



Dominion KX II-101

ユーザ ガイド

リリース **2.0**

Copyright © 2008 Raritan, Inc. KX2101-0A-J 2008 年 2 月 255-62-4031-00 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 2008 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ので、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。

CE CUUS 1F61 LISTED

目次

Dominion KX II-101 の概要	
製品の写真	
製品の特長	
インタフェース	
ネットワーク設定	
システム管理機能	
管理の特長	
ユーザ機能	
電源	
ビデオ解像度	
取り付け	
パッケージの内容	
用語	
オプションのアクヤサリ	

重要な情報

ログイン	6
デフォルト IP アドレス	6
サービス パック	6

インストールと設定

ターゲット サーバの設定	7
サーバ ビデオ解像度の設定	
マウス モード	
KX II-101 の接続	
ターゲット サーバへの接続	
ネットワークへの接続	
KX II-101 への電源供給	
Admin ポートの使用	
ローカル ユーザ ポートの使用	
ネットワーク ファイアウォールの設定	
KX II-101 の設定	
リモート コンソールの使用	
ターミナル エミュレーション プログラムの使用	



6

iv

KX II-101 への接続

言語サポート	
Java Runtime Environment (JRE)	
KX II-101 の起動	
ダイレクト ポート アクセスの有効化	
KX II-101 コンソールのレイアウト	
KX II-101 コンソールでの案内	
KX II-101 リモート コンソールのメニュー マップ	
ログオフ	
お気に入りの管理	
[Manage Favorites] (お気に入りの管理) メニュー	
[Favorites List] (お気に入りリスト)	
[Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット)	
[Discover Devices - KX II-101 Subnet] (Discover Devices (デバイス検出)- KX II-101 リ	ŀブネ ッ
۲)	41
[Add New Favorite] (新しいお気に入りの追加)	
[Port Access] (ポート アクセス) ページ	

ユーザ、グループ、アクセス許可

ユーザ	44
グループ	44
ユーザとグループの関係	45
[User Management] (ユーザ管理)	45
[User Management] (ユーザ管理) メニュー	45
リモート認証	58
CC-SG ユーザへの注意事項	58
サポートされているプロトコル	58
Microsoft Active Directory についての注意事項	58
認証と認可	58
[Authentication Settings] (認証設定)	59
LDAP スキーマの更新	66

Virtual KVM Client

概要	77
オプション	
メニュー ツリー	
ツール バー	79
マウス ポインタの同期	80
マウス同期のヒント	
[Connection] (接続) メニュー	
[Properties] (プロパティ) ダイアログ ボックス	
[Connection Info] (接続情報)	
[Connection Info] (接続情報)	



76



仮想メディア

既要1	102
反想メディアを使用するための前提条件1	104
反想メディアの使用	105
<vm td="" セッションを開く1<=""><td>106</td></vm>	106
反想メディアへの接続1	107
ローカル ドライブ1	107
読み取り/書き込み可能に設定できない状況1	108
CD-ROM/DVD-ROM/ISO イメージ1	109



目次

仮想メディアの切断		
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).	

デバイス管理

113

[Device Settings] (デバイス設定) メニュー	
[Network Settings] (ネットワーク設定)	114
ネットワーク基本設定	115
LAN インタフェース設定	117
[Device Services] (デバイス サービス)	119
キーボード/マウスの設定	
[Serial Port Settings] (シリアル ポート設定)	
[Date/Time Settings] (日付/時刻の設定)	
イベント管理	
SNMP の設定	
Syslog の設定	
[Event Management - Destinations] (イベント管理 - 送信先)	
- SNMP エージェント設定	
SNMP トラップ設定	130
[Port Configuration] (ポート設定)	

電源制御

134

144

概要	
パワー ストリップの接続	
パワー ストリップの名前の指定 (パワー ストリップの [Port] (ポート) ページ)	
コンセントへの KVM ターゲット サーバの関連付け ([Port] (ポート) ページ)	
コンセントの関連付けの表示	
電源タップ デバイスの制御	

[Security Settings] (セキュリティ設定)



vii



166 概要......166 CLI を使用しての KX II-101 へのアクセス......167 Windows PC からの SSH アクセス......167 UNIX ワークステーションからの SSH アクセス......168 ログイン......168 コマンドの完成......169 CLI 構文 - ヒントとショートカット......170 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......170

コマンド ライン インタフェース(CLI)

[Device Information] (デバイス情報)......159 [Backup and Restore] (バックアップと復元)160 [Firmware Upgrade] (ファームウェアのアップグレード)162 アップグレード履歴......164 [Reboot] (再起動)......164

メンテナンス

[IP Access Control] (IP	アクセス制御)	

目次

Diagnostics

[Diagnostics] (診断) メニュー	176
[Network Interface] (ネットワーク インタフェース) ページ	
[Network Statistics] (ネットワーク統計) ページ	
[Ping Host] (ホストへの Ping) ページ	
[Trace Route to Host] (ホストへのトレース ルート) ページ	
[Device Diagnostics] (デバイス診断)	

CC Unmanage

概要	184
CC-SG 管理からの KX II-101 の除外	185
プロキシ モードでの CC-SG の使用	187

仕様

KX II-101	188
コネクタ	189
Raritan Remote Client ソフトウェア	189

ラック マウント

AC-DC アダプタ クリップ取り付け具	
クリップ タイプの識別	
AC-DC 電源アダプタからのアタッチメント カバーの取り外し	
AC-DC 電源アダプタへのクリップの取り付け	
ブラケットの取り付け	
KX II-101 ブラケット部品	
横に取り付ける KX II-101 にブラケットを取り付けます	
縦に取り付ける KX II-101 にブラケットを取り付けます	



184

188

176

はじめに

この章の内容

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

Dominion KX II-101 の概要

1

Dominion KX II-101 をご購入いただきありがとうございます。 KX II-101 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 ユニット内では、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 外付けで小型なサイズにより、ターゲット サーバ近くにインストールすることが容易に行え、各 KX II-101 ユニットは、独自の IP アドレスを持ちます。各ユニットは、Power-over-Ethernet (PoE) または外部の AC-DC パワー パック経由で電源が供給できます。

Dominion KX II-101 はスタンドアロン装置として操作ができ、また、Raritan の CommandCenter Secure Gateway (CC-SG) 管理アプライアンスを使用して、 別の Raritan アクセス製品と併用し単一の論理ソリューション内に統合することも できます。





- 1 KX II-101
- 2 LAN
- 3 Windows, Linux, Sun $\forall -N_{\circ}$
- 4 TCP/IP
- 5 LAN
- 6 リモート (Network) アクセス

製品の写真







製品の特長

インタフェース

- 組み付けの PS/2 KVM 接続ケーブル
- 制御および仮想メディア用に選択できる USB 接続
- 初期デバイス設定、診断、外部モデム アクセス用のシリアル管理ポート
- 10/100-base-T 自動検出、全二重をサポートする Ethernet LAN ポート
- LED ネットワーク アクティビティ インジケータとステータス
- バックライト LED によるパワー ON インジケータ

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
- 管理者設定可能な時刻またはネットワーク タイム プロトコル (NTP/SNTP) サーバとの同期
- 管理者で選択可能なローカル時刻情報付き管理者操作ログ SNMP V2 エ ージェント
- RADIUS および LDAP 認証プロトコルをサポート

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) 管理アプライア ンスとの統合



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 Share" 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
- ずれないマウス同期
- プラグ&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

- Class 2 Power-over-Ethernet (PoE) による電源供給
- 外部の AC-DC 電源アダプタによる代替電源

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、「*ラック マウント*『p. 190』」を参照してください。

パッケージの内容

- 各 KX II-101 ユニットには、次の物品が同梱されています。
- メイン ユニット KX II-101 KVM over IP
- USB タイプ A 対タイプ B ミニ コネクタ
- AC 電源アダプタ AC-DC 6VDC
- 海外での使用に応じた 3 つの追加の電源コンセント プラグ
- ミニ DIN DB9 シリアル ケーブル
- マウント ブラケット キット
- Raritan ユーザ マニュアル & クイック セットアップ ガイド CD-ROM
- クイック ステップ ガイド
- アプリケーション ノート (該当する場合)
- テクニカル ノート (該当する場合)



用語

ターゲット サーバ ト	X II-101	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 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、Solaris、Apple Macintosh® コンピュータ。
- 管理シリアル ポート KX II-101 は管理シリアル ポートを使用して準備されます。 付属のミニ DIN DB9 ケ ーブルを使用して、PC のシリアル ポートを KX II-101 ユニットの管理シリアル ポートに 接続します。 次に、標準のターミナル エミュレーション ソフトウェア (例、 HyperTerminal) 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の設定に利用されます。
- ローカル ユーザ ポート ターゲット サーバの直近にいるユーザが KX II-101 を取り外さないでサーバに接続されて いたキーボードとマウスを使用できるようにするポートです。
- 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。

オプションのアクセサリ

DB15 から PS/2 および VGA へのローカル ユーザ ケーブル
 詳細については、「コネクタ『p. 189』」を参照してください。



重要な情報

この章の内容

ログイン	6
デフォルト IP アドレス	6
サービス パック	6

ログイン

2

- KX II-101 のデフォルトのログイン ユーザ名は admin 、デフォルトのパスワー ドは raritan です。このユーザは、管理者特権を有します。
- 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。
- デフォルトのパスワード raritan は、すべて小文字で入力してください。
- セキュリティを確保するために、デフォルトのパスワードはできるだけ早く変更してく ださい。

デフォルト IP アドレス

KX II-101 は、出荷時に固定 IP アドレス (192.168.0.192) 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 シリアル管理コンソー ルまたは KX II-101 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 に割り当てる詳細につい ては、「IP アドレスの割り当て『p.21』」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詳細については、「*ローカル シリアル コンソー ルの使用*『p.25の"ターミナル エミュレーション プログラムの使用"参照先 』」を参 照してください。

サービス パック

 Microsoft Internet Explorer Version 5.01 または Windows 2000 と KX II-101 を使用する場合は Service Pack 4 (SP4) 以上にアップグレードす る必要があります。



インストールと設定

この章の内容

ターゲット サーバの設定	7
KX II-101 の接続	14
ネットワーク ファイアウォールの設定	19
KX II-101 の設定	19

ターゲット サーバの設定

3

この章では、KX II-101 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。

- 1. **ターゲット サーバの設定**『p.7』
- 2. *ネットワーク ファイアウォールの設定*『p. 19』
- 3. KX II-101 の接続『p. 14』
- 4. KX II-101 の設定『p. 19』

KX II-101 をインストールする前に、次の概説のように KX II-101 を経由してアク セスするターゲット サーバを設定し、パフォーマンスを最適にします。 次の設定条件 は、KX II-101 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 サー バのみに適用されます。



サーバ ビデオ解像度の設定

最適な帯域効率とビデオ 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表示に設定します。 写 真や複雑な階調を持つ背景は避けてください。

サーバのビデオ解像度とリフレッシュ レートが KX II-101 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 は次のビデオ解像度を サポートします。

テキスト モード〉

640x480、60Hz	1024x768、60Hz
640x480、72Hz	1024x768、70Hz
640x480、75Hz	1024x768、75Hz
640x480、85Hz	1024x768、85Hz
800x600、56Hz	1152x864、60Hz
800x600、60Hz	1152x864、75Hz
800x600、72Hz	1280x1024、60Hz
800x600、75Hz	1600 x 1200, 60Hz
800x600、85Hz	

Sun ビデオ解像度の設定

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 でサポートされる解像度の詳細については、「サーバビ デオ解像度の設定 『p.8』」を参照してください。

注: サポートされ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 and V sync では動作しません。

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。
- 次のコマンドを root から実行します。
 - # 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

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

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。
- 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

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

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

ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

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



ここで、1024x768x75 は KX II-101 でサポートされる任意の解像度です。

2. コンピュータを再起動します。

マウス モード

KX II-101 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 (アニメーション カー ソルを使用しないでください)、および標準マウス モード。 ずれないマウス (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 ションの説明に従って、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。

このセクションでは、さまざまなシステムで必要なマウスの設定について説明します。

Windows Vista

- ▶ マウスを設定するには、以下の手順に従います。
- 1. [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。
- [ポインタ オプション] タブをクリックします。 [速度] グループで、以下の操作を 行います。
 - a. 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。
 - b. [ポインタの精度を高める] オプションをオフにします。
- 3. [OK] をクリックします。
- アニメーション効果とフェード効果を無効にするには、以下の操作を行います。
- Windows の [スタート] メニューから、[コントロール パネル]、[システム]、[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。
- 2. [詳細設定] タブをクリックします。
- [パフォーマンス] グループの [設定] ボタンをクリックします。 [パフォーマンス オ プション] ダイアログ ボックスが表示されます。
- 4. [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。
 - 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
 - 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
- 5. [OK] をクリックします。



6. [コントロール パネル]を閉じます。

Windows XP の設定

Microsoft Windows XP が稼動している KVM ターゲット サーバで、[ポインタの 精度を高める] オプションをオフにし、[ポインタの速度を選択する] で、速度をちょうど 中速に設定します。 これらのパラメータは、[コントロール パネル]、[マウス]、[マウス ポインタ] の順に選択すると表示できます。

注: Windows 2000 または XP を実行しているターゲット サーバの場合、KX II-101 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、他のユーザが高速なマウス速度を求めている場合に、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 接続専用に遅く設定できます。

注: Windows XP と 2000 のログイン画面では、マウスのパラメータが、最適な KX II-101 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。このため、これらの画面ではマウス同期は最適になりません。 Windows ターゲット サーバのレジストリを調節でき場合は、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、ログイン画面で KX II-101 のマウス の同期を改善することができます。Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0

Windows 2000 の設定

Microsoft Windows 2000 が稼動しているターゲット サーバで、マウス ポインタの 加速を [なし] に設定し、ポインタの速度をちょうど中速に設定します。 これらのパラ メータは、[コントロール パネル]、[マウス] の順に選択すると表示できます。

Linux の設定

Linux グラフィカル インタフェースを実行しているターゲット サーバで、マウスの加速 値を 1 に設定し、しきい値も 1 に設定します。

前述のように、Linux を実行しているターゲット サーバが、KX II-101 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。 また、ブランキング時間が VESA の標準値の +/-40% 以内に なるように Linux ターゲット サーバを設定することも必要になります。

- ▶ これらのパラメータを確認するには、以下の手順に従います。
- 1. Xfree86 設定ファイル XF86Config を表示します。
- テキスト エディタを使用して、KX II-101 でサポートされてていない解像度をす べて無効にします。
- 3. KX II-101 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。
- 4. ブランキング時間を確認します (VESA 標準の +/-40%)。



5. コンピュータを再起動します。

注: ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ (プラス記号)を 押すと、XF86Config ファイル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できます。

Sun Solaris の設定

Solaris ターゲット サーバは、KX II-101 でサポートされているいずれかの表示解像 度に設定する必要があります。 Sun マシンで一般的にサポートされる解像度を以 下に示します。

- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@75Hz
- 1024x768@85Hz
- 1280x1024@60Hz

Solaris オペレーティング システムが稼動しているターゲット サーバのビデオ出力は VGA である必要があります (コンポジット Sync ではなく H-and-V Sync)。 Sun のビデオ カード出力をコンポジット Sync からデフォルト以外の VGA 出力に変更 するには、最初に Stop+A コマンドを発行して bootprom モードに移行します。 次に、以下のコマンド、

eeprom output-device=screen:r1024x768x75



を発行して出力解像度を変更します。次に、boot コマンドを実行して、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 で使用するために、 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 で使用するために、APKMSUN Raritan Guardian が必要です。 KX II-101 は、APSUSB アダプタを使用した PS/2 バ ージョンのみをサポートします (コンポジット Sync はサポートされていません)。

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 サーバで、マウスの加速 値を正確に 1 に設定し、しきい値も正確に 1 に設定します。これは、グラフィカル ユーザ インタフェース (下記) 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。

Mouse motion
Acceleration
Slow Fast
Threshold
Small Large
· · · · ·

Apple® Macintosh の設定

ずれないマウス (Absolute Mouse Synchronization)を使用します。



KX II-101 の接続



KX II-101 には、下の図に示す物理接続が用意されています。

- 1 付属モニタおよび PS/2 ケーブル (項目 3 を参照)
- 2 ミニ USB ポート。 付属の USB ケーブルを使用してデバイス をターゲット サーバに接続するために使用します (付属の PS/2 ケーブルを使用しない場合)。ずれないマウスと仮想メディア機能 を使うには、USB で接続する必要があります。



- 3 組み付けのビデオおよび PS/2 ケーブル。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に使用します (USB ケーブルを 使用しない場合)。
- 4 ローカル ユーザ ポート。オプションのビデオおよび PS/2 ケーブ ルを使用して、ローカル キーボード、ビデオ、マウスをターゲット サ ーバに直接接続するために使用します。
- 5 Ethernet LAN/PoE ポート。LAN 接続および電源 (PoE LAN 接続を使用している場合)を供給します。
- 6 電源コネクタ。 PoE (Power over Ethernet) LAN 接続を使 用していない場合は、電源を接続します。
- 7 バックライト LED パワー ON および起動インジケータ。デバイ スの動作ステータス情報を表示します。
- 8 [Admin Port] (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。
 設定用の 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を実行します。
 パワー ストリップを設定および管理します。
 デバイスにダイヤルインする外部モデムを接続します。

ターゲット サーバへの接続

KX II-101 では、組み付けの PS/2 ケーブルまたは付属の USB ケーブルを使用し てターゲット サーバに接続できます。 接続する前に、「*サーバ ビデオ解像度の設定* 『p.8』」の説明に従って、ターゲット サーバのビデオをサポートされる解像度および垂 直走査周波数に設定します。

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 を設定するには、以下 の手順に従います。
- 1. 組み付けのキーボード、ビデオ、マウス ケーブルを使用して KX II-101 をターゲ ット サーバに接続します。
- オプションの PS/2 ケーブルを使用して、ローカルのキーボード、ビデオ、マウスを KX II-101 のローカル ユーザ ポートに接続します。

注: ローカル ユーザ ポートが機能するには、KX II-101 の電源が投入されて いる必要があります。

3. 仮想メディア (VM) 接続が必要な場合は、ミニ USB コネクタを KX II-101 に接続し、USB コネクタをターゲット サーバの USB ポートに接続します。





完了したら、下の図に示すような接続を得ることができます。

- 1 KX II-101 からターゲット サーバへの統合 PS/2 キーボード、ビデオ、マウスの接続
- 2 KX II-101
- 3 ローカル モニタへのビデオ接続 (オプション ケーブル)
- 4 ローカル モニタ
- 5 KX II-101 からマウスへの PS/2 接続 (オプション ケーブル)
- 6 KX II-101 からキーボードへの PS/2 接続 (オプション ケーブル)
- 7 ターゲット サーバ
- 8 KX II-101 からターゲット サーバへの付属のミニ USB USB コネクタ、仮想メディア接続用



USB の設定

- USB ターゲット サーバに KX II-101 を設定するには、以下の手順に従い ます。
- 1. ミニ USB コネクタを KX II-101 に接続し、USB コネクタをターゲット サーバ の USB ポートに接続します。
- 2. オプションの PS/2 DKX2-101-LPKVMC ケーブルを使用して、ローカル ビデ オのみを KX II-101 のローカル ユーザ ポートに接続します。

注: ローカル ユーザ ポートが機能するには、KX II-101 の電源が投入されて いる必要があります。

3. USB ケーブルを使用して、キーボードとマウスをターゲット サーバに直接接続します。

完了したら、下の図に示すような接続を得ることができます。

1 KX II-101 からターゲット サーバへの付属のミニ USB - USB ケーブル



- 2 KX II-101
- 3 ローカル モニタへのビデオ接続 (オプション ケーブル)
- 4 ローカル モニタ
- 5 ターゲット サーバからマウスへの USB 接続
- 6 ターゲット サーバからキーボードへの USB 接続
- 7 ターゲット サーバ

ネットワークへの接続

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 を使用中は、黄 色の LED が点滅し、10Mbps の IP トラフィックを示します。 緑色のライトは 100Mbps の接続速度を示します。

KX II-101 への電源供給

KX II-101 には、標準付属の AC 電源アダプタまたは PoE (Power over Ethernet) により電源を供給できます。

- 標準の AC 電源の場合は、AC 電源アダプタ キットの片側のプラグをパワー ポートに挿し込み、もう一端を近くの電源コンセントに挿し込みます。
- PoE の場合は、10/100Mbps ケーブルを LAN ポートに指し込み、もう一端 を PoE の給電された LAN に差し込みます。

KX II-101 は電源を ON にすると、起動シーケンスに進みます。この間、青色の Raritan ロゴ LED が約 45 秒間点滅します。起動が完了すると、バックライト LED が点灯したままになります。

Admin ポートの使用

Admin 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 の設定とセットアップを実行できます。 付属のシリ アル ケーブルのミニ DIN 側端部を KX II-101 の Admin ポートに指し込み、 DB9 側の端部を PC またはラップトップのシリアル ポートに差し込みます。 シリア ル接続の設定は、次の設定値にします。 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。

Admin ポートを使用して KX II-101 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 プログラムの使用」を参照してください。



ローカル ユーザ ポートの使用

KX II-101 では、オプションのビデオおよび PS/2 ケーブルを使用できます。これらの ケーブルを使用して、LOCAL USER ポート経由でキーボードやマウスをターゲット サーバに接続できます。 LOCAL USER ポートは、KX II-101 の接続先ターゲット サーバへのパススルーとして機能し、それ以外の目的はありません。 LOCAL USER ポートが機能するには、KX II-101 の電源が投入されている必要があります。

注: ローカル ポートでは、PS/2 ホスト インタフェース接続のみがサポートされており、 PS/2 コネクタを使用して KX II-101 に接続した後、ターゲット サーバを再起動す る必要があります。

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 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 の設定メニューで、指定した別の TCP ポートを使用することもできます。

KX II-101 の Web アクセス機能を活用するには、ファイアウォールが TCP ポート 443 (HTTPS 通信用の標準 TCP ポート) でのインバウンド通信を許可しておく 必要があります。HTTP 要求を HTTPS にリダイレクトする (これにより、ユーザは "https://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) KX II-101 の機能を活用するには、ファイアウォールが TCP ポー ト 80 (HTTPS 通信用の標準 TCP ポート) でのインバウンド通信も許可している 必要があります。

KX II-101 の設定

KX II-101 は、次の 2 とおりの方法で設定できます。

- Web ベース KX II-101 リモート コンソールを使用する。この場合、ユニットは 操作用 PC へのネットワーク接続を確立している必要があります。
- HyperTerminal のようなターミナル エミュレーション プログラムを使用する。この場合、ユニットの Admin ポートから操作用 PC への直接接続が必要です。この接続用のケーブルは KX II-101 に付属されています。

このセクションでは、両者の方法での KX II-101 の設定手順について説明します。



リモート コンソールの使用

KX II-101 リモート コンソールは、ユニット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 を設 定する前に、操作用 PC とユニットをネットワークに接続しておく必要があります。

KX II-101 を設定するには、以下の手順に従います。

- デフォルトのパスワードに代わる新しいパスワードを設定します。
- IP アドレスを割り当てます。
- ターゲット サーバに名前を付けます。
- ユーザおよびグループを作成します。

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 スワードの設定を求めるプロンプトが表示されます。その後、KX II-101 の設定が できます。

- 1. KX II-101 ユニットへのネットワーク接続可能な操作用 PC にログオンします。
- 2. サポートされる 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、ユニットのデフォルトの IP アドレス (下記) を 入力します。

192.168.0.192

- 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。
- [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、 [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 ワードを再入力します。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。
- [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

 KX II-101 リモート コンソールで、[Device Settings] (デバイス設定)の [Network Settings] (ネットワーク設定)を選択します。 [ネットワーク基本設 定] (Network Basic Settings) ページが開きます。

ome > Devi	e Settings > Network Settings
Network	Basic Settings
Device Na	me *1
Dominion	X2-101
IP auto co	nfiguration
DHCP 🔽	
Preferre	I host name (DHCP only)
ID addres	
102 168 5	0.244
132.100.3	0.241
Subnet n	ask
255.255.2	55.0
Gateway	IP address
192.168.5	0.126
Primary [IIS server IP address
192,168,5	0.114
Secondar	y DNS server IP address
192.168.5	0.112
OK	Reset To Defaults Cancel
	المعينية بالمحادثين المحمد بالقمص العنصيتين ا

- [Device Name] (デバイス名) フィールドで、最大 16 文字の英数字と特殊 文字を組み合わせて (スペースは使用できません)、KX II-101 ユニットのわかり やすいデバイス名を指定します。
- 3. [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)。 Dominion KX II-101 はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、これはデフォルトの推奨さ れるオプションです。 このオプションを選択した場合は、ネットワークの IP アドレスを手動で指定する必要があります。
 - [DHCP]。このオプションを選択した場合、KX II-101 を起動するたびに、 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。

ダイレクト ポート アクセスの設定

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



- [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。
- 3. グローバル Telnet または SSH アクセスを有効にします。
 - [Enable TELNET Access] (TELNET アクセスを有効にする) チェックボ ックスをオンにして、TELNET アクセスを有効にします。
 - [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 にして、SSH アクセスを有効にします。
- 4. 選択したアクセス タイプの有効な TCP ポートを指定します。たとえば、 Telnet TCP ポートを介したダイレクト ポート アクセスは 7770 として設定でき ます。

Home > Device Settings > Device Services
Services
Discovery Port * 5000
Enable TELNET Access
TELNET Port 23
Enable SSH Access
SSH Port 22
Enable Direct Port Access via URL
OK Reset To Defaults Cancel

5. [OK] をクリックしてこの情報を保存します。

ターゲット サーバに名前を付ける

- 1. 「*KX II-101 への接続* 『p. 30』」の説明に従って、KX II-101 をターゲット サ ーバに接続します (まだ接続していない場合)。
- [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。



Home > Device Settings > Port Configura	tion > Port	•
		ę.
Port 1		
		ł.
Type: VKP		1
Name:		1
Dominion_KX2_101_Port1		ŧ.
		1
		ą.
		€.
Power Association		ł
D O C H		9
Power Strip Name	Outlet Name	Ŧ.
None	💌	ł.
	🚩	1
	💌	1
	🕶	ł.
		1
		1
		1
		1
OK Cancel	Annalia and a second	5

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。

ユーザとグループの作成

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

- > ユーザ グループを作成するには、以下の手順に従います。
- 1. 次の方法のいずれかを使用して、[Group] (グループ) ページを開きます。
 - a. [User Management] (ユーザ管理) の [Add New User Group] (新 規ユーザ グループの追加) を選択します。または、
 - b. [User Group List] (ユーザ グループ リスト) ページの [Add] (追加) ボ タンをクリックします。
- 2. [Groupname] (グループ名) フィールドに、新しいユーザ グループの名前を入 力します。
- 3. グループの許可を設定します。このグループに属するすべてのユーザに対して割 り当てる許可について、その許可の左にあるチェックボックスをオンにします。



- [Port Permissions] (ポート権限) ([Access] (アクセス)、[VM Access] (VM アクセス)、[Power Control] (電源管理)) 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 ポートと、そのアクセスのタイプを指定します。デフォルトでは、VM (仮想メディア) アクセスは他のポート権限と同様にオフになっています。 仮想メディアを使用するには、許可を有効にする必要があります。
- 5. [OK] をクリックします。
- ▶ 新規ユーザを作成するには、以下の手順に従います。
- 1. 次の方法のいずれかを使用して、[User] (ユーザ) ページを開きます。
 - a. [User Management] (ユーザ管理)の [Add New User] (新規ユーザの追加)を選択します。または、
 - b. [User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックします。
- [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)。
- [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)。
- [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)。
- [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 ([Admin] (管理者)、[<Unknown>] (不明)、[Individual Group] (個別グ 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。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。
- 6. [OK] をクリックします。



ターミナル エミュレーション プログラムの使用

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 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 アクセス制御
- LAN 速度
- LAN インタフェースモード

KX II-101 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 のAdmin ポートと PC の COM1 ポートを接続する必要があります。詳細については、「Admin ポートの使 用『p.18』」を参照してください。

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 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 とローカル PC を 接続します。

KX II-101 の Admin ポートと PC の COM1 ポートを接続します。

- 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 を設定します。
- 3. ターミナル エミュレーション プログラムで次のポート構成を設定します。
 - Bits per second (ビット/秒): 115200
 - Data bits (データ ビット): 8
 - Parity (パリティ): None (なし)
 - Stop bits (ストップ ビット): 1



COM1 Properties	?×			
Port Settings				
Bits per second:	115200			
Data bits:	8			
Parity:	None			
Stop bits:	1			
Flow control:	None			
	Bestore Defaults			
OK Cancel Apply				

Flow control (フロー コントロール): None (なし)

4. KX II-101 に接続します。

ログイン画面が表示されます。

Logi	n :			

5. 管理者ユーザ名を入力して、Enter キーを押します。





Login: admin Password: _

6. パスワードを入力して、Enter キーを押します。

Admin Port (管理ポート)のプロンプトが表示されます。

- 7. Admin Port (管理ポート) のプロンプトで、「config」と入力し、Enter キー を押します。
- 8. Config (設定) のプロンプトで、「network」と入力し、Enter キーを押しま す。
- 9. 現在のインタフェース設定を確認するには、Interface (インタフェース) のプロンプ トで、「interface 」と入力し、Enter キーを押します。



次のように現在のインタフェース設定が表示されます。

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	オプション
ipauto none dhcp		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。
		interface ipauto none ip 192.168.50.12
		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。
ip	IP アドレス	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。
mask	subnetmask	サブネット マスク IP アドレス。
gw	IP アドレス	ゲートウェイ IP アドレス
mode	mode	Ethernet モード。次の選択肢があります。
		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 Mbs、半二重。
		10fdx - 10 Mbs、全二重
		100hdx - 100 Mbs、半二重
		100fdx - 100 Mbs、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 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。



KX II-101 への接続

この章の内容

言語サポート	30
Java Runtime Environment (JRE)	
KX II-101 の起動	31
お気に入りの管理	35
[Port Access] (ポート アクセス) ページ	43

言語サポート

4

KX II-101 は、次の言語のキーボード サポートを提供しています。 英語 (アメリカ)、 繁体字中国語、簡体字中国語、日本語、韓国語、フランス語、ドイツ語。

注: 中国語、日本語、および韓国語のキーボードについては、表示のみに使用でき ます。現時点での KX II-101 リモート コンソール機能では、ローカル言語の入力は サポートされていません。

Linux での言語設定

Linux での外国語キーボードの設定方法については、『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「キーボードの種類」を参照してください。

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。 詳細は、Java のドキュメントまたは『Raritan Multi-Platform Client / Raritan Remote Client ユーザ ガイド』を参照 してください。

KX II-101 リモート コンソールおよび MPC が動作するには、JRE が必要です。 KX II-101 リモート コンソールは、Java のバージョンをチェックします。バージョンが不 適切な場合または古い場合は、互換性のあ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、Java Runtime Environment (JRE) バージョン 1.5 を使用することを推奨しますが、KX II-101 リモート コンソールおよび MPC は JRE 1.6.x (1.6.2 を除く) など、JRE バージョン 1.4.2_05 以降 (JRE バージョン 1.5.0_02 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 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 Java Runtime Environment (JRE) をインストールしてください。



KX II-101 の起動

重要: ブラウザの種類を問わず、KX II-101 リモート コンソールを起動 するためには、Dominion デバイスの IP アドレスからのポップアップ を許可する必要があります。

ご使用のブラウザおよびセキュリティの設定により、セキュリティと証明書に関する各種の警告が表示されることがあります。 KX II-101 リモート コンソールを起動するには、 これらの警告を承諾する必要があります。

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

- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]
- KX II-101 リモート コンソールを起動するには、以下の手順に従います。
- KX II-101 ユニットにネットワークを介して接続でき、Java Runtime Environment v1.4.2_05 以降がインストールされている任意のワークステーションにログオンします (JRE は *http://java.sun.com*/ http://java.sun.com から入手できます)。
- サポートされる Web ブラウザ (Internet Explorer (IE) や Firefox など) を 起動します。「サポートされるブラウザ」を参照してください。
- 次の URL を入力します。http://IP-ADDRESS。ここで、IP-ADDRESS の 部分は、KX II-101 ユニットに割り当てた IP アドレスに置き換えます。また、 https を使用したり、管理者によって割り当てられた KX II-101 の DNS 名 を使用することもできます (DNS サーバが設定されている場合)。単に IP アド レスをブラウザに入力してもかまいません (KX II-101 は常に IP アドレスを HTTP から HTTPS にリダイレクトします)。ログイン ページが開きます。

Username:	
Password:	



- ユーザ名とパスワードを入力します。初めてログオンする場合は、工場出荷時 のデフォルト ユーザ名とパスワード (admin および raritan (すべて小文字))
 を使用してログオンします。デフォルトのパスワードを変更するように求められます。 詳細は、「デフォルトのパスワードの変更」を参照してください。
- 5. [Login] (ログイン) をクリックします。

ダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスを使用すると、通常のログイン ページに進まないで KX II-101 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 リモート コンソールを起動します。
- [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。
- [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) をクリックしてこの設定を保存します。
- ▶ 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、必要に応じて KX II-101 のポート番号を 使用して URL を定義します。

KVM ポートが 1 つのみある場合、ポート番号は不要です。

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 アドレス]/dpa.asp?username=[ユーザ名]&password=[パスワー ド]&port=[ポート番号]

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 コンソールのレイアウト

KX II-101 リモート コンソール インタフェースは、設定や管理、ターゲット サーバのリ ストや選択用に Web 形式の HTML インタフェースを提供します。 オプションは 複数のタブに配置されています。

正常にログインすると、[Port Access] (ポート アクセス) ページが表示され、ポート、 そのステータスと可用性が表示されます。



KX II-101 コンソールでの案内

KX II-101 リモート コンソール インタフェースは移動と選択の多くの方法を提供します。

- ▶ 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。使用可能なオプションのページが開きます。
- 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。

Category	Event	SNMP	Systog	Audit Log
Device Operation		N	F	R
	System Starbup	ম	₩	4
	System Shutdown	ঘ	9	R
	Power Supply Status Changed	v	R	₽
	Powership Outlet Statue Changed	ম	9	4
	Network Parameter Changed		₩	v
	Port Status Changed	ম	9	R
	Network Pallure			A
	Ethernist Failover	ম	1	P
Device Management		v i	9	9
	FactoryRead		R	N
	Begin CC Control	v	₩	4
	End CC Control	2	4	

- ▶ 画面に収まらないページをスクロールするには、以下の手順に従います。
- キーボードの Page Up キーと Page Down キーを使用します。または、
- 右側にあるスクロール バーを使用します。



KX II-101 リモート コンソールのメニュー マップ

以下の図に、KX II-101 リモート コンソールのすべてのメニュー オプションを示します。



ログオフ

- > KX II-101 リモート コンソールを終了するには、以下の手順に従います。
- ページの右上隅の [Logout] (ログアウト) をクリックします。

注: ログオフすると、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。



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。
- 名前または IP アドレス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 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 デバイスを接続されているデバイスから取得する (ログ インの後)。

Home > Mana	age Favorites > Favorit	e List	
	Name	IP/Hostname	
	Serial Target	192.169.59.40	A MARINE
	KVM Target	192.169.59.48	
Add	Edit Delete		



- ▶ お気に入りの KX II-101 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)目的のデ バイスの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。
- Favorite Devices] (お気に入りデバイス) リストの表示を名前順と IP アドレス順の間で切り替えるには、以下の手順に従います。

お気に入りを IP アドレス順に表示するに お気に入りを名前順に表示するには、以下の は、以下の手順に従います。 手順に従います。

[Display by IP] (IP 順) ボタンをク [Display by Name] (名前順) ボタンを リックします。 クリックします。

ボタンをクリックして切り替えます。

お気に入りのデバイスが名前別に表示され お気に入りのデバイスが IP アドレス別に表示 ている場合は、[Display by IP] (IP 順) されている場合は、[Display by Name] (名 前順) ボタンをクリックして切り替えます。

Favorite Devices: 192.169.59.40 192.169.59.48	Favorite Devices: K∨M Target Serial Target
Manage	Manage
Display By Name	Display By IP

[Manage Favorites] (お気に入りの管理) メニュー

- > [Manage Favorites] (お気に入りの管理) メニューを開くには、以下の手 順に従います。
- [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) ページが開きます。

-בבא	操作
[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)	ローカル サブネット上のデバイスを検出 します。
[Discover Devices - KX II-101 Subnet] (Discover Devices (デバイ ス検出)- KX II-101 サブネット)	KX II-101 デバイス サブネット上のデ バイスを検出します。



KX II-101 への接続

×=-	操作
[Add New Device to Favorites] (お気に入りリストのデバイスを追加、編
お気に入りへの新しいデバイスの追加)	集、および削除します。

[Favorites List] (お気に入りリスト)

[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。

Favorite	List	
	Name	IP/Hostname
	KVM Target	192.169.59.48
	Serial Target	192.169.59.40
Add	Edit Delete	

- > お気に入りを追加するには、以下の手順に従います。
- [Add] (追加) ボタンをクリックします。 [Add New Favorite 『p. 42の"[Add New Favorite] (新しいお気に入りの追加)"参照先 』] (新しいお気に入りの追加) ページが開きます。
- ▶ 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、確認メッセージが表示されないので注意してください。

- 1. 目的の KX II-101 デバイスの横にあるチェックボックスをオンにします。
- [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。
- ▶ 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 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) ページが開きます。

All fields are required		
Description		
KVM Target		
P Address		
192.169.59.48		
Port		
5000		
Product Type		
Dominion KSX G1 🗸		

- 3. 必要に応じてフィールドを更新します。
 - [Description] (説明)。わかりやすい説明を入力します。
 - [IP Address] (IP アドレス)。 KX II-101 ユニットの IP アドレスを入力します。
 - [Port] (ポート)。 必要に応じて検出ポートを変更します。
 - [Product Type] (製品タイプ)。
- 4. [OK] をクリックします。



[Discover Devices - Local Subnet] (デバイス検出 - ローカル サブネット)

このオプションを使用すると、ローカル サブネット (KX II-101 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できます。また、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。

Home > Mana	ge Favorites > Discover D	evices - Local Subnet
Discover	Devices - Local Sub	net
Vse D	efault Port 5000	
Discover 5000 Save	on Port:	
	Name	IP/Hostname
	DKX2-101	192.168.50.68
	KX_KIM-0050	192.168.50.12
	shoaib-sx	192.168.50.239
	shoaibkx2	192.168.50.234
Select	All Deselect /	All Add Refresh

- ▶ 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。
- [Favorites] (お気に入り)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)ページが開きます。
- 2. 目的の検出ポートを選択します (検出ポートについての詳細は、「ネットワークの その他の設定」を参照してください)。
 - 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) オプションをオンにします。
 - 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) オプションを 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。



[Discover Devices - KX II-101 Subnet] (Discover Devices (デ バイス検出)- KX II-101 サブネット)

このオプションを使用すると、デバイス サブネット (KX II-101 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できます。また、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。

この機能を使用すると、複数の KX II-101 ユニット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 リモート コンソールは、KX II-101 のサブネット内の KX II-101 ユニットを自動的に検出します。

Disser		404-250 Cubast
Discove	r Devices - WWDKX2	101-250 Subnet
_	Name	IP/Hostname
	Anil-KSX	192.168.59.193
	Annette_KSX188	192.168.59.228
	basker-ksx	192.168.59.250
	BuilderKX2	192.168.59.75
	DKSXII	192.168.59.227
	DKX2-101-TEST	192.168.59.80
	DKX201GA	192.168.59.21
	DKX2464-206GA	192.168.59.146
	DKXSG2-KSX2-188	192.168.59.218
	Dominion-KX	192.168.59.8
	DominionKSX	192.168.59.200
	DominionKSX	192.168.59.204
	DominionKSX	192.168.59.205
	DominionKX	192.168.59.202
	DominionKX	192.168.59.247
	JaviersBox	192.168.59.249
	kx2-101_vpn_tes	192.168.59.147
	LarsKX101	192.168.59.206
	lra-ksx2	192.168.59.207
	sai-KX101	192.168.59.34
	SE_KX2	192.168.59.53
	vj	192.168.59.224
	wwDKX2-101-250	192.168.59.140
Select	All Deselect	All
00100	Descrete	·····



- 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。
- [Favorites] (お気に入り)の [Discover Devices KX II-101 Subnet] (デバ イス検出 - KX II-101 サブネット)を選択します。 [Discover Devices - KX II-101 Subnet] (デバイス検出 - KX II-101 サブネット)ページが開きます。
- 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 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。

[Add New Favorite] (新しいお気に入りの追加)

- 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。
- [Manage Favorites] (お気に入りの管理)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)ページが開きます。
- 2. わかりやすい説明を入力します。
- 3. デバイスの IP アドレスを入力します。
- 4. 必要に応じて検出ポートを変更します。
- [OK] をクリックします。
 このデバイスがお気に入りのリストに追加されます。



[Port Access] (ポート アクセス) ページ

KX II-101 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) ページが開きます。このページには、KX II-101 ポート、そのステータ スおよび可用性が表示されます。 [Port Access] (ポート アクセス) ページは、KX II-101 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 サーバは、KX II-101 ユニットを介して制御したいサーバです。この サーバはデバイスに組み付けの PS/2 コネクタを使用して KX II-101 に接続されま す。

注: KVM ターゲット サーバへの接続ごとに、新しい Virtual KVM Client ウィン ドウが開きます。

- [Port Access] (ポート アクセス) ページを使用するには、以下の手順に従います。
- 1. KX II-101 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。

Home > Port Access			Logout
Port Access			
Click on the i	ndividual port name to see allowable operatio	ns.	:
0 of 1 Remote	KVM channels currently in use.		
▲ No.	Name	Availability	
1	Dominion_KX2_101_Port5	idle	

- [No.] (番号)。KX II-101 で使用できる 1 つのポートがあります。
- [Name] (名前)。KX II-101 ポートの名前です。最初は 「Dominion_KX101G2_Port1」に設定されていますが、わかりやすい名 前に変更できます。
- [Availability] (可用性)。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。
- ターゲット サーバに接続するには、デバイス/ターゲット サーバの名前をクリックし、 [Connect] (接続) ポップアップをクリックします。[Virtual KVM Client] ウィン ドウが表示され、可用性が [Busy] (ビジー) に変化します。
- 3. ターゲット サーバとの接続を切断するには、デバイス/ターゲット サーバの名前を クリックし、[Disconnect] (切断) ポップアップをクリックします。[Virtual KVM Client] ウィンドウが閉じて、可用性が [Idle] (アイドル) に変化します。



ユーザ、グループ、アクセス許可

この章の内容

ユーザ	44
グループ	
コーザとグループの関係	45
[User Management] (ユーザ管理)	
リモート認証	58

ユーザ

5

KX II-101 は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内 部リストを保持しています。この情報は、暗号化形式で内部に保存されます。認 証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。すべてのユ ーザは認証を受ける必要があります。LDAP または RADIUS 認証を行うように KX II-101 が設定されている場合、LDAP/LDAPS または RADIUS 認証が行 われた後に、ローカル認証が行われます。

KX II-101 ユニット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 ユニット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。 ユーザを追加および編集する方法についての詳細は、「*ユーザ管理* 『p. 45の "[User Management] (ユーザ管理)"参照先 』」を参照してください。

グループ

すべての KX II-101 ユニットには、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)	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) ユーザは [Admin] (管理) 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。



ユーザ、グループ、アクセス許可

[Individual	個別グループとは、基本的に個人の「グループ」です。 つまり、
Group] (個別	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
グループ)	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。

システムによって定義されているデフォルトのグループに加えて、グループを作成し、目 的に合った適切な許可を指定できます。 ユーザ グループを作成および編集する方 法についての詳細は、「ユーザ管理」を参照してください。

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 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、ユニット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。

[User Management] (ユーザ管理)

[User Management] (ユーザ管理) メニュー

[User Management] (ユーザ管理) メニューは次のように構成されています。

メニュー	操作
[User List] (ユーザ リスト)	すべてのユーザをアルファベット順に表示します。ユー ザの追加、変更、または削除を行うこともできます。
[Add New User] (新規 ユーザの追加)	新規ユーザを追加します。ユーザ情報の変更も行う ことができます。
[User Group List] (ユー ザ グループ リスト)	すべてのユーザ グループをアルファベット順に表示します。ユーザ グループの追加、変更、または削除を行うこともできます。
「Add New User Group] (新規ユーザ グル ープの追加)	新規ユーザ グループを追加します。ユーザ グループ 情報の変更も行うことができます。
[Change Password] (パ スワードの変更)	特定のユーザのパスワードを変更します。



[User Management] (ユーザ管理)

אבשא-	操作
[Authentication	KX II-101 に対するアクセスに使用する認証の種
Settings] (認証設定)	類を設定します。

[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。

	4 Username	Full Name	User Group	
	admin	Admin	Admin	
Г	marketing	Addie Consumer	@marketing	
	tester	Joe Tester	@tester	

- ▶ 新規ユーザを追加するには、以下の手順に従います。
- [Add] (追加) ボタンをクリックします。 [User] (ユーザ) ページが開きます。
 [User] (ユーザ) ページについての詳細は、「新規ユーザの追加 『p. 47の
 "[Add New User] (新規ユーザの追加)"参照先 』」を参照してください。
- ▶ 既存のユーザを変更するには、以下の手順に従います。
- 1. リストから目的のユーザを探します。
- 2. ユーザ名をクリックします。 [User] (ユーザ) ページが開きます。ユーザの編集 方法についての詳細は、「*既存のユーザの変更* 『p. 48』」を参照してください。
- ▶ ユーザを削除するには、以下の手順に従います。
- 1. リストのユーザ名の左にあるチェックボックスをオンにして、目的のユーザを選択します。
- 2. [Delete] (削除) をクリックします。 削除を確認するプロンプトが表示されます。
- 3. [OK] をクリックします。



[Add New User] (新規ユーザの追加)

KX II-101 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] (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([Active](アクティブ) チェックボックスがオフになります)。詳細は、 「セキュリティの設定」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. 次の方法のいずれかを使用して、[User] (ユーザ) ページを開きます。
 - [User Management] (ユーザ管理)の [Add New User] (新規ユーザの追加)を選択します。または、
 - [User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックします。

rt Access	Virtual Media	User Management	Device Settings	Security	Ma
-11-1° C		Roat & All		\sim	/
me > User M	lanagement > Use	er :			
User					
Username	·				
<u> </u>					
Full Name					
Password	*				
Confirm P	assword *				
User Grou	p '				
select -		*			
Active	e				
IN					
OK	Cancel				

- [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)。
- [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)。



[User Management] (ユーザ管理)

- [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)。
- [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 ([<Unknown>] (不明) (デフォルト設定)、[Admin] (管理者)、[Individual Group] (個別グループ)) 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。このユーザを既存のユーザ グループに関連付 けない場合は、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。

注: [Admin] (管理) ユーザは [Admin] (管理) グループのメンバーである 必要があります。

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*『p.52』」を参照してください。

- この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] をクリックします。

既存のユーザの変更

- ▶ 既存のユーザを変更するには、以下の手順に従います。
- [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*『p. 47の "[Add New User] (新規ユーザの追加)"参照先』」を参照してください)。
- 2. [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。詳細は、「*ユーザ ブロック* 『p. 149の"[User Blocking] (ユ ーザ ブロック)"参照先 』」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。
- [User Management] (ユーザ管理)の [User] (ユーザ)を選択します。
 [User] (ユーザ)ページが表示されます。
- 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 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 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。

[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。

me > User Managem	ent > Groups	Logo
User Group Li	st	
	A Group Name	
	<unknown></unknown>	
Г	@marketing	
	Otesting	
	Admin	

- ▶ 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。
- [Add] (追加) ボタンをクリックします。 [Group] (グループ) ページが開きます。
 [Group] (グループ) ページについての詳細は、「新規ユーザ グループの追加」
 を参照してください。
- ▶ 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. リストから目的のユーザ グループを探します。



[User Management] (ユーザ管理)

- 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。 グループ を編集する方法についての詳細は、「*既存のユーザ グループの変更*『p.56』」 を参照してください。
- ▶ 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 リストをで並べ替えます。

- 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。

[Add New User Group] (新規ユーザ グループの追加)

- ▶ 新規ユーザ グループを追加するには、以下の手順に従います。
- 1. 次の方法のいずれかを使用して、[Group] (グループ) ページを開きます。
 - [User Management] (ユーザ管理)の [Add New User Group] (新 規ユーザ グループの追加)を選択します。または、



ome > User Management > Group			
Group			
Group Name *			
T Permissions			
Device Settings			
Diagnostics Maintenance			
PC-Share			
Security			
Port Permissions			
Port	Access	VM Access	Power Control
Dominion_KX2_101_Port1 Power Port 1	Deny V	Deny	Deny V
▼ IP ACL			
Rule # Starting IP	Ending IP	Action	
		ACCEPT	Τ 💌
Append Insert Replac	e Delete		
OK Cancel			

 [User Group List] (ユーザ グループ リスト) ページの [Add] (追加) ボ タンをクリックします。

[Group] (グループ) ページは、[Group] (グループ)、[Permissions] (許可)、 [Port Permissions] (ポート権限)、および [IP ACL] (IP ACL) のカテゴリに 分かれています。

- [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 い名前を入力します。
- グループの許可を設定します。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。詳細は、「許可の設定 『p. 52』」を参照してください。
- [Port Permissions] (ポート権限)を設定します。 KVM およびパワー ポートに与えるアクセスの種類を指定します。 詳細は、「ポート権限の設定」を参照してください。
- グループベースの IP ACL (IP アクセス制御リスト)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によって、その IP アドレスから KX II-101 デバイスへのアクセスを制限します。この機能は、デバイスへのすべてのア クセスに適用される (および優先される) IP アクセス制御『p. 153の"[IP Access Control] (IP アクセス制御)"参照先 』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。
- 6. [OK] をクリックします。



注: 複数の管理機能を MPC 内で利用できます (これらの機能を利用できるの は、デフォルトの ADMIN (管理者) グループのメンバーに限られます)。

許可の設定

重要: [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	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 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/RADIUS)、ロ グイン設定

個別グループの許可の設定

- ▶ 個別ユーザ グループに許可を設定するには、以下の手順に従います。
- 1. リストから目的のユーザ 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。



ポート権限の設定

サーバ ポートに対して、アクセスのタイプ、仮想メディアへのアクセスのタイプ、および 電源管理を指定できます。すべての許可についてデフォルト設定はすべて無効になっていることに注意してください。

[Access	5] (アクセス)	[VM Acces ス)	ss] (VM アクセ	電源制御	
オプション	説明	オプション	説明	オプション	説明
[None] (なし)*	アクセスを完全に 拒否します。	[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。	[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)。	[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。	[Deny] (拒否)*	アクセスを完 全に拒否しま す。
[Control] (制御)	接続先のターゲッ ト サーバを制御 します。	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-Only] (読み取り専 用) 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)。	[Access] (アクセス)	完全なアクセ ス。
[Control] (制御)	接続先のターゲッ ト サーバを制御 します。	[Read-Writ e] (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)。	[Access or Deny] (アクセスま たは拒否)	完全なアクセ ス。またはアク セスを完全に 拒否します。

* デフォルト設定

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 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 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。 詳細は、「*IP アクセス制御* 『p. 153の"[IP Access Control] (IP アクセス制御)"参照先 』」を参 照してください。

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。

▼ IP ACL	т				
	1				
Please note: Il Control as we	P Access Control is enabled ell.	I! IP ranges blocked by IP Access C	ontrol will be blocked for Group based System Access		
Rule ≇	Starting IP	Ending IP	Action		
			ACCEPT 🛩		
Append	Insert Repl	ace Delete			

- ▶ 新しいルールを追加するには、以下の手順に従います。
- 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. [Action] (アクション) で、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 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 デバイスへのアクセス が拒否されます。
- [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。
- 5. 入力する各ルールについて、手順 1 ~ 4 を繰り返します。
- ▶ ルールを挿入するには、以下の手順に従います。
- [Rule] (ルール) 番号を入力します。 [Insert] (挿入) コマンドを使用するとき は、ルール番号が必要です。
- [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。
- [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。
- ▶ ルールを置き換えるには、以下の手順に従います。
- 1. 置き換える [Rule] (ルール) 番号を指定します。



- [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 [Rule] (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 #	Starting IP	Ending IP	Action
1	192.168.50.1	192.168.55.255	ACCEPT
2	0.0.0.0	255.255.255.255	DROP
· · · · ·			ACCEPT .

とント: 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。



[User Management] (ユーザ管理)

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。

lome > User Management > Gro	up		
Group Group Name '		(
▼ Permissions			
Device Settings Diagnostics Maintenance PC-Share Security User Managem	ent		
▼ Port Permissions			
Port Dominion_KX2_101_Port1 Power Port 1	Access Deny V Deny V	VM Access Deny	Power Control Deny V Deny V
▼ IP ACL			
Rule # Starting IP	Ending IP	Action	
OK Cancel	101900 may a shifting a wear - Adverting and Ad	antina, and a star for a star well, the summer	ana analaha a kasha sili aka pakisa san shin mili ka ma ma

- グループの許可を設定します。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。詳細は、「許可の設定 『p. 52』」を参照してください。
- [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。 詳 細は、「ポート権限の設定」を参照してください。
- 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 デバイスへのアクセスを制限します。 詳細は、「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] をクリックします。



[Change Password] (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。
- [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。

ort Access	Virtual Media	User Management	Device Settings	Security
142470	TO DO T	finality ()		\sim
iome > User M	lanagement > Ch.	ange Password		
Change P	assword			
Old Passw	ord			
New Pass	word			
Confirm N	ew Password			
OK	Cancel			
				A

- 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。
- [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、 [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] 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] 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、 「[Security Settings] (セキュリティ設定) - [Strong Passwords] (強力なパスワー ド) 『p. 147の" [Strong Passwords] (強力なパスワード)"参照先 』」を参照してくだ さい。

[Authentication Settings] (認証設定)

認証設定は、この章で後述のリモート認証で説明されています。 詳細は、「認証設定」を参照してください。



リモート認証

CC-SG ユーザへの注意事項

CommandCenter Secure Gateway を使用して KX II-101 を制御している場 合、(ローカル ポート アクセスを必要とする) ローカル ユーザを除き、ユーザおよびグ ループは CC-SG によって認証されます。 CC-SG で KX II-101 を制御している 場合、ローカル ポート ユーザは、KX II-101 上で設定されているローカル ユーザ データベースまたはリモート認証サーバ (LDAP/LDAPS または RADIUS) に対し て認証され、CC-SG ユーザ データベースに対して認証されません。

CC-SG 認証についての詳細は、Raritan の Web サイト (*http://www.raritan.com/support/* http://www.raritan.com/support) か ら入手できる CommandCenter Secure Gateway のユーザ ガイド、管理者ガイ ド、またはデプロイメント ガイドを参照してください。

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、KX II-101 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 の認証元として機能することが可能です。 IAS (インタフェース認証サーバ) 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。

認証と認可

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 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。



[Authentication Settings] (認証設定)

[Authentication Settings] (認証設定) ページでは、KX II-101 へのアクセスに使用する認証の種類を設定できます。認証と認可の動作および相違点についての詳細は、「**認証と認可** 『p. 58』」を参照してください。

注: ローカル認証はリモート認証(LDAP または RADIUS)を選択した場合で も使用されます。

- > 認証を設定するには、以下の手順に従います。
- [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。

Home > User Management > Authentication Settings
Andres Carles Sediare
Authentication Settings
 Local Authentication
C LDAP
Primary LDAP Server
Secondary LDAP Server
Secret Phrase
Confirm Secret Phrase
Enable Secure LDAP
Port
389
Secure LEAP Port
Certificate File
Branse
un un rumming/fatric user
User Search DN
Type of External I BAP Server
Generic LDAP server
Active Directory Domain
C RADIUS
Primary RADIUS Server
Shared Secret
Authentication Port
Accounting Port
1913
1 1
Retries
3
Secondary RADIUS Server
shared secret
Authentication Port
1512
1813
Timeout (in seconds)
Retries
3
Cickal Authoritation Turn
DAP 4
OK Reset To Defaults Cancel
the second s



- 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] (LDAP)、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。
- [LDAP] (LDAP) を選択した場合は、「LDAP 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。
- [RADIUS] (RADIUS) を選択した場合は、「RADIUS リモート認証の実装 『p. 64』」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。
- > 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。
- ▶ 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。



ユーザ、グループ、アクセス許可

LDAP リモート認証の実装

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プ ロトコル: LDAP) は、TCP/IP 上で動作するディレクトリ サービスを照会および変 更するためのネットワーキング プロトコルです。 クライアントは、LDAP 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 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、以下の情報を入力します。

Authentication Settings	
Local Authentication	
O case	
Printary LDAP Server	
Secondary LDAP Server	
Secret Planse	
Confirm Secret Placese	
Enable Secure LDAP	
Pert	
Secure LDAP Port	
6.5m	
Certificate File	
Utroom 2	
en of Automistrative User	
User Search DII	
Type of External LDAP Server	
Active Directory Domain	
- DAMES	
O Patrice	
Printary RADIUS Server	
Shared Secret	
Authentication Port	
Accounting Port	
(ets)	
Timeout (in seconds)	
1	
2	
Secondary RADIUS Server	
Church Cound	
Sum on Sector	
Authentication Port	
10(2	
Accounting Port	
Timeout (in seconds)	
t	
Retries	
4	
Global Authentication Type	
DAD -	



- [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP 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。 [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。
- (オプション) [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 サーバの IP アドレスまたは DNS 名を入力します。 [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。
- [Secret Phrase] (秘密フレーズ) フィールドに、リモート認証サーバへの認証に 必要となるサーバの秘密フレーズ (パスワード) を入力します。次に、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドに、サーバの秘密フレーズ (パ スワード) を再入力します。既存のスキーマを変更しないでください。 LDAP サーバで使用している文字列を使用します。
- 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。[Secure LDAP Port] (セキュア LDAP ポート) フィールドが有効になります。 Secure Sockets Layer (SSL) は、KX II-101 が LDAP 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。
- 5. [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。
- [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 がオンのときに有効になります。
- [Certificate File] (証明書ファイル)。LDAP 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。このフィールドは、[Enable Secure LDAP] (セキュア LDAP を 有効にする) ボックスがオンのときに有効になります。
- [DN of administrative User] (管理者ユーザの DN)。管理者ユーザの識別名です。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。たとえば、管理者ユーザの DN として、 "cn=Administrator,dc=Users=,dc=testradius,dc=com"と設定します。
- [User Search DN] (ユーザ検索 DN)。これは、LDAP に対しバインドする 名前、およびデータベース内で指定されたベース DN の検索を開始する場所 を示します。たとえば、"cn="Users,dc=raritan,dc=com" というベース検索値 を設定します。このフィールドに入力する適切な値については、担当の認証サ ーバ管理者に問い合わせてください。
- 10. [Type of external LDAP server] (外部 LDAP サーバの種類)。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 ディレクトリ サービスの実装です。
- 11. [Active Directory Domain] (Active Directory ドメイン)。 Active Directory ドメインの名前を入力します。

ユーザ グループ情報を Active Directory サーバから返す

KX II-101 では、ユーザを KX II-101 でローカルに定義する必要なく、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 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。

注: Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、KX II-101 はこの設定をサポートします。こ の場合、以下に示す手順を実行する必要はありません。 AD LDAP スキーマを更 新する方法についての詳細は、「LDAP スキーマの更新『p. 66』」を参照してくださ い。

- > KX II-101 で AD サーバを有効にするには、以下の手順に従います。
- KX II-101 を使用して、特殊なグループを作成し、適切な許可および特権をグ ループに割り当てます。たとえば、KVM_Admin や KVM_Operator という グループを作成します。
- 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 ユーザを割り当て ます。
- 4. KX II-101 で、AD サーバを有効にし、適切に設定します。 「LDAP リモート 認証の実装」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 には、[Admin] (管理者) と [<Unknown>] (不明) のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることは できません。 Active Directory サーバでこれらと同じグループ名が使用されて いないことを確認してください。
- Active Directory サーバから返されたグループ情報が KX II-101 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)、アカウンティング (accounting)) プロトコルです。

\triangleright	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。
------------------	--------	-----------------	-------------

Shared	Secret			
Authen	tication F	Port		
1812				
Accoun	ting Port	ú.		
1813				
Timeou	t (in sec	onds)		
1	8			
Retries				
3				
Second	ary Radii	us Ser	ver	
Second Shared	ary Radii Secret	us Ser	ver	
Second Shared	ary Radii Secret	us Ser	ver	
Second Shared Authen 1812	ary Radii Secret Lication F	us Ser Port	ver	
Second Shared Authen 1812 Accoun	ary Radii Secret Lication F	us Ser Port	ver	
Second Shared Authen 1812 Account 1813	ary Radii Secret Lication F	Port	ver	
Second Shared Authen 1812 Accoum 1813 Timeou	Secret	Port	ver	
Second Shared Authen 1812 Account 1813 Timeou	ary Radii Secret Lication F ting Port	onds)	ver	
Second Shared Authen 1812 Accoun 1813 Timeou 1 Retries	ary Radii Secret Lication F Ling Port	Port onds)	ver	
Second Shared Authen 1812 Accoum 1813 Timeou 1 Retries 3	ary Radii	Port	ver	

- 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、[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 ィールド) に入力します。
- 2. (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。 共有の秘密とは、KX II-101 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。
- 3. [Authentication Port] (認証ポート)。デフォルトの認証ポートは 1812 です。 このポートは必要に応じて変更できます。


- 4. [Accounting Port] (アカウンティング ポート)。 デフォルトのアカウンティング ポ ートは 1813 です。このポートは必要に応じて変更できます。
- [Timeout (in seconds)] (タイムアウト (秒))。デフォルトのタイムアウトは 1 秒です。この値は必要に応じて変更できます。このタイムアウトは、KX II-101 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。
- [Retries] (再試行回数)。デフォルトの再試行回数は 3 回です。この回数は 必要に応じて変更できます。これは、KX II-101 が RADIUS サーバに対し て認証要求を送信する回数です。
- 7. [Global Authentication Type] (グローバル認証タイプ)。ドロップダウン リストのオプションから選択します。
 - [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 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。

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 デバイスは、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、次の形 式となります。

Raritan:G{GROUP_NAME}

GROUP_NAME は文字列で、ユーザが属するグループの名前を示します。

RADIUS 通信交換仕様

KX II-101 ユニットは、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログオン	
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 ユニットの IP アドレス



リモート認証

属性	データ
ログオン	
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL(5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX II-101 ユニットの IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログオフ	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL(5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KX II-101 ユニットの IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

LDAP スキーマの更新

注: この章に記載されている手順は、経験豊富なユーザのみが行うようにしてください。

ユーザ グループ情報を返す

この章の情報を参考にして、認証の成功後にユーザ グループ情報を返すよう設定します (認証を補助します)。



ユーザ、グループ、アクセス許可

LDAP から返す場合

LDAP/LDAPS 認証に成功すると、KX II-101 では、ユーザ 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 LDAP サーバは、以下の名前の 属性を返すことで、これらのユーザ グループ名を指定できます。

rciusergroup attribute type: string

これには、LDAP/LDAPS サーバ上でスキーマの拡張が必要な場合があります。 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: この操作は、経験豊富な Active Directory 管理者のみが行うようにしてください。

Windows 2000 Server 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 の該当するマニュアルを参照してください。

- Active Directory のスキーマ プラグインをインストールします。手順については 、Microsoft Active Directory のマニュアルを参照してください。
- 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ためのレジストリ設定

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には、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、以下の手順に従います。
- ウィンドウの左ペイン (メニューをクリックして表示される領域)の [Active Directory Schema] (Active Directory スキーマ) ルート ノードを右クリック し、次に [Operations Master] (オペレーション 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 ボックスが表 示されます。

Change Schema Master	<u>? ×</u>			
The schema master manages modifications to the schema. Only one server in the enterprise performs this role.				
C <u>u</u> rrent schema master (online):				
rci-gcf4j2nzmzt.mypc.mydomain.com				
To transfer the schema master role to the targeted domain controller below, click Change.	<u>Change</u>			
1				
	Close			

- (オプション) [The Schema may 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する) チェック ボックスをオンにします。
- 3. [OK] をクリックします。

新しい属性の作成

- rciusergroup クラスの新しい属性を作成するには、以下の手順に従います。
- ウィンドウの左ペインの [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. **左ペインの** [Attributes] (属性) を右クリックします。



 [New] (新規) をクリックして、[Attribute] (属性) を選択します。 警告メッセ ージが表示されたら、[Continue] (続ける) をクリックします。[Create New Attribute] (新規属性の作成) ダイアログ ボックスが表示されます。

Create New Attribute	<u>? ×</u>
Create a New Att	ribute Object
Common <u>N</u> ame:	rciusergroup
LDAP Display Name:	rciusergroup
Unique X500 <u>O</u> bject ID:	1.3.6.1.4.1.13742.50
Description:	Raritan's LDAP attribute
Syntax and Range	
<u>S</u> yntax:	Case Insensitive String
Mjnimum:	1
Ma <u>x</u> imum:	24
☐ <u>M</u> ulti-Valued	OK Cancel

- 4. [Common Name] (共通名) フィールドに「rciusergroup」と入力します。
- 5. [LDAP Display Name] (LDAP 表示名) フィールドに「rciusergroup」と入 力します。
- 6. [Unique x5000 Object ID] (一意の x5000 オブジェクト ID) フィールドに 「1.3.6.1.4.1.13742.50」と入力します。
- 7. わかりやすい説明を [Description] (説明) フィールドに入力します。
- [Syntax] (構文) ドロップダウン矢印をクリックし、リストから [Case Insensitive String] (大文字/小文字の区別のない文字列) を選択します。
- 9. [Minimum] (最小) フィールドに「1」を入力します。
- 10. [Maximum] (最大) フィールドに「24」を入力します。
- 11. [OK] をクリックして、新しい属性を作成します。

クラスへの属性の追加

- ▶ 属性をクラスに追加するには、以下の手順に従います。
- 1. ウィンドウの左ペインの [Classes] (クラス) をクリックします。



🚡 Console1 - [Console Root)	Active Directory Schema	[rci-gcf4j2nzmzl	t.mypc.mydomain.com	_ 🗆 🗙
📸 Eile Action View Favgrites <u>W</u> indow <u>H</u> elp				
	3 2			
🛄 Console Root	Name	Туре	Status	Desci 🔺
Active Directory Schema	serviceConnectionPoint	Structural	Active	Servi
🕂 🔁 Classes	serviceInstance	Structural	Active	Servi
···· 📔 Attributes	simpleSecurityObject	Auxiliary	Active	The s
	■t¦ site	Structural	Active	Site
	■t¦ siteLink	Structural	Active	Site-L
	📲 siteLinkBridge	Structural	Active	Site-L
	📲 sitesContainer	Structural	Active	Sites
	■t¦ storage	Structural	Active	Stora
	■t§ subnet	Structural	Active	Subn
	■t¦ subnetContainer	Structural	Active	Subn
	📲 🖁 subSchema	Structural	Active	SubS
	📲 🖁 top	Abstract	Active	Тор
	📲 trustedDomain	Structural	Active	Trust
	📲 typeLibrary	Structural	Active	Туре
	Cuser New Window	w From Here	Active	User
	Solume		Active	Volun 🖵
4	Refresh			•
	Properties	;		
	Help			

2. 右ペインで [user] (ユーザ) クラスまでスクロールし、右クリックします。

3. メニューから [Properties] (プロパティ)を選択します。 [user Properties] (ユ ーザ プロパティ) ウィンドウが表示されます。



Seneral Relation	onship Attributes Security		ses\user	
	user		Select Schema Object	<u>य</u> े
Mandatory:			Select a schema object: productCode profilePath proxiedDijectName. proxyAddresses	▲ OK Cancel
Optional	accountExpires aCSPolicyName admirCount badPasswordTime badPwdCount codePage controlAccessRights	Add Remove	proxyGenerationEnabled proxyLifetime publicKeyPolicy purportedSearch pwdHistoyLength pwdLastSet pwdProperties quelyFilter quelyFilter quelyFilter quelyPoint quelyPoint	
	defaultClassStore	1	queryProicyUbject rangeLower rangeUpper rclusergroup rclusergroup rDNAmD	-

4. [Attributes] (属性) タブをクリックして開きます。

- 5. [Add] (追加) をクリックします。
- [Select Schema Object] (スキーマ オブジェクト選択) リストから 「rciusergroup」を選択します。
- [Select Schema Object] (スキーマ オブジェクト選択) ダイアログ ボックスで [OK] をクリックします。
- 8. [User Properties] (ユーザ 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 キャッシュの更新

- ▶ スキーマ キャッシュを更新するには、以下の手順に従います。
- ウィンドウの左ペインの [Active Directory Schema] (Active Directory ス キーマ) を右クリックして、ショートカット メニューから [Reload the Schema] (ス キーマの再ロード) を選択します。
- 2. Active Directory スキーマ MMC (Microsoft Management Console) コ ンソールを最小化します。



ユーザ メンバの rciusergroup 属性の編集

Windows 2003 Server 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 2003 サーバ インス トール CD 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読み込まれます。 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、ディレクトリ サービスと共通の管理 タスクを実行できます。

- グループ rciusergroup 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。
- Windows 2003 サーバ インストール CD で [Support] (サポート)、[Tools] (ツール)を選択します。
- 2. SUPTOOLS.MSI をダブルクリックして、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ディレクトリに進みます。
- 4. adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。

🝕 ADST Edit				_ C X
🤣 Elle Action Yew Window He	þ			_ 6 ×
+ → 🗰 🗟 🖳 😫				
Apst Eckt Domain [rd-gdf4]2nemat.mypc.my Configuration [rd-gdf42nemat.my Schema [rd-gdf42nemat.mypc.m	Name Domain [roi-qof4i2namat.mypc Configuration [roi-qof4i2namat.myp Scheme [roi-qof4i2namat.myp	Cass domeinDV/S configuration dND	Ostinguished Name	
	•			
1				3

5. [Domain] (ドメイン)を開きます。



🝕 ADSI Edit			
🐳 Elle Action Yex Window He	þ		.
🌩 → 🗈 🗊 🗙 🗳 🖓	2		
📣 ADSI Edit	Name	Class	Distinguished Name
🗈 📑 Domain [rd-qdf4]2namat.mypc.ms	🛄 CN=Administrator	user	CN=Administrator, ON=Users, DC=mypc, DC=mydomain, G
E - 2 DC=mypc,DC=mydomain,DC	CN=Cert Publishers	group	CN=Cert Publishers, CN=Users, DC=nypc, DC=mydomain
🕑 - 🔛 ON - Bultin	CN=DrsAdmins	group	CN=DnsAdmins, CN=Users, DC=nypc, DC=mydomain, DC
HI-COMPUTERS	CN=DrsUpdateProxy	group	CN=DnsUpdateProxy, CN=Users, DC=mypc, DC=mydame
ti 🎯 CU=Doman Controllers	CN=Domain Admins	group	CN=Domain Admins, CN=Users, DC=nypc, DC=mydomain
B-B OV-Later Adda ad	CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=mypc,DC=mydor
H- CILENTOS Ductas	CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=mypc,DC=mydor
R-N CN-Program Data	CN=Domain Guests	group	CN=Domain Guests, CN=Users, DC=mypc, DC=mydomain
🕅 - 🔯 ON=System	CN=Domain Users	group	CN=Domain Users, CN=Users, DC=mypc, DC=mydomain, (
	CN-Enterprise Admins	group	CN-Enterprise Admins, CN-Users, DC-mypc, DC-mydam
E⊢ 🗄 Configuration [rcl-gcf4j2nzmat.ms	CN-Group Policy Greator Dw	group	CN=Group Policy Greator Owners, CN=Users, DC=mypc, t
🗄 🗍 Schema [rd-gdf4j@nzmat.mypc.mi	CN=Guest	user	CN=Guest, CN=Users, DC=mypc, DC=mydomain, DC=com
_	CN-HelpServicesGroup	group	CN=HelpServicesGroup, CN=Users, DC=mypc, DC=mydor
	CN-k/btgt	user	CN=krbtgt, CV=Users, DC=mypc, DC=mydomain, DC=con
	CN-RAS and JAS Servers	group	CN=RAS and IAS Servers, CN=Users, DC=mypc, DC=myp
	CN-Schema Admins	group	CN=Schema Admins, CN=Lisers, DC=mypc, DC=mydomair
	CN-SUPPORT_388945a0	user	CN=SUPPORT_388995a0,CN=Users,DC=mypc,DC=myd
	📴 CN—TelnetClients	group	CN=TeinetClients, CN=Users, DC=mypc, DC=mydomain, D
• • • •	•		•

6. ウィンドウの左側のペインで「CN=Users」フォルダを選択します。

- 7. 右側のペインからプロパティを編集するユーザ名を選択します。ユーザ名を右ク リックして、[Properties] (プロパティ)を選択します。
- 8. [Attribute Editor] (属性エディタ) タブをクリックします(まだ開いていなかった場合)。



9. [Attributes] (属性) リストから「rciusergroup」を選択します。

CN=Administrator Prope	rties	<u>?</u> ×
Attribute Editor Security		
1		
✓ Show mandatory attrib	outes	
🔽 Show <u>o</u> ptional attribut	es	
Show only attributes t	hat have values	
Attri <u>b</u> utes:	-	
Attribute	Syntax	Value 🔺
proxyAddresses	Unicode String	<not set=""></not>
pwdLastSet	Large Integer/	128299285248088608
queryPolicyBL	Distinguished	<not set=""></not>
rciusergroup	Case Insensiti	<not set=""></not>
registeredAddress	Octet String	<not set=""></not>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
replUpToDateVector	Octet String	<not set=""></not>
repsFrom	Octet String	<not set=""></not>
repsTo	Octet String	<not set=""></not>
revision	Integer	<not set=""></not>
rid	Integer	<not set=""></not>
roomNumber	Unicode String	<not set=""></not>
sAMAccountName	Unicode Strina	Administrator
1		
Edit		
	OK	Cancel Apply



🐳 ADSI Edit	_ <u> </u>
🏟 Eile Action Yiew Window Help	p
	Administrator Properties
Attri	ibute Editor Security
Configuration [rd-gcf4j2namst.my] Domain [rd-gcf4j2namst.my] Characteristic CN=Baltin CN=Baltin CN=Computers COmputers CN=Computers CN=Computers CN=Computers CN=Computers CN=Computers CN=Computers CN=Computers COmputers COmpu	Image: Show gandatory attributes N=Users, DC=mypc, DC=mydomain, IC Image: Show optional attributes CN=Users, DC=mypc, DC=mydomain, DC Image: Show only attributes that have galues Visition Image: Show only attribute Editor Visition
	Elear OK Cancel up,CN=Users,DC=mypc,DC=mydor DC=mypc,DC=mydor
	revision Integer «Not Set> rid Integer «Not Set> roomNumber Unicode String «Not Set> s&M&ccountName Unicode String Administrator ▼ Edit
	OK Cancel Apple
	×

10. [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 ボックスが表示されます。

11. ユーザ グループ (Dominion KX II-101 で作成済み) を [Edit Attribute] (属性の編集) フィールドに入力します。

String Attribute Editor		2	×
Attribute: roiusergroup			
<u>V</u> alue:			
Admin			1
<u>C</u> lear	OK	Cancel	

12. [OK] をクリックします。



Virtual KVM Client

この章の内容

6

概要	77
オプション	78
マウス ポインタの同期	80
[Connection] (接続) メニュー	
[Keyboard] (キーボード) メニュー	
[Video] (ビデオ) メニュー	
[Mouse] (マウス) メニュー	
VKC 仮想メディア	97
[Tools] (ツール) メニュー	
[View] (表示) メニュー	
[Help] (ヘルプ) メニュー	100



概要

KX II-101 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 のウィンドウが開きます。

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 ブラウザ表示を更新すると Virtual KVM Client 接続が切断されて しまうので注意してください。



Virtual KVM Client に用意されている機能は、メニューおよびツール バーを使用 してアクセスできます。

機能	説明
メニュー バー	コマンドや設定のドロップダウン メニュー
ツール バー	よく使う機能やコマンドのショートカット ボタン
ターゲット サーバのビデオ ウィン ドウ	ターゲット デバイスの表示
ステータス バー	接続パラメータ、ターゲット サーバのウィンドウ サイズ、同時接続、Caps Lock インジケータ、 Num Lock インジケータに関するリアルタイム 情報



オプション

メニュー ツリー

以下のリストに、Virtual KVM Client のすべてのメニューとメニュー項目を示します。

- [Connection] (接続) メニュー:
 - [Properties] (プロパティ)
 - [Connection Info] (接続情報)
 - [Exit] (終了)
- [Keyboard] (キーボード) メニュー:
 - [Send Ctrl + Alt + Delete] (Ctrl + Alt + Delete の送信)
 - [Keyboard Macros] (キーボード マクロ)
 - [Keyboard Mouse Options] (キーボード マウス オプション)
 - [User-Created Macros] (ユーザ作成マクロ) オプション
- [Video] (ビデオ) メニュー:
 - [Refresh Screen] (画面の更新)
 - [Auto-sense Video Settings] (ビデオ設定の自動検出)
 - [Calibrate Color] (色調整)
 - [Video Settings] (ビデオ設定)
- [Mouse] (マウス) メニュー:
 - [Synchronize Mouse] (マウスの同期)
 - [Single Mouse Cursor] (シングル マウス カーソル)
 - [Absolute] (絶対)
 - [Intelligent] (インテリジェント)
 - [Standard] (標準)
- [Virtual Media] (仮想メディア) メニュー:
 - [Connect Drive] (ドライブの接続)
 - [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)
- [Tools] (ツール) メニュー:
 - [Options] (オプション)
- [View] (表示) メニュー:
 - [View Toolbar] (ツール バーの表示)



Virtual KVM Client

- [Scaling] (拡大、縮小)
- [Target Screen Resolution] (ターゲット画面解像度)
- [Help] (ヘルプ) メニュー:
 - [About Raritan Virtual KVM Client] (バージョン情報)

ツール バー	
ボタン	説明
	[Properties] (プロパティ)
	[Video settings] (ビデオ設定)
Q	[Calibrate color] (色調整)
22	[Synchronize the target mouse cursor] (ターゲット マウ ス カーソルの同期)
¢	[Refresh screen] (画面の更新)
	[Auto-sense video] (ビデオ自動検出)
C A DEL	[Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)
ß	[Single mouse cursor] (シングル マウス カーソル)
X	[Full screen] (全画面)
	[Resize video to fit screen] (画面に合わせてビデオを調整)



マウス ポインタの同期

マウスが使用されているターゲット サーバをリモートで表示する場合、2 つのマウス ポ インタが表示されます。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、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することもできます。 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。 使用可能 なマウス モードについての詳細は、「[Mouse Menu] (マウス) メニュー 『p.93の "[Mouse] (マウス) メニュー"参照先 』」を参照してください。

マウス同期のヒント

マウスを同期するには、以下の手順に従います。

- 選択したビデオ解像度と垂直走査周波数が KX II-101 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、KX II-101 デバイスの表示で使用している実際の値が表示されます。サポートされるビデオ解像度についての詳細は、デバイスのユーザ ガイドの「サポートされるビデオ解像度」を参照してください。
- 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。詳細は、デバイス ユーザ ガイドの「ターゲット サーバの接続距離と ビデオ解像度」を参照してください。
- 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。
 詳細は、デバイス ユーザ ガイドの「インストールと設定」を参照してください。



- 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 11」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。



[Connection] (接続) メニュー

[Connection] (接続) メニュー

[Properties] (プロパティ) ダイアログ ボックス

KX II-101 の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。 KX II-101 ユニットの 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。

- ▶ 接続プロパティを設定するには、以下の手順に従います。
- [Connection] (接続)、[Properties] (プロパティ)を選択します。
 [Properties] (プロパティ) ダイアログ ボックスが開きます。

Connection Speed	10 Ethernet
Color Depth	15-bit RGB Color
Smoothing	Low

2. ドロップダウン リストから接続スピードを選択します。 KX II-101 では、使用可能な帯域幅を自動的に検知できるため、利用する帯域幅は制限されません。 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。

[1G Ethernet]

[100 Mb Ethernet]

[10 Mb Ethernet]

[1.5 Mb (MAX 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))

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

- 3. ドロップダウン リストから色深度を選択します。 KX II-101 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 ビット RGB カラー
 - 8 ビット RGB カラー
 - 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。

- 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。



- > 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。

[Connection Info] (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)、[Connection Info] (接続情報) 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)。 KX II-101 デバイスの名前です。
- [IP Address] (IP アドレス)。 KX II-101 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] 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。

[Exit] (終了)

- Virtual KVM Client (現在アクセスしているターゲット)を閉じるには、以下の手順に従います。
- [Connection] (接続)の [Exit] (終了)を選択します。



[Keyboard] (キーボード) メニュー

[Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)

頻繁に使用されるため、Ctrl+Alt+Delete キーボード マクロは、Virtual KVM Client にあらかじめ組み入れらています。

このキー シーケンスは、現在接続されているターゲット サーバに送信されます。 方、Virtual KVM Client の使用中に Ctrl+Alt+Delete キーを押した場合、キ ー シーケンスは意図したとおりにはターゲット サーバへ送信されず、オペレーティング システムの構造により、まず使用している PC がコマンドを解釈します。



- ターゲット サーバに Ctrl+Alt+Delete キー シーケンスを送信するには、以下の手順に従います。
- [Keyboard] (キーボード)の [Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信)を選択します。または、
- ツール バーの [Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送信) ボタンを クリックします。

[Keyboard Macros] (キーボード マクロ)

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

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



キーボード マクロの作成

- > キーボード マクロを作成 (追加) するには、以下の手順に従います。
- [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。

Run Macro
Add
Remove
Modify
Close

[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。

Add Keyboard Macro	1.5.1.5.2.4.4		x
Keyboard Macro Name			
Keys to Press	Keys to Release	Macro Sequence	
All Keys			
Left Ctrl Right Ctrl			
Left Alt Right Alt Left Shift			
Right Shift			
Press Key	Release Key	Remove ^ v	
	OK	Cancel Clear	

- [Keyboard Macro Name] (キーボード マクロ名) フィールドに名前を入力し ます。この名前は、マクロが作成された後に Virtual KVM Client メニュー バーに表示されます。この例では、「Minimize All Windows」(全ウィンドウ を最小化)を使用します。
- 4. [Keys to Press] (押すキー) ドロップダウン リストで、以下の操作を行います。
 - a. スクロールして、キー操作をエミュレートするキーを選択します (押す順番で 選択してください)。



 b. 1 つ選択するごとに、[Press Key] (キーを押す) ボタンをクリックします。キ ーを選択するたびに、そのキーが [Keys to Release] (リリースするキー) フ ィールドに表示されます。

この例では、Windows キーと D キーの 2 つのキーを選択します。

- 5. [Keys to Release] (リリースするキー) フィールドで、以下の操作を行います。
 - a. キー リリースをエミュレートするキーを選択します (リリースする順番で選択 してください)。
 - b. 1 つ選択するごとに、[Release Key] (キーをリリース) をクリックします。

この例では、押したキーが両方ともリリースされる必要があります。

 [Macro Sequence] (マクロ シーケンス) を確認します。この内容は、[Keys to Press] (押すキー) と [Keys to Release] (リリースするキー) の指定内容に応 じて自動的に生成されます。 [Macro Sequence] (マクロ シーケンス) の内容 が目的のキー シーケンスであることを確認します。 (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。)

eyboard Macro		
Keyboard Macro Name	Minimize All Window	15
Keys to Press	Keys to Release	Macro Sequence
All Keys 💌		
9 C)		PRESS Left Windows Key PRESS D
	-	RELEASE D
3	d	
Press Key	Freiense Key	Cancel Clear
Press Key	Release Key OK	Remove ^ v Cancel Clear

ヒント: [^] キー ボタンと [v] キー ボタンを使用すると、キー シーケンスを並べ 替えることができます。

 [Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスで [OK] をクリックしてマクロを保存します。



[Keyboard Macro] (キーボード マクロ) ダイアログ ボックスで [Close] (閉じる) をクリックします。 作成したキーボード マクロが [Keyboard] (キーボード) メニューのオプションとして表示されます。

Connection	USB Profile	Keyboard	Video	Mouse	Virtual Me
5 F Q Q Z F S	Send Ctrl Set CIM K	+Alt+Dele (eyboard/l	ete Mouse Opt	tions	
		Keyboard	Macros		
		Minimize	All Windo	ws C	trl+Alt+0

- すべてのフィールドをクリアして最初からやり直すには、以下の手順に従います。
- [Clear] (クリア) ボタンをクリックします。

キーボード マクロの実行

作成したキーボード マクロは、[Keyboard] (キーボード) メニューのマクロ名をクリック することで実行できます。

- > (この例を使用して)マクロを実行するには、以下の手順に従います。
- [Keyboard] (キーボード)の [Minimize All Windows] (全ウィンドウを最小化)を選択します。

また、[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスからマクロを 選択することもできます。

- > マクロを実行するには、以下の手順に従います。
- [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. [Run Macro] (マクロの実行) をクリックします。

キーボード マクロの変更

- ▶ マクロを変更するには、以下の手順に従います。
- [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] をクリックします。

キーボード マクロの削除

- ▶ マクロを削除するには、以下の手順に従います。
- [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。

[Video] (ビデオ) メニュー

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) オプションを使用すると、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) オプションを使用すると、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) オプションを使用すると、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) オプションを使用すると、手動で設定を調整できます。

[Refresh Screen] (画面の更新)

[Refresh Screen] (画面の更新) オプションを使用すると、ビデオ画面が更新されます。

な
[Refresh Screen] (画面の更新) ボタン

- 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)を選択します。
- 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] (ビデオ設定の自動検出)

[Auto-sense Video Settings] (ビデオ設定の自動検出) オプションを使用すると、 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。

[Auto-sense Video Settings] (ビデオ設定の自動
検出) ボタン

- > ビデオ設定を自動的に検出するには、次のいずれかの手順に従います。
- [Video] (ビデオ)の [Auto-sense Video Settings] (ビデオ設定の自動検出)を選択します。
- 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。

[Calibrate Color] (色調整)

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、 輝度、彩度) を最適化するために使用します。 KX II-101 の色設定は、ターゲット サーバごとに適用されます。



注: [Calibrate Color] (色調整) オプションは、現在の接続のみに適用されます。

- ▶ 色を調整するには、以下の手順に従います。
- 1. グラフィカル ユーザ インタフェースが動作しているターゲット サーバに対して KVM リモート接続を開きます。
- [Video] (ビデオ)の [Calibrate Color] (色調整)を選択します (または、 [Calibrate Color] (色調整) ボタンをクリックします)。 ターゲット デバイス画面 の色が調整されます。

[Video Settings] (ビデオ設定)

[Video Settings] (ビデオ設定) オプションを使用すると、ビデオ設定を手動で調整 できます。

[Video (ビデオ)	o Settings] 設定)	ビデオ パラメータを手動で調整するための [Video Settings] (ビデオ設定) 画面を開きま す。
-----------------	--------------------	---



- > ビデオ設定を変更するには、以下の手順に従います。
- [Video] (ビデオ)の [Video Settings] (ビデオ設定)を選択します。 [Video Settings] (ビデオ設定) ダイアログ ボックスが表示され、現在の設定が表示されます。

video Settings			×
Noise Filter		2	
Brightness Red		41	
Brightness Green		46	
Brightness Blue		58	
Contrast Red		223	
Contrast Green		214	
Contrast Blue		208	
Clock		1344	
Phase		13	
Horizontal Offset		281	
Vertical Offset		28	
	Auto Color Calibration		
	Best possible video mode		
	C Quick sense video mode		
	OK Cancel Ag	oly	

- 2. スライダを使用して、目的の結果が得られるように設定を調整します (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)。
 - [Noise Filter] (ノイズ フィルタ): KX II-101 では、グラフィック カードからの ビデオ出力の電気的干渉を除去することができます。この機能により、画 質が最適化され、消費される帯域幅が低減されます。設定値を大きくす ると、ピクセル変動は隣接するピクセルと比較して大きな色変化がある場合 にのみ送信されます。ただし、しきい値を高く設定しすぎると、正常な画面 変更が意図せずフィルタリングされてしまう場合があります。 設定値を低くすると、ほとんどのピクセル変動が送信されます。しきい値を 低く設定しすぎると、帯域幅の使用量が高くなることがあります。
 - [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。



- [Red] (赤)。赤信号の輝度を制御します。
- [Green] (緑)。緑信号の輝度を制御します。
- [Blue](青)。青信号の輝度を制御します。
- [Color Contrast Settings] (色のコントラストの設定): コントラストの調 節を制御します。
 - [Contrast Red] (赤コントラスト)。赤信号を制御します。
 - [Contrast Green] (緑コントラスト)。緑信号を制御します。
 - [Contrast Blue] (青コントラスト)。 青信号を制御します。
- 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、Raritan テクニカル サポートにお問い合わ せください。

- [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。クロック設定に変更を加えると、ビデオ画像が水平方 向に拡大または縮小されます。奇数値を設定することをお勧めします。 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。
- [Offset] (オフセット): 画面上の位置を制御します。
 - [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。
 - [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。
- [Auto Color Calibration] (自動色調整)。 色の調整を自動的に行う場合は、このオプションをオンにします。
- [Video Sensing] (ビデオ検出): 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。
- 3. [Apply] (適用) をクリックします。ビデオ設定が変更されます。

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。

[Mouse] (マウス) メニュー

ターゲット サーバを制御しているとき、KX II-101 リモート コンソールには、クライアン ト ワークステーションとターゲット サーバの 2 つのマウス カーソルが表示されます。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 モードにおいて設定が適切に行われている場合、2 つのマウス カー ソルは同調します。マウスの同期に問題がある場合は、「ターゲット サーバの設定」 を参照してください。

KX II-101 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。

- Absolute (ずれない) (マウス同期)
- Intelligent (インテリジェント) (マウス モード)
- Standard (標準) (マウス モード)

[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) オプションを使用 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。

0.000	
22	[Synchronize
	Mouse] (マウスの同期
)

- 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)を選択します。
- 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。



[Single Mouse Cursor] (シングル マウス カーソル)

[Single Mouse Cursor] (シングル マウス カーソル) を使用すると、「シングル マウ ス モード」になります。このモードでは、ターゲット サーバのマウス カーソルだけが画 面に表示され、ローカル PC のマウス ポインタは表示されません。 シングル マウス モードでは、[Synchronize Mouse] (マウスの同期) オプションは使用できません (単独のマウス カーソルを同期化する必要がないため)。

	[Single Mouse Cursor] (シングル マウ ス カーソル)
--	--

- ▶ シングル マウス モードに入るには、次のいずれかの手順に従います。
- [Mouse] (マウス)の [Single Mouse Cursor] (シングル マウス カーソル)を 選択します。
- ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カー ソル) ボタンをクリックします。
- > シングル マウス モードを終了するには、以下の手順に従います。
- 1. シングル マウス モードに切り替えるときは、次のメッセージが表示されます。 [OK] をクリックします。

×
this mode,
d keyboard.

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



[Standard] (標準)

これは、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、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 モードはデフォルトです。

- ▶ 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。



[Intelligent] (インテリジェント)

KX II-101 デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス 設定を検出し、それに応じてマウス ポインタを同期できるので、ターゲットでマウスの 加速を設定できます。 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 モードについての詳細は、『Raritan Multi-Platform Client ユーザ ガイド』(「付録 B: インテリジェント マウス同期の条件」) を参照してくださ い。このガイドは、Raritan の Web サイト

(http://www.raritan.com/support/productdocumentation) から入手可能 です。または、KX II-101 に付属の Raritan ユーザ マニュアルおよびクイック セット アップ ガイド CD-ROM を参照してください。

- ▶ インテリジェント マウス モードに切り替えるには、以下の手順に従います。
- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

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

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



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

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

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



[Absolute] (絶対)

注: Absolute Mouse Synchronization は、仮想メディアに対応する USB CIM (D2CIM-VUSB) でのみ使用できます。

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ポインタ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ます。マウス ポインタは、タ ーゲット サーバ上の正確な位置に移動します。

- ▶ 絶対マウス 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] (絶対)を選択します。

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*『p. 101』」を参照してください。



[Tools] (ツール) メニュー

[Options] (オプション)

[Tools] (ツール) メニューでは、Virtual KVM Client に関する特定のオプション (デュアル マウス モードでのマウスの同期、ログ記録の有効化、キーボードの種類、 ターゲット画面解像度モードを終了するホットキー)を指定できます。

- ▶ 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。
- [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。

Options			
F (Enable Logging)			
Keyboard Type:	US/International		
Exit Target Screen Resolution Mode - Hotkey.	Ctrl+Alt+M		
Exit Single Cursor Mode - Hotkey:	Ctrl+Alt+O 💌		
	OK Cancel		

- アクニカル 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)
 - ベルギー語 (ベルギー)
 - ノルウェー語 (ノルウェー)
 - デンマーク語 (デンマーク)
 - スウェーデン語 (スウェーデン)



- [Exit Target Screen Resolution Mode Hotkey] (ターゲット画面解像度モ ードの終了 - ホットキー)。ターゲット画面解像度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。ドロップダウン リストから選択します。
- [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 カーソルに戻るために使用するホットキーで、ドロップダウン リストから選択しま す。
- 6. [OK] をクリックします。

[View] (表示) メニュー

[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)

ターゲット画面解像度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)。

- > ターゲット画面解像度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 [Target Screen Resolution] (ターゲット画面解像度)を 選択します。
- > ターゲット画面解像度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。デフォルトは Ctrl+Alt+M です。

CC-SG ユーザへの注意事項: [Target Screen Resolution] (ターゲット画面解像 度) は無効になっています。KX II-101 デバイスが CC-SG 管理の下にない場合 に利用できるのは、全画面モードのみです。

[Help] (ヘルプ) メニュー

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

このメニュー オプションを選択すると、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、Raritan 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。
- [Help] (ヘルプ)の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。


仮想メディア

この章の内容

7

概要	
仮想メディアを使用するための前提条件	
仮想メディアの使用	
KVM セッションを開く	
仮想メディアへの接続	
仮想メディアの切断	110
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)	111



概要

概要

KVM の機能を拡張する仮想メディアを使うことで、クライアント PC やネットワーク ファイル サーバ上のメディアに、リモートの KVM ターゲット サーバからアクセスできる ようになります。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パッチ (patch) の適用
- オペレーティング システムの完全インストール (コンピュータの BIOS でメディア がサポートされる場合)

この拡張 KVM コントロール機能を利用することで、データ センタに出向く必要が なくなり、時間と費用が節約できます。





- 5 CD/DVD ドライブ
- 6 ハード ディスク イメージ ファイル



仮想メディアを使用するための前提条件

- 7 フロッピー ディスク
- 8 USB メモリスティック
- 9 リモート ファイル サーバ (ISO イメージ)
- 10 仮想接続

仮想メディアを使用するための前提条件

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

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス (VM アクセス ポート権限)を許可するように KX II-101 を設定する必要があります。ポート権限はグループレベルで設定されます。詳細は、ユーザ ガイドの「ポート権限の設定」を参照してください。
- KX II-101 デバイスとターゲット サーバ間に USB 接続が存在する必要があり ます。
- (オプション) PC 共有を使用する場合は、[Security Settings (セキュリティ設定)] ページで VM Share Mode (VM 共有モード) も有効にする必要があります。
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。 USB プロファイルの選択についての詳細は、ユーザ ガイドの「USB プロファイルの設定」を参照してください。

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 を使用している場合は、[ユーザ アカウント制御] をオ フにする必要があります。 [コントロール パネル]、[ユーザ アカウント] の順に選 択し、[ユーザ アカウント制御] をオフにします。

Vista アカウントの許可を変更したくない場合は、Internet Explorer を管理 者として実行します。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。

• USB 2.0 の方が高速なため、推奨されます。

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。



仮想メディアの使用

KX II-101 仮想メディア機能を使用する場合、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、VM セッションが有効な間だけアクセスできます。

- ▶ 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。
- 2. 適切な *前提条件* 『p. 104の" 仮想メディアを使用するための前提条件"参照 先』が満たされていることを確認します。
- (ファイル サーバ ISO イメージの場合のみ) ファイル サーバ ISO イメージにア クセスする場合は、KX II-101 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 『p. 111の"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)"参照先 』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。

注: Raritan は ISO9660 形式を標準でサポートしています。 ただし、それ 以外の CD-ROM 拡張も動作する場合があります。

- 4. 適切なターゲット サーバとの KVM セッションを開きます。
- 5. 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	[Connect Drive] (<i>ドライブの接続</i>)『 p. 107の"ローカル ドライブ"参照先 』
ローカル CD/DVD ドライブ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)『p. 109の"CD-ROM/DVD-ROM/ISO イメ ージ"参照先 』
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**『p.110の"仮想メディアの切断"参照先 』 します。



KVM セッションを開く

- ▶ KVM セッションを開くには、以下の手順に従います。
- 1. KX II-101 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。

Home > Port Access			Logou
Port Access			
Click on the i	individual port name to see allowable operatio	ns.	
0 of 1 Remote	e KVM channels currently in use.		
▲ No.	Name	Availability	
1	Dominion_KX2_101_Port5	idle	
	ىرى ئەرىلىدە ئەتىمەتلەردى ئەرەپىمىرىدىنى بىرىكى ئىرىكىيىتى ئەرەبىيەت بەرەبىيەت بىرىكىيىتىن ،		

- 2. [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。
 - a. ターゲット サーバの名前をクリックします。
 - b. ポップアップ メニューから [Connect] (接続) 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。



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 ドライブと外部ディスク 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、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選択肢で す。

注: 特定のバージョンの Windows オペレーティング システムが動作している KVM ターゲット サーバでは、NTFS 形式のパーティション (ローカル C ドライブな ど) がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合が あります。 その場合には、KX II-101 リモート コンソールを閉じて再接続した後で、 別の仮想メディア デバイスをリダイレクトしてください。 同じターゲット サーバに別の ユーザが接続している場合、そのユーザの接続も閉じる必要があります。

- ▶ 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。
- 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。

Map Virtual Media Drive	e: DominionKXII_Port_1 🛛 🔀
Select a local drive for m	ounting onto the target server.
Local Drive : C: (Hard Disk)	
Read-Write	
	Connect Cancel

- [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。
- 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* 『p. 108』」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。

注: ターゲット サーバへの USB 接続がない場合、次のような警告メッセージ が表示されます。「The virtual media capability is set up but will not be available until the USB cable is connected or the target is powered on. Please check your USB connectivity or see if the target is powered on. (仮想メディア機能が設定されましたが、USB ケーブルを接続す るか、ターゲット サーバの電源をオンにするまで利用できません。USB 接続を 確認するか、ターゲット サーバの電源がオンになっているかどうかを確認してくだ さい)」。 この問題を解決してからドライブに再接続してください。

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、それ以外 の CD-ROM 拡張も動作する場合があります。

- 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。
- 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。

ap Virtual Media CD/ISO Ima	ge: LPmachine		
elect a CD.DVD drive or an ISO	image to mou	nt onto the target server.	
Local CD/DVD Drive:			
D: (CD-ROM)	-		
C 120 Image:			
Image Path:			
innaye raui.			1
1		Brows	8
Remote Server ISO Image			
Hostname:		Image:	
[¥.		*
File Server Usemame:		File Server Password:	
			_
		Comment	0
		Connect	Cancel

- 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。 [KX II-101 ファイル サーバ セットアップ] (KX II-101 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。
 - 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。

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: 切断オプション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。



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。

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。

[KX II-101 File Server Setup] (KX II-101 ファイル サーバ セットアップ) ページで、 KX II-101 仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指 定します。ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image 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 ([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 『p. 109の"CD-ROM/DVD-ROM/ISO イメージ"参照先』)の選択肢として表 示されます。

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.	KX II-101 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。	

> File Serve	r Setup		
le Servei	r Setup		
Selected	Host Name/PAddress	Image Path	
V	192.168.1.193	Amages/disk1 iso	1
		[
П		[
		[
		[
		[
		[
П		[

2. 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 アドレスです。
- [Image Path] (イメージのパス)。 ISO イメージの場所を表す完全パス名です。
- 3. 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。
- [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。



デバイス管理

この章の内容

8

[Device Settings] (デバイス設定) メニュー	113
[Network Settings] (ネットワーク設定)	114
[Device Services] (デバイス サービス)	119
キーボード/マウスの設定	121
[Serial Port Settings] (シリアル ポート設定)	122
[Date/Time Settings] (日付/時刻の設定)	123
イベント管理	124
[Port Configuration] (ポート設定)	132

[Device Settings] (デバイス設定) メニュー

[Device Settings] (デバイス設定) メニューは次のように構成されています。 [Network] (ネットワーク)、[Device Settings] (デバイス設定)、 [Keyboard/Mouse] (キーボード/マウス)、[Serial Port] (シリアル ポート)、 [Date/Time] (日付/時刻)、[Event Management - Settings] (イベント管理 -設定)、[Event Management - Destinations] (イベント管理 - 送信先)、[Port Configuration] (ポート設定)。

メニュー	操作
[Network] (ネットワーク)	KX II-101 のネットワーク設定をカスタマイズします。
[Device Services] (デバ	KX II-101 ネットワーク ポートを設定し、TELNET および
イス サービス)	SSH アクセスを有効にします。
[Keyboard/Mouse] (キ	KX II-101 で送信されるキーボードおよびマウス信号をターゲッ
ーボード/マウス)	ト サーバが認識する方法を設定します。
[Serial Port] (シリアル ポ	KX II-101 のシリアル ポートの機能を選択および設定しま
ート)	す。
[Date/Time] (日付/時	日付、時刻、タイム ゾーン、ネットワーク タイム プロトコル
刻)	(NTP) を設定します。
[Event Management - Settings] (イベント管理 - 設定)	SNMP および Syslog を設定します。
[Event Management - Destinations] (イベント 管理 - 送信先)	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。



[Network Settings] (ネットワーク設定)

-בבא	操作
[Port Configuration] (ポート設定)	KVM ポート、コンセントを設定します。

[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 ユニットの 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。

基本的に、IP 設定を行うには 2 種類の方法があります。

- [None] (設定しない)。(デフォルト) 推奨されるオプションです (静的 IP)。 KX II-101 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 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。
- [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。

Network Basic Settings	LAN Interface Settings
evice Name * XK22-101 2 auto configuration DHCP V	Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100/Mbps/Full.
referred host name (DHCP only)	Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok
2 address 192.168.50.74	LAN Interface Speed & Duplex Autodetect
ubnet mask	Bandwidth Limit
255.255.255.0	No Limit 💉
iateway IP address 192.168.50.126	Set System ACL
rimary DNS server IP address	
.92.168.50.114	
econdary DNS server IP address	

- 2. ネットワーク基本設定を更新します。各フィールドの詳細については、「ネットワ ーク基本設定」を参照してください。
- LAN インタフェースの設定を更新します。各フィールドの詳細については、 「LAN インタフェース設定」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。
- > 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。
- ▶ 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

Device Name *		
DKX2-101	7	
IP auto configuratio DHCP 💙	n	
Preferred host nam	ie (DHCP only)	
IP address		
192.168.59.99		
Subnet mask		
255.255.255.0		
Gateway IP address	\$	
192.168.59.126		
Primary DNS server	IP address	
192.168.59.2		
Secondary DNS ser	ver IP address	
192.168.51.10		



- [Device Name] (デバイス名)。デバイスの一意の名前を入力します (最大で 16 文字です。スペースは使用できません)。デバイスには、簡単に識別できる 名前を付けてください。KX II-101 ユニットのデフォルトの名前は「DKX2-101」 です。 リモート ユーザにもこの名前が表示されます。ただし、MPC ユーザがこ のデバイスの [Connection Profile] (接続プロファイル)を作成した場合、その ユーザにはそのプロファイルの [Description] (説明) フィールドが代わりに表示 されます。
- [IP auto configuration] (IP 自動設定)。ドロップダウン リストの使用可能 なオプションから選択します。
 - [None] (設定しない)。 自動 IP 設定を使用せず、IP アドレスを自分で 設定する場合は、このオプションを選択します (静的 IP)。 推奨されるデ フォルトのオプションです。

[IP auto configuration] (IP 自動設定) でこのオプションを選択すると、次の [Network Basic Settings] (ネットワーク基本設定) フィールドが有効になり、 IP アドレスを手動で設定できるようになります。

- [IP Address] (IP アドレス)。デフォルトの IP アドレスは 「192.168.0.192」です。
- [Subnet Mask] (サブネット マスク)。 デフォルトのサブネット マスクは 「255.255.255.0」です。
- [Gateway IP Address] (ゲートウェイ IP アドレス)。ゲートウェイの IP アドレスです (使用している場合)。
- [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)。 名前を IP アドレスに変換するために使用されるプライマリ ドメイン ネーム サーバです。
- [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)。名前を IP アドレスに変換するために使用されるセカンダリ ドメイン ネーム サーバです (使用している場合)。
- [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。

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。



LAN インタフェース設定

Note: For reliable network communication, configure the Dominion KX2-101 and LAN Switch to the same LAN Interface Speed and Duplex. For example, configure both the Dominion KX2-101 and LAN Switch to Autodetect (recommended) or set both to a fixed speed/duplex such as 100Mbps/Full. Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok LAN Interface Speed & Duplex	LAN Interface Settings	
Current LAN interface parameters: autonegotiation on, 100 Mbps, full duplex, link ok LAN Interface Speed & Duplex	Note: For reliable network communica Dominion KX2-101 and LAN Switch to Interface Speed and Duplex. For exam Dominion KX2-101 and LAN Switch to (recommended) or set both to a fixed s 100Mbps/Full.	ation, configure the the same LAN ple, configure both the Autodetect speed/duplex such as
LAN Interface Speed & Duplex	Current LAN interface parameters: autonegotiation on 100 Mbps, full duplex, link	cok
	LAN Interface Speed & Duplex	
	Bandwidth Limit	
Bandwidth Limit	No Limit 💙	
Bandwidth Limit No Limit		

- 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)。
 設定可能な速度と二重化の組み合わせを選択します。

自動検出	デフォルト オプショ ン	
10 Mbps/半二重		両方の LED が 点滅
10 Mbps/全二重		両方の LED が 点滅
100 Mbps/半二重		黄色の LED が 点滅
100 Mbps/全二重		黄色の LED が 点滅
1000 Mbps/全二重	ギガビット	緑色の LED 点 滅

[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。

詳細は、「ネットワーク速度の設定」を参照してください。

- [Bandwidth Limit] (帯域幅の制限)。 使用可能な帯域幅の制限から選択します。
 - [128 Kilobit] (128 キロビット)
 - [256 Kilobit] (256 キロビット)
 - [512 Kilobit] (512 キロビット)
 - [2 Megabit] (2 メガビット)
 - [5 Megabit] (5 メガビット)
 - [10 Megabit] (10 メガビット)
 - [100 Megabit] (100 メガビット)
 - [No Limit] (制限なし)
- [Set System ACL] (システム ACL の設定)。このボタンをクリックして、KX II-101 に対するグローバル レベルのアクセス制御リストの設定を行い、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がない ようにします。[IP Access Control] (IP アクセス制御)『p. 153』ページが 開きます。

注: これらの ACL 値はグローバルで、KX II-101 ユニット全体に影響します。 グ ループレベルの ACL も作成できます。 たとえば、所定の範囲の IP アドレスからの み KX II-101 にアクセスできる「Outsourced Vendors」というユーザ グループを作成 できます (グループに固有のアクセス制御リストを作成する方法については、「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)。



[Device Services] (デバイス サービス)

[Device Services] (デバイス サービス) ページを使用して、KX II-101 の接続オプ ションを指定します。

Home > Device Settings > Device Services
f
Services
Discovery Port *
Enable TELNET Access
23
Enable SSH Access
SSH Port 22
Enable Direct Port Access via URL
OK Reset To Defaults Cancel

- ▶ 検出ポートを設定するには、以下の手順に従います。
- [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。
- 2. KX II-101 でクライアント PC との通信に使用するネットワーク ポートを入力 します。
- 3. [Save] (保存) をクリックしてこの設定を保存します。
- > TELNET アクセスを有効するには、以下の手順に従います。
- [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。
- 2. [Enable TELNET Access] (TELNET アクセスを有効する)を選択します。
- 3. KX II-101 への TELNET アクセスに使用するネットワーク ポートを入力しま す。
- 4. [Save] (保存) をクリックしてこの設定を保存します。



- > SSH アクセスを有効するには、以下の手順に従います。
- [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。
- 2. [Enable SSH Access] (SSH アクセスを有効する)を選択します。
- 3. KX II-101 への SSH アクセスに使用するネットワーク ポートを入力します。
- 4. [Save] (保存) をクリックしてこの設定を保存します。

ダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスを使用すると、通常のログイン ページに進まないで KX II-101 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。
- [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。
- [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。
- 3. [Save] (保存) をクリックしてこの設定を保存します。
- ▷ 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、必要に応じて KX II-101 のポート番号を 使用して URL を定義します。 KVM ポートが 1 つのみある場合、ポート番 号は不要です。

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 アドレス**]/dpa.asp?username=[ユーザ名]&password=[パスワー ド]&port=[ポート番号]

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。



キーボード/マウスの設定

[Keyboard/Mouse Setup] (キーボード/マウス設定) ページを使用して、KX II-101 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。



- [Host Interface] (ホスト インタフェース)。 KX II-101 がキーボードおよびマウス 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を 選択します。
 - [Auto] (自動)。この設定では、KX II-101 は 使用可能な場合に USB 接続を使用し、そうでない場合は代わりに PS/2 を使用します。
 - [USB]。この設定では、KX II-101 は USB 接続を使用して、キーボード およびマウスデータをホスト デバイスに送信します。
 - [PS/2]。この設定では、KX II-101 は PS/2 接続を使用して、キーボード およびマウスデータをホスト デバイスに送信します。
- ▶ 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 の内 蔵シリアルポートの使用方法を設定します。

- ▶ シリアル ポートを設定するには、以下の手順に従います。
- [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。

Seri	al Port Settings
۲	Admin Port
0	Powerstrip Control
0	Modem
Sei	rial Settings:
Sp	eed 115200 💙 Stop Bits 1 💙
Da	ta bits 8 💙 Handshake None 💙
Pa	rity none 🗸
OV	Percet To Defaulte
OK	Reset to belauits Cancel

- 2. シリアル ポートで利用する機能を選択するには、以下の手順に従います。
 - [Admin Port] (管理ポート)。 クライアント PC から KX II-101 に直接 接続して詳細な設定にアクセスするには、このオプションを選択します。
 - [PowerStrip Control] (パワー ストリップ制御)。 シリアル インターフェース で制御されるパワー ストリップに KX II-101 を接続する場合は、このオプ ションを選択します。
 - [Modem] (モデム)。ダイヤルイン アクセスを提供するために外部モデムを KX II-101 に接続する場合は、このオプションを選択します。
- 3. For the [Modem] (モデム) オプションでは、モデムの使用設定を次のように入 カして設定します。
 - a. KX II-101 とモデム間のデータ速度を [Serial line speed] (シリアル ライン速度) ドロップダウン リストから選択します。
 - b. モデム init 文字列を入力します。
 - c. モデム サーバ IP アドレスを入力します。これは、ユーザがモデムを介して 接続した後、KX II-101 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。
 - d. モデム クライアント IP アドレスを入力します。これは、ユーザがモデムを 介して接続した後、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。

[Date/Time Settings] (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 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。

- 日付と時刻を手動で設定する。
- ネットワーク タイム プロトコル (NTP) サーバと同期する。
- 注: KX II-101 は夏時間をサポートしません。
- > 日付と時刻を設定するには、以下の手順に従います。
- [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。

Date/Tim	e Settings			
(GMT +00)	e) England, Ireland,	Portugal		
User Date (May Time 9 Sync Prima	Specified Time Month, Day, Yea 2 (Hour, Minute) 4 hronize with Minute ary Time server	ar) , 2007 TP Server		
Secor	ndary Time serv	ver		
The NTP Se function, p provides c	erver configuratio lease make sure t orrect time server	in is obtained automa that the DHCP serve rinformation.	tically. For proper r used by this device	

- 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. 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。
- [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。
- [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、 以下の手順に従って日付と時刻を入力します。
 - a. ドロップダウン リストから [Month] (月) を選択します。
 - b. その月の [Day] (日)を入力します。
 - c. yyyy の形式で [Year] (年) を入力します。
 - d. hh:mm の形式で [Time] (時刻) を入力します (24 時間制で入力します)。
- 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。

イベント管理

KX II-101 イベント管理機能によって、一連の画面から、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。



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 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 エージ ェントとトラップの詳細については、「SNMP エージェント設定『p. 130』」および 「SNMP トラップ設定『p. 130』」を参照してください。

- SNMP を設定する (SNMP のログ作成を有効にする) には、以下の手順 に従います。
- [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。

ome > Device Settings > E	vent Management - :	Settings
SNMP Configuration		
SNMP Logging E	nabled	
Name		
sai-Dkx2101		
Contact		
SAI		
Location		
FSD		
Agent Community Str	ing	
Туре		
Read-Write 🔽		
Destination IP	Port #	Community
192.168.51.150	162	public
	162	public
Clic	k here to view the D	ominion KX2-101 SNMP MIB
SysLog Configuration	n	
Enable Cycles Ferwarding		
Linuxe system to	a search and	
IP Address		
OK Report T	o Defaulte	Cancel
Keset I		

 [Enable SNMP Logging] (SNMP ログを有効にする) オプションを選択しま す。これによって残りの SNMP フィールドが有効になります。



- [Name] (名前) フィールドには、KX II-101 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 (使用している Dominion ユニット)の 名前を、[Contact] (連絡先) フィールドには、そのユニットに関連する連絡先を、 [Location] (所在地) フィールドには、Dominion ユニットが物理的に設置さ れている場所を入力します。
- [Agent Community String] (エージェント コミュニティの文字列) (Dominion ユニットの文字列) 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。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特 定するために使用されます。これは、SNMP デバイスまたはエージェントが複数 の SNMP コミュニティに所属している場合があるためです。
- 5. [Type] (タイプ) ドロップダウン リストを使用して、コミュニティに読み取り専用と 読み書き可能のいずれかを指定します。
- [Destination IP] (送信先 IP)、[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。
- [Click here to view the KX II-101 SNMP MIB] (KX II-101 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 の設定

Sys	Log Configuration
	Enable Syslog Forwarding
IP A	ddress

- 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。
- [Enable Syslog Forwarding] (Syslog 送信有効) オプションを選択して、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 アドレスを入 力します。
- 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。
- > 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。



[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 跡するイベントと、その情報の送信先を選択します。

注: SNMP トラップは、[SNMP Logging Enabled] (SNMP ログを有効にする) オプションが選択されている場合にのみ生成されます。一方、Syslog イベントは、 [Enable Syslog Forwarding] (Syslog 送信有効) オプションが選択されている場合 にのみ生成されます。これらのオプションは、いずれも [Event Management -Settings] (イベント管理 - 設定) ページで設定します。「[Event Management -Settings] (イベント管理 - 設定)」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。
- [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。



Logow

ort Access Virtual Media User Management Device	Settings	Security	Maintenance	Diagnostics

Home > Device Settings > Event Management - Destinations

Event Management - Destinations

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

Category	Event	SHMP	Syslog	Audit Log
Device Operation		R	A	N
	System Startup	되	4	4
	System Shubdown	R	9	A
	Power Supply Status Changed	प	5	v
	Powerstrip Outlet Status Changed	R	N	R
	Network Parameter Changed	되	되.	되
	Port Status Changed	2	N	9
	Network Failure			ঘ
	Ethernet Failover	N	9	N
Device Management		되	v	4
	FactoryReset	R	N	R
	Begin CC Control	되	되	되
	End CC Control	ସ	9	A
	Device Update Started	되	A	A
	Device Update Completed	R	N	R
	Device Update Failed	되	4	4
	Firmware Update Failed	R	9	A
	Firmware File Discarded	되	되.	A
	Firmware Validation Failed	R	9	R
	Configuration Backed Up	되	되.	ম
	Configuration Restored	R	9	R
	Port Connection Denied	되	되.	되
Security		R	R	R
	Password Settings Changed	되	v	A
	Login Failed	R	A	R
	Password Changed	되	되	A
	User Blocked		9	R
User Activity		되	되.	A
	Port Connected	R	N	R
	Port Disconnected	A	A	<u>.</u>
the states all		1 1		and the second second

and a second second

システム イベントは、デバイス操作、デバイス管理、セキュリティ、ユーザ アクティ ビティ、ユーザ グループ管理に分類されます。

2. 有効または無効にする [Event] (イベント) ラインのアイテムと、情報の送信先 のチェックボックスをオンにします。

ヒント: [Category] (カテゴリ) ラインのチェックボックスをそれぞれオンまたはオフに すると、カテゴリ全体を有効または無効に設定できます。

3. [OK] 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。
- 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。

警告: UDP 経由の SNMP トラップを使用している場合、KX II-101 を再 起動したときに、KX II-101 と接続先のルータが同調できなくなり、SNMP トラッ プ「reboot completed (再起動の完了)」がログ記録されない可能性がありま 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 (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 のトラップを次の 表に示します。

トラップ名	説明
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定は復元されました。
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 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 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 システムに追加されました。
groupDeleted	グループがシステムから削除されました。



トラップ名	説明
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	パワー ストリップ デバイスのコンセントの状態の通知です。
rebootCompleted	KX II-101 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 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。
userLogin	ユーザが KX II-101 へ正常にログインし、認証されまし た。
userLogout	ユーザが KX II-101 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。



[Port Configuration] (ポート設定)

トラップ名	説明
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。
vmImageConnected	ユーザが仮想メディアを使用してターゲットにデバイスまたは イメージのマウントを試みました。 デバイスまたはイメージの マッピング (マウント) が試行されるたびに、このイベントが生 成されます。
vmImageDisconnected	ユーザが仮想メディアを使用してターゲットからデバイスまた はイメージのマウント解除を試みました。

[Port Configuration] (ポート設定)

[Port Configuration] (ポート設定) ページには、KX II-101 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。
- [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。

Home > Device Settings > Port Configuration Logou				
Port Configuration				
▲ No.	Name	Туре		
1	Dominion_KX2_101_Port1	KVM		
2	Power Port 1	PowerStrip		

最初このページはポートの番号順に表示されますが、列の見出しをクリックしてフィールドごとに並べ替えられます。

- [Port Number] (ポート番号)。1 から KX II-101 ユニットで使用できる ポートの合計数までの番号が振られています。
- [Port Name] (ポート名)。ポートに割り当てられている名前です。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	パワー ストリップ	
KVM	KVM ターゲット	

- 2. 編集するポートの [Port Name] (ポート名) をクリックします。
 - KVM ポートの場合は、[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。
 - パワー ストリップの場合は、パワー ストリップの [Port] (ポート) ページが 開きます。このページで、パワー ストリップとそのコンセントに名前を付けま す。

注: [Power Port 1] (パワー ポート 1) リンクは、Raritan 電源タップを KX II-101 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。



この章の内容

概要	134
パワー ストリップの接続	135
パワー ストリップの名前の指定 (パワー ストリップの [Port] (ポート) ^	ページ)136
コンセントへの KVM ターゲット サーバの関連付け ([Port] (ポート)	ページ)137
コンセントの関連付けの表示	141
電源タップ デバイスの制御	142

概要

9

KX II-101 では、ターゲット サーバの電源をリモートで制御できます。 この機能を 使用するには、Raritan リモート パワー ストリップが必要です。

- > KX II-101 の電源制御機能を使用するには、以下の手順に従います。
- 1. ターゲット サーバにパワー ストリップを接続します。
- 2. パワー ストリップに名前を付けます。
- 3. パワー ストリップのコンセントをターゲット サーバに関連付けます。
- 4. [Powerstrip Device] (パワーストリップ デバイス) 『p. 142の"電源タップ デバイスの制御"参照先 』ページで、パワー ストリップのコンセントをオン、オフします。



パワー ストリップの接続



- 1 KX II-101 から Raritan パワー ストリップまでの DKX2-101-SPDUC コネクタ (別売り)
- 2 Raritan パワー ストリップ。
- KX II-101 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。
- DKX2-101-SPDUC ケーブルのミニ DIN9M コネクタを KX II-101 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。



パワー ストリップの名前の指定 (パワー ストリップの [Port] (ポート) ページ)

[Port Configuration] (ポート設定) ページで、Raritan リモート パワー ストリップ 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。 [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 [Number] (番号)、[Name] (名前)、[Port Association] (ポートの関連付 け)。

このページを使用してパワー ストリップとそのコンセントに名前を付けます。いずれの 名前にも最大 32 文字の英数字を使用でき、特殊文字を含めることができます。

Home > Device Settings > Port Configuration > Port				
	1			
Port 1				
Туре:				
Nome:	1			
Name:				
Dominion_RX2_T01_Port1	- 1			
	1			
Power Association				
Power Strip Name	Outlet Name			
None				
	•			
	🞽			
	1			
Target Copyor Cottinge				
Target server settings				
Use Full Speed - Useful for B	ios			
that cannot handle High Spee	ed 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)				
(
	5			
OK Cancel	3			
and the second	a dealer a second s			


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。
- 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。

コンセントへの KVM ターゲット サーバの関連付け ([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、ポートの名前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、パワー ストリップと関連付けることができる、最大で 4 つの電源プラグを 接続できます。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。

tome > Port Access				Logout
Port Access				
Click on the indivi	Connect	to see allowable operations.		4
0 of 1 Remote KVM	Power On	rently in use.		
A lla.	Power Off		Availability	
t	Power Cycli	01 Port1	dle	

en and have a set of the second device a second device a set of the second device a set of the second device a second device a set of the second device a second device a set of the second device a second device a set of the second device a set of the second device a set of the second device a set of the



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。詳細は、パワー ストリップの接続『p. 135』」を参 照してください。

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。



ome > Device Settings > I	Port Configuration > Port
Port 1	
Туре:	
KVM	
Name:	
Dominion_KX2_101_Po	rt1
Power Association	
Devee Ctain Name	Outlint Name
Power Strip Name	Dominion KX2 101 Port1(7)
	Dominion KX2 101 Port1(8) V
	None V
	None 👻
Target Server Setti	ngs
- Use Full Speed -	Useful for BIOS
that cannot hand	le High Speed USB devices
Absolute mouse	scaling for MAC server
- (applies only if u	ad support
(applies only if U	SB is active Keyboard/Mouse Interface)
OK Cancel	

2 つのコンセントが関連付けられたパワー ストリップを以下に示します。

- ▶ ポート名を変更するには、以下の手順に従います。
- 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。
- 2. [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。
- > 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。



コンセントの関連付けの表示

- > 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。

Port 2		
Туре:		
Powerstr Name:	ip	
Power Po	ort 1]
1		-
Outlets		
Number	Name	Port Association
a ann ann ann ann ann ann ann ann ann a	Outlet 1	PortAssociation
1		
2	Outlet 2	
3	Outlet 3	
4	Outlet 4	
5	Outlet 5	
6	Outlet 6	
7	Dominion_KX2_101_Port1	Dominion_KX2_101_Port1
8	Dominion_KX2_101_Port1	Dominion_KX2_101_Port1

[Outlets] (コンセント) の下に、パワー ストリ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。
- [Port 2] (ポート 2)の [Name] (名前) フィールドを編集して、パワーポート名を変更します。
- [Outlets] (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 [Powerstrip Device] (パワーストリップ デバイス) ページに表示されます。詳細は、「パワーストリップ デバイスの制御 『p. 142の"電源タップ デバイスの制御"参照先 』」を参照してください。
- 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。 詳細は、 コンセントへの KVM ターゲット サーバの関連付け ([Port] (ポート) ページ 『p. 137』を参照してください。

電源タップ デバイスの制御

[Powerstrip Device] (パワーストリップ デバイス) ページを使用して電源タップ デ バイスを制御できます。このページで、電源タップの各コンセントをオン、オフできま す。

Home > Powerstrip				
Powerstrip Devi	ce			
Powerstrip: Powerstrip: Powerstrip: Power Name: Moo Power Port 1 PCR	er Port 1 - PCR8 💌 lel: Temperature: Curr 18 41 °C 0.67	Update entAmps: MaxAmps: A 1.2 A	Voltage: PowerlnWat 107 V 60 W	t: PowerlnVA: 60 VA
Outlet 1	Outlet 3	Outlet 5	Outlet 7	
0n Off	On Off	5 On Off	7 On Off	
Outlet 2	Outlet 4	Outlet 6 off 6	Outlet 8	
On Off	On Off	On Off	On Off	



- KX II-101 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。
- [Home] (ホーム)の [Powerstrip] (パワーストリップ)を選択します。
 [Powerstrip Device] (パワーストリップ 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。
- 確認のプロンプトが表示されたら、[OK] をクリックします。
 電源コンセントがオンまたはオフに切り替わります。
- 注: KX II-101 で制御できるのは、1 つの電源タップのみです。[Powerstrip] (パ ワーストリップ) 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。



10 [Security Settings] (セキュリティ設定)

この章の内容

[Security Settings] (セキュリティ設定) メニュー	144
[Security Settings] (セキュリティ設定)	145
[IP Access Control] (IP アクセス制御)	

[Security Settings] (セキュリティ設定) メニュー

[Security] (セキュリティ) メニューは次のように構成されています。 [Security Settings] (セキュリティ設定) および [IP Access Control] (IP アクセス制御)。

-בבא	操作
[Security Settings] (セキュリティ設定)	ログイン制限、強力なパスワード、ユーザ ブロック、暗号 化および共有に関するセキュリティを設定します。
[IP Access Control] (IP アクセ ス制御)	KX II-101 ユニットへのアクセスを制御します。 グローバ ル アクセス制御リストの設定を行い、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。



[Security Settings] (セキュリティ設定)

[Security Settings] (セキュリティ設定) ページで、ログイン制限、ユーザ ブロック、 パスワード ルール、暗号化および共有に関するセキュリティを指定できます。

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 Web サーバ証明書は自己署名され、 Java アプレット証明書は VeriSign 証明書によって署名されます。 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。
- [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。

Home > Security > Security Settings	
Login limitations	User Blocking
Enable Single Login Limitation	Disabled
Enable Password Aging	O Timer Lockout
Password Aging Interval (days)	Attempts 3
Log Out Idle Users	Lockout Time
After (minutes)	Deactivate User-ID
	Failed Attempts
Strong passwords	Encryption & Share
Enable strong passwords	Encryption Mode
Minimum length of strong password	Auto
Maximum length of strong password	PC Share Mode PC-Share
Figure A least one lower case character	☐ VM Share Mode
Find the set of the se	Disable Local Port Output
Find the second	Local Device Reset Mode
Enforce at least one printable special character	
Number of restricted passwords based on history	
OK Reset To Defaults Cancel	ستان و المحمد الم

フィールドの構成は次のグループに分けられます。 ログイン制限、強力なパスワ ード、ユーザ ブロック、暗号化および共有。

2. 必要に応じて、[Login Limitations] (ログイン制限) 『p. 146の"[Logon Limitations] (ログオン制限)"参照先 』の設定を更新します。



- 3. 必要に応じて、[Strong Passwords] (**強力なパスワート**) 『p. 147』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) 『p. 149』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] をクリックします。
- > 変更を保存せずにページを閉じるには、以下の手順に従います。
- [Cancel] (キャンセル) をクリックします。
- ▶ 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。

[Logon Limitations] (ログオン制限)

ログオン制限を使用して、シングル ログオン、パスワード エージング、アイドル ユーザ のログオフに関する制限を指定できます。

制限	
[Enable Single Login Limitation] (シングル ログオン制限 を有効にする)	これを選択すると、ユーザ名ごとに同時には 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) 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。
	[Password Aging Interval (days)] (パスワード エー ジング間隔 (日))。 [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。



[Security Settings] (セキュリティ設定)

制限	説明
[Log out idle users] (アイドル ユーザのログ アウト)	このチェック ボックスをオンにすると、非アクティブの状態で 一定の時間が経過した場合、ユーザ セッションを自動 的に切断します。 [After] (経過時間) フィールドに時 間を入力します。 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 がログオフされます。 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 (minutes)] (経過時間 (分))。アイドル ユーザ がログオフされるまでの時間です (分)。 [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。

[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 ローカル パスワードの形式を定義 する判別の基準を設定できます。





- [Enable strong passwords] (強力なパスワードを有効にする)。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規則が適用されます。パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログ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、標準の形式での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。
 - [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 文字まで拡張できます。
 - [Maximum length of strong password] (強力なパスワードの最大長)
 。 デフォルトでは 16 文字ですが、最大 64 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 case character] (1 文字以上の大文字の 使用を強制する)。これを選択すると、パスワードに 1 文字以上の大文 字が必要になります。
 - [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] (履歴を参照する制限パスワードの数)。このフィールドは、パスワード履歴の幅を表します。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1~12~12 で、デフォルトは5~です。



[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。

- [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関わらず、ユーザのアクセスはブロックされません。
- [Timer Lockout] (タイマー ロックアウト)。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。
 - [Attempts] (試行回数)。 失敗できるログインした回数を示し、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、デフォルトでは5分です。
- [Deactivate User-ID] (ユーザ ID の無効化)。このオプションを選択した場合は、[Failed Attempts] (失敗した回数) 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。
 - [Failed Attempts] (失敗できる試行回数)。失敗できるログインの試行 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。 [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。

Us	User Blocking		
c	Disabled		
c	Timer Lockout		
	Attempts 3		
	Lockout Time 5		
•	Deactivate User-ID	ļ	
	Failed Attempts	1.000	

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 『p. 47の"[Add New User] (新規ユ ーザの追加)"参照先 』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。



[Encryption and Share] (暗号化および共有)

[Encryption & Share] (暗号化および共有) の設定を使用して、使用する暗号 化のタイプ、PC と VM の共有モード、KX II-101 のリセット ボタンが押下された 場合に実行されるリセットのタイプを指定できます。

Encryption & Share				
Encryption Mode				
Apply Encryption Mode to KVM and Virtual Media				
PC Share Mode PC-Share 💙				
VM Share Mode				
Disable Local Port Output				
Local Device Reset Mode				
Enable Local Factory Reset 🔽				
آبا يعرى مسترى محمد من يستر بالمستحد المن المتحدة في يتريدون متحم المحمد المراج عالما من الما				

 [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た場合、使用しているブラウザが 選択したモードをサポートしていないと、KX II-101 に接続できないという警告が 表示されます。

Encryption & Share
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 Dominion KX2-101.
Encryption Mode
RC4 💙
Apply Encryption Mode to KVM and Virtual Media
PC Share Mode
Private 💙
VM Share Mode
Disable Local Port Output
Local Device Reset Mode
Enable Local Factory Reset 🛛 🗸
and an and the second

 [Auto] (自動)。 推奨されるオプションです。 KX II-101 はオート ネゴシエ ーションを行い、最も高い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 ユニットとリモート PC 間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] 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、「使用しているブラウザの AES 暗号化の確認『p. 152』」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] 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、「使用しているブラウザの AES 暗号化の確認『p. 152』」を参照してください。
- [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)。このオプションを選択すると、選択され 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 データにも 128 ビットの暗号化が適用され、転送 されます。
- [PC Share Mode] (PC 共有モード)。 グローバルな同時リモート KVM アク セスを特定し、最大 8 人までのリモート ユーザが KX II-101 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。 ドロップダウン リストをクリックして、次のオプションのいずれかを選択しま す。
 - [Private] (プライベート)。 PC を共有しません。デフォルトのモードです。
 一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。
 - [PC-Share] (PC 共有)。 KVM ターゲット サーバに最大 8 人のユーザ (管理者または非管理者) が同時にアクセスできます。 ただし、リモート ユ ーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウ スの操作を止めないユーザがいると、正しく操作できない場合があることに 注意してください。



- [VM Share Mode] (VM 共有モード)。このオプションは [PC-Share Mode] (PC 共有モード) が有効な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。デフォルトでは無効に 設定されています。
- [Local Device Reset Mode] (ローカル デバイス リセット モード)。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され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」を参照してください。次のオプションのいずれかを選択します。
 - [Enable Local Factory Reset] (ローカルでのファクトリ リセットを有効にする)(デフォルト)。 KX II-101 ユニットを工場出荷時のデフォルトに戻します。
 - [Enable Local Admin Password Reset] (ローカルでの管理者パスワードのリセットを有効にする)。ローカルの管理者パスワードのみをリセットします。パスワードは「raritan」に戻ります。
 - [Disable All Local Resets] (ローカルでのすべてのリセットを無効にする)。 リセットは一切実行されません。

使用しているブラウザの AES 暗号化の確認

使用しているブラウザで AES がサポートされているかどうかが不明な場合は、ブラウ ザ メーカーに問い合わせるか、暗号化方式を確認するブラウザを使用して次の Web サイトにアクセスしてください。 https://www.fortify.net/sslcheck.html。 この Web サイトでは、使用しているブラウザの暗号化方式を検出し、レポートを表 示できます。

注: IE6 は AES 128 または 256 ビット暗号化をサポートしません。

AES 256 の前提条件とサポートされる設定

AES 256 ビット暗号化は、次の Web ブラウザでのみサポートされます。

- Firefox 2.0.0.7
- Mozilla 1.7.13
- Internet Explorer 7

ブラウザによるサポートに加え、AES 256 ビット暗号化では、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、次のリンクの [その他のダウンロード] セクションで入手 できます。

- JRE1.4.2 http://java.sun.com/j2se/1.4.2/download.html
- JRE1.5 http://java.sun.com/javase/downloads/index_jdk5.jsp



[IP Access Control] (IP アクセス制御)

IP アクセス制御を使用して、KX II-101 ユニット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。 IP アクセス制 御はグローバルに作用し、KX II-101 ユニット全体に影響しますが、グループレベル でユニットへのアクセスを制御することもできます。 グループレベルの制御の詳細につ いては、「グループ ベースの IP ACL (アクセス制御リスト)」を参照してください。

重要: KX II-101 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 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。
- 次のいずれかの方法を使用して、[IP Access Control] (IP アクセス制御) ペ ージを開きます。
 - [Security] (セキュリティ)の [IP Access Control] (IP アクセス制御) を 選択します。または、
 - [Network Settings] (ネットワーク設定) ページで [Set System ACL] (システム ACL の設定) ボタンをクリックします。

[IP Access Control] (IP アクセス制御) ページが開きます。

TL ACCESS	Virtual Media	User Management	Device Settings	Security	Mainten
ome > Securit	y > IP Access Cor	ntrol			
IP Access	Control			Ê	1
Enable	e IP Access Co	ntrol			
Default poli	cy 1				
Rule #	IP/Mask		Policy		1
			ACCEPT		
Append	Insert	Replace	Delete		4
Annhi	Reset	To Defaults	Cancel		4

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。



[IP Access Control] (IP アクセス制御)

- 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 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 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。
- 2. ドロップダウン リストからポリシーを選択します。
- [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。
- 4. 入力する各ルールについて、手順 1 ~ 3 を繰り返します。
- ▶ ルールを挿入するには、以下の手順に従います。
- [Rule] (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。
- [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。
- ルールを置き換えるには、以下の手順に従います。
- 1. 置き換える [Rule] (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 [Rule] (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。



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。



メンテナンス

この章の内容

[Maintenance] (メンテナンス) メニュー	156
[Audit Log] (監査ログ)	157
[Device Information] (デバイス情報)	159
[Backup and Restore] (バックアップと復元)	160
[Firmware Upgrade] (ファームウェアのアップグレード)	162
- アップグレード履歴	164
[Reboot] (再起動)	164

[Maintenance] (メンテナンス) メニュー

11

[Maintenance] (メンテナンス) メニューには次のオプションが含まれます。 [Audit Log] (監査ログ)、[Device Information] (デバイス情報)、[Backup/Restore] (バ ックアップと復元)、[Firmware Upgrade] (ファームウェアのアップグレード)、[Factory Reset] (ファクトリ リセット)、[Upgrade History] (アップグレード履歴)、[Reboot] (再起動)。



[Audit Log] (監査ログ)

KX II-101 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 ユニットの監査ログを表示するには、以下の手順に従います。
- [Maintenance] (メンテナンス)の [Audit Log] (監査ログ)を選択します。
 [Audit Log] (監査ログ) ページが開きます。

udit Log			
Dider]			
Date	Event	Description	
11/13/2007 12:51:53	Access Logout	User 'admin' from host '192.168.61.209' logged out.	
11/13/2007 12:28:01	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'available'.	
11/13/2007 12:28:01	Port Disconnected	Port 'Dominion_KX2_101_Port5' disconnected by user 'admin'.	
11/13/2007 12:27:56	Port Status Changed	Status of port 'Dominion_KX2_101_Port5' changed to 'connected'.	
11/13/2007 12:27:56	Port Connected	Port 'Dominion_KX2_101_Port5' connected by user 'admin'.	
11/13/2007 11:39:00	Access Login	User 'admin' from host '192.168.61.209' logged in.	
11/13/2007 10:55:30	Access Login	User 'admin' from host '192.168.50.54' logged in.	
11/13/2007 10:55:15	Login Failed	Authentication failed for user 'admin' from host '192.168.50.54'.	
11/12/2007 17:53:55	Access Logout	User 'admin' from host '192.168.32.40' logged out.	
11/12/2007 17:53:28	Access Login	User 'admin' from host '192.168.32.40' logged in.	
11/12/2007 17:53:13	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.	
11/12/2007 17:53:13	End CC Control	CC management stopped by user 'CC admin' from host '192.168.59.246'.	
11/12/2007 17:50:19	Access Logout	User 'CC user session' from host '192.168.59.246' logged out.	
11/12/2007 17:48:21	Access Login	User 'CC user session' from host '192.168.59.246' logged in.	
11/12/2007 17:48:16	Access Logout	User 'CC admin' from host '192.168.59.246' logged out.	
11/12/2007 17:48:15	Access Login	User 'CC admin' from host '192.168.59.246' logged in.	
11/12/2007 17:48:14	Access Login	User 'CC admin' from host '192.168.59.246' logged in.	
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.	
11/12/2007 17:48:08	Begin CC Control	CC management started by user 'admin' from host '192.168.59.246'.	
11/12/2007 17:48:08	Access Logout	User 'admin' from host '192.168.59.246' logged out.	



[Audit Log] (監査ログ) ページには、日付と時刻順にイベントが表示されます (最 も新しいイベントが 1 番上に表示されます)。 監査ログには次の情報が含まれます。

- [Date] (日付)。イベントの発生した日付と時刻です。24 時間制で表示されます。
- [Event] (イベント)。 [Event Management] (イベント管理) ページに表示されるイベント名です。
- [Description] (説明)。イベントの詳細な説明です。
- ▶ 監査ログを保存するには、以下の手順に従います。

注: 監査ログの保存は KX II-101 リモート コンソールでのみ実行できます。ローカ ル コンソールでは実行できません。

- 1. [Save to File] (ファイルに保存) ボタンをクリックします。 [Save File] (ファイルの 保存) ダイアログ ボックスが開きます。
- 2. 対象のファイル名と保存先を選択し、[Save] (保存) をクリックします。 監査ロ グは、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。
- ▶ 監査ログのページを移動するには、以下の手順に従います。
- [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 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 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。

Device Information	
Model:	DKX2-101
Hardware Revision:	0x15
Firmware Version:	2.0.0.5.6201
Serial Number:	AAK7800006
MAC Address:	00:0d:5d:03:5d:1f

使用している KX II-101 に関する以下の情報が提供されます。 [Model] (モデル)、[Hardware Revision] (ハードウェア リビジョン)、[Firmware Version] (ファームウェア バージョン)、[Serial Number] (シリアル番号)、[MAC Address] (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、業務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 のユーザ設定をバックアップして、それを新しい KX II-101 に復元することで、別の KX II-101 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 でセットアップを行い、その設定を複数の KX II-101 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。

ort Access	Virtual Media	User Management	Device Settings	Security	Mair
14447	A TOTO N	Western Market		\sim	\sim
ome > Mainb	enance > Backup	/ Restore			
Backup /	Restore				
G Full F	Restore				
C Prote	ected Restore				
e curt	om Dectore				
C cust	om Kestore	200			
	User and Group	Restore			
E 1	Device Settings	Restore			
Restore Fi	le				
		Browse			
75					
Restor	e Backu	p Cancel			

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。

- > KX II-101 をバックアップするには、以下の手順に従います。
- 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。



- 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。
- KX II-101 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 を以前のバージョンに復元する際には、注意が 必要です。 バックアップ時点に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 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)。システム全体の完全な復元を行います。
 一般に、従来のバックアップと復元の目的で使用します。
 - [Protected Restore] (保護された復元)。 シリアル番号、MAC アドレス、 IP アドレス、名前などのデバイスに固有な情報を除き、システム全体が復 元されます。 このオプションを使用すると、1 台の KX II-101 でセットアッ プを行い、その設定を複数の KX II-101 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。 該当 するチェックボックスをオンにします。
 - [User and Group Restore] (ユーザとグループの復元)。このオプションに含まれるのは、ユーザとグループの情報だけです。このオプションを使用すると、別の KX II-101 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)。このオプションに 含まれるのは、デバイス設定だけです。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。
- [Browse] (参照) ボタンをクリックします。 [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。
- 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。



[Firmware Upgrade] (ファームウェアのアップグレード)

4. [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。

[Firmware Upgrade] (ファームウェアのアップグレード)

[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 ユニットのファームウェアをアップグレードします。 このページは、KX II-101 リ モート コンソールでのみ使用できます。

重要: アップグレードの実行中は、使用している KX II-101 ユニットの 電源を切断しないでください。ユニットが損傷する可能性があります。

- > KX II-101 ユニットをアップグレードするには、以下の手順に従います。
- [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。

Show Latest	Firmware	
Firmware File		
	Browse	

- [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] 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。



 [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。

Firmware Upgrade	
Current version:	2.0.0.5.6394
New version:	2.0.0.5.6487
Upgrade Cance	1
This may take some minutes update is in progress! After automatically.	. Please do NOT power off the device while the a successful update, the device will be reset

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。

5. [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、ユニットが再起動します。

Firmware Upgrade in Progress					
	Upgrade successful.				
DKX2-	101 has been updated with new firmware.				
Device willreb Please	oot now and this will take approximately 5 minutes. close the browser before logging in again.				
	Progress: Upgrade Finished				
	100%				

6. 表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 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 では、KX II-101 ユニットと接続されている CIM で実行したアップグレードに関する情報を確認できます。

- > 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。

grade History							
Гуре	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:30	January 09, 2000 20:32	2.0.0.5.6236	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.67	January 09, 2000 20:18	January 09, 2000 20:20	2.0.0.5.6191	2.0.0.5.6236	Successful
Full Firmware Upgrade	admin	192.168.50.65	January 06, 2000 17:58	January 06, 2000 18:01	2.0.0.1.6126	2.0.0.5.6191	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 2000 00:02	January 01, 2000 00:04	99.99.99.2.9999	2.0.0.1.6126	Successful
Full Firmware Upgrade	admin	192.168.59.35	January 01, 1970 00:06	January 01, 1970 00:09	2.0.0.1.5974	99.99.99.2.9999	Successful
Full Firmware Upgrade						2.0.0.1.5974	Failed

[Reboot] (再起動)

[Reboot] (再起動) ページを使用すると、安全かつ制御された順序で KX II-101 ユニットを再起動できます。そのため、この方法で再起動を行うことをお勧めします。

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

- > KX II-101 を再起動するには、以下の手順に従います。
- [Maintenance] (メンテナンス)の [Reboot] (再起動) を選択します。
 [Reboot] (再起動) ページが開きます。

d mb mo h	CTT OFFICIAL OFFIC			~
lome > Mainte	enance > Reboot	CONTRACTOR AND		
Reboo	t.			
	1	Reboot		
	This may	take up to two minutes	J	



ort Access	Virtual Media	User Manageme	nt Device Setting	s Security	Mainten
1-1-1-6	1 8 6 9	No. C. L		<u> </u>	\sim
fome > Mainb	enance > Reboot				
Reboo Do you	ting the syste want to pro	em will logoff : ceed with the	nll users. reboot?		
Reboo	t				
	E	Yes No			
	This may	take up to two minu	tes.		

2. [Reboot] (再起動) ボタンをクリックします。 操作を確認するプロンプトが表示 されます。

- 3. [Yes] (はい) をクリックして、再起動を続行します。
- ▶ 再起動せずに終了するには、以下の手順に従います。
- [No] (いいえ) をクリックします。



コマンド ライン インタフェース(CLI)

この章の内容

概要	
CLI を使用しての KX II-101 へのアクセス	167
KX II-101 への SSH 接続	
ログイン	168
CLI のナビゲーション	169
CLI コマンド	

概要

12

この章では、KX II-101 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『『p. 170の"CLI コマンド"参照先』」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: 次のコマンドは、前の図の CLI のすべてのレベルから使用できます。top、 history、logout、quit、help。



CLI を使用しての KX II-101 へのアクセス

次の方法のいずれかを使用して、KX II-101 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/
- ssh.com の SSH クライアント www.ssh.com http://www.ssh.com
- Applet SSH Client *www.netspace.org/ssh* http://www.netspace.org/ssh
- OpenSSH Client www.openssh.org http://www.openssh.org

注: Accessing the CLI by SSH または TELNET ヘのアクセスには、KX II-101 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、「デバイス サービス 『p. 119の" [Device Services] (デバイス サービス)"参照先 』」を参照してください。

KX II-101 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、「*デバイス サービス*『p. 119の"[Device Services] (デバイス サー ビス)"参照先 』」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 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、以下の手順に従います。
- 1. PuTTY などの SSH クライアント ソフトウェアを起動します。
- 2. KX II-101 サーバの IP アドレス「192.168.0.192」を入力します。
- 3. デフォルトの設定ポート 22 を使用する [SSH] を選択します。
- 4. [Open] (開く) ボタンをクリックします。



5. 次のプロンプトが表示されます。 login as:

ログイン情報の詳細は、「ログオン」セクションを参照してください。

UNIX 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には、次のコマンドを入力します。

ssh -l admin 192.168.30.222

パスワードのプロンプトが表示されます。

ログイン情報の詳細は、「ログオン」セクションを参照してください。

ログイン

ログインするには、次のように ユーザ名 admin を入力します。

Login: admin

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。

Password:

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。

Login: admin Password:		
Device Type: Dominion KX2-101 Device Name: DKX2-101-DOC IP Address: 192.168.50.153	Model: DKX2-101 FW Version: 2.0.0.5.6394 SN: AAX7800010 Idle Timeout: 30min	
Port Port Port Port No. Name Type Status Availability 1 - Dominion_KXII-101_Port KVM up idle Current Time: Wed Dec 26 14:37:00 2007		
Admin Port > _		

次の「CLI のナビゲーション『p. 169』」セクションを確認したら、「 管理シリアル コン ソールの使用 『p. 25の"ターミナル エミュレーション プログラムの使用"参照先 』」で 説明されている初期設定タスクを実行できます。



-1

CLI のナビゲーション

CLI を使用する前に、CLI のナビゲーションと構文を理解しておくことが重要です。 さらに、CLI の使用を簡素化するキーの組み合わせがあります。

CLI プロンプト

コマンド ライン インタフェースのプロンプトは、現在のコマンド レベルを示します。 プ ロンプトのルート部分はログイン名です。ターミナル エミュレーション アプリケーションを 使用する管理シリアル ポートへの直接接続の場合、Admin Port がコマンドのル ート プロンプトです。

Admin Port > Config > Network >

TELNET/SSH の場合、admin がコマンドのルート プロンプトです。

admin > config > network >

コマンドの完成

CLI は、部分的に入力されたコマンドの完成をサポートします。入力の最初の数 文字を入力して Tab キーを押します。文字例が一意に一致する場合、CLI は入 力を完成させます。

- 一致が見つからない場合、CLIはそのレベルの有効なエントリを表示します。
- 複数の可能性のある一致が見つかった場合、CLIは有効なエントリも表示します。
- エントリを一意にするために追加のテキストを入力し、Tab キーを押して入力を 完成させます。



CLI構文 - ヒントとショートカット

ヒント

- コマンドはアルファベット順に一覧表示されます。
- コマンドでは大文字と小文字を区別しません。
- パラメータ名は下線を含まない1 つの単語で表されます。
- 引数のないコマンドはデフォルトでコマンドの現在の設定を示します。
- コマンドの後に疑問符 (?) を入力すると、そのコマンドのヘルプが表示されます。
- 縦線(|)はオプションまたは必須のキーワードまたは引数内の選択肢を示します。

ショートカット

- 最後のエントリを表示するには、上向きの矢印を押します。
- 入力した最後の文字を削除するには、Backspace キーを押します。
- 間違ったパラメータを入力した場合は、Ctrl/C キーを使用してコマンドを終了またはキャンセルします。
- コマンドを実行するには、Enter キーを使用します。
- コマンドを完成するには、Tab キーを押します。例、Admin Port > Conf
 次に、システムは、Admin Port > Config > プロンプトを表示します。

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	
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 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 [p. 172]	[diagnostics] (診断) メニューに切り替えます。.
<i>debug</i> 『p. 172の "[Debug] (デバッグ)" 参照先 』	[debug] (デバッグ) メニューに切り替えます。
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 のネットワーク インタフェースを設定します。
<i>listports</i> 『p. 175の "Listports コマンド"参 照先 』	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。
logout	現在の CLI セッションをログアウトします。
<i>name</i> 『p. 174の "[Name] (名前) コマ ンド"参照先 』	デバイス名を設定します。
<i>network</i> 『p. 173の "[Network] (ネットワー ク)"参照先 』	ネットワーク設定を表示し、設定できます。
quit	前のコマンドに戻ります。
<i>setlog</i> 『p. 172の "Setlog コマンド"参照 先』	デバイスのログ記録オプションを設定します。
top	[root] (ルート) メニューに戻ります。
<i>userlist</i> 『p. 175の "Userlist コマンド"参 照先 』	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。



Diagnostics

[Diagnostics] (診断) メニューでは、KX II-101 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)

[Diagnostics] (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 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 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 から、これらの設定の指定方法をお伝えします。

コマンドのオプション	
module	モジュール名。
level	診断レベル:
	err
	warn
	info
	debug
	trace


コマンドのオプション	説明
vflag	verbose flag のタイプ:
	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。

[Network] (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	
interface	KX II-101 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] (名前) 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。

デバイス名の構文は、次のとおりです。

name devicename <>

ホスト名の構文は、次のとおりです。

name hostname <>

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 devicename <device name>

次のコマンドは、ホスト名を設定します。

Admin Port > Config > Network > name hostname <host name>

[Interface] (לעקדו-ג) ביאר (לעקדו-ג)

interface コマンドを使用して、KX II-101 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、ユニットは 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。詳細は、「*インストールと設定*『p.7』」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]</pre>

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	
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 の IP アドレス
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="" =""></auto>	[Ethernet Mode] (Ethernet モード) を auto に設定します。または、100Mbps 全二 重 (100fdx) を指定します。



コマンド ライン インタフェース (CLI)

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_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



13 Diagnostics

この章の内容

[Diagnostics] (診断) メニュー	
[Network Interface] (ネットワーク インタフェース) ページ	
[Network Statistics] (ネットワーク統計) ページ	
[Ping Host] (ホストへの Ping) ページ	
[Trace Route to Host] (ホストへのトレース ルート) ページ	
[Device Diagnostics] (デバイス診断)	

[Diagnostics] (診断) メニュー

[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 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 ([Diagnostics] (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。

[Diagnostics] (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。

次のオプションを使用できます	す	0

メニュー	操作
[Network Interface] (ネットワーク インタフェー ス)	ネットワーク インタフェースの状態を取得します。
[Network Statistics] (ネットワーク統計)	ネットワークについての統計を取得します。
[Ping Host] (ホストへの Ping)	特定のホストが IP ネットワーク上でアクセス可能かど うかを特定します。
[Trace Route to Host] (ホストへのトレース ルー ト)	選択したホストまでのすべてのルートを特定します。
[Device Diagnostics] (デバイス診断)	Raritan テクニカル サポートの指示があった場合に使用します (リモート コンソールのみ)。



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

KX II-101 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。

Home > Diagnostics > Network Interface
Network Interface
Refresh
Result:
Link state: autonegotiation on, 100 Mbps, full duplex, link ok eth0: <broadcast,multicast,up> mtu 1500 qdisc pfifo_fast qlen 1000 link/ether fe:05:0d:00:00:1b brd ff:ff:ff:ff:ff:ff inet 192.168.61.250/24 brd 192.168.61.255 scope global eth0 LAN 1 is active.</broadcast,multicast,up>
and a second second and a second s

次の情報が表示されます。

- Ethernet インタフェースが稼動しているか、ダウンしているか。
- ゲートウェイが Ping 可能か否か。
- 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 Statistics] (ネットワーク統計) ページ

KX II-101 では、ネットワーク インタフェースに関する統計を確認できます。

- > ネットワーク インタフェースの統計を表示するには、以下の手順に従います。
- [Diagnostics] (診断)の [Network Statistics] (ネットワーク統計)を選択します。 [Network Statistics] (ネットワーク統計) ページが開きます。



[Network Statistics] (ネットワーク統計) ページ

- 2. [Option] (オプション) ドロップダウン リストから適切なオプションを選択します。
 - [Statistics] (統計)。次に示すようなページが生成されます。





Diagnostics

	Virtual Media	User Management	Device Settings	Security	Maintenance	Diagnostics
1220	1001	Barris A		~~	$\sim \sim$	
ome > Diagn	ostics > Network Si	tatistics				
C						
Network	Statistics					
Options:						
Interface	5					
Refres	h					
Deside						
Result						
	nterface tab	le				
Kernel I	U Het RX-OK	RX-ERR RX-DRP RX	COVR TX-OK TX	-ERR TX-	DRP TX-OVR	Flg
Kernel I Iface HT						
Kernel I Iface MT ethl 150	0 0 13828 0	0 0 8680 0 0 0 E	MNRU			
Kernel I Iface HT ethl 150 10 16436	0 0 13828 0	0 0 8680 0 0 0 E 196 0 0 0 LRU	SMNRO			

■ [Interfaces] (インタフェース)。次に示すようなページが生成されます。

■ [Route] (ルート)。次に示すようなページが生成されます。

ort Access	Virtual Media	User Management	Device Settings	Security	Main
1-2-120	나는 않는 것 같은	March & March			\sim
lome > Diagn	ostics > Network St	tatistics			
-					
Network	Statistics				
Ontions:					
route	•				
Defeed	_				
Refres	n				
Result:					
Vernel T	D routing to	ble			
Destinat	ion Gateway	Genmask Flags MS	SS Window irtt	Iface	
192.168.	59.0 * 255.2	55.255.0 U 0 0 0) ethl		
default	192.168.59.1	26 0.0.0.0 UG 0	0 0 ethl		
	and a state	A	and the second second second second	A	

3. [Refresh] (更新) ボタンをクリックします。

[Result] (結果) フィールドに該当する情報が表示されます。



[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 ネットワーク上でアクセス可能であ るかどうかをテストするために使用される、ネットワーク ツールです。 [Ping Host] (ホ ストへの Ping) ページを使用すると、ターゲット サーバまたは別の KX II-101 ユニ ット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 を実行するには、以下の手順に従います。
- [Diagnostics] (診断)の [Ping Host] (ホストへの Ping)を選択します。
 [Ping Host] (ホストへの Ping) ページが開きます。

ort Access	Virtual Media	User Management	Device Settings	Security
	1.001	manife M		\sim
ome > Diagn	ostics > Ping Host			
Ping Host	l.			
Hostname	or IP Address:			
192.168.59	.97			
Ping				
Result				
		Sec. 20		
192.168.	59.97 is ali	vel		

- [Hostname or IP Address] (ホスト名または IP アドレス) フィールドにホスト 名または IP アドレスを入力します。
- 3. [Ping] をクリックします。 [Result] (結果) フィールドに Ping の結果が表示 されます。



[Trace Route to Host] (ホストへのトレース ルート) ページ

トレース ルートは、特定のホスト名または IP アドレスまでに辿るすべてのルートを特定するために使用されるネットワーク ツールです。

- ▶ ホストまでのルートをトレースするには、以下の手順に従います。
- [Diagnostics] (診断)の [Trace Route to Host] (ホストへのトレース ルート))を選択します。 [Trace Route to Host] (ホストへのトレース ルート) ページが開きます。

ort Access	Virtual Media	User Management	Device Settings	Security	Mainten
		Ostation Sa State			
ome > Diagno	ostics > Trace Roy	te to Host			
Trace Ro	ute to Host			÷	
Red and the second second					
Hostname	or IP Address:				
192.168.59	.97				
Maximum	Hons:				
5 -	nopo.				
<u> </u>					
Trace	Route				
Dent					
result.					
tracerou	te started a	main for 2mine			
1 192.16	8.59.97 (192	.168.59.97) 0.43	18 ms 0.434 ms	0.368 m	s
constantile .	1.0.00				en 10 10

- 2. [Hostname or IP Address] (ホスト名または IP アドレス) フィールドにホスト 名または IP アドレスを入力します。
- 3. ドロップダウン リストから [Maximum Hops] (最大ホップ数) を選択します (5 刻みで 5 ~ 50、)。
- [Trace Route] (トレース ルート) ボタンをクリックします。 トレース ルート コマンドは、所定のホスト名、IP アドレス、最大ホップ数で実行されます。
 [Result] (結果) フィールドにトレース ルートの出力結果が表示されます。



[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 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と共にまたは単独で、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。

- 診断スクリプト (オプション) 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。 スクリプトはユ ニットにアップロードされ、実行されます。
- 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 ユニットから クライアントにダウンロードします。この暗号化されたファイルは、その後 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 システム診断を実行するには、以下の手順に従います。
- [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。

Home > Diagnostics > Device Diagnostics	I.
	ł
Device Diagnostics	ł
	1
	ł,
Diagnostics Scripts:	ł
Script File:	ł.
Browse	ł
	1
	ł
Dominion KX2-101 Diagnostic Log:	C
Save To File	£
	ł

- (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. [Browse] (参照) ボタンを使用します。 [Choose File] (ファイルの選択) ダイアログ ボックスが開きます。
- 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。

Diagnostics So	ripts.	
C: Documents and S	etting:	Browse
Run Script	Cancel	

- 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) ボタンをクリックします。 [File Download] (ファイルのダウンロード) ダイアログ ボックスが開きます。

•••	Name:	diagnostics_sav	/e	
	From:	192.168.59.15	уре, оч.3 кр)	
			Save	Cancel

- 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 ボックスが開きます。
- 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。



14 CC Unmanage

この章の内容

概要	
CC-SG 管理からの KX II-101 の除外	
プロキシ モードでの CC-SG の使用	

概要

KX II-101 デバイスが CommandCenter Secure Gateway の管理下にあるとき、 KX II-101 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)。

Managed by Command Center Secure Gateway

This device is being managed by Command Center Secure Gateway (CC-SG)

192.168.61.129

Direct Login is disabled at this time!



CC-SG 管理からの KX II-101 の除外

CC-SG の制御対象から KX II-101 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 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 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、メンテナンス権限が必要です。

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。

Managed by CommandCenter Secure Gateway 192.168.59.246
This device is being managed by CommandCenter Secure Gateway
192.168.59.246
Do you want to remove it from CommandCenter Management?
Yes No



CC-SG 管理からの KX II-101 の除外

- 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) ボタンをクリックします。 操作を確認するプロンプトが表示されま す。

2. [Yes] (はい) ボタンをクリックします。 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. [Yes] (はい) をクリックします。 KX II-101 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 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。



仕様

この章の内容

KX II-101	188
コネクタ	189
Raritan Remote Client ソフトウェア	189

KX II-101

Α

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 キットを
	(付属)
寸法 (DxWxH)	
	4.055"x 2.913"x 1.063", 103 x 74 x 27mm
重量	0.6292lbs, 0.286kg
電源	
	AC/DC (100-240V~/ 6VDC) 電源アダプタ
	または
	Power over Ethernet (PoE)
	ミッドスパン給電方式
	シグナルペア給電方式
使用温度	
	$0^{\circ} \sim 40^{\circ} C (32^{\circ} \sim 104^{\circ} F)$
湿度	
	20% ~ 85% RH
インジケータ:	
青 RARITAN バックライト ロゴ	 記動おたび電力しベル インジケータ
ネットワーク ポート	
	ネットリーク アクティビティおよび接続速度1 フングータ
ローカル接続	
	1- USB ボート、USB キーホード / マウス、およひターケットへの仮想メティア接続 用
	1- ミニ DIN9 ポート、フル RS-232 機能、モデム接続、および Dominion PX 接続の多機能シリアル ポート用



リモート接続: ネットワーク プロトコル	10/100 Ethernet (RJ45) ポート × 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、 1152 X 864 @ 60/75Hz、 1280 X 1024 @ 60Hz、 1600 X 1200 @ 60Hz		
認定:	UL/CUL、FCC Class A、CB、CE Class A、VCCI Class A		

コネクタ

インタフェース タイプ	長さ (インチ、 cm)	説明
ビデオ	15″ 、 38 cm	統合ケーブル
PS/2	15″ 、 38 cm	統合ケーブル
ミニ USB - USB(M)	17.7″ 、 45 cm	USB 用ケーブル
ξΞ Din9(M) - DB9(F)	72″ 、 182 cm	シリアル用ケーブル
DKX2-101-LPKVMC	3.9" 、 10 cm	ローカル ポート統合用ケーブル
DKX2-101-SPDUC	70.86" 、 180 cm	Dominion PX への接続用ケーブル

Raritan Remote Client ソフトウェア

オペレーティング システムの要件: Windows XP / NT / ME / 2000



ラック マウント

KX II-101 ユニットは、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 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

AC-DC アダプタ クリップ取り付け具	
ブラケットの取り付け	

AC-DC アダプタ クリップ取り付け具

Β

クリップ タイプの識別

- 1. EU クリップ
- 2. オーストラリア クリップ
- 3. UK クリップ









AC-DC 電源アダプタからのアタッチメント カバーの取り外し

- 1. AC/DC 電源アダプタ
- 2. アタッチメント カバー。 押して取り外します。



AC-DC 電源アダプタへのクリップの取り付け

- 1. オーストラリア クリップ
- 2. EU クリップ
- 3. UK クリップ



4. 電源アダプタ



ブラケットの取り付け

- 1. KX II-101 ユニット
- 2. 右パネル
- 3. **左パネル**
- 4. ネジ



- KX II-101 ユニットからネジを取り外します。
- KX II-101 ユニットの左パネルおよび右パネルをスライドさせて外します。



- **KX II-101** ブラケット部品
- 1. U ブラケット
- 2. L ブラケット





横に取り付ける KX II-101 にブラケットを取り付けます

- 1. KX II-101 ユニット
- 2. U ブラケット
- 3. L ブラケット
- 4. ネジ
- 5. 取り付け穴
- 6. ラッチ レバー
- 付属のネジを使用して U ブラケットを L ブラケットに取り付けます。ネジを締め付ける前にブラケットの位置を調整します。
- ラック取り付けネジ (ラック メーカー提供品)を使用して U ブラケットと L ブラケットのアセンブリをラックに取り付けます。
- KVM ハーネスをターゲット側に向けて、KX II-101 ユニットを U ブラケット内 にスライドさせます。 ラッチ レバーを引っ張って解放し、KX II-101 ユニットを U ブラケットに固定します。.

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



縦に取り付ける KX II-101 にブラケットを取り付けます

1. KX II-101 ユニット



- 2. U ブラケット
- 3. L ブラケット
- 4. ネジ
- 5. 取り付け穴
- 6. ラッチ レバー

付属のネジを使用して U ブラケットを L ブラケットに取り付けます。 ネジを締め付ける前にブラケットの位置を調整します。

ラック取り付けネジ (ラック メーカー提供品) を使用して U ブラケットと L ブラケットのアセンブリをラックに取り付けます。

KVM ハーネスをターゲット側に向けて、KX II-101 ユニットを U ブラケット内にスラ イドさせます。 ラッチ レバーを引っ張って解放し、KX II-101 ユニットを U ブラケッ トに固定します。





Ľ

[About Raritan Virtual KVM Client] (バージョ ン情報) - 100 [Absolute] (絶対) - 97 [Add New Favorite] (新しいお気に入りの追 加) - 37, 42 [Add New User] (新規ユーザの追加) - 46, 47, 48, 149 [Audit Log] (監査ログ) - 157 [Authentication Settings] (認証設定) - 57, 59 [Auto-sense Video Settings] (ビデオ設定の自 動検出) - 90 [Backup and Restore] (バックアップと復元) -160 [Calibrate Color] (色調整) - 90 [Change Password] (パスワードの変更) - 57 [Configuration] (設定) - 173 [Connection Info] (接続情報)-84 [Connection] (接続) メニュー - 82 [Date/Time Settings] (日付/時刻の設定) - 123 [Debug] (デバッグ) - 171, 172 [Device Diagnostics] (デバイス診断) - 182 [Device Information] (デバイス情報) - 159 [Device Services] (デバイス サービス) - 119, 167 [Device Settings] (デバイス設定) メニュー -113 [Diagnostics] (診断) メニュー - 176 [Discover Devices - KX II-101 Subnet] (Discover Devices (デバイス検出)- KX II-101 サブネット)-41 [Discover Devices - Local Subnet] (デバイス検 出 - ローカル サブネット)-39 [Encryption and Share] (暗号化および共有) -150[Event Management - Destinations] (イベント 管理 - 送信先) - 128 [Exit] (終了) - 84 [Favorites List] (お気に入りリスト) - 37 [Firmware Upgrade] (ファームウェアのアッ プグレード)-162 [Help] (ヘルプ) メニュー - 100

[Intelligent] (インテリジェント) - 96 [Interface] (インタフェース) コマンド - 174 [IP Access Control] (IP アクセス制御) - 51, 54, 118, 153 [Keyboard Macros] (キーボード マクロ) - 85 [Keyboard] (キーボード) メニュー - 85 [Logon Limitations] (ログオン制限) - 145, 146 [Maintenance] (メンテナンス) メニュー - 156 [Manage Favorites] (お気に入りの管理) メニ ュー - 36 [Mouse] (マウス) メニュー - 80,93 [Name] (名前) コマンド - 171, 174 [Network Interface] (ネットワーク インタフ ェース) ページ - 177 [Network Settings] (ネットワーク設定) - 114 [Network Statistics] (ネットワーク統計) ペー ジ - 177 [Network] (ネットワーク) - 171, 173 [Options] (オプション) - 98 [Ping Host] (ホストへの Ping) ページ - 180 [Port Access] (ポート アクセス) ページ - 43 [Port Configuration] (ポート設定) - 132 [Properties] (プロパティ) ダイアログ ボック ス - 82 [Reboot] (再起動) - 164 [Refresh Screen] (画面の更新) - 89 [Scaling] (拡大、縮小) - 99 [Security Settings] (セキュリティ設定) - 144, 145 [Security Settings] (セキュリティ設定) メニュ ··· - 144 [Send Ctrl+Alt+Delete] (Ctrl+Alt+Delete の送 信) - 85 [Serial Port Settings] (シリアル ポート設定) -122 [Single Mouse Cursor] (シングル マウス カー ソル)-94 [Standard] (標準) - 95 [Strong Passwords] (強力なパスワード) - 57, 146, 147 [Synchronize Mouse] (マウスの同期) - 93 [Target Screen Resolution] (ターゲット画面解 像度) - 100



[Tools] (ツール) メニュー - 98
[Trace Route to Host] (ホストへのトレース ル ート) ページ - 181
[User Blocking] (ユーザ ブロック) - 48, 146, 149
[User Group List] (ユーザ グループ リスト) - 49
[User List] (ユーザ リスト) - 46
[User Management] (ユーザ管理) - 44, 45
[User Management] (ユーザ管理) メニュー - 45
[Video Settings] (ビデオ設定) - 90
[Video] (ビデオ) メニュー - 89
[View Toolbar] (ツール バーの表示) - 99
[View] (表示) メニュー - 99

A

AC-DC アダプタ クリップ取り付け具 - 190
AC-DC 電源アダプタからのアタッチメント カバーの取り外し - 191
AC-DC 電源アダプタへのクリップの取り付 け - 191
Admin ポートの使用 - 18, 25
AppleR Macintosh の設定 - 13

С

CC Unmanage - 184 CC-SG ユーザへの注意事項 - 58 CC-SG 管理からの KX II-101 の除外 - 185 CD-ROM/DVD-ROM/ISO イメージ - 105, 109, 111 CLI コマンド - 166, 170 CLI のナビゲーション - 168, 169 CLI プロンプト - 169 CLI を使用しての KX II-101 へのアクセス -167 CLI 構文 - ヒントとショートカット - 170

D

Diagnostics - 171, 172, 176 Dominion KX II-101 の概要 - 1

Ι

IP アドレスの割り当て - 6,21

J

Java Runtime Environment (JRE) - 30

Κ

KVM セッションを開く - 106
KX II-101 - 188
KX II-101 コンソールでの案内 - 33
KX II-101 コンソールのレイアウト - 32
KX II-101 の起動 - 31
KX II-101 の皮症 - 7, 14
KX II-101 の設定 - 7, 19
KX II-101 ブラケット部品 - 193
KX II-101 への SSH 接続 - 167
KX II-101 への権続 - 22, 30
KX II-101 への電源供給 - 18
KX II-101 リモート コンソールのメニュー マップ - 34

L

LAN インタフェース設定 - 117 LDAP から返す場合 - 67 LDAP スキーマの更新 - 63, 66 LDAP リモート認証の実装 - 61 Linux の設定 - 11 Listports コマンド - 171, 175

Μ

Microsoft Active Directory から返す場合 - 67 Microsoft Active Directory についての注意事 項 - 58

Ρ

PS/2 の設定 - 15

R

RADIUS リモート認証の実装 - 60,64 RADIUS 通信交換仕様 - 65 Raritan Remote Client ソフトウェア - 189

S

Setlog コマンド - 171, 172



SNMP エージェント設定 - 125, 130 SNMP トラップ設定 - 125, 130 SNMP の設定 - 125 Sun Solaris の設定 - 12 Sun ビデオ解像度の設定 - 8 Syslog の設定 - 126

U

UNIX ワークステーションからの SSH アク セス - 168 USB の設定 - 17 Userlist コマンド - 171, 175

V

Virtual KVM Client - 76 VKC 仮想メディア - 97

W

Windows 2000 の設定 - 11 Windows PC からの SSH アクセス - 167 Windows Vista - 10 Windows XP の設定 - 11

あ

アップグレード履歴 - 164 イベント管理 - 124 インストールと設定 - 7, 174 インタフェース - 3 オプション - 78 オプションのアクセサリ - 5 お気に入りの管理 - 35

か

キーボード マクロの作成 - 86 キーボード マクロの削除 - 89 キーボード マクロの実行 - 88 キーボード マクロの変更 - 88 キーボード/マウスの設定 - 121 クラスへの属性の追加 - 69 クリップ タイプの識別 - 190 グループ - 44 グループベースの IP ACL (アクセス制御リス ト) - 53 コネクタ - 5, 189 コマンド ライン インタフェース (CLI) - 166 コマンドの完成 - 169 コンセントの関連付けの表示 - 141 コンセントへの KVM ターゲット サーバの 関連付け ([Port] (ポート) ページ) - 137, 142

さ

サーバ ビデオ解像度の設定 - 8,15 サービス パック - 6 サポートされているプロトコル - 58 システム管理機能 - 3 スキーマ キャッシュの更新 - 71 スキーマへの書き込み操作を許可するための レジストリ設定 - 68 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 - 170

た

ターゲット サーバに名前を付ける - 22 ターゲット サーバの設定 - 7 ターゲット サーバへの接続 - 15 ターミナル エミュレーション プログラムの 使用 - 6, 25, 168 ダイレクト ポート アクセスの設定 - 21 ダイレクト ポート アクセスの育効化 - 32 ツール バー - 79 デバイス管理 - 113 デフォルト IP アドレス - 6

な

ネットワーク ファイアウォールの設定 -7,19 ネットワークへの接続 -18 ネットワーク基本設定 -115 ネットワーク設定 -3

は

はじめに - 1 パッケージの内容 - 4 パワー ストリップの接続 - 135, 138 パワー ストリップの名前の指定 (パワー ス トリップの [Port] (ポート) ページ) - 136 ビデオ解像度 - 4 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) - 105, 111 ブラケットの取り付け - 192 プロキシ モードでの CC-SG の使用 - 187



索引

ポート権限の設定 - 53

ま

マウス ポインタの同期 - 80 マウス モード - 10 マウス同期のヒント - 80 メニュー ツリー - 78 メンテナンス - 156

や

ユーザ - 44
ユーザ グループ情報を Active Directory サ ーバから返す - 63
ユーザ グループ情報を RADIUS 経由で返す - 65
ユーザ グループ情報を返す - 66
ユーザ ブロックとブロック解除 - 48
ユーザ メンバの rciusergroup 属性の編集 - 72
ユーザ、グループ、アクセス許可 - 44
ユーザとグループの関係 - 45
ユーザとグループの作成 - 23
ユーザ機能 - 4

ß

ラック マウント - 4, 190 リモート コンソールの使用 - 20 リモート認証 - 58 ローカル ドライブ - 105, 107 ローカル ユーザ ポートの使用 - 19 ログイン - 6, 168 ログオフ - 34

漢字

横に取り付ける KX II-101 にブラケットを取 り付けます - 194 仮想メディア - 97, 101 仮想メディアの使用 - 105 仮想メディアの切断 - 105, 110 仮想メディアへの接続 - 107 仮想メディアを使用するための前提条件 - 104, 105 概要 - 77, 102, 134, 166, 184 管理の特長 - 3 既存のユーザ グループの変更 - 50, 56 既存のユーザの変更 - 46,48 許可の設定 - 51, 52, 56 言語サポート - 30 個別グループの許可の設定 - 48,52 仕様 - 188 使用しているブラウザの AES 暗号化の確認 - 151, 152 取り付け-4 縦に取り付ける KX II-101 にブラケットを取 り付けます - 194 重要な情報 - 6 新しいパスワードの設定 - 20 新しい属性の作成 - 68 製品の写真 - 2 製品の特長 -3 電源 - 4 電源タップ デバイスの制御 - 134, 142 電源制御 - 134 読み取り/書き込み可能に設定できない状況 -107, 108 認証と認可 - 58,59 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:+81-3-3523-5994 電子メール:support.japan@raritan.com

*► ב−ם*שוו

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+1 CET) 電話:+44-20-7614-77-00 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(GMT+1CET) 電話:+49-20-17-47-98-0

▶ 韓国

月曜日~金曜日 午前 9 時~午後 6 時 (現地時間) 電話:+82-2-5578730

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:tech.rap@raritan.com