Cisco Catalyst IE3100H Heavy Duty シリーズ スイッチ ハードウェア設置ガイド

最終更新：2026 年 1 月 8 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.

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)

目 次

はじめに

対象読者

このガイドは、Cisco Catalyst IE3100H Heavy Duty シリーズスイッチの設置を担当するネットワーク技術者またはコンピュータ技術者を対象としています。このガイドを使用するには、LAN の概念および用語についての知識が必要です。

目的

各スイッチの物理特性およびパフォーマンス特性を紹介するとともに、スイッチの設置方法およびトラブルシューティングについて説明します。

その他の製品情報は次の場所にあります。

その他の資料については、次の場所にある Cisco Catalyst IE3100 Heavy Duty シリーズのマニュアルを参照してください。

Cisco IOS コマンドの詳細については、http://www.cisco.com/cisco/web/psa/configure.html?mode=prod&level0=268438303 を参照してください。

注目 この設置ガイドに記載された以外の方法で装置を使用すると、装置の保護機能が低下する可能性があります。

表記法

注釈、注意、および警告には、次の表記法および記号を使用しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 **ステートメント 1071 -** 警告の定義

安全上の重要な注意事項

装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。使用、設置、電源への接続を行う前にインストール手順を読んでください。各警告の冒頭に記載されているステートメント番号を基に、装置の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

この製品の安全上の警告は複数の言語に翻訳され、製品に付属の『*Regulatory Compliance and Safety Information for the Regulatory Compliance and Safety Information for the Cisco Catalyst IE3100H Heavy Duty Series Switches*』に記載されています。このガイドには、EMC 規制事項も記載されています。

関連資料

スイッチの設置、設定、またはアップグレードを行う前に、Cisco.com で提供されている製品リリース ノートで最新情報を確認してください。

www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html を参照してください。

通信、サービス、およびその他の情報

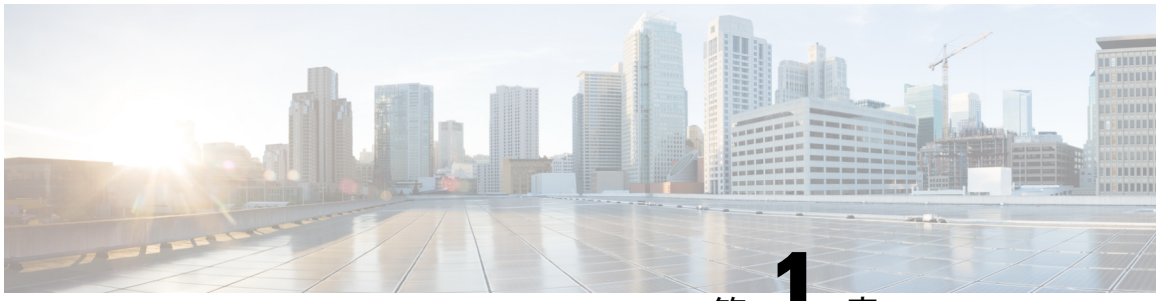
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービスリクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet [英語] にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

シスコのバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 1 章

製品概要

製品概要

Cisco Catalyst IE3100H Heavy Duty シリーズ スイッチ は、IP66/IP67 保護等級のコンパクト エントリレベルマネージドL2スイッチです。このスイッチは、8個のギガビットイーサネット（X コード）または 2 個のギガビットイーサネット（X コード）と、6 個のファストイーサネット（D コード）M12 インターフェイスモデルで使用可能な PLC レベル接続用の I/O ネットワークスイッチ専用に設計されています。これらのスイッチは、自動車製造、食品・飲料、クリーンルーム、または刺激の強い化学物質を扱い定期的にクリーニングする必要があるようなその他の環境などへの導入に対応し、24 時間 365 日の生産プロセスをサポートします。

このスイッチは密閉型装置であり、汚染度2の屋内または屋外環境下で、壁面に取り付けて、格納キャビネットなしで導入することができます。

スイッチ モデル

表 *1 : Cisco Catalyst IE3100H Heavy Duty* シリーズ スイッチ モデルの機能

ハードウェア仕様	IE-3100H-8T-E	IE-3100H-6FT2T-E
100 Mbps D コードポート	0	6
1 Gbps X コードポート	8	2
リムーバブルストレージ	SD カード[1]	
コンソール ポート	A コード M12 X1	
電源入力（標準定格）	12 ～ 48 VDC、1.5 A	

ハードウェア仕様	IE-3100H-8T-E	IE-3100H-6FT2T-E
電源コネクタ	L コード M12 X1	

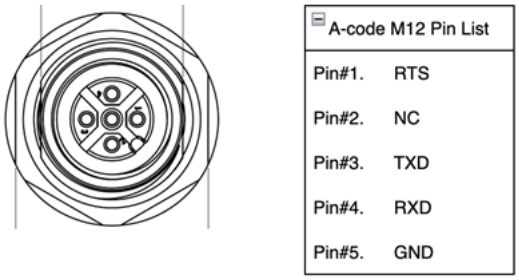
[1] SD カードはオプションで、デフォルトではスイッチに付属していません。

コンソール管理ポート

スイッチは、Microsoft Windows が実行されている PC またはターミナルサーバーに、A コード M12 コネクタコンソールポートを使用して接続し、CLI を使用して設定できます。コンソールポートのボー レートおよびフォーマット:

- 9600 ボー
- 8 データ ビット
- 1 ストップ ビット
- パリティなし
- なし（フロー制御）

図 *1:* コンソール コネクタ



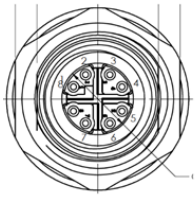
（注） 指定されたケーブルの場合は、シスコ製品 CAB-CONSOLE-M12= を使用してください

イーサネット ポート

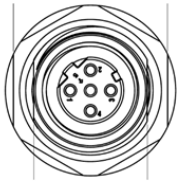
Catalyst IE-3100H-8T-E スイッチには、1000BASE-T、100BASE-TX、10BASE-T に対応した 8 個のイーサネットポートがあり、X コード M12 コネクタでの自動ネゴシエーション、自動 MDIX、およびケーブル診断をサポートします。

Catalyst IE-3100H-6FT2T-E スイッチには、2 個の 1Gigabit M12 X コードアップリンクイーサネットポートと、6 個の 10/100Mpbs M12 D コードダウンリンクイーサネットポートがあります。

図 *2 : M12* イーサネットポート



X-code M12 Pin List	
Pin#1.	MDI1_P
Pin#2.	MDI1_N
Pin#3.	MDI0_P
Pin#4.	MDI0_N
Pin#5.	MDI2_P
Pin#6.	MDI2_N
Pin#7.	MDI3_N
Pin#8.	MDI3_P



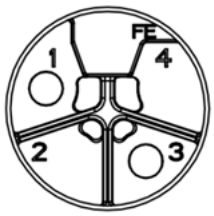
D-code M12 Pin List	
Pin#1.	TX+
Pin#2.	RX+
Pin#3.	TX-
Pin#4.	RX-

電源コネクタ

スイッチの DC 電源は、前面パネルのコネクタから供給します。パネルには電源コネクタのラベルがあります。電源接続は 10 インチポンドのトルクで締めます。

スイッチの電源には、Micro-Change（M12）シングルエンドコードセット、4 極、L コード、ジャック型の電源コードを使用する必要があります。

図 *3 :* 電源コネクタ



L-code M12 Pin List	
Pin#1.	DC+
Pin#2.	NC
Pin#3.	DC-
Pin#4.	NC

1	DC+	3	DC–
2	NC	4	NC

（注）

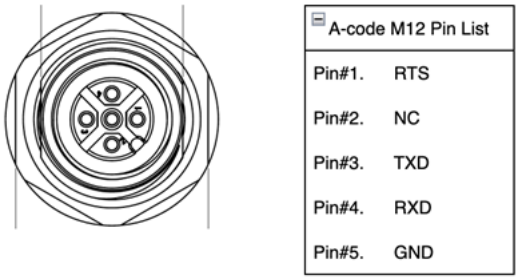
- UL 61010-2-201 の UL リスト要件を満たすには、Amphenol ADAD-DLFS0400152 コネクタを Cisco Catalyst IE3100H スイッチで使用する必要があります。
- CSA 61010-2-201 認定により、IE3100H では CSA/UL 認定の M12 L コードプラグ（ジャック）を使用できます

コンソール管理ポート

スイッチは、Microsoft Windows が実行されている PC またはターミナルサーバーに、A コード M12 コネクタコンソールポートを使用して接続し、CLI を使用して設定できます。コンソールポートのボー レートおよびフォーマット:

- 9600 ボー
- 8 データ ビット
- 1 ストップ ビット
- パリティなし
- なし（フロー制御）

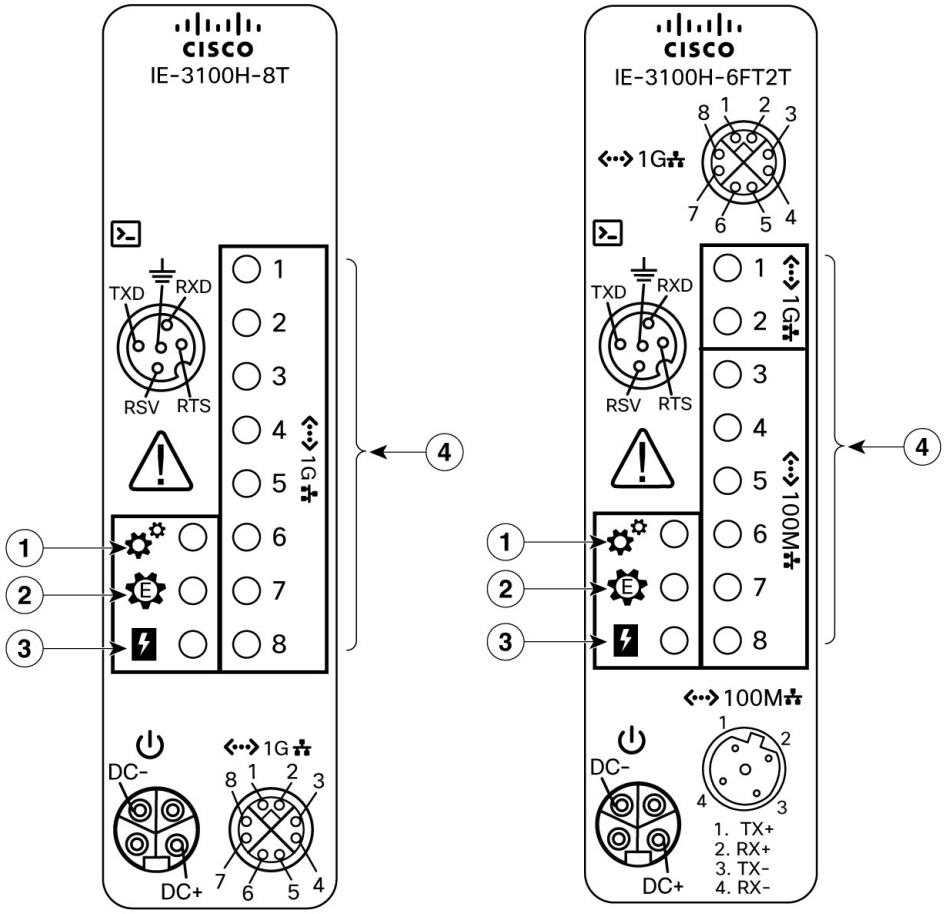
図 *4:* コンソール コネクタ



（注） 指定されたケーブルの場合は、シスコ製品 CAB-CONSOLE-M12= を使用してください

LED

LED は、システム全体、電源、およびイーサネットポートのステータスを表示します。



1	システム LED	3	電源 LED
2	Express Setup LED	4	イーサネットポートの LED

システム LED

システム LED は、デバイスに電力が供給され、正常に機能しているかどうかを示します。

表 *2 :* システム *LED*

色	ステータス
オフ	スイッチに電源が入っていません。
緑色の点滅	ブートファスト（電源投入時自己診断テスト）が進行中です。
緑色	スイッチは正常に動作しています。

色	ステータス
赤色	スイッチが正常に機能していません。

Express Setup ボタン

Express Setup は、新しいスイッチに初期 IP アドレス情報を設定する Web ベースの手順です。スイッチを管理し、ローカルルーターとインターネットの既存のネットワークに接続する簡単な方法を提供します。

Cisco Catalyst IE3100H Heavy Duty シリーズ スイッチの前面パネルには、Express Setup ボタンとセットアップ LED があります。ボタンは、偶発的な起動を防ぐために埋め込み型になっています。ボタンを押すには、ペーパークリップなどが必要です。ボタンを押す時間の長さを変えることによって、異なる Express Setup の機能をトリガーします。

表 *3 : Express* 設定モード

モード	モードの開始に必要な秒数	説明
短押し	1 ～ 5	スイッチを Express Setup モードにします
少し長めに押す	6 ～ 10	スイッチが、VLAN1 インターフェイスで DHCP 探索フェーズを開始するようにします
長押し	16 ～ 20	スイッチにスタートアップ設定を消去させ、リロードさせます。 これにより、スイッチは初期状態のデフォルト設定に戻ります。

初めてスイッチをセットアップする場合、Express Setup を使用して初期 IP 情報を入力することを推奨します。このプロセスによって、スイッチはローカルルータおよびインターネットに接続できるようになります。その後、その IP アドレスでスイッチにアクセスし、その他の設定を実行できるようになります。

詳細については、Express Setup の実行 （23 ページ）を参照してください。

表 *4 : Express Setup LED* のステータス

色	ステータス
消灯	システム稼働中
緑色の点滅	短押し
緑色と赤色の交互の点滅	少し長めに押す

色	ステータス
緑色の点滅（5 秒）、赤色の点滅（さらに 5 秒）、消灯（10 ～ 15 秒）、その後に緑色と赤色の点滅	長押し

電源ステータス LED

回路に電力が供給されている場合、LEDは緑色に点灯します。電力が供給されていない場合、LEDの色はアラーム設定によって異なります。アラームが設定されていれば、電力が供給されていない場合に LED は赤色に点灯しますが、それ以外の場合、LED は消灯します。

表 *5 :* 電源ステータス *LED*

色	システムステータス
緑色	関連する回路に電力が供給され、システムが正常に動作しています。
消灯	回路に電力が供給されていません。またはシステムが起動していません。
赤色	関連する回路に電源が供給されていないこと、または電源入力が最小有効レベルを下回っていることを示すアラームが設定されています。

ブートファストシーケンス中の電源 LED の色と動作については、「LED」セクションを参照してください。

ポートステータス LED

10/100BASE-T または 10/100/1000BASE-T ポート（番号 1 ～ 8 で識別、モデルごとに異なる）には、ポートステータス LED があります。

表 *6 :* ポートステータス *LED*

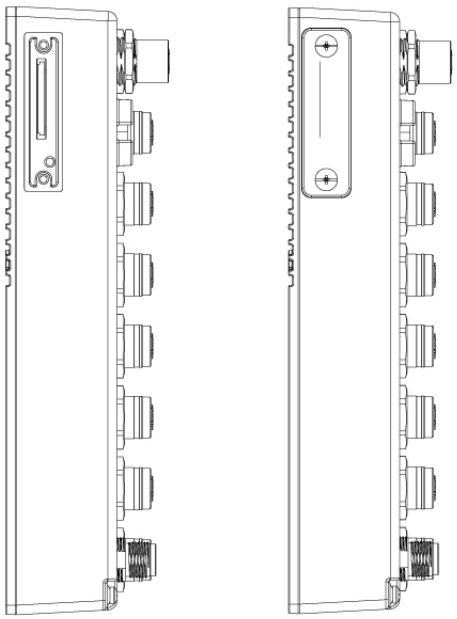
色	ステータス
消灯	リンクが確立されていません。
緑色の点灯	リンクが確立されています。アクティビティなし。
緑色の点滅	ポートは、アクティブにデータを送信中または受信中です。
緑色と橙色の交互の点滅	リンク障害が発生しています。大量のコリジョン、CRCエラー、アライメント/ジャバーエラーなど、接続やスループットに影響を及ぼすエラーが観測されています。

橙色の点灯	ポートは転送していません。管理者、アドレス違反、またはSTPによって、ポートは無効にされました。 （注） ポートを再設定すると、STP がスイッチ ループの検出を実行します。その間、ポート LED は橙色に点灯します（最大 30 秒）。

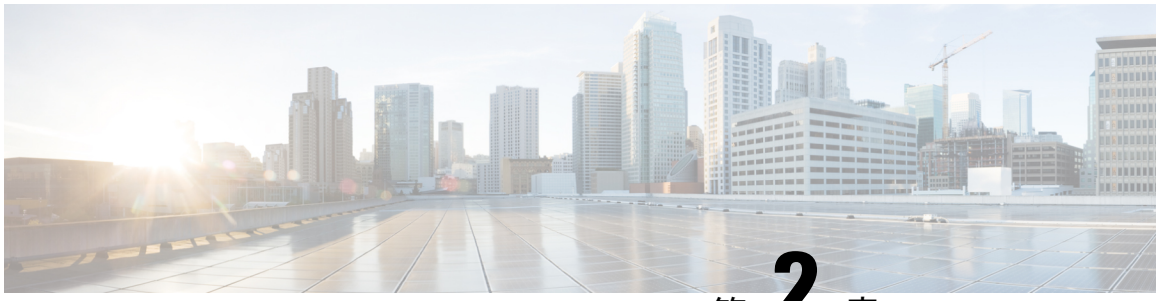
SD カードコネクタ

このスイッチは、SDカードをサポートしています。SDカードを使用することで、故障したスイッチを交換する際に交換用スイッチの設定を省けます。SD カードを使用して、システム内外にファイルをコピーすることもできます。

図 *5: SD* カードスロットとそのカバー



コネクタは、スイッチの側面の、SD カードを保護して所定の位置に保持するカバーの後ろにあります。このスイッチは、容量が最大 16 GB の SD カードをサポートします。



第 2 章

スイッチの設置

この章では、スイッチを設置し、ブートファストを確認し、他の装置にスイッチを接続する方法について説明します。

スイッチを永続的な場所に設置する前に、事前設定を実行することを推奨します。

インストールの準備

警告

これらの警告は、このスイッチの『Regulatory Compliance and Safety Information』の中で複数の言語に翻訳されています。

警告 **ステートメント 1003** - DC 電源の切断

感電や怪我のリスクを軽減するために、コンポーネントの取り外しや交換、またはアップグレードを実行する前に、DC 電源を切断してください。

警告 **ステートメント 1017** - 立ち入り制限区域

この装置は、出入りが制限された場所に設置されることを想定しています。熟練者、教育を受けた担当者、または資格保持者のみが立ち入り制限区域に入ることができます。

警告 **ステートメント 1033 -** 安全超低電圧（SELV）：IEC 60950/ES1–IEC 62368 DC 電源

感電のリスクを軽減するため、この装置は、IEC 60950 に基づく安全基準の SELV 要件または IEC 62368 に基づく安全基準の ES1 および PS1 要件に適合した DC 電源、またはクラス 2 電源に接続してください。

警告 **ステートメント 1074 -** 地域および国の電気規則への適合

感電または火災のリスクを軽減するため、機器は地域および国の電気規則に従って設置する必要があります。

警告 **ステートメント 1079 -** 高温表面

このアイコンは、高温表面の警告です。熱くなっている表面の近くで作業する場合は注意してください。

（注） **ステートメント 1089 -** 教育を受けた担当者および熟練者の定義

教育を受けた担当者とは、熟練者から教育やトレーニングを受け、機器を操作する際に必要な予防措置を講じられる人です。

熟練者または資格保持者とは、機器の技術に関するトレーニングを受けているか経験があり、機器を操作する際に潜む危険を理解している人です。

警告 **ステートメント 1091 -** 教育を受けた担当者による設置

この機器の設置、交換、または修理は、教育を受けた担当者または熟練者のみが実施できます。教育を受けた担当者または熟練者の定義については、「ステートメント 1089」を参照してください。

警告 **ステートメント 9001 -** 製品の廃棄

本製品の最終処分は、各国のすべての法律および規制に従って行ってください。

（注） **ステートメント 407 -** 日本語での安全上の注意

製品を使用する前に、安全上の注意事項を読むことを強くお勧めします。

https://www.cisco.com/web/JP/techdoc/pldoc/pldoc.html

製品を設置するときには、付属のまたは指定された接続ケーブル、電源コード、およびACアダプタを使用してください。

〈製品使用における安全上の注意〉

www.cisco.com/web/JP/techdoc/index.html

接続ケーブル、電源コードセット、ACアダプタ、バッテリなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外をご使用になると故障や動作不良、火災の原因となります。また、電源コードセットは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

注意 スイッチ周囲のエアーフローが妨げられないようにする必要があります。スイッチの過熱を防ぐため、次の最小スペースが必要です。– 上下：25 mm（1.0 インチ）– 左右：25 mm（1.0 インチ）– 正面：25 mm（1.0 インチ）

注意 IP66/IP67 およびタイプ 4 定格の環境で設置担当者がケーブル接続を提供する場合、ケーブルが IP66/IP67 およびタイプ 4 要件を満たす定格である必要があります

EU 内で設置される製品に関する EMC 環境条件

このセクションの記載は、EU 内で設置される製品に適用されます。

この装置は、EMC に関する次の環境条件の下で動作するように作られています。

- ユーザの管理下にある別の定義された場所。
- 接地およびボンディングは ETS 300 253 または CCITT K27 の要件に従うものとします。
- AC配電系統のタイプは、次のうち適用可能なもの1つとなっています：TN-S および TN-C（IEC 364-3 に定義）。

また、この装置を家庭環境で使用すると、干渉を引き起こす場合があります。

設置に関するガイドライン

スイッチの設置場所を決める際は、以下のガイドラインに従ってください。

環境およびラックに関する注意事項

設置作業を行う前に、次の環境およびラックの注意事項を参照してください。

- この装置は、IEC/CISPR パブリケーション 11 に従い、グループ 1、クラス A の工業設備と見なされます。適切な予防策を施さないと、伝導妨害や放射妨害により、別の環境での電磁適合性の確保が困難になる可能性があります。

⚠

注意 IP67 準拠のため、装置を作動状態にする前に、SD カード カバーのすべてのケーブル、ダストキャップ、非脱落型ネジが、推奨仕様を満たすよう、しっかりと締め付けられていなければなりません。

⚠

注意 ダストキャップを取り外す際は、注意が必要です。締め付けすぎた状態のダストキャップがコネクタのOリングシールに付着している場合があります。ダストキャップを取り外したあともOリングが正しい位置にあることを確認し、次に記載されたすべてのトルク仕様に従ってください。

一般的な注意事項

設置作業を行う前に、次の全般的な注意事項に従ってください。

⚠

注意 シスコ機器を扱う際には、必ず静電気防止対策を行ってください。設置およびメンテナンスの担当者は、スイッチの静電破壊のリスクを回避するために、アース ストラップを使用して適切に接地する必要があります。コンポーネントの基板上のコネクタやピンには触れないでください。スイッチ内部の回路コンポーネントに触れないように注意してください。装置を使用しないときは、静電気防止策が講じられた適切な梱包で装置を保管してください。

- 安全に関連するプログラマブル電子システム（PES）のアプリケーションを担当する場合は、システムのアプリケーションの安全要件に留意し、システムを使用するためのトレーニングを受ける必要があります。

スイッチの設置場所を決める際は、以下のガイドラインに従ってください。

- スイッチを設置する前に、まず電源を入れてブートファストを実行して、スイッチが動作可能であることを確認します。
- 10/100 ポートおよび 10/100/1000 ポートの場合、スイッチから接続先装置までのケーブル長が 328 フィート（100 m）を超えないこと。
- 動作環境が付録 F「技術仕様」に示されている範囲内にあること。
- 前面パネルおよび背面パネルに対しては、次の条件を満たすようにスペースを確保してください。

- 前面パネルの LED が見やすい。
- ポートに無理なくケーブルを接続できる。
- 前面パネルの DC 電源コネクタが、DC 電源に接続可能な距離にあること。

- スイッチ周囲のエアーフローが妨げられないようにする必要があります。スイッチの過熱を防止するには、少なくとも次のスペースを設ける必要があります。
  - 上下：25 mm（1.0 インチ）
  - 左右：25 mm（1.0 インチ）
  - 前面：25 mm（1.0 インチ）
- 周囲の温度が 60 °C（140 °F）を超えないこと。
- ケーブルが無線機、電力線、蛍光灯などの電気ノイズ源から離れていること。

梱包内容の確認

箱には、スイッチ本体とその設置マニュアルが入っています。不足または破損しているアイテムがある場合には、シスコの担当者か購入された代理店に連絡してください。

工具と機材

次の工具と機材を用意します。

- 保護接地コネクタとして使用するスタッド サイズ 6 の丸端子（Hollingsworth 製品番号 R3456B または同等のもの） を 1 個または 2 個一組。
- 圧着工具（Thomas & Bett 部品番号 WT2000、ERG-2001 または同等品）。
- 10 ゲージの銅製アース線。
- DC 電源接続用の UL および CSA 定格、1007 または 1569 型ツイストペア銅機器配線用電線（AWM）。
- 10、16、および 18 ゲージの導線の被覆を剥がすためのワイヤ ストリッパ
- No. 2 プラス ドライバ。
- マイナス ドライバ。
- トルク ドライバ（Torqueleader TT500 または同等品）

メモリカードの取り付けまたは取り外し（オプション）

スイッチは、ホットスワップ対応 SD メモリカードファームウェアをサポートしており、スタートアップ コンフィギュレーションが保存されます。それにより、交換用スイッチを再設定せずに、故障したスイッチと置き換えることができます。

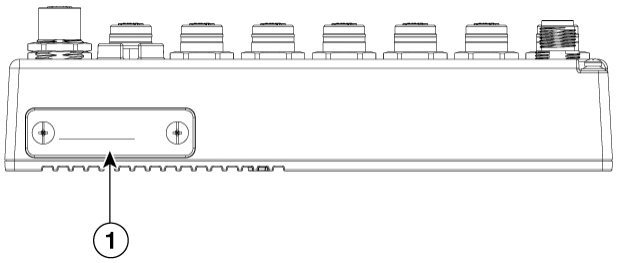
SD メモリカードカバーは、カードを固定することによって衝撃および振動からフラッシュカードを保護します。カバーにはストラップが付いており、非脱落型ネジでしっかり止められています。SD メモリカードのスロットは、スイッチの側面にあります。

（注） このスイッチは、容量が最大 16 GB の SD カードをサポートします。

SD メモリカードの取り付けまたは交換を行うには、次の手順に従ってください。

手順

ステップ 1 スイッチの側面にある非脱落型ネジを、シャーシから離れるまで緩めます。次の図を参照してください。



1	SD カードスロットカバー（非脱落型ネジ付き）（X2）

ステップ 2 カードの取り付けまたは取り外しを行うには、次の手順に従います。

- カードを押して離すと、カードが飛び出すので、取り外すことができます。それを静電気防止用袋に入れて、静電放電から保護します。
- カードを取り付けるには、スロット内をスライドさせ、カチッという音がするまで押し込みます。カードには誤った向きに挿入しないための切り欠きが付いています。

ステップ 3 保護ドアを閉じ、IP67 準拠を維持するため、3.5 ～ 4.5 インチポンド（0.40 ～ 0.51 Nm）で非脱落型ネジを締めます。

コンソール ポートへの PC または端末の接続

デバイスを設定するには、コンソール ポートに端末または PC を接続し、CLI により Cisco IOS コマンドを入力します。ここでは、PC をコンソールポートに接続し、PuTTy や HyperTerminal などの端末エミュレータ アプリケーションを使用してデバイスを設定する手順について説明します。

手順

ステップ 1 コンソールケーブル（Cisco PID CAB-CONSOLE-M12=）を、PC の 9 ピンシリアルポートに接続します。ケーブルのもう一方の端をスイッチのコンソール ポートに接続します。

ステップ 2 PC または端末上でターミナル エミュレーション ソフトウェアを起動します。プログラム（その多くは、PuTTy や HyperTerminal などの PC アプリケーション）は、使用可能な PC または端末とスイッチの間で通信を行います。

ステップ 3 PC または端末のボー レートおよびキャラクタ フォーマットを、次に示すコンソール ポートの特性に合わせて設定します。

- 9600 ボー
- 8 データ ビット
- 1 ストップ ビット
- パリティなし
- なし（フロー制御）

ステップ 4 スイッチに電源を接続します。

ステップ 5 PC または端末には、ブートアップシーケンスのステータスが表示されます。スイッチは自動起動します。IOS XE ソフトウェアがブートアッププロセスを完了すると、「Press RETURN to get started!」という言葉が表示されます。

（注）
プラグアンドプレイ（PNP）エージェントを使用して Day 1 インストールを自動化する場合は、Return を押さないでください。押すと、PNP の自動インストールが停止します。CLI を使用して Day 1 インストールプロセスを完了するには、Return のみを押します。

電源への接続

デバイスの電源を提供する必要があります。入力電圧は 9.6 ～ 60 Vdc の範囲内にする必要があります

カスタム電源を使用している場合は、ピグテール端子の電源ケーブルを使用します。電源ケーブルの M12 L コードジャック側をスイッチの電源コネクタに（トルク：0.60 Nm/5.3 インチポンドで）接続し、バラ線側を非標準電源に接続します。

スイッチの接地

設置場所の接地要件に従ってください。

警告 **ステートメント 2004 -** アース線機器

この装置は、放射およびイミュニティに関する要件に準拠するようにアースされていることが前提になっています。通常の使用時には、必ずスイッチのアース ラグがアースされているようにしてください。

（注） アース ラグはスイッチに同梱されていません。シングル丸端子ラグを使用します。

アース ネジを使用してスイッチを接地するには、次の手順に従います。

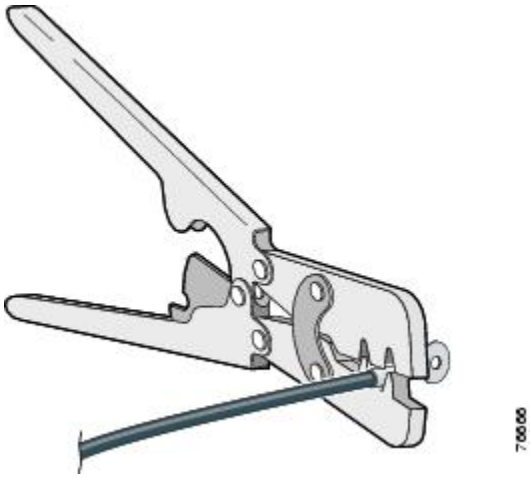
手順

ステップ 1 標準のプラス ドライバまたはラチェット式ドライバを使用して、スイッチからアース ネジを取り外します。後で使用できるようにアース ネジを保管しておきます。

ステップ 2 メーカーの注意事項に従い、ケーブルの被覆をはがす長さを決めます。

ステップ 3 丸端子ラグにアース線を挿入し、圧着工具を使用して端子を線に圧着します。

図 *6:* 丸端子の圧着



ステップ 4 端子の穴にアース ネジを通します。

ステップ 5 アース ネジ差し込み口にアース ネジを差し込みます。

ステップ 6 ラチェット トルク ドライバを使用して、スイッチの前面パネルにアース ネジと丸端子を 3.5 インチポンド（0.4 N-m）で締め付けます。トルクは 3.5 インチポンド（0.4 Nm）を超えないようにしてください。

ステップ 7 アース線のもう一方の端をアース バス、接地された DIN レール、接地されたベア ラックなどの接地されたむき出しの金属面に取り付けます。

アース線の接続

手順

ステップ 1 電源をアースに接続するのに十分な長さになるように、より銅線の単一の長さを計測します。配線色は、使用する国によって異なる場合があります。

（注）
電源からアースへの接続の場合、10 ～ 12 AWG より銅線を使用します。

ステップ 2 より銅線のもう一方の端をアース バス、接地された DIN レール、接地されたベア ラックなどの接地されたむき出しの金属面に取り付けます。

導線の反対側の端を電源の接地ネジに接続します。コネクタからは絶縁体に覆われた導線だけが出ているようにする必要があります。

（注）
スイッチ モデルによって、電源の位置が異なる可能性があります。

ステップ 3 アース線の接続ネジを締めます。

（注）
8 インチポンドに締めます。10 インチポンドを超えないようにします。

宛先ポートの接続

ここでは、宛先ポートへの接続について説明します。

10/100 および 10/100/1000 ポートへの接続

10/100 および 10/100/1000 ポートは、接続先デバイスの速度で動作するように自動的に設定されます。接続先のポートが自動ネゴシエーションをサポートしていない場合は、速度およびデュプレックスのパラメータを明示的に設定できます。自動ネゴシエーション機能のない装置または手動で速度とデュプレックスのパラメータが設定されている装置に接続すると、パフォーマンスの低下やリンク障害が発生することがあります。

最大限のパフォーマンスを実現するためには、次のいずれかの方法でイーサネットポートを設定してください。

- 速度とデュプレックスの両方について、ポートに自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスに関するパラメータを設定します。

注意 静電破壊を防ぐために、基板およびコンポーネントの取り扱い手順を順守してください。

10BASE-T、100BASE-TX、1000BASE-T デバイスに接続するには、次の手順に従います。

手順

ステップ 1 ワークステーション、サーバー、ルータ、および Cisco IP Phone に接続する際は、ストレートケーブルを前面パネルの M12 コネクタに接続します（IP67 トルク：4.43 ～ 7.08 インチ/ポンドまたは 0.5 ～ 0.8 Nm）。

1000BASE-T 対応の装置に接続する場合は、カテゴリ 5 以上の 4 対のツイストペアケーブルを使用します。

Auto-MDIX 機能は、デフォルトで有効になっています。

ステップ 2 他のデバイスの M12 コネクタにケーブルの反対側を接続します。スイッチと接続先装置の両方でリンクが確立されると、ポート LED が点灯します。

スパニングツリープロトコル（STP）がトポロジを検出し、ループの有無を確認している間、LED は橙色に点灯します。このプロセスには 30 秒ほどかかり、その後ポート LED は緑色に点灯します。ポート LED が点灯しない場合は、次のことを確認します。

- 接続先装置の電源がオンになっていない場合があります。
- ケーブルに問題があるか、または接続先装置に取り付けられたアダプタに問題がある可能性があります。ケーブル接続に関する問題の解決方法については、第4章「トラブルシューティング」を参照してください。

ステップ 3 必要に応じて、接続先装置を再設定してから再起動します。

ステップ 4 ステップ 1 ～ 3 を繰り返して、各装置を接続します。

次の作業

デフォルト設定で十分な場合は、これ以上のスイッチの設定作業は必要ありません。デフォルト設定は、次のいずれかの管理オプションを使用して変更できます。

- WebUI

個々のスイッチを管理および監視するには、WebUI の Web インターフェイスを使用できます。Device Manager には、スイッチの管理 IP アドレスを使用することによって、ネットワークのどこからでも Web ブラウザでアクセスできます。詳細については、Device Manager のオンライン ヘルプを参照してください。

- Cisco IOS-XE CLI

  スイッチ CLI は、スイッチを設定および監視するために使用できるバージョンの Cisco iOS ファームウェアです。CLI には、スイッチのコンソール ポートに直接管理ステーションを接続するか、リモート管理ステーションから Telnet を使用してアクセスできます。

- Cisco Catalyst Center は次の場所にあります：https://www.cisco.com/site/us/en/products/networking/catalyst-center/index.html

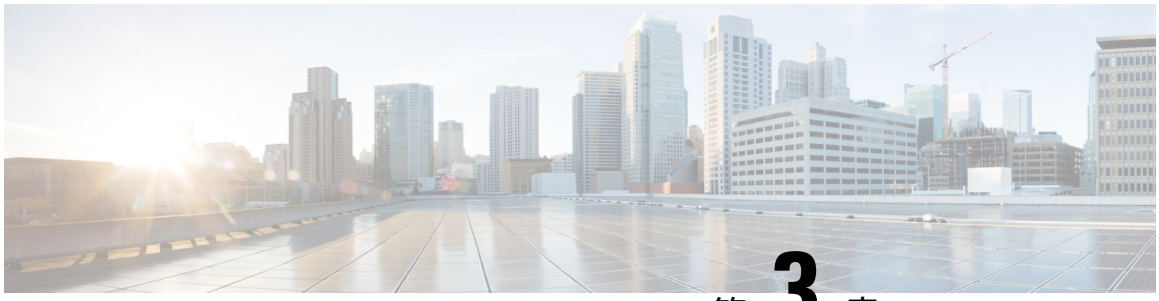
- SNMP

  スイッチは、HP OpenView や SunNet Manager などのプラットフォームで実行されている SNMP 互換管理ステーションを使用して管理できます。スイッチは、管理情報ベース（MIB）拡張機能の包括的なセットと 4 つの Remote Monitoring（RMON）グループをサポートしています。

- Common Industrial Protocol

  Common Industrial Protocol（CIP）管理オブジェクトは、スイッチによってサポートされ、1 つのツールにより工業オートメーション システム全体を管理できるようにします。

次の作業



第 3 章

スイッチの取り付け

スイッチの取り付け

この章では、スイッチの設置方法について説明します。

スイッチの設置

注意 スイッチの過熱を防ぐため、次の最小スペースが必要です。– 上下：25 mm（1.0 インチ）– 露出側（モジュールに接続されていない面）：25 mm（1.0 インチ）– 正面：25 mm（1.0 インチ）

壁面へのスイッチの取り付け

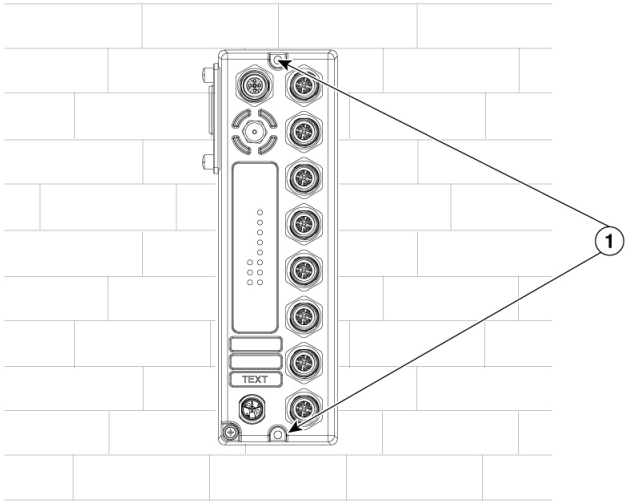
警告 **ステートメント 1094 -** 設置前に壁面への取り付けに関する説明を読む

設置を開始する前に、壁面への取り付けに関する説明を注意してお読みください。正しいハードウェアを使用しなかったり、正しい手順に従わなかったりすると、人体が危険にさらされたり、システムが損傷する場合があります。

手順

ステップ 1 スイッチを壁面またはパネルの目的の場所に配置します。次の図を参照してください。プラスネジでデバイスを壁面に取り付けます。

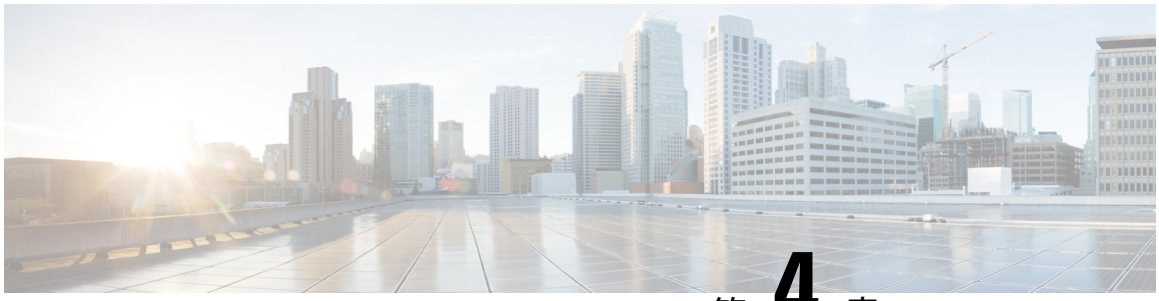
図 *7:* 壁面ブラケットの壁への取り付け



1	壁面取り付け穴

（注）
デバイスを壁面またはパネルに取り付けるときは、スイッチの重量を支えることができるスタッドまたは支持構造にネジがかみ合っていることを確認してください。

ステップ 2 スイッチを壁面またはパネルに取り付けた後、電源ケーブルとイーサネットケーブルを接続します。



第 4 章

Express Setup

Express Setup の実行

Express Setup を使用して、初期 IP 管理情報を入力します。その後、ブラウザにスイッチの IP アドレスを指定することで、スイッチの WebUI にアクセスして、Day 1 の設定を完了することができます。

スイッチを設定するには以下の機材が必要です。

- Windows または Mac を実行しているコンピューター。
- JavaScript が有効な Web ブラウザ。

  Google Chrome 38 以降、Mozilla Firefox 35 以降、または Apple Safari 7 以降。
- カテゴリ 5 または 6 のストレートケーブルまたはクロスケーブル
- ボタンに届く小さなペーパークリップ。

（注） 一方の端が RJ45 で、他方の端が M12 X コード（Catalyst IE-3100H-8T-E の場合）、または D コード、X コード（Catalyst IE-3100H-6FT2T-E の場合）のケーブルがそれぞれ必要です。

（注） Express Setup の実行前に、ブラウザのポップアップ ブロッカやプロキシ設定、および PC で実行しているワイヤレス クライアントを無効にします。

Express Setup を実行する方法

手順

ステップ 1 スイッチに何も接続されていないこと、および SD カードのカバーが取り外されていることを確認します。

Express Setup の実行中、スイッチは DHCP サーバとして動作します。PC に固定 IP アドレスが設定されている場合は、次の手順に進む前に、PC の固定 IP アドレスをメモし、PC の設定を変更して DHCP を使用するように一時的に設定します。

ステップ 2 スイッチに電源を接続します。

ブートシーケンスが開始されます。このプロセスには最大 90 秒かかります。ブート ファスト中は、SYS LED が緑色に点滅します。他の LED は緑色に点灯したままになります。ブートファストが完了すると、SYS LED が緑色に点灯し、Express Setup LED が緑色に点滅し始めます。

SYS LED が点灯しない場合（システムの電源が未投入）、緑色に点滅し続ける場合（POST が進行中）、または赤色に点灯する場合（障害が発生）は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

ステップ 3 Express Setup ボタンを 2 ～ 3 秒間押します。これは、パネルの後ろにあるくぼんだボタンです。ペーパー クリップなどの簡単な道具を使用できます。

Express Setup ボタンを押すと、スイッチポート 1/1 が緑色に点滅し始めます。

ステップ 4 スイッチを PC のイーサネットポートに接続します。

スイッチの接続を設定している間は、PC とスイッチのポート LED が緑色に点滅します。ポート LED が緑色のままの場合は、接続に成功したことを示しています。

約 30 秒経過してもポート LED が緑色にならない場合は、次を確認してください。

- 使用しているケーブルが破損していないこと。
- 他のデバイスがオンになっていること。

ステップ 5 PC 上でブラウザ セッションを開始します。

ブラウザの URL バーに IP アドレス 192.168.1.254 を入力します。セキュリティ警告が表示された場合は、クリックしてリスクを受け入れ、続行します。ログイン プロンプトが表示されます。

ステップ 6 [ユーザ名（Username）] と [パスワード（Password）] を入力します。

ユーザー名は「admin」、パスワードはスイッチ側面の SD カードカバーの横にあるシステム シリアル番号です。

また、コンソール経由で接続している場合は、ブートログでシステムのシリアル番号を確認できます。

[Configuration Setup Wizard Setup] Web ページが表示されます。

（注）

セットアップの Web ページが表示されない場合は、ブラウザのポップアップブロッカやプロキシ設定をすべて無効にし、PC のワイヤレスクライアントがオフになっていることを確認してください。

ステップ 7 4 つの Web ページの最初のページが表示されます。Express Setup を完了するには、4 つの Web ページすべてを順次移動する必要があります。[Account Settings] ページで、「*」が付いているすべてのフィールドに値を指定します。

- [Login Name] にログイン名を入力します。
- [Command Line Password] は、ドロップダウンメニューから [Command Line Password] に設定する必要があります。
- [Date & Time] は、オプションでドロップダウンメニューから [NTP Time] に設定します。

ステップ 8 設定が正しい場合は、[Basic Settings] をクリックします。

[Basic Settings] ウィンドウが表示されます。

- IP アドレスを入力します。（このフィールドは必須です）。
- SSH：有効化ボックスをクリックします。
- （すべての必須フィールドに対処するには、右側のスクロールバーを使用して下にスクロールします）

ステップ 9 [Switch Wide Settings] をクリックします。

[Switch Wide Settings] ウィンドウが表示されます（このページには必須フィールドはありません）。

ステップ 10 [Summary] をクリックします。

[Summary] ウィンドウが表示されます。

ステップ 11 要約に表示される情報が正しいことを確認し、準備ができたら [Submit] をクリックします。

エラーが発生した場合は、次の手順を実行します。

- 接続の確認：
  - コマンドプロンプトを開き、ping 192.168.1.254 と入力すると、すべての応答が受信されるはずです。
  - スイッチから PC を抜かないでください
- エラーが発生した場合、または IE スイッチを製造デフォルトに戻す場合：
  - IE スイッチを工場出荷時のデフォルトに戻すには、ペーパークリップ（または同等のもの）を Express Setup のくぼみに 15 ～ 20 秒間挿入します。Express Setup LED を確認し、赤色と緑色に交互に点滅したらペーパークリップを離します。

- 15 秒後にペーパークリップを離すと、IE スイッチが自動リロードします。
- 再起動後、IE スイッチは工場出荷時のデフォルトになります。約 120 秒待ちます。
- Express Setup LED が緑色に点滅したら、Express Setup 手順を再開します。

（注） Express Setup を長押しすると（ボタンを 15 秒間押すと、スイッチがリセットされ、工場出荷時のデフォルト設定が使用されます）、フラッシュおよびリムーバブルメディア（SD カード）から設定（nvram_config および vlan.dat）が削除されます。SD カードからファイルを削除したくない場合は、リムーバブルメディアを取り外します。

- リセット手順
- 画面の命名と [Power] ページの命名
- PC を切断し、もう一度やり直す

次のタスク

WebUI または CLI を使用してスイッチを管理できるようになりました。

WebUI の起動

次の手順で WebUI を表示します。

手順

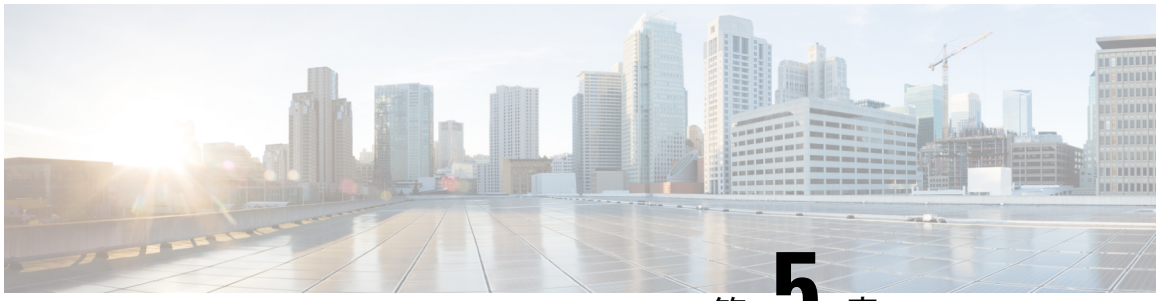
ステップ 1 PC またはラップトップ コンピュータで Web ブラウザを起動します。

ステップ 2 Web ブラウザでスイッチの IP アドレス、ユーザー名、およびパスワード（手順 8 で割り当て済み）を入力し、**Enter** を押します。WebUI ページが表示されます。

WebUI ページが表示されない場合：

- ネットワークに接続しているスイッチ ポートのポート LED が緑色になっていることを確認します。
- スイッチへのアクセスに使用している PC がネットワークに接続されていることを、ネットワーク内の既知の Web サーバに接続して確認します。ネットワークに接続していない場合は、PC でネットワーク設定のトラブルシューティングを実行してください。
- ブラウザで入力したスイッチの IP アドレスが正しいことを確認します。
- スイッチの IP アドレスと同じサブネット内の固定 IP アドレスを PC に設定します。

- PC やラップトップコンピュータに接続されているスイッチポートの LED が緑色の場合は、Web ブラウザにスイッチの IP アドレスを再入力し、WebUI を表示します。



第 5 章

CLI セットアップ プログラムによるスイッチの設定

初期設定情報の入力

この章では、スイッチのコマンドラインインターフェイス（CLI）ベースのセットアップ手順について説明します。

スイッチを設定するには、セットアッププログラムを完了する必要があります。セットアッププログラムは、スイッチの電源がオンになると自動的に実行されます。スイッチがローカルルータやインターネットと通信するのに必要な IP アドレスやその他の設定情報を割り当てる必要があります。この情報は、WebUI を使用してスイッチを設定および管理する場合にも必要です。

Cisco IOS XE 17.17.1 以降では、ユーザーのパスワードがプレーンテキストで保存されないように、パスワード暗号化レベルを設定することができます。ブートストラップファイルの生成については、 を指す DNS 名を設定します。

スイッチを電源に接続する前に、「警告」を参照して安全に関する注意事項を確認してください。

スイッチのコンソール ポートに PC を接続するには、コンソール ポートへの PC または端末の接続 （15 ページ）を参照してください。

IP とパスワードの設定

セットアッププログラムを完了するには、ネットワーク管理者から次の情報を入手しておく必要があります。

- 暗号化レベルとマスター鍵（Cisco IOS XE 17.17.1 以降）
- スイッチの IP アドレス

- サブネットマスク（IP ネットマスク）
- デフォルト ゲートウェイ（ルータ）
- イネーブル シークレット パスワード
- イネーブル パスワード
- SSH パスワード

システムのセキュリティ設定

セキュリティを強化するには、パスワードなどの機密情報を暗号化する必要があります。設定ダイアログには、パスワード暗号化レベルを設定できる [System Security Configuration Dialog] が含まれています。暗号化レベルには、タイプ 6 およびタイプ 7 の暗号化が含まれます。両方のタイプを有効にすることをお勧めします。

- タイプ 6 は、パスワードの暗号化に Advanced Encryption Standard（AES）を使用します。タイプ 6 パスワードの暗号化と暗号解読は、入力するマスター鍵と結合されます。マスター鍵はリカバリできないため、記憶しておく必要があります。
- マスター鍵は、AES 対称暗号を使用してスイッチ設定内の他のすべての鍵を暗号化するために使用されるパスワード/鍵です。マスター鍵はスイッチ設定には保存されず、スイッチに接続したとしてもどのような方法でも表示も取得もできません。設定されると、マスター鍵を使用して、スイッチ設定内の既存または新しい鍵が暗号化されます。**password encryption aes** コマンドを実行するまで、鍵は暗号化されません。
- タイプ 7 パスワードは、元のプレーンテキストパスワードを難読化したものです。これはヴィジュネル暗号に基づいており、設定内の実際のパスワードが誰かに見られるのを防ぎます。

セットアッププログラムを使用して、新しいスイッチと設定済みのスイッチの両方でパスワード暗号化レベルを設定できます。新しいスイッチについては、初期設定 - タイプ 6 暗号化 （30 ページ） または 初期設定 - タイプ 7 暗号化 （34 ページ） を参照してください。初期セットアップを実行せずにシステムセキュリティ設定を設定するには、パスワード暗号化レベルの設定 （37 ページ） を参照してください。

初期設定 - タイプ 6 暗号化

タイプ 6 暗号化とセットアッププログラムを使用して、スイッチの初期設定を行う手順は次のとおりです。

手順

ステップ 1 次のプロンプトで **Yes** を入力します。

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

ステップ 2 プロンプトで、適用するパスワード暗号化レベルを入力します。

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered


 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

（注）
Cisco IOS XE 17.17.1 では、タイプ 6 とタイプ 7 の両方の暗号化 [0] を選択すると、ユーザー名のみがタイプ 6 に自動的に変換され、イネーブルパスワードと回線 vty パスワードはタイプ 6 ではなくタイプ 7 に自動的に変換されます。

ステップ 3 スイッチの他のすべての鍵の暗号化に使用するマスター鍵を入力します。

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
 #, ;' : ************
```

ステップ 4 マスター鍵をもう一度入力して確定します。

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

（注）
このデバイスを交換する場合に必要になるため、マスター鍵は保存しておく必要があります。

ステップ 5 プロンプトで **2** を入力して、システムセキュリティ設定を保存します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

ステップ 6 プロンプトで **yes** と入力して、基本管理設定を設定します。

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

ステップ 7 スイッチのホスト名を入力します。

```
Enter host name [Switch]: Switch123
```

ステップ 8 イネーブル シークレット パスワードを入力します。

```
The enable secret is a password used to protect
 access to privileged EXEC and configuration modes.
 This password, after entered, becomes encrypted in
 the configuration.
 ------------------------------------------------
 secret should be of minimum 10 characters and maximum 32 characters with
 at least 1 upper case, 1 lower case, 1 digit and
 should not contain [cisco]
 ------------------------------------------------
 Enter enable secret: **********
```

ステップ 9 イネーブル シークレット パスワードをもう一度入力して確定します。

```
Confirm enable secret: **********
```

ステップ 10 イネーブルパスワードを入力します。

```
The enable password is used when you do not specify an
 enable secret password, with some older software versions, and
 some boot images.
 Enter enable password: ********
```

ステップ 11 仮想端末のパスワードを入力します。

このパスワードは 1 ～ 25 文字の英数字で指定できます。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。

```
 The virtual terminal password is used to protect
 access to the router over a network interface.
 Enter virtual terminal password: ********
```

ステップ 12 管理ネットワークに接続するインターフェイスのインターフェイス名（物理的なインターフェイスまたは VLAN（仮想 LAN）の名前）を入力します。このリリースでは、インターフェイス名には必ず **vlan1** を使用します。

（注）
スイッチは、**vlan1** インターフェイス上で DHCP 検出メッセージを送信します。CLI の初期セットアッププロセスが開始される前にスイッチがネットワークに接続されている場合は、インターフェイスにダイナミック IP アドレスが割り当てられている可能性があります。**vlan1** インターフェイスに IP アドレスが表示されていなくても問題ありません。このプロセスでは、動的に割り当てられた IP アドレスを上書きする管理用の静的 IP アドレスを設定できます。

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

ステップ 13 設定を保存するには、**2** と入力します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

次のタスク

セットアップ プログラムが完了すると、スイッチは作成されたデフォルト設定を実行できます。次のいずれかの方法を用いて、この設定の変更や他の管理タスクを実行できます。

- コマンドライン インターフェイス（CLI）
- Web ユーザインターフェイス（WebUI）

CLI を使用するには、端末エミュレーションプログラムを使用してコンソールポートから、または Telnet を使用してネットワークから、*Switch* > プロンプトにコマンドを入力します。設定情報については、次を参照してください

WebUI を使用するには、WebUI のオンライン ヘルプを参照してください。

初期設定 - タイプ 7 暗号化

タイプ 7 暗号化のみとセットアッププログラムを使用して、スイッチの初期設定を行う手順は次のとおりです。

始める前に

コンソール ポートへの PC または端末の接続 （15 ページ） の説明に従って CLI にアクセスします。

手順

ステップ 1 次のプロンプトで **Yes** を入力します。

```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

ステップ 2 プロンプトで **1** を入力して、タイプ 7 パスワード暗号化のみを適用します。

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered


 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 1
```

ステップ 3 プロンプトで **2** を入力して、システムセキュリティ構成を保存します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

```
Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

ステップ 4 プロンプトで **yes** と入力して、基本管理設定を設定します。

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

ステップ 5 スイッチのホスト名を入力します。

```
Enter host name [Switch]: Switch123
```

ステップ 6 イネーブル シークレット パスワードを入力します。

```
 The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
```

ステップ 7 イネーブル シークレット パスワードをもう一度入力して確定します。

```
 Confirm enable secret: **********
```

ステップ 8 イネーブルパスワードを入力します。

```
 The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********
```

ステップ 9 仮想端末のパスワードを入力します。

このパスワードは 1 ～ 25 文字の英数字で指定できます。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。

```
  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********
```

ステップ 10 管理ネットワークに接続するインターフェイスのインターフェイス名（物理的なインターフェイスまたは VLAN（仮想 LAN）の名前）を入力します。このリリースでは、インターフェイス名には必ず **vlan1** を使用します。

（注）
スイッチは、**vlan1** インターフェイス上で DHCP 検出メッセージを送信します。CLI の初期セットアッププロセスが開始される前にスイッチがネットワークに接続されている場合は、インターフェイスにダイナミック IP アドレスが割り当てられている可能性があります。**vlan1** インターフェイスに IP アドレスが表示されていなくても問題ありません。このプロセスでは、動的に割り当てられた IP アドレスを上書きする管理用の静的 IP アドレスを設定できます。

```
Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  10.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [10.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 10.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

ステップ 11 設定を保存するには、**2** と入力します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
```

```
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

次のタスク

セットアップ プログラムが完了すると、スイッチは作成されたデフォルト設定を実行できます。次のいずれかの方法を用いて、この設定の変更や他の管理タスクを実行できます。

- コマンドライン インターフェイス（CLI）
- Web ユーザインターフェイス（WebUI）

CLIを使用するには、端末エミュレーションプログラムを使用してコンソールポートから、またはTelnetを使用してネットワークから、*Switch*> プロンプトにコマンドを入力します。設定情報については、次を参照してください .

WebUI を使用するには、WebUI のオンライン ヘルプを参照してください。

パスワード暗号化レベルの設定

この手順に従って、初期セットアップを実行せずにシステムセキュリティ設定（タイプ6およびタイプ 7 暗号化）を設定します。

手順

ステップ 1 次のプロンプトで **No** を入力します。

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1

Would you like to enter the initial configuration dialog? [yes/no]: no
```

ステップ 2 プロンプトでイネーブルシークレットを入力します。

```
The enable secret is a password used to protect
access to privileged EXEC and configuration modes.
This password, after entered, becomes encrypted in
the configuration.
-------------------------------------------------
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-------------------------------------------------
Enter enable secret: **********
Confirm enable secret: **********
```

```
The following configuration command script was created:

enable secret 9 $9$YMkVvPLbxKn4bE$OAOX/akBBsukkRV1L.Tk7p2KaM0BXLQI.HbyGbXB8/g
!
end
```

ステップ 3 **2** を入力して設定を保存し、システムセキュリティ設定に移動します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
```

ステップ 4 プロンプトで、適用するパスワード暗号化レベルを入力します。

```
  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered


 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0
```

ステップ 5 スイッチの他のすべての鍵の暗号化に使用するマスター鍵を入力します。

```
Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
 #, ;' : ************
```

ステップ 6 マスター鍵をもう一度入力して確定します。

```
Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

（注）
このデバイスを交換する場合に必要になるため、マスター鍵は保存しておく必要があります。

ステップ 7 プロンプトで **2** を入力して、システムセキュリティ設定を保存します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
```

```
Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


Press RETURN to get started!


Switch>
```

CLI セットアップの例

初期設定の例

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered


 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
 #, ;' : ************

 Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
```

```
[OK]
Use the enabled mode 'configure' command to modify this configuration.


At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:
```

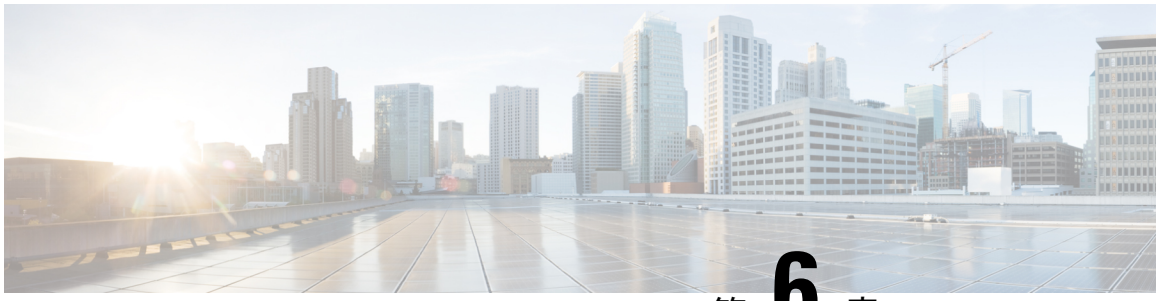
```
hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```

システムセキュリティ設定の例

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1   yes


  -----System Security Configuration Dialog-----

 Cisco recommends that for enchanced security users should encrypt sensitive info
 The configuration dialog will allow you to set encryption level
 It is recommended that both type-6 & type-7 encryption should be enabled by user
 For type-6 user will need to create and remember Master key as it cannot be recovered


 [0] for both type-6 & type-7 encryption to be applied on the box
 [1] for only type-7 encryption to be applied on the box
 [2] for no encryption to be applied on the box

 Enter your encryption selection [2]: 0

 Enter the Master key min 8 chars  & max 127 chars, Master key should not begin with '!,
 #, ;' : ************
```

```
 Confirm the master key: ************

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.


At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Switch]: Switch123

  The enable secret is a password used to protect
  access to privileged EXEC and configuration modes.
  This password, after entered, becomes encrypted in
  the configuration.
  ------------------------------------------------
  secret should be of minimum 10 characters and maximum 32 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  ------------------------------------------------
  Enter enable secret: **********
  Confirm enable secret: **********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: ********

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: ********

Current interface summary

Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  12.16.1.120     YES DHCP   up                    up
```

```
GigabitEthernet1/1     unassigned      YES unset  up                    up
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  up                    up
GigabitEthernet1/4     unassigned      YES unset  down                  down
GigabitEthernet1/5     unassigned      YES unset  down                  down
GigabitEthernet1/6     unassigned      YES unset  down                  down
GigabitEthernet1/7     unassigned      YES unset  up                    up
GigabitEthernet1/8     unassigned      YES unset  up                    up
GigabitEthernet1/9     unassigned      YES unset  down                  down
GigabitEthernet1/10    unassigned      YES unset  down                  down
AppGigabitEthernet1/1  unassigned      YES unset  up                    up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
    IP address for this interface [12.16.1.120]:
    Subnet mask for this interface [255.0.0.0] :
    Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVOk$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:  2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.



Press RETURN to get started!
```



第 6 章

トラブルシューティング

ケーブルの損傷、接続のゆるみなどの物理的な不具合、またはポート設定の誤りなどのソフトウェアの問題が原因で発生する接続の問題により、スイッチが誤作動する可能性があります。

物理的な接続の問題

ケーブルの損傷、接続のゆるみなどの物理的な不具合による接続の問題により、スイッチが正常に機能しない場合があります。

スイッチの LED は、問題の診断に役立ちます。これにより、ブート ファストの失敗、ポート接続の問題、およびスイッチ全体のパフォーマンスを把握できます。また、Device Manager、CLI、SNMP ワークステーションから統計情報を取得することもできます。

ポート LED が点灯していても、ケーブルが正常なことを示しているわけではありません。物理的な圧力がかかっている場合は、限界レベルで動作している可能性があります。ポート LED が点灯しない場合は、次のことを確認します。

- 接続にゆるみがないかどうかを確認します。完全に接続されているように見えても、そうでないことがあります。ケーブルをいったん外して、接続し直してください。
- ケーブルコネクタに破損または欠落したピンがないか確認します。
- 正しいケーブルタイプが使用されていることを確認します。
- 両方のデバイスの電源が投入されていることを確認します。
- ケーブルの両端が正しいポートに接続されていることを確認します。

- ケーブルをスイッチから外して、問題のない装置に接続します。

ソフトウェア設定の問題

10/100 および 10/100/1G ポートが異常を示している場合は、次のことを確認します。

- すべてのポートのステータスを確認します。LED とその意味については、「ポートステータス LED （7 ページ）」を参照してください。
- **show interfaces** 特権 EXEC コマンドを使用して、ポートが error-disabled、disabled、または shutdown の状態になっていないかどうかを確認します。必要に応じて、ポートを再度有効にします。

インターフェイスの設定

インターフェイスが無効になっていないか、電源がオフになっていないかを確認してください。リンクの片側でインターフェイスを手動でシャットダウンした場合は、そのインターフェイスが再度有効にされるまで復活しません。**show interfaces** 特権 EXEC コマンドを使用して、インターフェイスが errordisabled、disabled、または shutdown の状態になっていないかどうかを確認します。必要に応じて、インターフェイスを再度有効にします。

エンド デバイスへの ping

ping を使用して、最初は直接接続されているスイッチから始めて、接続できない原因となっている箇所を突き止めるまで、ポートごと、インターフェイスごと、トランクごとに段階的にさかのぼって調べます。各スイッチの連想メモリ（CAM）テーブル内に、エンド デバイスの MAC アドレスが存在していることを確認します。

スパニングツリーのループ

スパニングツリープロトコル（STP）にループが発生すると、重大な性能上の問題が引き起こされ、その状況がポートやインターフェイスの問題のように見えることがあります。

ループは、単方向リンクによって引き起こされることがあります。つまり、スイッチから送信されたトラフィックがネイバーで受信されるが、ネイバーからトラフィックを受信したという通知がスイッチで受信されない場合に発生します。破損したケーブル、その他のケーブル配線の問題、またはポートの問題によって、この単方向通信が引き起こされる可能性があります。

スイッチで単方向リンク検出（UDLD）を有効にすると、単方向リンク問題の特定に役立ちます。スイッチでの UDLD の有効化については、「UDLD について」（）を参照してください。Cisco.com で入手できます。

スイッチの性能

速度、デュプレックス、および自動ネゴシエーション

大量のアライメントエラー、フレームチェックシーケンス（FCS）、またはレイトコリジョンエラーを示すポート統計は、2台のデバイス間でデュプレックスと速度の設定に不一致がある場合によくある問題です。

スイッチの性能を最大限に引き出してリンクを保証するには、次のいずれかのガイドラインに従ってデュプレックスまたは速度の設定を変更してください。

- 両方のポートで、速度とデュプレックスの両方を自動ネゴシエーションします。
- 接続の両端でインターフェイスの速度とデュプレックスのパラメータを手動で設定します。
- リモートデバイスが自動ネゴシエートしない場合は、2つのポートのデュプレックス設定を同じにします。速度パラメータは、接続先ポートが自動ネゴシエーションを実行しない場合でも自動的に調整されます。

自動ネゴシエーションと NIC

スイッチとサードパーティ製ネットワークインターフェイスカード（NIC）間で問題が発生する場合があります。デフォルトで、スイッチポートとインターフェイスは自動ネゴシエートします。一般的にはラップトップコンピュータやその他の装置も自動ネゴシエーションに設定されていますが、それでも問題が発生することがあります。

自動ネゴシエーションの問題をトラブルシュートするには、速度とデュプレックスモードが接続の両側で同じになるように手動で設定してください。それでも問題が解決しない場合は、NIC 上のファームウェアまたはソフトウェアに問題がある可能性があります。その場合は、NIC ドライバを最新バージョンにアップグレードして問題を解決してください。

ケーブル接続の距離

ポート統計情報に、過剰な FCS、レイトコリジョン、またはアライメントエラーが示されている場合は、スイッチから接続先の装置までのケーブル長が推奨ガイドラインに従っていることを確認してください。

スイッチのリセット

スイッチをリセットすると、設定が削除されてスイッチが再起動されます。

工場出荷時のデフォルト設定にリセットする理由としては、次のことが考えられます。

- スイッチをネットワークに設置したが、不明な IP アドレスが割り当てられているため、スイッチに接続できない。

- スイッチのパスワードをリセットする必要がある。

注意 電源を入れる際にExpress Setupボタンを押した場合、自動ブート シーケンスは停止し、スイッチはブートローダ モードに入ります。

スイッチをリセットする方法

手順

ステップ 1 Express Setup ボタンを 15 秒以上押し続けます。スイッチがリブートします。システム LED が緑色に変わり、Express Setup LED が緑色に点滅し始めます。

ステップ 2 もう一度 [Express Setup] ボタンを 1 ～ 3 秒間押します。ポート 1/1 の LED が緑色に点滅します。

スイッチは、工場出荷時設定どおりに動作するようになります。上記のExpress Setupに関するセクションに移動して、再インストールを完了します。

セキュアデータワイプの有効化

セキュアデータワイプは、すべての IOS XE ベースのプラットフォーム上のストレージデバイスが NIST SP 800-88r1 準拠の安全な消去コマンドを使用して適切に消去されるようにするためのシスコ全体のイニシアチブです。

この機能は、すべてのライセンスレベルの次の IoT スイッチで Cisco IOS XE 17.17.1 以降でサポートされています。

- IE3100H

セキュアデータワイプが有効になっている場合、内部フラッシュメモリ内のすべてが消去されます。これには次が含まれます。

- ユーザー設定とパスワード
- Cisco IOS XE イメージ
- Embedded MultiMediaCard（eMMC）
- rommon 変数
- ACT2 セキュアストレージ

（注） 安全な消去では、SD カードまたは USB デバイスの内容は消去されません。外部ストレージデバイスは手動で消去または再フォーマットする必要があります。

コマンドの実行後、スイッチは工場出荷時のデフォルト設定（ボーレート 9600）で rommon プロンプトになります。内部フラッシュメモリは、IOS イメージが再起動されるまでフォーマットされません。

（注） 有効なイメージの入った sdflash/usbflash が挿入されている場合、デバイスは起動の優先順位に基づいて外部メディア内のイメージで起動します。イメージを含む外部メディアがデバイスに挿入されていない場合にのみ、デバイスは rommon になります。

セキュアデータワイプの実行

セキュアデータワイプを有効にするには、次の例に示すように、特権 EXEC モードで **factory-reset all secure** コマンドを入力します。

```
Switch#factory-reset ?
  all                 All factory reset operations
  keep-licensing-info  Keep license usage info
Switch#factory-reset all ?
secure  Securely reset all
Switch#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure?
[confirm]Y
```

factory-reset コマンドオプション：

- **factory-reset all**：フラッシュからすべてを削除します。
- **factory-reset keep-licensing-info**：工場出荷時状態へのリセット後もライセンス情報を保持し、他のすべてをフラッシュから削除します。
- **factory-reset all secure**：フラッシュからすべてを削除し、マウントを解除してパーティションをサニタイズしてからマウントし直します。これにより、これらのパーティションのデータを回復できないようにします。

重要 **factory-reset all secure** 操作には時間がかかる場合があります。電源を入れ直さないでください。

スイッチがコマンドを実行した後にログを確認するには、IOS XE を起動し、次の **show** コマンドを入力します。

```
Switch#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IE3100h
Purge ACT2 chip at 12-08-2024, 15:17:28
ACT2 chip Purge done at 12-08-2024, 15:17:29
```

```
mtd and backup flash wipe start at 12-08-2024, 15:17:29
mtd and backup flash wipe done at 12-08-2024, 15:17:29.
```

パスワードの回復方法

システム管理者は、パスワード回復機能を有効または無効にできます。パスワード回復機能を無効にした場合、紛失したパスワードや忘れたパスワードを回復するには、スイッチの設定を完全にクリアする以外に方法がありません。この手順については、スイッチのリセット （47 ページ）を参照してください。

Express Setup のトラブルシューティング

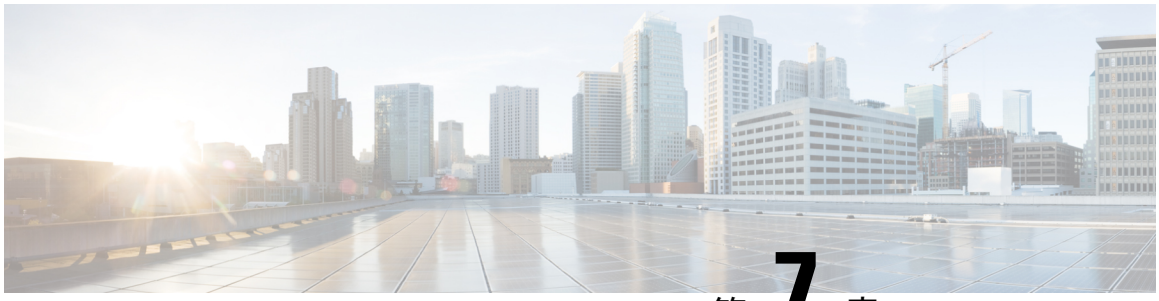
ここでは、スイッチの初期設定に関するトラブルシューティングのヒントを示します。

チェックリスト	推奨事項
Express Setup ボタンを押したとき、SETUP LED が点滅しましたか？	点滅しなかった場合、または不明な場合には、スイッチを再起動します。Express Setup ボタンを押したとき、SETUP LED が点滅することを確認してください。
PC を間違ったスイッチ ポートに接続していませんか？	LED が点滅しているスイッチ ポートに接続したかどうかを確認してください。
SETUP LED が緑色に点灯する前に、PC 上でブラウザ セッションを開始しましたか？	点灯前に開始している場合、または不明な場合には、スイッチを再起動して Express Setup の手順を繰り返します。
PC 上でブラウザ セッションを開始した際、設定ページが自動的に表示されましたか？	ウィンドウが表示されない場合には、*Cisco.com*、またはその他のよく知られているウェブサイトの URL をブラウザに入力してください。
スイッチ ポートに接続した時、PC 上でポップアップブロッカーを実行していませんでしたか？	実行していた場合は、ケーブルをスイッチ ポートから取り外してポップアップ ブロッカーを無効にし、Express Setup ボタンを押して点滅しているイーサネット ポートにケーブルを再接続します。
ブラウザ ソフトウェアのプロキシ設定を有効にしたまま、スイッチポートに接続しませんでしたか？	有効にしていた場合は、ケーブルをスイッチ ポートから取り外してプロキシ設定を無効にし、Express Setup ボタンを押して点滅しているイーサネット ポートにケーブルを再接続します。
PC 上でワイヤレス クライアントを実行したまま、スイッチポートに接続しませんでしたか？	実行していた場合は、ケーブルをスイッチ ポートから取り外してワイヤレス クライアントを無効にし、Express Setup ボタンを押して点滅しているイーサネット ポートにケーブルを再接続します。

チェックリスト	推奨事項
初期設定完了後、スイッチの IP アドレスを変更しようとしていますか？	**Configure > Express Setup** に移動し、[Device Manager] 画面でスイッチの IP アドレスを変更します。スイッチの IP アドレス変更の詳細については、Cisco.com で『Cisco IE 3100 Switch Software Configuration Guide』を参照してください。

スイッチのシリアル番号の確認

シスコの技術サポートに問い合わせを行う場合は、スイッチのシリアル番号を確認する必要があります。シリアル番号は、装置下部の準拠ラベル、または電源コネクタの横にある小さなラベルに記載されています。**show version** 特権 EXEC コマンドを使用して、スイッチのシリアル番号を取得することもできます。



第 7 章

技術仕様

技術仕様

表 7: 物理構成

物理仕様	IE-3100H-6FT2T-E	IE-3100H-8T-E
サイズ（高さ X 幅 X 奥行）	7.90 X 2.71 X 2.10 インチ 20.07 X 6.88 X 5.33 cm	7.90 X 2.71 X 2.10 インチ 20.07 X 6.88 X 5.33 cm
重量（取り付けられている付属のダストキャップを含む）	0.754 kg	0.738 kg
取り付け	壁面	壁面
環境条件		
保管温度	-40 ～ 85 °C（-40 ～ 185 °F）	

物理仕様	IE-3100H-6FT2T-E	IE-3100H-8T-E
動作温度 （ラック内、スイッチ底面より 2.54 cm（1 インチ）下で測定）	-40 °C ～ 75 °C（-40 ～ 167 °F） **注意** 60 °C を超える動作温度は、製品安全規格認定と承認の対象にはなりません。 • ファン冷却付きエンクロージャ動作時：-40 °C ～ 75 °C（-40 °F ～ 167 °F） • 開放型エンクロージャ動作時：-40 °C ～ 70°C（-40 °F ～ 158 °F）で、ユニットが 40 lfm 以上 • 密閉型エンクロージャ動作時：-40 °C ～ 60 °C（-40 °F ～ 140 °F） • 短期間の動作：85 °C（185 °F）で 16 時間	
湿度（動作時）	5 ～ 95 %（結露しないこと）	
IP 保護等級	IP66/IP67 保護等級の防塵および防水。 NEMA タイプ 4 **注意** すべての IP67 ケーブルを嵌合させ適切なトルクで締めるか、付属のダストキャップを取り付けた場合にのみ、IP66およびIP67、NEMA タイプ 4 準拠になります。	
動作時の高度	最大 4,572 メートル（15,000 フィート）まではディレーティングなし、最大 12,192 メートル（40,000 フィート）までは 25 °C 環境にディレーティング	
保管時の高度	最大 12,192 メートル（40,000 フィート）	

表 *8*：電力仕様

電力仕様	IE-3100H-6FT2T-E	IE-3100H-8T-E
標準入力電圧範囲	12 ～ 48 VDC	12 ～ 48 VDC
入力電圧範囲（絶対定格）	9.6 ー 60VDC	9.6 ー 60VDC
標準定格入力電流	1.5 A	1.5 A
入力電流 @（9.6V/60V）	0.998 A/0.174 A	1.265 A/0.210 A
消費電力 @（9.6V/60V）	9.58 W/10.44 W	12.14 W/12.60 W

コネクタとケーブル

表 *9 : Cisco Catalyst IE3100H Heavy Duty* シリーズ スイッチ のケーブルとコネクタ

データポート	• 銅製 100 BASE-T M12 D コード 4 極（ピン）ケーブル：M12 プラグおよび/または M12/RJ-45 コネクタ • 銅製 GE M12 X コード 8 極（ピン）シールド ケーブル：M12 プラグおよび/または M12/RJ-45 コネクタ
電源入力	M12 L コードコネクタ（ジャック）
コンソールケーブル:	A コード M12 コネクタ付き RS-232 コンソールケーブル CAB-CONSOLE-M12=

トルク仕様

表 *10 : Cisco Catalyst IE3100H Heavy Duty* シリーズ スイッチ トルク仕様

コンソール、イーサネットポート（M12 コネクタ）	4.43 ～ 7.08 インチ/ポンド（0.5 ～ 0.8 Nm）
M12 コネクタダストキャップ（コンソール、イーサネットポート）	4.5 ～ 5.5 インチポンド（0.51 ～ 0.62 Nm）
電源コネクタ（M12 L コード）	5.3 インチポンド（0.60 Nm）
SD カード カバー固定ねじ	4.43 ～ 7.08 インチ/ポンド（0.5 ～ 0.8 Nm）

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。