

Cisco IOS XE Cupertino 17.9.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

最終更新：2024 年 8 月 19 日

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Cisco IOS XE Cupertino 17.9.x のリリースノート

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ク機能とを統合して、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。

- コントローラには、高可用性、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 (SDA 展開用) 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 Catalyst Center、プログラマビリティ インターフェイス (NETCONF/YANG など)、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 デベロッパーサポートを通じて、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 17.9.5 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
Catalyst コントローラのクラウドモニタリング	<p>Catalyst コントローラのクラウドモニタリング機能は、Meraki ダッシュボードを使用してワイヤレスコントローラをモニターするのに役立ちます。現在、この機能は限定的なカスタマーベータ版であり、Cisco TAC ではサポートされていません。</p> <p>この機能の詳細については、「Cloud Monitoring for Catalyst」を参照してください。</p> <p>さらにサポートが必要な場合は、メーカーリスト (c9800-dashboard-monitoring@external.cisco.com) までお問い合わせください。</p>

機能名	説明とドキュメントのリンク
セキュアな固有デバイス識別子 (SUDI) 証明書のトラストポイントの変更	

機能名	説明とドキュメントのリンク
	<p>Cisco IOS XE 17.9.5以降、トラストポイントに次の変更が導入されています。</p> <ul style="list-style-type: none"> 既存の SUDI 証明書のトラストポイント名 デバイスで Cisco Manufacturing CA III 証明書がサポートされていて、無効になっていない場合、トラストポイント名は次のようになります。 <ul style="list-style-type: none"> Cisco Manufacturing CA III 証明書の場合、トラストポイント名は CISCO_IDEVID_SUDI から CISCO_IDEVID_CMCA3_SUDI に変更されました。 Cisco Manufacturing CA SHA2 証明書の場合、トラストポイント名は CISCO_IDEVID_SUDI_LEGACY から CISCO_IDEVID_CMCA2_SUDI に変更されました。 <p>デバイスで Cisco Manufacturing CA III 証明書がサポートされていない場合、または no platform sudi cmca3 コマンドを使用して証明書を無効にしている場合、トラストポイント名は次のようになります。</p> <ul style="list-style-type: none"> Cisco Manufacturing CA SHA2 証明書の場合、トラストポイント名は CISCO_IDEVID_SUDI から CISCO_IDEVID_CMCA2_SUDI に変更されました。 Cisco Manufacturing CA 証明書の場合、トラストポイント名は CISCO_IDEVID_SUDI_LEGACY から CISCO_IDEVID_CMCA_SUDI に変更されました。 <ul style="list-style-type: none"> ハードウェア SUDI 証明書 <ul style="list-style-type: none"> デバイスが High Assurance SUDI CA 証明書をサポートしている場合、この証明書は CISCO_IDEVID_SUDI トラストポイントの下にロードされます。 デバイスが High Assurance SUDI CA 証明書をサポートしていない場合、ACT2 SUDI CA 証明書は CISCO_IDEVID_SUDI トラストポイントの下にロードされます。 show wireless management trustpoint コマンドの出力 ワイヤレス展開用に Cisco Catalyst 9300 シリーズ スイッチを Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとともに使用する場合、show wireless management trustpoint コマンドの出力のトラストポイント名は、前述の変更されたトラストポイント名に更新されます。

機能名	説明とドキュメントのリンク
	<p>次の例は、show wireless management trustpoint コマンドのサンプル出力を示しています。デバイスで Cisco Manufacturing CA III 証明書がサポートされていない場合、または証明書が無効になっている場合は、次の出力のように、トラストポイント名は CISCO_IDEVID_CMCA2_SUDI と表示されます。</p> <pre>Device# show wireless management trustpoint Trustpoint Name : CISCO_IDEVID_CMCA3_SUDI Certificate Info : Available Certificate Type : MIC Certificate Hash : <SHA1 - hash> Private key Info : Available FIPS suitability : Not Applicable</pre> <ul style="list-style-type: none"> • show ip http server status コマンドの出力 <p>HTTP サーバーのトラストポイントを CISCO_IDEVID_SUDI として設定した場合、show ip http server status コマンドの出力には、設定されたトラストポイントとともに動作中のトラストポイントが表示されます。</p> <p>次に、設定されたトラストポイント名と動作中のトラストポイント名の両方を含む、show ip http server status コマンドの出力例を示します。デバイスで Cisco Manufacturing CA III 証明書がサポートされていない場合、または証明書が無効になっている場合は、次の出力のように、動作中のトラストポイントは CISCO_IDEVID_CMCA2_SUDI と表示されます。</p> <pre>Device# show ip http server status ... HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI</pre>

Cisco IOS XE Cupertino 17.9.4a の新機能

このリリースに新機能はありません。このリリースでは、[CSCwh87343](#) : Cisco IOS XE ソフトウェアの Web UI における特権昇格の脆弱性が修正されています。詳細については、「Security Advisory: [cisco-sa-iosxe-webui-privesc-j22SaA4z](#)」を参照してください。

Cisco IOS XE Cupertino 17.9.4 の新機能

表 2: 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
アラブ首長国連邦の ROW サポート	このリリースから、ROW ドメイン国コードのアラブ首長国連邦 (AE) が Cisco Catalyst IW9167E Heavy Duty アクセスポイントでサポートされます。
製品分析	<p>この機能により、シスコ製品の非個人の使用デバイスシステム情報を収集でき、製品の継続的な改善に役立ちます。この機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ (9800-80、9800-40、9800-L、および 9800-CL) でサポートされます。 pae コマンドを使用して、この機能を有効または無効にすることができます。</p> <p>この機能の一部として、次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • pae • show product-analytics kpi • show product-analytics report • show product-analytics stats <p>(注) スマート ライセンス デバイス システム情報をオフにしても、Cisco Catalyst Center や vManage などの他のシステム情報収集には影響しません。</p> <p>重要: シスコは、製品とサービスの向上に常に取り組んでいます。この目標を達成するには、お客様の当社製品の使用方法を知ることが重要です。そのため、シスコは、製品およびカスタマーエクスペリエンスの改善、分析、および導入のために、Cisco Smart Software Manager (CSSM) を介してデバイスおよびライセンスシステム情報を収集します。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お客様のデータを処理します。デバイスおよびライセンスシステム情報に関する組織の設定を変更するには、pae コマンドを使用します。『Cisco Catalyst 9800 Series Wireless Controller Command Reference』 → 「pae」を参照してください。</p> <p>この機能の詳細については、こちらを参照してください。</p>

Cisco IOS XE Cupertino 17.9.3 の新機能

表 3: 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 IW9167E Heavy Duty アクセスポイント	Cisco Catalyst IW9167E Heavy Duty アクセスポイントはこのリリースからサポートされ、Wi-Fi 6 AP または Cisco Ultra-Reliable Wireless Backhaul として動作できます。
サイトのロードバランシング	この機能では、サイトの負荷を指定して、より適切なロードバランシングを実現できます。 詳細については、「 Enhanced Site Tag-Based Load Balancing 」を参照してください。
プライベートクラウドでの Cisco Catalyst 9800-CL を使用した KVM/SUSE バージョン 15 SP3 のサポート	KVM/SUSE バージョン 15 SP3 で実行する Cisco Catalyst 9800-CL の SDA ワイヤレス展開に対する限定的なサポート。
Wave 1 アクセスポイント	次の Wave 1 AP のサポートが、今回のリリースから再導入されました。 <ul style="list-style-type: none"> • 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 <p>(注)</p> <ul style="list-style-type: none"> • 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。 <p>Wave 1 AP のサポートの詳細については、FAQ を参照してください。</p>

Cisco IOS XE Cupertino 17.9.2 の新機能

表 4: 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
APプライミングプロファイルを使用したコントローラへの AP フォールバック	<p>この機能は、正規表現 (regex) に一致する AP のグループ、またはプライミングプロファイルを使用する個々の AP のプライマリ、セカンダリ、およびターシャリコントローラを設定するのに役立ちます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • primary (ap prime) • secondary (ap prime) • tertiary (ap prime) • priming-override • profile (prime-filter) • wireless profile ap priming • show ap filters active type priming • show ap filters all type priming • show wireless profile ap priming all • show wireless profile ap priming summary <p>詳細については、「AP Fallback to Controllers Using AP Priming Profile」の章を参照してください。</p>
Cisco Catalyst 9136 シリーズ アクセスポイントおよび Cisco Catalyst 916x シリーズ アクセスポイントの国別コンプライアンスサポート	<p>Cisco Catalyst 916x シリーズ アクセスポイントおよび Cisco Catalyst 9136 シリーズ アクセスポイントでは、さらに 75 カ国がサポートされています。</p> <p>サポートされている国のリストの詳細については、「Regulatory Compliance Domain」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
<p>ワイヤレスクライアントの IPv6 アドレストラッキング</p>	<p>Cisco IOS XE 17.9.1 まで、コントローラはワイヤレスクライアントごとに最大 8 つの IPv6 アドレスをサポートしていました。ワイヤレスクライアントに対して 8 つの IPv6 アドレスが学習された後、コントローラは、新しい IPv6 送信元アドレスを持つワイヤレスクライアントのデータトラフィックをドロップしました。</p> <p>ただし、Cisco IOS XE 17.9.2 では、コントローラは、それぞれのワイヤレスクライアントに対して 8 つのアドレスが学習された後でも、新しい IPv6 送信元アドレスを持つワイヤレスクライアントのデータトラフィックを許可します。コントローラは、ワイヤレスクライアントの制御トラフィック (IPv6 NS/NA および DHCPv6) からワイヤレスクライアントの新しい IPv6 アドレスを学習し続けますが、ワイヤレスクライアントごとに最大 8 つの (最新の) アドレスのみを追跡します。</p> <p>(注) Cisco IOS XE 17.9.2 では、コントローラが 8 つの IPv6 アドレス制限を超えるアドレストラッキングなしで IPv6 トラフィックを許可するため、ユーザー定義ネットワーク、iPSK ピアツーピアブロッキング、ワイヤレス管理、ネイバー探索抑制、IP 盗難検出などの機能の一部は、8 つ以上のアドレスを使用するワイヤレスクライアントでは機能しない場合があります。Cisco IOS XE 17.9.2 イメージのロード時に IP ソースガード 機能を有効にすることで、新しい動作を無効にすることができます。</p> <p>次のコマンドがサポートされています。</p> <p>wireless ipv6 nd ns-forward</p> <p>詳細については、「IPv6 Client IP Address Learning」の章を参照してください。</p>
<p>Cisco Catalyst 9162I シリーズ Wi-Fi 6E アクセスポイントのサポート</p>	<p>Cisco IOS XE Cupertino 17.9.2 以降、Cisco Catalyst 9162I シリーズ Wi-Fi 6E アクセスポイントがサポートされます。</p>
<p>-E 規制ドメインの空港気象ドップラーレーダーチャンネル 120、124、128 のサポート</p>	<p>-E 規制ドメイン空港気象ドップラーレーダー (Terminal Doppler Weather Radar (TDWR)) チャンネル 120、124、および 128 は、次の AP でサポートされています。</p> <ul style="list-style-type: none"> • Cisco Catalyst 9124 シリーズ アクセスポイント • Cisco Catalyst 9130 シリーズ アクセスポイント

機能名	説明とドキュメントのリンク
UK Cisco Catalyst 9136I および Cisco Wireless 916xI アクセスポイントの ROW 規制ドメインの UNII-3 帯域	<p>Cisco IOS XE Cupertino 17.9.2 以降、UNII-3 チャンネルは、Cisco Catalyst 9136I および Cisco Wireless 916xI アクセスポイントの -ROW ドメインの下の国コード GB に対して有効になります。これらの非動的周波数選択 (DFS) チャンネルの最大 Tx 電力は 23dBm です。</p> <p>この機能は、Cisco IOS XE Cupertino 17.9.2 にアップグレードすると自動的に有効になります。アップグレード後にチャンネルリスト情報を確認するには、show controllers dot11Radio コマンドを使用します。</p>
Identity PSK による Wi-Fi Protected Access 3 Simultaneous Authentication of Equals Hash-to-Element のサポート	<p>Cisco IOS XE Cupertino 17.9.2 以降、ローカルモードでの SAE H2E 認証で iPSK パスフレーズがサポートされます。クライアント SAE 認証中に、RADIUS サーバーのクライアント認証ポリシーで構成された ID 事前共有キー (iPSK) パスフレーズが、WLAN プロファイルのパスフレーズに置き換わります。したがって、個人に一意の事前共有キーを使用することは、WLAN 内のすべてのユーザーに共通キーを使用するよりも、より安全で詳細な認証スキームと見なされます。認証ポリシーで iPSK パスフレーズが設定されていない場合、SAE H2E は WLAN プロファイルのパスフレーズにフォールバックします。</p> <p>詳細については、「Wi-Fi Protected Access 3」の章を参照してください。</p>
VMware vSphere vMotion のサポート	<p>VMware vSphere vMotion は、クラウド向け Cisco Catalyst 9800 ワイヤレスコントローラでサポートされています。詳細については、https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-wireless-controllers-cloud/218438-verify-support-vmware-vsphere-vmotion-wi.html#anc6 および https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-wirel-cloud-dep-guide-cte-en.html を参照してください。</p>

MIB

以下の MIB が新たに追加または変更されました。

- CISCO-ENVMON-MIB

Cisco IOS XE Cupertino 17.9.1 の新機能

表 5: 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
SAE (FT-SAE) 認証クライアントの 802.11r Fast Transition	<p>このリリースから、Fast Transition は、PMK キャッシングとともに SAE ベースの高速ローミングをサポートします。</p> <p>次のコマンドが導入されました。</p> <ul style="list-style-type: none"> • security wpa akm ft sae <p>詳細については、「802.11r BSS Fast Transition」の章を参照してください。</p>
Cisco Catalyst 9136 シリーズ アクセスポイント、Cisco Catalyst 9164 シリーズ Wi-Fi 6E アクセスポイント、および Cisco Catalyst 9166 シリーズ Wi-Fi 6E アクセスポイントでのアクセスポイント調査モードのサポート	<p>このリリースでは、ap-type survey コマンドを使用して AP を調査モードに切り替えることができます。AP GUI も、調査モードをサポートするように拡張されています。</p> <p>この機能は、Cisco Catalyst 9136 シリーズ AP、Cisco Catalyst 9164 シリーズ Wi-Fi 6E AP、および Cisco Catalyst 9166 シリーズ Wi-Fi 6E AP でサポートされています。</p> <p>詳細については、「Access Points Survey Mode」の章を参照してください。</p>
SSO ペアのスタンバイユニットの RADIUS サーバーと TACACS+ サーバーの両方に対する認証とアカウントリングのサポート	<p>このリリースから、認証とアカウントリングは、RMI インターフェイスを使用するスタンバイ HA ユニットの RADIUS および TACACS+ サーバーでサポートされます。</p> <ul style="list-style-type: none"> • RADIUS アカウントリング • TACACS+ 認証 • TACACS+ アカウントリング <p>詳細については、「Redundancy Management Interface」の章を参照してください。</p>
BLE 同時スキャンとビーコン	<p>このリリースから、BLE の同時スキャンとビーコンは、基本モードまたは Cisco IOx モードの Cisco Catalyst Wi-Fi 6 AP でサポートされます。AP の BLE 無線は、ビーコン送信のスキャンを停止し、ビーコン送信の完了後にスキャンに戻ることができます。</p> <p>詳細については、「Cisco Hyperlocation」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
RADIUS アカウンティングの Chargeable User Identity	<p>Chargeable User Identity (CUI) は、ネットワークにアクセスするクライアントの一意の識別子です。この属性は、認証プロセスの一部として、クライアントのユーザー名の代わりに使用できます。</p> <p>次のコマンドが導入されました。</p> <ul style="list-style-type: none"> • access-session wireless cui-enable <p>詳細については、「RADIUS Accounting」の章を参照してください。</p>
Cisco AI-Enhanced RRM の Wi-Fi 6E サポート	<p>このリリースから、Cisco DNA Center の Cisco の AI-Enhanced RRM 機能は Wi-Fi 6E をサポートします。</p> <p>詳細については、「Radio Resource Management」の章を参照してください。</p>
2.4 GHz および 5 GHz 帯域での CleanAir Pro Scanning のサポート	<p>CleanAir Pro Scanning 機能は、2.4 GHz および 5 GHz 帯域の非 Wi-Fi 干渉のさまざまなカテゴリを監視して報告します。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • ap dot11 6ghz cleanair • ap dot11 cleanair alarm air-quality • ap dot11 cleanair alarm device cont-tx • ap dot11 cleanair alarm unclassified <p>詳細については、「CleanAir」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
Cisco Catalyst アクセスポイントでのワークグループブリッジワイヤレスクライアントの同時無線サポート	<p>このリリース以降、ワークグループブリッジは、アップリンク（バックホール）接続用の1つの無線と、ワイヤレスクライアントにサービスを提供するための別の無線をサポートします。この機能は、Cisco Catalyst 9105 AP、Cisco Catalyst 9115 AP、および Cisco Catalyst 9120 AP でサポートされています。</p> <p>次のコマンドが AP コンソールに導入されました。</p> <ul style="list-style-type: none"> • configure ssid-profile ssid dtim-period • configure dot11Radio wlan add • configure dot11Radio wlan delete • configure dot11Radio channel • configure dot11Radio beacon-interval • configure radius address port • configure qos profile • configure ssid-profile ssid qos profile <p>詳細については、「Workgroup Bridges」の章を参照してください。</p>
ロケーショングループを使用した mDNS ロケーションベースのフィルタリングの設定	<p>このリリースから、mDNS の AP グループ化が拡張され、AP ロケーションが含まれるようになりました。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • wireless rule application mdns • group-method <p>詳細については、「Multicast Domain Name System」の章を参照してください。</p>
AP コンソールの構成	<p>この機能により、コントローラから AP コンソールを構成できます。</p> <p>次のコマンドが導入されました。</p> <ul style="list-style-type: none"> • console <p>詳細については、「Configuring the AP Console」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
Cisco Catalyst 9166I シリーズ Wi-Fi 6E アクセスポイントでのフレキシブル ラジオ アサインメントのサポート	<p>このリリース以降、Cisco Catalyst 9166I シリーズ Wi-Fi 6E アクセスポイントのデュアルバンドラジオは、同じ AP のモニターまたはスニファとして、5 GHz または 6 GHz 帯域でサービスを提供する機能を提供します。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • ap fra 5-6ghz • ap fra 5-6ghz freeze • ap fra 5-6ghz interval • ap dot11 6ghz rf-profile • client-aware-fra • show ap fra 5-6ghz <p>詳細については、「Cisco Flexible Radio Assignment」の章を参照してください。</p>
アプリケーション セントリック インフラストラクチャ (ACI) ネットワークの高可用性展開	<p>この機能は、次の機能を使用して、古いアクティブコントローラと新しいアクティブコントローラ間のトラフィックのインターリーブを回避します。</p> <ul style="list-style-type: none"> • ワイヤレス管理インターフェイス (WMI) をより迅速に停止します。 • 高速スイッチオーバー通知を無効にします。 <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • no redun-management fast-switchover • redun-management garp-retransmit burst • no redun-management garp-retransmit initial <p>詳細については、「High Availability」の章を参照してください。</p>
中間アカウントिंग	<p>このリリースから、中間アカウントिंगを無効にするために、ポリシープロファイルの下に no accounting-interim コマンドが導入されました。</p> <p>詳細については、「Interim Accounting」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
スタンバイコントローラでの Link Layer Discovery Protocol のサポート	<p>このリリースから、Link Layer Discovery Protocol (LLDP) プロセスが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サポートされます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none">• lldp run• lldp holdtime• lldp reinit• lldp timer• lldp tlv-select• show lldp• show lldp neighbors• show lldp neighbors detail• show lldp errors• show lldp traffic <p>詳細については、「Link Layer Discovery Protocol」の章を参照してください。</p>
TACACS+ サーバーでの Web UI ベースの設定変更のログイン	<p>この機能は、コントローラの UI で行われたすべての構成変更をログに記録します。</p> <p>詳細については、「Web UI Configuration Command Accounting in TACACS+ Server」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
Cisco Catalyst 916x シリーズ Wi-Fi 6E アクセスポイント (CW9164 および CW9166) での管理モードの移行	<p>このリリース以降、Cisco Catalyst 916x AP (CW9164 および CW9166) では、要件に応じて、Cisco DNA 管理モード (コントローラベース) と Meraki 管理モードの間で管理モードを移行できます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • ap name management-mode meraki • clear ap meraki stats • show ap management-mode meraki capability summary • show ap management-mode meraki failure summary • show ap management-mode meraki change summary <p>詳細については、「Management Mode Migration in Cisco Catalyst 916x Series Wi-Fi 6E Access Points」の章を参照してください。</p>
メッシュバックホール RRM サポート	<p>このリリース以降、wireless mesh backhaul rrm auto-dca コマンドを設定すると、RRM DCA は自動モードのメッシュバックホールで実行されます。専用 (RHL) 無線を持たない AP の場合、特権 EXEC モードでコマンドを実行すると DCA がトリガーされます。メッシュ RRM DCA は、RHL 無線対応 AP のバックグラウンドで実行されます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • ap dot11 rrm channel-update mesh • ap dot11 rrm channel-update mesh bridge-group • ap name dot11 rrm channel update mesh • show wireless mesh rrm dca status • wireless mesh backhaul rrm auto-dca <p>詳細については、「Mesh Access Points」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
gRPC テレメトリの相互認証	<p>相互認証にクライアント ID 証明書を指定できるように、トラストポイントのペアを含む新しい gRPC TLS プロファイルがテレメトリ構成に追加されました。この新しいプロファイルは、受信者プロファイルを設定するときに、サーバー CA 証明書を含まないトラストポイントの代わりに使用できます。サーバー CA 証明書を含まないトラストポイントは、gRPC TLS プロファイルの一部として構成されました。</p> <p>詳細については、『Programmability Configuration Guide』を参照してください。</p>
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのサービス品質のギャップと修正	<p>この機能は、RFC 8325 を参照して、既存のメタルポリシー実装のギャップに対処します。</p> <p>この拡張により、各メタルポリシーに関連付けられている既存のハードコードされたポリシーマップとクラスマップが RFC 8325 に従って変更され、アップストリームとダウンストリームの上限が達成されます。</p> <p>詳細については、「Quality of Service」の章を参照してください。</p>
規制ドメインの削減	<p>Cisco IOS XE Cupertino 17.9.1 以降、さらに多くの国が、その他の世界 (RoW) ドメインに追加されます。</p> <p>詳細については、「Regulatory Compliance Domain」の章を参照してください。</p>
Cisco Catalyst 9164 および 9166 シリーズ Wi-Fi 6E アクセスポイントでの不正検出機能の強化	<p>このリリースでは、不正の検出および封じ込め機能が強化され、Cisco Catalyst 9164 シリーズ Wi-Fi 6E AP および Cisco Catalyst 9166 シリーズ Wi-Fi 6E AP でデュアル 5 GHz 構成を処理できるようになりました。</p>
不正フルスケールクォータと優先度	<p>不正フルスケールクォータと優先度機能は、不正 AP の拡張性、パフォーマンス、管理性、および有用性を向上させるのに役立ちます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • wireless wps rogue scale quota • wireless wps rogue scale priority • wireless wps rogue scale mode hybrid <p>詳細については、「Managing Rogue Devices」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
RUM レポートスロットリング	<p>製品インスタンスが通信を開始するすべてのトポロジで、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが1日に複数のRUMレポートを送信しないことを意味します。</p> <p>影響を受けるトポロジは、CSSMに直接接続、CSLUを介してCSSMに接続（製品インスタンス開始型通信）、CSSMから切断されたCSLU（製品インスタンス開始型通信）およびSSM オンプレミス展開（製品インスタンス開始型通信）です。</p> <p>これにより、特定のライセンスに対して生成および送信されるRUMレポートが多すぎるという問題が解決されます。また、RUMレポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。</p> <p>特権 EXEC モードで license smart sync コマンドを入力すると、レポート頻度のスロットリングを無効にできます。これにより CSSM または CSLU、あるいは SSM オンプレミスとのオンデマンドの同期がトリガーされ、保留中のデータが送受信されます。</p> <p>RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。Cisco IOS XE Cupertino 17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。</p>
N+1 ネットワークでのサイトベースのローリング AP アップグレード	<p>N+1 ネットワークでのサイトベースのローリング AP アップグレード機能を使用すると、N+1 展開の各サイトで AP の段階的なアップグレードを実行できます。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • ap upgrade staggered iteration completion • ap upgrade staggered iteration error • ap upgrade staggered iteration timeout • show ap upgrade site <p>詳細については、「Site-Based Rolling AP Upgrade in an N+1 Network」の章を参照してください。</p>

機能名	説明とドキュメントのリンク
Netconf/YANG モデルを使用したサイトベースのローリング AP アップグレード	<p>Cisco IOS XE Cupertino 17.9.1 以降、NETCONF/YANG モデルを使用して、サイトベースの APSP および N+1 ヒットレス ソフトウェア アップグレードを設定できます。</p> <p>詳細については、 https://www.cisco.com/.../product/marketing/guides.html にある『<i>Programmability Configuration Guide</i>』を参照してください。</p> <p>YANG モデルの詳細については、 https://github.com/YangModels/yang/tree/master/vendor/cisco/xe にある『<i>Cisco IOS XE Programmability Configuration Guide</i>』および『<i>YANG Data Models on Github</i>』を参照してください。</p> <p>NETCONF/YANG 機能の開発者のサポートコミュニティに問い合わせることができます。 https://developer.cisco.com/</p>
カナダ向けの 6 GHz 無線のサポート	<p>このリリースでは、802.11 6 GHz 無線帯域をサポートする国のリストにカナダ (CA) が追加されています。</p>
Cisco Catalyst 9164I シリーズ Wi-Fi 6E アクセスポイントおよび Cisco Catalyst 9166I シリーズ Wi-Fi 6E アクセスポイントのサポート	<p>このリリース以降、Cisco Catalyst 9164I シリーズ Wi-Fi 6E アクセスポイントおよび Cisco Catalyst 9166I シリーズ Wi-Fi 6E アクセスポイントがサポートされます。</p>

機能名	説明とドキュメントのリンク
<p>コントローラでの RFC 5580 ロケーション属性のサポート</p>	<p>この機能は、RFC 5580 ロケーション属性を使用して、認証およびアカウント交換のためのロケーション関連情報を伝達します。</p> <p>次のコマンドが導入されています。</p> <ul style="list-style-type: none"> • radius-server attribute wireless location delivery out-of-band • location civic-location identifier • location geo-location identifier • location operator identifier • location civic-location-id • location geo-location-id • location operator-id • radius-server attribute wireless location civic-location-id • radius-server attribute wireless location geo-location-id • radius-server attribute wireless location operator-id <p>詳細については、「Configuring RFC 5580 Location Attributes」の章を参照してください。</p>
<p>DHCP および静的 IP クライアントをサポートする VLAN グループ</p>	<p>DHCP および静的 IP クライアントをサポートする VLAN グループ機能は、静的 IP アドレスが VLAN の IP リストに含まれていないクライアントのネットワークアクセスを処理することを目的としています。</p> <p>詳細については、「VLAN Groups」の章を参照してください。</p>
<p>使用状況とトラブルシューティングの Walkme</p>	<p>次の新しいワークフローが実装されました。</p> <ul style="list-style-type: none"> • AP 参加のトラブルシューティング : AP 参加が失敗した理由を見つけるために、さまざまなトラブルシューティングコマンドを実行するワークフローのコレクション。 • FlexConnect ワークフロー : FlexConnect の設定方法を示すワークフローのコレクション。

機能名	説明とドキュメントのリンク
ワイヤレス不正チャネル幅のサポート	<p>このリリースでは、ワイヤレス不正チャネル幅機能がサポートされています。</p> <p>不正チャネル幅の変更は、TDL レベルで実装されます。TDL の制限により、Cisco DNA Center はテレメトリの子テーブルにアクセスできないため、すべての無線帯域情報が最上位のテーブルで利用できるようになりました。テレメトリデータは、SSH Netconf コンソールを介して検証し、チャネル幅の値で正しい無線帯域を確認できます。</p>
Cisco Catalyst Wi-Fi 6 アクセスポイントでの TrustSec サポート	<p>このリリース以降、Cisco Catalyst Wi-Fi 6 アクセスポイントは、コントローラで TrustSec 機能をサポートします。</p> <p>(注) Wi-Fi 6 アクセスポイントは、以前のリリースのセキュリティグループタグ (SGT) 機能を備えた SD-Access ソリューションをサポートしています。</p>
ゼロ待機動的周波数選択	<p>アクセスポイント (AP) が動的周波数選択 (DFS) チャンネルに移動すると、サービスが停止する可能性があります。この機能は、規制ドメインでのサービス停止を回避するのに役立ちます。現在、サポートされているドメインは米国とヨーロッパのみです。詳細については、「Dynamic Frequency Selection」の章を参照してください。</p>

表 6: 新規および変更された GUI 機能

機能名	GUI パス
SAE 認証クライアントの 802.11r Fast Transition	<ul style="list-style-type: none"> • [Configuration] > [Tags & Profiles] > [WLANs]
クライアント 360 ビューの追加のクライアント情報	<ul style="list-style-type: none"> • [Monitoring] > [Wireless] > [Clients] > [360]
AP コンソールの構成	<ul style="list-style-type: none"> • [Configuration] > [Tags & Profiles] > [AP Join]
Cisco Catalyst 9166I シリーズ Wi-Fi 6E アクセスポイントでのフレキシブルラジオアサインメントのサポート	<ul style="list-style-type: none"> • [Configuration] > [Radio Configurations] > [RRM] > [FRA]

機能名	GUI パス
Cisco Catalyst 916x シリーズ Wi-Fi 6E アクセスポイント (CW9164 および CW9166) での管理モードの移行	<ul style="list-style-type: none"> • [Configuration] > [Wireless] > [Migrate to Meraki Management Mode]
N+1 ネットワークでのサイトベースのローリング AP アップグレード	<ul style="list-style-type: none"> • [Administration] > [Software Management]

MIB

以下の MIB が新たに追加または変更されました。

- AIRESpace-WIRELESS-MIB
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-MOBILITY-MIB
- CISCO-LWAPP-RF-MIB
- CISCO-LWAPP-RRM-MIB
- CISCO-LWAPP-SI-MIB
- CISCO-LWAPP-TAGS-MIB
- CISCO-LWAPP-WLAN-MIB
- CISCO-LWAPP-WLAN-SECURITY-MIB

動作の変更

- Cisco Centralized Key Management (CCKM) 機能は、Cisco IOS XE Dublin 17.10.x 以降で廃止されます。
- J2 国コードは日本ではサポートされていません。J2 ではなく、J4 を日本の国コードとして使用します。
- 次のコマンドは、サービスピアモードでのみ有効です。

サービスピアの詳細については、「[Configuring Local Area Bonjour for Wireless FlexConnect Mode](#)」の章の「Understanding Local Area Bonjour for Wireless FlexConnect Mode」セクションを参照してください。

- **query-response**
- **sdg-agent**
- **service-announcement-count**

- **service-announcement-timer**
 - **service-mdns-query**
 - **service-query-count**
 - **service-query-timer**
 - **service-receiver-purge**
 - **active-response**
- ワイヤレスマルチキャストがサービスピアモードで無効になっている場合、mDNS パケットは各 CAPWAP インターフェイスに送信されます。ワイヤレスマルチキャストとマルチキャストトンネルが有効になっている場合、mDNS パケットはマルチキャストトンネルを介して送信されます。
- プロンプトレベルオプションの有無にかかわらず、保存されていない構成がある場合、インストールコマンドは実行できません。
- サービスポリシーで場所が指定されていない場合、場所はグローバル mDNS ゲートウェイからと見なされます。デフォルトでは、グローバル mDNS ゲートウェイの場所は **lss** として定義されています。
- AP プロファイルで国が設定されている場合、AP ごとの国設定を使用してそれを上書きすることはできません。
- 802.1x パスワードは暗号化されているため、このリリースではクリアテキストで表示されません。暗号化されたパスワードをサポートしていない以前のイメージにダウングレードする場合は、AP がスタックし、誤ったクレデンシャルが原因で dot1x 認証に繰り返し失敗します。AP スイッチポートで 802.1x を無効にして、AP がコントローラに参加できるようにしてから、クリアテキストパスワードを設定する必要があります。
- 次の show コマンドの出力が更新されました。
- **show ap dot11 cleanair device type**
 - **show ap name dot11 cleanair device**
 - **show ap dot11 5ghz SI device type**
 - **show ap name dot11 SI device**
- 次のコマンドが導入されています。
- **ap name dot11 24ghz cleanair**
 - **ap name dot11 5ghz cleanair**
 - **ap name dot11 6ghz cleanair**
- 次のコマンドは廃止です。
- **ap name dot11 24ghz slot cleanair**
 - **ap name dot11 5ghz slot cleanair**

- **ap name dot11 dual-band cleanair band**
 - **ap name dot11 ap name dot11 dual-band slot cleanair band**
 - **ap name dot11 dual-band cleanair band**
 - **ap name dot11 ap name dot11 dual-band slot cleanair band**
 - **ap name dot11 ap name dot11 dual-band slot cleanair**
 - **ap name dot11 rx-dual-band slot cleanair band**
 - **ap name dot11 rx-dual-band slot cleanair**
- AP **show security system state** コマンドの出力に FIPS に関する情報が追加されました。
 - デバイス分析レポートは、5 分間キャッシュされてから、**show wireless client mac stats pc-analytics** コマンドで使用できるようになります。
 - このリリース以降、Web 管理での HTTPS 通信で TLS 1.3 がサポートされます。
 - 次の表では、廃止され、置き換えられた show コマンドについて説明します。

表 7: 廃止および置き換えられた *show* コマンド

廃止されたコマンド	置き換えられたコマンド
show ap persona meraki capability summary	show ap management-mode meraki capability summary
show ap persona meraki change summary	show ap management-mode meraki change summary
show ap persona meraki failure summary	show ap management-mode meraki failure summary

- **ap name <ap-name> persona meraki [force] [noprompt]** コマンドは廃止され、**ap name <ap-name> management-mode meraki [force] [noprompt]** コマンドに置き換えられました。
- AP プロファイルの USB ポートは、デフォルトで無効になっています。
Cisco IOx アプリケーションを USB ドングルとともに使用する場合は、リロード時に AP プロファイルで USB ポートを再設定し、USB ポートが有効になってから AP に接続します。
この回避策の詳細については、[CSCvz07021](#) を参照してください。
- コントローラは、製品分析と自動周波数調整 (AFC) のために [dnaservices.com](#) と通信します。コントローラで DNS が設定されていない場合でも、コントローラではハードコードされた DNS サーバーが使用されます。AFC の製品分析が無効になっている場合でも、コントローラは [dnaservices.com](#) にアクセスしようとします。



(注) これは、Cisco IOS XE Cupertino 17.9.4 リリース以降に適用されます。

- Cisco IOS XE Cupertino 17.9.5 リリース以降、製品分析はデフォルトで有効になっています。

製品分析の詳細については、「[Wireless Product Analytics FAQ](#)」を参照してください。

- 構成で CISCO_IDEVID_SUDI トラストポイントを設定している場合は、クライアント接続と AP 接続の問題を回避するために、トラストポイントを CISCO_IDEVID_CMCA3_SUDI に置き換える必要があります。これは、CISCO_IDEVID_SUDI が以前のリリースの SW-SUDI 証明書から HW-SUDI 証明書に変更されたことによる変更です。HW-SUDI 証明書の処理は、SW-SUDI よりもはるかに遅いため、ここで、CISCO_IDEVID_CMCA3_SUDI を新しい SW-SUDI 証明書にします。



(注) これは、Cisco IOS XE Cupertino 17.9.3 リリース以降に適用されます。

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。
- Dynamic Host Configuration Protocol (DHCP) によって特定の期間内に IP アドレスが解決されない場合、Cisco Aironet 2800 および 3800 AP はインターフェイスをリセットしません (イーサネット インターフェイスの物理層の問題を解消するため)。

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 10: 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 8: 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 9: 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	<ul style="list-style-type: none"> 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

ホスト環境	ソフトウェアバージョン
KVM	<ul style="list-style-type: none"> 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 KVM/SUSE バージョン 15 SP3 (SDA ワイヤレス展開に限定)
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 が表示されません。

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 10: 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)
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)。

コントローラ モデル	説明
C9800-L-C-K9	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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

次の表に、サポートされる SFP モデルを示します。

表 11: サポートされる SFP

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
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 1	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
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
GLC-EX-SMD	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	—
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
GLC-T	サポート対象	—	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
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
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	—	—	—
QSFP-40G-ER4	サポート対象	—	—	—
QSFP-40G-LR4	サポート対象	—	—	—

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
QSFP-40G-LR4-S	サポート対象	—	—	—
QSFP-40G-SR4	サポート対象	—	—	—
QSFP-40G-SR4-S	サポート対象	—	—	—
QSFP-40GE-LR4	サポート対象	—	—	—
SFP-10G-AOC10M	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	—	—
SFP-10G-AOC2M	サポート対象	サポート対象	—	—
SFP-10G-AOC3M	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	—	—
SFP-10G-AOC7M	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	—	—
SFP-10G-LR	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
SFP-10G-LR-X	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
SFP-10G-SR-S	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	—	—
SFP-H10GB-ACU10M	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
SFP-H10GB-CU1.5M	サポート対象	サポート対象	—	サポート対象
SFP-H10GB-CU1M	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

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
SFP-H10GB-CU2M	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
SFP-H10GB-CU5M	サポート対象	サポート対象	—	サポート対象

¹ 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。

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

ネットワークプロトコルとポートマトリックス

表 12: 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	送信元ポート	説明
任意 (Any)	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	22	いずれか	SSH
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	23	いずれか	Telnet
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	80	いずれか	HTTP
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	いずれか	HTTPS

送信元	接続先	プロトコル	宛先ポート	送信元ポート	説明
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	161	いずれか	SNMP エージェント
いずれか	いずれか	UDP	5353	5353	mDNS
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	69	69	TFTP
いずれか	DNS Server	UDP	53	いずれか	DNS
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	830	いずれか	NetConf
いずれか	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	いずれか	REST API
いずれか	WLC プロトコル	UDP	1700	いずれか	CoA パケットを受信します。
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5246	いずれか	CAPWAP 制御
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5247	いずれか	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	いずれか	CAPWAP MCAST
AP	Cisco Catalyst Center	UDP	57778	いずれか	インテリジェントキャプチャと RF テレメトリ

送信元	接続先	プロトコル	宛先ポート	送信元ポート	説明
AP	AP	UDP	16670	いずれか	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	いずれか	SNMP トラッ プ
Cisco Catalyst 9800 シリーズ ワイヤレス コ ントローラ	RADIUS	UDP	1812/1645	いずれか	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	いずれか	RADIUS ACCT
Cisco Catalyst 9800 シリーズ ワイヤレス コ ントローラ	TACACS+	TCP	49	いずれか	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	いずれか	NTP
Cisco Catalyst 9800 シリーズ ワイヤレス コ ントローラ	Syslog サー バー (Syslog Server)	UDP	514	いずれか	SYSLOG

送信元	接続先	プロトコル	宛先ポート	送信元ポート	説明
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	いずれか	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	いずれか	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 シリーズ ワイヤレス コ ントローラ	TCP	32222	いずれか	デバイス検出

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 9105AXI アクセスポイント
 - VID 04 以降 - 17.9.2 以降でサポート
 - VID 03 以前 - すべての 17.9.x リリースでサポート
- Cisco Catalyst 9105AXW アクセスポイント
 - VID 02 以降 - 17.9.2 以降でサポート
 - VID 01 以前 - すべての 17.9.x リリースでサポート
- Cisco Catalyst 9115AX (I/E) アクセスポイント
- Cisco Catalyst 9117AXI 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 - 17.9.2 以降でサポート
 - VID 06 以前 - すべての 17.9.x リリースでサポート
- Cisco Catalyst 9120AXP 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 - 17.9.2 以降でサポート

- VID 02 以前 - すべての 17.9.x リリースでサポート

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 9136I アクセスポイント
- Cisco Catalyst 9162I シリーズ アクセスポイント - 17.9.2 以降でサポート
- Cisco Catalyst 9164I シリーズ アクセスポイント
- Cisco Catalyst 9166I シリーズ アクセスポイント
- Cisco Aironet 1800I、1815 (I/W) 、1830 (I) 、1840 (I) 、および 1850 (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

17.9.3 から次の AP が再びサポートされるようになりました。

- 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

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
- Cisco Catalyst IW9167 (E) Heavy Duty アクセスポイント : 17.9.3 以降でサポート

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

プラグブルモジュール

- 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ン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ン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ンネル、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 13: 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 Catalyst Center	Cisco Spaces : コネクタ	Cisco CMX
Cupertino 17.9.5	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.196.0 8.10.190.0 8.10.183.0 8.10.182.0 8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 10.6.3
Cupertino 17.9.4a	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 10.6.3

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 Catalyst Center	Cisco Spaces : コネクタ	Cisco CMX
Cupertino 17.9.4	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 10.6.3
Cupertino 17.9.3	3.3 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 10.6.3

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 Catalyst Center	Cisco Spaces : コネクタ	Cisco CMX
Cupertino 17.9.2	3.3 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 10.6.3
Cupertino 17.9.1	3.3 3.0 2.7 2.6 2.4	3.10 MR1	8.10.181.0 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	Cisco Catalyst Center の互換性情報を参照	2.3.1 2.3 2.2	11.0 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 14: 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 ²	512 MB ³	256	1280 x 800 以上	小

² 1 GHz を推奨

³ 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。

Cisco IOS-XE 17.9.3 を実行している AP でソフトウェアをアップグレードしようとする、/tmp ディレクトリのスペース不足により問題が発生することがあります。AP の /tmp スペースがいっぱいになると、新しい AP イメージをダウンロードできなくなります。このような場合は、AP をリブートすることを推奨します。



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 を使用して以前の任意のリリースから Cisco IOS XE Dublin 17.12.x にコントローラをアップグレードする場合、**snmp-server enable traps license** コマンドが設定されているとアップグレードが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 license** コマンドを必ず削除してください。これは、Cisco IOS XE Dublin 17.12.x 以降で **snmp-server enable traps license** 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。
- WPA3 を設定する場合は、認証とキー管理 (AKM) 設定を必ず追加してください。古いリリースでは、このシナリオは必須ではなく、無効な設定になりますが、17.9 以降のリリースでは、この無効なシナリオが検出され、阻止されます。

WAN リンクを介してソフトウェアをアップグレードすると、Cisco Wave 2 AP がブートループ状態になることがあります。詳細については、<https://www.cisco.com/c/en/us/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、17.4 ~ 17.9.2、17.10.x、17.11.x、17.13.x、および 17.14.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。Cisco.com で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 以降) には直接移行できます。

- 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/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.htmlで入手可能な『SSH Algorithms for Common Criteria Certification』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。
 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
```



注意 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、**linevty** 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、以下に指定された順序で次の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
```

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。

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 Catalyst 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 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 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。
 - Virtual Routing and Forwarding (VRF) を使用した RLAN 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時刻がより早い時刻を反映するように変更されるたびに、コントローラのリロードを実行することを推奨します。



- (注) バンドルモードを使用して Cisco Catalyst 9800-40 シリーズ ワイヤレス コントローラのイメージを Cisco IOS XE Cupertino 17.9.x にアップグレードする前に、ROMMON バージョンが 17.7(3r) 以降であることを確認してください。

Cisco Catalyst 9800-80 シリーズ ワイヤレス コントローラなどの他のプラットフォームについては、17.3(3r) にアップグレードする必要があります。また、Cisco Catalyst 9800-L シリーズ ワイヤレス コントローラの場合は、ROMMON バージョンを 16.12(3r) 以降にアップグレードすることを推奨します。

アップグレード後、旧バージョンの ROMMON にダウングレードすることはできません。



- (注) 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
```

DTLS バージョンを 1.0 に設定すると、既存のすべての AP CAPWAP 接続に影響することに注意してください。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。

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、[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 \[英語\]](#) を参照してください。



- 重要** 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。

- AP を上位バージョンから Cisco IOS XE Amsterdam 17.3.x にダウングレードすると、AP がまだコントローラに参加していない場合、**enable** パスワードの拒否により、SSH またはコンソールを介して AP にアクセスできなくなります。AP がコントローラに参加すると、AP はパスワード拒否されずにアクセス可能になります。

Cisco IOS XE Cupertino 17.9.x へのアップグレードパス

表 15: Cisco IOS XE Cupertino 17.9.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	— ⁴	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.9.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、17.9.x にアップグレードします。
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てから、17.9.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、17.9.x にアップグレードします。
17.1.x	最初に 17.3.5 以降にアップグレードしてから、17.9.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、17.9.x にアップグレードします。
17.2.x	最初に 17.3.5 以降にアップグレードしてから、17.9.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、17.9.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てから、17.9.x にアップグレードします。	17.9.x に直接アップグレードします。
17.3.4c 以降	17.9.x に直接アップグレードします。	17.9.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、17.9.x にアップグレードします。	17.9.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、17.9.x にアップグレードします。	17.9.x に直接アップグレードします。

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
17.6.x	17.9.x に直接アップグレードします。	17.9.x に直接アップグレードします。
17.7.x	17.9.x に直接アップグレードします。	17.9.x に直接アップグレードします。
17.8.x	17.9.x に直接アップグレードします。	17.9.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てから、17.9.x にアップグレードします。	17.9.x に直接アップグレードします。
8.10.171.0 以降	17.9.x に直接アップグレードします。	17.9.x に直接アップグレードします。

⁴ 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。

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 17.9.x
- イメージ名 (9800-80、9800-40、および9800-L) :
 - C9800-80-universalk9_wlc.17.09.x.SPA.bin
 - C9800-40-universalk9_wlc.17.09.x.SPA.bin
 - C9800-L-universalk9_wlc.17.08.x.SPA.bin
- イメージ名 (9800-CL) :
 - クラウド : C9800-CL-universalk9.17.09.x.SPA.bin
 - Hyper-V/ESXi/KVM : C9800-CL-universalk9.17.09.x.iso, C9800-CL-universalk9.17.09.x.ova
 - KVM : C9800-CL-universalk9.17.09.x.qcow2
 - NFVIS : C9800-CL-universalk9.17.09.x.tar.gz

ソフトウェア インストール コマンド

Cisco IOS XE Cupertino 17.9.x	
<p>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。</p> <p>device# install add file filename [activate [commit]</p> <p>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。</p> <p>device# install ?</p> <p>(注) インストールには GUI を使用することを推奨します。</p>	
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。

Cisco IOS XE Cupertino 17.9.x	
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。 <https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

シスコライセンスの詳細については、 [cisco.com/go/licensingguide](https://www.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 16: 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 17.9.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 (26 ページ) 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。

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
無線機	<ul style="list-style-type: none"> • 802.11 ax • 802.11ac • 802.11a • 802.11g • 802.11n • 6 GHz で 802.11ax (Wi-Fi 6E)
セキュリティ	オープン、PSK (WPA2-AES) 、802.1X (WPA2-AES) (EAP-FAST、EAP-TLS) WPA3 AKM 802.11 ax
RADIUS	互換性マトリックス (36 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 17: 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
Apple Macbook Air 11 インチ	OS X Yosemite 10.10.5
MacBook M1 チップ	OS Catalina
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129

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
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、アダプタイズされた 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

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 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 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 14	iOS 16
Apple iPhone 15	iOS17
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1

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
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
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

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 A21	Android 10.0
Sony Xperia 1 ii	Android 11
Sony Xperia	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
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 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 6.4
Zebra ZQ610 産業用プリンタ	LINK OS 6.4

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 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
PhoenixContact FL WLAN 2010	ファームウェアバージョン : 2.71

問題

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問題は、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。

問題の詳細を表示するには、対応する識別子をクリックします。

Cisco IOS XE Cupertino 17.9.5 の未解決の不具合

ID	見出し
CSCwi51168	ペアワイズマスターキー (PMK) ID が一致しない場合、FlexConnect セットアップで 4 ウェイハンドシェイクの更新に失敗します。

ID	見出し
CSCwi55714	Cisco Network Mobility Services Protocol (NMSP) Transport Layer Security (TLS) 接続を処理すると、コントローラが再起動します。
CSCwi53481	SDA を介して Cisco IOS-XE 17.6.4 から 17.9.4a にアップグレードすると、コントローラで SUDI MIC トラストポイントが失われます。
CSCwh63050	Cisco IOS-XE 17.9.3 を搭載したコントローラから、非 WLC IP アドレスと MAC アドレスを使用して Internet Group Management Protocol (IGMP) クエリが送信されます。
CSCwi16509	Invalid radio slot id エラーで AP がコントローラに接続できません。
CSCwi60173	ソフトウェア定義型アクセス (SDA) ファブリックのワイヤレスクライアントにセキュリティグループタグ (SGT) が適用されません。
CSCwi28382	Keymgmt: Failed to eapol key m1 retransmit failure. Max retries for M1 over が原因でコントローラが予期せずリロードされます。
CSCwi57179	静的 IP を持つクライアントが、ローミング中に誤った VLAN (VLAN グループ) に割り当てられます。
CSCwh18613	password encryption aes が適用されるたびに、暗号化されたメッシュ事前共有キーが変更されます。
CSCwi62934	Cisco Catalyst 9120 AP で、ワイヤレスクライアントに向かう大きなフレームのダウンストリームがドロップされます。
CSCwi16104	Flex VLAN リストの取得中に、DBM でコントローラが予期せず再起動されます。
CSCwi66133	カーネルパニックが原因で Cisco Catalyst 9130 AP が予期せずリロードする。
CSCwi42112	有線クライアントが、Cisco Catalyst 9124 MAP ポートから MAC アドレスを学習します。
CSCwi56780	コントローラでデバイスの認証が解除されない限り、MAC 認証バイパス (MAB) が開始されません。
CSCwi04855	トレースバックを使用して、Cisco Catalyst 9115 AP の接続と接続解除が繰り返えされます。
CSCwi51025	Cisco Catalyst 9130 AP が予期せずリロードされ、カーネルパニッククラッシュが発生します。
CSCwi27380	メディアストリーム機能が動作しません。

ID	見出し
CSCwi29636	Cisco IOS-XE 17.9.3 WNCDC がダウンしている場合、Cisco Catalyst 9800-40 ワイヤレスコントローラが予期せずリロードされます。
CSCwi54064	同じコントローラに接続されている AP は、互いを不正な AP として分類し、「AP Impersonation」脅威警告を生成します。

Cisco IOS XE Cupertino 17.9.4a の未解決の不具合

このリリースから、不具合のリストは BST ツールを使用して表示されます。BST リンクをクリックすると、別のウィンドウが開き、バグが重大度別にソートされて一覧表示されます。ツールのオプションを使用して、さらにフィルタ処理することができます。

ID	見出し
CSCwh37783	ロビー管理ページがコントローラにロードされません。

その他の未解決の不具合を表示するには、次のリンクをクリックします。[BST リンク](#)

Cisco IOS XE Cupertino 17.9.4 の未解決の不具合

このリリースから、不具合のリストは BST ツールを使用して表示されます。BST リンクをクリックすると、別のウィンドウが開き、バグが重大度別にソートされて一覧表示されます。ツールのオプションを使用して、さらにフィルタ処理することができます。

未解決の不具合を表示するには、次のリンクをクリックします。[BST リンク](#)

Cisco IOS XE Cupertino 17.9.3 の未解決の不具合

ID	見出し
CSCwa67566	Cisco Catalyst 9800 シリーズ コントローラ/AireOS パリティ : AKM を FT から DOT1X に変更した後で FT に再び戻すと、不正な PMKID によりクライアントが拒否されます。
CSCwc06025	IW9167EH のルート AP で「バックホールクライアントアクセス」を無効にした後、メッシュ AP をルート AP に関連付けることができません。
CSCwc76174	DP へのクライアントダウンロードに失敗し、スタンバイコンソールに @cpp_wlclient_create のトレースバックメッセージが大量に表示されます。
CSCwd31523	Azure でホストされている C9800-CL で Flex WLAN のプロビジョニングに失敗します。
CSCwd46815	Cisco 2800、3800、4800、1562、6300 シリーズ AP の MAP の背後にある有線クライアントで EAP-TLS に失敗します。

ID	見出し
CSCwd56391	コントローラがデータベース内にある一部の RFID タグの RSSI ロケーションデータを提供していません。
CSCwd79502	アンカーされているクライアントが異なる VLAN で IPv4 と IPv6 を取得したため、コントローラは古いエントリを追跡しています。
CSCwd86288	Cisco Catalyst 9800-80 シリーズ コントローラが正常な場合でも、負荷平均の警告が表示されます。
CSCwd90742	Cisco Catalyst 9120AX AP でカーネルクラッシュが発生します (PC : rhb_del_interface+0xc)。
CSCwd91054	COS-AP で M1 ~ M4 の後に EAP_ID_REQ が暗号化されず、dot1xOKC の PMKID が更新されません。
CSCwd96484	「wncd」 コアファイルを生成した後、コントローラが予期せずリロードします。
CSCwd98332	コントローラがアンカーメッセージ内のインターフェイス ID と一致しなかった後、リロードします。
CSCwe04602	Cisco Catalyst 9120 AP が、ワイヤレスクライアントへのトラフィック転送に約 60 秒間失敗します。
CSCwe07802	2800、3800、4800、1562 などの Cisco AP が、アップストリーム EAP パケットをドロップしています。
CSCwe11315	Cisco IOS-XE 17.9.2 を実行している Cisco Catalyst 9164 および 9166 AP において、すべてのチャンネルで DFS 検知が発生しています。
CSCwe11747	Cisco Catalyst AX シリーズの AP が、EAP 要求 ID を正しく復号化していません。
CSCwe14729	DHCP 応答の Option82 の処理中にメモリが破損し、コントローラがリロードします。
CSCwe16892	チャンクヘッダーで不正なマジック番号が検出された後、トレースバックとリロードが発生します。
CSCwe18012	QoS テーブルの保存中にスタンバイコントローラがクラッシュします。
CSCwe22861	Flex COS AP で AID のリークが観察されます。
CSCwe25446	WNCD が原因で予期せぬ再起動が発生します。
CSCwe25610	クライアントの削除が開始されました。理由 : CO_CLIENT_DELETE_REASON_REMOTE_MOBILITY_DELETE - ローカルモビリティ。
CSCwe30473	RC キューのフリーズが原因で無線ファームウェアのクラッシュが発生します。

ID	見出し
CSCwe31030	Cisco Catalyst 9105AXW AP がクラッシュしています。
CSCwe31270	コントローラで帯域幅制限のAAA属性が欠落している場合、クライアントはトラフィックの通過を停止します。
CSCwe32005	Cisco Catalyst 9130 AP : デジタルサイネージデバイスでパケット損失が観察されます。
CSCwe38431	音声CACが設定されている場合、コントローラがアップストリームまたはダウンストリームでCS3からCS0へのSIPパケットを再マーキングしています。
CSCwe39039	Cisco DNA Center からコントローラをプロビジョニングした後にトレースバックが発生します。
CSCwe42211	GUIでEWC時間オフセットが更新されません。
CSCwe42302	プロファイル名が一致しない場合、IRCMモビリティクライアントはサイレントに削除されます。
CSCwe43294	Cisco Catalyst 9105AXW AP および Cisco Aironet 1815W Flex RLAN AP は、AAA VLAN オーバーライド後にイーサネットポートにVLANを適用しません。
CSCwe44216	カーネルパニックが原因でAPのクラッシュが発生します (PC : vfp_reload_hw+0x30/0x44) 。
CSCwe44991	Cisco Catalyst 9105AX AP : カーネルパニックが原因でクラッシュが発生します。
CSCwe45300	Cisco Catalyst 9120 AP : モード2のメッセージ2をhostapdに送信できませんでした。
CSCwe45894	APがワイヤレスクライアントにIGMPv3クエリを転送していません。
CSCwe45970	APがUBOOTでスタックします。
CSCwe49267	WNCD間のFTローミング後に、コントローラがGTK M5パケットを8821に送信しません。
CSCwe49356	Cisco Catalyst 9136 AP カーネルパニック : 予期せぬリロードがcsd_lock_wait+0x10/0x18で発生します。
CSCwe50033	Cisco Catalyst 9120AX AP : 10を超えるクライアントでMS TEAMSが使用されている場合、クライアントが継続的に切断されます。
CSCwe61084	17.3.7から17.9.3へのISSUアップグレードを実行中に、Pubdのクラッシュが発生します。

Cisco IOS XE Cupertino 17.9.2 の未解決の不具合

警告 ID	説明
CSCwc24994	カーネルパニックが原因で Cisco Aironet 3800 アクセスポイントが異常終了します。
CSCwc32182	Cisco Aironet 1852 アクセスポイントで無線ファームウェアのクラッシュが発生します。
CSCwc49992	ダイレクトメモリアクセス (DMA) トランザクション中にタイムアウトが発生すると、アクセスポイントでカーネルパニックが発生します。
CSCwc75732	Cisco Aironet 4800 アクセスポイントで、Cisco IOS-XE 17.3.5b リリースではファームウェア無線クラッシュが発生します。
CSCwd05213	gRPC サーバープロセスを実行すると、カーネルパニッククラッシュが発生します。
CSCwd05689	Cisco Catalyst 9124 アクセスポイント AXI RSSI は、他のアクセスポイントモデルと比較して、離れた場所で 7 dBm から 8 dBm 弱くなります。
CSCwd08068	wcpd プロセスがメモリを占有すると、OOM が原因で Cisco Aironet 1815W アクセスポイントがクラッシュします。
CSCwd10570	Cisco Catalyst 9130 アクセスポイントは、異なる基本サービスセット識別子 (BSSID) に対して異なるビーコンデータレートを表示します。
CSCwd22017	IP Learn のタイムアウトが原因で Apple iOS デバイスが削除されます。
CSCwd26693	FlexConnect アクセスポイントの N+1 ハイアベイラビリティセットアップが機能していません。
CSCwd30828	カーネルパニックが原因で Cisco Catalyst 9120 アクセスポイントがクラッシュし、リロードします。
CSCwd33981	PC が「cpuidle_not_available」の場合、カーネルパニッククラッシュが発生します。
CSCwd35577	ダブルビット ECC エラーにより、スタンバイコントローラがリロードされます。
CSCwc64201	Cisco Catalyst 9105 アクセスポイントは、ワークグループブリッジ (WGB) として動作しているときに通信ギャップが発生します。

警告 ID	説明
CSCwc87688	Cisco Catalyst 9120 アクセスポイントは、5 GHz 無線で高いノイズレベルをランダムに表示します。
CSCwd03803	PC が edma_poll にあるか、LR が dma_cache_maint_page にある場合、Cisco Aironet 1815I アクセスポイントがリブートします。
CSCwd20476	パッシブクライアントが有効になっている場合、ワイヤレスピアは相互に到達できません。
CSCwd21996	Cisco Catalyst 9120 アクセスポイントで、CleanAir センサーのクラッシュが発生します。
CSCwd22430	「archive download-sw」コマンドを使用した後、アクセスポイントはバックアップイメージを表示できません。
CSCwd25931	ワイヤレスクライアントは、有線 FlexConnect ローカルの動的ホスト構成プロトコル (DHCP) から IPv6 RA を受信しません。
CSCwd28109	Cisco Catalyst 9130 アクセスポイントでは、TFTP 中に高遅延またはパケットドロップが発生します。
CSCwd32900	Cisco Catalyst 9120 アクセスポイントは、4 ウェイハンドシェイク中に M4 をドロップします。
CSCwd34908	コントローラの動的チャンネル割り当て (DCA) デバッグでは、近くのアクセスポイントがチャンネル 36 を使用している場合にスロット 2 が表示されません。
CSCwd36187	コントローラは、ライセンス同期レポートを Cisco Smart Software Manager (CSSM) に定期的に送信しません。
CSCwc97199	ドライバと WCP の間で再関連付け要求の処理が遅延します。

Cisco IOS XE Cupertino 17.9.1 の未解決の不具合

警告 ID	説明
CSCwb70620	クライアントからの MIC エラーのため、WPA TKIP クライアントは参加できません。
CSCwc00005	Cisco Catalyst 9136 AP : 40/80 MHz 帯域幅が不正に使用されているときに、コントローラの Auto-RF がより低い干渉を報告しています。

警告 ID	説明
CSCwc05366	ワイヤレス AAA ダイナミック VLAN 割り当て：クライアントは相互に到達できません。
CSCwc15944	Cisco Catalyst 9800-L：マルチキャストトラフィックは、ワイヤレスシステムからワイヤレスクライアントに転送されません。
CSCwc24994	カーネルパニックが原因で Cisco AireOS 3800 シリーズ AP がクラッシュしています。
CSCwc25974	Cisco Catalyst 9136 AP：AP 自体で実行されるトラフィックは、隣接チャネルで干渉と見なされます。
CSCwc28757	Cisco AireOS 3800 シリーズ AP：スロット 0 で無線がクラッシュします。
CSCwc30314	FlexConnect ローカルスイッチングのローカル DHCP のときに CAPWAP で Cisco AireOS 4800 シリーズ AP からアップストリーム DHCP パケットが送信されています。
CSCwc31406	デバイス追跡データベースの古いエントリが原因で、IPv6 アドレスの偽の IP 盗難が発生しています。
CSCwc32182	Cisco AireOS 1852 AP：無線ファームウェアのクラッシュが観察されています。
CSCwc32360	IP 盗難が検出されたため、コントローラはクライアントを削除しています。
CSCwc39384	cnss_wait_for_fw_ready+0xd4/0x118 にあるときに PC で Cisco ワイヤレス 9164 AP がクラッシュします。
CSCwc41616	Cisco Catalyst 9105 AP：カーネルパニックが原因でクラッシュが発生します。
CSCwc46702	Cisco Catalyst 9800-L：rp_0_0 (rc=134) で重大なプロセス wncd 障害の理由でクラッシュが観察されます。
CSCwc60273	Cisco DNA Center の AAA ダッシュボードには、ソフトウェアのアップグレード後に AAA トランザクションデータが表示されません。

Cisco IOS XE Cupertino 17.9.5 の解決済みの不具合

ID	見出し
CSCwh60483	2023 年 4 月から 9 月の間に製造された Cisco Catalyst 9136I AP で誤った温度測定値が表示されます。
CSCwf79175	ペアワイズマスターキー ID (PMKID) が一致しない FlexConnect 中央認証で、ワイヤレスクライアントがローミングに失敗します。
CSCwf99932	Cisco Catalyst 9120 AP 無線 1 が予期せずリロードされます。
CSCwh09642	ゾーン ID が 0x00000000 の場合に IP 盗難が発生します。
CSCwd63620	RLAN スロットの RF タグマッピングを変更すると、コントローラで WNCID が予期せずリロードされます。
CSCwh63270	無線障害が原因で、Cisco Catalyst 9130AXI AP が予期せずリロードされます。
CSCwh71608	Cisco Aironet 1562 MAP が、Extensible Authentication Protocol (EAP; 拡張可能認証プロトコル) と flex-bridge サイトタグを使用して RAP に参加できません。
CSCwf22246	Cisco Catalyst 9130 AP における AP チップセット全体の管理フレーム数の計算が異なっています。
CSCwh27366	Cisco Aironet 3800 AP で無線ファームウェアのクラッシュが発生します。
CSCwf13879	Cisco Catalyst 9800-CL ワイヤレスコントローラが予期せずリロードされます。
CSCwf13107	Cisco Catalyst 9105 AP で長時間のテスト中に無線クラッシュが発生します。
CSCwf96138	Apple iPhone SE 第 3 世代でローミング障害が発生します。
CSCwh81332	Cisco IOS-XE 17.6.6 へのアップグレード後に、Cisco Catalyst 9130 AP でカーネルパニックが発生します。
CSCwh12481	Cisco Catalyst 9130 AXI-E AP が、国コードが TZ のコントローラに参加しません。
CSCwh57076	ブロードキャスト Address Resolution Protocol (ARP) 要求がコントローラからワイヤレスクライアントに転送されません。
CSCwf53520	Cisco IOS-XE Cupertino 17.9.2 でのカーネルパニックが原因で、Cisco Catalyst 1815 AP が異常終了します。

ID	見出し
CSCwh14232	モビリティイベント後に LLC または XID のスプーフィングフレームがコントローラから送信されません。
CSCwh92425	Cisco Catalyst 9130 または 9136 AP で、省電力モードのクライアントにデータフレームが送信されます。
CSCwh54762	SCB が削除保留状態の場合、AP でカーネルパニックが発生します。
CSCwf83292	Cisco Catalyst 9130 AP で、無線インターフェイスを介してクライアントに DHCP オファーと確認応答が送信されません。
CSCwi22895	リロードの理由が重要なプロセス Radio Resource Management (RRM; 無線リソース管理) の場合、コントローラが異常終了します。
CSCwi08147	ポリシープロファイルで QoS SSID policy が設定されていない場合、コントローラ GUI で Quality of Service (QoS) ポリシーを変更できません。
CSCwf07384	Cisco Catalyst 9105 AP の背後にある有線クライアントからトラフィックを渡せません。
CSCwf65794	無線障害が原因で Cisco Aironet 1852 AP が予期せずリロードされない。
CSCwh74663	Cisco Aironet 2800、3800、4800、1560、または Cisco Catalyst 6300 AP で、QoS データフレームがダウンストリームに送信されません。
CSCwh29924	Cisco Catalyst 9105、9115、または 9120 AP の設定に ab-Antenna が含まれている場合、アンテナ-a が正しく機能しません。
CSCwf52815	ICMP 到達不能 MTU 値を受け入れるように Cisco Wave 1 AP の PMTU 検出メカニズムが改善されています。
CSCwf75646	cRFStatusLastSwactReasonCode オブジェクトのすべてのコード化された整数値を含むコントローラ MIB ファイル。
CSCwf44441	Cisco Catalyst 9162 および 9164 AP で無線ファームウェアが異常終了します。
CSCwh82872	コントローラと AP 間のデータプレーンの問題により、アソシエーション要求がドロップされます。
CSCwf76119	認可変更 (CoA) および Access-Reject の後に、ペアワイズマスターキー (PMK) キャッシュを使用してクライアントが参加します。
CSCwe71996	Cisco Catalyst Center に関連付けられた AP が表示されません。
CSCwh59543	Cisco Catalyst 9120 AP 無線ファームウェアおよび CAPWAP がスケール期間中に異常終了します。

ID	見出し
CSCwf78066	フロアマップの「No radios in the selected band」メッセージが Cisco Catalyst Center ユーザーに表示されます。
CSCwfl3804	Cisco Catalyst 9120 AP が新しいクライアント関連付けのオンボーディングに失敗します。
CSCwh56147	AP ロケーションタグの SNMP OID がコントローラに表示されません。
CSCwh92459	rp_0_0 の wncd 障害でコントローラが異常終了します。
CSCwf40430	秘密共有キー (PSK) SSID パスワードの変更後、モバイルデバイスが Cisco Catalyst 9130 AP で誤ったパスワードを要求できません。
CSCwh20944	カーネルパニックが原因で Cisco Catalyst 9120 AP が異常終了します。
CSCwh70511	Closed transport communication channel メッセージが表示され、冗長性管理インターフェイス (RMI) がフラッシュします。
CSCwf32342	クライアントが正常にローミングできず、SDA 環境でトラフィックを渡せません。
CSCwi07401	ワイヤレスクライアント統計の収集中にコントローラが異常終了します。
CSCwh49810	WNCD 間ローミング後にクライアントがネットワークアクセスを失います。
CSCwf88890	特定の Cisco Aironet 3800 AP の [Monitoring] > [Wireless] > [AP Statistics] > [General] ページのロード中に、Cisco Catalyst 9800-L ワイヤレスコントローラ GUI がスタックします。
CSCwf54827	アイドルタイムアウト後に、ワイヤレスクライアントが認証解除されます。
CSCwh87903	特定のクライアント MAC アドレスに対して、Cisco Catalyst 9120 AP から認証応答エラーが送信されます。
CSCwh89539	クライアントスロットリングがオンになっている場合、CAPWAP メッセージが x 秒より長くキューに入れられます。
CSCwa16835	スイッチ仮想インターフェイス (SVI) MAC の変更後に、ファブリック AP と VXLAN トンネルが更新されません。
CSCwh63050	Cisco IOS-XE 17.9.3 を実行しているコントローラから、コントローラの IP アドレスと MAC アドレスのない IGMP クエリが送信されます。
CSCwh62342	ロケーション固有サービス (LSS) フィルタが 5 GHz 帯域で有効になっている場合、FlexConnect モードの AP が mDNS ゲートウェイとして正しく応答しません。

ID	見出し
CSCwh31966	WNCD プロセスでのデータベースの中断中にコントローラが異常終了します。
CSCwf93992	FlexConnect モードの Cisco Aironet 2800 AP で、遅延が 50 ミリ秒を超える EAP-TLS フラグメント化パケットが処理されません。
CSCwf81866	TFTP バックアップの設定中に、無線 0 ワークグループブリッジ (WGB) 設定が正しくバックアップされません。
CSCwf63818	カーネルパニックが原因で、Cisco IOS-XE Cupertino 17.9.2 バージョンを搭載した Cisco Aironet 1832 AP が異常終了します。
CSCwh58099	クライアントの削除と認可変更 (CoA) が終了すると、コントローラでクライアントの再接続が許可されます。
CSCvx90714	show interface status コマンドで、自動ネゴシエーションポートの最大リンク速度が表示されます。
CSCwf83132	ワイヤレス モビリティ グループ名を変更するときに、コントローラから 802.11r モビリティペイロードが送信されません。
CSCwh20306	Cisco Advanced Wireless Intrusion Prevention System (aWIPS) が有効になっている場合、FastLocate 機能が自動的に無効になります。
CSCwh87343	コントローラ GUI で特権昇格の脆弱性が発生します。
CSCwi08442	CBAR が有効になっている場合、AP がコントローラに接続しません。
CSCwf32806	コントローラが「Critical process wncd fault on rp_0_0 (rc=134)」で予期せずリロードされます。
CSCwf84639	XOR モードの Cisco Catalyst 9120 AP が radio_oper_data データベースで更新されません。
CSCwi07094	Simultaneous Authentication of Equals (SAE) が有効で、Opportunistic Key Caching (OKC) が無効になっている場合、Apple クライアントが Flex WPA2+WPA3 SSID に接続できません。
CSCwi06785	スイッチオーバー後、実行状態のワイヤレスクライアントに IPv4 の Gratuitous ARP (GARP) または IPv6 の Neighbor Advertisement (NA) がコントローラから送信されません。
CSCwf59348	Cisco Catalyst 9105、9115、および 9120 AP で、国 IE の最大送信電力レベルが -128dBm に設定されます。
CSCwh09879	国コードを変更後、FlexConnect モードの Wave1 AP で、クライアントの接続が許可されず、アソシエーション応答エラーが送信されます。

ID	見出し
CSCwh75431	Cisco Aironet 1830 または 1850 AP で誤って高いチャンネル使用率が報告され、5 GHz 帯域全体でパフォーマンスの問題が発生します。
CSCwh17592	デュアル無線が有効になっている場合、Cisco Catalyst 9130AXI AP スロット 1 で、HT (802.11an)、VHT (802.11ax)、および HE (802.11ax) 機能がアナウンスされません。
CSCwh30078	スループットテスト中に Cisco Aironet 1852 AP が異常終了します。
CSCwh88100	skb_unlink+0x40/0x54 で PC 使用時に、Cisco Aironet 3800 AP でカーネルパニックが発生します。
CSCwf92519	AP 電力プロファイルのステータスに予期しない「Insufficient De-rating」メッセージが表示されます。
CSCwf04815	カバレッジホール検出により、AP のスロット 0 と 1 の送信電力が削減されます。
CSCwh02698	コントローラから不完全なスケラブルグループタグ (SGT) 情報が Cisco ISE に送信されます。
CSCwf87281	ワイヤレス ネットワーク コントローラ デーモン (WNCd) プロセスでの予期しないリロードにより、コントローラが異常終了します。
CSCwd68141	show wireless wps rogue ap detail コマンドで、不正クライアントの封じ込めの詳細が表示されません。
CSCwh27425	Cisco Catalyst 9115AX AP で、CAPWAP データパケットの一部がアップリンク方向に転送されません。
CSCwh93655	Cisco Catalyst 9120 AP が 重大な状態 になっている場合、2.4 GHz と 5 GHz 無線の両方で 2x2 がストリーミングされます。
CSCwh08892	コントローラ GUI で、[User Login] ページの後に空白のページが表示されます。
CSCwh59048	コントローラで、グアテマラ (GT) 国の -A ドメインアクセスポイントがサポートされます。
CSCwh93462	show wireless stats ap loadbalance summary コマンドで、接続された AP または検出された AP の負の値が表示されます。
CSCwe24263	ビーコンフレームの国情報でアドバタイズされた送信電力レベルが Cisco Catalyst 9130 AP で一貫していません。
CSCwf62051	マルチキャスト DNS (mDNS) が有効になっている場合、カーネルパニックが原因で AP が予期せずリロードされます。

ID	見出し
CSCwh35072	Cisco Aironet 3800 AP が FIQ または NMI のリセットが原因で予期せずリロードされます。
CSCwi02479	セグメンテーション障害により、Cisco IOS-XE 17.9.3 を実行している Cisco Catalyst 9800-80 シリーズ ワイヤレス コントローラが予期せずリロードされます。
CSCwh99036	サポートされている AP チャネルの処理中に WNCd が異常終了すると、コントローラが予期せずリロードされます。
CSCwh61011	Cisco Catalyst 9120 および 9115 AP がコントローラから予期せず接続解除され、Datagram Transport Layer Security (DTLS) を再度確立できません。
CSCwh68360	カーネルパニックが原因で Cisco Catalyst 9120 AP が異常終了します。
CSCwh59420	Cisco IOS-XE Cupertino 17.9.4 で Cisco Catalyst 9136 AP が異常終了します。
CSCwh50681	Cisco IOS-XE Cupertino 17.9.3 ワイヤレスアップグレード後にのみ、新しい SSID arp0v0 がブロードキャストされます。
CSCwe81775	Apple デバイスは、Extensible Authentication Protocol (EAP) ログオフメッセージの送信後に削除されません。
CSCwh59109	重大なプロセス WNCd 障害により、コントローラがリロードします。
CSCwf69377	ERSPAN 送信元の更新で、コントローラ IOSd が span_db_port_bl_to_port_list で異常終了します。
CSCwh68768	パブリッククラウドの基本ワイヤレス設定を使用した Flex WLAN をコントローラで作成できません。
CSCwi03442	Real-time Transport Protocol (RTP) ストリームの中断を引き起こす不定期自動省電力配信 (U-APSD) トリガーフレームが、Cisco Catalyst 9130 AP で受け入れられません。
CSCwh08625	PC が _raw_spin_unlock 状態の場合、カーネルパニックが原因で Cisco Catalyst 9120 AP が異常終了します。
CSCwh20334	認可変更 (CoA) サーバーキーが、コントローラ GUI に空白で表示されます。
CSCwh49406	Cisco Catalyst 9130 AP で過剰な CleanAir syslog が表示されます。
CSCwh33190	カーネルパニックが原因で Cisco Catalyst 9115 AP が異常終了します。
CSCwi10656	大量のクライアントが WebAuth 保留状態になっているために IO ID が使い果たされると、新しいクライアントが参加できません。

ID	見出し
CSCwf50558	5 GHz で動的チャネル割り当て (DCA) アグレッシブを無効にしても効果がありません。
CSCwh61007	複数の AP をプロビジョニングすると、コントローラが異常終了します。
CSCwh33056	ロケーションから WLAN を削除すると、ポリシータグの説明が自動的に削除されます。
CSCwf83515	ビーコンフレームの国情報でアドバタイズされた送信電力レベルが一貫していないと、クライアント側の問題が発生します。
CSCwh68219	EAP-TLS を使用した 802.1x 経由での認証にクライアントが失敗します。
CSCwe58841	両方のポートでの Power over Ethernet (PoE) ネゴシエーションが Cisco Catalyst 9136 AP でサポートされていません。
CSCwe42200	完全修飾ドメイン名 (FQDN) を持つ RADIUS サーバーが、ドメインネームサービス (DNS) の定期更新中に正しく更新されません。
CSCwf64009	ループが発生しているポートの RLAN VLAN トラフィックが Cisco Aironet 1815 AP でリークされます。
CSCwh88246	設定が無効になると、URL フィルタが適用されません。
CSCwh45418	Cisco Catalyst 9124 AP で CDP を介して誤ったデュプレックス情報が送信されます。
CSCwf60519	無効なペアワイズマスターキー (PMK) ID が原因で、802.11r を使用して WNCN 間ローミングを実行するクライアントが失敗します。
CSCwh76420	In-Service Software Upgrade (ISSU) アップグレードの実行中にコントローラが異常終了します。
CSCwh44793	Cisco Catalyst 9130 AP がコントローラに接続できないと、サイトタグの変更後に BSSID に Fast Transition データが設定されます。
CSCwh20934	Cisco Wave 2 AP が繰り返し再起動し、Systemd の重大なプロセスがクラッシュします
CSCwe70039	N+1 高可用性スイッチオーバー後に、クライアントが認証ループでスタックします。
CSCwf86242	CAPWAP ウィンドウサイズが 0 に設定されると、コントローラが予期せずリロードされます。
CSCwi22847	AP から分析を受信後、Cisco Catalyst 9800-80 ワイヤレスコントローラが異常終了します。

Cisco IOS XE Cupertino 17.9.4a の解決済みの不具合

ID	見出し
CSCwh37783	コントローラ GUI で [Lobby Admin] ページがロードされません。
CSCwh22981	WNCD プロセスが異常終了します。
CSCwh21092	2つのコアファイル (cpp_cp_svr および cpp-mcplo-ucode) を含むシステムレポートの生成時にコントローラが異常終了します。
CSCwf68612	WNCdプロセスのセグメンテーション障害が原因で、コントローラが予期せずリロードされます。
CSCwf30701	静的 IP アドレスがないと、Cisco Aironet 2800 および Cisco Catalyst 9120 AP がサブリカントとして Extensible Authentication Protocol (EAP) プロセスを開始できません。
CSCwh29442	Cisco IOS-XE 17.9.x への In-Service Software Upgrade (ISSU) アップグレード後に、Cisco Catalyst 9800-40 ワイヤレスコントローラが異常終了します。
CSCwf83278	AP が CLIENT_DEL_STOP_REASSOC を送信すると、クライアントトラフィックが N+1 で失敗します。

Cisco IOS XE Cupertino 17.9.4a の解決済みの不具合

ID	見出し
CSCwh87343	Cisco IOS XE ソフトウェアの Web UI における特権昇格の脆弱性 詳細については、「Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z 」を参照してください。

Cisco IOS XE Cupertino 17.9.4 の解決済みの不具合

ID	見出し
CSCwf42824	Cisco Catalyst 9105AXW AP がアップグレード後に回復しません。
CSCwe38431	音声チャンネル可用性チェック (CAC) が設定されている場合、コントローラがアップストリームまたはダウンストリームで CS3 から CS0 に SIP パケットを再マーキングします。
CSCwe87973	Cisco Aironet 3800 AP が FIQ または NMI のリセットが原因で予期せずリロードされます。
CSCwd46815	Cisco Wave 2 AP : MAP の背後にある有線クライアントで EAP-TLS が失敗します。

ID	見出し
CSCwf34100	Samsung デバイス (Galaxy Tab S6 Lite - P610K) が Cisco AP との関連付けを試行すると、AP がステータスコード 40 で関連付け拒否を送信します。
CSCwd79502	FlexConnect と外部アンカー SSID で 2 つの異なる VLAN が使用されると、デバイストラッキングの古いエントリが観察されます。
CSCwe92340	カーネルパニックが原因で Cisco Catalyst 9136I-ROW AP が異常終了します。
CSCwe82892	プロファイルポリシーを使用して FlexConnect AP に接続されたクライアントが、ネイティブ VLAN ではなく VLAN 1 に割り当てられます。
CSCwe17593	Cisco Catalyst 9115 AP が、最初の接続から 60 秒後にルート AP へのトラフィックの送信を停止します。
CSCwf44483	Cisco Catalyst 9120AXI 5-GHz 無線 AP で、-A ドメインの AP がパナマ (PA) 国のコントローラに参加すると、動作がダウンしたままになります。
CSCwf04748	CALLBACK FULL による無線のリセットが原因で、AP が予期せずリロードされます。
CSCwd60034	ビーコンがスタックすると、Cisco Aironet 3800 AP 無線が予期せずリロードされます。
CSCwe25446	WNCD プロセスが原因でコントローラが予期せず再起動します。
CSCwe85742	コントローラが、N+1 AP フェールオーバー時にクライアントエントリの復元に失敗すると、PMK ID をクリアします。
CSCwe14729	DHCP 応答の Option 82 の処理時にメモリが破損することが原因で、コントローラが再起動する場合があります。
CSCwe04602	Cisco Wave 2 AP が、SDA ファブリック WLAN で約 60 秒間、ワイヤレスクライアントへのトラフィック転送に失敗します。
CSCwe11213	無線回復の失敗が原因で Cisco Catalyst 9130 AP がクラッシュします。
CSCwe30473	RC キューがスタックすると、Cisco Wave 2 AP 無線ファームウェアが予期せずリロードされます。
CSCwe49267	WNCD 間での Fast Transition ローミング後に、コントローラが GTK M5 パケットを Cisco IP Phone 8821 に送信しません。
CSCwe66216	インターフェイスの速度が 1000 に設定されている場合、Cisco Catalyst 9136 AP で MAC フラップ通知が発生します。
CSCwe73758	Cisco Catalyst 9115AX AP が 5 GHz 無線でビーコンを送信できません。

ID	見出し
CSCwe73403	SVI インターフェイスがダウンしている場合、EoGRE トンネルを使用する WLAN に DHCP Option 82 が追加されません。
CSCwe11315	Cisco IOS-XE 17.9.2 を実行する Cisco Catalyst 9164 および 9166 AP で、すべてのチャンネルにおいて DFS 検知が発生します。
CSCwe67580	パブリック IP を変更した後、OEAP とコントローラの間で CAWAP DATA トンネルが形成されません。
CSCwd91054	Cisco Wave 2 AP が、M1-M4 の後の EAP_ID_REQ を暗号化せず、dot1x Opportunistic Key Caching (OKC) の PMKID を更新しません。
CSCwe81552	伝送パワーコントロール (TPC) が、5 GHz 帯域で動作するセカンダリ無線で想定どおりに機能しません。
CSCwe56266	コントローラの起動中に RRM クラッシュが発生します。
CSCwe76818	Cisco Catalyst 9800-80 ワイヤレスコントローラ - Syslog 設定が AP に反映されません。
CSCwf29742	Cisco Catalyst 9120 AP : 80 以上のクライアントでマルチキャストを実行し、長時間実行すると、12 時間後にファームウェアのクラッシュが発生します。
CSCwe66515	Cisco Catalyst 9136 AP が、クライアントからの M2 応答に登録されません。
CSCwe74874	カーネルパニックが原因で Cisco Catalyst 9120 AP がランダムにクラッシュします。
CSCwf33623	AP が 802.3af (デフォルトモード) で動作している場合、Cisco Catalyst 9162I AP 無線で動作ステータスダウンが発生します。
CSCwe07802	Cisco Wave 2 AP が、アップストリームの Extensible Authentication Protocol (EAP) パケットをドロップします。
CSCwe01579	大規模なセットアップで RRM クライアントカバレッジを作成すると、WNCD がリロードされます。
CSCwe74653	Cisco Wave 2 AP がコントローラに DELETE の理由を送信しないため、古いエントリが残ります。
CSCwe18012	QOS テーブルをスタンバイコントローラに保存しているときに、そのスタンバイでクラッシュが発生します。
CSCwf07605	Cisco Catalyst 9105AXW AP および Cisco Aironet 1815W Flex RLAN AP が、AAA VLAN のオーバーライド後にイーサネットポートに VLAN を適用しません。

ID	見出し
CSCwe66730	動的周波数選択 (DFS) イベントの後、動的チャンネル割り当て (DCA) により誤ったチャンネルが割り当てられます。
CSCwf15582	ビーコンがスタックすると、AP 無線が予期せずリロードされます。
CSCwe62694	382 台の AP があるカスタマーネットワークで WNCD が無限ループに陥ります。
CSCwe91394	余分なバイトが原因で、Aeroscout T15e タグによって一時データが報告されません。
CSCwe70970	高可用性 SSO 展開用の冗長ポートではキープアライブを優先するオプションが必要です。
CSCwf44027	コントローラの GUI またはコンソールで、ワイヤレス 802.1x クライアントのユーザー名がランダムに欠落します。
CSCwf50177	Cisco Catalyst 9105AXW AP が多数の不良ブロックを検出します。
CSCwe39888	動的チャンネル割り当て (DCA) アルゴリズムの実行中に RRM プロセスがクラッシュします。
CSCwf07264	Crimson データベースにアクセスすると、WNCD が予期せずリロードされます。
CSCwe27839	長時間のテスト中に Cisco Catalyst 9120 AP でカーネルパニックが発生します。
CSCwe67810	Flexconnect スタンドアロンモードの Cisco Wave 2 AP が、18 分ごとの DHCP 更新時にクライアントを切断します。
CSCwe55390	Spectralink Phone のローミングによって音声の問題が発生した後、UP6 または音声トラフィックが 500 ミリ秒未満の場合に、Cisco Aironet 3802 AP でバッファリングが発生します。
CSCwe99957	AP の切断後、コントローラが AP からのキープアライブに応答しません。
CSCwe80617	入力または出力エラーメッセージの後、ワイヤレスクライアントが Cisco Aironet 1830 AP に接続できません。
CSCwb51757	チャンネルボンディングが 40 MHz に設定されている場合、5 GHz 無線でチャンネル使用率が高くなります。
CSCwf54714	コントローラが予期せずリロードされる。
CSCwe30429	Cisco Catalyst 9800-L シリーズ ワイヤレス コントローラで、最後にリロードした理由が「Critical process wncd fault」ではなく「reload」と表示されます。

ID	見出し
CSCwe35285	コントローラがクライアントを削除します。これは、CSCwd91054 の修正によって引き起こされた可能性があります。
CSCwf71255	APN+1 のフェールオーバーとポリシーの更新後にクライアントトラフィックが失敗します。
CSCwd72847	Cisco Catalyst 9115 AP がダウンストリームのマルチキャストトラフィックの送信を停止します。
CSCwf55303	RP リンクがアップ状態になると、アクティブコントローラが再起動します。
CSCwe53639	コントローラが「brain: +(awk sed)」に一致する大量のメッセージを送信します。
CSCwd56391	コントローラがデータベース内にある一部の RFID タグの受信信号強度 (RSSI) ロケーションデータを提供しません。
CSCwf22225	Cisco Catalyst 9120 AP : AP チップセット全体の管理フレーム数の計算を標準化します。
CSCwf42629	dot1x SSID に AAA オーバーライドによるセキュリティグループタグ (SGT) がある場合、VLAN グループはスタティック IP クライアントをサポートします。
CSCwe00848	Cisco Catalyst 9105 AP が予期せずリロードされます。
CSCwe15338	Cisco Catalyst 9120 AP : Tx がスタックし、AP がクライアントのプロンプトまたは認証に応答しません。
CSCwe07297	無線ファームウェアのクラッシュが原因で、Cisco Catalyst 9120 AP が予期せずリロードされます。
CSCwc49970	Cisco Aironet 2800、3800、4800 AP でチャンネル 165 が許可されません。
CSCwe92462	[Client Data Rate] チャートが、データレートではなく管理レートによって歪められます。
CSCwf09008	Cisco Catalyst 9800-L シリーズ ワイヤレス コントローラが、「Critical process wNCD fault on rp_0_0 (rc=139)」という最後にリロードした理由でクラッシュします。
CSCwe32853	Cisco Catalyst 9124AXI AP がリモート LAN (RLAN) トラフィックをアップストリーム ネットワークに転送しません。
CSCwd98332	アンカーメッセージ内のインターフェイス ID が一致しない場合、コントローラがリロードされます。

ID	見出し
CSCwe71081	macOS 設定アシスタント：ゲストの問題が発生します。
CSCwe84267	flex N+1 フェールオーバーモードの Cisco Wave 2 AP が、最初の CAPWAP データキープアライブを送信しません。
CSCwf67316	Cisco 2800、3800、4800、1560、IW6300 シリーズ AP が、CAC 時間後に必要なレベルのレーダーを検出しない場合があります。
CSCwe82287	保護された管理フレーム (PMF) の Wi-Fi Protected Access バージョン 3 (WPA3) クライアントが自己認証解除を開始した後、そのクライアントが関連付けを行うのを AP が防ぎます。
CSCwe30572	Cisco Wave 2 AP が iOX アプリからネットワークアドレス変換 (NAT) IP をリークします。
CSCwf45495	DHCP プロセス中にインターフェイスが 52 秒ごとにリセットされるため、Cisco Catalyst 9130 AP が CAPWAP の開始に失敗します。
CSCwf11117	Cisco Catalyst 9120 AP：ルート AP が、ローミング後にワークグループブリッジ (WGB) を継続的に認証解除します。
CSCwe95127	コントローラが、SNMP クエリ bsnAPIfDot11BSSID への応答で、特定の AP に誤ったデータを提供します。
CSCwe76817	AP で CAPWAP 最大伝送ユニット (MTU) の検出の問題が報告されます。
CSCwe91264	PC が get_partial_node.isra にある場合、AP が予期せずリロードされます。
CSCwd68141	show wireless wps rogue ap detail コマンドの出力で、不正阻止 LRAD が表示されません。
CSCwe19858	Cisco Catalyst 9130 AP が管理フレームで不適切なローカル電力制約値をアドバタイズします。
CSCwe17920	Cisco Catalyst 9124 AP が、セッションタイムアウト後にワークグループブリッジ (WGB) にトラフィックを転送しません。
CSCwf14803	アップグレード後、コントローラの Web UI メニューに暗号化された機能名が表示されます。
CSCwe74895	AP パケットキャプチャを実行すると、コントローラがクラッシュします。
CSCwf22788	show wireless client summary detail コマンドの出力に、すべての IPv6 アドレスが表示されません。
CSCwf88588	バージョン 17.9.3 への ISSU アップグレードの実行中に AP マネージャがクラッシュし、コントローラがブートループに入ります。

Cisco IOS XE Cupertino 17.9.3 の解決済みの不具合

ID	見出し
CSCwd41463	アクセスポイントが、Internet Group Management Protocol (IGMP) メンバシップレポートの送信を断続的に停止します。
CSCwf09259	AP LED の点滅が、再起動後に自動的にオンになります。
CSCwf57471	特殊文字を含むワイヤレス ポリシー プロファイルで Application Visibility and Control (AVC) を有効にすると、Web UI がハング状態になります。
CSCwe42302	プロファイル名が一致しない場合、リリース間コントローラモビリティ (IRCM) クライアントがサイレントに削除されます。
CSCwe45553	ワンショット AP サービスパック (APSP) のインストール中に表示されるエラーメッセージが明瞭になるように修正しました。
CSCwd86288	Cisco Catalyst 9800-80 シリーズ ワイヤレス コントローラが正常な場合でも、負荷平均の警告が表示されます。
CSCwe18185	新品の Cisco Catalyst 9130 AP (VID03) のデイズロ出荷時イメージに <code>iox.tar.gz</code> が含まれていません。
CSCwf71906	コントローラが、単一の IPv4 アドレスを持つクライアントの中央 Web 認証 (CWA) SSID の IP ソースガード (IPSG) データパスで IPv4 アドレスをプラミングしません。
CSCwd08068	メモリ不足 (OOM) が原因で Cisco Aironet 1815W AP がクラッシュします。WCPD により、8.10.171.0 (MR7) でメモリ不足が発生します。
CSCwe63089	AP の LED が散発的に白色に変化します。

Cisco IOS XE Cupertino 17.9.3 の解決済みの不具合

ID	見出し
CSCvx32806	イメージチェックサム検証の失敗により、COS-AP がブートループでスタックします。
CSCwb72924	FlexConnect クライアントが断続的に AP に再接続できません。
CSCwe10696	通常の ASR サポートフィールドが、サポート対象クライアントで無効になっています。
CSCwe24994	カーネルパニックが原因で Cisco Aironet 3800 シリーズ AP がクラッシュします (PC : <code>vfp_reload_hw+0x30/0x44</code>) 。
CSCwe32182	Cisco Catalyst 1852 AP : 無線ファームウェアのクラッシュが観察されます。

ID	見出し
CSCwc54410	スタンバイコントローラが HA ペアに再接続する際に、コントローラの HA デュアルアクティブシナリオが観察されます。
CSCwc55632	Cisco Catalyst 9124 MAP で MAP の最初のリロード後に Cisco Aironet 1562 RAP への接続に失敗します。
CSCwc75732	Cisco AireOS 4800 AP : ファームウェアの無線クラッシュが観察されます。
CSCwc79718	Cisco Catalyst 9166I AP : イメージのアップグレード後に複数のコアが報告されます。
CSCwc81656	AIR-CAP2702E-K-K9 でフラッシュファイルシステムの破損が観察されます。
CSCwc87688	Cisco Catalyst 9120 AP が、5 GHz 無線で非常に高いノイズレベルを示します。
CSCwc89183	コントローラのクラッシュが libewlc_client_dpath_svc.so で観察されます。
CSCwc97298	Cisco Catalyst 9166 AP : 無線-2 ファームウェアのクラッシュが観察されます (スレッド ID : 0x00000014、スレッド名 : WLAN_SCHED0、PC : 0x015dc73c)。
CSCwd02898	Cisco Catalyst 9300 シリーズ スイッチが、ローカル AP へのローミング後にリモート MAC アドレスをフラッシュしません。
CSCwd02960	Cisco Catalyst 9166 AP : XoR 無線 (スロット 2) で 5 GHz と 6 GHz を切り替えると、カーネルパニックが発生します。
CSCwd03803	PC が edma_poll にあるか、LR が dma_cache_maint_page にある場合、Cisco Aironet 1815I AP がリポートします。
CSCwd04025	PI 3.10.1 : コントローラに関連付けられた AP で、インターフェイスが「半二重」と表示されます。
CSCwd04571	負荷がかかると、WNCD プロセスでメモリークが発生します。
CSCwd06001	Cisco Catalyst 9800-L ワイヤレスコントローラのリロード中に、スタンバイコントローラで Linux IOSd のクラッシュが観察されます。

ID	見出し
CSCwd06018	WNCD間のローミング実行中に、無効なペアワイズマスターキー ID (PMKID) が原因で 802.11r の再認証に失敗しました。
CSCwd06122	古いクライアントエントリが原因の AP 接続の問題が報告されました。
CSCwd08678	タイマーが動作していません。古いクライアントがコントローラで削除されません。
CSCwd10570	Cisco Catalyst 9130 AP : 不正なデータレートでビーコンを送信します。異なる BSSID の同じスロットに対して異なるレートが送信されます。
CSCwd12120	IPv6_qos のコントローラスイッチでインジェクトパスのクラッシュが観察されます。
CSCwd12754	CAPWAP ワイヤレストラフィックのセキュリティグループタグ (SGT) が対応する着信有線トラフィックと同じです。
CSCwd19631	スイッチポートで EEE が有効になっている場合、Cisco Catalyst 9120 AP が mGig で動作しません。
CSCwd21996	Cisco Catalyst 9120 AP : CleanAir センサーがクラッシュしています。
CSCwd23681	「% Error: no ap_name exists」エラーにより、コントローラが AP 設定の更新に失敗します。
CSCwd26693	FlexConnect の N+1 HA が機能していません。
CSCwd28226	スニファモードの Cisco Catalyst 9136 AP で、capwapd のクラッシュに続いて、接続と接続解除のループが発生します。
CSCwd30828	Cisco Catalyst 9120 AP : カーネルパニックが原因でクラッシュが発生します。
CSCwd32107	Cisco Aironet 2700 AP : AP_LAN_CONFIG ペイロードに無効な RLAN ポートのイネーブル値があり、CAPWAP_PAYLOAD を無視します。
CSCwd34890	クライアントは、LWA+LocalSW+CentralAuth で IP アドレスを取得した直後に認証解除します。
CSCwd34908	コントローラが動的チャネル割り当て (DCA) の感度しきい値を満たしていません。

ID	見出し
CSCwd35393	ワイヤレス ロード バランシング アフィニティで、AP サイトタグがデフォルトサイトとして誤って表示されます。
CSCwd35577	ダブルビット ECC エラー時に冗長性障害が発生します。
CSCwd39605	カーネルパニックが原因で、Cisco Catalyst 9117 AP が console_unlock+0x320/0x3ac で予期せずリロードします。
CSCwd40731	カーネルパニックが原因で AP がリロードします。同期は実行されず、ソフトロックアップが発生し、タスクがハングします。
CSCwd41108	DART コネクタ搭載の Cisco Catalyst 9130AXE AP がチャンネル 36 でスタックします。
CSCwd46091	Cisco Catalyst 9105AXI AP が、15.4 ワットではなく 30 ワットの電力を要求します。
CSCwd46721	ODM データベース内の古いクライアントエントリが原因で、IP 盗難が発生します。
CSCwd46770	ライセンス：レポート間隔（固定 8 時間）が削除されて、同期レポートがユーザーアクションに変更されます。
CSCwd47741	コントローラが無線リソース管理（RRM）の動的チャンネル割り当て（DCA）のチャンネルを更新できません。
CSCwd49166	Cisco Aironet 3800 AP で、高い QoS Basic Set Service（QBSS）負荷が一貫して報告されます。
CSCwd49861	AIRESPACE-WIRELESS-MIB：bsnAPIfType OID ドキュメントが不完全です。
CSCwd52385	トークンの期限が切れた後、AP が Cisco DNA Center への gRPC 接続を正しく開始しません。
CSCwd52745	Cisco Aironet 3802 AP：カーネルクラッシュが観察されます。
CSCwd52938	ワークグループブリッジ（WGB）の背後にある有線クライアントがアンカー WLAN で IP アドレスを取得しません。
CSCwd55757	Wave 2 AP：Systemd の重要プロセスのクラッシュ - dnsmasq-host.service が失敗しました。
CSCwd56621	コントローラ GUI のログインバッファサイズが正しく表示されません。

ID	見出し
CSCwd59921	Cisco Catalyst 9130 AP が EAP-TLS フレームをドロップしています。
CSCwd60376	Cisco Catalyst 9120 AP : PC が pci_generic_config_read+0x34/0xa8 にあるとき、カーネルパニックが発生します。
CSCwd61428	Cisco Catalyst 9136I AP : gRPC クラッシュが観察されます。
CSCwd63516	プラグアンドプレイ (PnP) 設定がプッシュされた後、Cisco Catalyst 9120 AP が EAP-TLS ポート認証に失敗します。
CSCwd63665	Cisco Catalyst 9800-80 シリーズ ワイヤレス コントローラは、WSA が原因で 200 AP の WNCN で高い CPU 使用率を示しています。
CSCwd63861	ローミング統計をインクリメントすると、SIGSEGV のクラッシュが発生します。
CSCwd69780	NetFlow ウォッチドッグが原因のコントローラクラッシュが観察されます。また、拡張 NetFlow が原因の CPU 使用率の上昇が wncmgrd で観察されます。
CSCwd72295	Cisco Catalyst 9136 AP : 国コードが RO に設定されている場合、AP 無線がダウンします。
CSCwd74123	Cisco Catalyst 9105 OEAP : パーソナル SSID がビーコンで HE IE をアドバタイズしていません。
CSCwd74571	解放されたパケットを再利用すると、WCPD がクラッシュします。
CSCwd76693	プロファイルの不一致カウンタが増加しません。
CSCwd77188	Cisco Aironet 3802 AP : ビーコンの国 IE で複数の電力値をブロードキャストします。
CSCwd77823	Cisco Catalyst 9130 AP : 無線ファームウェアのクラッシュが観察されます。
CSCwd79178	Cisco Aironet 1840 OEAP : 無線障害が原因でクラッシュが発生します。
CSCwd79645	セッション中に AP が 1 回ドロップされると、ワイヤレスクライアントはセッションタイムアウト後に通信できなくなります。

ID	見出し
CSCwd80290	IOS AP イメージ証明書の検証失敗または期限切れのため、AP 接続の問題が発生しています。
CSCwd81523	Cisco Catalyst 9130 AP は、EAP ハンドシェイクの実行中、PMF クライアント TX 認証解除の後に EAP_ID_RESP の次の関連付け要求を送信しません。
CSCwd83840	Cisco Aironet 1830 AP : ワイヤレスクライアントが接続できず、「writing to fd 27 failed!」というエラーが表示されます。
CSCwd83841	EWC : AP が有線インターフェイスからサブネット 192.168.129.0/24 にパケットを送信していません。
CSCwd90472	デバイストラッキングに静的 IP MAC バインドを追加できません。
CSCwd90907	Cisco Catalyst 9164 AP : 無線 1 でクラッシュが観察されます。
CSCwd90909	Cisco Catalyst 9115 AP : 無線 1 でクラッシュが観察されます。
CSCwd93773	コントローラは、PoE+ (30W) を備えた 9124E では 2 つ目の 5 Ghz 無線を有効にすべきではありません。
CSCwd96376	Day-0 ウィザードで作成されたユーザーでコントローラ GUI や CLI にログインできません。
CSCwd99656	snmp-server host コマンドが文字列を適切にフィルタ処理しません (名前がたとえば TEST の場合に失敗します)。
CSCwe00248	Spectralink 84xx シリーズの電話機と Cisco Catalyst 9136 AP の間で、再関連付けの不正な動作が観察されます。
CSCwe06752	ワイヤレス管理インターフェイスが設定されていない場合、コントローラ GUI は HA/SSO を設定できません。
CSCwe08688	EWC : メッシュ AP の工場出荷時リセットモードを CAPWAP に変換して工場出荷時の状態にリセットした後、EWC に設定できません。
CSCwe11547	「rp_0_0 (rc=139) の重要プロセスの RRM 障害」でクラッシュが発生します。
CSCwe12057	アクセス制御リスト (ACL) の名前に二重引用符の特殊文字が含まれていると、QoS ページがロードされません。

Cisco IOS XE Cupertino 17.9.2 の解決済みの不具合

ID	見出し
CSCwe18524	編集または表示の後に追加操作を行うと、コントローラ GUI で AP フィルタエラーが発生します。
CSCwe26846	コンソールに「- check_dot1x_feature_status: config change or tams_init_not_done」のメッセージが大量に表示されます。
CSCwe28717	CMCA III を使用して AP を Cisco Catalyst 9800 コントローラに参加させると、証明書エラーが発生します。
CSCwe32728	無線障害が原因で Cisco Catalyst 9162 AP がクラッシュします。
CSCwe38326	Cisco Catalyst 9166 AP が CAPWAP 状態でスタックします。

Cisco IOS XE Cupertino 17.9.2 の解決済みの不具合

警告 ID	説明
CSCwa42620	Cisco Catalyst 9130 アクセスポイントで Phoenix WinNonlin アプリケーションの packets が送信中にドロップされます。
CSCwa86610	8.10.151.0 イメージの実行時に Cisco Aironet 2802 および 3802 アクセスポイントでカーネルパニッククラッシュが発生します。
CSCwc09461	Cisco Catalyst 9120 アクセスポイントは、長い遅延の後、認証応答フレームをクライアントに送信します。
CSCwc62021	Cisco Aironet 1815 および 1832 アクセスポイントで工場出荷時設定にリセットした後、デフォルトのクレデンシャルが機能しません。
CSCwc75102	DHCP オプション 43 を使用した ME から CAPWAP モードへの Mobility Express アクセスポイントの変換は機能しません。
CSCwc78435	Cisco Catalyst 9130 アクセスポイントは、アウトオブバンド DFS イベントで誤ったチャネルリストを送信し、クライアント接続の問題を引き起こします。
CSCwd00751	Cisco Aironet 2802 アクセスポイントは、8.10.171 リリースバージョンで予期せずリロードします。
CSCwd08259	Cisco Catalyst 9120、9115、および 9105 アクセスポイントでは、Cisco IOS-XE 17.3 以降のリリースで無線ファームウェアのクラッシュが発生します。

警告 ID	説明
CSCvv96364	Cisco Aironet 3800 アクセスポイントで、17.3.1 イメージの実行時に WCPd がクラッシュします。
CSCvx80422	10.128.128.127 または 10.128.128.128 アドレスを使用している場合、アクセスポイントはパケットの転送に失敗します。
CSCvz66623	メッシュアクセスポイント (MAP) の背後にある EAP-TLS クライアントで認証エラーが発生します。
CSCwb08291	Cisco Catalyst 9105AXW アクセスポイントでクライアントが RLAN ポートを使用していると遅延が発生します。
CSCwc05350	Cisco Wave2 アクセスポイント：アクセスポイントからコントローラまたはその逆の非対称の MTU が原因で、CAPWAP MTU フラッピングが発生します。
CSCwc10621	EWC に参加すると、CleanAir 統計は Cisco Catalyst 9130 アクセスポイントに表示されません。
CSCwc35321	ローカルモードの Cisco Wave2 アクセスポイントで、Address Resolution Protocol (ARP) 要求が IP アドレス 10.128.128.128 からワイヤレスクライアントに送信されます。
CSCwc38912	アクセスポイントサイトまたはポリシータグを Flex ローカルスイッチングセットに変更すると、ローカル Web 認証 WLAN へのクライアント接続が断続的に失敗します。
CSCwc51894	「dp_print_host_stats」ログによるカーネルパニックが原因で、Cisco Catalyst 9117 アクセスポイントが予期せずリロードします。
CSCwc56774	静的 IP を持つワークグループブリッジ (WGB) は、複数回のローミング後に IP アドレスを失います。
CSCwc71198	VRRPv3 がネットワークに存在する場合、CAPWAP フラッピングが観察されます。
CSCwc73462	RADIUS サーバーの共有秘密の末尾にあるバックスラッシュ「\」は、FlexConnect グループ設定では許可されません。
CSCwc81341	Cisco Catalyst 9130 アクセスポイントでは、フルデータパケットキャプチャが有効になっていると、ローカルモードでカーネルパニッククラッシュが発生します。
CSCwc89719	無線障害が原因で Cisco Aironet 1832 アクセスポイントがクラッシュします。

警告 ID	説明
CSCwc96683	Flex ローカルスイッチングで Cisco Aironet 3800 アクセスポイントを備えた Cisco IOS-XE 17.3.5a を実行しているコントローラは、DF で受信した IP フラグメント化パケットを転送しません。
CSCwd07572	アクセスポイントは、2.4 GHz または 5 GHz 帯域でアクティブな場合、6 GHz での UBPR の送信を停止します。
CSCwc05366	SSID で AAA を使用してダイナミック VLAN 割り当てを実行すると ARP 解決が失敗するため、ワイヤレスクライアントが相互に到達できません。
CSCwc15533	ポリシープロファイルへのスケール Flexible NetFlow (FNF) マッピングを使用した継続的な wncmgrd CPUHOG トレースバックにより、wncd 使用率が 100% になります。
CSCwc15944	マルチキャストデータはクライアントに送信されず、一部のアクセスポイントはコントローラに参加できません。
CSCwc22468	クライアントが dot11r と dot11i 間を遷移してアクセスポイント間をローミングすると、クライアントトラフィックが失敗します。
CSCwc26105	インターフェイスに複数のセカンダリアドレスがあることが原因で、ハイアベイラビリティのスプリットブレインが発生します。
CSCwc42784	プロトコルベースの Quality of Service (QoS) が構成されている場合にクライアントの接続に失敗します。
CSCwc57227	コントローラで予期しないリセットが発生し、wncd コアファイルを含むシステムレポートが生成されます。
CSCwc59518	Cisco Catalyst 9800-80 ワイヤレスコントローラは、32 文字の WLAN プロファイルを使用し、音声のチャネル可用性チェック (CAC) が無効になっているとクラッシュします。
CSCwc68682	Cisco Catalyst 9800 ワイヤレスコントローラ - ローカル障害が原因でリンクダウンします。
CSCwb47040	電波による固体識別 (RFID) のロケーションがコントローラで正しく更新されません。
CSCwb78191	iPSK 認証およびアンカー WLAN で AAA VLAN オーバーライドが考慮されません。

警告 ID	説明
CSCwc17774	Cisco IOS-XE 17.6.1 では、CISCO-ENHANCED-MEMPOOL-MIB のいくつかの OID で「スイッチオーバー後にインスタンスがありません」と表示されます。
CSCwc26819	モビリティイベント後に LLC または XID のスプーフィングフレームがコントローラから送信されません。
CSCwc28408	wncd の重大なプロセスの失敗により、コントローラが断続的にクラッシュします。
CSCwc36125	コントローラで最後の状態が追跡されないため、レポートのたびに Radio Resource Management (RRM : 無線リソース管理) の起動モードがトリガーされます。
CSCwc41358	コントローラの MAC フィルタリング : WLAN プロファイルの列に WLAN の名前と説明が表示されます。
CSCwc41903	Syslog 「LISP RELIABLE REGISTRATION」 を拡張する必要があります。
CSCwc57836	HTTP モードによる構成の復元は、EWC では機能しません。
CSCwc62824	モビリティイベント後に LLC または XID のスプーフィングフレームがコントローラから送信されません。
CSCwc69815	Cisco Catalyst 9300 スイッチのインターフェイスは、AIR コントローラライセンスが正しく処理されない場合、8 時間ごとに RUM レポートを生成します。
CSCwc72047	アクセスポイントは、Cisco IOS-XE 17.6.2 リリースバージョンで無効になっている RF プロファイルチャンネルで動作します。
CSCwc74020	コントローラのデータパスで 8 個の IP アドレス制限を増やす必要があります。
CSCwc76905	DHCP メッセージを処理するときに、スイッチの統合セキュリティ機能 (SISF) のクラッシュが観察されます。
CSCwd17349	Cisco IOS-XE 17.9 リリースバージョンで SSO フェールオーバー中にアクティブシャーシがスタックします。

Cisco IOS XE Cupertino 17.9.1 の解決済みの不具合

警告 ID	説明
CSCwb52755	Fast Transition 対応の Apple および Android クライアントが、IPSK プロファイルを使用した認証に失敗します。
CSCwb09248	Cisco Catalyst 9130 AP に関連付けられている場合、大きな遅延やパケットドロップが発生します。
CSCwb76935	Cisco Aironet 1815T AP : OEAP カーネルパニッククラッシュが観察されます。
CSCwb97557	Cisco Aironet 3800 AP : Slot0 BSSID ビーコンフレームは、slot1 無線で受信されます。
CSCwc04197	冗長スイッチオーバー中にセカンダリコントローラのクラッシュが観察されます。
CSCwc04328	6 GHz RRM : チャネル認識 TPC は、6 GHz TPC に対して常にオンです。
CSCwc04673	WLAN フラッピング時に、ieee80211_mbssid_del_profile で Cisco Wireless 9166 AP がクラッシュしました。
CSCwc07014	AP は、クライアント FT-SAE ローミングが成功した後、空の FlexConnect クライアント キャッシュ ペイロードをコントローラに送信します。
CSCwc08770	Cisco Wave 2 AP : AP SSH グローバル設定が無効になっている場合、AP への SSH を実行できます。
CSCwc15229	無線障害（ビーコンのスタック）が原因で Cisco Aironet 1832 AP がリロードされます。
CSCwc17898	コントローラにすでに存在する名前でも AP に参加しているときにクラッシュが観察されました。
CSCwc20929	APP ホスティング セグメンテーションは、17.6.3 を実行しているコントローラに接続された Cisco Catalyst 9100 AP では機能しません。
CSCwc21428	6GHz 無線 : 使用率が高いため、チャネルの変更が頻繁に発生します。
CSCwc27716	mDNS ルールの削除および追加中にメモリリークが発生します。

警告 ID	説明
CSCwc29238	wgb が 2.4 GHz で ap に関連付けられ、wgbwiredclient が ipv4 を取得するようにトリガーした後、WGB ping ゲートウェイが失敗しました。
CSCwc29760	Cisco Aironet 3800 AP : AP の led_core が原因でクラッシュが発生します。
CSCwc31277	6 GHz : ビーコンのスタック + QBSS 100% で、回復 AP はありません。
CSCwc40483	AP のスロット 1 に送信電力が適用されていません。
CSCwc43716	サイト調査モードでログイン情報を使用して AP CLI にログインできません。
CSCwc46228	Web UI でスペースを含む AP ロケーション名を追加できません。
CSCwc62021	Cisco Aironet 1815 および 1832 AP : 工場出荷時のリセット後、デフォルトのログイン情報が機能しません。
CSCwa65584	コントローラは、TrustSec 対応プラットフォームとして Cisco Catalyst C91xx シリーズ アクセスポイントを受け入れません。

トラブルシューティング

最新の詳細なトラブルシューティング情報については、『[トラブルシューティングテクニカルノート](#)』を参照してください。

関連資料

- [Cisco IOS XE](#)
- [シスコ検証済みデザイン - デザインゾーン](#)
- 選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするために使用する [MIB Locator](#)

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](#)
- [インサービス ソフトウェア アップグレードのマトリックス](#)
- [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](#)

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 ワイヤレスコントローラ データシート

- [Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ データシート](#)
- [Cisco Catalyst 9800-80 ワイヤレスコントローラ](#)
- [Cisco Catalyst 9800-40 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](#)

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

- [Compare specifications of Cisco wireless APs and controllers](#)
- [Wireless LAN Compliance Lookup](#)
- [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](#)

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 Connected Mobile Experiences**[Cisco Connected Mobile Experiences マニュアル](#)**Cisco Catalyst Center**[Cisco Catalyst Center のマニュアル](#)

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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2024 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。