検証済みソリューション：医療業界（非ファブリック）

改訂：2023 年 9 月 27 日

本書の目的と用途

このドキュメントの目的は、シスコが推奨する一般的な医療導入プロファイルの概要を示すことです。Cisco DNA Center を使用する一般的な非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も機能します。導入エンジニアがサービス要件を理解するのに役立つように、このドキュメントの理論的なセクションと実践的なセクションを組み合わせて使用する必要があります。このドキュメントは、導入エンジニアが導入および設定時に特定のネットワークに関する最適な決定を下すのにも役立ちます。

対象読者

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、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。ここでは、進化を続ける大規模な医療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な事項について説明します。

セキュリティ

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。米国の病院や医療センターでは、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。医療機関にとっては、事業継続を維持するためにセキュリティの復元力を確保することが最も重要です。今日の複雑な IT 環境では、進化し続ける脅威の中でビジネスの完全性を保護するために、信頼できるユーザーのみにネットワークへのアクセスを許可する必要があります。Cisco Identity Service Engine（ISE）を使用すると、組織は、信頼できるユーザーとエンドポイントを信頼できるリソースに接続するネットワークをセグメント化できます。Cisco ISE は、権限を持つユーザーとネットワークエンドポイントにセキュアなネットワーク アクセス コントロールを展開する柔軟性を組織に提供します。

暗号化トラフィックの急増により、脅威の状況も変化しています。デジタル化が進む中、多くのサービスやアプリケーションが、情報を保護するための主要な手段として暗号化を使用しています。暗号化技術により、インターネットを使用してビジネスの通信や取引を行う企業および個人のプライバシーとセキュリティが大幅に向上しました。Cisco Network as a Sensor（NaaS）ソリューションに実装されていて、NetFlow を使用している従来のフローモニタリングでは、フローのアドレス、ポート、バイト数とパケット数のレポートによってネットワーク通信の概要を表示できます。

Cisco DNA Center の不正管理アプリケーションは、脅威を検出して分類し、ネットワーク管理者、ネットワークオペレータ、およびセキュリティオペレータがネットワークの脅威をモニターできるようにします。Cisco DNA Center は、最も優先度の高い脅威を迅速に特定するのに役立ち、Cisco DNA アシュアランス 内の不正管理ダッシュボードで特定した脅威をモニターできます。

Cisco 適応型ワイヤレス侵入防御システム（aWIPS）は、無線侵入の脅威を検出して軽減するメカニズムであり、脅威の検出およびパフォーマンスの管理のための高度なアプローチが使用されます。アクセスポイントで脅威が検出されると、Cisco aWIPS がアクションを開始します。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。

モビリティ

今日の医療環境では、医療従事者、患者、および機器が常に移動しています。シスコのワイヤレスモビリティ ソリューションは、医療サービスの効率化を支援します。医療従事者は、ノートパソコン、タブレット PC、ワイヤレス IP 電話、新しいデュアルモード電話（病院の Wi-Fi ネットワークまたは携帯電話ネットワークのいずれかで接続可能）を使用して、どこからでも情報にアクセスしてサービスをオーダーできます。回診中の医師は、ワイヤレスラップトップを使用して患者のカルテを更新し、口頭で指示を出せます。更新されたカルテは他のスタッフがすぐに利用できるため、最新の患者情報に基づいて意思決定を行うことができます。栄養士、ナース、セラピストは、ワイヤレスタブレットを使用して、オーダーを確認したり、特別なニーズを把握したり、検査結果を確認したりできます。患者は登録のために列に並んで待つ必要がなくなり、ローミング登録担当者は、ロビーや緊急治療室にいる患者の所までワイヤレスタブレットを持ち込むことができます。緊急治療が必要な患者の場合、クリティカルケアを受けた後にベッドサイドで登録することもできます。

ネットワーク管理

Cisco DNA Center は、迅速で柔軟な導入とシンプルで一元化されたネットワーク管理により、ネットワークの設計、構築、および管理方法に革命をもたらしているため、システムを数か月ではなく数日で稼働させることができます。Cisco DNA Center のインフラストラクチャとソリューションは、患者対応業務とスマートな運用を促進するデジタル対応の基盤も提供します。組織は次のようなメリットを得ることができます。

- 自動化の使用による複雑さの緩和とコスト削減：自動化、管理、アシュアランスを通じて、臨床、研究、ファクトリネットワークの導入と更新を迅速化し、日常運用とネットワーク管理にかかるコストを削減できます。
- 実用的なインサイトによるイノベーションの高速化：ネットワーク全体の分析を実施することで、適切な治療と研究エクスペリエンスを提供し、臨床医とスタッフの生産性向上、スペース使用率の最適化を実現できます。
- Security Everywhere によるリスクの軽減：継続的かつ迅速な脅威検出による保護と、ネットワーク全体へのセキュリティ機能の組み込みによって重要な患者データを保護できます。

ハイ アベイラビリティ

このドキュメントでは、堅牢な医療環境のベストプラクティスに基づいて、高度な臨床アプリケーションと生体医療デバイスを、保護されたインタラクティブで復元力がある応答性の高い環境で動作させるためのネットワーク基盤とアーキテクチャについて説明します。

単一障害点が排除され、高速コンバージェンス アーキテクチャとテクノロジーがネットワーク全体で使用されます。アドバンスドテクノロジーを使用して、電子医療記録（EHR）、画像アーカイブおよび通信システム（PACS）、生体医療デバイスなどのミッションクリティカルなアプリケーションの稼働時間を最大化します。EtherChannel や SVL スイッチングファブリックは、サービスを中断することなく交換またはアップグレードできます。内部ゲートウェイプロトコル（IGP）は、ネットワーク コンバージェンス時に最高レベルの復元力を確保するのに役立ちます。継続的な稼働時間を確保する機能には、In-Service Software Upgrade（ISSU）、ローリング AP アップグレード（N+1）、およびステー

トフル スイッチオーバー（SSO）が含まれます。これらの機能により、ルータ、スイッチ、およびワイヤレスコントローラがアクティブな状態でソフトウェアのアップグレードを実行できるため、ネットワークのダウンタイムが短縮されます。

ロケーション サービス

モバイルリソースの場所に関するインテリジェンスにより、ビジネスプロセスと臨床プロセスが合理化され、スタッフが高品質のケアを提供できるようになります。現在、主要な医療機関は、機器や人を含む重要なリソースの認識を向上させるために、ロケーションソリューションを採用しています。Cisco Location-Aware Healthcare ソリューションは、医療機関がワークフローをモニターして最適化し、応答性、生産性、および効率を向上させるのに役立ちます。ロケーション認識型の医療サービスは、資産管理、ワークフローの最適化、患者の追跡という 3 つの主要なソリューション分野に集約されています。今日の市場にあるほとんどのロケーションベースのソリューションには、独自のベンダー固有のハードウェアとソフトウェアが必要なため、サービスを提供できるユースケースの種類が制限され、管理が複雑になります。一方、Cisco Spaces は、デバイスおよびソフトウェアパートナー、チャネルパートナー、業界団体からなる広範にわたるエコシステムを結ぶオープンなプラットフォームです。

ロケーションサービスの利点は次のとおりです。

- デバイスに最も近いアクセスポイントを特定して、Wi-Fi デバイスを見つけます。この方法は、三角測量よりも精度が低くなりますが、アクセスポイントの少ない施設に導入したり、Wi-Fi 位置分析を屋外のアクセスポイントに拡張したりできます。
- Cisco CleanAir ® テクノロジーと非 Wi-Fi 干渉源を使用して、接続済みおよび未接続の Wi-Fi デバイス、干渉源、アクティブ RFID タグを特定します。
- 高度な到来角（AoA）テクノロジーと FastLocate を組み合わせることで、接続されている Wi-Fi デバイスの正確な位置を 1 ～ 3 m（導入環境によって異なる）以内で特定します。
- Hyperlocation を使用して、RSSI 三角測量のプローブ信号やネットワークデータパケットを使用して、接続中の Wi-Fi デバイスを検出し、より迅速な更新とより詳細な位置の検出を実現します。
- 分析を使用して、場所と移動パターンに基づいて、施設の訪問者が使用する Wi-Fi デバイスに関するインサイトを生成します。

トラフィックの最適化

Quality of Service（QoS）は、輻輳した環境でトラフィックを効率的に伝送するための主要なコンポーネントです。QoS を利用することで、事業運営上の重要性を反映したマーキングをアプリケーションに適用できます。有線環境では、これらのマーキングを使用して、さまざまな優先順位レベルを設定し、帯域幅と制御を割り当てることができます。ワイヤレス環境では、8 つのユーザー プライオリティ キューの 1 つにアプリケーションを関連付けるためにもマーキングが使用されます。キューとの関連付けを使用して、アプリケーションがワイヤレスメディアにアクセスする頻度を統計に基づいて変更できます。インフラストラクチャ レベルで適切なマーキングを行うことで、ダウンストリーム トラフィックが最適化され、ビジネスへの関連性が高いアプリケーションは、統計上優先的にトラフィックを受信でき、リアルタイム アプリケーションには非インタラクティブ アプリケーションより高い優先順位を付けることができます。クライアント端末が QoS マーキングを適切に運用していれば、同じ効果がアップストリームにも適用されます。

ゲストアンカーリング

ますます一般的になっている医療アプリケーションはゲストアクセスです。ゲストアクセスは、医療システムの IT ポリシーの直接の制御下にない個人にインターネットアクセスを提供します。組織のニーズを維持するには、ゲストトラフィックの優先順位を医療アプリケーションよりも低くする必要があります。医療施設には、従来のゲストユーザークラスに加えて、医師のゲストユーザークラスも必要です。医師は、単純なインターネット接続以上のアクセスを必要とし、通常は施設のプライベートネットワーク内のリソースへのアクセスを必要とします。医師は必ずしも従業員ではないため、管理対象外のさまざまなクライアントデバイスを使用する可能性があります。ウイルスの拡散を防ぎ、プライベートネットワークへの扉を開く可能性を防ぐには、セキュリティに関する追加の考慮事項が必要です。Cisco DNA Center は、ワイヤレスゲストユーザーにゲスト アンカーリング ソリューションを提供します。ゲスト機能は、ネットワーク内のコントローラから非セキュアなネットワークエリア（DMZ）内のゲストコントローラへのセキュアなトンネルを使用して、エンタープライズ ネットワークの外部にゲストトラフィックを誘導します。

医療プロファイルの概要

次の表に、医療ソリューションプロファイルの主な焦点領域を示します。

主要な導入領域	機能
セキュリティ	• グループベースのポリシー（TrustSec ソフトウェア定義型セグメンテーションとも呼ばれる） • 暗号化トラフィック分析（ETA） • ピアツーピア ブロック • 不正管理および aWIPS
モビリティ	• 802.11r 高速ローミング • WLC 内および WLC 間ローミング
ネットワーク管理	Cisco DNA Center
高可用性	• AP SSO • N+1 SSO
ロケーション サービス	• Cisco Spaces • CMX
トラフィックの最適化	• FastLane • MQoS
ゲストアンカーリング	• ワイヤレスゲスト（中央 Web 認証） • 有線ゲスト

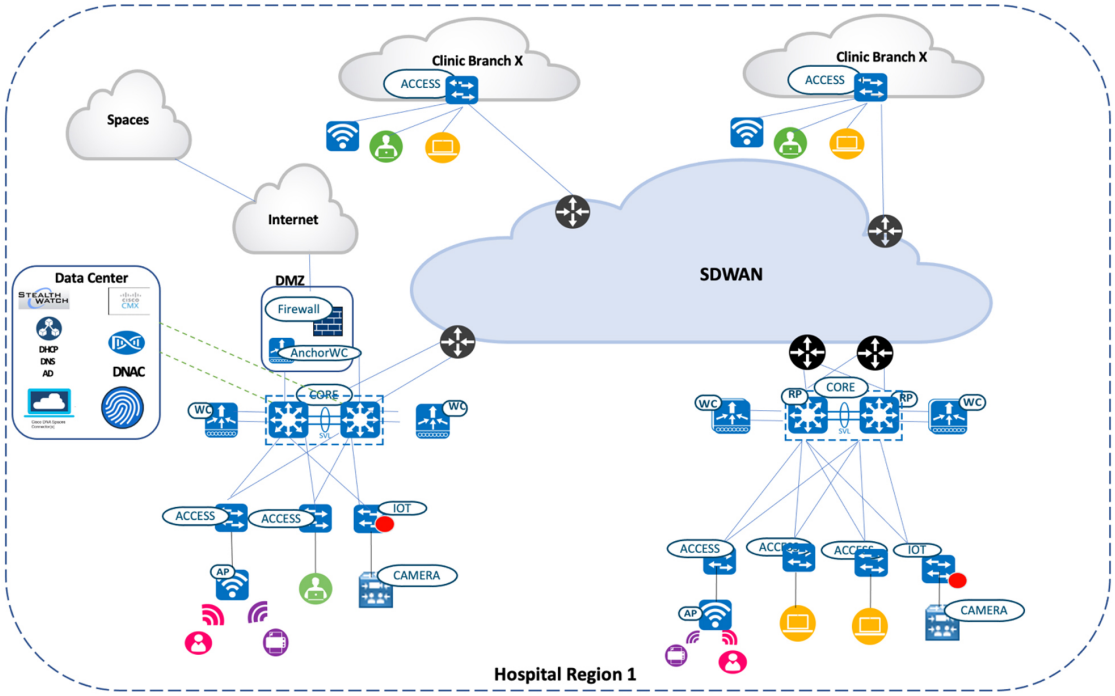
ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。

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 2.3.3.7
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 3.1 パッチ 4
Stealthwatch	SMCVE/FCVE	Stealthwatch Management Console/Stealthwatch フローコレクタ	7.3.2
Cisco SD WAN	vManage	Cisco vManage	20.6.3.1
	ASR1001-X/ASR1002-HX	Cisco ASR シリーズ アグリゲーション サービス ルータ	17.6.4
	ISR-4351 ISR-4431	Cisco ISR サービス統合型ルータ	17.6.4
	8300	Cisco Edge サービスルータ	17.6.4
Cisco コラプストコアノード	C9500-48Y4C C9600	Cisco Catalyst 9500 シリーズ スイッチ Cisco Catalyst 9600 シリーズ スイッチ	17.6.4、17.9.3
	C6807-XL	Cisco Catalyst 6800 シリーズ スイッチ	15.5(1)SY5
Cisco アクセスノード	C9300-48P C9300-24P C9407R C9200-48P	Cisco Catalyst 9300/9200/9400 シリーズ スイッチ	17.6.4、17.9.3
	3850-48U	Cisco Catalyst 3850 シリーズ	16.12.8
シスコ ワイヤレス コントローラ	C9800-40-K9 C9800-L-K9	Cisco Catalyst 9800 ワイヤレスコントローラ	17.9.3
Cisco IoT ノード	IE-5000	Cisco Catalyst IE5000 高耐久性シリーズ	15.2(8)E1

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 アクセス ポイント	9120-AXI 9130-AXI 2800 3700 3800	Cisco Catalyst/Cisco Aeronet アクセスポイント	17.9.3
無線電話	Cisco Wireless IP Phone 8821、Apple iPhone 12、Xiaomi 11i	—	—
有線電話	Cisco Wired Phone	—	—
ワイヤレスラップトップ	Apple macOS（M1 チップ）、Windows 10	—	—
有線ラップトップ	Windows 10	—	—

ソリューション トポロジ



ソリューションのユースケース

カテゴリ	機能	使用例
セキュリティ	インテントベースネットワーク	Cisco DNA Center と Cisco ISE の統合
		サイトの作成（[Network Hierarchy] の下）
		検出ツールと PnP を使用したデバイス検出
		[Template Programmer]
	グループベースポリシーのマイクロセグメンテーション	ナースステーションと医師間の通信
		重要な患者レコードへのアクセス
		インラインタギングを使用したサイト間セキュリティグループタグ（SGT）の伝達
	IPSK を使用した P2P ブロッキング	wpa_supplicant をサポートするレガシーデバイス
	不正および aWIPS	WLAN での脅威検出と軽減
	暗号化トラフィック分析	有線ワークステーションと緊急医療記録（EHR）間の TLS 通信での脅威検出
	AI エンドポイント分析	病院のネットワークに接続されたアドホックデバイス
モビリティ	ワイヤレスローミング	医師とナースが患者を訪問し、患者の記録を更新する
トラフィックの最適化	自動 QoS	Fastlane を使用した Apple クライアントのプライオリティキューイング
	MQoS	Cisco DNA Center アプリケーションポリシーを使用した CVD キューイングプロファイル
ゲストアンカーリング	ワイヤレスゲストアクセス	キャンパスサイトの外部ゲストと、ゲストクライアントにサービスを提供する DMZ 上のアンカーゲストコントローラ
	有線ゲスト アクセス	メンテナンス、ソフトウェアアップデート、またはファームウェアの更新のためにインターネットアクセスを必要とする有線医療エンドポイント
ロケーションサービス	Cisco Spaces の Detect and Locate	Wi-Fi アセットタグを使用して医療機器（フュージョンポンプやヘルスモニタリングデバイスなど）の場所を追跡する病院のスタッフ

カテゴリ	機能	使用例
ハイアベイラビリティ	AP/クライアント SSO	サイト内およびサイト間の冗長性と復元力を備えたネットワークにより、予期しないネットワーク障害や計画的なメンテナンス期間中でも常に利用可能な医療従事者向けのネットワークサービス
	N+1 SSO	
	ISSU/ローリング AP アップグレード	

スケール

ソリューションのテストでは、次の表に示すスケール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を確認するには、*Cisco DNA Center* のデータシート [英語] を参照してください。

カテゴリ	値
デバイスインベントリ	4000
サイトごとのデバイスの数	100
複数の Cisco DNA Center アプライアンス	2
建物とフロアの数	1000
サイトあたりの WLC の数	2
インベントリ内の AP の数	6000
エンドポイントの数	75,000（有線 50,000、無線 25,000）
SSID の数	5
SGACL の数	200
SGT の数	100
アシュアランススケール（1 秒あたりの Syslog メッセージおよびトラップの数）	イベントタイプ別にカスタマイズ

ソリューションの基調講演

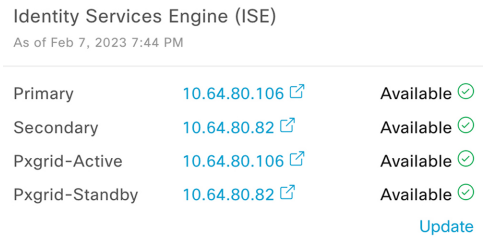
セキュリティ

医療環境では、患者のプライバシーを守り、可用性を確保するためにデータセキュリティが不可欠です。システムは、医療従事者が患者を効果的に治療するために必要なパフォーマンスレベルでデータを転送できる必要があります。高可用性を実現するには、偶発的および意図的なシステムの誤用によってシステムパフォーマンスが許容可能なサービスレベルを下回らないようにするための厳格なセキュリティ対策が必要です。

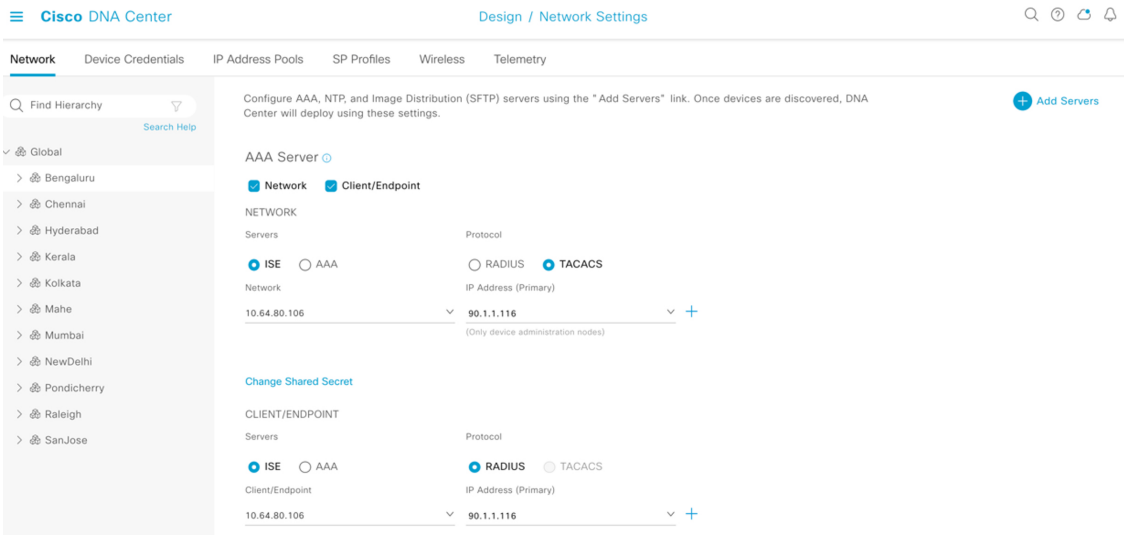
Cisco DNA Center を使用したインテントベース ネットワーク

管理者は、複数の地域にまたがる複数のサイトを反映するネットワーク階層を設計できます。この階層は、スイッチ、ルータ、ワイヤレスコントローラ、IOT ノード、およびアクセスポイントで構成されるノードを収容するエリア、ビルディング、およびフロアの統合ビューを提供します。これらのノードは、検出ツール（自動化を活用）を使用して Cisco DNA Center によって検出されます。管理者は、それらのノードを対応するサイトに割り当てることができますが、ノードがいずれかのサイトに物理的に存在する必要はありません。アクセスポイントは、PnP ワークフローを介して Cisco DNA Center インベントリに追加され、対応するワイヤレスコントローラにインテリジェントに割り当てられます。

Cisco Identity Services Engine（ISE）は pxGrid の関連付けを介して Cisco DNA Center と統合されます。この関連付けでは、本質的に、アクティブ/スタンバイ pxGrid および PAN ペルソナを備えた Cisco ISE クラスタ環境が認識されます。次の図は、Cisco DNA Center によって [System 360] ページに表示される Cisco ISE ペルソナ情報を示しています。



Cisco DNA Center の [Network Settings] ページでは、複数のポリシーサービスノード（PSN）を適切なサイトにマッピングして、さまざまな場所に伝達するポリシーサービス要求を効率的に管理およびロード バランシングできます。



この例でサイトに割り当てられたネットワークデバイスには、Cisco ISE の同等デバイスのネットワーク アクセス デバイス エントリが作成されます。

消費されるインテントは、前のステップまでに Cisco DNA Center で設計されています。インテントは、デバイス プロビジョニング ワークフローによって CLI に変換されます。その後、対応するネットワークノードで AAA/RADIUS の設定がプロビジョニングされ、[Access]、[Distribution]、および [Core/Router] デバイスロールの RADIUS およびグループベースのポリシー境界内のノードが完全にバインドされます。ワイヤレスコントローラは、Template Programmer を使用してグループベースのポリシー境界に配置されます。

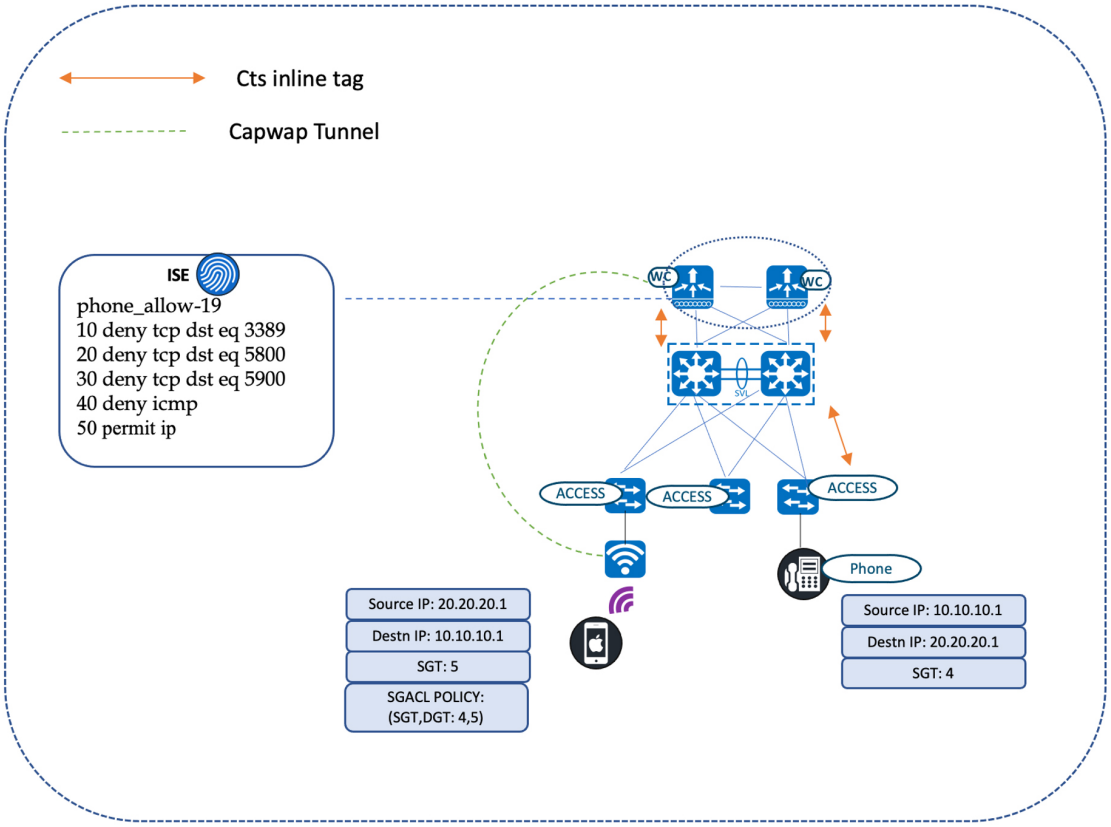
グループベースポリシーのマイクロセグメンテーション

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、ユーザー、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。

ここでは、ワイヤレスセグメントと有線セグメントである CTS 適用ポイントを使用して重要な患者レコードにアクセスする病院スタッフ間の通信を対象としたエンドツーエンドのユースケースについて説明します。このユースケースを理解するには、グループベースのポリシーに関する基本的な知識が必要です。

ナースステーションと医師間の通信

医療ネットワークには、有線電話と無線電話を使用する従業員がいます。この例では、ナースステーションの有線電話を使用するナースと無線電話を使用する医師の間の通話について説明します。アクセススイッチに接続された有線電話が MAB 認証され、その電話に対応する CTS タグがスイッチにインストールされます。アクセススイッチは、アクセススイッチとコア ネットワーキング デバイス間の直接接続されたリンクに手動で設定された CTS を介して、CTS タグをアップリンク SVL コアネットワーキングノードに伝達します。SVL コアにスプリットペア方式で接続されているワイヤレスコントローラには、直接接続されたリンクでCTS も手動で設定されています。ワイヤレスコントローラには、医師の無線電話に割り当てられている、対応する宛先グループタグ（DGT）用にダウンロードされたSGACL ポリシーがあります。医師の無線電話は、中央スイッチングパターンでクライアントにサービスを提供しているワイヤレスコントローラ宛てのすべてのトラフィックをバックホールするローカル モード アクセス ポイントに接続されています。医師の無線電話に送信されるトラフィックに最も適した SGACL ポリシーを次に示します。



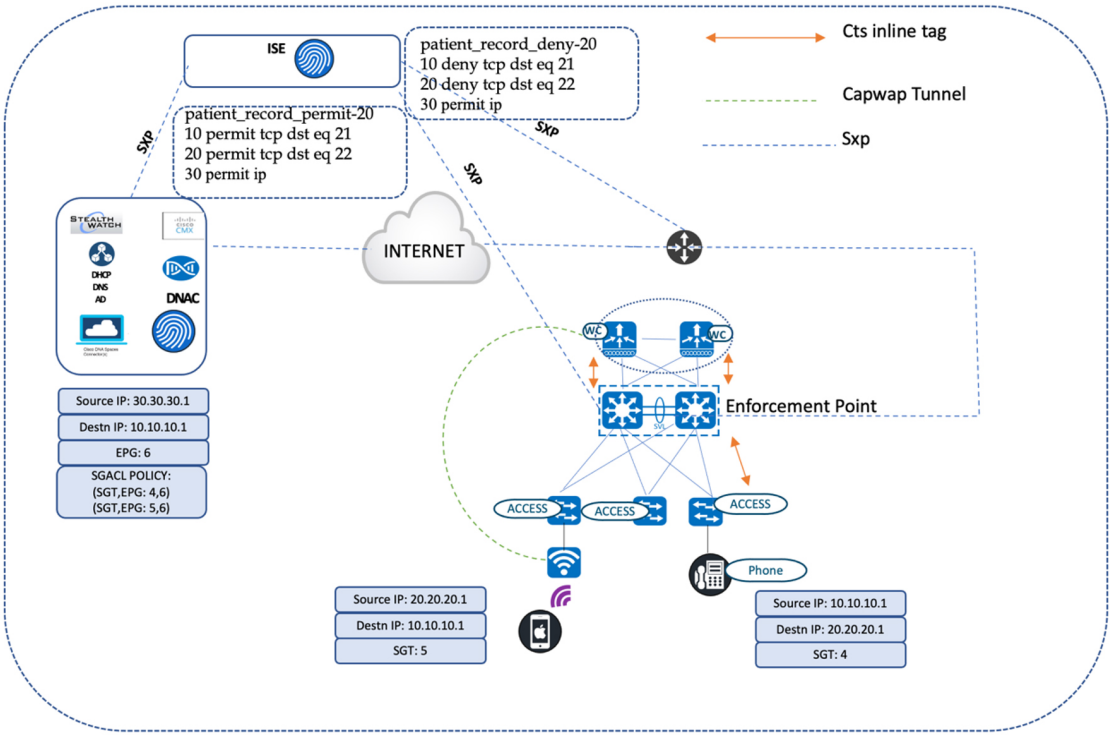

```
9840-ha#show cts role-based permissions from 4 to 5
IPv4 Role-based permissions from group 4:NurseStation to group 5:Doctors:
```

```
 Phone_allow-19
RBACL Monitor All for Dynamic Policies: FALSE
RBACL Monitor All for Configured Policies: FALSE

Role-based IP access list phone_allow-19 (downloaded)
    10 deny tcp dst eq 3389
    20 deny tcp dst eq 5800
    30 deny tcp dst eq 5900
    40 deny icmp
    50 permit ip
```

重要な患者レコードへのアクセス

データセンターに保存されている重要な患者レコードには、許可された担当者のみがアクセスする必要があります。すべてのサイトのコアネットワーキングデバイスは、エンタープライズドメインに出入りするトラフィックのゲートウェイです。クリティカルデータパスにあるコアデバイスは、ネットワークから出るトラフィックを強制するために、グループベースのポリシーバインディングを認識する必要があります。デバイスは、Cisco ISE ノードとの SXP セッションを介してリモートネットワークのポリシーバインディングを学習します。これは、患者レコードへのアクセスを要求するワイヤレスユーザーと有線ユーザーの両方から発信されるトラフィックに適用されます。送信元 CTS タグは、コアノードに到達するまでインラインで伝送されます。次に、コアデバイスは受信した SGT を検査し、ポリシーペア（送信元グループタグ（SGT）と宛先グループタグ（DGT））に一致する静的ポリシーを検索します。この場合、DGT は患者レコードの CTS タグです。要求元エンティティの認証レベルに基づいて、患者レコードへのアクセスがコアデバイスで許可または拒否されます。レコード保持サーバーによって権限を持たないユーザーのアクセスが拒否されるまで、トラフィックを伝達する必要はありません。次の図では、ナースステーションからは重要な患者レコードにアクセスできませんが、医師はアクセスできます。




```
cts sxp enable
cts sxp default password 7 14141B180F0B293F37
cts sxp connection peer 90.1.1.117 source 192.169.50.31 password default mode local both
```

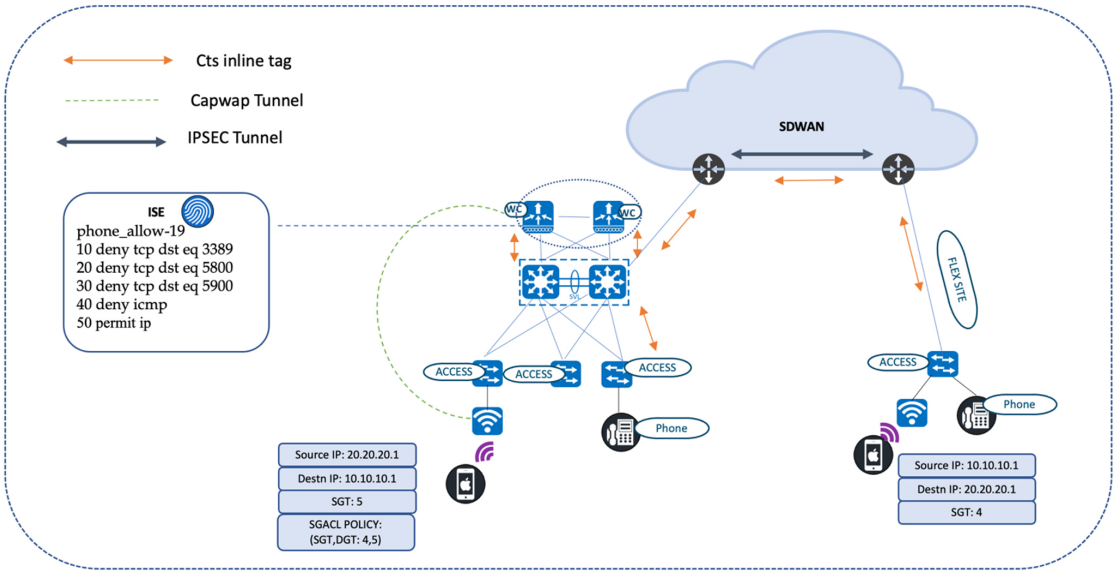
```
HCA-C3-CORE-9600-1#show cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Key-Chain: Not Set
 Default Key-Chain Name: Not Applicable
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 90.1.1.117
Source IP        : 192.169.50.31
Conn status      : On (Speaker) :: On (Listener)
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Speaker Conn hold time   : 120 seconds
Listener Conn hold time   : 120 seconds
Local mode       : Both
Connection inst# : 1
TCP conn fd      : 1(Speaker) 2(Listener)
TCP conn password: default SXP password
Keepalive timer is running
Duration since last state change: 49:17:02:47 (dd:hr:mm:sec) :: 49:17:02:47 (dd:hr:mm:sec)


Total num of SXP Connections = 1

9600-SVL#show cts role-based permissions from 4 to 6
IPv4 Role-based permissions from group 4:NurseStation to group 6:record_room:
 patient_record_deny-20
9600-SVL#show cts role-based permissions from 5 to 6
IPv4 Role-based permissions from group 5:Doctors to group 6:record_room:
 patient_record_permit-20
```

遠隔地のブランチクリニックでの重要な患者レコードへのアクセス

患者レコードは、小規模なブランチクリニック（フレックスサイトとも呼ばれる）からアクセスされます。メインキャンパスのワイヤレスコントローラは、ブランチクリニックのフレックスアクセスポイントにサービスを提供します。送信元CTSタグは、ブランチサイトのアクセスノードに到達するまでインラインで伝送されます。アクセスデバイスは、受信した SGT を検査し、ポリシーテーブルを検索して、ポリシーペア（送信元グループタグ（SGT）と宛先グループタグ（DGT））に一致するタグがあるか確認します。この例では、DGT は患者レコードの CTS タグです。

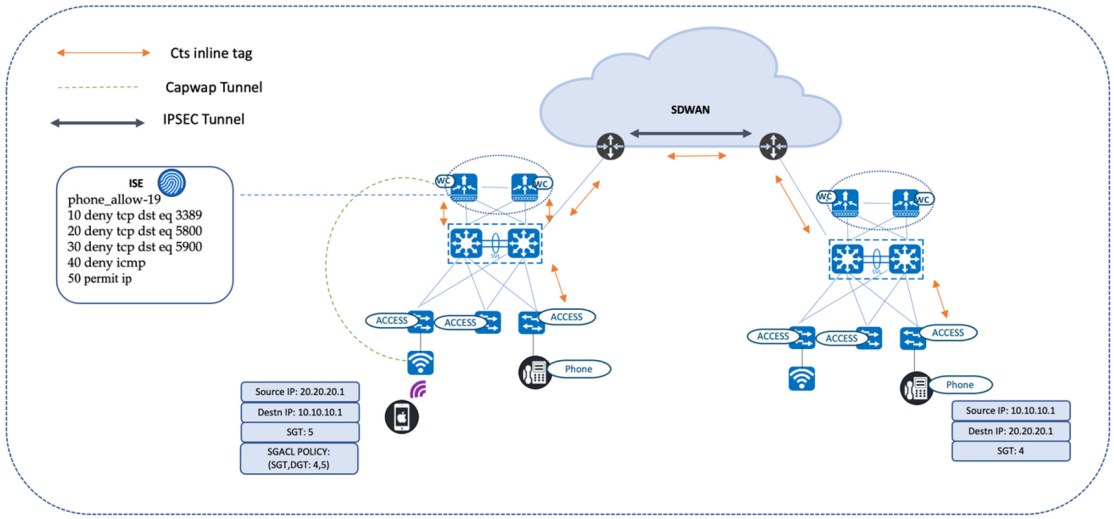


インラインタギングを使用したサイト間 SGT の伝達

さまざまな地域にある病院のエンドユーザーの CTS タグは、CTS インラインタグを使用して伝達されます。CTS タグは、IPsec ヘッダーにカプセル化されてサイト全体で伝送されます。

Outer IP HEADER	UDP HEADER	IPSEC HEADER	MPLS LABEL	MDATA SGT:X	Inner IP HEADER	Original Payload	Outer IP HEADER	Outer IP HEADER

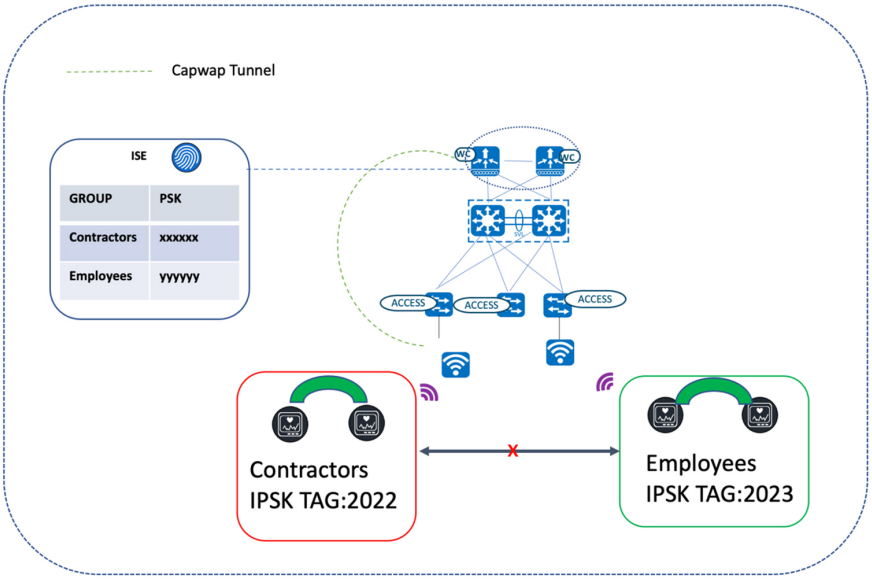
次の図は、異なる拠点におけるナースステーションと医師の間の通話を示しています。インラインタギングは、ナースステーションの電話が接続されているアクセススイッチから医師のワイヤレス電話が接続されているワイヤレスコントローラまでのすべての出力インターフェイスで有効になっています。インラインタギングは、コアデバイスや Cisco SD-WAN エッジなど、中間ノードの出力インターフェイスでも有効になります。IPsec 対応の Cisco SD-WAN エッジは、オーバーレイを使用して CTS タグを転送します。



IPSK を使用したピアツーピアブロッキング

ワイヤレスネットワーク内のすべてのエンドポイントが、セキュアな接続のために 802.1x サプリカントをサポートしているわけではありません。代わりに WPA-PSK を使用できないエンドポイント。PSK を使用する同じ WLAN 内のユーザーはすべて同じ事前共有キーを共有するため、キーが誤って使用され、不正アクセスが発生する可能性があります。このセキュリティギャップを克服するために、IPSK では特定のユーザーまたはユーザーグループに一意の事前共有キーを割り当てることができます。IPSK セキュリティは、同じ PSK を持つユーザー（または同じ WLAN や異なる WLAN 内のユーザー）が相互に通信できないようにする必要がある場合、ピアツーピアブロッキングを使用してさらに強化できます。

次の図は、WLAN プロファイルで **allow-private-group** オプションが有効になっている同じ WLAN に接続されているユーザーを示しています。このシナリオでは、Cisco ISE の同じ認証プロファイルによって認証されたユーザーは同じ IPSK タグを共有するため、相互に通信できます。異なる IPSK タグを持つユーザーは、一意の Cisco ISE 認証プロファイルを使用して認証されているため、それらのユーザーは相互に通信できなくなります。ピアツーピアブロッキングを有効にする方法の説明については、*Cisco DNA Center* ユーザーガイド [英語] の「Create a Model Config Design for Advanced SSID」のトピックを参照してください。




```
9840-ha#show wireless client summary ipsktag
Number of Clients: 5

MAC Address    AP Name                                          State            Ipsk Tag
-------------------------------------------------------------------------------------------
009a.d2f0.591a AP687D.B402.D02C                                Run              b0a8b704cbc54008
6887.c6f0.6176 AP687D.B402.D02C                                 Run               7166848ee93a1c8f
98af.65a6.d966 AP7079.B333.8CD2                                 Run               ea52373d6bfc33f0
b2aa.e402.9228 AP687D.B402.D02C                                Run              b0a8b704cbc54008
d037.45a7.f5f1 AP84F1.4782.1858                                    Run                 b0a8b704cbc54008
```

不正アクセス ポイントの管理

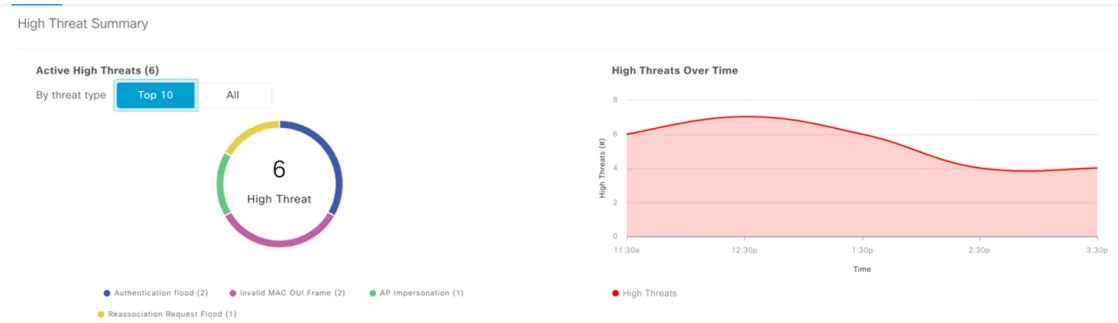
Cisco DNA Center には、WLAN の脅威を検出して分類し、ネットワーク管理者やオペレータが脅威をモニターできるようにする不正管理アプリケーションがあります。不正 AP は、WLAN 内の機密情報をハッキングするために使用されます。ハッカーが一連の Clear to Send（CTS）フレームを送信する場合、そのフレームによって AP が模倣され、1 つの

クライアントに送信し、他のクライアントに待機するように指示されるため、正規のクライアントへのサービスが中断されます。ユーザーはまた、WLANに不正なAPを接続し、アドホックネットワークを構築してネットワークトラフィックを傍受し、クライアントセッションをハイジャックできます。Cisco DNA Center は、近くにあるすべての AP を常にモニターし、不正 AP に関する情報を自動的に検出して収集します。Cisco DNA Center は 、管理対象 AP から不正なイベントを受信すると、次のように反応します。

- 不明な AP が Cisco DNA Center によって管理されていない場合は、Cisco DNA Center によって不正分類ルールが適用されます。
- 不明な AP がネットワークと同じ SSID を使用していない場合は、Cisco DNA Centerが、AP が企業の有線ネットワークに接続され、有線ネットワークに通じているかどうかを確認します。不正 AP が企業ネットワークのスイッチポートに物理的に接続されている場合、Cisco DNA Center はその AP を**有線ネットワーク上の不正**として分類します。有線ネットワーク上の不正機能を機能させるには、Cisco DNA Center で管理されているシスコスイッチが必要です。
- AP が Cisco DNA Center に対して不明で、ネットワークと同じ SSID を使用している場合、Cisco DNA Center はその AP を**ハニーポット**として分類します。
- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Centerは、干渉が発生しているかどうかを確認します。存在する場合、Cisco DNA Center は AP を**干渉源**として分類し、不正な状態を**潜在的な脅威**としてマークします。ネットワーク上の干渉源を分類するためのしきい値レベルは -75 dBm 以上です。
- 不明な AP がネットワークと同じ SSID を使用しておらず、社内ネットワークに接続されていない場合、Cisco DNA Center はその AP がネイバーであるかどうかを確認します。ネイバーである場合、Cisco DNA Center はその AP を**ネイバー**として分類し、不正状態を**情報**としてマークします。この分類のしきい値レベルは-75 dBm で、それ以下の場合に不正 AP がネイバー AP として分類されます。

適応型ワイヤレス侵入防御システム

Cisco 適応型ワイヤレス侵入防御システム（aWIPS）は、無線侵入の脅威を検出して軽減するアプリケーションです。このインフラストラクチャに完全に統合されたソリューションを使用すると、有線ネットワークとワイヤレスネットワークの両方でワイヤレストラフィックを継続的にモニターできます。このネットワーク インテリジェンスを使用すると、被害や危険が発生するまで待つことなく、攻撃を特定し、新しい攻撃をプロアクティブに防止できます。不正管理および aWIPS アプリケーションの詳細については、*Cisco DNA Center* 不正管理および *aWIPS* アプリケーション クイック スタート ガイド [英語] を参照してください。

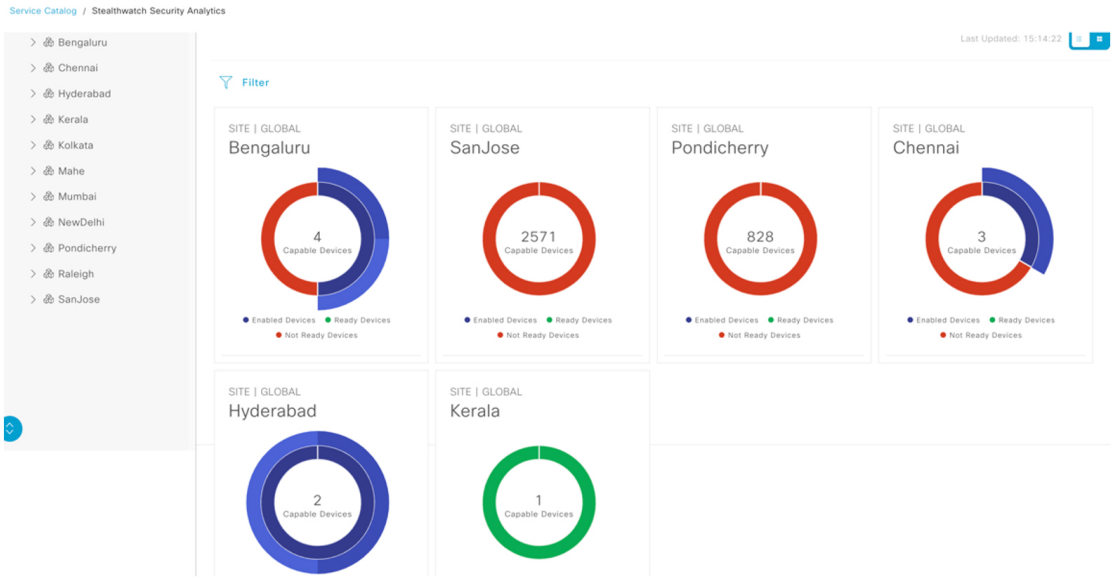


Cisco DNA Center では、さまざまなサービス妨害（DoS）攻撃を検出する次の標準シグニチャがサポートされています。

- 認証フラッド
- アソシエーションフラッド
- CTS フラッド
- RTS フラッド
- ブロードキャストプローブ
- ディスアソシエーション フラッド
- ディスアソシエーション ブロードキャスト
- 認証解除フラッド
- 認証解除ブロードキャスト
- EAPOL ログオフフラッド

暗号化トラフィック分析

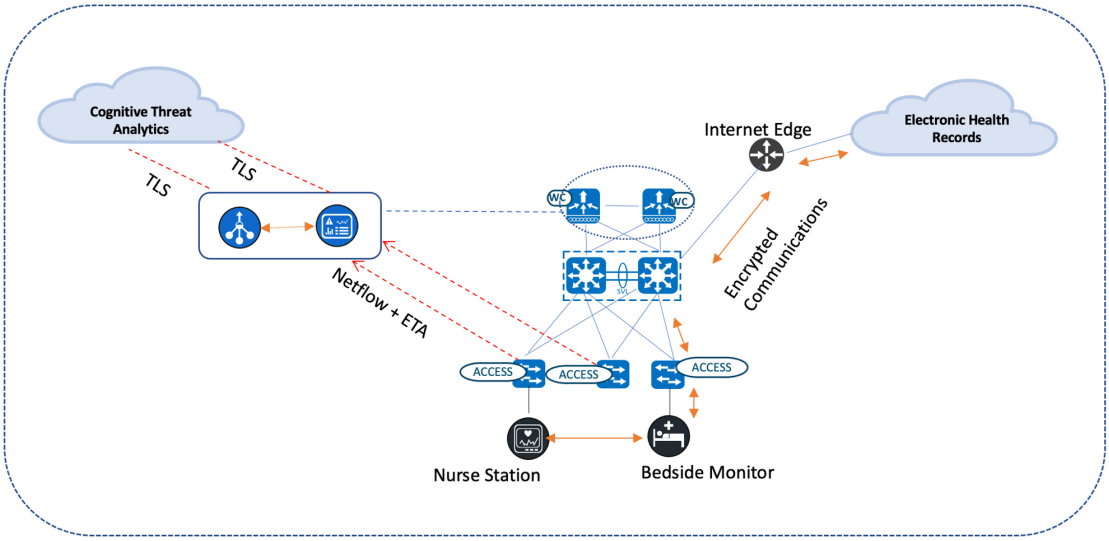
Cisco DNA Centerの Stealthwatch Security Analytics（SSA）アプリケーションを Catalyst アクセススイッチのプロビジョニング中に使用して、ETA/NaaS のユースケースを実行できます。医療機関は、ワークステーションと EHR システムが展開されている場所に関係なく、医療施設全体の有線ワークステーションと EHR システム間の通信に、最も安全な TLS ライブラリと暗号スイートを使用する必要があります。クラウド内の EHR サービスへのアクセスがより一般的（場合によっては必須）になるに従い、通信をより詳細に分析して、不審なアクティビティの兆候を確認する必要があります。



内部フローメタデータまたはフローの内部で発生したイベントに関する情報は、フロー モニタリング フレームワーク内で収集、保存、および分析できます。ディープ パケット インスペクションは今後実行できないため、このデータは

トラフィックが暗号化されている場合は特に重要となります。暗号化トラフィック分析（ETA）と呼ばれるこの内部フローメタデータは、フロー内のパケットの長さや到着時間など、プロトコルの詳細とは独立した新しいデータ要素やテレメトリを使用して導き出されます。それらのデータ要素は、暗号化および非暗号化フローの両方に等しく適用できます。ETA は、初期データパケット（IDP）とパケット長と時間のシーケンス（SPLT）の 2 つの主要なデータ要素を抽出します。それらの要素は、専用の NetFlow テンプレートを使用して Cisco Stealthwatch Enterprise に伝達されます。

Flexible NetFlow と組み合わせて使用すると、フローの寿命の完全なビューが利用可能になり、悪意のあるトラフィック、ネットワーク内の変則的挙動、およびカスタマイズ可能なポリシー違反を特定できます。ETA の実装時に、Cisco Stealthwatch が Cognitive Intelligence と統合されている場合、暗号化アセスメントに加えて、収集されたメタデータを使用して、トラフィックを復号化することなく、暗号化されたトラフィック内のマルウェアを検出できます。Flexible NetFlow および DNS 情報が IDP で見つかった ETA メタデータと組み合わされると、他の ETA データ要素（パケット長と時間のシーケンス（SPLT）など）による不審なトラフィックの検出を通じてマルウェアを識別するための有益な方法を得られます。デフォルトでは、企業のアドレス空間の外部にあるエンタープライズ ネットワーク境界を通過するトラフィック（つまり、DNS クエリを含む、インターネット向けトラフィック）のみが、マルウェア分析のために Cognitive Intelligence クラウドに送信されます。すべてのトラフィックがモニターされ、レコードが Cisco Stealthwatch フローコレクタにエクスポートされます。処理後、フローコレクタは、この外部トラフィックのメタデータのみをさらに分析するために、暗号化された TLS トンネルで Cognitive Intelligence クラウドに送信します。他のすべての内部トラフィックは、Cisco Stealthwatch で確立されたポリシーに準拠するため、および ETA データに基づく暗号化アセスメントのために、フローコレクタによって処理されます。次の図は、ローカル医療サーバー、ベッドサイドモニター、およびナースステーション間の通信、およびこれらのデバイスとクラウドベースの EHR システム間の通信を示しています。アクセススイッチでの SSA の有効化の詳細については、*Cisco DNA Center の Stealthwatch Security Analytics Service のユーザーガイド* [英語] を参照してください。



AI エンドポイント分析

Cisco AI Endpoint Analytics アプリケーションは、AI 主導の分析とネットワーク主導のディープ パケット インスペクションを組み合わせることで、次世代のエンドポイントの可視性を提供します。医療セグメントのエンドポイントの大部分は、Internet of Things（IoT）ベースであるため、エンドポイントをモニターするネットワーク管理者にとって、セキュリティは大きな課題となっています。病院のネットワークに接続されている患者のヘルスモニタリングデバイスに

接続している医師の場合を考えてみましょう。このデバイスがネットワーク全体にマルウェアを拡散し、広範な問題が発生した場合はどうなるでしょうか。Cisco AI Endpoint Analytics は、被害を最小限に抑えることで問題を解決します。

エンドポイントを保護するための最初のステップは、デバイスタイプの識別です。これは、エンドポイント プロファイリングとも呼ばれます。Cisco AI Endpoint Analytics は、ディープ パケット インスペクション（DPI）と機械学習（ML）に基づいて、エンタープライズネットワーク内の不明なエンドポイントの最大数を特定しようとします。エンドポイント プロファイリングは、さまざまなデータソースからのエンドポイントデータを集約して分析することから始まります。データソースの例には、ディープ パケット インスペクションや Cisco Identity Services Engine（ISE）をサポートするネットワークデバイスやアプライアンスなどがあります。Cisco AI Endpoint Analytics は、エンドポイントのタイプ、製造元、モデル、およびオペレーティングシステムを定義することで、詳細なエンドポイント プロファイリングを提供します。エンドポイントは、400 の使用可能な属性の組み合わせに基づいてプロファイリングされます。

エンドポイントを保護するための 2 番目のステップは、プロファイリングされたエンドポイントで、ネットワークセキュリティが侵害される変則的挙動が示されているかどうかを判断することです。信頼スコアは、ネットワークでの信頼性に基づいて、プロファイリングされたエンドポイントに割り当てられます。値の範囲は 1（低信頼）～ 10（高信頼）です。信頼スコアは、エンドポイント認証、コンプライアンス、エンドポイント異常検出など、利用可能なすべてのインサイトを使用して計算されます。Cisco AI Endpoint Analytics アプリケーションの詳細については、*Cisco DNA Center ユーザーガイド* [英語] を参照してください。

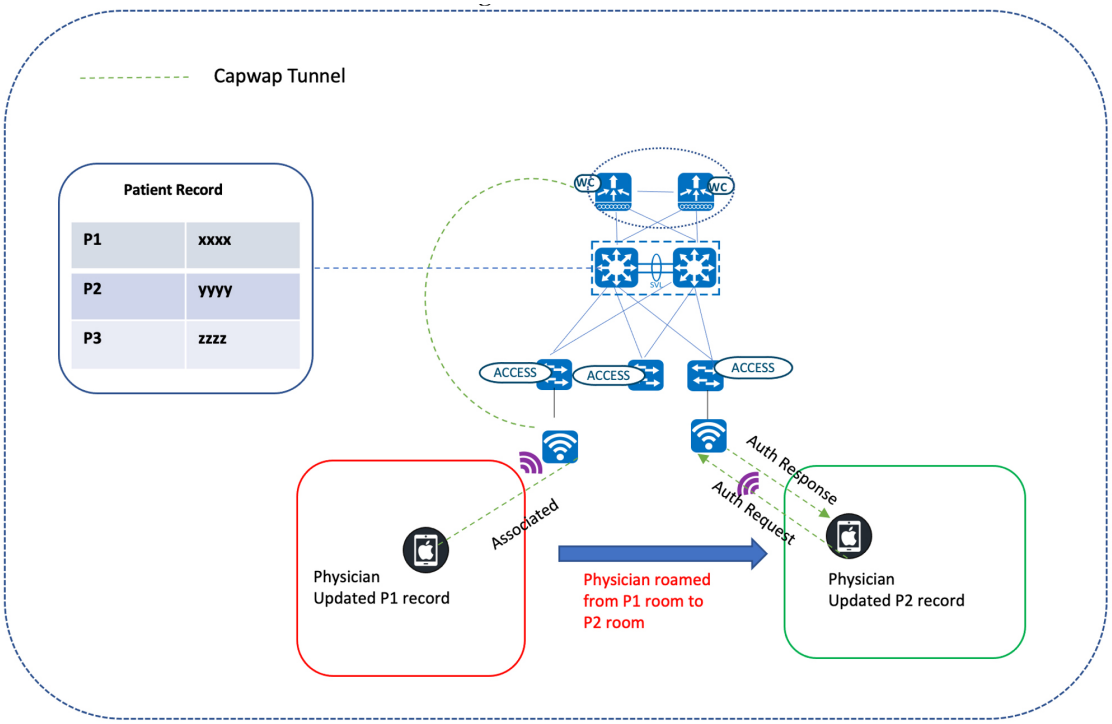
モビリティ

ワイヤレスローミング

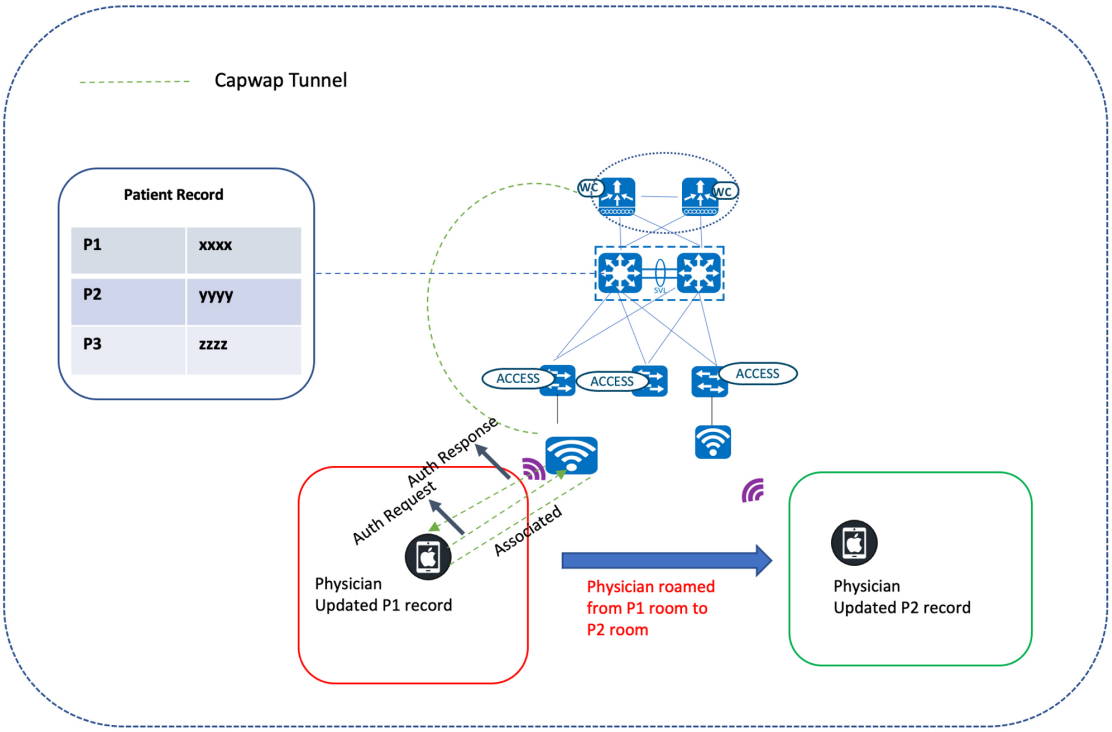
シスコのワイヤレス モビリティ ソリューションは、医療サービスの効率を向上させることを目的としています。回診中の医師は、ワイヤレスラップトップを使用して患者のカルテを更新できるため、他のスタッフは最新情報を入手できます。栄養士やナースは、ワイヤレスタブレットを使用して、最新のオーダーを確認したり、検査結果を確認したりできます。患者は、入院待ちの列で待つ必要がなくなります。登録係は、ワイヤレスタブレットを使用して、患者が診察を待っている間に登録を完了できます。中断のない音声およびデータサービスをサポートするには、多数のクライアントに対するシームレスなモビリティが不可欠です。医療業界では、CCKM や 802.11r/k/v などの高速ローミングが有効になっています。高速ローミングの IEEE 標準である 802.11r には、クライアントがターゲット AP にローミングする前でも新しい AP との最初のハンドシェイクが実行される、Fast Transition（FT）と呼ばれるローミングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換を送信した後で、クライアントと AP に適用されます。

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- **Over-the-Air**：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信します。



- **Over-the-DS**：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP の通信は、クライアントと現在の AP 間の FT アクションフレームで実行されてから、コントローラによって送信されます。



トラフィックの最適化

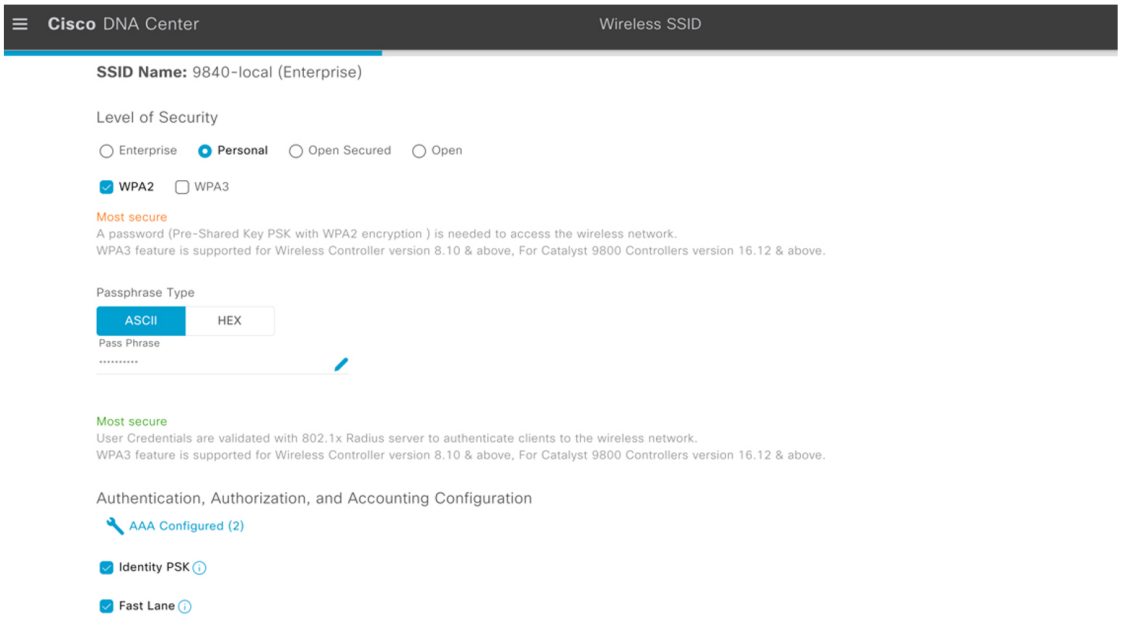
自動 QoS

ワイヤレス インフラストラクチャを使用するインタラクティブなアプリケーションが増えるにつれて、QoS の重要性がますます高まっています。QoS により、ネットワークマネージャはネットワークユーザーとの SLA を確立できます。また、より効率的なネットワークリソースの共有を可能にし、ミッションクリティカルなアプリケーションの処理を迅速化し、時間的制約のあるマルチメディアおよび音声アプリケーション トラフィックを優先できます。QoS では次の方法で実現されます。

- 重要なユーザーおよびアプリケーションの専用帯域幅の予約
- ジッタおよび遅延の制御（リアルタイム トラフィックに必要）
- ネットワークの輻輳の管理と最小化
- トラフィックフローをスムーズにするネットワークトラフィックのシェーピング
- ネットワーク トラフィックの優先度の設定

医療環境では、QoS の実装はポリシーにより決まり、さまざまな環境で使用されるアプリケーションによってそれぞれの QoS ポリシーが決まります。

Cisco DNA Center は、Apple クライアントから発信されるトラフィックの優先順位付けのために、SSID の作成時に AutoQoS Fastlane のプロビジョニングを有効にします。



次の設定は、Cisco DNA Center による WLC プロビジョニング中にワイヤレスコントローラにプッシュされます。

```
wireless profile policy 9840-local_Floor1_NF_5bfebcd0
 aaa-override
 accounting-list default
 autoqos mode fastlane
 cts inline-tagging
```

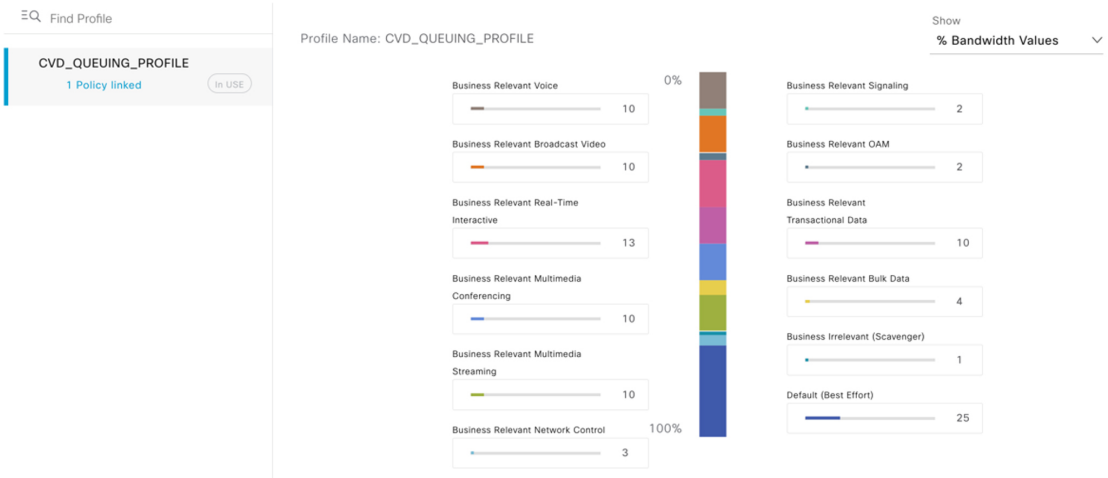
```
 cts role-based enforcement
 description 9840-local_Floor1_NF_5bfebcd0
 dhcp-tlv-caching
 exclusionlist timeout 180
 http-tlv-caching
 radius-profiling
 service-policy input platinum-up
 service-policy output platinum
 vlan Vlan510
```

さまざまな組み込み AutoQoS プロファイルは、トラフィックの特性に基づいて、さまざまなマクロに分類されます。

- エンタープライズ
- 音声
- ゲスト

MQoS

IOS-XE ベースのワイヤレスコントローラでの NBAR2 ベースのアプリケーション QoS ポリシーの一部として、Cisco DNA Center は Cisco Validated Design キューイングプロファイルをプロビジョニングします。



Cisco DNA Center は、そのマーキング、キューイング、およびドロッピング処理を、IETF RFC 4594、およびアプリケーションに割り当てた関連するビジネスカテゴリに基づいて実行します。詳細については、*Cisco DNA Center* ユーザーガイド [英語] の「Application Policies」を参照してください。

以下に設定例を示します。

```
9840-hca#show policy-map 9840-local_DNA-MARKING_0550e02f
  Policy Map 9840-local_DNA-MARKING_0550e02f
    Class 9840-local_VOICE_0550e02f
      set dscp ef
    Class 9840-local_TRANS_DATA_0550e02f
      set dscp af21
    Class 9840-local_SCAVENGER_0550e02f
      set dscp cs1
    Class 9840-local_REALTIME_0550e02f
      set dscp cs4
    Class 9840-local_MM_STREAM_0550e02f
      set dscp af31
    Class 9840-local_BROADCAST_0550e02f
```

```
    set dscp cs5
  Class 9840-local_OAM_0550e02f
    set dscp cs2
  Class 9840-local_SIGNALING_0550e02f
    set dscp cs3
  Class 9840-local_MM_CONF_0550e02f
    set dscp af41
  Class 9840-local_CONTROL_0550e02f
    set dscp cs6
  Class 9840-local_BULK_DATA_0550e02f
    set dscp af11
  Class class-default
    set dscp default
```

ゲストアンカーリング

無線ゲスト アクセス

Cisco DNA Center は、次の機能を備えたワイヤレス ゲスト アンカーリング ソリューションを提供します。

- サービス ワイヤレス コントローラをフォーリンコントローラとしてプロビジョニングする。
- DMZ エリア内のアンカーコントローラをプロビジョニングする（ゲストユーザーがインターネットに到達するためのゲートウェイとして機能します）。

ゲストトラフィックは、フォーリンコントローラに接続されたサービス AP から DMZ 内のアンカーコントローラまで、CAPWAP を介してトンネリングされます。

外部ゲスト

```
wireless profile policy guest-camp_Global_GA_7ae528ce
 aaa-override
 accounting-list default
 description guest-camp_Global_GA_7ae528ce
 dhcp-tlv-caching
 exclusionlist timeout 180
 http-tlv-caching
 mobility anchor 90.1.1.7 priority 3
 mobility anchor 90.1.1.8 priority 3
 nac
 service-policy input silver-up
 service-policy output silver
 no shutdown
!
wlan guest-camp_Global_GA_7ae528ce 18 guest-campus2
 mac-filtering dnac-cts-guest-camp-1d1eb5df
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
```

アンカーゲスト

```
wireless profile policy guest-camp_Global_GA_7ae528ce
 aaa-override
 accounting-list default
 description guest-camp_Global_GA_7ae528ce
 dhcp-tlv-caching
 exclusionlist timeout 180
```

```
 http-tlv-caching
 mobility anchor
 nac
 service-policy input silver-up
 service-policy output silver
 vlan Vlan91
 no shutdown
!
wlan guest-camp_Global_GA_7ae528ce 22 guest-campus2
 mac-filtering dnac-cts-guest-camp-1d1eb5df
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
```

有線ゲスト アクセス

有線ゲストアクセスを使用すると、有線ポートから製造業者またはベンダーの Web サイトに接続して機器のメンテナンス、ソフトウェアやファームウェアの更新ができます。有線ゲストセッションは、指定された有線イーサネットポートに接続され、設定された認証方式（OPEN または WebAuth）を使用して完了します。有線ゲストセッションは、ゲスト フォーリン コントローラから発信される CAPWAP トンネルを介して、DMZ 内のゲストアンカーコントローラで終了します。有線ゲストアクセスは、ゲストアンカーとゲストフォーリンコントローラを備えた 2 コントローラソリューションです。このタイプの展開では、有線ゲストトラフィックがエンタープライズ ユーザー トラフィックから分離されます。

外部ゲスト

```
wireless profile policy PP_PGN-VIP-Wired
guest-lan enable-session-timeout
 mobility anchor 90.1.1.8 priority 3
 no shutdown
!
guest-lan profile-name PP_PGN-VIP-Wired 1 wired-vlan 515
 no security web-auth
 no shutdown
```

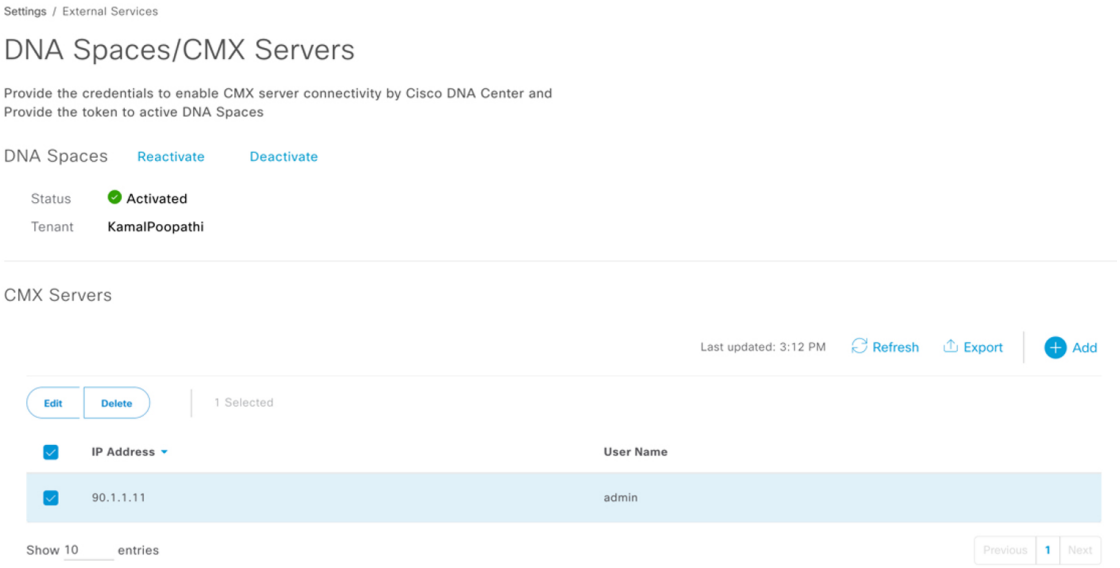
アンカーゲスト

```
wireless profile policy PP_PGN-VIP-Wired
guest-lan enable-session-timeout
 mobility anchor
 vlan Vlan91
 no shutdown
!
guest-lan profile-name PP_PGN-VIP-Wired 1
 no security web-auth
 no shutdown
```

ロケーション サービス

CMX および Cisco Spaces

患者と医療機器のモビリティは、高品質の患者ケアに不可欠です。Cisco DNA Center は、Wi-Fi タグ、ラップトップ、電話などのモバイルアセットを追跡する CMX と Cisco Spaces の統合により、これらのユースケースに対応します。



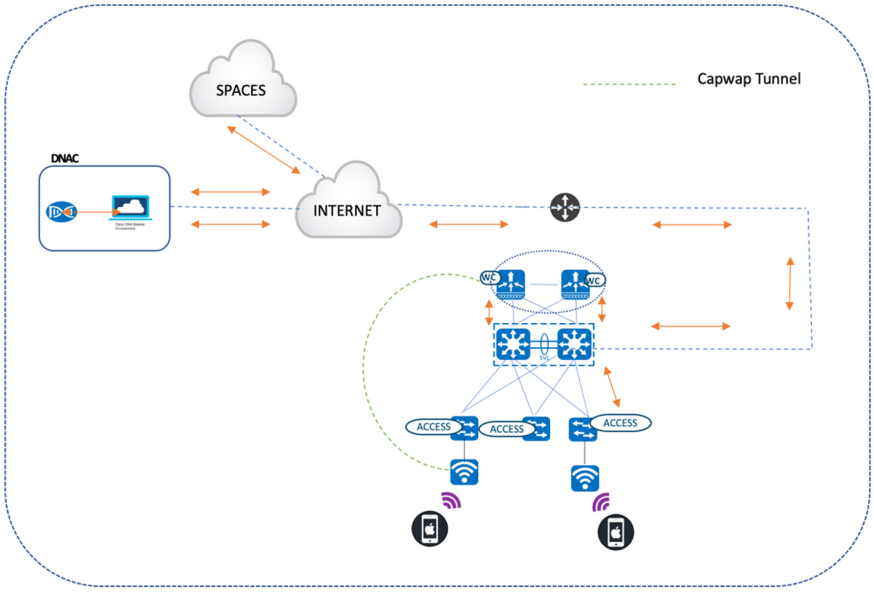
Cisco Spaces コネクタはオンプレミスにインストールされ、ワイヤレスコントローラとの NMSP 接続を確立します。この接続を介して、集約データがコントローラとアクセスポイントから Cisco Spaces にリレーされます。Cisco Spaces コネクタの設定については、*Cisco Spaces：コネクタ コンフィギュレーション ガイド* [英語] の「Prerequisites」の章を参照してください。

次に、Cisco Spaces コネクタ/CMX を Cisco DNA Center の [Wireless Network Settings] ページで対応するサイトにマッピングし、WLC の Cisco Spaces コネクタに NMSP マッピングをプッシュするようにワイヤレスコントローラをプロビジョニングします。

アクセスポイントは、Cisco DNA Center の [Network Hierarchy] ページで設定されたワイヤレスマップの対応するフロアの下に配置されます。アクセスポイントの同じ位置が Cisco Spaces（Detect and Locate アプリケーション内）に反映されます。このアプリケーションは、アクセスポイントに関連付けられたクライアント、不正 AP、不正クライアント、および干渉源も追跡します。Wi-Fi アセットタグが添付されている医療アセットは、Cisco Spaces でも追跡できます。

次のトポロジは、イベントの論理フローを示し、Cisco Spaces と Cisco DNA Center がどのように同期しているかを示しています。

- Cisco DNA Center が Cisco Spaces に登録されている。
- WLC が Cisco Spaces コネクタに登録されている。
- Cisco Spaces コネクタが、WLAN 内の AP とエンドポイントの集約情報を Cisco Spaces に転送する。
- Cisco DNA Center のワイヤレスマップが Cisco Spaces と同期される。
- Cisco Spaces の Detect and Locate アプリケーションが、Cisco DNA Center によって管理されているワイヤレスマップにクライアントマップの場所を転送する。Cisco DNA Center と Cisco Spaces の統合の詳細については、*Cisco Spaces コンフィギュレーション ガイド* [英語] の「Cisco DNA Center Integration」の章を参照してください。



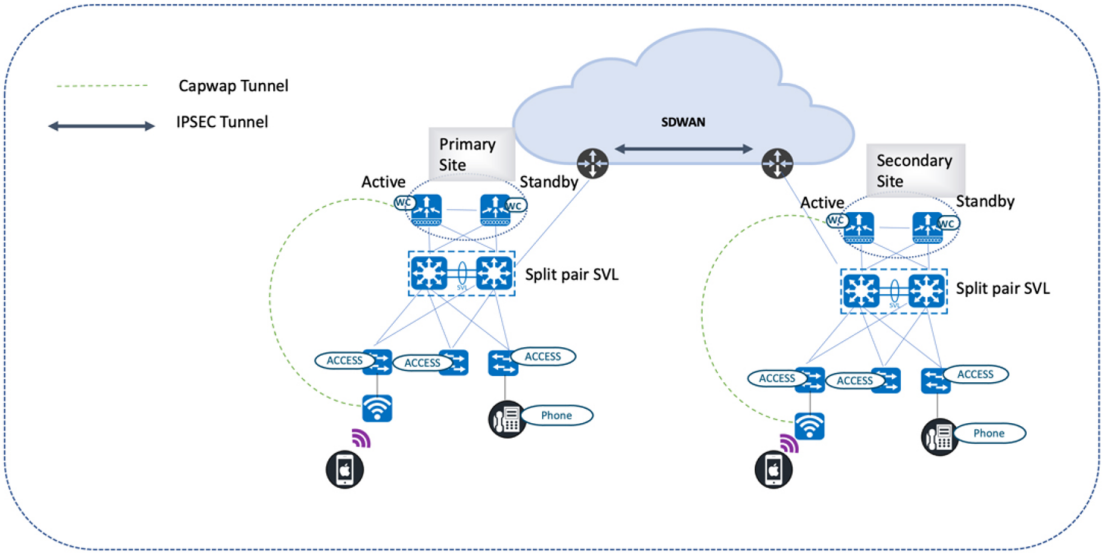
ハイ アベイラビリティ

AP/クライアント SSO

医療ネットワークは、継続的なサービスを提供するために十分な復元力を備えている必要があります。高可用性機能（AP SSO/クライアント SSO）は、この目的を達成するために特に重要です。Cisco DNA Center では、RP+RMI HA セットアップを形成でき、2 つの物理ワイヤレスコントローラを接続して、1 つのコントロール/データプレーンでアクティブとスタンバイのペアを形成できます。アクセスポイントとアクティブ WLC の間には、常に単一の CAPWAP トンネルがあり、アクティブ WLC とスタンバイ WLC の両方の AP データベースが同期されます。フェールオーバーが発生すると、スタンバイ WLC が新しいアクティブ WLC になります。また、接続されたアクセスポイントの詳細がすでにデータベースに格納されているため、AP がダウンして CAPWAP トンネルの再確立が必要になることはないため、AP が稼働し続けるシームレスなフェールオーバーが実現します。同様に、RUN 状態にあるワイヤレスクライアントが、アクティブとスタンバイの WLC 間で同期されます。フェールオーバー中、クライアントを再度関連付ける必要がなく、継続的なセッションを維持できます。

N+1 SSO

Cisco DNA Center は N+1 HA 機能も提供し、複数の地域にまたがるコントローラのコントローラ冗長性を提供します。RP+RMI HA セットアップとは異なり、AP SSO とクライアント SSO は N+1 セットアップではサポートされません。プライマリコントローラに障害が発生すると、AP がプライマリコントローラから接続解除されてセカンダリ バックアップ コントローラに接続するため、CAPWAP ステートマシンが再起動します。プライマリコントローラが動作を再開すると、AP がバックアップコントローラから接続解除されてプライマリ WLC に再接続します。詳細については、*Cisco Catalyst 9800* ワイヤレスコントローラ *N+1* 高可用性に関するホワイトペーパー [英語] の「Cisco DNA Center Configuration for N+1 High Availability」のトピックを参照してください。



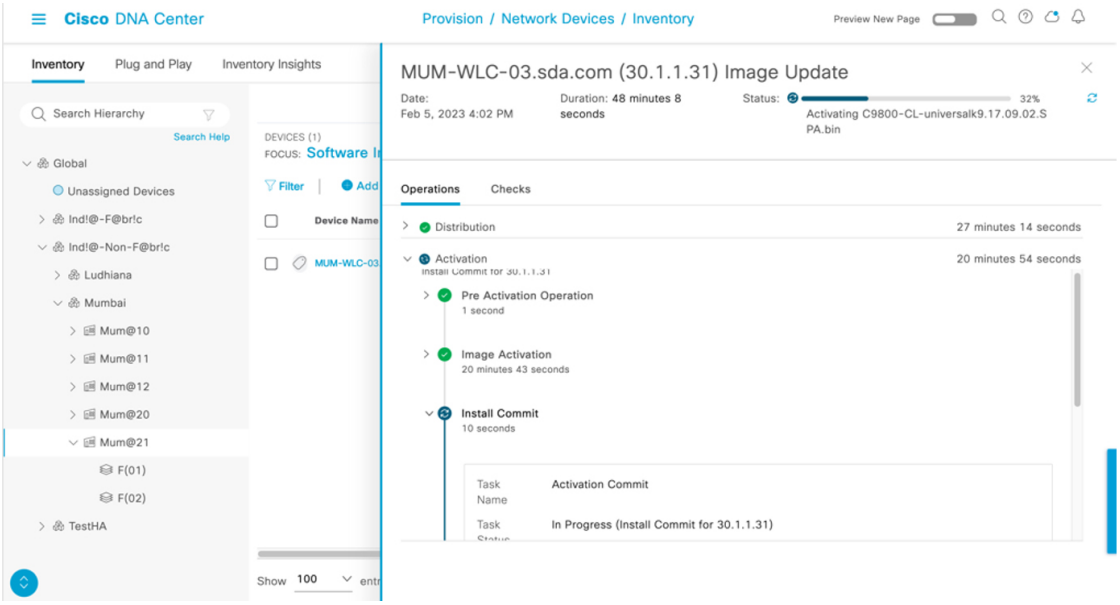
インサービス ソフトウェア アップグレード

Cisco DNA Center には、Cisco DNA Center ネットワーク内のデータ転送を中断することなく、HA 対応ワイヤレスコントローラを新しいバージョンにアップグレードできる In-Service Software Upgrade（ISSU）が用意されています。ISSU を使用する場合は、新しいメジャーバージョンにのみアップグレードできることに注意してください（つまり、ポイントまたはパッチバージョンにはアップグレードできません）。

ISSU を使用する場合は、次のタスクを完了する必要があります。

1. コントローラのソフトウェアイメージをフラッシュメモリにオンボードします。
2. アクセスポイントイメージを関連するアクセスポイントにダウンロードします。
3. コントローラのソフトウェアイメージをインストールします。
4. 変更を保存します。

この機能の詳細については、*Cisco DNA Center* ユーザーガイド [英語] の「Upgrade a Software Image with ISSU」のトピックを参照してください。

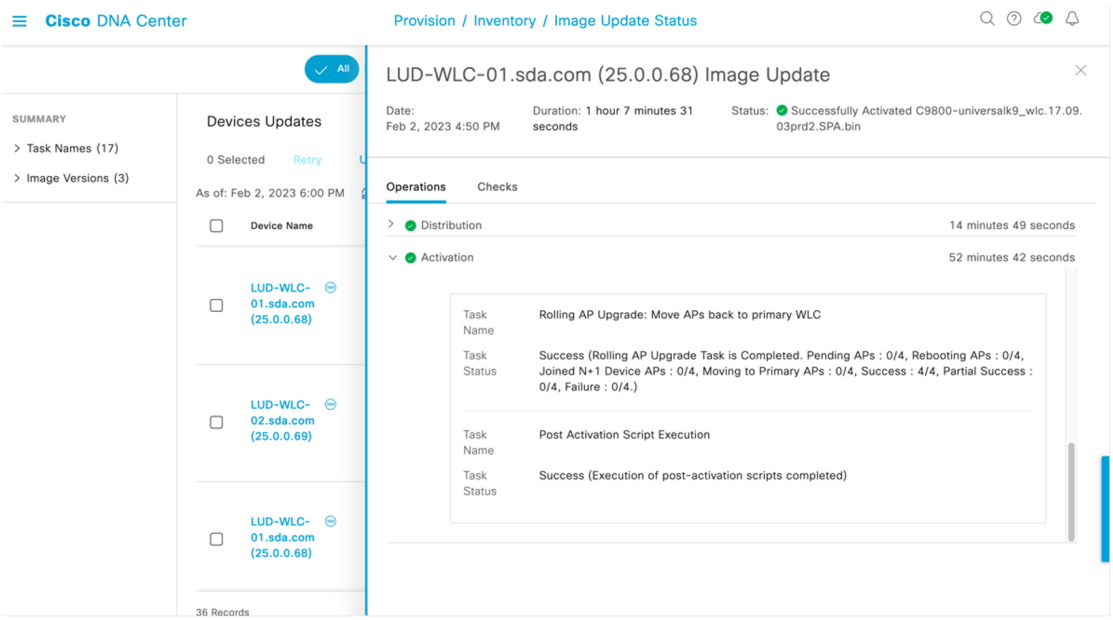


ローリング アクセス ポイント アップグレード

高可用性（HA）は、ワイヤレスコントローラ専用ではありません。また、Cisco DNA Center は、ローリング アクセスポイントアップグレード機能により、HA をアクセスポイントに拡張します。この機能を有効にすると、次の利点があります。

- N+1 トポロジでの段階的なアクセスポイントのアップグレードが可能になる。
- アップグレードの実行中に、ネットワークに接続しているユーザーが継続的なサービスを利用できる。
- RRM ベースのネイバー情報と、ユーザーが指定したアップグレードの割合（5、15（デフォルト）、または 25）を使用して、候補アクセスポイントが自動的に選択される。

この機能の詳細については、*Cisco DNA Center* ユーザーガイド [英語] の「About N+1 Rolling AP Upgrade」のトピックを参照してください。



テレメトリベースのアシュアランス

医療機関には、複数のエンドポイントを持つ大規模なデバイスサイトがあります。管理者は、これらのサイトの管理、追跡、およびモニタリングが面倒であると指摘しています。Cisco DNA アシュアランス は、ネットワークとそのエンドポイントの正常性を継続的に評価することで、これらのタスクを簡素化します。テレメトリデータロガー（TDL）は、Cisco DNA Center によって管理されるデバイスからストリーミングテレメトリ データを収集するため、ネットワーク管理者は、ネットワーク ノードおよび有線クライアントとワイヤレスクライアントの両方をリアルタイムでモニターできます。このデータを使用して、管理者は発生した技術的な問題をトラブルシューティングできます。

テクニカル リファレンス

- https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/CLA_HealthcareSolution.pdf
- https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/07cs1084-mobforhc_bro_aha_pdf_102307.pdf
- https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/mobility/wireless-design-guide-healthcare.pdf
- https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/Cisco-Validated-Solution-Profiles/b_cisco_validated_solution_profile_healthcare_vertical.html
- https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html?oid=wpretr023097
- https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-ha-rau-apsp-apdp-issu-rel-17-1.pdf
- https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc24

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。