CHAPTER 1

概要

この章では、IE 3000 スイッチ ソフトウェアについて説明します。この章の内容は次のとおりです。

このマニュアルでは、特に IP Version 6（IPv6）に言及していない限り、IP という用語は IP Version 4（IPv4）を指します。

機能

このスイッチには、次のいずれかのソフトウェア イメージがすでにインストールされています。

- LAN ベースのイメージは、Access Control List（ACL; アクセス制御リスト）や Quality of Service（QoS; サービス品質）などの基本的なレイヤ 2 インテリジェント機能をサポートします。
- IP サービス イメージには、すべてのレイヤ 2+ 機能と、すべてのレイヤ 3 ルーティング（IP ユニキャスト ルーティング、IP マルチキャスト ルーティング、フォールバック ブリッジング）が含まれています。

この章で説明する機能の中には、暗号化（暗号化をサポートする）バージョンのソフトウェアでしか使用できないものがあります。この機能を使用するため、および Cisco.com から暗号化バージョンのソフトウェアをダウンロードするためには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

Ease-of-Deployment 機能および Ease-of-Use 機能

- Express Setup により、最初にブラウザベースのプログラムから、スイッチの基本 IP 情報、連絡先情報、スイッチおよび Telnet のパスワード、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）情報をすばやく設定できます。Express Setup の詳細については、クイック スタート ガイドを参照してください。
- ユーザ定義および Cisco のデフォルトの SmartPort マクロにより、カスタム スイッチ コンフィギュレーションを作成して、ネットワーク経由での配置を簡素化できます。
- 着脱式のコンパクト フラッシュ カードに、Cisco IOS ソフトウェア イメージと、スイッチのコンフィギュレーション ファイルが格納されています。ソフトウェア機能を再設定せずに、スイッチの交換やアップグレードを実行できます。更新版のブート ローダーに含まれるセカンダリ ブート ローダー イメージがサポートするコンパクト フラッシュ ファイル システム ドライバにより、コンパクト フラッシュ メモリ カードにアクセスできます。スイッチのブート ローダーにはプライマリ ブート ローダーとセカンダリ ブート ローダーが含まれ、どちらもブート フラッシュに格納されています。
- 組み込みデバイス マネージャの GUI により、Web ブラウザから単一スイッチの設定とモニタを実行できます。デバイス マネージャの起動の詳細については、クイック スタート ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Cisco Network Assistant（以後、*Network Assistant と表記*）により、次のことを実行できます。
  - コミュニティを管理できます。コミュニティはクラスタのような装置グループですが、ルーターとアクセス ポイントを含めることができ、セキュリティを強化できます。
  - イントラネット内の任意の場所からスイッチとスイッチ クラスタの管理を簡素化および最小化できます。
  - 特定の作業を実行する CLI（コマンドライン インターフェイス）コマンドを覚えなくても、単一のグラフィカル インターフェイスから複数の設定作業を実行できます。
  - 対話式のガイド モードで、VLAN、ACL、Quality of Service（QoS）などの複雑な機能をガイドに従って設定できます。
  - コンフィギュレーション ウィザードのプロンプトに従って、必要最小限の情報を指定するだけで、トラフィックの QoS プライオリティ、データ アプリケーションのプライオリティ レベル、セキュリティなどの複雑な機能を設定できます。
  - スイッチにイメージをダウンロードできます。
  - VLAN 設定と QoS 設定、目録レポートと統計レポート、リンク レベルとスイッチ レベルのモニタおよびトラブルシューティング、複数のスイッチ ソフトウェアのアップグレードなど、複数のポートや複数のスイッチに対して同時にアクションを適用できます。
  - 相互接続された装置のトポロジを表示して、既存のスイッチ クラスタとクラスタに参加できる適格なスイッチを識別し、スイッチ間のリンク情報を識別できます。
  - フロントパネル イメージで表示される LED から、1 つまたは複数のスイッチのリアルタイム ステータスをモニタできます。イメージに表示されるシステム LED、Redundant Power System（RPS; 冗長電源システム）LED、およびポート LED の色は、物理的な LED の色と類似しています。

（注） Network Assistant は cisco.com/go/cna からダウンロードする必要があります。

- スイッチ クラスタリング テクノロジーにより、次のことが可能になります。
  - 複数のクラスタ対応スイッチの設定、モニタ、認証、ソフトウェア アップグレードをまとめて実行できます。地理的な距離や相互接続メディア（イーサネット、ファスト イーサネット、Fast EtherChannel、Small Form-Factor Pluggable（SFP）モジュール、ギガビット イーサネット、Gigabit EtherChannel 接続など）は問いません。クラスタ対応スイッチのリストについては、リリース ノートを参照してください。
  - 候補スイッチを自動検出し、単一 IP アドレスを通して管理できるスイッチ（最大 16 台）のクラスタを作成できます。
  - コマンド スイッチに直接接続していないクラスタ候補を拡張検出できます。

パフォーマンス機能

- Cisco EnergyWise により、Power over Ethernet（PoE）デバイスおよび非シスコ デバイスを含むエンド ポイントのエネルギー使用量を管理します。詳細については、『*Cisco EnergyWise Configuration Guide*』を参照してください。
- すべてのスイッチ ポートの速度自動検知、およびデュプレックス モードの自動ネゴシエーションにより、帯域幅の利用を最適化します。
- 10/100 インターフェイス、10/100/1000 Mb/s インターフェイス、および 10/100/1000 BASE-TX SFP モジュール インターフェイス上の Automatic Medium-Dependent Interface Crossover（Auto-MDIX）機能により、インターフェイスが自動的に必要なケーブル接続タイプ（ストレートまたはクロス）を検出し、接続を適切に設定できるようにします。
- ルーテッド フレームでは最大 1546 バイト、ハードウェアでブリッジングされるフレームでは最大 9000 バイト、ソフトウェアによってブリッジングされるフレームでは最大 2000 バイトをサポートします。
- 全ポート上で IEEE 802.3x フロー制御を行います（スイッチはポーズ フレームを送信しません）。
- EtherChannel により、耐障害性を高め、スイッチ、ルータ、およびサーバ間に最大 8 Gbps（ギガビット EtherChannel）または 800 Mbps（ファスト EtherChannel）全二重の帯域幅が確保されます。
- Port Aggregation Protocol（PAgP; ポート集約プロトコル）および Link Aggregation Control Protocol（LACP）により、EtherChannel リンクが自動的に作成されます。
- レイヤ 2 およびレイヤ 3 のパケットをギガビットのラインレートで転送します。
- マルチキャスト Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）Lite により、ネットワークの仮想化およびマルチキャスト仮想私設網に使用する複数のプライベート ルーティング ドメインを設定できます（IP サービス イメージを実行しているスイッチ上）。
- ポート単位でのストーム制御により、ブロードキャスト ストーム、マルチキャスト ストーム、およびユニキャスト ストームを防止できます。
- レイヤ 2 の不明なユニキャスト、マルチキャスト、およびブリッジド ブロードキャスト トラフィック転送に対するポート ブロッキングを行います。
- Cisco Group Management Protocol（CGMP）サーバのサポートと、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピング（IGMP バージョン 1、2、3 に対応）については、次のようになります。
  - （CGMP 装置の場合）CGMP が特定のエンド ステーションへのマルチキャスト トラフィックを制限し、ネットワーク全般のトラフィックを軽減します。
  - （IGMP 装置の場合）IGMP スヌーピングにより、マルチメディア トラフィックおよびマルチキャスト トラフィックを転送します。

- IGMP レポート抑制により、1 つのマルチキャスト ルータ クエリーにつき 1 つの IGMP レポートだけをマルチキャスト デバイスへ送信します（IGMPv1 または IGMPv2 クエリーだけをサポート）。
- IGMP スヌーピング クエリアのサポートにより、IGMP の一般的なクエリー メッセージを定期的に生成するようスイッチを設定できます。
- IGMP ヘルパーにより、スイッチでホスト要求を転送して、特定の IP 宛先アドレスにマルチキャスト ストリームを加入させることができます。
- Multicast VLAN Registration（MVR; マルチキャスト VLAN レジストレーション）により、マルチキャスト VLAN でマルチキャスト ストリームを連続送信すると同時に、帯域幅やセキュリティ上の理由により、それらのストリームを加入者 VLAN から分離します。
- IGMP フィルタリングにより、スイッチ ポート上のホストが所属できるマルチキャスト グループセットを管理します。
- IGMP スロットリングにより、IGMP 転送テーブルのエントリ数が最大になったときのアクションを設定できます。
- IGMP Leave タイマーにより、ネットワークに対する脱退の待ち時間を設定できます。
- Switch Database Management（SDM）テンプレートにより、ユーザ側で選択する機能へのサポートを最大化するようにシステム リソースを割り当てられます。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）により、ローカルの広域アプリケーション エンジンへのトラフィックのリダイレクト、コンテンツ要求のローカル対応、ネットワーク内の Web トラフィック パターンのローカライズを実行できます（IP サービス イメージが必要）。
- Cisco IOS ソフトウェアの一部である Cisco IOS IP Service Level Agreement（SLA; サービス レベル契約）により、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます。
- 設定可能なスモール フレーム到達スレッシュホールドにより、スモール フレーム（64 バイト以下）が指定したレート（スレッシュホールド）でインターフェイスに到達した場合のストーム制御を防ぎます。
- Flex Link マルチキャスト高速コンバージェンスにより、Flex Link 障害の発生後にマルチキャスト トラフィックのコンバージェンスにかかる時間を短縮できます。
- RADIUS サーバのロード バランシングにより、アクセス要求と認証要求をサーバ グループ内で均等に配分できるようにします。
- 出力ネットワーク ポート上で、CPU 生成トラフィックと、キューの CPU 生成トラフィックの QoS マーキングをサポートします。

管理オプション

- 組み込みデバイス マネージャ：このデバイス マネージャは、ソフトウェア イメージに統合された GUI です。これを使用して、単一スイッチの設定とモニタを行います。デバイス マネージャの起動の詳細については、クイック スタート ガイドを参照してください。デバイス マネージャの詳細については、スイッチのオンライン ヘルプを参照してください。
- Network Assistant：Network Assistant は、Cisco.com からダウンロードできるネットワーク管理アプリケーションです。これを使用して、単一のスイッチ、スイッチのクラスタ、または装置のコミュニティを管理します。Network Assistant の詳細については、Cisco.com から入手可能な『*Getting Started with Cisco Network Assistant*』を参照してください。

- CLI：Cisco IOS ソフトウェアは、デスクトップ スイッチング機能とマルチレイヤ スイッチング機能をサポートしています。CLI にアクセスするには、管理ステーションを直接スイッチ コンソール ポートに接続するか、PC をイーサネット管理ポートに直接接続するか、またはリモート管理ステーションあるいは PC から Telnet を使用します。CLI の詳細については、第 2 章「CLI（コマンドライン インターフェイス）の使用」を参照してください。
- SNMP：CiscoWorks2000 LAN Management Suite（LMS）や HP OpenView などの SNMP 管理アプリケーションです。HP OpenView や SunNet Manager などのプラットフォームが稼動している SNMP 対応の管理ステーションから管理できます。スイッチは、Management Information Base（MIB; 管理情報ベース）拡張機能の包括的なセットと 4 つの Remote Monitoring（RMON; リモート モニタリング）グループをサポートしています。SNMP の詳しい使用方法については、第 36 章「SNMP の設定」を参照してください。
- Cisco IOS Configuration Engine（旧称 Cisco IOS CNS エージェント）：コンフィギュレーション サービスにより、ネットワーク装置およびサービスの配置と管理が自動化されます。スイッチ固有の設定変更を生成し、それらをスイッチに送信し、設定変更を実行し、結果をログに記録することで、初期設定と設定更新を自動化できます。

  CNS の詳細については、第 5 章「Cisco IOS Configuration Engine の設定」を参照してください。
- CIP：Common Industrial Protocol（CIP）はピアツーピアのアプリケーション プロトコルであり、スイッチと工業用装置（I/O コントローラ、センサー、リレーなど）間でアプリケーション レベルの接続を実現します。CIP ベースの管理ツール（RSLogix など）を使用してスイッチを管理できます。スイッチでサポートされる CIP コマンドの詳細については、コマンド リファレンスを参照してください。
- Common Industrial Protocol（CIP）の機能拡張により、CIP で DHCP パラメータを設定できるようになりました。

管理機能

- CNS 組み込みエージェントにより、スイッチの管理、設定の保管、および配信を自動化できます。
- DHCP により、スイッチ情報（IP アドレス、デフォルト ゲートウェイ、ホスト名、Domain Name System（DNS; ドメイン ネーム システム）、TFTP サーバ名など）の設定を自動化できます。
- DHCP リレーにより、IP アドレス要求を含む User Datagram Protocol（UDP）ブロードキャストを DHCP クライアントから転送します。
- DHCP サーバにより、IP アドレスなどの DHCP オプションを IP ホストに自動的に割り当てます。
- DHCP ベースの自動設定とイメージ更新により、指定の設定と新しいイメージを多数のスイッチにダウンロードできます。
- DHCP サーバのポート ベースのアドレス割り当てにより、IP アドレスをスイッチ ポートに事前に割り当てることができます。
- ユニキャスト要求を DNS サーバに転送することにより、スイッチの IP アドレスとそれに対応するホスト名でスイッチを識別できます。また、ユニキャスト要求を TFTP サーバに転送することにより、TFTP サーバからソフトウェア アップグレードを管理できます。
- Address Resolution Protocol（ARP; アドレス解決プロトコル）により、スイッチの IP アドレスとそれに対応する MAC アドレスでスイッチを識別できます。
- ユニキャスト MAC アドレス フィルタリングにより、特定の送信元または宛先 MAC アドレスを持つパケットを廃棄できます。
- MAC アドレス スケーリングを設定することにより、VLAN 上で MAC アドレス学習をディセーブルにして、MAC アドレス テーブルのサイズを制限できます。

- Cisco Discovery Protocol（CDP; シスコ検出プロトコル）バージョン 1 および 2 により、ネットワーク上にあるスイッチと他のシスコ デバイス間のネットワーク トポロジを検出およびマッピングできます。
- Link Layer Discovery Protocol（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）により、サードパーティ製の IP 電話とのインターオペラビリティを実現します。
- LLDP メディア拡張（LLDP-MED）のロケーション TLV により、スイッチからエンドポイント装置までのロケーション情報が提供されます。
- CDP および LLDP 拡張のサポートにより、サーバからの動的ロケーション ベースのコンテンツ配布用にビデオ エンド ポイントとロケーション情報を交換できます。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）により、すべてのスイッチで一貫したタイム スタンプが外部ソースから提供されます。
- IEEE 1588 標準で定められた Precision Time Protocol（PTP; 高精度時間プロトコル）により、ネットワーク内の装置のリアルタイム クロックをナノ秒精度で同期できます。
- Cisco IOS File System（IFS）により、スイッチが使用するすべてのファイル システムに単一のインターフェイスが提供されます。
- SSM PIM プロトコルのサポートにより、ビデオなどのマルチキャスト アプリケーションを最適化できます。
- マルチキャスト アプリケーション用の Source Specific Multicast（SSM）マッピングにより、ソースとグループをマッピングしてリスナーがマルチキャスト ソースにダイナミックに接続できるようにし、アプリケーションへの依存を軽減します。
- Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 のサポートにより、IPv6 トランスポートの利用、IPv6 ピアとの通信、および IPv6 ルートのアドバタイズを実行できます。
- HSRP、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute、ping の各 IP サービスのサポートにより、これらを VRF 認識にして、複数のルーティング インスタンスで動作できるようにします。
- コンフィギュレーション ロギングにより、スイッチ設定の変更をログに記録および表示できます。
- 固有の装置 ID により、**show inventory** ユーザ EXEC コマンド出力を通じて製品の ID 情報が提供されます。
- Netscape Navigator または Microsoft Internet Explorer のブラウザ セッション上で、デバイス マネージャを通じて帯域内管理アクセスできます。
- ネットワーク上で CLI ベースのセッションを複数実行するために、同時に最大 16 の Telnet 接続に対して帯域内管理アクセスできます。
- ネットワーク上で CLI ベースのセッションを複数実行するために、同時に最大 5 つの暗号化 Secure Shell（SSH; セキュア シェル）接続に対して帯域内管理アクセスできます。
- SNMP バージョン 1、2c、3 の get 要求と set 要求を通じて帯域内管理アクセスできます。
- スイッチ コンソール ポートを通じて、直接接続された端末またはシリアル接続やモデムを介したリモート端末に帯域外管理アクセスできます。
- Secure Copy Protocol（SCP）機能により、セキュアかつ認証済みの方法でスイッチ設定またはスイッチ イメージ ファイルをコピーできます（暗号化バージョンのソフトウェアが必要）。
- コンフィギュレーションの交換とロールバックにより、スイッチ上で実行中の設定を、任意の保存済み Cisco IOS コンフィギュレーション ファイルと交換することができます。
- Cisco IOS サポートの HTTP クライアントは IPv4 と IPv6 の両方の HTTP サーバに要求を送信でき、Cisco IOS の HTTP サーバは IPv4 と IPv6 の両方の HTTP クライアントからの HTTP 要求を処理できます。

- IPv6 ホストが、IPv6 を実行している装置へ SNMP クエリーを送信したり、その装置から SNMP 通知を受信したりできるように、IPv6 トランスポート上で Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を設定できます。
- IPv6 ステートレス自動設定により、リンク、サブネット、サイトのアドレッシング変更を管理できます（ホストおよびモバイル IP アドレスの管理など）。
- VLAN 上で MAC アドレス学習をディセーブル化できます。
- DHCP サーバのポート ベースのアドレス割り当てにより、IP アドレスをスイッチ ポートに事前に割り当てることができます。
- 有線ロケーション サービスにより、接続されているデバイスのロケーション情報およびアタッチメント追跡情報を Cisco Mobility Services Engine（MSE）に送信します。
- CPU 使用率スレッシュホールド トラップにより、CPU の使用率をモニタします。
- LLDP-MED ネットワークポリシー プロファイルの Time, Length, Value（TLV; 時間、長さ、値）により、VLAN、Class of Service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP）、およびタギング モードの値を指定して、音声と音声信号のプロファイルを作成できます。
- DHCPDISCOVER パケットの Option 12 フィールドにホスト名を含めることができます。これにより、DHCP プロトコルを使用して同一の設定ファイルが送信されます。
- DHCP スヌーピング拡張により、オプション 82 DHCP フィールドで circuit-id サブオプションに固定文字列ベースの形式の選択がサポートされます。
- PROFINET IO（分散型オートメーション アプリケーション用のモジュラー通信フレームワーク）をサポートします。スイッチから IO コントローラへの PROFINET 管理接続が可能です。

アベイラビリティ機能および冗長性機能

- HSRP により、コマンド スイッチおよびレイヤ 3 ルータの冗長構成が可能です（IP サービス イメージが必要）
- 拡張オブジェクト追跡により、HSRP から追跡メカニズムが分離され、HSRP 以外のプロセスで使用できる個別のスタンドアロン追跡プロセスが作成されます（IP サービス イメージが必要）。
- UniDirectional Link Detection（UDLD; 単方向リンク検出）およびアグレッシブ UDLD により、間違った光ファイバ配線やポート障害によって発生する光ファイバ インターフェイス上の単方向リンクを検出し、ディセーブルにすることができます。
- IEEE 802.1D Spanning Tree Protocol（STP; スパニング ツリー プロトコル）により、冗長構成のバックボーン接続とループフリー ネットワークを実現します。STP には次の機能があります。
  - 最大 128 のスパニング ツリー インスタンスがサポートされます。
  - Per-VLAN Spanning-Tree Plus（PVST+）により、VLAN 間のロード バランシングを実行できます。
  - Rapid PVST+ により、VLAN 間のロード バランシングを実行し、スパニング ツリー インスタンスの高速コンバージェンスを実現します。
  - UplinkFast および BackboneFast により、スパニング ツリー トポロジの変更後に高速コンバージェンスを実現し、ギガビット アップリンクを含む冗長アップリンク間のロード バランシングを実行できます。
- IEEE 802.1s Multiple Spanning Tree Protocol（MSTP）により、VLAN をスパニング ツリー インスタンスにグループ化し、データ トラフィックとロード バランシング用に複数の転送パスを提供できます。また、IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）ベースの Rapid Per-VLAN Spanning Tree Plus（Rapid PVST+）により、ルートおよび指定ポートを直ちにフォワーディング ステートに変更して、スパニング ツリーの高速コンバージェンスを実現します。

- PVST+、Rapid-PVST+、および MSTP モードで使用可能なオプションのスパニング ツリー機能は次のとおりです。
  - PortFast により、ポートがブロッキング ステートからフォワーディング ステートに直ちに変更できるようにして、転送遅延を解消できます。
  - BPDU ガードにより、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）を受信する PortFast 対応ポートをシャットダウンできます。
  - BPDU フィルタリングにより、PortFast 対応ポートが BPDU を送受信できないようにします。
  - ルート ガードにより、ネットワーク コアの外部にあるスイッチがスパニング ツリー ルートとして使用されないようにします。
  - ループ ガードにより、単一方向リンクの原因となる障害によって代替ポートまたはルート ポートが指定ポートとして使用されないようにします。
- 等価コスト ルーティングにより、リンクレベルおよびスイッチレベルの冗長性を実現します（IP サービス イメージが必要）。
- Flex Link レイヤ 2 インターフェイスは、互いをバックアップすることにより、STP の代替として基本的なリンクの冗長構成を実現します。
- リンクステート トラッキングにより、接続されたホストとサーバからのアップストリーム トラフィックを伝送するポートのステートをミラーリングし、サーバ トラフィックを別のシスコ製イーサネット スイッチ上の動作リンクにフェールオーバーできるようにします。
- 短い Resilient Ethernet Protocol（REP）hello：REP Link Status Layer（LSL; リンク ステータス レイヤ）のエージング タイマーの範囲を 3000 ～ 10000 ms（500 ms 間隔）から 120 ～ 10000 ms（40 ms 間隔）に変更します。

VLAN 機能

- 最大 1005 の VLAN のサポートにより、適切なネットワーク リソース、トラフィック パターン、および帯域幅と関連付けて、VLAN にユーザを割り当てることができます。
- IEEE 802.1Q 標準で許可される、1 ～ 4094 の範囲の VLAN ID をサポートします。
- VLAN Query Protocol（VQP）により、ダイナミック VLAN メンバーシップに対応します。
- 全ポート上での IEEE 802.1Q トランキング カプセル化により、ネットワークの移動/追加/変更、ブロードキャスト トラフィックとマルチキャスト トラフィックの管理/制御、高セキュリティのユーザおよびネットワーク リソース用の VLAN グループの確立によるネットワーク セキュリティを実現します。
- Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）により、2 つの装置間のリンク上でトランキングをネゴシエートし、使用するトランキング カプセル化のタイプ（IEEE 802.1Q）をネゴシエートします。
- VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）および VTP プルーニングにより、トラフィックを受信するステーション宛てのリンクにフラッディング トラフィックを制限することでネットワーク トラフィックを低減できます。
- 音声 VLAN により、Cisco IP Phone からの音声トラフィック用のサブネットを作成できます。

- VLAN 1 の削除により、任意の各 VLAN トランク リンク上で VLAN 1 をディセーブルにできるようにして、スパニング ツリー ループまたはストームのリスクを低減します。この機能がイネーブルの場合は、トランク上でユーザ トラフィックの送受信が行われません。スイッチの CPU は制御プロトコル フレームの送受信を継続します。
- プライベート VLAN により、VLAN のスケーラビリティ問題に対処し、制御性の高い IP アドレス割り当てを実現し、スイッチ上の他のポートからレイヤ 2 ポートを分離することができます（IP サービス イメージが必要）。
- PVLAN ホスト上のポート セキュリティにより、ポート上で学習する MAC アドレスの数を制限したり、ポート上で学習できる MAC アドレスを定義することができます。
- VLAN Flex Link ロード バランシングにより、スパニング ツリー プロトコル（STP）を必要とせずにレイヤ 2 の冗長構成を実現できます。プライマリ リンクおよびバックアップ リンクとして設定した 2 つのインターフェイス間で、VLAN ベースでトラフィックのロード バランシングを実行できます。
- 制限 VLAN（*認証失敗 VLAN* とも呼ばれる）での 802.1X 認証をサポートします。
- VTP バージョン 3 のサポートにより、任意の VTP モードでの拡張範囲 VLAN（VLAN 1006 ～ 4094）、機能強化された認証（非表示またはシークレット パスワード）、VTP 以外のデータベースの伝播、VTP プライマリおよびセカンダリ サーバ、ポートごとの VTP のオン / オフ切り替えオプションなどを設定できます。

セキュリティ機能

- IP サービス レベル契約（IP SLA）のサポートにより、アクティブなトラフィック モニタリングを使用してネットワーク パフォーマンスを測定できます（IP サービス イメージが必要）。
- IP SLA EOT により、スタンバイ ルータのフェールオーバー引き継ぎを行うために、遅延、ジッタ、パケット損失などのアクションによってトリガーされる IP SLA 追跡動作からの出力を使用できます（IP サービス イメージが必要）。
- Web 認証により、Web ブラウザを使用して、IEEE 802.1x 機能をサポートしていないサプリカント（クライアント）を認証できます。
- ローカルの Web 認証バナーにより、カスタム バナーやイメージ ファイルを Web 認証のログイン画面に表示できます。
- MAC Authentication Bypass（MAB; MAC 認証バイパス）のエージング タイマーにより、MAB を使用して認証済みの非アクティブ ホストを検出できます。
- 管理インターフェイス（デバイス マネージャ、Network Assistant、CLI）へパスワード保護付きアクセス（読み取り専用アクセス、読み取り / 書き込みアクセス）により、不正な設定変更を防ぎます。
- 複数レベルのセキュリティにより、セキュリティ レベル、通知、および対応するアクションを選択できます。
- スタティック MAC アドレッシングにより、セキュリティを実現します。
- 保護ポート オプションにより、同じスイッチ上の指定ポートへのトラフィック転送を制限できます。
- ポート セキュリティ オプションにより、ポートへのアクセスが許可されるステーションの MAC アドレスを制限および識別できます。
- VLAN 認識ポートのセキュリティ オプションにより、違反の発生時にポート全体をシャットダウンするのではなく、ポート上の VLAN をシャットダウンすることができます。
- ポート セキュリティ エージングにより、ポート上のセキュア アドレスにエージング タイムを設定できます。

- BPDU ガードにより、無効な設定が発生した場合に PortFast 設定ポートをシャットダウンできます。
- 標準および拡張 IP アクセス制御リスト（ACL）により、ルーテッド インターフェイス（ルータ ACL）と VLAN 上の双方向、およびレイヤ 2 インターフェイス上の受信方向（ポート ACL）に関するセキュリティ ポリシーを定義できます。
- 拡張 MAC アクセス制御リストにより、レイヤ 2 インターフェイス上の受信方向でセキュリティ ポリシーを定義できます。
- VLAN ACL（VLAN マップ）により、MAC、IP、および TCP/UDP ヘッダー内の情報に基づいてトラフィックをフィルタリングすることで、VLAN 内のセキュリティを実現できます（IP サービス イメージが必要）。
- 送信元および宛先 MAC ベースの ACL により、非 IP トラフィックをフィルタリングできます。
- IPv6 ACL をインターフェイスに適用して、IPv6 トラフィックをフィルタリングできます（IP サービス イメージが必要）。
- DHCP スヌーピングにより、信頼できないホストと DHCP サーバ間で、信頼できない DHCP メッセージをフィルタリングできます。
- IP ソース ガードにより、DHCP スヌーピング データベースと IP 送信元バインディングに基づいてトラフィックをフィルタリングすることで、非ルーテッド インターフェイス上のトラフィックを制限できます。
- ダイナミック ARP インスペクションにより、無効な ARP 要求と ARP 応答を同じ VLAN 内の他のポートにリレーしないことで、スイッチに対する悪意ある攻撃を防止できます。
- IEEE 802.1Q トンネリングにより、サービス プロバイダー ネットワークを介したリモート サイトのユーザがいるカスタマーが、VLAN を他のカスタマーから分離することができます。また、レイヤ 2 プロトコル トンネリングにより、カスタマーのネットワークで全ユーザに関する完全な STP、CDP、および VTP 情報を取得することができます（IP サービス イメージが必要）。
- レイヤ 2 ポイントツーポイント トンネリングにより、EtherChannels を自動的に作成できます（IP サービス イメージが必要）。
- レイヤ 2 プロトコル トンネリング バイパス機能により、サードパーティ ベンダーとの相互運用性を実現します。
- IEEE 802.1x ポートベースの認証により、無認可の装置（クライアント）によるネットワークへのアクセスを防止します。次の機能がサポートされます。
  - Multidomain Authentication（MDA; マルチドメイン認証）により、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方が、同じ IEEE 802.1x 対応スイッチ ポート上で独立して認証を行うことができます。
  - MDA 対応のダイナミック音声 VLAN により、MDA 対応ポート上でダイナミック音声 VLAN を実現できます。
  - VLAN 割り当てにより、802.1x で認証されたユーザを指定の VLAN に制限できます。
  - マルチ認証モード用に設定されたポートでの VLAN 割り当てをサポートします。RADIUS サーバが VLAN をポートで最初のホストに割り当てて認証を行い、後続のホストは同じ VLAN を使用します。音声 VLAN 割り当ては、1 台の IP Phone に対してサポートされます。
  - ポート セキュリティにより、802.1x ポートへのアクセスを制御できます。
  - 音声 VLAN により、ポートが認可ステートか無認可ステートかを問わず、Cisco IP Phone から音声 VLAN へのアクセスを許可できます。
  - IP Phone 検出機能拡張により、Cisco IP Phone の検出と認識を行うことができます。
  - ゲスト VLAN により、802.1x に準拠していないユーザに限定的なサービスを提供できます。

  - 制限 VLAN により、802.1x には準拠しているが、標準の 802.1x プロセスで認証するためのクレデンシャルを持たないユーザに、限定的なサービスを提供できます。
  - 802.1x アカウンティングにより、ネットワークの使用状況を追跡できます。
  - 802.1x と Wake-on-LAN（WoL）により、特定のイーサネット フレームの受信に基づいて、休止中の PC を起動できます。
  - 802.1x 準備状態チェックにより、スイッチ上で IEEE 802.1x を設定する前に、接続されたエンド ホストの準備状態を判別できます。
  - 音声認識 802.1x セキュリティにより、セキュリティ違反が発生した VLAN 上だけでトラフィック違反アクションを適用できます。
  - MAC 認証バイパスにより、クライアント MAC アドレスに基づいてクライアントを認可できます。
  - 802.1X スイッチ サプリカントを使用した Network Edge Access Topology（NEAT; ネットワーク エッジ アクセス トポロジ）、CISP を使用したホスト認可、および自動イネーブル化により、ワイヤリング クローゼットの外部にあるスイッチを別のスイッチのサプリカントとして認証できます。
  - IEEE 802.1x とオープン アクセスにより、認証前にホストからネットワークにアクセスできます。
  - ダウンロード可能 ACL とリダイレクト URL を使用した IEEE 802.1x 認証により、Cisco Secure ACS サーバから認証済みスイッチにユーザごとの ACL をダウンロードできます。
  - 柔軟な認証シーケンス設定により、新しいホストの認証時にポートが試行する認証方式の順序を設定できます。
  - 複数ユーザの認証により、802.1x 対応ポート上で複数のホストが認証を実行できます。
- Network Admission Control（NAC）の機能は次のとおりです。
  - NAC レイヤ 2 802.1x 検証により、装置にネットワーク アクセス権を与える前に、エンドポイント システムまたはクライアントのアンチウイルス状態または*ポスチャ*を検証します。

    NAC レイヤ 2 802.1x 検証の設定については、「NAC レイヤ 2 802.1X 検証の設定」（P.12-59）を参照してください。
  - NAC レイヤ 2 IP 検証により、装置にネットワーク アクセス権を与える前に、エンドポイント システムまたはクライアントのポスチャを検証します。

    NAC レイヤ 2 IP 検証の設定については、『*Network Admission Control Software Configuration Guide*』を参照してください。
  - IEEE 802.1x アクセス不能認証バイパス。

    この機能の設定については、「アクセス不能認証バイパス機能の設定」（P.12-54）を参照してください。
  - ホストの NAC レイヤ 2 IP 検証に関する Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）ダウン ポリシー（ポスチャ検証の発生時に AAA サーバが使用できない場合）。

    この機能の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- 自社開発機能の TACACS+ により、TACACS サーバを通じてネットワーク セキュリティを管理できます。
- RADIUS により、AAA サービスを通じてリモート ユーザの ID の確認、アクセス権の付与、アクションの追跡を実行できます。
- Kerberos セキュリティ システムにより、信頼できるサードパーティを使用して、ネットワーク リソースの要求を認証できます（暗号化バージョンのソフトウェアが必要）。

- Secure Socket Layer（SSL; セキュア ソケット レイヤ）バージョン 3.0 により、HTTP 1.1 サーバ認証、暗号化、メッセージ完全性および HTTP クライアント認証がサポートされ、セキュアな HTTP 通信が実現されます（暗号化バージョンのソフトウェアが必要）。
- 音声認識 IEEE 802.1x および MAC 認証バイパス（MAB）のセキュリティ違反機能により、セキュリティ違反の発生時にポート上でデータ VLAN だけをシャットダウンできます。
- スタティック ホスト上での IP ソース ガードをサポートします。
- RADIUS Change of Authorization（CoA）により、特定のセッションの認証後にそのセッションの属性を変更できます。AAA でユーザまたはユーザ グループに関するポリシーが変更された場合、管理者は Cisco Secure ACS などの AAA サーバから RADIUS CoA パケットを送信して認証を再初期化し、新しいポリシーに適用することができます。
- IEEE 802.1X ユーザ分散により、（ユーザ グループ用に）複数の VLAN を使用した配置が可能になり、異なる VLAN 間でユーザのロード バランシングを行うことで、ネットワークのスケーラビリティを向上できます。認可されたユーザは、RADIUS サーバによって割り当てられた、グループ内で最もユーザ数の少ない VLAN に割り当てられます。
- 複数のホストの認証を使用したクリティカル VLAN のサポートにより、ポートが multi-auth に設定されていて、AAA サーバが到達不能になった場合、クリティカル リソースへのアクセスを引き続き許可するために、そのポートがクリティカル VLAN に配置されます。
- カスタマイズ可能な Web 認証の機能拡張により、ローカルの Web 認証用にユーザ定義の *ログイン*、*成功*、*失敗*、*期限切れ*の各 Web ページを作成できます。
- ネットワーク エッジ アクセス トポロジ（NEAT）のサポートにより、ポートのホスト モードを変更し、オーセンティケータのスイッチ ポート上で標準のポート設定を適用することができます。
- VLAN ID ベースの MAC 認証により、VLAN と MAC アドレスの組み合わせ情報をユーザ認証に使用して、無認可の VLAN からのネットワーク アクセスを防止することができます。
- MAC 移行により、ホスト（IP 電話の背後で接続されているホストを含む）が同じスイッチ内のポートを制約なしで移行して、モビリティを実現できます。MAC 移行を使用すると、スイッチは別のポート上で同じ MAC アドレスを検出しても、まったく新しい MAC アドレスと同様に扱います。
- 簡易ネットワーク管理プロトコル バージョン 3（SNMPv3）で 3DES および AES をサポートします。このリリースでは、168 ビットの Triple Data Encryption Standard（3DES）と、128 ビット、192 ビット、256 ビットの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムが SNMPv3 に追加されています。

QoS 機能および CoS 機能

- Automatic QoS（auto-QoS）により、トラフィックを分類し、出力キューを設定することで、既存の QoS 機能を容易に配置できます。
- Automatic Quality Of Service（QoS）Voice over IP（VoIP）の機能拡張により、ポートベースで DSCP を信頼し、出力トラフィックのプライオリティ キューイングを実行することができます。
- 分類
  - ポートごとの IP Type-of-Service/Differentiated Services Code Point（IP ToS/DSCP）および IEEE 802.1p CoS マーキング プライオリティにより、基幹業務アプリケーションのパフォーマンスを保護できます。
  - フローベースのパケット分類（MAC、IP、および TCP/UDP ヘッダー内の情報に基づく分類）に基づく IP ToS/DSCP および IEEE 802.1p CoS マーキングにより、ネットワーク エッジでハイパフォーマンスの Quality of Service を実現して、各種ネットワーク トラフィックに合わせたサービス レベルの差別化を可能にし、ネットワーク内の基幹業務トラフィックを優先することができます。

  - QoS ドメイン内で、別の QoS ドメインと隣接するポートを使用して、信頼できるポート ステート（CoS、DSCP、および IP precedence）を実現します。
  - 信頼境界により、Cisco IP Phone の存在を検出し、受信した CoS 値を信頼して、ポート セキュリティを実現することができます。
- ポリシング
  - スイッチ ポート上のトラフィック ポリシング ポリシーにより、特定のトラフィック フローに割り振るべきポート帯域幅の量を管理できます。
  - 階層ポリシー マップに複数のクラス マップを設定する場合、各クラス マップを専用のポート レベル（第 2 レベル）のポリシー マップと関連付けることができます。第 2 レベルの各ポリシー マップには、異なるポリサーを使用できます。
  - 集約ポリシングにより、集約内のトラフィック フローをポリシングして、特定のアプリケーションやトラフィック フローを計測済みの事前定義レートに制限することができます。
- 不適合
  - 帯域幅利用限度を超えているパケットに対して、不適合マークダウンを行います。
- 入力キューイングおよびスケジューリング
  - ユーザ トラフィックに対して、2 つの入力キューを設定できます（一方のキューをプライオリティ キューに設定できます）。
  - 輻輳回避メカニズムとしての Weighted Tail Drop（WTD）により、キューの長さを管理して、さまざまなトラフィック分類の廃棄優先度を設定できます。
  - スケジューリング サービスとして Shaped Round Robin（SRR; シェイプド ラウンド ロビン）を使用することにより、パケットが内部リングに送信される際のレートを指定できます（入力キューでサポートされるモードは共有だけです）。
- 出力キューおよびスケジューリング
  - ポートあたり 4 つの出力キューを使用できます。
  - 輻輳回避メカニズムとして WTD を使用することにより、キューの長さを管理して、さまざまなトラフィック分類の廃棄優先度を設定できます。
  - スケジューリング サービスとして SRR を使用することにより、出力インターフェイスにパケットが送り出される際のレートを指定できます（出力キューではシェーピングまたは共有がサポートされます）。シェーピングされた出力キューには割り当て分のポート帯域幅が保証されますが、その帯域幅しか使用できません。シェーピングされた出力キューには設定済みの割り当て帯域幅も保証されますが、他のキューが空になり、それらのキューの割り当て帯域幅が使用されていない場合は、保証分以上の帯域幅を使用することができます。
- auto-QoS 拡張によって、ビデオ装置（Cisco Telepresence System や Cisco Surveillance Camera など）からのトラフィック フローの自動設定分類が追加されます。

レイヤ 3 機能

（注）　ここに記載する機能は、IP サービス イメージだけで使用できます。

- HSRP バージョン 1（HSRPv1）および HSRP バージョン 2（HSRPv2）により、レイヤ 3 ルータの冗長構成を実現できます。

- IP ルーティング プロトコルにより、ロード バランシングを実行し、拡張可能なルーテッド バックボーンを構築することができます。
  - RIP バージョン 1 および 2。
  - 完全な OSPF（IP サービス フィーチャ セットが必要）

    Cisco IOS Release 12.2(55)SE 以降、IP ベース フィーチャ セットによって、レイヤ 3 ルーティング機能をアクセスまたはワイヤリング クローゼットに拡張できるようにするルーテッド アクセス対応の OSPF がサポートされています。
  - Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6 により、IPv6 トランスポートの利用、IPv6 ピアとの通信、および IPv6 ルートのアドバタイズを実行できます。
  - HSRP for IPv6。
  - Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）バージョン 4。
- VLAN 間の IP ルーティング（VLAN 間ルーティング）により、2 つ以上の VLAN 間で完全なレイヤ 3 ルーティングが実現され、各 VLAN で専用の自律データリンク ドメインを維持できるようになります。
- Policy-Based Routing（PBR; ポリシーベース ルーティング）により、トラフィック フローに対して定義済みのポリシーを設定できます。
- カスタマー エッジ装置内の Multiple VPN Routing/Forwarding（multi-VRF）インスタンスにより、サービス プロバイダーが複数の Virtual Private Networks（VPN; 仮想私設網）をサポートし、VPN 間で IP アドレスが重複できるようにします。
- フォールバック ブリッジングにより、2 つ以上の VLAN 間で非 IP トラフィックを転送できます。
- スタティック IP ルーティングにより、ネットワーク パス情報のルーティング テーブルを手動で作成できます。
- 等価コスト ルーティングにより、ロード バランシングを実行して冗長構成を実現することができます。
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）および ICMP Router Discovery Protocol（IRDP）により、ルータ アドバタイズ メッセージとルータ請求メッセージを使用して、直接接続されたサブネット上のルータのアドレスを検出できます。
- Protocol-Independent Multicast（PIM）により、ネットワーク内でマルチキャスト ルーティングを実現し、ネットワーク内の装置が要求されたマルチキャスト フィードを受信でき、マルチキャストに参加していないスイッチがプルーニングされるようにします。PIM Sparse Mode（PIM-SM; PIM sparse（疎）モード）、PIM Dense Mode（PIM-DM; PIM dense（密）モード）、および PIM sparse-dense モードのサポートが含まれます。
- Multicast Source Discovery Protocol（MSDP）により、複数の PIM-SM ドメインを接続できます。
- Distance Vector Multicast Routing Protocol（DVMRP）トンネリングにより、非マルチキャスト ネットワークを経由した 2 つのマルチキャスト対応ネットワーク間のインターオペラビリティが実現されます。
- DHCP リレーにより、IP アドレス要求を含む UDP ブロードキャストを DHCP クライアントから転送できます。
- DHCP for IPv6 リレー、クライアント、サーバのアドレス割り当てとプレフィクスの委任を実行できます。
- IPv6 ユニキャスト ルーティング機能により、設定したインターフェイスを通じて IPv6 トラフィックを転送できます。
- IPv6 Default Router Preference（DRP; デフォルト ルータ プリファレンス）により、ホストが適切なルータを選択する機能を強化できます。

- Nonstop Forwarding（NSF; ノンストップ フォワーディング）認識により、プライマリ Route Processor（RP; ルート プロセッサ）に障害が発生したためにバックアップ RP が引き継ぐ場合や、中断のないソフトウェア アップグレードのためにプライマリ RP が手動でリロードされる場合に、レイヤ 3 スイッチが NSF 対応のネイバー ルータからパケット転送を継続できるようにします。
- SVI ラインステート アップ/ダウン計算から、VLAN 内のポートを除外できます。
- Intermediate System-to-Intermediate System（IS-IS）ルーティングにより、Connectionless Network Service（CLNS; コネクションレス型ネットワーク サービス）ネットワーク対応のダイナミック ルーティング プロトコルがサポートされます。

モニタリング機能

- EOT および IP SLA EOT スタティック ルートにより、事前設定されたスタティック ルートや DHCP ルートがダウンした場合にそれを判別できます。
- デバイスおよびシステム管理用の Embedded Event Manager（EEM; 組み込みイベント マネージャ）により、主要なシステム イベントをモニタし、ポリシーを使用して処理できます。
- MAC アドレス通知トラップおよび RADIUS アカウンティングにより、スイッチが学習または削除した MAC アドレスを保管することで、ネットワーク上のユーザを追跡できます。
- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）および Remote SPAN（RSPAN; リモート SPAN）により、任意のポートまたは VLAN 上でトラフィックをモニタできます。
- SPAN および RSPAN の Intrusion Detection System（IDS; 侵入検知システム）サポートにより、ネットワーク セキュリティ違反のモニタ、撃退、レポートを実行できます。
- 組み込み RMON エージェントの 4 つのグループ（履歴、統計、アラーム、イベント）により、ネットワークのモニタとトラフィック分析を実行できます。
- Syslog 機能により、認証または認可エラー、リソースの問題、タイムアウト イベントに関するシステム メッセージをログに記録できます。
- レイヤ 2 traceroute により、パケットが送信元装置から宛先装置に送られる際の物理パスを識別できます。
- Time Domain Reflector（TDR）により、銅線のイーサネット 10/100 および 10/100/1000 ポート上のケーブル接続の問題を診断し、解決することができます。
- SFP モジュール診断管理インターフェイスにより、SFP モジュールの物理ステータスまたは動作ステータスをモニタできます。
- 温度、電源状態、イーサネット ポートのステータスに関するアラームの処理機能が備わっています。
- 外部のリレー システムに使用できるアラーム リレー接点が備わっています。
- On-Board Failure Logging（OBFL）により、スイッチとそれに接続されている電源装置の情報を収集します（Catalyst 2960-S のみ）。
- HSRP 対応のオブジェクト追跡が機能強化されています。
- Digital Optical Monitoring（DOM）により、X2 SFP（着脱可能小型フォーム ファクタ）モジュールのステータスをチェックできます。

スイッチの初期設定後のデフォルト設定

このスイッチはプラグアンドプレイ動作に対応しているため、スイッチに基本 IP 情報を割り当て、ネットワーク内の他の装置に接続するだけで済みます。特定のネットワーク要件がある場合は、インターフェイス固有の設定およびシステム規模の設定を変更できます。

（注） ブラウザベースの Express Setup プログラムを使用した IP アドレスの割り当てについては、クイック スタート ガイドを参照してください。CLI ベースのセットアップ プログラムを使用した IP アドレスの割り当てについては、ハードウェア インストレーション ガイドを参照してください。

スイッチの設定を行わない場合、スイッチは次のデフォルト設定で動作します。

- スイッチのデフォルトの IP アドレス、サブネット マスク、およびデフォルト ゲートウェイは 0.0.0.0 です。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- デフォルトのドメイン名は設定されていません。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」を参照してください。
- DHCP クライアントはイネーブル、DHCP サーバはイネーブル（DHCP サーバとして動作する装置が設定済みでイネーブルの場合だけ）、DHCP リレー エージェントはイネーブル（DHCP リレー エージェントとして動作する装置が設定済みでイネーブルの場合だけ）です。詳細については、第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」および第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- スイッチ クラスタはディセーブルです。スイッチ クラスタの詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com で入手可能な『*Getting Started with Cisco Network Assistant*』を参照してください。
- パスワードは定義されていません。詳細については、第 7 章「スイッチの管理」を参照してください。
- システム名とプロンプトは *Switch* です。詳細については、第 7 章「スイッチの管理」を参照してください。
- NTP はイネーブルです。詳細については、第 7 章「スイッチの管理」を参照してください。
- DNS はイネーブルです。詳細については、第 7 章「スイッチの管理」を参照してください。
- TACACS+ はディセーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- RADIUS はディセーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- 標準 HTTP サーバと Secure Socket Layer（SSL）HTTPS サーバはどちらもイネーブルです。詳細については、第 11 章「スイッチベース認証の設定」を参照してください。
- IEEE 802.1x はディセーブルです。詳細については、第 12 章「IEEE 802.1X ポートベースの認証の設定」を参照してください。
- ポート パラメータ
  - 動作モードはレイヤ 2（switchport）です。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
  - インターフェイス速度とデュプレックス モードは自動ネゴシエーションです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
  - Auto MDIX は、イネーブルです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。

  - フロー制御はオフです。詳細については、第 14 章「インターフェイスの特性の設定」を参照してください。
- VLAN
  - デフォルトの VLAN は VLAN 1 です。詳細については、第 16 章「VLAN の設定」を参照してください。
  - VLAN トランキング設定は dynamic auto（DTP）です。詳細については、第 16 章「VLAN の設定」を参照してください。
  - トランク カプセル化はネゴシエーションです。詳細については、第 16 章「VLAN の設定」を参照してください。
  - VTP モードはサーバです。詳細については、第 17 章「VTP の設定」を参照してください。
  - VTP バージョンはバージョン 1 です。詳細については、第 17 章「VTP の設定」を参照してください。
  - プライベート VLAN は設定されていません。詳細については、第 19 章「プライベート VLAN の設定」を参照してください。
  - 音声 VLAN はディセーブルです。詳細については、第 18 章「音声 VLAN の設定」を参照してください。
- IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングはディセーブルです。詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。
- STP、PVST+ は VLAN 1 上でイネーブルです。詳細については、第 21 章「STP の設定」を参照してください。
- MSTP はディセーブルです。詳細については、第 22 章「MSTP の設定」を参照してください。
- オプションのスパニング ツリー機能はディセーブルです。詳細については、第 23 章「オプションのスパニング ツリー機能の設定」を参照してください。
- Flex Link は設定されていません。詳細については、第 25 章「Flex Link および MAC アドレス テーブル移行更新機能の設定」を参照してください。
- DHCP スヌーピングは、ディセーブルです。DHCP スヌーピング情報オプションはイネーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- IP ソース ガードはディセーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- DHCP サーバ ポートベースのアドレス割り当てはディセーブルです。詳細については、第 26 章「DHCP 機能と IP ソース ガード機能の設定」を参照してください。
- ダイナミック ARP インスペクションはすべての VLAN 上でディセーブルです。詳細については、第 27 章「ダイナミック ARP 検査の設定」を参照してください。
- IGMP スヌーピングはイネーブルです。IGMP のフィルタは適用されていません。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スロットリング設定は拒否です。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- IGMP スヌーピング クエリア機能はディセーブルです。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。
- MVR はディセーブルです。詳細については、第 28 章「IGMP スヌーピングおよび MVR の設定」を参照してください。

- ポート ベースのトラフィック
  - ブロードキャスト、マルチキャスト、およびユニキャスト ストーム制御はディセーブルです。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - 保護ポートは定義されていません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - ユニキャストおよびマルチキャスト トラフィック フラッディングはブロックされません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
  - セキュア ポートは設定されていません。詳細については、第 29 章「ポートベースのトラフィック制御の設定」を参照してください。
- CDP はイネーブルです。詳細については、第 32 章「CDP の設定」を参照してください。
- UDLD はディセーブルです。詳細については、第 33 章「UDLD の設定」を参照してください。
- SPAN および RSPAN はディセーブルです。詳細については、第 30 章「SPAN および RSPAN の設定」を参照してください。
- RMON はディセーブルです。詳細については、第 34 章「RMON の設定」を参照してください。
- Syslog メッセージはイネーブルで、コンソール上に表示されます。詳細については、第 35 章「システム メッセージ ロギングの設定」を参照してください。
- SNMP はイネーブルです（バージョン 1）。詳細については、第 36 章「SNMP の設定」を参照してください。
- ACL は設定されていません。詳細については、第 38 章「ACL によるネットワーク セキュリティの設定」を参照してください。
- QoS はディセーブルです。詳細については、第 39 章「QoS の設定」を参照してください。
- EtherChannels は設定されていません。詳細については、第 40 章「EtherChannel およびリンクステート トラッキングの設定」を参照してください。
- IP ユニキャスト ルーティングはディセーブルです。詳細については、第 41 章「IP ユニキャスト ルーティングの設定」を参照してください。
- IPv6 ユニキャスト ルーティングはディセーブルです。詳細については、第 42 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。
- HSRP グループは設定されていません。詳細については、第 45 章「HSRP の設定」を参照してください。
- IP マルチキャスト ルーティングはすべてのインターフェイス上でディセーブルです。詳細については、第 49 章「IP マルチキャスト ルーティングの設定」を参照してください。
- MSDP はディセーブルです。詳細については、第 50 章「MSDP の設定」を参照してください。
- フォールバック ブリッジングは設定されていません。詳細については、第 51 章「フォールバック ブリッジングの設定」を参照してください。

ネットワークの設定例

ここでは、ネットワーク設定の概念について説明し、スイッチを使用した専用ネットワーク セグメントの作成例と Fast Ethernet および Gigabit Ethernet 接続を通じたセグメントの相互接続例を示します。

スイッチを使用するための設計概念

ネットワーク ユーザ間でネットワーク帯域幅を取り合う状態になると、データの送受信に時間がかかるようになります。ネットワークの設定時には、ネットワーク ユーザに必要な帯域幅と、ユーザが利用するネットワーク アプリケーションの相対的なプライオリティを考慮します。

表 1-1 で、ネットワーク パフォーマンスの低下を引き起こす原因と、ネットワーク設定によってネットワーク ユーザが利用できる帯域幅を増やす方法について説明します。

表 1-1　ネットワーク パフォーマンスの向上

ネットワーク デマンド	推奨される設計方法
単一ネットワーク セグメント上のユーザ数過多、およびインターネットにアクセスするユーザ数の増加	• 小規模なネットワーク セグメントを作成して、帯域幅を共有するユーザ数を減らします。また、VLAN および IP サブネットを使用して、アクセス頻度の高いユーザと同じ論理ネットワーク内にネットワーク リソースを配置します。 • スイッチと接続先ワークステーションとの間で全二重動作を使用します。
• 新しい PC、ワークステーション、およびサーバの性能向上 • ネットワーク アプリケーション（大きな添付ファイル付き E メールなど）および帯域幅を大量に使用するアプリケーション（マルチメディアなど）からの帯域幅要求の増大	• グローバル リソース（ネットワーク ユーザが同等にアクセスできる必要のあるサーバやルータなど）を高速スイッチ ポートに直接接続して、ユーザが専用の高速セグメントを使用できるようにします。 • スイッチと接続先サーバおよびルータとの間で EtherChannel 機能を使用します。

ネットワークの設計時の考慮事項は、帯域幅だけではありません。ネットワーク トラフィックのプロファイルが発展してきたら、音声とデータの統合、マルチメディアの統合、アプリケーションの優先付け、セキュリティなどのアプリケーションをサポートできるネットワーク サービスの提供を検討してください。表 1-2 で、ネットワーク デマンドと各デマンドに対応する方法について説明します。

表 1-2　ネットワーク サービスの提供

ネットワーク デマンド	推奨される設計方法
マルチメディア アプリケーションにおける帯域幅の効率的な利用および基幹業務アプリケーションに対する帯域幅の保証	• IGMP スヌーピングを使用して、マルチメディアおよびマルチキャスト トラフィックを効率的に転送します。 • その他の QoS メカニズム（パケット分類、マーキング、スケジューリング、輻輳回避など）を使用して適切なプライオリティ レベルでトラフィックを分類し、それによって最大限の柔軟性と、基幹業務アプリケーション、ユニキャスト アプリケーション、マルチキャストおよびマルチメディア アプリケーションのサポートを実現します。 • MVR を使用して、マルチキャスト VLAN でマルチキャスト ストリームを連続送信すると同時に、帯域幅やセキュリティ上の理由から、それらのストリームを加入者 VLAN から分離します。
基幹業務アプリケーションを *常時オン* にするための、ネットワークの冗長構成と可用性に対する高いデマンド	• Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用して、クラスタ コマンド スイッチおよびルータを冗長構成にします。 • VLAN トランクおよび BackboneFast を使用して、アップリンク ポート上でトラフィックのロード バランシングを実行し、VLAN トラフィックの伝送時にポート コストが相対的に低いアップリンク ポートが選択されるようにします。

表 1-2　ネットワーク サービスの提供 （続き）

ネットワーク デマンド	推奨される設計方法
IP テレフォニーに対する高いデマンド	• QoS を使用して、輻輳中に IP テレフォニーなどのアプリケーションを優先付け、ネットワーク内の遅延とジッタの両方を制御できるようにします。 • 1 ポートあたり 2 つ以上のキューをサポートするスイッチを使用して、音声およびデータ トラフィックを IEEE 802.1p/Q に基づいてハイプライオリティかロープライオリティのいずれかとして優先付けます。このスイッチでは、ポートあたり少なくとも 4 つのキューをサポートしています。 • 音声 VLAN ID（VVID）を使用して、音声トラフィック用に個別の VLAN を提供します。
既存のインフラストラクチャを使用して、自宅やオフィスからインターネットまたはイントラネットに高速でデータおよび音声を転送するデマンドの増大	Catalyst Long-Reach Ethernet（LRE; 長距離イーサネット）スイッチを使用して、既存のインフラストラクチャ（既存の電話回線など）上で最大 15 Mb の IP 接続を提供します。 **（注）** LRE は、Catalyst 2900 LRE XL および Catalyst 2950 LRE スイッチで使用されているテクノロジーです。LRE の詳細については、これらのスイッチに固有のマニュアル セットを参照してください。

Ethernet-to-the-Factory アーキテクチャ

ここでは、Ethernet-to-the-Factory（EttF）アーキテクチャについて概説します。EttF は、オートメーション システムや制御システム内の装置やアプリケーションにネットワーク サービスとセキュリティ サービスを提供します。そして、それらをより大規模な企業ネットワークに統合します。

EttF アーキテクチャはさまざまなタイプの製造環境に応用できますが、産業タイプ、製造タイプ、および生産施設の規模に合わせて調整する必要があります。また、小規模ネットワーク（装置が 50 台未満）から中規模ネットワーク（装置が 200 台未満）および大規模ネットワーク（装置が最大 1000 台およびそれ以上）まで、さまざまな規模での配置が可能です。

EttF アーキテクチャには*ゾーン*と呼ばれる概念構造が含まれています。ゾーンとは、最上位となる企業レベルのスイッチおよびプロセスから、より詳細なプロセスを制御する最小の装置、あるいは工場のフロアにある装置に至るまでのさまざまな機能を区分するものです。図 1-1 を参照してください。

EttF アーキテクチャの詳細については、次の URL を参照してください。

http://wwwin.cisco.com/enterprise/solutions/manufacturing/solutions/ettf.shtml

企業ゾーン

*企業ゾーン*は、一元管理されている IT システムと機能で構成されます。企業リソース管理サービス、企業間（B2B）サービス、企業/顧客間（B2C）サービスなどの企業ネットワーク サービスへの有線およびワイヤレス アクセスが可能です。サイト ビジネス プランニングやロジスティクスなどの基本的なビジネス管理作業はここで実行され、標準の IT サービスに依存します。ゲスト アクセス システムは多くの場合ここに置かれますが、企業レベルでは実現しにくい柔軟性を得るために、より下位レベルのフレームワークに置かれることも珍しくありません。

非武装ゾーン

非武装ゾーン（DMZ）は、企業ゾーンと製造ゾーンの間でデータやサービスを共有するためのバッファを提供します。DMZ では、可用性の維持、セキュリティ上の脆弱性への対処、および適合認定の義務の遵守を行います。DMZ は、たとえば IT 部門と生産部門を分けるなど、組織的な管理区分を提供します。組織ごとに異なるポリシーの適用や組み込みが可能です。たとえば、製造部門では、IT 部門と異なるセキュリティ ポリシーを製造ゾーンに適用できます。

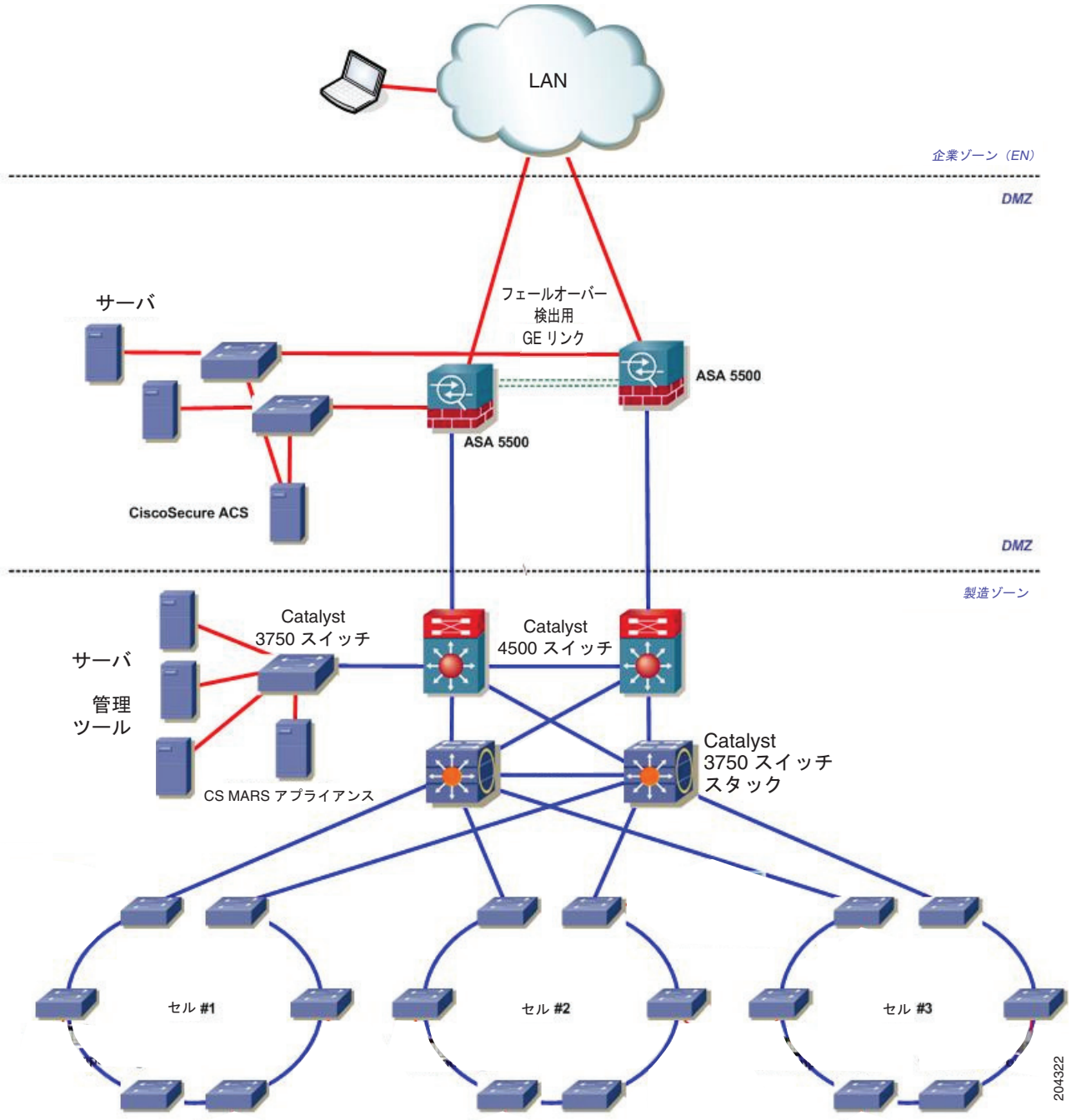
製造ゾーン

*製造ゾーン*は、セル ネットワークとサイトレベルのアクティビティで構成されます。工場のオペレーションをモニタするシステム、装置、コントローラはすべてこのゾーンに置かれます。生産施設内の 1 つの機能エリアを表すのが、セル ゾーンです。

セル ゾーンは、オートメーション プロセスの機能面をリアルタイムで制御する装置やコントローラなどで構成されます。これらはすべて互いにリアルタイム通信を行います。このゾーンは、工場や企業における他のレベルのオペレーションから明確に分離し、保護する必要があります。

図 1-1 に、EttF アーキテクチャを示します。

図 1-1　Ethernet-to-the-Factory アーキテクチャ



トポロジのオプション

トポロジの設計ではまず、装置をネットワークに接続する方法を検討します。セル ネットワークでは、生産フロアの物理的な制約に応じた物理トポロジも必要です。ここでは、トポロジの設計に関する注意事項を示し、トランク廃棄トポロジ、リング トポロジ、および冗長構成のスター トポロジについて説明します。

- 物理レイアウト：トポロジの設計は、生産環境のレイアウトに左右されます。たとえば、長いコンベアベルト システムにはトランク廃棄トポロジやリング トポロジが適していますが、冗長構成のスター トポロジは適していません。
- リアルタイム通信：遅延やジッタの主な発生原因は、トラフィックの量や、パケットが宛先に到達するまでに必要とするホップの数です。レイヤ 2 ネットワーク内のトラフィックの量はさまざまな要因に左右されますが、装置の数が重要となります。リアルタイム通信については、次の注意事項に従ってください。
  - レイヤ 2 ホップごとに生じる遅延の量を考慮してください。たとえば、100 Mb のインターフェイスを使用した場合は、1 ギガビットのインターフェイスを使用した場合に比べて遅延が大きくなります。
  - どのスイッチでも常に、帯域幅がインターフェイス キャパシティの 50% を継続的に超えることがないようにしてください。
  - CPU の使用率は、50 ～ 70% を継続的に超えることがないようにしてください。このレベルを超えると、スイッチが制御パケットを正しく処理できない可能性や、異常な動作をする可能性があります。

接続に関する主な考慮事項は次のとおりです。

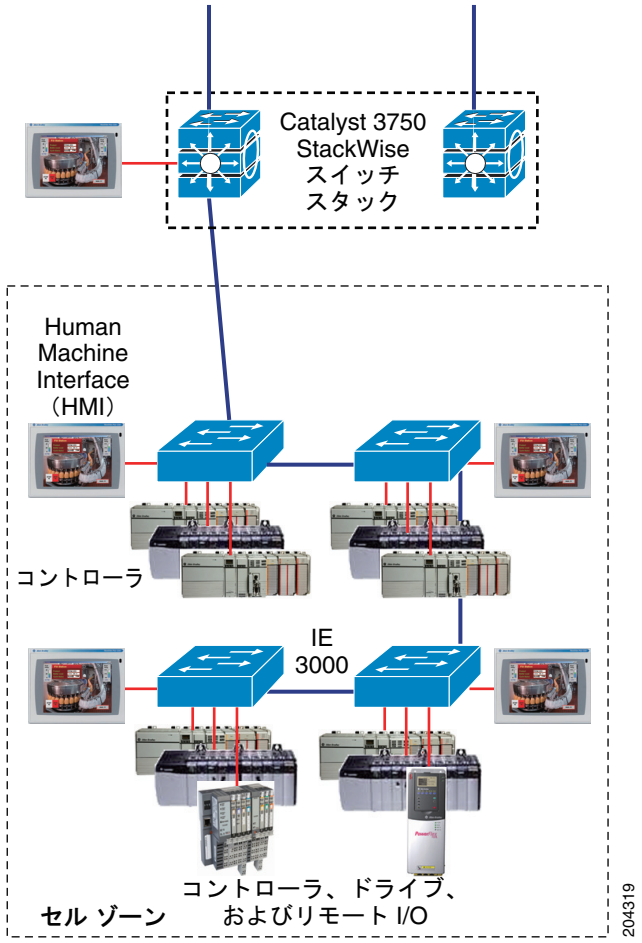
- 装置は、単一のネットワーク接続または IP 対応の I/O ブロックやリンク装置（イーサネットがサポートされていない場合）を通じてスイッチに接続されます。大半の装置にはフェールオーバー機能がないか、あっても機能が制限されているため、冗長構成のネットワーク接続を効果的に利用できません。
- 冗長構成の接続は、基幹インフラストラクチャに該当するプロセス関連の産業など、特定の産業やアプリケーションで利用されます。

セル ネットワーク：トランク廃棄トポロジ

*トランク廃棄*トポロジ（*カスケード*トポロジとも呼ばれる）では、スイッチが互いに接続され、スイッチ チェーンが形成されます。図 1-2 を参照してください。

- レイヤ 3 スイッチと最初のレイヤ 2 スイッチ間の接続はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。
- 接続損失に対する冗長構成はありません。

図 1-2　セル ネットワーク：トランク廃棄トポロジ

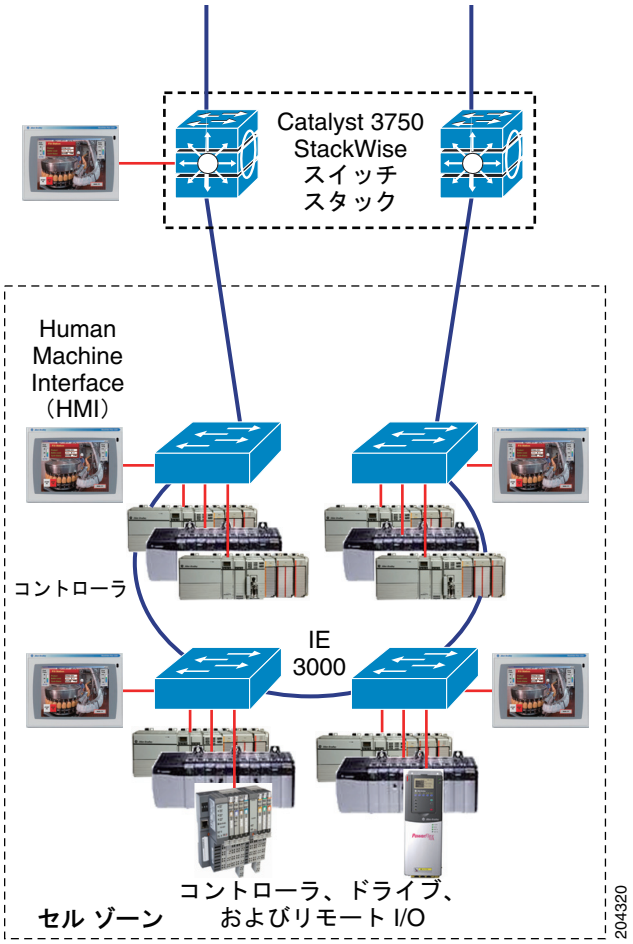


セル ネットワーク：リング トポロジ

リング トポロジはトランク廃棄トポロジと似ていますが、チェーンの最後のスイッチがレイヤ 3 スイッチに接続され、ネットワーク リングが形成される点が異なります。リング内で接続損失が発生しても、各スイッチは他のスイッチとの接続を維持します。図 1-3 を参照してください。

- ネットワークは、単一の接続損失からだけ回復できます。
- 追加プロトコルの実装と Rapid Spanning Tree Protocol（RSTP）を必要とするため、このトポロジの実装は比較的難しくなります。
- トランク廃棄よりも優れていますが、リングの最上部（レイヤ 3 スイッチとの接続）がボトルネックになる可能性があります。この部分はオーバーサブスクリプションの影響を受けやすく、これが発生するとネットワーク パフォーマンスが低下する可能性があります。

図 1-3　セル ネットワーク：リング トポロジ

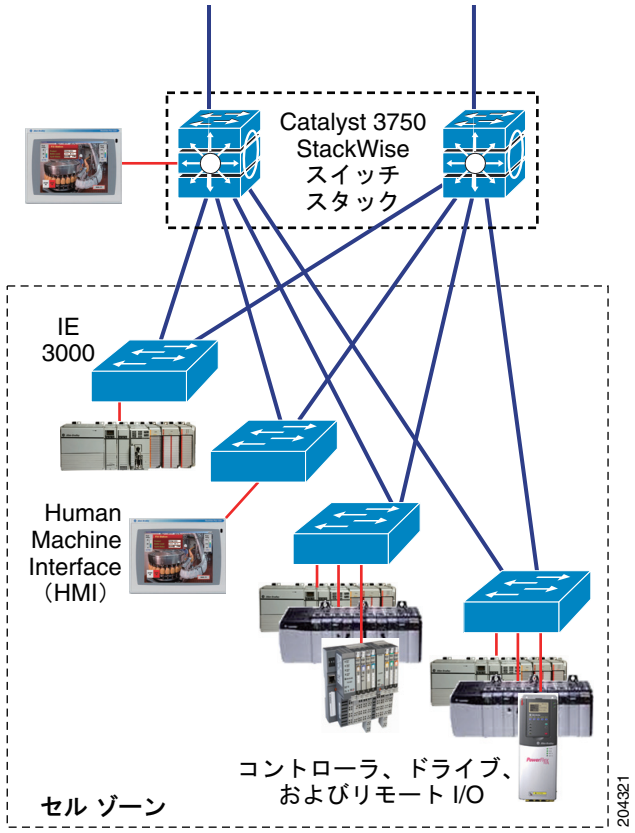


セル ネットワーク：冗長構成のスター トポロジ

冗長構成のスター トポロジでは、各レイヤ 2 アクセス スイッチがレイヤ 3 ディストリビューション スイッチにデュアル接続します。装置はレイヤ 2 スイッチに接続されます。図 1-4 を参照してください。

- どのレイヤ 2 スイッチでも、他のレイヤ 2 スイッチまでのホップ数は常に 2 つだけです。
- レイヤ 2 ネットワークでは、各スイッチがレイヤ 3 装置にデュアル接続します。
- 複数の接続損失が発生した場合でも、レイヤ 2 ネットワークは維持されます。

図 1-4　セル ネットワーク：冗長構成のスター トポロジ



次の作業

スイッチを設定する前に、次の項でスタートアップ情報を確認してください。

- 第 2 章「CLI（コマンドライン インターフェイス）の使用」
- 第 4 章「スイッチの IP アドレスとデフォルト ゲートウェイの割り当て」