検証済みプロファイル：大学業界

2025 年 6 月 27 日

ソリューションの概要

本ドキュメントは、Catalyst Center と Cisco Software-Defined Access（SD-Access）ソリューションを用いた大学ネットワークの導入に関するガイドラインを提供し、検証済みの参照資料として機能することを目的としています。

教育業界は現在大きな変革期にあり、スマートキャンパス技術の導入、自動化、ハイブリッド学習環境、安全な遠隔教育の普及が進んでいます。学生や教職員がデバイスをキャンパスに持ち込むことで接続端末が爆発的に増加し、独自の課題を発生させています。さらに、大学の学生や教員は広い範囲を移動することが多く、研究資料への即時アクセスを必要とします。

他の産業と同様に、教育ネットワークにも高度なネットワークサービス、シームレスなモビリティ、高可用性、効率的な管理が要求されます。ただし、大学ネットワークには特有の要件があり、寮サービス向けのセキュリティ強化、ワイヤレス主体のインフラストラクチャ、堅牢なワイヤレスモビリティのサポートが必要です。

本ドキュメントでは、教育分野の特定のニーズに対応するための主要な考慮事項を取り上げます。

スコープ

本ガイドは、大学ネットワークが直面する課題を理解し、一般的なユースケースを検討し、Cisco SD-Access がそれらのニーズにどのように対応できるかを示すための包括的なロードマップとして機能します。詳細な設定手順には踏み込みませんが、効果的な大学ネットワーク戦略の策定を支援するための有益なインサイトを提供します。

従来のネットワークと Cisco SD-Access の比較

このセクションでは、従来型ネットワークと Cisco SD-Access の主な違いを概観します。

従来型ネットワーク

- 従来のネットワークでは、ネットワークデバイスを手動で設定する必要がある。
- セグメンテーションのために別のオーバーレイネットワークが必要になることが多い。
- セキュリティポリシーは通常、ネットワーク境界間で適用される。
- ネットワークの拡張は複雑で、時間がかかる場合がある。
- 障害対応は多くの場合リアクティブで、手作業が必要。
- ネットワークトラフィックやアプリケーションのパフォーマンスに関する可視性が限定的。

Cisco SD-Access

- SD-Access は、インテントベースの自動化により、ネットワークのプロビジョニングと管理を自動化。
- 単一のアンダーレイネットワークを用いて接続性とセグメンテーションを両立させ、VXLAN オーバーレイ内で仮想ネットワーク（VN）とセキュリティグループタグ（SGT）の情報を伝送ことで設計を簡素化。
- ユーザーやデバイスのアイデンティティに基づき、セキュリティポリシーを動的に適用。
- SD-Access は自動化と集中管理により、より容易にスケール可能。
- ネットワーク全体の可視性と分析により、障害対応をプロアクティブに実施可能。
- SD-Access は、ネットワークトラフィックやアプリケーション性能に関する詳細なインサイトを提供。

つまり、Cisco SD-Access は従来型ネットワークと比べて、中央管理、拡張性の向上、強化されたセキュリティ機能により、より効率的で柔軟なアプローチを実現します。

従来のネットワークの課題

今日、手作業による設定や断片化されたツールのために、ネットワーク管理には多くの課題が発生しています。手動運用は遅く、エラーが発生しやすい上、常に変化する環境によって問題はさらに深刻化しています。ユーザー数やデバイスの種類が増加することで、ネットワーク全体で一貫したユーザーポリシーを設定および維持する作業はますます複雑化します。

- ネットワーク導入の課題

  単一のネットワークスイッチの設定または導入は、スケジュール要件およびさまざまなインフラストラクチャグループへの対応ニーズにより、数時間かかる場合があります。場合によっては、スイッチのバッチの導入に数週間がかかることもあります。

- ネットワークセキュリティの課題

  セキュリティは最新ネットワークを管理するための 重要な構成要素です。組織はリソースを保護し、リアルタイムのニーズに応じて効率的に変更を加える必要があります。従来型ネットワークでは、最適なポリシーやセキュリティ コンプライアンスを確保するために VLAN、アクセス制御リスト（ACL）、IP アドレスを追跡することが難しい場合があります。

- ワイヤレスおよび有線ネットワークの課題

  異種ネットワークは多くの組織に共通しています。これは、システムがそれぞれ異なる部門で管理されているからです。通常、メインの IT ネットワークは、ビルの管理システム、セキュリティシステムおよび他の生産システムとは別に運用されます。これにより、ネットワークハードウェアの調達の重複や、管理作業の不一致が生じます。

- ネットワーク運用の課題

  IT チームは、時代遅れの変更管理ツールを使わざるを得ないことが多く、生産性の維持や迅速な問題解決が困難だと感じています。

Cisco SD-Access の利点

Cisco SD-Access は、急速なデジタル化の要求に対応するために設計されています。Cisco SD-Access のアーキテクチャの核心はポリシーベースの自動化であり、有線とワイヤレスを問わず安全なユーザーおよびデバイスのセグメンテーションを可能にします。

自動化と簡素化によって生産性を高め、IT スタッフが迅速にイノベーションを進めてデジタル トランスフォーメーションを主導することを可能にし、運用効率を向上させます。一貫したセグメンテーションのフレームワークをビジネスポリシーと整合させ、有線と無線両方の伝送メディアに適用することが、核心となる効率性のために不可欠です。

Cisco SD-Access が提供する技術的な利点は以下のとおりです。

- 運用の簡素化

  直感的な単一インターフェイスでインフラストラクチャ全体を管理し、複雑さと運用負荷を軽減することで、ネットワーク運用を簡素化します。

- 自動化

  設定、プロビジョニング、管理といった日常的なネットワーク業務を自動化します。人的ミスのリスクを減らし、効率を向上させます。Catalyst Center によって導入を合理化することで、CLI（コマンド ライン インターフェイス）への依存を最小化します。

- 俊敏性

  手動設定を最小限に抑えることで、ネットワーク運用をアジャイルにし、ビジネス要件に合わせることができます。

- セキュリティ

  仮想ネットワーク（VN）と Security グループタグ（SGT）によって、セキュリティ強化とセグメンテーションを可能にします。SD-Access は、仮想ネットワーク（VN）によるマクロセグメンテーション、およびセキュリティグループタグ（SGT）によるマイクロセグメンテーションを介して、複雑な企業ネットワークを保護および管理するための強力なフレームワークを提供します。

- 有線およびワイヤレスに対応した一貫性のあるポリシー

  有線から無線までセグメンテーション、可視性、ポリシーを拡張します。分散型ワイヤレス終端処理により、スループットを拡張しつつ、管理とトラブルシューティングを一元化します。

- ビジネス分析のサポート

  分析やテレメトリ情報を単一のプラットフォームに集約し、ビジネス上の意思決定や、成長と多角化の計画を支援します。

大学のネットワークの概要

大学のネットワークにおける課題とユースケースに合わせて、Cisco SD-Access ファブリックの新規グリーンフィールド展開を構築するためのガイダンスと推奨事項については、SD-Access ファブリックのコンポーネントを詳細に解説しているセクションを参照してください。教育分野特有の要件や課題に対応するために、Cisco SD-Access ソリューションがもたらすメリットをご覧ください。

従来のネットワークは、Cisco Prime Infrastructure または Catalyst Center を使用して管理できます。Catalyst Center は、従来のネットワークと SD-Access 環境の両方に対して、高度な自動化、監視、テレメトリ機能を提供します。現在 Cisco Prime Infrastructure でネットワークを管理しており、Catalyst Center への移行を計画している場合は、『Cisco Prime Infrastructure to Cisco Catalyst Center Migration』を参照してください。

既存の Cisco Catalyst レガシーネットワークを Cisco SD-Access ファブリックに移行するには、有線および無線エンドポイントの両方で既存のネットワークを移行するためのオプションを概説している『Migration to Cisco SD-Access』を参照してください。

Cisco Catalyst Center

Catalyst Center（旧 Cisco DNA Center）は、ネットワークの運用と管理を簡素化するために設計された、一元的なネットワーク管理およびオーケストレーション プラットフォームです。スイッチ、ルータ、ワイヤレスアクセスポイント（AP）を含むネットワーク インフラストラクチャを管理および監視するための単一のダッシュボードを提供します。

Catalyst Center を使用することで、ネットワーク管理者は以下のような様々なタスクを実行できます。

- 自動ネットワーク プロビジョニング

  自動化されたワークフローを使用してネットワークデバイスやサービスを簡単に展開し、設定に必要な時間と労力を削減します。

- ネットワークの正常性の監視

  デバイスの状態、トラフィックパターン、評価指標など、ネットワーク全体を可視化することで、問題を迅速に特定し解決します。

- セキュリティポリシーの導入

  ネットワーク全体でセキュリティポリシーを定義して適用することで、コンプライアンスを確保し、脅威から保護します。

- ソフトウェアアップデートの管理

  デバイスのソフトウェアやファームウェアのアップデートプロセスを簡素化し、ネットワークデバイスが最新の機能とセキュリティパッチで更新されていることを保証します。

- ネットワークの問題のトラブルシュート

  内蔵のツールと分析機能を使用して、ネットワークの問題を迅速に診断および解決し、ダウンタイムと中断を最小限に抑えます。

全体として、Catalyst Center は組織がネットワーク運用を合理化し、効率性を向上させ、セキュリティを強化するのに役立ちます。そのため、最新のネットワーク インフラストラクチャを管理するための不可欠なツールとなっています。

Catalyst Center プラットフォームは、物理アプライアンスや仮想アプライアンスなど、さまざまなフォームファクタで利用できます。詳細については、次の資料を参照してください。

- 『Cisco Catalyst Center Data Sheet』（サポートされているプラットフォームと拡張について）
- Cisco Catalyst Center Installation Guide [英語]

Cisco Identity Service Engine

Cisco Identity Services Engine（ISE）は、セキュリティポリシー管理および制御プラットフォームです。有線、ワイヤレス、VPN 接続のアクセス制御とセキュリティ コンプライアンスを自動化し、シンプルにします。Cisco ISE は、ネットワークリソースへのセキュアなアクセスを提供し、セキュリティポリシーを適用し、ネットワークアクセスを包括的に可視化します。

Cisco ISE の主要機能は以下のとおりです。

- ポリシーベースのアクセス制御

  ユーザーロール、デバイスタイプ、その他のコンテキスト情報に基づいてポリシーを定義し、適用します。

- 認証と承認

  さまざまな認証方式（802.1X、MAB、Web 認証など）をサポートしており、変化する条件に基づいた動的な承認を可能にします。

- エンドポイント コンプライアンス

  エンドポイントがセキュリティポリシーに準拠しているかどうかを評価し、必要に応じて是正アクションを実行します。

- ゲストアクセス

  カスタマイズ可能なゲストポータルとスポンサー承認ワークフローを通じて、ネットワークへの安全なゲストアクセスを提供します。

- Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）サポート

  デバイスのオンボーディングとポリシーの適用により、セキュアな BYOD イニシアチブを可能にします。

- 統合とエコシステム

  API とパートナーエコシステムを通じて、他のセキュリティおよびネットワーキング技術と統合します。

- 可視性とレポート

  包括的なレポートと分析機能を通じて、ネットワークアクセスとセキュリティ態勢に関するインサイトを得ることができます。

Cisco ISE は、シスコのセキュリティおよびネットワークアクセス制御ポートフォリオの重要なコンポーネントであり、組織のセキュリティおよびアクセス制御のニーズに対応する、一元的で拡張性に優れたソリューションを提供します。Cisco Identity Services Engine（ISE）は、スタンドアロンおよび分散型の両方の導入モデルをサポートしています。複数の分散ノードをまとめて導入することで、フェールオーバー時の復元力と拡張性を高めることができます。SD-Access 単一サイト展開環境における ISE の最小展開としては、基本的な 2 ノード構成で各 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、以下を参照してください。

- Cisco Identity Services Engine Administrator Guides
- Cisco Identity Services Engine のパフォーマンスと拡張性ガイド

Cisco SD-Access ファブリック

Cisco SD-Access ファブリックは、ソフトウェア定義型ネットワーキング（SDN）の概念を使用してネットワークのプロビジョニング、セグメンテーション、ポリシーの適用を自動化するネットワーキング アーキテクチャです。現代のデジタルワークプレイスにおいて、ネットワーク運用を簡素化し、セキュリティを強化し、ユーザー体験を向上させることを目的としています。

Cisco SD-Access ファブリックの主な機能は以下のとおりです。

- 有線とワイヤレスの統合的自動化

  SD-Access の優れた機能の 1 つは、有線とワイヤレスネットワークを単一の自動管理フレームワークに統合できることです。

- ネットワーク セグメンテーション

  ユーザーやデバイスの ID に基づいてネットワークを仮想セグメントに分割し、アクセスやセキュリティポリシーをきめ細かく制御できるようにします。

- ポリシー管理の一元化

  ポリシーは一元的に定義され、ネットワーク全体で一貫して適用されるため、設定不備やポリシーの競合のリスクが低減します。

- ISE：

  認証と承認のサービスを提供し、承認されたユーザーとデバイスのみがネットワークにアクセスできるようにします。

- Catalyst Center

  SD-Access の管理およびオーケストレーション プラットフォームとして機能し、ネットワーク管理と障害対応のための単一の管理画面を提供します。

- 拡張性

  大規模な展開をサポートし、組織がニーズの拡大に合わせてネットワークを簡単に拡張できるようにします。

- セキュリティの強化

  ネットワークを動的にセグメント化し、ユーザーおよびデバイスアイデンティティに基づいてセキュリティポリシーを適用することで、ネットワークセキュリティを向上させます。

全体として、Cisco SD-Access ファブリックはネットワーク管理を簡素化し、セキュリティを向上させ、拡張性を高めることを目的としており、ネットワーク インフラストラクチャの最新化を検討している組織にとって魅力的な選択肢です。

ファブリックアーキテクチャの概要

Cisco SD-Access ファブリックアーキテクチャは、ネットワーク運用の簡素化、セキュリティの強化、ユーザー体験の向上を目的に設計されています。ソフトウェア定義型ネットワーキング（SDN）の原則に基づいており、以下の目標を達成するためのさまざまなコンポーネントが組み込まれています。

- アンダーレイネットワーク

  デバイス間の基本的な接続性を提供する物理的なネットワーク インフラストラクチャ。通常、スイッチ、ルータ、ケーブルで構成されます。

- オーバーレイネットワーク

  アンダーレイネットワークの上に構築された論理ネットワークで、デバイス間の仮想化された接続性を提供します。これにより、物理的な再設定を行うことなく、ネットワークのセグメンテーションとポリシー適用を可能にします。

- コントロールプレーン：

  ルーティング、転送、ポリシー適用など、ネットワーク全体の動作を管理します。通常、Catalyst Center のような一元的なコントローラを使用して実装されます。

- データプレーン：

  ネットワーク内で実際のデータパケットの転送を処理します。スイッチやルータなどのネットワークデバイス上に実装され、コントロールプレーンから提供される指示に基づいて動作します。

- ポリシープレーン：

  アクセス制御やセグメンテーションなどのネットワークポリシーを定義して適用します。これにより、ネットワークリソースが効率的かつ安全に使用されることを保証します。

- 管理プレーン：

  ネットワークの管理と監視のためのツールやインターフェイスを提供します。設定管理、監視、障害対応などの機能が含まれています。

全体として、Cisco SD-Access ファブリックアーキテクチャは、ネットワーク インフラストラクチャを最新化するための包括的なソリューションを提供し、進化するデジタルビジネスのニーズを満たすための拡張性、セキュリティ、および自動化機能を提供します。

ネットワークアーキテクチャ

ファブリック技術は、キャンパス内の SD-Access アーキテクチャをサポートしており、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 VN（オーバーレイネットワーク）を利用して、デバイスを接続するための代替トポロジを作成できるようにします。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仮装ルーティング及び転送（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。これらのソフトウェア構造は、モジュール性と柔軟性を念頭に置いて設計されています。たとえば、1 つのデバイスが単一のロール、あるいは複数のロールを実行できます。SD-Access のファブリックロールは、基盤となるネットワークアーキテクチャに合わせてプロビジョニングし、分散機能アプローチを確保するように注意する必要があります。さまざまなデバイス間にロールを分散することで、最高レベルの可用性、復元力、確定的なコンバージェンス、および拡張性が提供されます。

SD-Access のファブリックロールには以下が含まれます。

- コントロール プレーン ノード
- ボーダー ノード
- エッジ ノード
- 中間ノード
- ファブリック ワイヤレス コントローラ
- ファブリックモード AP

コントロール プレーン ノード

SD-Access ファブリックのコントロールプレーンノードは、LISP のマップサーバー機能とマップリゾルバ機能を単一のノードに統合したものです。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するデータベースを保持し、それらをファブリックノードにマッピングします。この設計により、エンドポイントの IP アドレスまたは MAC アドレスがその物理的な位置（最寄りのルータ）から分離され、効率的なネットワーク運用が保証されます。

コントロールプレーンノードの主要機能は以下のとおりです。

- ホスト トラッキング データベース（HTDB）

  EID と RLOC のバインディング（ルーティングロケータ（RLOC）はファブリックノードのループバックゼロ IP アドレス）の中央リポジトリとして機能します。従来型の LISP サイトと同様に、エンドポイントの登録を保存します。

- エンドポイント識別子（EID）

  MAC、IPv4、または IPv6 アドレスを使用して、SD-Access ネットワーク内のエンドポイントデバイスを識別します。

- マップサーバー

  エンドポイントの登録を受け取り、対応する RLOC と関連付け、それに従って HTDB を更新します。

- マップリゾルバ

  ファブリックデバイスからのクエリに応答し、HTDB から EID と RLOC のマッピングを提供します。これにより、デバイスはトラフィックを転送する適切なファブリックノードを決定できます。

ボーダー ノード

SD-Access ファブリックのボーダーノードは、ファブリックサイトと外部ネットワーク間のゲートウェイとして機能し、ネットワーク仮想化のインターワーキングと、ファブリック外への SGT の伝達を処理します。

ボーダーノードの主要な機能は以下のとおりです。

- EID サブネットのアドバタイズ

ボーダー ゲートウェイ プロトコル（BGP）を使用して、ファブリック外部にエンドポイントのプレフィックスをアドバタイズし、戻りトラフィックが正しくルーティングされるようにします。

- ファブリックサイトの出口ポイント

  LISP Proxy Tunnel Router（PxTR）を使用するエッジノードのデフォルトゲートウェイとして機能します。内部ボーダーノードは、既知のサブネットをコントロールプレーンノードに登録できます。

- ネットワーク仮想化の拡張

  VRF-lite および VRF 認識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ファブリック外に拡張します。

- ポリシーマッピング

  SGT Exchange Protocol（SXP）または Cisco のメタデータ内のインラインタギングを介して、ファブリック外の SGT 情報を維持します。

- VXLAN のカプセル化と非カプセル化

  外部トラフィックをファブリック用の VXLAN に変換し、外部へ向かうトラフィックから VXLAN を削除することで、ファブリックと非ファブリックネットワーク間のブリッジとして機能します。

エッジ ノード

SD-Access ファブリックのエッジノードは、従来のキャンパス LAN におけるアクセスレイヤスイッチのように機能します。これらは LISP の入力/出力トンネルルータ（xTR）に基づいて動作し、レイヤ 3 ルーテッドアクセス設計を使用して展開する必要があります。これらのエッジノードは、以下のようないくつかの重要な機能を実行します。

- エンドポイントの登録

  各エッジノードは、すべてのコントロールプレーンノードとの LISP コントロールプレーンセッションを維持します。エンドポイントが検出されると、EID テーブルと呼ばれるローカルデータベースに追加されます。その後、エッジノードは LISP マップ登録メッセージを送信し、コントロールプレーンの HTDB（ホスト トラッキング データベース）を更新します。

- エニーキャストレイヤ 3 ゲートウェイ

  同じ EID サブネットを共有するすべてのエッジノードは、シームレスなモビリティと最適な転送のために、共通の IP アドレスと MAC アドレスを使用します。エニーキャストゲートウェイは、ファブリック内のすべてのエッジノードで統一された MAC アドレスを持つスイッチ仮装インターフェイス（SVI）として実装されます。

- レイヤ 2 ブリッジング

  エッジノードは、同じ VLAN 内のエンドポイントに対するレイヤ 2 トラフィックを処理します。パケットをブリッジするかルーティングするかを判断し、VXLAN レイヤ 2 VNI（VLAN に相当）を使用して、トラフィックを正しい接続先にブリッジします。トラフィックがファブリック外に出る必要がある場合は、レイヤ 2 ボーダーノードが使用されます。

- ユーザーと VN のマッピング

  エンドポイントは、SVI および VRF にリンクされた VLAN と関連付けられることで、VN に割り当てられます。このマッピングにより、コントロールプレーンレベルでも、レイヤ 2 と レイヤ 3 の両方の LISP VNI でファブリック セグメンテーションが確保されます。

- AAA 認証

エッジノードは、802.1X 認証を使用して、エンドポイントを VLAN に静的または動的に割り当てることができます。ネットワーク アクセス デバイス（NAD）として機能し、認証情報を収集して認証サーバーに送信し、アクセスポリシーを適用します。

- VXLAN のカプセル化と非カプセル化

  エッジノードがエンドポイント（直接接続、拡張ノード経由、または AP 経由）からトラフィックを受信すると、それを VXLAN にカプセル化し、ファブリック全体に転送します。接続先に応じて、トラフィックは別のエッジノードまたはボーダーノードに送信されます。カプセル化されたトラフィックがエッジノードに到着すると、非カプセル化され、エンドポイントに配信されます。このメカニズムにより、端末モビリティが実現し、デバイスは IP アドレスを変更することなくエッジノード間を移動できます。

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接続など、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。これらの相互接続は、デバイス上のグローバル ルーティング テーブルで確立され、総称してアンダーレイネットワークと呼ばれます。たとえば、コアスイッチがボーダーノードとして、アクセススイッチがエッジノードとしてプロビジョニングされている 3 層キャンパス展開では、ディストリビューション スイッチが中間ノードとして機能します。

中間ノードは、VXLAN のカプセル化/非カプセル化、LISP コントロール プレーン メッセージング、SGT 認識を必要としません。その主な機能は、IP 到達可能性と物理的な接続性を提供することであり、ファブリックの VXLAN 情報でカプセル化されたより大きな IP パケットに対応するために、最大伝送ユニット（MTU）の増加もサポートします。基本的に、中間ノードは、ファブリックロールで動作しているデバイス間で IP トラフィックをルーティングおよび転送します。

ファブリック ワイヤレス コントローラ

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、ワイヤレスクライアントのジョインイベント中にクライアントの MAC アドレスをファブリック コントロール プレーンノードの HTDB に登録したり、クライアントのローミング時にファブリックエッジノードの RLOC 関連付けの更新を HTDB に提供したりするなど、ファブリック統合のための追加サービスを提供します。ワイヤレスコントローラとのファブリック統合は、SSID ごとに実施されます。ファブリック対応の SSID トラフィックは、AP によって VXLAN カプセル化を使用してファブリックエッジノードにトンネリングされます。一方、中央スイッチングされた SSID トラフィックは、AP によって CAPWAP（Control and Provisioning of Wireless Access Points）プロトコルを使用してワイヤレスコントローラにトンネリングされます。したがって、ワイヤレスコントローラは、一部の SSID がファブリック対応で他の SSID が中央スイッチングされる、ハイブリッドまたは混合モードで動作できます。

- 従来のデータ処理と SD-Access のデータ処理

  従来の Cisco Unified Wireless Network または非ファブリック展開では、制御トラフィックとデータトラフィックの両方が CAPWAP を使用してワイヤレスコントローラにトンネリングされます。CAPWAP コントロールプレーンの観点から見ると、AP 管理トラフィックは一般的に軽量ですが、クライアント データ トラフィックはより大きな帯域幅を消費します。ワイヤレス規格は、ワイヤレスクライアントのデータレートを次第に大きくすることを可能にし、その結果、より多くのクライアントデータがワイヤレスコントローラにトンネリングされるようになっています。これには、クライアントトラフィックの増加をサポートするために、複数の高帯域幅インターフェイスを備えた、より大規模なワイヤレスコントローラが必要になります。

  非ファブリックのワイヤレス展開では、有線とワイヤレスのトラフィックはネットワーク内で異なるエンフォースメントポイントを持ちます。ワイヤレスコントローラは、ワイヤレストラフィックを有線ネットワークにブリッジする際に、サービス品質とセキュリティに対応します。有線トラフィックの場合、適用は最初のホップ アクセス レイヤ スイッチで行われます。SD-Access ワイヤレスでは、このパラダイムが完全に変わります。SD-Access ワイヤレスでは、ワイヤレスコントローラと AP 間の CAPWAP トンネルは制御トラ

フィックにのみ使用されます。ワイヤレスエンドポイントからのデータトラフィックは、最初のホップ ファブリック エッジ ノードにトンネリングされ、そこで有線トラフィックと同じ方法でセキュリティとポリシーを適用できます。

- ネットワーク接続とワイヤレスコントローラの配置

  通常、ファブリック ワイヤレス コントローラは、ファブリックおよびファブリックボーダーの外に位置するディストリビューション ブロックまたはデータセンターネットワークを介して共有サービスネットワークに接続され、ワイヤレスコントローラの管理 IP アドレスはグローバル ルーティング テーブルに存在します。ワイヤレス AP がワイヤレスコントローラ管理のための CAPWAP トンネルを確立するには、AP は外部デバイスへのアクセス権を持つ VN に存在する必要があります。これは、AP がグローバル ルーティング テーブルに展開され、ワイヤレスコントローラの管理サブネットまたは特定のプレフィックスが、ファブリックサイト内のグローバル ルーティング テーブル（GRT）に存在しなければならないことを意味します。

  SD-Access ソリューションでは、Cisco Catalyst Center が、グローバル ルーティング テーブルにマッピングされる INFRA_VN というオーバーレイ VN 内にワイヤレス AP を配置するように設定します。この設定により、ワイヤレスコントローラと AP 間の接続を確立するためのルートリーキングやフュージョンルーティング（複数の VRF デバイスがルーティング情報を選択的に共有すること）が不要になります。各ファブリックサイトには、そのサイト専用のワイヤレスコントローラが必要です。ローカルモードの AP には遅延要件があるため、ほとんどの展開では、ワイヤレスコントローラを WAN ではなく、ローカルのファブリックサイト自体に配置します。

- 遅延要件と展開の考慮事項

  ファブリック AP はローカルモードで動作するため、AP とワイヤレスコントローラ間のラウンドトリップ時間（RTT）が 20 ミリ秒以下である必要があります。これは通常、ワイヤレスコントローラが AP と同じ物理サイトに展開されることを意味します。ただし、専用のダークファイバーやその他の非常に低遅延な回線によって物理サイト間でこの遅延要件が満たされ、ワイヤレスコントローラが中央データセンターなど物理的に別の場所に展開されている場合、ワイヤレスコントローラと AP は異なる物理的な場所に置くことができます。

  ファブリック AP がファブリック ワイヤレス コントローラから離れて配置されるこの展開タイプは、メトロエリアネットワークや分散キャンパス環境向けの SD-Access で一般的に使用されます。SD-Access ネットワークでは、AP をワイヤレスコントローラから WAN やその他の高遅延回線を介して展開すべきではありません。これらのデバイス間で最大 20 ミリ秒の RTT を維持することが、パフォーマンスにとって極めて重要です。

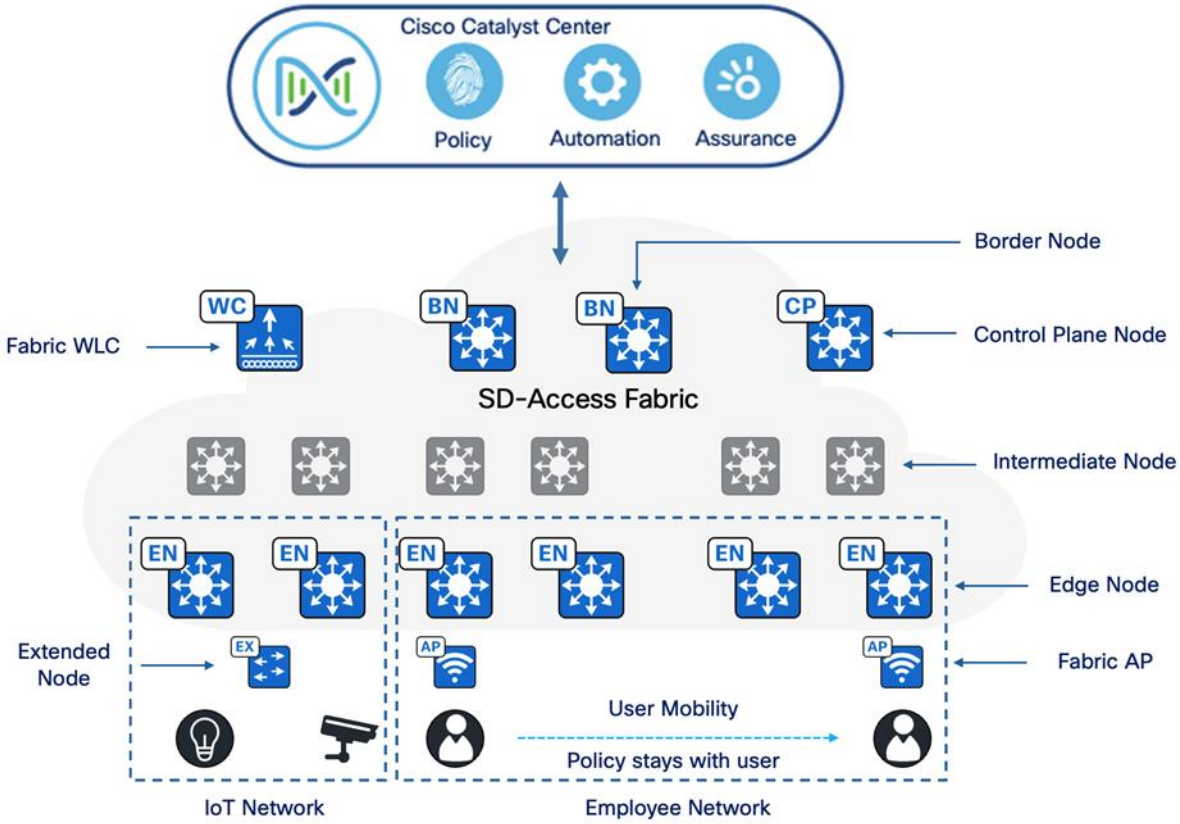
ファブリックモード AP

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 7（802.11be）Wi-Fi 6（802.11ax）および 802.11ac Wave 2 AP です。これらのファブリックモード AP は、Cisco Application Visibility and Control（AVC）、Quality of Service（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引き続きサポートします。ファブリック AP は、ワイヤレスコントローラへの CAPWAP コントロール プレーン トンネルを確立し、ローカルモード AP として参加します。これらは、ファブリックサイト内のファブリックエッジノードまたは拡張ノードスイッチに直接接続されている必要があります。データプレーンについては、ファブリック AP は最初のホップとなるファブリックエッジスイッチに VXLAN トンネルを確立し、そこでワイヤレスクライアントのトラフィックが終了され、有線ネットワークに配置されます。

ファブリック AP は、特殊な有線ホストと見なされます。エッジノードは、Cisco Discovery Protocol を使用して AP をこれらの有線ホストとして認識し、特定のポート設定を適用し、AP を INFRA_VN という固有のオーバーレイネットワークに割り当てます。有線ホストとして、AP は専用の EID 空間を持ち、コントロールプレーンノードに登録されます。この EID 空間は、Cisco Catalyst Center の UI で事前定義された INFRA_VN オーバーレイネットワークに関連付けられます。これは、ファブリックサイト内のすべてのファブリック AP に共通の EID 空間（プレフィックス空間）および VN です。このオーバーレイ VN への割り当てにより、単一のサブ

ネットを使用してファブリックサイト内の AP インフラストラクチャ全体をカバーできるため、管理が簡素化されます。

図 1.　SD-Access ファブリック展開に関わる主要コンポーネントと、SD-Access ネットワーク内における各コンポーネントの位置付け



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（FIAB）は、従来の SD-Access ネットワークが持つボーダーノード、コントロールプレーンノード、エッジノードといったすべての機能を単一の物理デバイスに統合したものです。このデバイスは、単一のスイッチ、ハードウェアスタック機能を備えたスイッチ、または StackWise Virtual 展開の一部にすることができます。

FIAB の利点は以下のとおりです。

- 簡易性
- 高い費用対効果
- 展開の高速化
- ブランチや小規模の展開に最適

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

拡張ノード

SD-Access の拡張ノードは、エンタープライズネットワークをオフィス以外のエリアに拡張することを可能にします。拡張ノードは、セグメンテーションを確保し、接続されたエンドポイントにグループベースのポリシーを適用しながら、ファブリックエッジノードへのレイヤ 2 ポート拡張を提供します。拡張ノードを使用することで、組織はセキュリティの強化、管理の簡素化、一貫したポリシー適用といった SD-Access のメリットを、ネットワーク内のより広範なデバイスやエンドポイントにまで広げることができます。

詳細については、「Extended Node Design」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

ワイヤレスコントローラと従来のワイヤレスコントローラは、AP のイメージと設定の管理、クライアントセッションの処理、およびモビリティサービスの提供を行います。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ポートを提供します。

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 7（802.11be）Wi-Fi 6（802.11ax）および 802.11ac Wave 2 AP です。これらのファブリックモード AP は、AVC、Quality of Service（QoS）、および従来の AP が持つその他のワイヤレスポリシーなどのワイヤレスメディアサービスを引き続きサポートします。

詳細については、『SD-Access Wireless Design and Deployment Guide』を参照してください。

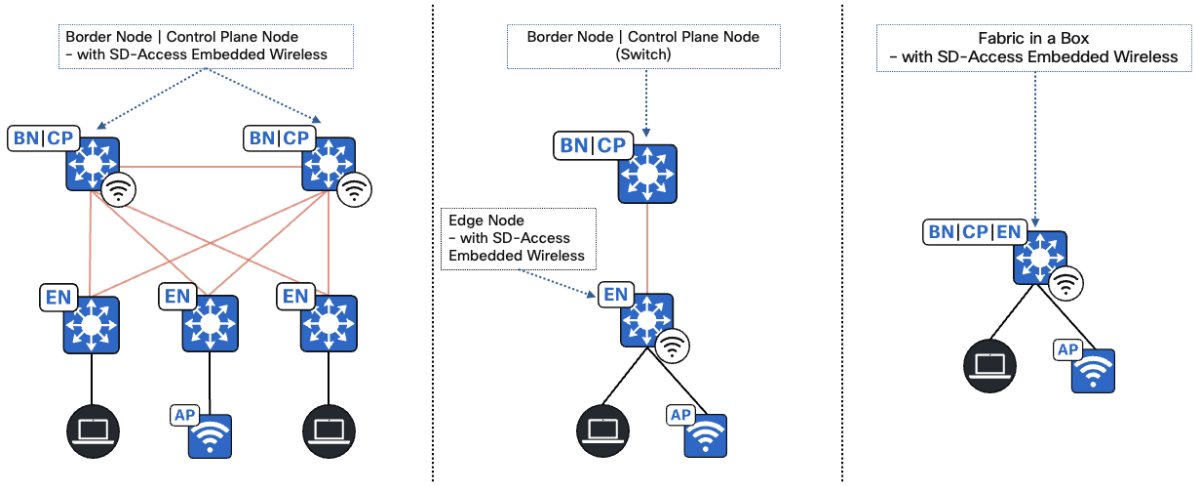
SD-Access 組み込み型ワイヤレス

分散したブランチや小規模なキャンパスでは、Cisco Catalyst 9000 シリーズ スイッチのソフトウェアパッケージとして利用できる Cisco Catalyst 9800 組み込み型ワイヤレスコントローラを使用することで、ハードウェアのワイヤレスコントローラなしでその機能を実現できます。

Cisco Catalyst 9800 組み込み型ワイヤレスコントローラは、以下の 3 つのトポロジでの 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。
- ファブリック統合として機能する Cisco Catalyst 9000 シリーズ スイッチ。

図 2.　　SD-Access でサポートされるトポロジ



トランジット

トランジットは、複数のファブリックサイトを接続したり、ファブリックサイトをデータセンターやインターネットなどの非ファブリックドメインにリンクしたりすることができます。トランジットは、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ドメイン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 Cisco SD-Access コンストラクトです。トランジットネットワークには以下の 2 つのタイプがあります。

- IP ベースのトランジット

  IP ベースのトランジットでは、ファブリックの VXLAN ヘッダーが削除され、元のネイティブ IP パケットが残ります。ネイティブ IP 形式になると、パケットはファブリックサイト間で従来のルーティングおよびスイッチングプロトコルを使用して転送されます。SD-Access トランジットとは異なり、IP ベースのトランジットは、アップストリームのピアデバイスへの VRF-Lite 接続でプロビジョニングされます。IP ベースのトランジットは通常、データセンター、 WAN、またはインターネットに接続します。VRF 認識ピアを使用して共有サービスに接続する場合は、IP ベースのトランジットを使用します。

- SD-Access トランジット：

  SD-SD-Access トランジットは VXLAN カプセル化を使用し、アップストリームのピアへの VRF-Lite 接続に依存しません。IP ベースのトランジットと同様に、パケットはファブリックサイト間で従来のルーティングおよびスイッチングプロトコルを使用して転送されます。ただし、IP ベースのトランジットとは異なり、SD-Access トランジットは、SD-WAN や DMVPN のように WAN/MAN ネットワーク上で動作するオーバーレイです。

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、『Cisco SD-Access』を参照してください。

IP ベースのトランジットと SD-Access トランジットの比較

IP ベースのトランジット

- 既存の IP インフラストラクチャを活用

  従来の IP ベースのルーティングプロトコルを使用してファブリックサイトを接続します。

- VRF の再マッピングが必要

  サイト間で VRF とセキュリティグループタグ（SGT）を再マッピングする必要があり、複雑さが増します。

- 既存の IP ネットワークをサポート

  このアプローチは、確立された IP ベースの WAN インフラストラクチャをすでに持っている場合に理想的です。

- 柔軟性の提供

  ルーティングプロトコルとトラフィック エンジニアリングのオプションに関して、より高い柔軟性を提供します。

SD-Access トランジット：

- ネイティブ SD-Access ファブリック

  サイト間の通信に LISP、VXLAN、CTS を使用します。

- SGT を保持

  ファブリックサイト間で SGT を維持し、セキュリティとポリシー適用を強化します。

- 集中管理

  ドメイン全体にわたるコントロールプレーンノードを使用して、管理を簡素化します。

- 専用インフラストラクチャが必要

  SD-Access トランジット コントロール プレーンのために追加のインフラストラクチャが必要です。

Cisco Catalyst 9000 シリーズ スイッチ

Cisco Catalyst 9000 シリーズ スイッチは、より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 switches』を参照してください。

Cisco Catalyst ワイヤレスコントローラと AP

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと 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

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、互換性マトリックスを参照してください。

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

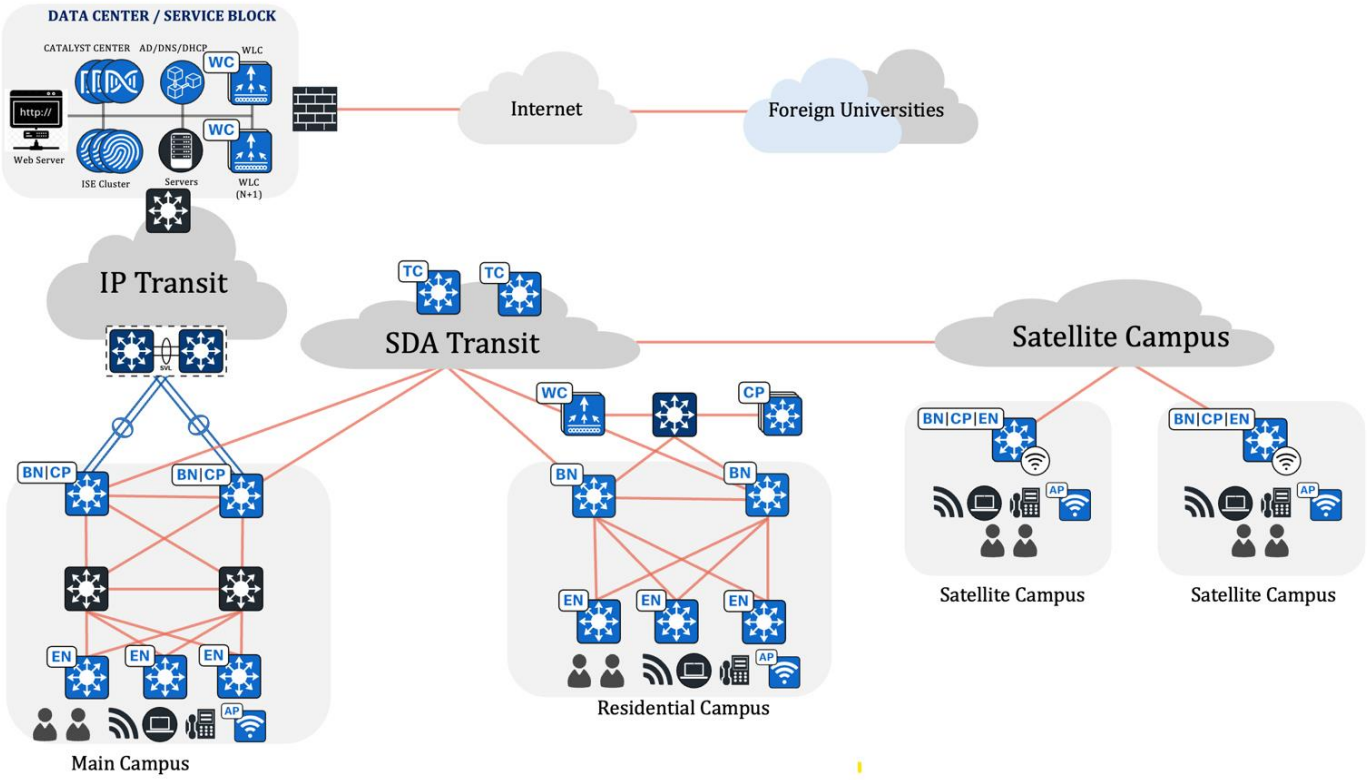
大学への展開および設計ソリューション

プロファイル展開

このセクションでは、教育分野向けの設計ガイダンスを提供します。シンプルで、安全で、柔軟なネットワークを構築するための要件と Cisco SD-Access の活用法を紹介しています。ここでは、大学向けの標準的な展開オプションに合わせたトポロジ、ユースケース、およびソリューションについて、特定のテーマと要件にも触れながら説明します。

ソリューショントポロジ

図 3.　　大規模な大学展開向けトポロジソリューション



大学のビジネス成果と課題

特定のビジネス成果に合わせて調整された最新のネットワーク インフラストラクチャは、大学が競争力を維持し、イノベーションを推進し、学生、教職員、およびより広範な学術コミュニティの増大する期待に応えることを可能にします。大学は、教育上および運用上の目標を達成するために、高度で信頼性の高いネットワーク インフラストラクチャへの依存度を高めています。大学が直面する課題と潜在的な成果には、以下のようなものがあります。

- セキュリティ
- コンプライアンス
- 使用可能
- 財務
- エクスペリエンス

セキュリティ

大学は、堅牢なセキュリティプロトコルの実装、定期的なリスク評価の実施、関連する業界規制や基準の順守によって、セキュリティ対策の強化、リスクの軽減、および規制コンプライアンスの確保が可能です。学生、教職員、研究者に対するアクセシビリティと、機密データの保護とのバランスを取らなければならない大学の環境は、その開放的で動的な性質から、特にセキュリティの脅威に対して脆弱です。適切に管理されない場合、悪意のある攻撃者に脆弱性を悪用され、多大な金銭的および評判上の損害につながる可能性があります。

使用可能

大学にとって、ネットワークの稼働時間を維持することは、シームレスな運用とビジネス目標の達成に不可欠です。大学のネットワークはミッションクリティカルな性質を持つため、主要な目標は 100% の可用性を目指すことです。ファイブナイン（99.999%）の可用性を達成することは、この目標を大幅に進めることになりますが、年間わずか 5 分 16 秒のダウンタイムしか許容されません。中断のないサービスは、学生や研究者の生産性を確保し、機関全体の成功をサポートするために不可欠です。自動化、監視、負荷分散、およびフェールオーバーメカニズムを活用することで、大学は 99.999% の可用性ベンチマークを達成するか、それを上回ることさえ可能です。

財務

最新のネットワーク インフラストラクチャを導入することで、リソースの利用を最適化し、コストを削減し、革新的な収益創出の機会を生み出すことができ、大学に大きな財務上の利点がもたらされます。たとえば、複数のキャンパスにわたる展開を自動化することで、経費を合理化し、効率を向上させることができます。最新のネットワークソリューションを導入することで、大学は運用の有効性とサービス提供を強化し、ますますデジタル化され競争が激化する教育環境において自らを位置づけることで、長期的な財務的成長を目指すことができます。

エクスペリエンス

重要なビジネス機能を可能にする最新技術を活用することで、ユーザーおよびアプリケーション体験を最適化します。セキュリティ、コンプライアンス、可用性は不可欠ですが、Quality of Service（QoS）が一貫しない、または遅いネットワークは、ユーザーの満足度と生産性に悪影響を与える可能性があります。遅延が致命的になりうる時間制約のある環境では、低遅延と信頼性の高い QoS を確保することが、機関の要求に効果的に応えるために不可欠です。

大学ビジネスの成果に対するソリューション

このセクションでは、大学ネットワーク展開で定義されたビジネス成果を達成するのに役立つソリューションの概要を説明します。

セキュリティ上の課題

教育分野は、その複雑で絶えず変化する環境から、多大なセキュリティの課題に直面しています。これには、攻撃対象の拡大、データ侵害、組織内に潜む脅威、規制コンプライアンス要件、高度なサイバー攻撃、リモートワークのセキュリティ確保が含まれます。SD-Access フレームワークは、以下の堅牢なツールと機能スイートでこれらの問題に効果的に対処します。

- マクロセグメンテーション
- マイクロセグメンテーション
- ポリシー適用モデル
- グループベースポリシーの分析
- AI エンドポイント分析
- ゼロトラストソリューションによるエンドポイントセキュリティ
- ゲストユーザーの分離

マクロセグメンテーション

大学のネットワークでは、推奨されるセグメンテーション戦略を実装するために、学生、監視デバイス、ゲストなどのネットワークエンドポイントに異なる VRF インスタンスを割り当てます。SD-Access は、Catalyst Center を使用してネットワーク内で設定できる、個別の VRF にエンドポイントをマクロセグメント化する機能を提供します。

VN の実装例は以下のとおりです。

- インフラストラクチャ VN

  この VN は、AP、従来の拡張ノード、およびポリシー拡張ノード専用で、接続性を確保します。これはグローバル ルーティング テーブルにマッピングされます。

- 学生 VN

  この VN は通常の学生アクセスに使用され、すべての内部ユーザーに対して安全で分離された接続性を確保します。

- ゲスト VN

  この VN は、訪問者やゲストにインターネットアクセスを提供し、内部ネットワークにアクセスできないようにします。

- 監視 VN

  この VN は、ネットワーク監視および管理デバイス専用で、通常のユーザーのトラフィックから隔離されることを保証します。

- 常駐 VN

  この VN は居住ユーザーに使用され、すべての内部ユーザーに対して安全で分離された接続性を確保します。

SD-Access ネットワークに VN を実装することで、大学は多様な種類のトラフィックを効果的にセグメント化して保護し、ネットワーク全体のパフォーマンスとセキュリティを向上させることができます。

マイクロセグメンテーション

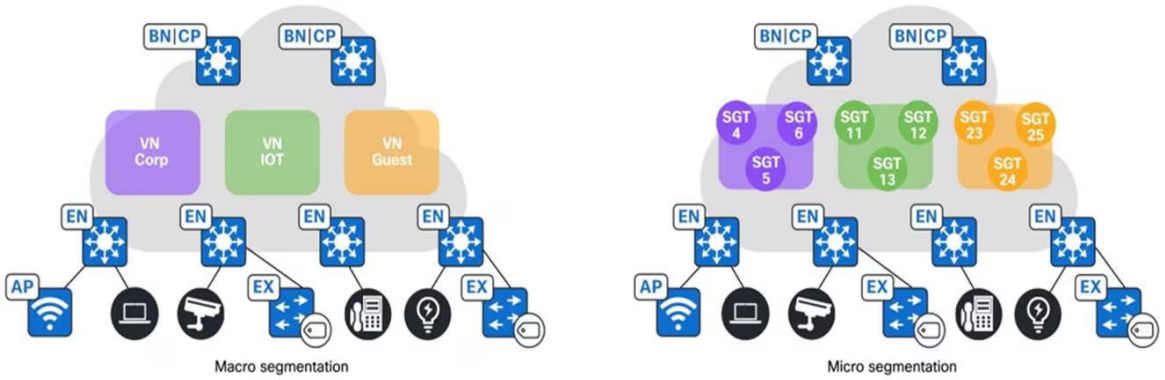
マイクロセグメンテーションは、セキュリティグループを使用してトラフィックを分類し、ポリシーを適用することで、ネットワークアクセス制御のプロビジョニングと管理を簡素化し、SD-Access VN 内でのより精度の高いセキュリティを可能にします。

通常、単一の VN 内では、部門に基づいて従業員をグループ化したり、プリンタなどのデバイスを異なるセキュリティグループに配置したりすることで、さらにセグメント化する必要があります。従来、これは IP ACL によって適用される異なるサブネットにグループを配置することで行われていました。しかし、Cisco SD-Access は、ユーザーとエンドポイントを中心としたアプローチで同じサブネットを使用できる、マイクロセグメンテーションによる柔軟性を提供します。動的承認は、認証情報に基づいて異なる SGT を割り当て、セキュリティ グループ アクセス制御リスト（SGACL）がこれらの SGT ベースのルールを適用します。

ユーザーがネットワークに接続すると、802.1X や MAC 認証バイパス（MAB）などの方法を使用して認証されます。その後、ネットワーク承認は、アイデンティティ、LDAP グループメンバーシップ、場所、アクセスの種類などの情報を使用して、ユーザーのトラフィックを分類します。この分類情報は、動的にダウンロードされたポリシーを適用するネットワークデバイスに伝達され、トラフィックを許可するか拒否するかを決定します。

詳細は、『Software-Defined Access Macro Segmentation Deployment Guide』を参照してください。

図 4.　　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を示す例



ポリシー適用モデル

Cisco TrustSec は、組織全体でセキュリティポリシーを適用しながら、ネットワークアクセスのプロビジョニングと管理を簡素化するために設計されたセキュリティソリューションです。従来の IP ベースの方法ではなく、ロールとポリシーに基づいて包括的なセグメンテーションとアクセス制御を可能にし、有線およびワイヤレス環境全体でセキュリティと運用の効率を向上させます。

コンピューティングとネットワークセキュリティの適用において、ポリシー適用モデルは通常、以下の 2 つのカテゴリに分類されます。

- 拒否リストモデル（デフォルト許可 IP）

  デフォルトのアクションは IP トラフィックを許可し、制限はセキュリティ グループ アクセス制御リスト（SGACL）を使用して明示的に設定する必要があります。このモデルは、ネットワーク内のトラフィックフローの理解が不完全な場合に使用します。比較的簡単に実装できます。

- 許可リストモデル（デフォルト拒否 IP）

  デフォルトのアクションは IP トラフィックを拒否するため、必要なトラフィックは SGACL を使用して明示的に許可する必要があります。このモデルは、ネットワーク内のトラフィックフローをよく理解している顧客

向けに使用します。アクティブ化時にすべてのトラフィックをブロックする可能性があるため、コントロールプレーンのトラフィックに関する詳細な調査が必要です。

詳細については、『Cisco ISE TrustSec Allow-List Model (Default Deny IP) with SD-Access』を参照してください。

グループベースポリシーの分析

サイバー攻撃に関する世間の注目度の高いニュースにより、大学は境界セキュリティ以外にも、内部ネットワークセグメンテーションを実装するようになっています。しかし、ネットワーク内のユーザーやデバイスの振る舞いに対する可視性の欠如が、効果的なセグメンテーションポリシーの作成を困難にしています。ビジネスは、この複雑な状況を乗り切るためのソリューションを求めています。

シスコは、グループベースのポリシー分析（GBPA）を提供することで、これらの課題に対処する Catalyst Center 上のソリューションを提供しています。GBPA は、以下のような機能を提供します。

- グループ間の相互作用の発見と可視化

  GBPA は、ネットワーク トラフィック フローを分析し、部門や機能など、異なるネットワークグループがどのように通信しているかを特定します。

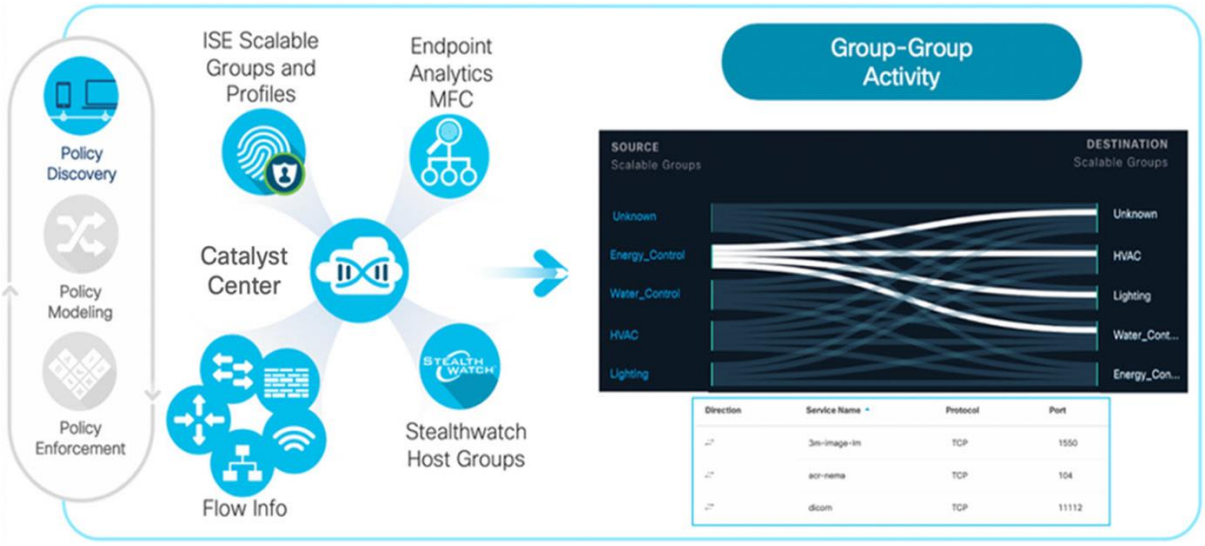
- 通信パターンの特定

  GBPA は、異なるグループによって使用される特定のポートとプロトコルを特定し、ネットワークの振る舞いに関する精度の高いインサイトを提供します。

- ポリシー作成の簡素化

  GBPA は、発見された情報に基づいて、グループ間の通信を制御するための効果的なセキュリティポリシーを構築するプロセスを合理化します。

図 5.　　ネットワークの全体像を作成するための GBPA 情報ソース



GBPA は、以下のソースからの情報を活用してネットワークの全体像を作成します。

- Cisco ISE

  ISE と統合することで、GBPA はスケーラブルグループ（SGT）およびプロファイルグループとして定義されたネットワークグループについて学習します。

- エンドポイント分析

  エンドポイント分析は、機械学習と多要素分類を活用して、ネットワーク上の識別不能なデバイスを減らし、セグメンテーションのためにより正確なプロファイルグループを提供します。

- Cisco Secure Network Analytics（オプション）

  Cisco Secure Network Analytics（SNA）との統合により、GBPA は SNA によって識別されるホストグループについて学習し、ネットワークの可視性をさらに強化できます。

- NetFlow データの統合

  GBPA は、ネットワークデバイスからの NetFlow データを取り込み、グループ情報にコンテキストを提供します。この結合データは、グラフやテーブルを通じて可視化され、管理者がグループ間の相互作用に基づくネットワークの振る舞いを明確に理解できるようにします。

GBPA は、ネットワークの検出、可視化、およびセキュリティポリシー要件を分析するためのツールをネットワーク管理者に提供します。この包括的なアプローチは、今日の動的な脅威の状況に対応するための、より効果的で的を絞ったセキュリティポリシーの作成につながります。

AI エンドポイント分析

次世代のエンドポイント可視化ソリューションである Cisco AI エンドポイント分析は、ネットワークと IT エコシステムからより深いインサイトを提供し、すべてのエンドポイント可視化して検索可能にします。次の技術を使用して、企業内の不明なエンドポイントの数を検出および削減します。

- ディープ パケット インスペクション（DPI）

  IT、ビルオートメーション、ヘルスケアのエンドポイントについて、アプリケーションや通信プロトコルをスキャンして理解することで、より深いエンドポイントコンテキストを収集します。

- 機械学習（ML）

  共通の属性を持つエンドポイントを直感的にグループ化し、IT 管理者によるラベル付けを支援します。これらの固有のラベルは、新しいラベルに基づいて未知のエンドポイントを削減およびグループ化するのに役立つ提案として、匿名で他の組織と共有されます。

- シスコおよびサードパーティ製品との統合

  エンドポイントをプロファイリングするための、追加のネットワークおよび非ネットワークコンテキストを提供します。

つまり、Cisco AI エンドポイント分析は、多くの顧客がセキュリティポリシーを実装する際に直面する重要な課題、すなわちエンドポイントの可視性不足を高い精度で克服します。この機能は、Catalyst Center リリース 2.1.2.x 以降で新しいアプリケーションとして利用できます。Cisco Catalyst Advantage 以上のサブスクリプションレベルを持つ顧客は、Cisco AI エンドポイント分析にアクセスできます。この技術入門書では、Cisco AI エンドポイント分析と、それがシスコの顧客にもたらすメリットについて解説します。

詳細については、以下のリソースを参照してください。

- Cisco SD-Access AI Endpoint Analytics
- Cisco Catalyst Center Guide – AI Endpoint Analytics

ゼロトラストソリューションによるエンドポイントセキュリティ

SD-Access におけるゼロトラストソリューションによるエンドポイントセキュリティは、SD-Access 環境内のノートパソコン、スマートフォン、IoT デバイスなどのエンドポイントを保護することを目的とした、包括的なネットワーク セキュリティ アプローチです。ゼロトラストの原則を適用することは、たとえネットワーク境界内にいるデバイスやユーザーであっても、自動的には信頼されないことを意味します。ネットワークリソースへのアクセスを許可する前に、各デバイスは検証および認証されます。

Cisco SD-Access のゼロトラスト セキュリティ ソリューションは、以下の機能を使用してネットワーク アクセス ポリシーを自動化します。

- エンドポイントの可視性

  エンドポイントを識別してグループ化できます。トラフィックフロー分析を通じて相互作用をマッピングし、アクセスポリシーを定義します。

- 信頼の監視

  エンドポイントの動作を継続的に監視し、脆弱性をスキャンし、持続的なアクセスの信頼性を検証し、不正なエンドポイントや侵害されたエンドポイントを隔離します。

- ネットワーク セグメンテーション

  グループベースのアクセスポリシーを適用し、多層的なセグメンテーションを通じてネットワークを保護できます。

Cisco SD-Access では、IEEE 802.1x メカニズムを使用して、AP やスイッチなどのネットワークデバイスの安全なオンボーディングを実行することができます。これにより、すべてのエッジノードアクセスポートでクローズド認証を維持することで、不正なデバイスの接続からネットワークを保護します。クローズド認証を使用して安全にオンボーディングされたスイッチは、サプリカントベース拡張ノード（SBEN）と呼ばれます。

SBEN は、エッジノードへのアップリンクで EAP-TLS 認証を使用するサプリカントを持つように、Catalyst Center によってポリシー拡張ノードとしてプロビジョニングされます。EAP-TLS 証明書は、Catalyst Center の認証局（CA）を使用して Catalyst Center によってプロビジョニングされます。オンボーディングが成功した後は、ポートへのアクセスは認証ステータスのみに基づいて行われます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが復旧すると、dot1x 認証を経て、Cisco SD-Access ネットワークへのアクセスが回復します。

AP の安全なオンボーディングは、クローズド認証ポート上の AP を認証し、PnP ワークフローのために DHCP/DNS および Catalyst Center への限定的なアクセスを許可します。Catalyst Center 上の PnP ワークフローは拡張され、AP が Cisco ISE で認証するために使用する dot1x サプリカントを AP 上で有効にします。

SBEN の詳細については、『Cisco Catalyst Center User Guide』の「Steps to Configure Supplicant-Based Extended Nodes」セクションを参照してください。

ゲストユーザーの分離

ゲストワイヤレスの分離は、ゲストユーザーが大学のネットワークから完全に分離された状態を保ちながら、インターネットへのアクセスを制御して提供する重要なセキュリティ機能です。この要件に対応するため、SD-Access はマルチサイト リモート ボーダー（MSRB）ソリューションを導入しています。

このソリューションにより、複数の分散サイトにまたがる VN からのトラフィックを、アンカーサイトと呼ばれる中央の場所に集約できます。サイトごとに個別のサブネットを設定する代わりに、アンカーサイトはゲスト VN に対して単一の共有サブネットを活用します。一元化および合理化されたサブネット構造を実装することで、VN アンカーは大学環境における一貫した安全なトラフィックセグメンテーションを維持しながら、複数の場所でのゲストサービスの展開を簡素化します。

外部ゲートウェイによるセキュリティの強化

SD-Access では、特定のファブリックサイト内の VN における各サブネットについて、すべてのエッジノード上にデフォルトゲートウェイが存在します。リモートサブネット宛てのトラフィックは、エッジノード上のデフォルトゲートウェイによって処理され、適切な接続先にルーティングされます。

多くのネットワークでは、デフォルトゲートウェイはローカルのエッジノードではなく、外部のファイアウォール上にある必要があります。ファイアウォールのトラフィック検査は、そのようなネットワークにおける一般的なセキュリティおよびコンプライアンス要件です。ファブリック機能の外部でゲートウェイを有効にすることで、デフォルトゲートウェイはエッジノード上にプロビジョニングされません。代わりに、ファイアウォールなどの

外部デバイス上にプロビジョニングすることができ、トラフィックが接続先に到達する前に検査することができます。

シームレスでセキュアなキャンパス ネットワーク アクセス

個人用モバイルデバイスの使用が増加し、クラウドベースのサービスへの依存が高まるにつれて、大学によるテクノロジーとネットワークアクセスの扱い方も変化しました。学生と教職員は、場所を問わず、自身のデバイスから大学のリソースに中断なくアクセスできることを期待するようになりました。

この進化は、ネットワークセキュリティ、アクセス制御、リソース管理を変化させました。機関所有のデバイスと、制限されたネットワークに依存する従来のアプローチは、時代遅れになりつつあります。これらの変化に対応するため、大学はデータセキュリティと規制コンプライアンスを維持しながら柔軟性を提供するために、Bring Your Own Device（BYOD; 個人所有デバイス持ち込み）戦略を導入しています。

BYOD と SD-Access を統合することで、大学はセキュアで適応性の高いネットワーク環境を構築できます。SD-Access は、アクセス制御を適用し、ネットワーク セグメンテーションを通じて機密データを保護し、デバイスのオンボーディングを自動化することで、IT チームの負担を軽減します。このアプローチは、セキュリティを強化し、運用の効率を改善し、より接続された、テクノロジー主導の学習体験を促進します。

コンプライアンス規制

コンプライアンス規制とは、機関が特定の領域または管轄区域内で合法的に運営するために従わなければならない規則と基準です。高度なテクノロジーは、規制プロセスの自動化、データセキュリティの改善、およびリアルタイムの監視とレポートを可能にすることで、規制要件を効果的に満たすことを支援します。

業界規制を遵守し続けることは、複雑なタスクになる可能性があります。Cisco SD-Access は、このプロセスを簡素化できるいくつかの機能を提供します。

- RBAC
- 監査ログ
- 設定コンプライアンス
- 設定のばらつき

ロールベース アクセス コントロール

Catalyst Center におけるロールベース アクセス コントロール（RBAC）は、組織内の個々のユーザーのロールに基づいて、機能や操作へのアクセスを制御する方法を提供します。RBAC は、最小権限の原則を適用するのに役立ち、ユーザーがそのロールに必要なリソースのみにアクセスできるようにします。Catalyst Center は、ローカルまたは外部の RADIUS/TACACS データベースのいずれかに基づいてユーザーに権限を割り当てることができる柔軟性をサポートしています。ユーザーにロールを割り当て、Catalyst Center 内の特定のアプリケーションへのアクセス権を付与することもできます。

監査ログ

監査ログは、Catalyst Center アプリケーション内で発生したイベントまたはアクションの記録です。これらのログには通常、アクションを実行したユーザー、実行されたアクション、発生時期などの詳細が含まれます。監査ログは、管理者がネットワーク インフラストラクチャに加えられた変更を追跡し、潜在的なセキュリティ侵害を特定し、ユーザーが適切な手順に従っていることを確認するのに役立つため、セキュリティおよびコンプライアンスの目的で重要です。監査ログを確認することで、管理者は Catalyst Center アプリケーション内のアクティビティに関するインサイトを得て、必要に応じて適切なアクションを実行できます。

詳細については、「View audit logs」を参照してください。

設定コンプライアンス

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性があるネットワークのインテント逸脱やアウトオブバンドの変更を特定するのに役立ちます。ネットワーク管理者は、Catalyst Center でソフトウェアイメージ、PSIRT、ネットワークプロファイルなど、コンプライアンスのさまざまな側面でコンプライアンス要件を満たさないデバイスを簡単に特定できます。

以下のスケジュールオプションを使用して、コンプライアンスチェックを自動化したり、オンデマンドで実行したりできます。

- コンプライアンスチェックの自動化

  Catalyst Center 内のデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリや SWIM などさまざまなサービスからのトラップと通知をリッスンして、データを評価します。

- 手動コンプライアンスチェック

  Catalyst Center でコンプライアンスを手動でトリガーできます。

- コンプライアンスチェックのスケジュール設定

  スケジュールされたコンプライアンスジョブは毎日午後 11:00 に実行され、過去 7 日間コンプライアンスチェックが実行されなかったデバイスのコンプライアンスチェックをトリガーします。

Catalyst Center は現在、以下のタイプのコンプライアンスチェックをサポートしています。

- ネットワークデバイス上の実行中の設定が、デバイスに対する Catalyst Center の起動設定ビューと異なる場合に、コンプライアンスエラーをフラグ付けします。
- ネットワークデバイス上でゴールデンイメージが実行されていない場合に、ソフトウェア イメージ コンプライアンスをフラグ付けします。
- SD-Access ファブリックワークフローによって展開された設定が改ざんされ、帯域外の PSIRT コンプライアンスに違反した場合に、ネットワーク内に存在する脆弱性をネットワーク管理者に通知するために、ファブリック コンプライアンス エラーにフラグを立てます。
- デバイスが Catalyst Center で特定のサイトに要求されたインテント通りの構成で実行されていない場合に、ネットワーク コンプライアンス アラートを出します。

詳細については、『Compliance User Guide』を参照してください。

運用の効率化

運用の効率性は、生産性、コスト管理、学生や職員に提供されるサービスの質に直接影響するため、大学にとって非常に重要です。ワークフローを最適化し、デジタル変換を活用することで、大学は教員の出力を最大化し、管理プロセスを強化し、評判と各機関の価値を強化できます。SD-Access は、以下のような業務効率の重要な側面に対応します。

- HA
- システムのレジリエンス
- レポート
- 効率的な障害対応

ハイ アベイラビリティ

高可用性高可用性（HA）は、ハードウェアの故障やソフトウェアの不具合といった技術的な問題が発生した場合でも、システムやアプリケーションが最小限の中断で稼働し、ユーザーがアクセスできる状態を維持するための重要なコンポーネントです。コンポーネントの HA を達成するための概要には、以下が含まれます。

- ディザスタ リカバリ

- レジリエンスのあるネットワークアーキテクチャ
- フォールバックセグメント

ディザスタリカバリ

大学では、管理、制御、データ運用を含む重要なシステムの中断に対する許容度が低くなっています。Catalyst Center は、運用を保護するために、クラスター内とクラスター間の両方でレジリエンスを確保します。そのディザスタリカバリのフレームワークは、プライマリサイト、リカバリサイト、および監視サイトの 3 つの主要なコンポーネントで構成されています。プライマリサイトとリカバリサイトは、常にアクティブまたはスタンバイのいずれかのロールで運用されます。アクティブサイトでネットワークが監視され、アクティブサイトで更新されたデータおよびサービスの最新のレプリカがスタンバイサイトで維持されます。アクティブサイトに障害が発生した場合、Catalyst Center は自動的にフェールオーバーを開始し、スタンバイサイトをアクティブロール移行させて、継続性を確保します。

詳細については、「Implement Disaster Recovery」を参照してください。

レジリエンスのあるネットワークアーキテクチャ

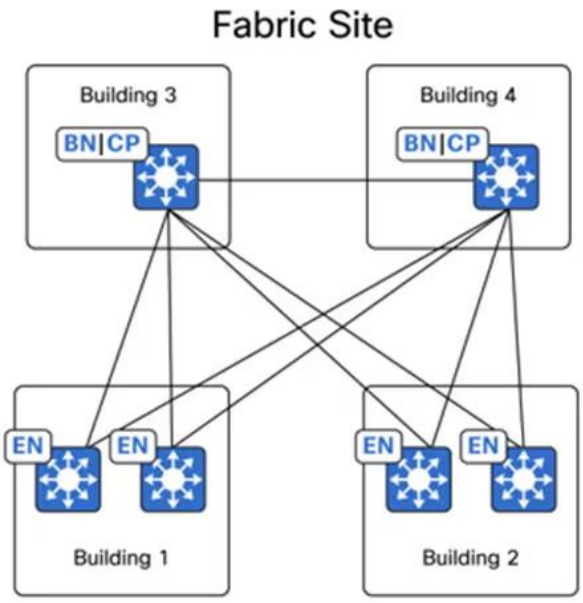
Cisco SD-Access の復元力の高いネットワークアーキテクチャは、高い可用性と信頼性を確保するように設計されており、中断が発生した場合でも重要な大学サービスが稼働し続けることを可能にします。

- 仮想スイッチングシステム（VSS）と同様に、StackWise Virtual（SVL）は、2 つの物理スイッチを制御および管理プレーンレベルで 1 つの論理スイッチに結合することで、レイヤ 2 の運用を簡素化します。これにより、スパニングツリープロトコルや最初のホップ冗長構成が不要になり、ネットワーク管理が合理化されます。
- レイヤ 3 ルーテッドアクセスを実装することで、レイヤ 2 とレイヤ 3 の境界はディストリビューション レイヤからアクセスレイヤに移行します。この移行により、レイヤ 2 隣接関係と冗長性を管理するためにディストリビューション レイヤとコラプストコアレイヤに依存することが減ります。

大学のネットワークでは、スタッキングや StackWise Virtual といった従来のレジリエンス技術が、地域ハブやキャンパス本部を建物レベルの障害から保護するための戦略によって補完されます。これらの対策により、重要な学術および管理アプリケーションのために、データセンターへの中断のない接続が確保されます。

図 6 に示されているように、Cisco SD-Access は、ファブリックボーダーが複数の物理サイトにまたがりながら、それらを単一のファブリックサイト内にシームレスに統合できる柔軟な展開モデルを提供します。

図 6.　建物 1 ー 4 は同じファブリックサイトに属し、同じ場所に配置されたボーダーノードとコントロールプレーンノードは異なる建物に配置されています。



Cisco SD-Access は、これらのボーダーノードの展開に優先順位を割り当てる柔軟性を提供します。これにより、特定のボーダーノードを優先したり、トラフィックのアクティブボーダーとして排他的に使用したりすることが可能になります。建物に障害が発生した場合でも、代替の建物にあるボーダーノードが、エッジノードからのすべてのトラフィックをシームレスに引き継ぐことができます。

フォールバックセグメント

Cisco SD-Access では、クリティカル VLAN 機能がサポートされており、WAN の障害などでエンドポイントが ISE サーバーへの接続を失った場合でも、最低限のネットワーク接続を維持できます。

すでにオンボーディング済みの有線クライアント（ワイヤレスクライアントは除外）の場合、ISE ポリシーサービスノード（PSN）への接続が失われると、認証パスの障害がデータプレーンに影響を与えるのを防ぐために、システムは定期的な再認証を一時停止します。まだオンボーディングされていないクライアントについては、ISE への接続が失われた場合にクリティカル VLAN 機能が特定の VLAN にそれらを割り当て、限定的なネットワークアクセスを提供します。

これらのクリティカル VLAN は、ISE が存在しない環境でポリシーを適用するためにマイクロセグメンテーションを利用できます。ただし、これを実現するには、クリティカル VLAN のエニーキャストゲートウェイ（VLAN-SGT マッピングなど）のプロビジョニング中にセキュリティグループを割り当て、適切なポリシーマトリックスがスイッチにダウンロードされるように設定する必要があります。

つまり、SD-Access のクリティカル VLAN は、デバイスが適切に認証できない場合でも、ネットワークから完全に切断されるのではなく、修復や障害対応のために限定的なアクセスが与えられることを保証します。

システムのレジリエンス

システムのレジリエンシを確保するには、ネットワーク インフラストラクチャの重要なコンポーネントに高可用性ソリューションと冗長性ソリューションを実装することが重要です。これらのコンポーネントでこれを達成するための概要は以下のとおりです。

- Catalyst Center HA
- ISE HA

- ワイヤレス LAN コントローラの冗長性

Catalyst Center HA

Catalyst Center HA は、ダウンタイムを最小限に抑え、ネットワークのレジリエンスを高めるように設計された機能です。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、重要なサービスが利用可能な状態を維持することでこれを実現します。Catalyst Center の HA は、通常、冗長なハードウェアとソフトウェア設定を展開して、シームレスなフェールオーバーと継続的な運用性を提供します。これにより、組織は予期せぬ事態が発生した場合でも、ネットワークの安定性と信頼性を維持できます。

詳細については、『Cisco Catalyst Center High Availability Guide』を参照してください。

ISE HA

Cisco ISE は、スタンドアロンと分散型という 2 つの主要な設定で展開できます。

- スタンドアロン展開

  スタンドアロン展開では、単一の ISE ノードが管理、ポリシーサービス、監視など、すべての必要な機能を提供します。このは設定、単一ノードでワークロードを処理でき、冗長性が必須の要件ではない小規模ネットワークに適しています。

- 分散型の展開

  分散型展開では、ISE ノードが複数の物理マシンまたは仮想マシンに分散され、拡張性、冗長性、高可用性を提供します。この設定は、拡張性と冗長性が重要となる大規模ネットワークに適しています。

各展開オプションにはそれぞれの利点があり、拡張性、冗長性、およびパフォーマンスに関するネットワークの特定の要件に基づいて選択されます。フェールオーバーをサポートし、パフォーマンスを改善するために、複数の Cisco ISE ノードを分散方式でセットアップできます。

詳細については、『Cisco Identity Services Engine Installation Guide』の「Distributed Deployment Scenarios」を参照してください。

シスコ ワイヤレス コントローラの冗長性

シスコ ワイヤレス コントローラの冗長性は、ワイヤレス ネットワーク サービスを継続的に維持するために不可欠です。HA ペアの設定では、2 台のワイヤレスコントローラがペアとして構成されます。1 台のワイヤレスコントローラがプライマリ（アクティブ）コントローラとして機能し、すべてのワイヤレスクライアントとトラフィックを管理します。もう 1 台はセカンダリ（スタンバイ）コントローラとして機能します。セカンダリコントローラは、プライマリコントローラの設定および状態との同期を維持します。

プライマリコントローラに問題が発生した場合、セカンダリコントローラがシームレスに引き継ぎ、ワイヤレスサービスの中断を防ぎます。この冗長性機能は、ワイヤレスコントローラのハードウェアまたはソフトウェアに障害が発生した場合にフェールオーバー機能を提供することで、ワイヤレスネットワークの信頼性を大幅に向上させます。その結果、ユーザーは中断を最小限に抑え、ワイヤレスネットワークへの接続を維持できます。

詳細については、『Cisco Catalyst 9800 Series Wireless Controllers HA SSO Deployment Guide』を参照してください。

レポート

Catalyst Center のレポート機能は、ネットワーク運用の効率性に関する実用的なインサイトを取得するための包括的なツール群を提供します。この機能により、柔軟なスケジューリングと設定オプションを備えた複数の形式でデータを生成できるため、特定の運用ニーズに合わせてカスタマイズが可能です。

レポート機能は、以下のようなさまざまなユースケースをサポートしています。

- キャパシティプランニング

ネットワーク内のデバイス使用率を把握します。

- パターン変更分析

  クライアント、デバイス、バンド、アプリケーションなどの使用パターンにおける変化を追跡します。

- 運用レポート

  アップグレード完了やプロビジョニング障害などのネットワーク運用に関するレポートを確認できます。

- ネットワークの正常性評価

  詳細なレポートによってネットワークの全体的な正常性を判断できます。

Catalyst Center のレポート機能を活用することで、ネットワークの運用効率を大幅に向上させ、円滑に動作する高パフォーマンスのネットワーク環境を実現できます。

詳細については、『Cisco Catalyst Center Platform User Guide』を参照してください。

効率的な障害対応

効率的なトラブルシューティングは、大学の IT インフラストラクチャ内で途切れることのない運用を維持するための重要な側面です。Catalyst Center は、これらの要件を効果的に満たすために調整された高度なデバッグ機能を提供します。これらのツールにより、IT 管理者は Catalyst Center 関連の問題を迅速に特定、診断、および解決でき、大学のネットワークシステムの最適なパフォーマンスを確保できます。これらのツールには、以下のような障害対応に役立ちます。

検証ツール：
Catalyst Center バージョン 2.3.5.x 以前は、アップグレードの準備状況を評価するために監査およびアップグレード準備状況分析（AURA）ツールが使用されていました。バージョン 2.3.5.x での制限付きシェルの実装に伴い、ほとんどの AURA アップグレードチェックが Catalyst Center に統合されました。検証ツールは、Catalyst Center アプライアンスのハードウェアと接続された外部システムの両方を評価し、大学のネットワークに影響を与える前に潜在的な問題を特定します。

詳細については、以下のリンクを参照してください。

- Validate Cisco DNA Center Upgrade Readiness
- 検証ツールの使用

Catalyst Center 検証ツールは、大学のネットワーク管理者にとって非常に役立つサポートを提供します。これらのツールは、能動的なメンテナンス、効率的な障害対応、ネットワークの安定性の向上を可能にし、大学の IT サービスの運用効率を大幅に向上させます。

財務効率

運用コストの削減と収益の増加は、財務の持続可能性を目指す大学にとっての主要な優先事項です。大規模で複数サイトにわたるネットワークの展開と監視を自動化することで、大学は運用コストを大幅に削減し、管理プロセスを合理化し、効率的な IT 運用を維持できます。このアプローチにより、複雑なキャンパスネットワークを最小限の人的介入で管理でき、全体的な効率を向上させ、リソースのより適切な割り当てを可能にします。大学が財務効率を達成するために採用している戦略には、以下のようなものがあります。

- 自動化およびモニタリング
- IP アドレス管理（IPAM）の統合
- IT サービス管理（ITSM）の統合
- SD-Access の拡張

自動化およびモニタリング

自動化とモニタリングは、現代の IT インフラストラクチャ管理に不可欠な要素です。自動化には、ソフトウェアの展開、設定の管理、システムのプロビジョニング、ワークフローのオーケストレーションなどのタスクを含めることができます。反復的で時間のかかるタスクを自動化することで、組織は効率を向上させ、エラーを減らし、人間がより戦略的な活動に集中できるようにリソースを解放できます。一方で、監視では、IT システム、ネットワーク、アプリケーション、およびサービスのパフォーマンスと正常性を継続的に観察および分析します。以下は、これらのコンポーネントに対して上記の戦略を実装する方法の概要です。

- LAN の自動化
- プラグアンドプレイと返品許可（RMA）
- ソフトウェアイメージの管理
- インテリジェントキャプチャ
- アシュアランスと可視性

LAN の自動化

Catalyst Center の LAN 自動化は、ネットワークデバイスの設定とプロビジョニングを自動化することで、ネットワーク インフラストラクチャの展開と管理を簡素化するために設計された機能です。この自動化により、手動での設定に伴う複雑さとエラーの可能性が減少し、より効率的で信頼性の高いネットワーク運用が実現します。

シスコの LAN 自動化には、主に以下のような利点があります。

- ゼロタッチプロビジョニング

  ネットワークデバイスが動的に検出およびオンボーディングされ、工場出荷時の状態からネットワークに完全に統合されるまでが自動化されます。

- エンドツーエンドのトポロジ

  新しいネットワークシステムとその物理接続を動的に検出するように、検出プロセスをモデル化してプログラミングできます。それらの新しいシステムをレイヤ 3 IP アドレッシングおよびルーティングプロトコルを使用して自動化し、エンドツーエンドのルーティングトポロジを動的に構築できます。

- レジリエンス

  LAN 自動化には、転送トポロジと冗長性を最適化するシステムとネットワークの設定パラメータが統合されています。LAN 自動化でシステムレベルの冗長性を確保し、ベストプラクティスを自動的に適用することで、計画的または計画外のネットワーク停止時もクラス最高水準の復元力が提供されます。

- セキュリティ

  シスコ推奨のネットワークアクセスおよびインフラストラクチャの保護パラメータが自動的に適用され、最初の導入時点からセキュリティが提供されます。

- コンプライアンス

  LAN 自動化によって人的ミスや設定の誤りが排除され、IT リソースの浪費につながるルールや設定の不整合を減らすことができます。新しいシステムのオンボーディング時、LAN 自動化で Catalyst Center のグローバルに管理されるパラメータを自動化することにより、ネットワーク インフラストラクチャ全体でコンプライアンスが確保されます。

詳細については、『Cisco Catalyst Center SD-Access LAN Automation Deployment Guide』を参照してください。

プラグアンドプレイと返品許可（RMA）

Catalyst Center は、Cisco Catalyst スイッチ、ルータ、ワイヤレス AP の展開を簡素化するプラグアンドプレイ（PnP）機能を備えています。PnP を使用すると、ネットワーク管理者は手動での設定を必要とせずに、新しいデバイスをネットワークに簡単にオンボーディングできます。PnP 機能を備えたデバイスは、Catalyst Center などの PnP サーバーから必要なソフトウェアイメージと設定を自動的にダウンロードできるため、展開プロセスがより迅速かつ効率的になります。

Catalyst Center は、返品許可（RMA）プロセスをサポートしています。ハードウェアの故障や交換が発生した場合、RMA 機能により、管理者は故障したデバイスの返品と交換を簡単に管理できます。これには、RMA リクエストの生成、RMA のステータス追跡、および一元的なインターフェイスによる交換プロセスの管理が含まれます。全体として、Catalyst Center の PnP および RMA 機能は、デバイスの展開と交換プロセスを合理化し、複雑さを軽減し、ネットワーク管理の効率を向上させるのに役立ちます。

詳細については、『Network Device Onboarding for Cisco Catalyst Center Deployment Guide』を参照してください。

ソフトウェアイメージの管理

Catalyst Center のソフトウェアイメージ管理（SWIM）機能は、ネットワーク内の Catalyst スイッチ、ルータ、およびワイヤレスデバイスにわたるソフトウェアイメージの管理プロセスを簡素化し、自動化します。ブランチやキャンパスで Catalyst 9000 シリーズ スイッチのアップグレードを自動化したいネットワーク管理者は、Catalyst Center の SWIM ソリューションを使用できます。

Catalyst Center は、ネットワーク内のデバイスについて、すべての固有のソフトウェアイメージをイメージタイプとバージョンに従って保存します。これにより、ソフトウェアイメージの表示、インポート、削除、およびネットワークデバイスへのプッシュが可能になります。ソフトウェアの配布とアクティベーションを分離することで、メンテナンスウィンドウ内のダウンタイムを最小限に抑え、ソフトウェアアップグレードを最適化できます。全体として、SWIM は Catalyst デバイス全体のソフトウェアイメージ管理を簡素化および自動化することで、運用の効率性を高め、ダウンタイムを削減し、ネットワークのセキュリティとコンプライアンスを確保するのに役立ちます。

詳細については、『SWIM Deployment Guide』を参照してください。

インテリジェントキャプチャ

Catalyst Center のインテリジェントキャプチャ（iCAP）は、ネットワークの障害対応とパフォーマンスの監視を強化するために設計された強力な機能です。高度な分析と機械学習を活用して、ネットワークトラフィックとクライアントの振る舞いに関する深いインサイトを提供します。iCap は、Catalyst Center と AP 間の直接通信リンクをサポートしており、各 AP が Catalyst Center と直接通信できます。このチャネルを使用することで、Catalyst Center はパケットキャプチャ（PCAP）データ、AP とクライアントの統計、およびスペクトルデータを受信できます。gRPC を介した AP から Catalyst Center への直接リンクにより、iCap はワイヤレスコントローラからは利用できない AP からのデータにアクセスすることを可能にします。

詳細については、『Cisco Intelligent Capture Deployment Guide』を参照してください。

アシュアランスと可視性

Catalyst Center は、ネットワークのデバイスとサービスを自動化することでネットワークを管理するだけでなく、ネットワークのアシュアランスと分析の機能を提供します。Catalyst Center は、ネットワークデバイス、Cisco ISE、ユーザー/エンドポイント、アプリケーション、およびネットワーク全体のその他の統合からテレメトリを収集します。Catalyst Center のネットワーク分析は、さまざまなソースからのデータを関連付けて、管理者やオペレータが以下の包括的なネットワークインサイトを提供できるようにします。

- デバイス 360 およびクライアント 360

さまざまな時間およびさまざまなアプリケーションからの、デバイスまたはクライアントの接続を表示する機能を提供します（トポロジ、スループット、および遅延に関する情報を含む）。

- ネットワークタイムトラベル

  過去にさかのぼり、ネットワーク問題の原因を確認する機能を提供します。

- アプリケーション体験

  コア ビジネスにとって重要なアプリケーションをユーザー単位でこれまでにないレベルにまで可視化し、それらのパフォーマンスを制御します。

- ネットワーク分析

  ネットワークで発見された問題に対する是正措置を推奨します。これらの措置には、ガイド付きの修復が含まれる場合があり、エンジンによってネットワーク管理者が実行すべき手順が指定されます。

詳細については、『Cisco Catalyst Assurance』を参照してください。

IP アドレス管理の統合

Catalyst Center における IP アドレス管理（IPAM）の統合は、ネットワーク内での IP アドレス管理プロセスを合理化します。この統合により、IP アドレスの割り当て、追跡、管理を自動化し、簡素化するための一元的なプラットフォームが提供されます。SD-Access 展開では、IPAM の統合により、既存の IP アドレス範囲への Catalyst Center のアクセスが提供されます。Catalyst Center で新しい IP アドレスプールを設定すると、IPAM サーバーが自動的に更新されるため、IP アドレスの管理タスクが軽減されます。

Catalyst Center には、サードパーティの統合モジュールが 2 つ含まれており、1 つは IPAM プロバイダーの Infoblox 用、もう 1 つは BlueCat 用です。他の IPAM プロバイダーも、Catalyst Center IPAM プロバイダー仕様を満たす IPAM プロバイダー REST API サービスを提供することで、Catalyst Center で使用するように設定できます。

詳細は、「Configure an IP Address Manager」を参照してください。

IT サービス管理の統合

IT サービス管理（ITSM）とは、ビジネスのニーズを満たす高品質な IT サービスの実装と管理を指します。ServiceNow は、組織が IT サービスを自動化し、合理化するのに役立つアプリケーションスイートを提供する、人気の高い ITSM プラットフォームです。

Catalyst Center と ServiceNow の統合により、以下の機能がサポートされます。

- ITSM のインシデント、イベント、変更および問題管理プロセスへの Catalyst Center の統合。
- ITSM の承認および事前承認チェーンへの Catalyst Center の統合。
- 正式な変更およびメンテナンス ウィンドウ スケジュールと Catalyst Center の統合。

統合の範囲は、主に、アシュアランスおよびメンテナンスの問題についてと、コンプライアンス、セキュリティ、またはその他の操作のトリガーのためにソフトウェアイメージを更新する必要があるイベントについて、ネットワークをチェックすることです。これらの問題に関する詳細は、ITSM（ServiceNow）システムまたは REST エンドポイントに公開されます。

詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

SD-Access の拡張

SD-Access の拡張は、組織が SD-Access ファブリックの範囲を拡大することを可能にする重要な機能であり、より広範な環境とデバイス全体で一貫したポリシー適用、セキュリティの強化、管理の簡素化、およびネットワークパフォーマンスの向上を実現します。

拡張ノードは、レイヤ 2 モードで SD-Access に接続し、IoT エンドポイントの接続を容易にしますが、ファブリックテクノロジーはサポートしていません。Catalyst Center を使用すると、拡張ノードは PnP 方式を通じて工場出荷時の設定からオンボーディングでき、拡張ネットワークでセキュリティ制御を有効にし、拡張ノードに接続されたエンドポイントに対してファブリックポリシーを適用できます。

SD-Access の拡張を実装するには、以下の 3 つのタイプで利用可能な拡張ノードを展開します。

- 拡張ノード（EX）

  拡張ノードは、Cisco SD-Access ネットワーク内のファブリックエッジノードに接続するレイヤ 2 スイッチです。完全な SD-Access 機能をサポートしていない IoT エンドポイントおよびその他のデバイスの接続を提供します。拡張ノードは通常、Catalyst Center などの集中型コントローラを介して管理および設定されます。LISP、VXLAN、SGACL の適用などの高度なネットワーク機能は、ファブリックエッジに依存します。

- ポリシー拡張ノード（PEN）

  ポリシー拡張ノードは、追加機能を提供する特定のタイプの拡張ノードです。802.1X/MAB 認証を実行し、エンドポイントに VLAN と SGT を動的に割り当て、SGACL を適用できます。このタイプのノードは、標準規格の拡張ノードと比較してより精度の高いポリシー制御を提供し、より柔軟なネットワーク セグメンテーションとセキュリティを可能にします。

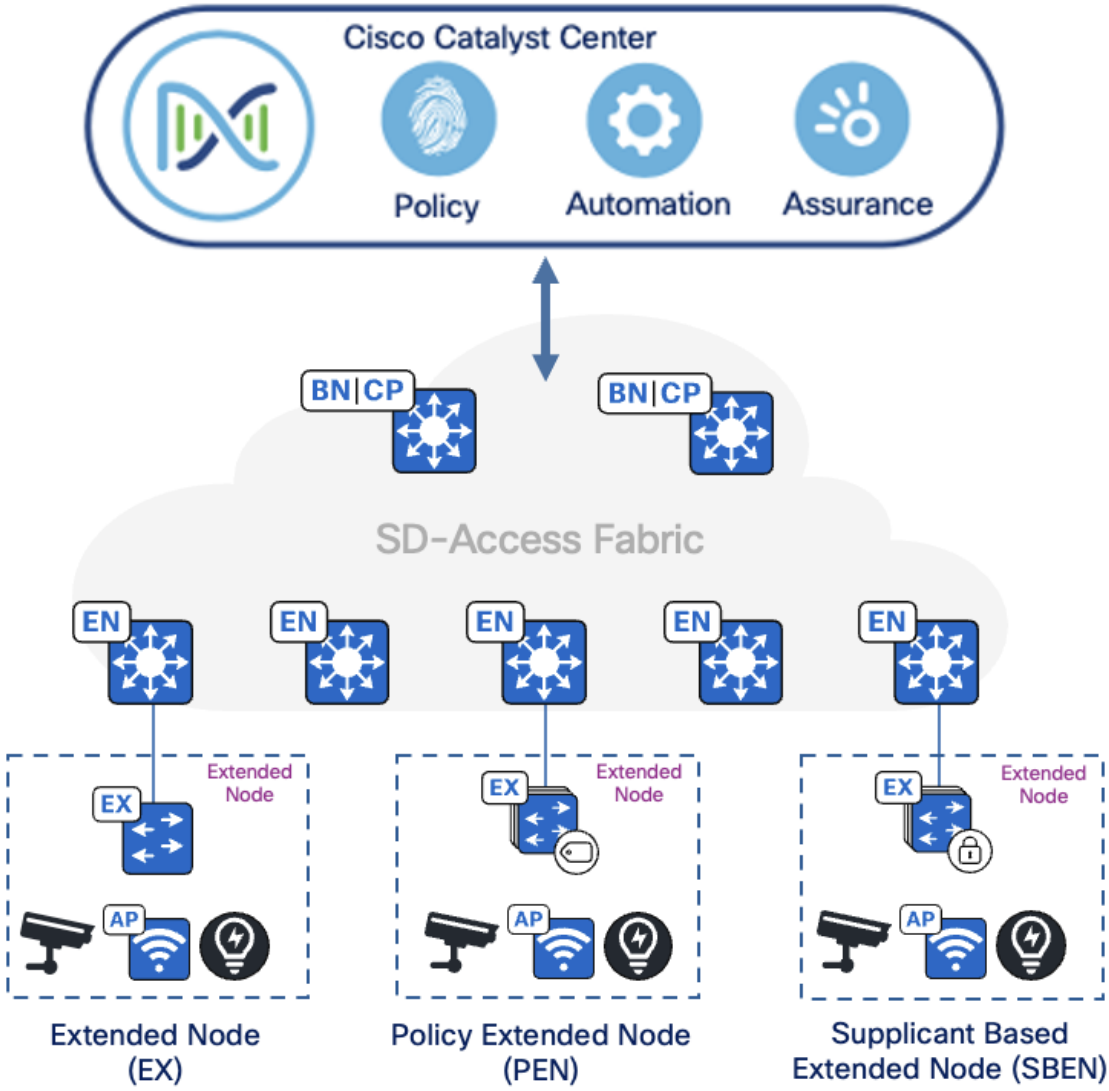
- サプリカントベースの拡張ノード（SBEN）

  サプリカントベースの拡張ノードは、より厳密なオンボーディングプロセスが必要な拡張ノードです。IEEE 802.1X サプリカントの設定が必要であり、SD-Access ネットワークに許可される前に完全な認証および承認プロセスを完了する必要があります。このアプローチにより、許可されたデバイスのみがネットワークにアクセスできるようにすることで、セキュリティが強化されます。SBEN は、セキュリティ要件が厳しい環境でよく使用されます。

キーポイント：

- 拡張ノードは、SD-Access に直接参加できないエンドポイントに接続を提供します。
- ポリシー拡張ノードは、強化されたポリシー適用機能を提供します。
- サプリカントベースの拡張ノードは、802.1X 認証による厳格なセキュリティ対策を実装します。

図 7.　拡張ノード（EX）、ポリシー拡張ノード（PEN）、サプリカントベースの拡張ノード（SBEN）を使用する企業



詳細については、以下を参照してください。

- Cisco SD-Access Solution Design Guide
- Connected Communities Infrastructure - General Solution Design Guide

体験の向上

最新のテクノロジーを戦略的に活用してユーザーおよび顧客体験を向上させるには、特にパフォーマンスがビジネス運営や顧客満足度に直接影響する環境において、Quality of Service（QoS）を優先し、アプリケーションの可視性を活用し、ビデオストリーミングを実装する必要があります。今日の競争の激しい状況では、QoS を優先することは単なる選択肢ではなく、卓越したユーザーおよび顧客体験を提供するために不可欠です。

これらの分野を強化する戦略の概要は以下のとおりです。

- QoS
- アプリケーションの可視性
- サイト間のビデオストリーミング

QoS

QoS とは、選択された種類のネットワークトラフィックに対して、サービスを優先または差別化するネットワークの機能を指します。QoS を設定することで、エンタープライズグレードの音声品質を確保したり、ビデオに高い Quality of Experience（QoE）を提供したりするなど、ビジネス目標を満たしながらネットワークリソースが効率的に利用することができます。Catalyst Center は、アプリケーションポリシーを通じてネットワーク内の QoS 設定を容易にします。

これらのポリシーには、以下のようなコアパラメータが含まれます。

- アプリケーションセット

  類似したネットワークトラフィック要件を持つアプリケーションのグループです。各アプリケーションセットは、トラフィックの優先度を決定するビジネス関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）に分類されます。各グループの QoS パラメータは、Cisco Validated Design（CVD）に従って定義され、特定のビジネス目標に合わせて調整できます。

- サイトの範囲

  アプリケーションポリシーが適用される範囲を定義します。たとえば、有線ポリシーは指定されたサイト範囲内のすべての有線デバイスに適用され、ワイヤレスポリシーは定義されたスコープ内の特定のサービスセット識別子（SSID）を使用するデバイスに適用されます。

アプリケーションの可視性

アプリケーションの可視性は、ネットワーク管理者がネットワーク上でどのアプリケーションが実行されているかを確認し、パフォーマンスを監視し、ネットワークリソースがどのように利用されているかを把握できるようにする機能です。これは、最適なネットワークパフォーマンスを維持し、セキュリティを確保し、ユーザー体験を向上させるために不可欠です。

Catalyst Center は、ネットワークを通過するアプリケーションを管理し、インサイトを得ることを可能にします。これには、組み込みアプリケーションやカスタムアプリケーションの識別、およびネットワークトラフィックの分類が含まれます。アプリケーション可視性サービスは、Catalyst Center 内でアプリケーションスタックとしてホストされているため、特定のデバイスでコントローラベースのアプリケーション認識（CBAR）機能を使用して、数千のネットワークと自社製のアプリケーションおよびネットワークトラフィックを分類することができます。

アプリケーションの可視性は、ディープ パケット インスペクション（DPI）、フロー分析、アプリケーション認識技術の組み合わせによって達成され、ネットワークのアクティビティとアプリケーションのパフォーマンスに対する包括的なビューを提供します。CBAR を実装することで、組織は重要なアプリケーションが最適に動作することを保証し、全体的な生産性とユーザーの満足度を向上させることができます。

以下のパッケージをインストールできます。

- アプリケーションポリシー

  キャンパスやブランチ内の LAN、WAN、およびワイヤレスで QoS ポリシーを自動化できます。

- アプリケーションレジストリ

  アプリケーションとアプリケーションセットを表示、管理、および作成できます。

- アプリケーション可視性サービス

  Network-Based Application Recognition（NBAR）および CBAR の技術を使用してアプリケーションを分類できます。

サイト間のビデオストリーミング

大学では、ライブ講義、セミナー、ワークショップといった教育セッションを、複数のキャンパスや学部をまたいで定期的に実施する必要があります。これらのセッションには通常、講義、デモンストレーション、およびインタラクティブな質疑応答のためのライブビデオ配信が含まれます。ネットワークに過度な負荷をかけることなく、すべてのキャンパスに同時にビデオコンテンツを効率的に配信するために、大学はマルチキャスト技術を利用できます。

マルチキャスト データ ストリームは、地域のデータセンターや集中管理された学術サーバーなど、さまざまなソースから発信されることがあります。Cisco SD-Access アーキテクチャは、ローカルかグローバルかを問わず、大学ネットワーク内でシームレスなエンドツーエンドのマルチキャスト データ トラフィックが効率的に流れることを可能にします。SD-Access は、ヘッドエンド レプリケーションとネイティブマルチキャストの両モードをサポートしており、SD-Access ファブリックの内外でマルチキャスト ランデブー ポイント（RP）を柔軟に指定できます。

SD-Access は、マルチキャストトラフィックを転送するために 2 つのトランスポート方法をサポートしています。1 つはヘッドエンド レプリケーションと呼ばれるオーバーレイを使用し、もう 1 つはネイティブマルチキャストと呼ばれるアンダーレイを使用します。

- ヘッドエンド レプリケーション

  ヘッドエンド レプリケーション（または入力レプリケーション）は、マルチキャスト送信元がファブリックオーバーレイ内にある場合はマルチキャスト ファーストホップ ルータ（FHR）によって行われ、送信元がファブリックサイト外にある場合はボーダーノードによって行われます。

- ネイティブマルチキャスト

  ネイティブマルチキャストにより、入力ファブリックノードでユニキャスト レプリケーションを実行する必要がなくなります。代わりに、中間ノードを含むアンダーレイネットワーク全体がレプリケーションを処理します。ネイティブマルチキャストをサポートするには、最初のホップルータ（FHR）、最後のホップルータ（LHR）、およびすべての中間ネットワーク インフラストラクチャ コンポーネントがマルチキャスト対応である必要があります。

SD-Access フ レームワーク内にマルチキャスト技術を統合することで、大学は大規模なトレーニングセッションを効果的に配信でき、すべてのキャンパスでより良いコミュニケーションと学習を促進できます。

学術的モビリティの簡素化

今日のアカウンディカルの世界では、学生、教職員、研究者にとってグローバルな連携が不可欠です。大学は学際的な研究、パートナーシップ、国際プロジェクトにますます注力しており、シームレスなコミュニケーションとリソース共有が極めて重要になっています。しかし、異なる機関で Wi-Fi にアクセスするには、一時的なゲストアカウント、手動での設定、または IT サポートが必要になることが多く、不便さとセキュリティリスクにつながります。

Eduroam は、100 ヵ国以上の何千もの機関で、安全で手間のかからないワイヤレスアクセスを提供することで、この問題を解決します。ユーザーは、所属機関の認証情報を使用して即座に接続できるため、個別のログインや複雑な設定が不要になります。これによって途切れることのないインターネットアクセスが確保され、学術および研究活動がサポートされると同時に、グローバルなモビリティが促進されます。大学は、セキュリティの向上、IT ワークロードの削減、および知識共有とイノベーションを促進する接続された学術コミュニティの恩恵を受けることができます。

SD-Access を活用することで、大学は Eduroam を既存のネットワークに効率的に組み込むことができ、キャンパス内でも世界中のどの Eduroam 参加機関でも、学生、職員、教員に一貫した安全なインターネットアクセスを保証できます。

シームレスなサービスの発見

大学、企業、複数キャンパス環境といった大規模なネットワークでは、プリンタ、Apple TV、共有リソースなどのネットワークデバイスやサービスを見つけてアクセスすることが複雑になる場合があります。従来の Bonjour サービス発見は、小規模なローカルネットワーク向けに設計されており、マルチキャスト通信に依存しているため、VLAN やサブネットをまたいで効果的に拡張できません。その結果、ユーザーは自身のネットワークセグメント外にあるサービスを見つけて接続するのに苦労しています。

Wide Area Bonjour は、VLAN、サブネット、さらには地理的に分散した場所を越えてサービスの発見を拡張することで、この課題に対処します。SD-Access やその他のネットワークアーキテクチャと統合することで、効率的なサービスアドバタイズ、強力なセキュリティ、最適なネットワークパフォーマンスを確保しながら、共有リソースへのシームレスなアクセスを可能にします。これにより、ユーザー体験が向上し、最新の大規模ネットワーク環境がサポートされます。

ネットワーク展開のオプション

以下のセクションでは、大学ネットワークの展開オプションについて概説します。

ファブリック サイト リファレンス モデル

大学の SD-Access 展開では、学術ビル、研究センター、寮、管理事務所など、さまざまなキャンパスの場所で異なるサイトテンプレートが使用されます。主要な設計上の課題は、既存のネットワークを評価し、これらのエリアに SD-Access ファブリックサイトをどのように統合するかを決定することです。設計をリファレンスモデルに標準化することで、このプロセスが簡素化されます。

これらのテンプレートは、キャンパスネットワーク設計に構造的なアプローチを提供し、ネットワークサイズ、エンドポイントキャパシティ、アーキテクチャの複雑さなどの要因に基づいてサイトを分類します。このセクションで提供されるガイドラインは一般的な推奨事項であり、必ずしも特定のリファレンスモデルにおけるデバイスの最大規模やパフォーマンス制限を表すものではありません。

サイトのリファレンスモデルには以下があります。

- FIAB サイト

  小規模な大学の建物や専門ラボ向けに設計されており、1,000 未満のエンドポイントと 50 未満の AP をサポートします。ファブリックインアボックスは、スイッチスタッキングまたは StackWise Virtual を介してレジリエンスを提供します。ボーダー、コントロールプレーン、エッジ、ワイヤレス機能は、単一の冗長スイッチング プラットフォーム上に併置されます。

- 小規模サイト

  単一の学術ビルまたは管理事務所に適しており、10,000 未満のエンドポイントと 500 未満の AP をサポートします。ボーダープレーン機能とコントロールプレーン機能は 1 つまたは 2 つのデバイスに併置されますが、必要に応じて高可用性（HA）を備えた個別のワイヤレスコントローラが展開されます。

- 中規模サイト

  複数の配線用ボックスを持つ大学の建物、または小規模な建物のグループ向けに設計されており、50,000 未満のエンドポイントと 2,500 未満の AP をサポートします。ボーダーとコントロールプレーン機能は併置されるか、個別のデバイス上にプロビジョニングされ、専用のワイヤレスコントローラが HA 構成で動作します。

- 大規模サイト

  大規模な大学キャンパスや研究機関向けで、最大 100,000 のエンドポイントと 10,000 の AP をサポートします。ボーダー機能は、コントロールプレーンとは別に冗長デバイスに分散され、複数のワイヤレスコントローラが HA で構成されます。

各ファブリックサイトには、リストされているカテゴリから適切にサイズ設定された、コントロールプレーンノード、エッジノード、ボーダーノード、およびワイヤレスコントローラのサポートセットが含まれます。ISE PSN は、存続可能性の要件を満たすためにサイト全体に分散されます。

注： これらのリファレンスモデルは、有益なガイダンスを提供します。特定のネットワーク要件と制約に基づいて、調整が必要になる場合があります。SD-Access ファブリックの最適な展開のために、ネットワーク設計の専門家にご相談いただくことを推奨します。

ファブリック サイト リファレンス モデルの詳細については、『Cisco SD-Access Solution Design Guide』を参照してください。

FIAB サイトリファレンスモデル

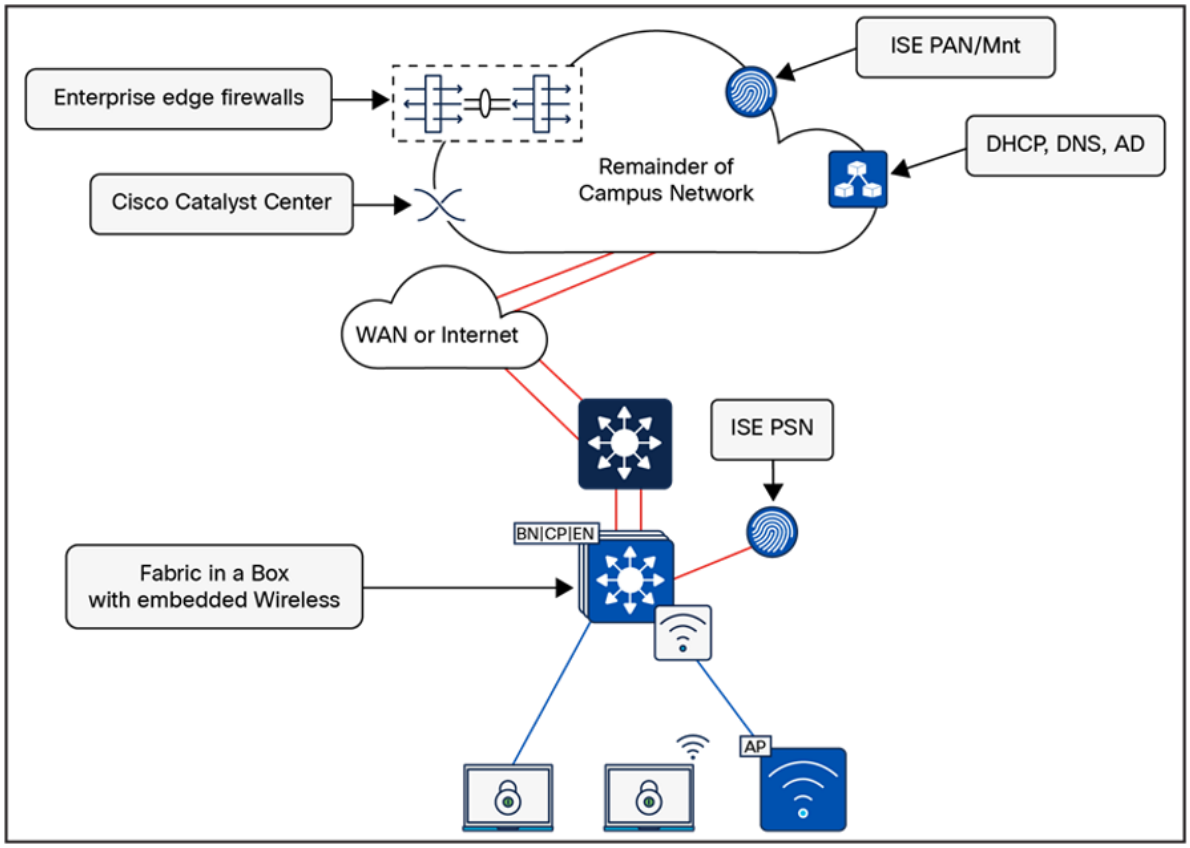
FIAB サイトリファレンスモデルは、小規模な大学キャンパスまたはリモートサイト向けに設計されており、通常は 1,000 未満のエンドポイントをサポートします。この設計の核となるのは、コントロールプレーンノード、ボーダーノード、エッジノードという 3 つのファブリックロールすべてを実行する、スイッチスタックまたは StackWise Virtual です。このような展開では、サイトローカルなワイヤレスコントローラ機能を提供するために、SD-Access 組み込み型ワイヤレスが一般的に使用されます。さらに、WAN またはインターネット回線と遅延に応じて、サイトにはポリシー適用と認証のために ISE PSN が含まれる場合があります。

同様のキャンパスサイトサイズに対する一般的な設計ガイドラインについては、表 1 を参照してください。これらの数値は推奨値であり、この規模の展開で使用される特定のデバイスの正確な制限を表すものではありません。

表 1. FIAB サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	1000
コントロール プレーン ノード数	1
外部ボーダーノード	1
AP、ターゲットの上限	50

図 8. 物理トポロジ：FIAB サイトの設計



FIAB サイトの考慮事項：

- エンドポイント数が少なく、それに伴う影響も少ないため、FIAB 設計では高可用性やサイトの耐障害性は一般的な要件ではありません。他のすべてリファレンスデザインと同様に、DHCP、DNS、ワイヤレスコントローラ、ISE などのサイトローカルサービスはレジリエンスと生存性を高めることができますが、これによって複雑さが増し、サービスブロックのような追加の機器が必要となります。
- この設計における高可用性は、複数の物理スイッチを単一の論理スイッチに結合する StackWise-480 または StackWise Virtual によって実現されます。シャーシベースのスイッチを使用する場合は、デュアルスーパーバイザと電源により冗長性が確保されます。
- ワイヤレスコントローラは、FIAB に直接接続された物理ユニットとして展開することも、組み込み Catalyst 9800 コントローラとして展開することもできます。スイッチスタックまたは冗長スーパーバイザを備えた組み込み Catalyst 9800 を使用すると、AP とクライアント ステートフル スイッチオーバー（SSO）が自動的に提供されます。

小規模サイトリファレンスモデル

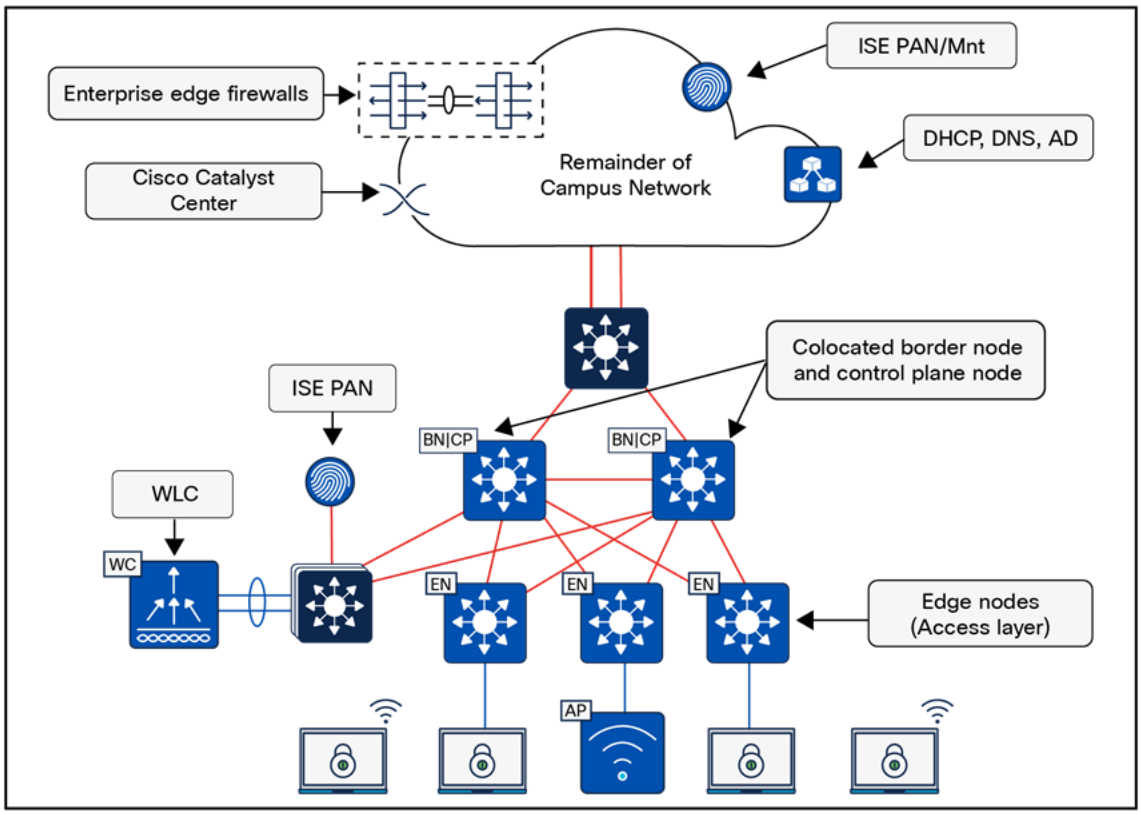
小規模サイトリファレンスモデルは、集中型配線用ボックスを備えた単一の学術ビルまたは管理事務所向けに設計されており、通常、最大 4,000 のエンドポイントと 100 の AP をサポートします。物理ネットワークは通常、コラプストコア/ディストリビューション レイヤとアクセスレイヤからなる 2 層設計です。

同様のサイトサイズに対する一般的な設計ガイドラインについては、表 2 を参照してください。これらの数値は参考値であり、このような設計で使用される特定のデバイスの正確な制限を表すものではありません。

表 2. 小規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	10,000
ファブリックノード、ターゲットの上限	100
コントロール プレーン ノード数	2
外部ボーダーノード	2
AP、ターゲットの上限	500

図 9. 物理トポロジ：小規模サイトのリファレンス設計



小規模サイトの考慮事項

- 小規模な導入では、通常、2 層設計を使用して SD-Access ファブリックが実装されます。小規模サイトでは、ボーダーおよびコントロールプレーンノードの機能をコラプストコアスイッチに併置し、ペアとして展開することで高可用性を実現します。オーバーレイとアンダーレイの両方でレジリエンスを確保し、代替転送パスを提供するために、コラプストコアスイッチはクロスリンクを介して直接接続する必要があります。
- クライアントと AP の数が多い場合、専用のワイヤレスコントローラを使用する必要があります。物理的な接続を介してワイヤレスコントローラへの高可用性リンクを確立するために、サービスブロックが展開されます。ワイヤレスコントローラは、レイヤ 2 ポートチャネルを介してサービスブロックスイッチに接続し、冗長インターフェイスを確保します。スイッチスタックまたは StackWise Virtual で構成されるサービスブロックは、レイヤ 3 ルーテッドリンクを介して両方のコラプストコアスイッチに接続します。DHCP、DNS、およびその他の共有サービスがサイトローカルの場合、サービスブロックは VRF 認識ピアとして展開されることがあります。

中規模サイトリファレンスモデルのガイドライン

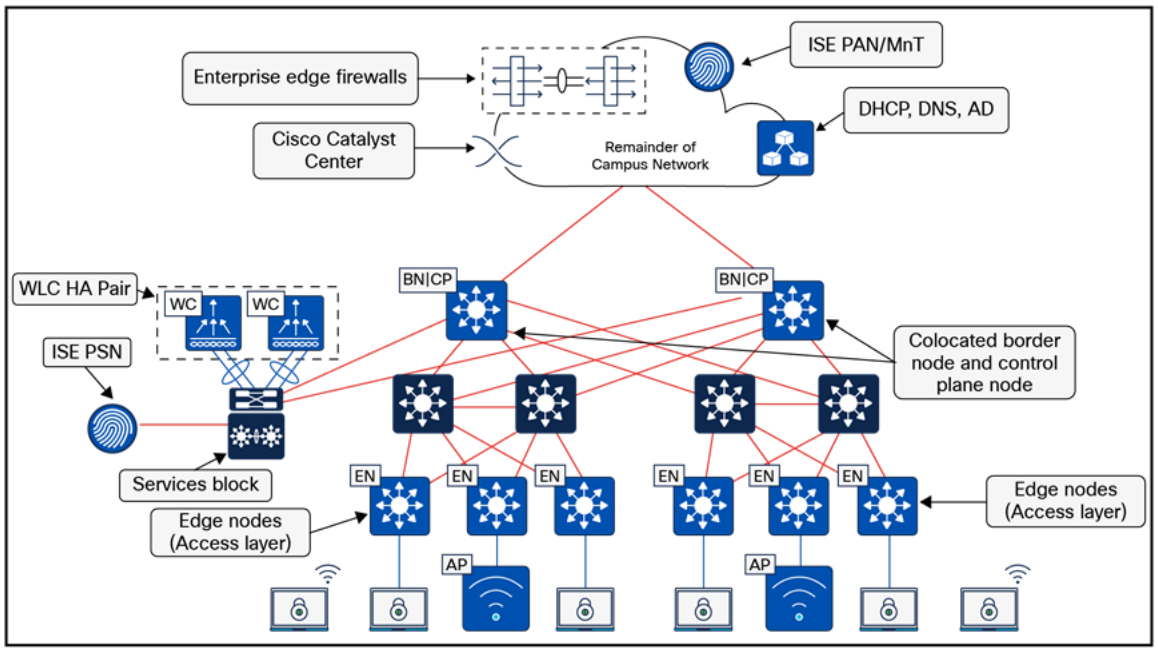
中規模サイトリファレンスモデルは、複数の建物を持つ大学キャンパス、または複数の配線用ボックスを持つ単一の建物向けに設計されており、最大 50,000 のエンドポイントをサポートします。物理ネットワークは通常、コア、ディストリビューション、アクセスレイヤで構成される 3 階層アーキテクチャに従います。ボーダーおよびコントロールプレーンノード機能は、同じ場所に併置することも、別々のデバイスに展開することもできます。

この規模のサイトの一般的な設計ガイドラインについては、表 3 を参照してください。これらの数値は推奨値であり、特定のネットワークデバイスの正確な制限を表すものではありません。最大のエンドポイントキャパシティをサポートするには、大規模な Cisco Catalyst Center アプライアンスが必要です。また場合によっては、超大規模のアプライアンスが必要になる場合があります。

表 3. 中規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	50,000
ファブリックノード、ターゲットの上限	500
コントロールプレーンノード（FEW/SD-Access ワイヤレスの場合は 2 台まで）	2 ー 6
外部ボーダーノード	2
AP、ターゲットの上限	2500

図 10.　　物理トポロジ - 中規模のサイトのリファレンス設計



中規模サイトの考慮事項

- 中規模サイトでは、オーバーレイとアンダーレイのレジリエンシと代替転送パスのために、特定のレイヤ内のすべてのデバイス（アクセスレイヤを除く）を相互にクロスリンクする必要があります。複数のディストリビューション ブロックを相互接続する必要はありませんが、ブロック内のすべてのディストリビューション スイッチに相互接続する必要があります。専用コントロールプレーンノードを使用する場合、通常、さまざまなディストリビューション ブロックの任意のエッジノードに高可用性を確保するためにコアスイッチに接続されます。最適な転送と冗長性のために、両方のコアスイッチに接続する必要があります。インターフェイスと光ファイバが使用可能な場合は、相互にクロスリンクすることもできます。ただし、これは厳密な要件ではありません。
- ワイヤレスユーザーをサポートするには、物理ワイヤレスコントローラを展開する必要があります。高可用性を有効にするには、ワイヤレスコントローラ HA- SSO ペアを、レイヤ 2 ポートチャネルを使用したサービスブロックへの冗長物理接続で展開します。サービスブロックは通常、StackWise Virtual として動作する固定設定スイッチで実装され、レイヤ 3 ルーテッドリンクを介してコアに接続されます。このサービスブロックは、DHCP、DNS、およびその他の共有サービスがサイトローカルの場合、VRF 認識ピアとして機能する可能性があります。

大規模サイトリファレンスモデルのガイドライン

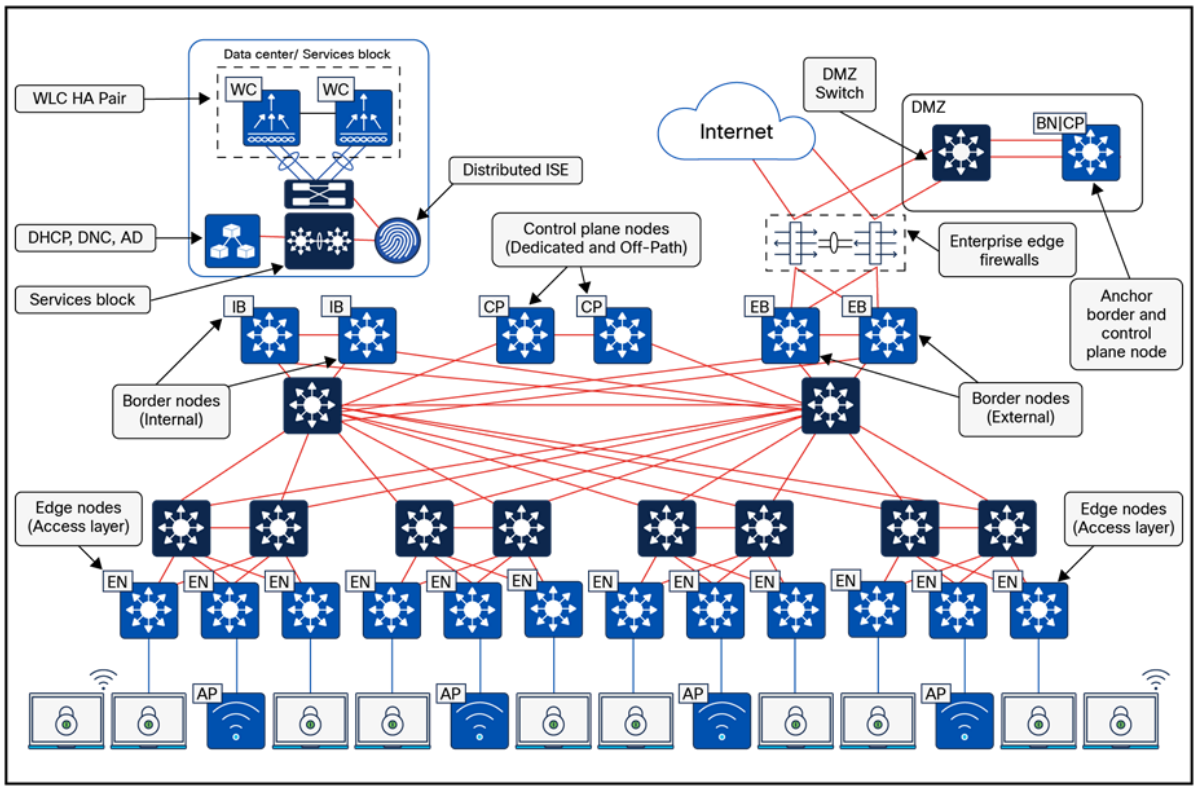
大規模サイトリファレンスモデルは、複数の配線用ボックスを持つ単一の建物、または複数の建物を持つキャンパス向けに設計されています。物理ネットワークは通常、コア、ディストリビューション、アクセスレイヤからなる 3 層アーキテクチャに従い、最大 100,000 のエンドポイントをサポートできます。

この規模のサイトの一般的な設計ガイドラインについては、表 4 を参照してください。これらの数値は参考値であり、特定の設計内の特定のデバイス制限を表すものではありません。最大のエンドポイントキャパシティをサポートするには、少なくとも超大規模の Cisco Catalyst Center アプライアンスが必要であり、場合によっては超大規模の Catalyst Center アプライアンスの 3 ノードクラスターが必要になることもあります。Cisco Catalyst Center のデータシートには、SD-Access ファブリックサイトの実装に使用されるさまざまなネットワーキング インフラストラクチャ デバイスの拡張性に関する詳細が記載されています。

表 4. 大規模サイトのガイドライン（制限は異なる場合があります）

ネットワーク要素	スケール
エンドポイント、ターゲットの上限	100,000
ファブリックノード、ターゲットの上限	1200
コントロール プレーン ノード数	2 ー 6
ボーダーノード（内部として 2 つ、外部として 2 つ） *****非常に例外的な設計シナリオでは、内部ボーダーノードの複数のペアが存在する場合があります。	2 ～ 4*
IP プール、ターゲットの上限	1000
AP、ターゲットの上限	10,000

図 11.　　物理トポロジ：大規模サイトのリファレンス設計



大規模サイトの考慮事項

- Cisco Catalyst Center とプライマリ ISE ポリシー管理ノードは通常、大規模サイトに展開されます。
- コントロールプレーンノードとボーダーノードは、冗長ペアで展開される専用デバイスである必要があります。専用のコントロールプレーンノードは、レジリエンスを確保し、冗長な転送パスを提供するために、各コアスイッチに接続する必要があります。インターフェイスと光ファイバが使用可能な場合は、追加のアンダーレイ転送パスを提供するためにコントロールプレーンノードをクロスリンクすることを推奨しますが、必須ではありません。
- 1 つ以上のワイヤレスコントローラの HA-SSO ペアが、レイヤ 2 ポートチャネルを使用したサービスブロックへの冗長物理接続で展開されます。サービスブロックは通常、オンプレミスのデータセンターネットワークの一部です。
- 専用の内部ボーダーノードは、ファブリックサイトをデータセンターコアに接続するために使用されることがあり、専用の外部ボーダーノードは、サイトを MAN、WAN、およびインターネットに接続するために使用されます。ボーダーノードの数が増えると SD-Access の管理作業とルーティングの複雑さも増すため、ネットワーク設計要件を満たす最小限のボーダーノードを展開することを推奨します。サイトを外部リソースに接続する場合は冗長化された専用ルーティング インフラストラクチャとファイアウォールが使用され、ボーダーノードはこのインフラストラクチャと相互にフルメッシュ接続されます。
- 大規模サイトには、ゲストワイヤレスのためのアンカー ファブリック ボーダーとコントロールプレーンノードが展開される Demilitarized Zone（DMZ; 緩衝地帯）が含まれる場合があります。

分散キャンパス向け SD-Access リファレンスモデル

大学環境において、分散キャンパス向け SD-Access は、複数の独立したファブリックサイトを接続しながら、これらのサイト間でセキュリティポリシーの構成要素（VRF と SGT）を維持するソリューションです。ファブリックサイト間では、ファブリック VXLAN カプセル化とともに、LISP プロトコルを介したコントロール プレーン シグナリングが使用されます。これにより、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

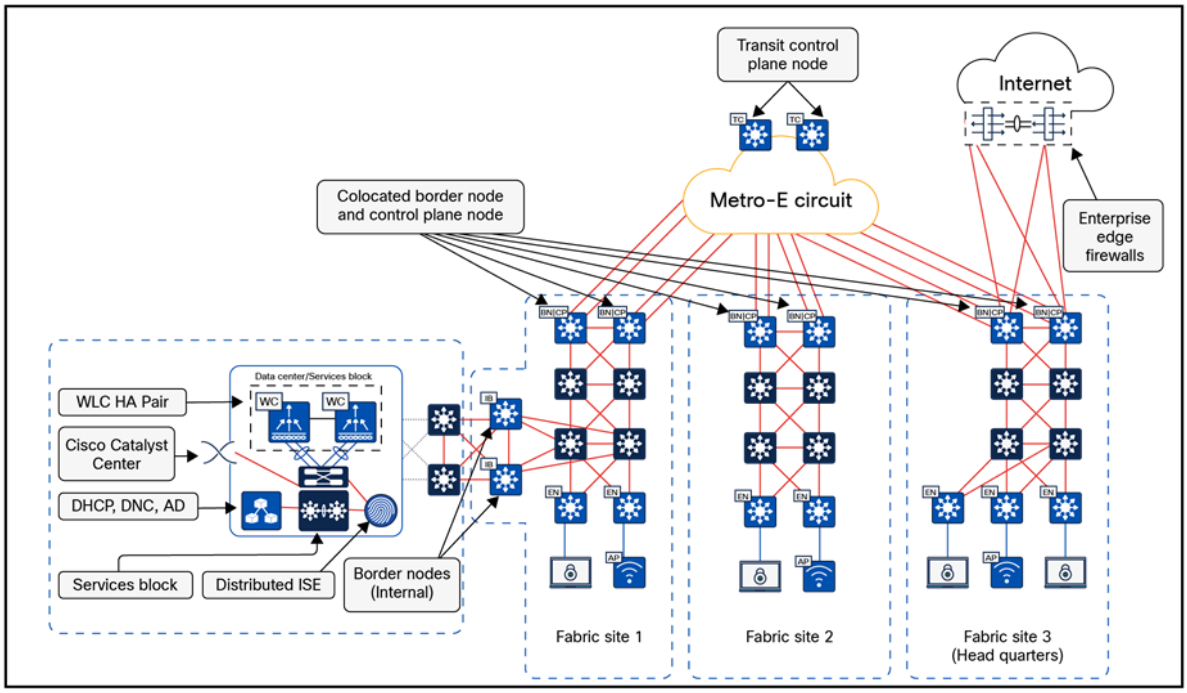
のポリシー構成要素である VRF と SGT のそれぞれが保持されます。その結果、ネットワークはアドレスに依存しない状態を保ち、グループメンバーシップに基づいてエンドツーエンドのポリシーを適用します。

図 12 では、各ファブリックサイトがメトロイーサネット（Metro-E）プライベート回路を介して接続されています。この展開は、同じ地理的エリア内に複数の建物が分散された大規模なエンタープライズキャンパスを表しており、各建物が独立したファブリックサイトとして機能します。この回路に接続されるボーダーノードは外部ボーダーとして設定され、コントロールプレーンノードと併置されます。IGP ピアリングが回路を越えて発生し、デバイスのループバックインターフェース（RLOC）間の IP 到達性を確立します。Metro-E 回路は、ファブリックサイト間の SD-Access トランジットとして機能します。

本部にはダイレクト インターネット アクセスがありますが、ファブリックサイト 1 は共有サービスがホストされているデータセンターに接続しています。ファブリックサイト 1 の内部ボーダーノードがデータセンターのプレフィックスをオーバーレイ空間にインポート（登録）し、各ファブリックサイトの VN がこれらのサービスにアクセスできるようにします。インターネット宛てのトラフィックは、本部に転送されて共通のセキュリティスタックを通過し、インターネットに送信されます。

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 Metro-E ネットワークを介してアクセス可能な別のエリアに展開されますが、直接の転送パスにはありません。

図 12.　　物理トポロジ：分散キャンパス向け SD-Access のリファレンス設計



分散キャンパスに関する考慮事項

- 分散キャンパスソリューションを可能にする核となるコンポーネントは、SD-Access トランジットとトランジット コントロール プレーン ノードです。これらのアーキテクチャ構造は、分散キャンパスの展開でのみ使用されます。SD-Access トランジットは、同じ都市、同じ WAN 上、または大規模なエンタープライズキャンパス内の建物をまたいだファブリックサイト間の物理ネットワーク接続として機能します。

ワイヤレス設計

大学環境で Cisco SD-Access フレームワーク内のワイヤレスソリューションを設計するには、シームレスな運用と管理を確保するために複数のコンポーネントを設定および統合する必要があります。有線ネットワークに SD-Access ファブリックを実装する大学は、ワイヤレスアクセスを組み込むための 2 つのオプションがあります。

- SD-Access ワイヤレス アーキテクチャ
- Cisco Unified Wireless Network ワイヤレスオーバーザトップ（OTT）

SD-Access ワイヤレス アーキテクチャ

ワイヤレス コントロール プレーンを有線のオーバーレイ コントロール プレーンと統合することで、Cisco SD-Access は独自の差別化要因を提供します。Cisco SD-Access ワイヤレスは、ワイヤレスコントローラを介した集中型コントロールプレーンと管理プレーン、および分散型データプレーンを提供し、集中型と分散型のワイヤレス設計の長所を兼ね備えています。

ワイヤレスコントローラはコントロールプレーンノードと統合され、オンボーディング時にエンドポイントを登録し、ローミング時にエンドポイントの位置を更新します。これは、ワイヤレス コントロール プレーンと有線コントロールプレーンの間に相乗作用が発生する最初のインスタンスです。有線とワイヤレスのこの独自の統合は、ネットワークユーザーと、それらをサポートする運用チームに、いくつかの利点をもたらします。

- 簡素化：

  ネットワークは、有線クライアントとワイヤレスクライアントの両方に対して単一のサブネットを持つことができます。

- ポリシーの一貫性：

  有線のポリシーをワイヤレストラフィックに拡張し、両方がエッジノードで適用されます。

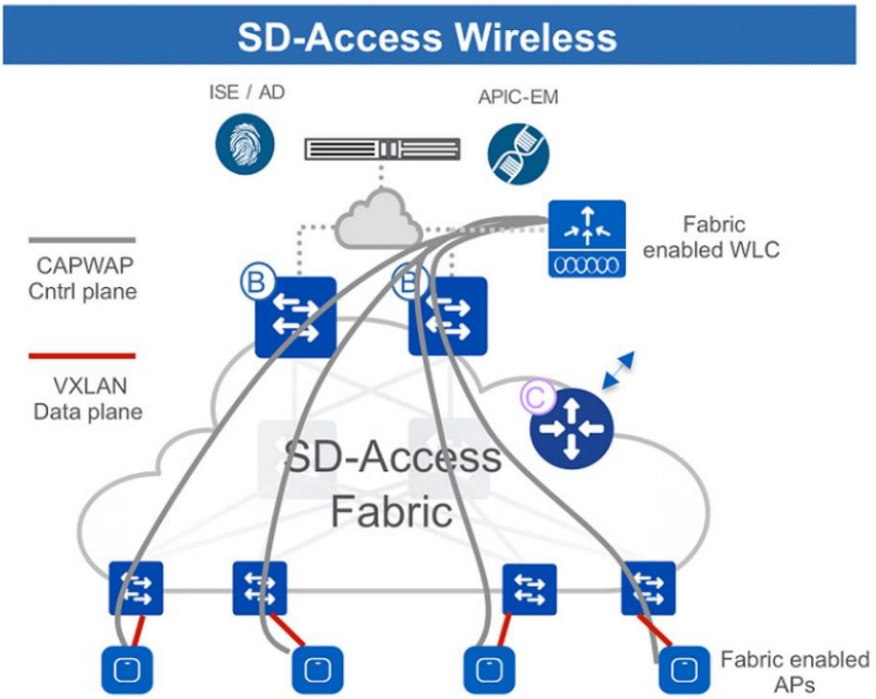
- パフォーマンスの向上：

  レイヤ 2 でのワイヤレスローミングを使用した、あらゆる形式のアンカーリングの要件を排除します。

- 分散データプレーン：

  集中型スイッチングのワイヤレスアーキテクチャと比較して、全体的なワイヤレススループットを向上させます。

図 13.　Cisco SD-Access ワイヤレスにおけるコントロールプレーンとデータプレーンのトラフィックフローの例



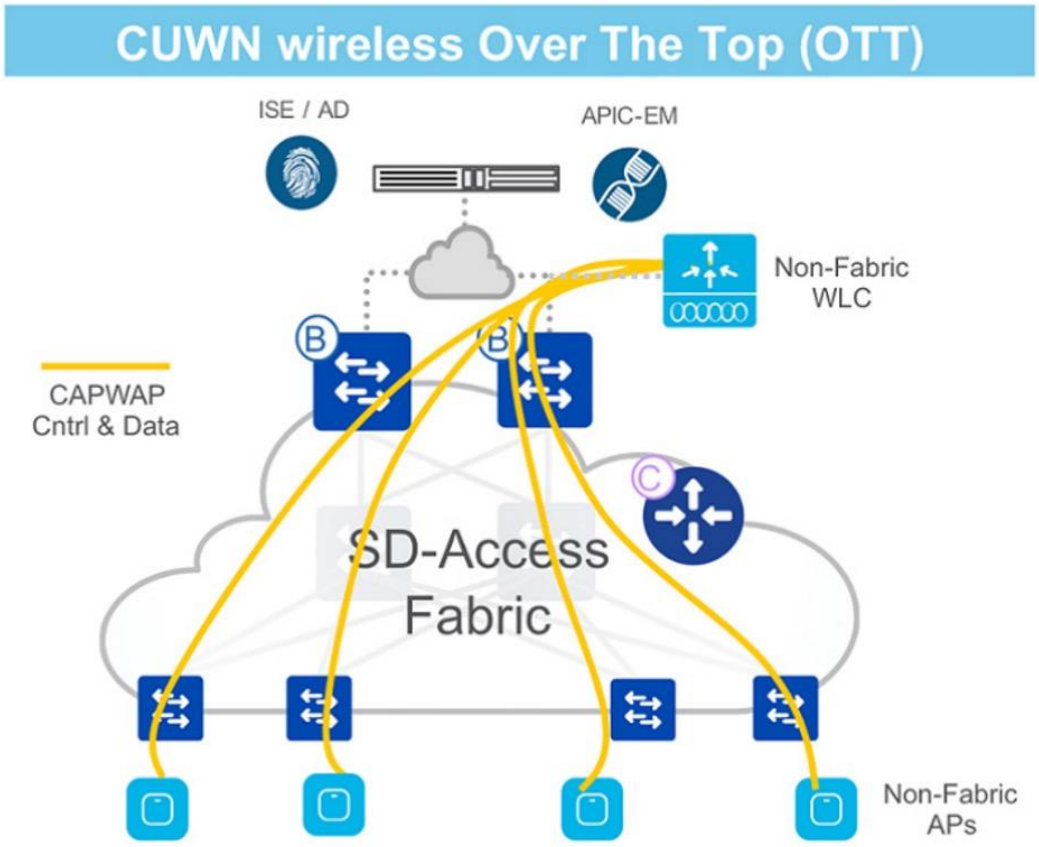
Cisco Unified Wireless Network ワイヤレスオーバーザトップ（OTT）

Cisco SD-Access は、ワイヤレス オーバーザトップ（OTT）と呼ばれる集中型ワイヤレス展開を柔軟にサポートします。このサポートは、以下のようないくつかのシナリオで重要です。

- 既存のシスコ ワイヤレス コントローラと AP が SD-Access ワイヤレスに対応していない場合。
- ネットワークにサードパーティのワイヤレスデバイスが存在する場合。
- 有線ネットワークとワイヤレスネットワークの間で移行ペースが非対称である場合。

ワイヤレス OTT 展開では、ワイヤレスのコントロール、管理、およびデータプレーントラフィックは、AP とワイヤレスコントローラ間の CAPWAP トンネル内でファブリックを通過します。この CAPWAP トンネルは、Cisco SD-Access ファブリックを転送メディアとして利用します。他のベンダーのワイヤレス機器が異なるトンネリングプロトコルを使用する場合でも、SD-Access ファブリックをトランスポートとして使用するという概念は同じです。

図 14.　　ワイヤレス OTT におけるコントロールプレーンとデータプレーントラフィックのフローの例



詳細については、『Cisco SD-Access Wireless Design』および「Cisco Wireless Design and Deployment Guide」を参照してください。

分散サイト設計

分散キャンパス向け Cisco SD-Access は、複数の独立したファブリックサイトを接続しながらサイト間で VRF や SGT といった一貫したセキュリティポリシーを維持するように設計された、メトロエリア接続ソリューションです。SD-Access は以前からマルチサイト環境をサポートしていましたが、サイト間でポリシーを同期させるためのシンプルで自動化された方法はありませんでした。以前は、各サイトのファブリックボーダーノードで、ファブリックパケットがネイティブ IP にカプセル化解除されていました。サイト間のポリシー拡張は可能でしたが、手動プロセスが必要で、ポリシーの伝達を SXP に依存し、ISE 内での IP から SGT へのバインディングの複雑な設定が必要でした。

分散キャンパス向け SD-Access トランジットでは、SXP は不要となり、設定は自動化され、複雑なマッピングは簡素化されました。このソリューションは、メトロネットワーク全体で一貫したエンドツーエンドの自動化とポリシーによるサイト間通信を可能にします。

分散キャンパス向け SD-Access トランジットは、LISP プロトコルからのコントロール プレーン シグナリングを使用し、ファブリックサイト間でパケットの VXLAN カプセル化を維持します。これにより、VRF と SGT のマクロおよびマイクロセグメンテーションのポリシー構成要素が、ファブリックサイト間でそれぞれ保持されます。パケットの元のイーサネットヘッダーが維持され、SD-Access ワイヤレスのレイヤ 2 オーバーレイサービスが有効になります。ポリシーがグループメンバーシップによって維持されるため、結果としてアドレスに依存しないネットワークが実現されます。

詳細については、『Cisco SD-Access Distributed Campus Deployment Guide』および「Cisco SD-Access Distributed Campus Design」を参照してください。

MSRB

MSRB は、ファブリックネットワーク内の信頼されていないトラフィックのルーティングを、ファイアウォールや DMZ などの指定された場所に集約します。たとえば、ゲスト VN が複数のサイトにまたがるシナリオでは、すべてのゲストトラフィックが DMZ にあるリモートボーダーを経由するように誘導され、エンタープライズトラフィックから効果的に隔離されます。

マルチサイトネットワーク展開では、指定された MSRB が、複数のサイトにまたがって拡張された特定の VN との間のトラフィックを管理します。この設定により、これらの場所で統一されたサブネットを維持しながら、複数のファブリックサイトにわたる VN の展開が可能になります。複数のファブリックサイト間でサブネットを一貫して維持することで、IP アドレスの利用を最適化できます。また、その VN のための一元的なエントリポイントとイグジットポイントを確立し、いくつかの利点を提供します。

- 集中管理

  特定の VN のすべてのトラフィックをさまざまなサイトにわたって処理する共通のボーダースイッチ（アンカーボーダー）を指定できます。これにより、管理とポリシーの適用が簡素化されます。

- サブネットの一貫性

  MSRB を使用すると、すべてのサイトで VN に同じサブネットを使用できます。これにより、各ロケーションで異なるサブネットを管理する必要がなくなり、IP アドレス空間を節約し、設定を簡素化できます。

- トラフィックの分離

  MSRB は、ゲスト Wi-Fi などの信頼できないトラフィックを分離する場合に特に役立ちます。異なるサイトをまたがるすべてのゲストトラフィックは、セキュリティ目的で DMZ のような中央の場所にトンネリングできます。

MSRB のコンテキストで使用される一般的な用語を以下に示します。

- アンカー VN：

  ネットワーク内の複数のファブリックサイトにまたがって存在する VN です。関連付けられた IP サブネットとセグメントは、これらの複数のサイトで共通です。

- アンカーサイト：

  アンカー VN の共通のボーダーとコントロールプレーンをホストするファブリックサイト。アンカーサイトは、アンカー VN への入力トラフィックとそこからの出力トラフィックを処理します。

- アンカーサイト：

  アンカー VN が展開されているアンカーサイト以外のファブリックサイトです。

- アンカーボーダーノードまたは MSRB：

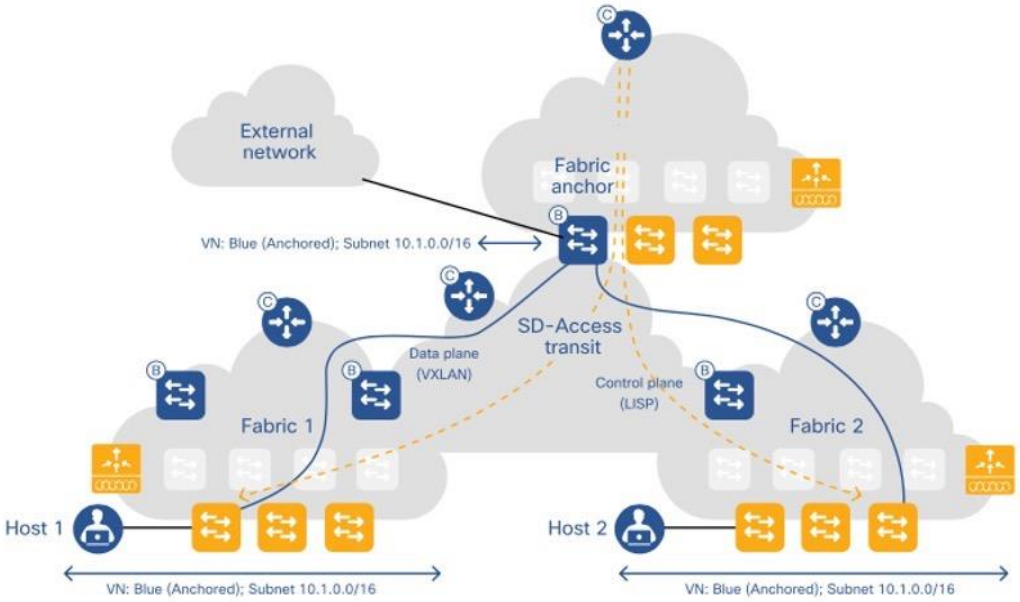
  アンカー VN との間のトラフィックの入出力場所を提供する、アンカーサイトのファブリックボーダーノードです。

- アンカー コントロール プレーン ノード：

  アンカー VN のエンドポイントの登録を受け入れ、要求に応答する、アンカーサイトのファブリック コントロール プレーン ノードです。

つまり、MSRB は、複数のサイトを持つ Cisco SD-Access 展開において、ネットワーク管理を簡素化し、隔離されたトラフィックのセキュリティを強化し、IP アドレスの利用を最適化します。

図 15.　　MSRB 展開の例



MSRB の詳細については、『LISP VXLAN Fabric Configuration Guide』を参照してください。

注：　追加の 50 バイトの VXLAN ヘッダーのオーバーヘッドに対応するには、パス全体で MTU を考慮することが重要です。これは、アンカーサイトのボーダーノードの到達可能性のために複数の IP ネットワークを通過する必要があるため、特に重要です。

LISP パブリッシュおよびサブスクライブ設計

LISP パブリッシュおよびサブスクライブ（Pub/Sub）モデルは、従来の LISP アーキテクチャの大幅な拡張です。ネットワーク全体のエンドポイント位置情報の配信を合理化し、すべてのノードが迅速に正確なデータを受信できるようにします。その効率性、拡張性、および動的な環境を管理する能力により、LISP Pub/Sub モデルは、現代の大規模ネットワーク設計における重要なコンポーネントとなっています。

LISP Pub/Sub 設計により、ファブリック内のコントロールプレーンノードに LISP サイト登録テーブルを登録するための追加プロトコルが不要になります。LISP Pub/Sub 機能は、Catalyst Center を通じて完全に自動化されており、SD-Access ファブリックの展開を簡素化し、手動でのルーティング設定の必要性を排除します。

LISP Pub/Sub アーキテクチャは、次のような他の機能の構成要素です。

- LISP ダイナミック デフォルト ボーダー ノード
- LISP バックアップインターネット
- LISP アフィニティ ID
- LISP エクストラネット

LISP Pub/Sub は、情報のルーティングにパブリッシュおよびサブスクライブモデルを使用します。エッジノードは、両方のボーダーノードのネクストホップ IP アドレスを含むデフォルトルートをサブスクライブします。ボーダーノードがアップストリーム接続（および BGP ピアリング）を失うと、影響を受ける VN のルーティングテーブルからデフォルトルートも削除されます。その後、ボーダーノードはコントロールプレーンを更新して、もはやデフォルトルートとして機能できないことを通知します。その結果、コントロールプレーンはデフォルトルートをサブスクライブしているすべてのエッジノードに通知し、障害が発生したルートの使用を停止させ、代わりに残りのアクティブなボーダーノードへのデフォルトルートに依存するようにします。このアプローチにより、ルーティングの冗長性を維持するためにボーダーノード間で VRF/VN ごとに BGP ピアリングを行う必要がなくなり、手動での設定が削減されます。

展開の考慮事項

- LISP/BGP ファブリックサイトと LISP Pub/Sub ファブリックサイトは、同じ SD-Access トランジット コントロール プレーン ノードと共存できません。
- 一方からもう一方への移行はまだサポートされていません。
- 新しいネットワークの実装には、LISP Pub/Sub が推奨されています。

SD-Access への移行

Cisco SD-Access への移行には、評価、設計、実装、および継続的な最適化を含む包括的なアプローチが必要です。自動化と管理のために Catalyst Center を活用することで、合理化された効率的な移行プロセスが保証され、最終的にはよりセキュアで拡張性に優れ、かつ管理しやすいネットワーク環境が実現します。

既存のネットワークを Cisco SD-Access に移行する前に、以下の側面を考慮してください。

- Network

  MTU、ネットワークトポロジ、アンダーレイおよびオーバーレイの IP アドレス指定、共有サービスの場所。

- ポリシー：

  既存のポリシーの定義と適用ポイント、VN、SGT。

- ハードウェア プラットフォーム

  SD-Access をサポートするスイッチ、ルータ、ワイヤレスコントローラ、および AP。

- ソフトウェアプラットフォーム

  Catalyst Center、 ISE、ネットワーク データ プラットフォーム。

- 展開の規模

  SD-Access アーキテクチャでのロールに基づくハードウェア プラットフォームの規模。

- 既存のネットワーク設計

  レイヤ 2 アクセスまたはルーテッドアクセス。

既存のネットワークを SD-Access に移行するための主なアプローチは以下の通りです。

- 並行アプローチ

  SD-Access ネットワークが既存のブラウンフィールド ネットワークと並行して構築されます。スイッチは、ケーブルを物理的にパッチングすることで、ブラウンフィールド ネットワークから SD-Access ネットワークに移行されます。このアプローチにより、変更管理とロールバックの手順が簡素化されます。ただし、並行ネットワークをセットアップするには、ブラウンフィールド ネットワークが現在使用しているものに加えて、追加のラックスペース、電力、およびケーブル インフラストラクチャが必要です。

- 段階的アプローチ

  この戦略では、従来のスイッチをブラウンフィールド ネットワークから移行し、SD-Access ファブリック エッジノードに変換します。次のセクションで説明するレイヤ 2 ボーダーハンドオフは、この段階的な移行を促進します。このアプローチは、SD-Access をサポートできる既存の機器がある、または限られたスペースや電力などの環境上の制約に直面しているネットワークに適しています。

既存の従来型ネットワークを Cisco SD-Access に移行するための完全なガイダンスとさまざまなオプションについては、『Cisco Software-Defined Access for Industry Verticals』の「Migration to Cisco SD-Access」の章を参照してください。

検証済みのソリューションのユースケース

これらのセクションでは、大学ネットワーク向けに検証された主要なユースケースの概要を説明します。これらは、機関が IT インフラストラクチャを設計および構築するのに役立つ信頼できるテンプレートとして機能します。これらのソリューションは厳密にテストされ、学術環境の固有の要件に対処するために調整されており、信頼性、拡張性、および最適なパフォーマンスを保証します。

Day 0 および Day 1 ネットワークの立ち上げのユースケース

- 新規キャンパス向けに、Catalyst Center を展開し、外部サーバーと統合する。
- LAN 自動化と PnP を使用してデバイスをオンボーディングする。
- ネットワークデバイスとファブリックのプロビジョニングを自動化および簡素化する。
- Catalyst Center を使用してインベントリを監視し、ネットワークデバイスを管理する。
- Cisco ISE と統合し、デバイスとクライアントの認証および承認を行う。
- Catalyst Center を使用してワイヤレスコントローラと AP を管理および展開する。
- 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。
- SD-Access マルチサイトキャンパスを展開し、キャンパス全体のトラフィックを管理する。

Day-n ネットワーク運用のユースケース

- Catalyst Center を使用して、スイッチ、ルータ、ワイヤレスコントローラなどの複数のデバイスをアップグレードする。
- 既存のファブリックサイトに新しいフロアをオンボーディングする。
- 有線およびワイヤレスクライアントを持つ新しいファブリックノードをオンボーディングする。
- ブラウンフィールドの AP を Wave2 から 11 Ax に置き換える
- 組み込みワイヤレスコントローラを備えた FIAB を使用して小規模キャンパスを追加する。
- Day-n の認証情報の変更（デバイスパスワードの変更後のデバイスプロビジョニングなど）を実行する。

ソリューションのユースケースシナリオ

以下のユースケースは、示されたトポロジに基づき、この大学業界のプロファイル向けに実装されています。

Catalyst Center を活用した大学ネットワークのインテントベース ネットワーキング

大学のネットワーク管理者は、Catalyst Center を使用して以下の目標を達成できます。

- グローバルなネットワーク階層を設計し、グローバルおよびサイト固有のネットワーク構成の両方を設定して、大学全体のパフォーマンスを最適化する。
- デバイスを自動的にプロビジョニングして、ネットワーク展開と管理を合理化する。
- 冗長性と拡張性のために、デュアルボーダーノードとデュアル コントロール プレーン ノードを備えたメインキャンパス ネットワークを展開し、大学の成長に伴う信頼性の高い接続性を確保する。
- 以下のような新しいデバイスをオンボーディングすることで、メインキャンパスとサテライトキャンパスの両方の場所でネットワークを簡単に拡張する。
    - ゼロタッチ プラグアンドプレイの LAN 自動化を使用するか、アンダーレイの到達可能性のために既存の IP/MPLS インフラストラクチャを使用したファブリックエッジスイッチ。
    - ゼロタッチ プラグアンドプレイで IoT デバイスをサポートするためにファブリックにクラシック拡張されたノード。
    - SGT の直接サポートと拡張トラフィック適用のためにファブリックにポリシー拡張されたノード。
- Cisco SD-Access トランジットを使用して分散キャンパスサイトを接続し、すべてのキャンパスで共有データセンターやインターネットサービスへの効率的なアクセスを可能にする。

このアプローチにより、大学は、手動での設定作業を最小限に抑えながら、柔軟で拡張性に優れたセキュアなネットワーク環境を実現できます。

機密性の高い大学データを保護する多層セキュリティ

大学の管理者は、機密性の高い機関データを保護するために以下の対策を実装できます。

- 学生、教職員、ゲスト、IoT デバイス、キャンパス機器を適切な論理ネットワークにセグメント化し、大学ネットワーク内での脅威のラテラルムーブメントを制限する。
- 有線およびワイヤレスの両方のエンドポイントに対して、802.1X（dot1x）や MAC 認証バイパス（MAB）などのクローズド認証メカニズムを利用して、大学リソースへの不正アクセスを防止する。
- Catalyst Center を通じて信頼できる認証局（CA）の FQDN ベース証明書を適用し、ネットワークのセキュリティフレームワークを強化する。
- ユーザーグループを作成し、ユーザーとエンドポイントをアイデンティティに基づいて分類し、グループベースのポリシーを定義して異なるグループ間のトラフィックのやり取りを規制する。
- Catalyst Center の包括的な監査ログを通じて活動を監視し、何が、いつ、どこで、どのユーザーによって発生したかを含むシステムイベントを追跡する。
- Catalyst Center ユーザーの精度の高いロールベースのアクセス権限を確立し、管理者、教員、および IT スタッフに、ロールに適したアクセス権を付与する。

この多層セキュリティフレームワークは、大学データの保護を強化し、キャンパスネットワーク全体で適切なアクセス制御を保証します。

Cisco AI Endpoint Analytics

大学の管理者は、以下を実装することで、未知のエンドポイントを効果的に管理し、エンドポイントのセキュリティを強化できます。

- Cisco AI エンドポイント分析を設定して、大学のネットワーク環境に合わせて調整された分類と動作モデルの学習に基づいてスプーフィングされているエンドポイントを特定する。
- 大学のネットワーク内で侵害されたエンドポイントを検出してフラグを立てるように Catalyst Center を設定する。設定された影響パラメータに基づいて、各エンドポイントの包括的な信頼スコアが計算されます。
- 信頼スコアを監視し、各エンドポイントに関連する脅威のタイプを特定する。是正措置を講じるか、悪意のあるエンドポイントを検疫し、大学のネットワークを保護します。

これにより、大学のネットワークのセキュリティ脅威が継続的に監視され、安全で信頼できる環境を維持するために能動的に措置が取られます。

サービスとネットワークの復元力

大学の管理者は、以下のレジリエンス対策を実装して、信頼性の高いサービス提供を確保し、ネットワークの中断を最小限に抑えることができます。

- デュアル Cisco SD-Access ボーダー、デュアル コントロール プレーン ノード、ボーダーおよびエッジ タッキング、デュアル トランジット コントロール プレーンなどの機能を備えた冗長ネットワークインフラストラクチャを展開する。これにより、迅速なフェールオーバーが保証され、ネットワーク障害時のサービスの中断を最小限に抑えることができます。
- Catalyst Center を 3 ノードの HA クラスターで展開し、ノードまたはサービスの障害時に手動での介入を必要とせずに、継続的なサービス提供を保証する。
- 信頼性を高め、障害時のサービス中断を最小限に抑えるために、PAN、PSN、M&T、および pxGrid サービスのフェールオーバーを備えた分散 Cisco ISE 展開を実装する。
- Catalyst Center とデバイスの設定を定期的にバックアップし、予期せぬインシデントが発生した場合に以前の設定に迅速に復元できるようにする。

これらの対策によって、大学のサービスに安定したレジリエンスのあるネットワーク環境を確保できます。

簡素化されたネットワーク管理

大学の管理者は、Catalyst Center で以下の機能を活用することで、ネットワーク管理を簡素化できます。

- Catalyst Center を使用して、IP アドレスやソフトウェアバージョンなどの詳細を含むすべてのネットワークデバイスを管理し、監視と管理を簡素化する。
- VN を作成および管理して、異なる大学の学部や場所に対して、安全で組織的なネットワーク セグメンテーションを確保する。
- ユーザーのロールに基づいて、VN 内のトラフィックを制御するために SGT とアクセスポリシーを適用し、セキュリティとパフォーマンスを向上する。
- Catalyst Center SWIM を使用してネットワークデバイスを標準規格イメージにアップグレードすることで、一貫性を維持し、管理タスクを削減する。
- 大学ネットワークの拡大に合わせて、効率的なネットワーク運用と拡張性のために VLAN 設定を最適化する。
- ゼロタッチプロビジョニング（ZTP）により新しいネットワークデバイスのセットアップを自動化し、時間を節約して人的エラーを軽減する。
- テンプレートを使用してネットワーク設定を作成および展開し、一貫性を確保し、デバイスのセットアップや設定変更を迅速化する。

これらの機能により、ネットワーク管理が簡素化され、大学の IT チームは信頼性の高い、安全で拡張性に優れたネットワーク環境を維持できます。

Assurance と Analytics による運用とメンテナンス

大学の管理者は、以下のタスクを実行することで、Catalyst Center Assurance および Analytics を活用してネットワーク運用を最適化できます。

- 有線およびワイヤレス インフラストラクチャを含む大学のネットワークのパフォーマンスを継続的に追跡し、リンク障害、AP のダウンタイム、デバイスの誤動作などの問題を検出して解決する。
- 有線クライアントとワイヤレスクライアントの両方の正常性とパフォーマンスを監視し、クライアント接続の問題を特定および対処して、学生、教員、およびスタッフのスムーズなオンボーディングを保証する。
- 最大 100,000 の同時接続エンドポイントと 250,000 の一時的エンドポイントを追跡することで、ネットワークの拡張性を管理する。これは、多くのユーザーとデバイスを持つ大規模キャンパスにとって非常に重要です。
- ネットワーク内の不正 AP を特定し、レポートを生成して迅速な修正措置を講じ、ネットワークセキュリティを向上させる。
- アプリケーションのパフォーマンスとエンドユーザー体験に関するインサイトを獲得し、重要な教育サービスと管理サービスが最小限のダウンタイムでスムーズに動作するようにする。
- ネットワークデバイスを監視および管理することで大学のセキュリティポリシーに準拠し、脆弱性や不正なデバイスに迅速に対処する。
- カスタマイズされたダッシュボードを作成して主要業績評価指標（KPI）を視覚化し、ネットワークパフォーマンスに関する実用的なインサイトを獲得する。

このアプローチにより、大学のネットワークの堅牢性と安全性を維持し、学生、教員、スタッフのニーズに対応できます。

教育用ローミング

大学の管理者は以下の設定で eduroam を実装することにより、eduroam を使用してコラボレーションと接続をグローバルに強化できます。

- Catalyst Center を使用して、エンタープライズセキュリティを有効にし、802.1X 認証を使用した eduroam Wi-Fi SSID を設定する。
- 外部の eduroam サーバーからの認証リクエストを管理し、外部ユーザーの認証リクエストを検証のために eduroam サーバーに転送するように Cisco ISE を設定する。
- 他の大学からの外部ユーザーがローカルキャンパスの eduroam SSID に接続し、認証が成功すると安全なネットワークアクセスを獲得できるようにする。
- 現地の大学から旅行中のユーザーが、外国の大学の eduroam SSID に接続し、ネットワークに安全にアクセスできるようにする。

この設定により、大学は、ローカルユーザーと訪問者の両方にシームレスでセキュアなネットワークアクセスを提供し、国際的なコラボレーションとモビリティを促進できます。

詳細については、『Configuring eduroam on Cisco Identity Services Engine (ISE)』を参照してください。

Cisco Wide Area Bonjour

大学の管理者は、以下の機能を実装することで、Cisco Wide Area Bonjour を活用して大学ネットワーク全体でのサービスの発見を有効にできます。

- 大学ネットワーク全体で効率的なサービスルーティングを可能にするために、SDG-Agent とネットワーク情報を設定する。
- サービスポリシーベースの ZeroConf サービス管理を設定し、Cisco Wide Area Bonjour アプリケーションを通じてエンドユーザーデバイスから共通の Bonjour サービスを配信する。
- 大学ネットワークのユーザーが、レイヤ 3 ドメインを超えて印刷や画面共有などの Bonjour サービスにアクセスできるようにする。
- Cisco Wide Area Bonjour ダッシュボードを使用して、サブドメインごとのサービス数やポリシーの稼働状況など、SDG-Agent の統計情報を監視する。

このアプローチにより、サービスの発見が簡素化され、さまざまな大学キャンパスまたはネットワークセグメント全体でのユーザー体験が向上します。

詳細については、『Cisco DNA Service for Bonjour: Quick Configuration Guide』を参照してください。

BYOD

大学の管理者は、以下の機能を実装することで、Cisco ISE を使用して安全な BYOD アクセスを確保できます。

- 大学ネットワーク上の個人デバイスに特権アクセスを許可するように Cisco ISE を設定する。
- Catalyst Center を使用して BYOD エンドポイントにエンタープライズ SSID をプロビジョニングする。
- 学生または教職員が自分の個人デバイスを大学ネットワークに接続し、特権アクセスを取得できるようにする。
- Cisco ISE のデバイスポータルを使用して、BYOD エンドポイントの便利な管理と制御を行う。
- 802.1X や WebAuth などの認証方式を適用し、許可されたデバイスのみが大学ネットワークに接続できるようにする。
- 大学リソースを保護するために、BYOD デバイスを機密システムから分離する。
- デバイスプロファイリングを使用してデバイスタイプを自動的に識別し、適切なポリシーを適用する。

これらの対策により、学術ネットワークの整合性とセキュリティを維持しながら、大学キャンパスで BYOD デバイスをシームレスかつ安全に管理できます。

詳細については、『Cisco ISE BYOD Prescriptive Deployment Guide』を参照してください。

MSRB を使用したゲストサービス

大学の管理者は、以下の機能を実装することで、ゲストサービスを効率的に管理できます。

- ゲスト VN を設定し、複数の大学サイトにわたって拡張する。この VN は、中央のアンカーサイトにあるリモートボーダーにアンカーできます。
- ゲストトラフィックをゲスト VN 内に隔離しトラフィックをアンカーボーダーにトンネル化して安全なインターネットアクセスを確保する。
- アンカーサイトと継承されたファブリックサイトの両方でゲストユーザーをシームレスにオンボーディングするために、共通のゲストサブネットをセットアップする。
- Catalyst Center を使用してキャプティブウェブ認証（CWA）付きのゲスト SSID をプロビジョニングし、同じゲスト SSID がすべての大学サイトで一貫するようにする。
- 物理的に異なる場所にデュアルアンカーボーダーとコントロールプレーンを備えたアンカーサイトを実装し、ネットワーク障害時の冗長性を確保する。
- 接続されたデバイスの信頼スコアと脅威タイプを監視し、必要に応じて是正措置を取ったり、悪意のあるエンドポイントを検疫したりする。

このアプローチにより、すべての大学キャンパスで安全で拡張性と頼性の高いゲストアクセスを確保し、キャンパスネットワーク全体の体験を向上させることができます。

ファブリック外のレイヤ 2 終端

大学のネットワーク管理者は、以下のタスクを実行できます。

- Catalyst Center を使用して必要なレイヤ 2 VN を設定する。
- 専用のレイヤ 2 ボーダーノードでレイヤ 2 ハンドオフを設定する。
- トラフィック検査のために、ファブリック外部（通常はファイアウォール上）でトラフィックを終端する。

この設定により、ファブリック外部のレイヤ 2 トラフィックの適切なルーティングと検査が保証されるため、大学ネットワーク内での効率的なトラフィック管理が可能になります。

ソリューションの重要事項

このセクションでは、大学の業界プロファイルに向けたソリューション検証の主要な技術詳細を説明し、大学管理者が実装を深く理解するための包括的なリファレンスを提供します。

大学向けの Eduroam ワイヤレス ネットワーク アクセス

Eduroam は、研究者、教職員、学生が他の教育機関を訪問した際にネットワークアクセスを提供するグローバルなワイヤレスネットワークサービスです。Eduroam Wi-Fi ネットワークに接続することで、ユーザーは世界中のどこにいても、所属機関の認証情報を使用してリソースやインターネットにアクセスできます。インターネットアクセスやその他のネットワークリソースの承認は、訪問先の機関によって管理されます。

Eduroam サービスは認証に IEEE 802.1X を使用し、参加する RADIUS サーバーの階層システムを通じて動作します。適切に機能するためには、所属機関と訪問先の機関の両方の RADIUS サーバーが Eduroam ネットワークの一部である必要があります。

Eduroam Wi-Fi SSID は、エンタープライズセキュリティで保護され、Catalyst Center を使用してプロビジョニングされます。Eduroam を実装するには、Cisco ISE と Catalyst Center の両方で設定が必要です。Eduroam のポリシー設定と外部 RADIUS サーバーの設定は、Cisco ISE 内で管理されます。

図 16 と図 17 は、Eduroam 外部サーバーの設定を示しています。

図 16.　　外部 RADIUS サーバー設定 – 1

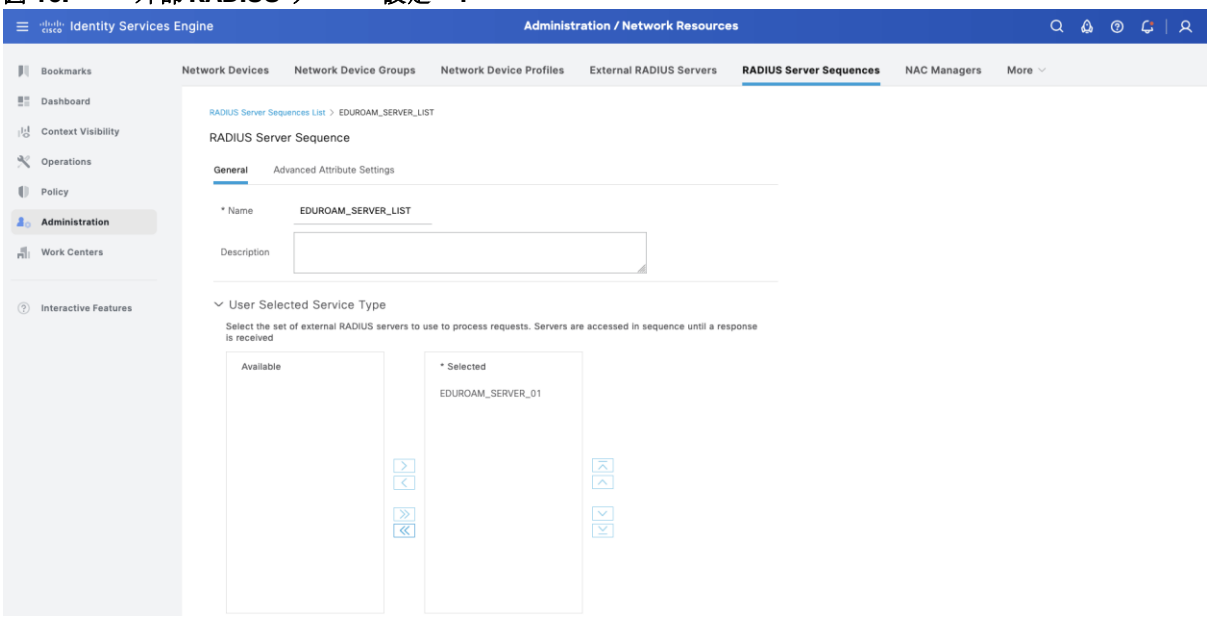


図 17.　　外部 RADIUS サーバー設定 – 2

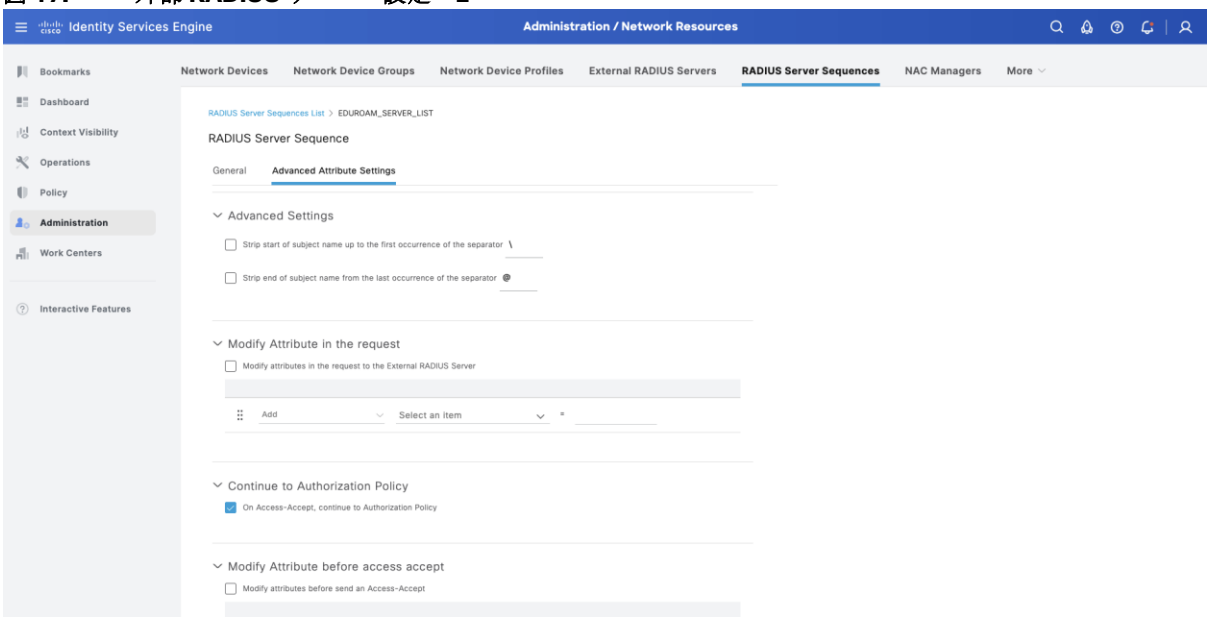


図 18 は、Eduroam ポリシーセットの設定を示しています。

図 18.　　Cisco ISE での Eduroam ポリシーセットの設定

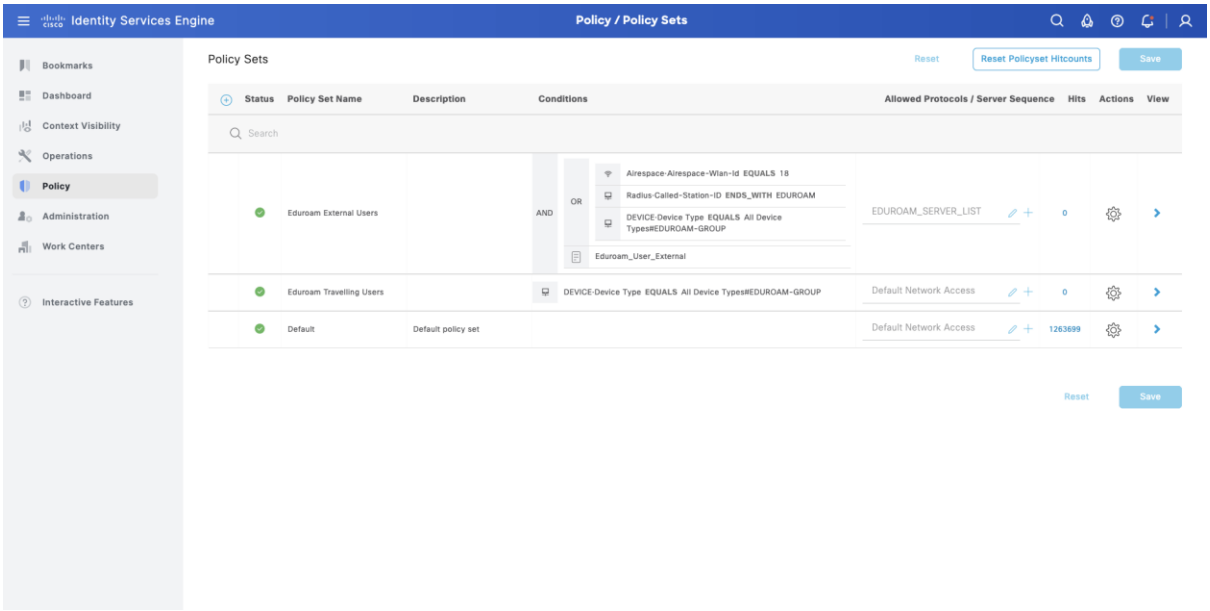
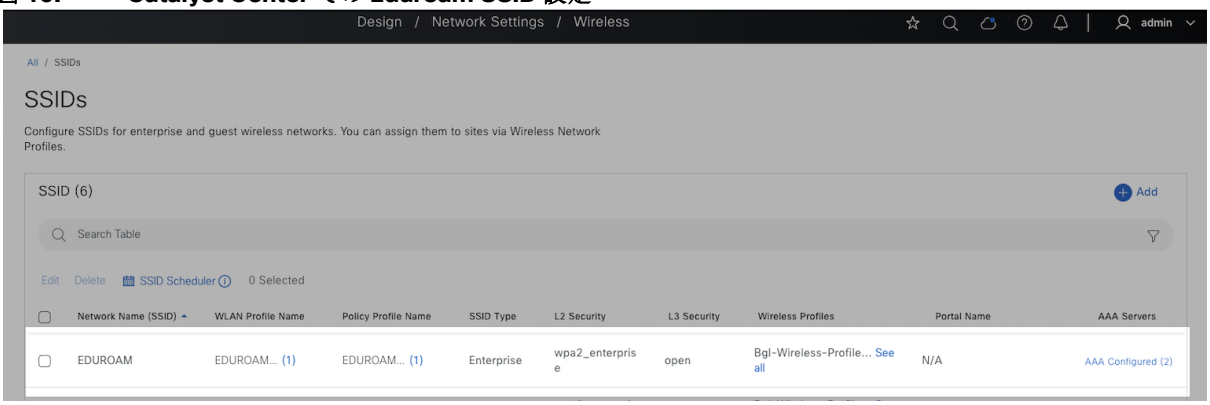


図 19 は、Catalyst Center での Eduroam SSID 設定を示しています。

図 19.　　Catalyst Center での Eduroam SSID 設定



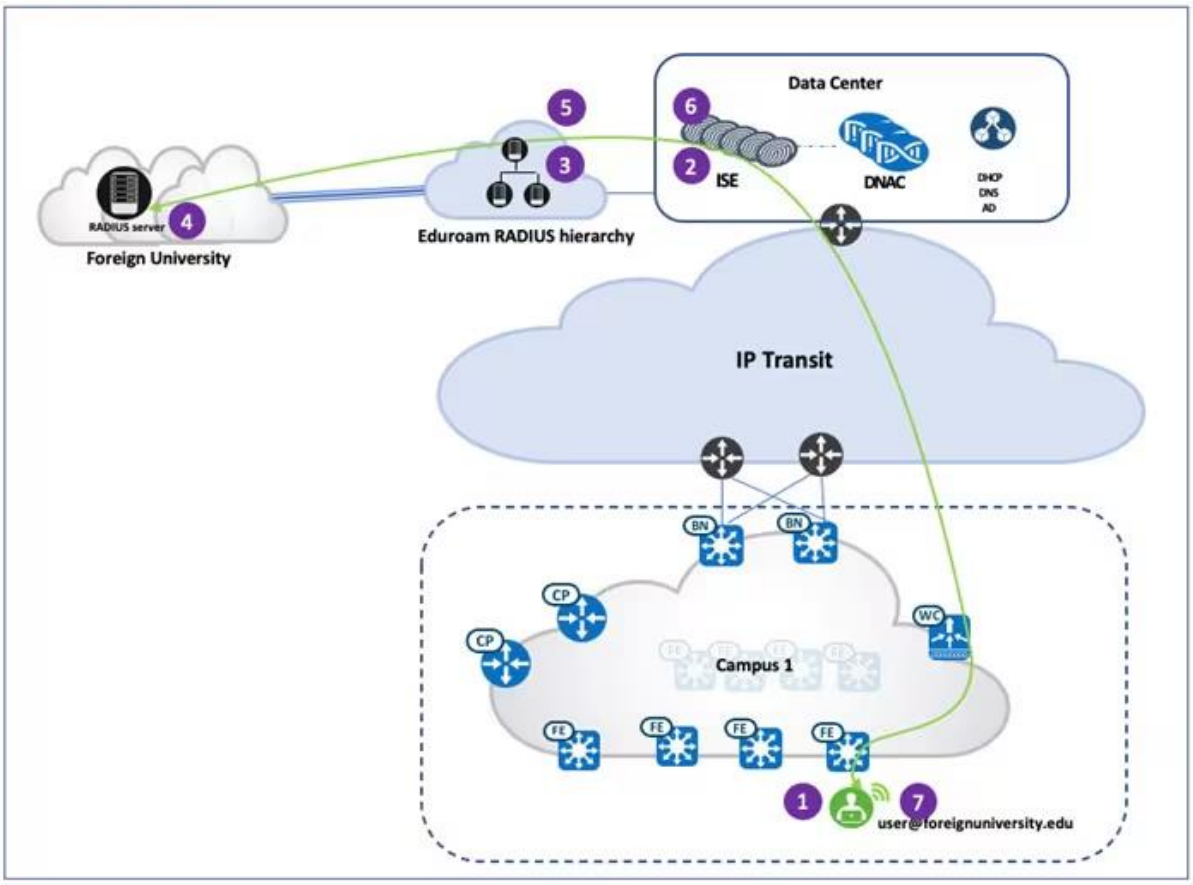
Eduroam は、大学生や教職員の 2 つの主なユースケースをサポートしています。

1. 外部ユーザー

   このシナリオでは、外部の大学の学生または教職員が、ローカルキャンパスを訪問します。ユーザーは Eduroam SSID に接続し、所属機関の認証情報を使用して認証を行います。リクエストは Eduroam サーバーに転送され、そこからユーザーの所属機関にルーティングされます。認証が成功すると、ユーザーはネットワークへのアクセスを許可されます。

   図 20 は、認証フローを示しています。

図 20.　　外部ユーザーの認証フロー

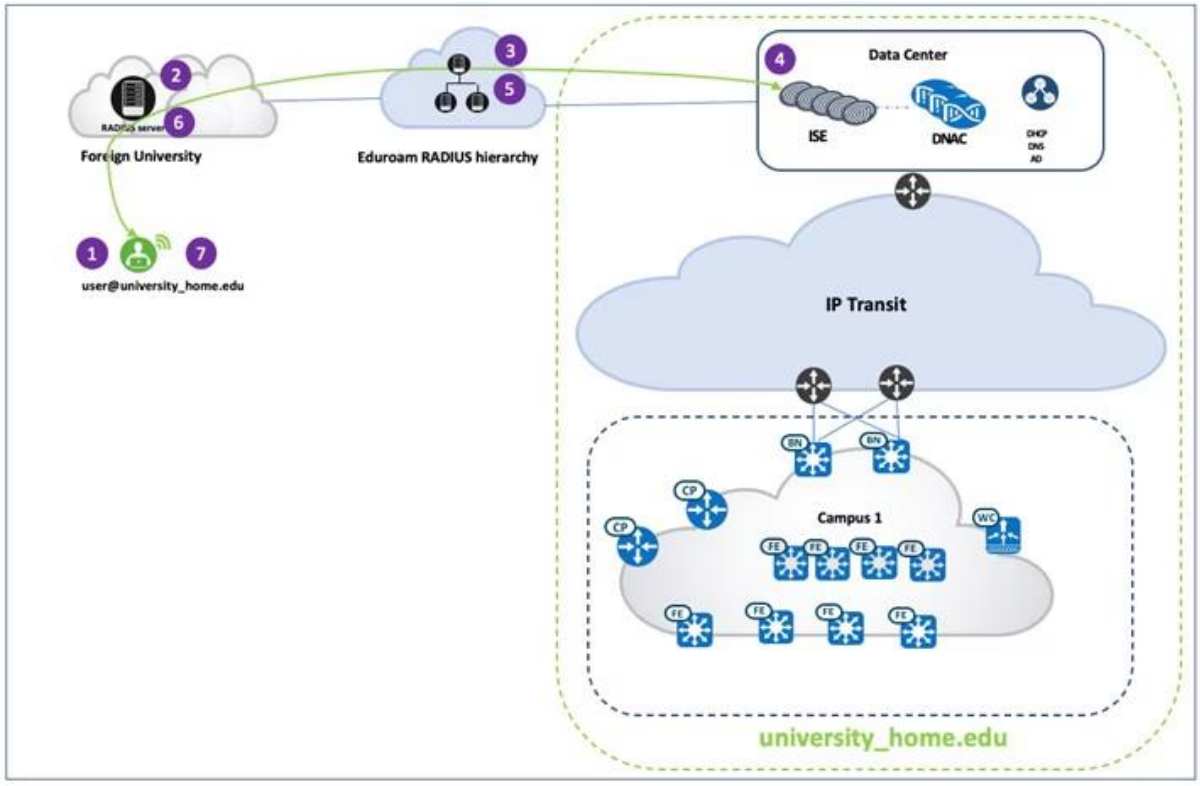


2. 旅行中のユーザー

このケースでは、所属機関の学生または教職員が、物理的に外国の大学キャンパスにいます。ユーザーが外国のキャンパスで Eduroam SSID に接続すると、認証リクエストが Eduroam RADIUS サーバーに送信され、そこからユーザーの所属機関の RADIUS サーバーに転送されます。認証が成功すると、所属機関の RADIUS サーバーは「アクセス許可」応答を Eduroam サーバーに送信し、それが外国の大学に転送されます。ユーザーは認証され、外国の大学でネットワークアクセスが付与されます。

図 21 は、認証フローを示しています。

図 21.　　旅行中のユーザーの認証フロー



この構造により、大学のユーザーは、外国を訪問中でも旅行中でも、シームレスで安全にネットワークにアクセスできます。

詳細については、『Configuring eduroam on Cisco Identity Services Engine (ISE)』を参照してください。

大学展開における MSRB を使用したゲストサービス

MSRB は VN 単位で有効になります。アンカー VN の場合、アンカーリングサイト内のすべてのエッジは、データプレーンと制御通信にアンカーボーダーノードとコントロールプレーンノードを使用します。アンカーリングサイトのワイヤレスコントローラは、アンカー VN に固有のワイヤレスエンドポイントの登録のためにアンカー コントロール プレーン ノードと通信します。

アンカーボーダーに到達するには複数の IP ネットワークを通過する可能性があるため、50 バイトの VXLAN ヘッダーオーバーヘッドに対応するために、パス全体の MTU に特別な注意を払う必要があります。アンカーされた VN は、アンカーサイトを使用するように設定されます。ゲストエンドポイントがゲスト SSID に参加し、Cisco ISE を使用した中央ウェブ認証を正常に完了すると、アンカーされたゲスト VN に関連付けられますゲストトラフィックはアンカーサイトのボーダーノードにトンネリングされ、ファイアウォールを介してインターネットに到達します。

また、ゲストトラフィックは VXLAN でカプセル化され、ファブリックを通過しますが、ゲストトラフィックのファーストホップまたはゲートウェイはファブリックの外部にあり、レイヤ 2 で MSRB に接続される可能性があります。設計で必要とされる場合、このようなデバイスは検査目的でファイアウォールにすることができます。

図 22 と図 23 は、Catalyst Center GUI で有効にされた MSRB を示しています。

図 22.　　アンカーおよびアンカーサイトのゲスト VN

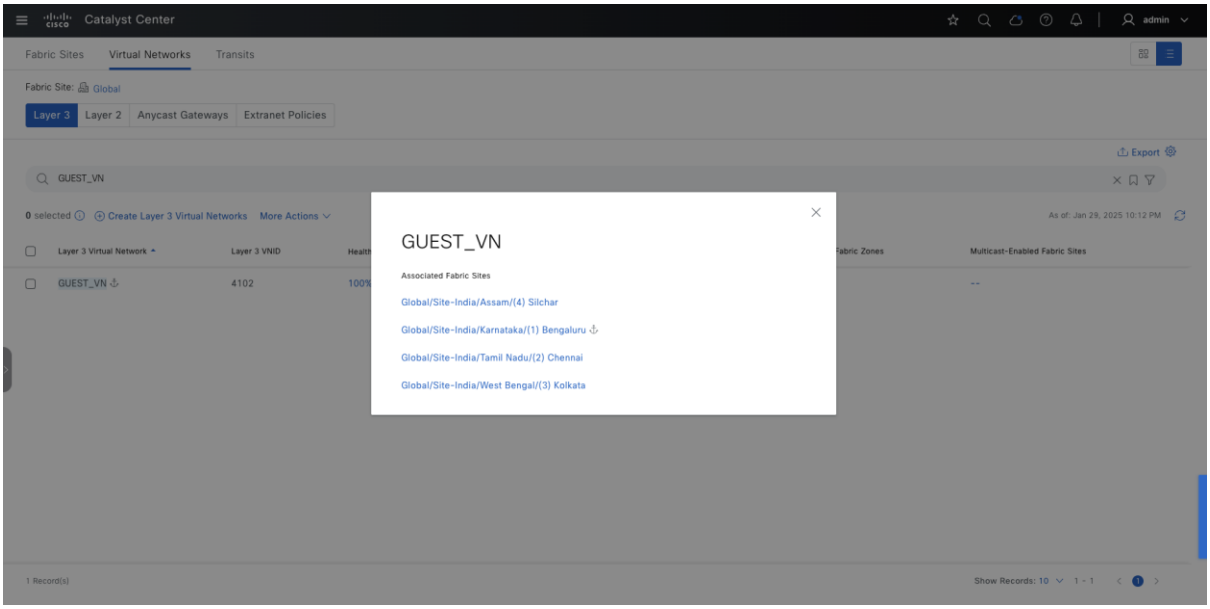


図 23.　　複数のサイトにまたがってプロビジョニングされた同じ IP サブネット

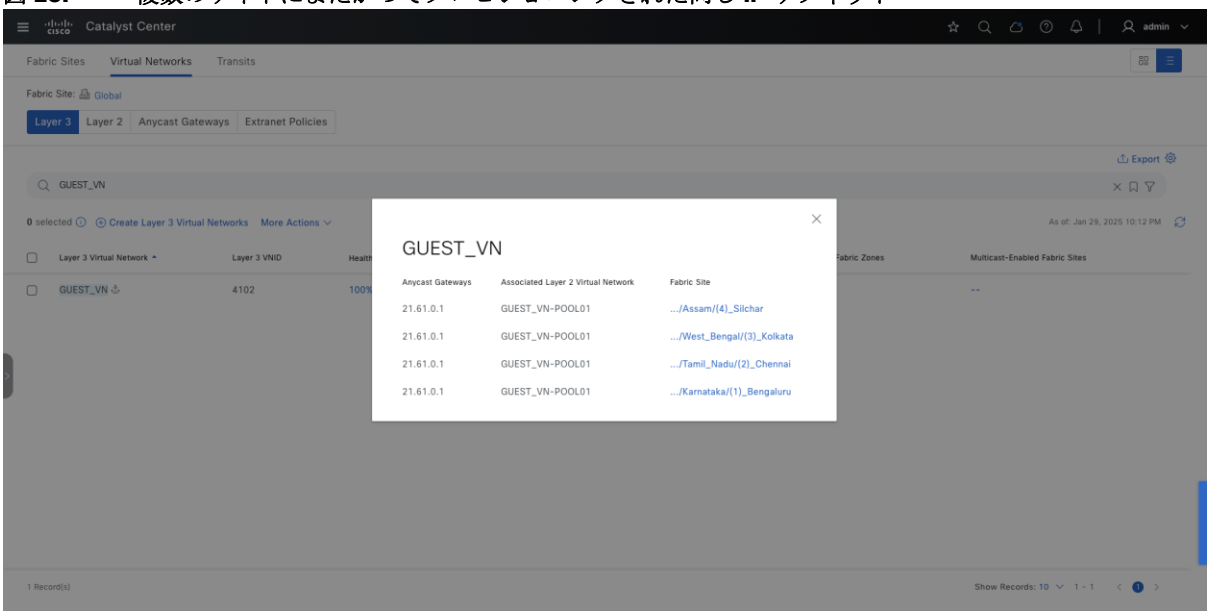
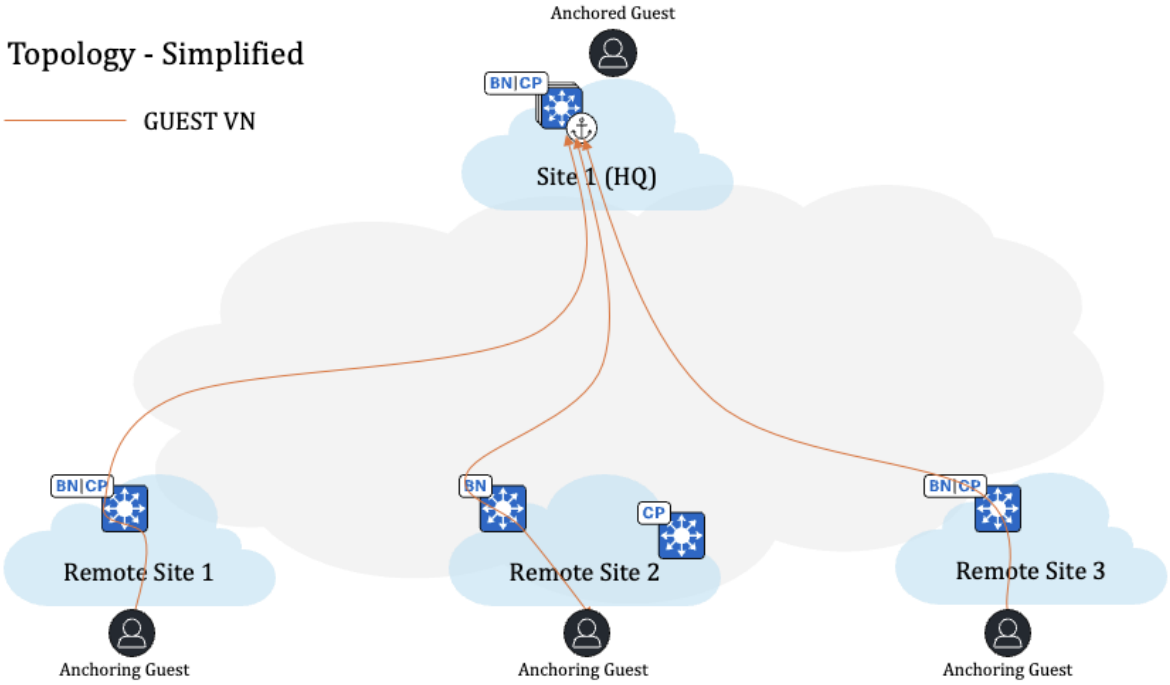


図 24 は、アンカーゲストトラフィックのトラフィックフローを示しています。

図 24.　　アンカー VN が実装されたゲストトラフィックフロー



Catalyst Center の GUI を通じてアクセスできるこの MSRB ソリューションは、複数の大学サイトにわたるゲストサービス管理を簡素化し、セキュリティを強化し、学生と訪問者の両方にシームレスな体験を保証します。

大学ネットワークの AI エンドポイント分析

大学では、多数のユーザーとそのデバイスを管理する必要があります。BYOD ポリシーでは、学生や教職員は通常、2 台から 3 台のデバイスをネットワークに接続します。ネットワークが拡大すると、セキュリティの問題も増加します。現代のセキュリティ脅威は、貴重な機関データへのアクセスを得るために、しばしば脆弱な侵入ポイントを悪用します。ネットワーク上のすべてのデバイスを識別し、追跡することは、時間と労力がかかる複雑な作業です。

Cisco AI エンドポイント分析機能は、パッシブ ネットワーク テレメトリ監視とディープ パケット インスペクションを使用して、タイプ、製造元、モデル、OS タイプ、通信プロトコル、およびポート別にデバイスを識別することで、この課題に対処します。この機能を使用すると、管理者は、属性に基づいてデバイスを分類するためのプロファイリングルールを作成できます。機械学習と組み合わせることで、Catalyst Center はスプーフィングされたエンドポイントを検出し、管理者が適切な措置を講じるのを支援できます。

Cisco AI エンドポイント分析は、Catalyst Center 内で実行される追加のアプリケーションです。展開するには、以下の手順を実行します。

- Catalyst Center のカタログサーバーからアプリケーションをダウンロードしてインストールします。
- Catalyst Center の [System Settings] で有効にします。
- Catalyst Center がクラウドに接続され、最新のエンドポイント分析モデルをダウンロードできることを確認します。

インストール後、Cisco AI エンドポイント分析は、メニューアイコンをクリックしてポリシーを選択することで、Catalyst Center のホームページからアクセスできます。Cisco AI エンドポイント分析は、以下のような複数の方法を使用して悪意のあるエンドポイントを検出します。

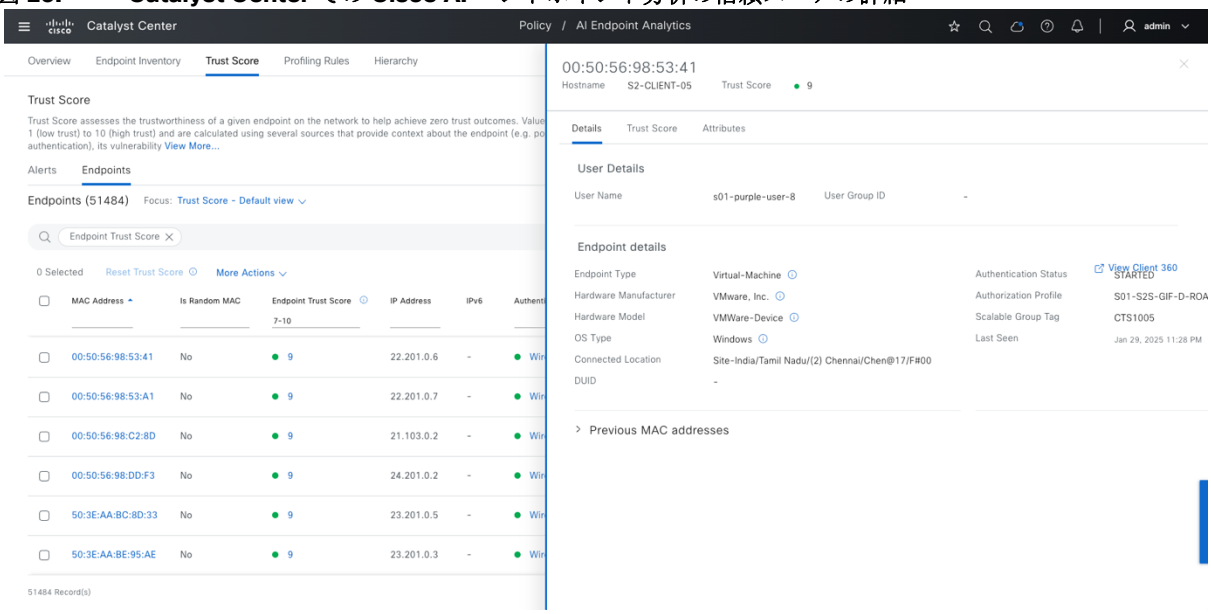
- プロファイルラベルの変更
- NAT モード検出
- 同時 MAC アドレス分析

- ポスチャと認証方法の分析
- 機械学習に基づく異常検出

各エンドポイントには、複数のリスク要因の加重平均である全体的な信頼スコアが割り当てられます。信頼スコアが低いほどリスクが高いことを示し、管理者が潜在的な脅威を特定して対応するのに役立ちます。

たとえば、 Cisco AI エンドポイント分析は、学生のラップトップが図書館のプリンタをスプーフィングして大学のネットワークに不正にアクセスしようとしているかどうかを検出できます。

図 25.　　Catalyst Center での Cisco AI エンドポイント分析の信頼スコアの詳細



AI を活用したエンドポイントの可視化、自動化されたセキュリティポリシーの適用、およびリアルタイムの脅威検出により、Cisco AI エンドポイント分析は、大学が安全でスケーラブルかつ効率的な IT インフラストラクチャを維持し、重要な学術データと研究データを保護すると同時に、学生と教職員にシームレスなデジタル体験を保証します。

大学のネットワークファブリック外のレイヤ 2 トラフィック終端

大学では、特定のネットワークセグメントに対してレイヤ 2 レベルのトラフィック検査を必要とする場合があります。この要件を満たすために、これらのセグメント内のすべてのトラフィックは、最初のホップが大学のネットワークファブリックの外部にある必要があります。この設定は、Catalyst Center と専用のレイヤ 2 ボーダーノードの組み合わせを使用して実装されます。トラフィックがファブリックを通過する間は VXLAN でカプセル化されたままですが、最初のゲートウェイはファブリックの外部に配置されます。

これを設定するには、必要なネットワークまたは SSID を Catalyst Center を介して展開します。さらに、対応する VN のために、ファブリックサイトのボーダーでレイヤ 2 ハンドオフを設定します。ファイアウォールまたはレイヤ 2 終端ポイントは、このハンドオフの受信側に配置されます。ファイアウォールには、ネットワークと同じサブネット内の IP アドレスが割り当てられます。IP アドレスを割り当てる DHCP サーバーは、ファブリックのエニーキャストゲートウェイ IP ではなく、ファイアウォールのレイヤ 2 終端 IP としてゲートウェイ IP を指定する必要があります。

これらの変更により、ファイアウォールの IP は VN 内のクライアントとして機能します。デバイスが IP アドレスを取得して通信を開始すると、最初のホップ（ファブリック外部のレイヤ 2 終端ポイント）がレイヤ 2 LISP を介して解決され、外部ネットワークとの通信が成功します。この設定により、大学のネットワークファブリックの外部で高度なレイヤ 2 トラフィック検査が可能になります。

図 26 と図 27 は、ボーダーノードでのレイヤ 2 VN の設定とレイヤ 2 ハンドオフを示しています。

図 26.　　Catalyst Center UI を使用したレイヤ 2 VN 設定

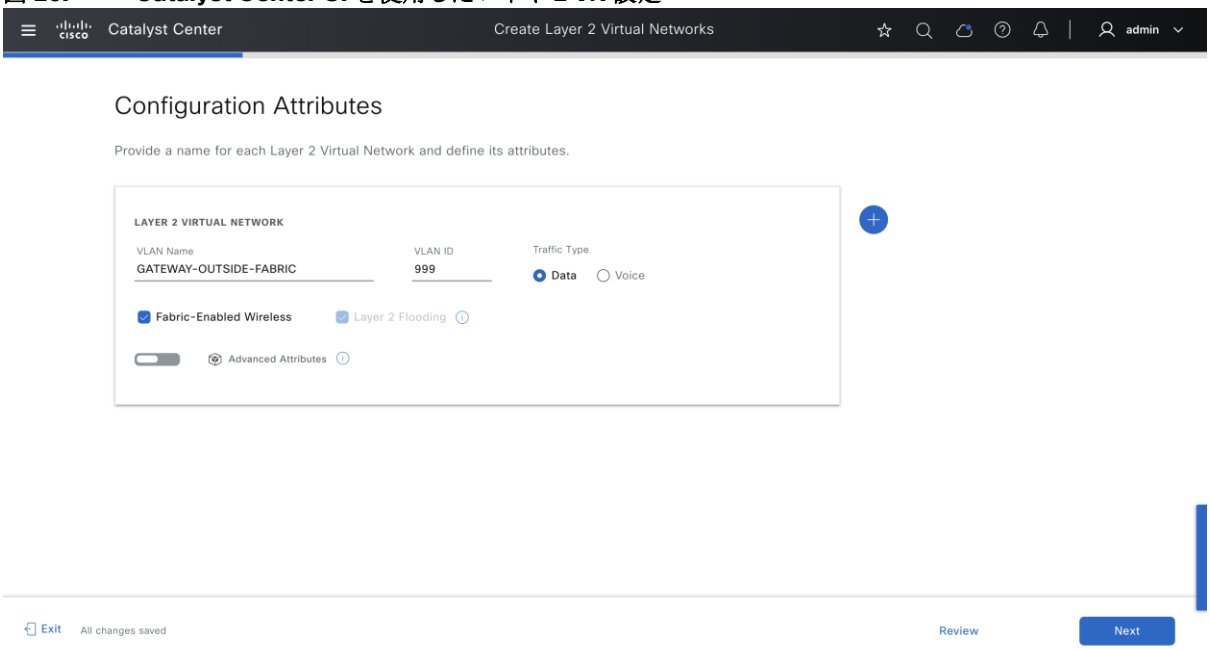
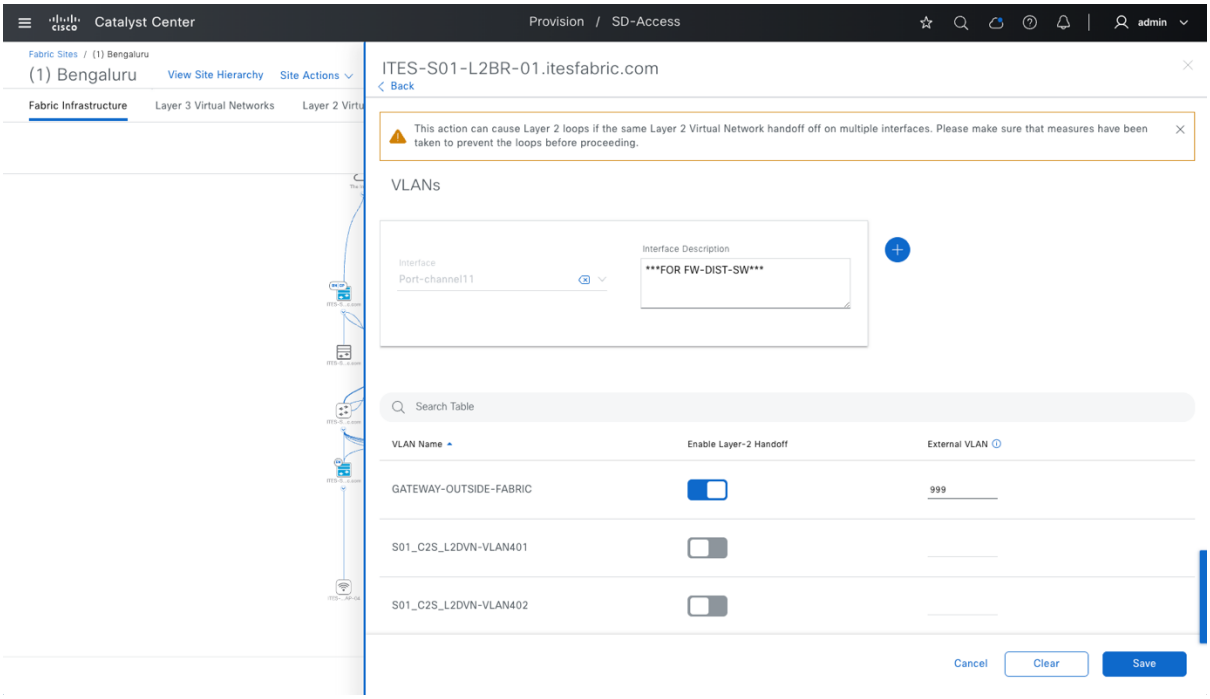


図 27.　　専用のレイヤ 2 ボーダーノードでのレイヤ 2 ハンドオフの実行



大学ネットワーク向け Wide Area Bonjour

近年、主要なベンダーがラップトップやモバイルデバイスで画面共有機能をサポートするようになり、この機能を持つクライアントの数が大幅に増加しています。この成長はマルチキャストソースの増加につながり、ネットワークテーブルのサイズに負担をかけています。これを管理するためには、ソースとレシーバーデバイスを規制することで、マルチキャスト環境を制御する必要があります。

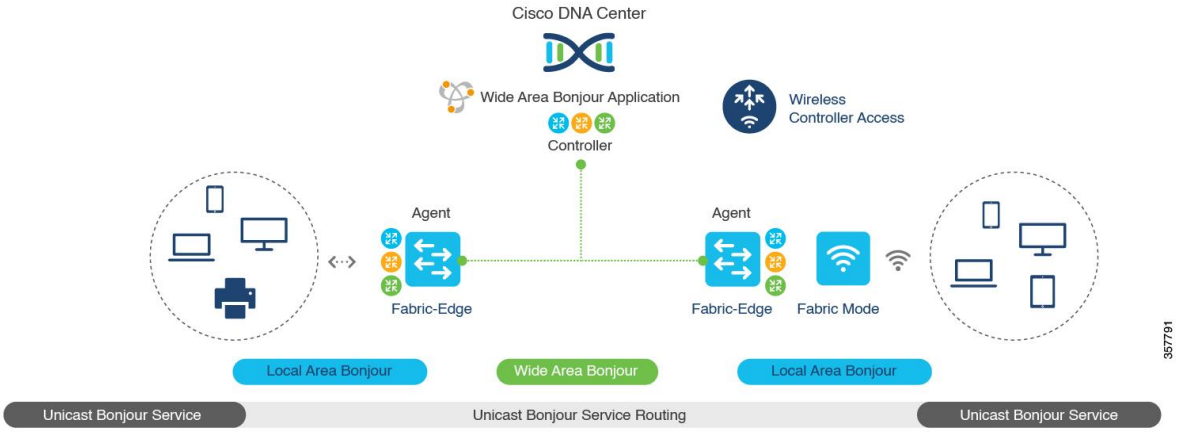
これには以下の 2 つの主な方法が役立ちます。

- ランデブーポイント（RP）と ACL を使用してストリームサブスクリプションを制限し、レジリエンスの高いマルチキャストネットワークを設計する。
- Cisco Catalyst Center Wide Area Bonjour（WAB）を利用して、トラフィックを制御および拡張する。

クライアントは仮想ネットワークで動作するため、マルチキャストトラフィックは VXLAN オーバーレイ内で伝送されます。Wide Area Bonjour を展開するには、その拡張性と、mDNS クライアントとの通信を容易にするサービス検出ゲートウェイ（SDG）の役割を理解する必要があります。Cisco SD-Access はファブリックベースのネットワーク全体で Bonjour サービスをサポートしており、Catalyst 9000 シリーズ スイッチを展開している大学にメリットをもたらします。VRF 認識の Wide Area Bonjour は、レイヤ 2 フラッディングなしで安全かつセグメント化された mDNS サービスの発見を可能にし、パフォーマンスと拡張性を向上させます。

大学における主要なユースケースは、ファブリックエッジスイッチが複数の場所にわたる有線およびワイヤレスユーザーにプリンタサービスを提供することです。これにより、学生や教職員は、物理的にプリンタの近くにいなくても、リモートで印刷できます。

図 28.　Cisco SD-Access 有線およびワイヤレスネットワーク設計



Catalyst Center での Cisco Wide Area Bonjour の設定

- Wide Area Bonjour アプリケーション

  Cisco Wide Area Bonjour は、Catalyst Center のデフォルトのアプリケーションではありません。このアプリケーションは、シスコのカタログサーバーからダウンロードしてインストールします。Cisco Wide Area Bonjour アプリケーションを正常にインストールしたら、Catalyst Center ホームページからメニューアイコンをクリックし、[Tools] をクリックしてアクセスできます。

- 手動またはテンプレートベースの設定

  Catalyst Center の Cisco Wide Area Bonjour アプリケーションは、サービス検出ゲートウェイ（SDG）エージェントスイッチまたはサービスピアデバイスに設定をプッシュしません。SDG エージェントとサービスピアは、手動で、または Catalyst Center のテンプレートエディタを使用して作成されたテンプレートを通じて設定する必要があります。

- グローバルサービスフィルタ

  最初のステップは、IP ネットワーク全体の信頼できる Cisco Catalyst SDG エージェントスイッチ間でサービス情報を動的に検出し配信することを Cisco Wide Area Bonjour アプリケーションに許可するグローバルサービスフィルタを実装することです。

- サービスフィルタの作成

  Cisco Wide Area Bonjour application アプリケーションから、管理者がサービスフィルタを追加するサービスドメインを選択し、アナウンスとクエリを許可するサービスタイプを選択します。管理者は、作成後にこの設定を編集、有効化、または無効化できます。

- ソース SDG エージェントの設定

  Cisco Wide Area Bonjour アプリケーションから、サービスをアナウンスする SDG エージェントと VLAN を選択します。管理者は、IPv4 または IPv6 ネットワークのサービスを有効または無効にすることができます。

- クエリ SDG エージェントの設定

  Cisco Wide Area Bonjour アプリケーションから、サービス（プリンタ）のクエリを受信する SDG エージェントと VLAN を選択します。管理者は、IPv4 または IPv6 ネットワークのサービスを有効または無効にすることができます。

図 29 から 30 は、Catalyst Center の Cisco Wide Area Bonjour ダッシュボード、SDG エージェント、およびサービスインスタンスを示しています。

図 29.　　Catalyst Center の Cisco Wide Area Bonjour ダッシュボード

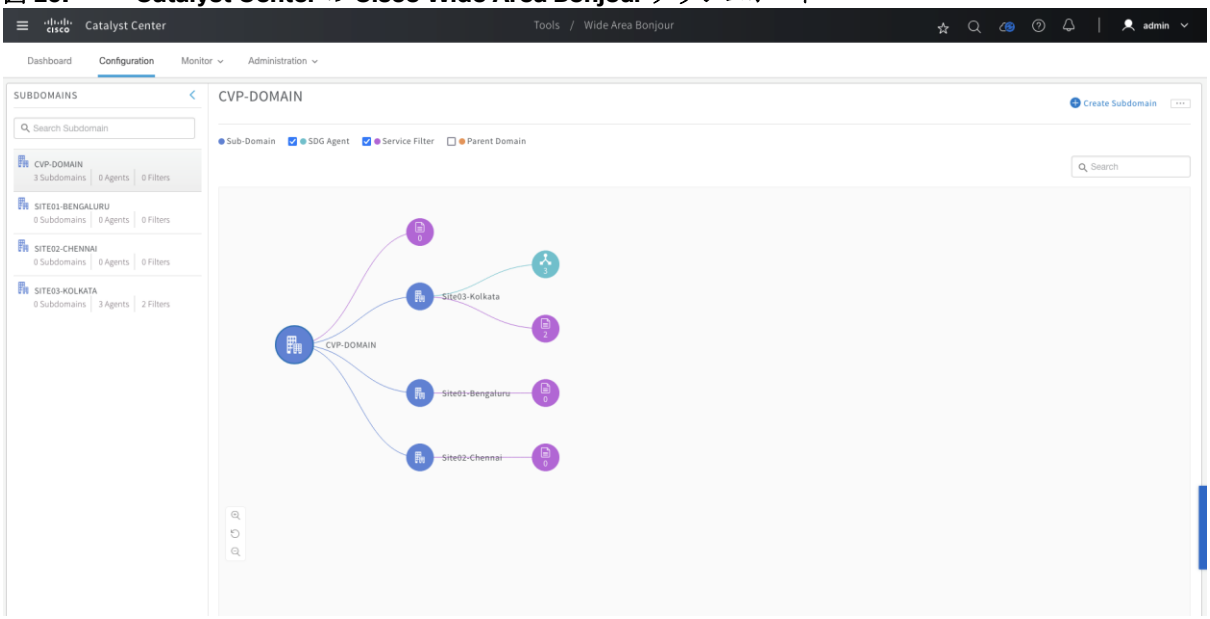


図 30.　Catalyst Center の SDG エージェントの詳細

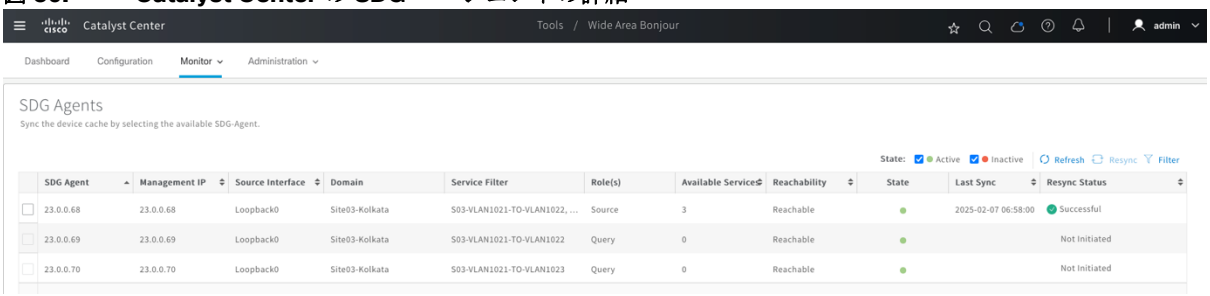
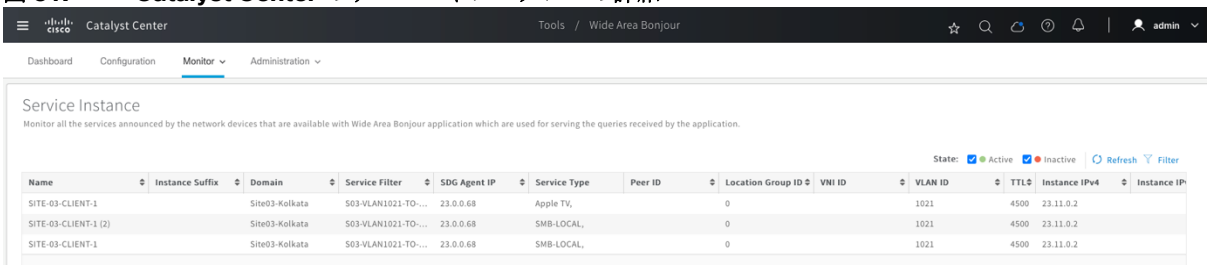


図 31.　Catalyst Center のサービスインスタンスの詳細



注：
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでグローバル ワイヤレス マルチキャスト モードを有効にする必要があります。シスコ ワイヤレス コントローラおよび AP は、デフォルトで、ワイヤレス ネットワーク インフラストラクチャと有線ネットワーク インフラストラクチャ間でレイヤ 2 またはレイヤ 3 のマルチキャストフレームを転送しません。

サービスフィルタのステータスが緑色の場合、ポリシーがアクティブであることを示します。ユーザーのラップトップが VLAN-B からリモートで接続すると、 VLAN-A で利用可能なプリンタサービスを検出してアクセスできます。

大学ネットワークにおける BYOD

Cisco ISE は、大学向けに BYOD 機能を提供し、学生や教職員が自身の個人デバイスを安全にキャンパスネットワークに接続できるようにします。ユーザーは、ネイティブサプリカントのプロビジョニング、またはデバイスポータルを通じてデバイスをオンボーディングできます。大学の管理者は、ジェイルブレイクやルート化されていない、コンプライアンスに準拠した安全なデバイスのみがネットワークにアクセスできるようにすることができます。このシステムは、ユーザー、デバイス、アプリケーションを可視化し、セキュリティポリシーを満たす許可されたデバイスのみが接続できるようにします。

シングル SSID BYOD では、ユーザーが安全な大学 WLAN に接続すると、デバイスがオンボーディングされます。自動再接続後、デバイスは同じ WLAN 上で完全なネットワークアクセス権を取得します。

大学環境における Cisco ISE BYOD 設定の主要なコンポーネントは以下の通りです。

- クライアント プロビジョニング ポリシー

  デバイスタイプまたはユーザーグループに基づいて、証明書テンプレート、SSID 名、プロキシ設定などを含む BYOD プロファイルを定義します。

- 認証および承認ポリシー

  オンボーディング中のユーザーポータル体験、認証方法、および必要なネットワークポリシーを決定します。

- エンドポイント オンボーディング

  デバイスは BYOD ポータルを介してオンボーディングプロセスを開始し、デジタル証明書を生成し、ネットワークプロファイルを設定します。Windows デバイスの場合、Cisco ISE は Network Setup Assistant

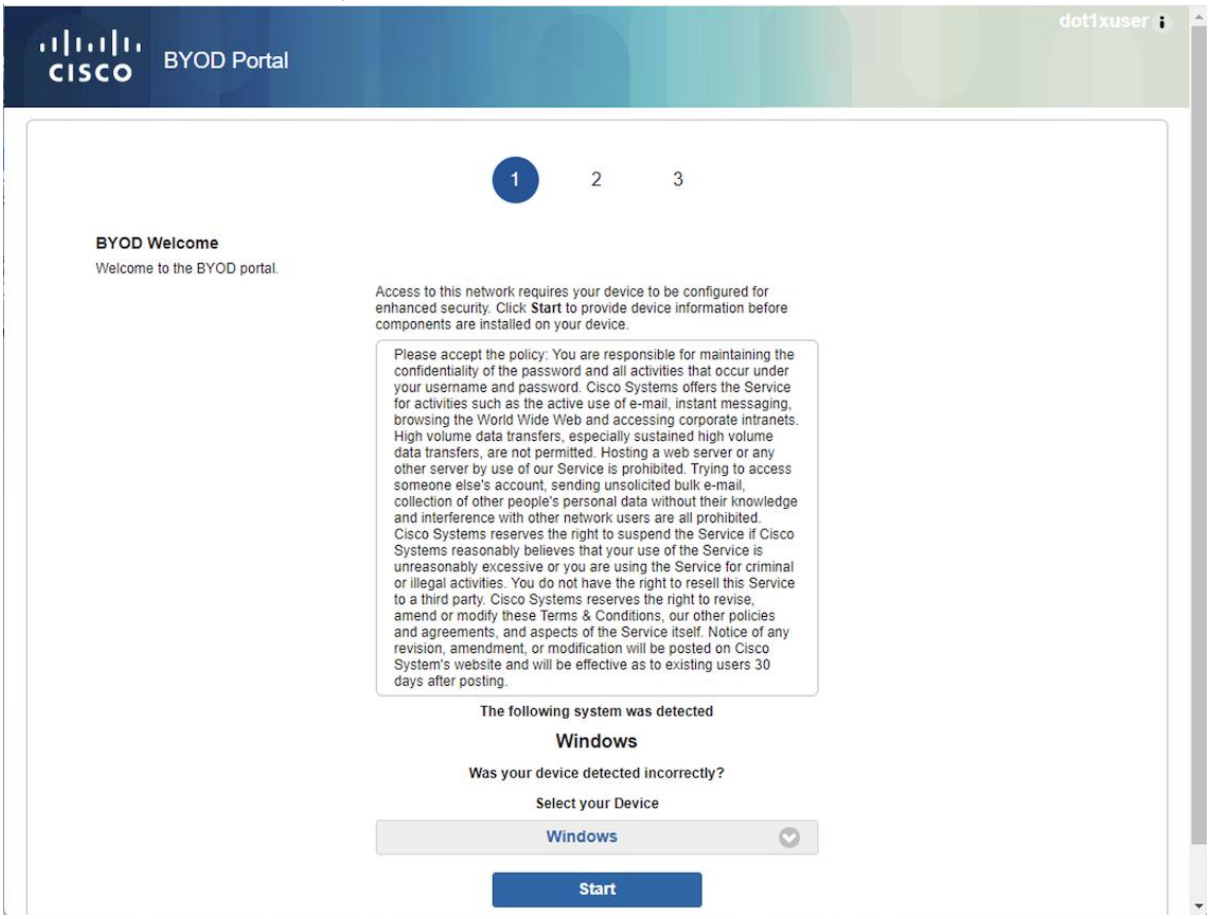
（NSA）（サプリカント プロビジョニング ウィザードとも呼ばれる）を活用して、オンボーディングを合理化します。管理者は、新しいオペレーティングシステムとの互換性を確保するために、NSA を定期的に更新する必要があります。

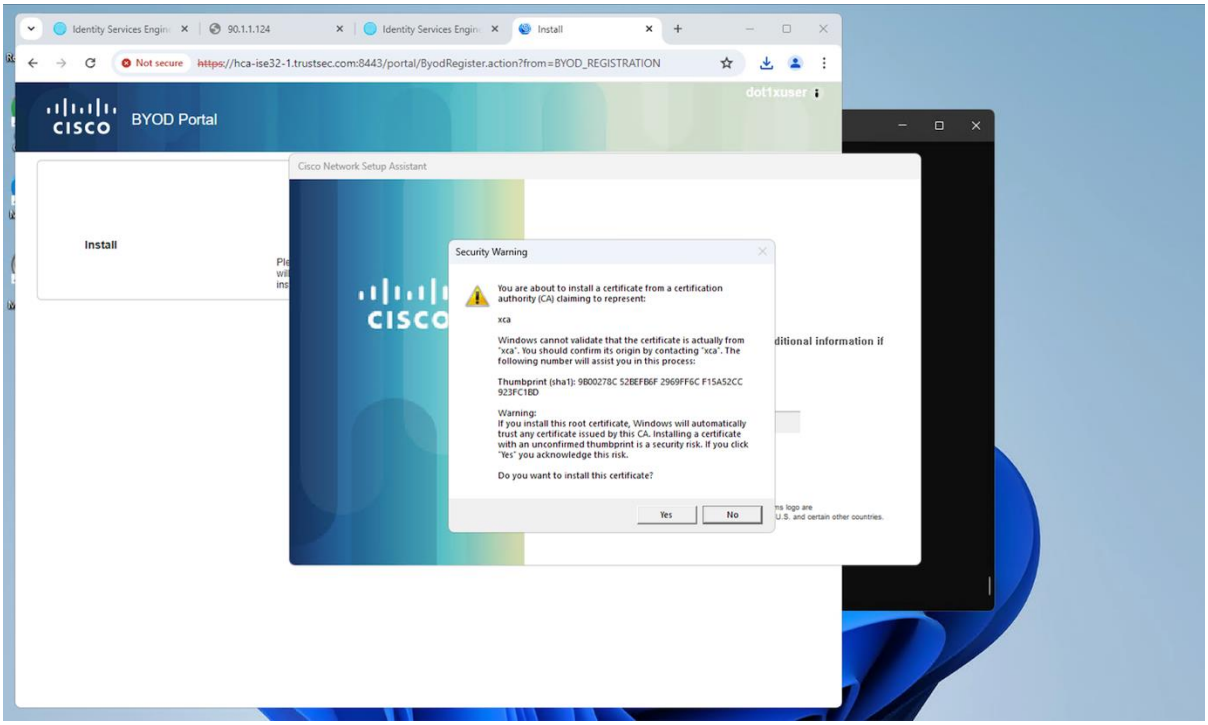
- ポスチャポリシー

  ポスチャは、 Cisco ISE のサービスです。ポスチャを使用すると、ネットワークへの接続を許可する前に、エンドポイントのコンプライアンス（ポスチャとも呼ばれる）をチェックできます。Cisco ISE AnyConnect ポスチャエージェントなどのポスチャエージェントは、エンドポイントで実行されます。クライアント プロビジョニング サービスは、エンドポイントが適切なポスチャエージェントを受信できるようにします。エンドポイントがコンプライアンスに対応し、正常にオンボーディングされると、ポータルはユーザーにフルアクセスが付与されたことを通知します。Cisco ISE がエンドポイントを BYOD デバイスとして登録している間、ユーザーはブラウザを開いて他の接続先に移動できます。図 32 は、クライアント プロビジョニング ワークフローを示しています。

図 32 は、Windows 10 ラップトップでの BYOD オンボーディングプロセスを示しています。

図 32.　　BYOD オンボーディング ワークフロー





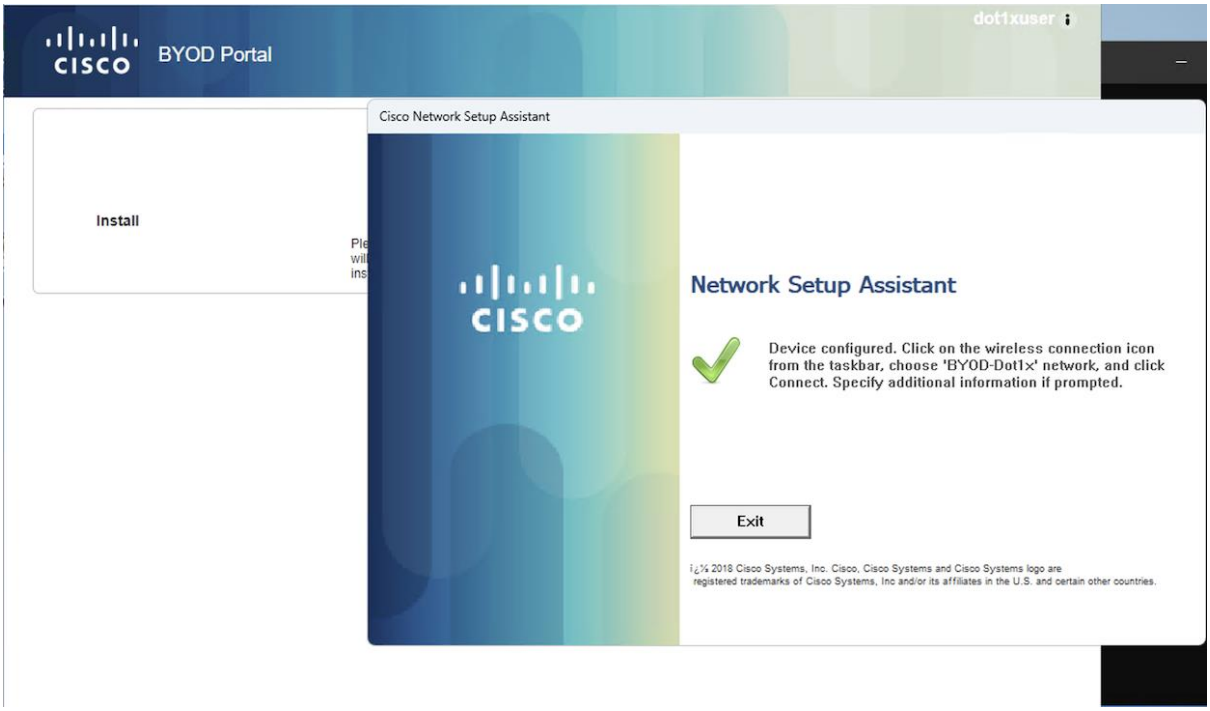
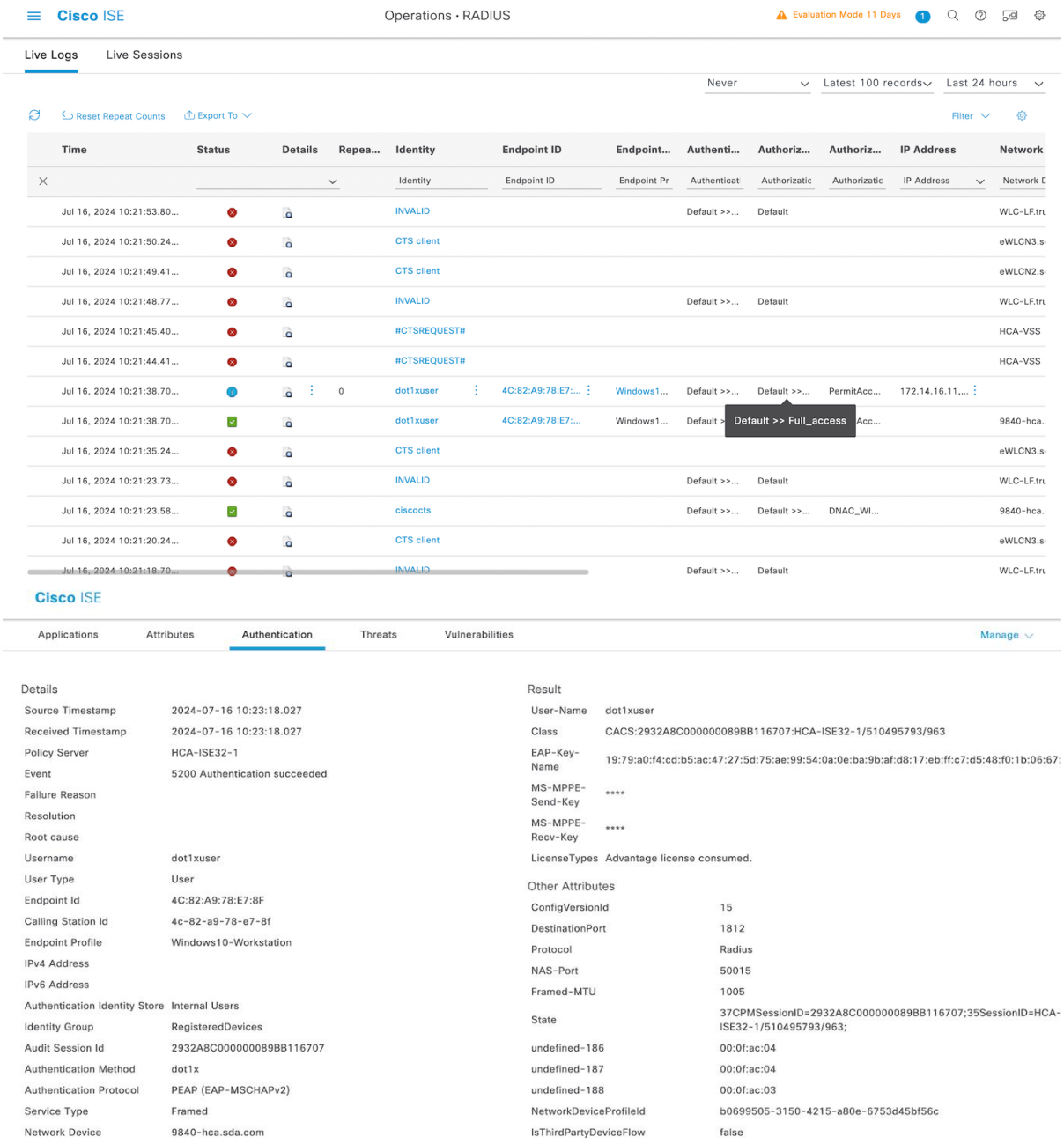


図 33 は BYOD デバイスの ISE 認証を示しています。

図 33.　BYOD デバイス認証



ハードウェアとソフトウェアの仕様

大学業界向けプロファイルは、表に記載されたハードウェアとソフトウェアを用いてテストされています。サポートされているハードウェアの完全なリストについては、『Cisco Software-Defined Access 互換性マトリックス』を参照してください。

ハードウェアまたはソフトウェアコンポーネント	サポートされているソフトウェアバージョン	
Catalyst Center アプライアンス （製品番号：DN2-HW-APL-XL）	2.3.7.7	2.3.7.9
Identity Services Engine（ISE）	3.3 パッチ 4	3.3 パッチ 4
コントロールプレーンノード Catalyst 9500 シリーズ スイッチ	17.9.5、17.12.4	17.9.6a、17.12.5、17.15.3
ファブリック ボーダー ノード： Catalyst 9200、9300、9400 シリーズ スイッチ	17.9.5、17.12.4	17.9.6a、17.12.5、17.15.3
ワイヤレスコントローラ Catalyst 9800-40 および 9800-CL	17.9.5、17.12.4	17.12.5, 17.9.6
Cisco SD-Access 拡張ノード CATALYST 9200 IE-4000	15.2(7)E10	17.15.3 15.2(8)E5

多方向スケール数

カテゴリ	値
デバイス インベントリ	2000
ファブリックサイトごとのデバイス	600
建物とフロア	3000
ファブリックサイトごとの VN	64
ファブリックサイトごとの IP プール	500
ファブリックサイトごとの WLC	2
ファブリックサイト	4
インベントリの AP	8000
エンドポイント	100,000（ワイヤレス 80,000、有線 20,000）
SSID	8
SDG	25
Bonjour サービスインスタンス	16,000

注： 公式にサポートされているスケールはこのデータシートに概説されおり、ここで提供されるデータはラボで検証されています。

関連するシスコのドキュメントへのリンク

- Cisco SD-Access Solution Design Guide (CVD)
- Catalyst Center のユーザーロール権限
- Implement Disaster Recovery
- Cisco Catalyst Center リリースノート
- Cisco Catalyst Center Security Best Practices Guide
- Software Defined Access (SD-Access) 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。