# Raritan.

## Dominion® LX II

DLX2-108	DLX2-108-LED
DLX2-116	DLX2-116-LED
DLX2-216	DLX2-216-LED

# クイックセットアップガイド



このたびは Dominion LX II/Dominion LEDドロワー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、LX IIの初期設定についてご説明します。DLX2は、KVM-over-IPスイッチとLEDドロワーー体型の2タイプが用意され、 1~2のリモートユーザーと1つのローカルアクセスによる最大16台までのサーバー制御を提供します。また、仮想メディア、ずれないマウス、AD認証、 PC SHARE等のエンタープライズ向けKVM-over-IPの機能についても一部サポートします。また、オプションで用意されたDSAMを使用することにより、シリアル デバイスへのアクセスも提供します。

#### 内容物一覧

- ▶ KVM-over-IP単体モデル: DLX2-108, DLX2-116, DLX2-216
- LX II本体
- ラックマウントキット
- AC電源コード
- デスクトップ設置用ゴム足(4つ)
- ▶ LEDドロワーー体型モデル: DLX2-108-LED, DLX2-116-LED, DLX2-216-LED
- LEDドロワー本体
- ラックマウントキット(スライドレール含む)
- AC電源コード
- 管理者ガイドに記載されたLX IIの動作温度範囲から逸脱しない環境で ご利用ください。
- 適切なエアフローを確保した環境でご利用ください。
- 不均一な機械的負荷を避けるため、LX II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、LX II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 - DLX2-108, DLX2-116, DLX2-216

LX IIのKVM-over-IP単体モデルは、標準的な19インチサーバーラックの1U (44mm)の垂直スペースを利用して、ラックの前面もしくは背面に取り付け ることが可能です。取付には、同梱されているラックマウントキットをご利用 ください。 **ラック前面への取付 - DLX2-108, DLX2-116, DLX2-216** 図の番号と手順番号が対応しています。



- 付属している2本のネジを使用して、ケーブルサポートバーを側 面ブラケットの後端に固定します。
- LX IIの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、前面パネルが側面ブラケットの「耳」と揃うように調整します。
- 3. 付属しているネジを使用して、LX IIの両側(片側3本ずつ)を側 面ブラケットに固定します。
- サーバーラックの前面にラック専用のネジ・ボルト・ケージナットで側 面ブラケットの耳を固定します。
- 5. LX II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を通します。

Raritan.

ラック背面への取付 - DLX2-108, DLX2-116, DLX2-216

図の番号と手順番号が対応しています。



- 付属している2本のネジを使用して、ケーブルサポートバーを側 面ブラケットの前端(ブラケットの「耳」付近)に固定します。
- LX IIの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、前面パネルが側面ブラケットの後端に揃うように調整します。
- 3. 付属しているネジを使用して、LX IIの両側(片側3本ずつ)を側 面ブラケットに固定します。
- サーバーラックの前面にラック専用のネジ・ボルト・ケージナットで側 面ブラケットの耳を固定します。
- 5. LX II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を通しま す。

#### ラックマウント- DLX2-108-LED, DLX2-116-LED, DLX2-216-LED

 サーバーラックの奥行に合わせてブラケットの長さを調整します。ブラ ケットには、ラック前方の目印となるラベルが貼付されています。



ブラケットは以下のように左右対称となります。



サーバーラックに対応したネジおよびケージナット使用して、ブラケットをラックレールに緩みがないように固定します。



3. ブラケットの間にLX IIをスライドさせてサーバーラックに搭載します。



4. ネジを使用してLX IIをサーバーラックに固定します。



### Step 1: Firewallの設定

- TCP Port 5000: リモートアクセスで許可します。
- TCP Port 443: WebによるHTTPSアクセスを許可します。
- TCP Port 80: WebによるHTTPアクセスを許可します。

Step 2: ターゲットサーバーの設定

#### 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、仮想メディアに対応したCIMでサポートされる機能です。

 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/lx-ii/v3.1.0/en/#32872.htm)



Step 3: 機器の接続

▶ KVM-over-IP単体モデル: DLX2-108, DLX2-116, DLX2-216



▶ LEDドロワーー体型モデル: DLX2-108-LED, DLX2-116-LED, DLX2-216-LED



#### A. AC電源

• 添付されている電源コードを使用して、ACコンセントに差し込みます。

#### B: KVM-over-IP単体モデルのUSBおよびLocalポート

- マルチシンクVGAモニター、USBマウス/キーボードを接続します。
  注:LEDドロワーー体型モデルにVGAポートは用意されておりません。
- C: LANポート
- EthernetケーブルをLANポートへ接続してネットワークに参加します。
- D: ターゲットサーバーポート
- CIMのUSBおよびビデオポートをターゲットサーバーの各対応ポート に接続します。
- 2. Cat5/5e/6ケーブルでCIMとLX IIのターゲットサーバーポートを接続します。

#### E: Modemポート (オプション)

日本市場では、LX II対応モデムSierra Wirelessの販売をしておりません。

F: 電源スイッチ (LEDドロワーー体型モデルのみ)

ON/OFFスイッチでLEDスクリーンの表示を操作します。

#### Step 4: LX IIの初期設定

初期設定では、工場出荷時のパスワードを変更し、ローカルコンソールでLX II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、 もしくはリモートアクセスで行います。

#### 初回ログイン時のパスワード変更

LX IIの工場出荷時設定は、以下になります。初回ログイン時に、パスワード を変更する必要があり、最大64文字の英数字と特殊文字を使用できます。

- 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ことができ ます。

\_\_\_\_\_



#### デバイス名の設定

リモートクライアントから Device Settings > Network を選択して「Basic Network Settings」ページを開きます。

#### Basic Network Settings

#### Device Name \*





- LX IIに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。スペースは使用不可です。
- IPアドレスとサブネットマスクとデフォルトゲートウェイを設定します。

#### ネットワーク設定: IPv4 および IPv6 設定

- 1. IPv4設定において「IP Auto Configuration」を「None」にします。
- 2. 初期設定IPアドレス (192.168.0.192) から任意の値に変更します。
- サブネットマスク (初期値: 255.255.255.0) を任意の値に変更 します。
- 4. 必要に応じてIPv6設定の変更を行ないます。
- 5. IP Auto Configurationを「None」にした場合、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または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。 7. 「OK」をクリックして、ネットワーク設定は完了です。

#### ターゲットサーバーの名称設定

- 1. 全てのターゲットサーバーをLX IIに接続します。
- Device Settings > Port Configurationから、名前を設定したターゲッ トサーバーのポート名をクリックします。

#### Port 2

Type: Sub Type: Standard KVM Port DVM-DP KVM Switch Name:



3. 名称は最大32文字の英数字と一部の特殊文字を利用できます。

#### 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。設定補法は2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,
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 (Mo	ont	th, D	ay, ۱	/ea	ar)		
Februar	y	V	19		, ,	2019	)
Time (Ho	bu	r, Miı	nute	)			
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

- 1. Device Settings > Date/Time を選択します。
- 2. 任意のTime Zone をドロップダウンリストから選択します。
- 夏時間を利用する場合は「Adjust for daylight savings time」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、任意の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

- LX IIでサポートされているWebブラウザを起動して、LX II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 詳細については、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「Accept (同意)」します。
- 4. セキュリティ警告が表示された場合は「Accept (同意)」します。

#### ターゲットサーバーへのリモートアクセス

Port Accessには、LX IIの全てのポートリストが表示されます。このリストには、ター ゲットサーバーのステータスと利用可否も表示されます。

#### Port Access

•

Click on the individual port name to see allowable operations. 0 / 2 Remote KVM channels currently in use.

#### View By Port Set Scan ▲ No. Status Туре Availabi Connect minion\_LX2\_Port1 VM up idle Dominion\_LX2\_Port2 Not Available idle 2 down Dominion\_LX2\_Port3 Not Available idle 3 down

- 「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。
- 2. 「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

Click on the individual port name to see allowable operations. 1 / 2 Remote KVM channels currently in use.

View By Port	Set Scan	3		
Switch Fro	m Dominion_LX2_Por	Туре	Status	Availability
Connect		VM	up	busy
2	Openinion_LX2_Port2	DVM-DP	up	idle
3	Dominion_LX2_Port3	Not Available	down	idle
4	Dominion_LX2_Port4	Not Available	down	idle

- 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。
- 2 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。
- 3 「Switch From (ポート名)」を選択すると、選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からの切断

#### 接続の終了手順

「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、クライアントと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。

#### Step 7: SSL証明書の作成とインストール

ご利用になるLX II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LX II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

LX II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、LX IIにインストールできませんので、 変換してください。

#### バイナリ形式のSSL証明書を変換する手順

Field	Value
Version Serial number	V3 0c e7 e0 e5 17 d8 46 fe 8f e5
Signature algorithm	sha1RSA
Issuer	DigiCert Assured ID Root CA,
Valid from	Thursday, November 09, 2006
Valid to	Sunday, November 09, 2031 7
Subject	DiniCert Assured TD Root CA
am more about certificate data	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



X



 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。

Exp	Export File Format Certificates can be exported in a variety of file formats.		
	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 (.P7B)		
	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)		
Lear	n more about <u>certificate file formats</u>		

- 5. 「Base-64 encoded X.509」を選択します。
- 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LX IIにインストールします。

#### その他

LX II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-source-software-statement/