Cisco IOS XE Cupertino 17.7.x（Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ）リリースノート

初版：2021 年 12 月 7 日

最終更新：2022 年 2 月 8 日

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、 Cisco IOS XE Cupertino 17.7.x

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク向けに設計された次世代のワイヤレスコントローラ群で構成されています。Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Cisco Aironet の無線周波数（RF）機能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Catalyst 9800 コントローラは企業のニーズに対応しており、ビジネスクリティカルな業務の遂行を促進し、エンドユーザーのエクスペリエンスを変革します。

- 高可用性（HA）、およびホットパッチとコールドパッチによって実現されるシームレスなソフトウェアアップデートが組み込まれています。これにより、計画内のイベントでも計画外のイベントでもクライアントおよびサービスの稼働が常に維持されます。
- 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。
- オンプレミスのデバイス、クラウド（パブリックまたはプライベート）、Cisco Catalyst スイッチまたは Cisco Catalyst アクセスポイント（AP）への組み込みなど、場所を問わず展開して、ワイヤレス接続を実現できます。
- Cisco Digital Network Architecture（DNA）Center、プログラマビリティ インターフェイス（たとえば、NETCONF および YANG）、または Web ベースの GUI または CLI を使用して、コントローラを管理できます。
- モジュラ型のオペレーティングシステムに基づいて構築されています。プログラム可能なオープン API により、すべて（Day 0 から Day n まで）のネットワーク運用を自動化できます。モデル駆動型のストリーミングテレメトリにより、ネットワークおよびクライアントの健全性に関する深い洞察が提供されます。

Catalyst 9800 シリーズ コントローラは、次のように、さまざまなフォームファクタに対応しており、展開オプションに合わせて選択できます。

- Catalyst 9800 シリーズ ワイヤレス コントローラ アプライアンス
- クラウド向け Catalyst 9800 シリーズ ワイヤレス コントローラ
- Cisco スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ

（注） Cisco Catalyst 9800 コントローラに関する Cisco IOS-XE のプログラマビリティ関連のトピックはすべて、コミュニティベースのサポートまたは DevNet 開発者サポートを通じて、DevNet によってサポートされます。詳細については、https://developer.cisco.com を参照してください。

Cisco IOS XE Cupertino 17.7.1 の新機能

表 *1:* ソフトウェアの新機能および変更された機能

機能名	説明とドキュメントのリンク
Cisco Catalyst 9136I アクセスポイントでの 6 GHz クライアントステアリングのサポート	Cisco IOS XE Cupertino 17.7.1 以降、6 GHz クライアントステアリングは Cisco Catalyst 9136I アクセスポイントでサポートされます。 コントローラが 2.4 GHz 帯域または 5 GHz 帯域から定期的なクライアント統計レポートを受信すると、6 GHz クライアントステアリングが実行されます。クライアントステアリング構成は WLAN で有効になり、6 GHz 対応のクライアントに対してのみ構成されます。レポートのクライアントが 6 GHz に対応している場合、クライアントステアリングがトリガーされ、クライアントは 6 GHz 帯域にステアリングされます。 次のコマンドが導入されています。 • **client-steering** • **wireless client client-steering client-count** • **wireless client client-steering window-size** • **wireless client client-steering util-threshold** • **wireless client client-steering min-rssi-24ghz -70** • **wireless client client-steering min-rssi-5ghz -75** 詳細については、「6-GHz Band Operations」の章を参照してください。

機能名	説明とドキュメントのリンク
Cisco Catalyst 9136I アクセスポイントでの 6 GHz 無線帯域のサポート	Cisco IOS XE Cupertino 17.7.1 以降、Cisco Catalyst 1936I アクセスポイントは 6 GHz 無線帯域をサポートします。 次のコマンドが導入されています。 • **channel psc** • **dot11ax bcast-probe-response time-interval** • **dot11ax fils-discovery** • **dot11ax multi-bssid-profile** • **dot11ax {downlink-mumimo | downlink-ofdma | target-waketime | twt-broadcast | uplink-mumimo | uplink-ofdma}**
ローカル EAP 認証での暗号スイートの選択	Cisco IOS XE Cupertino 17.7.1 以降、コントローラには、ローカル認証を使用するときに暗号スイートのリストを制御するノブが装備されます。 詳細については、「Local EAP Ciphersuite」の章を参照してください。
Cisco AI 拡張 RRM	AI 拡張無線リソース管理（RRM）は、シスコで受賞歴のある RRM の最新版です。 AI 拡張 RRM は、Cisco DNA Center（オンプレミスアプライアンス）を介してサービスとして調整されます。現在の RRM サイトは、インテリジェントかつ一元化されたサービスにシームレスに移行されます。AI 拡張 RRM は、他の Cisco DNA Center サービスとともに多数の新機能を提供します。 詳細については、「Radio Resource Management」の章を参照してください。
Cisco OEAP スプリットトンネリング	Cisco OfficeExtend アクセスポイント（OEAP）のスプリットトンネリング機能は、パケットの内容を基にアクセス制御リスト（ACL）を使用してクライアントトラフィックを分類するメカニズムを提供します。 次のコマンドが導入されました。 • **show split-tunnel client access-list** 詳細については、「Cisco OEAP Split Tunneling」の章を参照してください。

機能名	説明とドキュメントのリンク
インテリジェントキャプチャ（iCAP）または IoT サービスの共存：デュアル gRPC チャネル	Cisco IOS XE Cupertino 17.7.1 以降、IoT サービスとインテリジェントキャプチャ（iCAP）のポート構成が共存できるようになります。つまり、コントローラで IoT サービスと iCAP 機能が両方有効になっている場合、対応する AP から 2 つの gRPC が接続されます。 AP から接続される gRPC は次のとおりです。 • AP から Cisco DNA Center への gRPC 接続（iCAP 用）。 • AP から Cisco DNA Spaces Connector への gRPC 接続（IoT サービス用）。 詳細については、「IoT Services Management」の章を参照してください。
NAS-ID でのカスタマイズされた文字列の構成	ネットワーク アクセス サーバー識別子（NAS-ID）は、送信元に RADIUS アクセス要求を通知するために使用されます。これにより、RADIUS サーバーはその要求のポリシーを選択できます。各 WLAN プロファイル、VLAN インターフェイス、またはアクセスポイントグループで 1 つ設定できます。 次のコマンドが変更されました。 • **nas-id** 詳細については、「Network Access Server Identifier」の章を参照してください。
IOS コマンドの XML への変換	この機能は、シスコの IOS コマンドを関連する NETCONF-XML または RESTCONF/JSON 要求メッセージに自動的に変換するために役立ちます。 詳細については、『Programmability Configuration Guide』を参照してください。

機能名	説明とドキュメントのリンク
メッシュアクセスポイントの高速ティアダウン	この機能では、ルートアクセスポイントのアップリンク障害を検出し、アップリンク障害が発生した場合にメッシュネットワークの高速ティアダウンに対処します。 次のコマンドが導入されています。 • **fast-teardown** • **wireless profile mesh** （注） メッシュ AP の高速ティアダウンは、Cisco Industrial Wireless（IW）3702 アクセスポイントではサポートされていません。 詳細については、「Mesh Access Points」の章を参照してください。
gNOI factory-reset サービス	gNOI factory-reset サービスは、現在の状態を消去し、工場出荷時と同じ状態でデバイスを起動するようにターゲットデバイスに指示するインターフェイスを提供します。 詳細については、『Programmability Configuration Guide』を参照してください。
Microsoft Azure クラウドサービスへの Cisco Catalyst 9800-CL クラウドワイヤレス コントローラのインストール	Microsoft Azure クラウドサービスは、クラウドインフラストラクチャでコントローラを起動する機能をユーザーに提供します。 詳細については、『Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide』を参照してください。
不正なデバイスの管理	Cisco IOS XE Cupertino 17.7.1 以降、次の署名を使用して、AP のなりすましがマネージド AP で使用されている番号とは異なるチャネル番号を使用しているかどうかを識別できます。 • Beacon DS Attack • ビーコン不正チャネル 詳細については、「Managing Rogue Devices」の章を参照してください。

機能名	説明とドキュメントのリンク
メッシュ シリアル バックホール	Cisco Catalyst 9124AXE シリーズ屋外アクセスポイントでは、メッシュ シリアルバックホール機能が Cisco IOS XE Cupertino 17.7.1 以降のコントローラでサポートされます。無線プロファイルに新しいノブが導入され、その無線プロファイルが RF タグに関連付けられて、メッシュ シリアルバックホール機能が有効になります。 次のコマンドが導入されています。 • **mesh backhaul** • **mesh designated downlink** • **show ap name config slot 2 | inc Mesh** 詳細については、「Mesh Access Points」の章を参照してください。
リアルタイム アクセスポイント統計	無線モニタリングでは、Cisco IOS XE Cupertino 17.7.1 以降、サンプリング期間中に対応する AP から送信された統計に基づいて無線をリセットできます。コントローラで無線を設定するとき、無線の稼働時に Tx または Rx の統計で増分がない場合、無線のリセットがトリガーされます。 次のコマンドが導入されています。 • **show wireless stats ap join summary** • **show wireless stats ap history** 詳細については、「Real-Time Access Points Statistics」の章を参照してください。
Cisco Catalyst 9124AXE アクセスポイントでのリモート LAN のサポート	Cisco IOS XE Cupertino 17.7.1 以降、リモート LAN は Cisco Catalyst 9124AXE アクセスポイントのローカルモードおよびデュアル無線モードでサポートされます。 詳細については、「Remote LANs」の章を参照してください。
ファブリックでの RLAN のサポート	Cisco IOS XE Cupertino 17.7.1 以降、RLAN 機能はファブリックでサポートされます。 詳細については、「Remote LANs」の章を参照してください。

機能名	説明とドキュメントのリンク
ポリシーを使用したスマートライセンシング：ACK および show コマンドの出力に含まれるアカウント情報	RUM 確認応答（ACK）には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれます。次に、さまざまな**show** コマンドを使用してアカウント情報を表示できます。このアカウント情報は、製品インスタンスで使用可能な最新の ACK に基づいて常に表示されます。 詳細については、「Smart Licensing Using Policy」の章を参照してください。
ポリシーを使用したスマートライセンシング：Linux 向け CSLU のサポート	Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入できるようになりました。 詳細については、「Smart Licensing Using Policy」の章を参照してください。
ポリシーを使用したスマートライセンシング：プレインストールされた信頼コード	新しいハードウェアの注文では、信頼コードは製造時にインストールされるようになりました。注：出荷時にインストールされた信頼コードを使用して CSSM と通信することはできません。 詳細については、「Smart Licensing Using Policy」の章を参照してください。
ポリシーを使用したスマートライセンシング：Cisco Catalyst 9800-CL ワイヤレスコントローラのリソース使用率測定（RUM）レポートと確認応答（ACK）の要件	Cisco Catalyst 9800-CL ワイヤレスコントローラを使用している場合は、RUM レポートを完了し、製品インスタンスで ACK が少なくとも 1 回利用できるようにする必要があります。これは、正しい最新の使用状況情報が CSSM に反映されるようにするためです。 次のコマンドが導入されました。 • **show license air entities** 詳細については、「Smart Licensing Using Policy」の章を参照してください。
ポリシーを使用したスマートライセンシング：RUM レポートの最適化と統計情報の可用性	RUM レポートの生成と関連プロセスが最適化されました。これには、RUM レポートの処理にかかる時間の短縮、メモリとディスク領域の使用率の向上、および製品インスタンス上の RUM レポートの可視性（エラーがある場合、エラーの数、各プロセスの処理状態など）が含まれます。 詳細については、「Smart Licensing Using Policy」の章を参照してください。

機能名	説明とドキュメントのリンク
ポリシーを使用したスマートライセンシング：追加のトポロジでの信頼コードのサポート	信頼コードは、製品インスタンスが *CSLU* へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。 詳細については、「Smart Licensing Using Policy」の章を参照してください。
ポリシーを使用したスマートライセンシング：スマート ライセンス エージェントによるソフトウェアバージョン収集のサポート	バージョンプライバシーが無効になっている場合（**no license smart privacy version** グローバル コンフィギュレーション コマンド）、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョン情報が RUM レポートに含まれます。 詳細については、「Smart Licensing Using Policy」の章を参照してください。
Software-Defined Application Visibility and Control	Software-Defined Application Visibility and Control（SD-AVC）は、複数のデバイスおよびソースからのアプリケーションデータを集約し、複合的なアプリケーション情報を提供するネットワークレベルの AVC コントローラです。 次のコマンドが導入されています。 • **address** • **avc sd-service** • **controller** • **destination-ports** • **dscp** • **segment** • **source-interface** • **transport application-updates** • **vrf** • **show sdavc ap download status** • **show sdavc status ap** 詳細については、「Software-Defined Application Visibility and Control」の章を参照してください。

機能名	説明とドキュメントのリンク
ストリーミングテレメトリ	Cisco IOS XE Cupertino 17.7.1 以降、XPath のサブセットで変更時のテレメトリがサポートされます。 次のコマンドが導入されています。 • **show ap name dot11 neighbor summary** • **show wireless stats ap join summary sort** • **show ap summary sort name** 詳細については、「Streaming Telemetry」の章を参照してください。
SUDI99 証明書のサポート	コントローラおよびAPプラットフォームで使用される証明書の一部が 2029 年 5 月に期限切れとなるため、新しい証明書セットへの移行が必要になります。SUDI99 証明書のサポートは、この移行シナリオに対応しています。 次のコマンドが導入されています。 • **no platform sudi cmca3** • **show platform sudi pki** 詳細については、「SUDI99 Certificate Support」の章を参照してください。
メッシュアクセスポイントでの連邦情報処理標準（FIPS）モードのサポート	このリリース以降、FIPS モードはメッシュアクセスポイントでサポートされます。

機能名	説明とドキュメントのリンク
SAE 認証での Wi-Fi Protected Access 3 Hash-to-Element（H2E）サポート	Hash-to-Element（H2E）は、SAE プロトコルで使用されるパスワード要素生成の新しい方法です。これは、サイドチャネル攻撃を軽減するための計算効率の良い手法です。 WLAN 構成でサポートされているパスワード要素の方法は次のとおりです。 • h2e：Hash-to-Element のみ。HnP を無効にします。 • hnp：Hunting and Pecking のみ。H2E を無効にします。 • Both-h2e-hnp：Hash-to-Element と Hunting and Pecking の両方をサポート（デフォルトのオプションです）。 次のコマンドが変更されました。 • **security wpa akm sae pwe {h2e | hnp | both-h2e-hnp}** 詳細については、「Wi-Fi Protected Access 3」の章を参照してください。
Wi-Fi Protected Access 3 での移行無効化のサポート	移行の無効化は、AP から STA に関する説明です。この機能により、AP のネットワークへの後続の接続でいくつかの移行モードを無効にします。 次のコマンドが導入されました。 • **transition-disable** 詳細については、「Wi-Fi Protected Access 3」の章を参照してください。
YANG モデルバージョン 1.1	Cisco IOS XE Cupertino 17.7.1 では YANG バージョン 1.0 を使用しています。ただし、GitHub フォルダから YANG バージョン 1.1 をダウンロードできます。migrate_yang_version.py スクリプトまたは Cisco IOS XE YANG 移行プロセスに関するお問い合わせは、xe-yang-migration@cisco.com にメールをお送りください。 詳細については、『Programmability Configuration Guide』を参照してください。
YANG による ZTP の設定	ゼロタッチプロビジョニングは、NETCONF が有効であれば、YANG モデルを介して有効化されます。 詳細については、『Programmability Configuration Guide』を参照してください。

表 *2 :* 新規および変更された *GUI* 機能

機能名	GUI パス
Cisco Catalyst 9136I アクセスポイントでの 6 GHz クライアントステアリングのサポート	• [Configuration] > [Tags & Profiles] > [WLANs]
Cisco Catalyst 9136I アクセスポイントでの 6 GHz 無線帯域のサポート	• [Configuration] > [Tags & Profiles] > [RF/Radio] > [RF]
メッシュアクセスポイントの高速ティアダウン	• [Configuration] > [Wireless] > [Mesh] > [Profiles]
メッシュ シリアル バックホール	• [Configuration] > [Tags & Profiles] > [RF/Radio]
ネットワークアクセスサーバー識別子	• [Configuration] > [Security] > [Wireless AAA Policy]
リアルタイム アクセスポイント統計	• [Configuration] > [Tags & Profiles] > [AP Join]
SUDI99 証明書のサポート	• [Configuration] > [Security] > [PKI Management] > [Trustpoint]
SAE 認証での Wi-Fi Protected Access 3 Hash-to-Element（H2E）サポート	• [Configuration] > [Tags & Profiles] > [WLANs]

MIB

以下の MIB が新たに追加または変更されました。

- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-AP-MIB.my
- CISCO-LWAPP-AP-RADIOSTUCK-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-RRM-MIB.my
- CISCO-LWAPP-RF-MIB.my

動作の変更

- シリアルポートを介したコンソールへのアクセスは、コンソールのアクティビティが低い場合にのみ許可されます。Telnet セッションでコンソールを使用することを推奨します。
- ローカルモードで 802.11w が有効になっている場合、コントローラは再アソシエーション要求を拒否し、前の認証が成功した場合にのみセキュリティ アソシエーション クエリを送信します。
- Cisco TrustSec（CTS）の手動設定と 802.1x 設定は、セキュリティ アソシエーション プロトコル（SAP）が設定されていない場合に共存できます。
- スマートライセンスまたはライセンスレベルが設定されている場合、HA システム（GRUB3 インスタンス）で Cisco IOS XE Bengaluru 17.6.1 にダウングレードすることはできません。したがって、HA のスマートライセンスは Cisco IOS XE Bengaluru 17.6 では機能しないため、スマートライセンスやライセンスデータは保持されません。17.6.2 バージョンを使用し、HA システム全体でライセンストラストストアとライセンスレベルの構成を保持することを推奨します。
- このリリース以降、事前ダウンロードされる AP イメージは、イメージタイプではなく AP モデルをベースとします。事前ダウンロードは、モデルが新しい機能 XML ファイルに存在する場合にのみ許可されます。また、機能 XML を適切に変更することで、コントローラは特定のモデルに対する既存の AP イメージをオーバーライドできます。

インタラクティブヘルプ

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の GUI には、GUI 全体を順を追って説明し、複雑な設定をガイドするインタラクティブヘルプがあります。

次の方法でインタラクティブヘルプを開始できます。

- GUI のウィンドウの右隅にある青いフラップの上にカーソルを置き、[Interactive Help] をクリックします。
- GUI のウィンドウの左ペインで [Walk-me Thru] をクリックします。
- GUI に表示される [Show me How] をクリックします。[Show me How] をクリックすると、現在のコンテキストに関連する具体的なインタラクティブヘルプが表示されます。

  たとえば、[Configure] > [AAA] の [Show me How] をクリックすると、RADIUS サーバーを設定するための各手順の説明が表示されます。[Configuration] > [Wireless Setup] > [Advanced] の順に選択し、[Show me How] をクリックすると、さまざまな種類の認証に関連する手順を説明するインタラクティブヘルプがトリガーされます。

次の機能には、インタラクティブヘルプが関連付けられています。

- AAA の設定

- FlexConnect 認証の設定
- 802.1X 認証の設定
- ローカル Web 認証の設定
- OpenRoaming の設定
- メッシュ AP の設定

（注） Safari で WalkMe ランチャーが使用できない場合は、次のように設定を変更します。

1. [Preferences] > [Privacy] の順に選択します。
2. [Website tracking] セクションで、[Prevent cross-site tracking] チェックボックスをオフにしてこのアクションを無効にします。
3. [Cookies and website data] セクションで、[Block all cookies] チェックボックスをオフにしてこのアクションを無効にします。

特記事項

- パブリック IP アドレスを 16.12.x から 17.x に移行するには、**service internal** コマンドを必ず設定してください。**service internal** コマンドを設定しなければ、IP アドレスは引き継がれません。

サポート対象ハードウェア

次の表に、サポートされている仮想プラットフォームおよびハードウェア プラットフォームを示します。（サポートされているモジュールのリストについては、「表 5 : サポートされている PID およびポート」を参照してください）。

表 *3 :* サポートされている仮想プラットフォームおよびハードウェア プラットフォーム

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレスコントローラ	最大 100 GE のモジュールアップリンクおよびシームレスなソフトウェアアップデートを備えたモジュール型ワイヤレスコントローラ。 コントローラは 2 ラックユニットスペースを占有し、複数のモジュールアップリンクをサポートします。

プラットフォーム	説明
Cisco Catalyst 9800-40 ワイヤレスコントローラ	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。 コントローラは1ラックユニットスペースを占有し、4つの1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-L ワイヤレスコントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、パフォーマンスと機能を大幅に向上させる、最初のローエンド コントローラです。
クラウド向け Cisco Catalyst 9800 ワイヤレスコントローラ	Catalyst 9800 ワイヤレスコントローラの仮想フォームファクタは、エンタープライズ ネットワーク コンピューティング システム（ENCS）ハイパーバイザ上の VMware ESXi、カーネルベース仮想マシン（KVM）、Microsoft Hyper-V、Cisco Enterprise NFV インフラストラクチャ ソフトウェア（NFVIS）をサポートするプライベートクラウドに展開することも、Amazon Web Services（AWS）、Google Cloud Platform（GCP）マーケットプレイス、Microsoft Azure 内のパブリッククラウドに Infrastructure as a Service（IaaS）として展開することもできます。
スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Cisco Catalyst 9000 スイッチ用 Catalyst 9800 ワイヤレス コントローラ ソフトウェアは、有線およびワイヤレス インフラストラクチャを一貫性のあるポリシーおよび管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションであるソフトウェア定義型アクセス（SDA）のみをサポートします。

次の表に、プライベートクラウドとパブリッククラウドでサポートされているホスト環境を示します。

表 *4:* パブリッククラウドとプライベートクラウドでサポートされているホスト環境

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0、6.5、6.7 および 7.0 • VMware ESXi vCenter 6.0、6.5、6.7 および 7.0
KVM	• Red Hat Enterprise Linux 7.6、7.8、および 8.2 をベースとした Linux KVM • Ubuntu 16.04.5 LTS、Ubuntu 18.04.5 LTS、Ubuntu 20.04.5 LTS

ホスト環境	ソフトウェア バージョン
AWS	AWS EC2 プラットフォーム
NFVIS	ENCS 3.8.1 および 3.9.1
GCP	GCP マーケットプレイス
Microsoft Hyper-V	Windows 2019 Server および Windows Server 2016（バージョン 1607）と Hyper-V マネージャ（バージョン 10.0.14393）
Microsoft Azure	Microsoft Azure

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのサポートされているハードウェアモデルを示します。

ベース PID は、コントローラのモデル番号です。

バンドルされた PID は、特定のネットワークモジュールにバンドルされているベース PID のオーダー可能な製品番号を示しています。このようなコントローラ（バンドルPID）で、**show version**、**show module** または **show inventory** コマンドを実行すると、ベース PID が表示されます。

サポートされていない SFP はポートをダウンさせることに注意してください。C9800-80-K9 および C9800-40-K9 のルートプロセッサ（RP）ポートでは、シスコがサポートする SFP（GLC-LH-SMD および GLC-SX-MMD）のみを使用する必要があります。

表 *5 :* サポートされている *PID* およびポート

コントローラ モデル	説明
C9800-CL-K9	クラウド向けインフラストラクチャとしての Cisco Catalyst ワイヤレスコントローラ。
C9800-80-K9	1/10 ギガビットイーサネット SFP または SFP+ ポート（8 個）、電源スロット（2 個） 次の SFP がサポートされています。 • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

コントローラ モデル	説明
	次の拡張 SFP がサポートされています。 • 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

コントローラ モデル	説明
	次の QSFP+ がサポートされています。 • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	1/10 ギガビットイーサネット SFP または SFP+ ポート（4 個）、電源スロット（2 個）。 次の SFP がサポートされています。 • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE

コントローラ モデル	説明
	次の拡張 SFP がサポートされています。 • 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

コントローラ モデル	説明
C9800-L-C-K9	• 2.5/2 ギガビット ポート x 4 • 10/5/2.5/1 ギガビット ポート x 2 次の SFP がサポートされています。 • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • GLC-T
C9800-L-F-K9	• 2.5/2 ギガビット ポート x 4 • 10/1 ギガビット ポート x 2 次の SFP がサポートされています。 • GLC-BX-D • GLC-BX-U • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • SFP-10G-LR • SFP-10G-LR-S • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X

次の表に、サポートされる SFP モデルを示します。

光モジュール

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、さまざまなオプティカルモジュールをサポートしています。サポートされる光モジュールのリストは、定期的に更新されます。最新のトランシーバ モジュールの互換性情報については、次の場所にある表を参照してください。

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

サポート対象の AP

このリリースでは、次のシスコ AP がサポートされます。

屋内用アクセスポイント

- Cisco Catalyst 9105AX（I）アクセスポイント
  - VID 04 以降 - 17.6.4 以降でサポート
  - VID 03 以前
- Cisco Catalyst 9105AX（W）アクセスポイント
  - VID 02 以降 - 17.6.4 以降でサポート
  - VID 01 以前
- Cisco Catalyst 9115AX（I/E）アクセスポイント
- Cisco Catalyst 9117AX（I）アクセスポイント
- Cisco Catalyst 9120AX（I/E）アクセスポイント
  - VID 07 以降 - 17.6.4 以降でサポート
  - VID 06 以前
- Cisco Catalyst 9120AX（P）アクセスポイント
- Cisco Catalyst 9130AX（I/E）アクセスポイント
  - VID 03 以降 - 17.6.4 以降でサポート
  - VID 02 以前

  Cisco Catalyst 9105、9120、または 9130 アクセスポイントのバージョンサポートについては、「Field Notice 72424」を参照してください。
- Cisco Catalyst 9136 アクセスポイント
- Cisco Aironet 1815（I/W）、1830（I）、1840（I）、1852（I/E）アクセスポイント
- Cisco Aironet 2800（I/E）シリーズ アクセスポイント

- Cisco Aironet 3800（I/E/P）シリーズ アクセスポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco Catalyst 9120AXP アクセスポイント：16.12.2s 以降でサポート

屋外用アクセスポイント

- Cisco Aironet 1540 シリーズ アクセス ポイント
- Cisco Aironet 1560 シリーズ アクセス ポイント
- Cisco Industrial Wireless 3700 シリーズ アクセスポイント
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty シリーズ アクセスポイント
- Cisco 6300 シリーズ組み込みサービスアクセスポイント
- Cisco Catalyst 9124AX（I/D）アクセスポイント

統合アクセスポイント

- Cisco 1100 ISR の統合アクセスポイント（ISR-AP1100AC-x、ISR-AP1101AC-x、および ISR-AP1101AX-x）

ネットワーク センサー

- Cisco Aironet 1800s アクティブ センサー

プラガブルモジュール

- 産業用ルータ向け Wi-Fi 6 着脱可能モジュール

サポートされているアクセスポイントチャネルと最大電力設定

Cisco AP でサポートされているアクセスポイントチャネルと最大電力設定は、アクセスポイントが販売されているすべての国のチャネル、最大電力レベル、およびアンテナゲインの規制仕様に準拠しています。Cisco IOS XE ソフトウェアリリースでサポートされているアクセスポイントの伝送値の詳細については、https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-technical-reference-list.html にある『*Detailed Channels and Maximum Power Settings*』ドキュメントを参照してください。

特定の Cisco AP モジュールをサポートしている Cisco Wireless ソフトウェア リリースの詳細については、『Cisco Wireless Solutions Software Compatibility Matrix』ドキュメントの「Software Release Support for Specific Access Point Modules」のセクションを参照してください。

互換性マトリックス

次の表に、ソフトウェア互換性情報を示します。

表 *6:* 互換性に関する情報

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM の相互運用性	Cisco DNA Center	Cisco DNA Spaces - コネクタ	Cisco DNA Spaces - オンプレミス
Cupertino 17.7.x	3.0 2.7 2.6 2.4	3.10 MR1 3.10 3.9	8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104 8.5.152.103 8.5.164.216	Cisco DNA Center の互換性情報を参照	2.3.1 2.3 2.2	10.6.3

GUI システム要件

次のサブセクションには、Cisco Catalyst 9800 コントローラ GUI にアクセスするために必要なハードウェアとソフトウェアがリストされています。

表 *7:* ハードウェア要件

プロセッサ速度	DRAM	色数	解像度	フォント サイズ
233 MHz 以上[1]	512 MB[2]	256	1280 x 800 以上	小

[1] 1 GHz を推奨
[2] 1 GB DRAM を推奨

ソフトウェア要件

オペレーティング システム：

- Windows 7 以降
- Mac OS X 10.11 以降

ブラウザ：

- Google Chrome：バージョン 59 以降（Windows および Mac）
- Microsoft Edge：バージョン 40 以降（Windows）
- Safari：バージョン 10 以降（Mac）
- Mozilla Firefox：バージョン 60 以降（Windows および Mac）

（注） Firefox バージョン 63.x はサポートされていません。

コントローラ GUI は、HTTP 要求の処理に仮想端末（VTY）回線を使用します。複数の接続が開いていると、デバイスによって設定されたデフォルトの VTY 回線数である 15 が使い果たされることがあります。したがって、VTY 回線の数を 50 に増やすことを推奨します。

デバイスの VTY 回線を増やすには、次の順序でコマンドを実行します。

1. **device#** configure terminal
2. **device(config)#** line vty 50

   ベストプラクティスは、service tcp-keepalives を設定して、デバイスへの TCP 接続を監視することです。
3. **device(config)#** service tcp-keepalives-in
4. **device(config)#** service tcp-keepalives-out

アップグレードする前に

アップグレードを始める前に、次の点をよく理解してください。

注意 コントローラのアップグレードまたはリブート中に、ルートプロセッサポートがいずれかのシスコ製スイッチに接続されている場合は、ルートプロセッサポートがフラッピング（shut/no shut プロセス）していないことを確認してください。フラッピングしていると、カーネルがクラッシュする可能性があります。

- ISSU 機能は、メジャーリリース内およびメジャーリリース間でのみサポートされます。たとえば、17.3.x（単一リリース内）および 17.3.x から17.6.x（メジャーリリース間）です。
- **domain** コマンドが設定されている場合、ISSU を使用して Cisco IOS XE Bengaluru 17.3.x から Cisco IOS XE Bengaluru 17.6.x または Cisco IOS XE Cupertino 17.9.x 以降にコントローラをアップグレードすると、エラーが発生することがあります。Cisco IOS XE Bengaluru 17.6.x 以降では **domain** コマンドが削除されているため、ISSU によるアップグレードを開始する前に必ず **no domain** コマンドを実行してください。
- ISSU を使用して Cisco IOS XE Bengaluru 17.3.x から任意のリリースにアップグレードする場合、**snmp-server enable traps hsrp** コマンドが設定されているとアップグレードに失敗することがあります。ISSU アップグレードを開始する前に、設定から **snmp-server enable traps hsrp** コマンドを必ず削除してください。これは、Cisco IOS XE Bengaluru 17.4.x 以降で **snmp-server enable traps hsrp** コマンドが 削除されているためです。
- ISSU 機能の一部であるローリング AP アップグレードは、メッシュ AP ではサポートされません。

次の Wave 1 AP は、17.4 ～ 17.9.2、17.10.x および 17.11.x ではサポートされません。

- **Cisco Aironet 1570 シリーズ アクセスポイント**
- **Cisco Aironet 1700 シリーズ アクセスポイント**
- **Cisco Aironet 2700 シリーズ アクセス ポイント**
- **Cisco Aironet 3700 シリーズ アクセスポイント**

（注）
- 上記の AP のサポートは、Cisco IOS XE Cupertino 17.9.3 から再導入されました。
- これらの AP のサポートが通常の製品ライフサイクルサポートを超えることはありません。個々のサポート終了のお知らせを参照してください。
- 機能のサポートは、17.3.x リリースと同等です。17.4.1 以降で導入された機能は、17.9.3 リリースのこれらの AP ではサポートされていません。
- 17.3.x から 17.9.3（x=4c 以上）には直接移行できます。

- **archive download-sw** コマンドの実行後に AP がバックアップイメージを検出できない場合は、次の手順を実行します。

1. **archive download-sw** コマンドの **no-reload** オプションを使用してイメージをアップロードします。

```
Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
```

2. **capwap ap restart** コマンドを使用して CAPWAP プロセスを再起動します。これにより、再起動後に AP が正しいバックアップイメージを使用できるようになります（リロードは必要ありません）。

```
Device# capwap ap restart
```

（注） AP は、参加プロセス中にコントローラへの接続を失います。AP が新しいコントローラに参加すると、バックアップパーティションに新しいイメージが表示されます。したがって、AP はコントローラから新しいイメージをダウンロードしません。

- NETCONF データストアと Cisco IOS 設定の間で完全な同期が発生すると、高い Confd CPU が観察されることがあります。この動作は正常であり、**line vty** コマンドによってトリガーされます。
- Cisco IOS XE Cupertino 17.7.1 以降、Cisco Catalyst 9800-CL ワイヤレスコントローラでは、リソース使用率測定（RUM）レポートを完了し、製品インスタンスで ACK が少なくとも 1 回利用できるようにする必要があります。これは、正しい最新の使用状況情報が Cisco Smart Software Manager（CSSM）に反映されるようにするためです。
- Cisco IOS XE Amsterdam 17.3.1 以降、新規導入時は Cisco Catalyst 9800-CL ワイヤレスコントローラに 16 GB のディスク容量が必要となります。

  以前のリリースから Cisco IOS XE Amsterdam 17.3.x にアップグレードしている場合、ディスク容量のサイズ変更はサポートされません。現在のディスク容量が 16 GB 未満の場合は、新しいディスク容量の要件を満たすように VM を再展開する必要があります。
- 1500 未満のフラグメンテーションは、Gi0（OOB）インターフェイスのワイヤレスクライアントによって生成された RADIUS パケットではサポートされません。
- Cisco IOS XE では、機器で使用されるすべてのパスワードを暗号化できます。これには、ユーザーパスワードと SSID パスワード（PSK）が含まれます。詳細については、『Cisco Catalyst 9800 Series Configuration Best Practices』の「Password Encryption」に関する項を参照してください。
- Cisco IOS XE 17.3.x 以降のリリースにアップグレードする場合、**ip http active-session-modules none** コマンドが有効になっていると、HTTPS を使用してコントローラの GUI にアクセスできません。HTTPS を使用して GUI にアクセスするには、次の順序でコマンドを実行します。

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend アクセスポイントは、コントローラに接続するとローカルモードになります。ただし、スタンドアロン AP として機能する場合は、FlexConnect モードに変換されます。

- Cisco Catalyst 9800-L ワイヤレスコントローラは、ブート時にコンソールポートで受信した BREAK 信号に応答できず、ユーザーが ROMMON にアクセスできなくなる場合があります。この問題は、デフォルトの config-register 設定が 0x2102 の、2019 年 11 月までに製造されたコントローラで発生します。この問題は、config-register を 0x2002 に設定すると回避できます。この問題は、Cisco Catalyst 9800-L ワイヤレスコントローラの 16.12(3r)ROMMON で修正されています。ROMMON のアップグレード方法については、『Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers』ドキュメントの「Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers」のセクションを参照してください。
- デフォルトでは、コントローラは TFTP ブロック サイズの最小許容値である 512 を使用します。このデフォルト設定は、レガシー TFTP サーバーとの相互運用性を確保するために使用されます。必要に応じてグローバル コンフィギュレーション モードで **ip tftp blocksize** コマンドを使用して、ブロックサイズの値を 8192 に変更し、転送プロセスを高速化することができます。
- **password encryption aes** および **the key config-key password-encrypt** *key* コマンドを設定して、パスワードを暗号化することを推奨します。
- 再起動またはシステムクラッシュの後に次のエラーメッセージが表示された場合は、トラストポイント証明書を再生成することを推奨します。

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  次の順序でコマンドを実行して、新しい自己署名トラストポイント証明書を生成します。

  1. **device#** configure terminal
  2. **device(config)#** no crypto pki trustpoint *trustpoint_name*
  3. **device(config)#** no ip http server
  4. **device(config)#** no ip http secure-server
  5. **device(config)#** ip http server
  6. **device(config)#** ip http secure-server
  7. **device(config)#** ip http authentication *local/aaa*

- OVA ファイルを VMware ESXi 6.5 に直接展開しないでください。OVF ツールを使用して OVA ファイルを展開することをお勧めします。
- Netconf-YANG を無効または有効にする前に、Cisco Prime Infrastructure からコントローラを必ず削除してください。そうしないと、システムが予期せずリロードする可能性があります。
- 単一方向リンク検出（UDLD）プロトコルはサポートされていません。
- SIP メディア セッション スヌーピングは、FlexConnect ローカルスイッチング展開ではサポートされません。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（C9800-CL、C9800-L、C9800-40、および C9800-80）は、内部 DHCP スコープで最大 14,000 のリースをサポートします。
- **wireless mobility mac-address** コマンドを使用したモビリティ MAC アドレスの設定は、HA と 802.11r の両方で必須です。
- ネットワーク上の Cisco Catalyst 9120 (E/I/P) および Cisco Catalyst 9130 (E) の AP をダウングレードする場合は、Cisco IOS XE Gibraltar 16.12.1t のみを使用してください。Cisco IOS XE Gibraltar 16.12.1s にダウングレードしないでください。
- 次の SNMP 変数はサポートされていません。
  - CISCO-LWAPP-WLAN-MIB：cLWlanMdnsMode
  - CISCO-LWAPP-AP-MIB.my：cLApDot11IfRptncPresent、cLApDot11IfDartPresent
- Cisco IOS XE Gibraltar 16.11.x 以前のリリースからアップグレードする場合は、アップグレード前に **no license boot level advipservices** コマンドを使用して、アクティブコントローラとスタンバイコントローラの両方で advipservices ブートレベルライセンスを設定解除してください。**license boot level advipservices** コマンドは、Cisco IOS XE Gibraltar 16.12.1s および 16.12.2s では使用できないことに注意してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラには、GigabitEthernet 0 ポートと呼ばれるサービスポートがあります。

  このポートでは、次のプロトコルと機能がサポートされています。
  - Cisco DNA Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - コントローラの GUI
  - DNS
  - ファイル転送
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - CSSM と通信するスマートライセンス機能のライセンス
  - Netconf
  - NetFlow
  - NTP

- RADIUS（CoA を含む）
- Restconf
- SNMP
- SSH
- SYSLOG
- TACACS+

- GUI を使用したデバイスのアップグレード中にスイッチオーバーが発生すると、セッションが期限切れになり、アップグレードプロセスが終了します。これにより、GUI でアップグレードの状態またはステータスを表示できなくなります。
- Cisco IOS XE Bengaluru 17.4.1 以降、テレメトリソリューションでは、テレメトリデータの IP アドレスではなく、受信者アドレスの名前が提供されます。これは追加のオプションです。コントローラのダウングレードおよびその後のアップグレード中に問題が発生する可能性があります。アップグレードバージョンでは、新しく指定された受信者が使用されますが、これらはダウングレードでは認識されません。新しい設定は拒否され、後続のアップグレードで失敗します。Cisco DNA Center からアップグレードまたはダウングレードを実行すると、設定の損失を回避できます。
- Cisco IOS XE Bengaluru 17.4.1 以降では、ポリシープロファイルでのセッションタイムアウトがサポートされています。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco Prime Infrastructure 間の通信では、以下に示すように複数のポートが使用されます。
  - Cisco Prime Infrastructure で使用可能なすべての構成とテンプレートは、UDP ポート 161 を使用して SNMP および CLI 経由でプッシュされます。
  - コントローラの運用データは、UDP ポート 162 を使用してSNMP 経由で取得されます。
  - AP およびクライアントの運用データは、ストリーミングテレメトリを活用します。
    - Cisco Prime Infrastructure からコントローラへ：Cisco Prime Infrastructure は、TCP ポート 830 を使用してコントローラにテレメトリ設定をプッシュします（NETCONF を使用）。
    - コントローラから Cisco Prime Infrastructure へ：Cisco IOS-XE 16.10.x および 16.11.x では TCP ポート 20828 が使用され、Cisco IOS-XE 16.12.x、17.1.x、およびそれ以降のリリースでは TCP ポート 20830 が使用されます。
- パブリック IP アドレスを 16.12.x から 17.x に移行するには、**service internal** コマンドを必ず設定してください。**service internal** コマンドを設定しなければ、IP アドレスは引き継がれません。
- SNMP エラー「SNMP_ERRORSTATUS_NOACCESS 6」が発生した場合は、指定した SNMP 変数にアクセスできないことを意味します。

Cisco IOS XE Cupertino 17.7.x へのアップグレードパス

表 *8 : Cisco IOS XE Cupertino 17.7.x* へのアップグレードパス

現在のソフトウェア	9130 または 9124 を使用した展開のアップグレード パス	9130 または 9124 を使用しない展開のアップグレード パス
16.10.x	—	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
16.11.x	—	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
16.12.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	17.7.x に直接アップグレードできます。
17.1.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
17.2.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
17.3.1 ～ 17.3.4	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	17.7.x に直接アップグレードできます。
17.3.4c 以降	17.7.x に直接アップグレードできます。	17.7.x に直接アップグレードできます。
17.4.x	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。
17.5.x	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。
17.6.x	17.7.x に直接アップグレードできます。	17.7.x に直接アップグレードできます。

Cisco IOS XE Cupertino 17.7.x へのアップグレードパス

表 *9 : Cisco IOS XE Cupertino 17.7.x* へのアップグレードパス

現在のソフトウェア	**9130** または **9124** を使用した展開のアップグレード パス	**9130** または **9124** を使用しない展開のアップグレードパス
16.10.x	—	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
16.11.x	—	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
16.12.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	17.7.x に直接アップグレードします。
17.1.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
17.2.x	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.3.x にアップグレードしてから、17.7.x にアップグレードします。
17.3.1 ～ 17.3.4	最初に 17.3.4c 以降にアップグレードしてから、17.7.x にアップグレードします。	17.7.x に直接アップグレードします。
17.3.4c 以降	17.7.x に直接アップグレードします。	17.7.x に直接アップグレードします。
17.4.x	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。
17.5.x	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。	最初に 17.6.x にアップグレードしてから、17.7.x にアップグレードします。
17.6.x	最初に 17.3.5 にアップグレードしてから、17.7.x にアップグレードします。	17.7.x に直接アップグレードします。

コントローラ ソフトウェアのアップグレード

このセクションでは、コントローラ ソフトウェアのアップグレードに関するさまざまな側面について説明します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアのアップグレードプロセスとアップグレード方法については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』[英語] の「Upgrade the Cisco Catalyst 9800 Wireless Controller Software」の章を参照してください。

ソフトウェア バージョンの確認

Cisco IOS XE ソフトウェアのパッケージファイルは、システムボードのフラッシュデバイス（flash:）に保存されます。

show version 特権 EXEC コマンドを使用すると、コントローラで稼働しているソフトウェアバージョンを確認できます。

（注） **show version** の出力にはコントローラで実行されているソフトウェアイメージが常に表示されますが、この出力の最後に示されているモデル名は、工場出荷時の設定であり、ソフトウェアライセンスをアップグレードしても変更されません。

アクティブなパッケージに関する情報を表示するには、**show install summary** 特権 EXEC コマンドを使用します。

フラッシュメモリに保存している他のソフトウェアイメージのディレクトリ名を表示するには、**dir** *filesystem:* 特権 EXEC コマンドを使用します。

ソフトウェア イメージ

- リリース：Cisco IOS XE Cupertino 17.7.x
- イメージ名（**9800-80、9800-40、および9800-L**）：
  - C9800-80-universalk9_wlc.17.07.01.SPA.bin
  - C9800-40-universalk9_wlc.17.07.01.SPA.bin
  - C9800-L-universalk9_wlc.17.07.01.SPA.bin
- イメージ名（**9800-CL**）：
  - クラウド：C9800-CL-universalk9.17.07.01.SPA.bin
  - **Hyper-V/ESXi/KVM**：C9800-CL-universalk9.17.07.01.iso、C9800-CL-universalk9.17.07.01.ova
  - **KVM**：C9800-CL-universalk9.17.07.01.qcow2

- **NFVIS**：C9800-CL-universalk9.17.07.01.tar.gz

ソフトウェア インストール コマンド

Cisco IOS XE Cupertino 17.7.x	
指定したファイルをインストールしてアクティブ化し、リロード後も維持されるように変更をコミットするには、次のコマンドを実行します。 **device# install add file** *filename* **[activate |commit]** インストールファイルを個別にインストール、アクティブ化、コミット、終了、または削除するには、次のコマンドを実行します。 **device# install ?** （注） インストールには GUI を使用することを推奨します。	
add file tftp: *filename*	インストール ファイル パッケージをリモート ロケーションからデバイスにコピーし、プラットフォームとイメージのバージョンの互換性チェックを実行します。
activateauto-abort-timer］	ファイルをアクティブ化し、デバイスをリロードします。**auto-abort-timer** キーワードがイメージのアクティブ化を自動的にロールバックします。
commit	リロード後も変更が持続されるようにします。
rollback to committed	最後にコミットしたバージョンに更新をロールバックします。
abort	ファイルのアクティブ化を中止し、現在のインストール手順の開始前に実行していたバージョンにロールバックします。
remove	未使用および非アクティブ状態のソフトウェアインストール ファイルを削除します。

ライセンス

ポリシーを使用したスマートライセンス機能は、コントローラで自動的に有効になります。これは、このリリースにアップグレードする場合にも当てはまります。デフォルトでは、Cisco Smart Software Manage（CSSM）のスマートアカウントとバーチャルアカウントは、ポリシーを使用したスマートライセンスで有効になっています。詳細については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』の「Smart Licensing Using Policy」の章を参照してください。

（注） Cisco IOS XE Cupertino 17.7.1 以降、スマートライセンスが接続されていない場合、Cisco Catalyst 9800-CL ワイヤレスコントローラは 50 を超える AP を受け入れません。

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

クライアントとの相互運用性

このセクションでは、コントローラ ソフトウェアとクライアント デバイスとの相互運用性について説明します。

次の表に、クライアントデバイスのテストに使用される設定を示します。

表 *10*：相互運用性のテスト設定

ハードウェアまたはソフトウェア パラメータ	ハードウェアまたはソフトウェア タイプ
リリース	Cisco IOS XE Cupertino 17.7.x
シスコ ワイヤレス コントローラ	サポート対象ハードウェアを参照してください。
アクセスポイント	サポート対象の AP を参照してください。
無線機	• 802.11 ax • 802.11ac • 802.11a • 802.11g • 802.11n
セキュリティ	オープン、PSK（WPA2-AES）、802.1X（WPA2-AES）（EAP-FAST、EAP-TLS） 802.11 ax
RADIUS	互換性マトリックス （22 ページ） を参照してください
テストのタイプ	2 つの AP 間の接続、トラフィック（ICMP）、およびローミング

次の表に、テストが実施されたクライアント タイプを示します。クライアント タイプには、ラップトップ、ハンドヘルド デバイス、電話機、プリンタが含まれます。

表 *11 :* クライアント タイプ

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
ラップトップ	
Acer Aspire E 15 E5-573-3870（Qualcomm Atheros QCA9377）	Windows 10 Pro（12.0.0.832）
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Catalina
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Macbook Pro OS X	OS X 10.8.5
MacBook Air	OS Sierra v10.12.2
Macbook Air 11 inch	OS X Yosemite 10.10.5
MacBook M1 チップ	OS Catalina
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude（Intel AX210）	Windows 11（22.110.xx）
Dell Latitude 3480（Qualcomm DELL wireless 1820）	Win 10 Pro（12.0.0.242）
Dell Inspiron 15-7569（Intel Dual Band Wireless-AC 3165）	Windows 10 Home（21.40.0）
Dell Latitude E5540（Intel Dual Band Wireless AC7260）	Windows 7 Professional（21.10.1）
Dell Latitude E5430（Intel Centrino Advanced-N 6205）	Windows 7 Professional（15.17.0.1）
Dell Latitude E6840（Broadcom Dell Wireless 1540 802.11 a/g/n）	Windows 7 Professional（6.30.223.215）
Dell XPS 12 v9250（Intel Dual Band Wireless AC 8260）	Windows 10 Home（21.40.0）
Dell Latitude 5491（Intel AX200）	Windows 10 Pro（21.20.1.1）
Dell XPS Latitude12 9250（Intel Dual Band Wireless AC 8260）	Windows 10 Home

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home（18.40.0.12）
FUJITSU Lifebook E556 Intel 8260（Intel Dual Band Wireless-AC 8260（802.11n））	Windows 8（19.50.1.6）
Lenovo Yoga C630 Snapdragon 850（Qualcomm AC 2x2 Svc）	Windows 10 Home
Lenovo Thinkpad Yoga 460（Intel Dual Band Wireless-AC 9260）	Windows 10 Pro（21.40.0）
（注） Intel 無線カードを使用しているクライアントの場合、アドバタイズされた SSID が表示されない場合は、最新の Intel ワイヤレスドライバに更新することをお勧めします。	
タブレット	
Apple iPad 2021	iOS 15.0
Apple iPad 第 7 世代 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 インチ（Intel AX201）	Windows 10（21.40.1.3）
Microsoft Surface Pro 3 15 インチ（Qualcomm Atheros QCA61x4A）	Windows 10
Microsoft Surface Pro 7（Intel AX201）	Windows 10
Microsoft Surface Pro 6（Marvell Wi-Fi チップセット 11ac）	Windows 10
Microsoft Surface Pro X（WCN3998 Wi-Fi チップ）	Windows
携帯電話	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
Apple iPhone 8	iOS 13.5
Apple iPhone 8 plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 15.1
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Pro	iOS 15.1
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP 電話 8821	11.0.6 SR1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2（1.2.6）
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10（SM-G973U1）	Android 11.0
Samsung S10e（SM-G970U1）	Android 11.0
Samsung S20 Ultra	Android 10.0
Samsung S21 Ultra 5G	Android 11.0
Samsung Fold 2	Android 10.0
Samsung Note20	Android 10.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 シリーズ	7.5.0.x257
Spectralink 87 シリーズ	Android 5.1.1
Spectralink Versity Phones 92/95/96 シリーズ	Android 10.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM バージョン 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
Zebra TC57	Android 10.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC8000	Android 4.4.3
プリンタ	
Zebra QLn320 モバイルプリンタ	LINK OS 6.4
Zebra ZT230 産業用プリンタ	LINK OS 6.4
Zebra ZQ310 モバイルプリンタ	LINK OS 6.4
Zebra ZD410 産業用プリンタ	LINK OS 6.4
Zebra ZT410 デスクトッププリンタ	LINK OS 6.4
Zebra ZQ610 産業用プリンタ	LINK OS 6.4
Zebra ZQ620 モバイルプリンタ	LINK OS 6.4
ワイヤレスモジュール	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Intel AX 210	Driver v22.110.x.x 以降
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901

不具合

ここでは、製品における Cisco IOS リリースでの予期しない動作について説明します。以前のリリースで未解決になっている警告は、未解決または解決済みとして次のリリースに引き継がれます。

（注） すべての増分リリースには、現在のリリースからの修正が含まれます。

Cisco Bug Search Tool

Cisco Bug Search Tool（BST）を使用すると、パートナーとお客様は製品、リリース、キーワードに基づいてソフトウェアバグを検索し、バグ詳細、製品、バージョンなどの主要データを集約することができます。BST は、ネットワーク リスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。このツールでは、クレデンシャルに基づいてバグをフィルタし、検索入力に関する外部および内部のバグ ビューを提供することもできます。

警告の詳細を表示するには、対応する ID をクリックします。

Cisco IOS XE Cupertino 17.7.1 の未解決の不具合

警告 ID	説明
CSCvz89115	Flexconnect AP は、802.1x 暗号化を使用した VLAN の変更による認可変更（CoA）の後で DHCP パケットを転送しない。
CSCvz94692	無線障害が原因で AP がクラッシュする（無線障害が多すぎる）。
CSCwa01168	mobilityd クラッシュが原因でコントローラが予期せずリロードされる。
CSCwa12278	カーネルパニックが原因で Cisco Catalyst 9115 AP がクラッシュする。
CSCwa13091	無線リソース管理（RRM）：Tx 電力の変更が AP に適用されない。
CSCwa14307	カーネルパニックが原因で AP がクラッシュする。
CSCvz82490	スイート B：誤った TLS 認証パラメータテストを使用した STA への APUT 応答が正しくない。
CSCwa23783	IOS-XE ベースの RLAN 対応 AP が、AireOS または Cisco Catalyst 9800 コントローラに接続できない。

Cisco IOS XE Cupertino 17.7.1 の解決済みの不具合

警告 ID	説明
CSCvv94885	**show ap cdp neighbors** コマンドで、ドメイン名ではなくスイッチ名が表示されます。

警告 ID	説明
CSCvx71141	無線リソース管理（RRM）プロセスでのCPU使用率の上昇が原因で、Cisco Catalyst 9800-80 ワイヤレスコントローラがクラッシュする。
CSCvx78215	IOS XE デバイスが、DoubleExceptionVector でクラッシュする可能性がある。
CSCvx81815	Datagram Transport Layer Security（DTLS）暗号化を有効にすると、コントローラがサーバーの hello パケットを AP に送信しない。
CSCvy01360	Cisco Catalyst 9115AX AP が、チャネル 100 ー 112 での誤ったレーダー検出を報告する。
CSCvy02120	Cisco Catalyst 9130AX AP が、再関連付け応答をローミングクライアントに送信できず、クライアントを削除する。
CSCvy05019	**show platform software system all** コマンドの出力で、10 を超えるインターフェイスが表示されない。
CSCvy11011	コントローラに、EVENTLIB-3-CPUHOG - ewlc_client_location - remove_weakest_radio_measurement のようなトレースバックが表示される。
CSCvy11394	コントローラのL2 ポートチャネルでネットフローを構成できる。
CSCvy11981	AP名が31文字を超えると、コントローラが予期せずリロードする。
CSCvy14956	クライアント SVI インターフェイスがシャットダウンされている場合でも、コントローラがリレープロキシとして DHCP を送信します。
CSCvy25684	CLIおよびRF プロファイルで、異なるデータ レートが観察されます。
CSCvy36744	コントローラがクライアントへのブロードキャストの転送を断続的に停止する。
CSCvy46043	l2_socket_counter レコードへのスイッチ統合セキュリティ機能（SISF）ヒープポインタに対して、コントローラが予期せずリロードする。
CSCvy58934	フィルタが適用されて AP 名が変更された場合に、コントローラが CAPWAP 再起動ペイロードを送信しない。

警告 ID	説明
CSCvy72750	**wireless broadcast vlan X** コマンドを使用できない。
CSCvy73836	Cisco Catalyst 9800-80 コントローラが、電源の再投入による複数回のフェールオーバー後に ROMMON に移行します。
CSCvy74904	AP 認証関連の RADIUS 要求に、発信側ステーション ID と NAS ポートタイプが含まれません。
CSCvy76922	Cisco IOS XE 17.3.2a のスイッチスタックが、ハイメモリアラートを表示します。
CSCvy87749	クライアント SVI インターフェイスから IP ヘルパーを削除した後も、コントローラがリレープロキシとして DHCP を送信する。
CSCvy89423	セグメンテーション障害が原因で、WNCMGRD プロセスがクラッシュする。
CSCvy89508	スタンバイがリカバリモードであっても、プライマリメンバーには「スタンバイホット」と表示されます。
CSCvy90646	コントローラは、ランダム AP の着信 CAPWAP キープアライブをドロップします。
CSCvy94284	**clear wlan id** コマンドを実行すると、コントローラがクラッシュする。
CSCvy99116	ワイヤレスクライアントが接続を試み、接続がタイムアウトすると、クラッシュが発生します。
CSCvz11154	FMAN データベースで、複数のテーブルエントリによる継続的なメモリリークが観察されます。
CSCvz14394	Web 認証パラメータマップのカスタムページが、リロード後に実行コンフィギュレーションにロードされない。
CSCvz15015	Cisco Catalyst 9130AX AP が、コントローラ間を移動すると WLAN 設定を失います。
CSCvz17623	エミュレートされたデータベースと AP 参加でメモリリークが観察されます。
CSCvz28378	17.3.3 を実行している WNCD プロセスで、1 日あたり約 200MB のメモリリークが発生する。
CSCvz39749	プローブ要求の解析が失敗すると、クライアントのロケーションプローブでエラーが表示されます。

警告 ID	説明
CSCvz45305	スリープ状態のクライアントに送信する場合に、コントローラにアクセス要求内のフィールドがありません。
CSCvz45488	OPERATIONAL_DB でメモリリークが発生し、dbm がクラッシュする。
CSCvz45576	コントローラが多くの不正レポートを Cisco DNAC に送信するため、不正テレメトリの更新を抑制する必要がある。
CSCvz51976	**show ap config general** コマンドの出力に AP イーサネット速度とデュプレックス情報が含まれている。
CSCvz52851	SSO スイッチオーバーが、CP への LISP セッションを再確立しません。
CSCvz53408	セッションタイムアウト後に、M3 で高速移行 IE が 0 として送信される。
CSCvz63742	フォレンジック Advanced Wireless Intrusion Prevention System（aWIPS）が設定されている場合、コントローラは SNMP を介して cLApAdminStatus 情報を提供しない。
CSCvz68857	パフォーマンスを向上させるには、bsnMobileData OID クエリを最適化します。
CSCvz77768	Cisco IOS AP は、non-DFS チャネルが使用可能な場合でも、動的周波数選択（DFS）イベントが発生すると無線を停止する。
CSCvz80697	新しいプローブが別のスロットで受信された場合、コントローラが古い NMSP エントリを削除しません。
CSCvz84691	クライアントの IP アドレスを学習するときに、WNCD プロセスが原因でコントローラがクラッシュします。
CSCvz89976	ワークグループブリッジ（WGB）が原因で、17.3.4 を実行しているコントローラがクラッシュする。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、次の URL にある Cisco TAC Web サイトを参照してください。

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html

[Product Support] に移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、[Troubleshoot and Alerts] を参照してください。

関連資料

Cisco IOS XE に関する情報は、次の URL から入手できます。

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

シスコ検証済みデザイン（CVD）のドキュメントは、次の URL から入手できます。

https://www.cisco.com/go/designzone

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

シスコ ワイヤレス コントローラ

シスコ ワイヤレス コントローラ、Lightweight AP、およびメッシュ AP の詳細については、次のドキュメントを参照してください。

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices

コントローラのインストールガイドは、次の URL から入手できます。

- Hardware Installation Guides

シスコ ワイヤレス コントローラ ソフトウェア関連のすべてのドキュメントについては、次を参照してください。

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Cisco Catalyst 9800 ワイヤレスコントローラ データシート

- Cisco Catalyst 9800-CL ワイヤレスコントローラ：https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-cloud-wirel-data-sheet-ctp-en.html
- Cisco Catalyst 9800-80 ワイヤレスコントローラ：https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-80-wirel-mod-data-sheet-ctp-en.html
- Cisco Catalyst 9800-40 ワイヤレスコントローラ：https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html

- Cisco Catalyst 9800-L ワイヤレスコントローラ：https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html

Cisco Embedded Wireless Controller on Catalyst Access Points

Cisco Embedded Wireless Controller on Catalyst Access Points の詳細については、次を参照してください。

https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/tsd-products-support-series-home.html

ワイヤレス製品の比較

- 次のツールを使用して、Cisco ワイヤレス AP とコントローラの仕様を比較します。

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- 無線 LAN コンプライアンス検索：

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

- Cisco AireOS と Cisco Catalyst 9800 ワイヤレスコントローラの機能比較マトリックス：

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AireOS_Cat_9800_Feature_Comparison_Matrix.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure マニュアル

Cisco Connected Mobile Experiances

Cisco Connected Mobile Experiences マニュアル

Cisco DNA Center

Cisco DNA Center マニュアル

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。

- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

【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。

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。