Cisco Catalyst 9800 シリーズワイヤレスコントローラ（Cisco IOS XE 26.1.x）リリースノート

目次

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 26.1.x	3
New software features	3
Change in behavior	7
Resolved issues	9
Open issues	15
Known issues	21
Compatibility	22
Supported hardware	36
Related content	47
Communications, services, and additional information:	48
Legal information	48

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、Cisco IOS XE 26.1.x

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。

コントローラは、次のように、さまざまな形式に対応しているため、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
  - Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ（C9800-L、C9800-40、C9800-80）
  - Cisco CW9800 シリーズ ワイヤレス コントローラ（CW9800L、CW9800M、CW9800H1、CW9800H2）
- クラウド向け Catalyst 9800 シリーズ ワイヤレス コントローラ
- Catalyst 9000 シリーズ スイッチに組み込まれた Embedded Wireless Controller（EWC）

このドキュメントでは、Cisco IOS XE 26.1.x で導入された、または強化された新しいソフトウェア機能、動作の変更、問題、サポート対象ハードウェアなどについて説明します。

新しいソフトウェア機能

このセクションでは、26.1.x リリースで導入された新しいソフトウェア機能について概説します。

表 1. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、リリース 26.1.2 の新しいソフトウェア機能

製品への影響	機能	説明
ソフトウェアの信頼性	MACsec フェールオーバーのメカニズム	このリリースでは、AP 有線アップリンクに対する自動 MACsec フェールオーバーが導入されています。AP が有効な MACsec ピアを検出できない場合、タイムアウト後にフォールバックしてコントローラの接続を維持します。複数のアップリンクを持つ AP では、該当するすべてのリンクで MACsec が失敗した場合にのみフォールバックが発生します。いずれかのアップリンクで MACsec が正常に確立されると、AP はそのリンク上でセキュアな動作を続行します。
	MACsec リプレイ保護ウィンドウのサポート	このリリースでは、設定可能なリプレイ保護ウィンドウが追加され、不適切なパケット配信にも安全に対応します。この設定では、パケットが潜在的なリプレイ攻撃と識別されてドロップされる前に、誤って到達する可能性のあるシーケンス番号の数が定義されます。

表 2. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.1 の新しいソフトウェア機能

製品への影響	機能	説明
ソフトウェアの信頼性	RMI を使用したスタンバイのモニタリング	この機能を使用すると、コントローラの高可用性セットアップで RMI インターフェイスのみがスタンバイコントローラ上で稼働し、他のすべてのインターフェイスは管理上ダウンします。ポリシープロファイルでレイヤ 3（L3）を有効にすると、アクティブコントローラは RMI サブネットをアドバタイズします。その結果、アクティブコントローラは、非 RMI サブネットからスタンバイコントローラ宛てのパケットを RMI インターフェイスを介してルーティングします。 スタンバイが RMI 送信元パケットを受信すると、RIB（ルーティング情報ベース）送信元パケットよりも優先され、RMI 送信元パケットに基づいて転送情報ベース（FIB）テーブルが更新されます。このように、スタンバイコントローラは、RMI インターフェイスでアクティブコントローラを介してすべての発信パケットをルーティングします。 L3 が有効になっている場合、ゲートウェイモニタリングは無効になります。この機能では、新しい CLI コマンドは導入されていません。

© 2026 Cisco and/or its affiliates. All rights reserved.

製品への影響	機能	説明
	アクセスポイントでの MACsec のサポート	このリリースでは、AP に MACsec サポートが導入され、AP と接続されたスイッチの間で送信されるデータのレイヤ 2 ホップバイホップ暗号化と整合性保護が提供されます。 この機能では IEEE 802.1AE 規格を利用し、AP のパフォーマンスに影響を与えることなく、盗聴および中間者攻撃に対する堅牢なセキュリティを確保します。 次のコマンドが導入されています。 • **key chain** *chain-name* **macsec** • **ap profile** *name* **macsec** • **show ap macsec summary** • **show macsec** • **debug macsec** 詳細については、「MACsec support on APs」を参照してください。
	IOx アプリケーションと Wi-Fi の共存実装	このリリース以降、IOx アプリケーションをベースとして Wi-Fi 共存が実装され、2.4 GHz ISM 帯域上の Wi-Fi および IoT 無線間の信号干渉を最小限に抑制します。Packet Traffic Arbitration（PTA）を使用してエアタイムシェアリングを調整するこのコラボレーションメカニズムにより、高い IoT デバイス密度の環境におけるパフォーマンスと信頼性を確実に向上させます。
	レジリエントなインフラストラクチャ	ネットワークセキュリティに対する継続的なコミットメントの一環として、このリリースでは、レガシーコマンドの安全な代替方法を導入しています。この更新は潜在的なリスクを軽減し、より堅牢で安全な運用ベースラインの確立を支援するように設計しています。 特定された安全でないなコマンドは、次のように分類されます。 • 回線トランスポート：安全なリモートアクセス方式に更新。 • デバイスサーバー設定： サーバー側設定の強化。 • ファイル転送プロトコル： 暗号化した転送方式への移行。 • SNMP： 管理トラフィックを保護するための機能拡張。 • パスワード： 認証方式と認証情報の管理を強化。 • その他： さまざまなシステム機能の一般的なセキュリティの改善。 Cisco IOS XE 17.18.2 リリースで導入した **show system insecure configuration** コマンドを使用すると、デバイスで設定されている安全性の低いコマンドがすべて一覧表示されます。デバイスの再起動やアップグレード中に検出したすべての安全でない設定について、エラーメッセージを表示します。 Cisco IOS XE 26.1.1 リリースでは、すべての安全でない CLI コマンドをデフォルトでブロックし、ネットワーク インフラストラクチャを強化しています。レガシーコマンドを使用する必要がある環境では、グローバル コンフィギュレーション モードで **system mode insecure** コマンドを有効にする必要があります。 • 推奨：非セキュアモードを使用しないでください。このモードは一時的なもので、今後のリリースで削除する予定です。安全でないコマンドをすべて特定し、セキュアな代替コマンドに置き換えます。 • アップグレード動作：実行コンフィギュレーションに安全でないコマンドがすでに存在する状態で Cisco IOS XE 26.1.1 リリースにアップグレードすると、system mode insecure コマンドが自動的に設定に追加され、サービスの中断を防止します。 詳細については、「Cisco 9800 Wireless Controller Resilient Infrastructure」を参照してください。
使いやすさ	GNSS の機能拡張	このリリース以降、次の 2 つの拡張機能を利用できます。 • コントローラから GNSS を有効または無効にするオプション、および • 改善された **show gnss info** コマンドの出力。これにより、詳細なランタイムステータスと診断が提供されるようになります。このコマンドには、GNSS をサポートする他のシスコ ワイヤレス AP で改善された同等の出力がすでに含まれています。 詳細については、次のマニュアルを参照してください。

© 2026 Cisco and/or its affiliates. All rights reserved.

製品への影響	機能	説明
		9167I：GNSS 9167E：AP Mode Configuration 9165E：Control and Provisioning of Wireless Access Points 9165D：Control and Provisioning of Wireless Access Points
	URWB パラメータの動的な設定	この機能を使用すると、デバイスを再起動することなく、サポート対象のアクセスポイント（AP）で特定の超信頼性ワイヤレスバックホール（URWB）設定パラメータを調整できます。 詳細については、「URWB」を参照してください。
	PAT のポート制限を削除	このリリース以降、TCP と UDP の両方に 1 ～ 1024 のポート番号を使用できるようになります。ただし、これらは予約済みポートであるため、注意して使用してください。有効なポート範囲は 1 ～ 65535 です。 詳細については、「Workgroup Bridge-Advanced features and optimizations」を参照してください。
	SCEP を使用した証明書の自動登録および更新	この機能により、Simple Certificate Enrolment Protocol（SCEP）を使用した IW916x ワークグループブリッジ（WGB）の証明書の自動登録および更新が可能になります。WGB では、認証局（CA）サーバーからデジタル証明書を安全に取得して更新し、大規模な EAP-TLS 展開のデバイス認証と管理を合理化できます。 詳細については、「Workgroup Bridges」を参照してください。
	センサー接続の改善	このリリースでは、センサー接続アプリケーション（IoT Orchestrator）の設定および使用に関するユーザーエクスペリエンスが向上し、顧客やパートナー様が BLE の成果を向上させることができるようになりました。顧客は、自動化された IP アドレスおよび NAT 設定ルールを使用した、より直感的なネットワークのパラメータ化によって、セットアップワークフロー時にこれまで以上に合理化されたセンサー接続アプリケーションのインストールおよび設定方法を目の当たりにするでしょう。
アップグレード プロセス	カーネルミニダンプおよび Trustzone アップグレードのサポート	Cisco IOS XE 26.1.1 以降、カーネルミニダンプおよび TrustZone のアップグレードが、Cisco Catalyst 9162 シリーズ アクセス ポイント、Cisco Catalyst 9164 シリーズ アクセス ポイント、および Cisco Catalyst 9166 シリーズ アクセス ポイントでサポートされています。
セットアップの容易さ	SSID レベルでのレガシーデータレートの選択	このリリース以降、SSID レベルでのレガシーデータレートの選択機能により、WLAN ごとに 802.11a/b/g データレートの設定が有効になります。この機能を使用すると、特定の SSID の最小ビットレートを指定でき、AP が設定された最小値より低いレートをアドバタイズしないようにすることができます。さまざまなユーザーグループやアプリケーションに対して、特定のパフォーマンスしきい値を満たすために必要なきめ細かい制御が提供されます。 詳細については、「Data Rate Selection at SSID Level」を参照してください。
	アクセスポイントに対する加速度センサーのサポート	このリリースでは、アップグレード後に AP がコントローラに接続したときに、デフォルトで加速度センサーを有効にできます。加速度センサーは、アンテナの下への傾きを判断するための情報を提供します。 加速度センサーをサポートする AP は、以下のとおりです。 • Cisco Catalyst ワイヤレス 9166D1 AP • Cisco Wireless 9176I / 9176D1 AP • Cisco Wireless 9178I AP • Cisco Wireless 9179F AP • Cisco Wireless 9174E* AP（*CW-ANT-T-D2-D8 アンテナで使用する場合） 次の show コマンドが導入されました。 • **show ap name** *ap-name* **accelerometer**

© 2026 Cisco and/or its affiliates. All rights reserved.

製品への影響	機能	説明
		詳細については、「AP Configuration」を参照してください。
	URWB AP のリカバリ CLI コマンド	URWB のリカバリ CLI がアップグレードされ、アクセスポイント（AP）の初期プロビジョニングと自動リカバリが有効になりました。この更新により、AP はリカバリコマンドを使用してコントローラとの接続を復元できます。 詳細については、「URWB」を参照してください。
	静的 AP 名の設定	静的 AP 名を設定すると、管理者はコントローラに接続する前に AP の具体的な名前を事前設定できます。これにより、AP は最初の接続時に指定された名前を採用し、ネットワーク全体で命名の一貫性が厳密に維持されます。また、AP がオフラインの場合でも誤った名前の重複や不正な変更が防止されます。 次のコマンドが導入されました。 • **name** *ap-name* 詳細については、「New Configuration Model」を参照してください。
	Cisco TrustSec-ISE 通信でのネイティブ IPv6 サポート	このリリースで Cisco TrustSec-ISE 通信のネイティブ IPv6 サポートが導入され、組織がネットワーク セキュリティ インフラストラクチャを最新化できるようになりました。 この更新により、IPv6 対応ネットワーク全体でのシームレスなアイデンティティベースのアクセス制御とポリシーの適用が容易になり、アドレスの枯渇や非効率なルーティングなど、IPv4 の制約事項に効果的に対応します。CLI および GUI を介して使用できる簡素化された構成オプションにより、エンタープライズ環境にとって堅牢で拡張性のある、将来に備えたセキュリティ管理を提供できるようになりました。 詳細については、「Cisco TrustSec」を参照してください。
ハードウェアの信頼性	CW9800M、CW9800H1、および Nexus スイッチ間での前方誤り訂正（FEC）モード cl74 を使用した SFP のサポート	このリリースでは、SFP-25G-CSR-S、SFP-25G-LR-S、および SFP-25G-SR-S トランシーバを使用するインターフェイスにより、前方誤り訂正（FEC）モード cl74 用に設定された Nexus スイッチとのリンクが正常に確立されます。 これまで、これらのインターフェイスはこの設定で起動できませんでした。この更新によって接続の問題が解決され、FEC モード cl74 でこれらの SFP を使用するコントローラと Nexus スイッチ間の安定したリンクが有効になります。 **注**：リンクが適切に動作するよう、両方のデバイスで FEC モード cl74 が有効になっていることを確認してください。この更新により、これまでの接続の問題が解決され、リンクの安定性が向上します。
コンプライアンス	6 GHz 帯のサポート対象国が追加	Cisco IOS XE 26.1.1 以降、アゼルバイジャン（AZ）、エジプト（EG）、カザフスタン（KZ）、モーリシャス（MU）、チュニジア（TN）、モナコ（MC）が 6 GHz 無線帯域のサポート対象国リストに追加されます。 詳細については、「Countries and Regulations」を参照してください。
API エクスペリエンス	DHCP 向けネットワークサービス分析（NSA）での IPv6 のサポート	この機能により、メッセージ数、メッセージ遅延、アドレス割り当て数、リクエスト成功率、およびエラーメトリックを含む DHCPv6 統計情報を Catalyst Center などのネットワークサービス分析フレームワークに公開し、DHCPv6 運用のモニタリングとトラブルシューティングを有効にします。 運用の主な利点は、IPv6 アドレス割り当て動作の可視性向上と、割り当ての失敗やパフォーマンス回帰の迅速な特定であり、これにより運用の信頼性が向上し、インシデント対応が強化されます。
	Cisco TrustSec REST ベースのポリシーおよび環境データプロビジョニングの機能拡張	この機能を使用すると、Cisco TrustSec 対応デバイスでセキュアな REST ベースのトランスポートプロトコルを使用して、Cisco Identity Services Engine（ISE）サーバーから SGACL ポリシーと環境データをダウンロードできます。このアプローチでは、古い RADIUS ベースの方式を置き換えまたは補完することで、ポート 9063 での TLS 1.2 暗号化による、より高速で信頼性の高いデータ配信と、セキュリティの強化が実現します。 この機能では、順序付き選択ロジックとランダムな選択ロジックの両方を使用した複数のサーバー設定がサポートされ、効果的な負荷分散が可能になります。さらに、サーバーの稼働状況

© 2026 Cisco and/or its affiliates. All rights reserved.

製品への影響	機能	説明
		チェックや HTTP 429 「過負荷」応答の処理機能といった堅牢なフェールオーバー メカニズムが含まれているため、ネットワークデバイスが同期された最新のセキュリティポリシーを維持できます。 詳細については、「Cisco TrustSec」を参照してください。

MIB

次の MIB が変更されました。

- AIRESPACE-WIRELESS-MIB.my

製品分析

Cisco IOS XE 製品分析は、製品の使用状況を把握し、製品の改善と開発を可能にし、製品の導入と販売サポートを支援する目的で、デバイスのシステム情報を収集します。機能の使用状況の要約データと設定の統計カウンタのみが収集されます。Cisco IOS XE 製品分析の一部として、MAC/IP アドレス、ユーザー名、カスタム設定名、ユーザー指定文字列などの個人を特定できる情報は収集されません。シスコは、一般利用規約、シスコプライバシーポリシー、およびその他の該当するシスコとの契約に従ってこのデータを処理します。

「Cisco Enterprise Networking Product Analytics Frequently Asked Questions」を参照してください。

動作における変更

表 3. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.1 の動作における変更

機能	説明
スロット 0 の 5GHz で show AP コマンドが機能しない	デュアルバンド無線を備えた CW9176D1 や CW9176I などの AP モデルは、スロット 0 での 5 GHz 動作をサポートしますが、コントローラは 5 GHz コマンドに対してスロット 1 および 2 のみを認識します。その結果、スロット 0 で 5 GHz をターゲットとするコマンドを実行すると、無効な入力エラーを返します。 この制限は、コマンドの実行とスロット選択の両方のプロンプトに影響し、AP の管理に影響を与えます。 動作の変更により、**show ap** *ap-name* **dot11 dual-band urwb detail** コマンドが追加され、このギャップに対処するためにデュアルバンド無線の詳細が表示されるようになりました。
自動周波数調整（AFC）での標準電力バイアスのサポート	AFC および標準電力の導入により、標準電力バイアスの管理がますます重要になっています。特に、信頼性が不可欠な天井の高い環境で CW9179F または外部アンテナの 6 GHz AP を使用する展開では非常に重要です。 この機能拡張により、RRM 内で標準電力バイアスを有効にするオプションが提供され、特に AFC 環境での最適なパフォーマンスとコンプライアンスが確保されています。 AP を標準電力モードで動作させるには、次が必要です。 • 設定（チャネル幅、DCA チャネルリスト、および PSC 設定を含む）に基づいて少なくとも 5 つの AFC チャンネルを使用できる必要があります。 • AFC ライセンスで、最小電力レベル 1 をサポートしている必要があります。

© 2026 Cisco and/or its affiliates. All rights reserved.

機能	説明
古い機能に対するコマンドの廃止	この更新では、機能廃止プロセスの一環として、特定のワイヤレス設定コマンドに対する警告メッセージが導入されています。 以前は、次の設定コマンドは警告なしで使用できていました。 • OSEN：**security wpa osen** • アグレッシブ ロード バランシング：**load-balance** • WEP：**security static-wep-key** • Air Time Fairness（ATF）：**wireless profile airtime-fairness** *profile-name id* 17.18.2 以降、これらのコマンドを使用すると、この機能が廃止されたことを示す警告メッセージが表示されます。
CW9179F 環境パックのシリアル番号を AP コマンドの出力に表示	**show** コマンド（**show ap name** *ap-name* **config general** など）の出力が更新され、CW9179F 環境パックのシリアル番号が含まれるようになりました。以前のリリースでは、この情報はコマンド出力に表示されませんでした。この機能拡張により、CW9179F 環境パックのシリアル番号をコマンド出力から直接、簡単に表示できるようになり、可視性が向上し、デバイス管理が簡素化されます。
SSH 経由で Netconf を介した大規模な RPC 設定はプッシュ不可	以前は、特定のサイトタグに関するプラットフォームの AP 制限を超過すると、入力レベルで構成がブロックされていました。 システムでは設定を適用できるようになりましたが、入力の検証に時間がかかることによる設定エラーを回避するために、実際の制限の適用（AP の接続回避）は設定バリデータによって処理されます。
メッシュ PSK のダウングレード手順を更新（リリース 26.1.1）	Cisco IOS XE 26.1.1 から 17.18.x や 17.15.x などの古いリリースへのダウングレードプロセス中に、認証方式が PSK であれば、MAP を接続できません。 メッシュ認証に PSK を使用していて、この修正を含まないバージョンにダウングレードする必要がある場合は、次の手順を実行します。 1. ダウングレード前：デフォルトの PSK を有効にします。 2. ダウングレード後：プロビジョニングした PSK を変更しない場合、MAP は通常、コントローラに正常に参加します。PSK を使用して MAP が参加に失敗した場合は、次のリカバリ手順を実行します。 • メッシュ認証方式を EAP に変更します。 • MAP が EAP を介してコントローラに参加したら、影響を受ける各 AP のコントローラで次のコマンドを実行します。**ap name** *ap-name* **mesh security psk provisioning delete** • メッシュ認証方式を PSK に戻します。MAP はデフォルトの PSK を使用して参加し、プロビジョニングした PSK に自動的に更新します。 3. すべての AP がコントローラに正常に参加したら、デフォルトの PSK を無効にします。
Cisco Catalyst 9800 コントローラ モビリティ トンネル暗号化のダウングレード	以前のリリースでは、2 つのモビリティピアでモビリティ DTLS 暗号化の設定が異なっている場合、トンネルの設定が許可されていました。動作の変更により、トンネルを確立（稼働）するには、両方のピアで DTLS 暗号化を有効にする必要があります。
FPGA アップグレード後の SELinux による電源再投入の拒絶	FPGA のアップグレード後、変更を確実に適用するには手動での電源再投入が必要でした。動作の変更により、FPGA のアップグレード完了後は、システムで自動的に電源が再投入されます。

© 2026 Cisco and/or its affiliates. All rights reserved.

機能	説明
デュアルバンドチャネル幅における非標準的な CLI の命名規則	CLI コマンドの **ap name** *ap-name* **dot11 dual-band channel width** で、非標準的なサブオプションが表示され、各チャネル幅の値に誤って「w」が付記されます（たとえば、標準的な「160」ではなく「160w」と表示）。この問題は、ローカルモードと FlexConnect モードの両方で XOR 無線を使用するすべての AP で発生します。動作の変更により、コマンドのサブオプションから「w」が削除されました。
コントローラ GUI のクライアントグリッドで、ポリシータイプ、暗号化方式、および AKM に対するサポートが追加	以前のリリースでは、ユーザーは、クライアントが現在接続されている WLAN ポリシー、暗号化、および AKM を 1 ヵ所に表示できませんでした。この制限により、管理者は各クライアントに対して個別に手動による CLI チェックを実行するか、必要な情報を集約するためのカスタムスクリプトを作成する必要があり、運用の効率が大幅に低下していました。 動作の変更により、ポリシータイプ、暗号化方式、および AKM の詳細がコントローラ GUI のクライアントグリッドに追加されます。
加速度計のサポート：傾斜情報（加速度計）を **show ap config general** コマンド出力に統合	物理的な取り付け時の監視効率を向上させるために、加速度データ（特に傾斜角と最終更新タイムスタンプ）が、**show ap config general** コマンドと **show tech wireless** 出力に直接統合されました。 この情報は特定の詳細なコマンド内に隔離されていたため、取り付けや設置の問題を自動的かつ大規模に検出することができませんでした。 このデータを一般的な設定の概要に追加することで、AP のネットワーク全体での物理的な方向を合理化して自動検証できるようになります。
CW9171I AP での 5 GHz 帯無線リセット統計情報のコマンド障害	5 GHz 無線帯域で動作する CW9171I AP に対して、**show** *ap-name* **dot11 5ghz radio-reset stats** コマンドが機能していませんでした。この問題に対処するため、**show ap name** *ap-name* **dot11 dual-band slot** *0-2* **radio-reset stats** **という新しいコマンドが導入されました。**
jumbo-mtu の廃止および AP プロファイルからの CAPWAP ジャンボフレームの削除	CAPWAP ジャンボフレームは、AP 側ではサポートされていません。そのため、**jumbo-mtu** コマンドは廃止され、CAPWAP ジャンボフレームが AP プロファイルから削除されます。
show ap location stats コマンドの出力を改善	**show ap location stats** コマンドの以前の CLI 出力形式では、「Clients on 11a」の詳細が正しく表示されませんでした。動作の変更により、スロット 0、1、2、および 3 のクライアントに関する詳細を表示するように出力が変更されました。

解決済みの問題

問題に関する追加情報を参照するには、不具合 ID をクリックし、バグ検索ツール（BST）にアクセスしてください。

表 4. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.2 で解決済みの問題

不具合 ID	説明
CSCwu04310	CAPWAP モビリティトンネルでフラグメント化されたパケットにより、CW9800-M/H プラットフォームでデータプレーンがクラッシュする
CSCwp12919	コールドおよびウォームリブート中に、不確実なパラメータをインポートする必要がある
CSCws98862	ビーコン保護によるビーコン損失が原因でクライアントの承認解除を引き起こす MLO クライアントに対して、コントローラが単一の M5 パケットを送信する

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwt19092	9179 で 17.18.2 を実行すると 1 時間未満で 4 回を超える DFS が発生する
CSCwt22893	17.18.2 でコントローラが WNCD コアで想定外の SISF 再起動を実行する
CSCwt65349	CW9172I AP が ar_wal_mlo_ipc.c アサートとウォッチドッグパニックでクラッシュする
CSCwt83641	アップストリームパスで CW9172 AP 無線転送に失敗する
CSCwt94577	CAPWAP モビリティパスでの CPP データパスのクラッシュが原因で、CW9800-M/H ワイヤレスコントローラがリロードする場合がある
CSCwu04279	無効な GPM のロード後に発生するシステムの不安定性とサービス中断の可能性
CSCwu04935	9178：vlan タグが有効になっているときに、AP が「NSS CAPWAP tunnel creation failed」ログにより継続的にリロードする
CSCwu20280	wlan_sm_dispatch+0xb8/0x208 [umac] でのカーネルパニックにより、9176 AP がクラッシュする
CSCwt77092	AP - KFENCEメモリ破損イベントにより RCU が停止し、HW ウォッチドッグがリセットされる
CSCwt77136	連続した KFENCE IPv6 MLD メモリ破損により RCU が停止し、HW ウォッチドッグがリセットされる
CSCwt86133	Wi-Fi 7 AP が、TID ごとのパケットを多数報告する
CSCwt87345	コントローラによるワイヤレス デバイストラッキング カウンタ vlan < vlanid> のクリアが機能しない
CSCwt98260	URL が FQDN ではなく IP アドレスを指す場合でも、AWIPS に対して NameServer の設定が必須となる
CSCwu17364	AP のリブート後に OEAP で個人用 SSID の DHCP が有効になる
CSCws23072	CW9800 プラットフォームで RRM クラッシュとトレースバックが発生する
CSCws47700	WGB ローミングにより wncd プロセスの想定外のリロードとワイヤレスコントローラのリロードを引き起こす可能性がある
CSCws68160	クライアントの削除後、コントローラが「Critical process wncd fault on rp_0_0 (rc=139)」で想定外のリロードを実行する
CSCws76688	Flex モードで AP が「4 ウェイハンドシェイクの後に EAP アイデンティティ要求を送信」した状態で OKC が有効になっている場合、Catalyst 9800 でクライアントが AUTHENTICATING 状態でスタックする
CSCwt07093	フラグメントのドロップにより capwap メッセージがキューに入るため、AP が接続できない
CSCwt09034	C9800-CL での DTLS アラートメッセージの処理およびオープン SSL 復号により、WNCD でウォッチドッグがクラッシュする
CSCwt13732	WNCD プロセスが予期せず終了し、WLC がクラッシュする（重要なプロセス wncd が失敗（rc 0））
CSCwt31826	不正なプロセスでの SIGSEGV が原因で絶え間なくスイッチオーバーやリロードが発生する
CSCwt37351	無線 WLAN ID のハンドラ ID が無効なため、wncd プロセスが予期せず終了し、wlc がリロードされる可能性がある
CSCwt38788	変数が初期化されていないためモビリティプロセスが予期せず終了し、wlc がリロードされる可能性がある

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwt52617	SSO後 - ファブリック外のデバイスへの接続が失われるワイヤレスクライアントがほとんどない
CSCwt52815	AP 無線での変更後、WLC がクライアントの関連するチャネル幅の更新に失敗する
CSCws17199	WPA3 エンタープライズに GCMP256 のサポートを追加（192 ビット以外）
CSCws80754	アンカー WLC のローカル DHCP が、DHCP オファーや ACK の転送を断続的に停止する
CSCwt40423	ID なしで Cloudm トレースバックが実行される
CSCwt43333	スニファモードでの AP（9120/9166）および無線ロールがスニファの場合の 9120 での XPath 設定エラー
CSCwt53740	コントローラからの一部のポリシー設定プッシュが失敗したため AP が SSID をブロードキャストしない

表 5. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.1 で解決済みの問題

不具合 ID	説明
CSCwq60926	IOT AP が地理位置情報レポートを非常に頻繁に送信する
CSCws39961	URWB：Wi-Fi2 チャネルがデュアル無線モードで適用されない
CSCws98340	長時間のローミング中に IW9165E WGB の 6 GHz 無線ファームウェアがクラッシュする
CSCwq72187	WGB で進行中のトラフィックで組み込みのパケットダンプを無効にすると、カーネルパニックがクラッシュする
CSCwr00889	URWB スタンドアロン：ネイティブ VLAN が無効になると CDP がドロップされ、PoE をネゴシエートできない
CSCwr25112	IW916x WGB：Radio2 がアップリンクになると、グループキー（GTK）のキー再生成が失敗する
CSCwr70521	スタンドアロン URWB：**mcs maxmcs** ライブコマンドにより HE レートが無効になる
CSCwr83518	IW9165：ソフトウェアバージョン 17.18.1 の URWB モードで Cisco IW9165 の SNMPd がクラッシュする
CSCws60129	NAPT ポート範囲の設定手順により WGB サービスが停止する
CSCws61721	スタンドアロン URWB：LNO がデフォルト設定では完全に有効になっていないが、CLI では有効であると示されている
CSCws68524	Fluidity 5845 MHz が IW9165 と IW9167 の間で動作していない
CSCwp14628	Cisco Aironet 3800 AP が、バージョン 17.15.3 を実行しているコントローラに AP を移行した後、クライアント認証の問題を表示する
CSCwp20385	Cisco Catalyst 9136 AP の有線 0 インターフェイスが孤立状態になり、RX パケットが処理されない
CSCwp27601	無線 1 FW を 3802 AP で約 20 超のクライアントを使用して長時間実行中にクラッシュが発生する
CSCwp65769	802.1X 認証で高速トランジションを実行している Cisco Wave 2 AP が、セッションタイムアウト時のキー再生成中に誤った M2 メッセージを送信する

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwq12607	9120 AP が、無線ファームウェアビーコン TX がスタックしたために、予期せずリロードする
CSCwq18287	17.15.4：CAPWAPd が spaces_grpcd への通知中に 9162 AP でクラッシュする
CSCwq50978	9176 アクセス ポイント スロット 1 が理由によりリセットされる（無線障害（ファームウェアのクラッシュ））
CSCwq71415	クライアントがデータに応答しないことが原因で、AP1852 が過剰な BAR フラッディングを送信する
CSCwq93561	[SIT]17.18.2：CW9172 を長時間実行するとクラッシュする
CSCwq96192	17.18.2：9171/9174：qdf_bug カーネルパニック lr：vap_wait_for_vdev_init_state+0x27c/0x2c0
CSCwq97854	9800 コントローラを使用した COS AP で Flex WLAN VLAN マッピングが保持されない
CSCwr21290	Catalyst 9105 AP が RX スタック状態のために ACK フレームを停止し、5 GHz スロットで接続されたクライアントで失敗する
CSCwr21879	Wi-Fi7 AP で SKB メモリ関連のクラッシュが発生する
CSCwr56409	FlexConnect AP でワイヤレスクライアントが有線から IPv6 RA を受信しない
CSCwr67024	AP の IP 送信元が正しくないため、エッジはアクセストンネルではなく L2LI0 インターフェイスで AP から検出を受信する
CSCwr77247	17.18.2 を実行している 9174I での AP のクラッシュ：カーネルパニック
CSCwr81031	kmalloc スラブにて 9176 AP でメモリリークが発生する
CSCwr94814	9115 AP が、無線ファームウェアビーコン TX がスタックしたために、予期せずリロードする
CSCwr98669	C9176 FW クラッシュ - cnss_pci 0004:01:00.0: クラッシュ発生
CSCws01793	9178 AP で起動中に NSS ドライバの初期化に失敗する
CSCws06706	C9178：MAC HW ハング/PHY エラーが原因でクライアントが 2.4 無線に参加できない
CSCws08240	Wi-Fi 7 AP：パワーオンリセットにより、コントローラで理由のリロードを伴うクラッシュファイルが生成される - 33
CSCws08681	CW9178I AP：NSS カウントが増加しないため、クライアントが接続できない
CSCws22667	Cisco 9105AWX/9172H AP の RLANポート 2 と 3 を介したアップロードでスループットに問題が発生する（ポート1は影響なし）
CSCws26825	9105 が「RX too late errors」というエラーが原因でクライアントの受け入れを停止する
CSCws32577	9130 RAP、systemd[1]：CAPWAPd.service ウォッチドッグタイムアウト（制限時間は 1 分 30 秒）により、継続的にリロードされコントローラに接続されない
CSCws67290	BGL18 Alpha：AP CW9174I で無線がクラッシュし、破損したコアダンプが確認される
CSCws77227	AP CW9176I カーネルパニッククラッシュ

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCws77337	sdavc アプリケーションパックが原因で /tmp に十分なスペースがないため、9166 SDA APにイメージのダウンロードの問題が発生する
CSCws80385	AP CW9176I カーネル パニック ランダム クラッシュ
CSCws87617	別のアップグレードが進行中のため、9130 を 17.18.2 CCO イメージにアップグレードできない
CSCwt19117	Dot11u 設定が AP から削除されるため、OpenRoaming に影響を与える dot11u で AP のビーコンが停止する
CSCwt26500	CSCwq11842 をすべての AP モデルで機能させるための変更が必要
CSCwt33908	9136-26.2.1：製品寿命内に「ERR_IN_PHY_OFF:0 Ucode Asserted」で無線 1 がクラッシュし、続けて「lr : ol_ath_wifi_ssr+0xde4/0x10e0 [qca_ol]」で AP がクラッシュする
CSCwt53021	国コードが SR に設定されている場合、CW9163-E AP の 2.4G 無線が起動しない
CSCwp63176	Cisco Catalyst 9136 AP での IOx アプリケーションと CAF アプリケーション間の状態の不一致により、Cisco IOx アプリケーションチャネルがダウンする
CSCwp65077	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）
CSCwq66265	クライアントが Wi-Fi 5 AP に HE 機能を送信すると、関連付けエラーが発生する
CSCwq73441	CW9172I AP：17.15.4 実行中のカーネルパニック
CSCwq73700	COS AP を再起動しても手動の地理位置情報座標が保持されない
CSCwr01343	プロセスの起動後に 9166 AP 無線インターフェイスがダウンする
CSCwr26505	C9130 AP で、障害後に IPv6 アドレスを含むディスカバリ要求を送信できない
CSCwr28328	カーネルログメッセージ「wlan_crypto_encap: Key is NULL」で AP syslog がいっぱいになる
CSCwr32085	1815 APトレースイベントクラッシュ
CSCwr69841	CW9176 のスイッチポートの背後に 2 つの MAC アドレスが表示される
CSCwr77108	FlexConnect ローカル認証で FT11r または OKC を使用している場合、AP が RADIUS サーバーによってプッシュされた VLAN を破棄する
CSCwr77143	CW9166/IW9167：17.15 実行中のカーネルパニッククラッシュ
CSCwr96590	C9120 AP NMI ウォッチドッグのクラッシュ：ソフトロックアップ、CPU#3 が s 秒間スタック状態になっている[kclick:]
CSCwr97281	9105 AP が「auto-rf」結果で干渉を過剰に報告している
CSCws25172	コントローラバージョン 17.15.3 で RO の国コードを使用する 6GHz 無線がオンになっている場合、9166 AP がクラッシュし続ける
CSCws35315	AP から CAPWAP 接続を引き継ぐ補助クライアントインターフェイス
CSCws47852	AP が断続的にコントローラに接続しているが、コントローラで AP タイプの取得に失敗し、AP が拒否される

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCws60984	9166 クラッシュ systemd[1] : CAPWAPd.service が失敗した
CSCws70285	/storage/cnssdaemon.log のクリーンアップ
CSCws72425	9136I IOX アプリケーションのアクティブ化失敗
CSCws76582	17.15.3 - 古いクライアントエントリによる、APでの新しい関連付けの禁止
CSCws79118	2.4 GHz in -Z 規制ドメインでの 9124-AXE の送信電力が想定外に低下する
CSCwt09003	AP が 中央認証により FlexConnect モードになっている場合、クライアントが「FT+SAE」に接続しない
CSCwq66623	SJC Alpha - 17.18.2 alpha AP がコントローラに接続せず、DTLS でスタック状態になる
CSCwr20303	AP ロケーション名の設定の変更後にコントローラを想定外にリロードする
CSCwr65627	プライマリがダウンすると、多数の AP（2K 以上）が N+1 コントローラに参加するまでに数分かかる
CSCwr67652	wsa_db が原因でコントローラのメモリ異常が通知される
CSCwr90981	5GHz 無線での AP 数の変動
CSCws16148	「ap geolocation ranging accurate method uwb」コマンドを発行した後に、コントローラがクラッシュする
CSCws18528	[APCI] すべての帯域の MLO 不正の封じ込めが機能しない
CSCws38733	AP レンジング CLI がコントローラのスイッチオーバーをトリガーし、コアファイルが作成される
CSCws39889	RF ベースの AP ロードバランシング：ロード バランシング アルゴリズムの実行中に観測されたことが原因でコントローラがクラッシュする
CSCws58494	WebAuth クライアントがコントローラで実行状態に移動したが AP の WebAuth でスタックしている
CSCws58703	SST：17.15.x から 17.18.2 への ISSU アップグレードの後に ndbmand コアが確認され、CatC と NETCONF が機能しない
CSCws65956	コントローラが wncmgrd でクラッシュし制限される（rc 139）
CSCws91899	FlexConnect クライアントの処理中に C9800 がクラッシュする
CSCws93542	フェールオーバー後の DHCP オファーをコントローラがクライアントに転送しない
CSCwr30777	9800 スタンバイシャーシが、17.12.4「show inventory」からの出力で Cisco Unknown Power Supply および同じ SN を表示する
CSCwr74373	不正な関連付け解除が発生しても、C9800 コントローラ アカウンティング要求パケットが送信されない
CSCwr79853	ファイルマネージャで、ロケーションボックスにあるファイルを選択すると、ダウンロードが失敗する
CSCwr80088	サイトタグとポリシータグがコントローラ上で 9130AP に正しくマッピングされない
CSCwr96860	AP モデル 3800E および 9120AXE の RESTCONF RPC を介したアンテナゲイン設定が失敗し、「slot: 0 does not have a dedicated radio」エラーが発生する

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCws10863	9800 - 未解決の規制ドメインを持つ AP が、他の AP の RRM の実行を停止させる
CSCws17702	レコードプルーニングおよび DB クエリエラーの後、PAED プロセスが 24 時間ごとにクラッシュする
CSCws19686	重複する AP 名を設定すると、重複名の警告ではなく「Internal Error, Check Logs」と表示される
CSCws22542	17.15.3：RW ドメインでトルコでの 6GHz 帯域のサポートが欠落している
CSCws26758	コントローラのクライアントエントリにより、AP が無線ごとの最大クライアント数に達する
CSCws30144	仮想ワイヤレスコントローラのクラウドサービス OTP トークンが、一部のエッジケースで表示されない
CSCws31873	GTK キーのローテーションが有効になっている場合、SSO 後にメディアストリームおよびマルチキャストトラフィックが失敗する
CSCws46519	コントローラで「Ap lldp ネイバーの表示」を実行すると、古い情報が残り続ける
CSCws49525	SIT：CleanAir Pro - スペクトルキャプチャが、アップロードの応答（成功）にもかかわらず eWLC 上で Spectral_recording ディレクトリ/ファイルを提供できない
CSCws62182	GUI に誤ったチャネル帯域幅（ネゴシエート/対応）が表示される
CSCws66137	ローカル認証（中央認証ではなく）が行われている間、クライアントの関連付け時刻が「01/01/1970 00:00:00」と表示される
CSCws82703	webui からインストールファイルへのアクセスを試行中に、「SeLinux: qwlc: subject polaris_iosd_t denials 2026-01-16 11:14:35」と表示される
CSCws83128	AP 名の変更は、特定のホスト名文字列（APデータベースに存在しない）の競合により「AP 名がすでに存在します」というエラーを示して失敗し、コントローラは AP をデフォルト名に戻す
CSCws93326	SJC Alpha 26.1.1 ERRログ: (ERR): MAC: 0000.0000.0000 \u00a0 RAトレースエントリをマルチリンククライアント用に設定。dot11 操作データを取得できない
CSCwt21195	新しいロケーションの作成時にデフォルトの 6 GHz RF プロファイルを選択できない
CSCwt21642	802.11r PMK キャッシュで検索しないため、誤ったクライアント認証タイプが使用される
CSCwt25978	ワイヤレス バンドル クライアントの名前にサイトタグスペースがあると機能しない
CSCwt41808	AP が AVL 木に参加中に無効な文字列ポインタが原因で wncmgrd プロセスがクラッシュする
CSCwt41939	selinux 拒否後の IOS_PRIV_OPER_DB tbl_ewlc_critical_events テーブルでの TMPFS メモリリーク

未解決の問題

問題に関する追加情報を参照するには、不具合 ID をクリックし、バグ検索ツール（BST）にアクセスしてください。このセクションには、現在のリリースに適用される未解決の問題と、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ リリース 26.1.x より前のリリースに適用される可能性がある未解決の問題をリストしています。これまでのリリースで未解決でまだ解決されていない問題は、解決されるまで今後のすべてのリリースに適用されます。

表 6. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.2 で未解決の問題

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwu19389	デバイスが「%DBAL-4-LONG_EXEC_BATCH:」メッセージを報告する。Switch 1 R0/0: pubd: Long exec
CSCwt71091	SSL/TLS ハンドシェイクが正常に実行された CNDP 接続の再試行ループ中に、pubd プロセスでメモリリークが発生する
CSCwt10857	evconfd での整数アンダーフローにより後続のサブスクリプションがデータを送信しない
CSCwt09028	exceed-set-dscp-transmit-table での不正な参照により Netconf-yang 同期が失敗する
CSCwt00058	NETCONF を有効にすると、「confd_mgrd」および「ncsshd」プロセスがクラッシュする
CSCwr77437	SDAVC 関連の破損が原因だと考えられる HTTP CORE でのセグメント障害
CSCws80808	Mgmt-intf VRF のループバック インターフェイスが、管理インターフェイス経由で到達不能になる
CSCwt95273	特殊文字を含む 6 暗号化タイプを使用した SNMPv3 ポーリングでスイッチがクラッシュする
CSCwu58859	CTS の設定が存在し、DNA-advantage ライセンスが設定されていない場合、アップグレード時に IOSXE がクラッシュする
CSCwt76906	C9K：CTS CORE で保持しているメモリが継続的に増加する
CSCwt07061	DNS SRV-1 プロセスが原因で CPU 使用率が高くなる
CSCuv03769	MOTD でのエラー発生 - ログパケットのオーバーラン、PC 0x12D60814
CSCwn80721	sessmgrd プロセスでの予期しない再起動
CSCwt47516	AAA 処理中に長さフィールドが破損したため、コントローラがクラッシュする
CSCwt87294	mDNS のキャッシュフラッシュ動作に一貫性がない。ベースラインのバグ
CSCwk79990	9800-L で、Intel Reset Request が原因でカーネルが応答しなくなる
CSCws42581	ダイナミック マルチキャスト ルータ ポートとグループの処理中に、L2 マルチキャストでメモリが破損する
CSCwt26121	APMGR：APMGR のコードスキャンの修正
CSCwt31565	17.12.6a を実行している Cisco 9800-40-K9 で、ワイヤレスクライアントが RUN 状態でスタックする
CSCwt91818	APSP のインストール中に C9800 WLC がクラッシュする
CSCwu08974	ARP プローブデバッグログで C9800 wncd がクラッシュする
CSCwu14554	9105/9172H RLAN AP が中央スイッチングのマルチキャストトラフィックを通過しない
CSCwu50927	カーネルパニックにより C9120 COS AP がクラッシュする（PC は bpm_alloc_mult_skb）
CSCwu52200	クライアントが接続を試みた後に C9800 が予期せずリロードする
CSCwu52744	C9120 COS AP がクラッシュする（PC は phy_ac_noise_lte_avg、LR は phy_noise_lte_avg）
CSCwu58946	802.1X 認証失敗：EAP 要求 ID が AP によって無線で転送されない

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwu66197	17.15.5.201（APSP 1）にアップグレードした後に、カーネルパニックが原因で C9130AXI AP がクラッシュする
CSCwu66664	AP 9136 が capwapd コアを生成中にクラッシュする
CSCwu77375	バックホールとして設定された AP9167EH slot1 と、クライアントにサービスを提供するように設定された slot2 では、RRM DCA が発生しない
CSCwu84328	スケジューラがスタック状態であるため、9176 AP でクライアント接続の問題が発生する
CSCwu92389	RMI リンクフラップが WLC にログオンしたが、スイッチオーバーが発生しない
CSCwu92593	SLAAC を使用した AP 9176I IPV6 RA パケットのドロップ
CSCwu96599	9120 AP がダウンリンクパケットを IW9167E に送信しない
CSCwv04941	17.18.3 での 9176 AP による DHCP パケットのドロップ
CSCwv17189	17.15.4bESW1 EWC RAP でカーネルスラブがリークする可能性がある
CSCwv17525	[C9105AXI] カーネルパニックのクラッシュ：17.15.5 へのアップグレード後に新しい AP がクラッシュする
CSCwv27458	異なる PC および LR でのカーネルパニックが原因で AP がクラッシュする
CSCwv28280	Broadcom アクセスポイントがクラッシュする（PC は wlc_ap_process_assocreq_done.isra.28、LR も wlc_ap_process_assocreq_done.isra.28 を示す）
CSCwv29655	17.18.3.18 を実行している CW9172I AP で、メモリ破損のシグニチャによるランダムなカーネルパニックが発生する
CSCwv30224	17.18.3.18 を実行している CW9172I が、RRMReceive::process_rx_frame_from_driver でクラッシュする
CSCwv33315	wncd のクラッシュ（SIGABRT）：CAPWAP TX の完了パスでヒープ バッファ オーバーフローが発生する
CSCwv33856	CAPWAP メッセージにより WLC で WNCD プロセスのリークが発生する
CSCwv36063	bss カラーの変更が発生すると、グローバルに無効になっている場合でも Wifi6E および Wifi7 AP が 6GHz 帯ですべてのクライアントを切断する
CSCwv38974	6 GHz チャネル電力ペイロードの予期しない値による 9800 のクラッシュ
CSCwv40106	リリース 17.15.5 へのアップグレード後に aWIPS 機能が破損する
CSCwv40579	カーネルパニックが原因で CW9176I AP がクラッシュする
CSCwv41569	夜間のカレンダープロファイルのスケジュールにより SSID ブロードキャストに障害が発生する
CSCws94151	SFP「SFP-H25G-CU1M」が C9800M で機能しない - 17.15.03 と Nexus C93180YC-EX
CSCwt20158	ごく少数のクライアントのみを表示する bsnMobileStation - 根本原因は Wifi7
CSCwt44343	名前を変更すると、AP に変更を加えることができない場合がある。% Error: no ap_name exists

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwt61816	[Monitoring] > [Wireless Clients] を実行すると、誤ってクライアント数が多く表示される
CSCwt84933	チャネル 100 ～ 140 はナイジェリアで使用できるが、それらはライセンス取得済みの周波数帯域である
CSCwu20316	9800 で dot1x pmf クライアントの承認解除が CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE と表示される
CSCwu24905	CW9166 COS AP が、NSS ファームウェアのクラッシュが原因でクラッシュする
CSCwu32896	LWA コントローラが HTTP 200 のリダイレクトを送信しない
CSCwu34251	コントローラが AP ネイバーを報告していない
CSCwu42825	Wi-Fi 7 syslog が WLC で大量に生成されている
CSCwu50245	いずれかのスロットが 6 Mbps を除外する 5 GHz レガシーレートであるにもかかわらず、9130 でビーコンレートが 6 Mbps にプログラムされているため、DOT11_STATUS_DENIED_RATES が発生する
CSCwu50455	AP C9124AXE でオレンジ色の LED が点灯する
CSCwu52741	C9120 COS で AP がクラッシュする（PC は rhb_init_rfic_mdata_ptrs、LR は rhb_init_cfg80211）
CSCwu52776	RHL プローブエラーにより C9120 COS で AP がクラッシュする（リブートして回復）
CSCwu86004	コントローラがクライアントから DHCP リリースを受信すると、クライアントを認証解除する
CSCwu96018	EWC スマートライセンスの AIR AP に「Non Compliant」および「Never Licensed」と表示される
CSCwu98499	9105AW WGB モードのポート 1/2/3 が 17.15/17.18 で起動しない
CSCwv03367	17.18.3 無線で 9172I AP が定期的にクラッシュする
CSCwv07349	9176、9120、9164 プローブクライアントデータを 91xx シリーズの AP 17.12、17.15 で使用できない
CSCwv07586	電源モジュールの取り外し/挿入後に、CW9800M FAN のステータスが入力されない
CSCwv10846	C9130/C9124 を 17.18.2/26.1.1 以降にアップグレードすると、AP で 17.9 より前のコードをブートできない
CSCwv20470	クライアントが、ローミングによってトリガーされ、AAA オーバーライドを介して割り当てられた VLAN ではなく、ポリシープロファイルの下にマッピングされた VLAN から IP アドレスを取得する
CSCwv22511	Cisco Spaces コネクタを使用すると、一部の関連付けられたクライアントのクライアント詳細に情報要素が表示されない
CSCwv26370	重複する VLAN 名のマッピングで 17.15.4b が削除された後に、C9800 FlexConnect クライアントがポリシー VLAN を使用する
CSCwv31549	bsnStationBlacklistingReasonCode トラップでのクライアント除外理由が正しくない
CSCwv38891	AI-RRM が設定されていない場合でも、FRA に DNAC 管理として表示される
CSCwv38912	XOR 無線が設定されていない場合、クライアント対応 FRA を使用してモニターモードとクライアントサービスモードが切り替えられる

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwv40607	ThousandEyes で、WAT が以前の接続から誤った DNS IP を報告する

表 7. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 26.1.1 で未解決の問題

不具合 ID	説明
CSCwp26522	IW9167E スロット 2 がクライアントとして 5G バンドで機能するとき、ビーコンがスタックする
CSCwt37025	URWB コントローラ：工場出荷時状態へのリセット後の（コントローラへの）接続の問題
CSCwr37961	GNSS フィルタリングロジックによって QZSS コンステレーションが正しく報告されない
CSCwr74409	モビリティクライアントのスキャン後、シグナリングパケット 0x998 が転送されない
CSCws62538	IW9165E WGB 6G 帯域のダウンリンク ブロードキャスト パケットが 17.15 WIFI7 インフラ AP と相互運用する場合、信頼性の高いユニキャストに変換されない
CSCwt40834	ダイナミックチャネル幅の変更後に、IW9165E リモート モビリティ クライアントが無線バックホールを介してコントローラに再接続できない
CSCwt42516	チャネルのホット設定適用後に、AP とコントローラ間の AP URWB 無線チャネルの表示に不整合が発生する
CSCwt38787	有線専用モビリティコーディネータで MPO を有効にするには、スロットでモビリティプロファイルが必要
CSCwt31537	AP が MACsec で設定され、スイッチが設定されていない場合、AP は IP アドレスの取得に失敗する
CSCwk79990	9800-L で、Intel Reset Request が原因でカーネルが応答しなくなる
CSCws42581	ダイナミック マルチキャスト ルータ ポートとグループの処理中に、L2 マルチキャストでメモリが破損する
CSCws47700	WGB ローミングにより wncd プロセスの想定外のリロードとワイヤレスコントローラのリロードを引き起こす可能性がある
CSCws68160	クライアントの削除後、コントローラが「Critical process wncd fault on rp_0_0 (rc=139)」で想定外のリロードが発生する
CSCws68479	wifi6/6e regdb の特定のバンドおよびチャネルのサポートが未対応になっている
CSCwt03837	スタンバイプラットフォームに LocalSoft が原因で予期しないリロードに直面している HA がある
CSCwt07093	CAPWAP メッセージがキューに入っていることが原因で AP が接続できない
CSCwt08175	PCが _ZN17SPSCPriorityQueue4pushEiP6Packet+0x7c/0x4c8 に、LRが _ZN17SPSCPriorityQueue4pushEiP6Packet+0x40/0x4c8 にあるため AP カーネルパニックが発生する
CSCwt09034	C9800-CL での DTLS アラートメッセージの処理およびオープン SSL 復号により、WNCD でウォッチドッグがクラッシュする
CSCwt13732	WNCD プロセスが予期せず終了し、コントローラがクラッシュする（重要なプロセス wncd が失敗（rc 0）））
CSCwt19011	9166 17.15.4b AP は SDA モードで、DHCP 後に IPv4 ARP アップストリームや他の IPv4 パケットを転送しない

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCwt19092	9179 で 17.18.2 を実行すると 1 時間未満で 4 回を超える DFS が発生する
CSCwt19490	9800コントローラ：RADIUS アカウンティングで使用している古いクライアント IP により ISE IP-SGT/SXP が上書きされる
CSCwt20299	アプリケーション トラフィックが、補助クライアント インターフェイスの代わりに出力インターフェイスとして wired0 を使用する
CSCwt22893	17.18.2 でコントローラが WNCD コアで想定外の SISF 再起動を実行する
CSCwt26353	ISSU を 17.12.5 から 17.15.4d にアップグレードすると、SSID が AP にプッシュされない
CSCwt26718	wncmgrd から応答がないために eCA アップグレード操作が失敗する
CSCwt31565	17.12.6a を実行している Cisco 9800-40-K9 で、ワイヤレスクライアントが RUN 状態でスタックする
CSCwt31826	不正なプロセスでの SIGSEGV が原因で絶え間なくスイッチオーバーやリロードが発生する
CSCwt37351	無線 WLAN ID のハンドラ ID が無効なため、wncd プロセスが予期せず終了し、コントローラがリロードする可能性がある
CSCwt38788	変数が初期化されていないためモビリティプロセスを予期せず終了、コントローラがリロードされる場合がある
CSCwt42369	C9136I 無線のクラッシュ
CSCwt50389	AP が EAP_ID_REQ か M2 の確認応答をせず、Ascom Myco2 電話が 9176 AP に接続できない
CSCwt52617	SSO後 - ファブリック外のデバイスへの接続が失われるワイヤレスクライアントがほとんどない
CSCwt52815	コントローラが AP 無線で変更されると、クライアントの関連するチャネル幅の更新に失敗する
CSCwt53635	C9800-40-K9 の wncmgrd プロセスでメモリリークが発生する
CSCwt58260	AP がドライバでの dot11 オープン認証要求をドロップする
CSCwt58849	CAPWAPd プロセスが継続してクラッシュする
CSCwk07132	Flex Connect ローカル スイッチングを使用した AP における AAA クライアントレート制限が 17.12.3 でストリームごとに変更される
CSCwr96781	コントローラで 6 GHz 帯域の「show ap dot11 6ghz cleanair air-quality summary」コマンドの AQ 情報が出力されない
CSCws03721	9120/9115/9105 AP が iOS デバイスから送信されたフレームを確認応答せず、CSCwj91255 のフォローアップを行う
CSCws17518	コントローラでコマンドを実行した後に予期しないリロードが発生する
CSCws78457	WGB の背後にある有線クライアントが数日後にトラフィックの通過を停止する
CSCws80754	アンカーコントローラのローカル DHCP が、DHCP オファーや ACK の転送を断続的に停止する
CSCws93044	クライアントが接続した直後 1 秒を経過しても AP からビーコンが送信されない

© 2026 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明
CSCws94151	SFP「SFP-H25G-CU1M」が C9800M で機能しない - 17.15.03 と Nexus C93180YC-EX
CSCws95359	さまざまな SPF モデルの CW9800M、CW9800H1 で 10Gポートが稼働しない
CSCwt20158	ごく少数のクライアントのみを表示する bsnMobileStation - 根本原因は Wifi7
CSCwt39820	AP が AP 参加プロファイルから加速計設定を受信しない
CSCwt40423	ID なしで Cloudm トレースバックが実行される
CSCwt43333	C9120E デュアルバンドロール XPath は HTTP 204 に成功しても 5 GHz スニファ設定を適用しない
CSCwt44743	CW9166I が Zebra MC9300 RF ガンから ARP クエリをランダムにドロップする
CSCwt47490	CW9166 COS の AP が、カーネルパニックが原因で最初の起動後にクラッシュする
CSCwt51709	静的 IP が設定されていても COS の AP で DHCP プロセスが開始されるため、DHCP フォールバックの問題が断続的に発生する
CSCwt53740	コントローラからの一部のポリシー設定プッシュが失敗したため、AP が SSID をブロードキャストしない
CSCwt58405	チャネルが変更されていないにもかかわらず、フェールオーバー後に C9800-CL-K9/CAC がトリガーされる

既知の問題

Cisco IOS XE 26.1.2 の既知の問題は次のとおりです。

ローミング時間が長いと Cisco Wireless 9176 AP 無線ファームウェアがクラッシュする

バージョン 26.1.2.30 を実行している Cisco Wireless 9176 の AP と 26.1.2 を実行している Catalyst 9800-40 コントローラで、無線ファームウェアのクラッシュがランダムに確認されています。

ISSU 後のローリング AP のアップグレード中に、show ap upgrade コマンドが GREEN 検証エラーを返す

ISSU を Cisco IOS XE 26.1.2 にアップグレードした後、ローリング AP のアップグレードが進行中に `show ap upgrade` コマンドが失敗することがあります。AP のアップグレードステータスを表示する代わりに、以下を返します。

```
% Error: Internal error - failed in GREEN request/response handling
```

Cisco IOS XE 26.1.1 の既知の問題は次のとおりです。

Cisco Catalyst 9130 シリーズおよび 9124 シリーズ AP で、アップグレード後に 17.9 より前のソフトウェアを起動できない

Cisco Catalyst 9130 または 9124 AP を Cisco IOS XE 17.18.2、26.1.1、またはそれ以降のリリースにアップグレードすると、AP で Cisco IOS XE 17.9 より前のイメージを起動できません。Cisco AireOS 8.10 や Cisco IOS XE 17.3 などのイメージを起動しようとすると、失敗します。詳細については、CSCwv10846 を参照してください。

© 2026 Cisco and/or its affiliates. All rights reserved.

17.18.2、17.18.3、または 26.1.1 から開始した場合に Cisco CW9800L で ISSU 障害が発生する

問題：17.18.2、17.18.3、または 26.1.1 からの IOS XE リリースを実行している Cisco CW9800L ワイヤレスコントローラで、ISSU操作が失敗します（CSCwt98619 を参照）。

回避策：**install activate issu force** コマンドを使用して CLI でアップグレードを完了するか、GUI で [Override] オプションを使用します。

解決策：ネイティブ ISSU サポート（Catalyst Center 経由で強制フラグなし）は、リリース 17.18.4 と 26.1.2 で復元されます。

新規展開の場合：シスコは ISSU をサポートするために 17.18.2、17.18.3、26.1.1 でコールド SMU を公開します。

互換

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。詳細については、「Cisco Wireless Solutions Software Compatibility Matrix」を参照してください。

表 8. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、リリース 26.1.x の互換性マトリックス

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 Catalyst Center	Cisco CMX
IOS XE 26.1.x	3.4 3.3 3.2 3.1 3.0 * すべて最新パッチを適用済み	「Cisco Catalyst Center Compatibility Information」を参照	11.1.1

ソフトウェア要件

オペレーティング システム：

- Windows 10 以降
- macOS 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）

  Firefox バージョン 63.x はサポートされていません。

© 2026 Cisco and/or its affiliates. All rights reserved.

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 が枯渇する可能性があります。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。

```
Device# configure terminal
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。

```
Device(config)# service tcp-keepalives-in
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。

- アップグレードをスムーズに行い、AP での潜在的なブートループ問題を防止するには、次の Field Notice と技術文書を確認してください。アップグレードを開始する前にこれらのアクションを完了することが重要です。

  FN74383 : Field Notice

  Validate and Recover Catalyst APs on 17.12

- **Cisco IOS XE 17.18.3 から 26.1.1 へのアップグレード**：
  GCMP-256 暗号を使用して WPA3 Enterprise（非SuiteB）で設定した WLAN は、現在リリース 17.18.3 では Wi-Fi 7 でサポートされていますが、リリース 26.1.1 へのアップグレード時に管理上の理由でシャットダウンします。これは、バージョン 26.1.1 では GCMP-256 暗号が特定の WLAN タイプでサポートされていないために発生します。その結果、該当する WLAN はブロードキャストを停止し、アップグレード後すぐに使用できなくなります。

  該当する WLAN のタイプは以下のとおりです。

  ◦ GCMP-256 暗号を使用する WPA3 Enterprise（802.1X SHA256）

  ◦ GCMP-256 暗号を使用する WPA3 FT（802.1X）

  回避策：アップグレード後にこれらの WLAN のサービスを復元するには、該当する WLAN から GCMP-256 暗号設定を手動で削除する必要があります。設定を削除すると、WLAN は稼働状態に戻ります。

  アップグレード前に暗号の互換性を検証し、サービスの中断を避けてください。

- WAN リンクの背後のリモートサイトに AP がある場合は、イメージのダウンロードを高速化し、信頼性を高めるために、次のドキュメントをお読みください。
  https://www.cisco.com/c/ja_jp/support/docs/wireless/catalyst-9800-series-wireless-controllers/223125-understand-access-point-image-upgrades.html。

- Cisco IOS XE 17.9.5 以前または 17.12.2 以前から Cisco IOS XE 17.18.2 にアップグレードする場合、コントローラの WebUI は 1.5 GB を超えるイメージをサポートしません。

  回避策：

  ◦ CLI コマンドを使用してアップグレードします。または、

  ◦ 17.9.6、17.12.3 、またはそれ以降にアップグレードしてから、17.18.2 以降にアップグレードします。

© 2026 Cisco and/or its affiliates. All rights reserved.

- イメージの場合：17.9.6 以前、17.12.4 以前、または 17.15.1 以前から 17.18.2 にアップグレードする場合、Cisco Catalyst Wi-Fi 6 AP は、一時パーティションの空き容量不足によりイメージのアップグレードに失敗する可能性があります。

  回避策：

  ◦ 影響を受ける AP をパワーサイクルで再起動し、その後、通常どおりにアップグレードを続行します。

  詳細については、CSCwm08044 および CSCwm07499 を参照してください。

- 古いリリースコード（8.10.190.0、17.3.8、17.6.5、17.9.3 以前）を実行している AP では、WAN リンク経由でソフトウェアをアップグレードすると、ブートループに陥ることがあります。詳細については、https://www.cisco.com/c/ja_jp/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html を参照してください。

- 次の Wave 1 AP は 17.18.2 以降ではサポートされないため、コントローラに参加しません。アップグレードする前に、現在のモデルを検証することを推奨します。

  ◦ 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

- Cisco IOS XE Dublin 17.10.x 以降、キー交換および MAC アルゴリズム（diffie-hellman-group14-sha1、hmac-sha1、hmac-sha2-256、hmac-sha2-512 など）はデフォルトでサポートされておらず、これらのアルゴリズムのみをサポートする一部の SSH クライアントに影響を与える可能性があります。必要に応じて、手動でこれらを追加できます。これらのアルゴリズムを手動で追加する方法については、https://www.cisco.com/c/ja_jp/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html で「コモン クライテリア認定用の SSH アルゴリズム」を参照してください。

- 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。

  ◦ 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>
  ```

  ◦ **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
  ```

  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。

- クライアント認証用の RADIUS パケットのフラグメンテーションを引き起こす可能性のある、G0（OOB）インターフェイスでの 1500 未満の MTU の使用はサポートしていません。

- 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、以下に指定された順序で次のコマンドを実行します。

```
ip http session-module-list pkilist OPENRESTY_PKI
ip http active-session-modules pkilist
```

© 2026 Cisco and/or its affiliates. All rights reserved.

- 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。
- 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、ERR_SSL_VERSION_OR_CIPHER_MISMATCH を再生成することを推奨します。

  以下に指定された順序で次のコマンドを使用して、新しい自己署名トラストポイント証明書を生成します。

```
device# configure terminal
device(config)# no crypto pki trustpoint trustpoint_name
device(config)# no ip http server
device(config)# no ip http secure-server
device(config)# ip http server
device(config)# ip http secure-server
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。
- 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 Catalyst 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 Centralized Key Management（CCKM）機能は、Cisco IOS XE 17.10.x で廃止されましたが、現在もサポートされています。ただし、CCKM の今後のリリースでサポート対象外となります。そのため、802.1X 認証を使用した Fast Transition（FT）に移行し、サポートされているキー キャッシュ メカニズムで構成を検証することを推奨します。
- 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。

© 2026 Cisco and/or its affiliates. All rights reserved.

- Virtual Routing and Forwarding（VRF）を使用した RLAN はサポートされていません。
- 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。
- 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。
- コントローラのクロックをより早い時刻を反映するように変更するたびに、コントローラのリロードを実行することを推奨します。
- DTLS バージョン（DTLSv1.0）は、最新のセキュリティポリシーに基づいて Cisco Aironet 1800 で廃止されています。そのため、Cisco Aironet 1800 AP の新しいアウトオブボックス展開はコントローラに参加できず、次のエラーメッセージが表示されます。

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join,
AP <AP-name>,

mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

  新しい Cisco Aironet 1800 AP をオンボーディングし、CAPWAP 接続を確立するには、次の設定を使用して、コントローラで DTLS バージョンを明示的に 1.0 に設定します。

```
config terminal

ap dtls-version dtls_1_0

end
```

  注：DTLS バージョンを 1.0 に設定すると、既存のすべての AP CAPWAP 接続に影響します。メンテナンス時にのみ設定を適用することをお勧めします。AP が新しいイメージをダウンロードしてコントローラに参加したら、必ず設定を削除してください。

- ダウングレードプロセスを開始する前に、現在のバージョンに適用可能で、古いバージョンには適用できない設定を手動で削除する必要があります。これを行わないと、予期しない動作が発生する可能性があります。
- Cisco Catalyst 9800 シリーズ ワイヤレスコントローラの Field Programmable ハードウェアデバイス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』を参照してください。

Cisco IOS XE 26.1.x へのアップグレードパス

表 9. Cisco IOS XE Dublin 26.1.x へのアップグレードパス

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレード パス
16.10.x	– 注： Cisco Catalyst 9130 および 9124 AP は、16.10.x および 16.11.x リリースではサポートされていません。	最初に 16.12.5 または 17.3.x にアップグレードしてから、26.1.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、26.1.x にアップグレードします。

© 2026 Cisco and/or its affiliates. All rights reserved.

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレード パス
16.12.x	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	最初に 17.3.5 以降または 17.6.x 以降にアップグレードしてから、26.1.x にアップグレードします。
17.1.x	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	最初に 17.3.5 以降にアップグレードしてから、26.1.x にアップグレードします。
17.2.x	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	最初に 17.3.5 以降にアップグレードしてから、26.1.x にアップグレードします。
17.3.1 ～ 17.3.4	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.3.4c 以降	17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.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、26.1.x にアップグレードします。	26.1.x に直接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、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.6.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.7.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.8.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.9.1 ～ 17.9.5	17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.9.6 以降	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
17.10.x	17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.11.x	17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.x に直接アップグレードします。
17.12.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
17.13.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。

© 2026 Cisco and/or its affiliates. All rights reserved.

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレード パス
17.14.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
17.15.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
17.16.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
17.17.x	26.1.x に直接アップグレードします。	26.1.x に直接アップグレードします。
8.9.x または 8.10.171.0 より前の 8.10.x バージョン	最初に 8.10.171.0 以降、17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、26.1.x にアップグレードします。	26.1.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。

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 26.1.x

イメージ名（9800-80、9800-40、および 9800-L）：

- C9800-80-universalk9_wlc.26.01.x.SPA.bin
- C9800-40-universalk9_wlc.26.01.x.SPA.bin
- C9800-L-universalk9_wlc.26.01.x.SPA.bin

イメージ名（CW9800M、CW9800H1/CW9800H2、CW9800L）

- CW9800H-wlc-universalk9.26.01.x.SPA.bin
- CW9800M-wlc-universalk9.26.01.x.SPA.bin
- CW9800L-wlc-universalk9.26.01.x.SPA.bin

イメージ名（9800-CL）：

- クラウド：C9800-CL-universalk9.26.01.x.SPA.bin

© 2026 Cisco and/or its affiliates. All rights reserved.

- **Hyper-V/ESXi/KVM**：C9800-CL-universalk9.26.01.x.iso、C9800-CL-universalk9.26.01.x.ova
- **KVM**：C9800-CL-universalk9.26.01.x.qcow2
- **NFVIS**：C9800-CL-universalk9.26.01.x.tar.gz

ソフトウェア インストール コマンド

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。

コマンド	説明
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 キーワードは、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

Cisco Wireless ライセンス

Cisco Networking Subscription ライセンスモデルの一部である Cisco Wireless ライセンスは、Wi-Fi 7 アクセスポイントをオンプレミスネットワーク、ハイブリッドネットワーク、またはクラウド マネージド ネットワークに展開するのに役立つソフトウェアライセンスです。Cisco IOS XE 17.15.2 以降、Cisco Wireless ライセンスは Wi-Fi 7 アクセスポイント（AP）およびそれ以降のモデルでサポートされています。

Cisco Wireless ライセンスは、次の階層で構成しています。

- Cisco Wireless Essentials：ネットワークの管理に不可欠な基本的な機能を提供する階層です。
- Cisco Wireless Advantage：追加の機能と能力をサポートし、ネットワークを管理するための高度な機能に加えて、必要不可欠なすべての機能を提供する階層です。

詳細については、「Cisco Wireless Licensing」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。

© 2026 Cisco and/or its affiliates. All rights reserved.

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 26.1.x
シスコ ワイヤレス コントローラ	「サポートされるハードウェア」を参照
アクセスポイント	「サポート対象の AP」を参照
無線機	• 802.11ac • 802.11ax • 802.11a • 802.11g • 802.11n • 802.11be（Wi-Fi 7）
セキュリティ	オープン、PSK（WPA2-AES）、802.1X（WPA2-AES）（EAP-FAST、EAP-TLS）、WPA3 AKM
RADIUS	「互換性マトリックス」を参照
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	MacOS Sierra 10.12.6
Apple MacBook Air 13 inch	MacOS High Sierra 10.13.4
MacBook Pro Retina	MacOS Catalina
MacBook Pro Retina 13 inch early 2015	MacOS Mojave 10.14.3
MacBook Pro OS X	MacOS X 10.8.5
MacBook Air	MacOS Sierra v10.12.2
MacBook Air 11 inch	MacOS Yosemite 10.10.5
MacBook M1 チップ	MacOS Catalina
MacBook M1 チップ	MacOS Ventura 13.2.1

© 2026 Cisco and/or its affiliates. All rights reserved.

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
MacBook Pro M2 チップ	MacOS Ventura 13.3 ベータ版
MacBook Pro M2 チップ	MacOS Ventura 13.1
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
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 Pro（12.9 インチ）第 6 世代	iOS 16.4
Apple iPad Pro（11 インチ）第 4 世代	iOS 16.4
Apple iPad 2021	iOS 15.0

© 2026 Cisco and/or its affiliates. All rights reserved.

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 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
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 16.0
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Mini Pro	iOS 15.1

© 2026 Cisco and/or its affiliates. All rights reserved.

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 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 Phone 8821	11.0.6 SR4
Drager Delta	VG9.0.2
Drager M300.3	VG3.0
Drager M300.4	VG3.0
Drager M540	VG4.2
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
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
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 Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0

© 2026 Cisco and/or its affiliates. All rights reserved.

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 S22 Ultra	Android 13.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
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
Spectralink Versity Phones 9540 シリーズ	Android 8.1.0
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
Zebra TC57	Android 10.0

© 2026 Cisco and/or its affiliates. All rights reserved.

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 TC58	Android 11.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	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 5.2
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 6.2
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 AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8、v22.190.0.4
Intel AX 210	Driver v22.230.0.8、v22.190.0.4、v22.170.2.1
Intel AX 200	Driver v22.130.0.5
Intel 11AC	Driver v22.30.0.11
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901
PhoenixContact FL WLAN 2010	ファームウェアバージョン：2.71

© 2026 Cisco and/or its affiliates. All rights reserved.

サポートされるハードウェア

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

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、「サポートされる PID およびポート」を参照してください）。

表 12. 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。
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 9800 シリーズ 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。
Catalyst 9000 シリーズ スイッチに組み込まれた Embedded Wireless Controller	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。
Cisco CW9800 シリーズ ワイヤレス コントローラ（CW9800M、CW9800H1、CW9800H2、および CW9800L）	CW9800M コントローラは、次世代の Cisco CW9800 シリーズ ワイヤレス LAN コントローラであり、前世代のモデルと比較して、パフォーマンスが 53% 向上し、消費電力が 18% 削減されます。 さらに、CW9800M コントローラは 3,000 個の AP と 32,000 個のクライアントをサポートし、ビジネスクリティカルなネットワークのパフォーマンスと拡張性を向上させます。スペースを節約し、データセンターの柔軟性を高めるように設計されたシングル RU でありながら、通常のパケットと暗号化されたパケットの両方に対して最大 40 Gbps の転送スループットを実現します。
	CW9800H1 および CW9800H2 コントローラは、次世代の Cisco CW9800 ワイヤレス LAN コントローラであり、以前の製品と比較して、パフォーマンスが最大 36% 向上し、消費電力が最大 40% 削減されます。 さらに、CW9800H1 および CW9800H2 モデルは、省スペースのシングル RU 設計で構築されており、最大 6,000 の AP と 64,000 のクライアントをサポートし、最大スループットは 100 Gbps です。また、4 X 25 Gbps（CW9800H1）または 2 X 40 Gbps（CW9800H2）構成のアップリンクを選択して、次世代ワイヤレス要件における高スループットの要求に対応できます。

© 2026 Cisco and/or its affiliates. All rights reserved.

プラットフォーム	説明
	CW9800L 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、次世代のローエンドコントローラです。CW9800L は、最大 10 Gbps のスループット、500 個の AP、および 10,000 個のクライアントをサポートし、ベースとなる C9800-L に比べて 2 倍のキャパシティとパフォーマンスの向上をもたらします。

サポートされているホスト環境：パブリッククラウドとプライベートクラウド

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 13. 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	ソフトウェアのバージョン
VMware ESXi	• VMware ESXi vSphere 6.5、6.7、7.0 および 8.0 • VMware ESXi vCenter 6.5、6.7、7.0 および 8.0
KVM	• Red Hat Enterprise Linux 9.2 または最新バージョンをベースとした Linux KVM • Ubuntu 16.04.5 LTS、Ubuntu 18.04.5 LTS、Ubuntu 20.04.5 LTS
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 Server 2019、Windows Server 2025、Hyper-V マネージャ（バージョン 10.0.x）
Microsoft Azure	Microsoft Azure

サポートされる PID およびポート

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。

注：サポートされていない SFP はポートをダウンさせます。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 14. サポートされる 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）

© 2026 Cisco and/or its affiliates. All rights reserved.

コントローラモデル	説明
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）
C9800-L-C-K9	• 2.5/1 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
C9800-L-F-K9	• 2.5/1 ギガビットポート x 4 • 10/1 ギガビット ポート x 2
CW9800H1	• 1 GE/10 GE SFP ポート X 8 • 25 GE SFP インターフェイス X 4
CW9800H2	• 1 GE/10 GE SFP ポート X 8 • 40 GE QSFP インターフェイス X 2
CW9800M	• 内蔵 1 GE/10 GE SFP ポート X 4 • 組み込み 25 GE SFP ポート X 2
CW9800L	• 10G/1G SFP ポート（データポート）X 2 • 1G 銅線（RP および SP ポート）X 2

サポートされる SFP

次の表に、サポートされる SFP モデルを示します。

表 15. サポートされる SFP モデル

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
COLORCHIP-C040-Q020-CWDM4-03B	サポート対象	–	–	–	–	–	–
DWDM-SFP10G-30.33	サポート対象	サポート対象	–	–	–	–	–
DWDM-SFP10G-61.41	サポート対象	サポート対象	–	–	–	–	–
FINISAR-LR – FTLX1471D3BCL （FINISAR SFP はシスコ固有ではなく、DOM などの一部の機能が正しく動作しない場合があります。）	サポート対象	サポート対象	サポート対象	–	–	–	–
FINISAR-SR – FTLX8574D3BCL	サポート対象	サポート対象	サポート対象	–	–	–	–
GLC-BX-D	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–
GLC-BX-U	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
GLC-EX-SMD	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	–
GLC-LH-SMD	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象
GLC-SX-MMD	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
GLC-T	サポート対象	–	–	–	–	–	–
GLC-TE	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
GLC-ZX-SMD	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–
QSFP-100G-LR4-S	サポート対象	–	–	–	–	–	–
QSFP-100G-SR4-S	サポート対象	–	–	–	–	–	–
QSFP-40G-BD-RX	サポート対象	–	–	サポート対象	サポート対象	サポート対象	–
QSFP-40G-ER4	サポート対象	–	–	–	サポート対象	–	–
QSFP-40G-LR4	サポート対象	–	–	–	サポート対象	–	–
QSFP-40G-LR4-S	サポート対象	–	–	–	サポート対象	–	–
QSFP-40G-LR4-S-RF			–	サポート対象	サポート対象	サポート対象	–
QSFP-40G-CSR4	–	–	–	–	サポート対象	–	–
QSFP-40G-SR4	サポート対象	–	–	–	サポート対象	–	–
QSFP-40G-SR4-S	サポート対象	–	–	–	サポート対象	–	–
QSFP-40G-SR-BD	–	–	–	サポート対象	サポート対象	サポート対象	–
QSFP-40GE-LR4	サポート対象	–	–	–	–	–	–
QSFP-H40G-ACU7M	–	–	–	サポート対象	サポート対象	サポート対象	–

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
QSFP-H40G-ACU10M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU1M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU2M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU3M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU4M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU5M	–	–	–	–	サポート対象	–	–
QSFP-H40G-CU0-5M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC1M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC2M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC3M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC5M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC7M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC10M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC15M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC20M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC25M	–	–	–	–	サポート対象	–	–
QSFP-H40G-AOC30M	–	–	–	–	サポート対象	–	–
SFP-10G-AOC10M	サポート対象	サポート対象	–	–	–	–	サポート対象
SFP-10G-AOC1M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-AOC2M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-10G-AOC3M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-AOC5M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-AOC7M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-BXD-I				サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-BXU-I				サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-CSR-S				サポート対象	サポート対象	サポート対象	–
SFP-10G-ER	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	–
SFP-10G-LR	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-LR-I			–	サポート対象	サポート対象	サポート対象	–
SFP-10G-LR-S	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-LR-X	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–
SFP-10G-LRM	サポート対象	サポート対象	サポート対象	–	–	–	–
SFP-10G-SR	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-S	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-I	–	–	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-X	サポート対象	サポート対象	サポート対象	–	–	–	–
SFP-10G-ZR			–	サポート対象	サポート対象	サポート対象	–
SFP-10G-ZR-I	–	–	–	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-T-X	–	–	–	サポート対象	サポート対象	サポート対象	–

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-25G-CSR-S	–	–	–	サポート対象	サポート対象	サポート対象	–
SFP-25G-SR-S	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-ER-I	–	–	–	サポート対象	–	サポート対象	–
SFP-10/25G-LR-I	–	–	–	サポート対象	–	サポート対象	–
SFP-10/25G-LR-S	–	–	–	サポート対象	–	サポート対象	–
SFP-10/25G-CSR-S	–	–	–	サポート対象	–	サポート対象	–
SFP-10/25G-BXD-I	–	–	–	サポート対象	–	サポート対象	サポート対象
SFP-10/25G-BXU-I	–	–	–	サポート対象	–	サポート対象	サポート対象
SFP-H25G-CU1M	–	–	–	サポート対象	–	サポート対象	–
SFP-H25G-CU5M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC1M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC2M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC3M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC5M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC7M	–	–	–	サポート対象	–	サポート対象	–
SFP-25G-AOC10M	–	–	–	サポート対象	–	サポート対象	–
SFP-H10GB-ACU10M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-ACU7M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU1.5M	サポート対象	サポート対象	サポート対象	–	–	–	–

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-H10GB-CU1M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–
SFP-H10GB-CU2.5M	サポート対象	サポート対象	サポート対象	–	–	–	サポート対象
SFP-H10GB-CU2M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	–
SFP-H10GB-CU3M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU5M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU1-5M	サポート対象	サポート対象	–	サポート対象	サポート対象	サポート対象	–
SFP-H10GB-CU2-5M				サポート対象	サポート対象	サポート対象	
Finisar-LR（FTLX1471D3BCL）	–	–	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Finisar-SR（FTLX8574D3BC）	–	–	–	サポート対象	サポート対象	サポート対象	サポート対象

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、次のロケーションにある表を参照してください。

https://www.cisco.com/c/ja_jp/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

ネットワークプロトコルとポートマトリックス

表 16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ - ネットワークプロトコルとポートマトリックス

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	22	任意	SSH
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	23	任意	Telnet
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	80	任意	HTTP

© 2026 Cisco and/or its affiliates. All rights reserved.

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	任意	HTTPS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	161	任意	SNMP エージェント
任意	任意	UDP	5353	5353	mDNS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	69	69	TFTP
任意	DNS Server	UDP	53	任意	DNS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	830	任意	NetConf
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	任意	REST API
任意	WLC プロトコル	UDP	1700	任意	CoA パケットを受信
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5246	任意	CAPWAP 制御
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5247	任意	CAPWAP データ
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5248	任意	CAPWAP MCAST
AP	Cisco Catalyst Center	TCP	32626	任意	インテリジェントキャプチャと RF テレメトリ
AP	AP	UDP	16670	任意	クライアントポリシー（AP-AP）
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	16666	16666	モビリティ制御
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	SNMP	UDP	162	任意	SNAMPトラップ

© 2026 Cisco and/or its affiliates. All rights reserved.

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	RADIUS	UDP	1812/1645	任意	RADIUS 認証
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	RADIUS	UDP	1813/1646	任意	RADIUS ACCT
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TACACS+	TCP	49	任意	TACACS+
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	16667	16667	モビリティ
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	NTP サーバー	UDP	123	任意	NTP
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Syslog サーバー	UDP	514	任意	SYSLOG
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	HTTPS	8443	任意	アウトオブバンド AP イメージのダウンロード Cisco CleanAir スペクトル キャプチャ
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	NetFlow サーバー	UDP	9996	任意	NetFlow
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Connected Mobile Experiences（CMX）	UDP	16113	任意	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	32222	任意	デバイス検出
Cisco Catalyst Center	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	25103	任意	テレメトリ サブスクリプション

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。

© 2026 Cisco and/or its affiliates. All rights reserved.

表 17. サポート対象の AP

AP タイプ	AP 名
屋内用アクセスポイント	• Cisco Catalyst 9105AX（I/W）アクセスポイント • Cisco Catalyst 9115AX（I/E）アクセスポイント • Cisco Catalyst 9120AX（I/E/P）アクセスポイント • Cisco Catalyst 9130AX（I/E）アクセスポイント • Cisco Catalyst 9136AX アクセス ポイント • Cisco Catalyst 9162（I）シリーズ アクセスポイント • Cisco Catalyst 9164（I）シリーズ アクセスポイント • Cisco Catalyst 9166（I/D1）シリーズ アクセスポイント • Cisco Wireless 9171（I）シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9172（I/H）シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9174（I/E）シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9176（I/D1）シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9178（I）シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9179（F）シリーズ Wi-Fi 7 アクセスポイント • Cisco Aironet 1815（I/W/M/T）、1830（I）、1840（I）、および 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（I）シリーズ アクセスポイント
屋外用アクセスポイント	• Cisco Aironet 1540（I/D）シリーズ アクセスポイント • Cisco Aironet 1560（I/D/E）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/E）アクセスポイント • Cisco Catalyst 9163（E）シリーズ アクセスポイント • Cisco Catalyst Industrial Wireless 9167（I/E）Heavy Duty アクセスポイント • Cisco Catalyst Industrial Wireless 9165E 高耐久性アクセスポイント • Cisco Catalyst Industrial Wireless 9165D Heavy Duty 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	Cisco Wi-Fi インターフェイスモジュール（WIM） - WP-WIFI6-x

サポートされている AP 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/wireless/catalyst-9100ax-access-points/products-technical-

© 2026 Cisco and/or its affiliates. All rights reserved.

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 Access Points Supported in Cisco Wireless Controller Platform Software Releases」を参照してください。

関連情報

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

In-Service Software Upgrade Matrix

Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

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

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ データシート：

データシートリスト

ワイヤレス製品の比較

Compare specifications of Cisco wireless APs and controllers

Wireless LAN Compliance Lookup

Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix

シスコ アクセスポイント：揮発性に関する報告：

揮発性に関する報告は、デバイス、メモリコンポーネントの位置、およびデバイスメモリのクリア方法に関する情報を提供するエンジニアリング ドキュメントです。組織のデータセキュリティポリシーとプラクティスを参照し、デバイスまたはネットワーク環境を保護するために必要な手順を実行できます。

Cisco Aironet および Catalyst AP の揮発性に関する報告（SoV）のドキュメントは、Cisco Trust Portal で入手できます。

AP モデルで検索して SoV ドキュメントを表示できます。

Cisco Prime Infrastructure：

Cisco Prime Infrastructure マニュアル

Cisco Spaces：

Cisco Spaces ドキュメント

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst Center：

Cisco Catalyst Center のマニュアル

製品分析

Cisco Enterprise Networking Product Analytics Frequently Asked Questions

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 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 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 DevNet 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。

シスコバグ検索ツール

シスコのバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

法的情報

Cisco および Cisco ロゴは、シスコ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/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、シスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2026 Cisco Systems, Inc. All rights reserved.

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。