の手順に従います。
   - 標準 Ethernet ケーブルを、「LAN2」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
   - [Network Configuration] (ネットワーク設定) ページで [Enable Automatic Failover] (自動フェイルオーバを有効にする) をオンにします。

注: 1 つをフェイルオーバ用のポートとして使用する場合のみ、ネットワーク ポートを 2 つ使用してください。

D. ローカル アクセス ポート (ローカル ビデオ ディスプレイ、キーボード、およびマウス)

KX II のローカル アクセス ポートを使用することによって、ラックからターゲット サーバに簡単にアクセスできます。ローカル アクセス ポートはインストールおよび設定に必要ですが、それ以降の使用についてはオプションです。ローカル アクセス ポートでは、管理およびターゲット サーバへのアクセスに KX II ローカル コンソールのグラフィカル ユーザ インタフェースも使用できます。

KX2-808、KX2-808 および KX2-864 には、ローカルでターゲット サーバにアクセスできるように、デバイスの背面に「EXT LOCAL」というラベルの付いた拡張ローカル ポートも用意されています。拡張ローカル ポートは、最初のインストールおよび設定には必要ありません。これはデフォルトでは有効になっていません。ローカル コンソールおよびリモート コンソールから設定します。 詳細については、「*KX II のローカル ポートの設定 『246*p. 』」を参照してください。

▶ ローカル ポートに接続するには、以下の手順に従います。

- マルチシンク VGA モニタ、マウス、キーボードを、対応するローカル ユーザ ポートに接続します。キーボードとマウスは、PS/2 または USB 互換のものを使用します (KX2-808、DKX2-832 および DKX2-864 では USB のみ)。ローカル ユーザ ポートおよび拡張ローカル ポートの物理的な接続位置は、KX II の背面パネルです。

接続	説明
モニタ	標準マルチシンク VGA モニタを HD15 (メス) ビデオ ポートに接続します。
キーボード	標準 PS/2 キーボードを Mini-DIN6 (メス) キーボード ポートに接続するか、標準 USB キーボードを USB タイプ A (メス) ポートのいずれかに接続します。
マウス	標準 PS/2 マウスを Mini-DIN6 (メス) マウス ポートに接続するか、標準 USB マウスを USB タイプ A (メス) ポートのいずれかに接続します。

注: 今後の KX II モデルでは、PS/2 ローカル ポートではなく USB ポートを提供します。

E. ターゲット サーバ ポート

KX II は、標準 UTP ケーブル (Cat5/5e/6) を使用して各ターゲット サーバに接続します。KX II とターゲット サーバとの間のサポートされている距離については、「*サポートされているターゲット サーバとの接続距離/リフレッシュ レート/画面解像度* 『*345*p. の"*サポートされているターゲット サーバとビデオ*"参照 』」を参照してください。デジタル CIM (DCIM) を使用している場合は、「*デジタル CIM ターゲット サーバのタイミングおよび画面解像度* 『*349*p. 』」を確認してください。

▶ ターゲット サーバを **KX II** に接続するには、以下の手順に従います。

1. 適切なコンピュータ インタフェース モジュール (CIM) またはデジタル コンピュータ インタフェース モジュール (DCIM) を使用します。 各オペレーティング システムに対応する CIM の詳細については、「*サポートされているコンピュータ インタフェース モジュール (CIM) の仕様* 『*345*p. 』」を参照してください。
2. お使いの CIM/DCIM の HD15 ビデオ コネクタをターゲット サーバのビデオ ポートに接続します。ターゲット サーバのビデオが、サポートされている解像度と垂直走査周波数に設定されていることを確認します。Sun サーバの場合は、ターゲット サーバのビデオ カードがコンポジット Sync ではなく標準 VGA (H-and-V Sync) を出力するように設定されていることも確認してください。
3. お使いの CIM/DCIM のキーボード/マウス コネクタを、ターゲット サーバの該当するポートに接続します。ターゲット サーバのビデオ ポートから KX II に接続する場合は、DCIM を使用します。
4. KX II の背面にあるサーバ ポートに CIM を接続します。CIM には標準のストレート UTP (Cat5/5e/6) ケーブルを、DCIM には標準の USB ケーブルを使用します。

注: DCIM-USB G2 の背面には小さいスライド型スイッチがあります。PC ベースの USB ターゲット サーバの場合はスイッチを P にします。Sun の USB ターゲット サーバの場合はスイッチを S にします。

変更後のスイッチ位置が有効になるのは、CIM に給電し直した後です。CIM に給電し直すには、ターゲット サーバから USB コネクタをいったん取り外し、数秒経ってから再度取り付けます。

手順 4: KX II の設定

KX II デバイスの電源を初めてオンにしたときは、KX II ローカル コンソールで以下の操作を行う必要があります。

- デフォルト パスワードの変更
- IP アドレスの割り当て
- 日付/時刻の設定（オプション）
- KVM ターゲット サーバの命名

Web ブラウザを使用して KX II をリモートで設定できます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。

デフォルト パスワードの変更

KX II の出荷時には、デフォルトのパスワードが設定されています。KX II を初めて起動したときは、このパスワードを変更する必要があります。

▶ **デフォルトのパスワードを変更するには、以下の手順に従います。**

1. 本体が起動したら、デフォルトのユーザ名（admin）とパスワード（raritan）を入力します。[ログイン] をクリックします。
2. 古いパスワード（raritan）を入力し、新しいパスワードを入力した後、もう一度新しいパスワードを入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。[適用] をクリックします。[確認] ページで [OK] をクリックします。
3. 注: デフォルトのパスワードは Raritan Multi-Platform Client (MPC) からも変更できます。

注: デフォルトのパスワードは Raritan Multi-Platform Client (MPC) からも変更できます。

IP アドレスの割り当て

ここでは、[ネットワーク設定] ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作の詳細については、「*ネットワーク設定 『173p. 』*」を参照してください。

▶ **IP アドレスを割り当てるには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KX II デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。

3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。
   e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。
   - [None] (なし) (静的 IP) - このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

     KX II はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。
   - [DHCP] (DHCP) - DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

     このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。
4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。
   a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。
   b. [Global/Unique IP Address] (グローバル/一意の IP アドレス) を入力します。これは、KX II に割り当てられる IP アドレスです。
   c. [Prefix Length] (固定長) を入力します。これは、IPv6 アドレスで使用されるビット数です。
   d. [Gateway IP Address] (ゲートウェイ IP アドレス) を入力します。
   e. [Link-Local IP Address] (リンク - ローカル IP アドレス)。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索で、またはルータが存在しない場合に使用されます。
      [Read-Only] (読み取り専用)
   f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。[Read-Only] (読み取り専用)
   g. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None]（設定しない）– 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します（静的 IP）。推奨されるデフォルトのオプションです。

  [IP auto configuration]（IP 自動設定）で [None]（設定しない）を選択すると、[Network Basic Settings]（ネットワーク基本設定）フィールド（[Global/Unique IP Address]（グローバル/一意の IP アドレス）、[Prefix Length]（固定長）、[Gateway IP Address]（ゲートウェイ IP アドレス））が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery]（ルータ検出）– このオプションを使用して、直接接続されるサブネットにのみ適用される [Link Local]（リンクローカル）を超える [Global]（グローバル）または [Unique Local]（一意ローカル）を意味する IPv6 アドレスを自動的に割り当てます。

5. [DHCP] が選択され、[Obtain DNS Server Address]（DNS サーバ アドレスを取得）が有効になっている場合は、[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得）を選択します。[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得）が選択されると、DHCP サーバが提供する DNS 情報が使用されます。
6. [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用）を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバの接続に使用されます。

   [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用）オプションを選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

   a. [Primary DNS Server IP Address]（プライマリ DNS サーバ IP アドレス）
   b. [Secondary DNS Server IP Address]（セカンダリ DNS サーバ IP アドレス）
7. 完了したら [OK] をクリックします。

[ネットワーク設定] ページのこのセクションの設定については、「*LAN インタフェース設定* 『*178*p. 』」を参照してください。

*注: 一部の環境では、[LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のデフォルトである [Autodetect] (自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、KX II の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) フィールドを [100 Mbps/Full Duplex] (またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細については、「*ネットワーク設定 『*173*p. 』」を参照してください。*

日付/時刻の設定 (オプション)

必要に応じて、日付と時刻を設定します。日付と時刻の設定は、LDAPS が有効になっている場合に SSL 証明書の検証に影響します。

▶ **日付と時刻を設定するには、以下の手順に従います。**

1. [デバイス設定] の [日付/時刻] を選択します。[日付/時刻の設定] ページが開きます。
2. [タイム ゾーン] ドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、[夏時間用の調整] チェックボックスをオンにします。
4. 日付と時刻の設定で用いる方法を選択します。
   - [ユーザによる時刻定義]: 日付と時刻を手動で入力するには、このオプションを選択します。[ユーザによる時刻定義] オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - [NTP サーバと同期]: 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期するには、このオプションを選択します。
5. [NTP サーバと同期] オプションを選択した場合は、以下の手順に従います。
   a. プライマリ タイム サーバの IP アドレスを入力します。
   b. セカンダリ タイム サーバの IP アドレスを入力します。(オプション)
6. [OK] をクリックします。

ターゲット サーバの命名

▶ **ターゲット サーバに名前を付けるには、以下の手順に従います。**

1. まだすべてのターゲット サーバを接続していない場合は、接続します。装置の接続方法の詳細については、「**手順 3: 装置の接続**『32p. 』」を参照してください。
2. KX II ローカル コンソールを使用して、[デバイス設定] の [ポート設定] を選択し、名前を付けるターゲット サーバの [ポート名] をクリックします。
3. サーバの名前を入力します。名前には最大 32 文字の英数字と特殊文字を使用できます。[OK] をクリックします。

ターゲット名で使用できる有効な特殊文字

ﾎﾄﾗｮ	説明	ﾎﾄﾗｮ	説明
!	感嘆符	;	セミコロン
″	二重引用符	=	等号
#	シャープ記号	>	大なり記号
$	ドル記号	?	疑問符
%	パーセント記号	@	アット記号
&	アンパサンド	[	左角かっこ
(	左かっこ	¥	バックスラッシュ
)	右かっこ	]	右角かっこ
*	アスタリスク	^	キャレット
+	プラス記号	_	アンダースコア
,	コンマ	`	低アクセント
−	ダッシュ	{	左中かっこ
.	ピリオド	|	パイプ記号
/	前方スラッシュ	}	右中かっこ
<	小なり記号	~	ティルデ
:	コロン		

電源の自動検出の指定

KX II には二重化電源が搭載されており、これらの電源の状態を検出し、通知できます。正しく設定することで、電源に障害が発生した場合に KX II によって適切な通知が送信されます。

[Power Supply Setup]（電源設定）ページは、2 つの電源が使用されている場合に両方の電源を自動的に検出するように設定されています。お使いの設定で電源を 1 つだけ使用している場合は、[Power Supply Setup]（電源設定）ページから自動検出を無効にできます。

▶ **使用中の電源の自動検出を有効にするには、以下の手順に従います。**

1. [Device Settings]（デバイス設定）の [Power Supply Setup]（電源設定）を選択します。[Power Supply Setup]（電源設定）ページが開きます。
2. 電源入力を 1 番目の電源（デバイス背面の左端の電源）に接続している場合は、[Powerln1 Auto Detect]（Powerln1 自動検出）チェック ボックスをオンにします。
3. 電源入力を 2 番目の電源（デバイス背面の右端の電源）に接続している場合は、[Powerln2 Auto Detect]（Powerln2 自動検出）チェック ボックスをオンにします。
4. [OK]（OK）をクリックします。

注: これらのチェック ボックスのいずれかをオンにしたにもかかわらず、電源入力が実際には接続されていない場合は、デバイス前面の電源 LED が赤色で点灯します。

▶ **使用されていない電源の自動検出を無効にするには、以下の手順に従います。**

1. KX II ローカル コンソールで、[Device Settings]（デバイス設定）の [Power Supply Setup]（電源設定）を選択します。[Power Supply Setup]（電源設定）ページが開きます。
2. 使用されていない電源の自動検出をオフにします。

詳細は、「*電源設定『205*p. の*"[Power Supply Setup]（電源設定）"*参照 』」を参照してください。

CC-SG ユーザへの注意事項

KX II を CC-SG 設定で使用している場合は、インストールを行い、その後、**CommandCenter Secure Gateway のユーザ ガイド**、**管理者ガイド**、**デプロイメント ガイド**のいずれかを参照して作業を続行してください（これらのガイドはラリタンの Web サイト（www.raritan.com）内の「Support」セクションから入手できます）。

注: このヘルプの以降のセクションでは、CC-SG の統合機能なしに KX II デバイスを展開する作業を中心に説明します。

リモート認証

CC-SG ユーザへの注意事項

CommandCenter Secure Gateway を使用して KX II を制御している場合、ローカル ポート アクセスを必要とするローカル ユーザを除き、ユーザおよびグループは CC-SG によって認証されます。CC-SG で KX II を制御している場合、ローカル ポート ユーザは、KX II 上で設定されているローカル ユーザ データベースまたはリモート認証サーバ (LDAP/LDAPS または RADIUS) に対して認証され、CC-SG ユーザ データベースに対して認証されません。

CC-SG 認証についての詳細は、*ラリタンの Web サイト http://www.raritan.com* の「Support」セクションからダウンロードできる CommandCenter Secure Gateway のユーザ ガイド、管理者ガイド、またはデプロイメント ガイドを参照してください。

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、KX II には認証要求を外部認証サーバへ転送する機能があります。LDAP/LDAPS と RADIUS の 2 つの外部認証プロトコルがサポートされています。

Microsoft Active Directory についての注意事項

Microsoft® Active Directory® は、LDAP/LDAPS プロトコルをネイティブに使用し、LDAP/LDAPS サーバおよび KX II の認証元として機能することが可能です。IAS (インタフェース認可サーバ) のコンポーネントを装備している場合、Microsoft Active Directory サーバは、RADIUS 認証元としても機能します。

ユーザ グループおよびユーザを作成する

KX II にアクセスするためには、初期設定の一環としてユーザ グループおよびユーザを定義する必要があります。

KX II では、システムによって定義されているデフォルトのユーザ グループを使用して、グループの作成および目的に合った適切な許可の指定を行えるようになります。

KX II にアクセスするには、ユーザ名とパスワードが必要です。この情報は、KX II にアクセスしようとしているユーザを認証するために使用されます。 ユーザ グループやユーザの追加方法および編集方法の詳細については、「ユーザ管理『145p. の"[User Management] (ユーザ管理)"参照 』」を参照してください。

手順 5: KX II リモート コンソールの起動

▶ **KX II リモート コンソールを起動するには、以下の手順に従います。**

1. KX II には、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、ネットワーク接続機能を備えた任意のコンピュータからログインできます (JRE® は *Java の Web サイト http://java.sun.com/*から入手できます)。
2. サポートされている Web ブラウザ (Internet Explorer® や Firefox® など) を起動します。
3. .NET の URL 「*http://IP-ADDRESS*」または「*http://IP-ADDRESS/akc*」を入力します。IP-ADDRESS は KX II に割り当てられる IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた KX II の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (KX II では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
4. ユーザ名とパスワードを入力します。[ログイン] をクリックします。

リモートからのターゲット サーバのアクセスと制御

KX II の [ポート アクセス] ページには、すべての KX II ポート、接続中のターゲット サーバ、ターゲット サーバの状態およびその可用性が表示されます。

ターゲット サーバへのアクセス

▶ **ターゲット サーバにアクセスするには、以下の手順に従います。**

1. アクセスしたいターゲット サーバのポート名をクリックします。[ポート アクション] メニューが開きます。
2. [ポート アクション] メニューの [接続] をクリックします。[KVM] ウィンドウが開き、ターゲットへの接続が示されます。

ターゲット サーバの切り替え

▶ **KVM ターゲット サーバを切り替えるには、以下の手順に従います。**

1. ターゲット サーバを使用しているときに、KX II の [ポート アクセス] ページを開きます。
2. アクセスするターゲットの [ポート名] をクリックします。[ポート アクション] メニューが表示されます。
3. [ポート アクション] メニューの [切り替え元] を選択します。選択した新しいターゲット サーバが表示されます。

ターゲット サーバの切断

▶ ターゲット サーバを切断するには、以下の手順に従います。

- 切断するターゲットのポート名をクリックします。[ポート アクション] メニューが表示されたら、[切断] をクリックします。

手順 6: キーボード言語の設定 (オプション)

注: 英語 (アメリカ)/インターナショナル キーボードを使用している場合は、この手順を実行する必要はありません。

英語 (アメリカ) 以外の言語を使用する場合、キーボードを適切な言語に設定する必要があります。また、クライアント マシンおよび KVM ターゲット サーバのキーボード言語を同じにする必要があります。

キーボード レイアウトを変更する方法の詳細については、お使いのオペレーティング システムのマニュアルを参照してください。

キーボード レイアウト コードの変更 (Sun ターゲット)

この手順は、DCIM-SUSB を使用していて、キーボード レイアウトを別の言語に変更する場合に使用します。

▶ キーボード レイアウト コードを変更するには、以下の手順に従います (DCIM-SUSB のみ)。

1. Sun™ ワークステーション上で [テキスト エディタ] ウィンドウを開きます。
2. Num Lock キーが有効であることを確認した後、キーボードの左の Ctrl キーと Del キーを押します。Caps Lock ライトが点滅して、CIM がレイアウト コード変更モードであることを示します。テキスト ウィンドウに、「`Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`」と表示されます。
3. 適切なレイアウト コード (たとえば日本語キーボードは *31*) を入力します。
4. Enter キーを押します。
5. デバイスの電源を切った後、再度電源を入れます。DCIM-SUSB がリセット (電源の再投入) されます。
6. 入力した文字が正しく表示されることを確認します。

手順 7: カスケード接続の設定 (オプション)

オプションのカスケード接続機能を利用することにより、カスケード接続 KX II をベース KX II に接続できます。これにより、ベース ProductName からサーバおよび PX PDU にアクセスできます。ローカル アクセスとリモート アクセスのどちらも可能です。 この機能の詳細については、**KX II ヘルプ**の「**[Device Management] (デバイス管理)** 『173p. の"**デバイス管理**"参照 』」セクションを参照してください。

ベース KX II デバイスのターゲット サーバ ポートとカスケード接続 KX II デバイスのローカル アクセス ポート (ビデオ/キーボード/マウス ポート) を、D2CIM-DVUSB で接続します。

カスケード接続デバイスが KX2-808、KX2-832 または KX2-864 である場合は、ベース デバイスのターゲット サーバ ポートと KX2-808/KX2-832/KX2-864 の拡張ローカル ポートを直接接続します。

▶ ティアー接続を有効にするには

1. ティアー接続構成内のベース デバイスで、[Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services Settings] (デバイス サービス設定) ページが表示されます。
2. [Enable Tiering as Base] (ベースとしてのティアー接続を有効にする) を選択します。
3. [Base Secret] (ベース秘密ワード) フィールドに、ベース デバイスとティアー接続デバイスの間で共有される秘密ワードを入力します。この秘密ワードは、ティアー接続デバイスでベース デバイスを認証する際に必要となります。同じ秘密ワードをティアー接続デバイスに対して入力します。
4. [OK] (OK) をクリックします。
5. ティアー接続デバイスを有効にします。ティアー接続デバイスで、[Device Settings] (デバイス設定) の [Local Port Settings] (ローカル ポート設定) を選択します。
6. このページの [Enable Local Ports] (ローカル ポートを有効にする) セクションで、[Enable Local Port Device Tiering] (ローカル ポート デバイスのティアー接続を有効にする) を選択します。
7. [Tier Secret] (ティアー接続秘密ワード) フィールドに、ベース デバイスの [Device Settings] (デバイス設定) ページで入力したのと同じ秘密ワードを入力します。
8. [OK] (OK) をクリックします。

Ch 3 ターゲット サーバの使用

この章の内容

KX II インタフェース 46
KX II ローカル コンソール インタフェース: KX II デバイス 47
KX II リモート コンソール インタフェース 47
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 66
Virtual KVM Client (VKC) および Active KVM Client (AKC) 68
Multi-Platform Client (MPC) 112

KX II インタフェース

KX II には、いつでも、どこからでもターゲットへの簡単なアクセスを可能にするいくつかのユーザ インタフェースが用意されています。このようなユーザ インタフェースには、KX II ローカル コンソール、KX II リモート コンソール、Virtual KVM Client (VKC)、Active KVM Client (AKC)、および Multi-Platform Client (MPC) があります。以下の表に、ターゲット サーバのアクセスおよび管理のためにこれらのインタフェースをローカルおよびリモートで使用できるかどうかを示します。

ユーザ インタフェース	ローカル		リモート	
	アクセス	管理	アクセス	管理
KX II ローカル コンソール	✓	✓		
KX II リモート コンソール			✓	✓
Virtual KVM Client (VKC)			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

ヘルプの以降のセクションでは、以下のインタフェースを使用した KX II へのアクセスおよびターゲット管理の方法について説明します。

- ローカル コンソール
- リモート コンソール
- Virtual KVM Client
- Multi-Platform Client

KX II ローカル コンソール インタフェース: KX II デバイス

サーバ ラックに設置した KX II の場合は、KX II ローカル コンソールを介して、標準 KVM 管理を行います。KX II ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。

KX II ローカル コンソールと KX II リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

[KX II Local Console Factory Reset] (KX II ローカル コンソール ファクトリ リセット) オプションは、KX II ローカル コンソールには用意されていますが、KX II リモート コンソールには用意されていません。

KX II リモート コンソール インタフェース

KX II リモート コンソールは、ブラウザ ベースのグラフィカル ユーザ インタフェースで、このコンソールを通じて、KX II に接続されている KVM ターゲット サーバおよびシリアル ターゲットにログインして、KX II をリモート管理できます。

KX II リモート コンソールは、接続されているターゲット サーバへのデジタル接続を提供します。KX II リモート コンソールを使用して KVM ターゲット サーバにログインすると、Virtual KVM Client のウィンドウが開きます。

KX II ローカル コンソールと KX II リモート コンソールのグラフィカル ユーザ インタフェースには多くの類似点があります。相違点については、ユーザ マニュアルに記載されています。以下のオプションは KX II リモート コンソールに用意されていますが、KX II ローカル コンソールには用意されていません。

- 仮想メディア
- [Favorites] (お気に入り)
- [Backup/Restore] (バックアップ/リストア)
- [Firmware Upgrade] (ファームウェアのアップグレード)
- SSL 証明書
- 音声

KX II リモート コンソールの起動

重要: ブラウザの種類を問わず、KX II リモート コンソールを起動するためには、デバイスの IP アドレスからのポップアップを許可する必要があります。

お使いのブラウザおよびセキュリティの設定により、セキュリティと証明書に関する各種の警告が表示されることがあります。KX II リモートコンソールを起動するには、これらの警告を承諾する必要があります。

セキュリティと証明書に関する警告メッセージに対して以下のオプションをオンにすることにより、それ以降にログインしたときに表示される警告メッセージを減らすことができます。

- ［今後、この警告を表示しない］
- ［この発行元からのコンテンツを常に信頼する］

▶ KX II リモート コンソールを起動するには、以下の手順に従います。

1. KX II には、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、ネットワーク接続機能を備えた任意のコンピュータからログインできます (JRE® は *Java の Web サイト http://java.sun.com/*から入手できます)。
2. サポートされている Web ブラウザ (Internet Explorer® や Firefox® など) を起動します。
3. .NET の URL 「*http://IP-ADDRESS*」または「*http://IP-ADDRESS/akc*」を入力します。IP-ADDRESS は KX II に割り当てられる IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた KX II の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (KX II では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
4. ユーザ名とパスワードを入力します。初めてログインする場合は、工場出荷時のデフォルト ユーザ名 (admin) とパスワード (すべて小文字の raritan) を使用してログインします。デフォルトのパスワードを変更するように求められます。 ［Login］(ログイン) をクリックします。

注: デバイスにアクセスする際にセキュリティ同意書を読むことまたはその内容に同意することを、管理者から要求されている場合、ログイン証明書を入力して ［Login］(ログイン) をクリックした後にセキュリティ バナーが表示されます。

リモート コンソールを介して利用できる KX II の機能についての詳細は、「*Virtual KVM Client および Active KVM Client (AKC)* 『*68*p. の *"Virtual KVM Client (VKC) および Active KVM Client (AKC)"*参照 』」を参照してください。

インタフェースおよび画面操作

KX II インタフェース

KX II リモート コンソール インタフェースと KX II ローカル コンソール インタフェースは、デバイス設定および管理、ターゲット サーバのリストおよび選択用に、Web ベース インタフェースを備えています。オプションは複数のタブに配置されています。

正常にログインすると、[ポート アクセス] ページが表示され、すべてのポートについて、そのステータスと可用性が表示されます。このページの 4 つのタブでは、ポート別またはグループ別に表示したり、検索して表示したりできます。列の見出しをクリックすることで、ポート番号、ポート名、ステータス ([Up] (アップ) および [Down] (ダウン))、可用性 ([Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、[Unavailable] (使用不可能)、[Connecting] (接続中)) で並べ替えを行うことができます。詳細については、「*[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)* 『*53*p. 』」を参照してください。

[Set Scan] (スキャン設定) タブを使用して、KX II に接続されているターゲットを 32 台までスキャンできます。「*ポートのスキャン* 『*59*p. 』」を参照してください。

左パネル

KX II インタフェースの左パネルにある情報は次のとおりです。なお、一部の情報は特定の条件下でのみ表示されます。たとえば、自分が特定のユーザである場合や、特定の機能を利用している場合などです。各情報が表示される条件もこの表に示します。

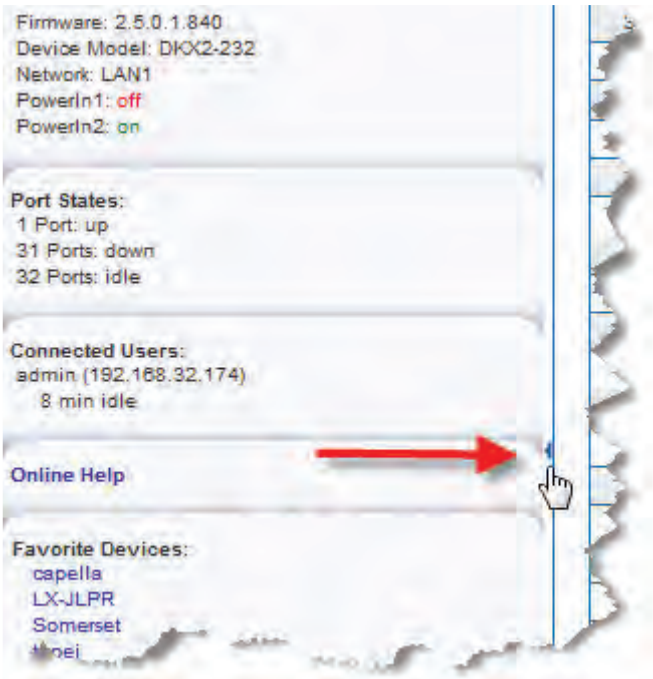
情報	説明	表示される条件
[Time & Session] (日時およびセッション)	現在のセッションが開始した日時。	常時
ユーザ	ユーザ名。	常時
[State] (状態)	アプリケーションの現在の状態 (アイドルまたはアクティブ)。アイドル状態の場合、セッションがアイドル状態になっている時間が追跡および表示されます。	常時
[Your IP] (あなたの IP アドレス)	KX II にアクセスする際に使用された IP アドレス。	常時
[Last Login] (最終ログイン日時)	最後にログインした日時。	常時
[Under CC-SG Management] (CC-SG の管理下)	KX II を管理している CC-SG デバイスの IP アドレス。	KX II が CC-SG の管理下にある場合。
[Device Information] (デバイス情報)	使用している KX II に特有の情報。	常時
[Device Name] (デバイス名)	デバイスに割り当てられている名前。	常時
IP アドレス	KX II の IP アドレス。	常時
[Firmware] (ファームウェア)	ファームウェアの現在のバージョン。	常時
[Device Model] (デバイス モデル)	KX II のモデル。	常時

情報	説明	表示される条件
[Serial number] (シリアル番号)	KX II のシリアル番号。	常時
ネットワーク	現在のネットワークに割り当てられている名前。	常時
[PowerIn1] (電源入力 1)	電源コンセント 1 の接続状態 オンまたはオフ、または自動検出オフ。	常時
[PowerIn2] (電源入力 2)	電源コンセント 2 の接続状態 オンまたはオフ、または自動検出オフ。	常時
[Configured As Base] (ベース デバイスとして設定) または [Configured As Tiered] (カスケード接続デバイスとして設定)	カスケード接続を使用している場合、現在アクセスしている KX II がベースデバイスとカスケード接続デバイスのどちらであるかが表示されます。	KX II がカスケード接続構成の一要素になっている場合
ポートの状態	KX II によって現在使用されているポートのステータス。	常時
[Connect Users] (接続しているユーザ)	現在 KX II に接続している、ユーザ名と IP アドレスによって識別されるユーザ。	常時
オンライン ヘルプ	オンライン ヘルプへのリンク。	常時
お気に入りデバイス	「*お気に入りの管理* 『*62*p. 』」を参照してください。	常時
[FIPS Mode] (FIPS モード)	FIPS モード: 有効、SSL 証明書: FIPS モード準拠。	FIPS が有効になっている場合

左パネルを折りたたんで、ページの表示領域を拡大することができます。

▶ 左パネルを折りたたむには、以下の手順に従います。

- パネルの左側のほぼ中ほどにある青色の左向き矢印をクリックします。パネルが折りたたまれたら、青色の矢印をもう一度クリックすると展開されます。



KX II コンソールでの案内

KX II コンソール インタフェースでは、いくつかの方法でナビゲーションや選択を行うことができます。

▶ オプションを選択するには、以下のいずれかの手順に従います。

- タブをクリックします。利用可能なオプションのページが表示されます。
- タブ上にカーソルを移動し、メニューから適切なオプションを選択します。
- 表示されるメニュー階層（階層リンク）からオプションを直接クリックします。

▶ 画面に収まらないページをスクロールするには、以下のいずれかの手順に従います。

- キーボードの Page Up キーと Page Down キーを使用します。
- 右側にあるスクロール バーを使用します。

[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)

KX II リモート コンソールへのログオンが正常に完了すると、[Port Access] (ポート アクセス) ページに [View by Port] (ポート別に表示) タブが表示されます。このページには、KX II のすべてのポート、そうしたポートに接続されているターゲット サーバ、ポート グループ、およびブレード シャーシが一覧表示されます。

デフォルトでは、情報はポート番号別に並べられますが、表示されているいずれかの列の見出しをクリックすると、その列で並べ替えて表示されます。タブに一度に表示する行数を増減する場合は、[Rows per Page] (ページ当たりの行数) フィールドに行数を入力し、[Set] (設定) をクリックします。

このページでは、各ポートの次の情報が表示されます。

- [Port Number] (ポート番号) - 1 から KX II デバイスで使用できるポートの合計数までの番号が振られています。

  注: 電源タップに接続されているポートは一覧に表示に表示されないため、ポート番号が抜けることになります。

- [Port Name] (ポート名) - KX II ポートの名前です。最初は、「Dominion-KX2-Port#」に設定されていますが、わかりやすい名前に変更できます。
- [Status] (ステータス) - サーバのステータスは [up] (アップ) または [down] (ダウン) のどちらかです。
- [Type] (タイプ) - サーバまたは CIM/DCIM のタイプです。

  ブレード シャーシの場合、タイプは、[Blade Chassis] (ブレード シャーシ)、[Blade] (ブレード)、[BladeChassisAdmin] (ブレードシャーシ管理)、および [BladeChassisURL] (ブレードシャーシ URL) です。

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

▶ **利用可能なターゲット サーバまたはデュアル モニタ ターゲット サーバに接続するには、以下の手順に従います。**

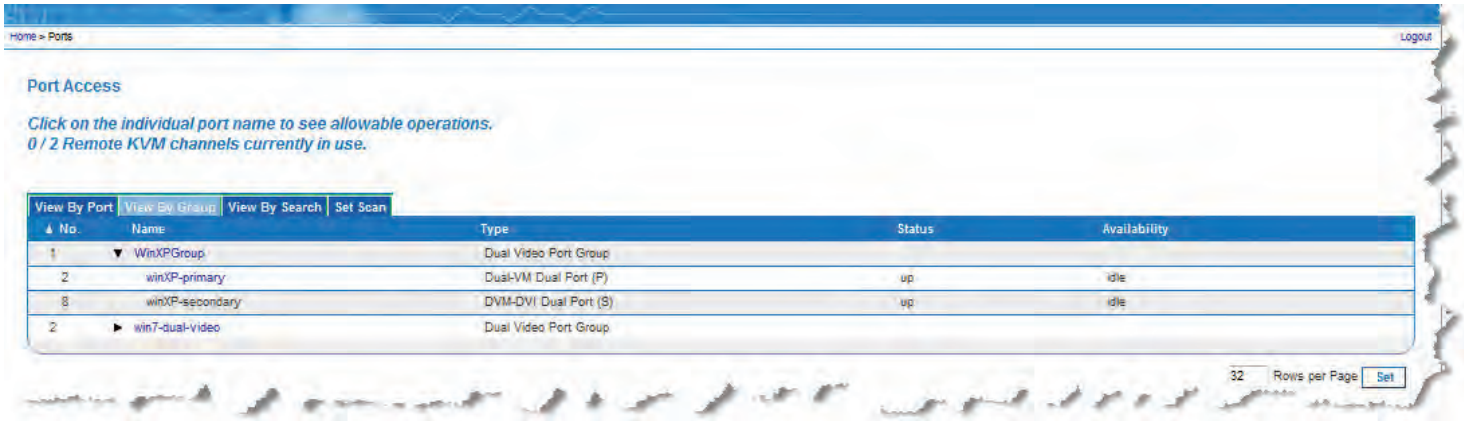
1. ポート名をクリックします。[Port Action] (ポート アクション) メニューが開きます。
2. [接続] をクリックします。ターゲットまたはデュアル モニタ ターゲット サーバに接続したら、ポート グループ名をクリックし、[Disconnect] (切断) をクリックして切断します。

使用可能な他のメニュー オプションの詳細については、「*[Port Action] (ポート アクション) メニュー* 『*57*p. 』」を参照してください。

[View by Group] (グループ別表示) タブ

[View by Group] (グループ別表示) タブには、ブレード シャーシ、「標準の」ポート グループ、およびデュアル ビデオ ポート グループが表示されます。グループの横の展開矢印アイコン ▶ クリックすると、ポート グループに割り当てられたポートが表示されます。

こうしたタイプの各ポート グループの作成方法については、「*デバイス管理 『173p. 』*」を参照してください。



[View by Search] (検索して表示) タブ

[View by Search] (検索して表示) タブでは、ポート名で検索できます。検索時にアスタリスク (*) をワイルドカードとして使用できます。また、名前全体で検索することも名前の一部だけで検索することもできます。

[Set Scan] (スキャン設定) タブ

ポート スキャン機能には、[ポート アクセス] ページの [スキャンの設定] タブからアクセスします。この機能によって、スキャンするターゲットのセットを定義できます。スキャンしたターゲットのサムネイル表示も使用できます。サムネイルを選択すると、そのターゲットが Virtual KVM Client ウィンドウに表示されます。

詳細については、「*ポートのスキャン 『59p. 』*」を参照してください。

カスケード接続デバイス - [Port Access] (ポート アクセス) ページ

ティアー接続構成にしており、ベース KX II デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、 カスケード接続デバイスは、[ポート アクセス] ページでカスケード接続デバイス名の左にある展開矢印アイコン ▶ をクリックすると表示されます。カスケード接続の詳細については、「*カスケード接続の設定および有効化 『181*p. の*"カスケード接続を設定および有効化する"*参照 』」を参照してください。

ブレード シャーシ - [Port Access] (ポート アクセス) ページ

ブレード サーバは、[Port Access] (ポート アクセス) ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ▶ を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

デュアル ビデオ ポート グループ - [Port Access] (ポート アクセス) ページ

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

リモート クライアントからデュアル ポート ビデオ グループにアクセスする場合は、プライマリ ポートに接続すると、デュアル ポート グループのプライマリ ポートおよびセカンダリ ポートの両方に対する KVM 接続ウィンドウが開きます。

注: デュアル ビデオ プライマリ ポートは、ポート グループの作成時に定義されます。

注: プライマリ ポートをクリックしてリモートでデュアル ビデオ ポート グループに接続するには、2 つの KVM チャネルが必要です。2 つのチャネルが利用できない場合、[Connect] (接続) リンクは表示されません。

注: デュアル ビデオ ポート グループのセカンダリ ポートをクリックしても、[Action] (アクション) メニューは表示されません。

注: ローカル ポートからプライマリ ポートおよびセカンダリ ポートに同時に接続することはできません。

[Port Action] (ポート アクション) メニュー

[ポート アクセス] リストで [ポート名] をクリックすると、[ポート アクション] メニューが表示されます。対象のポートに対して適切なメニュー オプションを選択して実行します。[ポート アクション] メニューには、ポートのステータスと可用性に応じて、その時点で利用可能なオプションだけが表示されます。

- [Connect] (接続) – ターゲット サーバへの新しい接続を作成します。KX II リモート コンソールの場合は、新しい Virtual KVM Client ページが表示されます。KX II ローカル コンソールの場合は、ローカル ユーザ インタフェースからターゲット サーバに表示が切り替わります。ローカル ポートで切り替えを行うためには、KX II ローカル コンソール インタフェースが表示されている必要があります。ローカル ポートからのホット キー切り替えも利用できるようになりました。

  注:すべての接続がビジー状態の場合、KX II リモート コンソールで使用可能なポートに対してこのオプションは使用できません。

- [Switch From] (切り替え元) – 既存の接続から選択したポート (KVM ターゲット サーバ) に切り替えます。このメニュー項目は、KVM ターゲットに対してのみ使用できます。このオプションは Virtual KVM Client が開いている場合にのみ表示されます。

  注: KX II ローカル コンソールでは、このメニュー項目は使用できません。

- [Disconnect] (切断) – このポートを切断し、このターゲット サーバの Virtual KVM Client ページを閉じます。このメニュー項目は、ポート ステータスが [Up] (アップ) かつ [Connected] (接続済み) の場合、または [Up] (アップ) かつ [Busy] (ビジー) の場合にのみ使用できます。

  注: KX II ローカル コンソールでは、このメニュー項目は使用できません。ローカル コンソールで切り替えたターゲットを切断する唯一の方法は、ホットキーを使用することです。

- [Power On] (電源オン) – 関連付けられているコンセントを介してターゲット サーバの電源をオンにします。このオプションは、1 つまたは複数の電源がこのターゲットに関連付けられているときにのみ表示されます。
- [Power Off] (電源オフ) – 関連付けられているコンセントを介してターゲット サーバの電源をオフにします。このオプションは、1 つまたは複数の電源がターゲットに関連付けられているとき、ターゲットの電源がオン (ポート ステータスが [Up] (アップ)) のとき、およびこのサービスを操作する許可がユーザーに与えられているときにのみ表示されます。
- [Power Cycle] (電源の再投入) – 関連付けられているコンセントを介してターゲット サーバの電源をいったんオフにしてから再びオンにします。このオプションは、1 つまたは複数の電源がターゲットに関連付けられているとき、およびこのサービスを操作する許可がユーザーに与えられているときにのみ表示されます。

ポートのスキャン

KX II では、選択されたターゲットを検索してそれをスライド ショー ビューで表示するポート スキャン機能を使用すると、最大 32 のターゲットを一度にモニタできます。ターゲットに接続することも、必要に応じて特定のターゲットをフォーカスすることもできます。スキャン対象は、標準ターゲット、ブレード サーバ、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。Virtual KVM Client (VKC) または Active KVM Client (AKC) からスキャン設定を指定します。詳細については、「*VKC および AKC でのスキャンの設定* 『*98*p. 』」を参照してください。

注: デュアル ビデオ ポート グループでは、プライマリ ポートはポートスキャンの対象になりますが、リモート クライアントから接続している場合、セカンダリ ポートは対象になりません。両方のポートをローカルポートからスキャンの対象にすることができます。デュアル ビデオ ポート グループは、KX II 2.5.0 (以降) でサポートされています。

注: カスケード接続デバイスのスキャンは、Multi-Platform Client (MPC) ではサポートされていません。

スキャンを開始すると、[Port Scan] (ポート スキャン) ウィンドウが開きます。ターゲットが見つかるたびに、スライド ショーのサムネイルとして表示されます。スライド ショーでは、デフォルト間隔の 10 秒ごとに、またはユーザが指定した間隔に従ってターゲットのサムネイルがスクロールされます。スキャンによってターゲットがスクロールされるときは、スライド ショーでフォーカスされているターゲットがページの中央に表示されます。「*VKC および AKC でのスキャンの設定* 『*98*p. 』」を参照してください。

スライド ショーでサムネイルのローテーションにかかる時間、サムネイルのフォーカス間隔、ページの画面の設定は、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Multi-Platform Client (MPC) の [Tools] (ツール) の [Options] (オプション) ダイアログの [Scan Settings] (スキャン設定) タブから変更します。「*VKC および AKC でのスキャンの設定* 『*98*p. 』」を参照してください。

ターゲット名はサムネイルの下とウィンドウ下部のタスクバーに表示されます。ターゲットがビジーである場合は、ターゲット サーバへのアクセス ページの代わりに空白の画面が表示されます。

各ターゲットのステータスは、ターゲットのサムネイルの下およびタスクバー (ターゲットがローテーションにおいてフォーカスされている場合) に表示される緑、黄色、赤のライトで示されます。ステータス ライトは、以下を示します。

- 緑 – ターゲットはアップ/アイドルまたはアップ/接続済み
- 黄色 – ターゲットはダウンしているが接続済み
- 赤 – ターゲットはダウン/アイドル、ビジー、またはアクセス不可能

この機能は、ローカル ポート、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Multi-Platform Client (MPC) から使用できます。

---

*注: MPC は、他の Raritan クライアントとは異なる方法を使用してスキャンを開始します。詳細については、『KVM and Serial Client Guide』の「Set Scan Group」を参照してください。リモート コンソールとローカル コンソールでは、スキャンの結果およびオプションが異なります。「*ポートのスキャン - ローカル コンソール *『*318*p. 』」を参照してください。*

▶ ターゲットをスキャンするには、以下の手順に従います。

1. [Port Access] (ポート アクセス) ページの [Set Scan] (スキャン設定) タブをクリックします。
2. 各ターゲットの横にあるチェックボックスをオンにしてスキャン対象に含めるターゲットを個別に選択するか、ターゲット列の上部にあるチェックボックスをオンにしてすべてのターゲットを選択します。
3. アップ ステータスのターゲットだけをスキャンに含める場合は、[Up Only] (アップのみ) チェックボックスをオンのままにします。アップかダウンかに関係なくすべてのターゲットを含める場合は、このチェックボックスをオフにします。
4. [Scan] (スキャン) をクリックしてスキャンを開始します。スキャンされたターゲットは、ページのスライド ショー ビューに表示されます。
5. [Options] (オプション) の [Pause] (一時停止) をクリックすると、スライド ショーが一時停止してターゲット間での移動が停止します。[Options] (オプション) の [Resume] (再開) をクリックするとスライド ショーが再開されます。
6. ターゲットのサムネイルをクリックすると、それが次にスキャンされます。
7. サムネイルをダブルクリックすると、そのターゲットに接続されます。

スキャン オプションの使用

ターゲットのスキャン中は、次のオプションを使用できます。これらのすべてのオプションは、[Expand]（展開）/[Collapse]（折りたたみ）アイコンを除き、[Port Scan]（ポート スキャン）ビューアの左上の [Options]（オプション）メニューから選択します。ウィンドウを閉じると、オプションはデフォルトに戻ります。

注: Virtual KVM Client（VKC）または Active KVM Client（AKC）から表示間隔などのスキャン設定を指定します。詳細については、「VKC および AKC でのスキャンの設定 『98p. 』」を参照してください。

サムネイルの表示または非表示

- ウィンドウの左上の [Expand]（展開）/[Collapse]（折りたたみ）アイコン を使用して、サムネイルを表示または非表示にします。デフォルト表示では展開されています。

サムネイル スライド ショーの一時停止

- [Options]（オプション）の [Pause]（一時停止）を選択すると、あるターゲットから次のターゲットへのサムネイルのローテーションが一時停止します。サムネイルのローテーションはデフォルト設定です。

サムネイル スライド ショーの再開

- [Options]（オプション）の [Resume]（再開）を選択すると、サムネイルのローテーションが再開されます。

[Port Scan]（ポート スキャン）ビューアのサムネイルのサイズ変更

- サムネイルを拡大するには、[Options]（オプション）、[Size]（サイズ）、[360x240] の順に選択します。
- サムネイルを最小化するには、[Options]（オプション）、[Size]（サイズ）、[160x120] の順に選択します。これはデフォルトのサムネイル サイズです。

[Port Scan]（ポート スキャン）ビューアの表示方向の変更

- [Options]（オプション）、[Split Orientation]（分割方向）、[Horizontal]（横）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの下部に沿って表示されます。
- [Options]（オプション）、[Split Orientation]（分割方向）、[Vertical]（縦）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの右側に沿って表示されます。これがデフォルト表示です。

お気に入りの管理

お気に入り機能を利用すると、よく使用するデバイスにすばやくアクセスできます。[ポート アクセス] ページの左下隅（サイドバー）にある [お気に入りデバイス] セクションでは、以下の操作が可能です。

- お気に入りデバイスのリストを作成および管理する。
- よく使用するデバイスにすばやくアクセスする。
- 名前、IP アドレス、または DNS ホスト名別にお気に入りのリストを表示する。
- サブネット上の KX II デバイスを検出する（ログインの前および後）。
- 検出された KX II デバイスを接続されている Dominion デバイスから取得する（ログインの後）。

お気に入りの KX II デバイスにアクセスするには、以下の手順に従います。

- ([Favorite Devices]（お気に入りデバイス）の下に表示されている）デバイス名をクリックします。新しいブラウザが開き、デバイスが表示されます。

お気に入りを名前順に表示するには、以下の手順に従います。

- [Display by Name]（名前順）をクリックします。

お気に入りを IP アドレス順に表示するには、以下の手順に従います。

- [Display by IP]（IP 順）をクリックします。

お気に入りをホスト名順に表示するには、以下の手順に従います。

- [Display by Host Name]（ホスト名順）をクリックします。

[お気に入りの管理] ページ

▶ [お気に入りの管理] ページを開くには、以下の手順に従います。

- 左パネルの［管理］をクリックします。次の内容を含む［お気に入りの管理］ページが表示されます。

メニュー	目的
［お気に入りリスト］	お気に入りデバイスのリストを管理します。
［デバイス検出 － ローカル サブネット］	クライアント PC のローカル サブネット上の Raritan デバイスを検出します。
［デバイス検出 －KX II サブネット］	KX II デバイス サブネット上の Raritan デバイスを検出します。
［お気に入りへの新しいデバイスの追加］	お気に入りリストのデバイスを追加、編集、および削除します。

[お気に入りリスト] ページ

[お気に入りリスト] ページでは、お気に入りリストのデバイスを追加、編集、および削除できます。

▶ **[お気に入りリスト] ページを開くには、以下の手順に従います。**

- [管理] の [お気に入りリスト] を選択します。[お気に入りリスト] ページが開きます。

ローカル サブネット上のデバイスの検出

ローカル サブネット (KX II リモート コンソールが実行されているサブネット) 上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ『64p. 』*」を参照してください。

▶ **ローカル サブネット上のデバイスを検出するには、以下の手順に従います。**

1. [管理] の [デバイス検出 - ローカル サブネット] を選択します。[デバイス検出 - ローカル サブネット] ページが表示されます。
2. 目的の検出ポートを選択します。
   - デフォルトの検出ポートを使用するには、[デフォルト ポート 5000 を使用] チェックボックスをオンにします。
   - 別の検出ポートを使用するには、以下の手順に従います。
   a. [デフォルト ポート 5000 を使用] チェックボックスをオフにします。
   b. [検出ポート] フィールドに、ポート番号を入力します。
   c. [保存] をクリックします。
3. [更新] をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ **デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。**

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. [追加] をクリックします。

▶ **検出されたデバイスにアクセスするには、以下の手順に従います。**

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

KX II サブネット上のデバイスの検出

デバイス サブネット（KX II デバイスの IP アドレスそのもののサブネット）上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ 『64p. 』*」を参照してください。

この機能を使用すると、複数の KX II デバイスが相互に作用し合い、自動的にデバイスを検知し構成を拡張します。KX II リモート コンソールは、KX II のサブネット内の KX II デバイスおよびその他の Raritan デバイスを自動的に検出します。

▶ デバイス サブネット上のデバイスを検出するには、以下の手順に従います。

1. ［管理］の［デバイス検出 – KX II サブネット］を選択します。［デバイス検出 – KX II サブネット］ページが表示されます。
2. ［更新］をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ デバイスを ［お気に入りリスト］ に追加するには、以下の手順に従います。

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. ［追加］をクリックします。

▶ 検出されたデバイスにアクセスするには、以下の手順に従います。

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

お気に入りの追加、削除、および編集

▶ デバイスを ［お気に入りリスト］ に追加するには、以下の手順に従います。

1. ［管理］の［お気に入りへの新しいデバイスの追加］を選択します。［新しいお気に入りの追加］ページが表示されます。
2. わかりやすい説明を入力します。
3. デバイスの IP アドレス/ホスト名を入力します。
4. 必要に応じて検出ポートを変更します。
5. 製品タイプを選択します。
6. ［OK］をクリックします。デバイスがお気に入りのリストに追加されます。

▶ お気に入りを編集するには、以下の手順に従います。

1. [お気に入りリスト] ページで、目的の KX II デバイスの横にあるチェックボックスをオンにします。
2. [編集] をクリックします。[編集] ページが表示されます。
3. 必要に応じてフィールドを更新します。
   - 説明
   - [IP アドレス/ホスト名]: KX II デバイスの IP アドレスを入力します。
   - [ポート] (必要な場合)
   - [製品タイプ]
4. [OK] をクリックします。

▶ お気に入りを削除するには、以下の手順に従います。

重要: お気に入りを削除する場合は注意してください。削除を確認するプロンプトは表示されません。

1. 目的の KX II デバイスの横にあるチェックボックスをオンにします。
2. [削除] をクリックします。お気に入りのリストからお気に入りが削除されます。

ログアウト

▶ **KX II を終了するには、以下の操作を行います。**

- ページの右上隅の [Logout] (ログアウト) をクリックします。

注:ログアウトすると、開いているすべての Virtual KVM Client セッションとシリアル クライアント セッションが閉じられます。

MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定

プロキシ サーバを使用する必要がある場合、リモート クライアント PC 上で SOCKS プロキシを設定する必要があります。

注: インストールされているプロキシ サーバが HTTP プロキシ プロトコルにのみ対応している場合は、接続できません。

▶ **SOCKS プロキシを設定するには**

1. クライアント上で [コントロール パネル] の [インターネット オプション] を選択します。

a. [接続] タブで [LAN の設定] をクリックします。[ローカル エリア ネットワーク (LAN) の設定] ダイアログ ボックスが開きます。

b. [LAN にプロキシ サーバを使用する] チェック ボックスをオンにします。

c. [詳細] をクリックします。[プロキシの設定] ダイアログ ボックスが開きます。

d. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

---

2. 各ダイアログ ボックスで [OK] をクリックし、設定内容を適用します。

3. Java™ アプレット用のプロキシを設定するため、[コントロール パネル] の [Java] を選択します。

e. [基本] タブで [ネットワーク設定] をクリックします。[ネットワーク設定] ダイアログ ボックスが開きます。

f. [プロキシ サーバを使用] をクリックします。

g. [詳細] をクリックします。[詳細ネットワーク設定] ダイアログ ボックスが開きます。

h. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

---

4. スタンドアロン MPC を使用している場合は、次の手順も実行する必要があります。

i. テキスト エディタで、MPC ディレクトリにある start.bat ファイルを開きます。

j. コマンド ラインにパラメータを挿入します。このパラメータは、"-classpath" の前に挿入します。挿入するパラメータは、「-DsocksProxyHost=<SOCKS プロキシ IP アドレス> -DsocksProxyPort=<SOCKS プロキシ ポート番号>」です。

挿入後のコマンドは次のようになります。

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .¥sdeploy.jar;.¥sFoxtrot.jar;.¥jaws.jar;.¥sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC) および Active KVM Client (AKC)

Virtual KVM Client (VKC) および Active KVM Client (AKC) は、リモートターゲットへのアクセスに使用されるインタフェースです。AKC と VKC は、以下の点を除いて特徴が似ています。

- 最小システム要件
- サポートされているオペレーティング システムとブラウザ
- AKC で作成されたキーボード マクロは、VKC では使用できません。
- ダイレクト ポート アクセス設定（「**URL を経由したダイレクト ポート アクセスの有効化**」を参照）
- AKC サーバ証明書検証設定（「**AKC を使用するための前提条件**『70p. の"Prerequisites for Using AKC"参照 』」を参照）

Active KVM Client について

AKC は Microsoft Windows .NET 技術に基づいています。したがって、Raritan の VKC および MPC の実行に必要な Java Runtime Environment (JRE) を使用することなくクライアントを Windows 環境で実行できます。AKC は CC-SG とも連動します。

注: AKC でダイレクト ポート アクセスを使用する場合は、アクセスするターゲットごとに新しいブラウザ ウィンドウまたはブラウザ タブを開く必要があります。現在ターゲットへのアクセスに使用しているのと同じブラウザ ウィンドウまたはブラウザ タブに DPA URL を入力して別のターゲットにアクセスしようとすると、接続できずにエラーが表示される場合があります。

AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ

.NET Framework

AKC には、Windows .NET® バージョン 3.5 または 4.0 が必要です。AKC は、インストールされている 3.5 および 4.0 の両方と連動します。

オペレーティング システム

AKC を Internet Explorer® から起動することで、KX II 2.2 (以降) および LX 2.4.5 (以降) を利用してターゲット サーバに接続できます。 AKC は、.NET Framework 3.5 が実行されている以下のプラットフォームに対応しています。

- Windows XP® オペレーティング システム
- Windows Vista® (64 ビット版も可)
- Windows 7® (64 ビット版も可)

注: WINDOWS PC FIPS を有効にし、かつ、AKC とスマート カードを使用してターゲットにアクセスする場合、Windows 7 を使用する必要があります。

AKC を実行するには .NET が必要になるため、.NET がインストールされていない場合、またはサポートされていないバージョンの .NET がインストールされている場合は、.NET バージョンの確認を指示するメッセージが表示されます。

注: Windows XP® オペレーティング システムのユーザは、AKC を起動する前に、基盤となる .NET 3.5 または 4.0 がインストールされているか確認することをお勧めします。.NET バージョンが機能していることを確認できない場合は、.NET バージョンの確認を求めるデフォルトのメッセージが表示される代わりにファイルをダ ウンロードするよう求められる場合があります。

ブラウザ

- Internet Explorer 6 以降

IE 6 以降ではないブラウザから AKC を開こうとすると、ブラウザの確認と Internet Explorer への切り替えを指示するエラー メッセージが表示されます。

Prerequisites for Using AKC

In order to use AKC:

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの［信頼済みサイト］ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

Enable AKC Download Server Certificate Validation

If the device (or CC-SG) administrator has enabled the Enable AKC Download Server Certificate Validation option:

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書（または自己署名証明書のコピー）をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

When launching AKC from the CC-SG Admin Client, you must have JRE™ 1.6.0_10 or above.

ツール バーのボタンおよびステータス バーのアイコン

ボタン	ボタン名	説明
	[Connection Properties]（接続プロパティ）	帯域幅のオプションを（接続スピード、色深度など）を手動で調節するための［Modify Connection Properties］（接続プロパティの変更）ダイアログ ボックスを開きます。
	[Video Settings]（ビデオ設定）	ビデオ変換パラメータを手動で調節するための［ビデオ設定］ダイアログ ボックスを開きます。
	[Color Calibration]（色調整）	色設定を調節し、余分な色ノイズを低減します。［Video］（ビデオ）の［Color Calibrate］（色調整）を選択した場合と同じです。 *注: KX II-101-V2 では使用できません。*
	[Target Screenshot]（ターゲット スクリーンショット）	クリックすると、ターゲット サーバのスクリーンショットを取得して、それを選択したファイルに保存します。

ボタン	ボタン名	説明
	音声	クライアント PC に接続されている音声デバイスのリストから選択するためのダイアログ ボックスを開きます。 音声デバイスがターゲットに接続されたら、デバイスを選択して切断します。 *注: この機能は、KX II 2.4.0 (以降) で使用できます。* *注: この機能は LX ではサポートされていません。*
	[Synchronize Mouse] (マウスの同期)	デュアルマウス モードで、マウス ポインタとターゲット サーバのマウス ポインタを同期させます。 注: ずれないマウス モードが選択されている場合は、使用できません。
	[Refresh Screen] (画面の更新)	ビデオ画面を強制的に更新します。
	[Auto-sense Video Settings] (ビデオ設定の自動検出)	ビデオ設定を強制的に更新します (解像度、垂直走査周波数)。
	スマート カード	クライアント PC に接続されているスマート カード リーダーのリストから選択するためのダイアログ ボックスを開きます。 *注: この機能は、KSX II 2.3.0 (以降) および KX II 2.1.10 (以降) で提供されます。* *注: この機能は LX ではサポートされていません。*
	[Send Ctrl+Alt+Del] (Ctrl+Alt+Del の送信)	ターゲット サーバに Ctrl+Alt+Del のキー操作を送信します。

ボタン	ボタン名	説明
	[Single Cursor Mode] (シングル カーソル モード)	ローカルのマウス ポインタを画面に表示しない「シングル カーソルモード」になります。 このモードを終了するには、Ctrl+Alt+O キーを押します。 *注: KX II-101-V2 では使用できません。*
	[Full Screen Mode] (全画面モード)	ターゲット サーバのデスクトップを表示する画面を最大化します。
	[Scaling] (拡大、縮小)	ターゲットのビデオ サイズを拡大、縮小して、スクロール バーを使用せずにターゲット サーバ ウィンドウの内容をすべて表示できるようにします。

アイコン	アイコン名	説明
	スピーカー	クライアント ウィンドウの下部のステータス バーにあります。 緑色の波が点滅している場合は、音声再生セッションがストリーム配信されていることを示しています。 セッションがミュートされると、黒色のスピーカー アイコンが表示されます。 音声が接続されていない場合、このアイコンはグレーで表示されます。 *注: 音声は、KX II 2.4.0 (以降) でサポートされています。*
	マイク	クライアント ウィンドウの下部のステータス バーにあります。 赤色の波が点滅している場合は、音声キャプチャセッションが現在進行中であることを示しています。 セッションが進行中の場合は、再生セッションがストリーム配信されていることを示すスピーカー アイコンも表示されます。 セッションがミュートされると、黒色のマイク アイコンが表示されます。 音声が接続されていない場合、マイク アイコンはグレーで表示されます。 *注: 音声は、KX II 2.5.0 (以降) でサポートされています。*

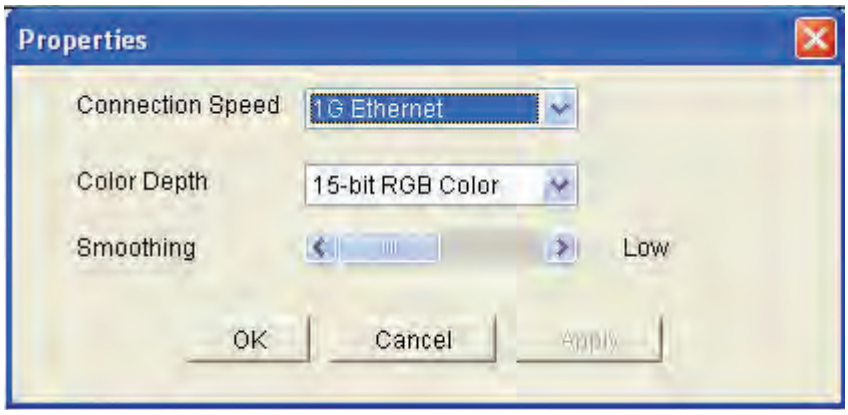
[Connection Properties] (接続プロパティ)

動的ビデオ圧縮アルゴリズムは、さまざまな帯域幅条件で KVM コンソールの使用を可能にします。デバイスの KVM 出力は、LAN 経由だけでなく WAN 経由でも使用できるように最適化されます。さらに、色深度を制御してビデオ出力を制限できるため、さまざまな帯域幅でビデオ画質とシステム応答性のバランスを最適に維持することができます。

[Properties] (プロパティ) ダイアログ ボックスのパラメータは、さまざまな動作環境の要件に合わせて最適に設定できます。 接続プロパティは、一度設定して保存すると、それ以降の第 2 世代デバイスへの接続に使用されます。

▶ 接続プロパティを設定するには、以下の手順に従います。

1. [Connection] (接続) の [Properties] (プロパティ) を選択するか、ツールバーの [Connection Properties] (接続プロパティ) ボタン をクリックします。[Properties] (プロパティ) ダイアログ ボックスが表示されます。



注:KX II-101 は 1G Ethernet をサポートしていません。

2. ドロップダウン リストから接続スピードを選択します。デバイスでは、使用可能な帯域幅を自動的に検出できるため、帯域幅利用は制限されません。ただし、帯域幅の制限に応じて帯域幅利用を調整することもできます。
   - 自動
   - [1G Ethernet] (1G Ethernet)
   - [100 Mb Ethernet] (10 Mbps Ethernet)
   - [10 Mb Ethernet] (10 Mbps Ethernet)
   - [1.5 Mb (MAX DSL/T1)] (1.5 Mbps (最高速 DSL/T1))
   - [1 Mb (Fast DSL/T1)] (1 Mbps (高速 DSL/T1))
   - [512 Kb (Medium DSL/T1)] (512 Kbps (中速 DSL/T1))

- [384 Kb (Slow DSL/T1)] (384 Kbps (低速 DSL/T1))
- [256 Kb (Cable)] (256 Kbps (ケーブル))
- [128 Kb (Dual ISDN)] (128 Kbps (デュアル ISDN))
- [56 kb (ISP Modem)] (56 Kbps (ISP モデム))
- [33 kb (Fast Modem)] (33 Kbps (高速モデム))
- [24 kb (Slow Modem)] (24 Kbps (低速モデム))

これらの設定は、実際の速度ではなく特定の条件に対して最適化されています。クライアントおよびサーバは、現在のネットワーク速度やエンコード設定に関係なく、常に最高速度でネットワークにビデオを配信しようとします。ただし、システムの応答性が最も高くなるのは、設定が実際の環境と一致するときだけです。

3. ドロップダウン リストから色深度を選択します。デバイスでは、リモート ユーザに送信される色深度を動的に調整することで、さまざまな帯域幅で最適な使いやすさを実現します。
   - [15-bit RGB Color] (8 ビット RGB カラー)
   - [8-bit RGB Color] (8 ビット RGB カラー)
   - [4-bit Color] (4 ビット カラー)
   - [4-bit Gray] (2 ビット グレー)
   - [3-bit Gray] (2 ビット グレー)
   - [2-bit Gray] (2 ビット グレー)
   - [Black and White] (モノクロ)

   重要: 多くの管理タスク (サーバの監視、再設定等) において、最新のビデオ グラフィック カードのほとんどで利用できる 24 ビットまたは 32 ビットのフルカラー表示は必要ありません。このような高い色深度を送信すると、ネットワークの帯域幅を浪費することになります。

4. スライダを使用して、スムージングのレベルを指定します (15 ビット カラー モードのみ)。ここで設定したスムージングのレベルにより、色がわずかに異なる画面領域をできるだけ滑らかな単色の組み合わせにするかが決まります。スムージングにより、表示されるビデオノイズを軽減することで、対象ビデオの画質が向上します。
5. [OK] をクリックして、これらのプロパティを保存します。

接続情報

▶ **Virtual KVM Client 接続に関する情報を取得するには、以下の手順に従います。**

- [Connection] (接続) の [Info...] (情報...) を選択します。[Connection Info] (接続情報) ウィンドウが開きます。

現在の接続に関する以下の情報が表示されます。

- [Device Name] (デバイス名) - デバイスの名前です。
- [IP Address] (IP アドレス) - デバイスの IP アドレスです。
- [Port] (ポート) - ターゲット デバイスへのアクセスに使用される KVM 通信 TCP/IP ポートです。
- [Data In/Second] (データ入力/秒) - 入力データ レートです。
- [Data Out/Second] (データ出力/秒) - 出力データ レートです。
- [Connect Time] (接続時間) - 接続時間です。
- [FPS] (FPS) - ビデオで送信される毎秒フレーム数です。
- [Horizontal Resolution] (水平解像度) - 水平方向の画面解像度です。
- [Vertical Resolution] (垂直解像度) - 垂直方向の画面解像度です。
- [Refresh Rate] (垂直走査周波数) - 画面の更新頻度を表します。
- [Protocol Version] (プロトコル バージョン) - RFB プロトコル バージョンです。

▶ **この情報をコピーするには、以下の手順に従います。**

- [Copy to Clipboard] (クリップボードにコピー) をクリックします。これにより、任意のプログラムにこの情報を貼り付けることができます。

キーボードのオプション

[Keyboard Macros] (キーボード マクロ)

キーボード マクロを利用することで、ターゲット サーバに対するキー入力が確実にターゲット サーバに送信され、ターゲット サーバのみで解釈されます。キーボード マクロを利用しない場合、Virtual KVM Client が実行されているコンピュータ（クライアント PC）によって解釈される可能性があります。

マクロはクライアント PC に保存され、その PC 専用になります。したがって、別の PC を使用したときは、作成したマクロを使用できません。さらに、キーボード マクロはコンピュータ単位で管理されるので、あるユーザが使用している PC に別のユーザが自分の名前でログインした場合でも、1 人目のユーザが作成したマクロが 2 人目のユーザに対して表示されます。

Virtual KVM Client 内で作成したキーボード マクロは Multi-Platform Client (MPC) で使用でき、またその逆も可能です。ただし、Active KVM Client (AKC) で作成したキーボード マクロは、VKC または MPC で使用できません。また、その逆でも使用できません。

注:KX II-101 は AKC をサポートしていません。

キーボード マクロのインポート/エクスポート

Active KVM Client (AKC) からエクスポートされるマクロは、Multi-Platform Client (MPC) および Virtual KVM Client (VKC) にはインポートできません。MPC または VKC からエクスポートされるマクロは、AKC にはインポートできません。

注:KX II-101 は AKC をサポートしていません。

▶ **マクロをインポートするには、以下の手順に従います。**

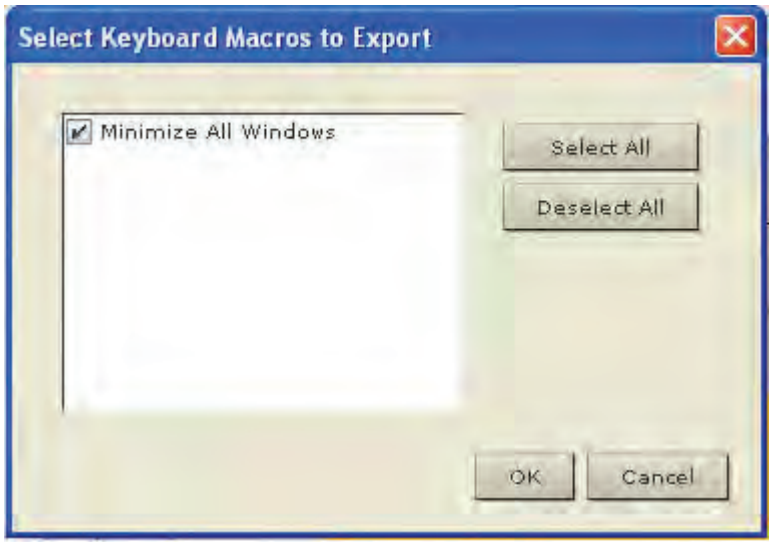
1. [Keyboard] (キーボード) の [Import Keyboard Macros] (キーボード マクロのインポート) をクリックして、[Import Macros] (マクロのインポート) ダイアログ ボックスを開きます。マクロ ファイルがあるフォルダに移動します。
2. マクロ ファイルをクリックし、[Open] (開く) をクリックしてマクロをインポートします。
   a. ファイル内のマクロ数が多い場合は、エラー メッセージが表示され、[OK] を選択するとインポートが中断されます。
   b. インポートが失敗した場合は、エラー ダイアログ ボックスが表示され、失敗した理由についてのメッセージが表示されます。[OK] をクリックすると、インポートできなかったマクロをスキップしてインポートが続行されます。

3. インポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All]（すべて選択）または [Deselect All]（すべて選択解除）オプションを使用して選択します。
4. [OK] をクリックしてインポートを開始します。
   a. 重複するマクロが見つかった場合は、[Import Macros]（マクロのインポート）ダイアログ ボックスが表示されます。以下のいずれかの手順に従います。
      - [Yes]（はい）をクリックして、既存のマクロを、インポートしたマクロで置き換えます。
      - [Yes to All]（すべてはい）をクリックして、現在選択されているマクロとその他に見つかった重複マクロすべてを置き換えます。
      - [No]（いいえ）をクリックすると、元のマクロが維持され、次のマクロに進みます。
      - [No to All]（すべていいえ）をクリックすると、元のマクロが維持され、次のマクロに進みます。その他に見つかったすべての重複マクロも同様にスキップされます。
      - [Cancel]（キャンセル）をクリックすると、インポートが終了します。
      - または、[Rename]（名前変更）をクリックして、マクロの名前を変更してそれをインポートします。[Rename]（名前変更）が選択された場合は、[Rename Macro]（マクロ名の変更）ダイアログ ボックスが表示されます。フィールドに新しいマクロ名を入力し、[OK] をクリックします。ダイアログ ボックスが閉じられ、処理が続行されます。入力した名前が別のマクロと重複している場合は、アラートが表示されるので、別のマクロ名を入力する必要があります。
   b. インポート処理中にインポート済みマクロの許容数を超えた場合は、ダイアログ ボックスが表示されます。[OK] をクリックして、マクロのインポート試行を続行するか、[Cancel]（キャンセル）をクリックしてインポート処理を中止します。

これでマクロがインポートされます。既に存在するホットキーを含むマクロがインポートされた場合、インポートされたマクロのホットキーが破棄されます。

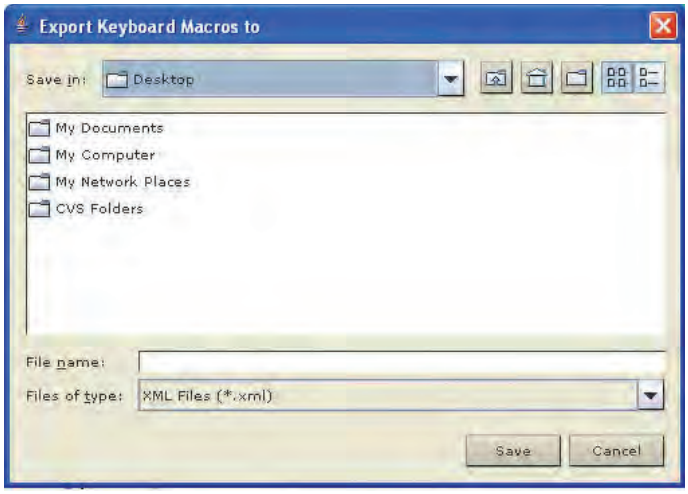
▶ マクロをエクスポートするには、以下の手順に従います。

1. [Tools] (ツール) の [Export Macros] (マクロのエクスポート) を選択して、[Select Keyboard Macros to Export] (エクスポートするキーボード マクロの選択) ダイアログ ボックスをクリックします。



2. エクスポートするマクロを、それに対応するチェックボックスをオンにするか、[Select All] (すべて選択) または [Deselect All] (すべて選択解除) オプションを使用して選択します。
3. [OK] (OK) をクリックします。マクロ ファイルの検索と選択を行うためのダイアログ ボックスが表示されます。デフォルトでは、マクロはデスクトップにあります。

4. マクロ ファイルを保存するフォルダを選択し、ファイル名を入力し、[Save]（保存）をクリックします。マクロが既に存在する場合は、警告メッセージが表示されます。[Yes]（はい）を選択して既存のマクロを上書きするか、[No]（いいえ）をクリックしてマクロを上書きせずに警告を閉じます。



キーボード マクロの作成

▶ マクロを作成するには、以下の手順に従います。

1. [Keyboard]（キーボード）の [Keyboard Macros]（キーボード マクロ）をクリックします。[Keyboard Macros]（キーボード マクロ）ダイアログ ボックスが表示されます。
2. [Add]（追加）をクリックします。[Add Keyboard Macro]（キーボード マクロの追加）ダイアログ ボックスが表示されます。
3. [Keyboard Macro Name]（キーボード マクロ名）フィールドにマクロの名前を入力します。この名前は、マクロが作成された後に [Keyboard]（キーボード）メニューに表示されます。
4. [Hot-Key Combination]（ホットキーの組み合わせ）フィールドで、ドロップダウン リストからキー操作の組み合わせを選択します。これにより、定義済みのキー入力を使ってマクロを実行することができます。**（オプション）**
5. [Keys to Press]（押すキー）ドロップダウン リストで、コマンドの実行に使用されるキー操作のエミュレート用のキーを選択します。キーは、押す順番で選択します。1 つ選択するごとに、[Add Key]（キーを追加）を選択します。キーを選択するごとに、[Macro Sequence]（マクロ シーケンス）フィールドに表示されます。また、1 つ選択するごとに、その [Release Key]（キーのリリース）コマンドが自動的に追加されます。

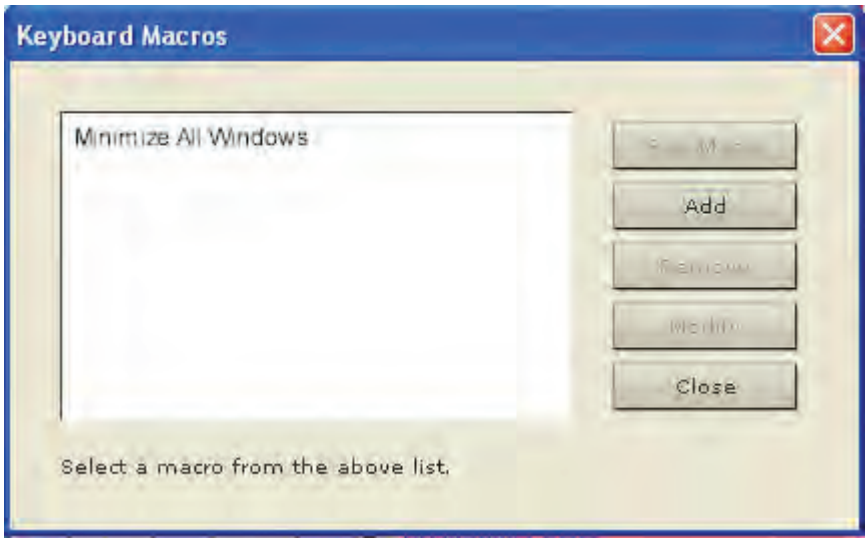
6. マクロでテキストをターゲットに送信する機能を使用するには、[Construct Macro from Text]（テキストからマクロを作成）ボタンをクリックします。
7. たとえば、左 Ctrl + Esc キーを選択してウィンドウを閉じるマクロを作成します。これは、[Macro Sequence]（マクロ シーケンス）ボックスに以下のように表示されます。

   [Press Left Alt]（左 Alt の押下）

   [Press F4]（F4 の押下）

   [Release F4]（F4 のリリース）

   [Release Left Alt]（左 Alt のリリース）
8. [Macro Sequence]（マクロ シーケンス）フィールドで、マクロ シーケンスが正しく定義されていることを確認します。
   a. キー操作の 1 つの手順を削除するには、手順を選択して [Remove]（削除）をクリックします。
   b. キー操作の手順の順番を変更するには、手順をクリックし、上向きまたは下向きの矢印ボタンを使用して必要に応じて並べ替えます。
9. [OK] をクリックしてマクロを保存します。[Clear]（クリア）をクリックすると、すべてのフィールドがクリアされ、最初の状態に戻ります。[OK] をクリックすると [Keyboard Macros]（キーボード マクロ）ダイアログ ボックスが現れ、新しいキーボード マクロがリスト表示されます。
10. [Close]（閉じる）をクリックして、[Keyboard Macro]（キーボード マクロ）ダイアログ ボックスを閉じます。マクロがアプリケーションの [Keyboard]（キーボード）メニューに表示されます。マクロを実行するには、メニューで新しいマクロを選択するか、マクロに割り当てたキー操作を使用します。



キーボード マクロの実行

作成したキーボード マクロは、割り当てたキーボード マクロを使用するか、[Keyboard] (キーボード) メニューからそれを選択して起動します。

メニュー バーからのマクロの実行

マクロを作成すると、そのマクロが [Keyboard] (キーボード) メニューに表示されます。キーボード マクロを実行するには、[Keyboard] (キーボード) メニューでそれをクリックします。

キー操作の組み合わせを使用したマクロの実行

マクロの作成時にキー操作の組み合わせを割り当てた場合は、割り当てたキー入力を押すことでマクロを実行できます。たとえば、Ctrl+Alt+0 キーを同時に押すと、Windows ターゲット サーバの全ウィンドウが最小化されます。

キーボード マクロの変更および削除

▶ マクロを変更するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Modify] (変更) をクリックします。[Add/Edit Keyboard Macro] (キーボード マクロの追加/編集) ダイアログ ボックスが表示されます。
4. 必要な変更を加えます。
5. [OK] (OK) をクリックします。

▶ マクロを削除するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Remove] (削除) をクリックします。マクロが削除されます。

Ctrl+Alt+Del マクロ

Ctrl+Alt+Delete マクロは、頻繁に使用されるため事前にプログラムされています。ツール バーの [Ctrl+Alt+Delete] ボタン をクリックすると、現在接続中のサーバまたは KVM スイッチにこのキー操作が送信されます。

一方、Ctrl キー、Alt キー、Delete キーを同時に押すと、Windows オペレーティング システムの構造により、コマンドはターゲット サーバへ送信されずに操作中の PC に適用されます。

CIM キーボード/マウス オプションの設定

DCIM-USBG2 の設定メニューにアクセスするには、以下の手順に従います。

1. Windows® のメモ帳などのウィンドウにマウス ポインタを置きます。
2. [Set CIM Keyboard/Mouse options] (CIM キーボード/マウス オプションを設定する) を選択します。この操作は、左 Ctrl + Num Lock キーをターゲットに送信することと同じです。CIM セットアップ メニュー オプションが表示されます。
3. 言語とマウスを設定します。
4. メニューを終了し、通常の CIM 機能に戻ります。

ビデオのプロパティ

画面を更新する

[Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。ビデオの設定を自動的に更新する方法はいくつかあります。

- [Refresh Screen] (画面の更新) コマンドを使用すると、ビデオ画面が更新されます。
- [Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ターゲット サーバのビデオ設定が自動的に検出されます。
- [Calibrate Color] (色調整) コマンドを使用すると、ビデオの表示色が調整されます。

これに加え、[Video Settings] (ビデオ設定) コマンドを使用すると、手動で設定を調整できます。

ビデオ設定を更新するには、次のいずれかの手順に従います。

- [Video] (ビデオ) の [Refresh Screen] (画面の更新) を選択するか、ツールバーの [Refresh Screen] (画面の更新) ボタン をクリックします。

[Auto-sense Video Settings] (ビデオ設定の自動感知)

[Auto-sense Video Settings] (ビデオ設定の自動検出) コマンドを使用すると、ビデオ設定 (解像度、垂直走査周波数) が再検出され、ビデオ画面が再描画されます。

▶ ビデオ設定を自動的に検出するには、以下の手順に従います。

- [Video] (ビデオ) の [Auto-sense Video Settings] (ビデオ設定の自動検出) を選択するか、ツールバーの [Auto-sense Video Settings] (ビデオ設定の自動検出) ボタン をクリックします。調整が行われていることを示すメッセージが表示されます。

色の調整

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、輝度、彩度) を最適化するために使用します。色設定は、ターゲット サーバごとに適用されます。

注: [Calibrate Color] (色調整) コマンドは、現在の接続のみに適用されます。

注: KX II-101 では、色の調整はサポートされません。

▶ 色を調整するには、以下の手順に従います。

- [Video] (ビデオ) の [Calibrate Color] (色調整) を選択するか、ツールバーの [Calibrate Color] (色調整) ボタン をクリックします。ターゲット デバイス画面の色が調整されます。

ビデオ設定を調整する

[Video Settings] (ビデオ設定) コマンドを使用すると、ビデオ設定を手動で調整できます。

▶ ビデオ設定を変更するには、以下の手順に従います。

1. [Video] (ビデオ) の [Video Settings] (ビデオ設定) を選択するか、ツールバーの [Video Settings] (ビデオ設定) ボタン をクリックして、[Video Settings] (ビデオ設定) ダイアログ ボックスを開きます。
2. 必要に応じて、以下の設定を調整します。設定を調整すると、その効果が即座に表示に反映されます。
   a. [Noise Filter] (ノイズ フィルタ)

デバイスでは、グラフィック カードからのビデオ出力の電気的干渉を除去することができます。この機能により、画質が最適化され、消費される帯域幅が低減されます。設定値を大きくすると、ピクセル変動は隣接するピクセルと比較して大きな色変化がある場合にのみ送信されます。ただし、しきい値を高く設定しすぎると、正常な画面変更が意図せずフィルタリングされてしまう場合があります。
設定値を低くすると、ほとんどのピクセルの変更が送信されます。しきい値を低く設定しすぎると、帯域幅の使用量が高くなることがあります。

b. [PLL Settings] (PLL 設定)

[Clock] (クロック) – ビデオ画面上にビデオ ピクセルが表示される速度を制御します。クロック設定値を変更すると、ビデオ画像が水平方向に伸縮します。設定値は奇数を推奨します。通常は自動検出機能によって適切に設定されるため、ほとんどの環境ではこの設定を変更する必要はありません。

[Phase] (位相) – 位相の値の範囲は 0 ～ 31 です。これより大きな値は反復されます。アクティブなターゲット サーバ用に最適なビデオ画像が得られる位相の位置で停止してください。

c. [Brightness] (明るさ): この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。

d. [Brightness Red] (赤輝度) – ターゲット サーバの画面に表示される赤の信号の輝度を制御します。

e. [Brightness Green] (緑輝度) – 緑の信号の輝度を制御します。

f. [Brightness Blue] (青輝度) – 青の信号の輝度を制御します。

g. [Contrast Red] (赤コントラスト) – 赤の信号のコントラストを制御します。

h. [Contrast Green] (緑コントラスト) – 緑の信号のコントラストを制御します。

i. [Contrast Blue] (青コントラスト) – 青の信号のコントラストを制御します。

ビデオ画像が大幅にぼやけている場合、設定でクロックと位相を調節することで、アクティブなターゲット サーバの画像を改善します。

警告: クロック設定と位相設定を変更する際には、注意が必要です。ビデオ画像が消えたり歪んだりする可能性があるだけでなく、元の状態に戻せなくなることがあります。変更を加える前に、ラリタン テクニカル サポートにお問い合わせください。

---

j. [Horizontal Offset] (水平オフセット) – ターゲット サーバの画面がモニタに表示されるときの水平位置を制御します。

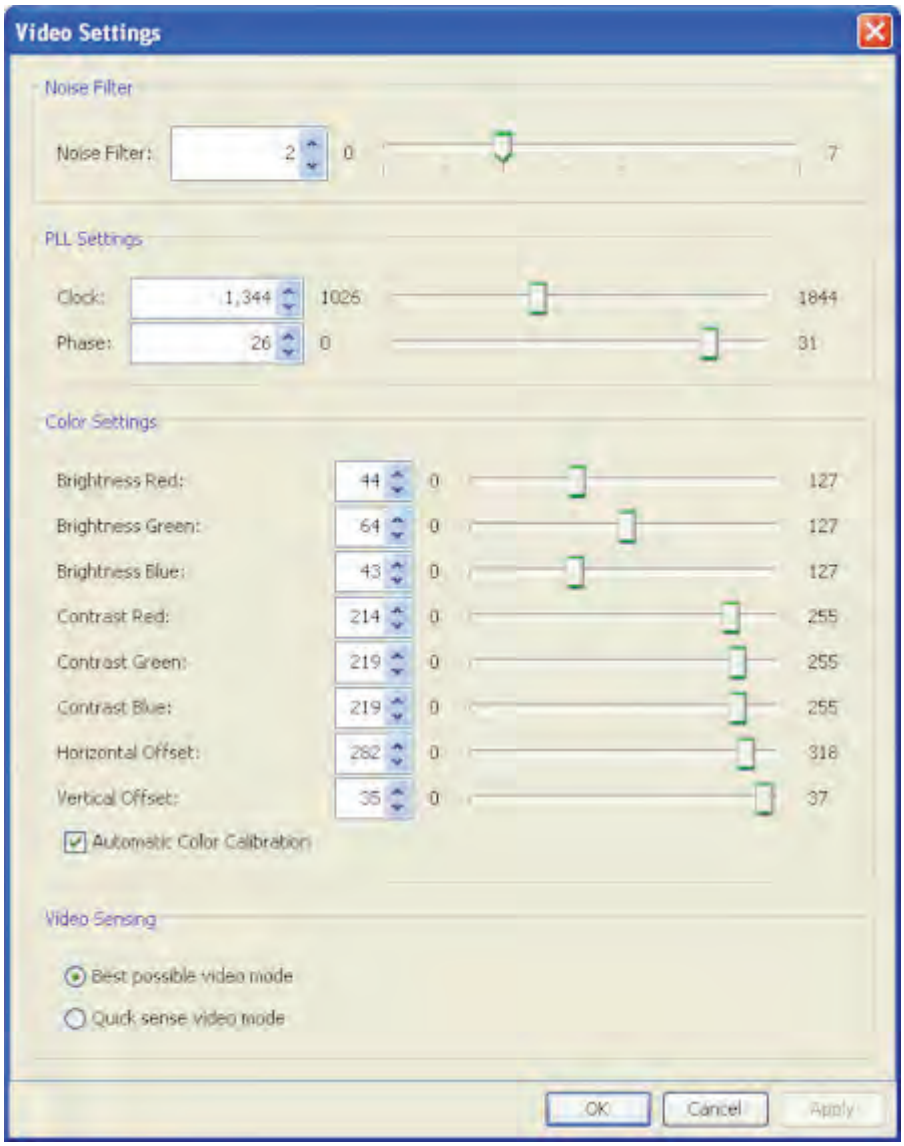
k. [Vertical Offset] (垂直オフセット) – ターゲット サーバの画面がモニタに表示されるときの垂直位置を制御します。

3. [Automatic Color Calibration]（自動色調節）を選択して、この機能を有効にします。
4. ビデオ検出モードを選択します。
   - [Best possible video mode]（最適ビデオ モード）

     ターゲットやターゲットの解像度が変更されたときに、すべての自動検出処理が実行されます。このオプションを選択すると、最適な画像品質になるようにビデオが調整されます。
   - [Quick sense video mode]（クイック検出ビデオ モード）

     このオプションを使用すると、クイック ビデオ自動検出が使用され、ターゲットのビデオがより早く表示されます。このオプションは、再起動直後のターゲット サーバの BIOS 設定を入力するときに特に有効です。
5. 設定を適用してダイアログ ボックスを閉じるには、[OK] をクリックします。ダイアログ ボックスを閉じずに設定を適用するには、[Apply]（適用）をクリックします。

注: 一部の Sun サーバでは、ある種の Sun 背景画面（外周部が非常に暗いものなど）が中央の位置に正確に表示されない場合があります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

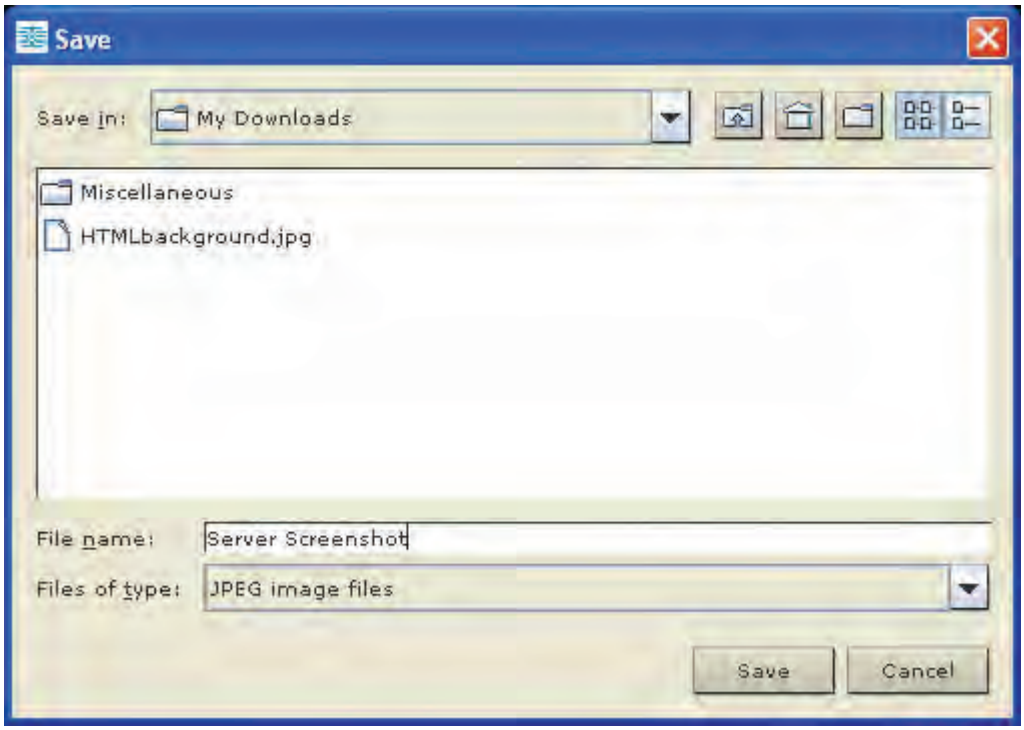


[Screenshot from Target] (ターゲットからのスクリーンショット) を使用する

[Screenshot from Target] (ターゲットからのスクリーンショット) サーバコマンドを使用してターゲット サーバのスクリーンショットを撮ることができます。必要に応じて、選択した場所にこのスクリーンショットをビットマップ、JPEG、または PNG ファイルとして保存します。

▶ ターゲット サーバのスクリーンショットを撮るには、次の手順に従います。

1. [Video] (ビデオ) の [Screenshot from Target] (ターゲットからのスクリーンショット) を選択するか、ツールバーの [Screenshot from Target] (ターゲットからのスクリーンショット) ボタン をクリックします。
2. [Save] (保存) ダイアログ ボックスで、ファイルの保存場所を選択し、ファイルに名前を付けて、[Files of type] (ファイルの種類) ドロップダウンからファイル形式を選択します。
3. [Save] (保存) をクリックしてスクリーンショットを保存します。



最大垂直走査周波数の変更

ターゲットで使用しているビデオ カードでカスタム ソフトウェアが使用されている場合、MPC または VKC を介してターゲットにアクセスするには、垂直走査周波数がターゲットで有効になるように、モニタの最大垂直走査周波数を変更する必要があります。

▶ **モニタの垂直走査周波数を調整するには、以下の手順に従います。**

1. Windows® では、[画面のプロパティ] ダイアログ ボックスを開き、[設定]、[詳細設定] の順に選択してプラグ アンド プレイのダイアログ ボックスを開きます。
2. [モニタ] タブをクリックします。
3. [画面のリフレッシュ レート] を設定します。
4. [OK] をクリックし、もう一度 [OK] をクリックして設定を適用します。

マウス オプション

ターゲット サーバを制御しているとき、リモート コンソールには、2 つのマウス カーソルが表示されます。1 つはクライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。

この場合、シングル マウス モードとデュアル マウス モードのどちらかを使用できます。デュアル マウス モードで、オプションが正しく設定されている場合は、2 つのマウス カーソルが同調します。

デバイスでは、2 つのマウス カーソルが存在するときに以下のマウス モードが提供されます。

- 絶対 (マウス同期)
- インテリジェント (マウス モード)
- 標準 (マウス モード)

マウス ポインタの同期

マウスが使用されているターゲット サーバをリモートで表示する場合、2 つのマウス カーソルが表示されます。1 つはリモート クライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。マウス ポインタが Virtual KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。

高速 LAN 接続の場合、Virtual KVM Client のマウス ポインタを無効にしてターゲット サーバのマウス ポインタのみを表示できます。この 2 つのモード（シングル マウスとデュアル マウス）は自由に切り替えることができます。

マウス同期のヒント

マウスの同期を設定するには、以下の手順に従います。

1. 選択したビデオ解像度と垂直走査周波数がデバイスでサポートされていることを確認します。[Virtual KVM Client Connection Info]（Virtual KVM Client 接続情報）ダイアログ ボックスには、デバイスの表示で使用している実際の値が表示されます。
2. KX II および LX デバイスについては、ケーブルの長さが選択したビデオ解像度に指定されている限度内であることを確認します。
3. インストール プロセス中にマウスとビデオが正しく構成されていることを確認します。
4. [Virtual KVM Client auto-sense]（Virtual KVM Client の自動検出）ボタンをクリックして自動検出を強制します。
5. 以上の手順で Linux、UNIX、Solaris KVM ターゲット サーバのマウス同期が改善しない場合は、以下の手順に従います。
   a. ターミナル ウィンドウを開きます。
   b. 次のコマンドを入力します。`xset mouse 1 1`
   c. ターミナル ウィンドウを閉じます。
6. [Virtual KVM Client mouse synchronization]（Virtual KVM Client マウス同期）ボタン をクリックします。

インテリジェント マウス モードでの追加の注意事項

- 同期ルーチンが利用する領域を空けるため、画面の左上隅にアイコンやアプリケーションがないことを確認します。
- アニメーション カーソルを使用しないでください。
- KVM ターゲット サーバでアクティブなデスクトップを無効にします。

マウスの同期

デュアル マウス モードで [Synchronize Mouse] (マウスの同期) コマンドを使用すると、ターゲット サーバのマウス ポインタと Virtual KVM Client のマウス ポインタとの同期化が再実行されます。

▶ **マウスを同期するには、次のいずれかの手順に従います。**

- [Mouse] (マウス) の [Synchronize Mouse] (マウスの同期) を選択するか、ツールバーの [Synchronize Mouse] (マウスの同期) ボタン をクリックします。

注: このオプションは、標準マウス モードとインテリジェント マウス モードでのみ使用可能です。

標準マウス モード

標準マウス モードは、相対マウス位置を使用した標準のマウス同期アルゴリズムです。標準マウス モードを使用する場合、クライアントとサーバのカーソルが同期するように、マウスの加速を無効にし、マウスに関連するその他のパラメータを適切に設定する必要があります。

▶ **標準マウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Standard] (標準) を選択します。

インテリジェント マウス モード

デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス設定を検出し、それに応じてマウス カーソルを同期できるので、ターゲットでマウスの加速を設定できます。インテリジェント マウス モードは、VM ターゲット以外のデフォルトです。

同期中は、マウス カーソルが画面の左上隅で ″ダンス″ をし、加速が計算されます。このモードが正常に動作するには、特定の条件が満たされる必要があります。

▶ インテリジェント マウス モードに切り替えるには、以下の手順に従います。

- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

[Mouse] (マウス) メニューにある [Intelligent Mouse Synchronization] (インテリジェント マウス同期) コマンドを選択すると、マウスが動いていないときにマウス カーソルが自動的に同期されます。この機能を適切に動作させるには、次の条件が満たされている必要があります。

- ターゲットにおいて、アクティブ デスクトップが無効であること。
- ターゲット ページの左上隅にウィンドウが表示されていないこと。
- ターゲット ページの左上隅にアニメーション背景が表示されていないこと。
- ターゲットのマウス カーソルが通常のものであり、アニメーション カーソルでないこと。
- ターゲット マウスの速度が、非常に遅い値や非常に速い値に設定されていないこと。
- [ポインタの精度を高める] や [ポインタを自動的に既定のボタン上に移動する] などの高度なマウス プロパティが無効であること。
- [ビデオ設定] ウィンドウで [最適ビデオ モード] を選択していること。
- ターゲットのビデオの外周部が明確に表示されていること (つまり、ターゲットのビデオ画像の端にスクロールしたときに、ターゲット デスクトップとリモート KVM コンソール ウィンドウの間に黒いボーダーが表示されている必要があります)。
- インテリジェント マウス同期機能を使用中に、デスクトップの左上隅にファイル アイコンやフォルダ アイコンがあると、この機能が正しく動作しない可能性があります。この機能での問題を避けるために、デスクトップの左上隅にファイル アイコンやフォルダ アイコンを置かないことを推奨します。

ターゲット ビデオが自動検出された後で、ツール バーの [Synchronize Mouse] (マウス同期) ボタンをクリックして、手動でマウス同期を開始する必要があります。ターゲットの解像度が変更された場合や、マウス カーソルが互いに同期しなくなった場合にも、この操作を行います。

インテリジェント マウス同期が失敗した場合、標準マウス同期と同じ動作になります。

マウス設定は、ターゲットのオペレーション システムよって異なります。詳細については、使用する OS のマニュアルを参照してください。また、インテリジェント マウス同期は UNIX ターゲットでは機能しません。

ずれないマウス モード

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのカーソルを同期するために絶対座標が使用されます。このモードは USB ポートを備えたサーバでサポートされ、VM およびデュアル VM ターゲットではデフォルトのモードです。

▶ ずれないマウス モードに切り替えるには、以下の手順に従います。

- [Mouse] (マウス) の [Absolute] (ずれない) を選択します。

注: KX II の場合、ずれないマウス機能は、仮想メディアに対応する USB CIM (D2CIM-VUSB と D2CIM-DVUSB) およびデジタル CIM でのみ使用できます。

シングル マウス モード

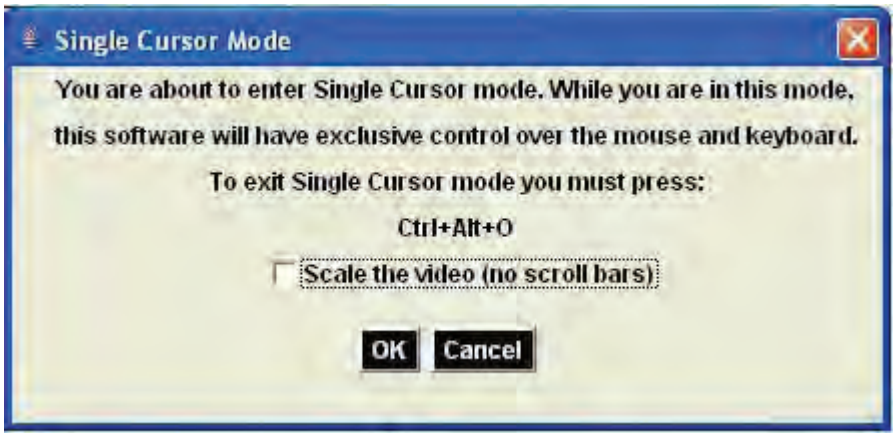
シングル マウス モードでは、ターゲット サーバのマウス カーソルだけを使用します。ローカル マウス ポインタは画面に表示されません。シングル マウス モードでは、[Synchronize Mouse] (マウスの同期) コマンドは使用できません (単独のマウス カーソルを同期化する必要がないため)。

注: クライアントが仮想マシン上で実行している場合、シングル マウス モードは Windows および Linux のターゲットでは機能しません。

▶ シングル マウス モードに入るには、以下の手順に従います。

1. [Mouse] (マウス) の [Single Mouse Cursor] (シングル マウス カーソル) を選択します。

2. ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カーソル) ボタン をクリックします。



▶ シングル マウス モードを終了するには、以下の手順に従います。

- シングル マウス モードを終了するには、キーボードの Ctrl+Alt+O を押します。

ツール オプション

[全般]

▶ ツール オプションを設定するには、以下の手順に従います。

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. テクニカル サポートから指示されたときだけ、[ログ記録を有効にする] チェックボックスをオンにします。このオプションをオンにすると、ホーム ディレクトリにログ ファイルが作成されます。
3. 必要に応じて、ドロップダウン リストからキーボードの種類を選択します。含まれるオプションは次のとおりです。
   - [アメリカ英語/インターナショナル]
   - [フランス語 (フランス)]
   - [ドイツ語 (ドイツ)]
   - [日本語]
   - [イギリス英語]
   - [韓国語 (韓国)]
   - [フランス語 (ベルギー)]
   - [ノルウェー語 (ノルウェー)]
   - [ポルトガル語 (ポルトガル)]

- [デンマーク語 (デンマーク)]
- [スウェーデン語 (スウェーデン)]
- [ドイツ語 (スイス)]
- [ハンガリー語 (ハンガリー)]
- [スペイン語 (スペイン)]
- [イタリア語 (イタリア)]
- [スロベニア語]
- [変換: フランス語 – アメリカ英語]
- [変換: フランス語 – アメリカ英語/インターナショナル]

AKC では、デフォルトのキーボードの種類はローカル クライアントであるため、このオプションは適用されません。また、KX II-101 および KX II-101-V2 は、シングル カーソル モードをサポートしていないので、これらのデバイスには [シングル カーソル モードの終了] 機能は適用されません。

4. ホットキーを設定します。
   - [全画面モードの終了 – ホットキー]: 全画面モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。これは、このモードを終了するためのホットキーです。
   - [シングル カーソル モードの終了- ホットキー]: シングル カーソル モードに入ると、ターゲット サーバのマウス カーソルのみが表示されます。これは、シングル カーソル モードを終了して、クライアント マウス カーソルに戻るために使用するホットキーです。
   - [ターゲットから切断 – ホットキー]: このホットキーを有効にすると、ターゲットからすばやく切断できます。

   アプリケーションでは、同じホットキーの組み合わせを複数の機能に割り当てることはできません。たとえば、Q が既に [ターゲットから切断] 機能に割り当てられている場合、それを [全画面モードの終了] 機能に割り当てることはできません。さらに、ホットキーがアップグレードによってアプリケーションに追加されたときにそのキーのデータ値が既に使用されていた場合は、次に利用できる値が、代わりにその機能に適用されます。
5. [OK] をクリックします。

キーボードの制限

トルコ語キーボード

トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

スロベニア語キーボード

JRE の制限により、< キーは、スロベニア語キーボードでは機能しません。

Linux での言語設定

Linux 上の Sun JRE では、システムの環境設定を使用して設定される外国語のキーボードで正しいキー イベントを生成する際に問題があるので、外国語キーボードは、次の表で説明する方法を使用して設定することをお勧めします。

言語	設定方法
アメリカ英語/国際	デフォルト設定
フランス語	Keyboard Indicator
ドイツ語	[System Settings] (システム設定) (Control Center)
日本語	[System Settings] (システム設定) (Control Center)
イギリス英語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control Center)
ベルギー語	Keyboard Indicator
ノルウェー語	Keyboard Indicator
デンマーク語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

クライアント起動設定

KX II ユーザは、クライアント起動設定をカスタマイズし、KVM セッションにおける画面設定を定義できます。

▶ クライアント起動設定をカスタマイズするには、以下の手順に従います。

1. ［ツール］メニューの［オプション］を選択します。［オプション］ウィンドウが表示されます。
2. ［クライアント起動設定］タブをクリックします。
   - ターゲット ウィンドウ設定をカスタマイズするには、以下の手順に従います。
     a. ターゲットの現在の解像度に合ったサイズのウィンドウを開くには、［標準 － ターゲットの解像度に合わせる］を選択します。ターゲットの解像度がクライアントの解像度よりも高い場合、画面全体にターゲット ウィンドウが表示され、表示しきれない部分がある場合は、スクロール バーが追加表示されます。
     b. ターゲット ウィンドウを全画面モードで開くには、［全画面］を選択します。
   - ターゲット ビューアが起動するモニタをカスタマイズするには
     a. クライアント上で使用されているアプリケーション（例: Web ブラウザ、アプレット）を表示しているモニタと同じモニタを使用してターゲット ビューアを起動するには、［クライアントが起動されているモニタ］を選択します。
     b. アプリケーションによって現在検出されているモニタの一覧から選択するには、［検出されたモニタの中から選択］を選択します。以前選択したモニタが検出されなくなった場合、″現在選択されているモニタは検出されませんでした″ というメッセージが表示されます。
   - 追加の起動設定をカスタマイズするには、以下の手順に従います。
     a. サーバにアクセスされたときにデフォルト マウス モードとしてシングル マウス モードを有効にするには、［シングル カーソル モードを有効にする］を選択します。
     b. ターゲット サーバにアクセスされたときに、ディスプレイのサイズを自動的に拡大、縮小するには、［ビデオの拡大、縮小を有効にする］選択します。
     c. 全画面モードの場合でもターゲットのツールバーを表示したままにする場合は、［メニュー ツールバーを常に表示］を選択します。デフォルトでは、ターゲットが全画面モードの場合、メニューは、マウスを画面上部に移動した場合にのみ表示されます。
3. ［OK］をクリックします。

VKC および AKC でのスキャンの設定

KX II では、選択されたターゲットを検索してそれをスライド ショー ビューで表示するポート スキャン機能を使用すると、最大 32 のターゲットを一度にモニタできます。ターゲットに接続することも、必要に応じて特定のターゲットをフォーカスすることもできます。スキャン対象は、標準ターゲット、ブレード サーバ、カスケード接続 Dominion デバイス、KVM スイッチの各ポートです。Virtual KVM Client (VKC) または Active KVM Client (AKC) からスキャン設定を指定します。詳細については、「*VKC および AKC でのスキャンの設定* 『*98*p. 』」を参照してください。「*ポートのスキャン* 『*59*p. 』」を参照してください。[スキャン設定] タブを使用して、スキャン間隔およびデフォルト表示オプションをカスタマイズします。

▶ スキャン設定をカスタマイズするには、以下の手順に従います。

1. [ツール] メニューの [オプション] を選択します。[オプション] ウィンドウが表示されます。
2. [スキャン設定] タブを選択します。
3. [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
4. [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
5. [表示] セクションで、[ポート スキャン] ウィンドウのサムネイルのサイズと分割方向のデフォルト表示オプションを変更します。
6. [OK] をクリックします。

表示オプション

[View Toolbar] (ツール バーの表示)

Virtual KVM Client では、ツール バーの表示/非表示を切り替えることができます。

▶ ツール バーの表示/非表示 (オン/オフ) を切り替えるには、以下の手順に従います。

- [View] (表示) の [View Toolbar] (ツール バーの表示) を選択します。

[View Status Bar] (ステータス バーの表示)

デフォルトでは、ステータス バーはターゲット ウィンドウの下部に表示されます。

▶ ステータス バーを非表示にするには、以下の手順に従います。

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択解除します。

▶ ステータス バーを復元するには、以下の手順に従います。

- [View] (表示) の [Status Bar] (ステータス バー) をクリックして選択します。

[Scaling] (拡大、縮小)

ターゲットのウィンドウを拡大、縮小することで、ターゲット サーバ ウィンドウ全体の内容を表示することができます。Virtual KVM Client のウィンドウ サイズに合わせて、縦横比を維持したまま、ターゲット ビデオのサイズを拡大または縮小することができるため、スクロール バーを使用することなくターゲット サーバのデスクトップ全体を表示することができます。

▶ 拡大、縮小 (オン/オフ) を切り替えるには、以下の手順に従います。

- [View] (表示) の [Scaling] (拡大、縮小) を選択します。

[Full Screen Mode] (全画面モード)

全画面モードに切り替えると、ターゲットの全画面が表示され、ターゲット サーバと同じ解像度になります。このモードを終了するためのホットキーは、[Options] (オプション) ダイアログ ボックスで指定します。「*ツール オプション* 『*94*p. 』」を参照してください。

全画面モードになっているときに、マウス ポインタを画面上端に移動すると、全画面モード メニュー バーが表示されます。全画面モードの場合でもメニュー バーを表示したままにする場合は、[Tool] (ツール) の [Options] (オプション) ダイアログ ボックスの [Pin Menu Toolbar] (メニュー ツールバーを常に表示] を有効にします。「*ツール オプション* 『*94*p. 』」を参照してください。

▶ 全画面モードに切り替えるには、以下の手順に従います。

- [View] (表示) の [Full Screen] (全画面) を選択します。

▶ 全画面モードを終了するには、以下の手順に従います。

- [Tool] (ツール) の [Options] (オプション) ダイアログで設定されているホットキーを押します。デフォルトは Ctrl+Alt+M です。

常に全画面モードの状態でターゲットにアクセスしたい場合、全画面モードをデフォルトにすることができます。

▶ 全画面モードをデフォルトに設定するには

1. [Tools] (ツール) メニューの [Options] (オプション) をクリックし、[Options] (オプション) ダイアログ ボックスを開きます。
2. [Enable Launch in Full Screen Mode] (全画面モードで起動する) を選択し、[OK] (OK) をクリックします。

デジタル音声

KX II では、リモート クライアントのデジタル音声再生デバイスおよびキャプチャ デバイスとターゲット サーバ間のエンドツーエンドの双方向デジタル音声接続をサポートしています。音声デバイスには、USB 接続を介してアクセスされます。D2CIM-DVUSB および現在のデバイスのファームウェアが必要です。

デジタル音声機能は、以下に対応しています。

- *音声設定の保存* 『*102*p. 』
- *単一のリモート クライアントから複数のターゲットへの接続* 『*102*p. 』
- *複数のリモート クライアントから単一のターゲット サーバへの接続* 『*104*p. 』
- *デジタル音声デバイスの接続および切断* 『*105*p. 』
- *キャプチャ/再生バッファ サイズの調整（音声設定）*『*107*p. 』

Windows®、Linux®、Mac® の各オペレーティング システムがサポートされています。Virtual KVM Client (VKC)、Active KVM Client (AKC)、Multi-Platform Client (MPC) は、音声デバイスへの接続をサポートしています。

注: 音声 CD は、仮想メディアでサポートされていないので、音声機能では使用できません。

音声機能の使用を始める前に、以下のヘルプ セクションに記載されている音声関連情報を確認することを推奨します。

- *サポートされている音声デバイス形式* 『*359*p. 』
- *デュアル ポート ビデオに関する推奨事項* 『*376*p. 』
- *サポートされているマウス モード* 『*376*p. 』
- *デュアル ビデオ サポートに必要な CIM* 『*377*p. 』
- *留意事項* 『*392*p. 』、*音声* 『*403*p. 』

音声設定の保存

音声デバイス設定は、KX II デバイス単位で適用されます。KX II の音声デバイス設定が指定され、保存されたら、同じ設定がそのデバイスに適用されます。

たとえば、ステレオ、16 ビット、44.1K の形式を使用するように Windows® 音声デバイスを設定できます。さまざまなターゲットに接続してその Windows 音声デバイスを使用すると、各ターゲット サーバにはステレオ、16 ビット、44.1K の形式が適用されます。

再生デバイスおよび録音デバイスの両方について、デバイスに適用されるデバイス タイプ、デバイス形式、およびバッファ設定が保存されます。

音声デバイスの接続方法および設定方法については、「*デジタル音声デバイスの接続および切断 『105*p. 』」を参照し、音声デバイスのバッファ設定については、「*キャプチャ/再生バッファ サイズの調整（音声設定）『107*p. 』」を参照してください。

複数のユーザがターゲット上の同じ音声デバイスに同時にアクセスできるように、PC 共有モードおよび VM 共有モードでの動作中に音声機能を使用している場合は、セッションを開始するユーザの音声デバイス設定が、セッションに参加するすべてのユーザに適用されます。

したがって、ユーザが音声セッションに参加する場合は、ターゲット マシンの設定が使用されます。「*複数のリモート クライアントから単一のターゲット サーバへの接続 『104*p. 』」を参照してください。

単一のリモート クライアントから複数のターゲットへの接続

KX II 2.5.0 (以降) では、単一のリモート クライアントから最大 4 つのターゲット サーバの音声を同時に聞くことができます。音声デバイスの接続方法については、「*デジタル音声デバイスの接続および切断『105*p. 』」を参照してください。

注: 音声セッションが進行中の場合は、必ずセッションをアクティブなままにするか、KX II のアイドル状態のタイムアウト時間を変更して音声セッションがタイムアウトにならないようにしてください。

次の表で、オペレーティング システムごとに音声再生/キャプチャが機能する Raritan クライアントを確認できます。

オペレーティング システム	音声再生およびキャプチャをサポートしているクライアント
Windows®	• Active KVM Client (AKC) • Virtual KVM Client (VKC) • Multi-Platform Client (MPC)

オペレーティング システム	音声再生およびキャプチャをサポートしているクライアント
Linux®	• Virtual KVM Client (VKC) • Multi-Platform Client (MPC)
Mac®	• Virtual KVM Client (VKC) • Multi-Platform Client (MPC)

スピーカー アイコン がクライアント ウィンドウの下部のステータス バーに表示されます。音声が使用されていない場合、このアイコンはグレーで表示されます。スピーカー アイコンとマイク アイコン がステータス バーに表示されている場合は、セッションがキャプチャされ、ストリーム配信されます。

複数のリモート クライアントから単一のターゲット サーバへの接続

KX II 2.5.0 (以降) では、異なるリモート クライアントの最大 8 ユーザが、同じターゲット サーバに同時に接続して音声再生を聞くことができます。

この機能を使用するには、ターゲットの PC 共有モードおよび VM 共有モードを有効にする必要があります。PC 共有モードおよび VM 共有モードを有効にする方法については、「*暗号化および共有 『269*p. の *"[Encryption & Share] (暗号化および共有)"*参照 』」を参照してください。

---

*注: PC 共有モードおよび VM 共有モードでの動作中に音声機能を使用している場合、重要な情報については、「*音声の再生とキャプチャに関する推奨事項と要件 *『*359*p. 』」を参照してください。*

ユーザが同じターゲット上で音声セッションに参加する場合は、セッションを開始したユーザの音声デバイス設定が使用されます。たとえば、音声デバイスを最初に設定したユーザが、音声デバイスにステレオ、16 ビット、44.1K の形式を適用している場合、他のユーザが共有セッションでターゲット サーバの音声デバイスにアクセスするたびに、その形式が使用されます。

この設定は、音声デバイスが最初に追加されたときにターゲットに対して設定され、ユーザが変更することはできません。ただし、ユーザは、特定のネットワーク設定に対応するためにキャプチャ/再生バッファ サイズの設定を調整することができます。たとえば、バッファ サイズを拡大すると、音声品質が改善されます。「*キャプチャ/再生バッファ サイズの調整 (音声設定) 『107*p. 』」を参照してください。

セッションに参加している各ユーザは、音声デバイスに接続する場合と同じように VKC、AKC、または MPC を介してターゲットに接続します。「*デジタル音声デバイスの接続および切断 『105*p. 』」を参照してください。

スピーカー アイコン がクライアント ウィンドウの下部のステータス バーに表示されます。音声が使用されていない場合、このアイコンはグレーで表示されます。スピーカー アイコンとマイク アイコン がステータス バーに表示されている場合は、セッションがキャプチャされ、ストリーム配信されます。

注: 音声セッションが進行中の場合は、必ずセッションをアクティブなままにするか、KX II のアイドル状態のタイムアウト時間を変更して音声セッションがタイムアウトにならないようにしてください。

デジタル音声デバイスの接続および切断

音声デバイス設定は、KX II デバイス単位で適用されます。KX II の音声デバイス設定が指定され、保存されたら、同じ設定がそのデバイスに適用されます。詳細については、「*音声設定の保存 『102p. 』*」を参照してください。

---

*注: PC 共有モードおよび VM 共有モードでの動作中に音声機能を使用している場合、重要な情報については、「*音声の再生とキャプチャに関する推奨事項と要件 *『359p. 』」を参照してください。「*複数のリモート クライアントから単一のターゲット サーバへの接続 *『104p. 』」も参照してください。*

*注: 単一のリモート クライアントから複数のターゲット サーバの音声デバイスに同時に接続する場合は、音声再生/キャプチャが機能する Raritan クライアントをオペレーティング システム タイプごとに確認してください。「*単一のリモート クライアントから複数のターゲットへの接続 *『102p. 』」を参照してください。*

注: 音声セッションが進行中の場合は、必ずセッションをアクティブなままにするか、KX II のアイドル状態のタイムアウト時間を変更して音声セッションがタイムアウトにならないようにしてください。

▶ 音声デバイスに接続するには、以下の手順に従います。

1. 音声デバイスをリモート クライアント PC に接続してから、 KX II とのブラウザ接続を起動します。
2. [Port Access] (ポート アクセス) ページでターゲットに接続します。
3. 接続できたら、ツールバーの [Audio] (音声) アイコン をクリックします。[Connect Audio Device] (音声デバイスに接続) ダイアログボックスが表示されます。リモート クライアント PC に接続されている利用可能な音声デバイスの一覧が表示されます。

   注: リモート クライアント PC に接続されている利用可能な音声デバイスがない場合、[Audio] (音声) アイコンはグレーで表示されます。

4. 再生デバイスを接続する場合は、[Connect Playback Device] (再生デバイスを接続) をオンにします。
5. 接続するデバイスをドロップダウン リストから選択します。
6. 再生デバイスの音声形式を [Format:] (形式:) ドロップダウン リストから選択します。

   注: 使用する形式は、利用可能なネットワーク帯域幅に基づいて選択します。サンプリング レートが低い形式であるほど、消費する帯域幅は少なくなり、ネットワークの輻輳を許容できます。

7. 録音デバイスを接続する場合は、[Connect Recording Device] (録音デバイスを接続) をオンにします。

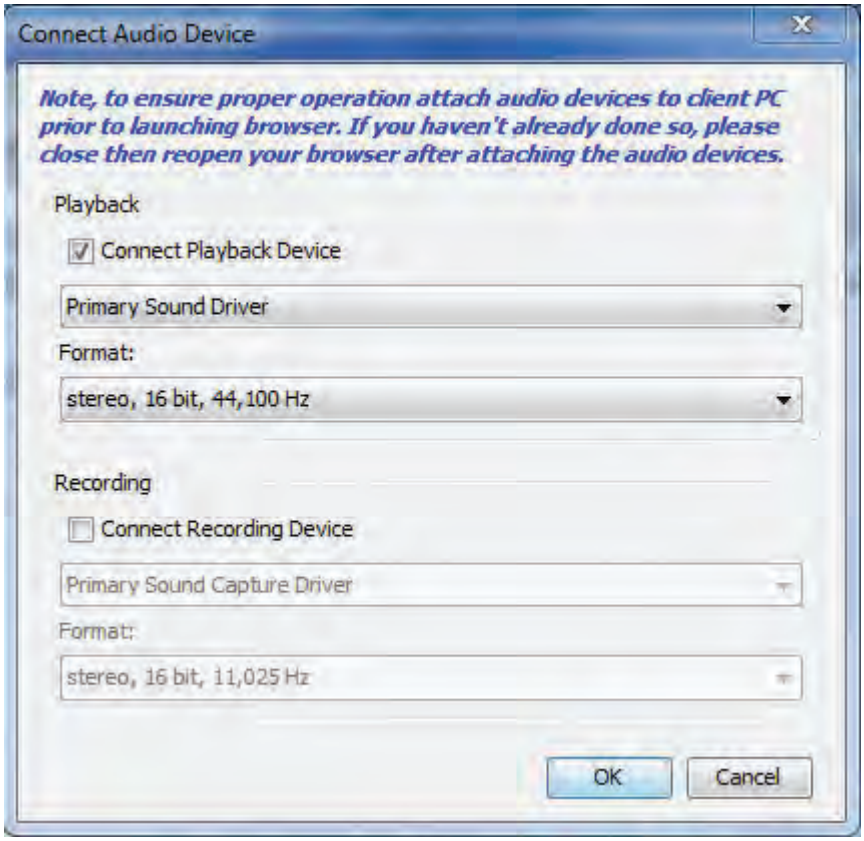
注: [Connect Recording Device] (録音デバイスを接続) ドロップダウンに表示されるデバイス名は、Java クライアント向けに 30 文字に切り捨てられます。

8. 接続するデバイスをドロップダウン リストから選択します。
9. 録音デバイスの音声形式を [Format:] (形式:) ドロップダウン リストから選択します。
10. [OK] (OK) をクリックします。音声接続が確立されると、確認メッセージが表示されます。[OK] (OK) をクリックします。

    音声接続が確立されない場合は、エラー メッセージが表示されます。

    音声接続が確立されると、[Audio] (音声) メニューが [Disconnect Audio] (音声の切断) に変わります。さらに、音声デバイス用の設定は保存され、音声デバイスに適用されます。

    スピーカー アイコン がクライアント ウィンドウの下部のステータス バーに表示されます。音声が使用されていない場合、このアイコンはグレーで表示されます。スピーカー アイコンとマイク アイコン がステータス バーに表示されている場合は、セッションがキャプチャされ、ストリーム配信されます。



▶ 音声デバイスを切断するには、以下の手順に従います。

- ツールバーの [Audio] (音声) アイコン をクリックし、切断を確認するダイアログ ボックスが開かれたら [OK] をクリックします。確認メッセージが表示されます。[OK] (OK) をクリックします。

キャプチャ/再生バッファ サイズの調整 (音声設定)

音声デバイスが接続されたら、必要に応じてキャプチャ/再生バッファ サイズを調整できます。この機能は、音声の品質を管理する場合に役に立ちます。音声の品質は、帯域幅の制限やネットワーク使用量の急増による影響を受けることがあります。

バッファ サイズを増やすと、音声の品質は改善されますが、配信速度が低下することがあります。有効な最大バッファ サイズは 400 ミリ秒であり、それより大きくすると、音声品質が大幅に低下します。

バッファ サイズは、音声セッション中も含めて、必要なときにいつでも調整できます。

音声設定は、AKC、VKC、または MPC クライアントで設定されます。

▶ 音声設定を調整するには、以下の手順に従います。

1. [Audio] (音声) メニューから [Audio Settings] (音声設定) を選択します。[Audio Settings] (音声設定) ダイアログ ボックスが開きます。
2. 必要に応じてキャプチャや再生のバッファ サイズを調整します。[OK] (OK) をクリックします。

スマート カード

KX II を使用すると、スマート カード リーダーをターゲット サーバにマウントして、スマート カード認証および関連アプリケーションをサポートできます。

サポートされているスマート カード、スマート カード リーダー、およびシステム要件の一覧については、「*サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー*『*110*p. 』」を参照してください。

注: USB スマート カード トークン（eToken NG-OTP）は、リモート クライアントからのみサポートされています。

サーバにリモートでアクセスすると、接続されたスマート カード リーダーを選択し、それをサーバにマウントできます。スマート カード認証はターゲット サーバで使用されますが、デバイスへのログインには使用されません。したがって、スマート カードの PIN と資格情報を変更するのにデバイス アカウントを更新する必要はありません。

カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

デバイスで PC 共有モードを有効にすると、複数のユーザがターゲット サーバへのアクセスを共有できます。ただし、スマート カード リーダーがターゲットに接続されている場合は、PC 共有モードの設定にかかわらず、デバイスによってプライバシーが強化されます。さらに、ターゲット サーバで共有セッションに加わっている場合は、ターゲット サーバへの排他的アクセスが可能になるまでスマート カード リーダーのマウントが無効になります。

ターゲット サーバへの KVM セッションが確立されると、Virtual KVM Client (VKC)、Active KVM Client (AKC)、および Multi-Platform Client (MPC) でスマート カードのメニューとボタンが使用可能になります。メニューを開くか [Smart Card] (スマート カード) ボタンを選択すると、リモートクライアントに接続されているスマート カード リーダーが表示されます。このダイアログ ボックスでは、追加のスマート カード リーダーを接続したり、ターゲット サーバに接続されているスマート カード リーダーのリストを更新したり、スマート カード リーダーの接続を解除したりできます。スマート カードの取り外しと再挿入も行うことができます。この機能を使用して、適切なログイン ダイアログ ボックスを表示するために、カードの取り外しまたは再挿入が必要であるターゲット サーバの OS に通知を送信できます。通知は、他のアクティブな KVM セッションに影響を与えることなく 1 台のターゲット サーバに送信できます。

▶ **スマート カード リーダーをマウントするには、以下の手順に従います。**

1. [Smart Card] (スマート カード) メニューをクリックし、[Smart Card Reader] (スマート カード リーダー) を選択します。または、ツールバーの [Smart Card] (スマート カード) ボタン をクリックします。
2. [Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスでスマート カード リーダーを選択します。
3. [Mount] (マウント) をクリックします。
4. 進行状況を示すダイアログ ボックスが開きます。次回ターゲット サーバに接続したときにスマート カード リーダーを自動的にマウントするには、[Mount selected card reader automatically on connection to targets] (選択したカード リーダーをターゲットへの接続時に自動的にマウントする) チェックボックスをオンにします。[OK] をクリックして、マウント処理を開始します。

▶ **[Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスのスマート カード リーダーを更新には、以下の手順に従います。**

- 新しいスマート カード リーダーがクライアント PC に接続された場合は、[Refresh List] (リストの更新) をクリックします。

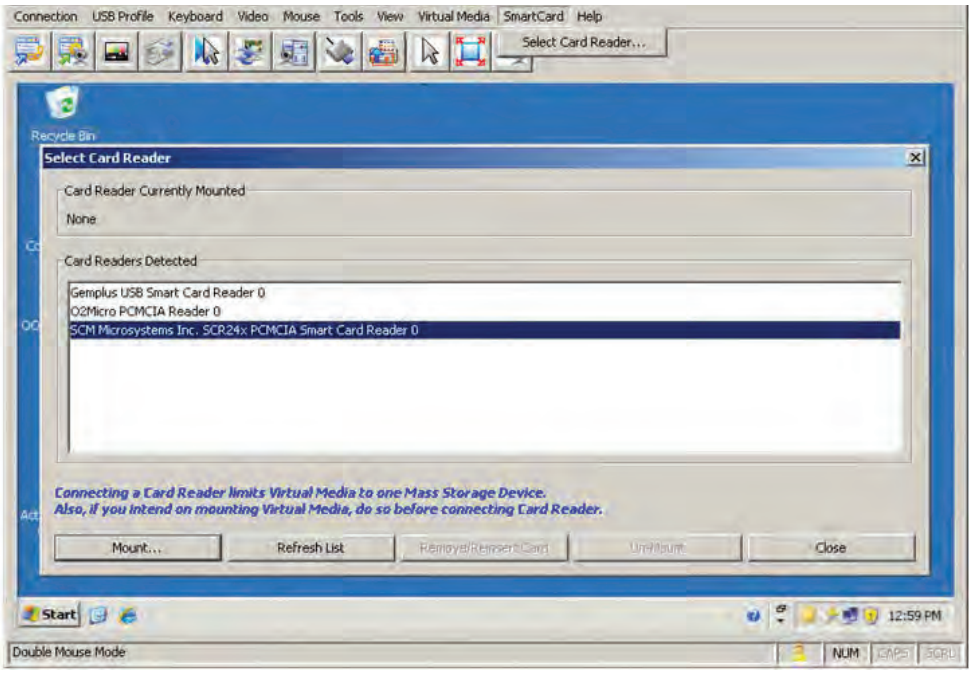
▶ **スマート カードの取り外しおよび再挿入の通知をターゲット サーバに送信するには、以下の手順に従います。**

- 現在マウントされているスマート カード リーダーを選択し、[Remove/Reinsert] (取り外し/再挿入) ボタンをクリックします。

▶ **スマート カード リーダーのマウントを解除するには、以下の手順に従います。**

- マウントを解除するスマート カード リーダーを選択し、[Unmount] (マウント解除) ボタンをクリックします。

ローカル コンソールからのスマート カード リーダーのマウントもサポートされます。詳細については、「*ローカル コンソールのスマート カード アクセス* 『*321*p. 』」を参照してください。



サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー

外付けの USB スマート カード リーダーがサポートされています。

サポートされているスマート カード リーダー

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	ローカルおよびリモートで検証済み
USB	ActivIdentity	ActivIdentity USB Reader v3.0	ローカルおよびリモートで検証済み
USB	Gemalto®	GemPC USB-SW	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Dell®	USB Smart Card Reader Keyboard	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Cherry GmbH	G83-6744 SmartBoard	ローカルおよびリモートで検証済み
SIM サイズのカードに対応した USB リーダー	Omnikey	6121	ローカルおよびリモートで検証済み
統合型 (Dell Latitude D620)	O2Micro	OZ776	リモートのみ
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	リモートのみ
PCMCIA	SCM Microsystems	SCR243	リモートのみ

注: SCM Microsystems の SCR331 スマート カード リーダーでは、SCM Microsystems のファームウェア v5.25 を使用する必要があります。

サポートされていないスマート カード リーダー

この表は、Raritan がテストし、Raritan デバイスでは動作しないことが判明しているリーダーの一覧です。したがって、これらのリーダーはサポートされていません。サポートされているスマート カード リーダーの表にもサポートされていないスマート カード リーダーの表にもないスマート カード リーダーについては、デバイスでの動作を保証できません。

タイプ	ベンダ	[Model] (モデル)	注意
USB キーボード/カー	HP®	ED707A	インタラプト エンド

タイプ	ベンダ	[Model] (モデル)	注意
ド リーダーの組み合わせ			ポイントなし => Microsoft® ドライバとの互換性なし
USB キーボード/カード リーダーの組み合わせ	SCM Microsystems	SCR338	独自のカード リーダー実装 (CCID 非準拠)
USB トークン	Aladdin®	eToken PRO™	独自の実装

ヘルプのオプション

[About Raritan Virtual KVM Client] (バージョン情報)

このメニュー コマンドを選択すると、Virtual KVM Client のバージョン情報が表示されます。このバージョン情報は、ラリタン テクニカル サポートを利用するときに必要になります。

▶ バージョン情報を調べるには、以下の手順に従います。

1. [Help] (ヘルプ) の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。
2. 後でサポート時にアクセスできるように、[Copy to Clipboard] (クリップボードにコピー) ボタンを使用して、ダイアログ ボックスに含まれている情報をクリップボード ファイルにコピーします (必要な場合)。

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) は、Raritan 製品ラインに対応するグラフィカル ユーザ インタフェースです。Raritan KVM over IP デバイスに接続されているターゲット サーバへのリモート アクセスを提供します。MPC の使用方法については、Raritan の Web サイトでユーザ ガイドと同じページから入手できる『KVM and Serial Access Client Guide』を参照してください。MPC の起動手順が記載されています。

このクライアントは Raritan の各種製品で使用されていることに注意してください。このように、ヘルプのこのセクションには、他の製品への参照が表示される場合があります。

Web ブラウザからの MPC の起動

重要: ブラウザの種類を問わず、MPC を開くためには、Dominion デバ

イスの **IP** アドレスからのポップアップを許可する必要があります。

重要: Intel® プロセッサを搭載した Mac OS X 10.5/10.6 コンピュータは JRE 1.6 を実行できるので、クライアントとして使用できます。Mac OS X 10.5.8 は、スタンドアロン クライアントとして MPC をサポートしていません。

1. サポートされるブラウザを実行しているクライアントから MPC を開くには、アドレス フィールドに「http://IP-ADDRESS/mpc」と入力します（IP-ADDRESS はラリタン デバイスの IP アドレスに置き換えてください）。MPC が新しいウィンドウに開かれます。

   注: Alt+Tab コマンドで、ローカル システム上のウィンドウ間のみでの切り替えができます。

   MPC が開かれると、自動的に検出されたラリタン デバイスおよびサブネット上で見つかったラリタン デバイスがナビゲータにツリー形式で表示されます。
2. 使用しているデバイスの名前がナビゲータに表示されていない場合は、以下の手順に従って手動で追加します。
   a. [Connection]（接続）、[New Profile]（新しいプロファイル）の順に選択します。[Add Connection]（接続の追加）ウィンドウが開きます。
   b. [Add Connection]（接続の追加）ウィンドウで、デバイスの説明を入力し、接続タイプを指定し、デバイスの IP アドレスを追加して、[OK] をクリックします。この指定内容は後で編集できます。
3. 画面左のナビゲータ パネルで、接続するラリタン デバイスに対応するアイコンをダブルクリックします。

注: お使いのブラウザおよびブラウザのセキュリティ設定によっては、さまざまなセキュリティや証明書に関する確認メッセージまたは警告メッセージが表示されることがあります。MPC を開くには、オプションを承諾する必要があります。

注: Firefox 3.0.3 を使用している場合は、アプリケーションの起動で問題が発生することがあります。この場合は、ブラウザのキャッシュをクリアして、アプリケーションを再起動してください。

Ch 4 ラック PDU (電源タップ) のコンセントの制御

この章の内容

概要 114
コンセントの電源オン/オフの切り替えまたは電源再投入を行う 115

概要

KX II では、Raritan PX および RPC シリーズのラック PDU (電源タップ) コンセントを制御できます。 これは、D2CIM-PWR を使用して KX II に接続されています。

PX または RPC シリーズをセットアップして KX II に接続すると、そのラック PDU および各コンセントを KX II のユーザ インタフェース (UI) 画面の [Powerstrip] (電源タップ) ページで制御できるようになります。このページを開くには、UI の上端にある [Power] (電源) メニューをクリックします。

[Powerstrip] (電源タップ) ページが開きます。このページには、KX II に接続されており、かつ、ユーザが適切なポートアクセス権限を付与されている、ラック PDU が表示されます。 カスケード接続の場合は、ベース KX II またはカスケード接続 KX II に接続されており、かつ、ユーザが適切なポートアクセス権限を付与されている、ラック PDU が表示されます。

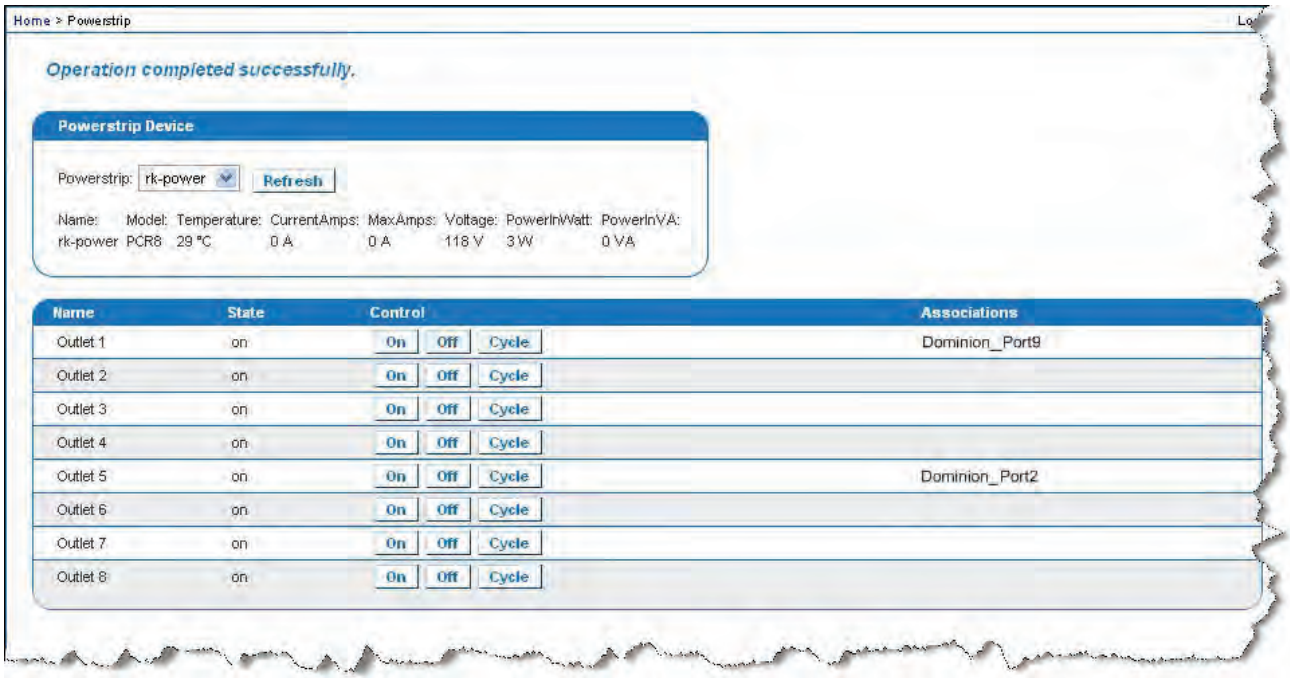
注: PX のセットアップ手順については、『Dominion PX ユーザ ガイド』を参照してください。

[Powerstrip] (電源タップ) ページでは、各コンセントの電源のオン/オフを切り替えること、および、各コンセントの電源を再投入することができます。また、電源タップおよび各コンセントに関する次の情報を表示できます。

- 電源タップに関する情報:
  - 名前
  - モデル
  - 温度
  - 電流 (A)
  - 最大電流 (A)
  - 電圧 (V)
  - 電力 (W)
  - 電力 (VA)

- コンセントに関する情報:
  - [Name] (名前): 設定時にコンセントに割り当てた名前。
  - [State] (状態): コンセントの状態 (″on″ (オン) または ″off″ (オフ))。
  - [Control] (制御): コンセントの電源を制御するボタン ([On] (オン)、[Off] (オフ)、および [Cycle] (電源再投入))。
  - [Association] (関連ポート): コンセントに関連付けられているポート。

[Powerstrip] (電源タップ) ページを開くと、KX II に接続されている電源タップが [Powerstrip] (電源タップ) ボックスの一覧に表示されます。また、そのボックスに、現在選択されている電源タップに関する情報が表示されます。KX II に接続されている電源タップが 1 台もない場合は、このページの [Powerstrip Device] (電源タップ) セクションに ″No powerstrips found″ (電源タップが見つかりません) というメッセージが表示されます。

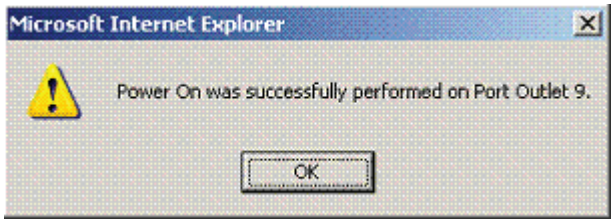


コンセントの電源オン/オフの切り替えまたは電源再投入を行う

▶ コンセントの電源をオンにするには

1. [Power] (電源) メニューをクリックし、[Powerstrip] (電源タップ) ページを開きます。
2. [Powerstrip] (電源タップ) ボックスの一覧で、コンセントの電源をオンにする PX ラック PDU (電源タップ) を選択します。

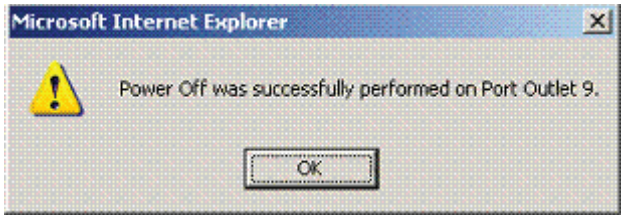
3. [Refresh] (最新の情報に更新) ボタンをクリックし、各電源制御ボタンを表示します。
4. [On] (オン) ボタンをクリックします。
5. 電源オン完了ダイアログ ボックスが開くので、[OK] をクリックして閉じます。コンセントの電源がオンになり、[State] (状態) 列の表示が "on" (オン) になります。



コンセントの電源をオフにするには

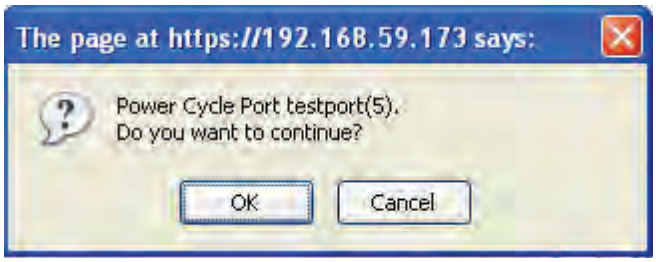
1. [Off] (オフ) ボタンをクリックします。
2. 電源オフ確認ダイアログ ボックスが開くので、[OK] をクリックして閉じます。

3. 電源オフ完了ダイアログ ボックスが開くので、[OK] をクリックして閉じます。コンセントの電源がオフになり、[State] (状態) 列の表示が "off" (オフ) になります。

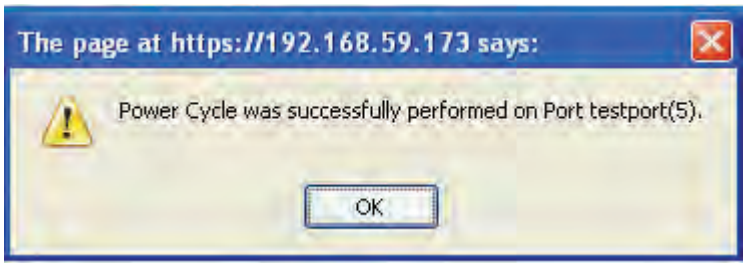


▶ コンセントの電源を再投入するには

1. [Cycle] (電源再投入) をクリックします。電源再投入確認ダイアログボックスが開きます。



2. [OK] (OK) をクリックします。コンセントの電源が再投入されます。電源再投入には数秒かかることがあります。



3. 電源再投入が完了すると、電源再投入完了ダイアログ ボックスが開きます。[OK] をクリックしてこのダイアログ ボックスを閉じます。

Ch 5 仮想メディア

この章の内容

概要 119
仮想メディアの使用 127
仮想メディアへの接続 130
仮想メディアの切断 133

概要

KVM の機能を拡張する仮想メディアを使うことで、クライアント PC やネットワーク ファイル サーバ上のメディアに、リモートの KVM ターゲット サーバからアクセスできるようになります。KX II では、ハード ディスク ドライブおよびリモートにマウントされたイメージの仮想メディアにアクセスできます。仮想メディアのセッションは、256 ビットの AES または RC4 暗号化によって保護されます。

この機能を使用すると、クライアント PC やネットワーク ファイル サーバでマウントされたメディアが、ターゲット サーバでも仮想的にマウントされます。これにより、そのメディアはターゲット サーバ自体に物理的に接続されているような形で読み書きできるようになります。仮想メディアによるデータ ファイルのサポートに加え、USB 接続を介した仮想メディアによるファイルのサポートもあります。

デジタル CIM、D2CIM-VUSB CIM、および D2CIM-DVUSB CIM（コンピュータ インタフェース モジュール）では、USB 2.0 インタフェースをサポートする KVM ターゲット サーバへの仮想メディア セッションがサポートされます。これらの CIM では、ずれないマウス機能やリモート ファームウェア アップデートもサポートされます。

仮想メディアを使用することで、以下のような作業をリモートから実行できるようになります。

- ファイルの転送
- 診断の実行
- アプリケーションのインストールと修正パッチ（patch）の適用
- オペレーティング システムの完全インストール
- デジタル音声の録音および再生*

Windows®、Mac®、Linux™ の各クライアントでは、以下の仮想メディア タイプがサポートされています。

- 内蔵または USB マウントされた CD ドライブや DVD ドライブ
- USB マス ストレージ デバイス
- PC ハード ディスク ドライブ
- ISO イメージ（ディスク イメージ）
- デジタル音声デバイス*

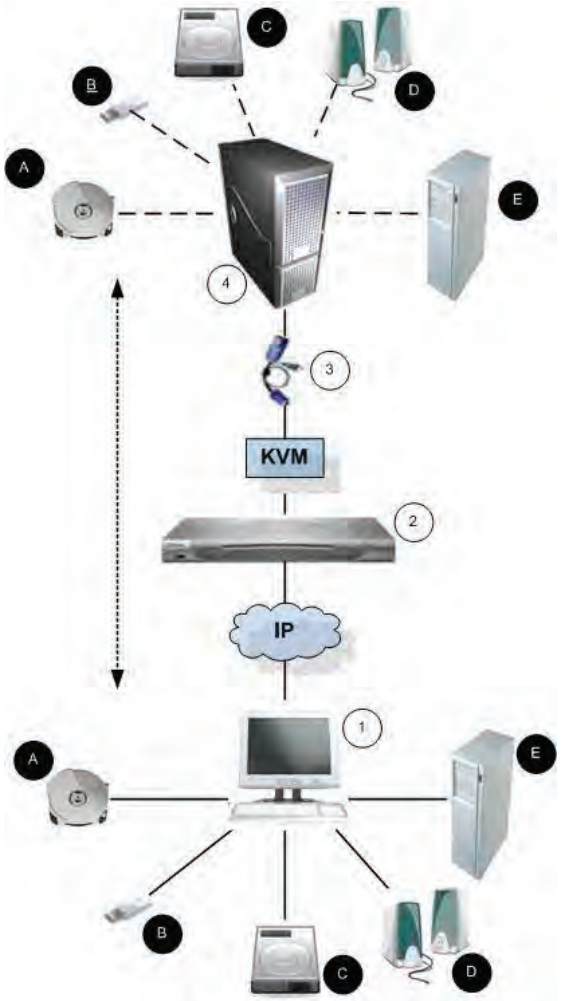
注: ラリタンは ISO9660 を標準でサポートしています。ただし、他の ISO 標準も使用できます。

サポートされているクライアント オペレーティング システムは次のとおりです。

- Windows
- Mac OS X 10.5、10.6、および 10.7
- Red Hat Desktop 4.0 および 5.0

- openSUSE 10、11
- Fedora 13 および 14

仮想メディア タイプのマウントには、Virtual KVM Client (VKC) および Multi-Platform Client (MPC) を使用できます。ただし、Mac OS X 10.5 の場合は、MPC だけを使用できます。



図の説明			
1	デスクトップ PC	B	USB マス ストレージ デバイス
2	KX II	C	PC ハード ディスク ドライブ
3	CIM	D	音声スピーカー
4	ターゲット サーバ	E	リモート ファイル サーバ (ISO イメージ)
A	CD/DVD ドライブ		

仮想メディアを使用するための条件

仮想メディア機能では、現在ターゲットに適用されている USB プロファイルがサポートする最大 2 台のドライブ（異なるタイプ）をマウントできます。このドライブは、KVM セッションの間のみアクセスできます。

たとえば、特定の CD-ROM をマウントして、それを使用し、作業が終了したらアンマウントすることができます。それでも、別の CD-ROM を仮想的にマウントできるように、この CD-ROM 仮想メディアの ″チャンネル″ は開いたままになります。こうした仮想メディアの ″チャンネル″ は、USB プロファイルでサポートされている限り、KVM セッションが閉じられるまで開いたままになります。

仮想メディアを使用するには、ターゲット サーバからアクセスするメディアをクライアントまたはネットワーク ファイル サーバに接続します。この手順を最初に行う必要はありませんが、このメディアへのアクセスを試行する前に行う必要があります。

仮想メディアを使用するには、次の条件が満たされている必要があります。a

Dominion デバイス

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス（VM アクセス ポート権限）を許可するようにデバイスを設定する必要があります。ポート権限はグループレベルで設定されます。
- デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- PC 共有を使用する場合は、[Security Settings]（セキュリティ設定）ページでセキュリティ設定を有効にする必要があります。**(オプション)**
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。

クライアント PC

- 仮想メディアの一部のオプションを使用するには、クライアント PC に対する管理者特権が必要です（ドライブ全体のドライブ リダイレクト機能など）。

注:Microsoft Vista または Windows 7 を使用している場合は、ユーザー アカウント制御を無効にするか、Internet Explorer を起動するときに［管理者として実行］を選択します。このためには、［スタート］メニューの［Internet Explorer］を右クリックし、［管理者として実行］を選択します。

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- Windows 2000 が動作する KVM ターゲット サーバには、最新の修正プログラムがすべてインストールされている必要があります。
- USB 2.0 の方が高速なため、推奨されます。

Windows XP 環境での仮想メディア

Virtual KVM Client または Active KVM Client を Windows® XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Linux 環境での仮想メディア

以下は、Linux® ユーザ向けの仮想メディアの使用に関する重要情報です。

root ユーザ権限の要件

Linux クライアントからターゲットに CD ROM をマウントし、その後 CD ROM のマウントを解除する場合は、仮想メディア接続が切断されることがあります。フロッピー ドライブをマウントし、その後フロッピーディスクを削除した場合も、接続が切断されます。この問題を回避するには、root ユーザであることが必要です。

注: Mac® および Linux® クライアントからマップされたドライブは、接続されたターゲットにマウントされた場合にロックされません。これは、Mac および Linux のサポートを提供する KX II 2.4.0 (以降) および LX 2.4.5 (以降) にのみ該当します。

権限

ドライブ/CD-ROM をターゲットに接続するためには、ユーザが適切なアクセス権限を持っている必要があります。そのためには、以下を使用してチェックします。

```
guest_user@administrator-desktop:~$ ls -l /dev/sr0
brw-rw----+ 1 root cdrom 11, 12-03-2010 11:52 /dev/sr0
```

上の例で、権限は読み取りアクセスの許可に変更されます。

ファイル ユーティリティで ACL をサポートしているシステムでは、ls コマンドの動作は次のように変わります。

- デフォルト ACL または 4 つ以上の必須 ACL エントリを含むアクセス ACL を持つファイルの場合、ls -l で出力される long 形式の ls(1) ユーティリティでは、権限文字列の後に常にプラス記号 (+) が表示されます。

これは、/dev/sr0 を使用した例で示されています。getfacl -a /dev/sr0 を使用して、ユーザが ACL に含まれるアクセスを付与されているかどうかを表示しています。この場合は、アクセスが付与されているので、cd-rom をターゲットに接続できます。これは、ls -l コマンドの出力ではそれ以外を示していても関係ありません。

```
guest_user@administrator-desktop:~$ getfacl -a /dev/sr0
getfacl:Removing leading '/' from absolute path names
# file:dev/sr0
# owner:root
# group:cdrom
user::rw-
user:guest_user:rw-
group::rw-
mask::rw-
other::---
```

リムーバブル デバイスの同様の権限チェックを示します。

```
guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1

guest_user@administrator-desktop:~$ ls -l /dev/sdb1
brw-rw---- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
&gt;   getfacl -a /dev/sdb1
getfacl:Removing leading '/' from absolute path names
# file:dev/sdb1
# owner:root
# group:disk
user::rw-
group::rw-
other::---
```

これは、ユーザにそのリムーバブル デバイスの読み取り専用許可が付与されていることを要求します。

```
root@administrator-desktop:~# chmod 664 /dev/sdb1
root@administrator-desktop:~# ls -l /dev/sdb1
brw-rw-r-- 1 root disk 8, 17 12-03-2010 12:02 /dev/sdb1
```

これで、ドライブをターゲットに接続できるようになります。

Mac 環境での仮想メディア

KX II 2.4.0 (以降) および LX 2.4.5 (以降) は、Linux 環境での仮想メディアをサポートします。 以下は、Mac® ユーザ向けの仮想メディアの使用に関する重要情報です。

アクティブ システム パーティション

- 仮想メディアを使用して、Mac クライアントのアクティブ システム パーティションをマウントすることはできません。

ドライブ パーティション

- オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。
  - Windows および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
  - Windows® および Linux® では Mac 形式のパーティションの読み取りはできない
  - Linux でサポートされているのは Windows Fat パーティションのみ
  - Windows FAT および NTFS は Mac でサポートされている
- Mac ユーザがターゲットサーバに接続するためには、既にマウントされているデバイスをアンマウントする必要があります。デバイスをアンマウントするには、>diskutil umount /dev/disk1s1 を使用し、再マウントするには、diskutil mount /dev/disk1s1 を使用します。

読み取り/書き込み可能に設定できない状況

以下の場合、仮想メディアを読み取り/書き込み可能にすることはできません。

- Linux® および Mac® の各クライアント
- 複数のハード ディスク ドライブすべてが対象の場合
- ドライブが書き込み保護されている場合
- ユーザに読み取り/書き込みの権限がない場合。
  - ポート権限の [Access] (アクセス) が [None] (なし) または [View] (表示) に設定されている場合。
  - ポート権限の [VM Access] (VM アクセス) が [Read-Only] (読み取り専用) または [Deny] (拒否) に設定されている場合。

仮想メディアの使用

仮想メディアの使用を開始する前に「*仮想メディアを使用するための前提条件* 『*122*p. の"*仮想メディアを使用するための条件*"参照 』」を参照してください。

▶ 仮想メディアを使用するには、以下の手順に従います。

1. ファイル サーバ ISO イメージにアクセスする場合は、リモート コンソールの［ファイル サーバのセットアップ］ページを使用して、ファイル サーバとイメージを指定してください。「*仮想メディア ファイル サーバのセットアップ（ファイル サーバ ISO イメージの場合のみ）* 『*128*p. 』」を参照してください。

   注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

2. 適切なターゲット サーバとの KVM セッションを開きます。
   a. リモート コンソールで［ポート アクセス］ページを開きます。
   b. ［ポート アクセス］ページでターゲット サーバに接続します。
   - 適切なサーバのポート名をクリックします。
   - ［ポート アクション］メニューの［接続］コマンドを選択します。Virtual KVM Client ウィンドウにターゲット サーバが表示されます。
3. 仮想メディアに接続します。

対象メディア	選択する **VM** オプション
ローカル ドライブ	［ドライブの接続］
ローカル CD/DVD ドライブ	［CD-ROM/ISO の接続］
ISO イメージ	［CD-ROM/ISO の接続］
ファイル サーバ ISO イメージ	［CD-ROM/ISO の接続］

作業が終わったら、仮想メディアを切断します。「*仮想メディアの切断* 『*133*p. 』」を参照してください。

仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)

注: この機能は、仮想メディアを使用してファイル サーバ ISO イメージにアクセスする場合にのみ必要です。Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

注: ファイル サーバには、SMB/CIFS のサポートが必要です。

リモート コンソールの [File Server Setup] (ファイル サーバのセットアップ) ページで、仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指定します。ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image] (リモート サーバの ISO イメージ) で [Hostname] (ホスト名) および [Image] (イメージ) ドロップダウンリスト ([Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックス) の選択肢として表示されます。「*CD-ROM/DVD-ROM/ISO イメージのマウント 『131*p. 』」を参照してください。

▶ 仮想メディアとしてアクセスするファイル サーバ ISO イメージを指定するには、以下の手順に従います。

1. リモート コンソールから仮想メディアを選択します。[File Server Setup] (ファイル サーバのセットアップ) ページが開きます。
2. 仮想メディアとしてアクセスするすべてのメディアについて、[Selected] (選択) チェックボックスをオンにします。
3. アクセスするファイル サーバ ISO イメージに関する情報を入力します。
   - [IP Address/Host Name] (IP アドレス/ホスト名) - ファイル サーバのホスト名または IP アドレスです。
   - [Image Path] (イメージのパス) - ISO イメージの場所を表す完全パス名です。たとえば、/sharename0/path0/image0.iso、¥sharename1¥path1¥image1.iso などです。

   注: ホスト名は 232 文字以内で指定してください。
4. [Save] (保存) をクリックします。これで、指定したすべてのメディアが [Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスで選択できるようになりました。

注: LX、KX、KSX、または KX101 G2 デバイスで使用されるサードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

注:Windows 2003® サーバに接続してサーバから ISO イメージをロードしようとしている場合は、「Virtual Media mounting on port failed. (ポート上でマウントしている仮想メディアに障害が発生しました。)Unable to connect to the file server or incorrect File Server username and password (ファイル サーバに接続できないか、ファイル サーバのユーザ名またはパスワードが正しくありません)」というエラーが発生することがあります。このエラーが発生する場合は、[Microsoft Network Server: Digitally Sign Communications] (Microsoft ネットワーク サーバ: デジタル的に、通信にデジタル署名を行う) を無効にします。

注: Windows 2003 Server に接続し、サーバから ISO イメージをロードしようとすると、「Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password」(ポートで仮想メディアのマウントに失敗しました。ファイル サーバに接続できないか、ファイル サーバのユーザ名とパスワードが正しくありません) というエラーが表示される場合があります。このエラーが発生した場合は、ドメイン コントローラ ポリシーでサーバの [Microsoft ネットワーク サーバー: 通信にデジタル署名を行う] オプションを無効にします。

仮想メディアへの接続

ローカル ドライブのマウント

このオプションを使用すると、ドライブ全体がマウントされます。つまり、クライアントコンピュータのディスク ドライブ全体がターゲット サーバに仮想的にマウントされます。このオプションは、ハード ディスク ドライブと外部ドライブにのみ使用してください。ネットワーク ドライブ、CD-ROM ドライブ、または DVD-ROM ドライブは対象外です。これは、[Read/Write]（読み取り/書き込み可能）を指定できる唯一のオプションです。

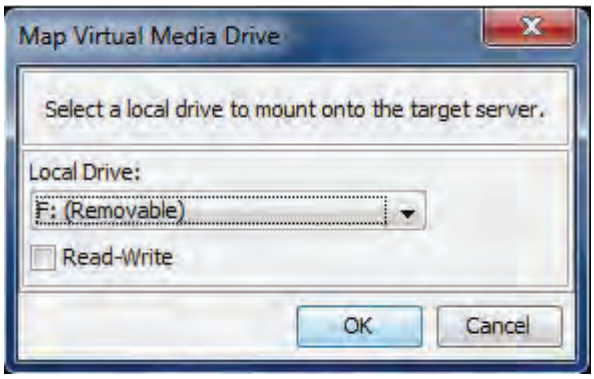
注: Windows XP® オペレーティング システムが稼動している KVM ターゲット サーバでは、NTFS 形式のパーティション（ローカル C ドライブなど）がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合があります。

その場合には、リモート コンソールを閉じて再接続した後で、別の仮想メディア デバイスをリダイレクトしてください。同じターゲット サーバに別のユーザーが接続している場合、そのユーザーの接続も閉じる必要があります。

注: KX II 2.1.0（以降）では、フロッピー ディスクなどの外部ドライブをマウントすると、ドライブの LED ライトが点灯したままになります。これは、デバイスが 500 ミリ秒ごとにドライブをチェックして、ドライブがまだマウントされているかどうかを確認するからです。

▶ クライアント コンピュータのドライブにアクセスするには、以下の手順に従います。

1. Virtual KVM Client で、[Virtual Media]（仮想メディア）の [Connect Drive]（ドライブの接続）を選択します。[Map Virtual Media Drive]（仮想メディア ドライブの割り当て）ダイアログ ボックスが表示されます。()



2. [Local Drive]（ローカル ドライブ）ドロップダウン リストから、ドライブを選択します。

3. 読み取りと書き込みの機能が必要な場合には、[Read-Write] (読み取り/書き込み可能) チェックボックスをオンにします。このオプションは、リムーバブル ドライブ以外では無効になっています。詳細は、「*読み取り/書き込み可能に設定できない状況 『126p. 』*」を参照してください。このチェックボックスをオンにすると、接続した USB ディスクに読み取りと書き込みを実行できるようになります。

   警告: 読み取り/書き込みアクセスを有効にすると危険な場合があります。同じドライブに対して同時に複数のクライアント PC からアクセスすると、データが壊れる恐れがあります。書き込みアクセスが不要な場合は、このオプションをオフのままにしてください。

4. [接続] をクリックします。メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

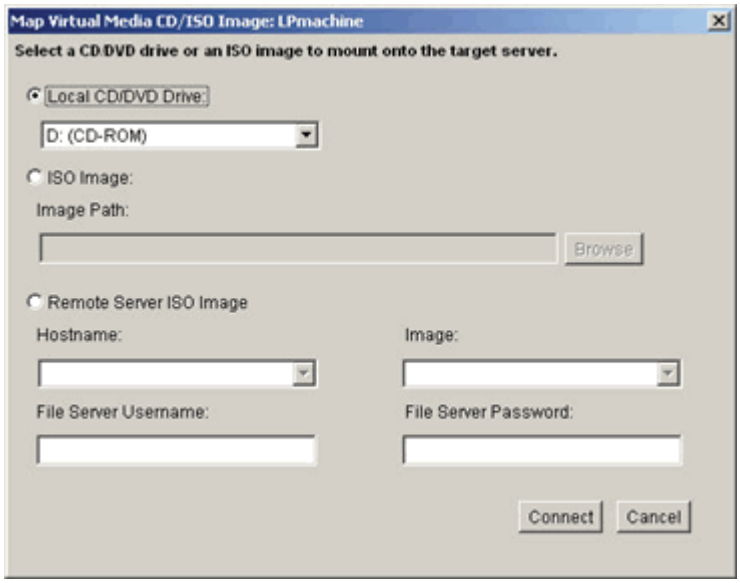
CD-ROM/DVD-ROM/ISO イメージのマウント

このオプションを使用して、CD-ROM、DVD-ROM、ISO イメージをマウントします。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

▶ CD-ROM、DVD-ROM、ISO イメージにアクセスするには、以下の手順に従います。

1. Virtual KVM Client で、[仮想メディア] の [CD-ROM/ISO イメージに接続] を選択します。[仮想メディア CD/ISO イメージの割り当て] ダイアログ ボックスが表示されます。



2. 内部および外部の CD-ROM ドライブまたは DVD-ROM ドライブの場合
   a. ［ローカル CD/DVD ドライブ］を選択します。
   b. ［ローカル CD/DVD ドライブ］ドロップダウン リストから、ドライブを選択します。使用可能なすべての内部/外部の CD ドライブおよび DVD ドライブの名前が、ドロップダウン リストに表示されます。
   c. ［接続］をクリックします。
3. ISO イメージの場合
   a. ［ISO イメージ］オプションを選択します。CD、DVD、またはハード ディスクのディスク イメージにアクセスする場合に、このオプションを使用します。サポートされる形式は ISO 形式のみです。
   b. ［参照］をクリックします。
   c. 使用するディスク イメージが含まれるパスを指定して、［開く］をクリックします。パスが［イメージのパス］フィールドに入力されます。
   d. ［接続］をクリックします。
4. ファイル サーバ上のリモート ISO イメージの場合
   a. ［リモート サーバの ISO イメージ］オプションを選択します。
   b. ドロップダウン リストから、ホスト名とイメージを選択します。ファイル サーバとイメージ パスは、［ファイル サーバのセットアップ］ページを使用して設定できます。［ファイル サーバのセットアップ］ページで設定した項目がドロップダウン リストに表示されます。
   c. ［ファイル サーバ ユーザ名］: ファイル サーバへのアクセスに必要なユーザ名です。名前には、mydomain/username のようにドメイン名を含めることができます。
   d. ［ファイル サーバ パスワード］: ファイル サーバへのアクセスに必要なパスワードです（入力時、フィールドはマスクされます）。
   e. ［接続］をクリックします。

   メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

注: Linux® ターゲット上のファイルを操作する場合、仮想メディアを使用してコピーしたファイルを表示するには、コピー後に Linux の Sync コマンドを使用します。Sync コマンドを実行するまではファイルを表示できません。

注: Windows 7® オペレーティング システム® を使用している場合、デフォルトでは、ローカル CD/DVD ドライブまたはリモート ISO イメージをマウントしたとき、リムーバブル ディスクは Windows の［マイ コンピュータ］フォルダに表示されません。ローカル CD/DVD ドライブまたはリモート ISO イメージをこのフォルダに表示するには、［ツール］メニューの［フォルダ オプション］をクリックし、［空のドライブは［コンピュータ］フォルダに表示しない］チェック ボックスをオフにします。

注: サードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

仮想メディアの切断

▶ **仮想メディア ドライブを切断するには、以下の手順に従います。**

- ローカル ドライブの場合は、[Virtual Media]（仮想メディア）の [Disconnect Drive]（ドライブの切断）を選択します。
- CD-ROM、DVD-ROM、ISO イメージの場合は、[Virtual Media]（仮想メディア）の [Disconnect CD-ROM/ISO Image]（CD-ROM/ISO イメージの切断）を選択します。

注: 切断コマンドを使用する方法だけでなく、KVM 接続を閉じても仮想メディアが切断されます。

Ch 6 USB プロファイル

この章の内容

概要 134
CIM の互換性 135
使用できる USB プロファイル 135
KVM ポート用のプロファイルの選択 143

概要

さまざまな KVM ターゲット サーバと KX II との互換性を高めるために、ラリタンは、幅広いオペレーティング システムおよび BIOS レベルのサーバ実装に対応する USB 設定プロファイルの標準的な選択肢を提供しています。

Generic (デフォルト) USB プロファイルは、展開された KVM ターゲット サーバ設定の大部分のニーズを満たしています。その他のプロファイルは、一般的に展開される他のサーバ設定 (例: Linux® や Mac OS X®) の特定のニーズを満たすように提供されています。たとえば BIOS レベルで実行される場合に、ターゲット サーバとの仮想メディア機能の互換性を強化するための、(プラットフォーム名および BIOS のリビジョンによって指定された) プロファイルも多数あります。

USB プロファイルは、KX II リモート コンソールおよびローカル コンソールで、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定)、[Port] (ポート) ページの順に選択して設定します。デバイス管理者は、ユーザおよびターゲット サーバの設定のニーズに最適なプロファイルでポートを設定できます。

KVM ターゲット サーバに接続するユーザは、KVM ターゲット サーバの動作状態に応じて、Virtual KVM Client で、これらの設定済みのプロファイルの中から選択します。たとえば、サーバが実行中で、ユーザが Windows® オペレーティング システムを使用することを希望している場合は、Generic プロファイルが最適です。しかし、BIOS メニューの設定の変更または仮想メディア ドライブからの起動を行う場合は、ターゲット サーバ モデルに応じた BIOS プロファイルの方が適している場合があります。

特定の KVM ターゲットで、ラリタンが提供する標準 USB プロファイルがいずれも適切に機能しない場合は、ラリタン テクニカル サポートにお問い合わせください。

CIM の互換性

USB プロファイルを使用するには、ファームウェアが最新であるデジタル CIM、D2CIM-VUSB、または D2CIM-DVUSB を使用する必要があります。ファームウェアを更新していない VM-CIM は、幅広い設定（キーボード、マウス、CD-ROM、およびリムーバブル ドライブ）をサポートしますが、特定のターゲット設定用に最適化されたプロファイルを使用することはできません。この場合に、USB プロファイルにアクセスするためには、既存の VM-CIM を最新のファームウェアでアップグレードする必要があります。なお、アップグレードする前でも、"Generic" プロファイルに相当する機能は利用できます。

VM-CIM ファームウェアは、ファームウェアの更新中に自動的にアップグレードされますが、ファームウェアをアップグレードしていない VM-CIM は、次のページの説明に従ってアップグレードできます。 *CIM をアップグレードする* 『*290*p. の"*CIM アップグレード*"参照 』

詳細については、「*サポートされているコンピュータ インタフェース モジュール（CIM）の仕様* 『*345*p. 』」を参照してください。

使用できる USB プロファイル

現在のリリースの KX II には、次の表に示した USB プロファイルが用意されています。新しいプロファイルは、Raritan が提供する各ファームウェア アップグレードに含まれています。新しいプロファイルが追加されると、それがヘルプに記載されます。

USB プロファイル	説明
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Dell PowerEdge 1950/2950/2970/6950/R200 BIOS には、このプロファイルまたは 'Generic' プロファイルを使用します。 制限: • なし
BIOS Dell OptiPlex ™ キーボードのみ	Dell OptiPlex BIOS アクセス（キーボードのみ） D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell OptiPlex BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。

USB プロファイル	説明
	注意: • Optiplex 210L/280/745/GX620 では、仮想メディアをサポートするために、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。 制限: • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • 仮想メディアはサポートされていません。
BIOS DellPowerEdge Keyboard Only	Dell PowerEdge BIOS アクセス (キーボードのみ) D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell PowerEdge BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。 注意: • PowerEdge 650/1650/1750/2600/2650 BIOS では、USB CD-ROM およびディスクドライブは起動可能デバイスとしてはサポートされていません。 • PowerEdge 750/850/860/1850/2850/SC1425 BIOS で仮想メディアをサポートするには、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。 • BIOS で実行している場合は、PowerEdge 1950/2950/2970/6950/R200 に 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' または 'Generic' プロファイルを使用します。 制限: • USB バス速度はフルスピード (12

USB プロファイル	説明
	MBit/s）に制限されます。 • ずれないマウス（Absolute mouse synchronization™）はサポートされていません。 • 仮想メディアはサポートされていません。
BIOS ASUS P4C800 マザーボード	BIOS にアクセスしたり、Asus P4C800 ベースのシステムで仮想メディアから起動したりするには、このプロファイルを使用します。 制限: • USB バス速度はフルスピード（12 MBit/s）に制限されます。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS 汎用	BIOS 汎用 このプロファイルは Generic OS プロファイルが BIOS で機能しない場合に使用します。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。 制限: • USB バス速度はフルスピード（12 MBit/s）に制限されます。 • ずれないマウス（Absolute mouse synchronization™）はサポートされていません。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS HP Proliant DL145 PhoenixBIOS では、OS のインストール中に、このプロファイルを使用します。 制限: • USB バス速度はフルスピード（12

USB プロファイル	説明
	MBit/s) に制限されます。
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 HP Compaq DC7100/DC7600 シリーズのデスクトップを仮想メディアから起動するにはこのプロファイルを使用します。 制限: • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS BIOS 操作中は IBM® Thinkcentre Lenovo システム ボード (828841U モデル) にこのプロファイルを使用します。 制限: • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
アドバンスト マネージメント モジュールを装備した IBM BladeCenter H	D2CIM-VUSB または D2CIM-DVUSB がアドバンスト マネージメント モジュールに接続されている場合に、仮想メディア機能を有効にするには、このプロファイルを使用します。 制限: • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 および X61 (仮想メディアから起動) T61 および X61 シリーズのラップトップを仮想メディアから起動するには、このプロファイルを使用します。 制限: • USB バス速度はフルスピード (12 MBit/s) に制限されます。

USB プロファイル	説明
BIOS Mac	BIOS Mac このプロファイルは Mac® BIOS に使用します。 制限: • ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Generic (汎用)	汎用 USB プロファイルは、オリジナルの KX2 リリースの動作と似ています。このプロファイルは、Windows 2000®、Windows XP®、Windows Vista®、およびそれ以降の Windows に対して使用します。 制限: • なし
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用して OS をインストールする場合に使用します。 制限: • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
HP Proliant DL360/DL380 G4 (Windows® Server 2003 インストール)	HP Proliant DL360/DL380 G4 (Windows Server 2003 インストール) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用せずに Windows Server 2003 をインストールする場合に使用します。 制限: • USB バス速度はフルスピード (12

USB プロファイル	説明
	MBit/s) に制限されます。
Linux®	汎用 Linux プロファイル これは、汎用 Linux プロファイルです。Redhat Enterprise Linux、SuSE Linux Enterprise Desktop、および類似のディストリビューションで使用されます。 制限: • ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
MAC OS X® (10.4.9 以降)	MAC OS X (10.4.9 以降) このプロファイルは、最近のバージョンの Mac OS-X で導入されたマウス座標のスケーリングを補正します。リモートおよびローカルのマウスの位置がデスクトップの境界の近くで同期しない場合はこれを選択します。 制限: • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
RUBY 工業用メインボード (AwardBIOS)	RUBY 工業用メインボード (AwardBIOS) このプロファイルは、Phoenix/AwardBIOS v6.00PG を使用する RUBY-9715VG2A シリーズの工業用メインボードで使用します。 制限: • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro メインボード Phoenix (AwardBIOS) このプロファイルは、Phoenix AwardBIOS を使用する Supermicro シリーズのメインボードで使用されま

USB プロファイル	説明
	す。 制限: • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Suse 9.2	SuSE Linux 9.2 これは SuSE Linux 9.2 ディストリビューションで使用されます。 制限: • ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 • USB バス速度はフルスピード (12 MBit/s) に制限されます。
Troubleshooting 1	トラブルシューティング プロファイル 1 • マス ストレージが優先 • キーボードおよびマウス (タイプ 1) • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 2	トラブルシューティング プロファイル 2 • キーボードおよびマウス (タイプ 2) 優先 • マス ストレージ • USB バス速度はフルスピード (12 MBit/s) に制限されます。 • 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
	警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 3	トラブルシューティング プロファイル 3 ● マス ストレージが優先 ● キーボードおよびマウス（タイプ 2） ● USB バス速度はフルスピード（12 MBit/s）に制限されます。 ● 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
仮想メディア CIM でフルスピードを使用	仮想メディア CIM でフルスピードを使用 このプロファイルは、[Full Speed for Virtual Media CIM]（仮想メディア CIM でフルスピードを使用）オプションを選択したオリジナルの KX2 リリースの動作に似ています。高速 USB デバイスを処理できない BIOS に便利です。 制限: ● USB バス速度はフルスピード（12 MBit/s）に制限されます。

USB プロファイル	説明
キーボードおよびマウスの USB でフル スピードを使用	このプロファイルでは、デュアル VM CIM のキーボードおよびマウスの USB インタフェースがフル スピードに設定されます。低速 USB 設定では正しく動作できないデバイスに有効です。 制限: • キーボードおよびマウスの USB インタフェースの USB バス速度は、フル スピード（12 MBit/s）に設定されます。

KVM ポート用のプロファイルの選択

KX II には、USB プロファイルのセットが含まれているので、接続先の KVM ターゲット サーバの特性に基づいて KVM ポートを割り当てることができます。KX II リモートまたはローカル コンソールで、[Device Settings]（デバイス設定）、[Port Configuration]（ポート設定）、[Port]（ポート）ページの順に選択し、USB プロファイルを KVM ポートに割り当ています。

特定のターゲットで必要になる可能性が最も高いプロファイルを指定するのは、管理者です。これらのプロファイルは、MPC、AKC、および VKC 経由での選択に使用できるようになります。プロファイルを利用できない場合は、[USB Profile]（USB プロファイル）の [Other Profiles]（他のプロファイル）を選択して、使用可能なプロファイルにアクセスできます。

USB プロファイルを KVM ポートに割り当てると、ユーザが KVM ターゲット サーバに接続するときにそれらのプロファイルを使用できるようになります。必要な場合は、VKC、AKC、または MPC の [USB Profile]（USB プロファイル）メニューから USB プロファイルを選択できます。

USB プロファイルを KVM ポートに割り当てる方法の詳細は、「*USB プロファイルの設定（[Port]（ポート）ページ）『243*p. 』」を参照してください。

DCIM-VUSB で Mac OS-X USB プロファイルを使用する場合のマウスモード

DCIM-VUSB で Max OS X® USB プロファイルを使用し、Mac OS X 10.4.9 以降を実行している場合は、再起動時にブート メニューでマウスを使用するためにシングル マウス モードに切り替える必要があります。

▶ ブート メニューで動作するようにマウスを設定するには、以下の手順に従います。

1. Mac を再起動し、再起動中に option キーを押してブート メニューを開きます。この時点では、マウスは応答しません。
2. [Intelligent Mouse] (インテリジェント マウス) モードを選択してから [Single Mouse] (シングル マウス) モードを選択します。マウスが応答します。

   注: シングル マウス モードでは、マウスの速度が遅くなることがあります。

3. ブート メニューを終了してオペレーティング システムが起動したら、マウスのパフォーマンスを向上させるために、シングル マウス モードを終了してずれないマウス モードに戻ります。

Ch 7 [User Management] (ユーザ管理)

この章の内容

ユーザ グループ 145
ユーザ 154
[Authentication Settings] (認証設定) 159
パスワードの変更 172

ユーザ グループ

KX II は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内部リストを保持しています。この情報は、暗号化形式で内部に保存されます。認証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。すべてのユーザは認証を受ける必要があります。LDAP/LDAPS または RADIUS 認証を行うように KX II が設定されている場合、その認証が行われた後に、ローカル認証が行われます。

すべての KX II には、3 つのデフォルト ユーザ グループが存在します。これらのグループは削除できません。

ユーザ	説明
Admin (管理者)	このグループに所属するユーザは、完全な管理者特権を持ちます。元の製品出荷時のデフォルト ユーザはこのグループのメンバーであり、完全なシステム特権を持ちます。さらに、Admin (管理者) ユーザは Admin (管理者) グループのメンバーである必要があります。
Unknown (不明)	LDAP/LDAPS または RADIUS を使用して外部的に認証されるユーザまたはシステムで既知のユーザのデフォルト グループです。外部 LDAP/LDAPS サーバまたは RADIUS サーバによって有効なユーザ グループが識別されなかった場合、Unknown (不明) グループが使用されます。さらに、新規に作成されたユーザは別のグループに割り当てられるまでこのグループに自動的に配置されます。
Individual Group (個別グループ)	個別グループとは、基本的に個人の「グループ」です。つまり、特定のユーザは独自のグループに属し、他の実際のグループには属しません。個別グループは、グループ名の先頭に "@" が付けられているので区別できます。個別グループでは、グループと同じ権限をユーザ アカウントに割り当てることができます。

KX II 内では最大 254 個のユーザ グループを作成できます。 KX II 内では最大 254 個のユーザ グループを作成できます。

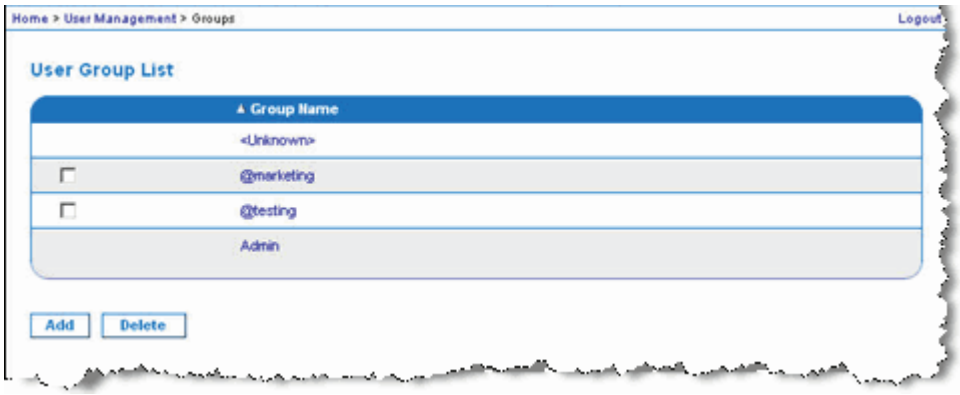
ユーザ グループ リスト

ユーザ グループは、ローカル認証とリモート認証（RADIUS または LDAP/LDAPS）で使用されます。個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

[ユーザ グループ リスト] ページには、すべてのユーザ グループのリストが表示されます。このリストは、[グループ名] 列見出しをクリックすることで、昇順または降順に並べ替えることができます。[ユーザ グループ リスト] ページでは、ユーザ グループを追加、変更、または削除することもできます。

▶ ユーザ グループのリストを表示するには、以下の手順に従います。

- [ユーザ管理] の [ユーザ グループ リスト] を選択します。[ユーザ グループ リスト] ページが開きます。



ユーザとグループの関係

ユーザはグループに属し、グループには特権が割り当てられています。KX II の各種のユーザをグループに分けることにより、ユーザごとに許可を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能です。その場合は、ユーザを「個別」として分類します。

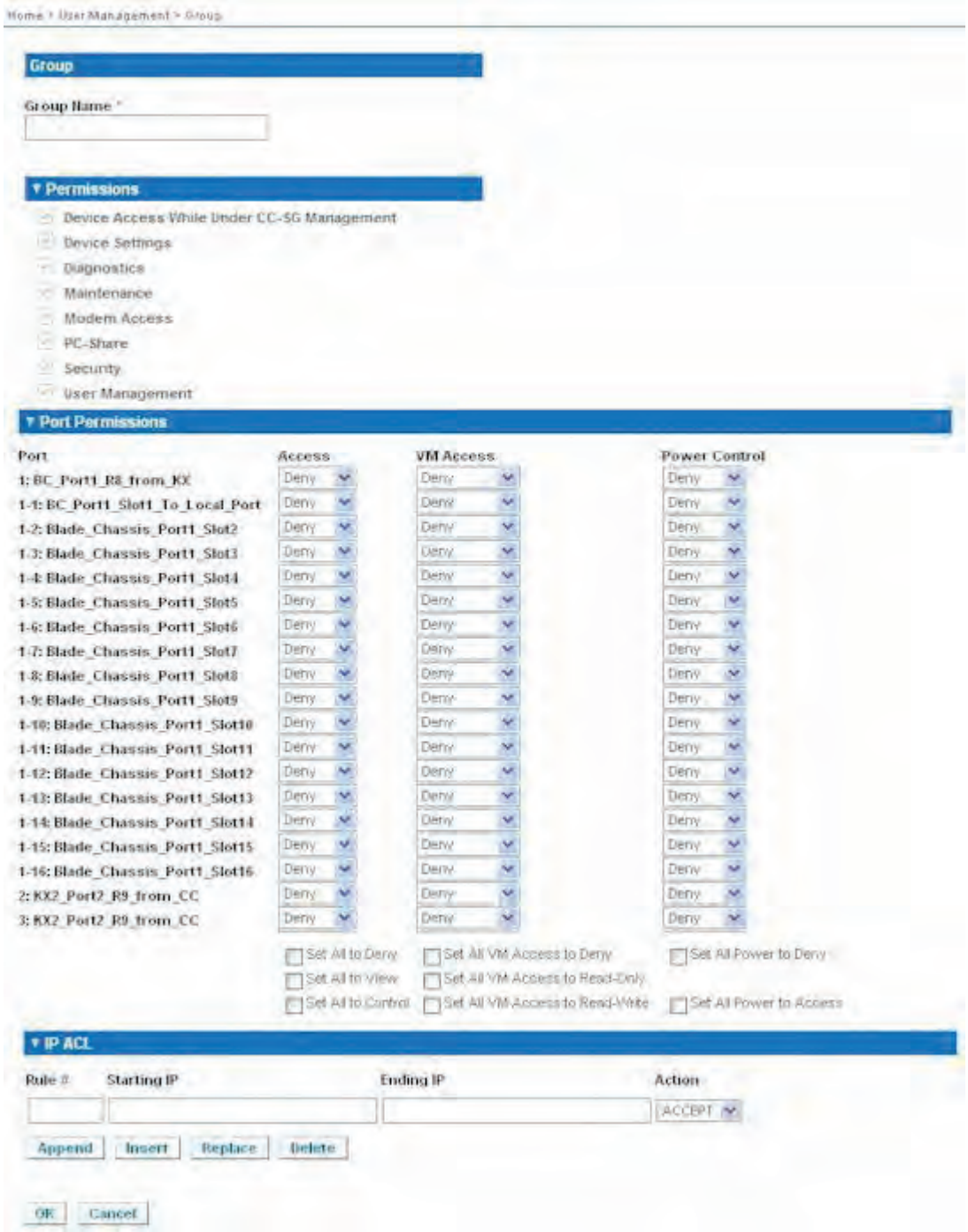
認証が成功すると、デバイスは、グループ情報を使用して、アクセスできるサーバ ポート、デバイスの再起動を許可するかどうかなど、そのユーザの許可を決定します。

新規ユーザ グループの追加

▶ 新規ユーザ グループを追加するには、以下の手順に従います。

1. [ユーザ管理] の [新規ユーザ グループの追加] を選択するか、[ユーザ グループ リスト] ページの [追加] をクリックします。
2. [グループ名] フィールドに、新しいユーザ グループのわかりやすい名前 (最大 64 文字) を入力します。
3. このグループに属するすべてのユーザに対して割り当てる許可の横にあるチェックボックスをオンにします。「*許可の設定* 『*149*p. 』」を参照してください。
4. このグループに属するユーザがアクセスできるサーバ ポートと、そのアクセスのタイプを指定します。「*ポート権限の設定* 『*150*p. 』」を参照してください。
5. IP ACL を設定します。この機能は、IP アドレスを指定することで、KX II デバイスへのアクセスを制限します。この機能は、特定のグループに属するユーザにのみ適用されます。このデバイスに対するすべてのアクセス試行に適用され、優先される、IP アクセス制御リスト機能とは異なります。「*グループベースの IP ACL (アクセス制御リスト)* 『*152*p. 』」を参照してください。(オプション)
6. [OK] (OK) をクリックします。

注: 複数の管理機能を MPC 内および KX II ローカル コンソールから利用できます。これらの機能を利用できるのは、デフォルトの Admin (管理者) グループのメンバーに限られます。



許可の設定

重要: [ユーザ管理] チェックボックスをオンにすると、グループのメンバーは、自身も含むすべてのユーザの許可を変更することができます。これらの許可を付与する場合は注意してください。

許可	説明
[Device Access While Under CC-SG Management] (CC-SG 管理下のデバイス アクセス)	この許可を持つユーザとユーザ グループは、CC-SG のデバイスに対してローカル アクセスが有効になっている場合に IP アドレスを使用して直接 KX II にアクセスできます。デバイスには、ローカル コンソール、リモート コンソール、MPC、VKC、および AKC からアクセスできます。 CC-SG の管理下にあるデバイスに直接アクセスすると、KX II でアクセスおよび接続アクティビティがログに記録されます。ユーザ認証は、KX II の認証設定に基づいて実行されます。 *注: 管理者ユーザ グループには、この許可がデフォルトで付与されます。*
[Device Settings] (デバイス設定)	ネットワーク設定、日付/時刻設定、ポート設定(チャンネル名、電源の関連付け)、イベント管理(SNMP、Syslog)、仮想メディア ファイル サーバのセットアップ。
診断	ネットワーク インタフェース ステータス、ネットワーク統計、ホストへの Ping、ホストへのトレース ルート、KX II 診断
保守	データベースのバックアップと復元、ファームウェアのアップグレード、ファクトリ リセット、再起動
[Modem Access] (モデム アクセス)	モデムを使用して KX II デバイスに接続する許可。
[PC-Share] (PC 共有)	複数のユーザによる同一ターゲットへの同時アクセス カスケード接続構成を使用しており、ベース KX II デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合は、すべてのデバイス間で同じ PC 共有設定を共有する必要があります。カスケード接続の詳細につい

許可	説明
	ては、「*カスケード接続を設定および有効化する 『181*p. 』」を参照してください。
セキュリティ	SSL 証明書、セキュリティ設定 (VM 共有、PC 共有)、IP ACL
[User Management] (ユーザ管理)	ユーザおよびグループの管理、リモート認証 (LDAP/LDAPS/RADIUS)、ログイン設定。 カスケード接続構成にしており、ベース KX II デバイスから他の複数台のカスケード接続デバイスにアクセスしている場合、ユーザ設定、ユーザ グループ設定、およびリモート認証設定をすべてのデバイス間で統一する必要があります。カスケード接続の詳細については、「*カスケード接続を設定および有効化する『181*p. 』」を参照してください。

ポート権限の設定

それぞれのサーバ ポートに対して、そのグループが持つアクセスのタイプ、仮想メディアへのポート アクセスのタイプ、および電源管理を指定できます。すべての権限についてデフォルト設定はすべて [Deny] (拒否) になっていることに注意してください。

ポート アクセス	
オプション	説明
[Deny] (拒否)	アクセスを完全に拒否します。
[View] (表示)	接続先のターゲット サーバのビデオを表示します (操作はできません)。
[Control] (制御)	接続先のターゲット サーバを制御します。VM および電源管理アクセスも付与される場合は、[Control] (制御) を割り当てる必要があります。 追加された KVM スイッチをユーザ グループ内のすべてのユーザが表示できるようにするためには、各ユーザに [Control] (制御) アクセスが付与されている必要があります。この権限を持たないユーザには、KVM スイッチが後で追加されても、スイッチは表示されません。 アクティブになるコントロールに関連する音声または

	スマート カードに対する [Control] (制御) アクセスの付与が必要です。

VM アクセス	
オプション	説明
[拒否]	ポートに対して仮想メディア許可はすべて拒否されます。
[読み取り専用]	仮想メディア アクセスは、読み取りアクセスのみに制限されます。
[読み取り/書き込み可能]	仮想メディアに対する完全なアクセス (読み取り、書き込み) が許可されます。

電源管理アクセス	
オプション	説明
[Deny] (拒否)	ターゲット サーバに対する電源管理を拒否します。
[Access] (アクセス)	ターゲット サーバでの電源管理を完全に許可します。

ブレード シャーシの場合、ポート アクセス権限によって、そのブレード シャーシに設定されている URL へのアクセスを制御します。オプションは、[Deny] (拒否) または [Control] (制御) です。また、シャーシ内の各ブレードには、固有の独立ポート権限設定があります。

ティアー接続構成にしており、ベース KX II デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、カスケード接続デバイスでは個別のポート制御レベルが適用されます。カスケード接続の詳細については、「*カスケード接続を設定および有効化する 『181*p. 』」を参照してください。

個別グループの許可の設定

▶ 個別ユーザ グループに許可を設定するには、以下の手順に従います。

1. グループ リストから目的のグループを探します。個別グループは、グループ名の先頭に @ が付けられているので区別できます。
2. グループ名をクリックします。[Group] (グループ) ページが開きます。
3. 適切な許可を選択します。
4. [OK] をクリックします。

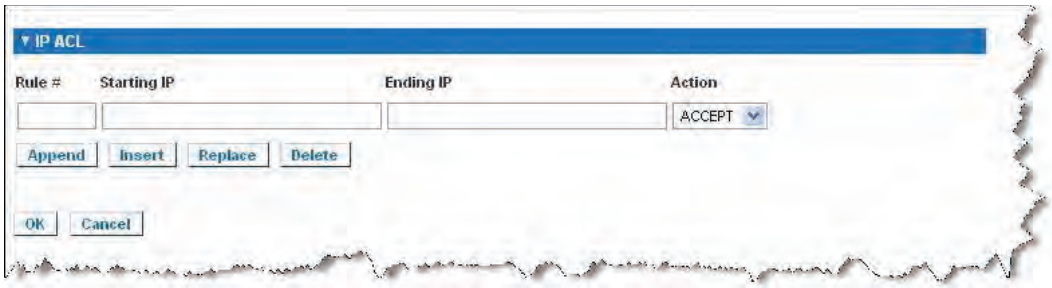
グループベースの **IP ACL** (アクセス制御リスト)

重要: グループベースの IP アクセス制御を使用する場合は注意が必要です。アクセスが拒否されている IP アドレスの範囲に自分の IP アドレスが含まれている場合、KX II がロックアウトされてしまいます。

この機能は、選択したグループに含まれるユーザによる KX II デバイスへのアクセスを特定の IP アドレスに制限します。この機能は、デバイスへのすべてのアクセス試行に適用される (および最初に処理され、優先される) IP アクセス制御リスト機能とは異なり、特定のグループに属するユーザにのみ適用されます。

重要: KX II ローカル ポートでは、IP アドレス 127.0.0.1 が使用され、ブロックはできません。

グループレベルで IP アクセス制御ルールの追加、挿入、置換、削除を行うには、[Group] (グループ) ページの [IP ACL] (IP ACL) セクションを使用します。



ルールを一覧の末尾に追加するには

1. [Starting IP] (開始 IP) フィールドに、開始 IP アドレスを入力します。
2. [Ending IP] (終了 IP) フィールドに、終了 IP アドレスを入力します。
3. 利用可能なオプションからアクションを選択します。
   - [Accept] (承諾) – その IP アドレスによる KX II デバイスへのアクセスが許可されます。
   - [Drop] (拒否) – その IP アドレスによる KX II デバイスへのアクセスが拒否されます。
4. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。入力する各ルールについて、手順 1 ～ 4 を繰り返します。

ルールを一覧の途中に挿入するには

1. ルール番号 (#) を入力します。[Insert] (挿入) コマンドを使用する際にルール番号が必要です。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。

3. [Action] (アクション) ドロップダウン リストからアクションを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号が既存のルール番号と同じである場合は、新しいルールは既存のルールの上に挿入され、リスト内のすべてのルールが下に下がります。

ルールの内容を置換するには

1. 置き換えるルール番号を指定します。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。
3. ドロップダウン リストからアクションを選択します。
4. [Replace] (置換) をクリックします。同じルール番号を持つ元のルールが新しいルールに置き換わります。

ルールを削除するには

1. 削除するルール番号を指定します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

重要: ACL のルールは、リスト表示されている順に評価されます。たとえばこの例において、2 つの ACL ルールの順番が逆になると、Dominion は通信を全く受けることができなくなります。

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```

ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

既存のユーザ グループの変更

注: Admin (管理者) グループに対しては、すべての許可が有効になっています。この設定は変更できません。

既存のユーザ グループを変更するには、以下の手順に従います。

1. [グループ] ページで、適切なフィールドを変更し、適切な許可を設定します。
2. グループに対する許可を設定します。このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。「*許可の設定* 『*149*p. 』」を参照してください。

3. ［ポート権限］を設定します。このグループに属するユーザがアクセスできるサーバ ポート（およびアクセスのタイプ）を指定します。「*ポート権限の設定 『150p. 』*」を参照してください。
4. IP ACL を設定します（オプション）。この機能は、IP アドレスを指定することで、KX II デバイスへのアクセスを制限します。「*グループベースの IP ACL（アクセス制御リスト）『152p. 』*」を参照してください。
5. ［OK］（OK）をクリックします。

▶ ユーザ グループを削除するには、以下の手順に従います。

重要: ユーザを含むグループを削除すると、そのユーザは <不明> ユーザ グループに自動的に割り当てられます。

ヒント: 特定のグループに属しているユーザを調べるには、ユーザ グループ別にユーザ リストを並べ替えます。

1. リストのグループ名の左にあるチェックボックスをオンにして、目的のグループを選択します。
2. ［削除］をクリックします。
3. 削除を確認するプロンプトが表示されたら、［OK］をクリックします。

ユーザ

ユーザが KX II にアクセスするには、ユーザ名とパスワードを付与されている必要があります。この情報は、KX II にアクセスしようとしているユーザを認証するために使用されます。 各ユーザ グループに対して最大 254 個のユーザを作成できます。

ティアー接続構成にしており、ベース KX II デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ユーザは、ベース デバイスにアクセスする許可、および、（必要に応じて）個々のティアー接続デバイスにアクセスする許可を必要とします。ユーザがベース デバイスにログオンすると、各ティアー接続デバイスが照会され、ユーザは、アクセス許可を得ている各ターゲット サーバにアクセスできます。 ティアー接続の詳細については、「*ティアー接続を設定および有効化する『181p. の"カスケード接続を設定および有効化する"参照 』*」を参照してください。

KX II ユーザ リストの表示

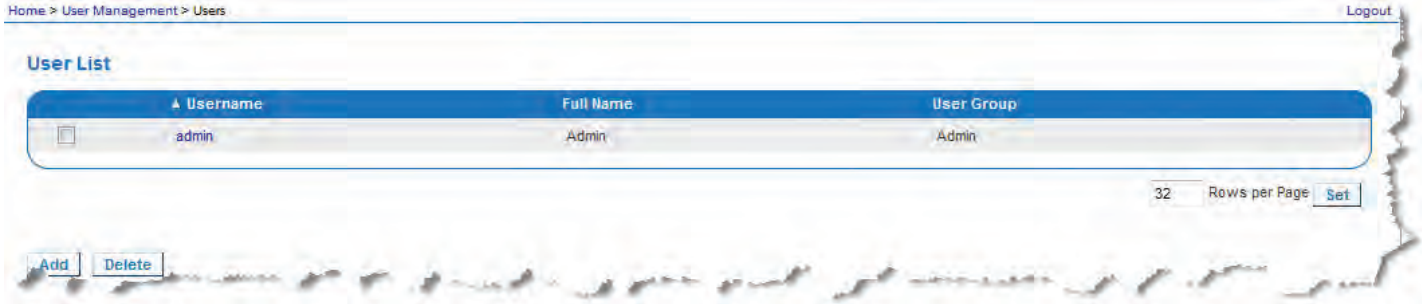
[User List] (ユーザ リスト) ページには、すべてのユーザについて、ユーザ名、フル ネーム、およびユーザ グループが表示されます。このリストは、任意の列名をクリックすることで並べ替えることができます。[User List] (ユーザ リスト) ページでは、ユーザを追加、変更、または削除できます。

ユーザ管理権限を持つ KX II ユーザは、必要に応じてユーザをポートから切断するか、ログオフ (強制ログオフ) することができます。「*ポートからのユーザの切断 『156p. 』*」および「*KX II からのユーザのログオフ (強制ログオフ) 『157p. 』*」をそれぞれ参照してください。

各ユーザの接続先ターゲット ポートを表示するには、「*ポート別のユーザの表示 『156p. 』*」を参照してください。

▶ ユーザ リストを表示するには、以下の手順に従います。

- [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択します。[User List] (ユーザ リスト) ページが開きます。



ポート別のユーザの表示

[User By Ports] (ポート別ユーザ) ページには、認証済みのすべてのローカル ユーザとリモート ユーザおよび各ユーザの接続先のポートが表示されます。ポートへの永続的な接続のみが表示されます。ポートのスキャン時にアクセスされているポートは表示されません。

同じユーザが複数のクライアントからログオンしている場合は、接続ごとにユーザ名がページに表示されます。たとえば、ユーザが 2 つの異なるクライアントからログオンしている場合、そのユーザ名が 2 回表示されます。

このページには、次のユーザ情報およびポート情報が表示されます。

- [Port Number] (ポート番号) – ユーザの接続先ポートに割り当てられているポート番号
- [Port Name] (ポート名) – ユーザの接続先ポートに割り当てられているポート名

  注: ユーザがターゲットに接続されていない場合は、[Port Name] (ポート名) の下に [Local Console] (ローカル コンソール) または [Remote Console] (リモート コンソール) が表示されます。

- [Username] (ユーザ名) – ユーザ ログインやターゲット接続用のユーザ名
- [Access From] (アクセス元) – アクセス元の KX II の IP アドレス
- [Status] (ステータス) – 接続の現在のステータス (アクティブまたは非アクティブ)

▶ ポート別にユーザを表示するには、以下の手順に従います。

- [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。

ポートからのユーザの切断

ユーザの切断では、ユーザは KX II をログオフしなくてもターゲット ポートから切断されます。

注: ユーザのログオフでは、ユーザはターゲット ポートから切断され、KX II からログオフされます。ユーザの強制ログオフについては、「KX II からのユーザのログオフ (強制ログオフ) 『157p. 』」を参照してください。

▶ ユーザをポートから切断するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。

3. [Disconnect User from Port] (ポートからのユーザの切断) をクリックします。
4. 確認メッセージに対して [OK] をクリックすると、ユーザがポートから切断されます。
5. ユーザがポートから断されたことを示す確認メッセージが表示されます。

KX II からのユーザのログオフ (強制ログオフ)

管理者である場合は、KX II にログオンしているユーザのうち、認証されているユーザをログオフすることができます。また、ユーザをポート レベルでポートから切断することもできます。「*ポートからのユーザの切断 『156p. 』*」を参照してください。

▶ **ユーザを KX II からログオフするには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. [Force User Logoff] (ユーザの強制ログオフ) をクリックします。
4. [Logoff User] (ユーザのログオフ) の確認メッセージに対して [OK] をクリックします。

新規ユーザの追加

KX II ユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。「**新規ユーザ グループの追加 『147p. 』**」を参照してください。

[User] (ユーザ) ページでは、新規ユーザの追加、ユーザ情報の変更、無効化されているユーザの再有効化を行うことができます。

*注: ユーザがログインに失敗した回数が [Security Settings] (セキュリティ設定) ページで設定されているログイン失敗の最大許容回数を超えた場合、そのユーザ名は無効化されます。「**セキュリティの設定 『263p. 』**」を参照してください。*

▶ **新規ユーザを追加するには、以下の手順に従います。**

1. [ユーザ管理] の [新規ユーザの追加] を選択するか、[ユーザ リスト] ページの [追加] をクリックします。
2. [ユーザ名] フィールドに、一意のユーザ名を入力します (最大 16 文字)。
3. [フル ネーム] フィールドに、ユーザのフル ネームを入力します (最大 64 文字)。

4. [パスワード] フィールドにパスワードを入力し、[パスワードの確認] フィールドにパスワードを再入力します (最大 64 文字)。
5. [ユーザ グループ] ドロップダウン リストからグループを選択します。

   このユーザを既存のユーザ グループに関連付けたくない場合は、ドロップダウン リストから [Individual Group] (個別グループ) を選択します。個別グループの許可についての詳細は、「*個別グループの許可の設定 『151*p. 』」を参照してください。
6. 新規ユーザを有効にするには、[アクティブ] チェックボックスをオンのままにします。[OK] をクリックします。

既存のユーザ グループの変更

▶ 既存のユーザを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択して、[User List] (ユーザ リスト) ページを開きます。
2. [User List] (ユーザ リスト) ページのリストから目的のユーザを探します。
3. ユーザ名をクリックします。[User] (ユーザ) ページが開きます。
4. [User] (ユーザ) ページで、目的のフィールドを変更します [User] (ユーザ) ページにアクセスする方法についての詳細は、「*新規ユーザの追加 『157*p. 』」を参照してください。
5. ユーザを削除するには、[Delete] (削除) をクリックします。削除してよいかどうかを確認するダイアログ ボックスが開きます。
6. [OK] (OK) をクリックします。

[Authentication Settings] (認証設定)

認証とは、ユーザが本物であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

KX II がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

ティアー接続構成にしており、ベース KX II デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、ベース デバイスと各ティアー接続デバイスで同じ認証設定を使用する必要があります。

[Authentication Settings] (認証設定) ページでは、KX II へのアクセスに使用する認証の種類を設定できます。

注: リモート認証 (LDAP/LDAPS または RADIUS) を選択すると、ユーザが見つからない場合はローカル認証データベースも確認されます。

▶ **認証を設定するには、以下の手順に従います。**

1. [ユーザ管理] の [認証設定] を選択します。[認証設定] ページが開きます。
2. 使用する認証プロトコルのオプションを選択します ([ローカル認証]、[LDAP/LDAPS]、または [RADIUS])。[LDAP] オプションを選択した場合、LDAP に関連するフィールドが有効になります。[RADIUS] オプションを選択した場合、RADIUS に関連するフィールドが有効になります。
3. [ローカル認証] を選択した場合は、手順 6 に進みます。
4. [LDAP/LDAPS] を選択した場合は、「LDAP/LDAPS リモート認証の実装」を参考にして、[認証設定] ページの [LDAP] セクションの各フィールドを指定してください。
5. [RADIUS] を選択した場合は、「RADIUS リモート認証の実装」を参考にして、[認証設定] ページの [RADIUS] セクションの各フィールドを指定してください。
6. [OK] をクリックして保存します。

▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [デフォルトに戻す] をクリックします。

LDAP/LDAPS リモート認証の実装

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクトリ サービスを照会および変更するためのネットワーキング プロトコルです。クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアントは、オペレーション要求をサーバに送信します。サーバは、この要求に対して応答を返します。

メモ: Microsoft Active Directory は、LDAP/LDAPS 認証サーバとしてネイティブに機能します。

LDAP 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [LDAP] (LDAP) ラジオ ボタンを選択して、ページの [LDAP] (LDAP) セクションを有効にします。
3. LDAP アイコンをクリックして、ページの [LDAP] (LDAP) セクションを展開します。

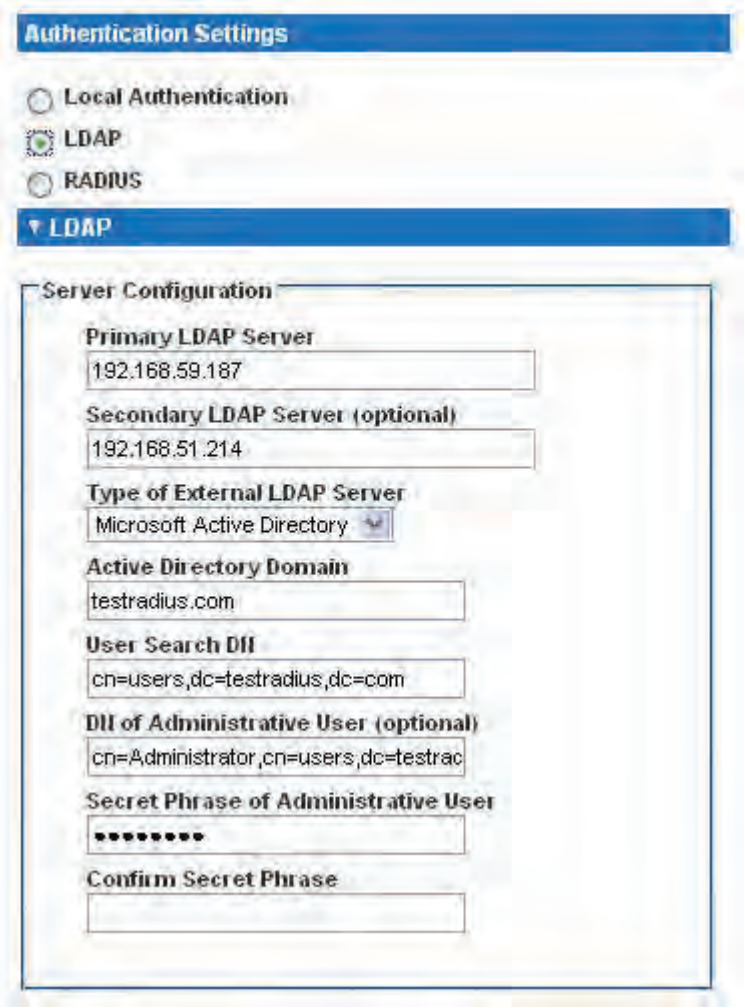
   サーバの設定

4. [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP/LDAPS リモート認証サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにし、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。
5. [Secondary LDAP Server] (セカンダリ LDAP サーバ) フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) オプションをオンにした場合は、DNS 名を使用する必要があります。残りのフィールドについては、[Primary LDAP Server] (プライマリ LDAP サーバ) フィールドの場合と同じ設定を使用します。**(オプション)**
6. [Type of External LDAP Server] (外部 LDAP サーバの種類)。
7. 外部 LDAP/LDAPS サーバを選択します。使用可能なオプションを選択します。
   - [Generic LDAP Server] (一般的な LDAP サーバ)。

- [Microsoft Active Directory]。Active Directory は、Windows 環境向けの Microsoft による LDAP/LDAPS ディレクトリ サービスの実装です。

8. Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。たとえば、*acme.com* などです。特定のドメインの名前については、Active Directive 管理者にお問い合わせください。
9. [User Search DN] (ユーザ検索 DN) フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。最大 64 文字まで使用できます。たとえば、`cn=Users,dc=raritan,dc=com` というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。
10. [DN of administrative User] (管理者ユーザの DN) フィールドに管理者ユーザの識別名を入力します (最大 64 文字)。このフィールドは、LDAP サーバで管理者に管理者ユーザの役割を使用したユーザ情報の検索を許可している場合にのみ入力します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。たとえば、管理者ユーザの DN として、以下のように設定します。
    `cn=Administrator,cn=Users,dc=testradius,dc=com`(オプション)

11. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリモート認証サーバに対して認証するために使用するパスワードを入力する必要があります。[Secret Phrase] (秘密フレーズ) フィールドにパスワードを入力し、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドにパスワードを再入力します (最大 128 文字)。



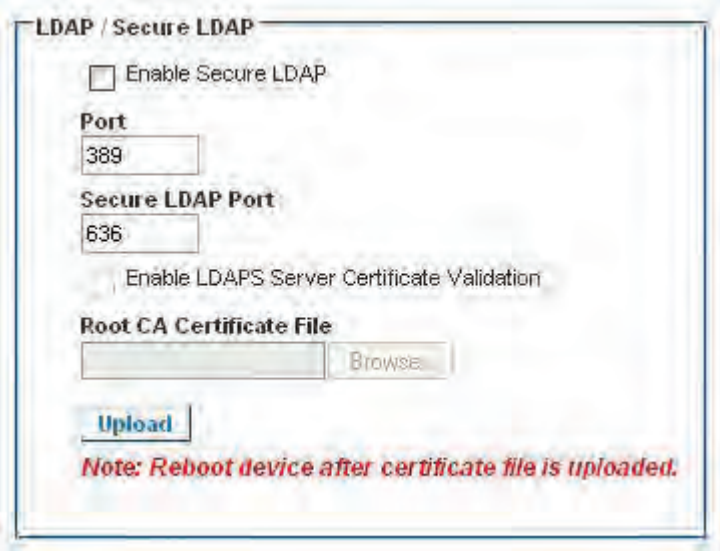
LDAP/LDAP Secure

12. SSL を使用する場合は、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにします。これにより、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスがオンになります。Secure Sockets Layer (SSL) は、KX II が LDAP/LDAPS サーバと安全に通信できるようにする暗号プロトコルです。
13. [Port] (ポート) のデフォルトは 389 です。標準 LDAP TCP ポートを使用するか、または別のポートを指定します。

14. [Secure LDAP Port] (セキュア LDAP ポート) のデフォルトは 636 です。デフォルトのポートを使用するか、または別のポートを指定します。このフィールドは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用します。
15. 前にアップロードしたルート CA 証明書ファイルを使用してサーバから提供された証明書を検証するには、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにします。前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。この機能を無効にすることは、不明な証明機関によって署名された証明書を受け取ることと同じです。このチェックボックスは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用できます。

注: 検証にルート CA 証明書を使用し、さらに [Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにする場合は、サーバ ホスト名がサーバ証明書に記載された共通名と一致する必要があります。

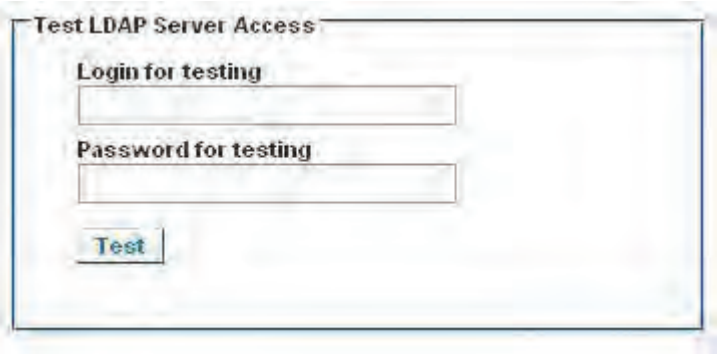
16. 必要な場合は、ルート CA 証明書のファイルをアップロードします。このフィールドは、[セキュア LDAP を有効にする] チェックボックスがオンのときに有効になります。LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせてください。[参照] を使用して証明書ファイルを選択します。LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、新しい証明書を有効にするために KX II を再起動する必要があります。



LDAP サーバ アクセスのテスト

17. LDAP サーバおよび KX II をリモート認証用に正しく構成するために複雑な設定が必要になることがあるので、KX II には、[Authentication Settings] (認証設定) ページから LDAP の設定をテストする機能が用意されています。LDAP の設定をテストするには、[Login for testing] (テスト用ログイン) フィールドと [Password for testing] (テスト用パスワード) フィールドにそれぞれログイン名とパスワードを入力します。これは、KX II にアクセスするときに入力したユーザ名とパスワードです。LDAP サーバはこれを使用してユーザを認証します。[Test] (テスト) をクリックします。

    テストが完了すると、テストが成功したことを知らせるメッセージが表示されます。テストが失敗した場合は、詳細なエラー メッセージが表示されます。成功したことが表示されるか、または失敗した場合は詳細なエラー メッセージが表示されます。成功時には、リモート LDAP サーバから取得されたテスト ユーザのグループ情報も表示されることがあります。



ユーザ グループ情報を Active Directory サーバから返す

KX II では Active Directory® (AD) を使用したユーザ認証がサポートされているので、ユーザを KX II でローカルに定義する必要はありません。これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認可と AD ユーザ特権は、標準の KX II ポリシー、および AD ユーザ グループにローカルに適用されるユーザ グループ特権によって制御および管理されます。

重要: Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、KX II はこの設定をサポートします。この場合、以下に示す手順を実行する必要はありません。AD LDAP/LDAPS スキーマを更新する方法の詳細については、「*LDAP スキーマの更新* 『*384*p. の"*LDAP スキーマを更新する*"参照 』」を参照してください。

▶ KX II で AD サーバを有効にするには、以下の手順に従います。

1. KX II を使用して、特殊なグループを作成し、適切な許可および特権をグループに割り当てます。たとえば、KVM_Admin や KVM_Operator というグループを作成します。
2. Active Directory サーバで、前の手順で作成したのと同じグループ名を持つ新しいグループを作成します。
3. AD サーバ上で、手順 2 で作成したグループに KX II ユーザを割り当てます。
4. KX II で、AD サーバを有効にし、適切に設定します。「*LDAP/LDAPS リモート認証の実装 『160p. 』*」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- KX II には、[管理者] と [<不明>] のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることはできません。Active Directory サーバでこれらと同じグループ名が使用されていないことを確認してください。
- Active Directory サーバから返されたグループ情報が KX II のグループ設定と一致しない場合、正常に認証されたユーザに対して自動的に [<不明>] グループが割り当てられます。
- ダイヤルバック番号を使用する場合は、次の文字列を入力する必要があります。大文字と小文字は区別されます。*msRADIUSCallbackNumber*
- Microsoft からの推奨に基づいて、ドメイン ローカル グループではなく、ユーザ アカウントを含むグローバル グループを使用する必要があります。

RADIUS リモート認証の実装

Remote Authentication Dial-in User Service (RADIUS) は、ネットワーク アクセス アプリケーションのための AAA (認証 (authentication)、認可 (authorization)、アカウンティング (accounting)) プロトコルです。

▶ RADIUS 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [RADIUS] (RADIUS) ラジオ ボタンをクリックして、ページの [RADIUS] (RADIUS) セクションを有効にします。
3. ▶ RADIUS アイコンをクリックして、ページの [RADIUS] (RADIUS) セクションを展開します。

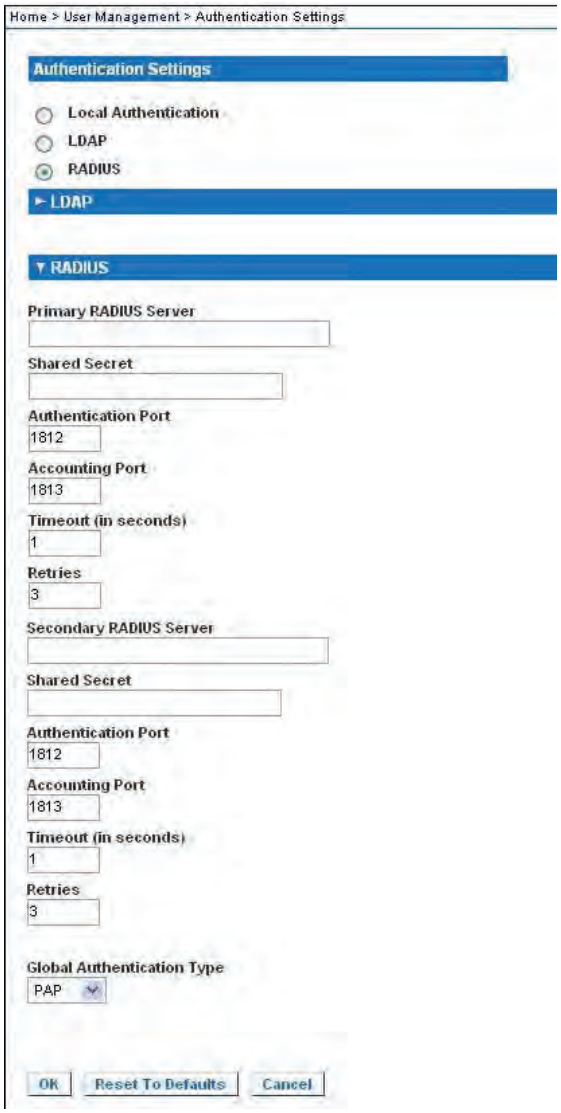
4. [Primary Radius Server] (プライマリ Radius サーバ) フィールドおよび [Secondary Radius Server] (セカンダリ Radius サーバ) フィールドに、プライマリ認証サーバの IP アドレスおよびオプションでセカンダリ認証サーバの IP アドレスを入力します (最大 256 文字)。
5. [Shared Secret] (共有の秘密) フィールドに、認証に使用するサーバの秘密フレーズを入力します (最大 128 文字)。

   共有の秘密とは、KX II と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。
6. [Authentication Port] (認証ポート) のデフォルトは 1812 ですが、必要に応じて変更できます。
7. [Accounting Port] (アカウンティング ポート) のデフォルトは 1813 ですが、必要に応じて変更できます。
8. [Timeout] (タイムアウト) は秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。

   このタイムアウトは、KX II が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。
9. デフォルトの再試行回数は 3 回です。

   これは、KX II が RADIUS サーバに対して認証要求を送信する回数です。
10. ドロップダウン リストのオプションから、適切な [Global Authentication Type] (グローバル認証タイプ) を選択します。
    - [PAP] (PAP) - PAP の場合、パスワードは平文 (ひらぶん) - 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが 1 つのデータ パッケージとして送信されます。

- [CHAP] (CHAP) – CHAP の場合、サーバはいつでも認証を要求できます。CHAP は、PAP よりも高いセキュリティを実現します。



RADIUS 認証用の Cisco ACS 5.x

Cisco ACS 5.x サーバを使用している場合は、KX II に RADIUS 認証を設定した後に、Cisco ACS 5.x サーバで以下の手順を完了する必要があります。

注: 以下の手順には、各ページへのアクセスに使用される Cisco のメニューおよびメニュー項目が含まれます。各手順の最新情報とその実行の詳細については、Cisco のマニュアルを参照してください。

- AAA クライアントとしての KX II の追加（**必須**）– [Network Resources]（ネットワーク リソース）、[Network Device Group]（ネットワーク デバイス グループ）、[Network Device and AAA Clients]（ネットワーク デバイスと AAA クライアント）の順に選択
- ユーザの追加/編集（**必須**）– [Network Resources]（ネットワーク リソース）、[Users and Identity Stores]（ユーザ ストアと ID ストア）、[Internal Identity Stores]（内部 ID ストア）、[Users]（ユーザ）の順に選択
- CHAP プロトコルを有効にするデフォルト ネットワーク アクセスの設定（**オプション**）– [Policies]（ポリシー）、[Access Services]（アクセス サービス）、[Default Network Access]（デフォルト ネットワーク アクセス）の順に選択
- アクセスを制御する認可ポリシー ルールの作成（**必須**）– [Policy Elements]（ポリシー要素）、[Authorization and Permissions]（認可と許可）、[Network Access]（ネットワーク アクセス）、[Authorization Profiles]（認可プロファイル）の順に選択
  - [Dictionary Type]（ディクショナリ タイプ）: RADIUS-IETF
  - [RADIUS Attribute]（RADIUS 属性）: Filter-ID
  - [Attribute Type]（属性タイプ）: String
  - [Attribute Value]（属性値）: Raritan:G{KVM_Admin}（KVM_Admin は Dominion KVM Switch でローカルに作成されたグループ名）。大文字と小文字が区別されます。
- セッション状況（日時）の設定（**必須**）– [Policy Elements]（ポリシー要素）、[Session Conditions]（セッション状況）、[Date and Time]（日時）の順に選択
- ネットワーク アクセス認可ポリシーの設定/作成（**必須**）– [Access Policies]（アクセス ポリシー）、[Access Services]（アクセス サービス）、[Default Network Access]（デフォルト ネットワーク アクセス）、[Authorization]（認可）の順に選択

ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、KX II は、ユーザのグループの許可に基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性を返すことによって、これらのユーザ グループ名を提供できます。FILTER-ID は、Raritan:G{*GROUP_NAME*} という形式となります。*GROUP_NAME* は、ユーザが属するグループの名前を示す文字列です。

```
Raritan:G{GROUP_NAME}:D{Dial Back Number}
```

GROUP_NAME は、ユーザが属するグループの名前を示す文字列です。Dial Back Number は、ユーザ アカウントに関連付けられている番号で、KX II モデムがユーザ アカウントへのダイヤルバックに使用します。

RADIUS 通信交換仕様

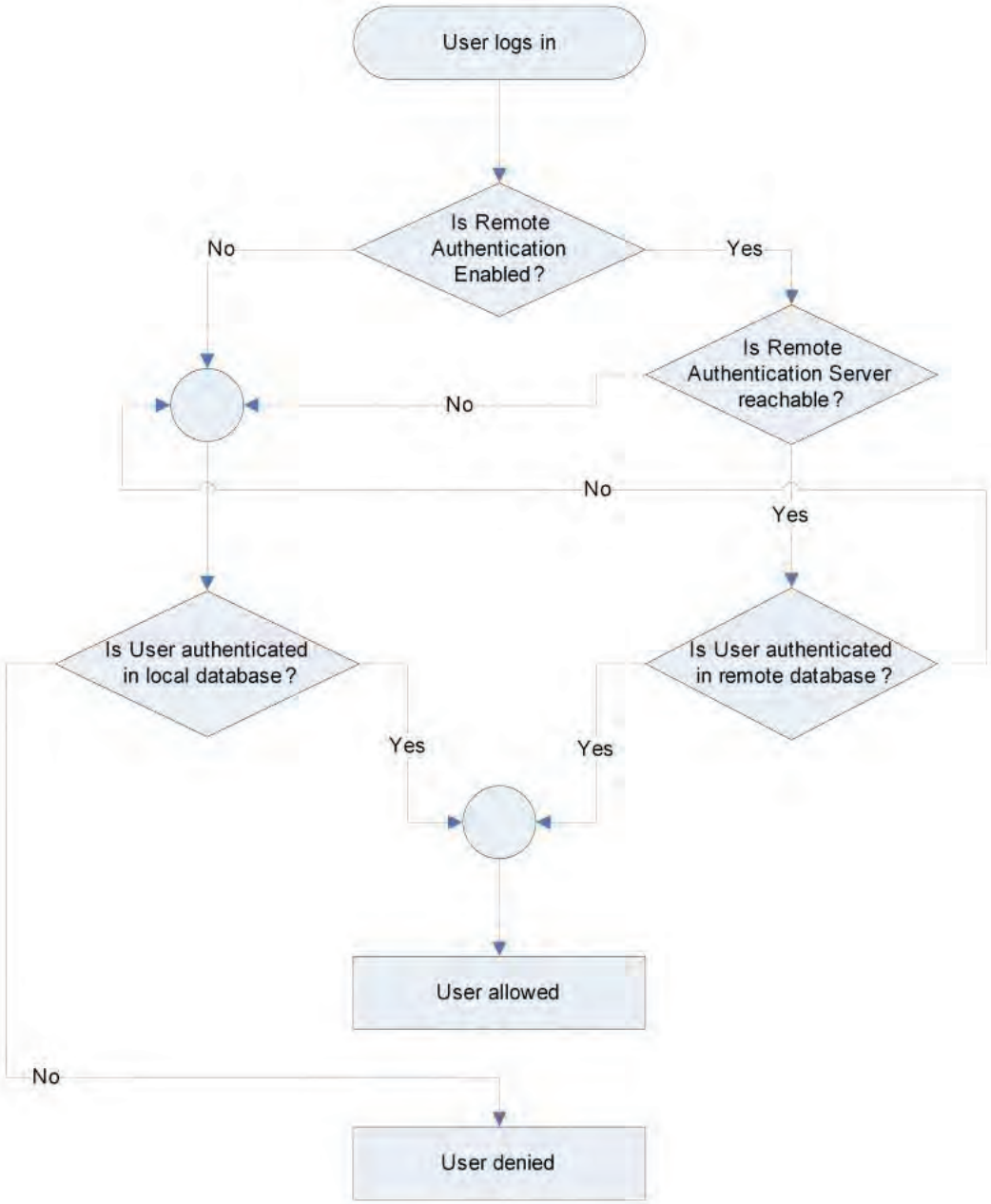
KX II は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	KX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログアウト	
Accounting-Request(4)	

属性	データ
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

ユーザ認証プロセス

リモート認証は、その後のフローチャートに指定されたプロセスに従います。

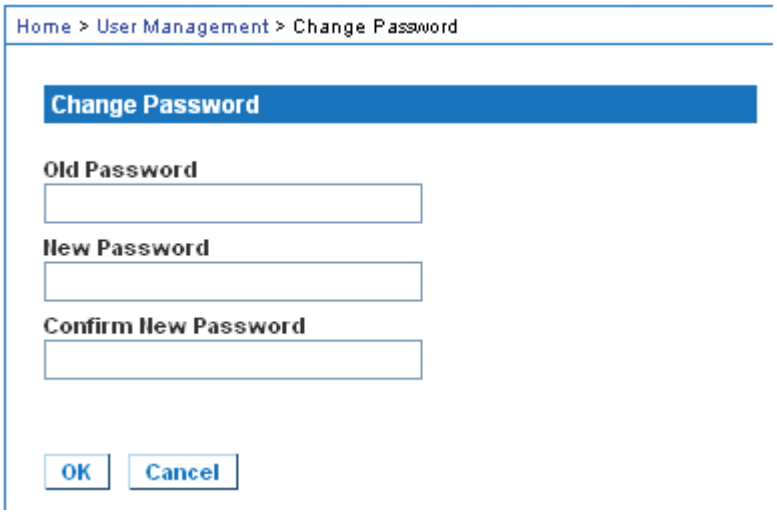


パスワードの変更

▶ パスワードを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Change Password] (パスワードの変更) を選択します。[Change Password] (パスワードの変更) ページが開きます。
2. [Old Password] (旧パスワード) フィールドに現在のパスワードを入力します。
3. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力します。[Confirm New Password] (新しいパスワードの確認) フィールドにパスワードを再入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
4. [OK] (OK) をクリックします。
5. パスワードが正常に変更された旨のメッセージが表示されます。[OK] (OK) をクリックします。

注: 強力なパスワードが使用されている場合は、パスワードに必要な形式に関する情報がこのページに表示されます。パスワードと強力なパスワードについての詳細は、「[Strong Passwords] (強力なパスワード) 『266p. の [強力なパスワード] "参照 』」を参照してください。



Ch 8 デバイス管理

この章の内容

ネットワーク設定 173
[Device Services] (デバイス サービス) 179
[Power Supply Setup] (電源設定) 205
ポートの設定 206
スクリプトの接続と切断 252
ポート グループ管理 258
デフォルトの GUI 言語設定の変更 262

ネットワーク設定

[Network Settings] (ネットワーク設定) ページを使用して、KX II のネットワーク設定 (たとえば、IP アドレス、検出ポート、LAN インタフェースパラメータなど) をカスタマイズします。

IP 設定を行うには 2 つのオプションがあります。

- [None] (なし) (デフォルト) - 推奨されるオプションです (静的 IP)。KX II はネットワーク インフラストラクチャの一部であるため、IP アドレスを頻繁に変更されると手間がかかります。このオプションにより、ネットワーク パラメータを固定できます。
- [DHCP] (DHCP) - DHCP サーバによって IP アドレスが自動的に割り当てられます。

▶ ネットワーク設定を変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. ネットワーク基本設定を更新します。「*ネットワーク基本設定* 『*174*p. 』」を参照してください。
3. LAN インタフェースの設定を更新します。「*LAN インタフェース設定* 『*178*p. 』」を参照してください。
4. [OK] (OK) をクリックして、これらの設定を保存します。変更を適用するために再起動が必要な場合は、再起動メッセージが表示されます。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

ネットワーク基本設定

ここでは、[ネットワーク設定] ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作の詳細については、「*ネットワーク設定* 『*173*p. 』」を参照してください。

▶ IP アドレスを割り当てるには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KX II デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。
   e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。
   - [None] (なし) (静的 IP) – このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

     KX II はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。
   - [DHCP] (DHCP) – DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

     このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。
4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。
   a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。

b. [Global/Unique IP Address]（グローバル/一意の IP アドレス）を入力します。これは、KX II に割り当てられる IP アドレスです。

c. [Prefix Length]（固定長）を入力します。これは、IPv6 アドレスで使用されるビット数です。

d. [Gateway IP Address]（ゲートウェイ IP アドレス）を入力します。

e. [Link-Local IP Address]（リンク - ローカル IP アドレス）。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索で、またはルータが存在しない場合に使用されます。
[Read-Only]（読み取り専用）

f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。[Read-Only]（読み取り専用）

g. [IP Auto Configuration]（IP 自動設定）を選択します。次のオプションを使用できます。

- [None]（設定しない）- 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します（静的 IP）。推奨されるデフォルトのオプションです。

  [IP auto configuration]（IP 自動設定）で [None]（設定しない）を選択すると、[Network Basic Settings]（ネットワーク基本設定）フィールド（[Global/Unique IP Address]（グローバル/一意の IP アドレス）、[Prefix Length]（固定長）、[Gateway IP Address]（ゲートウェイ IP アドレス））が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery]（ルータ検出）- このオプションを使用して、直接接続されるサブネットにのみ適用される [Link Local]（リンクローカル）を超える [Global]（グローバル）または [Unique Local]（一意ローカル）を意味する IPv6 アドレスを自動的に割り当てます。

5. [DHCP] が選択され、[Obtain DNS Server Address]（DNS サーバ アドレスを取得）が有効になっている場合は、[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得）を選択します。[Obtain DNS Server Address Automatically]（DNS サーバ アドレスを自動的に取得）が選択されると、DHCP サーバが提供する DNS 情報が使用されます。

6. [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用）を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバの接続に使用されます。

   [Use the Following DNS Server Addresses]（次の DNS サーバ アドレスを使用）オプションを選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

a. [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)

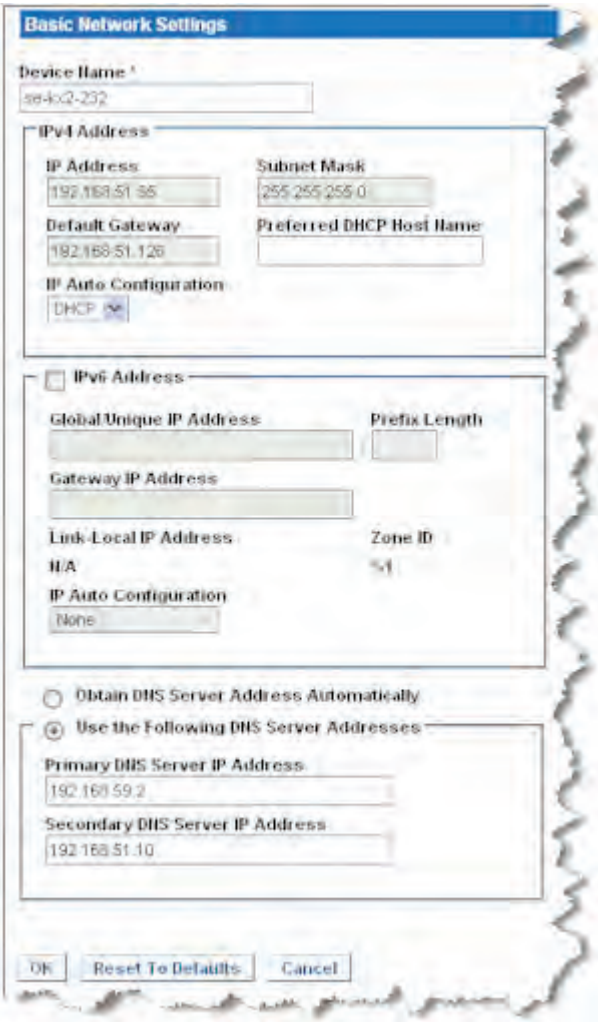
b. [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)

7. 完了したら [OK] をクリックします。

［ネットワーク設定］ページのこのセクションの設定については、「*LAN インタフェース設定* 『*178*p. 』」を参照してください。

---

*注: 一部の環境では、［LAN Interface Speed & Duplex］(LAN インタフェースの速度と二重化) のデフォルトである［Autodetect］(自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、KX II の［LAN Interface Speed & Duplex］(LAN インタフェースの速度と二重化) フィールドを［100 Mbps/Full Duplex］(またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細については、「*ネットワーク設定 『*173*p. 』」を参照してください。*



LAN インタフェース設定

現在のパラメータ設定は、[現在の LAN インタフェース パラメータ] フィールドで確認します。

1. [デバイス設定] の [ネットワーク] を選択します。[ネットワーク設定] ページが開きます。
2. 以下の [LAN インタフェースの速度と二重化] のオプションから適切なものを選択します。
   - [自動検出] (デフォルト オプション)
   - [10 Mbps/半二重]: 両方の LED が点滅
   - [10 Mbps/全二重]: 両方の LED が点滅
   - [100 Mbps/半二重]: 黄色の LED が点滅
   - [100 Mbps/半二重]: 黄色の LED が点滅
   - [1000 Mbps/全二重] (ギガビット): 緑色の LED が点滅
   - [半二重] の場合、双方向の通信は可能ですが、一度に通信できるのは一方向だけです (同時に通信できません)。
   - [全二重] の場合、同時に双方向の通信が可能です。

   注: 半二重または全二重で 10 Mbps で実行しているときに、問題が発生する場合があります。問題が発生した場合は、別の速度と二重化の設定を選択してください。

   詳細については、「*Network Speed Settings* 『*367*p. の*"ネットワーク速度の設定"*参照 』」を参照してください。
3. この [Enable Automatic Failover] (自動フェイルオーバを有効にする) チェックボックスをオンにすると、アクティブなネットワーク ポートに障害が発生した場合、KX II では 2 番目のネットワーク ポートを使用して、自動的にネットワーク接続を回復します。

   注: フェイルオーバ ポートは実際にフェイルオーバが発生するまで有効にならないので、ポートを監視しないか、フェイルオーバが発生した後にのみ監視するようにすることをお勧めします。

   このオプションを有効にすると、次の 2 つのフィールドが使用されます。
   - [Ping Interval (seconds)] (Ping インターバル (秒)) - Ping インターバルの設定により、KX II が指定されたゲートウェイへのネットワーク パスの状態をチェックする頻度が決まります。デフォルトの Ping インターバルは 30 秒です。
   - [Timeout (seconds)] (タイムアウト (秒)) - タイムアウトの設定により、指定されたゲートウェイにネットワーク接続経由でアクセスできなくなってからフェイルオーバが発生するまでの時間が決まります。

注: Ping インターバルとタイムアウトは、ローカル ネットワーク状態に合わせて最適な値に設定できます。タイムアウトは、送信する 2 つ以上の Ping 要求と返される応答に対応できるように設定する必要があります。たとえば、ネットワークの利用率が高いためにフェイルオーバの発生する確率が高い場合は、タイムアウトを Ping インターバルの 3 ～ 4 倍に延ばす必要があります。

4. 帯域幅を選択します。
5. [OK] をクリックして LAN 設定を適用します。

[Device Services] (デバイス サービス)

[デバイス サービス] ページでは、次のことができます。

- SSH アクセスを有効にする。
- ベース KX II に対してカスケード接続を有効にする。
- 検出ポートを入力する。
- ダイレクト ポート アクセスを有効にする。
- AKC を使用している場合に、AKC ダウンロード サーバ証明書の検証を有効にする。

SSH を有効にする

管理者が SSH v2 アプリケーションを使用して KX II にアクセスできるようにするには、[Enable SSH Access] (SSH アクセスを有効にする) チェック ボックスをオンにします。

▶ SSH アクセスを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable SSH Access] (SSH アクセスを有効にする) を選択します。
3. [SSH Port Information] (SSH ポート情報) を入力します。標準の SSH TCP ポート番号は 22 ですが、ポート番号を変更して高いレベルのセキュリティ処理を提供することもできます。
4. [OK] (OK) をクリックします。

HTTP ポートおよび HTTPS ポートの設定

KX II によって使用される HTTP ポートまたは HTTPS ポートを設定できるようになりました。 たとえば、デフォルトの HTTP ポートであるポート 80 を別の用途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

▶ HTTP ポートまたは HTTPS ポートの設定を変更するには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [HTTP Port] (HTTP ポート) フィールドまたは [HTTPS Port] (HTTPS ポート) フィールド (あるいはその両方) に新しいポート番号を入力します。
3. [OK] (OK) をクリックします。

検出ポートを入力する

KX II の検出は、設定可能な 1 つの TCP ポートで行われます。デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう設定してもかまいません。ファイアウォールの外側から KX II にアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

▶ 検出ポートを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Discovery Port] (検出ポート) を入力します。
3. [OK] (OK) をクリックします。

カスケード接続を設定および有効化する

カスケード接続機能を利用した場合、1 台のベース KX II デバイスを介して KX II ターゲットと PDU にアクセスできます。この機能は、標準の KX II のほかに、KX2-808、KX2-832、および KX2-864 で利用できます。

注: ベース デバイスとカスケード接続デバイスはすべて同じファームウェア リビジョンで動作している必要があります。

注: カスケード接続デバイスに接続されているデュアル ビデオ ポートのターゲットには、カスケード接続ベース デバイス以外のカスケード接続デバイスを介して接続する必要があります。「デュアル ビデオ ポート グループの作成」を参照してください。

必要に応じて、カスケード接続構成にデバイスを追加することやカスケード接続構成からデバイスを削除することができます。カスケード接続レベルは最大 2 段階です。

デバイスをセットアップする際、特定のカスケード接続構成に対して特定の CIM を使用します。カスケード接続構成に追加できるターゲット、CIM の互換性、およびデバイス設定情報については、「***カスケード接続: ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成***『*183*p. 』」を参照してください。

カスケード接続デバイスを追加する前に、ベース デバイスおよびカスケード接続デバイスにおいてカスケード接続を有効にする必要があります。ベース デバイスでカスケード接続を有効にするには、[Device Settings] (デバイス設定) ページを使用します。カスケード接続デバイスでカスケード接続を有効にするには、[Local Port Settings] (ローカル ポート設定) ページを使用します。デバイスに対してカスケード接続を有効化および設定すると、そのデバイスが [Port Access] (ポート アクセス) ページに表示されます。

KX II をベース デバイスまたはカスケード接続デバイスとして機能するように設定すると、そのデバイスは次のように表示されます。

- ベース デバイスとして設定した場合、KX II 画面の左パネルの [Device Information] (デバイス情報) セクションに、[Configured As Base Device] (ベース デバイスとして設定) と表示されます。
- カスケード接続デバイスとして設定した場合、KX II 画面の左パネルの [Device Information] (デバイス情報) セクションに、[Configured As Tier Device] (カスケード接続デバイスとして設定) と表示されます。
- ベース デバイスは、カスケード接続デバイスの画面の左パネルの [Connect User] (接続しているユーザ) の下で [Base] (ベース) として表示されます。
- ベース デバイスのカスケード接続ポートに接続しているターゲットは、2 つのポートに接続しているように表示されます。

ベース デバイスからは、[Port Access] (ポート アクセス) ページに表示されている統合ポート リストを使用して、リモート アクセスおよびローカル アクセスできます。カスケード接続デバイスからは、そのデバイスのポート リストを使用してリモート アクセスできます。カスケード接続が有効になっている場合、カスケード接続デバイスからローカル アクセスすることはできません。

CIM 名の変更などのポート設定は、各デバイスから直接行う必要があります。カスケード接続ターゲット ポートの設定は、ベース デバイスから行うことはできません。

カスケード接続構成では、KVM スイッチを使用してサーバを切り替えることもできます。詳細については、「*KVM スイッチを設定する『209*p. 』」を参照してください。

カスケード接続を有効にする

ベース KX II デバイスのターゲット サーバ ポートとカスケード接続 KX II デバイスのローカル アクセス ポート (ビデオ/キーボード/マウス ポート) を、D2CIM-DVUSB で接続します。

カスケード接続デバイスが KX2-808、KX2-832 または KX2-864 である場合は、ベース デバイスのターゲット サーバ ポートと KX2-808/KX2-832/KX2-864 の拡張ローカル ポートを直接接続します。

▶ ティアー接続を有効にするには

1. ティアー接続構成内のベース デバイスで、[Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Services Settings] (デバイス サービス設定) ページが表示されます。
2. [Enable Tiering as Base] (ベースとしてのティアー接続を有効にする) を選択します。
3. [Base Secret] (ベース秘密ワード) フィールドに、ベース デバイスとティアー接続デバイスの間で共有される秘密ワードを入力します。この秘密ワードは、ティアー接続デバイスでベース デバイスを認証する際に必要となります。同じ秘密ワードをティアー接続デバイスに対して入力します。
4. [OK] (OK) をクリックします。
5. ティアー接続デバイスを有効にします。ティアー接続デバイスで、[Device Settings] (デバイス設定) の [Local Port Settings] (ローカル ポート設定) を選択します。
6. このページの [Enable Local Ports] (ローカル ポートを有効にする) セクションで、[Enable Local Port Device Tiering] (ローカル ポート デバイスのティアー接続を有効にする) を選択します。

7. [Tier Secret] (ティアー接続秘密ワード) フィールドに、ベース デバイスの [Device Settings] (デバイス設定) ページで入力したのと同じ秘密ワードを入力します。
8. [OK] (OK) をクリックします。

カスケード接続: ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成

[ブレード シャーシ]

ベース デバイスに直接接続しているブレード シャーシにアクセスできます。

[電源管理]

カスケード接続構成に含まれているターゲットの電源を入れたり切ったりできます。これらのターゲットにアクセスするには、[ポート アクセス] ページを使用します。

KX II、または KX2-808、KX2-832、KX2-864 の各モデルからカスケード接続経由で KX II PDU コンセントにアクセスできます。ターゲットとコンセントが関連付けられている場合、[ポート アクセス] ページで電源を制御できます。ターゲットと PDU コンセントを関連付けることができるのは、両者が同じ KX II に接続されている場合だけです。

ベース KX II またはカスケード接続 KX II に接続されている PDU は、[電源] ページのドロップダウン リストに表示されます。電源タップを選択すると、その統計情報が表示されます。

コンセント レベルも制御できます。具体的に言うと、現在オンになっているコンセントをいったんオフにしてから再度オンにすることができます。ただし、現在オフになっているコンセントをオンにすることはできません。

KX II と KX II または KX2-8xx のローカル ポートを接続する構成 - 互換性のある CIM

ベース KX II を、別の KX II、または KX2-808、KX2-832、KX2-864 の各モデル、および KX II PDU やブレード シャーシにアクセスしてそれらを制御するよう設定する場合に適した CIM は、次のとおりです。

KX II — KX II 構成を使用する場合、D2CIM-DVUSB を使用する必要があります。KX II — KX2-8xx 構成を使用する場合、拡張ローカル ポートしか使用できません。

KX II、および KX2-808、KX2-832、または KX2-864 から成る構成を使用する場合、各デバイスで同じファームウェア バージョンを使用する必要があります。カスケード接続構成の中にブレード シャーシが含まれている場合、各ブレード シャーシは 1 つのターゲット ポートとして数えられます。

カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能

カスケード接続ターゲットでサポートされていない機能は次のとおりです。

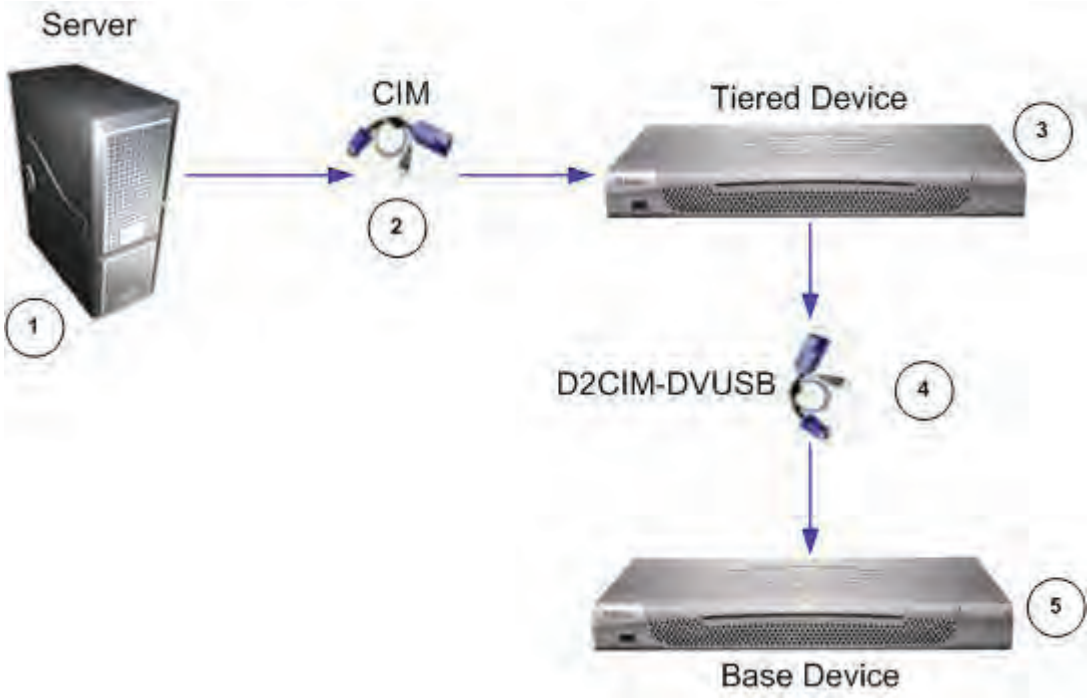
- ブレード シャーシ
- 音声
- カスケード接続デバイスでのスマート カード
- 仮想メディア
- MCCAT

ポート グループ管理機能に制限があります。ベース デバイスに直接接続されているメンバのポート グループしか作成できません。

カスケード接続構成における接続例

次の図に、カスケード接続 KX II デバイスとベース KX II デバイスの接続例を示します。 ベース KX II デバイスのターゲット サーバ ポートとカスケード接続 KX II デバイスのローカル アクセス ポート（ビデオ/キーボード/マウス ポート）を、D2CIM-DVUSB で接続します。

カスケード接続デバイスが KX2-808、KX2-832 または KX2-864 である場合は、ベース デバイスのターゲット サーバ ポートと KX2-808/KX2-832/KX2-864 の拡張ローカル ポートを直接接続します。



図の説明	
1	ターゲット サーバ
2	ターゲット サーバとカスケード接続 KX II デバイスを接続する CIM
3	カスケード接続 KX II デバイス
4	カスケード接続 KX II デバイスとベース KX II デバイスを接続する D2CIM-DVUSB CIM
5	ベース KX II デバイス

URL を経由したダイレクト ポート アクセスの有効化

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login]（ログイン）ダイアログ ボックスと [Port Access]（ポート アクセス）ページを使用する必要がなくなります。この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

ダイレクト ポート アクセスに関する重要な URL 情報は次のとおりです。

VKC とダイレクト ポート アクセスを使用する場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

AKC とダイレクト ポート アクセスを使用する場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

説明:

- username と password はオプションです。指定しない場合はログイン ダイアログ ボックスが表示され、認証後、ユーザはターゲットに直接接続されます。
- port には、ポート番号またはポート名を指定できます。ポート名を使用する場合は、一意の名前にしなければ、エラーが報告されます。port を省略した場合もエラーが報告されます。
- ブレード シャーシの場合、port は「<port number>'-'<slot number>」の形式で指定します。たとえば、ポート 1、スロット 2 に接続されたブレード シャーシの場合は「1-2」のように指定します。
- client=akc は、AKC クライアントを使用しない場合はオプションです。client=akc を指定しない場合、VKC がクライアントとして使用されます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。デュアル ポート ビデオ グループ機能については、「*デュアル ビデオ ポート グループの作成* 『*260*p. 』」を参照してください。

▶ ダイレクト ポート アクセスを有効するには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。

2. URL で必要なパラメータを渡してユーザに Dominion デバイス経由でターゲットに直接アクセスさせる場合は、[Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) を選択します。
3. [OK] をクリックします。

AKC ダウンロード サーバ証明書の検証の有効化

AKC クライアントを使用する場合は、[Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効にする) 機能を使用するかどうかを選択できます。

注: [Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効にする) 機能と共に IPv4 および IPv6 デュアル スタック モードで動作している場合、Microsoft® ClickOnce® では、サーバ証明書 CN に IPv6 アドレスのゼロ圧縮形式を含めてはなりません。ゼロ圧縮形式を含めると、AKC を正常にダウンロードして起動することができなくなります。ただし、これは IPv6 アドレスの形式に対するブラウザの設定と競合する場合があります。共通名 (CN) でサーバのホスト名を使用するか、証明書の「サブジェクトの別名」に IPv6 アドレスの圧縮形式や非圧縮形式を含めてください。

オプション 1: AKC ダウンロード サーバ証明書の検証を有効にしない (デフォルト設定)

AKC ダウンロード サーバ証明書の検証を有効にしない場合は、以下の操作を行います。すべての Dominion デバイス ユーザおよび CC-SG Bookmark and Access Client ユーザは、次のことを行う必要があります。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

オプション 2: AKC ダウンロード サーバ証明書の検証を有効にする

AKC ダウンロード サーバ証明書の検証を有効にする場合は、以下の操作を行います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

▶ Windows Vista® または Windows 7® を使用する場合、自己署名証明書をインストールするには、以下の手順に従います。

1. [信頼済みサイト] ゾーンに KX II の IP アドレスを追加し、保護モードがオフになっていることを確認します。
2. URL に KX II の IP アドレスを使用して Internet Explorer® を起動します。証明書エラー メッセージが表示されます。
3. [証明書の表示] を選択します。

4. [全般] タブで、[証明書のインストール] をクリックします。証明書が信頼されたルート証明機関ストアにインストールされます。
5. 証明書のインストール後、KX II の IP アドレスを [信頼済みサイト] ゾーンから削除する必要があります。

▶ AKC ダウンロード サーバ証明書の検証を有効にするには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [AKC ダウンロード サーバ証明書の検証を有効にする] チェックボックスをオンにします。なお、この機能は無効のままにしておくこともできます (デフォルト設定は無効)。
3. [OK] をクリックします。

SNMP エージェントの設定

SNMP に準拠したデバイスはエージェントと呼ばれます。それ自体のデータは Management Information Base (MIB) に格納され、デバイスはそのデータを SNMP マネージャに返します。KX II の MIB の表示方法については、「*KX II の MIB の表示 『201p.』*」を参照してください。

KX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。

注: 安全な SNMP v3 データは、安全な KX II FIPS から切り離されています。

▶ SNMP エージェントを設定するには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. MIB-II システム グループ オブジェクトに次の SNMP エージェント識別子情報を設定します。
   a. System Name – SNMP エージェントの名前/デバイス名
   b. System Contact – デバイスに関連する連絡先名
   c. System Location – デバイスの場所
3. [Enable SNMP v1/v2c] (SNMP v1/v2c を有効にする) または [Enable SNMP v3] (SNMP v3 を有効にする) を選択するか、その両方を選択します。少なくとも 1 つのオプションを選択する必要があります。**必須。**
4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。

a. Community – デバイスのコミュニティ文字列

b. Community Type – コミュニティ ユーザに読み取り専用または読み書き可能のアクセスを許可

注: SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステータスが所属するグループのことです。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特定するために使用されます。SNMP デバイスまたはエージェントは複数の SNMP コミュニティに所属している場合があります。

---

5. SNMP v3 用の次のフィールドに入力します (必要な場合)。

   a. 必要な場合は、[Use Auth Passphrase] (認証パスフレーズの使用) を選択します。プライバシー パスフレーズが必要な場合は、[Use Auth Passphrase] (認証パスフレーズの使用) により、認証パスフレーズを再入力しなくても、両方に同じパスフレーズを設定できます。

   b. [Security Name] (セキュリティ名) – SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名 (32 文字以内)

   c. [Authentication Protocol] (認証プロトコル) – SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル

   d. [Authentication Passphrase] (認証パスフレーズ) – SNMP v3 エージェントへのアクセスに必要なパスフレーズ (64 文字以内)

   e. [Privacy Protocol] (プライバシー プロトコル) – 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム

   f. [Privacy Passphrase] (プライバシー パスフレーズ) – プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ (64 文字以内)

6. [OK] をクリックすると、SNMP エージェント サービスが開始されます。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

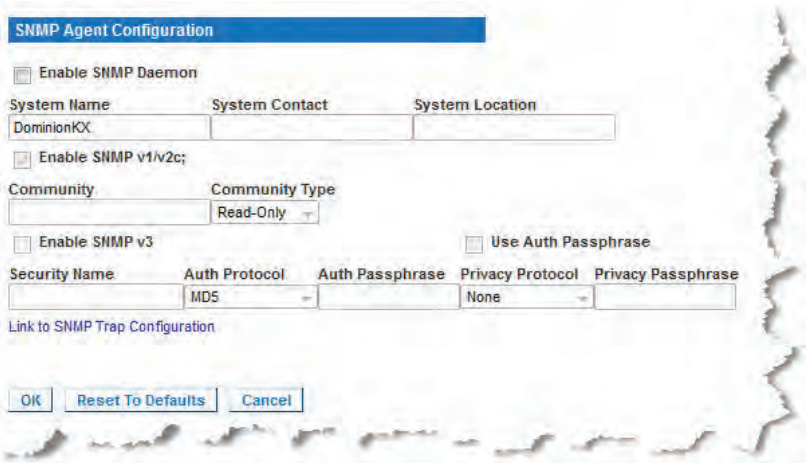
- [Reset to Defaults] (デフォルトに戻す) をクリックします。ページのすべての項目がデフォルト値に戻されます。

[Event Management – Settings] (イベント管理 – 設定) ページで SNMP トラップを設定します。SNMP トラップの作成方法については、「*SNMP トラップの設定 『195p. 』*」を参照し、KX II の使用可能な SNMP トラップの一覧については、「*KX II SNMP トラップのリスト 『198p. 』*」を参照してください。

ヒント: [Link to SNMP Trap Configuration] (SNMP トラップ設定へのリンク) リンクをクリックすると、[Event Management – Settings] (イベント管理 – 設定) ページにすばやく移動できます。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management – Destinations] (イベント管理 – 送信先) ページで選択されます。「*[Event Management – Destinations] (イベント管理 – 送信先) の設定 『203p. 』*」を参照してください。

警告: UDP 経由の SNMP トラップを使用している場合は、KX II を再起動したときに、KX II と接続先のルータが同調できなくなり、SNMP トラップの再起動の完了がログ記録されない可能性があります。



モデムを設定する

▶ モデムを設定するには、以下の手順に従います。

1. [デバイス設定] の [モデム設定] をクリックし、[モデム設定] ページを開きます。
2. [モデムを有効にする] チェックボックスをオンにします。これで、[シリアル ライン速度] フィールドと [モデム Init] フィールドが有効になります。

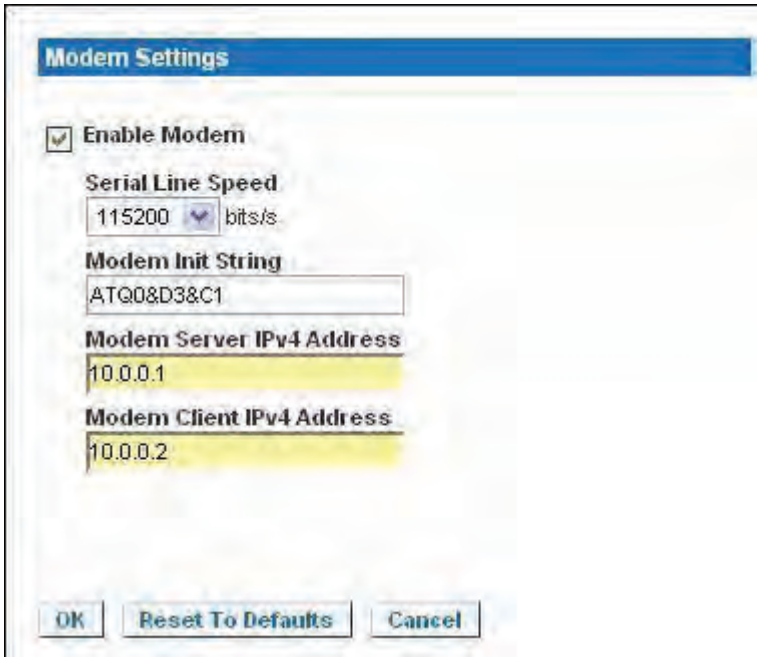
3. モデムの［シリアル ライン速度］は 11520 に設定されます。
4. ［モデム Init 文字列］フィールドにモデム初期化文字列を入力します。モデム文字列を空白のままにすると、デフォルトで、文字列「ATZ OK AT OK」がモデムに送信されます。

   この情報がモデムの設定に使用されます。 以下の値の設定方法はモデムの種類によってさまざまなので、このドキュメントでは、これらの値の設定方法は指定しません。モデム固有の適切な設定を作成するには、モデムを参照する必要があります。

   a. ［モデム設定]:
      - RTS/CTS フロー制御を有効にします。
      - RTS 受信時にコンピュータにデータを送信します。
      - CTS は、必要な場合にフロー制御によって切断だけ行うように設定する必要があります。
      - DTR は、DTR トグルでリセットするようにモデムに対して設定する必要があります。
      - DSR は常にオンに設定する必要があります。
      - DCD は、キャリア信号の検出後に有効にするように設定する必要があります（つまり、DCD はリモート側とのモデム接続が確立されたときにのみ有効にする必要があります)。
5. ［モデム サーバの IPv4 アドレス］フィールドに IPv4 モデム サーバ アドレスを入力し、［モデム クライアントの IPv4 アドレス］フィールドにクライアント モデム アドレスを入力します。

   注: モデム クライアントおよびサーバの IP アドレスは、同じサブネット上にある必要があり、デバイスのサブネットとオーバーラップすることはできません。

6. ［OK］をクリックして変更を確認するか、［デフォルトに戻す］をクリックして設定をデフォルトに戻します。



KX II で使用するに認定済みのモデムの詳細については、「*認定モデム『361*p. 』」を参照してください。モデムを介して KX II に接続する場合の最適なパフォーマンスを確保する設定の詳細については、『KVM and Serial Access Clients Guide』の「Creating, Modifying and Deleting Profiles in MPC – Generation 2 Devices」を参照してください。

注: KX II HTML インタフェースへの直接モデム アクセスはサポートされていません。モデムを介して KX II にアクセスするには、スタンドアロン MPC を使用する必要があります。

日付/時刻の設定

［Date/Time Settings］（日付/時刻の設定）ページを使用して、KX II の日付と時刻を指定します。これには 2 とおりの方法があります。

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル（NTP）サーバと同期する。

▶ 日付と時刻を設定するには、以下の手順に従います。

1. ［デバイス設定］の［日付/時刻］を選択します。［日付/時刻の設定］ページが開きます。
2. ［タイム ゾーン］ドロップダウン リストから適切なタイム ゾーンを選択します。

3. 夏時間用の調整を行うには、[夏時間用の調整] チェックボックスをオンにします。
4. 日付と時刻の設定で用いる方法を選択します。
   - [ユーザによる時刻定義]: 日付と時刻を手動で入力するには、このオプションを選択します。[ユーザによる時刻定義] オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - [NTP サーバと同期]: 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期するには、このオプションを選択します。
5. [NTP サーバと同期] オプションを選択した場合は、以下の手順に従います。
   a. プライマリ タイム サーバの IP アドレスを入力します。
   b. セカンダリ タイム サーバの IP アドレスを入力します。**(オプション)**

[OK] をクリックします。

イベント管理

KX II イベント管理機能によって、SNMP マネージャ、Syslog、監査ログへのシステム イベントの送信を有効または無効にすることができます。これらのイベントはカテゴリ分けされるため、イベントごとに 1 つまたは複数の宛先に送信するかどうかを指定できます。

[Event Management - Settings] (イベント管理 - 設定) の設定

[Event Management - Settings] (イベント管理 - 設定) ページで SNMP トラップおよび syslog を設定します。「*SNMP トラップの設定『195*p. 』」を参照してください。

設定したら、[Event Management - Destinations] (イベント管理 - 送信先) ページで SNMP トラップを有効にします。「*[Event Management - Destinations] (イベント管理 - 送信先) の設定『203*p. 』」を参照してください。

SNMP トラップの設定

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御し、ネットワーク デバイスとその機能を監視するためのプロトコルです。SNMP トラップは、情報を収集するためにネットワーク上に送信されます。SNMP トラップは、[Event Management - Settings] (イベント管理 - 設定) ページで設定されます。KX II SNMP トラップの一覧については、「*KX II SNMP トラップのリスト* 『*198*p. 』」を参照してください。

SNMP に準拠したデバイスは、エージェントと呼ばれ、そのデバイスのデータを Management Information Bases (MIB) に格納し、SNMP トラップに応答します。SNMP エージェントは、[Device Services] (デバイス サービス) ページで設定されます。SNMP エージェントの設定方法については、「*SNMP エージェントの設定* 『*189*p. 』」を参照し、KX II の MIB の表示方法については、「*KX II の MIB の表示* 『*201*p. 』」を参照してください。

SNMP を設定する (SNMP のログ作成を有効にする) には、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。
2. 残りの SNMP フィールドを有効にするには、[SNMP Logging Enabled] (SNMP ログを有効にする) を選択します。**必須。**
3. [SNMP v1/v2c Traps Enabled] (SNMP v1/v2c トラップを有効にする) または [SNMP Trap v3 Enabled] (SNMP Trap v3 トラップを有効にする) を選択するか、その両方を選択します。少なくとも 1 つのオプションを選択する必要があります。選択したら、関連するすべてのフィールドが有効になります。**必須。**
4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。
   a. [Destination IP/Host Name] (送信先 IP/ホスト名) - SNMP マネージャの IP またはホスト名。最大 5 つの SNMP マネージャを作成できます。

   注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

   b. [Port Number] (ポート番号) - SNMP マネージャで使用されるポート番号
   c. Community - デバイスのコミュニティ文字列

   注: SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステータスが所属するグループのことです。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特定するために使用されます。SNMP デバイスまたはエージェントは複数の SNMP コミュニティに所属している場合があります。

5. [SNMP Trap v3 Enabled] (SNMP Trap v3 トラップを有効にする) チェックボックスをまだオンにしていない場合は、オンにすると、次のフィールドが有効になります。SNMP v3 用の次のフィールドに入力します (必要な場合)。
   a. [Destination IP/Host Name] (送信先 IP/ホスト名) - SNMP マネージャの IP またはホスト名。最大 5 つの SNMP マネージャを作成できます。

   注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

   b. [Port Number] (ポート番号) - SNMP マネージャで使用されるポート番号
   c. [Security Name] (セキュリティ名) - SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名 (32 文字以内)
   d. [Authentication Protocol] (認証プロトコル) - SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル
   e. [Authentication Passphrase] (認証パスフレーズ) - SNMP v3 エージェントへのアクセスに必要なパスフレーズ (64 文字以内)
   f. [Privacy Protocol] (プライバシー プロトコル) - 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム
   g. [Privacy Passphrase] (プライバシー パスフレーズ) - プライバシー プロトコル アルゴリズムへのアクセスに使用されるパスフレーズ (64 文字以内)

   注: ローカル コンソールから [Event Management - Settings] (イベント管理 - 設定) ページにアクセスしており、画面解像度を 1280 x 1024 未満にしている場合、このページには [Privacy Passphrase] (プライバシー パスフレーズ) 列が表示されないことがあります。このような場合は、KX II の左パネルを非表示にします。「左パネル 『50p. 』」を参照してください。

6. [OK] をクリックして、SNMP トラップを作成します。

ヒント: [Link to SNMP Agent Configuration] (SNMP エージェント設定へのリンク) リンクを使用すると、[Event Management - Settings] (イベント管理 - 設定) ページから [Devices Services] (デバイス サービス) ページにすばやく移動できます。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management - Destinations] (イベント管理 - 送信先) ページで選択されます。「*[Event Management - Destinations] (イベント管理 - 送信先) の設定* 『*203*p. 』」を参照してください。

KX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およびプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提供します。

注: 安全な SNMP v3 データは、安全な KX II FIPS から切り離されています。

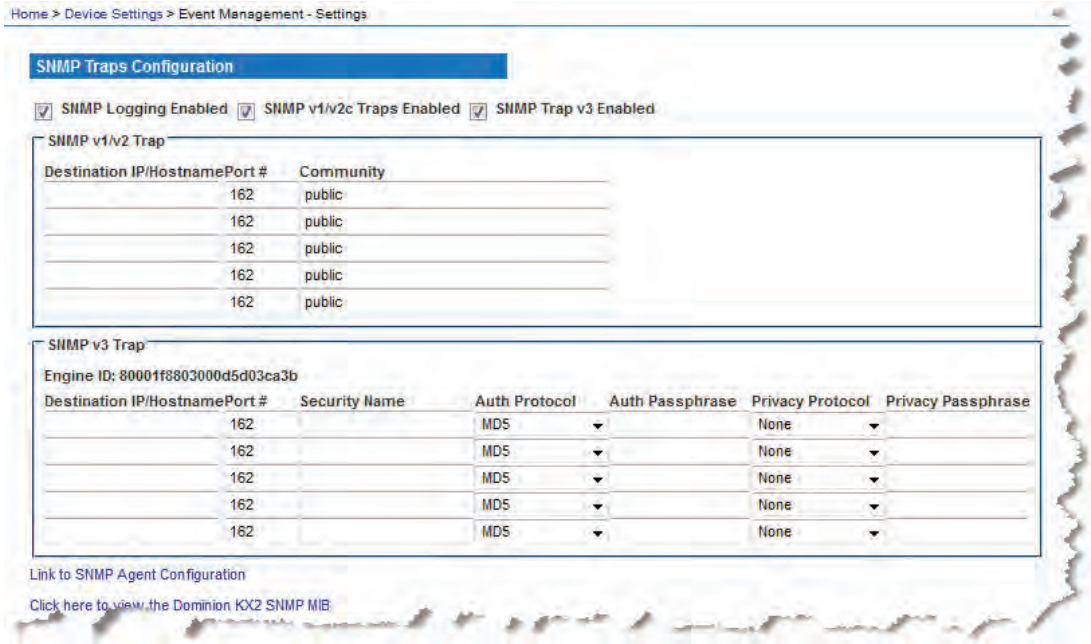
▶ 既存の SNMP トラップを編集するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。
2. 必要に応じて変更し、[OK] をクリックして変更を保存します。

注: どの時点で [SNMP Settings] (SNMP 設定) を無効にしても、SNMP 情報は保持されるので、設定を有効にし直す場合に再入力する必要はありません。

▶ SNMP トラップを削除するには、以下の手順に従います。

- SNMP トラップ フィールドをすべてクリアして保存します。



出荷時のデフォルトにリセットする機能を使用して、SNMP 設定を削除し、KX II を最初の出荷時のデフォルトに設定します。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

警告: UDP 経由の SNMP トラップを使用している場合は、KX II を再起動したときに、KX II と接続先のルータが同調できなくなり、SNMP トラップの再起動の完了がログ記録されない可能性があります。

KX II SNMP トラップのリスト

SNMP によって、トラップまたは通知を送信する機能と、1 つ以上の条件が満たされた場合に管理者に忠告する機能が提供されます。KX II のトラップを次の表に示します。

トラップ名	説明
bladeChassisCommError	このポートに接続されているブレード シャーシ デバイスで通信エラーが検出されました。

トラップ名	説明
	注: KX II-101 および LX ではサポートされていません。
cimConnected	CIM は接続されています。
cimDisconnected	CIM は切断されています。
cimUpdateStarted	CIM の更新が開始されています。
cimUpdateCompleted	CIM の更新が完了しました。
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定はリストアされました。
deviceUpdateFailed	デバイスの更新に失敗しました。
deviceUpgradeCompleted	RFP ファイルを使用した KX II のアップデートが完了しました。
deviceUpgradeStarted	RFP ファイルを使用した KX II のアップデートが開始されました。
factoryReset	デバイスが工場出荷時のデフォルトにリセットされました。
firmwareFileDiscarded	ファームウェア ファイルが破棄されました。
firmwareUpdateFailed	ファームウェアを更新できませんでした。
firmwareValidationFailed	ファームウェアの検証に失敗しました。
groupAdded	グループが KX II システムに追加されました。
groupDeleted	グループがシステムから削除されました。
groupModified	グループが変更されました。
ipConflictDetected	IP アドレスの競合が検出されました。
ipConflictResolved	IP アドレスの競合が解決されました。
networkFailure	製品の Ethernet インタフェースがネットワーク経由で通信できなくなりました。
networkParameterChanged	ネットワーク パラメータに変更が加えられました。
networkParameterChangedv2	KX II-101-V2 ネットワーク パラメータに変更が加えられました。
passwordSettingsChanged	強力なパスワードの設定が変更されました。
portConnect	以前認証されたユーザが KVM セッションを開始

トラップ名	説明
	しました。
portConnectv2	以前認証された KX II-101-V2 ユーザが KVM セッションを開始しました。
portConnectionDenied	ターゲット ポートへの接続が拒否されました。
portDisconnect	KVM セッションを実行中のユーザが正常にセッションを終了しました。
portDisconnectv2	KVM セッションを実行中の KX II-101-V2 ユーザが正常にセッションを終了しました。
portStatusChange	ポートが使用不可能な状態になっています。
powerNotification	電源コンセントの状態の通知です。1: アクティブ、0: 非アクティブ
powerOutletNotification	電源タップ デバイスのコンセントの状態の通知です。
rebootCompleted	KX II の再起動が完了しました。
rebootStarted	システムへの電源の入れ直しまたは OS からのウォーム起動により、KX II は再起動を開始しました。
scanStarted	ターゲット サーバのスキャンが開始されました。
scanStopped	ターゲット サーバのスキャンが停止されました。
securityBannerAction	セキュリティ バナーが承諾または拒否されました。
securityBannerChanged	セキュリティ バナーに変更が加えられました。
securityViolation	セキュリティ違反です。
setDateTime	デバイスの日付と時刻が設定されました。
setFIPSMode	FIPS モードが有効になりました。 *注: FIPS は LX ではサポートされていません。*
startCCManagement	デバイスが CommandCenter の管理下におかれました。
stopCCManagement	デバイスが CommandCenter の管理下から除外されました。
userAdded	ユーザ アカウントがシステムに追加されました。
userAuthenticationFailure	不正なユーザ名または/およびパスワードでのログ

トラップ名	説明
	イン試行がありました。
userConnectionLost	あるユーザのアクティブ セッションが、タイムアウトにより異常終了しました。
userDeleted	ユーザ アカウントが削除されました。
userForcedLogout	ユーザは管理者によって強制的にログアウトされました。
userLogin	ユーザが KX II へ正常にログインし、認証されました。
userLogout	ユーザが KX II から正常にログアウトしました。
userModified	ユーザ アカウントが変更されました。
userPasswordChanged	デバイスのいずれかのユーザのパスワードが変更されると、このイベントが発生します。
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了しました。
userUploadedCertificate	ユーザが SSL 証明書をアップロードしました。
vmImageConnected	ユーザが仮想メディアを使用してターゲットにデバイスまたはイメージのマウントを試みました。デバイスまたはイメージのマッピング（マウント）が試行されるたびに、このイベントが生成されます。
vmImageDisconnected	ユーザが仮想メディアを使用してターゲットからデバイスまたはイメージのマウント解除を試みました。

KX II の MIB の表示

▶ **KX II の MIB を表示するには、以下の手順に従います。**

1. [Device Settings]（デバイス設定）の [Event Management - Settings]（イベント管理 - 設定）を選択します。[Event Management - Settings]（イベント管理 - 設定）ページが開きます。
2. [Click here to view the Dominion KX2 SNMP MIB]（Dominion KX2 SNMP MIB を表示するにはここをクリックします）リンクをクリックします。ブラウザ ウィンドウで MIB ファイルが開きます。

注: MIB ファイルに対して読み書き可能な場合は、MIB エディタを使用してファイルに変更を加えます。

```
-- This is a common MIB for Dominion KX/KSX G1 and KX/KSX G2 and LX traps

-- 12/20/11 H.
-- notifications updated
-- Added new traps for userDisconnectedFromPort

-- 07/08/11 H.
-- Corrected description for portStatusChange

-- 12/20/10 H.
-- notifications updated
-- Added new traps for scanStarted, scanStopped
-- Also added defn for portList

-- 03/09/10 H.
-- notifications updated
-- Added new traps for securityBannerChanged, securityBannerAction
-- Also added defn for bannerChanges, bannerAction

-- 09/08/09 H.
-- notifications updated
-- Added new traps for setDateTime, setFIPSMode
-- Also added defn for sysDateAndTime, fipsModeStatus

-- 10/14/08 H.
-- notifications updated
-- Added new traps for userForcedLogout, userUploadedCertificate
-- and bladeChassisCommError
-- Also added defn for certificateAuthorityName
```

syslog 設定

▶ Syslog を設定する (Syslog の送信を有効にする) には、以下の手順に従います。

1. [Enable Syslog Forwarding] (Syslog 送信有効) を選択して、リモート Syslog サーバにデバイス メッセージのログを送信します。
2. [IP Address] (IP アドレス) フィールドに Syslog サーバの IP アドレスまたはホスト名を入力します。
3. [OK] (OK) をクリックします。

注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

出荷時のデフォルトにリセットする機能を使用して、syslog 設定を削除し、KX II を最初の出荷時のデフォルトに設定します。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

1. [Reset to Defaults] (デフォルトに戻す) をクリックします。

[Event Management - Destinations] (イベント管理 - 送信先) の設定

システム イベントを有効にすると、SNMP 通知イベント（トラップ）を生成できます。また、システム イベントを Syslog または監査ログにログ記録できます。[Event Management – Destinations]（イベント管理 – 送信先）ページを使用して、追跡するイベントと、その情報の送信先を選択します。

注: SNMP トラップは、[SNMP Logging Enabled]（SNMP ログを有効にする）オプションが選択されている場合にのみ生成されます。一方、Syslog イベントは、[Enable Syslog Forwarding]（Syslog 送信有効）オプションが選択されている場合にのみ生成されます。これらのオプションは、いずれも [Event Management – Settings]（イベント管理 – 設定）ページで設定します。 /[Event Management – Settings]（イベント管理 – 設定）の設定 *『*194*p. 』」を参照してください。*

▶ イベントとその送信先を選択するには、以下の手順に従います。

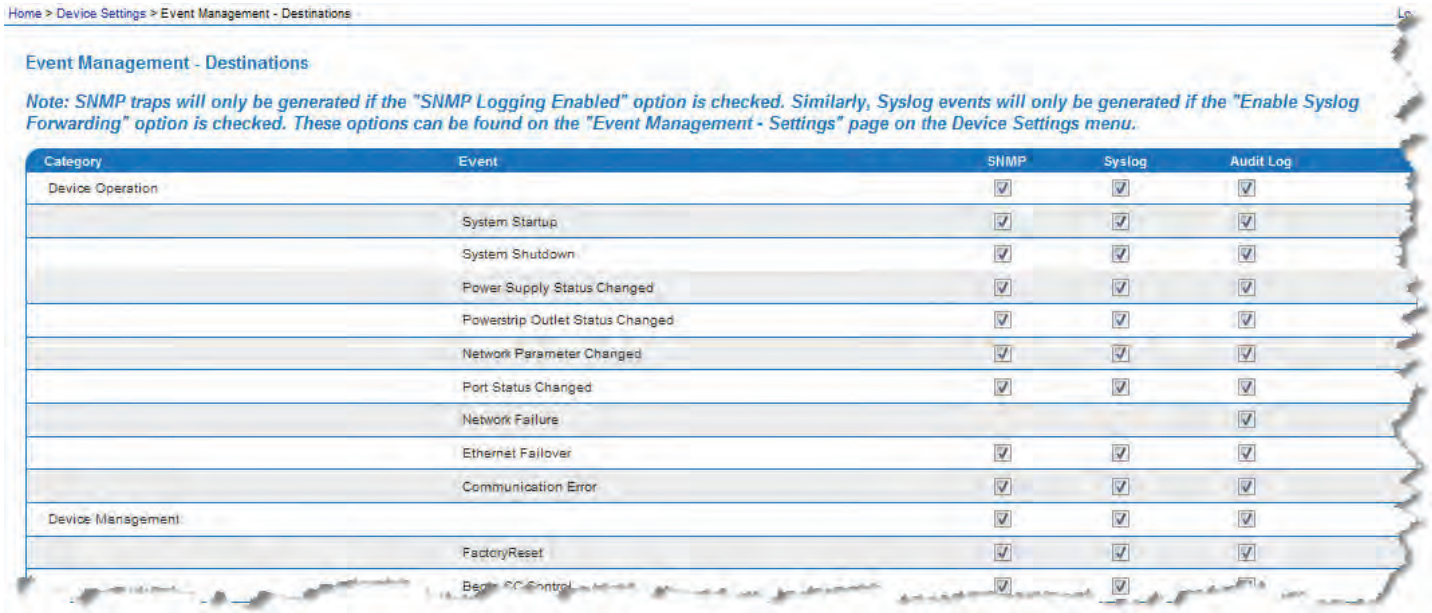
1. [Device Settings]（デバイス設定）の [Event Management – Destinations]（イベント管理 – 送信先）を選択します。[Event Management – Destinations]（イベント管理 – 送信先）ページが開きます。

   システム イベントは、デバイス操作、デバイス管理、セキュリティ、ユーザ アクティビティ、ユーザ グループ管理に分類されます。

2. 有効または無効にする [Event]（イベント）ラインのアイテムと、情報の送信先のチェックボックスをオンにします。

   ヒント: [Category]（カテゴリ）のチェックボックスをそれぞれオンまたはオフにすると、カテゴリ全体を有効または無効に設定できます。

3. [OK] (OK) をクリックします。



▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

警告: UDP 経由の SNMP トラップを使用している場合は、KX II を再起動したときに、KX II と接続先のルータが同調できなくなり、SNMP トラップの再起動の完了がログ記録されない可能性があります。

[Power Supply Setup] (電源設定)

KX II にはデュアル電源が搭載されており、これらの電源の状態を検出し、通知できます。[Power Supply Setup] (電源設定) ページを使用して、片方の電源を使用しているのか、それとも両方の電源を使用しているのかを指定します。正しく設定することで、電源に障害が発生した場合に KX II によって適切な通知が送信されます。たとえば、1 番目の電源に障害が発生した場合は、ユニットの正面の電源 LED が赤色に変わります。

▶ 使用中の電源の自動検出を有効にするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Power Supply Setup] (電源設定) を選択します。[Power Supply Setup] (電源設定) ページが開きます。

2. 電源入力を 1 番目の電源 (ユニット背面の左端の電源) に接続している場合は、[PowerIn1 Auto Detect] (PowerIn1 自動検出) チェックボックスをオンにします。
3. 電源入力を 2 番目の電源 (ユニット背面の右端の電源) に接続している場合は、[PowerIn2 Auto Detect] (PowerIn2 自動検出) チェックボックスをオンにします。
4. [OK] (OK) をクリックします。

注: これらのチェックボックスのいずれかをオンにしたにもかかわらず、電源入力が実際には接続されていない場合は、ユニット前面の電源 LED が赤色で点灯します。

▶ **自動検出を無効にするには、以下の手順に従います。**

- 該当する電源のチェックボックスをオフにします。

▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

注: KX II では、CommandCenter に対して電源状態の報告を行いません。ただし、Dominion I (第 1 世代) では、CommandCenter に対して電源状態の報告を行います。

ポートの設定

[Port Configuration] (ポート設定) ページには、KX II のポートの一覧が表示されます。KVM ターゲット サーバ (ブレード サーバおよび標準サーバ) およびラック PDU (電源タップ) に接続されているポートは青色で表示され、編集できます。CIM が接続されていないポート、または CIM 名が空白のポートについては、デフォルトのポート名 Dominion-KX2_Port# が割り当てられます。「Port#」は KX II の物理ポートの番号を表します。

ポートのステータスがダウンである場合、ステータスとして「使用不可」が表示されます。ポートの CIM が削除されているか電源が切られている場合、ポートがダウンになる可能性があります。

注: ブレード シャーシの場合、ブレード シャーシ名は変更できますが、そのブレード スロット名は変更できません。

ポートの名前を変更した後でも、[Reset to Default] (デフォルトに戻す) 機能を使用すれば、いつでもデフォルトのポート名に戻ります。ポート名をデフォルトにリセットすると、既存の電源の関連付けが削除され、さらにポートがポート グループに含まれている場合は、そのグループから削除されます。

▶ **ポート設定にアクセスするには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。

   最初このページはポートの番号順に表示されますが、列の見出しをクリックしてフィールドごとに並べ替えられます。

   - [Port Number] (ポート番号) - 1 から KX II デバイスで使用できるポートの合計数までの番号が振られています。
   - [Port Name] (ポート名) - ポートに割り当てられている名前です。

または、現在 CIM を介して KX II に接続されていないため [Not Available] (使用不可) ステータスになっているポートの名前を変更します。[Not Available] (使用不可) ステータスのポートの名前を変更するには、以下のいずれかの手順に従います。

- ポートの名前を変更します。CIM が接続されると、その CIM 名が使用されます。
- ポート名を変更し、[Persist name on Next CIM Insertion] (次回の CIM 挿入時に名前を維持) を選択します。CIM が接続されると、割り当てられている名前が CIM にコピーされます。
- [Reset to Defaults] (デフォルトに戻す) を選択して、ポート (名前を含む) を工場出荷時のデフォルトに戻します。CIM が接続されると、その CIM 名が使用されます。

注: ポート (CIM) 名にアポストロフィ (" ' ") を使用することはできません。

- [Port Type] (ポート タイプ):
  - [DCIM] (DCIM) - Dominion CIM
  - [Not Available] (使用不可) - CIM の接続不可
  - [MCUTP] (MCUTP) - マスタ コンソール MCUTP、ケーブル内の CIM
  - [PCIM] (PCIM) - Paragon CIM
  - [PowerStrip (rack PDU)] (電源タップ (ラック PDU)) - 電源タップを接続済み
  - [Dual - VM] (デュアル - VM) - 仮想メディア CIM (D2CIM-VUSB および D2CIM-DVUSB)
  - [Blade Chassis] (ブレード シャーシ) - ブレード シャーシとそのシャーシに関連付けられているブレード (階層順に表示)
  - [KVM Switch] (KVM スイッチ) - 汎用 KVM スイッチ接続
  - [DVM-DP] (DVM-DP) - 表示ポート
  - [DVM-HDMI] (DVM-HDMI) - HDMI CIM
  - [DVM-DVI] (DVM-DVI) - DVI CIM

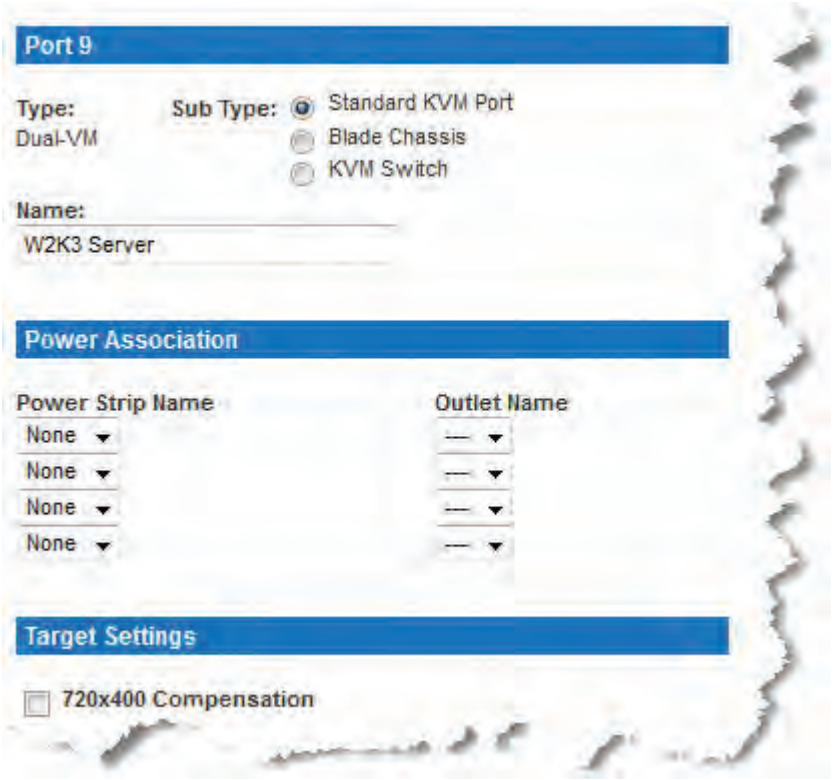
2. 編集するポートの [Port Name] (ポート名) をクリックします。
   - KVM ポートについては、KVM およびブレード シャーシ ポートの [Port] (ポート) ページが開きます。
   - ラック PDU については、ラック PDU (電源タップ) の [Port] (ポート) ページが開きます。このページで、ラック PDU とそれらのコンセントに名前を付けられます。

標準ターゲット サーバの設定

▶ ターゲット サーバに名前を付けるには、以下の手順に従います。

1. まだすべてのターゲット サーバを接続していない場合は、接続します。装置の接続方法の詳細は、「*手順 3: 装置の接続 『32p. 』*」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
3. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
4. ポートのサブタイプとして [標準 KVM ポート] を選択します。
5. 当該ポートに接続されているサーバを識別するための名前を割り当てます。名前には最大 32 文字の英数字と特殊文字を使用できます。
6. 必要な場合は、[Power Association] (電源の関連付け) セクションで、電源タップをポートに関連付けます。
7. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
8. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

9. [OK] (OK) をクリックします。



KVM スイッチを設定する

KX II では、ホット キー シーケンスを使用してターゲットを切り替えることもできます。ホット キー シーケンスを使用して標準サーバを切り替えることができるだけでなく、ブレード シャーシに対しても、また、カスケード接続構成でも KVM 切り替えが可能です。

重要: 作成する KVM スイッチがユーザ グループに表示されるようにするには、まずスイッチを作成してから、グループを作成する必要があります。作成中の KVM スイッチが既存のユーザ グループに表示されるようにする必要がある場合は、ユーザ グループを再作成する必要があります。

▶ KVM スイッチを設定するには

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
3. [KVM Switch] (KVM スイッチ) を選択します。
4. KVM スイッチのモデルを選択します。

注: ドロップダウン リストにはスイッチが 1 つしか表示されません。

5. [KVM Switch Hot Key Sequence] (KVM 切り替えホット キー シーケンス) を選択します。
6. ターゲット ポートの最大数を 2 ～ 32 の範囲で入力します。
7. [KVM Switch Name] (KVM スイッチ名) フィールドに、このポート接続を参照する際に使用する名前を入力します。
8. KVM スイッチ ホット キー シーケンスを適用するターゲットをアクティブ化します。KVM スイッチ ポートにターゲットが接続されていることを示すため、各ポートに対して [Active] (アクティブ) を選択します。
9. このページの [KVM Managed Links] (KVM 管理下リンク) セクションで、Web ブラウザ インタフェースを使用できる場合にその Web ブラウザ インタフェースへの接続を設定できます。
   a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL Name] (URL 名) - インタフェースの URL を入力します。
   c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。
   e. [Username Field] (ユーザ名フィールド) - URL で使用されるユーザ名パラメータを入力します。たとえば、「*username*=admin」と入力します。*username* はユーザ名フィールドです。
   f. [Password Field] (パスワード フィールド) - URL で使用されるパスワード パラメータを入力します。たとえば、「*passname*=raritan」と入力します。*passname* はパスワード フィールドです。
10. [OK] (OK) をクリックします。

▶ KVM スイッチ ポートまたは URL のアクティブ ステータスを変更するには

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。

2. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
3. KVM スイッチ ターゲット ポートまたは URL の [Active] (アクティブ) チェック ボックスをオフにし、アクティブ ステータスを変更します。
4. [OK] (OK) をクリックします。

CIM ポートの設定

KX II では、標準の CIM およびデジタル CIM を使用して、サーバを KX II に接続できます。

▶ CIM を設定するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 名前を変更するターゲット サーバのポート名をクリックします。[Port] (ポート) ページが開きます。
3. ポートのサブタイプとして [標準 KVM ポート] を選択します。
4. 当該ポートに接続されているサーバを識別するための名前を割り当てます。名前には最大 32 文字の英数字と特殊文字を使用できます。
5. 必要な場合は、[Power Association] (電源の関連付け) セクションで、電源タップをポートに関連付けます。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. デジタル CIM の場合、モニタ本来のターゲットの表示解像度に合わせて解像度を設定するには、[Display Native Resolution] (本来の表示解像度) ドロップダウンから解像度を選択します。これは、
8. HDMI CIM を使用している場合、オペレーティング システムとビデオ カードの組み合わせによっては、RGB 値の範囲が限られることがあります。[DVI Compatibility Mode] (DVI 互換モード) チェックボックスをオンにすると、色の範囲が拡大されます。
9. [OK] (OK) をクリックします。

ラック PDU (電源タップ) ターゲットの設定

KX II では、ラック PDU (電源タップ) を KX II ポートに接続できます。KX II のラック PDU の設定は、KX II の [Port Configuration (ポート設定)] ページから行います。

ラック PDU の接続

Raritan PX シリーズのラック PDU（電源タップ）は D2CIM-PWR CIM を使用して Dominion デバイスに接続されます。

▶ **ラック PDU を接続するには、次の手順に従います。**

1. D2CIM-PWR の RJ-45（オス）を、ラック PDU のシリアル ポートの RJ-45（メス）コネクタに接続します。
2. D2CIM-PWR の RJ-45（メス）コネクタを、Cat5 ストレート ケーブルで KX II の使用できるいずれかのシステム ポートのメス コネクタに接続します。
3. AC 電源コードをターゲット サーバと空いているラック PDU アウトレット（コンセント）に接続します。
4. ラック PDU を AC 電源に接続します。
5. デバイスの電源をオンにします。

ラック PDU の名前の指定 (電源タップの [Port] (ポート) ページ)

注: PX ラック PDU (電源タップ) の名前は、PX および KX II で指定できます。

Raritan リモート ラック PDU が KX II に接続されると、それが [Port Configuration (ポート設定)] ページに表示されます。そのページにある電源ポート名をクリックしてアクセスします。[Type (タイプ)] および [Name (名前)] フィールドはあらかじめ指定されています。

注: (CIM) タイプは変更できません。

ラック PDU の各アウトレット (コンセント) に関する次の情報が表示されます。コンセントの [Number (番号)]、[Name (名前)]、[Port Association (ポートの関連付け)]。

このページを使用して、ラック PDU とそのアウトレット (コンセント) に名前を付けます。名前には最大 32 文字の英数字が使用でき、特殊文字を含めることができます。

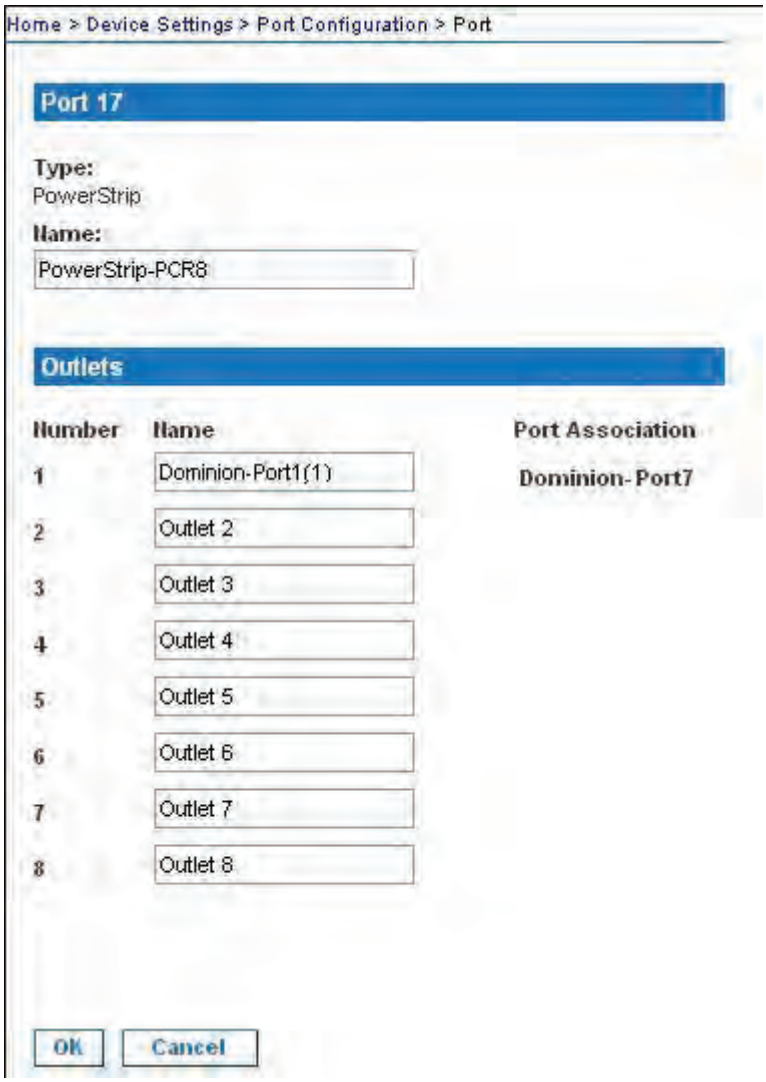
注: ラック PDU がターゲット サーバ (ポート) と関連付けられると、アウトレット (コンセント) 名はターゲット サーバ名に置き換えられます。アウトレット (コンセント) に別の名前を割り当てている場合も同様です。

▶ ラック PDU とアウトレット (コンセント) に名前を付けるには、次の手順に従います。

注: CommandCenter Secure Gateway では、スペースを含むラック PDU 名を認識できません。

1. ラック PDU の名前を入力します (必要な場合)。
2. 必要に応じて、([アウトレット (コンセント)]) [Name (名前)] を変更します。(アウトレット (コンセント) 名は「outlet #」です。)

3. ［OK］をクリックします。



コンセントとターゲット サーバとの関連付け

[Port Configuration (ポート設定)] ページでポートをクリックすると、[Port (ポート)] ページが開きます。このページで電源の関連付けを行えます。ポートの名前を入力しやすい名前に変更し、D2CIM-VUSB CIM を使用している場合はターゲット サーバの設定を更新します。(CIM) [Type (タイプ)] および (ポート) [Name (名前)] フィールドはあらかじめ指定されています。CIM タイプは変更できないことに注意してください。

サーバには最大で 4 つの電源プラグを接続でき、それぞれに別のラック PDU (電源タップ) を関連付けられます。このページでそれらの関連付けを定義して、[Port Access (ポート アクセス)] ページからサーバの電源オン、オフ、再投入を行えます。

この機能を使用するには、以下が必要です。

- Raritan リモート ラック PDU
- Power CIM (D2CIM-PWR)

▶ 電源の関連付けを行う (ラック PDU コンセントを KVM ターゲット サーバに関連付ける) には、以下の手順に従います。

注: ラック PDU がターゲット サーバ (ポート) に関連付けられると、アウトレット (コンセント) 名はターゲット サーバ名に置き換えられます (アウトレット (コンセント) に別の名前を割り当てている場合も同様です)。

---

1. [Power Strip Name (電源タップ名)] ドロップダウン リストからラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name (アウトレット (コンセント) 名)] ドロップダウン リストからアウトレット (コンセント) を選択します。
3. 該当するすべての電源の関連付けで、手順 1 および 2 を繰り返します。
4. [OK] をクリックします。確認メッセージが表示されます。

▶ ポート名を変更するには、次の手順に従います。

1. [Name (名前)] フィールドにわかりやすい名前を入力します。候補としてはターゲット サーバ名が挙げられます。名前には最大 32 文字の英数字が使用でき、特殊文字を含めることができます。
2. [OK] をクリックします。

電源の関連付けの削除

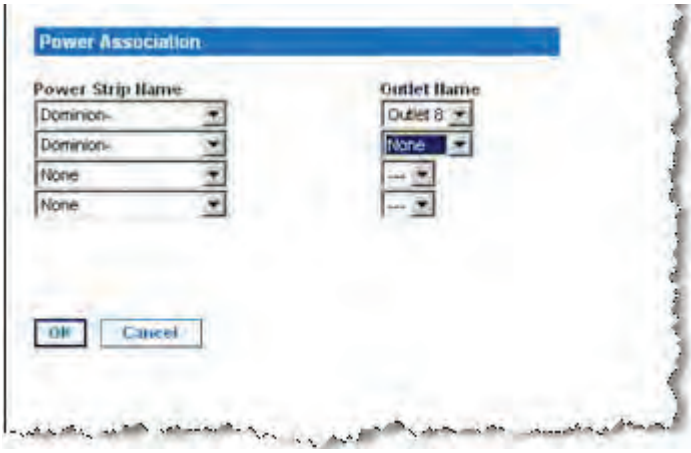
ターゲット サーバまたはラック PDU をデバイスから取り外す場合は、まずすべての電源の関連付けを削除する必要があります。ターゲットがラック PDU に関連付けられたままでターゲットをデバイスから取り外した場合、電源の関連付けは残ります。この場合、電源の関連付けを適切に削除するために [Device Settings (デバイス設定)] で切断されたターゲット サーバの [Port Configuration (ポート設定)] にアクセスすることはできません。

▶ ラック PDU の関連付けを削除するには、次の手順に従います。

1. [Power Strip Name (電源タップ名)] ドロップダウン リストから適切なラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name (アウトレット (コンセント) 名)] ドロップダウン リストから適切なアウトレット (コンセント) を選択します。
3. [Outlet Name (アウトレット (コンセント) 名)] ドロップダウンリストから [None (なし)] を選択します。
4. [OK] をクリックします。そのラック PDU/アウトレット (コンセント) の関連付けが削除され、確認メッセージが表示されます。

▶ ラック PDU がターゲットから削除されている場合にラック PDU の関連付けを削除するには、以下の手順に従います。

1. [Device Settings (デバイス設定)] > [Port Configuration (ポート設定)] をクリックし、アクティブなターゲットをクリックします。
2. アクティブなターゲットを切断された電源ポートに関連付けます。これで、切断されたターゲットの電源の関連付けが破棄されます。
3. 最後に、アクティブなターゲットを、正しい電源ポートに関連付けます。



ブレード シャーシの設定

標準型サーバとラック PDU（電源タップ）に加えて、KX II のポートに接続されているブレード シャーシを制御することができます。一定時間に最大 8 台のブレード シャーシを管理できます。

ブレード シャーシは、ブレード シャーシ サブタイプとして設定する必要があります。ブレード シャーシ タイプがサポートされている場合、ブレード シャーシは、接続されると自動的に検出されます。シャーシ タイプがサポートされていない場合は、そのブレードを手動で設定する必要があります。

ブレード サーバ シャーシが検出された場合は、デフォルト名が関連付けられ、それが [Port Access]（ポート アクセス）ページに、標準ターゲット サーバおよびラック PDU と共に表示されます。「*[Port Access]（ポート アクセス）ページ（リモート コンソール ディスプレイ）*『*53*p. 』」を参照してください。

ブレード サーバは、[Port Access]（ポート アクセス）ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ▶ を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

HP ブレード シャーシおよび Cisco® UCS ブレード シャーシを除く、汎用、IBM®、Dell® の各ブレード シャーシは、[Port Access]（ポート アクセス）ページで設定されます。ブレード シャーシに接続されるポートは、ブレード シャーシ モデルで設定されている必要があります。ブレード サーバに設定できる特定の情報は、使用しているブレード サーバのブランドによって異なります。サポートされているこれらの各ブレード シャーシ固有の情報は、このセクションのヘルプにある対応するトピックを参照してください。

次のブレード シャーシがサポートされています。

- IBM BladeCenter® モデル E および H
- Dell PowerEdge® 1855、1955、および M1000e

[Generic]（汎用）オプションでは、上のリストに含まれていないブレード シャーシを設定できます。HP BladeSystem c3000 と c7000 のブレード サーバ、および Cisco UCS ブレード サーバは、Dominion デバイスから各ブレードへの個別の接続を介してサポートされます。ポートは、ポート グループ管理機能を使用して、シャーシにまとめてグループ化されます。

注: Dell PowerEdge 1855/1955 ブレードも、各個別ブレードから Dominion デバイス上のポートに接続できます。この方法で接続した場合、それらをグループ化してブレード サーバ グループを作成できます。

ブレード シャーシでは、手動設定と自動検出の 2 つの操作モードがあり、ブレード シャーシの機能によって決まります。ブレード シャーシが自動検出で設定される場合、Dominion デバイスは、以下を追跡および更新します。

- 新しいブレード サーバがいつシャーシに追加されるか。
- 既存のブレード サーバがいつシャーシから削除されるか。

注: IBM Blade Center モデル E および H を使用する場合、KX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ホット キー シーケンスを使用してブレード シャーシへの KVM アクセスを切り替えることもできます。ユーザがホットキー シーケンスを選択できるブレード シャーシの場合、これらのオプションは、[Port Configuration] (ポート設定) ページにあります。ホットキー シーケンスがあらかじめ定義されているブレード シャーシの場合、これらのシーケンスは、ブレード シャーシが選択されると [Port Configuration] (ポート設定) ページに自動的に入力されます。たとえば、IBM BladeCenter H に対する KVM を切り替えるためのデフォルト ホットキー シーケンスは、NumLock+NumLock+SlotNumber なので、設定中に IBM BladeCenter H が選択されたときに、このホットキー シーケンスがデフォルトで適用されます。ホットキー シーケンスについての詳細は、ブレード シャーシのマニュアルを参照してください。

ブレード シャーシ Web ブラウザ インタフェースがある場合は、それに対する接続を設定できます。シャーシ レベルでは、最大 4 つのリンクを定義できます。1 つ目のリンクは、ブレード シャーシ管理モジュール GUI への接続用に予約されています。たとえば、このリンクは、テクニカル サポートがシャーシ設定をすばやく検証する場合に使用されることがあります。

ブレード シャーシは、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Raritan の Multi-Platform Client (MPC)、および CC-SG から管理できます。VKC、AKC、および MPC を介したブレード サーバの管理は、標準ターゲット サーバの管理と同じです。詳細は、「**ターゲット サーバの使用** 『46p. 』」および『**CC-SG 管理者ガイド**』を参照してください。ブレード シャーシ設定に対する変更は、これらのクライアント アプリケーションに反映されます。

重要: ブレード シャーシを Dominion デバイスに CIM 接続することによって、電源がオフになったり Dominion デバイスから切断されたりした場合、ブレード シャーシに対して確立されているすべての接続が切断されます。CIM が再接続されるか電源オンにした場合は、接続を再確立する必要があります。

重要: ブレード シャーシをある Dominion デバイス ポートから別の Dominion デバイス ポートに移動する場合、CC-SG でブレード シャーシ ノードに追加されたインタフェースが CC-SG で失われます。他の情報はすべて維持されます。

汎用ブレード シャーシの設定

[Generic] (汎用) ブレード シャーシを選択した場合の操作モードは、手動設定モードだけです。 ブレード シャーシを設定する際の重要な情報および追加情報については、「*サポートされているブレード シャーシ モデル* 『*235*p. 』」、「*ブレード シャーシでサポートされている CIM* 『*236*p. 』」、および「*ブレード シャーシの必須および推奨設定* 『*239*p. 』」を参照してください。Dell® のシャーシで KX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「*Dell シャーシを接続する場合のケーブル長と画面解像度* 『*359*p. の"*Dell 筐体を接続する場合のケーブル長と画面解像度*"参照 』」を参照してください。

▶ シャーシを設定するには、以下の手順に従います。

1. ブレード シャーシを KX II に接続します。装置の接続方法の詳細は、「*手順 3: 装置の接続* 『*32*p. 』」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから [Generic] (汎用) を選択します。
6. ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード シャーシへの切り替えに使用されるホットキー シーケンスを定義します。[Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - 適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。
   f. [Password] (パスワード) - 適用されません。

7. 必要に応じてブレード シャーシ名を変更します。
8. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。
9. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▸ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) – インタフェースへの URL を入力します。 **必須。**
   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。 **(オプション)**
   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。 **(オプション)**

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のままにしないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「*Web ブラウザ インタフェースの追加に関するヒント* 『*231*p. 』」を参照してください。 **(オプション)**

10. USB プロファイル情報は汎用設定には適用されません。
11. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
12. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。
13. CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。選択されない場合は、デフォルトの解像度 1280 x 1024 が使用されます。
14. [OK] をクリックして設定を保存します。

Dell ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「*サポートされているブレード シャーシ モデル* 『*235*p. 』」、「*ブレード シャーシでサポートされている CIM* 『*236*p. 』」、および「*ブレード シャーシの必須および推奨設定* 『*239*p. 』」を参照してください。Dell® のシャーシで KX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「*Dell シャーシを接続する場合のケーブル長と画面解像度* 『*359*p. の"*Dell 筐体を接続する場合のケーブル長と画面解像度*"参照 』」を参照してください。

▶ ブレード シャーシを追加するには、以下の手順に従います。

1. ブレード シャーシを KX II に接続します。装置の接続方法の詳細は、「*手順 3: 装置の接続* 『*32*p. 』」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。

4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから Dell ブレード シャーシ モデルを選択します。

Dell PowerEdge M1000e を設定するには、以下の手順に従います。

1. [Dell PowerEdge™ M1000e] (Dell PowerEdge M1000e) を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります (「*[Device Services] (デバイス サービス)* 『*179*p. 』」を参照してください)。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 [Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username] (ユーザ名) - ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password] (パスワード) - ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KX II でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery] (ブレードの自動検出) チェックボックスをオンにし、[Discover Blades on Chassis Now] (ブレード シャーシを今すぐ検出) をクリックします。ブレードが検出されると、それがページに表示されます。

3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KX II によってシャーシに名前が割り当てられます。KX II では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

   自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。
5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▸ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) – インタフェースへの URL を入力します。 Dell M1000e のサンプル設定の詳細は、「*ブレード シャーシのサンプル URL フォーマット 『242p. 』*」を参照してください。
   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のままにしないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*231*p. 』」を参照してください。

6. USB プロファイルは Dell シャーシには適用されません。
7. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
8. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。
9. CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。選択されない場合は、デフォルトの解像度 1280 x 1024 が使用されます。
10. [OK] をクリックして設定を保存します。

▶ Dell PowerEdge 1855/1955 を設定するには、以下の手順に従います。

1. [Dell 1855/1955] (Dell 1855/1955) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 Dell 1855/1955 モデルの場合は、KX II によって既存のすべてのホットキー シーケンスをブロックします。汎用設定を Dell 1855 に適用する場合は、既存のホットキー 1 つだけがブロックされます。
   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。

c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - 適用されません。

d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。

e. [User Name] (ユーザ名) - 適用されません。

f. [Password] (パスワード) - 適用されません。

2. 必要に応じてブレード シャーシ名を変更します。

3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▶ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

   b. [URL] (URL) - インタフェースへの URL を入力します。 Dell PowerEdge 1855/1955 のサンプル設定の詳細は、「ブレード シャーシのサンプル URL フォーマット」を参照してください。

   c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。

   d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** *『231*p. *』*」を参照してください。

5. USB プロファイルは Dell シャーシには適用されません。
6. [OK] をクリックして設定を保存します。

IBM ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「***サポートされているブレード シャーシ モデル*** *『235*p. *』*」、「***ブレード シャーシでサポートされている CIM*** *『236*p. *』*」、および「***ブレード シャーシの必須および推奨設定*** *『239*p. *』*」を参照してください。Dell® のシャーシで KX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度*** *『359*p. の*"Dell 筐体を接続する場合のケーブル長と画面解像度"*参照 *』*」を参照してください。

▶ **ブレード シャーシを追加するには、以下の手順に従います。**

1. ブレード シャーシを KX II に接続します。装置の接続方法の詳細は、「***手順 3: 装置の接続*** *『32*p. *』*」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから IBM® ブレード シャーシ モデルを選択します。

▶ IBM BladeCenter H および E を設定するには、以下の手順に従います。

1. IBM BladeCenter® H または E を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります（「*[Device Services]（デバイス サービス）*『*179*p. 』」を参照してください）。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。 KX II では、AMM[1] の自動検出のみサポートされます。
   a. [Switch Hot Key Sequence]（切り替えホットキー シーケンス）– 定義済みです。
   b. [Maximum Number of Slots]（最大スロット数）– ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name]（管理モジュールのプライマリ IP アドレス/ホスト名）– ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number]（ポート番号）– ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username]（ユーザ名）– ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password]（パスワード）– ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KX II でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery]（ブレードの自動検出）チェックボックスをオンにし、[Discover Blades on Chassis Now]（ブレード シャーシを今すぐ検出）をクリックします。ブレードが検出されると、それがページに表示されます。
3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KX II によってシャーシに名前が割り当てられます。KX II では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed]（インストール済み）チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All]（すべて選択）チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。

5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▸ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

   b. [URL] (URL) – インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「*ブレード シャーシのサンプル URL フォーマット 『242p. 』*」を参照してください。

   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。

   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のままにしないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「*Web ブラウザ インタフェースの追加に関するヒント* 『*231*p. 』」を参照してください。

6. 適用できる場合は、ブレード シャーシの USB プロファイルを定義するか、既存の USB プロファイルを選択します。[Select USB Profiles for Port] (ポートの USB プロファイルを選択) アイコン **Select USB Profiles for Port** または [Apply Select Profiles to Other Ports] (選択したプロファイルを他のポートに適用) アイコン **Apply Selected Profiles to Other Ports** をクリックして、ページ内のこのセクションを展開します。「*USB プロファイルの設定 ([Port] (ポート) ページ)* 『*243*p. 』」を参照してください。
7. [OK] をクリックして設定を保存します。

IBM BladeCenter (その他) を設定するには、以下の手順に従います。

1. [IBM BladeCenter (Other)] (IBM BladeCenter (Other) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。
   f. [Password] (パスワード) - 適用されません。
2. 必要に応じてブレード シャーシ名を変更します。

3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。まだ名前が付いていない場合は、KX II によってブレード サーバに名前が割り当てられます。ブレード サーバにはデフォルトで「Blade_Chassis_Port#_Slot#」という名前が付けられます。
4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▸ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) – インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「*ブレード シャーシのサンプル URL フォーマット 『242p. 』*」を参照してください。
   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のままにしないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*231*p. 』」を参照してください。

5. USB プロファイルは [IBM (Other)] (IBM (その他)) 設定では使用されません。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。
8. CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。選択されない場合は、デフォルトの解像度 1280 x 1024 が使用されます。
9. [OK] をクリックして設定を保存します。

Web ブラウザ インタフェースの追加に関するヒント

Web ブラウザ インタフェースを追加して、埋め込み Web サーバを持つデバイスとの接続を作成できます。Web ブラウザ インタフェースは、RSA、DRAC、または ILO Processor カードに関連付けられている Web アプリケーションなどの任意の Web アプリケーションへの接続にも使用できます。

DNS を設定しておく必要があります。そうしないと、URL が解決されません。IP アドレスの場合は DNS を設定する必要はありません。

▶ Web ブラウザ インタフェースを追加するには、以下の手順に従います。

1. Web ブラウザ インタフェースのデフォルト名が提供されます。必要な場合は、[Name] (名前) フィールドで名前を変更します。
2. [URL] (URL) フィールドに Web アプリケーションの URL またはドメイン名を入力します。Web アプリケーションでユーザ名とパスワードの読み取りが行われる URL を入力する必要があります。

正しいフォーマットについては、以下の例を参照してください。

- http(s)://192.168.1.1/login.asp
- http(s)://www.example.com/cgi/login
- http(s)://example.com/home.html

3. このインタフェースへのアクセスが許可されるユーザ名とパスワードを入力します。**(オプション)**
4. ユーザ名とパスワードが入力された場合、[Username Field] (ユーザ名フィールド) と [Password Field] (パスワード フィールド) に、Web アプリケーションのログイン画面で使用されるユーザ名フィールドとパスワード フィールドのフィールド名を入力します。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの名前を探す必要があります。

フィールド名検索に関するヒント:

- Web アプリケーションのログイン ページの HTML ソース コードで、Username や Password などのフィールドのラベルを検索します。
- フィールド ラベルが見つかったら、隣接するコードで ″name=″user″″ のようなタグを探します。引用符内の語がフィールド名です。

HP および Cisco USC のブレード シャーシ設定 (ポート グループ管理)

KX II は、特定のタイプのブレードに接続されるポートをまとめてブレード シャーシを示すグループとしてサポートします。特に、Cisco® USC ブレード、HP® BladeServer ブレード、および Dell® PowerEdge™ 1855/1955 ブレード (Dell PowerEdge 1855/1955 ブレードが個別の各ブレードから KX II 上のポートに接続されている場合) がこれにあたります。

シャーシは、[Port Group Name] (ポート グループ名) によって特定され、グループは、[Port Group Management] (ポート グループ管理) ページの [Blade Server Group] (ブレード サーバ グループ) として指定されます。ポート グループには、標準 KVM ポートとして設定されたポートのみで構成され、ブレード シャーシとして設定されたポートは含まれません。ポートは、1 つのグループだけに属することができます。

ブレード シャーシで組み付けの KVM モジュールに接続されているポートは、ブレード シャーシ サブタイプとして設定されます。これらのポートは、ポート グループに含めることができます。

KX II ポートがブレード シャーシ内で組み付けの KVM モジュールに接続され、個別のブレードに接続されていない場合、ポートはブレード シャーシ サブタイプとして設定されます。これらのポートはポート グループに含めることはできないので、[Select Port for Group] (グループ化するポートの選択) の [Available] (利用可能) リストには表示されません。

ポート グループに含まれている標準 KVM ポートを、後でブレード シャーシ サブタイプとして用途変更する場合は、まず、ポート グループからそれを削除する必要があります。

ポート グループは、[Backup and Restore] (バックアップとリストア) オプションを使用してリストアされます (「*バックアップと復元 『286*p. 』」を参照してください)。

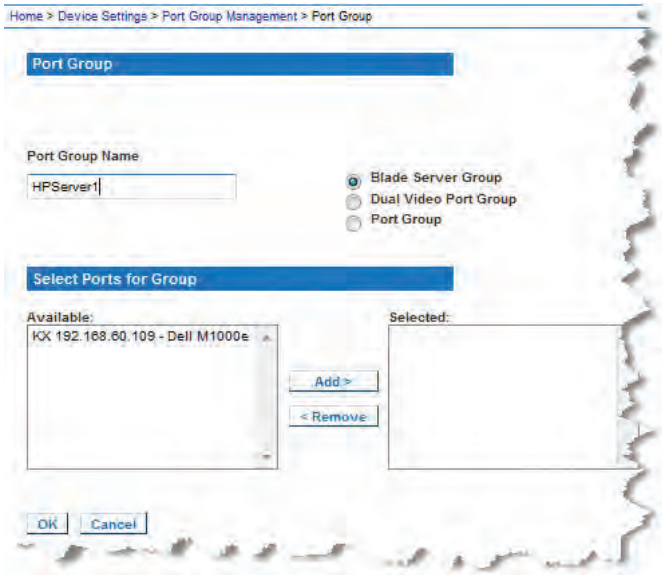
▶ ポート グループを追加するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) をクリックし、[Port Group Management] (ポート グループ管理) ページを開きます。
2. [Add] (追加) をクリックすると、[Port Group] (ポート グループ) ページが開きます。
3. ポート グループ名を入力します。ポート グループでは、最大 32 文字で、大文字と小文字は区別されません。
4. [Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   これらのポートをブレード シャーシ (たとえば、HP c3000 または Dell PowerEdge 1855) 内のブレードに接続するように指定する場合は、[Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   注: 各ブレードは KX II のポートに独自に接続されていますが、これは、HP ブレードをシャーシ ベースで整理する CC-SG ユーザにとっては特に重要です。

5. [Select Ports for Group] (グループ化するポートの選択) セクションの [Available] (利用可能) ボックスで、ポートをクリックします。[Add] (追加) をクリックして、ポートをグループに追加します。ポートは [Selected] (選択) ボックスに移動されます。
6. [OK] をクリックして、ポート グループを追加します。



▶ ポート グループ情報を編集するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページで、編集するポート グループのリンクをクリックします。[Port Group] (ポート グループ) ページが開きます。
2. 必要に応じて情報を編集します。
3. [OK] をクリックして変更を保存します。

▶ ポート グループを削除するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページをクリックし、削除するポート グループのチェックボックスをオンにします。
2. [Delete] (削除) をクリックします。
3. 警告メッセージで [OK] をクリックします。

サポートされているブレード シャーシ モデル

この表には、KX II でサポートされているブレード シャーシ モデルと、それらを KX II アプリケーションで設定する際にシャーシごとに選択する必要がある対応プロファイルが含まれています。これらのモデルのリストは、[Port Configuration] (ポート設定) ページの [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストで選択できます。これは、[Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択している場合に表示されます。各ブレード シャーシ モデルの設定方法についての詳細は、このセクションのヘルプ内の対応するトピックを参照してください。

ブレード シャーシ モデル	KX II プロファイル
Cisco® USC	ポート グループ管理機能を使用して設定します。「*HP および Cisco USC のブレード シャーシ設定 (ポート グループ管理)* 『*233*p. 』」を参照してください。
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	ポート グループ管理機能を使用して設定します。「*HP および Cisco USC のブ*

ブレード シャーシ モデル	KX II プロファイル
	レード シャーシ設定（ポート グループ管理）『*233*p. 』」を参照してください。

ブレード シャーシでサポートされている CIM

以下の CIM は、KX II を通じて管理されるブレード シャーシでサポートされています。

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

以下の表に、KX II がサポートする各ブレード シャーシ モデルでサポートされている CIM を示します。

ブレード シャーシの場合	接続方法	推奨 CIM
Generic（汎用）	Generic（汎用）として設定されたブレード シャーシへの接続時に D2CIM-VUSB または D2CIM-DVUSB が使用されている場合は、[Port Configuration]（ポート設定）ページおよびクライアントの［USB Profile］（USB プロファイル）メニューから USB プロファイルを選択できます。ただし、汎用ブレード シャーシでは仮想メディアがサポートされないので、クライアントの［Virtual Media］メニューは無効になります。	• DCIM-PS2 • DCIM-USBG2
Cisco® UCS サーバ シャーシ	Cisco KVM ケーブル（N20-BKVM）を使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ソース: *『Cisco UCS 5108 Server Chassis Installation Guide』*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB

ブレード シャーシの場合	接続方法	推奨 CIM
Dell® PowerEdge™ 1855	以下の 3 つの KVM モジュールのいずれかを含みます。 • アナログ KVM Ethernet スイッチ モジュール (標準) • デジタル アクセス KVM スイッチ モジュール (オプション) • KVM スイッチ モジュール (2005 年 4 月以前に販売されたシステムでの標準) これらのスイッチは、2 つの PS/2 および 1 つのビデオ デバイスをシステムに接続できるカスタム コネクタを提供します。 ソース: *Dell PowerEdge 1855 システム ユーザーズ ガイド*	• DCIM-PS2
Dell PowerEdge 1955	2 種類の KVM モジュールのいずれかがインストールされる可能性があります。 • アナログ KVM スイッチ モジュール • デジタル アクセス KVM スイッチ モジュール どちらのモジュールでも、PS/2 互換のキーボード、マウス、およびビデオ モニタをシステムに接続できます (システムに付属のカスタムケーブルを使用)。 ソース: *Dell PowerEdge 1955 ハードウェア オーナーズ マニュアル*	• DCIM-PS2
Dell PowerEdge M1000e	KVM スイッチ モジュール (iKVM) はこのシャーシに組み付けられています。 iKVM は、次の周辺機器に対応しています。 • USB キーボード、USB ポインティング デバイス • VGA モニタ (DDC サポート) ソース: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide*	• DCIM-USBG2
HP® BladeSystem c3000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、ブレード シャーシの管理、設定、および診断プロシージャを実行できます。 ソース: HP Proliant™ BL480c Server Blade	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (KVM オプションを使用しない標準 KVM ポート操作の

ブレード シャーシの場合	接続方法	推奨 CIM
	Maintenance and Service Guide	場合)
HP BladeSystem c7000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ソース: *HP ProLiant BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (標準 KVM ポート操作)
IBM® BladeCenter® S	Advanced Management Module (AMM) は、すべてのブレード シャーシのシステム管理機能およびキーボード/ビデオ/マウス (KVM) マルチプレキシングを提供します。 AMM 接続は、シリアル ポート、ビデオ接続、リモート管理ポート (Ethernet)、およびキーボードとマウス用の 2 つの USB v2.0 ポートが含まれます。 ソース: *Implementing the IBM BladeCenter S Chassis*	• DCIM-USBG2
IBM BladeCenter H	BladeCenter H 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 つ標準で付属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	現在のモデル BladeCenter E シャーシ (8677-3Rx) には、アドバンスト マネージメント モジュールが 1 つ標準で属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	BladeCenter T 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 つ標準で付属しています。 標準の BladeCenter シャーシとは異なり、BladeCenter T シャーシの KVM モジュールおよびマネージメント モジュールは、個別のコンポーネントになります。マネージメント モジュールの前面にあるのは、ステータスを表示する LED だけです。Ethernet および KVM 接続はすべて背面の LAN および KVM モジュ	• DCIM-PS2

ブレード シャーシの場合	接続方法	推奨 CIM
	ールで行います。 KVM モジュールは、ホット スワップ モジュールです。シャーシの背面にキーボードとマウス用の 2 つの PS/2 コネクタ、システム ステータス パネル、および HD-15 ビデオ コネクタがあります。 ソース: *IBM BladeCenter Products and Technology*	
IBM BladeCenter HT	BladeCenter HT 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 つ標準で付属しています。このモジュールは、シャーシを管理する機能とともに、ローカル KVM 機能も提供します。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2

注: 自動検出をサポートするために、IBM BladeCenter モデル H および E では、ファームウェア バージョンが BPET36K 以降の AMM を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

注: 音声は、すべての KVM スイッチ ターゲットで無効になります。

ブレード シャーシの必須および推奨設定

この表は、KX II で機能させるためのブレード シャーシの設定に適用される制限についての情報を示します。以下のすべての情報に従うことをお勧めします。

ブレード シャーシの場合	必須/推奨アクション
Dell® PowerEdge™ M1000e	• iKVM GUI スクリーンセーバを無効にします。無効にしていない場合は、認可のダイアログが表示され、iKVM が正しく機能しません。 • Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 • iKVM GUI の［メイン］メニューを設定して、名前ではなくスロ

ブレード シャーシの場合	必須/推奨アクション
	ットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 • iKVM GUI の［設定］メニューの［スキャン］でスキャン操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。 • iKVM GUI の［設定］メニューの［ブロードキャスト］でキーボード/マウスのブロードキャスト操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。 • iKVM GUI を呼び出す 1 つのキー シーケンスを指定します。このキー シーケンスを、KX II でポートを設定するときにも指定する必要があります。そうしないと、クライアントのキー入力の結果として、iKVM 操作が無差別に発生する可能性があります。 • Dell の CMC GUI を通じて iKVM を設定する際に、［フロントパネル USB/ビデオ有効］が*オフ*になっていることを確認します。オンになっている場合、シャーシの前面パネルでの接続が、背面の KX II 接続よりも優先されるので、適切な iKVM 処理が行われなくなります。"User has been disabled as front panel is currently active"（フロント パネルが現在アクティブになっているのでユーザは無効です）というメッセージが表示されます。 • Dell の CMC GUI を通じて iKVM を設定する際に、［iKVM から CMC CLI へのアクセスを許可する］が*オフ*になっていることを確認します。 • ブレード シャーシに接続するときに iKVM GUI が表示されないようにするには、［画面遅延時間］を 8 秒に設定します。 • iKVM GUI のフラグ設定中に、［時間指定］および［表示］を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
Dell PowerEdge 1855/1955	• iKVM GUI スクリーンセーバを無効にします。これを行わない場合は［Authorize］（認可）ダイアログ ボックスが表示され、iKVM が正しく機能しなくなります。 • Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 • iKVM GUI の［メイン］メニューを設定して、名前ではなくスロットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 • iKVM GUI の［設定］メニューの［スキャン］でスキャン操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。

ブレード シャーシの場合	必須/推奨アクション
	• ブレード シャーシに接続するときに iKVM GUI が表示されないようにするには、[画面遅延時間] を 8 秒に設定します。 • iKVM GUI のフラグ設定中に、[時間指定] および [表示] を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
IBM®/Dell® 自動検出	• ブレード レベルのアクセス許可を適用する場合は、自動検出を有効にすることをお勧めします。有効にしない場合は、ブレード シャーシ全体でのアクセス許可を設定します。 • ブレード シャーシ管理モジュールで、Secure Shell (SSH) を有効にする必要があります。 • ブレード シャーシ管理モジュールで設定された SSH ポートと、[Port Configuration] (ポート設定) ページで入力されるポート番号が一致する必要があります。
IBM KX2 仮想メディア	• Raritan KX II 仮想メディアは、IBM BladeCenter® モデル H および E でのみサポートされます。これは、D2CIM-DVUSB を使用する必要があります。黒の D2CIM-DVUSB 低速 USB コネクタは、本体背面の Administrative Management Module (AMM) に取り付けられます。グレーの D2CIM-DVUSB 高速 USB コネクタは、本体前面のメディア トレイ (MT) に取り付けられます。これには、USB 延長ケーブルが必要です。
Cisco® UCS サーバ シャーシ	• Cisco KVM ケーブル (N20-BKVM) を使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 • ソース: Cisco UCS 5108 Server Chassis Installation Guide (DCIM-USBG2、D2CIM-VUSB、D2CIM-DVUSB)

注: AMM を使用するすべての IBM BladeCenter では、KX II で動作する AMM ファームウェア バージョン BPET36K 以降を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ブレード シャーシのサンプル URL フォーマット

この表には、KX II で設定されるブレード シャーシのサンプル URL フォーマットが示されます。

ブレード シャーシの場合	サンプル URL フォーマット
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login • ユーザ名: root • ユーザ名フィールド: user • Password:calvin • パスワード フィールド: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • ユーザ名: root • ユーザ名フィールド: TEXT_USER_NAME • Password:calvin • パスワード フィールド: TEXT_PASSWORD
IBM® BladeCenter® E または H	• http://192.168.84.217/private/welcome.ssi

USB プロファイルの設定 ([Port] (ポート) ページ)

ポートで使用できる USB プロファイルを、[Port] (ポート) ページの [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで選択します。[Port] (ポート) ページで選択された USB プロファイルが、ポートから KVM ターゲット サーバに接続するときに VKC でユーザが使用できるプロファイルになります。デフォルト値は、Windows 2000®/Windows XP®/Windows Vista® 用のプロファイルです。USB プロファイルについての詳細は、「*USB プロファイル 『134p. 』*」を参照してください。

*注: ポートの USB プロファイルを設定するには、デジタル CIM、VM-CIM、またはデュアル VM-CIM を、KX II の現在のファームウェアバージョンと互換性のあるファームウェアに接続しておく必要があります。「*CIM をアップグレードする *『290p. の "CIM アップグレード" 参照 』」を参照してください。*

ポートへの割り当てに使用できるプロファイルは、左側の [Available] (使用可能) リストに表示されます。ポートで使用するように選択したプロファイルは、右側の [Selected] (選択) リストに表示されます。いずれかのリストでプロファイルを選択した場合、プロファイルとその使用についての説明が [Profile Description] (プロファイルの説明) フィールドに表示されます。

KVM ポートで使用可能にする一連のプロファイルを選択する他に、ポートの優先プロファイルを指定して、あるポートに対する設定を他の KVM ポートに適用することもできます。

*注: DCIM-VUSB または DCIM-DVUSB の使用時に Mac OS X® USB プロファイルを使用する方法の詳細については、「*DCIM-VUSB で Mac OS X USB プロファイルを使用する場合のマウス モード *『144p. の "DCIM-VUSB で Mac OS-X USB プロファイルを使用する場合のマウス モード" 参照 』」を参照してください。*

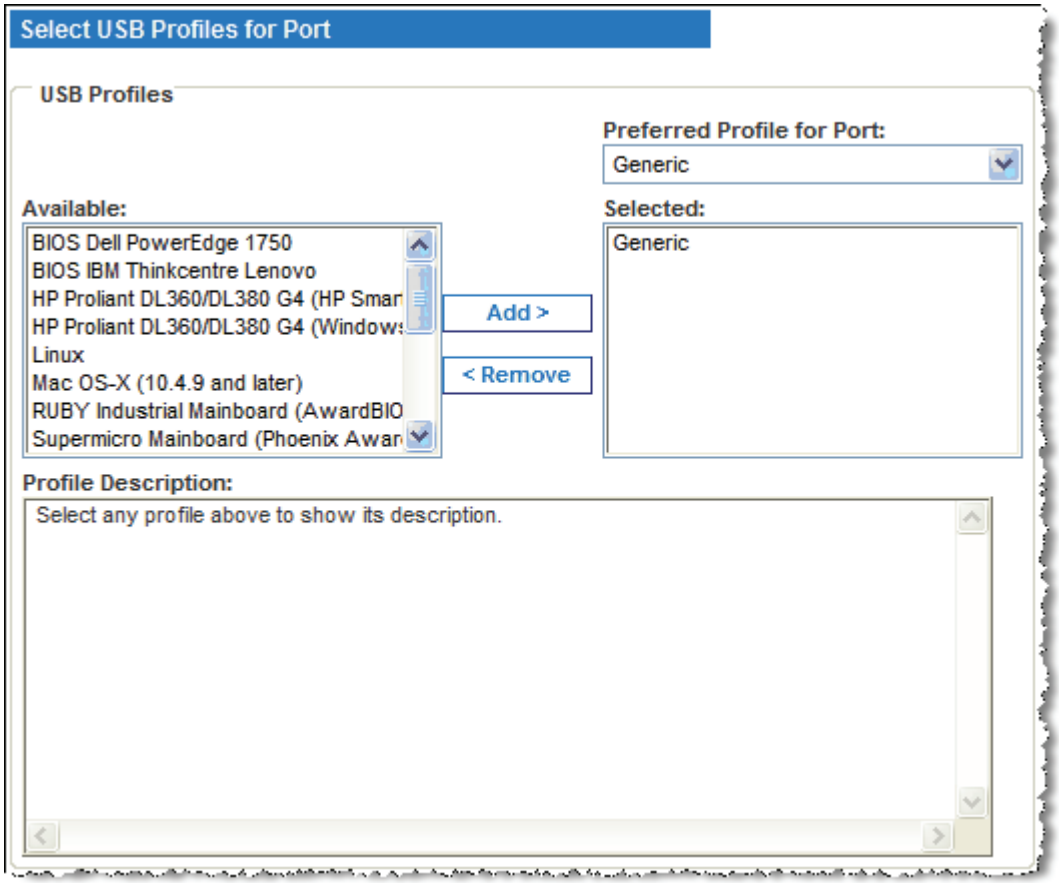
▶ [Port] (ポート) ページを開くには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 編集する KVM ポートの [Port Name] (ポート名) をクリックします。[Port] (ポート) ページが開きます。

▶ KVM ポートの USB ポートを選択するには、以下の手順に従います。

1. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで、1 つ以上の USB プロファイルを [Available] (使用可能) リストから選択します。
   - Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。

- Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。



2. [Add]（追加）をクリックします。選択したプロファイルが [Selected]（選択）リストに表示されます。これらは、ポートに接続された KVM ターゲット サーバで使用できるプロファイルです。

▶ 優先 USB プロファイルを指定するには、以下の手順に従います。

1. ポートで使用可能なプロファイルを選択した後、[Port]（ポート）メニューの [Preferred Profile]（優先プロファイル）から 1 つを選択します。デフォルトは [Generic]（汎用）です。選択したプロファイルは、KVM ターゲット サーバに接続するときに使用されます。必要に応じて、他の USB プロファイルに変更できます。

▶ 選択した USB プロファイルを削除するには、以下の手順に従います。

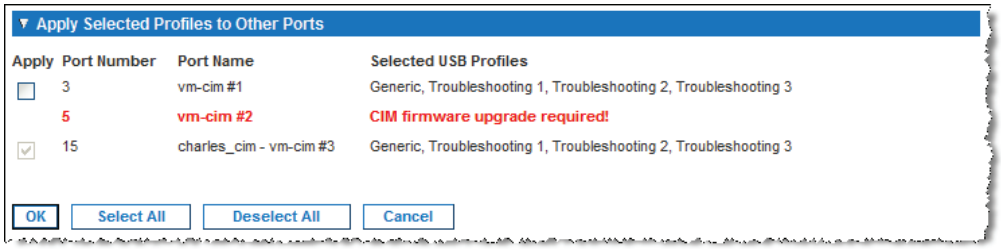
1. [Select USB Profiles for Port]（ポートの USB プロファイルの選択）セクションで、1 つ以上の USB プロファイルを [Selected]（選択）リストから選択します。

- Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。
- Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。

2. [Remove] (削除) をクリックします。選択したプロファイルが [Available] (使用可能) リストに表示されます。これらのプロファイルは、このポートに接続された KVM ターゲット サーバでは使用できなくなります。

▶ プロファイルの選択を複数のポートに適用するには、以下の手順に従います。

1. [Apply Selected Profiles to Other Ports] (選択したプロファイルを他のポートに適用) セクションで、選択した USB プロファイルの現在の設定を適用する各 KVM ポートの [Apply] (適用) チェックボックスをオンにします。



- すべての KVM ポートを選択するには、[Select All] (すべて選択) をクリックします。
- すべての KVM ポートの選択を解除するには、[Deselect All] (すべての選択を解除) をクリックします。

KX II のローカル ポートの設定

[Local Port Settings] (ローカル ポート設定) ページでは、KX II ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。また、ローカル ポートの USB プロファイルを変更することもできます。

KX2-808、KX2-832、および KX2-864 では、[Local Port Settings] (ローカル ポート設定) ページで拡張ローカル ポートを設定することもできます。拡張ローカル ポートを Paragon スイッチまたはユーザ ステーションに接続して、ローカル ポートの接続距離を延長できます。標準ローカル ポートと同様に、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証の設定を指定できます。拡張ローカル ポートは、リモート コンソールとローカル コンソールの両方から設定できます。標準ローカル ポートと拡張ローカル ポートの詳細については、「*KX2-808、KX2-832、および KX2-864 の標準ローカル ポートと拡張ローカル ポートの設定* 『*251*p. 』」を参照してください。

注: KX2-808、KX2-832、および KX2-864 で拡張ローカル ポートを有効にしてポートに何も接続しない場合、ローカル ポートを経由したターゲットへの切り替え時に 2 ～ 3 秒の遅延が発生します。

▶ ローカル ポートに関する設定値をカスタマイズするには

注: [Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. 標準ローカル ポートを有効にするには、[標準ローカル ポートを有効にする] チェック ボックスをオンにします。無効にするにはチェックボックスをオフにします。デフォルトでは、標準ローカル ポートは有効になっていますが、必要に応じて無効にすることができます。この設定を変更すると、ブラウザが再起動します。 カスケード接続機能を利用する場合、この機能は無効になります。両方の機能を同時に利用することができないからです。

3. KX2-808、KX2-832、または KX2-864 デバイスを使用している場合、拡張ローカル ポートを有効にするには、その横にあるチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。スマート カード機能を使用する場合は、拡張ローカル ポートを無効にする必要があります。この設定を変更すると、ブラウザが再起動します。

   標準ローカル ポートと拡張ローカル ポートの両方が無効になっている場合は、ローカル ポートにアクセスできません。無効になっているローカル ポートを使用して KX2-808、KX2-832、または KX2-864 にアクセスしようとすると、デバイスがリモート管理の対象になっていること、およびログインが無効になっていることを示すメッセージが表示されます。

   注: カスケード接続デバイスとして KX2-808、KX2-832、または KX2-864 を使用する場合は、拡張ローカル ポートを使用して、これらのデバイスをベース KX II に接続する必要があります。

4. カスケード接続機能を利用する場合、[ローカル ポート デバイスのカスケード接続を有効にする] チェック ボックスをオンにし、[カスケード接続秘密ワード] フィールドにカスケード接続秘密ワードを入力します。カスケード接続を設定するには、[デバイス サービス] ページでベース デバイスを設定する必要があります。カスケード接続の詳細については、「***カスケード接続の設定および有効化*** *『181p. の"カスケード接続を設定および有効化する"参照 』*」を参照してください。
5. 必要な場合は、[ローカル ポート スキャン モード] 設定をカスタマイズします。これらの設定は、[ポート] ページからアクセスされるスキャン設定機能に適用されます。「***ポートのスキャン*** *『59p. 』*」を参照してください。
   - [表示間隔 (10 ～ 255 秒):]: フィールドで、フォーカスを持つターゲットを [ポート スキャン] ウィンドウの中央に表示する秒数を指定します。
   - [ポート間の間隔 (10 ～ 255 秒):] フィールドで、ポート間でデバイスを一時停止する間隔を指定します。
6. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)
   - [United Kingdom] (イギリス英語)
   - [French (France)] (フランス語 (フランス))
   - [German (Germany)] (ドイツ語 (ドイツ))
   - [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
   - [Simplified Chinese] (簡体字中国語)

- [Traditional Chinese] (繁体字中国語)
- [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
- [German (Switzerland)] (ドイツ語 (スイス))
- [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
- [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
- [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
- [Danish (Denmark)] (デンマーク語 (デンマーク))
- [Belgian (Belgium)] (ベルギー語 (ベルギー))

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

注: トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

7. [Local Port Hotkey] (ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KX II ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock] (Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock] (Caps Lock キーを 2 回押す)	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。

8. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。その後ホットキーを使用して、そのターゲット サーバの画面から KX II ローカル コンソールの画面に戻すことができます。接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー シーケンスの例については、「*接続キーの例*『*324*p. 』」を参照してください。 接続キーは、標準型サーバとブレード シャーシのどちらに対しても機能します。
9. 必要に応じて、[画面切り替え遅延 (秒)] ボックスに 0 ～ 5 秒の範囲の数値を入力します。通常は「0」と入力します。ただし、一部のモニタでは画面切り替えに時間がかかるので、その場合は適切な値を入力します。
10. 省電力機能を利用する場合、次の手順を実行します。
    a. [省電力モード] チェック ボックスをオンにします。
    b. [省電力モードのタイムアウト (分)] ボックスに、省電力モードに移行するまでの時間 (単位: 分) を入力します。
11. [解像度] ボックスの一覧で、KX II ローカル コンソールの画面解像度を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
    - 800 x 600
    - 1024 x 768
    - 1280 x 1024
12. [垂直走査周波数 (Hz)] ボックスの一覧で垂直走査周波数を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
    - 60 Hz
    - 75 Hz
13. [ローカル ユーザ認証] でローカル ユーザ認証タイプを選択します。
    - [ローカル/LDAP/RADIUS]: これは推奨オプションです。認証の詳細については、「*リモート認証*『*42*p. 』」を参照してください。
    - [なし]: KX II ローカル コンソールからのアクセスに対して認証は行われません。このオプションは、安全な環境でのみ選択することをお勧めします。
    - KX II が CommandCenter Secure Gateway (CC-SG) の管理下にある場合にローカル ユーザを認証するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにします。

注: 最初は [Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオフにしていたが、後でローカル ポートからのアクセスを CC-SG の管理対象から除外したくなった場合、CC-SG 側で KX II を CC-SG の管理対象から除外する必要があります。その後、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにすることができます。

注: KX II が CC-SG の管理下にある場合に標準ローカル ポートと拡張ローカル ポートを使用するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェックボックスをオンにする必要があります。KX II が CC-SG の管理下にある場合に標準ローカル ポートまたは拡張ローカル ポート経由のローカル ユーザを認証するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにします。または、ダイレクト デバイス アクセス機能を利用します (CC-SG の管理下にある場合)。

14. [OK] (OK) をクリックします。

KX2-808、KX2-832、および KX2-864 の標準ローカル ポートと拡張ローカル ポートの設定

KX2-808、KX2-832、および KX2-864 には、2 つのローカル ポート オプションが用意されています。それは、標準ローカル ポートと拡張ローカル ポートです。これらの各ポート オプションを有効にしたり無効にしたりするには、リモート コンソールまたはローカル コンソールで [Local Port Settings] (ローカル ポート設定) ページを使用します。詳細については、「*KX II のローカル ポートの設定* 『*246*p. 』」を参照してください。

デフォルトでは、標準ローカル ポートは有効、拡張ローカル ポートは無効になっています。ローカル ポートの接続距離を延長する場合は、拡張ローカル ポートを有効にし、Cat5/5e/6 ケーブルを使用して Paragon II UMT、EUST、UST、または URKVMG から KX2-808、KX2-832、または KX2-864 に接続します。

注: KX2-808、KX2-832、および KX2-864 で拡張ローカル ポートを有効にしてポートに何も接続しない場合は、ローカル ポートを経由したターゲットへの切り替え時に 2 ～ 3 秒の遅延が発生します。

これらのオプションを設定するには管理者権限が必要です。ポートにアクセスするには、ユーザ名とパスワードを一度入力するだけです。これらの資格情報を、アクセスするポートごとに入力する必要はありません。

拡張ローカル ポートでサポートされているデバイスの詳細、および距離の仕様とサポートされている CIM については、「*仕様* 『*339*p. 』」を参照してください。

KX2-808、KX2-832、および KX2-864 の接続の制限事項

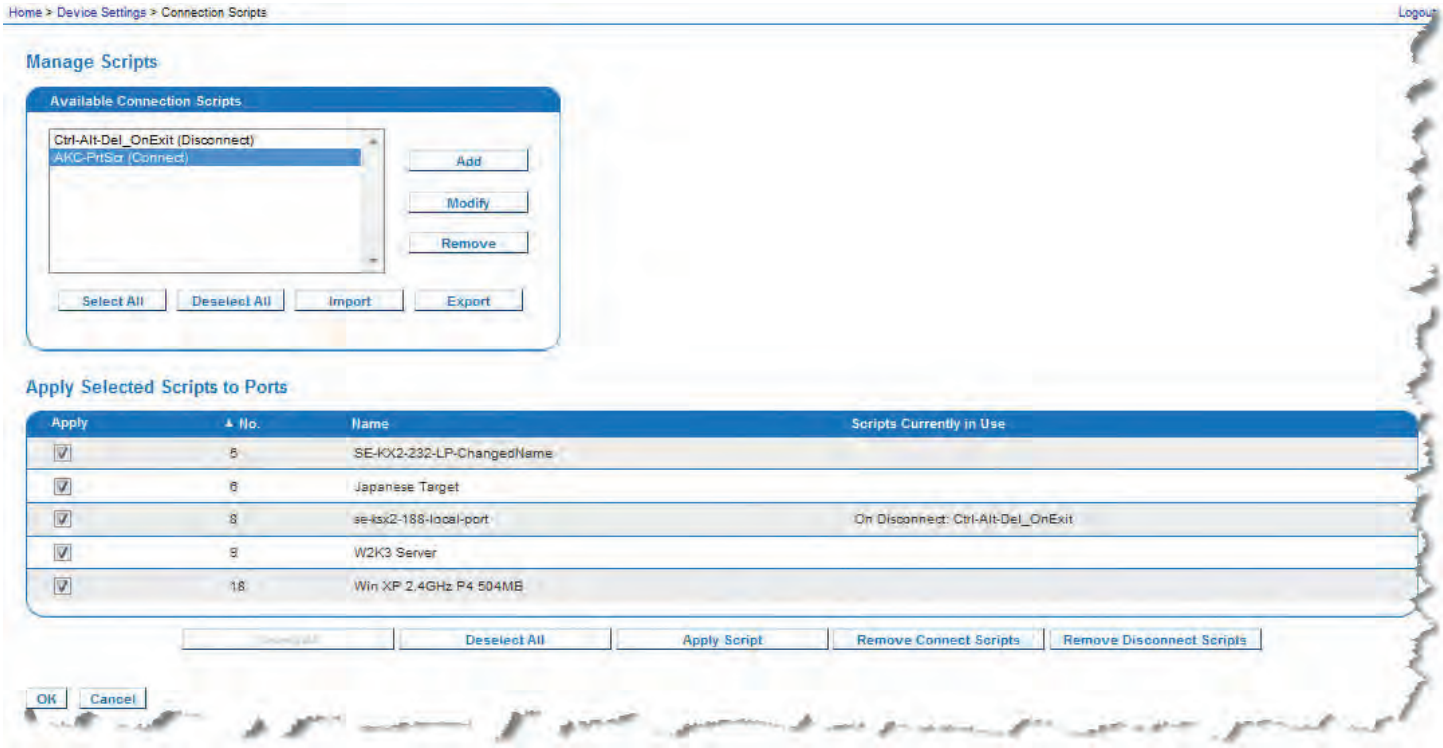
標準ローカル ポートおよび拡張ローカル ポートは、ターゲットへのアクセスを共有します。両方のポートが有効になっている場合、キーボード、ビデオ、およびマウスは標準ローカル ポートと拡張ローカル ポートで共有されます。両方のポートがターゲットに接続されるか、またはターゲットから切断されます。

標準ローカル ポートと拡張ローカル ポートのどちらか一方が無効になっている場合、そのポートのキーボード、ビデオ、およびマウスは無効になり、ローカル ポートが無効になっていることを示すメッセージが表示されます。

スクリプトの接続と切断

KX II では、ターゲットとの接続を確立または切断する場合にキー マクロ スクリプトを実行できます。これらのスクリプトは、[Connection Scripts] (接続スクリプト) ページで定義および管理されます。

[Connection Scripts] (接続スクリプト) ページで独自のスクリプトを作成および編集し、ターゲットの接続を確立または切断するときに追加アクションを実行できます。また、既存の XML ファイル形式の接続スクリプトをインポートすることもできます。KX II で作成したスクリプトを XML ファイル形式でエクスポートすることもできます。KX II では、合計 16 個のスクリプトに対応できます。



スクリプトの適用および削除

▶ スクリプトをターゲットに適用するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。

2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、ターゲットに適用するスクリプトを選択します。'On Connect' スクリプトを 1 つと 'On Disconnect' スクリプトを 1 つターゲットに適用できます。

注: ターゲットに一度に追加できるスクリプトは 1 つだけです。

3. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットにのみスクリプトを適用する場合) スクリプトに適用するターゲットを選択します。
4. [Apply Scripts] (スクリプトを適用) をクリックします。スクリプトがターゲットに追加されると、それが [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションの [Scripts Currently in Use] (現在使用中のスクリプト] の下に表示されます。

▶ スクリプトをターゲットから削除するには、以下の手順に従います。

1. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットからのみスクリプトを削除する場合) スクリプトを削除するターゲットを選択します。
2. [Remove Connect Scripts] (接続スクリプトを削除) をクリックして接続スクリプトを削除するか、[Remove Disconnect Scripts] (切断スクリプトを削除) をクリックして切断スクリプトを削除します。

スクリプトの追加

*注: KX II の外部で作成したスクリプトを追加したり、それらを XML ファイルとしてインポートしたりすることもできます。「**スクリプトのインポートとエクスポート 『256p. 』**」を参照してください。*

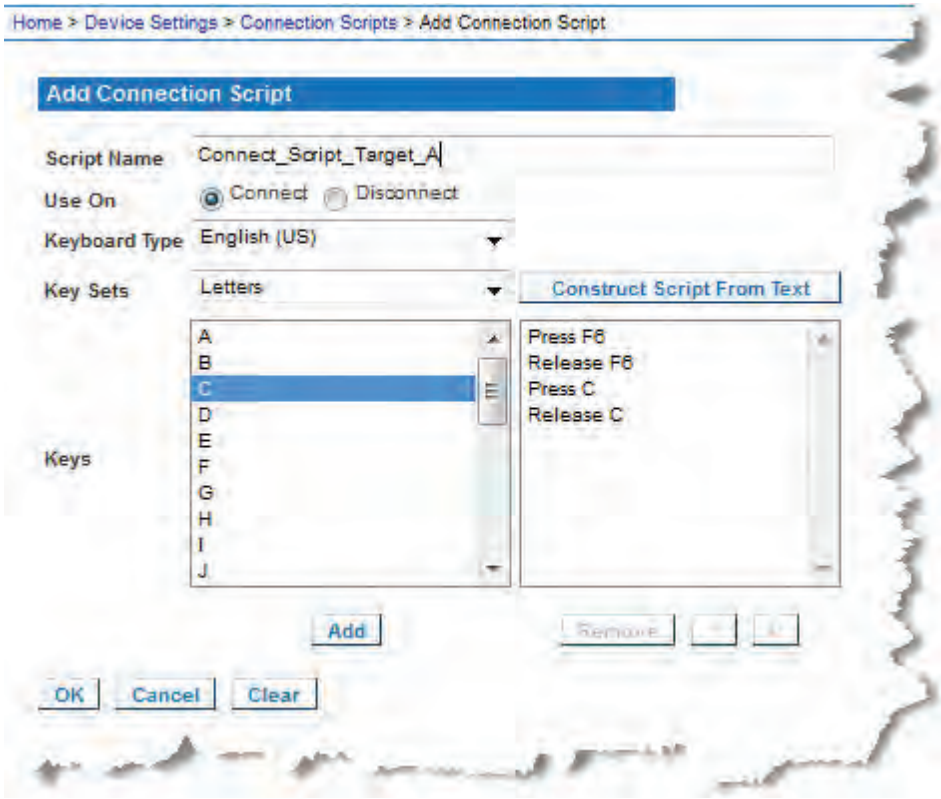
▶ スクリプトを作成するには、以下の手順に従います。

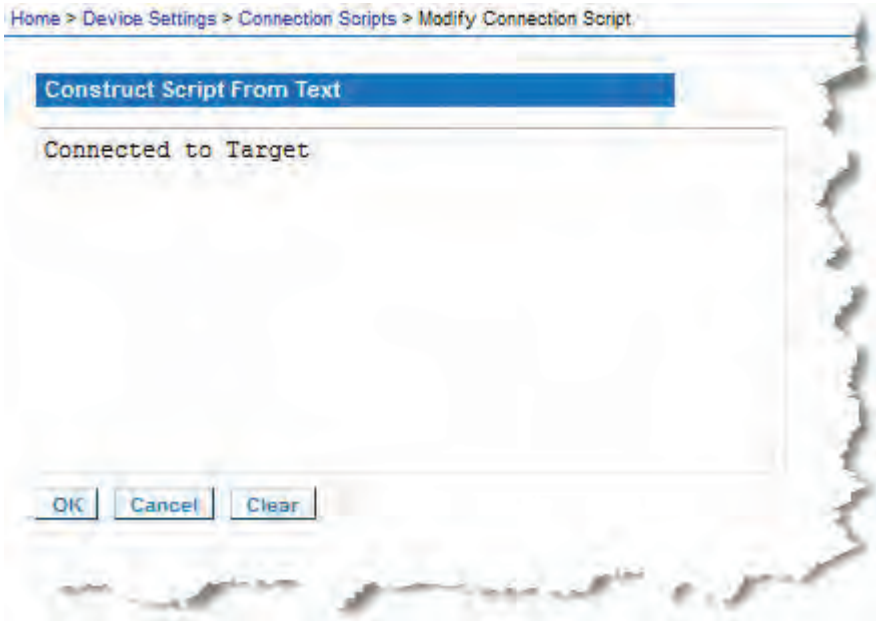
1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、[Add] (追加) をクリックします。[Add Connection Script] (接続スクリプトの追加) ページが開きます。
3. スクリプトの名前を最大 32 文字で入力します。スクリプトが作成されると、この名前が [Configure Scripts] (スクリプトの設定) ページの [Available Connection Scripts] (使用できる接続スクリプト) セクションに表示されます。

4. 作成中のスクリプトのタイプとして、[Connect]（接続）または [Disconnect]（切断）を選択します。接続スクリプトは、新規接続で、またはターゲットの切り替え時に使用されます。
5. 使用するターゲットで要求されるキーボード タイプを選択します。
6. [Key Sets]（キー セット）ドロップダウン リストから、スクリプトの作成に使用するキーボードのキー セットを選択します。選択すると、[Key Sets]（キー セット）ドロップダウン リストの下の [Add]（追加）ボックスに、選択したキー セット オプションが入力されます。
7. [Add]（追加）ボックスからキーを選択し、[Add]（追加）をクリックしてそれを [Script]（スクリプト）ボックスに移動します。キーを [Script]（スクリプト）ボックスから削除するには、キーを選択して [Remove]（削除）をクリックします。キーを並べ替えるには、それらを選択して [Up]（上へ）および [Down]（下へ）アイコンを使用します。

   スクリプトは、1 つ以上のキーで構成できます。また、スクリプトで使用されるキーを組み合わせることもできます。

   たとえば、F1 ～ F16 を選択すると、[Add]（追加）ボックスにファンクション キー セットが表示されます。ファンクション キーを選択して、それを [Script]（スクリプト）ボックスに移動します。次に、[Key Sets]（キー セット）ドロップダウン リストから [Letters]（文字）を選択して、文字キーをスクリプトに追加します。
8. スクリプトの実行時に表示されるテキストを追加することもできます。
   a. [Construct Script from Text]（テキストからスクリプトの作成）をクリックして、[Construct Script From Text]（テキストからスクリプトの作成）ページを開きます。
   b. テキスト ボックスにスクリプトを入力します。たとえば、「Connected to Target」（ターゲットに接続済み）と入力します。
   c. [Construct Script From Text]（テキストからスクリプトの作成）ページで [OK] をクリックします。
9. [OK] をクリックして、スクリプトを作成します。


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

スクリプトの変更

▶ 既存のスクリプトを変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、変更するスクリプトを選択して、[Modify] (変更) をクリックします。ページが編集モードになります。
3. 必要に応じて変更します。完了したら [OK] をクリックします。

スクリプトのインポートとエクスポート

XML ファイル形式の接続スクリプトおよび切断スクリプトは、インポートおよびエクスポートできます。キーボード マクロのインポートまたはエクスポートはできません。

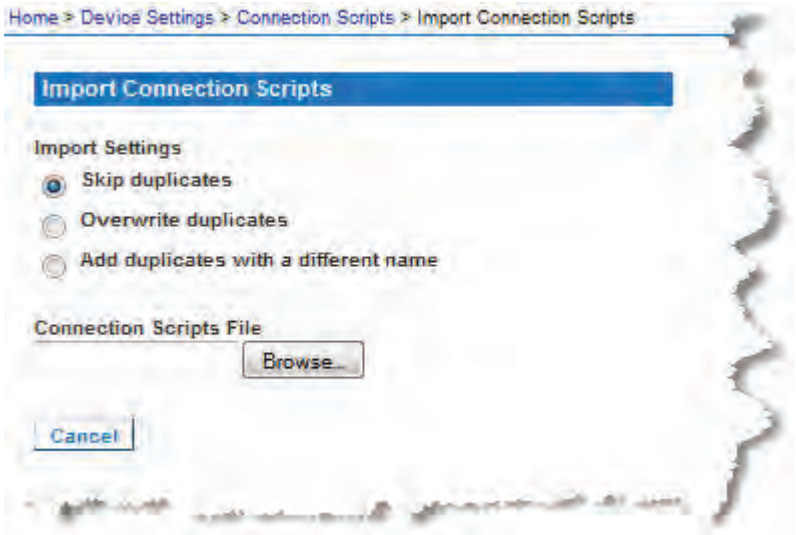
注: インポートおよびエクスポート機能は、ローカル コンソールからは使用できません。

インポートされたスクリプトは、KX II で変更機能を使用して編集できます。ただし、インポートされたスクリプトがポートに関連付けられると、変更できなくなります。変更するためには、ポートからスクリプトを削除します。「*スクリプトの適用および削除 『252p. 』*」を参照してください。

▶ スクリプトをインポートするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、[Import] (インポート) をクリックします。[Import Connection Scripts] (接続スクリプトのインポート) ページが開きます。
3. インポート設定を選択します。
   - [Skip duplicates] (重複をスキップ) – 既に KX II に存在するスクリプトは、インポートから除外されます。
   - [Overwrite duplicates] (重複を上書き) – 既に KX II に存在するスクリプトは、インポートされた新しいスクリプトで上書きされます。
   - [Add duplicates with a different name] (別の名前で重複を追加) – 重複スクリプトの名前がインポート中に変更されるので、既存のスクリプトは上書きされません。元のスクリプトと区別できるように、KX II によってファイル名に数字が割り当てられます。

4. 参照機能を使用して、インポートする XML スクリプト ファイルを検索します。
5. [Import] (インポート) をクリックします。[Configuration Scripts] (設定スクリプト) ページが開き、インポートされたスクリプトが表示されます。



▶ 切断スクリプトをエクスポートするには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Configuration Scripts] (設定スクリプト) をクリックします。[Configuration Scripts] (設定スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、エクスポートするスクリプトを選択して、[Export] (エクスポート) をクリックします。XML ファイルを開くか保存するためのダイアログ ボックスが表示されます。
3. XML ファイルを保存するか、XML エディタで開きます。XML ファイルを保存する場合は、デフォルトの Download フォルダに保存されます。

ポート グループ管理

ポート グループ管理では、以下が表示されます。

- [Blade Server Group] (ブレード サーバ グループ) – 特定のタイプのブレードに接続されるポートを、ブレード シャーシを示すグループにまとめたもの。詳細については、「*HP および Cisco USC のブレード シャーシ設定 (ポート グループ管理)* 『*233*p. 』」を参照してください。
- [Dual Video Port Group] (デュアル ビデオ ポート グループ) – ターゲット サーバ上で拡張デスクトップ設定を提供するポート グループの作成。「*デュアル ビデオ ポート グループの作成* 『*260*p. 』」を参照してください。
- [Port Group] (ポート グループ) – プライマリ ポートに適用されている設定がグループ内のすべてのセカンダリ ポートに適用される、「標準の」ポート グループの作成。「*ポート グループの作成* 『*259*p. 』」を参照してください。

ポート グループの作成

KX II は、複数のポートをまとめた 1 つのポート グループをサポートします。ポート グループは、標準の KVM ポートとして設定されたポートだけで構成されます。ポートは、1 つのグループだけに属することができます。

ポート グループに追加可能なポートは、[Select Port for Group]（グループ化するポートの選択）の [Available]（利用可能）リストに表示されます。一度ポート グループに追加されたポートは、別のポート グループには追加できません。新しいポート グループでポートを使用するには、既存のポート グループからポートを削除します。

プライマリ ポートから実行される接続操作や切断操作は、電源制御を除いてグループ内のセカンダリ ポートに適用されます。

ポート グループは、[Backup and Restore]（バックアップとリストア）オプションを使用してリストアされます（「*バックアップと復元*『*286*p. 』」を参照してください）。

注: ブレード シャーシのポート グループを作成する方法については、「**HP および Cisco USC のブレード シャーシ設定（ポート グループ管理）**『233*p.* 』」*を参照し、デュアル ビデオ ポート グループを作成する方法については、「デュアル ビデオ ポート グループの作成」を参照してください。*

▶ ポート グループを作成するには、以下の手順に従います。

1. [Device Settings]（デバイス設定）の [Port Group Management]（ポート グループ管理）を選択します。[Port Group Management]（ポート グループ管理）ページが開きます。既存のポート グループすべてが表示されます。
2. [Add]（追加）をクリックします。ページが更新され、利用可能なポート グループ オプションがすべて表示されます。
3. [Port Group]（ポート グループ）ラジオ ボタンを選択します。
4. グループに追加するポートを選択するには、[Available]（利用可能）テキスト ボックス内のポートをクリックし、[Add]（追加）をクリックして該当するポートを [Selected]（選択）テキスト ボックスに追加します。
5. [OK] をクリックして、ポート グループを作成します。これで、[Port Group Management]（ポート グループ管理）ページにポート グループが表示されます。

デュアル ビデオ ポート グループの作成

デュアル ビデオ ポート グループ機能により、2 つのビデオ ポートを 1 つのグループにまとめることができます。この機能は、2 つのビデオ カードまたはビデオ ポートを搭載したサーバに接続する必要がある場合や、同じリモート クライアントから同時に両方のポートにアクセスする場合に使用します。

注: デュアル ポート ビデオ グループは、KX2-108 や KX2-116 のような、KVM チャネルが 1 つしかない KX II モデルではサポートされません。

注: デュアル ビデオ ポート グループは、作成すると、ローカル コンソールおよびリモート クライアントから利用できます。ただし、ローカル コンソールでは拡張デスクトップはサポートされていません。

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

各グループには、プライマリ ポートおよびセカンダリ ポートが含まれている必要があります。プライマリ ポートに適用される設定は、グループ内のすべてのセカンダリ ポートに適用されます。グループから削除されたポートは、独立したポートと見なされ、新しい設定を適用することができます。

リモート クライアントからデュアル ポート ビデオ グループにアクセスする場合は、プライマリ ポートに接続すると、デュアル ポート グループのプライマリ ポートおよびセカンダリ ポートの両方に対する KVM 接続ウィンドウが開きます。

セッションを開始し、必要に応じてリモート クライアントから 1 つ以上のモニタに表示できます。

KX II で設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。できれば、接続元のクライアントの画面方向が同じに設定されていることが望まれます。

重要: 特定の環境に影響を与える可能性がある制限、推奨設定などについては、「*デュアル ビデオ ポート グループ* 『*370*p. 』」の情報を確認してください。

▶ デュアル ポート ビデオ グループを作成するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) を選択します。[Port Group Management] (ポート グループ管理) ページが開きます。既存のポート グループすべてが表示されます。
2. [Add] (追加) をクリックします。[Port Group] (ポート グループ) ページが開き、利用可能なすべてのポートが [Select Ports for Group] (グループ化するポートの選択) セクションに表示されます。

   注: ポートが既にブレード サーバ ポート グループ、別のデュアル ビデオ ポート グループ、または「標準の」ポート グループに属している場合、そのポートを選択することはできません。これは、ポートは一度に 1 つのポート グループにしか属すことができないためです。

3. [Dual Video Port Group] (デュアル ビデオ ポート グループ) ラジオ ボタンを選択します。
4. [Select Ports for Group] (グループ化するポートの選択) セクションで、プライマリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。必ず最初にプライマリ ポートを追加してください。

   *注: 理想的には、ポート グループの各ポートに適用される権限は、同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。たとえば、あるポートに [VM Access] (VM アクセス) の [Deny] (拒否) が適用されており、別のポートに [VM Access] (VM アクセス) の [Read-Write] (読み取り/書き込み可能) が適用されている場合、ポート グループには、[VM Access] (VM アクセス) の [Deny] (拒否) が適用されます。ポートの権限によりデュアル ビデオ ポート グループがどのような影響を受けるかについては、「**権限およびデュアル ビデオ ポート グループ アクセス 『379p. 』**」を参照してください。*

5. セカンダリ ポートとして指定するポートをクリックし、[Add] (追加) をクリックして該当するポートを [Selected] (選択) テキスト ボックスに追加します。
6. ページの方向を選択します。選択する方向は、現在のモニタ設定に対する最適性によって異なります。
7. [OK] をクリックして、ポート グループを作成します。

デュアル ビデオ ポート グループは、[Port Access] (ポート アクセス) ページにデュアル ポート タイプとして表示されます。ポート グループに属しているプライマリ ポートおよびセカンダリ ポートは、[Port Access] (ポート アクセス) ページに、それぞれ [Dual Port (P)] (デュアル ポート (P)) および [Dual Port (S)] (デュアル ポート (S)) として表示されます。たとえば、CIM タイプが DCIM である場合は、[DCIM Dual Port (P)] (DCIM デュアル ポート (P)) が表示されます。

注: カスケード接続デバイスに接続されているデュアル ビデオ ポートのターゲットには、カスケード接続ベース デバイス以外のカスケード接続デバイスを介して接続する必要があります。

デフォルトの GUI 言語設定の変更

KX II の GUI では、以下のローカライズ言語がサポートされています。

- 日本語
- 簡体字中国語
- 繁体字中国語

GUI 言語を変更するには、以下の手順に従います。

1. [デバイス設定] の [言語] を選択します。[言語設定] ページが開きます。
2. [言語] ボックスの一覧で、GUI に適用する言語を選択します。
3. [適用] をクリックします。[デフォルトに戻す] をクリックして、[英語] に戻します。

注: 新しい言語を適用すると、オンライン ヘルプも、選択言語に合わせてローカライズされます。

Ch 9 セキュリティ上の問題

この章の内容

セキュリティの設定 263
IP アクセス制御を設定する 275
SSL 証明書 278
セキュリティ バナー 281

セキュリティの設定

[Security Settings] (セキュリティ設定) ページで、ログオン制限、ユーザ ブロック、パスワード ルール、および暗号化と共有に関する設定を行うことができます。

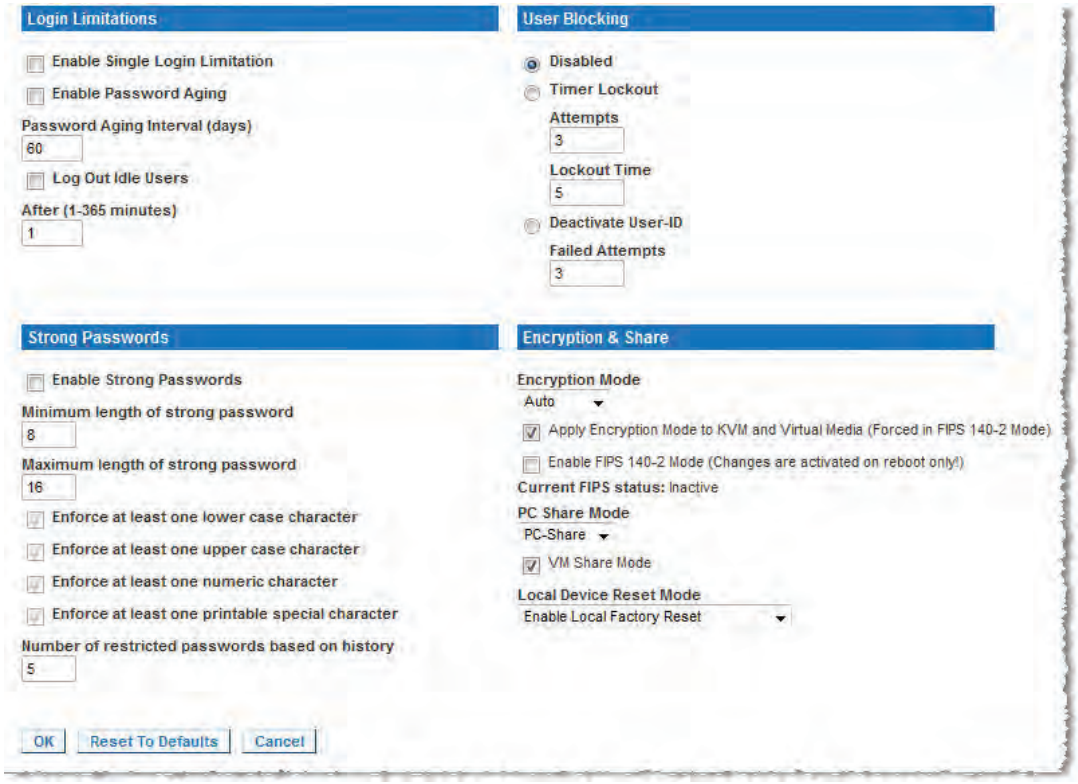
パブリック キーとプライベート キーの交換には Raritan SSL 証明書が使用され、セキュリティのレベルを高めます。Raritan の Web サーバ証明書は自己署名されています。Java アプレット証明書は、VeriSign の証明書によって署名されています。暗号化を行うと、情報が漏洩しないよう保護されていることを保証できます。またこれらの証明書によって、事業体の身元が Raritan, Inc であることが証明されます。

▶ セキュリティ設定を行うには、以下の手順に従います。

1. [Security] (セキュリティ) の [Security Settings] (セキュリティ設定) を選択します。[Security Settings] (セキュリティ設定) ページが開きます。
2. 必要に応じて、*[Login Limitations] (ログイン制限)* 『*264*p. の"*[ログイン制限]*"参照 』 の設定を更新します。
3. 必要に応じて、*[Strong Passwords] (強力なパスワード)* 『*266*p. の"*[強力なパスワード]*"参照 』 の設定を更新します。
4. 必要に応じて、*[User Blocking] (ユーザ ブロック)* 『*267*p. の"*[ユーザ ブロック]*"参照 』 の設定を更新します。
5. 必要に応じて、[Encryption & Share] (暗号化および共有) の設定を更新します。
6. [OK] (OK) をクリックします。

▶ デフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

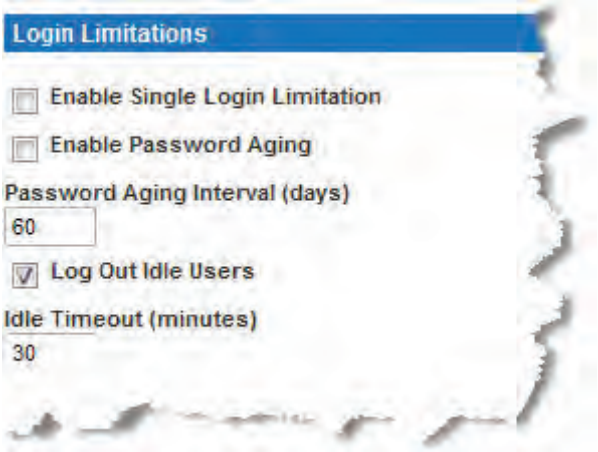


[ログイン制限]

[ログイン制限] セクションでは、シングル ログイン、パスワード エージング、アイドル ユーザのログアウトに関する制限を指定できます。

制限	説明
[シングル ログイン制限を有効にする]	このチェック ボックスをオンにした場合、ユーザ名ごとに同時に 1 人しかログオンできません。このチェック ボックスをオフにした場合、所定のユーザ名とパスワードの組み合わせで、複数のクライアント ワークステーションからデバイスに同時接続できます。
[パスワード エージングを有効にする]	これを選択すると、[パスワード エージング間隔] で指定した日数に基づいて、すべてのユーザに対して定期的にパスワードを変更するよう要求します。

制限	説明
	[パスワード エージングを有効にする] チェックボックスをオンにするとこのフィールドが有効になるため、設定する必要があります。パスワードの変更が要求される間隔を日数で入力します。デフォルトの日数は 60 日です。
[アイドル ユーザをログアウトする]、[分後 (1 ～ 365)]	[アイドル ユーザをログオフする] チェック ボックスをオンにした場合、[分後 (1 ～ 365)] ボックスに入力した時間が経過した後にアイドル ユーザが自動ログオフされます。キーボードまたはマウスで操作が行われない場合は、すべてのセッションおよびすべてのリソースがログアウトされます。ただし、実行中の仮想メディア セッションはタイムアウトしません。 [分後 (1 ～ 365)] ボックスに入力した時間が経過した後にアイドル ユーザが自動ログアウトされます。このボックスが有効になるのは、[アイドル ユーザをログオフする] チェック ボックスをオンにした場合です。このボックスに入力できる値は 1 ～ 365 の範囲です。



[強力なパスワード]

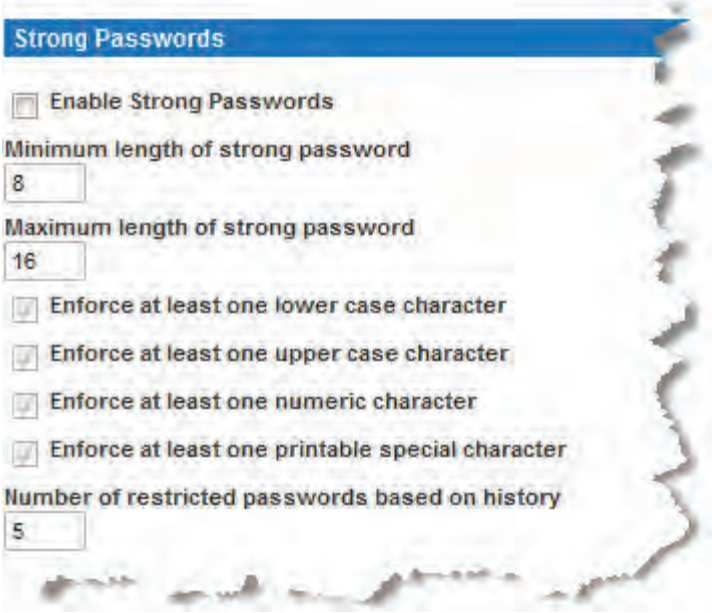
[強力なパスワード] セクションで値を指定すると、このシステムにおけるローカル認証の安全性が高まります。強力なパスワードを使用すると、最小長と最大長、必要な文字、パスワード履歴の保持など、有効な KX II ローカル パスワードの形式を設定できます。

強力なパスワードには、アルファベットとアルファベット以外の文字（句読点または数字）をそれぞれ 1 文字以上含むパスワードを指定する必要があります。また、パスワードとユーザ名の最初の 4 文字には同じ文字列を使用できません。

[強力なパスワードを有効にする] チェック ボックスをオンにした場合、強力なパスワードの規則が適用されます。パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログオンする際にパスワードを変更するよう自動的に求められます。[強力なパスワードを有効にする] チェック ボックスをオフにした場合、標準の形式になっているかどうかだけが検査されます。[強力なパスワードを有効にする] チェックボックスをオンにした場合、次のフィールドが有効になるので、指定する必要があります。

フィールド	説明
[強力なパスワードの最小長]	パスワードは 8 文字以上でなければなりません。デフォルトでは 8 文字ですが、最大 63 文字まで拡張できます。
[強力なパスワードの最大長]	The default is 8 minimum and 16 the is the default maximum. (デフォルトでは 16 文字ですが、最大 64 文字まで拡張できます。)
[1 文字以上の小文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の小文字が必要になります。
[1 文字以上の大文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の大文字が必要になります。
[1 文字以上の数字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の数字が必要になります。
[1 文字以上の印刷可能な特殊文字の使用を強制する]	これを選択すると、パスワードに 1 文字以上の印刷可能な特殊文字が必要になります。
[履歴を参照する制限パスワードの数]	このボックスの値は、パスワード履歴の深さ、つまり、繰り返し使用することのできない以前のパスワードの数を意味します。範囲は 1 ～ 12 で、デフォル

フィールド	説明
	トは 5 です。



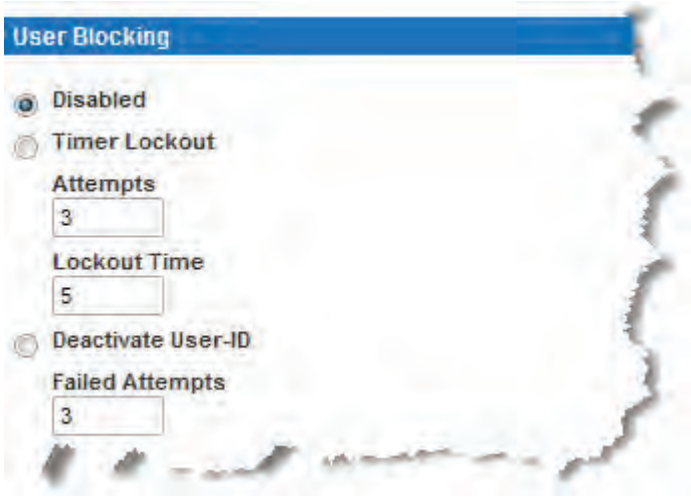
[ユーザ ブロック]

[ユーザ ブロック] セクションでは基準を指定し、ユーザが指定回数ログオンに失敗するとシステムにアクセスできなくなるようにします。

次の 3 つのオプションは、相互に排他的です。

オプション	説明
[無効]	デフォルト値です。認証に失敗した回数に関わらず、ユーザのアクセスはブロックされません。

オプション	説明
[タイマ ロックアウト]	ユーザが指定回数より多くログオンに失敗すると、システムへのアクセスが指定の時間拒否されます。これを選択した場合は次のフィールドが有効になります。 ▪ [試行回数]: この回数より多くログオンに失敗すると、ユーザはロックアウトされます。有効な範囲は 1 ～ 10 で、デフォルトの試行回数は 3 です。 ▪ [ロックアウト時間]: ユーザがロックアウトされる時間です。有効な範囲は 1 ～ 1440 分で、デフォルトでは 5 分です。 *注: [タイマ ロックアウト] で指定した値は、Administrator の役割が割り当てられているユーザには適用されません。*
[ユーザ ID を無効化]	このオプションを選択した場合は、[試行回数] フィールドで指定した回数より多くログオンに失敗すると、ユーザはシステムからロックアウトされます。 ▪ [試行回数]: この回数より多くログオンに失敗すると、そのユーザのユーザ ID が無効になります。このボックスが有効になるのは、[ユーザ ID を無効化] オプションを選択した場合です。有効な範囲は 1 ～ 10 です。 指定回数より多くログオンに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、[ユーザ] ページの [有効化] チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。



[Encryption & Share] (暗号化および共有)

[Encryption & Share] (暗号化および共有) セクションでは、使用する暗号化のタイプ、PC と VM の共有モード、KX II のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

警告: ご使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから KX II にアクセスできなくなります。

▶ 暗号化と共有を設定するには、以下の手順に従います。

1. [暗号化モード] ボックスの一覧で暗号化モードを選択します。選択した暗号化モードがご使用のブラウザでサポートされていない場合 KX II に接続できない、という内容の警告が表示されます。この警告は、"暗号化モードを選択する際、ご使用のブラウザでその暗号化モードがサポートされていることを確認してください。サポートされていない場合、KX II に接続できません" という意味です。

暗号化モード	説明
自動	これは推奨オプションです。使用可能な最高強度の暗号化モードに自動設定されます。 デバイスとクライアントが FIPS 準拠アルゴリズムの使用を正常にネゴシエートできるようにするには、[Auot] (自動) を選択する必要があります。
[RC4] (RC4)	RSA RC4 暗号方式を使用して、ユーザ名、パスワード、ビデオ送信を含む KVM データが保護されます。これは、最初の接続認証中に KX II とリモート PC 間のプライベート通信

暗号化モード	説明
	チャンネルを提供する 128 ビットの SSL (セキュア ソケット レイヤ) プロトコルです。 FIPS 140-2 モードを有効にして [RC4] (RC4) を選択すると、エラー メッセージが表示されます。[RC4] (RC4) は FIPS 140-2 モードでは使用できません。
[AES-128]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"128" はキーの長さを意味します。[AES-128] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「*ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する 『273*p. の*"ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する"*参照 』」を参照してください。
[AES-256]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"256" はキーの長さを意味します。[AES-256] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「*ご使用のブラウザで AES 暗号化モードがサポートされているかどうかを確認する 『273*p. の*"ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する"*参照 』」を参照してください。

注: [自動] を選択しなかった場合、MPC は最高強度の暗号化モードに設定されます。

注: Windows XP® (Service Pack 2 適用) と Internet Explorer® 7 を使用している場合、AES-128 暗号化モードで KX II にリモート接続することはできません。

2. [Apply Encryption Mode to KVM and Virtual Media] (暗号化モードを KVM および仮想メディアに適用する) チェック ボックスの値を指定します。このチェック ボックスをオンにした場合、選択した暗号化モードが KVM と仮想メディアの両方に適用されます。認証後、KVM データと仮想メディア データが 128 ビットの暗号化モードで転送されます。
3. 政府やその他のセキュリティの高い環境では、[Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして FIPS 140-2 モードを有効にします。FIPS 140-2 を有効にする方法については、「*FIPS 140-2 の有効化 『273*p. 』」を参照してください。
4. [PC Share Mode] (PC 共有モード) - グローバルな同時リモート KVM アクセスを特定し、最大 8 人までのリモート ユーザが KX II に同時にログオンし、デバイスを介してターゲット サーバを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
   - [Private] (プライベート): PC を共有しません。これはデフォルト値です。一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。
   - [PC-Share] (PC 共有): KVM ターゲット サーバに最大 8 人のユーザ (管理者または非管理者) が同時にアクセスできます。ただし、リモート ユーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウスの操作を止めないユーザがいると、制御が不規則になる場合があることに注意してください。
5. 必要に応じて、[VM Share Mode] (VM 共有モード) チェック ボックスをオンにします。このチェック ボックスは [PC-Share Mode] (PC 共有モード) ボックスの一覧で [PC-Share] (PC 共有) を選択した場合にのみ有効になります。このオプションを選択すると、複数のユーザで仮想メディアを共有できるようになります。つまり、複数のユーザが同じ仮想メディア セッションにアクセスできます。デフォルトでは、このチェック ボックスはオフになっています。
6. 必要に応じて、[Local Device Reset Mode] (ローカル デバイス リセット モード) ボックスの一覧で値を選択します。このオプションでは、ユニットの背面にあるハードウェア リセット ボタンが押下された際に実行するアクションを指定します。詳細については、「*リセット ボタンを使用して KX II をリセットする 『337*p. 』」を参照してください。次のいずれかの値を選択します。

ローカル デバイス リセット モード	説明
[Enable Local Factory Reset] (ローカルで出荷時設定にリセットする) (デフォルト)	KX II を出荷時設定にリセットします。

ローカル デバイス リセット モード	説明
[Enable Local Admin Password Reset] (ローカルで管理者パスワードだけをリセットする)	ローカルの管理者パスワードだけをリセットします。パスワードは raritan に戻ります。
[Disable All Local Resets] (ローカルでリセットしない)	リセットは一切実行されません。

注: P2CIM-AUSBDUAL または P2CIM-APS2DUAL を使用してターゲットを 2 台の KX II に接続しており、かつ、ターゲットへのプライベートアクセスが必要である場合、両方の KX II において PC 共有モードを [Private] (プライベート) に設定する必要があります。

Paragon CIM と ProductName を組み合わせて使用する場合の詳細については、「*サポートされている Paragon CIM および設定 『350*p. の*″サポートされている Paragon CIMS および設定″*参照 』」を参照してください。

ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する

KX II では AES 256 ビット暗号化方式がサポートされています。ご使用のブラウザで AES がサポートされているかどうか不明な場合は、そのブラウザの製造元に問い合わせるか、または、確認したい暗号化方式を使用してそのブラウザで https://www.fortify.net/sslcheck.html にアクセスしてください。この Web サイトでは、ご使用のブラウザの暗号化方式が検出され、レポートが表示されます。

注: Internet Explorer® 6 では、AES 128 ビットおよび 256 ビット暗号化方式はサポートされていません。

AES (256 ビット) を使用する際の前提条件とサポート対象構成

AES 256 ビット暗号化方式は、次のブラウザでのみサポートされています。

- Firefox® 2.0.0.x および 3.0.x 以降
- Internet Explorer 7 および 8

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java™ Cryptography Extension® (JCE®) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。

各種 JRE™ の管轄ファイルは、次のページの [other downloads] セクションで入手できます。

- JRE1.6: http://java.sun.com/javase/downloads/index_jdk5.jsp

FIPS 140-2 の有効化

政府やその他のセキュリティの高い環境では、FIPS 140-2 モードを有効にすることが望ましい場合があります。KX II では、『FIPS 140-2 Implementation Guidance』(FIPS 140-2 実装ガイダンス) の G.5 セクションのガイドラインに従って、Linux® プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。このモードを有効にすると、SSL 証明書の生成に使用される秘密鍵を内部で生成する必要があり、ダウンロードしたりエクスポートしたりすることはできません。

FIPS 140-2 を有効にするには、以下の手順に従います。

1. [Security Settings] (セキュリティ設定) ページを開きます。

2. [Security Settings] (セキュリティ設定) ページの [Encryption & Share] (暗号化および共有) セクションで [Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして、FIPS 140-2 モードを有効にします。FIPS 140-2 モードでは、外部通信に FIPS 140-2 で承認されたアルゴリズムを利用します。ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、FIPS 暗号化モジュールが使用されます。
3. KX II を再起動します。**必須。**

   FIPS モードが有効になると、「FIPS Mode: Enabled」(FIPS モード: 有効) というメッセージが画面の左パネルの [Device Information] (デバイス情報) セクションに表示されます。

   FIPS モードが有効になったら、セキュリティを強化するために、新しい証明書署名要求を作成することもできます。この要求は、必要な鍵暗号を使用して作成されます。署名された証明書をアップロードするか、自己署名証明書を作成します。SSL 証明書の状態は、[Not FIPS Mode Compliant] (FIPS モード非準拠) から [FIPS Mode Compliant] (FIPS モード準拠) に更新されます。

   FIPS モードが有効になっている場合は、鍵ファイルをダウンロードまたはアップロードできません。最後に作成された CSR が内部で鍵ファイルに関連付けられます。さらに、CA からの SSL 証明書とその秘密鍵は、バックアップされたファイルの完全な復元に含まれません。鍵を KX II からエクスポートすることはできません。

FIPS 140-2 サポートの要件

KX II では、FIPS 140-20 で承認された暗号化アルゴリズムの使用がサポートされます。これにより、クライアントが FIPS 140-2 専用モードに設定されている場合に、SSL サーバとクライアントでは、暗号化されたセッションに使用されている暗号スイートを正常にネゴシエートできます。

KX II で FIPS 140-2 を使用する場合の推奨事項を以下に示します。

KX II

- [Security Settings] (セキュリティ設定) ページで、[Encryption & Share] (暗号化および共有) を [Auto] (自動) に設定します。「*暗号化および共有 『269ρ. の"[Encryption & Share] (暗号化および共有)"参照 』*」を参照してください。

Microsoft クライアント

- クライアント コンピュータと Internet Explorer で FIPS 140-2 を有効にする必要があります。

Windows クライアントで FIPS 140-2 を有効にするには、以下の手順に従います。

1. [コントロール パネル]、[管理ツール]、[ローカル セキュリティ ポリシー] の順に選択して、[ローカル セキュリティ設定] ダイアログボックスを開きます。
2. ナビゲーション ツリーで、[ローカル ポリシー]、[セキュリティ オプション] の順に選択します。
3. [システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] を有効にします。
4. クライアント コンピュータを再起動します。

Internet Explorer で FIPS 140-2 を有効にするには、以下の手順に従います。

1. Internet Explorer で、[ツール] の [インターネット オプション] を選択し、[詳細設定] タブをクリックします。
2. [TLS 1.0 を使用する] チェックボックスをオンにします。
3. ブラウザを再起動します。

IP アクセス制御を設定する

IP アクセス制御機能を利用することにより、KX II に対するアクセスを制御できます。IP アクセス制御では、あらゆるタイプのトラフィックによる KX II へのアクセスが制限されるので、NTP サーバ、RADIUS ホスト、DNS ホストなどは、KX II へのアクセスが許可されている必要があります。

グローバル アクセス制御リスト (ACL) の設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することのないようにします。IP アクセス制御はグローバルに作用し、KX II 全体に影響しますが、グループ レベルで KX II へのアクセスを制御することもできます。グループ レベルの制御の詳細については、「*グループ ベースの IP アクセス制御リスト 『152*p. の*"グループベースの IP ACL (アクセス制御リスト)"*参照 』」を参照してください。

重要: KX II のローカル ポートでは、IP アドレス 127.0.0.1 が使用されます。IP アクセス制御リストを作成する際に、ブロックされる IP アドレス範囲に 127.0.0.1 を含めないでください。そうしなければ、KX II ローカル ポートにアクセスできなくなります。

IP アクセス制御機能を利用するには

1. [Security] (セキュリティ) の [IP Access Control] (IP アクセス制御) を選択すると、[IP Access Control] (IP アクセス制御) ページが開きます。
2. [Enable IP Access Control] (IP アクセス制御を有効にする) チェックボックスをオンにし、このページの他のフィールドを有効にします。
3. [Default policy] (デフォルト ポリシー) ボックスの一覧で値を選択します。これは、指定した範囲内にない IP アドレスに対して実行されるアクションです。
   - [ACCEPT] (許可): 指定した範囲内にない IP アドレスから KX II へのアクセスを許可します。
   - [Drop] (拒否): 指定した範囲内にない IP アドレスから KX II へのアクセスを拒否します。

ルールを一覧の末尾に追加するには

1. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。

   注: IP アドレスは Classless Inter-Domain Routing (CIDR) 方式で入力してください。つまり、先頭の 24 ビットをネットワーク アドレスとして使用します。

2. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
3. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。

ルールを一覧の途中に挿入するには

1. ルール番号を入力します。ルールを一覧の途中に挿入する場合、ルール番号は入力必須です。
2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号と同じルール番号のルールが存在する場合、新しいルールはそのルールの上に挿入され、以降のすべてのルールが 1 行下に下がります。

ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

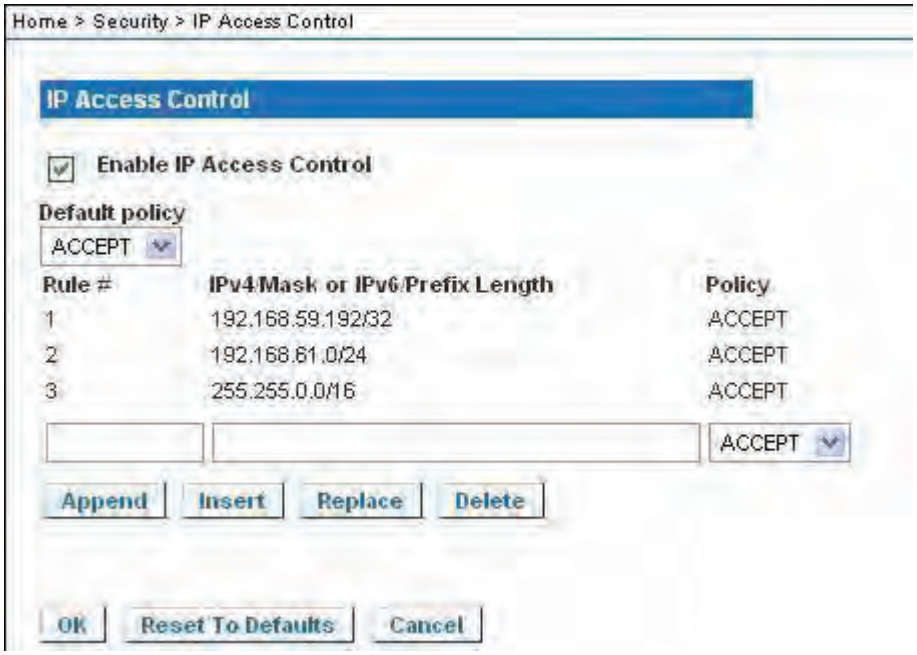
ルールの内容を置換するには

1. 置換したいルールのルール番号を入力します。

2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Replace] (置換) をクリックします。同じルール番号の既存ルールが、新しいルールに置き換わります。

ルールを削除するには

1. 削除したいルールのルール番号を入力します。
2. [Delete] (削除) をクリックします。
3. 削除してよいかどうかを確認するダイアログ ボックスが開きます。[OK] (OK) をクリックします。



SSL 証明書

KX II では、接続先クライアントとの間で送受信されるトラフィックを暗号化するために Secure Sockets Layer (SSL) が使用されます。KX II とクライアントとの接続を確立する際、暗号化された証明書を使用して、KX II の正当性をクライアントに示す必要があります。

KX II 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって署名された証明書をインストールすることができます。CA はまず、CSR 発行元の身元情報を検証します。続いて、署名された証明書を発行元に返します。有名な CA によって署名されたこの証明書は、証明書発行者の身元を保証する目的で使用されます。

重要: KX II の日付と時刻が正しく設定されていることを確認します。

自己署名証明書が作成されると、KX II の日付と時刻を使用して、有効期間が計算されます。KX II の日付と時刻が正確でない場合、証明書の有効な日付範囲が正しくなくなり、証明書の検証に失敗するおそれがあります。「*日付/時刻の設定 『193p. 』*」を参照してください。

注: CSR は、KX II で生成する必要があります。

注: ファームウェアをアップグレードしても、アクティブな証明書および CSR は置き換えられません。

▶ SSL 証明書を作成してインストールするには

1. [Security] (セキュリティ) メニューの [Security Certificate] (セキュリティ証明書) をクリックします。
2. 次の各フィールドの値を指定します。
   a. [Common name] (共通名) - KX II をネットワークに追加したときに指定した、KX II のネットワーク名。通常は完全修飾ドメイン名です。共通名は、Web ブラウザで KX II にアクセスする際に使用する名前から、プレフィックスである「http://」を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合は、HTTPS を使用して KX II にアクセスする際に、ブラウザでセキュリティ警告が表示されます。
   b. [Organizational unit] (組織内部門): KX II が属する、組織内の部門。
   c. [Organization] (組織): KX II が属する組織。
   d. [Locality/City] (市区町村): 組織が存在する市区町村。
   e. [State/Province] (都道府県): 組織が存在する都道府県。
   f. [Country (ISO code)] (国 (ISO コード)): 組織が存在する国。2 文字の ISO コードを入力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」と入力します。

g. [Challenge Password] (チャレンジ パスワード): 一部の CA は、証明書が失効した場合などに証明書の変更を許可するための、チャレンジ パスワードを要求します。必要に応じて、パスワードを入力します。

h. [Confirm Challenge Password] (チャレンジ パスワードの確認入力): 確認のためチャレンジ パスワードを再度入力します。

i. [Email] (電子メール): KX II とそのセキュリティを担当する人の電子メール アドレス。

j. [Key length (bits)] (キー長 (単位: ビット)): 生成されるキーの長さ (単位: ビット)。デフォルト値は [1024] (1024) です。

3. 以下のいずれかの手順に従います。

a. 自己署名証明書を生成する必要がある場合は、[Create a Self-Signed Certificate] (自己署名証明書の作成) チェックボックスをオンにします。このオプションを選択すると、入力内容に基づいて証明書が生成され、KX II が署名証明機関として機能します。CSR をエクスポートして署名入り証明書の生成に使用する必要はありません。

b. 有効期限の日数を指定します。KX II の日付と時刻が正しいことを確認し、正しくない場合は、有効な日付を使用して、証明書の有効期限を作成できます。

c. [Create] (作成) をクリックします。

d. 確認ダイアログ ボックスが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

e. KX II を再起動して CSR を有効にします。

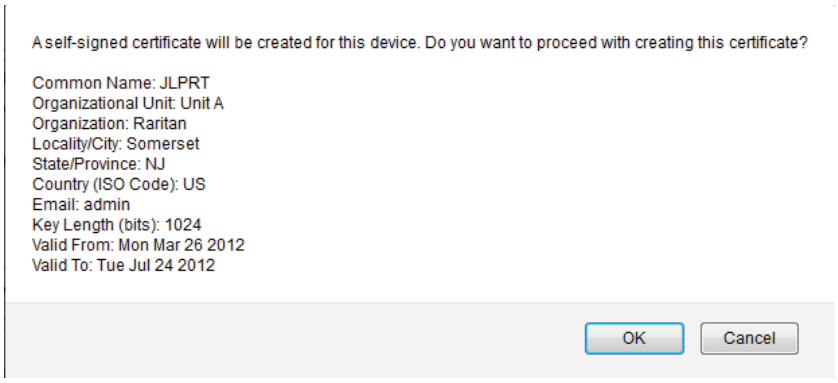
または

f. 有効期限の日数を指定します。KX II の日付と時刻が正しいことを確認し、正しくない場合は、有効な日付を使用して、証明書の有効期限を作成できます。

g. [Create] (作成) をクリックします。

h. 入力したすべての情報および証明書の有効期限を示すダイアログ ボックスが表示されます。情報が正しい場合は、[OK] をクリックして CSR を生成します。

i. KX II を再起動して CSR を有効にします。



CSR 証明書をダウンロードするには

1. CSR、および、CSR 生成時に使用された秘密鍵を含むファイルをダウンロードするには、[Download] (ダウンロード) をクリックします。

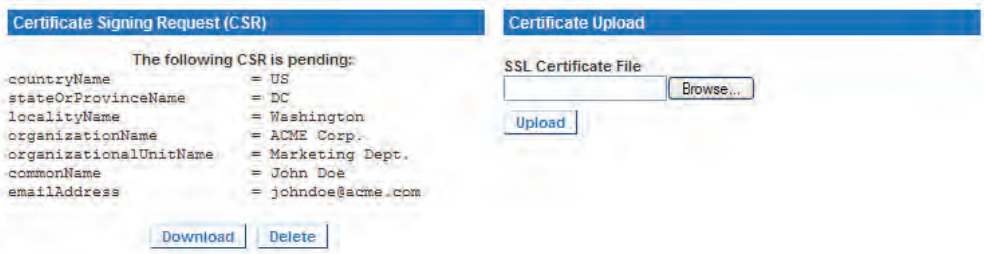
   注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。

2. 証明書を取得するため、保存されている CSR を CA に送信します。CA から新しい証明書が届きます。

自己署名証明書をアップロードするには、以下の手順に従います。

1. 証明書を KX II にアップロードするには、[Upload] (アップロード) をクリックします。

   注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。



この 3 つの手順が完了すると、KX II 専用の証明書が入手されます。この証明書は、KX II の身元をクライアントに対して示す際に使用されます。

重要: KX II 上の CSR を破棄した場合、復旧する方法はありません。誤って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

セキュリティ バナー

KX II ログイン プロセスにセキュリティ バナーを追加できます。この機能により、ユーザは、KX II にアクセスできるようになる前に、セキュリティ同意書に同意するかどうかの選択を求められます。セキュリティ バナーの内容は、ユーザが自分のログイン資格情報を使用して KX II にアクセスした後、[Restricted Service Agreement] (制限付きサービス同意書) ダイアログ ボックスに表示されます。

セキュリティ バナーの見出しおよび本文はカスタマイズできます。デフォルトのテキストをそのまま使用することもできます。また、セキュリティ バナーは、ユーザがセキュリティ同意書に同意してからでないと KX II にアクセスできないように設定することも、単にログイン プロセス終了後に表示することもできます。同意/不同意機能が有効になっている場合、ユーザが選択した内容が監査ログに記録されます。

▶ セキュリティ バナーを設定するには

1. [Security] (セキュリティ) — [Banner] (バナー) をクリックし、[Banner] (バナー) ページを開きます。
2. [Display Restricted Service Banner] (制限付きサービス バナーを表示する) チェック ボックスをオンにし、この機能を有効にします。
3. ユーザがセキュリティ バナーに同意してからでないとログイン プロセスを続行できないようにするには、[Require Acceptance of Restricted Service Banner] (制限付きサービス バナーに対する同意を義務付ける) チェック ボックスをオンにします。ユーザがセキュリティ バナーに同意するには、チェック ボックスをオンにします。この設定を有効にしない場合、ユーザがログインした後にセキュリティ バナーが表示されるだけであり、ユーザがセキュリティ バナーに同意する必要はありません。
4. 必要があれば、バナー タイトルをカスタマイズします。この情報は、バナーの一部としてユーザに対して表示されます。最大 64 文字まで使用できます。
5. [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックス内のテキストをカスタマイズします。入力できるテキストは最大 6,000 文字です。直接入力する方法と、テキスト ファイルからアップロードする方法があります。次のいずれかの手順を実行します。

a. このボックス内のテキストを手動で編集します。[OK] (OK) をクリックします。

b. .txt ファイル内のテキストをアップロードします。具体的には、[Restricted Services Banner File] (制限付きサービス バナー ファイル) を選択し、[Browse] (参照) をクリックしてファイルを探し、アップロードします。[OK] (OK) をクリックします。ファイルがアップロードされると、そのファイル内のテキストが [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックスに表示されます。

注: ローカル ポートからテキスト ファイルをアップロードすることはできません。

Ch 10 保守

この章の内容

[Audit Log] (監査ログ) 283
[Device Information] (デバイス情報) 284
バックアップと復元 286
[USB Profile Management] (USB プロファイルの管理) 288
CIM アップグレード 290
[Upgrading Firmware] (ファームウェアのアップグレード) 290
アップグレード履歴 293
KX II の再起動 293
CC-SG 管理の終了 295

[Audit Log] (監査ログ)

KX II のシステム イベントに関するログが作成されます。監査ログは最大で約 2K 分のデータを保持でき、これを超えると最も古いエントリから上書きされます。監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、[Device Settings] (デバイス設定) の [Event Management] (イベント管理) ページから設定します。 監査ログおよび Syslog でキャプチャされる内容については、「*監査ログおよび Syslog でキャプチャされるイベント 『367*p. 』」を参照してください。

KX II の監査ログを表示するには

1. [Maintenance] (保守) メニューの [Audit Log] (監査ログ) をクリックします。[Audit Log] (監査ログ) ページが開きます。

   [Audit Log] (監査ログ) ページでは、日時順にイベントが表示されます (最も新しいイベントが先頭に表示されます)。監査ログに含まれる情報は次のとおりです。

   - [Date] (日時): イベントが発生した日時 (24 時間形式)。
   - [Event] (イベント): [Event Management] (イベント管理) ページに一覧表示されるイベント名。
   - [Description] (説明): イベントの詳細な説明。

▶ 監査ログを保存するには

注: 監査ログの保存は KX II リモート コンソールでのみ実行できます。KX II ローカル コンソールでは実行できません。

1. [Save to File] (ファイルに保存) をクリックします。[Save File] (ファイルに保存) ダイアログ ボックスが開きます。
2. ファイル名と保存先フォルダを選択し、[Save] (保存) をクリックします。監査ログが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

▶ 監査ログのページ間を移動するには

- [Older] (古いログへ) リンクおよび [Newer] (新しいログへ) リンクを使用します。

[Device Information] (デバイス情報)

[デバイス情報] ページには、使用している KX II デバイスとコンピュータ インタフェース モジュール (CIM) に関する詳細情報が表示されます。これらの情報は、Raritan のテクニカル サポート部門に問い合わせをする際に役立ちます。

▶ KX II と CIM に関する情報を表示するには、以下の手順に従います。

- [保守] メニューの [デバイス情報] をクリックします。[デバイス情報] ページが開きます。

使用している KX II に関する以下の情報が提供されます。

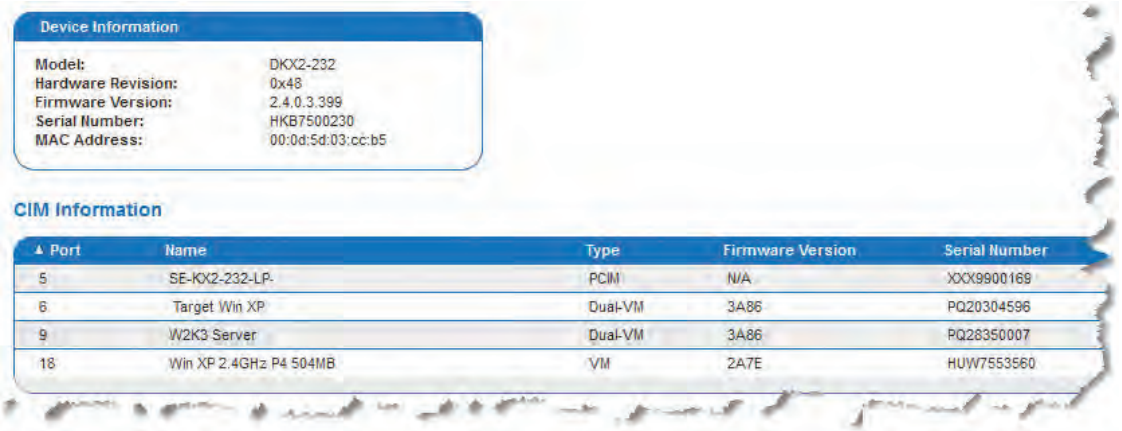
- モデル
- ハードウェア リビジョン
- ファームウェア バージョン
- シリアル番号
- MAC アドレス

CIM に関して表示される情報は次のとおりです。

- [Port] (ポート) (番号)
- [Name] (名前)
- [Type of CIM] (CIM のタイプ) - DCIM、PCIM、ラック PDU、VM、DVM-DP、DVM-HDMI、DVM-DVI
- [Firmware Version] (ファームウェア バージョン)
- [Serial Number of the CIM] (CIM のシリアル番号) - サポートされている CIM からこの番号を直接入手できます。
  - P2CIM-PS2
  - P2CIM-APS2DUAL

- P2CIM-AUSBDUAL
- P2CIM-AUSB
- P2CIM-SUN
- P2CIM-SUSB
- P2CIM-SER
- DCIM-PS2
- DCIM-USB
- DCIM-USBG2
- DCIM-SUN
- DCIM-SUSB
- DVM-DP
- DVM-HDMI
- DVM-DVI

注: DCIM-USB、DCIM-PS2、DCIM-USB G2 の各 CIM の数値部分またはシリアル番号だけが表示されます。たとえば、XXX1234567 が表示されます。フィールドにシリアル番号が設定されている CIM の場合は、シリアル番号プレフィックス GN が表示されます。



Device Information

Model:	DKX2-232
Hardware Revision:	0x48
Firmware Version:	2.4.0.3.399
Serial Number:	HKB7500230
MAC Address:	00:0d:5d:03:cc:b5

CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
5	SE-KX2-232-LP-	PCIM	N/A	XXX9900169
6	Target Win XP	Dual-VM	3A86	PQ20304596
9	W2K3 Server	Dual-VM	3A86	PQ28350007
18	Win XP 2.4GHz P4 504MB	VM	2A7E	HUW7553560

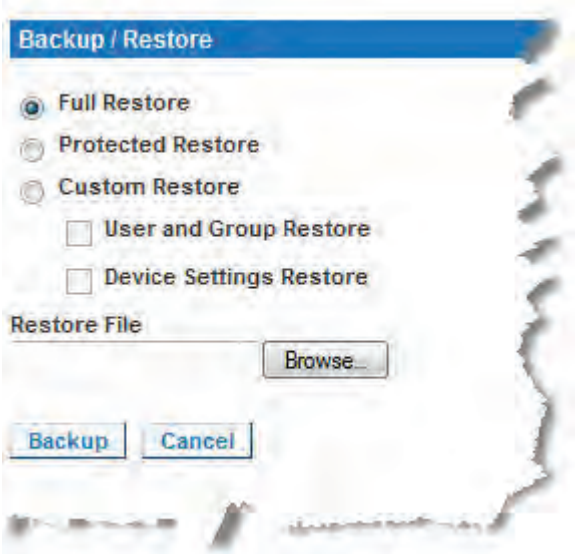
バックアップと復元

［バックアップ/復元］ページでは、KX II の設定情報をバックアップおよび復元できます。

バックアップ/復元機能には、業務継続性を確保するというメリットに加え、時間節約効果もあります。たとえば、使用中の KX II のユーザ設定情報をバックアップして別の KX II に復元することにより、その復元先 KX II をすぐに使用できるようになります。また、1 台の KX II をセットアップし、その設定情報を複数台の KX II にコピーすることもできます。

▶ **[バックアップ/復元] ページを開くには、以下の手順に従います。**

- ［保守］メニューの［バックアップ/復元］をクリックします。［バックアップ/復元］ページが開きます。



注: バックアップ処理では、常にシステム全体がバックアップされます。復元処理では、全体を復元するか一部を復元するかをユーザが選択できます。

▶ **Firefox® または Internet Explorer® 5 以前を使用している場合、KX II をバックアップするには、以下の手順に従います。**

1. ［バックアップ］をクリックします。［ファイルのダウンロード］ダイアログ ボックスが開きます。
2. ［保存］をクリックします。［名前を付けて保存］ダイアログ ボックスが開きます。
3. 保存先フォルダを選択してファイル名を入力し、［保存］をクリックします。［ダウンロードの完了］ダイアログ ボックスが開きます。

4. ［閉じる］をクリックします。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

▶ Internet Explorer 6 以降を使用している場合、KX II をバックアップするには、以下の手順に従います。

1. ［バックアップ］をクリックします。［開く］ボタンを含む［ファイルのダウンロード］ダイアログ ボックスが開きます。［開く］をクリックしないでください。

   IE 6 以降では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように求められます。これを回避するには、ファイルを開くために使用されるデフォルトのアプリケーションをワードパッド® に変更する必要があります。

2. このためには、以下の手順に従います。
   a. バックアップ ファイルを保存します。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
   b. 保存されたら、ファイルを探して右クリックします。［プロパティ］を選択します。
   c. ［全般］タブで［変更］をクリックし、［WordPad］を選択します。

▶ KX II を復元するには、以下の手順に従います。

警告: 使用している KX II を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。つまり、バックアップ時点での管理者のユーザ名とパスワードを覚えていない場合、KX II からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた場合、その IP アドレスも同様に復元されます。IP アドレスの割り当てに DHCP を使用している場合、ローカル ポートにアクセスして復元後の IP アドレスを調べる必要があります。

1. 実行する復元処理のタイプを選択します。
   - ［完全復元］: システム全体を復元します。この復元タイプの主な用途は、一般的なバックアップ/復元処理です。
   - ［部分復元］: デバイス固有情報（例: IP アドレス、名前）以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の KX II をセットアップし、その設定情報を複数台の KX II にコピーするケースなどが考えられます。
   - ［カスタム復元］: この復元タイプを選択した場合、［ユーザとグループの復元］チェック ボックスと［デバイス設定の復元］チェック ボックスのいずれか一方または両方をオンにすることができます。

- [ユーザとグループの復元]: このチェック ボックスをオンにした場合、ユーザ情報とグループ情報だけが復元されます。証明書および秘密鍵ファイルは*復元されません*。別の KX II 上でユーザ情報をセットアップする際に便利です。
- [Device Settings Restore] (デバイス設定の復元): このチェックボックスをオンにした場合、デバイス設定情報 (例: 関連電源、USB プロファイル、ブレード シャーシ関連の設定パラメータ、ポート グループの割り当て) だけが復元されます。デバイス情報をコピーする際に便利です。

2. [参照] をクリックします。[ファイルを選択] ダイアログ ボックスが開きます。
3. 適切なバックアップ ファイルを探して選択し、[開く] をクリックします。選択したファイルが [復元ファイル] ボックスに表示されます。
4. [復元] をクリックします。選択した復元タイプに基づいて、設定情報が復元されます。

[USB Profile Management] (USB プロファイルの管理)

[USB Profile Management] (USB プロファイル管理) ページでは、Raritan のテクニカル サポート部門から提供されたカスタム プロファイル情報をアップロードできます。これらのプロファイルは、標準プロファイルがターゲット サーバ構成のニーズに対応していない場合にそのニーズに対応できるよう、設計されています。Raritan のテクニカル サポート部門は、カスタム プロファイルを提供し、ターゲット サーバ固有のニーズに対する解決策をお客様と一緒に探します。

▶ [USB Profile Management] (USB プロファイル管理) ページを開くには

- [Maintenance] (保守) メニューの [USB Profile Management] (USB プロファイル管理) をクリックします。[USB Profile Management] (USB プロファイル管理) ページが開きます。

▶ カスタム プロファイル情報を KX II にアップロードするには

1. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
2. 適切なカスタム プロファイル ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [USB Profile File] (USB プロファイル ファイル) ボックスに表示されます。
3. [Upload] (アップロード) をクリックします。カスタム プロファイル情報がアップロードされ、プロファイル一覧に表示されます。

注: アップロード処理中にエラーまたは警告が表示された場合 (例: 既存のカスタム プロファイルが上書きされる場合)、アップロード処理を続行するには [Upload] (アップロード)、アップロード処理をキャンセルするには [Cancel] (キャンセル) をクリックします。

▶ カスタム プロファイル情報を KX II から削除するには

1. 削除するカスタム プロファイルのチェック ボックスをオンにします。
2. [Delete] (削除) をクリックします。カスタム プロファイル情報が削除され、プロファイル一覧に表示されなくなります。

アクティブになっているカスタム プロファイルでも削除できます。ただしその場合、確立されていた仮想メディア セッションがすべて終了します。

プロファイル名の競合を処理する

ファームウェアをアップグレードしたとき、カスタム USB プロファイルと標準 USB プロファイルの名前が競合することがあります。たとえば、あるカスタム プロファイルを作成して標準プロファイル リストに組み込んでおり、ファームウェアのアップグレード時に同名の USB プロファイルがダウンロードされた場合などです。

この場合、既存のカスタム プロファイルの名前に old_ というプレフィックスが付加されます。たとえば、GenericUSBProfile5 という名前のカスタム プロファイルが存在しており、かつ、ファームウェアのアップグレード時に同名のプロファイルがダウンロードされた場合、既存のカスタム プロファイルの名前が old_GenericUSBProfile5 に変更されます。

必要に応じて、既存のプロファイルを削除できます。詳細については、「*USB プロファイルの管理 『288*p. の*"[USB Profile Management] (USB プロファイルの管理)"*参照 』」を参照してください。

CIM アップグレード

この項で説明する手順に従って、KX II のメモリに格納されているファームウェア バージョンを基に CIM をアップグレードします。一般に、[ファームウェアのアップグレード] ページを使用してデバイスのファームウェアをアップグレードする場合、すべての CIM がアップグレードされます。

USB プロファイルを使用するには、ファームウェアが最新であるデジタル CIM、D2CIM-VUSB、または D2CIM-DVUSB を使用する必要があります。ファームウェアがアップグレードされていない VM-CIM でもさまざまな構成（Windows®、キーボード、マウス、CD-ROM、およびリムーバブル デバイス）がサポートされていますが、特定の構成に最適なプロファイルを使用することはできません。そのため、USB プロファイルを使用するには、VM-CIM のファームウェアを最新バージョンにアップグレードする必要があります。なお、アップグレードする前でも、"Generic" プロファイルに相当する機能は利用できます。

▶ **KX II のメモリを使用して CIM をアップグレードするには、以下の手順に従います。**

1. [保守] メニューの [CIM ファームウェアのアップグレード] をクリックします。[CIM のアップグレード] ページが開きます。

   [ポート]、[名前]、[タイプ]、[現在の CIM バージョン]、[アップグレード先の CIM バージョン] の各列に情報が表示されるので、各 CIM を簡単に識別できます。
2. アップグレードしたい各 CIM の [選択] チェック ボックスをオンにします。
3. [アップグレード] をクリックします。アップグレードしてもよいかどうかを確認するダイアログ ボックスが開きます。
4. [OK] をクリックしてアップグレード処理を続行します。アップグレード処理中は、進行状況バーが表示されます。アップグレード処理には、CIM ごとに最長で約 2 分かかります。

[Upgrading Firmware] (ファームウェアのアップグレード)

[ファームウェアのアップグレード] ページを使用して、KX II および接続するすべての CIM のファームウェアをアップグレードします。このページは、KX II リモート コンソールでのみ使用できます。

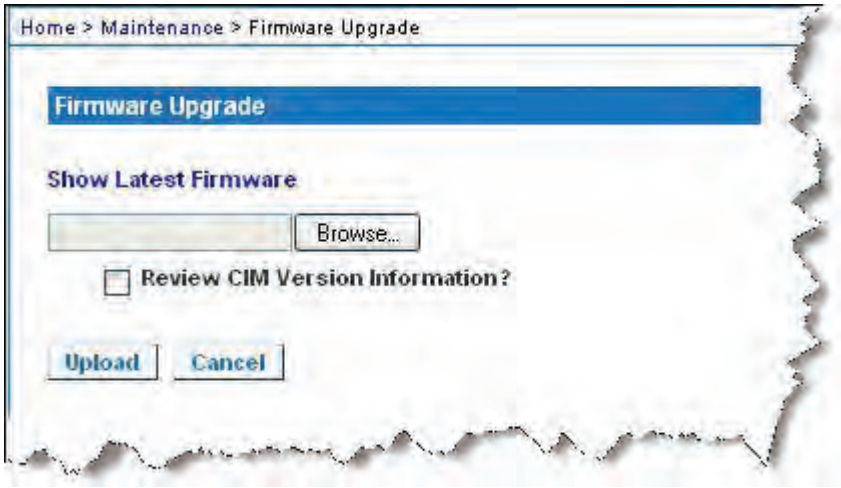
重要: アップグレード処理中に、KX II の電源を切断したり CIM を取り外したりしないでください。KX II または CIM が損傷するおそれがあります。

KX II をアップグレードするには

1. *Raritan の Web サイト http://www.raritan.com* の［ファームウェアのアップグレード］ページで、適切な Raritan ファームウェア配布ファイル（.rfp ファイル）を探してダウンロードします。
2. そのファイルを解凍します。アップグレードを実行する前に、解凍したファイルに記載されている指示をすべてお読みください。

   注: アップグレードを実行する前に、そのファームウェア配布ファイルをローカル PC にコピーしておいてください。また、そのファームウェア配布ファイルをネットワーク ドライブからロードしないでください。

3. ［保守］メニューの［ファームウェアのアップグレード］をクリックします。［ファームウェアのアップグレード］ページが開きます。



4. ［参照］をクリックし、ファームウェア配布ファイルを解凍したフォルダに移動します。
5. 使用している CIM のバージョン情報を表示したい場合、［CIM のバージョン情報を確認する］チェック ボックスをオンにします。
6. ［ファームウェアのアップグレード］ページの［アップロード］をクリックします。アップグレードとバージョン番号に関する情報が、確認のために表示されます。CIM 情報を表示するよう指定した場合は、その情報も表示されます。

   注: この時点で接続していたユーザはログオフされ、新たにログオンしようとしたユーザはブロックされます。

7. ［アップグレード］をクリックします。アップグレード処理が完了するまで待機します。アップグレード処理中は、ステータス情報および進行状況バーが表示されます。アップグレード処理が完了すると、KX II が再起動します。再起動が完了するとビープ音が 1 回鳴ります。

指示に従ってブラウザを終了し、約 5 分待ってから再度 KX II にログオンします。 再度。Multi-Platform Client を使用してデバイスのファームウェアをアップグレードする手順については、『KVM and Serial Access Client Guide』の「Upgrading Device Firmware」を参照してください。

注: モデムを介してファームウェアをアップグレードすることはできません。

注: ティアー接続構成にしており、ベース KX II デバイスから他の複数台のティアー接続デバイスにアクセスしている場合、 ユーザ グループの数が多いと、ファームウェアのアップグレード時にメモリ不足エラーが通知されることがあります。このエラーが通知された場合は、デバイスを再起動し、アップグレード処理を再実行してください。再起動してもこのエラーが解消しない場合は、ベース デバイス上でカスケード接続を無効にしてから、アップグレード処理を再実行してください。

注: ファームウェアをアップグレードしても、アクティブな証明書および CSR は置き換えられません。

アップグレード履歴

KX II および接続されている CIM に対して実行されたアップグレード処理に関する情報を表示できます。

▶ アップグレード履歴を表示するには、以下の手順に従います。

- [保守] メニューの [アップグレード履歴] をクリックします。[アップグレード履歴] ページが開きます。

実行された KX II アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。CIM に関する情報を表示するには、[CIM] 列の [表示] リンクをクリックします。表示される CIM 情報は次のとおりです。

- [タイプ]: CIM のタイプ。
- [ポート]: CIM が接続されているポート。
- [ユーザ]: アップグレード処理を実行したユーザ。
- [IP]: IP アドレス。
- [開始日時]: アップグレード処理の開始日時。
- [終了日時]: アップグレード処理の終了日時。
- [前のバージョン]: アップグレード前の CIM ファームウェア バージョン。
- [アップグレード バージョン]: 現在の CIM ファームウェア バージョン。
- [CIM]: アップグレードされた CIM。
- [結果]: アップグレード処理の結果 (成功または失敗)。

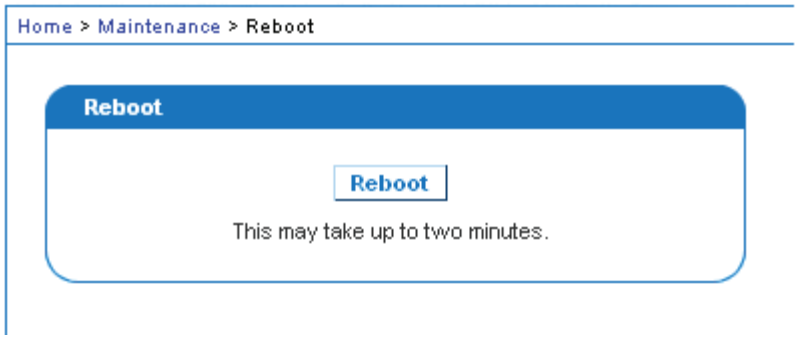
KX II の再起動

[Reboot] (再起動) ページでは、KX II を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

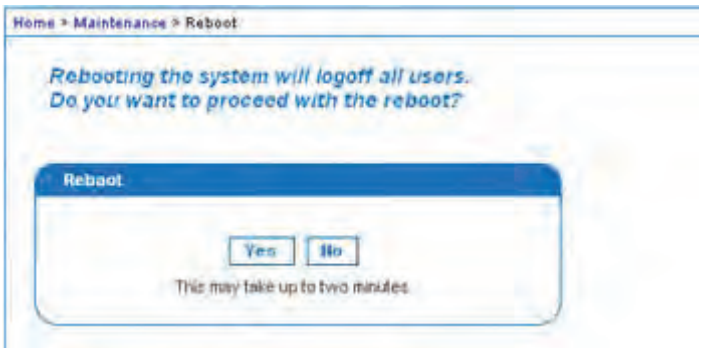
重要: すべての KVM 接続およびシリアル接続が切断され、また、すべてのユーザがログオフされます。

KX II を再起動するには

1. [Maintenance] (保守) メニューの [Reboot] (再起動) をクリックします。[Reboot] (再起動) ページが開きます。



2. [Reboot] (再起動) をクリックします。再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes] (はい) をクリックし、再起動処理を続行します。



CC-SG 管理の終了

KX II が CommandCenter Secure Gateway (CC-SG) の管理下にあるのに、KX II に直接アクセスしようとすると、KX II が CC-SG の管理下にあることを示すメッセージが表示されます。

KX II が CC-SG の管理下にあるが、指定タイムアウト間隔 (通常は 10 分) が経過した後に CC-SG と KX II の間の接続が切断された場合、KX II コンソールから CC-SG 管理セッションを終了できます。

注: KX II を CC-SG の管理対象から除外するには、適切な権限が必要です。また、KX II が現在 CC-SG の管理下にない場合、[Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) コマンドは無効になります。

KX II を CC-SG の管理対象から除外するには、以下の手順に従います。

1. [Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) をクリックします。"KX II が CC-SG の管理下にある" という内容のメッセージが表示されます。また、KX II を CC-SG の管理対象から除外するためのボタンも表示されます。

2. [Yes] (はい) をクリックし、KX II を CC-SG の管理対象から除外する処理を開始します。KX II を CC-SG の管理対象から除外してもよいかどうかを確認するためのメッセージが表示されます。

3. [Yes] (はい) をクリックし、KX II を CC-SG の管理対象から除外します。KX II が CC-SG の管理対象から除外されると、処理完了メッセージが表示されます。

Ch 11 診断

この章の内容

[Network Interface (ネットワーク インタフェース)] ページ 298
[Network Statistics] (ネットワーク統計) ページ 299
[ホストに ping する] ページ 301
[Trace Route to Host (ホストへのルートの追跡)] ページ 301
KX II 診断 303

[Network Interface (ネットワーク インタフェース)] ページ

KX II では、使用しているネットワーク インタフェースのステータスに関する情報が提供されます。

▶ ネットワーク インタフェースに関する情報を表示するには、次の手順に従います。

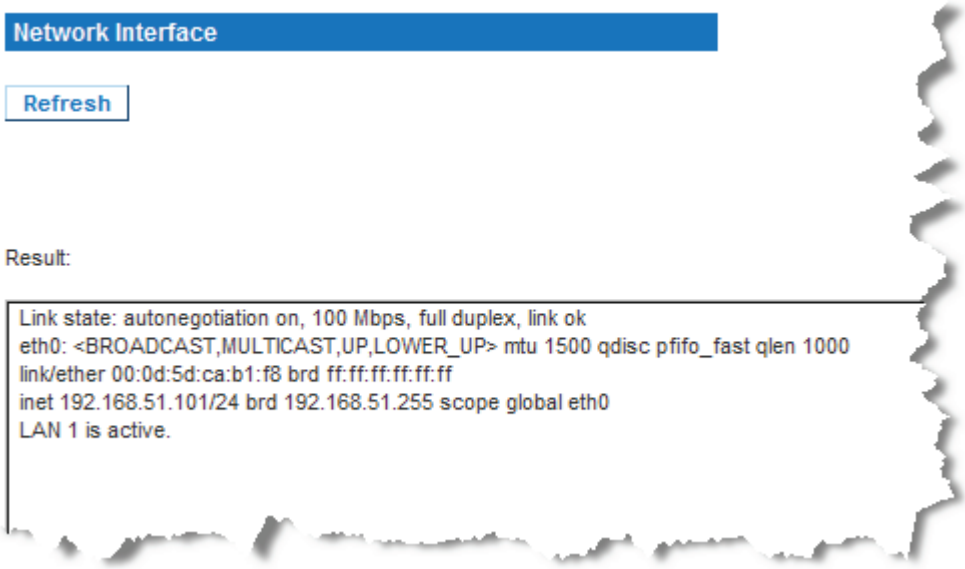
- [Diagnostics (診断)] > [Network Interface (ネットワーク インタフェース)] を選択します。[Network Interface (ネットワーク インタフェース)] ページが開きます。

次の情報が表示されます。

- Ethernet インタフェースが稼働しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

▶ この情報を更新するには、次の手順に従います。

- [Refresh (更新)] をクリックします。



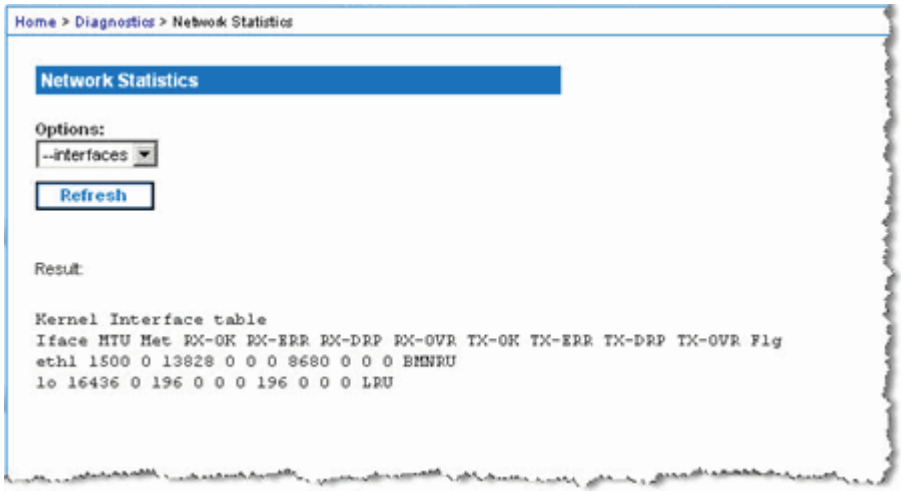
[Network Statistics] (ネットワーク統計) ページ

KX II では、ネットワーク インタフェースに関する統計情報を表示できます。

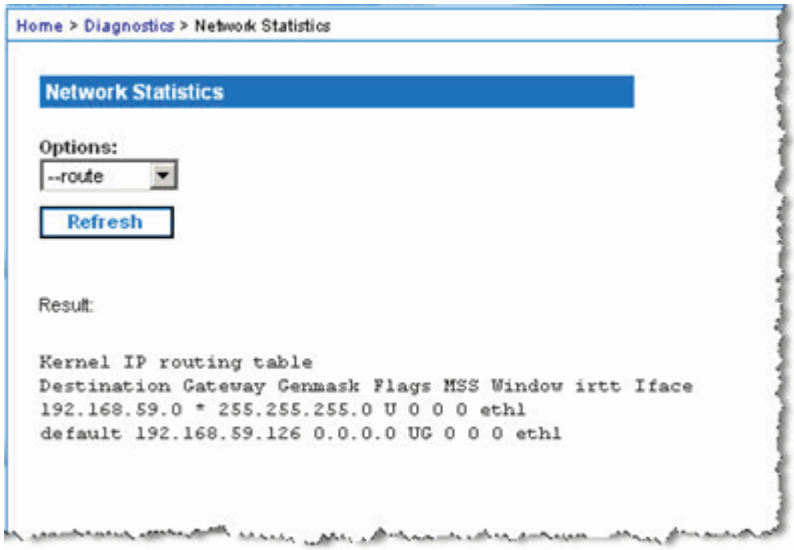
▶ ネットワーク インタフェースに関する統計情報を表示するには

1. [Diagnostics] (診断) メニューの [Network Statistics] (ネットワーク統計) をクリックします。[Network Statistics] (ネットワーク統計) ページが開きます。
2. [Options] (オプション) ボックスの一覧で値を選択します。
   - [Statistics] (統計): 次に示すような情報が表示されます。

- [Interfaces] (インタフェース): 次に示すような情報が表示されます。



- [Route] (経路): 次に示すような情報が表示されます。



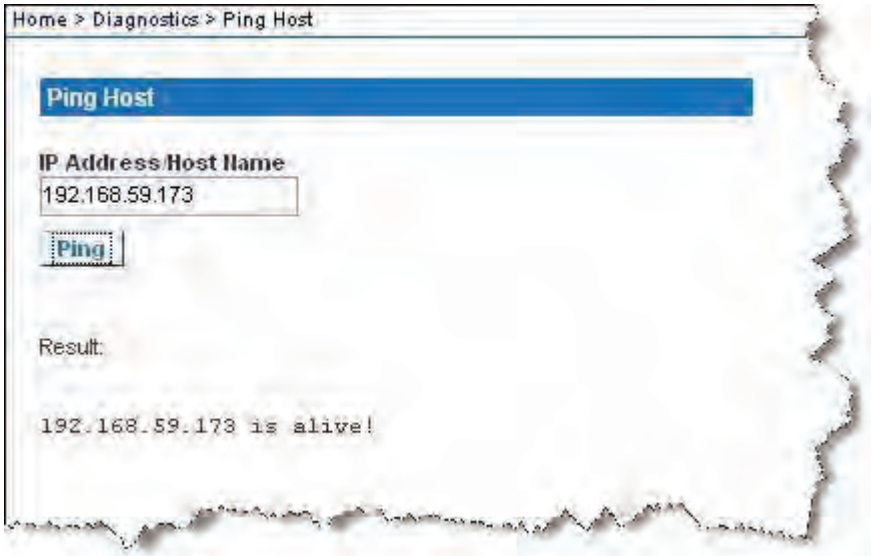
3. [Refresh] (更新) をクリックします。[Options] (オプション) ボックスの一覧で選択した値に応じた情報が、[Result] (結果) フィールドに表示されます。

[ホストに ping する] ページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続可能であるかどうかをテストするためのネットワーク コマンドです。[Ping Host] (ホストに ping する) ページでは、ターゲット サーバまたは別の KX II がアクセス可能であるかどうかを調べることができます。

▶ ホストに ping するには

1. [Diagnostics] (診断) メニューの [Ping Host] (ホストに ping する) をクリックします。[Ping Host] (ホストに ping する) ページが開きます。



2. [IP Address/Host Name] (IP アドレス/ホスト名) ボックスに IP アドレスまたはホスト名を入力します。

   注: ホスト名は 232 文字以内で指定してください。

3. [Ping] (ping) をクリックします。ping の実行結果が [Result] (結果) フィールドに表示されます。

[Trace Route to Host (ホストへのルートの追跡)] ページ

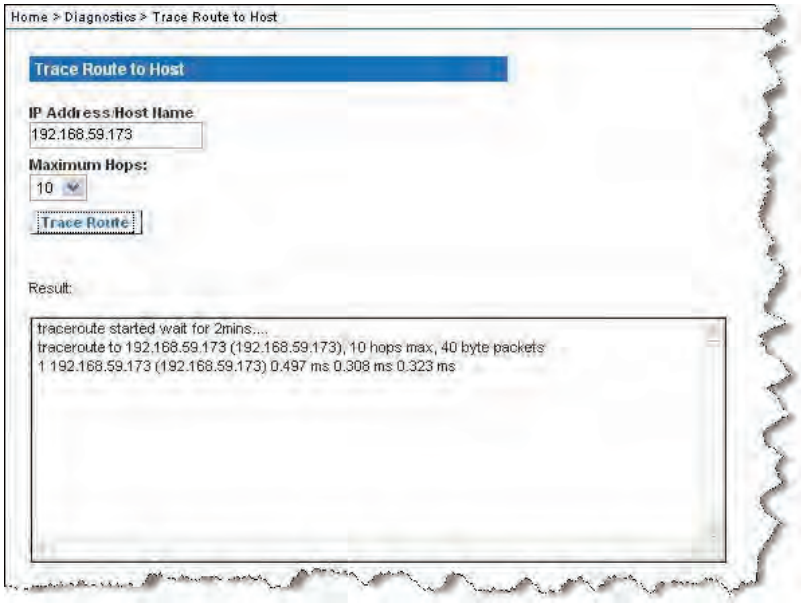
trace route (ルートの追跡) は、指定したホスト名または IP アドレスへのルートを調べるためのネットワーク ツールです。

▶ ホストへのルートを追跡するには、次の手順に従います。

1. [Diagnostics (診断)] > [Trace Route to Host (ホストへのルートの追跡)] を選択します。[Trace Route to Host (ホストへのルートの追跡)] ページが表示されます。
2. [IP Address/Host Name (IP アドレス/ホスト名)] フィールドに IP アドレスまたはホスト名を入力します。

注: ホスト名は最大 232 文字です。

3. ドロップダウン リストから最大ホップ数を選択します (5 刻みで 5 ～ 50)。
4. [Trace Route (ルートの追跡)] をクリックします。指定したホスト名または IP アドレスに対して、trace route コマンドが、指定した最大ホップ数以内で実行されます。trace route の実行結果が [Result (結果)] フィールドに表示されます。



KX II 診断

注: これは、Raritan フィールド エンジニアが使用するためのページです。Raritan のテクニカル サポート部門から指示された場合に限り、ユーザも使用できます。

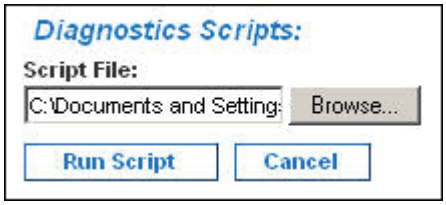
[KX II 診断] ページでは、診断情報を KX II からクライアント コンピュータにダウンロードできます。このページでは、次の 2 種類の処理を行うことができます。

- 重大エラー デバッグ セッション中に、Raritan のテクニカル サポート部門から提供された特別な診断スクリプトを実行する。このスクリプトは、KX II にアップロードされ、実行されます。このスクリプトの実行が完了した後、[ファイルに保存] 機能を使用して診断メッセージをダウンロードできます。
- 診断メッセージのスナップショットに対するデバイス診断ログを、KX II からクライアント コンピュータにダウンロードする。このダウンロードされたデバイス診断ログは暗号化ファイルであり、Raritan のテクニカル サポート部門に送信されます。このファイルを解析できるのは Raritan だけです。

注: このページを開くことができるのは、管理者権限を持つユーザだけです。

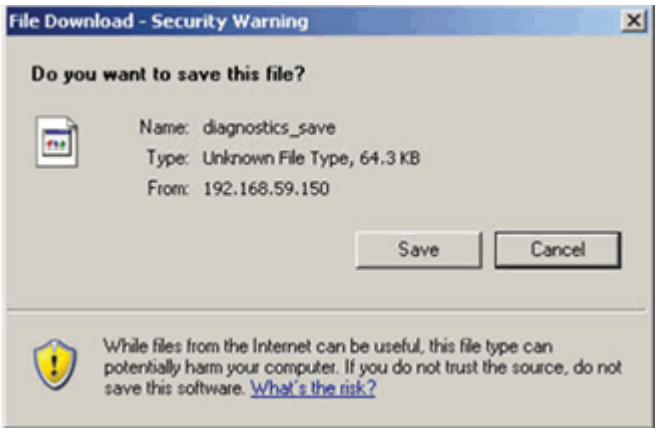
KX II のシステム診断を実行するには、以下の手順に従います。

1. [診断] メニューの [KX II 診断] をクリックします。[KX II 診断] ページが開きます。
2. Raritan のテクニカル サポート部門から電子メールで受け取った診断スクリプト ファイルを実行するため、次の手順を実行します。
   a. Raritan から提供されている診断スクリプト ファイルを入手します。圧縮されている場合は解凍します。
   b. [参照] をクリックします。[ファイルを選択] ダイアログ ボックスが開きます。
   c. 診断スクリプト ファイルを探して選択します。
   d. [開く] をクリックします。診断スクリプト ファイルの名前が [スクリプト ファイル] ボックスに表示されます。



   e. [スクリプトを実行] をクリックします。この診断スクリプト ファイルを Raritan のテクニカル サポート部門に送信します。

3. 診断ファイルを作成して Raritan のテクニカル サポート部門に送信するため、次の手順を実行します。
   a. ［ファイルに保存］をクリックします。［ファイルのダウンロード］ダイアログ ボックスが開きます。



   b. ［保存］をクリックします。［名前を付けて保存］ダイアログ ボックスが開きます。
   c. 保存先フォルダに移動し、［保存］をクリックします。
   d. Raritan のテクニカル サポート部門の指示に従って、このファイルを E メールで送信します。

Ch 12 コマンド ライン インタフェース (CLI)

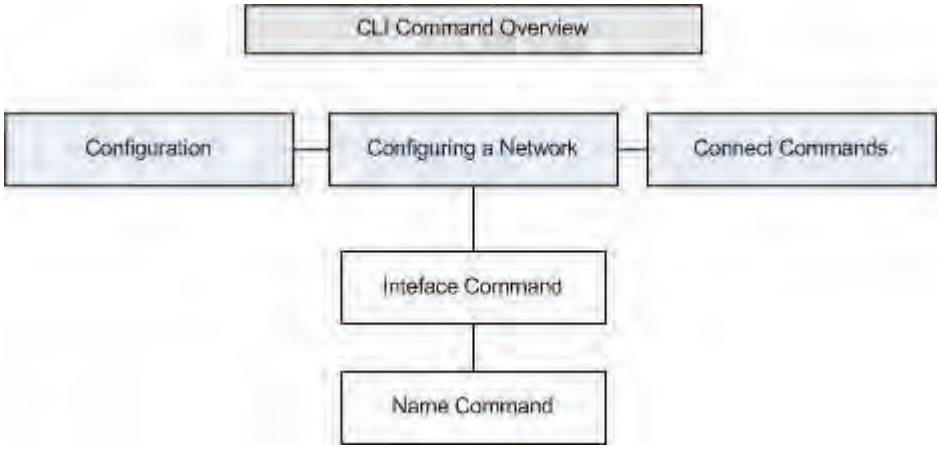
この章の内容

概要 305
CLI を使用しての KX II へのアクセス 306
KX II への SSH 接続 306
ログイン 307
CLI の画面操作 307
CLI を使用した初期設定 309
CLI プロンプト 310
CLI コマンド 310
KX II コンソール サーバ設定用コマンドを使用する 311
ネットワークを設定する 312

概要

KX II のネットワーク インタフェースを設定する権限や診断処理を実行する権限を持っている場合、コマンド ライン インタフェース (CLI) を使用してそれらの処理を実行できます。

次の図に CLI コマンドの概要を示します。コマンドの一覧については、「*CLI コマンド 『310p. 』*」を参照してください。この一覧には、各コマンドの説明、および、各コマンドの記述例が書かれている項へのリンクがあります。



top、history、log off、quit、show、help の各コマンドは、この図のどの CLI レベルからでも使用できます。

CLI を使用しての KX II へのアクセス

次の方法のいずれかを使用して、KX II にアクセスします。

- IP 接続を介した SSH (Secure Shell)

複数の SSH クライアントを使用可能で、次の場所から取得できます。

- Putty: *http://www.chiark.greenend.org.uk/~sgtatham/putty/* *http://www.chiark.greenend.org.uk/~sgtatham/putty/*参照
- ssh.com の SSH クライアント: *www.ssh.com http://www.ssh.com* 参照
- Applet SSH Client: *www.netspace.org/ssh http://www.netspace.org/ssh* 参照
- OpenSSH Client: *www.openssh.org http://www.openssh.org* 参照

KX II への SSH 接続

SSHv2 をサポートする Secure Shell (SSH) クライアントを使用して、KX II に接続します。[Devices Services] (デバイス サービス) ページで SSH 接続を有効にしておく必要があります。

注: セキュリティ上の理由により、SSHv1 接続は KX II でサポートされていません。

Windows PC から SSH で接続する

Windows® PC から SSH セッションを開くには

1. SSH クライアント ソフトウェアを起動します。
2. KX II サーバの IP アドレスを入力します (例: 「192.168.0.192」)。
3. SSH を選択します。SSH では、デフォルトの設定ポート 22 が使用されます。
4. [Open] (開く) をクリックします。

`login as:` (ログイン) プロンプトが表示されます。

「*ログイン 『307*p. 』」を参照してください。

UNIX/Linux ワークステーションから SSH で接続する

▶ **UNIX®/Linux® ワークステーションから SSH セッションを開き、ユーザ admin としてログオンするため、次のコマンドを入力します。**

```
ssh -l admin 192.168.30.222
```

パスワードの入力を求めるプロンプトが表示されます。

「*ログイン* 『*307*p. 』」を参照してください。

ログイン

▶ **ログインするには、次のようにユーザ名 admin を入力します。**

1. admin としてログインします。
2. パスワードの入力を求めるプロンプトが表示されます。デフォルトパスワード（*「raritan」*）を入力します。

   歓迎メッセージが表示されます。これで、管理者としてログオンしたことになります。

次項「*CLI の画面操作* 『*307*p. 』」の内容を確認した後、初期設定処理を実行します。

CLI の画面操作

CLI を使用する前に、CLI の画面操作と構文について理解しておくことが重要です。また、CLI の使用を簡素化するキー入力の組み合わせについても、理解しておく必要があります。

コマンドのオート コンプリート

CLI にはオート コンプリート機能（コマンドの一部を入力すると、残りの部分が自動入力される機能）が備わっています。先頭の数文字を入力した後、Tab キーを押します。入力した文字列で始まるコマンドの候補が 1 つしかない場合、オート コンプリート機能によって残りの部分が自動入力されます。

- 入力した文字列で始まるコマンドの候補が見つからない場合、そのレベルに対する有効な入力候補が表示されます。
- 入力した文字列で始まるコマンドの候補が複数個見つかった場合、すべての入力候補が表示されます。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、Tab キーを押してコマンドを自動入力します。

CLI 構文: ヒントとショートカット キー

ヒント

- コマンドは、アルファベット順に表示されています。
- コマンドでは、大文字と小文字は区別されません。
- パラメータ名は、アンダスコアを含まない 1 つの単語です。
- コマンドに対して引数を指定しない場合、そのコマンドに対する現在の設定値が指定されていると見なされます。
- コマンドの後ろに疑問符 (?) を指定した場合、そのコマンドに対するヘルプが表示されます。
- 縦線 (|) は、任意指定または必須指定のキーワードまたは引数における、選択肢を意味します。

ショートカット

- 末尾のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、Backspace キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- コマンドを実行するには、Enter キーを押します。
- コマンドの入力中に残りの部分を自動入力するには、Tab キーを押します。たとえば、Admin Port > プロンプトで Conf と入力した後に Tab キーを押すと、`Admin Port > Config >` プロンプトが表示されます。

すべての CLI レベルで使用できるコマンド

次の表に、すべての CLI レベルで使用できるコマンドを示します。これらのコマンドは、CLI の画面操作にも役立ちます。

コマンド	説明
top	CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
history	KX II の CLI で入力した最後の 200 個のコマンドが表示されます。
help	CLI 構文の概要が表示されます。
quit	1 レベル上に戻ります。
logout	ユーザ セッションが終了し、ユーザがログオフされます。

CLI を使用した初期設定

注: この項で説明する、CLI を使用した手順の実行は任意です。KX II ローカル コンソールで同じ設定作業を実行できるからです。詳細については、「最初に行う作業 『18p. の"入門"参照 』」を参照してください。

KX II は、デフォルト値に設定された状態で工場から出荷されます。初めて電源を入れて接続を行う際、次のとおりに基本パラメータ値を設定し、ネットワーク上から KX II に安全にアクセスできるようにする必要があります。

1. 管理者パスワードを再設定します。KX II は、すべてのデバイスに同じデフォルト パスワードが設定された状態で出荷されます。したがって、セキュリティ侵害を回避するため、管理者パスワードをデフォルトの raritan から変更する必要があります。新しいパスワードは、KX II の管理者になるユーザが決めます。
2. IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値を設定し、リモート アクセスできるようにします。

パラメータ値を設定する

パラメータ値を設定するには、管理者権限でログオンする必要があります。CLI 階層の最上位である `username >` プロンプトが表示されます。初期設定を行うため、`admin` と入力します。top コマンドを入力し、最上位レベルに戻ります。

注: admin 以外のユーザ名でログオンした場合、admin の代わりにそのユーザ名が表示されます。

ネットワーク パラメータの設定

ネットワーク パラメータ値を設定するには、interface コマンドを使用します。

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

このコマンドが受け付けられると、KX II との接続が自動切断されます。新たに設定した IP アドレス、および、「パラメータ値を設定する」で作成したユーザ名とパスワードを使用して、KX II に再接続します。

重要: パスワードを忘れてしまった場合は、KX II の背面にあるリセットボタンを押し、出荷時設定に戻す必要があります。この場合、初期設定作業を再度実行する必要があります。

これで KX II の基本情報が設定されたので、SSH またはグラフィカル ユーザ インタフェース (GUI) を使用してリモート アクセスすることや、ローカル シリアル ポートを使用してローカル アクセスすることができます。管理者は、ユーザ、グループ、サービス、セキュリティ、およびシリアル ポートを設定する必要があります。シリアル ポートは、シリアル ターゲットを KX II に接続するためのポートです。

CLI プロンプト

CLI プロンプトは、現在のコマンド レベルを意味しています。プロンプトのルート部分はログオン名です。端末エミュレーション ソフトウェアを使用して管理用シリアル ポートに直接接続している場合、コマンドのルート部分は Admin Port になります。

```
admin >
```

CLI コマンド

- `admin > help` と入力した場合に使用できるコマンドは、次のとおりです。

コマンド	説明
config	config サブメニューに切り替えます。
diagnostics	diag サブメニューに切り替えます。
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
listports	使用可能なポートを一覧表示します。
logout	現在の CLI セッションを終了し、ログオフします。
top	ルート メニューに戻ります。
userlist	アクティブなユーザ セッションを一覧表示します。

- 「admin > config > network」と入力します。

コマンド	説明
help	コマンドの概要を表示します。
history	現在のセッションのコマンド ライン履歴を表示します。
interface	ネットワーク パラメータ値を取得および設定します。
ipv6_interface	IPv6 のネットワーク パラメータ値を取得および設定します。
logout	現在の CLI セッションを終了し、ログオフします。
name	デバイス名を設定します。
quit	前のメニューに戻ります。
stop	ルート メニューに戻ります。

セキュリティ上の問題

コンソール サーバにおけるセキュリティを確保する際に検討すべき点は、次のとおりです。

- 運用担当者用コンソールと KX II との間で送受信されるデータ トラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- セキュリティ プロファイルを設定する。

KX II にはこの 3 つの機能がすべて備わっています。ただし、設定作業は運用開始前に済ませておく必要があります。

KX II コンソール サーバ設定用コマンドを使用する

注: SSH 接続とローカル ポート接続では、CLI コマンドは同じです。

network コマンドは、Configuration メニューで使用できます。

ネットワークを設定する

network メニューのコマンドを使用して、KX II のネットワーク インタフェースを設定します。

コマンド	説明
interface	KX II のネットワーク インタフェースを設定します。
name	ネットワーク名を設定します。
ipv6	IPv6 のネットワーク パラメータ値を取得および設定します。

interface コマンド

interface コマンドを使用して、KX II のネットワーク インタフェースを設定します。interface コマンドの構文は次のとおりです。

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]
Ethernet パラメータ値を設定/取得します。
ipauto <none|dhcp>: IP アドレスを自動設定するかどうか
(none/dhcp)。
ip <ipaddress>: IP アドレス。
mask <subnetmask>: サブネット マスク。
gw <ipaddress>: デフォルト ゲートウェイ。
mode <mode>: Ethernet モードを設定
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)。
```

interface コマンドの例

次のコマンドを実行すると、インタフェース番号 1 が有効になり、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値が設定され、Ethernet モードが自動検出に設定されます。

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

name コマンド

name コマンドを使用して、ネットワーク名を設定します。name コマンドの構文は次のとおりです。

```
name [devicename <devicename>] [hostname <hostname>]
```

デバイス名の設定

```
devicename <devicename>: デバイス名。
hostname <hostname>: 優先ホスト名 (DHCP 使用時のみ)。
```

name コマンドの例

次のコマンドを実行すると、ネットワーク名が設定されます。

```
Admin > Config > Network > name devicename My-KSX2
```

ipv6 コマンド

ipv6 コマンドを使用して、IPv6 関連のネットワーク パラメータ値の設定と取得を行います。

Ch 13 KX II ローカル コンソール

この章の内容

概要 314
ユーザが同時接続可能 314
KX II ローカル コンソール インタフェース: KX II デバイス 315
セキュリティと認証 315
有効な解像度 316
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ) 317
ターゲット サーバにアクセスする 318
ポートのスキャン - ローカル コンソール 318
ローカル コンソールのスマート カード アクセス 321
ローカル コンソールの USB プロファイル オプション 323
ホット キーと接続キー 324
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ 325
KX II ローカル コンソールの画面に切り替える 326
ローカル ポートの管理 326
スクリプトの接続と切断 333
リセット ボタンを使用して KX II をリセットする 337

概要

KX II のローカル ポートにコンピュータを接続して KX II ローカル コンソールを使用することにより、設置場所で管理作業を行うことができます。この KX II ローカル コンソールの特徴は、ブラウザを使用する、という点であり、サーバをすばやく切り替えることができます。KX II ローカル コンソールでは、KX II に接続されているサーバのキーボード ポート、マウス ポート、およびビデオ ポートに直接接続している場合と同等のパフォーマンスが得られます。また、KX II ローカル コンソールには、KX II リモート コンソールと同等の管理機能が備わっています。

ユーザが同時接続可能

KX II ローカル コンソールを使用する場合、接続されている各 KVM ターゲット サーバへの独立したアクセス パスが設定されます。つまり、KX II ローカル コンソールを使用している最中でも、他ユーザがネットワーク経由で KX II に同時接続できます。また、リモート ユーザが KX II に接続している最中でも、KX II ローカル コンソールを使用してラックからサーバに同時接続できます。

KX II ローカル コンソール インタフェース: KX II デバイス

サーバ ラックに設置した KX II の場合は、KX II ローカル コンソールを介して、標準 KVM 管理を行います。KX II ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。

KX II ローカル コンソールと KX II リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

[KX II Local Console Factory Reset] (KX II ローカル コンソール ファクトリ リセット) オプションは、KX II ローカル コンソールには用意されていますが、KX II リモート コンソールには用意されていません。

セキュリティと認証

KX II ローカル コンソールを使用するには、まず有効なユーザ名とパスワードで認証を受ける必要があります。KX II には認証機能とセキュリティ機能が備わっています。これらの機能は、ネットワークから接続するユーザとローカル ポートから接続するユーザの両方に対して有効です。ユーザは、どちらの方法で接続する場合でも、アクセス権限を持っているサーバにしかアクセスできません。サーバ アクセスとセキュリティに関する設定情報を指定する手順については、「*ユーザ管理* 『*145*p. の *"[User Management] (ユーザ管理)"* 参照 』」を参照してください。

KX II が外部認証サービス (LDAP/LDAPS、RADIUS、または Active Directory) を使用するように設定されている場合、ユーザが KX II ローカル コンソールを使用して接続する際でも、外部認証サービスによって認証が行われます。

注: KX II ローカル コンソールを使用して接続しようとするユーザに対して認証を行わないように、設定することもできます。ただし、この方法は安全な環境でのみ使用することを推奨します。

▶ KX II ローカル コンソールを使用するには

1. キーボード、マウス、およびモニタを、KX II の背面にあるローカル ポートに接続します。
2. KX II を起動します。KX II ローカル コンソール画面が表示されます。

有効な解像度

KX II ローカル コンソールは次の解像度に対応しており、さまざまなモニタで適切に表示されます。

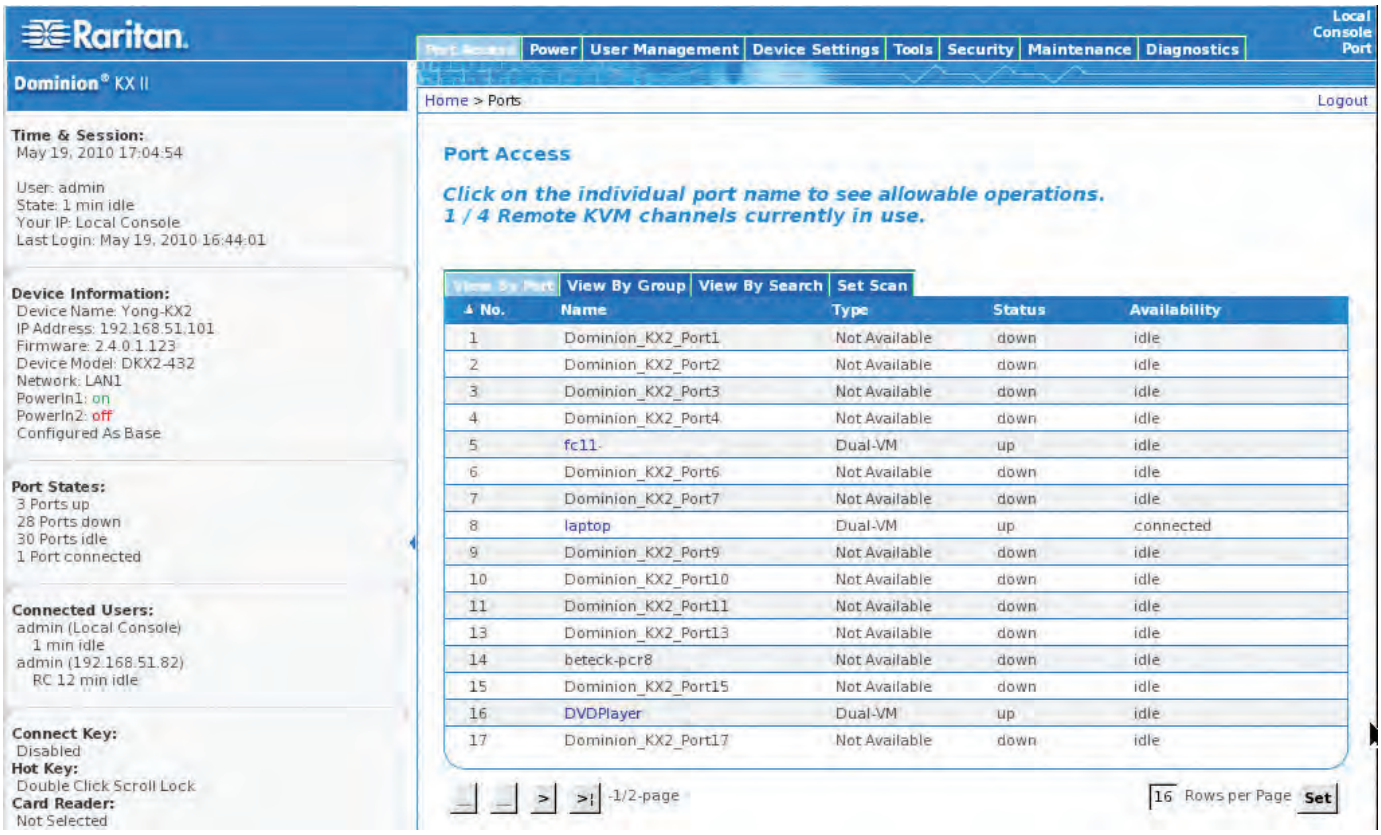
- 800x600
- 1024 x 768
- 1280 x 1024

これらの各解像度について、60 Hz と 75 Hz のリフレッシュ レートがサポートされています。

[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ)

KX II ローカル コンソールにログオンすると、[Port Access] (ポート アクセス) ページが開きます。このページには、KX II のすべてのポート、そうしたポートに接続されているターゲット サーバ、ポート グループ、およびブレード シャーシが一覧表示されます。

リモート コンソールとローカル コンソールのどちらからアクセスしても、[Port Access] (ポート アクセス) ページには同じ情報が表示されます。さらに、このページから同じ方法でターゲットやポート グループにアクセスできます。詳細については、「*[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)* 『*53*p. 』」を参照してください。



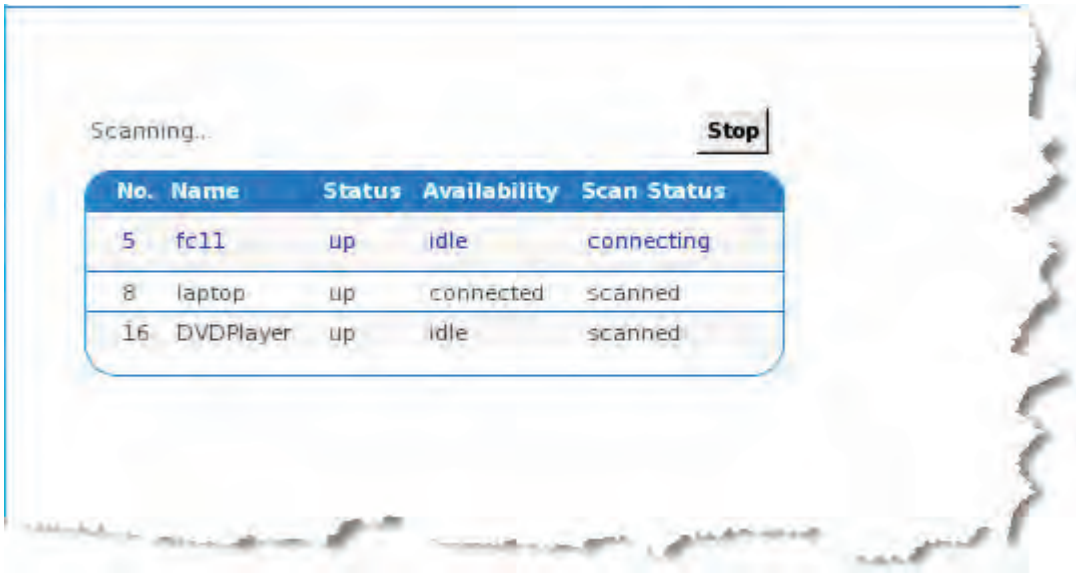
ターゲット サーバにアクセスする

▶ ターゲット サーバにアクセスするには

1. アクセスしたいターゲット サーバのポート名をクリックします。ポート アクション メニューが開きます。
2. ポート アクション メニューの [Connect] (接続) をクリックします。そのターゲット サーバの画面に切り替わります。

ポートのスキャン - ローカル コンソール

KX II のスキャン機能は、ローカル コンソールでサポートされています。スキャンで見つかったターゲットは、1 つずつ [スキャン] ページに表示されます。これは、リモート コンソールのポート スライド ショーとは異なります。各ターゲットがページにデフォルトで 10 秒間表示されるので、ターゲットを確認して接続できます。表示されているターゲットに接続するには、ローカル ポートの ConnectKey シーケンスを使用します。また、そのターゲットから切断するには、DisconnectKey のシーケンスを使用します。



▶ ターゲットをスキャンするには、以下の手順に従います。

1. ローカル コンソールで、[ポート アクセス] ページの [スキャン設定] タブをクリックします。
2. 各ターゲットの横にあるチェックボックスをオンにしてスキャン対象に含めるターゲットを個別に選択するか、ターゲット列の上部にあるチェックボックスをオンにしてすべてのターゲットを選択します。

3. アップ ステータスのターゲットだけをスキャンに含める場合は、[アップのみ] チェックボックスをオンのままにします。アップかダウンかに関係なくすべてのターゲットを含める場合は、このチェックボックスをオフにします。
4. [スキャン] をクリックしてスキャンを開始します。[ポート スキャン] ウィンドウが開きます。ターゲットが見つかるたびに、それがウィンドウに表示されます。
5. ターゲットが表示されたら、ConnectKey シーケンスを使用してそれに接続します。
6. [スキャンの停止] をクリックしてスキャンを停止します。

スキャン オプションの使用

ターゲットのスキャン中は、次のオプションを使用できます。これらのすべてのオプションは、[Expand]（展開）/[Collapse]（折りたたみ）アイコンを除き、[Port Scan]（ポート スキャン）ビューアの左上の [Options]（オプション）メニューから選択します。ウィンドウを閉じると、オプションはデフォルトに戻ります。

*注: Virtual KVM Client（VKC）または Active KVM Client（AKC）から表示間隔などのスキャン設定を指定します。詳細については、「*VKC および AKC でのスキャンの設定 *『98p. 』」を参照してください。*

サムネイルの表示または非表示

- ウィンドウの左上の [Expand]（展開）/[Collapse]（折りたたみ）アイコン を使用して、サムネイルを表示または非表示にします。デフォルト表示では展開されています。

サムネイル スライド ショーの一時停止

- [Options]（オプション）の [Pause]（一時停止）を選択すると、あるターゲットから次のターゲットへのサムネイルのローテーションが一時停止します。サムネイルのローテーションはデフォルト設定です。

サムネイル スライド ショーの再開

- [Options]（オプション）の [Resume]（再開）を選択すると、サムネイルのローテーションが再開されます。

[Port Scan]（ポート スキャン）ビューアのサムネイルのサイズ変更

- サムネイルを拡大するには、[Options]（オプション）、[Size]（サイズ）、[360x240] の順に選択します。
- サムネイルを最小化するには、[Options]（オプション）、[Size]（サイズ）、[160x120] の順に選択します。これはデフォルトのサムネイル サイズです。

[Port Scan]（ポート スキャン）ビューアの表示方向の変更

- [Options]（オプション）、[Split Orientation]（分割方向）、[Horizontal]（横）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの下部に沿って表示されます。
- [Options]（オプション）、[Split Orientation]（分割方向）、[Vertical]（縦）の順に選択すると、サムネイルが [Port Scan]（ポート スキャン）ビューアの右側に沿って表示されます。これがデフォルト表示です。

ローカル コンソールのスマート カード アクセス

ローカル コンソールでスマート カードを使用してサーバにアクセスするには、KX II に搭載されているいずれかの USB ポートを使用して USB スマート カード リーダーを KX II に接続します。スマート カード リーダーは、KX II に接続したり KX II から取り外したりすると、KX II によって自動検出されます。サポートされているスマート カードおよびシステム要件の一覧については、「*サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー* 『*110*p. 』」および「*スマート カードの最小システム要件* 『*357*p. 』」を参照してください。

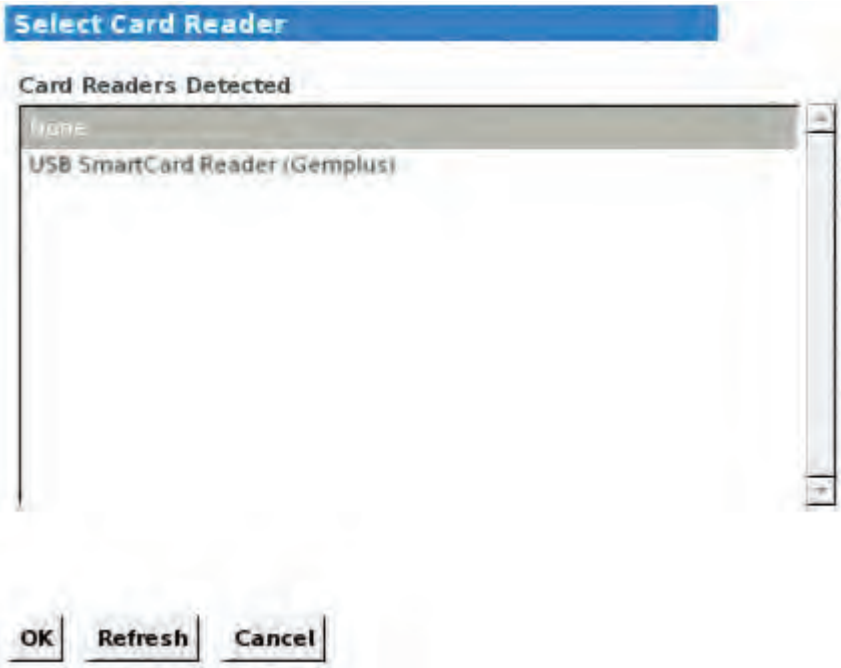
カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

▶ **KX II ローカル コンソールからスマート カード リーダーをターゲットにマウントするには、以下の手順に従います。**

1. デバイスに搭載されているいずれかの USB ポートを使用して、USB スマート カード リーダーを KX II に接続します。接続すると、スマート カード リーダーは KX II によって検出されます。
2. ローカル コンソールで [Tools] (ツール) をクリックします。
3. [Card Reader Detected] (検出されたカード リーダー) リストからスマート カード リーダーを選択します。スマート カード リーダーをマウントしない場合は、リストから [None] (なし) を選択します。
4. [OK] (OK) をクリックします。スマート カード リーダーを追加すると、操作が正常に完了したことを示すメッセージがページに表示されます。ページの左パネルの [Card Reader] (カード リーダー) に、状態として [Selected] (選択) または [Not Selected] (未選択) が表示されます。

▶ **[Card Readers Detected] (検出されたカード リーダー) リストを更新するには、以下の手順に従います。**

- 新しいスマート カードがマウントされた場合は、[Refresh] (更新) をクリックします。[Card Readers Detected] (検出されたカード リーダー) リストが更新され、新しく追加されたスマート カード リーダーが表示されます。



KX2 8xx デバイスでのスマート カード アクセス

KX2-808、KX2-832、または KX2-864 デバイスでローカル コンソールからスマート カード リーダーを使用してサーバにアクセスするには、拡張ローカル ポート ([Local Port Settings] (ローカル ポート設定) ページ) を無効にする必要があります。拡張ローカル ポートでは、スマートカード認証はサポートされません。

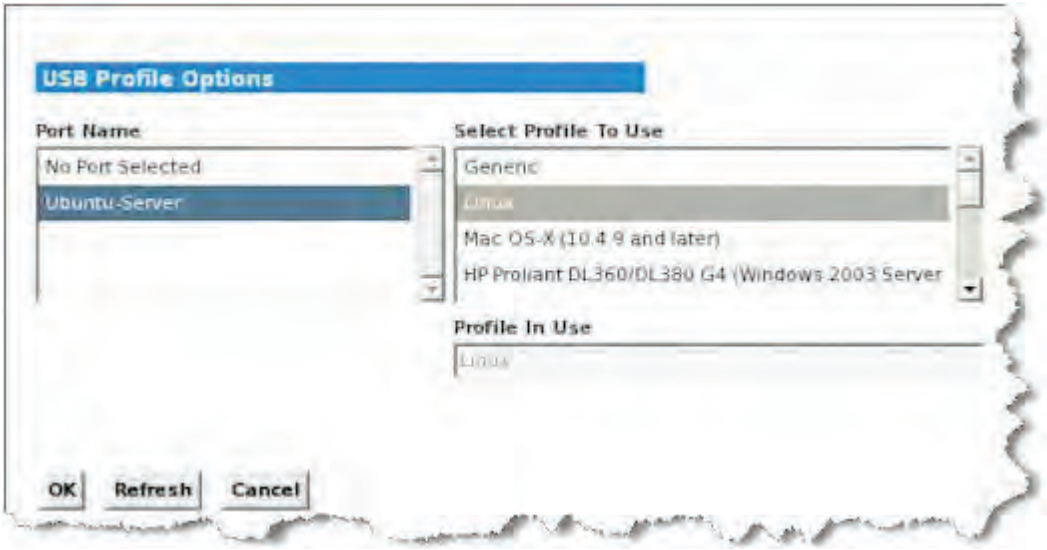
ローカル コンソールの USB プロファイル オプション

[Tools] (ツール) ページの [USB Profile Options] (USB プロファイル オプション) セクションで、USB プロファイルを選択できます。

プロファイルを適用可能なポートが [Port Name] (ポート名) フィールドに表示されます。ポートを選択すると、そのポートに適用可能なプロファイルが [Select Profile To Use] (使用するプロファイルを選択) フィールドに表示されます。ポートに対して選択したプロファイルは、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。

▶ USB プロファイルをローカル コンソール ポートに適用するには

1. [Port Name] (ポート名) フィールドで、USB プロファイルを適用するポートを選択します。
2. [Select Profile To Use] (使用するプロファイルを選択) フィールドで、そのポートに適用するプロファイルを選択します。
3. [OK] (OK) をクリックします。その USB プロファイルがローカルポートに適用され、また、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。



ホット キーと接続キー

KX II ローカル コンソールの画面は、現在アクセスしているターゲット サーバの画面に完全に置き換えられます。ターゲット サーバから切断し、ローカル コンソールの画面に戻るには、ホット キーを使用します。接続キーは、ターゲット サーバに接続したり、ターゲット サーバを切り替えたりする際に使用します。

ターゲット サーバの画面が表示されているときにホットキーを使用することにより、KX II ローカル コンソールの画面をすばやく開くことができます。デフォルトでは、Scroll Lock キーをすばやく 2 回押します。別のキー シーケンスをホットキーとして指定することもできます。指定するには、[ローカル ポート設定] ページを使用します。詳細については、「*KX II ローカル コンソールのローカル ポートの設定* 『*327*p. 』」を参照してください。

接続キーの例

標準型サーバの場合 接続キーを押したときのアクション	キー シーケンスの例
KX II ローカル コンソールからポートに接続する	KX II ローカル コンソールからポート 5 に接続するには • 左 Alt キーを押す → 5 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 からポート 11 に切り替えるには • 左 Alt キーを押す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KX II ローカル コンソールの画面に戻る	ポート 11 から切断し、KX II ローカル コンソールの画面（ターゲット サーバに接続する時に開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す

ブレード シャーシの場合 接続キーを押したときのアクション	キー組み合わせの例
KX II ローカル コンソールからポートに	ポート 5 のスロット 2 に接続するには

標準型サーバの場合 接続キーを押したときのアクション	キー シーケンスの例
接続する	• 左 Alt キーを押す → 5 キーを押して離す → 2 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 のスロット 2 からポート 5 のスロット 11 に切り替えるには • 左 Alt キーを押す → 5 キーを押して離す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KX II ローカル コンソールの画面に戻る	ポート 11 のスロット 11 から切断し、KX II ローカル コンソールの画面（ターゲット サーバに接続する時に開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す

•

Sun サーバへのアクセス時に使用できる特別なキー組み合わせ

ローカル ポートでは、Sun Microsystems™ サーバの特別なキーに対して、次のキー組み合わせが機能します。これらの特別なキー組み合わせは、Sun ターゲット サーバに接続しているときに使用できます。

Sun サーバのキー	ローカル ポートにおけるキー組み合わせ
Again	Ctrl+ Alt +F2
Props	Ctrl+ Alt +F3
Undo	Ctrl+ Alt +F4
Stop A	Break a
Front	Ctrl+ Alt +F5
Copy	Ctrl+ Alt +F6
Open	Ctrl+ Alt +F7
Find	Ctrl+ Alt +F9
Cut	Ctrl+ Alt +F10
Paste	Ctrl+ Alt +F8

Sun サーバのキー	ローカル ポートにおけるキー組み合わせ
Mute	Ctrl+ Alt +F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol –	Ctrl + Alt + KPAD –
Stop	キー組み合わせなし
電力	キー組み合わせなし

KX II ローカル コンソールの画面に切り替える

重要: KX II ローカル コンソールのデフォルトのホットキーは、Scroll Lock キーをすばやく 2 回押すことです。このキー組み合わせを変更するには、[Local Port Settings] (ローカル ポート設定) ページを使用します。「*ローカル コンソールからの KX II ローカル ポートの設定* 『*330*p. 』」を参照してください。

▶ ターゲット サーバの画面から KX II ローカル コンソールの画面に戻るには

- ホットキーを押します (デフォルトでは Scroll Lock キーをすばやく 2 回押す)。ターゲット サーバの画面から KX II ローカル コンソールの画面に切り替わります。

ローカル ポートの管理

KX II を管理するには、KX II ローカル コンソールまたは KX II リモート コンソールを使用します。KX II ローカル コンソールには次のページもあります。

- [Factory Reset] (出荷時設定にリセット)
- [Local Port Settings] (ローカル ポート設定)(KX II リモート コンソールにもある)

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

KX II ローカル コンソールのローカル ポートの設定

[Local Port Settings] (ローカル ポート設定) ページでは、KX II ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

ローカル ポートに関する設定値をカスタマイズするには

注: [Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)
   - [United Kingdom] (イギリス英語)
   - [French (France)] (フランス語 (フランス))
   - [German (Germany)] (ドイツ語 (ドイツ))
   - [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
   - [Simplified Chinese] (簡体字中国語)
   - [Traditional Chinese] (繁体字中国語)
   - [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
   - [German (Switzerland)] (ドイツ語 (スイス))
   - [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
   - [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
   - [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
   - [Danish (Denmark)] (デンマーク語 (デンマーク))
   - [Belgian (Belgium)] (ベルギー語 (ベルギー))

   注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

   注: トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

3. [Local Port Hotkey]（ローカル ポート ホットキー）ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KX II ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock]（Scroll Lock キーを 2 回押す）ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock]（Num Lock キーを 2 回押す）	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock]（Caps Lock キーを 2 回押す）	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key]（左 Alt キーを 2 回押す）	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key]（左 Shift キーを 2 回押す）	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key]（左 Ctrl キーを 2 回押す）	左 Ctrl キーをすばやく 2 回押します。

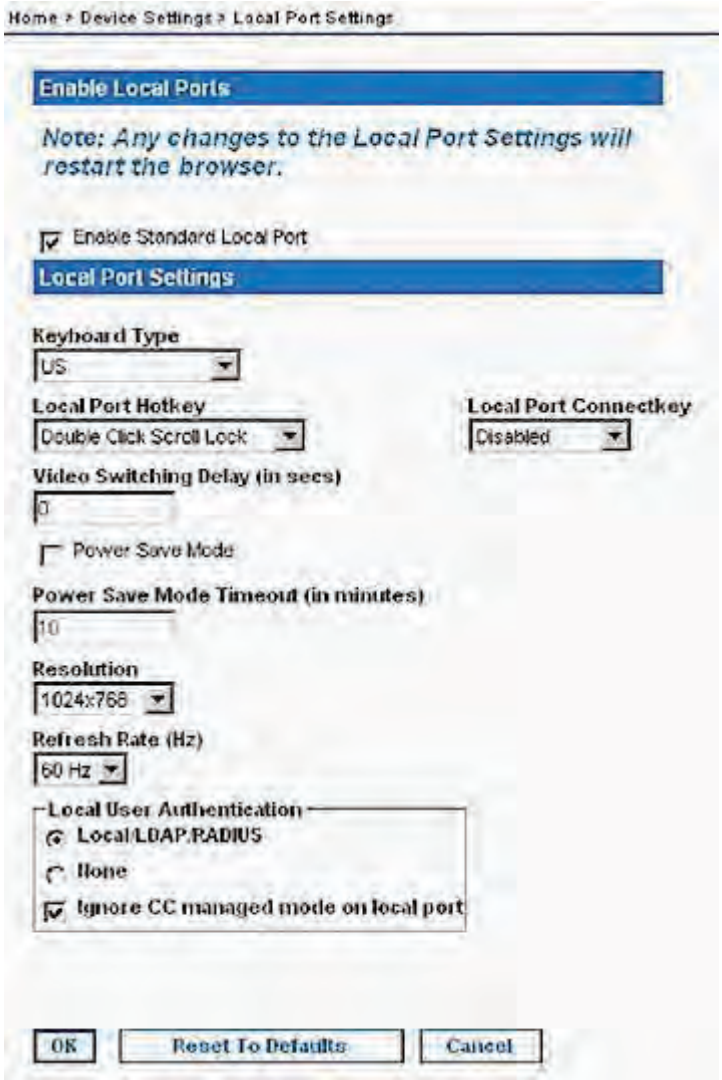
4. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。その後ホットキーを使用して、そのターゲット サーバの画面から KX II ローカル コンソールの画面に戻すことができます。接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー シーケンスの例については、「*接続キーの例『324*p. 』」を参照してください。 接続キーは、標準型サーバとブレード シャーシのどちらに対しても機能します。
5. 必要に応じて、[画面切り替え遅延（秒）] ボックスに 0 ～ 5 秒の範囲の数値を入力します。通常は「0」と入力します。ただし、一部のモニタでは画面切り替えに時間がかかるので、その場合は適切な値を入力します。
6. 省電力機能を利用する場合、次の手順を実行します。
   a. [省電力モード] チェック ボックスをオンにします。
   b. [省電力モードのタイムアウト（分）] ボックスに、省電力モードに移行するまでの時間（単位: 分）を入力します。

7. [解像度] ボックスの一覧で、KX II ローカル コンソールの画面解像度を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
8. [垂直走査周波数 (Hz)] ボックスの一覧で垂直走査周波数を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - 60 Hz
   - 75 Hz
9. [ローカル ユーザ認証] でローカル ユーザ認証タイプを選択します。
   - [ローカル/LDAP/RADIUS]: これは推奨オプションです。認証の詳細については、「*リモート認証* 『*42*p. 』」を参照してください。
   - [なし]: KX II ローカル コンソールからのアクセスに対して認証は行われません。このオプションは、安全な環境でのみ選択することをお勧めします。
   - KX II が CommandCenter Secure Gateway (CC-SG) の管理下にある場合にローカル ユーザを認証するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにします。

注: 最初は [Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオフにしていたが、後でローカル ポートからのアクセスを CC-SG の管理対象から除外したくなった場合、CC-SG 側で KX II を CC-SG の管理対象から除外する必要があります。その後、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにすることができます。

---

10. [OK] (OK) をクリックします。



ローカル コンソールからの KX II ローカル ポートの設定

標準ローカル ポートと拡張ローカル ポートを設定するには、リモートコンソールで [Port Configuration] (ポート設定) ページを使用するか、ローカル コンソールで [Local Port Settings] (ローカル ポート設定) ページを使用します。これらのポートの設定の詳細については、「*KX II のローカル ポートの設定 『246p. 』*」を参照してください。

KX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ

注: このページは、KX II ローカル コンソールでのみ使用できます。

KX II ローカル コンソールでは、さまざまなリセット モードの中から適切なものを選択できます。

注: 出荷時設定にリセットする前に、監査ログを保存しておくことをお勧めします。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「監査ログ 『283p. の"[Audit Log] (監査ログ)"参照 』」を参照してください。

▶ 出荷時設定にリセットするには、以下の手順に従います。

1. [保守] メニューの [出荷時設定にリセット] をクリックします。[出荷時設定にリセット] ページが開きます。
2. リセット モードを選択します。選択できるオプションは次のとおりです。
   - [完全リセット]: すべての設定値を削除し、工場出荷時のデフォルト値にリセットします。KX II が CC-SG の管理下にある場合は、CC-SG との関連付けが解除されます。このリセット モードではすべての設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
   - [ネットワーク パラメータ値をリセット]: KX II のネットワーク パラメータ値を出荷時設定にリセットします。現在設定されているネットワーク パラメータ値を表示するには、[デバイス設定] メニューの [ネットワーク設定] をクリックします。リセットされる設定値は次のとおりです。

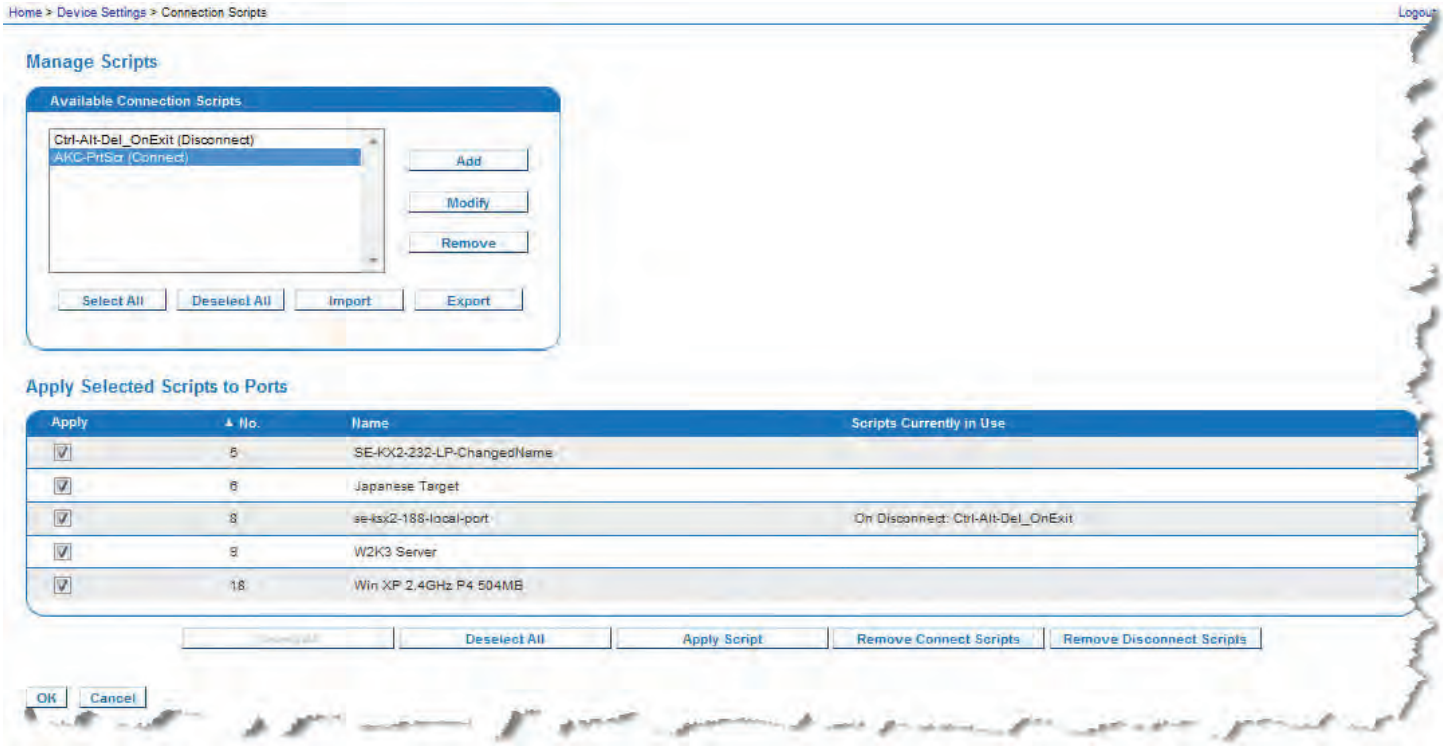
- IP を自動設定するかどうか
- IP アドレス
- サブネット マスク
- デフォルト ゲートウェイ
- プライマリ DNS サーバの IP アドレス
- セカンダリ DNS サーバの IP アドレス
- 検出ポート
- 帯域幅制限
- LAN インタフェースの速度と通信方式（全二重/半二重）
- 自動フェイルオーバを有効にするかどうか
- ping 間隔（単位: 秒）
- タイムアウト時間（単位: 秒）

3. ［リセット］をクリックして続行します。すべてのネットワーク設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
4. ［OK］をクリックして続行します。リセットが完了すると、KX II が自動再起動します。

スクリプトの接続と切断

KX II では、ターゲットとの接続を確立または切断する場合にキー マクロ スクリプトを実行できます。これらのスクリプトは、[Connection Scripts] (接続スクリプト) ページで定義および管理されます。

[Connection Scripts] (接続スクリプト) ページで独自のスクリプトを作成および編集し、ターゲットの接続を確立または切断するときに追加アクションを実行できます。また、既存の XML ファイル形式の接続スクリプトをインポートすることもできます。KX II で作成したスクリプトを XML ファイル形式でエクスポートすることもできます。KX II では、合計 16 個のスクリプトに対応できます。



スクリプトの適用および削除

▶ スクリプトをターゲットに適用するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、ターゲットに適用するスクリプトを選択します。'On Connect' スクリプトを 1 つと 'On Disconnect' スクリプトを 1 つターゲットに適用できます。

注: ターゲットに一度に追加できるスクリプトは 1 つだけです。

3. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットにのみスクリプトを適用する場合) スクリプトに適用するターゲットを選択します。
4. [Apply Scripts] (スクリプトを適用) をクリックします。スクリプトがターゲットに追加されると、それが [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションの [Scripts Currently in Use] (現在使用中のスクリプト] の下に表示されます。

▶ **スクリプトをターゲットから削除するには、以下の手順に従います。**

1. [Apply Selected Scripts to Ports] (選択したスクリプトをポートに適用) セクションで、[Select All] (すべて選択) を使用するか、各ターゲットの左のチェックボックスをクリックして (選択したターゲットからのみスクリプトを削除する場合) スクリプトを削除するターゲットを選択します。
2. [Remove Connect Scripts] (接続スクリプトを削除) をクリックして接続スクリプトを削除するか、[Remove Disconnect Scripts] (切断スクリプトを削除) をクリックして切断スクリプトを削除します。

スクリプトの追加

*注: KX II の外部で作成したスクリプトを追加したり、それらを XML ファイルとしてインポートしたりすることもできます。「**スクリプトのインポートとエクスポート** 『256p. 』」を参照してください。*

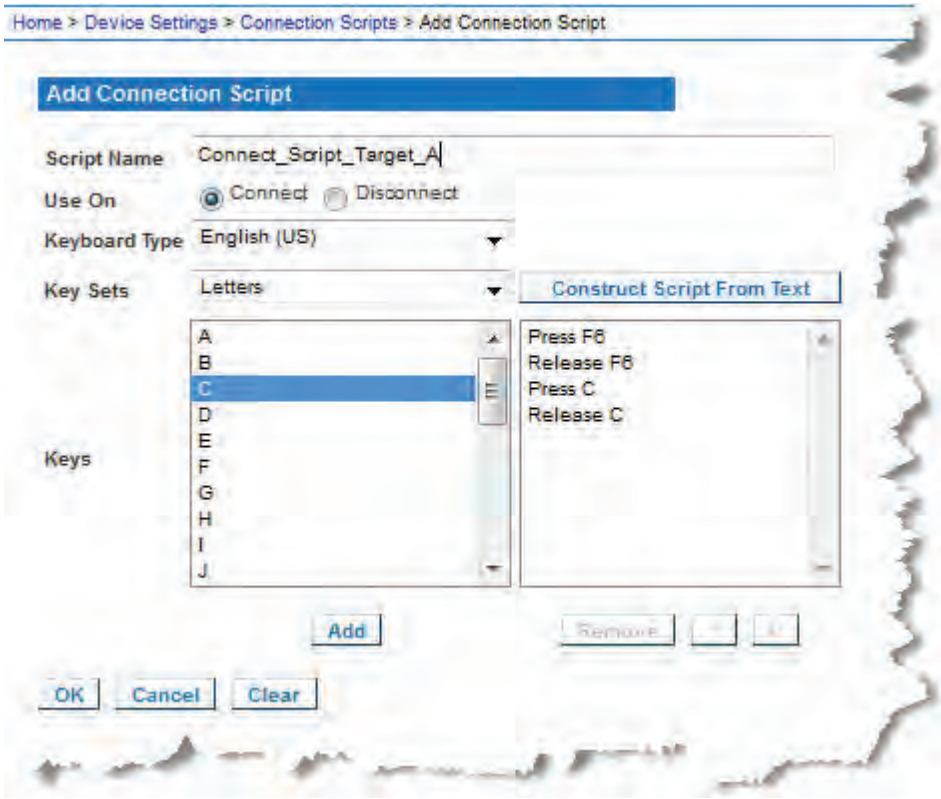
▶ **スクリプトを作成するには、以下の手順に従います。**

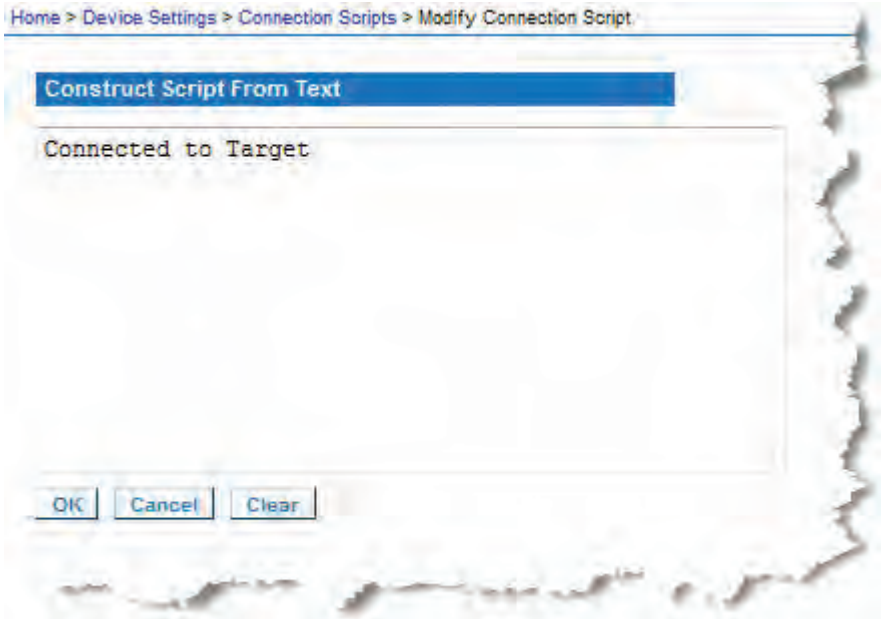
1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、[Add] (追加) をクリックします。[Add Connection Script] (接続スクリプトの追加) ページが開きます。
3. スクリプトの名前を最大 32 文字で入力します。スクリプトが作成されると、この名前が [Configure Scripts] (スクリプトの設定) ページの [Available Connection Scripts] (使用できる接続スクリプト) セクションに表示されます。
4. 作成中のスクリプトのタイプとして、[Connect] (接続) または [Disconnect] (切断) を選択します。接続スクリプトは、新規接続で、またはターゲットの切り替え時に使用されます。

5. 使用するターゲットで要求されるキーボード タイプを選択します。
6. [Key Sets]（キー セット）ドロップダウン リストから、スクリプトの作成に使用するキーボードのキー セットを選択します。選択すると、[Key Sets]（キー セット）ドロップダウン リストの下の [Add]（追加）ボックスに、選択したキー セット オプションが入力されます。
7. [Add]（追加）ボックスからキーを選択し、[Add]（追加）をクリックしてそれを [Script]（スクリプト）ボックスに移動します。キーを [Script]（スクリプト）ボックスから削除するには、キーを選択して [Remove]（削除）をクリックします。キーを並べ替えるには、それらを選択して [Up]（上へ）および [Down]（下へ）アイコンを使用します。

   スクリプトは、1 つ以上のキーで構成できます。また、スクリプトで使用されるキーを組み合わせることもできます。

   たとえば、F1 ～ F16 を選択すると、[Add]（追加）ボックスにファンクション キー セットが表示されます。ファンクション キーを選択して、それを [Script]（スクリプト）ボックスに移動します。次に、[Key Sets]（キー セット）ドロップダウン リストから [Letters]（文字）を選択して、文字キーをスクリプトに追加します。
8. スクリプトの実行時に表示されるテキストを追加することもできます。
   a. [Construct Script from Text]（テキストからスクリプトの作成）をクリックして、[Construct Script From Text]（テキストからスクリプトの作成）ページを開きます。
   b. テキスト ボックスにスクリプトを入力します。たとえば、「Connected to Target」（ターゲットに接続済み）と入力します。
   c. [Construct Script From Text]（テキストからスクリプトの作成）ページで [OK] をクリックします。
9. [OK] をクリックして、スクリプトを作成します。


Home > Device Settings > Connection Scripts > Add Connection Script
Add Connection Script
Script Name
Connect_Script_Target_A
Use On
Connect
Disconnect
Keyboard Type
English (US)
Key Sets
Letters
Construct Script From Text
Keys
A
B
C
D
E
F
G
H
I
J
Press F6
Release F6
Press C
Release C
Add
Remove
OK
Cancel
Clear


Home > Device Settings > Connection Scripts > Modify Connection Script
Construct Script From Text
Connected to Target
OK
Cancel
Clear

スクリプトの変更

▶ 既存のスクリプトを変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Connection Scripts] (接続スクリプト) をクリックします。[Connection Scripts] (接続スクリプト) ページが開きます。
2. [Available Connection Scripts] (使用できる接続スクリプト) セクションで、変更するスクリプトを選択して、[Modify] (変更) をクリックします。ページが編集モードになります。
3. 必要に応じて変更します。完了したら [OK] をクリックします。

リセット ボタンを使用して KX II をリセットする

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように、ボタンはパネルに埋め込まれています (このボタンを使用するには、先端が尖った道具が必要です)。リセット ボタンを押したときに実行される処理については、[Encryption & Share] (暗号化および共有) ページで定義します。「*暗号化および共有 『269p. の"[Encryption & Share] (暗号化および共有)"参照 』*」を参照してください。

注: 出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「監査ログ 『283p. の"[Audit Log] (監査ログ)"参照 』」を参照してください。

▶ デバイスをリセットするには、以下の手順に従います。

1. KX II の電源を切ります。
2. 先端の尖った道具を使用してリセット ボタンを押し続けます。
3. リセット ボタンを押したまま、KX II の電源を入れ直します。

4. リセット ボタンを 10 秒間押したままにします。 KX II がリセットされると、短いビープ音が 2 回鳴り、リセットが完了した旨が通知されます。

Ap A 仕様

この章の内容

KX II の物理的仕様 339
サポートされているオペレーティング システム（クライアント）..... 342
サポートされている画面解像度 343
サポートされているターゲット サーバとビデオ 345
サポートされているブラウザ 345
サポートされているコンピュータ インタフェース モジュール（CIM）の仕様 345
デジタル CIM ターゲット サーバのタイミングおよび画面解像度 349
サポートされている Paragon CIMS および設定 350
スマート カード リーダー 355
Dell 筐体を接続する場合のケーブル長と画面解像度 359
音声 359
サポートされている音声/仮想メディアおよびスマート カード接続の数 361
認定モデム 361
拡張ローカル ポートでサポートされているデバイス 362
KX2 8xx 拡張ローカル ポートの推奨最大距離 362
サポートされているリモート接続 362
各言語に対してサポートされているキーボード 363
使用される TCP ポートおよび UDP ポート 364
監査ログおよび Syslog でキャプチャされるイベント 367
ネットワーク速度の設定 367

KX II の物理的仕様

DKX2-832 - 二重化電源 AC 100 V/240 V、ローカル USB ポート、モデム ポート、拡張ローカル ポート、二重化 10/100/1000 Ethernet アクセス、ローカル ポート VGA、32 KVM ポート UTP 配線（Cat5/5e/6）

DKX2-864 - 二重化電源 AC 100 V/240 V、ローカル USB ポート、モデム ポート、拡張ローカル ポート、二重化 10/100/1000 Ethernet アクセス、ローカル ポート VGA、64 KVM ポート UTP 配線（Cat5/5e/6）

Dominion KX II モデル	説明	寸法 (W x D x H)	重量	電源と発熱量
DKX2-864	サーバ ポート x 64、リモート ユーザ x 8、ローカル ポート x 1 + 拡張ロ	17.3 x 13.8 x 3.5 インチ 439 x 360 x 88 mm	5.8 kg (12.88 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1.2 A、発熱量: 67 W、58 kcal

Dominion KX II モデル	説明	寸法 (W x D x H)	重量	電源と発熱量
	ーカル ポート			
DKX2-832	サーバ ポート x 32、リモート ユーザ x 8、ローカル ポート x 1 + 拡張ローカル ポート	17.3 x 13.8 x 1.75 インチ 439 x 360 x 44 mm	4.7 kg (10.40 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1 A、発熱量: 55 W、47 kcal
DKX2-808	サーバ ポート x 8、リモート ユーザ x 8、ローカル ポート x 1 + 拡張ローカル ポート	17.3 x 13.8 x 1.75 インチ 439 x 360 x 44 mm	4.7 kg (10.40 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1 A、発熱量: 55 W、47 kcal
DKX2-464	サーバ ポート x 64、リモート ユーザ x 4、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 3.5 インチ 439 x 290 x 90 mm	6.24 kg (13.73 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1.5 A、発熱量: 64 W、55 kcal
DKX2-432	サーバ ポート x 32、リモート ユーザ x 4、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	4.3 kg (9.48 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1 A、発熱量: 63 W、54 kcal
DKX2-416	サーバ ポート x 16、リモート ユーザ x 4、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	4.1 kg (9.04 lbs)	二重化電源: 100 V/240 V、47/63 Hz、1 A、発熱量: 63 W、54 kcal
DKX2-232	サーバ ポート x 32、リモート ユーザ x 2、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	4.1 kg (9.0 lbs)	二重化電源: 100 V/240 V、47/63 Hz、0.6A、発熱量: 63 W、54 kcal
DKX2-216	サーバ ポート x 16、リモート ユーザ x 2、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	3.9 kg (8.65 lbs)	二重化電源: 100 V/240 V、47/63 Hz、0.6 A、発熱量: 62 W、53 kcal
DKX2-132	サーバ ポート x 32、リモート ユー	17.3 x 11.4 x 1.75 インチ	4.1 kg (9.0 lbs)	二重化電源: 100 V/240 V、47/63 Hz、0.6 A、発

Dominion KX II モデル	説明	寸法 (W x D x H)	重量	電源と発熱量
	ザ x 1、ローカル ポート x 1 (ラックで使用)	439 x 290 x 44 mm		熱量: 62 W、53 kcal
DKX2-116	サーバ ポート x 16、リモート ユーザ x 1、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	3.9 kg (8.65 lbs)	二重化電源: 100 V/240 V、47/63 Hz、0.6 A、発熱量: 62 W、53 kcal
DKX2-108	サーバ ポート x 8、リモート ユーザ x 1、ローカル ポート x 1 (ラックで使用)	17.3 x 11.4 x 1.75 インチ 439 x 290 x 44 mm	3.9 kg (8.58 lbs)	二重化電源: 100 V/240 V、47/63 Hz、0.6 A、発熱量: 61 W、53 kcal

Dominion KX II の全モデルの仕様	
フォーム ファクタ	1U および 2U 全幅、ラックマウント対応、ブラケット付属
使用温度	0° ～ 40° C (32° ～ 104° F)
湿度	20 ～ 85% (相対湿度)
リモート接続	二重化 10/100/1000 ギガビット Ethernet アクセス、デュアル スタック: IPv4 および IPv6
ネットワーク モデム	DB9(F) DTE
ポート プロトコル	TCP/IP、HTTP、HTTPS、UDP、RADIUS、SNTP、DHCP、PAP、CHAP、LDAP、SNMP v2 と v3
ローカル ポート アクセス	
ビデオ	HD15(F) VGA
[Keyboard/Mouse] (キーボード/マウス)	USB(F)、USB x 1 (前面)、USB x 3 (背面)
保証	標準 2 年 (先出し交換)*

サポートされているオペレーティング システム (クライアント)

Virtual KVM Client (VKC) および Multi-Platform Client (MPC) でサポートされているオペレーティング システム (OS) は、次のとおりです。

クライアント オペレーティング システム	クライアントで仮想メディア (VM) がサポートされているか
Windows 7®	はい
Windows XP®	はい
Windows 2008®	はい
Windows Vista®	はい
Windows 2000® SP4 Server	はい
Windows 2003® Server	はい
Windows 2008® Server	はい
Red Hat® Desktop 5.0	はい
Red Hat Desktop 4.0	はい
openSUSE 10、11	はい
Fedora® 13 および 14	はい
Mac® OS	はい
Solaris™	いいえ
Linux®	はい

Java Runtime Environment (JRE™) プラグインは、32 ビット版および 64 ビット版 Windows® で使用できます。MPC および VKC は、32 ビット版ブラウザ、64 ビット版 Internet Explorer 7、または 64 ビット版 Internet Explorer 8 からのみ起動できます。

次の表に、Java™ 32 ビットおよび 64 ビット Windows におけるソフトウェア要件を示します。

モード	オペレーティング システム	ブラウザ
Windows x64 32 ビット モード	Windows XP®	• Internet Explorer® 6.0 SP1 以降、IE 7、IE 8 • Firefox® 1.06 ～ 3

モード	オペレーティング システム	ブラウザ
	Windows Server 2003®	• Internet Explorer 6.0 SP1 以降、IE 7、IE 8 • Firefox 1.06 ～ 3
	Windows Vista®	• Internet Explorer 7.0 または 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 ～ 3
Windows x64 64 ビット モード	Windows XP	64 ビット OS 対応の 32 ビット版ブラウザ • Internet Explorer 6.0 SP1 以降、7.0、または 8.0 • Firefox 1.06 ～ 3 64 ビット OS 対応の 64 ビット版ブラウザ • Internet Explorer 7.0 または 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

サポートされている画面解像度

各ターゲット サーバの画面解像度とリフレッシュ レートが KX II でサポートされているかどうか、および、映像信号がノンインタレース方式であるかどうかを確認してください。

画面解像度とケーブル長は、マウスを同期させるうえで重要な要素です。

KX II でサポートされている画面解像度は次のとおりです。

解像度	
640x350、70Hz	1024x768、85Hz
640x350、85Hz	1024x768、75Hz
640x400、56Hz	1024x768、90Hz
640x400、84Hz	1024x768、100Hz
640x400、85Hz	1152x864、60Hz
640x480、60Hz	1152x864、70Hz
640x480、66.6Hz	1152x864、75Hz

解像度	
640x480、72Hz	1152x864、85Hz
640x480、75Hz	1152x870、75.1Hz
640x480、85Hz	1152x900、66Hz
720x400、70Hz	1152x900、76Hz
720x400、84Hz	1280x720、60Hz
720x400、85Hz	1280x960、60Hz
800x600、56Hz	1280x960、85Hz
800x600、60Hz	1280x1024、60Hz
800x600、70Hz	1280x1024、75Hz
800x600、72Hz	1280x1024、85Hz
800x600、75Hz	1360x768、60Hz
800x600、85Hz	1366x768、60Hz
800x600、90Hz	1368x768、60Hz
800x600、100Hz	1400x1050、60Hz
832x624、75.1Hz	1440x900、60Hz
1024x768、60Hz	1600 x 1200、60Hz
1024x768、70Hz	1680x1050、60Hz
1024x768、72Hz	1920x1080、60Hz

注: 映像信号が Composite Sync 方式または Sync on Green 方式である場合は、アダプタを増設する必要があります。

注: 一部の解像度は、デフォルトでは使用できない可能性があります。解像度が表示されない場合は、まずモニタを接続し、モニタを取り外してから CIM を接続します。

注: 解像度 1440x900 および 1680x1050 がターゲット サーバのグラフィック アダプタ カードでサポートされているにもかかわらず表示されない場合は、DDC-1440 または DDC-1680 アダプタが必要である可能性があります。

サポートされているターゲット サーバとビデオ

ProductName とターゲット サーバの間の最大接続距離は、さまざまな要素によって決まります。たとえば、Cat5 ケーブルのタイプと品質、サーバのタイプと製造元、ビデオ ドライバ、モニタ、環境条件、ユーザの要求レベルなどに左右されます。次の表に、各種の画面解像度とリフレッシュ レートにおける最大接続距離を示します。

画面解像度	リフレッシュ レート	最大接続距離
1920 x 1080	60	15 m (50 フィート)
1600 x 1200	60	15 m (50 フィート)
1280 x 1024	60	30 m (100 フィート)
1024 x 768	60	45 m (150 フィート)

注: サーバの製造メーカーやタイプ、OS のバージョン、ビデオ ドライバなどは多種多様であるうえ、ビデオ品質にはユーザーの主観が反映されるため、Raritan ではあらゆる環境でのすべての距離におけるパフォーマンスを保証することはできません。

KX II でサポートされている画面解像度については、「*サポートされている画面解像度 『343p. 』*」を参照してください。

サポートされているブラウザ

KX II でサポートされているブラウザは、次のとおりです。

- Internet Explorer® 6 ～ 9
- Firefox® 1.5、2.0、3.0 (ビルド 3.6.17 まで) および 4.0
- Safari® 3 以降

サポートされているコンピュータ インタフェース モジュール (CIM) の仕様

CIM モデル	説明	寸法 (W x D x H)	重量
D2CIM-DVUSB	デュアル USB CIM (BIOS 仮想メディア、スマートカード/CAC、音声、およびずれないマウス用)	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)

CIM モデル	説明	寸法 (W x D x H)	重量
D2CIM-VUSB	USB CIM (仮想メディアおよびずれないマウス用) 	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)
DCIM-PS2	CIM (PS/2 用) 	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)
DCIM-SUN	CIM (Sun 用) 	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)
DCIM-USBG2	CIM (USB および Sun USB 用) 	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)

CIM モデル	説明	寸法 (W x D x H)	重量
D2CIM-PWR	CIM (リモート電源管理用)	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)
P2CIM-SER	Paragon II/Dominion KX II CIM (シリアル (ASCII) デバイス用)	33 x 76 x 15mm (1.3 x 3.0 x 0.6 インチ)	0.09kg (0.20lb)
DVM-DVI	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)
D2CIM-DVUSB DP (ディスプレイ ポート)	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)

CIM モデル	説明	寸法 (W x D x H)	重量
DVM-HDMI USB	デジタルとアナログの変換を行い、仮想メディア、スマートカード/CAC、音声、絶対および相対マウス同期をサポートするデジタル CIM	43 x 90 x 19 mm (1.7 x 3.5 x 0.8 インチ)	0.11 kg (0.25 lb)

注: KX II 2.5.0 (以降) でサポートされているデジタル CIM

デジタル CIM ターゲット サーバのタイミングおよび画面解像度

デジタル CIM は、Display Data Channels (DDC) および Enhanced Extended Display Identification Data (E-EDID) に対応しています。CIM の仕様については、「*サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 『345*p. 』」を参照してください。

タイミング モード

以下は、KX II がデジタル CIM を介してビデオ ソースとやり取りするときに使用されるデフォルトのタイミング モードです。使用されるタイミング モードは、ビデオ ソースの本来の解像度によって異なります。

- 1920x1080、60Hz
- 1600x1200、60Hz
- 1280x1024、60Hz (デジタル CIM に適用されるデフォルトの解像度)
- 1440x900、60Hz

確立されたモードおよび標準モード

以下の確立された解像度とタイミング モード、および標準の解像度とタイミング モードは、KX II 2.5.0 (以降) でサポートされています。

確立されたモード

- 720 x 400、70Hz (IBM、VGA)
- 640 x 480、60Hz (IBM、VGA)
- 640 x 480、67Hz (Apple、Mac II)
- 640 x 480、72Hz (VESA)
- 640 x 480、75Hz (VESA)
- 800 x 600、56Hz (VESA)
- 800 x 600、60Hz (VESA)
- 800 x 600、72Hz (VESA)
- 800 x 600、75Hz (VESA)
- 832 x 624、75Hz (Apple、Mac II)
- 1024 X 768、60Hz (VESA)
- 1024 X 768、70Hz (VESA)
- 1024 X 768、75Hz (VESA)
- 1280 X 1024、75Hz (VESA)
- 1152 x 870、75Hz (Apple、Mac II)

標準モード

- 1152 x 864、75Hz (VESA)
- 1280 x 960、60Hz (VESA)
- 1280 x 1024、60Hz (VESA)
- 1360 x 768、60Hz (VESA)
- 1400 x 1050、60Hz (VESA)

- 1440 x 900、60Hz (VESA)
- 1600 x 1200、60Hz (VESA)
- 1680 x 1050、60Hz (VESA)
- 1920 x 1080、60Hz (VESA)

本来の表示解像度

[Port Configuration] (ポート設定) ページの [Display Native Resolution] (本来の表示解像度) ドロップダウンから CIM の本来の解像度を選択できます。デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。選択されない場合は、デフォルトの解像度 1280 x 1024 が使用されます。「*CIM ポートの設定『211*p. 』」を参照してください。

DVI 互換モード

DVI 互換モードは、Intel のビデオ カードを搭載した Dell Optiplex ターゲットまたは HDMI コントローラを搭載した Mac® Mini に HDMI CIM を使用して接続する場合に使用されます。このモードを選択すると、ターゲットからの優れた画質が保証されます。「*CIM ポートの設定 s『211*p. の*″CIM ポートの設定″*参照 』」を参照してください。

サポートされている Paragon CIMS および設定

KX II では P2CIM-APS2DUAL CIM および P2CIM-AUSBDUAL CIM がサポートされています。これらの CIM を使用した場合、RJ45 で 2 台の異なる KVM スイッチに接続できます。これらの CIM がサポートされているので、KVM スイッチのいずれかに障害が発生した場合に備えて、ターゲットにアクセスするための 2 つ目の経路を確保できます。

Paragon CIM	サポートされるもの	サポートされないもの
P2CIM-APS2DUAL	• IBM® PS/2 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KX II に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成

Paragon CIM	サポートされるもの	サポートされないもの
P2CIM-AUSBDUAL	• USB 型または Sun™ USB 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KX II に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成

KX II ー KX II 構成に関するガイドライン

KX II ー KX II 構成において Paragon CIM を使用する場合、次に示すシステム構成ガイドラインに従ってください。

同時アクセス

両方の KX II KVM スイッチで、ターゲットへの同時アクセスに対して同じポリシーを設定する必要があります。つまり、どちらも [PC-Share] (PC 共有) にするかどちらも [Private] (プライベート) に設定します。

ターゲットへのプライベート アクセスが必要な場合は、どちらの KVM スイッチもそれに応じて構成する必要があります。

- [Security] (セキュリティ)、[Security Settings] (セキュリティ設定)、[Encryption & Share] (暗号化および共有) を選択し、[PC Share Mode] (PC 共有モード) を [Private] (プライベート) に設定します。

これにより、すべてのユーザ グループおよびすべてのターゲットにおいて、ターゲットへの同時アクセスはできなくなります。

KX II では、ターゲットへの同時アクセスをより高い粒度で、ユーザ グループ単位で制御できます。これは、ユーザ グループの PC 共有権限を設定することで行われます。ただし、これが適用されるのは KX II の範囲内のみです。P2CIM-APS2DUAL または P2CIM-AUSBDUAL を KX II と組み合わせて使用する際にプライバシーを保証する必要がある場合、ユーザ グループに対する PC 共有権限を使用しないでください。

CIM 名の更新

P2CIM-APS2 および P2CIM-AUSB の名前は CIM のメモリに保持されています。メモリ上には、Paragon CIM の名前 (最大 12 文字) を保持するための領域と、KX II の名前 (最大 32 文字) を保持するための領域の、2 つの領域があります。

Paragon CIM を KX II に初めて接続したとき、CIM の名前がメモリから取得され、KX II によって使用される CIM のメモリ領域に書き込まれます。続いて、KX II から、KX II によって使用されるメモリ領域に対して、CIM 名の照会または更新が行われます。KX II から、Paragon II によって使用されるメモリ領域に対して更新が行われることはありません。

一方の KX II によって CIM 名が更新されると、もう一方の KX II がそのターゲットへの接続を試みるときに、更新後の CIM 名が検出および取得されます。そのときまで、この CIM 名がもう一方の KX II 上で更新されることはありません。

ポートのステータスと可用性

ポートのステータスは、KX II の [Port Access] (ポート アクセス) ページに [Up] (稼動) または [Down] (非稼動) として表示されます。このステータスは最新の情報に更新され、CIM の電源が入っていて KX II のポートに接続されているかどうかが示されます。

ポートの可用性は、KX II の [Port Access] (ポート アクセス) ページに [Idle] (アイドル)、[Busy] (ビジー)、または [Connected] (接続) として表示されます。この可用性情報は、同じ KX II から起動されたターゲットの稼動状況を反映するように更新されます。

もう一方の KX II からそのターゲットに接続している場合は、この KX II から接続が試みられたときに可用性が検査されます。KX II に対して設定されている PC 共有ポリシーに基づいて、アクセスが拒否または許可されます。そのときまで、この可用性情報がもう一方の KX II 上で更新されることはありません。

ターゲットがビジーであるためにアクセスが拒否された場合、通知が表示されます。

CC-SG との連係動作

CC-SG から起動される処理は、管理対象 KX II から通知されるステータス、可用性情報、および CIM 名に基づいて決まります。ターゲットが 2 台の管理対象 KX II に接続されており、これらの KX II が CC-SG に追加されている場合、ノードが 2 つ作成されます。各ノードには固有の oob-kvm インタフェースが関連付けられます。各 KX II の oob-kvm インタフェースで、単一のノードを設定することもできます。

KX II がプライベート モードに設定されている場合、2 つ目の接続が試みられると、"接続できず、アクセスが拒否された" という内容のメッセージがユーザに表示されます。

CC-SG の [Port Profile] (ポート プロファイル) ペインでポート名を変更すると、変更後の名前が管理対象 KX II にプッシュ送信されます。もう一方の KX II の対応するポート名は、そのもう一方の oob-kvm インタフェース経由でターゲットへの接続が試みられるまで、CC-SG 内で更新されません。

KX II ー Paragon II 構成に関するガイドライン

P2CIM-APS2DUAL または P2CIM-AUSBDUAL を使用して KX II と Paragon II を接続できます。

同時アクセス

KX II と Paragon II の両方において、ターゲットへの同時アクセスに関して同じポリシーを設定してください。

Paragon II の動作モード	モードの説明	サポート
プライベート	特定のチャネル ポートに接続されているサーバなどのデバイスに、同時に 1 人のユーザだけが排他アクセスできます。	サポートされています。 Paragon II と KX II の両方をプライベートに設定する必要があります。プライベート設定は、ユーザ グループご

Paragon II の動作モード	モードの説明	サポート
		とではなく KX II に対して適用されます。 Paragon II では、赤は ″ビジー″、緑は ″使用可能″ を意味します。
PC 共有	特定のチャネル ポートに接続されているサーバなどのデバイスを、複数のユーザが選択して制御することができます。ただし、キーボードとマウスを制御できるユーザは同時に 1 人だけです。	サポートされています。 ただし、Paragon II で設定される PC 共有アイドル タイムアウトはサポートされていません。両方のユーザが、キーボードとマウスを同時に制御できます。 Paragon II では、緑は ″使用可能″ を意味します。このことは、別のユーザが既にターゲットにアクセスしている場合にも当てはまります。
パブリック表示	一方のユーザが、特定のチャネル ポートに接続されているサーバなどのデバイスにアクセスしている間、もう一方のユーザは、そのチャネル ポートを選択し、そのデバイスからのビデオ出力を表示することができます。ただし、キーボードとマウスを制御できるのは、最初にアクセスしたユーザだけです。両方のユーザが切断するか、またはキーボードとマウスを取り外すと、この状態が解消されます。	サポートされていません。 Paragon II と KX II を CIM で接続している場合、このモードは使用できません。 Paragon II では、黄色はパブリック表示モードを意味します。

CIM 名の更新

- Paragon II から更新された CIM 名は、Paragon の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- KX II から更新された CIM 名は、KX II の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- CIM 名が更新されても、Paragon II と KX II の間で互いに反映されることはありません。

KX II の統合向けにサポートされている距離

KX II を Paragon システムのフロント エンドとして使用する場合は、優れた画質が得られるようにケーブル長（距離）を制限する必要があります。

Paragon ユーザ ステーションからターゲット サーバまでのサポートされているケーブル長は、152 m（500 フィート）です。さらに距離を延ばすと、満足できるかどうかわからないビデオ パフォーマンスになることがあります。

KX II から Paragon ユーザ ステーションまでのサポートされているケーブル長は、最大 45 m（150 フィート）です。

スマート カード リーダー

サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー

外付けの USB スマート カード リーダーがサポートされています。

サポートされているスマート カード リーダー

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	ローカルおよびリモートで検証済み
USB	ActivIdentity	ActivIdentity USB Reader v3.0	ローカルおよびリモートで検証済み
USB	Gemalto®	GemPC USB-SW	ローカルおよびリモートで検証済み
USB キーボード/カード リーダ	Dell®	USB Smart Card	ローカルおよびリ

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
ーの組み合わせ		Reader Keyboard	モートで検証済み
USB キーボード/カード リーダーの組み合わせ	Cherry GmbH	G83-6744 SmartBoard	ローカルおよびリモートで検証済み
SIM サイズのカードに対応した USB リーダー	Omnikey	6121	ローカルおよびリモートで検証済み
統合型 (Dell Latitude D620)	O2Micro	OZ776	リモートのみ
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	リモートのみ
PCMCIA	SCM Microsystems	SCR243	リモートのみ

注: SCM Microsystems の SCR331 スマート カード リーダーでは、SCM Microsystems のファームウェア v5.25 を使用する必要があります。

サポートされていないスマート カード リーダー

この表は、Raritan がテストし、Raritan デバイスでは動作しないことが判明しているリーダーの一覧です。したがって、これらのリーダーはサポートされていません。サポートされているスマート カード リーダーの表にもサポートされていないスマート カード リーダーの表にもないスマート カード リーダーについては、デバイスでの動作を保証できません。

タイプ	ベンダ	[Model] (モデル)	注意
USB キーボード/カード リーダーの組み合わせ	HP®	ED707A	インタラプト エンドポイントなし => Microsoft® ドライバとの互換性なし
USB キーボード/カード リーダーの組み合わせ	SCM Microsystems	SCR338	独自のカード リーダー実装 (CCID 非準拠)
USB トークン	Aladdin®	eToken PRO™	独自の実装

スマート カードの最小システム要件

ローカル ポートの要件

KX II へのローカル ポート接続の相互運用性の基本要件は、以下のとおりです。

- ローカルに接続されたすべてのデバイス（スマート カード リーダーまたはトークン）は、USB CCID に準拠している必要があります。

ターゲット サーバの要件

スマート カード リーダーを使用する場合、ターゲット サーバにおける相互運用性の基本要件は以下のとおりです。

- IFD（スマート カード リーダー）Handler は、標準の USB CCID デバイス ドライバ（汎用の Microsoft® USG CCID ドライバに相当）である必要があります。
- デジタル CIM または D2CIM-DVUSB（デュアル VM CIM）が必要であり、そのファームウェア バージョンは 3A6E 以降である必要があります。
- ブレード シャーシのサーバ接続（ブレードごとに CIM を使用）がサポートされます。
- ブレード シャーシのサーバ接続（シャーシごとに CIM を使用）は、自動検出が有効になっている IBM® BladeCenter® モデル H および F でのみサポートされます。

Windows XP ターゲット

Windows XP® ターゲットでは、KX II でスマート カードを使用するために Windows XP SP3 が実行されている必要があります。ターゲット サーバ上の Windows XP 共有で .NET 3.5 を実行している場合、SP1 を適用する必要があります。

Linux ターゲット

Linux® ターゲットを使用している場合、Raritan デバイスでスマート カード リーダーを使用するには、以下の要件を満たす必要があります。

- CCID の要件

  Linux ターゲットで Raritan D2CIM-DVUSB VM/CCID がスマート カード リーダーとして認識されない場合は、CCID ドライバのバージョンを 1.3.8 以上に更新し、ドライバ設定ファイル（Info.plist）を更新する必要があります。

オペレーティング システム	CCID の要件
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

リモート クライアントの要件

リモート クライアントにおける相互運用性の基本要件は、以下のとおりです。

- IFD (スマート カード リーダー) Handler は、PC/SC 準拠のデバイスドライバである必要があります。
- ICC (スマート カード) Resource Manager が使用可能で、PC/SC 準拠である必要があります。
- スマート カード API を含む JRE™ 1.6.x が Raritan クライアントアプリケーションで使用可能である必要があります。

Linux クライアント

Linux® クライアントを使用している場合、Raritan デバイスでスマートカード リーダーを使用するには、以下の要件を満たす必要があります。

注: ターゲットへの 1 つ以上の KVM セッションがアクティブになっている場合、スマート カードを挿入すると、クライアントへのユーザ ログインに時間がかかることがあります。これらのターゲットへのログイン プロセスも進行中です。

- PC/SC の要件

オペレーティング システム	必要な PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Java™ ライブラリ リンクの作成

  RHEL 4、RHEL 5、および FC 10 のアップグレード後、libpcsclite.so へのソフト リンクを作成する必要があります。たとえば、パッケージのインストールによってライブラリが /usr/lib または /user/local/lib に配置される場合、「ln -s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so」と入力します。

- PC/SC デーモン

  pcsc デーモン（フレームワークのリソース マネージャ）を再起動する場合は、ブラウザと MPC も再起動します。

Dell 筐体を接続する場合のケーブル長と画面解像度

KX II に Dell® 製ブレード筐体を接続する場合、画質を維持するために次のケーブル長と画面解像度を使用することを推奨します。

ケーブル長	画面解像度
15 m	1024 x 768、60 Hz
15 m	1280 x 1024、60 Hz
9 m	1600 x 1200、60 Hz

音声

サポートされている音声デバイス形式

KX II では、ターゲット上の再生デバイスと録音デバイスを 1 台ずつサポートします。サポートされている音声デバイス形式は次のとおりです。

- ステレオ、16 ビット、44.1K
- モノラル、16 ビット、44.1K
- ステレオ、16 ビット、22.05K
- モノラル、16 ビット、22.05K
- ステレオ、16 ビット、11.025K
- モノラル、16 ビット、11.025K

音声の再生とキャプチャに関する推奨事項と要件

音声レベル

ターゲットの音声レベルを中域に設定します。たとえば、Windows® クライアントでは、音声を 50 以下に設定します。この設定は、クライアントの音声デバイス コントロールではなく、再生またはキャプチャ用の音声デバイスで行う必要があります。

PC 共有モードが有効になっている場合の音声接続に関する推奨事項

PC 共有モードでの動作中に音声機能を使用している場合は、さらに音声デバイスがターゲットに接続されると、音声の再生やキャプチャが中断されます。

たとえば、ユーザ A がターゲット 1 に再生デバイスを接続して音声再生アプリケーションを実行し、ユーザ B が同じターゲットにキャプチャデ バイスを接続するとします。この場合、ユーザ A の再生セッションは中断されるので、音声アプリケーションを再起動する必要があります。

この中断が発生する理由は、新しいデバイス設定で USB デバイスを再列挙する必要があるためです。ターゲットで新しいデバイスのドライバをインストールする場合は、少し時間がかかることがあります。音声アプリケーションは、再生の完全な停止、次のトラックへの移動、または再生の続行となる可能性があります。正確な動作は、音声アプリケーションで切断/再接続イベントがどのように処理されるかによって異なります。

帯域幅要件

次の表は、選択した各形式で音声を転送する場合の音声再生およびキャプチャの帯域幅要件の詳細です。

音声形式	ネットワーク帯域幅要件
44.1 KHz、16 ビット ステレオ	176 kbps
44.1 KHz、16 ビット モノラル	88.2 kbps
2.05 KHz、16 ビット ステレオ	88.2 kbps
22.05 KHz、16 ビット モノラル	44.1 kbps
11.025 KHz、16 ビット ステレオ	44.1 kbps
11.025 KHz、16 ビット モノラル	音声 22.05 kbps

実際に、音声デバイスをターゲットに接続するときに使用される帯域幅は、ターゲットで音声アプリケーションを開いたり使用したりする際に消費されるキーボード データやビデオ データがあるため、広くなっています。

一般的には、再生およびキャプチャを実行する前に、1.5 MB 以上の接続を維持していることを推奨します。ただし、ターゲット画面の解像度を高くして高品質なビデオ コンテンツをフル カラー接続すると、さらに多くの帯域幅を消費するため、音声の品質が大幅に劣化します。品質の低下を軽減できるように、帯域幅が狭い場合にビデオが音声品質に与える影響を軽減するための推奨のクライアント設定は数多くあります。

- 音声の再生を低品質の形式で接続します。帯域幅を消費するビデオによる影響は、44k よりも 11k で接続した方が大幅に減少します。
- [Connection Properties]（接続プロパティ）で、接続速度を、クライアントからサーバへの接続に最適な値に設定します。
- [Connection Properties]（接続プロパティ）で、色深度をできる限り低い値に設定します。色深度を 8 ビット カラーにすると、消費される帯域幅が大幅に減少します。
- [Smoothing]（スムージング）を [High]（高）に設定します。これにより、表示されるビデオ ノイズが減少し、ターゲット ビデオの画質が向上します。
- [Video]（ビデオ）設定で、[Noise Filter]（ノイズ フィルタ）を最も高い設定 7（最高値）にすると、ターゲットの画面変更に使用される帯域幅が小さくなります。

サポートされている音声/仮想メディアおよびスマート カード接続の数

クライアントからターゲットに確立する音声/仮想メディア、およびスマート カードの同時接続数を以下に示します。

- 1 スマート カード
- 1 仮想メディア
- 1 スマート カードおよび 1 仮想メディア
- 2 仮想メディア

認定モデム

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

拡張ローカル ポートでサポートされているデバイス

拡張ローカル ポートでは、以下のデバイスからの接続がサポートされます。

- 拡張ローカル ポートに直接接続された Paragon II User Station (P2-UST)
- 拡張ローカル ポートに直接接続された Paragon II Enhanced User Station (P2-EUST)
- 拡張ローカル ポートに直接接続された Cat5Reach URKVMG レシーバー
- 拡張ローカル ポートに接続された Paragon II アナログ KVM スイッチ (UMT)。これと Paragon II Enhanced User Station を併用した場合が、アクセスできる拡張ローカル ポートまでの距離が最大になります。

KX2 8xx 拡張ローカル ポートの推奨最大距離

拡張デバイス	1024x768、60 Hz	1280x1024、60 Hz
EUST を使用した Paragon II UMT	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

サポートされているリモート接続

リモート接続	詳細情報
ネットワーク	10BASE-T、100BASE-T、および 1000BASE-T (Gigabit) Ethernet
プロトコル	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS、LDAP/LDAPS

各言語に対してサポートされているキーボード

次の表に、各言語に対して KX II でサポートされているキーボードを示します。

*注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。アメリカ英語以外のキーボードの詳細については、「**留意事項** 『392p. 』」を参照してください。*

注: Linux 環境で作業する場合は、system-config-keyboard を使用して言語を変更することをお勧めします。

言語	地域	キーボード レイアウト
US 英語	米国および大半の英語圏の諸国: カナダ、オーストラリア、ニュージーランドなど	US キーボード レイアウト
US インターナショナル	米国および大半の英語圏の諸国: オランダなど	US キーボード レイアウト
UK 英語	英語（イギリス）	UK レイアウト キーボード
繁体字中国語	香港、中国（台湾）	繁体字中国語
簡体字中国語	中国	簡体字中国語
韓国語	韓国	Dubeolsik ハングル
日本語	日本	JIS キーボード
[French]（フランス語）	フランス	フランス語（AZERTY）レイアウト キーボード
[German]（ドイツ語）	ドイツおよびオーストリア	ドイツ語キーボード（QWERTZ レイアウト）
[French]（フランス語）	ベルギー	ベルギー語（ベルギー）
ノルウェー語（ノルウェー）	ノルウェー	ノルウェー語（ノルウェー）
デンマーク語（デンマーク）	デンマーク	デンマーク語（デンマーク）
スウェーデン語（スウェー	スウェーデン	スウェーデン語（スウェーデン）

言語	地域	キーボード レイアウト
デン)		
ハンガリー語	ハンガリー	ハンガリー語
スロベニア語	スロベニア	スロベニア語
イタリア語	イタリア	イタリア語
スペイン語	スペインおよび大半のスペイン語圏の諸国	スペイン語
ポルトガル語	ポルトガル	ポルトガル語

使用される TCP ポートおよび UDP ポート

ポート	説明
HTTP、ポート 80	このポートは、必要に応じて設定できます。詳細については、「*HTTP ポートおよび HTTPS ポートの設定 『180p. 』*」を参照してください。セキュリティを確保するため、デフォルトでは、KX II によって HTTP (ポート 80) で受信された要求は、すべて HTTPS に自動変換されます。要求はポート 80 で受け付けられるので、ユーザはブラウザのアドレスボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも確保されます。
HTTP、ポート 443	このポートは、必要に応じて設定できます。詳細については、「*HTTP ポートおよび HTTPS ポートの設定 『180p. 』*」を参照してください。デフォルトでは、このポートはさまざまな目的で使用されます。たとえば、クライアントから HTML で Web サーバにアクセスする場合、クライアント ソフトウェア (MPC/VKC) をクライアントにダウンロードする場合、KVM データと仮想メディア データをクライアントに転送する場合などです。
KX II (Raritan KVM-over-IP) プロトコル、ポート 5000 (変更可)	このポートは、他の Dominion デバイスの検出、および Raritan デバイスと各種システム (CC-SG 管理で利用可能なデバイス向けの CC-SG など) との間の通信に使用されます。このポートはデフォルトで 5000 に設定されていますが、別の TCP ポートに変更することもできます。この設定を変更する手順については、「*ネットワーク設定 『173p. 』*」を参照してください。
SNTP (時刻サーバ)、UDP ポート 123 (変更可)	KX II の内部クロックを中央の時刻サーバと同期させることができます。この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を使用する必要がありますが、別のポートに変更することもできます。**(オプション)**
LDAP/LDAPS、ポート 389 または 636 (変更可)	LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように KX II が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
RADIUS、ポート 1812 (変更可)	RADIUS プロトコルを使用してユーザをリモート認証するように KX II が設定されている場合、デフォルトでポート 1812 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
設定可能なポート 1813 を使用する RADIUS アカウンティング	RADIUS プロトコルを使用してユーザをリモート認証するように KX II が設定されており、かつ、イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。
SYSLOG、UDP ポート 514 (変更可)	メッセージを Syslog サーバに送信するように KX II が設定されている場合、通信にデフォルトでこのポートが使用されます。ただし、別のポートに変更することもできます。

SNMP、デフォルトの UDP ポート	送受信の読み取り/書き込み SNMP アクセスにはポート 161 が使用されます。SNMP トラップの送信トラフィックにはポート 162 が使用されます。(オプション)
TCP ポート 21	ポート 21 は、KX II のコマンド ライン インタフェース (CLI) を利用する際に使用されます (お客様が Raritan のテクニカル サポート部門と協力して作業する場合)。

監査ログおよび Syslog でキャプチャされるイベント

KX II の監査ログと syslog でキャプチャされるイベントの一覧と説明は以下のとおりです。

- Access Login (アクセス ログイン) - ユーザが KX II にログインしました。
- Access Logout (アクセス ログアウト) - ユーザが KX II からログアウトしました。
- Active USB Profile (アクティブ USB プロファイル) - USB プロファイルがアクティブになりました。
- CIM Connected (CIM 接続) - CIM が接続されました。
- CIM Disconnected (CIM 切断) - CIM が切断されました。
- Connection Lost (切断) - ターゲットへの接続が切断されました。
- Disconnected User (ユーザの切断) - ユーザがポートから切断されました。
- End CC Control (CC 制御終了) - CC-SG 管理対象から除外されました。
- Login Failed (ログイン失敗) - ユーザのログインが失敗しました。
- Password Changed (パスワード変更) - パスワードが変更されました。
- Port Connect (ポート接続) - ポートが接続されました。
- Port Disconnect (ポート切断) - ポートが切断されました。
- Port Status Change (ポート ステータス変更) - ポート ステータスが変更されました。
- Scan Started (スキャン開始) - ターゲットのスキャンが開始されました。
- Scan Stopped (スキャン停止) - ターゲットのスキャンが停止されました。
- Session Timeout (セッション タイムアウト) - セッション タイムアウトが発生しました。
- VM Image Connected (VM イメージ接続) - VM イメージが接続されました。
- VM Image Disconnected (VM イメージ切断) - VM イメージが切断されました。

ネットワーク速度の設定

KX II におけるネットワーク速度の設定

ネットワーク スイッチにおけるポ	自動	1000/全二重	100/全二重	100/半二重	10/全二重	10/半二重
自動	使用可能な最高速度	1000/全二重	KX II: 100/全二重	100/半二重	KX II: 10/全二重	10/半二重

KX II におけるネットワーク速度の設定

ートの設定			スイッチ: 100/半二重		スイッチ: 10/半二重	
1000/全二重	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
100/全二重	KX II: 100/半二重 スイッチ: 100/全二重	KX II: 100/半二重 スイッチ: 100/全二重	100/全二重	KX II: 100/半二重 スイッチ: 100/全二重	通信不可	通信不可
100/半二重	100/半二重	100/半二重	KX II: 100/全二重 スイッチ: 100/半二重	100/半二重	通信不可	通信不可
10/全二重	KX II: 10/半二重 スイッチ: 10/全二重	通信不可	通信不可	通信不可	10/全二重	KX II: 10/半二重 スイッチ: 10/全二重
10/半二重	10/半二重	通信不可	通信不可	通信不可	KX II: 10/全二重 スイッチ: 10/半二重	10/半二重

凡例:

- 通信できません。
- サポートされています。
- 通信は行えますが、推奨できません。
- Ethernet 仕様でサポートされていません。通信は行えますが、衝突が発生します。
- Ethernet 仕様では通信できないことになっています。KX II は期待どおりに動作しません。

注: ネットワーク通信の信頼性を高めるため、KX II とネットワーク スイッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえば、KX II とネットワーク スイッチの双方で "自動検出" に設定するか (推奨)、または、双方の通信速度と通信速度を同じ設定にします (例: 100 Mbps/全二重)。

Ap B　デュアル ビデオ ポート グループ

この章の内容

概要 370
デュアル ポート ビデオ グループ設定の例 371
デュアル ポート ビデオに関する推奨事項 376
サポートされているマウス モード 376
デュアル ビデオ サポートに必要な CIM 377
デュアル ポート ビデオ グループの使いやすさに関する注意事項 ... 378
権限およびデュアル ビデオ ポート グループ アクセス 379
デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作 379
ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ380
[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ380

概要

ビデオ カードを 2 枚搭載したサーバには、拡張デスクトップ設定を利用してリモートからアクセスできます。この設定は、リモート ユーザが利用できます。このためには、デュアル ポート ビデオ グループを作成します。

拡張デスクトップ設定により、標準的な 1 台のモニタでの表示に対して 2 台のモニタでターゲット サーバのデスクトップを表示できるようになります。デュアル ポート ビデオ グループを選択すると、そのグループのポート チャネルがすべて同時に開かれます。デュアル ポート ビデオ グループの作成方法については、「*デュアル ビデオ ポート グループの作成 『260*p. 』」を参照してください。

デュアル ポート ビデオ グループに関する重要な情報については、このセクションの内容を確認してください。

注: デュアル ポート ビデオ グループは、KX2-108 や KX2-116 のような、KVM チャネルが 1 つしかない KX II モデルではサポートされません。

デュアル ポート ビデオ グループ設定の例

以下の手順は、一般的な例として示しています。設定は、使用する CIM のタイプ、プライマリ ポートとして指定するポート、接続先の KX II ポートなどによって変わる可能性があります。

この例では、以下を前提にしています。

- 2 つのビデオ ポートを搭載したターゲット サーバ
- ターゲット サーバのビデオ ポート 1 がプライマリ ポート、およびビデオ ポート 2 がセカンダリ ポート
- KX II-832 デバイス
- D2CIM-DVUSB-DP CIM
- Microsoft® Windows 7® オペレーティング システムが稼動しているターゲット サーバおよびリモート クライアント
- インテリジェント マウス モード
- ターゲット サーバおよびリモート クライアントで拡張デスクトップを表示するので、画面の方向が「水平 - プライマリ (左)、セカンダリ (右)」になるように KX II を設定しています。

図の説明	
A	ターゲット サーバ
B	デジタル CIM

図の説明	
C	KX II
D	リモート クライアント
P	ターゲットの最初のビデオ ポートから KX II への接続
S	ターゲットの 2 番目のビデオ ポートから KX II への接続
1	KX II とリモート クライアント間の IP 接続
2	KX II でのデュアル ビデオ ポート グループの作成
3	デュアル ビデオ ポート グループを開く
P	プライマリ ポートの表示（KX II の [Port Group Management]（ポート グループ管理）ページで定義済み）
S	セカンダリ ポートの表示（KX II の [Port Group Management]（ポート グループ管理）ページで定義済み）

手順 1: ターゲット サーバの画面の設定

KX II で設定されている、ターゲットの方向設定が、ターゲットのオペレーティング システムでの実際の設定と一致している必要があります。できれば、接続元のクライアントの画面方向が同じに設定されていることが望まれます。

画面の方向およびマウス モードについては、「デュアル ビデオ ポート グループの画面の方向、位置合わせ、およびマウス モード」を確認してください。

注: 画面の設定の指定方法に関する正確な手順については、ターゲット サーバまたはオペレーティング システムのユーザ マニュアルを参照してください。

▶ **ターゲット サーバの画面の設定およびマウスの設定を指定するには、以下の手順に従います。**

1. ターゲット サーバで、ビデオ ポートごとにターゲット サーバの画面の方向を、リモート クライアントの画面の方向と一致するように設定します。

たとえば、リモート クライアントで 2 つのモニタにわたって左から右に移動するように拡張デスクトップの方向を設定している場合は、ターゲット サーバの画面の方向を同じに設定します。

2. ターゲット サーバのビデオが、サポートされている解像度とリフレッシュ レートに設定されていることを確認します。「*サポートされている画面解像度* 『*343*p. 』」を参照してください。

注: ターゲットのプライマリ画面およびセカンダリ画面が異なる解像度に設定されている場合、マウスは同期が維持されなくなるので、左上のターゲット ウィンドウで定期的に再同期する必要があります。

手順 2: KX II へのターゲット サーバの接続

デュアル ポート ビデオ グループは、既存のポート接続または新しいポート接続から作成できます。ここに示す手順では、新しい接続を作成すると想定しています。既存の接続からデュアル ポート ビデオ グループを作成する場合は、「*手順 4: デュアル ビデオ ポート グループの作成* 『*374*p. 』」を参照してください。

▶ 機器を接続するには、以下の手順に従います。

1. まだの場合は、製造元の手順に従ってターゲット サーバを設置し、電源を投入します。
2. 各 CIM のビデオ コネクタをターゲットの各ビデオ出力ポートに接続し、USB ケーブルをターゲット上の使用可能な USB ポートに接続します。
3. CAT5/6 ケーブルを使用して各 CIM を KX II に接続します。
4. まだの場合は、用意されている電源ケーブルを使用して KX II を AC 電源に接続し、KX II のネットワーク ポートとローカル ポート（必要な場合）に接続して、KX II を設定します。KX II の使用を開始するために必要な手順については、「*入門* 『*18*p. 』」を参照してください。
5. KX II には、Microsoft .NET® または Java Runtime Environment® (JRE) がインストールされている、ネットワーク接続機能を備えた任意のコンピュータからログインできます（JRE® は *Java の Web サイト http://java.sun.com/*から入手できます）。
6. サポートされている Web ブラウザ（Internet Explorer® や Firefox® など）を起動します。

7. .NET の URL 「*http://IP-ADDRESS*」または「*http://IP-ADDRESS/akc*」を入力します。IP-ADDRESS は KX II に割り当てられる IP アドレスです。また、HTTPS を使用することや、管理者によって割り当てられた KX II の DNS 名を使用することもできます (DNS サーバが設定されている場合)。IP アドレスをそのまま入力してもかまいません (KX II では常に IP アドレスが HTTP から HTTPS にリダイレクトされます)。
8. ユーザ名とパスワードを入力します。[Login] (ログイン) をクリックします。
9. ターゲット サーバのマウス モードを設定します。

   たとえば、リモート クライアントでインテリジェント マウス モードを使用している場合は、インテリジェント マウス モードを使用するようにターゲット サーバを設定します。使用しているオペレーティング システムに基づいて適用する必要があるマウス モードの設定については、「***マウスの設定*** 『*18*p. 』」を参照してください。

手順 3: マウス モードおよびポートの設定

ターゲット サーバのビデオ ポートを介してターゲット サーバを KX II に接続すると、KX II で接続が検出され、[Port Configuration] (ポート設定) ページに該当するポートが表示されます。手順については、「***標準ターゲット サーバの設定*** 『*208*p. 』」を参照してください。

ポートを設定した後に、それらのポートをデュアル ビデオ ポート グループにまとめることができます。

---

*注: 設定済みの既存のポートを設定する必要はありません。デュアル ポート ビデオ グループの作成方法については、「***デュアル ビデオ ポート グループの作成** 『*260p. 』」を参照してください。*

ターゲットに接続した後にターゲット サーバのマウス モードを設定します。たとえば、リモート クライアントでインテリジェント マウス モードを使用している場合は、インテリジェント マウス モードを使用するようにターゲット サーバを設定します。使用しているオペレーティング システムに基づいて適用する必要があるマウス モードの設定については、「***マウスの設定*** 『*18*p. 』」を参照してください。

手順 4: デュアル ビデオ ポート グループの作成

「***デュアル ビデオ ポート グループの作成*** 『*260*p. 』」を参照してください。

手順 5: デュアル ビデオ ポート グループを開く

デュアル ビデオ ポート グループを作成したら、そのグループを [Port Access] (ポート アクセス) ページで使用できます。プライマリ ポートをクリックしてリモートでデュアル ビデオ ポート グループに接続するには、2 つの KVM チャネルが必要です。2 つのチャネルが利用できない場合、[Connect] (接続) リンクは表示されません。

KX II で設定されているセッション タイムアウトは、デュアル ビデオ グループの両方のポートに適用されます。

▶ デュアル ポート ビデオ グループを開くには、以下の手順に従います。

- [Port Access] (ポート アクセス) ページで、プライマリ ポート名をクリックし、[Connect] (接続) をクリックします。一度に両方の接続が開かれ、2 種類のウィンドウに表示されます。

ウィンドウが表示されたら、使用している画面の設定に基づいてウィンドウを移動できます。たとえば、拡張デスクトップ モードを使用している場合は、ポート ウィンドウをモニタ間で移動できます。

デュアル ポート ビデオに関する推奨事項

マウスの同期を維持して定期的な再同期を最小限に抑えるために、ターゲット サーバのプライマリ画面およびセカンダリ画面を同じ画面解像度に設定してください。

設定する方向に応じて、上の画面（垂直方向）または左の画面（水平方向）をプライマリ画面として指定する必要があります。この画面で、仮想メディア、音声、スマート カード、およびマウスを操作するためのアクティブなメニュー選択が可能になります。

直観的なマウスの動作や制御を実現するために、クライアント PC のプライマリ画面とセカンダリ画面、KX II のデュアル ビデオ ポート グループ設定、およびターゲット サーバのプライマリ画面とセカンダリ画面は、画面の方向を同じにする必要があります。

デュアル ポート ビデオ画面には、次のクライアント起動設定だけが適用されます。

- KVM クライアントを起動する場合は、標準画面または全画面ウィンドウ モードを選択します。
- ビデオの拡大/縮小を有効にします。
- 全画面モードのときにメニュー ツールバーの固定機能を有効にします。

1 台のクライアント モニタでデュアル ビデオ ポートを全画面モードで表示する場合、シングル マウス モードの使用はお勧めできません。このような場合は、シングル マウス モードを終了してから、他方の画面にアクセスして表示する必要があります。

サポートされているマウス モード

対象のオペレーティング システム	サポートされているマウス モード	コメント
すべての Windows® オペレーティング システム	インテリジェント モード、標準モード、およびシングル マウス モード	ターゲット サーバのビデオ カードで「ストレッチ」モードがサポートされている場合は、ずれないマウス モードが正しく動作します。 ストレッチ モードにより、ターゲット サーバでは、2 つの画面が 1 つの仮想画面として管理されます。それに対して、拡張モードで設定されている

対象のオペレーティング システム	サポートされているマウス モード	コメント
		場合、各画面は 2 つの独立した画面と見なされます。拡張モードの場合は、インテリジェント マウス モードにすることをお勧めします。
Linux®	インテリジェント マウス モードおよび標準マウス モード	Linux® VKC/MPC ユーザは、シングル マウス モードを使用すると画面やマウスの動作に関する問題が発生する場合があります。Linux ユーザは、できればシングル マウス モードを使用しないでください。
Mac® オペレーティング システム	シングル マウス モード	マウスは、Mac のデュアル ビデオ ポートのターゲットでは同期しません。

デュアル ビデオ サポートに必要な CIM

次のデジタル CIM は、デュアル ビデオ ポート機能をサポートしています。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-DP
- D2CIM-DVUSB-HDMI
- DCIM-USBG2

デジタル CIM に関する重要な情報については、「*デジタル CIM ターゲット サーバのタイミングおよび画面解像度 『349p. 』*」を確認してください。CIM の仕様については、「*サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 『345p. 』*」を参照してください。

プライマリ ビデオ ポートまたはセカンダリ ビデオ ポートに最初に接続されていた CIM がつながらなくなったので別の CIM に交換すると、そのポートはデュアル ポート ビデオ グループから削除されます。必要に応じて、ポートをグループに追加し直します。

注: 使用する CIM は、ターゲット サーバの要件によって異なります。

デュアル ポート ビデオ グループの使いやすさに関する注意事項

以下は、デュアル ポート ビデオ グループ機能を使用するときに影響を受ける各種機能です。

- [Tools]（ツール）メニューの［Options］（オプション）の［Client Launch Settings］（クライアント起動設定）を介して VKC、AKC、MPC の各クライアントで設定されるクライアント起動設定は、次のようにデュアル ビデオ ポート グループに適用されます。
  - ウィンドウ モード設定が適用されます。
  - モニタ設定は適用されません。代わりに、[Port Group Management]（ポート グループ管理）で設定した「画面の方向」が適用されます。
  - その他 －[Enable Single Mouse Cursor]（シングル マウス カーソルを有効にする）設定は適用されません。
  - その他 －[Enable Scale Video]（ビデオの拡大、縮小を有効にする）設定が適用されます。
  - その他 －[Pin Menu Toolbar]（メニュー ツールバーを常に表示）設定が適用されます。
- プライマリ ターゲットとセカンダリ ターゲットのウィンドウ間で項目をドラッグして移動する場合は、マウス ボタンを押したまま移動して離すと、一方のウィンドウから他方のウィンドウに項目が移動されます。
- Linux® および Mac® のターゲット サーバで、Caps Lock および Num Lock をオンにすると、プライマリ ポート ウィンドウのステータス バーに Caps Lock インジケータが表示されますが、このインジケータは、セカンダリ ポート ウィンドウのステータス バーには表示されないことがあります。
- デュアル ポートのターゲットが全画面モードで開かれている場合、MPC メニューを有効にすることはできません。このメニューを有効にするには、もう一方のポート ウィンドウに切り替えた後、元のポート ウィンドウに戻ります。

権限およびデュアル ビデオ ポート グループ アクセス

理想的には、ポート グループの各ポートに適用される権限は、同じでなければなりません。権限が同じでない場合は、最も制限の厳しいポートの権限がポート グループに適用されます。

たとえば、あるポートに [VM Access] (VM アクセス) の [Deny] (拒否) が適用されており、別のポートに [VM Access] (VM アクセス) の [Read-Write] (読み取り/書き込み可能) が適用されている場合、ポート グループには、[VM Access] (VM アクセス) の [Deny] (拒否) が適用されます。

デュアル ポート ビデオ グループに属しているポートにアクセスするための適切な権限がないユーザには、アクセスできるポートだけが表示されます。どのポートにアクセスする権限もない場合、アクセスは拒否されます。

それでもポートにアクセスしようとすると、ポートを利用できないか、ポートにアクセスするための権限がないことを示すメッセージが表示されます。

デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作

画面操作

クライアントで全画面モードを使用する場合は、次の方法でポートを切り替えます。

- VKC

  Alt+Tab キーを押す

  Mac® クライアントの場合は、F3 キーを押して、ポート画面を選択する

- AKC

  表示ウィンドウの外でマウスをクリックし、Alt+Tab キーを押す

- MPC

  「接続されているサーバ」のツールバーからポートを選択する

ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login] (ログイン) ダイアログ ボックスと [Port Access] (ポート アクセス) ページを使用する必要がなくなります。この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

デュアル ポート ビデオ グループに属しているターゲットにアクセスする場合は、ダイレクト ポート アクセスにより、プライマリポートを使用して、プライマリ ポートおよびセカンダリ ポートの両方を開きます。セカンダリ ポートへのダイレクト ポート接続は拒否され、通常の権限ルールが適用されます。デュアル ポート ビデオ グループ機能については、「*デュアル ビデオ ポート グループの作成* 『*260*p. 』」を参照してください。ダイレクト ポート アクセスについては、「*URL を経由したダイレクト ポート アクセスの有効化* 『*186*p. 』」を参照してください。

[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ

注: デュアル ビデオ プライマリ ポートは、ポート グループの作成時に定義されます。

注: プライマリ ポートをクリックしてリモートでデュアル ビデオ ポート グループに接続するには、2 つの KVM チャネルが必要です。2 つのチャネルが利用できない場合、[Connect] (接続) リンクは表示されません。

デュアル ビデオ ポート グループでは、プライマリ ポートはポート スキャンの対象になりますが、リモート クライアントから接続している場合、セカンダリ ポートは対象になりません。両方のポートをローカル ポートからスキャンの対象にすることができます。

[Ports] (ポート) ページに表示される内容の詳細については、「*[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)* 『*53*p. 』」を参照し、スキャンの実行については、「*ポートのスキャン* 『*59*p. 』」を参照してください。

Ap C KX II を使用した Paragon II へのアクセス

この章の内容

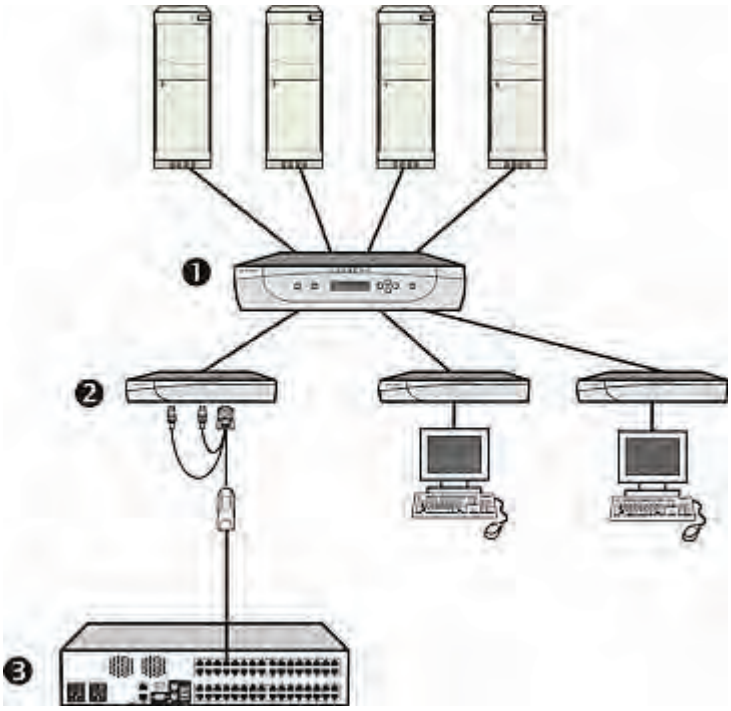
概要 381
KX II への Paragon II の接続 382

概要

P2SC デバイスがない場合は、CC-SG の管理下にある KX II に Paragon II システムを接続し、CC-SG から Paragon II へのアクセスを可能にすることができます。完全な互換性が保てるように、Paragon II の接続先の KX II ではバージョン 2.1 以降が実行されていることが望まれます。

注: Paragon II には、P2-USTIP を介して IP 経由でリモートからアクセスすることもできます。ただし、P2-USTIP は、LDAP や Active Directory のような認証/承認プラットフォーム (AA) と統合することはできません。KX II が、これらや他の AA プラットフォームをサポートしています。

この図は、KX II の統合構成を示しています。



❶	Paragon のスイッチ、サーバ、およびユーザ ステーショ

	ンが接続されている Paragon II システム
❷	DCIM-USB-G2 または DCIM-PS2 が接続されているユーザ ステーション
❸	KX II

KX II または CC-SG から Paragon システムにアクセスすると（KX II が CC-SG の管理下にある場合）、Paragon OSUI ログイン画面が表示されます。

この統合では、現在の Paragon ファームウェアで実装されている OSUI 機能または現在の KX II ファームウェアで実装されている KX II 機能（仮想メディア機能を除く）を実行できます。

KX II を介して Paragon OSUI にアクセスする場合は、手動でマウスを同期しないでください。OSUI 画面ではマウスは不要であり、マウスを同期すると、キーボードの応答が数秒遅れます。

詳細については、「*サポートされている Paragon CIMS および設定『350*p. 』」を参照してください。

KX II への Paragon II の接続

▶ **Paragon II システムを KX II に接続するには、以下の手順に従います。**

1. KX II に接続するユーザ ステーションにバージョン 4.6 以降のファームウェアが実装されているかどうかを確認します。実装されていない場合は、ファームウェアをアップグレードします。アップグレード手順については、「[Firmware Upgrade]（ファームウェアのアップグレード）」を参照してください。ユーザ ステーションは、次のいずれかです。
   - P2-UST
   - P2-EUST
   - P2-EUST/C
2. このユーザ ステーションに適した DCIM を接続します。システムが 2 層または 3 層になっている場合は、ユーザ ステーションがベースユニット（1 層目）に接続されているうちの 1 つであることを確認します。

   この統合では、2 種類の DCIM だけがサポートされています。
   - DCIM-USB G2 を使用する場合は、そのコネクタをユーザ ステーションの USB ポートおよびビデオ ポートに接続します。
   - DCIM-PS2 を使用する場合は、そのコネクタをユーザ ステーションの PS/2 ポートおよびビデオ ポートに接続します。
3. 最長 45 m（150 フィート）の Cat5 UTP ケーブルでユーザ ステーションを KX II に接続します。

- ケーブルの片側を DCIM の RJ-45 ポートに接続し、反対側を KX II のチャネル ポートのいずれかに接続します。

4. KX II または CC-SG で同じ Paragon II システムへのアクセス パスを増やす場合は、手順 1 ～ 3 を繰り返して、さらにユーザ ステーションを KX II に接続します。

Ap D LDAP スキーマを更新する

注: この章で説明する手順は、経験豊富なユーザだけが実行してください。

この章の内容

ユーザ グループ情報を返す 384
スキーマへの書き込み操作を許可するようにレジストリを設定する.. 385
新しい属性を作成する 386
属性をクラスに追加する 387
スキーマ キャッシュを更新する 388
ユーザ メンバの rciusergroup 属性を編集する 389

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、KX II では、そのユーザの所属グループに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような属性が返されるので、ユーザ グループ名がわかります。

rciusergroup attribute type: string

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

注: この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000® オペレーティング システム サーバ 上の Microsoft® Active Directory からユーザ グループ情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

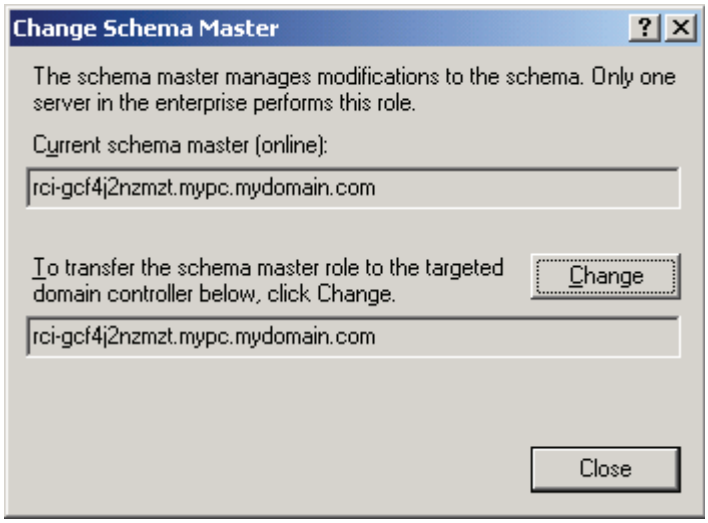
1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



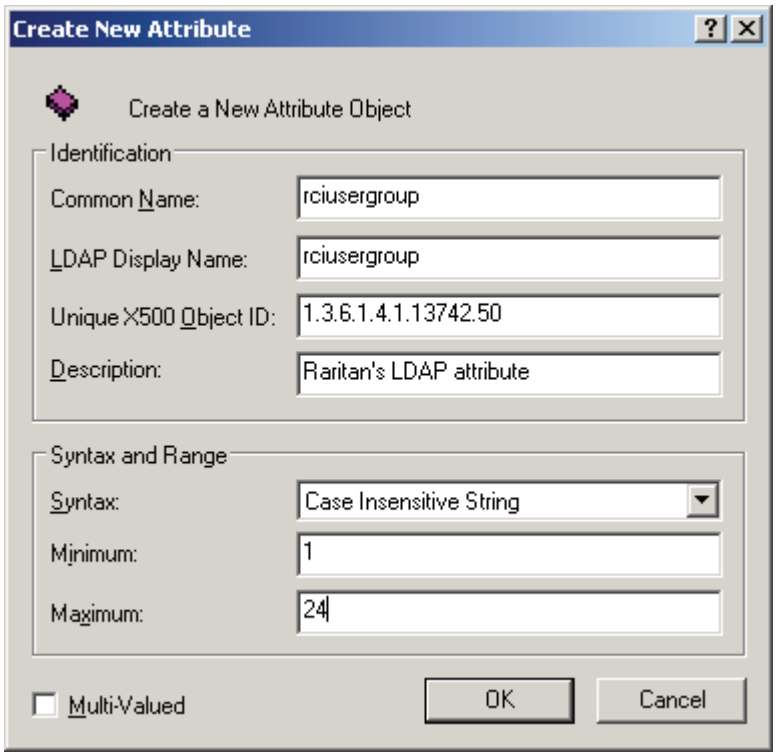
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**

3. [OK] (OK) をクリックします。

新しい属性を作成する

rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。
3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。



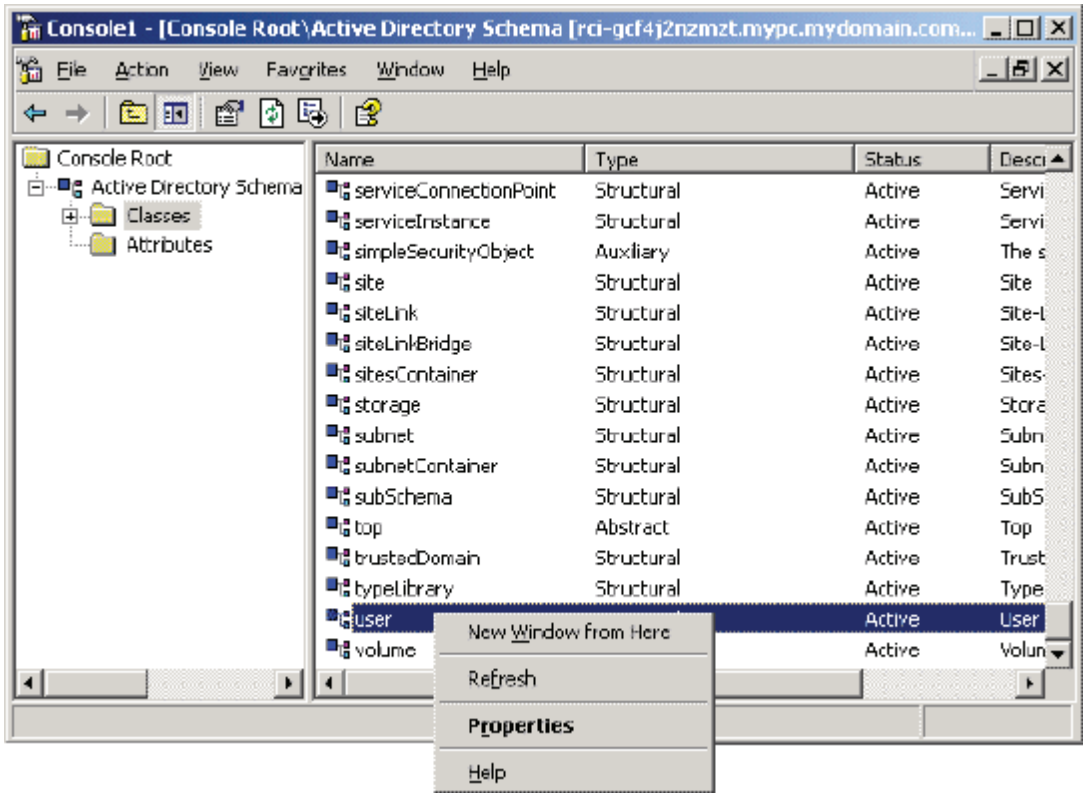
4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。

9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

▶ 属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。
2. 右ペインをスクロールして [user] (user) を表示し、右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。

7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

スキーマ キャッシュを更新するには

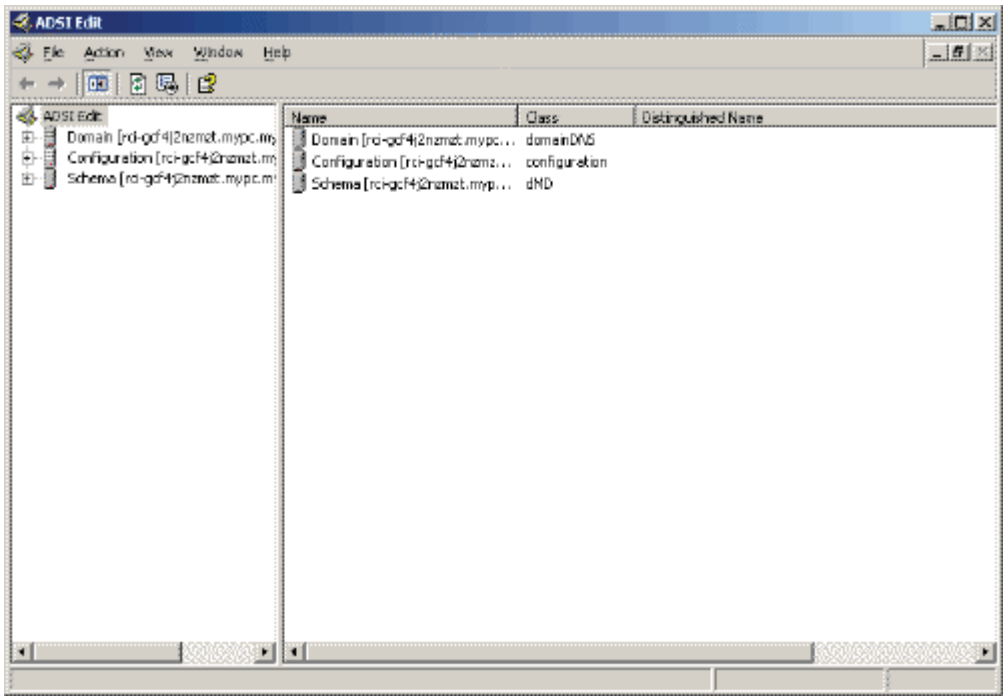
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003® 上で Active Directory® スクリプトを実行するには、Microsoft® から提供されるスクリプトを使用します (Windows Server 2003 のインストール用 CD-ROM に収録されています)。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

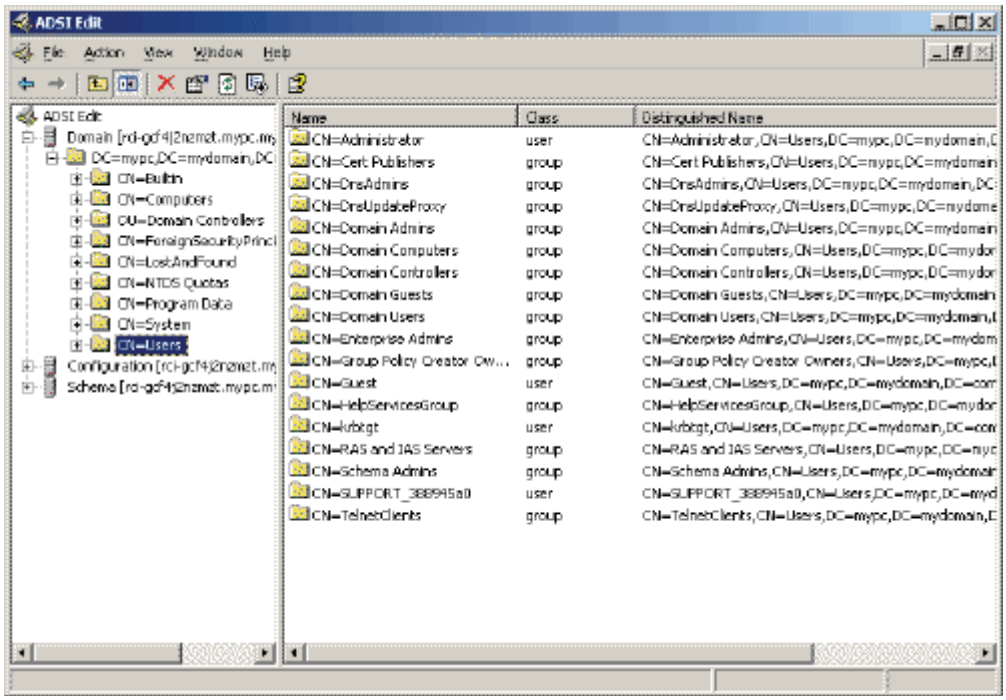
▶ **rciusergroup グループ内の個別のユーザ属性を編集するには、以下の手順に従います。**

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。



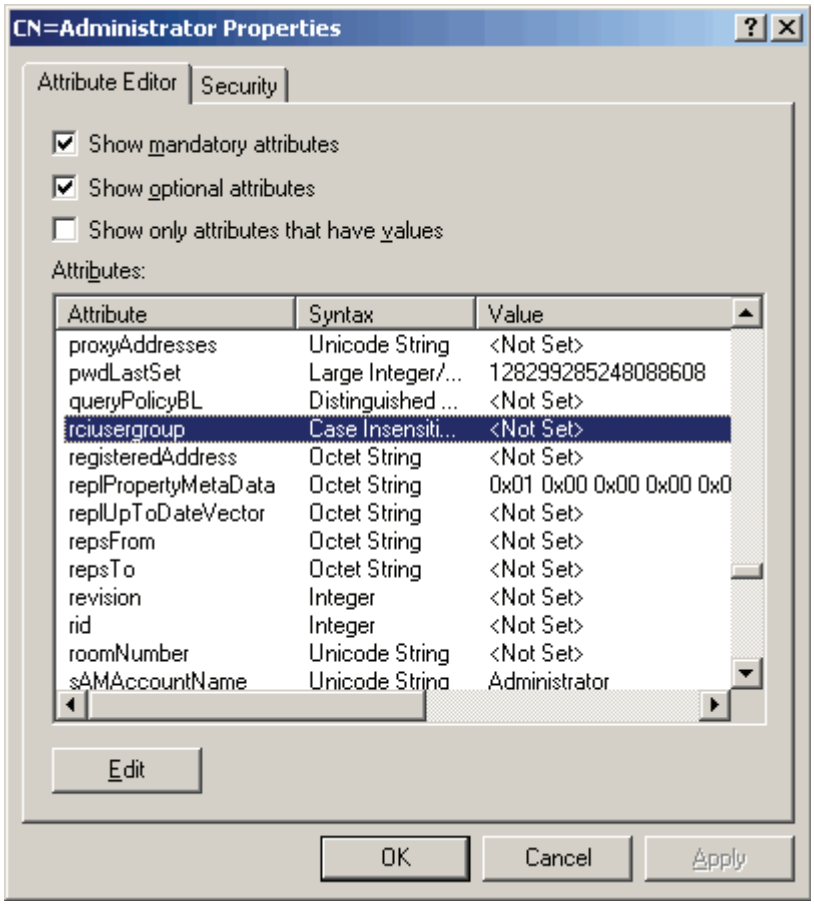
4. [Domain] (ドメイン) を開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

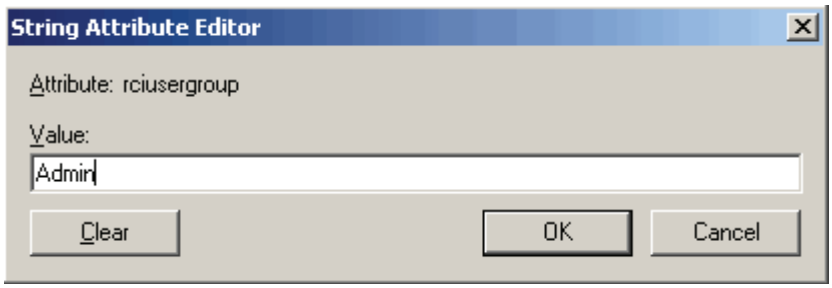


6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューの [Properties] (プロパティ) をクリックします。

7. [Attribute Editor]（属性エディタ）タブをクリックします。[Attributes]（属性）ボックスの一覧で [rciusergroup]（rciusergroup）を選択します。



8. [Edit]（編集）をクリックします。[String Attribute Editor]（文字列属性エディタ）ダイアログ ボックスが開きます。
9. [Value]（値）ボックスに、KX II で作成したユーザ グループを入力します。[OK] をクリックします。



Ap E 留意事項

この章の内容

概要 392
Java Runtime Environment (JRE) 392
IPv6 のサポートに関する注意事項 394
デュアル スタック ログインのパフォーマンスに関する問題 395
Mac に関する注意事項 395
キーボード 397
Fedora 400
ビデオ モードと解像度 402
音声 403
USB ポートとプロファイル 404
仮想メディア 408
CIM 410
CC-SG 412

概要

この章では、KX II の使用に関する重要事項について説明します。今後更新される情報については、弊社 Web サイトで提供されます。更新情報を表示するには、KX II リモート コンソールの [Help] (ヘルプ) リンクをクリックしてください。

注: このセクションの一部のトピックでは、記載されている情報がさまざまなデバイスに影響を与えるため、他の複数の Raritan デバイスにも言及しています。

Java Runtime Environment (JRE)

重要: Java のキャッシュ機能を無効にし、Java™ キャッシュをクリアすることをお勧めします。詳細については、Java のドキュメントまたは『KVM and Serial Access Clients Guide』を参照してください。

LX、KX II、KX II-101、および KX II-101-V2 リモート コンソールおよび MPC では、リモート コンソールで Java のバージョンをチェックするので、実行に Java Runtime Environment™ (JRE™) が必要です。バージョンが不適切であるかまたは古い場合、互換性のあるバージョンをダウンロードするよう指示されます。

パフォーマンスを最大化するため、JRE バージョン 1.6 を使用することをお勧めします。ただし、リモート コンソールおよび MPC は、JRE バージョン 1.6.x 以降 (1.6.2 を除く) でも動作します。

注: 多言語対応のキーボードを LX、KX II、KX II-101、および KX II-101-V2 リモート コンソール (Virtual KVM Client (VKC)) で使用できるようにするには、多言語バージョンの JRE をインストールする必要があります。

IPv6 のサポートに関する注意事項

Java

Java™ 1.6 では、次のオペレーティング システム (OS) に対して IPv6 がサポートされています。

- Solaris™ 10 (以降)
- Linux® カーネル 2.1.2 (以降)/RedHat 6.1 (以降)

Java 5.0 以降では、次の OS に対して IPv6 がサポートされています。

- Solaris 10 (以降)
- Linux カーネル 2.1.2 (以降)、カーネル 2.4.0 (以降) (優れた IPv6 サポートを求める場合に推奨)
- Windows XP® SP1、Windows 2003®、および Windows Vista®

Java では、次の IPv6 構成は*サポートされていません*。

- Microsoft® Windows® 上の J2SE 1.4 では、IPv6 はサポートされていません。

Linux

- IPv6 を使用する場合、Linux カーネル 2.4.0 以降を使用することを推奨します。
- IPv6 対応のカーネルをインストールするか、または、IPv6 関連オプションを有効にしてカーネルを再ビルドする必要があります。
- IPv6 を使用する場合、Linux 用のネットワーク ユーティリティをいくつかインストールする必要があります。詳細については、http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html を参照してください。

Windows

- Windows XP ユーザや Windows 2003 ユーザは、Microsoft の IPv6 対応サービス パックをインストールし、IPv6 を有効にする必要があります。
- Windows XP に IPv6 を搭載した AKC の場合は、ファイアウォールの例外リストに実行可能ファイル kxgui.exe を追加します。クライアントのログ ファイルを表示し、ファイル kxgui.exe の場所の完全パスを確認します。

Mac Leopard

- KX II バージョン 2.0.20 では、Mac® Leopard® に対して IPv6 はサポートされていません。

Samba

- Samba を使用する場合、IPv6 と仮想メディアを併用することはできません。

デュアル スタック ログインのパフォーマンスに関する問題

デュアル スタック設定で KX II を使用する場合は、ログイン時に遅延が発生しないように KX II でドメイン ネーム システム (DNS) を正しく設定しておくことが重要です。KX II で DNS を設定する方法については、「*Web ブラウザ インタフェースの追加に関するヒント* 『*231*p. 』」を参照してください。

Mac に関する注意事項

Mac Mini BIOS のキー入力コマンド

次の BIOS コマンドは、D2CIM-DVUSB CIM および D2CIM-VUSB CIM を使用して KX II に接続されている MAC® Mini ターゲット サーバ上でテスト済みです。

キー入力	説明	D2CIM-DVUSB (5A89)	D2CIM-VUSB (4A7F)
起動時に D キーを押す	Apple Hardware Test (AHT) で起動します。	機能しない	機能しない
2 回目の起動音が聞こえるまで Option-Command-P-R キーを押す	NVRAM をリセットします。	機能する	機能する
起動時に Option キーを押す	スタート アップマネージャで起動。起動元の Mac OS X ボリュームを選択できます。注: N キーを押すと、起動可能な最初のネットワーク ボリュームも表示されます。	機能しない	機能する
イジェクト キー または F12 キーを押すか、マウスまたはトラックパッドのボタンを押し続ける	マウスまたはトラックパッドのボタンで、光ディスクなどのリムーバブル メディアを取り出します。	機能する	機能する
起動時に N キーを押す	互換性のあるネットワーク サーバからの起動 (NetBoot) を試みます。	機能する	機能する
起動時に T キーを押す	ターゲット ディスク モードで起動します。	機能する	機能する

キー入力	説明	D2CIM-DVUSB (5A89)	D2CIM-VUSB (4A7F)
起動時に Shift キーを押す	セーフ モードで起動し、ログイン項目を一時的に無効にします。	機能しない	機能する
起動時に Command-V キーを押す	Verbose モードで起動します。	機能する	機能する
起動時に Command-S キーを押す	シングル ユーザ モードで起動します。	機能する	機能する
起動時に Option-N キーを押す	デフォルトのブート イメージを使用して NetBoot サーバから起動します。	機能する	機能する
起動時に Command-R キーを押す	Lion Recovery から起動します。		T

Mac Lion クライアントでの MPC の起動

クライアントで Mac® Lion を使用している場合、Raritan の Multi-Platform Client (MPC) は起動しません。MPC を起動するには、次の回避策を使用します。

インストール環境から JavaApplicationStub を削除し、正しい JavaApplicationStub からのリンクを作成します。

- rm /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub
- ln -s /System/Library/Frameworks/JavaVM.framework/Resources/MacOS/JavaApplicationStub /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

実行するには、次のコマンドを使用します。

- /Applications/Raritan/Raritan Multi-Platform Client/<MPC Version>/Raritan Multi-Platform Client.app/Contents/MacOS/JavaApplicationStub

キーボード

アメリカ英語以外のキーボード

フランス語キーボード

キャレット記号 (Linux® クライアントのみ)

Linux クライアントとフランス語キーボードを併用する場合、VKC および MPC では Alt Gr + 9 というキー組み合わせがキャレット記号（^）として処理されません。

▶ キャレット記号を入力するには

フランス語キーボードの ^ キー（P キーの右にある）を押し、すぐに Space キーを押します。

次のコマンドを実行するマクロを作成する方法もあります。

1. 右 Alt キーを押す。
2. 9 キーを押す。
3. 9 キーを離す。
4. 右 Alt キーを離す。

注: これらの手順は、母音の上に付ける曲折アクセントには当てはまりません。フランス語キーボードで ^ キーと他の文字を組み合わせて使用した場合、曲折アクセントになります。

アクセント記号 (Windows XP® クライアントのみ)

Windows XP クライアントでフランス語キーボードを使用する場合、VKC および MPC で Alt Gr + 7 というキー組み合わせを使用すると、アクセント記号付き文字が 2 つ表示されます。

注: この現象は、Linux クライアントでは発生しません。

数字キーパッド

VKC および MPC でフランス語キーボードを使用する場合、数字キーパッドにある記号は次のとおりに表示されます。

数字キーパッド上の記号キー	表示
/	;
.	;

ティルデ記号

VKC および MPC でフランス語キーボードを使用する場合、Alt Gr + 2 というキー組み合わせがティルデ記号（~）として処理されません。

▶ ティルデ記号を入力するには

次のコマンドを実行するマクロを作成します。

- 右 Alt キーを押す。
- 2 キーを押す。
- 2 キーを離す。
- 右 Alt キーを離す。

キーボード言語の設定 (Fedora クライアント)

Linux® 版の JRE™ には、[System Preferences]（システム基本設定）で設定した外国語キーボードに対して正しいキー イベントが生成されない、という問題があります。したがって、次の表に示す方法を使用して外国語キーボードを設定することを推奨します。

言語	設定方法
アメリカ英語/国際	デフォルト設定
イギリス英語	[System Settings]（システム設定）(Control Center)
フランス語	Keyboard Indicator
ドイツ語	Keyboard Indicator
ハンガリー語	[System Settings]（システム設定）(Control Center)
スペイン語	[System Settings]（システム設定）(Control Center)
ドイツ語（スイス）	[System Settings]（システム設定）(Control Center)
ノルウェー語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
デンマーク語	Keyboard Indicator
日本語	[System Settings]（システム設定）(Control Center)
韓国語	[System Settings]（システム設定）(Control

言語	設定方法
アメリカ英語/国際	デフォルト設定
	Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

Linux クライアントでハンガリー語キーボードを使用している場合、ダブル アキュート付き U およびダブル アキュート付き O は、JRE 1.6 でのみ入力できます。

Fedora® クライアントでは、キーボード言語を設定する方法がいくつかあります。VKC および MPC でキーを正しく対応付けるには、次に示す方法を使用します。

[System Settings] (システム設定) を使用してキーボード言語を設定するには

1. ツールバーで [System] (システム) > [Preferences] (基本設定) > [Keyboard] (キーボード) を選択します。
2. [Layouts] (レイアウト) タブをクリックします。
3. 言語を追加または選択します。
4. [Close] (閉じる) をクリックします。

Keyboard Indicator を使用してキーボード言語を設定するには

1. タスク バーを右クリックし、[Add to Panel] (パネルに追加) をクリックします。
2. [Add to Panel] (パネルに追加) ダイアログ ボックスで、Keyboard Indicator を右クリックし、メニューの [Open Keyboard Preferences] (キーボード基本設定) をクリックします。
3. [Keyboard Preferences] (キーボード基本設定) ダイアログ ボックスで、[Layouts] (レイアウト) タブをクリックします。
4. 必要に応じて言語を追加または削除します。

Macintosh キーボード

クライアントとして Macintosh® を使用している場合、Macintosh キーボードの次のキーは、JRE™ によって取り込まれません。

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

つまり、Macintosh クライアントのキーボードでこれらのキーが押されても、VKC および MPC では処理できません。

Fedora

Fedora Core のフォーカスに関する問題を解決する

MPC を使用しているときに、LX、KX II、または KSX II デバイスにログインできなくなったり、Windows® や SUSE を実行している KVM ターゲット サーバにアクセスできなくなったりすることがあります。また、Ctrl + Alt + M キーを押してもキーボード ショートカット メニューが表示されないことがあります。このような問題が発生するのは、Fedora® Core 6 と Firefox® 1.5 または 2.0 を組み合わせて使用している場合です。

Raritan でテストした結果、libXp をインストールすれば Fedora Core 6 のウィンドウ フォーカスに関する問題を解決できることがわかりました。Raritan がテストで使用したのは libXp-1.0.0.8.i386.rpm です。この libXp をインストールした結果、ウィンドウ フォーカスとポップアップ メニューに関する問題がすべて解決しました。

注: libXp は、SeaMonkey (旧称: Mozilla®) ブラウザで Java™ プラグインを使用する場合にも必要となります。

マウス ポインタの同期 (Fedora)

Fedora® 7 を実行しているターゲット サーバにデュアル マウス モードで接続しているときに、ターゲット サーバとローカルのマウス ポインタが同期しなくなった場合、マウス モードをインテリジェント モードに、またはインテリジェント モードから標準モードに変更すると同期が回復することがあります。シングル マウス モードを使用すると、制御しやすくなります。

▶ マウス ポインタを再度同期させるには、以下の手順に従います。

- VKC の [Synchronize Mouse] (マウスを同期) オプションを使用します。

Fedora サーバへの VKC および MPC のスマート カード接続

MPC または VKC でスマート カードを使用して Fedora® サーバに接続する場合は、pcsc-lite ライブラリを 1.4.102-3 以降にアップグレードします。

注: この機能は、KSX II 2.3.0 (以降) および KX II 2.1.10 (以降) で提供されます。

Fedora 使用時の Firefox のフリーズに関する問題の解決

Fedora® サーバを使用している場合に Firefox® にアクセスすると、Firefox を開くときに Firefox がフリーズすることがあります。この問題を解決するには、libnpjp2.so という Java™ プラグインをサーバにインストールします。

ビデオ モードと解像度

SUSE と VESA のビデオ モード

SUSE の X.org 設定ツールである SaX2 を実行すると、X.org 設定ファイル内の Monitor セクションの Modeline エントリにビデオ モードが書き込まれます。これらのビデオ モードは、VESA モニタを選択している場合であっても、VESA のビデオ モード タイミングと正確に対応していません。一方 KX II では、正確に同期させるため、VESA のビデオ モード タイミングが使用されています。このビデオ モード タイミングの不一致により、黒の境界線が表示される、画面の一部が表示されない、ノイズが発生する、などの問題が発生することがあります。

SUSE のビデオ表示を設定するには

1. 生成された設定ファイル /etc/X11/xorg.conf 内に Monitor セクションがあり、その中に UseModes というオプションがあります。たとえば、
   UseModes "Modes[0]" と書き込まれています。
2. この行の先頭に # を付加してコメント行にするか、または、この行全体を削除します。
3. X サーバを再起動します。

これにより、X サーバの内部ビデオ モード タイミングが使用されるようになるので、VESA のビデオ モード タイミングと正確に対応します。この結果、KX II 経由で画面が正しく表示されます。

サポートされている画面解像度が表示されない

CIM を使用する場合、「*サポートされている画面解像度* 『*343*p. 』」の一覧にある画面解像度がデフォルトでは選択できないことがあります。

表示されない場合に利用可能なすべての画面解像度を表示するには、以下の手順に従います。

1. モニタを接続します。
2. 次に、モニタを取り外し、CIM を接続します。すべての画面解像度が利用可能とは限りませんが、使用できる場合もあります。

音声

音声の再生とキャプチャに関する問題

音声接続を妨げる可能性がある機能

音声デバイスに接続中、以下の機能を使用している場合は、音声接続が妨げられる可能性があります。音声デバイスに接続する場合は、これらの機能を使用しないことを推奨します。

- ビデオの自動検出
- ローカル ポートを頻繁に使用する機能
- ユーザの追加

キャプチャ デバイスおよび再生デバイスをターゲットで同時に使用した場合の問題

一部のターゲットでは、USB ハブ コントローラーとその USB ポートの管理方法により、キャプチャ デバイスと再生デバイスの同時接続が機能しない場合があります。必要な帯域幅が小さい音声形式を選択することを検討してください。

それでも問題が解決しない場合は、ターゲットで D2CIM-DVUSB CIM のキーボードおよびマウス コネクタを別のポートに接続してください。それでも問題が解決しない場合は、デバイスを USB ハブに接続し、ハブをターゲットに接続してください。

Linux 環境での音声

以下は、Linux® 環境で音声機能を使用する場合の既知の問題です。

- Linux® ユーザは、再生にデフォルト音声デバイスを使用してください。デフォルト以外のサウンド カードを選択した場合は、音が出力されない可能性があります。
- SuSE 11 クライアントでは、YAST を介して Javas_1_6_0-sun-alsa (ALSA 対応の java-1_6_0-sun) をインストールしておく必要があります。
- マイクが組み込まれた Logitech ヘッドセットの場合は、[Mono Capture] (モノラル キャプチャ) オプションのみを使用できます。
- SUSE 11 を実行しながら ALSA デバイスを使用している場合にデバイスが表示されるようにするためには、KX II からログアウトして再度ログインする必要があります。また、音声デバイスの接続と切断を数回繰り返した場合、本来は 1 回だけリストされるべきデバイスが、複数回リストされる可能性があります。
- Fedora Core 13 ターゲットで音声機能を使用している場合、モノラル 16 ビット、44k に設定すると、再生が著しく妨げられる可能性があります。

Mac 環境での音声

以下は、Mac® 環境での既知の問題です。

- Mac クライアントでは、Virtual KVM Client (VKC) および Multi-Platform Client (MPC) を使用してデバイスにアクセスする場合、[Connect Audio] (音声に接続) パネルに再生デバイスが 1 つだけリストされます。リストされたデバイスはデフォルトであり、[Connect Audio] (音声に接続) パネルに「Java Sound Audio Engine」として表示されます。
- Mac ターゲットで Skype® を介して音声を使用すると、音声が破損する可能性があります。

Windows 環境での音声

Windows ® 64 ビット クライアントでは、Virtual KVM Client (VKC) および Multi-Platform Client (MPC) を使用してデバイスにアクセスする場合、[Connect Audio] (音声に接続) パネルに再生デバイスが 1 つだけリストされます。音声デバイスはデフォルト デバイスであり、[Connect Audio] (音声に接続) パネルに「Java Sound Audio Engine」として表示されます。

USB ポートとプロファイル

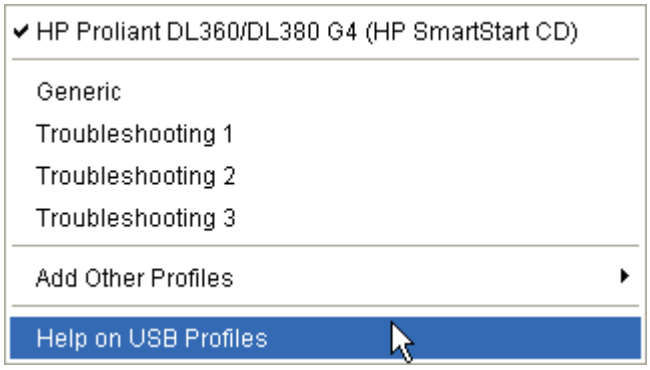
VM-CIM および DL360 の USB ポート

HP® DL360 サーバの背面と前面には、USB ポートがそれぞれ 1 つあります。DL360 では、両方の USB ポートを同時に使用することはできません。つまり、DL360 サーバに対してデュアル VM-CIM を使用することはできません。

ただし、代替策として、DL360 サーバの背面の USB ポートに USB2 ハブを接続し、そのハブにデュアル VM-CIM を接続することはできます。

USB プロファイルの選択に関するヘルプ

Virtual KVM Client (VKC) で KVM ターゲット サーバに接続しているとき、[USB Profile] (USB プロファイル) メニューの [Help on USB Profiles] (USB プロファイルに関するヘルプ) をクリックすると、USB プロファイルに関する情報が表示されます。



USB プロファイルに関するヘルプは、[USB Profile Help] (USB プロファイルに関するヘルプ) ウィンドウに表示されます。個々の USB プロファイルの詳細については、「*選択可能な USB プロファイル 『135*p. の*″使用できる USB プロファイル″*参照 』」を参照してください。

サーバで使用されている多様な OS および BIOS に対応する USB プロファイルが、標準で用意されています。このため、リモート USB デバイスとターゲット サーバを最適な方法で対応付けることができます。

″Generic″ プロファイルは、一般に使用されているほとんのターゲット サーバ構成のニーズに対応しています。

その他のプロファイルは、一般的に展開される他のサーバ設定 (例: Linux® や Mac OS X®) の特定のニーズを満たすように提供されています。

さらに、ターゲット サーバが BIOS レベルで動作しているときなどに仮想メディア機能の互換性を高めるための、さまざまなプロファイルが用意されています (プロファイルの名前がプラットフォーム名と BIOS のリビジョンで構成されている)。

[Add Other Profiles] (他のプロファイルを追加) をクリックすると、システムで使用可能なその他のプロファイルが一覧表示されます。この一覧で設定したプロファイルは、[USB Profile] (USB プロファイル) メニューに追加されます。この一覧には、トラブルシューティング用プロファイルのセットがあります。これらのプロファイルは、構成における制限事項を明確化するのに役立ちます。

[USB Profile] (USB プロファイル) メニューの項目を変更するには、KX II ローカル コンソールまたは KX II リモート コンソールの [Device Settings] (デバイス設定) メニューの [Port Configuration] (ポート設定) ページを使用します。

Raritan から提供されている標準の USB プロファイルがどれもターゲット サーバの要件を満たさない場合、Raritan のテクニカル サポート部門がお客様と協力し、そのターゲット サーバに対する解決策を探ることができます。次の手順を実行することを推奨します。

1. Raritan の Web サイト (www.raritan.com) の [Firmware Upgrade] (ファームウェアのアップグレード) ページで最新のリリース ノートを調べ、ご使用のターゲット サーバ構成に合った解決策が提供されているかどうかを確認します。
2. 提供されていない場合は、Raritan のテクニカル サポート部門に問い合わせます。その際、次の情報を準備してください。
   a. ターゲット サーバに関する情報 (製造元、モデル、BIOS、およびバージョン)。
   b. 用途 (例: イメージをリダイレクトし、サーバの OS を CD-ROM から再ロードする)。

スマート カード リーダー使用時の USB プロファイルの変更

ターゲット サーバの USB プロファイルの変更が必要になる場合があります。たとえば、接続速度が [High Speed USB] (高速 USB) のときにターゲットに問題が発生する場合、接続速度を [Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) に変更する必要があります。

プロファイルを変更すると、「新しいハードウェアが検出されました」というメッセージが表示されることがあります。この場合は、管理者権限でターゲットにログインして USB ドライバを再インストールする必要があります。この現象は、ターゲットで USB デバイスの新しい設定が検出される最初の数回だけ発生する可能性があります。その後はターゲットによって正しいドライバが選択されます。

注: この機能は、KX II 2.4.0 (以降) で使用できます。

仮想メディア

Windows 環境での VKC および AKC を介した仮想メディア

Windows XP® の Administrator 権限および標準ユーザ権限は、Windows Vista® および Windows 7® とは異なります。

Vista または Windows 7 でユーザ アクセス制御 (UAC) を有効にすると、ユーザがアプリケーションの実行に必要とする最低レベルの権限が与えられます。たとえば、Internet Explorer® でユーザに管理者レベルのタスクの実行を明示的に許可するための [管理者として実行] オプションが用意されています。このオプションを使用しない場合、ユーザは管理者としてログインしていても管理者レベルのタスクを実行できません。

これらの両方の機能は、ユーザが Virtual KVM Client (VKC) および Active KVM Client (AKC) を使用してアクセスできる仮想メディアのタイプに影響します。これらの機能の詳細および使用方法については、Microsoft® のヘルプを参照してください。

ユーザが Windows 環境で VKC および AKC を使用してアクセスできる仮想メディアのタイプを以下に示します。機能をクライアント別に分類し、各 Windows ユーザ役割がアクセスできる仮想メディア機能を示します。

Windows XP

VKC および AKC を Windows XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Windows Vista および Windows 7

VKC および AKC を Windows Vista または Windows 7 環境で実行し、UAC が有効になっている場合は、ユーザの Windows 役割に応じて以下の仮想メディア タイプにアクセスできます。

クライアント	管理者	標準ユーザ
AKC および VKC	アクセス先: • 固定ドライブと固定ドライブ パーティション • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ	アクセス先: • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ

ファイル追加後に仮想メディアが最新の情報に更新されない

仮想メディア ドライブがマウントされた後、そのドライブにファイルを追加した場合、ターゲット サーバ側でそのファイルがすぐに表示されないことがあります。表示するには、仮想メディア接続をいったん解除し、再確立します。

アクティブ システム パーティション

Mac または Linux クライアントからアクティブ システム パーティションをマウントすることはできません。

Linux Ext3/4 ドライブ パーティションは、仮想メディアを接続する前に umount /dev/<device label> でアンマウントしておく必要があります。

ドライブ パーティション

オペレーティング システム間のドライブ パーティションの制限は、以下のとおりです。

- Windows および Mac の各ターゲットでは Linux 形式のパーティションの読み取りはできない
- Windows® および Linux® では Mac 形式のパーティションの読み取りはできない
- Linux でサポートされているのは Windows Fat パーティションのみ
- Windows FAT および NTFS は Mac でサポートされている
- Mac ユーザがターゲットサーバに接続するためには、既にマウントされているデバイスをアンマウントする必要があります。デバイスをアンマウントするには、>diskutil umount /dev/disk1s1 を使用し、再マウントするには、diskutil mount /dev/disk1s1 を使用します。

仮想メディアの **Linux** ドライブが **2** 回リストされる

KX II 2.4.0 以降および LX 2.4.5 以降では、ユーザが Linux™ クライアントに root ユーザとしログインしている場合、ドライブが［ローカル ドライブ］ドロップダウン リストに 2 回リストされます。たとえば、eg /dev/sdc と eg /dev/sdc1 が表示されます。1 つ目のドライブはブートセクタ、2 つ目のドライブはディスクの最初のパーティションです。

Mac および **Linux** でマップしてロックしたドライブ

Mac® および Linux® クライアントからマップされたドライブは、接続されたターゲットにマウントされた場合にロックされません。これは、Mac および Linux のサポートを提供する KX II 2.4.0（以降）および LX 2.4.5（以降）にのみ該当します。

D2CIM-VUSB を使用して Windows 2000 サーバ上の仮想メディアにアクセスする

D2CIM-VUSB を使用して Windows 2000® サーバ上の仮想メディアに仮想メディア ローカル ドライブにアクセスすることはできません。

仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間

ターゲット サーバにおいてメディアが仮想マウントされている場合、そのターゲット サーバの BIOS の起動に要する時間が長くなることがあります。

▶ 起動に要する時間を短縮するには

1. VKC を終了し、仮想メディア ドライブを完全に解放します。
2. ターゲット サーバを再起動します。

高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー

[高速 USB] 接続でターゲットに問題が発生する場合、またはターゲットで接続やケーブルの追加（たとえば、ドングルを使用したブレード サーバへの接続）に起因する信号劣化により USB プロトコル エラーが発生する場合は、[仮想メディア CIM でフル スピードを使用] の選択が必要になることがあります。（たとえば、ドングルを介したブレード サーバへの接続）。

CIM

Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合

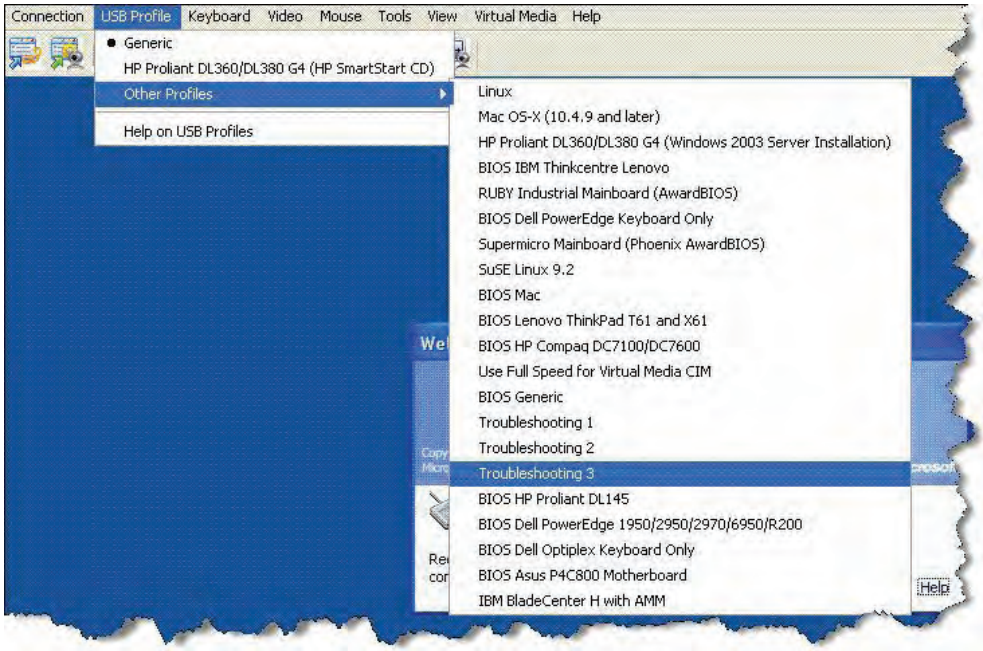
Linux® ターゲット サーバに接続している Windows® クライアントで 3 ボタン マウスを使用する場合、左マウス ボタンがその 3 ボタン マウスの中央ボタンに対応付けられることがあります。

Windows 2000 での複合 USB デバイスの動作

Windows 2000® では、Raritan の D2CIM-VUSB のような複合 USB デバイスはサポートされていないので、非複合 USB デバイスと同じように扱われます。

したがって、D2CIM-VUSB によってマッピングされているドライブに対する [Safely Remove Hardware] (ハードウェアの安全な取り外し) アイコンがシステム トレイに表示されません。また、D2CIM-VUSB を取り外す際、警告メッセージが表示されることがあります。ただし、Raritan が確認したところでは、このメッセージが表示されても何の問題も発生しません。

米国にある Raritan の設計部門は、この [Safely Remove Hardware] (ハードウェアの安全な取り外し) アイコンを表示すると共にこの警告メッセージの表示を回避するための構成を考え出しました。この構成では、D2CIM-DVUSB 仮想メディア アダプタと "Troubleshooting 3" USB プロファイルを使用する必要があります。この USB プロファイルは、D2CIM-DVUSB を、仮想メディア接続を 1 本しかサポートしない非複合 USB デバイスとして設定するものです。Raritan は、米国と日本でこの構成を十分にテストしました。



CC-SG

VKC のバージョンが CC-SG プロキシ モードで認識されない

VKC を CommandCenter Secure Gateway (CC-SG) からプロキシ モードで起動した場合、VKC のバージョンが認識されません。[About Raritan Virtual KVM Client] (VKC のバージョン情報) ダイアログ ボックスで、バージョンが "Version Unknown" (不明なバージョン) と表示されます。

シングル マウス モード: Firefox を使用して CC-SG の管理下にあるターゲットに VKC を介してアクセスする場合

Firefox® と DCIM-PS2 または DCIM-USBG2 を使用して、CC-SG の管理下にある KX II または KSX II ターゲットに接続しているとき、VKC でシングル マウス モードに切り替えると、VKC ウィンドウからフォーカスが外れ、マウスが応答しなくなります。この場合、マウスの左ボタンをクリックするかまたは Alt キーを押しながら Tab キーを押し、フォーカスを VKC ウィンドウに戻します。

プロキシ モードと MPC

KX II を CC-SG の管理下で使用しており、MPC の使用を計画している場合、CC-SG プロキシ モードを使用しないでください。

デバイスのポート間の移動

同じ Raritan デバイスのポート間で移動し、1 分以内に管理作業を再開した場合、CC-SG によってエラー メッセージが表示されることがあります。管理作業を再開すると、最新の情報に更新されます。

Ap F FAQ

この章の内容

一般的な FAQ 414
リモート アクセス 416
ユニバーサル仮想メディア 419
帯域幅と KVM-over-IP のパフォーマンス 423
Ethernet と IP ネットワーキング 428
IPv6 ネットワーキング 431
サーバ 433
ブレード サーバ 434
インストール 437
ローカル ポート 439
拡張ローカル ポート (Dominion KX2-832 および KX2-864 モデルのみ) 442
インテリジェント電源タップ (PDU) の管理 443
ローカル ポートの統合およびカスケード接続 445
コンピュータ インタフェース モジュール (CIM) 448
セキュリティ 450
スマート カード認証と CAC 認証 452
管理機能 453
ドキュメントおよびサポート 454
その他 455

一般的な FAQ

質問	回答
Dominion KX II とは何ですか。	Dominion KX II は第 2 世代のデジタル KVM (キーボード、ビデオ、マウス) スイッチです。1、2、4、または 8 人の IT 管理者は BIOS レベルの機能を使用して、ネットワーク上の 8、16、32、または 64 台のサーバにアクセスし、そのサーバを制御できます。Dominion KX II ではハードウェアと OS が完全に独立しているため、サーバがダウンしているときでも、ユーザはトラブルシューティングや再設定を行えます。 ラックからアクセスする場合も Dominion KX II では従来のアナログ KVM スイッチと同様の機能性と利便性が提供され、スペースやコストを削減できます。その一方、Dominion KX II には業界最高のパフォーマンスを誇る KVM-over-IP 技術も組み込まれているため、複数の管理者がネットワーク接続されたワークステーション、iPhone®、iPad® からサーバ KVM コンソールにアクセスできます。

質問	回答
Dominion KX II がリモート制御ソフトウェアと異なるのは、どのような点ですか。	Dominion KX II をリモートで使用すると、インタフェースは一見 pcAnywhere™、Windows® Terminal Services/Remote Desktop、VNC などのリモート制御ソフトウェアと同じに見えます。しかし Dominion KX II はソフトウェアではなく、ハードウェア ソリューションであるため、より強力な機能を提供します。 ハードウェアや OS に依存しない: Dominion KX II を使用して、Windows、Linux®、Solaris™ などを実行している Intel®、Sun®、PowerPC など、一般的なさまざまな OS を実行しているサーバを管理できます。 状態に依存せず、エージェントも不要 - Dominion KX II では、管理サーバで OS を起動している必要がありません。さらに、管理サーバに特別なソフトウェアをインストールする必要もありません。 アウトオブバンド – 管理サーバ自身のネットワーク接続が利用できない場合でも、Dominion KX II を経由して管理できます。 BIOS レベルのアクセス - サーバが起動時に停止した場合や、セーフ モードでの起動が必要な場合、またはシステム BIOS パラメータの変更が必要な場合でも、Dominion KX II は問題なく動作し、これらの設定を行えます。
Dominion KX II をラックにマウントすることができますか。	はい。Dominion KX II には、標準 19 インチ ラック マウント ブラケットが同梱されています。また、逆向きに収容して、サーバ ポートがある面を前にすることもできます。
Dominion KX II のサイズはどのくらいですか。	Dominion KX II の高さはわずか 1U であり (2U である KX2-864 および KX2-464 を除く)、標準の 19 インチ ラックに収容できます。奥行きはわずか 29 cm です。Dominion KX2-832 および KX2-864 の奥行きは 36 cm です。

リモート アクセス

質問	回答
Dominion KX II ごとに何人のユーザがサーバにリモート アクセスできますか。	Dominion KX II では、ユーザ チャネルごとに最大 8 人のユーザが 1 台のターゲット サーバに同時にリモート アクセスし、そのターゲット サーバを制御することができます。DKX2-116 のような 1 チャネルのデバイスの場合、最大 8 人のリモート ユーザが 1 台のターゲット サーバにアクセスして制御することができます。DKX2-216 のような 2 チャネルのデバイスの場合は、チャネル 1 で最大 8 人のユーザがあるターゲット サーバにアクセスして制御し、また、チャネル 2 で別の最大 8 人のユーザが別のターゲット サーバにアクセスして制御することができます。4 チャネルのデバイスの場合は、チャネルごとに最大 8 人のユーザ（合計で 8 x 4 = 32 人のユーザ）が、最大 4 台のターゲット サーバにアクセスし、それらのターゲット サーバを制御することができます。同様に、8 チャネルのデバイスの場合は、最大 8 人のユーザが 1 台のターゲット サーバにアクセスし、8 チャネルで最大 32 人のユーザがターゲット サーバにアクセスできます。
iPhone または iPad からリモートでサーバにアクセスできますか。	はい。Dominion KX II リリース 2.4 および CC-SG リリース 5.2 から、KX II に接続されたサーバに、iPhone または iPad を使用してアクセスできるようになりました。
2 人のユーザが同じターゲット サーバの画面を同時に表示できますか。	はい。最大 8 名のユーザが 1 台のサーバに同時にアクセスし、制御できます。
2 人のユーザが同じターゲット サーバにアクセスするとき、一方のユーザがリモートでアクセスし、もう一方のユーザがローカル ポートからアクセスすることはできますか。	はい。ローカル ポートはリモート ″ポート″ からは完全に独立しています。PC 共有機能を使用することで、ローカル ポートから同じサーバにアクセスできます。

<table>
<tr><th>質問</th><th>回答</th></tr>
<tr><td>クライアントから Dominion KX II にアクセスする場合、どのようなハードウェア、ソフトウェア、ネットワーク設定が必要ですか。</td><td>Dominion KX II は Web アクセスが可能なため、アクセスするための特別なソフトウェアをお客様がクライアントにインストールする必要はありません（なお、www.raritan.com でオプションのクライアント ソフトウェアを入手することもできます。このクライアント ソフトウェアは、外部モデムを使用してアクセスする場合に必要となります。）

Dominion KX II には、主要な Web ブラウザ Internet Explorer® および Firefox® を使用してアクセスできます。Windows、Linux、Macintosh® の各デスクトップ コンピュータ上で、Raritan の Windows クライアント、および Java™ ベースの Multiplatform や Virtual KVM Client™ を使用して Dominion KX II にアクセスできます。

Dominion KX II 管理者は、便利なブラウザベースのインタフェースを使用して、リモート管理（パスワードとセキュリティの設定、サーバ名の変更、IP アドレスの変更など）を行うこともできます。</td></tr>
<tr><td>Dominion KX II へのアクセスに使用されるアプレットのファイル サイズはどのくらいですか。また、この VKC アプレットを取得するのにどのくらいの時間がかかりますか。</td><td>Dominion KX II へのアクセスに使用される Virtual KVM Client (VKC) アプレットのサイズは約 500 キロバイトです。以下の表に、Dominion KX II のアプレットの取得に必要な時間をネットワークの速度ごとに示します。
<table>
<tr><td>100 Mbps</td><td>100 Mbps ネットワークの理論上の速度</td><td>0.05 秒</td></tr>
<tr><td>60 Mbps</td><td>100 Mbps ネットワークの実効速度</td><td>0.08 秒</td></tr>
<tr><td>10 Mbps</td><td>10 Mbps ネットワークの理論上の速度</td><td>0.4 秒</td></tr>
<tr><td>6 Mbps</td><td>10 Mbps ネットワークの実効速度</td><td>0.8 秒</td></tr>
<tr><td>512 Kbps</td><td>標準的なケーブル モデムのダウンロード速度</td><td>8 秒</td></tr>
</table></td></tr>
</table>

質問	回答
ネットワークが利用できなくなった場合、Dominion KX II に接続されているサーバにはどのようにアクセスするのですか。	サーバには、ローカル アクセスするか、モデムを使用してアクセスできます。 Dominion KX II は、外付けモデムを接続する専用モデム ポートを搭載しています。
Windows KVM クライアントは用意されていますか。	はい。Raritan Active KVM Client (AKC) というネイティブの .NET Windows クライアントが用意されています。
Windows 以外の KVM クライアントは用意されていますか。	はい。Windows 以外のユーザも、Virtual KVM Client (VKC) と Multi-Platform Client (MPC) からデータ センタのターゲット サーバに接続できます。MPC は、Web ブラウザ経由でもスタンドアロンでも実行でき、Dominion KX I と KX II の両方のスイッチに接続されているサーバにアクセスできます。Raritan の Dominion KX II および KVM Client のユーザ ガイドを参照してください。
KVM クライアントは多言語対応ですか。	はい。Dominion KX II のリモート HTML ユーザ インタフェースおよび KVM クライアントでは、日本語、簡体中国語、繁体中国語に対応します。スタンドアロンでも CC-SG 経由でも多言語をサポートします。
KVM クライアントにおいてデュアル液晶モニタはサポートされていますか。	はい。机上で複数台の液晶モニタを使用して生産性を向上させたいお客様のために、Dominion KX II では複数台のモニタに対して KVM セッションを確立できるようになっています。全画面モードと標準モードのどちらも使用できます。
ビデオ カードを 2 枚搭載したサーバをサポートしますか。	はい。リリース 2.5 では、ビデオ カードを 2 枚搭載したサーバは、リモート ユーザが利用できる拡張デスクトップ設定でサポートされています。

ユニバーサル仮想メディア

質問	回答
Dominion KX II のどのモデルで仮想メディアがサポートされていますか。	すべての Dominion KX II モデルにおいて仮想メディアがサポートされています。スタンドアロンでも、Raritan の集中管理アプライアンスである CommandCenter® Secure Gateway を通じても使用できます。
Dominion KX II では、どのタイプの仮想メディアがサポートされていますか。	Dominion KX II では、以下のタイプのメディアがサポートされています。内蔵または USB 接続された CD/DVD ドライブ、USB 接続された大容量ストレージ デバイス、PC の内蔵ハード ディスク、および ISO イメージです。

質問	回答
仮想メディアに必要なものは何ですか。	Dominion KX II 用の仮想メディア CIM として、デジタル CIM、D2CIM-VUSB、または D2CIM-DVUSB が必要です。 D2CIM-VUSB には USB コネクタが 1 つあり、仮想メディアを OS レベルで利用したいお客様に適しています。 D2CIM-DVUSB には USB コネクタが 2 つあり、仮想メディアを BIOS レベルで利用したいお客様に適しています。 D2CIM-DVUSB は、スマート カード認証、カスケード接続、デジタル音声にも必要です。 どちらの CIM でも、USB 2.0 インタフェースに対応しているターゲット サーバへの仮想メディア セッションがサポートされています。32 個セットおよび 64 個セットのお得な CIM パッケージが用意されています。これらの CIM でも、ずれないマウス (Absolute Mouse Synchronization™) やリモート ファームウェア更新がサポートされています。 弊社の CIM は、従来からアナログ VGA ビデオをサポートしています。3 つの新しいデュアル仮想メディア CIM では、DVI、HDMI、DisplayPort などのデジタル ビデオ形式をサポートしています。この新しい CIM には、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、 および D2CIM-DVUSB DP があります。
仮想メディアは安全ですか。	はい。仮想メディアのセッションは、256 ビットの AES、128 ビットの AES または RC4 暗号化によって保護されます。

質問	回答
仮想メディアは実際に音声をサポートしていますか。	はい。音声の再生と Dominion KX II に接続されたサーバへの録音が可能です。データセンタ内のリモート サーバで再生するサウンドや音声を、デスクトップ PC またはラップトップに接続したスピーカーを使用して聞くことができます。また、PC またはラップトップに接続したマイクを使用してリモート サーバに録音することもできます。デジタル CIM または D2CIM-DVUSB デュアル仮想メディア CIM が必要です。
USB プロファイルとは何ですか。	一部のターゲット サーバでは、仮想メディアなど USB ベースのサービスを利用するために、特別に構成された USB インタフェースを必要とします。USB プロファイルは、KX II の USB インタフェースをターゲット サーバの特性に合わせて調整するものです。
USB プロファイルを使用するのはなぜですか。	USB プロファイルは、BIOS レベルで特に必要となります。仮想メディア ドライブにアクセスする際、BIOS レベルでは USB 仕様が完全にサポートされていないことがあります。一方、USB プロファイルは OS レベルで使用されることもあります。たとえば、Mac サーバや Linux サーバにおいてマウス動作を同期させる場合などです。
USB プロファイルはどのように使用しますか。	管理者は KX II の [Port Configuration] (ポート設定) ページで、特定の USB プロファイルを使用するように個々のポートまたはポート グループを設定できます。必要があれば、USB プロファイルを KX II クライアントで選択することもできます。詳細については、ユーザ ガイドを参照してください。
仮想メディアを利用する際、USB プロファイルを必ず設定する必要がありますか。	いいえ。仮想メディアを OS レベルで利用する場合や、仮想メディアにアクセスせずに BIOS レベルで操作する場合、デフォルトの USB プロファイルで十分なケースがほとんどです。

質問	回答
使用可能なプロファイルはどれですか。詳細情報はどこで入手できますか。	使用できるプロファイルや詳細については、ユーザ ガイドを参照してください。

帯域幅と KVM-over-IP のパフォーマンス

質問	回答
KVM-over-IP システムで使用される帯域幅はどのくらいですか。	Dominion KX II には、次世代の KVM-over-IP 技術が搭載されています。この技術によって、最高のビデオ圧縮を実現できます。Raritan は、高品質ビデオ伝送と帯域幅節約に関する数多くの技術賞を獲得しています。 Dominion KX II は、ターゲット サーバから受信したキーボード信号、ビデオ信号、およびマウス信号をデジタル化、圧縮、および暗号化し、IP ネットワーク上で IP パケットをリモート クライアントに送信し、ユーザに対するリモート セッションを確立します。KX II は業界最高水準のビデオ処理アルゴリズムを備えているので、ローカル アクセスする場合と遜色ない画質が得られます。 画面が変更される際、帯域幅の大部分が使用されるので、キーボードとマウスの処理に割り当てられる帯域幅がかなり狭くなります。 重要なのは、帯域幅はユーザがアクティブであるときにのみ使用される、という点です。使用される帯域幅は、サーバの画面表示の変更量に基づいて決まります。 画 面が変更されない場合、つまり、ユーザがサーバとの間で対話操作をしていない場合、一般に帯域幅は使用されません。ユーザがマウスを動かした場合やキー ボードで文字を入力した場合、少量の帯域幅が

	使用されます。複雑なスクリーンセーバを実行している場合や動画を再生している場合、多量の帯域幅が使用される可能性があります。
帯域幅は KVM-over-IP システムのパフォーマンスにどのような影響を及ぼしますか。	一般に、帯域幅とパフォーマンスはトレードオフの関係にあります。使用できる帯域幅が広いほど、パフォーマンスが向上します。帯域幅に制約のある環境では、パフォーマンスが低下するおそれがあります。Dominion KX II は、多種多様な環境で高いパフォーマンスを得られるように最適化されています。
帯域幅に影響を及ぼす要素は何ですか。	帯域幅の使用量を決める要素はいろいろあります。最大の要素は前述のとおり、ターゲット サーバの画面表示の変更量です。画面表示の変更量は、ユーザの操作内容によって異なります。 その他の要素としては、サーバのビデオ解像度、ネットワーク速度、ネットワーク特性、クライアント PC のリソース、ビデオ カードのノイズなどがあります。 Dominion KX II は高度なビデオ処理アルゴリズムを備えているので、多種多様な環境で帯域幅とパフォーマンスを最適化することができます。また、帯域幅使用を最適化するための設定項目が多数あるので、きめ細かい設定が可能です。特に、リモート クライアント (VKC および MPC) の接続速度では、使用する帯域幅を減らすように設定することができます。 KX I と異なり、ノイズ フィルタの設定値は、Dominion KX II の使用帯域幅の縮小やパフォーマンスの向上

<table>
<tr><td></td><td>にあまり影響を及ぼしません。</td></tr>
<tr><td>KX II で一般的な作業を行う際に使用される帯域幅はどのくらいですか。</td><td>使用帯域幅は、主にユーザの操作内容によって決まります。画面表示の変更量が多いほど、使用される帯域幅も広くなります。

次 の表に、ネットワークが 100 Mbps LAN、ターゲット サーバの OS が Windows XP、画面解像度が 1024 x 768、という環境における、標準的な操作と使用帯域幅を示します。使用帯域幅については、デフォルト設定の場合、接続速度に 1 Mbps/15 ビット カラーを指定した場合、接続速度に 1 Mbps/8 ビット カラーを指定した場合、の 3 つのケースの値を示します。

<table>
<tr><td>ユーザの操作</td><td>デフォルト設定</td><td>1Mbps および 15 ビット カラー</td><td>1Mbps および 8 ビット カラー</td></tr>
<tr><td>アイドル状態の Windows デスクトップ</td><td>0 kbps</td><td>0 kbps</td><td>0 kbps</td></tr>
<tr><td>マウス ポインタを動かす</td><td>5 〜 15 kbps</td><td>2 〜 6 kbps</td><td>2 〜 3 kbps</td></tr>
<tr><td>アイコンをドラッグする</td><td>40 〜 70 kbps</td><td>10 〜 25 kbps</td><td>5 〜 15 kbps</td></tr>
<tr><td>フォルダをドラッグする</td><td>10 〜 40 kbps</td><td>5 〜 20 kbps</td><td>5 〜 10 kbps</td></tr>
<tr><td>テキスト ウィンドウ</td><td>50 〜 100</td><td>25 〜 50</td><td>10 〜 15</td></tr>
</table></td></tr>
</table>

を開く	kbps	kbps	kbps
キーを連続入力する	1 kbps	0.5 ～ 1 kbps	0.2 ～ 0.5 kbps
テキストウィンドウをスクロールする	1050 kbps	5 ～ 25 kbps	2 ～ 10 kbps
テキストウィンドウを閉じる	50 ～ 100 kbps	20 ～ 40 kbps	10 ～ 15 kbps
パネルを開く	50 ～ 100 kbps	60 ～ 70 kbps	20 ～ 30 kbps
パネル内のタブを切り替える	40 ～ 50 kbps	20 ～ 50 kbps	10 ～ 20 kbps
パネルを閉じる	50 ～ 100 kbps	40 ～ 60 kbps	20 ～ 30 kbps
パネルのオプションを変更する	2 ～ 10 kbps	1 ～ 5 kbps	1 ～ 3 kbps
ブラウザで Web ページを開く	100 ～ 300 kbps	50 ～ 200 kbps	40 ～ 80 kbps
ブラウザをスクロールする	75 ～ 200 kbps	50 ～ 200 kbps	30 ～ 100 kbps
ブラウザを閉じる	100 ～ 150 kbps	75 ～ 100 kbps	30 ～ 60 kbps
[スタート] メニューを開く	75 ～ 100 kbps	50 ～ 75 kbps	20 ～ 30 kbps
[スタート] メニューを閉じる	75 ～ 100 kbps	25 ～ 50 kbps	10 ～ 15 kbps

<table>
<tr><td></td><td>
<table>
<tr><td>「宇宙飛行」スクリーンセーバ</td><td>25 ～ 50 kbps</td><td>10 ～ 15 kbps</td><td>7 ～ 10 kbps</td></tr>
<tr><td>「3D パイプ」スクリーンセーバ</td><td>10 ～ 100 kbps</td><td>5 ～ 20 kbps</td><td>2 ～ 10 kbps</td></tr>
<tr><td>Windows Media 動画</td><td>500 ～ 1,200 kbps</td><td>300 ～ 500 kbps</td><td>150 ～ 300 kbps</td></tr>
<tr><td>QuickTime® 動画 1</td><td>700 ～ 2,500 kbps</td><td>400 ～ 500 kbps</td><td>150 ～ 350 kbps</td></tr>
<tr><td>QuickTime 動画 2</td><td>1500 ～ 2,500 kbps</td><td>400 ～ 550 kbps</td><td>200 ～ 350 kbps</td></tr>
</table>

使用帯域幅を縮小するように設定した場合、ほぼすべての操作において使用帯域幅が大幅に縮小します。15 ビット カラー設定にした場合、パフォーマンスはデフォルト設定時に近くなります。他にも、使用帯域幅を縮小できる設定項目があります。

この表に示した帯域幅値は単なる例であり、さまざまな要素によって変動します。</td></tr>
<tr><td>使用帯域幅を縮小するにはどうすればよいですか。</td><td>KX II の、ユーザ向けのリモート クライアントでさまざまな設定を行うことにより、帯域幅とパフォーマンスを最適化できます。デフォルト設定では、標準の LAN/WAN 環境において、ローカル アクセスする場合と同等のパフォーマンスが得られると共に、使用帯域幅が節約されます。

帯域幅管理に関する設定項目は、接続速度と色深度です。使用帯域幅を縮小するには、次のとおりにしま</td></tr>
</table>

	す。 接 続速度。接続速度を下げると、使用帯域幅を大幅に縮小できます。標準的な LAN/WAN 環境において、接続速度を 1.5 Mbps または 1 Mbps に設定した場合、パフォーマンスを比較的良好なレベルに維持したまま、使用帯域幅を縮小できます。接続速度をさらに下げると、使用帯域幅をさらに縮小でき るので、低速ネットワークに適しています。 色深度。色深度を下げると、使用帯域幅を大幅に縮小し、パフォーマンスを高めることができます。ただし、使用される色が少なくなるので画質が低下します。この設定は、一部のシステム管理作業に適しています。 低速インターネットの場合、8 ビット カラーを使用するかまたは色深度を下げると、使用帯域幅を縮小し、パフォーマンスを向上させることができます。 使用帯域幅を縮小するためのその他のヒントを次に示します。 デスクトップの壁紙に、複雑な画像ではなく無地の画像を使用する。 スクリーンセーバを無効にする。 ターゲット サーバで低いビデオ解像度を使用する。 Windows のコントロール パネルの [画面] で、[ドラッグ中にウィンドウの内容を表示する] チェック ボッ

	クスをオフにする。 シンプルな画像、テーマ (例: Windows クラシック)、およびデスクトップを使用する
ネットワークが低速である場合、どうすればよいですか。	接続速度と色深度を下げることにより、低速ネットワークでもパフォーマンスを最大化できます。 たとえば、MPC または VKC で、接続速度を 1.5 Mbps または 1 Mbps、色深度を 8 ビットに設定します。 ネットワークが非常に低速な場合は、接続速度と色深度をさらに下げることができます。 モデム接続の場合、パフォーマンスを最適化するために、KX II のデフォルト設定は、非常に低速の接続速度と縮小された色深度に自動的に設定されます。
インターネット経由で接続したいと考えています。どの程度のパフォーマンスが期待できますか。	パフォーマンスは、リモート クライアントと KX II の間のインターネット接続の帯域幅と伝送遅延によって決まります。ケーブル モデム接続または高速 DSL 接続の場合、LAN/WAN 接続に近いパフォーマンスが得られる可能性があります。低速ネットワークの場合は、前述の推奨値に設定し、パフォーマンスを向上させてください。
帯域幅の広い環境で KX II を使用することを検討しています。パフォーマンスを最大化するにはどうすればよいですか。	デフォルト値を使用した場合、帯域幅の広い環境において高いパフォーマンスが得られます。 接続速度を 100 Mbps または 1 Gbps、色深度を 15 ビット RGB カラーにそれぞれ設定してください。
IP ネットワーク上でのリ	Dominion KX は、フル HD リモート

モート アクセスにおいてサポートされている最大ビデオ解像度はどのくらいですか。	ビデオ解像度 (1920 x 1080) をサポートしている、業界初かつ唯一の KVM-over-IP スイッチです。 また、よく使われる横長画面形式 (例: 1600 x 1200、1680 x 1050、1440 x 900) もサポートされているので、リモート ユーザは最近販売されている高解像度モニタを使用できます。
音声はどれくらいの帯域幅を使用しますか。	使用する音声形式のタイプにもよりますが、CD 品質の音声を聞く場合は、約 1.5 Mbps が使用されます。
DVI ポート搭載サーバはどのように接続できますか。	DVI-A (アナログ) と DVI-I (アナログ/デジタル統合) をサポートする DVI ポートを備えたサーバでは、Raritan の低価格の ADVI-VGA パッシブ アダプタを使用して、サーバの DVI ポートを VGA プラグに変換し、KX II CIM の VGA プラグに接続することができます。 DVI-I または DVI-D (デジタル) をサポートする DVI ポートを搭載したサーバでは、新しい D2CIM-DVUSB DVI CIM を使用できます。

質問	回答
使用帯域幅を縮小するにはどうすればよいですか。	KX II の、ユーザ向けのリモート クライアントでさまざまな設定を行うことにより、帯域幅とパフォーマンスを最適化できます。デフォルト設定では、標準の LAN/WAN 環境において、ローカル アクセスする場合と同等のパフォーマンスが得られると共に、使用帯域幅が節約されます。 帯域幅管理に関する設定項目は、接続速度と色深度です。使用帯域幅を縮小するには、次のとおりにします。 接続速度。接続速度を下げると、使用帯域幅を大幅に縮小できます。標準的な LAN/WAN 環境において、接続速度を 1.5 Mbps または 1 Mbps に設定した場合、パフォーマンスを比較的良好なレベルに維持したまま、使用帯域幅を縮小できます。接続速度をさらに下げると、使用帯域幅をさらに縮小できるので、低速ネットワークに適しています。 色深度。色深度を下げると、使用帯域幅を大幅に縮小し、パフォーマンスを高めることができます。ただし、使用される色が少なくなるので画質が低下します。この設定は、一部のシステム管理作業に適しています。 低速インターネットの場合、8 ビット カラーを使用するかまたは色深度を下げると、使用帯域幅を縮小し、パフォーマンスを向上させることができます。 使用帯域幅を縮小するためのその他のヒントを次に示します。 デスクトップの壁紙に、複雑な画像ではなく無地の画像を使用する。 スクリーンセーバを無効にする。 ターゲット サーバで低いビデオ解像度を使用する。 Windows のコントロール パネルの［画面］で、［ドラッグ中にウィンドウの内容を表示する］チェック ボックスをオフにする。 シンプルな画像、テーマ（例: Windows クラシック）、およびデスクトップを使用する

質問	回答
ネットワークが低速である場合、どうすればよいですか。	接続速度と色深度を下げることにより、低速ネットワークでもパフォーマンスを最大化できます。 たとえば、MPC または VKC で、接続速度を 1.5 Mbps または 1 Mbps、色深度を 8 ビットに設定します。 ネットワークが非常に低速な場合は、接続速度と色深度をさらに下げることができます。 モデム接続の場合、パフォーマンスを最適化するために、KX II のデフォルト設定は、非常に低速の接続速度と縮小された色深度に自動的に設定されます。
インターネット経由で接続したいと考えています。どの程度のパフォーマンスが期待できますか。	パフォーマンスは、リモート クライアントと KX II の間のインターネット接続の帯域幅と伝送遅延によって決まります。ケーブル モデム接続または高速 DSL 接続の場合、LAN/WAN 接続に近いパフォーマンスが得られる可能性があります。低速ネットワークの場合は、前述の推奨値に設定し、パフォーマンスを向上させてください。
帯域幅の広い環境で KX II を使用することを検討しています。パフォーマンスを最大化するにはどうすればよいですか。	デフォルト値を使用した場合、帯域幅の広い環境において高いパフォーマンスが得られます。 接続速度を 100 Mbps または 1 Gbps、色深度を 15 ビット RGB カラーにそれぞれ設定してください。
IP ネットワーク上でのリモート アクセスにおいてサポートされている最大ビデオ解像度はどのくらいですか。	Dominion KX は、フル HD リモート ビデオ解像度（1920 x 1080）をサポートしている、業界初かつ唯一の KVM-over-IP スイッチです。 また、よく使われる横長画面形式（例: 1600 x 1200、1680 x 1050、1440 x 900）もサポートされているので、リモート ユーザは最近販売されている高解像度モニタを使用できます。

質問	回答
音声はどれくらいの帯域幅を使用しますか。	使用する音声形式のタイプにもよりますが、CD 品質の音声を聞く場合は、約 1.5 Mbps が使用されます。
DVI ポート搭載サーバはどのように接続できますか。	DVI-A (アナログ) と DVI-I (アナログ/デジタル統合) をサポートする DVI ポートを備えたサーバでは、Raritan の低価格の ADVI-VGA パッシブ アダプタを使用して、サーバの DVI ポートを VGA プラグに変換し、KX II CIM の VGA プラグに接続することができます。 DVI-I または DVI-D (デジタル) をサポートする DVI ポートを搭載したサーバでは、新しい D2CIM-DVUSB DVI CIM を使用できます。

Ethernet と IP ネットワーキング

質問	回答
Dominion KX II の Ethernet インタフェースの速度はどのくらいですか。	Dominion KX II では、10/100 Ethernet に加えてギガビット Ethernet もサポートされています。Dominion KX II では 2 つの 10/100/1000 Ethernet インタフェースがサポートされており、速度と二重化の設定を変更できます (自動検知または手動で設定)。
ワイヤレス接続で Dominion KX II にアクセスできますか。	はい。Dominion KX II は標準の Ethernet を使用するだけでなく、高品質なビデオ表示を保ちつつ、使用する帯域幅を抑えます。そのため、ワイヤレス クライアントを Dominion KX II にネットワーク接続していても、サーバの BIOS レベルの設定と管理をワイヤレスで行えます。

質問	回答
Dominion KX II には、冗長フェイルオーバまたは負荷分散を行うためのデュアル ギガビット Ethernet ポートが用意されていますか。	はい。Dominion KX II には、冗長フェイルオーバ機能を実現するためのデュアル ギガビット Ethernet ポートが搭載されています。プライマリ Ethernet ポート（またはポートに接続されているスイッチやルータ）に障害が発生した場合、Dominion KX II が同じ IP アドレスを持つセカンダリ ネットワーク ポートにフェイルオーバすることにより、サーバの動作が中断されないようにします。自動フェイルオーバは、管理者が有効にする必要があります。
Dominion KX II を VPN で使用できますか。	はい。Dominion KX II では、レイヤ 1 ～ 4 において標準的なインターネット プロトコル (IP) 技術が使用されています。そのため、標準的な Virtual Private Network (VPN) から届いたトラフィックを簡単にトンネリングできます。
KX II とプロキシ サーバを組み合わせて使用できますか。	はい。リモート クライアント PC が適切に設定されている場合、KX II を SOCKS プロキシ サーバと組み合わせて使用することができます。詳細については、ユーザマニュアルまたはオンライン ヘルプを参照してください。
Dominion KX II にネットワーク アクセスできるようにするためには、ファイアウォールで TCP ポートをいくつ開く必要がありますか。	2 つのポートが必要です。TCP ポート 5000 で他の Dominion デバイスを検知して Raritan デバイスと CC-SG 間の通信を行います。また、もちろんポート 443 で HTTPS 通信を行います。
また、これらのポートは変更できますか。	はい。Dominion KX II の TCP ポートは管理者が設定できます。
Dominion KX II は Citrix® と共に使用できますか。	設定を適切に行えば、Dominion KX II を Citrix などのリモート アクセス製品と共に使用できます。ただし、Raritan では十分なパフォーマンスを維持しつつ作業できるかどうかは保証できません。Citrix のような製品は、デジタル KVM スイッチと概念が似ているビデオ リダイレクト技術が使用されています。したがって、併用した場合 2 種類の KVM-over-IP 技術が同時に使用されるという点にご注意ください。

質問	回答
Dominion KX では DHCP を使用できますか。	DHCP アドレス割り当ては使用できますが、Raritan では固定 IP アドレスの設定を推奨しています。Dominion KX II はインフラストラクチャ デバイスであるため、固定 IP アドレスを使用した方が、Dominion KX II に対してより効率的にアクセスし、管理できます。
IP ネットワークから Dominion KX II にアクセスできなくなりました。原因は何でしょうか。	Dominion KX II はお客様の LAN または WAN ネットワークに依存しています。考えられる原因は次のとおりです。 Ethernet のオートネゴシエーション。ネットワークによっては、10/100 オート ネゴシエーションが適切に機能しないため、Dominion KX II ユニットを 100 Mb/全二重に設定するか、ネットワークに最適な設定を行う必要があります。 IP アドレスの重複。Dominion KX II の IP アドレスが他のデバイスと 重複していると、ネットワーク接続を確立できない場合があります。 ポート 5000 の競合。他のデバイスでポート 5000 を使用している場合は、Dominion KX II のデフォルト ポートを変更する必要があります（または、他のデバイスのポートを変更する必要があります)。 Dominion KX II の IP アドレスを変更するか、新しい Dominion KX II に切り替える場合、KX II の IP アドレスと Mac® アドレスがレイヤ 2、レイヤ 3 のネットワークに通知されるまで、十分な時間が必要です。

IPv6 ネットワーキング

質問	回答
IPv6 とは何ですか。	IPv6 は ″Internet Protocol Version 6″ の頭字語です。IPv6 は次世代の IP プロトコルであり、現在使用されている Internet Protocol Version 4 (IPv4) プロトコルを置き換えるものです。 IPv6 は、IPv4 が抱えているさまざまな問題を解決します (例: IPv4 アドレスの枯渇)。 経路選択やネットワーク自動設定などの機能が IPv4 よりも向上しています。IPv6 は徐々に IPv4 を置き換えていくと予想されています。つまり、数年間は両者が共存することになります。 管理者の観点から見ると、IPv6 は IP ネットワークの大きな問題の 1 つを解消します。その問題とは、IP ネットワークの設定作業と保守作業です。
Dominion KX II で IPv6 ネットワーキングがサポートされているのはなぜですか。	米国のさまざまな政府機関と国防総省は、調達時に IPv6 対応製品を購入するよう義務付けられています。また、多くの企業および国 (例: 中国) が、今後数年間で IPv6 に移行する予定です。
デュアル スタックとは何ですか。また、デュアル スタックが必要なのはなぜですか。	デュアル スタックは、IPv4 と IPv6 の両方を同時にサポートする機能です。IPv4 から IPv6 に徐々に移行していくことを考えると、デュアル スタックは IPv6 をサポートするうえで必須機能であると言えます。
Dominion KX II 上で IPv6 を有効にするにはどうすればよいですか。	[Device Settings] (デバイス設定) タブから [Network Settings] (ネットワーク設定) ページを開きます。次に、[IPv6 Address] (IPv6 アドレス) チェック ボックスをオンにし、[IP Auto Configuration] (IP 自動設定) ボックスの一覧で値を選択します。詳細については、ユーザ ガイドを参照してください。

質問	回答
IPv6 アドレスが設定された外部サーバがあります。この外部サーバを Dominion KX II と併用する場合、どうなるでしょうか。	Dominion KX II から外部サーバ (例: SNMP マネージャ、syslog サーバ、LDAP サーバ) の IPv6 アドレスを使用してそれらの外部サーバにアクセスすることができます。 具体的に言うと、Dominion KX II のデュアル スタック アーキテクチャを使用することにより、IPv4 アドレス、IPv6 アドレス、またはホスト名を指定してこれらの外部サーバにアクセスすることができます。つまり Dominion KX II は、今後多くのお客様の社内で発生する IPv4/IPv6 混在環境に対応できます。
Dominion KX I (前世代の KX) で IPv6 はサポートされていますか。	いいえ。Dominion KX I で IPv6 はサポートされていません。
社内ネットワークで IPv6 がサポートされていない場合、どうなるでしょうか。	Dominion KX II は、出荷時設定では IPv4 だけを使用するようになっています。社内ネットワークで IPv6 を使用できる状態になったら、前述の「Dominion KX II 上で IPv6 を有効にするにはどうすればよいですか。」の手順を実行し、IPv4/IPv6 デュアル スタックを有効にします。
IPv6 に関する詳細情報はどこで入手できますか。	www.ipv6.org に、IPv6 に関する全般情報が掲載されています。また、『Dominion KX II ユーザ ガイド』では Dominion KX II における IPv6 のサポートについて説明されています。

サーバ

質問	回答
Dominion KX II の操作は Windows サーバに依存しますか？	必要ありません。ユーザーは、どのようなシナリオでも必ず使用できる KVM インフラストラクチャに依存しているため（問題を解決するために KVM インフラストラクチャを使用するような場面も考えられます）、Dominion KX II は外部サーバからも完全に独立するよう設計されています。
Dominion KX II の Web ブラウザ機能を使用するために、Microsoft Internet Information Services (IIS) などの Web サーバをインストールする必要がありますか。	必要ありません。 Dominion KX II は完全自立型の装置です。IP アドレスを Dominion KX II に割り当てるだけで使用できます。Web ブラウザや認証機能はすべて内蔵されています。
Dominion KX II に特定のワークステーションからアクセスするためには、どのソフトウェアをインストールする必要がありますか？	特別なアクセス用ソフトウェアをインストールする必要はありません。Dominion KX II には Web ブラウザだけを使用してアクセスできます（ただし、モデム接続に必要な、オプションのインストール クライアントは Raritan の Web サイト www.raritan.com から入手できます）。また、Windows を使用していないユーザー向けに、Java ベースのクライアント ソフトウェアが提供されるようになりました。
Dominion KX II に接続するには、サーバでどのような準備が必要ですか？	理想的なマウス同期を実現し、画面表示に影響するスクリーンセーバや電源管理の機能をオフにするように、マウス パラメータ オプションを設定します。
マウス同期機能はどのようになっていますか。	これまでの KVM-over-IP のマウス同期は、不満が残るものでした。Dominion KX II には「ずれないマウス」機能が備わっています。これにより、Windows サーバまたは Apple® Mac サーバを使用している場合は、サーバ側のマウス設定を変更することなく、マウスの動きを厳密に同期させることができます。その他のサーバの場合は、インテリジェント マウス モードまたは高速なシングル マウス モードを使用すれば、サーバ側のマウス設定を変更せずに済みます。

質問	回答
Dominion KX II には何が同梱されていますか？	次のアイテムが同梱されています。(1) Dominion KX II ユニット、(2) クイック セットアップ ガイド、(3) 標準 19 インチ ラック マウント ブラケット、(4) ユーザ マニュアル CD-ROM、(5) ネットワーク ケーブル、(6) クロス ケーブル、(7) 使用地域の AC ライン コード、(8) 保証書とその他の文書。

ブレード サーバ

質問	回答
ブレード サーバを Dominion KX II に接続できますか。	はい。Dominion KX II では、代表的なブレード サーバ メーカー (HP®、IBM®、Dell®、および Cisco®) の主要なブレード サーバ モデルがサポートされています
サポートされているブレード サーバはどれですか。	サポートされているモデルは次のとおりです。Dell PowerEdge® 1855、1955、および M1000e、HP BladeSystem c3000 と c7000、IBM BladeCenter® H、E、および S、Cisco UCS B-Series。
Paragon® ブレード用 CIM は使用できますか。	いいえ。Dominion KX II では、Paragon II のような特別なブレード サーバ用 CIM を使用する必要はありません。
どの CIM を使用すればよいですか。	使用する CIM は、ご使用のブレード サーバの製造元とモデルにおける KVM ポートのタイプによって決まります。サポートされている CIM は、DCIM-PS2、DCIM-USBG2、D2CIM-VUSB、および D2CIM-DVUSB です。
使用可能なアクセスおよび制御の方法はどれですか。	Dominion KX II では、(1) ローカル ポートからアクセス、(2) IP を使用してリモート アクセス、(3) CC-SG 経由でアクセス、(4) モデムを使用してアクセス、という 4 種類の方法により、自動で安全な KVM アクセスが可能です。

質問	回答
複数台のブレード サーバを切り替える際、ホットキーを使用する必要がありますか。	一部のブレード サーバでは、複数台のブレード サーバを切り替える際にホットキーを使用する必要があります。Dominion KX II では、ホットキーを使用する必要はありません。ブレード サーバの名前をクリックするだけで、自動的にそのブレード サーバに切り替わります。ホットキーを明示的に使用する必要はありません。
ブレード サーバの管理モジュールにアクセスできますか。	はい。管理モジュールの URL を定義し、Dominion KX II または CommandCenter Secure Gateway からアクセスすることができます。ワンクリック アクセスが設定されている場合、1 回のクリック操作でアクセスできます。
Dominion KX II には何台のサーバを接続できますか。	パフォーマンス上および信頼性上の理由により、1 台の Dominion KX II に接続できるブレード シャーシは、モデルにかかわらず最大 8 台です。接続するブレード サーバ筐体の台数は、KX II でサポートされているリモート接続数の 2 倍以内にすることを推奨します。たとえば、リモート チャネルが 2 本ある KX2-216 の場合、接続するブレード サーバ シャーシを 4 台以内にすることをお勧めします。もちろん、残りのサーバ ポートにブレード サーバを接続することもできます。
当社は中小企業であり、Dominion KX II を数台しか使用していません。CommandCenter Secure Gateway 管理ステーションを使用する必要がありますか。	いいえ、使用する必要はありません。中小企業のお客様は、新しいブレード サーバを利用する際に CommandCenter Secure Gateway を使用する必要はありません。
当社は大企業であり、CommandCenter Secure Gateway を使用しています。CommandCenter Secure Gateway からブレード サーバにアクセスできますか。	はい。Dominion KX II 上でブレード サーバの設定が完了したら、CommandCenter Secure Gateway から KVM 接続を使用してブレード サーバにアクセスできるようになります。さらに、ブレード サーバは、シャーシ別に CommandCenter Secure Gateway のカスタム ビューにも表示されます。

質問	回答
インバンド KVM アクセスまたは埋め込み KVM アクセスも必要な場合はどうなりますか。	ブレード サーバに対するインバンド アクセスおよび埋め込みアクセスは、CommandCenter Secure Gateway で設定できます。
一部のブレード サーバ上で VMware® を実行しています。この構成はサポートされていますか。	はい。CommandCenter Secure Gateway を使用して、ブレード サーバ上で実行されている仮想マシンを表示し、また、その仮想マシンにアクセスすることができます。
仮想メディアはサポートされていますか。	これは、ブレード サーバによって異なります。HP ブレードは、仮想メディアをサポートできます。IBM BladeCenter (BladeCenter T 以外) は、適切に設定されている場合には仮想メディアをサポートします。仮想メディア CIM (D2CIM-VUSB または D2CIM-DVUSB) を使用する必要があります。
ずれないマウス機能はサポートされていますか。	ブレード筐体内に KVM スイッチを備えているサーバの場合、通常、ずれないマウス機能はサポートされません。HP ブレードおよび Dell の一部のブレード サーバの場合は、CIM を各ブレードに接続できるので、ずれないマウス機能がサポートされます。
ブレード サーバへのアクセスは安全ですか。	はい。ブレード サーバへのアクセスには、Dominion KX II の標準的なセキュリティ機能 (128 ビットまたは 256 ビットの暗号化など) がすべて使用されます。その他、ブレード サーバ特有のセキュリティ機能があります。たとえば、ブレード サーバごとにアクセス権限を付与する機能や、入力されたホットキーを拒否する機能などがあるので、不正アクセスの防止に役立ちます。
Dominion KSX II および KX II-101 で、ブレード サーバはサポートされていますか。	現時点では、これらの製品ではブレード サーバはサポートされていません。

インストール

質問	回答
Dominion KX II をインストールするには、ユニット本体のほかに何を Raritan に注文する必要がありますか？	Dominion KX II に接続するサーバごとに、サーバのキーボード、ビデオ、マウス ポートに直接接続するアダプタである Dominion または Paragon コンピュータ インタフェース モジュール (CIM) が必要です。
導入時、どのタイプの Cat5 ケーブルを使用すればよいですか。	Dominion KX II では、Cat5、Cat5e、または Cat6 の標準 UTP (非シールド ツイスト ペア) ケーブルを使用できます。Raritan のマニュアルや販売資料では、単に「Cat5」と記載されています。実際には、Dominion KX II にはどのブランドの UTP ケーブルも使用できます。
Dominion KX II にはどのような種類のサーバを接続できますか。	Dominion KX II はサーバのベンダを選びません。標準に準拠したキーボード ポート、ビデオ ポート、およびマウス ポートを搭載しているあらゆるサーバを接続できます。さらに、シリアル ポートを搭載したサーバは、P2CIM-SER CIM を使用して管理できます。
どのようにサーバを Dominion KX II に接続すればよいですか？	Dominion KX II に接続するサーバには、サーバのキーボード ポート、ビデオ ポート、マウス ポートに直接接続する Dominion CIM または Paragon CIM が必要です。Cat5、Cat5e、Cat6 などの標準 UTP (非シールド ツイスト ペア) ケーブルを使用して、各 CIM を Dominion KX II に接続します。
サーバは、Dominion KX II からどのくらいの距離に設置できますか?	サーバの種類にもよりますが、一般に、サーバは Dominion KX II から最大で 45 m (150 フィート) 離れた場所に設置できます (印刷版のユーザ マニュアルまたは Raritan Web サイトのユーザ マニュアルを参照してください)。仮想メディア機能とずれないマウス機能をサポートする D2CIM-VUSB の場合は、接続距離を 30 m (100 フィート) 以内にすることをお勧めします。

質問	回答
オペレーティング システムによっては、操作中にキーボードかマウスを切断した場合、システムがロックする場合があります。それらを切断しても Dominion KX II に接続しているサーバがロックしないようにするには、どうすればよいですか？	Dominion コンピュータ インターフェース モジュール (DCIM) ドングルは、それぞれ接続されているサーバに対する仮想キーボードや仮想マウスとして動作します。この技術は、KME (キーボード/マウス エミュレーション) と呼ばれます。Raritan の KME 技術は、データ センタでの使用に耐えるグレードであり、厳正にテストされています。また、ローエンドの KVM スイッチの技術に比べてはるかに高い信頼性が確保されています。この技術には 15 年間以上に及ぶ実績も生かされており、世界中で何百万台ものサーバに実装されています。
Dominion KX II に接続されているサーバには何らかのエージェントをインストールする必要がありますか。	Dominion KX II はハードウェアを介してサーバのキーボード用、ビデオ用、マウス用の各ポートに直接接続されるため、Dominion KX II に接続されたサーバには、ソフトウェア エージェントを一切インストールする必要がありません。
Dominion KX II ユニットごとに何台のサーバを接続できますか？	Dominion KX II モデルでは、1U シャーシの場合は 8、16、または 32 個のサーバ ポートを、2U シャーシの場合は 8 ～ 64 個のサーバ ポートが用意されています。このデジタル KVM スイッチ ポートの密度は、業界の最高水準です。
サーバを Dominion KX II から切断して別の Dominion KX II に再接続した場合、または同じ Dominion KX II ユニットの別のポートに接続した場合、どうなりますか？	サーバ接続先ポートを変更した場合、サーバ ポート名が自動更新されます。この変更内容は、ローカル クライアントおよびすべてのリモート クライアントに反映されます。CC-SG を使用している場合は、CC-SG にも反映されます。

質問	回答
Cisco のルータやスイッチ、Sun ヘッドレス サーバなど、シリアル制御 (RS-232) デバイスは、どのように Dominion KX II に接続すればよいですか。	シリアル制御デバイスの数が少ない場合は、Raritan の P2CIM-SER シリアル変換器を使用して Dominion KX II に接続できます。 お客様は、Dominion KSX II (KVM およびシリアルの統合スイッチ) の導入を検討することもできます。DKSX-144 は、4 つの KVM-over-IP ポートおよび 4 つのシリアル ポートを装備しています。 DKSX-188 は、8 つの KVM-over-IP ポートおよび 8 つのシリアル ポートを装備しています。 ただし、シリアル制御デバイスの数が多い場合は、Raritan のセキュア コンソール サーバである Dominion SX 製品を使用することをお勧めします。Dominion SX は、Dominion KX II よりも割安な価格で、より優れたシリアル機能を提供できます。この SX は使いやすく、設定や管理が簡単であるうえに、展開している Dominion シリーズと完全に統合できます。

ローカル ポート

質問	回答
ラックからサーバに直接アクセスできますか。	はい。Dominion KX II は、ラックで従来の KVM スイッチと同じように機能し、1 組のキーボード、モニタ、マウスを使用して、最大 64 台のサーバを制御できます。ブラウザベースのユーザ インターフェイスまたはホットキーによってサーバを切り替えることができます。

質問	回答
複数台の KX II のローカル ポートを統合できますか。	はい。KX II のカスケード接続機能を利用すれば、複数台の KX II のローカル ポートを別の KX II に接続できます。これにより、データ センタ内の 1 か所から統合ポート リストを使用して、KX II に接続されているサーバにアクセスできます。
自分がローカル ポートを使用しているとき、他ユーザがサーバにリモート アクセスできないように設定できますか。	妨げません。Dominion KX II のローカル ポートには、サーバへの完全に独立したアクセス パスがあります。つまり、ユーザーはラックからサーバにローカル アクセスできます。ラックに同時にリモート アクセスするユーザーの数を制限する必要はありません。
USB キーボードまたは USB マウスをローカル ポートで使用できますか。	はい。Dominion KX II ローカル ポート エリアには、USB キーボード ポートおよびマウス ポートがあります。2011 年 4 月現在、Dominion KX II スイッチには PS/2 ローカル ポートが装備されなくなっています。PS/2 のキーボードおよびマウスを使用しているお客様は、PS/2 – USB アダプタを利用する必要があります。
ローカル アクセスする場合、オンスクリーン ディスプレイ（OSD）は表示されますか。	表示されます。ただし、Dominion KX II のラックからのアクセスは、従来の OSD よりもはるかに優れています。Dominion KX II にはローカル アクセス用に業界初のブラウザベースのインタフェースが実装されされています。また、ローカル ポートではローカル アクセスとリモート アクセスに同じインタフェースが使用されます。さらに、大半の管理機能をローカルで実行できます。
ローカル ポートを使用しているとき、サーバを切り替えるにはどうすればよいですか。	ローカル ポートを使用しているとき、接続されているサーバが、リモート クライアントと同じ画面に表示されます。サーバを切り替えるには、切り替え先サーバをマウスでクリックするか、ホットキーを使用します。

質問	回答
承認されたユーザだけがローカル ポートからサーバにアクセスできるようにするには、どうすればよいですか。	ユーザがローカル ポートを使用するには、リモートでアクセスする場合と同レベルの認証を受ける必要があります。これは次のことを意味します。 Dominion KX II が外部 RADIUS、LDAP、または Active Directory® サーバと連動するよう設定している場合、ユーザがローカルポートへのアクセスを試みると、同じサーバで認証されます。 外部認証サーバが利用できない場合は、Dominion KX II は自身の内部認証データベースにフェイルオーバします。 Dominion KX II は独自のスタンドアロン認証を備えているため、即座にインストールを有効にできます。
ローカル ポートを使用して、接続されているサーバの名前を変更した場合、この変更内容はリモート クライアントにも反映されますか。オプションの CommandCenter アプライアンスには反映されますか？	はい。ローカル ポートの表示は、Raritan の CommandCenter Secure Gateway 管理アプライアンスに加え、リモート アクセス クライアントともまったく同じで、完全に同期しています。つまり、Dominion KX II のオンスクリーン ディスプレイでサーバの名前を変更すると、すべてのリモート クライアントと外部管理サーバがリアルタイムで更新されます。
Dominion KX II のリモート管理ツールを使用して接続されているサーバの名前を変更した場合、ローカル ポート OSD にもその変更が反映されますか？	はい。サーバの名前がリモートで変更された場合や、Raritan のオプションの CommandCenter Secure Gateway 管理アプライアンスを介して変更された場合、この更新は直ちに Dominion KX II のオンスクリーン ディスプレイに反映されます。

拡張ローカル ポート (Dominion KX2-832 および KX2-864 モデルのみ)

質問	回答
拡張ローカル ポートとは何ですか。	Dominion KX2-832 および KX2-864 には、拡張ローカル ポートが搭載されています。KX II の 8 ユーザ モデルには、標準ローカル ポートと新しい拡張ローカル ポートがあります。拡張ローカル ポートを使用すると、Cat5 ケーブルを使用して、ローカル ポートからラックを越えて制御室、データ センタ内の別のポイント、Dominion KX II または Paragon II スイッチにアクセスできます。
拡張ローカル ポートを別の KX II に接続できますか。	はい。KX II のカスケード接続機能を利用すれば、拡張ローカル ポートを別の KX II のサーバ ポートに接続できます。
拡張ローカル ポートにユーザ ステーションは必要ですか。	はい。拡張ローカル ポートの「ユーザ ステーション」として使用できるデバイスには、Paragon II EUST、Paragon II UST、および Cat5 Reach® URKVMG デバイスがあります。さらに、Cat5 ケーブルを使用して拡張ローカル ポートを Dominion KX II または Paragon II スイッチのサーバ ポートに接続できます。この構成を使用して、多くの KX2-8xxx デバイスのローカル ポートを 1 つのスイッチに統合できます。
ユーザ ステーションは Dominion KX II からどのくらい離すことができますか。	接続距離は 61 ～ 304 m (200 ～ 1,000 フィート) ですが、ユーザ ステーションのタイプ、ビデオ解像度、ケーブルのタイプと品質によって異なります。詳細については、ユーザ ガイドまたはリリース ノートを参照してください。
CIM は必要ですか。	CIM は必要ありません。Cat5 ケーブルを接続するだけです。

質問	回答
拡張ローカル ポートを使用する必要はありますか。	いいえ。拡張ローカル ポートは、オプション機能であり、デフォルトでは無効になっています。有効にするには、[Local Port Settings]（ローカル ポート設定）ページを使用します。セキュリティを高めるために標準ローカル ポートを使用しない場合は、標準ローカル ポートを無効にすることもできます。
二重化電源	
Dominion KX II にはデュアル電源オプションがありますか?	はい。Dominion KX II の全モデルは、AC 入力と AC 電源が二重化されており、自動フェイルオーバ機能を備えています。KX II では一方の電源入力や電源に障害が発生すると、もう一方に自動的に切り替えられます。
Dominion KX II で使用する電源では、電圧設定が自動検知されますか？	はい。Dominion KX II の電源は、100 ～ 240 V、50 ～ 60 Hz の範囲の AC 電圧で使用できます。
電源または入力電力に障害が発生した場合、通知されますか。	電源障害は Dominion KX II の前面パネルにある LED でユーザに通知されます。同時に、エントリも監査ログに送信され、KX リモート クライアント ユーザ インタフェースに表示されます。管理者によって設定されている場合は、その後 SNMP イベントまたは syslog イベントが発生します。

インテリジェント電源タップ (PDU) の管理

質問	回答
Dominion KX II にはどのようなタイプのリモート電源管理機能が用意されていますか。	Raritan のインテリジェント PDU は、ターゲット サーバやその他の機器の電源を管理するために Dominion KX II に接続できます。サーバの場合は、簡単な設定作業を一度行えば、サーバ名をクリックするだけで電源を投入または切断したり、停止したサーバに電源を再投入したりできます。

質問	回答
Dominion KX II ではどのようなタイプのパワー ストリップがサポートされていますか?	Raritan の Dominion PX™ 電源タップおよび Remote Power Control (RPC) 電源タップ。 この電源タップには、さまざまなコンセント、コネクタ、およびアンペアの製品があります。PM シリーズの電源タップはコンセントレベルで切り替えできないので、こうした電源タップを Dominion KX II に接続しないでください。
Dominion KX II ユニットには何台の PDU を接続できますか。	1 台の Dominion KX II に最大 8 台の PDU を接続できます。
PDU をどのように Dominion KX II に接続すればよいですか。	電源タップを Dominion KX II に接続するには、D2CIM-PWR を使用します。D2CIM-PWR は別途購入する必要があります。PDU には付属していません。
Dominion KX II では、複数の電源を持つサーバはサポートされていますか?	はい。Dominion KX II では、複数の電源タップに接続された複数の電源でサーバをサポートするよう簡単に設定できます。ターゲット サーバごとに 4 つの電源を接続できます。
Dominion KX II には PDU の統計情報と測定値が表示されますか。	はい。PDU レベルの電源統計情報 (例: 電力、電流、電圧) が PDU から取得され、ユーザに対して表示されます。
リモート電源管理では、接続されているサーバを特別に設定する必要がありますか。	一部のサーバでは、電源をいったん切断して再投入したときにサーバが自動再起動しないように、BIOS が設定されています。このようなサーバを使用する場合、そのサーバのドキュメントを読み、この設定を変更してください。
サーバの電源を入れ直すとどうなりますか。	これは、サーバの AC 電源コードをいったん抜いて再度差し込むのと同じことです。
PDU に接続されている他の装置 (サーバ以外) の電源をオン/オフできますか。	はい。Dominion KX II のブラウザ ベース画面を使用して、コンセント単位で、PDU に接続されているその他の装置の電源をオン/オフできます。

ローカル ポートの統合およびカスケード接続

質問	回答

質問	回答
複数の Dominion KX II を 1 つのソリューションとして統合するには、物理的にどのように接続すればよいですか。	複数台の KX II を互いに物理接続してローカル アクセスを統合するには、KX II のカスケード接続機能を利用して、複数台のカスケード接続 KX II のローカル ポートをベース KX II に接続します。これにより、データ センタ内の 1 か所から統合ポート リストを使用して、KX II に接続されているサーバにアクセスできます。 カスケード接続 KX II をベース KX II に接続するには、D2CIM-DVUSB CIM を使用する必要があります。KX2-832 および KX2-864 の場合は、Cat 5/6 ケーブルを使用して拡張ローカル ポートをベース KX II に接続できます（CIM は不要）。 統合ポート リストを使用したアクセスは、データ センタ内だけでなくリモート PC からでも可能です。階層型ポート リストまたは検索機能（およびワイルドカード）を使用することにより、カスケード接続 KX II に接続されているすべてのサーバにアクセスできます。 カスケード接続レベルは 2 段階までサポートされています。また、カスケード接続構成内の最大 1,024 個のデバイスにアクセスできます。リモート電源制御もサポートされています。 将来のリリースでは、カスケード接続構成内で仮想メディア、スマート カード、およびブレード サーバへのアクセスがサポートされる予定です。もちろん、これらの機能は標準リモート接続においても利用できます。 利便性を考慮して、IP ネットワーク上で統合ポート リストを使用してリモート IP サーバにアクセスできるようになっています。ただし、CommandCenter から、またはサーバが接続されている KX II からカスケード接続サーバにリモート アクセスする方法の方が、パフォーマンスが高くなるので推奨されます。

質問	回答
Dominion KX II どうしを物理接続する必要がありますか。	複数の Dominion KX II ユニットを物理的に相互接続する必要はありません。その代わりに、各 Dominion KX II ユニットをネットワークに接続します。Raritan の CommandCenter Secure Gateway (CC-SG) 管理アプライアンスを使用して展開すると、1 つのソリューションとして自動的に一体となって機能します。 CC-SG は、リモート アクセスおよびリモート管理用の単一のアクセス ポイントとして機能します。 たとえば、設定作業の集中管理、ファームウェア更新作業の集中管理、認証データベースの一元化などが可能になるので便利です。 リモート アクセスを集中化する目的で CC-SG を使用しているお客様は、KX II のカスケード接続機能を利用することにより、複数台の KX II のローカル ポートを統合し、データ センタ内の 1 か所のコンソールから最大 1,024 台のサーバにローカル アクセスすることができます。
CC-SG は必要ですか。	集中管理システムを使用せずに Dominion KX II をスタンドアロンで使用したいお客様は、従来どおり、複数台の KX II を IP ネットワーク上で相互運用して規模を拡張することになります。Dominion KX II の Web ベース画面および Multi-Platform Client (MPC) から複数台の KX II にアクセスできます。

質問	回答
既存のアナログ KVM スイッチを Dominion KX II に接続できますか？	はい。アナログ KVM スイッチは、Dominion KX II のサーバ ポートのいずれかに接続できます。PS/2 または USB コンピュータ インタフェース モジュール (CIM) を使用して、既存のアナログ KVM スイッチのユーザ ポートにつなぐだけです。 ローカル ポートでホットキーベースの切り替えをサポートしているアナログ KVM スイッチを Dominion KX II にカスケード接続すると、統合ポート リストを介してリモートおよびデータ センタを切り替えることができます。 アナログ KVM スイッチの仕様はそれぞれ異なっているため、Raritan では、サードパーティ製の特定のアナログ KVM スイッチについての相互運用性は保証していません。詳細については、Raritan のテクニカル サポート部門にお問い合わせください。

コンピュータ インタフェース モジュール (CIM)

質問	回答
CIM でサポートされているビデオのタイプはどれですか。	弊社の CIM は、従来からアナログ VGA ビデオをサポートしています。3 つの新しい CIM では、DVI、HDMI、DisplayPort などのデジタル ビデオ形式をサポートしています。この新しい CIM には、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、および D2CIM-DVUSB DP があります。

質問	回答
Raritan のアナログ マトリックス KVM スイッチである Paragon のコンピュータ インタフェース モジュール (CIM) を Dominion KX II と共に使用できますか。	はい。特定の Paragon コンピュータ インタフェース モジュール (CIM) は、Dominion KX II と連動する可能性があります (認定済みの CIM の最新リストについては、Raritan の Web サイトで Dominion KX II リリース ノートを確認してください)。 ただし、Paragon CIM は Dominion KX II CIM より高額のため (最大 304 m (1,000 フィート) のビデオ送信向けの技術が組み込みまれているため)、通常は Dominion KX II 用に Paragon CIM を購入することをお勧めします。また、Paragon CIM を Dominion KX II に接続すると、ビデオ送信距離は Dominion KX II CIM と同じく最大で 46 m (150 フィート) となります。Paragon に接続した場合の 304 m (1,000 フィート) ではありません。
Dominion KX II コンピュータ インタフェース モジュール (CIM) を Raritan のアナログ マトリックス KVM スイッチである Paragon で使用できますか。	使用できません。Dominion KX II コンピュータ インタフェース モジュール (CIM) のビデオ送信距離は 15 m ～ 46 m (50 ～ 150 フィート) であるため、ビデオ送信距離が 300 m (1,000 フィート) の CIM が必要な Paragon では動作しません。Raritan のお客様には業界最高水準のビデオ品質を提供するというのが Raritan の一貫した方針です。そのため、Dominion シリーズの CIM は Paragon では使用できません。
Dominion KX II において Paragon Dual CIM はサポートされていますか。	はい。Dominion KX II で Paragon II Dual CIM (P2CIM-APS2DUAL および P2CIM-AUSBDUAL) がサポートされるようになりました。これらの CIM を使用すれば、データ センタ内のサーバを 2 台の異なる Dominion KX II に接続できます。 一方の KX II が使用不能になった場合でも、もう一方の KX II からサーバにアクセスできます。つまり、冗長構成になり、リモート KVM アクセスを二重化できます。 なお、これらは Paragon CIM なので、KX II の拡張機能 (仮想メディア、ずれないマウスなど) はサポートされません。

セキュリティ

質問	回答
Dominion KX II は FIPS 140-2 に対応していますか。	Dominion KX II では、FIPS 140-2 実装ガイダンスに従って、Linux プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、この暗号化モジュールが使用されます。
Dominion KX II ではどのような種類の暗号化が使用されますか？	Dominion KX II の SSL 通信と自身のデータ ストリームでは、業界標準である極めて安全な 256 ビット AES、128 ビット AES、または 128 ビットの暗号化が使用されます。事実、暗号化によって完全に保護されていないリモート クライアントと Dominion KX II の間ではデータは転送されません。
Dominion KX II では、米国政府の NIST および FIPS 規格で推奨される AES 暗号化がサポートされていますか。	はい。Dominion KX II では、セキュリティを高めるために Advanced Encryption Standard (AES) が使用されます。256 ビットおよび 128 ビットの AES を利用できます。 AES は米国政府の承認した暗号アルゴリズムです。NIST (米国の国立標準技術研究所) の FIPS 規格 197 で推奨されています。
Dominion KX II では、ビデオデータの暗号化を行いますか？それとも、キーボードデータとマウス データだけが暗号化されますか。	キーボードとマウスのデータのみを暗号化する競合他社のソリューションとは異なり、Dominion KX II ではセキュリティに関して妥協していません。Dominion KX II では、キーボード、マウス、ビデオ、および仮想メディアのデータの暗号化を行います。

質問	回答
Dominion KX II と、Active Directory、RADIUS、LDAP などの外部認証サーバは、どのように統合して機能しますか。	Dominion KX II には、非常に簡単な設定で、すべての認証要求を LDAP、Active Directory、RADIUS などの外部サーバに転送するよう指定できます。Dominion KX II は、認証されたユーザーごとに認証サーバからユーザーが属するユーザー グループを受け取ります。次に Dominion KX II は、ユーザーが属するユーザー グループに基づいてそのユーザーのアクセス許可を決定します。
ユーザ名とパスワードはどのように保存されますか。	Dominion KX II の内部認証機能が使用される場合、ユーザ名やパスワードなどの機密情報はすべて暗号化形式で保存されます。実際に、Raritan のテクニカル サポートやプロダクト エンジニアリング部門を含め、誰もこれらのユーザ名やパスワードを読み出せません。
Dominion KX II では強力なパスワードがサポートされていますか。	はい。Dominion KX II には管理者が設定できる強力なパスワード チェック機能があります。この機能によって、ユーザーの作成したパスワードが企業または政府の標準を満たし、悪意のあるハッキング行為によって暴かれないようにします。
自社固有のデジタル証明書を Dominion KX II にアップロードできますか。	はい。お客様は、自己署名されたデジタル証明書または認証局発行のデジタル証明書を Dominion KX II にアップロードできます。これにより、認証機能を強化し、通信のセキュリティを高めることができます。
Does the KX II ではセキュリティ バナーをカスタマイズできますか。	はい。政府機関や軍のようなセキュリティを重視するお客様では、ユーザがログインする前にセキュリティ メッセージを表示する必要があります。KX II では、カスタマイズ可能なバナー メッセージを表示できます。また、このメッセージへの同意を義務付けることもできます。
当社のセキュリティ ポリシーでは、標準の TCP ポート番号の使用を許可していません。TCP ポート番号を変更できますか。	はい。セキュリティを強化するために標準の TCP/IP ポート番号を使用したくないお客様の場合、Dominion KX II では管理者が代替ポート番号を設定できるようになっています。

スマート カード認証と CAC 認証

質問	回答
Dominion KX II では、スマート カード認証と CAC 認証はサポートされていますか。	はい。リリース 2.1.10 以降では、ターゲット サーバへのスマート カード認証と DoD Common Access Card (CAC) 認証がサポートされています。
CAC とは何ですか。	Homeland Security Presidential Directive 12 (HSPD-12) によって義務付けられている CAC は、米国政府が作成し、米軍および政府職員が使用するスマート カードの一種です。CAC カードは、多彩な技術に基づく多目的カードであり、識別カードを 1 つにまとめることを目標にしています。詳細については、FIPS 201 規格を参照してください。
スマート カードと CAC がサポートされている KX II のモデルはどれですか。	すべての Dominion KX II モデルでサポートされています。Dominion KSX II および KX II-101 では、現在スマート カードと CAC はサポートされていません。
大企業や中小企業でもスマート カードは使用されていますか。	はい。なお、スマート カードを最も積極的に導入しているのは米国連邦政府です。
スマート カードと CAC がサポートされている CIM はどれですか。	D2CIM-DVUSB、D2CIM-DVUSB DVI、D2CIM-DVUSB HDMI、D2CIM-DVUSB DP の各 CIM が必要です。
サポートされているスマート カード リーダーはどれですか。	必要なリーダー標準は、USB CCID と PC/SC です。認定済みのリーダーの一覧および詳細については、ユーザ マニュアルを参照してください。
スマート カードと CAC の認証は、ローカル ポートおよび CommandCenter で利用できますか。	はい。スマート カードと CAC の認証は、ローカル ポートおよび CommandCenter で機能します。ローカル ポートを使用する場合は、互換性のあるスマート カード リーダーを Dominion KX II の USB ポートに接続します。

質問	回答
Paragon のスマート カードに対応した UST および CIM は使用されていますか。	いいえ。P2-EUST/C および P2CIM-AUSB-C は、Dominion KX II ソリューションに含まれていません。
KX II のスマート カードのサポートに関する詳細情報はどこで入手できますか。	詳細については、リリース ノートおよび『Dominion KX II ユーザ ガイド』を参照してください。

管理機能

質問	回答
Dominion KX II は Web ブラウザを介してリモートで管理および設定できますか?	はい。Dominion KX II は、Web ブラウザを介して完全にリモートで設定できます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。Dominion KX II の IP アドレスの初期設定のほか、ソリューションの関連事項をすべてネットワーク上で設定できます(実際に、Ethernet クロス ケーブルと Dominion KX II のデフォルト IP アドレスを使用すると、Web ブラウザを介して初期設定も変更できます)。
Dominion KX II の設定のバックアップや復元は可能ですか。	はい。非常事態が発生した際に復旧を行うため、Dominion KX II のデバイス設定とユーザー設定は完全にバックアップされます。 Dominion KX II のバックアップ機能と復元機能は、ネットワークや Web ブラウザを介してリモートで使用できます。
Dominion KX II では、どのような監視機能またはログ機能が提供されますか?	ユーザーのアカウンタビリティをサポートするため、Dominion KX II では主要なユーザー イベントを日付やタイム スタンプと共に記録します。記録されるイベントの例としては、ユーザー ログイン、ユーザー ログアウト、特定のサーバへのユーザー アクセス、ログインの失敗、設定の変更など。

質問	回答
Dominion KX II と syslog は一元化できますか。	はい。Dominion KX II の独自の内部ログ機能に加え、Dominion KX II ではログ記録されたすべてのイベントを集中 syslog サーバに送信できます。
Dominion KX II と SNMP は一元化できますか?	はい。Dominion KX II の独自の内部ログ機能に加え、Dominion KX II では SNMP トラップを SNMP 管理システムに送信できます。SNMP v2 および v3 がサポートされています。
管理者はユーザをログオフすることができますか。	はい。管理者は、どのユーザがどのポートにログインしているかを調べ、必要に応じて特定のポートから、またはデバイスからユーザをログオフすることができます。
Dominion KX II の内部クロックは時刻サーバと同期できますか?	はい。Dominion KX II では、企業の時刻サーバとパブリック時刻サーバのいずれかに同期するための業界標準の NTP プロトコルがサポートされています (企業ファイアウォール経由のアウトバウンド NTP リクエストが許可されている場合)。

ドキュメントおよびサポート

質問	回答
Dominion KX II のドキュメントはどこにありますか。	ドキュメントは、raritan.com の KX II ファームウェアおよびマニュアルに関するページ (http://www.raritan.com/support/dominion-kx-ii) から入手できます。ドキュメントは、ファームウェア リリース別に一覧表示されています。
どのようなドキュメントを入手できますか。	クイック セットアップ ガイド、ユーザ ガイド、KVM and Serial Client のガイドのほかに、リリース ノートやその他の情報を入手できます。

質問	回答
オンライン ヘルプは利用できますか。	はい。オンライン ヘルプは、ドキュメントと共に raritan.com にあり、KX II ユーザインタフェースから利用できます。
特定のサーバにどのような CIM を使用する必要がありますか。	KX II ドキュメントとして用意されている CIM ガイドを調べてください。DVI、HDMI、DisplayPort の各ビデオ規格は、新しいデジタル ビデオ CIM (リリース 2.5 以降で使用可能) でサポートされています。
KX II のハードウェア保証期間はどのくらいですか。	Dominion KX II の保証期間は標準で 2 年ですが、保証期間を 5 年に延長することもできます。

その他

質問	回答
Dominion KX II のデフォルト IP アドレスは？	192.168.0.192
Dominion KX II のデフォルトユーザー名とパスワードは？	Dominion KX II のデフォルトのユーザ名とパスワードは「admin/raritan」です (すべて小文字)。ただし、最高レベルのセキュリティを確保するため、Dominion KX II ではユニットが最初に起動した際に、管理者が Dominion KX II のデフォルト管理者ユーザ名とパスワードを変更するよう要求されます。
Dominion KX II の管理者パスワードを変更したところ、新しいパスワードを忘れてしまいました。パスワードを取得してもらえますか？	Dominion KX II では、ハードウェア リセット ボタンを使用してデバイスを工場出荷時の設定に戻すことができます。このとき、デバイスの管理者パスワードもデフォルトのパスワードにリセットされます。

質問	回答
Dominion KX I から Dominion KX II にはどのような方法で移行すればよいですか?	一般に、KX I のお客様には既存のスイッチを長期間お使いいただけます。データ センタを拡張する場合、お客様は新しい KX II モデルを購入して使用することが考えられます。Raritan の集中管理アプライアンスである CommandCenter Secure Gateway (CC-SG) および Multiplatform Client (MPC) は、KX I スイッチおよび KX II スイッチをシームレスにサポートします。
現在使用している KX I CIM は、Dominion KX II スイッチでも動作しますか。	はい。既存の KX I CIM は、Dominion KX II スイッチでも動作します。また、KX II で動作する Paragon CIM をお選びください。これにより、KVM over IP への切り替えを検討している Paragon I のお客様は、KX II に簡単に移行できます。ただし、仮想メディアとずれないマウス機能をサポートする D2CIM-VUSB CIM および D2CIM-DVUSB CIM を検討することをお勧めします。さらに、DVI、HDMI、および DisplayPort をサポートするデジタル ビデオ CIM も利用できます。

索引

[

[Audit Log] (監査ログ) - 283, 331, 337
[Authentication Settings] (認証設定) - 159
[Auto-sense Video Settings] (ビデオ設定の自動感知) - 84
[Connection Properties] (接続プロパティ) - 74
[Device Information] (デバイス情報) - 284
[Device Services] (デバイス サービス) - 179, 222, 227
[Encryption & Share] (暗号化および共有) - 104, 269, 274, 337
[Event Management - Destinations] (イベント管理 - 送信先) の設定 - 191, 194, 197, 203
[Event Management - Settings] (イベント管理 - 設定) の設定 - 194, 203
[Full Screen Mode] (全画面モード) - 100
[Keyboard Macros] (キーボード マクロ) - 77
[Network Interface (ネットワーク インタフェース)] ページ - 298
[Network Statistics] (ネットワーク統計) ページ - 299
[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ) - 49, 53, 217, 317, 381
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ) - 317
[Port Action] (ポート アクション) メニュー - 54, 57
[Ports] (ポート) ページに表示されるデュアル ポート ビデオ グループ - 381
[Power Supply Setup] (電源設定) - 32, 41, 205
[Scaling] (拡大、縮小) - 99
[Screenshot from Target] (ターゲットからのスクリーンショット) を使用する - 88
[Set Scan] (スキャン設定) タブ - 55
[Trace Route to Host (ホストへのルートの追跡)] ページ - 301
[Upgrading Firmware] (ファームウェアのアップグレード) - 290
[USB Profile Management] (USB プロファイルの管理) - 288, 289
[User Management] (ユーザ管理) - 42, 145, 315
[View by Group] (グループ別表示) タブ - 55
[View by Search] (検索して表示) タブ - 55
[View Status Bar] (ステータス バーの表示) - 99
[View Toolbar] (ツール バーの表示) - 98
[お気に入りの管理] ページ - 63
[お気に入りリスト] ページ - 64, 65
[ホストに ping する] ページ - 301
[ユーザ ブロック] - 263, 267
[ログイン制限] - 263, 264
[強力なパスワード] - 172, 263, 266
[全般] - 94

A

A. AC 電源: - 32
Active KVM Client について - 68
AKC ダウンロード サーバ証明書の検証の有効化 - 188
AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ - 69
Apple Macintosh の設定 - 31

B

B. モデム ポート (オプション) - 33

C

C. ネットワーク ポート - 33
CC-SG - 413
CC-SG ユーザへの注意事項 - 42
CC-SG 管理の終了 - 295
CD-ROM/DVD-ROM/ISO イメージのマウント - 129, 132
CIM - 411
CIM アップグレード - 136, 243, 290
CIM キーボード/マウス オプションの設定 - 83
CIM の互換性 - 136
CIM ポートの設定 - 211, 350
CLI コマンド - 305, 310
CLI の画面操作 - 307
CLI プロンプト - 310

CLI を使用した初期設定 - 309
CLI を使用しての KX II へのアクセス - 306
CLI 構文
ヒントとショートカット キー - 308
Ctrl+Alt+Del マクロ - 83

D

D. ローカル アクセス ポート (ローカル ビデオ ディスプレイ、キーボード、およびマウス) - 34
D2CIM-VUSB を使用して Windows 2000 サーバ上の仮想メディアにアクセスする - 411
DCIM-VUSB で Mac OS-X USB プロファイルを使用する場合のマウス モード - 144, 243
Dell ブレード シャーシの設定 - 221
Dell 筐体を接続する場合のケーブル長と画面解像度 - 219, 221, 226, 359

E

E. ターゲット サーバ ポート - 35
Ethernet と IP ネットワーキング - 429

F

FAQ - 414
Fedora - 401
Fedora Core のフォーカスに関する問題を解決する - 401
Fedora サーバへの VKC および MPC のスマート カード接続 - 402
Fedora 使用時の Firefox のフリーズに関する問題の解決 - 402
FIPS 140-2 サポートの要件 - 274
FIPS 140-2 の有効化 - 271, 273

H

HP および Cisco USC のブレード シャーシ設定 (ポート グループ管理) - 233, 235, 258, 259
HTTP ポートおよび HTTPS ポートの設定 - 180, 365

I

IBM AIX 5.3 の設定 - 30
IBM ブレード シャーシの設定 - 226
interface コマンド - 312
IP アクセス制御を設定する - 275
IP アドレスの割り当て - 36
ipv6 コマンド - 313
IPv6 ネットワーキング - 432
IPv6 のサポートに関する注意事項 - 395

J

Java Runtime Environment (JRE) - 393

K

KVM スイッチを設定する - 182, 209
KVM ポート用のプロファイルの選択 - 144
KX II ― KX II 構成に関するガイドライン - 352
KX II ― Paragon II 構成に関するガイドライン - 353
KX II SNMP トラップのリスト - 191, 195, 198
KX II インタフェース - 46, 49
KX II からのユーザのログオフ (強制ログオフ) - 155, 156, 157
KX II コンソール サーバ設定用コマンドを使用する - 311
KX II コンソールでの案内 - 52
KX II サブネット上のデバイスの検出 - 65
KX II デバイスの写真 - 7
KX II の MIB の表示 - 189, 195, 201
KX II のクライアント アプリケーション - 5
KX II のローカル ポートの設定 - 34, 246, 251, 330
KX II の概要 - 2
KX II の再起動 - 293
KX II の統合向けにサポートされている距離 - 355
KX II の物理的仕様 - 8, 339
KX II への Paragon II の接続 - 383
KX II への SSH 接続 - 306
KX II ヘルプ - 4
KX II ユーザ リストの表示 - 155
KX II リモート コンソール インタフェース - 47
KX II リモート コンソールの起動 - 47
KX II ローカル コンソール - 314

KX II ローカル コンソール インタフェース KX II デバイス - 47, 315
KX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ - 331
KX II ローカル コンソールのローカル ポートの設定 - 324, 327
KX II ローカル コンソールの画面に切り替える - 326
KX II を使用した Paragon II へのアクセス - 382
KX II 診断 - 303
KX2 8xx デバイスでのスマート カード アクセス - 322
KX2 8xx 拡張ローカル ポートの推奨最大距離 - 362
KX2-808、KX2-832、および KX2-864 の標準ローカル ポートと拡張ローカル ポートの設定 - 246, 251

L

LAN インタフェース設定 - 39, 173, 177, 178
LDAP スキーマを更新する - 164, 385
LDAP/LDAPS から返す場合 - 385
LDAP/LDAPS リモート認証の実装 - 160, 165
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合 - 411
Linux の設定の永続化 - 26
Linux 環境での音声 - 404
Linux 環境での仮想メディア - 125
Linux 設定 (Red Hat 4、Red Hat 5、および Fedora 14) - 23
Linux 設定 (標準マウス モードの場合) - 25

M

Mac Lion クライアントでの MPC の起動 - 397
Mac Mini BIOS のキー入力コマンド - 396
Mac および Linux でマップしてロックしたドライブ - 411
Mac に関する注意事項 - 396
Mac 環境での音声 - 405
Mac 環境での仮想メディア - 127
Macintosh キーボード - 401
Microsoft Active Directory から返す場合 - 386
Microsoft Active Directory についての注意事項 - 42
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 - 66
Multi-Platform Client (MPC) - 113

N

name コマンド - 313

P

PC 共有モードが有効になっている場合の音声接続に関する推奨事項 - 360
Prerequisites for Using AKC - 68, 70

R

RADIUS リモート認証の実装 - 165
RADIUS 通信交換仕様 - 169
RADIUS 認証用の Cisco ACS 5.x - 168

S

SNMP エージェントの設定 - 189, 195
SNMP トラップの設定 - 191, 194, 195
SSH を有効にする - 179
SSL 証明書 - 278
Sun Solaris の設定 - 27
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ - 325
SUSE Linux 10.1 の設定 - 26
SUSE と VESA のビデオ モード - 403
syslog 設定 - 202

U

UNIX の設定の永続化 - 31
UNIX/Linux ワークステーションから SSH で接続する - 307
URL を経由したダイレクト ポート アクセスの有効化 - 186, 381
USB プロファイル - 135, 243
USB プロファイルの設定 ([Port] (ポート) ページ) - 144, 229, 243
USB プロファイルの選択に関するヘルプ - 406
USB ポートとプロファイル - 405

V

Virtual KVM Client (VKC) および Active KVM Client (AKC) - 48, 68

VKC および AKC でのスキャンの設定 - 59, 61, 98, 320
VKC のバージョンが CC-SG プロキシ モードで認識されない - 413
VM-CIM および DL360 の USB ポート - 405

W

Web ブラウザ インタフェースの追加に関するヒント - 221, 224, 226, 229, 231, 396
Web ブラウザからの MPC の起動 - 113
Windows 2000 での複合 USB デバイスの動作 - 412
Windows 2000 の設定 - 22
Windows 7 および Windows Vista の設定 - 20
Windows PC から SSH で接続する - 306
Windows XP 環境での仮想メディア - 124
Windows XP、Windows 2003、および Windows 2008 の設定 - 19
Windows 環境での VKC および AKC を介した仮想メディア - 409
Windows 環境での音声 - 405

あ

アクティブ システム パーティション - 410
アップグレード履歴 - 293
アメリカ英語以外のキーボード - 398
イベント管理 - 194
インストール - 438
インストールと設定 - 14
インタフェースおよび画面操作 - 49
インテリジェント マウス モード - 18, 92
インテリジェント電源タップ (PDU) の管理 - 444
お気に入りの管理 - 51, 62
お気に入りの追加、削除、および編集 - 65

か

カスケード接続
ターゲット タイプ、サポート対象 CIM、およびカスケード接続構成 - 181, 183
カスケード接続ターゲットでサポートされていない機能および限定的にサポートされている機能 - 184
カスケード接続デバイス - [Port Access] (ポート アクセス) ページ - 56
カスケード接続を設定および有効化する - 9, 56, 149, 150, 151, 154, 181, 247
カスケード接続を有効にする - 182
カスケード接続構成における接続例 - 184
キーボード - 398
キーボード マクロのインポート/エクスポート - 77
キーボード マクロの作成 - 80
キーボード マクロの実行 - 82
キーボード マクロの変更および削除 - 82
キーボード レイアウト コードの変更 (Sun ターゲット) - 44
キーボードのオプション - 77
キーボードの制限 - 96
キーボード言語の設定 (Fedora クライアント) - 399
キャプチャ/再生バッファ サイズの調整 (音声設定) - 101, 102, 104, 107
クライアント起動設定 - 97
グループベースの IP ACL (アクセス制御リスト) - 147, 152, 154, 275
コマンド ライン インタフェース (CLI) - 305
コマンドのオート コンプリート - 307
コンセントとターゲット サーバとの関連付け - 215
コンセントの電源オン/オフの切り替えまたは電源再投入を行う - 116
コンピュータ インタフェース モジュール (CIM) - 449
ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する - 270, 273

さ

サーバ - 434
サポートされている Paragon CIMS および設定 - 272, 350, 383
サポートされているオペレーティング システム (クライアント) - 13, 342
サポートされているコンピュータ インタフェース モジュール (CIM) の仕様 - 8, 35, 136, 345, 349, 378

サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー - 108, 111, 321, 355
サポートされているターゲット サーバとビデオ - 35, 345
サポートされているブラウザ - 345
サポートされているブレード シャーシ モデル - 219, 221, 226, 235
サポートされているプロトコル - 42
サポートされているマウス モード - 101, 377
サポートされているリモート接続 - 363
サポートされている音声/仮想メディアおよびスマート カード接続の数 - 361
サポートされている音声デバイス形式 - 101, 359
サポートされている画面解像度 - 26, 31, 343, 345, 373, 403
サポートされている画面解像度が表示されない - 403
シングル マウス モード - 93
Firefox を使用して CC-SG の管理下にあるターゲットに VKC を介してアクセスする場合 - 413
スキーマ キャッシュを更新する - 389
スキーマへの書き込み操作を許可するようにレジストリを設定する - 386
スキャン オプションの使用 - 61, 320
スクリプトのインポートとエクスポート - 253, 256, 334
スクリプトの接続と切断 - 252, 333
スクリプトの追加 - 253, 334
スクリプトの適用および削除 - 252, 256, 333
スクリプトの変更 - 256, 337
ステップ 2
ネットワーク ファイアウォールの設定 - 14, 31
すべての CLI レベルで使用できるコマンド - 308
スマート カード - 108
スマート カード リーダー - 355
スマート カード リーダー使用時の USB プロファイルの変更 - 408
スマート カードの最小システム要件 - 321, 357
スマート カード認証と CAC 認証 - 453
ずれないマウス モード - 93
セキュリティ - 451
セキュリティ バナー - 281
セキュリティと認証 - 315
セキュリティの設定 - 157, 263
セキュリティ上の問題 - 263, 311
その他 - 457
ソフトウェア - 10

た

ターゲット サーバにアクセスする - 318
ターゲット サーバの使用 - 5, 46, 218
ターゲット サーバの切り替え - 43
ターゲット サーバの切断 - 44
ターゲット サーバの命名 - 40
ターゲット サーバの要件 - 357
ターゲット サーバへのアクセス - 43
ダイレクト ポート アクセスおよびデュアル ポート ビデオ グループ - 381
ツール オプション - 94, 100
ツール バーのボタンおよびステータス バーのアイコン - 70
デジタル CIM ターゲット サーバのタイミングおよび画面解像度 - 35, 349, 378
デジタル音声 - 101
デジタル音声デバイスの接続および切断 - 101, 102, 104, 105
デスクトップの背景 - 18
デバイスのポート間の移動 - 413
デバイス管理 - 45, 55, 173
デフォルト パスワードの変更 - 36
デフォルトの GUI 言語設定の変更 - 262
デフォルトのログイン情報 - 14, 17
デュアル スタック ログインのパフォーマンスに関する問題 - 396
デュアル ビデオ サポートに必要な CIM - 101, 378
デュアル ビデオ ポート グループ - 260, 370
デュアル ビデオ ポート グループ - [Port Access] (ポート アクセス) ページ - 57
デュアル ビデオ ポート グループの作成 - 186, 258, 260, 370, 375, 381
デュアル ビデオ ポート グループを使用する際の Raritan クライアントの画面操作 - 380
デュアル ポート ビデオ グループの使いやすさに関する注意事項 - 379

デュアル ポート ビデオ グループ設定の例 - 371
デュアル ポート ビデオに関する推奨事項 - 101, 377
ドキュメントおよびサポート - 456
ドライブ パーティション - 410

な

ネットワーク パラメータの設定 - 309
ネットワークを設定する - 312
ネットワーク基本設定 - 173, 174
ネットワーク設定 - 32, 36, 39, 173, 174, 177, 365
ネットワーク速度の設定 - 178, 367

は

ハードウェア - 9
はじめに - 1
パスワードの変更 - 172
バックアップと復元 - 233, 259, 286
パッケージの内容 - 13
パラメータ値を設定する - 309
ビデオ モードと解像度 - 403
ビデオのプロパティ - 83
ビデオ設定を調整する - 84
ファイル追加後に仮想メディアが最新の情報に更新されない - 410
フランス語キーボード - 398
ブレード サーバ - 435
ブレード シャーシ - [Port Access] (ポート アクセス) ページ - 56
ブレード シャーシでサポートされている CIM - 219, 221, 226, 236
ブレード シャーシのサンプル URL フォーマット - 223, 228, 230, 242
ブレード シャーシの設定 - 217
ブレード シャーシの必須および推奨設定 - 219, 221, 226, 239
プロキシ モードと MPC - 413
プロファイル名の競合を処理する - 289
ヘルプでの最新情報 - 5
ヘルプのオプション - 112
ポート グループの作成 - 258, 259
ポート グループ管理 - 258
ポートからのユーザの切断 - 155, 156, 157
ポートのスキャン - 49, 55, 59, 98, 247, 381
ポートのスキャン - ローカル コンソール - 60, 318
ポートの設定 - 206
ポート権限の設定 - 147, 150, 154
ポート別のユーザの表示 - 155, 156
ホット キーと接続キー - 324

ま

マウス オプション - 89
マウス ポインタの同期 - 90
マウス ポインタの同期 (Fedora) - 402
マウスの設定 - 18, 374, 375
モデムを設定する - 33, 191

や

ユーザ - 154
ユーザ グループ - 145
ユーザ グループ リスト - 146
ユーザ グループおよびユーザを作成する - 42
ユーザ グループ情報を Active Directory サーバから返す - 164
ユーザ グループ情報を RADIUS 経由で返す - 169
ユーザ グループ情報を返す - 385
ユーザ メンバの rciusergroup 属性を編集する - 390
ユーザが同時接続可能 - 314
ユーザとグループの関係 - 146
ユーザ認証プロセス - 171
ユニバーサル仮想メディア - 420

ら

ラック PDU (電源タップ) ターゲットの設定 - 212
ラック PDU (電源タップ) のコンセントの制御 - 115
ラック PDU の接続 - 212
ラック PDU の名前の指定 (電源タップの [Port] (ポート) ページ) - 213
ラック マウント - 14
リセット ボタンを使用して KX II をリセットする - 271, 337
リモート アクセス - 417

リモート クライアントの要件 - 358
リモートからのターゲット サーバのアクセスと制御 - 43
リモート認証 - 42, 249, 329
ローカル コンソールからの KX II ローカル ポートの設定 - 326, 330
ローカル コンソールの USB プロファイル オプション - 323
ローカル コンソールのスマート カード アクセス - 110, 321
ローカル サブネット上のデバイスの検出 - 64
ローカル ドライブのマウント - 131
ローカル ポート - 441
ローカル ポートの管理 - 326
ローカル ポートの統合およびカスケード接続 - 446
ローカル ポートの要件 - 357
ログアウト - 66
ログイン - 306, 307

漢字

一般的な FAQ - 415
音声 - 101, 359, 404
音声の再生とキャプチャに関する推奨事項と要件 - 104, 105, 360
音声の再生とキャプチャに関する問題 - 404
音声レベル - 360
音声設定の保存 - 101, 102, 105
仮想メディア - 6, 119, 409
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) - 128, 129
仮想メディアの Linux ドライブが 2 回リストされる - 410
仮想メディアの使用 - 128
仮想メディアの切断 - 128, 134
仮想メディアへの接続 - 131
仮想メディアを使用するための条件 - 123, 128
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間 - 411
画面を更新する - 83
概要 - 14, 115, 120, 135, 305, 314, 370, 382, 393
各言語に対してサポートされているキーボード - 363
拡張ローカル ポート (Dominion KX2-832 および KX2-864 モデルのみ) - 443
拡張ローカル ポートでサポートされているデバイス - 362
監査ログおよび Syslog でキャプチャされるイベント - 283, 367
管理機能 - 455
関連文書 - 5
既存のユーザ グループの変更 - 153, 158
許可の設定 - 147, 149, 153
検出ポートを入力する - 180
権限およびデュアル ビデオ ポート グループ アクセス - 261, 380
個別グループの許可の設定 - 151, 158
後向きの取り付け - 16
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー - 411
左パネル - 50, 196
最大垂直走査周波数の変更 - 89
仕様 - 33, 251, 339
使用される TCP ポートおよび UDP ポート - 364
使用できる USB プロファイル - 136, 407
手順 1
KVM ターゲット サーバの設定 - 14, 18
ターゲット サーバの画面の設定 - 373
手順 2
KX II へのターゲット サーバの接続 - 373
手順 3
マウス モードおよびポートの設定 - 375
装置の接続 - 14, 32, 40, 208, 219, 221, 226
手順 4
KX II の設定 - 14, 36
デュアル ビデオ ポート グループの作成 - 373, 375
手順 5
KX II リモート コンソールの起動 - 14, 43
デュアル ビデオ ポート グループを開く - 376
手順 6
キーボード言語の設定 (オプション) - 14, 44
手順 7

カスケード接続の設定 (オプション) - 14, 45
色の調整 - 84
新しい属性を作成する - 387
新規ユーザ グループの追加 - 147, 157
新規ユーザの追加 - 157, 158
診断 - 297
製品の特長 - 9
接続キーの例 - 249, 324, 328
接続情報 - 76
前向きの取り付け - 15
属性をクラスに追加する - 388
帯域幅と KVM-over-IP のパフォーマンス - 424
帯域幅要件 - 360
単一のリモート クライアントから複数のターゲットへの接続 - 101, 102, 105
電源の自動検出の指定 - 41
読み取り/書き込み可能に設定できない状況 - 127, 132
日付/時刻の設定 - 193, 278
日付/時刻の設定 (オプション) - 39
入門 - 18, 309, 374
認定モデム - 193, 362
汎用ブレード シャーシの設定 - 219
標準ターゲット サーバの設定 - 208, 375
標準マウス モード - 91
表示オプション - 98
複数のリモート クライアントから単一のターゲット サーバへの接続 - 101, 102, 104, 105
保守 - 283
有効な解像度 - 316
用語 - 11, 18
留意事項 - 101, 363, 393

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 : +44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : rg-support@raritan.com

メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール : support.apac@raritan.com