ThinkSystem SE350 および ThinkSystem SE350 エンクロージャー

セットアップ・ガイド

マシン・タイプ: 7Z46、7D1X、7D27 および 7D1R

注

本書および本書で紹介する製品をご使用になる前に、以下に記載されている安全情報および安全上の注意を読んで理解してください。
https://pubs.lenovo.com/safety_documentation/

さらに、ご使用のサーバーに適用される Lenovo 保証規定の諸条件をよく理解してください。以下に掲載されています。
http://datacentersupport.lenovo.com/warrantylookup

第 34 版 (2022 年 11 月)

© Copyright Lenovo 2019, 2022.

制限付き権利に関する通知: データまたはソフトウェアが GSA (米国一般調達局) 契約に準じて提供される場合、使用、複製、または開示は契約番号 GS-35F-05925 に規定された制限に従うものとします。

目次

目次 i

安全について iii

安全検査のチェックリスト iv

第 1 章 . 概要 1

サーバーのパッケージ内容 1

機能 2

仕様 3

衝撃および振動の仕様 12

粒子汚染 12

管理オプション 13

第 2 章 . サーバー・コンポーネント . . 17

前面図 18

前面オペレーター・パネル 20

背面図 21

システム・ボード・コネクター 23

LOM パッケージ 24

PCIe ライザー・アセンブリー 26

M.2 ドライブおよびスロットの番号 27

部品リスト 29

電源コード 34

第 3 章 . サーバーのハードウェアのセットアップ 35

サーバー・セットアップ・チェックリスト . . . 35

取り付けのガイドライン 36

システムの信頼性に関するガイドライン . . 37

電源オンされているサーバーの内部での作業 38

静電気の影響を受けやすいデバイスの取り扱い 38

メモリー・モジュールの取り付けの規則および順序 38

サーバー・ハードウェア・オプションの取り付け 39

ノードの取り外し 40

トップ・カバーの取り外し 43

エアー・バッフルの取り外し 45

PCIe ライザー・アセンブリーの取り外し . . 46

前面オペレーター・パネルの取り外し . . . 48

ロック位置スイッチの取り外し 49

侵入検出スイッチ・ケーブルの取り外し . . 50

電源アダプターの取り付け 52

M.2 ブート・アダプターの取り付け 56

M.2 データ・アダプターの取り付け 57

M.2 WLAN/LTE ワイヤレス・アダプターの取り付け 60

SIM カードの取り付け 61

PCIe アダプターの取り付け 63

PCIe ライザー・アセンブリーの取り付け . . 64

侵入検出スイッチ・ケーブルの取り付け . . 66

DIMM の取り付け 68

前面オペレーター・パネルの取り付け . . . 69

ロック位置スイッチの取り付け 70

エアー・バッフルの取り付け 72

トップ・カバーの取り付け 73

ノードの取り付け 74

ラックへのサーバーの取り付け 77

サーバーの配線 78

サーバーの電源をオンにする 78

サーバーのセットアップの検証 78

サーバーの電源をオフにする 78

第 4 章 . システム構成 81

システムをアクティブにする 81

ロックダウン・モードと動作検出 83

自己暗号化ドライブ認証キー (SED AK) のバックアップ 83

Lenovo XClarity Controller のネットワーク接続の設定 83

ファームウェアの更新 84

ファームウェアの構成 89

メモリー構成 90

RAID 構成 90

ワイヤレス対応 LOM パッケージ構成 91

ワイヤレス対応 LOM パッケージ・プリセット 94

ワイヤレス LOM パッケージ構成の組み込みスイッチ CLI 101

ファイアウォール設定 115

OpenVPN クライアントの設定 126

オペレーティング・システムのデプロイ 127

サーバー構成のバックアップ 128

重要プロダクト・データ (VPD) の更新 128

Universal Unique Identifier (UUID) の更新 . . . 128

資産タグの更新 130

第 5 章 . インストールに関する問題の解決 133

付録 A. ヘルプおよび技術サポートの入手 137

依頼する前に 137

© Copyright Lenovo 2019, 2022

サービス・データの収集 138
サポートへのお問い合わせ 139

索引 141

安全について

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 Safety Information （安全信息）。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

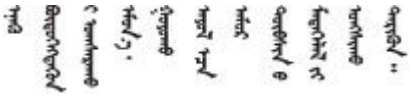
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.



Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

© Copyright Lenovo 2019, 2022

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྒྲིག་མ་བྱས་གོང་། ཁྱོད་ཀྱི་ཡིད་གཟབ་
བྱ་འདྲ་མིན་ཡོད་པའི་བོད་སྐོར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen canjbinj soengq cungj vahgangj ancien siusik.

安全検査のチェックリスト

サーバーで危険をもたらす可能性のある状況を識別するには、このセクションの情報を使用します。各マシンには、設計され構築された時点で、ユーザーとサービス技術員を障害から保護するために義務づけられている安全装置が取り付けられています。

注：

1. この製品は、職場規則の §2 に従って、視覚的なディスプレイ作業場での使用には適していません。
2. サーバーのセットアップは、サーバー・ルームでのみ行います。

警告：
この装置は、NEC、IEC 62368-1 および IEC 60950-1、および電子機器 (オーディオ/ビデオ、情報および通信テクノロジ分野に属するもの) の安全基準に定められているように、訓練を受けた担当員のみが設置および保守できます。Lenovo では、お客様が装置の保守を行う資格を持っており、製品の危険エネルギー・レベルを認識する訓練を受けていることを想定しています。装置へのアクセスにはツール、ロック、鍵、またはその他のセキュリティー手段を使用して行われ、その場所に責任を持つ認証機関によって制御されます。

重要：オペレーターの安全確保とシステム機能の正常実行のためには、サーバーの接地が必要です。電源コンセントの適切な接地は、認定電気技術員により検証できます。

危険をもたらす可能性のある状況がないことを確認するには、次のチェックリストを使用します。

1. 電源がオフになっていて、電源コードが切断されていることを確認します。
2. 電源コードを検査します。
   - 接地線を含む 3 線式の電源コードのコネクターが良好な状態であるかどうか。3 線式接地線の導通が、外部接地ピンとフレーム・アース間を計器で測定して、0.1 オーム以下であることを確認します。
   - 電源コードが、正しいタイプのものであるか。

     サーバーで使用できる電源コードを参照するには、次のようにします。

     a. 以下へ進んでください。

http://dcsc.lenovo.com/#/

b. 「**Preconfigured Model (事前構成モデル)**」または「**Configure to order (注文構成製品)**」をクリックします。

c. コンフィギュレーター・ページを表示するサーバーのマシン・タイプとモデルを入力します。

d. すべての電源コードを表示するには、「**Power (電源)**」 → 「**Power Cables (電源ケーブル)**」をクリックします。

- 絶縁体が擦り切れたり摩耗していないか。

3. 明らかに Lenovo によるものでない改造個所をチェック します。Lenovo 以外の改造個所の安全については適切な判断を行ってください。
4. 金属のやすりくず、汚れ、水やその他の液体、あるいは火災や煙による損傷の兆候など、明らかに危険な状態でないか、サーバーの内部をチェックします。
5. 磨耗したケーブル、擦り切れたケーブル、または何かではさまれているケーブルがないかをチェックします。
6. パワー・サプライ・カバーの留め金具 (ねじまたはリベット) が取り外されたり、不正な変更がされていないことを確認します。

© Copyright Lenovo 2019, 2022

第 1 章　概要

この ThinkSystem SE350 は、新しいエッジ・サーバー製品です。IoT やエッジにおけるニーズを満たすように特別に設計されています。ThinkSystem SE350 は、スマートな接続性、ビジネスのセキュリティー、過酷な環境での管理性を重視したコンパクトなサイズのエッジ・ソリューションです。エッジにおける要求の厳しい IoT ワークロードをサポートするため、長持ちして信頼できるパフォーマンスを実現するように構築されています。非データ・センター環境向けにコンパクトに設計されており、小売店、製造現場、工場などのリモートの場所に最適です。

注：*セキュリティー・パック付きの SE350* は、2021 年 7 月より前は単に *SE350* と呼ばれていました。

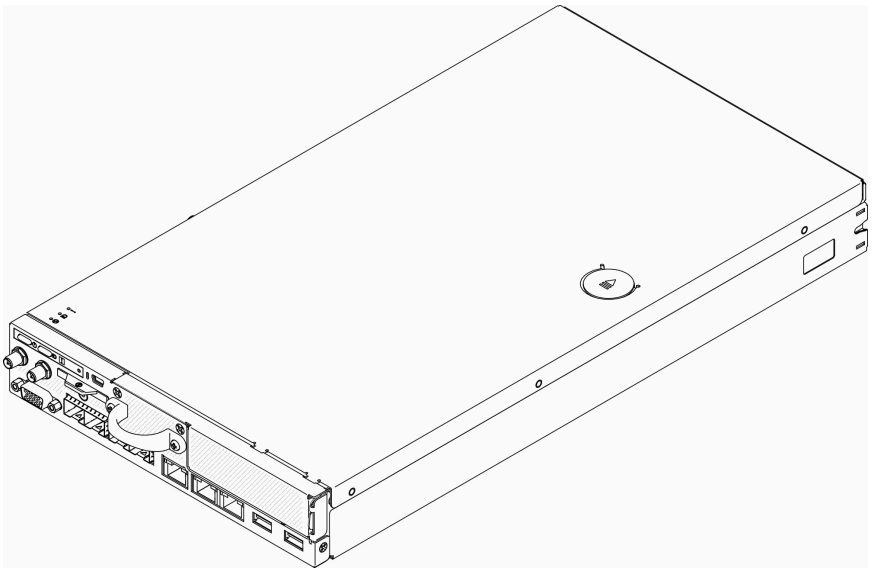


図 1. ThinkSystem SE350

このサーバーには限定保証が適用されます。保証に関する詳細については、次を参照してください。
https://support.lenovo.com/us/en/solutions/ht503310

お客様固有の保証に関する詳細については、次を参照してください。
http://datacentersupport.lenovo.com/warrantylookup

サーバーのパッケージ内容

サーバーを受け取ったら、受け取るべきものがすべて含まれていることを確認します。

サーバー・パッケージには、以下の品目が含まれます。

注：リストされている項目の一部は、一部のモデルでのみ使用できます。

- サーバー
- レール取り付けキット (オプション)。レールの取り付けキットを取り付けるための詳細な手順は、レールの取り付けキットにパッケージで同梱されています。
- 資料ボックス (電源コード、ラック取り付けテンプレート、アクセサリー・キットなどが同梱)

© Copyright Lenovo 2019, 2022

機能

サーバーの設計においては、パフォーマンス、使いやすさ、信頼性、および拡張機能などが重要な考慮事項でした。これらの設計機能を用いることで、現在のニーズに応じてシステム・ハードウェアをカスタマイズしたり、将来に備えて柔軟性の高い機能拡張を準備したりすることができます。

サーバーは、次の機能とテクノロジーを実装しています。

- **Features on Demand**

  サーバーまたはサーバー内に取り付けたオプション・デバイスに Features on Demand 機能が組み込まれている場合、アクティベーション・キーを注文して機能をアクティブ化することができます。Features on Demand の詳細については、以下を参照してください。

  https://fod.lenovo.com/lkms

- **Lenovo XClarity Controller (XCC)**

  Lenovo XClarity Controller は、Lenovo ThinkSystem サーバー・ハードウェア用の共通管理コントローラーです。Lenovo XClarity Controller は、複数の管理機能を、サーバーのシステム・ボードにある単一のチップに統合します。

  Lenovo XClarity Controller に固有の機能として、パフォーマンスの改善、リモート・ビデオの解像度の向上、およびセキュリティー・オプションの強化が挙げられます。Lenovo XClarity Controller に関する追加情報については、以下にあるご使用のサーバーと互換性のある XCC に関する資料を参照してください。

  https://pubs.lenovo.com/lxcc-overview/

  重要：Lenovo XClarity Controller (XCC) でサポートされるバージョンは、製品によって異なります。本書では、特に指定がない限り、 Lenovo XClarity Controller のすべてのバージョンを Lenovo XClarity Controller および XCC と記載します。ご使用のサーバーでサポートされる XCC バージョンを確認するには、https://pubs.lenovo.com/lxcc-overview/ にアクセスしてください。

- **UEFI 準拠のサーバー・ファームウェア**

  Lenovo ThinkSystem ファームウェアは、Unified Extensible Firmware Interface (UEFI) に対応しています。UEFI は、BIOS に代わるものであり、オペレーティング・システム、プラットフォーム・ファームウェア、外部デバイス間の標準インターフェースを定義します。

  Lenovo ThinkSystem サーバーは、UEFI 準拠オペレーティング・システム、BIOS ベースのオペレーティング・システム、および BIOS ベースのアダプターのほか、UEFI 準拠アダプターをブートすることができます。

  注：このサーバーでは、ディスク・オペレーティング・システム (DOS) はサポートされていません。

- **大容量のシステム・メモリー**

  サーバーは、エラー訂正コード (ECC) 付きの SDRAM registered デュアル・インライン・メモリー・モジュール (RDIMM) をサポートします。固有のメモリーのタイプおよび最大容量について詳しくは、3 ページの 「仕様」を参照してください。

- **内蔵ネットワーク・サポート**

  サーバーのオプション・パッケージには、10G SFP+ LOM パッケージまたはワイヤレス対応 LOM パッケージの 2 つのパッケージがあります。選択したパッケージに応じて、10Gb SFP+ コネクター、10/100MB/1Gb 銅線、WLAN 機能を使用できます。

- **内蔵 Trusted Platform Module (TPM)**

  この内蔵セキュリティー・チップは、暗号機能を実行し、セキュアな秘密鍵と公開鍵を保管します。これは Trusted Computing Group (TCG) 仕様に対するハードウェア・サポートを提供します。TCG 仕様をサポートするためのソフトウェアをダウンロードできます。

  TPM 構成の詳細については、「*メンテナンス・マニュアル*」の「TPM の有効化」を参照してください。

注：中国本土のお客様は、Lenovo が認定した TPM 2.0 アダプターまたは TPM カードが事前に取り付けられていることがあります。

- **大きいデータ・ストレージ容量**

  サーバーは、最大 8 台の M.2 NVMe ドライブをサポートします。

- **前面オペレーター・パネル**

  前面オペレーター・パネルは、問題の診断に役立つ LED を提供します。前面オペレーター・パネルの詳細については、20 ページの「前面オペレーター・パネル」を参照してください。

- **Lenovo Service Information Web サイトへのモバイル・アクセス**

  サーバーには、サーバーのカバーにあるシステム・サービス・ラベルに QR コードが記載されています。モバイル・デバイスの QR コード・リーダーとスキャナーを使用してこのコードをスキャンすると、Lenovo Service Information Web サイトにすぐにアクセスすることができます。Lenovo Service Information Web サイトでは、追加情報として部品の取り付けや交換用のビデオ、およびサーバー・サポートのためのエラー・コードが提供されます。

- **Active Energy Manager**

  Lenovo XClarity Energy Manager は、データ・センターの電源および温度管理ソリューションで使用するツールです。コンバージド、NeXtScale、System x、および ThinkServer サーバーを使用して、の電力使用量と温度を監視および管理し、Lenovo XClarity Energy Manager を使用してエネルギー効率を向上させることができます。

- **リダンダント冷却およびオプションの電源機能**

  サーバーは最大 2 個の 240 ワット・ホット・スワップ電源アダプターおよび 3 個の内蔵ファンをサポートします。これらにより、標準的な構成に対して冗長性が提供されます。サーバー内のファンのリダンダント冷却により、ファンの 1 つに障害が起きても、サーバーの操作を続行できます。

- **ThinkSystem RAID のサポート**

  ThinkSystem RAID アダプターは、構成を形成するためのハードウェア RAID (新磁気ディスク制御機構) サポートを提供します。ソフトウェア RAID コントローラーは、RAID レベル 0、1、5、10 をサポートしています。

仕様

以下は、ご使用のサーバーの機能と仕様を要約したものです。ご使用のモデルによっては、使用できない機能があったり、一部の仕様が該当しない場合があります。

表 1. サーバー仕様

仕様	説明
セキュリティー・オプション (モデルによって異なる)	• セキュリティー・バック付きの SE350 – SE350 の自動データ保護 (侵入検出センサーや動作検出センサーを含む) を有効にできます。 – 不正のイベントで SED のデータへのアクセスをロックできます。 – データのロックを解除してアクセスするために、システムを登録してアクティブにする必要があります。 – ブートおよび完全に機能させるには、アクティベーションが必要です。 • 標準の SE350 (セキュリティー・パックが無効) – SE350 の自動データ保護 (侵入検出センサーや動作検出センサーを含む) は無効になっています。 – データへのアクセスはロックされません。SED の管理は無効になっています。不正の設定は無効になっています。 – アクティベーションは不要です。

表 1. サーバー仕様 (続き)

仕様	説明
	– システムの登録は任意です。登録には、セキュア・アクティベーション・コードが必要です。 **注：** • *セキュリティー・パック付きの SE350* は、2021 年 7 月より前は単に *SE350* と呼ばれていました。 • システムがセキュリティー・パック付きの SE350 か標準の SE350 かは、Lenovo XClarity Controller で確認できます。
寸法	ノード • 高さ: 43.2 mm (1.7 インチ) • 幅: 209 mm (8.2 インチ) • 奥行き: 376.1 mm (14.8 インチ) E1 エンクロージャー (1U 2-ノード): • 高さ: 43 mm (1.69 インチ) • 幅: 439.2 mm (17.29 インチ、EIA ブラケットから EIA ブラケットまで) • 奥行き: 773.12 mm (30.44 インチ) • 重量: 10 kg (1 つのノードと 2 個の電源アダプターを使用)、15 kg (4 個の電源アダプターを使用) E2 エンクロージャー (2U 2-ノード): • 高さ: 86.9 mm (3.42 インチ) • 幅: 439.2 mm (17.29 インチ、EIA ブラケットから EIA ブラケットまで) • 奥行き: 476.12 mm (18.74 インチ) • 重量: 10 kg (1 つのノードと 2 個の電源アダプターを使用)、15 kg (4 個の電源アダプターを使用)
重量	ノード • 最大: 3.6 kg (7.9 ポンド)
プロセッサー (モデルによって異なる)	Intel® Xeon® プロセッサー D-2100 製品ファミリー x1 **注：** 1. ノード内のプロセッサーのタイプと速度を判別するには、Setup Utility プログラムを使用します。 2. サポートされるプロセッサーのリストについては、https://serverproven.lenovo.com/server/se350 を参照してください。

表 1. サーバー仕様 (続き)

仕様	説明
メモリー	メモリーの構成およびセットアップについて詳しくは、38 ページの 「メモリー・モジュールの取り付けの規則および順序」を参照してください。 • スロット: DIMM スロット 4 個 • 最小: 8 GB (1 x 8GB RDIMM) • 最大: 256 GB (4 x 64GB LRDIMM) • タイプ: – TruDDR4 2666 MHz RDIMM: 8GB (1Rx8)、16GB (2Rx8)、32GB (2Rx4)、64GB (4Rx4) – TruDDR4 3200 MHz RDIMM: 16GB (2Rx8)、32GB (2Rx4) **注：**サポートされているメモリー・モジュールのリストについては、https://serverproven.lenovo.com/server/se350 を参照してください。
M.2 ドライブ	M.2 ブート・アダプター • 最大 2 台の同一 M.2 SATA ドライブをサポート • M.2 ドライブの 3 種類の物理サイズをサポートします: – 42 mm (2242) – 60 mm (2260) – 80 mm (2280) M.2 データ・アダプター • PCIe および M.2 ライザー・アセンブリー: – 最大 4 台の M.2 SATA/NVMe ドライブをサポート • M.2 ライザー・アセンブリー – 最大 8 台の M.2 NVMe ドライブをサポート – 最大 4 台の NVMe および 4 台の SATA ドライブをサポート • M.2 ドライブの 4 種類の物理サイズをサポートします: – 42 mm (2242) – 60 mm (2260) – 80 mm (2280) – 110 mm (22110) **注：** • ブート・アダプターとデータ・アダプターに取り付けられた M.2 ドライブは、交換できません。 • M.2 コネクター・タイプ: ソケット 3 (M キー) • 同じ M.2 SATA/NVMe 4 ベイ・データ・アダプターでの SATA ドライブと NVMe ドライブの混在はサポートされていません。
PCIe ライザー・アセンブリー	PCIe および M.2 ライザー・アセンブリー: • スロット 6: PCI Express 3.0 x16 (75W 未満、ロー・プロファイル、ハーフハイト、ハーフサイズ PCIe アダプターをサポート)

表 1. サーバー仕様 (続き)

仕様	説明
WLAN	• WLAN: IEEE 802.11 a/b/g/n/ac • MIMO: 2x2 MIMO • インターフェース: WLAN: PCIe x1 • アンテナ構成: 2xIPEX (MHF4) コネクター • フォーム・ファクター: M.2 2230 • 同時ユーザー接続の最大数 (AP モード): 8 • セキュリティー: – AP モードは WPA2 パーソナルをサポート – ステーション・モードは WPA2 エンタープライズおよび WPA2 パーソナルの両方をサポート • 動作バンド: – AP モード: 2.4 GHz – ステーション・モード: 2.4 GHz/5 GHz **注：** • WLAN のパフォーマンスは、構成や環境によって異なります。 • ラックやキャビネットに取り付けると、無線信号の品質に影響する場合があります。
LTE	• 3GPP リリース 11 • カテゴリー: Cat9 • リージョン: グローバル • オペレーティング・モード: FDD/TDD • データ転送: 最大 450Mbps DL/50Mbps UL • 機能インターフェース: USB 3.0 • アンテナ構成: 2xIPEX (MHF4) コネクター • フォーム・ファクター: M.2 3042 **注：** • LTE のパフォーマンスは、構成や環境によって異なります。 • ラックやキャビネットに取り付けると、無線信号の品質に影響する場合があります。
内蔵機能	• Lenovo XClarity Controller。サービス・プロセッサーの制御および監視機能、ビデオ・コントローラー、およびリモート・キーボード、ビデオ、マウス、ならびにリモート・ハードディスク・ドライブ機能を提供します。 • 前面オペレーター・パネル • LOM モジュール・コネクター (サーバー前面): – 10G SFP+ LOM パッケージ – USB 3.1 Gen 1 コネクター 2 個 – 1Gb イーサネット・コネクター 2 個 – Lenovo XClarity Controller ネットワーク・コネクター 2 個 – 10Gb SFP+ コネクター 2 個 – VGA コネクター 1 個

表 1. サーバー仕様 (続き)

仕様	説明

	– ワイヤレス対応 LOM パッケージ
	  – USB 3.1 Gen 1 コネクター 2 個
	  – 1Gb イーサネット・コネクター 2 個
	  – Lenovo XClarity Controller ネットワーク・コネクター 1 個
	  – 1Gb SFP コネクター 2 個
	  – 10Gb SFP+ コネクター 2 個
	  – VGA コネクター 1 個
	– 10G BASE-T LOM パッケージ
	  – Lenovo XClarity Controller ネットワーク・コネクター 2 個
	  – 10Gb BASE-T RJ45 コネクター 2 個
	  – 1Gb イーサネット・コネクター 2 個
	  – USB 3.1 Gen 1 コネクター 2 個
	  – VGA コネクター 1 個
	• 背面 I/O コネクター (サーバー背面):
	– WLAN アンテナ・コネクター 2 個
	– RS-232 ポート (RJ-45) 1 個
	– LTE アンテナ・コネクター 2 個
	– USB 2.0 コネクター 2 個
	– 2 種類の分電モジュール:
	  – 2 個の電源コネクターを搭載した 12V 分電モジュール (PDM)
	  – 1 個の電源コネクターを搭載した -48V 分電モジュール (PDM)

RAID コントローラー	ソフトウェア RAID: ソフトウェア RAID コントローラーは、システム・ボード上に組み込まれていて、RAID レベル 0、1、5、10 がサポートされます。
	• 標準 Intel SATA ソフトウェア RAID、RSTe をサポート
	• Intel VROC NVMe RAID をサポート
	  – VROC Intel-SSD-Only は、Intel NVMe ドライブを搭載した RAID レベル 0、1、5、および 10 をサポートします。
	  – VROC プレミアムは、アクティベーション・キーを必要とし、非 Intel NVMe ドライブを搭載した RAID レベル 0、1、5、および 10 をサポートします。アクティベーション・キーの取得とインストールについて詳しくは、https://fod.lenovo.com/lkmsを参照してください。
	
	ハードウェア RAID: M.2 ハードウェア RAID モジュールはハードウェア RAID ストレージに必要で、RAID レベル 0 および 1 がサポートされます。

ビデオ・コントローラー (Lenovo XClarity Controller に内蔵)	Matrox G200 • ASPEED • SVGA 互換ビデオ・コントローラー • Avocent デジタル・ビデオ圧縮 • 16 MB のビデオ・メモリー (拡張不可) **注：**最大ビデオ解像度は 60 Hz で 1920 x 1200 です。
ファン	40 mm システム・ファン x3

表 1. サーバー仕様 (続き)

仕様	説明
電源アダプター	外部電源アダプター: 正弦波入力 (50 ～ 60 Hz) が必須 • 240W 外部電源アダプター 100-127 V AC/ 200-240 V AC、3.2/1.6 A **注：** • 電源アダプターは 12V PDM でのみサポートされています。 **警告：** – **ノードへの電源アダプターは、同じブランド、電源定格、ワット数、または効率レベルでなければなりません。** – **電源アダプターを区別するには、電源アダプターのサイズ、コネクターの位置、およびラベルを確認します。** • GPU が取り付けられている場合、システムは 2 つの電源アダプターを使用して取り付ける必要があります EU ErP (エコデザイン) 指令 (2009/125/EC) の実施措置 (2019 年 10 月 1 日付けの委員会規則 (EU) 2019/1782) では、製造業者がエネルギー効率および評価情報を提供する必要があります。Lenovo 製品は、互換性のあるさまざまな充電器で動作するように設計されており、異なる充電器が同梱されている場合があるほか、後で購入していただくこともできます。互換性のある充電器のリストが、EU 適合宣言書 (DoC) に記載されており、こちら (https://www.lenovo.com/us/en/compliance/eu-doc) からご覧いただけます。お使いの充電器のエネルギー効率について情報が必要な方は、以下の Web ページにアクセスし、完全なモデル番号を使用して製品を検索し、該当するユーザー・ガイドまたはパワー・サプライ・データ・シートを選択してください。https://support.lenovo.com/
音響放出ノイズ (ベース構成)	• 操作時: – 最小: 5.3 ベル – 標準: 5.4 ベル – 最大: 5.7 ベル • アイドル – 最小: 4.9 ベル – 標準: 5.0 ベル – 最大: 5.4 ベル **注：** 1. 音響出力レベルは、管理された音響環境のもとで、ISO 7779 の規定の手順に従って測定されたもので、ISO 9296 に従って報告されています。 2. 公称音響ノイズ・レベルは、指定された構成に基づいているため、構成または状況によって若干変化する場合があります。 3. このサーバーでは、機能、消費電力、および必要とされる冷却能力がそれぞれ異なる複数のオプションがサポートされます。これらのオプションに必要な冷却が増加すると、ファン速度とそれによって発生する音響レベルが上がります。インストール・システムで計測される実際の音圧レベルは、さまざまな要因によって異なります。この要因には、インストール・システム内のラックの台数、部屋の構成、他の装置からのノイズ・レベル、部屋の周囲温度および気圧、および従業員と装置の位置関係が含まれます。

表 1. サーバー仕様 (続き)

仕様	説明
発熱量 (消費電力)	概算発熱量: • 最小構成: 287.46 BTU/時間 (84.25 ワット) • 最大構成: 783.02 BTU/時間 (229.49 ワット)
電源入力	分電モジュール: 12V PDM • 電源アダプターごとに 12.2V/20A をサポートします • 各ノードは最大 2 個の電源アダプターをサポートします 分電モジュール: -48V PDM • -48V ～ -60V DC/8.4 A 最大直接 -48V 入力 **注：** • システムの消費電力が 210W 未満の場合、電源の冗長性はデュアル電源モードです。 • 電力リソースが不十分な場合、システムはキャッピング/スロットル・モードで動作します。 • システムの消費電力が 210W を超える場合は、2つの電源アダプターを取り付けてください。
NEBS の注意および規制準拠に関する事項	NEBS GR-1089-CORE の注意書き、規制準拠に関する事項、および要件に従います。 • 共通ボンディング・ネットワーク (CBN) のインストールをサポートします。 • システムは、National Electric Code が適用されるネットワーク通信設備でインストールできます。 • テスト条件を「最小動作電圧」に設定する場合、UEFI「電源復元ポリシー」をオンにする必要があります。 • NEBS 規格によって評価される 1 Gb イーサネットおよび SFP+ のケーブルは、シールドが必要です。 • NEBS セクション 4 の評価における通常のシステム起動時間は、4 分 55 秒です。 • 警告: この装置または半組立品のイントラビルディング・ポート (1Gb イーサネットおよび SFP+ のポート) は、イントラビルディングまたは屋外に露出していない配線やケーブル接続にのみ適しています。この装置または半組立品のイントラビルディング・ポートを OSP やその 6 メートル (約 20 フィート) を超える配線に接続されているインターフェースの金属部と絶対に接続しないでください。これらのインターフェースは、イントラビルディング・インターフェース (GR-1089 記載のタイプ 2 ポート) としてのみ使用するように設計されており、屋外に露出した OSP 配線とは分離する必要があります。1 次保護装置を追加しても、これらのインターフェースと OSP 配線の金属部の接続を十分に保護することはできません。

表 1. サーバー仕様 (続き)

仕様	説明
環境	ThinkSystem SE350 は、ASHRAE クラス A4 規格に準拠しています。動作温度が ASHRAE A4 規格を外れている場合またはファンが故障して A2 規格を外れている状態では、システムのパフォーマンスに影響が出る場合があります。 ThinkSystem SE350 は、以下の環境でサポートされます。 • 標準: – サーバー電源オン時: 0°C ～ 45°C (32°F ～ 113°F) – サーバー電源オフ時: 0°C ～ 45°C (32°F ～ 113°F) • ASHRAE クラス A4 – サーバー電源オン時: 5°C ～ 45°C (41°F ～ 113°F)。900 m (2,953 フィート) を超える高度では、高度が 125 m (410 フィート) 上がるごとに、最大周辺温度が 1°C 減少。 – サーバー電源オフ時: 5°C ～ 45°C (41°F ～ 113°F) • 拡張動作温度 (限定構成1): – サーバー電源オン時: 0°C ～ 55°C (32°F ～ 131°F) – サーバー電源オフ時: 0°C ～ 55°C (32°F ～ 131°F) **注：**限定構成1: – GPU なし – Micron なし/LITE-ON M.2 – Lenovo 認定 PCIe カードのみ。例えば: • ThinkSystem Broadcom NX-E PCIe 10Gb 2 ポート Base-T イーサネット・アダプター • ThinkSystem Mellanox ConnectX-4 Lx 10/25GbE SFP28 2-ポート PCIe イーサネット・アダプター • 配送時/保管時: -40°C ～ 60°C (-40°F ～ 140°F) • 最大高度: 3,050m (10,000 フィート) • 相対湿度 (結露なし): – 作動時: 8% ～ 90%、最大露点: 24°C (75.2°F) – 配送時/保管時: 8% ～ 90%、最大露点: 27°C (80.6°F) • 動作していない (開梱状態) ストレージは、5% ～ 95%、最大乾球温度 38.7°C (101.7°F) 条件に 48 時間耐えることができます。 • 粒子汚染 **注意：**浮遊微小粒子や反応性ガスは、単独で、あるいは湿気や気温など他の環境要因と組み合わされることで、サーバーにリスクをもたらす可能性があります。微粒子およびガスの制限に関する情報は、「*ThinkSystem SE350 メンテナンス・マニュアル*」の「粒子汚染」を参照してください。 **注：**ThinkSystem SE350 は、エンクロージャー前面配送用ブラケットまたはセキュリティー・ベゼルの内部に取り付けられた一連の防塵フィルターの使用をサポートします。防塵フィルターは、ASHRAE Standard 52.2–2017 に従って 最小効率評価値 (MERV) が 4 になっています。
オペレーティング・システム	サポートおよび認定オペレーティング・システム: • Microsoft Windows Server • VMware ESXi

表 1. サーバー仕様 (続き)

仕様	説明
	注：VMware ESXI のブート・ドライブ: VMware ESXi ブート・サポートの場合、特定の M.2 ドライブのみが、その耐久性に基づいてサポートされます。特定の情報については、Lenovo サポートのヘルプ HT512201 を参照してください。 • Red Hat Enterprise Linux • SUSE Linux Enterprise Server 参照: • オペレーティング・システムの全リスト:https://lenovopress.lenovo.com/osig。 • OS デプロイメント手順: 127 ページの 「オペレーティング・システムのデプロイ」

衝撃および振動の仕様

以下の情報は、サーバーの衝撃および振動仕様の要約です。ご使用のモデルによっては、使用できない機能があったり、一部の仕様が該当しない場合があります。

SE350 システム構成		振動 (サーバーが稼働している場合)	衝撃 (サーバーが稼働している場合)	環境振動基準		
左翼	右翼			IEC Stationary 0.15Grms、30mins15G、11ms	3.06 Grms、15mins 30G、11ms	3.06 Grms、60mins 30G、11ms
M.2 SATA ドライブ x4	なし	3.06Grms、3 ～ 500Hz、60 分/軸	30G、11ms、ハーフサイン、± X、± Y、± Z	√	√	√
M.2 SATA ドライブ x4	NVIDIA T4 GPU	3.06Grms、3 ～ 500Hz、15 分/軸	30G、11ms、ハーフサイン、± X、± Y、± Z	√	√	
M.2 NVMe ドライブ x4 (ヒートシンク付き)	M.2 NVMe ドライブ x4 (ヒートシンク付き)	0.21Grms、5 ～ 500Hz、15 分/軸	15G、3ms、ハーフサイン、± X、± Y、± Z	√		
M.2 NVMe ドライブ x4 (ヒートシンク付き)	NVIDIA T4 GPU	0.21 Grms、5 ～ 500 Hz、15 分/軸	15G、3ms、ハーフサイン、± X、± Y、± Z	√		

粒子汚染

注意: 浮遊微小粒子 (金属片や微粒子を含む) や反応性ガスは、単独で、あるいは湿気や気温など他の環境要因と組み合わされることで、本書に記載されているデバイスにリスクをもたらす可能性があります。

過度のレベルの微粒子や高濃度の有害ガスによって発生するリスクの中には、デバイスの誤動作や完全な機能停止の原因となり得る損傷も含まれます。以下の仕様では、このような損傷を防止するために設定された微粒子とガスの制限について説明しています。以下の制限を、絶対的な制限として見なしたり、あるいは使用したりしてはなりません。温度や大気中の湿気など他の多くの要因が、粒子や環境腐食性およびガス状の汚染物質移動のインパクトに影響することがあるからです。本書で説明されている特定の制限が無い場合は、人体の健康と安全の保護に合致するよう、微粒子やガスのレベル維持のための慣例を実施する必要があります。お客様の環境の微粒子あるいはガスのレベルがデバイス損傷の原因であると Lenovo が判断した場合、Lenovo は、デバイスまたは部品の修理あるいは交換の条件として、かかる環境汚染を改善する適切な是正措置の実施を求める場合があります。かかる是正措置は、お客様の責任で実施していただきます。

表 2. 微粒子およびガスの制限

汚染物質	制限
反応性ガス	ANSI/ISA 71.04-1985 準拠の重大度レベル G1[1]: • 銅の反応レベルが 1 か月あたり 200 オングストローム未満 (Å/月 ～ 0.0035 µg/cm^2-時間の重量増加)。[2] • 銀の反応レベルが 1 か月あたり 200 オングストローム (Å/月 ～ 0.0035 µg/cm^2-時間の重量増加)。[3]

表 2. 微粒子およびガスの制限 (続き)

汚染物質	制限
	• ガス腐食性の反応監視は、床から 4 分の 1 および 4 分の 3 のフレーム高さ、または気流速度がより高い場所で、吸気口側のラックの前面の約 5 cm (2 インチ) で行う必要があります。
浮遊微小粒子	データ・センターは、ISO 14644-1 クラス 8 の清潔レベルを満たす必要があります。 エアサイド・エコノマイザーのないデータ・センターの場合、以下のいずれかのろ過方式を選択して、ISO 14644-1 クラス 8 の清潔レベルを満たすことができます。 • 部屋の空気は、MERV 8 フィルターで継続的にフィルタリングできます。 • データ・センターに入る空気は、MERV 11 またはできれば MERV 13 フィルターでフィルタリングできます。 エアサイド・エコノマイザーを備えるデータ・センターの場合、ISO クラス 8 の清潔レベルを実現するためのフィルターの選択は、そのデータ・センターに存在する特定の条件によって異なります。 • 粒子汚染の潮解相対湿度は、60% RH を超えていなければなりません。[4] • データ・センターには、亜鉛ウィスカーがあってはなりません。[5]

[1] ANSI/ISA-71.04-1985。「*プロセス計測およびシステム制御のための環境条件: 気中浮遊汚染物質*」。Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

[2] Å/月における腐食生成物の厚みにおける銅腐食の増加率と重量増加率との間の同等性の導出では、Cu_2S および Cu_2O が均等な割合で増加することを前提とします。

[3] Å/月における腐食生成物の厚みにおける銀腐食の増加率と重量増加率との間の同等性の導出では、Ag_2S のみが腐食生成物であることを前提とします。

[4] 粒子汚染の潮解相対湿度とは、水分を吸収した塵埃が、十分に濡れてイオン導電性を持つようになる湿度のことです。

[5] 表面の異物は、データ・センターの 10 のエリアから、金属スタブの導電粘着テープの直径 1.5 cm のディスクでランダムに収集されます。電子顕微鏡の解析における粘着テープの検査で亜鉛ウィスカーが検出されない場合、データ・センターには亜鉛ウィスカーがないと見なされます。

管理オプション

このセクションで説明されている XClarity ポートフォリオおよびその他のシステム管理オプションは、サーバーをより効率的に管理するために使用できます。

概要

オプション	説明
Lenovo XClarity Controller	ベースボード管理コントローラー (BMC)。 サービス・プロセッサー機能、Super I/O、ビデオ・コントローラー、およびリモート・プレゼンス機能をシステム・ボード上の単一のチップに一元化します。 **インターフェース** • CLI アプリケーション • Web GUI インターフェース • モバイル・アプリケーション • REST API **使用方法およびダウンロード**

オプション	説明
	https://pubs.lenovo.com/lxcc-overview/
Lenovo XClarity Administrator	マルチサーバー管理のための一元管理インターフェース。 **インターフェース** • Web GUI インターフェース • モバイル・アプリケーション • REST API **使用方法およびダウンロード** http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html
Lenovo XClarity Essentials ツールセット	サーバー構成、データ収集、ファームウェア更新のための持ち運び可能で軽量なツール・セット。単一サーバーまたはマルチサーバーの管理コンテキストに適しています。 **インターフェース** • **OneCLI**: CLI アプリケーション • **Bootable Media Creator**: CLI アプリケーション、GUI アプリケーション • **UpdateXpress**: GUI アプリケーション **使用方法およびダウンロード** https://pubs.lenovo.com/lxce-overview/
Lenovo XClarity Provisioning Manager	管理タスクを簡略化できる単一のサーバー上の UEFI ベースの組み込み GUI ツール。 **インターフェース** • Web GUI インターフェース (BMC 遠隔アクセス) **使用方法およびダウンロード** https://pubs.lenovo.com/lxpm-overview/ **重要：** Lenovo XClarity Provisioning Manager(LXPM) でサポートされるバージョンは、製品によって異なります。本書では、特に指定がない限り、Lenovo XClarity Provisioning Manager のすべてのバージョンを Lenovo XClarity Provisioning Manager および LXPM と記載します。ご使用のサーバーでサポートされる LXPM バージョンを確認するには、https://pubs.lenovo.com/lxpm-overview/ にアクセスしてください。
Lenovo XClarity Integrator	VMware vCenter、Microsoft Admin Center、Microsoft System Center など、特定のデプロイメント・インフラストラクチャーで使用されるソフトウェアと Lenovo 物理サーバーの管理および監視機能を統合し、追加のワークロード回復力を提供する一連のアプリケーション。 **インターフェース** GUI アプリケーション **使用方法およびダウンロード** https://pubs.lenovo.com/lxci-overview/

オプション	説明
Lenovo XClarity Energy Manager	サーバーの電力および温度を管理およびモニターできるアプリケーション。 **インターフェース** • Web GUI インターフェース **使用方法およびダウンロード** https://datacentersupport.lenovo.com/solutions/lnvo-lxem
Lenovo Capacity Planner	サーバーまたはラックの電力消費量計画をサポートするアプリケーション。 **インターフェース** • Web GUI インターフェース **使用方法およびダウンロード** https://datacentersupport.lenovo.com/solutions/lnvo-lcp

機能

オプション		機能							
		マルチ・システム管理	OS 展開	システム構成	ファームウェア更新[1]	イベント/アラートの監視	インベントリー/ログ	電源管理	電源計画
Lenovo XClarity Controller				√	√[2]	√	√[4]		
Lenovo XClarity Administrator		√	√	√	√[2]	√	√[4]		
Lenovo XClarity Essentials ツールセット	OneCLI	√		√	√[2]	√	√[4]		
	Bootable Media Creator			√	√[2]		√[4]		
	UpdateXpress			√	√[2]				
Lenovo XClarity Provisioning Manager			√	√	√[3]		√[5]		
Lenovo XClarity Integrator		√	√[6]	√	√	√	√	√[7]	
Lenovo XClarity Energy Manager		√				√		√	
Lenovo Capacity Planner									√[8]

注：

1. ほとんどのオプションは、Lenovo Tools を使用して更新できます。GPU ファームウェアや Omni-Path ファームウェアなど一部のオプションでは、サプライヤー・ツールを使用する必要があります。
2. オプション ROM のサーバー UEFI 設定を「**自動**」または「**UEFI**」に設定して、Lenovo XClarity Administrator、Lenovo XClarity EssentialsまたはLenovo XClarity Controllerを使用してファームウェアを更新する必要があります。
3. ファームウェア更新は、Lenovo XClarity Provisioning Manager、Lenovo XClarity ControllerおよびUEFI の更新に限られます。アダプターなど、オプション・デバイスのファームウェア更新はサポートされません。

4. Lenovo XClarity Administrator、Lenovo XClarity Controller または Lenovo XClarity Essentials に表示されるモデル名やファームウェア・レベルなどのアダプター・カードの詳細情報について、オプション ROM のサーバー UEFI を「**自動**」または「**UEFI**」に設定する必要があります。
5. 制限されたインベントリー。
6. System Center Configuration Manager (SCCM) 用Lenovo XClarity Integratorデプロイメント・チェックでは、Windows オペレーティング・システム・デプロイメントをサポートします。
7. 電源管理機能は VMware vCenter 用 Lenovo XClarity Integrator でのみサポートされています。
8. 新しい部品を購入する前に、Lenovo Capacity Planner を使用してサーバーの電力要約データを確認することを強くお勧めします。

第 2 章　サーバー・コンポーネント

サーバーに関連する各コンポーネントについての説明は、このセクションの情報を使用します。

重要な製品情報

このセクションでは、以下の位置を確認するために役立つ情報について説明します。

- **マシン・タイプおよびモデル情報**: Lenovo のサポートを受ける場合に、マシン・タイプ、モデル、およびシリアル番号の情報をお知らせいただけると、技術担当者がお客様のサーバーを特定して迅速なサービスを提供するのに役立ちます。モデル番号とシリアル番号は ID ラベルに記載されています。以下の図は、マシン・タイプ、モデル、シリアル番号が記載された ID ラベルの位置を示しています。
- **FCC ID および IC 認定情報**: FCC および IC 認定情報は、次の図に示すようにエッジ・サーバーにあるラベルによって識別されます。

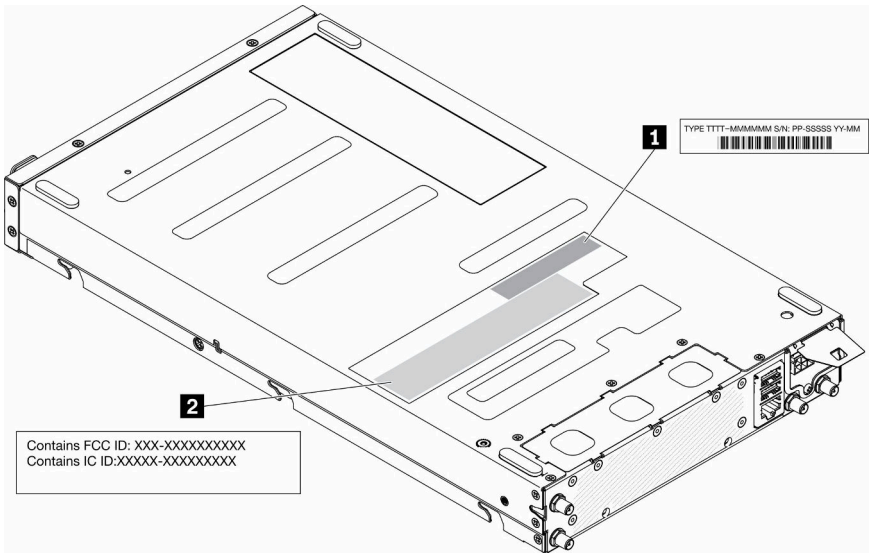


図 2. ID ラベルと FCC ID/IC ラベルの位置

表 3. ID ラベルと FCC ID/IC ラベル

1 ID ラベル (マシン・タイプとモデル情報)	**2** FCC ID および IC 認定ラベル

プリインストールされたワイヤレス・モジュールの場合、このラベルは Lenovo によって取り付けられたワイヤレス・モジュールの実際の FCC ID および IC 認定番号を示します。

注：事前にインストールされているワイヤレス・モジュールの取り外しや交換はお客様ご自身で行わないでください。モジュールを交換するには、まず Lenovo サービスにアクセスする必要があります。Lenovo は、許可されていない交換による損傷に対して一切責任を負わないものとします。

ネットワーク・アクセス・タグ

ネットワーク・アクセス・タグは、サーバーの前面にあります。ネットワーク・アクセス・タグをはがして、ホスト名、システム名、インベントリー・バーコードなどの情報を記録するための独自のラベルを貼り付けることができます。後で参照できるようにネットワーク・アクセス・タグを取っておいてください。

© Copyright Lenovo 2019, 2022

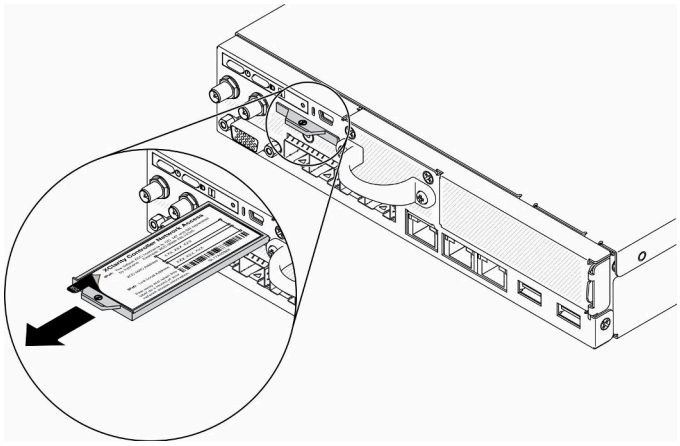


図 3. ネットワーク・アクセス・タグの位置

QR コード

さらに、システム・サービス・カードがサーバーのトップ・カバーにあり、サービス情報にモバイル・アクセスするためのクイック・リファレンス (QR) コードも記載されています。モバイル・デバイスで QR コード読み取りアプリケーションを使用して QR コードをスキャンすると、サービス情報 Web ページにすぐにアクセスできます。サービス情報 Web ページでは、追加情報として部品の取り付けや交換用のビデオ、およびサーバー・サポートのためのエラー・コードが提供されます。

図 4. SE350 QR コード

前面図

サーバーの前面図はモデルによって異なります。

サーバーの前面図

- 10G SFP+ LOM パッケージ

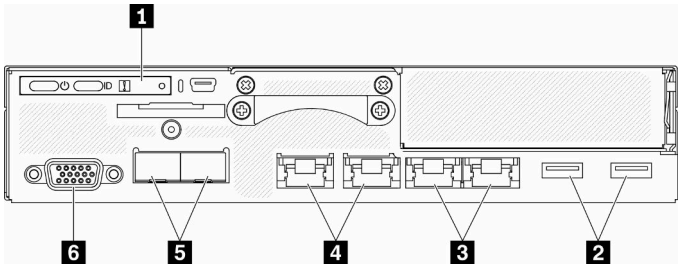


図 5. 10g SFP+ LOM パッケージの前面図

表 4. 10G SFP+ LOM パッケージ前面図のコンポーネント

1 前面オペレーター・パネル	**4** 共有 XClarity Controller (XCC) ネットワーク・コネクター コネクターのレンチ・アイコンは、このコネクターが Lenovo XClarity Controller への接続用に設定可能であることを示しています。 **注意：**ネットワーク IP は 1 つのみ使用できます。 デイジー・チェーン接続をサポートする 2x RJ45 ポート。デュアル・ポートには、イーサネット管理接続をデイジー・チェーン接続する機能が備わっているため、管理スイッチ内のポートの数が減り、システム管理に必要となる全体的なケーブル密度が低下します。この機能を使用すると、ユーザーは最初の XCC 管理ポートを管理ネットワークに接続し、2 番目の XCC 管理ポートを次のサーバー・システムに接続することができます。
2 USB 3.1 Gen 1 コネクター	**5** 10Gb SFP+ イーサネット・コネクター
3 1Gb イーサネット・コネクター	**6** VGA コネクター

- ワイヤレス対応 LOM パッケージ

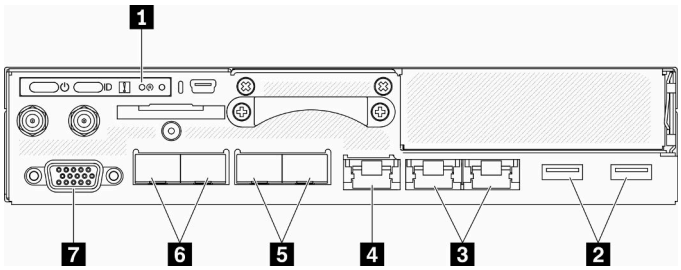


図 6. ワイヤレス対応 LOM パッケージの前面図

表 5. ワイヤレス対応 LOM パッケージ前面図のコンポーネント

1 前面オペレーター・パネル	**5** 1Gb SFP コネクター
2 USB 3.1 Gen 1 コネクター	**6** 10Gb SFP+ イーサネット・コネクター

表 5. ワイヤレス対応 LOM パッケージ前面図のコンポーネント (続き)

3 1Gb イーサネット・コネクター	**7** VGA コネクター
4 XClarity Controller (XCC) ネットワーク・コネクター コネクターのレンチ・アイコンは、このコネクターが Lenovo XClarity Controller への接続用に設定可能であることを示しています。	

フィラーの取り付け

コネクターが使用されていない場合は、フィラーを取り付けます。フィラーを適切に保護しないと、コネクターが破損する場合があります。

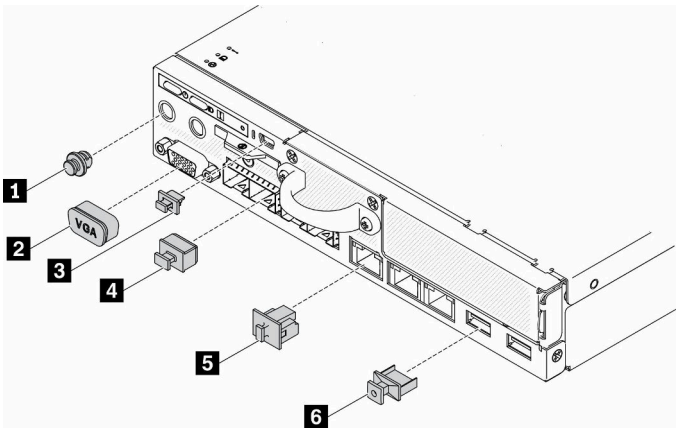


図 7. フィラー

表 6. フィラー

1 アンテナ・ポート・フィラー (x2 または使用不可、モデルによって異なる)	**4** SFP イーサネット・コネクター・フィラー (x2 または x4、モデルにより異なる)
2 フィラー VGA	**5** イーサネット・コネクター・フィラー (x3 または x4、モデルにより異なる)
3 ミニ USB フィラー	**6** USB フィラー x2

前面オペレーター・パネル

サーバーの前面操作情報パネルには、コントロール、コネクター、および LED があります。前面オペレーター・パネルはモデルによって異なります。

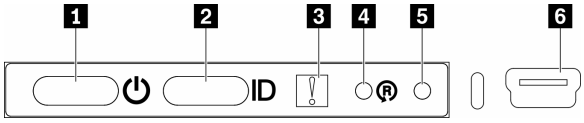


図 8. 前面オペレーター・パネル

表 7. 前面オペレーター・パネルのコントロールとインジケーター

1 電源ボタン/LED (緑色)	**4** ワイヤレス対応 LOM パッケージ・リセット・ボタン
2 識別ボタン/LED (青色)	**5** NMI ボタン
3 システム・エラー LED (黄色)	**6** XClarity Controller mini USB コネクター

1 電源ボタン/LED (緑色): サーバーの電源を手動でオンまたはオフにするには、このボタンを押します。電源 LED の状態は次のとおりです。

オフ: 電源が入っていないか、電源アダプターまたは LED 自体に障害があります。

高速で点滅 (毎秒 4 回): サーバーの電源がオフになっていて、オンにする準備ができていません。電源ボタンは無効です。この状態は約 5 秒から 10 秒続きます。

ゆっくり点滅 (毎秒 1 回): サーバーの電源がオフになっていて、オンにする準備ができています。電源ボタンを押して、サーバーをオンにすることができます。

オン: サーバーの電源がオンになっています。

2 ID ボタン/LED (青色): この青色の LED は、他のサーバーの中から該当のサーバーを視覚的に見つけるのに使用します。この LED はプレゼンス検出ボタンとしても使用されます。Lenovo XClarity Administrator を使用して、この LED をリモートで点灯させることができます。識別 LED の状態は次のとおりです。

オフ: Presence Detection がオフです。

高速で点滅 (毎秒 4 回): (XCC ファームウェア・バージョン 3.10 以降) サーバーがまだアクティブになっておらず、電源許可がありません。システムをアクティブにするには、*アクティベーション・ガイド*を参照してください。

低速で点滅 (1 秒に 1 回): プレゼンス検出がオンです。

オン: プレゼンス検出がオンです。

3 システム・エラー LED (黄色): この黄色の LED が点灯している場合、システム・エラーが発生したことを示しています。

4 ワイヤレス対応 LOM モジュールのリセット・ボタン: ワイヤレス対応 LOM モジュールのリセット・ピン。

5 NMI ボタン: このボタンを押すと、プロセッサーにマスク不能割り込み (NMI) を強制します。こうすることで、サーバーをブルー・スクリーンにしてメモリー・ダンプを取ることができます。ボタンを押すには、ペンまたは真っすぐに伸ばしたペーパー・クリップの先を使用することが必要な場合があります。

6 XClarity Controller mini USB コネクター: XClarity Controller を使用してシステムを管理するための mini USB の接続に使用されます。

背面図

サーバーの背面から、パワー・サプライ、PCIe アダプター、シリアル・ポート、およびイーサネット・ポートなど複数のコンポーネントにアクセスできます。

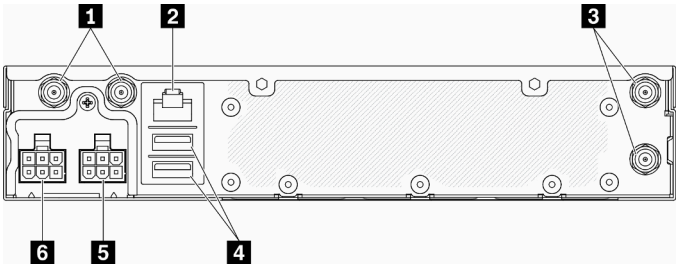


図 9. 背面図 - 12V 分電モジュール (PDM)

表 8. 背面図 - 12V 電源アダプター・モデル

1 WLAN アンテナ・コネクター (M.2 WLAN モジュールが取り付けられている場合にのみ使用可能)	**4** USB 2.0 コネクター
2 RS-232 ポート (RJ-45)	**5** 電源コネクター 1
3 LTE アンテナ・コネクター (M.2 LTE モジュールが取り付けられている場合にのみ使用可能)	**6** 電源コネクター 2

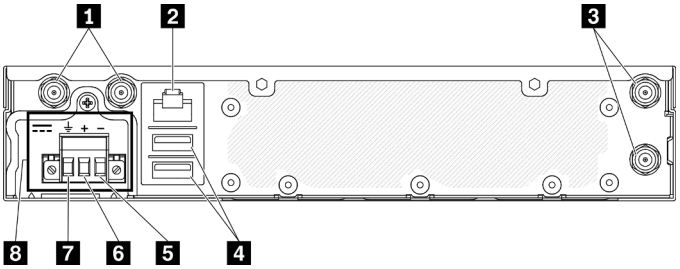


図 10. 背面図 - -48V 分電モジュール (PDM)

表 9. 背面図 - -48V 電源アダプター・モデル

1 WLAN アンテナ・コネクター (M.2 WLAN モジュールが取り付けられている場合にのみ使用可能)	**5** Vin- ターミナル
2 RS-232 ポート (RJ-45)	**6** Vin+ ターミナル
3 LTE アンテナ・コネクター (M.2 LTE モジュールが取り付けられている場合にのみ使用可能)	**7** GND ターミナル
4 USB 2.0 コネクター	**8** 電源コネクター

カバーの取り付け

カバーを取り付けます。カバーを適切に保護しないと、コネクターが破損する場合があります。

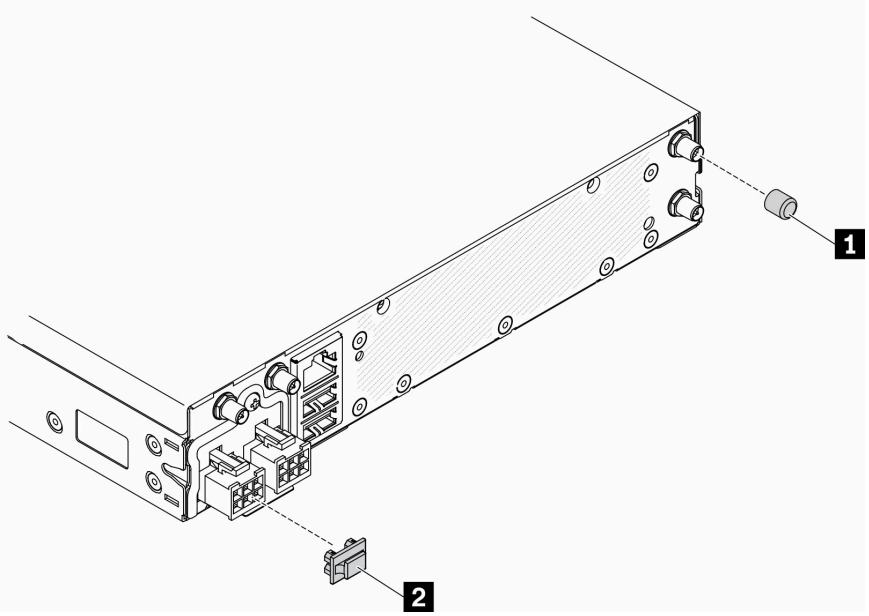


図 11. カバー

表 10. カバー

1 アンテナ・カバー x 4 (アンテナが取り付けられていない場合は、アンテナ・ポート・フィラーを使用します。18 ページの 「前面図」を参照)	**2** 電源アダプター・カバー

システム・ボード・コネクター

次の図は、システム・ボード上のコネクターを示しています。

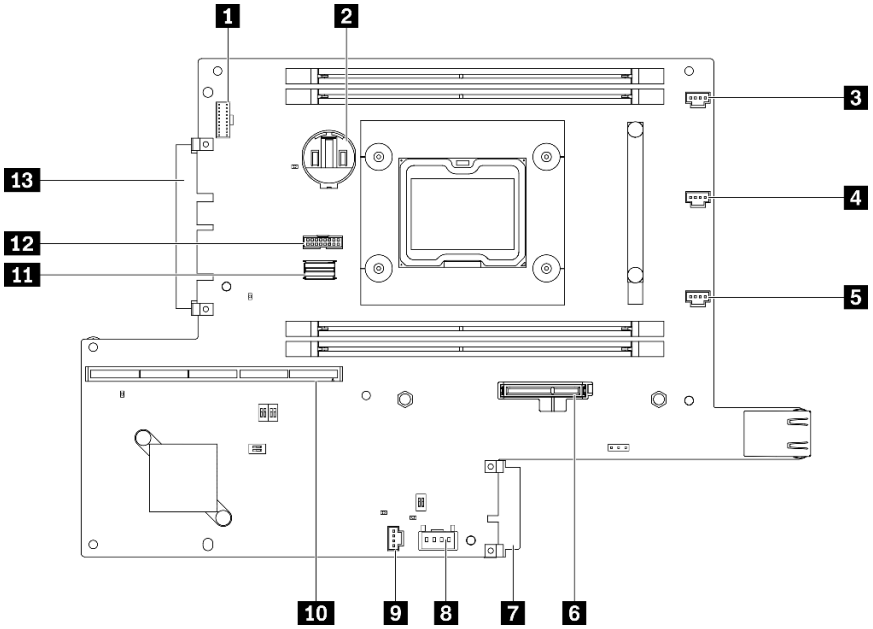


図 12. システム・ボード・コネクター

表 11. システム・ボード・コネクター

1 前面オペレーター・パネル・コネクター	**8** ロック・スイッチ・コネクター
2 3V バッテリー (CR2032)	**9** 侵入検出スイッチ・コネクター
3 ファン 1 コネクター	**10** ライザー・コネクター
4 ファン 2 コネクター	**11** SATA ケーブル・コネクター
5 ファン 3 コネクター	**12** TPM コネクター
6 M.2 ブート・アダプター・コネクター	**13** LOM モジュール・コネクター
7 分電モジュール・コネクター	

LOM パッケージ

次の図は、ワイヤレス対応 LOM パッケージ、10G SFP+ LOM パッケージ、および 10G BASE-T LOM パッケージを示しています。

サーバー構成に応じて、LOM パッケージのひとつをシステム・ボード上の LOM モジュール・コネクターに接続します (23 ページの 「システム・ボード・コネクター」 を参照)。

ワイヤレス対応 LOM パッケージ

ワイヤレス対応 LOM パッケージは、サーバーのワイヤレス機能を有効にします。パッケージ上のコネクターは、M.2 WLAN/LTE ワイヤレス・アダプター用に設計されています。ワイヤレス・アダプターには 2 つのタイプがあり、両方とも同じ方式で取り付けられています。詳しくは、60 ページの 「M.2 WLAN/LTE ワイヤレス・アダプターの取り付け」を参照してください。

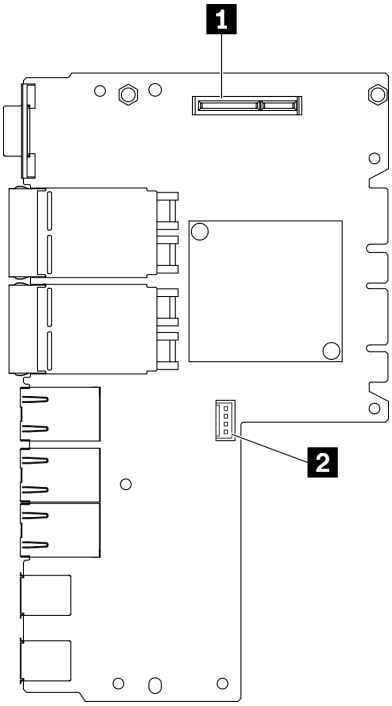


図 13. ワイヤレス対応 LOM パッケージ

表 12. ワイヤレス対応 LOM パッケージ

1 M.2 WLAN/LTE ワイヤレス・コネクター	**2** サービス専用コネクター

注：サービス専用コネクターは一部のモデルで使用可能で、サービス専用に予約されています。

10G SFP+ LOM パッケージ

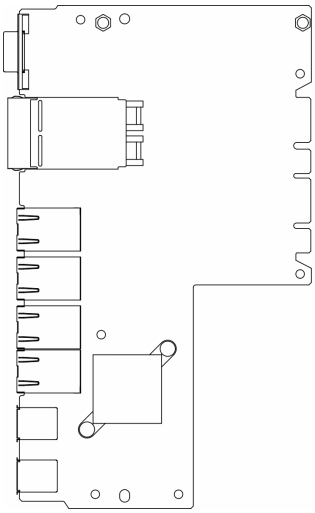


図 14. 10G SFP+ LOM パッケージ

10G BASE-T LOM パッケージ

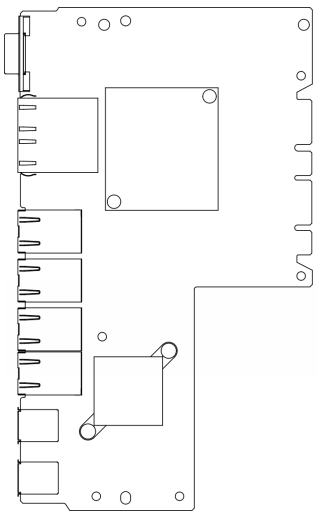


図 15. 10G BASE-T LOM パッケージ

PCIe ライザー・アセンブリー

PCIe ライザー・アセンブリー上のコネクターの位置を確認するには、この情報を使用します。

PCIe および M.2 ライザー・アセンブリー

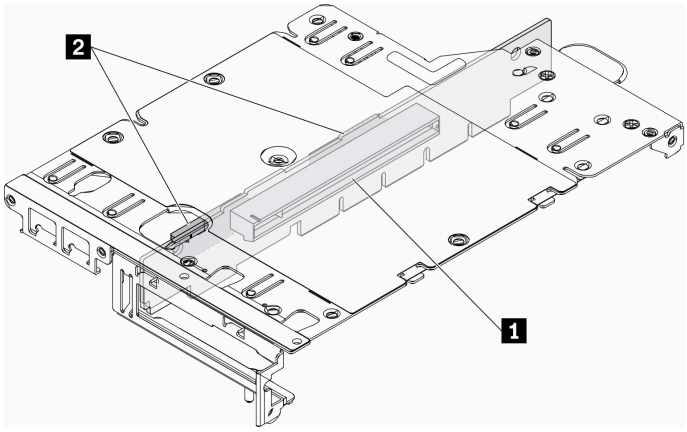


図 16. PCIe および M.2 ライザー・アセンブリー

表 13. PCIe および M.2 ライザー・アセンブリー

1 スロット 6: PCIe 3.0 x16 (75W 未満、ロー・プロファイル、ハーフハイト、ハーフサイズ PCIe アダプターをサポート)	**2** ドライブ (スロット) 2-5、M.2 データ・アダプター

M.2 ライザー・アセンブリー

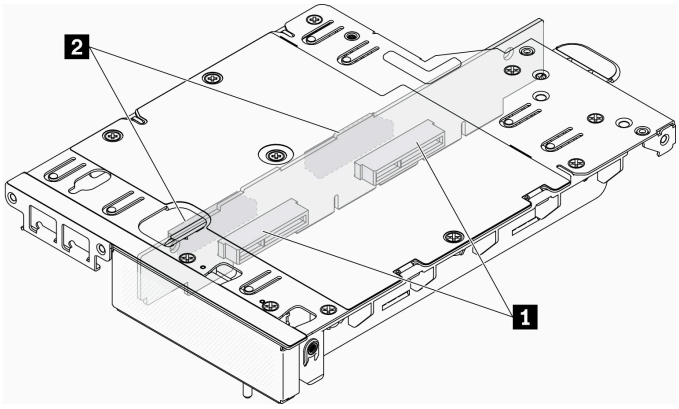


図 17. M.2 ライザー・アセンブリー

表 14. M.2 ライザー・アセンブリー

1 ドライブ (スロット) 6-9、M.2 データ・アダプター	**2** ドライブ (スロット) 2-5、M.2 データ・アダプター

M.2 ドライブおよびスロットの番号

M.2 ドライブとスロットの番号を見つけるには、この情報を使用します

M.2 ブート・アダプター

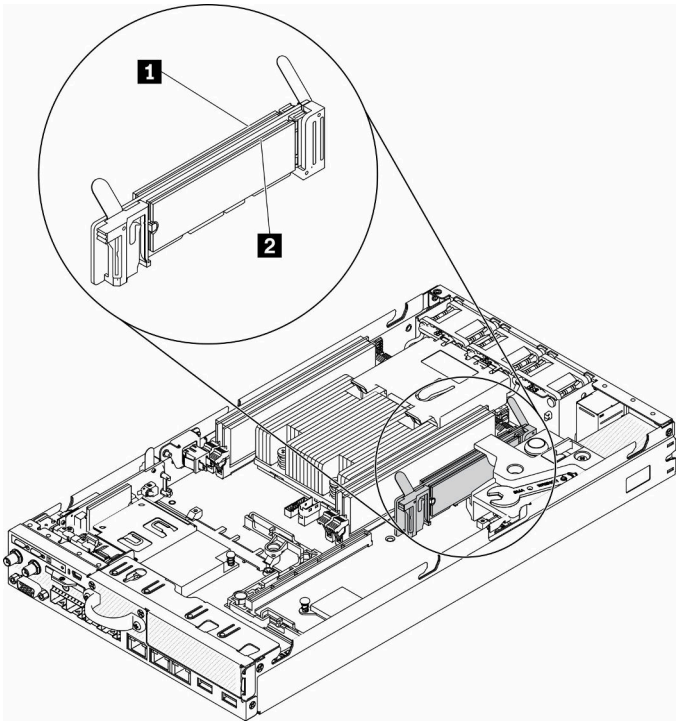


図 18. M.2 ブート・アダプター

重要：アダプターの反対側にある M.2 ドライブのペアは、同じマウント・クリップを共有するため、同じフォーム・ファクター (つまり、同じ物理長) である必要があります。

表 15. M.2 ブート・アダプター・スロットの番号

1 ドライブ 0	**2** ドライブ 1

M.2 データ・アダプター

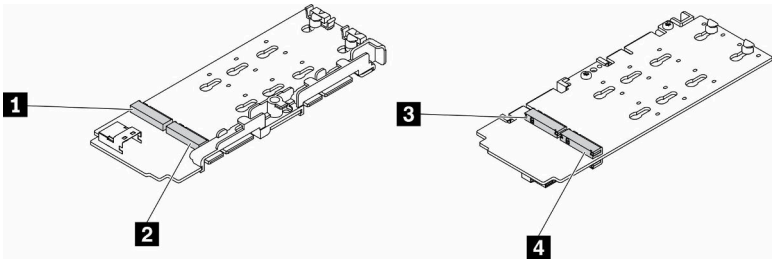


図 19. M.2 データ・アダプター

重要：データ・ドライブ・アダプターとブート・ドライブ・アダプターの場合、アダプターの反対側にある M.2 ドライブのペアは、同じマウント・クリップを共有するため、同じフォーム・ファクター (つまり、同じ物理長) である必要があります。

この M.2 データ・アダプターの図では、

- ドライブ位置 **1** および **4** のペアは、同じマウント・クリップを共有するため、同じフォーム・ファクター (つまり、同じ物理長) である必要があります。
- ドライブ位置 **2** および **3** のペアは、同じマウント・クリップを共有するため、同じフォーム・ファクター (つまり、同じ物理長) である必要があります。

表 16. M.2 データ・アダプター

1 ドライブ 2 または 9	**3** ドライブ 5 または 6
2 ドライブ 4 または 7	**4** ドライブ 3 または 8

次の表は、M.2 ドライブおよびスロットの番号を示しています。

- PCIe および M.2 ライザー・アセンブリー

左側 (M.2 データ・アダプター)		右側 (PCIe アダプター)	
アダプターでのドライブの番号	**UEFI 設定メニューでのスロット番号**	**アダプターでのドライブの番号**	**UEFI 設定メニューでのスロット番号**
ドライブ 2	スロット 2	PCIe アダプター	スロット 6
ドライブ 3	スロット 3		
ドライブ 4	スロット 4		
ドライブ 5	スロット 5		

左側 (M.2 データ・アダプターとハードウェア RAID)		右側 (PCIe アダプター)	
アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号	アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号
ドライブ 2	スロット 2/3	PCIe アダプター	スロット 6
ドライブ 3			
ドライブ 4	スロット 4/5		
ドライブ 5			

- 2 個の M 2 データ・アダプターを搭載した M.2 ライザー・アセンブリー

左側 (M.2 データ・アダプター)		右側 (M.2 データ・アダプター)	
アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号	アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号
ドライブ 2	スロット 2	ドライブ 9	スロット 9
ドライブ 3	スロット 3	ドライブ 8	スロット 8
ドライブ 4	スロット 4	ドライブ 7	スロット 7
ドライブ 5	スロット 5	ドライブ 6	スロット 6

左側 (M.2 データ・アダプターとハードウェア RAID)		右側 (M.2 データ・アダプターとハードウェア RAID)	
アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号	アダプターでのドライブの番号	UEFI 設定メニューでのスロット番号
ドライブ 2	スロット 2/3	ドライブ 9	スロット 8/9
ドライブ 3		ドライブ 8	
ドライブ 4	スロット 4/5	ドライブ 7	スロット 6/7
ドライブ 5		ドライブ 6	

部品リスト

部品リストを使用して、サーバーで使用できる各コンポーネントを識別します。

31 ページの 図 20「サーバー・コンポーネント」に記載されている部品の注文について詳しくは、以下を参照してください。

https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/parts

注：モデルによっては、ご使用のサーバーの外観は、図と若干異なる場合があります。

次の表にリストした部品は、次のいずれかとして識別されます。

- **Tier 1 の、お客様での取替え可能部品 (CRU)**: Lenovo が Tier 1 と指定する CRU の交換はお客様ご自身の責任で行っていただきます。サービス契約がない場合に、お客様の要請により Lenovo が Tier 1 CRU の取り付けを行った場合は、その料金を請求させていただきます。
- **Tier 2 のお客様での取替え可能部品 (CRU)**: Lenovo が Tier 2 と指定する CRU は、お客様ご自身で取り付けることができますが、対象のサーバーに関して指定された保証サービスの種類に基づき、追加料金なしで Lenovo に取り付け作業を依頼することもできます。
- **現場交換可能ユニット (FRU)**: FRU の取り付け作業は、トレーニングを受けたサービス技術員のみが行う必要があります。

- **消耗部品および構造部品**: 消耗部品および構造部品 (カバーやベゼルなどのコンポーネント) の購入および交換はお客様の責任で行っていただきます。お客様の要請により Lenovo が構成部品の入手または取り付けを行った場合は、サービス料金を請求させていただきます。

サーバー・コンポーネント

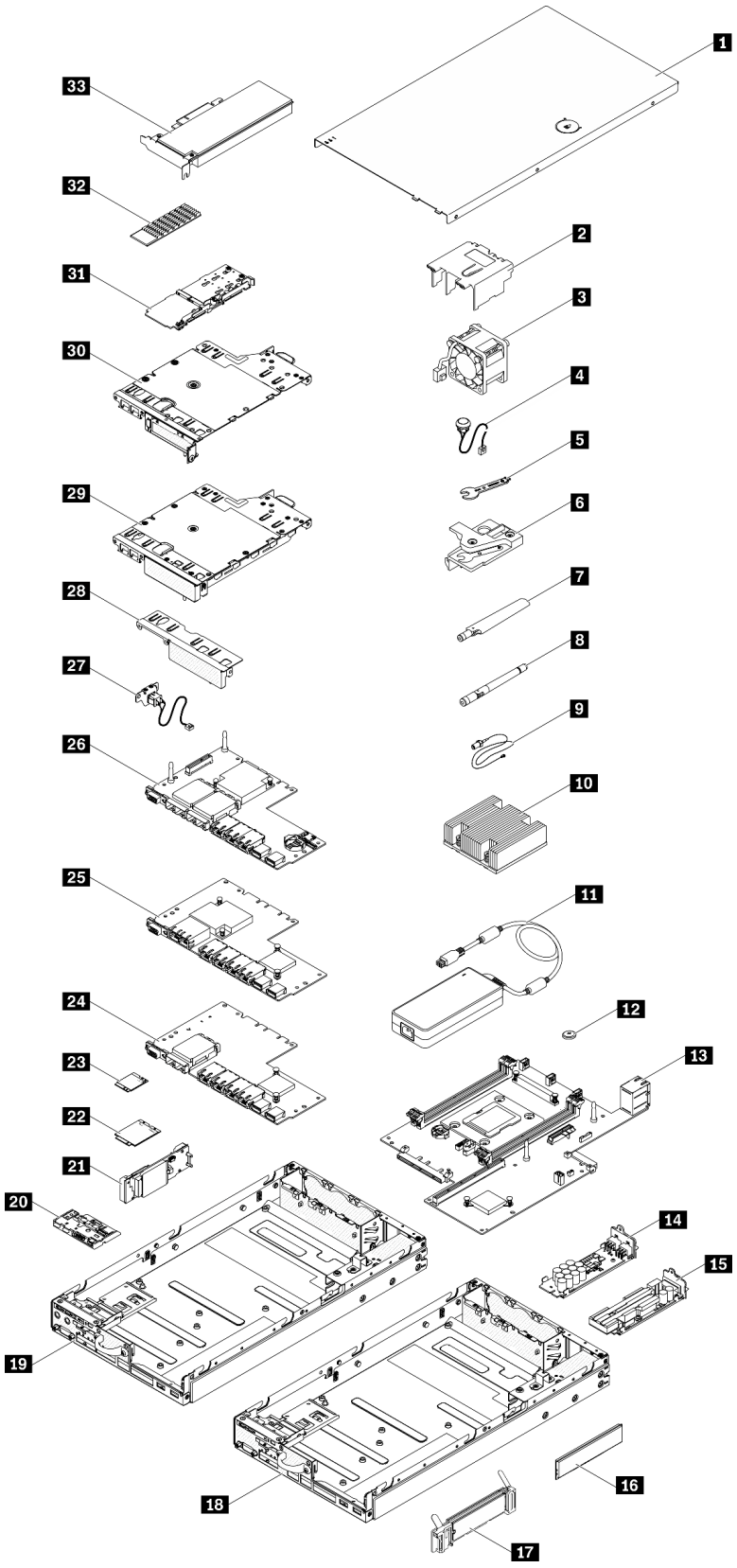


図 20. サーバー・コンポーネント

表 17. 部品リスト

番号	説明	Tier 1 CRU	Tier 2 CRU	FRU	消耗部品および構造部品
31 ページの 図 20「サーバー・コンポーネント」に記載されている部品の注文の詳細については、以下を参照してください。 https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/parts					
1	トップ・カバー				√
2	エアー・バッフル				√
3	ファン	√			
4	侵入検出スイッチ・ケーブル	√			
5	その他のキットにあるドライバー				√
6	侵入検出スイッチ	√			
7	LTE アンテナ	√			
8	WLAN アンテナ	√			
9	M.2 WLAN/LTE モジュール・ケーブル			√	
10	プロセッサー・ヒートシンク			√	
11	電源アダプター	√			
12	CMOS バッテリー (CR2032)				√
13	システム・ボード			√	
14	12 V 分電モジュール		√		
15	-48 V 分電モジュール		√		
16	DIMM	√			
17	M.2 ブート・アダプター		√		
18	10G SFP+ LOM パッケージ・シャーシ				√
19	ワイヤレス対応 LOM パッケージ・シャーシ				√
20	前面オペレーター・パネル				√
21	M.2 WLAN/LTE ワイヤレス・アダプター			√	
22	M.2 LTE モジュール			√	
23	M.2 WLAN モジュール			√	
24	10G SFP+ LOM パッケージ				√
25	10G BASE-T LOM パッケージ				√
26	ワイヤレス対応 LOM パッケージ				√
27	ロック・ケーブル	√			
28	前面フィラー				√
29	M.2 ライザー・アセンブリー		√		
30	PCIe および M.2 ライザー・アセンブリー		√		
31	M.2 SATA/NVMe データ・アダプター		√		

表 17. 部品リスト (続き)

番号	説明	Tier 1 CRU	Tier 2 CRU	FRU	消耗部品および構造部品
32	M.2 SATA/NVMe ヒートシンク				√
33	PCIe アダプター		√		

電源コード

サーバーが設置されている国および地域に合わせて、複数の電源コードを使用できます。

サーバーで使用できる電源コードを参照するには、次のようにします。

1. 以下へ進んでください。

   http://dcsc.lenovo.com/#/

2. 「**Preconfigured Model (事前構成モデル)**」または「**Configure to order (注文構成製品)**」をクリックします。
3. コンフィギュレーター・ページを表示するサーバーのマシン・タイプとモデルを入力します。
4. すべての電源コードを表示するには、「**Power (電源)**」 → 「**Power Cables (電源ケーブル)**」をクリックします。

注：

- 本製品を安全に使用するために、接地接続機構プラグ付き電源コードが提供されています。感電事故を避けるため、常に正しく接地されたコンセントで電源コードおよびプラグを使用してください。
- 米国およびカナダで使用される本製品の電源コードは、Underwriter's Laboratories (UL) によってリストされ、Canadian Standards Association (CSA) によって認可されています。
- 115 ボルト用の装置には、次の構成の、UL 登録、CSA 認定の電源コードをご使用ください。最小 18 AWG、タイプ SVT または SJT、3 線コード、最大長 4.5 m (15 フィート)、平行ブレード型、15 アンペア 125 ボルト定格の接地端子付きプラグ。
- 230 ボルト (米国における) 用の装置には、次の構成の、UL 登録、CSA 認定の電源コードをご使用ください。最小 18 AWG、タイプ SVT または SJT、3 線コード、最大長 4.5 m (15 フィート)、タンデム・ブレード型、15 アンペア 250 ボルト定格の接地端子付きプラグ。
- 230 ボルト (米国以外における) 用の装置には、接地端子付きプラグを使用した電源コードをご使用ください。これは、装置を使用する国の安全についての適切な承認を得たものでなければなりません。
- 特定の国または地域用の電源コードは、通常その国または地域でだけお求めいただけます。

第 3 章　サーバーのハードウェアのセットアップ

サーバーをセットアップするには、購入したオプションを取り付け、サーバーを配線し、ファームウェアを構成して更新して、オペレーティング・システムをインストールします。

サーバー・セットアップ・チェックリスト

サーバー・セットアップ・チェックリストを使用して、サーバーのセットアップに必要なすべてのタスクを実行したことを確認できます。

サーバー・セットアップ・チェックリストは、納品時のサーバー構成によって異なります。サーバーが完全に構成されている場合は、サーバーをネットワークと AC 電源に接続し、サーバーの電源をオンにするだけで済みます。他の場合では、サーバーへのハードウェア・オプションの取り付け、ハードウェアやファームウェアの構成、およびオペレーティング・システムのインストールが必要となります。

以下のステップで、サーバーをセットアップするための一般的な手順を説明します。

1. サーバー・パッケージを開梱します。1 ページの「サーバーのパッケージ内容」を参照してください。
2. サーバーのハードウェアをセットアップします。
   a. 必要なハードウェアまたはサーバー・オプションを取り付けます。39 ページの「サーバー・ハードウェア・オプションの取り付け」の関連トピックを参照してください。
   b. 必要に応じて、サーバーに付属のレール・キットを使用して、標準的なラック・キャビネットにサーバーを取り付けます。オプション・レール・キットに付属の「*ラック搭載手順*」を参照してください。
   c. イーサネット・ケーブルおよび電源コードをサーバーに接続します。コネクターの位置を確認するには、21 ページの「背面図」を参照してください。配線のベスト・プラクティスについては、78 ページの「サーバーの配線」を参照してください。
   d. サーバーの電源をオンにします。78 ページの「サーバーの電源をオンにする」を参照してください。

      注：サーバーの電源をオンにしなくても、管理プロセッサー・インターフェースにアクセスしてシステムを構成できます。サーバーが電源に接続されているときは常に、管理プロセッサー・インターフェースを使用できます。管理サーバー・プロセッサーへのアクセスについて詳しくは、以下を参照してください。

      https://pubs.lenovo.com/lxcc-overview/にある、ご使用のサーバーと互換性のある XCC に関する資料の「XClarity Controller Web インターフェースの開始と使用」セクション。
   e. サーバー・ハードウェアが正常にセットアップされたことを検証します。サーバーのセットアップの検証を参照してください。
3. システムを構成します。
   a. 81 ページの「システムをアクティブにする」の詳細な手順に従って、システムをアクティブにします。
   b. Lenovo XClarity Controller を管理ネットワークに接続します。Lenovo XClarity Controller のネットワーク接続の設定を参照してください。
   c. 必要に応じて、サーバーのファームウェアを更新します。84 ページの「ファームウェアの更新」を参照してください。
   d. サーバーのファームウェアを構成します。89 ページの「ファームウェアの構成」を参照してください。

      以下の情報は、RAID 構成に使用可能です。

© Copyright Lenovo 2019, 2022

- https://lenovopress.com/lp0578-lenovo-raid-introduction
- https://lenovopress.com/lp0579-lenovo-raid-management-tools-and-resources

e. オペレーティング・システムをインストールします。127 ページの 「オペレーティング・システムのデプロイ」を参照してください。

f. サーバー構成をバックアップします。128 ページの 「サーバー構成のバックアップ」を参照してください。

g. サーバーが使用するプログラムおよびアプリケーションをインストールします。

取り付けのガイドライン

サーバーにコンポーネントを取り付けるには、この取り付けのガイドラインを使用します。

オプションのデバイスを取り付ける前に、以下の注意をよくお読みください。

注意：静電気の影響を受けやすいコンポーネントは取り付け時まで帯電防止パッケージに収め、システム停止やデータの消失を招く恐れのある静電気にさらされないようにしてください。また、このようなデバイスを取り扱う際は静電気放電用リスト・ストラップや接地システムなどを使用してください。

- 安全に作業を行うために、「安全について」およびガイドラインをお読みください。
  - すべての製品の安全情報の完全なリストは、以下の場所で入手できます。

    https://pubs.lenovo.com/safety_documentation/
  - 以下のガイドラインも同様に入手できます。38 ページの 「静電気の影響を受けやすいデバイスの取り扱い」および38 ページの 「電源オンされているサーバーの内部での作業」。
- 取り付けるコンポーネントがサーバーによってサポートされていることを確認します。サーバーでサポートされているオプションのコンポーネントのリストについては、https://serverproven.lenovo.com/server/se350 を参照してください。
- 新規のサーバーを取り付ける場合は、最新のファームウェアをダウンロードして適用してください。既知の問題が対処され、ご使用のサーバーが最適なパフォーマンスで動作するようになります。ご使用のサーバー用のファームウェア更新をダウンロードするには、ThinkSystem SE350 ドライバーおよびソフトウェアにアクセスしてください。

  重要：一部のクラスター・ソリューションには、特定のコード・レベルまたは調整されたコード更新が必要です。コンポーネントがクラスター・ソリューションの一部である場合は、コードを更新する前に、クラスターでサポートされているファームウェアとドライバーの最新の Best Recipe コード・レベル・メニューを確認してください。
- オプションのコンポーネントを取り付ける場合は、サーバーが正しく作動していることを確認してから取り付けてください。
- 作業スペースは清潔に保ち、取り外したコンポーネントは、振動したり傾いたりしない平らで滑らかな平面に置いてください。
- 自分 1 人では重すぎるかもしれない物体を持ち上げようとしないでください。重い物体を持ち上げる必要がある場合は、以下の予防措置をよくお読みください。
  - 足元が安定しており、滑るおそれがないことを確認します。
  - 足の間でオブジェクトの重量が同量になるよう分散します。
  - ゆっくりと力を入れて持ち上げます。重い物体を持ち上げるときは、決して身体を急に動かしたり、ひねったりしないでください。
  - 背筋を痛めないよう、脚の筋肉を使用して立ち上がるか、押し上げるようにして持ち上げます。
- サーバー、モニター、およびその他のデバイス用に、適切に接地されたコンセントの数量が十分にあることを確認してください。
- ディスク・ドライブに関連した変更を行う前に、重要なデータをバックアップしてください。

- 小型のマイナス・ドライバー、小型のプラス・ドライバー、および T8 TORX ドライバーを用意します。
- システム・ボードおよび内部コンポーネントのエラー LED を表示するには、電源をオンのままにしてください。
- ホット・スワップ・パワー・サプライ、ホット・スワップ・ファン、またはホット・プラグ USB デバイスを取り外したり、取り付けたりするために、サーバーの電源をオフにする必要はありません。ただし、アダプター・ケーブルの取り外しや取り付けが必要なステップを実行する場合は、前もってサーバーの電源をオフにする必要があります。また、ライザー・カードの取り外しや取り付けが必要なステップを実行する場合は、前もってサーバーから電源を切り離しておく必要があります。
- コンポーネント上の青色は、コンポーネントをサーバーから取り外したり、取り付けたり、あるいはラッチの開閉などを行う際につかむことができるタッチ・ポイントを示します。
- コンポーネント上の赤茶色の表示、またはコンポーネント上やその付近にある赤茶色のラベルは、そのコンポーネントがホット・スワップ可能であることを示しています。サーバーとオペレーティング・システムがホット・スワップ機能をサポートしていれば、サーバーの稼働中でもそのコンポーネントの取り外しや取り付けを行うことができます(赤茶色のラベルは、ホット・スワップ・コンポーネントのタッチ・ポイントも示す場合もあります)。特定のホット・スワップ・コンポーネントの取り外しまたは取り付けを行う前に、そのコンポーネントの取り外しまたは取り付けに関して行う可能性があるすべての追加指示を参照してください。
- ドライブのリリース・ラッチの隣にある赤い帯は、サーバーおよびオペレーティング・システムがホット・スワップ機能をサポートしている場合、そのドライブがホット・スワップ可能であることを示します。つまり、サーバーを稼働させたままドライブの取り外しまたは取り付けが可能です。

  注：ドライブの取り外しまたは取り付けを行う前に、ホット・スワップ・ドライブの取り外しまたは取り付けについてシステム固有の指示を参照し、追加手順が必要かどうかを確認してください。
- サーバーでの作業が終わったら、必ずすべての安全シールド、ガード、ラベル、および接地ワイヤーを再取り付けしてください。

システムの信頼性に関するガイドライン

適切なシステム冷却および信頼性を確保するために、システムの信頼性に関するガイドラインを確認してください。

以下の要件を満たしていることを確認してください。

- サーバーにリダンダント電源が付属している場合は、各電源アダプター・ベイに電源アダプターが取り付けられていること。
- サーバー冷却システムが正しく機能できるように、サーバーの回りに十分なスペースを確保してあること。約 50 mm (2 インチ) の空きスペースをサーバーの前面および背面の周囲に確保してください。ファンの前には物を置かないでください。
- 冷却と通気を確保するため、サーバーの電源を入れる前にサーバー・カバーを再取り付けしてください。サーバー・カバーを外した状態で 30 分以上サーバーを作動させないでください。サーバーのコンポーネントが損傷する場合があります。
- オプションのコンポーネントに付属する配線手順に従っていること。
- 障害のあるファンは、障害が発生してから 48 時間以内に交換すること。
- 取り外したホット・スワップ・ファンは、取り外してから 30 秒以内に交換すること。
- 取り外したホット・スワップ・ドライブは、取り外してから 2 分以内に交換すること。
- 取り外したホット・スワップ電源アダプターは、取り外してから 2 分以内に交換すること。
- サーバーに付属の各エアー・バッフルが、サーバー起動時に取り付けられていること (一部のサーバーではエアー・バッフルが複数付属している場合があります)。エアー・バッフルがないままサーバーを作動させると、プロセッサーが損傷する可能性があります。
- すべてのプロセッサー・ソケットには、ソケット・カバーまたはプロセッサーとヒートシンクが取り付けられていること。

- 複数のプロセッサーが取り付けられている場合、各サーバーのファン装着規則が厳格に守られていること。

電源オンされているサーバーの内部での作業

電源オンされているサーバー内部での作業のガイドライン

注意：サーバーの内部コンポーネントが静電気にさらされると、サーバーが停止したりデータが消失する恐れがあります。このような問題が起きないように、電源をオンにしたサーバー内部の作業を行うときは、常に静電気放電用のリスト・ストラップを着用するか、またはその他の接地システムを使用してください。

- 特に腕の部分がゆったりした衣服を着用しないでください。サーバー内部の作業の前に、長袖はボタン留めするか捲り上げてください。
- ネクタイ、スカーフ、ネック・ストラップ、長い髪などがサーバー内に垂れ下がらないようにしてください。
- ブレスレット、ネックレス、リング、カフス・ボタン、腕時計などの装身具は外してください。
- シャツのポケットからペンや鉛筆などを取り出してください。サーバーの上に身体を乗り出したときに落下する可能性があります。
- クリップや、ヘアピン、ねじなどの金属製品がサーバー内部に落ちないように注意してください。

静電気の影響を受けやすいデバイスの取り扱い

静電気の影響を受けやすいデバイスを取り扱うには、この情報を使用します。

注意：静電気の影響を受けやすいコンポーネントは取り付け時まで帯電防止パッケージに収め、システム停止やデータの消失を招く恐れのある静電気にさらされないようにしてください。また、このようなデバイスを取り扱う際は静電気放電用リスト・ストラップや接地システムなどを使用してください。

- 動作を制限して自分の周囲に静電気をためないようにしてください。
- 気温の低い時期は、デバイスの取り扱いに特に注意してください。暖房で室内の湿度が下がり、静電気が増えるためです。
- 特に電源をオンにしたサーバーの内部で作業を行うときは、常に静電気放電用のリスト・ストラップまたはその他の接地システムを使用してください。
- 部品を帯電防止パッケージに入れたまま、サーバーの外側の塗装されていない金属面に 2 秒以上接触させてください。これにより、パッケージとご自分の身体から静電気が排出されます。
- 部品をそのパッケージから取り出して、それを下に置かずに直接サーバーに取り付けてください。デバイスを下に置く必要がある場合は、帯電防止パッケージに入れます。デバイスをサーバーや金属面の上には置かないでください。
- デバイスを取り扱う際は、端またはフレームを持って慎重に持ってください。
- はんだの接合部、ピン、または露出した回路には触れないでください。
- 損傷の可能性を防止するために、デバイスに他の人の手が届かない位置を維持してください。

メモリー・モジュールの取り付けの規則および順序

メモリー・モジュールは、サーバーに実装されたメモリー構成に基づいて、特定の順序で取り付ける必要があります。

次の図は、システム・ボード・コンポーネント (DIMM コネクターを含む) を示しています。

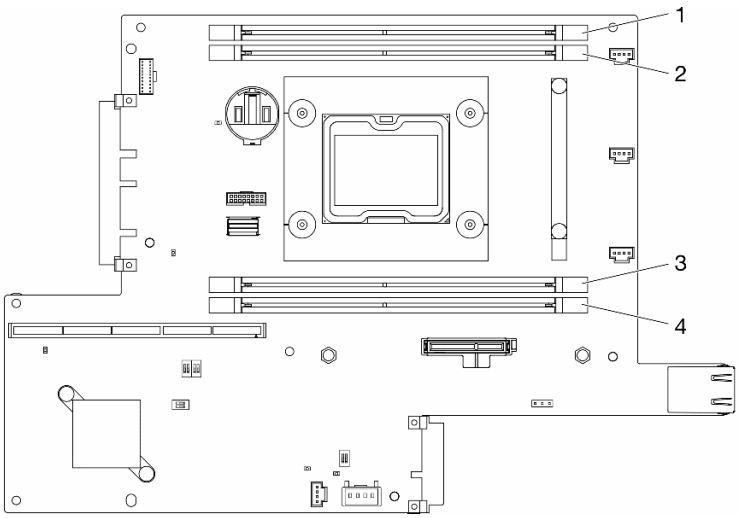


図 21. DIMM コネクター

次の表は、DIMM の取り付けの順序を示しています。

取り付けられた DIMM の合計	DIMM 1	DIMM 2	DIMM 3	DIMM 4
1	√			
2	√			√
3	√	√		√
4	√	√	√	√

サーバー・ハードウェア・オプションの取り付け

このセクションでは、オプションのハードウェアの初期取り付けを実行する手順を示します。各コンポーネントの取り付け手順では、交換するコンポーネントにアクセスするために実行する必要がある作業に触れています。

取り付け手順は、作業をできる限り少なくするための最適なシーケンスを示します。

注意：取り付けるコンポーネントが問題なく正常に動作するために、次の予防措置をよくお読みください。

- 取り付けるコンポーネントがサーバーによってサポートされていることを確認します。サーバーでサポートされているオプションのコンポーネントのリストについては、https://serverproven.lenovo.com/server/se350 を参照してください。
- 常時 最新のファームウェアをダウンロードして適用してください。既知の問題が対処され、ご使用のサーバーが最適なパフォーマンスで動作するようになります。ご使用のサーバー用のファームウェア更新をダウンロードするには、ThinkSystem SE350 ドライバーおよびソフトウェアにアクセスしてください。
- オプションのコンポーネントを取り付ける場合は、サーバーが正しく作動していることを確認してから取り付けてください。
- このセクションの取り付け手順に従い、適切なツールを使用してください。誤って取り付けられたコンポーネントは、ピンの損傷、コネクターの損傷、配線の緩み、あるいはコンポーネントの緩みによって、システム障害の原因となる可能性があります。

ノードの取り外し

ノードを取り外すには、この情報を使用します。

ノードを取り外す前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

ステップ 1. ノードをエンクロージャーから取り外すには、以下のステップを実行してください。

a. 配送用ブラケットの 5 本のねじを取り外し、2 個のつまみねじを緩めます。

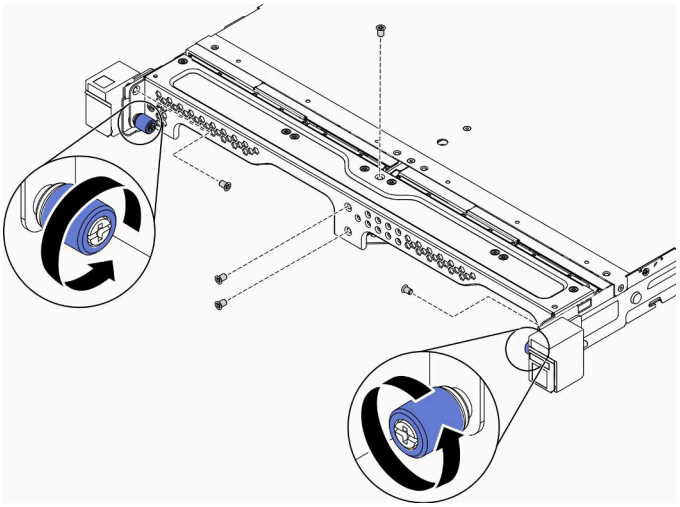


図 22. ノードの取り外し

b. 配送用ブラケットをエンクロージャーから取り外します。

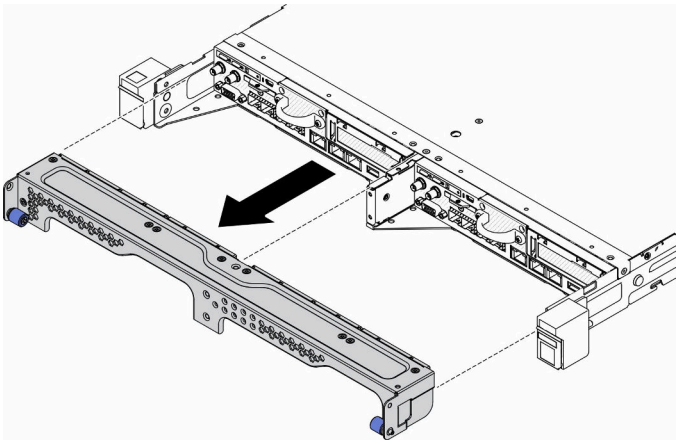


図 23. ノードの取り外し

c. リリース・ボタンを押し、ノードをエンクロージャから引き出します。

- E1 エンクロージャー (1U 2 ノード)

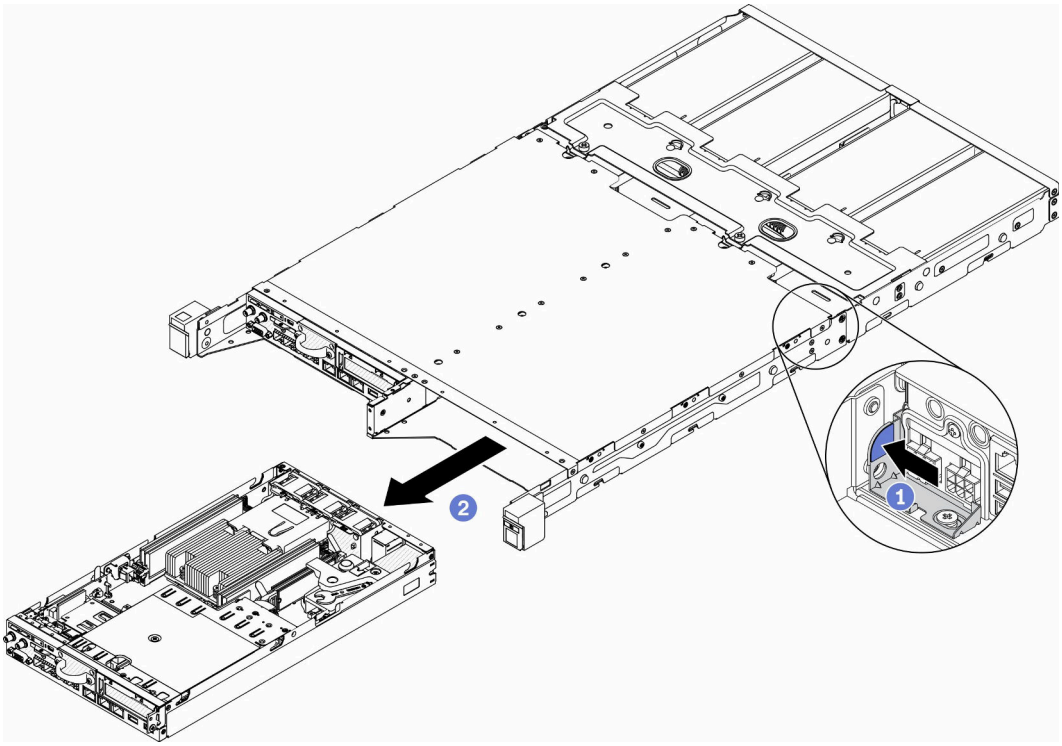


図 24. ノードの取り外し

- E2 エンクロージャー (2U 2 ノード)

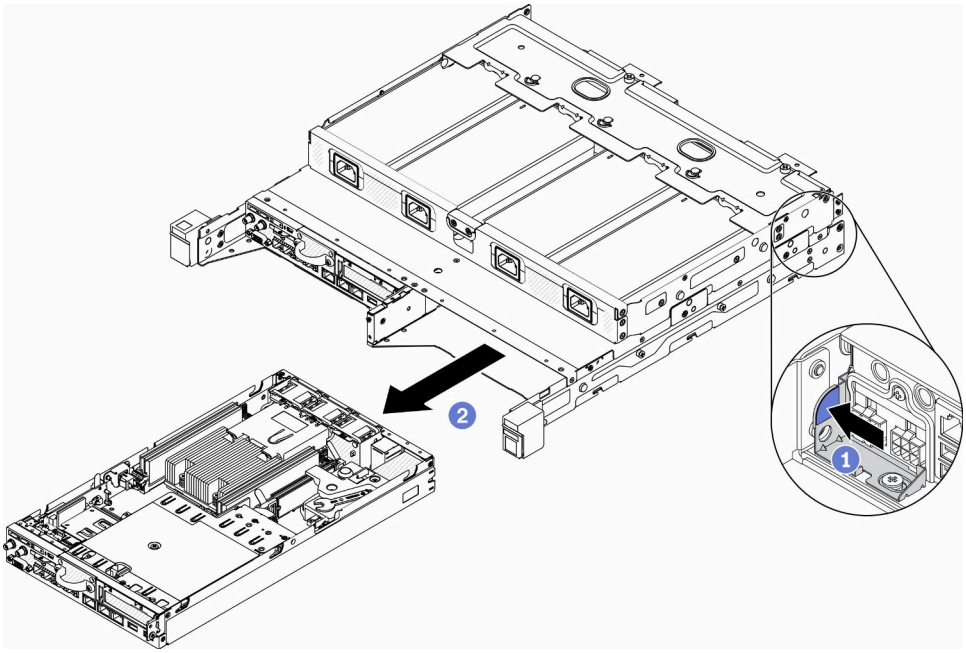


図 25. ノードの取り外し

注：

- エンクロージャーから取り外したノードにはトップ・カバーがありません。ノードをエンクロージャーに再取り付けしない場合は、必ずトップ・カバーを取り付けます。73 ページの「トップ・カバーの取り付け」を参照してください。
- ノードを E1 エンクロージャー (1U 2 ノード) から取り外した場合や、E1 エンクロージャーに再取り付けしていない場合、適切に動作させるには重要プロダクト・データ (VPD) をデフォルト・モードに変更してください。「*メンテナンス・マニュアル*」の「*E1 エンクロージャー構成の VPD の変更 (トレーニングを受けた技術員のみ)*」を参照してください。

ステップ 2. ノードをノード・スリーブから取り外すには、以下のステップを実行してください。

a. 2 本のつまみねじを緩め、ノード・スリーブからノードをスライドさせて取り出します。

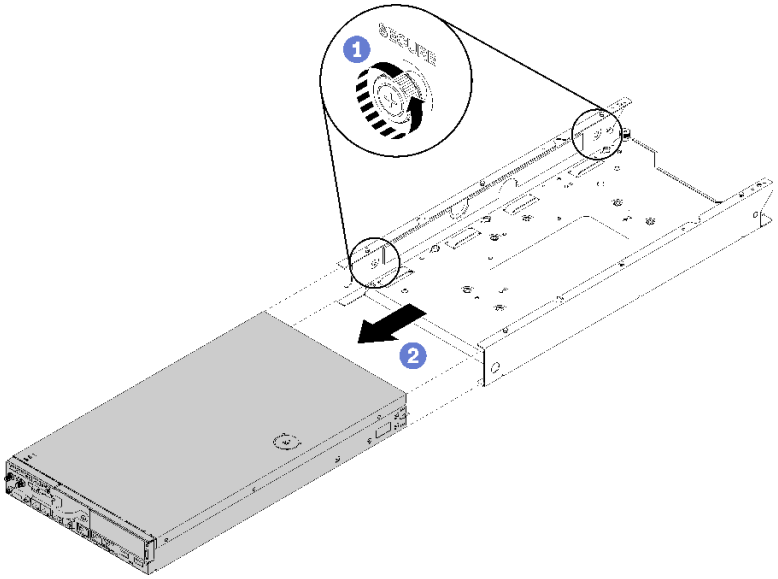


図 26. ノードの取り外し

注：ブックシェルフ構成、DIN レール構成、壁掛け用構成の取り付けの詳細については、必要に応じて、「*構成部品取り付けガイド*」を参照してください。

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=N_3TsrEYPP0

トップ・カバーの取り外し

トップ・カバーを取り外すには、この情報を使用します。

起こり得る危険を回避するために、以下の安全についてをお読みになり、それに従ってください。

S012

警告：
高温の面が近くにあります。

S014

警告：
危険な電圧、電流、エネルギー・レベルが存在する可能性があります。ラベルが貼られている場所のカバーを外すことが許されるのはトレーニングを受けたサービス技術員だけです。

S033

警告：
危険な電力が存在します。金属とショートさせると熱を発生し、金属の飛散、やけど、またはその両方を引き起こす可能性のある危険な電力の電圧です。

トップ・カバーを取り外す前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

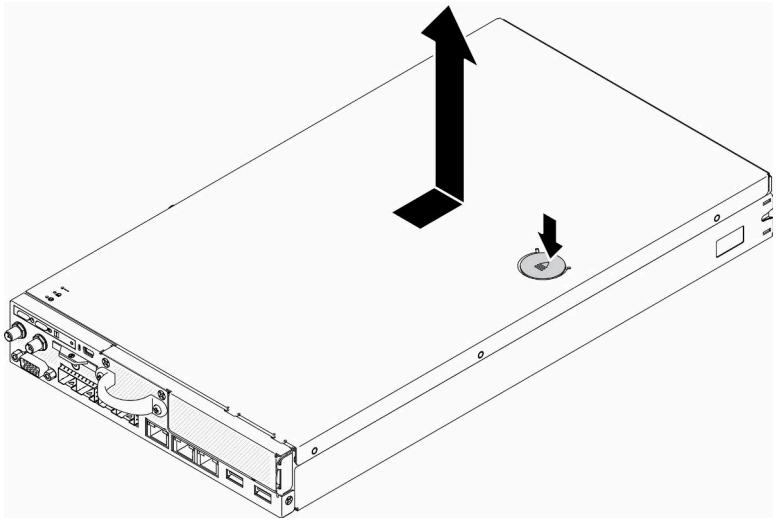


図 27. トップ・カバーの取り外し

ステップ 1. リリース・ボタンおよびプッシュ・ポイントを同時に押した後、カバーをサーバーの後部に向けてスライドさせます。

ステップ 2. トップ・カバーを持ち上げてサーバーから取り外します。

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=7pGlqu5xVNk

エアー・バッフルの取り外し

以下の情報を使用して、エアー・バッフルを取り外します。

起こり得る危険を回避するために、以下の安全の注記をお読みになり、それに従ってください。

- S012

警告：
高温の面が近くにあります。

このエアー・バッフルを取り外す前に、以下のステップを実行します。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。

手順

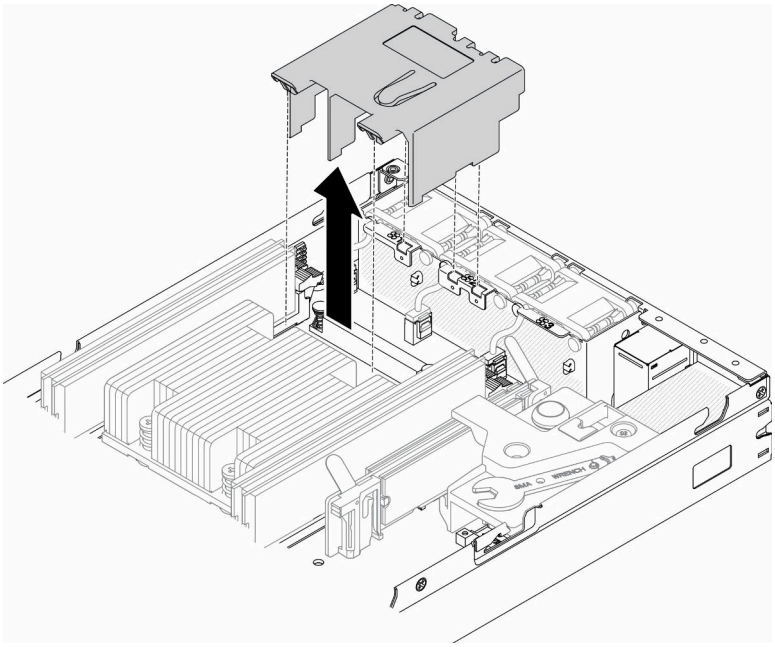


図 28. エアー・バッフルの取り外し

ステップ 1. エアー・バッフルを持ち上げて、横に置きます。

注意：適切な冷却と空気の流れを確保するために、エア・バッフルを再度取り付けてからサーバーの電源をオンにしてください。エアー・バッフルを取り外したままサーバーを作動させると、サーバーのコンポーネントが損傷する可能性があります。

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=Oiu0xpF9-XY

PCIe ライザー・アセンブリーの取り外し

以下の情報を使用して、PCIe ライザー・アセンブリーを取り外します。

起こり得る危険を回避するために、以下の安全の注記をお読みになり、それに従ってください。

- S012

警告：
高温の面が近くにあります。

PCIe ライザー・アセンブリーを取り外す前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。

手順

ステップ 1. 図のように 7 本のねじを取り外します。

ステップ 2. 次に、PCIe ライザー・アセンブリーの端と青色のタブを持ち、慎重に持ち上げてサーバーから取り外します。

注：

1. 以下の図は、ご使用のハードウェアと多少異なる場合があります。
2. PCIe ライザー・アセンブリーを上にまっすぐ慎重に持ち上げます。PCIe ライザー・アセンブリーを大きく傾けないようにしてください。傾けると、コネクターが破損する可能性があります。

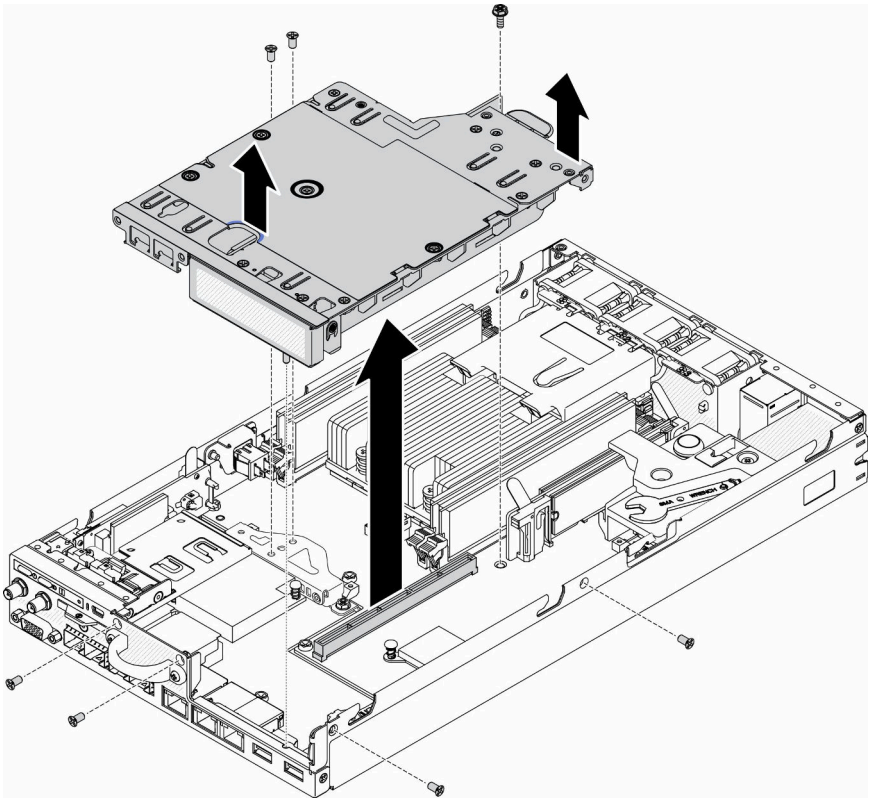


図 29. PCIe ライザー・アセンブリーの取り外し

PCIe ライザー・アセンブリーを取り外したら、以下のステップを実行してください。

1. フィラーを取り付け、3 本のねじを締めます。

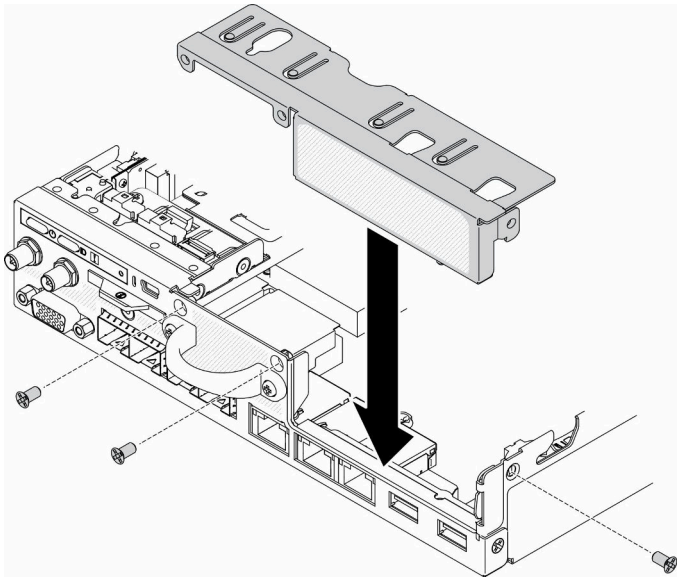


図 30. フィラーの取り付け

2. 不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=TPQz8cyiqGM

前面オペレーター・パネルの取り外し

前面オペレーター・パネルを取り外すには、この情報を使用します。

前面オペレーター・パネルを取り外す前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。
4. 必要に応じて、M.2 WLAN/LTE ワイヤレス・アダプターを取り外します。
5.
6. ロック位置スイッチを取り外します (取り付けられている場合) (49 ページの 「ロック位置スイッチの取り外し」を参照)。

手順

ステップ 1. 金属のプルタブ・ホルダーからケーブルを慎重に取り外します。

ステップ 2. ケーブル・ラッチを慎重に押して、2 つの Y 字コネクターを切り離します。

ステップ 3. ねじを取り外します。

ステップ 4. リリース・タブを引きます。

ステップ 5. 前面オペレーター・パネルをサーバーからスライドさせます。

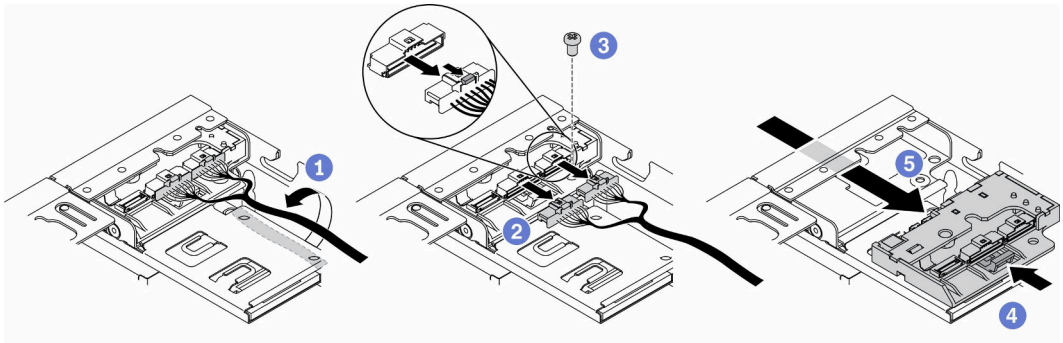


図 31. 前面オペレーター・パネルの取り外し

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=qE1pfiR1T3M

ロック位置スイッチの取り外し

ロック位置スイッチを取り外すには、この情報を使用します。

起こり得る危険を回避するために、以下の安全についてをお読みになり、それに従ってください。

S002

警告：
装置の電源制御ボタンおよびパワー・サプライの電源スイッチは、装置に供給されている電流をオフにするものではありません。デバイスには 2 本以上の電源コードが使われている場合があります。デバイスから完全に電気を取り除くには電源からすべての電源コードを切り離してください。

S009

警告：
けがを避けるため、ファンをデバイスから取り外す場合はファンのケーブルを先に外してください。

ロック位置スイッチを取り外す前に、以下のステップを実行してください。ロック位置スイッチを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。
4. PCIe ライザー・ケージを取り外します (46 ページの 「PCIe ライザー・アセンブリーの取り外し」を参照)。

手順

ステップ 1. ケーブルを切り離します。

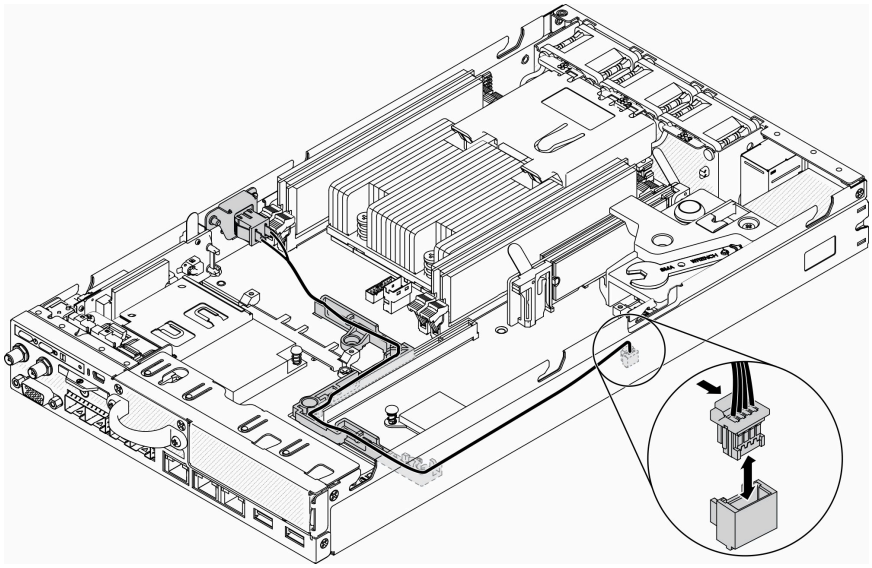


図 32. ロック位置スイッチ・ケーブル

ステップ 2. ねじを取り外します。

ステップ 3. ロック位置のスイッチをわずかに右方向に押し、サーバーから取り外します。

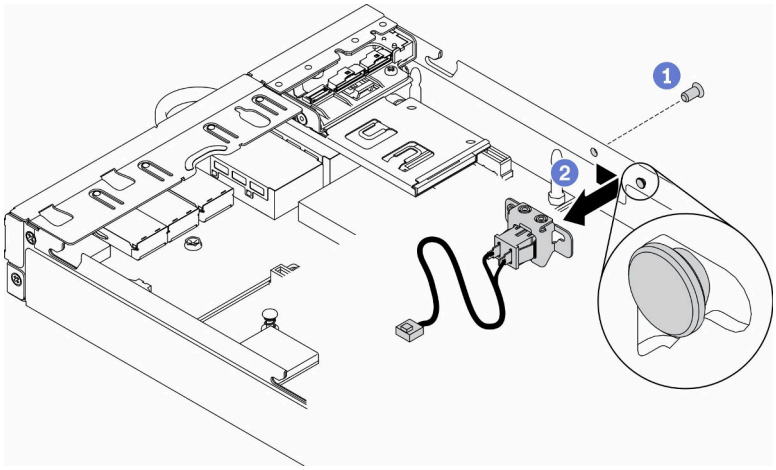


図 33. ロック位置スイッチの取り外し

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=z1Fh-VkIA0A

侵入検出スイッチ・ケーブルの取り外し

侵入検出スイッチ・ケーブルを取り外すには、この情報を使用します。

侵入検出スイッチを取り外す前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。

手順

ステップ 1. 2 つのねじを緩めます。

ステップ 2. ケーブル・ラッチを押し続けます。

ステップ 3. ケーブルをコネクターから切り離します。

ステップ 4. 侵入検出スイッチ・キャリアを慎重に持ち上げてサーバーから取り外します。

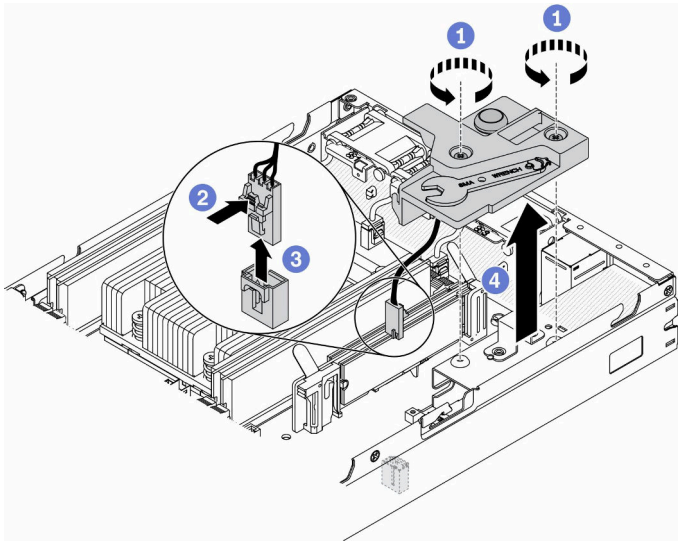


図 34. 侵入検出スイッチ・ケーブルの取り外し

ステップ 5. ケーブルの両側にあるラッチを押したままにします。

ステップ 6. 侵入検出スイッチのケーブルをキャリアから取り外します。

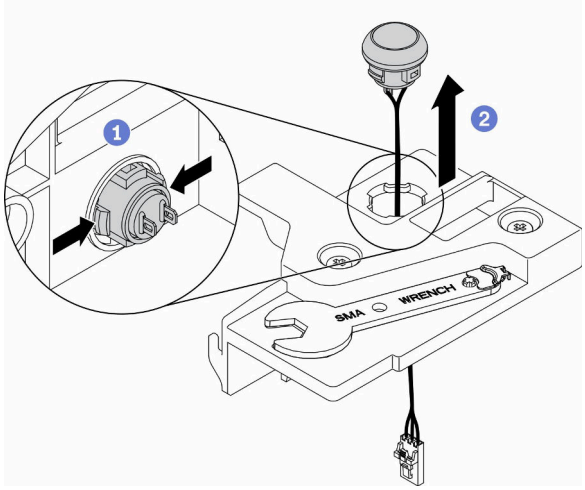


図 35. 侵入検出スイッチ・ケーブルの取り外し

不良部品を返却するように指示された場合は、輸送上の損傷を防ぐために部品を梱包してください。到着した新しい部品の梱包を再利用し、すべての梱包上の指示に従ってください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=MPb1b7dJCjY

電源アダプターの取り付け

電源アダプターを取り付けるには、この情報を使用します。

製品の外部電源に関する欧州議会および理事会の指令 2009/125/EC および委員会規則 (EC) No 278/2009 (ErP Lot7)を撤廃して、外部電源のエコデザイン要件を定める 2019 年 10 月 1 日の委員会規制 (EU) 2019/1782 の要件に準拠しています。

表 18. ThinkEdge 240W 230V/115V 外部パワー・サプライ

公開された情報	値と精度	単位
製造元の名前	Lenovo	-
モデル ID	FSP240-A12C14	-
入力電圧	100-240	V
入力 AC 周波数	50-60	Hz
出力電圧	12.2	V
出力電流	20.0	A
出力電力	240.0	W
平均アクティブ効率	92.73	%
低負荷での効率 (10%)	87.35	%
無負荷での消費電力	0.13	W

表 19. ThinkEdge 240W 230V/115V 外部パワー・サプライ v2

公開された情報	値と精度	単位
製造元の名前	Lenovo	-
モデル ID	GA240SD1-12020000	-
入力電圧	100-240	V
入力 AC 周波数	50-60	Hz
出力電圧	12.2	V
出力電流	20.0	A
出力電力	240.0	W
平均アクティブ効率	93.21	%
低負荷での効率 (10%)	79.0	%
無負荷での消費電力	0.097	W

電源アダプターを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要に応じてノードをエンクロージャーから取り外します (40 ページの 「ノードの取り外し」を参照)。

警告：

- **ノードへの電源アダプターは、同じブランド、電源定格、ワット数、または効率レベルでなければなりません。**
- **電源アダプターを区別するには、電源アダプターのサイズ、コネクターの位置、およびラベルを確認します。**

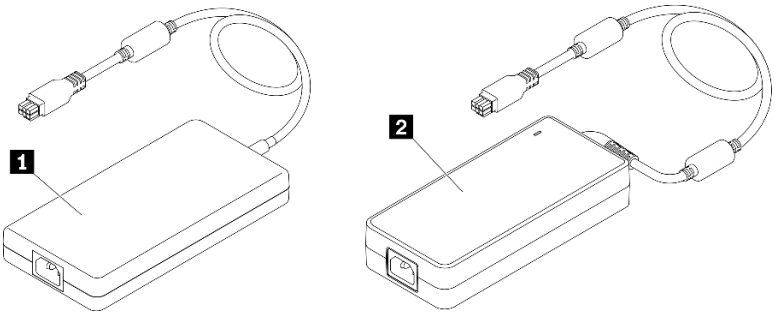


表 20. 電源アダプター

1 ThinkEdge 240W 230V/115V 外部パワー・サプライ	**2** ThinkEdge 240W 230V/115V 外部パワー・サプライ v2

注：電源アダプターの違いを確認するには、電源コネクターの物理サイズ、ラベル、およびコネクター位置で確認できます。

図 36. 電源アダプター

手順

ステップ 1. 電源アダプターを取り付けます。

- ノードがエンクロージャーに取り付けられているときに電源アダプターを取り付ける場合は、以下のステップを実行してください。
  1. 電源アダプターをケージに挿入します。
     - E1 エンクロージャー (1U 2 ノード)

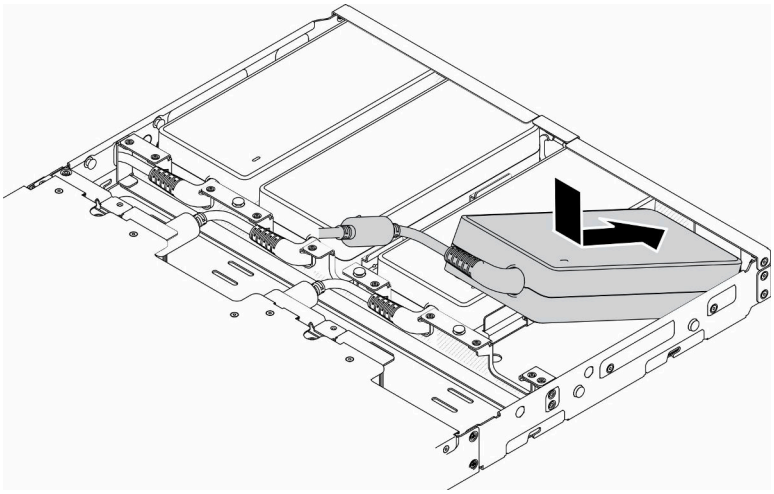


図 37. 電源アダプターの取り付け

     - E2 エンクロージャー (2U 2 ノード)

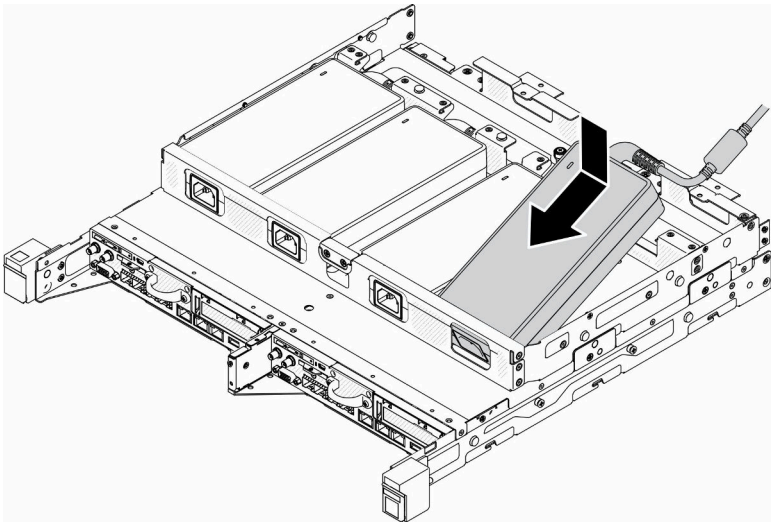


図 38. 電源アダプターの取り付け

  2. ブラケットを後方に少し押し、ブラケットを取り付けます。
  3. 2 個のねじを取り付けます。
     - E1 エンクロージャー (1U 2 ノード)

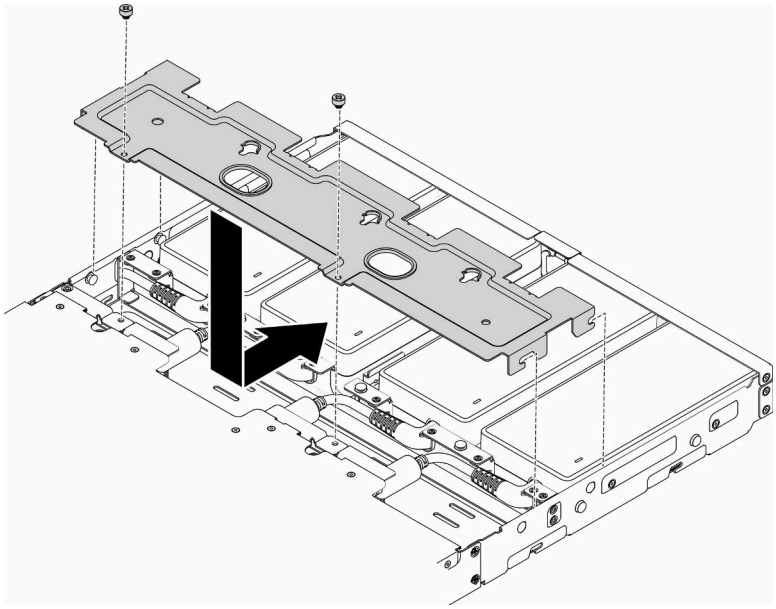


図 39. ブラケットの取り付け

– E2 エンクロージャー (2U 2 ノード)

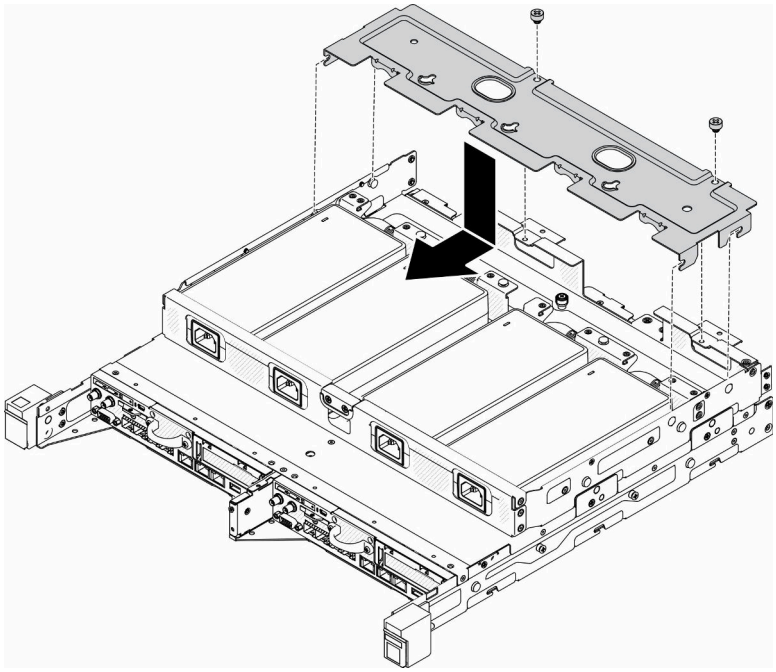


図 40. ブラケットの取り付け

- 電源アダプターを電源アダプター・ブラケットに取り付ける場合は、次の手順を実行します。
  1. 電源アダプターを電源アダプター・ブラケットに合わせます。次に、電源アダプターを所定の位置にスライドさせます。

2. タブをスロットに合わせ、タブを慎重に所定の位置に引っ掛けます。
3. つまみねじを締めます。

注：DIN レール構成、壁掛け用構成の取り付けの詳細については、必要に応じて、「*構成部品取り付けガイド*」を参照してください。

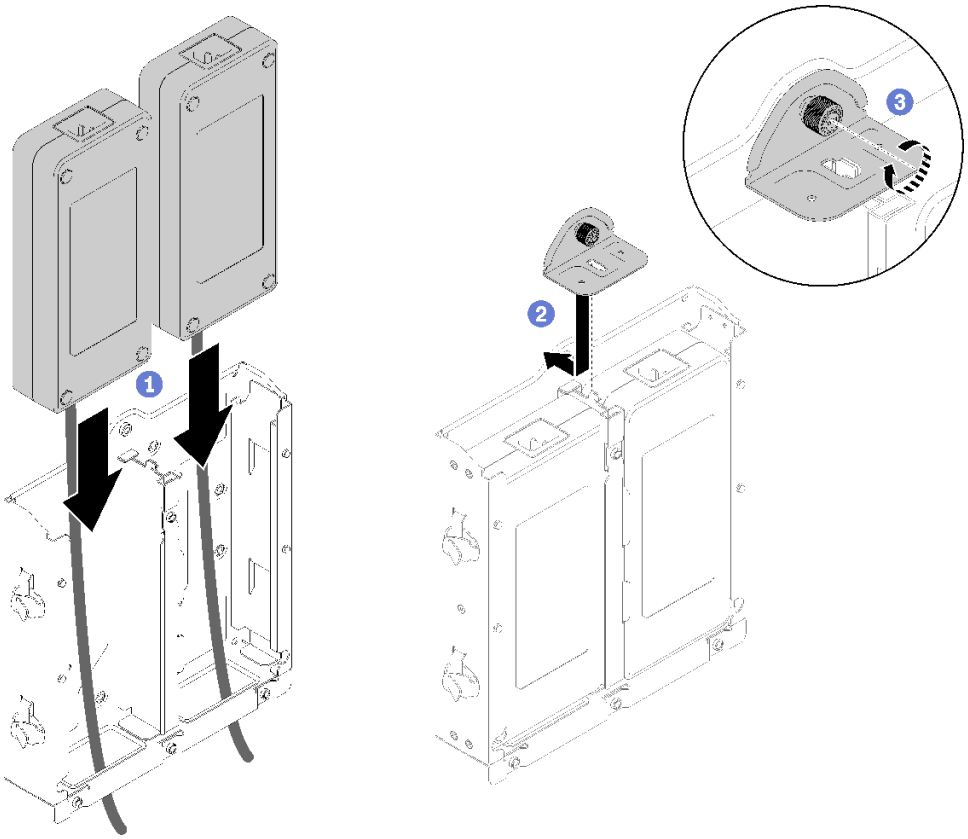


図 41. 電源アダプターの取り付け

1. 必要に応じて、エンクロージャーをラックの中に取り付けます。
2. DIN レール構成、壁掛け用構成の取り付けの詳細については、必要に応じて、「*構成部品取り付けガイド*」を参照してください。
3. 電源コードおよびすべての外部ケーブルを再接続します。
4. サーバーの電源をオンにします (78 ページの 「サーバーの電源をオンにする」を参照)。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=MyPVTlRwTkk

M.2 ブート・アダプターの取り付け

M.2 ブート・アダプターを取り付けるには、この情報を使用します。

M.2 ブート・アダプターを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」

2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの「サーバーの電源をオフにする」を参照)。

重要：

- VMware ESXI のブート・ドライブ: VMware ESXi ブート・サポートの場合、特定の M.2 ドライブのみが、その耐久性に基づいてサポートされます。特定の情報については、Lenovo サポートのヘルプ HT512201 を参照してください。
- アダプターの反対側にある M.2 ドライブのペアは、同じマウント・クリップを共有するため、同じフォーム・ファクター (つまり、同じ物理長) である必要があります。

  M.2 ドライブおよびスロットの番号について詳しくは、27 ページの「M.2 ドライブおよびスロットの番号」を参照してください。

M.2 アダプターの詳細については、https://lenovopress.com/lp0769-thinksystem-m2-drives-adapters を参照してください。

手順

ステップ 1. M.2 ブート・アダプターの位置を、システム・ボード上のコネクターと合わせ、コネクターにアダプターをまっすぐ押し込みます。

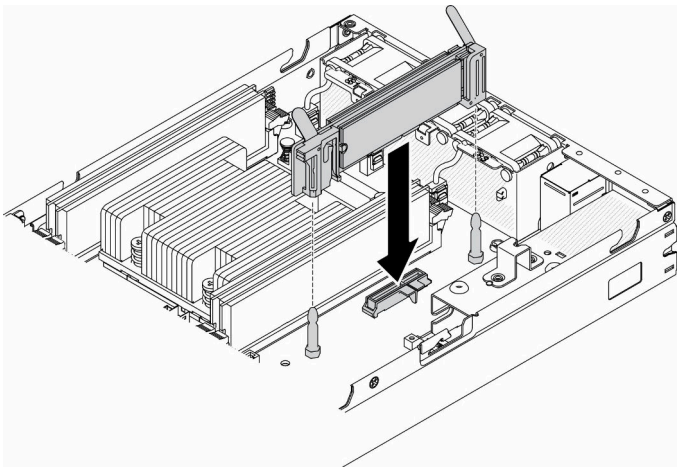


図 42. M.2 ブート・アダプターの取り付け

M.2 ブート・アダプターを取り付けた後、以下のステップを実行してください。

1. 侵入検出スイッチを取り付けます (66 ページの「侵入検出スイッチ・ケーブルの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=UQCntTJVQ_o

M.2 データ・アダプターの取り付け

M.2 データ・アダプターを取り付けるには、この情報を使用します。

M.2 データ・アダプターを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

注：M.2 ドライブおよびスロットの番号について詳しくは、27 ページの 「M.2 ドライブおよびスロットの番号」を参照してください。

手順

ステップ 1. M.2 データ・アダプターをライザー・カード上のスロットと合わせて挿入します。次に、M.2 データ・アダプターを完全に装着されるまでスロットにまっすぐ慎重に押し込みます。

ステップ 2. ねじを取り付けます。

- M.2 ライザー・アセンブリー

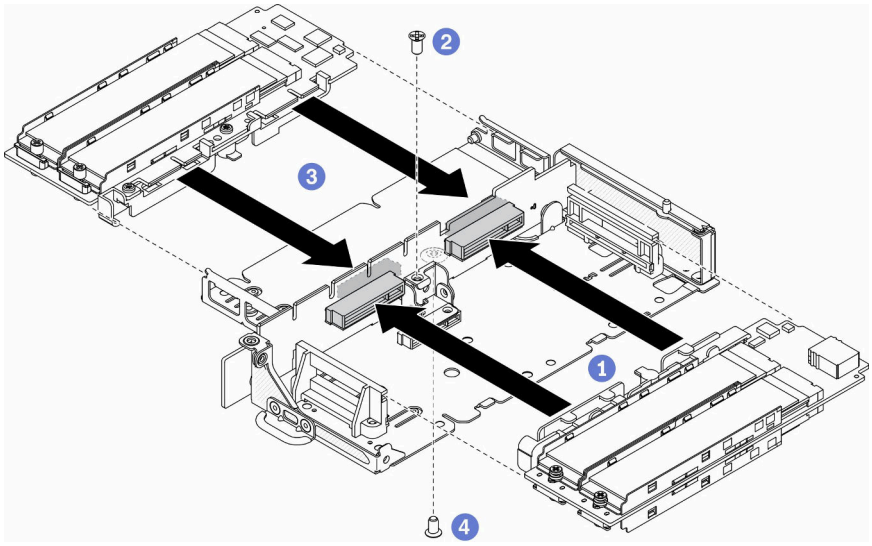


図 43. M.2 データ・アダプターの取り付け

- PCIe および M.2 ライザー・アセンブリー

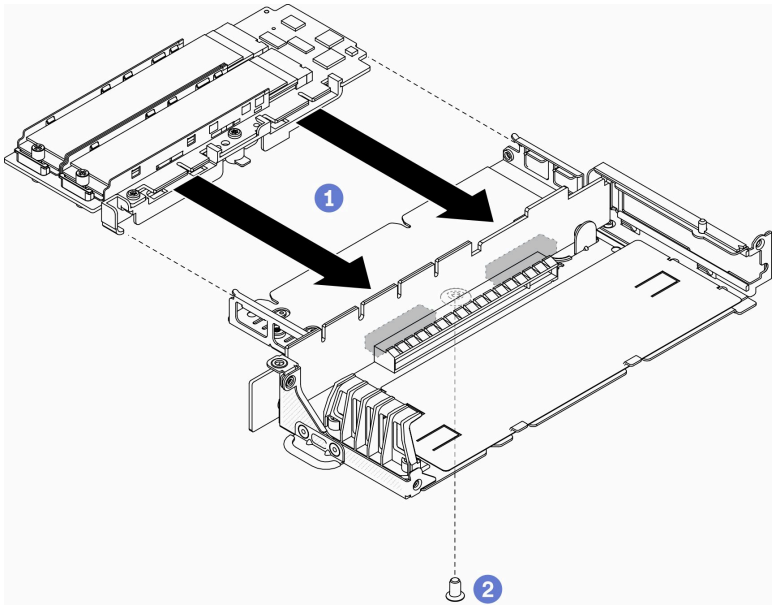


図 44. M.2 データ・アダプターの取り付け

ステップ 3. ベゼルを両側のライザー・アセンブリーに挿入し、図のように 6 本のねじを取り付けます。

注：両側のねじの色およびサイズが異なる場合は、必ず、短いものを左側に、長いものを右側に取り付けるようにします。

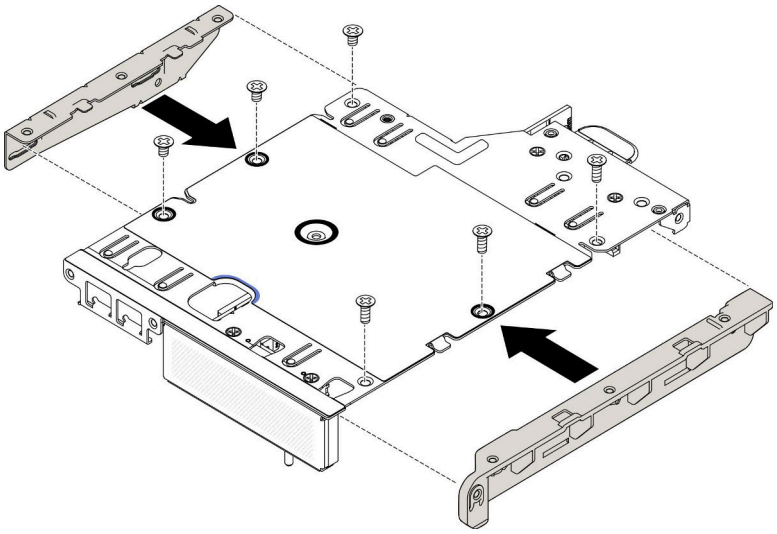


図 45. M.2 データ・アダプターの取り付け

M.2 データ・アダプターを取り付けたら、次のステップを実行してください。

1. PCIe ライザー・アセンブリーを取り付けます (手順については、64 ページの 「PCIe ライザー・アセンブリーの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=bucg3_aMYLY

M.2 WLAN/LTE ワイヤレス・アダプターの取り付け

M.2 WLAN/LTE ワイヤレス・アダプターを取り付けるには、この情報を使用します。

M.2 WLAN/LTE ワイヤレス・アダプターを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

注：

- LTE および WLAN のパフォーマンスは、構成や環境に応じて変化する場合があります。
- サーバーのワイヤレス・アダプターには 2 つのタイプがありますが、両方を同時に使用することはできません。どちらも取り付け方法は同じです:
  - M.2 WLAN/LTE ワイヤレス・アダプターは、WLAN と 4G LTE のモジュールに付属しています。
  - M.2 WLAN ワイヤレス・アダプターは、WLAN モジュールにのみ付属しています。
- WLAN/LTE モジュールの欠落、取り外し、欠陥によって、システム・エラー・イベントが起きる可能性があります。

WLAN/LTE 構成エラー・イベントが発生した場合は、以下の手順を実行してください。

1. システム・ファームウェア (UEFI、XCC 等) およびスイッチ・ボードのファームウェアが最新であることを確認します。
2. システムの電源をオフにして、WLAN/LTE モジュールが正しく取り付けられているかどうかを確認し、必要に応じて再取り付けします。サーバー操作には WLAN/LTE モジュールが必要です。
3. 取り付けをやり直した後でもエラー・メッセージが表示される場合は、モジュールを交換します。この場合、モジュールに障害がある可能性があります。

手順

ステップ 1. M.2 ワイヤレス・アダプターの位置を、システム・ボード上のコネクターと合わせ、コネクターにアダプターをまっすぐ押し込みます。

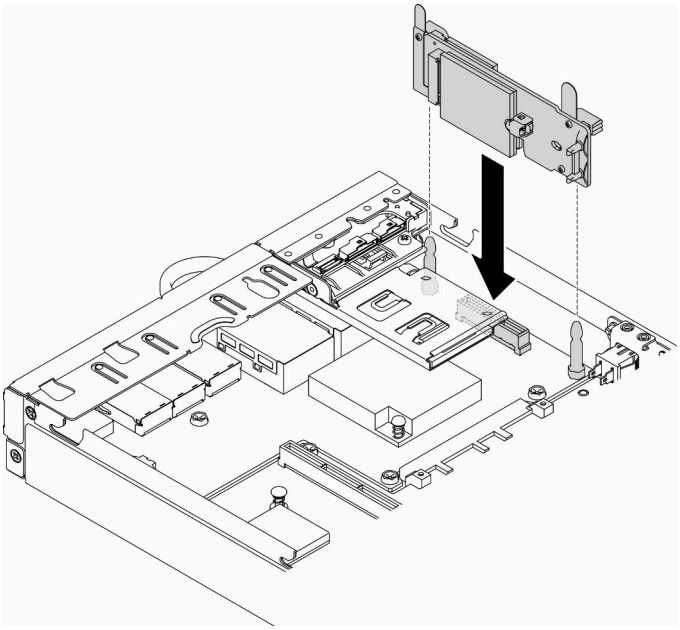


図 46. M.2 WLAN/LTE ワイヤレス・アダプターの取り付け

M.2 WLAN/LTE ワイヤレス・アダプターを取り付けたら、以下のステップを実行してください:

1. ロック位置スイッチを取り付けます (取り外した場合) (70 ページの 「ロック位置スイッチの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=T3SEbjlZYCI

SIM カードの取り付け

SIM カードを取り付けるには、この情報を使用します。

SIM カードを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

注 : LTE を有効にするには、SIM カードを取り付ける必要があります。LTE サービスは、それぞれの国または地域で認可されたモバイル・サービス・キャリアによって提供されます。LTE ネットワークに接続するには、サーバーにサービス・キャリアからのセルラー・プランが必要です。

手順

ステップ 1. M.2 WLAN/LTE ワイヤレス・アダプターで SIM カードの位置を確認します。

ステップ 2. 保持カバーを後方にスライドさせて、上に回転します。

ステップ 3. SIM カードをスロットに慎重に置きます。

ステップ 4. 保持カバーを下に回転して、前方にスライドさせます。

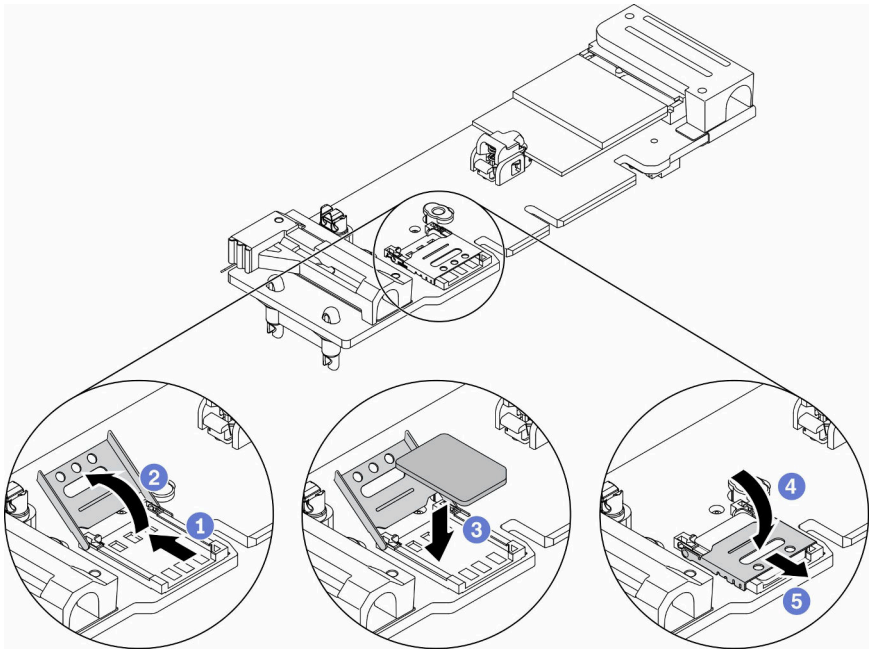


図 47. SIM カードの取り付け

SIM カードを取り付けた後、以下のステップを実行してください。

1. M.2 WLAN/LTE ワイヤレス・アダプターを取り付けます (60 ページの 「M.2 WLAN/LTE ワイヤレス・アダプターの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。
4. セットアップ・プロセスに従って、SIM カードを有効にします。

   注：通信事業者または SIM プロバイダーから PIN コード、APN、その他の設定を入手して、安全な場所に保管してください。

   - PIN コード
     - SIM カードのピン・コードが必要な場合は、次のコマンド・ラインを使用します (PIN コードの例として 1234 を使用します)。

       ```
       sudo uci set network.lte_wan.pincode='1234'
       sudo uci commit network
       sudo /etc/init.d/network restart
       ```

     - SIM カードのピン・コードを必要としない場合は、次のコマンド・ラインを使用します。

       ```
       sudo uci del network.lte_wan.pincode
       sudo uci del network.lte_wan.auth
       sudo uci del network.lte_wan.username
       sudo uci commit network
       ```

```
sudo reboot
```

- APN:
  - APN 設定が必要な場合は、次のコマンドラインを使用します (APN の例として 1234 を使用)。

```
sudo uci set network.lte_wan.apn='1234'
sudo uci commit network
sudo reboot
```

  - APN 設定を必要としない場合は、次のコマンド・ラインを使用します。

```
sudo uci set network.lte_wan.apn='internet'
sudo uci commit network
sudo reboot
```

注：LTE 設定について詳しくは、101 ページの「ワイヤレス LOM パッケージ構成の組み込みスイッチ CLI」の「**LTE 設定の構成**」を参照してください。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=izsv4NKEj_E

PCIe アダプターの取り付け

PCIe アダプターを取り付けるには、この情報を使用します。

起こり得る危険を回避するために、以下の安全の注記をお読みになり、それに従ってください。

- S012

警告：
高温の面が近くにあります。

PCIe アダプターを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの「サーバーの電源をオフにする」を参照)。

手順

ライザー・アセンブリーの背面にあるフィラーを取り外します。アダプター保持具のねじを取り外して、アダプターを取り外します。

ステップ 1. アダプターをライザー・カード上のスロットと合わせて挿入します。次に、アダプターを完全に装着されるまでスロットにまっすぐ慎重に押し込みます。

ステップ 2. アダプターのねじを取り付けます。

ステップ 3. アダプター保持具のねじを取り付けます。

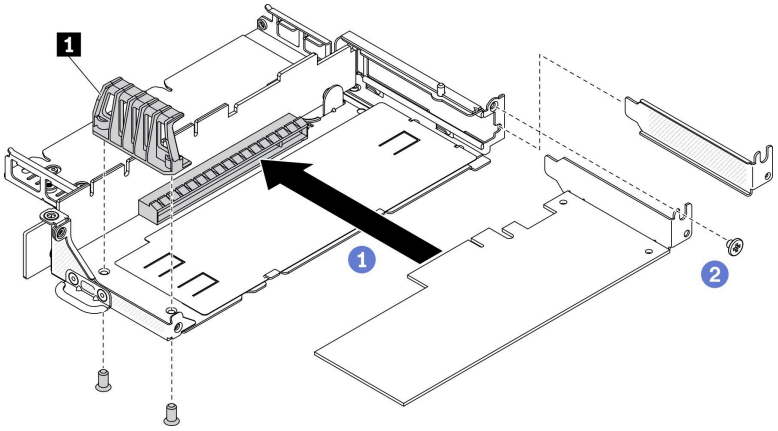


図 48. PCIe アダプターの取り付け

表 21. PCIe アダプターの取り付け

1	アダプター保持具

PCIe アダプターを取り付けた後、以下のステップを実行します。

1. PCIe ライザー・アセンブリーを取り付けます (手順については、64 ページの 「PCIe ライザー・アセンブリーの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。
4. L4 GPU を取り付ける場合は、必ずシステム・ファームウェアを最新バージョンに更新してください (84 ページの 「ファームウェアの更新」)。

PCIe ライザー・アセンブリーの取り付け

以下の情報を使用して、PCIe ライザー・アセンブリーを取り付けます。

起こり得る危険を回避するために、以下の安全の注記をお読みになり、それに従ってください。

- S012

警告：
高温の面が近くにあります。

PCIe ライザー・アセンブリーを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 必要なアダプターを取り付けます。
4. フィラーが取り付けられている場合は取り外します。

a. 3 本のねじを取り外します。
b. 次に、フィラーの端を持ち、慎重に持ち上げてサーバーから取り外します。

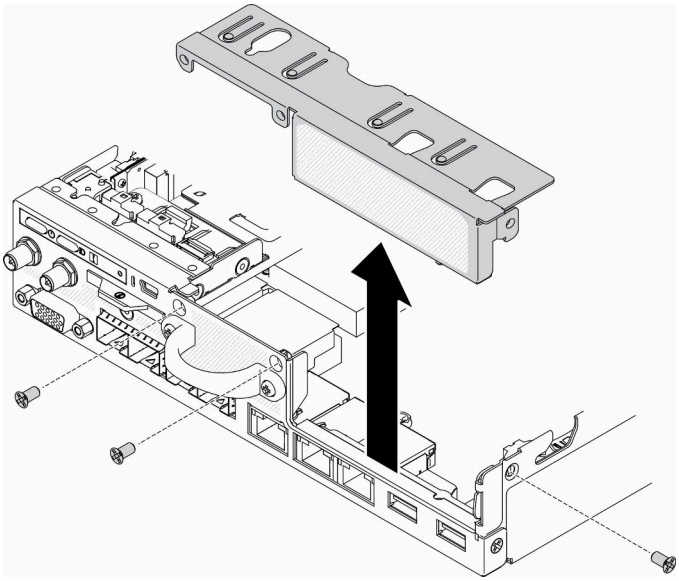


図 49. フィラーの取り外し

手順

ステップ 1. アダプター・ブラケットが取り付けられていない場合は、図のように 2 本のねじを固定して取り付けます。

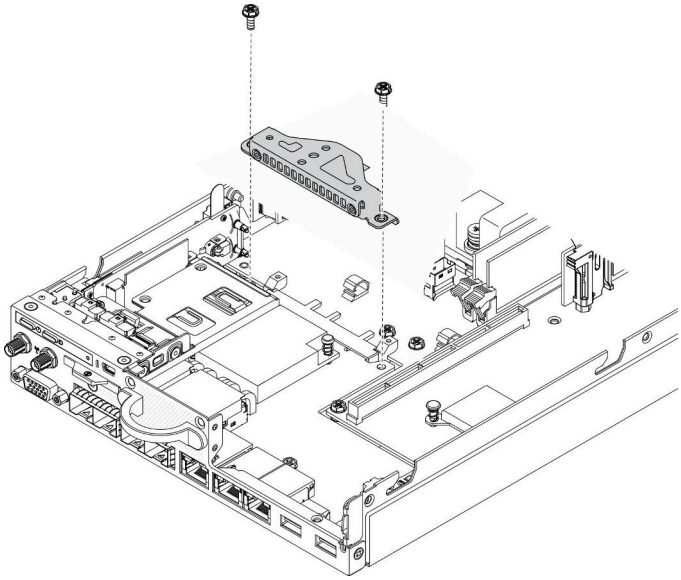


図 50. PCIe ライザー・アセンブリーの取り付け

ステップ 2. PCIe ライザー・アセンブリーをシャーシに下げ、しっかり固定されるまで PCIe ライザー・アセンブリーを押し下げます。

ステップ 3. 7 本のねじを取り付けます。

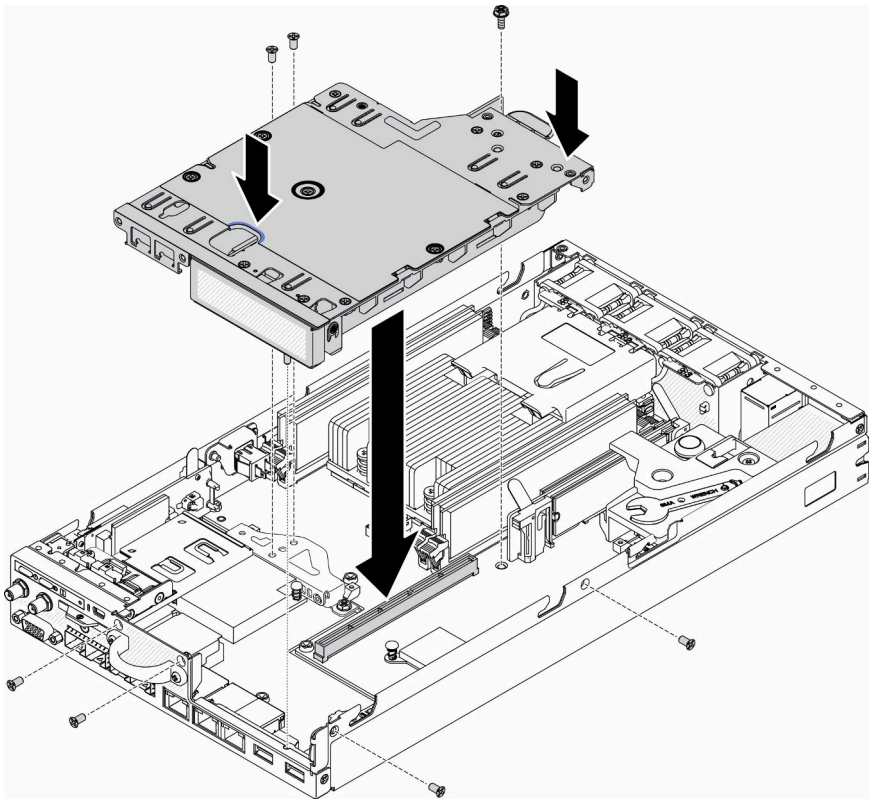


図 51. PCIe ライザー・アセンブリーの取り付け

PCIe ライザー・アセンブリーを取り付けた後、以下のステップを実行してください。

1. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
2. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=gb2GUg6zM5U

侵入検出スイッチ・ケーブルの取り付け

侵入検出スイッチ・ケーブルを取り付けるには、この情報を使用します。

侵入検出スイッチを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

キャリアの穴を通して侵入検出スイッチ・ケーブルを挿入します。

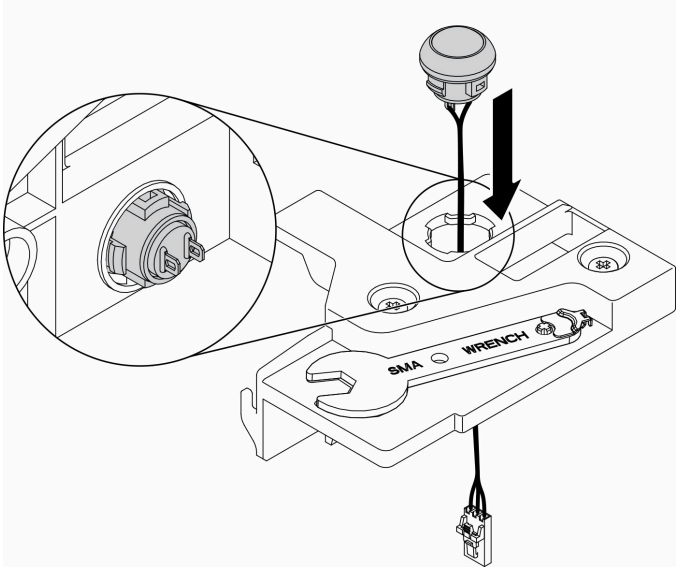


図 52. 侵入検出スイッチ・ケーブルの取り付け

ステップ 1. 侵入検出スイッチ・キャリアをシャーシ内に収め、しっかり固定されるまで侵入検出スイッチ・キャリアを押します。

ステップ 2. 2 個のねじを締めます。

ステップ 3. ケーブルをコネクターに接続し、カチッと音がするまで下に押します。

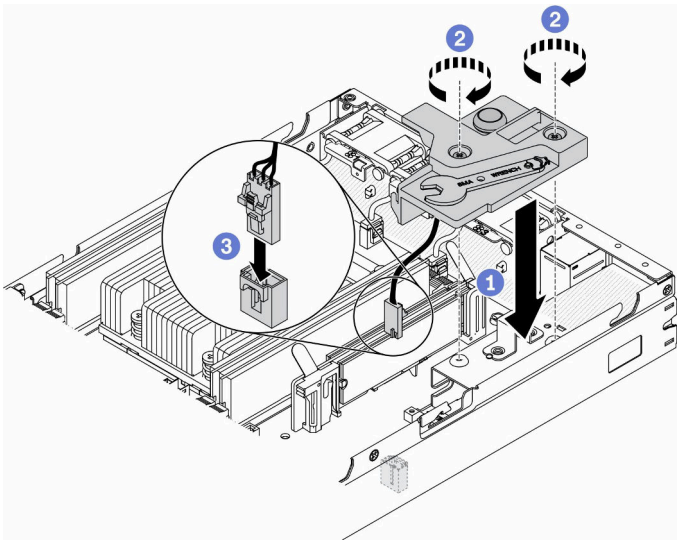


図 53. 侵入検出スイッチの取り付け

侵入検出スイッチを取り付けたら、次のステップを実行してください。

1. 必要に応じてノードを取り付けます (74 ページの「ノードの取り付け」を参照)。
2. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=NREyfSHp0so

DIMM の取り付け

DIMM を取り付けるには、この情報を使用します。

メモリーの構成およびセットアップについて詳しくは、38 ページの 「メモリー・モジュールの取り付けの規則および順序」を参照してください。

DIMM を取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. コンポーネントが入っている帯電防止パッケージをサーバーの塗装されていない金属面に接触させてから、コンポーネントをパッケージから取り出し、帯電防止面の上に置きます。

次の図は、システム・ボード・コンポーネント (DIMM コネクターを含む) を示しています。

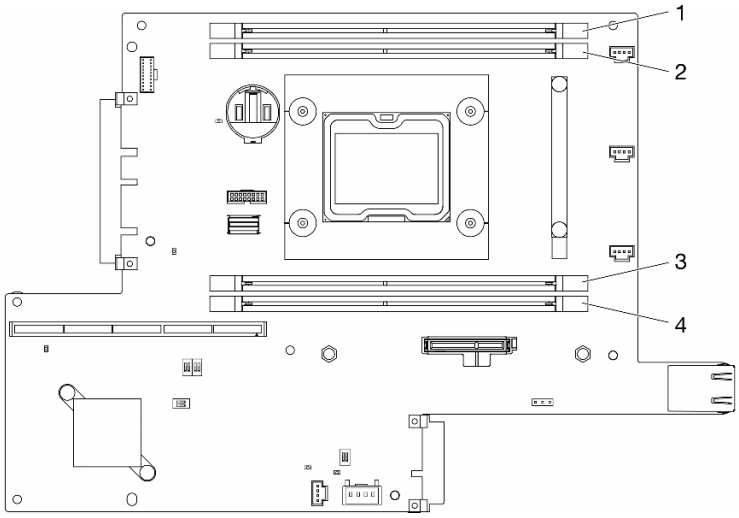


図 54. DIMM コネクター

DIMM を取り付けるには、次のステップを実行してください。

注意：メモリー・モジュールは静電気放電の影響を受けやすく、特別な取り扱いが必要です。38 ページの 「静電気の影響を受けやすいデバイスの取り扱い」の標準のガイドラインに加え、以下の指示に従ってください。

- メモリー・モジュールの取り外しまたは取り付けの際には、必ず静電放電ストラップを着用してください。静電気放電グローブも使用できます。
- 2 つ以上のメモリー・モジュールを接触させないでください。保管中にメモリー・モジュールを直接重ねて積み重ねないでください。
- 金色のメモリー・モジュール・コネクターの接点に触れたり、これらの接点をメモリー・モジュール・コネクターのエンクロージャーの外側に接触させたりしないでください。
- メモリー・モジュールを慎重に扱ってください。メモリー・モジュールを曲げたり、ねじったり、落としたりしないでください。

手順

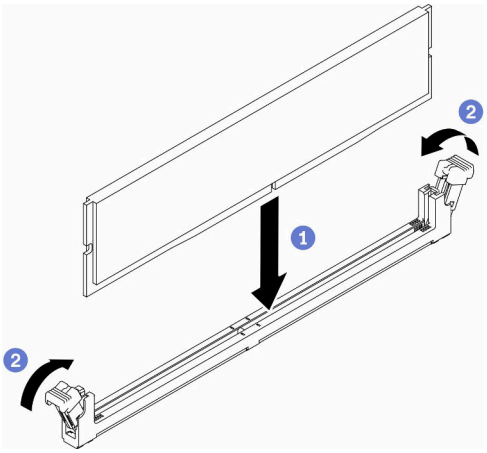


図 55. DIMM の取り付け

ステップ 1. 保持クリップが完全に開いた位置にあることを確認し、DIMM 上のキーをコネクターに合わせます。

ステップ 2. 保持クリップがロック位置にはまるまで DIMM の両端を、強く真っすぐに押し下げて、コネクターに取り付けます。

ステップ 3. 追加の DIMM を取り付ける場合は、ここで実行してください。

DIMM を取り付けた後、以下のステップを実行してください。

1. エアー・バッフルを取り外した場合は、再取り付けします (72 ページの 「エアー・バッフルの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=rdNqcD88sKs

前面オペレーター・パネルの取り付け

前面オペレーター・パネルを取り付けるには、この情報を使用します。

前面オペレーター・パネルを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

ステップ 1. 前面オペレーター・パネルをアセンブリー・ベイにスライドさせます。

ステップ 2. ねじを取り付けて前面オペレーター・パネルを固定します。

ステップ 3. 2 本の Y 字ケーブル・コネクターを慎重に接続します。

ステップ 4. 金属のプルタブ・ホルダーの下にケーブルを慎重に配線します。

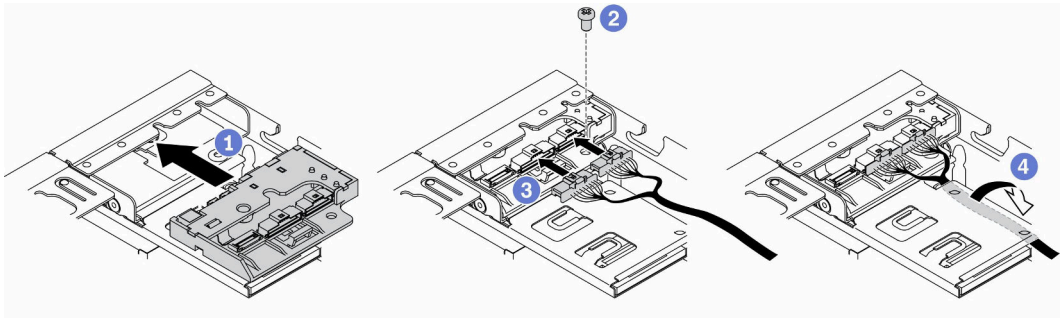


図 56. 前面オペレーター・パネルの取り付け

前面オペレーター・パネルを取り付けたら、以下のステップを実行してください。

1. 必要に応じて、M.2 WLAN/LTE ワイヤレス・アダプターを取り付けます。
2.
3. ロック位置スイッチを取り付けます (取り外した場合) (70 ページの 「ロック位置スイッチの取り付け」を参照)。
4. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
5. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=brfIcu2bLa8

ロック位置スイッチの取り付け

ロック位置スイッチを取り付けるには、この情報を使用します。

ロック位置スイッチを取り付ける前に、次のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

ステップ 1. ロック位置スイッチをピンに引っ掛けた後、左に少し押します。

ステップ 2. ねじを取り付けて締めます。

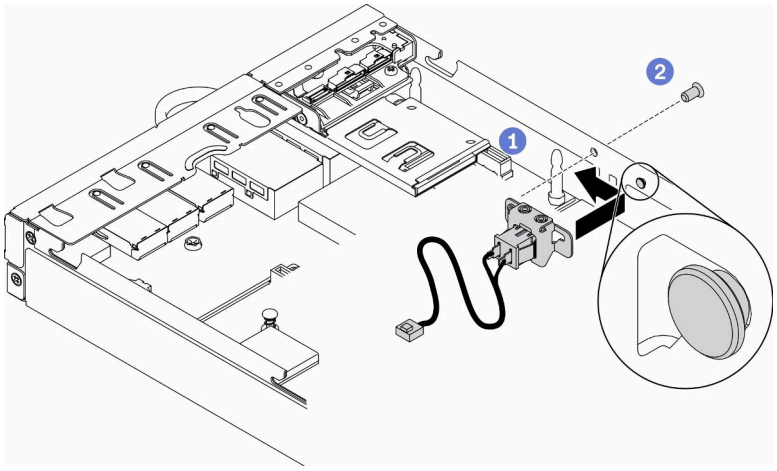


図 57. ロック位置スイッチの取り付け

ステップ 3. 次の図に示すようにケーブルを慎重に配線し、コネクターを接続します。

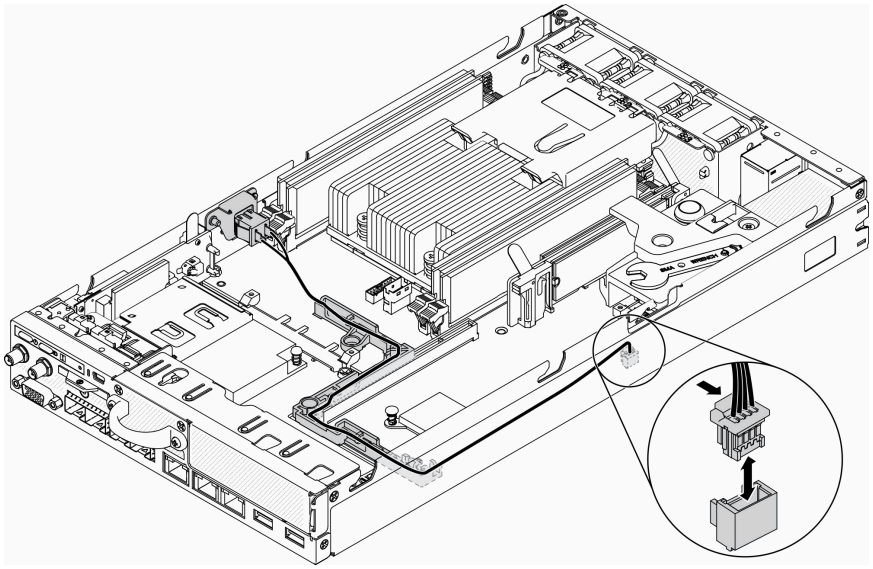


図 58. ロック位置スイッチ・ケーブル

ロック位置スイッチを取り付けたら、次のステップを実行してください。

1. PCIe ライザー・ケージを再び取り付けます (64 ページの 「PCIe ライザー・アセンブリーの取り付け」を参照)。
2. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
3. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=6kb5ahC0UFs

エアー・バッフルの取り付け

以下の情報を使用して、エアー・バッフルを取り付けます。

起こり得る危険を回避するために、以下の安全の注記をお読みになり、それに従ってください。

- S012

警告：
高温の面が近くにあります。

このエアー・バッフルを取り付ける前に、以下のステップを実行します。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。

手順

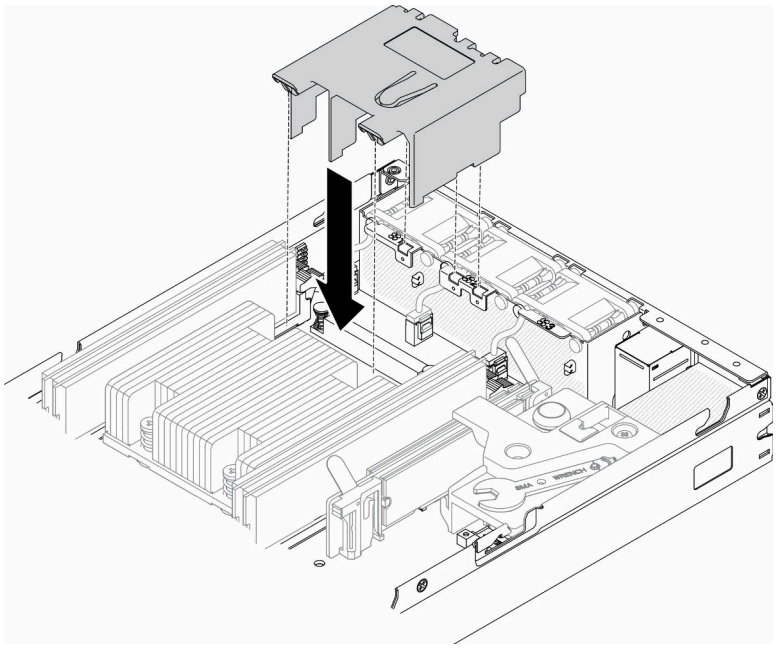


図 59. エアー・バッフルの取り付け

ステップ 1. エアー・バッフルの両側のタブを対応するスロットに合わせます。次に、エアー・バッフルをシャーシに下ろし、しっかりと固定されるまでエアー・バッフルを押し下げます。

このエアー・バッフルを取り付けたら、以下のステップを実行します。

1. 必要に応じてノードを取り付けます (74 ページの 「ノードの取り付け」を参照)。
2. 電源コードおよびすべての外部ケーブルを再接続します。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=5HpaVy2ZgOM

トップ・カバーの取り付け

トップ・カバーを取り付けるには、この情報を使用します。

起こり得る危険を回避するために、以下の安全についてをお読みになり、それに従ってください。

S012

警告：
高温の面が近くにあります。

S014

警告：
危険な電圧、電流、エネルギー・レベルが存在する可能性があります。ラベルが貼られている場所のカバーを外すことが許されるのはトレーニングを受けたサービス技術員だけです。

S033

警告：
危険な電力が存在します。金属とショートさせると熱を発生し、金属の飛散、やけど、またはその両方を引き起こす可能性のある危険な電力の電圧です。

このトップ・カバーを取り付ける前に、以下のステップを実行します。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」
2. サーバーの電源を切ります。電源コードとすべての外部ケーブルを取り外します (78 ページの 「サーバーの電源をオフにする」を参照)。
3. 取り外したコンポーネントがすべて取り付けられ、サーバー内の切り離したケーブルがすべて再接続されていることを確認してください。

手順

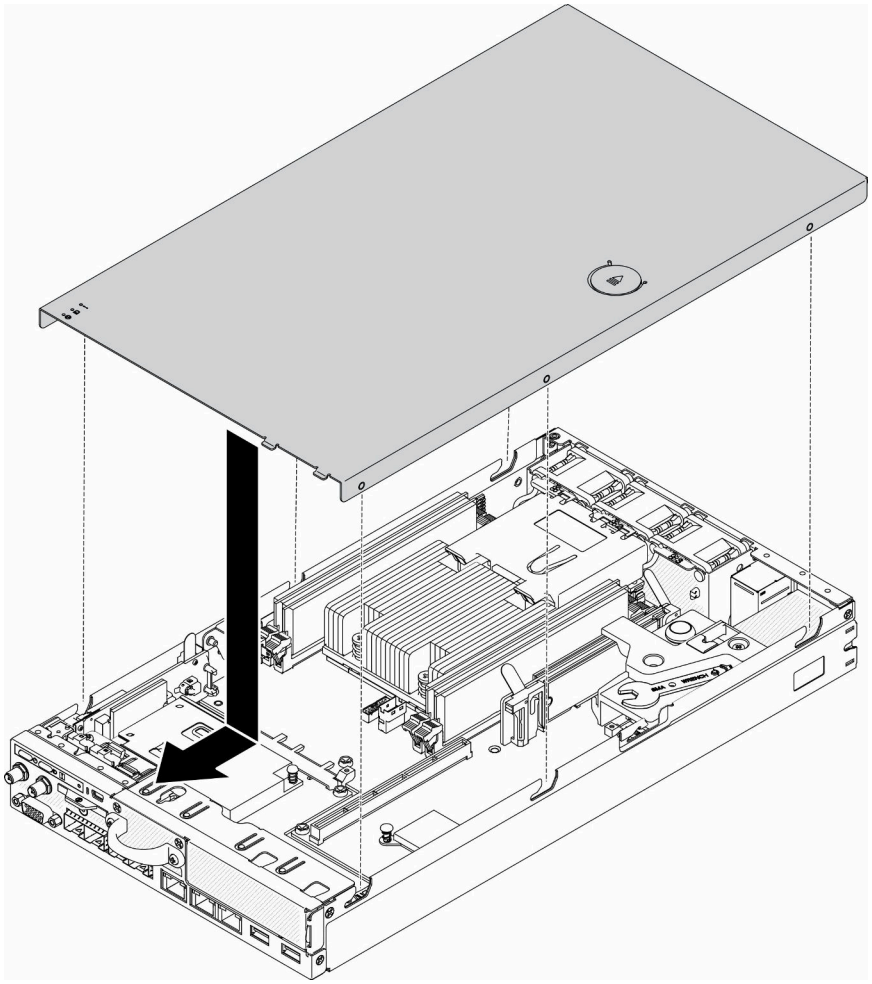


図 60. トップ・カバーの取り付け

ステップ 1. トップ・カバー内のポストをシャーシのスロットと位置合わせします。

ステップ 2. サーバーの前部を持ち、カチッと音がして所定の位置に収まるまでトップ・カバーをサーバー前面の方向にスライドさせます。

トップ・カバーを取り付けた後、以下のステップを実行してください。

1. 電源コードおよびすべての外部ケーブルを再接続します。
2. サーバーの電源をオンにします (78 ページの 「サーバーの電源をオンにする」を参照)。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=84O4Mv7aaiw

ノードの取り付け

ノードを取り付けるには、この情報を使用します。

ノードを取り付ける前に、以下のステップを実行してください。

1. 安全に作業を行うために、以下のセクションをお読みください。
   - 36 ページの 「取り付けのガイドライン」

2. 取り外したコンポーネントがすべて取り付けられ、サーバー内の切り離したケーブルがすべて再接続されていることを確認してください。

手順

ステップ 1. ノード・スリーブにノードを取り付けるには、以下の手順を実行します。

a. ノードをノード・スリーブに合わせ、ノードを所定の位置にスライドさせます。

b. 2 本のつまみねじを締めます。

注：ブックシェルフ構成、DIN レール構成、壁掛け用構成の取り付けの詳細については、必要に応じて、「*構成部品取り付けガイド*」を参照してください。

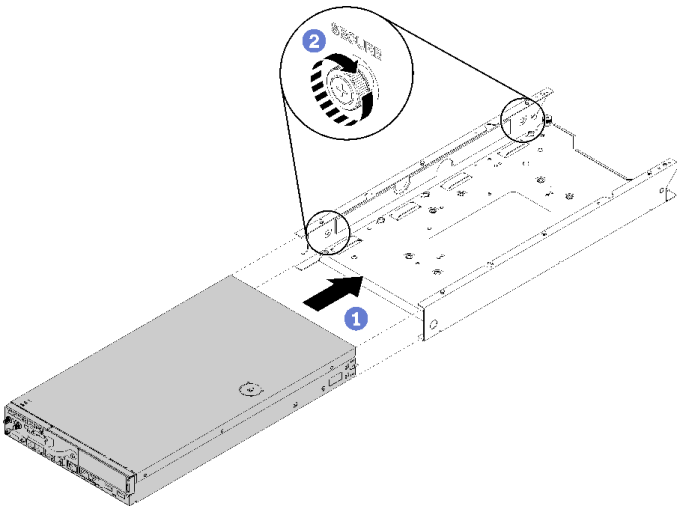


図 61. ノードの取り付け

ステップ 2. エンクロージャーにノードを取り付けるには、以下の手順を実行します。

注意：ノードを E1 エンクロージャー (1U 2 ノード) に取り付ける場合、適切に動作させるには重要プロダクト・データ (VPD) を変更してください。「*メンテナンス・マニュアル*」の「*E1 エンクロージャー構成の VPD の変更 (トレーニングを受けた技術員のみ)*」を参照してください。

a. ノードを取り付けるためのノード・ベイを決定します。

b. ノードを止まるまでノード・ベイに差し込みます。

- E1 エンクロージャー (1U 2 ノード)

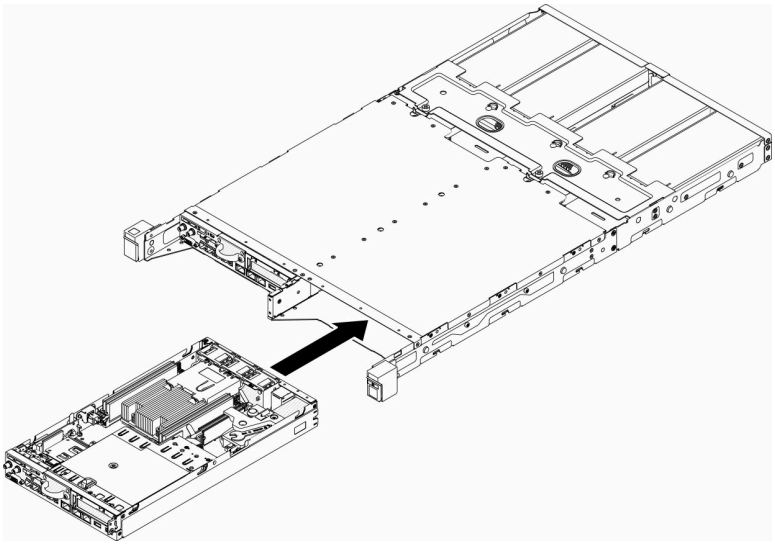


図 62. ノードの取り付け

- E2 エンクロージャー (2U 2 ノード)

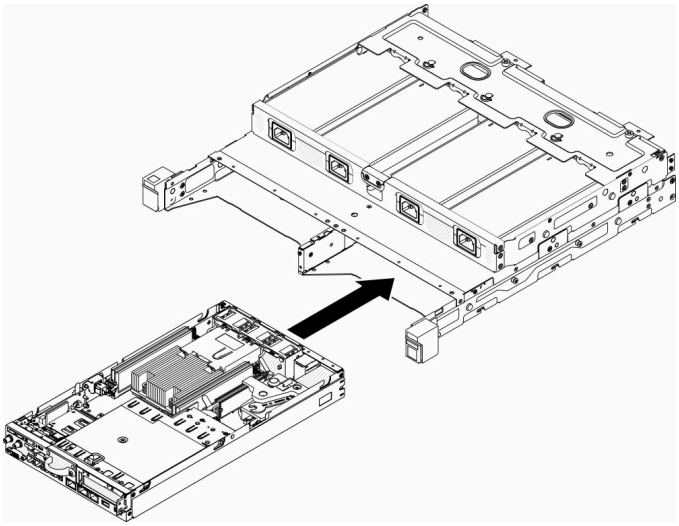


図 63. ノードの取り付け

c. 配送用ブラケットを位置合わせし、エンクロージャーの前面に挿入します。

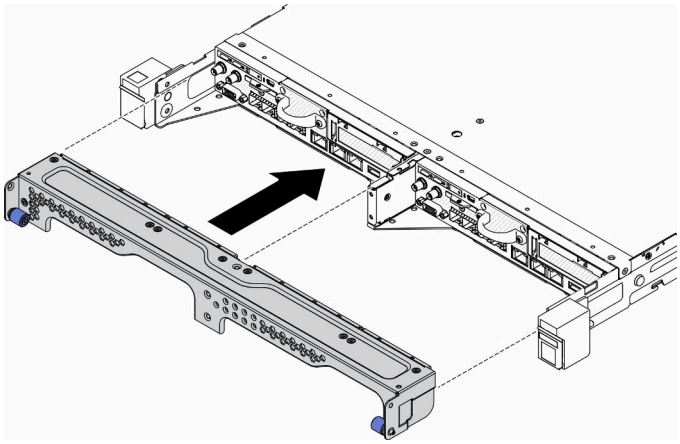


図 64. ノードの取り付け

d. 5 本のねじを取り付け、2 個のつまみねじを締めて配送用ブラケットを固定します。

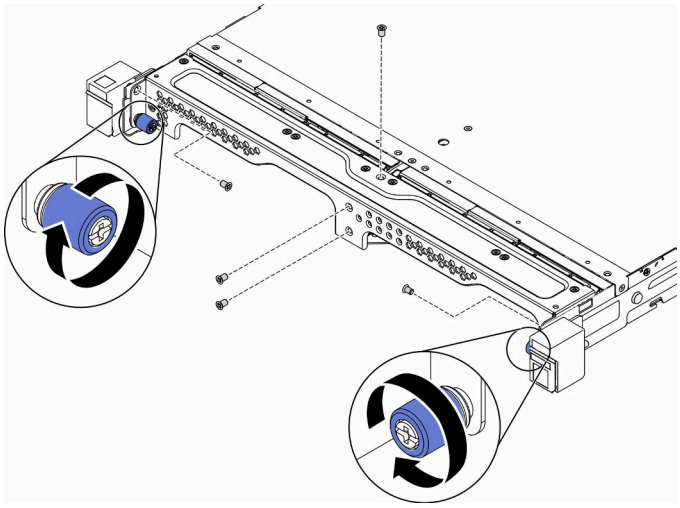


図 65. ノードの取り付け

ノードを取り付けた後、以下のステップを実行してください。

1. 必要に応じて、エンクロージャーをラックの中に取り付けます。
2. 電源コードおよびすべての外部ケーブルを再接続します。
3. サーバーの電源をオンにします (78 ページの「サーバーの電源をオンにする」を参照)。

デモ・ビデオ

- YouTube で手順を参照: https://www.youtube.com/watch?v=SkYYnMect9w

ラックへのサーバーの取り付け

ラックにサーバーを取り付けるには、以下に記載されている手順に従ってください。

ラックにサーバーを取り付けるには、サーバーを取り付けるレールで、レール取り付けキットに記載されている手順に従ってください。

サーバーの配線

すべての外部ケーブルをサーバーに接続します。通常は、サーバーを電源、データ・ネットワーク、およびストレージに接続する必要があります。さらに、サーバーを管理ネットワークにも接続する必要があります。

電源への接続

サーバーを電源に接続します。

ネットワークへの接続

サーバーをネットワークに接続します。

ストレージへの接続

サーバーを任意のストレージ・デバイスに接続します。

サーバーの電源をオンにする

サーバーが入力電力に接続されると、短いセルフテスト (電源状況 LED がすばやく点滅) を実行した後、スタンバイ状態になります (電源状況 LED が 1 秒に 1 回点滅)。

次のいずれかの方法で、サーバーの電源をオン (電源 LED が点灯) にできます。

- 電源ボタンを押します。
- 停電の後、サーバーを自動的に再起動させることができます。
- サーバーは、Lenovo XClarity Controller に送信されるリモート・パワーオン要求に応答できます。

サーバーの電源オフについては、78 ページの「サーバーの電源をオフにする」を参照してください。

サーバーのセットアップの検証

サーバーの電源をオンにした後、LED が点灯し緑色であることを確認します。

サーバーの電源をオフにする

電源に接続されているときは、サーバーはスタンバイ状態を維持し、Lenovo XClarity Controller がリモートのパワーオン要求に応答できるようになっています。サーバーからすべての電源を切る (電源状況 LED がオフ) には、すべての電源コードを抜く必要があります。

サーバーをスタンバイ状態にするには (電源状況 LED が 1 秒に 1 回点滅):

注：Lenovo XClarity Controller は、重大なシステム障害への自動的な応答としてサーバーをスタンバイ状態にできます。

- オペレーティング・システムを使用して正常シャットダウンを開始します (この機能がオペレーティング・システムでサポートされている場合)。
- 電源ボタンを押して正常シャットダウンを開始します (オペレーティング・システムでサポートされている場合)。
- 電源ボタンを 4 秒以上押して、強制的にシャットダウンします。

スタンバイ状態では、サーバーは Lenovo XClarity Controller に送信されるリモート・パワーオン要求に応答できます。サーバーの電源オンについては、78 ページの 「サーバーの電源をオンにする」を参照してください。

第 4 章　システム構成

システムを構成するには、以下の手順を実行します。セキュリティー・パック付きの SE350 では、自動データ保護が有効になっており、不正のイベントで SED のデータへのアクセスをロックできるため、データのロックを解除してアクセスするためにシステムを登録してアクティブにする必要があります。標準の SE350 では、データへのアクセスはロックされません。標準の SE350 では、SED の管理と不正の設定は無効になっています。

注：

- *セキュリティー・パック付きの SE350* は、2021 年 7 月より前は単に *SE350* と呼ばれていました。
- システムがセキュリティー・パック付きの SE350 か標準の SE350 かは、Lenovo XClarity Controller で確認できます。

セキュリティー・パック付きの SE350 を使用する前に、以下の手順を実行する必要があります。

- 81 ページの 「システムをアクティブにする」
- 83 ページの 「ロックダウン・モードと動作検出」
- 83 ページの 「自己暗号化ドライブ認証キー (SED AK) のバックアップ」

システムをアクティブにする

セキュリティー・バック付きの ThinkSystem SE350 は、出荷時にはセキュリティーのためにロック状態になっています。稼働の前に、ブートおよび完全に機能させるにはサーバーをアクティブにする必要があります。以下の詳細な手順に従って、システムをアクティブにします。

Lenovo ID の作成

既存の Lenovo ID を使用するか、新しい ID を作成して ThinkSystem Key Vault Portal または ThinkShield モバイル・アプリにログインします。

- Lenovo ID のセットアップについては、https://passport.lenovo.com を参照してください。
- Lenovo ThinkSystem Key Vault Portal にログインするには、https://portal.thinkshield.lenovo.com を参照してください。

アクティブにする方法

システムをアクティブにする方法は 2 つあります。サーバーの環境に応じて、サーバーをアクティブにするための最適な方法を決定します。

1. **モバイル・アプリによるアクティベーション**

   モバイル・アプリのアクティベーション方式では、モバイル・データ接続機能がある Android または iOS ベースのスマートフォンと、そのスマートフォン付属の USB ケーブルが必要です。XCC 管理 USB ポートに入るように、追加のミニ USB ドングルが提供されています。

   注：スマートフォンが USB ケーブルを接続する目的を入力するよう指示した場合、データ転送を選択します。

   a. セキュリティー・バック付きの ThinkSystem SE350 に電源ケーブルを接続します。

   b. Google Play Store、Apple App Store、Baidu または Lenovo App Store から ThinkShield Edge Mobile Management アプリを、Android または iOS フォンにダウンロードします (検索用語は、「ThinkShield Edge」)。

   c. 組織で登録した ID を使用して、ThinkShield Edge Mobile Management アプリにログインします。

© Copyright Lenovo 2019, 2022

d. アプリの指示に従って、USB ケーブルと USB 携帯電話充電ケーブルをセキュリティー・パック付きの ThinkSystem SE350 に接続します。

e. 画面の「デバイスのアクティブ化」の指示に従って、ThinkSystem SE350 のセキュアなアクティベーションを完了します。

f. 正常にアクティブになると、ThinkShield Edge Mobile Management アプリに「デバイスがアクティブ化」画面が表示されます。

手順について詳しくは、https://download.lenovo.com/servers_pdf/thinkshield-mobile-application-user-guide-v6.pdf または https://support.lenovo.com/tw/en/solutions/ht509033 を参照してください。

2. **インターネット接続によるアクティベーション**

インターネット接続によるアクティベーションでは、マシン・タイプ、シリアル番号、アクティベーション・コードが必要です。

a. セキュリティー・パック付きの ThinkSystem SE350 に電源ケーブルを接続します。

b. XClarity Controller 管理イーサネット・ポートを、インターネットにアクセスできるネットワークに接続します。

注：アクティベーションを行うには、アウトバウンド TCP ポート 443 (HTTPS) が開いている必要があります。

c. 組織で登録した ID を使用して ThinkShield Key Vault Portal にログインします。

d. セキュリティー・パック付きの ThinkSystem SE350 を登録するには、デバイス マネージャーの「デバイス」の横にあるオレンジ色のプラス記号をクリックしてデバイスを追加します。対応するフィールドに、マシン・タイプ、シリアル番号、セキュア・アクティベーション・コードを入力します。

e. デバイス・マネージャーでアクティブにするサーバーを選択して、「アクティブ化」をクリックします。サーバーのステータスが「準備完了」に変わります。

f. サーバーが 15 分以内にアクティブになり、自動的に電源がオンになります。正常にアクティブになると、ThinkShield Key Vault Portal でサーバーのステータスがアクティブになります。

注：電源ケーブルを差し込んでから 2 時間以内にサーバーのアクティベーションを行っていない場合は、セキュリティー・パック付きの ThinkSystem SE350 から電源ケーブルを抜いてから、もう一度接続してください。

手順について詳しくは、https://download.lenovo.com/servers_pdf/thinkshield-web-application-user-guide-v2.pdf を参照してください。

お客様の責任:

- セキュア・アクティベーション・コード (チラシで提供) を保持します。
- SED AK のバックアップを管理します。83 ページの 「自己暗号化ドライブ認証キー (SED AK) のバックアップ」を参照してください。
- SE350 システムを安全な作業場所に移動して、サービスを利用できるようにします。
- 携帯電話のケーブルを準備します。
- 必要に応じてデバイスを登録したりアクティブにしたりできるように、IT 部門に協力を要請します。
- SE350 システムが登録されているかどうかを確認します。登録されていない場合は、IT 部門と協力してデバイスを登録します。
- バックアップ・ファイルから SED AK を復元し、パスワードを設定します。
- サービスの後で、SE350 システムを作業場所に戻します。
- ワイヤレス (ネットワーク) 接続が機能していることを確認します。サービス技術員は、デバイスのネットワークへの接続を調べることができません。

ロックダウン・モードと動作検出

セキュリティー・パック付きの ThinkSystem SE350 は、出荷時にはセキュリティーのためにロック状態になっています。ステータスは、XCC で変更できます。

詳しくは、https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/system_lockdown_mode.html を参照してください。

自己暗号化ドライブ認証キー (SED AK) のバックアップ

セキュリティー・パック付きの ThinkSystem SE350 をセットアップするか、構成を変更した後、ハードウェア障害が発生した場合のデータ損失を防ぐために、自己暗号化ドライブ認証キー (SED AK) をバックアップする必要があります。

SED 認証キー (AK) マネージャー

Lenovo XClarity Controller でサーバーの SED AK を変更、バックアップ、または復元するには、SED 認証キー (AK) マネージャーを見つけます。詳しくは、https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_ch1_introduction.html を参照してください。

SED AK の変更

- **パスフレーズから SED AK を生成する**: パスワードを設定し、確認のためにもう一度入力します。「**再生成**」をクリックして、新しい SED AK を取得します。
- **SED AK をランダムに生成する**:「再生成」をクリックして、ランダム SED AK を取得します。

  注：システム・ロックダウン・モードが有効になっている場合、SED AK の生成機能は使用することはできません。

SED AK のバックアップ

パスワードを設定し、確認のためにもう一度入力します。「**Start Backup (バックアップの開始)**」をクリックして SED AK をバックします。次に、SED AK ファイルをダウンロードして、今後の使用に備えて安全に保管します。

注：バックアップ SED AK ファイルを使用して構成を復元する場合、システムはここで設定したパスワードを要求します。

SED AK のリカバリー

- **パスフレーズを使用して SED AK をリカバリーする**: **SED AK をパスフレーズから生成する**で設定されたパスワードを使用して、SED AK をリカバリーします。
- **バックアップ・ファイルから SED AK をリカバリーする**: **SED AK のバックアップ・**モードで生成されたバックアップファイルをアップロードし、対応するバックアップ・ファイルのパスワードを入力して、SED AK リカバリーします。

Lenovo XClarity Controller のネットワーク接続の設定

ネットワーク経由で Lenovo XClarity Controller にアクセスする前に、Lenovo XClarity Controller がネットワークに接続する方法を指定する必要があります。ネットワーク接続の実装方法によっては、静的 IP アドレスも指定する必要がある場合があります。

DHCP を使用しない場合、Lenovo XClarity Controller のネットワーク接続の設定に次の方法を使用できます。

- モニターがサーバーに接続されている場合、 Lenovo XClarity Provisioning Managerを使用してネットワーク接続を設定できます。

Lenovo XClarity Provisioning Manager を使用して Lenovo XClarity Controller をネットワークに接続するには、以下の手順を実行します。

1. サーバーを起動します。
2. 画面の指示に従って指定されたキーを押し、Lenovo XClarity Provisioning Manager インターフェースを表示します。(詳しくは、https://pubs.lenovo.com/lxpm-overview/ にあるご使用のサーバーと互換性のある LXPM 資料の「スタートアップ」セクションを参照してください)
3. **LXPM → 「UEFI セットアップ」 → 「BMC 設定」**に移動し、Lenovo XClarity Controller がネットワークに接続する方法を指定します。
   - 静的 IP 接続を選択する場合は、ネットワークで使用できる IPv4 アドレスまたは IPv6 アドレスを指定してください。
   - DHCP 接続を選択する場合は、サーバーの MAC アドレスが DHCP サーバーで構成されていることを確認します。
4. 「**OK**」をクリックして設定を適用し、2 分から 3 分待ちます。
5. IPv4 または IPv6 アドレス使用して、Lenovo XClarity Controllerに接続します。

   重要：Lenovo XClarity Controller は、最初はユーザー名 USERID とパスワード PASSW0RD (英字の O でなくゼロ) を使用して設定されます。このデフォルトのユーザー設定では、Supervisor アクセス権があります。拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更する必要があります。

- モニターがサーバーに接続されていない場合は、Lenovo XClarity Controller インターフェースを経由してネットワーク接続を設定できます。ラップトップから Lenovo XClarity Controller コネクター (サーバー前面にあります) にイーサネット・ケーブルを接続します。Lenovo XClarity Controller コネクターの位置については、18 ページの 「前面図」を参照してください。

  注：サーバーのデフォルト設定と同じネットワークになるように、ラップトップの IP 設定を変更してください。

  デフォルトの IPv4 アドレスおよび IPv6 リンク・ローカル・アドレス (LLA) は、引き出し式情報タブに貼付されている Lenovo XClarity Controller ネットワーク・アクセス・ラベルに記載されています。

- モバイル・デバイスから Lenovo XClarity Administrator モバイル・アプリを使用している場合、サーバー前面の Lenovo XClarity Controller USB コネクターを介して Lenovo XClarity Controller に接続できます。Lenovo XClarity ControllerUSB コネクターの位置については、18 ページの 「前面図」を参照してください。

  注：Lenovo XClarity Controller USB コネクター・モードは、Lenovo XClarity Controller を管理するように (標準 USB モードではなく) 設定する必要があります。標準モードから Lenovo XClarity Controller 管理モードに切り替えるには、前面パネルの青色の ID ボタンを、LED がゆっくりと (2 秒に 1 回) 点滅するまで、3 秒以上押し続けます。

  Lenovo XClarity Administrator モバイル・アプリを使用して接続するには:

  1. モバイル・デバイスの USB ケーブルを前面パネルの Lenovo XClarity Administrator USB コネクターに接続します。
  2. モバイル・デバイスで、USB テザリングを有効にします。
  3. モバイル・デバイスで、Lenovo XClarity Administrator モバイル・アプリを起動します。
  4. 自動検出が無効になっている場合は、USB 検出ページで「**検出**」をクリックして Lenovo XClarity Controller に接続します。

  Lenovo XClarity Administrator モバイル・アプリの使用法についての詳細は、以下を参照してください。

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

ファームウェアの更新

サーバーのファームウェア更新には、いくつかのオプションを使用できます。

以下にリストされているツールを使用してご使用のサーバーの最新のファームウェアおよびサーバーに取り付けられているデバイスを更新できます。

- ファームウェアの更新に関するベスト・プラクティスは、以下のサイトで入手できます。
  - http://lenovopress.com/LP0656
- 最新のファームウェアは、以下のサイトにあります。
  - https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/downloads
- 製品に関する通知を購読して、ファームウェア更新を最新の状態に保つことができます。
  - https://datacentersupport.lenovo.com/tw/en/solutions/ht509500

UpdateXpress System Packs (UXSP)

Lenovo は通常、UpdateXpress System Packs (UXSP) と呼ばれるバンドルでファームウェアをリリースしています。すべてのファームウェア更新に互換性を持たせるために、すべてのファームウェアを同時に更新する必要があります。Lenovo XClarity Controller と UEFI の両方のファームウェアを更新する場合は、最初に Lenovo XClarity Controller のファームウェアを更新してください。

更新方法の用語

- **インバンド更新**。サーバーのコア CPU で稼働するオペレーティング・システム内のツールまたはアプリケーションを使用してインストールまたは更新が実行されます。
- **アウト・オブ・バンド更新**。Lenovo XClarity Controller が更新を収集してから、ターゲット・サブシステムまたはデバイスに更新を指示することで、インストールまたは更新が実行されます。アウト・オブ・バンド更新では、コア CPU で稼働するオペレーティング・システムに依存しません。ただし、ほとんどのアウト・オブ・バンド操作では、サーバーが S0 (稼働) 電源状態である必要があります。
- **オン・ターゲット更新**。ターゲット・サーバー自体で実行されているインストール済みのオペレーティング・システムからインストールまたは更新が実行されます。
- **オフ・ターゲット更新**。サーバーの Lenovo XClarity Controller と直接やり取りするコンピューティング・デバイスからインストールまたは更新が実行されます。
- **UpdateXpress System Packs (UXSP)**。UXSP は、互いに依存するレベルの機能、パフォーマンス、互換性を提供するように設計されテストされたバンドル更新です。UXSP は、サーバーのマシン・タイプ固有であり、特定の Windows Server、Red Hat Enterprise Linux (RHEL) および SUSE Linux Enterprise Server (SLES) オペレーティング・システム・ディストリビューションをサポートするように (ファームウェアおよびデバイス・ドライバーの更新で) 作成されています。マシン・タイプ固有ファームウェア専用の UXSP も使用できます。

ファームウェア更新ツール

ファームウェアのインストールとセットアップに使用する最適な Lenovo ツールを判別するには、次の表を参照してください。

ツール	サポートされる更新方法	コア・システム・ファームウェア更新	I/O デバイス・ファームウェア更新	グラフィカル・ユーザー・インターフェース	コマンド・ライン・インターフェース	UXSP のサポート
Lenovo XClarity Provisioning Manager	インバンド[2]	√		√		

ツール	サポートされる更新方法	コア・システム・ファームウェア更新	I/O デバイス・ファームウェア更新	グラフィカル・ユーザー・インターフェース	コマンド・ライン・インターフェース	UXSP のサポート
(LXPM)	オン・ターゲット					
Lenovo XClarity Controller (XCC)	アウト・オブ・バンド オフ・ターゲット	√	選択された I/O デバイス	√		
Lenovo XClarity Essentials OneCLI (OneCLI)	インバンド アウト・オブ・バンド オン・ターゲット オフ・ターゲット	√	すべての I/O デバイス		√	√
Lenovo XClarity Essentials UpdateXpress (LXCE)	インバンド アウト・オブ・バンド オン・ターゲット オフ・ターゲット	√	すべての I/O デバイス	√		√
Lenovo XClarity Essentials Bootable Media Creator[3] (BoMC)	インバンド アウト・オブ・バンド オフ・ターゲット	√	すべての I/O デバイス	√ (BoMC アプリケーション)	√ (BoMC アプリケーション)	√

ツール	サポートされる更新方法	コア・システム・ファームウェア更新	I/O デバイス・ファームウェア更新	グラフィカル・ユーザー・インターフェース	コマンド・ライン・インターフェース	UXSP のサポート
Lenovo XClarity Administrator (LXCA)	インバンド[1] アウト・オブ・バンド[2] オフ・ターゲット	√	すべての I/O デバイス	√		√
VMware vCenter 用 Lenovo XClarity Integrator (LXCI)	アウト・オブ・バンド オフ・ターゲット	√	選択された I/O デバイス	√		
Microsoft Windows Admin Center 用 Lenovo XClarity Integrator (LXCI)	インバンド アウト・オブ・バンド オン・ターゲット オフ・ターゲット	√	すべての I/O デバイス	√		√
Microsoft System Center Configuration Manager 用 Lenovo XClarity Integrator (LXCI)	インバンド オン・ターゲット	√	すべての I/O デバイス	√		√

注：

1. I/O ファームウェア更新の場合。
2. BMC および UEFI ファームウェア更新の場合。

- **Lenovo XClarity Provisioning Manager**

  Lenovo XClarity Provisioning Manager から、Lenovo XClarity Controller ファームウェア、UEFI ファームウェア、Lenovo XClarity Provisioning Manager ソフトウェアを更新できます。

  注：サーバーを起動して画面の指示に従って指定されたキーを押すと、デフォルトでは、Lenovo XClarity Provisioning Manager グラフィカル・ユーザー・インターフェースが表示されます。このデフォルトをテキスト・ベースのシステム・セットアップに変更した場合は、テキスト・ベースのシステム・セットアップ・インターフェースからグラフィカル・ユーザー・インターフェースを起動できます。

Lenovo XClarity Provisioning Manager を使用したファームウェアの更新に関する追加情報については、以下を参照してください。

https://pubs.lenovo.com/lxpm-overview/ にある、ご使用のサーバーと互換性のある LXPM に関する資料の「ファームウェア更新」セクション

- **Lenovo XClarity Controller**

  特定の更新をインストールする必要がある場合、特定のサーバーに Lenovo XClarity Controller インターフェースを使用できます。

  注：

  – Windows または Linux でインバンド更新を実行するには、オペレーティング・システム・ドライバーがインストールされており、Ethernet-over-USB (LAN over USB と呼ばれることもあります) インターフェースが有効になっている必要があります。

    Ethernet over USB の構成に関する追加情報については、以下を参照してください。

    https://pubs.lenovo.com/lxcc-overview/ にある、ご使用のサーバーと互換性のある XCC に関する資料のバージョンの「Ethernet over USB の構成」セクション

  – Lenovo XClarity Controller を経由してファームウェアを更新する場合は、サーバーで実行されているオペレーティング・システム用の最新のデバイス・ドライバーがダウンロードおよびインストールされていることを確認してください。

  Lenovo XClarity Controller を使用したファームウェアの更新に関する追加情報については、以下を参照してください。

  https://pubs.lenovo.com/lxcc-overview/ にある、ご使用のサーバーと互換性のある XCC に関する資料の「サーバー・ファームウェアの更新」セクション

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI は、Lenovo サーバーの管理に使用できる複数のコマンド・ライン・アプリケーションのコレクションです。これの更新アプリケーションを使用して、サーバーのファームウェアおよびデバイス・ドライバーを更新できます。更新は、サーバー (インバンド) のホスト・オペレーティング・システム内で、またはサーバー (アウト・オブ・バンド) の BMC を介してリモートで実行できます。

  Lenovo XClarity Essentials OneCLI を使用したファームウェアの更新に関する追加情報については、以下を参照してください。

  https://pubs.lenovo.com/lxce-onecli/onecli_c_update

- **Lenovo XClarity Essentials UpdateXpress**

  Lenovo XClarity Essentials UpdateXpress は、グラフィカル・ユーザー・インターフェース (GUI) を介して OneCLI のほとんどの更新機能を提供します。これを使用して、UpdateXpress System Pack (UXSP) 更新パッケージおよび個別の更新を取得してデプロイします。UpdateXpress System Packs には、Microsoft Windows と Linux のファームウェアおよびデバイス・ドライバーの更新が含まれます。

  Lenovo XClarity Essentials UpdateXpress は、次の場所から入手できます。

  https://datacentersupport.lenovo.com/solutions/lnvo-xpress

- **Lenovo XClarity Essentials Bootable Media Creator**

  Lenovo XClarity Essentials Bootable Media Creator を使用して、ファームウェア更新の適用、VPD の更新、インベントリーおよび FFDC 収集、高度なシステム構成、FoD キー管理、安全な消去、RAID 構成、サポートされるサーバーでの診断に適したブート可能メディアを作成することができます。

  Lenovo XClarity Essentials BoMC は、以下の場所から入手できます。

  https://datacentersupport.lenovo.com/solutions/lnvo-bomc

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator を使用して複数のサーバーを管理している場合は、このインターフェースを使用してすべての管理対象サーバーでファームウェアを更新できます。ファームウェア管理は管理対

象エンドポイントに対してファームウェア・コンプライアンス・ポリシーを割り当てることによって簡略化されます。コンプライアンス・ポリシーを作成して管理対象エンドポイントに割り当てると、Lenovo XClarity Administrator はこれらのエンドポイントに対するインベントリーの変更を監視し、コンプライアンス違反のエンドポイントにフラグを付けます。

Lenovo XClarity Administrator を使用したファームウェアの更新に関する追加情報については、以下を参照してください。

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/update_fw.html

- **Lenovo XClarity Integrator 製品**

  Lenovo XClarity Integrator 製品は、VMware vCenter、Microsoft Admin Center、または Microsoft System Center などの特定のデプロイメントインフラで使用されるソフトウェアに、Lenovo XClarity Administrator およびお使いのサーバーの管理機能を統合することができます。

  Lenovo XClarity Integrator を使用したファームウェアの更新に関する追加情報については、以下を参照してください。

  https://pubs.lenovo.com/lxci-overview/

ファームウェアの構成

サーバーのファームウェアのインストールとセットアップには、いくつかのオプションを使用できます。

重要：Lenovo サポートから指示されない限り、オプション ROM を「**レガシー**」に設定するように構成しないでください。この設定により、スロット・デバイス用の UEFI ドライバーがロードされなくなり、Lenovo XClarity Administrator や Lenovo XClarity Essentials OneCLI のような Lenovo ソフトウェアや、Lenovo XClarity Controller に負の副作用を引き起こす可能性があります。この副作用には、モデル名やファームウェア・レベルなどのアダプター・カードの詳細を判断できないことが含まれます。アダプター・カードの情報が使用できない場合は、「ThinkSystem RAID 930-16i 4GB Flash」のような実際のモデル名ではなく、「アダプター 06:00:00」のようなモデル名の汎用情報が表示されます。場合によっては、UEFI ブート・プロセスがハングすることもあります。

- **Lenovo XClarity Provisioning Manager**

  Lenovo XClarity Provisioning Manager では、サーバーの UEFI 設定を構成できます。

  注：Lenovo XClarity Provisioning Manager には、サーバーを構成するためのグラフィカル・ユーザー・インターフェースが用意されています。システム構成へのテキスト・ベースのインターフェース (Setup Utility) も使用できます。Lenovo XClarity Provisioning Manager で、サーバーを再起動してテキスト・ベースのインターフェースにアクセスすることを選択できます。さらに、テキスト・ベースのインターフェースを、LXPM を起動して表示されるデフォルト・インターフェースにすることも選択できます。これを行うには、**Lenovo XClarity Provisioning Manager → UEFI セットアップ → システム設定 → <F1> スタート制御 → テキスト・セットアップ**に移動します。グラフィック・ユーザー・インターフェースを使用してサーバーを起動するには、「**自動**」または「**ツール・スイート**」を選択します。

  詳しくは、次の資料を参照してください。

  - 「*Lenovo XClarity Provisioning Manager*ユーザー・ガイド」
    - https://pubs.lenovo.com/lxpm-overview/で、ご使用のサーバーと互換性のある LXPM に関する資料のバージョンを検索します。
  - 「*UEFI ユーザー・ガイド*」
    - https://pubs.lenovo.com/uefi-overview/

- **Lenovo XClarity Essentials OneCLI**

構成アプリケーションおよびコマンドを使用して現在のシステム構成設定を表示し、Lenovo XClarity Controller と UEFI に変更を加えることができます。保存された構成情報は、他のシステムを複製またはリストアするために使用できます。

Lenovo XClarity Essentials OneCLI を使用したサーバーの構成については、以下を参照してください。

https://pubs.lenovo.com/lxce-onecli/onecli_c_settings_info_commands

- **Lenovo XClarity Administrator**

  一貫した構成を使用して、すべてのサーバーを簡単にプロビジョニングおよび事前プロビジョニングできます。構成設定 (ローカル・ストレージ、I/O アダプター、ブート設定、ファームウェア、ポート、Lenovo XClarity Controller や UEFI の設定など) はサーバー・パターンとして保管され、1 つ以上の管理対象サーバーに適用できます。サーバー・パターンが更新されると、その変更は適用対象サーバーに自動的にデプロイされます。

  Lenovo XClarity Administrator を使用したファームウェアの更新に関する特定の詳細情報は、以下から入手できます。

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/server_configuring.html

- **Lenovo XClarity Controller**

  サーバーの管理プロセッサーは、Lenovo XClarity Controller Web インターフェースまたはコマンド・ライン・インターフェース経由で構成できます。

  Lenovo XClarity Controller を使用したサーバーの構成については、以下を参照してください。

  https://pubs.lenovo.com/lxcc-overview/にある、ご使用のサーバーと互換性のある XCC に関する資料の「サーバーの構成」セクション

メモリー構成

メモリー・パフォーマンスは、メモリー・モード、メモリー速度、メモリー・ランク、メモリー装着構成、プロセッサーなど、複数の変動要素よって決まります。

メモリー・パフォーマンスの最適化とメモリーの構成について詳しくは、Lenovo Press Web サイトを参照してください。

https://lenovopress.com/servers/options/memory

さらに、以下のサイトで入手可能なメモリー・コンフィギュレーターを活用できます。

http://1config.lenovo.com/#/memory_configuration

実行しているシステム構成およびメモリー・モードに基づくメモリー・モジュールの必要な取り付け順序についての具体的な情報は、68 ページの 「DIMM の取り付け」を参照してください。

RAID 構成

RAID (Redundant Array of Independent Disks) を使用したデータの保存は今でも、サーバーのストレージ・パフォーマンス、可用性、容量を向上するために最もよく利用され、最もコスト効率のいい方法の 1 つです。

RAID は、複数のドライブが I/O 要求を同時に処理できるようにすることによりパフォーマンスを高めます。さらに、RAID は、障害が発生したドライブの欠落データを残りのドライブのデータを使用して再構築することにより、ドライブに障害が発生した場合でもデータ損失を防ぐことができます。

RAID アレイ (RAID ドライブ・グループともいいます) は、特定の一般的な方法を使用してドライブ間でデータを分散する複数の物理ドライブのグループです。仮想ドライブ (仮想ディスクまたは論理ドライブともいいます) は、ドライブ上の連続したデータ・セグメントで構成されるドライブ・グループのパー

ティションです。仮想ドライブは、OS 論理ドライブまたはボリュームを作成するために分割できる物理ディスクとしてホスト・オペレーティング・システムに表示されます。

RAID の概要は、以下の Lenovo Press Web サイトで参照できます。

https://lenovopress.com/lp0578-lenovo-raid-introduction

RAID の管理ツールおよびリソースに関する詳細情報は、以下の Lenovo Press Web サイトで参照できます。

https://lenovopress.com/lp0579-lenovo-raid-management-tools-and-resources

注：

- NVMe ドライブの RAID をセットアップする前に、以下の手順に従って VROC を有効にします。
  1. システムを再起動します。オペレーティング・システムが起動する前に、「**F1**」を押して Setup Utility に入ります。
  2. 「**システム設定**」 → 「**デバイスおよび I/O ポート**」 → 「**Intel VMD**」に移動し、オプションを有効にします。
  3. 変更を保存して、システムをリブートします。
- VROC Intel-SSD-Only は、Intel NVMe ドライブを搭載した RAID レベル 0、1、5、および 10 をサポートします。
- VROC プレミアムは、アクティベーション・キーを必要とし、非 Intel NVMe ドライブを搭載した RAID レベル 0、1、5、および 10 をサポートします。アクティベーション・キーの取得とインストールについて詳しくは、https://fod.lenovo.com/lkmsを参照してください。

ワイヤレス対応 LOM パッケージ構成

ワイヤレス対応 LOM パッケージの構成を設定するには、この情報を使用します。

サーバーのワイヤレス機能を有効にするには、次の手順を実行します。

1. ワイヤレス対応 LOM パッケージをインストールします。
2. 使用シナリオを定義して、プリセット・トポロジーから最適なものを選択します。94 ページの 「ワイヤレス対応 LOM パッケージ・プリセット」を参照してください。
3. プリセットに適用可能なトポロジーがない場合は、オプションでカスタマイズしたものを作成します。「カスタマイズされた構成」を参照してください。
4. Lenovo XClarity Controller で「**Wi-Fi/LTE 接続**」を有効にします。

   注：LTE を有効にするには、SIM カードを取り付ける必要があります (61 ページの 「SIM カードの取り付け」 を参照)。LTE サービスは、それぞれの国または地域で認可されたモバイル・サービス・キャリアによって提供されます。LTE ネットワークに接続するには、サーバーにサービス・キャリアからのセルラー・プランが必要です。

ワイヤレス対応 LOM パッケージ内には、組み込みスイッチがあります。これは LTE 機能、WLAN (AP/クライアント・モード)、およびアップリンクとダウンリンク用の 1 GbE ポートを備えたルーターとして機能します。ポートの詳細情報は以下を参照してください。

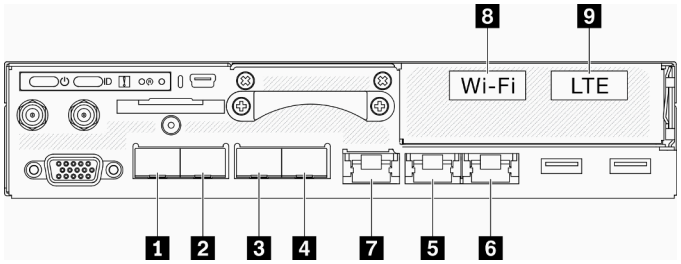


図 66. 前面パネルの有線/ワイヤレス・ポート

表 22. 前面パネルの有線/ワイヤレス・ポート

	物理ポート	インターフェース名 (組み込みスイッチ CLI で使用)
1	10 GbE SFP+	該当なし
2	10 GbE SFP+	該当なし
3	1 GbE SFP	eth6
4	1 GbE SFP	eth3
5	1 GbE RJ45	eth1
6	1 GbE RJ45	eth2
7	1 GbE RJ45	eth4
8	Wi-Fi (WLAN)	wlan0
9	LTE	wwan0

- 2x 1GbE SFP ポート (ポート 3 および 4): 1000 Base–X SFP のみサポートします
- 2x 1GbE RJ45 ポート (ポート 5 および 6): 10/100/1000 Mbps をサポートします
- WLAN インターフェース: クライアント・モードでのアップリンクまたは AP モードでのダウンリンクとして機能します
- LTE インターフェース: アップリンク・ポートとしてのみ機能します。nano SIM のみをサポートします
- 専用内部 10GbE ポート: OS への接続 (Windows OS では「LOM1-Switchboard」と呼ばれます)
- 組み込みスイッチ CLI は管理ポート (ポート 7) から SSH でアクセスできますが、専用アドレス (192.168.70.254) となります
  - ユーザー名: oper
  - パスワード: (XCC と同じパスワードを使用します)
- デフォルトでは、組み込みスイッチにはすべての物理ダウンリンク・ポート上にアクティブな DHCP サーバー、含まれている Wi-Fi (AP モードの場合) があります。
- IP の割り当て範囲:
  - ダウンリンク・ポート: 192.168.71.x
  - WLAN (AP モード): 192.168.74.x
  - OS への専用内部 10GbE ポート (Windows OS では「LOM1-Switchboard」と呼ばれます): 192.168.73.x

有線ネットワーク・ポート (ポート 1 – 7) はデフォルトで有効になっています。LOM1-Switchboard、アップリンク、ダウンリンク、管理、WLAN、および LTE インターフェースは、異なる VLAN に属しています。組み込みスイッチは、L3 ルーティングで動作します。

- LOM1-Switchboard (br-x86_lan): デフォルト IP は 192.168.73.254/24 です。デフォルトでは DHCP サーバーが有効になっています
- アップリンク (cloud_wan/lte_wan/wifi_wan_sta): デフォルト設定は DHCP クライアントです
- ダウンリンク (br-edge_lan): デフォルト IP は 192.168.71.254/24 です。デフォルトでは DHCP サーバーが有効になっています
- AP モードでの WLAN (br-wifi_lan_ap): デフォルト IP は 192.168.74.254/24 です。デフォルトでは DHCP サーバーが有効になっています
- クライアント・モードでの WLAN (wifi_wan_sta): デフォルト設定は DHCP クライアントです
- 管理ポート (br-mgmt_xcc_lan)
- XCC: デフォルトでは、管理ポートからのみアクセスできます。デフォルト設定は DHCP クライアントで、XCC のフォールバック IP は 192.168.70.125/24 です。デフォルト IP は 192.168.70.254/24 です。DHCP クライアントまたは DHCP サーバーとして設定できます。

注：

- アップリンク/ダウンリンク・ポートは、トポロジー・プリセットに基づいて変更されます。ユーザーは「uci」CLI コマンドで構成を適応させ、カスタマイズされたプリセットに保存することができます。
- フェイルオーバー (クラウド・ポートおよび LTE) 機能はデフォルトで無効になっています。ユーザーは、次のように組み込みスイッチ CLI で有効にする必要があります:

```
sudo uci set network.cloud_wan.metric='10'
sudo uci set network.lte_wan.metric='30'
sudo uci set network.wifi_wan_sta.metric='20'
sudo uci commit network
sudo /etc/init.d/network restart
```

  設定が完了した後、システムは、ポート **6** (cloud_wan/eth2)、クライアント・モードの WLAN (wifi_wan_sta/wlan0)、および LTE ポート (lte_wan/wwan0) の間のフェイルオーバー/フォールバックの機能を開始します。

WLAN 構成

ThinkSystem SE350 の WLAN ネットワーク (AP モードおよびクライアント・モード) は、デフォルトで無効になっています。ユーザーは、XCC GUI (Edge ネットワーキング・ページ) または組み込みスイッチ CLI でワイヤレス・ネットワークを有効/無効にしてモードを選択できます。

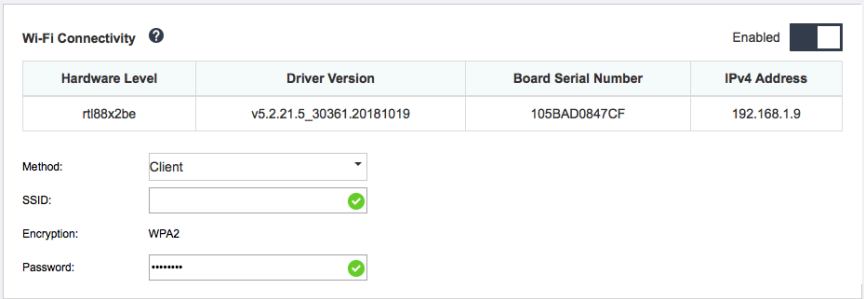


図 67. WLAN 設定

LTE 構成

ThinkSystem SE350 のワイヤレス・ネットワーク (LTE) は、デフォルトで無効になっています。ユーザーは、XCC GUI (Edge ネットワーキング・ページ) または組み込みスイッチ CLI で LTE を有効/無効にすることができます。

- 組み込みスイッチ CLI を使用して LTE 構成を設定します。
- LTE を有効にするには、SIM カードの PIN 番号および APN が必要です。

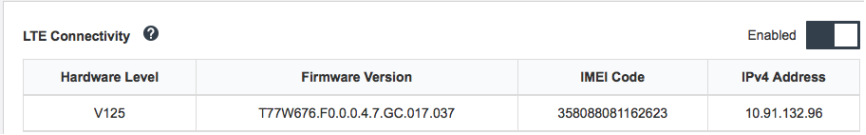


図 68. LTE 設定

BMC ネットワーク・ブリッジ

BMC ネットワーク・ブリッジは、BMC 管理ポートにアクセスするためのアウトバウンド・インターフェースを選択する構成です。以下に示すように、4 つのオプションがあります。デフォルトは「None」で、これは管理ポートのみが XCC インターフェースにアクセスできることを意味します。

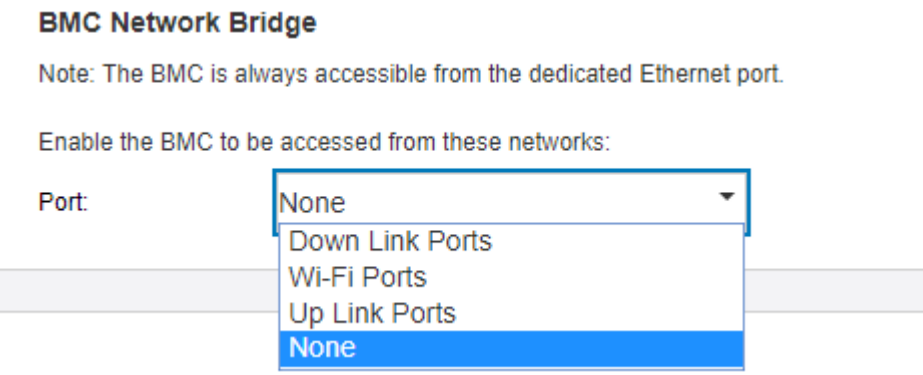


図 69. BMC ネットワーク・ブリッジ

注：

- ポートの割り当ては、ネットワーク・トポロジーのプリセットによって異なります。このパラメーターは、「ネットワーク・トポロジーのプリセット」と一緒にセットアップします。
- 「アップリンク・ポート」を「BMC ネットワーク・ブリッジ」に設定し、ネットワークのプリセットの #1 ～ #4 を選択している場合は、XCC GUI (Edge ネットワーキング・ページ) で「DHCP サーバー」を有効にする必要があります。

ワイヤレス対応 LOM パッケージ・プリセット

ワイヤレス対応 LOM パッケージのプリセット構成を適用するには、この情報を使用します。

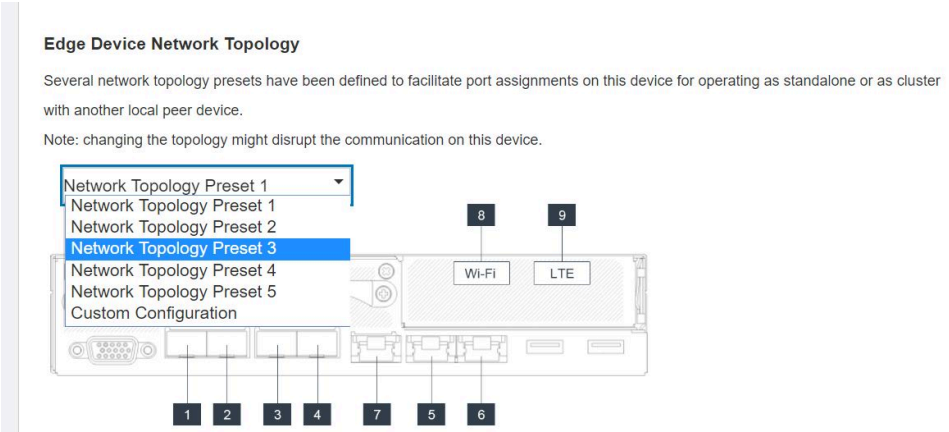
ネットワーク・トポロジーのセットアップ

ネットワーク・トポロジーは、すべてのノードがネットワーク・リンクを使用して相互に接続されるネットワークの配置です。サーバーのポート割り当てを容易にするために、複数のネットワーク・トポロジー・プリセットが定義されています。使用シナリオに応じて、サーバーはスタンドアロン・システムまたは他のピア・サーバーとともにクラスターとして動作できます。

6 つのタイプのネットワーク・トポロジーから選択できます (構成 1-5 はプリセットで、構成 6 はカスタマイズできます)。

トポロジーを変更するには、Lenovo XClarity Controller または組み込みスイッチ CLI (SSH 経由でアクセス) を使用します。

- Lenovo XClarity Controller: **Edge ネットワーキング**でトポロジー・タイプを選択します



- 組み込みスイッチ CLI (SSH 経由でのアクセス): コマンド `sudo set_topology`*1* を使用します
  - コマンドで数値を変更して、トポロジーを変更します。数値は 1-6 で選択できます。トポロジー 6 は、カスタマイズされた設定を作成した後にのみ使用できます。

注：

- LTE/WLAN および IPMI over KCS アクセスはデフォルトで無効になっています。XCC を介して有効にする必要があります。
- ユーザーがネットワーク・トポロジーを変更した後、システムはポートのネットワーク設定をデフォルトにリセットします。

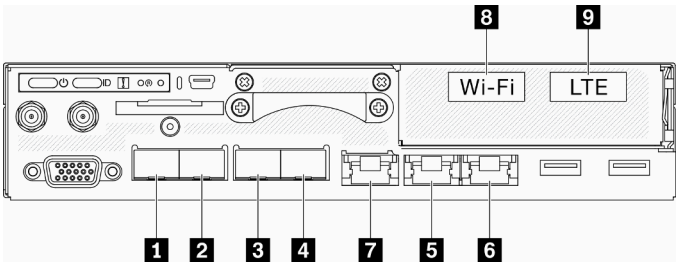


図 70. サーバー前面のポート

表 23. 前面パネルの有線/ワイヤレス・ポート

	物理ポート	インターフェース名 (組み込みスイッチ CLI で使用)
1	10 GbE SFP+	該当なし
2	10 GbE SFP+	該当なし
3	1 GbE SFP	eth6
4	1 GbE SFP	eth3

表 23. 前面パネルの有線/ワイヤレス・ポート (続き)

	物理ポート	インターフェース名 (組み込みスイッチ CLI で使用)
5	1 GbE RJ45	eth1
6	1 GbE RJ45	eth2
7	1 GbE RJ45	eth4
8	Wi-Fi	wlan0
9	LTE	wwan0

構成 1:

構成 1 では、ほとんどのポートがダウンリンク・ポート (エッジ・ポート) として使用されます。サーバーには、他のデバイスの最大接続容量が備わっています。ただし、フェイルオーバー保護はありません。この構成では、LTE および WLAN AP モードの両方が使用可能です。

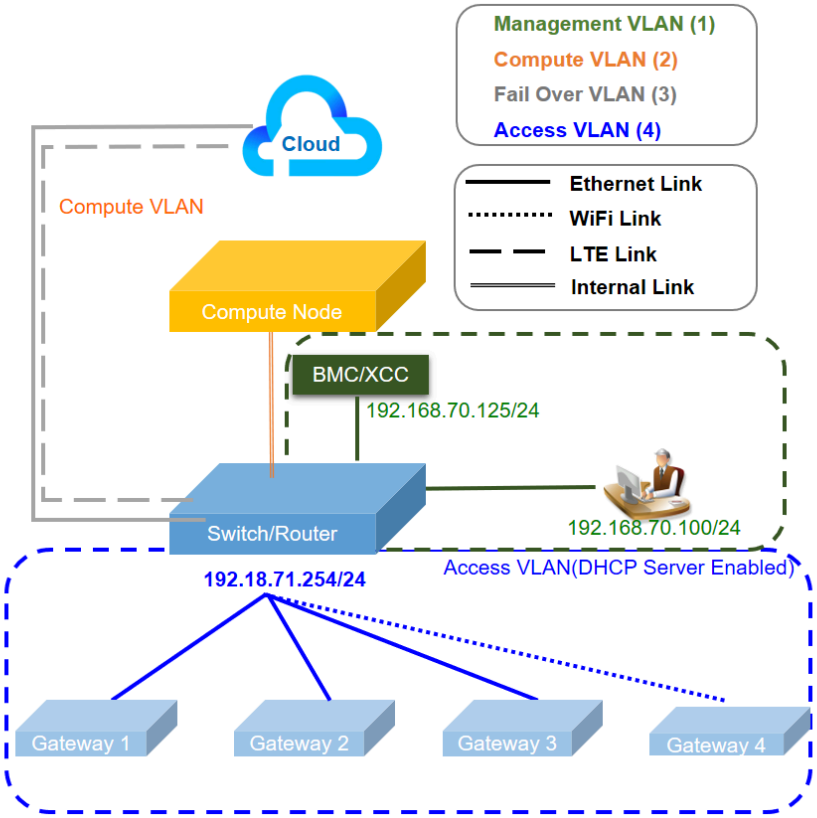


表 24. 構成 1 - IOT ゲートウェイへの最大アクセス・リンク (デフォルト構成)

機能	ポート
ホスト・ポート	1 および 2 2 個の 10Gb イーサネット SFP+
XCC 管理ポート	7 1Gb イーサネット RJ45

表 24. 構成 1 - IOT ゲートウェイへの最大アクセス・リンク (デフォルト構成) (続き)

機能	ポート
アップリンク・ポート (クラウド・ポート)	**6** 1Gb イーサネット RJ45 **9** LTE (物理ポートではなくノード内のアダプター。デフォルトでは無効)
ダウンリンク・ポート (エッジ・ポート)	**3** および **4** 2 個の 1Gb イーサネット SFP **5** 1Gb イーサネット RJ45 **8** WLAN (物理ポートではなくノード内のアダプター。デフォルトでは無効)

構成 2:

構成 2 では、ポート **3** がクラスター・ポート (スイッチ間ポート) として使用されます。サーバーには、設定に応じた冗長性、バックアップ、またはその他の用途が備わっています。この構成では、LTE および WLAN AP モードの両方が使用可能です。

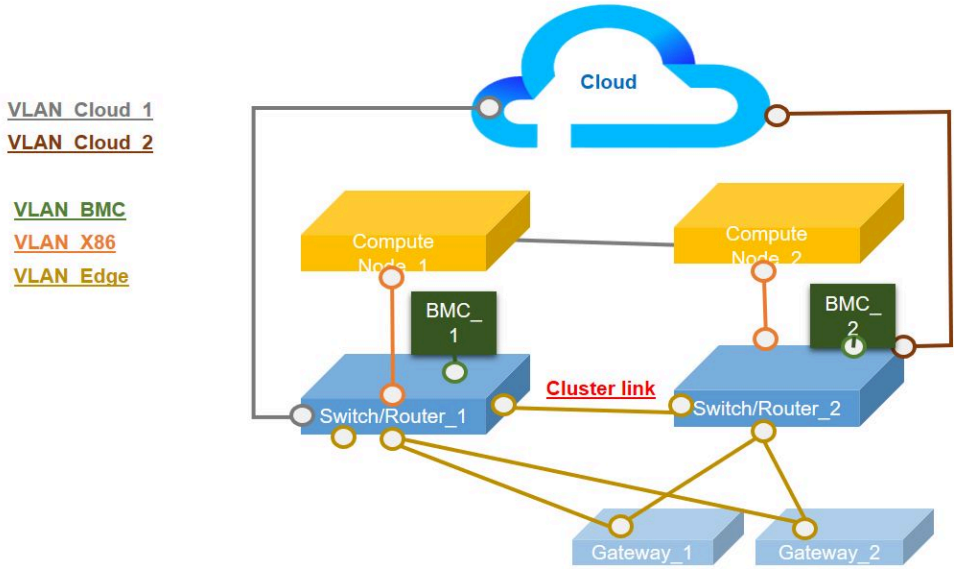


表 25. 構成 2 - クラスター・モードでは 2 個の ThinkSystem SE350 が冗長性のために接続されます

機能	ポート
ホスト・ポート	**1** および **2** 2 個の 10Gb イーサネット SFP+
XCC 管理ポート	**7** 1Gb イーサネット RJ45
アップリンク・ポート (クラウド・ポート)	**6** 1Gb イーサネット RJ45 **9** LTE (物理ポートではなくノード内のアダプター。デフォルトでは無効)

表 25. 構成 2 - クラスター・モードでは 2 個の ThinkSystem SE350 が冗長性のために接続されます (続き)

機能	ポート
クラスター・ポート (スイッチ間ポート)	**3** 1Gb イーサネット SFP
ダウンリンク・ポート (エッジ・ポート)	**4** 1Gb イーサネット SFP **5** 1Gb イーサネット RJ45 **8** WLAN (物理ポートではなくノード内のアダプター。デフォルトでは無効)

構成 3:

構成 3 では、ポート **3** およびポート **4** がクラスター・ポート (スイッチ間ポート) として使用されます。サーバーには、最大レベルのクラスター・トポロジー (最大 3 台のサーバー) が備わっています。この構成では、LTE および WLAN AP モードの両方が使用可能です。

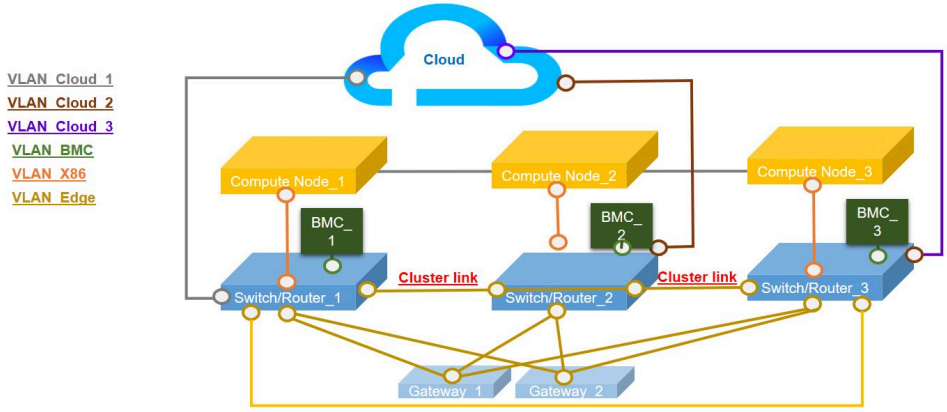


表 26. 構成 3 - クラスター・モードでは 3 個の ThinkSystem SE350 が冗長性のために接続されます

機能	ポート
ホスト・ポート	**1** および **2** 2 個の 10Gb イーサネット SFP+
XCC 管理ポート	**7** 1Gb イーサネット RJ45
アップリンク・ポート (クラウド・ポート)	**6** 1Gb イーサネット RJ45 **9** LTE (物理ポートではなくノード内のアダプター。デフォルトでは無効)
クラスター・ポート (スイッチ間ポート)	**3** および **4** 2 個の 1Gb イーサネット SFP
ダウンリンク・ポート (エッジ・ポート)	**5** 1Gb イーサネット RJ45 **8** WLAN (物理ポートではなくノード内のアダプター。デフォルトでは無効)

構成 4:

構成 4 では、ポート 8 がフェイルオーバー・バックアップの WLAN クライアント・ポートとして使用されます。サーバーは、クライアントとして既存の Wi-fi に接続します。ユーザーは物理的な有線接続ではなく Wi-fi で Lenovo XClarity Controller にアクセスできます。この構成では、WLAN クライアント・モードのみが使用可能です。

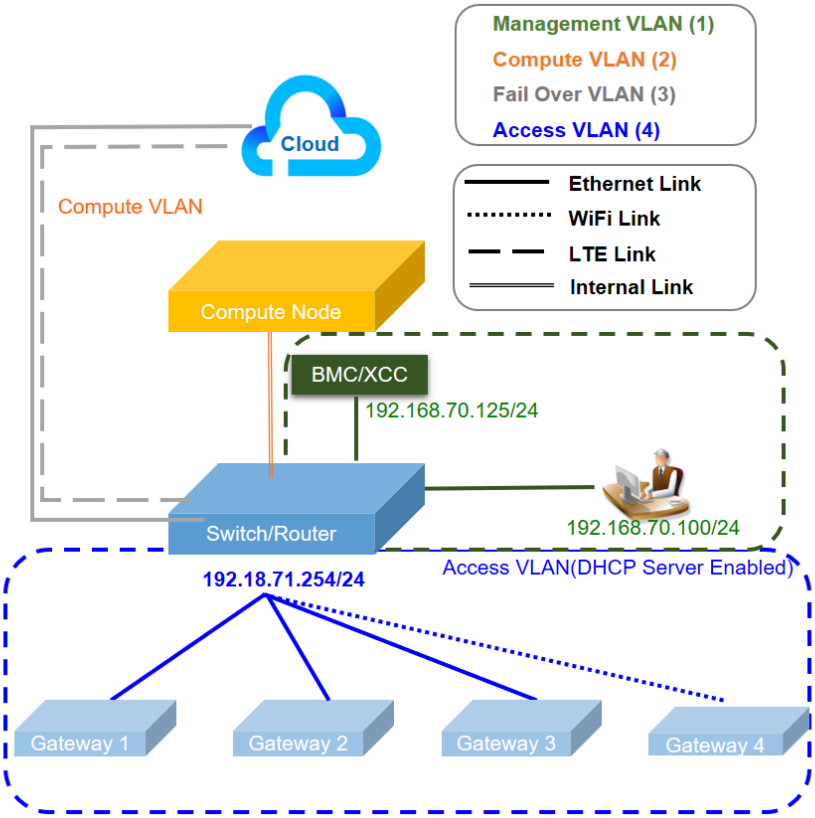


表 27. 構成 4 - WLAN ポートがアップリンク・フェイルオーバーとして動作します

機能	ポート
ホスト・ポート	1 および 2 2 個の 10Gb イーサネット SFP+
XCC 管理ポート	7 1Gb イーサネット RJ45
アップリンク・ポート (クラウド・ポート)	6 1Gb イーサネット RJ45 8 WLAN クライアント (物理ポートではなくノード内のアダプター。デフォルトでは無効) 9 LTE (物理ポートではなくノード内のアダプター。デフォルトでは無効)
ダウンリンク・ポート (エッジ・ポート)	3 および 4 2 x GbE SFP 5 1Gb イーサネット RJ45

構成 5:

構成 5 では、LTE/WLAN 機能はオプションです。サーバーは有線環境で動作できます。

表 28. 構成 5 - 追加の WLAN クライアントがアップリンク・フェイルオーバーとして動作します

機能	ポート
ホスト・ポート	**1** および **2** 2 個の 10Gb イーサネット SFP+
プレート (構成済み IP 設定なし、プレート内のポートは L2 ダンプ・スイッチと同様)	**3** および **4** 1 GbE SFP **5** および **6** 1 GbE RJ45
ユーザー構成	**8** WLAN (物理ポートではなくノード内のアダプター。デフォルトでは無効)
XCC 管理ポート	**7** 1Gb イーサネット RJ45
アップリンク・ポート (クラウド・ポート)	**9** LTE (物理ポートではなくノード内のアダプター。デフォルトでは無効)

構成 6(カスタム構成):

要件を満たす構成が見つからない場合は、カスタマイズされた構成を使用できます。要件と類似したプリセットを選択してから、組み込みスイッチ CLI で設定を調整することをお勧めします。以下のコマンド例を参照してください。

表 29. 構成 6 - カスタマイズされた構成

```
# Disable DHCP server on Down Link ports
sudo uci set dhcp.lan.dhcpv4=disabled
sudo uci commit dhcp
sudo /etc/init.d/dnsmasq restart

# Includes physical ports into Down link
# Refer to Wired/wireless table in the manual for the detailed interface name
sudo uci set network.edge_lan.ifname='eth1 eth3 eth6'
sudo uci commit network.edge_lan
sudo /etc/init.d/network restart


# Configure static IP of Down link ports
sudo uci set network.edge_lan.proto=static
sudo uci set network.edge_lan.ipaddr=192.168.70.254
sudo uci set network.edge_lan.netmask=255.255.255.0
sudo uci commit network.edge_lan
sudo /etc/init.d/network restart


# Save the change into custom preset
sudo save_topology_config


# Change to custom preset (Or go to XCC web,”Edge Networking”, select “custom configuration”)
sudo set_topology 6
```

注：カスタム構成の内容を表示するには、101 ページの「ワイヤレス LOM パッケージ構成の組み込みスイッチ CLI」 の「構成表示」を参照してください。

BMC ネットワーク・ブリッジ

BMC ネットワーク・ブリッジは、BMC 管理ポートにアクセスするためのアウトバウンド・インターフェースを選択する構成です。以下に示すように、4 つのオプションがあります。デフォルトは「None」で、これは管理ポートのみが XCC インターフェースにアクセスできることを意味します。

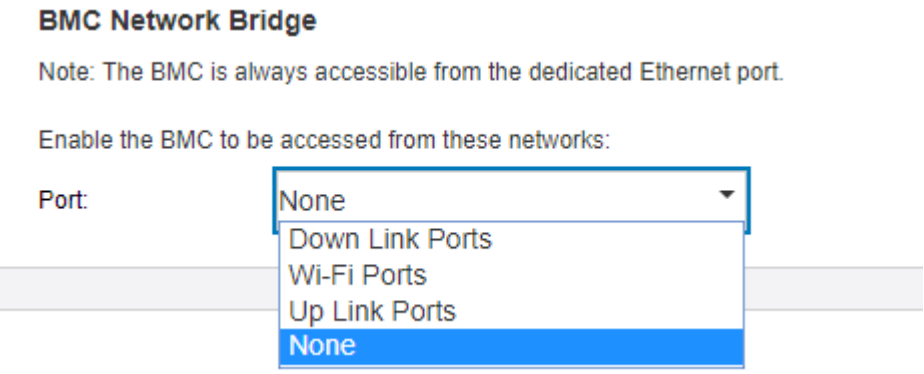


図 71. BMC ネットワーク・ブリッジ

ワイヤレス LOM パッケージ構成の組み込みスイッチ CLI

ワイヤレス LOM パッケージの構成を設定するには、この情報を使用します。

UCI (統合構成インターフェース) を使用して、ワイヤレス LOM パッケージ・コア・サービスを構成します。

組み込みスイッチ CLI は管理ポートから SSH でアクセスできますが、専用アドレス (192.168.70.254) となります

- ユーザー名: oper
- パスワード: (XCC と同じパスワードを使用します)

構成の表示

システムのワイヤレス機能の構成を表示するには、以下のコマンドを使用します。

- `sudo uci show` → システム構成全体を表示します
- `sudo uci show config_profile` → すべてのインターフェースの特定の構成プロファイルを表示します
- `sudo uci show config_profile.interface` → 特定のインターフェースのプロファイルの構成を表示します
- `sudo uci show config_profile.interface.configName` → 特定の構成設定を表示します

表 30. 共通プロファイル

プロファイルの構成	説明
dhcp	DHCP および DNS 設定
firewall	ファイアウォール (NAT)、パケット・フィルター、およびポート転送の設定
network	スイッチ、インターフェース、および経路構成
wireless	ワイヤレス設定および wifi ネットワーク定義

表 31. 共通インターフェース

インターフェース名	説明
mgmt_xcc_lan	XCC アクセスの管理ポート
edge_lan	ダウンリンク・ポート
cloud_wan	アップリンク・ポート (有線)
x86_lan	OS への専用内部 10Gb ポート (Windows では「LOM1-Switchboard」と呼ばれます)
lte_wan	4G LTE ポート
wifi_lan_ap	WLAN ポート (AP モード)
wifi_wan_sta	WLAN ポート (ステーション・モード)

コマンド例:

```
sudo uci show network
sudo uci show network.edge_lan
sudo uci show network.edge_lan.ipaddr
```

構成設定

表 32. DHCP サーバーの構成 (プロファイル dhcp)

構文

```
sudo uci set dhcp.<name>=dhcp
sudo uci set dhcp.<name>.ignore=<ignore>
sudo uci set dhcp.<name>.interface=<interface>
sudo uci set dhcp.<name>.start=<start>
sudo uci set dhcp.<name>.limit=<limit>
sudo uci set dhcp.<name>.leasetime=<leasetime>
sudo uci set dhcp.<name>.dynamicdhcp=<dynamicdhcp>
sudo uci set dhcp.<name>.force=<force>
sudo uci set dhcp.<name>.netmask=<netmask>
sudo uci set dhcp.<name>.dhcp_option=<dhcp_option>
sudo uci set dhcp.<name>.ra=<ra>
sudo uci set dhcp.<name>.dhcpv6=<dhcpv6>
sudo uci set dhcp.<name>.ndp=<ndp>
sudo uci set dhcp.<name>.ra_management=<ra_management>
sudo uci set dhcp.<name>.ra_default=<ra_default>
sudo uci add_list dhcp.<name>.dns=<dns>
sudo uci add_list dhcp.<name>.domain=<domain>
sudo uci commit dhcp
```

表 33. パラメーター

名前	タイプ	必須	デフォルト	説明
name	文字列	いいえ	なし	dhcp プール名。
ignore	ブール値	いいえ	0	dnsmasq が 1 に設定された場合にこのプールを無視するかどうかを指定します。
interface	論理インターフェース名	はい	なし	この DHCP アドレス・プールに関連付けられたインターフェースを指定します。/etc/config/network で定義されているインターフェースのいずれかでなければなりません。
start	整数	はい	100	クライアントにリースできる最小アドレスを計算するために、基になるインターフェースのネットワーク・アドレスからのオフセットを指定します。255 より大きな値にして、サブネットをまたがることができます。
limit	整数	はい	150	アドレス・プールのサイズを指定します (例: start=100、limit=150、最大アドレスは .249 になります)。
leasetime	文字列	はい	12h	12h や 30m などクライアントに分配するアドレスのリース時間を指定します。
dynamicdhcp	ブール値	いいえ	1	クライアント・アドレスを動的に割り当てます。0 に設定した場合、ethers ファイルにあるクライアントのみ提供します。
force	ブール値	いいえ	0	別の DHCP サーバーが同じネットワーク・セグメントで検出された場合でも、指定されたインターフェースで DHCP を強制的に機能させます。

表 33. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
dhcp_option	文字列のリスト	いいえ	なし	ここの ID dhcp_option は、アンダースコアで書かれている必要があります。これは最終的に dnsmasq によって使用されるため、ハイフンで –dhcp-option に変換されます。複数のオプションの値がこの network-id に対して指定でき、それらと全体の文字列の間にスペースが入ります。たとえば、「26,1470」や「option:mtu, 1470」とすると、DHCP ごとに MTU を割り当てることができます。これを機能させるには、クライアントが DHCP ごとの MTU を受け入れる必要があります。また、「3,192.168.1.1 6,192.168.1.1」とすると、ゲートウェイ・アドレスおよび dns サーバー・アドレスを提供します。
ra	文字列	いいえ	なし	ルーター・アドバタイズを有効 (server)、中継 (relay)、または無効 (disabled) のいずれにするかを指定します。
dhcpv6	文字列	いいえ	なし	DHCPv6 サーバーを有効 (server)、中継 (relay)、または無効 (disabled) のいずれにするかを指定します。
ndp	文字列	いいえ	なし	NDP を中継 (relay) するか、無効 (none) にするかを指定します。
ra_management	整数	いいえ	1	RA 管理モード: M フラグなし A フラグあり (0)、M フラグおよび A フラグともにあり (1)、M フラグあり A フラグなし (2)。

表 33. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
ra_default	整数	いいえ	0	RA メッセージでのデフォルト・ルーターの存続時間が次のように設定されます。デフォルト経路が存在し、グローバル IPv6 アドレスがある場合 (0)、デフォルト経路が存在し、グローバル IPv6 アドレスがない場合 (1)、両方の条件に当てはまらない場合 (2)。
dns	文字列	いいえ	なし	公表した DNS サーバー。
domain	文字列	いいえ	なし	公表したした DNS ドメイン。

コマンド例:

表 34. DHCPv4 サーバーの構成

ダウンリンク/内部リンクで x86/ WiFi AP/専用管理ポートを listen している DHCPv4 サーバーの構成

ダウンリンク・ポートの場合、IP の割り当て範囲: 1 ～ 100
`# sudo uci set dhcp.edge.start='1'`
`# sudo uci set dhcp.edge.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

内部リンク (X86 へ) の場合、IP の割り当て範囲: 1 ～ 100 (プリセット 5、x86_lan インターフェースなし): 1 ～ 100
`# sudo uci set dhcp.x86.start='1'`
`# sudo uci set dhcp.x86.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

WiFi AP モードの場合 (WiFi がステーション・モードに構成されているためにプリセット 4 を除く): 1 ～ 100
`# sudo uci set dhcp.wifi_lan_ap.start='1'`
`# sudo uci set dhcp.wifi_lan_ap.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

専用管理ポートの場合、IP の割り当て範囲: 1 ～ 100
`sudo uci set dhcp.lan.start='1'`
`sudo uci set dhcp.lan.limit='100'`
`sudo uci commit dhcp`
`sudo /etc/init.d/dnsmasq restart`

IP 関連設定の構成 (プロファイル: network)

表 35. IP 関連設定の構成 (プロファイル: network)

構文

```
sudo uci set network.<interface>=interface
sudo uci set network.<interface>.ifname=<ifname>
sudo uci set network.<interface>.proto=static
sudo uci set network.<interface>.ipaddr=<ipaddr>
sudo uci set network.<interface>.netmask=<netmask>
sudo uci set network.<interface>.gateway=<gateway>
sudo uci set network.<interface>.broadcast=<broadcast>
sudo uci set network.<interface>.dns=<dns>
sudo uci set network.<interface>.ip6assign=<ip6assign>
sudo uci set network.<interface>.ip6hint=<ip6hint>
sudo uci set network.<interface>.ip6ifaceid=<ip6ifaceid>
sudo uci set network.<interface>.auto=<auto>
sudo uci set network.<interface>.force_link=<force_link>
sudo uci set network.<interface>.macaddr=<macaddr>
sudo uci set network.<interface>.mtu=<mtu>
sudo uci set network.<interface>.metric=<metric>
```

表 36. パラメーター

名前	タイプ	必須	デフォルト	説明
interface	文字列	はい	なし	作成する論理インターフェース名。
ifname	文字列	はい	なし	デバイスの物理インターフェース名。
ipaddr	IP アドレス	はい (ip6addr が設定されていない場合)	なし	IP アドレス。ipaddr のリストにできます。つまり、複数の IP アドレスがインターフェースに割り当てられます。リストではなく、複数の ipaddr がオプションとして指定されている場合、最後のもののみが適用されます。
netmask	ネットマスク	はい (ip6addr が設定されていない場合)	なし	ネットマスク。
gateway	IP アドレス	いいえ	なし	デフォルト・ゲートウェイ。
broadcast	IP アドレス	いいえ	なし	ブロードキャスト・アドレス (設定されていない場合は自動生成されます)。
dns	IP アドレスのリスト	いいえ	なし	DNS サーバー。

表 36. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
ip6assign	プレフィックスの長さ	いいえ	なし	指定された長さのプレフィックスをこのインターフェースにデリゲートします (Barrier Breaker 以降のみ)。
ip6hint	プレフィックスのヒント (16 進数)	いいえ	なし	16 進数としてデリゲートする必要のあるサブプレフィックス ID のヒントとなります (Barrier Breaker 以降のみ)。
ip6ifaceid	ipv6 サフィックス	いいえ	::1	指定可能な値: 「eui64」、「random」、「::1:2」などの固定値です。IPv6 プレフィックス (「a:b:c:d::」など) をデリゲート・サーバーから受け取る場合は、サフィックス (「::1」など) を使用してこのインターフェースの IPv6 アドレス (「a:b:c:d::1」) を形成します。LAN 内の複数のルーターで役立ちます。
auto	ブール値	いいえ	proto なしの場合は 0、それ以外の場合は 1	ブート時にインターフェースを起動するかどうかを指定します。
force_link	ブール値	いいえ	protocol 静的の場合は 1、それ以外の場合は 0	IP アドレス、経路、ゲートウェイ (オプション) がインターフェースに割り当てられるタイミングを、リンクがアクティブであるかに関係ない (「1」)、あるいはリンクがアクティブになった後のみ (「0」) に指定します。「1」に設定されると、キャリア検出イベントがホット・プラグ・ハンドラーを起動しません。
macaddr	MAC アドレス	いいえ	なし	このインターフェースの MAC アドレスをオーバーライドします。

表 36. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
mtu	数値	いいえ	なし	このインターフェースのデフォルトの MTU をオーバーライドします。
metric	整数	いいえ	0	使用するデフォルト経路のメトリックを指定します。

コマンド例:

表 37. ダウンリンク/内部リンクから x86/ WiFi AP/専用管理ポートのベース IP の変更

ダウンリンク/内部リンクから x86/ WiFi AP/専用管理ポートのベース IP の変更

ダウンリンク・ポートを 192.168.71.254 に構成します。
`# sudo uci set network.edge_lan.ipaddr='192.168.71.254'`
`# sudo uci commit network`
`# sudo /etc/init.d/network restart`

内部リンク (X86 へ) の 192.168.73.254 への構成 (プリセット 5 に x86_lan インターフェースなし):
`# sudo uci set network.x86_lan.ipaddr='192.168.73.254'`
`# sudo uci commit network`
`# sudo /etc/init.d/network restart`

WiFI ポートの構成 (AP モード、プリセット 4 はステーション・モード): 192.168.74.254
`# sudo uci set network.wifi_lan_ap.ipaddr='192.168.74.254'`
`# sudo uci commit network`
`# sudo /etc/init.d/network restart`

専用管理ポートの 192.168.70.254 への構成
`# sudo uci set network.mgmt_xcc_lan.ipaddr='192.168.70.254'`
`# sudo uci commit network`
`# sudo /etc/init.d/network restart`

eth3 と eth6 の edge_lan を取り外します:

```
# show interfaces in edge ports

sudo uci show network.edge_lan.ifname



# Remove eth3 and eth6 from edge_lan.ifname

sudo uci set network.edge_lan.ifname='eth1'

sudo uci commit

sudo /etc/init.d/network restart
```

注：ネットワーク・インターフェースに割り当てられていないポート (ethx) は、**disable** として設定されます。

ワイヤレス設定の構成 (WLAN)

Wifi デバイスは、システム上にある物理無線デバイスを参照します。このセクションに記載されているオプションでは、チャネルなどこの無線デバイスのすべてのワイヤレス・インターフェースで共通のプロパティについて説明しています。

表 38. ワイヤレス・デバイス

構文

```
sudo uci set wireless.radio0.type=<type>
sudo uci set wireless.radio0.channel=<channel>
sudo uci set wireless.radio0.hwmode=<hwmode>
sudo uci set wireless.radio0.htmode=<htmode>
sudo uci set wireless.radio0.disabled=<disabled>
```

表 39. パラメーター

名前	タイプ	必須	デフォルト	説明
type	文字列	はい	(自動検出)	このタイプは、最初の無線デバイスの検出中の初回ブート時に決定されます。通常は変更する必要はありません。
hwmode	文字列	いいえ	11n	使用するワイヤレス・プロトコルを選択します。使用可能な値は 11b、11g、および 11a です。11ng および 11ng は使用可能なオプションではないことに注意してください。
htmode	文字列	いいえ	HT40	802.11n および 802.11ac モードでのチャネル幅を指定します。指定可能な値は HT20、HT40-、HT40+、HT40、または VHT20、VHT40、VHT80、VHT160、NOHT disables 11n です

表 39. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
disabled	ブール値	いいえ	1	1 に設定した場合、無線アダプターを無効にします。このオプションを削除するか、0 に設定すると、アダプターが有効になります
channel	整数 (1 ～ 11)	はい	11	使用するワイヤレス・チャネルを指定します。

コマンド例:

表 40. デフォルトのチャネル設定

802.11n モードでワイヤレス機能を有効にするには、デフォルト・チャネルを 11 に設定します

```
sudo uci set wireless.radio0.channel='11'
sudo uci set wireless.radio0.hwmode='11n'
sudo uci set wireless.radio0.disabled='0'
sudo uci commit wireless
sudo wifi
```

ワイヤレス・インターフェース

表 41. ワイヤレス・インターフェース

構文

```
sudo uci set wireless.default_radio0.encryption=<encryption>
sudo uci set wireless.default_radio0.ssid=<ssid>
sudo uci set wireless.default_radio0.mode=<mode>
sudo uci set wireless.default_radio0.key=<key>
sudo uci set wireless.default_radio0.network=<network>
```

表 42. パラメーター

名前	タイプ	必須	デフォルト	説明
network	文字列	はい	wifi_lan_ap	ワイヤレスを接続するネットワーク・インターフェースを指定します。指定可能な値は wifi_lan_ap、wifi_wan_sta です。
mode	文字列	はい	ap	ワイヤレス・ネットワーク・インターフェース・コントローラーの動作モードを選択します。指定可能な値は ap、sta です。

表 42. パラメーター (続き)

名前	タイプ	必須	デフォルト	説明
ssid	文字列	はい	hodaka_ap	ワイヤレス・ネットワークのブロードキャストされた SSID。管理対象モードの場合は、接続しているネットワークの SSID
encryption	文字列	はい	psk2	ワイヤレス暗号化方式。 1. AP モード: WPA2 パーソナルのみ、値: psk2 2.ステーション・モード: WPA2 エンタープライズおよび WPA2 パーソナル
key	整数または文字列	はい	ユーザー定義	どの WPA-PSK モードでも、これは事前共有鍵を導き出す事前共有パスフレーズを指定する文字列があります。平文キーの長さは 8-63 文字にする必要があります。64 文字の 16 進数の文字列が指定されている場合は、代わりに事前共有鍵として直接使用されます。どの **WPA-エンタープライズ** AP モードでも、このオプションには異なる解釈があります。

WPA エンタープライズ (クライアント・モード)

WPA エンタープライズのクライアント関連オプションのリスト:

名前	デフォルト	説明
eap_type	(なし)	使用する EAP プロトコルを定義します。指定可能な値は EAP-TLS の場合は tls、EAP-PEAP の場合は peap または ttls です
auth	MSCHAPV2	“auth=PAP”/PAP/MSCHAPV2 - 使用するフェーズ 2 (内部) 認証方式を定義します。eap_type が peap または ttls である場合のみ指定可能です
identity	(なし)	認証中に送信する EAP ID

名前	デフォルト	説明
password	(なし)	EAP 認証中に送信するパスワード
ca_cert	(なし)	認証に使用される CA 証明書のパスを指定します
client_cert	(なし)	認証に使用されるクライアント証明書を指定します
priv_key	(なし)	認証に使用される秘密鍵ファイルへのパスを指定します。eap_type が tls に設定されている場合のみ指定可能です
priv_key_pwd	(なし)	秘密鍵ファイルをロック解除するためのパスワードで、priv_key と組み合わせた場合のみ機能します

注：Active Directory サーバーで WPA エンタープライズ・タイプ PEAP を使用する場合は、「auth」オプションを「auth=MSCHAPV2」または「auth=PAP」に設定する必要があります。

コマンド例:

表 43. ワイヤレス・クライアント・モード

ワイヤレスをステーション・モードに構成するには、WPA2 パーソナルで SSID が Hoda-WF2G-TEST である AP に接続します。
`sudo uci set wireless.default_radio0.encryption='psk2'`
`sudo uci set wireless.default_radio0.ssid='Hoda-WF2G-TEST'`
`sudo uci set wireless.default_radio0.mode='sta'`
`sudo uci set wireless.default_radio0.key='hodaka#1'`
`sudo uci set wireless.default_radio0.network='wifi_wan_sta'`
`sudo uci commit wireless`
`sudo wifi`

ワイヤレスをステーション・モードに構成するには、WPA2 エンタープライズで SSID が Hoda-WF2G-TEST である AP に接続します。
`sudo uci set wireless.default_radio0.network='wifi_wan_sta'`
`sudo uci set wireless.default_radio0.mode='sta'`
`sudo uci set wireless.default_radio0.ssid='Hoda-WF2G-TEST'`
`sudo uci set wireless.default_radio0.encryption='wpa2'`
`sudo uci set wireless.default_radio0.doth='1'`
`sudo uci set wireless.default_radio0.eap_type='peap'`
`sudo uci set wireless.default_radio0.auth='EAP-MSCHAPV2'`
`sudo uci set wireless.default_radio0.identity='123'`
`sudo uci set wireless.default_radio0.password='123'`
`sudo uci commit wireless`
`sudo wifi`

LTE 設定の構成

表 44. LTE 設定の構成

構文

`sudo uci set network.lte_wan.apn=<apn>`
`sudo uci set network.lte_wan.pincode=<pincode>`
`sudo uci set network.lte_wan.username=<username>`
`sudo uci set network.lte_wan.password=<password>`
`sudo uci set network.lte_wan.pdptype=<pdptype>`
`sudo uci set network.lte_wan.auth=<auth>`

表 45. パラメーター

名前	タイプ	必須	デフォルト	説明
apn	文字列	はい	インターネット	使用される APN
pincode	数値	いいえ	(なし)	SIM カードをロック解除する PIN コード
username	文字列	いいえ	(なし)	PAP/CHAP 認証のユーザー名
password	文字列	いいえ	(なし)	PAP/CHAP 認証のパスワード
auth	文字列	いいえ	chap	認証タイプ: **pap**、**chap**、**both**、**none**
pdptype	文字列	いいえ	IPv4	使用される IP スタック・モード、IP (IPv4 の場合)、IPV6 (IPv6 の場合)、または IPV4V6 (デュアル・スタックの場合)
plmn	数値	いいえ	(なし)	最初の 3 桁は **mcc** (モバイル国別コード) で、最後の 3 桁は **mnc** (モバイル・ネットワーク・コード) です。たとえば、plmn=338020 の場合、mcc は 338 で、mnc は 020 となります

コマンド例:

```
sudo uci set network.lte_wan.pincode='0000'
sudo uci set network.lte_wan.apn='testapn'
sudo uci set network.lte_wan.username='Name1'
sudo uci set network.lte_wan.password='Password'
sudo uci commit network
sudo /etc/init.d/network restart
```

構成のインポートおよびエクスポート

表 46. 構成のインポートおよびエクスポート

ローカル PC に組み込みスイッチ構成をバックアップします。
 	
`# Generate backup`
 	
`sudo sysupgrade -b /tmp/backup.tar.gz`
 	
`ls /tmp/backup.tar.gz`
 	
`# Download backup`
 	
`scp oper@192.168.70.254://tmp/backup.tar.gz ./`

ローカル PC から以前に保存した組み込みスイッチ構成を復元します。
 	
`# Upload backup`
 	
`scp backup.tar.gz oper@192.168.70.254://tmp/backup.tar.gz`
 	
`# Restore backup`
 	
`ls /tmp/backup.tar.gz`
 	
`sudo sysupgrade -r /tmp/backup.tar.gz`
 	
`sudo reboot`

注：バックアップ・ファイルで構成を変更した場合は、バックアップ・ファイルの tar を展開して変更した後に、「home」および「etc」フォルダーが含まれるルート・ディレクトリーに移動し、次のコマンドを実行してバックアップ・ファイルの tar をもう一度行います。`tar cvfz backup.tar.gz`

組み込みスイッチのファームウェアのアップグレード

1. ラップトップを BMC 管理ポートに接続し、ラップトップの IP を「192.168.70.xxx」に構成します。
2. scp でクライアントからスイッチ・ボードにイメージを転送します。
   - [Linux OS] `$> scp -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null ./se350-hyl403g-r378-bd144013.bin.sign oper@192.168.70.254://tmp/`
   - [Windows OS] `.\pscp.exe -scp .\se350-hyl403g-r378-bd144013.bin.sign oper@192.168.70.254://tmp/`
3. スイッチ・ボードの CLI でファームウェアを更新します: (「sudo sysupgrade -n」の場合、すべての設定が出荷時のデフォルト値にリセットされます) `$> sudo sysupgrade /tmp/se350-hyl403g-r378-bd144013.bin.sign`

組み込みスイッチ上のリモート構成の静的経路

クラウド・ポートがアクティブな場合、クラウド・ポートから取得されたデフォルト・ゲートウェイによって、組み込みスイッチの既存のデフォルト・ゲートウェイが上書きされます。管理ポートに戻るネットワーク・トラフィックがクラウド・ポートにリダイレクトされるため、ユーザーは組み込みスイッチ IP に (異なる IP セグメントから) リモートで接続できなくなります。次の例では、「静的経路」を追加して、クラウド・ポートがアクティブなときに組み込みスイッチ IP へのリモート構成を許可する方法を示しています。

```
#.If ip domain of management port is "172.18.x.x", with default gateway "172.18.221.254".


#.To force traffic targets to 172.18.0.0/16 & 10.0.0.0/8 to go through gateway 172.18.221.254


sudo uci set network.rtmgmt1=route

sudo uci set network.rtmgmt1.interface='mgmt_xcc_lan'

sudo uci set network.rtmgmt1.target='172.18.0.0'

sudo uci set network.rtmgmt1.netmask='255.255.0.0'

sudo uci set network.rtmgmt1.gateway='172.18.221.254'


sudo uci set network.rtmgmt2=route

sudo uci set network.rtmgmt2.interface='mgmt_xcc_lan'

sudo uci set network.rtmgmt2.target='10.0.0.0'

sudo uci set network.rtmgmt2.netmask='255.0.0.0'

sudo uci set network.rtmgmt2.gateway='172.18.221.254'


sudo uci commit

sudo /etc/init.d/network restart
```

ファイアウォール設定

ファイアウォールを設定するには、以下の情報を使用します。

デフォルト・ファイアウォールの設定

デフォルト・セクションでは、特定のゾーンに属していないグローバル・ファイアウォール設定を宣言します。

表 47. デフォルト・ファイアウォールの設定

構文

`sudo uci set firewall.@defaults[0].input=<input>`
`sudo uci set firewall.@defaults[0].output=<output>`
`sudo uci set firewall.@defaults[0].forward=<forward>`
`sudo uci set firewall.@defaults[0].syn_flood=<syn_flood>`
`sudo uci set firewall.@defaults[0].drop_invalid=<drop_invalid>`

表 48. パラメーター

名前	タイプ	必須	デフォルト	説明
input	文字列	いいえ	REJECT	フィルター・テーブルの INPUT チェーンのポリシーを設定します。
output	文字列	いいえ	REJECT	フィルター・テーブルの OUTPUT チェーンのポリシーを設定します。
forward	文字列	いいえ	REJECT	フィルター・テーブルの FORWARD チェーンのポリシーを設定します。
syn_flood	ブール値	いいえ	0	SYN フラッド保護を有効にします (synflood_protect の設定により廃止)。
drop_invalid	ブール値	いいえ	0	無効なパケットをドロップします (たとえば、どのアクティブな接続にも一致しない場合)。

コマンド例:

表 49. コマンド例

```
sudo uci set firewall.@defaults[0].input=ACCEPT
sudo uci set firewall.@defaults[0].output= ACCEPT
sudo uci set firewall.@defaults[0].forward= ACCEPT
sudo uci set firewall.@defaults[0].syn_flood=1
sudo uci set firewall.@defaults[0].drop_invalid=1
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

新しいゾーンの追加

このセクションでは、「test」の共通プロパティを定義します。input および output のオプションで、このゾーンへのトラフィックの出力および入力に関するデフォルト・ポリシーを設定し、forward のオプションでゾーン内の異なるネットワーク間で転送されるトラフィックのポリシーを記述します。カバーされるネットワークによって、このゾーンのメンバーである利用可能なネットワークを指定します。

表 50. 新しいゾーンの追加

構文

```
sudo uci add firewall zone
sudo uci set firewall.@zone[-1].name=<name>
sudo uci set firewall.@zone[-1].input=<input>
sudo uci set firewall.@zone[-1].output=<output>
sudo uci set firewall.@zone[-1].forward=<forward>
sudo uci set firewall.@zone[-1].masq=<masq>
sudo uci set firewall.@zone[-1].mtu_fix=<mtu_fix>
sudo uci set firewall.@zone[-1].network=<network>
sudo uci set firewall.@zone[-1].family=<family>
sudo uci set firewall.@zone[-1].masq_src=<masq_src>
sudo uci set firewall.@zone[-1].masq_dest=<masq_dest>
sudo uci set firewall.@zone[-1].conntrack=<conntrack>
sudo uci set firewall.@zone[-1].log=<log>
sudo uci set firewall.@zone[-1].log_limit=<log_limit>
udo uci commit firewall
```

表 51. パラメーター

パラメーター	タイプ	必須	デフォルト	説明
name	ゾーン名	はい	なし	固有のゾーン名。動作するファイアウォール・ゾーン名の最大長は、11 文字です。
input	文字列	いいえ	REJECT	フィルター・テーブルの INPUT チェーンのポリシーを設定します。
output	文字列	いいえ	REJECT	フィルター・テーブルの OUTPUT チェーンのポリシーを設定します。
forward	文字列	いいえ	REJECT	フィルター・テーブルの FORWARD チェーンのポリシーを設定します。
masq	ブール値	いいえ	0	送信ゾーンのトラフィックをマスカレードするかどうかを指定します。これは通常、wan ゾーンで有効になっています。
mtu_fix	ブール値	いいえ	0	送信ゾーン・トラフィックの MSS クランプを有効にします。

表 51. パラメーター (続き)

パラメーター	タイプ	必須	デフォルト	説明
network	リスト	いいえ	なし	このゾーンに接続されているインターフェースのリスト。省略して、追加* オプション、サブネット、またはデバイスを指定しない場合は、デフォルトで name の値が使用されます。ネットワーク構成で定義されているエイリアス・インターフェースは、有効な「スタンドアロン」ネットワークとして使用できません。リスト構文は uci に説明されているように使用します。
family	文字列	いいえ	0	iptables 規則を生成するプロトコル・ファミリー (ipv4、ipv6、または any)。
masq_src	サブネットのリスト	いいえ	0.0.0.0/0	指定された送信元サブネットに対するマスカレードを制限します。サブネットの前に！をつけることで否定が可能です。複数のサブネットを使用できます。
masq_dest	サブネットのリスト	いいえ	0.0.0.0/0	指定された宛先サブネットに対するマスカレードを制限します。サブネットの前に！をつけることで否定が可能です。複数のサブネットを使用できます。
conntrack	ブール値	いいえ	マスカレードが使用されている場合は 1、そうでない場合は 0	このゾーンの接続追跡を強制します (接続追跡については注を参照)。
log	ブール値	いいえ	0	このゾーンのトラフィックのリジェクトとドロップに関するログ規則を作成します。
log_limit	文字列	いいえ	10/分	一定間隔のログ・メッセージの量を制限します。

コマンド例:

表 52. コマンド例

```
sudo uci add firewall zone
sudo uci set firewall.@zone[-1].name=test
sudo uci set firewall.@zone[-1].input=ACCEPT
sudo uci set firewall.@zone[-1].output= ACCEPT
sudo uci set firewall.@zone[-1].forward= ACCEPT
sudo uci set firewall.@zone[-1].masq=<masq>
sudo uci set firewall.@zone[-1].mtu_fix=<mtu_fix>
sudo uci set firewall.@zone[-1].network=<network>
sudo uci set firewall.@zone[-1].family=<family>
sudo uci set firewall.@zone[-1].masq_src=<masq_src>
sudo uci set firewall.@zone[-1].masq_dest=<masq_dest>
sudo uci set firewall.@zone[-1].conntrack=<conntrack>
sudo uci set firewall.@zone[-1].log=<log>
sudo uci set firewall.@zone[-1].log_limit=<log_limit>
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

新しい転送の追加

次のセクションでゾーン間のトラフィック・フローを制御し、特定の方向の MSS クランプを有効にすることができます。1 方向のみが転送規則によってカバーされます。2 つのゾーン間での双方向トラフィック・フローを許可するには、互いに逆の src と dest がある 2 つの転送が必要になります。

表 53. 新しい転送の追加

構文

```
sudo uci set firewall.@zone[-1].src=<src>
sudo uci set firewall.@zone[-1].dest=<dest>
sudo uci commit firewall
```

表 54. パラメーター

パラメーター	タイプ	必須	デフォルト	説明
src	ゾーン名	はい	なし	トラフィックの送信元ゾーンを指定します。定義されたゾーン名の 1 つを参照する必要があります。
dest	ゾーン名	はい	なし	トラフィックの宛先ゾーンを指定します。定義されたゾーン名の 1 つを参照する必要があります。

コマンド例:

表 55. コマンド例

```
sudo uci set firewall.@zone[-1].src=test
sudo uci set firewall.@zone[-1].dest=lan
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

新しいポート転送の追加

ポート転送 (DNAT) は、リダイレクト・セクションによって定義されます。特定の規則に一致する指定された送信元ゾーンでのすべての着信トラフィックが、指定された内部ホストに送られます。リダイレクトは、一般に「ポート転送」および「仮想サーバー」としても知られています。ポート範囲は 6666:6670 のように「開始:停止」で指定されます。これは iptables 構文に類似しています。

表 56. 新しいポート転送の追加

構文

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=<enabled>
sudo uci set firewall.@redirect[-1].name=<name>
sudo uci set firewall.@redirect[-1].proto=<proto>
sudo uci set firewall.@redirect[-1].src=<src>
sudo uci set firewall.@redirect[-1].src_mac=<src_mac>
sudo uci set firewall.@redirect[-1].src_ip=<src_ip>
sudo uci set firewall.@redirect[-1].src_port=<src_port>
sudo uci set firewall.@redirect[-1].src_dip=<src_dip>
sudo uci set firewall.@redirect[-1].src_dport=<src_dport>
sudo uci set firewall.@redirect[-1].dest=<dest>
sudo uci set firewall.@redirect[-1].dest_ip=<dest_ip>
sudo uci set firewall.@redirect[-1].dest_port=<dest_port>
sudo uci set firewall.@redirect[-1].reflection=<reflection>
sudo uci commit firewall
```

表 57. パラメーター

パラメーター	タイプ	必須	デフォルト	説明
enabled	文字列	いいえ	1 または yes	リダイレクト規則を有効にするかどうかを設定します。
name	文字列	いいえ	なし	固有のリダイレクト名。
proto	プロトコル名または数値	はい	tcp udp	指定されたプロトコルを使用して、着信トラフィックを照合します。

表 57. パラメーター (続き)

パラメーター	タイプ	必須	デフォルト	説明
src	ゾーン名	いいえ	DNAT ターゲットの場合は yes	トラフィックの送信元ゾーンを指定します。定義されたゾーン名の 1 つを参照する必要があります。一般的なポート転送の場合、これは通常 wan です。
src_mac	MAC アドレス	いいえ	なし	指定された MAC アドレスからの着信トラフィックを照合します。
src_ip	IP アドレス	いいえ	なし	指定された送信元 IP アドレスからの着信トラフィックを照合します。
src_port	ポートまたは範囲	いいえ	なし	クライアント・ホストで指定された送信元ポートまたはポート範囲 (例: 「5000-5100」) から発信された着信トラフィックを照合します。
src_dip	IP アドレス	はい (SNAT ターゲットの場合)	なし	DNAT の場合、特定の宛先 IP アドレスに向けられた着信トラフィックを照合します。SNAT の場合、送信元アドレスを特定のアドレスに書き換えます。
src_dport	ポートまたは範囲	いいえ	なし	DNAT の場合、このホストで指定された宛先ポートまたはポート範囲 (例: 「5000-5100」) に向けられた着信トラフィックを照合します。SNAT の場合、送信元ポートを特定の値に書き換えます。

表 57. パラメーター (続き)

パラメーター	タイプ	必須	デフォルト	説明
dest	ゾーン名	はい (SNAT ターゲットの場合)	なし	トラフィックの宛先ゾーンを指定します。定義されたゾーン名の 1 つを参照する必要があります。Attitude Adjustment の DNAT ターゲットの場合、これが lan に等しい場合にのみ NAT リフレクションが機能します。
dest_ip	IP アドレス	はい (DNAT ターゲットの場合)	なし	DNAT の場合、照合した着信トラフィックを指定された内部ホストにリダイレクトします。SNAT の場合、特定のアドレスに向けられたトラフィックを照合します。DNAT では、ifconfig に示されているように、dest_ip の値がルーターのローカル IP アドレスと一致する場合は、規則が DNAT + input「受諾」規則に変換されます。それ以外の場合は、DNAT + forward 規則です。
dest_port	ポートまたは範囲	いいえ	なし	DNAT の場合、照合した着信トラフィックを内部ホストの指定されたポートにリダイレクトします。SNAT の場合、特定のポートに向けられたトラフィックを照合します。ポートまたは範囲は 1 つしか指定できません (例:「5000-5100」)。規則と異なるポートを指定することはできません (以下を参照)。
reflection	ブール値	いいえ	1	このリダイレクトの NAT リフレクションをアクティブにします。DNAT ターゲットに適用可能です。

コマンド例:

表 58. http (HTTPS ではない) トラフィックを 192.168.1.10 で実行されている Web サーバーに転送します。

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=1
sudo uci set firewall.@redirect[-1].proto=tcp
sudo uci set firewall.@redirect[-1].src=wan
sudo uci set firewall.@redirect[-1].src_dport=80
sudo uci set firewall.@redirect[-1].dest=lan
sudo uci set firewall.@redirect[-1].dest_ip=192.168.1.10
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

新しいトラフィック規則の追加

ポート転送 (DNAT) は、リダイレクト・セクションによって定義されます。特定の規則に一致する指定された送信元ゾーンでのすべての着信トラフィックが、指定された内部ホストに送られます。リダイレクトは、一般に「ポート転送」および「仮想サーバー」としても知られています。ポート範囲は 6666:6670 のように「開始:停止」で指定されます。これは iptables 構文に類似しています。

表 59. 新しいトラフィック規則の追加

構文

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].enabled=<enabled>
sudo uci set firewall.@rule[-1].name=<name>
sudo uci set firewall.@rule[-1].family=<family>
sudo uci set firewall.@rule[-1].proto=<proto>
sudo uci set firewall.@rule[-1].src=<src>
sudo uci set firewall.@rule[-1].src_mac=<src_mac>
sudo uci set firewall.@rule[-1].src_ip=<src_ip>
sudo uci set firewall.@rule[-1].src_port=<src_port>
sudo uci set firewall.@rule[-1].dest=<dest>
sudo uci set firewall.@rule[-1].dest_ip=<dest_ip>
sudo uci set firewall.@rule[-1].dest_port=<dest_port>
sudo uci set firewall.@rule[-1].target=<target>
sudo uci set firewall.@rule[-1].weekdays=<weekdays>
sudo uci set firewall.@rule[-1].monthdays=<monthdays>
sudo uci set firewall.@rule[-1].start_time=<start_time>
sudo uci set firewall.@rule[-1].stop_time=<stop_time>
sudo uci set firewall.@rule[-1].start_date=<start_date>
sudo uci set firewall.@rule[-1].stop_date=<stop_date>
sudo uci set firewall.@rule[-1].utc_time=<utc_time>
uci commit firewall
```

表 60. パラメーター

パラメーター	タイプ	必須	デフォルト	説明
enabled	ブール値	いいえ	はい	規則を有効または無効にします。
name	文字列	いいえ	なし	固有の規則名。
family	文字列	いいえ	any	iptables 規則を生成するプロトコル・ファミリー (ipv4、ipv6、または any)。
proto	プロトコル名または数値	いいえ	tcp udp	指定されたプロトコルを使用して、着信トラフィックを照合します。tcp、udp、tcpudp、udplite、icmp、esp、ah、sctp、またはすべてのいずれか、あるいはこれらのプロトコルのいずれかや別のプロトコルを表す数値に設定できます。/etc/protocols のプロトコル名も使用できます。数値 0 はすべてに相当します。
src	ゾーン名	はい (ファイアウォール v2、バージョン 58 以降はオプション)	なし	トラフィックの送信元ゾーンを指定します。定義されたゾーン名の 1 つを参照する必要があります。
src_mac	MAC アドレス	いいえ	なし	指定された MAC アドレスからの着信トラフィックを照合します。
src_ip	IP アドレス	いいえ	なし	指定された送信元 IP アドレスからの着信トラフィックを照合します。
src_port	ポートまたは範囲	いいえ	なし	関連する proto を指定した場合、指定された送信元ポートまたはポート範囲 (例:「5000:5100」、ポート範囲はすべてのプロトコルに適用されない) の着信トラフィックを照合します。複数のポートは '80 443 465' 1 のように指定できます。
dest	ゾーン名	いいえ	なし	トラフィックの宛先ゾーンを指定します。定義されたゾーン名の 1 つまたは任意のゾーンの * を参照する必要があります。指定した場合、転送されるトラフィックに規則が適用されます。それ以外の場合は、input 規則として扱われます。
dest_ip	IP アドレス	いいえ	なし	指定された宛先 IP アドレスに向けられた着信トラフィックを照合します。dest ゾーンがない場合、input 規則として扱われます。
dest_port	ポートまたは範囲	いいえ	なし	関連する proto を指定した場合、特定の宛先ポートまたはポート範囲 (例:「5000:5100」、ポート範囲はすべてのプロトコルに適用されない) に向けられた着信トラフィックを照合します。複数のポートは '80 443 465' 1 のように指定できます。
target	文字列	はい	DROP	このリダイレクトの NAT リフレクションをアクティブにします。DNAT ターゲットに適用可能です。

表 60. パラメーター (続き)

パラメーター	タイプ	必須	デフォルト	説明
weekdays	平日のリスト	いいえ	(常時)	指定した場合は、指定された曜日のトラフィックのみ照合します。たとえば、日曜日、月曜日、木曜日、日曜にのみ照合するには sun mon thu fri とします。頭に感嘆符をつけることでリストを逆転させることができます。たとえば、! sat sun で土曜日と日曜日以外は常時照合します。
monthdays	日付のリスト	いいえ	(常時)	指定した場合、月の指定された日のトラフィックのみ照合します。たとえば、月の 2 日、5 日、30 日にのみ照合するには 2 5 30 とします。頭に感嘆符をつけることでリストを逆転させることができます。たとえば、!31 で月の 31 日以外は常時照合します。
start_time	時刻 (hh:mm:ss)	いいえ	(常時)	指定した場合、1 日の指定した時間 (この時間を含む) 以降のトラフィックのみ照合します。
stop_time	時刻 (hh:mm:ss)	いいえ	(常時)	指定した場合、1 日の指定した時間 (この時間を含む) 以前のトラフィックのみ照合します。
start_date	日付 (yyyy-mm-dd)	いいえ	(常時)	指定した場合、指定した日 (この日を含む) 以降のトラフィックのみ照合します。
stop_date	日付 (yyyy-mm-dd)	いいえ	(常時)	指定した場合、指定した日 (この日を含む) 以前のトラフィックのみ照合します。
utc_time	ブール値	いいえ	0	指定されたすべての時間値を現地時間ではなく UTC 時間として扱います。

コマンド例:

表 61. 指定されたホスト・アドレスへの接続試行をすべてブロックします。

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].enabled=1
sudo uci set firewall.@rule[-1].src=lan
sudo uci set firewall.@rule[-1].dest=wan
sudo uci set firewall.@rule[-1].dest_ip=123.45.67.89
sudo uci set firewall.@rule[-1].target=REJECT
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

新しい送信元 NAT の追加

送信元 NAT は、組み込みスイッチ・システムがパケットの送信元であるかのように発信パケットを変更します。

コマンド例:

表 62. UDP および TCP トラフィックの送信元 NAT の定義

IP アドレス 10.55.34.85 のホストから発信してポート 123 に向けられた UDP および TCP トラフィックの送信元 NAT を定義します。

送信元アドレスは 63.240.161.99 に書き換えられます。

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=1
sudo uci set firewall.@redirect[-1].src=lan
sudo uci set firewall.@redirect[-1].src_ip=10.55.34.85
sudo uci set firewall.@redirect[-1].src_dip=63.240.161.99
sudo uci set firewall.@redirect[-1].dest=wan
sudo uci set firewall.@redirect[-1].dest_port=123
sudo uci set firewall.@redirect[-1].target=SNAT
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

OpenVPN クライアントの設定

OpenVPN クライアントの設定を適用するには、この情報を使用します。

OpenVPN クライアントの設定を適用するには、SE350 が以下の前提条件を満たしている必要があります。

- クラウド・ポート (インターネット接続) がセットアップされている。
- SE350 のシステム時刻が正しい (XCC Web UI の右上で確認)。
- SE350 で OpenVPN (SSL VPN) クライアントのみをサポートしている。
- VPN のセットアップ前に VPN サービス・プロバイダーに構成ファイルを要求している。

VPN サービス・プロバイダーが提供する OpenVPN 構成ファイル (my-vpn.conf や pass.txt など) をインポートするには、以下の手順を実行します。

ステップ 1. SCP を使用して、構成ファイル (my-vpn.conf や pass.txt) を `/home/oper/openvpn/` に転送します。

```
oper@OpenWrt:~$ scp jackshih@192.168.70.200:/home/jackshih/my-vpn.conf /home/oper/openvpn/
my-vpn.conf
oper@OpenWrt:~$ scp jackshih@192.168.70.200:/home/jackshih/pass.txt /home/oper/openvpn/pass.txt
```

注：OpenVPN の「config」オプションを変更して、構成ファイル名を指定することもできます。

```
oper@OpenWrt:~$ sudo uci set openvpn.custom_config.config='/home/oper/openvpn/my-vpn.conf'
oper@OpenWrt:~$ sudo uci commit openvpn
```

ステップ 2. VPN クライアントを有効にします。

```
oper@OpenWrt:~$ sudo uci set openvpn.custom_config.enabled='1'
oper@OpenWrt:~$ sudo uci commit openvpn
```

ステップ 3. ネットワークを構成します。

注：VPN クライアントのネットワーク・インターフェース名は、VPN 構成ファイルのトンネル・デバイスに基づきます。たとえば、my-vpn.conf に「dev tun0」がある場合は、「tun0」に設定する必要があります。

```
oper@OpenWrt:~$ sudo uci set network.vpn.ifname='tunnel_name'
oper@OpenWrt:~$ sudo uci commit network
oper@OpenWrt:~$ sudo /etc/init.d/network restart
```

ステップ 4. サービスを再開します。

```
oper@OpenWrt:~$ sudo /etc/init.d/openvpn restart
```

ステップ 5. 数秒経ってからインターフェース名 (例: 「tun0」) を確認して、IP アドレスが取得されていることを確認します。

オペレーティング・システムのデプロイ

サーバーにオペレーティング・システムをデプロイするには、いくつかのオプションが使用できます。

利用可能なオペレーティング・システム

- Microsoft Windows Server
- VMware ESXi

  注：VMware ESXI のブート・ドライブ: VMware ESXi ブート・サポートの場合、特定の M.2 ドライブのみが、その耐久性に基づいてサポートされます。特定の情報については、Lenovo サポートのヘルプ HT512201 を参照してください。
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

オペレーティング・システムの全リスト:https://lenovopress.lenovo.com/osig。

ツール・ベースのデプロイメント

- **マルチサーバー**

  使用可能なツール:

  – Lenovo XClarity Administrator

    http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/compute_node_image_deployment.html

  – Lenovo XClarity Essentials OneCLI

    https://pubs.lenovo.com/lxce-onecli/onecli_r_uxspi_proxy_tool

  – Lenovo XClarity IntegratorSCCM 向けデプロイメント・パック (Windows オペレーティング・システム専用)

    https://pubs.lenovo.com/lxci-deploypack-sccm/dpsccm_c_endtoend_deploy_scenario
- **シングル・サーバー**

  使用可能なツール:

  – Lenovo XClarity Provisioning Manager

    https://pubs.lenovo.com/lxpm-overview/にある、ご使用のサーバーと互換性のある LXPM に関する資料の「OS インストール」セクション

  – Lenovo XClarity Essentials OneCLI

    https://pubs.lenovo.com/lxce-onecli/onecli_r_uxspi_proxy_tool

  – Lenovo XClarity IntegratorSCCM 向けデプロイメント・パック (Windows オペレーティング・システム専用)

    https://pubs.lenovo.com/lxci-deploypack-sccm/dpsccm_c_endtoend_deploy_scenario

手動デプロイメント

上記のツールにアクセスできない場合は、以下の手順に従って、対応する「*OS インストール・ガイド*」をダウンロードし、ガイドを参照してオペレーティング・システムを手動でデプロイしてください。

1. https://datacentersupport.lenovo.com/solutions/server-os へ進んでください。
2. ナビゲーション・ウインドウでオペレーティング・システムを選択して**Resources (リソース)**をクリックします。
3. 「OS インストール・ガイド」を見つけ、インストール手順をクリックします。次に、指示に従って操作システム・デプロイメント・タスクを完了します。

サーバー構成のバックアップ

サーバーをセットアップしたり、構成に変更を加えたりした後は、サーバー構成の完全なバックアップを作成することをお勧めします。

以下のサーバー・コンポーネントのバックアップを作成してください。

- **管理プロセッサー**

  管理プロセッサー構成は、Lenovo XClarity Controller インターフェースを使用してバックアップすることができます。管理プロセッサー構成のバックアップについて詳しくは、以下を参照してください。

  https://pubs.lenovo.com/lxcc-overview/ にある、ご使用のサーバーと互換性のある XCC に関する資料の「BMC 構成のバックアップ」セクション。

  または、Lenovo XClarity Essentials OneCLI から `save` コマンドを使用して、すべての構成設定のバックアップを作成することもできます。`save` コマンドについて詳しくは、以下を参照してください。

  https://pubs.lenovo.com/lxce-onecli/onecli_r_save_command

- **オペレーティング・システム**

  サーバーでオペレーティング・システムおよびユーザー・データをバックアップするには、各ユーザーに合わせたバックアップ方式を使用します。

重要プロダクト・データ (VPD) の更新

システムの初期セットアップ後、資産タグや汎用固有 ID (UUID) など、一部の重要プロダクト・データ (VPD) を更新できます。

Universal Unique Identifier (UUID) の更新

必要に応じて、汎用固有 ID (UUID) を更新できます。

UUID を更新する方法は 2 つあります。

- Lenovo XClarity Provisioning Manager から

  Lenovo XClarity Provisioning Manager から UUID を更新するには、次のようにします。

  1. サーバーを起動して画面の指示に従ってキーを押します。(詳しくは、https://pubs.lenovo.com/lxpm-overview/ にあるご使用のサーバーと互換性のある LXPM 資料の「スタートアップ」セクションを参照してください) デフォルトでは、Lenovo XClarity Provisioning Manager インターフェースが表示されます。
  2. 始動管理者パスワードが必要な場合は、パスワードを入力します。
  3. 「システムの要約」ページで「**VPD の更新**」をクリックします。
  4. UUID を更新します。

- Lenovo XClarity Essentials OneCLI から

Lenovo XClarity Essentials OneCLI が Lenovo XClarity Controller で UUID を設定します。以下のいずれかの方法を選択して Lenovo XClarity Controller にアクセスし、UUID を設定します。

– ターゲット・システムから操作 (LAN またはキーボード・コンソール・スタイル (KCS) のアクセスなど)
– ターゲット・システムへのリモート・アクセス (TCP/IP ベース)

Lenovo XClarity Essentials OneCLI から UUID を更新するには、次のようにします。

1. Lenovo XClarity Essentials OneCLI をダウンロードしてインストールします。

   Lenovo XClarity Essentials OneCLI をダウンロードするには、次のサイトにアクセスします。

   https://datacentersupport.lenovo.com/solutions/HT116433

2. OneCLI パッケージ (他の必要なファイルも含まれています) をサーバーにコピーし、解凍します。OneCLI と必要なファイルを必ず同じディレクトリーに解凍してください。
3. Lenovo XClarity Essentials OneCLI を配置した後で、以下のコマンドを入力して UUID を設定します。

   ```
   onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID [access_method]
   ```

   ここで、それぞれ以下の意味があります。

   [access_method]
   以下の方式からユーザーが選択したアクセス方式。

   – オンライン認証 LAN アクセスの場合、次のコマンドを入力します。

     ```
     [-bmc-username <xcc_user_id> -bmc-password <xcc_password>]
     ```

     ここで、それぞれ以下の意味があります。

     xcc_user_id
     BMC/IMM/XCC アカウント名 (12 アカウントのうちの 1 つ)。デフォルト値は USERID です。

     xcc_password
     BMC/IMM/XCC アカウントのパスワード (12 アカウントのうちの 1 つ)。

     コマンドの例は次の通りです。

     ```
     onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID --bmc-username <xcc_user_id>
     --bmc-password <xcc_password>
     ```

   – オンライン KCS アクセス (非認証およびユーザー制限付き) の場合:

     このアクセス方式を使用する場合は、*access_method* の値を指定する必要はありません。

     コマンドの例は次の通りです。

     ```
     onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID
     ```

     注：KCS アクセス方式では、IPMI/KCS インターフェースを使用します。これには IPMI ドライバーがインストールされている必要があります。

   – リモート LAN アクセスの場合、次のコマンドを入力します。

     ```
     [--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>]
     ```

     ここで、それぞれ以下の意味があります。

     xcc_external_ip
     BMC/IMM/XCC 外部 IP アドレス。デフォルト値はありません。このパラメーターは必須です。

     xcc_user_id

BMC/IMM/XCC アカウント名 (12 アカウントのうちの 1 つ)。デフォルト値は USERID です。

xcc_password
BMC/IMM/XCC アカウントのパスワード (12 アカウントのうちの 1 つ)。

注：BMC、IMM、または XCC の外部 IP アドレス、アカウント名、およびパスワードは、すべてこのコマンドで有効です。

コマンドの例は次の通りです。

```
onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID
--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>
```

4. Lenovo XClarity Controller を再起動します。
5. サーバーを再起動します。

資産タグの更新

必要に応じて、資産タグを更新できます。

資産タグを更新する方法は 2 つあります。

- Lenovo XClarity Provisioning Manager から

  Lenovo XClarity Provisioning Manager から資産タグを更新するには、次の手順を実行します。

  1. サーバーを起動して、画面の指示に従って指定されたキーを押し、Lenovo XClarity Provisioning Manager インターフェースを表示します。
  2. 始動管理者パスワードが必要な場合は、パスワードを入力します。
  3. 「システムの要約」ページで「**VPD の更新**」をクリックします。
  4. 資産タグ情報を更新します。

- Lenovo XClarity Essentials OneCLI から

  Lenovo XClarity Essentials OneCLI が Lenovo XClarity Controller で資産タグを設定します。以下のいずれかの方法を選択して Lenovo XClarity Controller にアクセスし、資産タグを設定します。

  – ターゲット・システムから操作 (LAN またはキーボード・コンソール・スタイル (KCS) のアクセスなど)
  – ターゲット・システムへのリモート・アクセス (TCP/IP ベース)

  Lenovo XClarity Essentials OneCLI から資産タグ情報を更新するには、次の手順を実行します。

  1. Lenovo XClarity Essentials OneCLI をダウンロードしてインストールします。

     Lenovo XClarity Essentials OneCLI をダウンロードするには、次のサイトにアクセスします。

     https://datacentersupport.lenovo.com/solutions/HT116433
  2. OneCLI パッケージ (他の必要なファイルも含まれています) をサーバーにコピーし、解凍します。OneCLI と必要なファイルを必ず同じディレクトリーに解凍してください。
  3. Lenovo XClarity Essentials OneCLI を配置した後で、以下のコマンドを入力して DMI を設定します。

     ```
     onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> [access_method]
     ```

     ここで、それぞれ以下の意味があります。

     <asset_tag>
     サーバーの資産タグ番号。`aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa` と入力します。ここで、*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* は資産タグ番号です。

     [access_method]
     以下の方式からユーザーが選択したアクセス方式。

– オンライン認証 LAN アクセスの場合、次のコマンドを入力します。

```
[-bmc-username <xcc_user_id> -bmc-password <xcc_password>]
```

ここで、それぞれ以下の意味があります。

xcc_user_id
BMC/IMM/XCC アカウント名 (12 アカウントのうちの 1 つ)。デフォルト値は USERID です。

xcc_password
BMC/IMM/XCC アカウントのパスワード (12 アカウントのうちの 1 つ)。

コマンドの例は次の通りです。

```
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> --bmc-username <xcc_user_id>
--bmc-password <xcc_password>
```

– オンライン KCS アクセス (非認証およびユーザー制限付き) の場合:

このアクセス方式を使用する場合は、*access_method* の値を指定する必要はありません。

コマンドの例は次の通りです。

```
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
```

注：KCS アクセス方式では、IPMI/KCS インターフェースを使用します。これには IPMI ドライバーがインストールされている必要があります。

– リモート LAN アクセスの場合、次のコマンドを入力します。

```
[--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>]
```

ここで、それぞれ以下の意味があります。

xcc_external_ip
BMC/IMM/XCC IP アドレス。デフォルト値はありません。このパラメーターは必須です。

xcc_user_id
BMC/IMM/XCC アカウント (12 アカウントのうちの 1 つ)。デフォルト値は USERID です。

xcc_password
BMC/IMM/XCC アカウントのパスワード (12 アカウントのうちの 1 つ)。

注：BMC、IMM、または XCC の内部 LAN/USB IP アドレス、アカウント名、およびパスワードは、すべてこのコマンドで有効です。

コマンドの例は次の通りです。

```
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>
```

4. Lenovo XClarity Controller を出荷時のデフォルト値にリセットします。https://pubs.lenovo.com/lxcc-overview/ にある、ご使用のサーバーと互換性のある XCC に関する資料の「BMC の出荷時のデフォルト値へのリセット」セクションを参照してください。

第 5 章 インストールに関する問題の解決

この情報を使用して、システムのセットアップ時に発生する可能性のある問題を解決します。

サーバーの初期インストールおよびセットアップ時に発生する可能性がある問題を診断し、解決するには、このセクションの情報を使用します。

- 133 ページの 「サーバーの電源がオンにならない」
- 133 ページの 「サーバーをオンにすると、すぐに POST イベント・ビューアーが表示される」
- 133 ページの 「組み込みハイパーバイザーがブート・リストにない」
- 134 ページの 「表示されるシステム・メモリーが取り付けられている物理メモリーよりも小さい」
- 135 ページの 「新たに取り付けられた Lenovo オプション・デバイスが作動しない」
- 135 ページの 「電圧プレーナー障害がイベント・ログに表示される」

サーバーの電源がオンにならない

問題が解決するまで、以下のステップを実行します。

1. 電源を投入していないサーバーに関連するイベントがないか、イベントログをチェックしてください。
2. 橙色で点滅している LED がないかチェックしてください。
3. システム・ボード上の電源 LED をチェックしてください。
4. 電源アダプターを取り付け直します。
5. 電源アダプターを交換し、それぞれを取り付けた後に電源ボタンの機能を確認します。
6. 上記の操作を行っても問題が解決しない場合は、サービスに電話して問題の現象を確認してもらい、システム・ボードを交換する必要があるかどうかを確認します。

サーバーをオンにすると、すぐに POST イベント・ビューアーが表示される

問題が解決するまで、以下のステップを実行します。

1. 前面オペレーター・パネルとエラー LED が示しているエラーを訂正します。
2. サーバーがプロセッサーをサポートし、プロセッサーの速度とキャッシュ・サイズが相互に一致していることを確認します。

   システム・セットアップからプロセッサーの詳細を表示できます。

   プロセッサーがサーバーでサポートされているかどうかを判別するには、https://serverproven.lenovo.com/server/se350 を参照してください。
3. (トレーニングを受けた技術員のみ) システム・ボードが正しく取り付けられていることを確認します。
4. (トレーニングを受けた技術員のみ) プロセッサーが正しく取り付けられていることを確認します
5. 次のコンポーネントを、リストに示されている順序で一度に 1 つずつ交換し、そのたびにサーバーを再起動します。

   a. (トレーニングを受けた技術員のみ) プロセッサー

   b. (トレーニングを受けた技術員のみ) システム・ボード

組み込みハイパーバイザーがブート・リストにない

問題が解決するまで、以下のステップを実行します。

1. サーバーの取り付け、移動、あるいは保守を最近行った場合、あるいは組み込みハイパーバイザーを初めて使用する場合は、デバイスが適切に接続されていること、およびコネクターに物理的損傷がないことを確認します。

© Copyright Lenovo 2019, 2022

2. オプションの組み込みハイパーバイザー・フラッシュ・デバイスに付属の資料を参照して、セットアップおよび構成情報を確認します。
3. https://serverproven.lenovo.com/server/se350 で、組み込みハイパーバイザー・デバイスがサーバーでサポートされていることを確認します。
4. 組み込みハイパーバイザー・デバイスが使用可能なブート・オプションのリストに含まれていることを確認します。管理コントローラーのユーザー・インターフェースから、「**サーバー構成**」 → 「**ブート・オプション**」の順にクリックします。

   管理コントローラー・ユーザー・インターフェースへのアクセスについては、次の URL にあるご使用のサーバーと互換性のある XCC に関する資料の「XClarity Controller Web インターフェースの開始と使用」セクションを参照してください。

   https://pubs.lenovo.com/lxcc-overview/
5. http://datacentersupport.lenovo.com で、組み込みハイパーバイザーおよびサーバーに関連する技術ヒント (service bulletins) がないかを確認します。
6. サーバー上で他のソフトウェアが作動していることを確認し、サーバーが正常に機能していることを確認します。

表示されるシステム・メモリーが取り付けられている物理メモリーよりも小さい

以下の手順に従って、問題を修正します。

注：メモリー・モジュールの取り付けあるいは取り外しを行う場合は、必ずサーバーを電源から切り離す必要があります。サーバーを再起動する場合は、10 秒間待ってから行ってください。

1. 次の点を確認します。
   - オペレーター情報パネル上のエラー LED がどれも点灯していない。
   - システム・ボードのメモリー・モジュール・エラー LED が何も点灯していない。
   - メモリー・ミラーリング・チャネルが不一致の原因ではない。
   - メモリー・モジュールが正しく取り付けられている。
   - 正しいタイプのメモリー・モジュールを取り付けている (要件については3 ページの 「仕様」を参照してください)。
   - メモリー・モジュールを変更または交換すると、Setup Utility でメモリー構成がそれに応じて更新されます。
   - すべてのメモリー・バンクが有効になっている。サーバーが問題を検出したときにメモリー・バンクを自動的に無効にしたか、メモリー・バンクが手動で無効にされた可能性があります。
   - サーバーを最小メモリー構成にしたときに、メモリー・ミスマッチがない。
2. メモリー・モジュールを取り付け直し、サーバーを再起動します。
3. 以下のようにして、POST エラー・ログをチェックします。
   - メモリー・モジュールがシステム管理割り込み (SMI) によって無効にされていた場合は、そのメモリー・モジュールを交換します。
   - メモリー・モジュールがユーザーまたは POST によって無効にされた場合は、メモリー・モジュールを取り付け直します。その後、Setup Utility を実行して、メモリー・モジュールを有効にします。
4. メモリー診断を実行します。ソリューションを起動して画面の指示に従ってキーを押すと、デフォルトでは、LXPM インターフェースが表示されます。(詳細については、https://pubs.lenovo.com/lxpm-overview/ にあるご使用のサーバーと互換性のある LXPM 資料の「起動」セクションを参照してください)。このインターフェースでメモリー診断を実行できます。診断ページで、「**診断の実行**」 → 「**メモリー・テスト**」に移動します。
5. Setup Utility を使用してすべてのメモリー・モジュールを再度使用可能にし、サーバーを再始動します。
6. (トレーニングを受けた技術員のみ) システム・ボードを交換します。

新たに取り付けられた Lenovo オプション・デバイスが作動しない

1. 次の点を確認します。
   - デバイスがサーバーでサポートされている (https://serverproven.lenovo.com/server/se350 を参照)。
   - デバイスに付属の取り付け手順に従い正しい取り付けがされている。
   - 取り付けた他のデバイスやケーブルを外していない。
   - システム・セットアップで構成情報を更新した。サーバーを起動して画面の指示に従ってキーを押すと、デフォルトでは、Setup Utility が表示されます。(詳細については、https://pubs.lenovo.com/lxpm-overview/ にあるご使用のサーバーと互換性のある LXPM 資料の「起動」セクションを参照してください)。メモリーまたは他のデバイスを変更する場合は、必ず構成を更新する必要があります。
2. 取り付けたデバイスを取り付け直します。
3. 取り付けたデバイスを交換します。
4. ケーブルの接続を抜き差しして、ケーブルに物理的損傷がないことを確認します。
5. ケーブルに損傷がある場合は、ケーブルを交換します。

電圧プレーナー障害がイベント・ログに表示される

問題が解決するまで、以下のステップを実行します。

1. システムを最小構成に戻します。最低限必要なプロセッサーと DIMM の数については、3 ページの「仕様」 を参照してください。
2. システムを再起動します。
   - システムが再起動する場合は、取り外した部品を一度に 1 つずつ追加して、そのたびにシステムを再起動し、これをエラーが発生するまで繰り返します。エラーが発生した部品を交換します。
   - システムが再起動しない場合は、システム・ボードが原因の可能性があります。

付録 A　ヘルプおよび技術サポートの入手

ヘルプ、サービス、技術サポート、または Lenovo 製品に関する詳しい情報が必要な場合は、Lenovo がさまざまな形で提供しているサポートをご利用いただけます。

WWW 上の以下の Web サイトで、Lenovo システム、オプション・デバイス、サービス、およびサポートについての最新情報が提供されています。

http://datacentersupport.lenovo.com

注：IBM は、ThinkSystem に対する Lenovo の優先サービス・プロバイダーです。

依頼する前に

連絡する前に、以下の手順を実行してお客様自身で問題の解決を試みてください。サポートを受けるために連絡が必要と判断した場合、問題を迅速に解決するためにサービス技術員が必要とする情報を収集します。

お客様自身での問題の解決

多くの問題は、Lenovo がオンライン・ヘルプまたは Lenovo 製品資料で提供するトラブルシューティング手順を実行することで、外部の支援なしに解決することができます。Lenovo 製品資料にも、お客様が実行できる診断テストについての説明が記載されています。ほとんどのシステム、オペレーティング・システムおよびプログラムの資料には、トラブルシューティングの手順とエラー・メッセージやエラー・コードに関する説明が記載されています。ソフトウェアの問題だと考えられる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

ThinkSystem 製品については、以下の場所で製品ドキュメントが見つかります。

http://thinksystem.lenovofiles.com/help/index.jsp

以下の手順を実行してお客様自身で問題の解決を試みることができます。

- ケーブルがすべて接続されていることを確認します。
- 電源スイッチをチェックして、システムおよびすべてのオプション・デバイスの電源がオンになっていることを確認します。
- ご使用の Lenovo 製品用に更新されたソフトウェア、ファームウェア、およびオペレーティング・システム・デバイス・ドライバーがないかを確認します。Lenovo 保証規定には、Lenovo 製品の所有者であるお客様の責任で、製品のソフトウェアおよびファームウェアの保守および更新を行う必要があることが明記されています (追加の保守契約によって保証されていない場合)。お客様のサービス技術員は、問題の解決策がソフトウェアのアップグレードで文書化されている場合、ソフトウェアおよびファームウェアをアップグレードすることを要求します。
- ご使用の環境で新しいハードウェアを取り付けたり、新しいソフトウェアをインストールした場合、https://serverproven.lenovo.com/server/se350 でそのハードウェアおよびソフトウェアがご使用の製品によってサポートされていることを確認してください。
- http://datacentersupport.lenovo.com にアクセスして、問題の解決に役立つ情報があるか確認してください。
  - 同様の問題が発生した他のユーザーがいるかどうかを調べるには、https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg の Lenovo Forums (Lenovo フォーラム) を確認してください。

多くの問題は、Lenovo がオンライン・ヘルプまたは Lenovo 製品資料で提供するトラブルシューティング手順を実行することで、外部の支援なしに解決することができます。Lenovo 製品資料にも、お客様が実行できる診断テストについての説明が記載されています。ほとんどのシステム、オペレーティン

© Copyright Lenovo 2019, 2022

グ・システムおよびプログラムの資料には、トラブルシューティングの手順とエラー・メッセージやエラー・コードに関する説明が記載されています。ソフトウェアの問題だと考えられる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

サポートへの連絡に必要な情報の収集

ご使用の Lenovo 製品に保証サービスが必要であると思われる場合は、連絡される前に準備をしていただけると、サービス技術員がより効果的にお客様を支援することができます。または製品の保証について詳しくは http://datacentersupport.lenovo.com/warrantylookup で参照できます。

サービス技術員に提供するために、次の情報を収集します。このデータは、サービス技術員が問題の解決策を迅速に提供する上で役立ち、お客様が契約された可能性があるレベルのサービスを確実に受けられるようにします。

- ハードウェアおよびソフトウェアの保守契約番号 (該当する場合)
- マシン・タイプ番号 (Lenovo の 4 桁のマシン識別番号)
- 型式番号
- シリアル番号
- 現行のシステム UEFI およびファームウェアのレベル
- エラー・メッセージやログなど、その他関連情報

Lenovo サポートに連絡する代わりに、https://support.lenovo.com/servicerequest にアクセスして Electronic Service Request を送信することもできます。Electronic Service Request を送信すると、お客様の問題に関する情報をサービス技術員が迅速に入手できるようになり、問題の解決策を判別するプロセスが開始されます。Lenovo サービス技術員は、お客様が Electronic Service Request を完了および送信するとすぐに、解決策の作業を開始します。

サービス・データの収集

サーバーの問題の根本原因をはっきり特定するため、または Lenovo サポートの依頼によって、詳細な分析に使用できるサービス・データを収集する必要がある場合があります。サービス・データには、イベント・ログやハードウェア・インベントリーなどの情報が含まれます。

サービス・データは以下のツールを使用して収集できます。

- **Lenovo XClarity Provisioning Manager**

  Lenovo XClarity Provisioning Manager のサービス・データの収集機能を使用して、システム・サービス・データを収集します。既存のシステム・ログ・データを収集するか、新しい診断を実行して新規データを収集できます。

- **Lenovo XClarity Controller**

  Lenovo XClarity Controller Web インターフェースまたは CLI を使用してサーバーのサービス・データを収集できます。ファイルは保存でき、Lenovo サポートに送信できます。

  – Web インターフェースを使用したサービス・データの収集について詳しくは、https://pubs.lenovo.com/lxcc-overview/にある、ご使用のサーバーと互換性のある XCC に関する資料のバージョンの「サービス・データのダウンロード」セクションを参照してください。

  – CLI を使用したサービス・データの収集について詳しくは、https://pubs.lenovo.com/lxcc-overview/にある、ご使用のサーバーと互換性のある XCC に関する資料のバージョンの「ffdc コマンド」セクションを参照してください。

- **Lenovo XClarity Administrator**

  一定の保守可能イベントが Lenovo XClarity Administrator および管理対象エンドポイントで発生した場合に、診断ファイルを収集し自動的に Lenovo サポートに送信するように Lenovo XClarity Administrator をセットアップできます。Call Homeを使用して診断ファイルを Lenovo サポート に送信するか、SFTP を使

用して別のサービス・プロバイダーに送信するかを選択できます。また、手動で診断ファイルを収集したり、問題レコードを開いたり、診断ファイルを Lenovo サポート・センターに送信したりもできます。

Lenovo XClarity Administrator 内での自動問題通知のセットアップに関する詳細情報は http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html で参照できます。

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI には、サービス・データを収集するインベントリー・アプリケーションがあります。インバンドとアウト・オブ・バンドの両方で実行できます。サーバーのホスト・オペレーティング・システムで実行する場合、OneCLI では、ハードウェア・サービス・データに加えて、オペレーティング・システム・イベント・ログなどオペレーティング・システムに関する情報を収集できます。

  サービス・データを取得するには、`getinfor` コマンドを実行できます。`getinfor` の実行についての詳細は、https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command を参照してください。

サポートへのお問い合わせ

サポートに問い合わせて問題に関するヘルプを入手できます。

ハードウェアの保守は、Lenovo 認定サービス・プロバイダーを通じて受けることができます。保証サービスを提供する Lenovo 認定サービス・プロバイダーを見つけるには、https://datacentersupport.lenovo.com/serviceprovider にアクセスし、フィルターを使用して国別で検索します。Lenovo サポートの電話番号については、https://datacentersupport.lenovo.com/supportphonelist で地域のサポートの詳細を参照してください。

索引

l

Lenovo Capacity Planner　13
Lenovo XClarity Essentials　13
Lenovo XClarity Provisioning Manager　13

お

汚染、微粒子およびガス　12

か

ガス汚染　12
管理製品　13

り

粒子汚染　12

© Copyright Lenovo 2019, 2022

Lenovo