



Dominion KX II-101-V2

ユーザ ガイド
リリース 3.3.0

Copyright © 2011 Raritan, Inc.
KX2101V2-v3.3.0-A-E
2011 年 4 月
255-62-3059-00

このドキュメントには著作権によって保護されている所有者情報が含まれています。無断で転載することは、禁じられており、このドキュメントのどの部分も Raritan, Inc. (Raritan 社) 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はできません。

© Copyright 2011 Raritan, Inc.、CommandCenter®、Dominion®、Paragon®、Raritan 社のロゴは、Raritan, Inc. の商標または登録商標です。無断で転載することは、禁じられています。Java® は Sun Microsystems, Inc. の登録商標、Internet Explorer® は Microsoft Corporation の登録商標です。また、Netscape® および Netscape Navigator® は Netscape Communication Corporation の登録商標です。その他すべての商標または登録商標は、その所有会社に帰属します。

FCC 情報

この装置は FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが試験により証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設けられています。この装置は、無線周波数を生成、利用、放射する可能性があるため、指示に従った設置および使用をしないと、無線通信への干渉を招く恐れがあります。この装置を居住環境で操作すると、干渉を招く場合があります。

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。

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、通常の運用条件以外での使用による製品の故障については、Raritan 社は一切責任を負いかねます。



目次

はじめに	1
KX II-101-V2 ヘルプ	1
関連文書	1
KX II-101-V2 の概要	2
製品の写真	3
製品の特長	4
インタフェース	4
ネットワーク設定	4
システム管理機能	4
管理の特長	4
ユーザ機能	5
電源	5
ビデオ解像度	5
取り付け	5
用語	5
パッケージの内容	6
インストールと設定	7
概要	7
デフォルトのログイン情報	7
入門	8
手順 1: ターゲット サーバの設定	8
手順 2: ネットワーク ファイアウォールの設定	20
手順 3: 装置の接続	21
手順 4: KX II-101-V2 の設定	26
ターゲット サーバを操作する	34
インタフェース	34
KX II-101-V2 リモート コンソール インタフェース	34
Multi-Platform Client (MPC)	43
Virtual KVM Client (VKC)	43
概要	43
KVM ターゲット サーバへの接続	44
ツール バー	44
ターゲット サーバの電源管理	45
KVM ターゲット サーバの切断	46
[Connection Properties] (接続プロパティ)	47

接続情報	49
キーボードのオプション	50
ビデオのプロパティ	56
マウス オプション	61
VKC 仮想メディア	65
[Tools] (ツール) オプション	65
表示オプション	69
ヘルプのオプション	70

Virtual Media 71

概要	72
Prerequisites for Using Virtual Media	74
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)	75
仮想メディアの使用	76
仮想メディアへの接続	77
ローカル ドライブ	77
読み取り/書き込み可能に設定できない状況	78
CD-ROM/DVD-ROM/ISO イメージ	79
仮想メディアの切断	81

User Management 82

ユーザ グループ	82
[User Group List] (ユーザ グループ リスト)	83
ユーザとグループの関係	83
新規ユーザ グループを追加する	84
既存のユーザ グループの変更	89
ユーザ	89
[User List] (ユーザ リスト)	90
新規ユーザを追加する	90
既存のユーザ グループの変更	91
ユーザ ブロックとブロック解除	92
[Authentication Settings] (認証設定)	92
LDAP/LDAPS リモート認証を実装する	93
ユーザ グループ情報を Active Directory サーバから返す	97
RADIUS リモート認証の実装	98
ユーザ グループ情報を RADIUS 経由で返す	101
RADIUS 通信交換仕様	101
ユーザ認証プロセス	103

パスワードの変更	105
デバイス管理	106
[Network Settings] (ネットワーク設定)	106
ネットワーク基本設定	107
LAN インタフェース設定	109
[Device Services] (デバイス サービス)	109
Telnet を有効にする	110
SSH を有効にする	110
検出ポートを入力する	111
URL を介してダイレクト ポート アクセスを有効にする	111
キーボード/マウス設定	112
[Serial Port Settings] (シリアル ポート設定)	113
管理ポート	113
Raritan の電源タップ制御	113
モデム	114
日付/時刻の設定	116
イベント管理	117
Configuring Event Management - Settings	118
[Event Management - Destinations] (イベント管理 - 送信先)	119
[Port Configuration] (ポート設定)	123
KVM ターゲット サーバを管理する ([Port] (ポート) ページ)	125
Power Control	127
アナログ KVM スイッチ	132
リセット ボタンを使用して KX II-101-V2 をリセットする	134
USB 接続を管理する	135
概要	136
USB 接続設定	137
USB 接続の詳細設定	138
セキュリティ管理	140
[Security Settings] (セキュリティ設定)	140
[Login Limitations] (ログイン制限)	141
[Strong Passwords] (強力なパスワード)	142
[User Blocking] (ユーザ ブロック)	144
[Encryption & Share] (暗号化および共有)	146

[IP Access Control] (IP アクセス制御).....	149
保守	153
[Audit Log] (監査ログ).....	153
[Device Information] (デバイス情報).....	154
[Backup and Restore] (バックアップと復元).....	155
ファームウェアをアップグレードする.....	157
アップグレード履歴.....	159
[Factory Reset] (ファクトリ リセット).....	160
再起動.....	161
診断	162
[Network Interface] (ネットワーク インタフェース) ページ.....	163
[Network Statistics] (ネットワーク統計) ページ.....	163
[Ping Host] (ホストへの Ping) ページ.....	166
[Trace Route to Host] (ホストへの経路をトレースする) ページ.....	167
[Device Diagnostics] (デバイス診断).....	168
コマンド ライン インタフェース (CLI)	170
概要.....	170
CLI を使用しての KX II-101-V2 へのアクセス.....	171
KX II-101-V2 への SSH 接続.....	171
Windows PC からの SSH アクセス.....	171
UNIX/Linux ワークステーションからの SSH アクセス.....	172
ログインする.....	172
CLI の画面操作.....	172
CLI プロンプト.....	172
コマンドのオート コンプリート.....	173
CLI 構文: ヒントとショートカット キー.....	173
すべてのコマンド ライン インタフェース レベルに共通のコマンド.....	174
CLI コマンド.....	174
Diagnostics.....	175
[Configuration] (設定).....	176
Listports コマンド.....	178
Userlist コマンド.....	179

CC Unmanage	180
概要.....	180
CC-SG 管理から KX II-101-V2 を除外する.....	181
プロキシ モードでの CC-SG の使用.....	182
仕様	183
KX II-101-V2 の仕様.....	183
サポートされているビデオ解像度.....	184
サポートされているキーボード言語.....	185
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).....	186
サポートされているブラウザ.....	188
認定モデム.....	188
コネクタ.....	188
使用される TCP ポートおよび UDP ポート.....	189
Network Speed Settings.....	191
9 ピンのピン配列.....	192
Updating the LDAP Schema	193
ユーザ グループ情報を返す.....	193
LDAP から返す場合.....	193
Microsoft Active Directory から返す場合.....	193
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.....	194
新しい属性を作成する.....	194
属性をクラスに追加する.....	195
スキーマ キャッシュを更新する.....	197
ユーザ メンバの rciusergroup 属性を編集する.....	198
ラック マウント	201
横取り付け用 L ブラケットを KX II-101-V2 に取り付ける.....	201
情報メモ	203
Java Runtime Environment (JRE).....	203
キーボード、ビデオ、およびマウスに関するメモ.....	203
Sun Blade ビデオ、キーボード、およびマウスのサポート制限.....	204
Sun キーボードのキー サポートの制限.....	204
ローカル キーボードからの BIOS アクセスの制限.....	205
HP UX RX 1600 キーボードおよびマウスの設定.....	206
Compaq Alpha および IBM P Server のマウス モードの制限.....	206

目次

Windows 2000 および Windows 2003 Server のキーボードの制限.....206

FAQ **207**

索引 **209**

この章の内容

KX II-101-V2 ヘルプ	1
KX II-101-V2 の概要	2
製品の写真.....	3
製品の特長.....	4
用語.....	5
パッケージの内容.....	6

KX II-101-V2 ヘルプ

KX II-101-V2 ヘルプでは、**KX II-101-V2** 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、ターゲットサーバおよび電源タップに対するアクセス、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-101-V2** の保守と診断に関する情報も提供します。

PDF バージョンのヘルプは、Raritan の Web サイトの「**Firmware and Documentation**」ページ

<http://www.raritan.com/support/firmware-and-documentation/>参照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推奨します。

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。

関連文書

KX II-101-V2 ヘルプには、**KX II-101-V2 デバイス 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 サイトの「**Firmware and Documentation**」ページ

<http://www.raritan.com/support/firmware-and-documentation/>参照にあります。

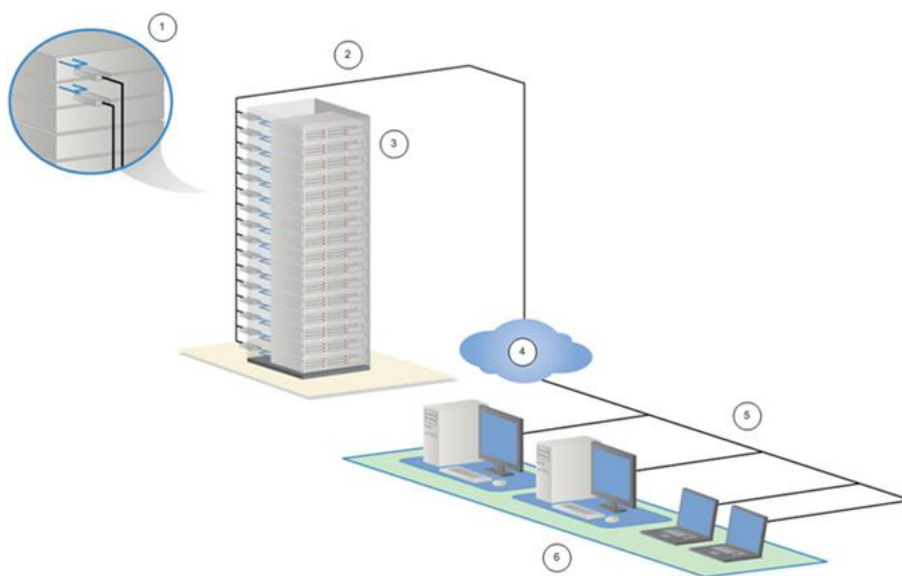
KX II-101-V2 で使用するクライアント アプリケーションのインストールの要件および手順についても、Raritan の Web サイトにある『**KVM and Serial Access Clients Guide**』を参照してください。適用できる場合は、**KX II-101-V2** で使用される特定のクライアント機能がこのヘルプに含まれています。

KX II-101-V2 の概要

Dominion KX II-101-V2 をご購入いただきありがとうございます。KX II-101-V2 は、ターゲット サーバへの接続用の 1 つのキーボード、ビデオ、およびマウス (KVM) ポートおよび IP ネットワークへの接続用の 1 つの IP ポートを提供します。KX II-101-V2 デバイス内では、サーバからの KVM 信号が IP 形式に変換され、IP ネットワーク経由で送信するために圧縮されます。

KX II-101-V2 ドングル フォームファクタのため、ターゲット サーバの近くに容易にインストールでき、各 KX II-101-V2 デバイスは、独自の IP アドレスを持ちます。各デバイスには、外部の AC-DC 電源アダプタ経由で電力が供給されます。

KX II-101-V2 は、スタンドアロン装置として動作できます。また、Raritan の CommandCenter Secure Gateway (CC-SG) 管理ユニットを使用して、その他の Raritan アクセス製品と共に単一の論理ソリューションに統合できます。



図の説明	
①	KX II-101-V2
②	LAN
③	Windows®、Linux®、および Sun™ サーバ
④	TCP/IP
⑤	LAN
⑥	リモート (ネットワーク) アクセス

製品の写真



KX II-101-V2

製品の特長

インタフェース

- 統合 PS/2 KVM 接続
- 制御および仮想メディア用の USB 接続
- 初期デバイス設定、診断、外部のモデム アクセス、および Raritan の電源タップ制御用のシリアル管理ポート
- モニタ接続用のローカル ポート
- 10/100-base-T 自動検出、全二重をサポートする Ethernet LAN ポート

ネットワーク設定

- DHCP または固定 IP デバイス アドレス

システム管理機能

- Ethernet 経由でアップグレード可能なファームウェア
- フェールセーフ ファームウェア アップグレード機能
- 手動で、またはネットワーク タイム プロトコル (NTP/SNTP) を使用した同期によって設定できるクロック
- ローカルのタイムスタンプ付き管理者アクティビティ ログおよび管理者が無効にすることができる SNMP V2 エージェント
- RADIUS および LDAP/LDAPS 認証プロトコルのサポート

管理の特長

- Web ベース管理
- LDAP、Active Directory®、RADIUS、または内部認証および認可
- DHCP または固定 IP アドレス指定
- Raritan の CommandCenter Secure Gateway (CC-SG) 管理ユニットとの統合

ユーザ機能

- 共通のブラウザによる Web ベースのアクセス
- わかりやすいグラフィカル ユーザ インタフェース (GUI)
- 複数のリモート ユーザを有効にする PC 共有モード
- TCP 通信
- 英語ユーザ インタフェース
- 仮想メディア アクセス
- ずれないマウス (Absolute Mouse Synchronization™)
- プラグアンドプレイ
- ビデオおよび仮想メディアを含む全 KVM 信号の 256 ビット暗号化

電源

- 外部の AC/DC アダプタによる電力供給

ビデオ解像度

- 60 Hz まで最大 1600X1200 の解像度

取り付け

- ラック マウント ブラケット

詳細については、「AC-DC Adapter and Rack Mount」を参照してください。

用語

用語	説明
ターゲット サーバ	KX II-101-V2 経由でリモートでアクセスされるサーバとその接続済み KVM の設定。
リモート PC	KX II-101-V2 に接続しているターゲット サーバへのアクセスとその制御に使用する、Windows®、Linux®、Apple Macintosh® の各コンピュータ。
管理シリアル ポート	管理シリアル ポートを使用して、DB9 (オス) ケーブルで PC のシリアル ポートに接続します。次に、標準のエミュレーション ソフトウェア パッケージ (ハイパーターミナルなど) を使用して、管理シリアル ポートにアクセスします。管理シリアル ポートはネットワーク設定に使用されます。
ローカル ユーザ ポート	ターゲット サーバのすぐ近くにいるユーザが、KX II-101-V2 の電源を切らずにネイティブ モニタ

用語	説明
	を使用できます。
仮想メディア	KVM ターゲット サーバがクライアント PC やネットワーク ファイル サーバからメディアにリモートでアクセスできるようにします。

パッケージの内容

各 KX II-101-V2 デバイスには、次の品目が同梱されています。

- KX II-101-V2 - KVM over IP
- KVM ケーブル
- 電源アダプタ - AC/DC 5VDC (汎用アダプタ付き)
- マウント ブラケット キット
- 印刷版クイック ステップ ガイド
- 印刷版アプリケーション リリース ノート (該当する場合)
- 印刷版テクニカル ノート (該当する場合)

この章の内容

概要.....	7
デフォルトのログイン情報	7
入門.....	8

概要

この章では、KX II-101-V2 のインストールおよび設定方法について説明します。インストールと設定は、次の手順で構成されています。

- **手順 1: ターゲット サーバの設定** 『8p. 』
- **手順 2: ネットワーク ファイアウォールの設定** 『20p. 』
- **手順 3: 装置の接続** 『21p. 』
- **手順 4: KX II-101-V2 の設定** 『26p. 』

最適なパフォーマンスを確保するために、KX II-101-V2 をインストールする前に、KX II-101-V2 を経由してアクセスするターゲット サーバを設定します。次の設定要件は、KX II-101-V2 へのリモート アクセスに使用するコンピュータではなく、ターゲット コンピュータのみに適用されます。

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-101-V2 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-101-V2 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

デフォルト設定 値
とを強くお勧めします。

入門

Microsoft® Internet Explorer® バージョン 6 または Windows 2000® を使用している KX II-101-V2 ユーザは、Service Pack 4 (SP4) 以上にアップグレードする必要があります。

KX II-101-V2 は、出荷時に固定 IP アドレスが設定されています。DHCP サーバを使用していないネットワークでは、KX II-101-V2 シリアル管理コンソールまたは KX II-101-V2 リモート コンソールを使用して、新しい固定 IP アドレス、ネット マスク、およびゲートウェイ アドレスを設定する必要があります。

リモート コンソールを使用して IP アドレスを KX II-101-V2 に割り当てる方法の詳細については、「IP アドレスの割り当て」を参照してください。シリアル管理コンソールを使用して IP アドレスを設定する方法の詳細については、「**ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定する (オプション) 『31p.』**」を参照してください。

手順 1: ターゲット サーバの設定

KX II-101-V2 をインストールする前に、KX II-101-V2 を経由してアクセスするターゲット サーバを設定して、最適なパフォーマンスを確保します。次の設定要件は、KX II-101-V2 へのリモート アクセスに使用するコンピュータではなく、ターゲット コンピュータのみに適用されます。

サーバ ビデオ解像度を設定する

最適な帯域幅効率とビデオ パフォーマンスを得るために、Windows®、X-Windows®、Solaris™、および 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ターゲット サーバは、デスクトップの背景を無地でシンプルな明るい色のグラフィックに設定する必要があります。写真や複雑な階調を特徴とする背景は避ける必要があります。

サーバのビデオ解像度と更新レートが KX II-101-V2 でサポートされていることと、信号がノンインタレースであることを確認します。KX II-101-V2 は、以下のビデオ解像度をサポートしています。

解像度		
640x350、70 Hz	720x400、85 Hz	1024x768、90 Hz
640x350、85 Hz	800x600、56 Hz	1024x768、100 Hz
640x400、56 Hz	800x600、60 Hz	1152x864、60 Hz
640 x 400、84 Hz	800x600、70 Hz	1152x864、70 Hz
640 x 400、85 Hz	800x600、72 Hz	1152x864、75 Hz
640x480、60 Hz	800x600、75 Hz	1152x864、85 Hz
640x480、66.6 Hz	800x600、85 Hz	1152x870、75.1 Hz
640x480、72 Hz	800x600、90 Hz	1152 x 900、66 Hz
640x480、75 Hz	800x600、100 Hz	1152 x 900、76 Hz
640x480、85 Hz	832 x 624、75.1 Hz	1280 x 960、60 Hz
640x480、90 Hz	1024x768、60 Hz	1280x960、85 Hz
640x480、100 Hz	1024x768、70 Hz	1280x1024、60 Hz
640x480、120 Hz	1024x768、72 Hz	1280x1024、75 Hz
720 x 400、70 Hz	1024x768、75 Hz	1280x1024、85 Hz
720 x 400、84 Hz	1024x768、85 Hz	1600 x 1200、60 Hz

Sun ビデオ解像度

Sun™ システムには、コマンド ライン解像度と GUI 解像度の 2 種類の解像度設定があります。KX II-101-V2 でサポートされている解像度の詳細については、「[サーバ ビデオ解像度を設定する『9p.』](#)」を参照してください。

注: サポートされている解像度が機能しない場合は、モニタがマルチシンクであることを確認してください。一部のモニタは、H&V sync で機能しません。

コマンド ライン解像度

▶ **コマンド ライン解像度を確認するには、以下の手順に従います。**

1. 次のコマンドを root で実行します。# `eeprom output-device`

▶ **コマンド ライン解像度を変更するには、以下の手順に従います。**

1. 次のコマンドを実行します。# `eeprom output-device=screen:r1024x768x75` (1024x768x75 は KX II-101-V2 がサポートしている解像度です。)
2. コンピュータを再起動します。

GUI 解像度/32 ビット

▶ **32 ビット カードの GUI 解像度を確認するには、以下の手順に従います。**

1. 次のコマンドを実行します。# `/usr/sbin/pgxconfig -prconf`

▶ **32 ビット カードの GUI 解像度を変更するには、以下の手順に従います。**

1. 次のコマンドを実行します。# `/usr/sbin/pgxconfig -res1024x768x75` (1024x768x75 は KX II-101-V2 がサポートしている解像度です。)
2. コンピュータを再起動します。

GUI 解像度/64 ビット

▶ **64 ビット カードの GUI 解像度を確認するには、以下の手順に従います。**

1. 次のコマンドを実行します。# `/usr/sbin/m64config -prconf`

▶ **64 ビット カードの GUI 解像度を変更するには、以下の手順に従います。**

1. 次のコマンドを実行します。# `/usr/sbin/m64config -res1024x768x75` (1024x768x75 は KX II-101-V2 がサポートしている解像度です。)
2. コンピュータを再起動します。

GUI 解像度/Solaris 8

- ▶ **32 ビット カードおよび 64 ビット カードの Solaris™ 8 の解像度を確認するには、以下の手順に従います。**

1. 次のコマンドを実行します。# /usr/sbin/fbconfig -prconf

- ▶ **32 ビットおよび 64 ビット カードの Solaris 8 の解像度を変更するには、以下の手順に従います。**

1. 次のコマンドを実行します。# /usr/sbin/fbconfig -res1024x768x75 (1024x768x75 は KX II-101-V2 がサポートしている解像度です。)

2. コンピュータを再起動します。

マウスの設定

KX II-101-V2 は、次のマウス モードで動作します。ずれないマウス (Absolute Mouse Synchronization™)、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。

注:インテリジェント マウス モードを使用している際は、アニメーション カーソルを使用しないでください。

Absolute Mouse Synchronization 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。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、このセクションで説明するマウス 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、さまざまなターゲット 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 OS のマニュアルを参照してください。

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] (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 **[Mouse]** (マウス) メニューの **[Synchronize Mouse]** (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]** ボタンをクリックしてします。
 - 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] (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-101-V2** 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-101-V2** 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-101-V2** 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。

警告! **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-101-V2** 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 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] 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 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-101-V2 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-101-V2 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-101-V2 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。

警告! 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-101-V2 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 の設定 (Red Hat 9)

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-101-V2 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-101-V2 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、ビデオ解像度を変更されます。

- ▶ **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-101-V2 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-101-V2 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-101-V2 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 9 KVM 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® 9 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 を使用している Red Hat 9 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 の設定 (Red Hat 4)

注: 以下の設定は、標準マウス モード専用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-101-V2 でサポートされている解像度を選択します。
 - c. [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、ビデオ解像度を変更されます。

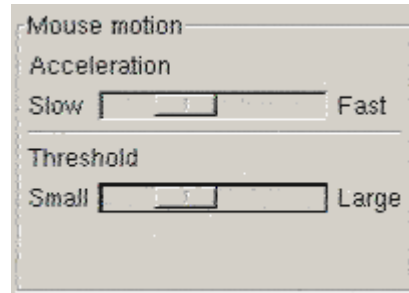
注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

Sun Solaris の設定

Solaris™ ターゲット サーバは、KX II-101-V2 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ている解像度を以下に示します。

解像度
1024x768@60Hz
1024x768@70Hz
1024x768@75Hz
1024x768@85Hz
1280x1024@60Hz

マウスの加速値をちょうど 1 に設定し、しきい値もちょうど 1 に設定します。Solaris オペレーティング システムを実行しているターゲットサーバのビデオ出力は VGA (コンポジット Sync ではなく H-and-V Sync) である必要があります。これは、グラフィカル ユーザ インタフェースで設定するか、コマンド ライン `xset mouse a t` を使用して設定します。ここで、**a** は加速値、**t** はしきい値です。



▶ **Sun のビデオ カード出力を複合同期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. `#eeprom output-device=screen:r1024x768x75` コマンドを発行して、出力解像度を変更します。
3. 次に、boot コマンドを発行して、サーバを再起動します。

または、Raritan 社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。コンポジット Sync 出力を使用する Sun では、KX II-101-V2 用の APSSUN II Raritan Guardian が必要です。独立同期出力を使用する HD15 Sun では、KX II-101-V2 用の APKMSUN Raritan Guardian が必要です。

Apple Macintosh の設定

Mac® は「初期状態のまま」KX II-101-V2 と連動します。ただし、ずれないマウス (Absolute Mouse Synchronization) を使用して、[KX II-101-V2 Port] (KX II-101-V2 ポート) ページでずれないマウス モードおよび Mac サーバのずれないマウス スケーリングを有効にする必要があります。

▶ **この設定を有効にするには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [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. 編集するポートの [Port Name] (ポート名) をクリックします。

3. [USB Connection Settings] (USB 接続設定) セクションで、[Enable Absolute Mouse] (ずれないマウスを有効にする) チェックボックスと [Enable Absolute mouse scaling for MAC server] (Mac サーバのずれないマウス スケーリングを有効にする) チェックボックスをオンにします。[OK] をクリックします。

詳細については、「[Port Configuration] (ポート設定)」を参照してください。

IBM AIX の設定

1. スタイル マネージャを開きます。
2. [Mouse Settings] (マウスの設定) をクリックし、[Mouse Acceleration] (マウスの加速) を 3.0 に設定し、[Threshold] (しきい値) を 1.0 に設定します。

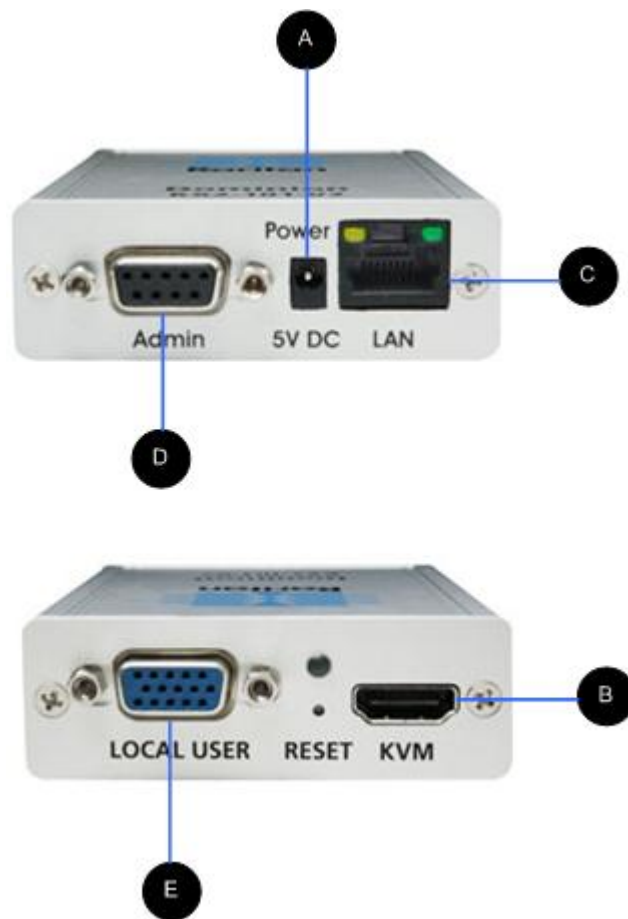
手順 2: ネットワーク ファイアウォールの設定

ネットワーク ファイアウォールを介して KX II-101-V2 にアクセスするには、ファイアウォールが TCP ポート 5000 での通信を許可している必要があります。または、KX II-101-V2 を設定して、指定した別の TCP ポートを使用することができます。

KX II-101-V2 の Web アクセス機能を利用するには、ファイアウォールで TCP ポート 443 (HTTPS 通信用の標準 TCP ポート) のインバウンド通信が許可されている必要があります。KX II-101-V2 で HTTP 要求を HTTPS にリダイレクトする機能 (これにより、ユーザは `https://xxx.xxx.xxx.xxx` の代わりに、より一般的な `http://xxx.xxx.xxx.xxx` を入力できます) を利用するには、ファイアウォールで TCP ポート 80 (HTTPS 通信用の標準 TCP ポート) のインバウンド通信も許可されている必要があります。

手順 3: 装置の接続

KX II-101-V2 には、下の図に示す物理接続が用意されています。図中の各文字は、ここで説明する機器接続プロセスの各手順に対応しています。



図の説明

A	電源コネクタ	単一の電源アダプタ。
B	モニタ、PS/2、USBコネクタ付きの KVM ケーブル (付属)	デバイスをモニタおよびターゲット サーバに接続するための KVM ケーブルを接続します。
C	Ethernet LAN	LAN に接続できます。

図の説明		
D	管理ポート	次のいずれかの作業を行うために使用します。 <ul style="list-style-type: none"> • PC 上でターミナル エミュレーション プログラムを使用してデバイスを設定および管理します。 • 電源タップの設定および管理を行います (別売のアダプタが必要です)。 • デバイ스에ダイヤルインする外部モデムを接続します。
E	ローカル ポート	ローカル ポートからモニタに接続します。

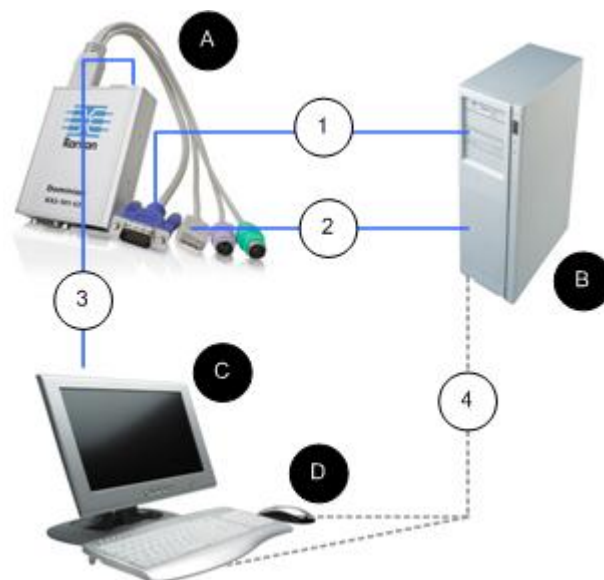
A: 電源

KX II-101-V2 には、デバイスに用意されている 100 ~ 240V AC 入力 /5V DC 出力の電源アダプタによって電力が供給されます。標準の AC 電源の場合は、付属の AC 電源アダプタを電源ポートに差し込み、反対側を近くの AC 電源コンセントに差し込みます。

B: ターゲット サーバ

PS/2 または USB を使用してターゲットに接続します。接続する前に、ターゲット サーバのビデオをサポートされている解像度に設定します。仮想メディアまたはずれないマウス モードを使用している場合は、USB 接続を使用します。

USB の設定



▶ **USB ターゲット サーバ**で使用するように **KX II-101-V2** を設定するには、以下の手順に従います。

1. 付属のビデオ ケーブルを使用して KX II-101-V2 をターゲット ビデオ ポートに接続します。
2. KVM ケーブルの USB コネクタを KX II-101-V2 に、およびターゲット サーバの USB ポートに接続します。
3. ローカル ビデオを使用する必要がある場合は、モニタを KX II-101-V2 のローカル ポートに接続します。**オプション**
4. USB キーボードおよびマウスをターゲットに直接接続します。**オプション**

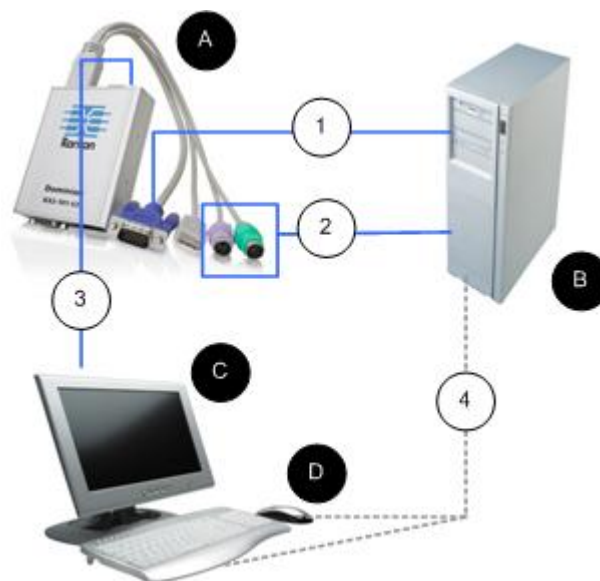
注:仮想メディアを使用している場合は、**USB 接続**を使用する必要があります。

USB 接続に関する図の説明

A	KX II-101-V2
B	ターゲット サーバ
C	ローカル モニタ (オプション)
D	ローカル マウスおよびキーボード (オプション)

USB 接続に関する図の説明	
①	KX II-101-V2 からターゲットへのビデオ接続
②	KX II-101-V2 からターゲットへの USB 接続
③	KX II-101-V2 のローカル ポートからモニタへのオプションのモニタ接続
④	ターゲット サーバからマウスおよびキーボードへのオプションの USB 接続 (ケーブルは別売)

PS/2 の設定



▶ **PS/2** ターゲット サーバで使用するように **KX II-101-V2** を設定するには、以下の手順に従います。

1. 付属のビデオ ケーブルを使用して **KX II-101-V2** をターゲット ビデオ ポートに接続します。
2. KVM ケーブルの **PS/2** コネクタをターゲットの **PS/2** ポートに接続します。
3. ローカル ビデオを使用する必要がある場合は、モニタを **KX II-101-V2** のローカル ポートに接続します。オプション

4. PS/2 キーボードおよびマウスがある場合は、PS/2 - USB アダプタ(別売) を使用してターゲットの USB ポートに直接接続します。オプション

注:仮想メディアを使用している場合は、USB 接続を使用する必要があります。

PS/2 接続に関する図の説明	
	KX II-101-V2
	ターゲット サーバ
	ローカル モニタ
	ローカル マウスおよびキーボード (オプション)
	KX II-101-V2 からターゲットへのビデオ接続
	KX II-101-V2 からターゲット サーバへの KVM ケーブル接続
	KX II-101-V2 からモニタへのオプションの接続
	ターゲットからキーボードおよびマウスへのオプションの PS/2 - USB アダプタ接続 (ケーブルは別売)

C: ネットワーク

標準 Ethernet ケーブルを、「LAN」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。

Ethernet 接続の上にある LAN LED は Ethernet のアクティビティを示します。KX II-101-V2 の使用中は、黄色の LED が点滅し、10 Mbps の IP トラフィックを示します。緑色のライトは 100 Mbps の接続速度を示します。

D: 管理ポート

管理ポートを使用すると、HyperTerminal のようなターミナル エミュレーション プログラムを使用して、KX II-101-V2 の設定とセットアップを実行できます。1 本の DB9M - DB9F ストレート シリアル ケーブルを使用して、KX II-101-V2 から PC またはラップトップのシリアルポートに接続します。シリアル ポート通信の設定は、次のように設定する必要があります。

- 115,200 Baud
- 8 データ ビット
- 1 ストップ ビット
- パリティなし
- フロー制御なし

E: ローカル ユーザ ポート

ローカル ユーザ ポートは、モニタに直接接続するための、ターゲット サーバ ビデオへのパススルーとして機能します。ローカルのキーボードとマウスは、ターゲット サーバに直接接続する必要があります。

USB 設定の場合、ローカル ビデオのみをローカル ユーザ ポートでターゲット サーバに接続します。キーボードとマウスは、USB ポートを使用してターゲット サーバに直接接続します。

手順 4: KX II-101-V2 の設定

注: Web ブラウザを介して KX II-101-V2 を設定している場合は、KX II-101-V2 とクライアントの間にクロスオーバー ケーブルを使用する必要があります。

リモート コンソールを使用して KX II-101-V2 を設定する

KX II-101-V2 リモート コンソールは、デバイスを使用および管理する前に設定できる Web ベースのアプリケーションです。リモート コンソールを使用して KX II-101-V2 を設定する前に、ワークステーションとデバイスをネットワークに接続しておく必要があります。

ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定することもできます。詳細については、「**ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定する (オプション)**」『31p. 』を参照してください。

新しいパスワードの設定

リモート コンソールに最初にログインすると、デフォルトのパスワードに代わる新しいパスワードの設定を確認するプロンプトが表示されます。次に、KX II-101-V2 を設定できます。

1. KX II-101-V2 デバイスにネットワーク接続されているワークステーションにログインします。
2. サポートされている Web ブラウザ (Internet Explorer® (IE) や Firefox® など) を起動します。
3. ブラウザのアドレス フィールドに、デバイスのデフォルトの IP アドレス「192.168.0.192」を入力します。
4. Enter キーを押します。ログイン ページが開きます。
5. ユーザ名に「admin」、パスワードに「raritan」と入力します。
6. [Login] (ログイン) をクリックします。[Change Password] (パスワードの変更) ページが表示されます。
7. [Old Password] (旧パスワード) フィールドに「raritan」と入力します。
8. [New Password] (新しいパスワード) フィールドと [Confirm New Password] (新しいパスワードの確認) フィールドに新しいパスワードを入力します。パスワードには、英数字と印刷可能な特殊文字を 64 文字まで使用できます。
9. [Apply] (適用) をクリックします。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。
10. [OK] をクリックします。[Port Access] (ポート アクセス) ページが開きます。

IP アドレスの割り当て

▶ IP アドレスを割り当てるには、次の手順に従います。

1. KX II-101-V2 リモート コンソールで、[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. [Device Name] (デバイス名) フィールドで、KX II-101-V2 デバイスにわかりやすい名前を指定します。スペースなしで英数字および特殊文字を最大 32 文字入力できます。
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-101-V2 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ため、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. **[IP auto configuration] (IP 自動設定)** ドロップダウン リストで、IP 設定を選択します。
 - **[None] (なし) (静的 IP)** - **KX II-101-V2** 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ため、これはデフォルトの推奨オプションです。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。
 - **[DHCP] (DHCP)** - 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、**KX II-101-V2** を起動するたびに DHCP サーバによって割り当てられます。
5. これで、**[DHCP] (DHCP)** が選択されており、**[Obtain DNS Server Address] (DNS サーバ アドレスを取得する)** 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する)** 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する)** を選択した場合は、DHCP サーバから得られた DNS 情報が使用されます。
6. **[Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用する)** が選択されている場合は、**[DHCP] (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したアドレスを使用して DNS サーバに接続されます。

[Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用する) が選択されている場合は、以下の情報を入力します。これらのアドレスは、停電のためにプライマリ DNS サーバ接続が失われた場合に使用されるプライマリおよびセカンダリの DNS アドレスです。

- a. プライマリ DNS サーバ IP アドレス
 - b. 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。ProductName< デバイスからネットワークにアクセスできるようになります。クロスオーバーケーブルを取り外し、Cat5 ケーブルを使用して KX II-101-V2 をスイッチに接続します。

ターゲット サーバに名前を付ける

1. KX II-101-V2 をターゲット サーバに接続します。
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. 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. 名前を入力します。英数字と特殊文字を 32 文字まで入力できます。
5. [OK] をクリックします。

Port 1

Type:
KVM

Name:

Power Association

Power Strip Name

Outlet Name

---	▼
---	▼
---	▼
---	▼

▶ USB Connection Settings

▶ Advanced USB Connection Settings

リモート認証

CC-SG ユーザへの注意事項

KX II-101-V2 が CommandCenter Secure Gateway で制御されている場合、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 認証の詳細については、**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。これらのガイドは、Raritan の Web サイト (www.raritan.com) のサポート セクションからダウンロードできます。

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-101-V2 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-101-V2 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-101-V2 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-101-V2 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-101-V2 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-101-V2 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 『82p. の "User Management" 参照 』**」を参照してください。

ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定する (オプション)

管理シリアル コンソールを HyperTerminal のようなターミナル エミュレーション プログラムと共に使用して、KX II-101-V2 の次の設定パラメータを設定できます。

- IP アドレス
- サブネット マスク アドレス
- ゲートウェイ アドレス
- IP 自動設定
- LAN 速度
- LAN インタフェースモード

KX II-101-V2 でターミナル エミュレーション プログラムを使用するには、まず付属の RS-232 シリアル ケーブルを使用して KX II-101-V2 の管理ポートと PC の COM ポートを接続する必要があります。

手順を説明するために、このセクションではターミナル エミュレーション プログラムに HyperTerminal を使用しています。任意のターミナル エミュレーション プログラムを使用できます。

▶ ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定するには、以下の手順に従います。

1. 付属の RS-232 シリアル ケーブルを使用して、KX II-101-V2 とローカル PC を接続します。
2. KX II-101-V2 の管理ポートと PC の COM1 ポートを接続します。
3. 使用するターミナル エミュレーション プログラムを起動し、KX II-101-V2 を設定します。
4. ターミナル エミュレーション プログラムで次のポート設定を設定します。
 - ビット/秒 - 115200
 - データ ビット - 8
 - パリティ - なし
 - ストップ ビット - 1
 - フロー制御 - なし
5. KX II-101-V2 に接続します。ログイン ページが開きます。
6. 管理者ユーザ名を入力して、Enter キーを押します。パスワードの入力を確認するプロンプトが表示されます。
7. デフォルトの管理者名「*admin*」を入力して、Enter キーを押します。パスワードの入力を確認するプロンプトが表示されます。
8. Admin Port > プロンプトで、「*config*」と入力して、Enter キーを押します。

9. **Config >** プロンプトで、「*network*」と入力して、**Enter** キーを押します。
10. 現在のインタフェース設定を確認するには、**Interface >** プロンプトで、「*interface*」と入力して、**Enter** キーを押します。現在のインタフェース設定が表示されます。
11. 新規ネットワーク設定を設定するには、**Network (ネットワーク)** のプロンプトで、「*interface*」と入力し、その後次に次のいずれかのコマンドとその適切な引数 (省略可能) を入力して **Enter** キーを押します。

コマンド	引数	[Options] (オプション)
ipauto	none dhcp	<p>none - デバイスの IP アドレスを手動で指定できます。次の例に示すように、このオプションの後に ip コマンドと IP アドレスを続ける必要があります。</p> <pre>interface ipauto none ip 192.168.50.12</pre> <p>dhcp - 起動時に、IP アドレスをデバイスに自動的に割り当てます。</p> <pre>interface ipauto dhcp</pre>
ip	IP アドレス	<p>デバイスに割り当てる IP アドレス。初めて IP アドレスを手動で設定するときは、ipauto コマンドと none オプションと共にこのコマンドを使用する必要があります。詳細については、「ipauto」を参照してください。IP アドレスを手動で割り当てたら、ip コマンドを単独で使用して IP アドレスを変更できます。</p>
mask	サブネットマスク	<p>コマンド列は "interface" でなければなりません。</p> <pre>interface ip ... interface mask サブネット マスク IP アドレス</pre>

コマンド	引数	[Options] (オプション)
		interface gw ゲート ウェイ IP アドレス interface mode
gw	IP アドレス	ゲートウェイ IP アドレス
mode	mode	<p>Ethernet モード。次の選 択肢があります。</p> <ul style="list-style-type: none"> ▪ auto - ネットワークに 応じて速度とインタフ ェースを自動で設定し ます。 ▪ 10hdx - 10 Mb/s、半二 重。 ▪ 10fdx - 10 Mb/s、全二 重。 ▪ 100hdx - 100 Mb/s、半 二重。 ▪ 100fdx - 100 Mb/s、全 二重。

設定が正常に変更されると、次のような確認メッセージが表示されま
す。

```
Admin Port > config
Admin Port > Config > network
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.126
Network interface configuration successful.
```

KX II-101-V2 の設定を完了したら、コマンド プロンプトで「logout」と
入力し、Enter キーを押します。コマンドライン インタフェースから
ログアウトされます。

この章の内容

インタフェース	34
Virtual KVM Client (VKC).....	43

インタフェース

KX II-101-V2 リモート コンソール インタフェース

KX II-101-V2 リモート コンソールとは、KVM ターゲット サーバおよび KX II-101-V2 に接続されているシリアル ターゲットにログインしたり、リモートから KX II-101-V2 を管理したりすることができるブラウザ ベースのグラフィカル ユーザ インタフェースのことです。

KX II-101-V2 リモート コンソールは、接続されている KVM ターゲット サーバへのデジタル接続を提供します。KX II-101-V2 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。

注: Internet Explorer® 7 を使用している場合は、ターゲット サーバへの接続時に権限の問題が生じる可能性があります。これを回避するには、以下の手順に従います。

1. *Internet Explorer* で [ツール] メニューの [インターネット オプション] をクリックして、[インターネット オプション] ダイアログ ボックスを開きます。
 2. [インターネット一時ファイル] セクションで [設定] ボタンをクリックします。[設定] ダイアログ ボックスが開きます。
 3. [保存しているページの新しいバージョンの確認] セクションで [自動的に確認する] を選択します。
 4. [OK] をクリックして設定を適用します。
-

ダイレクト ポート アクセスを有効にする

ダイレクト ポート アクセスを使用すると、通常のログイン ページに進まないで KX II-101-V2 リモート クライアントにアクセスできます。ダイレクト ポート アクセスを有効にすると、[Port Access] (ポート アクセス) ページに直接移動する URL を定義できます。

▶ **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. KX II-101-V2 リモート コンソールを起動します。

2. [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] (デバイス サービス) ページが開きます。
3. [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) チェックボックスをオンにします。
4. [Save] (保存) をクリックします。

▶ **ダイレクト ポート アクセス URL を設定するには、以下の手順に従います。**

- IP アドレス、ユーザ名、パスワード、および必要に応じて KX II-101-V2 のポート番号を使用して URL を定義します。

ダイレクト ポート アクセス URL の形式は、次のとおりです。

```
https://IP  
address/dpa.asp?username=username&password=password
```

ヒント:ダイレクト ポート アクセス URL を定義し、Web ブラウザにブックマークとして保存すると、再使用が容易になります。

KX II-101-V2 コンソールでの案内

KX II-101-V2 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

KX II-101-V2 リモート コンソールへのログインが正常に完了すると、[Port Access] (ポート アクセス) ページが表示されます。このページには、KX II-101-V2 ポート、接続されている KVM ターゲット サーバ、およびその可用性がリスト表示されます。[Port Access] (ポート アクセス) ページは、KX II-101-V2 に接続されている KVM ターゲット サーバへのアクセスを提供します。KVM ターゲット サーバとは、KX II-101-V2 デバイスを介して制御するサーバのことです。KVM ターゲット サーバは、デバイスの背面で KX II-101-V2 ポートに接続されます。

▶ **[Port Access] (ポート アクセス) ページを使用するには**

1. KX II-101-V2 リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。以下の情報が表示されます。
 - [Port Name] (ポート名) - KX II-101-V2 ポートの名前です。当初、これには「Dominion_KX2_101_Port1」が設定されていますが、わかりやすい別の名前に変更できます。[Port Name] (ポート名) のリンクをクリックすると、[Port Action] (ポート アクション) メニューが表示されます。
 - [Availability] (可用性) - [Availability] (可用性) は、[Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、または [Unavailable] (使用不可能) のいずれかです。
2. アクセスするターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。使用可能なメニュー オプションについての詳細は、「[Port Action] (ポート アクション) メニュー」を参照してください。
3. [Port Action] (ポート アクション) メニューから、目的のメニュー コマンドを選択します。

Port Action Menu

[Port Access] (ポート アクセス) リストで [Port Name] (ポート名) をクリックすると、[Port Action] (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。[Port Action] (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 - Creates a new connection to the target server. For the KX II-101-V2 Remote Console, a new **Virtual KVM Client** 『43p. の "**Virtual KVM Client (VKC)**"参照』 page appears.

注: すべての接続がビジー状態の場合、KX II-101-V2 リモート コンソールでは使用可能なポートに対して、このオプションを使用できません。

- [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) および [connected] (接続済み) であるか、または [up] (アップ) および [busy] (ビジー) であるときにのみ使用できます。
- [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 つ以上の電源が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 つ以上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 つ以上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に与えられているときにのみ表示されます。

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。[Port Access] (ポート アクセス) ページの左下隅 (サイドバー) にある [Favorite Devices] (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-101-V2 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-101-V2 デバイスを接続されている KX デバイスから取得する (ログインの後)。

▶ **お気に入りの KX II-101-V2 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。**

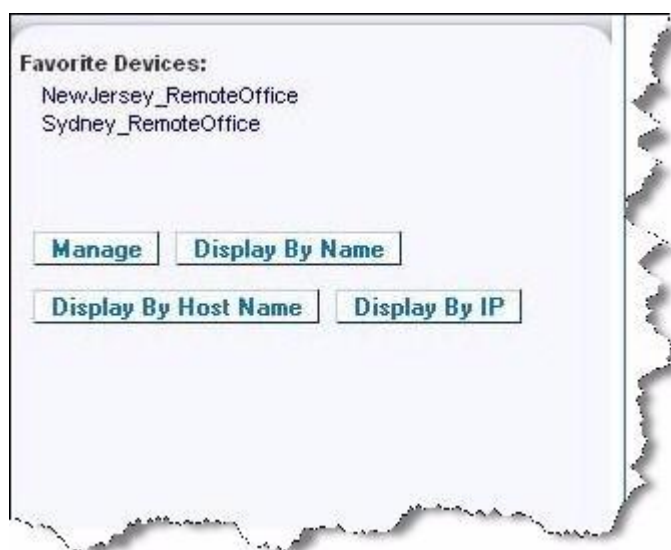
- [Display by Name] (名前順) をクリックします。

▶ **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。



[Manage Favorites] (お気に入りの管理) ページ

▶ **[Manage Favorites] (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。**

- 左のパネルの [Manage] (管理) ボタンをクリックします。次の内容を含む [Manage Favorites] (お気に入りの管理) ページが表示されます。

メニュー名	目的
[Favorites List] (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。
[Discover Devices - Local Subnet] (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。
[Discover Devices - KX II-101-V2 Subnet] (デバイス検出 - KX II-101-V2 サブネット)	KX II-101-V2 デバイス サブネット上の Raritan デバイスを検出します。
[Add New Device to Favorites] (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。

[Favorites List] (お気に入りリスト) ページ

[Favorites List] (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。

▶ **[Favorites List] (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。**

- [Manage] (管理) の [Favorites List] (お気に入りリスト) を選択します。[Favorites List] (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 Raritan デバイスを検出する

ローカル サブネット (KX II-101-V2 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。「**[Favorites List] (お気に入りリスト) ページ『40p.』**」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. [Manage] (管理) の [Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット) を選択します。[Discover Devices - Local Subnet] (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、[Use Default Port 5000] (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. [Use Default Port 5000] (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. [Discover on Port] (検出ポート) フィールドに、ポート番号を入力します。
 - c. [Save] (保存) をクリックします。
3. [Refresh] (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 [Favorites List] (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. [Add] (追加) をクリックします。

ヒント: **[Select All]** (すべて選択) および **[Deselect All]** (すべての選択を解除) ボタンを使用すれば、リモート コンソール サブネット上のデバイスをすべて選択したり、すべての選択を解除したりできます。

▶ **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-101-V2 サブネット上の Raritan デバイスを検出する

デバイス サブネット (KX II-101-V2 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。「**[Favorites List]** (お気に入りリスト) ページ『40p.』」を参照してください。

この機能を使用すると、複数の KX II-101-V2 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-101-V2 リモート コンソールは、KX II-101-V2 のサブネット内の KX II-101-V2 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. **[Manage]** (管理) の **[Discover Devices - KX II-101-V2 Subnet]** (デバイス検出 - KX II-101-V2 サブネット) を選択します。**[Discover Devices - KX II-101-V2 Subnet]** (デバイス検出 - KX II-101-V2 サブネット) ページが表示されます。
2. **[Refresh]** (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 **[Favorites List]** (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. **[Add]** (追加) をクリックします。

ヒント: **[Select All]** (すべて選択) および **[Deselect All]** (すべての選択を解除) ボタンを使用すれば、KX II-101-V2 デバイス サブネット上のデバイスをすべて選択したり、すべての選択を解除したりできます。

▶ **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。

お気に入りを追加、編集、削除する

▶ デバイスを **[Favorites List] (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. **[Manage] (管理)** の **[Add New Device to Favorites] (お気に入りへの新しいデバイスの追加)** を選択します。**[Add New Favorite] (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. **[Favorites List] (お気に入りリスト)** ページで、目的の **KX II-101-V2** 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. **[Edit] (編集)** ボタンをクリックします。**[Edit] (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 Address/Host Name] (IP アドレス/ホスト名) - KX II-101-V2** デバイスの **IP アドレス** を入力します。
 - **[Port] (ポート)** (必要な場合)
 - **[Product Type] (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-101-V2** 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. **[Delete] (削除)** ボタンをクリックします。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-101-V2 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。

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。

Virtual KVM Client (VKC)

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。

概要

リモート コンソールを使用してターゲット サーバにアクセスすると、Virtual KVM Client (VKC) のウィンドウが開きます。接続先のターゲット サーバ用に 1 つの Virtual KVM Client があります。このウィンドウには、Windows® タスク バーを介してアクセスします。

Virtual KVM Client ウィンドウは、お使いのコンピュータのデスクトップ上で最小化、最大化、および移動できます。

注: HTML ブラウザを更新すると *Virtual KVM Client* 接続が切断されてしまうので注意してください。

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。







KVM ターゲット サーバへの接続

▶ KVM 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. KX II-101-V2 リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. 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。[Port Action] (ポート アクション) メニューが表示されます。
3. [Connect] (接続) をクリックします。Virtual KVM Client ウィンドウが開き、そのポートに接続されているターゲット サーバが表示されます。

ツール バー

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 (接続速度、色深度など) を手動で調整できる [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できる [Video Settings] (ビデオ設定) ダイアログ ボックスを開きます。
	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 [Calibrate Color] (色調整) を選択するのと同じです。 <i>注: KX II-101-V2 では使用できません。</i>
	[Target Screenshot] (ターゲット スクリーンショット)	ターゲット サーバのスクリーンショットを撮って選択したファイルに保存する場合にクリックします。
	[Synchronize Mouse] (マウスの同期)	デュアル マウス モードで、強制的にターゲット サーバのマウス ポインタがこのマウス ポインタと同調されます。 <i>注: KX II-101-V2 では使用できません。</i>
	[Refresh Screen] (画面)	ビデオ画面を強制的に更新します。

ボタン	ボタン名	説明
	の更新)	
	ビデオ設定の自動感知	ビデオ設定 (解像度、垂直走査周波数) を強制的に更新します。
	[Smart Card] (スマートカード)	ダイアログ ボックスが開き、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できるようになります。 <hr/> <i>注: この機能は、KSX II 2.3.0 以降および KX II 2.1.10 以降でのみ使用できます。</i>
	[Send Ctrl+Alt+Del] (Ctrl+Alt+Delete の送信)	ターゲット サーバに Ctrl+Alt+Delete というキーの組み合わせを送信します。
	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」を開始します。 このモードを終了するには、 Ctrl+Alt+O キーを押します。 <hr/> <i>注: KX II-101-V2 では使用できません。</i>
	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。

ターゲット サーバの電源管理

注: これらの機能は、電源の関連付けを行っている場合にのみ使用できます。

▶ **KVM ターゲット サーバの電源を再投入するには、以下の手順に従います。**

1. KX II-101-V2 リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。

3. [Power Cycle] (電源の再投入) を選択します。確認メッセージが表示されます。

▶ **ターゲット サーバの電源をオンにするには、以下の手順に従います**

1. KX II-101-V2 リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。
3. [Power On] (電源オン) を選択します。確認メッセージが表示されます。

▶ **ターゲット サーバの電源をオフにするには、以下の手順に従います**

1. KX II-101-V2 リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。
3. [Power Off] (電源オフ) を選択します。確認メッセージが表示されます。

KVM ターゲット サーバの切断

注: KX II-101-V2 ローカル コンソールでは、この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。

▶ **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。**

1. 切断するターゲットのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。
2. [Disconnect] (切断) を選択します。


ヒント: Virtual KVM メニューの [Connection] (接続) の [Exit] (終了) を選択することによっても Virtual KVM Client ウィンドウを閉じることができます。

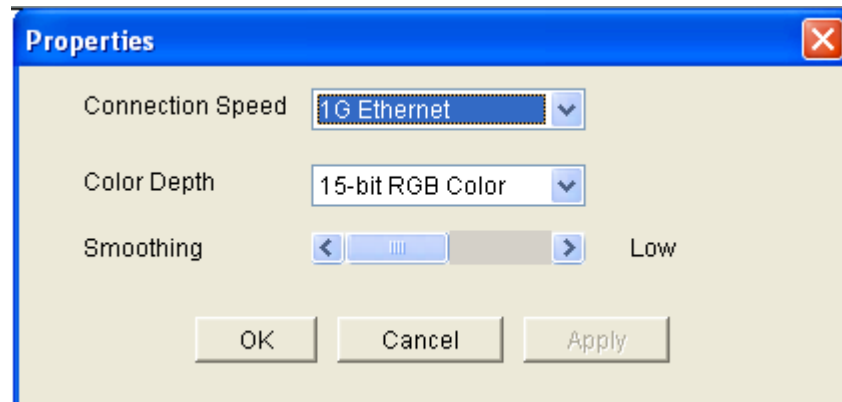
[Connection Properties] (接続プロパティ)

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 リストから接続速度を選択します。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ています。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 マクロをインポート/エクスポートする

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、次の手順に従います。

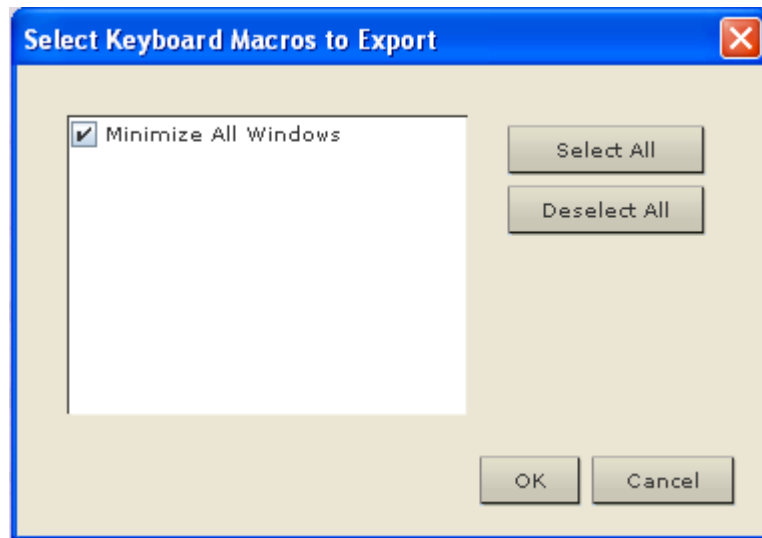
1. [Keyboard] (キーボード) の [Import Keyboard Macros] (キーボード マクロのインポート) を選択して、[Import Macros] (マクロのインポート) ダイアログ ボックスを開きます。マクロ ファイルが格納されているフォルダを参照します。
2. マクロ ファイルをクリックし、[開く] (Open) をクリックしてマクロをインポートします。
 - a. ファイル内で見つかったマクロが多すぎる場合は、エラー メッセージが表示され、[OK] をクリックすると、インポートは終了します。

- 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、インポートの失敗理由に関するメッセージが表示されます。[OK] をクリックし、インポートできないマクロはインポートせずにインポートを続行します。
3. インポートするマクロを選択するには、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] (すべての選択を解除) オプションを使用します。
 4. [OK] をクリックしてインポートを開始します。
 - a. 重複した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。次のいずれかを実行します。
 - [Yes] (はい) をクリックし、既存のマクロをインポートしたバージョンに置き換えます。
 - [Yes to All] (すべてにははい) をクリックし、現在選択されているマクロおよび他の重複しているマクロを置き換えます。
 - [No] (いいえ) をクリックし、元のマクロはそのままで次のマクロに進みます。
 - [Noto All] (すべてにいいえ) をクリックし、元のマクロはそのままで次のマクロに進みます。他の重複しているマクロも同様にスキップされます。
 - [Cancel] (キャンセル) をクリックしてインポートを停止します。
 - あるいは、[Rename] (名前の変更) をクリックし、マクロの名前を変更して、そのマクロインポートします。[Rename] (名前の変更) を選択すると、[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。マクロの新しい名前をフィールドに入力して [OK] をクリックします。ダイアログ ボックスが閉じ、プロセスが進みます。入力する名前が既存のマクロと重複している場合は、警告が表示され、そのマクロに対して別の名前を入力するよう求められます。
 - b. インポート プロセス中に、インポートされたマクロ数が許容値を超えた場合は、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を続行するか、[Cancel] (キャンセル) をクリックしてインポート プロセスを停止します。

その後、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は破棄されます。

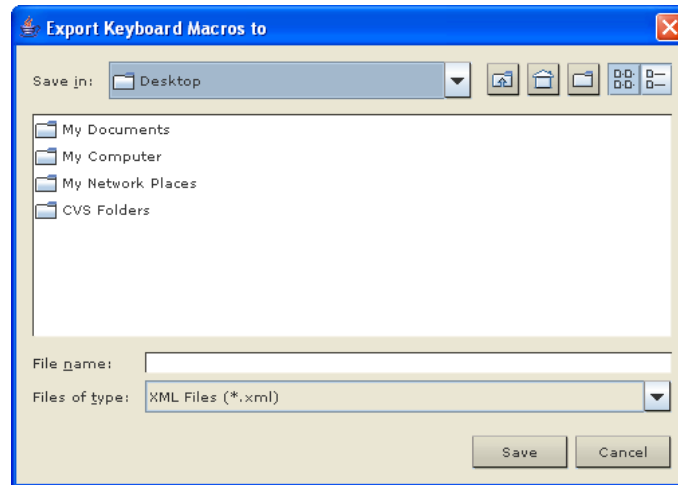
▶ マクロをエクスポートするには、次の手順に従います。

1. [Tools] (ツール) の [Export Macros] (マクロのエクスポート) を選択し、[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 ボックスを開きます。



2. エクスポートするマクロを選択するには、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] (すべての選択を解除) オプションを使用します。
3. [Ok] をクリックします。エクスポートするキーボード マクロ。マクロ ファイルを探して選択するためのダイアログ 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存在します。

4. マクロ ファイルの保存先フォルダを選択し、ファイルの名前を入力して **[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に上書きするか、**[No]** (いいえ) を選択してマクロを上書きせずに警告を閉じます。

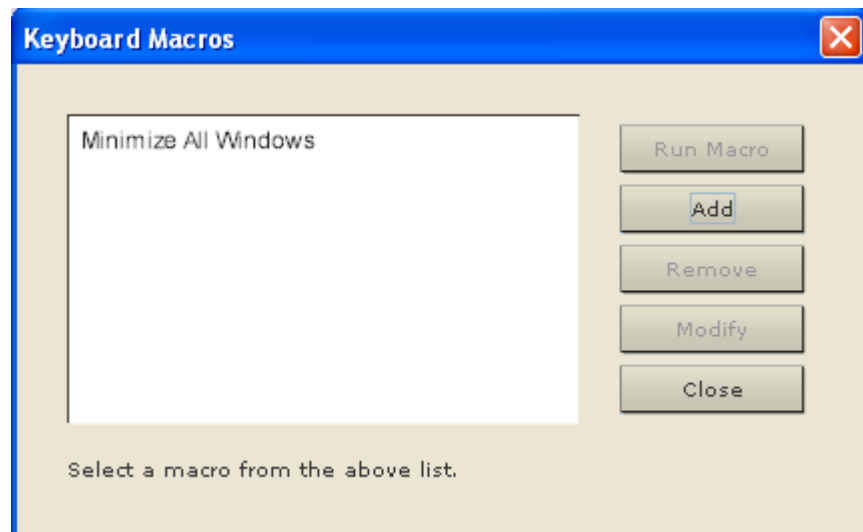


キーボード マクロの作成

▶ 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、マクロの作成後に **[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用してマクロを実行できます。**オプション**
5. **[Keys to Press]** (押すキー) ドロップダウン リストで、コマンドの実行用のキー入力をエミュレートするための各キーを選択します。押される順にキーを選択します。各キーの選択後に、**[Add Key]** (キーの追加) を選択します。選択した各キーは、**[Macro Sequence]** (マクロ シーケンス) フィールドに表示され、選択するたびに **[Release Key]** (キーをリリース) コマンドが自動的に追加されます。
6. マクロの **[Send Text to Target]** (テキストをターゲットに送信) 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** を選択して、ウィンドウを閉じるマクロを作成します。このマクロは、**[Macro Sequence]** (マクロ シーケンス) ボックスに次のように表示されます。
 - [Press Left Ctrl] (左 **Ctrl** を押す)
 - [Release Left Ctrl] (左 **Ctrl** をリリースする)
 - [Press Esc] (**Esc** を押す)
 - [Release Esc] (左 **Esc** をリリースする)
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、必要に応じて上/下の矢印ボタンをクリックして順序を変更します。
9. **[OK]** をクリックしてマクロを保存します。**[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) ウィンドウが表示され、新しいキーボード マクロのリストが表示されます。
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。これで、アプリケーションの **[Keyboard]** (キーボード) メニューにマクロが表示されます。メニューの新しいマクロを選択して実行するか、マクロに割り当てたキー入力を使用します。



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+O** 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。

ブレード シャーシの切り替えキー シーケンスと一致するホットキーの組み合わせは、それらのシャーシ内のブレードには送信されません。

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。

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氣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場合があります。

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。

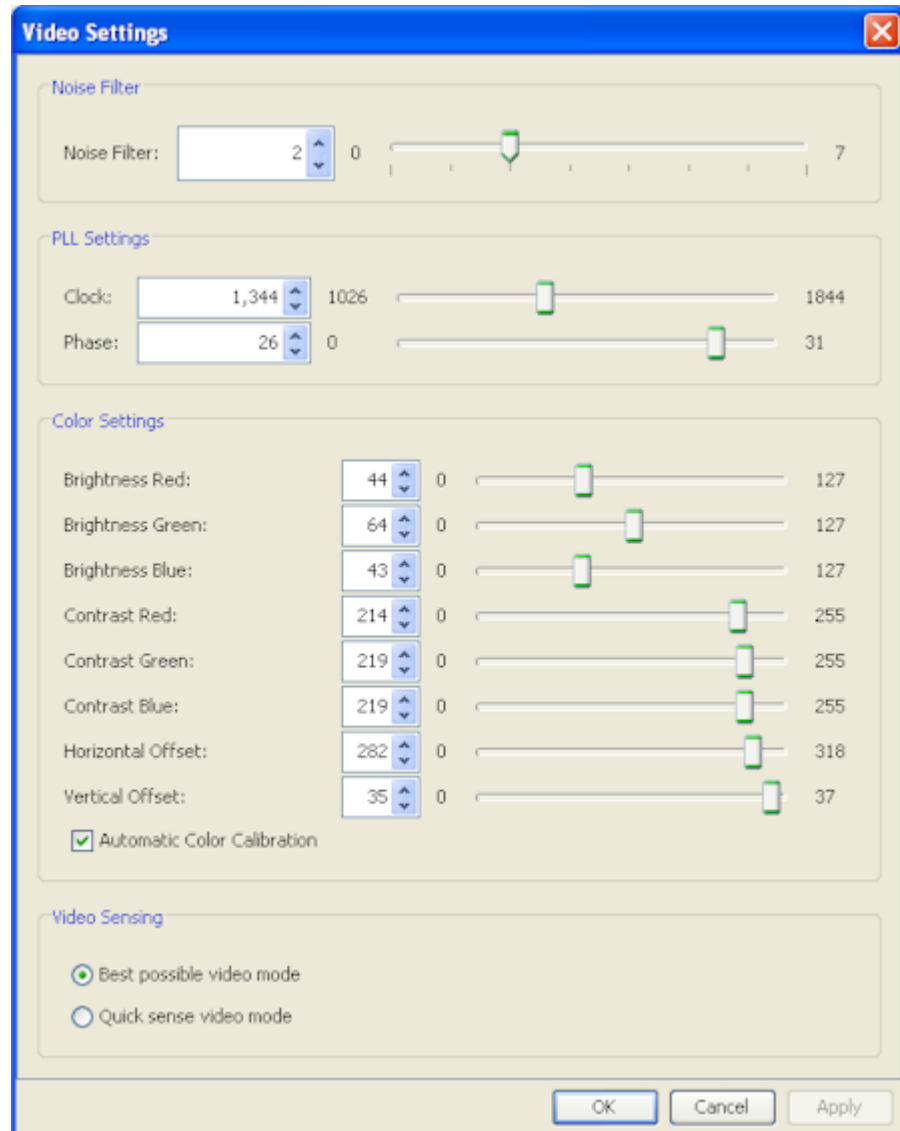
- c. **[Brightness] (明るさ)**: この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。
- d. **[Brightness Red] (赤輝度)** - ターゲット サーバの画面に表示される赤の信号の輝度を制御します。
- e. **[Brightness Green] (緑輝度)** - 緑の信号の輝度を制御します。
- f. **[Brightness Blue] (青輝度)** - 青の信号の輝度を制御します。
- g. **[Contrast Red] (赤コントラスト)** - 赤の信号のコントラストを制御します。
- h. **[Contrast 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。

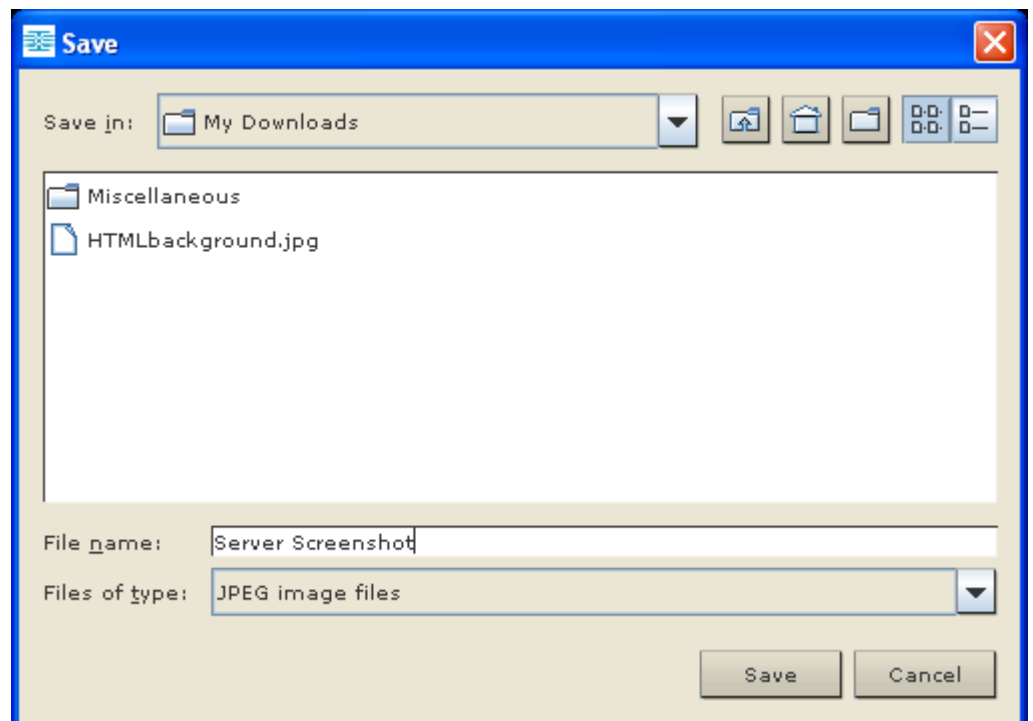


[Screenshot from Target] (ターゲットからのスクリーンショット) を使用する

[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

マウスを使用するターゲット サーバをリモートで表示すると、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 ポインタで、もう 1 つはターゲット サーバのマウス ポインタです。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 接続の場合は、**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されている実際の値が表示されます。
2. **KX II** デバイスの場合は、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. コマンド「`xset mouse 1 1`」を入力します。
 - 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。

[Synchronize Mouse] (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

インテリジェント マウス モードでは、デバイスでターゲットのマウス設定が検出され、それに応じてマウス カーソルが同期されるので、ターゲットでマウスの加速を設定できるようになります。インテリジェント マウス モードは、非 VM ターゲットのデフォルトです。

このモードでは、マウス カーソルが画面の左上隅で "ダンス" をし、加速を計算します。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 システムによって異なります。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。

Absolute (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: ずれないマウス設定を適用するには **USB** ターゲット システムが必要です。KX II-101 の場合、これが推奨のマウス設定です。

*注:*KX II デバイスの場合、ずれないマウス (Absolute Mouse Synchronization) は、仮想メディア対応の **USB CIM (D2CIM-VUSB と D2CIM-DVUSB)** でのみ使用できます。

VKC 仮想メディア

仮想メディアの設定方法および使用方法についての詳細は、「**仮想メディア** 『71p. の"Virtual Media"参照』」を参照してください。

[Tools] (ツール) オプション

[Tools] (ツール) メニューで、Virtual KVM Client 用の特定のオプションを指定できます。このオプションには、ログ作成、キーボードの種類の設定、全画面モードやシングル カーソル モードを終了するホットキーの定義などがあります。

*注:*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ません。

▶ **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. [Tools] (ツール) の [Options] (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、[Enable Logging] (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。

- 英語 (アメリカ)/(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
- 英語 (イギリス)
- 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 - US 英語
- 変換 - フランス語 - US インターナショナル

注:AKC では、キーボードの種類¹のデフォルトがローカル クライアントになる²ので、このオプションは適用されません。

注:KX II-101 は *AKC* をサポートしていません。

4. **[Exit Full Screen Mode]** (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。
5. **[Exit Single Cursor Mode]** (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 カーソルを復活させるホットキーです。[OK] をクリックします。

Client の起動設定

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サイズを定義することができます。

6. **[Client Launch Settings]** (クライアント起動設定) タブを選択します。
 - a. ターゲット ウィンドウ設定をカスタマイズするには

- 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、[Standard - sized to target Resolution] (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。
 - ウィンドウを全画面モードで開くには、[Full Screen] (全画面) を選択します。
 - a. 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
 - 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、[Monitor Client Was Launched from] (クライアントが起動されているモニタ) を選択します。
7. アプリケーションによって現在検出されているターゲット モニタの一覧から選択するには、[Select From Detected Monitors] (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、"Currently Selected Monitor Not Detected" (現在選択されているモニタが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。
8. [OK] をクリックします。

キーボードの制限

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、システム的环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)

言語	設定方法
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。

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。

[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。

[Target Screen Resolution] (ターゲット画面解像度)

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 (デフォルトは **Ctrl+Alt+M** です)。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。**

- [Tools] (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。デフォルトのホット キーは **Ctrl+Alt+M** です。AKC の場合、マウス ポインタを画面上端に移動して、非表示になっているメニュー バーを表示し、[Connection/Exit] (接続/終了) を選択します。

注: KX II-101 は AKC をサポートしていません。

あるいは、常に全画面モードでターゲットにアクセスする場合は、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のモードとして設定するには、以下の手順に従います。**

1. [Tools] (ツール) の [Options] (オプション) をクリックして [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] (全画面モードで開く) を選択して [OK] をクリックします。

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)。

Ch 4

Virtual Media

この章の内容

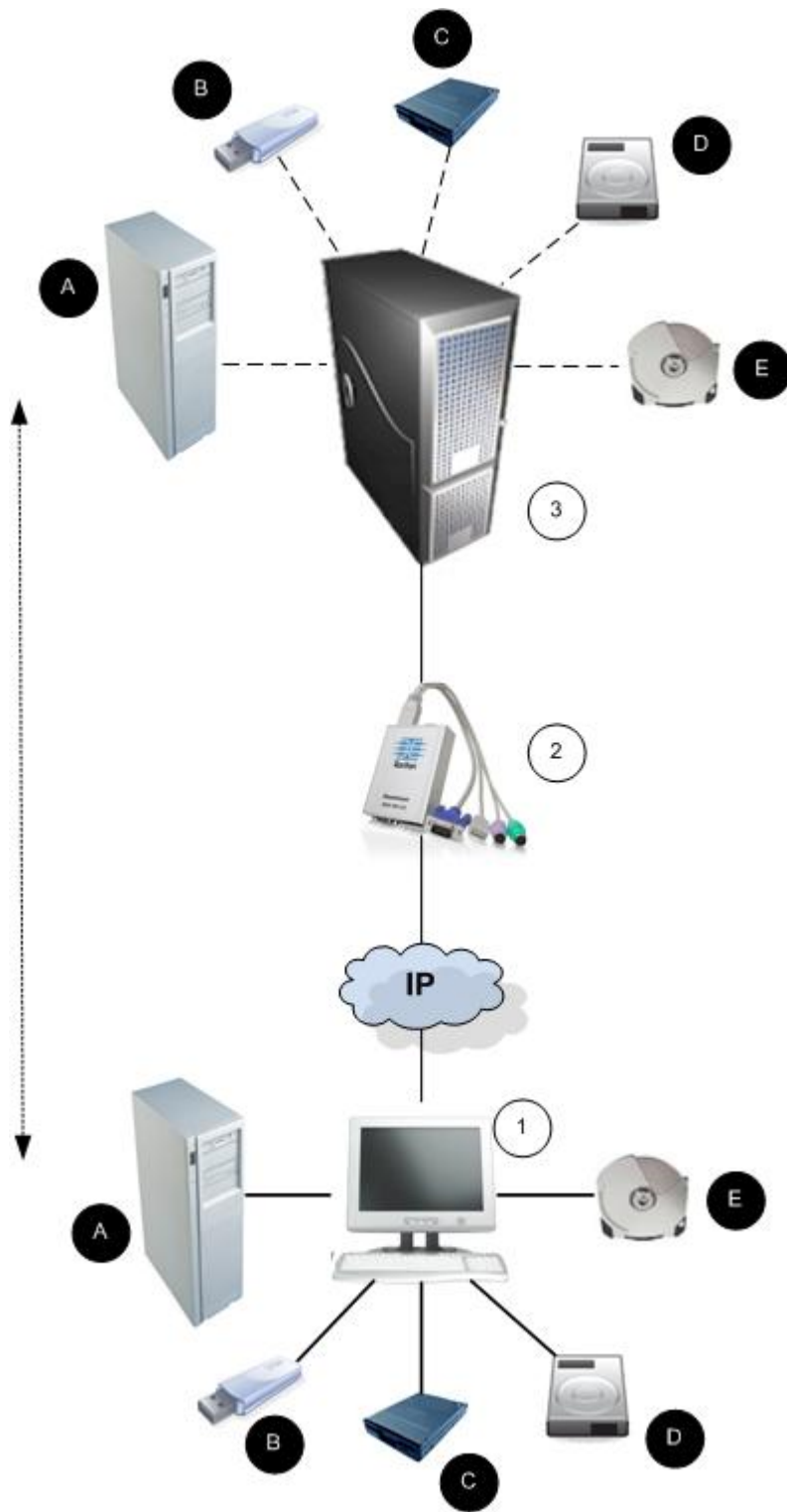
概要.....	72
Prerequisites for Using Virtual Media	74
ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)	75
仮想メディアの使用	76
仮想メディアへの接続.....	77
仮想メディアの切断	81

概要

KVM の機能を拡張する仮想メディアにより、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。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。仮想メディアには、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 のハード ディスク、フロッピー ディスク、ISO イメージ (ディスク イメージ) などを使用できます。

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プログラムの適用
- オペレーティング システムの完全インストール (コンピュータの BIOS でサポートされる場合)
- この拡張 KVM コントロールを利用することで、データ センタに出向く必要がなくなり、時間と費用の節約になります。



注:仮想メディアを使用している場合は、USB 接続を使用する必要があります。

Prerequisites for Using Virtual Media

仮想メディア機能を使用する場合、現在ターゲットに適用されている USB プロファイルでサポートされている異なる種類のドライブを 2 台までマウントできます。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、作業が終了したら切断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。このような仮想メディアの "チャンネル" は、USB プロファイルがサポートしている限り、KVM セッションが閉じられるまで開いたままになっています。

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できるようにするメディアを、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、このメディアにアクセス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。

KX II-101-V2

- For users requiring access to virtual media, the KX II-101-V2 device permissions must be set to allow access to the relevant ports, as well as virtual media access (VM Access port permission) for those ports. Port permissions are set at the group-level.
- If you want to use PC-Share, Security Settings must also be enabled in the Security Settings page. **Optional**

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 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 が稼動する 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 ポートの方が高速なため、推奨されます。
- ▶ **仮想メディアを使用するには、以下の手順に従います。**
- ターゲット サーバからアクセスできるようにするメディアを、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する前に行う必要があります。

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 拡張も動作します。

*注:*ファイル サーバで SMB/CIFS がサポートされている必要があります。

[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、[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 [Remote Server ISO Image Hostname] (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 リストの選択肢として表示されます。詳細については、「**CD-ROM/DVD-ROM/ISO イメージ**」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。
 - [Host Name/IP Address] (ホスト名/IP アドレス) - ファイル サーバのホスト名または IP アドレス。
 - [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:ホスト名の長さは、232 文字以内にする必要があります。

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す。

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。

仮想メディアの使用

仮想メディアを使用する前に「**仮想メディアを使用するための前提条件** 『74p. の"Prerequisites for Using Virtual Media"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 [File Server Setup] (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。「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)」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 [Port Access] (ポート アクセス) ページを開きます。
 - b. [Port Access] (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。
 - [Port Action] (ポート アクション) メニューの [Connect] (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	この VM オプションを選択
ローカル ドライブ	[Local Drives] (ローカル ドライブ)
ローカル CD/DVD ドライブ	CD-ROM/DVD-ROM/ISO イメージ
ISO イメージ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)
ファイル サーバ ISO イメージ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)

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『81p.』](#)」を参照してください。

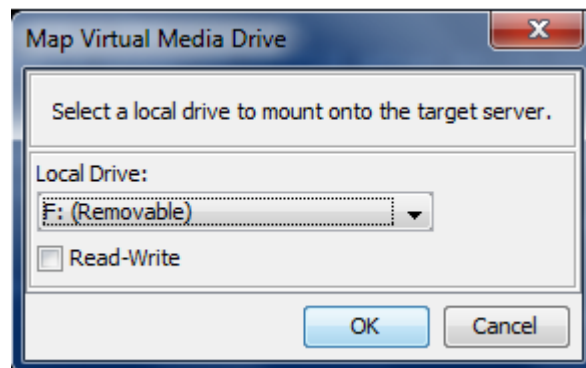
仮想メディアへの接続

ローカル ドライブ

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。

▶ 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 『78p.』**」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. [Connect] (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。

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。

- 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。

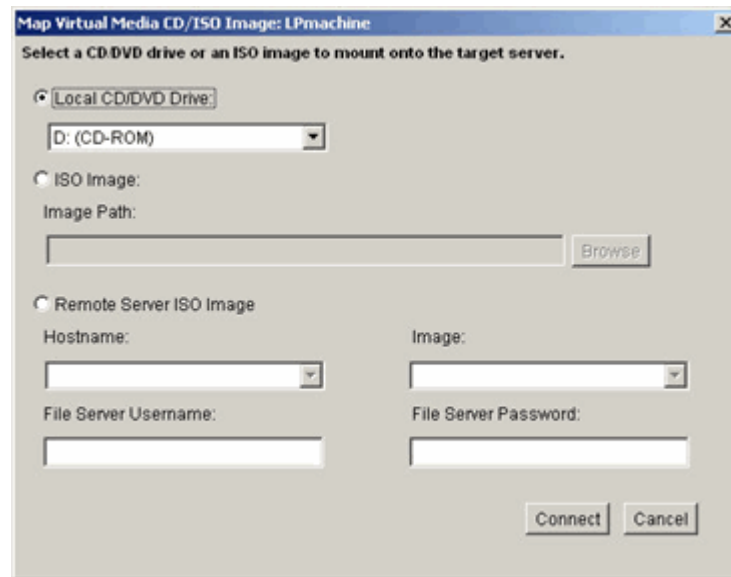
CD-ROM/DVD-ROM/ISO イメージ

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、[Virtual Media] (仮想メディア) の [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続) を選択します。[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. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) を選択します。
 - b. [Local CD/DVD Drive] (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. [Connect] (接続) をクリックします。
3. ISO イメージの場合

- a. **[ISO Image]** (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. **[Browse]** (参照) ボタンをクリックします。
 - 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、**[Open]** (開く) をクリックします。パスが **[Image Path]** (イメージのパス) フィールドに入力されます。
 - d. **[Connect]** (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. **[Remote Server ISO Image]** (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、**[File Server Setup]** (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。**[File Server Setup]** (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. **[File Server Username]** (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。この名前には、**mydomain/username** のようなドメイン名を含めることができます。
 - d. **[File Server Password]** (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. **[Connect]** (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® ターゲットのファイルを操作している場合は、仮想メディアを使用してファイルがコピーされた後に **Linux** の同期 (**sync**) コマンドで、コピーされたファイルを表示します。同期が実行されるまでファイルは表示されません。

注:Windows 7® オペレーティング システム® を使用している場合は、ローカル **CD/DVD** ドライブまたはローカル/リモート **ISO** イメージをマウントしても、デフォルトでは **Windows** の **[マイ コンピュータ]** フォルダにリムーバブル ディスクは表示されません。このフォルダにローカル **CD/DVD** ドライブまたはローカル/リモート **ISO** イメージを表示するには、**[ツール]**、**[フォルダ オプション]**、**[表示]** の順に選択し、**[空のドライブは [コンピューター] フォルダーに表示しない]** の選択を解除します。

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。

この章の内容

ユーザ グループ	82
ユーザ	89
[Authentication Settings] (認証設定)	92
パスワードの変更	105

ユーザ グループ

すべての KX II-101-V2 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-101-V2 内では最大 254 個のユーザ グループを作成できます。

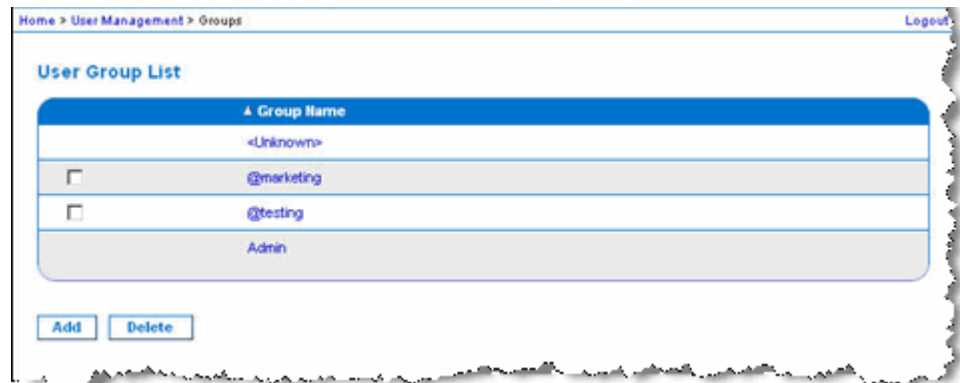
[User Group List] (ユーザ グループ リスト)

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。

[User Group List] (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、[Group Name] (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。[User Group List] (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。

- [User Management] (ユーザ管理) の [User Group List] (ユーザ グループ リスト) を選択します。[User Group List] (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-101-V2 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 グループを追加する

▶ 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. [User Management] (ユーザ管理) の [Add New User Group] (ユーザグループを新規に追加) を選択するかまたは [User Group List] (ユーザグループ一覧) ページの [Add] (追加) ボタンをクリックして、[Group] (グループ) ページを開きます。

[Group] (グループ) ページには、[Group] (グループ)、[Permissions] (権限)、[Port Permissions] (ポート使用権限)、[IP ACL] の 4 つのカテゴリがあります。

2. [Group Name] (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. グループの権限を設定します。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。

Home > User Management > Group

Group

Group Name *

▼ Permissions

Device Settings
 Diagnostics
 Maintenance
 PC-Share
 Security
 User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
1: Dominion_KX2_101_Port1	Deny	Deny	Deny
2: Power Port 1	Deny		Deny

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append Insert Replace Delete

OK Cancel

© 2008 Raritan, Inc.

ポート許可の設定

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

オプションで 説明
す。

[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。

VM アクセス

オプションで 説明
す。

[Deny] (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。
[Read-Only] (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。
[Read-Write] (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

オプションで説明
す。

[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。

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-101-V2** 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-101-V2 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-101-V2** 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。

The screenshot shows a web interface for configuring IP ACL rules. At the top, there is a blue header with a dropdown arrow and the text 'IP ACL'. Below this is a table with four columns: 'Rule #', 'Starting IP', 'Ending IP', and 'Action'. The 'Action' column contains a dropdown menu currently set to 'ACCEPT'. Below the table are four buttons: 'Append', 'Insert', 'Replace', and 'Delete'. At the bottom of the form are 'OK' and 'Cancel' buttons.

▶ 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-101-V2 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-101-V2 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で挿入するには

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。

許可の設定

重要:[User Management] (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 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
[Diagnostics] (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-101-V2 診断
メンテナンス	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
[PC-Share] (PC 共有)	複数のユーザーによる同一ターゲットへの同時アクセス
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

個別グループの許可を設定する

▶ **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。

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. [Group] (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」を参照してください。
3. [Port Permissions] (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」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-101-V2 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)」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 <Unknown (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. [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。

ユーザ

ユーザが KX II-101-V2 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-101-V2 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。

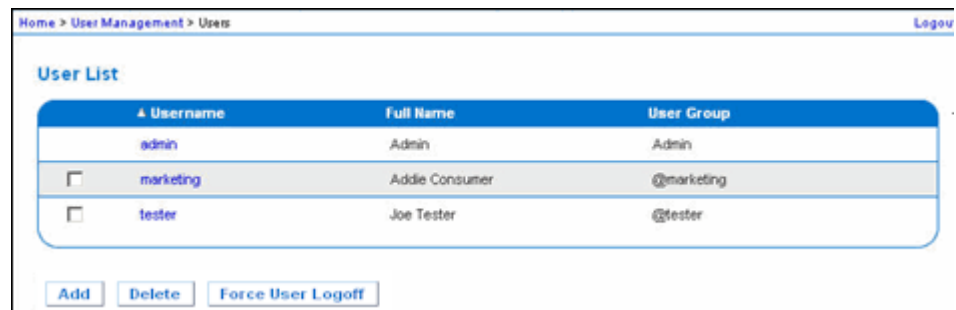
[User List] (ユーザ リスト)

[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、または削除することもできます。

▶ 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。



新規ユーザを追加する

KX II-101-V2 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。この理由は、ユーザを追加するときに、その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ためです。詳細については、「新規ユーザ グループを追加する」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。詳細については、「セキュリティ設定」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. [User Management] (ユーザ管理) の [Add New User] (新規ユーザの追加) を選択するか、[User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックして、[User] (ユーザ) ページを開きます。
2. [Username] (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. [Full Name] (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. [Password] (パスワード) フィールドにパスワードを入力し、[Confirm Password] (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. [User Group] (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。このリストには、システムによって定義されているデフォルト グループに加えて、ユーザによって作成されたグループを含むすべてのグループが表示されます。デフォルト グループは、デフォルト設定である [Unknown] (不明)、[Admin] (管理者)、[Individual Group] (個別グループ) です。
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」を参照してください。
6. 新規ユーザを有効にするには、[Active] (アクティブ) チェックボックスをオンにします。デフォルトはアクティブ状態 (有効) です。
7. [OK] (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** 『90p. の"新規ユーザを追加する"参照』」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。

ユーザ ブロックとブロック解除

システムへのユーザのアクセスは、管理者により、またはセキュリティ設定を基に自動的にブロックできます。詳細については、「**[User Blocking] (ユーザ ブロック)** 『144p. 』」を参照してください。ブロックされたユーザは非アクティブになり、管理者が再びアクティブにすることでブロック解除できます。

▶ **ユーザをブロックまたはブロック解除するには、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) を選択します。[User List] (ユーザ リスト) ページが開きます。
2. [Active] (アクティブ) チェックボックスをオンまたはオフにします。
 - オンにした場合、ユーザはアクティブになり、KX II-101-V2 にアクセスできます。
 - オフにした場合、ユーザは非アクティブになり、KX II-101-V2 にアクセスできません。
3. [OK] をクリックします。ユーザのアクティブ ステータスが更新されます。

[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-101-V2 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。

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. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) を選択します。[Authentication Settings] (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 ([Local Authentication] (ローカル認証)、[LDAP/LDAPS] (LDAP/LDAPS)、または [RADIUS] (RADIUS))。[LDAP] (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] (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. [Local Authentication] (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] (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、[Authentication Settings] (認証設定) ページの [LDAP] (LDAP) セクションの各フィールドを指定してください。
5. [RADIUS] (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、[Authentication Settings] (認証設定) ページの [RADIUS] (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。**

- **[Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。**

LDAP/LDAPS リモート認証を実装する

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クング 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 Directory 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お問い合わせください。
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お問い合わせください。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)。

Authentication Settings

- Local Authentication
 LDAP
 RADIUS

LDAP

Server Configuration

Primary LDAP Server

Secondary LDAP Server (optional)

Type of External LDAP Server

Active Directory Domain

User Search DN

DN of Administrative User (optional)

Secret Phrase of Administrative User

Confirm Secret Phrase

LDAP/Secure LDAP

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-101-V2 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、[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。[Browse] (参照) ボタン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-101-V2 を再起動する必要があります。

LDAP / Secure LDAP

Enable Secure LDAP

Port

Secure LDAP Port

Enable LDAPS Server Certificate Validation

Root CA Certificate File

Note: Reboot device after certificate file is uploaded.

テスト LDAP サーバ アクセス

17. LDAP サーバおよび KX II-101-V2 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-101-V2 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-101-V2 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。

The screenshot shows a dialog box titled "Test LDAP Server Access". Inside the dialog, there are two text input fields. The first is labeled "Login for testing" and the second is labeled "Password for testing". Below these fields is a button labeled "Test".

ユーザ グループ情報を Active Directory サーバから返す

KX II-101-V2 では、ユーザを KX II-101-V2 でローカルに定義しなくても、Active Directory® (AD) へのユーザ認証がサポートされます。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-101-V2 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は、KX II-101-V2 で引き続きこの設定がサポートされます。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については、「LDAP スキーマの更新『193p. の"Updating the LDAP Schema"参照』」を参照してください。

▶ **KX II-101-V2 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-101-V2 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、KVM_Operator などの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-101-V2 ユーザを割り当てます。
4. KX II-101-V2 で、AD サーバを有効にし、適切に設定します。「LDAP/LDAPS リモート認証を実装する」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-101-V2 には、変更も削除もできないデフォルトのグループとして [Admin] (管理者) および [<Unknown>] (不明) が用意されています。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-101-V2 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 [<Unknown>] (不明) グループが割り当てられます。

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)、アカウントिंग (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-101-V2 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]** (アカウントティング 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-101-V2 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-101-V2 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。

Home > User Management > Authentication Settings

Authentication Settings

Local Authentication
 LDAP
 RADIUS

▶ LDAP

▼ RADIUS

Primary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Secondary RADIUS Server

Shared Secret

Authentication Port

Accounting Port

Timeout (in seconds)

Retries

Global Authentication Type
PAP ▼

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-101-V2 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。

RADIUS 通信交換仕様

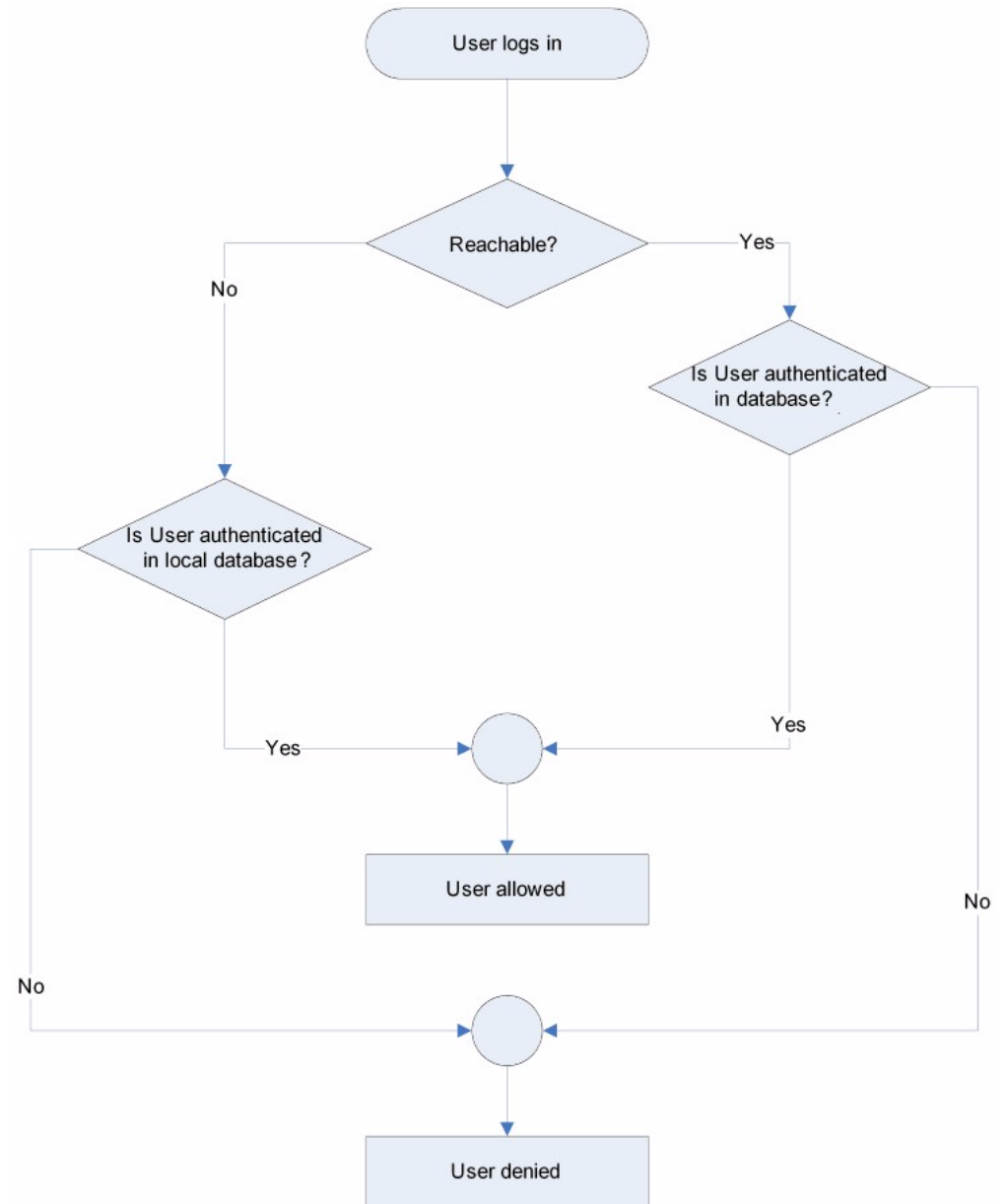
KX II-101-V2 は、以下の RADIUS 属性を RADIUS サーバに送信します。

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-101-V2 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)	アカウント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) - アカウント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-101-V2 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)	アカウントティングのセッション ID
ログアウト	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - アカウント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)

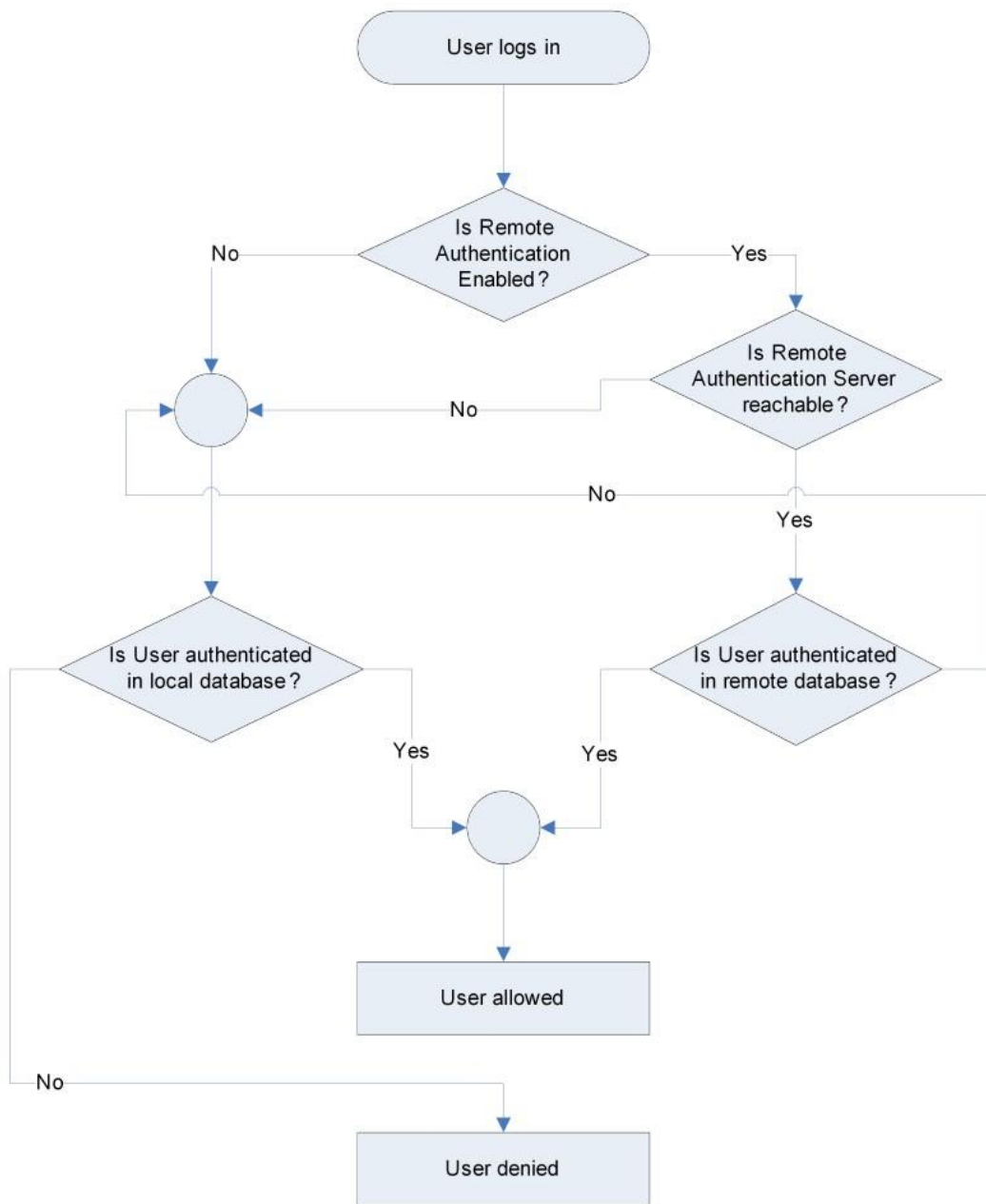
属性	データ
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX II-101-V2 の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウントティングのセッション ID

ユーザ認証プロセス

ローカル ユーザを認証および認可するようにデバイスが設定されている場合、ユーザ資格情報の検証順序は、以下のプロセスに従います。



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)**』142p.』を参照してください。

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK

Cancel

この章の内容

[Network Settings] (ネットワーク設定).....	106
[Device Services] (デバイス サービス).....	109
キーボード/マウス設定.....	112
[Serial Port Settings] (シリアル ポート設定).....	113
日付/時刻の設定	116
イベント管理	117
[Port Configuration] (ポート設定).....	123
アナログ KVM スイッチ	132
リセット ボタンを使用して KX II-101-V2 をリセットする.....	134

[Network Settings] (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-101-V2 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-101-V2 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**『107p. 』」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**『109p. 』」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

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. 最大 32 文字の英数字と有効な特殊文字 (スペースなし) を組み合わせて、KX II-101-V2 デバイスにわかりやすいデバイス名を指定します。
3. [IPv4 Address] (IPv4 アドレス) セクションで、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。

注:ホスト名の推奨最大長は 80 文字です。

- 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-101-V2 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ため、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 80 文字まで使用できます。
4. [DHCP] (DHCP) が選択されており、[Obtain DNS Server Address] (DNS サーバ アドレスを取得する) 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する) 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する) を選択した場合は、DHCP サーバから得られた DNS 情報が使用されます。

5. [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用する) が選択されている場合は、[DHCP] (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したアドレスを使用して DNS サーバに接続されます。

[Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用する) が選択されている場合は、以下の情報を入力します。これらのアドレスは、停電のためにプライマリ DNS サーバ接続が失われた場合に使用されるプライマリおよびセカンダリの DNS アドレスです。

- a. プライマリ DNS サーバ IP アドレス
 - b. セカンダリ DNS サーバ IP アドレス
6. 完了したら [OK] をクリックします。これで、KX II-101-V2 からネットワークにアクセスできるようになります。

Basic Network Settings

Device Name *
DKX2-101-V2

IPv4 Address

IP Address	Subnet Mask
192.168.51.101	255.255.255.0
Default Gateway	Preferred DHCP Host Name
192.168.51.126	

IP Auto Configuration
None ▼

Obtain DNS Server Address Automatically

Use the Following DNS Server Addresses

Primary DNS Server IP Address
192.168.51.10

Secondary DNS Server IP Address
192.168.50.114

OK Reset To Defaults Cancel

LAN インタフェース設定

現在のパラメータ設定は、[Current LAN interface parameters] (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。

- [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) 設定を選択します。
 - 自動検出 (デフォルトのオプション)
 - [10 Mbps/Half] (10 Mbps/半二重) - 黄色の LED が点滅
 - [10 Mbps/Full] (10 Mbps/全二重) - 黄色の LED が点滅
 - [100 Mbps/Half] (100 Mbps/半二重) - 黄色の LED が点滅し、緑色の LED が常時点灯
 - [100 Mbps/Full] (100 Mbps/全二重) - 黄色の LED が点滅し、緑色の LED が常時点灯

[Half-duplex] (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)。

[Full-duplex] (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、別の速度と二重化を選択してください。

詳細については、「**ネットワーク速度の設定** 『191p. の"Network Speed Settings"see 』」を参照してください。

- [Bandwidth Limit] (帯域幅の制限) を選択します。
 - [No Limit] (制限なし)
 - [512 Kilobit] (128 キロビット)
 - [512 Kilobit] (256 キロビット)
 - [512 Kilobit] (512 キロビット)
 - [2 Megabit] (100 メガビット)
 - [5 Megabit] (100 メガビット)
 - [10 Megabit] (100 メガビット)
 - [100 Megabit] (100 メガビット)

新しいスクリーンショットが必要

[Device Services] (デバイス サービス)

[Device Services] (デバイス サービス) ページでは、以下のことができます。

- SSH アクセスを有効にする。
- 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。

Telnet を有効にする

Telnet を使用して KX II-101-V2 に接続したい場合、まず、CLI またはブラウザを使用して KX II-101-V2 に接続します。

▶ Telnet 接続を有効にするには

1. [Device Settings] (デバイス設定) を選択し、[Enable TELNET Access] (TELNET アクセスを有効にする) チェックボックスを選択します。
2. Telnet ポートを入力します。
3. [OK] をクリックします。

Telnet 接続が有効になったら、Telnet を使用して KX II-101-V2 に接続し、他のパラメータ値を設定することができます。

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-101-V2 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。

検出ポートを入力する

KX II-101-V2 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-101-V2 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。

URL を介してダイレクト ポート アクセスを有効にする

ダイレクト ポート アクセスにより、ユーザは、デバイスの [Login] (ログイン) ダイアログ ボックスおよび [Port Access] (ポート アクセス) ページを使用しなくても済むようになります。この機能では、URL でユーザ名とパスワードが指定されていない場合に、ユーザ名とパスワードを直接入力してターゲットに進むこともできます。

以下に、ダイレクト ポート アクセスに関する重要な URL 情報を示します。

VKC およびダイレクト ポート アクセスを使用している場合:

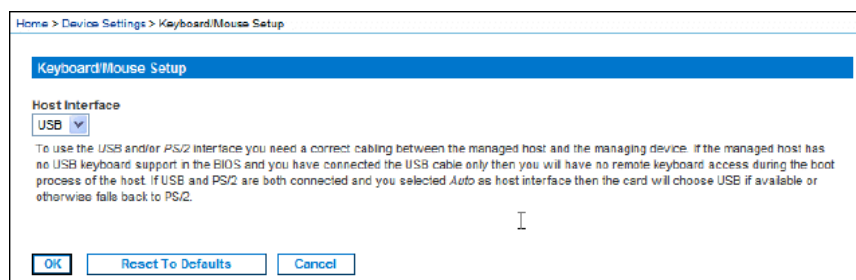
- <https://IPAddress/dpa.asp?username=username&password=password&port=port number>

▶ 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。

キーボード/マウス設定

[Keyboard/Mouse Setup] (キーボード/マウス設定) ページを使用して、KX II-101-V2 とホスト デバイス間のキーボードおよびマウス インタフェースを設定します。



1. [Device Settings] (デバイスの設定) の [Keyboard/Mouse] (キーボード/マウス)をクリックします。
2. [Host Interface] (ホスト インタフェース) を選択します。この選択によって、KX II-101-V2 でキーボード データやマウス データを PS/2 接続を介して送信するか、USB 接続を介して送信するかが決定されます。
 - [Auto] (自動) - この設定では、KX II-101-V2 で使用可能な場合は USB 接続が使用され、そうでない場合は、PS/2 接続がデフォルトに設定されます。
 - [USB] (USB) - この設定では、KX II-101-V2 で USB 接続を使用して、キーボード データやマウス データがホスト デバイスに送信されます。
 - [PS/2] (PS/2) - この設定では、KX II-101-V2 で PS/2 接続を使用して、キーボード データやマウス データがホスト デバイスに送信されます。

注:KX II-101-V2 を搭載したフロントエンドで Raritan スイッチを使用している場合は、正しく機能する設定となるように [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定する必要があります。詳細については、「アナログ KVM スイッチ 『132p.』」を参照してください。

3. [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。

[Serial Port Settings] (シリアル ポート設定)

[Serial Port Settings] (シリアル ポート設定) ページを使用して、KX II-101-V2 の内蔵シリアルポートの使用方法を設定します。

管理ポート

▶ **管理シリアル ポートを設定するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Serial Port] (シリアル ポート) を選択します。[Serial Port Settings] (シリアル ポート設定) ページが表示されます。
2. [Admin Port] (管理ポート) ラジオ ボタンを選択します。
3. いずれかのオプションを選択して、クライアント PC から KX II-101-V2 に直接接続したり、ハイパーターミナルのようなプログラムによってコマンドライン インタフェースにアクセスしたりします。詳細については、「**コマンド ライン インタフェース (CLI) 『170p.』**」を参照してください。
4. [Serial Settings] (シリアル設定) セクションで、以下のフィールドを設定します。
 - [Speed] (速度)
 - [Stop Bits] (ストップ ビット)
 - [Data Bits] (データ ビット)
 - [Handshake] (ハンドシェイク)
 - [Parity] (パリティ)
5. [OK] をクリックします。

Raritan の電源タップ制御

▶ **電源タップ シリアル ポートを設定するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Serial Port] (シリアル ポート) を選択します。[Serial Port Settings] (シリアル ポート設定) ページが開きます。
2. [PowerStrip Control] (電源タップ制御) ラジオ ボタンを選択します。Raritan の電源タップに KX II-101-V2 を接続する場合は、このオプションを選択します。
3. [OK] をクリックします。

モデム

▶ **モデム シリアル ポートを設定するには、以下の手順に従います。**

1. **[Device Settings]** (デバイス設定) の **[Serial Port]** (シリアル ポート) を選択します。**[Serial Port Settings]** (シリアル ポート設定) ページが開きます。
2. **[Modem]** (モデム) ラジオ ボタンを選択します。ダイヤルアップ アクセスを提供するために外部モデムを **KX II-101-V2** に接続する場合は、このオプションを選択します。
3. **[Modem Settings]** (モデム設定) セクションで、以下のフィールドを設定します。
 - **[Serial line speed]** (シリアル ライン速度)
 - **[Modem init string]** (モデム init 文字列) - モデム アクセスを有効にするは、フィールドに表示されるデフォルトの文字列を使用する必要があります。
 - **[Modem server IP address]** (モデム サーバ IP アドレス) - モデムを介して接続した後に、ユーザが **KX II-101-V2 Web** インタフェースにアクセスするために入力するアドレスです。
 - **[Modem client IP address]** (モデム クライアント IP アドレス) - モデムを介して接続した後にユーザに割り当てられるアドレスです。

4. [OK] をクリックします。

Home > Device Settings > Serial Port Settings

Serial Port Settings

Admin Port
 Powerstrip Control
 Modem

Modem Settings:

Serial line speed
 115200 bits/s

Modem init string
 ATZHO OK ATL0M0&K3X1 OK

Modem server IP address
 192.168.3.1

Modem client IP address
 192.168.3.2

モデム アクセス用のケーブル接続の詳細については、「**モデム アクセス ケーブル接続** 『115p.』」を参照してください。また、KX II-101-V2 で機能する認定モデムの詳細については、「**Certified Modems (認定モデム)** 『188p. の"認定モデム"参照』」を参照してください。モデムを介して KX II-101-V2 に接続する場合に最高のパフォーマンスが得られる設定については、『**KVM およびシリアル アクセス クライアント ユーザ ガイド**』の「**Creating, Modifying and Deleting Profiles in MPC (MPC でプロファイルを作成、変更、および削除する)**」を参照してください。

モデム アクセス ケーブル接続

以下のケーブル接続設定を使用して、KX II-101-V2 をモデムに接続します。

1. 管理シリアル ケーブルを KX II-101-V2 に接続します。

2. 9 ピンのオス/オス変換アダプタを管理シリアル ケーブルに接続します。
3. 変換アダプタの反対側にヌル モデム ケーブルを接続します。
4. 9 ピンのオス/オス変換アダプタをヌル モデム ケーブルの反対側に接続します。
5. ヌル モデム ケーブルとモデムの間に DB9 - DB25 (オス) モデム ケーブルを接続します。

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-101-V2 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. [Device Settings] (デバイス設定) の [Date/Time] (日付/時刻) を選択します。[Date/Time Settings] (日付/時刻の設定) ページが開きます。
2. [Time Zone] (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、[Adjust for daylight savings time] (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。
 - [User Specified Time] (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。
[User Specified Time] (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)。
 - [Synchronize with NTP Server] (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. [Synchronize with NTP Server] (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. [Primary Time server] (プライマリ タイム サーバ) の IP アドレスを入力します。
 - b. [Secondary Time server] (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。

Home > Device Settings > Date/Time Settings

Date/Time Settings

Time Zone
(GMT -05:00) US Eastern

Adjust for daylight savings time

User Specified Time

Date (Month, Day, Year)
May 09, 2008

Time (Hour, Minute)
10 18

Synchronize with NTP Server

Primary Time server

Secondary Time server

イベント管理

KX II-101-V2 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。

Configuring Event Management - Settings

SNMP 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。KX II-101-V2 では、イベント管理を通じて SNMP エージェントがサポートされます。

▶ **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. [SNMP Logging Enabled] (SNMP ログを有効にする) を選択します。これにより、残りの SNMP フィールドが有効になります。
3. [Name] (名前) フィールドには、KX II-101-V2 コンソール インタフェースに表示されているとおりに SNMP エージェントの名前 (つまりデバイスの名前) を、[Contact] (連絡先) フィールドには、このデバイスに関連する連絡先名を、[Location] (所在地) フィールドには、Dominion デバイスが物理的に設置されている場所を入力します。
4. [Agent Community String] (エージェント コミュニティの文字列) (デバイスの文字列) を入力します。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ションが所属するグループのことです。SNMP コミュニティは、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、グループを識別するために使用されます。SNMP デバイスや SNMP エージェントは、複数の SNMP コミュニティに所属できます。
5. [Type] (タイプ) ドロップダウン リストを使用して、コミュニティに [Read-Only] (読み取り専用) または [Read-Write] (読み取り/書き込み可能) を指定します。
6. [Destination IP/Hostname] (送信先 IP/ホスト名)、[Port #] (ポート番号)、[Community] (コミュニティ) を指定して、最大で 5 つの SNMP マネージャを設定します。
7. [Click here to view the Dominion SNMP MIB] (Dominion SNMP MIB を表示するにはここをクリックします) というリンクをクリックして、SNMP Management Information Base にアクセスします。
8. [OK] をクリックします。

▶ **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/ホスト名を入力します。
3. [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。

[Event Management - Destinations] (イベント管理 - 送信先)

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、追跡するシステム 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。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。詳細については、『118p. の"Configuring Event Management - Settings"参照』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イベント ラインのアイテムのチェックボックスと、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) 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] をクリックします。

Home > Device Settings > Event Management - Destinations Logout

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit Log
Device Operation	System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	System Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Power Supply Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Powerstrip Outlet Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Parameter Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Status Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Network Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Ethernet Failover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Management		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Management	FactoryReset	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Begin CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	End CC Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Started	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Completed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Device Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Update Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware File Discarded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Firmware Validation Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Backed Up	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Configuration Restored	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Connection Denied	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	Password Settings Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Login Failed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Password Changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	User Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
User Activity	Port Connected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Port Disconnected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

▶ 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-101-V2 を再起動したときに KX II-101-V2 と接続先のルータが同期しなくなり、再起動完了の SNMP トラップがログ記録されなくなるおそれがあります。

SNMP エージェント設定

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-101-V2 (SNMP エージェント) と SNMP マネージャとの間の SNMP 接続を設定するには、イベント ログ ページを使用します。

SNMP トラップ設定

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-101-V2 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。 <i>注: KX II-101 ではサポートされていません。</i>
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-101-V2 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-101-V2 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-101-V2 システムに追加されました。

トラップ名	説明
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。
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。
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-101-V2 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-101-V2 は再起動を開始しました。
securityViolation	セキュリティ違反です。
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

トラップ名	説明
	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-101-V2 へ正常にログインし、認証されました。
userLogout	ユーザが KX II-101-V2 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。
vmlImageConnected	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。
vmlImageDisconnected	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。

[Port Configuration] (ポート設定)

[Port Configuration] (ポート設定) ページには、KX II-101-V2 のポートの一覧が表示されます。KVM ターゲット サーバまたはパワー ストリ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。

▶ **ポート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 [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。

並べ替える

当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 Name]** (ポート名) - ポートに割り当てられている名前です。ポート名が黒色で表示されている場合は、名前の変更およびポートの編集はできません。ポートが青色で表示されている場合は、編集できます。

注:ポート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) - ポートに接続されているターゲットのタイプです。

ポート タイプ	説明
PowerStrip	電源タップ/PDU
KVM	KVM ターゲット

▶ **ポート名を編集するには、次の手順に従います。**

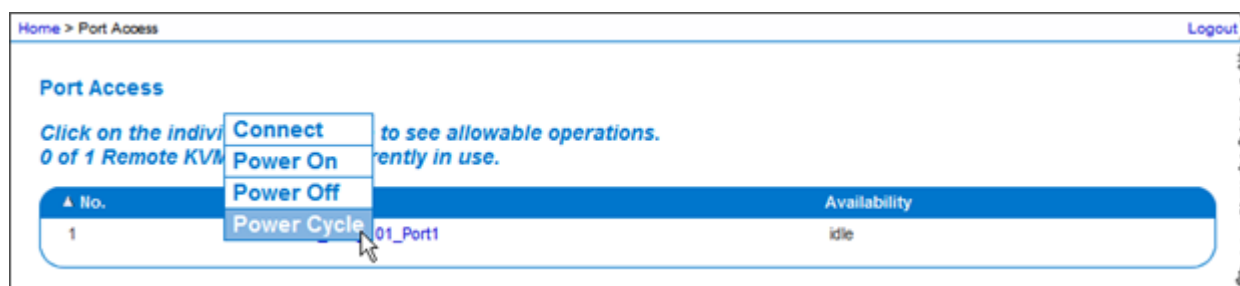
1. 編集するポートの **[Port Name]** (ポート名) をクリックします。
 - KVM ポートの場合は、**[Port]** (ポート) ページが開きます。このページで、ポートに名前を付け、電源を関連付けて、ターゲット サーバ設定を設定します。
 - 電源タップの場合は、電源タップの **[Port]** (ポート) ページが開きます。このページで、電源タップとそのコンセントに名前を付けることができます。詳細については、「**電源制御**『127p. の "**Power Control**"参照先』」を参照してください。

注:[Power Port 1] (パワー ポート 1) リンクは、Raritan の電源タップを KX II-101-V2 に接続し、設定している場合にのみ有効です。そうでない場合、このリンクは無効です。

KVM ターゲット サーバを管理する ([Port] (ポート) ページ)

[Port Configuration] (ポート設定) ページで、ターゲット サーバに接続しているポートを選択すると、この [Port] (ポート) ページが開きます。このページで、電源の関連付けを実行したり、ポート名をわかりやすい名前に変更したりすることができます。

サーバには電源プラグを最大 4 つ接続でき、それぞれを電源タップに関連付けることができます。このページで、これらの関連付けを定義して、以下に示すように [Port Access] (ポート アクセス) ページからサーバの電源の投入、切断、再投入を行えます。



注: この機能を使用するには、Raritan Dominion PX パワー ストリップをデバイスに接続しておく必要があります。詳細については、「電源タップを接続する」を参照してください。

▶ 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。
2. 編集するポートの [Port Name] (ポート名) をクリックします。

注: [Power Port 1] (パワー ポート 1) リンクは、Raritan の電源タップを KX II-101-V2 に接続し、設定している場合にのみ有効です。そうでない場合、このリンクは無効です。

ポートの名前を変更する

▶ ポート名を変更するには、以下の手順に従います。

1. ターゲット サーバの名前など、わかりやすい名前を入力します。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: ポート名にアポストロフィを使用することはできません。

2. [OK] をクリックします。

有効な特殊文字

ホトヲヨ	説明	ホトヲヨ	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		

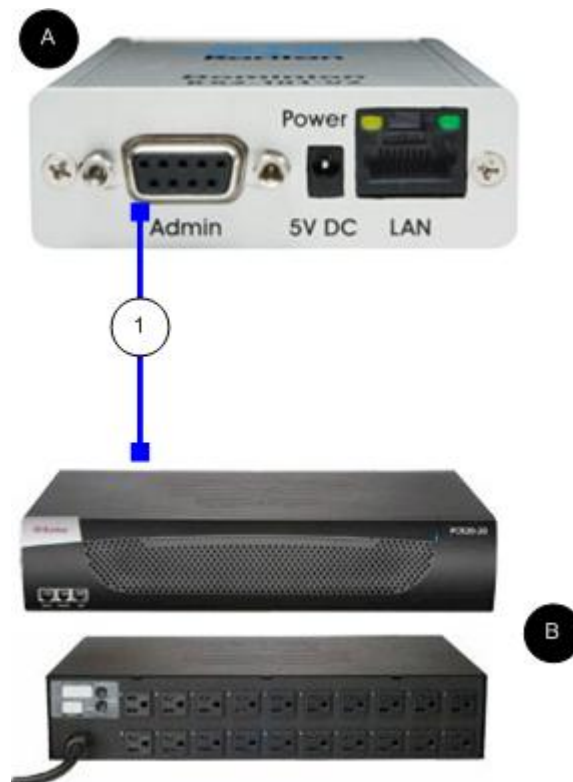
Power Control

The KX II-101-V2 provides remote power control of a target server. To utilize this feature, you must have a Raritan remote power strip.

▶ To use the KX II-101-V2 power control feature:

- Connect the power strip to your target server using the DKX2-101-SPDUC connector (not included but available from your reseller or Raritan). See Connecting the Power Strip.
- Name the power strip (not included but available from your reseller or Raritan. See **Naming the Power Strip (Port Page for Power Strips)** 『129p. の"電源タップに名前を付ける (電源タップの [Port] (ポート) ページ)see 』.
- Associate outlet in the power strip to the target server. See **Managing KVM Target Servers (Port Page)** 『125p. の"KVM ターゲット サーバを管理する ([Port] (ポート) ページ)see 』.
- Turn the outlets on the power strip on and off in the Power Strip Device page. See Controlling a Power Strip Device.

電源タップを接続する



図の説明	
	KX II-101-V2
	Raritan パワー ストリップ。
	KX II-101-V2 から Raritan の電源タップまでの DKX2-101-SPDUC コネクタ (別売)

▶ **KX II-101-V2 を Raritan パワー ストリップを接続するには、以下の手順に従います。**

1. DKX2-101-SPDUC ケーブルのミニ DIN9M コネクタを KX II-101-V2 の Admin ポートに接続します。
2. DKX2-101-SPDUC ケーブルの RJ45M コネクタを Raritan パワー ストリップのシリアル ポート 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、パワー ストリップの空いているパワー ストリップ コンセントに接続します。
4. パワー ストリップを AC 電源に接続します。
5. Raritan パワー ストリップの電源をオンにします。
6. [Device Settings] (デバイスの設定) の [Serial Port] (シリアル ポート) をクリックして、[Serial Port] (シリアル ポート) ページを開きます。
7. [Power Strip Control] (電源タップ制御) ラジオ ボタンを選択して、[OK] をクリックします。この操作を完了したら、リモート コンソールで [Power] (電源) メニューを利用できるようになります。

電源タップに名前を付ける (電源タップの [Port] (ポート) ページ)

KX II-101-V2 が Raritan のリモート電源タップに接続されたら、[Port] (ポート) ページにポートが表示され、[Port] (ポート) 設定ページからそのポートを開くことができます。[Type] (タイプ) フィールドと [Name] (名前) フィールドには、あらかじめ入力されています。パワー ストリップの各コンセントに関する次の情報が表示されます。コンセントの番号、名前、ポートの関連付け。

このページを使用して、電源タップとその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: パワー ストリップがターゲット サーバ (ポート) に関連付けられると、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 (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)。

- ▶ **パワー ストリップ (およびコンセント) に名前を付けるには、以下の手順に従います。**

注: CommandCenter Service Gateway では、スペースを含むパワー ストリップ名を認識できません。

1. パワー ストリップの [Name] (名前) を覚えやすい名前に変更します。
2. 必要に応じて、([Outlet] (コンセント)) [Name] (名前) を変更します (デフォルトのコンセント名は、「Outlet #」です)。
3. [OK] をクリックします。

▶ 変更を保存せずに終了するには、以下の手順に従います。

- [Cancel] (キャンセル) をクリックします。

Home > Device Settings > Port Configuration > Port

Port 2

Type:
PowerStrip

Name:
Power Port 1

Outlets

Number	Name	Port Association
1	Outlet 1	
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Outlet 7	

OK Cancel

© 2008 Raritan, Inc.

電源の関連付けを管理する

▶ 電源の関連付けを行う (パワー ストリップ 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: パワー ストリップがターゲット サーバ (ポート) に関連付けられると、コンセント名はポート名に置き換えられます。この名前は、[Port 2] (ポート 2) ページで変更できます。

1. [Power Strip Name] (パワー ストリップ名) ドロップダウン リストからパワー ストリップを選択します。
2. [Outlet Name] (コンセント名) ドロップダウン リストからコンセントを選択します。
3. 必要な電源の関連付けごとに、手順 1 と 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。

▶ **パワー ストリップの関連付けを削除するには、以下の手順に従います。**

1. [Power Strip Name] (パワー ストリップ名) ドロップダウン リストから該当するパワー ストリップを選択します。
2. そのパワー ストリップに対して、[Outlet Name] (コンセント名) ドロップダウン リストから該当するコンセントを選択します。
3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし) を選択します。
4. [OK] をクリックします。そのパワー ストリップとコンセントの関連付けが削除されます。確認メッセージが表示されます。

▶ **パワー ポートの設定を表示するには、以下の手順に従います。**

- [Home] (ホーム)、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定) [power port name] (パワー ポート名) の順に選択します。[Outlets] (コンセント) の下に、電源タップに対するコンセントの関連付けが表示されます。

▶ **パワー ポートの設定を編集するには、以下の手順に従います。**

1. ポートの [Name] (名前) フィールドを編集して電源ポート名を変更します。
2. コンセントの [Name] (名前) フィールドを編集してコンセント名を変更します。コンセント名は [Power Strip Device] (電源タップ デバイス) ページに表示されます。詳細については、「電源タップ デバイスを管理する」を参照してください。
3. コンセント名の横にある [Port Association] (ポートの関連付け) リンクをクリックし、[Port 1] (ポート 1) ページで編集して、コンセントの関連付けを変更します。

電源タップ デバイスを管理する

[Power Strip Device] (電源タップ デバイス) ページを使用して電源タップ デバイスを制御します。このページで、電源タップの各コンセントをオン/オフにすることができます。

▶ **KX II-101-V2 に接続されている電源タップを制御するには、以下の手順に従います。**

1. [Home] (ホーム) の [Powerstrip] (パワーストリップ) を選択します。[Power Strip Device] (電源タップ デバイス) ページが開きます。
2. コンセントごとに [On] (オン) または [Off] (オフ) をクリックして、オンまたはオフにします。
3. 確認のプロンプトが表示されたら、[OK] をクリックします。

注:KX II-101-V2 で制御できるのは、1 つの電源タップのみです。
[Powerstrip] (電源タップ) メニューで別の電源タップを選択することはできません。

アナログ KVM スイッチ

KX II-101-V2 と連動する Raritan アナログ KVM スイッチを設定できます。

以下の Raritan KVM スイッチは、KX II-101-V2 と連動することが確認されています。

- SwitchMan SW2、SW4、および SW8
- Master Console MX416 および MXU

Raritan または他のベンダーの類似製品も連動する可能性があります、サポートは保証されません。

注:KX II-101-V2 がアナログ KVM スイッチと連動するためには、ターゲットを切り替えられるスイッチ ホットキーをデフォルトの **Scroll Lock** に設定する必要があります。

▶ **Raritan アナログ KVM スイッチを設定するには、次の手順に従います。**

1. [Keyboard/Mouse Setup] (キーボード/マウス設定) ページで [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定します。この操作を行わずにアナログ KVM スイッチを設定しようとすると、「PS/2 is needed to access the KVM Switch. (KVM スイッチにアクセスするには PS/2 が必要です。)Please enable PS/2 first! (最初に PS/2 を有効にしてください!)」というエラーが [Analog KVM Switch Configuration] (アナログ KVM スイッチ設定) ページに表示されます。詳細については、「**キーボード/マウス設定** 『112p.』」を参照してください。
2. [Device Settings] (デバイスの設定) の [Analog KVM Switch] (アナログ KVM スイッチ) をクリックします。[Analog KVM Switch Configuration] (アナログ KVM スイッチ設定) ページが開きます。
3. [Use Analog KVM Switch] (アナログ KVM スイッチを使用する) チェックボックスをオンにして各フィールドを有効にします。
4. [Switch Type] (スイッチ タイプ) ドロップダウンから Raritan スイッチ タイプを選択します。
 - Raritan MCC
 - Raritan MX
 - Raritan MXU
 - Raritan Switchman

5. [Port Count] (ポート カウント) フィールドで、選択されているスイッチ タイプに基づいて使用可能なポートの数を入力します。必要に応じてポート カウントを変更するか、デフォルトのカウントを使用します。選択したスイッチのデフォルトのポート カウントは、それぞれ次のとおりです。
 - Raritan MCC - 8
 - Raritan MX - 16
 - Raritan MXU - 16
 - Raritan Switchman - 2
 6. [Security] (セキュリティ) チェックボックスをオンにしてセキュリティを有効にします。
 7. KVM スイッチのアクセスに使用されるパスワードを入力します。
 8. [OK] をクリックしてアナログ KVM スイッチを設定します。
- ▶ アナログ KVM スイッチのデフォルトを復元するには、次の手順に従います。
- [Reset to Defaults] (デフォルトに戻す) をクリックします。

Analog KVM Switch Configuration

Note: Changing one of the following options will close all kvm and virtual media sessions.

Use Analog KVM Switch

Switch Type

Raritan MCC ▼

Port Count

8

Security Setting

Password

OK

Reset To Defaults

Cancel

リセット ボタンを使用して KX II-101-V2 をリセットする

デバイスの上部には、リセット ボタンがあります。誤ってリセットされないように、ボタンはパネルに埋め込まれています (このボタンを押すには、先端の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、グラフィカル ユーザ インタフェースで定義します。詳細については、「**[Encryption & Share] (暗号化および共有)**」を参照してください。

▶ KX II-101-V2 をリセットするには

1. KX II-101-V2 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-101-V2 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。
5. リセット ボタンをリリースすると、KX II-101-V2 が再起動されます。この処理には、通常 3 分かかります。

注: KX II-101-V2 が、リセット時に工場出荷時のデフォルトに戻るよう設定されている場合は、それに応じて IP アドレス、ユーザ名などのオプションが設定されます。



Ch 7

USB 接続を管理する

この章の内容

概要.....	136
USB 接続設定	137
USB 接続の詳細設定	138

概要

さまざまな KVM ターゲット サーバと KX II-101-V2 との互換性を高めるために、幅広いオペレーティング システムおよび BIOS レベル サーバのサーバ実装に対応する USB 設定プロファイル オプションが、ユーザ定義に基づいてリアルタイムに選択できるようになっています。

デフォルトの [USB Connection Settings] (USB 接続設定) で、展開された大多数の KVM ターゲット サーバ設定のニーズが満たされます。その他の設定項目は、一般的に展開される他のサーバ設定 (Linux®、Mac OS X など) の特有のニーズを満たすために用意されています (プラットフォーム名や BIOS リビジョンによって指定されている設定項目も数多くあります)。これにより、BIOS レベルで動作する場合などに、仮想メディアの機能とターゲット サーバとの互換性を高めることができます。

USB プロファイルは、KX II-101-V2 リモート コンソールの [Device Settings] (デバイスの設定) の [Port Configuration] (ポート設定) を選択し、表示される [Port] (ポート) ページで設定します。デバイス管理者は、ユーザのニーズに最も適したプロファイルおよびターゲット サーバ設定でポートを設定できます。

警告:[Advanced USB Connection Settings] (USB 接続の詳細設定) セクションでの選択によっては、KX II-101-V2 とターゲット サーバの間で設定の問題が発生する場合があります。

したがって、最新の [User Defined KX II-101-V2 USB Profile Configuration Table] (ユーザ定義の KX II-101-V2 USB プロファイル設定テーブル) ハイパーリンクを参照することをお勧めします。このリンクには、[Port] (ポート) ページの [Advanced USB Connection Settings] (USB 接続の詳細設定) セクションから直接アクセスできます。本書の公開時点で入手可能な情報は、「Known USB Profiles (既知の USB プロファイル)」にあります。

KVM ターゲット サーバに接続しているユーザは、KVM ターゲット サーバの動作状態に基づいて、この [USB Connection Settings] (USB 接続設定) から選択します。たとえば、サーバが実行しており、ユーザが Windows® オペレーティング システムを使用する場合は、デフォルトの設定を使用することをお勧めします。しかし、ユーザが BIOS メニューで設定を変更する場合や、仮想メディア ドライブから起動する場合、ターゲット サーバ モデルによっては、別の USB 接続設定が適している可能性があります。

Raritan が用意している USB 接続設定のどれを使用しても指定した KVM ターゲットと連動しない場合は、Raritan テクニカル サポート チームにお問い合わせください。

USB 接続設定

- ▶ ターゲット サーバの **USB 接続を定義するには、次の手順に従います。**
- 1. [Device Settings] (デバイスの設定) の [Port Configuration] (ポート設定) をクリックして、[Port Configuration] (ポート設定) ページを開きます。設定するポートをクリックします。
- 2. [USB Connection Settings] (USB 接続設定) をクリックして、[USB Connection Settings] (USB 接続設定) セクションを展開します。
- 3. 使用する USB 接続設定を選択します。
 - [Enable Absolute Mouse] (ずれないマウスを有効にする) - USB がアクティブなキーボード/マウス インタフェースである場合にのみ適用されます。
 - [Use Full Speed] (フル スピードを使用) - BIOS が高速 USB デバイスに対応していない場合に役立ちます。
 - [Absolute mouse scaling for MAC server] (MAC サーバの絶対マウス スケーリング) - USB がアクティブなキーボード/マウス インタフェースである場合にのみ適用されます。
 - [USB Sun Keyboard support] (USB Sun キーボード サポート) - USB がアクティブなキーボード/マウス インタフェースである場合にのみ適用されます。
- 4. [OK] をクリックします。

▼ USB Connection Settings

- Enable Absolute Mouse**
(applies only if USB is active Keyboard/Mouse Interface)
- Use Full Speed - Useful for BIOS**
that cannot handle High Speed USB devices
- Absolute mouse scaling for MAC server**
(applies only if USB is active Keyboard/Mouse Interface)
- USB SUN Keyboard support**
(applies only if USB is active Keyboard/Mouse Interface)

▶ Advanced USB Connection Settings

USB 接続の詳細設定

警告:[Advanced USB Connection Settings] (USB 接続の詳細設定) セクションでの選択によっては、KX II-101-V2 とターゲット サーバの間で設定の問題が発生する場合があります。したがって、「Known USB Profiles (既知の USB プロファイル)」を参照するか、[User Defined KX II-101-V2 USB Profile Configuration Table] (ユーザ定義の KX II-101-V2 USB プロファイル設定テーブル) リンクを参照することをお勧めします。このリンクにアクセスするには、[Port] (ポート) ページの [Advanced USB Connection Settings] (USB 接続の詳細設定) セクションの対応するリンクをクリックします。

- ▶ **ターゲット サーバの USB 接続の詳細を定義するには、次の手順に従います。**
- 1. [Device Settings] (デバイスの設定) の [Port Configuration] (ポート設定) をクリックして、[Port Configuration] (ポート設定) ページを開きます。設定するポートをクリックします。
- 2. [Advanced USB Connection Settings] (USB 接続の詳細設定) をクリックしてセクションを展開します。
- 3. [User Defined KX II-101 USB Profile Configuration Table] (ユーザ定義の KX II-101 USB プロファイル設定テーブル) リンクをクリックして、[Advanced USB Connection Settings] (USB 接続の詳細設定) セクションに適用される推奨設定にアクセスします。
- 4. 必要に応じて以下を設定します。
 - a. [Virtual Media Interface #1 Type] (仮想メディア インタフェース #1 タイプ)
 - b. 指定された VM タイプ インタフェース (#1 用) を削除するには、[Remove Unused VM Interface #1 From Device Configuration] (デバイス設定から未使用の VM インタフェース #1 を削除する) チェックボックスをオンにします。
 - c. [Virtual Media Interface #2 Type] (仮想メディア インタフェース #2 タイプ)
 - d. 指定された VM タイプ インタフェース (#2 用) を削除するには、[Remove Unused VM Interface #2 From Device Configuration] (デバイス設定から未使用の VM インタフェース #2 を削除する) チェックボックスをオンにします。

5. [OK] をクリックします。

▼ Advanced USB Connection Settings

IMPORTANT: Please follow the reference guide provided at this link.

User Defined KX II-101 USB Profile Configuration Table

Virtual Media Interface #1 Type

CD-ROM ▼

Remove Unused VM Interface #1 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

Virtual Media Interface #2 Type

Removable Disk ▼

Remove Unused VM Interface #2 From Device Configuration
(useful for BIOS that cannot accommodate empty drives)

この章の内容

[Security Settings] (セキュリティ設定)	140
[IP Access Control] (IP アクセス制御).....	149

[Security Settings] (セキュリティ設定)

[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)** 『141p.』 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)** 『142p.』 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)** 『144p.』 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。

[Login Limitations] (ログイン制限)

ログイン制限を使用して、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
[Enable Single Login Limitation] (シングル ログイン制限を有効にする)	これを選択すると、常時ユーザ名ごとに 1 人のログインしか許可されません。この選択を解除すると、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。
[Enable password aging] (パスワード エージングを有効にする)。	これを選択すると、 [Password Aging Interval] (パスワード エージング間隔) フィールド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。 [Enable Password Aging] (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。
[Log out idle users] (アイドル ユーザのログアウト)、 [After (1-365 minutes)] (経過時間 (1 ~ 365 分))	[Log out idle users] (アイドル ユーザのログアウト) チェックボックスをオンにして、 [After (1-365 minutes)] (経過時間 (1 ~ 365 分)) フィールドで指定した時間の経過後にユーザを自動的に切断します。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。 [After] (経過時間) フィールドは、アイドル ユーザがログアウトされるまでの時間 (分) を設定するために使用されます。 [Log out idle users] (アイドル ユーザのログアウト) オプションをオンにすると、このフィールドが有効になります。フィールド値として最大 365 分を入力できます。

[Strong Passwords] (強力なパスワード)

[Strong Passwords] (強力なパスワード) によってシステムの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-101-V2 ローカル パスワードの形式を指定できます。

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。

これを選択すると、強力なパスワードのルールが適用されます。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、ユーザは次回ログイ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。この選択を解除すると、標準の形式検証だけが適用されます。これを選択した場合は次のフィールドが有効になるため、設定する必要があります。

フィールド	説明
[Minimum length of strong password] (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 文字まで指定できます。
[Maximum length of strong password] (強力なパスワードの最大長)	デフォルトでは 8 文字ですが、最大 16 文字まで拡張できます。
[Enforce at least one lower case character] (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。
[Enforce at least one upper	これを選択すると、パスワードに 1 文

フィールド	説明
case character] (1 文字以上の大文字の使用を強制する)	字以上の大文字が必要になります。
[Enforce at least one numeric character] (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。
[Enforce at least one printable special character] (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。
[Number of restricted passwords based on history] (履歴に基づく制限パスワードの数)	このフィールドは、パスワード履歴数を表示します。つまり、繰り返し使用できない以前のパスワードの数を表します。範囲は 1 ~ 12 で、デフォルトは 5 です。

Strong Passwords

Enable Strong Passwords

Minimum length of strong password

8

Maximum length of strong password

16

Enforce at least one lower case character

Enforce at least one upper case character

Enforce at least one numeric character

Enforce at least one printable special character

Number of restricted passwords based on history

5

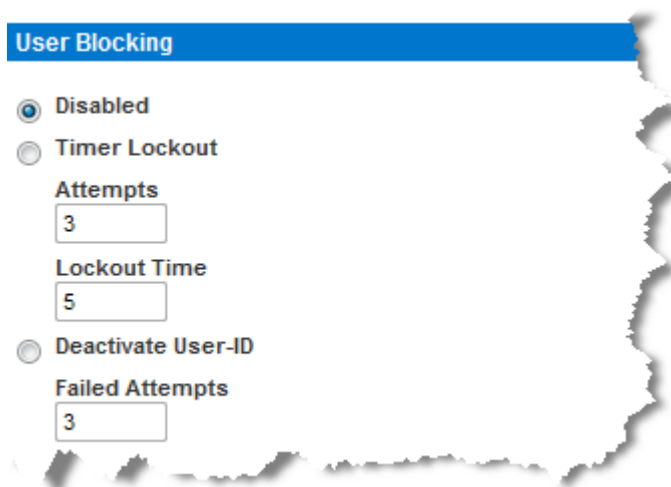
[User Blocking] (ユーザ ブロック)

ユーザ ブロック オプションでは基準を指定し、ユーザが指定回数ログイ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
[Disabled] (無効)	デフォルトのオプションです。認証に失敗した回数にかかわらず、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
<p>[Timer Lockout] (タイマー ロックアウト)</p>	<p>ユーザが指定回数より多くログインに失敗すると、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。</p> <ul style="list-style-type: none"> ▪ [Attempts] (試行回数) - 失敗可能なログインの試行回数を示し、この回数より多くログインに失敗すると、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。 ▪ [Lockout Time] (ロックアウト タイム) - 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、デフォルトは 5 分です。 <hr/> <p><i>注:管理者の役割のユーザは、タイマー ロックアウト設定から除外されています。</i></p>
<p>[Deactivate User-ID] (ユーザ ID の無効化)</p>	<p>このオプションを選択した場合は、[Failed Attempts] (失敗可能な試行回数) フィールドで指定した回数より多くログインに失敗すると、ユーザはシステムからロックアウトされます。</p> <ul style="list-style-type: none"> ▪ [Failed Attempts] (失敗可能な試行回数) - 失敗可能なログインの試行回数を示し、この回数より多くログインに失敗すると、そのユーザのユーザ ID が無効になります。 <p>[Deactivate User-ID] (ユーザ ID の無効化) オプションを選択すると、このフィールドが有効になります。有効な範囲は 1 ~ 10 です。</p> <p>指定回数より多くログイ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、[User] (ユーザ) ページの [Active] (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。</p>



[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-101-V2 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-101-V2 にアクセスできなくなります。

1. [Encryption Mode] (暗号化モード) ドロップダウン リストからオプションのいずれかを選択します。暗号化モードを選択しても、使用しているブラウザで、選択したモードがサポートされていない場合は、KX II-101-V2 に接続できないという警告が表示されます。警告「When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the ProductName. ([Encryption Mode] (暗号化モード) が指定されている場合は、ブラウザでこ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は、KX II-101-V2 に接続できません。)」が表示されます。

暗号化モード	説明
[Auto] (自動)	推奨のオプションです。KX II-101-V2 で、自動ネゴシエーションによって考えられる最高の暗号化レベルに設定されます。
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-101-V2 デバイスとリモート PC 間

暗号化モード	説明
	のプライベート通信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。
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 はキーの長さを表します。[AES-128] (AES-128) 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、「 Checking Your Browser for AES Encryption (使用しているブラウザの AES 暗号化を確認する) 」『149p. 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 はキーの長さを表します。[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、「 Checking Your Browser for AES Encryption (使用しているブラウザの AES 暗号化を確認する) 」『149p. 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:MPC では、常にネゴシエーションによって最高の暗号化レベルに設定され、[Auto] (自動) に設定されていない場合は、[Encryption Mode] (暗号化モード) 設定に合わされます。

注:Windows XP (Service Pack 2) を実行している場合は、Internet Explorer 7 から AES-128 暗号化を使用してリモートで KX II-101-V2 に接続することはできません。

- [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. **[PC Share Mode] (PC 共有モード)** ボックスの一覧で値を選択します。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-101-V2 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 ユーザはキーボード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。
4. 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。
5. If needed, select the Disable Local Port Output checkbox. If this option is selected, there is no video output on the local port. This setting applies only to the KX2 832 and KX2 864. If you are using smart card readers, the local port *must* be disabled.
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-101-V2 をリセットする」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-101-V2 を出荷時設定にリセットします。
[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 <code>raritan</code> に戻ります。

ローカル デバイス リセット モード	説明
[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。

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-101-V2 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

[IP Access Control] (IP アクセス制御)

IP アクセス制御によって、KX II-101-V2 へのアクセスを制御できます。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。

重要: KX II-101-V2 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 が含まれていると、KX II-101-V2 ローカルポートにアクセスできなくなります。

▶ **IP アクセス制御を使用するには、以下の手順に従います。**

1. [Security] (セキュリティ) の [IP Access Control] (IP アクセス制御) を選択して、[IP Access Control] (IP アクセス制御) ページを開きます。[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、IP アクセス制御とページの残り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) を選択します。これは、指定した範囲内にはない IP アドレスに対して実行されるアクションを表します。
 - [Accept] (承諾) - その IP アドレスによる KX II-101-V2 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-101-V2 デバイスへのアクセスが拒否されます。

▶ **新しいルールを追加するには、以下の手順に従います。**

1. [IP/Mask] (IP/マスク) フィールドに 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、CIDR (Classless Inter-Domain Routing) 表記に従って入力する必要があります。CIDR 表記は、2 つの部分からなります。上位部分はネットワーク アドレスであり、ネットワーク全体またはサブネットを識別します。下位部分は識別子です。/ の後のプレフィックス長は、サブネット マスクの長さを表します。

2. ドロップダウン リストからポリシーを選択します。
3. [Append] (追加) をクリックします。ルール リストの 1 番下にルールが追加されます。

▶ **ルールを挿入するには、以下の手順に従います。**

1. ルール番号 (#) を入力します。挿入コマンドを使用する際にルール番号が必要です。
2. [IP/Mask] (IP/マスク) フィールドに IP アドレスとサブネット マスクを入力します。
3. ドロップダウン リストから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。

ヒント:ルール番号を使用すると、ルールが作成された順番を基により詳細に制御できます。

▶ **ルールを置き換えるには、以下の手順に従います。**

1. 置き換えるルール番号を指定します。
2. [IP/Mask] (IP/マスク) フィールドに IP アドレスとサブネット マスクを入力します。
3. ドロップダウン リストからポリシーを選択します。
4. [Replace] (置き換え) を選択します。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、以下の手順に従います。**

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ます。[OK] をクリックします。

Home > Security > IP Access Control

IP Access Control

Enable IP Access Control

Default policy
ACCEPT

Rule #	IP/Mask	Policy
		ACCEPT

Append Insert Replace Delete

OK Reset To Defaults Cancel

1 つの IP アドレスへのアクセスだけを許可し、他のすべてをブロックするには、ルールのサブネット マスクを「/32」に変更します。たとえば、「192.168.51」サブネットからのアクセスをすべて除外しており、[Default Policy] (デフォルト ポリシー) が [Accept] (承諾) になっている場合は、[IP/Mask] (IP/マスク) が「192.168.51.0/24」で [Policy] (ポリシー) が [Drop] (拒否) に設定されているルールを追加します。または、特定の IP アドレス (192.168.51.105) を除く、「192.168.51」サブネットからのアクセスをすべて除外しており、[Default Policy] (デフォルト ポリシー) が [Accept] (承諾) になっている場合は、次のようにします。

1. [IP/Mask] (IP/マスク) が「192.168.51.105/32」で [Policy] (ポリシー) が [Accept] (承諾) に設定されているルール 1 を追加します。
2. [IP/Mask] (IP/マスク) が「192.168.51.0/24」で [Policy] (ポリシー) が [Drop] (拒否) に設定されているルール 2 を追加します。

ルール 1 とルール 2 を入れ替えると、検出された最初のルールで拒否されているので、「192.168.51.105」も KX II-101-V2 にアクセスできなくなります。

この章の内容

[Audit Log] (監査ログ).....	153
[Device Information] (デバイス情報)	154
[Backup and Restore] (バックアップと復元).....	155
ファームウェアをアップグレードする	157
アップグレード履歴	159
[Factory Reset] (ファクトリ リセット)	160
再起動.....	161

[Audit Log] (監査ログ)

KX II-101-V2 のシステム イベントに関するログが作成されます。

▶ **KX II-101-V2 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**

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作成されます。

▶ **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)

[Device Information] (デバイス情報) ページでは、使用している KX II-101-V2 デバイスに関する詳細な情報を確認できます。この情報は、Raritan のテクニカル サポートにご連絡いただく際に役立ちます。

▶ **KX II-101-V2 に関する情報を表示するには、以下の手順に従います**

-
- [Maintenance] (メンテナンス) の [Device Information] (デバイス情報) を選択します。[Device Information] (デバイス情報) ページが開きます。

使用している KX II-101-V2 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

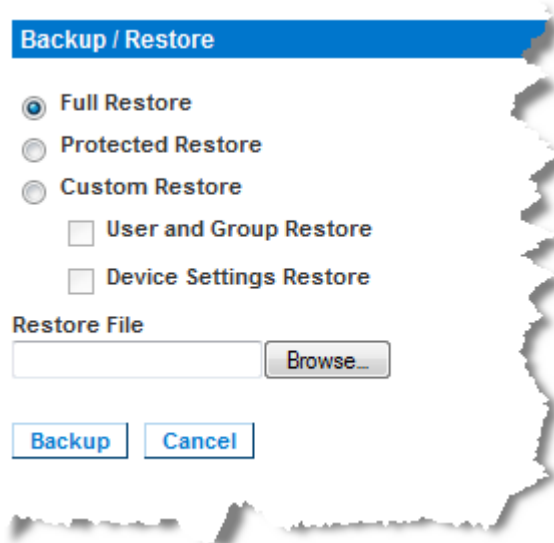
[Backup and Restore] (バックアップと復元)

[Backup/Restore] (バックアップ/復元) ページでは、Dominion KX II の設定と構成をバックアップおよび復元できます。

バックアップと復元は、事業の継続性に貢献するだけではありません。この機能は、時間を節約するためのメカニズムとしても役立ちます。たとえば、使用中の KX II-101-V2 のユーザ設定をバックアップして、それを新しい KX II-101-V2 に復元することで、別の KX II-101-V2 から自分のチームにすばやくアクセスできます。また、1 台の KX II-101-V2 でセットアップを行い、その設定を複数の KX II-101-V2 デバイスにコピーすることもできます。

▶ **[Backup/Restore] (バックアップ/復元) ページを表示するには、以下の手順に従います。**

- [Maintenance] (メンテナンス)の [Backup/Restore] (バックアップ/復元) を選択します。[Backup/Restore] (バックアップ/復元) ページが開きます。



注:バックアップを行うと、常にシステム全体がバックアップされます。復元については、全体の復元と部分的な復元のどちらかを選択できます。

▶ **Firefox® または Internet Explorer® 5 以前を使用している場合、KX II-101-V2 をバックアップするには、次の手順に従います。**

1. [Backup] (バックアップ) をクリックします。[File Download] (ファイルのダウンロード) ダイアログ ボックスが表示されます。
2. [Save] (保存) をクリックします。[Save As] (名前を付けて保存) ダイアログ ボックスが表示されます。

3. 保存先を選択し、ファイル名を指定してから、[Save] (保存) をクリックします。[Download Complete] (ダウンロードの完了) ダイアログ ボックスが表示されます。
4. [Close] (閉じる) をクリックします。バックアップ ファイルは、使用しているクライアント マシン上で指定した場所に指定した名前で、ローカルに保存されます。

▶ **Internet Explorer 6 以降を使用している場合、KX II-101-V2 をバックアップするには、次の手順に従います。**

1. [Backup] (バックアップ) をクリックします。[開く] (Open) ボタンを備えた [File Download] (ファイルのダウンロード) ダイアログ ボックスが表示されます。[開く] (Open) はクリックしないでください。

IE 6 以降では、IE がファイルを開くデフォルトのアプリケーションとして使用されるので、ファイルを開くか保存するように求めるプロンプトが表示されます。これを回避するには、ファイルを開く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 ファイルは、使用しているクライアント マシン上で指定した場所に指定した名前で、ローカルに保存されます。
 - 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-101-V2 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-101-V2 を以前のバージョンに復元する際には、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。以前の管理者ユーザ名とパスワードを記憶していないと、KX II-101-V2 からロックアウトされます。

また、バックアップの時点で現在とは異なる IP アドレスを使用していた場合は、その IP アドレスも同様に復元されます。設定で DHCP を使用している場合は、更新後にローカル ポートにアクセスし、IP アドレスを確認する際にのみこの操作を行うことが考えられます。

1. 実行する復元のタイプを選択します。

- **[Full Restore] (完全な復元)** - システム全体を完全に復元します。通常は、従来のバックアップおよび復元のために使用されます。
 - **[Protected Restore] (保護された復元)** - IP アドレス、名前のようなデバイス固有の情報以外のすべての情報が復元されます。このオプションを使用すると、1 台の **KX II-101-V2** でセットアップを行い、その設定を複数の **KX II-101-V2** デバイスにコピーすることもできます。
 - **[Custom Restore] (カスタム復元)** - このオプションでは、**[User and Group Restore] (ユーザとグループの復元)**、**[Device Settings Restore] (デバイス設定の復元)** のどちらか一方または両方を選択できます。
 - **[User and Group Restore] (ユーザとグループの復元)** - このオプションでは、ユーザとグループの情報のみが復元されます。このオプションでは、証明書およびプライベート キー ファイルは復元されません。このオプションを使用すると、別の **KX II-101-V2** にすばやくユーザを設定できます。
 - **[Device Settings Restore] (デバイス設定の復元)** - このオプションでは、デバイス設定 (電源の関連付け、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など) のみが復元されます。このオプションを使用すると、デバイス情報をすばやくコピーできます。
1. **[参照] (Browse)** をクリックします。**[Choose file] (ファイルの選択)** ダイアログ ボックスが表示されます。
 2. 適切なバックアップ ファイルに移動して選択し、**[Open] (開く)** をクリックします。選択したファイルは、**[Restore File] (復元ファイル)** フィールドにリスト表示されます。
 3. **[Restore] (復元)** を選択します。選択した復元のタイプに基づいて、設定が復元されます。

ファームウェアをアップグレードする

[Firmware Upgrade] (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-101-V2** のファームウェアをアップグレードします。

重要:アップグレードの実行中は、使用している **KX II-101-V2** デバイスの電源を切断しないでください。デバイスが損傷するおそれがあります。

▶ **KX II-101-V2** デバイスをアップグレードするには、以下の手順に従います。

1. [Maintenance] (メンテナンス) の [Firmware Upgrade] (ファームウェアのアップグレード) を選択します。[Firmware Upgrade] (ファームウェアのアップグレード) ページが開きます。

Firmware Upgrade

Show Latest Firmware

Firmware File

2. [Show Latest Firmware] (最新のファームウェアの表示) リンクをクリックし、[Firmware Upgrades] (ファームウェア アップグレード) の [KX II-101-V2] ページで適切な Raritan ファームウェアの配布ファイル (*.RFP) を確認し、ダウンロードします。
3. ファイルを解凍して、アップグレードを実行する前に、ファームウェアの ZIP ファイルに含まれる手順をすべてお読みください。

注: アップロードの前に、ファームウェア更新ファイルをローカル PC にコピーしてください。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。[Browse] (参照) ボタンをクリックして、アップグレード ファイルを解凍したディレクトリに移動します。

4. [Firmware Upgrade] (ファームウェアのアップグレード) ページで [Upload] (アップロード) をクリックします。アップグレードに関する情報とバージョン番号が確認のために表示されます。

Home > Maintenance > Firmware Upgrade

Firmware Upgrade

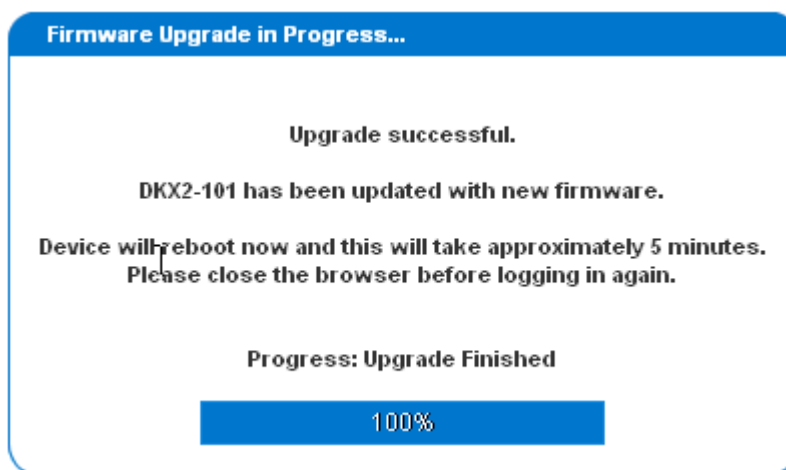
Current version: 2.0.0.5.6394

New version: 2.0.0.5.6487

This may take some minutes. Please do NOT power off the device while the update is in progress! After a successful update, the device will be reset automatically.

注:この時点で接続していたユーザはログアウトされ、新たなログインの試行はブロックされます。

- [Upgrade] (アップグレード) をクリックします。アップグレードが完了するまで待機します。アップグレード中は、ステータス情報と進捗状況を示すバーが表示されます。アップグレードが完了すると、デバイスが再起動します。



- 指示に従ってブラウザを閉じ、約 5 分待ってから、再度 KX II-101-V2 にログインします。
Multi-Platform Client を使用してデバイス ファームウェアのアップグレードを行う方法については、『**Raritan Multi-Platform Client (MPC) ユーザ ガイド**』を参照してください。

アップグレード履歴

KX II-101-V2 では、KX II-101-V2 デバイス上で実行されたアップグレード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。
 - [Maintenance] (メンテナンス) の [Upgrade History] (アップグレード履歴) を選択します。[Upgrade History] (アップグレード履歴) ページが開きます。

Upgrade History

Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.51.76	January 16, 2000 01:03	January 16, 2000 01:06	3.3.0.1.9999	3.3.0.5.1046	Successful
Full Firmware Upgrade	admin	192.168.51.76	January 16, 2000 00:23	January 16, 2000 00:25	3.3.0.5.1046	3.3.0.1.9999	Successful
Full Firmware Upgrade	admin	192.168.51.76	January 15, 2000 02:15	January 15, 2000 02:18	3.3.0.1.123	3.3.0.5.1046	Successful
Full Firmware Upgrade	admin	192.168.51.76	January 14, 2000 00:16	January 14, 2000 00:18	3.3.0.1.9999	3.3.0.1.9999	Successful
Full Firmware Upgrade	admin	192.168.51.76	January 13, 2000 22:39	January 13, 2000 22:42	3.3.0.1.9999	3.3.0.1.9999	Successful

[Factory Reset] (ファクトリ リセット)

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」を参照してください。

▶ 出荷時設定にリセットするには

1. [Maintenance] (保守) メニューの [Factory Reset] (出荷時設定にリセット) をクリックします。[Factory Reset] (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。
 - [Full Factory Reset] (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-101-V2 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。
 - [Network Parameter Reset] (ネットワーク パラメータ値をリセット): KX II-101-V2 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、[Device Settings] (デバイス設定) メニューの [Network Settings] (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ー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)
1. [Reset] (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。

2. [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-101-V2 が自動再起動します。

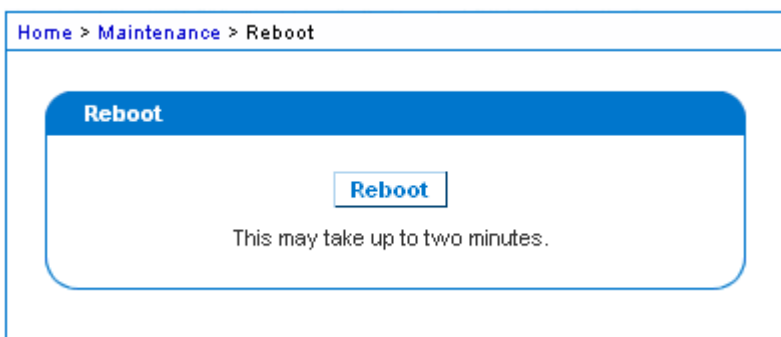
再起動

[Reboot] (再起動) ページでは、KX II-101-V2 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。

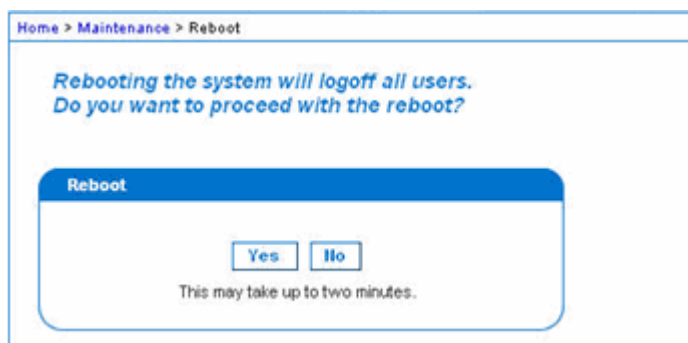
重要: すべての KVM 接続およびシリアル接続が切断され、また、すべてのユーザがログオフされます。

▶ KX II-101-V2 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。



[Diagnostics] (診断) ページはトラブルシューティングの目的で使用されるページであり、主に KX II-101-V2 デバイスの管理者を対象としています。すべての [Diagnostics] (診断) ページで ([Device Diagnostics] (デバイス診断) を除く)、標準的なネットワーク コマンドが実行されます。表示される情報は、それらのコマンドの出力結果です。[Diagnostics] (診断) メニュー オプションは、ネットワーク設定のデバッグと変更に役立ちます。

[Device Diagnostics] (デバイス診断) は、Raritan テクニカル サポートの指示に従って使用するオプションです。

この章の内容

[Network Interface] (ネットワーク インタフェース) ページ	163
[Network Statistics] (ネットワーク統計) ページ	163
[Ping Host] (ホストへの Ping) ページ	166
[Trace Route to Host] (ホストへの経路をトレースする) ページ	167
[Device Diagnostics] (デバイス診断)	168

[Network Interface] (ネットワーク インタフェース) ページ

KX II-101-V2 では、ネットワーク インタフェースの状態に関する情報を確認できます。

▶ **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、以下の手順に従います。**

- [Diagnostics] (診断) の [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、ダウンしているか。
- ゲートウェイから Ping を実行可能かどうか。
- 現在アクティブな LAN ポート。

▶ **この情報を更新するには、以下の手順に従います。**

- [Refresh] (更新) ボタンをクリックします。

Network Interface

Refresh

Result:

```
Link state: autonegotiation on, 100 Mbps, full duplex, link ok
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0d:5d:ca:b1:f8 brd ff:ff:ff:ff:ff:ff
inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
LAN 1 is active.
```

[Network Statistics] (ネットワーク統計) ページ

KX II-101-V2 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。

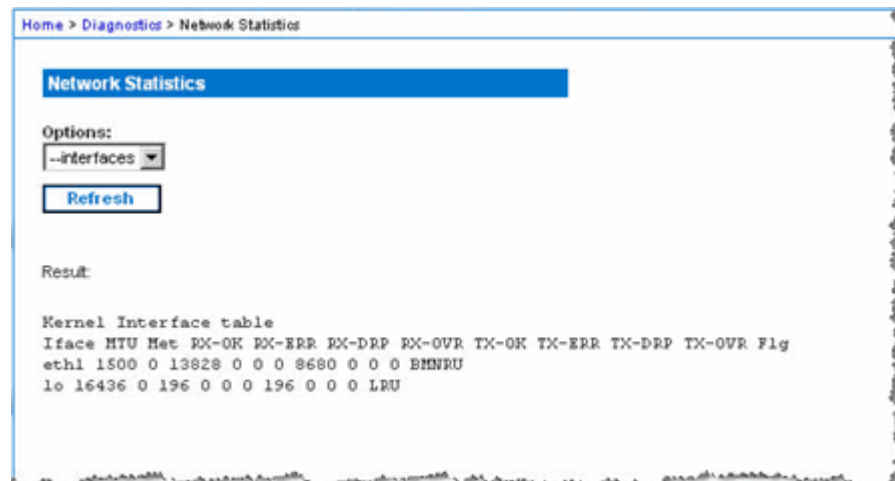
▶ **ネットワーク インタフェースに関する統計情報を表示するには**

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。

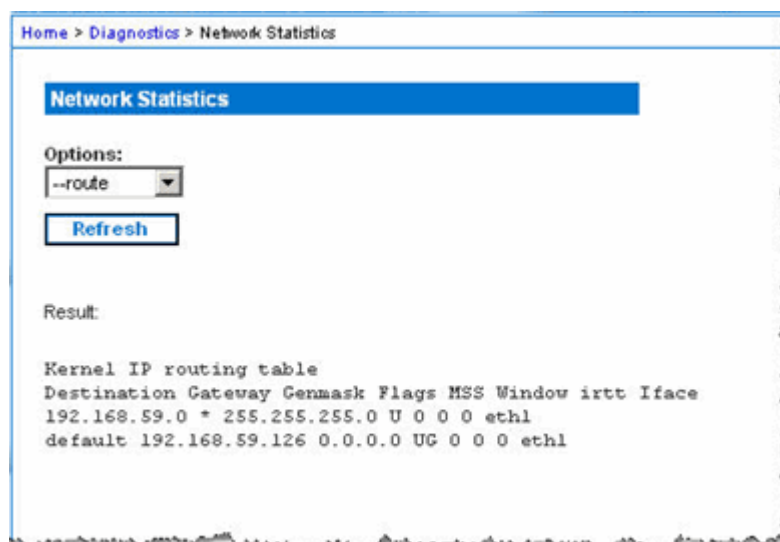
2. [Options] (オプション) ボックスの一覧で値を選択します。
 - [Statistics] (統計): 次に示すような情報が表示されます。



- [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。



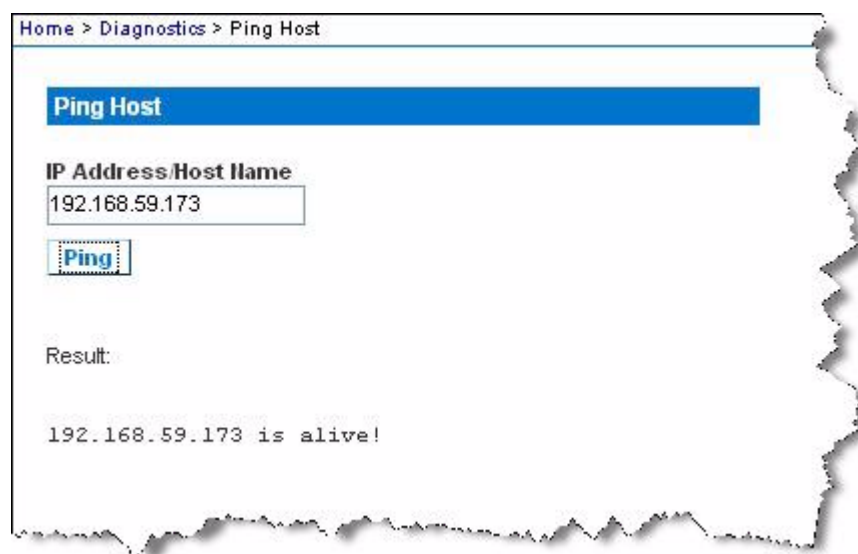
3. [Refresh] (更新) をクリックします。[Options] (オプション) ボックスの一覧で選択した値に応じた情報が、[Result] (結果) フィールドに表示されます。

[Ping Host] (ホストへの Ping) 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-101-V2 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] (ホストへの経路をトレースする) ページ

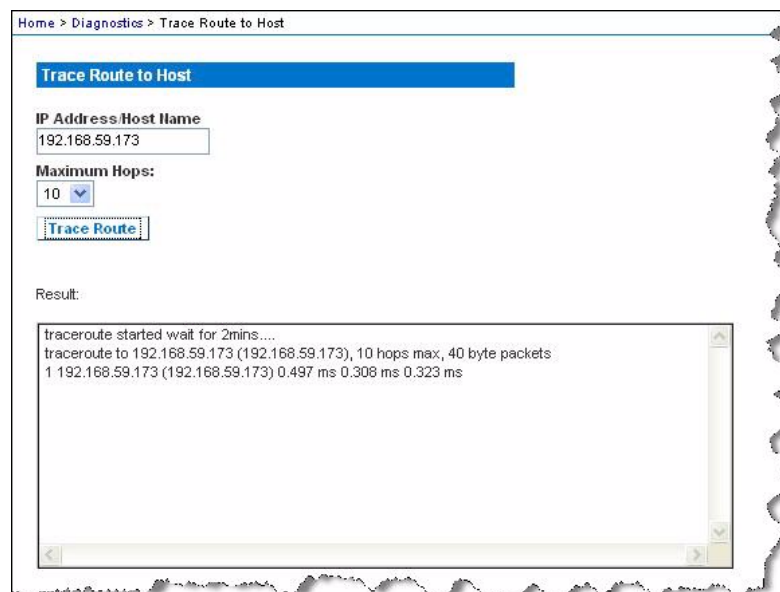
tracert は、指定したホスト名または IP アドレスへの経路を調べるためのネットワーク コマンドです。

▶ ホストまでの経路をトレースするには

1. [Diagnostics] (診断) メニューの [Trace Route to Host] (ホストへの経路をトレースする) をクリックします。[Trace Route to Host] (ホストへの経路をトレースする) 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. [Maximum Hops] (最大ホップ数) ボックスの一覧で最大ホップ数を選択します (5 刻みで 5 ~ 50)。
4. [Trace Route] (経路をトレースする) をクリックします。tracert コマンドが、指定したホスト名または IP アドレスに対して、指定した最大ホップ数以内で実行されます。tracert コマンドの実行結果が [Result] (結果) フィールドに表示されます。



[Device Diagnostics] (デバイス診断)

注:このページは、Raritan フィールド エンジニアによる使用を目的としたページです。Raritan テクニカル サポートに指示された場合に限り、ユーザも使用できます。

[Device Diagnostics] (デバイス診断) ページでは、診断情報を KX II-101-V2 からクライアント マシンにダウンロードします。Raritan テクニカル サポートが提供するオプションの診断スクリプトを使用または使用しないで、デバイス診断ログを生成できます。診断スクリプトを使用すると、問題を診断するための多くの情報が得られます。

次の設定を使用します。

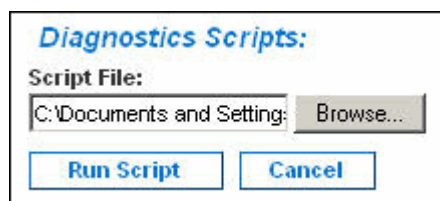
- [Diagnostics Scripts] (診断スクリプト) - 重大なエラーのデバッグ セッション中に Raritan テクニカル サポートの提供する特別なスクリプトを読み込みます。スクリプトはデバイスにアップロードされ、実行されます。オプション
- [Device Diagnostic Log] (デバイス診断ログ) - 診断メッセージのスナップショットを KX II-101-V2 デバイスからクライアントにダウンロードします。その後、この暗号化されたファイルは Raritan テクニカル サポートに送信されます。このファイルは、Raritan でのみ解析できます。

注:このページにアクセスできるのは管理者特権を持つユーザだけです。

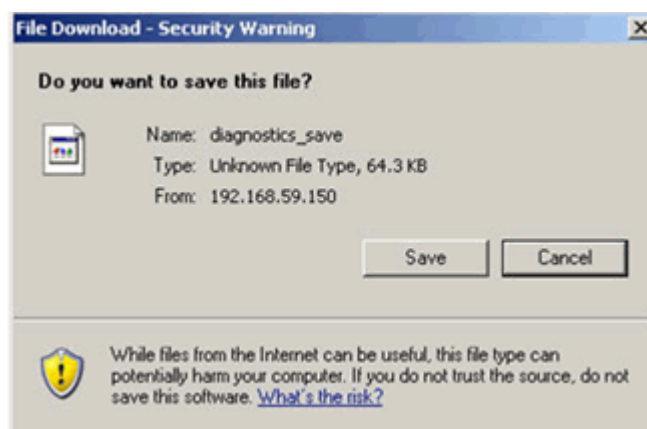
▶ **KX II-101-V2 システム診断を実行するには、以下の手順に従います。**

1. [Diagnostics] (診断) の [Device Diagnostics] (デバイス診断) を選択します。[Device Diagnostics] (デバイス診断) ページが開きます。
2. (オプション) Raritan テクニカル サポートから診断スクリプトを入手した場合は、以下の手順を実行します。そうでない場合は、手順 3 に進みます。
 - a. Raritan から提供される診断ファイルを取得し、必要に応じて解凍します。
 - b. [参照] (Browse) をクリックします。[Choose file] (ファイルの選択) ダイアログ ボックスが表示されます。
 - c. その診断ファイルに移動し、選択します。

- d. [Open] (開く) をクリックします。[Script File] (スクリプト ファイル) フィールドにファイルが表示されます。



- e. [Run Script] (スクリプトを実行する) をクリックします。
3. 診断ファイルを作成して Raritan テクニカル サポートに送信するには、以下の手順に従います。
- a. [Save to File] (ファイルに保存) をクリックします。[File Download] (ファイルのダウンロード) ダイアログ ボックスが表示されます。



- b. [Save] (保存) をクリックします。[Save As] (名前を付けて保存) ダイアログ ボックスが表示されます。
- c. 適切なディレクトリに移動し、[Save] (保存) をクリックします。
4. Raritan テクニカル サポートの指示に従ってこのファイルを電子メールで送信します。

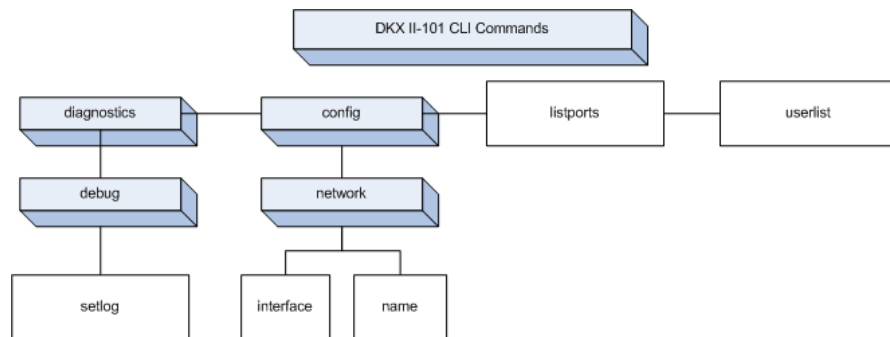
この章の内容

概要.....	170
CLI を使用しての KX II-101-V2 へのアクセス.....	171
KX II-101-V2 への SSH 接続.....	171
ログインする.....	172
CLI の画面操作.....	172
CLI コマンド.....	174

概要

この章では、KX II-101-V2 で使用できる CLI コマンドの概要について説明します。コマンドの一覧および定義、コマンドの例が示されているこの章のセクションへのリンクについては、「**CLI コマンド**『174p.』」を参照してください。

以下の図は CLI コマンドの概要です。



注: コマンド *top*、*history*、*logout*、*quit*、および *help* は、上図のあらゆる CLI レベルから使用できます。

CLI を使用しての KX II-101-V2 へのアクセス

次のいずれかの方法で、KX II-101-V2 にアクセスします。

- IP 接続を介した TELNET
- IP 接続を介した SSH (Secure Shell)
- 付属のケーブルと HyperTerminal のようなターミナル エミュレーション プログラムを使用しての RS-232 シリアル インタフェースを介した多機能管理シリアルポート

複数の SSH/TELNET 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

注: Accessing the CLI by SSH または TELNET へのアクセスには、KX II-101-V2 Remote Client の [Device Services] (デバイス サービス) ページでアクセスを設定する必要があります。詳細については、「[Device Services] (デバイス サービス)」を参照してください。

KX II-101-V2 への SSH 接続

SSHv2 をサポートする SSH クライアントを使用してデバイスに接続します。[Devices Services] (デバイス サービス) ページで SSH アクセスを有効にする必要があります。詳細については、「[Device Services] (デバイス サービス)」を参照してください。

注: セキュリティ上の理由から、SSH V1 は KX II-101-V2 でサポートされていません。

Windows PC からの SSH アクセス

▶ 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-101-V2 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。

5. login as: (ログイン) プロンプトが表示されます。

UNIX/Linux ワークステーションからの SSH アクセス

- ▶ **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。

ログインする

- ▶ ログインするには、次の手順に従います。

1. Login:admin
2. パスワードの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。
ようこそメッセージが表示されます。以上で、管理者としてログインしています。

次の「**CLI のナビゲーション**『172p. の**"CLI の画面操作"**参照』」セクションを確認したら、「**ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定する (オプション)**『31p. 』」で説明されている初期設定タスクを実行できます。

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。

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>
```

TELNET または SSH で接続している場合、コマンドのルート部分は **admin** になります。

```
admin > config > network >
```

0

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。

すべてのコマンド ライン インタフェース レベルに共通のコマンド

「CLI コマンド」には、すべての CLI レベルで使用できるコマンドが一覧で表示されています。これらのコマンドは CLI 内での移動にも役立ちます。

コマンド	説明
top	CLI 階層の最上位または「username」プロンプトに戻ります。
history	KX II-101-V2 CLI で入力された最新の 200 個のコマンドが表示されます。
help	CLI 構文の概要を表示します。
quit	1 レベルだけ戻ります。
logout	ユーザ セッションをログアウトします。

CLI コマンド

下の表は、使用可能なすべての CLI コマンドの一覧とその説明です。

コマンド	説明
config	[Configuration] (設定) メニューに切り替えます。
diagnostics	[diagnostics] (診断) メニューに切り替えます。詳細については、「 Diagnositics (診断) 『175p. の" Diagnositics " 参照先 』」を参照してください。
debug	[debug] (デバッグ) メニューに切り替えます。詳細については、「 Debug (デバッグ) 『175p. の" [Debug] (デバッグ) "参照先 』」を参照してください。
help	CLI 構文の概要を表示します。
history	現在のセッションのコマンド ラインの履歴を表示します。
interface	KX II-101-V2 のネットワーク インタフェースを設定します。
listports	ポート、ポート名、ポート タイプ、ポート ステータス、およびポートの可用性を一覧表示します。詳細については、「 Listports コマンド 『178p. 』」を参照してください。
logout	現在の CLI セッションをログアウトします。

コマンド	説明
config	[Configuration] (設定) メニューに切り替えます。
diagnostics	[diagnostics] (診断) メニューに切り替えます。詳細については、「 Diagnosics (診断) 『175p. の " Diagnosics " 参照先 』」を参照してください。
name	デバイス名を設定します。詳細については、「 Name コマンド 『177p. 』」を参照してください。
network	ネットワーク設定を表示し、設定できます。詳細については、「 ネットワーク 『177p. 』」を参照してください。
quit	前のコマンドに戻ります。
setlog	デバイスのログ記録オプションを設定します。詳細については、「 Setlog コマンド 『176p. 』」を参照してください。
top	[root] (ルート) メニューに戻ります。
userlist	アクティブなユーザ数、ユーザ名、ポート、およびステータスを一覧表示します。詳細については、「 Userlist コマンド 『179p. 』」を参照してください。

Diagnosics

[Diagnosics] (診断) メニューでは、KX II-101-V2 の各種モジュールのログ記録オプションを設定できます。Raritan テクニカル サポートのエンジニアに指示された場合のみ、ログ記録オプションを設定する必要があります。サポート エンジニアは、これらのログ記録オプションを使用して、デバッグおよびトラブルシューティングに関する正しい情報を取得できます。サポート エンジニアが指示した場合、ログ記録オプションの設定方法とログ ファイルを生成して Raritan テクニカル サポートに送信する方法が指示されます。

重要: Raritan テクニカル サポート エンジニアの監督下でのみログ記録オプションを設定してください。

[Debug] (デバッグ)

[Diagnosics] (診断) の [Debug] (デバッグ) メニューでは、Setlog コマンドを使用して KX II-101-V2 のログ記録オプションを設定できます。

Setlog コマンド

Setlog コマンドを使用すると、KX II-101-V2 の各種モジュールのログ記録レベルを設定し、モジュールごとに現在のログ記録レベルを表示できます。**setlog** コマンドの構文は、次のとおりです。

```
setlog [module <module>] [level <level>] [vflag <vflag>] [verbose <on|off>]
Set/Get diag log level
```

次の表で、**Setlog** コマンドのオプションを説明します。Raritan テクニカル サポートは、これらの設定の設定方法を指示します。

コマンドのオプション	説明
module	モジュール名。
level	診断レベル: <ul style="list-style-type: none"> ▪ err ▪ warn ▪ info ▪ debug ▪ trace
vflag	verbose flag のタイプ: <ul style="list-style-type: none"> ▪ timestamp ▪ module ▪ thread ▪ fileline
verbose [on off]	ログ記録をオンまたはオフにします。

Setlog コマンドの例

次の **Setlog** コマンドは、libpp_serial モジュールの **verbose** ログ記録をオンにしたデバッグのログ記録レベルを設定しています。

```
Setlog module libpp_serial level debug verbose on
```

[Configuration] (設定)

[Configuration] (設定) メニューでは、ネットワーク インタフェースの設定とデバイス名の設定に使用する **network** コマンドにアクセスできます。

ネットワーク

[Configuration] (設定) の [Network] (ネットワーク) コマンドを使用して、KX II-101-V2 のネットワーク接続とデバイス名を設定します。

コマンド	説明
interface	KX II-101-V2 デバイスのネットワーク インタフェースを設定します。
name	デバイス名を設定します。

Name コマンド

name コマンドを使用して、デバイス名とホスト名を設定します。

構文

```
name [unitname name] [domain name] [force <true|false>]
```

name コマンドの例

次のコマンドは、デバイス名を設定します。

```
Admin Port > Config > Network > name unitname <device name> domain <host name> force trues
```

Interface コマンド

interface コマンドを使用して、KX II-101-V2 のネットワーク インタフェースを設定します。コマンドが受け入れられると、デバイスは HTTP/HTTPS 接続を切断して新しいネットワーク接続を初期化します。すべての HTTP/HTTPS ユーザは、新しい IP アドレスと正しいユーザ名およびパスワードを使用してデバイスに再接続する必要があります。詳細については、「インストールと設定『7p.』」を参照してください。

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 <auto/10hdx/10fdx/100hdx/100fdx>]
```

次の表で、network コマンドのオプションを説明します。

コマンドのオプション	説明
ipauto	固定または動的 IP アドレス
ip ipaddress	IP ネットワークからのアクセスに割り当てられる KX II-101-V2 の IP アドレス

コマンドのオプション	説明
mask subnetmask	IP 管理者から取得したサブネット マスク
gw ipaddress	IP 管理者から取得したゲートウェイ IP アドレス
mode <auto 100fdx>	Ethernet モードを auto に設定して、100 Mbps 全二重 (100fdx) を検出または強制します。

Interface コマンドの例

次のコマンドは、IP アドレス、マスク、ゲートウェイ アドレスを設定し、モードを自動検出に設定します。

```
Admin Port > Config > Network > interface ipauto none
ip 192.168.50.12 mask 255.255.255.0 gw 192.168.51.12
mode auto
```

Listports コマンド

Listports コマンドは、アクティブなユーザ数、ユーザ名、ポート、およびステータスを一覧表示します。

Listports コマンドの例

```
Admin Port > listports
Port Port                Port Port  Port
No.  Name                    Type Status Availability
1 - Dominion_KXII-101_V2_Port KVM  up      idle
```

Userlist コマンド

Userlist コマンドは、ポート、ポート名、ポート タイプ、ポート ステータス、およびポートの可用性を一覧表示します。

Userlist コマンドの例

```
Admin Port > Userlist
Active user number:1
User Name | From      | Status
-----
-
admin     | Admin Port | active
```

Ch 12 CC Unmanage

この章の内容

概要.....	180
CC-SG 管理から KX II-101-V2 を除外する	181
プロキシ モードでの CC-SG の使用	182

概要

KX II-101-V2 デバイスが CommandCenter Secure Gateway の管理下にあるとき、KX II-101-V2 リモート コンソールを使用してデバイスに直接アクセスを試みると、次のメッセージが表示されます (有効なユーザ名とパスワードの入力後)。

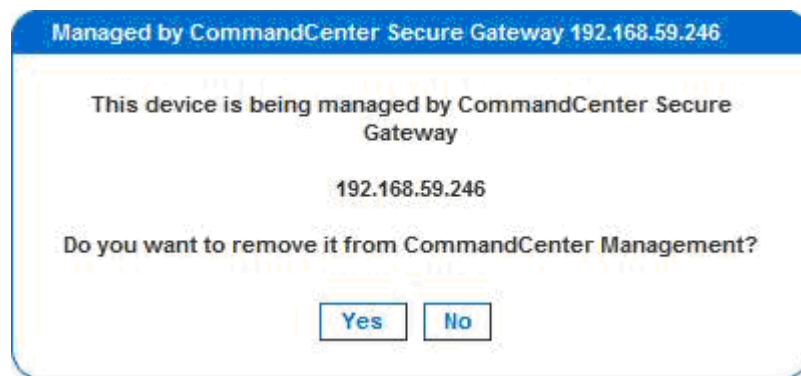


CC-SG 管理から KX II-101-V2 を除外する

CC-SG の制御対象から KX II-101-V2 を除外しない限り、デバイスには直接アクセスできません。ただし、CommandCenter からのハートビートメッセージを KX II-101-V2 で受信しない場合 (CommandCenter がネットワーク上に存在しない場合など) は、CC-SG の制御対象から KX II-101-V2 を除外してデバイスにアクセスできます。これは、CC Unmanage 機能を使用することで行えます。

注: この機能を使用するには、メンテナンス許可が必要です。

ハートビートメッセージを受信していない場合にデバイスに直接アクセスを試みると、次のメッセージが表示されます。

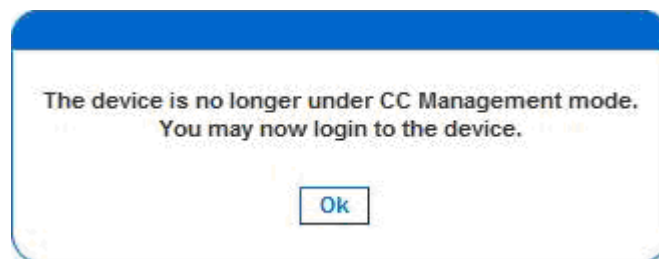


▶ **CC-SG 管理からデバイスを除外する (CC Unmanage を使用する) には、以下の手順に従います。**

1. [Yes] (はい) をクリックします。操作を確認するプロンプトが表示されます。



2. [Yes] (はい) をクリックします。CC の管理対象からのデバイスの除外を確認するメッセージが表示されます。



3. [OK] をクリックします。KX II-101-V2 ログイン ページが開きます。

プロキシ モードでの **CC-SG** の使用

Virtual KVM Client バージョンが CC-SG プロキシ モードで認識されない

Virtual KVM Client を CommandCenter Secure Gateway (CC-SG) からプロキシ モードで起動すると、Virtual KVM Client バージョンが認識されません。[About Raritan Virtual KVM Client] (バージョン情報) ダイアログ ボックスに、バージョンは「Version Unknown (不明なバージョン)」と表示されます。

プロキシ モードと MPC

KX II-101-V2 を CC-SG 管理下で使用していて、Multi-Platform Client (MPC) の使用を計画している場合は、CC-SG プロキシ モードを使用しないでください。

この章の内容

KX II-101-V2 の仕様	183
サポートされているビデオ解像度	184
サポートされているキーボード言語	185
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)	186
サポートされているブラウザ	188
認定モデム	188
コネクタ	188
使用される TCP ポートおよび UDP ポート	189
Network Speed Settings	191
9 ピンのピン配列	192

KX II-101-V2 の仕様

仕様	説明
フォーム ファクタ	Zero U フォーム ファクタ。ラックに縦または横に取り付け可能 (ブラケット キット付属)。
寸法 (DxWxH)	2.8" x 0.9" x 3.74" (71 mm x 24 mm x 95 mm)
重量	0.42 lbs (0.19 kg)
電源	単一電源 100 ~ 240 Vac、47 ~ 63Hz、0.2 A
使用温度	0° ~ 40°C (32° ~ 104°F)
湿度	20% ~ 85% RH
インジケータ: • ネットワーク ポート	• ネットワーク アクティビティおよび接続速度インジケータ
リモート接続: • ネットワーク プロトコル	• 10/100 Ethernet (RJ45) ポート x 1 • TCP/IP、HTTP、HTTPS、UDP、RADIUS、LDAP、SNTP、DHCP
画面解像度: • PC グラフィック モード • Sun™ ビデオ モード	• 720x400 (DOS) • 640 X 480 @ 60/72/75/85Hz、 • 800 X 600 @ 56/60/72/75/85Hz、 • 1024 X 768 @ 60/70/75/85Hz、

仕様	説明
ド	<ul style="list-style-type: none"> • 1152 X 864 @ 60/75Hz、 • 1280 X 1024 @ 60Hz、 • 1600 X 1200 @ 60Hz
認定	sUL/CUL、FCC Class A、CB、CE Class A、VCCI Class A

サポートされているビデオ解像度

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-101-V2 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。

KX II-101-V2 は、以下の解像度をサポートしています。

解像度		
640x350、70 Hz	720x400、85 Hz	1024x768、90 Hz
640x350、85 Hz	800x600、56 Hz	1024x768、100 Hz
640x400、56 Hz	800x600、60 Hz	1152x864、60 Hz
640 x 400、84 Hz	800x600、70 Hz	1152x864、70 Hz
640 x 400、85 Hz	800x600、72 Hz	1152x864、75 Hz
640x480、60 Hz	800x600、75 Hz	1152x864、85 Hz
640x480、66.6 Hz	800x600、85 Hz	1152x870、75.1 Hz
640x480、72 Hz	800x600、90 Hz	1152 x 900、66 Hz
640x480、75 Hz	800x600、100 Hz	1152 x 900、76 Hz
640x480、85 Hz	832 x 624、75.1 Hz	1280 x 960、60 Hz
640x480、90 Hz	1024x768、60 Hz	1280x960、85 Hz
640x480、100 Hz	1024x768、70 Hz	1280x1024、60 Hz
640x480、120	1024x768、72	1280x1024、75

解像度		
Hz	Hz	Hz
720 x 400、70 Hz	1024x768、75 Hz	1280x1024、85 Hz
720 x 400、84 Hz	1024x768、85 Hz	1600 x 1200、60 Hz

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。

サポートされているキーボード言語

次の表に、各言語に対して KX II-101-V2 でサポートされているキーボードを示します。

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)

言語	地域	キーボード レイアウト
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 (スウェーデン)	スウェーデン	スウェーデン語 (スウェーデン)
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

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。ローカルに保存されている ISO イメージである Remote File Server を、ターゲット サーバに直接マウントできます。
Red Hat Desktop 4.0	はい。ローカルに保存されている ISO イメージである Remote File Server を

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
	、ターゲット サーバに直接マウントできます。
openSUSE 10、11	はい。ローカルに保存されている ISO イメージである Remote File Server を、ターゲット サーバに直接マウントできます。
Fedora® 8 ~ 11	はい。ローカルに保存されている ISO イメージである Remote File Server を、ターゲット サーバに直接マウントできます。
Mac® OS	いいえ
Solaris™	いいえ

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®	<ul style="list-style-type: none"> Internet Explorer® 6.0 SP1 以降、IE 7、IE 8 Firefox® 1.06 ~ 3 	
	Windows Server 2003®	<ul style="list-style-type: none"> Internet Explorer 6.0 SP1 以降、IE 7、IE 8 Firefox 1.06 ~ 3 	
	Windows Vista®	<ul style="list-style-type: none"> Internet Explorer 7.0 または 8.0 	
	Windows 7®	<ul style="list-style-type: none"> Internet Explorer 7.0 または 8.0 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	
	Windows XP Professional®		<ul style="list-style-type: none"> Internet Explorer 6.0 SP1 以降、7.0、または
	Windows XP Tablet®		

モード	オペレーティング システム	ブラウザ
	Windows Vista	8.0
	Windows Server 2003	64 ビット OS 対応の 64 ビット版ブラウザ
	Windows Server 2008	
	Windows 7	
		<ul style="list-style-type: none"> Firefox 1.06 ~ 3 Internet Explorer 7.0 または 8.0

サポートされているブラウザ

KX II-101-V2 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、7、および 8
- Firefox® 1.5、2.0、および 3.0 (ビルド 3.0.10 まで)
- Safari®
- Safari® 2.0

認定モデム

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

コネクタ

インタフェース タイプ	長さ		説明
	インチ	センチメートル	
KVM ケーブル (PS/2 および USB 付き)	15"	38 cm	統合ケーブル
ミニ Din9(M) - DB9(F)	72"	182 cm	シリアル用ケーブル
DKX2-101-SPDUC (オプション)	70.86"	180 cm	Dominion PX への接続用ケーブル

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」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-101-V2 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」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-101-V2 (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 (例: CommandCenter Secure Gateway (CC-SG)) 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 『106p. の "[Network Settings] (ネットワーク設定)" 参照』」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-101-V2 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-101-V2 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-101-V2 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)
RADIUS アカウンティング、ポート 1813 (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-101-V2 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-101-V2 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-101-V2 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)。


Network Speed Settings


KX II-101-V2 network speed setting					
Network switch port setting	Auto	100/Full	100/Half	10/Full	10/Half
Auto	Highest Available Speed	KX II-101-V2: 100/Full Switch: 100/Half	100/Half	KX II-101-V2: 10/Full Switch: 10/Half	10/Half
100/Full	KX II-101-V2: 100/Half Switch: 100/Full	100/Full	KX II-101-V2: 100/Half Switch: 100/Full	No Communication	No Communication
100/Half	100/Half	KX II-101-V2: 100/Full Switch: 100/Half	100/Half	No Communication	No Communication
10/Full	KX II-101-V2: 10/Half Switch: 10/Full	No Communication	No Communication	10/Full	KX II-101-V2: 10/Half Switch: 10/Full
10/Half	10/Half	No Communication	No Communication	KX II-101-V2: 10/Full Switch: 10/Half	10/Half


Legend:

 Does not function as expected

 Supported

 Functions; not recommended

 NOT supported by Ethernet specification; product will communicate, but collisions will occur

 Per Ethernet specification, these should be “no communication,” however, note that the KX II-101-V2 behavior deviates from expected behavior

Note: For reliable network communication, configure the KX II-101-V2 and the LAN switch to the same LAN Interface Speed and Duplex. For example, configure both the KX II-101-V2 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100MB/s/Full.

9 ピンのピン配列

ピン定義	
1	DTR (出力)
2	TXD (出力)
3	RXD (入力)
4	DCD/DSR (入力) *
5	GND
6	DTR (出力)
7	CTS (入力)
8	RTS (出力)
9	RI (入力)

Note: The procedures in this chapter should be attempted only by experienced users.

この章の内容

ユーザ グループ情報を返す.....	193
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 ..	194
新しい属性を作成する.....	194
属性をクラスに追加する	195
スキーマ キャッシュを更新する	197
ユーザ メンバの rciusergroup 属性を編集する.....	198

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 から返す場合

LDAP/LDAPS 認証に成功すると、KX II-101-V2 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。

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。

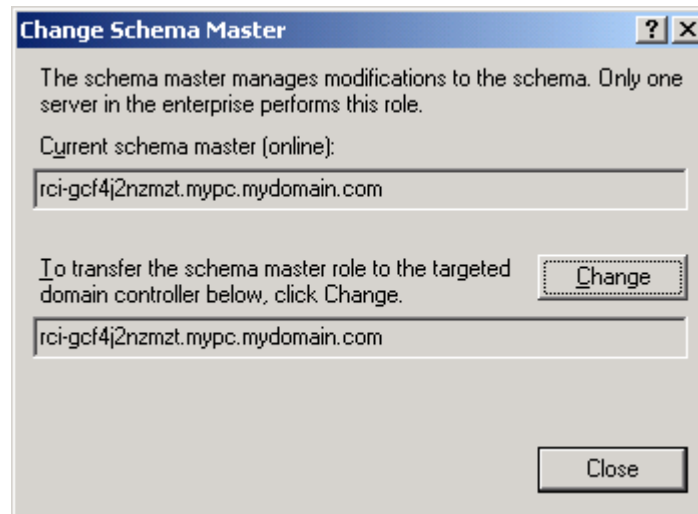
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

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。

- 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。

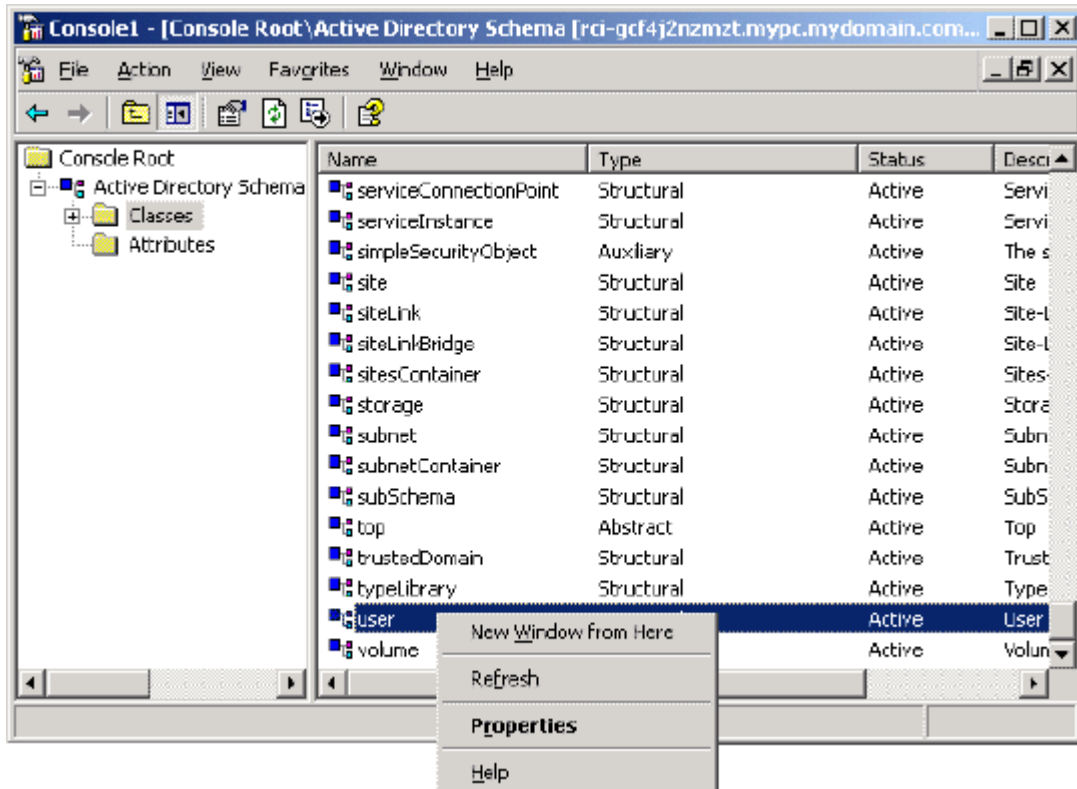
- [Common Name]** (共通名) ボックスに「rciusergroup」と入力します。
- [LDAP Display Name]** (LDAP 表示名) ボックスに「rciusergroup」と入力します。
- [Unique X500 Object ID]** (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
- [Description]** (説明) ボックスにわかりやすい説明を入力します。
- [Syntax]** (構文) ボックスの一覧で **[Case Insensitive String]** (大文字/小文字の区別がない文字列) を選択します。
- [Minimum]** (最小) ボックスに「1」と入力します。
- [Maximum]** (最大) ボックスに「24」と入力します。
- [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

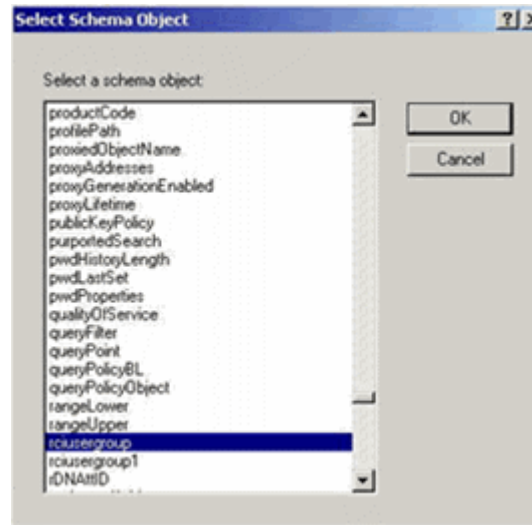
- ウィンドウの左ペインで **[Classes]** (クラス) をクリックします。

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

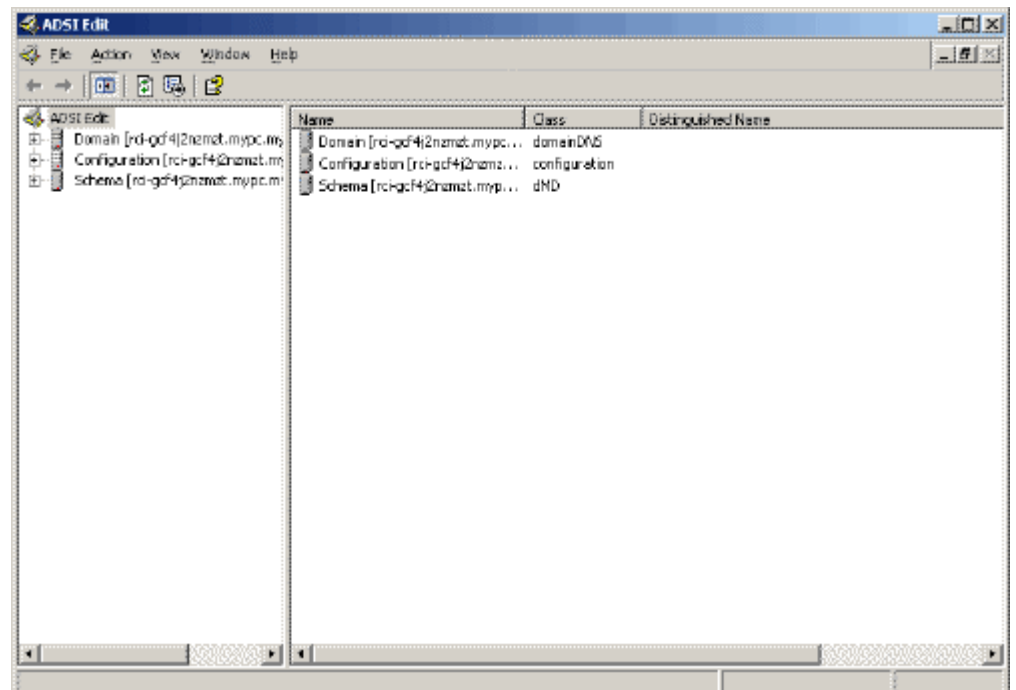
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

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。

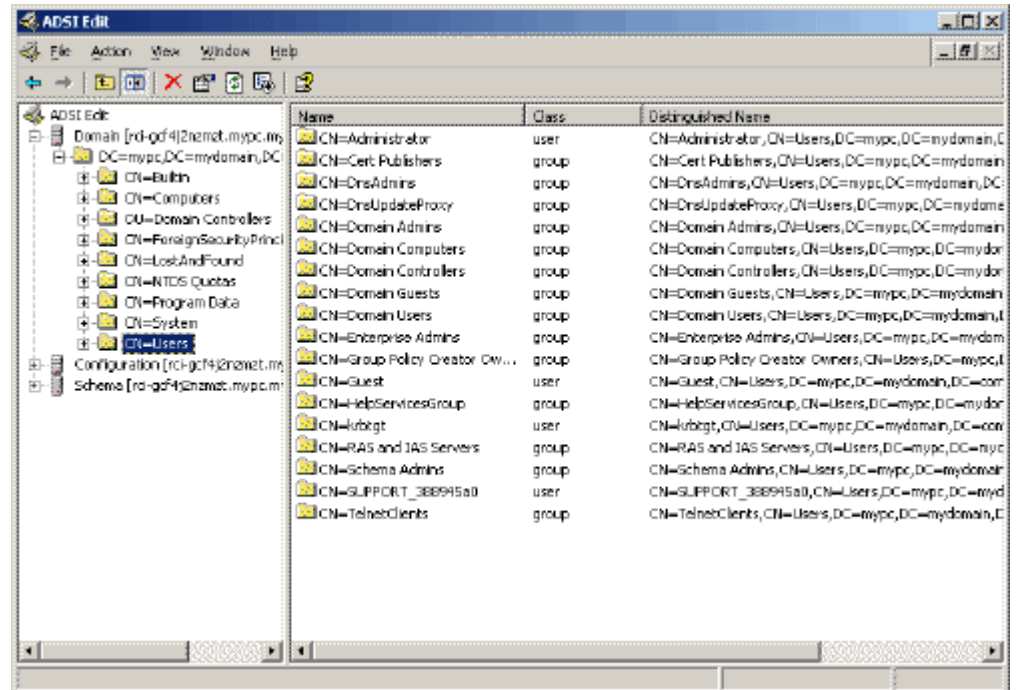
▶ **rciusergroup** グループ内の個別のユーザ属性を編集するには、以下の手順に従います。

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。



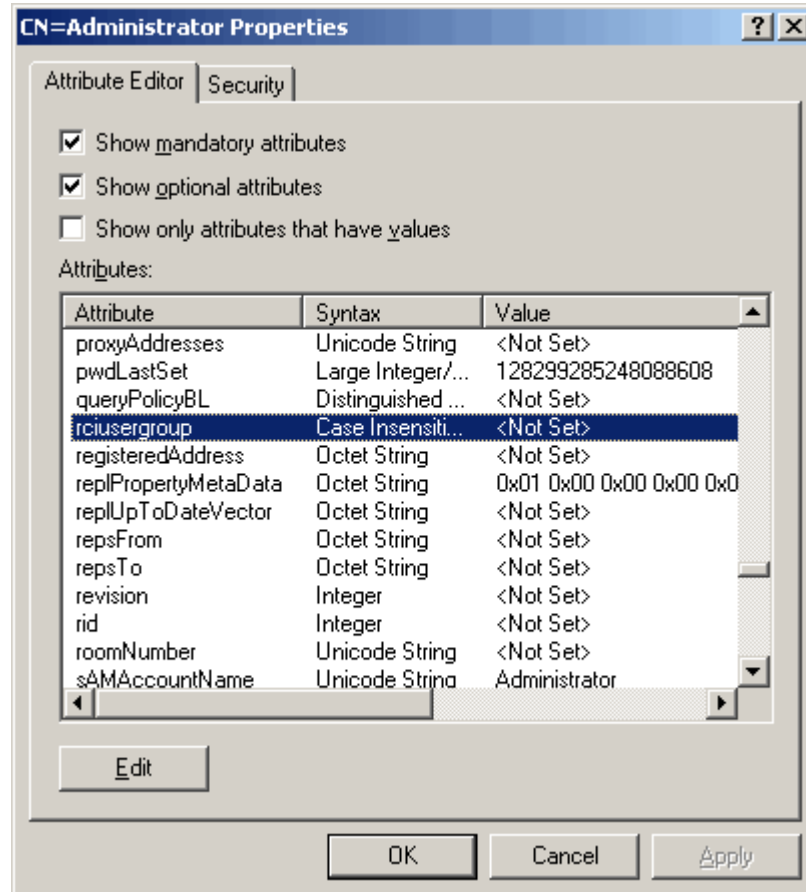
4. [Domain] (ドメイン) を開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

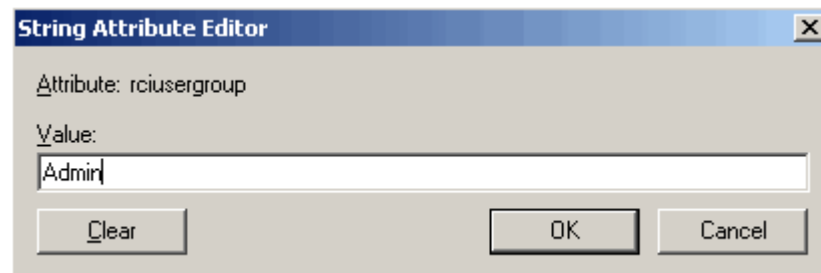


6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキストメニューの [Properties] (プロパティ) をクリックします。

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-101-V2 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。



KX II-101-V2 デバイスは、サーバ ラックのいずれの側にも縦または横、前向きまたは後ろ向きに取り付けることができます。KX II-101-V2 キットに付属のブラケットとネジを使用します。

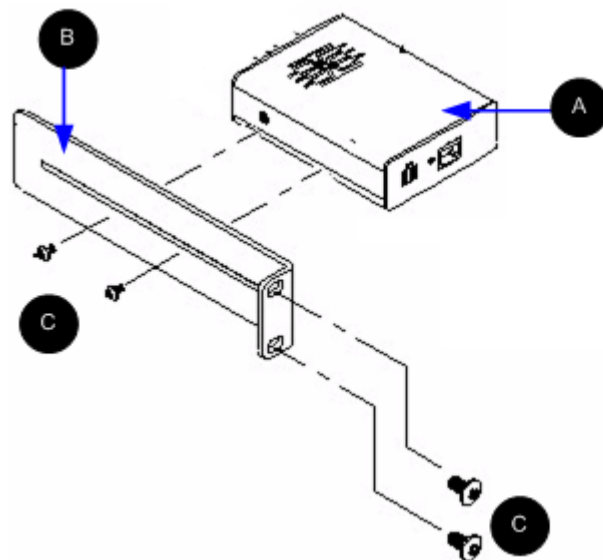
この章の内容

横取り付け用 L ブラケットを KX II-101-V2 に取り付ける.....201

横取り付け用 L ブラケットを KX II-101-V2 に取り付ける

1. 付属のネジを使用して L ブラケットを KX II-101-V2 に取り付けます。ネジを締め付ける前にブラケットの位置を調整します。
2. ラック取り付けネジ (ラック メーカー提供品) を使用して L ブラケット アセンブリをラックに取り付けます。

次の図では、KX II-101-V2 を左側に取り付けています。KX II-101-V2 を右側に取り付けるには、ブラケットを KX II-101-V2 の右側に取り付けることを除き、上記の指示に従います。



図の説明	
A	KX II-101-V2
B	L ブラケット

Ap B: ラック マウント

図の説明	
	ネジ

この章の内容

Java Runtime Environment (JRE)	203
キーボード、ビデオ、およびマウスに関するメモ	203

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 およびシリアル アクセス クライアント ユーザ ガイド』を参照してください。

KX II-101-V2 リモート コンソールおよび MPC を使用する場合は、Java Runtime Environment™ (JRE™) が必要です。KX II-101-V2 リモート コンソールで Java のバージョンがチェックされます。バージョンが不適切な場合または古い場合は、適合するバージョンをダウンロードするように求められます。

最適なパフォーマンスを得るには、JRE バージョン 1.6 を使用することをお勧めしますが、KX II-101-V2 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で KX II-101-V2 リモート コンソール (Virtual KVM Client) を使用するには、多言語バージョンの JRE をインストールしてください。

キーボード、ビデオ、およびマウスに関するメモ

次の機器には、キーボード、ビデオ、またはマウスの特定の制限が適用されます。必要に応じて、回避策が提供されます。

Sun Blade ビデオ、キーボード、およびマウスのサポート制限

ビデオ

KX II-101-V2 で Sun™ Blade 100 にアクセスしている場合は、Sun Blade の起動中にローカル ポートでのビデオやリモート接続が正しく機能しないことがあります。この問題を回避するには、必ず Sun Open Boot ファームウェア 4.17.1 以降を使用してください。

キーボードおよびマウス

Sun Blade では複数のキーボードがサポートされておらず、キーボードまたはマウス用のローカル ポートが用意されていないので、KX II-101-V2 およびローカル キーボードを同時に使用することはできません。ただし、Sun Blade のリモート キーボードおよびマウスは使用できます。

Sun キーボードのキー サポートの制限

Sun™ キーボードの以下のキーは、KX II-101-V2 でサポートされていません。

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
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

ローカル キーボードからの BIOS アクセスの制限

ずれないマウス (Absolute Mouse Synchronization) を使用する場合は、USB 接続が必要です。ただし、ここで説明するキーボードは、ローカル キーボードに USB 接続することはできません。ローカル ポート経由で BIOS または仮想メディアを介してローカル キーボードにアクセスするには、以下の設定に従います。

キーボード	使用する設定
Dell® OptiPlex™ GX280 - BIOS A03	ローカル キーボードおよびリモート キーボードに対する BIOS や仮想メディアには、Newlink USB - PS/2 アダプタを使用してアクセスできません。 [Keyboard/Mouse Setup] (キーボード/マウス設定) ページで [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定します。詳細については、「 キーボード/マウス設定 『112p.』 」を参照してください。
Dell Dimension 2400– BIOS A05	[Keyboard/Mouse Setup] (キーボード/マウス設定) ページで [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定します。詳細については、「 キーボード/マウス設定 『112p.』 」を参照してください。
Dell Optiplex 170L - BIOS A07	PS/2 および PS/2 - USB アダプタ。 [Keyboard/Mouse Setup] (キーボード/マウス設定) ページで [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定します。詳細については、「 キーボード/マウス設定 『112p.』 」を参照してください。
Dell Server 1850	BIOS バージョン A06 で、リムーバブル USB フラッシュ ドライブがマウントされている仮想メディアを認識できるように、Dell サーバと KX II-101-V2 の間に PS/2 接続や USB 接続を使用します。 [Keyboard/Mouse Setup] (キーボード/マウス設定) ページで [Host Interface] (ホスト インタフェース) を [PS/2] (PS/2) に設定します。詳細については、「 キーボード/マウス設定 『112p.』 」を参照してください。

HP UX RX 1600 キーボードおよびマウスの設定

UNIX® を実行している HP® UX RX 1600 を使用している場合は、以下を実行して、デバイスをターゲットに接続します。

- KX II-101-V2 ファームウェア 2.0.20.5.6964 以上を使用していることを確認します。
- KX II-101-V2 に付属している USB ケーブルを使用します。
- [Keyboard/Mouse Setup] (キーボード/マウス設定) ページの [Host Interface] (ホスト インタフェース) フィールドを [USB] (USB) に設定します。詳細については、「**キーボード/マウス設定** 『112p.』」を参照してください。
- [Port] (ポート) ページの [Enable Absolute Mouse] (ずれないマウスを有効にする) と [Use Full Speed] (フル スピードを使用) のチェックボックスがオンになっていないことを確認します。詳細については、「[Port Configuration] (ポート設定)」を参照してください。
- インテリジェント マウス モードまたは標準マウス モードを使用します。ずれないマウス モードは使用しないでください。

Compaq Alpha および IBM P Server のマウス モードの制限

KX II-101-V2 を介して Compaq® Alpha サーバまたは IBM® P Server を接続する場合は、シングル マウス モードを使用する必要があります。詳細については、「**ターゲット サーバを操作する** 『34p.』」を参照してください。

Windows 2000 および Windows 2003 Server のキーボードの制限

オペレーティング システムの制限のために、Windows 2000® オペレーティング システムおよび Windows 2003® Server を使用する場合、US インターナショナル キーボード レイアウトでは、以下のキーボードの組み合わせは機能しません。

- 右 Alt+D
- 右 Alt+I
- 右 Alt+L

注: 右 Alt は、特にキーの表記が US/インターナショナルになっているキーボードでは、AltGr というラベルになっている場合があります。

質問	回答
Dominion KX2-101 と Dominion KX2-101-V2 の違いは何ですか？	Dominion KX II-101-V2 は、 KX II-101 製品ファミリーの新しい低価格モデルです。V2 では、既存の KX2-101 のほぼすべての機能をサポートしていますが、 Power-over-Ethernet も PS/2 ローカルポートもサポートしていません。
Dominion KX II-101 はどのように動作しますか？	Dominion KX II-101 は、サーバのキーボード、ビデオ、マウスの各ポートに接続し、リモートクライアント PC に送信する前に、 Raritan の多彩な機能のフレームグラバおよび圧縮技術を使用してビデオ信号のキャプチャ、デジタル化、および圧縮を行います。 Dominion KX II-101 では、わかりやすいユーザ インタフェースを介して豊富な機能を実現しています。また、 CommandCenter® SecureGateway を介して他の管理デバイスで集中管理することもできます。
Dominion KX II-101 では、どのタイプのコンピュータをリモートで制御できますか？	Dominion KX II-101 は、ターゲット サーバのハードウェア、オペレーティング システム、アプリケーション ソフトウェアにかかわらずに機能し、ターゲット サーバの主要な入出力デバイス (キーボード、ビデオ、およびマウス) へのアクセスを実現します。したがって、 PC のキーボードとマウスの標準インタフェースをサポートするハードウェア、および PC の標準のビデオ (VGA) を Dominion KX II-101 で使用できます。

質問	回答
Dominion KX2-101 と Dominion KX2-101-V2 の違いは何ですか？	Dominion KX II-101-V2 は、KX II-101 製品ファミリの新しい低価格モデルです。V2 では、既存の KX2-101 のほぼすべての機能をサポートしていますが、Power-over-Ethernet も PS/2 ローカルポートもサポートしていません。
リモートからターゲットサーバに無断で接続できないようにするセキュリティ機能はありますか？	同期できます。KX II-101 には、数多くのセキュリティレイヤ (リモートセッション中の接続認証、データ転送セキュリティなど) が用意されています。ユーザ名、パスワード、プライベートキーは、ユーザの認証に使用されます。 Dominion KX101 では、Dominion KX101 上にローカルに存在するデータベースに対して、または外部の AAA サーバ (LDAP、Active Directory、または RADIUS) に対してユーザを認証できます。キーボード、ビデオ、およびマウスのすべてのデータは、最大 256 ビットの AES に暗号化されます。
Dominion KSX 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？	KX II-101 では、内蔵または USB 接続された CD ドライブと DVD ドライブ、USB マスストレージデバイス、PC のハードディスク、リモートドライブイメージなどがサポートされています。
仮想メディアは安全ですか？	同期できます。仮想メディアのセッションは、256 ビットの AES 暗号化によって保護されます。
どの KX II-101 モデルを購入したらよいでしょうか？	Power over Ethernet を必要とするお客様、PS2 ローカルポートを必要とするお客様、または初代の KX II-101 との互換性を求めるお客様は、初代の KX II-101 を購入してください。 それ以外のお客様は、新しい低価格の KX II-101 V2 を購入してください。

索引

[

- [Audit Log] (監査ログ) - 153
- [Authentication Settings] (認証設定) - 93
- [Auto-sense Video Settings] (ビデオ設定の自動感知) - 57
- [Backup and Restore] (バックアップと復元) - 155
- [Configuration] (設定) - 176
- [Connection Properties] (接続プロパティ) - 48
- [Debug] (デバッグ) - 174, 175
- [Device Diagnostics] (デバイス診断) - 168
- [Device Information] (デバイス情報) - 154
- [Device Services] (デバイス サービス) - 109
- [Encryption & Share] (暗号化および共有) - 146
- [Event Management - Destinations] (イベント管理 - 送信先) - 119
- [Factory Reset] (ファクトリ リセット) - 160
- [Favorites List] (お気に入りリスト) ページ - 41, 42
- [IP Access Control] (IP アクセス制御) - 149
- [Keyboard Macros] (キーボード マクロ) - 51
- [Login Limitations] (ログイン制限) - 140, 141
- [Manage Favorites] (お気に入りの管理) ページ - 40
- [Network Interface] (ネットワーク インタフェース) ページ - 163
- [Network Settings] (ネットワーク設定) - 106, 190
- [Network Statistics] (ネットワーク統計) ページ - 164
- [Ping Host] (ホストへの Ping) ページ - 166
- [Port Access] (ポート アクセス) ページ - 37
- [Port Configuration] (ポート設定) - 123
- [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 - 61
- [Security Settings] (セキュリティ設定) - 140
- [Serial Port Settings] (シリアル ポート設定) - 113
- [Strong Passwords] (強力なパスワード) - 105, 140, 142
- [Tools] (ツール) オプション - 66

- [Trace Route to Host] (ホストへの経路をトレースする) ページ - 167
- [User Blocking] (ユーザ ブロック) - 93, 140, 144
- [User Group List] (ユーザ グループ リスト) - 84
- [User List] (ユーザ リスト) - 91

9

- 9 ピンのピン配列 - 192

A

- A
 - 電源 - 22
- Absolute (ずれない) マウス モード - 66
- Apple Macintosh の設定 - 19

B

- B
 - ターゲット サーバ - 22

C

- C
 - ネットワーク - 25
- CC Unmanage - 180
- CC-SG ユーザへの注意事項 - 30
- CC-SG 管理から KX II-101-V2 を除外する - 181
- CD-ROM/DVD-ROM/ISO イメージ - 80
- CLI コマンド - 170, 174
- CLI の画面操作 - 172
- CLI プロンプト - 172
- CLI を使用しての KX II-101-V2 へのアクセス - 171
- CLI 構文
 - ヒントとショートカット キー - 173
- Compaq Alpha および IBM P Server のマウス モードの制限 - 206
- Configuring Event Management - Settings - 118, 119

D

- D

索引

管理ポート - 26
Diagnostics - 174, 175

E

E
ローカル ユーザ ポート - 26

F

FAQ - 207

H

HP UX RX 1600 キーボードおよびマウスの設定 - 206

I

IBM AIX の設定 - 20
Interface コマンド - 177
IP アドレスの割り当て - 27

J

Java Runtime Environment (JRE) - 203

K

KVM ターゲット サーバの切断 - 47
KVM ターゲット サーバへの接続 - 45
KVM ターゲット サーバを管理する ([Port]
(ポート) ページ) - 125, 127
KX II-101-V2 コンソールでの案内 - 36
KX II-101-V2 サブネット上の Raritan デバイ
スを検出する - 42
KX II-101-V2 の概要 - 2
KX II-101-V2 の仕様 - 183
KX II-101-V2 への SSH 接続 - 171
KX II-101-V2 ヘルプ - 1
KX II-101-V2 リモート コンソール インタフ
ェース - 35

L

LAN インタフェース設定 - 106, 109
LDAP から返す場合 - 193
LDAP/LDAPS リモート認証を実装する - 94
Linux の設定 (Red Hat 4) - 17
Linux の設定 (Red Hat 9) - 15
Listports コマンド - 174, 178

M

Microsoft Active Directory から返す場合 - 193
Microsoft Active Directory についての注意事
項 - 30
Multi-Platform Client (MPC) - 44

N

Name コマンド - 175, 177
Network Speed Settings - 109, 191

P

Port Action Menu - 37
Power Control - 124, 127
Prerequisites for Using Virtual Media - 75, 77
PS/2 の設定 - 24

R

RADIUS リモート認証の実装 - 99
RADIUS 通信交換仕様 - 102
Raritan の電源タップ制御 - 113

S

Setlog コマンド - 175, 176
SSH を有効にする - 110
Sun Blade ビデオ、キーボード、およびマウス
のサポート制限 - 204
Sun Solaris の設定 - 18
Sun キーボードのキー サポートの制限 - 204
Sun ビデオ解像度 - 10

T

Telnet を有効にする - 110

U

UNIX/Linux ワークステーションからの SSH
アクセス - 172
Updating the LDAP Schema - 98, 193
URL を介してダイレクト ポート アクセスを
有効にする - 111
USB の設定 - 23
USB 接続の詳細設定 - 138
USB 接続を管理する - 135
USB 接続設定 - 137
User Management - 31, 83

Userlist コマンド - 175, 179

V

Virtual KVM Client (VKC) - 37, 44

Virtual Media - 66, 72

VKC 仮想メディア - 66

W

Windows 2000 および Windows 2003 Server
のキーボードの制限 - 206

Windows 2000 の設定 - 14

Windows PC からの SSH アクセス - 171

Windows Vista の設定 - 13

Windows XP、Windows 2003、および
Windows 2008 の設定 - 11

あ

アップグレード履歴 - 159

アナログ KVM スイッチ - 112, 132

イベント管理 - 117

インストールと設定 - 7, 177

インタフェース - 4, 35

インテリジェント マウス モード - 65

お気に入りの管理 - 39

お気に入りを追加、編集、削除する - 43

か

キーボード マクロの作成 - 54

キーボード マクロの実行 - 56

キーボード マクロの変更および削除 - 56

キーボード マクロをインポート/エクスポートする - 51

キーボード、ビデオ、およびマウスに関するメモ - 203

キーボード/マウス設定 - 112, 132, 205, 206

キーボードのオプション - 51

グループベースの IP ACL (アクセス制御リスト) - 87

コネクタ - 188

コマンド ライン インタフェース (CLI) - 113, 170

コマンドのオート コンプリート - 173

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 - 147, 149

さ

サーバ ビデオ解像度を設定する - 9, 10

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) - 186

サポートされているキーボード言語 - 185

サポートされているビデオ解像度 - 184

サポートされているブラウザ - 188

サポートされているプロトコル - 30

システム管理機能 - 4

スキーマ キャッシュを更新する - 197

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 - 194

すべてのコマンド ライン インタフェース レベルに共通のコマンド - 174

セキュリティ管理 - 140

た

ターゲット サーバに名前を付ける - 29

ターゲット サーバの電源管理 - 46

ターゲット サーバを操作する - 35, 206

ターミナル エミュレーション プログラムを使用して KX II-101-V2 を設定する (オプション) - 8, 26, 31, 172

ダイレクト ポート アクセスを有効にする - 35

ツール バー - 45

デバイス管理 - 106

デフォルトのログイン情報 - 7

な

ネットワーク - 175, 177

ネットワーク基本設定 - 106, 107

ネットワーク設定 - 4

は

はじめに - 1

パスワードの変更 - 105

パッケージの内容 - 6

ビデオのプロパティ - 57

ビデオ解像度 - 5

ビデオ設定を調整する - 58

ファームウェアをアップグレードする - 157

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) - 76

索引

プロキシ モードでの CC-SG の使用 - 182
ヘルプのオプション - 71
ポートの名前を変更する - 125
ポート許可の設定 - 86

ま

マウス オプション - 62
マウス ポインタの同期 - 63
マウスの設定 - 11
モデム - 114
モデム アクセス ケーブル接続 - 115

や

ユーザ - 90
ユーザ グループ - 83
ユーザ グループおよびユーザを作成する - 31
ユーザ グループ情報を Active Directory サーバから返す - 98
ユーザ グループ情報を RADIUS 経由で返す - 101
ユーザ グループ情報を返す - 193
ユーザ ブロックとブロック解除 - 93
ユーザ メンバの rcigroup 属性を編集する - 198
ユーザとグループの関係 - 84
ユーザ機能 - 5
ユーザ認証プロセス - 103

ら

ラック マウント - 201
リセット ボタンを使用して KX II-101-V2 をリセットする - 134
リモート コンソールを使用して KX II-101-V2 を設定する - 26
リモート認証 - 30
ローカル キーボードからの BIOS アクセスの制限 - 205
ローカル サブネット上の Raritan デバイスを検出する - 41
ローカル ドライブ - 78
ログアウト - 44
ログインする - 172

漢字

横取り付け用 L ブラケットを KX II-101-V2 に取り付ける - 201
仮想メディアの使用 - 77
仮想メディアの切断 - 78, 82
仮想メディアへの接続 - 78
画面を更新する - 57
概要 - 7, 44, 73, 136, 170, 180
管理の特長 - 4
管理ポート - 113
関連文書 - 1
既存のユーザ グループの変更 - 90, 92
許可の設定 - 89
検出ポートを入力する - 111
個別グループの許可を設定する - 89
再起動 - 161
最大垂直走査周波数の変更 - 62
仕様 - 183
使用される TCP ポートおよび UDP ポート - 189
取り付け - 5
手順 1
 ターゲット サーバの設定 - 7, 8
手順 2
 ネットワーク ファイアウォールの設定 - 7, 20
手順 3
 装置の接続 - 7, 21
手順 4
 KX II-101-V2 の設定 - 7, 26
情報メモ - 203
新しいパスワードの設定 - 27
新しい属性を作成する - 194
新規ユーザ グループを追加する - 85
新規ユーザを追加する - 91, 92
診断 - 162
製品の写真 - 3
製品の特長 - 4
接続情報 - 50
属性をクラスに追加する - 195
電源 - 5
電源タップ デバイスを管理する - 131
電源タップに名前を付ける (電源タップの [Port] (ポート) ページ) - 127, 129

電源タップを接続する - 127
電源の関連付けを管理する - 130
読み取り/書き込み可能に設定できない状況 -
79
日付/時刻の設定 - 116
入門 - 8
認定モデム - 115, 188
標準マウス モード - 64
表示オプション - 70
保守 - 153
用語 - 5

▶ 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 :+81-3-3523-5991
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