Cisco Tetration（Cisco Secure Workload）M4 クラスタハードウェア導入ガイド

初版：2016 年 8 月 11 日

最終更新：2022 年 8 月 17 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

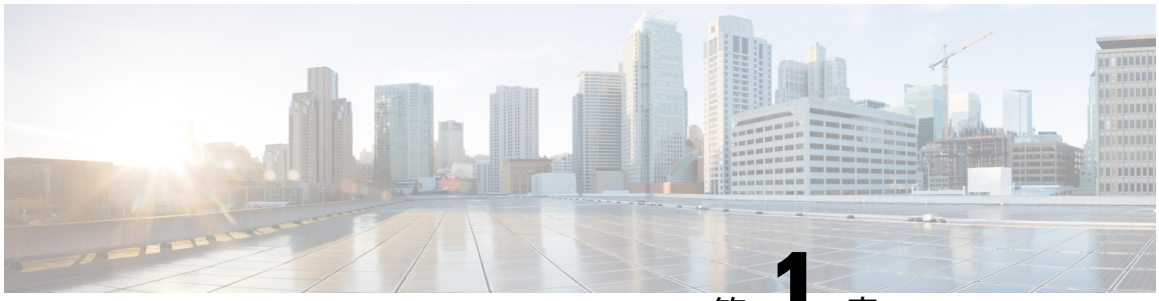
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



第 1 章

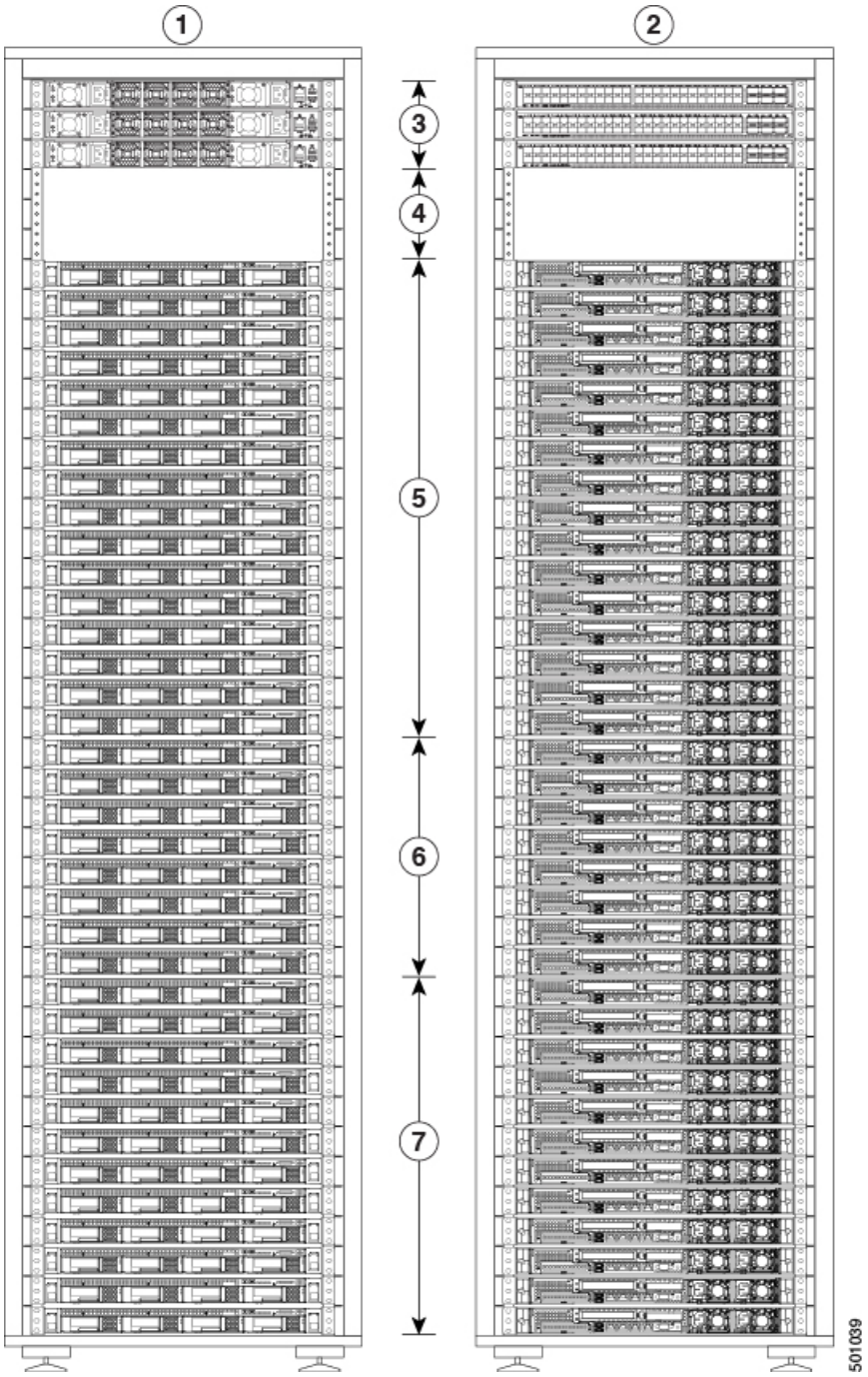
概要

インストールの概要

Cisco Tetration（Cisco Secure Workload）クラスタは、サーバーが 5000 台を超えるデータセンターには39ラックユニット（RU）の大型フォームファクタ プラットフォーム（C1-Tetration）、サーバーが 5000 台よりも少ないデータセンターには 8 RU の小型フォームファクタ プラットフォーム（C1-Tetration-M）として展開できます。さらに、大型フォームファクタ プラットフォームは、要件に応じて 1 ラックまたは 2 ラックのいずれかで展開できます。

Cisco Tetration（Cisco Secure Workload）M4 クラスタ展開の構成は次のとおりです。

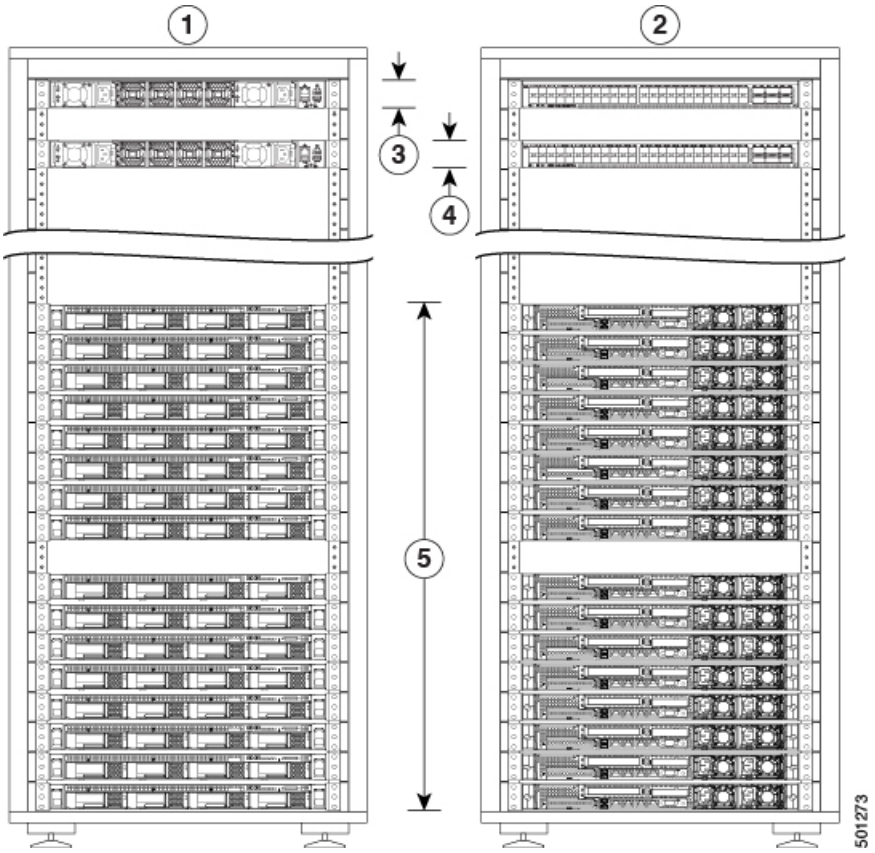
- 1 ラックの大型フォームファクタ 39 RU Cisco Tetration（Cisco Secure Workload）プラットフォーム（C1-Tetration シングルラック）



1	コールド アイルのビュー	5	16 台のコンピューティング サーバ (RU 21 ～ 36)
2	ホット アイルのビュー	6	8 台のキャッシュ サーバ (RU 13 ～ 20)

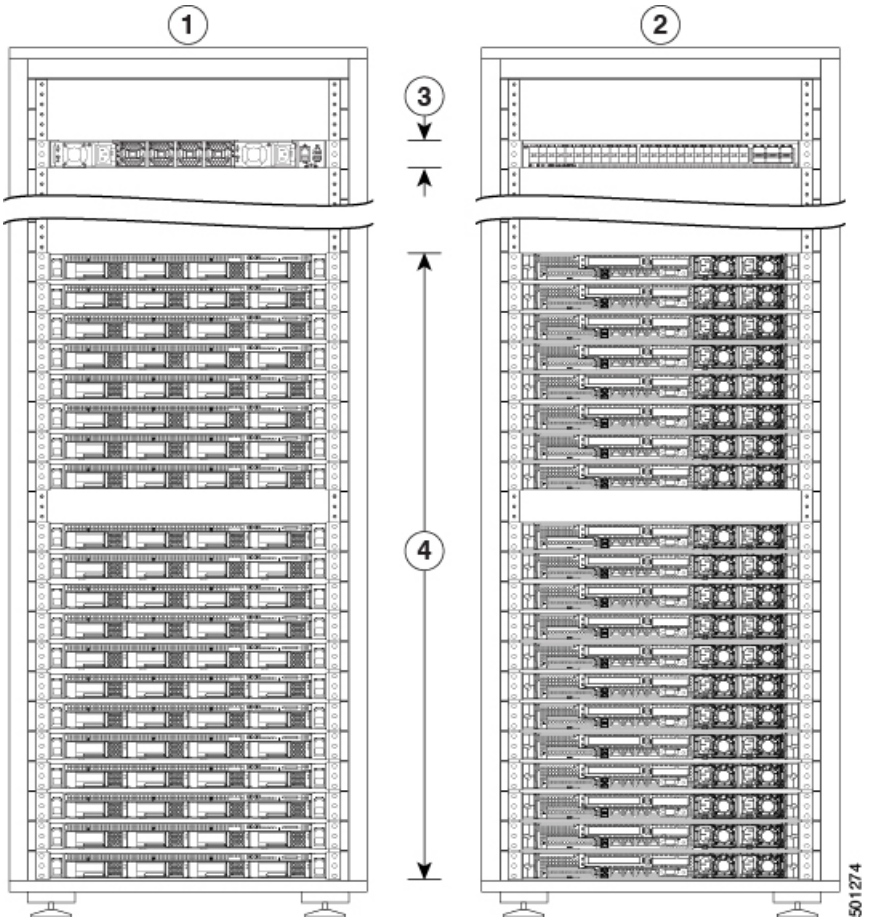
3	1 個のスパイン (RU 42) と 2個 のリーフ スイッチ (RU 40 および 41)	7	12 個のベース サーバ (RU 1 ~ 12)
4	ラック単位 (Ru 37 に 39) を開く		

- 2 ラックの大型フォームファクタ Cisco Tetration（Cisco Secure Workload）プラットフォーム（C1-Tetration デュアルラック）
  - ラック 1



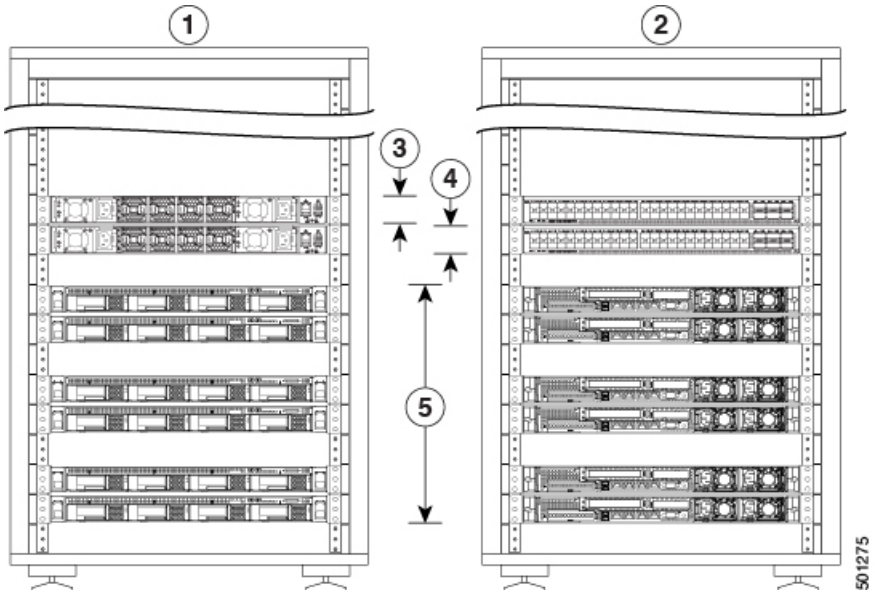
1	コールド アイルのビュー	4	1 個のリーフ スイッチ (RU 40)
2	ホット アイルのビュー	5	16 台のコンピューティング サーバ (RU 1 ~ 4、6 ~ 9)
3	1 個のスパイン スイッチ (RU 42)		

  - ラック 2



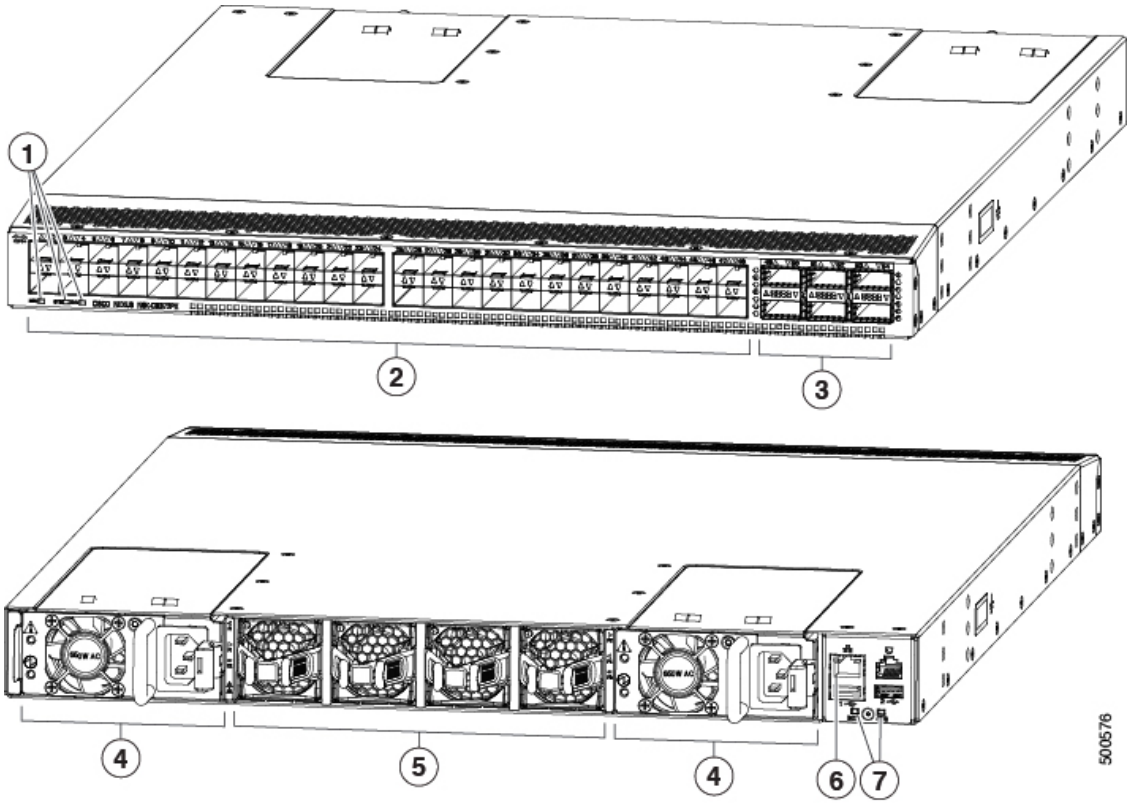
1	コールド アイルのビュー	3	2 個のリーフ スイッチ (RU 40)
2	ホット アイルのビュー	4	8 個のキャッシュ サーバ (RU 14 ～ 21) と 12 個のベース サーバ (RU 1 ~ 12)

- 1 ラックの小型フォームファクタ 8 RU Cisco Tetration（Cisco Secure Workload）プラットフォーム（C1-Tetration-M）



1	コールド アイルのビュー	4	リーフ スイッチ (RU 11)
2	ホット アイルのビュー	5	6 個のユニバーサル サーバ (RU 2、3、5、6、8、および 9)
3	リーフ スイッチ (RU 12)		

このスイッチには 1 から 48 番の 48 個の 10 ギガビットのイーサネット ポートと 49 から 54 番の 40 ギガビット イーサネット ポートがあります。次の図は、スイッチの両端を表示し、これらの機能を識別します。



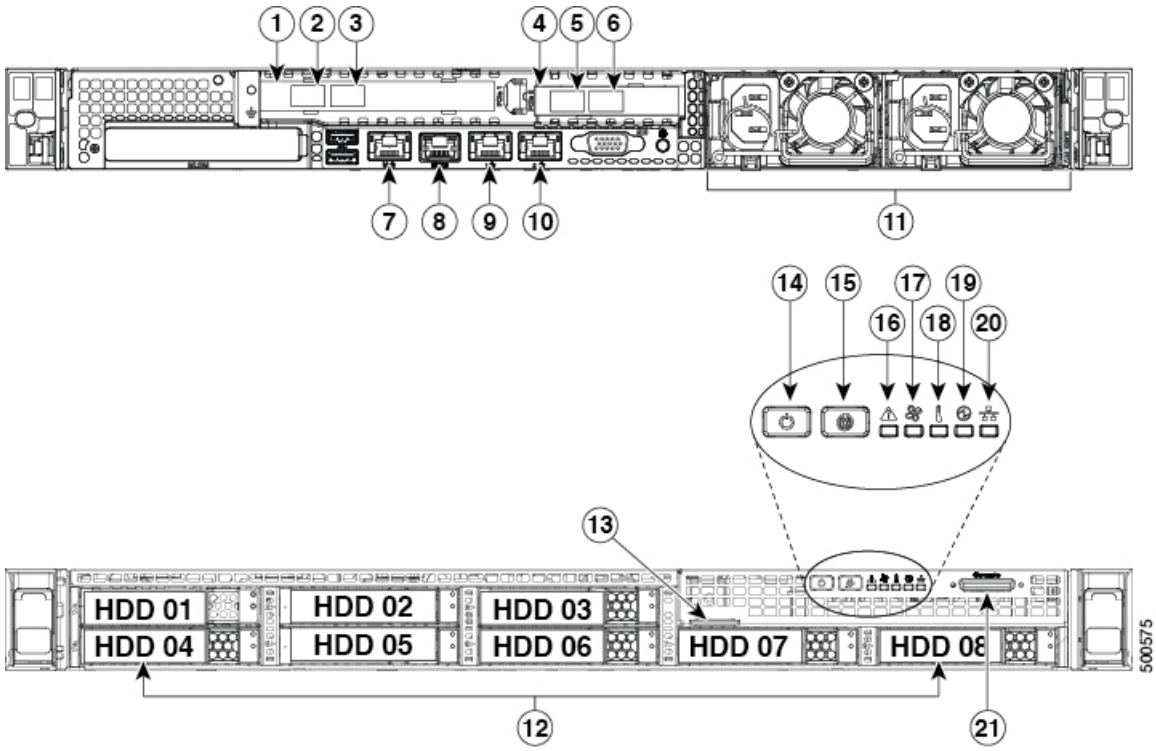
1	ビーコン（BCN）、ステータス（STS）および環境（ENV）LED	5	ファンのモジュール(青色ハンドルは、ポート側排気口へのエアフローを示す)
2	1 から 48 番の 10 ギガビット ポート (48)	6	管理ポート
3	49 から 54 番の 40 ギガビット ポート (6)	7	ビーコン（BCN）およびステータス（STS）LED
4	AC 電源 (青色はポート側排気口のエアフローを示す)		—

大規模フォーム ファクタ スイッチでは、コンピューティング、キャッシュ、および基本ノードとして実行するサーバがあります。小規模フォーム ファクタ スイッチでは、ユニバーサル ノードとして実行するサーバがあります。次の表は、これらのサーバの特性を指定します。

サーバ タイプ	各サーバのストレージ ドライブ	RAM	RAID キャッシュ
コンピューティング ノード(大規模なフォームファクタ プラットフォームの 16 個のサーバ)	1.2 TB ドライブ (スロット 1 の 1 個) 1.8 TB ドライブ (スロット 2 ~ 8 の 7 個)	512 GB	4 GB

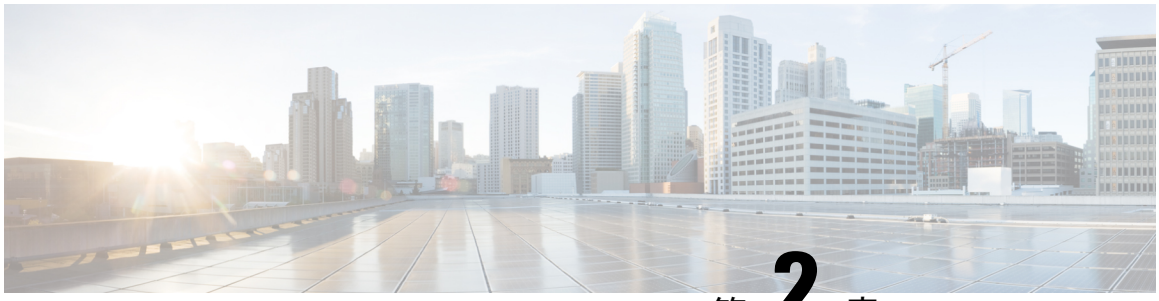
サーバ タイプ	各サーバのストレージ ドライブ	RAM	RAID キャッシュ
キャッシュ ノード (大規模フォーム ファクタの 8 個のサーバ)	400 GB ドライブ (8)	512 GB	2 GB
基本ノード (フォーム ファクタ大規模なプラットフォームでは 12 サーバ)	1.2 TB ドライブ (8)	256 GB	2 GB
ユニバーサル ノード (小規模のフォーム ファクタ プラットフォームの 6 個のサーバ)	1.6 TB SSD ドライブ (5) 3.6 TB SSD ドライブ (3)	1024 GB	2 GB

サーバに、10 ギガビット インターフェイス ポート (eth2、eth3、eth5、および eth4) は、2 つの PCIe ライザーに配置され、次の図に示すように、管理ポートが PCIe ライザーの下にあります。



1	PCIe ライザー 1	12	ドライブ ベイ
2	eth2 ポート (最初のインターフェイス ポート)	13	引き抜きアセット タグ

3	eth3 スイッチ ポート (2 番目のインターフェイス ポート)	14	電源ボタン/電源ステータス LED
4	PCIe ライザー 2	15	ビーコン LED
5	eth5 ポート (4 番目のインターフェイス ポート)	16	システム ステータス LED
6	eth4 ポート (3 番目のインターフェイス ポート)	17	ファンステータス LED
7	管理インターフェイス	18	温度ステータス LED
8	シリアル ポート	19	電源ステータス LED
9	eth0 ポート (CIMC ポート)	20	ネットワーク アクティビティ LED
10	eth1 ポート	21	コンソール ポート
11	AC 電源装置		—



第 2 章

設置場所の準備

温度要件

Cisco Tetration（Cisco Secure Workload）クラスタスイッチとサーバーでは、動作温度 5 ～ 35 °C（41 ～ 95 °F）で、海抜高度 305 m（1000 フィート）ごとに 1° Cの最大温度を低減させることが必要です。デバイスが非動作中の場合は、温度は -40 ー 65 °C（-40 ー 149 °F）でなければなりません。

湿度の要件

湿度が高いと、スイッチとサーバーに湿気が入ることがあります。湿気が原因で、内部コンポーネントの腐食、および電気抵抗、熱伝導性、物理的強度、サイズなどの特性の劣化が発生することがあります。スイッチとサーバーは 10~80 %の相対湿度で1時間当たり 10 % の湿度変化で動作するように定格が定められています。非動作時条件の場合、デバイスは相対湿度 5 ～ 93 % に耐えることができます。

温暖期の空調と寒冷期の暖房により室温が四季を通して管理されている建物内では、デバイスにとって、通常許容できるレベルの湿度が維持されています。ただし、デバイスを極端に湿度の高い場所に設置する場合は、除湿装置を使用して、湿度を許容範囲内に維持してください。

高度要件

標高の高い（気圧が低い）場所でラックデバイスを動作させると、対流型の強制空冷方式の効率が低下し、その結果、アーク現象およびコロナ放電による電気障害が発生することがあります。また、このような状況では、内部圧力がかかっている密閉コンポーネント、たとえば、電解コンデンサが損傷したり、その効率が低下したりする場合もあります。これらのデバイスは10,000フィート(0に3,050 m)、0から高度で動作するように評価し、0に40,000フィート(12,200 m)の高度に保存されていることができます。

埃および微粒子の要件

シャーシ内のさまざまな開口部を通じて空気を吸気および排気することによって、ファンは電源モジュール、スイッチ、サーバーを冷却します。しかし、ファンはほこりやその他の微粒子を吸い込み、スイッチに混入物質を蓄積させ、内部シャーシの温度が上昇する原因にもなります。清潔な作業環境を保つことで、ほこりやその他の微粒子による悪影響を大幅に減らすことができます。これらの異物は絶縁体となり、スイッチとサーバーの機械的なコンポーネントの正常な動作を妨げます。

定期的なクリーニングに加えて、ラック スイッチとサーバーの汚れを防止するために、次の予防策に従ってください。

- ラックの近くでの喫煙を禁止する。
- ラックの近くでの飲食を禁止する。

電磁干渉および無線周波数干渉の最小化

デバイスからの電磁干渉（EMI）および無線周波数干渉（RFI）は、Cisco Tetration（Cisco Secure Workload）クラスタ ラックの周辺で稼働している他のデバイス（ラジオおよびテレビ受信機）に悪影響を及ぼす可能性があります。また、ラックのデバイスから出る無線周波数が、コードレス電話や低出力電話の通信を妨げる場合もあります。逆に、高出力の電話からのRFIによって、デバイスモニターに意味不明の文字が表示されることがあります。

RFI は、10 kHz を超える周波数を発生させる任意の EMI として定義されます。このタイプの干渉は、電源ケーブルおよび電源を通じて、または送信された電波のように空気中を通じてスイッチから他の装置に伝わる場合があります。米国連邦通信委員会（FCC）は、コンピュータ装置が放出するEMIおよびRFIの量を規制する特定の規定を公表しています。各スイッチは、FCC の規格を満たしています。

電磁界内で長距離にわたって配線を行う場合、磁界と配線上の信号の間で干渉が発生することがあり、そのために次のような影響があります。

- 配線を適切に行わないと、プラント配線から無線干渉が発生することがあります。

- 特に雷または無線トランスミッタによって生じる強力な EMI は、シャーシ内の信号ドライバやレシーバーを破損したり、電圧サージが回線を介して装置内に伝導するなど、電気的に危険な状況をもたらす原因になります。

（注） 強力な EMI を予測して防止するには、RFI の専門家に相談してください。

アース導体を適切に配置してツイストペア ケーブルを使用すれば、配線から無線干渉が発生することはほとんどありません。推奨距離を超える場合は、データ信号ごとにアース導体を施した高品質のツイストペア ケーブルを使用してください。

注意 配線が推奨距離を超える場合、または配線が建物間にまたがる場合は、近辺で発生する落雷の影響に十分に注意してください。雷などの高エネルギー現象で発生する電磁波パルスにより、電子装置を破壊するほどのエネルギーが非シールド導体に発生することがあります。過去にこのような問題が発生した場合は、電力サージ抑止やシールドの専門家に相談してください。

衝撃および振動の要件

Cisco Tetration（Cisco Secure Workload）クラスタデバイスのデバイスは、動作範囲、取り扱い、耐震規格に対して衝撃および振動の試験が行われています。

アース要件

Cisco Tetration（Cisco Secure Workload）クラスタ内のデバイスは、電源によって提供される電圧の変動に敏感です。過電圧、低電圧、および過渡電圧（スパイク）によって、データがメモリから消去されたり、コンポーネントの障害が発生するおそれがあります。これらのタイプの問題に対して保護するために、デバイスにアース接続があることを確認してください。ラックを設備のアースに接続する必要があります。

この接続を行うアース線を用意する必要があります。地域および各国の設置要件を満たすようにアース線のサイズを選択してください。電源モジュールとシステムに応じて、米国での設置では 12 ～ 6 AWG の銅の導体が必要です（その場合は、市販されている 6 AWG ワイヤを使用することをお勧めします）。アース線の長さは、ラックと設備のアース接続の間の距離によって決まります。

電力要件

Cisco Tetration（Cisco Secure Workload）クラスタは、次の電力量をオペレーションに提供する電源をプロビジョニングする必要があります。

- 39-RU 大規模フォームファクタ プラットフォーム、シングルラック：22,500 W
- 39-RU大規模フォームファクタプラットフォーム、デュアルラック：ラックごとに11,500 W
- 8-RU 小規模フォームファクタ プラットフォーム：5,500 W

必要な *n*+*n* 電源の冗長性については、それぞれがその電力量を供給する各 2 つの AC 電源が必要です。

ラックの各シャーシには、2 つの電源装置、オペレーション用に 1 つと冗長性のためにもう 1 つがあります。各電源がラックの別の電源ストリップに接続され、各電源ストリップが異なる AC 電源に接続されています。1 つの電源に障害が発生すると、もう 1 つの電源がラックの各スイッチまたはサーバーに電力を提供します。

エアーフロー要件

Cisco Tetration（Cisco Secure Workload）クラスタでは、コールドアイル内の 3 つのスイッチで各ラックに電源とファンを配置する必要があります。このように配置するとき、ラック内のすべてのデバイスはコールドアイルから冷風を取り込み、ホットアイルに熱風を排出します。

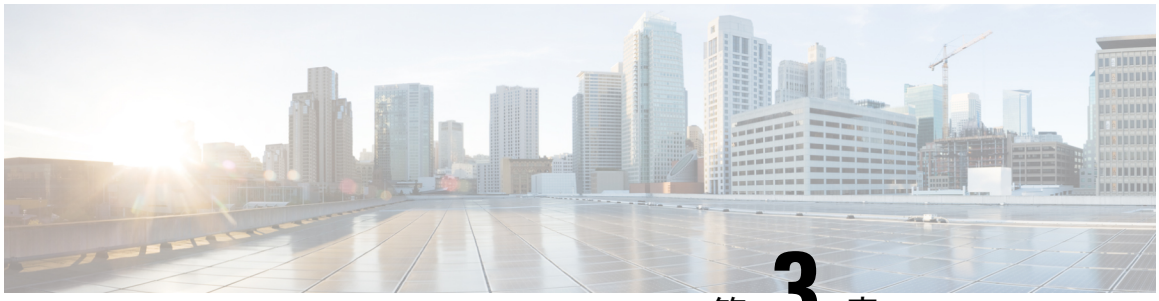
スペース要件

次の表では、39 RU ラージフォームファクタ (シングルまたはデュアルラック) または 8 RU スモールフォームファクタ Cisco Tetration（Cisco Secure Workload）クラスタのインストールに必要な大きさのスペースを示しています。インストール アイルはラックを挿入するために、24 インチ (61 cm) を超える幅が必要です。さらに、メンテナンスを実施するために前面と背面にアクセスするための十分な空き領域が必須です。

インストール タイプ	アイル最小幅[1]	ラックのインストールの最小スペース
C1-Tetration (シングル ラック) のインストール	61 cm（24 インチ）	幅 61 cm（24 インチ）奥行き 110.2 cm (43.38 インチ)
C1-Tetration (デュアル ラック)	61 cm（24 インチ）	幅 122 cm（48 インチ）奥行き 110.2 cm (43.38 インチ)
C1-Tetration M	61 cm（24 インチ）	幅 61 cm（24 インチ）奥行き 110.2 cm (43.38 インチ)

[1] 、インストールのためのアイルとラックの前面扉が開くためのアイルには、少なくとも 24 インチ (61 cm) の幅が必要です。もう一方の通路では両開きのキャビネットドアが開き、少なくとも12インチ（30.5 cm）の幅があればドアは完全に開きますが、人がメンテナンスを行うには少なくとも 24 インチ（61 cm）の幅が必要です。

ラックは、スイッチのファン（最大のドアをもつラックの側面）がコールドアイルに向けて配置され、スイッチポート（二重ドアのラックの側）がホットアイルに向けて配置されています。



第 3 章

電源の投入とデバイスの接続

Cisco Tetration（Cisco Secure Workload）クラスタデバイスの電源投入

Cisco Tetration（Cisco Secure Workload） クラスタのデバイスはラックに金属間の接続があるため、ラック（またはデュアルラックのインストールの場合は複数のラック) をデータセンターの地表に接地すると同時に、ラックのデバイスが接地されます。ラックを接地するためには、ラックホイールをアース地表に接続します。

Cisco Tetration（Cisco Secure Workload）クラスタデバイスの電源投入

スイッチに電源投入するには、2 つの AC 電源へのラックに付いている 2 つの電源ストリップを接続する必要があります。

（注） この装置をNFPA 70 National Electrical Code（NEC）に準拠するサービス機器で、サージ保護デバイス（SPD）に付属の AC 主電源に接続します。

設置手順を読んでから、システムを使用、取り付け、または電源に接続してください。

このユニットを電源回路に接続するときは、配線を過負荷にしないでください。

始める前に

- ラックはデータセンターに設置され、コールドアイル内に配置された吸気口を所定の位置に固定しました。
- ラックにデータセンター アース接地する必要があります。
- クラスタは、2 つの顧客が指定するルータ (別のリーフ スイッチに接続されたそれぞれのルータ) に接続する必要があります。
- 電源要件を満たす2つの電源が各ラック電源ストリップ ケーブルの近くにある必要があります。

手順

ステップ 1 AC 電源に 1 つの電源ストリップの電源ケーブルを差し込み、もう 1 つの AC 電源に 2 つ目の電源ストリップの電源ケーブルを差し込みます。

ステップ 2 LED が緑に点灯していることを確認するために、ラックのデバイスのそれぞれに設置された各電源を確認します。

- いずれの LED も点灯していない場合は、電源がオンになっていることとラック電源ストリップのオン/オフ スイッチがオンになっていることを確認します。
- これらの LED の一部が点灯しているが、他が点灯していない場合は、その電源から電源ケーブルがラックの電源ストリップに完全に接続されていることを確認します。

次のタスク

ユーザーインターフェイスを設定する準備ができました。

Cisco Tetration（Cisco Secure Workload）クラスタのルータへの接続

Cisco Tetration（Cisco Secure Workload）クラスタは、2つのルータに接続する必要があります。

手順

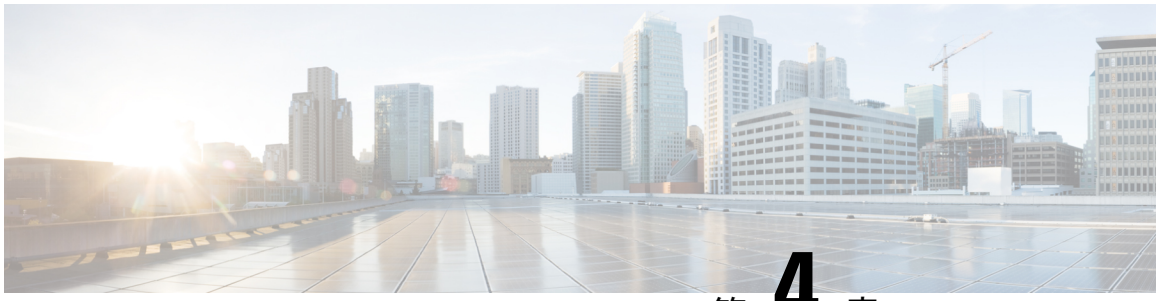
ステップ 1 39-RU 大規模フォーム ファクタ デュアル ラック クラスタをインストールする場合は、各ラックで部分的に接続されたインターフェイス ケーブルを接続します。これらのケーブルのそれぞれに対して、他のラックでラベルが付けられたポートに接続します。

ステップ 2 10 ギガビットケーブルを使用して、39 RU 展開の場合はリーフ 1 スイッチのポート E1/39、8 RU 展開の場合はポート E1/47 にルータを接続します。リーフ 1 スイッチは、次の場所にあります。

- 39-RU 大規模フォーム ファクタ シングル ラック プラットフォーム - プラットフォーム ラックで RU 40
- 39-RU 大規模フォーム ファクタ デュアル ラック プラットフォーム - ラック 1 で RU 40
- 8-RU 小規模フォーム ファクタ プラットフォーム - プラットフォーム ラック で RU 12

ステップ 3 10 ギガビットケーブルを使用して、39 RU 展開の場合はリーフ 2 スイッチのポート E1/39、8 RU 展開の場合はポート E1/47 にルータを接続します。リーフ 2 スイッチは、次の場所にあります。

- 39-RU 大規模フォーム ファクタ シングル ラック プラットフォーム - プラットフォーム ラックで RU 41
- 39-RU 大規模なフォーム ファクタ デュアル ラック プラットフォーム — ラック 2 の RU 41
- 8 RU 小規模フォーム ファクタ プラットフォーム - プラットフォーム ラック で RU 11



第 4 章

ユーザ インターフェイスの設定

（オプション）デュアルスタックモード（IPv6サポート）の要件と制限事項

物理ハードウェア上で実行される Cisco Secure Workload クラスタは、クラスタへの特定の通信とクラスタからの特定の通信に、IPv4 だけでなく IPv6 も使用するように設定できます。

（注） 3.6.1.5 リリースと 3.7.1.5 リリースをインストールまたはアップグレードする場合は、デュアルスタックモード（IPv6 サポート）機能を使用できますが、パッチリリースをインストールまたはアップグレードする場合は、この機能は使用できません。

制限事項

デュアルスタックモードの有効化を考慮している場合は、次の点に注意してください。

- IPv6 接続は、初期展開時またはメジャーリリースへのアップグレード時にのみ有効にできます（パッチアップグレード時にはこの機能は有効にできません）。
- デュアルスタックモードは、物理ハードウェア/ベアメタルクラスタでのみサポートされます。
- IPv6 専用モードはサポートされていません。
- クラスタでデュアルスタックモードを有効化した後は、IPv4 専用モードに戻すことはできません。
- デュアルスタック接続が有効な場合、データのバックアップと復元（DBR）はサポートされません。

- フェデレーションが設定されているクラスタでは、デュアルスタックモードを有効にしないでください。
- 次の機能では常に IPv4 のみを使用します（IPv6 が有効になっている場合も IPv4 は常に有効になっています）。
  - （リリース 3.7.1.5 と 3.6.x に適用）AIX エージェントでの適用
  - （リリース 3.6.x に適用）クラスタとのハードウェアエージェント通信
  - （リリース 3.6.x に適用）フローの取り込み、インベントリの強化、またはアラート通知用のコネクタ

要件

- FQDN の A および AAAA DNS レコードの両方を設定する必要があります。クラスタに対してデュアルスタックモードを有効にする前に、これを構成する必要があります。
- NTP、SMTP、DNS などの外部サービスは、冗長性のために IPv4 と IPv6 の両方で使用できる必要があります。
- クラスタにデュアルスタックモードを構成するには、次の手順を実行します。
  - 2つのクラスタリーフスイッチには、冗長性を確保するため、異なる2つのネットワーク上のルーティング可能な IPv6 アドレスをそれぞれ割り当てる必要があります。また、各ネットワークにデフォルトゲートウェイを提供する必要があります。
  - 39RU クラスタの場合、少なくとも 29 個のホストアドレス用のスペースを持つ、サイトでルーティング可能な IPv6 ネットワークが必要です。
  - 8RU クラスタの場合、少なくとも 20 個 のホストアドレス用のスペースを持つ、サイトでルーティング可能な IPv6 ネットワークが必要です。
  - サイトでルーティング可能な IPv6 ネットワークの最初の 3 つのホストアドレスは、Cisco Secure Workload クラスタ HSRP 設定用に予約されています。他のデバイスでは使用しないでください。

その他の情報

エージェントは、IPv6 を使用するように設定しない限り、IPv4 を使用してクラスタと通信します。手順については、Cisco Secure Workload Web ポータルから入手可能なユーザーガイドを参照してください。

ユーザーインターフェイスの設定

始める前に

- この設定を完了するには、インターネットにアクセスするために、イーサネットポート付きのラップトップコンピューターなどのデバイスが必要です。
- Tetration（Secure Workload）クラスタの最上位のサーバーにデバイスを接続するには、イーサネットケーブルが必要です。
- Google Chrome は、この手順の一部で必要となるセットアップポータルでサポートされる唯一のブラウザです。
- （オプション）バージョン 3.6 以降では、デュアルスタックモードでクラスタを設定できるため、一部の Cisco Secure Workload コンポーネント間、および Cisco Secure Workload と NTP や DNS などのネットワークサービス間の通信に、IPv4 と IPv6 の両方を使用できます。（デュアルワークロードモードを有効化するかどうかにかかわらず、Cisco Secure Workload はすでに IPv6 トラフィックを処理しています。）このサポートは、展開時またはアップグレード時にのみ有効化できます。

  IPv6 のサポートの有効化を検討している場合は、（オプション）デュアルスタックモード（IPv6 サポート）の要件と制限事項 （19 ページ）を参照してください。

重要 フィールド名に明示的に IPv6 と示されている場合を除き、次の手順のすべてのフィールドに IPv4 アドレスを入力します。

手順

ステップ 1 インターネット デバイスに IP アドレス 2.2.2.1/30 (255.255.255.252) を設定します。

ステップ 2 Cisco Tetration（Cisco Secure Workload）クラスタの最上位のサーバーの ETH1 ポートにインターネットデバイスのイーサネットポートを接続するには、イーサネットケーブルを使用します。

ステップ 3 インターネット デバイスで、Chrome ブラウザを開き http://2.2.2.2:9000 に移動します。

（注） Chrome ブラウザは、このプロセスでテストした唯一のブラウザです。

Cisco Tetration（Cisco Secure Workload）セットアップ診断ページが開きます。

ステップ 4 診断ページにエラーがある場合は、この手順を継続する前に、クラスタ デバイスの間のケーブル接続に破損した接続がないかどうか、またはケーブルが間違って経路指定されていないかどうかをチェックします (すべてのケーブル配線を検証するためには、付録の配線表を使用してください)。完了したら、ステップ 2 に戻ります。

ステップ 5 [継続（Continue）] をクリックします。

RPM アップロード ページが開きます。

（注） サイト設定ページが代わりに開いた場合、次の URL を入力して、RPM アップロード ページを開きます。

http://2.2.2.2:9000/upload

ステップ 6 RPM オブジェクトを、次のように Cisco Tetration（Cisco Secure Workload）クラウドにアップロードします。

1. [ファイルの選択（Choose File）] をクリックします。
2. 参照して、アドホックおよび母ファイルを検索してください。
3. [アップロード（Upload）] をクリックします。

   [サイト構成（Site Config）] ページが開きます。

ステップ 7 [サイト構成（Site Config）] ページを使用して、次のように新しいサイトを設定します。

- **[一般（General）]** フォーム
  1. [サイト名（Site Name）] フィールドに、一意のクラスタ名を入力します。
  2. [SSH パブリックキー（SSH Public Key）] フィールドに、認証キーを貼り付けます。

     （注） クラスタ SSH アクセスに使用できる独自の SSH キーペアを生成します。

  3. [次へ（Next）] をクリックします。

- **[電子メール（Email）]** フォーム
  1. 必要な電子メールアドレスを入力します。
  2. [次へ（Next）] をクリックします。

- **L3**フォーム

  要求された各アドレスを入力します。* が付いたすべてのフィールドは必須フィールドです。フィールド名に IPv6 が指定されていない場合は、すべてのアドレスを IPv4 として入力します。

  （オプション）ソフトウェアバージョン3.6以降をインストールする場合：デュアルスタックモード（ IPv4 と IPv6 の両方をサポート）を有効にします。
  1. [IPv6（IPv6）] チェックボックスをオンにします。
  2. Leaf 1 と Leaf 2 の両方のスイッチの IPv6 アドレスを CIDR 表記で入力します。
  3. Leaf 1 と Leaf 2 の IPv6 デフォルトゲートウェイを入力します。
  4. [次へ（Next）] をクリックします。

- **[ネットワーク（Network）]**フォーム

フィールド名に IPv6 が指定されていない場合は、すべてのアドレスを IPv4 として入力します。

1. [内部ネットワークIPアドレス（Internal network IP address）] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
2. [外部ネットワークIPアドレス（External network IP address）] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
3. [外部ゲートウェイIPアドレス（External gateway IP address）] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
4. [DNSリゾルバIPアドレス（DNS resolver IP address）] フィールドに、オーケストレータ展開出力からアドレスを貼り付けます。
5. **[DNS ドメイン（DNS domain）]** フィールドに、DNS ドメイン（たとえば、「cisco.com」）を入力します。
6. （ソフトウェアバージョン 3.6 以降）[L3] ページで IPv6 を有効化した場合は、[IPv6] が自動的に選択されます。

   IPv6 が選択された場合は、Cisco Secure Workload 用に予約されている IPv6 アドレスを指定する必要があります。

   - [外部 IPv6 ネットワーク（External IPv6 Network）] を入力します。

     [外部 IPv6 ネットワーク（External IPv6 Network）] フィールドの最初の 3 つの IPv6 アドレスは、常に Cisco Secure Workload クラスタのスイッチ用に予約されており、他の目的には使用できません。

   - 特定のアドレスにのみ IPv6 を使用する場合は、[外部 IPv6 ネットワーク（External IPv6 Network）] フィールドにそれらのアドレスを入力します。

   （注）
   - 39 RU クラスタの場合、[IPv6 外部 ネットワーク（IPv6 External Network）] または [外部 IPv6 IPs（External IPv6 IPs）] リストで、少なくとも 29 個の IPv6 アドレスが使用可能であることを確認します。
   - 8 RU クラスタの場合、[IPv6 外部 ネットワーク（IPv6 External Network）] または [外部 IPv6 IPs（External IPv6 IPs）] リストで、少なくとも 20 個の IPv6 アドレスが使用可能であることを確認します。

7. [次へ（Next）] をクリックします。

- **[サービス（Service）]** フォーム

1. **[NTP サービス（NTP Servers）]** フィールドに、オーケストレータ展開出力から NTP サーバ名または IP アドレスのスペース区切りのリストを入力します。
2. [SMTP サーバー（SMTP Server）] フィールドに、Cisco Tetration（Cisco Secure Workload）が電子メール メッセージの送信に使用できる SMTP サーバーの名前また

はIPアドレスを入力します（このサーバーはCisco Tetration（Cisco Secure Workload）からアクセス可能である必要があります）。

3. **[SMTPポート（SMTP Port）]**フィールドに、SMTPサーバーのポート番号を入力します。AWSは、ポート25と465の使用を制限します。アカウントを正しく構成するか、またはポート587を使用する必要があります。
4. **[SMTPユーザ名（SMTP Username）]**フィールドに、SMTP認証用のユーザ名を入力します。
5. **[SMTPパスワード（SMTP Password）]**フィールドに、SMTP認証用のパスワードを入力します。
6. （オプション）[HTTPプロキシサーバー（HTTP Proxy Server）]フィールドに、インターネットの外部サービスにアクセスするためにCisco Tetration（Cisco Secure Workload）で使用するHTTPプロキシサーバーの名前またはIPアドレスを入力します。
7. (オプション) **[HTTPプロキシサーバー（HTTP Proxy Port）]**フィールドに、HTTPプロキシ サーバーのポート番号を入力します。
8. （オプション）[HTTPSプロキシサーバー（HTTPs Proxy Server）]フィールドに、インターネットの外部サービスにアクセスするためにCisco Tetration（Cisco Secure Workload）で使用するHTTPSプロキシサーバーの名前またはIPアドレスを入力します。
9. (オプション)**[HTTPプロキシサーバー（HTTPs Proxy Port）]**フィールドに、HTTPsプロキシ サーバーのポート番号を入力します。
10. （オプション）[Syslogサーバー（Syslog Server）]フィールドに、アラートを送信するためにCisco Tetration（Cisco Secure Workload）で使用するsyslogサーバーの名前またはIPアドレスを入力します。
11. (オプション)**[Syslogポート（Syslog Port）]**フィールドに、syslogサーバのポート番号を入力します。
12. (オプション)**[Syslog重大度（Syslog Severity）]**フィールドに、syslogメッセージのシビラティ（重大度）レベルを入力します。可能な値には、情報、警告、エラー、緊急、アラート、重要な注意が含まれます。
13. [次へ（Next）]をクリックします。

- **[UI]**フォーム

1. **[UI VRRP VRID]**フィールドに、一意のVRIDが必要なければ、「77」を入力します。
2. **[UI FQDN]**フィールドに、クラスタにアクセスする完全修飾ドメイン名を入力します。
3. **[UI Airbrake Key]**フィールドは空白のままにします。
4. [次へ（Next）]をクリックします。

Cisco Tetration（Cisco Secure Workload）は、構成時の設定を検証し、設定のステータスを表示します。

- **[Advanced]** フォーム
  1. [External IPs] フィールドに、IPv4 アドレスを入力します。
  2. [継続（Continue）] をクリックします。

ステップ 8 障害がある場合は、[Back] をクリックし、設定を編集してください（ステップ 7 を参照してください）。

（注） このページを離れた後でこれらの設定をセットアップ GUI で変更することはできません。ただし、後で GUI の [company] ページから設定を変更できます。

ステップ 9 設定に対して検出された障害がなく、変更を加える必要がない場合は、[Continue] をクリックします。

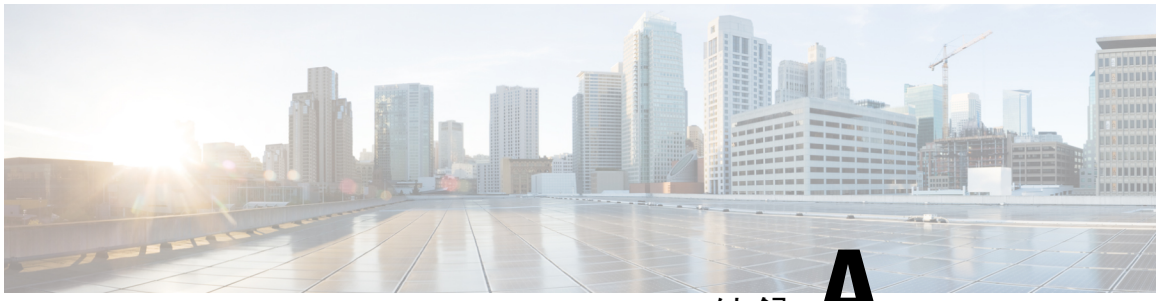
Cisco Tetration（Cisco Secure Workload）は指定された設定に従って構成します。このプロセスは、ユーザー側の操作なしで 1 ～ 2 時間かかることがあります。

次のタスク

ソフトウェアバージョン 3.6 以降を展開し、IPv6 接続を有効化した場合：

- IPv4 または IPv6 を使用して Cisco Secure Workload Webポータルにアクセスできます。
- デフォルトでは、クラスタが IPv6 をサポートするために有効化されていても、ソフトウェアエージェントは IPv4 を使用して Cisco Secure Workload クラスタと通信します。この目的のためにサポートされているエージェントで IPv6 を使用する場合は、Cisco Secure Workload Web ポータルの [Platform] > [Cluster Configuration] ページで、[Sensor VIP FQDN] フィールドを設定する必要があります。重要な指示については、Cisco Secure Workload Web ポータルまたは https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html から、オンラインヘルプとして入手可能なユーザーガイドを参照してください。

ユーザーインターフェイスの設定



付録 A

システムの仕様

環境仕様

次の表に、Cisco Tetration（Cisco Secure Workload）クラスタをインストールするために必要な環境仕様を示します。

表 *1* : 環境仕様

環境		仕様
温度	動作時	5 ～ 35 °C（41 ～ 95 °F）、海抜 305 m（1000 フィート）ごとに最高温低下
	ストレージ	-40 ～ 149°F（-40 ～ 65°C）
湿度	動作時	相対湿度 10 ～ 80 %、1 時間当たり 10 % の湿度上昇
	ストレージ	相対温度 5 ～ 93 %
高度	動作時	0 ～ 10,000 フィート（0 ～ 3050 m）
	ストレージ	0 ～ 40,000 フィート（0 ～ 12,200 m）

ハードウェアに同梱されているケーブル

次の表に、クラスタハードウェアに同梱されているケーブルを示します。

表 *2 : Cisco Tetration*（*Cisco Secure Workload*）*39 RU* クラスタ、シングルラック構成

部品番号	説明	数量
TA: ラック UCS2-INT	Cisco R42612 ダイナミックラック、Cisco Tetration のサイドパネル	1
TA-ETH-RJ45-シングル	39 RU Cisco Tetration シングルラック構成用の RJ45 ケーブルキット	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2 メートル ケーブル	16
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5 メートル ケーブル	32
TA-QSFP-H40G-CU1M	40GBASE-CR4 パッシブ銅ケーブル、1 メートル	4
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1 メートル ケーブル	25
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5 メートルケーブル	20

表 *3 : Cisco Tetration*（*Cisco Secure Workload*）*39 RU* クラスタ、デュアルラック構成

部品番号	説明	数量
TA: ラック UCS2-INT	Cisco R42612 ダイナミックラック、Cisco Tetration のサイドパネル	2
TA-ETH-RJ45-DUAL	39 RU Cisco Tetration シングルラック構成用の RJ45 ケーブルキット	1
TA-SFP-H10GB-CU2M	10GBASE-CU SFP+ 2 メートル ケーブル	15
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5 メートル ケーブル	19
TA-QSFP-H40G-CU1M	40GBASE-CR4 パッシブ銅ケーブル、1 メートル	1
TA-QSFP-H40G-CU5M	40GBASE-CR4 パッシブ銅線 5 メートルケーブル	3
TA-SFP-H10GB-CU2-5	10GBASE-CU SFP+ 2.5 メートルケーブル	12
TA-SFP-H10GB-CU5M	10GBASE-CU SFP+ 5 メートル ケーブル	47

表 *4 : Cisco Tetration*（*Cisco Secure Workload*）*8 RU* クラスタ

部品番号	説明	数量
TA: ラック UCS2-INT	Cisco R42612 ダイナミックラック、Cisco Tetration のサイドパネル	1

部品番号	説明	数量
ETH-S-RJ45	RJ-45 ストレート ケーブル、イーサネット用イエロー 6フィート ケーブル	6
TA-SFP-H10GB-CU1M	10GBASE-CU SFP+ 1 メートル ケーブル	13
TA-SFP-H10GB-CU1-5	10GBASE-CU SFP+ 1.5 メートル ケーブル	12
TA-QSFP-H40G-CU1M	40GBASE-CR4 パッシブ銅ケーブル、1 メートル	2
GLC-TE	カテゴリ 5 銅線用 1000BASE-T SFP トランシーバモジュール	6

C1-Tetration クラスタ デバイスの配線

次の図は、C1 Tetration ラック デバイスが相互接続する方法を示します。接続の詳細なリストについては、その図の下の表を参照してください。

（注） CIMC/PXE スイッチは、3 つのスイッチのそれぞれに管理 (管理) ポートと 36 個の コンピューティング、キャッシュ、およびベースのサーバ ホストのそれぞれの eth0 ポートに接続されています。

システムの仕様

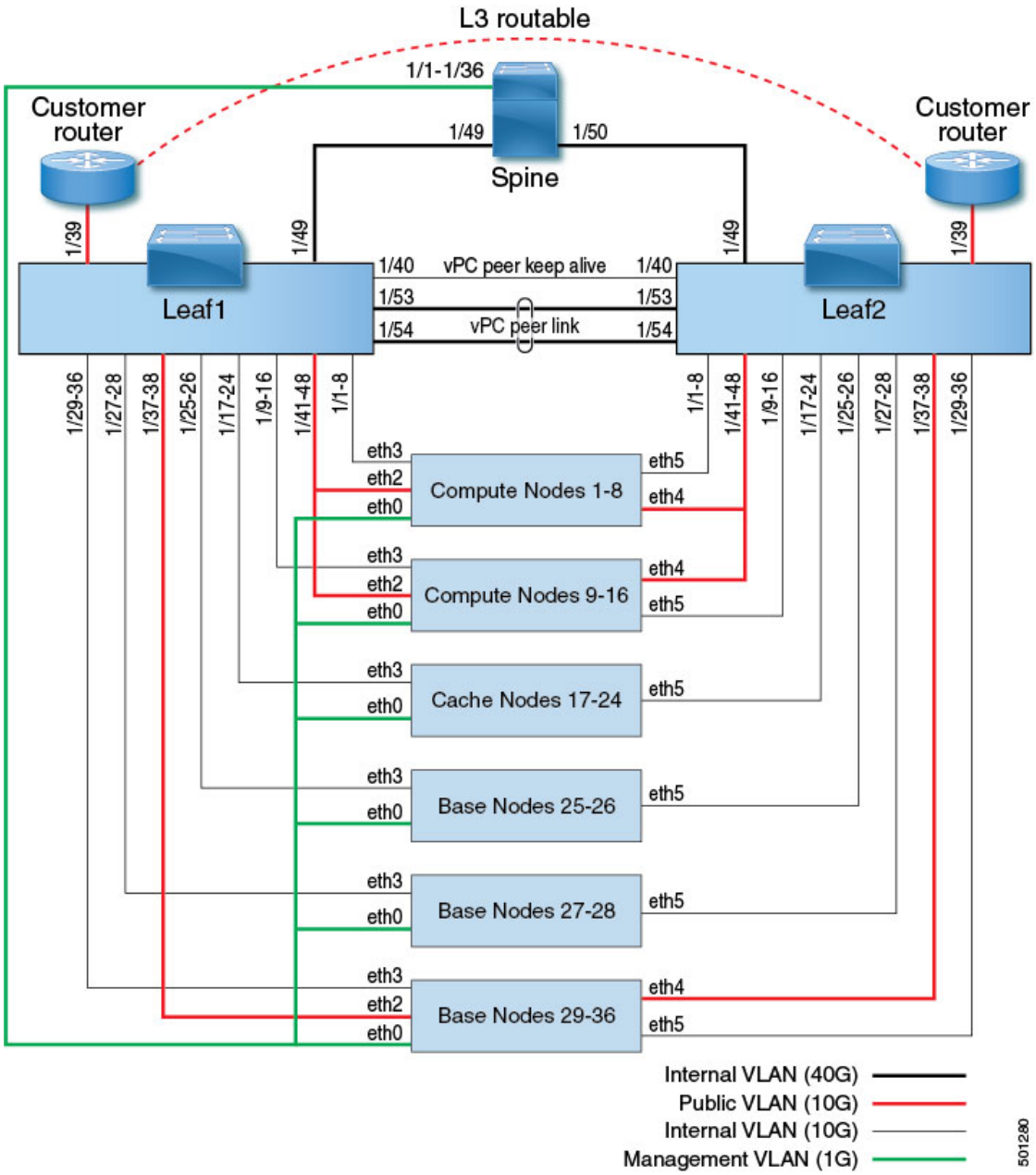


表 *5 :* スパイン スイッチ接続 *(RU 41* のシングル ラック インストールまたはデュアル ラック インストールで *RU 40)*

スパイン ポート	接続タイプ	接続			
		デバイス	シングル ラックの **RU**	デュアル ラックの **RU**	ポート
1	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 1 (コンピューティング サーバ 1)	RU 36	ラック 1 RU 17	eth0

システムの仕様

スパイン ポート	接続タイプ	接続			
		デバイス	シングル ラックの **RU**	デュアル ラックの **RU**	ポート
2	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 2 (コンピューティング サーバ 2)	RU 35	ラック 1 RU 16	eth0
3	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 3 (コンピューティング サーバ 3)	RU 34	ラック 1 RU 15	eth0
4	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 4 (コンピューティング サーバ 4)	RU 33	ラック 1 RU 14	eth0
5	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 5 (コンピューティング サーバ 5)	RU 32	ラック 1 RU 13	eth0
6	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 6 (コンピューティング サーバ 6)	RU 31	ラック 1 RU 12	eth0
7	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 7 (コンピューティング サーバ 7)	RU 30	ラック 1 RU 11	eth0
8	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 8 (コンピューティング サーバ 8)	RU 29	ラック 1 RU 10	eth0
9	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 9 (コンピューティング サーバ 9)	RU 28	ラック 1 RU 8	eth0
10	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 10 (コンピューティング サーバ 10)	RU 27	ラック 1 RU 7	eth0
11	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 11 (コンピューティング サーバ 11)	RU 26	ラック 1 RU 6	eth0
12	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 12 (コンピューティング サーバ 12)	RU 25	ラック 1 RU 5	eth0
13	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 13 (コンピューティング サーバ 13)	RU 24	ラック 1 RU 4	eth0
14	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 14 (コンピューティング サーバ 14)	RU 23	ラック 1 RU 3	eth0
15	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 15 (コンピューティング サーバ 15)	RU 22	ラック 1 RU 2	eth0
16	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 16 (コンピューティング サーバ 16)	RU 21	ラック 1 RU 1	eth0

スパイン ポート	接続タイプ	接続			
		デバイス	シングル ラックの **RU**	デュアル ラックの **RU**	ポート
17	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 17 (キャッシュ サーバ 1)	RU 20	ラック 2 RU 21	eth0
18	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 18 (キャッシュ サーバ 2)	RU 19	ラック 2 RU 20	eth0
19	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 19 (キャッシュ サーバ 3)	RU 18	ラック 2 RU 19	eth0
20	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 20 (キャッシュ サーバ 4)	RU 17	ラック 2 RU 18	eth0
21	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 21 (キャッシュ サーバ 5)	RU 16	ラック 2 RU 17	eth0
22	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 22 (キャッシュ サーバ 6)	RU 15	ラック 2 RU 16	eth0
23	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 23 (キャッシュ サーバ 7)	RU 14	ラック 2 RU 15	eth0
24	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 24 (キャッシュ サーバ 8)	RU 13	ラック 2 RU 14	eth0
25	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 25 (基本サーバ 1)	RU 12	ラック 2 RU 12	eth0
26	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 26 (基本サーバ 2)	RU 11	ラック 2 RU 11	eth0
27	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 27 (基本サーバ 3)	RU 10	ラック 2 RU 10	eth0
28	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 28 (基本サーバ 4)	RU 9	ラック 2 RU 9	eth0
29	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 29 (基本サーバの 5 分)	RU 8	ラック 2 RU 8	eth0
30	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 30 (基本サーバ 6)	RU 7	ラック 2 RU 7	eth0
31	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 31 (基本サーバ 7)	RU 6	ラック 2 RU 6	eth0

スパイン ポート	接続タイプ	接続			
		デバイス	シングル ラックの RU	デュアル ラックの RU	ポート
32	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 32 (基本サーバ 8)	RU 5	ラック 2 RU 5	eth0
33	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 33 (基本サーバ 9)	RU 4	ラック 2 RU 14	eth0
34	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 34 (基本サーバ 10)	RU 3	ラック 1 RU 3	eth0
35	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 35 (基本サーバ 11)	RU 2	ラック 2 RU 2	eth0
36	CIMC/PXE VLAN (1 ギガビット)	UCS サーバ ホスト 36 (基本サーバ 12)	RU 1	ラック 2 RU 1	eth0
49	内部 VLAN (40 ギガビット)	リーフ スイッチ 1 (1 つのラックの RU 41 またはデュアル ラックのラック 1 の RU 40)	RU 40	ラック 1 RU 40	49
50	内部 VLAN (40 ギガビット)	リーフ スイッチ 2 (1 つのラックで RU 40) またはデュアル ラックのラック 2 の RU 40) ポート 49	RU 41	ラック 2 RU 40	49

表 *6 :* リーフ スイッチ *2* 接続 *(RU 41* のシングル ラック インストールまたはデュアル ラック インストールで *RU 40)*

リーフ 2 ポート	接続タイプ	接続			
		デバイス	シングル ラックの RU	シングル ラックの RU	ポート
1	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 1 (コンピューティング サーバ 1)	RU 36	ラック 1 RU 17	eth5
2	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 2 (コンピューティング サーバ 2)	RU 35	ラック 1 RU 16	eth5
3	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 3 (コンピューティング サーバ 3)	RU 34	ラック 1 RU 15	eth5
4	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 4 (コンピューティング サーバ 4)	RU 33	ラック 1 RU 14	eth5

リーフ 2 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	シングルラックの RU	ポート
5	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 5 (コンピューティング サーバ 5)	RU 32	ラック 1 RU 13	eth5
6	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 6 (コンピューティング サーバ 6)	RU 31	ラック 1 RU 12	eth5
7	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 7 (コンピューティング サーバ 7)	RU 30	ラック 1 RU 11	eth5
8	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 8 (コンピューティング サーバ 8)	RU 29	ラック 1 RU 10	eth5
9	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 9 (コンピューティング サーバ 9)	RU 28	ラック 1 RU 8	eth5
10	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 10 (コンピューティング サーバ 10)	RU 27	ラック 1 RU 7	eth5
11	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 11 (コンピューティング サーバ 11)	RU 26	ラック 1 RU 6	eth5
12	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 12 (コンピューティング サーバ 12)	RU 25	ラック 1 RU 5	eth5
13	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 13 (コンピューティング サーバ 13)	RU 24	ラック 1 RU 4	eth5
14	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 14 (コンピューティング サーバ 14)	RU 23	ラック 1 RU 3	eth5
15	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 15 (コンピューティング サーバ 15)	RU 22	ラック 1 RU 2	eth5
16	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 16 (コンピューティング サーバ 16)	RU 21	ラック 1 RU 1	eth5
17	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 17 (キャッシュ サーバ 1)	RU 20	ラック 2 RU 21	eth5
18	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 18 (キャッシュ サーバ 2)	RU 19	ラック 2 RU 20	eth5
19	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 19 (キャッシュ サーバ 3)	RU 18	ラック 2 RU 19	eth5

リーフ 2 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	シングルラックの RU	ポート
20	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 20 (キャッシュ サーバ 4)	RU 17	ラック 2 RU 18	eth5
21	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 21 (キャッシュ サーバ 5)	RU 16	ラック 2 RU 17	eth5
22	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 22 (キャッシュ サーバ 6)	RU 15	ラック 2 RU 16	eth5
23	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 23 (キャッシュ サーバ 7)	RU 14	ラック 2 RU 15	eth5
24	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 24 (キャッシュ サーバ 8)	RU 13	ラック 2 RU 14	eth5
25	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 25 (基本サーバ 1)	RU 12	ラック 2 RU 12	eth5
26	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 26 (基本サーバ 2)	RU 11	ラック 2 RU 11	eth5
27	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 27 (基本サーバ 3)	RU 10	ラック 2 RU 10	eth5
28	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 28 (基本サーバ 4)	RU 9	ラック 2 RU 9	eth5
29	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 29 (基本サーバの 5 分)	RU 8	ラック 2 RU 8	eth5
30	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 30 (基本サーバ 6)	RU 7	ラック 2 RU 7	eth5
31	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 31 (基本サーバ 7)	RU 6	ラック 2 RU 6	eth5
32	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 32 (基本サーバ 8)	RU 5	ラック 2 RU 5	eth5
33	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 33 (基本サーバ 9)	RU 4	ラック 2 RU 14	eth5
34	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 34 (基本サーバ 10)	RU 3	ラック 1 RU 3	eth5

リーフ 2 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	シングルラックの RU	ポート
35	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 35 (基本サーバ 11)	RU 2	ラック 2 RU 2	eth5
36	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 36 (基本サーバ 12)	RU 1	ラック 2 RU 1	eth5
37	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 34 (基本サーバ 10)	RU 3	ラック 1 RU 3	eth2
38	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 36 (基本サーバ 12)	RU 1	ラック 2 RU 1	eth2
39	内部 VLAN (10 ギガビット)	カスタマー ルータ 1	対応	対応	対応
40	内部 VLAN (10 ギガビット)	リーフ スイッチ 1	RU 40	ラック 1 RU 40	40
41	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 2 (コンピューティング サーバ 2)	RU 35	ラック 1 RU 16	eth2
42	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 4 (コンピューティング サーバ 4)	RU 33	ラック 1 RU 14	eth2
43	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 6 (コンピューティング サーバ 6)	RU 31	ラック 1 RU 12	eth2
44	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 8 (コンピューティング サーバ 8)	RU 29	ラック 1 RU 10	eth2
45	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 10 (コンピューティング サーバ 10)	RU 27	ラック 1 RU 8	eth2
46	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 12 (コンピューティング サーバ 12)	RU 25	ラック 1 RU 6	eth2
47	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 14 (コンピューティング サーバ 14)	RU 23	ラック 1 RU 4	eth2
48	パブリック VLAN (10 ギガ ビット)	UCSサーバ ホスト 14 (コンピューティング サーバ 14)	RU 21	ラック 1 RU 2	eth2
49	内部 VLAN (40 ギガビット)	スパイン スイッチ	RU 42	ラック 1 RU 42	50

リーフ 2 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	シングルラックの RU	ポート
50	対応	対応	対応	対応	対応
51	対応	対応	対応	対応	対応
52	対応	対応	対応	対応	対応
53	内部 VLAN (40 ギガビット)	リーフ スイッチ 1	RU 40	ラック 1 RU 40	53
54	内部 VLAN (40 ギガビット)	リーフ スイッチ 1	RU 40	ラック 1 RU 40	54

表 *7:* リーフ スイッチ *2* 接続 *(*シングルおよびデュアル ラック インストールで *RU 40)*

リーフ 1 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	デュアルラックの RU	ポート
1	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 1 (コンピューティング サーバ 1)	RU 36	ラック 1 RU 17	eth3
2	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 2 (コンピューティング サーバ 2)	RU 35	ラック 1 RU 16	eth3
3	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 3 (コンピューティング サーバ 3)	RU 34	ラック 1 RU 15	eth3
4	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 4 (コンピューティング サーバ 4)	RU 33	ラック 1 RU 14	eth3
5	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 5 (コンピューティング サーバ 5)	RU 32	ラック 1 RU 13	eth3
6	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 6 (コンピューティング サーバ 6)	RU 31	ラック 1 RU 12	eth3
7	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 7 (コンピューティング サーバ 7)	RU 30	ラック 1 RU 11	eth3
8	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 8 (コンピューティング サーバ 8)	RU 29	ラック 1 RU 10	eth3

リーフ 1 ポート	接続タイプ	接続			
		デバイス	シングルラックの RU	デュアルラックの RU	ポート
9	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 9 (コンピューティング サーバ 9)	RU 28	ラック 1 RU 8	eth3
10	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 10 (コンピューティング サーバ 10)	RU 27	ラック 1 RU 7	eth3
11	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 11 (コンピューティング サーバ 11)	RU 26	ラック 1 RU 6	eth3
12	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 12 (コンピューティング サーバ 12)	RU 25	ラック 1 RU 5	eth3
13	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 13 (コンピューティング サーバ 13)	RU 24	ラック 1 RU 4	eth3
14	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 14 (コンピューティング サーバ 14)	RU 23	ラック 1 RU 3	eth3
15	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 15 (コンピューティング サーバ 15)	RU 22	ラック 1 RU 2	eth3
16	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 16 (コンピューティング サーバ 16)	RU 21	ラック 1 RU 1	eth3
17	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 17 (キャッシュ サーバ 1)	RU 20	ラック 2 RU 21	eth3
18	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 18 (キャッシュ サーバ 2)	RU 19	ラック 2 RU 20	eth3
19	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 19 (キャッシュ サーバ 3)	RU 18	ラック 2 RU 19	eth3
20	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 20 (キャッシュ サーバ 4)	RU 17	ラック 2 RU 18	eth3
21	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 21 (キャッシュ サーバ 5)	RU 16	ラック 2 RU 17	eth3
22	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 22 (キャッシュ サーバ 6)	RU 15	ラック 2 RU 16	eth3
23	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 23 (キャッシュ サーバ 7)	RU 14	ラック 2 RU 15	eth3

リーフ 1 ポート	接続タイプ	接続			
		デバイス	シングル ラックの RU	デュアル ラックの RU	ポート
24	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 24 (キャッシュ サーバ 8)	RU 13	ラック 2 RU 14	eth3
25	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 25 (基本サーバ 1)	RU 12	ラック 2 RU 12	eth3
26	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 26 (基本サーバ 2)	RU 11	ラック 2 RU 11	eth3
27	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 27 (基本サーバ 3)	RU 10	ラック 2 RU 10	eth3
28	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 28 (基本サーバ 4)	RU 9	ラック 2 RU 9	eth3
29	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 29 (基本サーバの 5 分)	RU 8	ラック 2 RU 8	eth3
30	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 30 (基本サーバ 6)	RU 7	ラック 2 RU 7	eth3
31	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 31 (基本サーバ 7)	6	ラック 2 RU 6	eth3
32	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 32 (基本サーバ 8)	RU 5	ラック 2 RU 5	eth3
33	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 33 (基本サーバ 9)	RU 4	ラック 2 RU 14	eth3
34	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 34 (基本サーバ 10)	RU 3	ラック 1 RU 3	eth3
35	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 35 (基本サーバ 11)	RU 2	ラック 2 RU 2	eth3
36	内部 VLAN (10 ギガビット)	UCS サーバ ホスト 36 (基本サーバ 12)	RU 1	ラック 2 RU 1	eth3
37	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 33 (基本サーバ 9)	RU 4	ラック 2 RU 8	eth2
38	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 35 (基本サーバ 11)	RU 2	ラック 2 RU 6	eth2

リーフ 1 ポート	接続タイプ	接続			
		デバイス	シングル ラックの RU	デュアル ラックの RU	ポート
39	内部 VLAN (10 ギガビット)	カスタマー ルータ 1	対応	対応	対応
40	内部 VLAN (10 ギガビット)	リーフ スイッチ 2	RU 41	ラック 2 RU 40	40
41	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 1 (コンピューティング サーバ 1)	RU 36	ラック 1 RU 17	eth2
42	パブリック VLAN (10 ギガ ビット)	UCSサーバ ホスト 3 (Compute server3)	RU 34	ラック 1 RU 15	eth2
43	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 5 (コンピューティング サーバ 5)	RU 32	ラック 1 RU 13	eth2
44	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 7 (コンピューティング サーバ 7)	RU 30	ラック 1 RU 11	eth2
45	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 9 (コンピューティング サーバ 9)	RU 28	ラック 1 RU 9	eth2
46	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 11 (コンピューティング サーバ 11)	RU 26	ラック 1 RU 7	eth2
47	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 13 (コンピューティング サーバ 13)	RU 24	ラック 1 RU 5	eth2
48	パブリック VLAN (10 ギガ ビット)	UCS サーバ ホスト 15 (コンピューティング サーバ 15)	RU 22	ラック 1 RU 3	eth2
49	内部 VLAN (40 ギガビット)	スパイン スイッチ	RU 42	ラック 1 RU 42	49
50	対応	対応	対応	対応	対応
51	対応	対応	対応	対応	対応
52	対応	対応	対応	対応	対応
53	内部 VLAN (40 ギガビット)	リーフ スイッチ	RU 40	ラック 1 RU 40	53
54	内部 VLAN (40 ギガビット)	リーフ 2 スイッチ	RU 41	ラック 2 RU 40	54

C1-Tetration-M クラスタのデバイスのケーブル配線

次の図は、C1-Tetration-M クラスタ ラックのデバイスを相互接続する方法を示します。接続の詳細なリストについては、その図の下の表を参照してください。

（注） CIMC/PXE スイッチは、3 つのスイッチのそれぞれに管理 (管理) ポートと 36 個の コンピューティング、キャッシュ、およびベースのサーバ ホストのそれぞれの eth0 ポートに接続されています。

システムの仕様

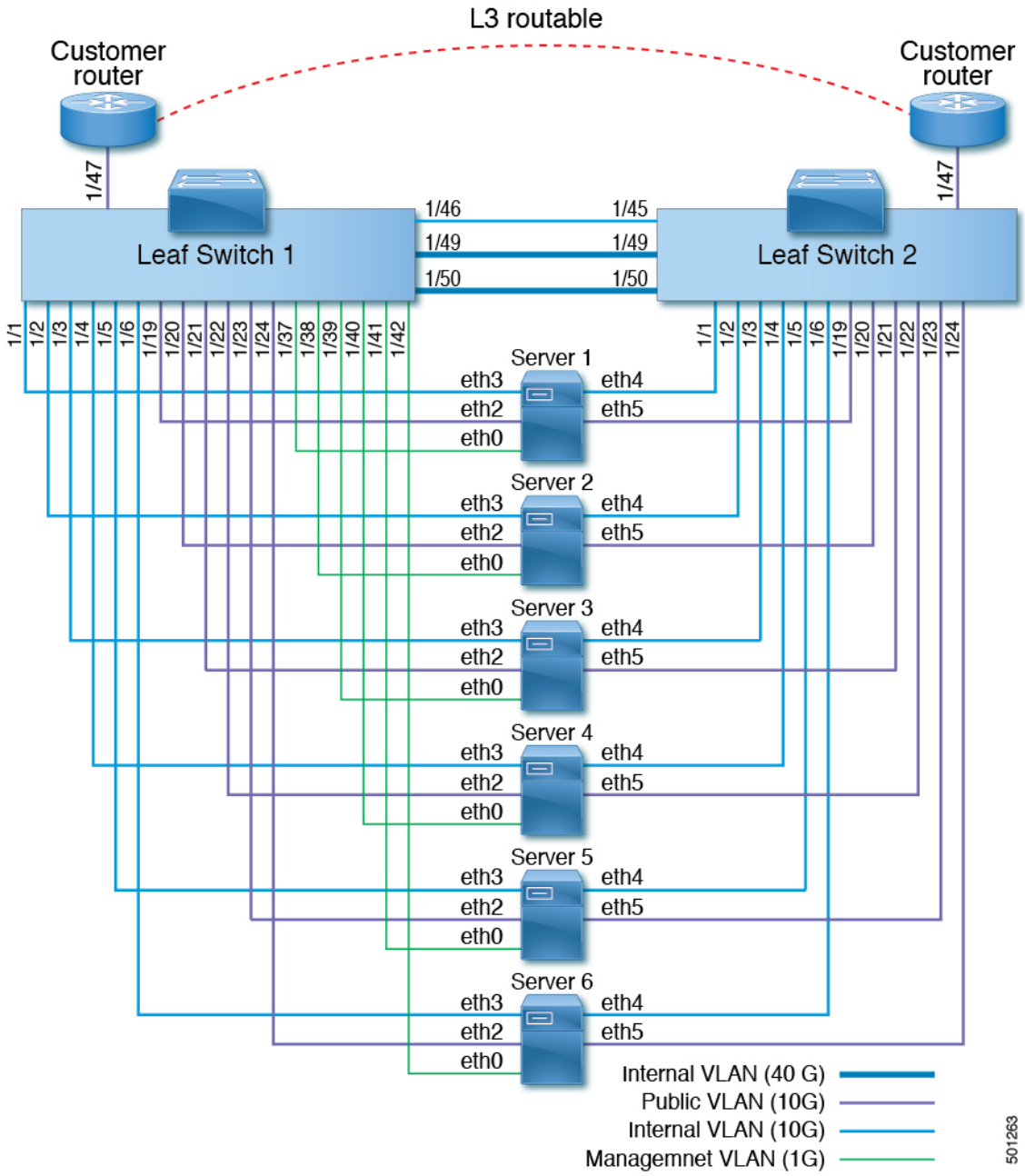


表 *8 :* リーフ スイッチ *1 (RU 12)* 接続

スパイン ポート	接続タイプ	接続		
		デバイス	シングル ラックの **RU**	ポート
1	内部 VLAN (10 ギガビット)	Server 1	9	eth3

スパイン ポート	接続タイプ	接続		
		デバイス	シングル ラックの **RU**	ポート
2	内部 VLAN (10 ギガビット)	Server 2	8	eth3
3	内部 VLAN (10 ギガビット)	Server 3	6	eth3
4	内部 VLAN (10 ギガビット)	[Server 4]	5	eth3
5	内部 VLAN (10 ギガビット)	サーバ 5	3	eth3
6	内部 VLAN (10 ギガビット)	サーバ 6	2	eth3
7	対応	対応	対応	対応
8	対応	対応	対応	対応
9	対応	対応	対応	対応
10	対応	対応	対応	対応
11	対応	対応	対応	対応
12	対応	対応	対応	対応
13	対応	対応	対応	対応
14	対応	対応	対応	対応
15	対応	対応	対応	対応
16	対応	対応	対応	対応
17	対応	対応	対応	対応
18	対応	対応	対応	対応
19	外部 VLAN (10 ギガビット)	Server 1	9	eth2
20	外部 VLAN (10 ギガビット)	Server 2	8	eth2

スパイン ポート	接続タイプ	接続		
		デバイス	シングルラックの RU	ポート
21	外部 VLAN (10 ギガビット)	Server 3	6	eth2
22	外部 VLAN (10 ギガビット)	[Server 4]	5	eth2
23	外部 VLAN (10 ギガビット)	サーバ 5	3	eth2
24	外部 VLAN (10 ギガビット)	サーバ 6	2	eth2
25	対応	対応	対応	対応
26	対応	対応	対応	対応
27	対応	対応	対応	対応
28	対応	対応	対応	対応
29	対応	対応	対応	対応
30	対応	対応	対応	対応
31	対応	対応	対応	対応
32	対応	対応	対応	対応
33	対応	対応	対応	対応
34	対応	対応	対応	対応
35	対応	対応	対応	対応
36	対応	対応	対応	対応
37	管理 VLAN (1 ギガビット)	Server 1	9	eth0
38	管理 VLAN (1 ギガビット)	Server 2	8	eth0
39	管理 VLAN (1 ギガビット)	Server 3	6	eth0

スパイン ポート	接続タイプ	接続		
		デバイス	シングル ラックの RU	ポート
40	管理 VLAN (1 ギガビット)	[Server 4]	5	eth0
41	管理 VLAN (1 ギガビット)	サーバ 5	3	eth0
42	管理 VLAN (1 ギガビット)	サーバ 6	2	eth0
43	対応	対応	対応	対応
44	対応	対応	対応	対応
45	対応	対応	対応	対応
46	内部 VLAN (10 ギガビット)	リーフ 2 スイッチ	11	45
47	外部 VLAN (10 ギガビット)	顧客のルータ	対応	対応
48	対応	対応	対応	対応
49	内部 VLAN (40 ギガビット)	リーフ 2 スイッチ	11	49
50	内部 VLAN (40 ギガビット)	リーフ 2 スイッチ	11	50
51	対応	対応	対応	対応
52	対応	対応	対応	対応
53	対応	対応	対応	対応
54	対応	対応	対応	対応

表 *9:* リーフ スイッチ *2 (RU 11)* 接続

スパイン ポート	接続タイプ	接続		
		デバイス	シングル ラックの **RU**	ポート
1	内部 VLAN (10 ギガビット)	Server 1	9	eth4
2	内部 VLAN (10 ギガビット)	Server 2	8	eth4
3	内部 VLAN (10 ギガビット)	Server 3	6	eth4
4	内部 VLAN (10 ギガビット)	[Server 4]	5	eth4
5	内部 VLAN (10 ギガビット)	サーバ 5	3	eth4
6	内部 VLAN (10 ギガビット)	サーバ 6	2	eth4
7	対応	対応	対応	対応
8	対応	対応	対応	対応
9	対応	対応	対応	対応
10	対応	対応	対応	対応
11	対応	対応	対応	対応
12	対応	対応	対応	対応
13	対応	対応	対応	対応
14	対応	対応	対応	対応
15	対応	対応	対応	対応
16	対応	対応	対応	対応
17	対応	対応	対応	対応
18	対応	対応	対応	対応
19	外部 VLAN (10 ギガビット)	Server 1	9	eth5

スパイン ポート	接続タイプ	接続		
		デバイス	シングル ラックの RU	ポート
20	外部 VLAN (10 ギガビット)	Server 2	8	eth5
21	外部 VLAN (10 ギガビット)	Server 3	6	eth5
22	外部 VLAN (10 ギガビット)	[Server 4]	5	eth5
23	外部 VLAN (10 ギガビット)	サーバ 5	3	eth5
24	外部 VLAN (10 ギガビット)	サーバ 6	2	eth5
25	対応	対応	対応	対応
26	対応	対応	対応	対応
27	対応	対応	対応	対応
28	対応	対応	対応	対応
29	対応	対応	対応	対応
30	対応	対応	対応	対応
31	対応	対応	対応	対応
32	対応	対応	対応	対応
33	対応	対応	対応	対応
34	対応	対応	対応	対応
35	対応	対応	対応	対応
36	対応	対応	対応	対応
37	管理 VLAN (1 ギガビット)	Server 1	9	eth0
38	管理 VLAN (1 ギガビット)	Server 2	8	eth0

スパイン ポート	接続タイプ	接続		
		デバイス	シングルラックの RU	ポート
39	管理 VLAN (1 ギガビット)	Server 3	6	eth0
40	管理 VLAN (1 ギガビット)	[Server 4]	5	eth0
41	管理 VLAN (1 ギガビット)	サーバ 5	3	eth0
42	管理 VLAN (1 ギガビット)	サーバ 6	2	eth0
43	対応	対応	対応	対応
44	対応	対応	対応	対応
45	内部 VLAN (10 ギガビット)	リーフ 1 スイッチ	12	45
46	対応	対応	対応	対応
47	外部 VLAN (10 ギガビット)	顧客のルータ	対応	対応
48	対応	対応	対応	対応
49	内部 VLAN (40 ギガビット)	リーフ 1 スイッチ	12	49
50	内部 VLAN (40 ギガビット)	リーフ 1 スイッチ	12	50
51	対応	対応	対応	対応
52	対応	対応	対応	対応
53	対応	対応	対応	対応
54	対応	対応	対応	対応

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。