検証済みプロファイル：製造（SD-Access）業界

2025 年 2 月 12 日

注記

製造業（非ファブリック）におけるシスコの検証済みプロファイルについては、「Validated Profile: Manufacturing (Non-Fabric) Vertical」で詳細を確認してください。

本書の目的と用途

このガイドでは、Cisco Catalyst Center と Cisco SD-Access を使用する製造業実稼働ネットワーク向けのシスコ検証済みプロファイル（CVP）について説明します。このガイドは、シスコの産業オートメーションおよび Converged Plant-wide Ethernet（CPwE）のシスコ検証済み設計（CVD）の設計および実装ガイダンスに準拠しており、一般的にこれらに従っています。このガイドは、導入エンジニアが導入および設定時にネットワークに関する最適な決定を下すのに役立ちます。

対象読者

このガイドの対象読者は、製造生産ネットワークを導入または管理する IT および運用技術（OT）の専門家です。このガイドは、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用の検証リファレンスとして機能します。

ソリューションの概要

実稼働環境は、過去 15 年間で大幅に進化し、独自のニッチ ネットワーキング テクノロジーから標準のネットワーキング テクノロジーとプラクティスに移行しました。実稼働ネットワークは通常、IT チームと OT チームが混在して導入および管理されます。実稼働環境には、大規模なネットワークを一貫して展開するためのネットワーク自動化の必要性、サイバーセキュリティがほとんどない環境向けのネットワークセキュリティの強化、重要な運用をサポートする可用性の高い復元力のあるネットワーク インフラストラクチャ、IT 以外のオペレータ向けのシンプルなモニタリング、効率的なトラブルシューティングなどの、独自の一連の要件があります。設計と導入に関する考慮事項は、最新の工場、生産施設、および倉庫の開発の基礎となるこれらの重要な領域で役立ちます。

このドキュメントの対象範囲

このガイドでは、製造業での導入で推奨され、使用可能なソリューションに関する詳細な設定ガイダンスは提供していません。このガイドを参照として使用して、一般的な使用例と課題、および Cisco SD-Access がそれらの要件にどのように対処するかを理解してください。

従来のネットワークと Cisco SD-Access の比較

次のセクションでは、従来のネットワークアーキテクチャの課題と、Cisco SD-Access がそれらに対処する方法について説明します。

従来のネットワークの課題

従来のネットワークアーキテクチャを導入している組織は、ユーザー、デバイス、およびデバイスの種類が増え続けるにつれて、ますます多くの課題に直面しています。すべてのユーザーとデバイスのトラフィックを識別、グループ化、および分析することは、デバイスが侵害された場合に企業のインフラストラクチャを保護する必要がある組織にとって、重大な懸念事項です。従来のネットワークでは、複数の異なるデバイス間で多数の VLAN と手動アクセス制御リスト（ACL）が必要になるため、手動での設定ミスによる障害が発生します。ビジネスが時間の経過とともに拡大するにつれて、より多くのデバイスと場所が追加され、複雑さが増し、エラーが発生する可能性が高くなります。新しい、より複雑なセキュリティルールは、企業全体で手動で更新する必要があります。

組織が企業に新しいブランチを追加する場合、ネットワーク運用チームは本社とブランチの場所で ACL を更新する必要があります。更新中にエラーが発生すると、セキュリティポリシーに一貫性がなくなり、セキュリティ違反が発生する可能性があります。ネットワーク管理者は、すべてのデバイスが適切なネットワークセグメントに安全にオンボーディングされるように、ネットワークの変更の計画と設定に多大な時間を費やす必要があります。ネットワークを構築する従来の方法では、進化するネットワークの要件と増え続けるセキュリティの懸念に対応できません。

Cisco SD-Access の重要性

Cisco SD-Access は、可視性、自動化、セキュリティ、簡素化を網羅するインテントベースのネットワーキング基盤上に構築されています。Catalyst Center の自動化とオーケストレーションを使用すると、ネットワーク管理者は直感的な UI インターフェイスを介して企業環境全体に変更を実装できます。管理者は同じコントローラを使用して、企業全体のファブリックアーキテクチャを構築し、セキュリティグループ化のためのエンドポイントを分類し、セキュリティポリシーを作成して配布し、ネットワークのパフォーマンスと可用性を監視できます。

SD-Access は、仮想ルーティングおよび転送（VRF）テーブルとセキュリティグループタグ（SGT）をそれぞれ使用して、マクロセグメンテーション レベルとマイクロセグメンテーション レベルでネットワークを保護します。このアプローチは多層セグメンテーションと呼ばれ、従来のネットワークでは最適ではありません。セキュリティ境界は、有線クライアントとワイヤレスクライアントのネットワーク インフラストラクチャのエッジにプッシュされます。

ユーザーおよびデバイスに関連付けられたセキュリティコンテキストは、ネットワーク接続を認証するときに動的に割り当てられます。Cisco SD-Access は、次の理由により、従来のネットワーク展開よりも優れています。

- オーケストレーションと自動化による複雑さの軽減と運用の一貫性。
- グループベースのポリシーを含む多層セグメンテーション。
- 有線およびワイヤレスクライアントのダイナミック ポリシー モビリティ。

グリーンフィールド Cisco SD-Access ファブリックガイドライン

製造ネットワーク用の Cisco SD-Access ファブリックの新規展開（グリーンフィールド展開）に関するガイドラインと推奨事項については、次のセクションに進んでください。これらのセクションでは、SD-Access ファブリックコンポーネントと、ネットワークの要件と課題に対処するために Cisco SD-Access ソリューションが提供する利点について説明します。

従来のネットワークは、Cisco Prime Infrastructure で管理できます。また、Catalyst Center で管理することもできます。Catalyst Center は、従来のネットワークと SD-Access のテレメトリを自動化、監視、収集します。Cisco Prime Infrastructure によって管理されている既存のネットワークがあり、Catalyst Center へ移行する場合は、『Cisco Prime Infrastructure to Cisco Catalyst Center Migration Guide』を参照してください。

Catalyst Center

Catalyst Center は、人工知能（AI）を活用してネットワーク運用を接続、保護、自動化する強力な管理システムです。Catalyst Center は、Cisco Catalyst ネットワーク インフラストラクチャの管理を簡素化し、有線およびワイヤレスネットワーク全体で一貫したユーザーエクスペリエンスを保証します。これにより、エンタープライズ規模のセキュアでシームレスな信頼性の高い接続がユーザーとアプリケーションとモノの間に提供されます。利点を次に示します。

- AI を活用してネットワーク運用を簡素化および自動化し、運用コストを削減します。
- ビジネスに不可欠なアプリケーションとクライアントの正常性に関する詳細なインサイトにより、ユーザーエクスペリエンスを向上させます。
- シスコとサードパーティのエコシステムを使用したビジネスプロセスの自動化により、デジタルアジリティを加速します。
- 直感的なセキュリティポリシー管理、AI 対応の適用、自動化されたコンプライアンスチェックにより、デジタルエンタープライズを保護します。
- スマートビルディングを実現し、Power over Ethernet（PoE）インフラストラクチャを最適化することで、持続可能性を促進します。

Catalyst Center プラットフォームは、物理アプライアンスと仮想アプライアンスの両方として、さまざまなフォームファクタでサポートされています。

詳細については、『Cisco Catalyst Center Data Sheet』を参照してください。『Cisco Catalyst Center Installation Guide』も参照してください。

Cisco Identity Services Engine

Cisco Identity Services Engine（ISE）は、組織のネットワークにアクセスするユーザーとデバイスに対する管理上の可視性、制御、一貫性を向上させる、セキュアなネットワーク アクセス プラットフォームです。Cisco ISE は、ネットワーク アクセス コントロール ポリシーを実装するための SD-Access の不可欠な部分です。Cisco ISE はポリシー導入を実行し、拡張可能なグループにユーザーとデバイスを動的にマッピングし、エンドツーエンドのセキュリティポリシー適用をシンプルにします。Catalyst Center は、拡張可能なグループタグ（SGT）を管理および作成し、そのポリシーを定義するためのペインとして使用されます。グループおよびポリシーサービスは、Cisco ISE によって駆動され、Catalyst Center のポリシー作成ワークフローによってオーケストレーションされます。Catalyst Center と統合された Cisco ISE を使用して、SD-Access ネットワークでアイデンティティサービスを使用したポリシー管理を有効にし、ユーザーとデバイスを拡張可能なグループに動的にマッピングします。これにより、IP アクセスリストに依存した従来のネットワークポリシー導入に比べ、大規模なエンドツーエンドのセキュリティポリシー管理とポリシー適用が容易になります。

Cisco ISE では、スタンドアロンおよび分散型の導入モデルがサポートされています。複数の分散ノードを一緒に展開して、フェールオーバーの復元力と拡張性を提供できます。さまざまな導入オプションにより、何十万ものエンドポイントデバイスをサポートできます。SD-Access 単一サイト導入環境における Cisco ISE の導入としては、基本的な 2 ノード構成で各 Cisco ISE ノードがすべてのサービス（ペルソナ）を実行し、冗長性を確保することが推奨されます。

詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。『Cisco ISE Performance and Scalability Guide』も参照してください。

Cisco Catalyst 9000 シリーズ スイッチ

Cisco Catalyst 9000 シリーズ スイッチは、柔軟で拡張性の高い設計オプションを提供します。さまざまなファブリックロールでサポートされているスイッチは、ネットワーク内のユーザーとエンドポイントに安全で高速で信頼性の高い接続を提供します。詳細については、『Catalyst 9000 Data Sheet』を参照してください。

Cisco Catalyst ワイヤレス LAN コントローラおよびアクセスポイント

Cisco Catalyst 9800 シリーズ ワイヤレス LAN コントローラ（WLC）とアクセスポイント（AP）は、ワイヤレスクライアントのオンプレミスとクラウドの両方でシームレスなネットワーク管理と展開を提供します。Catalyst 9800 および Catalyst 9100 デバイスの完全なデータシートについては、次を参照してください。

- Cisco Catalyst 9800 シリーズ
- Cisco Catalyst 9100 シリーズ
- シスコ アクセスポイントおよびワイヤレス コントローラ セレクタ

Cisco SD-Access ファブリック

Cisco SD-Access は、従来のキャンパス LAN 設計の進化形であり、組織の目的（インテント）を明確に反映できます。SD-Access は、有線およびワイヤレスのキャンパスネットワークを自動化するために使用されるソフトウェアソリューションです。SD-Access の不可欠な部分であるファブリックテクノロジーにより、有線/ワイヤレスのキャンパスネットワークとプログラム可能なオーバーレイおよび簡単に導入できるネットワーク仮想化を提供し、設計の意図を満たすように 1 つ以上の論理ネットワークをホストする物理ネットワークを可能にします。

ネットワーク仮想化に加えて、キャンパスネットワークにおけるファブリックテクノロジーでは、通信の制御が強化され、ユーザー ID とグループメンバーシップに基づいたソフトウェア デファインド セグメンテーションとポリシー適用が可能です。ソフトウェア デファインド セグメンテーションは、Cisco TrustSec によってシームレスに統合され、仮想ネットワーク内の SGT を使用したマイクロセグメンテーションを実現します。Catalyst Center を使用して、統合されたセキュリティとセグメンテーションを備えた仮想ネットワークの作成を自動化することで、運用コストを削減し、リスクを軽減します。ネットワークパフォーマンス、ネットワークインサイト、およびテレメトリは、アシュアランスおよび分析機能を通じて提供されます。Cisco SD-Access は有線とワイヤレスのクライアントにポリシーモビリティを提供します。

ファブリックアーキテクチャの概要

次のセクションでは、Cisco SD-Access のアーキテクチャとソリューションのコンポーネントの概要について説明します。

ソリューションのコンポーネント

Cisco SD-Access ソリューションは、Catalyst Center、Cisco ISE、およびファブリック機能を備えた有線およびワイヤレス デバイス プラットフォームの組み合わせによって提供されます。有線およびワイヤレス デバイス プラットフォームは、ファブリックサイトの要素を作成するために使用されます。SD-Access アプリケーションパッケージを含む Catalyst Center ソフトウェアは、Catalyst Center ハードウェアアプライアンスで実行されます。

運用プレーン

- コントロールプレーン：ファブリック内のインフラストラクチャ デバイス間のメッセージングおよび通信プロトコル。
- データプレーン：データパケットに使用されるカプセル化方式。
- ポリシープレーン：セキュリティとセグメンテーションに使用される。
- 管理プレーン：オーケストレーション、アシュアランス、可視性、および管理。

SD-Access では、コントロールプレーンは Locator/ID Separation Protocol（LISP）に基づいています。データプレーンは Virtual Extensible LAN（VXLAN）に基づいています。ポリシープレーンは Cisco TrustSec に基づいています。管理プレーンは、Catalyst Center によって有効化され、電源が供給されます。

ネットワーク アーキテクチャ

SD-Access アーキテクチャは、キャンパスに導入されたファブリック技術によってサポートされており、物理ネットワーク（アンダーレイネットワーク）上で動作する仮想ネットワーク（オーバーレイネットワーク）を使用して、デバイスを接続する代替トポロジを構築できます。SD-Access では、ユーザー定義のオーバーレイネットワークは、ルーティングテーブルの分離を提供する VRF インスタンスとしてプロビジョニングされます。

ファブリックロール

ファブリックロールは、物理ハードウェアで実行される SD-Access ソフトウェア構造です。さまざまなファブリックロールでサポートされるハードウェアモデルについては、『Cisco SD-Access Compatibility Matrix』を参照してください。

- コントロール プレーン ノード

  SD-Access ファブリック コントロール プレーン ノードは、同じノード上に統合された LISP Map-Server 機能と Map-Resolver 機能をベースにしています。コントロールプレーンノードのデータベースは、ファブリック サイト内のすべてのエンドポイントを追跡し、エンドポイントをファブリック ノードに関連付けて、ネットワーク内の場所（至近ルータ）からエンドポイント IP アドレスまたは MAC アドレスを分離します。

- エッジノード

  SD-Access ファブリックエッジノードは、従来のキャンパス LAN 設計内のアクセスレイヤスイッチと同等です。エッジノードはエンドポイントをローカルに登録し、コントロールプレーンノードを更新します。エッジノードは、ホストがファブリックネットワークに接続するためのエニーキャストレイヤ 3 ゲートウェイを提供し、ホストの認証リレーエージェントとして機能します。

- 中間ノード

  中間ノードは、ボーダーノードとエッジノード間の相互接続などの、ファブリックロールで動作しているデバイス間の相互接続に使用されるレイヤ 3 ネットワークの一部です。これらのノードは、IP 到達可能性と物理

接続を提供し、ファブリック VXLAN 情報を使用してカプセル化されたより大きなサイズの IP パケットに対応するための追加の MTU 要件をサポートしています。

- ボーダー ノード

  ファブリックボーダーノードは、SD-Access ファブリックサイトとファブリック外部のネットワーク間のゲートウェイとして機能します。ボーダーノードは、VRF-Lite および VRF 対応のルーティングプロトコルを使用してセグメンテーションを維持することで、ネットワーク仮想化をファブリック内からファブリック外に拡張できます。これは、単一のスイッチ、ハードウェアスタックを使用するスイッチ、または StackWise Virtual 展開にすることができます。

- ファブリック イン ア ボックス

  ファブリックインアボックスは、ボーダーノード、コントロールプレーンノード、およびエッジノードが同じファブリックノードで実行されている SD-Access コンストラクトです。これは、単一のスイッチ、ハードウェアスタックを使用するスイッチ、または StackWise Virtual 展開にすることができます。

  詳細については、『Cisco Catalyst 9000 Platform StackWise Virtual White Paper』を参照してください。

- 拡張ノード

  SD-Access 拡張ノードは、企業のオフィス外のスペースへの接続を提供することにより、企業ネットワークを拡張する機能を提供し、一般的に拡張エンタープライズと呼ばれます。拡張ノードは、レイヤ 2 ポート拡張をファブリックエッジノードへ提供し、セグメンテーションおよびグループベースのポリシーをそれらのスイッチに接続されているエンドポイントに提供します。拡張ノードの設計の詳細については、『Cisco SD-Access Solution Design Guide』を参照してください。

- ファブリック ワイヤレス コントローラと AP

  ファブリック ワイヤレス コントローラと非ファブリック ワイヤレス コントローラは、AP イメージと設定管理、クライアントセッション管理、モビリティサービスに対応しています。ファブリック ワイヤレス コントローラは、ファブリック コントロール プレーン ノードのホスト トラッキング データベースへのワイヤレスクライアントの MAC アドレスの登録など、ファブリック統合のための追加サービスを提供します。ファブリックモード AP は、1 つ以上のファブリック対応 SSID が設定されているファブリック ワイヤレス コントローラに関連付けられた、Cisco Wi-Fi 6 （802.11ax）および 802.11ac Wave 2 AP です。ファブリックモード AP は、AVC、QoS、その他のワイヤレスポリシーの適用など、従来の AP がサポートするのと同じワイヤレスメディアサービスをサポートします。

  ワイヤレス操作と SD-Access ワイヤレス、ファブリック ワイヤレス コントローラ、およびファブリック AP との通信については、『SD-Access Wireless Design and Deployment Guide』を参照してください。

- SD-Access 組み込み型ワイヤレス

  分散したブランチや小規模キャンパスで、ハードウェア ワイヤレス コントローラなしでのワイヤレスコントローラ機能は、ソフトウェアパッケージとして、Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込み型ワイヤレスコントローラで実現できます。Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込み型ワイヤレスコントローラは、次のトポロジでの SD-Access 展開でサポートされています。

  - 同じ場所に配置されたボーダーおよびコントロールプレーンとして機能する Cisco Catalyst 9000 シリーズ スイッチ
  - ボーダーおよびコントロールプレーンノードがルーティング プラットフォーム上にある場合に、エッジノードとして機能する Cisco Catalyst 9000 シリーズ スイッチ。
  - ボックス内のファブリックとして機能する Cisco Catalyst 9000 シリーズ スイッチ。

- トランジットネットワークおよびピアネットワーク

トランジットネットワークとピアネットワークは、ファブリックサイト間またはファブリックサイトと外部の間の接続のボーダーノード設定を Catalyst Center が自動化する方法を定義する SD-Access コンストラクトです。この接続には、MAN、WAN、またはインターネットがあります。SD-Access ファブリックで使用可能な 2 つの異なるタイプのトランジットネットワークは、分散キャンパスと外部ネットワークを接続するための SDA トランジットと IP トランジットです。

- トランジット コントロール プレーンノード

  トランジット コントロール プレーン ノードは、分散キャンパスの SD-Access でサポートされているファブリック ロール コンストラクトです。これは、ファブリック全体にサービスを提供することを除いて、サイト ローカル コントロール プレーン ノードと同じように機能します。トランジット コントロール プレーン ノードは、SD-Access トランジットを使用する場合にのみ必要です。詳細については、『Software-Defined Access for Distributed Campus Deployment Guide』を参照してください。

  Cisco SD-Access のコンポーネントとアーキテクチャの詳細については、こちらを参照してください。

高可用性

Cisco SD-Access の高可用性（HA）とは、SDA ソリューションの継続的で信頼性の高い運用を保証する機能とメカニズムの設計と実装を指します。HA は、特に重要な環境で、ダウンタイムを最小限に抑え、ネットワーク機能を維持するために不可欠です。

Cisco SD-Access HA は、冗長性、フェールオーバーメカニズム、ロードバランシング、ヘルスモニタリング、および高速コンバージェンスを組み合わせることで、堅牢で復元力のあるネットワーク インフラストラクチャを作成することを目的としています。これらの機能は、予期しないイベントやハードウェアまたはソフトウェアの障害が発生した場合でも、継続的で信頼性の高いネットワークサービスを確保するのに役立ちます。

製造 SDA ネットワークには、次の HA コンポーネントが組み込まれています。

- 3 ノード Catalyst Center クラスタ

  Catalyst Center は 3 ノードクラスタとして設定されます。このクラスタリングアプローチにより、スケーラビリティ、負荷分散が強化され、フェールオーバー機能が提供され、ノード障害が発生した場合でも継続的な運用が保証されます。

- 分散型 Cisco ISE クラスタ

  Cisco ISE は、スタンドアロンおよび分散展開をサポートする可用性と拡張性の高いアーキテクチャを使用します。分散環境では、冗長ポリシー管理ノード（PAN）、モニター、およびポリシーサービスノード（PSN）が展開されます。ネットワークに展開されているセカンダリ Cisco ISE ノードを管理するために、1 つのプライマリ管理 Cisco ISE ノードを設定できます。

- FTD ファイアウォール フェールオーバー ペア

  Firepower Threat Defense（FTD）ファイアウォールは、フェールオーバーペア構成で展開されます。1 つのファイアウォールで障害が発生した場合、スタンバイファイアウォールがアクティブロールを引き継ぎ、ネットワーク セキュリティ サービスの中断を防ぎます。

- Catalyst 9800 シリーズ ワイヤレス コントローラ SSO HA

  Catalyst 9800 シリーズ ワイヤレス コントローラは、ステートフル スイッチオーバー（SSO）HA で設定されています。これにより、障害が発生した場合にスムーズに移行し、中断することなくワイヤレス ネットワーク サービスを維持できます。

- ボーダーおよびコントロールプレーン用 Catalyst 9500 SVL ペア

  Catalyst 9500 シリーズ スイッチのペアは、ボーダーおよびコントロールプレーン機能を処理するために StackWise Virtual Link（SVL）モードで設定されます。この冗長性により、これらの重要なネットワークコンポーネントの信頼性が向上します。

- ボーダーおよびコントロールプレーン用 Catalyst 9600 クワッド SUP SVL ペア

  大容量が必要な場合は、クワッド Supervisor Engine（SUP）を搭載した Catalyst 9600 シリーズ スイッチのペアを SVL モードで設定し、ボーダーおよびコントロールプレーンノードとして機能させ、冗長性とパフォーマンスの両方を提供します。

- ファブリックエッジとしての Catalyst 9300 スタッキングスイッチ

  Catalyst 9300 シリーズ スイッチは、スタック構成で設定されます。スタック構成により、これらのスイッチは単一の論理ユニットとして動作し、高可用性が提供され、管理が簡素化されます。

- ファブリックエッジとしての Catalyst 9400 デュアルスーパーバイザ

Catalyst 9400 シリーズ スイッチは、ファブリックエッジでの HA を確保するためにデュアル SUP を備えています。デュアル SUP は冗長性を提供し、SUP に障害が発生した場合でも動作が中断されないようにします。

これらのメカニズムは、Catalyst Center の SD-Access 環境における復元力と可用性の高いネットワーク インフラストラクチャに貢献し、潜在的な障害の影響を最小限に抑え、ネットワークの全体的な信頼性を向上させます。

互換性マトリックス

Catalyst Center は、シスコのエンタープライズ スイッチング、ルーティング、およびモビリティ製品を対象としています。サポートされているシスコ製品の完全なリストについては、次を参照してください。

- Cisco Catalyst Center Compatibility Matrix
- Cisco SD-Access Compatibility Matrix

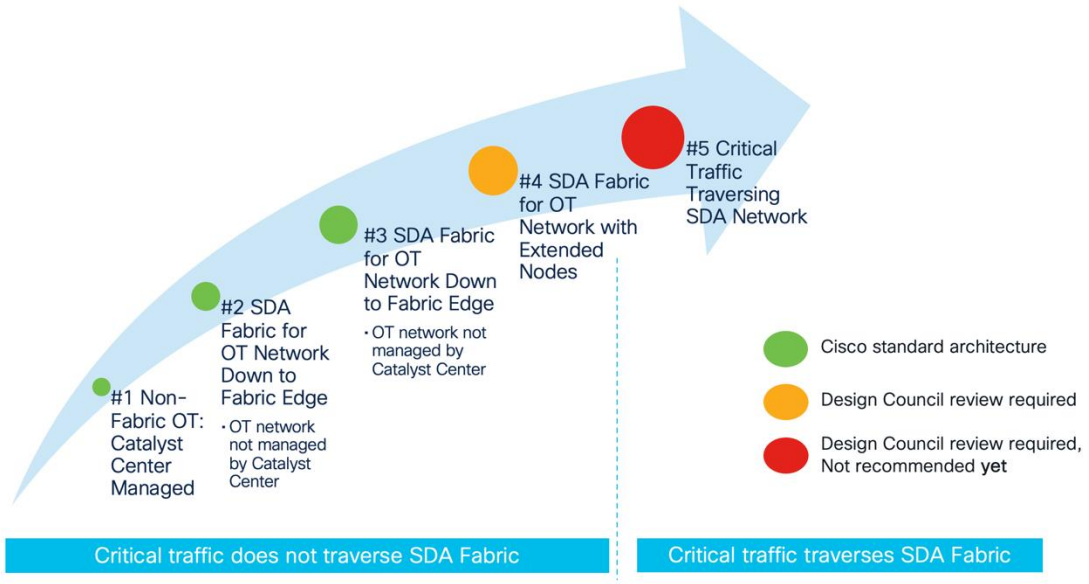
製造プロファイルの導入

このセクションでは、製造分野の設計ガイダンスを提供し、要件と、シンプルで安全性と柔軟性に優れたネットワークを実現するために Cisco SD-Access をこの業界でどのように使用するかに焦点を当てます。

製造業における SDA の進化を、次の図に視覚的に表します。最初のステップでは、Catalyst Center を使用して非 SDA ネットワークを管理し、自動化とアシュアランスのメリットを享受します。ステップ 2 は、ファブリックエッジに拡張された SDA ネットワークを示しています。OT アクセスネットワークは下に接続されていますが、Catalyst Center とは独立して、ファブリックの管理範囲外にあります。

ステップ 3 には、Catalyst Center の管理範囲に産業用スイッチが含まれます。産業用スイッチは、ファブリックの拡張として統合でき、拡張ノードまたはポリシー拡張ノードとして機能します。ただし、この導入オプションでは、インテントベースの設定との競合を精査する必要があるテンプレートが必要になる可能性があるため、設計審議会の承認が必要です。

導入モデル 2、3、および 4 には SDA ネットワークが組み込まれていますが、profinet や Ethernet/IP などの重要なトラフィックはファブリックエッジの下にローカライズされたままであり、ネットワークを通過しません。ステップ 5 では、重要なトラフィックが SDA ファブリックを通過します。この展開は現在推奨されていないことに注意してください。



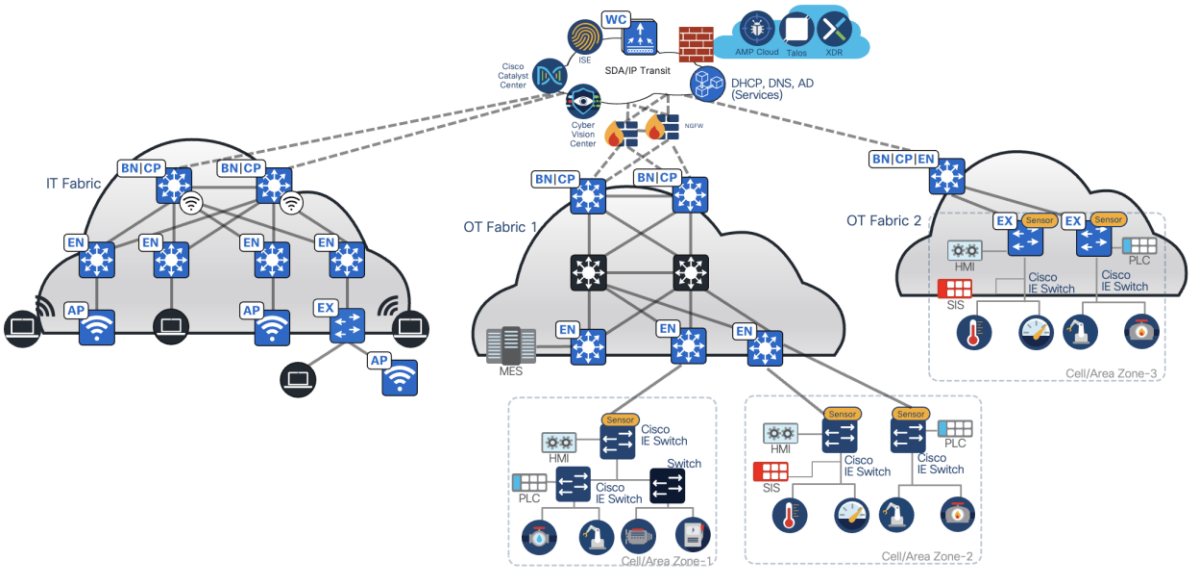
製造業のトポロジには、1 つの IT ネットワークサイト、1 つの中規模 OT サイト、および 1 つの小規模 OT ネットワークを管理するための 3 ノード Catalyst Center クラスタが含まれています。Cisco SD-Access トランジットは、これらのネットワークを接続するために展開されます。次の図は、製造業ソリューションのテストベッドの論理トポロジを示しています。

テストベッドのセットアップには、次のコンポーネントがあります。

- OT ファブリックサイト 1 には、デュアルボーダー、デュアル専用コントロールプレーンノード、デュアルワイヤレス コントローラ、10 個のファブリックエッジ、および 20 個の拡張ノードがあります。
- IT ネットワークサイトには、デュアル共存ボーダーおよびコントロールプレーンノード、ワイヤレスコントローラ、ファブリックエッジ、拡張ノードがあります。

- OT ファブリックサイト 2 は、ワイヤレスコントローラと拡張ノードを備えたハードウェアスタッキング上の一体型ファブリックを備えた小規模サイトです。
- SD-Access トランジットは、デュアル トランジット コントロール プレーン ノードで実装されます。IT ネットワークのボーダーは、SD-Access トランジットを介して他の OT サイトにインターネットアクセスを提供するように設定されています。

大規模製造：マルチサイト IT および OT の展開



ビジネスの成果と課題

製造ネットワークは広範で多様かつ複雑であり、固有の課題があります。これらのネットワークには、高度なレベルのセキュリティ、復元力、および規制コンプライアンスが必要です。次のセクションでは、ビジネス成果を達成するための製造ネットワークの最も重要な機能について説明します。

財務

数百ものサイトへの展開を自動化し、可能な限りオンサイトでのネットワーク運用の必要性を最小限に抑えることで、コストを合理化し、収益を向上させます。

大規模なマルチサイト展開

製造工場は通常、地理的に広い地域に数千の拠点を持つ大規模なマルチサイト展開です。オンサイトのネットワーク管理チームとともに、このような大規模なネットワークをボックスごとまたはサイトごとに導入および管理することは非常に困難です。製造ネットワークエンジニアは、最小限の手動作業で複雑なサイト展開を実行するための自動化を求めています。

自動化およびモニタリング

製造設備には、多数のデバイスと構成を持つ大規模で複雑なネットワークがあります。自動化により、ネットワークのプロビジョニング、設定の変更、およびメンテナンスタスクが合理化され、ダウンタイム、ワークロード、および人的エラーのリスクが削減されます。製造現場を対象としたネットワーク自動化ソリューションでは、これらの環境でのネットワーク接続を容易にする多数のネットワークデバイスがあるため、拡張性が不可欠です。

セキュリティ

今日の OT ネットワークでは、セグメンテーション機能が制限されている場合があり、多くのネットワークは VLAN ベースです。より深いセグメンテーションが必要な場合、多くの組織は物理的に分離された OT ネットワークを作成します。物理的な分離による強度を備えながら、単一のネットワークのシンプルさを備えた論理的なセグメンテーションが必要です。セグメンテーションは、サイバーセキュリティに対処するための手段として使用されることがあります。セグメンテーションが IP ACL によってインスタンス化される場合、ほとんどの単純な導入では、時間の経過とともに拡張、トラブルシューティング、および維持が困難になる可能性があります。

コンプライアンス規制

製造システムは、厳格な政府規制に従って、非常に機密性の高い財務記録と顧客情報を保護する必要があります。たとえば、決済カード業界（PCI-DSS）標準には、転送中のデータ暗号化、顧客データの保存に関するセキュリティ要件、ネットワークリソースとカード所有者データの追跡とモニタリングなどの要件が含まれています。

最後に、さまざまな部門とゲストがすべて同じネットワーク インフラストラクチャを共有しているため、すべてのグループを相互に分離し、アクセスが許可されているリソースのみに制限する必要があります。同時に、これらの多様なユーザーとデバイスのグループは、共有サービスにアクセスする必要があります。

エクスペリエンス

最新のテクノロジーを活用して主要なビジネス機能を実現し、サポートすることで、ユーザーエクスペリエンスとカスタマーエクスペリエンスを強化します。

サイレントホストの処理

OT ネットワークの最大の問題の 1 つは、製造現場のさまざまなエンドポイントです。一部のデバイスには静的 IP アドレスが割り当てられ、何年も変更されません。これらの中で、一部のエンドポイントはサイレントホストのカテゴリに属します。これは、通常、アドレス解決パケット（ARP）ブロードキャストパケットを受信して、サイレント状態から抜け出す必要があります。

QoS の影響を非常に受けやすい

セキュリティ、コンプライアンス、および可用性に関する懸念に加えて、低速で QoS がばらばらなネットワークは、顧客満足度の低下や金銭的損失につながる可能性があります。遅延の影響を受けやすい生産拠点では、組織のニーズを満たすために低遅延と一貫した QoS が必須です。

使用可能

生産性を最大化し、デジタル トランスフォーメーション イニシアチブを容易にしながら、評判を効果的に管理し、ブランド価値を高めます。

高可用性

多くの場合、製造作業は継続的に稼働します。ネットワークが中断すると、実稼働のダウンタイムや経済的損失が発生する可能性があります。HA は、ハードウェア障害、ソフトウェアの問題、接続の問題、またはその他の中断が発生した場合にネットワークが動作することを保証し、実稼働のダウンタイムを削減します。製造ネットワーク内の産業オートメーションおよび制御システム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。

一元化された一貫性のあるポリシー管理

ネットワークに接続するエンドポイントの数が急増し、大規模な工場が世界中に広がるにつれて、さまざまな地理的地域でセキュリティポリシーを管理する必要があります。

このことにより管理が複雑になります。ルールは現地の法律によって決定される可能性があるからです。セキュリティポリシーを直感的に管理できるように、ユーザーとデバイスのグループ化を簡素化する必要があります。

製造業のビジネス成果に対するソリューション

次のソリューションは、製造ネットワーク展開のビジネス成果を達成するのに役立ちます。

オフィス外でのスペース拡張

製造業では、OT ネットワーク内のデバイスは、オフィス外や起伏の激しい場所に配置されることがよくあります。この場合、Cisco Industrial Ethernet（IE）スイッチが拡張ノードとして使用されます。Cisco SD-Access 拡張ノードは、レイヤ 2 ポート拡張を提供し、既存のファブリックエッジノードへのポート密度を高めることでモビリティを実現すると同時に、セグメンテーションおよびグループベースのポリシーをそれらのスイッチに接続されているエンドポイントに提供します。Catalyst Center は、拡張ノードを検出、プロビジョニング、およびファブリックに追加するためのゼロタッチのプラグアンドプレイ自動ワークフローを提供することに注意してください。

Catalyst Center には、拡張ノードのサポートオプションとして、クラシック拡張ノード（EN）とポリシー拡張ノード（PEN）があります。PEN は、クラシック拡張ノードで提供される運用と管理に加えて、SGACL による SGT ポリシーの適用を直接サポートします。この SGACL のローカルサポートにより、PEN に水平方向のトラフィックを直接適用できます。

拡張ノードは、802.1Q トランクポートを介して単一のファブリックエッジスイッチに接続されます。このポートは、2 つ以上のリンクがアップストリーム ファブリック エッジで集約されている場合、EtherChannel として展開できます。トランクと EtherChannel の作成は Catalyst Center で自動化されています。ワークフローで拡張ノードがオンボーディングされた後、エンドポイント（ファブリックモード AP と他の Power over Ethernet（PoE）デバイスを含む）を拡張ノードに直接接続し、必要に応じて有線およびワイヤレスサービスをオフィス外のスペースに拡張できます。詳細については、『Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide』を参照してください。

シスコのプラグアンドプレイを使用した新しいスイッチの効率的なオンボーディング

製造工場では、新しいスイッチの迅速なオンボーディングがシームレスな運用にとって最も重要です。プロセスは次のようである必要があります。

- 迅速：新しいスイッチは迅速にオンボーディングされ、数分以内に運用の準備が整うようにする必要があります。
- シンプル：ネットワーキングに関するバックグラウンドを持たないオペレータでもオンボーディングプロセスを実行できる必要があります。
- スケーラブル：プロセスは、何百ものスイッチ間で複製できる必要があります。
- 一貫性：所定のワークフローに従うことで、均一な構成を保証し、人的エラーを防ぐ必要があります。

Catalyst Center のオンボーディングプロセスでは、プラグアンドプレイ（PnP）によるゼロタッチ導入（ZTD）を使用します。PnP は、サイトのネットワークプロファイルを活用して、ネットワーク内の新しい未設定のデバイスの自動設定を容易にします。サイトは、ネットワーク内の物理的な場所や機能によってデバイスをグループ化します。

IOS または IOS-XE ソフトウェアを実行しているシスコの産業用スイッチの場合、組み込みの PnP エージェントは PnP 導入サーバーと通信します。このエージェントは、新しく電源が投入されたデバイスや工場出荷時のデフォルトにリセットされたデバイスなど、スタートアップ コンフィギュレーションのないデバイスで動作します。エージェントは、Catalyst Center の DHCP または DNS を介して PnP 導入サーバーを検出します。PnP エージェントは、PnP サーバーとの通信を開始し、重要なソフトウェアとデバイスの設定をダウンロードします。

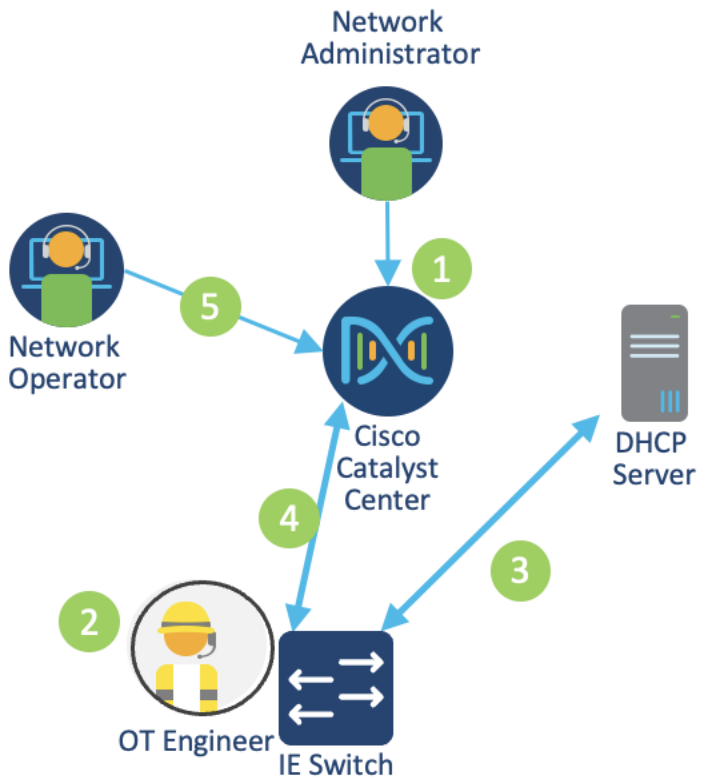
未設定のデバイスがネットワークに接続し、Catalyst Center に接続すると、デバイスのエントリが作成され、管理者が要求するまで要求元不明状態になります。または、インストール前にシリアル番号とデバイスファミリ

を入力して、デバイスを Catalyst Center に追加することもできます。接続後、デバイスは指定されたサイトに要求され、サイトの設定に基づいて事前に定義されたソフトウェアイメージと設定を使用して設定できます。

次の図は、PnP プロビジョニング ワークフローを示しています。

1. ネットワーク管理者が、Catalyst Center でサイト階層を作成し、サイトプロパティを設定し、プロビジョニング テンプレートを追加し、ゴールデンイメージを定義します。
2. OT エンジニアが産業用スイッチをネットワークに接続し、デバイスの電源を入れます。
3. スイッチは DHCP を使用して IP アドレスを取得し、PnP サーバーの IP アドレスを検出します（Catalyst Center）。
4. 産業用スイッチは Catalyst Center に接続します。
5. オペレータが Catalyst Center でデバイスを要求します。要求プロセス中に、Catalyst Center は次のことを行います。
   - ゴールデンイメージをインストールします。
   - ライセンスを含む設定を発行します。
   - Cisco ISE および Catalyst Center のインベントリにデバイスを追加します。

図 1.　　PnP プロビジョニング ワークフロー



Catalyst Center への設定済みデバイスの追加

PnP プロセスはスイッチのオンボーディングに対する効率的なアプローチを提供しますが、シナリオによっては別の方法が必要になる場合があります。次に例を示します。

- オフラインの新しいスイッチのプロビジョニング：特定の状況では、スイッチをネットワークに接続する前にプロビジョニングすることが必要です。これは、ネットワーク接続を確立する前にスイッチを設定する必要がある産業オートメーション環境に特に関連します。PnP プロセスは設定をネットワーク接続に依存しているため、オフラインでプロビジョニングされたスイッチには別のアプローチが必要です。
- 製造施設外で設定されたスイッチ：場合によっては、製造施設にスイッチが到着する前に、システムインテグレータがスイッチを設定します。この方法では、スイッチは事前設定されて到着し、すぐに導入できるため、オンボーディングプロセスが合理化されます。
- ブラウンフィールド展開：ブラウンフィールドとは、設定が確立された既存のサイトに統合されたデバイスを指します。ブラウンフィールド展開を扱う場合、ネットワークデバイスは検出と呼ばれるプロセスを通じて Catalyst Center に追加されます。

検出機能は、Catalyst Center にネットワークデバイスを追加するために使用されます。この機能は、ネットワーク内のデバイスのスキャンを実行し、検出されたデバイスのリストを送信し、インベントリにシームレスに統合します。

検出には、IP アドレス範囲、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）など、さまざまな方法を使用できます。このガイドでは、IP アドレス範囲が使用されます。検出タスク中に、Catalyst Center で CLI および SNMP 読み取りクレデンシャルを設定する必要があります。

サイトの割り当てとネットワークアシュアランス

デバイスの検出中に、デバイスを特定のサイトに割り当てるオプションを使用できます。これにより、Catalyst Center はテレメトリ設定をプッシュして、新しく追加されたデバイスにネットワークアシュアランスを提供します。

SD-Access フュージョンデバイスとしての Cisco Firepower 9300

ネットワークのセグメンテーションは、重要なビジネス資産を保護する上で重要な役割を果たします。SD-Access では、セグメンテーションによってセキュリティがネットワークにシームレスに統合されます。セグメンテーションでは、セキュリティ上の理由から、ユーザーまたはデバイスの特定のグループを他のグループから分離します。SD-Access では、マクロセグメンテーションとマイクロセグメンテーションの 2 つの主要なタイプのセグメンテーションが採用されています。

マクロセグメンテーション（仮想ネットワーク）

SD-Access のマクロセグメンテーションでは、統合ルーティングテーブルを使用して単一の大規模ネットワークを多数の小規模な論理ネットワーク（セグメントまたは仮想ネットワーク）に分割する必要があります。このプロセスは、セグメント間の分離を提供し、攻撃対象領域を縮小し、セグメント間に適用ポイントを導入します。SD-Access は、ネットワークの理解、設計、実装、およびサポートに対する簡単なアプローチを提供することで、環境でのセキュアなネットワーク展開を促進します。SD-Access ファブリック内では、VXLAN-GPO ヘッダー内の VXLAN ネットワーク識別子（VNI）フィールドで、仮想ネットワークを識別する情報と SGT が伝送されます。

マクロセグメンテーションは、一意のネットワーク識別子および個別の転送テーブルを使用して、ネットワークトポロジをより小さな仮想ネットワークに論理的に分割します。これは、Catalyst Center では仮想ネットワークと呼ばれる、スイッチまたはルータ上の VRF インスタンスとして実現されます。

SD-Access ファブリック内の仮想ネットワークは、論理ネットワークインスタンスであり、レイヤ 2 またはレイヤ 3 のサービスを提供し、レイヤ 3 のルーティングドメインを定義します。VXLAN ヘッダーの VNI フィー

ルドで、レイヤ 2（レイヤ 2 VNI）とレイヤ 3（レイヤ 3 VNI）の両方のセグメンテーションをサポートする、SD-Access ファブリック内の仮想ネットワークを識別する情報が伝送されます。

LISP は、コントロールプレーン転送情報を提供するために SD-Access ファブリック内で使用されます。LISP インスタンス ID により、コントロールプレーンで一意のアドレス空間が確保され、仮想化がサポートされます。外部の SD-Access ボーダーで、仮想ネットワークは VRF インスタンスに直接マッピングされ、ファブリックを超えて拡張される場合もあります。

このセグメンテーション アプローチにより、セキュリティが強化され、ネットワーク管理が簡素化され、複雑な環境でスケーラブルな展開が可能になります。

マイクロセグメンテーション（SGT）

シスコのグループベースポリシーにより、ネットワークのセキュリティと柔軟性を管理する方法が簡素化されます。複雑な技術的な詳細を扱う代わりに、ロールに基づいてデバイスをグループに編成します。これらのグループは、ネットワークのさまざまな部分で使用できるため、セキュリティルールの設定と管理が容易になります。

これは、デバイスを、デバイスのタイプやネットワーク内でのロールなど、使いやすいカテゴリに分類するようなものだと考えてください。複雑な IP アドレスに依存する従来の方法とは異なり、シスコのアプローチでは、これらの単純なカテゴリを使用してセキュリティルールを定義します。これにより、セキュリティ対策の制御と管理が簡単になります。

スケーラブルグループ（セキュリティグループとも呼ばれる）は、デバイスのロール、使用するアプリケーション、またはデバイスがもたらす脅威レベルなど、デバイスに関する情報を提供します。この追加のインサイトは、さまざまなネットワークデバイスでのファイアウォールルール、Web セキュリティポリシー、およびアクセス制御の設定を合理化するのに役立ちます。

シスコのグループベースのポリシーは、複雑な VLAN ベースのセグメンテーションを伴う従来の方法とは異なり、有効にして管理するのが簡単です。

SD-Access では、仮想ネットワークと SGT を使用して、マクロレベルとマイクロレベルの両方でネットワーク セグメンテーションが行われます。仮想ネットワークは、SD-Access ファブリック内の独立したドメインとして機能し、異なる仮想ネットワーク間のマクロセグメンテーションを提供し、各仮想ネットワーク内のデバイス間の通信を可能にします。デフォルトでは、仮想ネットワーク内のデバイスは相互に通信できますが、異なる仮想ネットワーク間の通信を容易にするために、フュージョンルータやファイアウォールなどの外部デバイスが VRF 間転送を処理する必要があります。より細かいスケールでは、SGT を介してマイクロセグメンテーションが実現され、仮想ネットワーク内の通信をより詳細に制御できます。このアプローチにより、SD-Access 内の構造化されたセキュアなネットワーク環境が保証されます。

SD-Access のフュージョンデバイスは、ファブリックドメイン間での VRF リークを促進し、データセンターまたはサービスブロック内の DHCP、DNS、NTP、Cisco ISE、Catalyst Center、ワイヤレス LAN コントローラなどの共有サービスへのホスト接続を可能にします。このロールはさまざまなデバイスで実行できますが、このガイドでは、フュージョンデバイスとしての Cisco FTD ルーテッドモードのファイアウォールに焦点を当てています。キャンパス内のすべての仮想ネットワークに共有サービスを提供するために、ボーダーノードと FTD ファイアウォールの間に BGP ピアリングが作成されます。フュージョンデバイスは、共有サービスへのアクセスを必要とするファブリック VRF サブネットをグローバル ルーティング テーブル（GRT）または共有サービス VRF にリークし、その逆も行います。

この検証では、コントロールプレーンとデータプレーンの分離に Cisco Firepower ファイアウォール上の仮想ルータを使用します。仮想ルータは、単一ファイアウォール上のインターフェイスグループの個別のルーティングテーブルを管理します。

REP リング

産業用オートメーションプロセスは、産業用自動化制御システム（IACS）アプリケーションの可用性と稼働時間に依存しています。これらのシステムの継続性を確保するには、復元力があり堅牢なネットワーク設計が不可欠です。標準イーサネットおよび IP コンバージド IACS ネットワーキング テクノロジーの復元力と堅牢さを強化する LAN アーキテクチャを実装することで、総合設備効率（OEE）を向上させ、障害の影響を最小限に抑え、平均修復時間（MTTR）を短縮できます。

復元力のある設計により、機器やリンクに障害が発生した場合に代替パスが提供されます。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アップリンクで、ネットワーク冗長性が提供されます。冗長リンク内のループを防止するには、復元力プロトコルを導入する必要があります。Resilient Ethernet Protocol（REP）は、リングトポロジ内のループを防止するプロトコルの例です。

REP はシスコ独自のプロトコルで、スパニングツリープロトコル（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、リンクまたはノード障害の処理、コンバージェンス時間の回避を実現します。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操作します。REP セグメントは、相互接続されたポートから構成され、固有のセグメント ID があります。各セグメントには、標準セグメントポートと、2 つのユーザー設定のエッジポートが含まれます。ネットワークセグメントは、エッジポートと呼ばれる終端ポートを使用して、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 スイッチで終端します。リング内のループの防止は、セグメント内の 1 つのポート（代替ポートとも呼ばれます）をブロックすることにより行われます。セグメント障害が発生した場合、代替ポートはフォワーディングステートに移行し、トラフィックが代替パスを通過できるようにし、ネットワーク障害をバイパスします。

産業オートメーションにおける復元力プロトコルの詳細については、「Networking and Security in Industrial Automation Environments」を参照してください。

Catalyst Center には、SDA ファブリックサイトで REP リングを作成して導入するワークフローが用意されており、IE スイッチはファブリックエッジに接続され、拡張ノードの 2 つのデイジーチェーンとしてオンボーディングされます。Catalyst Center で REP リングの自動化を設定するには、次の手順を実行します。

ステップ 1. メニューアイコンをクリックして、[Workflows] > [Create REP Ring] を選択します。

または、ファブリック サイト トポロジ ビューに移動して、REP リングを作成するファブリックエッジノードまたは FIAB ノードを選択し、[REP Rings] タブで [Create REP Ring] をクリックします。

ステップ 2. ドロップダウンリストからファブリックサイトを選択し、[Next] をクリックします。

ステップ 3. トポロジビューでファブリックエッジノードを選択し、[Next] をクリックします。

ステップ 4. ファブリックエッジノードに接続する拡張ノードを選択し、[Next] をクリックします。

ファブリックエッジノードに接続する 2 つの拡張ノードを選択できます。

ステップ 5. ファブリックサイト、エッジノード、および拡張ノードの選択を確認し、必要に応じて編集して、[Provision] をクリックします。

ステップ 6. [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。[次へ（Next）] をクリックします。

ステップ 7. REP リングの作成後、成功メッセージが表示されます。

ステップ 8. REP リングの作成を確認するには、ファブリック サイト ウィンドウに移動し、ファブリックエッジノードをクリックします。スライドインペインの [REP Ring] タブで、そのエッジノードに存在するすべての REP リングのリストを確認できます。

ゼロ損失冗長性：PRP を使用したデュアルファブリック

OT ネットワークが組織の機能にとって重要になるにつれて、ネットワークの完全な冗長オプションに至るまでの復元力を提供することが重要になります。これらの冗長性スキームでは、ネットワークが回復し、トラフィックが再び流れるまでに数ミリ秒から数秒かかることがあります。製造現場の品質管理システム（SAP など）がダウンしている場合、製造ラインもダウンします。ネットワークが影響を受けると、工場がダウンする可能性が高く、1 秒あたりの経済的損失が発生します。

ネットワーク障害から回復するために、RSTP、REP、MRP などのプロトコルを使用して、メッシュトポロジまたはリングトポロジで接続されたネットワーク要素によって冗長性を提供できます。ネットワーク障害が発生すると、通常はブロックされたポートを開くことによって、トラフィックが再び流れるようにネットワーク内で再構成されます。製造業のお客様には、パケット損失ゼロに対する厳しい要件があります。

Parallel Redundancy Protocol（PRP）は、国際規格 IEC 62439-3 で定義されています。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 は異なる方式を使用します。この方式では、2 つのネットワーク インターフェイスを 2 つの独立した分離されたパラレルネットワーク（LAN-A と LAN-B）に接続することで、（ネットワーク要素ではなく）エンドノードが冗長性を実装します。各デュアル通信ノード（DAN）には、ネットワーク内にある他のすべての DAN への冗長パスがあります。

SDA ネットワークで PRP を活用して、冗長 SDA ファブリックを作成し、メインサイトと冗長サイトの両方に拡張ノードを接続することで、パケット損失ゼロを実現するソリューションがあります。次のサンプルトポロジには、2 つの SDA ファブリックサイトが含まれています。

この実装は、拡張ノードのオンボーディングと CLI テンプレートを使用して、拡張ノードに PRP 固有の設定をプッシュする Catalyst Center で実現されます。

ステップ 1. 通常の PAgP ポートチャネルを介して拡張ノードをファブリック 1 に接続します。ファブリック 1 は、LAN 自動化プロセスによってポリシー拡張ノードとしてオンボーディングされます。

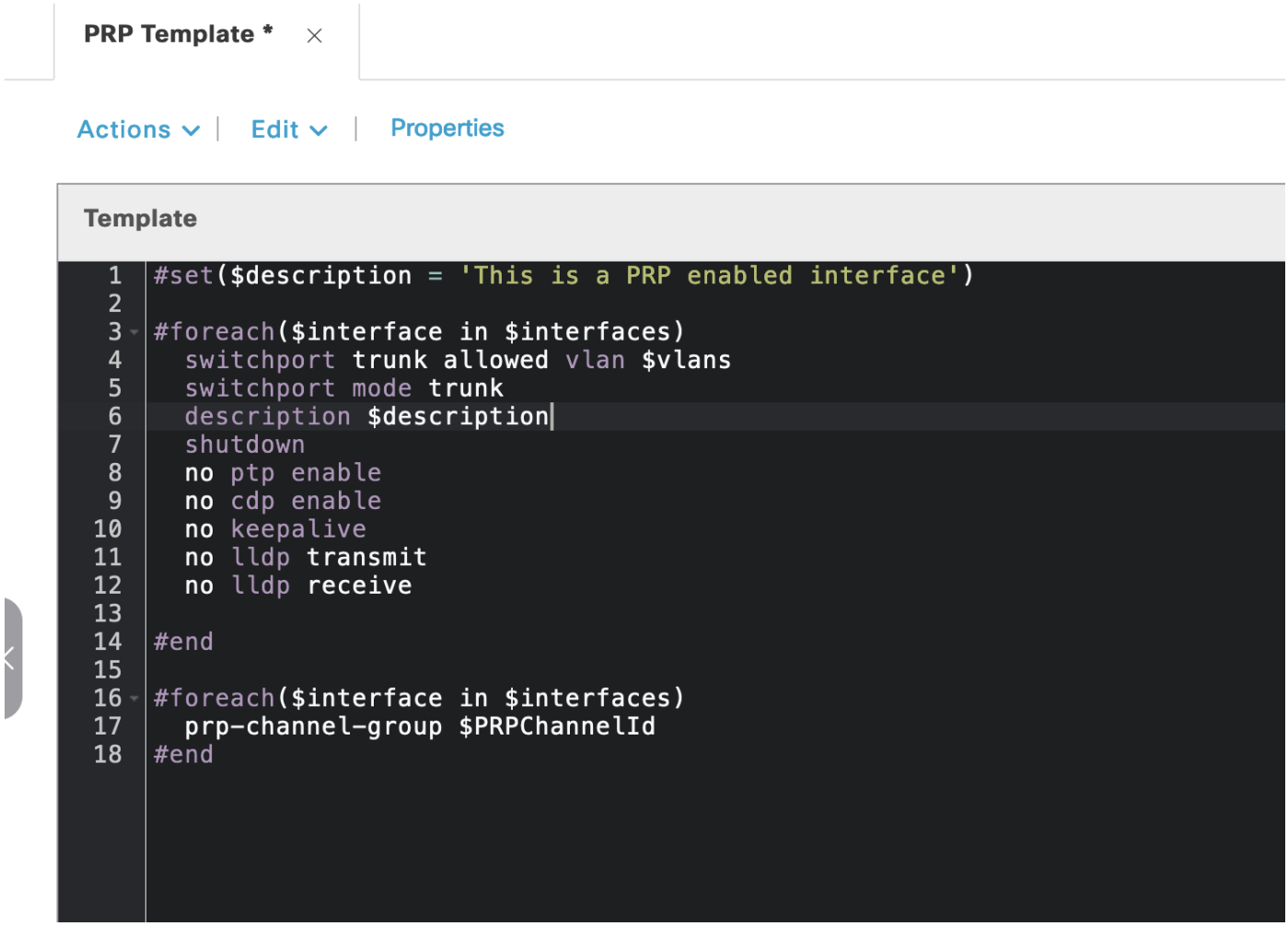
```
interface Port-channel1

 description Extended2

 switchport mode trunk

!

interface GigabitEthernet1/0/11

 switchport mode trunk

 cts manual

  policy static sgt 8000 trusted

 channel-group 1 mode desirable
```

ステップ 2. IE スイッチが正常にオンボーディングされると、ファブリック 2 エッジノードのダウンリンクポートが Catalyst Center GUI から PAgP トランクポートとして設定されます。

```
interface Port-channel1

 switchport mode trunk

 device-tracking attach-policy IPDT_POLICY

!
```

```
interface GigabitEthernet1/0/13

 switchport mode trunk

 channel-group 1 mode desirable
```

ステップ 3. 両方のファブリックサイトからのエッジが IE スイッチに接続され、プロビジョニングされたら、Catalyst Center テンプレートのプロビジョニングを使用して PRP 設定を IE スイッチのアップリンクポートに適用します。次の Velocity テンプレートのサンプルで PRP 設定を示します。



Cisco Cyber Vision による OT ネットワークの可視性

可視性の欠如は、産業用ネットワークの一般的な課題です。ネットワークが古く、広範囲に分散していて、多くの請負業者が関与している場合、多くの場合、運用担当者は、ネットワーク上にどんな機器があるかを正確に管理できていません。このように可視性が欠如しているため、セキュアな通信アーキテクチャを構築することが困難になっています。可視性が欠如しているということは、どのデバイスが相互に通信しているかを運用担当者が把握しておらず、さらには、外部から産業用デバイスに接続している通信さえ認識できていない可能性があるということです。可視性の欠如は、セグメンテーションや制御の欠如につながります。

OT の可視性は、OT 環境のすべてのペルソナが活用できるテクノロジーです。OT オペレータは、プロセスレベルの可視性を活用して、製造現場に存在するアセットを特定してトラブルシューティングすることができます。IT オペレータは、デバイスの通信パターンに関するインサイトを得て、ポリシーに情報を提供し、ネットワー

ク効率を向上させることができます。セキュリティチームは、デバイスの脆弱性とデバイスの通常の動作からの逸脱に関するインサイトを得ることができます。可視性は次の点で重要です。

- すべてのアセットを特定し、それらをゾーンにグループ化します。
- ゾーン間のコンジットを流れるデータを可視化します。
- 外部ネットワークを介して着信するソースデータを明確に把握できます。

Cisco Cyber Vision は、産業用ネットワークの可視性のニーズに対応します。Cisco Cyber Vision は、産業用ネットワーク内のディープ パケット インスペクション、プロトコル分析、および侵入検知を実行する複数のセンサーデバイスで構成されるエッジアーキテクチャ上に構築されています。Cyber Vision Center はアグリゲーション プラットフォームとして動作し、センサーからのデータを保存し、ユーザーインターフェイス、分析、振る舞い分析、レポート作成、API などを提供します。詳細については、『Industrial Automation Security Design Guide 2.0』を参照してください。

Cisco Cyber Vision センサーは、Catalyst Center によって管理されるスイッチに導入されます。テンプレートを使用して、Catalyst Center を介してセンサーを設置できるように産業用スイッチを準備することができます。

検証済みのソリューションの使用例

次のセクションでは、製造ネットワークについて検証済みの重要な使用例の一部について説明します。組織は、これらの設計が徹底的なテストを受け、ビジネス要件を効果的に満たすように調整されていることを確認しながら、確実に IT/OT インフラストラクチャを構築できます。

Day-0 運用の使用例

Catalyst Center で有線デバイスを使用して新しい製造拠点を立ち上げます。

- LAN 自動化によりネットワークをプロビジョニングする。
- デバイスとトポロジを検出する。
- 設定をプロビジョニングする。
- ファブリックを作成する。
- ファブリックにエッジデバイスと拡張ノードを追加する。
- デバイスとクライアントの認証、有線およびワイヤレスのプロファイリングのために Cisco ISE と統合する。
- ワイヤレスコントローラと AP を管理および導入する。
- ネットワークデバイスと AP のプラグアンドプレイを介してデバイスをオンボーディングする。
- 共有サービスに Cisco Catalyst を使用して、複数のサイトのネットワーク設定を管理する。

Catalyst Center で OT スペースのワイヤレスネットワークを展開します。

- Catalyst Center サイトにフロアマップをアップロードする。
- プラグアンドプレイを使用して新しい AP を追加し、新しい AP を新しいサイトの場所に割り当て、フロアマップ上に配置する。
- 新しいサイトでワイヤレスプロファイルとポリシーを作成してプロビジョニングする。

Day-1 運用の使用例

Catalyst Center を使用してワイヤレスネットワークを管理およびプロビジョニングします。

- ワイヤレス設定とネットワークプロファイルを変更する。
- 新しい SSID を作成し、既存の SSID を更新する。
- プロファイル、タグ、AP ゾーンなどを更新する。
- プラグアンドプレイを使用して新しい AP をオンボードする。
- Catalyst Center ワークフローを使用して AP を交換または更新する。
- AP の場所を変更し、AP を再プロビジョニングする。

Catalyst Center を使用してネットワークセキュリティを管理およびプロビジョニングします。

- 脅威をモニターし、不正ルールと Advanced Wireless Intrusion Prevention System（aWIPS）プロファイルを管理する。
- トラフィック セグメンテーションを使用してゲストアクセス Wi-Fi を設定する。
- AP オンボーディングに MAC 認証バイパス（MAB）または Dot1x 認証を適用する。
- Dot1x や事前共有キー（PSK）などの有線およびワイヤレスのエンドポイント セキュリティ ポリシーを設定する。
- ネットワークデバイスをスキャンし、セキュリティアドバイザリを提供する。

ネットワーク管理、モニタリング、およびトラブルシューティングの使用例

Catalyst Center でネットワークインベントリを管理します。

- プラグアンドプレイを使用してデバイスをオンボードする。
- IP アドレスまたは Cisco Discovery Protocol（CDP）でデバイスを検出する。
- 破損したデバイスを交換する。
- コンプライアンスチェックの実行。
- ロケーション間でのデバイスの移動。
- デバイス証明書の管理。
- パスワード変更の管理。

Catalyst Center でデバイス設定を管理します。

- デバイステンプレートを使用して新しい設定を展開する。
- デバイス設定の変更を追跡する。
- アシュアランス監査ログを使用して、設定中に発生したエラーをモニターする。

Catalyst Center を使用してデバイスソフトウェアを管理し、アップグレードをスケジュールします。

- ネットワークルータとスイッチをアップグレードする（SLV ペアとスタックスイッチを含む）。
- ワイヤレスデバイスをアップグレードする（ワイヤレスコントローラ SSO ペアと C9800-CL を含む）。
- AP のローリングアップグレードをスケジュールする。
- ソフトウェアイメージ管理（SWIM）レポートを生成する。

アシュアランスを使用して、ネットワークとデバイスの正常性、クライアントエンドポイント、およびネットワーク使用率をモニターします。

- ネットワークデバイスの正常性と使用率をモニターする。
- 各ロケーションのシステムの正常性をモニターする。
- AAA や DHCP などのネットワークサービスをモニターする。
- ワイヤレスコントローラおよび AP をモニターする。
- 有線およびワイヤレスクライアントの数と詳細をモニターする。

Catalyst Center を使用してネットワークの問題をトラブルシューティングします。

- デバイスにアクセスし、SSH を介して CLI コマンドを実行する。
- デバイス設定の変更内容を比較する。
- パストレースを実行し、リンク障害を検出する。
- 高 CPU 使用率の根本原因を分析する。
- アプリケーションまたはデバイスの Public Key Infrastructure（PKI）証明書のトラブルシューティングについて、監査ログを確認する。

システムとネットワークの堅牢性の使用例

以下のイベント発生時にシステムレベルの復元力を確認します。

- ワイヤレスコントローラ SSO。
- 単一 AP の障害。

以下のイベント発生時にシステムレベルの復元力を確認します。

- SVL ボーダーとコントロールプレーンのフェールオーバー。
- SVL ボーダーとコントロールプレーンのリンク障害。
- スタック アクセス スイッチ メンバーの障害。
- ディストリビューションとファブリックエッジ間のリンク障害。
- ディストリビューションとファブリックボーダーとコントロールプレーンノード間のリンク障害。

以下のイベント発生時にシステムレベルの復元力を確認します。

- ポリシーサービスノード（PSN）の障害。
- ポリシー管理ノード（PAN）のフェールオーバー。
- Cisco ISE PSN の変更。
- Cisco ISE のアップグレード。

スケールマトリックス

ソリューションでは、次の表に示すスケールの数値について確認しました。ソフトウェアおよびハードウェアの適合規格については、『Cisco Catalyst Center Data Sheet』を参照してください。

属性	SDA スケール番号
インベントリのデバイス数	5000
ファブリックサイトごとのデバイス	1000
建物とフロア	2000
ファブリックサイトごとの VN	64
ファブリックサイトの IP プール	500
ファブリックサイトのワイヤレスコントローラ	2
ファブリックサイト	500
インベントリの AP	12,000
エンドポイント	100,000（有線 80,000、ワイヤレス 20,000）
SSID	10
SGT	4000
REP リング内の IE デバイス	18

注： ESXi 仮想アプライアンス上の Catalyst Center は、小規模環境向けの 44 コア物理アプライアンスと同じ規模とパフォーマンスをサポートします。『Cisco Catalyst Center on ESXi Deployment Guide』を参照してください。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。サポートされているハードウェアとソフトウェアの完全なリストについては、『Cisco Catalyst Center Compatibility Matrix』を参照してください。

ロール	ハードウェア プラットフォーム	ソフトウェア バージョン
Catalyst Center	DN2-HW-APL-XL	2.3.7.7
Catalyst Center	DNA-SW-OVA	2.3.7.7
アイデンティティ管理、RADIUS サーバー	SNS-3695-K9	3.3 パッチ 4
Cisco ワイヤレス コントローラ	C9800-80-K9、C9800-CL	17.9.6、17.12.4
Cisco SD-Access ファブリックエッジ	C9200, C9300, C9400	17.9.5、17.12.4
ファブリックボーダー/コントロールプレーン	C9500-40x/C9606R	17.9.5、17.12.4
Cisco Firepower Threat Defense セキュリティ アプライアンス	FPR9300、FPR4100	7.2
Cisco Secure Firewall Management Center	FMC 仮想	7.2
Cisco Industrial Ethernet IE3400 拡張ノード	Cisco Catalyst IE3400 高耐久性 シリーズ	17.9.5、17.12.4
Cisco Cyber Vision	センターとセンサー	4.4

- ESXi 上の Catalyst Center には制限事項があります。『Cisco Catalyst Center on ESXi Release Notes』を参照してください。
- Catalyst Center アプリケーション プラットフォームとは異なり、VM を接続して 3 ノードクラスタを作成することはできません。HA を実現するには、VMware vSphere を使用する必要があります。『Cisco Catalyst Center on ESXi Administrator Guide』を参照してください。

テクニカル リファレンス

- Cisco SD-Access Solution Design Guide (CVD)
- Cisco Catalyst Center Administrator Guide
- Cisco Catalyst Center for Industrial Automation Design Guide
- Support for Multiple Cisco Catalyst Center Clusters with a Single Cisco ISE System
- Cisco Catalyst Center Release Notes
- Cisco Catalyst Center Security Best Practices Guide
- Software Defined Access (SDA) Provisioning Best Practice Guide

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。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/jp/go/offices）をご覧ください。

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