産業用オートメーション環境でのネットワーキングとセキュリティ

設計ガイド

更新:2020 年 3 月

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

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

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco は世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。

目次

産業用オートメーション環境での ネットワーキングとセキュリティ

要約

企業は、Industrial Internet of Things（IIoT）および インダストリー 4.0 の新しいパラダイムを活用して、コンバージェンスとデジタル化による生産システム/アセットの運用改善の促進を図っています。これらのイニシアチブを進めるには、標準ネットワーク テクノロジーによる実稼働環境への安全な接続が必要です。安全な接続により、企業とその主要パートナーは、運用環境において新しいデータの大量のストリームにアクセスし、リアルタイムの可視性を確保し、必要に応じてシステム/アセットにリモートアクセスすることが可能になります。

新しいデータと可視性は、新しいビジネス価値と革新的なユースケースへの扉を開く、IIoT およびインダストリー 4.0 イニシアティブの中核的要素です。産業エコシステムは、産業分野において、実稼働システムによるリアルタイム情報へのアクセスを改善することを通じて、継続的に効率性を向上させ、コストを削減し、総合設備効率（OEE）を改善することを目指しています。持続的なデータ フローにより、企業は、サプライヤ、従業員、およびパートナーとグローバルにつながり、より効率的に顧客のニーズを満たすための、より効果的な方法を開発できます。予知メンテナンス、リアルタイム品質検出、アセットトラッキング、安全性強化などのユースケースを実現するには、新しいデータへのアクセスを改善するための工場システム/アセットへの安全な接続が鍵になります。

シスコ® の産業用オートメーション ソリューションと関連製品テクノロジーは、産業環境および実稼働環境への安全な接続を確立し、それらの環境をデジタル化することで、事業運営を大幅に改善するための不可欠な基盤です。シスコのソリューションを使用することにより、セキュリティ上の懸念事項、柔軟性のないレガシー ネットワーク、複雑さといった、デジタル化とインダストリー 4.0 に対する顧客の最大の障壁を克服できます。このソリューションでは、産業用オートメーション/制御システム（IACS）と実稼働アセットを接続し、産業用セキュリティを向上させ、工場のデータ アクセスと運用の信頼性を向上させるための、実績のある検証済みのブループリントが提供されます。市場をリードするシスコのテクノロジーを使用した、このベストプラクティスのブルー プリントに従うことにより、導入時間を短縮し、リスクを軽減し、複雑さを解消し、全体的なセキュリティと業務稼働時間を改善することが容易になります。

図 1　　産業用オートメーションに関する顧客の目標と課題

図 2　産業用オートメーション ソリューションを導入する理由

産業用オートメーションのリファレンスアーキテクチャ

産業用オートメーション向け Cisco Validated Design（CVD）ソリューションでは、ネットワーク、セキュリティ、およびデータ管理テクノロジーが、産業用オートメーション/制御システム（IACS）工場環境と、運用環境の中核をなす主要実稼働アセットに適用されます。これにより、シスコによって検証されたリファレンス アーキテクチャと設計/導入ガイダンスが、顧客、パートナー、およびシステム実装者に提供されます。このソリューションは、広範な産業用デバイス（センサー、アクチュエータ、コントローラ、リモート端末ユニットなど）、アプリケーション、およびパートナーによって包括的にテストされています。このソリューションには、高速接続、高い拡張性、ハイアベイラビリティ、使いやすさ、市場をリードする産業用セキュリティ、オープンスタンダード、正確な時間の配信および情報テクノロジー（IT）環境と運用テクノロジー（OT）環境の連携/接続を実現する機能が含まれています。このソリューションは、さまざまな産業分野への適用が意図されており、製造、鉱業、石油/ガス、電力などの企業のプラント、工場、精製所、鉱山、処理施設、変電所、倉庫といった場所で産業用オートメーション システムの安全なネットワークを実現します。

また、このソリューションは、インダストリー 4.0 および IIoT の概念とモデルを導入して実装するために必要不可欠なセキュリティと接続性の基盤となるブループリントを提供します。そのため、このソリューションは、産業環境と実稼働環境をデジタル化して事業運営の成果を大幅に向上させるための鍵となります。

図 3　産業用オートメーションのリファレンスアーキテクチャ

業界を問わない適用性

この産業用オートメーション ソリューションは、幅広い産業分野/用途に適用されるネットワーキング、セキュリティ、およびデータ管理を網羅しており、各種業界に適用可能なさまざまな設計と実装の選択肢が用意されています。規模、ベンダー、アプリケーション、およびデバイスはこれらの施設間で大幅に異なる可能性がありますが、ネットワークとセキュリティの中核となる多数の概念を適用できます。たとえば、ハイアベイラビリティはすべての産業ユースケースにおいて重要な要件ですが、石油/ガスおよび電力企業は、製造施設よりも厳しいアベイラビリティ要件を持つ場合があります。それでも、CVD ソリューションのベストプラクティス ガイダンスは、多くの業界や産業の顧客環境に適用できます。

次のアプリケーションには、このリファレンスアーキテクチャを使用してください。

- IACS デバイス(センサー、アクチュエータ、コントローラなど)、主要な機器、アセット(ロボット、CNC マシン、ツール、プロセススキッド、RTU)の接続性
- IACS デバイスと通信のネットワークおよびセキュリティステータスの継続的な可視性とモニタリングを OT 担当者に提供します。
- 製造資産および担当者へのリモートアクセスの提供と、それによる稼働時間の改善
- 製造実行システム、遠隔監視制御・情報取得(SCADA)、履歴管理、資産管理といった工場全体のアプリケーションのサポート
- DNS、DHCP、サイト全体への正確な時間の配信、認証など、関連するネットワークサービスを実装します。
- 予知分析とメンテナンス、デジタルツイン、および機械学習、最適化などのエッジコンピューティングによる IoT アプリケーションを有効にします。

要約

表 1　業界を問わず適用可:パート 1/2

	製造業	変電所	石油/ガスプラント	鉱業生産	廃水
ビジネス上の必須目標	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 予知メンテナンス、機械学習、および Digital Twin アプリケーションの促進。 工場のパートナーやサプライヤへの接続。	顧客の獲得と維持。 安全性、セキュリティ、および信頼性の改善。 新しいエネルギー源と消費モデルの統合。 電力系統の刷新。	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 意思決定の改善と機械学習の促進。 精製所とパイプラインのパートナーやサプライヤへの接続。	自動化された工場による機械化の促進。 安全性、セキュリティ、および信頼性の改善。 資材と機器の流れの最適化。 障害の予測の改善。 リアルタイムパフォーマンスのモニタリング。	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 予知メンテナンスの促進。 リアルタイムパフォーマンスのモニタリング。
顧客の課題	生産アセットおよびデータへのアクセス。 セキュリティリスク。 サイロ化された複雑なネットワークが原因で発生するダウンタイム、データ分離、および脆弱性。柔軟性がなく高い運用コスト。 データ、ネットワーク、およびセキュリティを管理するための専門知識。	生産アセットおよびデータへのアクセス。 セキュリティリスク。 老朽化したインフラストラクチャ。 サイロ化された独自仕様のアプリケーションとネットワークを管理および保護するための多大なコスト。 データ、ネットワーク、およびセキュリティを管理するための専門知識。	アセットの信頼性。 人とアセットの最適化。 セキュリティリスク。 従業員の安全。 サイロ化された複雑なネットワークが原因で発生するダウンタイム、データ分離、および脆弱性。 柔軟性のないネットワークおよび高い運用コスト。 データ、ネットワーク、およびセキュリティを管理するための専門知識。	アセットの信頼性。 人とアセットの最適化。 セキュリティリスク。 従業員の安全。 サイロ化された複雑なネットワークが原因で発生するダウンタイム、データ分離、および脆弱性。	メンテナンス、機器、および消耗品のコストの上昇。 漏水問題への対処(特に干ばつの影響を受けた国々において)。 より少ない人員での地理的領域内の施設の管理。 変化しつづける規制への継続的準拠。

表 1 業界共通の適用性:パート 2/2

	製造業	変電所	石油/ガスプラント	鉱業生産	廃水
シスコの産業用オートメーションソリューションの機能	ハイ アベイラビリティ すべての主要産業制御システムプロトコルにわたって相互運用可能な単一のソリューション データ可視化のためのエンドツーエンド接続(物理的にセグメント化されていない) すべてのレベルで統合されたセキュリティ(OT と IT に対して機能) リアルタイム、確定的 産業用ベストプラクティス設計 修理と稼働時間の容易な管理 インテントベースの使いやすさ 柔軟性(モジュール方式)	ハイ アベイラビリティ すべての主要産業制御システムプロトコルにわたって相互運用可能な単一のソリューション データ可視化のためのエンドツーエンド接続(物理的にセグメント化されていない) すべてのレベルで統合されたセキュリティ(OT と IT に対して機能) リアルタイム、確定的 産業用ベストプラクティス設計 修理と稼働時間の容易な管理 インテントベースの使いやすさ 柔軟性(モジュール方式)	ハイ アベイラビリティ すべての主要産業制御システムプロトコルにわたって相互運用可能な単一のソリューション データ可視化のためのエンドツーエンド接続(物理的にセグメント化されていない) すべてのレベルで統合されたセキュリティ(OT と IT に対して機能) リアルタイム、確定的 産業用ベストプラクティス設計 修理と稼働時間の容易な管理 インテントベースの使いやすさ 柔軟性(モジュール方式)	ハイ アベイラビリティ すべての主要産業制御システムプロトコルにわたって相互運用可能な単一のソリューション データ可視化のためのエンドツーエンド接続(物理的にセグメント化されていない) すべてのレベルで統合されたセキュリティ(OT と IT に対して機能) リアルタイム、確定的 産業用ベストプラクティス設計 修理と稼働時間の容易な管理 インテントベースの使いやすさ 柔軟性(モジュール方式)	ハイ アベイラビリティ すべての主要産業制御システムプロトコルにわたって相互運用可能な単一のソリューション データ可視化のためのエンドツーエンド接続(物理的にセグメント化されていない) すべてのレベルで統合されたセキュリティ(OT と IT に対して機能) リアルタイム、確定的 産業用ベストプラクティス設計 修理と稼働時間の容易な管理 インテントベースの使いやすさ 柔軟性(モジュール方式)
お客様のメリット	信頼性の高い工場運用:データ可視性の改善による稼働時間と OEE の向上 リアルタイムのプロセス可視性の改善によるコストの削減とスクラップ 運用コストの削減によるコストの削減:容易な設定、アップグレード、交換、および保守 安全な工場運用 ダウンタイムの削減	運用上の信頼性の向上 リアルタイムのデータ可視性 セキュリティ攻撃のリスクの軽減 時間が重視されるミッションクリティカルな通信のための信頼性の高いネットワーク ハイ アベイラビリティ リアルタイムの可視性	信頼性の向上とリスクの管理 無駄と処理の削減 運用上の信頼性の向上 ターンアラウンド時間の短縮 罰金や違約金の最小化 労働者の安全と環境コンプライアンスの改善 リアルタイムの可視性 安全な工場運用	OEE とアベイラビリティ 生産力の向上 安全性と環境コンプライアンス 運用コストの削減:容易な設定、アップグレード、交換、および保守 機械や人への安全なワイヤレスまたは有線接続による優れた俊敏性とスタッフの安全および生産力の向上	安全な公益事業情報管理 セキュリティ攻撃のリスクの軽減 リモート モニタリング ハイ アベイラビリティ 運用コストの削減:容易な設定、アップグレード、交換、および保守 安全性と環境コンプライアンス

進化する工場環境

過去 10 年ほどで、産業用オートメーション分野の変化のペースは明らかに加速しています。これは主に、Industrial Internet of Things、フォグ/エッジ コンピューティング、スマート ファクトリー、インダストリー 4.0 などの用語によって代表されるテクノロジーの向上、つまり、第 4 次産業革命とデジタル化によって促進されています。ここでは、これらの動向のいくつかと、テクノロジーの向上を実現するためにこのソリューションをどのように適用するのかについて説明します。

Industrial Internet of Things（IIoT）

Industrial Internet of Things（IIoT）は、「接続されるデバイス」の広がりが、人によって使用されるコンピュータやモバイル デバイスによってではなく、あらゆる形態のオートメーションで使用される「モノ」や産業エコシステムの制御において使用される「モノ」によって促進されるという考えに基づいています。産業エコシステムは、イーサネット、802.11 ベースの Wi-Fi、IP プロトコルのポートフォリオ（たとえば、TCP や UDP）などの標準ネットワーキング上の通信プロトコルに対して独自ネットワークに基づくフィールドバステクノロジーから移行しつつあります。このようにオープンネットワーキング標準を重視することは基本的な側面です。産業エコシステムを構成するデバイスまたは「モノ」は、オープン コンバージドネットワークで通信できるため、データと情報へのアクセシビリティが大幅に向上します。そのため、この IIoT によって、デジタル変革と、「インダストリー 4.0」と呼ばれる産業エコシステムの革命が可能になります。このソリューションは、採用する顧客が IIoT を確立できるように、これらの産業エコシステムへのオープン コンバージドネットワークの導入を促進します。

インダストリー 4.0

インダストリー 4.0 は、製造、電力、鉱業、石油/ガスの産業で第 4 次産業革命が進行しているという考えに基づいています。これは、産業の動向とコンピューティングの動向の合流と見ることができます。中核となっているのは、物理デバイス、機械、プロセスを、サイバーシステム、IIoT、クラウド コンピューティング、人工知能、機械学習、およびその他の関連テクノロジーと組み合わせることで厳密に制御および運用できるという概念です。

インダストリー 4.0 では、次の 4 つの主要な設計原則が示されています。

- 相互接続：Internet of Things（IoT）によって、機械、デバイス、センサー、および人の相互接続/通信を可能にします。
- 情報の透明性: インダストリー 4.0 テクノロジーによって実現される透明性により、適切な決定を行うために必要な膨大な情報がオペレータに提供されます。相互接続により、オペレータは製造プロセスのすべてのポイントから膨大な量のデータと情報を収集できるため、イノベーションや改善によってメリットが得られる機能を促進し、重要な領域を特定することができます。
- テクニカルサポート: 第一に、情報に基づく決定を行って迅速に緊急の問題を解決できるよう包括的に情報を収集して可視化することで人間をサポートできる能力です。第二は、人間の同僚にとって好ましくない、疲労度が非常に高い、または安全でないさまざまなタスクを実施することによって、物理的に人間をサポートできるサイバー物理システムの能力です。
- 分散型決定：サイバー物理システムが自らの決定を下し、可能なかぎり自律的にタスクを実行します。例外、干渉、または矛盾する目標がある場合にのみ、タスクはより高いレベルに委任されます。

シスコの産業用オートメーション ソリューションは、インダストリー 4.0 アプローチの基盤となるものであり、産業環境の相互接続とサイバーセキュリティに重点を置いていますが、それだけではなく、データ管理機能によって情報透明性を、リモート接続およびコラボレーション機能によって技術的補助を、さらにはフォグ/エッジ コンピューティング機能によって分散型決定も実現します。

シスコの産業用オートメーション ソリューションの機能

この産業自動化ソリューションは、OT 要件とアプリケーションに合わせて調整された最良の IT 機能と専門知識を適用し、産業環境向けに提供します。

- すべての主要産業通信およびサービス向けのハイアベイラビリティ
- モーションコントロールなど、最も課題の多いアプリケーションのネットワーク遅延およびジッターの減少を実現するリアルタイムで確定的なアプリケーション
- 産業グレードの IT 機器を既製（COTS）の IT 機器とともにさまざまな産業環境条件で展開する機能

- 小規模の展開（数十～数百台の IACS デバイス）から非常に大規模な展開（数千～数万台の IACS デバイス）にまで対応できる高い拡張性
- 導入/メンテナンスを容易にするインテントベースの管理性と使いやすさ（特に、IT に関するスキルや知識が限られている OT 担当者のために）
- Rockwell Automation、Schneider Electric、Siemens、三菱電機、Emerson、Honeywell、オムロン、SEL などの産業ベンダーとの互換性
- 確実なベンダーの選択と独自の制約からの保護を実現するオープンスタンダードベース
- モーションアプリケーションとイベントデータ収集のスケジュールをサポートするためのサイト全体での正確な時間の配信
- 多数のインダストリー 4.0 ユースケースを可能にする、センサーからクラウドへの通信をサポートするコンバージドネットワーク
- OT コンテキストを統合し、産業用アプリケーション向けに適用可能な、検証済みの IT 対応セキュリティアーキテクチャ（OT 環境と IT 環境の両方でベストプラクティスを実現）
- エッジコンピューティングをサポートする IoT アプリケーションの導入
- OT にフォーカスした継続的な IACS デバイスと通信のサイバーセキュリティ モニタリング

産業環境に対するソリューションの利点

このソリューションおよび関連するシスコのテクノロジーを導入して、産業用オートメーションシステムを安全に接続することの利点は、次のとおりです。

- 業界最先端の IT/OT にフォーカスしたセキュリティによる実稼働環境のリスクの軽減
- 生産のアベイラビリティの向上と制御システム/アセットの可視性の強化による、運用設備効率（OEE）とアセットの利用率の改善
- 品質に影響を与えるイベントや状態の初期兆候を把握することによる、製品の不具合の削減
- 新しい回線または回線の変更または新しいプラントの迅速な導入
- 機器のトラブルシューティング（接続性の低下またはセキュリティ関連のダウンタイムが発生）にかかる時間の短縮

この CVD の産業環境向けの新機能

要約に示されているように、このソリューションでは、既存のドキュメンテーションとテストを活用および拡張します。このバージョンでは、既存機能に依存するとともに、さらに機能を強化するために、新しい製品およびテクノロジーが組み込まれています。このソリューションで拡張された機能は、次のとおりです。

- **石油およびガス**：ワイヤレス HART システムからのワイヤレス センサートラフィックをバックホーリングする、本質的に安全な、新しい IW6300 Wi-Fi アクセスポイントをベースにしたワイヤレスサポートにフォーカスしたプロセス制御および製油所アプリケーションをサポートします。このサポートには、レガシー 1552 Ap から IW6300s への中断のないサービス移行のサポートが含まれています。また、これらを管理するワイヤレス LAN コントローラのサポートも含まれます。
- **シスコのソフトウェアによって定義されるアクセス（SDA）対応プラットフォームのサポートを拡張**：Cisco IE 3200、Cisco IE 3300、Cisco IE 3400 高耐久性シリーズスイッチには、IP67 定格の Cisco IE 3400H が含まれるようになりました。Profinet、一連のレジリエンシー（復元力）プロトコルのサポートを拡張し、セル/エリアゾーンのセキュリティ機能に完全に加われるようになっています。
- **Cisco Cyber Vision 産業用サイバーセキュリティ**：OT にフォーカスした産業用サイバーセキュリティの可視性とモニタリングを統合した Cisco Cyber Vision

SDA 対応プラットフォームに関する注意：Cisco Catalyst 9300 スイッチは、セル/エリアゾーン用のディストリビューション スイッチとして導入され、検証されています。Cisco Catalyst 9300 プラットフォームは現時点で Software-Defined Access をサポートしています。そのため、ネットワークを再設計することなく、ユーザ、デバイス、およびアプリケーションのトラフィックを分離する自動コンフィギュレーションおよびエンドツーエンド セグメンテーションを実現できます。SDA によってユーザアクセスポリシーが自動化されるため、組織はユーザまたは端末を問わずネットワークのどのアプリケーションにも適切なポリシーを確立できます。管理のしやすさとポリシーを使用した目的主導型のネットワーキングは、産業工場環境にとって有益な追加機能になります。シスコは、産業プラント、倉庫、駐車場、車道/交差点などの部分を管理する非カーペット敷きスペース向けの Cisco IoT 拡張エンタープライズ ソリューションで SDA を利用しています（www.cisco.com/go/iotcvd を参照）。ただし、**SDA は、このソリューションでセル/エリアゾーン内の産業用オートメーションおよび制御（制御ループ）アプリケーションをサポートするために展開することについてはまだ検証されていません。**新しい IE プラットフォームは、SDA が産業工場の要件とプロトコルをサポートできるようになるまでの準備としてのアーキテクチャに位置付けられています。

対象読者

この CVD は、IACS システムの導入担当者を対象としています。IT および OT の両担当者が、エンタープライズ ネットワーク内で産業システムの安全なコンバージェンスを促進するために使用することを目的としています。このソリューションは、実稼働システムの設計、導入、または運用に携わるベンダー、パートナー、システム実装者、顧客、およびサービス プロバイダーに、産業用オートメーション ネットワーク/セキュリティの設計と実装に関するガイダンスを提供します。この設計および導入ガイドでは、IACS に関してシスコが推奨するネットワーキングおよびセキュリティについて包括的に説明します。これには、システムアーキテクチャ、導入モデルの候補、および実装と設定のガイドラインに関する情報が含まれます。また、検証済みのリファレンスアーキテクチャを導入する際の推奨されるベストプラクティスについても説明します。

産業用オートメーション アーキテクチャの考慮事項

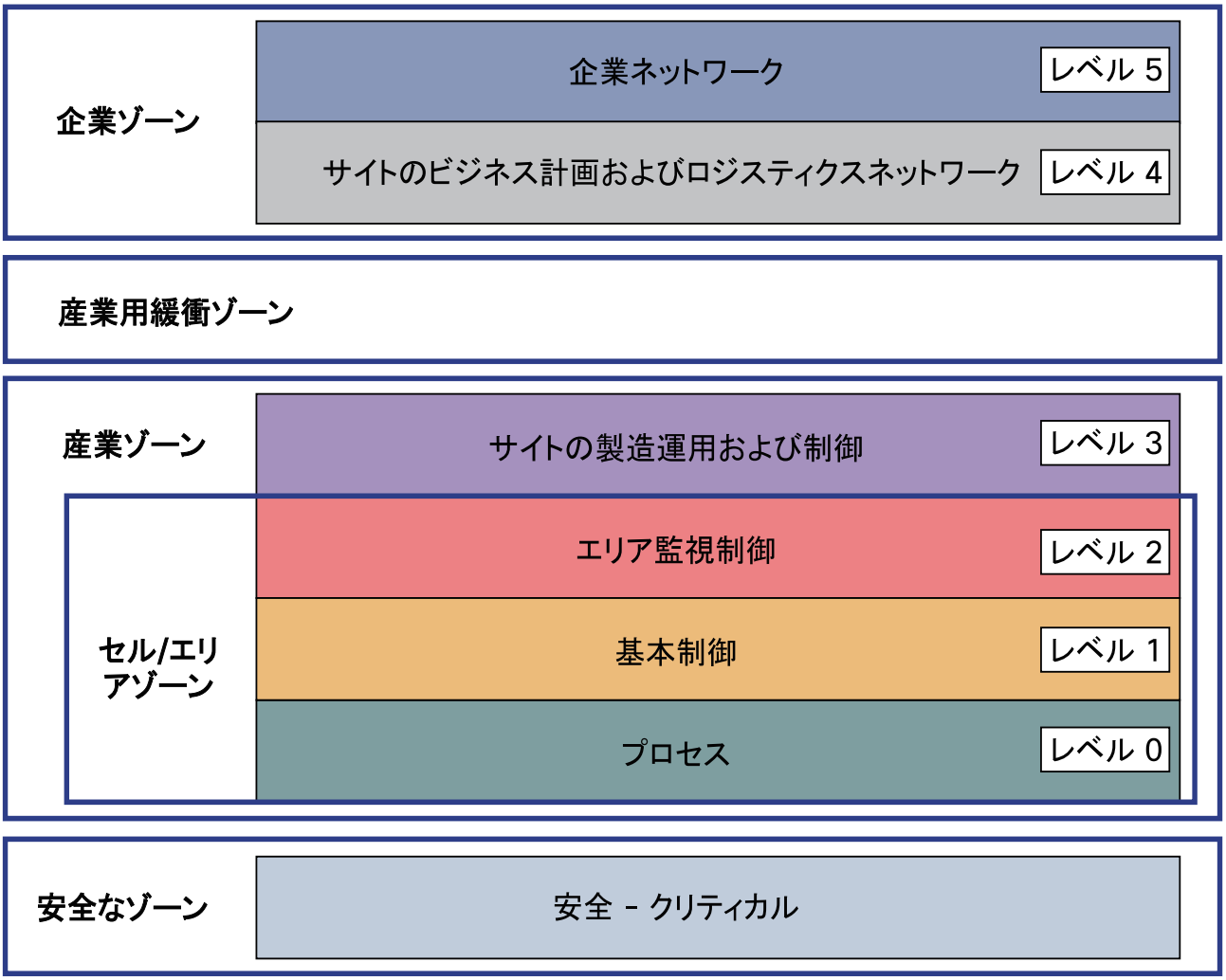
ここでは、産業用オートメーション環境の基本概念、構成要素、および考慮事項について説明します。

工場の論理フレームワーク

20 世紀は、ユーティリティからプロセスおよび個別の製造業まで、産業プロセスと業種の出力が大幅に増加しました。これらの開発は、プログラマブル ロジック コントローラ（PLC）、産業用ロボット、コンピュータ数値制御機械（工作機械）などの発明を含むオートメーションおよび制御テクノロジーの進歩によって大きく促進されました。これらが、SCADA、製造実行システム（MES）、履歴/アセット管理システムなどのソフトウェアベース アプリケーションと組み合わされることで、IACS が生まれました。

IACS のセキュリティおよびネットワークシステムの要件を理解するために、このガイドでは論理フレームワークを使用して、産業用システムの基本的な機能と構成について説明します。制御階層の Purdue モデル（参照 ISBN 1-55617-265-6）は、デバイスや機器を階層機能にセグメント化する、産業界で広く知られた一般的なモデルです。International Society of Automation ISA-99 Committee for Industrial and Control Systems Security と IEC 62443 産業用サイバーセキュリティ フレームワークでは、この IACS テクノロジーのセグメンテーションに基づいて、図 3 に示されているレベルと論理フレームワークが明確化されました。各ゾーンとその関連レベルについては、引き続き、次の場所にある『Converged Plantwide Ethernet（CPwE）Design and Implementation Guide』の第 2 章の「Industrial Automation and Control System Reference Model」で詳しく説明しています。
https://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf

図 4　工場の論理フレームワーク



このモデルは、運用のレベルを識別し、各レベルを定義します。この CVD では、「レベル」は、この運用レベルの概念を指します。ネットワーク アーキテクチャについて説明する際には、一般に、ネットワーク通信の層を定義するオープンシステム相互接続（OSI）リファレンスモデルも参照されます。OSI モデルは、ネットワーク通信機能の層を指します。この CVD では、特に指定がないかぎり、「層」は、OSI モデルの層を指します。

安全ゾーン：産業用オートメーション制御システムにおける安全性

産業環境では、必ず安全性が要求されます。たとえば、製造環境では、適切な安全手順に従わないと、ロボットが人に致命的な影響を与える可能性があります。また、そのような手順に従ったとしても、ロボットは、悪意のある制御下にある場合には害をおよぼす可能性があります。もう 1 つの例は、変電所の自動化です。このような高電圧環境では安全性要件が非常に重要です。製造業のロボットと同様に、隔離を実行することが期待されているリレーに悪意のある攻撃者が関与するだけで、簡単に安全性が影響を受ける可能性があります。

IACS の安全性は非常に重要であるため、安全ネットワークは他の IACS から分離され（また、その上に重ねられている）だけでなく、通常、色分けされたハードウェアが使用され、より厳格な規格が適用されます。さらに、安全性を高めるために、個人防護用具（PPE）および物理的障壁が必要です。産業用オートメーションにより、同じ物理インフラストラクチャ上で安全装置を標準 IACS デバイスと共存させ、相互運用することが可能になります。これにより、コストが削減され、運用効率が向上します。

セルエリア/ゾーン:アクセスと制御

セル/エリアゾーンは工場施設内の機能エリアであり、多くの工場には複数のセル/エリアゾーンがあります。大規模工場では、「ゾーン」がかなり広いプロセスに対して指定される場合があります。それらの中に「セルエリア」の小さなサブセットがあり、そこでプロセスがさらに小さなサブセットに分割されます。たとえば、自動車組み立て工場では、「ゾーン」は、未完成のシャーシがスタンプ工場から到着した場合には、塗装されている場合があります。その後、残りの組み立て工程へ進みます。この場合、そのゾーン内のある「セル」は、基調色のための別のセルにフィードする下塗りのセルである可能性があります。基調色のセルは、さらに上塗りのための別のセルにフィードします。

このエリアのほとんどのネットワークでは、クリティカルではないトラフィック(履歴など)と時間要件の厳しい確定的トラフィック(制御ループ用)の両方が伝送されるため、厳格なサービス品質(QoS)要件を満たすマネージド スイッチングが必要です。スイッチ、ルータ、ファイアウォールなどはすべて、厳密に管理されます。ただし、機械ネットワークには管理されていないスイッチも存在します(管理されていないルータやファイアウォールは存在しない)が、それらはトラフィックの高度に制御された性質のためにのみ使用可能になっています。これらの管理されていないスイッチは、トラブルシューティングおよびモニタリング機能を備えた完全に管理されたスイッチよりも、起動時間が短く、交換が容易であるために推奨されます。

以下で説明するように、このゾーンでは基本的に 3 つのレベルのアクティビティが発生します。

レベル 0:プロセス

レベル 0 は、基本的な産業プロセスに関わるさまざまなセンサーとアクチュエータで構成されます。これらのデバイスは、モーターの駆動、変数の測定、出力の設定、主要機能(塗装、溶接、曲げ加工など)の実行といった IACS の基本機能を実行します。これらの機能には、非常に単純なもの(温度計など)も非常に複雑なもの(移動ロボットなど)もあります。

これらのデバイスは、論理モデルのレベル 1 の制御デバイスから指示を受け、それらにステータスを伝達します。さらに、メンテナンスやデバイスの問題解決のために、その他の IACS デバイスまたはアプリケーションが、レベル 0 デバイスに直接アクセスする必要がある場合があります。レベル 0 デバイスの主な属性は次のとおりです。

- リアルタイムの確定的な通信要件を促進する。
- プロセス変数を測定し、プロセス出力を制御する。
- トポロジの制約を高める困難な物理環境に存在する。
- IACS ネットワークの規模に応じて、小規模(数十台)から大規模(数千台)までデバイス数が変動する。
- 設計と設置の完了後は、工場ラインのオーバーホールまたは交換が行われるまで(通常 5 年以上)、全部が一度に交換されることはない。

レベル 1:基本制御

レベル 1 は、主にレベル 0 デバイス(I/O、センサー、アクチュエータなど)とやり取りする、製造プロセスに対する指示/操作を行うコントローラで構成されます。個別の環境では、コントローラは通常 PLC ですが、プロセス環境では、コントローラは distributed control system(DCS)と呼ばれます。このソリューション アーキテクチャにおいては、「コントローラ」とは、業界を超えて使用される多目的コントローラを指します。

IACS コントローラは、エンジニアリング ワークステーションからプログラムされ、設定される業界固有のオペレーティング システムを実行します。IACS コントローラは、次の一部またはすべてで構成されるモジュラコンピュータです。

- すべてのデータを計算するとともに、ロードされているプログラムを実行するコントローラ
- レベル 0 デバイス、レベル 2 ヒューマン マシン インターフェイス(HMI)、または他のレベル 1 コントローラと通信する、I/O モジュールやネットワーク モジュール
- 残りのコントローラや、場合によってはその他のデバイスにも電力を供給する、統合電源モジュールや個別電源モジュール

IACS コントローラは、レベル 0 にあるデバイスからのフィードバックに基づいて基本的な決定を行う IACS のインテリジェンスです。コントローラは単独で、または他のコントローラと連携して動作して、デバイスを管理し、それによって産業プロセスを管理します。また、コントローラは、レベル 2 および 3 の IACS の他の機能(履歴、アセット管理、製造実行システムなど)と通信します。コントローラは、産業ゾーンでディレクタ機能として動作して、高レベルのパラメータ(レシピなど)を実行可能な命令に変換し、デバイスからの I/O トラフィックを統合し、I/O データを上位の工場フロア機能に渡します。

このようにして、コントローラは、レベルの観点から次の 3 方向に IACS ネットワークトラフィックを生成します。

- 制御および管理しているレベル 0 のデバイスへのダウンロード
- セル/エリアゾーンに関して IACS を管理するその他のコントローラへのピアツーピア
- レベル 2 および 3 の HMI と情報管理システムへのアップロード

レベル 2:エリア監視制御

レベル 2 は、セル/エリアゾーンのランタイム監視および操作に関連するアプリケーションと機能を表し、次のものが含まれます。

- オペレータインターフェイスまたは HMI
- アラームまたはアラートシステム
- 制御ルームのワークステーション

工場の規模や構造によっては、これらの機能がサイト レベル(レベル 3)に存在する場合があります。これらのアプリケーションは、レベル 1 のコントローラと通信し、緩衝地帯(DMZ)を介してサイトレベル(レベル 3)または企業(レベル 4 ～ 5)システム/アプリケーションとデータをやり取りするか共有します。これらのアプリケーションは、専用 IACS ベンダー オペレータ インターフェイス端末または標準コンピューティング機器/オペレーティングシステム(Microsoft Windows など)に実装できます。また、これらのアプリケーションは、多くの場合、標準イーサネットおよび IP ネットワークプロトコルと通信し、通常、業界団体によって実装および保守されます。

産業ゾーン

産業ゾーンは、セル/エリアゾーン(レベル 0 ～ 2)とサイトレベル(レベル 3)のアクティビティで構成されます。工場フロアの IACS 動作のモニタリングと制御に欠かせないすべての IACS アプリケーション、デバイス、およびコントローラが産業ゾーンにあるため、このゾーンは重要です。工場でのスムーズな作業と、IEC 62443 などの標準に合致した IACS アプリケーションや IACS ネットワークの機能を維持するため、このゾーンでは、レベル 4 および 5 からの明確かつ論理的なセグメンテーションと保護が必要とされます。

レベル 3:サイト運用および制御

レベル 3(サイトレベル)は、IACS の最高レベルを表します。このスペースは一般的に「カーペット敷きのスペース」です。つまり、このスペースは、HVAC を備え、商業用グレードの機器を利用したホット/コールド アイルに一般的な 19 インチ ラックマウント機器が配備されます。

名前が示すように、これはサイト運用に関連するアプリケーションが存在する場所です。「サイト運用」は生産を直接駆動するアプリケーションとサービスを意味します。たとえば、このレベルに含まれていない一般的なものは、エンジニアリング リソースプランニング(ERP)システムや製造業実行システム(MES)などの企業中心のアプリケーションです。これらのアプリケーションはビジネス管理アプリケーションが多くなり、企業アプリケーションとの密接な連携と統合が行われる傾向があるためです。このレベルでのサービスの例としては、Historians、制御アプリケーション、ネットワークおよび IACS 管理ソフトウェア、ネットワークセキュリティサービスなどがあります。制御アプリケーションは、工場の特性によって大きく異なります。自動車組立工場の例として、塗装調整アプリケーションがあります。このアプリケーションは、プレス工場から塗装ゾーンのロボット塗装コントローラにフィードされるシャーシを、直接制御している場合があります。レベル 1 コントローラ(この例ではロボットコントローラ)は、多くの場合、高耐久化され、それらの制御ループに関する決定を下す必要があり、実際の操作を行うか、それに近い役割を果たします。これとは対照的に、サイト レベルの塗装調整アプリケーションは、真の制御ループ アプリケーションではなく、カーペット敷きのスペースに配備することが可能です。

このレベルに存在するシステム/アプリケーションは、工場全体の IACS 機能を管理します。レベル 0 ～ 3 は、サイト運用に不可欠と見なされます。このレベルに存在するアプリケーションと機能には、次のものがあります。

- レベル 3 IACS ネットワーク
- レポート機能(サイクル タイム、品質指標、予知メンテナンスなど)
- 工場の履歴

- 詳細な生産スケジュール
- サイトレベルの運用管理
- アセットおよび資材の管理
- 制御ルームのワークステーション
- パッチ起動サーバ
- ファイルサーバ
- その他のドメインサービス(Active Directory(AD)、DHCP、ドメインネームシステム(DNS)、Windows インターネット ネーム サービス(WINS)、ネットワークタイムプロトコル(NTP)、Precision Time Protocol(PTP)グランドマスタークロックなど)
- リモートアクセスサポートのためのターミナルサーバ
- ステージングエリア
- 管理および制御アプリケーション

レベル 3 の IACS ネットワークは、レベル 1 コントローラおよびレベル 0 デバイスと通信し、産業ゾーンに変更を加えるためのステージングエリアとして機能し、DMZ を通じて企業(レベル 4 および 5)システム/アプリケーションとデータを共有することができます。これらのアプリケーションは、主に標準コンピューティング機器およびオペレーティングシステム(UNIX ベースまたは Microsoft Windows)に基づきます。このため、これらのシステムは、多くの場合、標準イーサネットおよび IP ネットワーク プロトコルと通信します。

さらに、これらのシステムは標準 IT テクノロジーとより緊密に連携する傾向があるため、これらのシステムも IT のスキルセットを持つ担当者によって実装およびサポートされる場合があります。

企業ゾーン

レベル 4:サイトのビジネス計画およびロジスティクス

レベル 4 は、企業ネットワークで提供されるサービスへの標準的なアクセスを必要とする機能とシステムがある場所です。このレベルは、企業ネットワークの拡張部分とみなされます。ここでは基本的なビジネス管理タスクが実行され、それらのタスクでは標準的な IT サービスが使用されます。これらの機能とシステムには、次のような、企業ネットワークサービスへの有線および無線アクセスが含まれています。

- インターネットおよび電子メール(データセンターでホストされる)へのアクセス
- 製造実行システムなどのクリティカルではない工場システムと、インベントリ、パフォーマンスなどの工場全体のレポート
- SAP、Oracle などの企業アプリケーション(データセンターでホストされる)へのアクセス

これらのサービスは、重要ではあっても IACS にとってクリティカルであるとは見なされないため、工場フロア運用にとってもクリティカルであるとは見なされません。企業ネットワーク内のシステムおよびアプリケーションのオープン性が高いため、このレベルは、しばしば、IACS ネットワークの脅威および中断の原因と見なされます。

多くの場合、レベル 4 のユーザとシステムは、IACS ネットワークの下位レベルからの要約データおよび情報を必要とします。ここでのネットワークトラフィックおよびパターンは、一般的な企業に見られるブランチまたはキャンパスネットワークの典型であり、ネットワークトラフィックの約 90 % がインターネットまたはデータセンター アプリケーションに流れます。

このレベルは、通常、IT 組織によって管理されます。

レベル 5:企業

レベル 5 は集中 IT システムおよび機能が存在する場所です。企業リソース管理(ERM)、Business-to-Business、および Business-to-Customer サービスは、通常、このレベルに存在します。多くの場合、外部パートナーまたはゲストアクセスシステムはここに存在しますが、企業レベルでは実現するのが難しい柔軟性を得るために、下位レベル(レベル 3)のフレームワークに置かれることも珍しくありません。ただし、このアプローチでは、IT セキュリティポリシーおよび標準の範囲内で実装しないと、重大なセキュリティリスクが生じる可能性があります。

IACS は、製造データおよびリソースデータを交換するために企業アプリケーションと通信する必要があります。一般に、IACS への直接アクセスは必要ありません。これに対する 1 つの例外は、従業員またはパートナー（システムインテグレータ、機械製造業者など）による IACS の管理のためのリモートアクセスです。データおよび IACS ネットワークへのアクセスは、IACS のセキュリティ、アベイラビリティ、および安定性を維持するために、DMZ を介して管理および制御する必要があります。

このレベルのサービス、システム、およびアプリケーションは、IT 組織によって直接管理および運用されています。

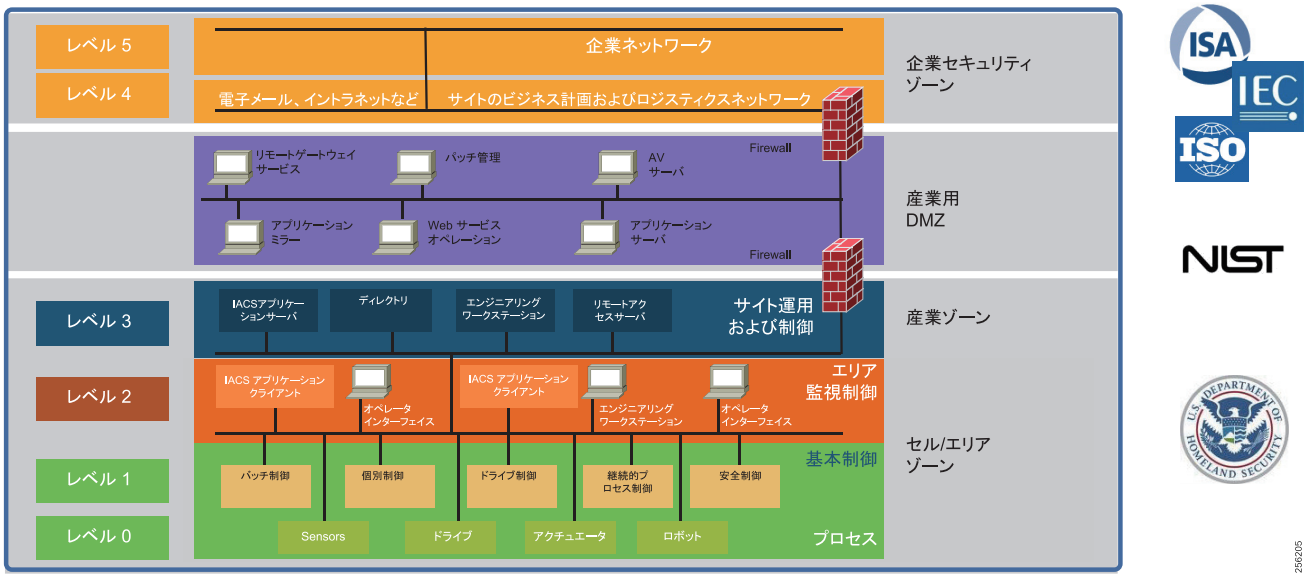
産業用 DMZ

Purdue リファレンスモデルの一部ではありませんが、産業用オートメーション ソリューションには産業ゾーンと企業ゾーンの間の DMZ が含まれます。産業用 DMZ は、企業ネットワークと工場環境運用ドメインを分離するために工場環境内に導入されます。IACS ネットワークのダウンタイムはコストがかかり、収益に深刻な影響を与える可能性があるため、運用ゾーンは外部の影響を受けないようにする必要があります。企業と工場の間での直接のネットワークアクセスは許可されませんが、データとサービスはゾーン間で共有される必要があるため、産業用 DMZ はデータの安全な転送のためのアーキテクチャを提供します。DMZ に導入される一般的なサービスには、リモートアクセスサーバとミラー化されたサービスが含まれます。産業用 DMZ の設計上の推奨事項の詳細については、このガイドの後半で説明します。

IT ネットワーク DMZ と同様に、産業用 DMZ は主に、この隔離されたネットワークに最も脆弱性の高いサービス（電子メール、Web、DNS サーバなど）を持ち込む企業やインターネットと工場フロアの間のバッファとして存在します。産業用 DMZ は、工場を外部から隔離するだけでなく、自社の企業ネットワークからも隔離します。この追加の分離が推奨される主な理由は、エンタープライズサービスとは異なり、工場フロアには会社の最もクリティカルなサービス（会社が販売する製品そのものを生産するサービス）が含まれることです。多くの場合、工場フロアのアプリケーションは時代遅れで、Windows 95 などの脆弱なオペレーティングシステム上で動作しています。産業用 DMZ は、これらの脆弱なシステムに別のレベルのセキュリティを提供します。

産業用 DMZ のもう 1 つの主な用途はリモートアクセスであり、企業の製品と収益に影響を与える実稼働機器のトラブルシューティングを支援することです。外部アクセスと時代遅れの機器の組み合わせによるリスクのために、いくつかの追加セキュリティ対策の必要性が高まります。産業用 DMZ がそうしたサービスのためにどのように使用されるかの詳細については、後で説明します。

図 5　産業工場リファレンスアーキテクチャと IDMZ



IACS の要件と考慮事項

運用テクノロジー アプリケーションの要件

OT の中核にある OT アプリケーションは、産業プロセスの安定性、継続性、および完全性の維持に重点が置かれています。その中心となるのは、産業プロセスを適切に運用するために維持する必要があるセンサー、コントローラ、およびアクチュエータのループです。さらに、その他の多数のアプリケーションが、ステータスを表示し、履歴を維持し、産業プロセスの運用を最適化するために情報を収集する必要があります。この観点から、このソリューションでは、OT アプリケーションをサポートするために、次のような一連の重要な要件を達成する方法の概要を示します。

- アプリケーションとしてのハイアベイラビリティは、毎日 24 時間、休まず提供される必要があります。
- IACS デバイス間のローカルリアルタイム通信の重視（制御ループの整合性を維持するために、通信が低遅延/ジッタである必要がある）
- IoT ベースのアプリケーション用に、IACS デバイスから診断およびテレメトリ情報にアクセスする機能
- デバイスやソフトウェアの更新/変更または設定の更新を容易にする機能（多くの場合、プロセスが長期間にわたって実行されるため）
- 産業グレードの IT 機器を既製の IT 機器とともにさまざまな産業環境条件で展開する機能（該当する場合）
- 小規模の展開（数十～数百台の IACS デバイス）から非常に大規模な展開（数千～数万台の IACS デバイス）にまで対応できる高い拡張性
- Motion 制御やイベントのシーケンスなどの難しいアプリケーションのための正確な時間へのアクセス
- 導入/メンテナンスを容易にするシンプルで使いやすい管理ツール（特に、IT に関するスキルや知識が限られている OT 担当者のために）
- 確実なベンダーの選択と独自の制約からの保護を実現するためのオープンスタンダードの使用

高耐久化および環境要件

一般的な企業ネットワーク デバイスは制御された環境に存在します。これが、IACS と一般的な企業アプリケーションの主な相違点です。IACS のエンドデバイスとネットワーク インフラストラクチャは、IEC 529（侵入保護）仕様や National Electrical Manufacturers Association（NEMA）仕様などの環境仕様への準拠を必要とする厳しい環境に配置されます。IACS のエンドデバイスとネットワーク インフラストラクチャは、物理的に離れた場所や、制御されていない（あるいはさらに厳しい）環境条件（温度、湿度、振動、ノイズ、爆発性、電気的干渉など）下に配置される場合があります。

これらの環境への配慮から、IACS のデバイスとネットワーク インフラストラクチャは、これらの厳しい条件に対応し、耐える必要があります。また、DIN レール準拠のフォームファクタは、一般に 19 インチ ラックに設置されている企業デバイスよりも産業環境に適しています。

産業用オートメーション制御システムのパフォーマンス

パフォーマンスは、ネットワークを設計する上で重要な考慮事項です。ネットワーキング エンジニアは一般に、特に VoIP ネットワークにおいて、長年にわたって遅延とジッタの両方に対処してきました。ただし、産業用オートメーション ネットワークでは、特にネットワーキングが低い Purdue レベル（ANSI/ISA 951/Purdue2 レベル 0 ～ 1、機械、リレー）に近づくにつれて、遅延とジッタの両方の要件が VoIP ネットワークよりも桁違いに厳しくなります。産業用オートメーション ネットワーク機器は非常に要求が厳しく、これらのデバイスの一部は、ソフトウェアや処理能力に限界があるため、ネットワーク関連の中断や外部からの通信の影響を受けやすくなっています。さらに、製造プロセスの頻繁な変更（製紙工場など）や複雑な自動化（多軸ロボットなど）のために、IACS では、パケット間の遅延を非常に高いレベルで確定的に予測できる必要があります。ネットワークに確定性がないと、産業プロセスの失敗や停止のために、ビジネスに影響を与えるダウンタイムが発生する可能性があります。産業用オートメーション ネットワークに必要なレベルの確定性を用意するために、次の点を考慮する必要があります。

- リアルタイムトラフィックを必要とするアプリケーションに高いプライオリティをマークする

- プライオリティの高いトラフィックに適切な帯域幅を保証する QoS ポリシーを作成する
- ネットワークリンク上の適切な帯域幅を計画する

アベイラビリティは IACS ネットワークの最も重要な側面です。これは他の非産業用ネットワークとのもう一つの重要な相違点を明確に示しています。ほとんどの IT ネットワークは年ごとにますます「ビジネス クリティカル」になっていますが、それらは一般にビジネスの中核ではなく、むしろサービス組織の一部です。対照的に、OT ネットワークは、企業が実際に行っていることの一部であるという点でビジネス クリティカルです。OT ネットワークのクリティカルな部分が停止すると、生産が停止して収益が低下します。IACS ネットワークの一部は他の部分よりもクリティカルであるため、より高いアベイラビリティ要件を持ちます。このようなクリティカル性は、最終的にアベイラビリティまたはサービス レベル契約（SLA）要件に変換されます。これらの要件の多くは、この CVD のさまざまな部分に見られますが、最も注目すべきものについては、アベイラビリティを高めるさまざまな方法に関するセクション（復元力プロトコルに関するセクションなど）で説明しています。

アベイラビリティを達成する方法：

- IACS ネットワーク インフラストラクチャのシングルポイント障害を排除します（冗長リンク、スイッチ、レイヤ 3 デバイス、ファイアウォールなど）。
- IACS アプリケーションの要件を満たすネットワーク復元力とコンバージェンスプロトコルを実装します。
- 産業環境にネットワーク デバイスの迅速かつ容易なゼロタッチ交換を導入します。

セキュリティ

産業用オートメーションに導入されるセキュリティの従来のアプローチは「隠蔽によるセキュリティ」です。つまり、非常に狭いエア ギャップ環境を実現するとともに、パブリックアクセスのない独自仕様のプロトコルを実装します。物理的セキュリティの必要性は、上記の例だけでなく、Stuxnet（https://en.wikipedia.org/wiki/Stuxnet）などの実世界の例でも容易に認められます。Stuxnet は、「隠蔽によるセキュリティ」が（さらには「エアギャップ」でさえ）不十分なセキュリティ対策であることを実証しました（これらのトピックについては後で詳しく説明します）。Stuxnet の例に加えて、物理的セキュリティの必要性は、より一般的な「中間者」攻撃や単純な「ネットワークタップ」でも認められます。これらの攻撃では、物理デバイスがネットワークに挿入されます。この物理とサイバーセキュリティの共通部分は、通常、すべての産業用自動化ネットワークのコンポーネントです。独自仕様のプロトコルは侵害が困難であり、セキュリティインシデントは、多くの場合、偶発的に発生すると考えられてきました。しかし、ここ数年で産業用エコシステムは独自仕様のネットワークテクノロジーの使用からイーサネット、Wi-Fi、IP などのオープン標準ネットワークの使用へと移行しました。

ネットワークを保護する方法として不明瞭さを追加するというこのアプローチは、次のような理由から、産業用オートメーションにおける現在の動向の要件を満たしません。

- 工場フロアでの多様なデバイスの急増：第 1 に、工場ネットワークでは、特にプロセス制御環境の場合、ゼロから構築されるデバイスの代わりに、既製テクノロジー製品を使用して運用タスクを実行することが増えています。第 2 に、ビッグデータおよび分析の一部として多数のセンサーが工場フロアに追加されています。これは、主に、工場フロアの生産性を向上させるために使用できる機械からのデータを取得するためと、機器の予防メンテナンスを実行する手段としてです。これらの新しいデバイスは、標準プロトコルをサポートしており、クラウドやインターネットなどの特定のリソースにアクセスする必要がある場合もあります。
- IT と OT の統合：組織では、歴史的に分離されていた IT と OT のチームおよびツールが統合されはじめており、運用アクティビティを支援するためにより伝統的な IT 中心のソリューションが導入されつつあります。従来は別々だった OT ドメインと IT ドメインの境界があいまいになるにつれて、エンドツーエンドのセキュリティを確保するために戦略を調整し、より密接に連携させる必要があります。

セキュリティの特性

製造業者のネットワークにおけるこれらの傾向により、安全なシステムを確保するために、工場ネットワークオペレータは次の基本原則を採用する必要があります。

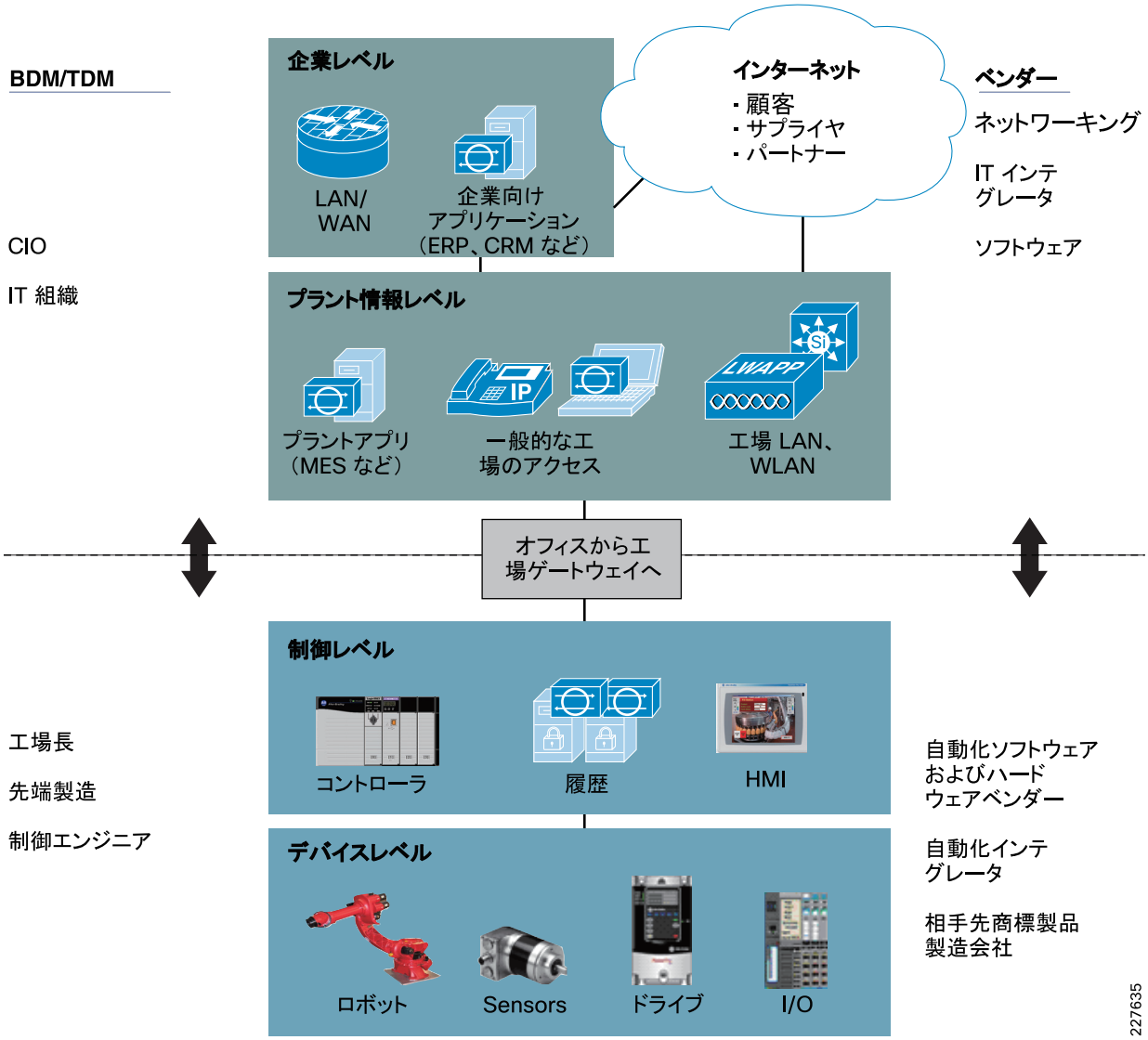
- 工場ネットワーク内のすべてのデバイスの可視性：従来、ラップトップ、携帯電話、プリンタ、スキャナなどの企業デバイスは、これらのデバイスがネットワークにアクセスするときに企業管理システムによって識別されていました。この可視性を、工場フロアのすべてのデバイスに拡張する必要があります。
- ネットワークのセグメンテーションとゾーン分割：セグメンテーションはデバイスの到達可能性を制限するプロセスであり、ゾーン分割はそのゾーン内のすべてのメンバーが同一のセキュリティ機能を持つレイヤを定義することです。ネットワークにゾーンを導入すると、ゾーン内およびゾーン全体でアクセスを管理するための体系的な方法が提供されます。デバイスをセグメント化すると、デバイスがマルウェアに感染したときに、感染が拡大するリスクがさらに減少します。
- 識別と制限されたデータフロー：工場フロアのすべてのデバイス（IT 部門で管理する企業デバイスと OT 部門で管理する運用デバイス）は識別され、認証され、承認される必要があり、ユーザおよび IACS がネットワークに接続するときは、ネットワークのポリシーが適用される必要があります。
- ネットワークの異常：ネットワークアクティビティにおける異常な動作は、変更が意図されているのか、それともデバイスの誤動作によるものかを判断するために、検出され、調査される必要があります。ネットワークの異常をできるだけ早く検出することで、工場の運用にネットワークの異常をより早く修復する手段が与えられ、それによってダウンタイムを減らすことに役立ちます。
- マルウェアの検出と軽減：感染したデバイスのために見られる異常な動作は、ただちに検出される必要があり、セキュリティツールは、感染したデバイスに対する対処を可能にする必要があります。
- 従来のファイアウォールは、通常、産業環境向けに開発されていません。IACS トラフィックフローにおける異常を識別するには、産業用プロトコル上で詳細なパケット検査を実行できる産業用ファイアウォールが必要です。
- 工場フロア内のネットワーキングアセットとインフラストラクチャの強化は、重要な考慮事項です。これには、特に Simple Network Management protocol（SNMP）のようなキー管理と管理プロトコルの保護が含まれます。
- 自動化および管理プロトコル：異常や悪用を防ぐために IACS プロトコル自体をモニタすることも重要です。
- セキュリティ標準への準拠：1990 年代には、Purdue リファレンスモデルと ISA 95 により、制御システムのさまざまな部分の間でセグメント化されたレベルを使用するアーキテクチャが強調されました。これは ISA99 と IEC 62443 でさらに発展させられ、リスク評価とプロセスに焦点が当てられました。セキュリティリスク評価により、どの PMS が「クリティカルな制御システム」、「クリティカルではない制御システム」、および「非制御システム」として定義されているかが特定されます。

情報テクノロジーと運用テクノロジーの統合

従来は、企業内の運用組織は実稼働環境とそれらに含まれる IACS だけを担当していました。IT 組織は企業アプリケーションとネットワークだけを担当していました。しかし、OT が標準ネットワーキングの採用を開始したため、これらの環境を相互接続するだけでなく、組織の機能を統合し、ベンダーとサプライヤ間のコラボレーションも促進する必要がありました。

IACS ネットワークに影響を与える決定は、通常、IT 部門ではなく、工場長と制御エンジニアが下します。さらに、IACS ベンダーおよびサポートサプライチェーンは、IT 部門が一般に使用するものとは異なります。ただし、製造業者の IT 部門が工場長や制御エンジニアと協力して、工場運用の利点のために標準ネットワーキング テクノロジーの専門知識を活用する状況が増加しています。

図 6　業務および技術面での意思決定者:IT と OT



業界共通の産業ネットワークの要件

表 2 顧客がさまざまなビジネス成果を達成するために役立つように、業界共通の産業用ネットワークの要件、課題、および産業用オートメーション ソリューションの機能をまとめます。

表 2　業界共通の産業ネットワークの要件：パート 1/2

業界	業界共通の産業ネットワークの要件	問題	産業用オートメーション ソリューションの機能
製造業 変電所 石油/ガスプラント 鉱業 廃水	すべての主要な通信およびサービスの**ハイアベイラビリティ**。	すべての複数の制御システムベンダーにわたってダウンタイムなしに機能するソリューション。 24 時間 365 日の運用。 99.999 %（「ファイブ ナイン」）を超える予想稼働時間。 過酷な環境。 シングルポイント障害の排除。 ダウンタイムによる高コスト。 修正やデバッグを行うオンサイトのエキスパートリソースの不在。	すべての主要な制御システムとの最高の信頼性での確実な連動。 堅牢で優れた MTBF のネットワーク インフラストラクチャ。 復元力のあるトポロジとプロトコルのサポートによる、インシデントの有無にかかわらない通信の維持。 冗長ネットワークサービス。 シンプルなデバイスの交換。 IACS 通信のプライオリティ付け。 攻撃からの通信リソースの保護。 障害の迅速な特定と修復の実現。 リモートアクセスとリモート管理の安全な実現。
	センサーからクラウドへの通信をサポートする**エンドツー エンド接続**：コンバージド	エアギャップ展開の実稼働環境。 実稼働環境内のデバイスのサイロ化。 セルまたはマシン実装の複製の必要性。 プライオリティが異なる複数のアプリケーション。 現在エアギャップ展開されているシステムからのデータの必要性。	最適化のための IACS デバイスまたはアプリケーションへの安全なアクセス。 重要なトラフィックにプライオリティを付けるためのきめ細かい QoS。 複製されたマシンまたはセル展開の、さまざまなレイヤ 2 NAT を介した統合。 産業用 DMZ モデルによって工場ネットワークを企業に統合することによる、エッジから分析までの安全なデータフローの実現。
	相互運用性とオープンスタンダードへの依存に基づく確実なベンダーの選択と独自の制約からの保護。	多数の独自仕様プロトコル。 多くの場合、数百または数千のデバイスおよびシステムサプライヤの統合。 数年または数十年にわたって利用されているアセット。 複数サプライヤ戦略の普及。	最新のオープンネットワーク標準（IEEE、イーサネット、IP、Wi-Fi、IETF など）がベース。 さまざまな産業用プロトコル（イーサネット/IP、PROFINET、Modbus、IEC 61850、CC-Link IE、DNP3 など）での確実な動作。 ネットワークの革新に必要な下位互換性。
	モーションコントロールなど、最も課題の多いアプリケーションのネットワーク遅延およびジッターの減少を実現する**リアルタイムで確定的な**アプリケーション。	イベントの正確なスケジュールは、監査およびトレース可能である必要があります。 迅速な調整/制御に必要な、レイテンシとジッターの少ないネットワーク。 すべての機器からより多くのデータを収集する必要性。	正確なネットワークベースの時刻同期のサポート。 高速ネットワーク インフラストラクチャ。 高度な QoS 機能。 複数のアプリケーションタイプをサポートするコンバージドネットワーク。

表 2 業界共通の産業ネットワークの要件：パート 2/2

業界	業界共通の産業ネットワークの要件	問題	産業用オートメーション ソリューションの機能
製造業 変電所 石油/ガスプラント 鉱業 廃水	過酷な環境条件のための**工業設計**。	本質的に安全なものを含む広範囲の過酷な環境条件。 大規模であることによる一般的なコストの増加。 すべての機器からより多くのデータを収集する必要性。	本質的に安全な環境でも対応および運用できる柔軟性を備えた、過酷な産業環境向けのソリューション。 正確なネットワークベースの時刻同期のサポート。 高速ネットワーク インフラストラクチャ。 高度な QoS 機能。 複数のアプリケーションタイプをサポートするコンバージドネットワーク。
	セキュリティ による脅威の阻止と産業運用インフラストラクチャの保護。	安全でないネットワーク デバイスによってもたらされるプラント全体への脅威。 パッチ未適用のレガシー システム。 セグメント化の欠如。 OT セキュリティのスキル。 可視性の欠如。 限定的なリモートアクセス。 OT システムに関する脅威モニタリングの欠如。	シスコのネットワーク HW および SW の本質的な安全性（安全な信頼の基点およびその他の多数のベストプラクティス機能）。 OT 環境のアセットを検出および分類する機能。 OT デバイスの動作を把握して脅威を特定する機能。 きめ細かくセキュリティポリシーをセットアップして適用する機能（たとえば、請負業者、リモートベンダ別、対話するデバイスの区別など）。 アクティブモニタリング ネットワークのセグメント化（基本的なものから高度なものまで）。
	導入/メンテナンスを容易にする**管理性**と使いやすさ（特に、IT に関するスキルや知識が限られている OT 担当者のために）。	ネットワークとセキュリティに関する専門知識の欠如。 動作中断への迅速な対応。 IACS デバイスの限られた機能。 IT と OT で使用される異なるツールセット。 非常に限られたアップグレード。 長期間（数年/数十年）使用されるアセット。	ネットワークによる産業用プロトコルのサポート（IACS アプリケーションによる可視性と設定を実現）。 ネットワーク インフラストラクチャの容易な交換。 OT 用に設計されたツール（IT ツールと統合）。 拡張可能なネットワークとセキュリティ管理のための IT ツール。 主要設定を導入するためのテンプレート。 プラグアンドプレイのサポートによる使いやすさと迅速な修理およびインストール。

業界標準と規制

標準とガイドラインは重要な基盤ですが、それらは特定のシステムを保護および設計する方法を規定していません。すべてのシステムが異なるため、標準とガイドラインはベストプラクティスのフレームワークとして活用し、ビジネスニーズに合わせて個別に調整する必要があります。ここでは、いくつかの業界標準について簡単に説明します。それらは、一般的に適用可能かつ一般的に適用されているものに限定されます。

ISA-95/PERA（Purdue）

ISA-95 と PERA は、すべてのタイプの IACS 向けに一般的なアーキテクチャを提供し、一般的な名称だけでなく一般的な構成要素も提供します。詳細については、次を参照してください。

- ISA 95 の Web サイト
  https://isa-95.com/
- PERA の Web サイト
  http://www.pera.net/

IEC 62443/ISA-99

IEC 62443 シリーズは、汎用 IT システムのセキュリティに関する確立された標準（ISO/IEC 27000 シリーズなど）に基づいており、産業用制御システム（ICS）に存在する重要な相違点を識別して対処します。これらの相違点の多くは、ICS 内のサイバーセキュリティリスクが「健康、安全、または環境」（HSE）に影響を与える可能性があり、その対応はこれらのリスクに対処する他の既存のリスク管理手法と統合される必要があるという現実に基づいています。

NIST サイバーセキュリティフレームワーク

米国国立標準技術研究所（NIST）のサイバーセキュリティフレームワーク（https://www.nist.gov/cyberframework）は、ベストプラクティスのガイドラインであり、要件の標準ではありません。これの起源は NIST の決議に 2014 年に加えられた変更であり、この変更では「（中略）クリティカルなインフラストラクチャに対するサイバーリスクをコスト効率よく削減するために、自発的な、合意に基づく、業界主導の一連の標準、ガイドライン、ベストプラクティス、方法論、手順、およびプロセスの開発を継続的に促進および支援する 」が追加されました。

NIST 800 シリーズ

NIST 800 シリーズは、その一般的な呼称のとおり、米国政府のセキュリティポリシー、手順、およびガイドラインを網羅する NIST の一連のドキュメントです。NIST は米国の政府機関（米国商務省所属）ですが、これらのガイドラインは米国だけでなく、世界中の多数の政府や企業、さらには公的部門に直接関与していない組織によっても参照され、事実上義務付けられています。特にこの CVD および関連 CVD では、NIST SP 800-82「Guide to Industrial Control Systems Security」と呼ばれるサブセットがとりわけ重要になります。これは、それが特に IACS 分野を対象とするものであるためです。このドキュメントの目的は、SCADA システム、DCS、および制御機能を実行するその他のシステムを含む、ICS を保護するためのガイダンスを提供することです。このドキュメントは、ICS の概念的な概要を示し、一般的なシステムトポロジおよびアーキテクチャを再検討し、これらのシステムに対する既知の脅威と脆弱性を識別し、関連リスクを軽減するための推奨セキュリティ対策を示します。さらに、NIST SP 800-53 Rev. 4 [22] に基づいて、ICS ドメイン固有の特性に合わせて制御をカスタマイズできるように、ICS に合わせたセキュリティ制御オーバーレイを提示します。

NERC CIP

NERC CIP つまり「北米電力信頼度協議会（NERC）重要インフラストラクチャ保護（CIP）」は、その名称が示すように、元来は電力会社に固有のものですが、電力業界以外でも広く参照および採用されています。やはりその名称が示すように、NERC CIP は「重要インフラストラクチャ保護（CIP）」を対象としています。「CIP」は広く使用されている用語であり、多数の標準、ガイドライン、およびベストプラクティスの主題となっています（詳細については、https://en.wikipedia.org/wiki/Critical_infrastructure_protection を参照）。特に NERC CIP がこの CVD および関連 CVD で使用される最大の理由は、NERC CIP が IACS インフラストラクチャの詳細に基づいて開発されている（したがって、その主題や手法において高い関連性を持ち、同じ用語が多数使用されている）ことです。

IEEE 1588 Precise Time Protocol

これは、IEEE 1588 で、ネットワーク化された測定/制御システムの精密クロック同期として定義されており、精度と安定性が異なる分散デバイス クロックを含むパケットベースのネットワークでクロックを同期させるために開発されました。Precise Time Protocol（PTP）は、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。PTP は、ピーク時の課金、仮想パワージェネレータ、停止のモニタリングと管理など、非常に正確な時間の精度と安定性を必要とするサービスを促進します。

PTP は 2002 年に開発されました。その後、2008年に（IEEE 1588-2008 で）強化され、PTPv2 と呼ばれています。このバージョンでは、正確な時間を配布するための基本的な概念とアルゴリズムが確立されます。これらの基本概念は、特定の使用例に対して設計された時間配分の特定の定義である「プロファイル」に採用されています。次の PTP プロファイルがあります。

- デフォルトプロファイル：このプロファイルは、IEEE 1588 ワーキンググループによって定義されています。これは、ODVA, Inc. の一般的な産業用プロファイル（CIP）などの多くの産業用アプリケーションで、CIP Sync サービスとして採用されています。このソリューションは、Sitewide の正確な時間分布機能のデフォルトプロファイルをサポートしています。さらに、Rockwell Automation および Cisco Converged Plantwide Ethernet（CPwE）ソリューションは、統合されたプラン Twide Ethernet Architecture（https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html）内で広範囲の時間配布を展開する際のデフォルトプロファイルをサポートしています。

- 電力プロファイル：このプロファイルは、国際電気標準会議（IEC）標準規格 62439 によって定義されました。電力プロファイルは、サブステーションの自動化のための通信プロトコル IEC 61850 規格で使用されます。このプロファイルは、Cisco Substation Automation Local Area Network and Security の CVD（https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.html）でサポートされています。

- 電気通信プロファイル：国際電気通信連合電気通信標準化部門（ITU-T）は、電気通信業界向けの一連の PTP プロファイルを確立しました。シスコのさまざまな製品はこれらのプロファイルをサポートしていますが、産業用オートメーションの分野ではあまり使われていません。このプロファイルは、このソリューションではサポートされていません。

- IEEE 802.1 AS プロファイル：IEEE は、音声ビジュアルブリッジング（AVB）の一連の技術の標準規格の一部として、このプロファイルで時間的な制約のあるアプリケーションのタイミングと同期を作成しました。このプロファイルは、IEEE 802.1 AS Rev ワーキンググループのもとで、産業用エコシステムによって推進される時間的な制約のあるネットワークセット（技術標準から成る）向けに強化されています。一部のシスコ製品は、AVB および TSN アプリケーション用の 802.1 をサポートしています。このソリューションは、現時点では 802.1 をサポートしていません。

産業用オートメーション ネットワークモデルと IACS リファレンスアーキテクチャ

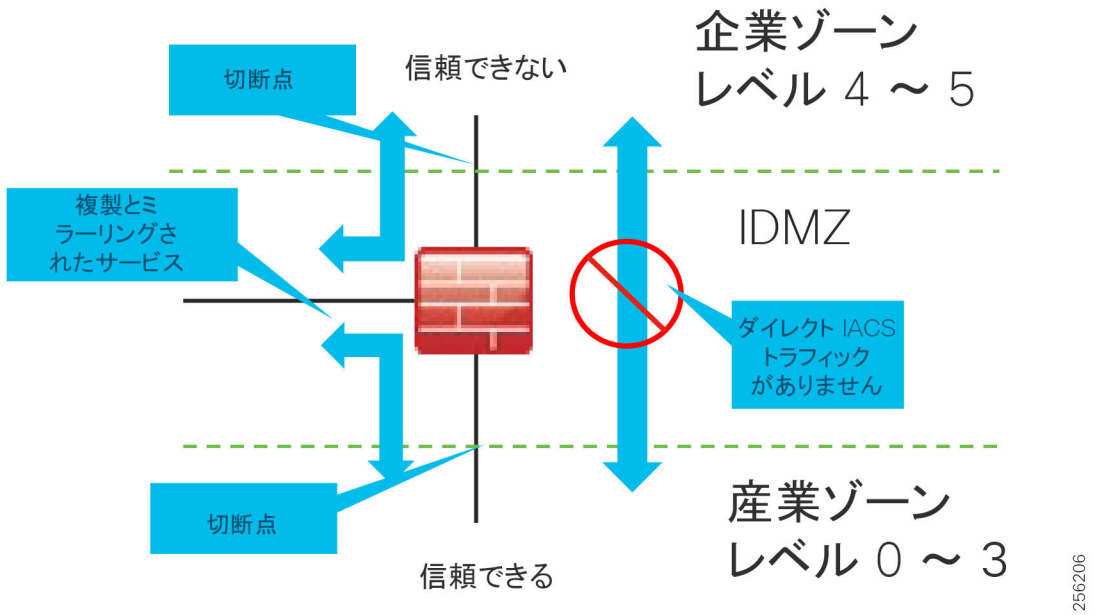
一般的な企業キャンパスネットワーク設計は、すべてのネットワークに復元力、高い拡張性、および安全な接続を提供するために最適です。キャンパスモデルは、コア、ディストリビューション、およびアクセスという 3 つの主要レイヤで構成される、実証済みの階層型設計です。運用工場ドメインの外部にセキュリティ インターフェイスを提供するために、DMZ レイヤが追加されます。以降では、企業キャンパスモデルを IACS リファレンスモデルにマッピングします。

産業工場向けのシスコ エンタープライズ ネットワーキング モデルの調整

DMZ および産業用 DMZ: レベル 3.5

キャンパスモデルの DMZ は、通常、インターフェイスを提供し、インターネットからの企業ネットワーク内のアセットおよびサービスへのアクセスを制限します。産業用 DMZ は、企業ネットワークと工場環境の運用ドメインを分離するために、工場環境内に導入されます。IACS ネットワークのダウンタイムはコストがかかり、収益に深刻な影響を与える可能性があります。そのため、IACS アセット/プロセスのアベイラビリティが最も重要であることから、運用ゾーンは外部の影響を受けないようにする必要があります。したがって、ネットワークアクセスは企業と工場間で直接は許可されませんが、データおよびサービスは運用ドメインと企業の間で共有する必要があるため、産業用 DMZ がゾーン間でデータを安全に伝送するための安全なアーキテクチャが必要です。DMZ に導入される一般的なサービスには、リモートアクセスサーバとミラー化されたサービスが含まれます。産業用 DMZ の設計上の推奨事項の詳細については、このガイドの後半で説明します。

図 7　　産業用 DMZ の機能モデル



コア ネットワーク

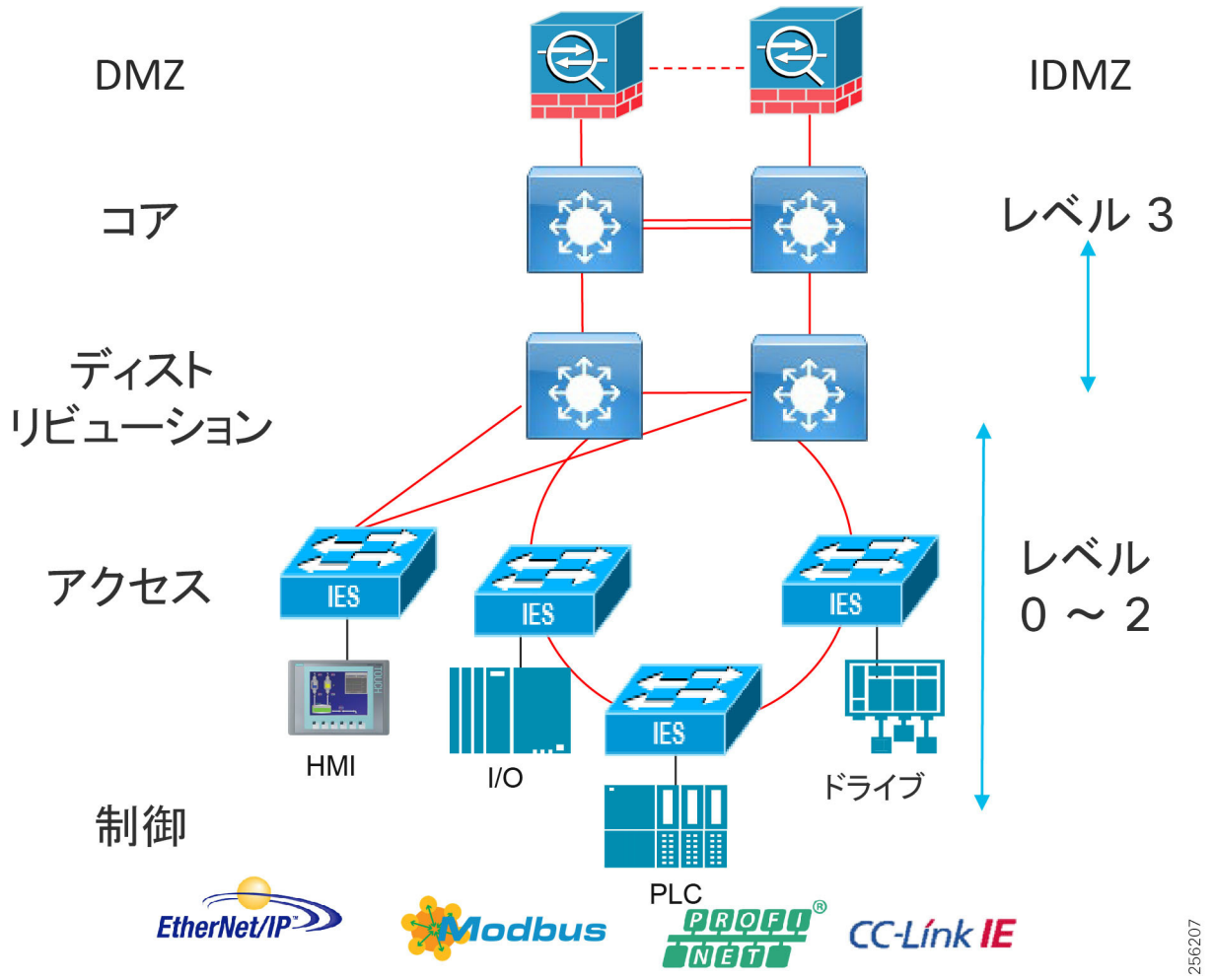
コアは、高速接続、冗長リンク、および冗長ハードウェアを使用して、高い信頼性と安定性を持ち、運用工場内のすべての要素（通常、レイヤ 3 デバイス）を集約できるように設計されます。コアは、工場アーキテクチャのコンテキスト内で、すべてのセル/エリアゾーンを集約し、産業用 DMZ および集中型サービスへのアクセスを可能にします。

産業用オートメーションの場合、工場全体で必要なサービスには、生産管理、履歴、ドメインコントローラ、ネットワーク セキュリティ プラットフォーム（Cisco Identity Services Engine（ISE）、Cisco Stealthwatch など）が含まれます。コアは、Purdue モデルのレベル 3 にある工場運用および制御ゾーンに対応します。

まとめ

- 拡張性とアベイラビリティに重点を置いた大規模サイト向けに、ディストリビューション レイヤ間の信頼性の高い接続を提供します。
- サイト全体の冗長性を実現します。
- 中断のないインサービスアップグレードが可能です。

図 8　産業用ゾーンを使用した企業モデル



ディストリビューション ネットワーク

最も単純な形式のディストリビューション レイヤは、アクセスレイヤとコアレイヤの間のポリシーベースの接続性と境界を提供します。Purdue モデルでは、このレイヤは、セル/エリアゾーンの一部として集約およびポリシー制御を提供し、セル/エリアゾーンと IACS ネットワークの他の部分の間の境界点として機能します。

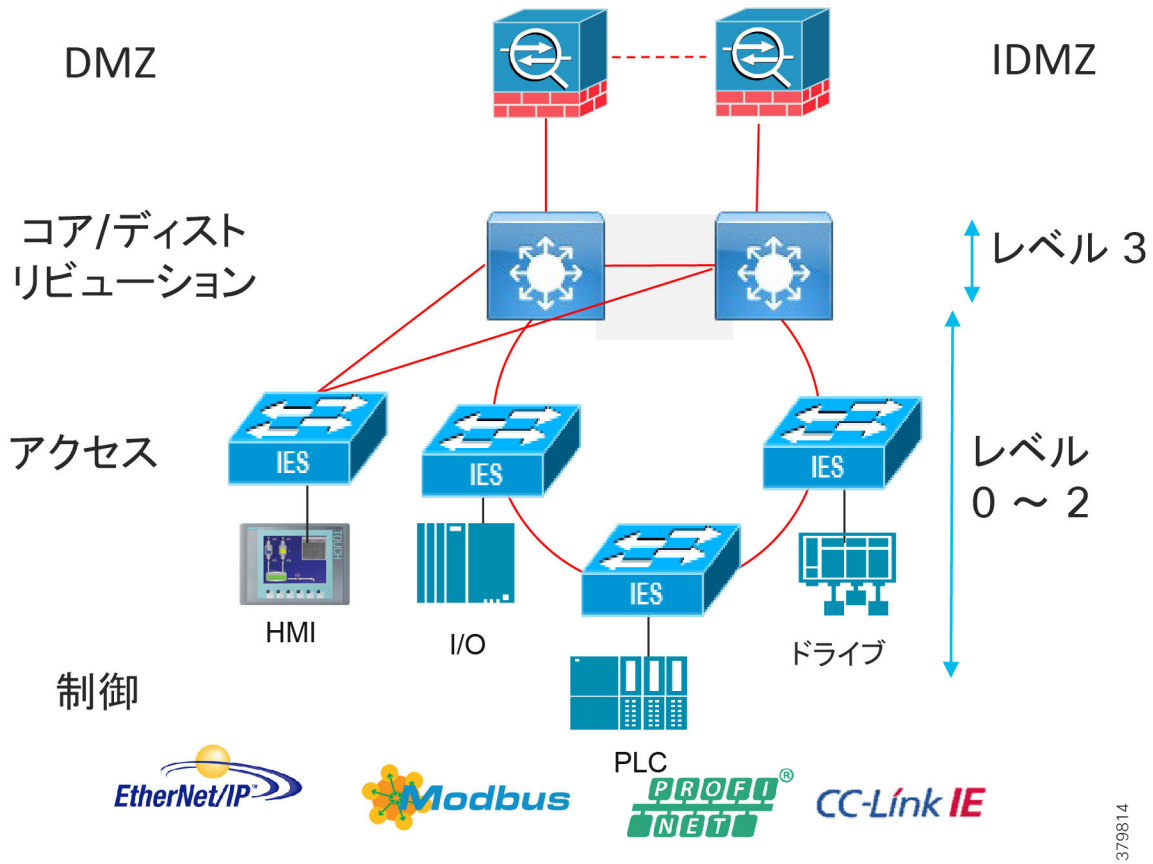
まとめ

- コアレイヤへのレイヤ 3 接続とアクセスへのレイヤ 2を提供します。
- アクセスレイヤを集約し、接続性サービスを提供します。
- アクセス/ディストリビューション ネットワーク内の接続性およびポリシー サービスを提供します。
- セル/エリアゾーンとネットワークの他の部分の間のディストリビューション、ポリシー制御、および分離/境界点を提供します。

コラプスト コア/ディストリビューション ネットワーク

中小規模の工場では、図 9 に示すように、コアをディストリビューション スイッチに組み込むことが可能です。ただし、多数のセル/エリアゾーンが存在する大規模工場では、このレベルの階層セグメンテーションは推奨されず、従来の 3 層レイヤが導入されます。

図 9　　コラプスト コア/ディストリビューション



アクセスネットワーク

アクセスレイヤは、ネットワーク インフラストラクチャとそのインフラストラクチャを活用するデバイスの間の境界を提供します。そのため、セキュリティ、QoS、およびポリシーの信頼境界を提供します。全体的な IACS ネットワーク設計を見ると、アクセススイッチはこれらのアクセスレイヤ サービスの大部分を提供し、複数の IACS ネットワーク サービスを有効にするための重要な要素となります。

セル/エリアゾーンは、IACS ネットワークに特化および最適化されたアクセスレイヤ ネットワークと見なすことができます。

まとめ

- エンドポイント（PC、コントローラ、I/O デバイス、ドライブ、カメラなど）とユーザにネットワークへのアクセスを提供します。
- セキュリティ、セグメンテーション、QoS、およびポリシーの信頼適用を実施します。
- パケットにラベルを付けてセグメンテーションを適用します。
- 高速収束リングトポロジまたはパラレル アクセス ネットワーク トポロジで構成されます。
- 潜在的なマルチキャストリッチ ローカル トラフィック フローが含まれます。
- ネットワークアドレス変換（NAT）オプションを提供します。

産業工場環境向けのアクセス ネットワーク トポロジ

従来の企業 IT ネットワークは、パフォーマンスと復元力が向上する傾向があるため、主に冗長スタートポロジに基づいてモデル化されていますが、IACS ネットワーク内には、アクセス ネットワークのレイアウトを定義するいくつかの要素があります。工場の物理的なレイアウト、ケーブル接続のコスト、および必要なアベイラビリティは、工場の 3 つの重要な要素です。たとえば、リングトポロジまたはリニアトポロジは、長い生産ラインではコスト効果が高くなります。冗長スタートポロジでこれらの長い生産ラインをケーブル接続するコストは非常に高く、アベイラビリティが必要な場合はリングトポロジマップが優先されます。PRP や HSR などのより新しいテクノロジーを使用すると、IACS 工場のリング復元力およびアベイラビリティを向上させることができます。HSR はリングトポロジ全体でロスレス冗長性を提供し、PRP は 2 つの異なるパラレル LAN（LAN-A と LAN-B、これらは 2 つの個別のリングにすることが可能）にわたってロスレス冗長性を提供します。

IACS 環境のトポロジを決定する際の重要な考慮事項は、次のとおりです。

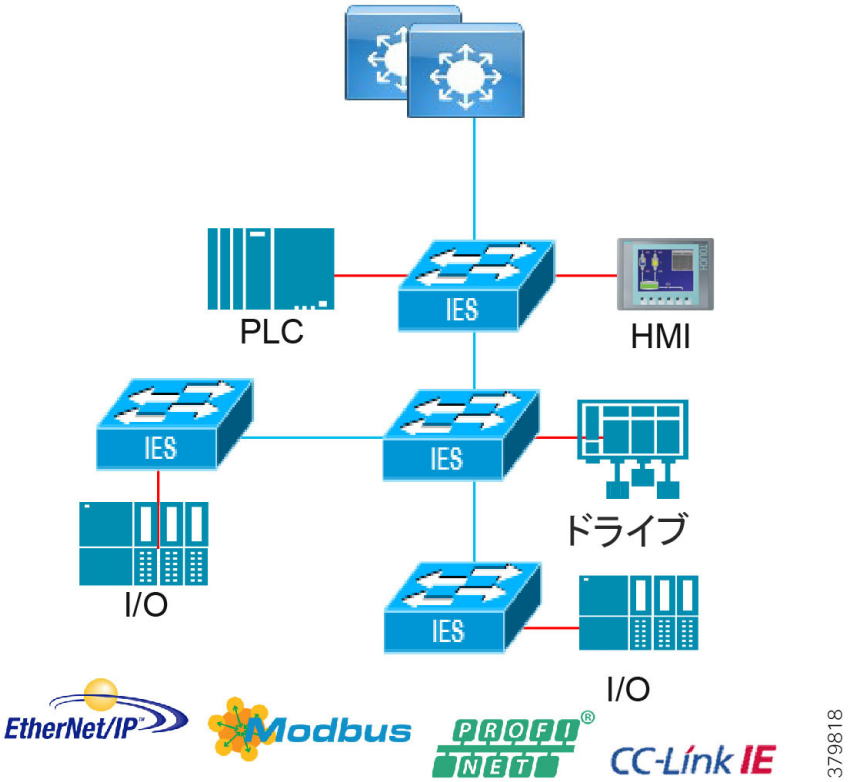
- 物理レイアウト：プロセス設備または製造ラインの物理レイアウトは、ネットワークトポロジに影響を与えます。ケーブル接続の設置は、産業環境では高コストになる可能性があり、企業でのケーブル接続より大幅に高くなります。スタートポロジは、長い生産ラインでは法外なコストになる可能性があります。リアルタイム通信とアベイラビリティの要件によって許容される場合は、リングネットワークトポロジによってコストを削減できます。
- アベイラビリティ：アベイラビリティは、工場の OEE に貢献する重要なパフォーマンス指標です。ネットワークの設計は、最大の稼働時間を実現する必要があります。復元力のあるネットワークトポロジを導入すると、リンクの損失やスイッチの障害が発生した後もネットワークが動作を継続できます。これらのイベントの中には依然として産業用オートメーション/制御システムのダウンタイムにつながる可能性があるものもありますが、復元力のあるネットワークトポロジによってその可能性を減らすことができ、リカバリ時間も改善されます。
- リアルタイム通信: リアルタイム通信の要件は、IACS アプリケーションが、予測可能なレベルでネットワーク上で確実に通信できることを示します。帯域幅やネットワークホップなどの複数の要因によって、遅延、ジッター、および予測不能なパフォーマンスが発生する可能性があります。専用スターネットワーク トポロジを使用すると、ネットワークが改善され、信頼性の高い通信が提供されますが、ケーブル接続コストが大きくなります。

セル/エリアゾーンのリニアトポロジ

リニアトポロジでは、一連のスイッチがシリアル方式で接続されます。この設計には次の特性があります。

- 潜在的なボトルネック（ディストリビューションと隣接するレイヤ 2 スイッチの間）
- 容易な実装
- ケーブル接続コストの削減
- 復元力の欠如
- 工場フロア レイアウトの柔軟性の向上

図 10　セル/エリアゾーンのリニアトポロジ

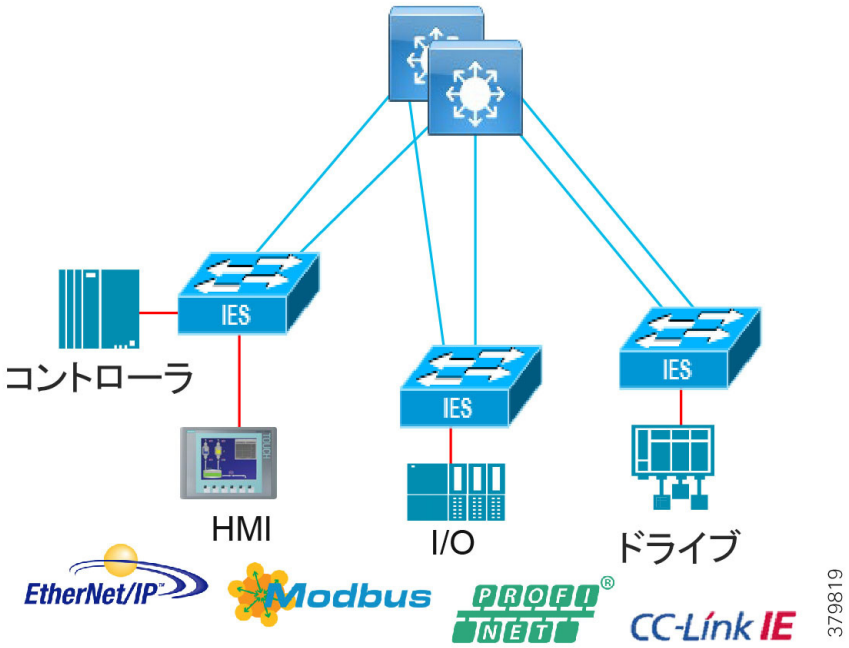


セル/エリアゾーンの冗長スタートポロジ

図 11 冗長スター アーキテクチャを示します。デバイス間のパスにはホップが 2 つしかなく、高速コンバージェンスを実現する冗長性があります。パス内のホップ数は一貫しているため、ネットワークには予測可能性の要素があります。このネットワークトポロジの主な特性は次のとおりです。

- 任意のアクセスレイヤ 2 スイッチ間の 2 つのホップによる予測可能なパス
- 冗長リンクと多重リンク障害発生時の復元力
- リングよりも高速な予測可能コンバージェンス（ロスレス リング復元力テクノロジーではない場合）
- 最も高価なケーブル配線の設計

図 11　セル/エリアゾーンの冗長スタートポロジ



セル/エリアゾーンのリングトポロジ

リングトポロジは、1 つのリンク障害が発生しても常にネットワークパスが使用可能であるという点で、復元力を提供します。これはリニアトポロジが発展したものであり、チェーンの最後のスイッチがディストリビューション スイッチに戻って接続され、リングを形成しています。リングはリングのまわりの二重パスを共有し、ボトルネックとオーバーサブスクリプションを減らすことができます。セル/エリアゾーンの設計のセクションで説明されているより新しいテクノロジーを使用すると、復元力は、リング展開でもヒットレスにすることができます。リングトポロジの主な考慮事項は次のとおりです。

- ケーブル接続コストを削減するシンプルさ
- 1 つのネットワーク接続が失われた状態からの復元力
- ハイ アベイラビリティ シームレス冗長性（HSR）によって導入可能なヒットレスまたはロスレステクノロジー

図 12　セル/エリアゾーンのリングトポロジ

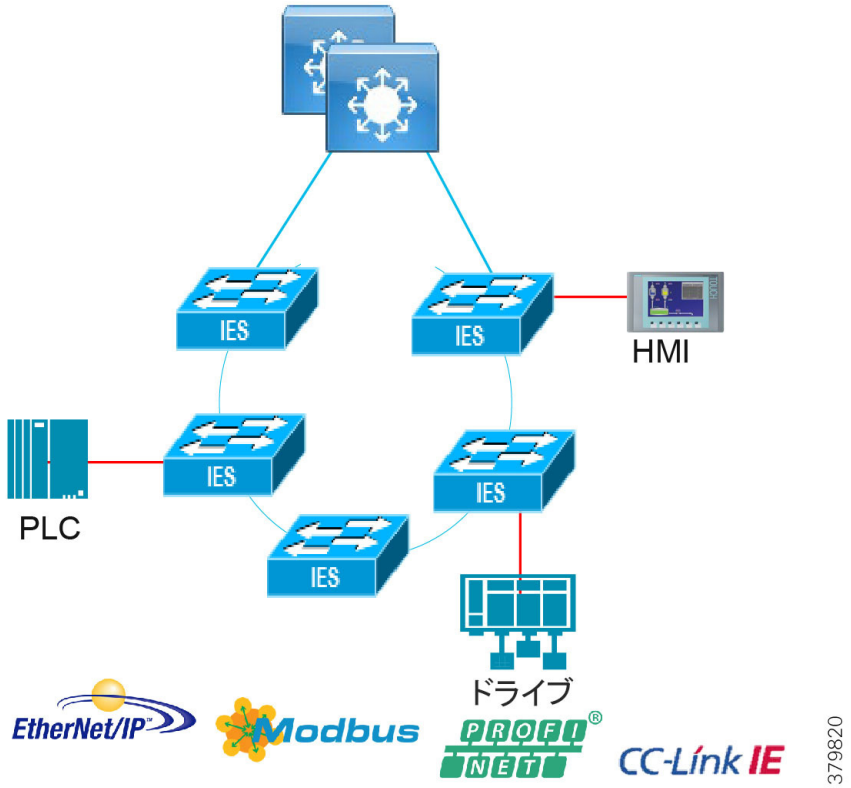


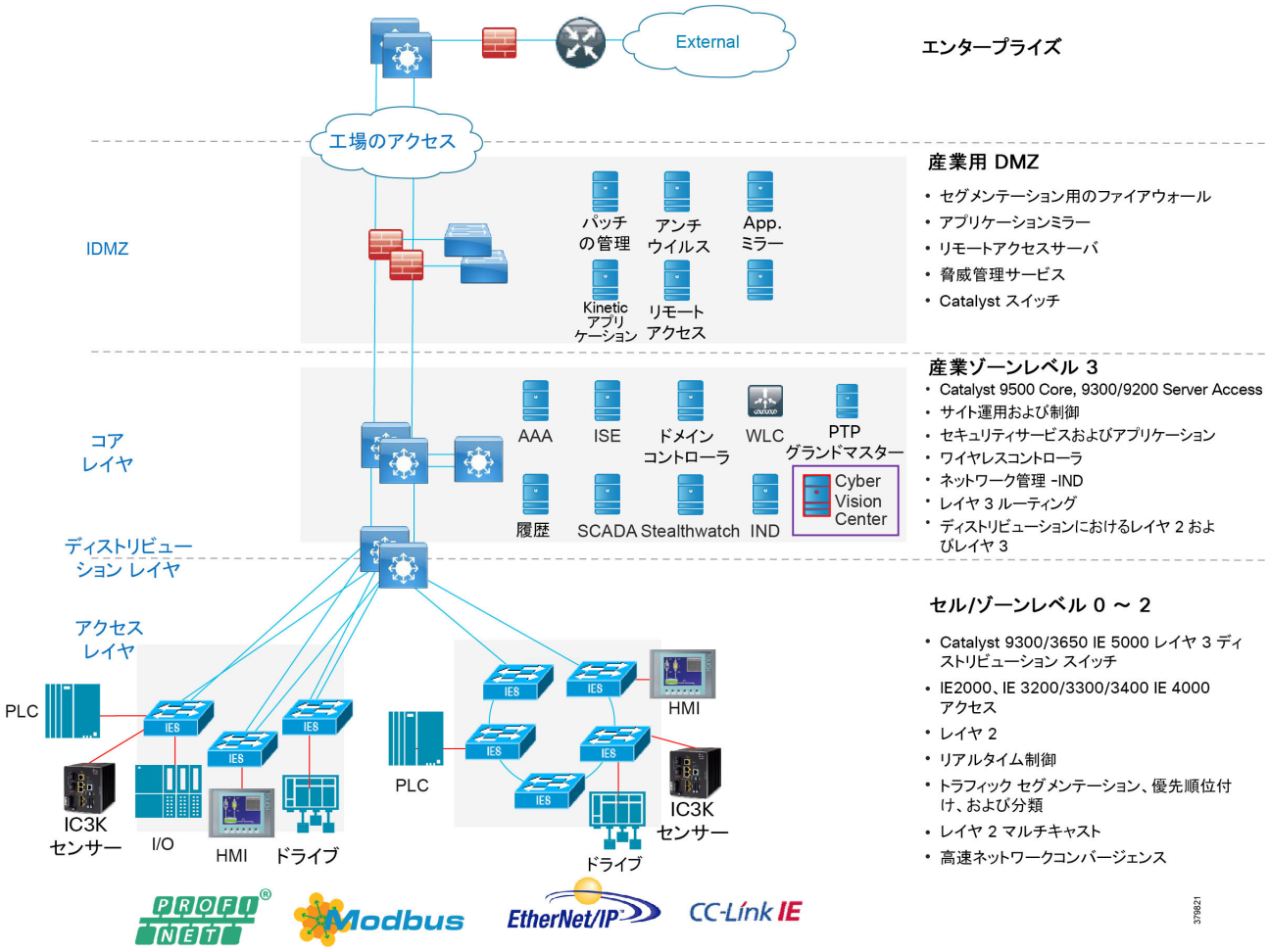
表 3 アクセス ネットワークに関する IACS ネットワーク トポロジ オプションの長所と短所の概要を示します。

表 3　ネットワーク アクセス トポロジ:長所と短所

タイプ	利点	欠点
冗長スター	複数の接続障害からの復元力。 接続喪失に対するより速いコンバージェンス。 一貫したホップ数(通常、フラットな設計では 2 つ)による、予測可能で一貫したパフォーマンスおよびリアルタイム特性。 設計上のボトルネックが少ないことによる、セグメントの過剰サブスクリプションの可能性の減少。	レイヤ 2 アクセススイッチをレイヤ 3 ディストリビューション スイッチに直接接続するために必要な追加の配線(および関連コスト)。 設定の複雑さの増加(複数のブロックを持つスパニング ツリーなど)。
リング	1 つのネットワーク接続が失われた状態からの復元力。 特定の工場フロアレイアウトでのケーブル配線の複雑さの減少。 複数のパスによる、過剰サブスクリプションとボトルネック発生の可能性の減少。	設定の複雑さの増加(単一のブロックを持つスパニングツリーなど)。 比較的長いコンバージェンス時間。 可変ホップ数による、予測可能なパフォーマンスの設計の複雑化。
線形/スター	容易な設計、設定、および実装。 最小の配線量(および関連コスト)。	接続障害が発生した場合のネットワーク サービスの喪失(復元力なし)。 レイヤ 3 デバイスに最も近いリンクでのボトルネックの発生。また、可変ホップ数による、信頼性の高いパフォーマンスの生成の困難化。

企業モデルを IACS アプリケーションおよび Purdue モデルと統合する場合の大まかなリファレンスアーキテクチャを図 13 に示します。このスキームでは、コア、ディストリビューション、アクセスの各レイヤ、サイトの運用と制御、およびセル/エリアゾーンがマッピングされます。これは有線ネットワークのリファレンスアーキテクチャのみです。

図 13　産業用オートメーション ネットワーク モデルと IACS リファレンスアーキテクチャ

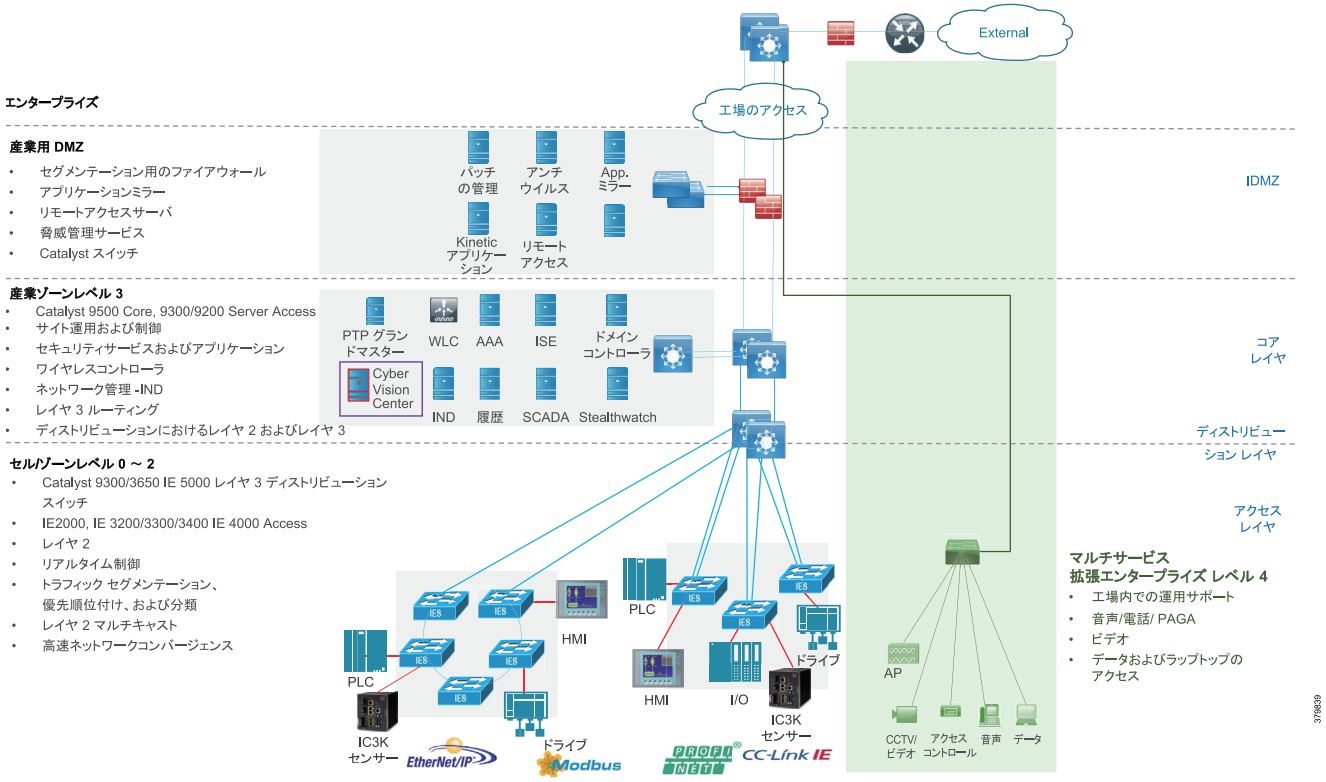


マルチサービストラフィック（非運用アプリケーション）

工場運用通信をサポートするために、複数のサービスを工場に導入できます。これらのサービスは、IACS インフラストラクチャ内で動作する運用システム/アプリケーションの一部ではありません。これらのサービスには、一般に、物理セキュリティ バッジ アクセス、ビデオ監視、およびビジネス対応アプリケーション（メール、テレフォニー、音声システムなど）が含まれます。IACS システムからのマルチサービス アプリケーションのセグメンテーションは、一般的な要件です。IACS プロセス/アセットと同じインフラストラクチャでマルチサービストラフィックを維持するための、規制上の要求、セキュリティ上の懸念事項、リスクの管理、およびビジネスの信頼性により、マルチサービス アーキテクチャが促進されます。

リスク許容度に基づいて検討できるモデルは 2 つあります。一般には、非運用アプリケーションおよびサービス用の個別の物理インフラストラクチャを使用できます。これは、本質的には、非運営アセットがカーペットのないスペースに移動する拡張企業です。図 14 企業から産業工場への接続を示しており、それによって企業ネットワークが拡張されています。より伝統的な企業スイッチを導入できないエリアでは、強化された産業用スイッチが使用されます。電話やビデオカメラなどのアセットも強化が必要になる場合があります。もう 1 つの選択肢は、レベル 3 の同じ物理インフラストラクチャにサービスを導入し、企業から産業用 DMZ を介してサービスを拡張することです。個別のスイッチネットワークをレベル 3 コア スイッチまたはディストリビューション スイッチの外部に導入することで、サービスをプロセスネットワークの外部で維持することができます。IACS トラフィックの確実なプライオリティ付けと確定性の維持を容易にするために、混在するエンタープライズ /IACS QoS モデルおよび帯域幅の使用についても考慮する必要があります。

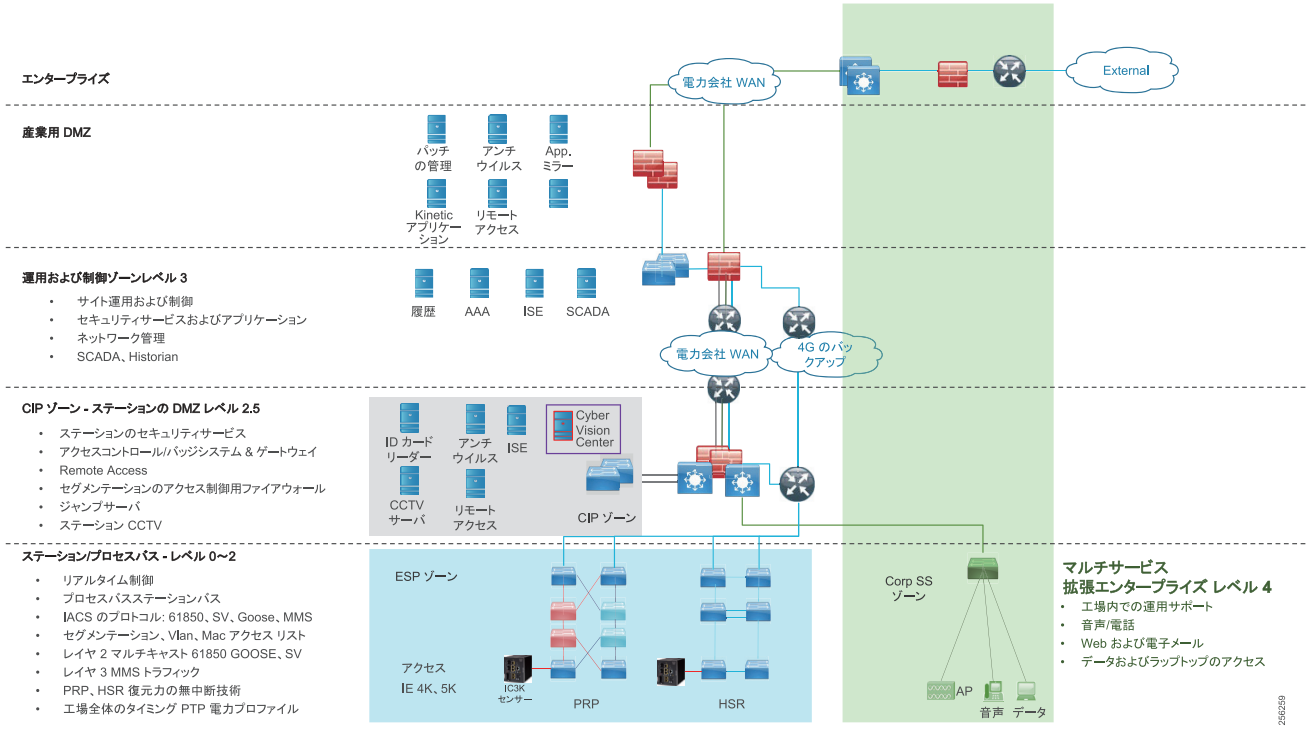
図 14　拡張エンタープライズを使用した産業用自動化



ユーティリティサブステーションのアーキテクチャ

変電所の通信アーキテクチャは、その他の産業と多くの点で共通しています。産業用オートメーションと電力会社はどちらも、プロセス ネットワーク、DMZ、運用/制御、高耐久化、およびタイミングの要件を持っています。ただし、この CVD は、産業工場のセル/エリアゾーン内の IACS プロセス ネットワーク レイヤでの実装と設計に焦点を合わせています。変電所の電子セキュリティ境界（ESP）は大きく異なります。機能ブロックの観点から、図 15 は、産業用オートメーション工場と変電所の 2 つのアーキテクチャに適合します。

図 15　ユーティリティサブステーションのアーキテクチャ



主な違いは、変電所アーキテクチャ内のレベル 3 運用は集中型かつオフサイトであるのに対し、製造/処理施設では、通常、それがオンサイトであり、そこで IACS プロセスが実行されることです。中央集中型サブステーション運用層には、分散型自動化と呼ばれるワイドエリアネットワーク（WAN）上の地理的に離れた場所で複数の変電所をモニタするコントロールセンターがあります。同様のアーキテクチャを持つ業界は、長いパイプラインに沿って製品を輸送/配布する石油/ガスです。パイプラインステーションは長いパイプラインに沿って分散され、プロセスは管理センターで集中管理されます（より大規模のパイプラインステーションおよび変電所では施設内の特定の IACS に対して局所的な管理を行うことができます）。

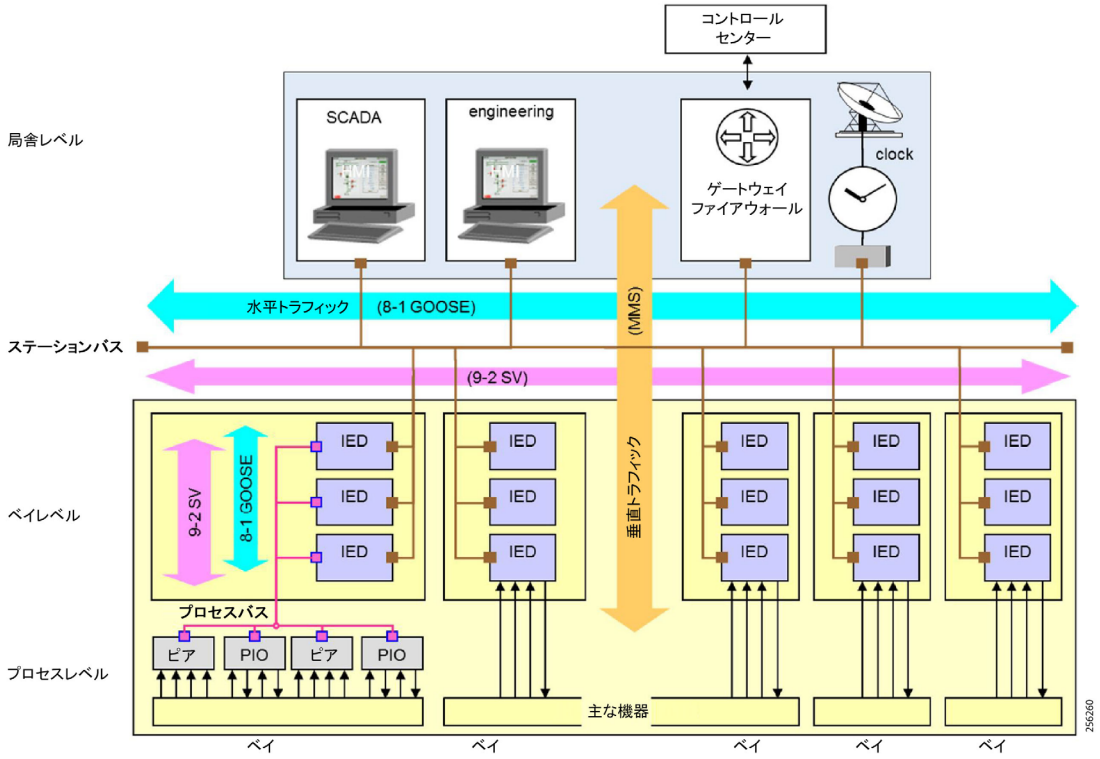
- Critical Infrastructure Protection（CIP）：DMZ は、産業工場アーキテクチャと電力会社アーキテクチャの両方の場所にあります。電力会社内では、この DMZ は、クリティカル インフラストラクチャ/保護ゾーンです。工場はこれをサイトレベル運用レイヤより上位に持っており、変電所はこれを運用レイヤの下位のステーションエッジに持っているという点でわずかに異なりますが、機能は同じままです。DMZ は工場のプロセス/オートメーション産業ゾーンを保護し、CIP は変電所の ESP を保護します。これにより、ゾーン間のセグメンテーションと分離が実現され、ESP へのアクセスが制御されます。調整された CIP 内のサービスには、リモートアクセス、物理セキュリティロギング、および認証、許可、およびアカウンティング（AAA）が含まれます。

- Corporate SubStation（CorpSS）：音声、Web アクセス、電子メールなどの企業および運用サポートサービスは、変電所内の CorpSS ゾーンに配置されます。このゾーンの設計は、産業工場のマルチサービスゾーンのものと同様の考え方に従います。これは企業の拡張であり、WAN を介して配信され、ESP プロセス ゾーンからセグメント化されます。産業工場内では、これらのマルチサービスおよび企業サービスも産業用 IACS ネットワークからセグメント化されます。マルチサービスの導入に関する論理セグメンテーションと物理セグメンテーションの相違については、この産業工場用の CVD で説明します。

- ESP ゾーン：ESP ゾーンは、電力会社のクリティカルなモニタリング/制御インフラストラクチャが存在するゾーンです。リモート端末ユニット（RTU）、インテリジェントな電子機器（IED）、PLC、リレーなどのデバイスは、すべて ESP ゾーン内にあります。これは、Purdue モデル内のレベル 0 ～ 2 に似ています。この ESP ゾーンにはステーションバスとプロセスバスがあります。ステーションバスは変電所全体を接続し、中央管理ベイと個別ベイの間の接続を提供します。ステーションバスは、ベイ内の IED に接続し、ベイを相互に接続して、ベイとゲートウェイルータを接続します。プロセスバスは、主要な測定および制御機器と I/O を IEDs に接続します。通常はベイに限定されますが、バスバー保護および差分保護トラフィックは複数のベイにまたがる場合があります。

図 16（IEC 61850 より）には、ESP とプロセスバスおよびステーションバスのアーキテクチャが示されています。

図 16　IEC 61850 ステーションバス、プロセスバス、およびトラフィックの例



表面のプロセスレイヤにも、同様の設計上の考慮事項があります。どちらのアーキテクチャにも、IACS プロセスの整合性とパフォーマンスを維持するために、高耐久化、安全なセグメンテーション、レイヤ 2 ネットワーキング、マルチキャストのサポート、リアルタイムネットワーク パフォーマンス、およびハイアベイラビリティが必要です。ただし、61850 で定義されているトラフィックタイプを理解することが重要です。これにより、変電所の実装と産業工場との間のプロセスレイヤにおける設計の差別化が進むためです（以下は IEC-61850-90-4 Ed1 から取得されたトラフィッククラスの定義です）。61850 では、変電所アーキテクチャ内の GOOSE およびサンプル値トラフィックを利用しています。GOOSE は、IED がベイ内またはベイ間で「水平に」データを交換することを可能にします。これが、回路ブレーカーのインターロック、測定、トリップなどの作業に使用されます。レイヤ 2 マルチキャストトラフィックに基づいて、GOOSE は、通常、ステーションバス上を流れますが、それをプロセスバスや WAN にまで拡張できます。サンプル値は、主に、センサーから IED にアナログ値（電流と電圧）を送信するために使用されます。このトラフィックは、通常、プロセスバス上を流れますが、ステーションバス上を流れることも可能です。このトラフィックもレイヤ 2 マルチキャストです。MMS トラフィックにより、SCADA、OPC サーバ、ゲートウェイなどの MMS クライアントがすべての IED オブジェクトに「垂直に」アクセスできます。これは、通常のレイヤ 3 IP ユニキャストトラフィックです。

IP ヘッダーなし、GOOSE 用の Ethertype マルチキャスト、および SV トラフィックが優勢であるため、設計は慎重に計画する必要があります。プロセスバスでは、一般に、SV トラフィックが高速であるために、プロセスバス内のデバイス数が 6 に制限されます。トラフィックのフィルタリングは、帯域幅を制限するために、非常に範囲の広い VLAN 設計と MAC アドレス アクセス リストを使用して手動で作成されます。何もルーティングされないために、計画から実装までのこの手動定義は、より複

雑であり、GOOSE と SV のクロス ステーション トラフィックフローを許可するための明確に定義された VLAN および VLAN トランキング設計を考慮する必要があります。トラフィックフローに IP ヘッダーがないために、NetFlow の使用は、GOOSE および SV トラフィックによる ESP でのベースライン トラフィックに制限されますが、このガイドで説明しているように、MMS トラフィックおよびその他の IP ベースのトラフィックは認識され、依然として変電所での異常を識別するために使用できます。セグメンテーションスキームは、主に、範囲指定 VLAN およびレイヤ 2 マルチキャスト アクセス リストを使用して、ステーション全体のマルチキャストトラフィックを制限または許可するために派生する帯域幅であるため、セキュリティアーキテクチャが異なる可能性があります。Trustsec の値と MMS フローの集中型セキュリティ実装（産業工場用に定義されたもの）を評価する必要があります。

表 4 パフォーマンス、アベイラビリティ、マルチキャスト、トラフィック管理、およびセキュリティのエリアにおける、セル/エリアゾーンと ESP の重要な設計上の考慮事項をまとめます。これらは、この CVD に示されている設計と検証のエリアです。アベイラビリティと冗長性では、同様の冗長性プロトコルが使用されます。そのため、設計の違いによる、この CVD での変電所の電力会社 ESP に固有の唯一の検証は、冗長性のエリアの HSR と PRP です。以前に説明した、表 4 で参照されている相違により、特定の変電所設計ガイドには ESP ゾーンの設計ガイダンスが示されています。

表 4　セル/エリアゾーンと ESP の主要な設計上の考慮事項

機能と考慮事項	セルエリアゾーン	ESP ゾーン
IACS プロトコル	CIP、PROFINET、MODBUS、CC-LINK IE。	SCADA Modbus と DNP3。 61850 GOOSE、SV、MMS。
セグメンテーション	VLAN、IP ACL、および TrustSec。	VLAN、MAC、および IP ACL。
マルチキャスト管理	IP IGMP。	伝達を制限し、帯域幅を制限する範囲指定 VLAN、MAC ACL。
タイミング	NTP、PTP デフォルト プロファイル。	PTP 電力プロファイル。
冗長性	REP、HSR、PRP（PRP を減らすにはデュアル インフラストラクチャが必要）。	HSR、PRP、および HSR。
高耐久化および製品	制御されたエリアのディストリビューション レイヤで使用される Cisco Catalyst 非強化型スイッチとアクセス全体で使用される産業用イーサネットスイッチ。 高耐久化コンプライアンスについては、IE 製品のデータ シートを参照してください。	産業用イーサネットスイッチ：一般に ESP 全体にわたって強化されている。 高耐久化コンプライアンスについては、次の IE 製品のデータ シートを参照してください。 https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html
Netflow	IP ベースの IACS トラフィックを使用して工場全体の完全な可視性を提供（PROFINET は例外）。	IP ベースのフローのみ（MMS）。

セル/エリアゾーンの産業用ネットワーキングおよびセキュリティ設計

設計の概要と成果物

ここでは、産業工場環境に見られるサービス、アプリケーション、機器、およびデバイス用の産業用オートメーション ネットワーキング/セキュリティ アーキテクチャについて説明します。産業用有線ネットワークソリューションの設計には、さまざまな業界にわたる多くの共通点があり、その目的は可能なかぎり再利用を促進することです。この設計は、大規模な自動車製造業者、製薬会社、鉱山、石油/ガス処理施設、または精製所のために参照することができます。

おおまかには、このガイドの主な成果物には、セル/エリアゾーン ネットワークおよびセキュリティ設計の提供と、このフレームワーク上に存在する複数の IACS アプリケーションの基盤の構築が含まれます。検証は、新しい復元力プロトコルのサポートし、可視性、セグメンテーション、および異常検出を提供する高度なセキュリティを備え、シスコの次世代産業用イーサネット スイッチ（Cisco IE 3200、Cisco IE 3300、および Cisco IE 3400）に加えてその他のシスコの産業用イーサネットスイッチング製品（Cisco IE 2000、Cisco IE 4000、Cisco IE 5000 など）が導入された、これらの工場のセル/エリアゾーン ネットワークに焦点を合わせています。産業用オートメーション CVD のこのフェーズに含まれる主な機能と新しいプラットフォームは、次のとおりです。

- **SDA 対応プラットフォーム**：セル/エリアゾーンのディストリビューション スイッチとしての Cisco Catalyst 9300 スイッチの導入と検証。Cisco Catalyst 9300 プラットフォームは、今日の SDA をサポートする次世代プラットフォームです。SDA は、Cisco Digital Network Architecture（DNA）の原則に基づいて構築された、業界初の企業向けのインテントベース ネットワーキング ソリューションです。SDA では、ネットワークを再設計することなく、ユーザ、デバイス、およびアプリケーションのトラフィックを分離する自動エンドツーエンド セグメンテーションを実現できます。SDA によってユーザアクセスポリシーが自動化されるため、組織はユーザまたは端末を問わずネットワークのどのアプリケーションにも適切なポリシーを確立できます。管理のしやすさとポリシーを使用した目的主導型のネットワーキングは、産業工場環境にとって有益な追加機能になります。シスコは、産業プラント、倉庫、駐車場、車道/交差点などの部分を管理する非カーペット敷きスペース向けの Cisco IoT 拡張エンタープライズ ソリューションで SDA を利用しています（www.cisco.com/go/iotcvd を参照）。ただし、**SDA は、このソリューションでセル/エリアゾーン内の産業用オートメーションおよび制御（制御ループ）アプリケーションをサポートするために展開することについてはまだ検証されていません。**新しい IE プラットフォームは、SDA が産業工場の要件とプロトコルをサポートできるようになるまでの準備としてのアーキテクチャに位置付けられています。このアーキテクチャにより、SDA スイッチの準備が促進されています。

- **次世代産業用イーサネットスイッチング**：Cisco IE 3200、Cisco IE 3300、および Cisco IE 3400 は、シスコの次世代産業用イーサネット スイッチです。これらのスイッチは、産業用オートメーション用のセル/エリアゾーンに挿入されます。SDA 対応の一環として、Cisco IE 3400 スイッチは、SDA ファブリックエッジスイッチ機能をサポートする産業用イーサネット スイッチング プラットフォームになります。Cisco IE 3400 スイッチと Cisco Catalyst 9300 スイッチは、有線インフラストラクチャで SDA に移行するための基盤を提供します。これにより、SDA 機能が利用可能になったときにそれを有効にするためのプラットフォームが提供されます。現在、これらのプラットフォームは、SDA 非対応スイッチとして導入され、従来のネットワーク スイッチング機能を実行します。

- **ロスレス復元力プロトコル**：Parallel Redundancy Protocol（PRP）、ハイ アベイラビリティ シームレス冗長性（HSR）、および HSR/PRP コンボ ボックスの導入により、業界全体での導入を考慮できる新しいロスレス復元力プロトコルおよびテクノロジー。産業用オートメーションアプリケーションは、従わなければならない厳格な可用性要件を伴う場合があります。したがって、ネットワークの復元力の設計とネットワークトポロジは、これらの要件を満たしやすくする上で非常に重要です。シスコの産業用イーサネット プラットフォームの Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000 は、ロスレス冗長プロトコルの HSR と PRP をサポートしています。これらは、セル/エリアゾーン内の産業用アプリケーションをサポートする際にネットワークのハイアベイラビリティを維持するために役立ちます。

- **ネットワーク可視性と OT 管理**：Cisco Industrial Network Director（IND）を使用したセル/エリアゾーン内の IACS デバイス、アセット、通信の可視性および識別。Cisco Cyber Vision は、OT チームおよびネットワーク管理者が、自社のアセットおよびアプリケーションフローを可視化し、セキュリティのベストプラクティスを実施し、ネットワーク セグメンテーション プロジェクトを推進し、セキュリティリスクを軽減できるようにします。Cisco Cyber Vision は、ベンダーの詳細、ファームウェアとハードウェアのバージョン、シリアル番号、PLC ラックスロットの設定など、実稼働インフラストラクチャの些細な詳細を自動的に発見します。アセットの関係、通信パターン、変数への変更などを特定します。この詳細情報は、さまざまなマップ、表、およびレポートに表示されており、産業用資産の完全なインベントリ、それらの関係、それらの脆弱性、および実行されるプログラムを維持し、産業用イーサネットネットワークにおける運用中心型のネットワーク管理を提供します。このシステムは、PLC、IO、HMI、ドライブなどのオートメーション デバイスを検出するために、ODVA, Inc.、Common Industrial Protocol（CIP）、PROFINET、OPC-UA、Modbus、BACnet などの産業用オートメーション プロトコルをサポートしており、オートメーションおよびネットワーキングアセットの統合トポロジ マップを提供します。このマップにより、工場の OT および IT 担当者に産業用ネットワークを管理および維持するための共通フレームワークが提供されます。この情報は、Cisco Stealthwatch に伝えられ、アセットにコンテキストを提供し、セキュリティモニタリングの属性を確認することに役立ちます。

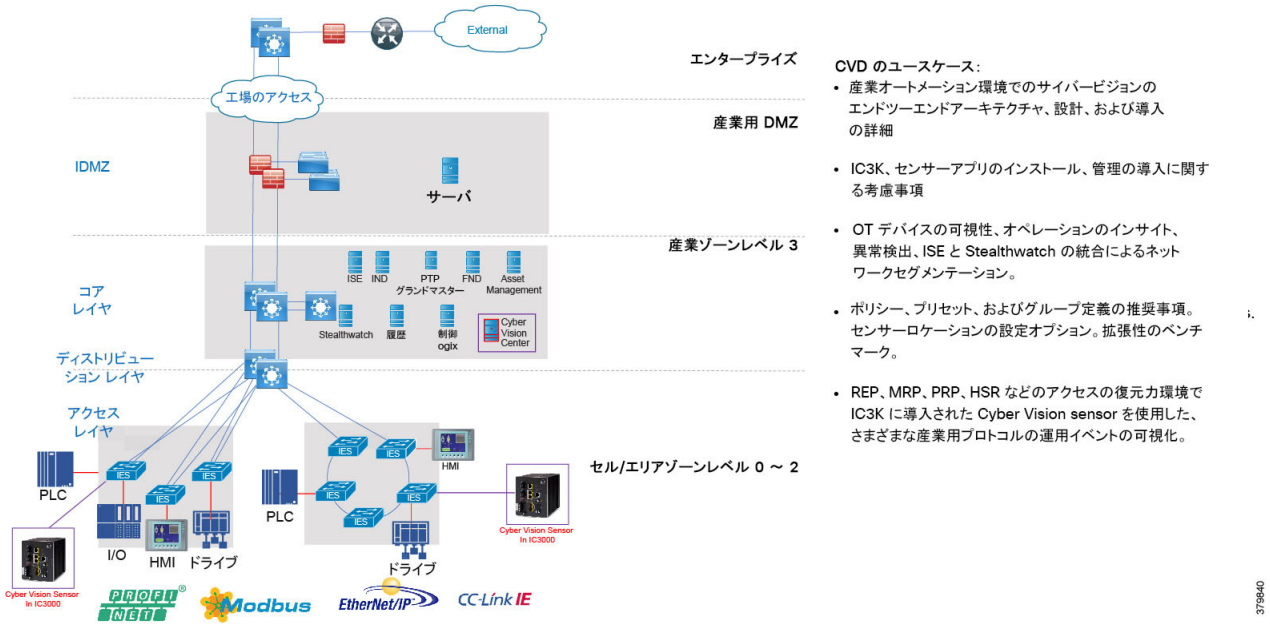
- **Cisco Cyber Vision**：予期しない変数の変更やコントローラの変更などの実際の産業プロセスのステータスについて、リアルタイムのインサイトを OT エンジニアに提供します。システムの整合性と実稼働の継続性を維持するための措置を講じることができます。サイバーエキスパートは、容易にこれらすべてのデータを調べて、攻撃を分析し、送信元を見つけ出すことができます。CISOs には、インシデントレポートを文書化するためのすべての情報が含まれています。Cisco Cyber Visionは、自動化機器によって使用される独自の OT プロトコルを「理解」し、プロセスの異常、エラー、設定ミス、および不正な産業イベントを追跡できます。また、すべてを記録し、産業インフラストラクチャの一種の「フライトレコーダー」として機能します。

  Cisco Cyber Visionは、プロトコル分析、侵入検知、および動作分析を組み合わせて、攻撃の戦術を検出します。この包括的なアプローチにより、Cisco Cyber Visionは、既知の攻撃と未知の攻撃の両方を検出し、攻撃の警告兆候となる悪意のある動作を検出できるようになります。Cisco Cyber Visionは、IT SOC（セキュリティオペレーションセンター）とシームレスに統合されるため、セキュリティアナリストは、OT と IT が相関する SIEM 内の産業イベントをトレースして、攻撃の発生時にファイアウォールフィルタ ルールを自動的にトリガーすることができます。

- **TrustSec と拡張セグメンテーション**:IEC 62443-3-3 に詳細が記載されているセキュリティ実装の重要な要素は、アセットのグループベースポリシーへのセグメンテーションです。産業工場全体にわたってセル/エリアゾーン内で、またセル/エリアゾーンの外部と通信する必要があるアセットとユーザを定義する必要があります。Cisco Cyber Vision は、接続されているアセットの可視性を Cisco ISE に提供します。Cisco ISE は、シスコのインフラストラクチャ全体にわたってセキュリティ チームと OT チームによって定義されるポリシーを作成し、管理します。このガイドでは、業界全体で導入できる、産業工場向けの、シスコのマネージド インフラストラクチャ全体にわたるアセットディスカバリ、ポリシー定義、および TrustSec アプリケーションの推奨事項および検証を提供します。
- **異常検出のための NetFlow と Stealthwatch を使用したセキュリティ**:このガイドには、Stealthwatch を実装し、NetFlow を有効にして、複数の産業における工場の産業ゾーン内で異常検出を実現するための設計提案が含まれています。工場インフラストラクチャを通過するトラフィックの可視性を強化すると、工場全体に広がっているマルウェアの検出といった、異常な動作のトラブルシューティング/強調に役立ちます。Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000 を使用すると、NetFlow を有効にして、データフローメトリックを Stealthwatch に提供できます。Stealthwatch は、ネットワークからフロー データを取得します。また、ネットワーク内で起こり得るマルウェアの伝播を IT セキュリティ担当者が検出することを支援できる、多数の組み込み機械学習アルゴリズムを備えています。

セル/エリアゾーンの設計と推奨事項

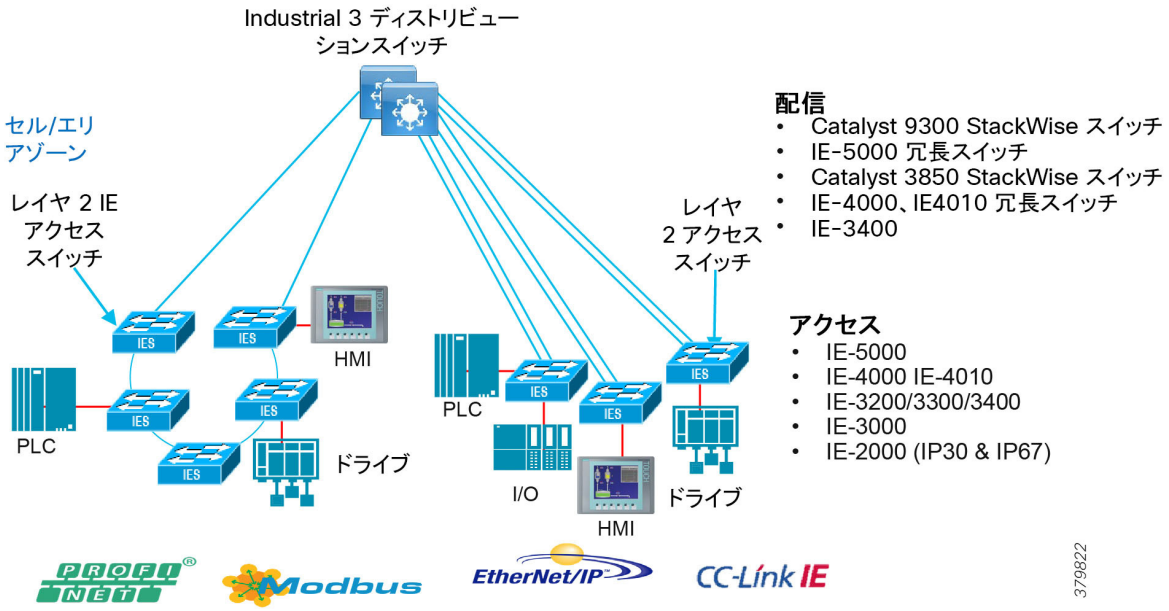
図 17　産業用オートメーション ネットワーク モデルと IACS リファレンスアーキテクチャ



産業ゾーンには、サイト運用(レベル 3)とセル/エリアゾーン(レベル 0 ～ 2)が含まれます。セル/エリアゾーンは、工場フロアの生産またはプロセスを稼働させつづけるためのすべてのシステム、デバイス、コントローラ、およびアプリケーションで構成されます。スムーズな工場フロアの運用と機能を維持することは非常に重要です。そのため、セキュリティ、セグメンテーション、およびアベイラビリティのベスト プラクティスは、設計の重要な要素です。

セル/エリアゾーンは、IACS デバイスおよびコントローラが産業プロセスのリアルタイム制御を実行している重要な機能ゾーンです。このネットワークは、リアルタイムで通信(I/O 通信)する必要があるセンサー、アクチュエータ、ドライブ、コントローラ、およびその他の IACS デバイスを接続します。これは、本質的に、産業用オートメーション アーキテクチャ内の主要な構成要素です。

図 18　セル/エリアゾーン



産業特性と設計上の考慮事項

セル/エリアゾーンはアクセスネットワークですが、従来の IT アクセスレイヤ ネットワークとは要件が大きく異なります。ネットワーキング プラットフォームが適合し、サポートする必要がある重要な要件と産業特性があります。温度、湿度、侵入物などの環境条件には、ネットワーク プラットフォームとは異なる物理特性が必要です。さらに、継続的なアベイラビリティは、産業プロセスの稼働時間を確保し、収益の減少を最小限に抑えるために不可欠です。最後に、産業ネットワークは、IACS システムと統合するために IACS プロトコルのサポートが必要であるという点で IT とも異なります。

以下に、セル/エリアゾーンの設計上の重要な考慮事項を示します。これらは、プラットフォームの選択、ネットワーク トポロジ、セキュリティの実装、および全体的な設計に直接影響します。

- 産業特性：環境条件、工場のレイアウト、およびケーブル接続コストはすべて、設計におけるプラットフォームの選択とネットワーク トポロジに影響を与えます。産業工場および加工施設では、通常、セル/エリアゾーンに物理的に強化されたプラットフォームが必要です。鉱山、石油/ガス精製所、および工場環境は、IT ネットワーキング プラットフォームでは耐えられない厳しい物理的条件にさらされています。広い温度範囲、衝撃/振動、および侵入性の材料に対応して、強化されたプラットフォームが使用されます。

- 相互運用性と相互接続性：産業ゾーン内では、イーサネットが、IACS デバイスおよびプロトコルの相互接続に最適なテクノロジーを提供します。IACS ベンダーは、イーサネットを使用した OSI モデルを標準として採用し、IACS デバイス、コントローラ、および管理サーバの混在する環境向けにネットワークを介した通信を提供しています。ただし、このネットワークは、リアルタイム通信、アベイラビリティ、およびセグメンテーションに重点を置いて、IACS 実装をサポートするように設計する必要があります。

- リアルタイム通信、確定性、およびパフォーマンス：IACS ネットワーク内のパケットの遅延とジッタは、基盤となる産業プロセスに大きな影響を与える可能性があります。産業用アプリケーションに応じて、ネットワークでの遅延または変動や確定性の欠如により、産業プロセスがシャットダウンし、その全体的な効率性が影響を受ける可能性があります。セル/エリアゾーンのネットワーク設計を成功させるための基本要件は、予測可能で信頼性の高いパケット配信を実現することです。設計では、リアルタイム アプリケーションおよび機能に対してより高い確定性とパフォーマンスを提供するために、ネットワークホップ数、帯域幅要件、およびネットワーク QoS/プライオリティ付けを考慮する必要があります。Precision Time Protocol（PTP）も、ネットワークとアプリケーションの確定的な性質を補強するのに役だちます。

- アベイラビリティ：産業用オートメーション内の重要なメトリックは、総合設備効率（OEE）です。クリティカルな IACS 通信のアベイラビリティは、OEE スコアに寄与する重要な要素です。ネットワーク トポロジと復元力の設計選択（QoS やセグメンテーションなど）は、IACS アプリケーションのアベイラビリティを維持し、障害やセキュリティ侵害の影響を軽減することを容易にするために不可欠です。

- セキュリティ：産業用ネットワークのセキュリティについて検討する場合、顧客は、環境を安全で運用可能な状態に保つ方法に関心を持っています。制御システムとプロセスドメインを保護するためのアーキテクチャ的アプローチに従うことをお勧めします。制御階層の Purdue モデル、International Society of Automation 95（ISA95）と IEC 62443、NIST 800-82、および変電所用の NERC CIP は、そのようなアーキテクチャの例です。セル/エリアゾーンの主なセキュリティ要件には、デバイスと IACS アセットの可視性、ネットワークへの安全なアクセス、セグメンテーション、グループベースのセキュリティポリシー、およびインフラストラクチャを保護するためのレイヤ 2 強化（コントロール プレーンとデータ プレーン）が含まれます。

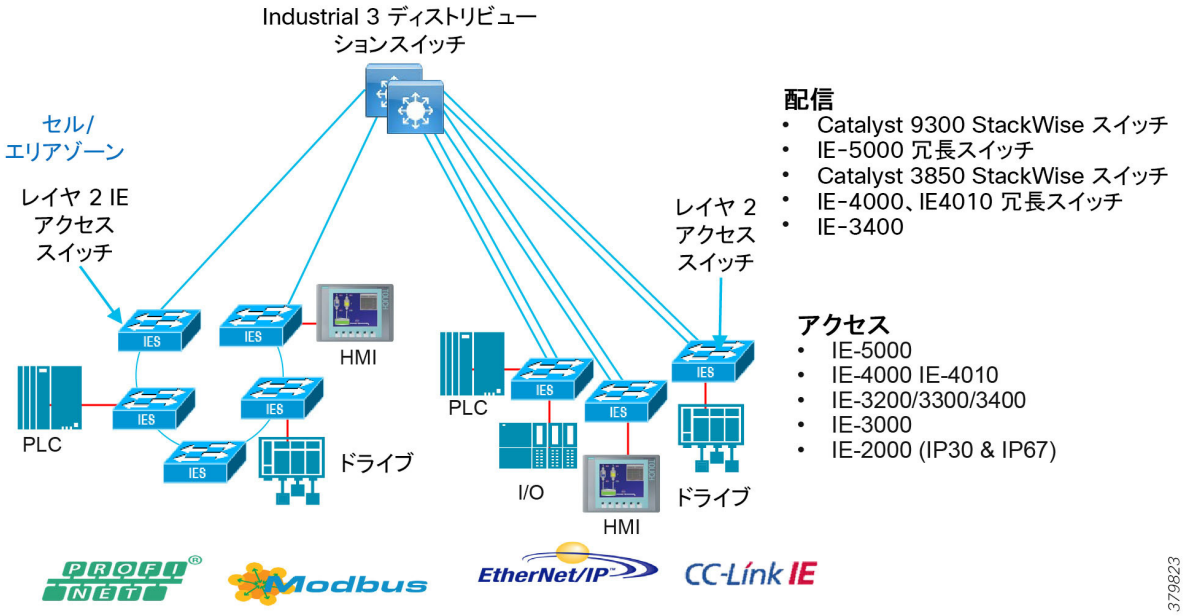
- 管理：工場インフラストラクチャは、これまで以上に高度化され、接続されています。セル/エリアゾーン内には、ネットワークインフラストラクチャを担当する 2 つのペルソナとスキルセット、つまり IT スタッフと OT スタッフが存在します。OT チームは、オートメーション機器のコンテキストでネットワーク情報を提示する、使いやすく、軽量で、インテリジェントなプラットフォームを必要とします。このレイヤの主な機能には、プラグ アンド プレイ、スイッチの容易な交換、およびネットワーク インフラストラクチャを維持するための使いやすさが含まれます。

- トラフィック タイプ：セル/エリアゾーン内の IACS トラフィックの大部分はローカルであり、同じレイヤ 2 ドメイン内に留まります。デバイスからコントローラやワークステーションまたは HMI への非常に短い間隔（数ミリ秒）で通信される周期的な I/O データはすべて、同じ LAN または VLAN 上で発生します。レイヤ 2 マルチキャストは、IACS ネットワークでも使用されます。

セル/エリアゾーンのコンポーネント

シスコには、広範な産業用イーサネットスイッチがあります。アクセスレイヤのセル/エリアゾーン内では、通常、前述の環境条件が、強化された DIN 対応アクセススイッチ（Cisco IE 3400、Cisco IE 4000 など）を選択する際の重要な要素になります。レイヤ 3 ディストリビューション スイッチの要件はそれほど厳しくないため、Cisco Catalyst 3800 や Cisco Catalyst 9300 などのモデルを使用できます。ディストリビューション スイッチは、通常、制御されたカーペット敷きのスペースに配置されますが、やはり産業用プロトコルが必要な場合は、Cisco IE 5000 または Cisco IE 4010 をこのレイヤに配置できます。

図 19　セル/エリアゾーンのコンポーネント



- レベル 0、1、および 2 コンポーネント（デバイス、コントローラ、HMI など）

- レイヤ 2 アクセススイッチ
- レイヤ 3 ディストリビューションスイッチ

表 5 産業環境に不可欠な複数の要因に基づいてスイッチを選択するためのガイダンスを示します。

表 5　産業用オートメーション スイッチングの考慮事項

機能	シスコの産業用イーサネット(IE)	一般的な非産業用スイッチ
フォームファクタ/設置オプション	Din レール、パネル、およびラックマウント	ラック マウント
インターフェイス オプション	6 ～ 28 ポートのポート密度	高いポート密度
PoE 密度/最大電力	6 ～ 28 ポートのポート密度	高いポート密度
電源オプション	DC 入力電圧範囲 = 10 ～ 300*	DC 入力電圧範囲 = 36 ～ 72
環境設計 ■ ファンレス(可動部分なし)対ファン ■ 動作時の温度範囲 ■ 侵入に対する保護(IP)等級 ■ 業界認定	■ ファンレス設計 ■ -30 ～ +60 ℃(+ 85 ℃タイプテスト)* ■ IP30(最大 IP67 のモデル) ■ 振動、衝撃、サージ、ノイズイミュニティのための強化*	■ Fans ■ -5 ～ +45 °C ■ IP XX(指定なし、IP20 以下) ■ エンタープライズクラスの認定
「スワップドライブ」:リムーバブルフラッシュ	可	不可
Dying Gasp:入力電力喪失時	可	不可
アラーム ポート	○(ほとんどのモデルで入力、すべてのモデルで出力)	不可
Deterministic Ethernet IEEE 802.1 TSN	○:Cisco IE 4000 および Cisco IE 5000 でサポート(開発中)	不可
正確なタイミング IEEE 1588 PTP IEEE C37.238-2011(電力プロファイル)	可 IEEE 1588(電力プロファイルの精度レベル(1 ホップあたり 50 ナノ秒)) Cisco IE 5000 での GPS および IRIG-B のオプション(Stratum 3E オンボードオシレータを持つグランドマスターを含む)	不可

セル/エリアゾーンのスイッチングプラットフォーム、産業用セキュリティアプライアンス、および産業用コンピューティングポートフォリオ

以前の産業用オートメーション アーキテクチャと検証済みの設計(Ethernet to Factory、CPWE、Connected Refinery/Processing 工場など)がリリースされて以来、スイッチング プラットフォームは進化してきました。産業用オートメーション アーキテクチャのパフォーマンス、セキュリティ、および機能を向上させるために、新しい機能とハードウェアの能力が追加されました。以下では、アーキテクチャのこのフェーズに強い関連性を持つこれらの機能のいくつかと、将来の利点を示す機能について説明します。

- 産業用スイッチで有効になっている NetFlow エクスポートは、セル/エリアゾーン内のトラフィックへのネットワーク可視性を提供します。Cisco Stealthwatch で NetFlow を使用すると、ネットワークの保護に役立つ異常検出が提供されます。NetFlow は、Cisco IE 3400、Cisco IE 4000、Cisco IE 4010 および Cisco IE 5000 スイッチで利用できます。
- Cisco TrustSec 対応の産業用スイッチは、産業用オートメーションアーキテクチャ全体に拡張可能なセグメンテーションを提供します。
- PRP や HSR などのネットワーク復元力プロトコルは、ロスレス フェールオーバーを提供することでアベイラビリティを向上させます。Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000 は、PRP と HSR の導入をサポートします。
- Cisco Catalyst 3400（SDA 対応）スイッチや Cisco Catalyst 9300 スイッチをアーキテクチャに挿入すると、SDA プラットフォームの準備が整い、インテントベースサービスの導入が可能になります。

図 20 産業用オートメーション工場環境の広範な産業用スイッチングポートフォリオ、セキュリティおよび Cisco Cyber Vision を示します。さまざまな機能要件に対応するために複数のプラットフォームが利用可能です。Cisco IND は、産業工場環境の産業用スイッチをサポートするための管理プラットフォームです。

図 20　シスコの IoT 産業用スイッチ、セキュリティ、サイバービジョン製品のポートフォリオ

表 6　シスコの IoT 産業用スイッチ製品のポートフォリオ

	Cisco IE 2000 access	Cisco IE 4000 access/ distribution	Cisco IE 4010 access/ distribution	Cisco IE 5000 access/ distribution	Cisco IE 3200 access	Cisco IE 3300 access/ distribution	Cisco IE 3400 access/ distribution	Cisco Catalyst 9300
19 インチ	不可	不可	可	可	不可	不可	不可	可
DIN レール	可	可	不可	不可	可	可	可	不可
TrustSec	不可	可	可	可	該当なし	該当なし	可	可
dot1X	可	可	可	可	可	可	可	可
QoS	可	可	可	可	可	可	可	可
NetFlow	不可	可	可	可	不可	HW 対応	可	可
REP	可	可	可	可	可	可	可	可
HSR（HSR-SAN、HSR-PRP）	不可	可	可	可	不可	不可	HW 対応	不可

表 6　シスコの IoT 産業用スイッチ製品のポートフォリオ（続き）

	Cisco IE 2000 access	Cisco IE 4000 access/ distribution	Cisco IE 4010 access/ distribution	Cisco IE 5000 access/ distribution	Cisco IE 3200 access	Cisco IE 3300 access/ distribution	Cisco IE 3400 access/ distribution	Cisco Catalyst 9300
PRP（RedBox）	不可	可	可	可	不可	不可	HW 対応	不可
PROFINET	可	可	可	可	HW 対応	HW 対応	可	不可
MRP	可	可	可	可	HW 対応	HW 対応	可	不可
IND サポート	可	可	可	可	可	可	可	可
SDA 拡張ノード	不可	可	不可	可	不可	HW 対応	可	可
SDA ファブリックエッジノード	不可	不可	不可	不可	不可	不可	可	可
Cisco DNA サポート	可	可	可	可	可	可	可	可

注：表 6 は、この CVD リリースの時点でサポートされているソフトウェアの機能と能力を示しています。最新の機能サポートについては、製品データシートを参照してください。
https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html

表 7 このバージョンの産業用オートメーション CVD で検証されたハードウェアおよびソフトウェア コンポーネントのリストを示します。

表 7　検証済みシスコハードウェア/ソフトウェアコンポーネント

製品の役割	製品	SW Version
アクセス スイッチ	Cisco IE 4000	15.2.7E1
アクセス スイッチ	Cisco IE 4010	15.2.6E2a
アクセス スイッチ	Cisco IE 3400	17.1.1
アクセス スイッチ	Cisco IE 3200	17.1.1
アクセス スイッチ	Cisco IE 2000	15.2.6E2a
アクセス スイッチ	Cisco IE 1000	1.6
ディストリビューション スイッチ	Cisco IE 5000	15.2.7E0s
ディストリビューション スイッチ	Cisco Catalyst 3850	Denali-16.3.7
ディストリビューション スイッチ	Cisco Catalyst 9300	Gilbraltar-16.12.2
コア スイッチ	Cisco Catalyst 6880	15.2.1SY1a
Firewall	Cisco ASA-5525-X	9.4.3、ASDM 7.4.3
ネットワーク ディスカバリ	Cisco IND	1.7
ポリシー管理	Cisco ISE	2.4
異常検出	Cisco Stealthwatch	7.0.2
ネットワークの可視性	Cisco Cyber Vision Sensor	3.0.1
ネットワークの可視性	Cisco Cyber Vision Center	3.0.1
アプリケーション管理とモニタリング	Cisco FND	4.5.1

セル/エリアゾーンの IP アドレス指定

IACS デバイスは、他の IACS デバイスと通信し、さらにレベル 3 サイト運用とも通信するために、IP アドレスを割り当てる必要があります。IACS デバイスの IP アドレスは、静的に、または DHCP サービスを使用して、割り当てることができます。ここでは、静的割り当てまたは DHCP サービスによる割り当てを選択の際に考慮する必要がある要因について説明します。

スタティック IP アドレス指定

一般に、IACS デバイスは、ポートに有線接続されているときにセル/エリアゾーンで移動されることはありません。これは、使いやすさと交換のしやすさに関する要件が存在するためです。最もよく使用されるデフォルトの方法は、運用チームが IACS デバイスに IP アドレスを静的に割り当てることです。IACS デバイスをアドレス指定するための手動 DIP スイッチまたはダイヤルは、依然として、オペレータによる静的な設定を必要とする工場フロアに導入されます。セル/エリアゾーンの IACS デバイスについては、起動プロセス後にデバイスが復帰するまでにかかる時間が非常に重要です。そのため、IACS デバイスが DHCP を使用している場合、IP アドレスの割り当てにかかる時間のために、デバイスが稼働状態になるまでの時間が長くなり、その動作が IACS デバイスのパフォーマンスに影響を与えます。ただし、IP アドレスの規模が増加するにつれて、IP アドレス テーブルの管理はより困難になります。

DHCP を使用した IP アドレスの割り当て

DHCP を使用して IACS デバイスに IP アドレスを割り当てることは、静的割り当てに代わる方法です。DCHP プロトコルは IP アドレスをプールから 割り当てることを可能にする自動プロセスであるため、この方法により、静的割り当て、IP アドレスの管理、および IACS デバイスの IP アドレスの変更に関する問題が解決されます。デバイスを交換したり別の場所に移動する必要がある場合、DHCP サービスが有効になっていると、IACS デバイスは常に DHCP プールから IP アドレスを取得します。

DHCP サービスの考慮事項

IP アドレスを IACS デバイスに割り当てることには、「別の VLAN によって有効になっている別のセルに IACS デバイスを移動するときに、デバイスの要求に応じて DHCP が IP アドレスを自動的に割り当てるため、デバイスに別の IP アドレスを再プロビジョニングする必要がない」といった、いくつかの利点があります。ただし、デバイスの再起動、移動、または交換後にすばやく稼働状態になる必要がある IACS アプリケーションの場合、この遅延の増加により、厳しい要件が満たされない可能性があります。

IP アドレス管理の問題を解決するとともに、DHCP による追加の遅延が生じないようにするため、このガイドでは、セル/エリアゾーンに導入された産業用スイッチで永続性を有効にして DHCP を使用することが推奨されます。DHCP の永続化により、IP アドレスはポートに割り当てられます。この機能により、同じ IP アドレスのプロビジョニングが可能になり、アセットを交換したときに同じ IP アドレスがプロビジョニングされます。IACS の静的な性質のために、これは、使いやすさと交換しやすさを向上させます。

セル/エリアゾーンのトラフィックパターンと考慮事項

IACS ネットワーク内には、リアルタイムトラフィックフローと非リアルタイムトラフィックフローの 2 つのトラフィックタイプがあります。

- リアルタイムトラフィックフローは、通常、IACS デバイスとコントローラの間または 2 つのコントローラの間に発生します。このトラフィックは、非常に頻繁に発生し、同じ VLAN 上のデバイスとコントローラの間で、非常に短い間隔で通信されている周期的な I/O データによって駆動されます。唯一の例外は、インターロックコントローラです。このコントローラでは、リアルタイム データ転送用のトラフィックが、1 つのレイヤ 3 スイッチ ホップを介して VLAN 間で送信されます。一部の IACS プロトコルは、リアルタイムトラフィック用にレイヤ 2/イーサネットのみをサポートします（PROFINET）。これは、確定性と予測可能性の要件も相まって、このトラフィックの大部分をレイヤ 2 でリアルタイムに維持することに適しています。

- 非リアルタイムトラフィックは、IACS 通信ではそれほど重要ではなく、リアルタイムトラフィックと同じ制約やネットワーク要件はありません。これは一般に、事実上、情報提供用であり、レベル 3 運用のワークステーションまたはサーバとレベル 0 ～ 2 のデバイスの間を流れます。このトラフィックは IP/TCP または IP/UDP であり、ルーティング可能です。

マルチキャストトラフィックは、いくつかの重要な IACS 通信プロトコルで使用されるため、セル/エリア IACS ネットワークの重要な考慮事項です。このトラフィックは、通常、ルーティング不可能なので、セル/エリアゾーン内に留まります。

CIP および PROFINET トラフィックフローについて説明している図 21、図 22、表 8、および表 9 に示されているように、リアルタイムトラフィックの大部分はローカルの非リアルタイム管理であり、情報トラフィックは運用および制御レベル 3 にルーティングされます。

表 8　CIP の一般的なトラフィックフロー

次の参照番号: 図 21	遷移元	目的	説明	プロトコル (Protocol)	タイプ	ポート
1a、b、c	プロデューサ (VFD ドライブなど)	コンシューマ (コントローラなど)	プロデューサ (VFD ドライブ、コントローラなど) は、CIP を介してデータを送信します 複数のコンシューマに向けた暗黙的 I/O (UDP マルチキャスト) トラフィック a: デバイスからコントローラへの I/O を表します。 b: コントローラ間の I/O を表します。 c: コントローラによる HMI へのリアルタイム ステータスのレポートを表します。	イーサネット /IP	UDP	2222
2	プロデューサ	コンシューマ	プロデューサは、CIP I/O (UDP ユニキャスト) トラフィックを介してデータをコンシューマに送信できます。	イーサネット /IP	UDP	2222
3	コンシューマ	プロデューサ	コンシューマ (コントローラ、HMI など) は、CIP I/O (UDP ユニキャスト) トラフィックを介して出力データまたはハートビートでプロデューサに応答します。	イーサネット /IP	UDP	2222

図 21　CIP セル/エリアゾーンのトラフィックフロー

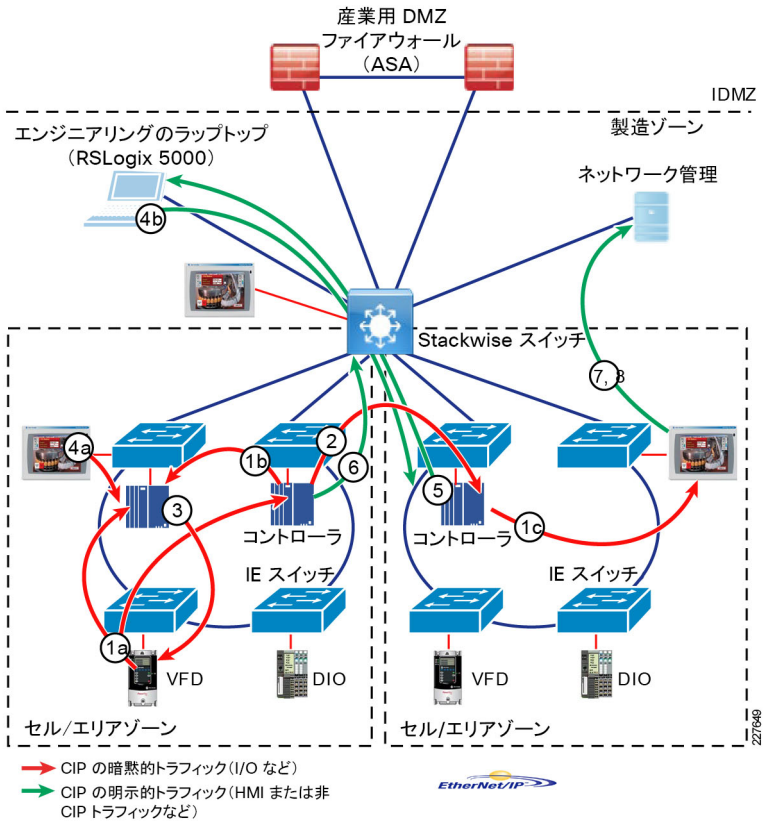


図 22　PROFINET セル/エリアゾーンのトラフィックフロー

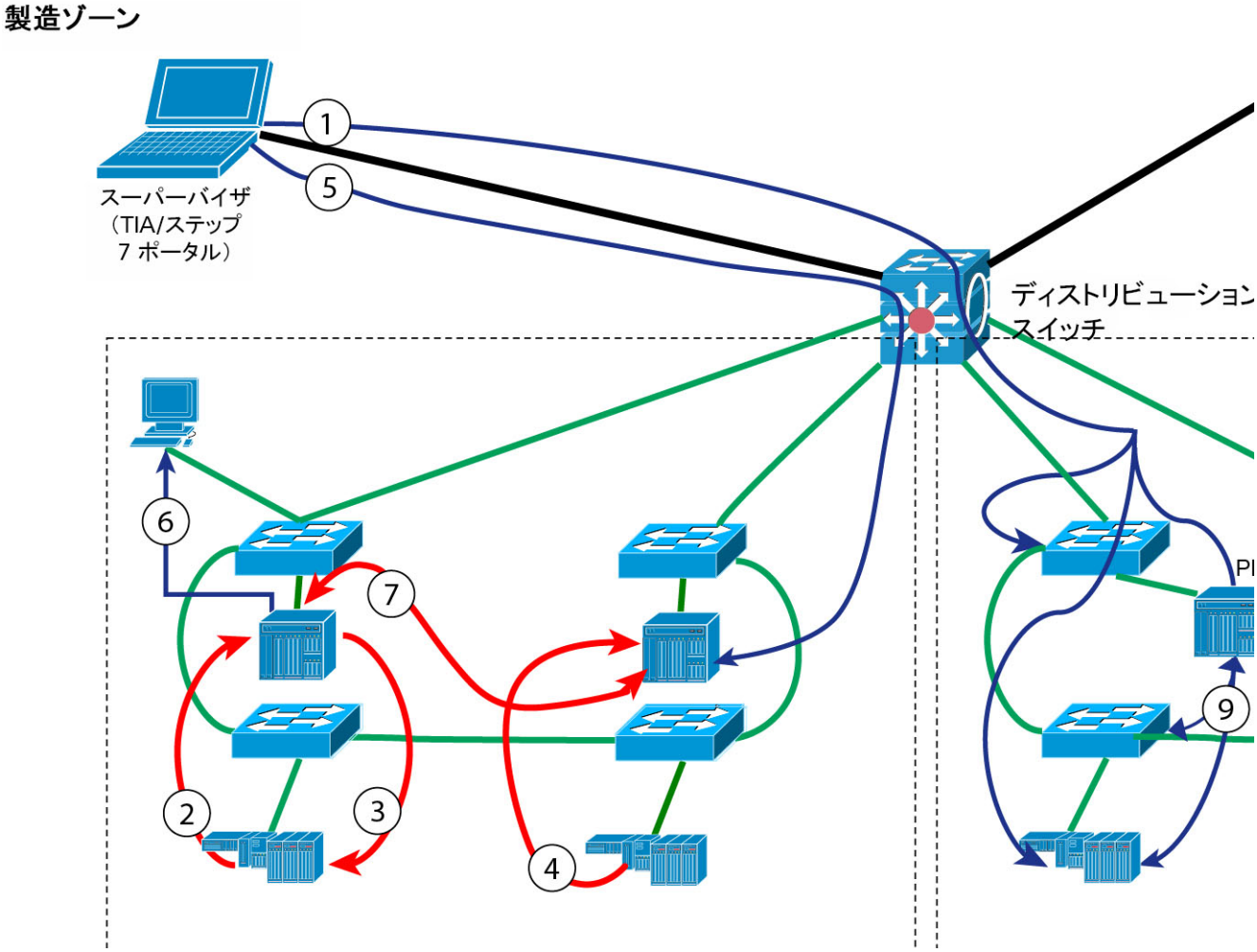


表 9　一般的な PROFINET データフロー

次のトラフィック番号:図 22	説明	遷移元	目的	プロトコル	タイプ
1	スーパーバイザは、PN-DCP または LLDP を使用して LAN 上のすべてのデバイスを検出し、IP アドレスとデバイス名を設定。	TIA ポータル	すべての PROFINET デバイス	PN-DCP/ LLDP	RT/NRT
2	アラーム	デバイス	PLC	PROFINET	RT
3	プロセスデータ	PLC	デバイス	PROFINET	RT
4	プロセスデータ	デバイス	PLC	PROFINET	RT
5	スーパーバイザからプッシュされる設定。	TIA	PLC	TCP/IP	NRT
6	処理情報（または HMI からのアクションの受け入れ）	PLC	HMI	TCP/IP	NRT
7	コントローラ間の通信。	PLC	PLC	PROFINET	RT
8	警告またはステータス通知のためのメール メッセージ。	HMI/PLC	メールサーバ	SMTP	イーサネット
9	すべてのネットワーク インフラストラクチャ（スイッチ、ルータなど）と多くのイーサネットデバイスが、SNMP メッセージを送信できます。	デバイス	ネットワークマネージャ	SNMP	イーサネット

セル/エリアゾーンのパフォーマンスおよび QoS 設計

QoS は、セル/エリアゾーン内のさまざまなトラフィックフローに対して分類、プライオリティ付け、および優先転送処理を提供します。一部の IACS アプリケーション（リアルタイム）には、専用の帯域幅と予測可能なジッタおよび遅延が必要です。QoS はセル/エリアゾーンでこれを提供するために役立ちます。つまり、最も高いパフォーマンス要件を持つ IACS リアルタイムトラフィックフローが、どのトラフィック タイプよりも優先されます。このプライオリティ付けは、ACS アプリケーションの稼働時間と効率性を確保し、最終的に OEE を向上させるために必要なネットワーク パフォーマンス、アシュアランス、および予測可能性の強化に役立ちます。

IACS デバイスを含まないトラフィックタイプもセル/エリアゾーン内に存在します。セル/エリアゾーン内のトラフィックフローの説明にも関係しますが、ワークステーションやサーバから、SNMP トラフィックや HTTP トラフィックなどのレベル 3 トラフィックが発生します。産業関連の顧客は、共有ネットワーク インフラストラクチャ上の産業ゾーンに音声やビデオなどの運用サポートサービスを導入することを選択できますが、これはリスク評価の一環として評価し、コンバージドアーキテクチャ用に定義された QoS モデルに合わせる必要があります。一方で、運用サポートサービスは、独立したネットワーク インフラストラクチャを使用して IACS デバイスおよびアプリケーションから物理的に分離できます。

ネットワークパフォーマンスの予測可能性と一貫性を提供するように設計する際は、IACS アプリケーションのリアルタイムのパフォーマンスと特性をよく理解する必要があります。前述のように、IACS アプリケーションおよびパフォーマンスは、稼働時間、効率性、最終的には OEE を確保するために最も重要です。セル/エリアゾーン内には、遅延、ジッタ、およびパケット損失に関するネットワーク要件が大きく異なるさまざまな IACS トラフィックを導入できます。過度の遅延またはジッタやパケット損失を引き起こすネットワークパフォーマンスの予測不可能性により、IACS システムエラーや機器のシャットダウンが発生する可能性があります。次の表は、さまざまなタイプの情報およびタイムクリティカル I/O トラフィッククラスの定義済みの一連の要件を示しています。

IACS アプリケーションのリアルタイム要件：シスコ

表 10　IACS アプリケーション要件の例

要件クラス	一般的なサイクル時間	一般的な RPI	接続タイムアウト
情報/プロセス（HMI など）	1 秒未満	100 ～ 250 ミリ秒	製品に依存
速度が重視されるプロセス（I/O など）	30 ～ 50 ミリ秒	20 ミリ秒	RPI の 4 間隔（ただし、100 ミリ秒に相当）
安全性	10 ～ 30 ミリ秒	10 ミリ秒	24 ～ 1000 ミリ秒
モーション	500 マイクロ秒～ 5 ミリ秒	50 マイクロ秒～ 1 ミリ秒	4 間隔

表 11　IACS アプリケーション要件の例：PROFINET

要件クラス	一般的なサイクル時間	一般的な RPI	通信クラス
情報/プロセス	1 秒未満	100 ～ 250 ミリ秒	非リアルタイム（NRT）
プロセス/個別	30 ～ 50 ミリ秒	20 ミリ秒	リアルタイム（RT）

表 10 と表 11 は、セル/エリアゾーンに導入できるさまざまな IACS アプリケーション間のネットワーク特性の違いを示しています。主な IACS パフォーマンス要件は、機械/プロセスサイクルタイムと要求パケット間隔（RPI）です。これらが満たされない場合、接続タイムアウトや機器/プロセスのシャットダウンが発生する可能性があります。これらは、通常、次のように定義されます。

- 機械/プロセスサイクルタイム：産業用オートメーションシステム アプリケーションが決定する処理時間。
- I/O 更新時間：入出力が送受信される処理時間。

また、表 10 と表 11 は、情報トラフィックよりもタイム クリティカル トラフィックにより高いネットワーク パフォーマンスを提供し、モーションおよび安全性アプリケーション/システムにはさらに高いパフォーマンスを提供する必要があるネットワークも示しています。産業用オートメーションの QoS 設計は、Common Industrial Protocol（CIP）および Precision Timing Protocol（PTP）トラフィックを使用した QoS モデルに関して、ODVA, Inc. で概説されているガイドラインおよび標準に準拠しています。これらは、次の前提に基づいて構築されています。

- 共有インフラストラクチャに導入する場合、セル/エリアゾーン内の非 IACS トラフィックよりも IACS トラフィックに高いプライオリティが付けられる。
- セル/エリアゾーン内の IACS 非リアルタイムトラフィックよりも IACS リアルタイムトラフィック IACS に高いプライオリティが付けられる。
- リアルタイムサービス内では、安全性やモーションなどのより高いパフォーマンスのアプリケーションをサポートするために、さらなる差別化が必要になる場合がある。
- QoS は一貫した方法で工場全体に導入される。工場全体のネットワークデバイスが同じポリシーに従う必要がある。

表 12　ODVA, Inc. の CIP および PTP トラフィック向け QoS モデル

トラフィックタイプ	CIP のプライオリティ	DSCP レイヤ 3	CoS レイヤ 2	CIP トラフィックの使用状況
PTP イベント（IEEE 1588）	該当なし	59	7	PTP イベントメッセージ（CIP Sync で使用）
PTP 一般（IEEE 1588）	該当なし	47	5	PTP 管理メッセージ（CIP Sync で使用）
CIP クラス 0 / 1	緊急（3）	55	6	CIP Motion
	スケジュール済み（2）	47	5	セーフティ I/O I/O
	高（1）	43	5	I/O
	低（0）	31	3	現時点では非推奨
CIP UCMM CIP クラス 3	すべて（All）	27	3	CIP メッセージ

Cisco QoS は、ツールセットを使用して、IACS トラフィックのプライオリティと優先処理を提供します。このバージョンの産業用オートメーションでは、プラットフォーム全体で使用される主なツールは次のとおりです。

- 分類とマーキング：後続の QoS ツール（スケジューリングなど）で使用される信頼境界を確立するための、トラフィックがネットワークに入るときのトラフィックの分類またはマーキング。クラスマップとポリシーマップは、ネットワーク分類を提供するためのメカニズムです。
- ポリシングとマークダウン：「ポリサー」と呼ばれるポリシング ツールは、パケットが管理上定義されたトラフィック レートに準拠しているかどうかを判断し、それに従って対応します。そのようなアクションには、パケットのマーキング、再マーキング、またはドロップが含まれる場合があります。
- スケジューリング（キューイングとドロップ）：スケジューリング ツールは、フレームまたはパケットがデバイスからどのように出るのかを決定します。速度の不適合などのために、パケットがデバイスを出ることができるよりも速くパケットがデバイスに入ると、輻輳またはボトルネック箇所が発生する可能性があります。デバイスには、プライオリティの高いパケットがより早く出るようにスケジューリングすることを可能にするバッファがあります。これは一般に「キューイング」と呼ばれます。

注：ポリシングとマークダウンは、制御トラフィックに影響を与える可能性があるため、IACS トラフィックの QoS 設計では使用されません。

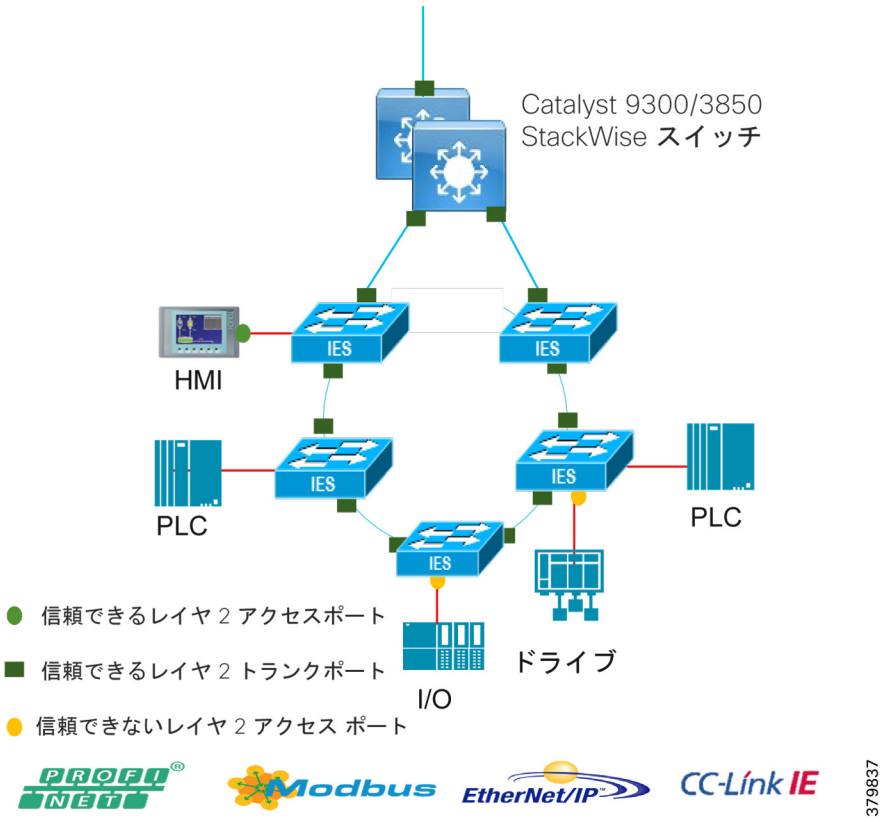
ネットワークへのアクセス ポイントですべてのトラフィックを分類してマーキングします。トラフィックをマーキングできるデバイスは、信頼できるポートを使用してアクセススイッチに接続できます。ネットワークトラフィックをマーキングできないデバイスは、アクセススイッチで分類およびマーキングする必要があり、これらのネットワークポートは信頼できません。一般的なガイダンスは、アクセススイッチに入る CoS/DSCP マーキングを信頼せず、ネットワークに入るすべてのトラフィックをアクセススイッチに分類させ、マーキングさせることです。これにより、ネットワークエッジで一定レベルのアシュアランスと適切な分類が提供されます。

ネットワークスイッチのアップリンクポートとアウトバウンドポートは、分類されれば、そのネットワークでは信頼でき、QoS プロファイルに従ってトラフィックをスケジュールするように設定することが可能です。図 23 信頼できるポートと信頼できないポートの説明を示します。

表 13　QoS の分類/マーキングおよびキューの詳細

	PTP イベント	CIP 緊急（Urgent）	PTP 管理、CIP スケジュール済み、CIP 高	ネットワーク制御	音声データ	CIP 低、CIP クラス 3	音声制御	ベストエフォート			
DSCP	59	55	47、43、	48	46	31、27	24	残り			
CoS	7	6	5	6	5	3	3	4	2	1	0
トラフィック タイプ	PTP イベント	CIP Motion	PTP 管理、セーフティ I/O、I/O	STP など	SIP など	CIP の明示的メッセージ	SIP	残りすべて			
CoS から入力キューへのマッピング	キュー 2							キュー 1			
入力キュー しきい値	3							2	3	2	3
CoS から出力キューへのマッピング	キュー 1	キュー 3				キュー 4		キュー 2			
出力キュー しきい値	3	3				3		3	3	2	3

図 23　QoS 信頼境界



ディストリビューションスイッチを含むセル/エリアゾーン内のすべてのスイッチの入力キューと出力キューは、共有ラウンドロビンメカニズムを使用して処理されます。分類されたトラフィックは、優先処理を提供し、リアルタイムトラフィックでのパケット損失を回避するために、特定の入力キューおよび出力キューにマッピングされます。ネットワーク輻輳時にも一定レベルのサービスが維持される状態を確保および保証し、それによって、特定のアプリケーションに必要な可用性と保証を維持するために、帯域幅をキューに割り当てることができます。ODVA, Inc. モデル内では、プライオリティキューが QoS 設計の最もクリティカルなトラフィックに割り当てられます。これにより、このキューの厳密なプライオリティ付けが確保されます。

表 14 と表 15 に、産業用オートメーションの一部としてテストされた設計内のスイッチの QoS 設定を示します。これらの設定は、CIP トラフィックに関する ODVA, Inc. の QoS 推奨設定から取得されました。

表 14　入力キューの詳細

入力キュー	キュー（Queue）#	CoS からキューへのマッピング	トラフィックタイプ	キューの重み	キュー（バッファ）サイズ
SRR 共有	1	0、1、2	残りすべて	40%	40%
プライオリティ	2	3、4、5、6、7	PTP、CIP、ネットワーク 制御、音声、ビデオ	60 %	60 %

表 15　出力キューの詳細

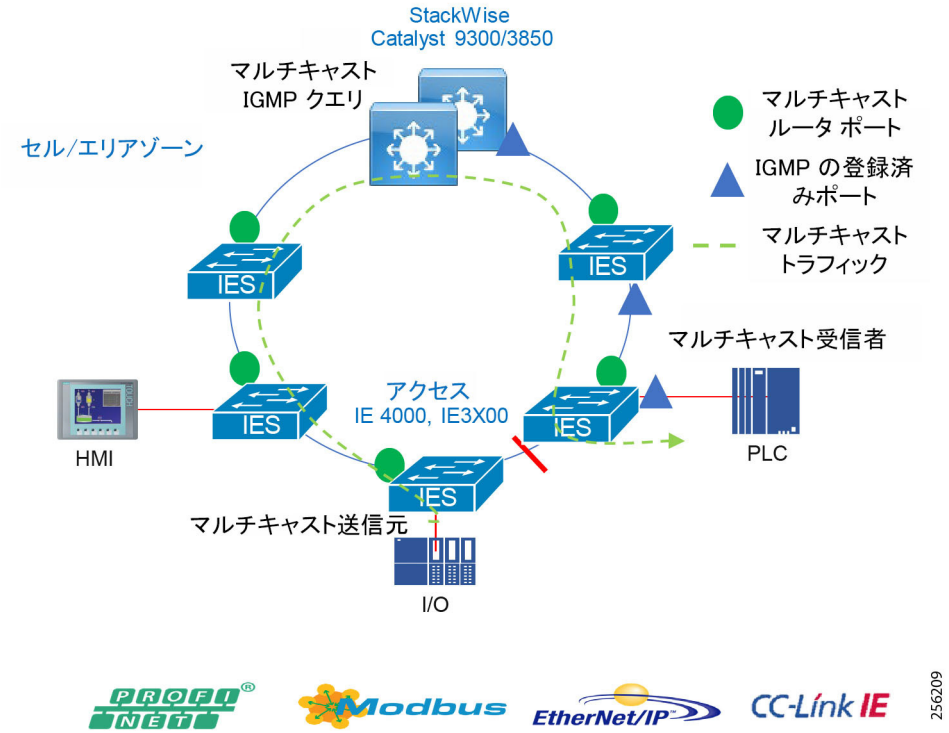
出力キュー	キュー #	CoS からキューへのマッピング	トラフィック タイプ	キュー の重み	Gb ポートのキュー サイズ	10/100 ポートのキュー サイズ
プライオリティ	1	7	PTP イベント	1	10	10
SRR 共有	2	0、1、2、4	残りすべて	19	25	25
SRR 共有	3	5、6	PTP 管理、CIP の暗黙的 I/O、ネットワーク制御および音声データ	40	40	40
SRR 共有	4	3	CIP の明示的メッセージ	40	25	25

設定の詳細と、すべてのスイッチのスケジューリングメカニズムの詳細については、「Quality of Service（211 ページ）」を参照してください。この一連のテストで評価されたスイッチには、Cisco IE 2000、Cisco IE 4000、Cisco IE 3200、および Cisco IE 3400 と、Cisco Catalyst 9300 および Cisco Catalyst 3850 が含まれていました。

セル/エリアゾーンおよび ESP でのマルチキャスト管理

一部の IACS プロトコルではマルチキャストが使用されるため、セル/エリアゾーン内のネットワークスイッチは、マルチキャストのサポートを支援する必要があります。一般に、セル/エリアゾーンのマルチキャストトラフィックはレベル 2 を超えません。一部のプロトコルでは、IP パケット内で TTL を 1 に維持するといった、ルーティングされる境界の通過を防ぐためのメカニズムが使用されます。レイヤ 2 マルチキャストネットワークのコンテキスト内では、マルチキャストトラフィックを管理および制御するために Internet Group Management Protocol（IGMP）スヌーピングが使用されます。図 24 マルチキャストを使用して導入される IACS トラフィックをサポートするためのセル/エリアゾーン内のコンポーネントと機能を示しています。

図 24　セル/ゾーンマルチキャスト



- IGMP スヌーピング：レイヤ 2 スイッチで IGMP スヌーピングを使用すると、スイッチはマルチキャストパケットのスイッチングを、それを必要とするポートだけに制限できます。
- IGMP クエリア：マルチキャストグループのメンバーシップを継続的に追跡します。クエリアは、指定されたマルチキャスト グループに属するネットワーク デバイスを検出するためのクエリー メッセージを送信するネットワーク デバイスです。
- マルチキャスト ルータ（Mrouter）ポート：IGMP クエリアに面しているポートまたはマルチキャストおよびクエリー トラフィックが受信されるポート。スヌーピング スイッチは、IGMP メンバーシップ レポートを、マルチキャストルータの接続先または IGMP クエリーの送信先（クエリア）のポートにだけ転送する必要があります。

セル/エリアゾーンへのマルチキャスト導入の推奨事項

- すべての産業用イーサネットスイッチおよびディストリビューション スイッチ/ルータで IGMP スヌーピング/クエリアを有効にします。IGMP スヌーピングのデフォルト設定は変更しないでください。
- ディストリビューション スイッチ上に、またはセル/エリアゾーン トポロジの中心に、IGMP クエリアを設定します。1 つの VLAN に複数の IGMP クエリアがある場合、IGMP プロトコルは、クエリア機能を引き継ぐために、最小の IP アドレスを持つクエリアを要求します。そのため、ディストリビューション スイッチは、サブネット内で最小の IP アドレスを持つ必要があります。

可用性

産業用オートメーションプロセスのアベイラビリティは、ビジネスに直接影響するため、非常に重要な要素です。IACS アプリケーションの稼働時間を確保するには、堅牢で復元力のあるネットワークが必要です。ここでは、プラットフォームプロトコルとパス冗長性によって IACS アプリケーションの可用性をサポートするためのネットワーク設計について説明します。

QoS とパフォーマンスのセクションでは、RPI とサイクル タイムが、ネットワークをサポート可能にするために必要な主要指標でした。サイクルタイムは、ネットワークアベイラビリティの不可欠な要件です。プロセスのシャットダウンを引き起こす可能性がある IACS アプリケーションのタイムアウトを防ぐために、ネットワークはサイクル タイム内に回復する必要があります。ネットワークがサイクル タイム内に障害から回復できる場合、理論上は、IACS アプリケーションが動作しつづけます。これを念頭に、表 16 に IACS のターゲット ネットワーク コンバージェンス時間のリストを示します。

表 16　産業用オートメーション ネットワーク コンバージェンスの目標

要件クラス	目標サイクル時間	目標 RPI	目標ネットワーク コンバージェンス
情報/プロセス（HMI など）	1 秒未満	100 ～ 250 ミリ秒	1 秒未満
速度が重視されるプロセス（I/O など）	30 ～ 50 ミリ秒	20 ミリ秒	100 ミリ秒未満
安全性	10 ～ 30 ミリ秒	10 ミリ秒	24 ミリ秒未満
モーション	500 マイクロ秒～ 5 ミリ秒	50 マイクロ秒～ 1 ミリ秒	1 ミリ秒未満

メディアの考慮事項

メディアは、ネットワークの障害発生時のコンバージェンス時間を改善する上で大きな役割を果たします。銅線イーサネットリンクを使用すると、光ファイバよりもコンバージェンス時間が長くなり、補足的なキープアライブメカニズムなしでは障害の検出にかかる時間が長くなります。これは、実施されたコンバージェンステストのいくつかに反映されています。Cisco IE 3x00 スイッチを使用するトポロジでは、REP Fast を使用して全体的なコンバージェンス時間を改善できます（特に銅線接続の場合）。リンク障害が発生すると、REP 高速コンバージェンス時間は光ファイバと銅線の間で比較されます。

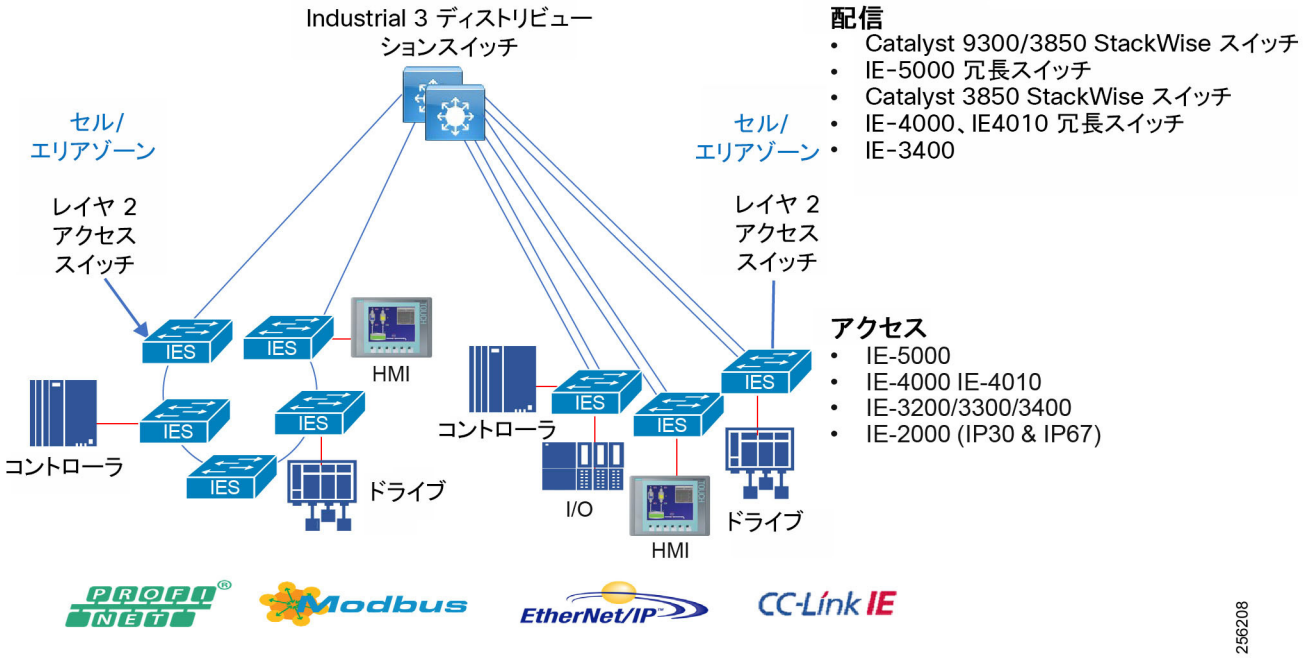
リングを集約した具体的な Cisco Catalyst 9300 プラットフォームは Cisco Catalyst 9300-48P でした。このプラットフォームのテスト時には、サポートされている銅線ダウンリンクのみがサポートされています。1/10 Gbps アップリンクモジュールは、光ファイバ メディア コンバージェンス番号を提供するために評価されました。特定のシナリオでは銅線ダウンリンクも評価されました。

ディストリビューション スイッチの復元力

ここでは、セル/エリアゾーン境界のディストリビューション スイッチで産業用オートメーション用に検証された復元力オプションについて説明します。

- Cisco StackWise-480
- ホットスタンバイ冗長プロトコル

図 25　ディストリビューション スイッチの復元力



Cisco StackWise-480

Cisco Catalyst 3850 および Cisco Catalyst 9300 は、StackWise-480 設定をサポートし、ディストリビューション レイヤでプラットフォームの復元力を提供します。スイッチ スタックは、StackWise-480 ポート経由で接続された最大 8 つのスタック対応スイッチで構成できます。スタック メンバーは 1 つの統合システムとして連携します。レイヤ 2 プロトコルとレイヤ 3 プロトコルが、スイッチ スタック全体を単一のエンティティとしてネットワークに提示します。

スイッチ スタックには、必ず 1 個のアクティブ スイッチおよび 1 個のスタンバイ スイッチがあります。アクティブスイッチは、スタックの管理プレーンの制御を提供します。アクティブスイッチが使用できなくなると、スタンバイスイッチがアクティブスイッチの役割を引き継ぎ、スタックの動作可能状態を維持します。このバージョンの産業用オートメーションでは、セル/エリアゾーンのディストリビューション スイッチの復元力を提供するために、スイッチスタックが 2 つのスイッチを使用して検証されました。

Cisco Catalyst 9300 のスイッチスタック設定および機能の詳細については、次のドキュメントを参照してください。
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/stck_mgr_ha/b_169_stck_mgr_ha_9300_cg/managing_switch_stacks.html

ホットスタンバイ冗長プロトコル

ホットスタンバイ冗長プロトコル（HSRP）は、ディストリビューション スイッチに関して StackWise-480 に代わるものです。HSRP は、ネットワーク上のホストからの IP トラフィックの冗長性を介してハイアベイラビリティを提供します。ルータインターフェイスのグループでは、アクティブルータがパケットを送信します。スタンバイルータは、アクティブルータに障害が発生した場合、または事前に設定された条件が満たされた場合に、ルーティング作業を引き継ぎます。CVD では、HSRP シナリオ用に 2 つのレイヤ 3 対応スイッチ（1 つはアクティブ、もう 1 つはスタンバイ）が導入されました。

StackWise Virtual

ディストリビューション レイヤのもう 1 つのプラットフォームの復元力オプションは StackWise Virtual です。Cisco Catalyst 9500 スイッチおよび Cisco IE 5000 スイッチは StackWise Virtual をサポートします。ここで 2 つのスイッチは冗長 10 ギガビットまたは 40 ギガビットのリンクを介して接続され、アクティブノードおよびスタンバイノードを備えた単一のスイッチとして動作します。StackWise-480 とほぼ同じように、レイヤ 2 およびレイヤ 3 機能は、単一の「仮想」エンティティから動作し、コントロール、マネジメント、およびデータプレーンは統合されています。StackWise Virtual の制限事項は、REP、RSPAN、および SDA のサポート十分ではないことです。そのため、本リリースでは、StackWise Virtual のコンフィギュレーションは検証されていません。

パス冗長性

ネットワークパスの冗長性は、機器またはリンクに障害が発生したときに、ネットワークを介して代替パスを提供します。セル/エリアゾーン内では、スタートポロジまたはリングトポロジを使用して、エッジ スイッチング プラットフォームからのすべてのアップリンクで、このネットワーク冗長性が提供されます。冗長リンク内でループが発生することを防ぐには、復元力プロトコルを導入する必要があります。同じ宛先への複数のアクティブパスがある場合、ループはレイヤ 2 ネットワークで作成されます。リングトポロジ内では、Resilient Ethernet Protocol（REP）、Media Redundancy Protocol（MRP）、PRP、および HSR によってフレームのループを防ぎ、スタートポロジ内では、EtherChannel または Flex Link によってフレームのループを防ぐことができます。

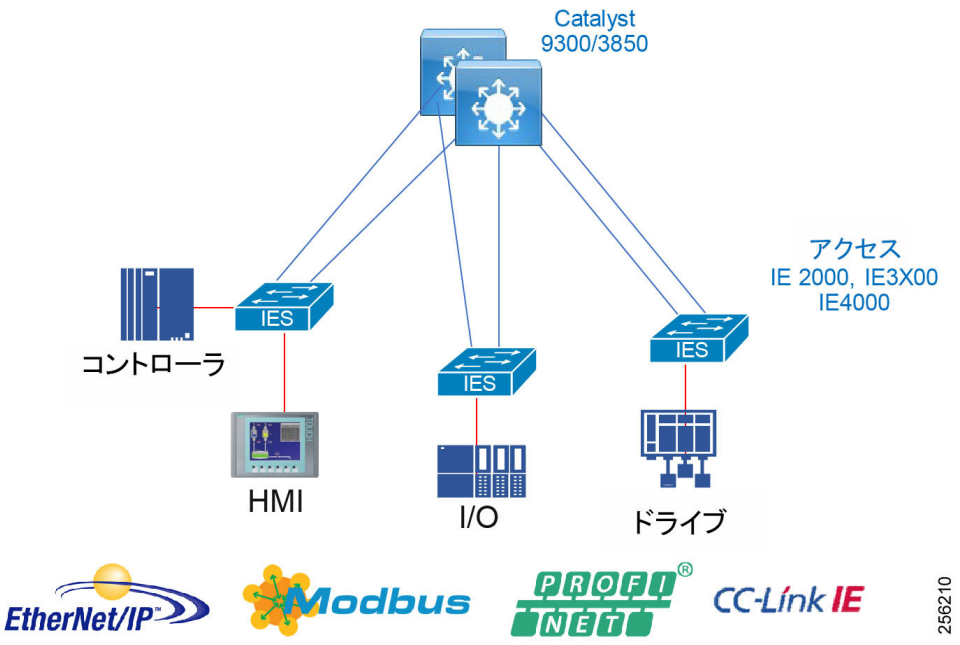
- スタートポロジの冗長性：EtherChannel または Flex Link
- リングトポロジの冗長性：MRP、REP、および HSR
- 複数の独立したネットワークの冗長性：PRP

冗長スタートポロジ

EtherChannel

EtherChannel は、複数の物理イーサネットリンクを 2 つのスイッチ間の単一の論理リンクにグループ化します。2 つのスイッチ間の論理リンクを通過するトラフィックは、物理リンクでロードバランスされます。EtherChannel 内で物理リンクに障害が発生すると、トラフィックは EtherChannel 内の他の利用可能なリンクに再ディストリビューションされます。厳密には復元力プロトコルではありませんが、同じ 2 つのスイッチ間に複数のリンクがある場合に復元力を提供するために EtherChannel を導入できます。産業用オートメーションでは、アクセススイッチ（Cisco IE 4000 など）と StackWise を実行しているディストリビューション スイッチを接続する場合、これが冗長スター構成のオプションとして設定されます。

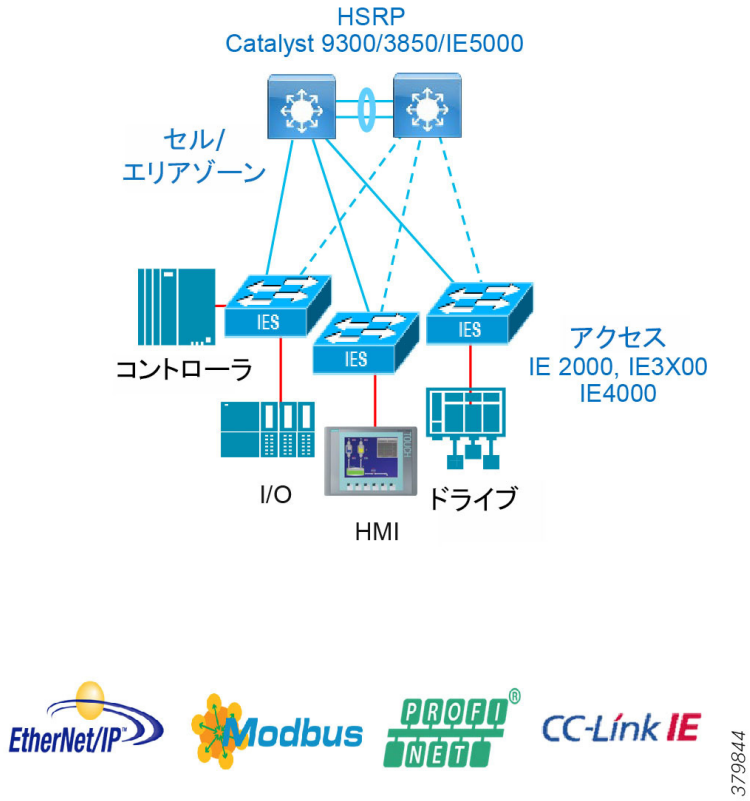
図 26　セル/エリアゾーンの冗長スタートポロジ



Flex Link

Flex Link は、レイヤ 2 インターフェイス（スイッチポートまたはポートチャネル）のペアで、1 つのインターフェイスがもう一方のバックアップとして機能するように設定されています。この機能は、スパニングツリープロトコル（STP）の代替ソリューションを提供し、アクセススイッチとディストリビューション スイッチの間に導入されます。アクティブリンクはフレームの送受信に使用され、スタンバイリンクはフレームを送受信しませんが、状態はアップ/アップです。アクティブリンクで障害が検出されると、スタンバイリンクがアクティブに移行し、すべての MAC アドレスとマルチキャストエントリがスタンバイリンクに移動します。このリンクは、障害が発生したリンクが復元されると、再びスタンバイ リンクになります。

図 27　セル/エリアゾーンの Flex Link



注：Cisco IE 3200、Cisco IE 3300、および Cisco IE 3400 スイッチは、この CVD で使用されているソフトウェアの Flex Link をサポートしていません。

冗長スターの設計と検証

以下の図は、産業用オートメーションとコンバージェンス時間に関して説明するさまざまなシナリオの詳細を示しています。

Cisco Catalyst 9300 スイッチと Cisco Catalyst 3850 スイッチは、EtherChannel を使用した冗長スター構成において Cisco IE 3200/Cisco IE 3400 スイッチおよび Cisco IE 4000 スイッチで評価されました。Cisco IE 3200/Cisco IE 3400 については、EtherChannel だけが評価されました。図 28 検証シナリオを示します。

図 28　冗長スターの設計と検証

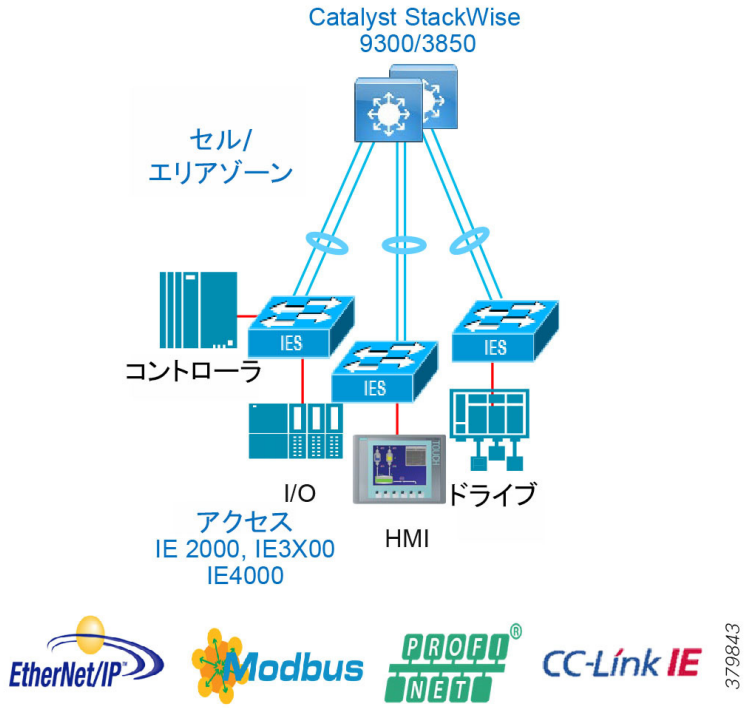


表 17 と表 18 に、複数のタイプの障害に関するコンバージェンスの結果の詳細を示します。「リンクの中断」は、リングでの単一のリンク障害を指します。「スイッチ障害」は、プライマリ ディストリビューション スイッチの障害を指します(バックアップスイッチがアクティブの役割を引き継ぎます)。最大コンバージェンス時間と平均コンバージェンス時間を記録した場所では、複数のリンクおよびスイッチの障害を発生させました。検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。

表 17　Cisco Catalyst 9300 によるスタートポロジ

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3200/Cisco IE 3400 光ファイバ		コンバージェンス Cisco IE 3200/Cisco IE 3400 銅線		コンバージェンス Cisco IE 4000 銅線	
		最大	平均	最大	平均	最大	平均
リンク	L2 マルチキャスト	90	69	320	95	94	53
	L2 ユニキャスト	90	69	320	95	94	53
	L3 ユニキャスト	90	69	320	95	94	53
スイッチ	L2 マルチキャスト	238	48	733	170	102	44
	L2 ユニキャスト	106	41	152	60	102	44
	L3 ユニキャスト	106	48	152	64	102	44

表 18　Cisco Catalyst 3850 によるスタートポロジ

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3x00 光ファイバ	
		最大	平均
リンク	レイヤ 2 マルチキャスト	248	86
	レイヤ 2 ユニキャスト	128	52
	レイヤ 3 ユニキャスト	128	60
スイッチ	レイヤ 2 マルチキャスト	228	176
	レイヤ 2 ユニキャスト	226	180
	レイヤ 3 ユニキャスト	226	170

結果の説明

Cisco Catalyst 9300 の銅線ダウンリンクと Cisco IE 3200/Cisco IE 3400 を使用したリンク障害のコンバージェンスは、Cisco IE 4000 を使用した場合よりもはるかに大きな値になりました。

これらのシナリオでは、Cisco Catalyst 3850 と Cisco Catalyst 9300 の両方をディストリビューション スイッチとして使用することで、Cisco IE 3200/Cisco IE 3400 の光ファイバテストが大幅に改善されました。

- ディストリビューション スイッチとして Cisco Catalyst 9300 を使用する場合、Cisco IE 3200/Cisco IE 3400 は、接続タイムアウトを引き起こす可能性がある異常値を持つ IACS アプリケーションに銅線メディアを使用するときは、Cisco IE 3200/Cisco IE 3400 は推奨されません。
- Cisco Catalyst 9300 を使用すると、ディストリビューション スイッチの障害により、レイヤ 2 マルチキャスト トラフィックのコンバージェンス時間が長くなり（238 ミリ秒）、マルチキャストを使用する IACS アプリケーションで接続タイムアウトが発生する可能性があります。アプリケーションは、マルチキャストに対応するか、マルチキャストが使用される可能性がなくなるように、調整することができます。

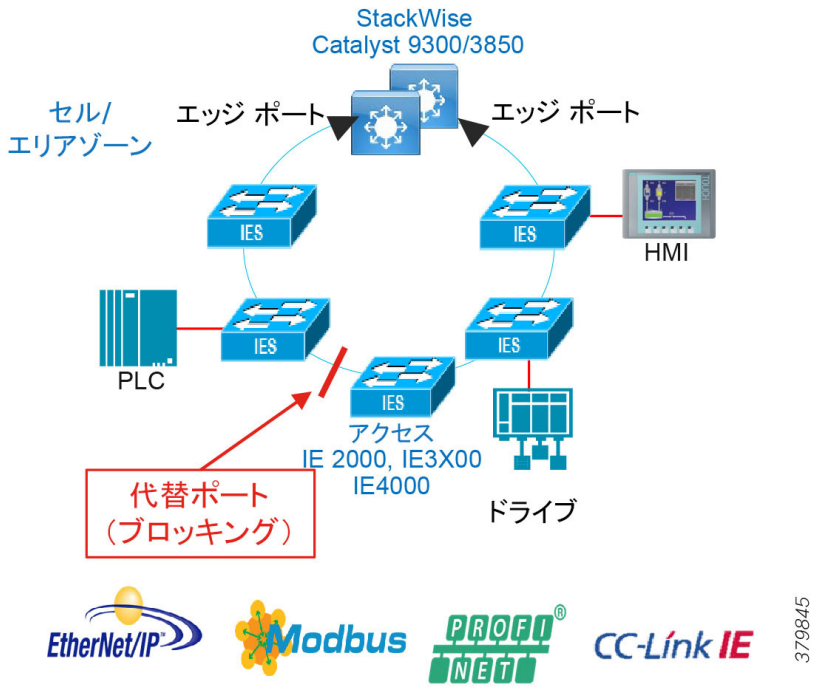
リング復元力プロトコル

REP

REP はシスコ独自のプロトコルで、STP に代わるプロトコルとして、ネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントまたは物理リングごとに単一の冗長インスタンスを実行します。1 REP セグメントは、相互接続しているポートのチェーンで、セグメント ID が設定されています。各セグメントは、標準(非エッジ)セグメント ポートと、2 つのユーザ設定エッジ ポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは 2 つまでで、各セグメントポートにある外部ネイバーは 1 つだけです。

ネットワーク セグメントの各エンドは、隣接する Cisco IE アクセススイッチまたはディストリビューション スイッチで終端されます。セグメントが終端するポートはエッジ ポートと呼ばれます。図 29 産業用オートメーションで導入される一般的な REP セグメントを示します。

図 29　REP の概要



リング内のループの防止は、セグメント内でブロック状態になっている 1 つのポート(「代替ポート」とも呼ばれます)によって維持されます。セグメントで障害が検出されると、代替ポートが転送状態に移行し、トラフィックが代替パスを通過してネットワーク障害を回避することが可能になります。

REP の基本動作とフェールオーバー

どの REP 対応ノードも、セグメント内で障害通知をトリガーできます。リンク障害は、STP の場合のように、リングマスターノード(障害時に他のすべてのノードを更新します)の存在に依存しません。REP ノードは、確認応答を求める hello パケットを送信するリンクステータスレイヤとのネイバー隣接関係を維持します。リングのセグメント障害は、信号の損失か接続の損失(hello への無応答)によって検出されます。ノードは、障害を検出すると、リンク障害通知をその REP ピアに送信します。産業環境で高速コンバージェンスを維持するために、Cisco REPは、高速障害通知を使用し、予約済みマルチキャストアドレスを使用して通知を伝播します。通知は、セグメント内の各ノードにただちに通知されるように転送されます。これにより、代替ポートが転送状態に移行し、セグメント上のすべてのスイッチの MAC アドレス テーブルのフラッシュが行われます。

図 30　障害発生時に削除される REP ブロッキングポート

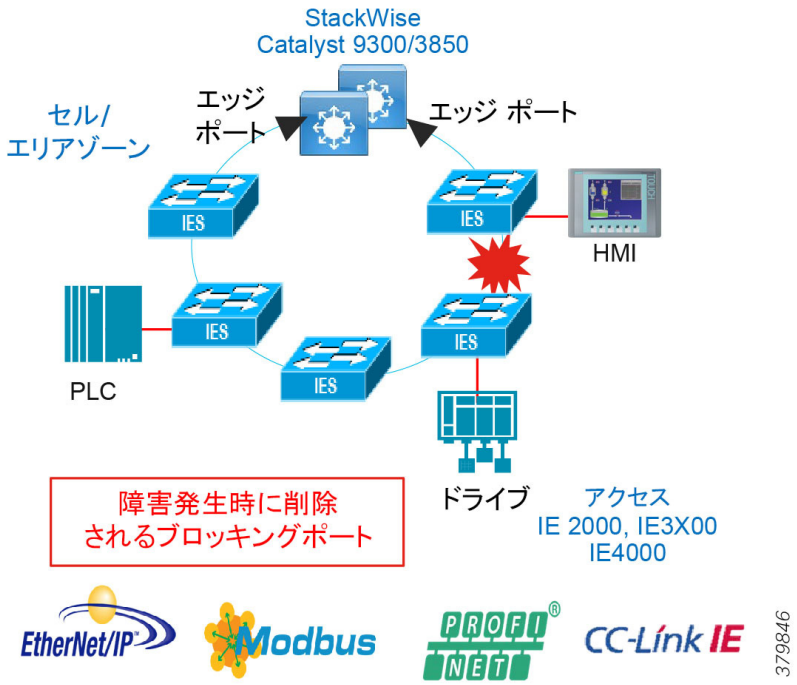
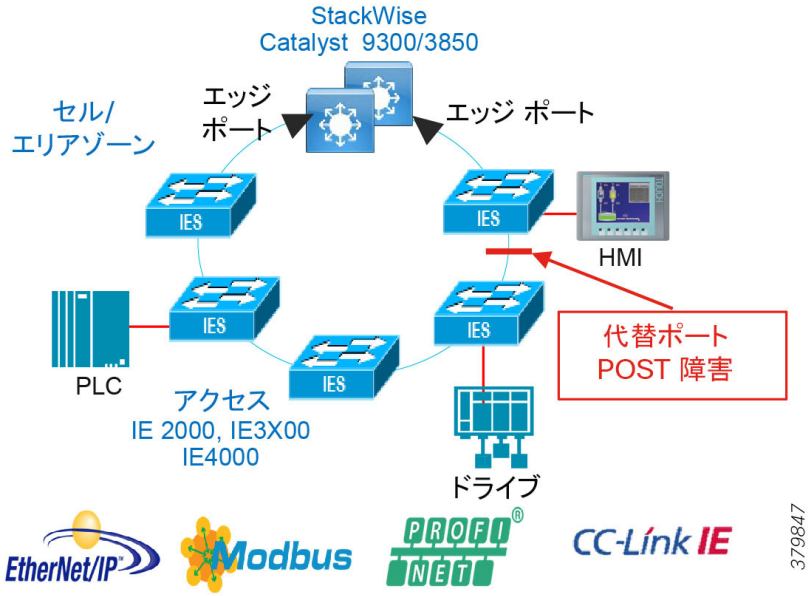


図 31　REP 代替ポート POST 障害



障害から回復すると、障害点が新しい代替ポートになり、リングの中断が回避されます。障害から回復した後に必要な既知の望ましい状態がある場合は、ブロックされたポートをリング内の特定の場所に配置するようにプリエンプションを設定できますが、このプリエンプション イベントにより、リングの中断が発生します。

REP トポロジの設計と推奨事項

表 19　ディストリビューションにおける Cisco IE 5000 による REP リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3x00 光ファイバ		コンバージェンス Cisco IE 3x00、IE4000 光ファイバ		コンバージェンス Cisco IE 3400H 銅線	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	344	88	380	93	538	259
	レイヤ 2 ユニキャスト	344	92	212	99	558	266
	レイヤ 3 ユニキャスト	344	70	484	149	732	282
スイッチ	レイヤ 2 マルチキャスト	500	114	234	117	4368	990
	レイヤ 2 ユニキャスト	502	119	234	126	4368	995
	レイヤ 3 ユニキャスト	1224	387	1322	546	4368	951

結果の説明

- コンバージェンスは、VLAN 内のレイヤ 2 トラフィックと同じリング内の VLAN 間のレイヤ 3 トラフィックに関して検証されました。
- 「リンクの中断」は、リングでの単一のリンク障害を指します。スイッチの障害は、一度に 1 つのスイッチの電源が中断したことを意味します。ディストリビューションメンバーと IE スイッチは、テスト中にリロードされました。
- 検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。
- このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。
- 次の 3 つの REP リングがあります。
  - 混合リング：Cisco IE 3200、Cisco IE 3300、Cisco IE 3400、および Cisco IE 4000（12 ノード）
  - IE 3x00 リング：Cisco IE 3200、Cisco IE 3300、および Cisco IE 3400（11 ノード）
  - IE 3400H リング：Cisco IE 3400H（4 ノード）

ディストリビューションにおける Cisco Catalyst 3850/Cisco Catalyst 9300 による REP リング

このトポロジの推奨事項：

- 銅線リンクより高速なコンバージェンスを提供する光ファイバ リンクを使用することをお勧めします。
- REP リングによるディストリビューションに StackWise を使用する場合は、プライマリ スタック メンバーに電源障害が発生した場合の レイヤ 3 コンバージェンスを向上させるために、アクセススイッチ間に代替ポートを配置することをお勧めします。

図 32　ディストリビューションにおける Cisco Catalyst 3850/Cisco Catalyst 9300 による REP リング

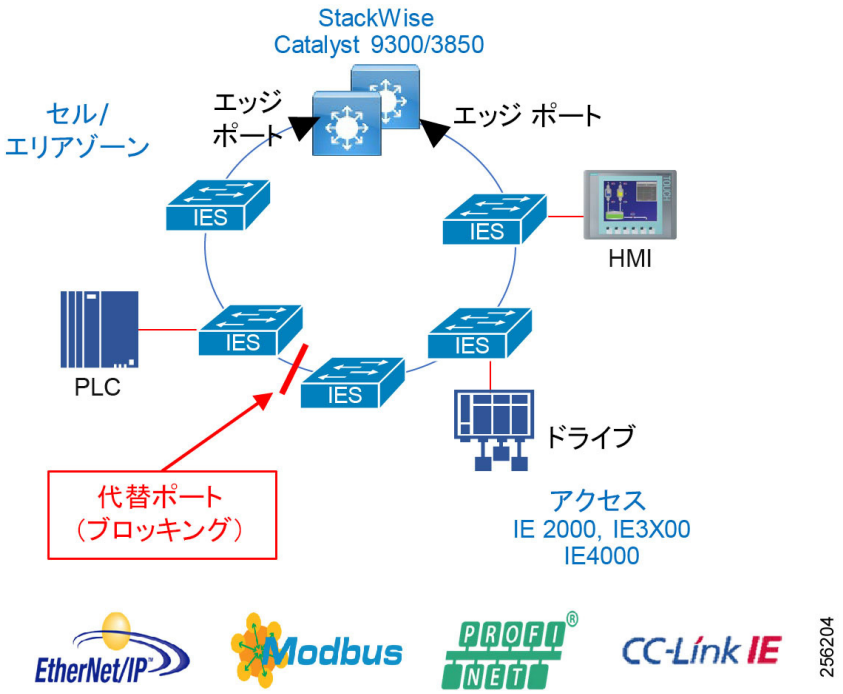


表 20 検証中のコンバージェンス結果の概要を示します。

表 20　ディストリビューションにおける Cisco Catalyst 9300 による REP リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3x00 光ファイバ		コンバージェンス Cisco IE 3x00、IE4000 光ファイバ		コンバージェンス Cisco IE 3400H 銅線	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	118	45	374	77	918	227
	レイヤ 2 ユニキャスト	116	44	284	75	920	232
	レイヤ 3 ユニキャスト	116	43	284	72	920	237
スイッチ	レイヤ 2 マルチキャスト	616	171	220	132	4116	475
	レイヤ 2 ユニキャスト	618	164	216	142	4116	1073
	レイヤ 3 ユニキャスト	972	436	1002	413	59128	1434

結果の説明

- コンバージェンスは、VLAN 内のレイヤ 2 トラフィックと同じリング内の VLAN 間のレイヤ 3 トラフィックに関して検証されました。
- 「リンクの中断」は、リングでの単一のリンク障害を指します。スイッチの障害は、一度に 1 つのスイッチの電源が中断したことを意味します。ディストリビューションメンバーと IE スイッチは、テスト中にリロードされました。
- 次のスイッチを使用して、3 つの REP リングが評価されました。
  - 混合リング：Cisco IE 3200、Cisco IE 3300、Cisco IE 3400、および Cisco IE 4000（12 ノード）
  - IE3x00 リング：Cisco IE 3200、Cisco IE 3300、および Cisco IE 4000（11 ノード）
  - IE3400H リング：Cisco IE 3400H（4 ノード）
- Cisco Catalyst 9300 ディストリビューション ノードには 2 つのスタックメンバが含まれています。
- 検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。

Cisco IE 3x00 アクセススイッチを使用した Cisco Catalyst 9300 ディストリビューション StackWise 設定は、IACS 環境向けの REP 導入に最適な選択と見なす必要がありますが、IACS アプリケーションの接続タイムアウトを引き起こす可能性があるコンバージェンスのための outlier Max 結果を考慮する必要があります。

REP Fast

Cisco IE 3x00 スイッチでサポートされている REP Fast 機能は、REP と同じ機能を備えていますが、参加しているスイッチ間の障害検出時間が改善されます。スイッチは、各 REP Fast インターフェイスに対して 2 つのタイマーを実行し、正常に送信されたかどうかを判断します。スイッチがネイバーノードにビーコンフレームを送信すると、最初のタイマーは 3 ミリ秒ごとに実行されます。フレームを受信すると、タイマーがリセットされます。フレームが受信されない場合、2 番目のタイマーが開始され、10 ミリ秒間継続します。フレームが依然として受信されない場合は、スイッチはリンクダウン通知を送信します。REP 高速コンバージェンスの仕様は 50 ミリ秒ですが、従来の REP の範囲は 50～250 ミリ秒です。

Cisco IE 3x00 シリーズスイッチは、銅線および光ファイバに対して REP Fast をサポートし、両方のメディアが同様のリンク障害コンバージェンス時間を生成します。さらに、REP と REP Fast を同じリングで使用して、Cisco IE 3x00 スイッチを REP Fast をサポートしていない他のモデルに接続することもできます。この REP Fast の検証は、それぞれのディストリビューションスイッチに Cisco IE 3x00 スイッチを接続する従来の REP を使用して、ハイブリッド REP および REP Fast リングにより行われました。

図 33　ディストリビューションにおける Cisco Catalyst 9300 による REP および REP Fast リング

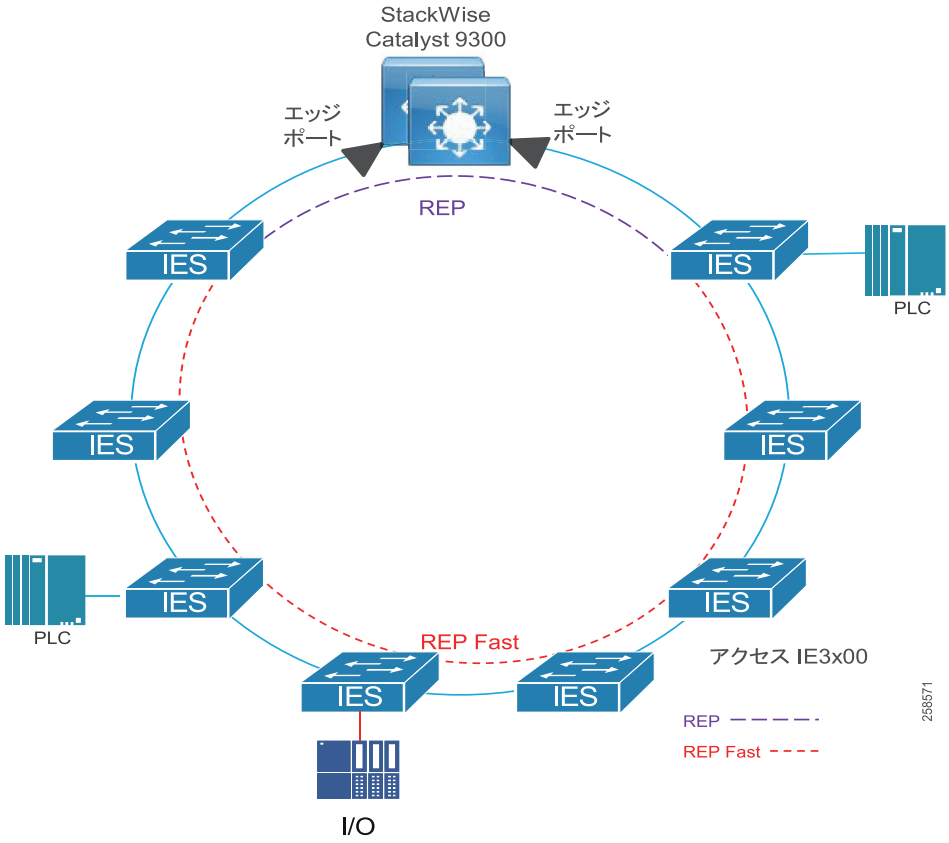


表 21　ディストリビューションにおける Cisco Catalyst 9300 による REP および REP Fast リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3x00 光ファイバ		コンバージェンス Cisco IE 3400H 銅線	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	118	61	62	32
	レイヤ 2 ユニキャスト	166	58	44	16
	レイヤ 3 ユニキャスト	166	55	48	23
スイッチ	レイヤ 2 マルチキャスト	212	72	4310	1002
	レイヤ 2 ユニキャスト	212	62	750	240
	レイヤ 3 ユニキャスト	212	77	846	432

図 34　ディストリビューションにおける Cisco IE 5000 による REP および REP Fast リング

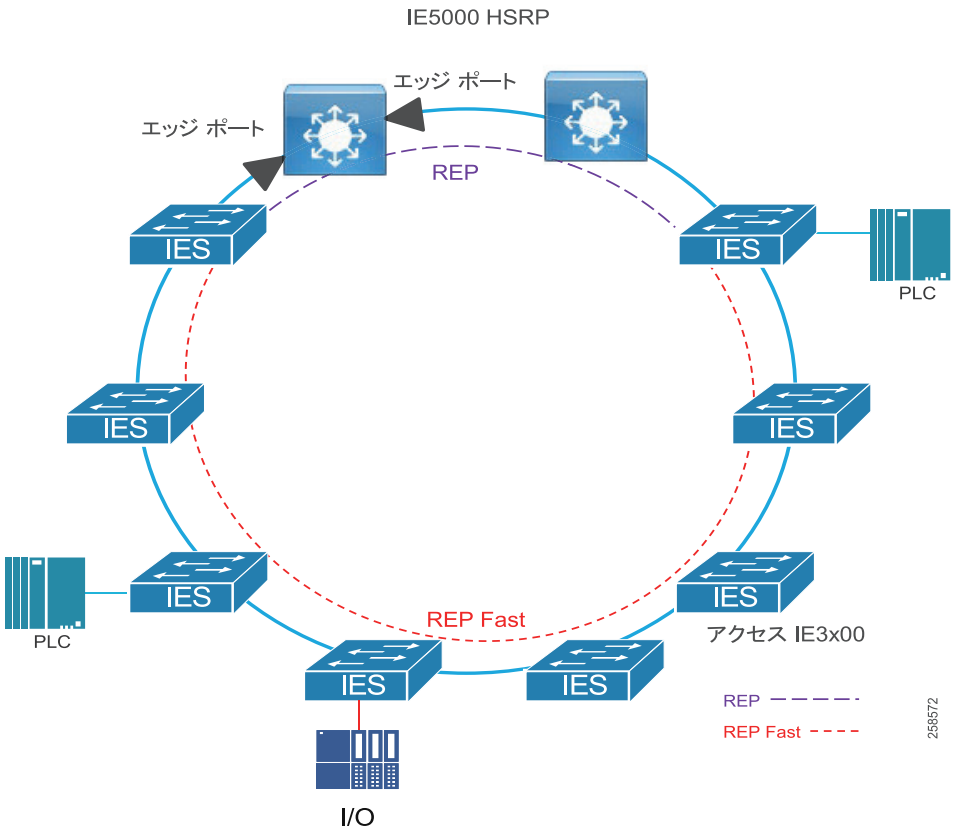


表 22　ディストリビューションにおける Cisco IE 5000 による REP および REP Fast リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 3x00 光ファイバ		コンバージェンス Cisco IE 3400H 銅線	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	210	76	70	24
	レイヤ 2 ユニキャスト	210	78	56	15
	レイヤ 3 ユニキャスト	210	79	66	23
スイッチ	レイヤ 2 マルチキャスト	58	32	3554	662
	レイヤ 2 ユニキャスト	80	35	376	193
	レイヤ 3 ユニキャスト	1040	268	1066	480

結果の説明。

- テストされた 2 つのリングには、次のタイプの IE スイッチが含まれています。
  - IE 3x00（11 ノード）：Cisco IE 3200、Cisco IE 3300、および Cisco IE 3400
  - Cisco IE 3400H（4 ノード）
- コンバージェンスは、VLAN 内のレイヤ 2 トラフィックと同じリング内の VLAN 間のレイヤ 3 トラフィックに関して検証されました。
- 「リンクの中断」は、リングでの単一のリンク障害を指します。リンク障害は、REP と REP Fast の両方のエリアのリング内にあるさまざまなポイントで処理されました。スイッチの障害は、一度に 1 つのスイッチの電源が中断したことを意味します。ディストリビューションメンバーと IE スイッチは、テスト中にリロードされました。
- 検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。
- このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。

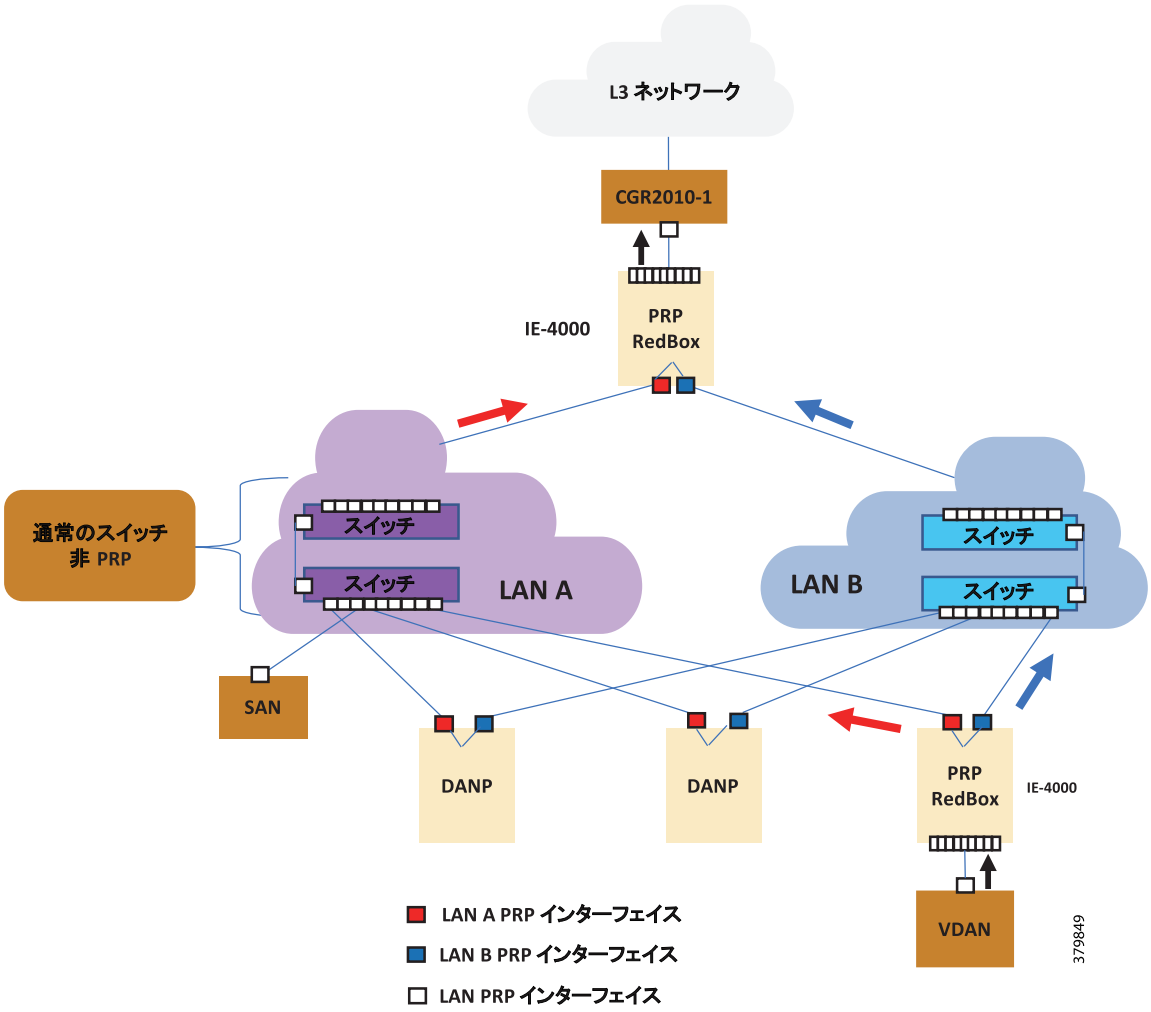
パラレル冗長プロトコル（PRP）（リングまたは非リング）

PRP は国際標準規格 IEC 62439-3 で定義されており、変電所に導入されていますが、IACS アプリケーションのロスレス冗長性を必要とする製造および工場ベースの環境に導入することもできます。PRP は PTP をサポートしますが、PRP は 2 つの独立した LAN を使用します。このため、リングベースの HSR よりも実装コストが大きくなる場合があります。

PRP は、イーサネット ネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。PRP は、アクセススイッチまたはブリッジング スイッチにある 2 つの個別のインターフェイスを使用して、2 つの独立したパラレル ネットワーク（LAN-A と LAN-B）に接続することによって、冗長性を実現します。2 つの独立したネットワークに接続しているデバイスは、「デュアル通信ノード（DAN）」と呼ばれます。この DAN は、現在、ネットワーク内の他のすべての DAN への冗長パスを持ちます。

DAN は、2 つのネットワーク インターフェイスを介して 2 つのパケットを宛先ノードに同時に送信します。宛先ノードが重複パケットを容易に区別できるように、シーケンス番号を含む冗長制御トレーラ（RCT）が各フレームに追加されます。宛先 DAN は最初のパケットを正常に受信すると RCT を削除してパケットを消費し、2 番目のパケットは廃棄されます。一方のパスで障害が発生すると、パケットはもう一方のネットワークで受信され、ロスレス冗長性が実現されます。可能性は低いですが、LAN-A と LAN-B の両方でまったく同時に障害が発生すると、ロスレス冗長性は失われます。冗長電源も推奨されます。

図 35　PRP の概要



冗長性ボックス（RedBox）は、エンド ノードが 2 つのネットワーク インターフェイスと PRP 冗長性をサポートしていない場合に導入されます。RedBox は、それに接続するデバイスの DAN 機能を提供します。これは、PRP 冗長の導入における Cisco IE 4000 または Cisco IE 4010 と Cisco IE 5000 の役割です。RedBox の背後にあるノードは、DAN などの他のノードに表示され、「仮想 DAN（VDAN）」と呼ばれます。

最後のノードは、単一のネットワークにのみ接続する非冗長ノードです。このノードは、LAN-A または LAN-B のいずれかに接続し、「シングル通信ノード（SAN）」と呼ばれます。

PRP は、独立したネットワークのトポロジに関係しませんが、2 つのネットワークの間でパケット遅延が一貫性を持つように、ネットワークを同様の構成にする必要があります。そのため、LAN-A と LAN-B の両方が同じトポロジを使用するかぎり、LAN-A と LAN-B の導入にはリングベース トポロジまたはスタートポロジを使用できます。

PRP の混合トラフィックとスーパバイザ フレーム

RedBox PRP チャネルグループから出力されるトラフィックは、混合可能、つまり宛先を SAN（LAN-A または LAN-B でのみ接続）または DAN にすることができます。SAN のパケットの複製を防ぐため、スイッチは受信した DAN エントリのスーパバイザフレームから、および SAN の非 PRP（通常トラフィック）フレームから送信元 MAC アドレスを学習し、これらのアドレスをノード テーブルに保存します。PRP チャネルから SAN の MAC アドレスにパケットを転送すると、スイッチはエントリを検索し、パケットを複製する代わりに送信先 LAN を決定します。

VDAN の RedBox で、これらの VDAN の代理でスーパバイザ フレームを送信する必要があります。他のすべてのポートと送信 PRP チャネル ポートに着信するトラフィックの場合、スイッチは、送信元 MAC アドレスを学習して VDAN テーブルに追加し、それらのアドレスのスーパバイザ フレームの送信を開始します。学習された VDAN エントリにはエージングが適用されます。

PRP を介した PTP

Precision Time Protocol（PTP）は、Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000 スイッチ上でパラレル冗長プロトコル（PRP）を介して動作できます。PRP は、PTP の冗長性を介してハイアベイラビリティを提供します。PTP の説明と、産業用オートメーションのこのフェーズでの PTP の実装については、PRP の PTP 設計を参照してください。

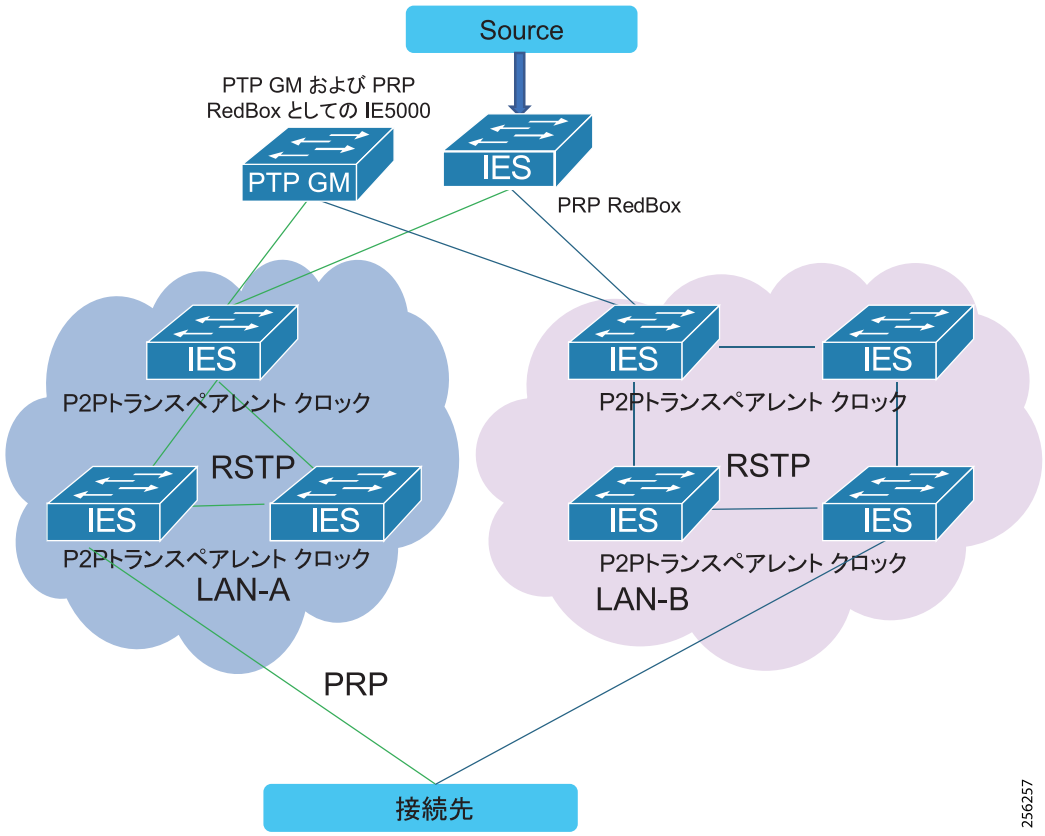
PRP とその機能の詳細については、
https://www.cisco.com/c/en/us/td/docs/switches/lan/industrial/software/configuration/guide/b_prp_ie4k_5k.html を参照してください。

PRP の概要

- 2 つのパラレル ネットワーク（LAN A と LAN B）を介したロスレス冗長性。
- LAN A スイッチと LAN B スイッチは PRP プロトコルを理解する必要はなく、あらゆるトポロジをサポートできる。
- 独立した LAN A と LAN B が必要であるために高コスト。
- 標準規格 IEC 62439-3 Clause 4。
- RedBox スイッチは PRP LAN を他のネットワークに接続。
- PRP 対応のエンドデバイスには、LAN A への 1 つの接続と LAN B への 1 つの接続がある。
- Cisco IE 4000、Cisco IE 4010、Cisco IE 5000、および 8/16 ポートの Cisco IE 2000U でサポートされている。

PRP トポロジの設計と推奨事項

図 36　PRP を使用したデュアル冗長スタートポロジ



このトポロジの推奨事項:

- 銅線リンクより高速なコンバージェンスを提供する光ファイバリンクを使用することをお勧めします。
- リンクの帯域幅は、遅延と、HSR および PRP ネットワークに含めることができるノードの数に影響を与えます。
- GOOSE とサンプル値は、出力インターフェイスのプライオリティ キューに分類されて送信されていました。
- マルチキャスト フラッディングを回避するために、各 IED に固有の VLAN を設定してください。
- アクセス/IED 側のインターフェイスでストーム制御を有効にしてください。

表 23　スター トポロジ

中断タイプ	トラフィックタイプ	遅延		パケットロス
		平均(ナノ秒)	最大(ナノ秒)	
リンク	GOOSE(300 バイト)	40066	41900	0
	サンプル値 (128 バイト)	31556	63680	0
	IP(Imix)	43140	109480	0
スイッチ	GOOSE(300 バイト)	40471	41140	0
	サンプル値 (128 バイト)	32077	61660	0

ハイアベイラビリティ シームレス冗長性(HSR)

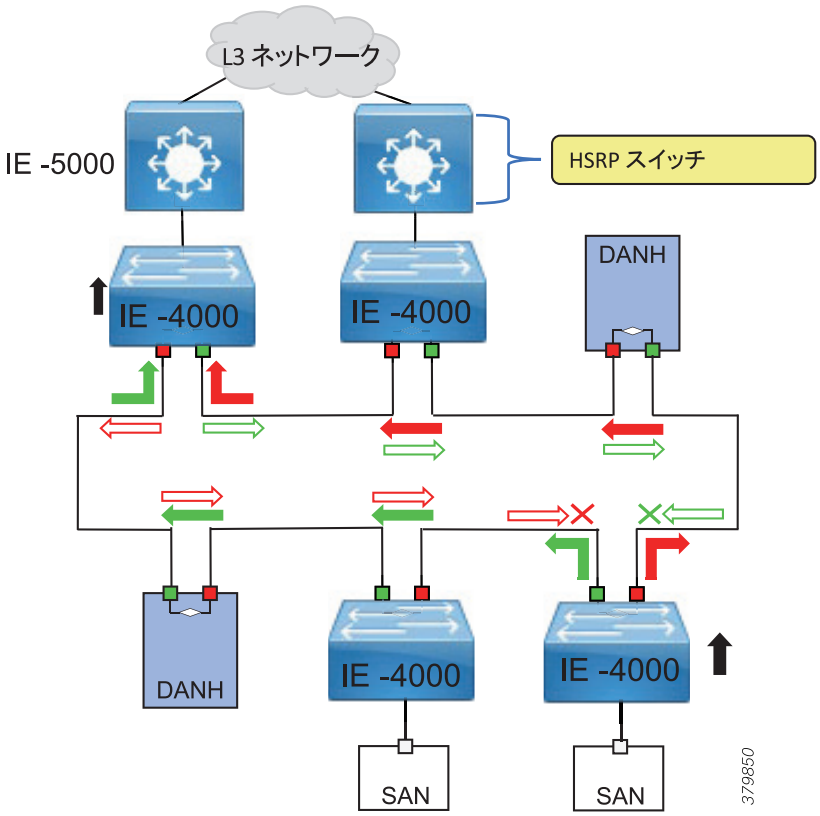
HSR は、国際標準規格 IEC 62439-3-2016 第 5 条で定義されています。HSR は、主に電力会社 IEC 61850 変電所アーキテクチャに見られますが、そのロスレス冗長性機能により、IACS アプリケーションが REP よりも優れたリングコンバージェンスを必要とする他の工場ベース環境にも適した選択肢となっています。HSR は PRP に似ていますが、リングトポロジで動作するように設計されています。任意のトポロジの並列独立ネットワーク 2 系統(LAN-A と LAN-B)の代わりに、HSR は反対方向のトラフィックを持つリングを定義します。このリングで、ポート A はトラフィックを反時計回りに送信し、ポート B はトラフィックを時計回りに送信します。重複パケット メカニズムは、リング内での単一の障害に対応するロスレス冗長性を提供します。

HSR は、パケット形式も PRP と異なります。スイッチが重複パケットを判別して廃棄できるように、追加のプロトコル固有情報がデータ フレームとともに送信されます。PRP の場合はこれが RCT の一部ですが、HSR の場合はこれがヘッダーの一部として送信されます。RCT ヘッダーと HSR ヘッダーの両方にシーケンス番号が含まれています。これは、受信したフレームが最初のインスタンスか重複したインスタンスかを判断するために使用されるプライマリデータです。

HSR リングに接続された 2 つのインターフェイスを持つ非スイッチングノードは、「HSR 実装ダブル接続ノード(DANH)」と呼ばれます。PRP と同様に、SAN は RedBox を介して HSR に接続されます。RedBox は、RedBox が送信元または接続先となるすべてのトラフィックに対して DANH として機能します。スイッチは、HSR リングへのギガビット イーサネット ポート接続を使用した RedBox 機能を実装しています。

図 37 IEC 62439-3 に記載されている HSR リングの例を示します。この例では、RedBox は Cisco IE 4000 スイッチです。HSR の導入をサポートするスイッチは、Cisco IE 4000 または Cisco IE 4010 スイッチと Cisco IE 5000 スイッチだけです。

図 37　HSR の概要とパケットフロー



追加設定なしで HSR をサポートしないデバイス(ラップトップやプリンタなど)を HSR リングに直接接続することはできません。これは、すべての HSR 対応デバイスが、リングから受信するパケットの HSR ヘッダーを処理でき、リングに送信するすべてのパケットに HSR ヘッダーを追加できる必要があるためです。これらのノードは、RedBox を介して HSR リングに接続されます。図 37 に示されているように、RedBox には DANH 側に 2 つのポートがあります。非 HSR SAN デバイスは、上流に位置するスイッチ ポートに接続されます。RedBox は、これらのデバイス向けに監視フレームを生成し、これらのデバイスがリング上で DANH デバイスとみなされるようにします。RedBox が DANH としてエミュレートするため、これらのデバイスは仮想ダブル接続ノード(VDAN)と呼ばれます。

HSR のループ回避

ループを避け、ネットワーク帯域を有効に使用するため、RedBox は、すでに同じ方向に転送されたフレームを送信しません。ノードがパケットをリングに入れると、そのパケットはループを避けるために次のように処理されます。

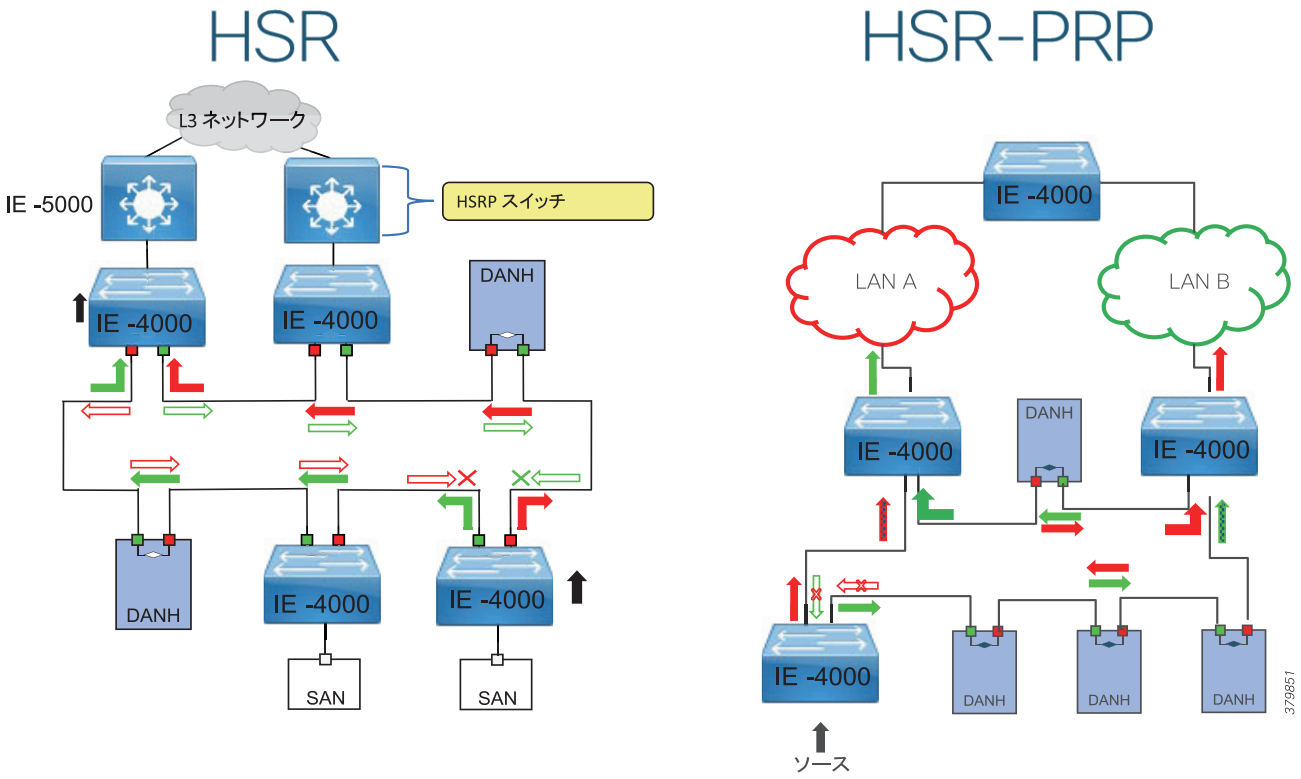
- 宛先がリング内のユニキャストパケット:ユニキャストパケットが宛先ノードに到達すると、パケットはそれぞれのノードによって消費され、転送されません。
- 宛先がリング内ではないユニキャストパケット:このパケットはリング内に宛先ノードがないため、送信元ノードに到達するまで、リング内のすべてのノードによって転送されます。各ノードは、送信したパケットの記録を、それが送信された方向とともに保持するため、送信元ノードは、パケットがループを 1 周したことを検出し、パケットをドロップします。このことは、図 37 の送信元ノードに示されています。
- マルチキャストパケット:マルチキャストパケットは、このパケットのコンシューマが複数存在する可能性があるため、各ノードによって転送されます。このため、マルチキャストパケットは常に送信元ノードに到達します。ただし、すべてのノードは、受信したパケットをすでに送信インターフェイスを介して転送したかどうかを確認します。パケットが送信元ノードに到達すると、送信元ノードは、このパケットをすでに転送したことを確認し、再度転送せずにパケットをドロップします。

HSR RedBox の動作モード

HSR RedBox は、HSR がさまざまなシナリオでパケットを処理する方法を定義する次のいずれかのモードで動作できます。

- HSR-SAN：最も基本的なモードです。このモードでは、RedBox が SAN デバイスを HSR リングに接続します。他の PRP または HSR ネットワークは、この構成に関与しません。このモードでは、上流に位置するスイッチのポート上のトラフィックには HSR/PRP タグがなく、RedBox がリングの VDAN として SAN デバイスとなります。
- HSR-PRP：この設定は、HSR ネットワークと PRP ネットワークをブリッジするために使用されます。RedBox は PRP フレームからデータを抽出し、このデータを使用して HSR フレームを生成します（逆方向のパケットには逆の処理を実行します）。これは、IEC 61850 を導入する変電所でより一般的に使用されますが、2 つのリングがブリッジされる場所で工場のロスレス冗長性が必要な場合にも、選択肢となる可能性があります。

図 38　HSR と HSR-PRP の概要



HSR とその機能の詳細については、https://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/hsr/b_hsr_ie4k.html#id_54474 を参照してください。

HSR の概要

- リングトポロジを介したロスレス冗長性。
- リング内のすべてのノードは、HSR をサポートするための特別なハードウェアを備えている**必要**があり、リング内のすべてのノードは HSR をサポートしている必要がある。
- ロスレス冗長性を提供するため、REP よりも高速なコンバージェンスが必要なネットワークに役立つ。
- 標準規格 IEC 62439-3 Clause 5。
- Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000 でのみサポートされている。
- リングで利用可能な帯域幅は、重複したパケットのために最大で半分に削減される。
- 一般的な実装では、受信ノードが HSR リングから両方のパケットを削除する。

HSR トポロジの設計と推奨事項

Cisco IE 4000 スイッチを使用した Cisco Catalyst 9300/Cisco Catalyst 3850 StackWise REP および HSR

このトポロジでは、ディストリビューション冗長性に StackWise が使用されます。図 39 に示すように、アクセス リングとディストリビューション間の接続には REP が使用されます。HSR はアクセスリングトポロジに実装されます。REP は、IE アクセススイッチと Cisco Catalyst 9300 ディストリビューション スイッチを直接接続するリンクの間で使用されます。図 39 に示すように、REP エッジポートは、アクセススイッチ アップリンク上に設定されます。このトポロジの中断では、リングのトラフィックのダウンタイムは発生しません。REP リングで障害が発生すると、REP のコンバージェンス時間に応じて、レイヤ 3 トラフィックが影響を受けます。このトポロジでは、REP がないと、ネットワーク ループが発生します。

図 39　Cisco IE 4000 スイッチを使用した Cisco Catalyst 9300/Cisco Catalyst 3850 StackWise REP および HSR

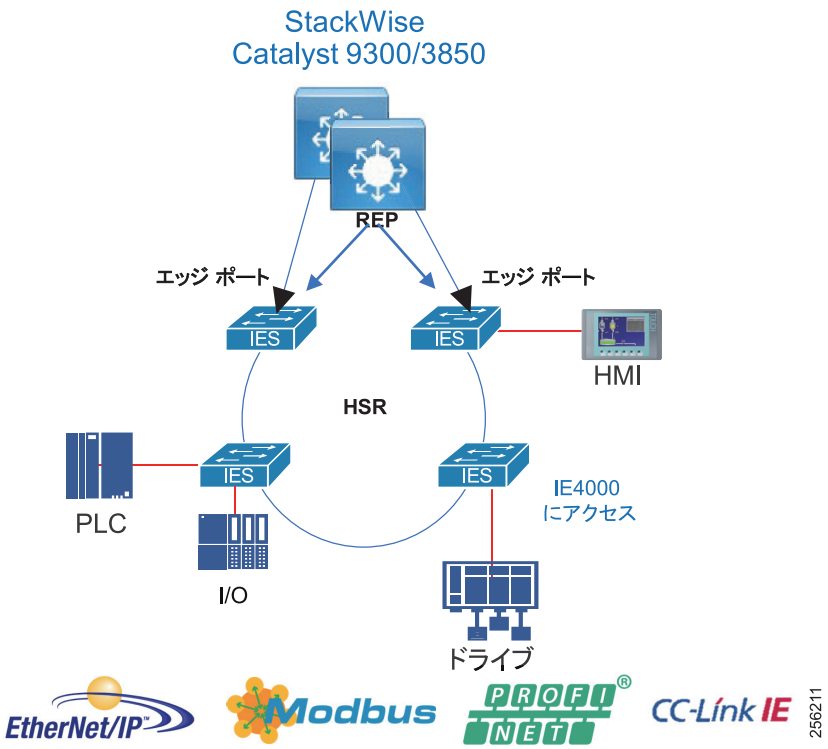


表 24 検証中のコンバージェンス結果の概要を示します。

表 24　Cisco Catalyst 3850 による HSR リング

中断タイプ	トラフィックタイプ	コンバージェンス	
		最大	平均
リンク	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	0	0
スイッチ	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	780	405

HSR-HSR

HSR リングも、キースイッチが 2 つの HSR リングに参加しているのと同様の方法で実装できます。これには、HSR-HSR または Quadbox と呼ばれるそれぞれのリングを接続するための 4 つのインターフェイスを使用します。HSR-HSR モードがライセンスされ、有効になっている場合、スイッチはトラフィックの干渉を回避するために、すべての非 HSR ポートを閉鎖します。HSR-HSR スイッチへの接続は、HSR HSR ポートまたはアウトオブバンド コンソール インターフェイスを介して行うことができます。

図 40　ディストリビューションにおける Cisco Catalyst 9300 による HSR-HSR リング

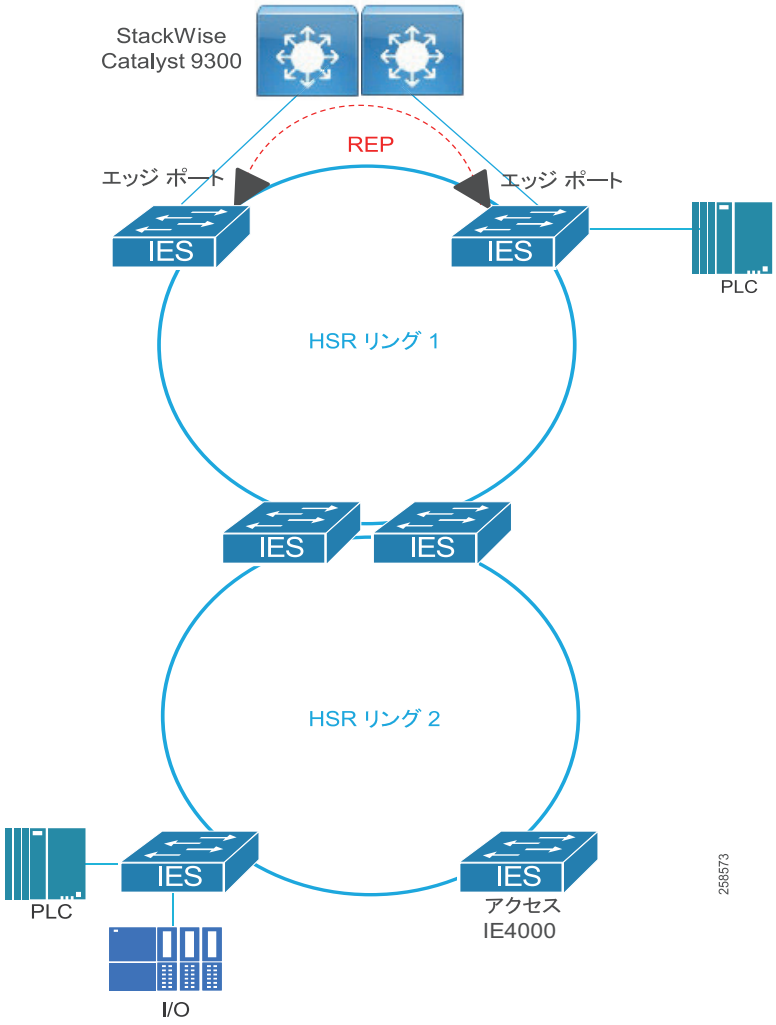


表 25　ディストリビューションにおける Cisco Catalyst 9300 による HSR-HSR リング

中断タイプ	トラフィックタイプ	コンバージェンス	
		最大	平均
リンク	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	0	0
スイッチ	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	0	0

図 41　ディストリビューションにおける Cisco IE 5000 による HSR-HSR リング

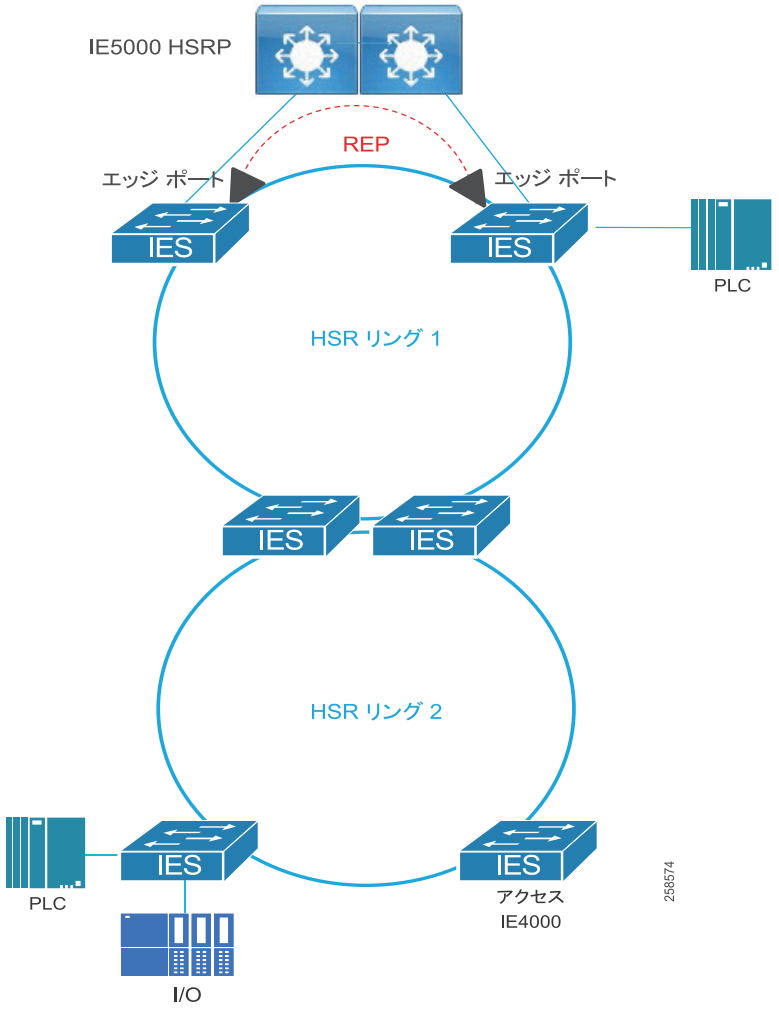


表 26　ディストリビューションにおける Cisco IE 5000 による HSR-HSR リング

中断タイプ	トラフィックタイプ	コンバージェンス	
		最大	平均
リンク	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	0	0
スイッチ	レイヤ 2 マルチキャスト	0	0
	レイヤ 2 ユニキャスト	0	0
	レイヤ 3 ユニキャスト	0	0

結果の説明。

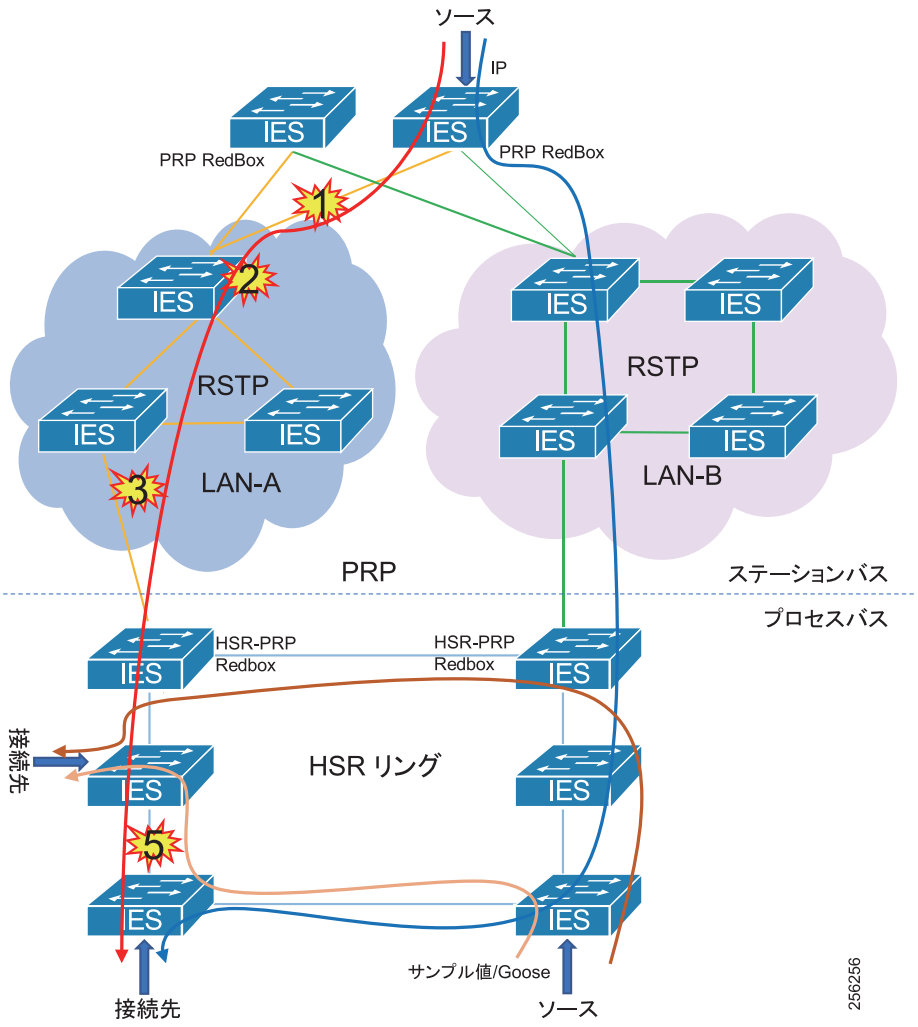
- HSR-HSR の検証は、銅線イーサネットに接続された Cisco IE 4000 スイッチを含む 2 つのリングで行われました。オープン REP セグメントは、銅線イーサネットを使用して、1 つの HSR リングをディストリビューション スイッチに接続しました。
- コンバージェンスは、VLAN 内のレイヤ 2 トラフィックと同じリング内の VLAN 間のレイヤ 3 トラフィックに関して検証されました。

- 「リンクの中断」は、リングでの単一のリンク障害を指します。リンク障害は、両方の HSR リングの異なるポイントで処理されました。スイッチの障害は、一度に 1 つのスイッチの電源が中断したことを意味します。ディストリビューションメンバーと IE スイッチは、テスト中にリロードされました。
- HSR の外部のリンクまたはスイッチの障害（つまり、ディストリビューションまたはディストリビューションスイッチ自体へのリンク）は、HSR リング内のスイッチのレイヤ 3 ユニキャストパケットの損失を引き起こしました。これらの障害のコンバージェンス時間は、銅線リンクを介した REP コンバージェンスの期待値に沿っています。
- 検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。
- このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。

マルチレベルリング用の HSR-PRP RedBox

HSR-PRP（「デュアル RedBox」とも呼ばれる）は、PRP ネットワークと HSR ネットワークを一緒に接続するために使用されます。これは一般に変電所に導入されます。そのため、テスト結果には GOOSE と サンプル値が示されていますが、他の IP プロトコルにも適用できます。次のトポロジは、2 つの RedBox（各 LAN に 1 つずつ）を介して PRP ネットワークに接続される HSR リングを示しています。この例では、IP フレームは PRP ネットワークで発生し、GOOSE フレームとサンプル値フレームは HSR リングで発生して終了します。このトポロジでの中断は、対応するトラフィックでダウンタイムを発生させず、異なるトラフィックストリームの遅延は期待される要件を確実に満たします。

図 42　マルチレベルリング用の HSR-PRP RedBox



このトポロジの推奨事項:

- リンクの帯域幅は、遅延と、HSR および PRP ネットワークに含めることができるノードの数に影響を与えます。
- HSR-PRP 機能は Cisco IE 4000 でのみサポートされています。
- GOOSE とサンプル値は、出力インターフェイスのプライオリティ キューに分類されて送信されていました。
- マルチキャスト フラッディングを回避するために、各 IED に固有の VLAN を設定してください。
- アクセス側のインターフェイスでストーム制御を有効にしてください。

表 27　HSR-PRP Redbox リング

中断タイプ	トラフィックタイプ	遅延		パケットロス
		平均(ナノ秒)	最大(ナノ秒)	
スイッチ	GOOSE(300 バイト)	31467	58940	0
	サンプル値（128 バイト）	21170	64400	0
	IP(Imix)	65321	208900	0
リンク	GOOSE(300 バイト)	37528	60780	0
	サンプル値（128 バイト）	26671	63460	0
	IP(Imix)	68430	189820	0

結果の説明。

- コンバージェンスとレイテンシは、レイヤ 2 GOOSE、サンプル値、および同じリング内の各タイプに固有の VLAN を持つ IP トラフィックに関して検証されました。
- 「リンクの中断」は、アクティブ転送パスのリンク障害を指します。「スイッチ障害」は、アクティブ転送パスのプライマリ スイッチ障害を指します。
- HSR リングには、8 つの Cisco IE 4000 スイッチがあります。
- PRP ネットワークには、ループ回避のために RSTP を実行している 2 つの異なる PRP LAN の一部として、3 つおよび 4 つの Cisco IE 4010 スイッチがありました。
- Cisco IE 4010 スイッチと Cisco IE 5000 スイッチは PRP 冗長ノードとして設定されました。
- テストは、ネットワーク内の GigabitEthernet リンクを使用して実行されました。

Media Redundancy Protocol(MRP):PROFINET の導入

Media Redundancy Protocol(MRP)は、国際電気標準会議(IEC)によって IEC 62439-2 として標準化されたデータ ネットワーク プロトコルです。MRP は、イーサネット スイッチのリングが、従来の STP よりもはるかに短い回復時間で単一の障害を克服することを可能にします。

役割:シスコの産業用イーサネット スイッチは、次の 2 つの役割をサポートしています。

- Media Redundancy Manager(MRM)
- Media Redundancy Client(MRC)

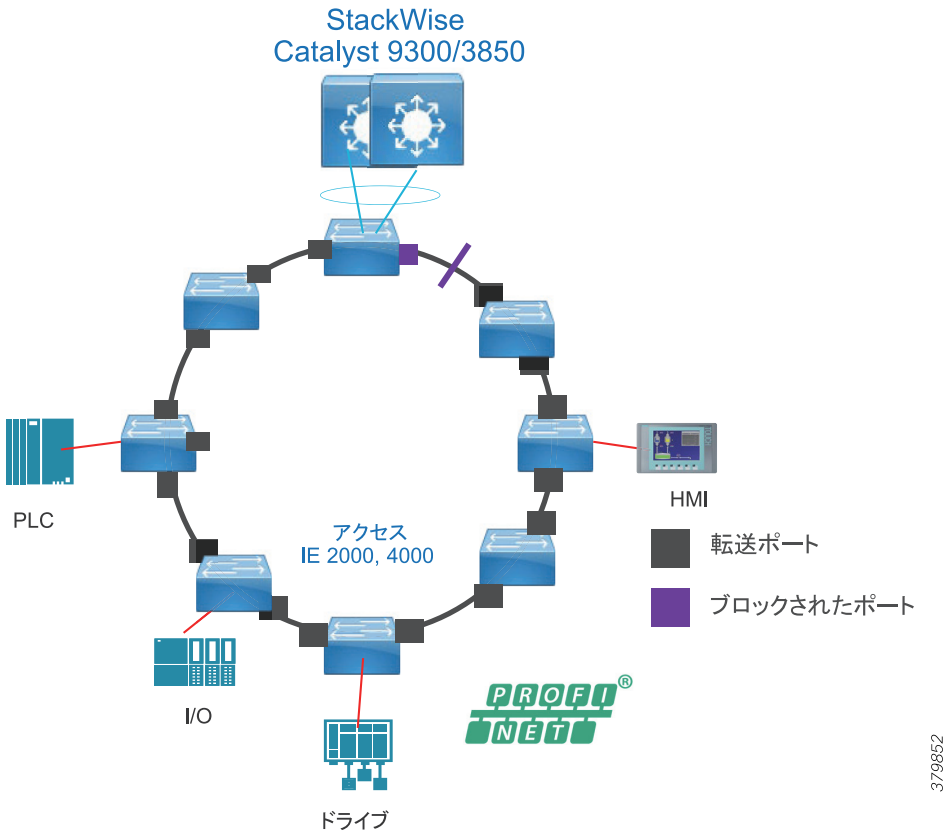
リングトポロジでは、1 つのスイッチまたは産業用オートメーションシステム デバイスのみが MRM として機能できます。その他のすべてのデバイスは MRC として機能します。MRM の目的は、障害が発生したときにリングループのフリー状態を維持し、冗長性を提供することです。MRM は、一方のリングポートから制御パケットを送信し、もう一方のリングポートでそれらを双方向で受信することによって、これを実現します。制御パケットを受信する場合、リングはエラーのない状態です。

MRP 内では次の 3 つのポート状態が使用されます。

- 切断/無効: この状態の場合、スイッチ ポートはすべての受信パケットをドロップします。
- ブロック: この状態の場合、制御パケット以外のすべての受信フレームがドロップされます。
- 転送: ポート上のすべての受信パケットを転送する通常の動作状態。

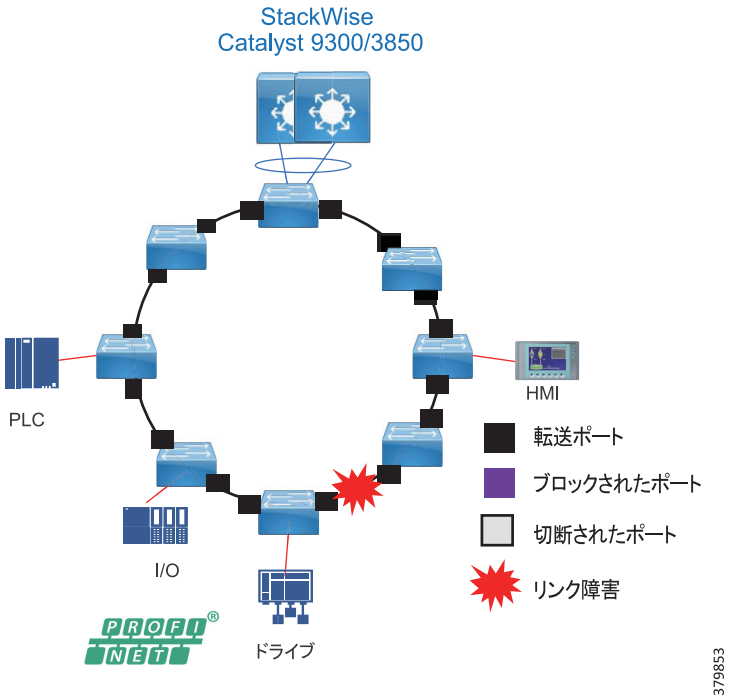
正常な動作では、ネットワークはクローズ状態で動作します。この状態では、1 つの MRM の 1 つのリング ポートがブロック ポート状態を維持し、その他のポートは転送状態になります。すべての MRC も転送状態になります。MRM のブロック ポートのために、ループが回避されます。

図 43　MRP の通常の動作モード



ネットワークリンクまたはデバイスに障害が発生すると、リングはオープンステータスに移行します。図 44 に示されているように、障害が発生すると、MRM は制御フレームを受信せず、リング内で障害が発生したと見なします。両方のポートが転送されるように、MRM は、ブロック状態だったポートを転送状態に移行させます。

図 44　MRP の障害



MRP の概要

このアプローチには以下の利点があります。

- 高速コンバージェンス：MRP は、200 ミリ秒のコンバージェンス時間を実現できます。
- リンクの完全性：MRP は、リンクの完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング機能を使用しません。ローカル リンク障害検出を実装しています。
- Resilient Ethernet Protocol（REP）との共存：MRP は REP とやり取りしませんが、同じスイッチ上に共存できます。これにより、ネットワーク設計者は高度な相互運用可能リングを作成できます。
- デバイス レベルのリングのサポート：MRPは、PROFINET 用の組み込み復元力プロトコルであるため、
- 産業用イーサネットスイッチは、IACS デバイス（PLC、リモート I/O など）でリングを形成できます。

欠点は次のとおりです。

- Manager ノードのライセンス要件。
- マルチリングトポロジがサポートされません。
- Manager（MRM）用のハードウェア レベルの冗長性がありません。
- Cisco REP よりもコンバージェンス時間が長くなります。

表 28　ディストリビューションにおける Cisco Catalyst 9300 による MRP リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 2000、3400、4000 光ファイバ		コンバージェンス Cisco IE 2000、3400、4000 光ファイバ - リカバリ	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	10070	2193	34102	11954
	レイヤ 2 ユニキャスト	54	24	1916	196
	レイヤ 3 ユニキャスト	40	28	1996	187
スイッチ	レイヤ 2 マルチキャスト	7034	1036	69158	30007
	レイヤ 2 ユニキャスト	46	32	15216	6149
	レイヤ 3 ユニキャスト	46	35	15216	7325

表 29　ディストリビューションにおける Cisco IE 5000 による MRP リング

中断タイプ	トラフィックタイプ	コンバージェンス Cisco IE 2000、3400、4000 光ファイバ		コンバージェンス Cisco IE 2000、3400、4000 光ファイバ - リカバリ	
		最大（ミリ秒）	平均合計時間（ミリ秒）	最大（ミリ秒）	平均合計時間（ミリ秒）
リンク	レイヤ 2 マルチキャスト	9974	2319	65446	17458
	レイヤ 2 ユニキャスト	58	29	230	24
	レイヤ 3 ユニキャスト	58	38	210	25
スイッチ	レイヤ 2 マルチキャスト	9420	1211	60690	25178
	レイヤ 2 ユニキャスト	74	41	15202	6851
	レイヤ 3 ユニキャスト	74	47	15206	11296

結果の説明。

- MRP リングには、次のタイプの IE スイッチが含まれています。
  - Cisco IE 2000
  - Cisco IE 3400
  - Cisco IE 4000
- スイッチの役割は、Siemens TIA ポータルを介して設定されています。
- コンバージェンスは、VLAN 内のレイヤ 2 トラフィックと同じリング内の VLAN 間のレイヤ 3 トラフィックに関して検証されました。
- 「リンクの中断」は、リングでの単一のリンク障害を指します。リンク障害は、リング内のさまざまなポイントで処理されました。スイッチの障害は、一度に 1 つのスイッチの電源の中断を示しています。
- 検証時には、シミュレートされたトラフィックと実際の IACS デバイスが使用されました。
- このシナリオは、250 の MAC アドレス、200 のマルチキャストグループ、および VLAN 間と VLAN 内のトラフィックで実行されました。

復元力の概要と比較

表 30 パフォーマンスと相互運用性に基づく復元力プロトコルのおおまかなガイダンスを示します。ノードの最大数は、一般に、絶対的な制限ではなく推奨値であることに注意してください。

表 30　復元力プロトコルの比較

プロトコル	トポロジ	ノード数	一般的なコンバージェンス	注記
RSTP/MSTP	いずれか	最大ホップ数の 255	50 ミリ秒～ 6 秒	最も幅広い相互運用性が実現されるが、コンバージェンスとトラブルシューティングは最低レベルになる。
MRP	リング	50	200 ～ 500 ミリ秒	Siemens が強力な主唱者。標準 IEC 62439-2 をサポートするスイッチと相互運用可能。PROFINET 環境では共通。
REP	リング	50	50 ～ 250 ミリ秒	シスコの独自規格。セットアップとトラブルシューティングが非常に容易。
PRP	いずれか	無制限	0 ミリ秒	重複 LAN が必要。(高コストの)標準 IEC 62439-3 Clause 4。
HSR	リング	50	0 ミリ秒	リング内のすべてのノードが HSR をサポートしている必要がある。標準 IEC 62439-3 Clause 5。

注:RSTP と MSTP は、この CVD では検証されておらず、情報提供のみを目的として追加されています。

プラットフォームの詳細とディストリビューション スイッチの冗長性メカニズムも検討事項に含まれるため、それらも考慮する必要があります。これらについては、このガイドの関連セクションにある、産業用オートメーション DIG の検証に関する各復元力プロトコルの説明を参照してください。検証されたノード数の詳細も記載されています。

セル/エリアゾーンの管理

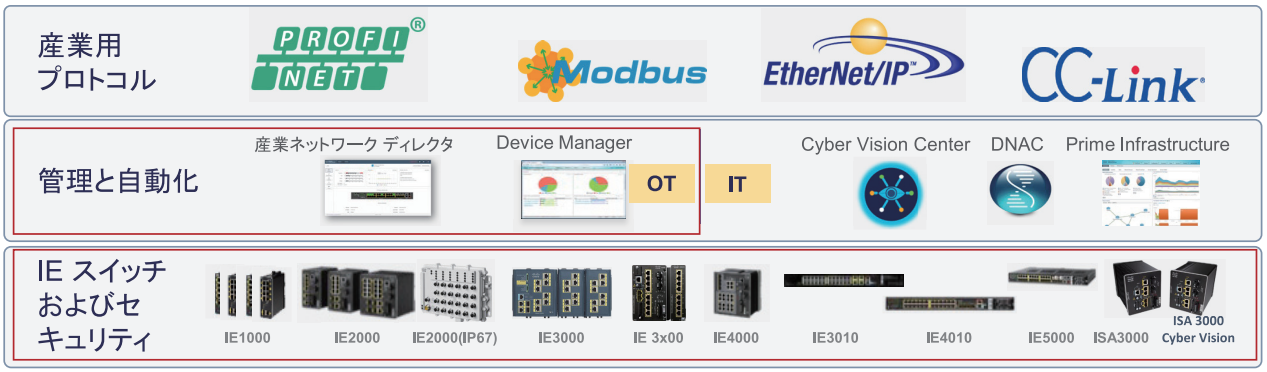
イーサネットネットワークは、現代の自動化および制御環境に不可欠です。運用担当者は、計画外のダウンタイムを削減するために、ネットワークモニタリングにますます依存するようになっています。そのため、OT 制御エンジニアは、基本的なネットワーク管理機能に関して、より多くの役割を担っています。制御エンジニアは、問題が発生した場合にネットワークの可視性とアクセスを必要とするため、ネットワーク管理で次の重要な考慮事項に対処する必要があります。

- ネットワーク強化:システム整合性のコンポーネント(90 ページ) で説明しているように、管理ネットワークには個別のアウトオブバンド インフラストラクチャが必要です。インバンド データ プレーン ネットワークに影響がおよぶ場合でもセル/エリアゾーンのネットワークデバイスへのネットワーク接続を提供できるように、少なくとも、独自の論理ネットワークが必要です。アウトオブバンド ネットワーク セグメントは、コンソールサーバ、ネットワーク管理ステーション、認証/許可/アカウンティング(AAA)サーバ、分析/相関ツール、FTP、syslog サーバ、ネットワーク コンプライアンス管理、およびその他の管理/制御サービスをホストします。次のベストプラクティスを使用して、アウトオブバンド管理ネットワークを導入する必要があります。
  - ネットワークの分離を提供します。
  - アクセス制御を実行します。
  - データ トラフィックが管理ネットワークを通過しないようにします。
  - ネットワーク管理トラフィック(SSH、簡易ネットワーク管理プロトコル バージョン 3(SNMPv3))の安全な使用を実現します。
  - syslog と SNMP を使用して、コントロールセンターのオペレータに、イベント、障害、およびネットワークパフォーマンスの可視性を提供します。
  - アウトオブバンド ネットワークを使用できない場合は、管理ネットワークのために専用 VLAN を使用する必要があります。

- セル/エリアゾーン内では、ネットワーク管理の支援を容易にするために提供されるツールによって、制御エンジニアが使いなれている OT ビューが提供される必要があります。それは、IT ネットワーク管理ツールではなく、IACS システムのコンポーネントまたは拡張機能のようなルックアンドフィールである必要があります。
- そのネットワークは、導入、設定、およびモニタが容易である必要があります。ネットワークコンポーネントは、OT の経験豊富な制御エンジニアが簡単に交換または設置できる必要があります。

シスコには、この分野の OT 制御エンジニアの要件に対応するツール（Cisco IND と IoT Device Manager（IoT-DM））があります。図 45 産業用自動化アーキテクチャ向けのネットワーク管理サポート モデルを示します。セル/エリアゾーンをサポートするツールとして IoT-DM と IND が示されています。Cisco DNA Center（DNA-C）は、IT ベースのチームが産業工場を支援するためにネットワーク管理機能を提供する運用レイヤでネットワーク管理を支援するツールと位置付けられています。

図 45　ネットワーク管理サポートモデル



注：Cisco Prime と DNA-C は、この CVD の一部としてテストされていません。

Cisco Industrial Network Director

Cisco IND は、産業用イーサネットネットワークにおける運用中心型のネットワーク管理を実現します。このシステムは、PLC、I/O、HMI、ドライブなどのオートメーションデバイスを検出するために、CIP、PROFINET、OPC-UA、Modbus、BACnet などの産業用オートメーションプロトコルをサポートしており、オートメーションおよびネットワーキングの統合トポロジマップを提供します。このマップにより、運用部門と工場 IT 担当者に産業用ネットワークを管理および維持するための共通フレームワークが提供されます。

システムはシスコの IE 製品ポートフォリオの全機能を使用し、IT 部門外の運用担当者がネットワークを利用できるようにします。シンプルなユーザインターフェイスにより、ネットワークモニタリングを合理化し、産業環境で発生する一般的なネットワーク問題を迅速にトラブルシューティングすることができます。詳細については、次の付録および項を参照してください。
https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

おおまかには、次の機能により、セル/エリアゾーンに関して以前に詳しく説明した管理要件に対処できます。

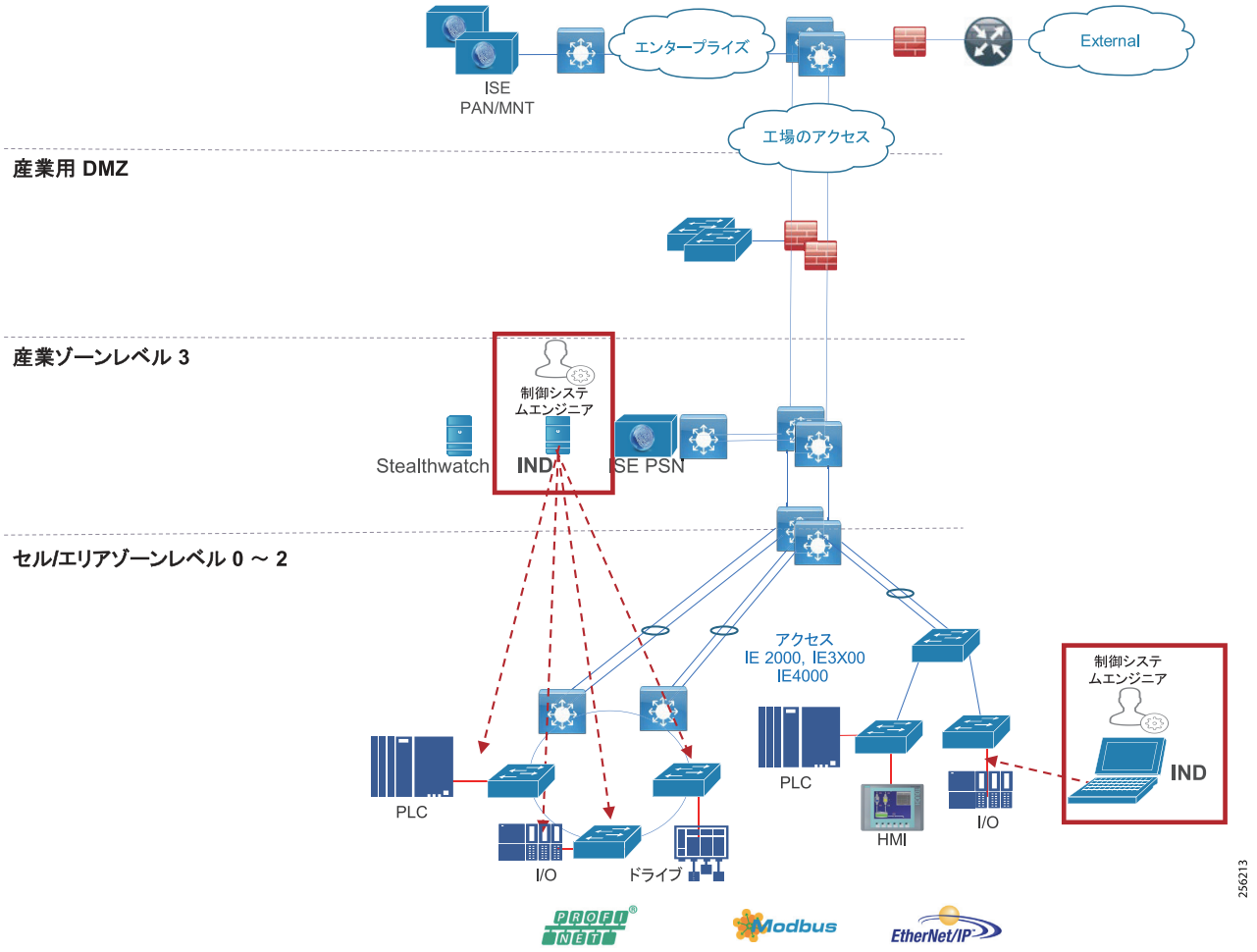
- ゼロタッチスイッチの試運転用のプラグアンドプレイサーバ：Cisco IND は、産業用イーサネットデバイスのゼロタッチプロビジョニングおよび交換用のプラグアンドプレイサーバを提供します。自動化されたネットワークの試運転用に事前プロビジョニングされた設定とソフトウェアは、一貫したネットワーク設計とセキュリティポリシーを確保するために役立ちます。これにより、制御エンジニアは、ネットワークスイッチなどの故障したネットワーク機器を容易に交換できるようになります。エンジニアは、スイッチに障害が発生したときにハードウェアを交換し、シスコのプラグアンドプレイを使用して、自動設定とソフトウェアイメージ交換によってネットワークに復帰させることができます。
- 産業用およびネットワークアセットの自動検出：Cisco IND はネットワーキング トポロジを検出するだけでなく、Common Industrial Protocol（CIP）、PROFINET、Modbus、OPC-UA、BACnet、Siemens S7、およびその他の産業用通信プロトコルでオートメーション デバイスを検出できます。ユーザインターフェイスにより、動的トポロジマップ上でオートメーションとネットワーキングアセットの間の接続性が可視化されます。
- ネットワーク管理：IE スイッチのプラグアンドプレイサポートを基盤として、Cisco IND は、スイッチの健全性とトラフィックの統計情報の継続的なモニタリングとスイッチ設定のバックアップを提供します。GUI 駆動型のアクションにより、IT 以外の運用の担当者は、既存のネットワーク インフラストラクチャにオートメーションデバイスを安全に追加できます。Cisco IND は、ネットワーク内の移動や変更を追跡および追加するための詳細な監査証跡を提供できます。

- 容易なトラブルシューティング：予定外のダウンタイムやネットワークの問題が発生した場合、管理プラットフォームは、問題を特定して迅速に復旧する必要があります。Cisco IND は、コンテキスト化された産業用アセットの可視性により、ネットワークイベントに可視化してアラートを提供することができます。
- ロール ベースのアクセス制御：Cisco IND は、さまざまなタイプのユーザがさまざまなレベルの情報とアクセスを必要とする環境に最適です。複数のユーザを作成し、それらのユーザのアクセスを Cisco IND ユーザインターフェイス内の特定の領域に制限する機能により、権限のある担当者だけが機密性の高い操作を実行可能な状態を確保できます。
- 産業用アプリケーションと迅速に統合するためのリッチ アプリケーション プログラミング インターフェイス（API）：Cisco IND には、既存の産業用資産管理ツール、オートメーション アプリケーション、および制御システムと簡単に統合できるようにする包括的な RESTful API が含まれています。Cisco IND には、システムインテグレータや開発者が API について迅速に学習し、採用ために役立つ直感的な API ツールが付属しています。

Cisco IND の導入オプションと考慮事項

Cisco IND は、ネットワークの他の領域へのアクセスが厳しく制限されている産業ゾーンのサーバにインストールできます。クリティカルなデータを保護するために、可能であれば、安全なプロトコル（HTTPS や SSH など）だけを使用することをお勧めします。Cisco IND は非常に軽量であるため、システム要件を満たしているかぎり、必要に応じて、工場フロアのゾーン内にある堅牢なラップトップにインストールできます。図 46 Cisco IND のアーキテクチャにおける位置付けを示します。この例は、産業ゾーンのサーバと、セル/エリアゾーンの安全で堅牢なラップトップを示しています（ラップトップの接続は示されていません）。

図 46　Cisco IND の導入と考慮事項



- Cisco IND アプリケーションには、検出とモニタリングを担当するすべてのネットワークアセットおよびオートメーション クライアントへのレイヤ 3 接続が必要です。つまり、検出およびモニタする必要があるすべてのデバイスにルーティング可能で、Cisco IND サーバに到達可能な IP アドレスを割り当てる必要があります。
- Cisco IND をホストする Windows サーバとモニタ対象デバイスの間にファイアウォールがある場合は、インバウンドとアウトバウンドの両方で TCP ポート 5432、8088、8443、443、80、21、および 50000 ～ 50050 を許可するようにファイアウォールを設定する必要があります。
- Cisco Active Advisor の統合を利用するには、Cisco IND Web インターフェイスにアクセスしているクライアントコンピュータも、ネットワーク インベントリ データをアップロードするためにインターネットにアクセスできる必要があります。

注：技術上およびビジネス上の要件によっては、Cisco Smart Licensing のためのインターネットへの直接アクセスが可能でない場合があります。このような場合には、Cisco Software Manager Satellite を IND サーバと Cisco Cloud の間の IDMZ に配置して、オンプレミスのライセンス管理を容易にすることができます。

Cisco IND でサポートされているプラットフォーム

- Cisco IE 1000
- Cisco IE 2000
- Cisco IE 3200
- Cisco IE 3300
- Cisco IE 3400
- Cisco IE 4000
- Cisco IE 4010
- Cisco IE 5000

Cisco IND でサポートされている産業用プロトコル

- CIP
- PROFINET I&M
- Siemens S7
- Modbus/TCP
- BACnet/IP
- OPC-UA

Cisco IND のシステム要件

図 47　Cisco IND のシステム要件

最小システム要件	
Windows オペレーティングシステム（OS）64 ビットバージョン	• Windows 7 Enterprise または Professional、サービスパック 2 • Windows 10 • Widows 2012 R2 サーバ • Windows 2016 サーバ（64 ビット版）
CPU	Qual コア 1.8 GHz
RAM	8 GB
ストレージ	50 GB
クライアントのブラウザの要件	
ブラウザ	• Chrome：バージョン 50.0.2661.102 以降 • Firefox：バージョン 46.01 以降

256214

Cisco IoT Device Manager

スイッチ メモリ内の Device Manager を使用すると、個々のスイッチやスタンドアロンスイッチを管理できます。この Web インターフェイスは、使いやすい Web デバイスマネージャを提供します。これにより、すぐに使用できる容易な設定と簡素化された運用管理性が実現されます。Device Manager には、Web ブラウザを介して、ネットワーク上のどこからでもアクセスできます。Device Manager を使用して、Cisco IND の機能を補完できます。Device Manager により、CLI を介してスイッチを設定する複雑な端末エミュレーションプログラムが不要になります。スイッチ設定を変更し、その後に変更を Cisco IND にバックアップできます。

Cisco Cyber Vision の概要

IACS は、発電所と重要なインフラストラクチャ、輸送ネットワークなどを実行する、水、ガス、および電気流通ネットワークの生産ラインの自動化のために導入されています。これらのシステムは、企業の IT ネットワークにより一層接続されるようになっています。また、企業は、さらなるデジタル化を促進するために Industrial Internet of Things（IIoT）も導入しています。このような IT、クラウド、産業ネットワークのより深い統合により、業界のデジタル化の取り組みにとっての障害である多くのセキュリティ問題が発生しています。

産業運用の保護は非常に具体的な課題です。産業プロセスを停止することはできません。中断すると、人間や環境上の大規模な危険を招く可能性があります。攻撃は、多くの場合カスタムメイドであり、アセットに対する正当な指示のように見えて、長時間を経た後に効果を発するので検出することは特に困難です。産業用自動化テクノロジーは、非常に古く、独自性があり、セキュリティを考慮して設計されていないことがあります。

Cisco Cyber Vision は、産業運用の継続性、復元力、安全性を確保するために、製造業、石油およびガス、電力と水の流通、および公共輸送の組織向けに特別に設計されたサイバーセキュリティソリューションです。これにより、IACS ネットワークに完全に可視化されたアセットオーナーが提供されるため、運用とプロセスの整合性を確保し、法規制の遵守を促進し、産業ネットワーク内で簡単に導入できるようになります。Cisco Cyber Vision は、シスコの産業用ネットワーク機器を活用して、産業運用を監視し、Cisco IT セキュリティプラットフォームを OT コンテキストにフィードして、統一された IT/OT サイバーセキュリティアーキテクチャを構築します。

Cisco Cyber Vision は、次の 3 つの主要な価値提案を提供します。

- 産業用ネットワークに組み込まれた可視性：何を保護すべきかがわかります。Cisco Cyber Vision は、シスコの産業用ネットワーク機器に組み込まれているため、接続されているすべてのものを確認でき、お客様がネットワークをセグメント化して、大規模な IoT セキュリティを導入することを可能にします。

- IACS および OT のセキュリティインサイト：システムの整合性と生産継続性を維持するために、IACS サイバーセキュリティの整合性を継続的に監視します。Cisco Cyber Vision は、独自の産業用プロトコルを理解し、プロセスデータ、資産の変更、変数の変更を追跡します。
- 360° の脅威検出：手遅れになる前に脅威を検出します。Cisco Cyber Vision は、シスコの脅威インテリジェンスと高度な行動分析を活用して、既知および新たな脅威を特定し、異常および未知の攻撃に対処します。シスコのセキュリティポートフォリオと完全に統合され、IT SOC を OT ドメインに拡張します。

主な機能と利点

産業用ネットワークに組み込まれたセキュリティ

OT サイバーセキュリティの導入は、特に産業用ネットワークが国全体または多くのリモート産業サイトに分散されている場合は、非常に複雑になる可能性があります。OT サイバーセキュリティ プロジェクトを成功させるには、組織全体にわたって適切なコストで、容易に拡張できるようにする必要があります。

Cisco Cyber Vision は、(IoT スイッチ、ルータ、アクセスポイント、産業用コンピュータなどの) シスコの産業用ネットワーク機器内でセキュリティ監視コンポーネントを実行できるようにする、独自のエッジ コンピューティング アーキテクチャを活用します。専用のアプライアンスを調達する必要はなく、それらをインストールする方法を検討したり、産業用ネットワークフローを中央のセキュリティプラットフォームに送信するアウトオブバンド ネットワークを構築したりする必要はありません。Cisco Cyber Vision により、産業用ネットワークは包括的な可視性、分析、脅威の検出を提供するために必要な情報を収集できます。大規模な OT セキュリティの導入を検討しているネットワークマネージャには、Cisco Cyber Vision のアーキテクチャの比類のないシンプルさと低コストのメリットを実感いただけるはずです。

可視性

OT インフラストラクチャの保護は、資産のインベントリ、通信パターン、およびネットワークトポロジの正確なビューの確保から始まります。Cisco Cyber Vision は、OT チームおよびネットワーク管理者が、自社のアセットおよびアプリケーションフローを可視化し、セキュリティのベストプラクティスを実施し、ネットワーク セグメンテーション プロジェクトを推進し、運用の復元力を向上できるようにします。

Cisco Cyber Vision は、ベンダーの詳細、ファームウェアとハードウェアのバージョン、シリアル番号、PLC ラックスロットの設定など、実稼働インフラストラクチャの些細な詳細を自動的に発見します。アセットの関係、通信パターン、変数への変更などを特定します。この詳細情報は、さまざまなマップ、表、およびレポートに表示されており、産業用資産の完全なインベントリ、それらの関係、それらの脆弱性、および実行されるプログラムを維持します。

運用に関するインサイト

Cisco Cyber Vision：予期しない変数の変更やコントローラの変更などの実際の産業プロセスのステータスについて、リアルタイムのインサイトを OT エンジニアに提供します。システムの整合性と実稼働の継続性を維持するための措置を講じることができます。サイバーエキスパートは、容易にこれらすべてのデータを調べて、攻撃を分析し、送信元を見つけ出すことができます。CISOs には、インシデントレポートを文書化するためのすべての情報が含まれています。

Cisco Cyber Visionは、自動化機器によって使用される独自の OT プロトコルを「理解」し、プロセスの異常、エラー、設定ミス、および不正な産業イベントを追跡できます。また、すべてを記録し、産業インフラストラクチャの一種の「フライトレコーダー」として機能します。

脅威の検出

産業用ネットワークは、これまで以上に IT ネットワークに接続されているため、マルウェアや侵入などの通常の IT 脅威から保護する必要があります。産業用ネットワークへの攻撃は、通常、アセットに対する正当な指示のように見えますが、不要なプロセスの変更を検出する必要もあります。産業用ネットワークを保護するには、さまざまな脅威検出メカニズムが必要です。

Cisco Cyber Visionは、プロトコル分析、侵入検知、および動作分析を組み合わせて、攻撃の戦術を検出します。このガイドの今後のバージョンでは、追加の詳細が提供されます。

ユースケース

セキュリティアセスメント

OT インフラストラクチャの保護は、資産のインベントリ、通信パターン、およびネットワークトポロジの正確なビューの確保から始まります。通常、産業用サイバーセキュリティ プロジェクトは、状況を理解し、何を行う必要があるかを定義するためのセキュリティアセスメントから始まります。

Cisco Cyber Vision は、すべての産業資産の正確なリストをコンポーネントレベルまで自動的に構築します。これにより、資産と IT ドメインとの間の通信フローを識別し、ネットワークマップを構築します。重大度、詳細な説明、ソリューションのガイドラインなどを含めた、脆弱性があるデバイスのリストが作成されます。また、デフォルトのパスワードなどの脆弱なクレデンシャルを持つデバイスを見分けます。

ネットワークのセグメント化

産業用セキュリティのベストプラクティスとして、IEC62443 ゾーンおよびコンジットに準拠したアーキテクチャにネットワークを移行することを推奨します。つまり、それは、相互に通信する必要がない資産をネットワークセグメントに配置し、それらのセグメントまたはゾーン間のアクセスを管理して、産業インフラストラクチャ全体への攻撃の拡散を回避することを望むことです。

Cisco Cyber Vision により、資産、ネットワーク接続、およびリモートアクセスの正確なビューを得られ、セキュアに設計された、効果的に監視できるネットワークを構築できます。これにより、資産をグループ化して「産業への影響」を定義できるため、独自の産業用安全目標に従ってイベントの優先順位付けとスコア付けを行うことができます。これにより、ゾーン間のすべてのフローが集約され、関連するトラフィックのモニタリングに集中できるようになります。

OT ドメインにサイバーセキュリティを拡張

生産の整合性、継続性、安全性を確保するには、サイバー攻撃から産業用ネットワークを保護することが重要です。産業用ドメインは、産業プロセスの修正を目的とする従来の IT 脅威とカスタム攻撃の両方にさらされているため、包括的な脅威検出手法が必要です。

Cisco Cyber Vision は、プロトコル分析、侵入検知、動作分析、および OT 脅威インテリジェンスを組み合わせて、資産の脆弱性、既知および新たな攻撃、および未知の攻撃の警告サインとなる可能性のある悪意のある動作を検出します。リアルタイムで脅威が検出されるように、アプリケーションフローを継続的に監視します。アラートは自動的に生成され、ファイアウォールなどの既存の IT セキュリティプラットフォームからの修復をトリガーするために使用できます。

統合 IT/OT SOC を実現

IT サイバーセキュリティ環境に投資した時間と資金を活用して、OT ネットワークを監視し、産業用ネットワークに対する脅威に対応します。IT SOC に OT コンテキストを提供することで、産業インフラストラクチャの特定の制約事項に準拠したセキュリティポリシーを構築し、適用することができます。

Cisco Cyber Visionは、シスコの業界トップクラスのセキュリティポートフォリオに含まれています。また、独自のセキュリティ機能を有効にするために、Firepower ファイアウォールおよび Stealthwatch Traffic Analyzer に対して OT 資産および産業脅威の検出に関する詳細情報を提供します。また、Cisco Cyber Vision は、主要な SIEM プラットフォームと統合されるため、IT SOC のすべての OT イベントを収集し、IT/OT の統合脅威管理を構築することができます。

ガバナンスとコンプライアンスの推進

重要なサイトの責任者にも、小規模な工場の責任者にも、最新の規制要件（EU NIS、NERC CIP、FDA など）に準拠して、IT と OT の両チームが協力してアクションを実行するため、OT セキュリティ態勢の詳細な情報が必要です。

Cisco Cyber Vision は、IACS からのすべてのイベントをログに記録して、履歴全体にアクセスできるようにします。これにより、効率的な監査を実行し、インシデントレポートを作成するためのアセットとイベントに関する詳細情報を取得できます。Cisco Cyber Vision は、現在起こっていることの共通の理解を全員が共有できるようにする、使いやすいユーザインターフェイスを提供します。これにより、OT および IT のプロフェッショナルは共通の目標に向けて協力することができます。

ターゲットペルソナ

IoT セキュリティを大規模に導入するには、制御エンジニア、セキュリティリーダー、およびネットワークマネージャのニーズを満たすテクノロジーが必要です。IT チームと OT チーム間のブリッジを構築するために完全に統合された包括的なセキュリティ製品のポートフォリオを提供するのはシスコだけです。これにより、IT チームと OT チームは共同作業をして、産業用ネットワークとプロセスのセキュリティを確保することができます。

- SOC チームは、実際のプロセスを明確に理解して、産業ドメインから SIEM プラットフォームにセキュリティイベントを収集し、生産を中断することなく適切な対策を講じることができます。
- CISO は、IT および OT のサイバーセキュリティに統合されたアプローチを構築するための適切なツールを備えています。すべてのセキュリティイベントを追跡し、すべての関係者と詳細なレポートを共有することにより、ガバナンスとコンプライアンスを促進します。
- 現在、制御エンジニアには、脆弱性、誤動作、異常な動作、およびプロセスの変更を自動的に識別することもできる、ダイナミックで包括的な資産のインベントリが用意されています。これにより、産業用のセットアップを最適化し、生産を維持できます。
- OT ネットワークマネージャは、シスコの産業用ネットワーク機器を活用して、専用のアプライアンスやアウトオブバンド ネットワークを必要とせずに、大規模のセキュリティモニタリングを導入します。また、Cisco Cyber Vision は、ネットワーク セグメンテーション プロジェクトを推進できるように、OT ネットワークマネージャに詳細情報を提供します。

まとめ

Cisco Cyber Vision は、IACS をセキュリティで保護するために特に設計された、資産のインベントリ、ネットワークモニタリング、および脅威インテリジェンス プラットフォームです。これは、シスコの産業用ネットワーク機器に組み込まれており、産業用アセットおよびプロセスに関するリアルタイム情報を収集し、生産インフラストラクチャを可視化し、産業コンテキストでセキュリティイベントを強化します。Cisco Cyber Vision により、IT チームと OT チームは、産業用ネットワークと運用イベントに関する共通の理解を共有し、ネットワークのセグメンテーション、脅威の検出、および修復を連携して行い、産業運営の継続性、復元力、安全性を確保できるようになります。

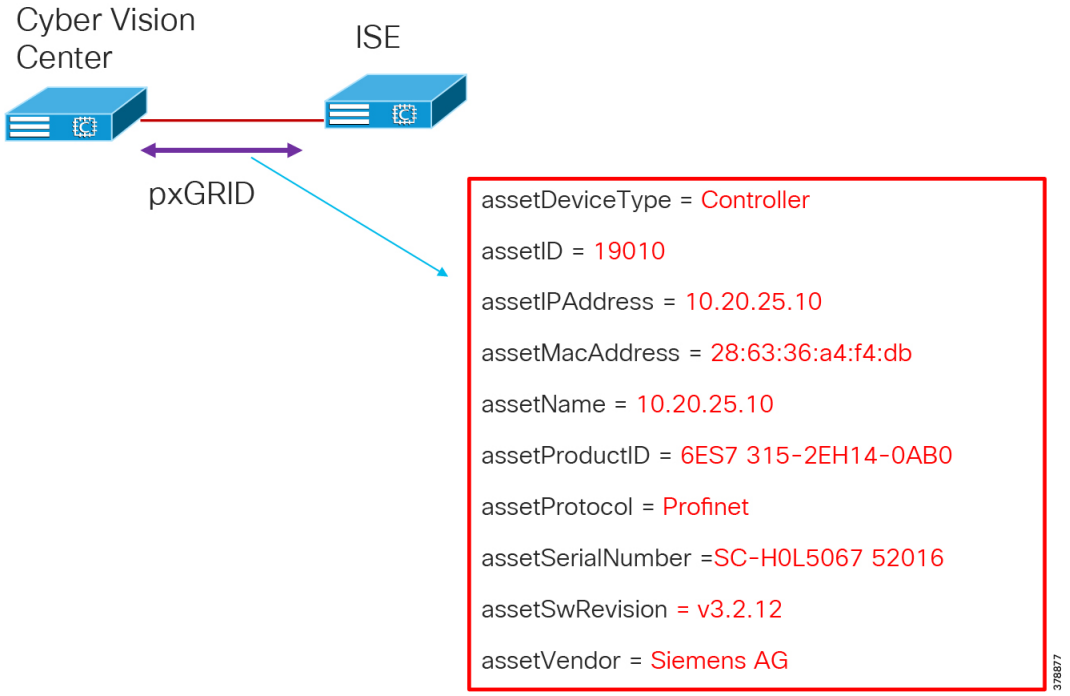
Cisco Identity Services Engine

Cisco ISE は、OT と IT のセキュリティ管理チームがアクセスレベルのセキュリティポリシーを作成および実行できるようにするセキュリティ管理製品です。Cisco ISE の主要な機能の 1 つは、ネットワークに接続されているエンドポイントを検出および分類して、サービスをプロファイリングすることです。ISE は、MAC アドレスを一意の識別子として使用し、ネットワーク エンドポイントごとにさまざまな属性を収集して、内部エンドポイント データベースを構築します。分類プロセスは、収集された属性と事前に定義された条件またはユーザ定義の条件を照合してから、拡張可能なプロファイル ライブラリに関連付けます。これらのプロファイルは、モバイル クライアント（iPad、Android タブレット、Blackberry フォンなど）、デスクトップ オペレーティングシステム（Windows 7、Mac OS X、Linux など）、およびプリンタ、電話機、カメラ、ゲームコンソールなどのさまざまな非ユーザシステムを含む広範囲のデバイスタイプに及びます。

ただし、IACS アセットの場合、ISE のビルトインプローブは、IACS からのすべての情報を取得して、詳細なプロファイリング ポリシーを作成することはできません。これは、IACS アセットが、デバイスのプロファイリングを行うために ISE が依存する従来の IT プロトコルをサポートしていない可能性があるためです。産業用自動化ソリューションは、IACS アセットの可視性を得るために、産業用ネットワークディレクタを使用します。これにより、OT チームは産業運用のコンテキストで IACS アセットを完全に可視化し、システムのアベイラビリティとパフォーマンスを向上させて、全体的な有効性を高めることができるようになります。

Cisco Cyber Vision は、Cisco pxGrid とインターフェイスで接続します。これは、オープンで拡張性があり、IETF 標準規格を重視したデータ共有および脅威制御プラットフォームであり、属性を介して ISE にデバイス情報を伝達します。この統合により、Cisco Cyber Vision によって検出されたエンドポイントを ISE にエクスポートできます。また、Cisco Cyber Vision は、図 48 に示すように、IACS アセットのプロファイリングポリシーを作成するために使用される ISE に複数の属性をエクスポートします。

図 48　Cisco Cyber Vision による ISE への属性のエクスポート



Cisco Cyber Visionと ISE の統合には、次のような利点があります。

- ISE エンドポイントデータベースに自動的に IACS を登録します。
- OT と IT のセキュリティ管理チームが、Cisco Cyber Vision から受信した属性に基づいてきめ細かいプロファイリングポリシーを作成できるようにします。
- OT エンジニアが、Cisco Cyber Vision と ISE の統合を利用して、ネットワークに新しいセキュリティポリシーを自動的に導入できるようにします。

Cisco Cyber Vision、Cisco Industrial Network Director、および Cisco Stealthwatch の比較

産業用ネットワークのセキュリティにはさまざまな要素が含まれています。シスコのアプローチは、すべての領域を網羅するカバレッジを提供することです。シスコは、Cisco Identity Services Engine を使用した補完的なテクノロジーである、Cisco Cyber Vision、Cisco Industrial Network Director、および Cisco Stealthwatch を提供し、広範なカバレッジのための効果的な組み合わせを提供します。

Cisco Stealthwatch はマルウェア、ゼロデイワーム、および企業に対するその他の IT 脅威に対応しています。

表 31　Cisco Cyber Vision、Cisco Industrial Network Director、および Cisco Stealthwatch の比較

	Cisco Cyber Vision	Cisco Industrial Network Director	Cisco Stealthwatch
内容	Cisco Cyber Vision は、産業運用の継続性、復元力、および安全性を確保するために特別に設計されたサイバーセキュリティ ソリューションです。産業用ネットワーク内に容易に展開することにより、産業アセットとアプリケーションフローを監視して、IT セキュリティを OT ドメインに拡張します。	Cisco IND は、産業用イーサネットネットワークにおける運用中心型のネットワーク管理を実現します。システムは、CIP、Profinet、OPC-UA、Modbus、BACnet などの産業用自動化プロトコルをサポートし、PLC、IO、HMI などの自動化デバイスを検出します。オートメーションおよびネットワーキングアセットの統合トポロジマップを作成して提供し、運用部門と工場 IT 担当者に産業用ネットワークを管理および維持するための共通フレームワークが提供されます。 OT チームに、ユーザフレンドリーなアクティブスキャン ネットワークモニタリング ソリューションを提供します。IND は ISE pxGrid と統合して、TrustSec セグメンテーションのプロファイリングで使用されるデバイスコンテキストの詳細を提供します。また pxGrid 統合により、OT スタッフは、運用上の目的に基づいてアセットの属性値を更新することによって、セキュリティポリシーを適用することができます。	Cisco Stealthwatch は、企業全体のネットワークの可視性を提供し、高度なセキュリティ分析を行い、リアルタイムで脅威を検出して対処します。行動モデリング、機械学習、およびグローバルな脅威インテリジェンスの組み合わせを使用することで、Stealthwatch は迅速かつ高い信頼性で、コマンドアンドコントロール（C & C）攻撃、ランサムウェア、分散型サービス妨害（DDoS）攻撃、違法仮想通貨マイニング、未知のマルウェア、および内部の脅威などの脅威を検出できます。単一のエージェントレス ソリューションにより、暗号化されている場合でも、ネットワークトラフィック全体にわたって包括的な脅威モニタリングを実現できます。
検出方法	パッシブ	アクティブなスキャン	パッシブ
重点	産業ネットワークおよびプロトコルに重点を置いています。これは、Purdue モデルのレベル 0 ~ 2 にほぼ対応します。	Purdue モデルのレベル 0 ~ 2 で、産業ネットワークおよびプロトコルに重点を置いています。	企業の IT ネットワークに重点を置いています。これは、Purdue モデルのレベル 3 ~ 5 に対応しています。パケットには IP アドレスが必要です。

アクティブディスカバリおよびパッシブディスカバリ

ネットワークの脆弱性検出には、アクティブとパッシブの 2 つのアプローチがあります。アクティブなアプローチには、組織がシステムの侵害を阻止するすべてのものが含まれていますが、パッシブ（またはモニタリング）アプローチには、組織がシステムセキュリティを監視する方法がすべて含まれています。2 つのタイプの保護間で選択する必要があると考えるのは誤りです。

パッシブアプローチにより、セキュリティ担当者は、現在使用されているオペレーティングシステム、システム内で送受信されているもの、利用可能なサービス、また、セキュリティの脅威に対して脆弱になる可能性があるシステムの場所を監視することができます。一方、アクティブなアプローチは、システムとアプリケーションの脆弱性に関するより詳細な情報を提供します。

つまり、2 つのタイプのディスカバリ/スキャナのメソッドは相互に補完します。表 32 2 つのディスカバリメカニズムの特性について説明します。

表 32　パッシブスキャンおよびアクティブスキャンの特性

特性	パッシブ	アクティブ
ネットワークへの影響の可能性	低：パッシブディスカバリはアセットを調査せず、単にパケットを検査してパッシブオブザーバとして動作します。パケットを観察するためには、必ずパケットを複製する必要があります。1 つの予防策は、観察されるトラフィックの重複によって、ネットワークの使用可能な帯域幅をオーバーサブスクライブしないようにすることです。このような状況にならないようにするため、シンプルなアーキテクチャソリューションが用意されています。 シスコは、ネットワークデバイスと Cisco Cyber Vision を使用する、非常に効果的な戦略を用意しています。基本的にパッシブディスカバリ センサーはネットワーク要素内で使用可能であり、ネットワーク上でトラフィックを複製する必要はありません。	中：アクティブスキャンにより、アセットまたはネットワークに悪影響が及ぼされる可能性があります。したがって、アクティブなスキャン方法を使用する場合は注意が必要です。特定のスキャンツールでは、すべての TCP プロトコルに対してテストを実行できますが、アセットとネットワークの膨大な負荷を発生させます。 実稼働環境では、アクティブスキャンおよび特に繰り返されるアクティブスキャンによって、実稼働中に影響が及ぶリスクが増加する可能性があります。デバイスへの ping または質問パケットの頻度を管理します。一部の古いコントローラとデバイスは、PING/ARP パケットを効率的に処理できない場合があります。 最良のアプローチは、リスクを封じ込める運用方法を考案することです。たとえば、アクティブスキャンは、実稼働での予定されたダウンタイム時に実行して、非常に抑制されたサブネットに限定できます。
アセットディスカバリの完全性	非常に効果的：アセットがパケットを送受信している場合は、アセットは検出されます。もちろん、これは、パケットを確認することができるパッシブスキャナのセンサー要素に依存します。そのため、センサーを効果的に配置することが非常に重要です。パケットの送受信を行っていないアセットは検出されません。	可変的：一部のアセットはスキャン中にオフラインになり、検出されません。ACL を使用すると、（SNMP などの）質問パケットがアセットやサブネットに到達できなくなり、アセットが検出されなくなる可能性があります。これは、複数のスキャンが実行される理由の 1 つですが、中断のリスクとのバランスをとる必要があります。 ディスカバリの完全性は、ネットワークの設計と ACL、およびアセットがオンラインで質問パケットに応答するかどうかに大きく依存します。 もう 1 つの課題は、新しいデバイスがオンラインになったときに、アクティブなスキャンが実行されない場合は、そのようなアセットが検出されるまでに時間がかかることです。
アセット情報の完全性	不確定的：性質上、パッシブディスカバリは、アセットによって送信された情報のみを特定できます。一部の情報は、長期間発信されず、未検出のままになる可能性があります。たとえば、Rockwell PLC が存在することがわかりますが、特定のコマンドによってファームウェアバージョンを含むパケットが送信されるまでは、その PLC のファームウェアのバージョンが不明である可能性があります。	高確定的：アセットがオンラインで到達可能で、質問コマンドに応答すると、そのアセットに関連するすべての情報が検出可能になります。アセットがオンラインでない場合、またはすべての質問要求に応答しない場合は、「応答不可」とマークできます。ただし、いずれの場合でも、オペレータは、認識しているものと認識していないものをかなりの確信のもとに把握することができます。

表 32　パッシブスキャンおよびアクティブスキャンの特性（続き）

特性	パッシブ	アクティブ
アセット情報の適時性	全体像を構築するためには時間がかかります。アクティブなアセットのアセットディスカバリは瞬間的に行われます。つまり、パケットを送信する瞬間です。ただし、アセットの全体像を取得するには時間がかかることがあります。これは、パッシブスキャナが必要な情報を含む関連パケットを送信して全体像の取得を完了するまで待機する必要があるためです。これは、オペレータが影響の少ない ping をアセットへ送信することにより高速化することができます。	オンデマンド：アクティブスキャンにより、オンデマンドでアセットを調査できます。ただし、無差別な調査は、アセットに意図しない問題を引き起こす場合があります。アセットへの問い合わせが殺到することにより、サービス妨害攻撃として認識される可能性があります。
脆弱性のモニタリングと攻撃のシミュレーション	パッシブディスカバリは脆弱性モニタリングのみに重点を置いています。攻撃のシミュレーションは実行しません。	アクティブスキャナは攻撃をシミュレートできますが、このようなシミュレーションには注意する必要があります。
シスコ製品	現在、Cisco Cyber Vision はパッシブスキャンに重点を置いています。Cisco Stealthwatch はパッシブモニタでもあります。	Cisco Industrial Network Director は、ネットワーク管理に加えて、アクティブスキャンに重点を置いています。

セル/エリアゾーンのセキュリティ

工場でのデジタル変革イニシアチブは、従来の OT の次元を変えつつあります。新しいネットワーキング テクノロジーと COTS のハードウェア/ソフトウェアがレガシー製品に取って代わり、新しいビジネス イニシアチブが IT/OT コンバージェンスへの動きを促しています。テクノロジー自体ではセキュリティレルム全体に対処できません。サイバーセキュリティの脅威に対処するには、人とプロセスが重要な役割を果たす必要があります。これは、OT セキュリティに対処する際の要点です。IT チームは、産業環境内で適用されるビジネスの要件とプロセスを完全に理解し、実装を支援する必要があります。このことは、従来の IT のスキルセットが限られており、IT チームおよび OT チームが従来のサイロ化されたネットワーク管理アプローチから移行して連携する必要があるセル/エリアゾーンにおいて、非常に大きな意味を持ちます。2015 年の Gartner の調査によると、IT セキュリティ チームが OT スタッフに協力し、派遣され、または統合されて、包括的なセキュリティ戦略が計画されることで、セキュリティの強化が可能になります。

セル/エリアゾーンでのセキュリティは、工場内の全体的なエンドツーエンド セキュリティ アーキテクチャのコンポーネントとみなす必要があります。セキュリティ機能は、工場の枠を超えて広げる必要があり、工場の安全性、24 時間 365 日のアベイラビリティ、および高い OEE 要件をサポートしながら、全体的なコンプライアンス活動に関連する既存のプロセスと戦略を網羅する必要があります。

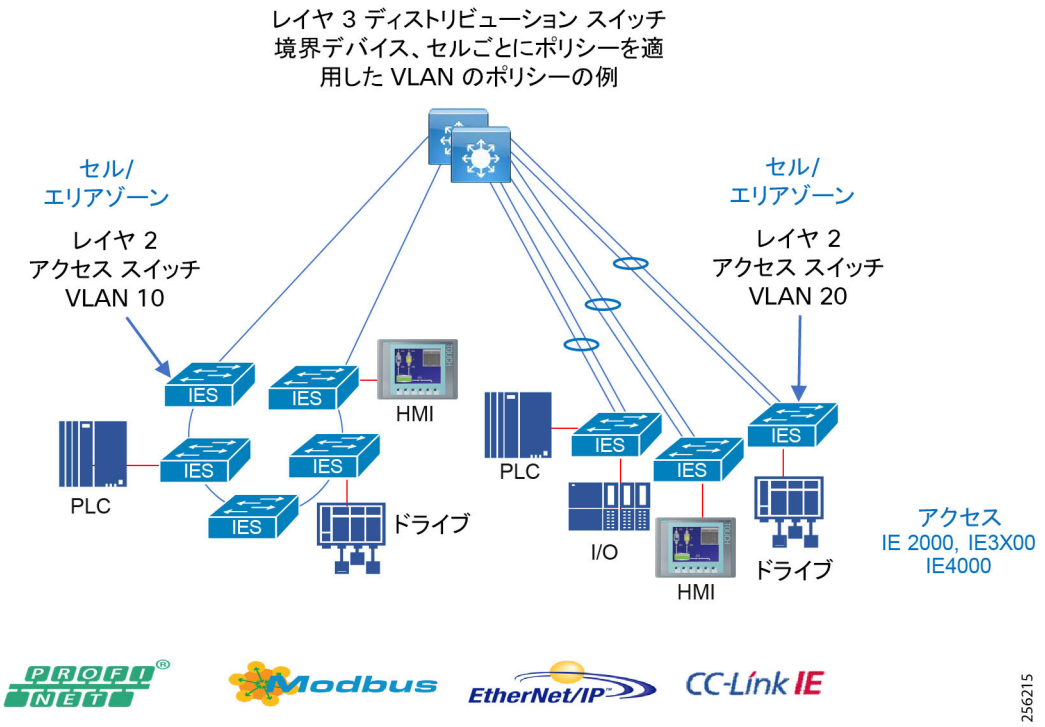
ここでは、セル/エリアゾーンおよび基本セグメンテーションのためのネットワーク強化と、VLAN セグメンテーションによる制限付きのデータフロー技術について説明します。このベースライン セキュリティ機能のより堅牢で拡張可能なセキュリティ アーキテクチャへの進化については、産業用オートメーション向けの OT インテントベース セキュリティのユースケース（121 ページ）で説明しています。そこでは、Cisco Cyber Vision によるアセットの可視性、Cisco ISE による TrustSec を使用したセグメンテーション、および Cisco Stealthwatch によるフローベースの異常検出に焦点が合わされています。

制限付きのデータフロー セグメンテーションとゾーン分割

セグメンテーションは、IACS のネットワークとプロセスの保護に役立つ信頼ゾーンを作成するための重要なコンポーネントです。IEC 62443 には、プロセス ネットワークまたはサービスの間の不要なデータフローを制限するために、制御システムをゾーンおよびコンジットに分割するための制限付きデータフローの推奨事項が詳述されています。信頼できないエンティティ間のトラフィックの意図的または偶発的な相互作用は制限する必要があります。産業用オートメーション ソリューションは、セル/エリアゾーン トラフィックをセグメント化するための基本的な論理的分離ガイダンスを提供します。一部の工場では、リスクに基づいてネットワークが物理的に分離されたネットワークに完全にセグメント化されています。たとえば、工場には、非運用マルチサービス タイプのアプリケーション（工場内の音声サービスなど）用に物理的に分離された専用ネットワークがある場合があります。

一般的な工場ネットワーク内では、ゾーンは、セル/エリア（レベル 0 ～ 2）、産業運用/制御（レベル 3）、IDMZ、および企業（レベル 5）として定義されています。セル/エリアゾーンの場合、一般にセルまたはエリアごとに、互いに通信する必要があるグループ化された IACS アセットにさらにセグメント化されます。VLAN セグメンテーションは、セル/エリアゾーン全体にセグメンテーションを作成するために採用されてきた従来のアプローチです。VLAN は、レイヤ 2 ドメイン/サブネット内で互いに通信する必要があるデバイスのグループに対して定義され、レイヤ 3 ルータ、スイッチ、ファイアウォールなどの境界デバイスが、VLAN の外部との通信を許可または拒否します。これにより、コントローラ間の通信やコントローラと IACS の間の通信などのセル/エリア間通信が実現されます。境界デバイスは、境界に導入されたデバイスで手動設定される従来の ACL またはファイアウォールルールにより、VLAN またはセル/エリアと工場のその他のエリアの間でアクセス制御を適用できます。レイヤ 3 ディストリビューション スイッチがこの機能を提供し、セル/エリアゾーンのポリシー適用ポイントになります。

図 49　セル/エリアゾーンのレイヤ 3 ディストリビューション境界デバイス



VLAN セグメンテーションと ACL は、IACS ネットワーク内で制限付きのデータフローを提供するための従来の方法です。小規模工場の場合は管理可能ですが、大規模工場の場合はアクセスポリシーの維持が煩雑で困難なものになる可能性があります。ネットワークに追加されるデバイスが増えるにつれて、ACL はポリシー適用ポイントで大きくなり始め、ネットワーク内のさまざまな場所に実装されるようになり、産業工場全体にポリシーの適用が分散されます。ACL を継続的に更新すると、設定ミスのリスクが高まります。また、そのような更新は一般的に拡張可能ではありません。産業用オートメーション向けの OT インテントベース セキュリティのユースケース（121 ページ）産業用オートメーション ネットワークのセキュリティを強化するために役立つユースケースと TrustSec アーキテクチャへの発展の詳細が示されています。

ネットワーク強化：システム整合性のコンポーネント

サイバーセキュリティの分野では、システムの強化は、システムの攻撃対象領域または脆弱性を削減し、強化手段によって攻撃に対する復元力を高めることと定義できます。強化の作業には、不要なサービス/アプリケーションの無効化、システムへの最小限の特権ユーザアクセスの設定、およびマルウェア対策、ウイルス対策、エンドポイントセキュリティなどのセキュリティ機能の追加が含まれます。一般的なシステム強化作業は、ネットワークにも適用されます。ネットワークの強化では、最小限の特権アクセス制御の導入、未使用のサービスの無効化または削除、ログの記録、およびセキュア プロトコルの有効化が行われます。これらの強化機能は、ネットワーキング システム内の 3 つの機能プレーンにわたって設定する必要があります。これらの 3 つの機能プレーンとは、管理プレーン、コントロールプレーン、およびデータ プレーンです。

- 管理プレーン: 管理プレーンは、ネットワーキングデバイスへのアクセスを提供し、ネットワーキングシステムの管理を提供する機能で構成されます。管理プレーンにより、デバイスのアクセス、設定、および管理と、デバイスの動作やデバイスが導入されているネットワークのモニタリングを行うことができます。これには、SSH を使用するインタラクティブ管理セッションや、SNMP または NetFlow による統計情報収集が含まれます。ネットワークデバイスのセキュリティを検討する場合は、管理プレーンを保護することが重要です。セキュリティインシデントによって管理プレーンの機能が弱体化すると、ネットワークを回復または安定化できなくなる可能性があります。可能であれば、ネットワーク管理用のアウトオブバンド ネットワークを導入する必要があります。これにより、ネットワーク管理トラフィックと IACS トラフィックが分離され、デバイスの到達可能性が IACS ネットワークで発生している可能性のある問題とは無関係に保たれるという利点があります。アウトオブバンド ネットワークが不可能な場合は、専用ネットワーク管理 VLAN を使用して論理的に分離されたネットワークを利用する必要があります。

- コントロール プレーン: ネットワーク デバイスのコントロール プレーンは、ネットワーク インフラストラクチャの機能を維持するために最も重要なトラフィックを処理します。コントロール プレーンは、ネットワーク デバイス間のアプリケーションとプロトコルで構成され、それらにはルーティング プロトコルと REP などのレイヤ 2 プロトコルが含まれます。管理プレーンとデータプレーンのイベントがコントロールプレーンに悪影響を与えないことが重要です。サービス妨害(DoS)攻撃などのデータプレーンイベントによってコントロールプレーンが影響を受けると、ネットワーク全体が不安定になる可能性があります。また、異常がネットワーク デバイスの CPU パフォーマンスに影響を与え、ネットワーク デバイスが不安定になり、それによってネットワーク全体の不安定性が発生/増加しないように、コントロール プレーン トラフィックを理解し、保護する必要があることにも注意してください。

- データ プレーン: データ プレーンは、ネットワーキング デバイスを介してネットワーキング システム全体にデータを転送します。これは、コントローラ、I/O、HMI といったネットワークに接続されるデバイスの間の IACS データ トラフィックです。データ プレーンには、ネットワークでサポートされているホスト、クライアント、サーバ、およびアプリケーションで生成され、それらのデバイス間で送受信される「顧客の」アプリケーション トラフィックの論理グループが含まれます。セキュリティの観点からは(また、データ プレーンは最も高いトラフィック レートを表すため)、例外パケットが CPU に送信されてコントロールプレーンや管理プレーンに影響を与えることを防ぐために、データプレーンを保護することが不可欠です。

以下に、ネットワーク強化のためのベストプラクティスを示します。

管理プレーン

- IDMZ を含む工場全体に、専用のアウトオブバンド ネットワークを導入する必要があります。
- AAA フレームワークは実装される必要があります。これは、ネットワーク デバイスへのインタラクティブ アクセスを保護するために不可欠であり、ネットワークのニーズに基づいて調整できる高度に設定可能な環境を提供します。
- ACL は、ネットワークデバイスへの不正な直接通信を防止するために実行する必要があります。
- ネットワーキング機器にアクセスするため、SSH および SNMP v3 などのセキュアなネットワーキング プロトコルを設定します。
- アーキテクチャ全体でネットワーク システム ロギングを有効にする必要があります。
- すべてのネットワークデバイス設定は、初期インストール、セットアップ、およびそれに続く変更の後にバックアップする必要があります。

コントロールプレーン

- ほとんどのルータやスイッチは、コントロールプレーンの保護またはポリシングと同等の機能によって、DoS 型攻撃から CPU を保護できます。

スイッチ

- スイッチドネットワーク内では、スイッチドネットワーク全体を不安定な状態から保護することが重要です。これらのタイプのネットワークでは、レイヤ 2 スイッチドドメインの整合性を保護するためのメカニズムが導入されます。たとえば、スパニング ツリー プロトコルをこれらのスイッチド ドメイン内で使用すると、冗長レイヤ 2 インフラストラクチャでループ フリー トポロジを維持するために役立ちます。レイヤ 2 ネットワーク内には、ネットワークの安定性に関する情報を提供するために役立つルートデバイスが存在します。これらのルートデバイスが変更されないように、ガードメカニズムを設定する必要があります。たとえば、ブリッジ プロトコル データ ユニット(BPDU)ガードやルートガードを設定して、レイヤ 2 ドメインの保護やスパニングツリーの不安定化の防止に役立てる必要があります。

ルータ/ルーティング保護/レイヤ 3 スイッチ

- ネイバー認証：設定すると、ネイバールータ間でルーティングアップデートが交換されるたびにネイバー認証が行われます。この認証により、ルータは、信頼できるデバイスから信頼できるルーティング情報を受信できるようになります。
- ルーティングピアの定義：ルータの導入やセットアップを容易にする動的ピア検出メカニズムを利用することで、不正なルータをルーティング インフラストラクチャに挿入することが可能になる場合があります。既知の IP アドレスを使用して信頼できるネイバーのリストを静的に設定し、そのような動的メカニズムを無効にすることで、この問題を回避できます。これは、ネイバー認証やルートフィルタリングなどの他のルーティングセキュリティ機能と組み合わせて使用できます。
- コントロール プレーンのポリシング/保護：不正なセッションの確立を防ぐことによって、セッション リセット攻撃の可能性を削減し、ルーティング セッションの保護を容易にするために、このオプションを設定する必要があります。

データ プレーン

- 未使用のポート：使用されていないポートをシャットダウン状態にします。スイッチのためには、未使用の VLAN（VLAN 1 以外）を使用して switchport VLAN コマンドを追加すれば、ポートが誤ってアクティブにされても、導入済みの VLAN に影響がおよびません。
- ポートのセキュリティにより、特定のインターフェイスの MAC 数が制限されます。これは、MAC 攻撃などの脅威を防ぐために役立ちます。ポートのセキュリティはスイッチ アクセス ポートで有効にする必要があります。
- DHCP スヌーピング：アーキテクチャ内のサーバまたはワークステーションが Dynamic Host Configuration Protocol（DHCP）を使用している場合は、DHCP スヌーピングと動的 ARP 検査（DAI）を検討する必要があります。
- トラフィック ストーム制御：トラフィックストームはパケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィックストーム制御機能を使用すると、ブロードキャスト、マルチキャスト、または未知のユニキャスト トラフィック ストームによってイーサネット インターフェイス経由の通信が妨害されるのを防ぐことができます。

VLAN のベスト プラクティス

- すべての未使用ポートを無効にして、それらを未使用 VLAN に配置します。有効になっているオープン ポートはすべて、ネットワークにアクセスする手段を提供します。
- VLAN 1 は決して使用しないでください。VLAN 1 はデフォルトの VLAN であり、デフォルトですべてのポートで有効になっています。そのため、すべてのスイッチのすべてのポートを VLAN 1 以外の VLAN に関連付けるように設定することがセキュリティ上のベスト プラクティスとなります。
- エンドステーションがスイッチとしてスプーフィングできる VLAN ホッピング攻撃の防止を支援するために、すべてのユーザ側ポートを非トランキングとして設定します。トランクでネイティブ VLAN のタグ付けを強制し、タグなしフレームをドロップして、VLAN ホッピングの防止を支援します。
- インフラストラクチャポートでのトランキングを明示的に設定します。スイッチを接続するポートの場合は、トランキングが、ネットワーク全体に VLAN を拡張するために使用されます。その他のスイッチに拡張する必要がある VLAN だけを明示的に設定してください。

注：DHCP スヌーピングまたは動的 Advance Resolution Protocol（ARP）検査では IP デバイス トラッキングが利用されます。IP デバイス トランキングを有効にすると、特定の産業環境で問題が発生しやすくなります。産業用オートメーション向けの OT インテントベース セキュリティのユースケース（121 ページ）で詳しく説明されている IP デバイストラッキングの設計上のベストプラクティスに従ってください。

OT インテントベースのネットワーキング セキュリティ

産業用工場ネットワークは、企業ネットワークよりも、マルウェアの伝播に対する耐性があります。たとえば、PLC Blaster ワーム（Ralf Spenneberg, n.d.）は、ラボで、PLC の脆弱性をどのように悪用する可能性があるかが確認されました。この PCL がワームに感染すると、ネットワーク内の他の脆弱なデバイス（PLC）が検出され、そのワームが検出されたターゲットに複製されます。この攻撃はラボで確認されていますが、の可視性、トラフィックのセグメンテーション、マルウェアの検出、感染デバイスの修復といった適切なセキュリティ保護が存在せず、OT インテントベースの制御メカニズムが工場に導入されていない、マルウェアが IACS デバイスを攻撃できることを示しています。

PLC Blaster などのマルウェアによる産業工場への攻撃を防ぐために、次のことを考慮する必要があります。

- 工場フロアに存在するすべての IACS デバイスおよび通信を可視化します。ネットワーク内でどのデバイスが存在してアクティブになっているのか、そして誰が通信しているのかを把握することは、デバイスの通信を制御するポリシーを設計する上で非常に重要です。たとえば、ネットワークに接続されている PLC が可視化されていれば、その PLC を保護するセキュリティポリシーを設計できます。
- 工場のフロアにあるデバイスの通信を制限します。PLC が有限数のデバイスとしか通信できない場合は、潜在的な脅威の対象領域を減らすことができます。
- ネットワーク内のマルウェアの拡散を検出します。PLC blaster ワームの 1 つの動作は、ネットワークをスキャンして他の脆弱なデバイスを検出することです。鍵となる防衛戦略は、ネットワーク内で予期しないスキャンが行われていることを検出して、修復アクションプランを計画することです。
- デバイスへのリモートアクセスの制限。IACS デバイスが停止している場合や高度なトラブルシューティングが必要な場合、状況によっては、リモート エキスパートがデバイスにアクセスして詳細な分析を行う必要があります。オペレーションズ チームは、リモートトラブルシューティングのための適切なデバイスのアクセシビリティを決定する必要があります。

注：シスコと Rockwell Automation は、EtherNet/IP ベース デバイス向けの OT インテントベース ネットワーク セキュリティを共同で設計し、検証しました。詳細については、「以前のドキュメントと関連ドキュメント（219 ページ）」に示されている CPwE ネットワークの CVD を参照してください。

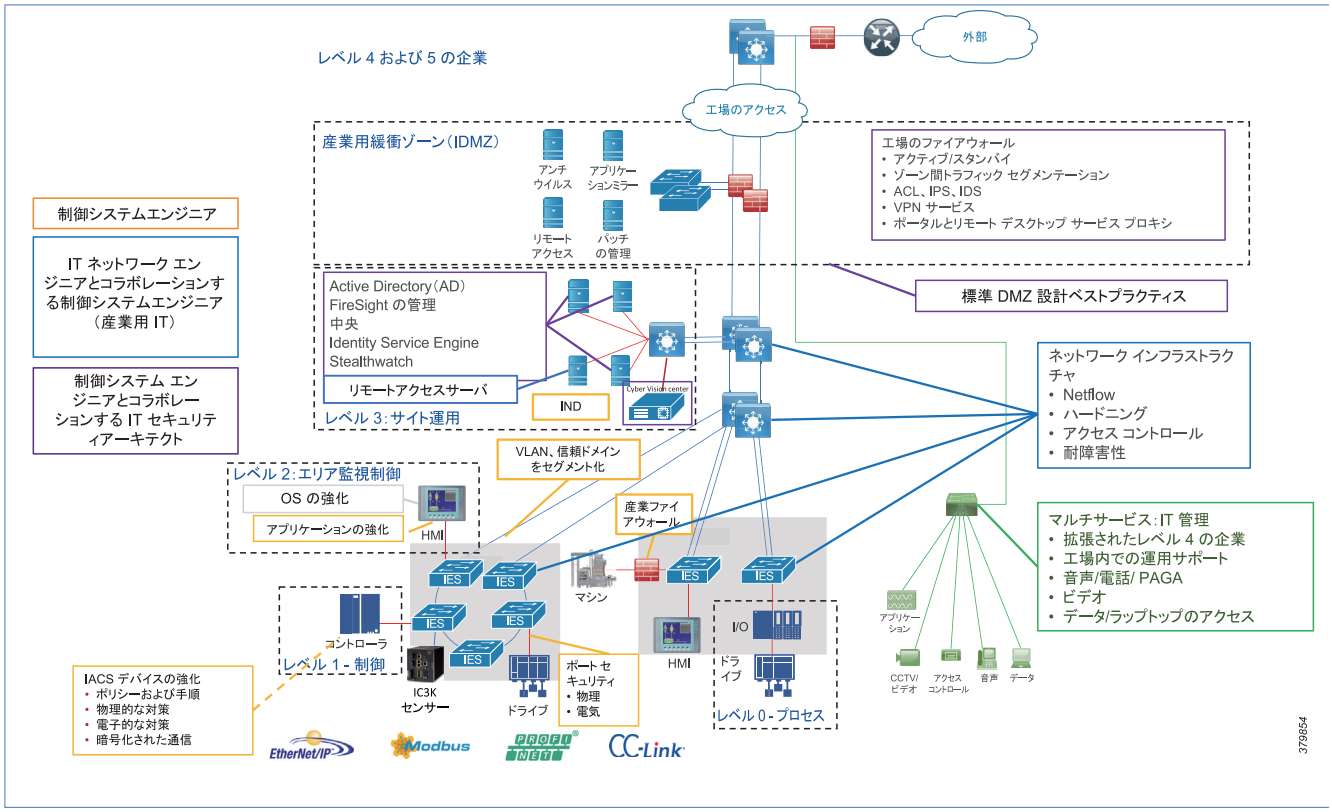
ここでは、次の内容について説明します。

- IACS 工場セキュリティのリファレンスアーキテクチャ
- システム コンポーネントの概要
- セル/エリアゾーン
- セル/エリアゾーンにネットワーク セキュリティを導入するための設計上の考慮事項

工場全体のセキュリティのリファレンスアーキテクチャ

図 50 に、工場全体のセキュリティの概要とセキュリティを展開するための推奨される責任エリアを示します。これには、制御システムエンジニア、IT ネットワークエンジニア、および IT セキュリティアーキテクトの間のコラボレーションが示されています。

図 50　工場全体のセキュリティの概要と責任エリア



CPwE CVD では、セキュリティアーキテクチャのペルソナが定義されています。次に、上の図に対応する詳細を示します。

- 制御システム エンジニア（黄色で強調表示）：IACS アセットの強化（物理的、電子的など）、インフラストラクチャ デバイスの強化（ポート セキュリティなど）、ネットワークのモニタリング/変更管理、ネットワーク セグメンテーション（信頼ゾーン分割）、IACS アプリケーション エッジの産業用ファイアウォール（検査機能付き）、および IACS アプリケーション AAA。

- IT ネットワークと連携する制御システム エンジニア（青色で強調表示）：コンピュータの強化（OS パッチ適用、アプリケーション ホワイトリスト登録）、ネットワーク デバイスの強化（アクセス制御、復元力など）、ネットワークのモニタリング/検査、および有線/ワイヤレス LAN アクセスポリシー。

- 制御システム エンジニアと連携する IT セキュリティ アーキテクト（紫色で強調表示）：アイデンティティ/モビリティ サービス（有線/ワイヤレス）、ネットワークモニタリングと異常検出、Active Directory（AD）、リモートアクセスサーバ、工場のファイアウォール、および IDMZ 設計上のベストプラクティス。

標準化は、人のプロセスとテクノロジーを合致させる全体的なセキュリティ戦略の提示を容易にするために重要な役割を果たします。セキュリティリスク評価は重要なステップであり、どのシステムがクリティカル制御か、非クリティカル制御か、非運用かを定義して、ビジネス要件と安全要件を満たしながら全体的なセキュリティ アーキテクチャ全体を定義することを支援するために役立ちます。リスク評価のガイドラインは、IEC 62443-3-2 に示されています。リスクを評価すると、IEC 62443-3-3 で定義されている基本的なセキュリティ要件によって、産業用制御システムを保護するためのガイダンスが得られます。産業用オートメーション プログラムの DIG は、次の基本要件と合致します。

- 基本要件 1「識別と認証の制御」：すべてのユーザ（人、ソフトウェア プロセス、およびデバイス）を識別し、制御システムへのアクセスを許可する前に認証します。

- 基本要件 2「使用の制御」:認証されたユーザに割り当てられた特権を適用し、IACS で要求されたアクションを IACS で実行して、これらの特権の使用をモニタします。
- 基本要件 3「システムの整合性」:不正操作を防止するために IACS の整合性を確保します。
- 基本要件 4「データの機密性」:通信ネットワーク上の情報とストレージ内の情報の機密性を確保します。これには、セグメンテーション、不正アクセスからの保護、データ暗号化などの手法が含まれる場合があります。
- 基本要件 5「制限付きデータフロー」:セグメンテーションとゾーンを使用して各環境およびコンジットを分離し、ゾーンとアーキテクチャ層の間の不要なデータフローを制限します。
- 基本要件 6「イベントへの適時の対応」:インフラストラクチャのセキュリティを管理、モニタ、記録、および管理して、セキュリティの脅威または侵害を防止します(管理監査、ロギング、および脅威検出が含まれます)。
- 基本要件 7「リソースのアベイラビリティ」:重要なサービスのパフォーマンス低下や妨害を防ぎ、制御システムのアベイラビリティを確保します。

システム コンポーネントの概要

以下のシスコのセキュリティ コンポーネントは、セル/エリアゾーンを保護するために役立ちます。

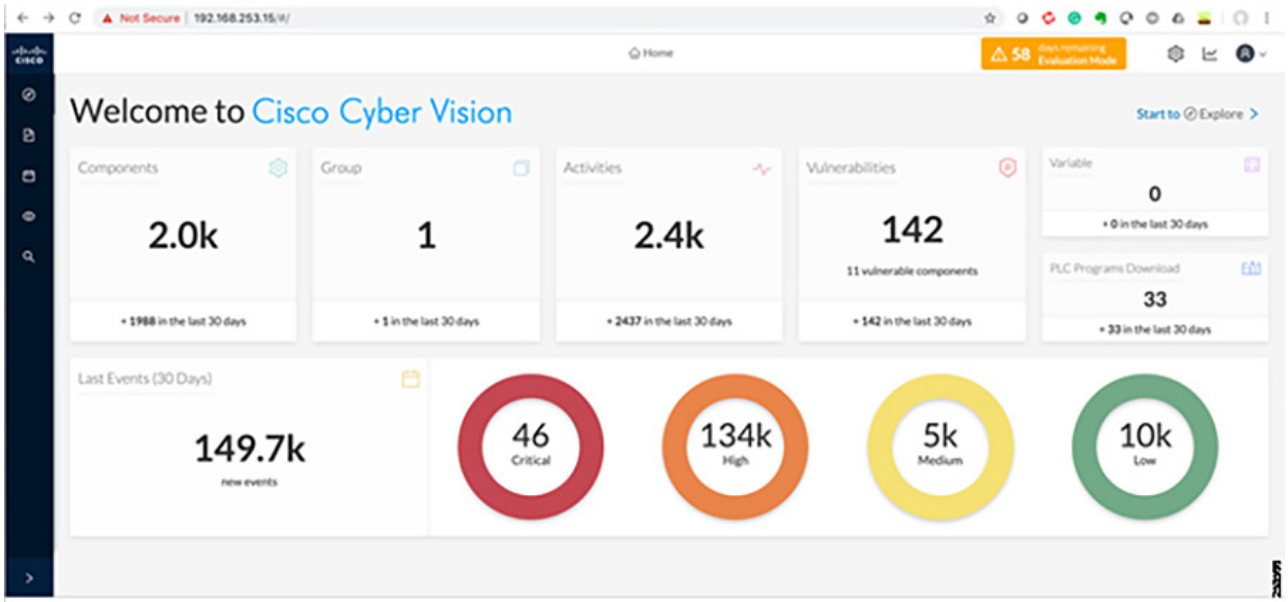
Cisco Cyber Vision

Cisco Cyber Visionには、Center と Sensor の 2 つの主要コンポーネントがあります。Sensor は、ディープ パケット インスペクション(DPI)を使用してパケットをフィルタリングし、メタデータを抽出します。これは、より詳細な分析のために Center に送信されます。ディープ パケット インスペクションは、ネットワークで発生している異常な動作を検出するために、アプリケーション層を含むパケットを検査する高度なプロセスです。Sensor は、ネットワークトラフィックの過負荷を防止するために、メタデータ情報だけを Center に送信します。

Cisco Cyber Vision Center

Cisco Cyber Vision Center は、仮想マシンとして、またはハードウェアアプライアンスとしてインストールできるアプリケーションです。Center は、OT オペレータがネットワーク インフラストラクチャを視覚的に把握できるようわかりやすい可視化を提供します。図 51 Cisco Cyber Vision Center ダッシュボードのハイレベルな概要を示します。

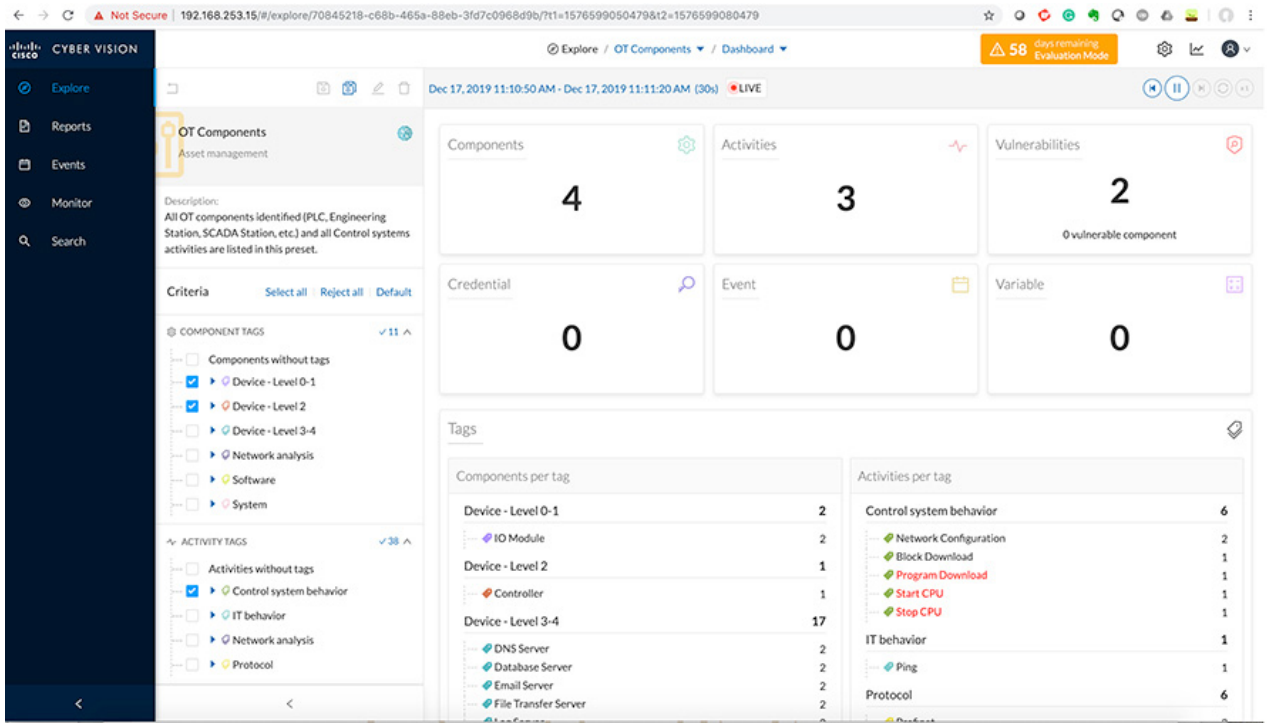
図 51　Cisco Cyber Vision Center ダッシュボード



Center は、次の機能を提供します。

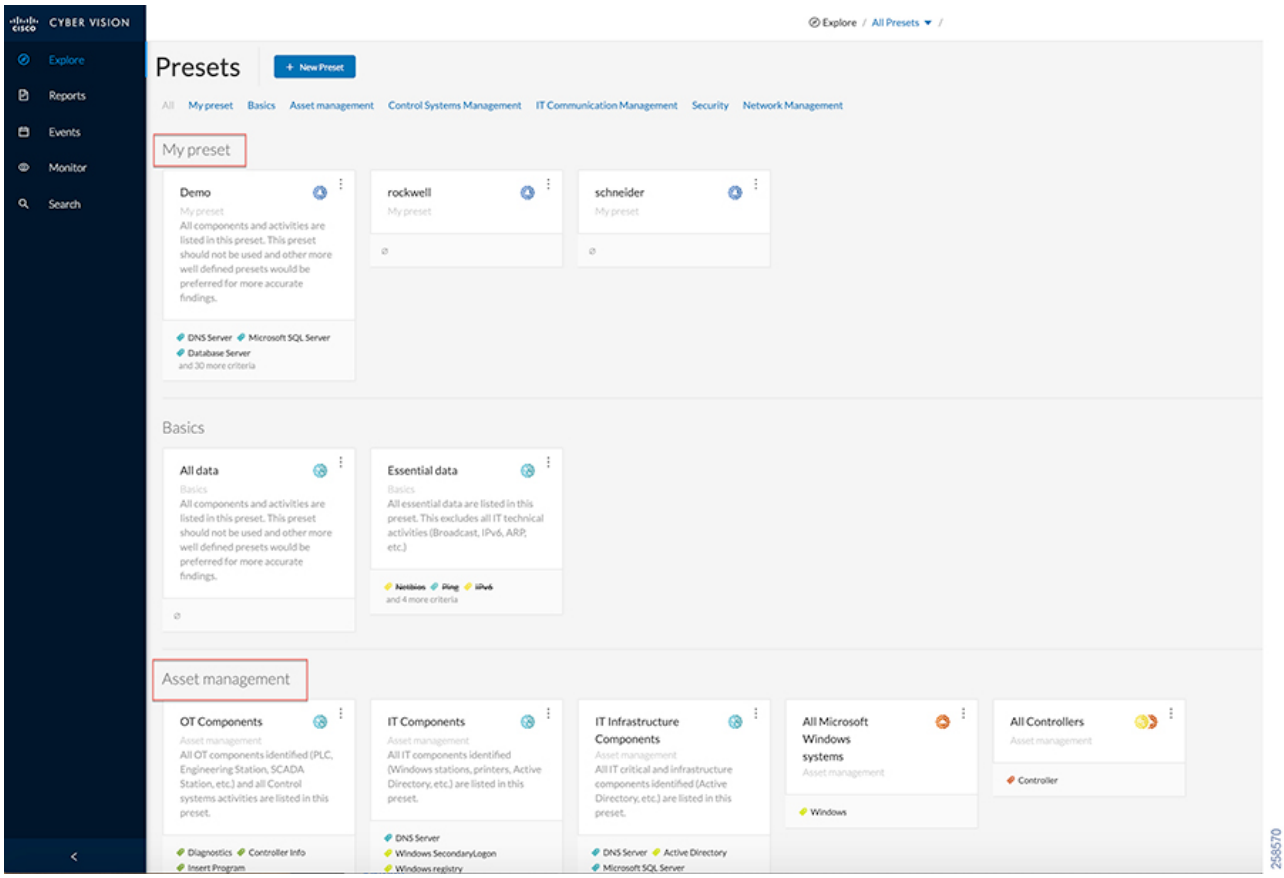
- ダイナミックインベントリ：Cisco Cyber Vision Center は、工場フロア上のすべての IACS デバイスのダイナミックインベントリを生成します。アクティブディスカバリおよびパッシブディスカバリ で説明されているように、Cisco Cyber Vision Center は、工場フロアで行われているイベントを継続的にリッスンします。これにより、Cisco Cyber Vision Center は工場フロア内のデバイスのダイナミックインベントリを構築および更新できます。OT オペレータは、工場フロア上の現在のデバイスリストを取得するためにスキャンを実行する必要はありません。また、特定のデバイスがオフラインになった場合、Cisco Cyber Vision Center はそのリストをダイナミックに更新します。図 52 Cisco Cyber Vision Center がコンポーネントを表示する方法を示します。

図 52　Cisco Cyber Vision Center のダイナミック コンポーネント インベントリの表示



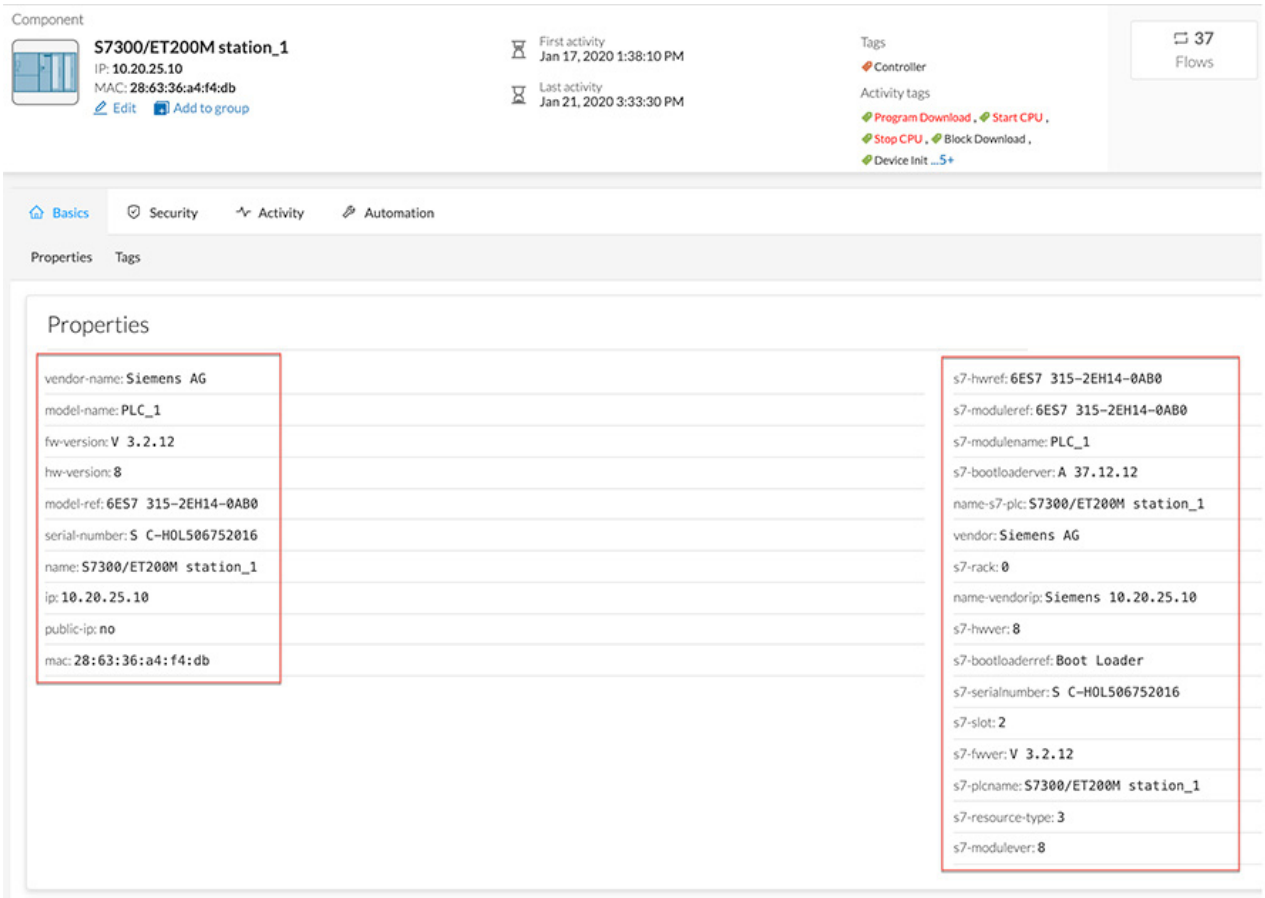
- 直感的なフィルタ：Cisco Cyber Vision Center は、OT オペレーターがデータを調べるのに役立つ、プリセットとしてラベル付けされた直感的なフィルタを提供します。たとえば、オペレーターは、OT コンポーネントまたはプロセス制御アクティビティの現在のリストを確認したい場合があります。Center は、オペレーターがカスタムフィルタを作成できるようにします。図 53 Cisco Cyber Vision Center で使用可能なプリセットのタイプを示しています。

図 53　Cisco Cyber Vision Center のプリセット



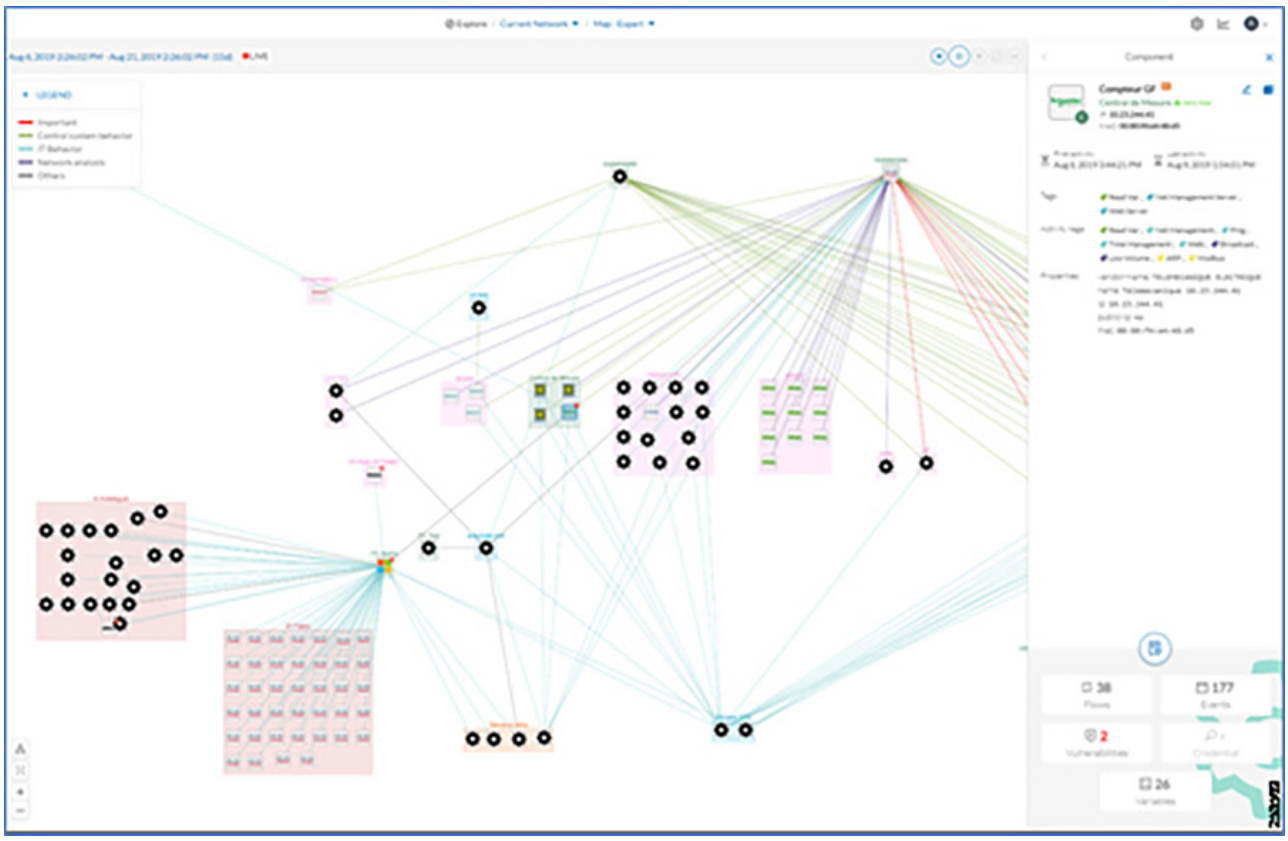
- IACS アセットの詳細情報：Cisco Cyber Vision ソリューションの大きな利点の 1 つは、IACS アセットに関する非常に詳細な情報を収集する機能です。図 54 Siemens コントローラに関する情報を表示します。

図 54　Siemens コントローラの詳細なアセット情報の例



- ダイナミックマッピング：Cisco Cyber Vision Center は、コンポーネントとそれらの間の通信フローを表示する非常に詳細なマップを提供します。図 55 Cisco Cyber Vision がネットワークマップを表示する方法を示しています。

図 55　Cisco Cyber Vision のネットワークマップ



- ベースライニング：Cisco Cyber Vision Center は、ベースライニングと呼ばれる機能をサポートしています。これにより、オペレーターは、監視する一連のコンポーネントを選択できます。ベースライニングが定義された後、オペレータは、この一連の要素に対して発生した変更を、異なるタイミングで比較することができます。

- 脆弱性管理：Cisco Cyber Vision Center は、IACS デバイスに存在する脆弱性を強調表示します。これにより、オペレーターはこれらの脆弱性を軽減することができます。

- レポート：Cisco Cyber Vision により、オペレーターは、インベントリ、アクティビティ、脆弱性、および PLC レポートなどのレポートを生成できます。

Cisco Cyber Vision Sensor

このガイドでは、アプリケーションとしてインストールされた Cisco Cyber Vision Sensor を備えた Cisco IC3000 がハードウェアセンサーとして導入されています。Cisco IC3000 は、管理イーサネットインターフェイス（int0）に加えて 4 つの物理インターフェイス（int1 in4）を持つことができる産業用 PC です。Cisco IC3000 がハードウェアセンサーとして導入されている場合、Cisco Cyber Vision Center に情報を転送するために管理インターフェイスが使用されます。4 つのインターフェイスがデータ収集に使用されます。Cisco IC3000 を使用して Cisco Cyber Vision Sensor を注文して導入するには、次の 2 つのオプションを使用できます。

- お客様は、既存の Cisco IC3000 があり、その Cisco IC3000 にアプリケーションとして Sensor のインストールを希望する場合があります。

- お客様は、アプリケーションとして Sensor アプリケーションが導入された新しい Cisco IC3000 を注文します。

両方のオプションがサポートされていますが、ほとんどの環境では、Sensor アプリケーション ソフトウェアがインストールされている Cisco IC3000 の導入が最も一般的です。Cisco Cyber Vision Sensor アプリケーションと一緒に注文された新しい Cisco IC3000 の設定に関する情報は、次の場所から入手できます。

- Cisco Cyber Vision Sensor のクイックスタートガイド
  https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco_Cyber_Vision_Sensor_Quickstart_Guide_Release_3_0_0.pdf

お客様が既存の Cisco IC3000 を持ち、Cisco Cyber Vision Sensor アプリケーションの導入を希望する場合、推奨される手順は、Cisco IC3000 の設定をリセットすることです。上記クイックスタートガイドの URL にある「Installing the Cyber Vision Sensor Application Using Local Manager after a Configuration Reset」の項の手順を参照してください。

展開の考慮事項

このセクションでは、産業用オートメーション環境に Cisco Cyber Vision ソリューションを導入する際に検討する必要がある、重要な設計上の考慮事項について説明します。Cisco Cyber Vision ソリューションでは、オフラインモードとオンラインモードの 2 つの導入モデルがサポートされています。

Cisco Cyber Vision のオフラインモード

Cisco Cyber Vision オフラインモードは、Cisco Cyber Vision Center が存在しない場合、または Cisco Cyber Vision Sensor と Cisco Cyber Vision Center との間にレイヤ 3 通信がない場合に、OT エンジニアによって導入されます。このような状況では、OT エンジニアはオフラインモードを使用できます。このモードでは、USB スティックを使用してデータパケットをキャプチャし、その後、Cisco Cyber Vision Center に手動でロードすることで、データパケットを分析します。このオプションは、コンセプト実証を実行するために、OT エンジニアによって使用されます。

Cisco Cyber Vision のオンラインモード

Cisco Cyber Vision のオンラインモードは、Cisco Cyber Vision Sensor と Center の間にレイヤ 3 接続があることを前提としています。このガイドでは、次の理由により、オンラインモードを使用することをお勧めします。

- オンラインモードでは、OT および IT オペレーションチームがリアルタイムで継続的にトラフィックの更新を確実に行うことができます。
- オフラインモードで説明されているような、データをキャプチャしてデータをアップロードする手動プロセスはありません。データは、Cisco Cyber Vision Center でリアルタイムにキャプチャされます。
- オフラインモードは、USB ディスクの使用可能なストレージ領域に依存し、データの長期的なストレージのソリューションとして使用することはできません。

図 56 Cisco Cyber Vision ソリューションがセル/エリアゾーンでオンラインモードで導入される方法を示しています。

図 56　セル/エリアゾーンでのオンラインモードによる導入

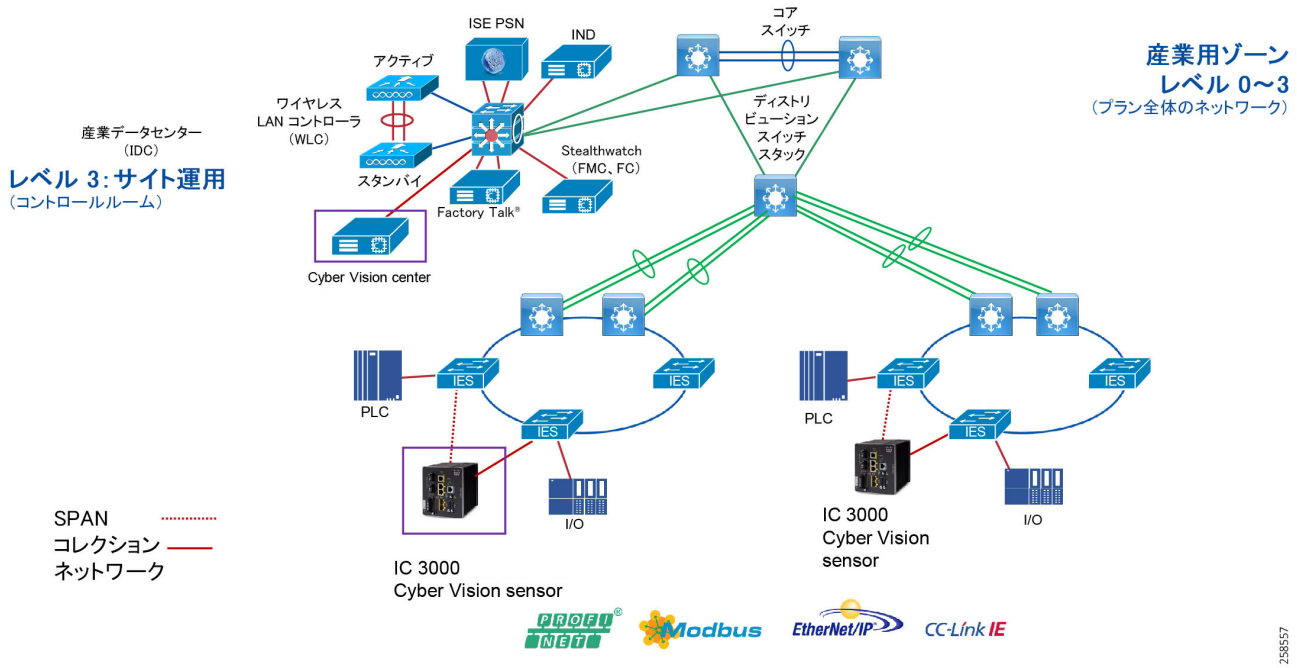


図 56 で説明されているように、Cisco Cyber Vision と一緒に導入された Cisco IC3000 には、コレクションインターフェイスとミラーインターフェイスという 2 つの異なるインターフェイスセットがあります。コレクションは、メタデータを Center に転送するために使用されるレイヤ 3 インターフェイスです。ミラーインターフェイスは、ネットワーク内の SPAN トラフィックを収集します。

パフォーマンス

Cisco IC3000 を導入するコントロールシステムエンジニアは、そのパフォーマンスの数値を考慮する必要があります。重要なパフォーマンスメトリクスは次のとおりです。

- 1 台の Cisco IC3000 でサポートされるフローの数は 15,000 です。
- 1 秒あたりのパケット数は 12,000 です。

ネットワーク内の Sensor の場所

ネットワーク内で Sensor の正しい場所を決定する際には、コントロールシステムエンジニアは注意する必要があります。Cisco Cyber Vision Sensor は、ディープパケット インスペクションを使用してトラフィックフローを分析します。推奨事項は次のとおりです。

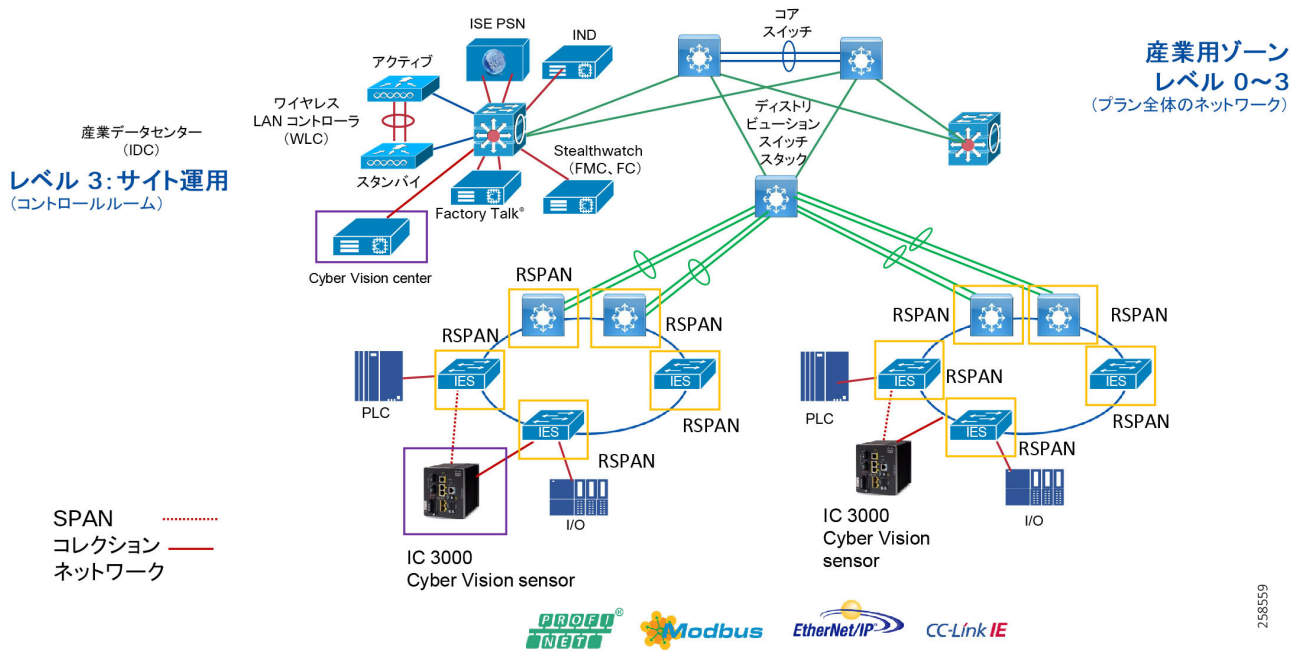
- Cisco IC3000 センサーで複数のモニタポートを使用する場合は、両方のポートが同じサブネットに属していることを確認します。図 56 で示されているように、2 つのリングの導入は異なるサブネットに属していて、そのシナリオでは、2 台の Cisco IC3000 を使用しています。
- 2 つのルーティングインターフェイスに属するトラフィックを同じ Cisco IC3000 に接続してはいけません。

キャプチャ ポイント

Cisco Cyber Vision ソリューションの有効性は、トラフィックを効果的にキャプチャすることに依存しているため、トラフィックをキャプチャする場所をどこに決定するかが重要です。たとえば、ネットワーク内の複数のスイッチに接続された多数の IACS デバイスがあり、それらすべてのデバイスからのトラフィックをモニタする場合は、次の 3 つの選択肢があります。

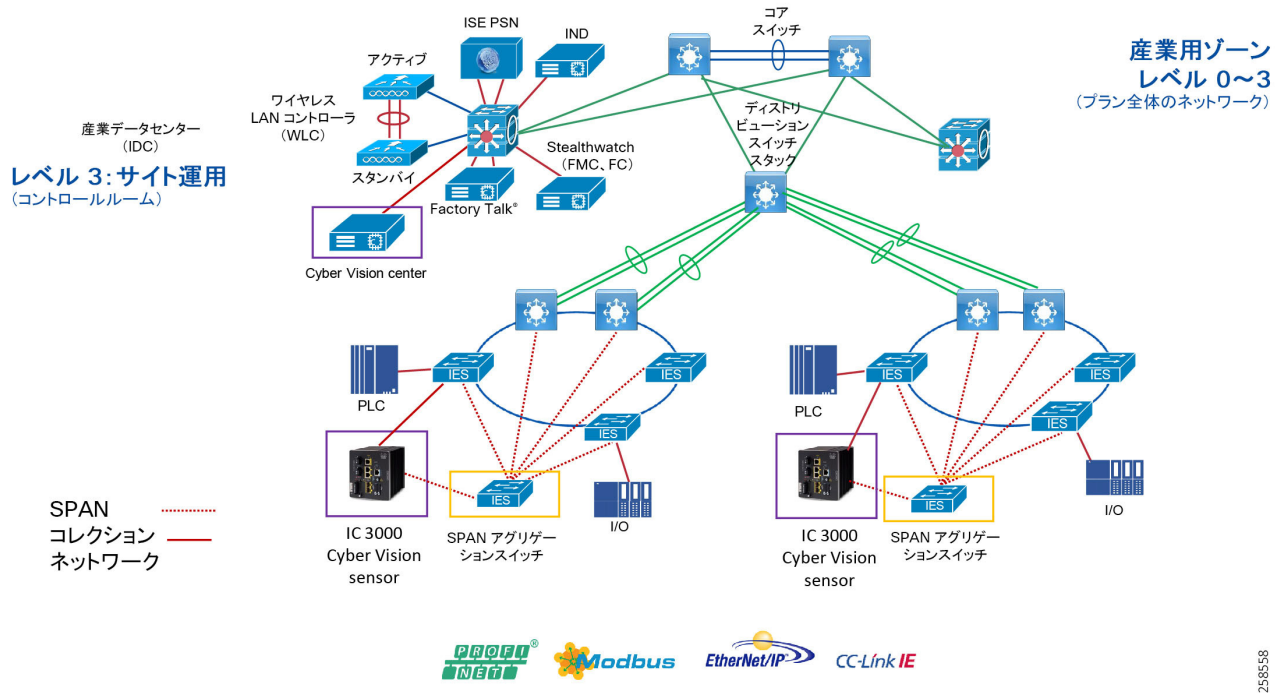
- すべてのスイッチで RSPAN を有効にします。
- モニタ対象の各スイッチで個々の SPAN を有効にし、それらを特定のスイッチに接続します。
- RSPAN は、そのスイッチから Cisco IC3000 センサーにトラフィックを送信し、トラフィックを選択的にモニタします。

図 57　すべてのスイッチで RSPAN を有効にする



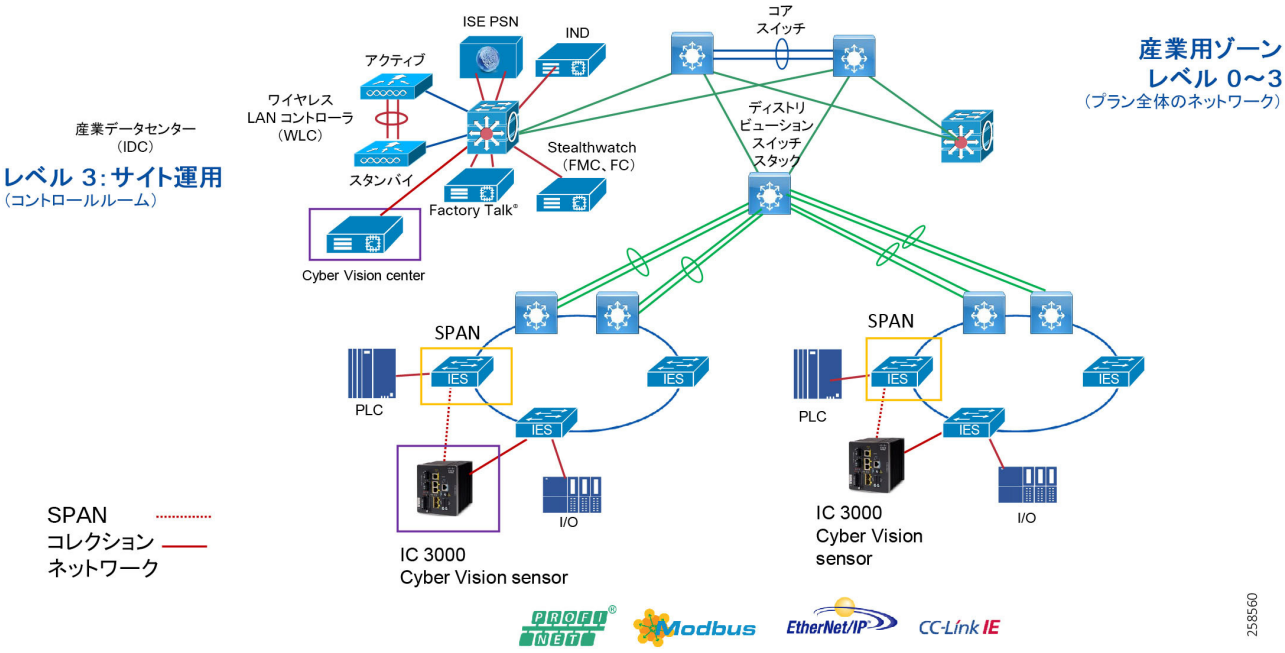
2 番目のオプションは、すべての SPAN トラフィックを SPAN アグリゲーションスイッチに集約してから、そのトラフィックを Cisco IC3000 センサーに転送することです。

図 58　モニタ対象スイッチの個々の RSPAN を有効にし、特定のスイッチに接続します。



3 番目のオプションは、選択ポイントで SPAN を有効にすることです。

図 59　選択ポイントでの SPAN の有効化



このガイドでは、次の理由により、最初に 3 番目のオプションを使用することを推奨します。

- 工場フロアの最も重要なトラフィックは、PLC から工場フロアの他のデバイスへの通信です。
- ほとんどのセキュリティ攻撃は、PLC の脆弱性をエクスプロイトすることから開始されます。
- すべてのデバイスをモニタする強い必要性がある場合は、2 番目のオプションが導入のためのより良い選択です。

Industrial Network Director（IND）

Cisco IND は、簡単に統合できるネットワーク管理製品であり、OT チームはネットワーク モニタリングとトラブルシューティングを合理化できるため、オペレータと技術者の生産性が向上します。Cisco IND はシスコの包括的な IoT ソリューションの一部です。

- シスコの IE スイッチの全機能を活用して、IT 部門外の運用担当者がネットワークを利用できるようにする、産業用アプリケーション向けに特化された使いやすいネットワーク管理システムです。
- 産業用プロトコル（CIP、PROFINET）を介した検出により、オートメーションおよびネットワーキングアセット の動的な統合トポロジを作成し、OT 担当者と IT 担当者に共通のフレームワークを提供します。これにより、ネットワークのモニタリングとトラブルシューティングが可能になり、計画外のダウンタイムから速やかに回復できるようになります。また、デバイス ディスカバリは、接続されている産業用デバイス（PLC、I/O、ドライブ、HMI など）のコンテキストの詳細も提供します。
- リッチ API により、既存の産業用アセット管理システムにネットワーク情報を簡単に統合できます。また、顧客やシステムインテグレータは、モニタリングとアカウンティングに関する特定のニーズに合わせてカスタマイズされたダッシュボードを作成できます。

詳細については、次の付録および項を参照してください。
https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/industrial-network-director/datasheet-c78-737848.pdf

Cisco Identity Services Engine

Cisco ISE は、ネットワークにアクセスしているデバイスの可視性を提供するのに役に立ちます。IT セキュリティプロフェッショナルは、Cisco ISE を使用して、ネットワーク全体の広範にわたって一貫したセキュリティポリシーを作成し、ネットワークへのアクセスを必要とするユーザと資産のためのポリシーエンジンを実現できます。ISE は、pxGrid を介してパートナー プラットフォームとユーザ、デバイス、およびネットワークの詳細を共有するため、他のプラットフォームでセキュリティポリシーを強化できます。たとえば、Cisco Cyber Vision は、セキュリティの可視性とコンテキストを強化するために、pxGrid を介して他のプラットフォームから情報を取り込むこともできます。Cisco Cyber Vision は、pxGrid と通信して、プロファイリングコンテキストの検出されたデバイスの詳細を共有できます。Cisco ISE は、ネットワークアクセスを動的に制御することでリスクを軽減し、脅威を封じ込めることもできます。Cisco ISE の詳細については、以下の『Cisco ISE Overview』を参照してください。
https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html#~stickynav=1

Stealthwatch

Cisco Stealthwatch は、ネットワーク可視性とセキュリティ分析によって脅威に対する防御を向上させます。Cisco Stealthwatch は、膨大な量のデータを収集して分析し、きわめて大規模で動的なネットワークさえも内部を包括的に可視化して保護します。また、セキュリティ運用チームが迅速かつ効果的に脅威に対応できるよう、拡張ネットワーク上のすべてのユーザ、デバイス、およびトラフィックの状況をリアルタイムで認識できるようにします。Stealthwatch では、ルータ、スイッチ、ファイア ウォール、プロキシ サーバ、エンドポイント、その他のネットワークデバイスなどの既存のインフラストラクチャから収集される NetFlow、IPFIX、その他のフロー データが活用されます。収集されたデータが分析され、ネットワークアクティビティの全容が示されます。

ネットワーク全体で進行する内容のすべてを詳細に把握することで、組織の規模や種類にかかわりなく、当該環境の標準的なふるまいをベースラインとしてすぐに設定することができます。このような情報により、不審な活動をより容易に特定できます。

産業工場への導入のユースケースは、次のとおりです。

- 拡張ネットワークの継続的なモニタリング
- 脅威のリアルタイム検出
- インシデント対応と調査の迅速化

- ネットワーク セグメンテーションの簡素化
- 法規制遵守要件への対応
- ネットワークのパフォーマンスおよびキャパシティプランニングの改善

詳細については、次のドキュメントを参照してください。
https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/at-a-glance-c45-736510.pdf

セル/エリアゾーンのセキュリティ設計の考慮事項

産業ゾーンは、セル/エリアゾーン（レベル 0 ～ 2）とサイト運用（レベル 3）のアクティビティで構成されます。工場全体の産業運用のモニタリングと制御に欠かせないすべての IACS アプリケーション、アセット、およびコントローラが産業ゾーンにあるため、このゾーンは重要です。スムーズな産業運用と IACS アプリケーションや IACS ネットワークの機能を維持するため、このゾーンでは、レベル 4 および 5 の企業運用からの明確かつ論理的なセグメンテーションと保護が必要とされます。

セル/エリアゾーンは、IACS アセットが互いにやり取りする機能的なゾーンです。すべての IACS アセットが通信して産業運用の要件が満たされた状態を確保する必要があるため、産業用ネットワークはセル/エリアゾーンのクリティカルな要素です。工場全体のアーキテクチャは、1 つまたは複数のセル/エリアゾーンを持つ場合があります。各セル/エリアゾーンは、同じネットワーク トポロジまたは異なるネットワーク トポロジを持つことができます。このガイドでは、その目的のために、設計、テスト、および検証用にリング トポロジ（図 60 を参照）が選択されました。これは、リング トポロジ設計で復元力が提供されるためです。

図 60　産業用オートメーション セル/エリアゾーンのネットワーク セキュリティ

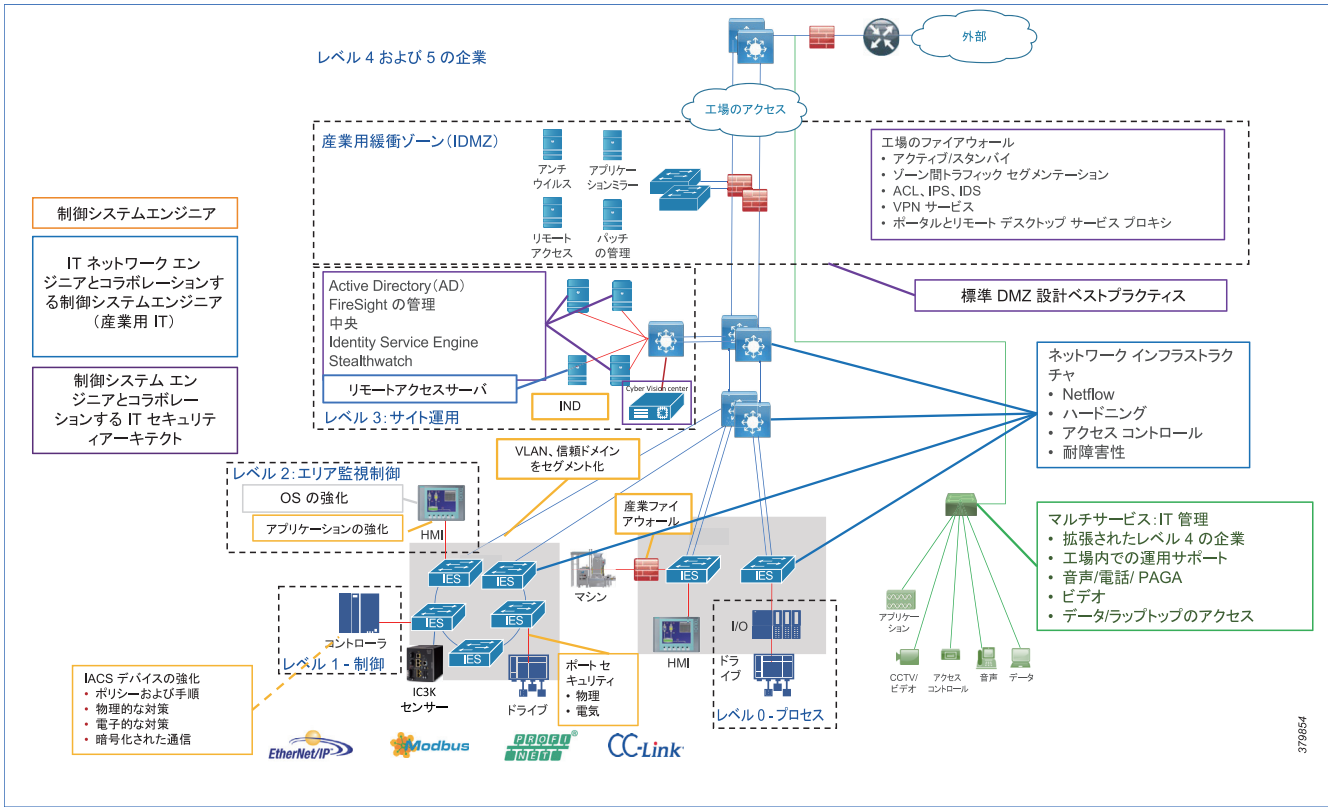


図 60 次のコンポーネントが次の位置に導入されています。

- ISE は分散設計に導入されます。ポリシーサービス ノード（PSN）はレベル 3 サイト運用に導入され、ISE プライマリ管理ノード（PAN）およびプライマリ モニタリング ノード（MnT）は企業ゾーンに導入されます。

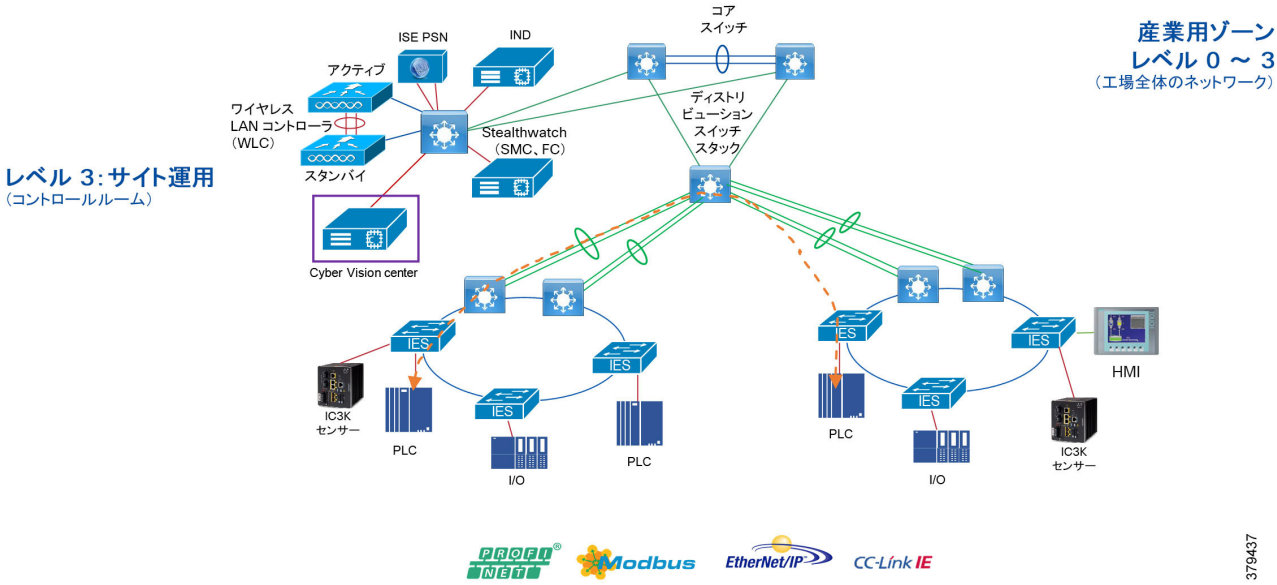
- VLAN、NetFlow、スパニングトラフィック、セキュアグループのタグ付け、動的なセキュリティ グループ アクセス コントロール リスト、および Cyber Vision Sensors をサポートする強化されたネットワーク インフラストラクチャ。
- Stealthwatch：フロー コレクタ（FC）と Stelathwatch 管理コンソール（SMC）は、レベル 3 サイト運用に導入されます。
- Cisco Cyber Visionは、レベル 3 サイト運用に導入されます。

次のセクションでは、産業用オートメーション ネットワーク セキュリティ ソリューションを導入する際に OT 制御システム エンジニアと IT セキュリティアーキテクトが検討する必要のある設計上の考慮事項について説明します。この設計上の考慮事項は、セグメンテーションの仕組みとさまざまなアプローチを理解するとともに、この設計のアプローチが選択された理由を理解する上で重要です。

ネットワークの IACS トラフィックフロー

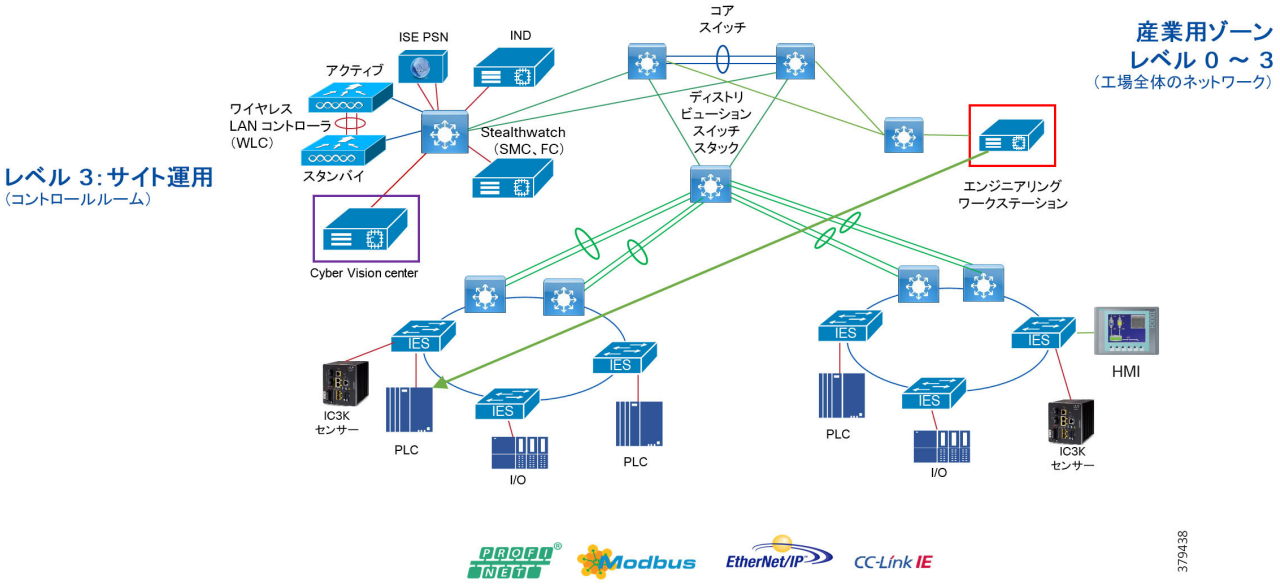
ネットワーク内のピアツーピア IACS デバイス間の水平通信は、「East-West（水平方向）通信」と呼ばれます。図 61 工場全体のアーキテクチャでの East-West（水平方向）通信を示しています。工場フロアの運用では、ピアツーピア通信は、相互にインターロック機能が有効になっているデバイス間で行われます。インターロックは、2 つのメカニズムの状態が通常相互に依存するようにする機能です。たとえば、ある機器の起動が許可される前にいくつかのプロセス条件が満たされる必要があり、これらのプロセスが異なるセル/エリアゾーンにある場合は、機器が起動するために、これらのプロセス間でピアツーピア通信が行われる必要があります。

図 61　セル/エリアゾーンの East-West（水平方向）トラフィックフロー



レベル 3 サイト運用、IDMZ、または企業ゾーン内のサーバまたはその他のデバイスがセル/エリアゾーン内の IACS と通信できるようにすることを、「North-South（垂直方向）通信」と呼びます。図 62 では、エンジニアリング ワークステーション（EWS）がセル/エリアゾーンのコントローラにアクセスしており、この通信フローが North-South（垂直方向）通信として定義されています。

図 62　工場全体のネットワークのNorth-South（垂直方向）通信



セル/エリアゾーンのセグメンテーション

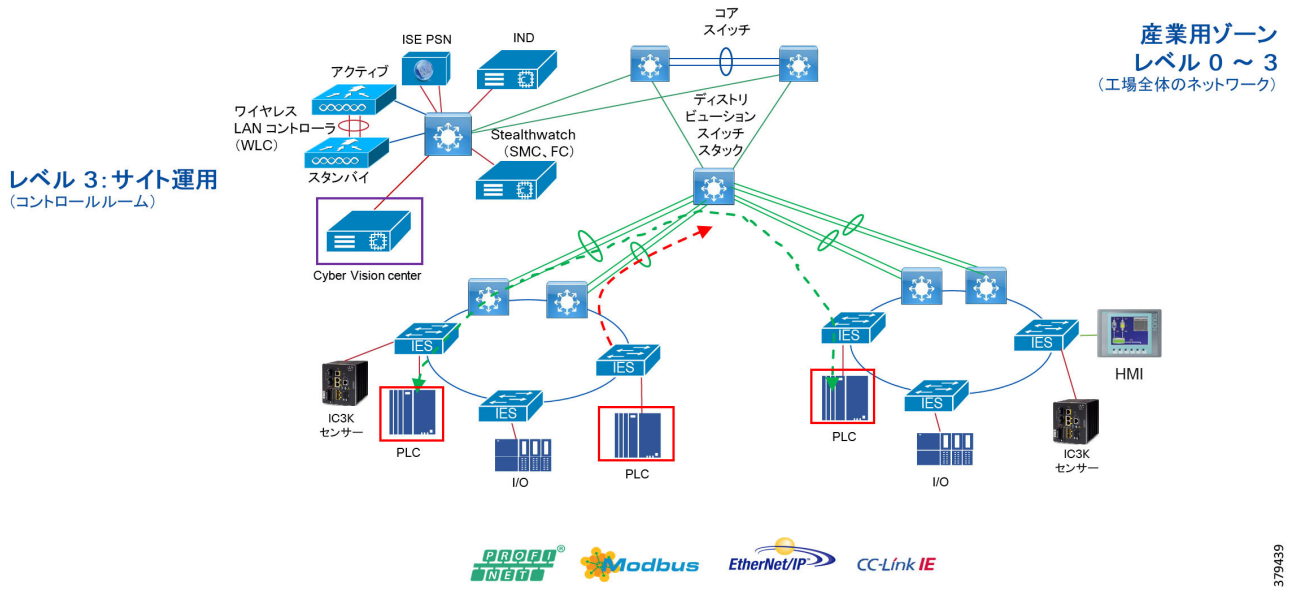
IT セキュリティ アーキテクトは、制御システム エンジニアと連携して、IACS ネットワークで許可する必要がある East-West（水平方向）および North-South（垂直方向）通信フローを指定するアクセスポリシーを設計する必要があります。IACS ネットワークでは、すべての IACS アセットがすべての IACS アセットと通信することを許可するオープンポリシーは便利ですが、そのアプローチは、サイバー脅威が伝播するリスクを高めます。一方で、特定の IACS は異なるセル/エリアゾーンに存在する他の IACS にアクセスする必要があるため、セル/エリアゾーン間の通信を許可しない制限的なポリシーを実装することも非生産的です。特定のシナリオの正確な要件は現在の IACS アプリケーションの要件に基づいているため、すべての導入に対して機能するポリシーを指定することは不可能です。そのため、この産業用オートメーション ネットワークセキュリティ CVD には、さまざまな環境での使用に合わせてカスタマイズできるアクセスポリシーの例が示されています。

IACS ネットワークのアクセスポリシーに関する前提条件：

- セル/エリアゾーン内のすべてのトラフィックは、暗黙的に許可されます。これは、IACS のグループが互いに通信する必要があり、そのためにセル/エリアゾーンのどのIESにも強制設定が適用されないことが想定されているためです。
- 2 つの異なるセル/エリアゾーン間のすべてのトラフィックがポリシングされます。たとえば、図 63 では、あるセル/エリアゾーンの Controller_A は別のセル/エリアゾーンの Controller_C へのアクセスが許可されますが、Controller_B は Controller_C へのアクセスが許可されません。

以下のいくつかのサブセクションでは、セグメンテーションの一般的な考え方、さまざまなタイプのセグメンテーション、およびセグメンテーション手法を選択することの長所と短所について説明します。

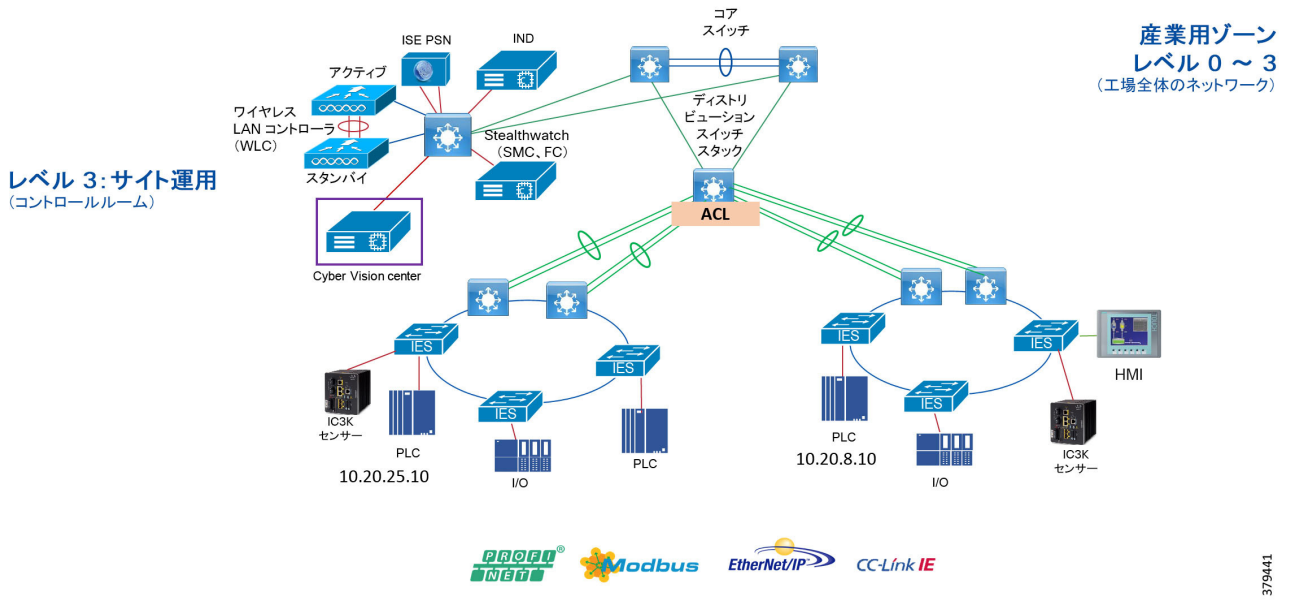
図 63　East-West（水平方向）トラフィックフローでの適用例



レイヤ3アクセスコントロールリスト（ACL）を使用したセグメンテーション

IACS アセットで MAC 認証バイパス（MAB）が設定されておらず、ISE からダウンロード可能アクセス制御リスト（dACL）を取得できない場合は、異なるセル/エリアゾーンを接続しているディストリビューション スイッチで静的 ACL を使用します。図 64 では、2 つのセル/エリアゾーンを接続しているディストリビューション スイッチで ACL が適用されます。図 64 では、Controller-A が Controller-B との通信を確立できるように、ACL によって 10.20.25.10 と 10.20.8.10 の間の通信が許可される必要があります。

図 64　レイヤ 3 ACL を使用したセグメンテーション

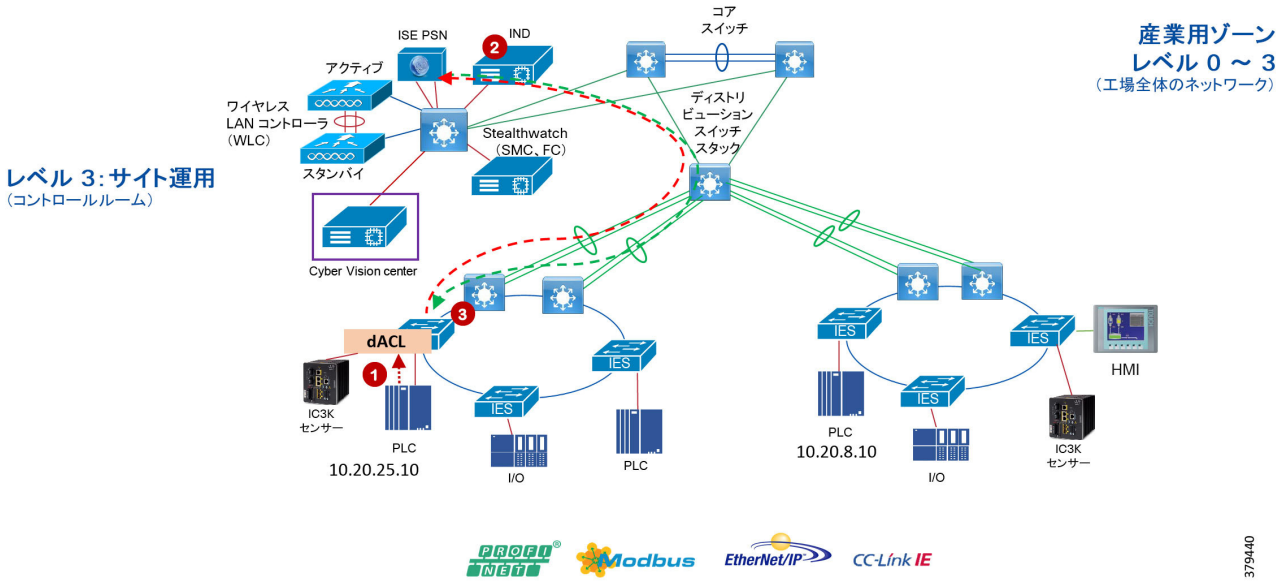


ACL を管理する上記の手法には、dACL と同様の欠点があります。コントローラの IP アドレスが変更されるか、別の場所に移動されるたびに、ACL を更新する必要があります。古いエントリを消去し、新しいエントリを追加する必要があります。このプロセスは負担の大きなものとなる場合があり、IT セキュリティアーキテクトのミスにつながる可能性があります。

ダウンロード可能アクセス制御リスト（dACL）を使用したセグメンテーション

セグメンテーションは、ネットワーク内の既知および未知のリスクから IACS ネットワークを保護するために、IACS ネットワークをゾーン分割して、より小規模な信頼のドメインを作成することを実践します。ここでは、dACL を使用したセグメンテーションの最初のアプローチについて説明します。IACS アセットがネットワークに接続されるときにデバイスで dACL がプロビジョニングされる仕組みが示されている図 65 を参照してください。図 65 には、ディストリビューション スイッチを介して接続された 2 つのセル/エリアゾーンがあります。また、Cell/Area Zone -1 の Controller-A（10.20.25.10）と Cell/Area Zone -2 の Controller-B（10.20.8.10）の 2 つのコントローラがあります。

図 65　dACL を使用したセグメンテーション



- コントローラは IES のアクセス ポートに接続し、そのアクセス ポートが 802.1X MAB 認証要求を Cisco ISE に送信します。
- Cisco ISE は、要求を受信すると、設定された認証および許可ポリシーを使用して要求を処理し、許可の結果を dACL としてディストリビューション レイヤ スイッチに送信します。
- コントローラ A に設定されている dACL は、その通信を制限します。新しいコントロールを適用する必要がある場合は、dACL にエントリを追加します。

dACL には、どの IP アドレスがどの IP アドレスと通信できるかを指定するアクセス制御エントリ（ACE）が必要です。図 65 で、IP アドレス 10.20.25.10 の Controller-A が IP アドレス 10.20.8.10 の Controller-B との通信を許可される場合、ACE には 10.20.25.10 から 10.20.8.10 への許可ステートメントが必要です。

上記の手法では、セル/エリアゾーンへのアクセスの制御と、セル/エリアゾーン間のアクセスの制御にも使用できます。しかし、この手法には次の欠点があります。

- Controller-A と Controller-B の間の通信が許可されることが前提となっています。Controller-B が別の IP アドレスを持つ新しい位置に移動した場合は、dACL が更新される必要があります。
- Controller-A が産業ゾーンの特定のサーバとの通信を許可される場合、サーバの IP アドレスが変更されると、dACL が再び更新される必要があります。
- 大規模な dACL がある場合は、ディストリビューション スイッチのパフォーマンスが低下する可能性があります。

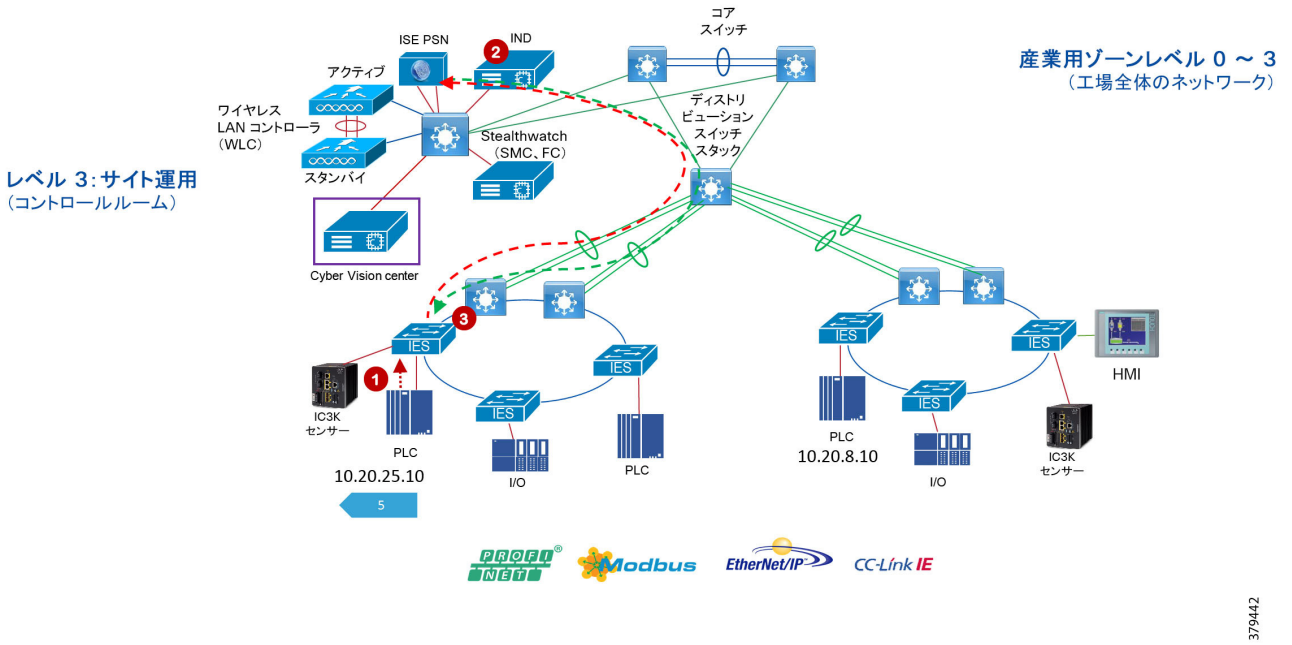
TrustSec テクノロジーを使用したセル/エリアゾーン セグメンテーション

Cisco TrustSec テクノロジーでは、IACS 、ネットワーク デバイス、およびユーザがネットワークに接続すると、それらに SGT が割り当てられます。これらのタグを使用することにより、IT セキュリティ アーキテクトは、アクセスポリシーを定義し、そのポリシーを任意のネットワーク デバイスに適用することができます。

Cisco TrustSec は、分類、伝達、および適用の 3 つのフェーズで定義されます。ユーザや IACS アセットがネットワークに接続すると、ネットワークはそれらに「分類」と呼ばれるプロセスで特定の SGT を割り当てます。分類は認証および許可ポリシーの結果に基づいて実行できます。たとえば、IACS アセットがコントローラ、I/O、HMI、または Windows ワークステーションである場合、IACS アセットを分類して特定のタグを割り当てることができます。IACS アセット タイプに応じて、個別のタグを IACS アセットに割り当てることができます。図 66 コントローラに SGT 値 5 がどのように割り当てられるかを示しています。SGT 割り当てのプロセスは、IACS アセットが IES に接続されるときに dACL がシスコのディストリビューション スイッチにプッシュされる方法と似ています。唯一の違いは、dACL の代わりに SGT 値が割り当てられることです。図 66 に示されているように、Controller-A が IES に接続すると、IES は ISE による 802.1X 認証および許可を行い、その結果として IACS アセットにタグが割り当てられます。

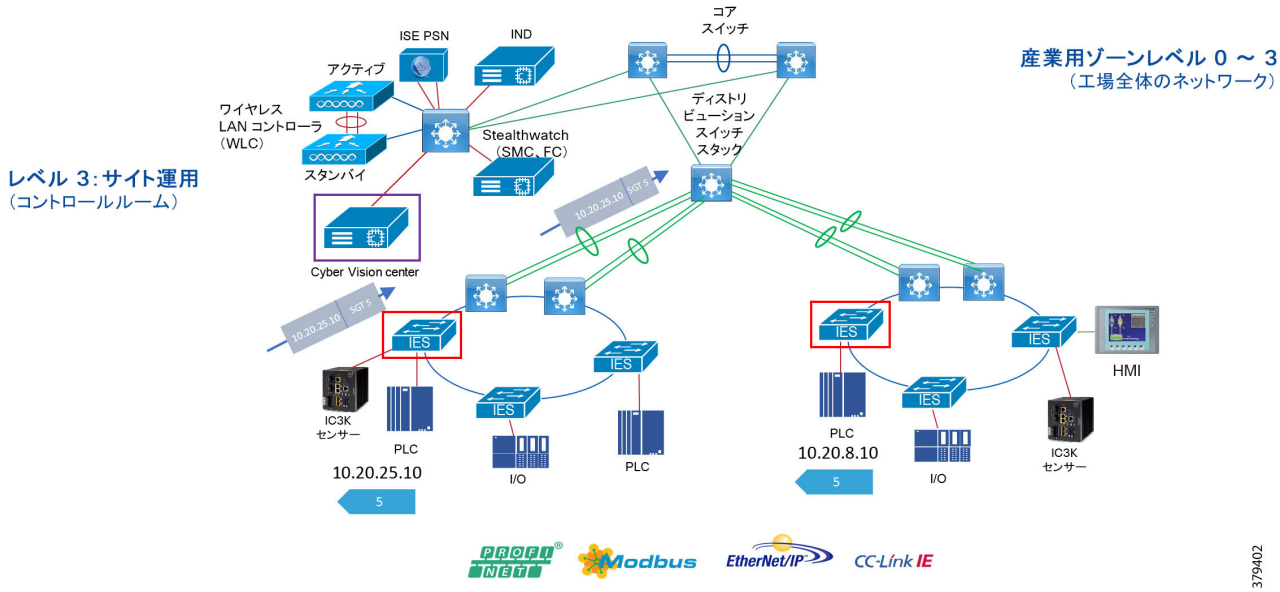
TrustSec にはスタティック Acl と Dacl よりも利点があります。ACL 方式は管理が困難であり、導入時にエラーが発生することがあります。また、ACL のサイズが非常に大規模になると、ディストリビューション スイッチのパフォーマンスが低下する可能性があります。最後に、両方の ACL 方式では、IP アドレスの変更による更新が必要です。

図 66　Cisco TrustSec デバイスの分類



TrustSec の次のフェーズは「伝達」です。このフェーズでは、イーサネットフレームの SGT タグが、あるスイッチまたはルータから別のデバイスに送信されます。IACS アセットに割り当てられた SGT タグは、IACS アセットによって生成されるすべてのパケットとともに伝達される必要があります。図 67 SGT が挿入されたフレームがネットワークでどのように伝達されるかを示しています。図 67 では、Controller-A は、IP アドレスが 10.20.25.10 で、SGT 値 5 が割り当てられます。イーサネットフレームが Controller-A によって生成されると、IES は SGT 値 5 を IP アドレスとともに挿入し、それを次のスイッチに送信します。次のスイッチで SGT インラインタギングが設定されていれば、同じフレームが次のスイッチに伝達され、この情報はホップバイホップ方式で宛先に転送されます。

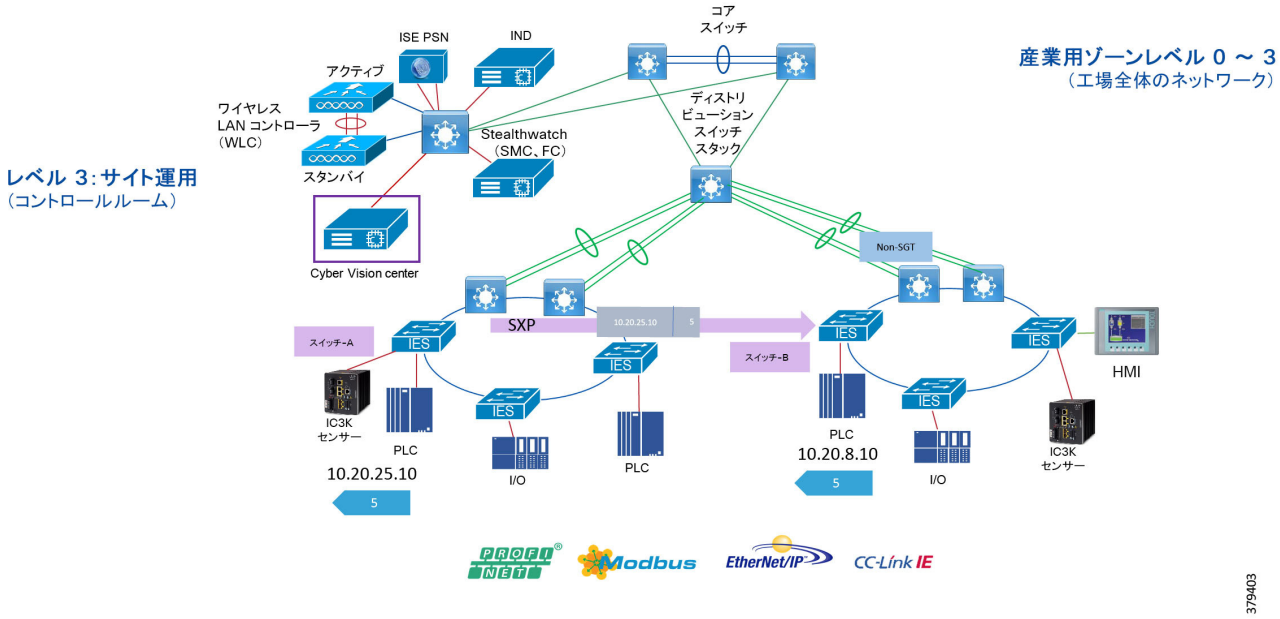
図 67　Cisco TrustSec の SGT 伝達



前のフェーズでは、「インラインタギング」と呼ばれる方式による伝達のシナリオについて説明しました。ただし、特定のネットワーク トポロジには、送信元から宛先へのパスのスイッチでインラインタギングがサポートされないシナリオが存在する場合があります。そのようなシナリオが発生すると、非 SGT 対応スイッチは、フレーム内の SGT を無視し、通常のイーサネットフレームを発信インターフェイスに送信します。つまり、インライン タギング機能を使用するには、パス内のすべてのスイッチがこの機能をサポートしている必要があります。

この問題を回避するために、Cisco TrustSec は、SGT Exchange Protocol（SXP）を使用して SGT に対応していない IE（たとえば、Cisco IE 2000）が存在する場合に、パスを介して SGT フレームを転送するための異なるメカニズムもサポートしています。SXP は、SGT から IP アドレスへのマッピングを安全に共有するために使用されます。図 68 SGT の動作を示します。図 68 では、Controller-A が SGT タグ値 5 を使用して Controller-B との通信を確立しています。パスには非 SGT デバイスが存在し、このスイッチはディストリビューション スイッチから送信される フレーム内の SGT 値を無視します。SGT 情報を Switch-B に送信するには、Switch-A と Switch-B の間に SXP トンネルが必要です。このトンネルによってバインディング情報（SGT 5 にマッピングされた 10.20.25.10）が伝送されます。

図 68　SXP トンネルを使用した Cisco TrustSec の SGT 伝達



Cisco TrustSec の 3 つ目のステージは「ポリシーの適用」です。適用デバイスは、タグ情報に基づいてトラフィックを制御します。シスコのファイアウォール、ルータ、またはスイッチを TrustSec の適用ポイントとすることができます。適用デバイスは送信元 SGT を取得し、それを宛先 SGT と比較して、トラフィックを許可するか拒否するかを決定します。Cisco TrustSec の利点は、送信元と宛先の間にあるスイッチ、ルータ、またはファイアウォールでポリシーを適用できることですが、重要な要件として、適用ポイントが宛先 IP アドレスをタグ値にマッピングできる必要があります。このプロセスの詳細は、図 69 に示されています。このシナリオでは、Controller-A に SGT 値 5 が割り当てられ、同様のデバイス タイプの Controller-B にも SGT 値 5 が割り当てられます。I/O デバイスはデバイス タイプが異なるため、異なるタグ値が割り当てられます。このシナリオでは、Controller-A は Controller-C との通信の確立が許可されます。ただし、I/O デバイスは Controller-C との通信の確立が許可されません。このアクセスポリシーを表 33 に示します。

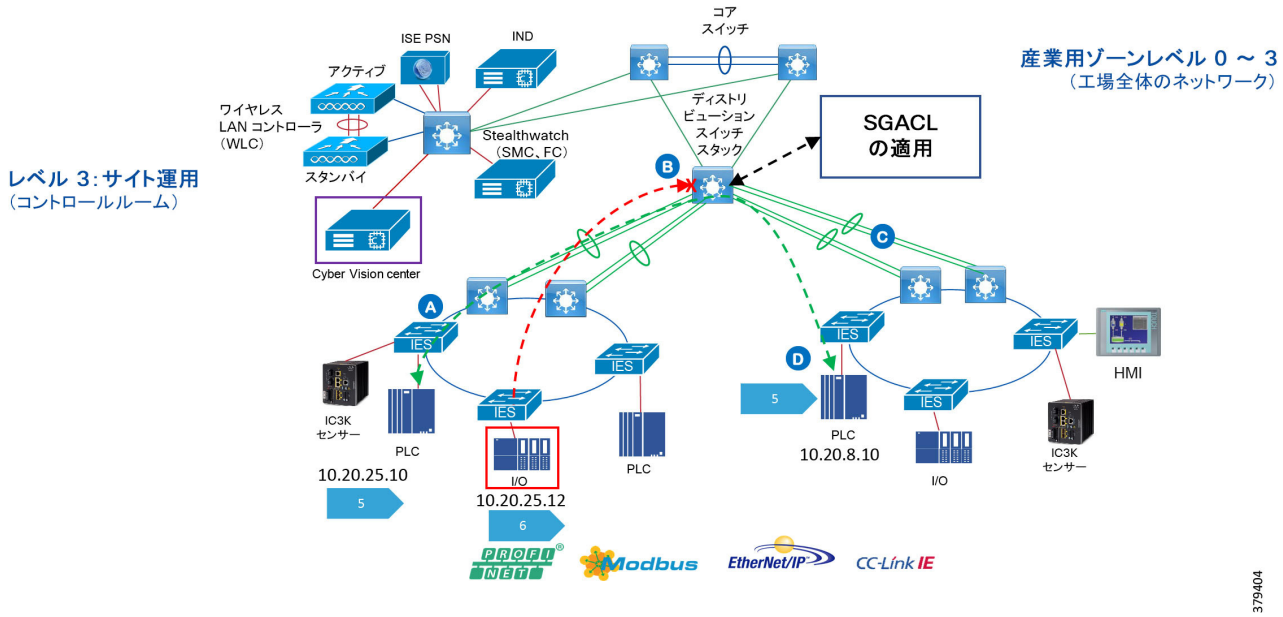
表 33　アクセスポリシーの例

	SGT 5	SGT 6
SGT 5	可	不可
SGT 6	不可	不可

次のステップは、ポリシーが適用される場所を決定することです。図 69 に示されているように、適用は、スイッチ A、B、C、または D で行うことができます。ただし、前述のように、スイッチがポリシーを適用するには、宛先 IP アドレスからタグ値を取得できる必要があります。たとえば、ポイント A では、10.20.25.10, 5から 10.20.8.10, 5 と 10.20.25.12,6 から 10.20.8.10,5 の 2 つのフローが発生します。ポイント A でアクセスポリシーが適用されている場合、スイッチは送信元タグを認識できるだけで、宛先 IP アドレスからタグへのマッピングに関する情報は持っていません。つまり、スイッチ A は、宛先 IP アドレスが 10.20.8.10 であることを認識しますが、10.20.8.10 がタグ値 5 にマッピングされる（つまり、許可される必要がある）という情報を持っていません。ポイント B でポリシーが適用される場合も同じ動作が見られます。ポイント C またはポイント D でポリシーが適用される場合は、そのポリシーが機能します。これは、スイッチ C（レイヤ 2 でスイッチ D に隣接）とスイッチ D（Controller-C に直接接続）の両方が、宛先 IP とそれに関連付けられた SGT 値の間の関連付けを取得できるため、ポリシーを正しく適用できるからです。

IACS アセットに最も近いポイントでアクセスポリシーを適用することが推奨されますが、場合によっては、別のポイントでポリシーを適用する必要があります。ただし、SGT と IP アドレスのマッピングは、IACS のローカルスイッチを超えて失われます。この問題を回避するには、IACS アセットが接続されている IES への SXP トンネルを確立します。SXP を使用したマッピング情報の取得の詳細については、以下で説明します。

図 69　アクセス ポリシーの適用例



TrustSec ネットワークポリシーの適用

次に、IT セキュリティアーキテクトは、設計のどこでアクセスポリシーを適用する必要があるのかを判断する必要があります。ポリシーの適用はディストリビューション スイッチで行われ、設計の選択ごとに長所と短所があります。たとえば、セル/エリアゾーンにある IES でポリシーが適用されるとします。前のセクションで説明したように、基本的な前提は、セル/エリアゾーン内のすべての IACS アセットが他のすべての IACS アセットにアクセスできる必要があるということです。2 つ目の前提は、セル/エリアゾーンを横断する East-West（水平方向）通信にポリシーが適用されることです。たとえば、Cell/Area Zone-1 と Cell/Area Zone-2 の 2 つのセル/エリアゾーンがあり、それぞれのセル/エリアゾーンに PAC と I/O デバイスが含まれているとします。Cell/Area Zone-1 のゾーン内ポリシーの観点からは、Cell/Area Zone-1 内のすべての PAC と I/O は互いにアクセスできる必要があります。セル/エリアゾーン間セキュリティ アクセス ポリシーにより、Cell/Area Zone-1 の I/O と Cell/Area Zone-2 の PAC の間の通信がブロックされます。このセキュリティ アクセス ポリシーを表 34 に示します。

表 34　ネットワーク ポリシー マトリクスの例

	PAC-Cell/Area-1	I/O-Cell/Area-1	PAC-Cell/Area-2	I/O-Cell/Area-2
PAC-Cell/Area-1	可	可	不可	不可
I/O-Cell/Area-1	可	可	不可	不可
PAC-Cell/Area-2	不可	不可	可	可
I/O-Cell/Area-2	不可	不可	可	可

TrustSec を使用してセキュリティポリシーを設計するときは、各 IACS アセットをタグに関連付けます。タグ 10 を持つ PAC とタグ 20 を持つ I/O デバイスの例では、次の 2 つのポリシーテーブルが必要です。1) Intra_Cell/Area Zone と 2) Inter_Cell/Area Zone。

表 35　Intra_Cell/Area Zone アクセスポリシーの適用の例

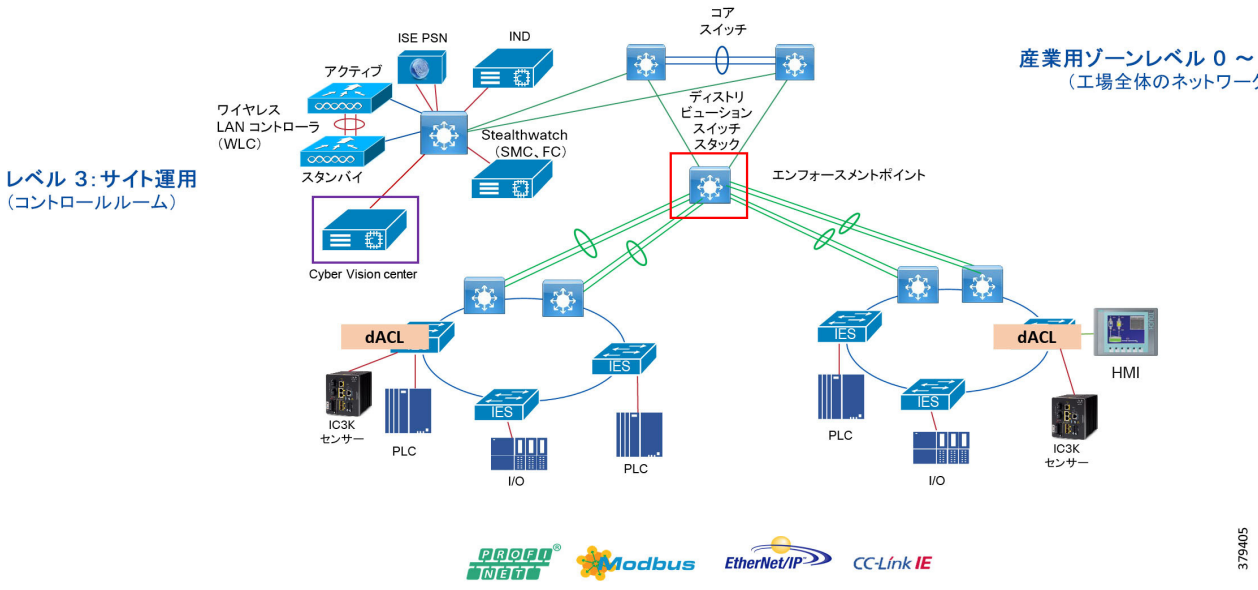
	10	20
10	可	可
20	可	可

表 36　Intra_Cell/Area Zone アクセスポリシーの適用

	10	20
10	不可	不可
20	不可	不可

上記のように、セル/エリアゾーン IES には 2 つのテーブルを実装する必要があり、現在の設計では不可能です。現在の TrustSec のポリシー適用では、単一のマトリックスだけがサポートされています。両方の目的を確実に達成するために、ディストリビューション スイッチにセキュリティ アクセス ポリシーを実装し、セル/エリアゾーンの IES には何も適用しないでください。セル/エリアゾーンの IES にポリシーが適用されない場合はセル/エリアゾーンの IES 上のすべての IACS アセッが互いに通信できるため、これにより、表 35 と表 36 のポリシー要件が満たされます。図 69 がディストリビューション スイッチに実装されると、セル/エリアゾーン間の通信または East-West（水平方向）通信が制限される可能性があります。図 70 セル/エリアゾーン間のセキュリティ アクセス ポリシーの適用ポイントを示します。産業用セキュリティ アクセス ポリシーでセル/エリアゾーン内のアクセス制御が必要である場合、この CVD では、ODVA, Inc. の CIP Security などの IACS アプリケーション セキュリティの使用を推奨しています。

図 70　産業用オートメーション ネットワーク セキュリティの適用ポイント



Scalable Group Tag Exchange Protocol の考慮事項

Scalable Group Tag Exchange Protocol（SXP）を使用すると、TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝達できます。SXP は、ある SGT 対応ネットワーク デバイスから別のデバイスに IP アドレスとともにエンドポイントの SGT を転送するために使用されます。SXP が転送するデータは、IP-SGT マッピングと呼ばれます。エンドポイントが属する SGT は静的または動的に割り当てることができ、SGT はネットワークポリシーで分類子として使用できます。

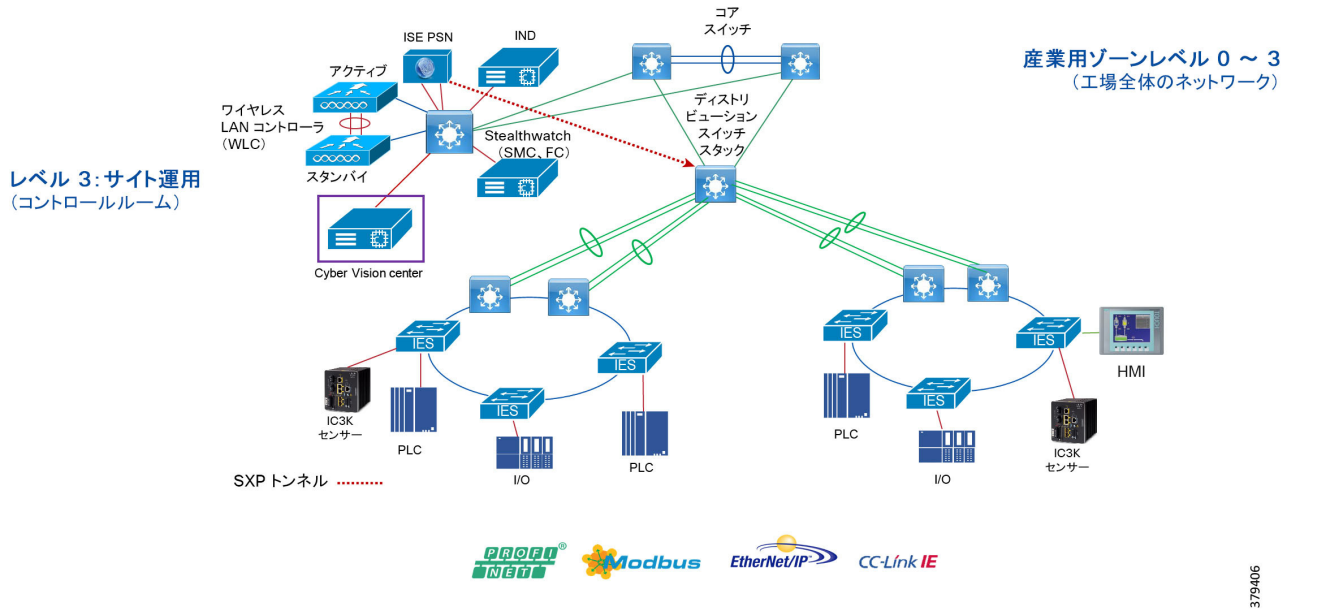
SXP は、トランスポート プロトコルとして TCP を使用して、2 台の異なるネットワーク デバイス間の SXP 接続を確立します。各 SXP 接続には、SXP スピーカーとして指定されたピアと、SXP リスナーとして指定されたピアがあります。これらのピアは、それぞれがスピーカーおよびリスナーの両方として機能する双方向モードにも設定できます。

接続はどちらのピアによっても開始できますが、マッピング情報は常にスピーカーからリスナーに伝達されます。

前のセクションに示されているように、適用がディストリビューション スイッチに移行されるため、ディストリビューション スイッチが 宛先 IP アドレスから SGT を取得する必要があります。これは、イーサネット フレームに送信元 SGT 情報しかなく、ディストリビューション スイッチが宛先 IP アドレスに関連付けられた SGT バインディングを学習するために必要なポリシーを適用するためです。ディストリビューション スイッチによる宛先タグの取得を支援するには、アクセスレイヤ IES からディストリビューションへの SXP トンネルが必要です。

現在の設計では、SXP トンネルはアクセスレイヤの IES から Cisco ISE へと確立され、ディストリビューション スイッチも Cisco ISE への SXP トンネルを持ちます。このようにして、IP-SGT バインディング情報が Cisco ISE に送信され、ディストリビューション スイッチは Cisco ISE から IP-SGT バインディング情報を学習します。図 71 この設計を示しています。

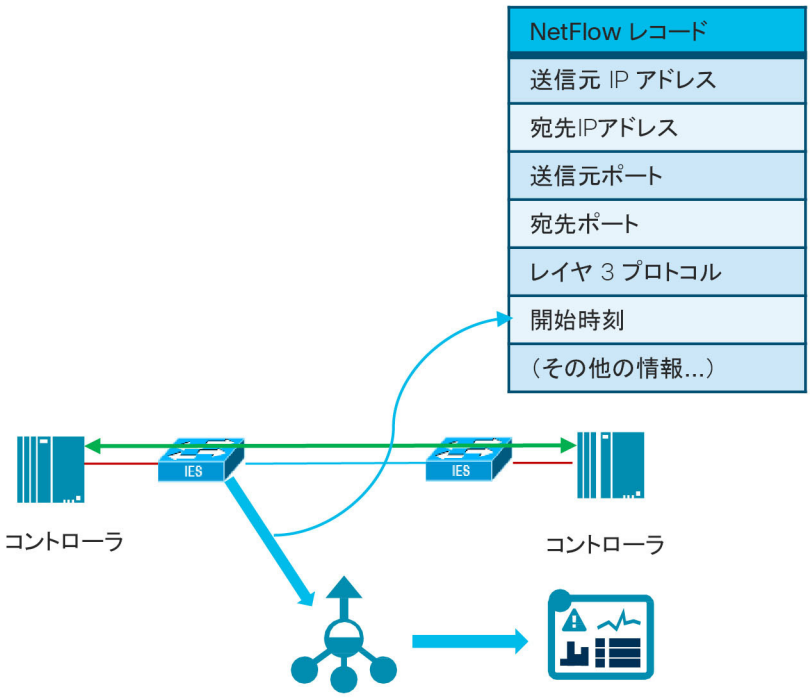
図 71　産業用オートメーション ネットワーク セキュリティ CVD の SXP 設計



NetFlow

Cisco IE 3400、Cisco IE 4000、Cisco IE 4010、Cisco IE 5000、Cisco Catalyst 3850、および Cisco Catalyst 9300 は、完全な Flexible NetFlow をサポートしています。NetFlow は、ネットワークの動作を分析するためにシスコのソフトウェアに組み込まれているインスツルメンテーションです。これにより、スイッチまたはルータを通過するデータフローが可視化されます。NetFlow を有効にすると、SPAN ポートがなくても、ネットワーク内のすべてのデータ通信をトレースできます。

図 72　NetFlow の例



ルータまたはスイッチ内を転送される各パケットは、IP パケット属性セットが検査されます。これらの属性は、IP パケットの ID、つまりパケットのフィンガープリントであり、パケットが一意であるか、または他のパケットと似ているのかが判断されます。

従来、IP フローは 5 ～ 7 個の IP パケット属性に基づいています。

NetFlow によって使用される IP パケットの属性は、次のとおりです。

- IP 送信元アドレス
- IP 宛先アドレス
- 送信元ポート
- 宛先ポート
- レイヤ 3 プロトコル タイプ
- サービスクラス
- ルータまたはスイッチのインターフェイス

同じ送信元/宛先 IP アドレス、送信元/宛先ポート、プロトコル インターフェイス、サービス クラスを持つすべてのパケットがグループ化されて 1 つのフローに入れられ、パケットとバイトが集計されて NetFlow キャッシュに格納されます。その後、このキャッシュを Cisco Stealthwatch などのシステムにエクスポートし、そこでネットワークデータの詳細な分析を使用して脅威やマルウェアを識別できます。詳細については、次の付録および項を参照してください。
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_5_e/configuration_guide/b_1525

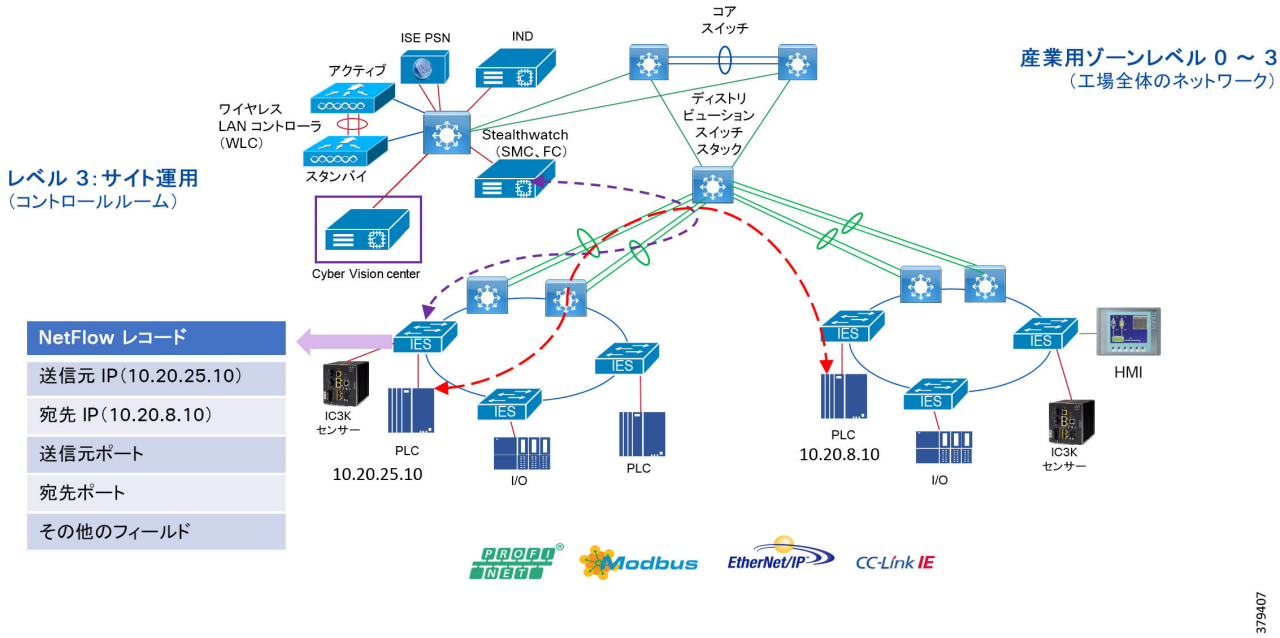
NetFlow データ収集

フローとは、送信元と宛先の間の単方向の接続です。2 つのデバイスの間の完全な交換を説明するには、2 つの独立した単方向フローが必要です。たとえば、データがクライアントとサーバの間を流れるとき、「クライアントからサーバへ」と「サーバからクライアントへ」の 2 つのフローが発生します。NetFlow は、エンドデバイス間のネットワーク内のスイッチおよびルータを通過するパケットのフローレコードを作成し、そのフローレコードをフローコレクタにエクスポートするプロトコルです。フローコレクタによって収集されたデータは、さまざまなアプリケーションで詳細な分析のために使用されます。当初、NetFlow はネットワークのトラフィック統計情報を提供するために使用されていましたが、その後、ネットワーク セキュリティツールとして注目を集めるようになりました。産業用オートメーション ネットワーク セキュリティ CVD では、NetFlow は主にマルウェアの検出やネットワークの異常などのセキュリティ分析を提供するために使用されます。NetFlow を導入することには多くの利点があります。

- NetFlow は、入力パケットと出力パケットの両方に使用できます。
- ネットワーク内の各ネットワーキング デバイスは、NetFlow を個別に有効にできます。
- NetFlow には、トラフィックを収集するための個別の管理ネットワークを使用しません。

図 73 に示すように、通常のフローでは、5 タプルの情報（送信元 IP、宛先 IP、送信元ポート、宛先ポート、およびプロトコル）が記録されます。

図 73　NetFlow データ収集



NetFlow の最新リリースでは、スイッチまたはルータは、ToS、送信元 MAC アドレス、宛先 MAC アドレス、インターフェイス入力、インターフェイス出力などの追加情報を収集できます。Cisco Cyber Vision と ISE の統合では、デバイスの MAC アドレスを収集することが極めて重要です。次の設定には、セル/エリアゾーンの IES で収集される情報が示されています。

```
flow record Cisco Stealthwatch_Record
description NetFlow record format to send to Cisco Stealthwatch match datalink mac source address input
match datalink mac destination address input match ipv4 tos



match ipv4 protocol
match ipv4 source address match ipv4 destination address match transport source-port
match transport destination-port collect transport tcp flags collect interface input
collect interface output collect counter bytes long collect counter packets long
collect timestamp sys-uptime first collect timestamp sys-uptime last
!
```

NetFlow 記録の設定は IND プラグアンドプレーを使用して行うことができます。詳細については、導入ガイドで説明されています。次の重要な考慮事項は、フローの管理に関するものです。ネットワーク トラフィックがシスコ デバイスを通過するとき、フローは継続的に作成され追跡されます。フローが期限切れになると、NetFlow キャッシュから StealthWatch Flow Collector にエクスポートされます。フローが特定の時間にわたって非アクティブの場合（たとえば、新しいパケットがフローで受信されていない場合）、またはフローが長時間存続しており（アクティブな状態で）、アクティブタイマーよりも長く存続している場合（たとえば、長時間の FTP ダウンロードや標準 CIP/IO 接続が行われている場合）、フローはエクスポートの準備ができています。フローが非アクティブか長時間存続しているかどうかを指定するタイマーがあります。

フローがタイムアウトになると、NetFlow 記録情報がフローコレクタに送信され、スイッチ上では削除されます。NetFlow の実装は主に、トラフィック分析ではなくセキュリティベースのインシデントを検出するために行われるため、Cisco IE 4000、Cisco IE 4010、Cisco IE 5000、および Cisco Catalyst 9300 スイッチで推奨されるタイムアウトは、アクティブタイムアウトの場合は 60 秒、非アクティブタイムアウトの場合は 30 秒です。Cisco IE 3400 の場合、アクティブタイムアウトは 1,800 秒、非アクティブタイムアウトは 60 秒、エクスポートタイムアウトは 30 秒です。

次の考慮事項は、ネットワークでの NetFlow の有効化に関するものです。このガイドでは、セキュリティのために NetFlow を使用することを推奨します。したがって、産業用オートメーションネットワーク内のすべてのインターフェイスで NetFlow モニタリングを有効にすることを推奨します。

Stealthwatch 導入の考慮事項

Steatlwatch システムの主要なコンポーネントは次のとおりです。

- フロー コレクタ
- StealthWatch 管理コンソール

注:それぞれのシステムは、異なる仮想アプライアンスまたはハードウェアアプライアンスに存在します。

フロー コレクタは、ネットワーク デバイスから NetFlow データを収集し、収集したデータを分析し、通常のネットワークアクティビティのプロファイルを作成し、通常のプロファイルの範囲に含まれない動作に関するアラートを生成します。ネットワーク フロー トラフィックに基づいて、ネットワーク内に 1 つまたは複数のフローコレクタが存在する場合があります。Stealthwatch 管理コンソール（SMC）により、IT セキュリティアーキテクトは、ネットワークトラフィック全体のコンテキスト ビューを 1 つのインターフェイスで取得できます。

SMC は、Java ベースのシッククライアントと、データと設定を表示するためのウェブインターフェイスを持っています。SMC は次のことを可能にします。

- 最大 25 のフロー コレクタに対する集中型の管理、設定およびレポート
- トラフィックの視覚化のためのグラフィカルチャート
- トラブルシューティングのためのドリルダウンの分析
- 統合型のカスタマイズ可能なレポート
  - トレンド分析
  - パフォーマンス モニタリング
  - セキュリティ違反の即時通知

Steathwatch システムを導入する際の重要な考慮事項は、次のとおりです。

- Stealthwatch は、ハードウェアアプライアンス（物理アプライアンス）と仮想アプライアンスのどちらとしても利用できます。ハードウェアアプライアンスおよびソフトウェアアプライアンスをインストールするには、次の Stealthwatch のガイドを参照してください。
  https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

- Stealthwatch フローコレクタ のリソース割り当ては、ネットワークで予想される 1 秒あたりのフローの数、エクスポータ（NetFlow が有効になっているネットワークデバイス）の数、および各ネットワークデバイスに接続されているホストの数によって異なります。フローコレクタの拡張性要件については、次のドキュメントを参照してください。https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

- データ ストレージ要件を考慮する必要があります。これも、ネットワーク内のフローの数によって異なります。データストレージのサイジングの表については、次のドキュメントを参照してください。https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

- 特定のポート セットは、インバウンド方向とアウトバウンド方向の両方で Stealthwatch ソリューションに対して開かれている必要があります。開くことが推奨されているポートの完全なリストについては、次のドキュメントを参照してください。https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_Installation_and_Configuration_Guide_DV_1_0.pdf

Cisco ISE の導入の考慮事項

大規模ネットワークに Cisco ISE を導入するには、IT セキュリティアーキテクトが、拡張性やハイアベイラビリティといった、いくつかの要素を考慮する必要があります。この設計ガイドでは、大規模な Cisco ISE の導入に関連するさまざまな要素について説明します。大規模なソリューションの導入を深く理解するには、CPwE DIG を参照することをお勧めします。設計ガイドに記載されている主な推奨事項の一部を、クイックリファレンスとしてここに示します。

分散型の展開では、Cisco ISE システムは、次のような管理、ポリシーサービス、モニタリングの 3 つの個別ノード（ペルソナ）に分割されます。

- ポリシー管理ノード（PAN）により、企業の IT チームは、分散型 Cisco ISE システムでのすべての管理操作を実行できます。企業ゾーンに配置される PAN では、認証ポリシーや承認ポリシーなどの機能に関連するすべてのシステム設定が処理されます。分散 Cisco ISE 導入では、管理ペルソナを持つノードを 1 つまたは 2 つ（最大）配備できます。これらのノードは、ハイ アベイラビリティに関して主要な役割または副次的な役割を果たすことができます。

- ポリシーサービスノード（PSN）は、クライアント認証、許可、プロビジョニング、プロファイリング、およびポスチャサービスを提供します。産業ゾーンおよび企業ゾーンに配置される PSN は、ポリシーを評価し、ポリシー評価の結果に基づいてデバイスへのネットワーク アクセスを提供します。分散セットアップ内の少なくとも 1 つのノードがポリシーサービスペルソナを引き受ける必要があり、通常、大規模な分散導入では複数の PSN が存在します。

- モニタリング ノード（MnT）は、ログコレクタとして機能し、ネットワーク内のすべての PAN および PSN からのログ メッセージと統計情報を格納します。企業ゾーンに配置される MnT は、データを収集して関連付け、企業の IT および OT 担当者に役立つレポートを提供します。分散システムでは、モニタリングペルソナを持つノードを 1 つ以上（最大 2 つ）配備できます。これらのノードは、ハイアベイラビリティに関して主要な役割または副次的な役割を果たすことができます。

最大限のパフォーマンスと復元力を実現するために、この CVD では、産業用オートメーション アイデンティティおよびモビリティ サービス アーキテクチャに関して次の推奨事項を提供します。

- 管理ペルソナとポリシー サービス ペルソナは、異なる Cisco ISE ノードで設定する必要があります。

- モニタリングペルソナとポリシーサービスペルソナは同じ Cisco ISE ノードで有効にしないでください。最大限のパフォーマンスを実現するために、モニタリングノードはモニタリング専用にする必要があります。

- 産業ゾーンのクライアントにサービスを提供するには、PSN を産業ゾーン（レベル 0 ～ 3）に配置する必要があります。企業ゾーンと産業ゾーンが分離されても、既存のクライアントはネットワークに安全にアクセスできます。ベストプラクティスについては、「以前のドキュメントと関連ドキュメント（219 ページ）」を参照して、産業用オートメーション IDMZ CVD DIG へのリンクを確認してください。

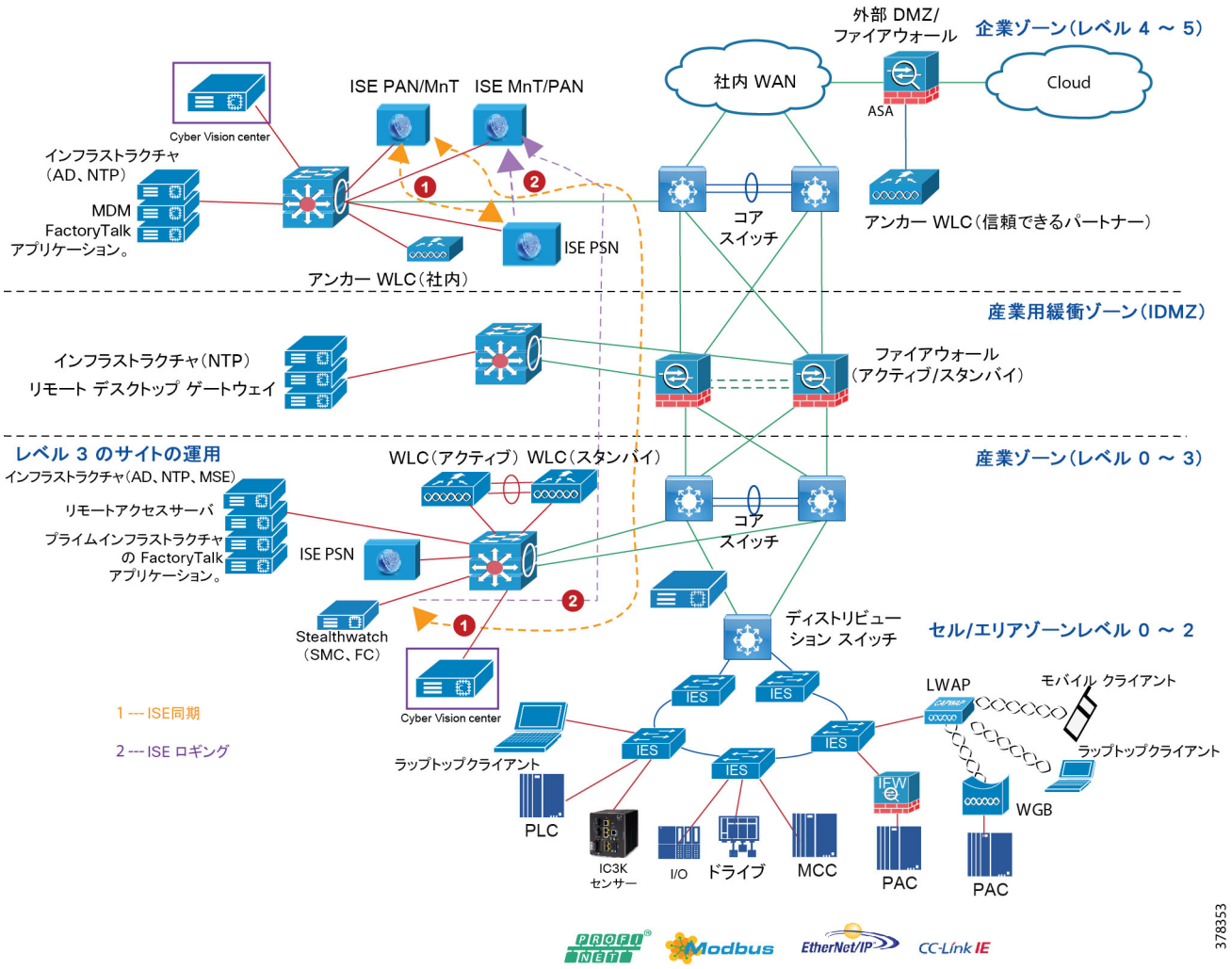
- 安全なデータ トンネル内の IDMZ を通じて企業ネットワークに接続する企業のモバイル ユーザを認証するには、PSN も企業ゾーンに配置する必要があります。このシナリオについては、このガイドの後半で詳しく説明します。

上記の推奨事項に基づき、産業用オートメーション アーキテクチャへの一般的な分散 Cisco ISE 導入は、図 74 に示すように、次のノード(ハードウェアアプライアンスまたは VM)で構成されます。

- 1 つのプライマリ管理/セカンダリ モニタリング ノード
- 1 つのセカンダリ管理/プライマリ モニタリング ノード
- 企業ゾーンの 1 つまたは複数の PSN
- 産業ゾーンの 1 つまたは複数の PSN

注:企業ゾーンおよび産業ゾーンの PSN の数は、企業の規模、アクティブクライアントの数、冗長性の要件、および地理的な分布(たとえば、各工場に 1 つの PSN)によって異なります。

図 74　ISE 導入モデル



IPDT の考慮事項

IP デバイス トラッキング（IPDT）は、IES またはその他のスイッチやルータが、それに接続されているホストを継続的にトラッキングすることを可能にする機能です。dot1x、MAB、Web 認証、認証プロキシなどのいくつかのセキュリティ機能のために IPDT 機能を有効にする必要

があります。IPDT 機能は、IP アドレスと MAC アドレスの間のマッピングを維持します。トラッキングを行うために、IES は、30 秒のデフォルト間隔で ARP プローブを送信します。このプローブは、送信元 IP アドレスが 0.0.0.0 に設定されている場所に、RFC5227 に従って実装されます。IPDT 機能がデフォルトの送信元 IP アドレス 0.0.0.0 で有効になっている場合は、IES と、やはりデバイス トラッキングを実行している IACS アセットの間で競合が発生する可能性があります（重複 IP アドレス 0.0.0.0 の問題の詳細については、次を参照してください。
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/8021x/116529-problemsolution-product-00.html）。

推奨されるオプションは、IPDT を実装する前に、IPDT 機能で使用される標準 IP アドレスを変更することです。IES で次のコマンドを使用できます。

```
ip device tracking probe auto-source fallback 169.254.26.64 0.0.0.0 override
```

このコマンドは、SVI へのプローブの送信元を使用し（存在する場合）、169.254.26.64（リンクローカル IP アドレス）にフォールバックします。リンクローカル IP アドレスをフォールバックとして使用することの有効性は、スイッチに接続されているデバイスがリンクローカル IP アドレスを持たないという前提に基づいています。リンクローカル IP アドレスは、ローカルセグメント内でパケットをルーティングするためだけに使用され、ルータは、リンクローカル IP アドレスを受信してもそのパケットを転送しません。IT セキュリティアーキテクトは、コマンドを有効にする前に、ネットワークにリンクローカル IP アドレスが存在するかどうかを確認する必要があります。

注：RADIUS ダウンロード可能 ACL および SGT を実装するには、RFC 5227 に従って動作する IPDT を IES で有効にする必要があります。IPDT は、ARP プローブを使用して、異なるポート上のホストの IP アドレスを特定します。この動作により、IACS アセットのデバイスおよびアプリケーションの動作が中断する場合があります。

IPDT は、802.1X 認証を使用する IES ポートで、次の場合にのみ有効にする必要があります。

- メンテナンスポートと指定された非 IACS 機器ポートのいずれかまたは両方
- MAC 認証バイパスを使用する IACS ポート（セキュリティポリシーが DACL を必要としており、適切な IPDT 回避策が適用され、IACS アセットのデバイスおよびアプリケーションでテストされている場合）

デフォルトでは、DACL 機能が不要な場合、IACS アセットのデバイスおよびアプリケーションに接続されているポートで IPDT を有効にしないでください。詳細および IPDT の回避策については、
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html を参照してください。

産業用オートメーション向けの OT インテントベース セキュリティのユースケース

ここでは、このガイドに記載されているネットワーク セキュリティ ユースケースの実装について説明します。その目的は、次の各ユースケースの詳細を示し、これらのユースケースをサポートするために IES、ISE、Cisco Cyber Vision、Stealthwatch などのさまざまなコンポーネントがどのように連携して機能するのかを詳しく説明することです。ここでは、次のユースケースについて説明します。

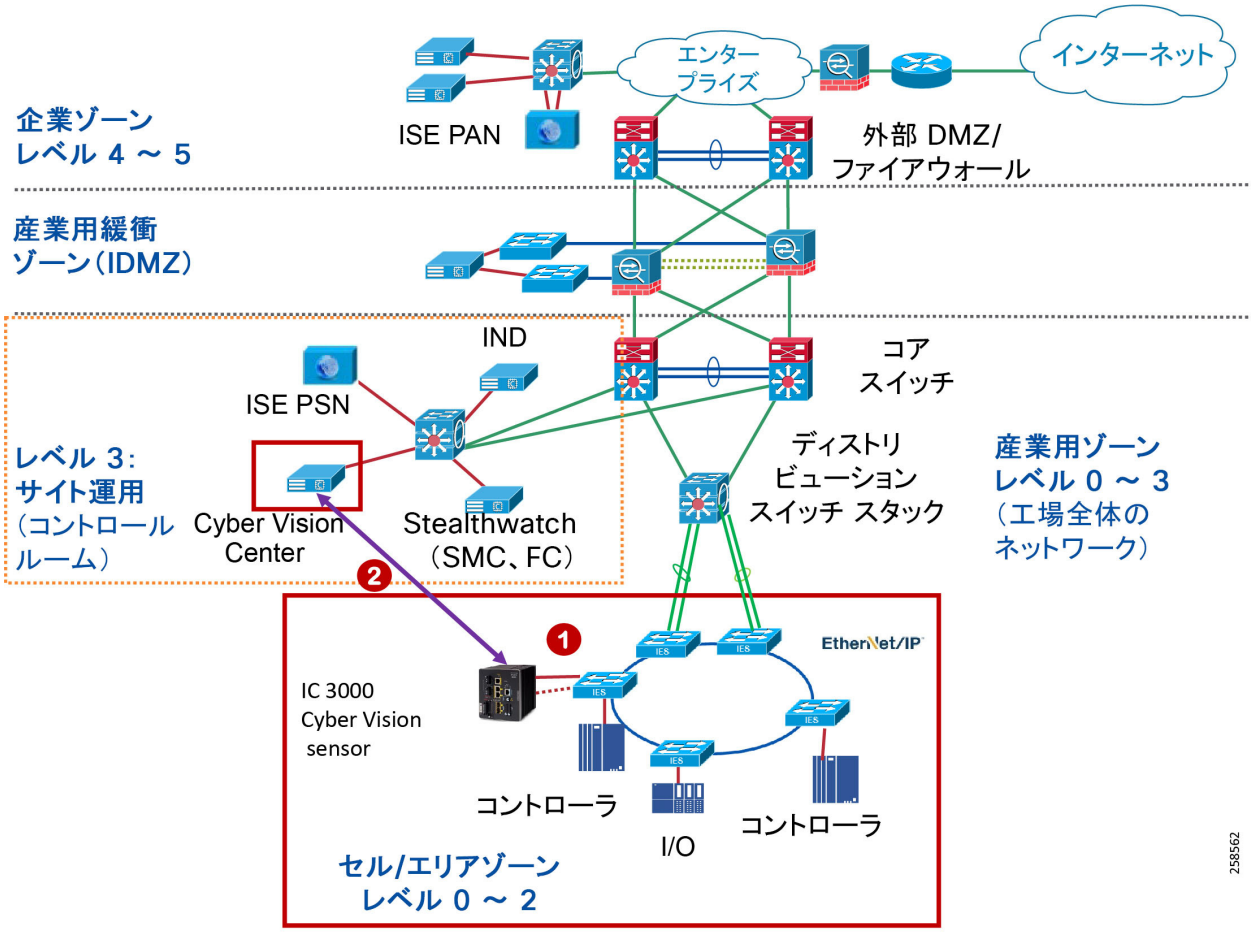
- セル/エリアゾーン内のネットワーク デバイスと IACS アセットの可視性および識別
- 産業ゾーンの IACS アセットのセキュリティ グループ ポリシー割り当て
- セル/エリアゾーンおよびレベル 3 サイトの操作ゾーンでの NetFlow を使用したマルウェア検出
- OT が管理するリモートユーザ（従業員またはパートナー）による工場インフラストラクチャへのアクセス
- （Cisco Cyber Vision による）運用イベントの検出

セル/エリアゾーン内の IACS アセットの可視性および識別

このユースケースの目的は、OT 制御システムエンジニアと IT セキュリティアーキテクトが、セル/エリアゾーン内のネットワークデバイスと IACS の可視性を得るためにどのように連携できるのかを示すことです。IT セキュリティアーキテクトが IACS のタイプ（コントローラ、I/O、ドライブ、HMI など）を認識できるように、可視性を十分にきめ細かくする必要があります。East-West（水平）方向または North-South（垂直）方向に流れるトラフィックフローをセグメント化するには、IT セキュリティアーキテクトが工場全体のネットワークで現在のネットワークトポロジの可視性を得ることが重要です。このガイドには、Cisco Cyber Vision と Cisco Industrial Network Director（IND）を使用して IACS を可視化する 2 つの方法があります。ここでは、両方のユースケースについて説明します。

図 75 このユースケースを実行する手順の概要を示しています。

図 75　Cisco Cyber Visionを使用した IACS の可視性



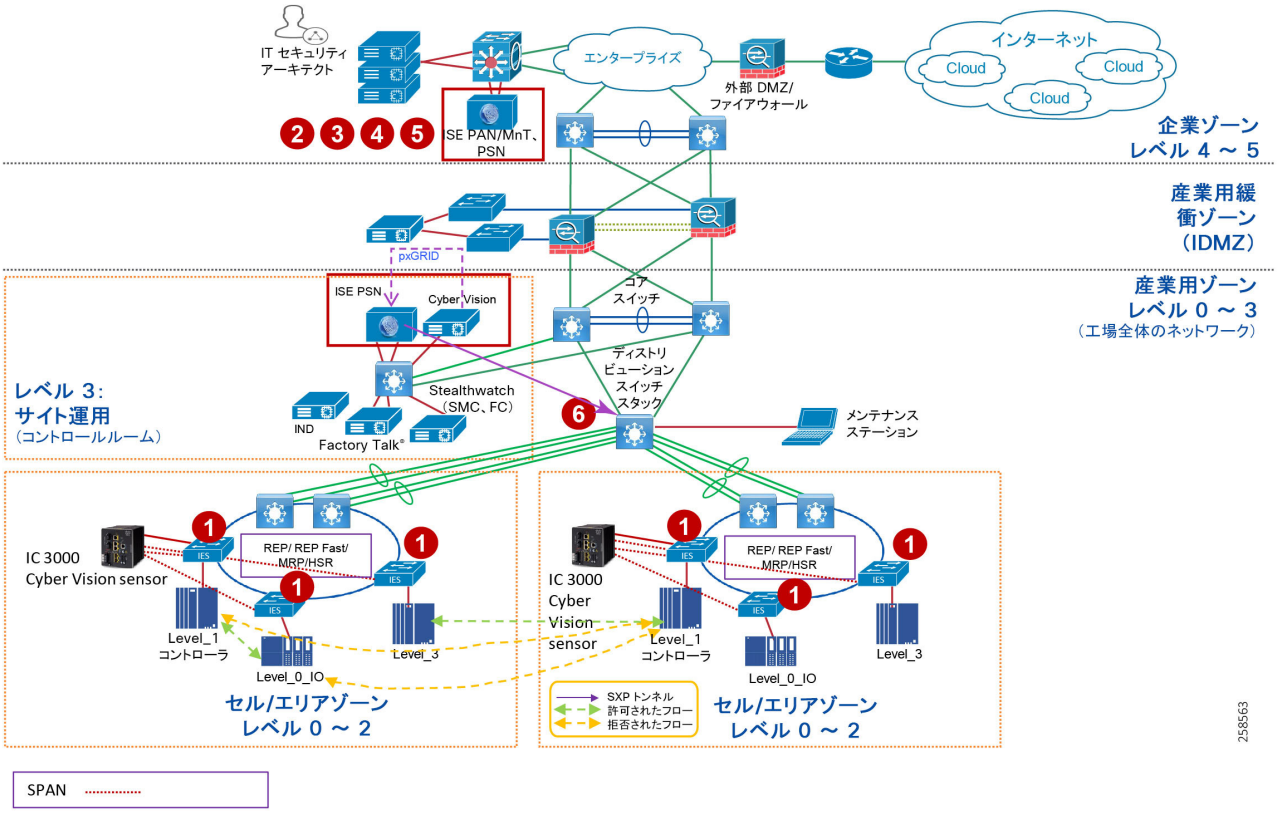
1. OT 制御システム エンジニアは、モニタする IACS を決定し、Cyber Vision の導入オプションを選択し、ポート上でパッシブモニタリング（SPAN）を設定します。導入ガイドを参照してください。
2. Cisco Cyber Vision Centerは、IACS のベンダー名、モデル名、シリアルナンバー、IP アドレス、MAC アドレス、ファームウェアバージョン、デバイス名、およびその他の関連情報を動的に学習します。導入ガイドを参照してください。

Cisco Cyber Visionを使用した IACS のセル/エリアゾーン セグメンテーション

このユースケースでは、Cisco ISE および Cyber Vision を使用して、セル/エリアゾーンでさまざまなトラフィックフローのセグメンテーションを実現する方法について詳しく説明します。トラフィックフローを理解するには、「ネットワークの IACS トラフィックフロー」を参照してください。セグメンテーションの背後にある考え方は、「セル/エリアゾーンのセグメンテーション」で定義されています。このユースケースでは、Cisco ISE および Cyber Vision を使用して、セル/エリアゾーンでさまざまなトラフィックフローのセグメンテーションを実現する方法について詳しく説明します。

Cisco Cyber Vision を使用したセグメンテーション

図 76　Cisco Cyber Vision を使用したセル/エリアゾーン セグメンテーション



1. IT セキュリティアーキテクトが、すべての IES でポートベースの認証を設定する必要があります。導入ガイドを参照してください。
2. IT セキュリティ アーキテクトが、ISE で異なる IACS（Level_1_Controller、Level_0_IO、および Level_3）の TrustSec SGT を設定する必要があります。導入ガイドを参照してください。
3. IT セキュリティアーキテクトが、ISE で認証および認可ポリシーを設定する必要があります。導入ガイドを参照してください。
4. IT セキュリティアーキテクトが、IES およびディストリビューション スイッチから ISE への SXP トンネルを設定する必要があります。導入ガイドを参照してください。
5. IT セキュリティアーキテクトが、ISE で TrustSec ポリシーマトリックスを設定する必要があります。導入ガイドを参照してください。
6. IT セキュリティ アーキテクトが、Cisco Catalyst 3850、Cisco Catalyst 9300、Cisco IE 5000 ディストリビューション スイッチで適用を設定する必要があります。導入ガイドを参照してください。

フローベース 異常検出

このユースケースでは、IT セキュリティアーキテクトが Stealthwatch を、IES と Cisco Catalyst 3850、Cisco Catalyst 9300、Cisco Catalyst 9500 で有効になっている NetFlow とともに使用して、工場全体のネットワーク内のネットワークフローをモニタする方法について説明します。さらに、このユースケースでは、Cisco Cyber Vision と Stealthwatch の統合も示しています。Cisco Cyber Visionと Stealthwatch の統合により、IT セキュリティアーキテクトは、セル/エリアゾーンで発生する OT フローのコンテキストを理解することができます。Cisco Cyber Visionと Stealthwatch の統合は、次の手順を実行することによって行われます。

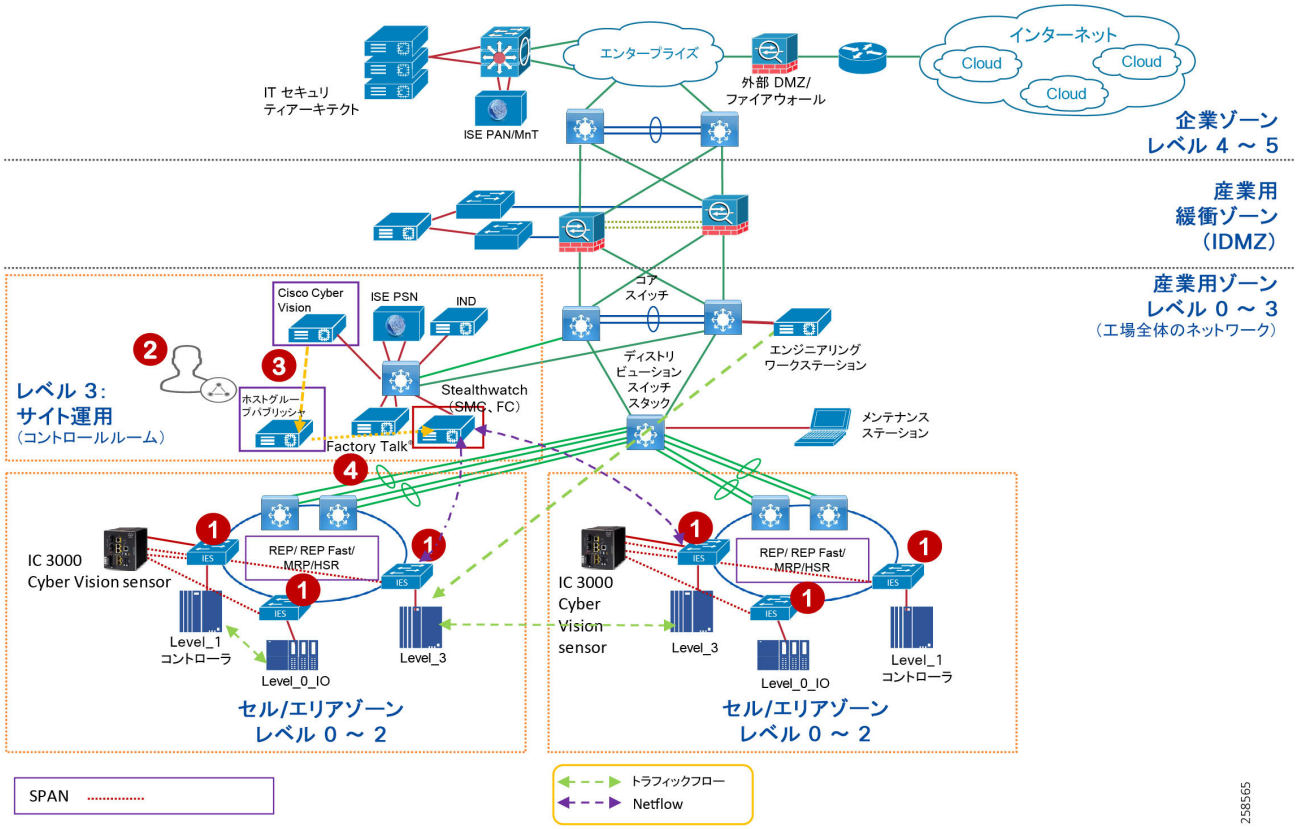
工場全体のネットワークで発生するトラフィックフローを検出するには、FlowCollector に送信されるトラフィックフローをキャプチャするためにすべてのネットワークデバイスで NetFlow を有効にすることが重要です。SMC は、FlowCollector からフロー データを取得し、事前に構築されたアルゴリズムを実行してネットワーク フローを表示し、さらに悪意のある動作や異常な動作がネットワークで発生しているかどうかを検出して警告します。このガイドには、NetFlow を使用して Stealthwatch の機能をデモンストレーションするための 3 つのフローが示されています。

- セル/エリアゾーンの IACS アセット間のトラフィック（セル/エリアゾーン内）
- セル/エリアゾーン全体の Level_3 IACS アセット間のトラフィック（East-West（水平）またはセル/エリアゾーン間トラフィック）
- EWS と Level_3 IACS アセット（垂直）の間のトラフィック

上記のフローを検出するには、IT セキュリティ アーキテクトが次のステップを実行する必要があります。

1. IT セキュリティ アーキテクトが、すべての IES および Cisco Catalyst 3850 スイッチで NetFlow を有効にする必要があります。導入ガイドを参照してください。
2. IT セキュリティアーキテクトは、サーバに Cisco Cyber Vision Python スクリプトを導入します。
3. Python スクリプトを使用する IT セキュリティアーキテクトは、Cisco Cyber Vision Center に接続し、ホストグループ情報をダウンロードします。
4. Python スクリプトを使用する IT セキュリティアーキテクトは、Stealtwatch 管理コンソール（SMC）に接続し、ホストグループ情報をパブリッシュします。

図 77　フローベース 異常検出



セル/エリアゾーンおよびレベル 3 運用のマルウェア検出

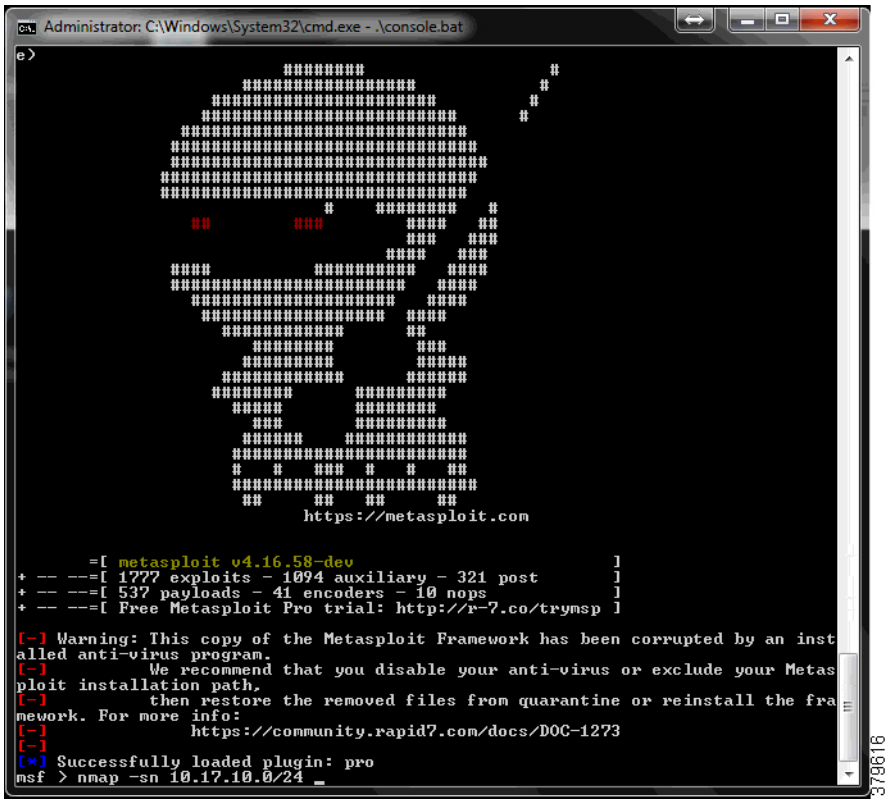
ここでは、工場ネットワークを通過する悪意のあるトラフィックを Stealthwatch が検出する方法について説明します。マルウェアがネットワーク内に拡散している場合、マルウェアの伝播の発生箇所を特定することは非常に困難になります。IT セキュリティアーキテクトは、原因を特定し、問題に対処するための修復計画を立てる必要があります。Stealthwatch は、ネットワーク内で起こり得るマルウェアの伝播を IT セキュリティ担当者が検出することを支援できる多数の組み込み機械学習アルゴリズムを備えています。また、異常な動作を検出し、伝播の原因となっているデバイスの IP アドレスを提供することもできます。この情報により、検出プロセスが大幅に簡素化されます。

Stealthwatch を使用しない場合、IT セキュリティアーキテクトは、悪意のあるアクティビティを検査するため、ネットワークの一部をシャットダウンしたり、多くのデバイスのログを確認したりするなど、多くの時間がかかる可能性がある手順を実行しなければならない場合があります。これらのステップを実行することで、問題の分離に時間がかかるだけでなく、他の脆弱なデバイスが感染するリスクが高まります。アクティブなマルウェアが検出された場合、マルウェアに対する防御を構築するには、修復計画を迅速に策定することが不可欠です。

マルウェアは大抵、ネットワーク全体を即座にスキャンして、工場全体のネットワーク内にある他の脆弱なデバイスを特定します。この CVD では、マルウェアに関連する 2 つのトラフィックフローについて説明します。

- IES に接続されている、感染したラップトップ。図 78 感染したラップトップによるスキャンの実行方法の例を示します。

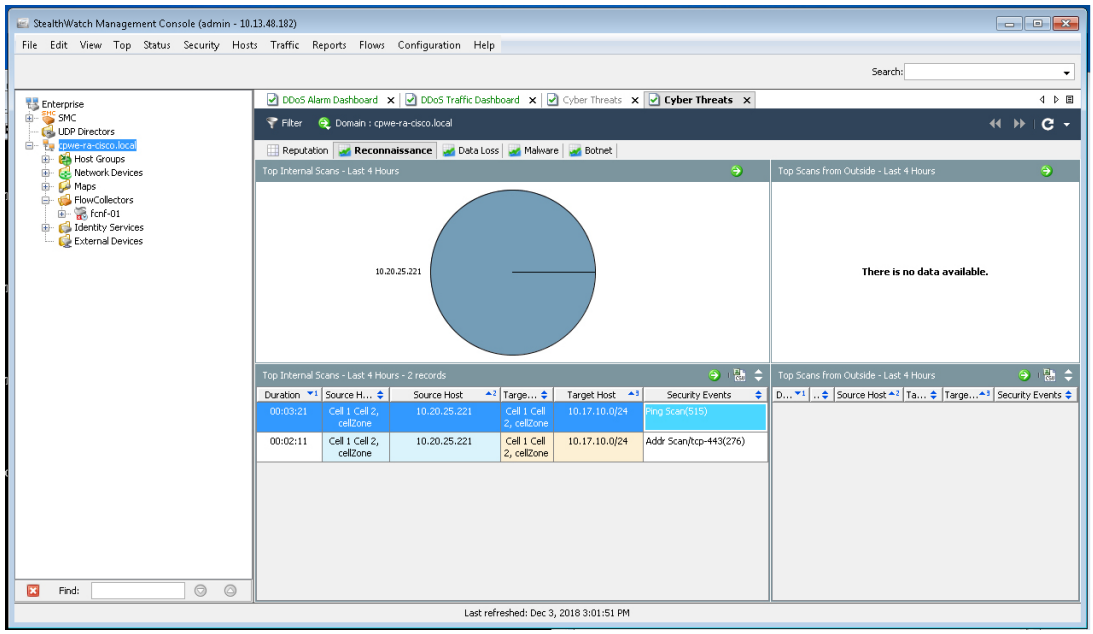
図 78　感染したラップトップによるスキャン



- Layer-3 サイト運用センターに接続されている、感染したラップトップ。

どちらの場合も、感染したラップトップは IP アドレス範囲全体をスキャンして、次の可能なターゲットを識別し、それらへの感染を試みます。Stealthwatch は、高懸念インデックスのアラームを生成することにより、潜在的な侵入を即座に検出します。高懸念インデックスのアラームはすべて、ただちに考慮する必要があります。また、アラームで検出される悪意のある動作が増えるにつれて、ホストの高懸念インデックスが増加して脅威が増加していることを示します。図 79 SMC でのアラームの表示方法を示します。図 79 では、ホスト 10.20.25.221 が、10.17.10.0/24 ネットワークのスキャンを試みています。

図 79　Stealthwatch 管理コンソールに表示されるアラーム

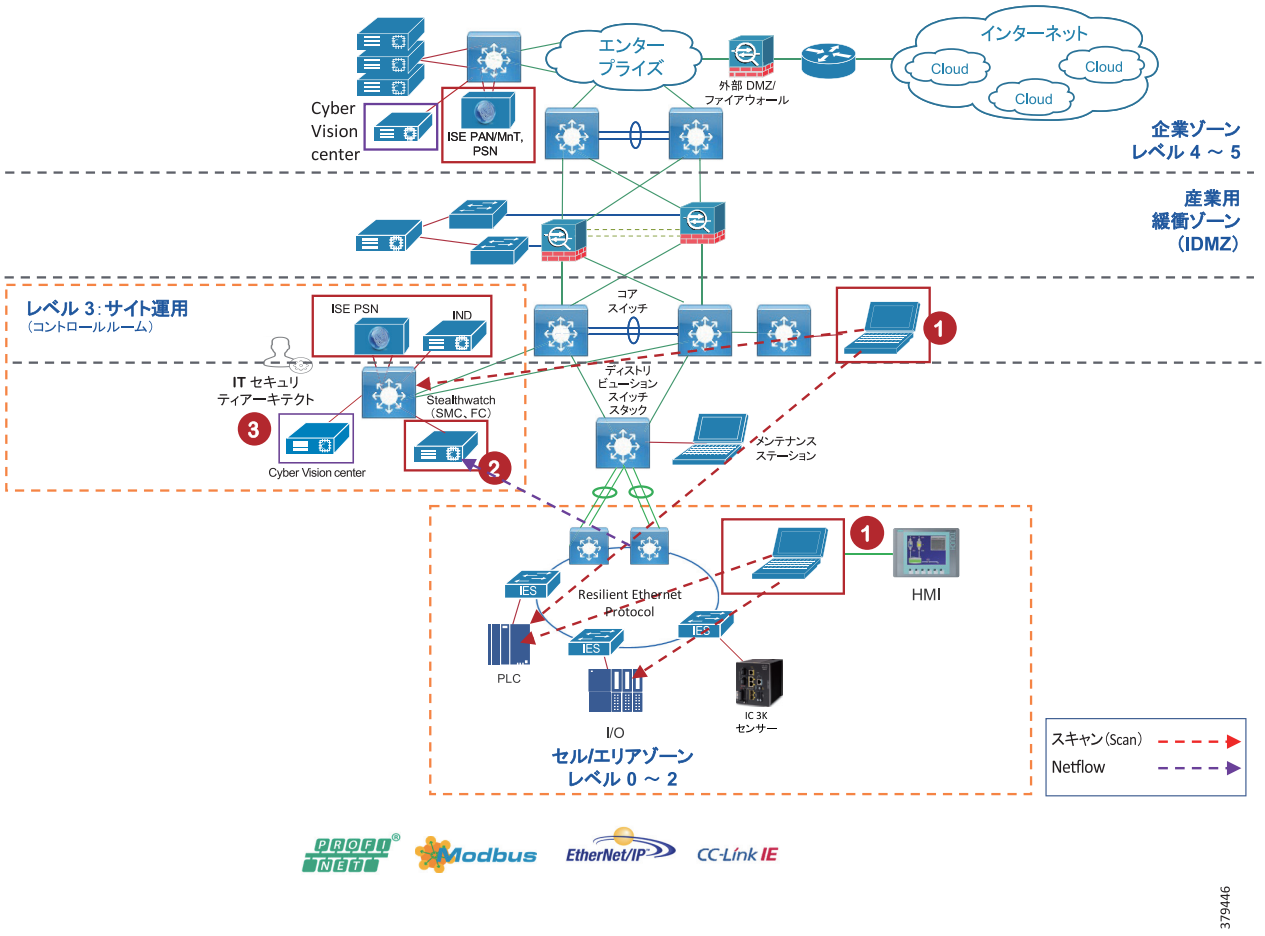


アラームの詳細については、次を参照してください。
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_6_9_0_SMC_Users_Guide_DV_1_2.pdf

図 80 感染したラップトップがセル/エリアゾーンまたは Level_3 サイトオペレーション ゾーンに接続されており、Stealthwatch によって検出されているシナリオを示しています。必要な手順は、次のとおりです。

1. セル/エリアゾーンの IES または Level_3 サイトオペレーションのディストリビューション スイッチで、NetFlow が有効になっています。導入ガイドを参照してください。
2. SMC が、ネットワークで悪意のあるアクティビティが発生していることを示すアラームをレポートします。
3. IT セキュリティアーキテクトが、次の修復段階（さらなる調査の実行、IACS アセットへのアクセスの制限などが含まれる可能性があります）を計画することで、このアラームに対応します。

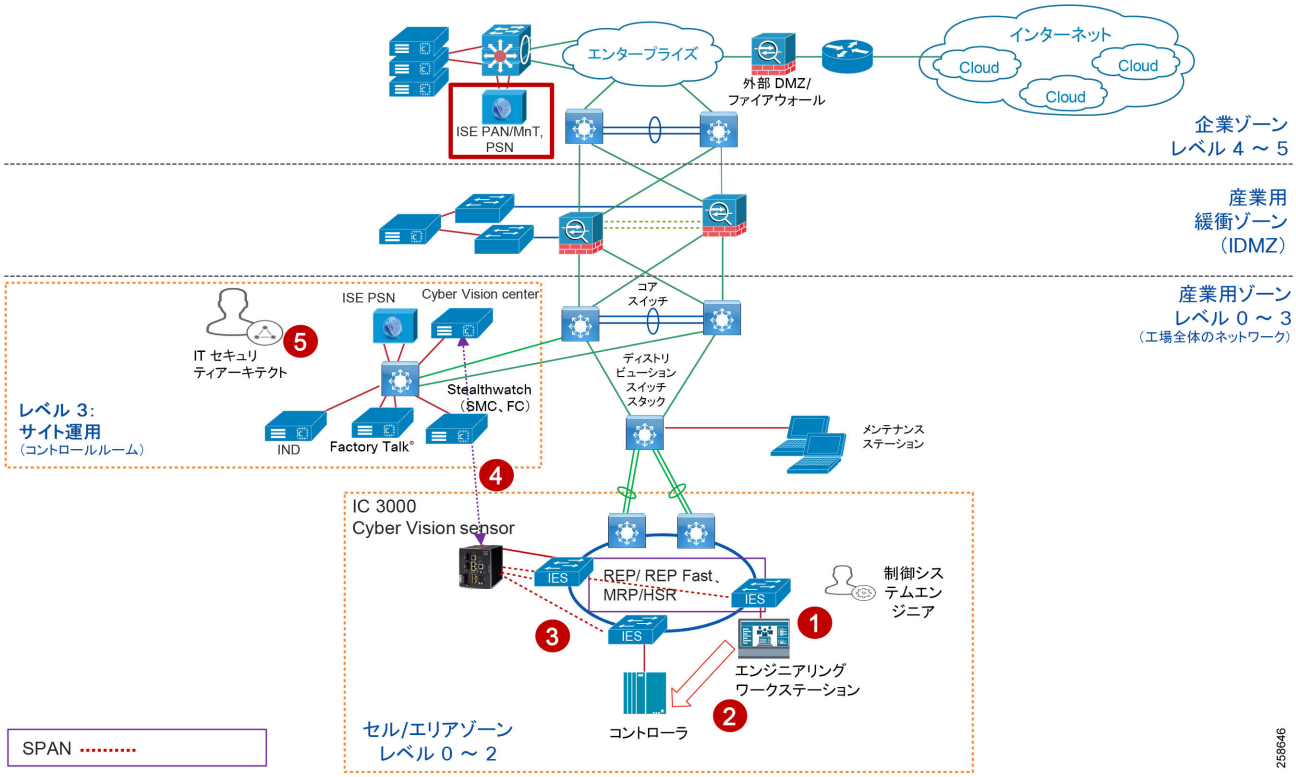
図 80　セル/エリアゾーンのマルウェアの検出



Cisco Cyber Vision による運用イベントの検出

このユースケースの目的は、Cisco Cyber Vision ソリューションがセル/エリアゾーン内の運用イベントを検出する方法を示すことです。運用イベントには、エンジニアリング ワークステーションから PLC へのプログラムのダウンロード、CPU の起動、CPU の停止などが含まれます。このようなイベントがセル/エリアゾーンで発生すると、これらのイベントを受動的にモニタしている Cisco Cyber Vision Sensor は、これらのイベントを検出して関連するメタデータを Cisco Cyber Vision Center に送信します。Cisco Cyber Vision Center は、フローのグラフィカルな説明、ワークステーションの IP アドレス、およびコントローラ情報などのすべての関連情報とともにそれらのイベントをダッシュボードに表示します。

図 81　Cisco Cyber Vision による運用イベントの検出



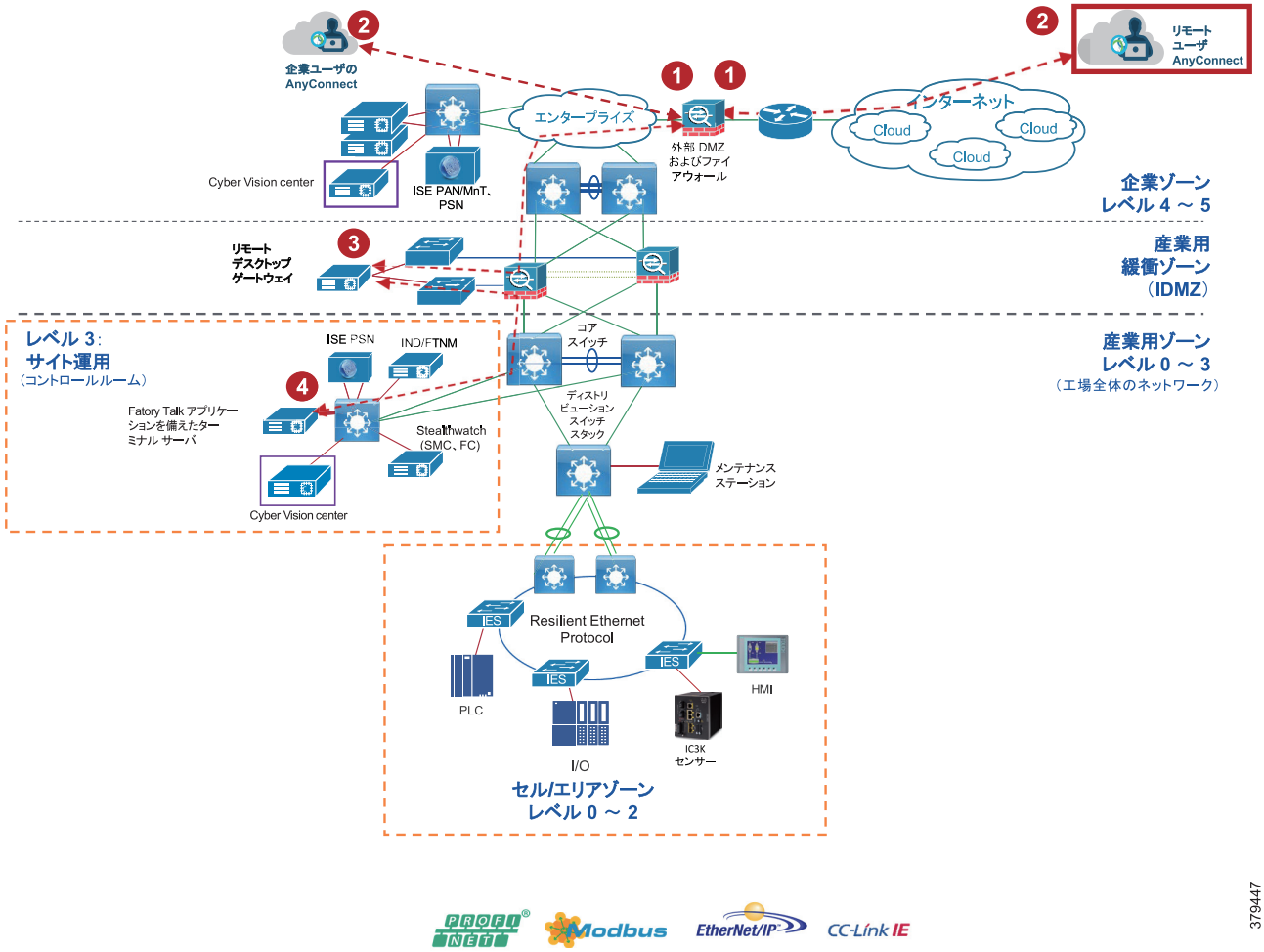
1. コントロールシステム エンジニアは、エンジニアリング ワークステーションで新しいアプリケーションを変更または構築します。
2. コントロールシステム エンジニアは、このプログラムをコントローラにプッシュします。
3. セル/エリアゾーンに展開されている Cisco Cyber Vision Sensor は、イベントを検出します。
4. Cisco Cyber Vision Sensor は、そのイベントを Cisco Cyber Vision Center に送信します。
5. IT セキュリティアーキテクトは、アラートをレビューし、イベントの正当性を判断します。

工場フロアへの OT 管理リモートアクセス

このユースケースでは、リモート ユーザ（従業員またはパートナー）がインターネットまたは企業ゾーンからネットワーク デバイスまたは IACS アセットにアクセスする方法について説明します。『*Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*』（ベスト プラクティスについては、「以前のドキュメントと関連ドキュメント（219 ページ）」を参照し、産業用オートメーション IDMZ CVD へのリンクを確認してください）に、リモートアクセスを提供するための設計上の考慮事項と実装の詳細が示されています。図 82 に示されている、この CVD のリモートアクセス ソリューションの大まかな手順は、次のとおりです。

1. リモート VPN ゲートウェイ（ASA ファイアウォール）は、リモートユーザを認証し、サービスを認可する VPN グループによって有効になります。今回の場合は、IDMZ 内のリモート デスクトップ ゲートウェイにアクセスします。
2. リモート ユーザ（従業員またはパートナー）が、リモートアクセス VPN クライアント（Cisco AnyConnect）を使用してリモート VPN ゲートウェイに接続し、VPN セッションを確立します。
3. リモート VPN ゲートウェイから、IDMZ 内のリモート デスクトップ ゲートウェイへの接続が確立されます。
4. リモート デスクトップ ゲートウェイから、Level_3 サイト運用の FactoryTalk アプリケーションを使用してターミナル サーバへの接続が確立されます。

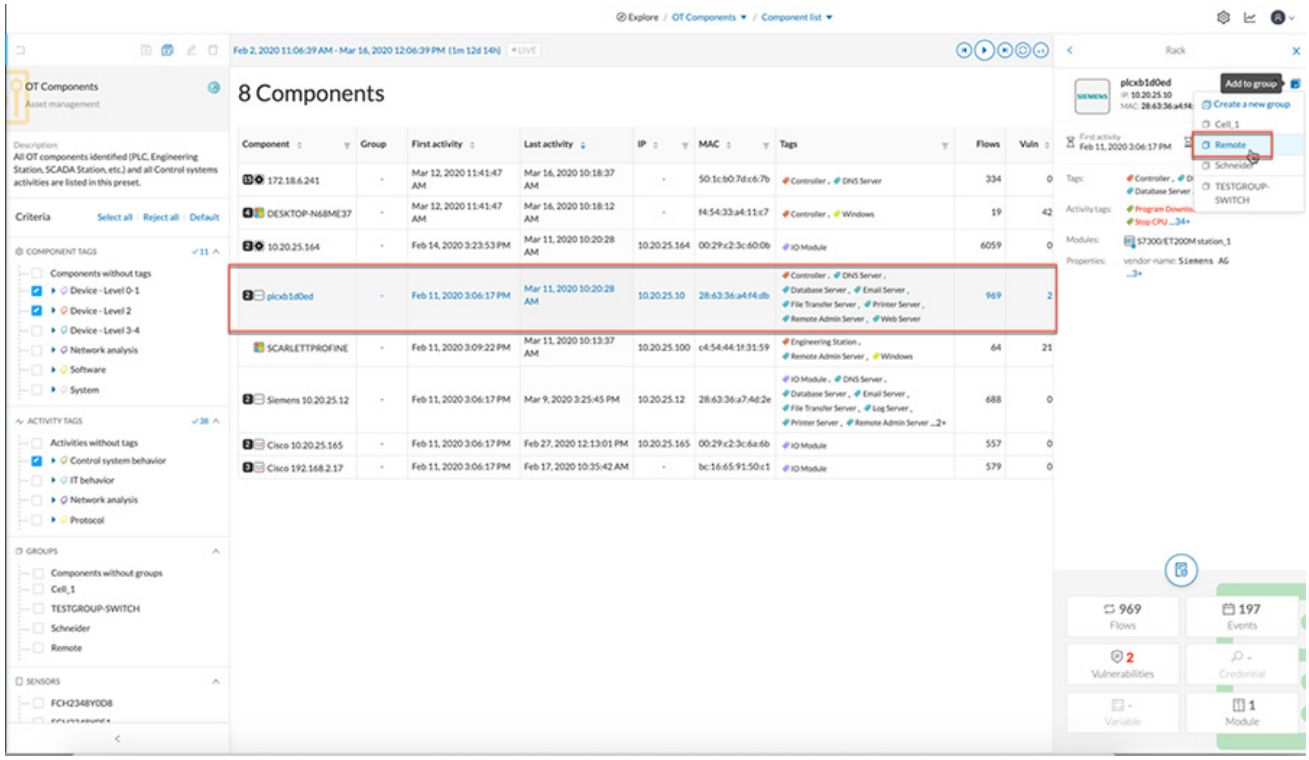
図 82　産業用オートメーションネットワークでのリモートユーザアクセス



このユースケースは、以前の「IACS データの産業用緩衝地帯の安全な通過」の CVD を基盤としており、リモートアクセスに影響を与える手段を OT 制御システムエンジニアに提供することで、リモートユーザのユースケースを拡張します。以前の CVD では、リモートユーザにアクセスが必要な場合に、OT 制御システムエンジニアが IT セキュリティアーキテクトに IACS アセットへのリモートアクセスを有効にするように要求します。その後、リモート ユーザが目的の IACS アセットにアクセスします。ただし、リモート ユーザが IACS アセットにアクセスする必要がなくなった場合、OT 制御システム エンジニアは、アクセスを削除するための別のケースを開く必要があります。このプロセスは動作しますが、アクセスが適時に削除されないと、セキュリティ違反のリスクが増加します。

PxGrid による ISE と Cisco Cyber Vision の統合は、IACS アセットの assetTag を変更することによって、OT 制御システム エンジニアがデバイスアクセスを制御する方法を提供します。OT 制御システム エンジニアが IACS アセットのグループを変更すると、ISE はアセットのプロファイルと SGT（および通信制限）を更新します。IACS アセットが元のグループに戻されると、アセットへのリモートアクセスは同じプロファイリング更新によって取り消されます。図 83 アセットのグループ情報を表示します。

図 83　IACS アセットのグループ情報の変更



この産業用オートメーション CVD では、リモートアクセス ユースケースが、「Remote」という別のグループを作成することによってデモンストレーションされます。リモートアクセスを必要とするデバイスは、このグループに移動する必要があります。このようなアクションが実行されると、次のイベントがトリガーされます。

1. Cisco Cyber Vision は、ISE の「assetGroup」フィールドにリンクされている新しいデバイス属性「Remote」を ISE に送信します。導入ガイドを参照してください。
2. ISE は、このデバイスを Remote_Access として分類し、IACS アセットに認可変更を発行します。これにより、新しい認証および認可がトリガーされ、その結果、新しい SGT 割り当て「Remote_Access」が生成されます。導入ガイドを参照してください。
3. Cisco Catalyst 9300 ディストリビューションスイッチは、ISE から新しい SGACL をダウンロードして、IACS デバイスへのアクセスを許可します。導入ガイドを参照してください。
4. IACS アセットへのアクセスが必要なくなると、OT 制御システム エンジニアが IACS アセットを元のグループに戻します。
5. Cisco Cyber Visionは、新しいグループ情報を ISE に伝達します。これにより、別の再認証と再許可がトリガーされ、IACS アセットは「Level_1_Controller」の元のプロファイルに戻されます。導入ガイドを参照してください。
6. Cisco Catalyst 3850 ディストリビューション スイッチには、Remote_Desktop から Level_1_Controller への通信を拒否する既存のポリシーがあるため、リモート通信はブロックされます。

注:新しい SGT が IACS アセットに割り当てられると、アプリケーションが IACS アセットと通信できるようになるまでに、数秒間、一時的に接続が失われます。

デバイスのオンボーディング

ここでは、ネットワークに接続されている IACS アセットの管理に関連するさまざまなシナリオについて説明します。ここで説明するシナリオは、次のとおりです。

- 新しい IACS アセットの IES への接続
- オンボーディングされた IACS アセットの IES の別のポートへの移動
- オンボーディングされた IACS アセットのオフラインへの移行と復帰
- 欠陥のある IACS アセットが交換される

新しい IACS アセットのオンボーディング

この CVD では、新しい IACS アセットの正常なオンボーディングは、次のことを意味します。

- IACS アセットが Cisco Cyber Vision によって正常にスキャンされます。
- ISE が pxGrid プローブを使用して Cisco Cyber Vision から IACS アセット情報について学習します。
- IACS アセットが ISE に対するポートベースの認証および認可を正常に完了し、適切な SGT を受け取ります。
- IACS アセットが、セル/エリアゾーン内とセル/エリアゾーン間の両方のトラフィックフローを開始します。
- ディストリビューション スイッチ(Cisco Catalyst 9300)は、ISE からポリシーマトリックスをダウンロードしてから、IACS アセットによって生成されたトラフィックフローに適用することができます。
- SMC は、IACS アセットによって開始されたトラフィックフローを検出でき、IACS によって生成された悪意のある動作がある場合はアラームを生成できます。

上記のすべてのアクティビティが完了すると、このソリューションは、IACS アセットがネットワークに正常にオンボードされたと見なします。すべてのアクティビティが完了すると、IT セキュリティ アーキテクトは次の目的を達成したことになります。

- IACS アセットの可視性:デバイスのタイプ、位置(接続先)、IP アドレス、MAC アドレス。
- IACS アセットのセグメンテーション: ポリシーマトリックスを適用し、IACS アセットとの間のアクセスを制御します。
- フロー検出:IACS アセット間の通信の完全な可視性を実現します。
- マルウェアの検出:ネットワーク内の IACS アセットまたはその他のデバイスを、感染したデバイスから保護します。IT セキュリティ アーキテクトは、感染源の把握し、即時修復計画を立て実行することができます。

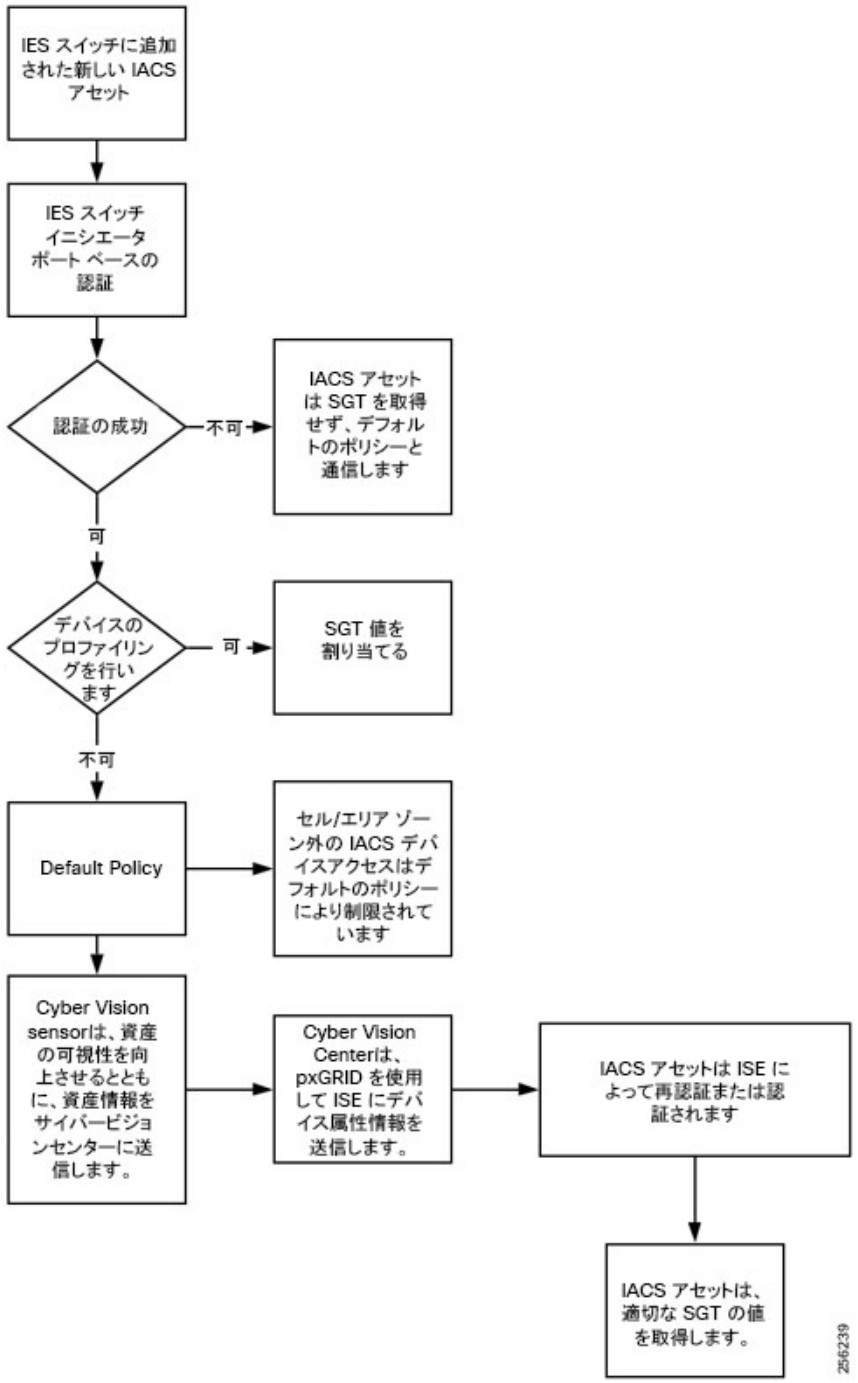
上記の説明では、タスクのどの部分が自動化され、ソリューションの展開においてどこがエンジニアに依存するのかを理解することが重要です。新しい IACS アセットがネットワークに接続されると、次のタスクが実行されます。

- アセットディスカバリ:Cisco Cyber Vision は、セル/エリアゾーンに新しい IACS アセットデバイスが追加されるたびにパッシブにモニタします。その結果、新しい IACS デバイスがネットワークに追加されると、デバイス属性情報は Cyber Visionによって学習され、この情報は pxGrid API を使用して ISE に送信されます。
- ISE による IACS アセットのプロファイリング:プロファイリング ポリシーは ISE で設定されることが予期されており(導入ガイドを参照)、IACS アセットを認証および認可する必要がある場合、ISE はポリシーを照合して適切な認証プロファイルを適用します(導入ガイドを参照) 。手動の介入は不要であり、このプロセスは設計どおりに実行されます。ただし、ISE が Cisco Cyber Vision から IACS アセットについて学習しておらず、そのイベントの前に IACS アセットがオンラインになった場合、ISE は単にデフォルト ポリシーを IACS アセットに適用します。
- ISE が IACS アセットの新しい属性を学習すると、再プロファイルし、IACS アセットに認可変更(CoA)を発行します。このプロセスでは、ISE に対する認証および許可の新しいインスタンスがトリガーされ、デバイスの SGT 値が再割り当てされます。
- NetFlow は、IACS アセットが接続できるすべてのポートで有効になっています。そのため、新しい IACS アセットが接続されるたびに、フローコレクタでトラフィックフローが自動的にキャプチャされます。OT 制御システム エンジニアや IT セキュリティ アーキテクトによる手動の介入は不要です。

- また、SMC は、収集した NetFlow データに対していくつかの機械学習アルゴリズムを有効にすることで、ネットワークで悪意のある動作が発生していないかどうかをモニタします。このプロセスも自動的に実行され、手動の介入は不要です。

図 84 新しい IACS アセットのオンボーディングに関する詳細なプロセス フロー図を示します。

図 84　新しい IACS アセットのオンボーディングに関するプロセス フロー図



オンボーディングされた IACS アセットの IES の別のポートへの移動

ここでは、IACS アセットが IES の別のポートに移動されるときのネットワークの動作について説明します。この例は、現在オンボードで、認証、承認済みで、SGT 割り当てが行われ、その後 IES の異なるポートへ移動される IACS アセットを対象としています。新しいポートの設定と以前のポートの設定が同じであることが前提となっています。このシナリオでは、次の手順が実行されます。

- ポートベースの認証(導入ガイドを参照)により、そこに接続されるすべてのデバイスが認証されます。そのため、IACS アセットは ISE に対して再認証される必要があります。
- ISE は、新しいデバイスがすでにプロファイリングされており、IP アドレスと MAC アドレスが一致していることを認識します。そのため、ISE は、IACS アセットを認可し、以前ポートで持っていた同じ SGT 値を発行します。
- IACS デバイスは、移動前と同じアクセスを持つことになります。

オンボーディングされた IACS アセットのオフラインへの移行と復帰

ここでは、オンボーディングされた IACS アセットがオフラインになり、ネットワークに復帰する状況について説明します。根本的な前提は、前のセクションと同様です。IACS アセットは、オフラインになる前に、SGT が割り当てられ、ポリシーマトリックスに基づいて他のデバイスと通信していました。デバイスが復帰すると、次の一連のイベントが発生します。

1. IACS アセットがエンドポイントデータストアに存在する場合、認証と認可は通常の方法で行われます。デフォルトでは、IACS アセットは PSN データベースに永続的に保存されます。そのため、長い時間が経過した後に IACS アセットが復帰した場合でも、IACS アセットは以前の特権を維持できます。
2. IACS アセットが何らかの理由でエンドポイントデータストアから削除されると、ISE は、IACS アセットを正しくプロファイリングできなくなり、デフォルトのポリシーが適用されます。
3. IACS アセットの再プロファイリングが必要な場合、OT 制御システムエンジニアは 、IND からデバイスを再スキャンする必要があります(導入ガイドを参照)。その後、ISE はデバイスを正しくプロファイリングできるようになり、元のアクセスを復元することができます。

障害が発生した IACS アセットの交換

ここでは、障害が発生した IACS アセットを交換するために OT 制御システム エンジニアが実行する必要のあるワークフローの項目について説明します。

1. 新しい IACS アセットは、以前の IACS アセットが接続されていたポートに接続される必要があります。
2. Cisco Cyber Vision は、セル/エリアゾーンに新しい IACS デバイスが追加されるたびにパッシブにモニタします。その結果、新しい IACS デバイスがネットワークに追加されると、デバイス属性情報は Cisco Cyber Visionによって学習され、この情報は pxGrid API を使用して ISE に送信されます。
3. ISE はデバイスを再プロファイリングし、CoA を発行して、SGT を IACS アセットに割り当てます。
4. このプロセス全体でも必要になるのは OT 制御システム エンジニアだけであり、残りのインフラストラクチャは自動的に処理されます。OT 制御システム エンジニアが実行する必要がある唯一のプロセスは新しいアセットをインストールしてスイッチに接続することです。

産業ゾーン:サイト運用と制御リファレンス

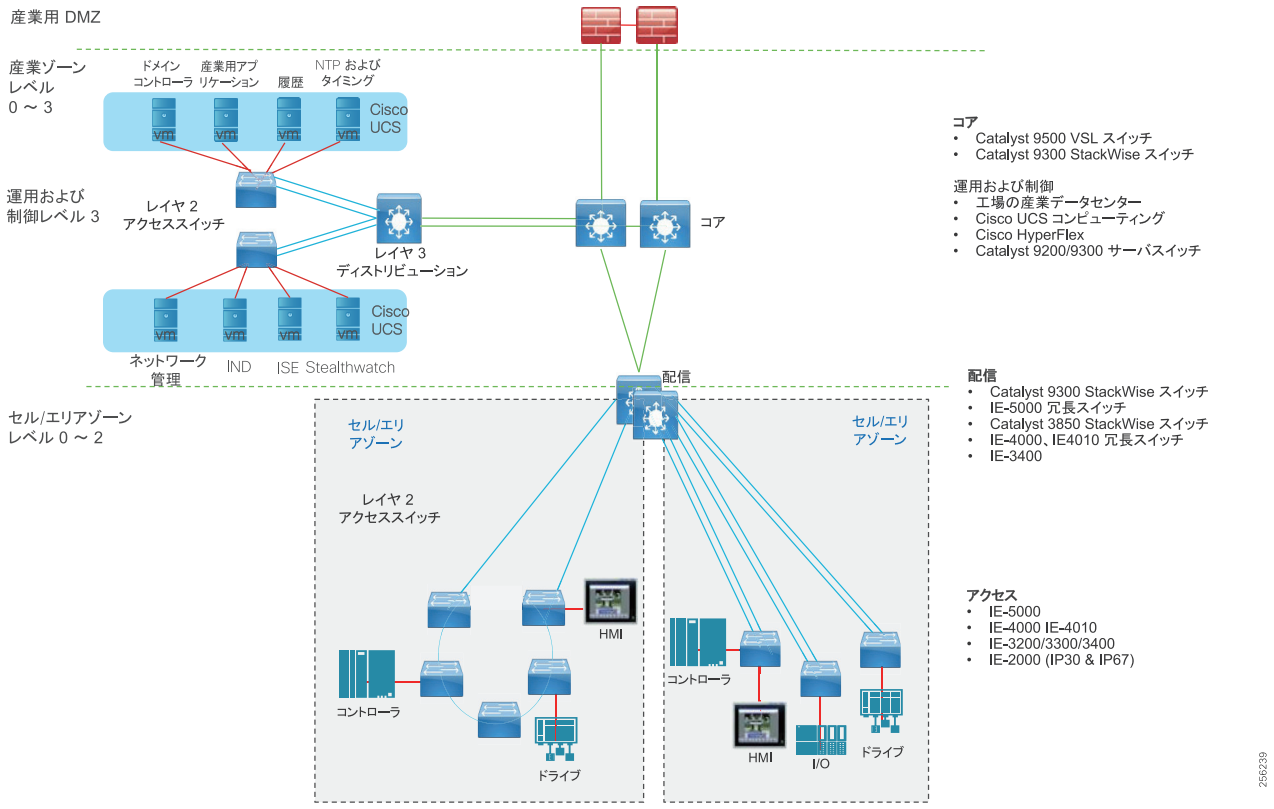
産業用オートメーションの主な目的は、セル/エリアゾーンのプラットフォーム、つまり Cisco IE および Cisco Catalyst 9300 スイッチの検証です。

図 82 の産業ゾーン リファレンスアーキテクチャには、産業用オートメーション内の運用および制御レベル 3 に導入されるサービスの一部の概要が示されています。アーキテクチャの主要な追加は、コアおよびディストリビューションレイヤの Cisco Catalyst 製品であり、可視性とセキュリティ管理プラットフォームも含まれます。

このレベルは、Purdue モデルのレベル 3 内で必要とされる機能を表しており、企業ネットワークモデルのコア/ディストリビューションと合致します。産業サイト運用および制御ゾーンは、履歴、アセット管理、工場フロアの可視化、モニタリング、レポート作成などの産業用アプリケーションおよびサーバを提供します。これらのアプリケーションは、工場または産業用データセンターで実行されます。IND、ISE、Stealthwatch などのネットワーク管理サービスおよびセキュリティ サービスがこのレベルで導入されます(「OT インテントベースのネットワーキング セキュリティ(93 ページ)」を参照)。このレベルでは、セル/エリアゾーンとサイト運用および制御内のアプリケーションの間でトラフィックをルーティングするためのネットワーク機能が提供されます。コアおよびディストリビューションでは、工場全体の接続をサポートするとともに次の重要な機能を提供するレイヤ 3 ルーティング プロトコルが実行されます。

- さまざまなセル/エリアの IACS ネットワークの相互接続
- レベル 3 サイト製造システムの相互接続
- レベル 0 ～ 3 システムおよびデバイスへのネットワーク管理サービスとセキュリティ サービスの提供
- 工場産業用 DMZ へのインターフェイス

図 85　サイト運用および制御



サイト運用および制御の産業特性

大部分の産業工場施設では、このアーキテクチャ レイヤに、セル/エリアゾーンレベル 2 以下とは大きく異なる物理環境があります。ネットワーキングの特性としては、産業用プロトコルのリアルタイム パフォーマンスがそれほど重視されず、機器は、環境的に管理されたエリア、キャビネット、または部屋に設置されます。

以下に、サイト運用および制御の設計上の重要な考慮事項を示します。これらは、プラットフォームの選択、ネットワーク トポロジ、セキュリティの実装、および全体的な設計に直接影響します。

- 産業特性:環境条件、工場のレイアウト、およびケーブル接続コストはすべて、設計におけるプラットフォームの選択とネットワーク トポロジに影響を与えます。すでに詳しく説明したように、産業工場および加工施設のセル/エリアゾーンには、通常、物理的に強化されたプラットフォームが必要です。一般的な位置と管理の戦略は、レベル 3 では変更されます。工場をサポートするためのアプリケーションがインストールされるネットワーキング プラットフォームおよびサーバは、通常、工場フロアではなく環境的に制御されたエリアに配置されます。このため、従来の IT プラットフォーム(Cisco Catalyst 9500/Cisco Catalyst 9300/Cisco Catalyst 9200 製品など)や、IACS、セキュリティ、およびネットワーク管理アプリケーションがインストールされるシスコの非強化型 UCS プラットフォームの選択に対応するプラットフォームの選択の基準が変わります。

- 相互運用性と相互接続性:産業ゾーン内のこのレベルで要求される重要な要件の 1 つは、セル/エリアゾーン間の相互ネットワーキングと工場全体の通信の提供です。レイヤ 3 は、さまざまなセル/エリアゾーンをサイト運用および制御に接続し、IDMZ からのパスを提供するために必要です。コアおよびディストリビューション レイヤ スイッチは、このルーティングを提供し、セル/エリアゾーン間のトラフィックに必要となる可能性があるパフォーマンスまたは QoS の要件に適合します。

- リアルタイム通信、確定性、およびパフォーマンス:IACS ネットワーク内のパケットの遅延とジッタは、基盤となる産業プロセスに大きな影響を与える可能性がありますが、レベル 3 サイト運用および制御では、この要件はセル/エリアゾーンの要件とは大きく異なります。クリティカルな I/O リアルタイムトラフィックは、通常、セル/エリアゾーンに制限されます。インターロック PLC タイプのトラフィックはセル/エリアゾーンの間を転送される可能性があるので、このトラフィックのプライオリティ付けを容易にするために、QoS モデルをこのレイヤで設定する必要があります。サイト運用レベル 3 とセル/エリアゾーンの間の大部分のトラフィックフローは、一般に、産業用アプリケーションの観点からは非リアルタイムであるため、一般的なパフォーマンス基準は、パケット遅延、レイテンシ、およびジッターの影響をあまり受けません。

- アベイラビリティ:産業用オートメーション内の重要なメトリックは、総合設備効率(OEE)です。このレベル 3 でもアベイラビリティは依然としてネットワークの重要な要件です。このレイヤのアプリケーションはセル/エリアゾーンよりもネットワークの停止に対して復元力がある場合がありますが、セル/エリアゾーン内の運用を維持するためにそれらを利用可能であることは依然として重要です。レイヤ 3 境界を通過するトラフィックをサポートするために、復元力ネットワーク プロトコルと QoS に対処する必要があります。

- セキュリティ:セキュリティ、安全性、およびアベイラビリティは、産業用セキュリティフレームワーク内で緊密に連携しています。産業用ネットワークのセキュリティについて検討する場合、顧客は、環境を安全で運用可能な状態に保つ方法に関心を持っています。制御システムとプロセスドメインを保護するためのアーキテクチャ的アプローチに従うことをお勧めします。

- 推奨モデルは、制御階層の Purdue モデル、International Society of Automation 95(ISA95)と IEC 62443、NIST 800-82、および変電所用の NERC CIP です。デバイスと IACS アセットの可視性、ネットワークへの安全なアクセス、アセットのセグメンテーションとグループ化といった、セル/エリアゾーンをサポートするための重要なセキュリティ機能が、このレベル 3 で設定されます。インフラストラクチャを保護するために、ネットワーク強化(制御プレーンとデータ プレーン)が設定されます。

- 管理:産業ゾーンとサイト運用および制御レイヤ内では、一貫した管理戦略が必要です。OT ペルソナと IT ペルソナの組み合わせによってセル/エリアゾーンに運用上の焦点が合わされている場合、運用および制御レベル 3 にはセキュリティ プラットフォームと IT プラットフォームが存在し、そのことが IT スキルセットの向上を促進します。ネットワークの管理とセキュリティには、セキュリティ アーキテクト、IT 担当者、および OT 制御エンジニアが連携し、共通ネットワーク管理フレームワーク全体で一体となって作業する必要があります。

- トラフィック タイプ:サイト運用および制御のこのレベルのトラフィックフローは、主に、履歴、アセット管理、IACS アラーム/レポート、およびネットワーク/セキュリティ管理アプリケーション(ISE、NetFlow、IND 検出)などの IACS アプリケーションをサポートします。セル/エリアゾーンの IACS アプリケーションをサポートしていると見られるマルチキャストトラフィックは、セル/エリアゾーンから出ないため、このレベルでは見られません。

サイト運用および制御のレベル 3 コンポーネント

上記のモデルは、従来の企業ネットワークモデルの概念を利用した中規模から大規模の工場モデルを表しています。レベル 3 ドメイン内にはコア、ディストリビューションが存在し、EIGRP や OSPF などの通常のルーティング プロトコルによって工場全体のネットワーキングを提供します。このコアは、「工場データセンター」への接続性を提供します。工場データセンターでは、Cisco UCS に産業用アプリケーションとその産業施設のネットワーク管理/セキュリティ機能（レベル 3 以下）が搭載されます。これらのコア スイッチは、産業用 DMZ と送受信する通信のための接続性を提供します。

産業データセンター内では、Cisco Catalyst 3850 または Cisco Catalyst 9300 が、データセンターに導入されたサーバの接続性を提供します。また、仮想ホスト アプリケーション用の物理ハードウェアを提供するために Cisco UCS が導入されます。このフェーズでは、セル/エリアゾーン コンポーネントで以前に強調表示された Cisco Catalyst 9300 スイッチが、産業用データセンターの接続性を提供しました。ただし、どのデータセンター設計でも、ホストされるアプリケーションのパフォーマンス要件と、これらのアプリケーションをサポートするためのネットワーク要件を考慮する必要があります。

シスコのサイト運用および制御のホステッド アプリケーション

シスコのセキュリティプラットフォーム

- Cisco ISE：前述のように、ISE は産業用データセンターに導入されています。ISE PSN は、このレイヤに置かれます。PSN は、アセット認証、認可、プロビジョニング、プロファイリング、およびポスチャ サービスを提供します。PSN は、接続されたデバイスにアクセスポリシーを適用します。

- Cisco Stealthwatch：Stealthwatch は、産業用データセンターでホストされます。Stealthwatch は、ネットワーク可視性とセキュリティ分析によって脅威に対する防御を向上させます。StealthWatch は、膨大な量のデータを収集して分析し、きわめて大規模で動的なネットワークさえも内部を包括的に可視化して保護します。

ネットワーク管理

Cisco IND：IND は、産業用データセンターでホストされることができます。これにより、セル/エリアゾーン内のアセットやネットワーキング機器を管理および通信し、ネットワークに接続されている IACS アセットに可視性を提供します。IND は、PLC、IO、HMI、ドライブなどのオートメーションデバイスを検出するために、CIP、PROFINET、OPC-UA、Modbus、BACnet などの産業用オートメーションプロトコルをサポートしており、オートメーションおよびネットワーキングアセットの統合トポロジマップを提供します。このマップにより、運用部門と工場 IT 担当者に産業用ネットワークを管理および維持するための共通フレームワークが提供されます。

Cisco DNA Center は、産業用オートメーションのこのフェーズでは検証されていませんが、Cisco Catalyst 製品の管理プラットフォームとして配置できます。これは、より IT に特化したナレッジベースを必要とするツールと協調して、制御エンジニアや産業要件と連携して動作します。

時刻の同期

時刻同期は、産業用インフラストラクチャ全体と相関関係を持つイベントおよびデータ分析にとって不可欠です。ただし、セル/エリアゾーンごとに孤立した時間が維持される場合があります。Network Timing Protocol（NTP）またはPrecision Time Protocol（PTP）をすべてのインフラストラクチャ コンポーネントで有効にして、一貫性のあるタイミングを維持し、イベントの相関関係を工場全体で提供できるようにする必要があります。これは、産業ゾーン全体からセル/エリアゾーンいたるまでのレベル 3 で有効にする必要があります。

共通ネットワークベース サービス

- DNS：工場環境内では、通常、専用 DNS サーバが産業ゾーン内のアプリケーション用に導入されます。

- DHCP：DHCP サービスは産業ゾーン全体に導入できますが、有線 IACS デバイス内では、IP アドレッシングは通常静的に定義されます。「セル/エリアゾーンの IP アドレス指定（42 ページ）」を参照してください。

- ドメインコントローラ/ディレクトリサービス：これらは通常、産業ゾーン専用ですが、IDMZ アーキテクチャを使用して企業と同期することもできます。CPwE IDMZ CVD に、EtherNet/IP 環境向けに企業と産業ゾーンの間で複製されるサービスに関する詳細が記載されています。

ネットワーク設計の概要

クリティカルな I/O リアルタイムトラフィックは、通常、セル/エリアゾーンに制限されます。インターロック PLC タイプのトラフィックはセル/エリアゾーンの間を転送される可能性があるので、このトラフィックのプライオリティ付けを容易にするために、QoS モデルをこのレイヤで設定する必要があります。サイト運用レベル 3 とセル/エリアゾーンの間の大部分のトラフィックフローは、一般に、産業用アプリケーションの観点からは非リアルタイムであるため、一般的なパフォーマンス基準は、パケット遅延、レイテンシ、およびジッターの影響をあまり受けません。レイヤ 3 はこのレベルで設定され、レイヤ 3 ネットワークのコンバージェンス時間は、トラフィックフローのサポートに組み込まれる必要がありますが、通常はこれで十分であると認識されています。

ハイ アベイラビリティ

次に、コア ルーティングとレイヤ 3 スイッチの復元力について説明します。レイヤ 3 ルーティングは、セル/エリアゾーンを集約するディストリビューションスイッチからレベル 3 で開始されます。レベル 3 サイトの運用および制御トラフィックのパフォーマンス要件は、セル/エリアゾーンおよび産業ゾーンとは大きく異なります。表 37 セル/エリアゾーンとコントロールレイヤ間の一般的なトラフィックの情報/プロセス時間を強調表示します。サイクルタイムは 2 つ目の列に示されている範囲ですが、これは製品に依存するため、やはりアプリケーションのパフォーマンスメトリックを把握することを検討する必要があり、それをネットワーク アベイラビリティ設計で考慮する必要があります。

表 37　IACS アプリケーション要件の例

要件クラス	一般的なサイクル時間	一般的な RPI	接続タイムアウト
情報/プロセス(HMI など)	1 秒未満	100 ～ 250 ミリ秒	製品に依存
たとえば、RSLinx の場合は 20 秒			
速度が重視されるプロセス(I/O など)	30 ～ 50 ミリ秒	20 ミリ秒	RPI の 4 間隔(ただし、100 ミリ秒に相当)
安全性	10 ～ 30 ミリ秒	10 ミリ秒	24 ～ 1000 ミリ秒
モーション	500 マイクロ秒～ 5 ミリ秒	50 マイクロ秒～ 1 ミリ秒	4 間隔

サイト運用および制御ネットワークのアベイラビリティに関する設計ガイダンスと推奨事項の概要を次に示します。

- コアとディストリビューションスイッチ間のレイヤ 3 ルーティング(大規模な工場展開)
- アクティブ/スタンバイまたは仮想スイッチの冗長性の特徴と機能を備えた冗長コアおよびディストリビューション ルータ。これには、ディストリビューションの Cisco Catalyst 9300 用のスタッキングまたは HSRP、ディストリビューションの Cisco IE 5000 用の HSRP、およびコアの Cisco Catalyst 9500 用の StackWise Virtual が含まれます。
- IDMZ とコア/ディストリビューション ルータの間のレイヤ 3 ルーティング。
- アーキテクチャ全体の冗長リンク
- すべてのネットワーキングデバイスの設定のバックアップ(cisco IND は Cisco IE スイッチに使用できます)
- ネットワークインフラストラクチャの管理、制御、およびデータプレーンを保護するためのネットワーク強化のベストプラクティス
- 同様の専用機能を持つ IACS アプリケーションのセグメント化。または、クリティカルなアプリケーションの、クリティカルでないアプリケーションから独自の VLAN への分離。たとえば、セル/エリアゾーンをサポートする産業用アプリケーションとは異なる VLAN にセキュリティおよびネットワーク管理を維持します。これにより、ホストが感染した場合のセキュリティとアベイラビリティが向上するため、レイヤ 3 境界デバイスを導入して、感染した VLAN の外側にあるデバイスを保護できます。
- セル/エリアゾーンで説明されているレイヤ 2 冗長スタートポロジは、サーバスイッチ接続用に導入されます。
- サーバから冗長スイッチへのデュアル NIC 接続性。仮想サーバからのデュアル NIC テクノロジー。
- サーバ、仮想サーバ、およびアプリケーションの冗長性(必要な場合)
- 産業ゾーンとの間の不正アクセスを防止する IDMZ

管理

ネットワークインフラストラクチャ用のレベル 3 のサポートモードにはシフトがあります。一般的に、レベル 3 以上では、サポートスタッフの IT に対する意識が高まります。導入されるセキュリティアプリケーションには、より高い IT スキルセットが必要です。それでも、ネットワークが依然として直感的でサポートしやすいものである必要があるという事実に変わりはありません。ネットワーク インフラストラクチャの管理をサポートするために役立つガイドラインと大まかな設計上の推奨事項は、次のとおりです。

- 可能な場所に個別のアウトオブバンド管理ネットワークを実装します。少なくとも、専用の管理 VLAN を提供します。
- ロギングは、適切なセキュリティおよびネットワーク管理戦略に不可欠な要素です。ネットワーク インフラストラクチャは、ロギング機能と、集中型セキュリティ管理システムへのレポート機能を使用して設定する必要があります。SNMPv3 とともに Syslog を有効にして、エンドポイントで検出されたイベントまたはインシデントがレポートされるようにする必要があります。
- 検証されてはいませんが、Cisco DNA Center または Cisco Prime Infrastructure は、このレイヤに配置されている Cisco Catalyst 製品を管理できます。Cisco Prime® Infrastructure 3.1.7 DP13、Cisco DNA Center、オンボード Cisco IOS XE ソフトウェア ウェブ ユーザインターフェイス、SNMP、または Netconf/YANG を使用して、Cisco IOS ソフトウェアコマンドラインインターフェイス(CLI)を使用して Cisco Catalyst 9000 シリーズのスイッチを管理できます。
- UCS サーバ管理の推奨事項は、このドキュメントの対象外です。産業用データセンターの物理サーバと仮想サーバの管理は、プラットフォームの選択、ストレージ アーキテクチャ、および仮想化ベンダーによって異なります。

セキュリティ

セグメンテーション

- 産業用データセンター内での、同様の専用機能を持つ IACS アプリケーションのセグメント化。または、クリティカルなアプリケーションの、クリティカルでないアプリケーションから独自の VLAN への分離。
- 高度なセグメンテーションのためのセル/エリアゾーンのユースケースのとおり、Cisco Cyber Vision、Cisco ISE、および TrustSec を使用したポリシーの適用。ポリシーの適用とセグメンテーションは、産業オートメーションのディストリビューション スイッチで管理されます。
- TrustSec が導入されていない場所への導入では、ドメインのセキュリティポリシーを提供するために ACL を使用する必要があります。
- レベル 3の、コアの、ディストリビューション、および産業データセンターのすべての NetFlow 対応スイッチで NetFlow を有効にして、Stewatch にエクスポートすると、工場全体のアプリケーショントラフィックとネットワークトラフィックが表示されます。これを使用することで、基準トラフィックプロファイルの提供と、ネットワークデータフローの異常の識別が容易になります。

ネットワークの強化

「ネットワーク強化:システム整合性のコンポーネント(90 ページ)」に示されている前提とガイダンスに従って、コントロール プレーン、管理プレーン、およびデータ プレーンを保護します。

サーバ強化の作業とエンドポイント セキュリティ

サーバ強化の作業の例は、次のとおりです。

- オペレーティングシステムのパッチおよびアップグレード:攻撃に対する脆弱性を軽減するため、システムは、最新のベンダー推奨ソフトウェアおよびファームウェアレベルにパッチを適用する必要があります。パッチは、必ず、実装前にテストしてください。パッチの実装計画を検討する必要があります。
- 不要なサービス、アプリケーション、およびネットワーク プロトコルの削除または無効化。
- OS ユーザ認証:最小権限アクセスを使用します。
- ホストベースの IDS および脆弱性スキャンとエンドポイント セキュリティ。実装時には、セキュリティ システムがアプリケーションのパフォーマンスに与える影響を考慮してください。
- セキュアなネットワーキングプロトコル:SFTP(セキュアファイル トランスファー プロトコル)、SCP(セキュアコピー)、および SSH(セキュアシェル)、および SNMPv3。

- バックアップデータベースまたは冗長データベース
- アプリケーションのアベイラビリティをサポートするための冗長サーバおよびネットワーキング。

サイト全体の正確な時間:設計上の考慮事項

このセクションでは、IEEE 1588-2008 Precision Time Protocol version 2(PTPv2)に基づくサイト全体の正確な時間について説明します。このセクションは、正確な時間のビジネス上の価値から始まり、その他のタイミングの概念について説明し、基本的な PTP アーキテクチャの概要を示し、サイト全体の正確な時間を導入するための設計上の考慮事項と推奨事項を提供します。

注:読者は、次のような高精度時間の標準とプロファイルを紹介する関連セクションを確認する必要があります。

- 時刻の同期(136 ページ)
- PRP を介した PTP(203 ページ)
  - PRP を介した PTP の設定(206 ページ)
  - PRP を介した PTP のトラブルシューティング(207 ページ)
- PTP グランドマスターとしての Cisco IE 5000(209 ページ)
  - PTP グランドマスターの設定(209 ページ)
  - PTP グランドマスターのトラブルシューティング(209 ページ)

はじめに

正確な時間が必要な理由

産業用自動化ソリューションは、IoT およびインダストリー 4.0 イニシアチブを推進する産業企業にとって重要な基盤となります。このソリューションは、IACS システム、デバイス、およびアプリケーションを安全に接続することによって、予知メンテナンス、デジタルツイン、ビッグデータ分析などの IoT アプリケーションを促進するための豊富なデータへのアクセスを可能にします。そのようなデータは、生成時に正確に把握されていると、価値が著しく高まります。これらの IoT 分析アプリケーションは、一貫性のある正確な時間認識に基づいて、より良い結果(たとえば、因果関係)を導き出せます。

さらに、このソリューションでサポートするように設計された主要な IACS アプリケーションは、ますます運用を実行するための正確な時間を必要とするようになっています。PTP は、一般的な(つまり、ネットワークベースの)正確な時間を提供します。アプリケーションは、これを使用して一定の範囲内のデバイスからの検知情報を処理して分析することができます。IACS の標準規格およびプロトコルは、イベントのシーケンスやモーションコントロール アプリケーションなどのさまざまな機能をサポートするために PTP を採用し始めています。この例としては、ODVA, Inc. の Common Industrial Protocols Sync (CIP-Sync)機能、OPC Foundations の統合アーキテクチャ、および、変電所の自動化のための IEC 61850 が含まれます。

通常、産業用制御システムには、表 38に示されているような時間の精度要件があります。[1]

表 38　産業制御システム:時間の精度要件

アプリケーション	精度	備考
変電所	10 マイクロ秒	絶対時間
電気グリッド	1 マイクロ秒	絶対時間
動作制御	500 マイクロ秒～ 5 ミリ秒	4 つの間隔
ドライブ	1 マイクロ秒	相対時間
IO	30 ～ 50 ミリ秒	RPI の 4 つの間隔
安全性	10 ～ 30 ミリ秒	RPI の 4 つの間隔

1. https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

NTP、IRIG-B、および PTP は、表 39に示されているように、上記の要件を満たすために開発された 3 つの一般的な時間同期プロトコルです。[1]

表 39　時刻同期プロトコル

プロトコル	メディア	精度
NTP	イーサネット	50 ~ 100 ミリ秒
IRIG-B	同軸	1～10 ミリ秒
PTP	イーサネット	20-100 ns

より正確な時間を必要とするアプリケーションおよびデータに対する顧客やアプリケーションの要求を受け、このソリューションでは、機能として、正確な時間のサイト全体へのディストリビューションがサポートされるようになりました。

その他のタイミングテクノロジー

ネットワーク内のデバイスとアプリケーションの同期は、新しい問題ではなく、いくつかの方法で対処されます。精度の低い要件を持つ多くの IT アプリケーションでは、Network Time Protocol（NTP）を使用します。産業用アプリケーションでは、GPS が特定のデバイスに使用されていたか、または IRIG がオーバーレイネットワークで時間を配布するために使用されていました。IRIG は、オーバーレイネットワークの導入をベースにしているため、コストは大幅に増加します。これで、PTP は、統合されたオープンな標準ネットワークに正確な時間を分散するという問題を解決しました。PTP の前に、高い精度を実現するために、独自の通信規格とオーバーレイネットワーク（たとえば、IRIG-B）が必要です。タイミングテクノロジーの概要を次に示します。

- グローバルポジショニングシステム（GPS）：正確な時刻と GEO ロケーションは、サテライトベースの信号を受信するデバイスによって実現されます。他の同様のサービスは、ロシア（GLONASS）、中国（BeiDou）、欧州（Galileo）によって開発されています。
- 国際射程間計装グループ（IRIG）タイムコード：PTP 以前、これは非イーサネット、単一機能のテクノロジーに基づいてネットワーク全体に正確な時間を配布するための最も一般的な手段でした。
- Network Time Protocol（NTP）：IT システムで一般的に見られる時間を配布するためのオープン スタンダード プロトコル（現在のバージョンは IETF RFC 5905）。
- 同期イーサネット（SnycE）：通信業界で一般的に使用されているイーサネットで正確な時間を配布するための ITU ベース方式。

このソリューションは、サイト全体のネットワーク上で PTP を介して正確な時間を配布することに重点を置いています。このアーキテクチャでは、GPS（または類似のシステム）または IRIG を使用して、協定世界時（UTC）と連動したアライメントを確立できます。

PTP アーキテクチャの概要

PTP（IEEE 1588 v2）標準規格では、ネットワーク上で時間が伝達される際の遅延とジッターの補正において、時間を正確に配布するための一連のメカニズムとアルゴリズムが提供されています。このプロトコルは階層形式で動作し、スレーブがクロックをマスタークロックと同期するデバイス間のマスター/スレーブ関係を確立します。IACS デバイスおよび IES は、マスターとスレーブの間で時間の差を修正できる情報を含む PTP イベントメッセージを送受信することによって、時刻の同期を維持します。

クロック階層を構築し、マスターまたはスレーブとして割り当てられるデバイスを決定するプロセスは、ベスト マスター クロック アルゴリズム（BMCA）を使用して実行されます。PTP 対応のクロックがネットワークに参加すると、PTP アナウンス メッセージと呼ばれる PTP メッセージをリッスンします。これらのメッセージには、タイムソース、クロック品質、プライオリティ番号などの情報が含まれています。BMCA は継続的に実行され、アナウンスメッセージの情報を使用して、必要に応じてこれらの割り当てと調整を行います。BMCA は「グランドマスター」クロックを確立し、ネットワーク インフラストラクチャの設定と機能に応じて、時間を配布するために使用されるマスタークロックとスレーブクロックの階層を構築します。

1. https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp030_-en-e.pdf

コンポーネント

PTP は、時間の配布を実行するための次の主要な役割を識別します。

- グランドマスタークロック（GM）
- オーディナリ クロック（OC）
- トランスペアレント クロック（TC）
- 境界クロック（BC）

グランドマスタークロック（GMC）

グランドマスタークロックは、PTP ドメイン内の時刻のプライマリソースです。GMC は、BMCA アルゴリズムによって選択されます。GMC は、高品質のオシレータを必要とし、たとえば GPS レシーバーから、UTC に同期される必要があります。

- サイト全体に正確な時間を配布するには、特定の「グランドマスター」デバイスを取得して複数の復元力を確保し、ネットワークアーキテクチャの製造/サイト全体のアプリケーションレベルの一部として運用することをお勧めします。

  または：

- 2 台の Cisco IE 5000 アグリゲーションスイッチを、GPS への適切なアクセス（または同様のサテライトベースの時間）または IRIG 接続を使用して、UTC に合うように GMC として確立します。

オーディナリ クロック（OC）

オーディナリクロックは、1 つの PTP ポートを持つデバイスです。これは PTP トポロジのエンドノードとして機能します。どのクロックも、他のクロックの有無に応じて、PTP ドメイン内のマスターまたはスレーブとして BMCA によって選択できます。オーディナリクロックは、システムのエンドノードとして使用されるため、PTP システムで最も一般的なクロックタイプです。IACS アプリケーションのオーディナリクロックの一般的な例としては、プログラマブル自動化コントローラ（PAC）や I/O デバイスがあります。

境界クロック（BC）

境界クロック（BC）は、マルチ PTP ポートデバイス（たとえば、IE スイッチ）です。BC は、透過的なクロックとともに、ネットワークを通じて時間を配布します。グランドマスターとして選択されていない場合、グランドマスターが到達可能な境界クロックのポートは「スレーブ」ポートになります。スレーブクロックとして、BC は内部クロックをマスターに同期します。その後、境界クロックは、IACS および他のポートに接続されているネットワークデバイスのマスターになります。これらのポートに接続されている他のクロックは、BC にスレーブになり、BC の内部クロックと同期します。BC は、GM がすべての OC クロックの PTP メッセージに応答する必要がないようにします。これは、重要なスケーリング上の考慮事項です。

また、BC は、GMC から受信した時間プロパティを無期限に保持するように設定することもできます。これは、デバイスの停止または接続の損失が原因で GM が使用できない場合に便利です。このような状況では、BC は一貫したタイム ディストリビューション サービスを維持し、これらのサービスに依存している IACS のアベイラビリティを維持します。この場合、お客様は、長期にわたって一貫した品質の時間を提供するように設計されたネットワークデバイスも考慮する必要があります。たとえば、温度補償水晶発振器（別名 TCXO）や恒温槽型水晶発振器（OXCO、たとえば Cisco IE 5000 は Stratum 3E です）があります。また、BC を使用して、PTP を異なる VLAN に配布することもできます。

また、BC クロックタイミングの設定が変更されたときに起動して再設定するのに時間がかかり、さらに多くの設定が必要になり、BC の深さが増えるにつれて、より大きな誤差が生じる傾向があります。

トランスペアレント クロック（TC）

トランスペアレントクロック（TC）は、ネットワーク インフラストラクチャ デバイスが時間を配布するためのもう 1 つの方法です。TC は、ネットワーク タイミングパケットの時間間隔フィールドの遅延を測定および考慮します。これにより、スイッチはネットワーク上の他のマスターおよびスレーブノードに一時的に透過的になります。TC は、遅延補正を PTP パケットに挿入することによって、ネットワーク全体の遅延を補正します。TC は PTP 階層内のノードにはなりません。したがって、マスタークロックもスレーブクロックにもなりません。TC は、マスタークロックとスレーブクロックの間でインラインに配置され、これらのデバイス間の時間訂正を提供します。

PTPv2 仕様では、次の 2 種類のトランスペアレントクロックが定義されています。

- エンドツーエンド（E2E）のトランスペアレントクロックは、ネットワーク内のデバイスが PTP パケットを処理して転送するまでの時間を測定することによって、ネットワーク全体の遅延を補正します。これらの測定値は、PTP パケットの修正フィールドに追加されます。このメカニズムは、両方のブラウンフィールドで動作します。ブラウンフィールドでは、ネットワーク インフラストラクチャ デバイスが PTP およびグリーンフィールドをサポートしません。グリーンフィールドでは、すべてのネットワーク インフラストラクチャ デバイスは PTP シナリオをサポートします。
- ピアツーピア（P2P）トランスペアレントは、ネットワーク全体に遅延測定値を配布します。これは、すべてのデバイスが PTP に準拠している必要があることを意味します。P2P TC は E2E TC と互換性がありません。P2P は、ユーティリティプロファイルの一部として指定され、サブステーションのユースケースで使用されます。P2P TC は、CI 同期アプリケーションでは使用されません。

また、TC クロックは、GM クロックタイミングの設定が変更された場合に、より迅速に起動して再設定する傾向があります。設定がほとんど必要なく、規模が拡大するほど正確な時間を維持する傾向があります。

このサイト全体の正確な時間配布の設計では、アクセスレベルのスイッチに E2E を使用する TC を推奨しています。

耐障害性

前述したように、産業用オートメーションおよび制御アプリケーション、およびそれらにアクセスする関連 IoT アプリケーションにとって、ネットワークベースの重要な機能として、正確な時間が重要になってきています。したがって、正確なタイミング機能が利用でき、実稼働運用のために一貫性があることが重要です。ここでは、PTP の復元力に関する考慮事項について説明します。

グランドマスタークロック

機能しているグランドマスターは、ネットワーク内で正確な時刻を一貫して配信するための要件です。BMCA は、グランドマスターが選択されていること、接続またはサービスが失われた場合に、2 つ目または 2 つの範囲内で別の選択肢が迅速に適用されることを保証します。このソリューションでは、一貫した時間を提供するために、ネットワークの製造ゾーンに冗長なサードパーティ製のグランドマスターデバイスを使用することを推奨します。さらに、このソリューションでは、特定の GM デバイスへの接続またはサービスが失われた場合に、特定の順序のグランドマスター「フェールオーバー」を確保するために、ネットワークインフラストラクチャの優先順位を設定することを推奨します。BMCA には次の GM プライオリティを設定することを推奨します。

1. サードパーティ製グランドマスター
2. コア スイッチ
3. アグリゲーションスイッチ
4. GM 機能対応のコントローラデバイス

これにより、時間プロパティの永続化設定とともに、ネットワーク接続が使用可能である限り、ネットワーク接続やサードパーティ製 GM サービスが復元され、PTP サービスが使用可能で一貫性があり、それに依存する IACS システムの中断を回避するために、単一のグランドマスターを使用できるようになります。詳細については、「サイト全体の PTP 設計の考慮事項（144 ページ）」を参照してください。

ネットワーク インフラストラクチャ

この産業用自動化ソリューションの大部分は、コア、アグリゲーション、およびアクセスレイヤでネットワークの復元力について説明するためのものです。特に、EtherChannel およびリングプロトコル（たとえば、REP、スパニングツリー、MRP、DLR、PRP、および HSR）などのレイヤ 2 の復元力プロトコル、およびレイヤ 3 機能のための仮想スイッチング、スイッチスタッキング、HSRP などのネットワークの復元力機能が使用されます。

残念ながら、PTP はこれらのプロトコルと機能のすべてでサポートされているわけではありません。PTP は現在、EtherChannel リンク、HSR、MRP、仮想スイッチバンドル、スタック構成スイッチ、またはレイヤ 3 リンクではサポートされていません。このソリューションでは、製造ゾーン内およびコアスイッチからアグリゲーションスイッチにかけての GMC 間で、個別のシングルパスレイヤ 2 接続を確立することを推奨します。製造ゾーン GMC への接続にシングルポイント障害が発生する可能性がありますが、プライオリティと BMCA の設定により、接続とサービスが再確立されるまで、品質のデバイスが GM 機能を迅速に引き継ぐ準備ができていることが保証されます。

このようにして、PTP サービスは、耐障害性の高いネットワークと正確なタイムサービスを提供する、復元力のあるネットワークインフラストラクチャとトポロジを介してサイト全体に配布されることができます。このソリューションでは、スパニングツリーまたは REP マネージドリング/マルチパスセル/エリアゾーントポロジに正確な時間を配布することを推奨しています。サブステーションの自動化ソリューションでは、電力プロファイルを適用することで、PRP トポロジを介した PTP が使用されます。

さらに、サイト全体で PTP をサポートするには、お客様が、一致したスイッチ間の HSRP を基にした、復元力のあるアグリゲーションおよびコア ネットワーキングサービスを維持することをお勧めします。

コンポーネント

サイト全体の高精度な時間の配布をテストするために使用されるコンポーネントを表 40に示します。

表 40　テストで使用されるコンポーネント

製品の役割	製品	ソフトウェアバージョン	備考
アクセス	Cisco IE 4000	15.2 (7) E0s	テスト対象ユニット（UUT）：境界とトランスペアレントクロック E2E
アクセス	Cisco IE 3000	15.2 (7) E0s	UUT：トランスペアレントクロック E2E
アクセス	Cisco IE 3400	16.11.1 a(ED)	UUT：トランスペアレントクロック E2E
配信	Cisco IE 5000	15.2 (7) E0s	UUT：境界クロック
コア スイッチ	Cisco Catalyst 9300	16.9.2	UUT：境界クロック
グランドマスタークロック	MeinBerg LANTime M600	6.24.021	サードパーティ製 GPS ベースの GM
PTP 分析ツール	Calnex Paragon-X	27.10.40	PTP プロトコル/パフォーマンスアナライザ

アーキテクチャの概要

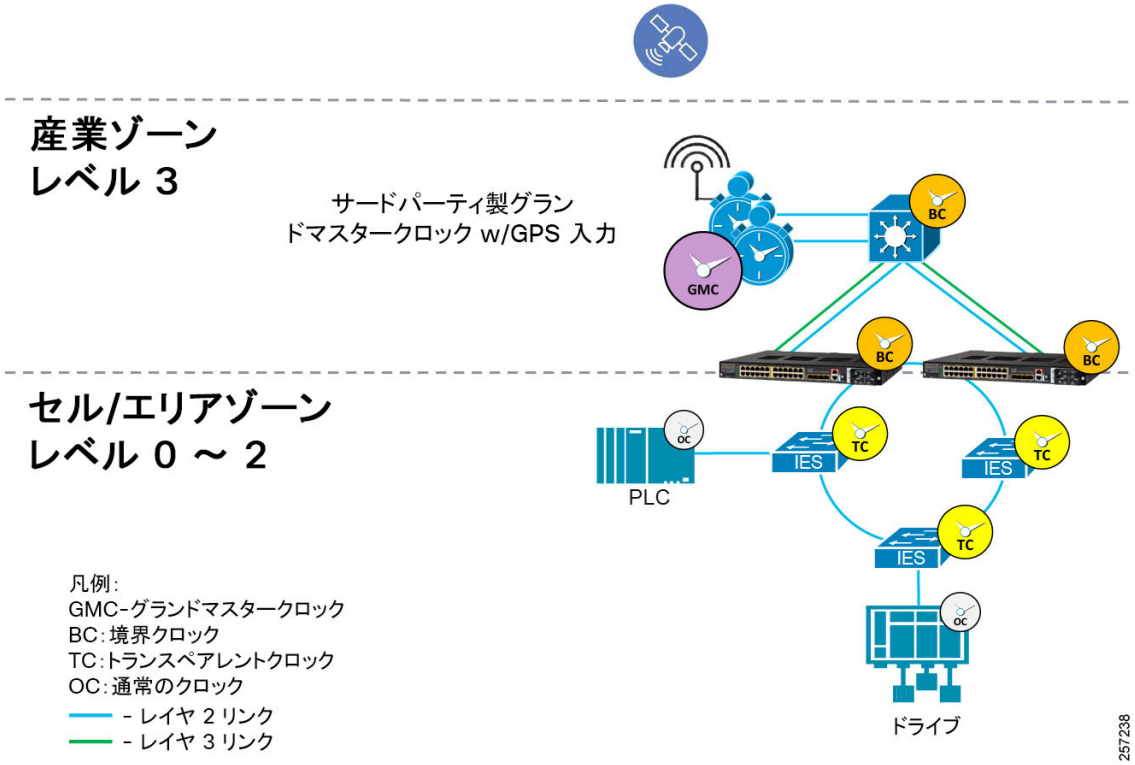
上記のセクションでは、PTP アーキテクチャの主要コンポーネントについて概要を説明しています。サイト全体で正確な時間を配布するために、このドキュメントでは次のことを推奨しています。

- 専用のサードパーティ製 GMC が製造ゾーンにインストールされている。復元力を考慮し、2 つの GMC が推奨されます。各 GMC は、クロックを UTC に合わせて GPS（または同様のサービス）を受信するために、外部アンテナをサポートして、そこに接続する必要があります。
- Cisco IE 5000 は、特定のシナリオ（特に、コラスプトコア/アグリゲーションスイッチングを備えた小規模ネットワーク）で GMC として実行できます。
- PTP、特にデフォルトプロファイルをサポートし、PTP 階層内の境界クロックとして設定されているコアおよびアグリゲーションスイッチを使用します。これらのデバイスは、PTP をサイトまたは生産施設の複数のセル/エリアゾーンに配布することができます。
- アクセススイッチは、IACS VLAN に時間を配布するに E2E TC になるように設定できます。

注：この設計では、セル/エリアゾーンをサポートする一連のアクセススイッチ上で、1 つの VLAN への時間の配布のみがサポートされています。

図 86 サイト全体の正確な時間アーキテクチャを示しています。

図 86　サイト全体の正確な時間アーキテクチャ



サイト全体の PTP 設計の考慮事項

詳細については、次の情報を参照してください。

- IEEE 1588 Precise Time Protocol（21 ページ）
- 統合された工場全体に渡るイーサネットアーキテクチャ内でのスケーラブルな時間の配布の導入
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/STD/DIG/CPwE-5-1-STD-DIG.html
- 変電所の自動化ローカルエリアネットワークおよびシスコ検証済みデザイン（CVD）セキュリティ
  https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Utilities/SA/2-3-2/CU-2-3-2-DIG.html

ベスト マスター クロック アルゴリズム

これは、クロック階層を構築し、マスターまたはスレーブとして割り当てられるデバイスを決定するプロセスであり、ベストマスタークロック アルゴリズム（BMCA）を使用して実行されます。本質的に、このプロセスは、スパニングツリープロトコルと同様の方法で動作します。GM はルートスイッチのようなものであり、すべてのマスター/スレーブ設定はこれに基づいて確立されます。PTP ネットワークが動作している場合、すべてのデバイスが起動して同期されます。接続またはデバイスのアベイラビリティの問題が原因で GM を移動しても、ネットワーク インフラストラクチャで一貫した時間を確保し、メタデータが変更されない場合、同期のレベルが損なわれることはありません。マスター/スレーブポートは GM の場所によって変更される可能性がありますが、同期は安定したままになります。この影響は、実装ガイドで測定および報告されます。

PTP 対応のクロックがネットワークに参加すると、PTP アナウンスメッセージと呼ばれる PTP メッセージをリッスンします。これらのメッセージには、タイムソース、クロック品質、プライオリティ番号などの情報が含まれます。お客様は、望ましくないデバイスが GM になり、PTP の動作に影響を与える可能性を防ぐため、ネットワークに参加する PTP デバイスが適切なプライオリティ設定で設定されていることを確認する必要があります。BMCA は継続的に実行され、アナウンスメッセージの情報を使用して、必要に応じてこれらの割り当てと調整を行います。サイト全体の正確な時間には、次の構造を推奨します。

グランドマスター（GM）層

グランドマスター階層には、PTP ドメイン用の指定グランドマスターが含まれています。サイト全体の正確な時間の配布には、サードパーティ製デバイスをプライマリグランドマスターとして選択し、復元力のために冗長化することをお勧めします。このデバイスには正確で信頼性の高いクロックが必要であり、基準クロックを使用して UTC に同期することが理想的です。プライマリグランドマスターは、PTP ドメインの安定性を向上させるため、電源障害などの障害から保護する必要があります。セカンダリグランドマスターがグランドマスターになったときの IACS アプリケーションへの影響を最小限に抑えるため、同じ PTP のタイムスケールと UTC オフセットを使用するセカンダリグランドマスターを指定することも推奨されます。ただし、プライマリグランドマスターからセカンダリグランドマスターへのフェールオーバーが発生し、その逆の場合、時刻の同期が中断されることがあります。

小規模な生産施設では、Cisco IE 5000 スイッチは、GPS または IRIG のタイミング信号を受信するように設計されているため、グランドマスターとして機能することもできます。

指定されたグランドマスターデバイスで BMCA の priority1 の値を低く設定して、BMCA の選択に勝つようにする必要があります。priority2 の値は、プライマリとセカンダリのグランドマスターの間で、最も低い priority2 値を持つプライマリとを区別するために使用する必要があります。

インフラストラクチャ層

ネットワーク インフラストラクチャ階層は、コア、集約、およびアクセススイッチで構成されます。GM デバイスが到達不能の場合、最初にコアスイッチが GM になるように、インフラストラクチャに priority1 の値を設定する必要があります。その後、コアスイッチが到達不能である場合、アグリゲーションスイッチが GM になります。さらに、**ptp time-property persist infinite** コマンドは、境界クロックとして設定されたすべてのスイッチに適用する必要があります。これにより、スレーブクロックが時間値の差異を検出しないようにするために、冗長 GMC がスタンバイ状態になったときに時間プロパティが維持されます。

IACS アプリケーションの全体的な信頼性を向上させるために、インフラストラクチャ層に電力保護を提供することをお勧めします。エンジニアは、専用の電源とバックアップ電源を使用して、インフラストラクチャを個別のエンクロージャ（該当する場合）に設置することを検討する必要があります。

コントローラ層

コントローラ層は、ネットワークがダウンしているときの時間同期の問題を削減するように設計されています。たとえば、IACS デバイスの起動する時間がそれぞれ異なるため、コントロールパネルの電源がオンになっている場合などです。プログラマブル オートメーションコントローラ（PAC）などの一部の IACS デバイスでは、リアルタイムクロックがバックアップされ、電源が切断されても継続時間が維持されます。これらの IACS デバイスは、ネットワークへの接続が復元されるまでグランドマスターになるように、priority1 の値を設定する必要があります。これにより、リアルタイムクロックを使用しないデバイスがグランドマスターになる機会を減らし、（1970年1月1日 00:00:00）のような任意の時刻に設定される可能性が低くなります。FactoryTalk Historian ME モジュールのような一部の IACS デバイスは、既存のデータポイントに対してログに記録された時間よりもかなり前の IACS アプリケーション時間を検出すると、障害を発生する可能性があります。

デバイス層

デバイス層には、他のすべての PTP 対応 IACS デバイスが含まれています。これらの IACS デバイスのほとんどは、電源によってバックアップされたリアルタイムクロックを除外し、スタートアップ時によく知られた（1970年1月1日 00:00:00）のような時刻に復帰します。したがって、これらのデバイスは、グランドマスタークロックとして信頼されないようにする必要があります。これらのデバイスがグランドマスターにならないように、priority1 と priority2 の値を設定する必要があります。デバイス層には、工場全体の IACS アーキテクチャにおけるほとんどの IACS デバイスが含まれている可能性があります。システム設定のオーバーヘッドは、デバイス層の IACS デバイスに対してデフォルトの priority1 および priority2 の値に 128 を使用することによって減らすことができます。

表 41 上記の推奨事項を確立するプライオリティ設定の例を示します。

表 41　プライオリティ設定

ロール	優先順位 1	優先順位 2
GM1	1	1
GM2(バックアップ)	1	2
コア スイッチ BC	10	11
コアスイッチ BC(バックアップ)	10	12
アグリゲーションスイッチ BC	100	101
アグリゲーションスイッチ BC(バックアップ)	100	102
アクセススイッチ BC	110	111
アクセススイッチ BC(バックアップ)	110	112
通常のクロック:PLC(時間モジュール)	120	120
オーディナリクロック:IACS	128	128

グランドマスターの設定

GMC 機能を実行するデバイスの推奨事項は次のとおりです。

- サードパーティ製 GM デバイスの PTP メッセージ更新間隔は、IES および PLC と揃え、カスタマー PLC のパフォーマンス要件に準拠している必要があります。
- IES GNSS は、バージョン ID (VID)v05 以降の SKU を持つ Cisco IE 5000 スイッチでのみサポートされています。GNSS は、PTP のデフォルトおよび電力プロファイルのタイミングソースとしてのみ使用できます。
- IES PTP グランドマスタークロックでアンテナ信号が失われると、クロック品質が低下し、GM スイッチオーバーが行われます。
- GNSS レシーバがセルフサーベイモードで起動し、最低 4 つの異なる衛星にロックオンして、現在位置で 3-D fix を取得しようとします。これらの衛星では約 2,000 の異なる位置を計算します。これには約 35 分かかります。セルフサーベイモードで取得されたタイミング信号は、20 秒間オフにすることができます。したがって、Cisco IOS は、OD モードでのみ PPS を収集します。
- 参加するグランドマスター クロック、スイッチ、およびスレーブ デバイスは、同じドメインに存在する必要があります。

ネットワーク インフラストラクチャ:PTP ポートの設定

PTP は重要なネットワーク機能であるため、高プライオリティで処理し、VLAN タグの QoS フィールドで適切にマーキングする必要があります。したがって、各 PTP 対応ネットワーク インフラストラクチャは、**global vlan dot1q tag native** コマンドを入力して、タグ付きパケットとして設定することを推奨します。

表 42 PTP デフォルトプロファイルと BC モードまたは TC モードのネットワーク インフラストラクチャのためのポートベース PTP 設定の推奨事項を示します。

表 42　ポートベースの PTP 設定の推奨事項

PTP ポートインターフェイスの特性	機能	使用するケース	推奨される設定
アナウンス間隔	BMCA 実行の頻度を確立します。	BMCA アルゴリズムの実行頻度を増減させる必要がある場合。 注:ドメイン全体で一貫している必要があります。	1(2 秒、デフォルト)
アナウンスタイムアウト	アナウンスメッセージのタイムアウトを宣言する時間間隔	タイムアウトメッセージをアナウンスする時間を 2 の係数で指定します。	3(8 秒、デフォルト)
遅延要求の間隔	ポートがマスターステート(デバイスがスレーブ)の場合に遅延要求を送信する間隔	スレーブに伝達される設定(たとえば、OC クロックの終端デバイス)。これにより、スタートアップ時にデバイスがオーバーサンプリングしない場合に、スタートアップ同期時間が短縮されます。遅延要求の数を増やすと、TC クロックのパフォーマンスに問題が発生する可能性があります。	0(1 pps)
同期間隔	同期メッセージの送信頻度の変更	BC または GMC は、同期メッセージを 1 秒毎に送信します。より頻繁に同期するほどコンバージェンスは速くなりますが、OC と BC では CPU 使用率が増加します。同期間隔が長くなるほどコンバージェンスは遅くなりますが、CPU 使用率は低くなります。	0(1 秒、デフォルト)
同期制限	再同期を試行するまでの最大オフセット	スイッチが BC モードで、スレーブポートに適用可能な場合にのみ有効です。スレーブポートがこの制限を超えると、スイッチ BC は、依存する PTP サービスとアプリケーションが中断するように再同期します。スレーブポートは変更可能であるため、すべてのポートで設定することを推奨します。	10,000 ナノ秒
vlan	トランクポート上の PTP VLAN	BCs の場合は、PTP メッセージ用に 802.1Q に従ってタグ付けされた VLAN を変更します。イーサネットリンクの両端で同じ VLAN タグを使用する必要があります。	1-4094

境界クロックの設定

同期アルゴリズム

境界クロックモードには 3 つの異なる転送機能があり、表 43 に示すように、パケット遅延変動(PDV)に対して境界クロックが調整される方法を変更し ます。PDV は、ネットワークフロー内のパケットの一方向エンドツーエンド遅延の差を測定したものであり、一般的にネットワーク「ジッター」と呼ばれているものをより正確に説明します。

表 43　境界クロック転送機能

転送機能	PDV フィルタリング	コンバージェンス時間
デフォルト(線形)	低い	平均
フィードフォワード	なし	速い
適応型	高	低速

このソリューションでは、実稼働環境でのフィードフォワード転送機能の使用を推奨します。フィードフォワード転送は、PDV がフィルタ処理されないため、すべてのネットワーク インフラストラクチャがハードウェアで PTP をサポートしているネットワークでのみ実装する必要があります。

適応型フィルタは、802.11 ワイヤレス LAN などの高い PDV のアプリケーションで使用できます。また、ネットワークが非 PTP 認識スイッチと高い PDV で構成されているアプリケーションでも使用できます。

注:適応型フィルタは、ITU-T g.8261 で指定された時間パフォーマンス要件を満たしていません。

PTP VLAN

PTP BC モードのスイッチは、異なる VLAN からの PTP トラフィックを処理する機能を備えています。これは、PTP が、レイヤ 2 プロトコルであるにもかかわらず、サイト全体のサービスになるという重要な意味を示しています。BC は、ネットワーク全体にわたって一貫した PTP をさまざまな VLAN やセル/エリアゾーンに配布するために使用されます。

- PTP サイト VLAN を確立して、GM から、またBC モードに設定されたコアおよびアグリゲーションスイッチ間で PTP を分散します。
- トランクポートで PTP VLAN を設定します。コアスイッチとアグリゲーションスイッチ間のトランクポートでは、これが PTP サイト VLAN である必要があります。セルエリアゾーン(つまりアクセススイッチ)に向けたトランクポートでは、VLAN は PTP サービスを必要とする IACS VLAN です。
- BC モードでは、ポートに関連付けられた PTP VLAN の PTP パケットのみが処理され、他の VLAN からの PTP パケットはドロップされます。
- トランクインターフェイスで PTP VLAN を設定する前に、PTP VLAN を作成し、トランクポートで許可する必要があります。
- グランドマスター クロックで VLAN が無効になっている場合は、PTP インターフェイスをアクセス ポートとして設定する必要があります。
- 現在 Cisco Catalyst 9300 プラットフォーム PTP は、レイヤ 3 リンク上ではなく、VLAN ベースの SVI インターフェイスでのみサポートされています。そのため、PTP を配布するには、追加のレイヤ 2 リンクを確立する必要があります。

設定の推奨事項の概要

- グランドマスター 層
  - IACS アプリケーションの信頼できるグランドマスターとして特定のデバイスを選択します。製造ゾーンでコアスイッチに直接接続します。
  - サイト全体で一貫して使用される PTP ドメインを選択します。
  - IACS アプリケーションの安定性を向上させるために、電源の中断などの障害からグランドマスターを保護します。
  - GPS または同様のテクノロジーを使用してグランドマスターを UTC に同期します。

- インフラストラクチャ層
  - PTP ドメインがサイト全体で一貫しているように設定します。
  - PTP が通信するすべてのリンクで、一貫した PTP VLAN 設定を確認します。
  - PTP 境界クロックモードのスイッチを使用して、VLAN 間、およびコアおよびアグリゲーションスイッチ間で時間を伝播します。
  - BC クロックでは、フィードフォワード転送機能と同期制限（たとえば、1万）を使用して、IACS アプリケーション間での同期を向上させます。
  - BC クロックスイッチでは、**ptp time-property persist infinite** コマンドを使用して、グランドマスターの損失を防ぐことができます。
  - タグ付きパケットとして PTP を送信するようにスイッチを設定します。**global vlan dot1q tag native** コマンドを入力します。
  - PTP E2E TC モードでスイッチを使用して、リングまたは線形トポロジの時間を伝播します。
  - レイヤ 2 および PTP トポロジの変更を減らすため、分離して、電源による電力をスイッチに供給します。
  - EtherChannel、仮想スイッチ、スタック構成スイッチ、またはレイヤ 3 リンクを介して PTP トラフィックを送信しないでください。
- コントローラ層
  - ネットワークがダウンしている場合に、PAC などのリアルタイムクロックを使用して IACS デバイスをグランドマスターに設定します。
- デバイス層
  - 設定を簡素化するには、デフォルトの priority1 と priority2 の値（つまり、128）を使用します。

業界を問わない適用性

この産業用オートメーション ソリューションは、幅広い産業分野/用途に適用されるネットワーキング、セキュリティ、およびデータ管理を網羅しており、各種業界に適用可能なさまざまな設計と実装の選択肢が用意されています。規模、ベンダー、アプリケーション、およびデバイスはこれらの施設間で大幅に異なる可能性がありますが、ネットワークとセキュリティの中核となる多数の概念を適用できます。たとえば、ハイアベイラビリティはすべての産業ユースケースにおいて重要な要件ですが、石油/ガスおよび電力企業は、製造施設よりも厳しいアベイラビリティ要件を持つ場合があります。それでも、CVD ソリューションのベストプラクティス ガイダンスは、多くの業界や産業の顧客環境に適用できます。

表 44　業界を問わない適用性

	製造業	変電所	石油/ガスプラント	鉱業生産	廃水
ビジネス上の必須目標	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 予知メンテナンス、機械学習、および Digital Twin アプリケーションの促進。 工場のパートナーやサプライヤへの接続。	顧客の獲得と維持。 安全性、セキュリティ、および信頼性の改善。 新しいエネルギー源と消費モデルの統合。 電力系統の刷新。	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 意思決定の改善と機械学習の促進 。 精製所とパイプラインのパートナーやサプライヤへの接続。	自動化された工場による機械化の促進。 安全性、セキュリティ、および信頼性の改善。 資材と機器の流れの最適化。 障害の予測の改善。 リアルタイムパフォーマンスのモニタリング。	稼働時間と品質の最大化。 安全性、セキュリティ、および信頼性の改善。 予知メンテナンスの促進。 リアルタイムパフォーマンスのモニタリング。

Cisco IC3000 産業用コンピューティングゲートウェイを使用したエッジコンピューティング

Internet of Things（IoT）の空間では、エッジにあるデバイスは、これらのデバイスが経時的にキャプチャするデータの価値を引き出すためにネットワーク接続を必要とします。従来のネットワーキングインフラストラクチャは、この接続を提供できます。環境によっては、より強化された産業用スイッチングハードウェアおよびルーティングハードウェアが必要です。シスコは、ファンレス型のそれらのデバイスを多く提供し、高い気温の過酷な環境に耐えることができます。また、従来のネットワークキャビネットの外側に配置することもできます。シスコの産業用イーサネット（IEx000）スイッチ、シスコのサービス統合型ルータ（IR8x9）、および Cisco IC3000 産業用コンピューティング ゲートウェイなどのデバイスは、トポロジと接続方法に応じてさまざまな機能を実行しながら、強化されたケーシング提供します。

ネットワーク接続が確立されている場合、ネットワークエンジニアが回答する必要がある最初の質問は、レイヤ3ネットワーク層の上にあるエッジデバイスと通信する方法です。ここで必要となるのは、多くの場合、デバイスの近くに配置されたコンピューティングデバイス（産業用 PC など）です。これは、アプリケーション/プロトコルレベルで通信し、デバイスからデータを抽出します。このため、シスコは IOx を導入しました。コンピューティング環境はこれらのデバイス内に存在するため、コンテナ形式でアプリケーションを展開してデバイスデータを抽出することができます。

Cisco IOx は、エッジでの IoT アプリケーションの実行、Cisco IOS とのセキュアな接続、および IoT センサーとクラウドとの迅速で信頼性の高い統合のための強力なサービスを組み合わせて、追加の管理、スペース、および電力を必要とする外部スタンドアロンコンピューティング導入の必要性を削減します。エッジ コンピューティング プラットフォームの登場により、革新的なアプリケーションを実現し、IoT の広範な機能を実証するために、Cisco IOx には多くの機会があります。

概要

Cisco IC3000 産業用コンピューティング ゲートウェイは、データインテリジェンスを IoT ネットワークのエッジに拡張して、インテリジェントな道路やスマートファクトリなどのアプリケーションの完全なエンドツーエンド ソリューションでインテントベース ネットワークと IoT データファブリックをシームレスにブリッジします。

- 次の場所にある「Cisco Industrial Compute 3000 Data Sheet」を参照してください。
  https://www.cisco.com/c/en/us/products/collateral/routers/3000-series-industrial-compute-gateways/datasheet-c78-741204.html

- Cisco IC3000 は、Cisco IoT Field Network Director 製品を使用して、大規模に管理できるデバイスです。次の場所にあるデータシートを参照してください。
  https://www.cisco.com/c/en/us/products/cloud-systems-management/iot-field-network-director/index.html

その他の関連資料には次のものが含まれます。

- Cisco IOx DevNet
  https://developer.cisco.com/site/iox/

- Cisco IOx DevNet スタートアップガイド
  https://developer.cisco.com/site/iox/documents/developer-guide/?ref=quickstart

- IOx App DevNet 開発者ガイド
  https://developer.cisco.com/site/iox/documents/developer-guide/

- Mtconnect は、通信のスタンダード
  http://www.mtconnect.org/

このセクションでは、Linux コンテナ（IOx パッケージ/OVA/Docker）ベースのアプリケーションを使用して、Cisco IC 3000 にエッジアプリケーションを導入するプロセスについて説明します。Cisco IOx の使用を実施するため、オープンソースの MTConnect エージェントはサンプルアプリケーションとして説明されます。

このプロセスは、Cisco IoT Field Network Director（FND）に依存して、IC3000 上で実行されているアプリケーションの導入、管理、およびモニタを行います。MTConnect エージェントの機能を実施するために、2 つのアプリケーションが Cisco IC3000 に導入されます。

- エージェント本体。これは、MTConnect 対応マシンと通信し、REST インターフェイスを介して必要なアプリケーションにデータを表示するためのアプリケーションです。
- マシンシミュレータ。デモンストレーションのために実際のマシンデータが存在しない場合に、エージェントにデータをフィードします。

Cisco IC3000 は、ネットワークデバイスではなくコンピューティングデバイスであるため、アプリケーション自体に必要なもの以外の設定を追加しなくても、このボックスから IOxI を実行する準備ができています。導入後は、Cisco FND を使用して、IOx 環境の最上位に大規模に展開されたアプリケーションをすぐに受信できるようになります。

ユースケース/サービス/導入モデル

ここでは、次のテクノロジーのユースケースについて説明します。

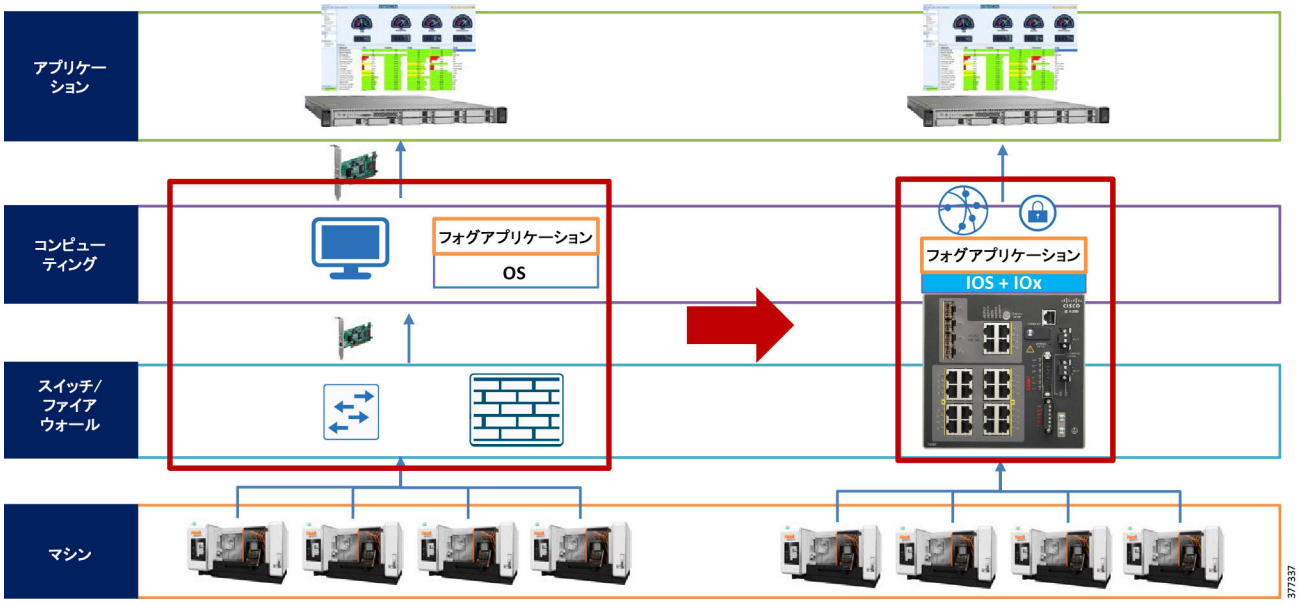
- エッジコンピューティングは、Cisco IOx を使用した Cisco IC 3000 と、サンプルアプリケーションとしての MTConnect エージェントを使用します。
- Cisco FND を使用した大規模なアプリケーション ライフサイクル管理、および IOx が内蔵されているローカルマネージャを使用した個々のデバイス向けのアプリケーション ライフサイクル管理。

システムの概要

コンバージド プラットフォームをマシンに統合することにより、ダウンタイムを削減し、総合設備効率（OEE）を向上できます。図 87（右側の）シスコによる提供と比較して、一般的なお客様の導入（左側）を示しています。このネットワークは、Cisco IC 3000 に接続されたマシンを持つサンプルゾーンを表します。これは、OEE のようなアプリケーションが存在するデータセンターに接続されます。

デジタル接続するマシンでは、マシン使用率に関する重要なデータをキャプチャする方法を製造業者に提供します。これは、運用の生産性を評価するための最も重要なメトリックの 1 つです。シスコのエッジ コンピューティングデバイスは、マシンデータをアップストリーム アプリケーションと統合、キャプチャ、および共有するために必要なツールを提供します。

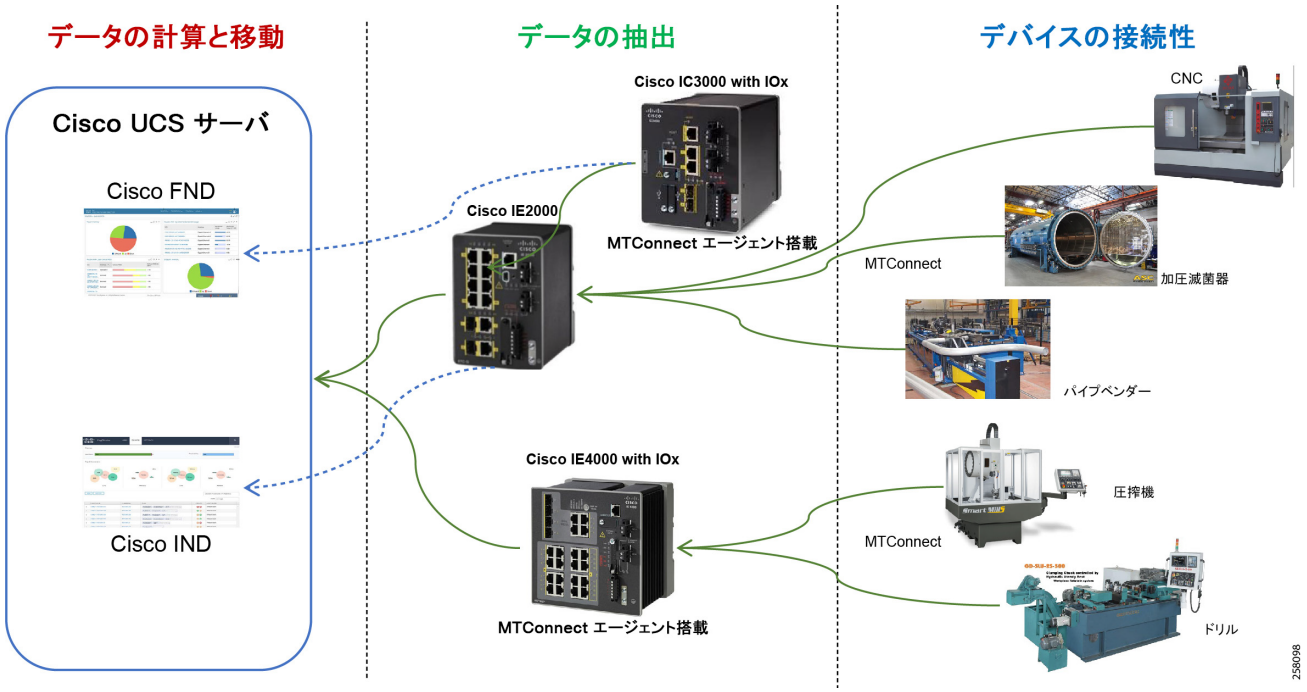
図 87　お客様の既存のシステム vs シスコの統合プラットフォーム



システム コンポーネント

Cisco IC3000 は、MTConnect などのアプリケーションと一緒に導入されると、ストリーミングデータをプルするさまざまなマシンと通信します。これはネットワーキングデバイスではないため、Cisco IE 2000 や Cisco IE 4000 などのスイッチに接続する必要があります。図 88 に示すように、スイッチは Cisco Industrial Network Director によって管理され、Cisco IC3000s は Cisco FND で管理されます。

図 88　Cisco IC3000 導入トポロジ



システムの機能に関する考慮事項

Cisco IC3000 は、管理イーサネットインターフェイスに加えて 4 つの物理インターフェイスを備えた産業用 PC であるため、アプリケーションがデータトラフィック用に 1 つ以上の物理インターフェイスを使用したり、同じサブネット上で通信する場合に、複数のアプリケーションが同じ物理インターフェイスを共有したりする可能性があります。MTConnect アプリケーションの場合、次の 2 つのバージョンのアプリケーションがテストされています。

- 最初に、単一のインターフェイス eth0 を使用し、単一の IP アドレスを使用して外部（マシン側と企業側の両方）と通信します。
- 2 番目のバージョンには、et0 と eth1 の 2 つのインターフェイスがあります。各インターフェイスは物理インターフェイスに割り当てることができ、各インターフェイスは異なるサブネットになります。これは、マシンのトラフィックの分離が必要な場合に重要です。アプリケーションは、1 つの物理インターフェイスを使用して 1 つのサブネットを介してマシンと通信し、2 番目の物理インターフェイスを介して 2 番目のサブネットを使用して企業と通信します。

設計の選択は、特定の導入の要件によって異なります。

注：ここでは、導入手順のためのサンプルアプリケーションとして MTConnect を使用していますが、IOx パッケージまたは Docker アプリケーションを IOx に移植することができ、導入手順は同じです。

システムの実装

ここで取り上げる主なトピックは次のとおりです。

Field Network Director のインストール

Cisco FND ソフトウェアは、既存の Linux OS に一度に 1 つのコンポーネントをインストールできます。ただし、ソフトウェアをインストールするさらに簡単な方法は、VMware ESXi 5.5/6.0 環境を使用して、Cisco が CCO で提供するすべてを含んだ OVA ファイルを展開することです。IC3000 コードを適切にサポートするには、FND バージョン 4.5.1-5 以降をダウンロードする必要があります。

ESXi での OVA のインストール手順については、次を参照してください。
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/install/ova/installation_ova.html

導入後は、UI のデフォルトのクレデンシャル（root/root123）を使用して、https://ip からサーバにログインできます。パスワードの変更を求められたら、新しいパスワードを作成し、新しいパスワードを使用してログインします。

この時点で、ソフトウェアは、サーバによって管理されるデバイスのデバイス設定を作成する準備ができています。このプロセスは、追加する IC3000 デバイスのシリアル番号を含む csv ファイルを使用して実行されます。1 台の IC3000 が登録されているこのようなファイルの例を次に示します。

```
eid,deviceType,lat,lng,IOxUserName,IOxUserPassword
IC3000-2C2F-K9+FCH2302Y003,IC3000,10,10,system,C!sco123
```

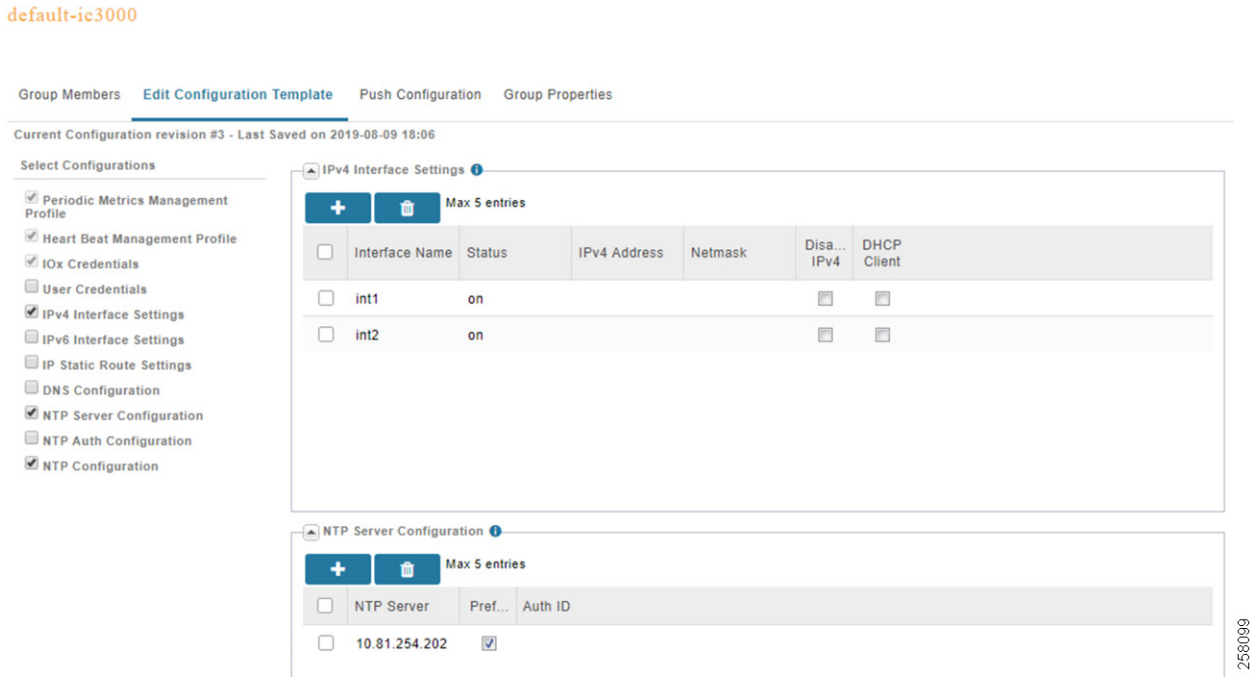
ファイルの内容は次のとおりです。

- eid：PID VID + Serial number off the IC3000 label
- devicetype：IC3000
- lat,lng：デバイスが配置されている GEO 座標を示します。
- IOxUserName：デバイス IOx にアクセスするために使用されるユーザ名を作成します。
- IOxUserPassword：デバイスに対して定義されている IOxUser にパスワードを割り当てます（8 文字以上）。

注：ユーザ ID とパスワードは、デバイスの IOx にアクセスするために使用されますが、ユーザはこれらのクレデンシャルを使用して、デバイスのローカルマネージャ インターフェイスにログインすることもできます。パスワードが 8 文字以上で、大文字と特殊文字が含まれていることを確認することが重要です。

次に、**[devices] -> [Add devices] -> [UPLOAD]** の下の FND にこの CSV ファイルをアップロードし、アップロード後の UI による成功のレポートを確認します。この時点で、インポートされたいずれかのシリアル番号を持つ IC3000 は、この FND と通信し、属しているデバイスのグループの設定またはデフォルトの設定をダウンロードできます。設定は、ハートビート頻度などのデバイスの多数の項目をキャプチャしますが、主に、物理インターフェイスが有効になるデバイスと、そのクロックを後に同期するために使用する NTP サーバに通知します。この最後の手順は、FND を使用して実稼働モードで実行されている IC3000 のクロックを設定する唯一の方法であるため非常に重要です。図 89 例として、4 つの物理インターフェイスのうちの 2 つを有効にし、1 つの NTP サーバを優先して追加する設定が挙げられます。

図 89　FND のデフォルトデバイス設定の例



IC3000 の起動とアプリケーションのインストール

IC3000 の起動と FND の接続

以下で説明する起動プロセスは、IC3000 が FND によって管理されている実稼働モードと呼ばれています。FND を使用せずにデバイスを起動する場合。これを開発者モードと呼びます。開発者モードの詳細については、「トラブルシューティング（159 ページ）」を参照してください。

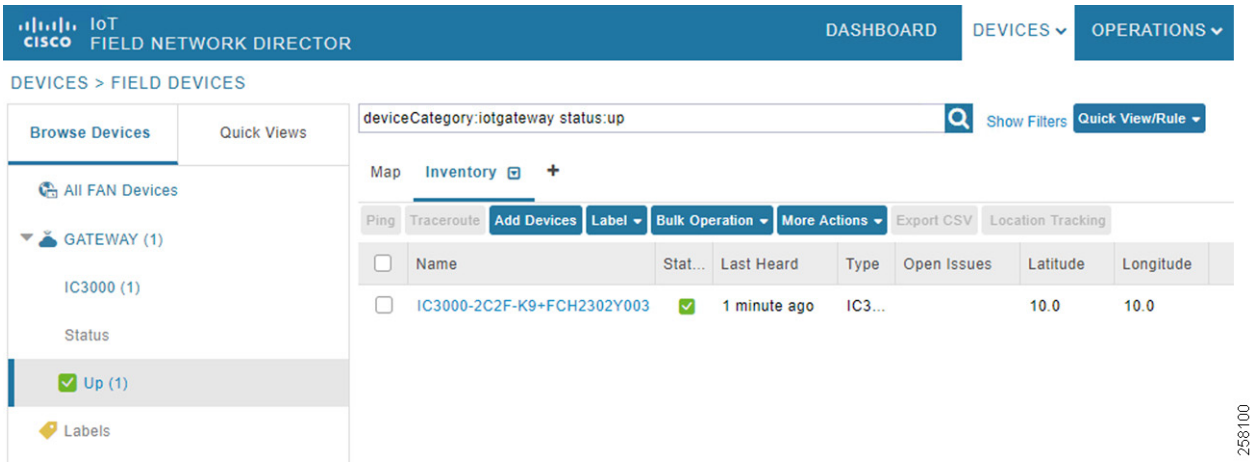
各 IC3000 には、管理インターフェイスが DHCP 対応ネットワークデバイスに接続されている必要があります。これは、DHCP が IP アドレスに加えて、この管理インターフェイスに関する重要な情報を提供するためです。現在、このインターフェイスの IP アドレスは、静的ではなく DHCP を介して割り当てる必要があります。特定の IP アドレスを割り当てる必要がある場合は、IOS の DHCP プールの下にある host および client identifier のステートメントを使用して、特定の IC3000 に特定のアドレスを強制することができます。次に、IOS DHCP プール設定の例を示します。この例では、IC3000 がシリアル番号がインポートされた FND に登録できるようになっています。次の重要なステートメントは、FND サーバの IP アドレスとポート（192.168.0.175: 9125）を指定するオプション 43 です。

注：FND が上記のように提供するため、オプション 42 を使用して NTP サーバ IP を提供する必要はなくなりました。オプション 42 が指定されている場合は、無視されます。

```
ip dhcp pool IC3KNET
   network 192.168.0.0 255.255.255.0
   default-router 192.168.0.50
   dns-server 192.168.0.15 8.8.8.8 1.1.1.1
   option 43 ascii 5A;K4;B2;I192.168.0.175;J9125
```

この DHCP 設定を使用して IC3000 デバイスがリブートされると、FND サーバに登録され、アップデバイスのリストに表示され、その色が緑色になります（図 90を参照）。また、ダウンロードされた設定によって有効になっているこの IC3000 の物理インターフェイスも緑色に変わり、別のデバイス（スイッチなど）に接続したときにアクティブであることを示します。これで、IC3000 は IOx アプリケーションをインストールする準備が整いました。

図 90　FND で登録された IC3000



IC3000 ファームウェアのアップグレード

IC3000 ソフトウェアのバージョンが工場出荷時のデフォルト（1.0.1）の場合は、最新の機能と修正にアクセスするためにバージョン1.1.1 にアップグレードする必要があります。アップグレードは、同じグループに属するすべての FND が接続された IC3000 で実行されます。アップグレードの手順は次のとおりです。

1. **[ADMIN] > [Provisioning Settings] > [IoT-FND URL]** が、DNS で到達可能な場合、IP または名前によって FND サーバを指していることを確認します。
2. **[CONFIG] > [Firmware Update] > [Images]** で、**IC3000**を左のパネルから選択して新しいイメージをアップロードします。
3. **[CONFIG] > [Firmware Update] > [Groups]** で、アップグレードするすべての IC3000s が同じグループに属していることを確認します。**[Upload Image]**をクリックし、IC3000 のイメージを選択してすべてのデバイスにアップロードします。
4. **[CONFIG] > [Firmware Update]** で、以前のステップで **[Group]** を選択してから **[Install Image]** をクリックします。この手順により、ダウンロードしたイメージがインストールされます。IOx のアップグレードだけでなく、ファームウェアのアップグレードが必要な場合は、15 分程度かかる場合があります。

注：何らかの理由でアップグレードが失敗した場合は、デバイスのリセットが必要になることがあります（「IC3000 のリセット（159 ページ）」を参照）。

アプリケーションのインストールと設定

次の手順では、一度に 1 つまたは複数の IC3000 デバイスに MTConnect エージェント アプリケーションをインストールします。ローカルマネージャによるアプリケーションのインストールとは異なり、次の手順では、ユーザの介入なしでアプリケーションを自動的にインストール、アクティブ化、および開始します。

1. FND の [Apps] タブで、**[Import apps]** を選択して、最初に FND カタログにアプリケーションを追加します。ここでは、アプリケーションを IOx SDK パッケージ化されたコンテナとして、OVA として、または Docker レジストリからインポートするオプションが提供されます。次の手順は、IOx SDK とともにパッケージ化されたアプリケーション tar ファイルを前提としています。
2. ローカルマシンのアプリケーションファイルを参照し、**[Upload]** をクリックしてアプリケーションを FND に保存します。
3. FND の [Apps] タブでアプリケーションを選択し、**[Install]** をクリックします。
4. 1 つ以上のデバイスを選択し、**[Add Selected devices]** をクリックしてインストールリストに入れます。
5. **[Next >]** をクリックして、アプリケーションを設定します。

6. この画面では多くの機能をカスタマイズできますが、int1（ブリッジ）インターフェイスをダイナミックモードで使用していることを確認するため、ネットワーキングのみをチェックします。選択したら、**[REASSIGN NETWORKS]** をクリックして変更を適用します。
7. VCPU の設定を求められた場合は、1～4 から値を選択し、**[REASSIGN VCPU]** をクリックして確認します。
8. **[Done Let's Go]** をクリックしてインストールを完了します。
9. 必要に応じて、シミュレータ アプリケーションに対して同じプロセスを繰り返します。

注：IC3000 に導入されたデバイス設定が 2 つのインターフェイスをアクティブにしている間は、MTConnect エージェント アプリケーションとシミュレータ アプリケーションの両方で 1 つだけの操作用インターフェイスが必要になります。導入環境でマシンとエンタープライズセグメントの分離が必要な場合は、2 つのインターフェイスを使用する MTConnect エージェント アプリケーションのバージョンも存在します。

アプリケーションのアンインストール

一度に 1 つまたは複数の IC3000 デバイスでアプリケーションをアンインストールする方法は、次のとおりです。

1. FND の **[Apps]** タブでアンインストールするアプリケーションを選択し、**[Uninstall]** をクリックします。
2. 1 つまたは複数のデバイスを選択し、**[Add Selected Devices]** をクリックしてアンインストールリストに追加します。
3. **[Done Let's Go]** をクリックして、アンインストールを完了します。

MTConnect エージェント アプリケーションのアクセスと設定

ここで展開されている MTConnect エージェント アプリケーションは、以下で公開されているエージェントのオープンソースバージョン 1.4 に基づいて構築されています。http://www.mtconnect.org/

アプリケーションには、多くのエージェントが事前に設定されています。インストールが完了して起動すると、これらのエージェントのうち 4 つが自動的に実行されます。各エージェントは（1 台のマシンにマッピングされた）特定のポートをリッスンし、別のポートで REST インターフェイスをノースバウンド アプリケーションに提供します。単一の MTConnect アプリケーションで実行されているエージェントを設定するには、次の 2 つの方法があります。

- 最初の方法は、Web UI に組み込まれたアプリケーションを使用する方法です。
- 2 番目の方法は、アプリケーションに直接 SSH 接続する方法です。

アプリケーションの IP アドレス情報は、デバイスを選択して FND で確認できます。その後、デバイス上のすべてのアプリケーションが展開されている **[Apps]** タブが、ステータスと IP アドレス情報とともにリストされます。

設定された各エージェントは、動作するために 次の 2 つの重要なファイルを必要とします。

- 1 つ目は、IP アドレス、ポート番号などを含む agent.cfg ファイルです。
- 2 番目は、マシン固有の XML ファイルであり、この特定の設定済みポート上のマシンから到着するデータのスキーマをエージェントに提供します。

次に、いくつかのインラインコメントを含む、agent.cfg ファイルの例を示します。

```
# name of the machine xml file to be used for this agent. Found in same directory
Devices = ./VMC-3Axis.xml
AllowPut = true
# this is the northbound port to be used by upstream applications
# needing access to the data from this agent via REST API.
Port = 5001
ReconnectInterval = 1000
BufferSize = 17
SchemaVersion = 1.3

Adapters {
   VMC-3Axis {
      # IP address of the machine/adapter where data is coming to the agent from (can be DNS)
      Host = gos.iotspdev.local
      # Port on the machine/adapter IP for access to streaming data
      Port = 7878
   }
```

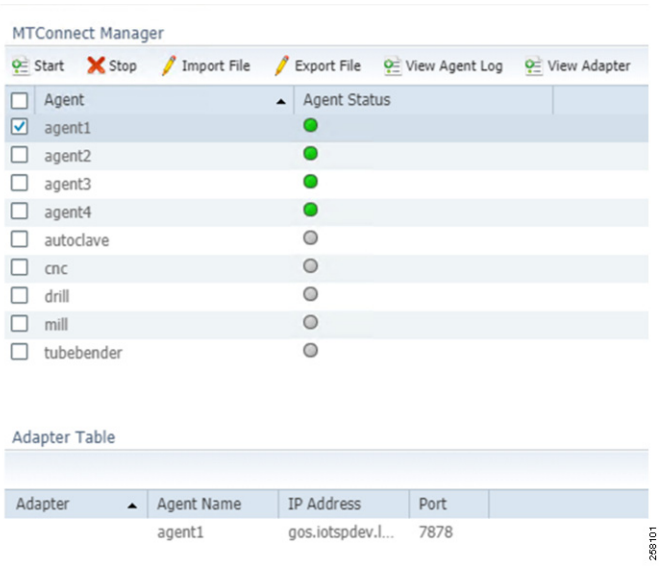
```
}

Files {
    schemas {
        Path = /home/root/schemas
        Location = /schemas/
    }
    styles {
        Path = /home/root/styles
        Location = /styles/
    }
    Favicon {
        Path = /home/root/styles/favicon.ico
        Location = /favicon.ico
    }
}

StreamsStyle {
  Location = /styles/Streams.xsl
}

# Logger Configuration
logger_config
{
    logging_level = info
    # location of log file, currently set to same dir as the agent.cfg
    output = file /home/root/data/appdata/agent1/agent.log
 }
```

マシンの XML ファイルは、このマシンに対して想定されるすべてのデータをエージェントに提供するので、そのマシンに固有のものになっています。通常、データは、組み込みアダプタまたはマシンと トランスレーションを提供する MTConnect アプリケーションの間に配置されたアダプタから直接着信します。サンプル XML ファイルは「サンプルマシンの XML ファイル（161 ページ）」に掲載されています。

Web UI を使用したエージェントの管理

Web UI に組み込まれた MTP 接続アプリケーションには、URL http://IP:5010/mtconnect.shtml でアクセスできます。ここで、IP はアプリケーション自体の IP アドレスです。図 91 は実行中の MTConnect アプリケーションの UI の例です。ユーザは 1 つ以上のエージェントを選択し、**[Start]** または **[Stop]** をクリックします。**[Import File]** および **[Export File]** オプションでは、編集のためにエージェントからローカルマシンに cfg ファイルまたは XML ファイルをコピーできます。その逆も同様です。**[View Agent Log]** オプションは、実行中のエージェントの現在のログを表示し、**[View Adapter]** オプションは、このエージェントが通信しているマシンとポート番号のクイックビューを提供します。

図 91　サンプルエージェントの組み込み Web UI



SSH を使用したエージェントの管理

MTConnect アプリケーションは、SSH をサポートし、ユーザは C!sco123 のクレデンシャルを使用してログインできます。次のログからわかるように、dir agent1 は実行中の 4 つのエージェントのうちの 1 つを表し、そのディレクトリ内のファイルは必要に応じて変更できます。

```
user@linux:~$ ssh root@192.168.0.136
root@192.168.0.136's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

ic3k:~# ls /home/root/data/appdata/agent1/
VMC-3Axis.xml  agent.cfg      agent.log
ic3k:~#
```

スケールの検証

このセクションでは、このテストの目的のためにすべてのメモリおよび CPU リソースを使用してデバイス上で実行されている MTConnect エージェント アプリケーションを表示する IC3000 で実行される、いくつかのスケール結果を提供します。制御された環境下のトラフィックシミュレーションを使用してテストを行い、1 つのデバイスがトラフィックを処理できるようにするために、1 秒あたりのタグ数と（マシン数に変換される）アプリケーション内のエージェント数を拡張できるようになりました。

IC3000 のテスト条件

- イメージ：バージョン：1.0.1、プラットフォーム ID：IC3000-2C2F-K9、HW ID: FCH2302Y003（1.4 MTConnect）
- 使用可能な最大 CPU リソース（9000 CPU および 6000 MB の RAM）を使用して、MTConnect エージェントコンテナがプロビジョニングされます。
- すべてのエージェントが、ストリーミングモードで EFM に追加されました。
- テストで使用される各エージェントには、4 台のデバイス（マシン）があります。各デバイスには 71 のデータ項目があり、エージェントごとに 284 のデータ項目があります。

表 45　2 つのエージェント：合計 8 台のマシン

タグ/秒/マシン	合計タグ数/秒	メモリ（MB）	使用されている CPU
14	112	838	35%
30	240	1037	37 %
43	344	1057	39%
62	500	1062	41%
125	1024	1057	45%

表 46　3 つのエージェント：合計 12 台のマシン

タグ/秒/マシン	合計タグ数/秒	メモリ（MB）	使用されている CPU
14	168	840	35%
30	360	1152	39%
43	516	1170	41%
60	720	1176	44 %
105	1260	1172	50 %

表 47　5 つのエージェント: 合計 20 台のマシン

タグ/秒/マシン	合計タグ数/秒	メモリ（MB）	使用されている CPU
14	275	857	40%
30	600	1382	41%
43	870	1388	45%
62	1240	1404	51%
100	2000	1401	59%

表 48　10 エージェント: 合計 40 台のマシン

タグ/秒/マシン	合計タグ数/秒	メモリ（MB）	使用されている CPU
14	550	1891	40%
30	1200	1957	47%
40	1600	1957	55%
55	2200	1973	64%
74	2960	1971	74%

トラブルシューティング

ここでは、基本的なトラブルシューティングについて説明し、さまざまな問題の根本原因を特定します。

IC3000 のリセット

管理ポートの左側にある **[Reset]** ボタンは、多機能ボタンです。この動作は、ボタンが押された時間（秒単位）によって異なります。次のガイドラインに従うことが重要です。これらのガイドラインから外れた範囲でボタンを押すと効果がありません。

- 10～15 秒：

  Reboot：電源の再投入と同等のデバイスの通常のリブート。

- 30～35 秒：

  Config-reset：アプリケーションを含むすべてのユーザ設定を消去して、デバイスを再起動します。デバイスは、実行されていた最後のソフトウェアイメージで再起動します。

- 60～65 秒：

  Factory-reset：すべての内容を消去して、工場出荷時のデフォルトイメージ（1.0.1）を使用して起動します。

IC3000 IOx のトラブルシューティング

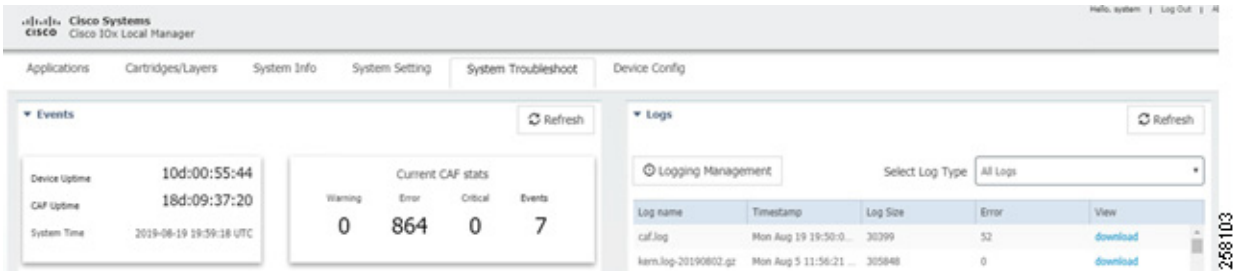
トラブルシューティングで、IC300 からログを収集するには、次の 3 つの方法があります。

- FND フィールドデバイスページを使用して、さまざまなタブとアップロード ログメカニズムを使用します。

図 92　FND フィールドデバイスページ

- Https://IP:8443 を介して、Ox ローカルマネージャのシステム トラブルシューティング ページを使用します。ここで、IP は管理 IP アドレスです。下の **[Device Config]** タブは、そのすべての設定を含めて、デバイスが開発者モードの場合にのみ有効であることを知っておく必要があります。このモードでは、ユーザはこのタブを使用して IC3000 インターフェイス、DNS、および NTP を設定し、ソフトウェアアップグレードを実行できます。

図 93　システムのトラブルシューティング ページ



- IC3000 のコンソールポートに接続されたシリアルケーブルを介した CLI の使用。ログインは必要ありません。
  - ソフトウェアとデバイスのシリアル番号を確認するには、バージョンを表示します。

```
ic3k> show version
Version: 1.1.1
Platform ID: IC3000-2C2F-K9
Hardware ID: FCH2307Y01M
```

  - IC3000 から NTP サーバへの接続とクロック同期を確認します。

```
ic3k> show clock
Mon Aug 19 20:20:15 UTC 2019

ic3k> show ntp association
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          14 l   51   64    1    0.000    0.000   0.000
*10.81.254.202   .GNSS.           1 u   40   64    1    0.501   -0.050   0.625

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 38631  9014   yes   yes  none    reject   reachable  1
  2 38632  961a   yes   yes  none  sys.peer    sys_peer  1

* master (synced), # master (unsynced), + selected, - candidate, ~ configured

ic3k> show ntp status
```

```
Clock is synchronized, stratum 2,reference is 10.81.254.202
nominal freq is 100.0000HZ, precision is 2**21
reference time is E1057F8C.4F5A814C (20:05:32.309000 Mon Aug 19 2019)
clock offset is -0.942843 msec, root delay is 0.478 msec
root dispersion is 938.569 msec, peer dispersion is 437.529 msec

NTP Servers received from DHCP:
10.81.254.202
```

- IC3000 のステータスと FND への接続を確認します。**bold** の値は、デバイスが実行中であり、実稼働モードであり、適切な FND に登録されて接続されていることを含む、検索するキー値を反映しています。

```
ic3k> show ida status
IDA Version: 2.0.1
Status: Running
Operation Mode: Production
FND Host: 192.168.0.175:9121
FND Connection Status: Connected
Periodic Metrics Interval: 300
Heartbeat Interval: 60
Is Registered: True
HTTP Server Status: N/A (Stopped)
Remote Device Management: N/A
```

- ゲスト OS IOx のステータスに関する日付を提供する、IOx のサマリーあるいは詳細を示します。

```
ic3k> show iox summary
IOx Infrastructure Summary:
---------------------------
eid: IC3000-2C2F-K9+FCH2302Y003
pfm: IC3000-2C2F-K9
s/n: FCH2302Y003
images: Lnx: 0.10.360., IOx: 1.8.0:r/1.8.0.0:74512d0
boot: 2019-08-09 19:03:34
time: 2019-08-19 20:21:33
load: 20:21:33 up 10 days, 1:17, 0 users, load average: 0.90, 0.56, 0.38
memory: ok, used: 6964/7798 (89%)
disk: ok, used: /:487868/543588 (89%), /software:34598976/87462892 (39%)
process: warning, running: 4/5, failed: sshd
networking: ok
logs: warning, errors: caf (1059)
apps: warning, Alleantia (D) MTConnect14 (D) MTCsim (D) Win12USB (R) centos7 (D) ubuntu18 (D)
```

サンプルマシンの XML ファイル

```
<?xml version="1.0" encoding="UTF-8"?>
<MTConnectDevices xmlns:m="urn:mtconnect.org:MTConnectDevices:1.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="urn:mtconnect.org:MTConnectDevices:1.1"
xsi:schemaLocation="urn:mtconnect.org:MTConnectDevices:1.1
http://www.mtconnect.org/schemas/MTConnectDevices_1.1.xsd">
        <Header creationTime="2010-03-04T18:44:40+00:00" sender="localhost" instanceId="1267728234"
bufferSize="131072" version="1.1"/>
        <Devices>
                <Device id="dev" iso841Class="6" name="VMC-3Axis" sampleInterval="10" uuid="000">
                        <Description manufacturer="SystemInsights"/>
                        <DataItems>
                                <DataItem category="EVENT" id="avail" type="AVAILABILITY"/>
                        </DataItems>
                        <Components>
                                <Axes id="ax" name="Axes">
                                        <Components>
```

```
                                        <Rotary id="c1" name="C">
                                                <DataItems>
                                                        <DataItem category="SAMPLE" id="c2"
name="Sspeed" nativeUnits="REVOLUTION/MINUTE" subType="ACTUAL" type="SPINDLE_SPEED"
units="REVOLUTION/MINUTE">
                                                                <Source>spindle_speed</Source>
                                                        </DataItem>
                                                        <DataItem category="SAMPLE" id="c3"
name="Sovr" nativeUnits="PERCENT" subType="OVERRIDE" type="SPINDLE_SPEED" units="PERCENT">
                                                                <Source>SspeedOvr</Source>
                                                        </DataItem>
                                                        <DataItem category="EVENT" id="cm"
name="Cmode" type="ROTARY_MODE">
                                                                <Constraints>
                                                                        <Value>SPINDLE</Value>
                                                                </Constraints>
                                                        </DataItem>
                                                        <DataItem category="CONDITION"
id="Cloadc" type="LOAD"/>
                                                        <DataItem category="CONDITION"
id="Csystem" type="SYSTEM"/>
                                                        <DataItem category="SAMPLE" id="c13"
name="Cload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                                                </DataItems>
                                        </Rotary>
                                        <Linear id="x1" name="X">
                                                <DataItems>
                                                        <DataItem category="SAMPLE" id="x2"
name="Xact" nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="x3"
name="Xcom" nativeUnits="MILLIMETER" subType="COMMANDED" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="n3"
name="Xload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                                                        <DataItem category="CONDITION"
id="Xloadc" type="LOAD"/>
                                                        <DataItem category="CONDITION"
id="Xsystem" type="SYSTEM"/>
                                                </DataItems>
                                        </Linear>
                                        <Linear id="y1" name="Y">
                                                <DataItems>
                                                        <DataItem category="SAMPLE" id="y2"
name="Yact" nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="y3"
name="Ycom" nativeUnits="MILLIMETER" subType="COMMANDED" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="y4"
name="Yload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                                                        <DataItem category="CONDITION"
id="Yloadc" type="LOAD"/>
                                                        <DataItem category="CONDITION"
id="Ysystem" type="SYSTEM"/>
                                                </DataItems>
                                        </Linear>
                                        <Linear id="z1" name="Z">
                                                <DataItems>
                                                        <DataItem category="SAMPLE" id="z2"
name="Zact" nativeUnits="MILLIMETER" subType="ACTUAL" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="z3"
name="Zcom" nativeUnits="MILLIMETER" subType="COMMANDED" type="POSITION" units="MILLIMETER"/>
                                                        <DataItem category="SAMPLE" id="z4"
name="Zload" nativeUnits="PERCENT" type="LOAD" units="PERCENT"/>
                                                        <DataItem category="CONDITION"
id="Zloadc" type="LOAD"/>
                                                        <DataItem category="CONDITION"
id="Zsystem" type="SYSTEM"/>
```

```
                                                </DataItems>
                                        </Linear>
                                </Components>
                        </Axes>
                        <Controller id="cn1" name="controller">
                                <DataItems>
                        <DataItem category="EVENT" id="msg" type="MESSAGE"/>
                                        <DataItem category="EVENT" id="estop"
type="EMERGENCY_STOP"/>
                                        <DataItem category="CONDITION" id="clp"
type="LOGIC_PROGRAM"/>
                                        <DataItem category="CONDITION" id="motion"
type="MOTION_PROGRAM"/>
                                        <DataItem category="CONDITION" id="system"
type="SYSTEM"/>
                                </DataItems>
                                <Components>
                                        <Path id="pth" name="path">
                                                <DataItems>
                                                        <DataItem category="EVENT" id="cn2"
name="block" type="BLOCK"/>
                                                        <DataItem category="EVENT" id="cn3"
name="mode" type="CONTROLLER_MODE"/>
                                                        <DataItem category="EVENT" id="cn4"
name="line" type="LINE"/>
                                                        <DataItem category="EVENT" id="cn5"
name="program" type="PROGRAM"/>
                                                        <DataItem category="EVENT" id="cn6"
name="execution" type="EXECUTION"/>
                                                        <DataItem category="EVENT" id="cnt1"
name="tool_id" type="TOOL_ID"/>
                                                        <DataItem category="SAMPLE" id="Ppos"
nativeUnits="MILLIMETER_3D" subType="ACTUAL" type="PATH_POSITION" units="MILLIMETER_3D"/>
                                                        <DataItem category="SAMPLE" id="Frt"
nativeUnits="MILLIMETER/SECOND" type="PATH_FEEDRATE" units="MILLIMETER/SECOND">
                                                                <Source>path_feedrate</Source>
                                                        </DataItem>
                                                        <DataItem category="SAMPLE" id="Fovr"
nativeUnits="PERCENT" type="PATH_FEEDRATE" units="PERCENT">
                                                                <Source>feed_ovr</Source>
                                                        </DataItem>
                                                </DataItems>
                                        </Path>
                                </Components>
                        </Controller>
                        <Systems id="systems" name="systems">
                                <Components>
                                  <Electric id="el" name="electric">
                                <DataItems>
                                        <DataItem category="EVENT" id="p2" name="power"
type="POWER_STATE"/>
                                </DataItems>
                            </Electric>
                                        <Coolant id="cool" name="coolant">
                                                <DataItems>
                                                        <DataItem category="CONDITION"
id="clow" type="LEVEL"/>
                                                        <DataItem category="CONDITION"
id="coolpres" type="PRESSURE"/>
                                                        <DataItem category="CONDITION"
id="filter" type="x:FILTER"/>
                                                        <DataItem category="CONDITION"
id="coolantmotor" type="ACTUATOR"/>
```

```
                                                        </DataItems>
                                                </Coolant>
                                                <Hydraulic id="hsys" name="hydrolic">
                                                        <DataItems>
                                                                <DataItem category="CONDITION"
id="hlow" type="LEVEL"/>
                                                                <DataItem category="CONDITION"
id="hpres" type="PRESSURE"/>
                                                                <DataItem category="CONDITION"
id="htemp" type="TEMPERATURE"/>
                                                        </DataItems>
                                                </Hydraulic>
                                        </Components>
                                </Systems>
                        </Components>
                </Device>
        </Devices>
</MTConnectDevices>
```

産業用 DMZ のリファレンス

ここでは、IDMZ の設計ガイダンスを提供します。設計の概要とガイダンスを提供する理由は単に、IDMZ を通過する必要があるトラフィック（ISE、リモートアクセスなど）がテストに含まれていたものの、このレイヤがこの産業用オートメーション CVD で特に検証されていないためです。CPwE IDMZ については、次のリンク先を参照してください。
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

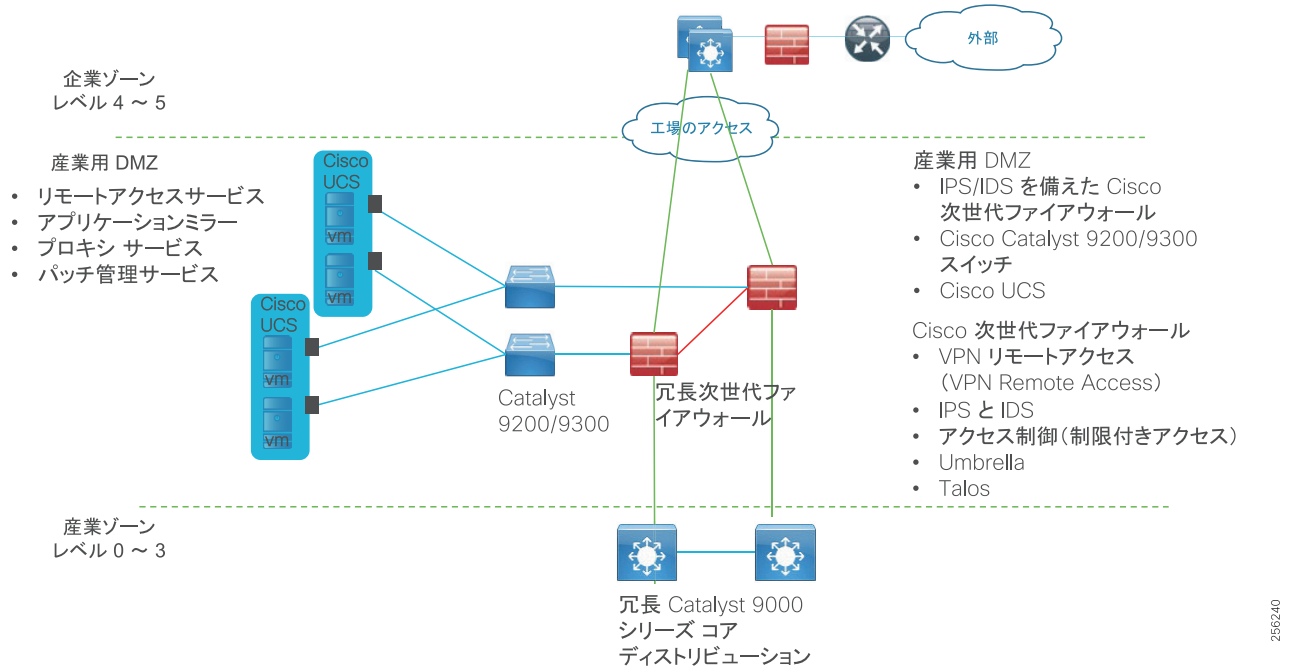
産業ゾーンには、工場全体の運用を制御し、モニタリングするために不可欠なすべて IACS ネットワークおよびオートメーション機器が含まれています。IEC-62443 を含む産業用セキュリティ標準では、産業ゾーン（レベル 0 ～ 3）と企業/ビジネスドメイン以上（レベル 4 ～ 5）を厳密に分離することが推奨されています。このセグメンテーションと厳格なポリシーは、安全な産業用インフラストラクチャと産業プロセスのアベイラビリティを提供するために役立ちます。MES や ERP などの 2 つのエンティティの間でデータを共有することが依然として必要ですが、企業ゾーンと産業ゾーンの全体でデータ/セキュリティ ネットワーキング サービスを管理および適用する必要がある場合があります。信頼できる産業ゾーンと信頼できない企業ゾーンの間にゾーンおよびインフラストラクチャが必要です。一般に「レベル 3.5」と呼ばれる IDMZ は、これらの 2 つのエンティティ間でのデータ アクセスおよび交換を可能にするアクセス/制御ポイントを提供します。

IDMZ アーキテクチャは、企業ドメインと産業ドメインに終端ポイントを提供し、2 つのドメイン間の通信を仲介およびポリシングするためのさまざまなサーバ、アプリケーション、およびセキュリティポリシーを備えています。

IDMZ の重要なガイドラインと概念は、次のとおりです。

- ベスト プラクティスとしては、企業ゾーンと産業ゾーンの間で直接通信が行われないようにする必要がありますが、産業ゾーンで企業システムを利用しているときは、それが不可能な場合があります（ISE の導入）。
- IDMZ は、IDMZ 内のミラー化または複製されたサーバおよびアプリケーションを使用して、企業ゾーンと産業ゾーンの間の安全な通信を提供する必要があります。
- IDMZ は、外部ネットワークから産業ゾーンへのリモートアクセス サービスを可能にします。
- IDMZ は、産業ゾーンへの不正な通信を防止するためのセキュリティバリアを提供する必要があり、そのため、認可された通信を明示的に許可するセキュリティポリシーを作成する必要があります（企業ゾーンと産業ゾーンの間の ISE）。
- これは、企業内に漏れる産業用トラフィックにも当てはまります。IACS トラフィックが IDMZ を直接通過することはありません（コントローラ、I/O トラフィック）。

図 94　産業用 DMZ のリファレンス



上記のリファレンス設計は、コンポーネントとアーキテクチャの概要を示しています。IDMZ に出入りするトラフィックを検査および制御するために、冗長ファイアウォールが導入されます。アプリケーション ミラーと IDMZ サービスをホストする UCS サーバにネットワーク アクセスを提供するために、Cisco Catalyst サーバが IDMZ 内に導入されます。ファイアウォールは、企業ゾーンと IDMZ の両方に対してレイヤ 3 を動作させます。図 94 に産業施設に関連する DMZ を通過するトラフィックの概念が再度示されています。

IDMZ の産業特性と設計上の考慮事項

大部分の産業工場施設では、このアーキテクチャ レイヤに、セル/エリアゾーンレベル 2 以下とは大きく異なる物理環境があります。ネットワーキングの特性としては、リアルタイム パフォーマンスがそれほど重視されず、機器は、環境的に管理されたエリア、キャビネット、または部屋に設置されます。

以下に、IDMZ の設計上の重要な考慮事項を示します。これらは、プラットフォームの選択、ネットワーク トポロジ、セキュリティの実装、および全体的な設計に影響します。

- 産業特性：環境条件、工場のレイアウト、およびケーブル接続コストはすべて、設計におけるプラットフォームの選択とネットワーク トポロジに影響を与えます。一般的な位置と管理の戦略は、レベル 3 では変更され、レベル 3.5 ではさらに変更されます。工場をサポートするためのアプリケーションがインストールされるネットワーキング プラットフォームおよびサーバは、通常、工場フロアではなく環境的に制御されたエリアに配置されます。IDMZ は、通常、企業ゾーンと産業ゾーンの間を移動する必要があるトラフィックのタイプに関して OT から得られる考慮事項と要件にも基づいて、セキュリティアーキテクトと IT のプロフェッショナルによって管理の観点から導入されます。このため、従来の IT プラットフォームの選択に対応するプラットフォームの選択の基準が変わります。これらのプラットフォームには、IT ベースの次世代ファイアウォール（ASA、Cisco Firepower Threat Defense（FTD）ファイアウォールなど）、Cisco Catalyst 9300/Cisco Catalyst 9200 製品、およびシスコの非強化 UCS プラットフォーム（パッチ管理、リモートアクセス、およびミラー サーバを収容）が含まれます。

- 相互運用性と相互接続性：IDMZ は、産業ゾーンと企業ゾーンの間の唯一の通信インターフェイスです。IDMZ は相互接続を可能にしますが、トラフィックフローと、リモートアクセスや IACS アプリケーションのミラー化されたサービスといったセキュリティ機能を厳密に制御および制限します。レイヤ 3 は、IDMZ と企業の間および IDMZ と産業ゾーンの間で有効にする必要があります。

- リアルタイム通信、確定性、およびパフォーマンス：IACS ネットワーク内のパケットの遅延とジッタは、基盤となる産業プロセスに大きな影響を与える可能性がありますが、IDMZ では、この要件はセル/エリアゾーンの要件とは大きく異なります。IDMZ を介した企業ゾーンと産業ゾーンの間の大部分のトラフィック フローは、産業アプリケーションの観点からは非リアルタイム（せいぜいリアルタイムに近いだけ）であるため、一般的なパフォーマンス基準は、パケット遅延、レイテンシ、およびジッターの影響をあまり受けません。

- アベイラビリティ：産業用オートメーション内の重要なメトリックは、総合設備効率（OEE）です。IDMZ でもアベイラビリティは依然としてネットワークの重要な要件です。ただし、IDMZ に障害が発生しても、産業ゾーンで、そしてより重要なこととしてセル/エリアゾーンで実行される操作とプロセスが機能しつづける必要があります。そのため、企業ゾーンのアプリケーションまたはシステムには、産業ゾーンの実稼働環境に関連するプロセスへの依存性はありません。産業用オートメーションは、冗長サーバ、ファイアウォール、イーサネットリンクなどを備えた IDMZ の復元力とアベイラビリティを促進しますが、小規模な工場環境では、これが適用されない場合があります。

- セキュリティ：セキュリティ、安全性、およびアベイラビリティは、産業用セキュリティフレームワーク内で緊密に連携しています。産業用ネットワークのセキュリティについて検討する場合、顧客は、環境を安全で運用可能な状態に保つ方法に関心を持っています。制御システムとプロセスドメインを保護するためのアーキテクチャ的アプローチに従うことをお勧めします。推奨モデルは、制御階層の Purdue モデル、International Society of Automation 95（ISA95）と IEC 62443、NIST 800-82、および変電所用の NERC CIP です。IDMZ は、企業ゾーンと産業ゾーンの間の重要なセキュリティ セグメンテーション レイヤです。セキュリティの概念と機能は、「生産の可視性」、「IACS アプリケーション機能のインターフェイス」、および「企業によって産業ゾーンに提供されるネットワーキング/セキュリティサービス」をサポートするために、ビジネスドメインの産業ゾーンへのインターフェイスを提供するように設計および実装されます。IDMZ 内の機能サブゾーンは、IACS データ/ネットワークサービスへのアクセスをセグメント化するように設定されます（IT、運用、および信頼できるパートナーのゾーン）。このレイヤのファイアウォールの性質により、侵入防御および検出（IPS/IDS）によるマルウェア検出、IDMZ に出入りするデータのコンテンツセキュリティ、リモートアクセスの制御された VPN 終端といった、拡張されたセキュリティ手段を次世代ファイアウォールにもたらす機能が実現されます。

- 管理：産業ゾーンとサイト運用および制御レイヤ内では、一貫した管理戦略が必要です。このコラボレーションは、IDMZ の設計とベストプラクティスのサポートにも拡大する必要があります。OT ペルソナと IT ペルソナの組み合わせによってセル/エリアゾーンに運用上の焦点が合わされており、セキュリティアーキテクトの支援を受けて IT ペルソナと OT ペルソナによって運用および制御レベルゾーンが導入されている場合、IDMZ の管理と設計は、IT セキュリティアーキテクトにより、OT エンジニアおよび IT エンジニアと協力して進められます。

IDMZ のファイアウォール

Cisco ASA with FirePOWER Services は、Cisco ASA 5500-X シリーズの次世代ファイアウォールに特化した脅威重視型の次世代セキュリティサービスを提供します。これにより、標的型や持続的なマルウェア攻撃からの保護を含む、既知の脅威や最先端の脅威からの包括的な保護を実現します（図 95）。Cisco ASA は、世界で最も幅広く導入されているエンタープライズクラスのステートフル ファイアウォールです。Cisco ASA with FirePOWER Services は、次の包括的な機能を備えています。

- サイトツーサイトとリモートアクセス VPN、および高度なクラスタリングにより、非常にセキュアで高パフォーマンスなアクセスおよびハイアベイラビリティを提供して、ビジネス継続性を実現しています。

- 4,000 を超えるアプリケーションレイヤとリスクベースの管理をサポートする、きめ細かい Application Visibility and Control（AVC）によって、最適な侵入防御システム（IPS）脅威検出ポリシーが起動され、セキュリティの有効性が向上します。

- 業界をリードする Cisco ASA with FirePOWER の次世代 IPS（NGIPS）は、きわめて効果的な脅威保護と、ユーザ、インフラストラクチャ、アプリケーション、およびコンテンツのフルコンテキスト認識機能を備え、マルチベクター脅威を検出し、防御対策を自動的に行います。

- レピュテーションとカテゴリに基づく URL フィルタリングによって、不審な Web トラフィックに対する包括的なアラートと制御が可能になり、80 を超えるカテゴリの何億もの URL に対してポリシーが適用されます。

- AMP は、業界トップクラスのセキュリティ侵害検出の有効性とサンドボクシングを備え、総所有コストを削減できるとともに、優れたセキュリティ保護を実現します。これにより、他のセキュリティレイヤでは見逃されるマルウェアや新たな脅威を検出、把握、阻止できます。

図 95　CIsco Collective Security

次世代ファイアウォールの詳細については、次のドキュメントを参照してください。
https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html?cachemode=refresh

IDMZ データと情報交換

産業ゾーンと企業ゾーンの間での IACS データおよび通信の安全な受け渡しを容易に実現するために IDMZ でホストされるサービスのタイプは、次のとおりです。企業ゾーンと産業ゾーンの間で直接アクセスが許可されない状態が助長されると、IDMZ にサーバまたはサービスを導入して 2 つのゾーン間の通信を仲介させ、サービスの配置場所として機能させるという要件が強調されます。

- IACS の複製またはミラー化されたデータサービス：前述のように、企業ゾーンと産業ゾーンのセキュリティ方法論および要件が異なるため、DMZ の使用が促進されます。ただし、ビジネスの俊敏性とビジネスインテリジェンスを向上させるために、産業ゾーンと企業でデータを共有する必要があります。DMZ には、産業ゾーンから企業ゾーンに安全にデータを複製またはミラー化するためのサーバ、アプリケーション、またはサービスが導入されます。IACS ベンダーに応じて、データを複製するためのこれらのサーバまたはテクノロジーは異なる場合がありますが、動作の原則と機能は変わりません。

- 安全なファイル転送サービス：産業ドメインのアセットにインストールするためのセキュリティ パッチまたはソフトウェア インストール ファイルの更新は、企業ゾーンから産業ゾーンにファイルを安全に持ち込む必要がある例です。これを安全な方法で達成するとともに、直接通信を行わないという前提を維持するために、安全なファイルサーバとパッチ管理サーバを導入して、IDMZ にサービスの配置場所を提供します。ファイルは IDMZ にダウンロードされ、その後に産業ゾーンに配置された産業用ファイルサーバに渡すことが可能です。

- リモートアクセスサービス：安全なリモートアクセスにより、許可されたユーザに、産業ゾーンのプロセスまたは産業用アセットのリアルタイムビューを提供できます。Windows リモート デスクトップ ゲートウェイなどのリモートアクセスサーバを IDMZ に導入できます。リモートユーザは、このサーバにアクセスしてから、産業ゾーンの認可されたアセットにリモートアクセスします。

セキュリティポリシーの例外：『*Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*』には、企業ゾーンと産業ゾーンの間での直接アクセスが許可されるいくつかのユースケースが記載されています。この DIG では、導入のための特定のポートとガイダンスが示されています。ただし、これは、各顧客が検討する必要のあるリスクの容認です。実装とサポートのコストが低いことや、導入されるアプリケーションのパフォーマンスが高いことに基づいて、ある程度のリスクが容認される場合があります。

IDMZ データフローの概要

セキュリティポリシーの例外:『*Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*』には、企業ゾーンと産業ゾーンの間での直接アクセスが許可されるいくつかのユースケースが記載されています。この設計ガイドでは、導入のための特定のポートとガイダンスが示されています(下記のリンク先を参照)。ただし、これは、各顧客が検討する必要のあるリスクの容認です。実装とサポートのコストが低いことや、導入されるアプリケーションのパフォーマンスが高いことに基づいて、ある程度のリスクが容認される場合があります。ただし、ISE 導入は、同期の実装による制約を受けます。ISE ポリシーサービスノード(PSN)は、ポリシー管理ノードと同期させる必要があります。現在のモデルでは、この管理ノードは企業内に配置され、このサービスについては、プロキシまたはミラー化されたサービス機能が存在しません。そのため、ISE は、IDMZ のファイアウォールを直接通過します。産業ゾーンと企業ゾーンの間を移動するデータフローの概要は、次のとおりです。

次のユースケースは、『*Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide*』で検証されています。このドキュメントには、詳細な設計ガイダンスと実装が記載されています。
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

- Remote Access
- IACS アプリケーション(履歴)
- 安全なファイル転送
- Active Directory サービス
- 証明書サービス
- Network Time Protocol(NTP)
- Identity Services
- WLAN 担当者のアクセス

ハイ アベイラビリティ

IDMZ でもアベイラビリティは依然としてネットワークの重要な要件です。ただし、IDMZ に障害が発生しても、産業ゾーンで、そしてより重要なこととしてセル/エリアゾーンで実行される操作とプロセスが機能しつづける必要があります。そのため、企業ゾーンのアプリケーションまたはシステムには、産業ゾーンの実稼働環境に関連するプロセスへの依存性はありません。アベイラビリティに関する設計ガイダンスは、次のとおりです。

ファイアウォールの復元力

- 冗長ファイアウォールを展開し、単一のセキュリティ コンテキストでアクティブ/スタンバイ フェールオーバー モードを設定します。
- フェールオーバーリンクとステートフル フェールオーバーリンクのそれぞれの専用インターフェイスでステートフル フェールオーバー設定を使用します。
- フェールオーバー キーでフェールオーバー通信を暗号化します。
- アクティブユニットとスタンバイユニットの EtherChannel で冗長スイッチに接続します。
- 企業ゾーン間で通信するようにレイヤ 3 ルーティングを設定します。

IDMZ ネットワークのアベイラビリティ

- IDMZ とコア/ディストリビューション ルータの間および IDMZ と企業の間のレイヤ 3 ルーティング。
- アーキテクチャ全体の冗長リンク
- すべてのネットワーク機器およびファイアウォールの設定のバックアップ。

- ネットワークインフラストラクチャの管理、制御、およびデータプレーンを保護するためのネットワーク強化のベストプラクティス
- サーバ スイッチ接続用に導入されるデュアル レイヤ 2 スイッチ。
- 物理サーバから冗長スイッチへのデュアル NIC 接続性。仮想サーバからのデュアル NIC テクノロジー。
- サーバ、仮想サーバ、またはアプリケーションの冗長性（必要な場合）。

セキュリティ

- IDMZ VLAN セグメンテーション：前述したように、VLAN セグメンテーションは、IACS レベル 3 サーバでのサービスの分離を支援するためのセキュリティフレームワークの共通コンポーネントです。これも IDMZ アーキテクチャで実装する必要があります。IDMZ および DSS 環境内にいくつかの VLAN を作成する場合、サーバを分離できます。これにより、セキュリティ侵害が発生した場合に、VLAN コンテナ内のサーバが IDMZ 内の他のサーバに影響を与えることを制限できます。
- シスコの次世代ファイアウォールを使用したポリシーの適用
- NetFlow と Stealthwatch による可視性：Cisco Catalyst 9000 シリーズは NetFlow をサポートしています。レベル 3、コア、ディストリビューション、および産業用データセンターと適合する IDMZ 内のすべての NetFlow 対応スイッチで NetFlow を有効にして、Stealthwatch にエクスポートすると、アプリケーションおよびネットワークトラフィックの工場全体のビューが得られます。これを使用することで、基準トラフィックプロファイルの提供と、ネットワークデータフローの異常の識別が容易になります。
- 強化された NGN 機能：
  - IDMZ を通過するすべてのトラフィックのために、IPS/IDS を IP NGN ファイアウォールに導入できます。
  - ファイアウォールを通過するすべてのファイルを検査するために、異常マルウェア検出を導入できます。

次世代ファイアウォールの詳細については、
https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-733916.html?cachemode=refresh を参照してください。

可用性

ここでは、セル/エリアゾーンのディストリビューション スイッチで産業用オートメーション用に検証された復元力オプションについて説明します。

ディストリビューション スイッチの復元力

Cisco StackWise-480

Cisco Catalyst 3850 および Cisco Catalyst 9300 は、StackWise-480 設定をサポートし、ディストリビューション レイヤでプラットフォームの復元力を提供します。スイッチ スタックは、StackWise-480 ポート経由で接続された最大 8 つのスタック対応スイッチで構成できます。スタック メンバーは 1 つの統合システムとして連携します。レイヤ 2 プロトコルとレイヤ 3 プロトコルが、スイッチ スタック全体を単一のエンティティとしてネットワークに提示します。

スイッチ スタックには、必ず 1 個のアクティブ スイッチおよび 1 個のスタンバイ スイッチがあります。アクティブスイッチは、スタックの管理プレーンの制御を提供します。アクティブスイッチが使用できなくなると、スタンバイスイッチがアクティブスイッチの役割を引き継ぎ、スタックの動作可能状態を維持しつづけます。このバージョンの産業用オートメーションでは、セル/エリアゾーンのディストリビューション スイッチの復元力を提供するために、スイッチスタックが 2 つのスイッチを使用して検証されました。

アクティブ スイッチは、スイッチ スタックの保存された実行コンフィギュレーション ファイルを保持します。スタンバイ スイッチは、自動的に、同期された実行コンフィギュレーション ファイルを受け取ります。スタック メンバーは、実行コンフィギュレーション ファイルがスタートアップ コンフィギュレーション ファイルに保存された時点で同期されたコピーを受け取ります。アクティブ スイッチが使用できなくなると、スタンバイ スイッチが現行の実行コンフィギュレーションを引き継ぎます。

Cisco StackWise の設定

スタックメンバーのプライオリティ

スタックメンバーのプライオリティ値が高いほど、アクティブスイッチとして選択され、自分のスタックメンバー番号を保持できる可能性が高くなります。プライオリティ値は 1 ～ 15 の範囲で指定できます。デフォルトのプライオリティ値は 1 です。**show switch** EXEC コマンドを使用すると、スタックメンバーのプライオリティ値を表示できます。

```
P5-9300-2#show switch
Switch/Stack Mac Address : 00bc.60ad.a500 - Local Mac Address
Mac persistency wait time: Indefinite
                             H/W   Current
Role    Mac Address              Priority  Version  State
-----------------------------------------------------------------------------------
*1       Active   00bc.60ad.a500     15      V01     Ready
 2       Standby  00bc.60ad.9b80     1       V01     Ready
```

アクティブスイッチにしたいスイッチには、最高のプライオリティ値を割り当てることをお勧めします。それにより、アクティブスイッチの再選択時に、そのスイッチが再びアクティブスイッチとして選択されます。

スタックメンバーのプライオリティ値を変更するには、次のコマンドを使用します。

switch *stack-member-number* priority *new priority-value*

次に例を示します。

```
switch 1 priority 15
```

新しいプライオリティ値はすぐに有効となりますが、現在のアクティブ スイッチには影響しません。新たなプライオリティ値は、現在のアクティブスイッチまたはスイッチスタックのリセット時に、どのスタックメンバーが新たなアクティブスイッチとして選択されるかを決定する場合に影響を及ぼします。

スタック MAC アドレスの永続化

スイッチ スタックは、そのブリッジ ID によって、または、レイヤ 3 デバイスとして動作している場合はそのルータ MAC アドレスによって、ネットワーク内で識別されます。ブリッジ ID とルータ MAC アドレスは、アクティブスイッチの MAC アドレスによって決まります。アクティブスイッチが変わると、新たなアクティブスイッチの MAC アドレスによって、新たなブリッジ ID とルータ MAC アドレスが決まります。デフォルトの動作では、新しい MAC アドレスがネットワークで学習されるため、トラフィックが中断される可能性があります。この状況を回避するには、スタック MAC アドレスが新しいアクティブスイッチの MAC アドレスに変更されないように、スタックの MAC 永続性を設定します。

設定するには、次のコマンドを使用します。

```
stack-mac persistent timer 0
```

スタックメンバー番号の変更

スタックメンバー番号(1 ～ 9)により、スイッチスタック内の各メンバーが識別されます。また、メンバー番号によって、スタック メンバーが使用するインターフェイス レベルの設定が決定します。**show switch** EXEC コマンドを使用すると、スタックメンバー番号を表示できます。

```
P5-9300-2#show switch
Switch/Stack Mac Address : 00bc.60ad.a500 - Local Mac Address
Mac persistency wait time: Indefinite
                             H/W   Current
Role    Mac Address              Priority  Version  State
-----------------------------------------------------------------------------------
*1       Active   00bc.60ad.a500     15      V01     Ready
 2       Standby  00bc.60ad.9b80     1       V01     Ready
```

新しい(つまり、スイッチ スタックに参加していない、またはスタック メンバー番号が手動で割り当てられていない)スイッチには、デフォルト スタック メンバー番号(1)が割り当てられた状態で出荷されます。このスイッチがスイッチ スタックに参加すると、デフォルト スタック メンバー番号は、スタック内で使用可能な、一番小さいメンバー番号に変更されます。

同じスイッチ スタック内のスタック メンバーは、同じスタック メンバー番号を持つことはできません。スタンドアロン スイッチを含む各スタック メンバーは、番号を手動で変更するか、番号がスタック内の別のメンバーによってすでに使用されていないかぎり、自分のメンバー番号を保持します。

次のように設定すると、手動でスタックメンバー番号を変更できます。

```
switch current-stack-member-number renumber new-stack-member-number
```

新しい番号がスタック内の他のメンバーにまだ割り当てられていない場合にのみ、そのスタックメンバーのリセット後（または、**reload slot stack-member-number** 特権 EXEC コマンドの使用後）に、その番号が有効になります。

Cisco Catalyst 3850 StackWise-480 の設定の詳細については、次のドキュメントを参照してください。

- Cisco Catalyst 3850 の場合：
  https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html#reference_5415C09868764F0FA05F88897F108139
- Cisco Catalyst 9300 の場合：
  https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/stck_mgr_ha/b_165_stck_mgr_ha_9300_cg/managing_switch_stacks.html

Cisco StackWise のトラブルシューティング

次の **show** コマンドにより、スタックに関する情報が表示されます。

表 49　スタック情報を表示するコマンド

コマンド	説明
show switch および **show switch detail**	割り当てられたスイッチやバージョン不一致モードのスイッチのステータスなど、スタックに関するサマリー情報を表示します。 これらのコマンドにより、設定に関する次の情報が表示されます。 ■ スイッチまたはスタックの MAC アドレス ■ MAC の永続性設定（「Indefinite」である必要がある） ■ スイッチ番号、MAC アドレス、プライオリティ値、および現在の状態 ■ 各スイッチのスタック ポートのステータスと各ポートが接続されているネイバー
show switchstack-member-number	特定のメンバーに関する情報を表示します。
show switch detail	スタックに関する詳細情報を表示します。
show switch neighbors	スタック ネイバーを表示します。
show switch stack-ports[summary]	スタックのポート情報を表示します。スタックのケーブル長、スタックのリンク ステータス、およびループバック ステータスを表示するには **summary** キーワードを使用します。
show redundancy	冗長システムと現在のプロセッサ情報を表示します。冗長システムの情報には、システム稼働時間、スタンバイ失敗、スイッチオーバーの理由、ハードウェア、および設定冗長モードと動作冗長モードが含まれます。表示される現在のプロセッサ情報には、アクティブ位置、ソフトウェアの状態、現在の状態での稼働時間などが含まれます。
show redundancy state	アクティブおよびスタンバイスイッチの冗長状態をすべて表示します。

Hot Standby Router Protocol

Hot Standby Router Protocol（HSRP）は、複数のスイッチが連携してディストリビューションサービスを提供できるようにするもう 1 つの冗長オプションです。インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。マスタールータが Internet Group Management Protocol（IGMP）スヌーピングクエリアになることを保証するために、ネットワーク内で最小の IP をスタンバイ IP として設定することをお勧めします。

推奨される実装では、HSRP はスイッチ仮想インターフェイス（SVI）で設定されます。HSRP を設定するには、仮想 IP とグループ番号をインターフェイスに割り当てます。次にマスター ピアでの HSRP 設定の例を示します。

```
interface Vlan10
ip address 10.17.10.2 255.255.255.0
standby 1 ip 10.17.10.1
```

次にスタンバイ ピアの例を示します。

```
interface Vlan10
ip address 10.17.10.3 255.255.255.0
standby 1 ip 10.17.10.1
```

仮想 IP は同じですが物理 IP はピアごとに異なっていることに注意してください。

HSRP のプライオリティの設定

プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプションが有効である場合は、障害から回復した後に、プライオリティが最高のルータが再びアクティブ ルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。最大の値（1 ～ 255）が、最高のプライオリティ（アクティブ ルータになる確率が最も高い）を表します。

インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティング テーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブ ルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティング テーブルを更新できるように遅延時間を設定します。

目的のアクティブ ピアにプライオリティを設定するには、インターフェイス設定に次の行を追加します（デフォルトのプライオリティは 100 なので、それより大きい数字を設定する必要があります）。

```
standby 1 priority 254
```

プリエンプションの設定

ローカル ルータのプライオリティがアクティブ ルータよりも高い場合、アクティブ ルータとして制御を行います。オプションとして「delay」を設定できます。これにより、ローカル ルータは、アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。

```
standby 1 preempt delay minimum 30
```

HSRP タイマー

HSRP は、次の 2 つのタイマーを使用します：hello interval と hold time。hello interval は、hello パケットが他方のピアに送信される頻度を定義します。hold time は、ピアをダウンとしてマーキングするまでの待機時間を示します。hold time は、hello interval の 3 倍以上である必要があります。次の例で使用されている値は、検証時に、デフォルト値よりも速いコンバージェンスを実現するために使用されました。これらのタイマーを設定するには、次のコマンドを使用します。

```
standby 1 timers msec 200 msec 750
```

HSRP のトラブルシューティング

show standby コマンドと **show standby brief** コマンドにより、設定と現在のステータスの詳細が表示されます。

```
IE5K-3#show standby
Vlan10 - Group 1
State is Active
7 state changes, last state change 2w1d
Virtual IP address is 10.17.10.1
Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 200 msec, hold time 750 msec
Next hello sent in 0.144 secs
Preemption enabled
Active router is local
Standby router is 10.17.10.3, priority 170 (expires in 0.736 sec)
Priority 200 (configured 200)
Group name is "hsrp-Vl10-1" (default)
IE5K-3#
IE5K-3#sh standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Vl10 1 200 P Active local 10.17.10.3 10.17.10.1
```

HSRP がその HSRP ピアを認識しない場合は、物理レイヤの接続と設定を確認してください。

Internet Group Management Protocol の考慮事項

IGMP スヌーピングは、特定のマルチキャスト グループからのトラフィックを要求するホストにだけマルチキャスト トラフィックをルーティングするように設定する必要があります。IGMP スヌーピングは Cisco IE スイッチではデフォルトで設定されていますが、次のコマンドを使用して、ディストリビューション スイッチで IGMP スヌーピングのクエリを設定する必要があります。

```
ip igmp snooping querier
```

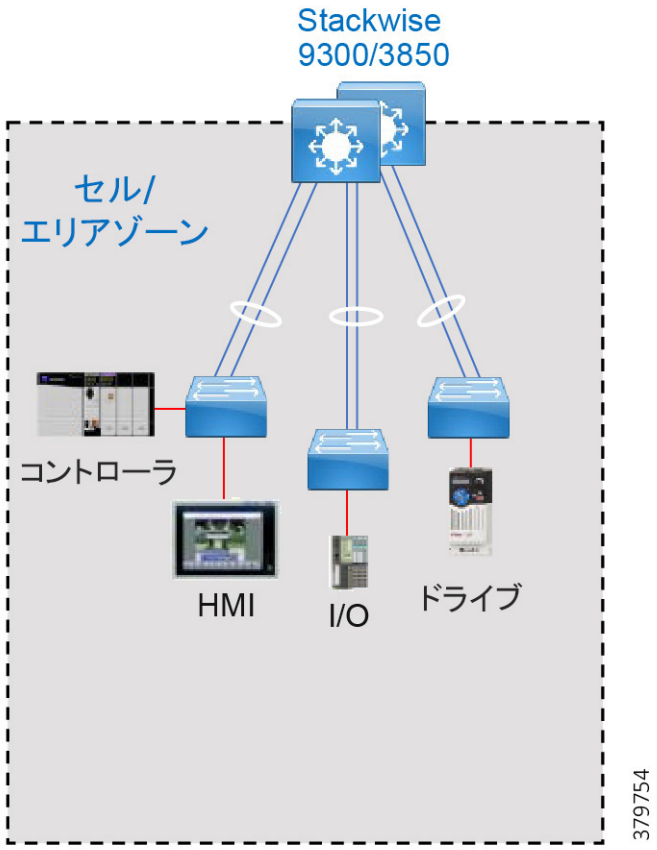
IGMP は、ネットワーク内で最小の IP を持つクエリアを選択します。そのため、HSRP IP をネットワーク内で最小の IP に設定することが重要です。

セル/エリアゾーンの復元力

EtherChannel

Link Aggregation Control Protocol（LACP）を使用してアクセススイッチとディストリビューション スイッチ間でアクティブモードで EtherChannel を設定するには、各スイッチでポートチャネル インターフェイスを設定し、そのリンクをポートチャネルのメンバーとして設定します。

図 96　セル/エリアゾーンの EtherChannel の例



channel-group コマンドにより、物理ポートと論理インターフェイスがバインドされます。次に EtherChannel 設定の例を示します。

```
interface Port-channel2
interface GigabitEthernet1/0/3
  channel-group 2 mode active
interface GigabitEthernet2/0/3
  channel-group 2 mode active
```

「アクティブ モード」は、LACP ネゴシエーション状態を指します。このモードでは、ポートは、LACP パケットを送信する他のポートとのネゴシエーションを開始できます。

EtherChannel の設定後、ポートチャネル インターフェイスに適用した設定変更は、そのポートチャネル インターフェイスに割り当てられたすべての物理ポートに適用されます。EtherChannel 内のすべてのポートのパラメータを変更するには、ポートチャネル インターフェイスに対してコンフィギュレーション コマンドを適用します。たとえば、**spanning-tree** コマンドを使用して、レイヤ 2 EtherChannel をトランクとして設定します。

EtherChannel のトラブルシューティング

表 50 の **show** コマンドにより、EtherChannel に関する情報が表示されます。

表 50　EtherChannel に関する情報を提供するコマンド

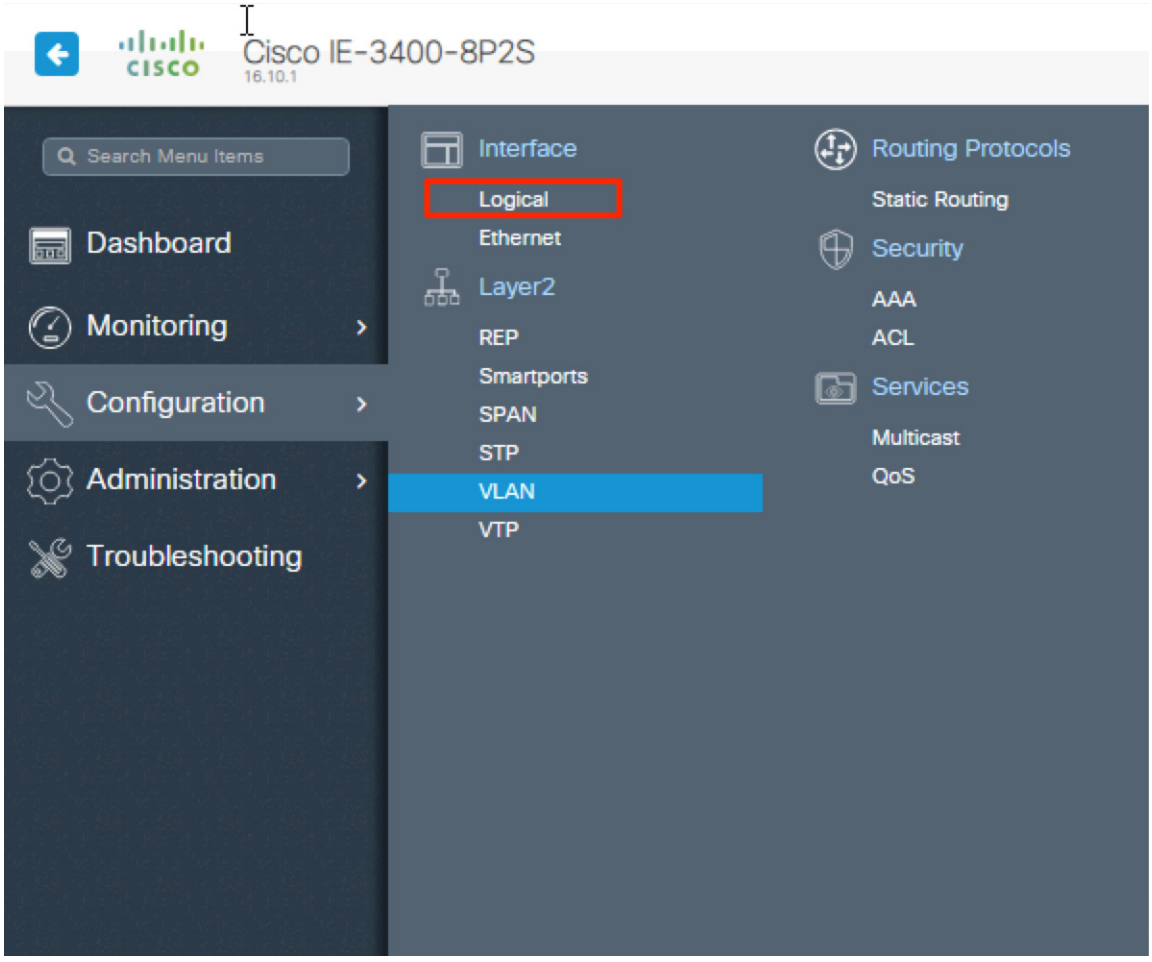
コマンド	目的
show etherchannel [channel-group-number{ detail | port | port-channel | protocol |summary }] { detail | load-balance | port |port-channel | protocol | summary}	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。ロード バランシング方式またはフレーム配布方式、ポート、ポートチャネル、プロトコルの情報も表示されます。
show lacp [channel-group-number] {counters | internal | neighbor}	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。

Device Manager を使用した EtherChannel の設定

このセクションでは、Cisco IE スイッチが管理用の IP アドレスを使用してインストールおよび設定されていることを前提としています。Cisco IE スイッチのセットアップの詳細については、対応するインストール ガイドを参照してください。

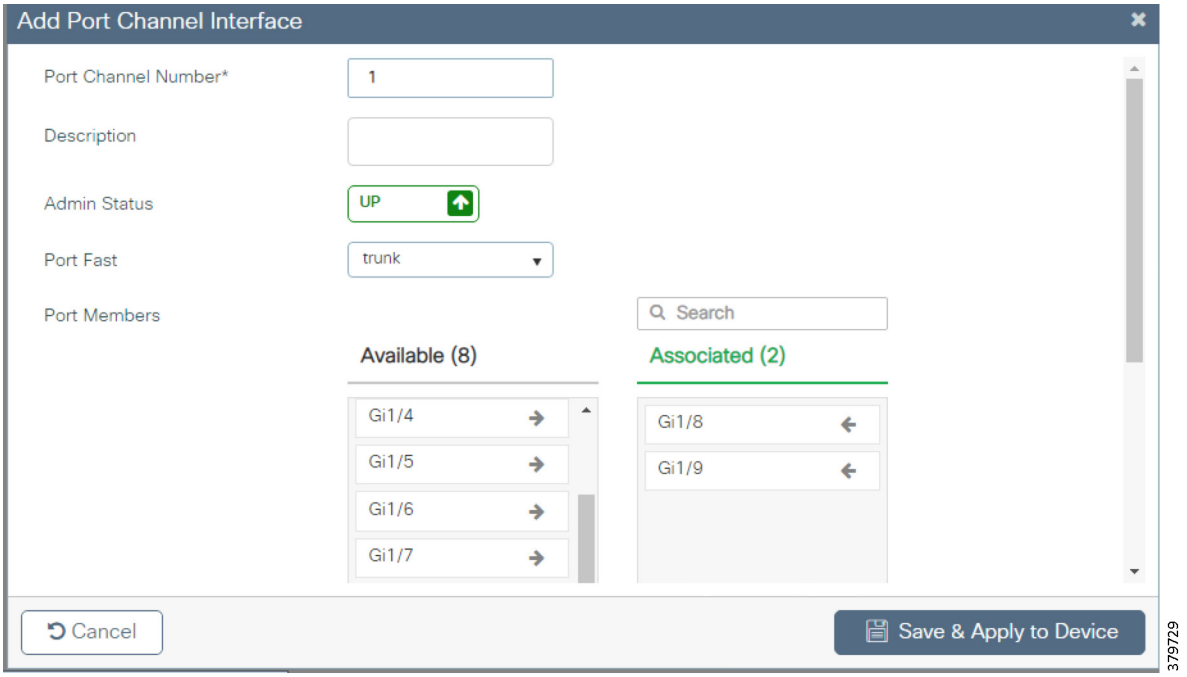
1. Device Manager のクレデンシャルを使用してスイッチにログインします。
2. [Configuration] メニューに移動します。
3. [Interface] -> [Logical] を選択します（図 97 を参照）。

図 97　Device Manager の設定オプション



4. ポート チャネルの詳細を入力し、インターフェイスを関連付けます（図 98 を参照）。

図 98　EtherChannel の設定



5. [Save & Apply to Device] をクリックします。

Resilient Ethernet Protocol

Resilient Ethernet Protocol（REP）は、で示されているように、セル/エリアゾーンのスイッチリングで使用される復元力のあるプロトコルです（図 99 を参照）。また、HSR リングをディストリビューションへ接続するためのオープンセグメントとして使用します（図 100 を参照）。リングで使用される場合、エッジポートはディストリビューション内の同じ論理スイッチ上に存在します。オープンセグメントとして使用される場合、エッジポートは別々のスイッチに配置されます。さまざまな分散レイヤ復元力プロトコルで使用されるエッジ ポートの位置については、表 51 を参照してください。

表 51　REP セグメントのエッジポートの位置

トポロジ	ディストリビューション レイヤの復元力プロトコル	エッジポートの位置
REP リング	Cisco StackWise	エッジポートがスタックスイッチ上にあり、各エッジポートが異なるスタックメンバー上にある必要があります。
REP リング	HSRP	両方のエッジ ポートがプライマリ HSRP ディストリビューション スイッチ上にある必要があります。
HSR リング	Cisco StackWise または HSRP	各エッジ ポートが、ディストリビューションに接続されたアクセススイッチ上にあり、アクセススイッチごとにエッジポートが 1 つだけである必要があります。

図 99　セル/エリアゾーンリング上の REP

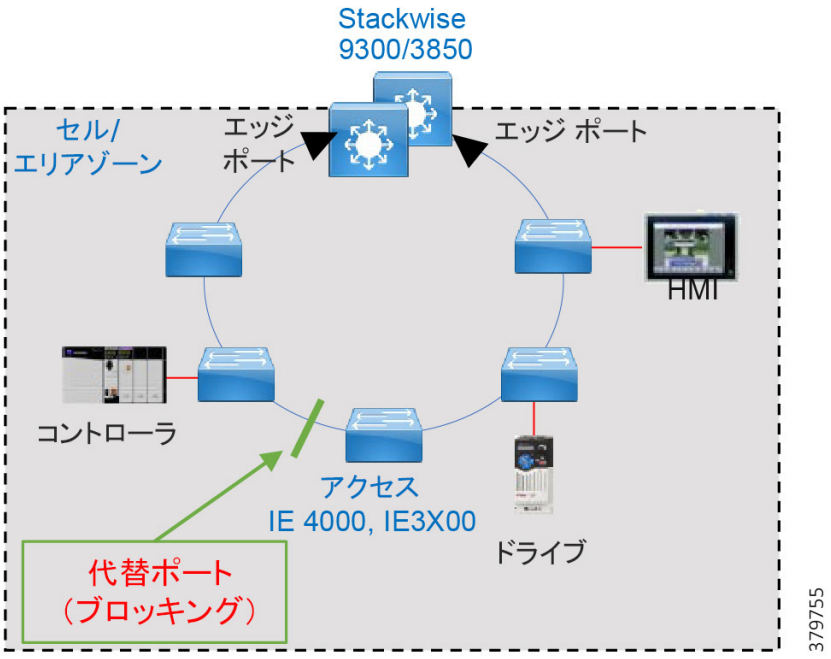
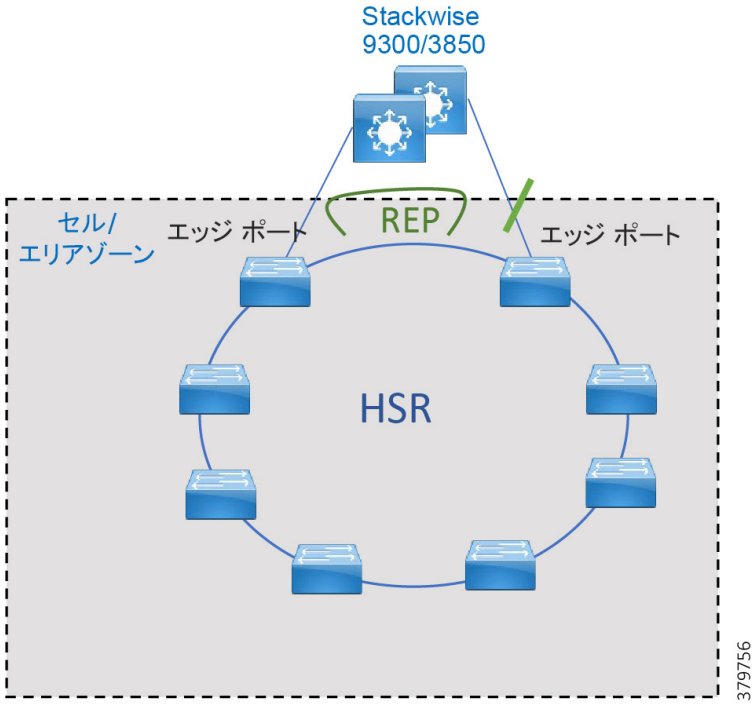


図 100　HSR リングをディストリビューションに接続するために使用される REP



REP のガイドライン

- REP ポートは、レイヤ 2 トランクポートである必要があります。
- REP およびスパニングツリープロトコル(STP)は、同じセグメントやインターフェイス上では実行できません。
- セグメントの最後の 1 つのポートを設定することから始めて、セグメント数とブロックされるポートの数を最小限に抑えるように隣接するポートを設定します。
- 1 つのデバイスに、同じセグメントに属するポートを複数設定することはできません。
- 各セグメントポートは、1 つの外部ネイバーのみを持つことができます。
- REP ポートは以下の規則に従います。
  - セグメント内のデバイスにポートが 1 つだけ設定されている場合、そのポートはエッジ ポートになります。
  - デバイスの 2 つのポートが同じセグメントに属している場合、両方のポートがエッジ ポートになるか、通常のセグメント ポートになります。
  - デバイス上の 2 つのポートが同じセグメントに属し、1 つがエッジポートとして設定され、もう 1 つが通常のセグメントポートとして設定されている場合は、**no-neighbor** コマンドオプションをエッジポートに適用する必要があります。

管理 VLAN の設定

VLAN ロード バランシング中のリンク障害または VLAN ブロッキング通知関連のメッセージ リレーで遅延が起こらないようにするには、REP は通常のマルチキャスト アドレスにハードウェア フラッド レイヤ(HFL)でパケットを大量に送信します。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 1 つのスイッチと 1 つのセグメント上には、1 つの管理 VLAN のみが存在できます。ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- インターフェイスで REP を設定する場合は、REP 管理 VLAN がトランキングカプセル化リストに含まれていることを確認します。

設定コマンド:

```
vlan <vlanID>
name REP_Admin_VLAN
rep admin vlan <vlanID>
```

インターフェイスでの REP の有効化

REP 動作の場合、各インターフェイス(セグメントの一部になる)で REP 有効にして、セグメント ID を指定します。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。その他のステップはすべて任意です。

Edge Port

ポートをエッジ ポートとして設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

```
rep segment ID edge (primary)
```

primary キーワードはオプションであり、プライマリエッジの手動選択を可能にします。primary キーワードを使用すると、もう一方のエッジポートがセカンダリエッジポート(キーワードは不要)になります。セカンダリエッジポートを設定するには、primary キーワードを省略します。

```
rep segment ID edge
```

非エッジポート

ポートを REP セグメントのメンバーとして設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

```
rep segment ID
```

プリエンプション

プリエンプションは、**rep preempt segment <** *ID* **>** コマンドを使用して手動で行うか、またはプライマリエッジポートに **rep preempt delay** *seconds* コマンドを設定すると自動的に実行されます。

リンク障害後にセグメントが回復すると、障害に隣接する 2 つのポートのうちの 1 つが ALT ポートとして起動します。その後、プリエンプションの後に、ALT ポートの位置がプライマリエッジポートになります（ロードバランシングと代替ポートの追加設定が行われていない場合）。

自動プリエンプションの例：

```
interface GigabitEthernet1/1
rep segment 30 edge primary
rep preempt delay 30
```

手動プリエンプションの例：

```
rep preempt segment 30
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]

Proceeding with Manual Preemption
```

代替ポートの選択

プライマリエッジポートでロードバランシング機能を設定し、次のコマンドでポート ID またはネイバーオフセット番号を使用して代替ポートを指定することで、エッジポート以外の代替ポートを選択できます。

```
rep block port id vlan vlan-list
```

Port ID

セグメント内のポートのポート ID を識別するには、次のコマンドを入力します。

```
show interface rep detail interface
```

ネイバーオフセット番号

セグメント内のポートのネイバーオフセット番号により、エッジポートのダウンストリーム ネイバー ポートが識別されます。ネイバー オフセット番号の範囲は -256 ～ 256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

例

次の例では、ネイバーオフセット番号を使用しています。この場合、代替ポートは 7 ポートダウンストリームです。

```
interface TenGigabitEthernet1/1/1
 rep segment 11 edge primary
 rep block port 7 vlan all
```

詳細については、『Cisco Industrial Ethernet 4000, 4010, and 5000 Switch Software Configuration Guide』を参照してください。
https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html

注:REP リングによるディストリビューションに Cisco StackWise を使用する場合は、プライマリスタックメンバーに電源障害が発生した場合の レイヤ 3 コンバージェンスを向上させるために、アクセススイッチ間に代替ポートを配置することをお勧めします。

REP のトラブルシューティング

REP 隣接関係のステータスを確認するために、次のコマンドを入力します。

```
show int gi1/7 rep
Interface Seg-id Type LinkOp Role
------------------------ ------ --------------- ----------- ----
GigabitEthernet1/7 10 Primary Edge TWO_WAY Alt
```

セグメント上の任意のルータで **show rep topology** コマンドを使用して、現在のトポロジを確認します。

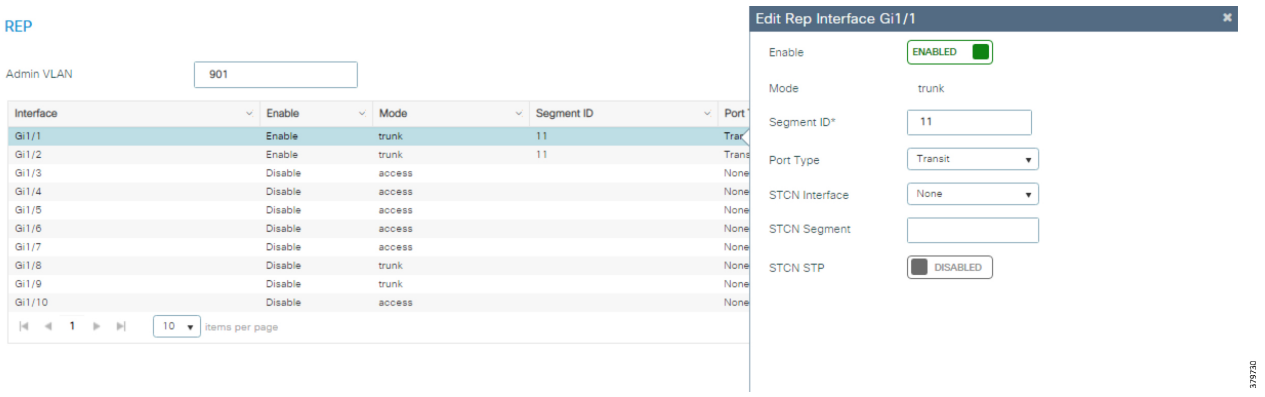
```
W2025-IE4K-RING#sh rep topology
REP Segment 10
BridgeName                       PortName   Edge Role
-------------------------------- ---------- ---- ----
W2024-IE4K-RING                  Gi1/1      Pri  Alt
W2023-IE4K-RING                  Gi1/1           Open
W2023-IE4K-RING                  Gi1/2           Open
W2022-IE4K-RING                  Gi1/2           Open
W2022-IE4K-RING                  Gi1/1           Open
W2021-IE4K-RING                  Gi1/1           Open
W2021-IE4K-RING                  Gi1/2           Open
W2026-IE4K-RING                  Gi1/2           Open
W2026-IE4K-RING                  Gi1/1           Open
W2025-IE4K-RING                  Gi1/1           Open
W2025-IE4K-RING                  Gi1/2           Open
W2024-IE4K-RING                  Gi1/2      Sec  Open
```

Device Manager を使用した REP の設定

このセクションでは、Cisco IE スイッチが管理アクセス用の IP アドレスを使用してインストールおよび設定されていることを前提としています。Cisco IE スイッチのセットアップの詳細については、対応するインストール ガイドを参照してください。

1. Device Manager のクレデンシャルを使用してスイッチにログインします。
2. [Configuration] メニューに移動します。
3. **[Layer 2] > [REP]** を選択します。
4. ドメイン全体(すべてのセグメント)の管理 VLAN を選択します。
5. インターフェイスの行をクリックして **[Edit Rep Interface]** ウィンドウを表示し、**[Enable]** をクリックしてインターフェイスで REP を有効にします。REP はデフォルトでは無効になっています。イネーブルにする際に、エッジ ポートとして設定されていなければインターフェイスは通常セグメント ポートになります。

図 101 REP の設定



6. **[Segment ID]** にセグメント ID を入力します。
7. [REPポートタイプ(REP Port Type)] で REP ポートタイプを選択します。

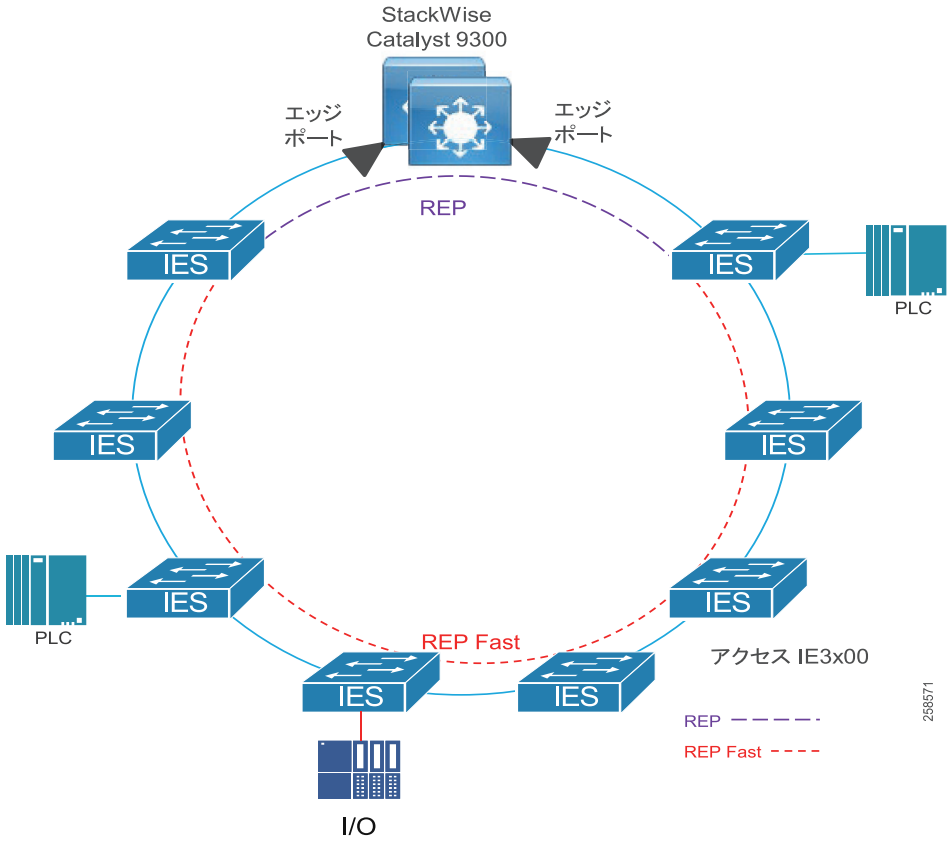
- [Edge]:VLAN ロード バランシングに参加するセカンダリ エッジ ポート。
- [Edge no-neighbor]:非 REP スイッチに接続されているセカンダリ エッジ ポート。
- [Preferred]:VLAN ロード バランシングの優先代替ポートであるセカンダリ エッジ ポート。
- [Edge no-neighbor preferred]:非 REP スイッチに接続されていて、VLAN ロード バランシングの優先ポートであるセカンダリ エッジ ポート。
- [Edge no-neighbor primary]:常にこの REP セグメントの VLAN ロード バランシングに参加し、非 REP スイッチに接続されているセカンダリ エッジ ポート。
- [Edge no-neighbor primary preferred]:常にこの REP セグメントの VLAN ロード バランシングに参加し、非 REP スイッチに接続されていて、VLAN ロード バランシングの優先ポートであるエッジ ポート。
- [Edge preferred]:VLAN ロード バランシングの優先代替ポートであるセカンダリ エッジ ポート。
- [Edge primary]:常にこの REP セグメントの VLAN ロード バランシングに参加するエッジ ポート。
- [Edge primary preferred]:常にこの REP セグメントの VLAN ロード バランシングに参加し、VLAN ロード バランシングの優先ポートであるエッジ ポート。
- [None]:このポートは REP セグメントの一部ではありません。これはデフォルトです。
- [Transit]:REP セグメントの非エッジ ポート。

8. (任意)セグメント トポロジ変更通知(STCN)を受信する物理インターフェイスを指定します。
9. (任意)STCN を受信する 1 つ以上のセグメントを識別します。STP ネットワークへの STCN の送信を有効にするには [Enable] を選択します。
10. [Update & Apply to Device] をクリックします。

REP Fast

Cisco IE 3x00 スイッチでサポートされている REP Fast 機能は、REP と同じ機能を備えていますが、参加しているスイッチ間の障害検出時間が改善されます。Rep Fast は、REP Fast をサポートしていないスイッチに対応するために、リング トポロジ内の従来の REP と組み合わせて使用できます。

図 102 REP Fast



REP のポートを設定した後、REP Fast に参加するすべてのポートで、インターフェイス コンフィギュレーション モードで次のコマンドを実行する必要があります。

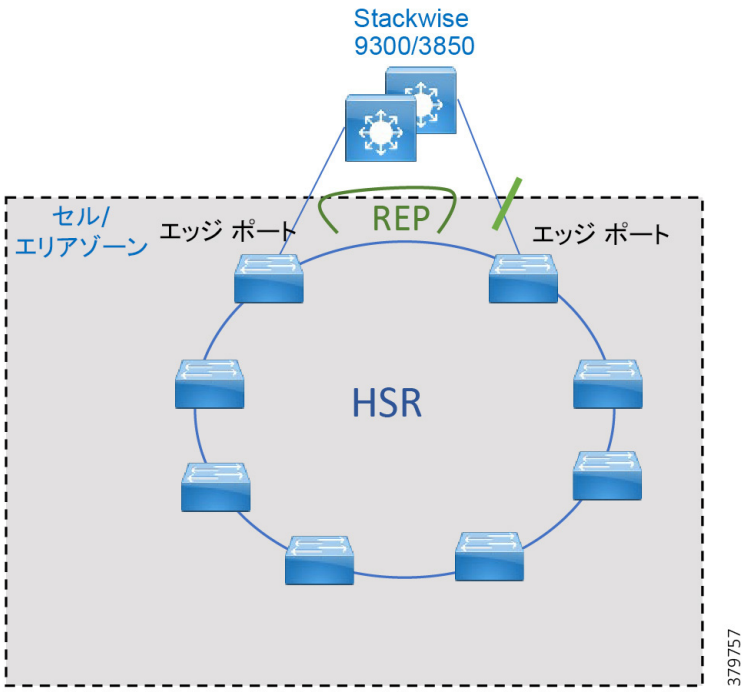
```
rep fastmode
```

Show rep topology コマンドに加えて、REP Fast に参加しているポートのビーコンフレーム数を表示するには、次のコマンドを使用できます。

```
show platform rep beacon interface interface-id
```

ハイ アベイラビリティ シームレス冗長性

図 103 HSR リング



HSR を設定する前に、HSR が有効になっているかどうかを確認してください。新しいバージョンではデフォルトで有効になっています。

```
show version | inc Feature
Feature Mode : 0x25 Enabled: HSR (Disabled: MRP TSN)
```

HSR が有効になっている場合は、この手順をスキップしてください。それ以外の場合は、次のコマンドを使用して有効にします。

```
license right-to-use activate hsr
```

変更を有効にするには、スイッチをリロードする必要があります。プロンプトが表示されたらリロードを確認し、スイッチがリロードして起動するのを待ちます。HSR 機能がアクティブになっていることを確認します。

HSR リングを設定する前に、HSR リングのメンバーインターフェイスが、FlexLinks、EtherChannel、REP などの冗長プロトコルに参加していないことを確認します。

HSR の設定

HSR を設定するには、次の手順に従います。

1. HSR リングを設定する前に、ポートをシャットダウンします。

```
interface range GigabitEthernet1/1-2
  shutdown
```

2. 必要に応じて、スイッチポートと Vlan を設定します。

```
switchport mode trunk
switchport trunk allowed vlan 10,20,900 switchport trunk native vlan 900
```

3. Precision Time Protocol（PTP）を無効にします（HSR インターフェイスではサポートされていません）。

```
no ptp enable
```

4. HSR リングインターフェイスを作成し、ポートを HSR リングに割り当てます。このコマンドは、インターフェイス コンフィギュレーション モードで発行する必要があります。2 つのインターフェイスは、HSR インターフェイスにバンドルされます。

```
hsr-ring 1
```

5. HSR インターフェイスをオンにします。

```
no shutdown
```

6. 有効な DualUplinkEnhancement 機能が無効にならないことを確認します。この機能は、ディストリビューション レイヤのデュアル ルータ（この場合は HSRP）への接続をサポートするために必要です。

```
show run | include fpgamode-DualUplinkEnhancement
```

7. 出力に「no hsr-ring 1 fpgamode-DualUplinkEnhancement」と表示される場合は、次のコマンドを発行します。

```
hsr-ring 1 fpgamode-DualUplinkEnhancement
```

8. HSR リング ノードに関する情報を提供するように CDP および LLDP を設定するには、次のオプション手順に従います。

   – LLDP をグローバルに有効にします。

```
lldp run
```

   – HSR リングに割り当てるポートで LLDP を有効にします。

```
interface range GigabitEthernet1/1-2
lldp transmit
lldp receive
```

   – HSR リングに割り当てるポートで CDP を有効にします。

```
interface range GigabitEthernet1/1-2
cdp enable
```

9. HSR アラームを有効にするには、次のオプション手順に従います。

   – HSR アラーム機能を有効にします。

```
alarm facility hsr enable
```

   – HSR アラームの SNMP 通知を有効にします。

```
alarm facility hsr notifies
```

   – HSR アラームをメジャーリレーに関連付けます。

```
alarm facility hsr relay major
```

REP による HSR のベストプラクティス

- REP プリエンプションが必要である場合は、計画外のダウンタイムを回避するために、手動プリエンプションを実行することをお勧めします。REP プリエンプションは、REP セグメントに接続されているノードに影響を与えるマルチキャスト ツリーの再コンバージェンスを引き起こす可能性があります。
- REP セグメントの場合、HSRP スレーブに直接接続されている Cisco IE 4000 のエッジポートはプライマリにする必要があるため、プリエンプションではそのポートがデフォルトでブロックされます。

- トポロジ変更後にポートがブロック状態にならないようにするには、HSR リングに参加している Cisco IE 4000 上のエンドデバイスおよびディストリビューションに接続しているポートでブリッジ プロトコル データ ユニット（BPDU）フィルタリングを有効にします。
- HSRP スプリットブレインシナリオを回避するために、リングで使用されている VLAN のディストリビューション スイッチのアクセス ポートは使用しないでください。デバイスをディストリビューション スイッチに直接接続する場合は、別の VLAN を使用してください。

HSR のトラブルシューティング

表 52 の **show** コマンドを使用して HSR をトラブルシューティングできます。

表 52　HSR トラブルシューティングコマンド

コマンド	目的
show hsr ring { 1 | 2 } [detail]	指定された HSR リングの設定の詳細と現在の状態が表示されます。
show hsr statistics	HSR コンポーネントの統計情報が表示されます。HSR 統計情報をクリアするには、**clear hsr statistics** コマンドを入力します。
show hsr node-table	HSR インターフェイスを使用してスイッチにアクセス可能なすべての MAC アドレスが表示されます。リング内の他のノードと、他のノードに接続されたデバイスが含まれます。
show hsr vdan-table	HSR 仮想二重接続ノード（VDAN）テーブルが表示されます。このスイッチがプロキシとなっているスイッチに直接接続されたデバイスが含まれます。この表は「プロキシノードテーブル」とも呼ばれます。
show cdp neighbors および **show lldp neighbors**	スイッチのネイバー情報が表示されます。この情報は、接続に関する問題のトラブルシューティングに役立ちます。
show alarm settings | begin hsr	HSR アラーム設定が表示されます。

HSR リングの詳細の例：

```
IE4000-1# sh hsr ring 2 detail
HSR-ring: HS2
------------
Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
1) Port: Gi1/3
Logical slot/port = 1/3 Port state = Inuse ' Port is up
Protocol = Enabled
2) Port: Gi1/4
Logical slot/port = 1/4 Port state = Inuse ' Port is up
Protocol = Enabled

Ring Parameters:
Redbox MacAddr: f454.3365.8a84
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
```

```
Life Check Interval: 2000 ms
Pause Time: 25 ms
fpgamode-DualUplinkEnhancement: Enabled
```

表 53　HSR イベントリスト

イベント番号	イベントの説明	システムログ（レベル）	アラート/アラームログ	アラーム LED と出力リレー
1	リングが稼働状態からダウン状態になります。	2	2	メジャーアラーム/アサート
2	リングがダウン状態から稼働状態になります。	6	6	デアサート
3	1 つのリングポートがダウン状態になり、別のリングポートとリング自体が稼働状態になります。	3	3	
4	両方のリングポートが再び稼働状態になっています。	6	6	

HSR イベント

show facility alarm status コマンドを使用して現在アクティブなアラームを表示できます。次の例は、マイナーおよびメジャー HSR アラームのアラームステータスを示しています。

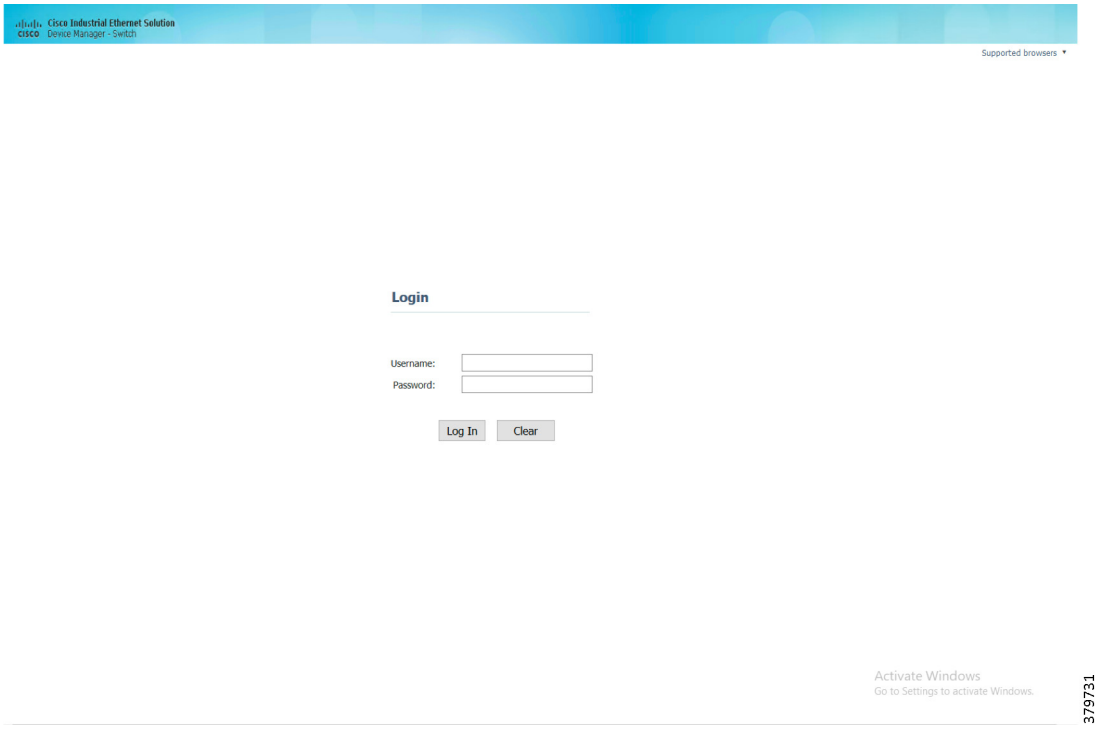
```
show facility-alarm status
Source Severity Description Relay Time
Switch MINOR 34 HSR ring is partially down MAJ Oct 24 2017 10:16:10
-------
show facility-alarm status
Source Severity Description Relay Time
Switch MAJOR 33 HSR ring is down MAJ Oct 24 2017 10:17:07
```

Device Manager を使用した HSR の設定

ここでは、Cisco IE スイッチが配備され、リモートアクセス用の IP アドレスを使用して設定されていることが前提となっています。Cisco IE スイッチのセットアップの詳細については、対応するインストール ガイドを参照してください。

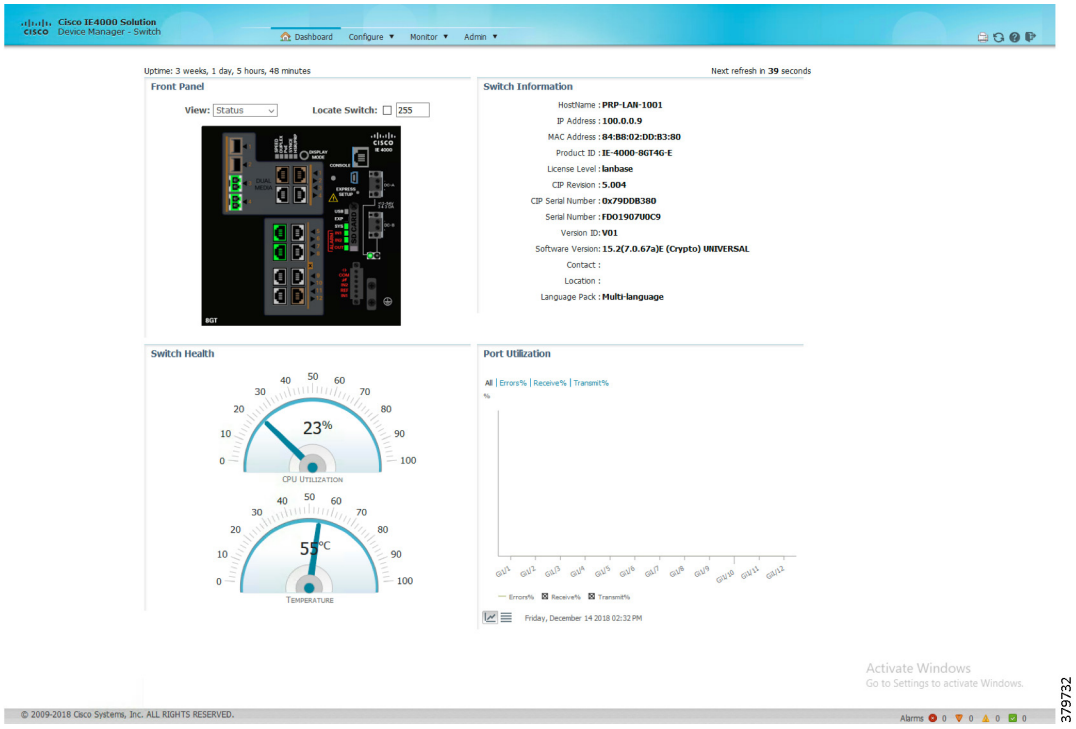
1. Device Manager のクレデンシャルを使用してスイッチにログインします。

図 104 Device Manager のログイン画面



2. ログインに成功すると、スイッチのダッシュボードがロードされます。

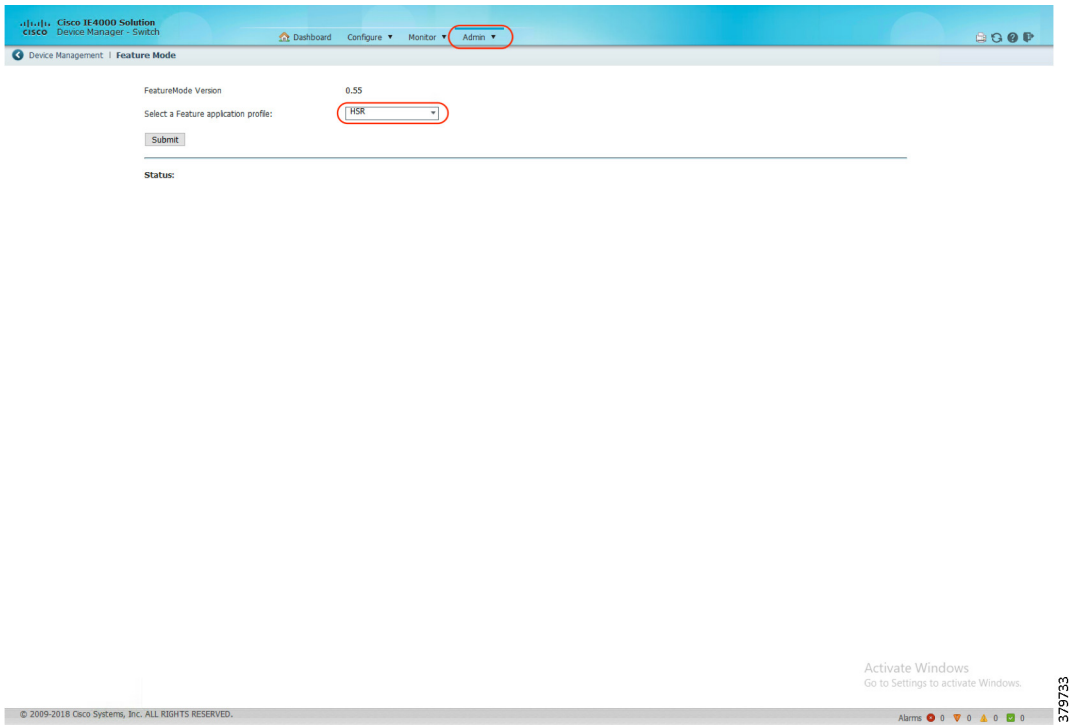
図 105 Cisco IE 4000 Device Manager のダッシュボード



379732

3. 図 106 に示されているオプションを使用して、Cisco IE スイッチで HSR 機能を有効にします。

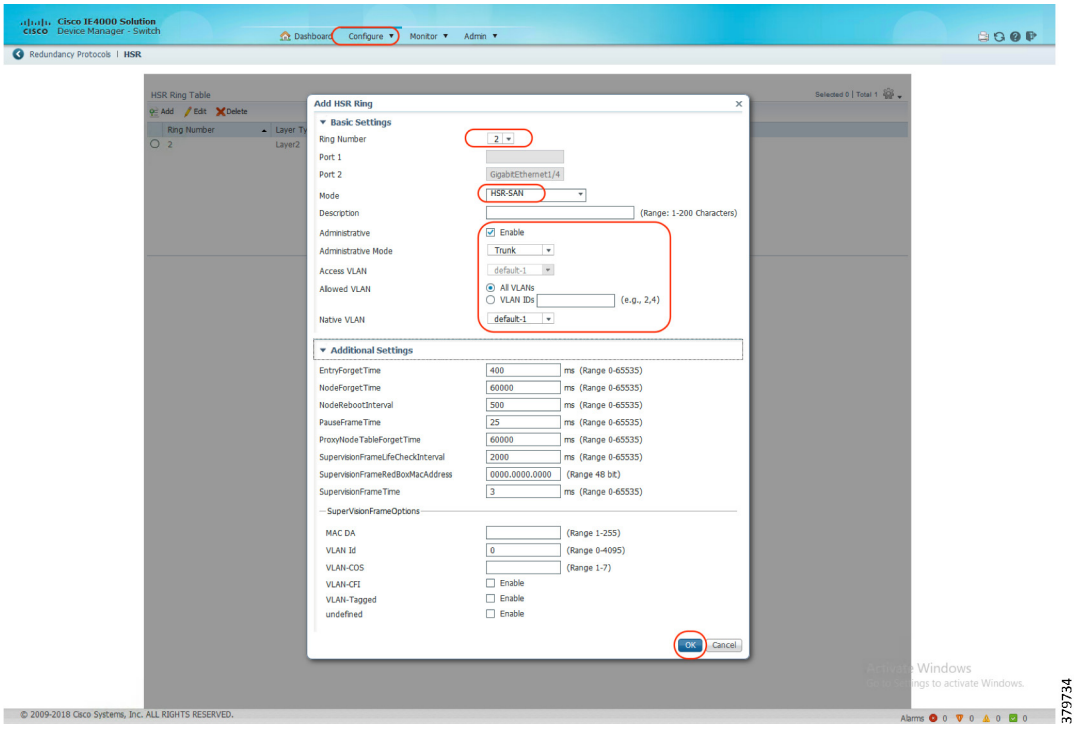
図 106 HSR 機能の有効化



379733

4. 図 107 に示されているオプションを使用して、Cisco IE スイッチで HSR リングとその関連パラメータを設定します。

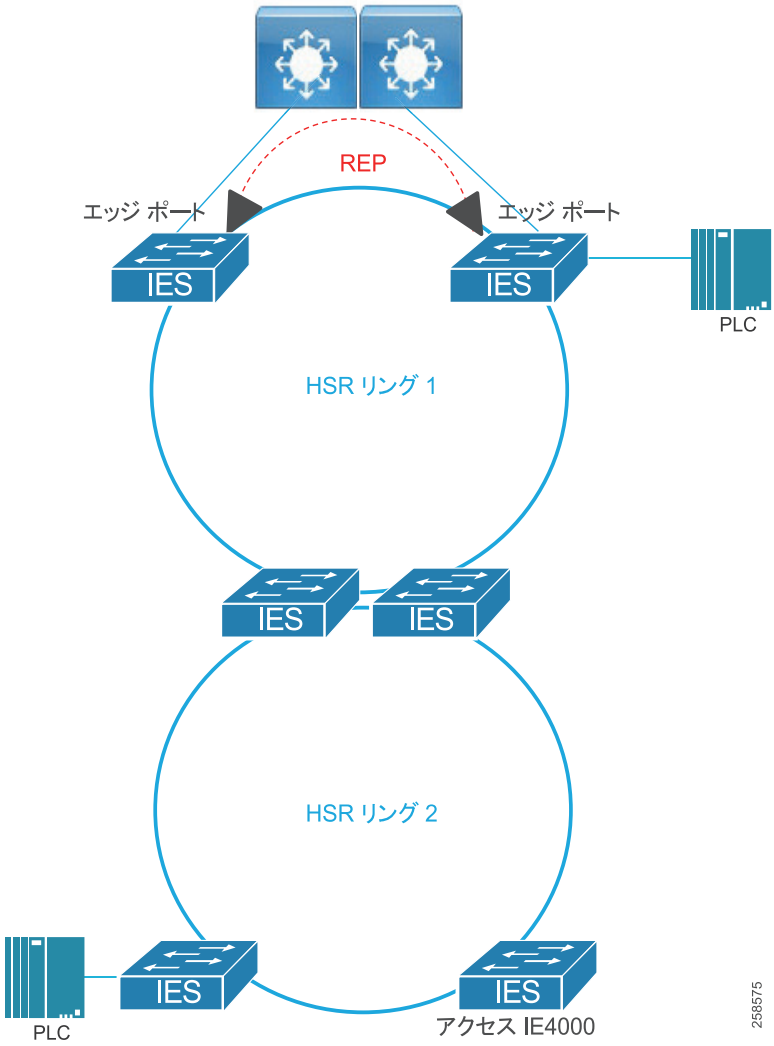
図 107 HSR リングのパラメータ



HSR-HSR

HSR リングも、キースイッチが 2 つの HSR リングに参加しているのと同様の方法で実装できます。これには、HSR-HSR または Quadbox と呼ばれるそれぞれのリングを接続するための 4 つのインターフェイスを使用します。HSR-HSR モードがライセンスされ、有効になっている場合、スイッチはトラフィックの干渉を回避するために、すべての非 HSR ポートを閉鎖します。HSR-HSR スイッチへの接続は、HSR-HSR ポートまたはアウトオブバンド コンソール インターフェイスを介して行うことができます。

図 108 HSR-HSR



上記のすべての HSR 設定は、リング内のすべてのスイッチに必要です。Quadbox スイッチでは、コンフィギュレーションモードで次の追加コマンドが必要です。

```
hsr-hsr-mode enable
```

最初の 2 つのギガビットインターフェイスは HSR-ring1 に使用され、2 番目の 2 つのギガビットインターフェイスは HSR-ring2 に使用されます。

HSR-HSR モードでの HSR リングのサマリーの例:

```
IE4000#sho hsr ring summary
Flags:  D - down        H - bundled in HSR-ring
        R - Layer3      S - Layer2
        U - in use

Number of hsr-rings in use: 2
Group   HSR-ring     Ports
------+------------+----------------------------------------
1       HS1(SU)       Gi1/1(H), Gi1/2(H)
2       HS2(SU)       Gi1/3(H), Gi1/4(H)
```

HSR-HSR モードでの HSR リングの詳細の例:

```
IE4000#show hsr ring detail
               HSR-ring listing:
               --------------------

HSR-ring: HS1
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-hsr
Ports in the ring:
  1) Port: Gi1/1
   Logical slot/port = 1/1      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/2
   Logical slot/port = 1/2      Port state = Inuse
        Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: 84b2.6177.4c82
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled

HSR-ring: HS2
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-hsr
Ports in the ring:
  1) Port: Gi1/3
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/4
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: 84b2.6177.4c84
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled
```

HSR-PRP RedBox（デュアル RedBox）

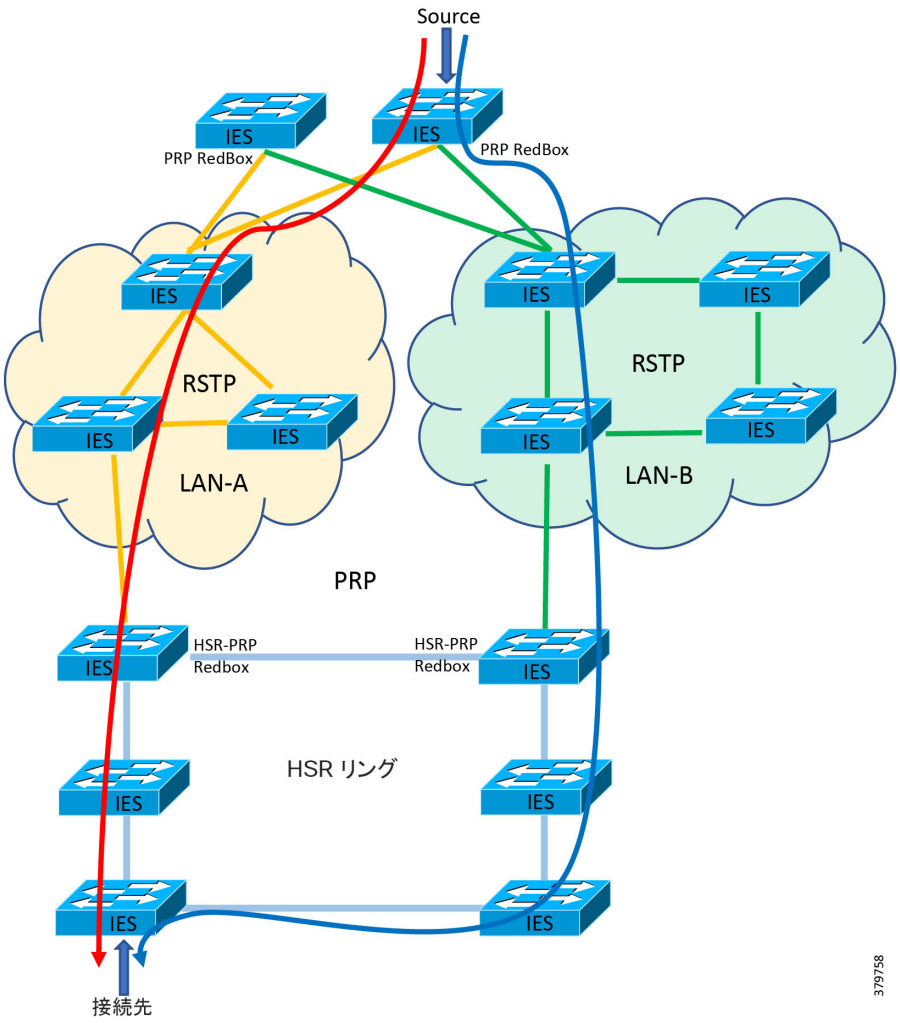
冗長性ボックス（RedBox）は、エンド ノードが 2 つのネットワーク インターフェイスと PRP 冗長性をサポートしていない場合に導入されます。RedBox は、それに接続するデバイスの DAN 機能を提供します。これは、PRP 冗長の導入における Cisco IE 4000 または Cisco IE 4010 と Cisco IE 5000 の役割です。RedBox の背後にあるノードは、DAN などの他のノードに表示され、「仮想 DAN（VDAN）」と呼ばれます。

HSR-PRP RedBox（「デュアル RedBox」とも呼ばれる）は、PRP ネットワークと HSR ネットワークをいっしょに接続するために使用されます。HSR-PRP 機能は Cisco IE 4000 でのみサポートされています。

HSR-PRP 機能の一般的な導入では、2 つのスイッチを使用して、2 つの異なる LAN、つまり PRP ネットワークおよび HSR ネットワークの LAN-A と LAN-B に接続します。PRP ネットワークと HSR ネットワーク間のトラフィックは RedBox を介して流れます。RedBox は、ループを避けるために、重複したフレームを同じ方向に転送しません。RedBox は PRP フレームを HSR フレームに（またその逆に）変換します。

図 109 に 2 つの RedBox（各 LAN に 1 つずつ）を介して PRP ネットワークに接続される HSR リングを示しています。この例では、送信元フレームは PRP ネットワーク内で発信され、HSR ネットワーク内の宛先に到達します。RedBox は、インターリンクポート上の PRP トラフィックとリングポート上の HSR トラフィックをサポートするように設定されます。

図 109 HSR-PRP RedBox



スイッチで HSR-PRP モードを設定するには、次の手順に従います。HSR-PRP モードを有効にすると、HSR リングと PRP チャネルが作成されます。

はじめる前に

- HSR-PRP モードを有効にすると、2 つの HSR ポートと 1 つの PRP ポート以外のすべてのポートが無効になり、これらの無効なポートのすべてのポート設定がデフォルト値に戻ります。インターフェイス設定が削除されることを通知する警告メッセージが表示されます。HSR-PRP モードを有効または無効にする前に、スイッチに接続されているケーブルを確認し、ポートのステータスを確認してください。
- HSR-PRP RedBox モードでは、ポート Gi1/3 とポート Gi1/4 が HSR リング 2 インターフェイスとして使用され、ポート Gi1/1（RedBox A 用）またはポート Gi1/2（RedBox B 用）が PRP チャネル 1 インターフェイスとして使用されます。これらのポート割り当ては固定されており、変更できません。そのため、HSR-PRP デュアル RedBox モードは HSR リング 2 でのみサポートされます。
- PRP アップリンクインターフェイスは、アクセス、トランク、またはルーテッドインターフェイスとして設定できます。
- PRP デュアル通信ノードと RedBoxes は、6 バイトの PRP トレーラーをパケットに追加します。すべてのパケットが PRP ネットワークを通過できるようにするには、PRP LAN-A と LAN-B ネットワーク内のスイッチの最大伝送ユニット（MTU）サイズを次のように1506に増やします。

```
system mtu 1506
system mtu jumbo 1506
```

- インテリジェント電子デバイス（IED）が VLAN 0 タグ付きパケットを送信する場合は、IED 側のインターフェイスとアップリンク インターフェイスを、VLAN 1 およびその他の必要な VLAN を許可するトランクポートとして設定することをお勧めします。

```
interface gigabitEthernet 1/5
    switchport mode trunkswitchport trunk
    allowed vlan 1
```

推奨されるベストプラクティス

- PTP が不要なインターフェイスで PTP を無効にします。
- アクセス側のインターフェイスでブロードキャスト、マルチキャストトラフィックのストーム制御を有効にします。

```
interface GigabitEthernet1/5
    storm-control broadcast level pps 1k
    storm-control multicast level pps 5k
    storm-control action shutdown
    storm-control action trap
```

- マルチキャスト、ブロードキャストメッセージの他のデバイスへのフラッディングを回避するために、異なる IED には異なる VLAN を設定します。

HSR-PRP RedBox の設定

1. HSR 機能モードをアクティブにします。

```
license right-to-use activate hsr
```

注:変更を有効にするために、スイッチをリロードします。プロンプトが表示されたらリロードを確認し、スイッチがリロードして起動するのを待ちます。

2. HSR 機能がアクティブになっていることを確認します。

```
show version | inc Feature
Feature Mode: 0x25 Enabled: HSR (Disabled: MRP TSN)
```

3. グローバル コンフィギュレーション モードを開始します。

```
configure terminal
```

4. HSR-PRP モードを有効にして、LAN-A または LAN-B と PRP ネット ID を選択します。

```
hsr-prp-mode enable prp-lan-a 1
```

注：PRP LAN：prp-lan-a-RedBox Interlink は LAN-A に接続され、prp-lan-b-RedBox Interlink は LAN-B に接続されます。

5. 「**yes**」と入力して、HSR-PRP モードの有効化を確認します。HSR-PRP RedBox モードを無効にするには、次のコマンドを使用します。

```
no hsr-prp-mode enable
```

6. インターフェイス コンフィギュレーション モードに入り、HSR リングに割り当てるポートで PTP を無効にします。

```
interface range gigabitEthernet 1/3-4
   no ptp enable
```

注：HSR リングを介した PTP 機能は、現在サポートされていません。

7. HSR リングを設定する前に、ポートをシャットダウンします。

```
shutdown
```

8. HSR リングインターフェイスを作成します。

```
interface HSR-ring2
    switchport mode trunk
```

9. HSR リングを物理インターフェイスに割り当てます。

```
interface range gigabitEthernet 1/3-4
    hsr-ring 2
    no shutdown
```

10. PRP LAN インターフェイスを作成します。2 つ目の HSR-PRP RedBox で手順を繰り返します。

```
interface PRP-channel1
   switchport mode trunk
```

11. PRP チャネルを物理インターフェイスに割り当てます。スイッチの役割と対応するインターフェイスを識別するガイドラインに従ってください。

```
interface range gigabitEthernet 1/1
    prp-channel-group 1
    no shutdown
```

表 54　HSR-PRP RedBox Cisco IE 4000 インターフェイスマッピング。

SKU	HSR モード	ポート タイプ	インターフェイス番号
IE4000	HSR-PRP	PRP-LAN-A（RedBox A）	PRP チャネル インターフェイス：Gi1/1（ポート 3） HSR リング インターフェイス：Gi1/3（ポート 1）、Gi1/4（ポート2） Gi 1/2 は使用されない。
		PRP-LAN-B（RedBox B）	PRP チャネル インターフェイス：Gi1/2（ポート 3） HSR リング インターフェイス：Gi1/3（ポート 1）、Gi1/4（ポート2） Gi 1/2 は使用されない

12. 「HSR の設定（183 ページ）」を参照して、HSR リングに含まれる他のスイッチで HSR リングを設定します。

13. 「PRP RedBox の設定（199 ページ）」を参照して、PRP ネットワークに含まれる、必要なスイッチで PRP を設定します。

HSR-PRP RedBox のトラブルシューティング

HSR-PRP Redbox を検証してトラブルシューティングするには、次のコマンドを使用します。

```
show prp channel detail
                PRP-channel listing:
                --------------------

PRP-channel: PR1
------------
 Layer type = L2
 Ports: 1       Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Disabled
Ports in the group:
  1) Port: Gi1/1
   Logical slot/port = 1/1      Port state = Inuse
        Protocol = Disabled

show hsr ring detail
                HSR-ring listing:
                --------------------

HSR-ring: HS2
------------
 Layer type = L2
 Operation Mode = mode-H
 Ports: 2       Maxports = 2
 Port state = hsr-ring is Inuse
 Protocol = Enabled  Redbox Mode = hsr-prp-lan-a  PathId = 1
Ports in the ring:
  1) Port: Gi1/3
   Logical slot/port = 1/3      Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/4
   Logical slot/port = 1/4      Port state = Inuse
        Protocol = Enabled

Ring Parameters:
 Redbox MacAddr: 84b8.02dd.c604
 Node Forget Time: 60000 ms
 Node Reboot Interval: 500 ms
 Entry Forget Time: 400 ms
 Proxy Node Forget Time: 60000 ms
 Supervision Frame COS option: 0
 Supervision Frame CFI option: 0
 Supervision Frame VLAN Tag option: Disabled
 Supervision Frame MacDa: 0x00
 Supervision Frame VLAN id: 0
 Supervision Frame Time: 3 ms
 Life Check Interval: 1600 ms
 Pause Time: 25 ms
 fpgamode-DualUplinkEnhancement: Enabled

show hsr statistics egressPacketStatistics
 HSR ring 1 EGRESS STATS:
   duplicate packets: 0
   supervision frames: 0
   packets sent on port A: 0
   packets sent on port B: 0
   byte sent on port a: 0
   byte sent on port b: 0
 HSR ring 2 EGRESS STATS:
```

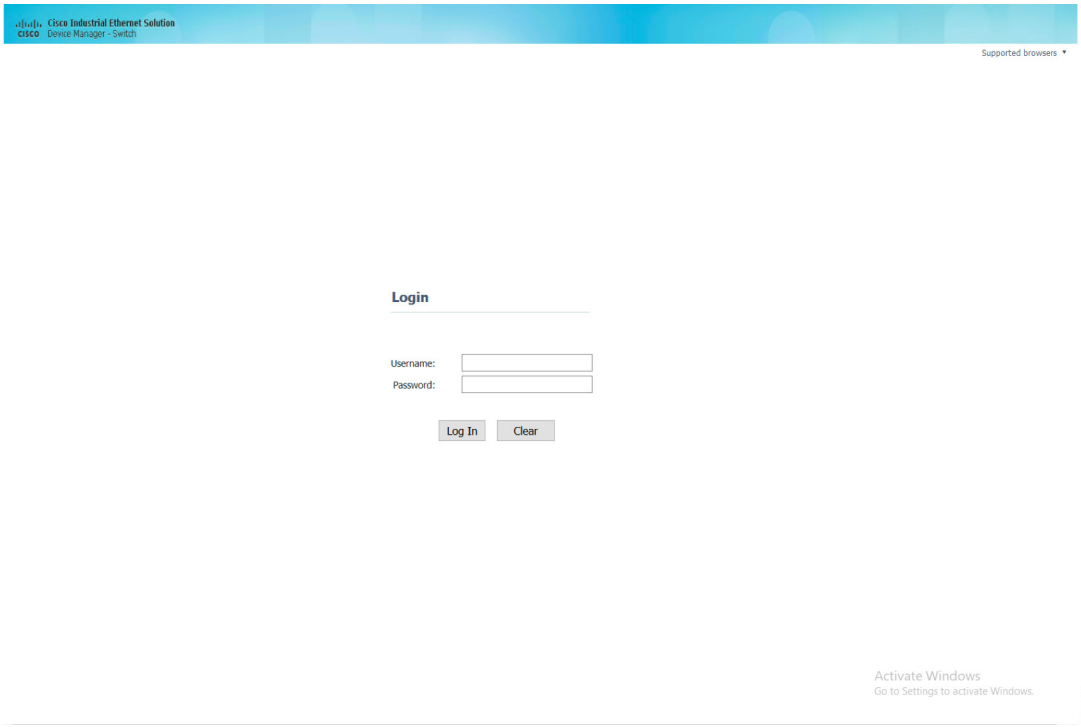
```
    duplicate packets: 472617535
    supervision frames: 2908371
    packets sent on port A: 472617493
    packets sent on port B: 472616962
    byte sent on port a: 806518995400
    byte sent on port b: 811359936926

show hsr statistics ingressPacketStatistics
 HSR ring 1 INGRESS STATS:
    ingress pkt port A: 0
    ingress pkt port B: 0
    ingress crc port A: 0
    ingress crc port B: 0
    ingress danh pkt portAcpt: 0
    ingress danh pkt dscrd: 0
    ingress supfrm rcv port A: 0
    ingress supfrm rcv port B: 0
    ingress overrun pkt port A: 0
    ingress overrun pkt port B: 0
    ingress byte port a: 0
    ingress byte port b: 0
 HSR ring 2 INGRESS STATS:
    ingress pkt port A: 4729843950
    ingress pkt port B: 5049046881
    ingress crc port A: 0
    ingress crc port B: 0
    ingress danh pkt portAcpt: 5325183746
    ingress danh pkt dscrd: 3939164759
    ingress supfrm rcv port A: 21780902
    ingress supfrm rcv port B: 28970004
    ingress overrun pkt port A: 0
    ingress overrun pkt port B: 0
    ingress byte port a: 714469348360
    ingress byte port b: 806539236074

clear hsr statistics
```

Device Manager を使用した HSR-PRP RedBox の設定

ここでは、Cisco IE スイッチが配備され、リモートアクセス用の IP アドレスを使用して設定されていることが前提となっています。Cisco IE スイッチのセットアップの詳細については、対応するインストール ガイドを参照してください。

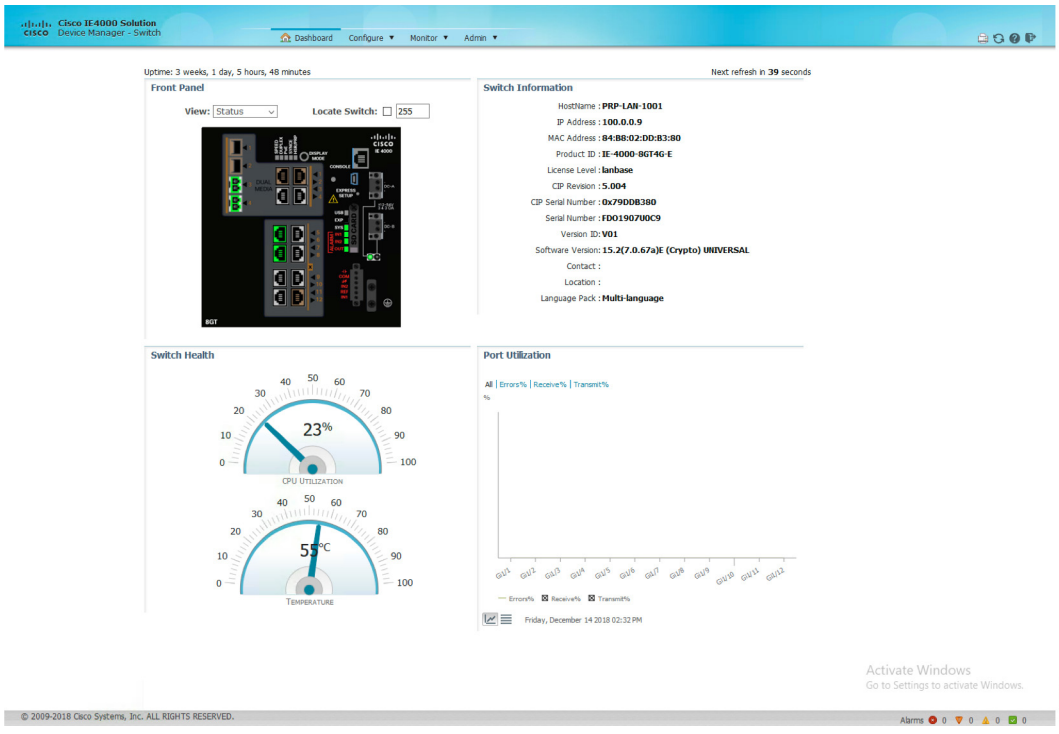
1. Device Manager のクレデンシャルを使用してスイッチにログインします。

図 110 Device Manager のログイン画面



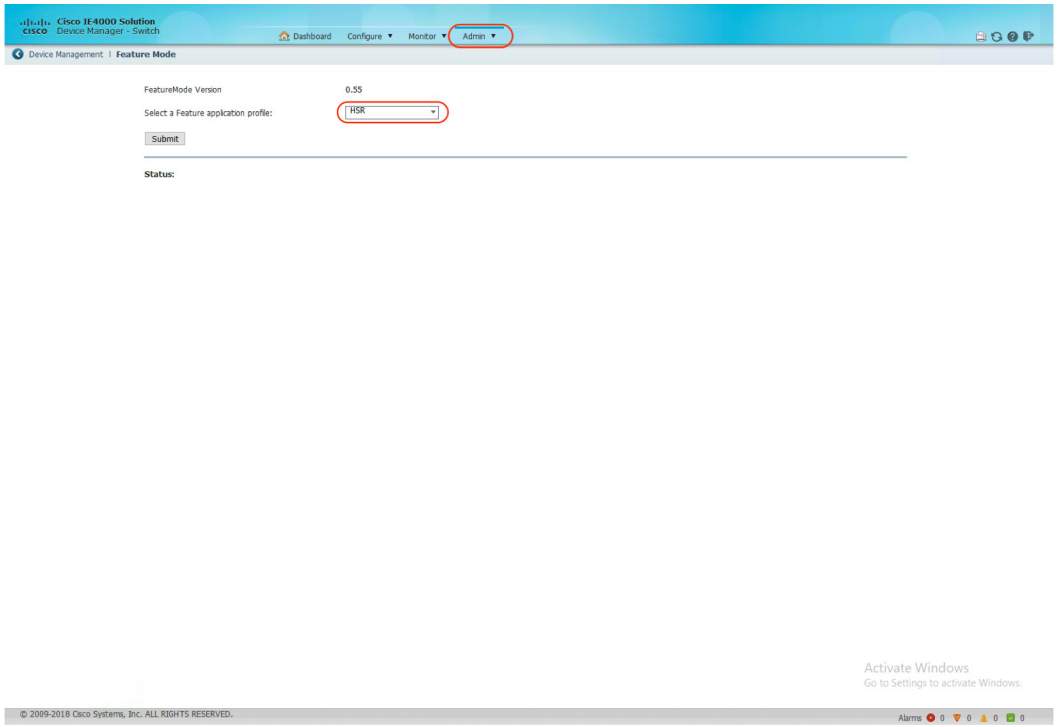
2. ログインに成功すると、スイッチのダッシュボードがロードされます。

図 111 Cisco IE 4000 Device Manager のダッシュボード



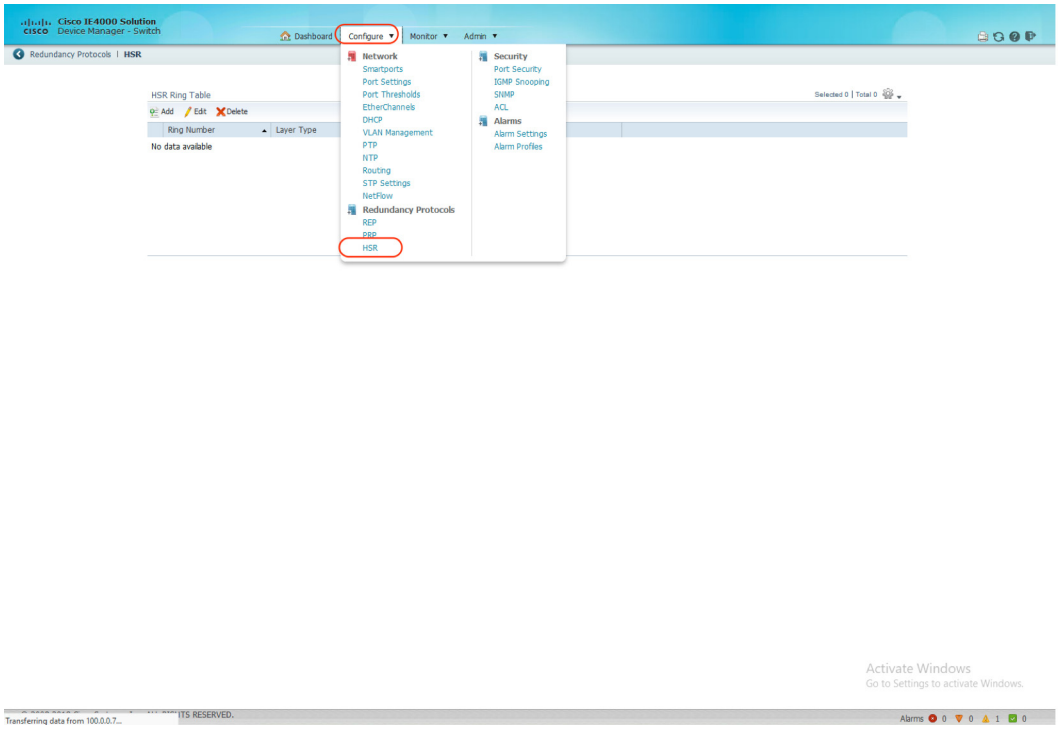
3. 図 112 に示されているオプションを使用して、Cisco IE スイッチで HSR 機能を有効にします。[Admin] タブを選択し、[Feature Mode] オプションを選択してから、必要な機能モードとして [HSR] を選択します。

図 112 HSR 機能の有効化



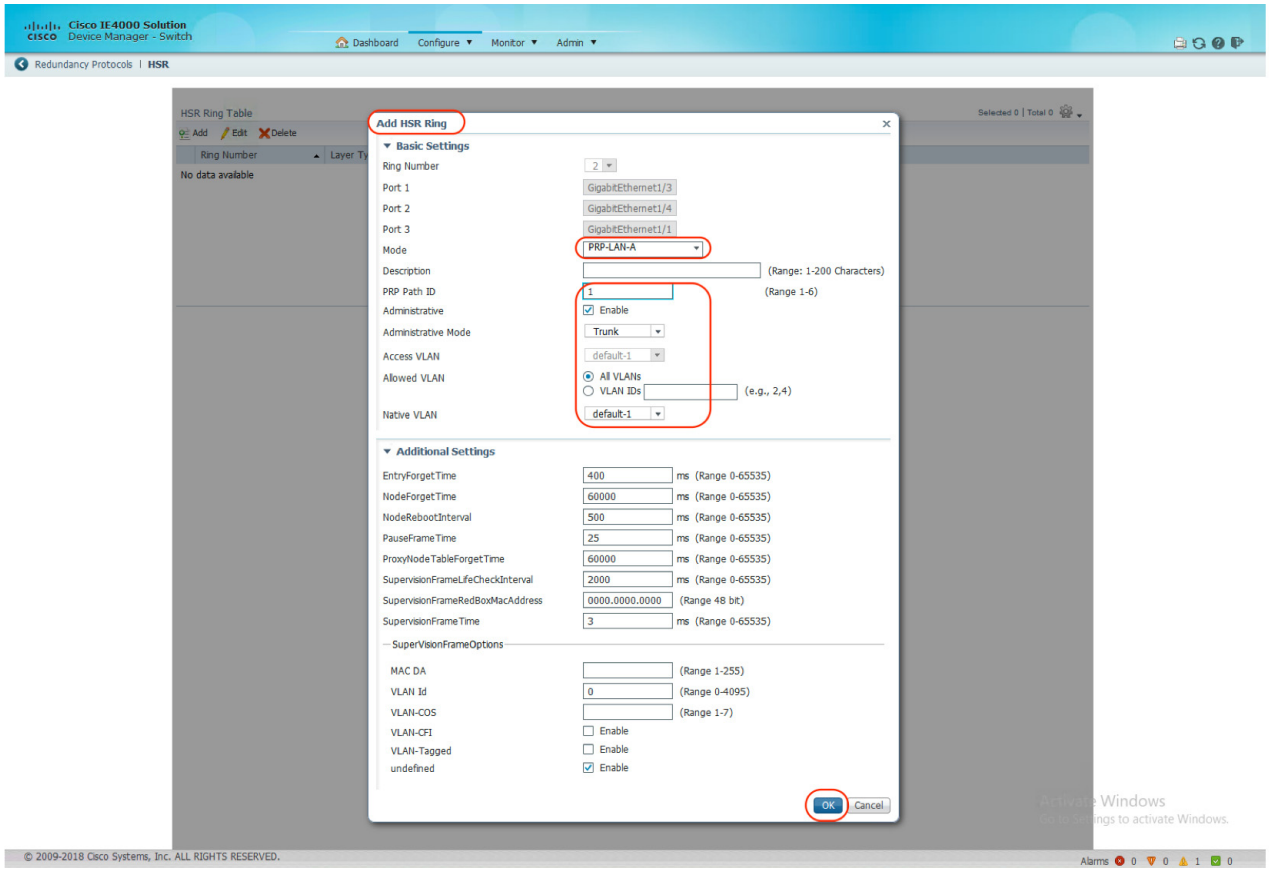
4. 図 113 に示されている手順を選択して、HSR-PRP Redbox を設定します。

図 113 HSR 機能の設定



5. 図 114 に示されているオプションを使用して、Cisco IE スイッチで HSR-PRP RedBox パラメータを設定します。

図 114 HSR-PRP パラメータの設定



PRP RedBox の設定

表 55 PRP Redbox インターフェイスマッピング

SKU	インターフェイス マッピング
IE4000	PRP チャネルグループ 1 は常に LAN_A には Gi1/1 を使用し、LAN_B には Gi1/2 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/3 を使用し、LAN_B には Gi1/4 を使用します。
IE4010	PRP チャネルグループ 1 は常に LAN_A には Gi1/25 を使用し、LAN_B には Gi1/26 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/27 を使用し、LAN_B には Gi1/28 を使用します。
IE5000	PRP チャネルグループ 1 は常に LAN_A には Gi1/17 を使用し、LAN_BP には Gi1/18 を使用します。 RP チャネルグループ 2 は常に LAN_A には Gi1/19 を使用し、LAN_B には Gi1/20 を使用します。

サポートされている Cisco IE スイッチで PRP チャネルおよびグループを作成して有効にするには、次の手順に従います。

1. グローバル コンフィギュレーション モードを開始します。

```
configure terminal
```

2. PRP LAN インターフェイスを作成します。

```
interface PRP-channel1
    switchport mode trunk
```

3. PRP チャネルを物理インターフェイスに接続します。スイッチの役割と対応するインターフェイスを識別するガイドラインに従ってください。

```
interface range gigabitEthernet 1/1
   prp-channel-group 1
   no shutdown
```

表 56　PRP Redbox インターフェイスマッピング

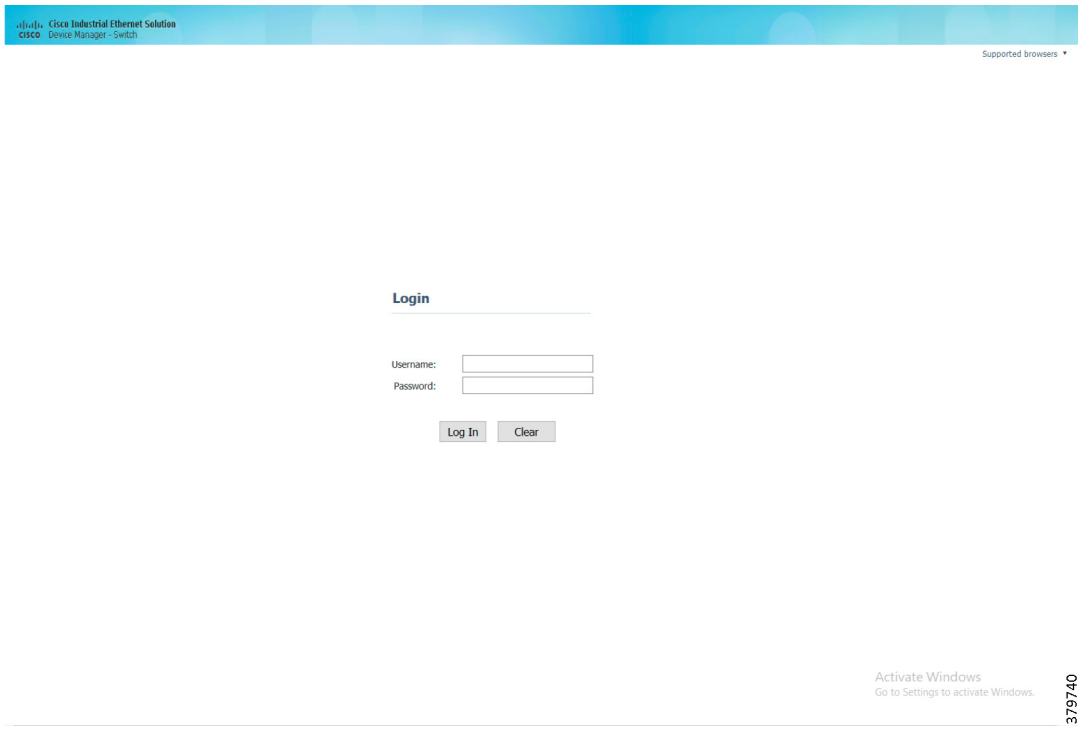
SKU	インターフェイス マッピング
IE4000	PRP チャネルグループ 1 は常に LAN_A には Gi1/1 を使用し、LAN_B には Gi1/2 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/3 を使用し、LAN_B には Gi1/4 を使用します。
IE4010	PRP チャネルグループ 1 は常に LAN_A には Gi1/25 を使用し、LAN_B には Gi1/26 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/27 を使用し、LAN_B には Gi1/28 を使用します。
IE5000	PRP チャネルグループ 1 は常に LAN_A には Gi1/17 を使用し、LAN_BP には Gi1/18 を使用します。 RP チャネルグループ 2 は常に LAN_A には Gi1/19 を使用し、LAN_B には Gi1/20 を使用します。

Device Manager を使用した PRP RedBox の設定とモニタ

ここでは、Cisco IE スイッチが配備され、リモートアクセス用の IP アドレスを使用して設定されていることが前提となっています。Cisco IE スイッチのセットアップの詳細については、対応するインストール ガイドを参照してください。

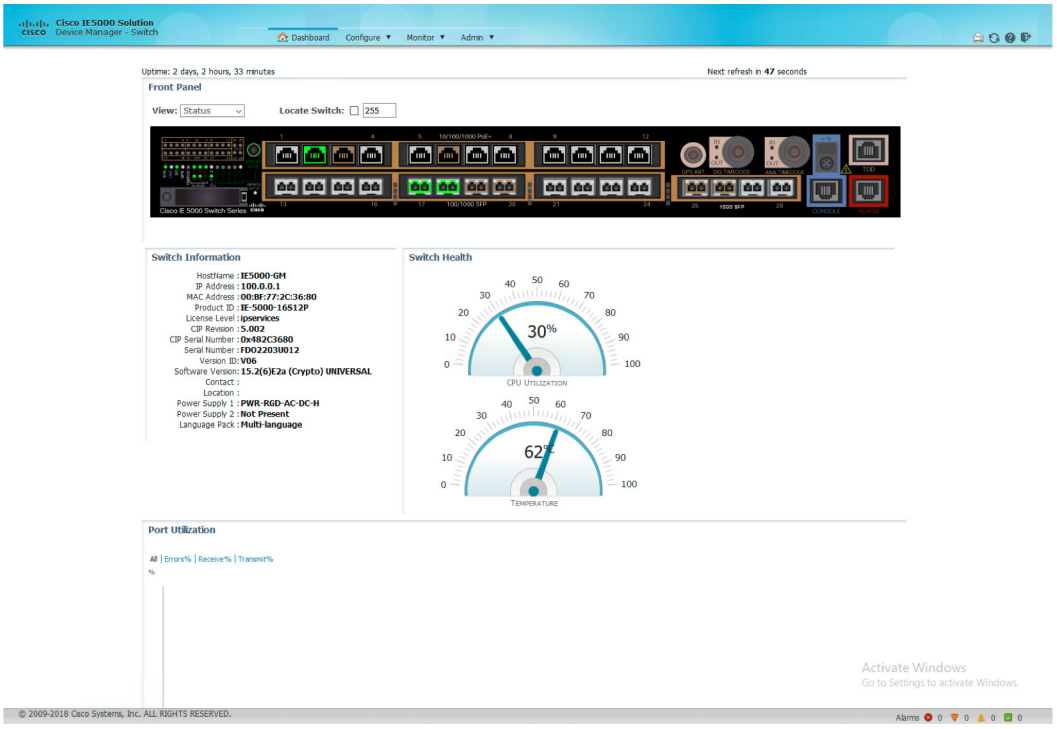
1. Device Manager のクレデンシャルを使用してスイッチにログインします。

図 115　Device Manager のログイン画面



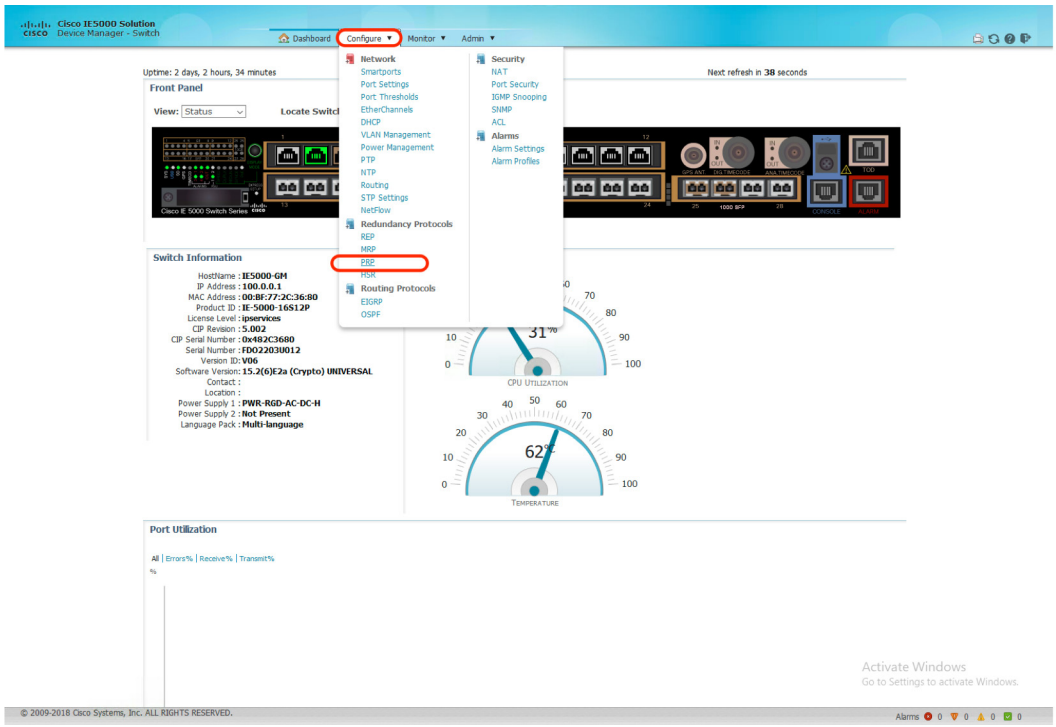
2. ログインに成功すると、スイッチのダッシュボードがロードされます。

図 116 Device Manager のダッシュボード



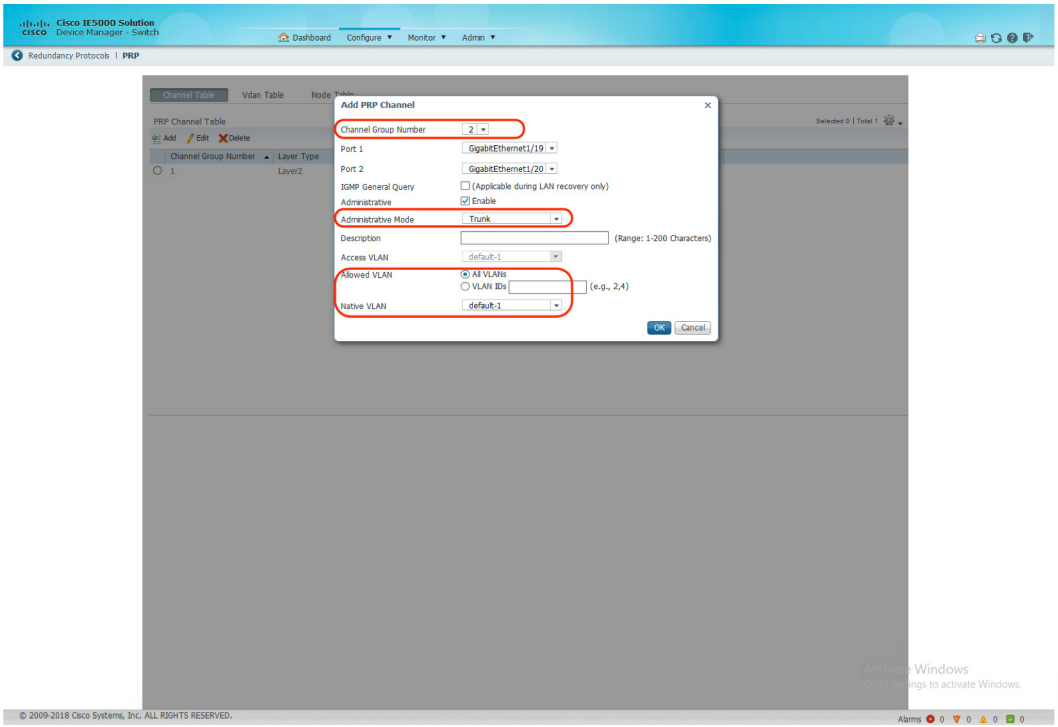
3. **[Configure]** タブの **[PRP]** オプションを選択して、PRP を設定します（図 117 を参照）。

図 117 Device Manager を使用した PRP の設定



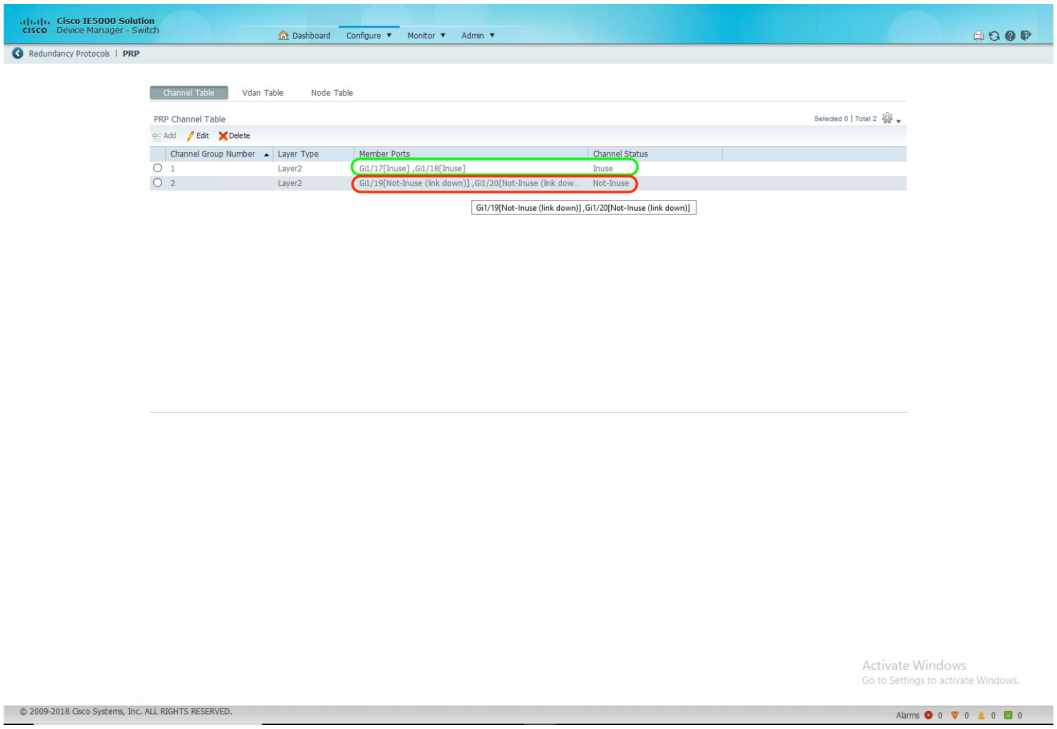
4. PRP チャネル プロパティ（チャネル番号、スイッチポート モード、許可された VLAN、ネイティブ VLAN など）を設定します（図 118 を参照）。

図 118 PRP チャネル プロパティの設定



5. PRP チャネルのステータスは、PRP チャネルの設定が完了するとすぐに反映されます（図 119 を参照）。

図 119 PRP チャネルステータス



6. [Monitor] タブに示されている [PRP] オプションを選択して、VDAN およびノード テーブルの詳細を確認します。

図 120 PRP のモニタ

PRP を介した PTP

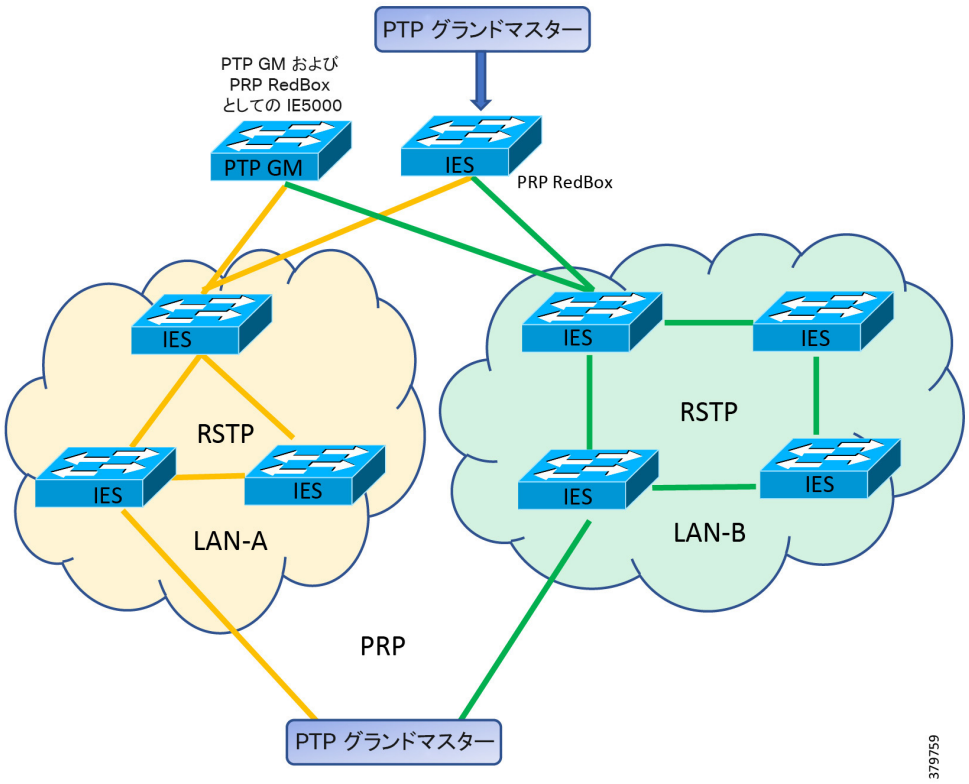
PTP は、IEEE 1588 で、ネットワーク化された測定/制御システムの精密クロック同期として定義されており、精度と安定性が異なる分散デバイス クロックを含むパケットベースのネットワークでクロックを同期させるために開発されました。PTP は、産業用ネットワーク測定/制御システム用に特別に設計されており、最小限の帯域幅しか必要とせず、処理オーバーヘッドもほとんど発生しないため、分散システムでの使用に最適です。

以前は、PTP トラフィックは PRP の LAN-A でのみ許可されていました。ただし、LAN-A が停止すると、PTP 同期は失われていました。PRP インフラストラクチャによって提供される冗長性の利点を PTP で活用できるようにするため、PRP ネットワーク上の PTP パケットは他のタイプのトラフィックとは異なる方法で処理されます。PRP を介した PTP の現在の実装は、PTP パケットにリカバリ制御タスク（RCT）を付加せず、PTP パケットの PRP 複製/廃棄ロジックをバイパスします。

PRP を介した PTP ネットワークを設定するには、次の手順に従います。

注：HSR リングを介した PTP 機能は、現在サポートされていません。

図 121 PRP を介した PTP



はじめる前に

グランドマスター(GM)は、PRP を介した PTP トポロジに次のいずれかのように配置できます。

- LAN-A と LAN-B の両方に接続される RedBox(RedBox としての PTP グランドマスター)。
- PRP RedBox に接続される VDAN(PRP RedBox に接続される PTP グランドマスター)。
- DAN(PRP の両方の LAN に直接接続される PTP グランドマスタークロック)。

LAN-A または LAN-B 内のデバイスだけがグランドマスターと同期されるため、PTP グランドマスターは LAN-A または LAN-B のどちらにも接続できません。

グランドマスター クロックに接続されたスイッチ ポートが次のように設定されている場合、スイッチはネイティブ VLAN 上でタグなし PTP パケットを送信します。

- スイッチがデフォルト プロファイル モードになっている。
- スイッチがトランク モードになっている。
- VLAN X がネイティブ VLAN として設定されている。

グランドマスター クロックにタグ付きパケットが必要な場合は、次のいずれかの設定変更を行います。

- グローバル コマンドの **vlan dot1q tag native** を入力することにより、スイッチがタグ付きフレームを送信することを強制します。

```
vlan dot1q tag native
```

- タグなしパケットを送受信するようにグランドマスター クロックを設定します。グランドマスター クロックでこの設定変更を行う場合は、スイッチ ポートをアクセス ポートとして設定できます。
- インターフェイス レベル コマンドの **ptp vlan <>** を入力することにより、スイッチが PTP パケットにタグ付けすることを強制します。この設定変更により、スイッチは、インターフェイスを通過するすべての PTP パケットを対応する VLAN にタグ付けします。

```
interface gigabitEthernet1/1
    ptp vlan <vlanID>
```

ネットワークで PTP パケットのサービスクラス（COS）値を設定する必要がある場合は、次のいずれかの設定変更を行います。

- デフォルトでは、スイッチは、PTP 電力プロファイルモードの IEEE C37.238 標準に従って、すべてのタグ付き PTP パケットに COS 値 4 を設定します。
- グローバル コマンドの **ptp packet** を入力することにより、スイッチが PTP パケットの COS 値を設定することを強制します。

```
ptp packet <cos>
```

推奨される方法

- PTP が不要なインターフェイスで PTP を無効にします。
- PTP トランスペアレントクロックのピアツーピア トランスペアレント モードを設定して、ジッターと遅延の累積を減らします。

```
ptp mode p2ptransparent
```

- 次のコマンドを使用して、Organization_extension および Alternate_timescale TLV なしでアナウンスメッセージを送信する、PTP 非準拠の PTP グランドマスターを処理するようにスイッチを設定します。

```
ptp allow-without-tlv
```

- 相互運用性のシナリオには、C37.238:2011 標準に準拠したデフォルト PTP ドメイン値の 0（ゼロ）の使用が最適です。Cisco IE スイッチのデフォルト PTP ドメイン値は 0（ゼロ）に設定されています。これは、次のコマンドを使用して設定することもできます。

```
ptp domain 0
```

PRP RedBox の設定

PRP は、イーサネットネットワークで障害発生後のリカバリ時間をゼロにするように設計されています。PRP は、ネットワークノードにその宛先に到達するための 2 つのトラフィック用代替パスを提供します。これにより、データ伝送における障害を防止できます。2 つの LAN が、独立した LAN セグメントを通過するトラフィック用の代替パスを提供します。PRP モード用に設定されたスイッチには、2 つの Lan のそれぞれに接続する 1 つのギガビットイーサネットポートがあります。スイッチは、2 つの異なるポートから宛先ノードに向けて、各 LAN に 2 つのパケットを同時に送信します。宛先ノードは重複したパケットを破棄します。

サポートされている Cisco IE スイッチで PRP チャネルおよびグループを作成して有効にするには、次の手順に従います。

1. グローバル コンフィギュレーション モードを開始します。

```
configure terminal
```

2. PRP LAN インターフェイスを作成します。

```
interface PRP-channel1
    switchport mode trunk
```

3. PRP チャネルを物理インターフェイスに接続します。スイッチの役割と対応するインターフェイスを識別するガイドラインに従ってください。

```
interface range gigabitEthernet 1/1
    prp-channel-group 1
    no shutdown
```

表 57　PRP Redbox インターフェイスマッピング

SKU	インターフェイス マッピング
IE4000	PRP チャネルグループ 1 は常に LAN_A には Gi1/1 を使用し、LAN_B には Gi1/2 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/3 を使用し、LAN_B には Gi1/4 を使用します。
IE4010	PRP チャネルグループ 1 は常に LAN_A には Gi1/25 を使用し、LAN_B には Gi1/26 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/27 を使用し、LAN_B には Gi1/28 を使用します。
IE5000	PRP チャネルグループ 1 は常に LAN_A には Gi1/17 を使用し、LAN_B には Gi1/18 を使用します。 PRP チャネルグループ 2 は常に LAN_A には Gi1/19 を使用し、LAN_B には Gi1/20 を使用します。

PRP を介した PTP の設定

1. グローバル コンフィギュレーション モードを開始します。

```
configure terminal
```

2. 電力プロファイルを設定します。

```
ptp profile power
```

3. 同期クロック モードを指定します。

```
ptp mode {boundary pdelay-req|p2ptransparent|forward}
```

   - mode boundary pdelay-req：遅延要求メカニズムを使用して、スイッチを境界クロック モードに設定します。このモードでは、スイッチが、最も正確なマスター クロックの選択に参加します。このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。
   - mode p2ptransparent：スイッチをピアツーピア トランスペアレント クロック モードに設定し、すべてのスイッチ ポートをマスター クロックと同期させます。参加している PTP ポート間のリンク遅延時間とメッセージ中継時間が常駐時間に追加されます。ジッタとエラーの累積を減らすには、このモードを使用します。これが電力プロファイル モードのデフォルトです。
   - mode forward：着信 PTP パケットを通常のマルチキャストトラフィックとして渡すようにスイッチを設定します。

4. TLV 設定を指定します。

```
ptp allow-without-tlv
```

5. スイッチが PTP 境界クロックとして設定されている場合は、同期アルゴリズムを指定します。

```
Switch(config)#ptp transfer {feedforward|filter{linear}}
```

   - feedforward：非常に速くて正確です。PDV フィルタリングはありません。
   - filter linear：単純な線形フィルタを提供します（デフォルト）。

PRP を介した PTP のトラブルシューティング

PTP クロックタイプ、グランドマスタープロパティ、およびクロックソースを確認するには、次のコマンドを使用します。

境界クロックの例:

```
show ptp clock (In case of Boundary clock)
 PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: Power Profile
  Clock Identity: 0x0:BF:77:FF:FE:2C:47:0
  Clock Domain: 10
  Number of PTP ports: 28
  PTP Packet priority: 4
  Time Transfer: Feedforward
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): N/A
  Offset From Master(ns): 12
  Mean Path Delay(ns): 20
  Steps Removed: 1
  Local clock time: 14:02:47 IST Dec 13 2018
```

ピアツーピアの透過クロックの例:

```
show ptp clock (In case of Peer to Peer Transparent clock)
 PTP CLOCK INFO
  PTP Device Type: Peer to Peer transparent clock
  PTP Device Profile: Power Profile
  Clock Identity: 0x0:BF:77:FF:FE:27:D3:80
  Clock Domain: 10
  Number of PTP ports: 28
  PTP Packet priority: 4
  Delay Mechanism: Peer to Peer
  Local clock time: 08:40:51 UTC Dec 13 2018

show ptp parent
//shows the parent to which the PTP is synchronized with//
 PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Parent Port Number: 17
  Observed Parent Offset (log variance): N/A
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Grandmaster Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
        Priority1: 128
        Priority2: 128

show clock detail
08:41:04.904 UTC Thu Dec 13 2018
Time source is PTP

show prp statistics ptpPacketStatistics
 PRP channel-group 1 PTP STATS:
   ingress lan a: 45
   ingress drop lan a: 0
```

```
    ingress lan b: 48
    ingress drop_lan b: 0
    egress lan a: 90
    egress lan b: 93
 PRP channel-group 2 PTP STATS:
    ingress lan a: 0
    ingress drop lan a: 0
    ingress lan b: 0
    ingress drop_lan b: 0
    egress lan a: 0
    egress lan b: 0
```

PRP RedBox としても PTP グランドマスターとしても動作している Cisco IE 5000 スイッチでは、次のコマンドを使用して、PRP メンバーポートの PTP 状態を確認できます。両方の PRP メンバポートには、マスターのポートステートが必要です。

```
show ptp port gigabitEthernet 1/17
 PTP PORT DATASET: GigabitEthernet1/17
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:36:80
  Port identity: port number: 17
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 23
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000
```

PRP RedBox および PTP 境界クロックとして動作している Cisco IE 5000 スイッチでは、次のコマンドを使用して、PRP メンバーポートの PTP 状態を確認できます。アクティブポートの状態は SLAVE、その他の状態は PASSIVE_SLAVE になります。アクティブポートに障害が発生した場合、他のポートは状態が SLAVE に変更されます。

```
show ptp port gigabitEthernet 1/17
 PTP PORT DATASET: GigabitEthernet1/17
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:47:0
  Port identity: port number: 17
  PTP version: 2
  Port state: SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 20
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000

show ptp port gigabitEthernet 1/18
 PTP PORT DATASET: GigabitEthernet1/18
  Port identity: clock identity: 0x0:BF:77:FF:FE:2C:47:0
  Port identity: port number: 18
  PTP version: 2
  Port state: PASSIVE_SLAVE
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 38
  Announce interval(log mean): 0
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000
```

PTP グランドマスターとしての Cisco IE 5000

Cisco IE スイッチは、PTP または IRIG マシン B を使用した正確な時刻配布に対応していますが、以前は外部ソースに依存して正確な時刻を提供しています。Cisco IE 5000 スイッチにはグローバルナビゲーション衛星システム（GNSS）レシーバが内蔵されているため、スイッチは自分の位置を特定し、衛星コンステレーションから正確な時刻を取得できます。スイッチは、ネットワーク内の時間配布のための PTP グランドマスタークロックになることができます。

はじめる前に

GNSS は、バージョン ID（VID）v05 以上の SKU を持ち GNSS ファームウェアバージョン 1.04 以上を備えた Cisco IE 5000 スイッチでのみサポートされます。**show version** の出力を使用して確認してください。

```
show version | i Version ID
Version ID                      : V06


show version | i GNSS
GNSS firmware version           : 1.04
```

GNSS 機能はすべての機能セット（lanbase、ipservices）で利用でき、個別のライセンスは不要です。

GNSS は、PTP のデフォルトおよび電力プロファイルの時刻源としてのみ使用できます。

GNSS は、GMC-BC モードでのみ PTP の時刻源として使用できます。

PTP グランドマスターの設定

1. グローバル コンフィギュレーション モードを開始します。

   ```
   configure terminal
   ```

2. GNSS を有効にします。

   ```
   gnss
   ```

3. スイッチをグランドマスター境界クロック モードに設定します。

   ```
   ptp mode gmc-bc
   ```

PTP グランドマスターのトラブルシューティング

```
Switch#show gnss status
 GNSS status: Enable
 Constellation: GPS
 Receiver Status: OD
 Survey progress: 100
 Satellite count: 11
 PDOP: 1.00    TDOP: 1.00
 HDOP: 0.00    VDOP: 0.00
 Alarm: None


Switch#show clock detail
14:09:13.378 IST Thu Dec 13 2018
Time source is GNSS

Switch#show gnss satellite all
SV Type Codes: 0 - GPS, 1 - GLONASS, 2 - Beidou

All Satellites Info:
SV PRN No    Channel No       Acq Flg    Ephemeris Flg     SV Type     Sig Strength
-------------------------------------------------------------------------------
       10            0             1                1           0               44
```

```
       32            1             1               1           0              42
       21            2             1               1           0              40
       20            3             1               1           0              44
       11            4             1               1           0              40
       18            6             1               1           0              44
       26            7             1               1           0              40
       25            8             1               1           0              39
       27            9             1               1           0              24
       31           10             1               1           0              49
       14           11             1               1           0              43

Switch#show gnss time
Current GNSS Time:
Time: 2018/12/13  07:07:18 UTC Offset: 18

Switch#show gnss location
Current GNSS Location:
  LOC: 12:56.184485149 N  77:41.767297649 E  828.854749999 m

Switch#show platform gnss
Board ID: 0x5000000 (Production SKU)
GNSS Chip:
  Hardware code: 3023 - RES SMT 360
  Serial Number: 1170159173
  Build Date: 3/15/2017

Switch#show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Power Profile
  Clock Identity: 0x0:BF:77:FF:FE:2C:36:80
  Clock Domain: 10
  Number of PTP ports: 28
  PTP Packet priority: 4
  Time Transfer: Feedforward
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 6
        Accuracy: Within 250ns
        Offset (log variance): N/A
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 0
  Local clock time: 12:37:40 IST Dec 13 2018

Switch#show ptp time-property
 PTP CLOCK TIME PROPERTY
  Current UTC offset valid: TRUE
  Current UTC offset: 37
  Leap 59: FALSE
  Leap 61: FALSE
  Time Traceable: TRUE
  Frequency Traceable: TRUE
  PTP Timescale: TRUE
  Time Source: GNSS
```

Quality of Service

ここでは、産業用オートメーション環境で Quality of Service（QoS）がどのように機能するのかを説明し、シスコの産業スイッチを産業用オートメーション ネットワークに導入するときの主な QoS 設計上の考慮事項を示します。

QoS は、産業用オートメーション ネットワーク内での実現テクノロジーです。Cisco IE スイッチは、組み込みの Express Setup およびスマートポート方式を採用しているため、追加の手順を実行することなく簡単に導入できます。ただし、QoS ソリューションとそのパフォーマンス上の影響を検討してし理解することは、産業用オートメーション ソリューション開発チームにとって非常に重要な作業です。

QoS とは、さまざまな産業用自動化デバイスやトラフィックフローに対してさまざまな優先順位を提供したり、アプリケーションプログラムからの要求に従ってトラフィックフローの特定のレベルのパフォーマンスを保証したりするネットワーク制御メカニズムを指します。専用の帯域幅、制御されたジッタと遅延（一部のリアルタイムのインタラクティブ トラフィックに必要）、および改善された損失特性を提供することによって、QoS は、選択されたネットワークトラフィックに対してより優れたサービスを確保できます。

トラフィック フロー

産業オートメーションネットワークのトラフィックフローには、IT ネットワーク内のクライアントサーバベースのアプリケーションと比較して、非常に異なるトラフィックパターンがあります。次に例を示します。

- 周期的な I/O データが、デバイスからコントローラおよびヒューマン マシン インターフェイス（HMI）またはワークステーションへ非常に短い間隔（数ミリ秒）で通信され、それらはすべて同じネットワーク セグメント上にあり、主にローカル セル/エリアゾーンに留まります。
- 産業用デバイスは、独自の DiffServ コードポイント（DSCP）マーキングを利用して、それ自身を IT 管理トラフィックフローによって識別します。たとえば、DSCP 59 でマーキングされた PTP イベント、DSCP 47 でマーキングされた PTP 管理、DSCP 55 でマーキングされた ODVA, Inc. Common Industrial Protocol（CIP）クラスなどです。
- 産業用オートメーション ネットワークトラフィックのタイプ（動作、I/O、および HMI）によって、遅延、パケット損失、およびジッターに関する要件が異なります。サービスポリシーは、これらのタイプのトラフィックフローに対してサービスを区別する必要があります。
- OT トラフィックは、通常、非常に小さなパケットサイズのパルスベースです。
- IT トラフィックと OT トラフィックは、しばしば産業用オートメーション ネットワーク内で共存します。OT トラフィックは、他の IT 管理ネットワークトラフィック フローよりも優先されます。

図 122、表 58、および表 59 に、一般的な産業用オートメーション ネットワークのトラフィックフロー、トラフィックタイプ、および差別化されたサービスマーキングを示します。

図 122 産業用オートメーション工場製造ゾーンのトラフィック フロー

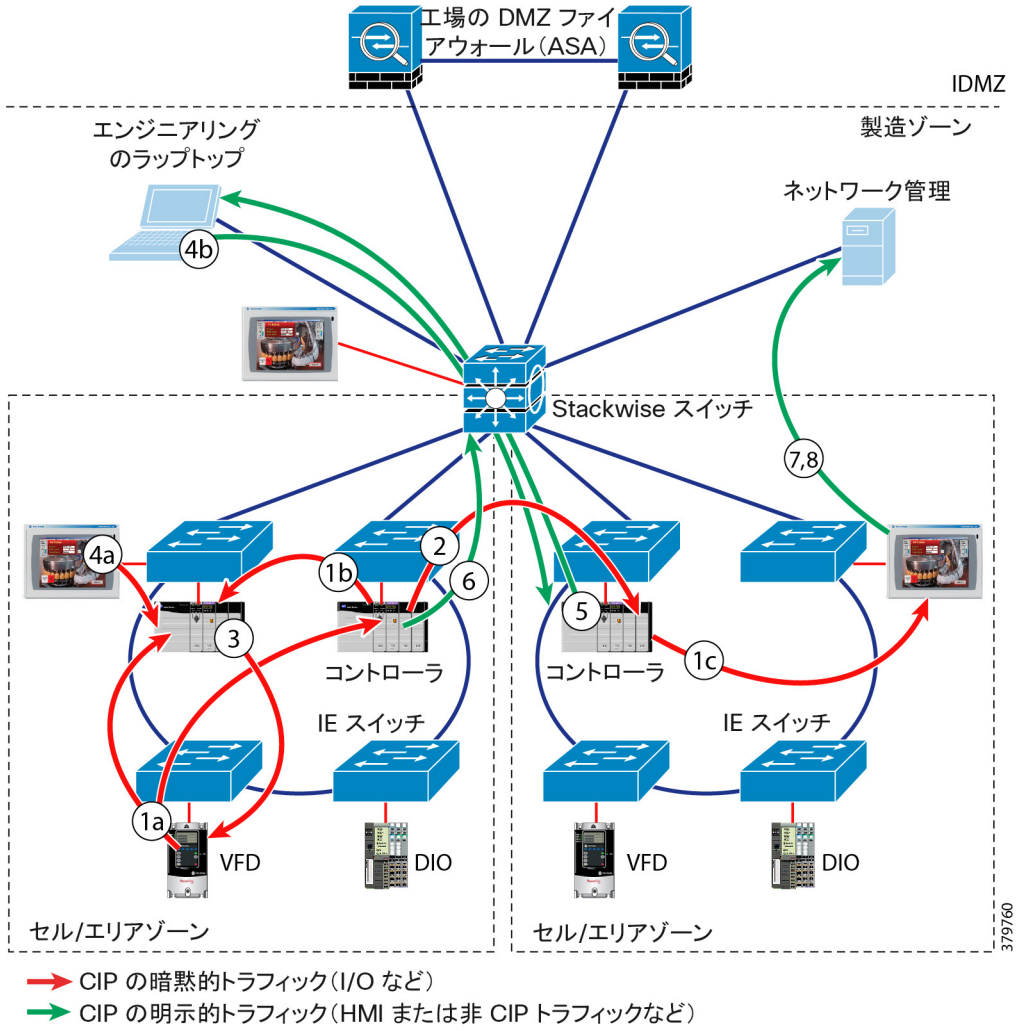


表 58 産業用オートメーション工場製造ゾーンのトラフィックタイプ

図の参照番号	遷移元	目的	説明	プロトコル	タイプ	ポート
1 a、b、c	プロデューサ（VFD ドライブなど）	コンシューマ（コントローラなど）	プロデューサ（VFD ドライブ、コントローラなど）は、CIP の暗黙的 I/O（UDP マルチキャスト）トラフィックを介して複数のコンシューマにデータを送信します。 a：デバイスからコントローラへの I/O を表します。 b：コントローラ間の I/O を表します。 c：コントローラによる HMI へのリアルタイム ステータスのレポートを表します。	イーサネット/IP	UDP	2222
2	プロデューサ	コンシューマ	プロデューサは、CIP I/O（UDP ユニキャスト）トラフィックを介してデータをコンシューマに送信できます。	イーサネット/IP	UDP	2222

表 58　産業用オートメーション工場製造ゾーンのトラフィックタイプ

図の参照番号	遷移元	目的	説明	プロトコル	タイプ	ポート
3	コンシューマ	プロデューサ	コンシューマ（コントローラ、HMI など）は、CIP I/O（UDP ユニキャスト）トラフィックを介して出力データまたはハートビートでプロデューサに応答します。	イーサネット/IP	UDP	2222
4a、b	デバイス	デバイス	CIP の診断、設定、情報、アップロード/ダウンロード、および識別データ。たとえば、HMI がコントローラとの CIP 接続を開く場合、CIP 接続要求が TCP を介して送信されます。図には示されていませんが、コントローラは TCP メッセージで応答します。 a：HMI はアプリケーション モニタリングのために CIP 接続を開きます。 b：エンジニアリング ワークステーションはプログラムをダウンロードします。	イーサネット/IP	TCP/UDP	44818
5	デバイス	ワークステーション/ラップトップ	ほとんどのイーサネット/IP デバイスは、Web ブラウザ（HTTP）を介して診断およびモニタ情報を提供できます。	HTTP	TCP	80
6	デバイス	DHCP/BootP サーバ	起動時の IP アドレス割り当て用のクライアント（IACS ネットワーク デバイスには推奨されない）。	DHCP/ BootP	UDP	67-88
7	コントローラ	メールサーバ	製造ゾーン内での警告または情報ステータスを知らせるためのメールメッセージ	SMTP	TCP	25
8	デバイス	ネットワーク マネージャ	すべてのネットワーク インフラストラクチャ（スイッチ、ルータなど）と多くのイーサネットデバイスが、SNMP メッセージを送信できます。	SNMP	UDP	161

表 59　産業用オートメーション工場製造ゾーンのトラフィックフロー マーキング

トラフィック タイプ	CIP のプライオリティ	デフォルトで有効になっている DSCP	デフォルトで無効になっている 802.1D プライオリティ	CIP トラフィックの使用状況
PTP イベント（IEEE 1588）	該当なし	59 (111011)	7	PTP イベントメッセージ（CIP Sync で使用）
PTP 管理（IEEE 1588）	該当なし	47 （101111）	5	PTP 管理メッセージ（CIP Sync で使用）
CIP クラス 0/1	緊急 （3）	55 （110111）	6	CIP Motion

表 59　産業用オートメーション工場製造ゾーンのトラフィックフロー マーキング

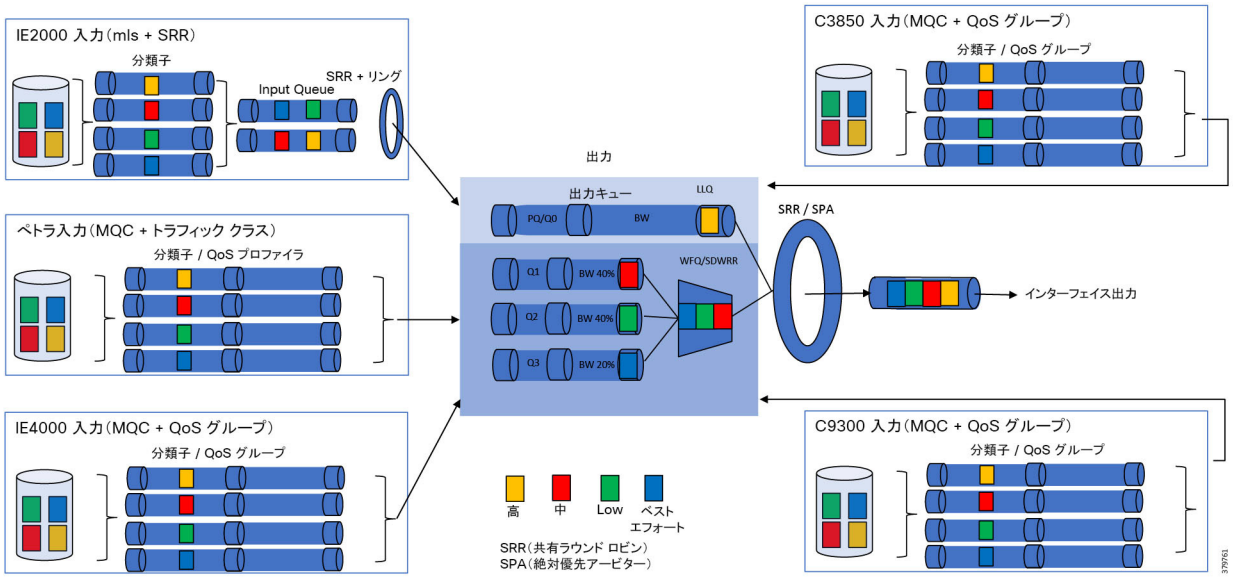
トラフィック タイプ	CIP のプライオリティ	デフォルトで有効になっている DSCP	デフォルトで無効になっている 802.1D プライオリティ	CIP トラフィックの使用状況
	スケジュール済み（2）	47 （101111）	5	セーフティ I/O、I/O
	高（1）	43 （101011）	5	I/O
	低（0）	31 （011111）	3	現時点では非推奨
CIP UCMM CIP クラス 3	すべて（All）	27 （011011）	3	CIP メッセージ

ネットワークデバイスと QoS モデル

産業用オートメーション工場では、ネットワークデバイスと機能を異なる機能ゾーンにセグメント化して管理を容易にするために、制御階層に関して一般的でよく理解されている Purdue モデル（ISBN 1-55617-265-6 を参照）が採用されます。各セグメントには、異なるネットワークアーキテクチャおよび機能セットを持つさまざまな種類のスイッチとルータが導入されます。すべてのトラフィックフローとさまざまなネットワークサービスを合理化し、パケット損失、ジッター、および遅延を削減するには、ネットワークのパフォーマンスと動作を保証する、適切に設計された QoS モデルが非常に重要です。

図 123 複数の Cisco IE スイッチ（Cisco IE 2000、Cisco IE 3x00、Cisco IE 4000、Cisco Catalyst 3850、および Cisco Catalyst 9300 など）が接続されている産業オートメーション工場内のセル/エリアゾーン領域用に設計された一般的な QoS モデルを示し、ネットワークトラフィック フローを分類およびポリシングするための入力および出力パイプラインを形成しています。

図 123　産業オートメーション工場製造ゾーンの QoS モデル



Cisco IE 2000 産業用イーサネットスイッチ

Cisco IE 2000 は、主に、産業用プログラム ロジック コントローラ（PLC）をブリッジするアクセススイッチの役割を担います。Cisco IE 2000 は、マルチレイヤスイッチング QoS（MLS）をグローバルに使用し、ネットワーク全体の信頼境界を確立します。これは、プロトコル、ポート、および QoS マーキングに基づいてネットワークトラフィック フローを正しく分類することによって実現されます。入力側には、プライオリティキューと共有ラウンドロビン（SRR）共有キューからなる 2 つのキューがあります。送信リングを通じて、ネットワークトラフィックは、重み付け帯域幅割り当てのために 1 つのプライオリティキューと 3 つの共有 SRR キューでポリシングされた出力側に入ります。さらに、トラフィックは送信リングに入って出力インターフェイスから出ます。

Cisco IE 3x00 シリーズの産業用イーサネットスイッチ

Cisco ie 3x00 スイッチは、Cisco IE 3000 を引き継ぐ次世代型スイッチです。このスイッチは、モジュラ QoS クラス（MQC）モデルを ASIC 事前プログラム トラフィック プロファイルとともに利用して、ネットワークトラフィックを分類し、信頼境界を確立します。簡素化されたハードウェアアーキテクチャにより、ASIC で QoS データ プレーンが完全に実現されます。入力側のパケット分類、マーキング、およびポリシングは、ASIC コードポイントベース テーブルまたは TCAM ルールを使用して実行されます。パケットエンキューおよびスケジューリング プロファイルは、QoS プロファイルに基づいて決定されます。出力側のパケットのキューイング、スケジューリング、およびシェーピングが実行されます。さまざまな QoS パケットがパケット 128 QoS プロファイルにマッピングされます。シェイプド不足荷重ラウンド ロビン（SDWRR）は、加重ラウンド ロビン（WRR）よりも動的なエンキューおよびデキュー処理を提供します。絶対優先アービター（SPA）は、出力ポートでのミッションクリティカルなパケット処理を迅速化します。

Cisco IE 4000 Industrial Ethernet スイッチ

より優れたポート密度と処理能力を備え、複数の産業用プロトコルをサポートする Cisco IE 4000 は、アクセスレイヤスイッチまたはディストリビューション スイッチの役割を担います。MQC と QoS グループを利用してトラフィックを分類し、それらを正しいキューにポリシングします。プライオリティキュー（PQ）を持つクラスベース均等化キュー（WFQ）が、出力側でトラフィックをポリシングするために選択されます。Cisco IE 4000 は SRR 送信リングを持ちません。

Cisco Catalyst 3850 ネットワークスイッチ

Cisco Catalyst 3850 StackWise スイッチは、レイヤ 2 デバイスリング/チェーンとレイヤ 3 ネットワーク インフラストラクチャを相互接続するためのセル/エリアゾーン ゲートウェイ デバイスです。Cisco Catalyst 3850 スイッチは、入力トラフィックの分類とポリシングのために MQC と QoS グループを利用します。ネットワークトラフィックは StackWise リングに入り、出力側の 1 つのプライオリティ キューと 3 つの重み付け均等化キュー（WFQ）に入ります。出力ポート SRR シェーパーは、異なるトラフィック クラス間で重み付けされた帯域幅割り当てを提供します。

Cisco Catalyst 9300 ネットワークスイッチ

Cisco Catalyst 9300 StackWise スイッチは、クラウド対応のソフトウェア定義型アクセス（SD アクセス）を提供します。このスイッチは、モビリティ、IoT、クラウド、およびセキュリティを 1 つのポートフォリオに統合できる、エッジからクラウドまでのポリシーベースのオートメーションを利用します。Csco Catalyst 9300 は、Cisco Catalyst 3850 StackWise スイッチのような QoS モデルを利用します。UADP 2.0 ASIC には、テンプレートベースの設定可能な QoS エントリが組み込まれており、きめ細かいワイヤレス帯域幅管理、均等化シェアリング、802.1 p サービスクラス（CoS）、Differentiated Services Code Point（DSCP）フィールドの分類、シェイプドラウンドロビン（SRR）のスケジューリング、認定情報レート（CIR）、およびポートあたり 8 つの出力キューイングを含む優れた QoS を実現します。

トラフィック分類

QoS ポリシーの最初の要素は、異なる方法で処理されるトラフィックを分類/識別することです。分類およびマーキングツールは、次のいずれかを調べることによって、この信頼境界を設定します。

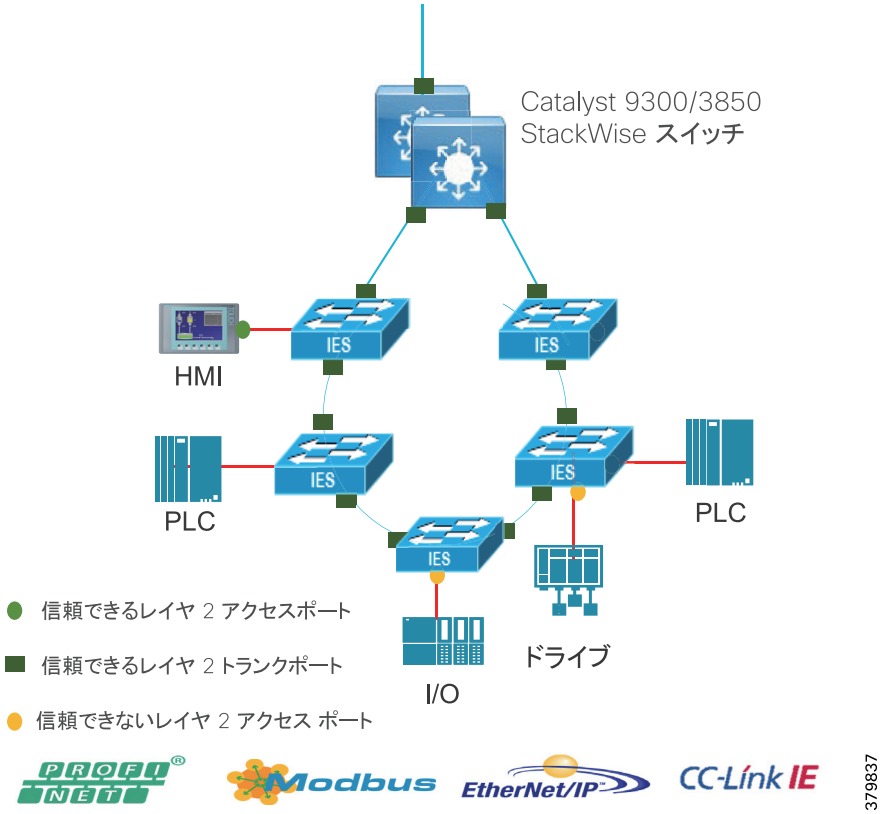
- レイヤ 2 パラメータ：802.1Q サービス クラス（CoS）ビット
- レイヤ 3 パラメータ：IP プレシデンス（IPP）、DiffServ コード ポイント（DSCP）、IP 明示的輻輳通知（ECN）、および送信元/宛先 IP アドレス

- レイヤ 4 パラメータ: レイヤ 4 プロトコル(TCP または UDP)および送信元ポートと宛先ポート
- レイヤ 7 パラメータ:アプリケーション署名

Cisco IE スイッチに実装されている QoS モデルでは、差別化サービス(DiffServ)モデルに焦点が合わされています。DiffServ の主な目標の一つは、トラフィックをできるだけ送信元に近い場所で分類してマーキングすることです。これにより、中間ルータおよびスイッチが所定のマーキングに基づいて単純にフレームを転送するエンドツーエンドモデルが実現されます。ユーザによる自分自身のトラフィックへのマーキングが許可されている場合、ユーザはプロビジョニングされる QoS ポリシーを簡単に悪用できるため、ユーザが自分の PC またはその他の同様のデバイスに設定できるマーキングを信頼しないでください。

分類後、マーキングツールはフレームまたはパケットの属性を特定の値に設定できます。そのようなマーキング(または再マーキング)により、スケジューリングツールが後で依存する信頼境界が確立されます。

図 124 産業用オートメーション工場の製造 QoS 信頼境界



次の手順は、入力 QoS の実装を示しています。

1. 産業用オートメーションネットワークのトラフィックタイプごとに ACL を確立します。これにより、産業用イーサネットスイッチは、トランスポートプロトコル(UDP または TCP)、ポートタイプ(CIP の明示的メッセージや暗黙的 I/O)、または既存の DSCP 値などの主要な特性に基づいてネットワークトラフィックをフィルタリングできます。
2. ACL フィルタリングされたトラフィックを分類と照合するようにクラスマップをセットアップします。
3. 分類をクラスマップに割り当てるポリシーマップをセットアップします。
4. 産業用オートメーション ネットワークトラフィックを転送する各ポートにサービスポリシーを割り当てます。

ポリシング、キューイング、およびスケジューリング

ネットワーク デバイスの出力ポートは、ポリシング、キューイング、およびスケジューリングツールを使用して、ミッション クリティカルなトラフィックをプライオリティキューに入れ、すべてのトラフィッククラスに適切な量の帯域幅を割り当てることによって、トラフィックフローのプライオリティを管理できます。以下のセクションでは、出力 QoS モデルの各構成要素について説明します。

ポリシング

ポリシングは、任意のトラフィッククラスの帯域幅を制限するメカニズムであり、あらゆるポートで使用できます。

ポリシングは、次の 3 つのアクションを発生させる可能性があります。

- 帯域幅を超えない場合はアクションが発生しません。
- 帯域幅を超えた場合、パケットがドロップされる可能性があります。
- 帯域幅を超えた場合、パケットが下方にマーキングされる（多くの場合、プライオリティを下げる分類変更が行われる）可能性があります。

キューイング

キューイングでは、パケットがスイッチに着信したとき（入力）とスイッチから発信されるとき（出力）にパケットを処理するためのバッファが確立されます。スイッチの各ポートが入力キューと出力キューを持ちます。入力キューと出力キューは両方とも、重み付けテール ドロップ（WTD）呼ばれるテールドロップ輻輳回避メカニズムの拡張バージョンを使用します。WTD はキュー長を管理したり、トラフィック分類ごとにドロップ優先順位を設定したりするために実装されています。各キューには、キューがいっぱいになる前にパケットを予防的にドロップするための 3 つのしきい値があります。キュー バッファが割り当てられたしきい値に達すると、しきい値 1 またはしきい値 2 に割り当てられたトラフィッククラスはドロップされます。特定のキューに関してしきい値 3 に割り当てられたトラフィッククラスは、そのキューのバッファスペースがいっぱいになった場合にのみドロップされます。

表 60　産業用オートメーション工場製造ゾーンのトラフィック タイプとキュー割り当て

	PTP イベント	CIP 緊急	PTP 管理、CIP スケジュール済み、CIP 高	ネットワーク制御	音声データ	CIP 低、CIP クラス 3	音声制御	ベスト エフォート			
DSCP	59	55	47、43、	48	46	31、27	24	残り			
CoS	7	6	5	6	5	3	3	4	2	1	0
トラフィックタイプ	PTP イベント	CIP Motion	PTP 管理、セーフティ I/O、I/O	STP など	SIP など	CIP の明示的メッセージ	SIP	残りすべて			
CoS から入力 キュー へのマッピング	キュー 2							キュー 1			
入力 キュー しきい値	3							2	3	2	3
CoS から出力 キュー へのマッピング	キュー 1	キュー 3				キュー 4		キュー 2			
出力 キュー しきい値	3	3				3		3	3	2	3

表 61　産業用オートメーション工場製造ゾーンの入力キュー割り当て

入力 キュー	キュー(Queue) #	CoS からキューへのマッピング	トラフィックタイプ	キューの重み	キュー(バッファ)サイズ
SRR 共有	1	0、1、2	残りすべて	40%	40%
プライオリティ	2	3、4、5、6、7	PTP、CIP、ネットワーク制御、音声、ビデオ	60 %	60 %

表 62　産業用オートメーション工場製造ゾーンの出力キュー割り当て

出力キュー	キュー(Queue) #	CoS からキューへのマッピング	トラフィック タイプ	キューの重み	Gb ポートのキュー サイズ	10/100 ポートのキュー サイズ
プライオリティ(Priority)	1	7	PTP イベント	1	10	10
SRR 共 有	2	0、1、2、4	残りすべて	19	25	25
SRR 共有	3	5、6	PTP 管理、CIP の暗黙的 I/O、ネットワーク制御および音声データ	40	40	40
SRR 共 有	4	3	CIP の明示的メッセージ	40	25	25

スケジューリング

入力キューと出力キューはどちらも、パケットの送信速度を制御する共有ラウンドロビン(SRR)スケジューリングまたは絶対優先アービター(SPA、Cisco IE 3x00 シリーズ スイッチ)のいずれかによって処理されます。

出力側の QoS の一般的な設定手順は、次のとおりです。

1. IACS ネットワークトラフィックを伝送するすべてのスイッチポート(アクセス ポートとトランクポート)で出力プライオリティキュー(キュー 1)を有効にします。これにより、キューに割り当てられた最高プライオリティのトラフィックが確実に、迅速に処理されるようになります。このキューは共有ラウンドロビンとして処理されなくなり、そのポートの SRR 設定は無効になります。

2. IACS ネットワークトラフィックおよび、存在しているならその他のプライオリティトラフィック(たとえば、音声およびネットワーク ルーティング トラフィック)に特定のキューを割り当てます。これらのキューには、その後に、パケット損失を最小限に抑え、スケジューリングを最適化するために、バッファとスケジューリングの重みが割り当てられます。その他のトラフィック用に 1 つの入力キューと出力キューを維持します。入力の場合、キュー 1 が他のトラフィック用です。出力の場合、キュー 2(4 つのうち)がベストエフォート型トラフィック用です。

3. 各キューおよびしきい値の COS マップおよび DSCP マップを介して、IACS ネットワークトラフィックを特定のキューにマッピングします。パケット損失を避けるために、IACS ネットワークトラフィックを 3 つ目のしきい値に割り当てる必要があります。キューバッファがいっぱいになるとパケット損失が発生しますが、それまでは発生しません。それらが割り当てられるキューは、それらが受け取る帯域幅の最小量を定義し、それらがどれくらい速く処理されるのかを定義します(プライオリティキューは常に最初に処理されます)。

4. すべてのポートの SRR キュー帯域幅共有重みを割り当てて、そのポートの出力キューに重みを割り当てます。これは、輻輳が発生したときのキュー内のトラフィック専用の帯域幅の相対量を表します。キューがその帯域幅を使用していない場合、その帯域幅は他のキューで使用可能になります。

5. バッファ領域をキューに割り当てるためにポートに割り当てられた出力キューバッファセットを定義します。より多くのキュースペースを IACS ネットワークトラフィック キューに割り当てることによって、パケット損失が回避されます。上記の設定により、他のタイプのトラフィックに対する基本サービスを維持しながら、CIP ネットワークトラフィックに特定のプライオリティを割り当てることができます。これらの設定は、QoS に関する ODVA, Inc. の推奨事項に合致しており、自分の CIP トラフィックをマーキングできない IACS デバイスが、確実に、自分の CIP トラフィックをマーキングする IACS デバイスと同じ優先 QoS 処理を受けるようにします。Express Setup を使用して適切な Smartport を選択する以外に、これらの QoS 推奨事項をシスコの産業用イーサネットスイッチに適用するために必要な特別な設定はありません。

設定例については、実装ガイドを参照してください。

以前のドキュメントと関連ドキュメント

この設計および実装ガイドは、シスコが発表した一連の重要な産業用ソリューションを発展させたものです。このドキュメントでは、産業用ソリューションで共有されている多数の概念、テクノロジー、および要件が、多数の方法で統合されています。垂直方向の関連性は維持されますが、共有される技術的側面は、本質的に、このドキュメントで収集され参照されています。

- 製造および石油/ガスに関する既存のドキュメントは、産業用ソリューションの Cisco Design Zone のページにあります。
  https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-industry-solutions/index.html
- Cisco Catalyst 9300 と Cisco Catalyst 3850 は、制御された IT 環境のディストリビューション スイッチとして位置づけられています。
  - Cisco Catalyst 3850 製品のページ:
    https://www.cisco.com/c/en/us/products/switches/catalyst-3850-series-switches/index.html
  - Cisco Catalyst 9000 スイッチ製品のページ:
    https://www.cisco.com/c/en/us/products/switches/catalyst-9000.html
- Cisco Catalyst 3850 StackWise-480 の設定:
  - Cisco Catalyst 3850 の場合:
    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/ha_stack_manager/configuration_guide/b_hastck_3se_3850_cg/b_hastck_3se_3850_cg_chapter_010.html#reference_5415C09868764F0FA05F88897F108139
  - Cisco Catalyst 9300 の場合:
    https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-5/configuration_guide/stck_mgr_ha/b_165_stck_mgr_ha_9300_cg/managing_switch_stacks.html
- 産業用イーサネット スイッチ製品のページ:
  https://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html
- Cisco IE 3x00 シリーズ スイッチ
  https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/16_10/release_note/b_1610_releasenote.html
- Cisco IE 4000、Cisco IE 4010、および Cisco IE 5000:
  - スイッチソフトウェア
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000.html
  - スイッチソフトウェア Smartport の設定
    https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4010/software/release/15-2_4_EC/configuration/guide/scg-ie4010_5000/swmacro.html
- Cisco Industrial Network Director:
  - http://www.cisco.com/go/ind
  - コネクテッド ファクトリ アーキテクチャにおける運用テクノロジーのためのネットワーク管理
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD/IND_Connected_Factory_CRD.html
- IEC 標準規格:
  - IEC 61588 Precision clock synchronization protocol for networked measurement and control systems
    http://s1.nonlinear.ir/epublish/standard/iec/onybyone/61588.pdf

表 63　以前の業界ドキュメント

Industry	ソリューション	説明
製造業	コネクテッドファクトリ：CPwE https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html	業界の自動化および制御システム（IACS）ネットワークを標準のイーサネットおよび IP ネットワーキングテクノロジーに統合またはアップグレードすることを求めている製造業者を支援するためのソリューション。
	コネクテッドファクトリ：PROFINET https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-factory/connected-factory-profinet.html	Cisco Industrial Ethernet スイッチをオートメーション ネットワークに統合するための、PROFINET ベースの産業環境向けのソリューション。
	コネクテッドファクトリ：CC-Link IE https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/MELCO/CC-Link_Connected_Factory.html	Cisco Industrial Ethernet スイッチをオートメーション ネットワークに統合するための、CC-Link IE ベースの産業環境向けのソリューション。
	コネクテッドマシン https://www.cisco.com/c/en/us/solutions/industries/manufacturing/connected-machines.html	迅速かつ反復可能なマシン接続を実現し、総合設備効率（OEE）やマシン モニタリングなどの活用によりビジネスを革新します。
	コネクテッドファクトリ：業務テクノロジーのためのネットワーク管理 https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/IND/IND_Connected_Factory_CRD.html	コネクテッド ファクトリ ソリューションのコンテキスト内で産業ネットワークアセットをモニタし、オートメーション デバイスを検出するための、Cisco Industrial Network Director アプリケーションの使用方法を説明します。
石油/ガス	コネクテッドパイプライン：コントロールセンター https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-control-center.html	セキュアなリモートアクセスと運用サポートを含む、石油/ガスパイプラインオペレータ向けのセキュアな仮想化コントロールセンター設計。
	コネクテッドパイプライン：業務電気通信 https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-pipeline-operational-telecoms.html	石油/ガスパイプライン ワイドエリアネットワークおよびパイプライン ステーション ネットワークに関するベストプラクティスとセキュアな設計のガイダンス。これには、コントロールセンターとパイプラインステーション間、パイプラインステーション間、および内部パイプラインステーション間のネットワークが含まれます。
	コネクテッド精製所および加工施設 https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/connected-refinery-processing-facility.html	次世代の精製および加工のための産業ワイヤレス/モビリティを活用するベストプラクティスとセキュアな設計のガイダンス