検証済みソリューション：医療業界

改訂：2022 年 10 月 12 日

医療向けソリューションの概要

このドキュメントの目的は、Cisco DNA Center と Cisco SD-Access を使用した一般的な医療向け展開プロファイルのガイダンスを示し、検証のための参考資料として提供することです。

医療業界では、遠隔医療や仮想診療の飛躍的な増加、リモートワークフォースの急増、セキュリティの懸念の高まり、一次医療モデルの急速な進化、医療提供サイトのシフト、従業員の安全と健康の優先度アップなど、大きな変化が起きています。

ここでは、進化を続ける大規模な医療ネットワークが今日の医療の要件を満たすために考慮する必要がある重要な事項について説明します。

サービスとネットワークの復元力

医療システムでは、長いダウンタイムは許容されないため、ネットワークレベルおよびサービスレベルの厳格な復元力が求められます。ネットワークレベルの復元力は、デュアル ファブリック ボーダー ノード、デュアル ファブリック コントロール プレーン ノード、デュアルアンカーボーダーおよび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、ハードウェアスタックまたは StackWise Virtual を備えたファブリックスイッチ、デュアル マルチキャスト ランデブー ポイント（RP）、デュアル ファブリック トランジット コントロール プレーン ノード（該当する場合）を含む堅牢なファブリックネットワーク設計で実現できます。サービスレベルの復元力は、次を展開することによって実現されます。

- Cisco DNA Center 3 ノードクラスタ。
- 複数のポリシー管理ノード（PAN）、モニタリングノード（MNT）、およびアクティブとスタンバイの Platform Exchange Grid（pxGrid）とポリシーサービスノード（PSN）を備えた分散型 Cisco Identity Services Engine（ISE）クラスタ。

ネットワークの拡張

医療ネットワークは、一般にいくつかの大規模なキャンパスサイトと多数の小規模なブランチサイトまたはクリニックサイトで構成されます。大手の医療サービスプロバイダーの場合、そのクリニックサイトは数百または数千にものぼります。遠隔医療や仮想診療の需要の急増に対応して、新しいクリニックサイトの動的な展開や既存のキャンパスおよびクリニックサイトの拡張に対する需要が高まっています。

Cisco DNA Center は、柔軟なサイトの追加とサイトの拡張を十分にサポートします。LAN 自動化機能には、新しいデバイスを検出し、既存のネットワークに多層式に接続する基盤となるレイヤ3ユニキャストおよびマルチキャストネットワークの作成を自動化するゼロタッチ プラグアンドプレイ ワークフローが用意されています。これらの新しく検出されたデバイスはインベントリに追加され、AAA設定でプロビジョニングして、ファブリックロールを持つファブリックに追加できるようになります。Cisco DNA Center には、拡張ノードデバイスを Cisco SD-Access ファブリックサイトに追加する独自のゼロタッチプラグアンドプレイ ワークフローもあります。このエンドツーエンドのワークフローは、検出から始まり、IP アドレスの割り当て、基本のプロビジョニング、ファブリックのプロビジョニングまで続きます。Cisco SD-Access 拡張ノードにより、病院の駐車場や倉庫のようなオフィス外のスペースへの接続が提供され、医療ネットワークの範囲が拡大します。また、ファブリックエッジスイッチを追加することなく、ポート密度が大幅に向上します。Cisco DNA Center には、Cisco SD-Access トランジット経由で新しいサイトにインターネットアクセスを提供する

ために、中央の場所にボーダーノードを設定するオプションがあります。このオプションを有効にすると、ローカルサイトからのインターネット宛てのすべてのトラフィックがローカルサイトのボーダーに転送され、次に中央のキャンパスサイトのボーダーを経由してから、ファブリックドメインの外に送信されるようになります。これにより、セキュリティポリシーの適用を一元化できるだけでなく、特に拡張環境において、新しいサイトの展開に柔軟性がもたらされ、運用オーバーヘッドも削減されます。

ネットワーク サービス

アンカーサービス：大規模な病院のネットワークの設計は、ほとんどの大規模キャンパスネットワークの設計とよく似ていますが、いくつかの違いがあります。病院の主な目的は、患者と訪問者にサービスを提供することです。病院のゲストサービスは、すべてのサイトにまたがり、常に大規模になる可能性があります。複数のサイトにまたがるすべてのワイヤレスゲストを安全かつ確実に処理することが運用上の課題となります。もう1つの違いは、病院のネットワークには、モニタ、ポンプ、医療用のステーション、サーバ、画像装置など、大量の医療機器が含まれていることです。これらのデバイスは異なる場所に設置されていることもありますが、L2 隣接関係を形成するには同じサブネットに属している必要があり、コントロールプレーンとデータプレーンの両方の観点から統一された方法で管理する必要があります。通常、個々のファブリックサイトにバインドされたエンドポイントはローカルサイトのアドレスプールから IP アドレスを受け取り、すべてのトラフィックがローカルサイトのボーダーを介して送信されます。そのため、各管理サイトのアドレス管理とポリシー適用が複雑になります。

Cisco DNA Center には、サイト間のサブネットの拡張を簡単に行えるマルチサイト リモート ボーダー ソリューションがあります。このソリューションは、サイト全体の有線エンドポイントとワイヤレスエンドポイントの両方に対して、固定された特定の仮想ネットワーク（VN）に対応するシンプルで一貫したアンカーサービスを提供します。アンカーサービスの場合、各分散サイトのアンカー VN に属するすべてのエンドポイントのトラフィックが集約され、Virtual Extensible LAN（VXLAN）を介して中央の場所（アンカーサイトのアンカーボーダー）にトンネリングされます。これにより、異なるサイトのクライアントに単一のサブネットを展開できます。このシンプルで一元化されたサブネット構造により、マルチサイト リモート ボーダー ソリューションは、マルチサイトの医療環境におけるサービスの展開を促進し、アンカートラフィックのクリーンでセキュアなセグメンテーションを実現します。

マルチキャストサービス：ほとんどの医療ネットワークは、医療用のコンピュータ、モニタ、セキュリティカメラ、画像分析機器など、医療スタッフや患者にサービスを提供する多数の幅広いデバイスに対応する必要があります。これらのデバイスによって生成されたデータは、ローカルとリモートの病院医療サーバの両方に保存する必要があります。このデータには、いつでもリアルタイムでアクセスできる必要があります。電子カルテサーバ、医療用画像処理サーバ、医療費請求サーバなどの各種サーバは、多くの場合、大規模な医療機関や医療研究センターのメインキャンパスまたは本部にある専用の医療サーバルームに配置されます。これらのサーバから分散キャンパスサイトの複数のエンドポイントにミッションクリティカルで時間が重視されるデータが配信されます。マルチキャストを有効にすると、医療サーバとエンドポイントデバイスの間のデータ通信に使用される帯域幅と CPU 使用率が最適化されます。

Cisco DNA Center には、オーバーレイとアンダーレイの両方で PIM Any-Source Multicast（PIM-ASM）と PIM Source-Specific Multicast（PIM-SSM）の両方を提供する多様なマルチキャストソリューションがあります。このソリューションは、さまざまなお客様のネットワーク設計に対応するように VN 単位で調整された 2 つの異なるマルチキャスト転送方式を提供します。1 つ目の方法はヘッドエンドレプリケーション（入力レプリケーション）です。アンダーレイネットワークでマルチキャストを必要としないため、クリーンなオーバーレイのみのマルチキャスト転送ソリューションが提供されます。もう 1 つの方法はネイティブマルチキャストです。マルチキャストレプリケーションがアンダーレイネットワーク全体で実行され、最もスケーラブルな帯域幅と CPU 効率が提供されます。

サイレントの医療機器の処理：医療ネットワークには、毎日、何千もの医療機器が接続しています。これらのデバイスのうち、一部のエンドポイントはサイレントホストに分類されます。これらのエンドポイントがサイレントから脱するには、通常、Address Resolution Prototol（ARP）ブロードキャストパケットを受信する必要があります。Cisco DNA Center

には、これらのサイレントホストをサポートするレイヤ 2 フラッディング機能があります。レイヤ 2 フラッディングは、特定のオーバーレイサブネットのブロードキャスト、リンクローカル マルチキャスト、および ARP トラフィックのフラッディングを可能にします。オーバーレイサブネットをアンダーレイの専用のマルチキャストグループにマッピングし、ターゲットのトラフィックをファブリックの VXLAN でカプセル化して、送信先のアンダーレイ マルチキャスト グループにトラフィックを送信します。アンダーレイでは PIM-ASM を使用します。これは、Cisco DNA Center の LAN 自動化ワークフローを使用して自動で設定するか、導入プロセスの後半で手動で設定できます。これにより、さまざまな組み込みの機能で幅広い医療機器に対応でき、医療ネットワークに大きな柔軟性がもたらされます。

セキュリティとネットワークのセグメンテーション

医療システムは、患者個人の医療記録と財務情報を保護する必要があります。米国では、病院や医療センターには、ネットワークトラフィックを完全かつ継続的に可視化できる HIPAA 準拠の有線およびワイヤレスネットワークを配備することが求められます。これらのネットワークで、悪意のあるデバイスがネットワークに侵入できないように、機密性の高いデータや医療機器（電子カルテ（EMR）サーバ、バイタルサインモニタ、看護師ワークステーションなど）を保護する必要があります。世界の他の地域でも、医療記録のプライバシーとセキュリティに関する同様の規制がすでに実施されています。

Cisco DNA Center と Cisco ISE は、Cisco SD-Access アーキテクチャ内で連動し、計画、設定、セグメンテーション、アイデンティティサービス、ポリシーサービスの自動化を実現します。Cisco ISE は Cisco DNA Center と動的に情報を交換しながら、デバイスプロファイリング、アイデンティティサービス、ポリシーサービスを提供します。

Cisco SD-Access ソリューションは、マクロセグメンテーションを使用することで、患者/訪問者のデバイスと医療/研究施設のデバイスのデータプレーンとコントロールプレーンを完全に分離するニーズに対応します。デバイスを異なるオーバーレイ仮想ネットワーク（VN）に配置することで、医療施設における完全なデータの分離を実現し、さまざまな部門やユーザにセキュリティを適用できます。

Cisco SD-Access は、グループベースポリシー（GBP）にスケーラブルグループタグ（SGT）によるマイクロセグメンテーションを使用して、同じ VN 内のエンドポイント間のデータプレーンの分離にさらに細かく対応できます。IT 管理者は、Cisco DNA Center でグループを作成し、従業員やデバイスをロールに基づいてグループに分け、それらのグループ間の通信を制御するポリシーを定義できます。

ネットワークのアシュアランスと分析

ネットワーク管理者は、医療システムの動的なニーズに迅速に対応するために、ネットワークを効率的に管理およびモニタできなければなりません。ネットワーク、デバイス、アプリケーションのパフォーマンスを向上させるには、テレメトリを使用してネットワーク関連やセキュリティ関連のリスクをプロアクティブに予測する必要があります。Cisco DNA アシュアランス は、Cisco AI Network Analytics を使用して、テレメトリデータを収集し、ネットワークデバイスのパフォーマンスと状態をモニタし、検出された問題にフラグを付け、修復手順を提示します。

管理者は、ネットワークアシュアランスを使用して、ネットワークデバイスと接続されたエンドポイント（有線とワイヤレスの両方）の全体的な状態をモニタできます。また、エンドポイントおよびアプリケーションアシュアランスを使用して、デバイス、エンドポイント、アプリケーションの個々の状態を確認できます。この詳細な分析により、管理者は、ワイヤレスラップトップや医療機器がワイヤレスネットワークに接続する際の問題など、ネットワーク要素が直面している個々の問題を特定できます。

エンドポイントの分析

最新のセキュリティ脅威は、ネットワークの有益な企業情報にアクセスするために悪用できる脆弱な侵入ポイントを探します。エントリポイントが侵害されると、わずか数秒でデバイスからデバイスへと侵害が拡大していきます。この種

の脅威を防ぐために、シスコの SD-Access ソリューションで実現されるような、きめ細かいネットワークセグメンテーションを行うことが推奨されます。医療ネットワークでは、さまざまなデバイスが複数の場所に分散しているため、ネットワーク内のすべてのデバイスを見つけて識別するのは時間がかかる煩雑な作業になります。シスコのエンドポイント分析を使用すると、種類、製造元、モデル、OS タイプ、通信プロトコル、ポートでデバイスを識別することで、この問題に対処できます。パッシブ ネットワーク テレメトリ モニタリングとディープ パケット インスペクションを使用してネットワークをスキャンし、それらの属性に基づいてデバイスを分類するプロファイリングルールを作成できます。Cisco DNA Center は、機械学習と連携してスプーフィングされたエンドポイントを検出し、管理者が適切なアクションを実行できるように支援します。

さらに、Cisco DNA Center はエンドポイントの分類属性を Cisco ISE と共有します。アイデンティティベースの認証で新しいデバイスがオンボーディングされると、製造元とタイプに基づいて自動的に識別され、該当するグループに追加されます。セキュリティポリシーの定義と適用は、個々のエンドポイントではなくグループに適用した方が簡単です。グループベースポリシーは、エンドポイントによるセキュリティ侵害などの新しい状況に合わせて簡単に更新でき、ネットワーク全体にグローバルに適用できます。

グループベースポリシーの分析

アクセスコントロール ポリシーの論理グループを作成するためのベースとして、デバイスタイプを把握する必要があります。グループベースポリシー分析（GBPA）は、グループ（SGT）間の相互の通信がわかるトラフィックパターンの全体像を提供します。この情報を使用して、管理者はポートとプロトコルをデバイスグループにマッピングし、ディープ パケット インスペクションを使用してトラフィック内のマルウェアを特定することで脅威に関する早期警告システムを構築できます。通信に別のポートやプロトコルを使用するようになったデバイスを疑わしいデバイスとして分離することができます。たとえば、医療機器として識別されたデバイスからコンプライアンスが重要な医療記録サーバへのトラフィックの送信が突然開始された場合、GBPA を使用して異常を特定できます。管理者は、異常なトラフィックパターンを確認した後、IT 部門が原因を調査するまでデバイスをブロックするようにポリシーを変更できます。

ハードウェアとソフトウェアの仕様

このソリューションは、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 Compatibility Matrix」を参照してください。

ロール	モデル名	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
Cisco DNA Center コントローラ	DN2-HW-APL-XL	Cisco DNA Center アプライアンス 3 ノードクラスタ	Cisco DNA Center 2.3.3.3
アイデンティティ管理、RADIUS サーバー	ISE-VM-K9	Cisco Identity Services Engine 仮想アプライアンス	Cisco Identity Services Engine 3.0 パッチ 5 または 3.1 パッチ 3
	SNS-3695-K9	ISE アプリケーション用の Secure Network Server（大規模）	

ロール	モデル名	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
Cisco SD-Access ファブリック コントロール プレーン ノード	ASR1001-X	Cisco 1000 シリーズ アグリゲーション サービス ルータ	17.6.2、17.8.1a
	C9500-24Y4C C9500-24Q C9300-48P C9300-24P	Cisco Catalyst 9300/9500 シリーズ スイッチ	17.6.2、17.8.1
Cisco SD-Access ファブリック ボーダー ノード	C9500-24Y4C C9500-40X C9500-12Q C9500-24Q C9300-48P C9300-24P	Cisco Catalyst 9300/9500 シリーズ スイッチ	17.6.2、17.8.1
Cisco SD-Access ファブリック エッジ ノード	C9300-48P C9300-24P C9404R	Cisco Catalyst 9300 シリーズ スイッチ	17.6.2、17.8.1
Cisco SD-Accessワイヤレス コントローラ	C9800-80-K9	Cisco Catalyst 9800-80 ワイヤレスコントローラ	17.6.2、17.8.1
Cisco SD-Access 拡張ノード	IE-3300-8P2S	Cisco Catalyst IE3300 高耐久性シリーズ	17.6.2、17.8.1
	IE-4010-4S24P	Cisco Catalyst IE4010 高耐久性シリーズ	15.2(7)E1a
	WS-C3560CX	Cisco Catalyst 3560-CX スイッチファミリ	15.2(7)E1a
Cisco SD-Access ポリシー拡張ノード	IE-3400H-16T	Cisco Catalyst IE3400 高耐久性シリーズ	17.6.2、17.8.1
	C9300-48P	Cisco Catalyst 9000 シリーズ スイッチ	17.6.2、17.8.1

ソリューションの導入例のシナリオ

医療業界のプロファイルについて、次のユースケースを実施しています。医療業界向けソリューションのテストベッドの論理トポロジについては、トポロジ （10 ページ）の図を参照してください。

- Cisco DNA Center を使用してインテントベース ネットワークを実装：
  - 管理者は、グローバルネットワーク階層を設計し、グローバルおよびサイトレベルのネットワーク設定を構成し、デバイスを自動的にプロビジョニングできます。
  - 管理者は、冗長性と拡張性を考慮して、デュアルボーダーとデュアル 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を展開できます。
  - 管理者は、デバイスのオンボーディングに自動化を活用することで、キャンパスおよびブランチサイトを柔軟に拡張できます。
    - ゼロタッチ プラグアンドプレイ LAN 自動化を使用してファブリックエッジをオンボーディング。
    - ゼロタッチ プラグアンドプレイを使用して IoT デバイス接続用にクラシック拡張ノードをファブリックにオンボーディング。
    - SGT の直接サポートと拡張トラフィック適用によりポリシー拡張ノードをファブリックにオンボーディング。
  - 管理者は、さまざまなボーダーオプションを使用して、多数の小規模なクリニックブランチサイトを自動的にプロビジョニングできます。
    - 組み込みのワイヤレスが有効でハードウェアスタックを備えた一体型ファブリック（FiaB）。
    - 組み込みまたはスタンドアロンのワイヤレスコントローラを備えた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。
  - 分散キャンパスサイトは、Cisco SD-Access トランジットを使用して共有のデータセンターやインターネットサービスに接続できます。
- 複数の Cisco DNA Center インスタンスを単一の Cisco ISE クラスタで統合：
  - 管理者は、仮想ネットワーク、スケーラブルグループタグ、アクセス契約、およびセキュリティポリシーを作成者ノードで一元管理し、自動的にリーダーノードと同期できます。
  - 管理者は、ポリシーオブジェクトの一貫性を損なうことなく、異なる Cisco DNA Center インスタンスでロールの変更（作成者ノードの昇格など）を実行できます。
  - ポリシー適用の検証と認可変更（CoA）について、複数の Cisco DNA Center インスタンスで構成される環境のデバイスに Cisco ISE を使用して正常に展開できます。
- 機密性が高い医療データを保護する多層セキュリティを実装：
  - 管理者は、ネットワークでの脅威の拡散を制限するために、ユーザ、ゲスト、IoT デバイス、医療機器を適切な論理ネットワークにセグメント化できます。

- 管理者は、不正アクセスを防ぐために、有線およびワイヤレスのエンドポイントに対してクローズド認証オンボーディング（dot1x）または MAC 認証バイパス（MAB）を有効にできます。
- 管理者は、グループを作成し、ユーザやエンドポイントを（アイデンティティに基づいて）グループに分け、グループ間のトラフィックを制御するグループベースポリシーを定義できます。
- 管理者は、病院のキャンパスに大規模なアクセスコントロールポリシーを実装できます。クライアントのオンボーディング時にセキュリティグループ ACL（SGACL）がエッジデバイスに適切にインストールされます。
- 管理者は、監査ログを使用して Cisco DNA Center のアクティビティをモニタできます。監査ログには、発生したシステムイベント、発生した時刻と場所、開始したユーザが記録されます。
- 管理者は、Cisco DNA Center へのアクセス権限が異なる詳細なロールベースのユーザを作成できます。

- サービスとネットワークの復元力：
  - デュアル Cisco SD-Access ボーダーとデュアル コントロール プレーン ノード、ボーダー SVL とボーダー/エッジスタック、およびトランジットネットワークのデュアル トランジット コントロール プレーンにより、ネットワーク全体でハイアベイラビリティを実現できます。ネットワーク障害後のフェールオーバーとリカバリで、トラフィックフローがほとんどまたはまったく中断されません。
  - 管理者は、3 ノード ハイ アベイラビリティ モードで Cisco DNA Center を設定できます。Cisco DNA Center クラスタでサービスやノードの障害が発生した場合、システムはユーザの介入なしで回復します。
  - Cisco ISE の分散展開モデルは、PAN、PSN、pxGrid サービスのフェールオーバー後に回復します。
  - 管理者は、Cisco ISE に到達できない場合にファブリックエッジに重要な VLAN を実装できます。
  - 管理者は、Cisco DNA Center の設定とデータのバックアップを特定の時間に実行するようにスケジュールしたり、オンデマンドでバックアップを開始したりできます。管理者は、以前の Cisco DNA Center の設定を復元するためにバックアップファイルを復元できます。

- シンプルな管理：
  - Cisco DNA Center により、デバイスインベントリが一元管理され、ユーザは IP アドレス、インストールされているソフトウェアバージョン、プロビジョニングステータス、インベントリ情報などのデバイス情報を確認できます。
  - 管理者は、Cisco DNA Center のソフトウェアイメージ管理（SWIM）機能を使用して、スイッチ、ルータ、拡張ノード、およびワイヤレスコントローラを選択したゴールデンイメージにアップグレードできます。
  - Cisco DNA Center のファブリックボーダーとコントロールプレーンの RMA ワークフローにより、デバイスの交換がシームレスになります。
  - サイトのボーダーの L3 ハンドオフによる VLAN の消費の最適化により、管理者が拡張マルチサイト環境で VLAN を割り当てる際の柔軟性がもたらされます。
  - LAN 自動化の重複プールオプションにより、異なるファブリックサイトのアンダーレイネットワークで同じアドレスを再利用することが可能になり、IP アドレスの使用が大幅に最適化されます。

- ネットワークサービス：

- 管理者は、ファブリックサイト全体のワイヤレスエンドポイントにゲストサービスを提供するために、中央の場所にマルチサイト リモート ボーダーを実装できます。ゲストトラフィックはゲスト VN 内で分離され、インターネットアクセスのためにアンカーボーダーにトンネリングされます。
- マルチサイト リモート ボーダー ソリューションで、複数のファブリックサイトの有線エンドポイントに同じサブネットを使用できます。
- 異なる場所にデュアルアンカーボーダー/CPがあるアンカーサイトを実装して、ネットワーク障害が発生した場合の冗長性を確保できます。
- メインキャンパスサイトおよびリモートサイトで有効になっているマルチキャストサービスをさまざまな設計オプションで設定できます。
  - RP は、Cisco SD-Access ファブリックの外側にあり、ファブリックボーダーから到達可能です。
  - PIM-ASM は、オーバーレイ仮想ネットワークのマルチキャストサービスに対して有効です。
  - PIM-SSM は、アンダーレイネットワークのネイティブマルチキャストに対して有効です。
  - メイン キャンパス ファブリック サイトのボーダーは、Cisco SD-Access トランジットネットワークを介して分散キャンパスサイトにマルチキャストサービスを提供できます。
  - サーバルームのマルチキャスト送信元は、異なるファブリックサイトのマルチキャスト受信者を含むトランクを使用してエッジノードおよびボーダーノードに接続されます。
- 管理者は、ファブリックサイト内のブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）トラフィックだけでなく、サイレントの医療機器を処理する L2 フラッディングを有効にすることができます。

- Cisco DNA アシュアランスとアナリティクスを使用してネットワークとクライアントをモニタ：
  - 管理者は、アシュアランスを使用してネットワークの状態をモニタし、ネットワークの問題を特定できます。アシュアランスは、リンクのダウン、APのダウン、スイッチスタックメンバーのダウンなど、さまざまなネットワーク障害に起因する問題を報告できます。
  - 管理者は、アシュアランスを使用して有線クライアントとワイヤレスクライアントの状態をモニタし、クライアントのオンボーディングの問題を特定できます。
  - 管理者は、テレメトリデータロガー（TDL）ベースのアシュアランスを有効にして、クライアントの状態を報告する際のスケールとパフォーマンスを向上させることができます。
  - 管理者は、多数の同時エンドポイントをモニタできます。アシュアランスチャートには、100,000 の同時エンドポイントと 250,000 の一時エンドポイントの情報が表示されます。
  - 管理者は、Cisco AI エンドポイント分析を使用して、エンドポイントと IoT デバイスを識別およびプロファイリングできます。
  - 管理者は、ワイヤレスセンサーを使用してワイヤレスネットワークのパフォーマンスをモニタできます。
  - 管理者は、アプリケーションテレメトリを有効にし、アシュアランスを使用してアプリケーションの遅延、ジッター、パケットドロップをモニタできます。

- 管理者は、既存のエンドポイント間の通信を可視化して、新しいアクセス制御の導入の必要性と影響を評価できます。
- 管理者は、Cisco AI エンドポイント分析を使用して（エンドポイントの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たエンドポイントを検出し、適切なアクションを実行できます。
- 管理者は、GBPA の機能を使用して、トラフィックパターンやプロトコルを確認できるほか、トラフィックフローを許可または拒否するマイクロセグメンテーション ポリシーを作成および実装できます。

ソリューション環境

トポロジ

医療業界向けソリューションのテストトポロジには、病院の地域 1 と地域 2 をそれぞれ管理する 2 つの Cisco DNA Center 3ノードクラスタがあります。これらはシスコの複数の DNA Center として設定され、同じ分散 ISE クラスタと統合されます。シスコの分散型 ISE クラスタ展開には、2 つのポリシー管理ノード（PAN）、2 つのモニタリングノード（MnT）、pxGrid、および複数のポリシーサービスノード（PSN）が含まれます。

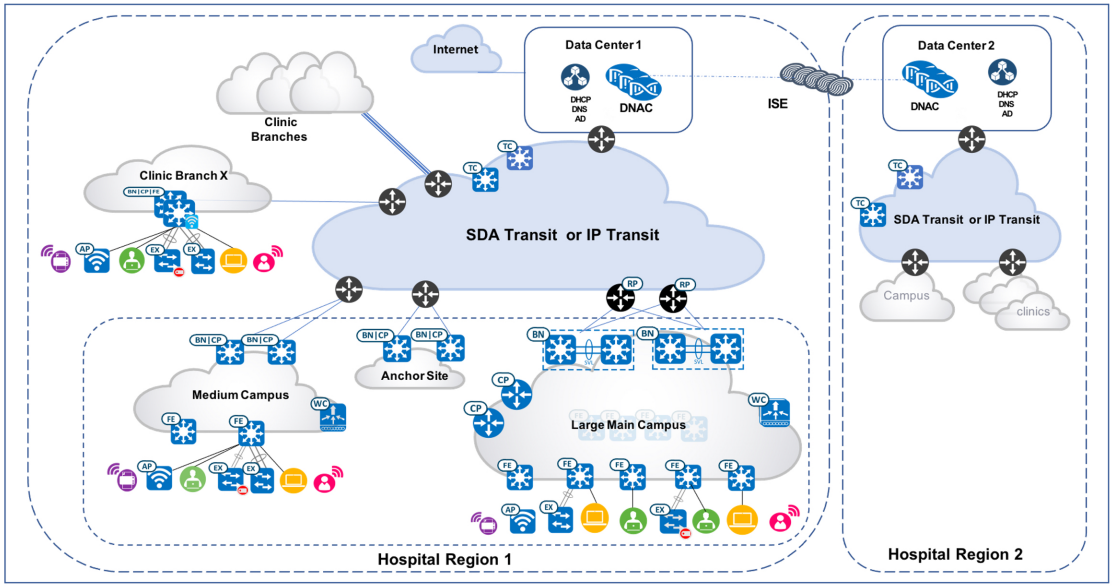
各 Cisco DNA Center クラスタは、1 つの大規模な病院のメインキャンパスサイト、1 つの中規模なキャンパスサイト、1 つのアンカーサイト、および一体型ファブリック（FiaB）を備えた 500 の小規模なクリニックブランチサイトで構成されるファブリックを管理します。分散キャンパスを接続するために Cisco SD-Access トランジットが展開されています。遠隔地のクリニックブランチは IP ネットワークを介してメインキャンパスに接続されます。図 1 は、医療業界向けソリューションのテストベッドの論理トポロジを示しています。

ファブリックのサイトは次のとおりです。

- 大規模キャンパスメインサイトには、デュアルボーダー、専用のデュアル コントロール プレーン ノード、デュアル WLC、100 のファブリックエッジがあります。
- 中規模サイトには、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、WLC、ファブリックエッジ、拡張ノードがあります。
- 小規模サイトには、組み込み WLC と拡張ノードを使用したハードウェアスタッキングに FiaB があります。
- アンカーサイトには、デュアル共存アンカーボーダーおよびコントロールプレーンノードがあり、複数のファブリックサイトにアンカーサービスを提供します。
- Cisco 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。メインキャンパスサイトのボーダーは、Cisco SD-Access トランジットを介して他のキャンパス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。

次の展開例では、外部 RP を使用した Cisco SD-Access マルチキャストを構成し、ファブリック内にあるサーバルームを複数のキャンパスサイトに展開しています。大規模なファブリックサイトでは、可能な限り最適なネットワークパフォーマンスを実現するためにネイティブマルチキャストを展開しています。小規模なファブリックサイトでは、サイト管理をシンプルにするためにヘッドエンドマルチキャストを展開しています。

図 *1*: ソリューションのテスト論理トポロジ



スケール番号

ソリューションのテストでは、次の表に示すスケールの数値について確認しました。Cisco DNA Center アプライアンスのスケールの数値については、Cisco DNA Center のデータシートを参照してください。

カテゴリ	値
デバイスインベントリ	5,000
ファブリックサイトあたりのデバイスの数	100
複数の Cisco DNA Center アプライアンス	2
建物とフロアの数	2000
ファブリックサイトあたりの VN の数	64
ファブリックサイトあたりの IP プール数	500
ファブリックサイトあたりの WLC の数	2
ファブリックサイトの数	502
インベントリ内の AP の数	13000
エンドポイントの数	100,000（有線 50,000、無線 50,000）
SSID の数	10
SGT の数	4000

ソリューションの重要事項

このセクションでは、医療業界プロファイルのソリューションの検証に関する主なテクニカルノートについて説明します。

段階的なサイトの展開と拡張

医療ネットワークには当然多くのサイトがあり、新しい場所へのネットワーク拡張の需要が常にあります。Cisco DNA Center の自動化ワークフローは、Cisco SD-Access が有効な新しいファブリックサイトを複数の場所に展開するための、コスト効率が高く、柔軟でスケーラブルなソリューションを提供します。医療業界向けソリューションで新しい Cisco SD-Access サイトを拡張するために実行したワークフローを次に示します。

- **メインサイトから分散キャンパスに Cisco SD-Access トランジット経由でインターネットアクセスと共有サービスを提供**：新しく展開されたファブリックサイトは、共有サービス（Cisco DNA Center、Cisco ISE クラスタ、DNS、AD、DHCP サーバなど）、ファブリックサイト全体の同じ VN 内のサービス、およびインターネットアクセスの各ドメインに到達できる必要があります。Cisco DNA Center は、新しいファブリックサイトの完全な到達可能性をシームレスに実現する、Cisco SD-Access トランジットによる最適化されたスケーラブルなソリューションを提供します。
    - **新しいファブリックサイトのインターネットアクセスの有効化**：一般的な医療機関の大規模展開では、本部またはメインキャンパスのサイトは、インターネットに直接接続されたボーダーまたはデータセンターのファイアウォールを介してインターネットにアクセスします。新しいファブリックの展開をシンプルにするために、Cisco DNA Center のボーダー設定ワークフローには、[This site provides internet access to other sites through SDA Transit] というオプションがあります。このチェックボックスをオンにすると、ローカルサイトのボーダーが、ローカルサイトだけでなく、同じファブリックドメイン内の Cisco SD-Access トランジット経由で接続された他のすべてのファブリックサイトに対するデフォルトゲートウェイとして機能します。医療機関の大規模展開では、大規模キャンパスと同様に、メインキャンパスサイトのサイトボーダーが [This site provides internet access to other sites through SDA Transit] オプションを選択して設定されます。展開された新しいファブリックサイトでは、メインキャンパスサイトのサイトボーダーを介して不明なトラフィックやインターネットアクセスを即座にルーティングできます。次の 2 つの図は、分散サイトにインターネットアクセスを提供するメインキャンパスサイトの GUI ワークフローとパケットフローを示しています。

図 *2*：リモートサイトのインターネットアクセスを提供する *GUI*

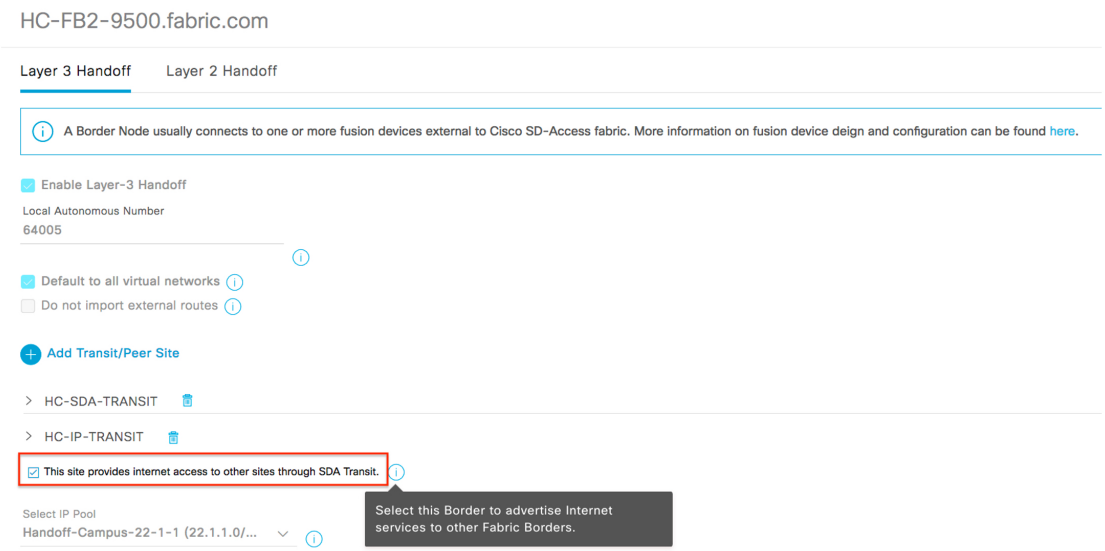
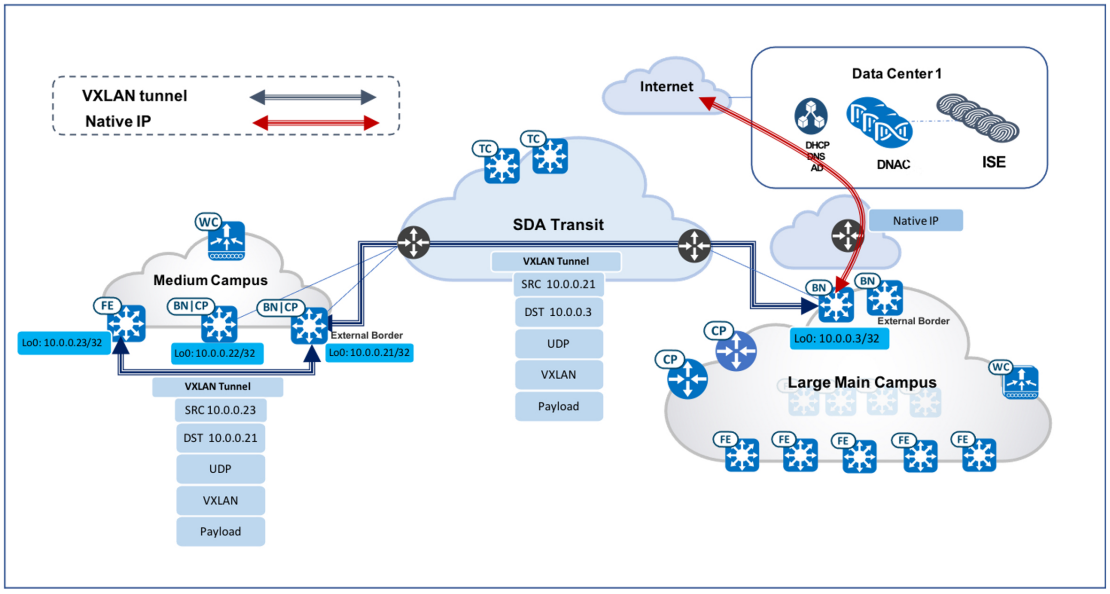


図 *3*：分散キャンパスサイトでの *Cisco SD-Access* トランジットを介したインターネットアクセスのパケットフロー



- **Cisco SD-Access トランジットの有効化**：新しいキャンパスサイトのサイトボーダーを設定する際に、Cisco SD-Access トランジットを有効にして、トランジット コントロール プレーン ノードを指定します。Cisco SD-Access を有効にする一般的なワークフローについては、『Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide』を参照してください。トランジット コントロール プレーン ノードは、ファブリック間の通信を処理し、集約プレフィックスをボーダーノードの RLOC に関連付けます。サイトローカル コントロール プレーン ノードは、ファブリック内の通信を処理し、エンドポイント ID（EID）をファブリック エッジノードに関連付けます。サイト間のデータトラフィックは、マクロ（VN）およびマイクロ（SGT）ポリシー構造を持つファブリック VXLAN カプセル化を使用してサイト間でカプセル化されます。Cisco

SD-Access トランジットを有効にすると、新しく展開されたファブリックサイトは、同じ VN 内のサービスについてサイト間で通信できます。これらの新しいサイトは、VN 間の適切なルートリークを通じて、中央のファブリックサイトの共有サービスにもアクセスできます。

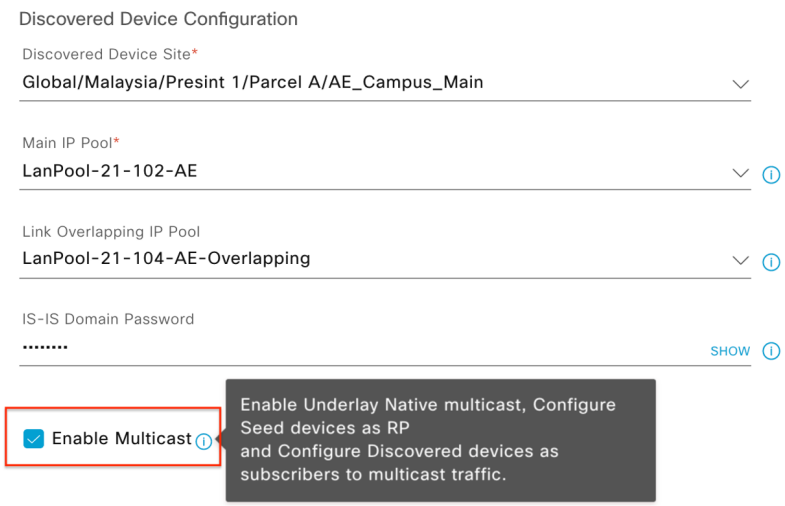
- **オフィス外のスペースの拡大**：新型コロナウイルスに対応する中で、医療の現場は大きく変わりました。その結果、医療システムは駐車場や倉庫などの屋外スペースに医療サービスを移してきました。Cisco SD-Access 拡張ノードは、レイヤ 2 ポート拡張を提供し、既存のファブリックエッジノードへのポート密度を高めることでモビリティを実現します。また、それらのスイッチに接続されたエンドポイントにセグメンテーションとグループベースポリシーを提供します。Cisco DNA Center は、拡張ノードを検出してプロビジョニングし、ファブリックに追加するためのゼロタッチ プラグアンドプレイ自動化ワークフローを提供します。

  Cisco DNA 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）の 2 つがあります。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 Cisco DNA 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。Cisco SD-Access 拡張ノードの展開の詳細については、『Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide』を参照してください。

- **アンダーレイマルチキャストの有効化**：将来のファブリック マルチキャスト サービスの導入に備え、物理アンダーレイネットワークでマルチキャストを有効にすることが不可欠です。LAN 自動化ワークフローでアンダーレイマルチキャストを有効にすることを強く推奨します。このワークフローには、新しいデバイスのアンダーレイ PIM-ASM 設定を自動化するオプションがあります。このワークフローでは、シードデバイスで Loopback60000 を作成し、このアドレスをアンダーレイ マルチキャスト ネットワークのデフォルト RP として使用します。次の図は、LAN 自動化ワークフローでアンダーレイマルチキャストを有効にするための GUI 画面を示しています。

図 *4 : LAN* 自動化でのアンダーレイマルチキャストの有効化



病院の有線およびワイヤレスエンドポイント向けアンカーサービス

医療機関では、多くの場合、すべてのサイトにまたがる大規模なゲストサービスを管理する必要があります。通常、ゲストエンドポイント（個々のファブリックサイトにバインドされたエンドポイント）はローカルサイトのアドレスプールから IP アドレスを取得し、すべてのトラフィックがローカルサイトのボーダーに送られます。そのため、複数サイトでのアドレス管理とポリシー適用が複雑になります。この課題に対処するために、Cisco DNA Center は VN アンカーを利用したマルチサイト リモート ボーダー ソリューションを提供しています。このソリューションでは、複数のサイトの VN からのトラフィックを集約し、単一の共通のサブネットを使用して中央の場所（アンカーサイト）に戻すことができます。その VN に対してサイトごとのサブネットを定義して使用する必要はありません。VN アンカーは、シンプルで一元化されたサブネット構造により、マルチサイトでのゲストサービスの展開を促進します。また、大規模な医療環境におけるゲストトラフィックのセキュアで一貫したセグメンテーションを実現します。

アンカーサービスを使用すると、各サイトのアンカー VN に属するすべてのエンドポイントのトラフィックが集約され、VXLAN を介してアンカーサイトにある中央のアンカーボーダーにトンネリングされます。アンカーサイトは従来のファブリックサイトと非常によく似ていますが、特定の VN にサービスを提供する仮想ファブリックサイトを形成します。この仮想ファブリックサイトには独自のサイトボーダーとコントロールプレーン（アンカーボーダーと CP）があり、それらがアンカーサイトに配置されます。アンカーサイトの特別な点は、このサイトのエッジとワイヤレスコントローラが複数のファブリックサイトに分散していることです。

マルチサイト リモート ボーダーは VN 単位で有効になります。アンカー VN（Guest_VNなど）の場合、アンカーサイトのすべてのエッジは、コントロールプレーンとデータプレーンの通信にアンカー CP/ボーダーを使用します。アンカーサイトのワイヤレスコントローラは、ワイヤレスエンドポイントの登録のためにアンカー CP と通信します。アンカーされていない従来の VN の場合、エッジおよびワイヤレスコントローラは、コントロールプレーンとデータプレーンの通信に独自のサイトローカル CP/ボーダーを使用します。ファブリックロールで動作するデバイスの他の RLOC と同様に、アンカーボーダー/CP ノードのループバック 0 アドレスは、アンカーサイトに配置されたエッジノードのグローバル ルーティング テーブルにある /32 ルートを介して到達可能である必要があります。

ワイヤレスゲストでマルチサイト リモート ボーダーが有効になっている場合、ゲストエンドポイントはゲスト SSID に参加し、Cisco ISE を介して中央 Web 認証（CWA）を完了し、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されたボーダーにトンネリングされ、ファイアウォールを通過してインターネットに到達します。次の 1 つ目の図は、マルチサイト リモート ボーダーを有効にするための Cisco DNA Center の GUI 画面を示しています。2 つ目の図は、アンカー VN と非アンカー VN の両方のパケットフローを示しています。

図 *5 : VN* アンカーの有効化

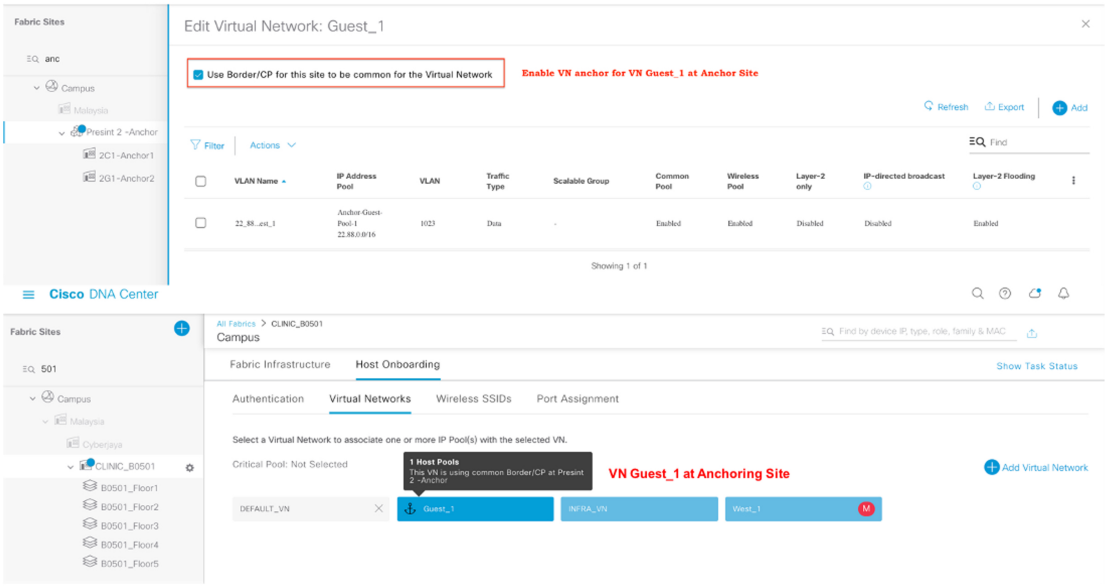
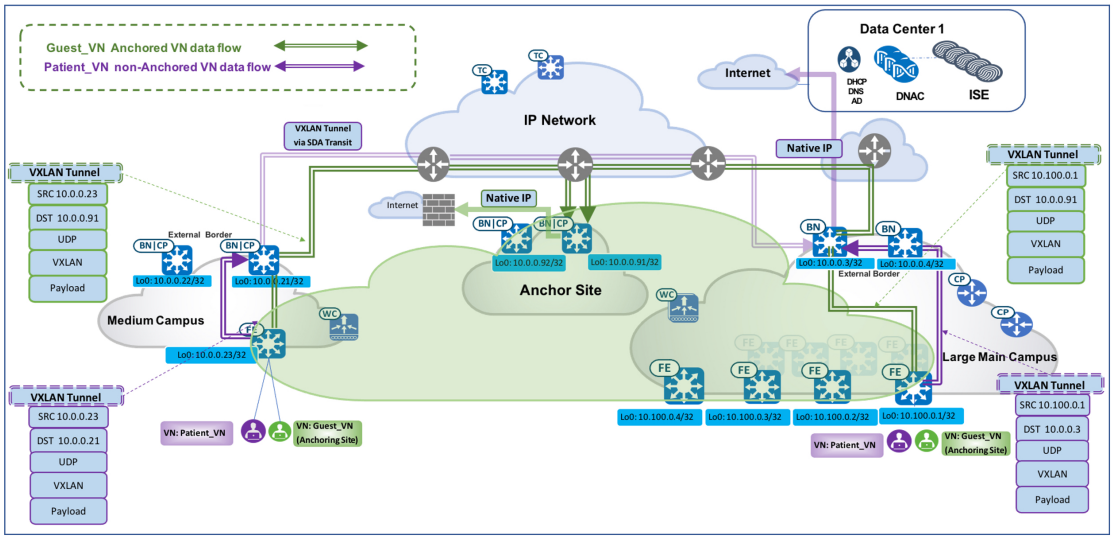


図 *6 :* アンカー *VN* と非アンカー *VN* のデータパケットフロー



医療サーバルーム：複数サイト間のマルチキャスト

Cisco SD-Access は、仮想オーバーレイネットワークと物理アンダーレイネットワークの両方で、マルチキャストの PIM Any-Source Multicast（PIM-ASM）と PIM Source-Specific Multicast（PIM-SSM）をサポートします。マルチキャスト送信元は、ファブリックドメイン外（通常はデータセンター内）またはファブリックオーバーレイ内（通常はエッジノードまたは拡張ノードに直接接続）のいずれかになります。マルチキャスト受信者は、通常、すべてのファブリックサイトのエッジノードまたは拡張ノードに直接接続されます。

Cisco DNA Center は、さまざまなお客様のネットワーク設計に対応するように VN 単位で調整された 2 つの異なるマルチキャスト転送方式を提供します。1 つ目の方法はヘッドエンドマルチキャスト（入力レプリケーション）です。アン

ダーレイネットワークでマルチキャストを必要としないため、クリーンなオーバーレイのみのマルチキャスト転送ソリューションが提供されます。もう1つの方法はネイティブマルチキャストです。マルチキャストレプリケーションがアンダーレイネットワーク全体で実行されるため、最もスケーラブルな帯域幅と CPU 効率が提供されます。

（注） マルチキャスト転送は VN 単位で有効になりますが、特定のファブリックサイト内で 2 つの転送方式を同時に有効にすることはできません。

医療業界向けの設計で検証した使用例のシナリオを次に示します。これは、Cisco DNA Center を使用した大規模なマルチサイト病院ネットワークでのマルチキャストの展開を示しています。このシナリオでは、医療サーバルームが大規模メインキャンパスサイトのオーバーレイのファブリックエッジに接続されています。サーバルームのサーバがマルチキャスト送信元です。それぞれ異なる VN にあり、患者、管理者、医療スタッフ、医療実習生など、さまざまな対象者にサービスを提供します。受信者は分散キャンパスサイト全体に位置しています。図 7 では、マルチキャスト受信者は病院の大規模メインキャンパスサイトと中規模キャンパスサイトに存在しています。ランデブーポイント（RP）がファブリックの外部にあるため、既存のファブリックサイトと新しく展開されたファブリックサイトの両方に一貫してサービスを提供できます。

マルチキャストの使用例の対応する要件は次のとおりです。

- 異なる VN の複数のサーバ（マルチキャスト送信元）を大規模メインキャンパスサイトのトランクポートを介して単一のファブリックエッジに接続する。
- マルチキャスト送信元と同じキャンパスサイトからのマルチキャスト受信者を展開する。
- マルチキャスト送信元と異なるキャンパスサイトからのマルチキャスト受信者を展開する。
- Cisco SD-Access トランジットを分散キャンパスサイト全体に展開する。
- マルチキャスト RP をファブリックの外部に配置する。

これらの要件を満たす検証済みのソリューションを次に示します。

- **サーバ接続用のトランクポートの展開**：ファブリックホストのオンボーディングのポート割り当てワークフローに、接続されたデバイスタイプをトランクとして設定するオプションがあります。その結果、エッジノードまたは拡張ノードのスイッチポートがトランクとして設定されます。これにより、サーバルームのサーバを VLAN タグが異なるファブリックエッジに接続できます。
- **ヘッドエンド レプリケーションによるマルチキャストの展開（オーバーレイの PIM-ASM）**：前述のように、マルチキャストのヘッドエンド レプリケーションがオーバーレイネットワークで実行され、マルチキャストインユニキャスト カプセル化が実行されます。このサーバルームの場合、分散サイトのボーダーはファーストホップルータ（FHR）になり、オーバーレイの各マルチキャストパケット（S、G）が複製されます。VXLAN トンネル（FHR_RLOC、LHR_RLOC）を介して、該当するサブスクライバを含むすべてのラストホップルータ（LHR）にユニキャストでパケットが送信されます。小規模なキャンパスサイトでは、多くの場合、エッジがファブリックボーダーに直接接続されます。このオプションは、トポロジがシンプルであり、サイトのボーダー（FHR）で過剰な帯域幅のオーバーヘッドが発生しないため、小規模なファブリックサイトに適しています。また、アンダーレイマルチキャストを設定する必要がないため、運用上のオーバーヘッドが大幅に軽減されます。

  拡張ノードに複数の受信者が接続されている場合（IGMP スヌーピング機能がデフォルトで有効になっている場合）、拡張ノードは受信者が接続されているすべてのポートでパケットレプリケーションを完了します。図 7 で

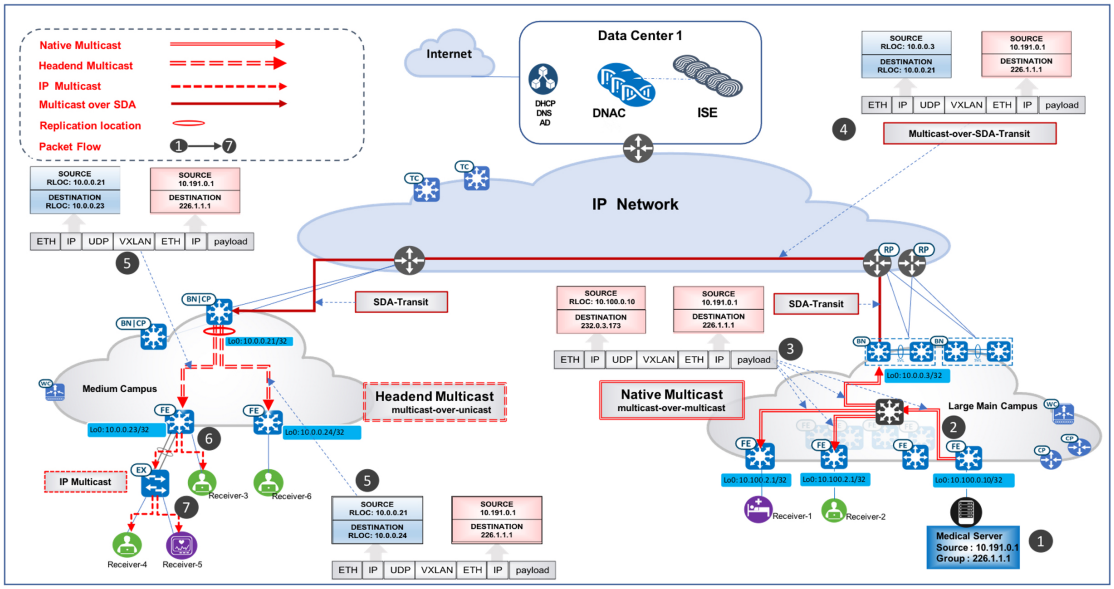
は、転送オプションとしてヘッドエンド レプリケーションを使用した小規模ファブリックサイトにおけるパケットデータの詳細なパスを示しています。

- **ネイティブマルチキャストの展開（オーバーレイの PIM-ASM、アンダーレイの PIM-SSM）**：ネイティブマルチキャストでは、FHR に依存せずにパケットが複製されます。中間ノードを含むアンダーレイ全体がパケットレプリケーションに参加します。パケットは、アンダーレイの Source Specific Multicast（SSM）ツリーの分岐点ごとに複製されます。つまり、受信者に最も近いノードでパケットが複製され、必要なときにのみ複製されます。このオプションは、FHR およびネットワークの残りの部分の帯域幅と CPU 効率が最大になるため、大規模なキャンパスサイトに適しています。

  ネイティブマルチキャストでは、アンダーレイマルチキャスト転送に PIM-SSM が必要であり、FHR でマルチキャストオーバーマルチキャスト カプセル化が実行されます。このサーバルームの場合、マルチキャスト送信元（医療サーバ）がエッジに接続されているため、ファブリックエッジが FHR です。FHR は、オーバーレイのマルチキャストパケット（S_overlay、G_overlay）を受信すると、このパケットをアンダーレイのマルチキャストパケット（S_underlay、G_underlay）のペイロードとしてトンネリングします。そこから、アンダーレイの SSM ツリーを使用してパケットレプリケーションを完了します。図 7 では、転送オプションとしてネイティブマルチキャストを使用したメインキャンパスサイトにおけるパケットデータの詳細なパスを示しています。

- **SD-Access トランジットを介したファブリックサイト間のマルチキャスト**：分散した医療キャンパスサイトは、Cisco SD-Access トランジットを介して RP およびマルチキャスト送信元と通信します。PIM パケットは、最初にローカルキャンパスサイトのボーダーに送信され、次に VXLAN 経由でメインキャンパスサイトのボーダーにトンネリングされます。その後、メインキャンパスサイトのボーダーから、IP トランジットを介して RP（この場合はファブリックの外部）に転送されるか、VXLAN を介して送信元（医療サーバ）が配置されているエッジに転送されます。サイト間でのマルチキャストデータ転送では、Cisco SD-Access トランジットも使用します。図 7 では、大規模メインキャンパスサイト内の医療サーバから大規模メインキャンパスサイトと中規模キャンパスサイトの両方の受信者に送信されるマルチキャストデータパケットの詳細なパスを示しています。

図 7：*Cisco SD-Access* マルチサイト間のマルチキャスト データ パケットのパス：ファブリックエッジのサーバルーム



テレメトリベースのアシュアランスへの移行

医療機関は、多数の医療機器とユーザを管理しています。検査室、処置室、および診察室には、多くのデバイス端末やモニタが設置されています。Cisco DNA Center では、ファブリック有線エンドポイントについて、通常はインベントリおよび SNMP ベースのポーリング方法を使用して、Cisco DNA Assurance のヘルスページで提供されるヘルスデータを取得、モニタ、レポートします。Cisco DNA Center バージョン 2.1.2.0 以降では、NETCONF を使用したテレメトリによるアシュアランスデータの収集がサポートされます。この新しいメソッドであるテレメトリデータロガー（TDL）ベースの有線アシュアランスは、拡張性とパフォーマンスに優れ、よりリアルタイムのステータスレポートを提供するため、有線クライアントの状態のモニタに推奨されます。医療業界については、現在の Cisco DNA Center のリリースにおいて、50,000 の有線ファブリッククライアントでインベントリから TDL ベースのアシュアランスへの移行が完了しています。

ファブリックデバイスで TDL ベースのアシュアランスに移行すると、ネットワークで Power Over Ethernet（PoE）テレメトリと分析も有効になります。Cisco DNA アシュアランス の PoE のページで、[PoE Operational State Distribution]、[PoE Powered Device Distribution]、[Power Load Distribution]、[PoE Insights] の各カテゴリについて PoE 対応デバイスをモニタできます。この情報は、ネットワーク内の全サイトのすべての PoE デバイスについて、配電および電力使用の詳細に関する包括的な情報を提供します。

Cisco SD-Access の関連ドキュメント

- Cisco SD-Access Solution Design Guide (CVD)
- Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide
- Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide
- Cisco Software-Defined Access Compatibility Matrix

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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。