検証済みプロファイル：医療機関

(Cisco SD-WAN)

2026 年 3 月 4 日

ドキュメントの目的と使用方法

このドキュメントの目的は、シスコが推奨する医療機関向けの一般的な展開プロファイルの概要を示すことです。Cisco Catalyst SD-WAN を使用する一般的なファブリック展開のガイドラインを提供し、プロセス中に参照できる検証ドキュメントとして機能します。デプロイエンジニアは、このドキュメントの理論に関する項と実践に関する項を一緒に使用して、サービス要件を把握するために役立て、展開および設定中にネットワークに最適な決定を行うことができます。

ターゲット層

この医療プロファイルの対象者は、ネットワークのエンジニアリングと運用を担当する技術スタッフ、および実装チームです。

ソリューションの概要

医療機関は、小規模なクリニックから複数の地域にまたがる大規模な病院まで、世界中で何千ものブランチを運営しています。それぞれの拠点に独自の要件がある一方、医療機関のネットワーク環境には、セキュリティ、強化されたネットワークサービス、効率的なネットワーク管理、シームレスなモビリティ、ネットワークの高可用性（HA）、ロケーションサービスなど、一連の特殊なニーズがあります。このドキュメントで取り上げるトピックでは、進化を続ける大規模な医療機関ネットワークで今日の要件を満たすために考慮する必要がある重要事項について説明します。

シスコのソフトウェア定義型 WAN（Cisco SD-WAN）は、オンプレミス、クラウドホスト型、およびクラウド提供型のオーバーレイ WAN アーキテクチャを可能にし、企業のデジタル化とクラウド化を支援します。特にクラウドホスト型アーキテクチャは、医療機関のお客様のネットワークプロファイルに強く関連します。それにより、WAN コストの大幅な削減、サービスのデプロイに要する時間の短縮、アプリケーションのレジリエンシの向上、およびハイブリッドネットワークのための堅牢なセキュリティアーキテクチャが実現します。

Cisco SD-WAN は、以下に示すように、企業における多数の重要な問題を解決します。

- トランスポートに依存しない WAN を低コストで確立し、多様性にも対応する
- セキュアな制御とデータプレーン接続を提供する
- ビジネスクリティカルなリアルタイム アプリケーションのサービスレベル契約（SLA）を満たす
- 企業の重要なコンピューティングリソースを保護するために、エンドツーエンドのセグメンテーションを提供する
- プライベート/パブリッククラウドにシームレスに拡張する
- Zone-Based ファイアウォールを使用して、ブランチからのダイレクト インターネット アクセスを提供する

Cisco SD-WAN では、（パブリックまたはプライベート）クラウド内にコントローラを配置することで、データプレーンとコントロールプレーンを分離します。

このドキュメントでは、医療機関向けに構築された企業ソリューションプロファイルについて取り上げ、その機能を説明します。

セキュリティ

Cisco SD-WAN ソリューションにより、ルータと制御コンポーネント間のセキュアな制御通信と管理通信が可能になります。WAN エッジルータ間のデータプレーン通信は、IPsec カプセル化に基づく暗号化と保護が行われます。

ハイブリッドトランスポート

このプロファイルには 2 つのデータセンターがあり、各データセンターには 2 つの SD-WAN ルータがあります。データセンターのすべての SD-WAN ルータは、インターネットおよびマルチプロトコル ラベル スイッチング（MPLS）トランスポートに接続されています。

ブランチにはさまざまな接続モデルがあります。

- ハイブリッドモデル：デュアル トランスポート インターネットおよび MPLS
- 単一サイト：インターネットまたは MPLS への単一トランスポート
- デュアルサイト：TLOC 拡張を使用したデュアルトランスポート

セグメンテーションと Zone-Based ファイアウォール

セグメンテーションと Zone-Based ファイアウォール（ZBFW）のために、ブランチ内に複数のセグメントを設けることができます。Cisco SD-WAN を使用すると、ユーザーはブランチ内とオーバーレイ上でセグメントを分離することができます。このプロファイルでは、4 つの VPN セグメントが定義されています。

- 営業 VPN（VPN 2）：企業の営業担当者および関連デバイス用
- 医療 VPN（VPN 3）：医療スタッフおよび医療業務専用で、重要な医療機関アプリケーションをサポート
- ゲスト VPN（VPN 10）：ゲスト Wi-Fi および訪問者アクセス用で、企業の内部通信から分離
- 研究開発（R&D）VPN（VPN 20）：研究開発施設および機密性の高い調査業務用
- 管理 VPN（VPN 511）アウトオブバンド管理通信用

Zone-Based ファイアウォールは、ゲスト Wi-Fi VPN から DIA への通信用に展開されます。

ポリシーベースのハブアンドスポークトポロジ

データセンターとブランチ間のハブアンドスポークトポロジを確立するために、集中型ポリシーが展開されます。

トポロジ図に示すように、あるセットのブランチはデータセンター 1（DC-HUB-1）からのデフォルトルートを選択し、別のセットのブランチはデータセンター 2（DR-Hub-1）からのデフォルトルートを選択しています。

QoS

すべてのデバイスで Quality of Service（QoS）が設定されています。WAN の帯域幅は、さまざまなタイプのアプリケーション間で適切に分散されます。音声については、WAN インターフェイスで専用の帯域幅が割り当てられ、低遅延キューに配置されます。他の通信クラスは、重みの割り当てに基づいて、残りの帯域幅を共有します。

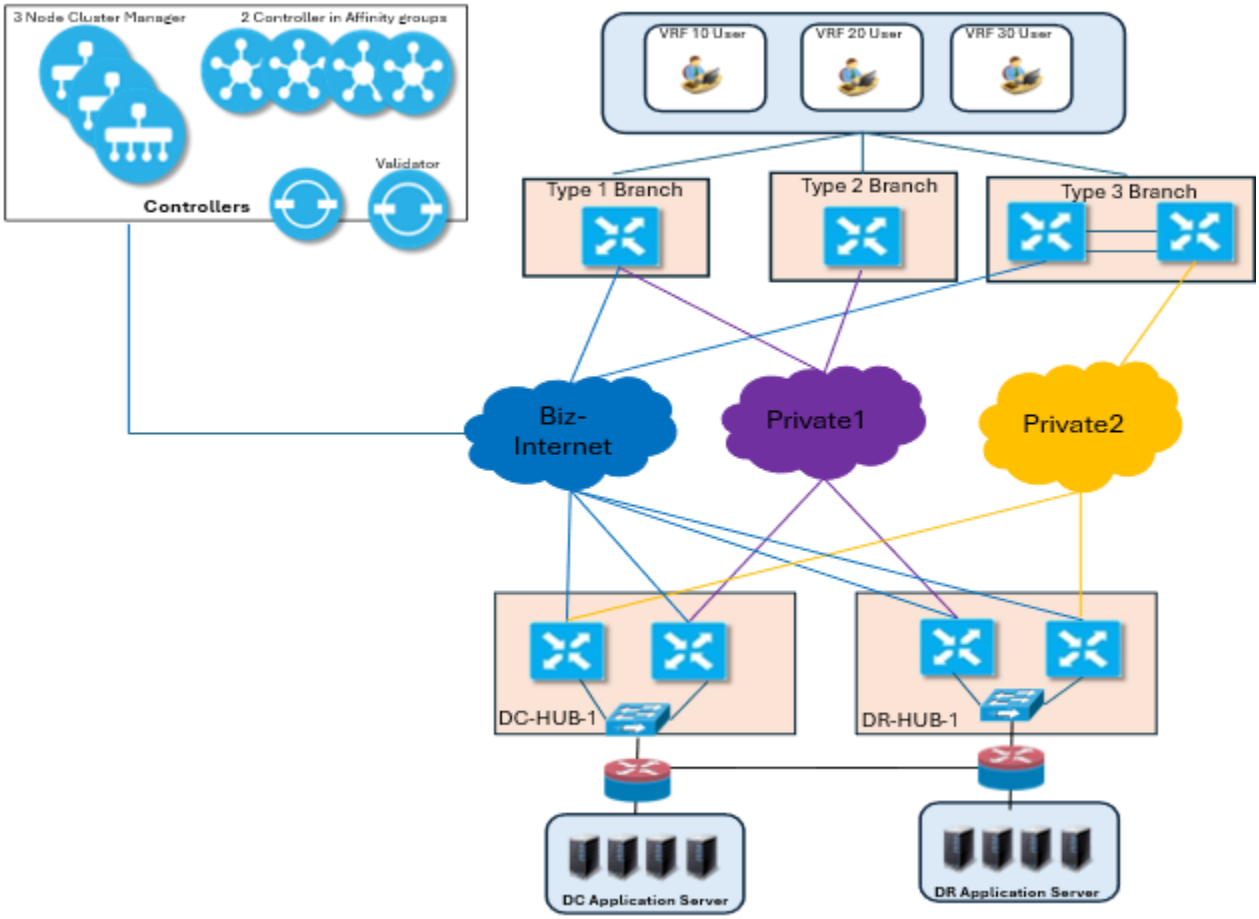
SLA に基づくアプリケーション認識型ルーティングポリシー

ハイブリッドサイト用の集中型ルーティングポリシーでは、定義済みの SLA に基づいて音声通信用の MPLS が優先される一方、ベストエフォート型通信はインターネット経由でルーティングされます。

ブランチ用の Dynamic Host Configuration Protocol（DHCP）サーバー

ブランチ内の WAN エッジルータは、クライアントに IP アドレスを割り当てるための一部のセグメント用の、Dynamic Host Configuration Protocol（DHCP）サーバーとして設定されます。

トポロジ



ハードウェアの詳細

ハードウェアデバイス	ロール	トンネル数
C8500-12X4QC	DC HUB	4000
ASR1002-HX	DR HUB	4000
ISR4451-X	T1 スポーク	8
ISR4461/K9	T2 スポーク	8
C8200-1N-4T	T3 スポーク	8
C8300-1N1S-4T2X	T3 スポーク	8

プロファイル内での主な機能

ロール	機能
ブランチ	QoS、DPI、ZBFW、NAT、BGP、OSPF、マルチキャスト、アフィニティ、オンデマンドトンネル、VRF、SNMP
ハブ	QoS、DPI、マルチキャスト、アフィニティ、SNMP、VRF
SD-WAN Manager	クラスター、SDAVC、機能テンプレート、CLI アドオンテンプレート

ロール	機能
SD-WAN コントローラ	ハブアンドスポーク、AAR、アフィニティを使用した集中型ポリシー

使用例

柔軟なブランチ展開

Cisco SD-WAN での柔軟なブランチ展開により、組織は高い効率性と拡張性を備えたブランチオフィスとリモートサイトを、迅速かつ安全に展開および管理できます。重要な側面は次のとおりです。

- ゼロタッチのプラグアンドプレイ展開
- 柔軟な導入モデル
- 一元的な管理と分析
- ブランチ用のハードウェア プラットフォーム
- 拡張性

多様なユーザーに対応する堅牢な LAN セグメンテーション

セグメンテーションは、事業部門の分離、認証済みユーザーとゲストユーザーの分離、IoT や監視カメラの通信の分離、および HIPAA や PCI などの標準に関するコンプライアンスの強制など、さまざまなシナリオをサポートします。

- VRF を使用したエンドツーエンドのネットワーク セグメンテーション
- ポリシーの適用とセキュリティ
- 集中管理

信頼性の高いパスモニタリングと保証付きのアプリケーション配信

Catalyst SD-WAN の Cisco Application-Aware Routing（AAR）は、リアルタイムのパフォーマンスデータと事前定義されたサービスレベル契約（SLA）に基づいて、アプリケーション通信に最適な WAN 経路を動的に選択するオーバーレイの機能です。Bidirectional Forwarding Detection（BFD）プローブとインラインデータを使用して、パケット損失、遅延、ジッターなどの主要なパス特性をモニタリングし、最適化されたアプリケーションデリバリと信頼性の高いパスモニタリングを可能にします。

このプロファイルでは、アプリケーション、DSCP、ポート、またはプレフィックスの一致と、それらのパスのリアルタイムの正常性とパフォーマンス（SLA）に基づいて、アプリケーション通信がアプリケーション ルート ポリシーによって、最適な WAN トランスポート（MPLS、インターネットなど）全体で動的にステアリングされます。

一致基準	SLA クラス	推奨カラー	バックアップカラー
dscp	Voice-And-Video_sclst	private1、private2	biz-internet
app-list	Transactional-Data_sclst	biz-internet、private1、private2	
source-ip	Default_sclst	private1、private2、biz-internet	

注： 優先カラーグループ（PCG）が選択されていない場合は、必要に応じて優先カラーグループを選択できます。カラーまたはパスの設定に基づいて、最大 3 段階の優先順位を設定します。

オンデマンドトンネルを使用したセキュアなリモートアクセス

オンデマンドトンネル（ODT）を使用したセキュアなリモートアクセスにより、リモートユーザーが必要な場合にのみネットワークリソースにアクセスできるようにする、制御された一時的かつセキュアな接続手段が得られます。

このプロファイルでは、エンドツーエンドのユニキャスト通信用に、単一サイトの WAN エッジからハイブリッドモードサイト（Biz-Internet 経由）まで、ダイナミック ODT が確立されます。

医療機関の重要業務に対するマルチキャスト サポート

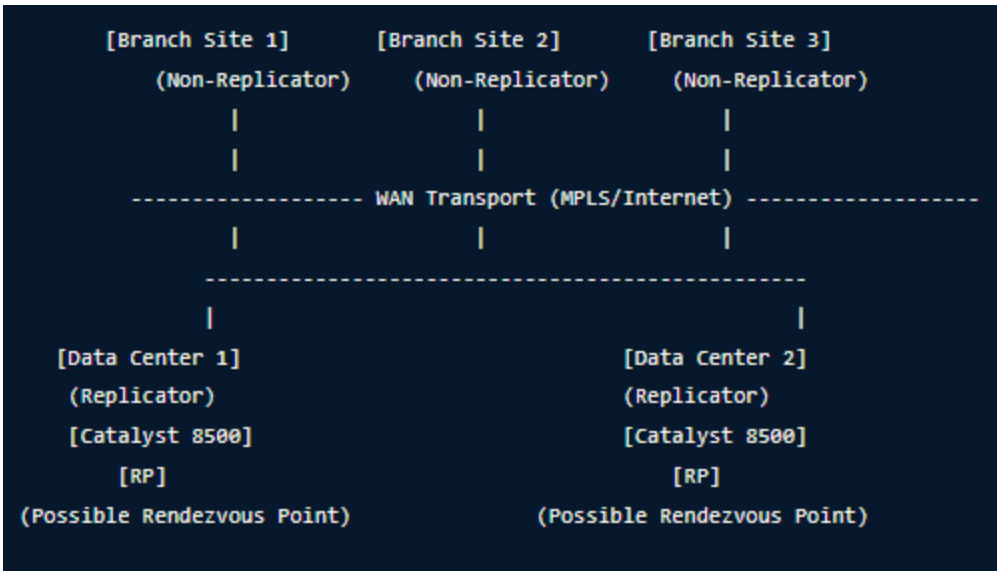
マルチキャストテクノロジーは医療機関の環境において不可欠であり、患者のモニタリング、ビデオ会議、リアルタイムアラートなどのデータストリームを、ネットワークに負荷をかけることなく、複数の受信者に効率的に配信できるようにします。Cisco SD-WAN マルチキャスト オーバーレイ ルーティングでは、オーバーレイ管理プロトコル（OMP）を使用して、最適化されたセキュアなマルチキャスト ディストリビューション ツリーを SD-WAN ファブリック全体に作成することで、ネイティブマルチキャスト機能を拡張します。

このプロファイルでは、マルチキャスト送信元はハブ（データセンター）に、マルチキャスト受信者はブランチサイトに所在しています。ブランチロケーションの WAN エッジルータがマルチキャストドメインに参加する一方、データセンターの Catalyst 8500 WAN エッジルータはレプリケータとして機能します。

データセンターでは、サービスインターフェイスで設定された PIM スパースモードを使用して、VRF 10 でマルチキャストルーティングが有効になります。SSM の範囲は「PIM-SSM-Range」（239.232.0.0/16）として定義されます。

リモートブランチでは、分散モードを使用して、IP マルチキャストルーティングが VRF 10 で有効になります。PIM スパースモードは LAN インターフェイス上で設定され、SSM 範囲はプレフィックスリスト「PIM-SSM-Range」（239.232.0.0/16）によって定義されます。

PIM スパースモード（PIM-SM/ASM）では、ランデブーポイント（RP）が必須です。このトポロジでは、RP をハブ/データセンター側でホストし、DC-HUB-1 をプライマリ、DR-HUB-1 をバックアップとして高可用性（HA）を実現する必要があります。安定したハブ側のレイヤ 3 インターフェイス（できればループバック）でランデブーポイント（RP）を設定し、すべてのブランチ マルチキャスト ドメインから RP に到達できるようにします。図に示すように、使用可能な RP はデータセンター内にあります。



注： マルチキャスト通信はハブツースポークトンネルでのみサポートされ、ユニキャスト通信を介して 2 つのブランチサイト間で動的に作成された ODT ではサポートされません。

トラブルシューティング

Cisco SD-WAN には、エンドツーエンドの可視性、コントロールプレーン診断、およびデータプレーン分析を提供するように設計された、障害対応機能の堅牢なスイートが組み込まれています。これらの機能は、主に Catalyst SD-WAN Manager によって一元管理されます。主な機能は次のとおりです。

- リアルタイムダッシュボードでは、デバイスのステータス、トンネルの正常性、アプリケーションのパフォーマンスなど、SD-WAN ファブリックの全体的な正常性を単一のペインで確認できます。
- パスの可視化は、オーバーレイ全体のパス通信を可視化するグラフィカルツールで、遅延、ジッター、パケット損失を特定するのに役立ちます。
- アラームおよびイベントリアルタイムは、コントロール、データ、および管理プレーンの問題に対処するための、分類されたアラートです。
- サイトトポロジでは、デバイス接続のマップベースのビューを提供します。
- 組み込みの速度テスト（サイト間またはインターネット）では、スループットとリンクのキャパシティを測定します。
- パケットキャプチャおよびトレース機能を使用すると、特定のインターフェイス上のパケット（TCP ダンプ /Wireshark）をキャプチャしたり、Network-wide Path Insight（NWPI）を実行してドロップポイントを分析したりできます。

表 1. 20.12.5/17.12.5 オーバーレイのスケーリングに関する設計上の考慮事項

デバイス	要素	最大制限	推奨
SD-WAN Manager	クラスタ	6	• 2,501 ～ 12,500 オーバーレイスケール用の 6 ノードクラスター • 501 ～ 2,500 スケール用の 3 ノードクラスター
	Instance Size	128 GB メモリ 64 vCPU 1 TB HDD	• インスタンスごとに DPI を有効化：64vCPU/128GB/1TB • インスタンスごとの DPI なし：32vCPU/64GB/500GB
SD-WAN コントローラ	Instance Size	8 vCPU、16 GB メモリ	16GB メモリ（最大 1200 ピア）
	OMP ピア	1500	• コントローラごとに 750 ～ 1,000 OMP ピア • アフィニティグループを有効化
	アフィニティグループ	63	12 vSmart の大規模なオーバーレイの場合は 6 グループ
	最大 RIB 出力	90,000,000	• コントローラあたり最大 90M の RIB 出力 • WAN エッジごとに 2 OMP セッション • アフィニティグループごとに 2 つのコントローラ
SD-WAN Validator	バリデータあたりのエッジデバイス	1500	1500
ハブ	トンネルのスケール	8000	8000
	ネクストホップのスケール	32,000	• ネクストホップスケールの 90% • トンネルグループを使用したハブアンドスポーク
	VPN のスケール	500	ネクストホップのスケールは、VPN の数と、ハブルータに接続されているブランチの総数に

デバイス	要素	最大制限	推奨
			よって異なります。 例： 2 VPN：最大 4,000 ブランチルータ 3 VPN：最大 2,900 ブランチルータ 4 VPN：最大 2,150 ブランチルータ
スポーク/ブランチ	TLOC の数	8	WAN エッジあたり 2 TLOC • 1 つのプライベート WAN • 1 つのパブリック WAN
	サービス VPN（VRF）の数	500	3 VPN

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。

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。