Cisco Catalyst Center 2.3.7

目次

はじめに

Cisco Catalyst™ Center（旧 Cisco DNA Center）は、ネットワークの管理、シスコへの投資の最適化、IT 支出の削減などを実現する強力なネットワークコントローラであり、管理ダッシュボードでもあります。Catalyst Center は、ネットワークの実行を簡素化するために、すべての基本的な管理タスクに対して単一のダッシュボードを提供します。このプラットフォームにより、IT 部門は変化や課題に迅速かつよりインテリジェントに対応できます。

設計：直感的なワークフローを使用し、ネットワークデバイスの展開場所からネットワークの設計を開始します。Cisco Prime® Infrastructure および Cisco® Application Policy Infrastructure Controller Enterprise Module（APIC-EM）のユーザーは、既存のネットワーク設計とデバイスイメージを Catalyst Center に簡単にインポートすることができます。

- **ポリシー：**ビジネスニーズに基づいて高度にセキュアなアクセスとネットワークのセグメント化を促進する、ユーザーとデバイスのプロファイルを定義します。アプリケーションポリシーを使用すると、ビジネスクリティカルなアプリケーションは、ネットワークの輻輳に関係なく、一貫したパフォーマンスを提供できます。
- **プロビジョニング：**ポリシーベースの自動化を使用して、ビジネスの優先順位に基づいてネットワークにサービスを配信し、デバイスの導入を簡素化します。ゼロタッチ デバイス プロビジョニングおよびソフトウェアイメージ管理機能により、デバイスのインストールまたはアップグレード時間が数時間から数分に短縮され、市販のシスコ製デバイスのプラグアンドプレイ機能を使用して、新しいリモートオフィスを容易にオンライン化できます。さらに、Cisco Secure Network Analytics（旧 Cisco Stealthwatch）サービスは、NetFlow および暗号化トラフィック分析（ETA）を分析サービスに送信するため、ネットワーク要素をプロビジョニングします。
- **アシュアランス：**ネットワーク上のすべてのポイントをセンサーに変え、アプリケーション パフォーマンスやユーザー接続に関する継続的なストリーミングテレメトリをリアルタイムで送信できます。これにより、自動的なパストレースの可視性とガイド付きの修復が連動し、ネットワークの問題が問題になる前に数分で解決されます。Cisco Secure Network Analytics の自動 NetFlow スイッチ設定は、暗号化されたトラフィックに隠されている場合でも、脅威の検出と軽減を提供します。
- **プラットフォーム：**オープンで拡張可能なプラットフォームにより、サードパーティのアプリケーションとプロセスは、Catalyst Center とデータやインテリジェンスを交換できます。これにより、Catalyst Center のネットワーク インテリジェンスに基づいてワークフロープロセスを自動化することで、IT 運用が向上します。

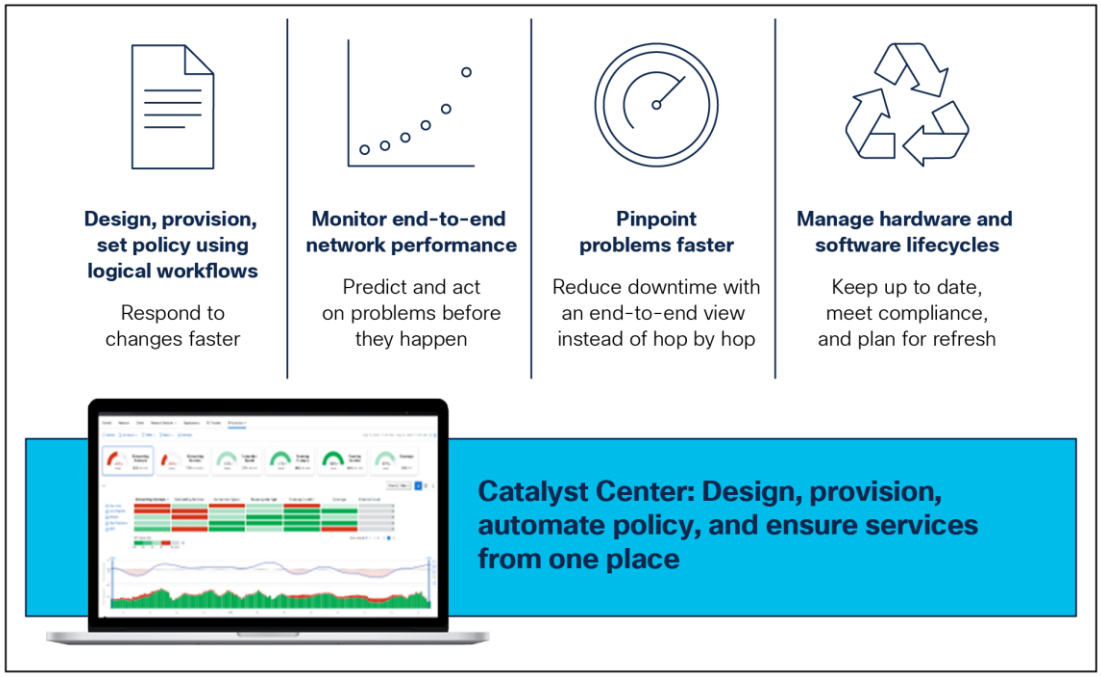

図 1.
Catalyst Center

Catalyst Center は、このすべての機能を統合コントローラに組み込み、一括管理によって提示する、集中型のネットワーク管理システムです。ハードウェアアプライアンスに展開することも、仮想アプライアンスとして展開することも可能です。

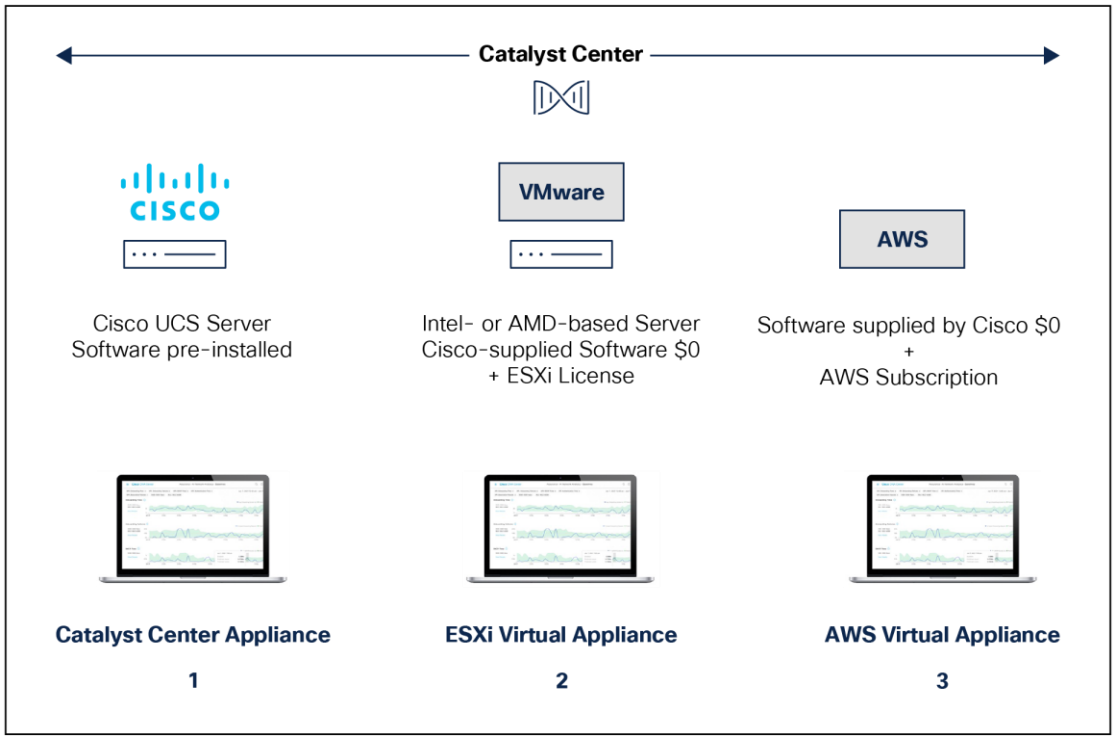

図 2.
Catalyst Center の仕組み

ライセンス

Catalyst Center は、柔軟な展開オプションを提供するソフトウェアソリューションです。Catalyst Center ハードウェアアプライアンスに展開することも、AWS 上に仮想アプライアンスとして展開することも可能です。このソリューションでは、スイッチ、ルータ、アクセスポイント、コントローラなどのネットワークデバイスからテレメトリデータを受信します。Catalyst Center へのデータ送信をデバイスに許可するには、そのデバイスを組織の Catalyst または Cisco DNA ライセンス サブスクリプションに含める必要があります。Catalyst または Cisco DNA Advantage ライセンス サブスクリプションによって Catalyst Center の完全な機能を購入することをお勧めします。Catalyst Center の限定機能は、Cisco DNA Essentials ライセンス サブスクリプションでも利用できます。ワイヤレス、スイッチング、および SD-WAN とルーティングのサブスクリプションは、3 年および 5 年の期間で利用できます。ワイヤレスとスイッチングは 7 年間の利用もできます。すべての Catalyst および Cisco DNA ソフトウェア ライセンス サブスクリプション オプションには、シスコの組み込みソフトウェアサポートおよびダウンロードが含まれています。

以下のリンクは、それぞれのスイートに含まれる主な機能の詳細を示すマトリックスを開いています。

- スイッチング機能マトリックス
- ワイヤレス機能マトリックス
- SD-WAN とルーティングのマトリックス

ライセンスに加えて、拡張パックは、Cisco Identity Services Engine（ISE）、Cisco Spaces、Cisco Secure Network Analytics（旧 Stealthwatch）、Cisco ThousandEyes®、その他のライセンス、アプライアンス、およびサービスを 1 つの便利なバンドルで柔軟に購入する方法です。SD-Access、Cisco Zero-Trust ソリューション、暗号化トラフィック分析（ETA）、位置分析、アシュアランスなどのシスコ ネットワーキング ソリューションを強化します。Catalyst または Cisco DNA ソフトウェアライセンスにパックを追加して、ニーズに合ったライセンス数を選択できます。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション：**スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。製品アクティベーションキー（PAK）は不要です。
- **管理の統合：**My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するため、ユーザーは所有および使用している製品やサービスを常に把握できます。
- **ライセンスの柔軟性：**ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの詳細については、cisco.com/go/licensingguide [英語] を参照してください。

自動化機能

表 1. Catalyst Center Automation の機能と利点

機能	説明と利点
ネットワーク検出	ネットワークデバイスを自動的に検出し、詳細なデバイスレベルのデータを使用して物理トポロジにマッピングします。ディスカバリ機能は次のプロトコルと方法を使用して、IP アドレス、ネイバーデバイス、デバイスに接続しているホストなどのデバイス情報を取得します。 • Cisco Discovery Protocol • エンドポイント用の Link Layer Discovery Protocol（LLDP） • ホスト検出用の IP Device Tracking（IPDT）および Address Resolution Protocol（ARP）エントリ • IP フォンと一部のサーバー検出用の LLDP Media Endpoint Discovery（LLDP-MED） • Simple Network Management Protocol（SNMP）バージョン 2 および 3
インベントリ	ホストの IP アドレス、MAC アドレス、およびそのデータベース内のデバイスに関するネットワーク アタッチメント ポイントなどの詳細を取得して保存します。最初の発見後、Catalyst Center は定期的にネットワークをスキャンして、IT の「信頼できる唯一の情報源」を作成します。このインベントリは、すべてのネットワーク デバイスを含み、また企業ネットワーク全体を抽象化します。バージョン管理のためにデバイスとそのデバイス上のソフトウェアイメージの更新されたインベントリを保持し、正しいデバイスとイメージのバージョンが使用されるようにアプリケーション（Software Image Management [SWIM] や Cisco Easy QoS など）にデータを提供します。これにより、アプリケーションはデバイス非依存となるため、デバイス間の構成の違いが問題になりません。
ネットワーク設計とプロファイルベースの管理	地理空間マップにエリアや建物を追加することで、ネットワークを階層的に管理できます。最初にサイトを定義してから、建物をサイトに追加し、詳細なフロアプランを持つフロアを建物に追加します。Catalyst Center では、ユーザーがプロファイルを定義できます。プロファイルは、デバイスクレデンシャル、DHCP、DNS サーバー、AAA サーバー、IP アドレスプールなどの一般的なネットワーク設定で構成されます。SSID や RF プロファイルなどのワイヤレス設定は、グローバルで作成し、サイトレベルでカスタマイズできます。これらのプロファイルは、ネットワーク自動化の基盤となります。ネットワークプロファイルは、Cisco Network Function Virtualization Infrastructure Software（NFVIS）、回送、ファイアウォール（Cisco 適応型セキュリティアプライアンス（ASA）を含む）、スイッチング、およびワイヤレス用に作成できます。
シスコ ネットワーク プラグ アンド プレイ（PnP）	市販のシスコ製デバイスをネットワークに接続するだけでプロビジョニングできます。シスコネットワークの PnP 機能は、シスコの有線デバイスおよびワイヤレスデバイスのエンタープライズ ネットワーク ポートフォリオ全体において、安全性、拡張性に優れ、シームレスで統一されたゼロタッチ導入をお客様に提供します。オンサイトサポート訪問なしで、数分で新しいデバイスを導入できます。反復作業を排除し、ステージングを排除します。ネットワーク PnP は、新しいデバイスの導入プロセスを大幅に簡素化することで、企業の負担を軽減します。これにより、運用コスト（OpEx）も大幅に削減することができます。詳細については、『Cisco ネットワーク プラグ アンド プレイ ソリューション ガイド』（https://www.cisco.com/c/ja_jp/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html）を参照してください。
ソフトウェアイメージ管理（SWIM）	ソフトウェアアップグレードを管理し、ネットワーク全体のイメージバージョンと設定の一貫性を制御します。新しいソフトウェアイメージとパッチの導入を迅速化および簡素化します。事前チェックと事後チェックにより、アップグレードによる悪影響がないことを確認できます。これは、ソフトウェアイメージの中央リポジトリを構築してデバイスに適用する簡単な方法です。管理者は、デバイスファミリのソフトウェアイメージをゴールデンとしてマークし、リポジトリで定義されているゴールデンバージョンに準拠するソフトウェアイメージおよびパッチバージョンにデバイスをアップグレードできます。Catalyst Center では、通常のイメージを管理するのと同じ方法で、インテントから事前チェックと事後チェックまでパッチがサポートされます。また、ソフトウェア メンテナンス アップデート、サブパッケージ、ROM モニタ、AP サービスパック、および AP デバイスパックのアップグレードがベースイメージに適用されるタイミングも追跡します。

機能	説明と利点
ネットワーク遵守の監査と修復	ネットワーク遵守監査機能により、ネットワーク事業者は企業標準に準拠していないデバイスを迅速に評価できます。ネットワーク遵守修復機能を使用すると、ネットワーク事業者は、すべてのネットワーク要素について、実行（実稼働）構成とスタートアップ構成を自動的に同期できます。ネットワーク事業者は、1 つまたは複数のデバイスを選択し、変更を表示および検証し、それらのデバイスを選択して同期し、コンプライアンスを維持するためにそれらを修復できます。これらの 2 つの機能を組み合わせることで、人の関与とエラーが減り、ネットワークが意図した構成標準を実行するように確保するうえで役立ちます。
デバイスのタギング	管理者は、共通の属性を共有するデバイスを関連付けるために、ネットワークデバイスにタグを付けることができます。たとえば、プラットフォーム ID、Cisco IOS リリース、またはロケーションに基づいて、タグを作成し、デバイスをグループ化できます。特殊なニーズに基づいてデバイスをグループ化できます。
設定の変動の可視性	ネットワーク事業者は、任意の 2 つのデバイス設定バージョンを非常に視覚的な方法で比較できます。デバイス設定の異なるバージョンを使用できるようにすることで、すべての設定変更の正確なアカウンタビリティが可能になります。
デバイス交換および RMA ワークフロー	ワークフローテンプレートでは、スイッチ、ルータ、およびアクセスポイントの交換（RMA）が可能です。Cisco IOS ソフトウェア、設定、およびライセンスの復元が含まれます。また、Cisco ISE、証明書サーバー、Catalyst Center インベントリなどの運用システムでのデバイスの交換もすべて含まれます。時間を節約し、既存のセットアップ、ライセンス、および KPI トレンドを保持します。
ブランチ展開の自動化	物理および仮想ブランチの自動化のためのワークフローが簡素化されました（0 日ルータ、および NFV 設計）。次の簡単な手順で WAN デバイスとサービスを導入準備できます。 ネットワーク設定、サービスプロバイダー、および IP プールを設定 ルータまたは仮想プロファイルを設計 サイトに割り当て、およびネットワークデバイスをプロビジョニング
ワイヤレスの自動化	シンプルなワイヤレス導入と自動化のためのインテントベースのワークフロー • ネットワークプロファイル：単一または複数のサイトを表すことができるワイヤレスプロパティのコンテナ • SSID の作成の簡素化 • ワイヤレスネットワークの高度な RF サポート • Cisco FlexConnect® または集中型ワイヤレス導入を可能にする単一のワークフロー。 • AP の PnP プロビジョニング • IP アクセスコントロールリスト（ACL）のサポート • SD-Access Wireless のみのアクセスおよびアクセス コントロール ポリシー 詳細については、ワイヤレス自動化のホワイトペーパーを参照してください。
Cisco StackWise® Virtual サポート	Cisco Catalyst® 9500 および 9400 シリーズ StackWise Virtual スイッチの基本自動化（インベントリ、ディスカバリ、SWIM、トポロジ、テンプレートプログラマ）およびアシュアランスのサポート。Cisco Catalyst 9000 プラットフォームの StackWise Virtual テクノロジーにより、2 つの物理スイッチを 1 つの論理エンティティにまとめてクラスタリングできるため、ハイアベイラビリティ、スケーラビリティ、管理、メンテナンスなど、ネットワーク設計のすべての領域が強化されます。お客様は、Catalyst Center を使用して StackWise Virtual デバイスを管理し、StackWise Virtual のポートとリンクの正常性とステータスを監視できるようになりました。

機能	説明と利点
ポリシーの作成	ネットワークの特定の部分のビジネス目的に基づいてポリシーを作成できます。ユーザーには、消費するサービスのポリシーを割り当てることができ、これらのポリシーはネットワーク全体で適用されます。ポリシーは、Catalyst Center によってネットワーク固有の設定とデバイス固有の設定に変換され、ネットワークの状態に基づいて動的に調整できます。インテントベース ネットワーキングにとって基本的に重要なポリシーは、必要なビジネス目的を定義し、ネットワークがサービスを保証できるようにします。
アプリケーションポリシーの作成	ビジネス関連性に基づいてアプリケーションにポリシーを割り当てることができます。これらのアプリケーションは、ポリシーを適用する必要があるサイト（場所）にアタッチできます。この機能により、ビジネスクリティカルなアプリケーションは、その使用が関連するサイトでより高い QoS 優先順位を持つことができます。これは、製造業でのマシンツーマシン制御や医療機関での救命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、およびカスタマー エクスペリエンス センターでのビデオやサポートサイトでの音声などのビジネスクリティカルなアプリケーションにとって重要です。
不正管理および aWIPS	Catalyst Center 内からのネットワーク上の不正および Cisco Adaptive Wireless Intrusion Prevention System（aWIPS）の脅威の検出をサポートします。[Rogue and aWIPS] ダッシュボードは、ネットワーク内で検出されたすべての不正アクセスポイントの詳細な攻撃分析とグローバルビューを提供し、最も優先順位の高い脅威を迅速に特定できるようにします。このダッシュボードの [Threat 360] ビューには、特定の脅威に関する詳細が表示されます。このビューには、クイックロケーションのマップビューと、影響を受けるすべてのクライアントが含まれます。
Meraki の検出と統合	ネットワーク上のすべての Cisco Meraki® デバイスを検出し、それらを Catalyst Center ダッシュボードに統合します。Cisco と Meraki の両方のデバイスの一括管理を提供します。
Meraki ワイヤレスプロビジョニング	Cisco Center 経由で Meraki アクセスポイントに SSID をプロビジョニングします。Meraki ダッシュボードを開くことなく、Catalyst Center を介して Meraki アクセスポイントに SSID を割り当てることができます。
Cisco Umbrella の統合	Cisco Umbrella® を Catalyst Center ダッシュボード内からサイトと SSID に展開できます。Cisco Umbrella は DNS レイヤセキュリティを提供します。これはセキュリティスタックを改善するための最も迅速かつ効果的な方法の 1 つです。次のブログを参照してください。https://blogs.cisco.com/networking/cisco-dna-center-and-cisco-umbrella-automate-your-journey-towards-dns-security [英語]

アシュアランス機能

表 2. Catalyst Center Assurance の機能と利点

機能	説明と利点
ネットワークおよびクライアント ヘルス ダッシュボード	有線および無線のネットワーク上のすべてのネットワークデバイスとクライアントの状態の概要を示す保証ダッシュボード。上位 10 件のグローバルな問題を示します。管理者は地理的サイト、デバイスリスト、クライアントリスト、またはトポロジごとにビューを展開できます。接続不良のデバイスまたは通信の問題がハイライトされ、推奨される修復アクションが示されます。ユーザーは、ヘルススコアの計算方法をカスタマイズできます。
Application Health ダッシュボード	ネットワーク上のすべてのアプリケーションの正常性の概要が示されます。ビジネス関連としてタグ付けされたアプリケーションに関する特別なセクションが含まれています。ビジネスに関連するアプリケーションの問題がハイライトされ、異常の推奨される修復アクションが示されます。

機能	説明と利点
ThousandEyes の統合	Cisco ThousandEyes エージェントは、Catalyst Center の GUI ベースのインストールプロセスを介して、サポートされているすべてのスイッチにインストールできます。アプリケーションはスイッチのフラッシュストレージに常駐するため、ThousandEyes を展開するための時間とコストを大幅に節約できます。ThousandEyes エージェントからのデータは、Catalyst Center によって使用され、アプリケーションのパフォーマンスを可視化し、管理者が問題のあるドメインを特定できるようにします。
Webex と Microsoft Teams の統合	音声、ビデオ、および共有コンポーネントの品質メトリックの統合ビューが表示され、管理者は Webex パフォーマンスおよび Microsoft Teams パフォーマンスをトラブルシューティングできます。ネットワーク事業者は、複数のインターフェイスを切り替えることなく、Catalyst Center の問題を迅速に特定して解決できます。
Cisco AI Network Analytics	AI と機械学習を使用することで、Cisco AI Network Analytics はネットワーク内のインテリジェンスを活用し、管理者がパフォーマンスの向上および問題解決を正確かつ効果的に行えるようにします。シスコは、お客様が問題、傾向、異常、および根本原因を非常に正確に特定できるようにすることで、ノイズと誤検出が大幅に削減される新しいレベルのネットワーク分析を採用しています。 **インテリジェントな問題の検出と分析** • AI 主導のパーソナライズされたベースライン：2 つのネットワークがあれば、それらは同じではありません。AI 主導のテクノロジーは、ネットワークに固有のユーザートレンド、サービス、およびアプリケーションメトリックを学習できます。次に、Catalyst Center Assurance で分析的な意思決定を行うためにカスタマイズされたパフォーマンス曲線を作成できます。ネットワークに固有のパフォーマンスパラメータの AI 主導のベースラインは、ネットワークの成長と変化に合わせて常に適応されます。これにより、AI 主導の分析エンジン（オンプレミスと Cisco Cloud の両方）が、このパーソナライズされたベースラインに基づいて、正常なものとそうでないものを正確に判断できます。 • AI 主導の異常検出：システムはパフォーマンスの問題を正確に検出し、異常ではあるが無害なネットワーク異常を無視できます。これにより、ネットワークに最も大きな影響を与える異常を正確に特定しながら、ノイズを減らすことができます。AI 主導の予測分析とプロアクティブなインサイトにより、ユーザーは障害を予測して防止できます。機械学習エンジンにより Wi-Fi 干渉、オンボーディング遅延、オフィストラフィック負荷などの増加を予測できます。これは、IP ネットワークでは、問題のあるイベントの前に、無害な単独または一連のイベントが発生することが多いためです。予測分析は、一連のイベントの相互関係を学習することで、ネットワーク管理者が予期しない事態を予測するのに役立ちます。 • AI 主導の高速修復：Cisco AI Network Analytics は、特定の問題の根本原因に関連する最も重要な変数を特定する、機械学習による高速修復を提供します。これにより、ユーザは問題や脆弱性を検出し、複雑な根本原因分析（Machine Reasoning Engine を使用、下記参照）を実行し、修正アクションをこれまでになく迅速に実行できます。今後のリリースでは、エンジニアが問題を解決するために実行する論理的なトラブルシューティング手順を実行するためにマシンの推論を有効にします。これらの機能はどちらも修復を促進し、チームの問題解決をより正確にし、全体的な生産性を向上させます。 • AI 主導のサイト分析：サイト分析は、IT チームがサイト全体のユーザー体験に影響を与える可能性のある根本的な問題を事前に特定するのに役立ちます。また、ネットワーク管理者にカスタマイズ可能な KPI の単一のビューを提供し、デバイス、ユーザー、およびアプリケーションの正常性を把握できるようにします。
機械推論エンジン（MRE）	次のインテリジェンスの進化を定義し、1 つのアクションの結果が次を決定する複雑なワークフローで役立ちます。これは、人間が物事を考え出し、多段階のタスクを達成する方法によく似ています。Catalyst Center が MRE を使用する例は、複数のデバイスにまたがる慎重な分析を必要とする、障害を起こす可能性のあるルーティングループの検出と修正です。これにより、IT チームの新しいメンバーは、エスカレーションすることなく複雑なタスクを実行できます。また、面倒なワークフローを自動化することで、IT チームの経験豊富なメンバーの時間を節約できます。 詳細については、ブログ https://blogs.cisco.com/networking/machine-reasoning-is-the-new-ai-ml-technology-that-will-save-you-time-and-facilitate-offsite-netops [英語] を参照してください。

機能	説明と利点
Wireless 3D Analyzer	Wireless 3D Analyzer は、数百万の空間 RF データポイントを詳細に分析し、ワイヤレスカバレッジを可視化する機能を提供します。ネットワーク事業者は、RF 強度によって最も影響を受けるエリアを特定し、クライアントの場所を表示して、さまざまな RF 環境をシミュレートし、内部環境の空間計画と予測を行うことができます。基本的なアーキテクチャ構造情報を読み込んだ後、ネットワーク事業者は、仮想オフィススペースに入り、アクセスポイントを移動するか、架空の壁を作成して、Wi-Fi 信号の伝播に与える影響を確認できます。Wireless 3D Analyzer は、ネットワーク事業者が WLAN のパフォーマンスを最大化し、問題箇所や WLAN の設計上の問題を迅速に特定するのに役立ちます。
ワイヤレス ネットワーク サービス分析	Cisco およびすべてのサードパーティサーバー全体のワイヤレスデバイスの認証、許可、アカウンティング（AAA）および Dynamic Host Configuration Protocol（DHCP）サービスをグローバルな包括的なビューで表示します。この機能は、これらの重要なサービスの全体的な正常性をすべて 1 つの場所にまとめ、最もパフォーマンスの低いサービスサーバー、サイトレベルの影響、およびエンドユーザーの影響の範囲を強調します。これにより、ネットワークオペレータはチケットの全体的な解決時間を短縮し、チケットの量を減らすことができます。
グローバル アシュアランス イベントビューア	グローバル アシュアランス イベントビューアは、ネットワーク管理者にすべてのデバイスからのイベントの統合されたビューを提供するため、そこで対処する最も重要なイベントを検索およびフィルタ処理することができます。イベントビューを使用すると、ユーザはネットワークの問題を特定、関連付け、トラブルシュートし、根本原因をすばやく見つけることができます。
Power over Ethernet（PoE）分析	スイッチで発生している電力負荷を可視化します。電力を過剰に消費しているエンドポイントデバイスと、過負荷になろうとしているスイッチにはフラグが付けられます。きめ細かな可視性により、スイッチで使用可能な電力が表示され、IoT エンドポイントデバイスを迅速にインストールできます。
Path Trace	オペレータは、クライアントからすべてのデバイスおよびサーバーへのアプリケーションまたはサービスのパスを可視化できます。クライアントやアプリケーションをクリックすると、通常は 6 ～ 10 分を要する日常の重要なトラブルシューティング タスクが瞬時に表示されます。ネットワークパスに沿って問題をトラブルシューティングします。 • 送信元から宛先へのパストレースを実行して、ネットワークパスに沿った各デバイスの主要なパフォーマンス統計をすばやく取得します。 • トラフィックフローをブロックまたは影響している可能性のある ACL を特定します。
True Trace	パス分析のためにデバイス上のライブトラフィックをキャプチャします。Catalyst Center の True Trace は、現在のパストレース機能を拡張し、各ホップの KPI、パスの劣化の詳細な理由、およびダウンロード可能なパケットキャプチャファイルを提供します。これらの詳細なインサイトにより、企業の展開におけるトラブルシューティングを迅速化し、運用コストを削減できます。
産業用スイッチのアプリケーション QoS（Quality of Service）サポート	Catalyst Center のアプリケーション QoS から QoS ポリシーを作成し、Cisco Catalyst IE3300 および IE3400 高耐久性シリーズ スイッチにプッシュします。Cisco Validated Design に基づいて、デフォルトの QoS トラスト設定とキューイング設定を適用したり、これらのデバイスのカスタム QoS ポリシーを作成したりします。これにより、QoS ポリシーをプッシュする複雑さが解消され、産業環境のエンドユーザーに優れたエクスペリエンスを提供できます。

機能	説明と利点
Wi-Fi 6 および 6e 対応ダッシュボード	新しい Wi-Fi の標準規格に合わせてネットワークを準備し、ハードウェアと設定の互換性を確認して、キャパシティの準備状況をチェックできます。この可視性により、アップグレードが迅速化され、最も必要な場所を最初にアップグレードできるようになります。アップグレード後、高度なワイヤレス分析により、Wi-Fi 6 の導入によるパフォーマンスとキャパシティの向上が示されます。 ワイヤレスクライアントを Wi-Fi バージョン（プロトコル）別に分類し、アップグレードの緊急度が最も高いエリアを示します。アップグレード後のワイヤレスシステムのパフォーマンスを表示します。 Wi-Fi 6 対応ダッシュボードを使用すると、お客様は 2 つの主要な側面を可視化できます。1 つは、複数の異なるサイトおよび場所にわたる Wi-Fi 6 に関するネットワークの対応状況を示します。準備評価の重要な側面には、ネットワークで見られる Wi-Fi 6 対応クライアントの数、ユーザーが Wi-Fi 6 をサポートする適切な AP モデルを持っているかどうか、AP とワイヤレス LAN コントローラ（WLC）が適切な OS バージョンを実行しているかどうか、Wi-Fi 6 構成が有効かどうかなどを評価することが含まれます。次に、ダッシュボードを使用すると、ユーザーは、Catalyst Center の分析とアシュアランスにおいて、大容量、優れた接続性、および低遅延という点で Wi-Fi 6 ネットワークの利点を可視化できます。アップグレード後、高度なワイヤレス分析により、Wi-Fi 6 の導入によるパフォーマンスとキャパシティの向上が示されます。 詳細については、https://blogs.cisco.com/networking/cisco-dna-your-fastest-route-to-wi-fi-6 [英語] を参照してください。
デバイス 360 およびクライアント 360	メモリまたは CPU 使用率、アップリンクの可用性、その他のKPIなどのパラメータを含む、デバイスの保証と全体的な状態を提供して、事業者がよりプロアクティブになり、将来の問題を予測できるようにします。デバイス 360 とクライアント 360 は、発生した問題、発生したタイミングと理由、および影響の程度を理解するのに役立ちます。また、問題のトラブルシューティングに役立つ、推奨される修正、解決された問題リスト、および履歴データも提供します。
アプリケーション エクスペリエンス	事前定義された「重要なビジネスアプリケーション」のパフォーマンスを追跡します。ユーザーエクスペリエンスとパフォーマンスのメトリックを示します。アプリケーションおよびクライアント単位で詳細かつ迅速なトラブルシューティングを行います。ユーザーごとに、コアビジネスに不可欠なアプリケーションの比類のない可視性とパフォーマンス制御を可能にします。マルチメディアモニタリングでは、Real-Time Protocol（RTP）ストリームにパフォーマンス処理を使用して、チームがマルチメディアなどの重要なリアルタイム アプリケーションの品質を確認できるようにします。URL モニタリングは、クラウドベース（URL ベース）アプリケーションの可視性を提供し、パフォーマンスを最適化します。アプリケーション エクスペリエンスにより、ユーザーは、自社における自身の役割を果たすのに重要なアプリケーションで、求めているパフォーマンスを得ることができます。
レポート	レポートを作成して、ネットワークとその運用に関するインサイトを引き出します。Catalyst Center は、いくつかのフォーマットで生成でき、運用ニーズに合わせてカスタマイズするための柔軟なスケジューリングと構成オプションを備えた、事前に用意された一連のレポートを提供します。サポートされるユースケースは次のとおりです。 • キャパシティプラン：ネットワーク内のデバイスがどのように利用されているのかを理解します。 • パターンの変更：ネットワークでの使用パターンの傾向の変化を追跡します。使用パターンの傾向には、クライアント、デバイス、バンド、またはアプリケーションが含まれる場合があります。 • 運用レポート：アップグレード完了やプロビジョニングの失敗などのネットワーク運用に関するレポートを確認します。 • ネットワークの正常性：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します。
Wireless Sensor ダッシュボード	Cisco Aironet Active センサーによって発見された全体的なテスト、接続統計、および主要なワイヤレスの問題を表示します。DHCP、DNS、ホスト到達可能性、RADIUS、電子メール、Microsoft Exchange サーバー、Web、FTP、ならびにデータスループット速度、遅延、ジッター、およびパケット損失に関する完全な IP SLA のテスト結果が含まれます。テストの失敗に対するガイド付き修復アクションを提供します。

機能	説明と利点
ストリーミングテレメトリ	ネットワークデバイスがほぼリアルタイムのテレメトリ情報を Catalyst Center に送信できるようにします。このデータを使用して、ネットワークを最適化し、問題が発生した場所を特定し、共同で問題を調査できます。テレメトリデータ（イベント、KPI）は、イベント駆動型の通知を介してエクスポートおよび表示できます。
トラフィック テレメトリ アプライアンス	このハードウェアソリューションは、ネットワーキングデータを収集して処理し、Catalyst Center にストリーミングテレメトリを提供します。これは、NetFlow、Application Visibility and Control（AVC）、Network-Based Application Recognition（NBAR）、NBAR2 など、ローカルネットワークから収集する必要のあるタイプのテレメトリをサポートするデバイスがないネットワークの領域で役立ちます。このアプライアンスは、Cisco AI Endpoint Analytics をサポートするために、ネットワークトラフィックに対してディープ パケット インスペクション（DPI）を実行することもできます。これは、レイヤ 2 ネットワークデバイスのみを含むエリアや、リアルタイムテレメトリの送信をサポートしないサードパーティ製スイッチを備えた分散拠点向けの強力なソリューションです。 詳細については、https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-traffic-telemetry-appliances/datasheet-c78-744352.html [英語] を参照してください。
ネットワークタイムトラベル	オペレータは、デバイスまたはクライアントのパフォーマンスをタイムラインビューで確認して、問題が発生したときのネットワークの状態を把握できます。オペレータは、ラボでネットワークの問題を再現するのではなく、最大 14 日前まで遡って問題の原因を確認できます。 • 問題が発生した時点まで時間を巻き戻します • 重要なイベントの履歴を表示します • ユーザまたはネットワークデバイスのすべての情報が、選択した時刻に変更されます
オンデバイス分析	異常が検出されたシスコのスイッチ、ルータ、またはワイヤレスコントローラでアシュアランスと分析を実行します。重要なメトリックを特定し、インシデントが発生する前に即座に対応が行えます。事業運営で重要となる KPI をリアルタイムで、しかもそれらを使用するユーザーの近くで維持できます。
Apple iOS、Samsung、および Intel デバイスの接続分析	デバイスにエージェントをインストールすることなく、デバイスの観点からの詳細な分析とインサイトを実行します。
インテリジェントキャプチャ	Catalyst Center と AP 間の直接通信リンクのサポートを提供し、各 AP が Catalyst Center と直接通信できるようにします。Catalyst Center はこのチャンネルを使用して、パケットキャプチャデータ、AP とクライアントの統計情報、およびスペクトルデータを受信できます。Cisco Intelligent Capture は、Catalyst Center と AP 間の直接通信リンクを利用することで、ワイヤレスコントローラからはアクセスできないデータに AP からアクセスできるようにします。
ServiceNow と IT サービス管理（ITSM）のクローズドループ統合	Catalyst Center は、ServiceNow およびその他の ITSM プラットフォームで、オープンチケット番号を自動解決できるようになりました。Catalyst Center Assurance は、障害が解決されたことを検出すると、ITSM チケット番号をチェックします。チケット番号が存在する場合は、チケットステータスの変更をチケット番号とともに ITSM システムに送信し、システム内のオープンチケットを自動的にクローズします。
AI 強化無線リソース管理（RRM）	AI を使用して、ネットワークの傾向とパターンをプロアクティブに学習し、時間の経過とともに、ワイヤレスエンドポイントの動作を強化することで、ワイヤレスネットワークのパフォーマンスとユーザー体験を向上させます。
AP の省電力	ユーザーがいない場合は、無線をオフにし、空間ストリームおよびポート速度を低下させて、USB ポートを無効にすることで、オフピーク時にワイヤレスネットワークが使用する電力を 20% 削減でき、サステナビリティを向上させます。
マルチベンダーのデバイスの可視性	到達可能性やトポロジなど、サードパーティ製デバイスの可視性を提供します。

SD-Access 機能

表 3. SD-Access 機能と利点

機能	説明
エンドポイントとトラフィックパターンの可視性の向上	Catalyst Center のエンドポイント分析アプリケーションは、AI/ML を使用してキャンパスネットワーク上のエンドポイントデバイスを識別および分類します。ディープパケット インスペクション（DPI）を含むさまざまなプロファイリング方法を使用して、ネットワーク上にあるものの可視性を確立し、新しいエンドポイントを認証して、ネットワークの使用、セキュリティ、およびセグメンテーションに適切なポリシーを割り当てることができるようにします。 グループベースのポリシー分析により、セグメンテーションポリシーの配信が簡素化されます。分析モデルを使用して、エンドポイントプロファイル、スケーラブルグループ、およびホストグループ間のアクティビティを可視化し、ネットワークポリシーがパフォーマンスとセキュリティを最適化していることを確認します。この機能は、ユーザーとエンドポイントを識別して分類し、各エンドポイントが必要とするリソースにきめ細かいアクセス権限を提供すると同時に、それらを他のすべてからセグメント化する方法を提供します。
きめ細かいマルチレベル セグメンテーション	SD-Access は、Catalyst Center を通じて、基盤となる物理インフラストラクチャ上に仮想オーバーレイを作成し、トポロジに関係なくネットワークをセグメント化します。また、SD-Accessは、ネットワーク インフラストラクチャを通じてグループベースのポリシーを適用することで、マイクロレベルでセグメント化します。結果として得られるきめ細かいセグメンテーションは、複雑なファイアウォールやアクセス制御リスト（ACL）を使用せずにトラフィックフローを制御します。これは、維持が困難でコストがかかる可能性があります。 **ファブリック インフラストラクチャの最適化の利点：** • VRF 構成（基幹業務、部門など）を自動化し、オーバーレイ仮想ネットワークを作成します。 • 802.1X、MAB、Active Directory、および静的認証を使用してユーザーをオンボードします。ISE が使用できないときに重要な VLAN でユーザーを移動するオプションを備えています。 • LISP pub/sub を使用した復元力のあるコントロール プレーン アーキテクチャにより、利用可能なインターネットサービスに向けた動的なパスの最適化が含まれます。ファブリックサイトの設計、ルーティングコンバージェンス、およびトラブルシューティングタスクを簡素化します。 • LAN 自動化を使用して、標準のエラーのないアンダーレイネットワークでネットワーク運用を簡素化します。 • 暗号化トラフィック分析（ETA）を使用して、AVC および NetFlow を介したトラフィックの分析をさらに強化します。 **SD-Access ファブリックへの移行が容易に** • 境界でのレイヤ 2 ハンドオフは、SD-Access ファブリック内のホストがレイヤ 2 で従来のネットワークと通信できるようにする重要な機能です。 • ファブリックは、ビル管理システム、オーディオビジュアル機器など、レイヤ 2 フラッディングを必要とするエンドホストをサポートします。 • SD-Access は、既存のアクセス VLAN のサポートを導入し、ユーザーがファブリックでマクロセグメントを作成するときに既存のアクセス VLAN ID を保持できるようにします。お客様は、SD-Access ファブリックエッジに直接接続するときに既存のアクセス VLAN ID を保持して、SD-Access セグメンテーションの過程を簡素化および高速化できます。 • ISE 機能のないマクロセグメンテーションは、外部レイヤ 2 スイッチングドメインにダウンストリームを接続するディストリビューション レイヤにファブリックがある展開に適しています。お客様は、自動化されたネットワークファブリックを展開し、ISEを使用せずに仮想ネットワークでマクロセグメンテーションを使用できます。 **SD-Access ファブリックによる導入の柔軟性：** • SD-Access は、エンドツーエンドのポリシーとセグメンテーションを備えた自動化された

機能	説明
	サイト間接続を備えた分散キャンパス設計を提供します。 • Fabric in a Box を使用すると、境界ノード、コントロールプレーンノード、およびエッジノードを同じファブリックノードで実行できるため、小規模なサイトまたはブランチでのファブリックの展開が簡素化されます。 • SD-Access 拡張ノードは、企業のカーペットのないスペースへの接続を提供することにより、エンタープライズ ネットワークを拡張します。これにより、IoT デバイスのネットワーク接続と管理、および配送センター、倉庫、キャンパスの駐車場などの屋外およびカーペットのない環境での従来のエンタープライズ エンド デバイスの展開が可能になります。 • SD-Access ファブリックには、ワイヤレスアクセスを統合するための 2 つのオプションがあります。 ◦ VXLAN 分散データプレーンと集中型コントロールプレーンを使用する SD-Access ワイヤレスは、一貫したファブリック エクスペリエンスを提供し、有線およびワイヤレスアクセスのポリシーを簡素化します。 ◦ Over the Top では、従来の Cisco Unified Wireless Network アーキテクチャを制御し、ファブリック有線ネットワーク上でワイヤレスアクセスポイントの制御とプロビジョニング（CAPWAP）を実行します。これは、完全な SD-Access ワイヤレス実装への可能な移行ステップです。 • マルチサイト リモート ボーダー機能により、ユーザーは信頼できないトラフィックをさまざまなファブリックサイトから DMZ のファイアウォールに分離できます。 • ファブリックゾーン機能を使用すると、管理者は特定のファブリックエッジノードで IP サブネットのプロビジョニングを制御して、サイトのスケーラビリティとセキュリティを向上させることができます。 • SD-Access は、IPv4 エンドポイントと IPv6 エンドポイントをサポートします。 • Cisco SD-Access は、Cisco Wide Area Bonjour アプリケーションをサポートしており、ユーザーは最小限の介入と設定で共有サービスを検出して使用できます。 • 802.1X ベースの認証および承認を使用した、Catalyst 9000 拡張ノードのネットワークデバイス導入準備を安全に行います。 **簡素化されたファブリック動作：** SD-Access アシュアランスを使用すると、ダウンタイムを最小限に抑え、エクスペリエンスを向上させながら、ファブリックの問題をリアルタイムで検出、診断、およびトラブルシューティングできます。新しく導入された SD-Access アシュアランス ランディング ページには、展開された各ファブリックサイトの全体的なファブリックヘルスが含まれています。ファブリックノードで設定された KPI は、問題をより迅速に特定するための洞察と、問題を修正するための推奨アクションを提供します。KPI はカテゴリに編成され、コントロールプレーン、インフラストラクチャ、および接続の問題を迅速に切り分けます。 • ファブリック コントロール プレーンは、ファブリックエッジ/ボーダーとファブリック コントロール プレーン ノード間の到達可能性チェックを提供します。 • ファブリック インフラストラクチャは、ファブリックエッジおよびポリシー拡張ノードから Identity Services Engine（ISE）までの AAA サーバーステータスを検証します。 • ファブリック接続は、エッジからファブリック境界への到達可能性チェック、およびファブリックエッジと拡張ノード間のコントロールプレーンおよびポートチャネル接続チェックを提供します。 • SD-Access ファブリックロールで動作する Catalyst 9000 スイッチでの ThousandEyes エージェントをサポートします。これにより、評価指標とエンドツーエンドの可視性を提供するテストを実行できます。 ファブリック UX2.0 は、シンプルさ、柔軟性、豊富で直感的なコンテキストを統合したユーザーインターフェイスの強化されたエクスペリエンスを管理者に提供します。
継続的な信頼性の検証	信頼分析は、さまざまな入力データとソースを 1 つの包括的で柔軟な信頼スコアに集約したものです。信頼分析は、異常な動作を示しているエンドポイントからのトラフィックを検出します。ネットワーク内の異常が検出されると、Trust Analyticsはエンドポイントの信頼スコアを下げ、ISEとの統合によってネットワークへのアクセスを制限または完全に拒否します。この機能は、セキュリティ侵害につながる可能性のある信頼できないエンドポイントの検出と封じ込めを促進します。

システムとプラットフォームの機能

表 4. Catalyst Center システムの機能

機能	説明と利点
Role Based Access Control（RBAC）	ユーザーを 4 つの定義済みロールのいずれかにマッピングできます。ロールは、ユーザーがシステム内で実行できる操作のタイプを決定します。
バックアップと復元	データベース全体の完全なバックアップと復元をサポートして、保護を強化します。
ISE の統合	ファブリックオーバーレイのサポートのために pxGrid または API を介して ISE と統合します。
ワークフロー	Catalyst Center のワークフローは、特定のタスクを順を追って説明するガイドです。たとえば、「ロールの作成」、「AP の更新」などです。ワークフローは、ワークフローのホームページ上の「進行中」ライブラリを介して一時停止または再試行される場合があります。ワークフローのホームページは、GUI のメニューアイコンをクリックし、[Workflows] をクリックすると表示されます。ホームページには、進行中のワークフローとともにワークフローのライブラリがあります。
アクティビティセンター	アクティビティセンターは、監査ログとスケジュールされたタスクを検索するための集中型スペースです。監査ログは、発生したシステムイベント、発生した場所、開始したユーザーを記録します。監査ログを使用すると、監査用の別のログファイルにシステムの設定変更が記録されます。[Scheduled Tasks] タブで、OS の更新やデバイスの交換などの予定（upcoming）、進行中（in progress）、完了（completed）および失敗（failed）管理タスクを表示します。
FIPS 140-2 のサポート	Catalyst Center には、FIPS 140-2 準拠の暗号モジュールのサポートが含まれているため、NIST 承認の強力な暗号のみが使用され、公共部門、金融、医療などのセキュリティを重視する業種での展開が可能になります。インストール中に、管理者は FIPS を有効にすることを選択できます。これにより、NIST 承認の暗号のみがデータ暗号化に使用されるようになります。

表 5. Catalyst Center プラットフォームの機能

機能	説明と利点
ノースバウンド REST API	Catalyst Center プラットフォームは、プログラマビリティのためにノースバウンドレイヤで Representational State Transfer（REST）API をサポートします。Catalyst Center API は、次の機能をサポートします。 • ディスカバリ、デバイスインベントリ、ネットワークトポロジ • SWIM、プラグアンドプレイ（PnP）、ワイヤレス、SD-Access、およびアプリケーションポリシー • テンプレートプログラマ、コマンドランナー • アシュアランス：サイト、デバイス、およびクライアントの正常性モニタリング、パスのトレース • NFV のプロビジョニング • API によるイベント管理通知の設定
IT サービス管理（ITSM）の統合	ハンドオフの必要性が最小限に抑えられ、問題が重複排除され、プロアクティブなインサイトと迅速な修復のためのプロセスが最適化されます。ServiceNow とすぐに使用できる統合が存在します。Catalyst Center プラットフォームによって公開される汎用 API により、パートナーおよび開発者は ITSM システムと統合できます。

機能	説明と利点
IP アドレス管理（IPAM）の統合	外部 IPAM システムから Catalyst Center ワークフローの IP プールをシームレスにインポートし、2 つのシステム間で IP プールとサブプールの使用状況情報を同期できます。Infoblox および BlueCat には、すぐに使用できる統合が存在します。Catalyst Center プラットフォームは、任意の IPAM システムと統合するための汎用 API を提供します。
イベントと通知	Catalyst Center プラットフォームのウェブフックにより、サードパーティ製アプリケーションは、通知を受信し、Catalyst Center Assurance、自動化、およびその他のタスクベースの運用ワークフローによって検出されたイベントをリッスンできます。

表 6. 情報の関連付け

カテゴリ	インサイト
ワイヤレスインサイトと分析	**クライアント オンボーディング** • 関連付けエラー • 認証エラー • IP アドレスの障害 • クライアント除外 • 過剰なオンボーディング時間 • 過剰な認証時間 • 過剰な IP アドレッシング時間 • AAA、DHCP 到達可能性 **クライアント エクスペリエンス** • スループット分析 • ローミングパターン分析 • スティッキクライアント • 低速ローミング • 過剰なローミング • RF、ローミングパターン • デュアルバンドクライアントは 2.4 GHz を優先する • 過剰な干渉 • Apple iOS クライアントの切断 **ネットワークのカバレッジとキャパシティ** • カバレッジホール • AP ライセンス使用率 • クライアントキャパシティ • 無線使用率 **ネットワークデバイスのモニタリング** • 可用性 • クラッシュ、AP 接続失敗 • ハイアベイラビリティ • CPU、メモリ • AP のフラッピング、無線の停止 • 電源の障害

カテゴリ	インサイト
センサーの問題	**センサーのオンボーディング** • 関連付けエラー • 認証エラー • IP アドレスの障害 • センサー除外 • 過剰なオンボーディング時間 • 過剰な認証時間 • 過剰な IP アドレッシング時間 • AAA、DHCP 到達可能性 **センサーエクスペリエンス** • スループット分析 • Outlook Web の応答時間 • Web サーバーの応答時間 • SSH サーバーの応答時間 • メールサーバーの応答時間 • FTP サーバーの応答時間 • 過剰な無線干渉
ルーティングの問題	**ルータの正常性** • 高いCPU使用率 • ハイメモリ **ルーティングテクノロジー** • BGP AS の不一致、フラップ • OSPF 隣接関係の障害 • Enhanced Interior Gateway Routing Protocol（EIGRP）隣接関係の障害 **接続** • インターフェイスの高使用率 • LAN 接続のダウン/フラップ • IP SLA から SP ゲートウェイへの接続

カテゴリ	インサイト
スイッチングの問題（非ファブリック）	**クライアント オンボーディング** • クライアントまたはデバイスの DHCP • クライアントまたはデバイスの DNS • クライアントの認証および許可 **スイッチ** • CPU、メモリ、温度 • モジュール • Power over Ethernet（PoE）電源 • Ternary Content-Addressable Memory（TCAM）テーブル
SD-Access の問題	**ボーダーおよびエッジの到達可能性** • コントロールプレーンの到達可能性 • エッジの到達可能性 • ボーダーの到達可能性 • ルーティングプロトコル • MAP サーバー **データ プレーン** • ボーダーおよびエッジの接続 • ボーダーノードの正常性 • アクセスノードの正常性 • ネットワークサービス DHCP、DNS、AAA **ポリシープレーン** • ISE または pxGrid の接続 • ボーダーノードポリシー • エッジノードポリシー **クライアント オンボーディング** • クライアントまたはデバイスの DHCP • クライアントまたはデバイスの DNS • クライアントの認証および許可 **スイッチ** • CPU、メモリ、温度 • モジュール • PoE 電源 • TCAM テーブル

遅延要件

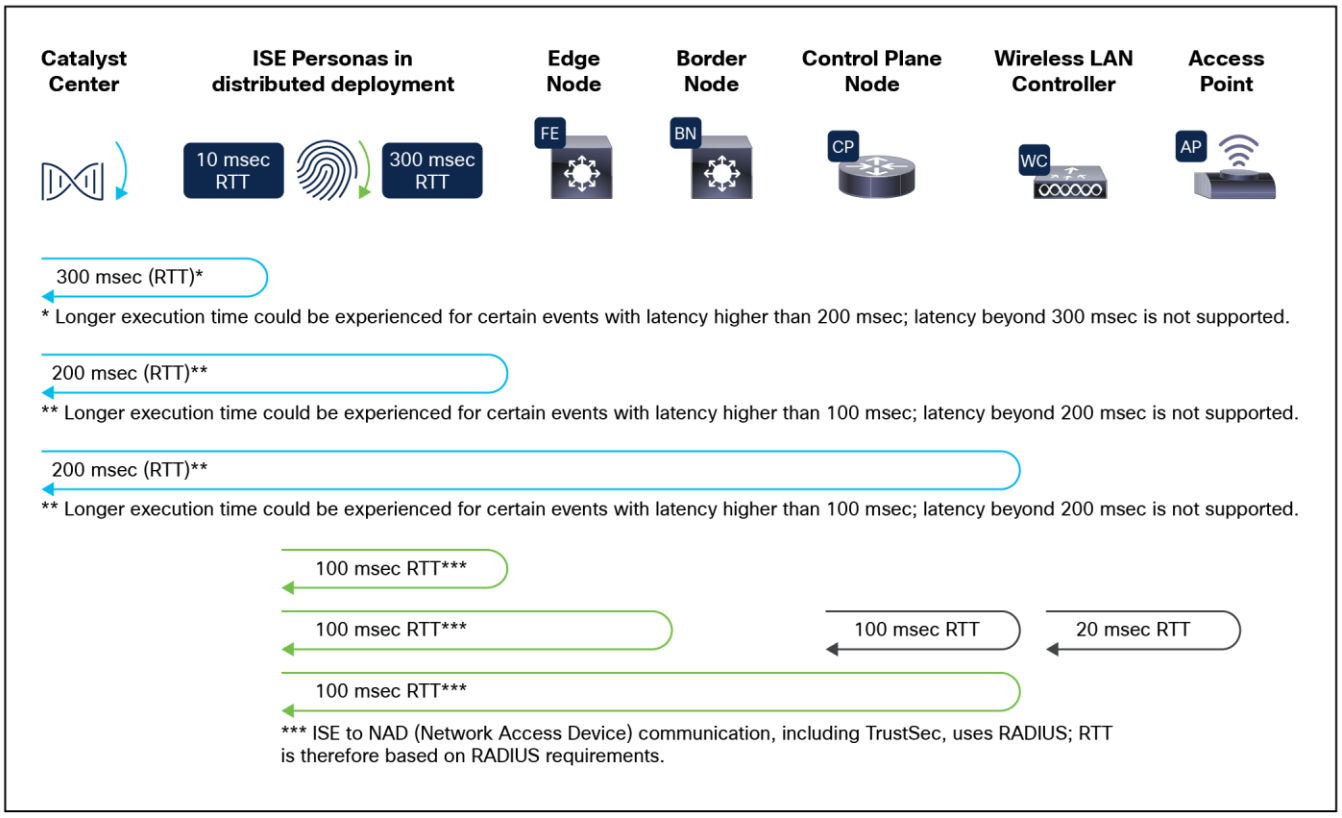

図 3.
サポートされる最大遅延、ラウンドトリップ時間。

SD-Access プラットフォームスケール

次の表に、Cisco SD-Access のプラットフォームスケールの概要を示します。このセクションの制限は、必ずしも Catalyst Center ではなく、デバイスのモデルとその容量設計に依存します。

表 7. Cisco SD-Access コントロールプレーンノード

Cisco SD-Access コントロールプレーンノード												
ファミリ	Cisco Catalyst									ASR 1000、4000 シリーズ ISR	ASR 1000 4000 シリーズ ISR	CSR
デバイス	9300/L	9300X	9400 Sup-XL/Y	9400X	9500	9500X	9500H	9600	9600X	8 GB RAM	16 GB RAM	1000v
エンドポイント	16,000	32,000	80,000	112,000	80,000	1,000,000	150,000	150,000	1,000,000	100,000	200,000	200,000

コントロールプレーンのスケールは Ternary Content-Addressable Memory（TCAM）に依存しません。メモリを消費するだけです。

表 8. Cisco SD-Access ボーダーノードのスケール

Cisco SD-Access ボーダーノードのスケール											
ファミリ	Cisco Catalyst									ASR 1000、4000 シリーズ ISR	ASR 1000、4000 シリーズ ISR
デバイス	9300/L	9300X	9400 Sup-XL/Y SD-Access sdm テンプレート	9400X	9500 SD-Access sdm テンプレート	9500H	9500X	9600	9600X	8 GB RAM	16 GB RAM
仮想ネットワーク[1]	256	256	256	1000	256	256	1000	256	1000	128	128
IPv4 ルート	8000	32,000	64,000	96,000	64,000	48,000	512,000	48,000	512,000	1,000,000	4,000,000
ファブリックホストエントリ[2]（ホスト /32 または /128）	16,000	32,000	70,000	96,000	70,000	150,000	512,000	150,000	512,000	1,000,000	4,000,000
IPv4：SGT バインディング	10,000	32,000	40,000	109,000	40,000	40,000	200,000	200,000	200,000	750,000	750,000
SGT/DGT ポリシー	8000	7400	8000	32,000	8000	16,000	32,000	32,000	32,000	64,000	64,000
SG-ACEs（契約アクション）	5000	4800	18,000	16,000	18,000	13,000	4000	27,000	4000	64,000	64,000

ファブリックホストエントリには、アクセスポイントと、クラシックおよびポリシー拡張ノードが含まれます。

その他のボーダーおよびスケールの考慮事項：

/32（IPv4）または /128（IPv6）エントリは、ファブリックの外部からファブリック内のホストにトラフィックを転送するときに使用されます。

[1] 仮想ネットワークのスケールは、Catalyst Center プラットフォーム VN のスケールにも依存します。SD-Access のスケールについては、表 7 を参照してください。

[2] エンドポイントに複数の IPv4 または IPv6 アドレスがある場合、各アドレスは個別のエントリとしてカウントされます。

Cisco Catalyst 9500 シリーズ ハイパフォーマンス スイッチおよび Cisco Catalyst 9600 シリーズ スイッチを除くすべてのスイッチ：

- IPv4 は、すべての IPv4 IP アドレスに対して 1 つの TCAM エントリ（ファブリックホストエントリ）を使用します。
- IPv6 は、すべての IPv6 IP アドレスに対して 2 つの TCAM エントリ（ファブリックホストエントリ）を使用します。

Cisco Catalyst 9500 シリーズ ハイパフォーマンス スイッチおよび Cisco Catalyst 9600 シリーズ スイッチ：

- IPv4 は、すべての IPv4 IP アドレスに対して 1 つの TCAM エントリ（ファブリックホストエントリ）を使用します。
- IPv6 は、すべての IPv6 IP アドレスに対して 1 つの TCAM エントリ（ファブリックホストエントリ）を使用します。

表 9. Cisco SD-Access レイヤ 2 ハンドオフボーダーノードのスケールに関する考慮事項

ファミリ	Cisco Catalyst							ASR 1000、4000 シリーズ ISR	ASR 1000、4000 シリーズ ISR
デバイス	9300/L	9300X	9400	9400X	9500	9500H	9600	8 GB RAM	16 GB RAM
エンドポイント	8,000	32,000	16,000	100,000	16,000	32,000	32,000	サポートなし	サポートなし

この表の数値は、サイトにレイヤ 2 ハンドオフのボーダーノードがある場合の、ファブリックサイト内外におけるエンドポイントの総数の合計です。

レイヤ 2 ボーダーハンドオフをサポートするすべてのプラットフォームで、ファブリックの外部に最大 6000 台のホストを接続できます。

レイヤ 2 ハンドオフを持つボーダーノードには、ローカルとリモートの LISP エントリの組み合わせが含まれています。

ローカルエントリ = LISP データベース

リモートエントリ = LISP マップキャッシュ

例：

Cisco Catalyst 9300 シリーズ スイッチは、合計 8000 エントリをサポートします。

ファブリックサイトに 6000 のエンドポイント（マップキャッシュ）がある場合、レイヤ 2 ハンドオフを超える従来のネットワークには 2000 のエンドポイント（データベース）しか存在できません。

表 10. Cisco SD-Access エッジノードのスケール

Cisco SD-Access エッジノードのスケール									
ファミリ	Cisco Catalyst							Cisco Catalyst	
デバイス	9200CX	9200-L	9200	9200 拡張 VN	9300/L	9300X	9400	9400X	9500/H
仮想ネットワーク	16	1[1]	4[2]	32[3]	256	256	256	1000	256
エンドポイント	4,000	2000	4000	4000	6000	18,000	6000	70,000	6000
IPv4：SGT バインディング	10,000	8000	10,000	10,000	10,000	32,000	40,000	109,000	40,000
SGT/DGT ポリシー	2000	2000	2000	2000	8000	7400	8000	32,000	8000
SG-ACEs（契約アクション）	1200	1,000	1000	1,000	5000	4800	18,000	16,000	18,000

[1] 9200-L = 1 つのユーザー定義 VN（VRF）

[2] 9200 = 4 つのユーザー定義 VN（VRF）

[3] 9200「強化された VN」の SKU = 32 のユーザー定義 VN（VRF）

補足事項：

INFRA_VN は VRF 定義ではありません。グローバル ルーティング テーブルに関連付けられています。

DEFAULT_VN はユーザー定義ではありません。Catalyst Center で自動的に作成されます。これは以前（下位互換性）のために存在するものです。使用は必要ではなく推奨もされません。2

DEFAULT_VN は、ホストオンボーディングで使用される場合、VRF 定義としてプロビジョニングされ、「ユーザー定義の VN」としてカウントされます。

表 11. Cisco SD-Access WLC スケール

Cisco SD-Access WLC スケール		
デバイス	アクセスポイントの数	クライアントの数
Catalyst 9800-L	250/500（Perf. ライセンス）	5000/10000（Perf. ライセンス）
Catalyst 9800-40	2000	32,000
Catalyst 9800-80	6000	64,000
Catalyst CW9800H1	6000	64,000
Catalyst CW9800H2	6000	64,000

Cisco SD-Access WLC スケール		
デバイス	アクセスポイントの数	クライアントの数
Catalyst CW9800M	3000	32,000
Catalyst 9800-CL（4 CPU/8 GB RAM）	1000	10,000
Catalyst 9800-CL（6 CPU/16 GB RAM）	3000	32,000
Catalyst 9800-CL（10 CPU/32 GB RAM）	6000	64,000

表 12. アクセスポイントとワイヤレスエンドポイントの Cisco SD-Access エッジノードのスケール

アクセスポイントとワイヤレスエンドポイントの Cisco SD-Access エッジノードのスケール						
ファミリ	Cisco Catalyst					
デバイス	9200-L	92001	9300-L1	9300/X	9400/X	9500/H
アクセスポイント	サポート対象外	25	50	200	200	200
ワイヤレス エンドポイント	サポート対象外	500	1000	4000	4000	4000

[1] 単一のスイッチとスイッチスタックは同じスケールです。

前述のスイッチのアクセストンネル数には制限があります。アクセストンネルは、ファブリックエッジノードと、直接接続された、または直接接続拡張ノードを介して接続されたファブリックモード AP との間に作成されます。

表 13. Cisco SD-Access 組み込みワイヤレスコントローラのスケール

Cisco SD-Access 組み込みワイヤレスコントローラのスケール					
ファミリ	Cisco Catalyst				
デバイス	9200/L	9300/L	9300	9400	9500/H
アクセスポイント	サポート対象外	50	200	200	200
ワイヤレス エンドポイント	サポート対象外	1000	4000	4000	4000

埋め込まれたワイヤレススケールは、デバイスの役割（エッジ、ボックス内のファブリック、境界線、またはコントロールプレーン）に関係なく同じです。

Meraki の統合

Catalyst Center および Cisco Catalyst 9000 スイッチの使用を検討したい既存の Meraki ブランチのお客様、または混在環境のお客様向けに、Catalyst Center は単一の一括管理ペインを提供します。これは、既存のすべての Meraki ハードウェアおよびソフトウェアを追加のライセンスコストなしでサポートする API 主導のダッシュボード統合です。

Meraki の統合により、次のことが可能になります。

- すべてのプラットフォーム（Meraki、Cisco Catalyst、Cisco Integrated Services Router（ISR; サービス統合型ルータ）、Aironet）での単一ダッシュボードインベントリ
- 単一プラットフォーム内のすべてのデバイスのアップ/ダウンステータス
- 既存の Meraki API キーを使用。追加ライセンスは不要
- Catalyst Center 内から Meraki アクセスポイントに SSID を割り当てる機能

アプライアンスのスケール

Catalyst Center は、柔軟な展開オプションを提供します。ハードウェアアプライアンスに展開することも、VMware ESXi または AWS 上に仮想アプライアンスとして展開することも可能です。

第 3 世代の Catalyst Center アプライアンスには 3 つのフォームファクタがあります。Catalyst Center イメージがプリロードされているので、すぐにインストールできます。

表 14 および 15 に、物理アプライアンスに展開した場合の Catalyst Center のスケール情報を示します。

表 14. スケールおよびハードウェア仕様

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
説明	Catalyst Center 仮想アプライアンス	Cisco UCS® C220 M6 ラックサーバー 32 コア	Cisco UCS C220 M6 ラックサーバー 56 コア	Cisco UCS C240 M6 ラックサーバー 80 コア
Catalyst Center のシステムスケール				
ネットワークデバイスの合計数（超過できません）	5000	5000	8,000	18,000
M スケールプロファイル 1（ファブリックおよび非ファブリック）	1,000（スイッチ、ルータ、WLC）+ 4,000 AP		意図的な空白	意図的な空白
M スケールプロファイル 2（ファブリックおよび非ファブリック）	2,000（スイッチ、ルータ、WLC）+ 3,000 AP		意図的な空白	意図的な空白
L および XL スケール非ファブリック	意図的な空白	意図的な空白	2,000（スイッチ、ルータ、WLC）+ 6,000 AP	5,000（スイッチ、ルータ、WLC）+ 13,000 AP
L および XL スケールファブリック	意図的な空白	意図的な空白	4,000（SW、ルータ、WLC）+ 4,000 AP	8,000（SW、ルータ、WLC）+ 10,000 AP

SKU	DN-SW-APL	DN3-HW-APL	DN3-HW-APL-L	DN3-HW-APL-XL
説明	Catalyst Center 仮想アプライアンス	Cisco UCS® C220 M6 ラックサーバー 32 コア	Cisco UCS C220 M6 ラックサーバー 56 コア	Cisco UCS C240 M6 ラックサーバー 80 コア
ワイヤレスセンサー	600	600	800	1600
同時エンドポイント	25,000	25,000	40,000	100,000
一時エンドポイント（14 日間以上）	75,000	75,000	120,000	250,000
エンドポイントの比率：有線、無線	任意 任意	任意 任意	任意 任意	任意 任意
サイト要素	2500	2500	5000	10,000
ワイヤレスコントローラ	500	500	1000	2000
物理ポート[2]	48,000	48,000	192,000	480,000
物理ポート[2]および論理ポートの組み合わせ	120,000	120,000	480,000	1,500,000
API レート制限	50 API/分	50 API/分	50 API/分	50 API/分
NetFlow（フロー数/秒）	30,000	30,000	48,000	120,000
ソフトウェアイメージの同時更新	100	100	100	100
Catalyst Center SD-Access のスケール				
ファブリックサイト[3]	500	500	1000	2000
ファブリックサイトごとの Catalyst Center のスケール				
レイヤ 3 仮想ネットワーク	64/サイト	64/サイト	128/サイト	256/サイト
ファブリックデバイス	500/サイト	500/サイト	600/サイト	1200/サイト
拡張可能グループ数	4000	4000	4000	4000
アクセス契約数	500	500	500	500
グループベースのポリシー	25,000	25,000	25,000	25,000
IP プール[4]	100[5]	100[5]	300[6]	1,000[7]
レイヤ 2 仮想ネットワーク[4]	200[5]	200[5]	600[6]	1,000[7]

注：

[1] スイッチスタック、StackWise Virtual ペア、VSS ペア、および WLC HA SSO ペアは、それぞれ 1 つのデバイスとしてカウントされます。

[2] コンソールポートを除くすべての物理ポートが含まれます。WLC の冗長ポート（RP）が含まれます。

[3] SD-Access の展開にファブリックサイトを追加しても、Catalyst Center システムの拡張性パラメータは増加しません。たとえば、10 のファブリックサイトにまたがる 1000 の同時エンドポイントと、単一のファブリックサイト内にある 1000 の同時エンドポイントは、どちらもシステムの規模に等しく活用できます。

[4] レイヤ 2 仮想ネットワークは、ファブリックサイトにエニーキャストゲートウェイがない SD-Access のレイヤ 2 セグメントです。レイヤ 2 仮想ネットワークでは IP プールは使用しません。

[5] IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 200 以下である必要があります。

[6] IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 600 以下である必要があります。

[7] IP プールとレイヤ 2 仮想ネットワークの合計は、ファブリックサイトあたり 1,000 以下である必要があります。

表 15. 3 ノード DN3-HW-APL-XL クラスタのスケール

説明	サポートされるスケール
デバイス[1]（スイッチ、ルータ、ワイヤレスコントローラ）	10,000
ワイヤレス アクセス ポイント	25,000
同時エンドポイント	300,000
一時エンドポイント（14 日間以上）	750,000
物理ポート[2]	768,000
物理ポート[2]および論理ポートの組み合わせ	2,000,000
NetFlow	250,000 フロー/秒

注：

[1] スイッチスタック、StackWise Virtual ペア、VSS ペア、および WLC HA SSO ペアは、それぞれ 1 つのデバイスとしてカウントされます。

[2] コンソールポートを除くすべての物理ポートが含まれます。WLC の冗長ポート（RP）が含まれます。

ハードウェアアプライアンスの仕様

Catalyst Center アプライアンスには 3 つのフォームファクタがあります。Catalyst Center イメージがプリロードされているので、すぐにインストールできます。これらの Cisco UCS アプライアンスの詳細については、表 16 の各ハードウェアシリーズの横にあるデータシートのリンクをクリックしてください。

表 16. 物理仕様

物理仕様	DN3-HW-APL および DN3-HW-APL-L	DN3-HW-APL-XL
発注用の製品番号	DN3-HW-APL および DN3-HW-APL-L	DN3-HW-APL-XL
ハードウェアシリーズ	UCS C220 M6（データシート）	UCS C240 M6（データシート）
電源モジュール	ホットプラグ可能な冗長 2300W Titanium 認定 AC X 2	ホットプラグ可能な冗長 2300W Titanium 認定 AC X 2
物理寸法	高さ：4.3 cm（1.70 インチ）	高さ：8.7 cm（3.42 インチ）

物理仕様	DN3-HW-APL および DN3-HW-APL-L	DN3-HW-APL-XL
（高さ X 幅 X 奥行）	幅：42.9 cm（16.9 インチ） 奥行：48.0 cm（18.9 インチ）	幅：42.9 cm（16.9 インチ） 奥行：48.0 cm（18.9 インチ）
温度：動作	10° C ～ 35° C（50° F ～ 95° F）の乾球温度	10° C ～ 35° C（50° F ～ 95° F）の乾球温度
温度：非動作	乾球温度 -40° C ～ 65° C（- 40° F ～ 149° F）	乾球温度 -40° C ～ 65° C（- 40° F ～ 149° F）
湿度：動作	10 ～ 90%、最大露点温度 28° C（82.4° F）、非凝縮環境	10 ～ 90%、最大露点温度 28° C（82.4° F）、非凝縮環境
湿度：非動作	相対湿度 5 ～ 93%、結露しないこと、乾球温度 20° C ～ 40° C の最大湿球温度は 28° C。	相対湿度 5 ～ 93%、結露しないこと、乾球温度 20° C ～ 40° C の最大湿球温度は 28° C。
高度：動作	最大標高 3050 メートル（10,006 フィート）	最大標高 3050 メートル（10,006 フィート）
高度：非動作	標高 0 ～ 12,000 メートル（39,370 フィート）	標高 0 ～ 12,000 メートル（39,370 フィート）
ネットワークおよび管理 I/O	サポートされるコネクタ： 1 Gb イーサネット専用管理ポート X 1 1/10 ギガビット BASE-T イーサネット LAN ポート X 2 RS-232 シリアル ポート（RJ-45 コネクタ）X 1 15 ピン VGA2 コネクタ X 1 USB 3.0 コネクタ X 2 USB 2.0 2 個、VGA 1 個、シリアル（DB-9）コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1	サポートされるコネクタ： 1 Gb イーサネット専用管理ポート X 1 1/10 ギガビット BASE-T イーサネット LAN ポート X 2 RS-232 シリアル ポート（RJ-45 コネクタ）X 1 15 ピン VGA2 コネクタ X 1 USB 3.0 コネクタ X 2 USB 2.0 2 個、VGA 1 個、シリアル（DB-9）コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1
適合規格：安全性および EMC		
適合規格の遵守	本製品は、指令 2014/30/EU および 2014/35/EU による CE マーキングに準拠しています。	
安全性	• UL 60950-1 第 2 版 • CAN/CSA-C22.2 No. 60950-1 第 2 版 • EN 60950-1 第 2 版 • IEC 60950-1 第 2 版 • AS/NZS 60950-1 • GB4943 2001	
EMC：エミッション	• 47CFR Part 15（CFR 47）クラス A • AS/NZS CISPR 32、クラス A • CISPR32 クラス A • EN55032 クラス A	

物理仕様	DN3-HW-APL および DN3-HW-APL-L	DN3-HW-APL-XL
	• ICES003 クラス A • VCCI クラス A • EN61000-3-2 • EN61000-3-3 KN32 クラス A • CNS13438 クラス A	
EMC：イミュニティ	• EN55024 • CISPR24 • EN300386 • KN35	

仮想アプライアンスの要件

Catalyst Center は、AWS または VMware ESXi 上に仮想アプライアンスとして展開できます。システム要件については、表 17 および 18 を参照してください。

表 17. VMware ESXi の仮想アプライアンスの要件

仕様	要件
プロセッサ	VM 専用の 32 の vCPU（64 GHz）
メモリ	VM 専用の 256 GB の Dynamic Random Access Memory（DRAM）
ストレージ	3 TB
ESXi	VMware vSphere（ESXi および vCenter Server を含む）7.0.x 以降とすべてのパッチ
I/O 帯域幅	180 MB/sec
IOPS（1 秒当たりの入出力処理）	2000 ～ 2500
ネットワーク インターフェイス カード（NIC）	ネットワークポートごとに 1 Gbps ネットワーク

表 18. AWS の仮想アプライアンスの要件

仕様	要件
インスタンス タイプ	r5a.8xlarge
コア	32 vCPU（Intel® または AMD ベースのホスト）
RAM	256 GB
ストレージ	4 TB
ストレージ タイプ	GP3 EBS

ファブリック VN スケール

表 19 に、Catalyst Center リリース 2.3.7 を展開する場合に適用される、ファブリック内のデバイスのファブリック VN 制限を示します。

表 19. ファブリック VN 制限（現在の最大 VRF 検証は、デバイスが 128 以上をサポートできる場合でも、下限 1 と上限 128 に基づきます）。

デバイスシリーズ	最大 VRF
Cisco Catalyst 6800 シリーズ スイッチ	1000（128）
Cisco Catalyst 6500 シリーズ スイッチ	1000（128）
データセンタースイッチ（**Cisco Nexus 7000** シリーズ スイッチ）	4000（128）
Cisco Cloud Services Router 1000V シリーズ	4000（128）
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	4000（128）
Cisco 4000 シリーズ サービス統合型ルータ	4000（128）
Cisco 4400 シリーズ サービス統合型ルータ	4000（128）
Cisco 4200 シリーズ サービス統合型ルータ	4000（128）
Cisco 4300 シリーズ サービス統合型ルータ	4000（128）
Cisco Catalyst 9300/9300X シリーズ スイッチ	256
Cisco Catalyst 9300 L シリーズ スイッチ	256
Cisco Catalyst 9500 シリーズ スイッチ	256
Cisco Catalyst 9500-H シリーズ スイッチ	256
Cisco Catalyst 9400 シリーズ スイッチ	256
Cisco Catalyst 9200-L スイッチスタック	1

デバイスシリーズ	最大 VRF
Cisco Catalyst 9200 スイッチスタック	4
Cisco Catalyst 9200-24PB スイッチ	32
Cisco Catalyst 9200-48PB スイッチ	32
Cisco Catalyst 9200CX スイッチ	16
Cisco Catalyst 9600 シリーズスイッチ	256

ロールと権限

表 20. ロールベース アクセス コントロール

ロール	特権
Network-Admin-Role	このロールを持つユーザーは、ネットワーク関連のすべての Catalyst Center 機能にフルアクセスできます。ネットワーク管理者は、アプリケーション管理、ユーザー（そのネットワーク管理者自身のパスワードの変更を除く）、バックアップと復元などのシステム関連機能にはアクセスできません。
Observer-Role	このロールを持つユーザーは、すべての Catalyst Center 機能に対する表示専用アクセス権を持ちます。
Telemetry-Admin-Role	このロールを持つユーザーは、Catalyst Center 内でシステムレベルの機能を実行できます。
Super-Admin-Role	このロールを持つユーザーは、すべての Catalyst Center 機能にフルアクセスできます。管理者は、Super-Admin-Role を含むさまざまなロールを持つ他のユーザープロファイルを作成できます。

互換性マトリックス

Catalyst Center は、シスコのエンタープライズ スイッチング、ルーティング、およびモビリティ製品を対象としています。サポートされているシスコ製品の完全なリストについては、定期的に更新される互換性マトリックスを参照してください。

Catalyst Center 互換性マトリックス：
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index.html [英語]。

Cisco SD-Access 互換性マトリックス：
https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/sda_compatibility_matrix/index.html [英語]。

シスコの環境保全への取り組み

シスコの企業の社会的責任（CSR）レポートの「環境保全」セクションでは、製品、ソリューション、運用、拡張運用、サプライチェーンに対する、シスコの環境保全ポリシーとイニシアチブを掲載しています。

次の表に、環境保全に関する主要なトピック（CSR レポートの「環境保全」セクションに記載）への参照リンクを示します。

表 21. 環境保全に関する主要なトピックへの参照リンク

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

次の表 22 に、このデータシートの関連するセクションに記載されている**製品固有の環境保全に関する情報**への参照リンクを示します。

表 22. 製品固有の環境保全に関する情報への参照リンク

持続可能性に関するトピック	参照先
一般	
製品の適合規格	安全性および準拠に関する情報
電源	
電源モジュール	電源モジュールと標準および最大電力仕様
素材	
寸法	物理寸法

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

製品使用状況テレメトリ

製品使用状況テレメトリは、Catalyst Center アプライアンスのステータスと機能に関する貴重な情報を提供します。Catalyst Center は、製品使用状況のデータを自動的にシスコに接続して送信するように設定されています。シスコは、Catalyst Center を導入した IT チームのアプライアンス ライフサイクル管理を改善するために製品使用状況テレメトリを使用します。このデータを収集することで、製品チームは顧客により優れたサービスを提供できるようになります。このデータと関連する分析情報により、シスコは潜在的な問題をプロアクティブに特定し、サービスとサポートを改善し、ディスカッションを促進して新規および既存の機能からより多くの価値を収集し、IT チームによるライセンス権限のインベントリレポートと今後の更新を支援します。

シスコに送信されるすべての製品使用状況のデータは、暗号化チャネルを介して送信されます。製品使用状況テレメトリで収集されるデータのカテゴリは、Cisco.com ID、システムテレメトリ、機能使用状況テレメトリ、およびネットワークデバイス（スイッチ、ルータなど）インベントリおよびライセンス権限です。製品使用状況テレメトリの収集はデフォルトで有効であり、製品から無効にすることはできません。収集設定の変更については、Cisco Technical Assistance Center（TAC）にお問い合わせください。

収集された製品使用状況のテレメトリ情報の詳細については、表 23 を参照してください。

表 23. Catalyst Center 製品使用状況テレメトリの使用状況と利点*

カテゴリ	データ要素	収集の目的
Cisco.com	• Cisco.com ユーザー ID	カスタマーアカウントの特定
システム	• 導入情報（Catalyst Center アプライアンスのシリアル番号、Catalyst Center アプライアンス プラットフォーム、Catalyst Center アプライアンスマシン ID） • Catalyst Center との接続 • ポッドの運用メトリック（CPU、メモリ、ファイルシステム、稼働時間） • サイン済みのエンドユーザーライセンス契約（EULA）フラグ • 展開されたアプリケーションスタックとパッケージ	問題を回避し、製品を改善するために、お客様の環境の潜在的な問題を特定します
機能の使用状況	• アプリケーション UI ページのカスタマー滞留時間 • Site_member_details：サイト名、デバイスのインスタンス UUID、デバイスのサポートレベル、デバイスファミリ、ホスト名 • アシュアランスの使用状況：サイト数、エリア、ビルディング、フロア、ワイヤレス LAN コントローラ（WLC）、スイッチ、アクセスポイント（AP）、クライアント数（有線およびワイヤレス）と正常性スコア、センサー数、センサーテスト数、AI ネットワーク分析構成フラグ、RF 統計情報が有効な AP カウント、有効な異常キャプチャ数、有効なデータパケットキャプチャ数、ネットワークテレメトリ最大入力レート（NetFlow、syslog、トラップ） • SD-Access の使用状況：作成されたファブリック数、ドメインタイプごとのファブリックドメイン数、サイト別のファブリックロールごとのデバイス数、エッジノード数とボーダーノード数およびデバイスタイプ別のコントロールプレーンノード数、ファブリック上のクライアント数、アクセス契約数、スケーラブルグループタグ数、サイト別の仮想ネットワーク数、IP プール数、SSID 数、Cisco ISE バージョンとステータス、グループベースのポリシー数、アクセスポリシー契約数、Cisco ACI スケーラブルグループ数、ファブリック内の AP および WLC の数、各トランジットタイプの数、不正 AP/クライアントメッセージ数、認証モード別のファブリックサイト数、静的ポート割り当てによるポート数 • 自動化の使用状況：PnP を使用してプロビジョニングされたデ	顧客導入と顧客価値の促進

カテゴリ	データ要素	収集の目的
	バイス数、ソース別の PnP デバイス数、ゴールデンイメージとイメージリポジトリの詳細の数、イメージのアクティブ化や配布の成功/失敗の数、タイプ別の SMU イメージ数、作成または展開されたアプリケーションポリシーの数、お気に入りのアプリケーション数、カスタムアプリケーション（セット）数、コンシューマ アプリケーション数、キューイングプロファイル数、除外されたデバイス数、各ポリシー内のデバイス数、ドラフトポリシー数、デフォルト以外のキューイングプロファイルを使用するポリシー数、デバイスの可制御性チェック、サイトエリア/ビルディング/フロアの数、ステータス別の SSA 有効化/無効化タスクの数、タイプ別の SSA 事前チェック失敗およびデバイスファミリごとの成功/失敗の数、Cisco Secure Network Analytics 登録ステータス、SSA 対応ステータス別のデバイス数、セキュリティアドバイザリに一致するデバイス数、セキュリティ アドバイザリ スキャンの数、vManage 統合ステータス、MRE の根本原因分析の数と期間、MRE ユーザーフィードバック数、CVSS スコアがあるデバイス数、交換ステータス別のデバイス数、WAB SDG ノード数、デバイスで正常に作成およびプロビジョニングされた導入準備テンプレートの数、テンプレートが適用されたデバイス数、サイトと名前空間別のネットワークプロファイル数 • Catalyst Center as a Platform の使用状況：ステータス別のイベントサブスクリプション数、DaaS ランタイムの使用率	
ネットワーク デバイス インベントリおよびライセンス権限	• ネットワーク デバイス インベントリ（シリアル番号、ソフトウェアバージョン、プラットフォーム ID、到達可能性エラー）。デバイスサポートレベルごとのデバイス数、デバイスロールごとのデバイス数、デバイスタイプごとのポートタイプ数、有効な IDP インスタンス、イーサネットチャンネル制御方式別のデバイス数、acltype 関連サイト情報別のデバイス数、デバイスタイプ別の稼働時間（日数）、デバイスタイプ別のホストカウント、構成タイプ別のデバイス数 • ライセンス権限情報（ネットワークデバイスタイプ、Cisco Smart Software Manager 登録ステータス、Catalyst Center サブスクリプションレベル、ハードウェアサポート契約範囲、ライセンスの有効期限までの日数）	ライセンス権限付与と更新の追跡と維持を支援します

Catalyst Center のプライバシーについては、シスコの個人データプライバシーを参照してください。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital® により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。100 ヵ国あまりの国々では、ハードウェア、ソフトウェア、サービス、およびサードパーティの補助機器を購入するのに、シスコの柔軟な支払いソリューションを利用して、簡単かつ計画的に支払うことができます。詳細はこちらをご覧ください。

詳細情報

Catalyst Center によって可能になる高速化、コスト削減、リスク低減については、https://cisco.com/go/catalystcenter をご覧ください。

文書の変更履歴

新規トピックまたは改訂されたトピック	説明箇所	日付
リリース **2.3.7** の更新	ドキュメント全体	2024 年 9 月
製品名を更新	ドキュメント全体	2024 年 9 月
DN3 の追加	表 14	2024 年 9 月
ファブリック展開と非ファブリック展開の統合スケール	表 14	2024 年 9 月
ファブリック展開と非ファブリック展開の統合スケールのアプライアンススケールを更新	表 14	2025 年 4 月

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。

Printed in USA C78-739686-29 04/25