The bridge to possible

Cisco Catalyst 9800-40 ワイヤレスコントローラ

インテントベース ネットワーキング向けに新たに構築

© 2022 Cisco and/or its affiliates. All rights reserved.

目次

© 2022 Cisco and/or its affiliates. All rights reserved.

製品の概要

図 1.
Cisco Catalyst 9800-40 ワイヤレスコントローラ

インテントベース ネットワーキングおよび Cisco DNA 向けに新たに構築された Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、Cisco IOS XE ベースで、Cisco Aironet アクセスポイントの優れた RF 性能を実装しています。これにより、クラス最高水準のワイヤレスエクスペリエンスで組織の進化と成長が実現されます。9800 シリーズは、組み込みのセキュリティ、ストリーミングテレメトリ、および豊富な分析機能を備えたオープンでプログラマブルなアーキテクチャに基づいて構築されています。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、優れたネットワーク性能の 3 つの柱（常時稼働、安全性、あらゆる場所に導入）に基づいて構築されています。これにより、侵害を受けることなく最高のワイヤレスエクスペリエンスを実現することでネットワークを強化し、同時に時間と費用も節約します。

Cisco Catalyst 9800-40 は、シームレスなソフトウェアアップデートを備えた、中規模および大規模の企業向けの固定ワイヤレスコントローラです。また、ビジネスクリティカルな業務を実行し、エンドカスタマー エクスペリエンスを変える機能を豊富に備えており、企業での使用に適しています。

- ホットパッチおよびコールドパッチ機能で使用可能になるハイアベイラビリティおよびシームレスなソフトウェアアップデートにより、計画内および計画外のイベント時にクライアントおよびサービスは**常時稼働**を維持します。
- Cisco Catalyst 9800-40 では、無線通信、デバイス、およびユーザーがセキュリティ**保護**されます。ワイヤレス インフラストラクチャは、シスコの暗号化トラフィック分析（ETA）とソフトウェア定義型アクセス（SD-Access）を備えた最強の第一防御線となります。コントローラには、セキュアブート、ランタイム防御、イメージ署名、整合性検証、ハードウェアの信頼性といったセキュリティが組み込まれています。
- モジュール型オペレーティングシステムに基づいて構築された 9800-40 には、オープンでプログラマブルな API 機能が搭載されており、0 日目から N 日目のネットワーク運用を**自動化**することができます。モデル駆動型のストリーミングテレメトリにより、**ネットワークとクライアントの正常性**に関する詳細なインサイトが提供されます。
- Cisco User Defined Network は Cisco DNA Center で使用可能な機能で、これにより IT 部門はエンドユーザに共有ネットワーク上の独自のワイヤレス ネットワーク パーティションの制御を任せることができます。エンドユーザは、このネットワークにデバイスをリモートで安全に導入できます。大学の学生寮や長期の病院での滞在に最適な Cisco User Defined Network は、デバイスのセキュリティと制御の両方を提供し、各ユーザはネットワークに接続できるユーザを選択できます。

© 2022 Cisco and/or its affiliates. All rights reserved.

- Wi-Fi 6 の対応状況を示すダッシュボードは、Cisco DNA Center のアシュアランスメニューにある新しいダッシュボードです。このダッシュボードではネットワーク上にある全デバイスが網羅され、デバイスやソフトウェア、クライアントが新しい Wi-Fi 6 規格との互換性を備えているかが検証されます。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。これはワイヤレスネットワークをアップグレードする場面とその方法をチームが定義するのに役立つ優れたツールであり、プロトコル別（802.11 ac/n/abg）のアクセスポイントの分布やプロトコル別のワイヤレス接続の通信時間の効率に関する情報を把握し、緻密な評価指標を入手できます。
- Cisco In Service Software Upgrade（ISSU）の機能により、ソフトウェアの更新やアップグレード中におけるネットワークのダウンタイムは過去のものとなります。ISSU はネットワークの機能を維持したまま、完全なイメージによるアップグレードと更新を実現します。ソフトウェアイメージまたはパッチは、トラフィックの転送を妨げることなくワイヤレスコントローラにプッシュされ、アップグレードのプロセスが進行中でもすべてのアクセスポイントとクライアントセッションが維持されます。ネットワークのアップグレードがクリック 1 つで済み、あとは自動で最新のソフトウェアに更新されます。

機能

表 1. 主な機能

メトリック	値
アクセスポイントの最大数	最大 2000 台
最大クライアント数	32,000
最大スループット	最大 40 Gbps
最大 WLAN 数	4096
最大 VLAN 数	4096
最大サイトタグ数	2000
サイトあたりの最大 Flex AP 数	100
最大ポリシータグ数	2000
最大 RF タグ数	2000
最大 RF プロファイル数	4000
最大ポリシープロファイル数	1000
最大 Flex プロファイル数	2000
インターフェイス	10G x 4、1G SFP+/SFP x 1
電源モジュール	AC 電源（オプションの冗長 AC 電源装置搭載）
最大消費電力	381W

© 2022 Cisco and/or its affiliates. All rights reserved.

メトリック	値
展開モード	一元化、Cisco FlexConnect、およびファブリックワイヤレス（SD-Access）
フォーム ファクタ	1 RU
ライセンス	スマートライセンス対応
オペレーティングシステム	Cisco IOS XE
管理	Cisco DNA Center、Cisco Prime Infrastructure、統合されたWebUI、およびサードパーティ（オープンスタンダード API）*
相互運用性	AireOS ベースのコントローラ*
ポリシーエンジン	Cisco Identity Services Engine（ISE）*
ロケーション プラットフォーム	Cisco Connected Mobile Experiences（CMX）、Cisco Spaces*
アクセスポイント	Aironet 802.11ac Wave 1 および Wave 2 アクセスポイント、Cisco Catalyst 9100 802.11ax アクセスポイント

*互換性については、『Compatibility Guide』を参照してください

常時稼働

シームレスなソフトウェアアップデートにより、重大な問題を迅速に解決したり、ダウンタイムなしで新しいアクセスポイントを導入することができるようになり、また、ソフトウェアアップデートの柔軟性も向上します。1：1 のアクティブ/スタンバイを使用したステートフル スイッチオーバー（SSO）と N+1 冗長性により、計画外のイベントが発生した場合でもネットワーク、サービス、およびクライアントは常時稼働を維持します。

セキュア

Cisco Catalyst 9800-40 ワイヤレスコントローラにより、無線通信、デバイス、およびユーザーがセキュリティ保護されます。ワイヤレス インフラストラクチャは、ETA と SD-Access を備えた最強の第一防御線となります。コントローラには、セキュアブート、ランタイム防御、イメージ署名、整合性検証、ハードウェアの信頼性といったセキュリティが組み込まれています。Cisco Advanced Wireless Intrusion Prevention System（aWIPS）は、Cisco Unified Access インフラストラクチャを使用して有線およびワイヤレスによる不正や脅威を検出し、場所を特定して緩和および封じ込めを行う完結型のワイヤレス セキュリティ ソリューションです。

オープンでプログラム可能

コントローラは、Cisco IOS XE オペレーティングシステムに基づいて構築されており、オープンスタンダードベースのプログラマブルな API やモデル駆動型のテレメトリが豊富に用意されています。これにより、0 日目から N 日目のネットワーク運用を簡単に自動化できます。

© 2022 Cisco and/or its affiliates. All rights reserved.

詳細

物理寸法

表 2. 物理寸法

寸法	値
幅	43.94 cm（17.3 インチ）
奥行	49.53 cm（19.5 インチ）
高さ	4.37 cm（1.72 インチ）
重量	10.34 kg（22.8 ポンド）

前面パネル

図 2.
前面パネル

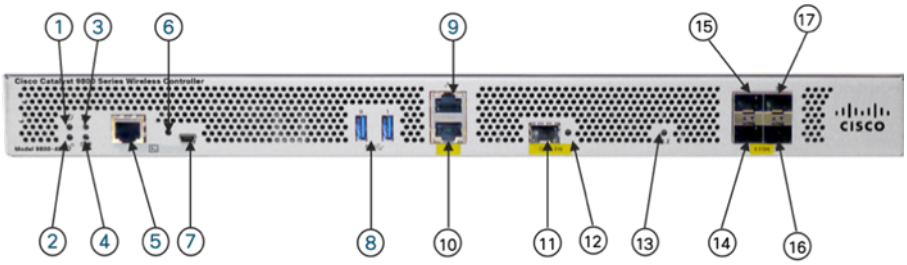

図 3.
前面パネルのコンポーネント

© 2022 Cisco and/or its affiliates. All rights reserved.

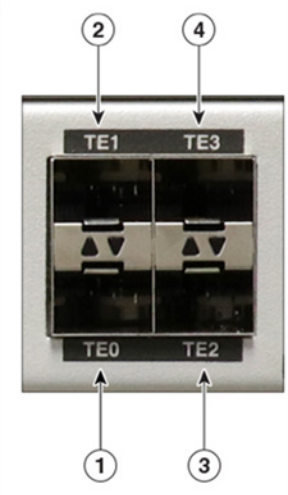

図 4.
10G/1G ポート

表 3. 前面パネルコンポーネントの説明

ラベル	コンポーネント
1	PWR：電源 LED
2	SYS：システム LED
3	ALM：アラーム LED
4	HA：ハイアベイラビリティ LED
5	CON：RJ-45 対応コンソールポート
6	EN：USB コンソール対応 LED
7	CON：ミニ USB コンソールポート
8	USB ポート 0 および 1
9	SP：RJ-45 10/100/1000 管理イーサネットポート
10	RP：RJ-45 10/100/1000 冗長イーサネットポート
11	RP：1 GE SFP ポート（RP ポートでサポートされる SFP は GLC-SX-MMD および GLC-LH-SMD のみ）
12	LINK：RJ-45 コネクタ LED
13	SSD：SSD アクティビティ LED
14	TE0：1 GE SFP/10 GE SFP+ ポート 0
15	TE1：1 GE SFP/10 GE SFP+ ポート 1

© 2022 Cisco and/or its affiliates. All rights reserved.

ラベル	コンポーネント
16	TE2：1 GE SFP/10 GE SFP+ ポート 2
17	TE3：1 GE SFP/10 GE SFP+ ポート 3

ポート

表 4. ポートとその目的

ポート	目的
RJ45 コンソールポート x 1	アウトオブバンド管理用コンソールポート
USB 3.0 コンソールポート x 1	アウトオブバンド管理用コンソールポート
USB 3.0 ポート x 2	外部メモリ接続用 USB 3.0 ポート
RJ-45 管理ポート x 1	アウトオブバンドの管理に使用される管理ポート。（別名：サービスポート）
RJ-45 冗長ポート x 1	SSO に使用される冗長ポート
SFP ギガビットイーサネット冗長ポート x 1	SSO に使用される冗長ポート • 冗長ポートは SSO に使用されます。RP ポート用のシスコ対応 SFP（GLC-LH-SMD および GLC-SX-MMD）を使用します
10G/1G SFP+ または SFP ポート x 4	アクセスポイントとコントローラの間のトラフィック、ノースバウンドトラフィック、インバンド管理トラフィック、およびワイヤレス クライアント トラフィックの送受信に使用されるポート。スイッチに接続する必要があります

前面パネル LED

表 5. 前面パネル LED

LED	色	機能
電源	緑	すべての電源レールが仕様範囲内の場合は緑になります
システム ステータス	緑	点灯：IOS が完全に起動 点滅：IOS ブートが進行中
	オレンジ	点灯：システムクラッシュ 点滅：セキュアブートの失敗 消灯：ROMMON ブート
高可用性	緑	点灯：HA アクティブ 点滅：HA スタンバイホット
	オレンジ	ゆっくり点滅：HA スタンバイコールドで起動 速い点滅：HA メンテナンス

© 2022 Cisco and/or its affiliates. All rights reserved.

LED	色	機能
アラーム	緑	点灯：ROMMON ブートの完了 点滅：システムアップグレードが進行中
	オレンジ	点灯：ROMMON ブートおよびシステムのブートアップ 点滅：温度エラーおよびセキュアブートの失敗
USB コンソール	緑	LED が点灯：USB コンソールが有効（RJ-45 コンソールは無効）
SSD アクティビティ	緑	ユニット内のハードディスク SSD メモリデバイスのアクティブな使用を示します
ネットワーク リンク	緑	緑の点灯はリンクを示します 緑の点滅はアクティビティを示します

背面パネル

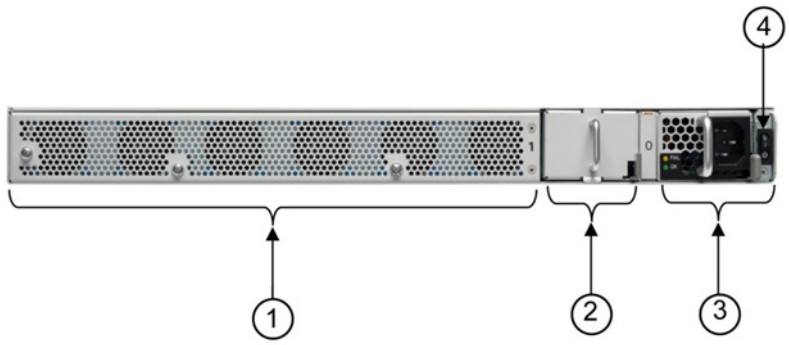

図 5.
背面パネル

表 6. 背面パネルコンポーネントの説明

ラベル	コンポーネント
1	ファン
2	オプションの冗長電源装置（PEM 1）
3	電源モジュール（PEM 0）
4	電源/スタンバイ スイッチ

© 2022 Cisco and/or its affiliates. All rights reserved.

背面パネル LED

表 7. 電源 LED

緑色の LED	オレンジ色の LED	電源装置ステータス
消灯	消灯	どの電源モジュールにも AC 電力が供給されていません
消灯	点灯	電源モジュールの障害（過電圧、過電流、過熱、ファン障害など）
消灯	1 Hz の点滅	電源が引き続き動作する場合（高温、高電力、および低速ファン）の電源の警告イベント
1 Hz の点滅	消灯	AC 電力があり、12VSB はオンになっています（電源オフ）
点灯	消灯	電源モジュールはオンで、正常に動作しています

電源

9800-40 コントローラは、オプションの冗長 AC 電源装置をサポートしています。

AC 入力範囲は次のとおりです。

- 国際的な AC 入力範囲（90 ~ 264 VAC）

電源入力モジュール（PEM）により、システムに冗長電源が提供されます。9800-40 は PEM を 1 つ搭載するだけで継続的に動作できます。PEM はホットスワップ可能です。システムへの電源を切断せずに 1 つの PEM を交換できます。PEM へのすべての外部接続はシャーシの背面パネルから行われ、背面から取り外しまたは挿入されます。装置の主電源スイッチはシャーシ背面の PEM のすぐ隣にあります。

サポートされる SFP

4 つのデータポートは 10G または 1G モードで動作できます。

注： 10/100-Mbps の動作はサポートされません。

表 8. サポートされる SFP

タイプ	サポートされるモジュール
小型フォーム ファクタ（SFP）	GLC-BX-D
	GLC-BX-U
	GLC-LH-SMD
	GLC-SX-MMD
	GLC-EX-SMD
	GLC-ZX-SMD
	GLC-TE

© 2022 Cisco and/or its affiliates. All rights reserved.

タイプ	サポートされるモジュール
拡張 SFP（SFP+）	SFP-10G-AOC1M
	SFP-10G-AOC2M
	SFP-10G-AOC3M
	SFP-10G-AOC5M
	SFP-10G-AOC7M
	SFP-10G-AOC10M
	SFP-10G-SR
	SFP-10G-SR-S
	SFP-10G-SR-X
	SFP-10G-LR
	SFP-10G-LRM
	SFP-10G-LR-X
	SFP-10G-ER
	SFP-10G-ZR
	SFP-H10GB-CU1M
	SFP-H10GB-CU1.5M
	SFP-H10GB-CU2M
	SFP-H10GB-CU2.5M
	SFP-H10GB-CU3M
	SFP-H10GB-CU5M
	SFP-H10GB-ACU7M
	SFP-H10GB-ACU10M
	DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41

© 2022 Cisco and/or its affiliates. All rights reserved.

利点

Cisco IOS XE により、ネットワーク自動化によるネットワークの設定、運用、モニターリングにまったく新しいパラダイムが展開されます。シスコの自動化ソリューションはオープンかつ標準ベースであり、ネットワークデバイスのライフサイクル全体をカバーします。デバイスのライフサイクルに基づき、ネットワーク自動化を実現するさまざまなメカニズムを以下に示します。

- **自動化されたデバイスプロビジョニング：**ネットワークでのシスコアクセスポイントの初回展開時に、ソフトウェアイメージのアップグレードプロセスおよびコンフィギュレーション ファイルのインストールプロセスを自動化します。シスコは、プラグアンドプレイ（PnP）などのターンキーソリューションを提供しています。これにより、自動化された負担の少ない展開が可能になります。
- **API 駆動型設定：**Cisco Catalyst 9800-40 ワイヤレスコントローラなどの最新ワイヤレスコントローラでは、多様な自動化機能をサポートしています。ネットワークリソースの自動プロビジョニング用途では、（既製およびカスタムビルドの）外部ツール向けとして YANG データモデルを使用するネットワーク設定プロトコル（NETCONF）を介した堅牢なオープン API を提供しています。
- **きめ細かな可視性：**モデル駆動型テレメトリは、ワイヤレスコントローラから宛先にデータをストリーミングするメカニズムを提供します。ストリーミングされるデータは、YANG モデルでのデータセット サブスクリプションを通じて伝達されます。サブスクライブされたデータセットは、設定された間隔で宛先に送信されます。さらに、Cisco IOS XE は、リアルタイムに近いネットワークモニタリングを実現するプッシュモデルを可能にします。これにより障害をすばやく検出・修正します。
- **シームレスなソフトウェアアップグレードとパッチ適用：**OS の復元力を強化するため、Cisco IOS XE では、通常のメンテナンスリリースの合間に、重大なバグやセキュリティの脆弱性に関する修正パッチを提供します。このサポートにより、お客様は次のメンテナンスリリースを待たずに修正パッチを適用できます。

常時稼働

- **ハイアベイラビリティ：**1：1 のアクティブ/スタンバイを使用したステートフル スイッチオーバーと N+1 冗長性により、計画外のイベントが発生した場合でもネットワーク、サービス、およびクライアントは常時稼働を維持します。
- **ホットパッチおよびコールドパッチを使用したソフトウェア メンテナンス アップグレード（SMU）：**パッチ適用により、ネットワーク全体をダウンさせることなくバグ修正としてパッチをインストールできます。これにより、ソフトウェアイメージ全体を再認定する必要がなくなります。SMU はシステムにインストールできるパッケージで、リリース済みのイメージにパッチ修正やセキュリティ上の問題の解決を行うことができます。SMU を使用するとネットワークの問題に迅速に対応できるだけでなく、テストに必要な時間と範囲も削減できます。Cisco IOS XE プラットフォームでは SMU の互換性が内部検証されるため、互換性のない SMU はインストールされません。すべて SMU が後続の Cisco IOS XE ソフトウェア メンテナンス リリースに統合されています。
- **アクセスポイントのインテリジェントなローリングアップグレードおよびシームレスなマルチサイトアップグレード：**Cisco Catalyst 9800-40 ワイヤレスコントローラには、ネットワーク運用を簡素化するためのアクセスポイントのインテリジェントなローリングアップグレードが搭載されています。マルチサイトアップグレードは複数のステージで実行できるようになりました。アクセスポイントは、ネットワーク全体を再起動することなくインテリジェントにアップグレードできます。

© 2022 Cisco and/or its affiliates. All rights reserved.

- ハイアベイラビリティ（HA）モードでの Cisco Catalyst 9800 ワイヤレスコントローラのスタンバイモニターリングにより、アクティブコントローラを経由せずに、プログラムインターフェイス（NETCONF/YANG、RESTCONF）および CLI を使用して、ハイアベイラビリティペアのスタンバイコントローラのシステム正常性をモニターできます。詳細については、技術マニュアルを参照してください。
- In-Service Software Upgrade（ISSU）：ISSU は、ネットワークを稼働したままで、ダウンタイムがゼロの、完全なイメージアップグレード/更新です。ソフトウェアイメージまたはパッチは、トラフィックの転送を妨げることなくワイヤレスコントローラにプッシュされ、アップグレードのプロセスが進行中でもすべてのアクセスポイントとクライアントセッションが維持されます。

  ネットワークのアップグレードがクリック 1 つで済み、あとは自動で最新のソフトウェアに更新されます。バックアップ 9800 コントローラは、アクティブな 9800 コントローラを介してプッシュされる新しいソフトウェアを受信します。バックアップ 9800 コントローラがアクティブに切り替わり、ネットワークを引き継ぐと同時にアクティブだった 9800 がバックアップ 9800 コントローラに切り替わって、ソフトウェアのアップグレードを処理します。インテリジェントな RF ベースのローリング アクセスポイント アップグレードによって、ワイヤレスセッションには影響を与えずにすべてのアクセスポイントが段階的にアップグレードされます。この手順は、コントローラからネイティブに手動で介入することなく、外部オーケストレータや追加ライセンスを必要とせずに実行されます。

セキュリティ

- **暗号化トラフィック分析（ETA）：**ETA は、アクセスレイヤから入ってくる暗号化トラフィックからマルウェアを特定できる独自機能です。トラフィックの暗号化は急増しているため、可視化して脅威を検出できるこの機能は、各レイヤでネットワークの安全性を保つために不可欠です。
- **信頼できるシステム：**Cisco Trust Anchor テクノロジーは、高い安全性の基盤をシスコ製品に提供します。高い信頼性を誇る Cisco Catalyst 9800-40 では、サプライチェーントラストに関するハードウェアとソフトウェアの信頼性を確保し、ソフトウェアやファームウェアでの中間者攻撃を大幅に軽減します。Trust Anchor の機能には、次のようなものがあります。
  - **イメージの署名：**暗号化で署名されたイメージは、ファームウェア、BIOS、およびその他のソフトウェアが正規のものであり、改ざんされていないことを保証します。システムのブート時に、ソフトウェアシグネチャの整合性が確認されます。
  - **セキュアブート：**シスコのセキュアブートテクノロジーは、ブートシーケンスの信頼チェーンを永続的なハードウェアに固定し、ユーザの権限レベルにかかわらず、システムの通常状態や実行されるソフトウェアに対する脅威を緩和します。不正に改ざんされたファームウェアに対しても、多層保護が実現します。
  - **Cisco トラストアンカーモジュール：**改ざん耐性と強力な暗号化を備えた単一チップのソリューションが製品を一意に識別します。これによりシスコが提供元を確認できるため、製品の真偽が保証されます。
  - **Cisco Wireless Intrusion Prevention System（WIPS）：**WIPS は、ワイヤレスネットワークへの侵入や脅威を検出、特定、軽減および阻止する高度なネットワークセキュリティを提供します。ワイヤレスネットワークの異常、不正アクセス、および RF 攻撃をモニタおよび検出できます。Cisco DNA Center には、不正および aWIPS 用の新しい専用分類エンジンが組み込まれています。WIPS ソリューションの完全統合スタックには、Cisco DNA Center、Cisco Catalyst 9800 コントローラ、Wave 2、および Cisco Catalyst 9100 アクセスポイントが含まれます。この新しいアーキテクチャにより、検出とセキュリティが向上し、シンプルで使いやすくなり、誤検出アラームが減少します。

© 2022 Cisco and/or its affiliates. All rights reserved.

Flexible NetFlow

- **Flexible NetFlow（FNF）：**Cisco IOS FNF は、柔軟性と拡張性が強化された次世代のフロー可視化テクノロジーです。ネットワーク インフラストラクチャの最適化や、運用コストの削減、キャパシティプランニングおよびセキュリティインシデント検出の改善に役立ちます。

アプリケーションの可視性と制御

- **次世代型 Network-Based Application Recognition（NBAR2）：**Cisco Catalyst 9800-40 では、NBAR2 により、最大 1400 の既知の事前定義済みアプリケーション署名と最大 150 の暗号化アプリケーションに対応する、高精度のアプリケーション分類技術が実現しています。最も一般的なアプリケーションには Skype、Office 365、Microsoft Lync、Cisco Webex、Facebook などがあります。その他の多数のアプリケーションがすでに事前定義されていて、簡単に設定できます。NBAR2 はエンドユーザによるアプリケーション使用を識別、制御、モニタするための重要なツールをネットワーク管理者に提供するとともに、ユーザエクスペリエンスの品質を確保し、悪意のある攻撃からネットワークを保護します。FNF を使用して、サポート対象の NetFlow コレクタ（Cisco Prime、Stealthwatch、準拠しているサードパーティツールなど）にネットワーク内のアプリケーション パフォーマンスやアクティビティを報告します。

サービス品質

- **優れた QoS：**QoS 技術はネットワークリソースを管理するツールおよび技術の集合であり、音声、ビデオおよびデータネットワークで透過的なコンバージェンスを実現するための鍵となる技術と考えられています。Cisco Catalyst 9800-40 の QoS は、パケットデータに基づいたトラフィックの分類とアプリケーションの認識やトラフィック制御アクション（ドロップ、マーキング、ポリシングなど）で構成されています。モジュール型の QoS コマンドライン フレームワークを採用することで、一貫性がありプラットフォームに依存しない、柔軟な構成による動作を実現します。また、9800-40 はターゲットの 2 つのレベル（BSSID とクライアント）のポリシーをサポートしています。ポリシーの割り当ては、クライアントレベルまで細かく下げることができます。

スマートオペレーション

- **Bluetooth 対応：**Cisco Catalyst 9800-40 では Bluetooth ドングルをコントローラに接続するハードウェアがサポートされており、このワイヤレスインターフェイスを管理ポートとして使用できます。このポートは IP 管理インターフェイスとして機能し、WebUI またはコマンドライン インターフェイス（CLI）を使った設定とトラブルシューティングに、あるいはイメージや設定の転送に使用できます。
- **WebUI：**WebUI は組み込み GUI ベースのデバイス管理ツールです。デバイスをプロビジョニングしたり、デバイスの導入および管理性を簡素化したり、ユーザーエクスペリエンスを向上したりする機能を提供します。WebUI にはデフォルトイメージが付属しています。デバイス上で何かを有効にしたり、ライセンスをインストールしたりする必要はありません。CLI の使用方法が分からなくても、WebUI を使用して 0 日目や 1 日目から設定を構築し、それ以降もデバイスをモニターしたり、トラブルシューティングしたりできます。

© 2022 Cisco and/or its affiliates. All rights reserved.

仕様

表 9. 仕様

項目	仕様	
ワイヤレス標準規格	IEEE 802.11a、802.11b、802.11g、802.11d、WMM/802.11e、802.11h、802.11n、802.11k、802.11r、802.11u、802.11w、802.11ac Wave 1 および Wave 2、802.11ax	
有線、スイッチング、およびルーティングの標準規格	IEEE 802.3 10BASE-T、IEEE 802.3u 100BASE-TX、1000BASE-T、1000BASE-SX、1000-BASE-LH、IEEE 802.1Q VLAN タギング、802.1AX リンクアグリゲーション	
データ標準規格	• RFC 768 User Datagram Protocol（UDP） • RFC 791 IP • RFC 2460 IPv6 • RFC 792 Internet Control Message Protocol（ICMP） • RFC 793 TCP • RFC 826 Address Resolution Protocol（ARP） • RFC 1122 インターネットホストの要件 • RFC 1519 Classless Inter-Domain Routing（CIDR） • RFC 1542 ブートストラッププロトコル （BOOTP） • RFC 2131 Dynamic Host Configuration Protocol（DHCP） • RFC 5415 Control and Provisioning of Wireless Access Points（CAPWAP）プロトコル • RFC 5416 802.11 向け CAPWAP バインディング	
セキュリティ規格	• Wi-Fi Protected Access（WPA） • IEEE 802.11i（WPA2、RSN） • Wi-Fi Protected Access 3（WPA3） • RFC 1321 MD5 メッセージ ダイジェスト アルゴリズム • RFC 1851 Encapsulating Security Payload（ESP） Triple DES（3DES）変換 • RFC 2104 HMAC：メッセージ認証用の鍵付きハッシュ • RFC 2246 TLS プロトコルバージョン 1.0 • RFC 2401 インターネットプロトコルのためのセキュリティアーキテクチャ • RFC 2403 ESP および AH における HMAC-MD5-96 • RFC 2404 ESP および AH における HMAC-SHA-1-96 • RFC 2405 明示的 IV を伴う ESP DES-CBC 暗号アルゴリズム • RFC 2407 Internet Security Association Key Management Protocol（ISAKMP）の解釈 • RFC 2408 ISAKMP • RFC 2409 インターネット キー エクスチェンジ（IKE） • RFC 2451 ESP CBC モード暗号アルゴリズム • RFC 3280 インターネット X.509 Public Key Infrastructure（PKI）証明書および証明書失効リスト（CRL）プロファイル • RFC 4347 データグラムトランスポート層セキュリティ（DTLS） • RFC 5246 TLS プロトコルバージョン 1.2	

© 2022 Cisco and/or its affiliates. All rights reserved.

項目	仕様	
暗号化標準規格	• スタティック Wired Equivalent Privacy（WEP）RC4 40、104、および 128 ビット • Advanced Encryption Standard（AES）：Cipher Block Chaining（CBC）、Counter with CBC-MAC（CCM）、Counter with CBC Message Authentication Code Protocol（CCMP） • DES：DES-CBC、3DES • セキュアソケットレイヤ（SSL）および Transport Layer Security（TLS）：RC4 128 ビットと、RSA 1024 ビットおよび 2048 ビット • DTLS：AES-CBC • IPsec：DES-CBC、3DES、AES-CBC • 802.1AE MACsec 暗号化	
認証、許可、およびアカウンティング（AAA）の標準規格	• IEEE 802.1X • RFC 2548 Microsoft ベンダー固有の RADIUS 属性 • RFC 2716 Point-to-Point Protocol（PPP）Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）- TLS • RFC 2865 RADIUS 認証 • RFC 2866 RADIUS アカウンティング • RFC 2867 RADIUS トンネルアカウンティング • RFC 2869 RADIUS 拡張 • RFC 3576 RADIUS への動的許可拡張機能 • RFC 5176 RADIUS への動的許可拡張機能 • RFC 3579 EAP の RADIUS サポート • RFC 3580 IEEE 802.1X RADIUS ガイドライン • RFC 3748 Extensible Authentication Protocol（EAP） • Web ベース認証 • 管理ユーザのための TACACS サポート	
管理標準規格	• Simple Network Management Protocol（SNMP）v1、v2c、v3 • Telnet（RFC 854） • RFC 1155 TCP/IP ベースのインターネットの管理情報 • RFC 1156 MIB • RFC 1157 SNMP • RFC 1213 SNMP MIB II • RFC 1350 Trivial File Transfer Protocol（TFTP） • RFC 1643 イーサネット MIB • RFC 2030 Simple Network Time Protocol（SNTP） • RFC 2616 HTTP • RFC 2665 Ethernet-Like インターフェイスタイプ MIB • RFC 2674 トラフィッククラス、マルチキャスト フィルタリング、および仮想拡張機能を使用したブリッジの管理対象オブジェクトの定義 • RFC 2819 リモートモニターリング（RMON）MIB • RFC 2863 インターフェイスグループ MIB • RFC 3164 Syslog • RFC 3414 SNMPv3 のユーザベース セキュリティ モデル（USM） • RFC 3418 SNMP MIB • RFC 3636 IEEE 802.3 MAU のマネージドオブジェクトの定義 • RFC 4741 Base NETCONF プロトコル • RFC 4742 NETCONF over SSH	

© 2022 Cisco and/or its affiliates. All rights reserved.

項目	仕様	
	• RFC 6241 NETCONF • RFC 6242 NETCONF over SSH • RFC 5277 NETCONF イベント通知 • RFC 5717 部分ロックのリモートプロシージャコール • RFC 6243 NETCONF のデフォルトあり機能 • RFC 6020 YANG • シスコのプライベート MIB	
管理インターフェイス	• Web ベース：HTTP/HTTPS • コマンドライン インターフェイス：Telnet、Secure Shell （SSH）プロトコル、シリアル ポート • SNMP • NETCONF	
ハードディスクドライブ (HDD)	• SATA ソリッドステートドライブ（SSD） • 240 GB のメモリ	
サポートされる環境条件	動作温度： • 通常：0 ~ 40 °C（32 ~ 104 °F） • 短時間：0 ~ 50° C（32 ~ 122° F） 温度（非動作時）： • -40 ～ 65° C（-104 ~ 149° F） 湿度（動作時）： • 通常：10 ~ 90%（結露しないこと） • 短時間：5 ~ 90%（結露しないこと） 非動作時温度湿度： • 5% ~ 93%（28 °C（82 °F）時） 動作時の高度： • アプライアンス動作環境：0 ~ 3000m（0 ~ 10,000 ft） • アプライアンス非動作環境：0 ~ 12,192 m（0 ~ 40,000 ft） 電源入力： • AC 入力周波数範囲：47 ~ 63 Hz • AC 入力範囲：90 ~ 264 VAC（AC PEM 搭載） • 1100W AC（オプションの冗長電源装置搭載、ホットスワップ可能） 最大電力：381 W 熱放散：1300 BTU/時 音響レベル測定： • A 特性音声レベルは 27C の公称動作温度で 74.1 LpAm（dBA）	

© 2022 Cisco and/or its affiliates. All rights reserved.

項目	仕様	
適合規格の遵守	安全性： • UL/CSA 60950-1 • IEC/EN 60950-1 • AS/NZS 60950.1 • CAN/CSA-C22.2 No. 60950-1	
	EMC：エミッション： • FCC 47CFR15 • AS/NZS CISPR 22 • CISPR 22 • EN55022/EN55032（EMI-1） • ICES-003 • VCCI • KN 32（EMI-2） • CNS 13438	**クラス A**
	EMC：エミッション： • EN61000-3-2 電源高調波（EMI-3） • EN61000-3-3 電圧変動、変動、およびフラッカ（EMI-3）	
	EMC：イミュニティ： • IEC/EN61000-4-2 静電放電イミュニティ • IEC/EN61000-4-3 放射電磁界イミュニティ • IEC/EN61000-4-4 EFT-B イミュニティ（AC 電源リード線） • IEC/EN61000-4-4 EFT-B イミュニティ（DC 電源リード線） • IEC/EN61000-4-4 EFT-B イミュニティ（信号リード線） • IEC/EN61000-4-5 サージ AC ポート • IEC/EN61000-4-5 サージ DC ポート • IEC/EN61000-4-5 サージシグナルポート • IEC/EN61000-4-6 伝導妨害に対するイミュニティ • IEC/EN61000-4-8 電源周波数磁界イミュニティ • IEC/EN61000-4-11 電圧ディップ、瞬断、および電圧変異 • K35（EMI-2）	
	EMC（ETSI/EN） • EN 300 386 電気通信ネットワーク機器（EMC）（EMC-3） • EN55022 情報技術機器（エミッション） • EN55024/CISPR 24 情報技術機器（イミュニティ） • EN50082-1/EN61000-6-1 一般イミュニティ標準（EMC-4）	

© 2022 Cisco and/or its affiliates. All rights reserved.

ソフトウェア要件

Cisco Catalyst 9800-40 は、Cisco IOS XE ソフトウェアバージョン 16.10.1 以降で実行されます。このソフトウェアリリースには、「プラットフォーム ソフトウェアの利点」セクションに記載されている機能がすべて含まれています。

表 10. ソフトウェアの最小要件

モデル	説明	ソフトウェアの最小要件
C9800-40-K9	Cisco Catalyst 9800-40 ワイヤレスコントローラ	Cisco IOS XE ソフトウェアリリース 16.10.1

ライセンス

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを起動するのにライセンスは必要ありません。ただし、**コントローラ**にアクセスポイントを接続するには、Cisco DNA ソフトウェア サブスクリプションが必要です。9800 シリーズ コントローラに接続する資格を得るには、各アクセスポイントに Cisco DNA サブスクリプション ライセンスが必要です。

© 2022 Cisco and/or its affiliates. All rights reserved.

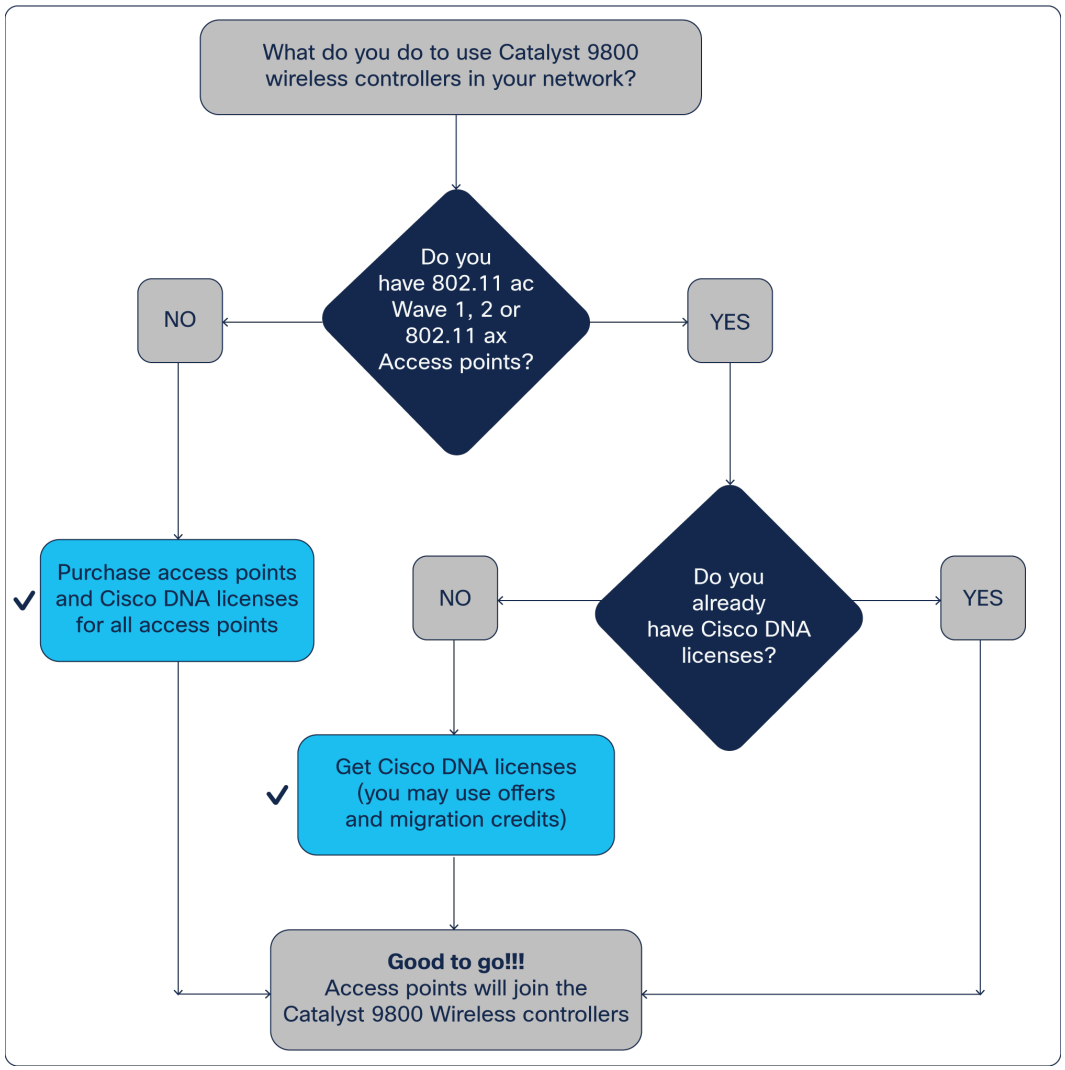

図 6.
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続するアクセスポイントのライセンス要件の決定

Cisco Catalyst 9800 シリーズに接続するアクセスポイントには、新しく簡素化されたソフトウェア サブスクリプション パッケージがあります。

Cisco DNA Essentials および Cisco DNA Advantage を含む Cisco DNA ソフトウェアの両方の層をサポートします。

Cisco DNA ソフトウェア サブスクリプションは、アクセスポイントに関するシスコのイノベーションを提供します。これらには永続的な Network Essentials と Network Advantage のライセンスオプションもあり、802.1X 認証、QoS、PnP のようなワイヤレスの基本要素だけでなく、テレメトリや可視性、SSO、セキュリティ制御にも対応します。

Cisco DNA サブスクリプション ソフトウェアは、3 年、5 年、または 7 年のサブスクリプション期間を購入する必要があります。サブスクリプションの有効期限が切れると Cisco DNA の機能も無効になりますが、Network Essentials と Network Advantage の機能はそのまま使えます。

© 2022 Cisco and/or its affiliates. All rights reserved.

永続的な Network Essentials および Network Advantage を含む Cisco DNA ソフトウェアの全機能リストについては、次の機能マトリックスを参照してください。https://www.cisco.com/c/m/en_us/products/software/dna-subscription-wireless/en-sw-sub-matrix-wireless.html?oid=porew018984

2 つのモードのライセンスを使用できます。

- 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、迅速かつ便利に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。PAK（製品アクティベーションキー）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ので、取得したもの、使用しているもの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概要については詳しくは、cisco.com/go/licensingguide を参照してください
- Specific License Reservation（SLR）は、非常にセキュリティの高いネットワークで使用される機能です。この機能により、お客様は使用状況をシスコと同期通信することなく、デバイス（製品インスタンス）にソフトウェアライセンスを導入できます。シスコまたはサテライトとは通信しません。ライセンスは、すべてのコントローラ向けに予約されます。これは、ノードベースのライセンスです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、4 つのレベルのライセンスがサポートされます。コントローラは、4 つのうちいずれかのレベルで機能するように設定できます。

- Cisco DNA Essentials：このレベルでは、Cisco DNA Essentials 機能セットがサポートされます。
- Cisco DNA Advantage：このレベルでは、Cisco DNA Advantage 機能セットがサポートされます。
- NE：このレベルでは、Network Essentials 機能セットがサポートされます。これは、Cisco DNA Essentials で使用できます。
- NA：このレベルでは、Network Advantage 機能セットがサポートされます。これは、Cisco DNA Advantage で使用できます。

Cisco DNA Essentials をご購入のお客様については、Network Essentials がサポートされ、有効期限終了後も引き続き機能します。また、Cisco DNA Advantage をご購入のお客様については、Network Advantage がサポートされ、有効期限終了後も引き続き機能します。

コントローラの初回起動は Cisco DNA Advantage レベルで実行されます。

ご質問がある場合は、ask-catalyst 9800 licensing で Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ライセンスのメールグループにお問い合わせください。

© 2022 Cisco and/or its affiliates. All rights reserved.

スマートアカウントによるライセンス管理

Cisco Smart Software Manager（SSM）を使用してスマートアカウントを作成すると、デバイスやライセンスパッケージの発注およびソフトウェアライセンスの管理を、一元化された Web サイトから実施できるようになります。スマートアカウントを設定すると、日単位で電子メールアラートが送信され、アドオンライセンスの更新期限通知を受け取ることができます。スマートアカウントは、Cisco Catalyst 9800 シリーズに必須です。スマートアカウントの詳細については、https://www.cisco.com/jp/go/smartaccounts を参照してください。

保証

保証については、Cisco.com の「製品保証」ページ [英語] を参照してください。

シスコ製品（ハードウェア）に関する 1 年間の Limited warranty 規定

ハードウェア保証には次の条件が適用されます。組み込みソフトウェアは、シスコ一般条件（後述のリンクを参照）および/または任意の SEULA、またはデバイスに読み込まれたその他のソフトウェア製品に固有のソフトウェア保証条件に従います。

ハードウェア保証期間：1 年間

ハードウェアの交換、修理、返金：シスコまたはシスコのサービスセンターでは、返品許可（RMA）要求を受領してから 10 営業日以内に交換部品を出荷できるように、ビジネスの範囲内で適正な努力を払っています。実際の配送期間は、お客様がお住まいの地域によって異なります。

シスコは購入代金を払い戻すことにより一切の保証責任とさせて頂く権利を留保します。

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 11. 持続可能性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
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
持続可能性に関するお問い合わせ	連絡先： csr_inquiries@cisco.com

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。

© 2022 Cisco and/or its affiliates. All rights reserved.

発注情報

表 12. 発注情報

タイプ	製品 ID	説明
コントローラ	C9800-40-K9	Cisco Catalyst 9800-40 ワイヤレスコントローラ
	LIC-C9800-DTLS-K9	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ DTLS ライセンス
アクセサリ、スペア	C9800-AC-750W R=	Cisco Catalyst 9800-40 750W AC 電源装置、リバース エア

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、および他社製製品を購入するのに、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。

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
Cisco DNA Spaces の名称変更	製品名を Cisco Spaces に更新	10/21/22

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。

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/jp/go/trademarks をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1110R)

Printed in USA C78-741545-12 10/22

© 2022 Cisco and/or its affiliates. All rights reserved.