Cisco Catalyst IE3400 Heavy Duty シリーズ ハードウェア設置ガイド

初版：2019 年 9 月 3 日

最終更新：2022 年 12 月 1 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/

目 次

はじめに

対象読者

このガイドは、Cisco Catalyst IE3400 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。

追加の製品情報は、http://www.cisco.com/en/US/products/ps12451/index.html で入手できます。

その他のマニュアルについては、
http://www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html の Cisco Catalyst IE3400 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。

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 この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器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。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

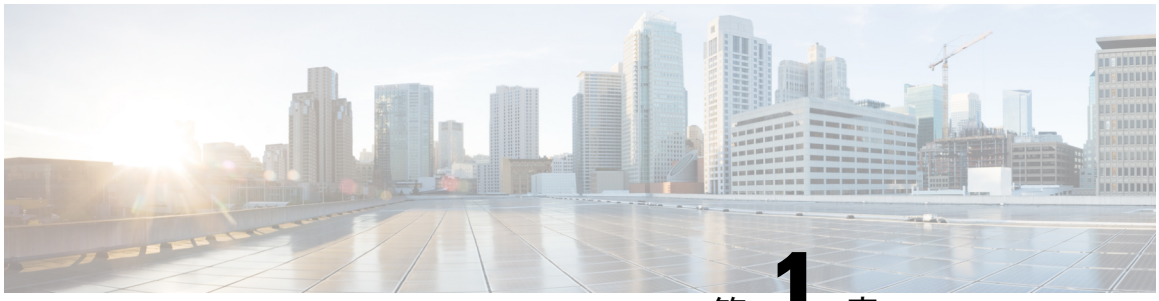
この製品の安全上の警告は複数の言語に翻訳され、製品に付属の『*Regulatory Compliance and Safety Information for the Regulatory Compliance and Safety Information for the Cisco Catalyst IE3400*

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。



第 1 章

製品概要

製品概要

Cisco® Catalyst® IE3400 Heavy Duty シリーズは、最も要求の厳しい産業環境でネットワークベースのセキュリティ、セグメンテーション、可視性を強化するように設計された、シスコの次世代 IP66 および IP67 対応スイッチング プラットフォームです。Cisco® Catalyst® IE3400 Heavy Duty シリーズ スイッチは、インテントベース ネットワークのパワーを最も過酷な Internet of Things（IoT）エッジに拡張します。

Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチは、埃や水にさらされる環境で Cisco Catalyst IE3400 高耐久性シリーズと同様の高度な機能を提供します。これらのスイッチは、8、16、または 24 ファストイーサネット（D-coded）またはギガビットイーサネット（X-coded）M12 インターフェイスで使用できます。スイッチは、壁面に取り付けて、設置キャビネットなしで導入できます。

（注） 設置方法の詳細については、「スイッチの設置」セクションを参照してください。

IE3400 Heavy Duty シリーズ スイッチは Cisco IOS® XE を搭載しています。Cisco IOS XE は、セキュリティ機能が組み込まれた信頼できる次世代オペレーティングシステムで、セキュアブート機能、イメージ署名機能、Cisco Trust Anchor モジュールを備えています。また、Cisco IOS XE は、オープン API およびデータモデルを備えた API 主導型の構成になっています。

Cisco IE3400 Heavy Duty シリーズは、Cisco DNA Center や Industrial Network Director などの強力なツールで管理できます。また、WebUI という、全面的に再設計された使いやすい最新の GUI ツールを使用して簡単に設定できます。また、プラットフォームでは Flexible NetFlow がサポートされるため、Cisco Stealthwatch® を使用してトラフィックパターンや攻撃分析をリアルタイムで把握できます。

この製品に関連するマニュアルのほとんどは、
http://www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html にあります。

スイッチのモデルと電源

図 *1 : Cisco Catalyst IE3400 Heavy Duty* シリーズ

次の表で、スイッチと電源について説明します。すべての IP66 および IP67 スイッチは、LAN Base Cisco iOS ファームウェアを使用します。

表 *1 :* スイッチと電源の説明

ハードウェア仕様	IE-3400H-8FT	IE-3400H-8T	IE-3400H-16FT	IE-3400H-16T	IE-3400H-24FT	IE-3400H-24T
合計 **100 Mbps D** コードポート	8	該当なし	16	N/A	24	該当なし
合計 **1 Gbps X** コードポート	該当なし	8	該当なし	16	N/A	24
リムーバブルストレージ	SD カード 注 1 を参照してください。	SD カード 注 1 を参照してください。	SD カード 注 1 を参照してください。	SD カード 注 1 を参照してください。	SD カード 注 1 を参照してください。	SD カード 注 1 を参照してください。
アラーム出力 注 2 および 3 を参照してください。	アラーム出力リレー X 1	アラーム出力リレー X 1	アラーム出力リレー X 1	アラーム出力リレー X 1	アラーム出力リレー X 1	アラーム出力リレー X 1
アラーム入力 注 2 を参照してください。	アラーム入力 X 1	アラーム入力 X 1	アラーム入力 X 1	アラーム入力 X 1	アラーム入力 X 1	アラーム入力 X 1

ハードウェア仕様	IE-3400H-8FT	IE-3400H-8T	IE-3400H-16FT	IE-3400H-16T	IE-3400H-24FT	IE-3400H-24T
コンソールポート 注 2 を参照してください。	1	1	1	1	1	1
電源入力	ミニチェンジ（単一電源）	ミニチェンジ（単一電源）	ミニチェンジ（単一電源）	ミニチェンジ（単一電源）	ミニチェンジ（単一電源）	ミニチェンジ（単一電源）

注 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。

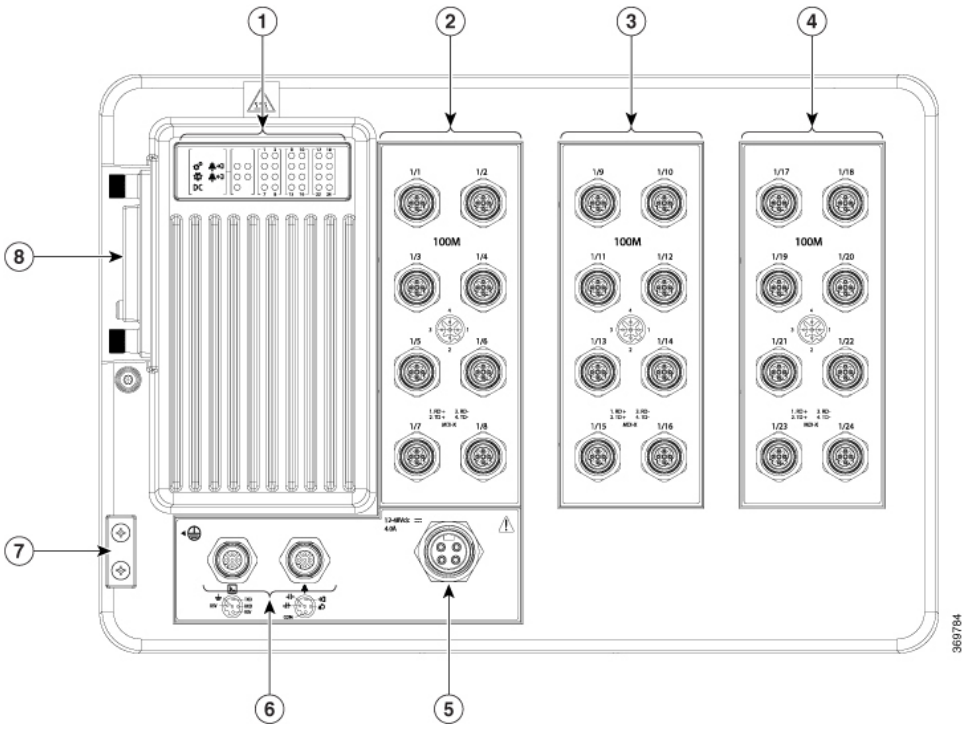
注 2：M12 A コード 5 ピンコネクタを使用。

注 3：最大リレー定格：1A で 24VDC、0.5A で 48VDC。

スイッチの前面パネル

ここでは、前面パネルコンポーネントについて説明します。次の図は、この製品ファミリのさまざまなモデルで使用できるコンポーネントを示しています。すべてのモデルが示されているわけではありません。

図 *2 : Catalyst IE3400H* フロントパネル



1	スイッチステータス LED	6	コンソールポート（左） アラームポート（右）

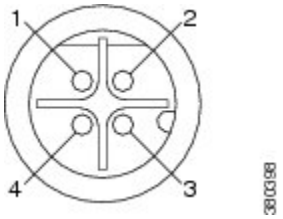
2、3、4	イーサネット ポート	7	アース ラグ
5	電源入力ポート	8	SD カードカバー

10/100BASE-T ポート

IP 標準 M12 ケーブルで 10 または 100 Mb/s で動作するよう、10/100BASE-T ポートを設定できます。ポートは、全二重、半二重、自動ネゴシエーション（デフォルト）、または半二重不可の各モードで動作可能です。

ポートの **Never Half Duplex** オプションは、その名前に示すとおりに機能します。リンクが半二重として確立されることは決してありません。全二重かリンクなしのいずれかになります。CSMA/CD ネットワークにおいて不可避な予測不能の応答時間が原因となって、安全装置が作動したりプロセスフローの再起動が必要になるような緊急停止が発生したりする可能性がありますが、半二重不可では、そのような事態を回避できます。

図 *3: FE* ポート

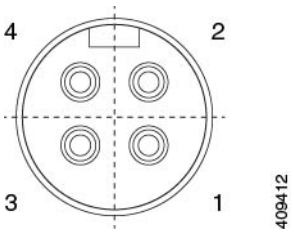


1	RD +	3	RD –
2	TD +	4	TD –

電源コネクタ

DC 電源は、前面パネルのコネクタを介してスイッチに接続します。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。

図 *4:* 電源コネクタ



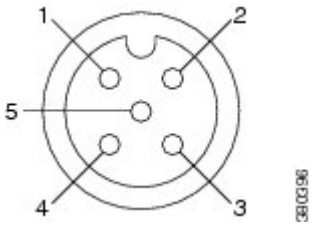
1	NC	3	DC–
2	DC+	4	NC

アラーム コネクタ

アラームコネクタを介してスイッチにアラーム信号を接続します。スイッチは1つのアラーム出力リレーをサポートします。

アラーム出力回路は、ノーマル オープン接点とノーマル クローズ接点のリレーです。スイッチの設定により、障害を検知したらリレーコイルに通電してリレー接点の両方の状態を切り替えます（ノーマルオープン接点を閉成、同時にノーマルクローズ接点を開放）。アラーム出力リレーは、ベルまたはライトなどの外部アラーム装置の制御に使用できます。アラーム出力の定格は 24Vdc/1A、最大 48Vdc/0.5A です。

図 *5:* アラーム コネクタ



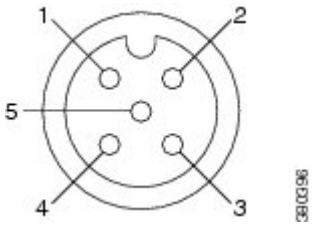
1	NOアラーム出力のノーマルオープン（NO）接続	4	アラーム入力基準
2	NCアラーム出力のノーマルクローズ（NC）接続	5	COMMONアラーム共通接続
3	アラーム入力		

コンソール管理ポート

スイッチは、5 極 A-coded コンソール ポートにより、Microsoft Windows が実行されている PC またはターミナル サーバに接続し、CLI を使用してそれを設定できます。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 *6:* コンソール コネクタ



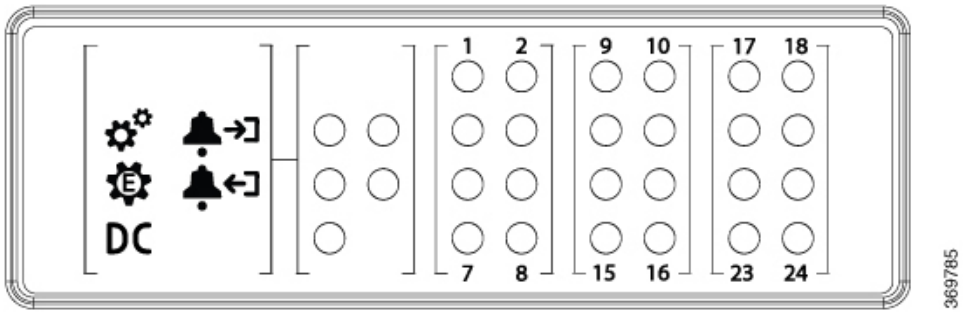
1	RTS	4	RXD
2	CTS	5	GND
3	TXD		

（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

ポートとアラームの状態に加えて、システム全体の状態および電源装置の入出力状態をモニタするために、LED を使用できます。

図 *1:* スイッチ *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
消灯	スイッチに電源が入っていません。
緑の点滅	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	スイッチは正常に動作しています。
赤	スイッチが正常に機能していません。

Express Setup LED

Express Setup の LED には、初期設定用の初期設定ステータスが表示されます。

表 *3 : Setup LED*

色	ステータス
消灯	マネージド スイッチとして設定済み。
緑の点灯	初期設定を実行して正常に動作中。
緑の点滅	初期設定、リカバリ、または初期設定の実行が完了していません。
赤の点灯	管理ステーションにスイッチを接続するために使用可能なポートがないため、初期設定またはリカバリを開始できませんでした。スイッチ ポートから装置の接続を外し、Express Setup ボタンを押してください。

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 *4 :* 電源ステータス *LED*

色	システムステータス
緑	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	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。

アラーム LED

次の表に、アラーム LED の色とその意味を示します。

表 *5 :* アラーム *OUT* ステータス *LED*

色	システムステータス
消灯	アラーム出力が設定されていないか、スイッチがオフになっています。
緑	アラーム出力は設定されていますが、アラームは検出されていません。

色	システムステータス
赤の点滅	メジャー アラームが検出されました。
赤	マイナー アラームが検出されました。

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 ～ 23 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。
緑と橙の交互の点滅	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モニタされています。
橙の点灯	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）。

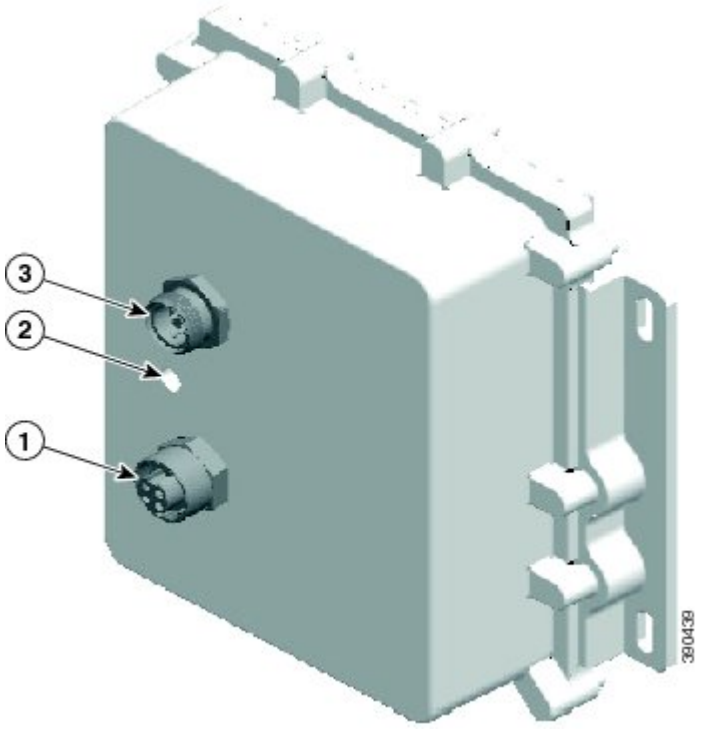
IP67 電源装置

スイッチは、オプションのIP67電源、（PWR-IE160W-67-DC=）および（PWR-IE180W-67-AC=）とともに利用可能です。IP67 DC 電源は、18 ～ 60Vdc の入力に対応し、54V、160W DC 出力を提供します。IP67 AC 電源は、85 ～ 264VAC 入力に対応し、54V、180W DC 出力を提供します。また、IP67 以外にもこのスイッチと互換性のある電源があります。

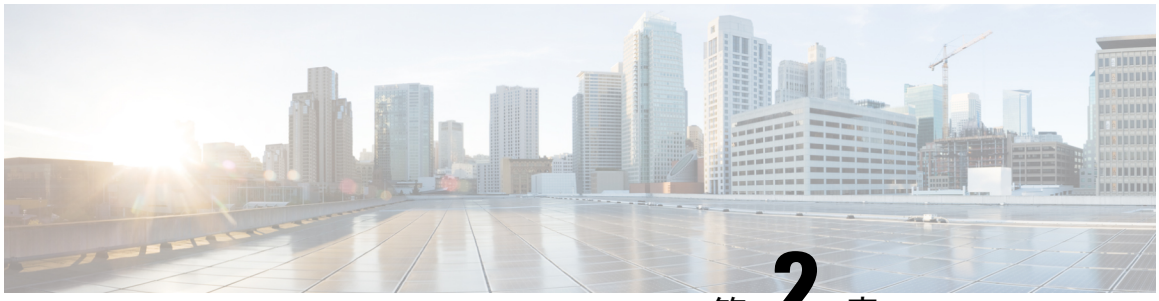
（注） 電源は別売りです。

次の図は、IP67 電源を示しています。

図 *8 : Cisco IP67* 電源



1	DC出力コネクタ	3	DC入力電源コネクタ
2	ステータス LED		



第 2 章

スイッチの設置

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。また、特に危険な環境に設置するための情報も含んでいます。

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。

設置の準備

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 電力系統に接続された装置で作業する場合は、事前に、指輪、ネックレス、腕時計などの装身具を外してください。金属は電源やアースに接触すると、過熱して重度のやけどを引き起こしたり、金属類が端子に焼き付いたりすることがあります。ステートメント 43

警告 雷が発生しているときには、システムに手を加えたり、ケーブルの接続や取り外しを行ったりしないでください。ステートメント 1001

警告 次の手順を実行する前に、DC 回路に電気が流れていないことを確認してください。ステートメント 1003

警告 設置の手順を読んでから、システムを電源に接続してください。ステートメント 1004

警告 この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊な工具、錠と鍵、またはその他の保安手段を使用しないと入れない場所を意味します。ステートメント 1017

警告 この装置は、接地させる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。ステートメント 1024

警告 この機器の設置、交換、または保守は、訓練を受けた相応の資格のある人が行ってください。ステートメント 1030

警告 装置は、必ず、IEC 60950 に基づいた安全基準の安全超低電圧（SELV）の要件に準拠する DC 電源に接続してください。ステートメント 1033

警告 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。ステートメント 1040

警告 装置の設置されている建物の外と接続する場合、次のポートは、集積回路の保護機能を備えた認定済みのネットワーク終端装置を介して接続する必要があります：10/100/1000 イーサネット、コンソール、アラームステートメント 1044。

警告 過熱防止のため、室温が 60 °C（140 °F）を超える環境ではスイッチを使用しないでください。ステートメント 1047

警告 装置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。ステートメント 1074

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：50.8 mm（2.0 インチ）– 左右：50.8 mm（2.0 インチ）– 正面：50.8 mm（2.0 インチ）

注意 IP66/IP67 およびタイプ 4X 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 4X 要件に適合している必要があります

EMC Environmental Conditions for Products Installed in the European Union

This section applies to products to be installed in the European Union.

The equipment is intended to operate under the following environmental conditions with respect to EMC:

- A separate defined location under the user's control.
- Earthing and bonding shall meet the requirements of ETS 300 253 or CCITT K27.
- AC-power distribution shall be one of the following types, where applicable: TN-S and TN-C as defined in IEC 364-3.

In addition, if equipment is operated in a domestic environment, interference could occur.

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。トルクの仕様については、「Cisco IE 2000 IP67 シリーズ スイッチの技術仕様」を参照してください。

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、「Cisco IE 2000 IP67 シリーズ スイッチの技術仕様」の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、アーススストラップを使用して適切にアース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ム可能な電子システム（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。14 ページの「次のステップ」セクションの手順に従います。
- 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 電源コネクタおよびアラーム 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：50.8 mm（2.0 インチ）
  - 左右：50.8 mm（2.0 インチ）
  - 前面：50.8 mm（2.0 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。

- 保護アース 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。
- IP67 ダスト キャップ用 15mm 12pt ソケット
- 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）

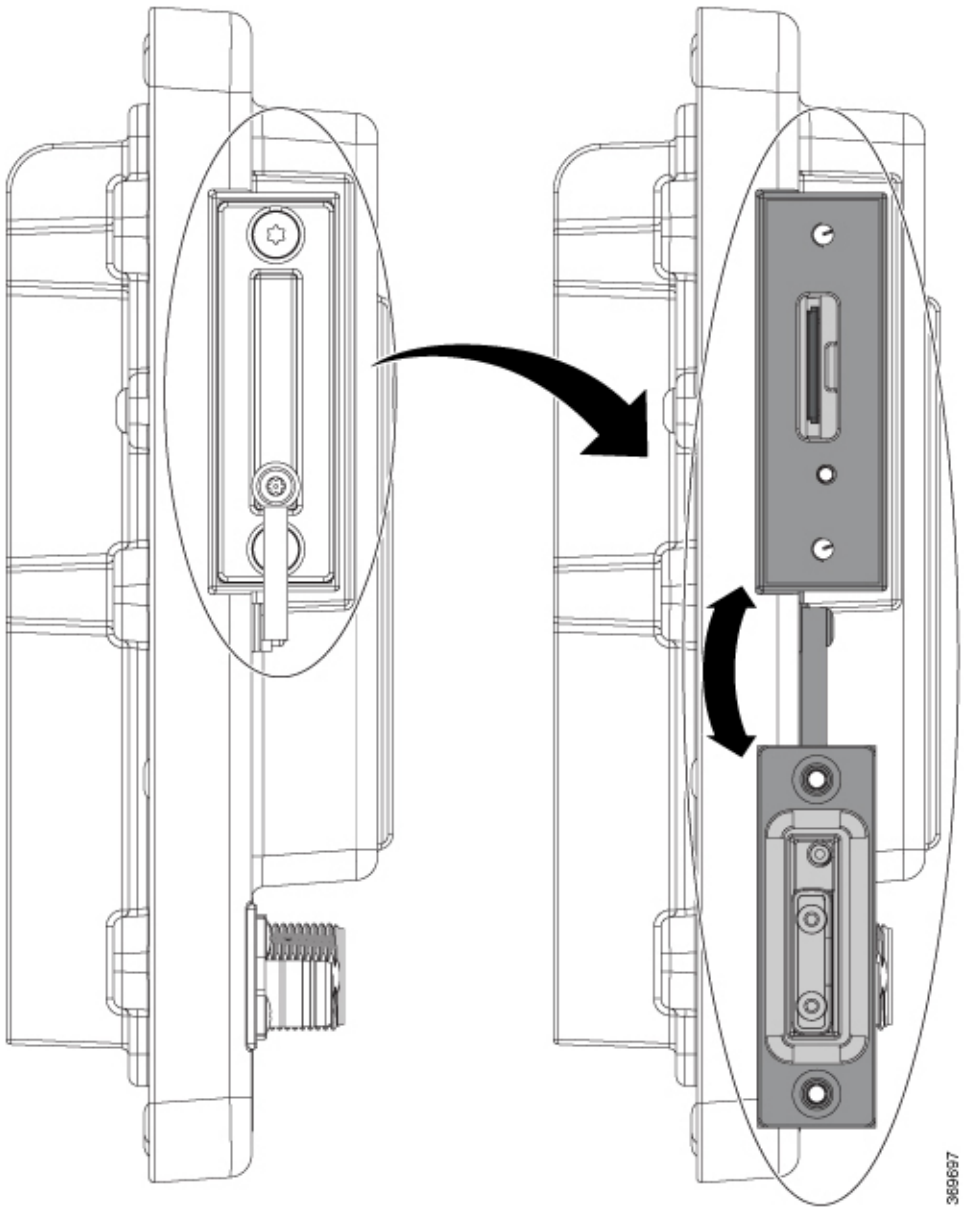
スイッチは、ホットスワップ SD メモリカード（SD-IE-4GB）ファームウェアをサポートしており、スタートアップ コンフィギュレーションが保存されます。それにより、交換用スイッチを設定せずに、故障したスイッチを置き換えることができます。

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。

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。



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、15.93 ～ 19.47 インチ ポンド（1.8 ～ 2.2Nm）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 5 極 DB-9 アダプタケーブル（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 電源への接続 （17 ページ）の説明に従い、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。

ステップ 6 IP67 に確実に準拠するため、すべてのコンソール ダスト キャップおよびケーブルは必ず 4.43 ～ 7.08 インチ ポンド（0.5 ～ 0.8 Nm）のトルクで取り付けます。

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 9.6V から 60Vdc の間でなければなりません。

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。円形ミニ交換ケーブルのメス側端子をスイッチの電源コネクタに（トルク = 10 インチ ポンドで）接続し、ピグテールを非標準電源に接続します。

警告 この製品は、設置する建物にショート（過電流）保護機構が備わっていることを前提に設計されています。保護デバイスの定格が 10 A を超えないことを確認してください。ステートメント 1005

IP67 準拠を達成するための推奨トルクは、スイッチの電源入力コネクタおよび Cisco IP67 電源の電源入出力コネクタについて 10 インチ/ポンド（1.13 Nm）です。

スイッチのアース接続

設置場所のアース要件に従ってください。

危険 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。ステートメント 1064

注意 装置を確実にアース接続するには、正しいアース接続手順に従い、10 AWG 導線に対応する UL 規格の丸端子ラグ（Hollingsworth 製、部品番号 R3456B または同等品など）を使用してください。

注意 外部アースネジに接続するには、少なくとも 4 mm 2 の導体が必要です。

アース ラグはスイッチに同梱されていません。次のオプションの中から選択できます:

- 一つ穴丸端子
- 2 個の一つ穴丸端子

アース ネジを使用してスイッチをアースするには、次の手順に従います。

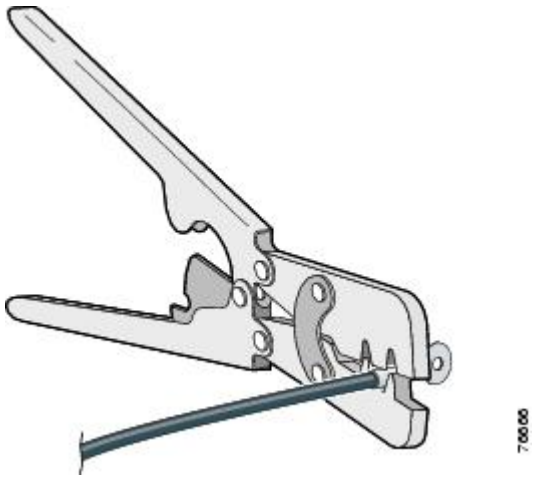
手順

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。次の図を参照してください。2個のリング端子が使用されている場合は、2番目の丸端子に対してこのアクションを繰り返します。

図 *9*: 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。

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）　ケーブルの一方の端には M12 Xcode または Dcode コネクタが、もう一方の端には RJ45 が必要です。Xcode ケーブルは、モデル IE-3400H-8T、IE-3400H-16T、および IE-3400H-24T 用です。Dcode ケーブルは、モデル IE-3400H-8FT、IE-3400H-16FT、および IE-3400H-24FT 用です。

（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（メモリ カードの取り付けまたは取り外し（オプション）（15 ページ）を参照）。

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。

電源への接続（17 ページ）の説明を参照してください。

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 はグリーン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（システムに電源が入っていない）場合、緑色に点滅し続ける（POST 中の）場合、または赤に点灯する（障害の）場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

ステップ 3 2 ～ 3 秒の間（カバ―の下の SD カードスロットの横にある）Express Setup ボタンを押し続けます。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ツールを使用できます。

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 カテゴリ 5 イーサネットケーブル（付属していません）をスイッチの左上のポートから PC のイーサネットポートに接続します。スイッチでは、モデルに関係なく常に左上のポートです。

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。

- 1/1 というラベルの付いた左上のポートにイーサネットケーブルを接続しました。
- 破損していないカテゴリ 5 またはカテゴリ 6 イーサネット ケーブルを使用していること。
- 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。ログイン プロンプトが表示されます。

ステップ 6 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 7 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。

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

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がすべて無効になっていることと、PC のワイヤレスクライアントがすべて無効になっていることを確認してください。

ステップ 8 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 9 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 10 [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 11 [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 12 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、橙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 が橙色に点滅します。これは、工場出荷時のデフォルトをリロード中であることを意味します。
  - 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。

アラーム回路の接続

スイッチを設置した後、アラームを接続できます。

スイッチのアースと電源の接続手順については、電源への接続 （17 ページ）を参照してください。

外部アラームの配線

スイッチのアラーム コネクタとの接続には、M12 A-coded ケーブルを使用します。推奨トルクは 4.43 ～ 7.08 インチ ポンド（0.5 ～ 0.8 Nm）です。

Molex の推奨ケーブルの製品番号は 1200650523 です。ケーブルの一方の端は M12 A-coded コネクタ、もう一方は開放端です。

次の表に、スイッチパネルにあるアラームコネクタのラベルを示します。

表 7: アラーム コネクタのラベル（上から下）

ピン	ラベル	接続
1	NO	アラーム出力のノーマル オープン（NO）接続
2	NC	アラーム出力のノーマル クローズ（NC）接続
3	UNCONNECTED	未使用
4	UNCONNECTED	未使用
5	COMMON	アラーム共通接続

注意 アラーム出力のリレー回路の入力電圧ソースは、24 VDC、1.0 A 以下または 48 VDC、0.5 A 以下に制限された独立ソースである必要があります。

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。

注意 すべてのケーブルのオス/メスを合わせて接続して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/IP67 UL50E タイプ 4X 準拠になります。

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。
- イーサネットケーブルをモデル IE-3400H-8FT、16FT、および 24FT に接続するには、D コード M12 コネクタ付きのケーブルを使用します。
- イーサネットケーブルをモデル IE-3400H-8T、16T、および 24T に接続するには、X コード M12 コネクタ付きのケーブルを使用します。

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）。図 1-2 を参照してください。

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。

ステップ 5 IP67 準拠のため、すべてのアラーム ダスト キャップおよびケーブルは必ず 4.43 ～ 7.08 インチポンド（0.5 ～ 0.8 Nm）のトルクで取り付けます。

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モニタするには、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モニタ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。

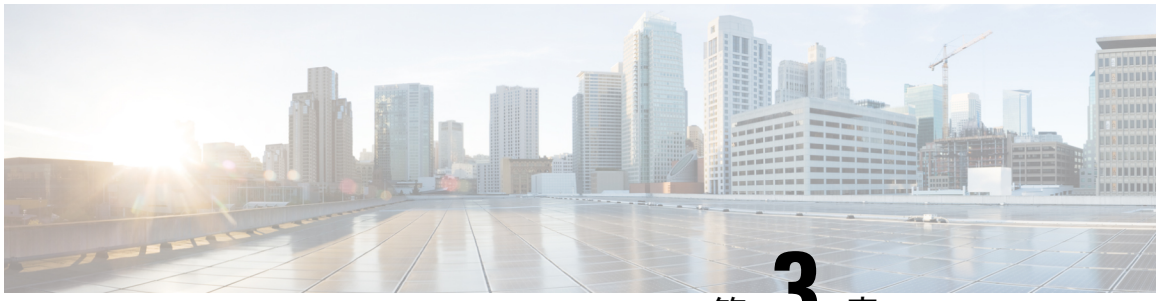
- Cisco DNA センターは次の場所にあります：https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

- 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。



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：50.8 mm（2.0 インチ）– 露出側（モジュールに接続されていない面）：50.8 mm（2.0 インチ）– 正面：50.8 mm（2.0 インチ）

壁面へのスイッチの取り付け

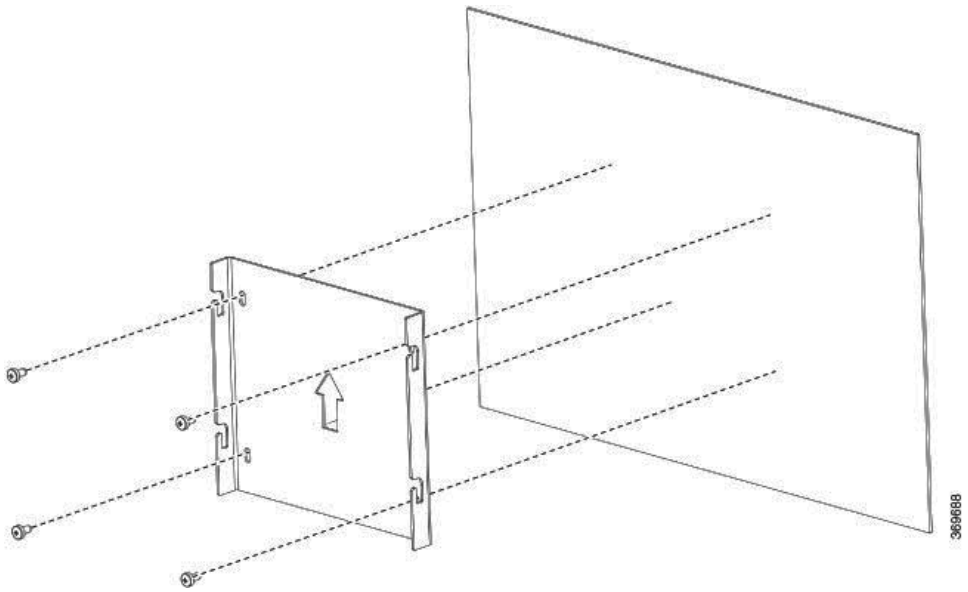
壁またはパネルにスイッチを取り付けるには、次の手順を実行します。

警告 壁面への設置手順をよく読んでから、設置を開始してください。適切なハードウェアを使用しなかった場合、または、正しい手順に従わなかった場合は、人体に危険が及んだり、システムが破損したりする可能性があります。ステートメント 378

手順

ステップ 1 スイッチ取り付けブラケットを、矢印を上にして、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。同梱の 4 本のプラスネジでブラケットを壁に取り付けます。

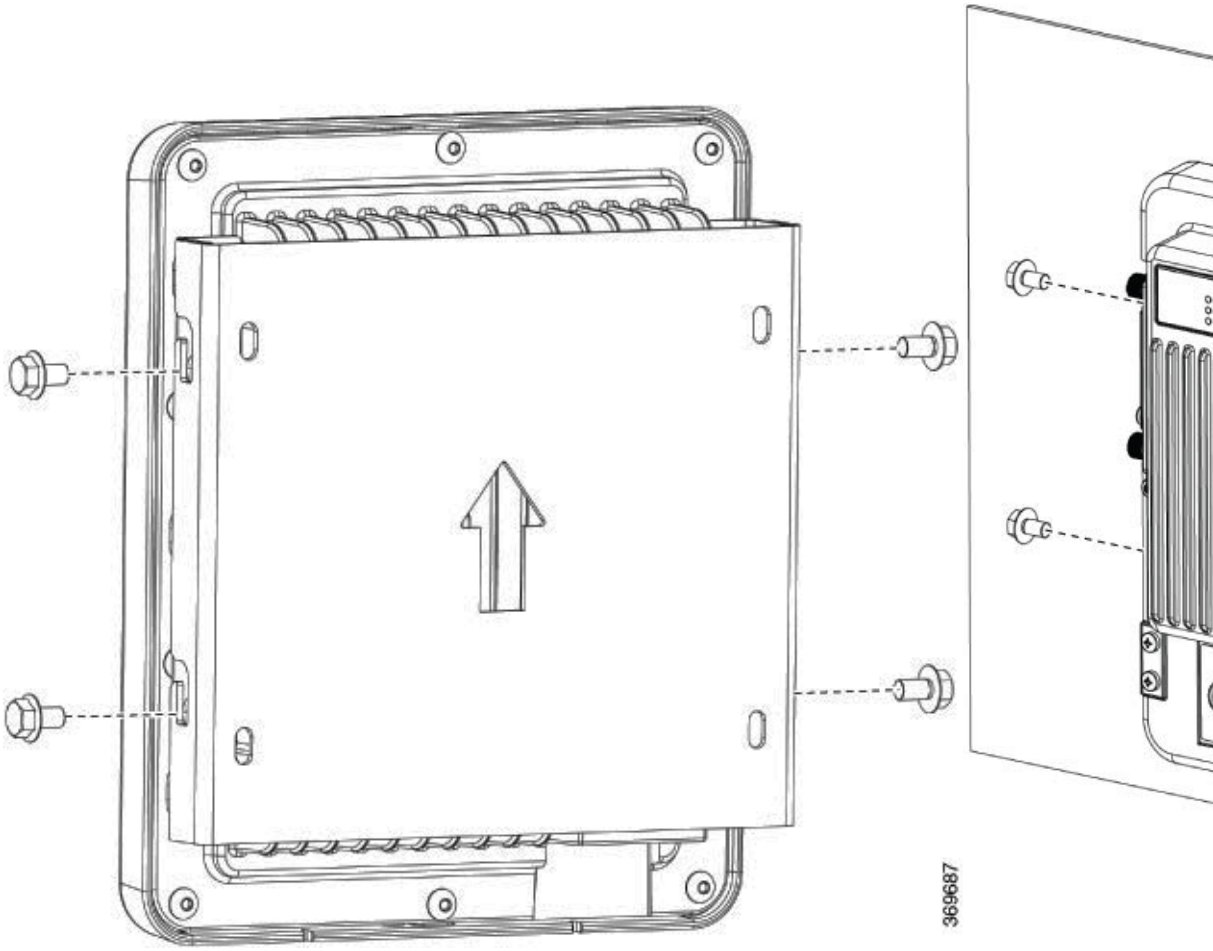
図 *10* : 壁面ブラケットの壁への取り付け



（注） ブラケットを壁またはパネルに取り付けるときは、ブラケットと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 4つの取り付けネジをスイッチに緩く取り付け、ブラケットに押し込み下にスライドさせます。次の図を参照してください。

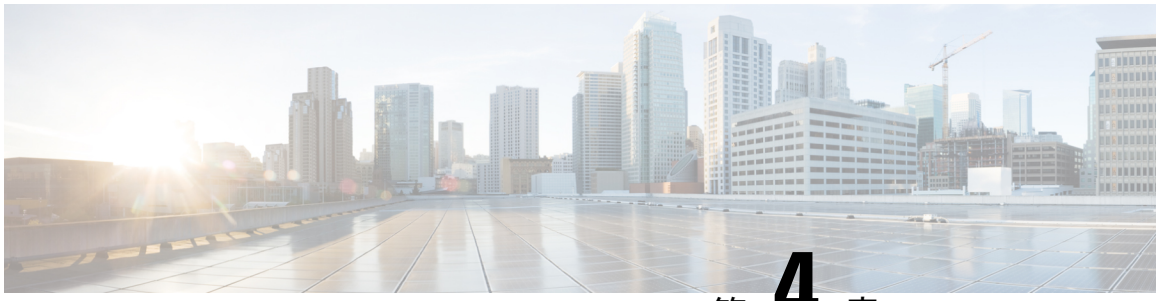
図 *11* : 取り付けブラケットへのスイッチの取り付け



ステップ 3 スイッチを取り外すには、4 つの取り付けネジを緩め、スイッチを上前方にスライドさせて取り付けブラケットから外します。次に、必要に応じて、ブラケット自体を壁面からネジを抜いて外すことができます。

次のタスク

スイッチを壁面またはパネルに取り付けたら、「アラーム回路の接続」セクション（12 ページ）の説明に従い、電源とアラームの導線を接続します。



第 4 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 17.10.1 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。「システムセキュリティ設定（Cisco IOS XE 17.10.1 以降） （34 ページ）」を参照してください。

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 （17 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キー（Cisco IOS XE 17.10.1 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

初期設定（Cisco IOS XE 17.9.x 以前）

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。

1. 次の 2 つのプロンプトで **Yes** と入力します。

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

2. スイッチのホスト名を入力し、Return を押します。

   指定できるホスト名の文字数は、コマンド スイッチでは 28 文字、メンバ スイッチでは 31 文字に制限されています。どのスイッチでも、ホスト名の最終文字として *-n*（n は数字）を使用しないでください。

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

3. イネーブル シークレット パスワードを入力し、Return を押します。

   このパスワードは 1 ～ 25 文字の英数字で指定できます。先頭の文字を数字にしてもかまいません。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。シークレット パスワードは暗号化されますが、イネーブル パスワードはプレーン テキストです。

```
Enter enable secret: secret_password
```

4. イネーブル パスワードを入力し、Return を押します。

```
Enter enable password: enable_password
```

5. 仮想端末パスワードを入力し、Return を押します。

   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。

```
Enter virtual terminal password: terminal-password
```

6. （任意）プロンプトに従って、簡易ネットワーク管理プロトコル（SNMP）を設定します。後から、CLI、Device Manager、または Cisco Network Assistant アプリケーションを使用して SNMP を設定することもできます。SNMP を後で設定する場合は、**no** と入力します。

```
Configure SNMP Network Management? [no]: no
```

7. 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）を入力して、**Return**を押します。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
Any interface listed with OK? value "NO" does not have a valid configuration
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned NO unset up down
GigabitEthernet1/1 unassigned YES unset down down
GigabitEthernet1/2 unassigned YES unset down down
GigabitEthernet1/3 unassigned YES unset down down
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 down down
GigabitEthernet1/8 unassigned YES unset down down
GigabitEthernet1/9 unassigned YES unset down down
GigabitEthernet1/10 unassigned YES unset down down
Enter interface name used to connect to the
management network from the above interface summary: vlan1
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

8. スイッチのIPアドレスとサブネットマスクを入力し、Returnキーを押してインターフェイスを設定します。ここに示す IP アドレスとサブネット マスクは一例です。

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface: 10.1.1.2
Subnet mask for this interface [255.255.255.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /24
```

9. 次のサマリーが表示されます。

```
The following configuration command script was created:
hostname ie3300
enable secret 9 $9$rkqtjJhIkZyANU$Ib4nfuxrpHBi.lixF.0Ir94k9XWYsW3nyF7Glmc6lkc
enable password cisco
line vty 0 15
password cisco
no snmp-server
!!
interface Vlan1
no shutdown
```

```
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
end
```

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。次のいずれかのツールを使用すれば、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）

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 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、スイッチの『Cisco Catalyst IE3x00 Rugged Switch software configuration guides』を参照してください。

システムセキュリティ設定（Cisco IOS XE 17.10.1 以降）

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、入力するマスターキーと結合されます。マスターキーはリカバリできないため、記憶しておく必要があります。
- マスターキーは、AES 対称暗号を使用してスイッチ設定内の他のすべてのキーを暗号化するために使用されるパスワード/キーです。マスターキー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、マスターキーを使用して、スイッチ設定内の既存または新しいキーが暗号化されます。**password encryption aes** コマンドを実行するまで、キー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 （35 ページ） または 初期設定 - タイプ 7 暗号化 （38 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 （42 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。

始める前に

コンソール ポートへの PC または端末の接続 （17 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、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 17.10.1 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キーの暗号化に使用するマスターキーを入力します。

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

ステップ 4 マスターキー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、マスターキー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。次のいずれかのツールを使用すれば、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、Cisco IE3x00 スイッチの設定ガイド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 （17 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。次のいずれかのツールを使用すれば、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、Cisco IE3x00 スイッチの設定ガイド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キーの暗号化に使用するマスターキーを入力します。

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

ステップ 6 マスターキー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、マスターキー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
!
!
```

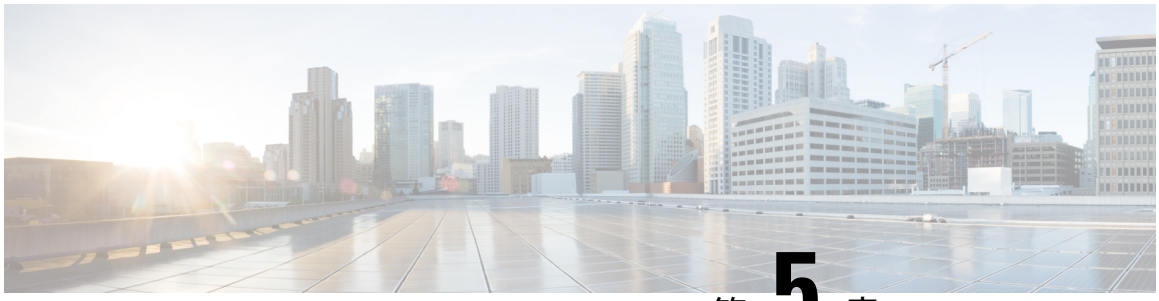
```
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4


[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 5 章

トラブルシューティング

トラブルシューティング

この章では、トラブルシューティングの推奨事項について説明します。

問題の診断

スイッチの LED は、スイッチに関するトラブルシューティング情報を提供します。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。

スイッチの接続状態

不良または破損したケーブル

ケーブルにわずかでも傷や破損がないか必ず確認してください。物理層の接続に問題がないように見えるケーブルでも、配線やコネクタのごくわずかな損傷が原因でパケットが破損することがあります。ポートでパケットエラーが多く発生したり、ポートがフラッピング（リンクの切断および接続）を頻繁に繰り返したりする場合は、ケーブルにこのような破損がある場合があります。

- 正常であることがわかっているケーブルと交換してください。
- ケーブル コネクタで破損または欠落したピンがないか確認します。
- 発信元と宛先の間のパッチ パネルの接続やメディア コンバータに問題がないことを確認します。可能な場合は、パッチパネルをバイパスします。
- ケーブルを別のポートに接続して、問題が発生するかどうかを確認します。

リンクステータス

両側でリンクが確立されていることを確認します。配線が切れていたり、ポートがシャットダウンしていたりすると、片側ではリンクが表示されても反対側では表示されない可能性があります。

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。

- 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。
- 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。
- 両方の装置の電源が入っていることを確認します。
- 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。
- 接触不良がないか確認します。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。

10/100 および 10/100/1000 ポートの接続

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、表 1-1 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、ポートを再び有効化します。
- ケーブル タイプを確認します。

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、重大なパフォーマンス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UDLDを有効にする方法の詳細については、Cisco.comにある『IOS-XE Software Configuration guide for the Cisco Catalyst IE 3x00 Switches』の「Information About UDLD」セクションを参照してください。

スイッチのパフォーマンス

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。

スイッチのパフォーマンス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。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 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 17.10.1 以降でサポートされています。

- IE3200
- IE3300

- IE3400
- IE3400H
- ESS3300

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:# IE3200
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 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」セクションを参照してください。

Express Setup のトラブルシューティング

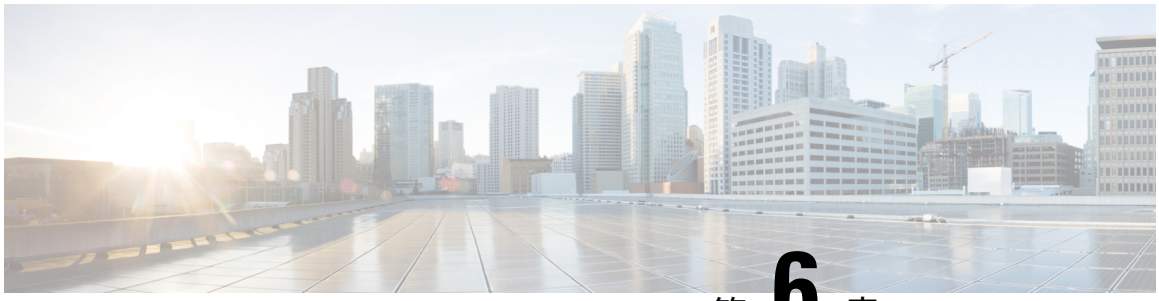
ここでは、スイッチの初期設定に関するトラブルシューティングのヒントを示します。

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。

チェックリスト	推奨事項
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。
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 2000 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、取り外し可能なドアの下の左側のコンプライアンスラベルにあります。**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 6 章

技術仕様

技術仕様

この付録では、Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチの技術仕様を示します。

動作温度仕様

次の表に、3 つの異なる環境での Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチの動作温度を示します。

表 *8 : Cisco Catalyst IE3400 Heavy Duty* シリーズ スイッチの動作温度

	エンクロージャが必要な産業用自動化およびその他の場所	変電所	交通信号
ラック タイプ	密閉型ラック 例：NEMA4、NEMA4X、NEMA12、NEMA13、IP54、IP66。	開放型ラック 例：NEMA1、IP66、IP67。	ファンまたはブロワーを搭載したラック 例：NEMA TS-2。 （注） 最小エアフローは 200 lfm です。[1].

[1] lfm = リニアフィート/分

（注） 安全性に関する認定規格は、周辺温度が 140 °F （60 °C）以下の場合にだけ適用されます。ただし、Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチは、次の表に示されている環境条件の変電所および交通信号設置場所で動作できます。

技術仕様

Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチの技術仕様は次のとおりです。

表 *9 : Cisco Catalyst IE3400 Heavy Duty* シリーズ の技術仕様

Environmental Ranges	
保管温度	–40 ～ 185 °F（–40 ～ 85 °C）
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 ～ 167 °F（–40 ～ 75 °C） **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。 • -40 ～ +70 °C（自然換気型ラック動作時） • -40 ～ +60 °C（密閉型ラック動作時） • -34 ～ +75 °C（200 LFM 以上のファンまたはブロワー搭載ラック動作時） • -40 ～ +85 °C（16 時間、+85 °C まで型式試験済み）
湿度（動作時）	5 ～ 95%（結露しないこと）
保護等級/タイプ定格	IP66/IP67 基準の防塵および防水 NEMA タイプ 4x **注意** すべての IP67 ケーブルのオス/メスを合わせて接続して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 4x 準拠になります。
動作時の高度	最大 4,570 m（15,000 フィート）
保管高度	最大 12,100 m（40,000 フィート）

表 *10 :* 電力仕様

電力仕様	IE-3400H-8FT	IE-3400H16FT	IE-3400H-24FT	IE-3400H-8T	IE-3400H-16T	IE-3400H-24T
標準入力電圧範囲	12 ～ 48VDC	12 ～ 48VDC	12 ～ 48VDC	12 ～ 48VDC	12 ～ 48VDC	12 ～ 48VDC
入力電圧範囲（絶対定格）	9.6 ー 60VDC	9.6 ー 60VDC	9.6 ー 60VDC	9.6 ー 60VDC	9.6 ー 60VDC	9.6 ー 60VDC
入力電流 @（**9.6V/60V**）	3.0A/0.51A	4.0A/0.65A	4.6A/0.75A	3.2A/0.54A	4.4A/0.71A	5.1A/0.83A

電力仕様	IE-3400H-8FT	IE-3400H16FT	IE-3400H-24FT	IE-3400H-8T	IE-3400H-16T	IE-3400H-24T
消費電力 @（9.6V/60V）	28.8W/30.6W	38.4W/39.0W	44.2W/45.0W	30.4W/32.2W	41.6W/42.3W	49.0W/49.8W

表 *11 :* 物理構成

物理仕様	IE-3400H-8FT	IE-3400H-8T	IE-3400H16FT	IE-3400H-16T	IE-3400H-24FT	IE-3400H-24T
サイズ（高さ X 幅 X 奥行）	9.58 X 7.90 X 3.15 インチ 24.33 X 20.07 X 8.00 cm	9.58 X 7.90 X 3.15 インチ 24.33 X 20.07 X 8.00 cm	9.58 X 10.90 X 3.15 インチ 24.33 X 27.69 X 8.00 cm	9.58 X 10.90 X 3.15 インチ 24.33 X 27.69 X 8.00 cm	9.58 X 13.90 X 3.15 インチ 24.33 X 35.31 X 8.00 cm	9.58 X 13.90 X 3.15 インチ 24.33 X 35.31 X 8.00 cm
重量（取り付けブラケットを含む）	8.45 ポンド 4.35 kg	8.45 ポンド 4.35 kg	11.25 ポンド 5.10 kg	11.25 ポンド 5.10 kg	13.90 ポンド 6.30 kg	13.90 ポンド 6.30 kg
取り付け	壁面取り付け	壁面取り付け	壁面取り付け	壁面取り付け	壁面取り付け	壁面取り付け

コネクタとケーブル

Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチのコネクタとケーブルは次のとおりです。

表 *12 : Cisco Catalyst IE3400 Heavy Duty* シリーズ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 オスおよび/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 オスおよび/または M12/RJ-45 コネクタ
アラーム ポート	• 銅製 M12 A コード 5 ピン コネクタ
電源入力	• 入力電源用のミニ 4 ピンコネクタ
コンソール ケーブル: CAB-CONSOLE-M12=	• IE3400H スイッチ用に M12 および DB9F を使用したコンソール ケーブル 6 フィート

トルク仕様

Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチのトルク仕様は次のとおりです。

表 *13 : Cisco Catalyst IE3400 Heavy Duty* シリーズのトルク仕様

アラーム、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（アラーム、コンソール、イーサネット ポート）	• 3.5 インチ/ポンド（0.4 Nm）
電源コネクタ（Mini-Change）	• 10 インチ/ポンド（1.13 Nm）
SD カード カバー固定ねじ	• 15.93 ～ 19.47 インチ/ポンド（1.8 ～ 2.2 Nm）

アラーム定格

Cisco Catalyst IE3400 Heavy Duty シリーズ スイッチのアラーム定格は以下のとおりです。

表 *14 : Cisco Catalyst IE3400 Heavy Duty* シリーズのアラーム定格

アラーム定格	仕様
アラーム	M12 A コード 5 ピン コネクタを使用する 1 つのアラーム出力リレー（最大定格：1 A 時 24 VDC/0.5 A 時 48 VDC）

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。