

クイックセットアップガイド



Dominion® KX III

このたびは、エンタープライズ向けデジタルKVM Dominion KX IIIをご購入いただきまして、誠にありがとうございます。 このクイックセットアップガイドでは、KX IIIの初期設定についてご説明いたします。詳細につきましては、ラリタンWebサイトのサポートページ にで、オンラインヘルプをご参照ください。 https://www.raritan.com/jp/support/product/dominion-kx-iii

・内容物一覧

KX III本体

KX IIIクイックセットアップガイド(本紙)

ラックマウントキット

AC電源コード (2本)

デスクトップ設置用ゴム足(4つ)

アプリケーションノート

製品保証書

- 管理者ガイドに記載されたKX IIIの動作温度範囲から逸脱し ない環境でご利用ください。
- 適切なエアフロー環境を確保してください。.
- 不均一な機械的負荷を避けるために、KX IIIをラックに 慎重に取り付けてください。
- 過負荷にならないように、適切に電源を接続してください。
- リモート接続の安定性を確保するために、KX IIIに関わる全ての機器の接地を適切に行ってください。

ラックマウント

KX IIIは、19インチラックの1Uスペースに取り付け可能です。 ※ 本紙の図は例であり、購入された製品を正確に示していない 場合がありますので、取り付けにあたっては注意してください。

ラック前面への取り付け

- 付属の2本のネジを使用して側面ブラケットの後端にケー ブルサポートバーを固定します。
- KX IIIを、背面パネルがケーブルサポートバーに面した状態で 側面ブラケットの間にはめ込み、その前面パネルを側面ブラ ケットの「耳」に揃えます。

- 3. KX IIIの両側を添付のネジ(片側3本ずつ)で固定します。
- 専用のネジ、ボルト、ケージナットなどで側面ブラケットの 耳をラックの前面レールに固定します。
- 5. KX IIIの背面に接続するケーブルは、ケーブルサポートバーの上 に掛けます。



ラック背面への取り付け

- 付属の2本のネジを使用して側面ブラケットの前端(側面ブラケットの「耳」の近く)にケーブルサポートバーを固定します。
- KX IIIを、背面パネルがケーブルサポートバーに面した状態で側面ブ ラケットの間にはめ込み、その前面パネルを側面ブラケットの後端に 揃えます。
- 3. KX IIIの両側を添付のネジ(片側3本ずつ)で固定します。
- 専用のネジ、ボルト、ケージナットなどで側面ブラケットの 耳をラックの前面レールに固定します。
- 5. KX IIIの背面に接続するケーブルは、ケーブルサポートバーの上 に掛けます。





Step 1: Firewall設定

-TCP Port 5000

TCPポート5000でのネットワークとファイアウォールの通信を 許可すると、KX IIIへのリモートアクセスが有効になります。

または、別のTCPボートを使用するようKX IIIを設定すると、そ のポートでネットワークとファイアウォールの通信ができるよ うになります。

-TCP Port 443

TCPポート443(標準HTTPS)へのアクセスを許可すると、Webブ ラウザ経由でKX IIIにアクセスできるようになります。

-TCP Port 80

TCP ポート80(標準HTTP)へのアクセスを許可すると、HTTP要求が自動 的にHTTPSにリダイレクトされます。

Step 2: KVMのターゲットサーバー設定

マウス設定

ターゲットサーバーのマウス設定は、特別な場合を除き、 Absolute Mouse(ずれないマウス)の利用を推奨します。

このモードでは、ターゲットマウスが異なる速度に設定されている 場合でも、絶対座標を使用してクライアントカーソルとターゲット カーソルの同期を維持します。 このモードは、仮想メディア対応 CIMでサポートされます。

 Absolute Mouseは、D2CIM-DVUSB, D2CIM-DVUSB-DVI, D2CIM-DVUSB-HDMI, D2CIM-DVUSB-DP, D2CIM-VUSB-USBC, D2CIM-VUSB で利用できます。

ターゲットサーバーのビデオ解像度

サポート対象の解像度は、オンラインヘルプを参照してください。(https://help.raritan.com/kx-iii/v3.8.0/en/#32872.htm)

Step 3: 機器の接続

※型番によって外観は異なります。



A: AC電源



1. KX IIIに添付されている電源コードを使用します。冗長 性を保つ場合は、2本接続します。

B: ネットワークポート

Ethernetケーブルを、「LAN1」のラベルの付いたネットワークポ ートから、ネットワーク機器に接続します。

Failover mode または Isolation mode (分離モード)機能を有効 にするためには、Ethernetケーブルを「LAN2」のラベルの付いた ネットワークポートから、ネットワーク機器に接続します。

C: ローカルユーザーポート

- ▶ キーボードとマウスを接続:
- USBキーボードおよびマウスを、KX IIIの背面のそれぞれの ローカルユーザーポートに接続します。

ラック前での管理およびターゲットデバイスアクセスのためにKX IIIローカルユーザーポートを使用できます。ローカルユーザーポ ートは、初期セットアップの際に必要ですが、それ以降の使用は 省略できます。また、Dominion シリアルアクセスモジュール (DSAM)を使用する場合、ローカルユーザーポートに接続可能です。

D: ローカルDVI-Dポート

シングルリンクのDVIケーブルは、DVIモニターまたはキーボード トレイ(T1700-LED-J/T1900-LED-J)利用時に接続します。

E. KX IIIへのターゲットサーバーの接続

1. CIMの各プラグをターゲットサーバーに接続します。



- 2. Cat5/5e/6ケーブルで、CIMとKX IIIのサーバーポートを接続 します。
- F. カスケード接続(オプション)

「Configuring and Enabling Tiering」をご参照ください。

G: モデムポート(オプション)

ラリタン・ジャパンは、KX III対応モデムである SierraWireless モ デムを販売しておりません。

H: Dominion シリアルアクセスモジュール(オプション)

KX IIIとDominionシリアルアクセスモジュール(DSAM)を接続 すると、スイッチやルーター等のシリアルデバイスへアクセスで きます。

- DSAMユニットのUSBケーブルをKX IIIのUSBポートに接続します。最大で2台までのDSAMを接続できますが、USBデバイスの接続数が限られているので、接続構成にはご注意ください。
- 2. シリアルデバイスとDSAMを接続します。

Step 4: KX IIIの設定

以下の手順において、ローカルコンソールで初期パスワードを変更 し、KX IIIにIPアドレスを割り当てます。その後の全ての操作は、 ローカルコンソール、もしくはKX IIIにWebブラウザ経由でアクセ スして行います。

初回ログイン時のパスワード変更

KX IIIの工場出荷時の設定は、以下になります。初回ログイン時に、 パスワードをStrong password (複雑なパスワード) へ変更します。

- ユーザー名= admin
- パスワード= raritan
- IPアドレス = 192.168.0.192

重要: 管理者権限を持つバックアップユーザーを作成し、その情 報を厳重に管理することによって、管理者パスワード紛失による トラブルを防ぐ事ができます。

KX IIIのデバイスの設定

KX IIIリモートクライアントで Device Settings > Network (デバイス設定 > ネットワーク) ページを開きます。

Basic Network Settings Device Name * Name IPv4 Address IP Address Subnet Mask 192.168.61.160 Default Gateway 192.168.61.126

- 任意のデバイス名を指定します。最大32文字の英数字と一部の特殊文字 を組み合わせて使用できます。スペースは利用不可です。
- IPアドレスとDefault Gateway, Subnet Maskを設定します。

Failover もしくは Isolation Modeの選択

Failover Modeの設定 (ページ 3) Isolation Modeの設定 (ページ 4)

Failover Mode の設定

LAN1とLAN2は、同じIPアドレスを共有し、自動フェイルオーバ ーをサポートします。LAN1がプライマリポートとして動作し、 LAN1が利用できなくなると、LAN2がアクティブとなります。

- Device Settings > Network から Basic Network Settings を開きます。
- 2. IPv4 Address セクション内の IP Auto Configuration を「None」に 設定します。
- LAN Interface Settings セクションの「Enable Automatic Failover」にチェックを入れます。
- 4. Default Gateway を入力します。
- 5. IPv4 IP Address を入力します。 (初期値:192.168.0.192)
- IPv4 Subnet Mask を入力します。 (初期値:255.255.255.0)

nd of **Diegrar**

7. フェイルオーバー時、LAN1の設定はLAN2に適用されます。



- 8. 必要に応じて IPv6 Address セクションを設定します。
- 9. IP Auto Configuration を選択します。

「None」が選択されている場合は以下の設定が必要です。

- Global/Unique IP Address
- . Prefix Length
- Gateway IP Address.

Link-Local subnetの代わりに Global もしくは Unique IPv6 address を検索するためには「Router Discovery」 を選択します。これにより、アドレスが自動で適用され ます。なお、このセクションには、以下の読み取り専用 の追加情報が表示されます。

- Link-Local IP Address .
- Zone ID
- 10. "Use the Following DNS Server Addresses" を選択して、 「Primary DNS Server IP Address」と「Secondary DNS

Server IP Address」を入力します。

注: Obtain DNS Server Address Automatically, Preferred DHCP Host Name は、DHCP環境でのみ利用可能です。

30-137		
Obtain DNS Se	rver Address Automatically	
Use the Follow	ving DNS Server Addresses	
Primary DNS Serv	ver IP Address	
Secondary DNS S	erver IP Address	

OK Reset To Defaults Cancel

11. LAN 1/LAN 2 Interface のSpeed & Duplex、MTU を設定し

ます。

- MTUの設定範囲は 576 1500 です。
- 12. 「OK」をクリックして、Failover modeのネットワーク設 定は完了です。

Isolation Mode の設定

Isolation modeは、異なるIPアドレスを各LANポートに割り当て てアクセスします。なお、このモードでは、フェイルオーバー機 能はサポートしません。

- 1. Device Settings > Network から Basic Network Settings を開きます。
- 2. IPv4 Address セクション内の IP Auto Configuration を「None」に 設定します。
- 3. LAN Interface Settings セクションの「Enable

Automatic Failover」にチェックが入っていない事を確 認します。

Current LAN Interface Parameters:

autonegotiation on, 1000 Mbps, full duplex, link ok

LAN Interface	Spee	d & Duplex
Autodetect	~	
LAN1 MTU		
1500		

Current LAN2 Interface Parameters: autonegotiation on, 10 Mbps, half duplex, no link

LAN2 Interfac	ce Spee	ed & Dupl	ex
Autodetect	\sim		
LAN2 MTU			
1500			
Enable A	utomati	c Failover	

- 4. Default Gateway を入力します。
- 5. IPv4 IP Address を入力します。 (初期値:192.168.0.192)
- 6. IPv4 Subnet Mask を入力します。 (初期値:255.255.255.0)
- 7. LAN2 IPv4 Address セクション内の IP Auto Configuration を 「None」に設定します。
- 8. LAN2 IPv4 Address セクション内の IP Address を入力し ます。



9. LAN2 IPv4 の Subnet Mask と Default Gateway を入力します。

Basic Network Settings	
Davias Name *	
DominionDevice	注: 0
Pv4 Address	
IP Address Subnet Mask	Obt
Default Gateway IP Auto Configuration	Prima
192.106.01.120 None V	192.10 Secon
IPv6 Address	192.1
Global/Unique IP Address Prefix Length	12. LAN 1,
Gateway IP Address	ます。
Link-Local IP Address Zone ID	■ MT 13. 「OK」
IP Auto Configuration	KX III
	ターゲット
LAN2 IPv4 Address	全てのター
192.168.61.105 255.255.255.0	Configurat
Default GatewayIP Auto Configuration192.168.61.126None	リックしま
	Port 1 Type: Dual-VM

- 10. 必要に応じて IPv6 Address セクションを設定します。
- 11. IP Auto Configuration を選択します。

「None」が選択されている場合は以下の設定が必要です。

- Global/Unique IP Address
- Prefix Length
- Gateway IP Address.

Link-Local subnetの代わりに Global もしくは Unique IPv6 address を検索するためには「*Router Discovery*」を選択します。 これにより、アドレスが自動で適用されます。なお、このセクシ ョンには、以下の読み取り専用の追加情報が表示されます。

- Link-Local IP Address
- Zone ID

"Use the Following DNS Server Addresses" を選択して、「Primary DNS Server IP Address」と「Secondary DNS Server IP Address」を入力します。

注: Obtain DNS Server Address Automatically, Preferred DHCP Host Name は、DHCP環境でのみ利用可能です。

Obtain DNS Server Address Automatically	
Use the Following DNS Server Addresses –	
Primary DNS Server IP Address	
192.168.55.100	
Secondary DNS Server IP Address	-

192.168.55.101

- 12. LAN 1/LAN 2 Interface のSpeed & Duplex、MTU を設定し ます。
 - MTUの設定範囲は 576 1500 です。
- 13. 「OK」をクリックして完了します。

KX III は、LAN1とLAN2のそれぞれからアクセスできます。

ターゲットサーバーの名称設定

全てのターゲットサーバーを接続し、Device Settings > Port Configuration から、名前を設定したいターゲットサーバーのポート名をク リックします。

Type: Dual-VM	Sub Type:	 Standard KVM Port Blade Chassis KVM Switch
Name:		\sim

名前は最大32文字の英数字と一部の特殊文字を利用して入力できます。

電源の自動検出設定

KX III は電源が二重化されており、両方の電源が使用されている場合は、そ れぞれのステータスが通知されます。また、初期状態で Power Supply Setup の「PowerIn1 Auto Detect」と「PowerIn2 Auto Detect」のチェ ックボックスがどちらも自動的にオンになります。1つの電源しか使用して いない場合、使用されている電源のみの自動検出を有効にすることができま す。KX IIIの前面の電源LEDは、1つだけ電源入力が接続されている場合、 接続されていない電源のチェックボックスがオンになっていると赤色で点灯 し、接続されていない電源のチェックボックスがオフになっていると青色で 点灯します。



▶ 電源の自動検出設定は以下を参照してください。



- 1. Device Settings > Power Supply Setup を選択します。
 - 電源1を使用している場合「PowerIn1 Auto Detect」を選 択します。(背面左端が電源1)

※電源2の場合

PowerIn1 Auto Detect		
PowerIn2 Auto Detect		
OK Reset To Defaults	Cancel	
2)		

- 電源2を使用している場合「Powerln2 Auto Detect」を選 択します。(背面左端から2つ目が電源2)
- 2. 「OK」をクリックします。

日付と時刻の設定

LDAPSを利用中の場合、日付と時刻の設定がSSL証明書の検証に影響 します。日付と時刻を正しく設定すると、Audit log (監査ログ) に記 録されるタイムスタンプは正しくなります。

設定方法は二つ用意されています。

● 手動設定
Date/Time Settings
Time Zone
(GMT-05:00) US Eastern
Adjust for daylight savings time
User Specified Time
Date (Month, Day, Year)
February ▼ 19 , 2019
Time (Hour, Minute)
03 : 22 : 19 (hh:mm:ss)
Synchronize with NTP Server
Primary Time Server
Secondary Time Server
OK Reset To Defaults Cancel
• NTP (Network Time Protocol) サーバーと同期

Date/Time Settings

Time Zone
(GMT -05:00) US Eastern ▼
Adjust for daylight savings time
User Specified Time
Date (Month, Day, Year)February▼19, 2019
Time (Hour, Minute)
03 : 26 : 37 (hh:mm:ss)
Synchronize with NTP Server
Primary Time Server
192.168.22.222
Secondary Time Server
192.168.22.224
OK Reset To Defaults Cancel



▶ 日付と時刻の設定手順

- Device Settings > Date/Time を選択して Date/Time Settings ページを開きます。
- Time Zone の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。
- 夏時間を利用する場合「Adjust for daylight savings time" checkbox」にチェックを入れます(オプション)。
- 4. 日付と時刻の設定方法を選択します。
 - 手動設定 ユーザーが日付と時刻設定をする場合には
 「User Specified Time」を選択して各値を入力します。
 (時刻は24時間制)
 - NTPサーバーと同期 日付と時刻をNTPサーバーと同 期させる場合には「Synchronize with NTP Server」 を選択します。

「Synchronize with NTP Server」設定

- 「Primary Time server」にIPアドレスかホストネームを入力します。
- 「Secondary Time server」はオプションです。

注: DHCP環境では、NTPサーバーのIPアドレスも自動取得され ます。もし、個別に設定したい場合、「Override DHCP」のチ ェックボックスを選択して、NTPサーバーのIPアドレスを入力 します。

5. 「OK」をクリックします。

Step 5: リモートコンソールの起動

- KX IIIでサポートされているWebブラウザを起動して、KX IIIの IPアドレスを入力すると、KVMクライアントが起動します。 KVMクライアントの詳細は、オンラインヘルプを参照してくだ さい。
- 2. ユーザー名とパスワードを入力してログインします。
- 3. User agreementが表示された場合は同意します。
- 4. セキュリティ警告が表示された場合は同意します。

Tip: ユーザーステーションをご利用の場合はページ8、もしくは ユーザーステーションのオンラインヘルプをご参照ください。

- ターゲットサーバーへのリモートアクセスと制御
- 「Port Access」ページは、ポートの一覧とステータス、利用可否を 表示します。

ターゲットサーバーへのアクセス

Port Access

Click on the individual port name to see allowable operations. 0 / 4 Remote KVM channels currently in use.

iew By Port A No.	View By Group View By Search Set Scan Name
1	Dominion_Port1
2 (2)	DP-0 Connect ort13
3	Dominion-KXX_Port3

- 「Port Access」ページで、ターゲットのポート名をクリック すると、 Port Action Menuが表示されます。
- Connect」を選択すると、KVMウインドウが起動して、ターゲットへ 接続します。

```
ターゲットサーバーの切替
```

Port Access - 1 Click on the individual port name to see allowable operations 0 / 4 Remote KVM channels currently in use.

View By Port View By Group A No. Name Switch From Windows Connect 3 Dominion-XCCCPort 2

- 1 ターゲットサーバーへ接続中に「Port Access」ペー ジにアクセスします。
- アクセスするターゲットのポート名をクリックすると
 Port Action menuが表示されます。
- 「Switch From (ポート名)」を選択すると、選
 3
 択したターゲットサーバーが表示されます。

ターゲットサーバーの切断

- ▶ ターゲットサーバーの 接続を終了する手順:
- 「Port Access」ページで終了するターゲットサーバーのポート名をクリックし、Port Action menuから「disconnect」を選択します。
 もしくは、KVMクライアントのウインドウを閉じることによっても、接続を終了できます。

Step 6: キーボード言語の設定

必要に応じて、使用するキーボード言語を設定します(初期値は 英語)。また、クライアントおよびターゲットサーバーのキーボ ード言語も揃える必要があります。 Raritan .

Step 7: SSL証明書の作成とインストール

ご利用になるKX IIIに、SSL証明書をインストールすることを推奨し ます。これにより、WebブラウザやJavaの警告メッセージを減らし、 中間者攻撃 (Man In The Middle Attack) を防ぐことができます。 また、今後リリースされるJavaやWebブラウザがKX IIIへのアクセス を中断する事を防ぎます。

SSL証明書の作成とインストールの詳細は、オンラインヘルプをご参照ください。

バイナリ証明書をBase64エンコードしたDER証明書へ変換する KX IIIは、Base64エンコードのDER形式もしくはPEM形式の SSL証明書をインストールできます。バイナリ形式の場合、KX IIIにインストールできませんので、変換してください。

ow: <all></all>	•	
field	Value	-
Version Serial number	V3 0c e7 e0 e5 17 d8 46 fe 8f e5	=
Signature algorithm	sha 1RSA	-
Signature hash algorithm	sha1	
Issuer	DigiCert Assured ID Root CA,	
Valid from	Thursday, November 09, 2006	
Valid to	Sunday, November 09, 2031 7	
Subject	DiniCert Assured ID Root CA	4
	3 Edit Properties Copy to File	

- Windowsクライアント上で、cer拡張子のバイナリファイルをダ ブルクリックして、証明書ダイアログを開きます。
- 2. 「Details (詳細)」タブをクリックします。
- 3. 「Copy to File... (ファイルにコピー)」をクリックします。
- Certificate Export Wizard (証明書のエクスポート ウィザ ード) が開くので、「Next (次へ)」 をクリックします。
- 5. 「Base-64 encoded X.509」を選択します

Expo (rt File Format Lertificates can be exported in a variety of file formats.
s	select the format you want to use:
	© DER encoded binary X.509 (.CER)
-	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Indude all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Microsoft Serialized Certificate Store (.SST)
Learn	more about <u>certificate file formats</u>

6. 「Next (次へ)」をクリックしてファイル名を設定して

保存します。

その後、新しく生成された証明書をKX IIIヘインストール

します。

Dominion ユーザーステーション

エンドユーザーは、KX IIIへWebブラウザを介したリモートアクセ スのほか、スタンドアロン・アプライアンス製品であるDominion ユーザーステーション (DKX3-UST, DKX4-UST) を利用することが 可能です。ユーザーステーションは、Raritanから購入することがで きます。



エンドユーザーは、1台のユーザーステーションから複数のKX III に接続されたターゲットサーバーにLAN/WANを介してアクセスす ることができ、高速に切り替えることが可能です。

ユーザーステーションの詳細につきましては、ラリタン・ジャパン のWebサイトのサポートページに用意されたオンラインドキュメ ントをご参照ください。

[ラリタン・ジャパン サポートページ]

https://www.raritan.com/jp/support/product/dominion-kxuser-station

その他

KX IIIおよびRaritanの全ての製品については、RaritanのWebサイトをご参照 ください。また、技術的なお問合せにつきましては、Raritanテクニカルサポ ートへお問合せください。日本のテクニカルサポートへの連絡につきましては、 RaritanのサポートWeb (<u>https://www.raritan.com/jp/support</u>) をご参照く ださい。

Raritanの製品は、GPLおよびLGPLに基づいてライセンスされたコードを使 用しています。オープンソースコードのコピーは、Raritanに要求することが 可能です。詳細については、RaritanのWebサイトにあるオープンソースソフ トウェアに関する記述をご参照ください。

[Open Source Software Statement]

http://www.raritan.com/about/legal-statements/open-sourcesoftware-statement/