

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ (Cisco IOS XE 17.18.3) リリースノート

目次

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、Cisco IOS XE 17.18.3	3
新しいソフトウェア機能	3
動作における変更	4
Cisco IOS XE 17.18.3 リリース以降の今後の変更に関するお知らせ	5
解決済みの問題.....	7
未解決の問題	10
既知の問題	12
互換	12
サポートされるハードウェア	28
関連情報.....	38
通信、サービス、およびその他の情報 :	39
法的情報.....	40

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、Cisco IOS XE 17.18.3

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク向けに設計された次世代のワイヤレスコントローラ群で構成されています。

コントローラは、次のように、さまざまな形式に対応しているため、展開オプションに合わせて選択できます。

- Catalyst 9800 シリーズ ワイヤレス コントローラ アプライアンス
 - Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ (C9800-L、C9800-40、C9800-80)
 - Cisco CW9800 シリーズ ワイヤレス コントローラ (CW9800L、CW9800M、CW9800H1、CW9800H2)
- クラウド向け Catalyst 9800 シリーズ ワイヤレス コントローラ
- Catalyst 9000 シリーズ スイッチに組み込まれた Embedded Wireless Controller (EWC)

このドキュメントでは、Cisco IOS XE 17.18.3 で導入された、または強化された新しいソフトウェア機能、動作の変更、問題、サポート対象ハードウェアなどについて説明します。

新しいソフトウェア機能

このセクションでは、このリリースで導入された新しいソフトウェア機能について簡単に説明します。

表 1. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 17.18.3 の新しいソフトウェア機能

製品への影響	機能	説明
ソフトウェアの信頼性	WPA3-Enterprise での GCMP-256 サポートの拡張 (AKM 3/5)	WPA3 仕様バージョン 3.4 では、AKM 00:0F:AC:05 (dot1X-SHA256) と 00:0F:AC:03 (FT-dot1X) を使用する場合に、WPA3-Enterprise (非 192 ビットモード) が GCMP-256 暗号をサポートするという必須要件を導入しています。この変更は、Wi-Fi 7 (802.11be) 機能を有効にするために必要です。これを容易に行うために、コントローラは AKM に GCMP-256 をサポートするようになりました。 さらにこのリリース以降、コントローラは自動アップグレードメカニズムを装備し、既存の WLAN の適合性と性能の維持を確保しています。システムは、次のすべての基準を満たす WLAN 設定に暗号 GCMP-256 を自動的に追加します。 • AKM 3 (FT dot1X) や AKM 5 (dot1X-SHA256) を使用して、WPA3-Enterprise (非 SuiteB) で設定した WLAN。 • 非 SuiteB モードで作動。 • ビーコン保護が有効。 • 802.11be (Wi-Fi 7) プロファイルは、少なくとも 1 つのアクティブリンクで適用されます。 この機能拡張により、暗号サポートの欠落により WLAN が 802.11ax (Wi-Fi 6) に自動的にダウングレードすることがなくなり、クライアントが正常に関連付けられ、高性能の Wi-Fi 7 接続が維持されます。
コンプライアンス	フェーズ 2 の国向けに CW9171I と CW9174I/E AP のチャンネルと電力テーブルを最適化	このリリースでは、CW9171I と CW9174I/E AP のチャンネルと電力テーブルを更新し、フェーズ 2 の国における地域の規制に基づいて性能を最適化しました。

製品分析

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

「[Cisco Enterprise Networking 製品分析に関する FAQ（よくある質問）](#)」[英語]を参照してください。

動作における変更

表 2. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 17.18.3 の動作における変更

機能	説明
メッシュ PSK のダウングレード手順を更新 (リリース 26.1.1)	Cisco IOS XE 26.1.1 から 17.18.x や 17.15.x などの古いリリースへのダウングレードプロセス中に、認証方式が PSK であれば、MAP を接続できません。 メッシュ認証に PSK を使用していて、この修正を含まないバージョンにダウングレードする必要がある場合は、次の手順を実行します。 1. ダウングレード前：デフォルトの PSK を有効にします。 2. ダウングレード後：プロビジョニングした PSK を変更しない場合、MAP は通常、コントローラに正常に参加します。PSK を使用して MAP が参加に失敗した場合は、次のリカバリ手順を実行します。 • メッシュ認証方式を EAP に変更します。 • MAP が EAP を介してコントローラに参加したら、影響を受ける各 AP のコントローラで次のコマンドを実行します。ap name <i>ap-name</i> mesh security psk provisioning delete • メッシュ認証方式を PSK に戻します。MAP はデフォルトの PSK を使用して参加し、プロビジョニングした PSK に自動的に更新します。 3. すべての AP がコントローラに正常に参加したら、デフォルトの PSK を無効にします。
コントローラ Web UI のモニタリング ワイヤレス クライアント グリッドの機能拡張	[モニタリング (Enhancements)] > [ワイヤレス (Wireless)] > [クライアント (Clients)] グリッドに [ポリシータイプ (Policy Type)]、[暗号化方式 (Encryption Cipher)]、[認証キー管理 (Authentication Key Management)] (AKM) を追加しました。
規制アクティベーションファイル (RAF) の NETCONF/YANG サポート	以前のリリースでは、CLI コマンド と GUI プロセスを介して AP 上の規制ドメインをアクティブ化すると、地域の規制を確実に遵守できました。 動作の変更により、NETCONF/YANG は規制アクティベーションファイル (RAF) をサポートするようになりました。 次の RAF EXEC CLI と show コマンドに RPC-YANG サポートを追加しています。 • ap regulatory activation file <i>file-name</i> • ap regulatory activation apply • ap regulatory activation clear all • ap regulatory activation clear <i>mac-address</i> • clear ap name <i>ap-name</i> country • show ap regulatory activation all • show ap regulatory activation mac <i>mac-address</i>

機能	説明
スロット 0 で 160 MHz のチャンネル幅サポート	以前のリリースでは、スロット 0 を 2.4 GHz と 5 GHz をサポートする FRA スロットとして設定している場合、スロット 0 のチャンネル幅は 80 MHz までのみ設定できました。160 MHz はサポートしていませんでした。動作の変更により、スロット 0 で 160 MHz をサポートするようになりました。
6 GHz 非対応の国で XOR バンドを 5 GHz に戻した後も、無線の電源はダウンを継続	バージョン 17.15、17.18、26.1.1 を実行しているシスコ ワイヤレス コントローラ WebUI では、6 GHz をサポートしていない国で XOR 無線を 6 GHz から 5 GHz に戻すと、5 GHz 無線が電源オフ状態のままになることがあります。動作の変更により、WebUI は無線状態を処理し、サポート非対応バンドに無線を移動したときに適切な警告を発します。こうしてバンド変更後に無線の電源がオフのままになるのを防ぎます。

Cisco IOS XE 17.18.3 リリース以降の今後の変更にに関するお知らせ

シスコは、ますます巧妙化する攻撃者から製品とお客様のネットワークを保護することに取り組んでいます。コンピューティング能力と脅威の状況が進化するにつれて、現在使用されている一部の機能やプロトコルが攻撃に対して脆弱になっています。より安全な代替プロトコルが利用できるようになったものの、一部の環境ではレガシープロトコルが依然として使用されている可能性があります。

ネットワークセキュリティを向上させ、攻撃対象領域を減らし、機密データを保護するために、シスコはレガシーの安全でない機能およびプロトコルの段階的な廃止を開始しています。これに伴い、お客様にはより安全な代替品への移行を推奨しています。このプロセスは段階的に行われ、運用への影響を最小限に抑えるように設計されています。これは、シスコ製品をデフォルトの状態より安全なものとし、設計段階から安全性を高めるための広範な計画の一環です。

Cisco IOS XE 17.18.2 リリース以降、シスコのソフトウェアでは、機密データを暗号化せずに送信したり、古い暗号化メカニズムを使用したりするなど、十分なセキュリティを提供しない機能またはプロトコルを設定すると警告メッセージが表示されます。警告は、セキュリティのベストプラクティスに従わない場合にも、安全な代替方法の提案とともに表示されます。

次に示すのは、バージョン Cisco IOS XE 17.18.2 以降のリリースで警告を生成する予定の機能とプロトコルのリストです（このリストは変更される可能性があります）。

各リリースのリリースノートに、そのリリースの正確な変更内容が記載されています。

- **プレーンテキストおよび脆弱なログイン情報の保存：**構成ファイルのタイプ 0（プレーンテキスト）、タイプ 5（MD5）、またはタイプ 7（ヴィジュネル暗号）。

推奨：可逆性ログイン情報にはタイプ 6（AES）を使用し、非可逆性ログイン情報にはタイプ 8（PBKDF2-SHA-256）またはタイプ 9（Scrypt）を使用します。

- **SSHv1：**

推奨：SSHv2 を使用します。

- **SNMPv1 および SNMPv2、または SNMPv3（認証および暗号化なし）：**

推奨：認証および暗号化（authPriv）付きの SNMPv3 を使用します。

- **SNMPv3 の MD5（認証）および 3DES（暗号化）：**

推奨：認証には SHA-1 か、できれば SHA-2 を使用し、暗号化には AES を使用します。

- **IP ヘッダーオプションに基づく IP 送信元ルーティング :**

推奨 : このレガシー機能は使用しないでください。

- **TLS 1.0 および TLS 1.1 :**

推奨 : TLS 1.2 以降を使用します。

- **デジタル署名に SHA1 を使用する TLS 暗号 :**

推奨 : SHA256 またはそれ以上の強度のデジタル署名を使用する暗号を使用します。

- **HTTP :**

推奨 : HTTPS を使用します。

- **Telnet :**

推奨 : リモートアクセスには SSH を使用します。

- **FTP および TFTP :**

推奨 : ファイル転送には SFTP または HTTPS を使用します。

- **オンデマンドルーティング (ODR) :**

推奨 : CDP ベースのルーティング情報交換の代わりに、標準的なルーティングプロトコルを使用します。

- **BootP サーバー :**

推奨 : DHCP またはセキュア ZTP などのセキュアブート機能を使用します。

- **TCP および UDP 小規模サーバー (echo、chargen、discard、daytime) :**

推奨 : ネットワークデバイスではこれらのサービスを使用しないでください。

- **IP フィンガー :**

推奨 : ネットワークデバイスではこのプロトコルを使用しないでください。

- **NTP 制御メッセージ :**

推奨 : この機能は使用しないでください。

- **事前共有キーと MD5 を使用した TACACS+ :**

推奨 : Cisco IOS XE 17.18.1 リリースで導入された、TACACS+ over TLS 1.3 を使用します。

- **ワイヤレス LAN コントローラ、CAPWAP DTLS :**

推奨 : DTLSv1.0 および弱い暗号スイートは使用しないでください。

- **ワイヤレス LAN コントローラ、WLAN :**

推奨 : 802.1x キー管理セキュリティは使用しないでください。

- **ワイヤレス LAN コントローラ、モビリティ :**

推奨 : 弱い暗号を使用せず、より強力な暗号を使用します。

- **ワイヤレス LAN コントローラ、NMSP :**

推奨 : 弱い暗号を使用せず、強力な暗号を使用します。

シスコは、この移行を通じてお客様のサポートに全力で取り組んでいます。Cisco IOS XE 17.18 トレインの後続のリリースでは、これらの機能が引き続きサポートされますが、使用時には警告が表示されます。将来のリリーストレインでは、これらの機能の使用がさらに制限される可能性があります、その場合はリリースノートを通じてお知らせします。

詳細については、「[Resilient Infrastructure IOS XE Security Warnings Reference](#)」を参照してください。

解決済みの問題

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

表 3. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 17.18.3 で解決済みの問題

不具合 ID	説明
CSCwo98441	GPS モジュールの未加工出力がわずかに変化すると、コントローラへの GNSS データが大きく変動する
CSCwp10723	CW9171I - 6Ghz 管理状態が無効になったときに、5Ghz 動作状態がダウンする
CSCwp34745	9130AX kernel panic pc : __qdf_bug+0x0/0x8 [qdf]
CSCwp59643	17.12.4 でのソフトロックアップと Null ポインタの参照解除が原因で COS AP がクラッシュする
CSCwr07706	次の原因により C9120 txerr が通知され、続いて Dot11BaseDriver が回復する : 48 - 無線の切り替え
CSCwr20303	AP ロケーション名の設定の変更後にコントローラを想定外にリロードする
CSCwr56409	Flexconnect の AP でワイヤレスクライアントが有線から IPv6 RA を受信しない
CSCwr65627	プライマリがダウンすると、多数の AP (2K 以上) が N+1 コントローラに参加するまでに数分かかる
CSCwr67024	AP の IP 送信元が正しくないため、エッジはアクセストンネルではなく L2LI0 インターフェイスで AP から検出を受信する
CSCwr75465	AP 名をコントローラにすでに存在する AP 名に変更した後、wncd 99% ~ 100% の高い CPU 使用率が発生する
CSCwr77247	17.18.2 を実行している 9174I での AP のクラッシュ : カーネルパニック
CSCwr77993	17.18.1 で実行している 9176 AP で、カーネルパニックがクラッシュ
CSCwr81031	kmalloc スラブにて 9176 AP でメモリーリーク
CSCwr90981	5GHz 無線での AP 数の変動
CSCwr98669	C9176 FW クラッシュ - cnss_pci 0004:01:00.0: クラッシュ発生
CSCws01793	9178 アクセスポイントで起動中に nss ドライバ初期化失敗
CSCws06706	C9178 : MAC HW ハング/PHY エラーが原因でクライアントが 2.4 無線に参加できない

不具合 ID	説明
CSCws08240	Wi-Fi 7 AP : パワーオンリセットにより、コントローラで理由のリロードを伴うクラッシュファイルを生成 - 33
CSCws08681	CW9178I AP - nss カウントが増加しないため、クライアントが接続できない
CSCws19380	ISSU アップグレード中にコントローラがクラッシュする
CSCws22667	Cisco 9105AWX/9172H AP の RLAN ポート 2 と 3 を介したアップロードでスループットに問題、ポート 1 は影響なし
CSCws26825	9105 が「RX too late errors」というエラーが原因でクライアントの受け入れを停止する
CSCws27309	CW9162I-ROW AP が 17.12.04 を実行している 9800-CL から切断中 - SMU パッチ済
CSCws32133	wncd プロセスでのクラッシュにより 9800 コントローラがリロードする
CSCws39889	RF ベースの AP ロードバランシング : ロード バランシング アルゴリズムの実行中の観測によるコントローラのクラッシュ
CSCws47700	WGB ローミングは wncd プロセスの想定外のリロードとワイヤレスコントローラのリロードを引き起こす可能性あり
CSCws53690	SST : 17.12.6a ->17.18.2 ISSU、アクティブ -> スタンバイ後に AP が切断される
CSCws58494	WebAuth クライアントがコントローラで実行状態に移動したが AP の WebAuth でスタックしている
CSCws58703	SST : 17.15.x から 17.18.2 への ISSU アップグレードの後に ndbmand コアが確認され、CatC と NETCONF が機能しない
CSCws65956	コントローラが wncmgrd でクラッシュし制限中 (rc 139)
CSCws66689	RLAN ポート 1 が接続されている場合、9172H は wired0 ではなく wired1 から DHCP Discover を送信
CSCws68160	クライアントの削除後、コントローラが「Critical process wncd fault on rp_0_0 (rc=139)」で想定外のリロード
CSCws68505	カーネルパニックが原因で AP がクラッシュする
CSCws76688	Flex モードで AP が「4 ウェイハンドシェイクの後に EAP アイデンティティ要求を送信」した状態で OKC が有効になっている場合、Catalyst 9800 でクライアントが AUTHENTICATING 状態でスタックする
CSCws77227	AP CW9176I カーネルパニッククラッシュ
CSCws77337	sdavc アプリケーションパックが原因で /tmp に十分なスペースがないため、9166 SDA AP にイメージのダウンロードの問題が発生
CSCws80385	AP CW9176I カーネル パニック ランダム クラッシュ
CSCws91899	Flex Connect クライアントの処理中に C9800 がクラッシュ
CSCws93542	フェールオーバー後の DHCP オファーをコントローラがクライアントに転送しない
CSCwt00254	WebAuth で欠落している SSL 非同期 FD の選択解除による匿名メモリリーク
CSCwt01278	17.18.2 で、9115/9120 AP がカーネルパニッククラッシュを起こす

不具合 ID	説明
CSCwt05272	カーネルパニックが原因で AP 9120 がクラッシュする
CSCwt08175	PC が _ZN17SPSCPRIORITYQueue4pushEiP6Packet+0x7c/0x4c8 に、LR が _ZN17SPSCPRIORITYQueue4pushEiP6Packet+0x40/0x4c8 にあるため AP カーネルパニックが発生
CSCwt08728	CW9179F : CA 国の 5GHz チャンネルマッピングが電源テーブルにない
CSCwt09003	AP が 中央認証によりフレックス接続モードになっている場合、クライアントが「FT+SAE」に接続しない
CSCwt20299	アプリケーション トラフィックは、補助クライアント インターフェイスの代わりに出力インターフェイスとして wired0 を使用
CSCwt31565	17.12.6a を実行している Cisco 9800-40-K9 で、ワイヤレスクライアントが RUN 状態でスタック
CSCwt31826	不正なプロセスでの SIGSEGV が原因で絶え間なくスイッチオーバーやリロードが発生
CSCwt37351	無線 WLAN ID のハンドラ ID が無効なため、wnacd プロセスが予期せず終了し、コントローラがリロードする可能性がある
CSCwt52617	SSO 後 - ファブリック外のデバイスへの接続が失われるワイヤレスクライアントがほとんどない
CSCwt53021	国コードが SR に設定されている場合、CW9163-E AP の 2.4G 無線が起動しない
CSCwo98826	[9179 屋外モード (9179 Outdoor Mode)] 6GHz 電力モードの理由は、DB10 屋外モード自動モードの場合、「AFC ライセンスは AP では使用できません」と表示される
CSCwq11290	17.15.4[SST] - Ble トランスポートでメモリリークが確認される
CSCwq73441	CW9172I AP : 17.15.4 実行中のカーネルパニック
CSCwr30777	9800 スタンバイシャーシが、17.12.4「show inventory」からの出力で Cisco Unknown Power Supply および同じ SN を表示する
CSCwr74373	不正な関連付け解除が発生しても、C9800 コントローラ アカウンティング要求パケットが送信されない
CSCwr77108	FlexConnect ローカル認証で FT11r または OKC を使用している場合、AP が RADIUS サーバーがプッシュした VLAN を破棄する
CSCwr77143	CW9166/IW9167 : 17.15 実行中のカーネルパニッククラッシュ
CSCwr79853	ファイルマネージャで、ロケーションボックスにあるファイルを選択すると、ダウンロードが失敗する
CSCwr87352	UI からメッシュの国別制限の警告を削除する
CSCwr87656	9800 コントローラ RADSEC - Acct-Session-Time 値が断続的に空白になる
CSCwr96614	C9120 COS AP が capwapd.service でクラッシュ : メインプロセスが終了、code=killed、status=4/ILL
CSCwr96860	AP モデル 3800E および 9120AXE の RESTCONF RPC を介したアンテナゲイン設定が失敗し、「slot: 0 does not have a dedicated radio」エラーが発生する
CSCwr97281	9105 AP が「auto-rf」結果で干渉を過剰に報告している
CSCws10863	9800 - 未解決の規制ドメインを持つ AP が、他の AP の RRM の実行を停止させる

不具合 ID	説明
CSCws17702	レコードプルーニングおよび DB クエリエラーの後、PAED プロセスが 24 時間ごとにクラッシュする
CSCws25172	コントローラバージョン 17.15.3 で RO の国コードを使用する 6GHz 無線がオンになっている場合、9166 AP がクラッシュし続ける
CSCws35315	AP から CAPWAP 接続を引き継ぐ補助クライアントインターフェイス
CSCws46519	コントローラで「Ap lldp ネイバーの表示」を実行すると、古い情報が残り続ける
CSCws60984	9166 クラッシュ systemd[1] : Capwapd.service が失敗した
CSCws62182	GUI に誤ったチャンネル帯域幅（ネゴシエート/対応）が表示される
CSCws66137	ローカル認証（中央認証ではなく）が行われている間、クライアントの関連付け時刻が「01/01/1970 00:00:00」と表示される
CSCws70285	/storage/cnssdaemon.log のクリーンアップ
CSCws72425	9136l IOX アプリケーションのアクティブ化失敗
CSCws76582	17.15.3 - 古いクライアントエントリによる、AP での新しい関連付けの禁止
CSCws79118	2.4 GHz in -Z 規制ドメインでの 9124-AXE の送信電力が想定外に低下
CSCws80754	アンカーコントローラのローカル DHCP が、DHCP オファーや ACK の転送を断続的に停止する
CSCws83128	AP 名の変更は、特定のホスト名文字列（AP データベースに存在しない）の競合により「AP 名がすでに存在します」というエラーを示して失敗し、コントローラは AP をデフォルト名に戻す
CSCws93326	26.1.1 ERR ログ: (ERR): MAC: 0000.0000.0000 \u00a0 RA トレースエントリをマルチリンククライアント用に設定、dot11 操作データを取得不能
CSCwt13894	CW9172H WAT エージェントが、先頭または末尾にスペースがある SSID への接続に失敗する
CSCwt20158	ごく少数のクライアントのみを表示する bsnMobileStation - 根本原因は Wifi7
CSCwt21195	新しいロケーションの作成時にデフォルトの 6 GHz RF プロファイルを選択できない
CSCwt40423	ID なしで Cloudm トレースバックを実行
CSCwt41808	AP が AVL 木に参加中に無効な文字列ポインタが原因で wncmgrd プロセスがクラッシュする
CSCwt41939	selinux 拒否後の IOS_PRIV_OPER_DB tbl_ewlc_critical_events テーブルでの TMPFS メモリリーク

未解決の問題

問題に関する追加情報を表示するには、不具合 ID をクリックして、不具合検索ツール（BST）にアクセスしてください。このセクションには、現在のリリースに適用される未解決の問題と、Cisco Catalyst 9800 シリーズワイヤレスコントローラ リリース 17.18.3 より前のリリースに適用される可能性がある未解決の問題をリスト表示しています。これまでのリリースで未解決で、まだ解決されていない問題は、解決されるまで、今後のすべてのリリースに適用されます。

表 4. Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ、リリース 17.18.3 で未解決の問題

不具合 ID	説明
CSCwt91818	APSP のインストール中に C9800 コントローラがクラッシュする
CSCwk79990	9800-L で、Intel Reset Request が原因でカーネルが応答しなくなる
CSCws23072	CW9800 プラットフォームで RRM クラッシュとトレースバックが発生する
CSCws42581	ダイナミック マルチキャスト ルータ ポートとグループの処理中に、L2 マルチキャストでメモリが破損する
CSCwt03837	スタンバイプラットフォームに LocalSoft が原因で予期しないリロードに直面している HA がある
CSCwt13732	WNCD プロセスが予期せず終了し、コントローラがクラッシュする（重要なプロセス wncd が失敗 (rc 0)）
CSCwt19011	9166 17.15.4b AP は SDA モードで、DHCP 後に IPv4 ARP アップストリームや他の IPv4 パケットを転送しない
CSCwt19092	9179 で 17.18.2 を実行すると 1 時間未満で 4 回を超える DFS が発生
CSCwt19490	9800 コントローラ：RADIUS アカウンティングで使用している古いクライアント IP により ISE IP-SGT/SXP が上書きされる
CSCwt22893	17.18.2 でコントローラが WNCD コアで想定外の SISF 再起動
CSCwt26718	wncmgrd から応答がなく eCA アップグレード操作に失敗
CSCwt38788	変数が初期化されていないためモビリティプロセスを予期せず終了、コントローラがリロードされる場合がある
CSCwt50389	AP が EAP_ID_REQ か M2 の確認応答をせず、Ascom Myco2 電話が 9176 AP に接続できない
CSCwt52815	AP 無線での変更後、コントローラがクライアントの関連するチャネル幅の更新に失敗する
CSCwt53635	C9800-40-K9 の wncmgrd プロセスでメモリリーク
CSCwt71615	プロセス「CPPHA-3-FAULT: F0/0: cpp_ha_top_level_server」がクラッシュしてコントローラが再起動する
CSCwt74576	Cisco Catalyst 9136 AP の wcpd プロセスメモリが徐々に増加
CSCwt79299	キープアライブタイマーがヒットしていないのにコントローラがモビリティトンネルをドロップ
CSCwt80081	IP 学習フェーズでユーザーがスタックし、NACK_IFID の理由で削除
CSCwt83133	SSL コードの null ポインタが原因でコントローラに予期しないリロードが発生し、wncd コアが発生
CSCws03721	9120/9115/9105 AP が iOS デバイスから送信されたフレームを確認応答せず、CSCwj91255 のフォロアップ
CSCws94151	SFP「SFP-H25G-CU1M」が C9800M で機能しない - 17.15.03 と Nexus C93180YC-EX
CSCws95359	さまざまな SPF モデルの CW9800M、CW9800H1 で 10G ポートが稼働しない

不具合 ID	説明
CSCwt39820	AP が AP 参加プロファイルから加速計設定を受信しない
CSCwt43333	C9120E デュアルバンドロール XPath は HTTP 204 に成功しても 5 GHz スニファ設定を適用しない
CSCwt44743	CW9166I が Zebra MC9300 RF ガンから ARP クエリをランダムにドロップする
CSCwt53740	コントローラからの一部のポリシー設定プッシュが失敗したため AP が SSID をブロードキャストしない
CSCwt65349	CW9172I AP が ar_wal_mlo_ipc.c アサートとウォッチドッグパニックでクラッシュする
CSCwt72800	CW9176I AP が pc do_undefinstr+0x30/0x50 によるカーネルパニックでクラッシュする
CSCwt75036	C9800-L での 802.1X 認証の失敗？ AP が EAP Request Identity を転送しない (CW9176I、17.15.4.160)
CSCwt77092	AP - KFENCE メモリ破損イベントにより RCU が停止し、HW ウォッチドッグがリセットされる
CSCwt77136	連続した KFENCE IPv6 MLD メモリ破損により RCU が停止し、HW ウォッチドッグがリセットされる
CSCwt79155	17.15.4d での 9105AXW AP カーネルパニッククラッシュ
CSCwt81695	WGB モードでは 91xx AP での DHCP ディスカバーにホスト名 (DHCP オプション 12) を含まず、DDNS レコードが作成されない
CSCwt84944	17.15.3 - 9120 が 5/24 GHz で誤ったノイズ レベルを報告する

既知の問題

Cisco IOS XE 17.18.3 の既知の問題は次のとおりです。

17.18.2、17.18.3、または 26.1.1 から開始した場合に Cisco CW9800L で ISSU 障害

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

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

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

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

互換

互換性マトリックス

次の表に、ソフトウェア互換性情報を示します。詳細については、「[Cisco Wireless Solutions Software Compatibility Matrix](#) [英語]」を参照してください。

表 5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、リリース 17.18.3 の互換性マトリックス

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア	Cisco Identity Services Engine	Cisco AireOS-IRCM の相互運用性	Cisco Catalyst Center	Cisco CMX
IOS XE 17.18.3	3.4 3.3 3.2 3.1 3.0 * すべて最新パッチを適用済み	8.10 最新の MR 8.5 最新の MR	「Cisco Catalyst Center の互換性情報 [英語]」 を参照してください。	11.1.1

ソフトウェア要件

オペレーティング システム：

- Windows 10 以降
- macOS X 10.11 以降

ブラウザ：

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

Firefox バージョン 63.x はサポートされていません。

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。

```
Device# configure terminal
Device(config)# line vty 50
```

ベストプラクティスは、service tcp-keepalives を設定して、デバイスへの TCP 接続を監視することです。

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

アップグレードする前に

アップグレードを始める前に、次の点をよく理解してください。

- **Cisco IOS XE 17.18.3 から 26.1.1 へのアップグレード：**

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

該当する WLAN のタイプは以下のとおりです。

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

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

アップグレード前に暗号の互換性を検証し、サービスの中断を避けてください。

- WAN リンクの背後のリモートサイトに AP がある場合は、イメージのダウンロードを高速化し、信頼性を高めるために、次のドキュメントをお読みください。

https://www.cisco.com/c/ja_ip/support/docs/wireless/catalyst-9800-series-wireless-controllers/223125-understand-access-point-image-upgrades.html。

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

回避策：

- CLI コマンドを使用してアップグレードします。または、
- 17.9.6、17.12.3、またはそれ以降にアップグレードしてから、17.18.2 以降にアップグレードします。
- イメージの場合：17.9.6 以前、17.12.4 以前、または 17.15.1 以前から 17.18.2 にアップグレードする場合、Cisco Catalyst Wi-Fi 6 AP は、一時パーティションの空き容量不足によりイメージのアップグレードに失敗する可能性があります。

回避策：

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

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

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

- 次の Wave 1 AP は 17.18.2 以降ではサポートされないため、コントローラに参加しません。アップグレードする前に、現在のモデルを検証することを推奨します。
 - Cisco Aironet 1570 シリーズ アクセスポイント
 - Cisco Aironet 1700 シリーズ アクセスポイント
 - Cisco Aironet 2700 シリーズ アクセス ポイント
 - Cisco Aironet 3700 シリーズ アクセスポイント
- Cisco IOS XE Dublin 17.10.x 以降、キー交換および MAC アルゴリズム (diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, hmac-sha2-512 など) はデフォルトでサポートされておらず、これらのアルゴリズムのみをサポートする一部の SSH クライアントに影響を与える可能性があります。必要に応じて、手動でこれらを追加できます。これらのアルゴリズムを手動で追加する方法については、https://www.cisco.com/c/ja_jp/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html で「コモン クライテリア認定用の SSH アルゴリズム」を参照してください。
- archive download-sw コマンドの実行後に AP がバックアップイメージを検出できない場合は、次の手順を実行します。
 - archive download-sw コマンドの no-reload オプションを使用してイメージをアップロードします。

```
Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
```
 - **capwap ap restart** コマンドを使用して CAPWAP プロセスを再起動します。これにより、再起動後に AP が正しいバックアップイメージを使用できるようになります (リロードは必要ありません)。

```
Device# capwap ap restart
```

AP は、参加プロセス中にコントローラへの接続を失います。AP が新しいコントローラに参加すると、バックアップパーティションに新しいイメージが表示されます。したがって、AP はコントローラから新しいイメージをダウンロードしません。
- クライアント認証用の RADIUS パケットのフラグメンテーションを引き起こす可能性のある、GO (OOB) インターフェイスでの 1500 未満の MTU の使用はサポートしていません。
- Cisco IOS XE 17.3.x 以降のリリースにアップグレードする場合、**ip http active-session-modules none** コマンドが有効になっていると、HTTPS を使用してコントローラの GUI にアクセスできません。HTTPS を使用して GUI にアクセスするには、以下に指定された順序で次のコマンドを実行します。

```
ip http session-module-list pkilist OPENRESTY_PKI
ip http active-session-modules pkilist
```
- Cisco Aironet 1815T OfficeExtend アクセスポイントは、コントローラに接続するとローカルモードになります。ただし、スタンドアロン AP として機能する場合は、FlexConnect モードに変換されます。
- Cisco Catalyst 9800-L ワイヤレスコントローラは、ブート時にコンソールポートで受信した BREAK 信号に応答できず、ユーザーが ROMMON にアクセスできなくなる場合があります。この問題は、デフォルトの config-register 設定が 0x2102 の、2019 年 11 月までに製造されたコントローラで発生します。この問題は、config-register を 0x2002 に設定すると回避できます。

この問題は、Cisco Catalyst 9800-L ワイヤレスコントローラの 16.12(3r)ROMMON で修正されています。

ROMMON のアップグレード方法については、『[Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers](#)』ドキュメントの「Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers」のセクションを参照してください。

- デフォルトでは、コントローラは TFTP ブロック サイズの最小許容値である 512 を使用します。このデフォルト設定は、レガシー TFTP サーバーとの相互運用性を確保するために使用されます。必要に応じてグローバル コンフィギュレーション モードで **ip tftp blocksize** コマンドを使用して、ブロックサイズの値を 8192 に変更し、転送プロセスを高速化することができます。
- 再起動またはシステムクラッシュの後に次のエラーメッセージが表示された場合は、トラストポイント証明書、ERR_SSL_VERSION_OR_CIPHER_MISMATCH を再生成することを推奨します。

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

```
device# configure terminal
device(config)# no crypto pki trustpoint trustpoint_name
device(config)# no ip http server
device(config)# no ip http secure-server
device(config)# ip http server
device(config)# ip http secure-server
device(config)# ip http authentication local/aaa
```

- OVA ファイルを VMware ESXi 6.5 に直接展開しないでください。OVF ツールを使用して OVA ファイルを展開することをお勧めします。
- Netconf-YANG を無効または有効にする前に、Cisco Prime Infrastructure からコントローラを必ず削除してください。そうしないと、システムが予期せずリロードする可能性があります。
- Cisco IOS XE Bengaluru 17.4.1 以降、テレメトリソリューションでは、テレメトリデータの IP アドレスではなく、受信者アドレスの名前が提供されます。これは追加のオプションです。コントローラのダウングレードおよびその後のアップグレード中に問題が発生する可能性があります。アップグレードバージョンでは、新しく指定された受信者が使用されますが、これらはダウングレードでは認識されません。新しい設定は拒否され、後続のアップグレードで失敗します。Cisco Catalyst Center からアップグレードまたはダウングレードを実行すると、設定の損失を回避できます。
- Cisco Centralized Key Management (CCKM) 機能は、Cisco IOS XE 17.10.x で廃止されましたが、現在もサポートされています。ただし、CCKM の今後のリリースでサポート対象外となります。そのため、802.1X 認証を使用した Fast Transition (FT) に移行し、サポートされているキー キャッシュ メカニズムで構成を検証することを推奨します。
- パブリック IP アドレスを 16.12.x から 17.x に移行するには、service internal コマンドを必ず設定してください。service internal コマンドを設定しなければ、IP アドレスは引き継がれません。
- 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をより早い時刻を反映するように変更するたびに、コントローラのリロードを実行することを推奨します。

- DTLS バージョン (DTLSv1.0) は、最新のセキュリティポリシーに基づいて Cisco Aironet 1800 で廃止されています。そのため、Cisco Aironet 1800 AP の新しいアウトオブボックス展開はコントローラに参加できず、次のエラーメッセージが表示されます。

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join,
AP <AP-name>,
mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

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

```
config terminal
ap dtls-version dtls_1_0
end
```

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

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

Cisco IOS XE 17.18.3 へのアップグレードパス

注：Cisco Catalyst 9136、9164、9166 AP の場合、17.9.1 から 17.15.x または 17.18.x への直接アップグレードは、容量不足により失敗します。アップグレードするには、17.15.x または 17.18.x に進む前に、まず 17.9.6 か 17.9.7 に更新する必要があります。

表 6. Cisco IOS XE Dublin 17.18.3 へのアップグレードパス

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレードパス
16.10.x	— 注： Cisco Catalyst 9130 と 9124 AP は、16.10.x、16.11.x リリースではサポートしていません。	最初に 16.12.5 または 17.3.x にアップグレードしてから、17.18.3 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、17.18.3 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、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 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、17.18.3 にアップグレードします。
17.1.x	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または	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、17.18.3 にアップグレードします。

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレードパス
	17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	
17.2.x	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 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、17.18.3 にアップグレードします。
17.3.1 ~ 17.3.4	最初に 17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.3.4c 以降	17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 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、17.18.3 にアップグレードします。	17.18.3 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、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.6.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.7.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.8.x	17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.9.1 ~ 17.9.5	17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。 注：Cisco Catalyst 9136、9164、9166 AP の場合、17.9.1 から 17.15.x または 17.18.x への直接アップグレードは、容量不足により失敗します。アップグレードするには、17.15.x または 17.18.x に進む前に、まず 17.9.6 か 17.9.7 に更新する必要があります。	17.18.3 に直接アップグレードします。
17.9.6 以降	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
17.10.x	17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.11.x	17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。
17.12.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
17.13.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。

現在のソフトウェア	9130、9124 または 916x を使用した展開のアップグレードパス	9130 および 9124 を使用しない展開のアップグレードパス
17.14.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
17.15.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
17.16.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
17.17.x	17.18.3 に直接アップグレードします。	17.18.3 に直接アップグレードします。
8.9.x または 8.10.171.0 より前の 8.10.x バージョン	最初に 8.10.171.0 以降、17.3.5 以降または 17.6.x 以降にアップグレードし、次に 17.9.6 以降または 17.12.x 以降にアップグレードしてから、17.18.3 にアップグレードします。	17.18.3 に直接アップグレードします。

コントローラ ソフトウェアのアップグレード

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

ソフトウェアバージョンの確認

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

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

注： **show version** の出力にはコントローラで実行されているソフトウェアイメージが常に表示されますが、この出力の最後に示されているモデル名は、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 17.18.3

イメージ名 (9800-80、9800-40、および 9800-L)：

- C9800-80-universalk9_wlc.17.18.03.SPA.bin
- C9800-40-universalk9_wlc.17.18.03.SPA.bin
- C9800-L-universalk9_wlc.17.18.03.SPA.bin

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

- CW9800H-wlc-universalk9.17.18.03.SPA.bin
- CW9800M-wlc-universalk9.17.18.03.SPA.bin
- CW9800L-wlc-universalk9.17.18.03.SPA.bin

イメージ名 (9800-CL) :

- クラウド : C9800-CL-universalk9.17.18.03.SPA.bin
- **Hyper-V/ESXi/KVM** : C9800-CL-universalk9.17.18.03.iso, C9800-CL-universalk9.17.18.03.ova
- **KVM** : C9800-CL-universalk9.17.18.03.qcow2
- **NFVIS** : C9800-CL-universalk9.17.18.03.tar.gz

ソフトウェア インストール コマンド

指定したファイルをインストールしてアクティブ化し、リロード後も維持されるように変更をコミットするには、次のコマンドを実行します。

```
device# install add file filename [activate |commit]
```

インストールファイルを個別にインストール、アクティブ化、コミット、終了、または削除するには、次のコマンドを実行します。

```
device# install ?
```

注 : インストールには GUI を使用することを推奨します。

コマンド	説明
add file tftp: filename	インストール ファイル パッケージをリモート ロケーションからデバイスにコピーし、プラットフォームとイメージのバージョンの互換性チェックを実行します。
activateauto-abort-timer	ファイルをアクティブ化し、デバイスをリロードします。auto-abort-timer キーワードは、イメージのアクティブ化を自動的にロールバックします。
Commit	リロード後も変更が持続されるようにします。
rollback to committed	最後にコミットしたバージョンに更新をロールバックします。
Abort	ファイルのアクティブ化を中止し、現在のインストール手順の開始前に実行していたバージョンにロールバックします。
Remove	未使用および非アクティブ状態のソフトウェア インストール ファイルを削除します。

ライセンス

Cisco Wireless ライセンス

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

Cisco Wireless ライセンスは、次の階層で構成しています。

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

詳細については、「[Cisco Wireless ライセンスの構成](#)」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 7. 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 17.18.3
シスコ ワイヤレス コントローラ	「 サポート対象ハードウェア 」を参照してください。
アクセスポイント	「 サポート対象の AP 」を参照してください。
無線機	802.11ac 802.11ax 802.11a 802.11g 802.11n 802.11be (Wi-Fi 7)
セキュリティ	オープン、PSK (WPA2-AES) 、802.1X (WPA2-AES) (EAP-FAST、EAP-TLS) 、WPA3 AKM
RADIUS	「 互換性マトリックス 」を参照してください。
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 8. 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)	最新
Apple MacBook Air 11 inch	最新
Apple MacBook Air 13 inch	最新
MacBook Pro Retina	最新
MacBook Pro Retina 13 inch early 2015	最新
MacBook Pro OS X	最新

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
MacBook Air	最新
MacBook Air 11 inch	最新
MacBook M1 チップ	最新
MacBook M1 チップ	最新
MacBook Pro M2 チップ	最新
MacBook Pro M2 チップ	最新
MacBook Pro M3 チップ	macOS Tahoe 26.4.1
MacBook/Mac-Mini Pro M4 チップ	macOS Tahoe 26.4.1
MacBook/Mac-Mini Pro M4 Pro チップ	macOS Tahoe 26.4.1
MacBook Air M5 チップ	macOS Tahoe 26.4.1
MacBook Pro M5 チップ	macOS Tahoe 26.4.1
MacBook Neo	macOS Tahoe 26.4.1
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP Chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	最新
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	最新
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	最新
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	最新
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	最新
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	最新
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	最新
Dell Latitude 5491 (Intel AX200)	最新
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	最新
Dell Inspiron 13-5368 Signature Edition	最新

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
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	最新
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	最新
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	最新
注 : Intel 無線カードを使用しているクライアントの場合、アドバタイズされた SSID が表示されない場合は、最新の Intel ワイヤレスドライバに更新することをお勧めします。	
タブレット	
Apple iPad Pro (12.9 インチ) 第 6 世代	iOS 16.4
Apple iPad Pro (11 インチ) 第 4 世代	iOS 16.4
Apple iPad 2021	iOS 15.0
Apple iPad 第 7 世代 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 インチ (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 インチ (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi チップセット 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi チップ)	Windows
携帯電話	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5

クライアントのタイプおよび名前	ドライバまたはソフトウェアのバージョン
Apple iPhone 8	iOS 13.5
Apple iPhone 8 plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 16.0
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Mini Pro	iOS 15.1
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
Apple iPhone 14	iOS 26.4.1
Apple iPhone 14 Pro	iOS 26.4.1
Apple iPhone 15	iOS 26.4.1
Apple iPhone 15 Pro	iOS 26.4.1
Apple iPhone 16	iOS 26.4.1
Apple iPhone 16e	iOS 26.4.1
Apple iPhone 16 Pro	iOS 26.4.1
Apple iPhone 17	iOS 26.4.1
Apple iPhone 17 Pro	iOS 26.4.1
Apple iPhone 17e	iOS 26.4.1
Apple iPhone Air	iOS 26.4.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP 電話 8821	11.0.6 SR4
Cisco 840/s	最新

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
Cisco 860	最新
Cisco 9821	最新
Cisco IP 電話 7800 シリーズ	最新
Cisco IP 電話 8800 シリーズ	最新
Cisco IP 電話 9800 シリーズ	最新
Drager Delta	VG9.0.2
Drager M300.3	VG3.0
Drager M300.4	VG3.0
Drager M540	VG4.2
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
Google Pixel 8	Android 15
Google Pixel 9	Android 15
Google Pixel 10	Android 15
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

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 S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Galaxy S23	Android 15.0
Samsung Galaxy S23 Ultra	Android 15.0
Samsung Galaxy S24	Android 15.0
Samsung Galaxy S24 Ultra	Android 15.0
Samsung Galaxy S25	Android 15.0
Samsung Galaxy S25 Ultra	Android 15.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony 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
Spectralink Versity Phones 9540 シリーズ	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4

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 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 TC58	Android 11.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	Android 10.0
Zebra TC8000	Android 4.4.3
プリンタ	
Zebra QLn320 モバイルプリンタ	LINK OS 5.2
Zebra ZT230 産業用プリンタ	LINK OS 6.4
Zebra ZQ310 モバイルプリンタ	LINK OS 6.4
Zebra ZD410 産業用プリンタ	LINK OS 6.4
Zebra ZT410 デスクトッププリンタ	LINK OS 6.2
Zebra ZQ610 産業用プリンタ	LINK OS 6.4
Zebra ZQ620 モバイルプリンタ	LINK OS 6.4
ワイヤレスモジュール	
Intel AX 411	最新
Intel AX 211	最新
Intel AX 210	最新
Intel AX 200	最新

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
Intel 11AC	最新
Intel AC 9260	最新
Intel Dual Band Wireless AC 8260	最新
Samsung S21 Ultra	最新
QCA WCN6855	最新
PhoenixContact FL WLAN 2010	最新

サポートされるハードウェア

サポートされている仮想プラットフォームおよびハードウェア プラットフォーム

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

表 9. サポートされている仮想プラットフォームおよびハードウェア プラットフォーム

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレス コントローラ	最大 100 GE のモジュールアップリンクおよびシームレスなソフトウェアアップデートを備えたモジュール型ワイヤレスコントローラ。 コントローラは 2 ラックユニットスペースを占有し、複数のモジュールアップリンクをサポートします。
Cisco Catalyst 9800-40 ワイヤレス コントローラ	シームレスなソフトウェア アップデートを備えた、中規模および大規模の企業向けの固定ワイヤレスコントローラ。 コントローラは 1 ラックユニットスペースを占有し、4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、パフォーマンスと機能を大幅に向上させる、最初のローエンド コントローラです。
クラウド向け Cisco 9800 シリーズ ワイヤレス コントローラ	Catalyst 9800 ワイヤレスコントローラの仮想フォームファクタは、エンタープライズ ネットワーク コンピューティング システム (ENCS) ハイパーバイザ上の VMware ESXi、カーネルベース仮想マシン (KVM)、Microsoft Hyper-V、Cisco Enterprise NFV インフラストラクチャ ソフトウェア (NFVIS) をサポートするプライベートクラウドに展開することも、Amazon Web Services (AWS)、Google Cloud Platform (GCP) マーケットプレイス、Microsoft Azure 内のパブリッククラウドに Infrastructure as a Service (IaaS) として展開することもできます。
Catalyst 9000 シリーズ スイッチに組み込まれた Embedded Wireless Controller	Cisco Catalyst 9000 スイッチ用 Catalyst 9800 ワイヤレス コントローラ ソフトウェアは、有線およびワイヤレス インフラストラクチャを一貫性のあるポリシーおよび管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションであるソフトウェア定義型アクセス (SDA) のみをサポートします。

プラットフォーム	説明
Cisco CW9800 シリーズ ワイヤレス コントローラ (CW9800M、CW9800H1、CW9800H2、および CW9800L)	CW9800M コントローラは、次世代の Cisco CW9800 シリーズ ワイヤレス LAN コントローラであり、前世代のモデルと比較して、パフォーマンスが 53% 向上し、消費電力が 18% 削減されます。
	さらに、CW9800M コントローラは 3,000 個の AP と 32,000 個のクライアントをサポートし、ビジネスクリティカルなネットワークのパフォーマンスと拡張性を向上させます。スペースを節約し、データセンターの柔軟性を高めるように設計されたシングル RU でありながら、通常のパケットと暗号化されたパケットの両方に対して最大 40 Gbps の転送スループットを実現します。
	CW9800H1 および CW9800H2 コントローラは、次世代の Cisco CW9800 ワイヤレス LAN コントローラであり、以前の製品と比較して、パフォーマンスが最大 36% 向上し、消費電力が最大 40% 削減されます。
	さらに、CW9800H1 および CW9800H2 モデルは、省スペースのシングル RU 設計で構築されており、最大 6,000 の AP と 64,000 のクライアントをサポートし、最大スループットは 100 Gbps です。また、4 X 25 Gbps (CW9800H1) または 2 X 40 Gbps (CW9800H2) 構成のアップリンクを選択して、次世代ワイヤレス要件における高スループットの要求に対応できます。
	CW9800L コントローラは、パフォーマンスと機能を大幅に向上させる、次世代のローエンドコントローラです。CW9800L は、最大 10 Gbps のスループット、500 個の AP、および 10,000 個のクライアントをサポートし、ベースとなる C9800-L に比べて 2 倍のキャパシティとパフォーマンスの向上をもたらします。

サポートされているホスト環境：パブリッククラウドとプライベートクラウド

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

表 10. パブリッククラウドとプライベートクラウドでサポートされているホスト環境

ホスト環境	ソフトウェアのバージョン
VMware ESXi	- VMware ESXi vSphere 6.5、6.7、7.0 および 8.0 - VMware ESXi vCenter 6.5、6.7、7.0 および 8.0
KVM	- Red Hat Enterprise Linux 9.2 または最新バージョンをベースとした Linux KVM - Ubuntu 16.04.5 LTS、Ubuntu 18.04.5 LTS、Ubuntu 20.04.5 LTS
AWS	AWS EC2 プラットフォーム
NFVIS	ENCS 3.8.1 および 3.9.1
GCP	GCP マーケットプレイス
Microsoft Hyper-V	Windows Server 2019、Windows Server 2025、Hyper-V マネージャ (バージョン 10.0.x)
Microsoft Azure	Microsoft Azure

サポートされる PID およびポート

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

ベース PID は、コントローラのモデル番号です。

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

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

表 11. サポートされる PID およびポート

コントローラモデル	説明
C9800-CL-K9	クラウド向けインフラストラクチャとしての Cisco Catalyst ワイヤレスコントローラ。
C9800-80-K9	1/10 ギガビットイーサネット SFP または SFP+ ポート（8 個）、電源スロット（2 個）
C9800-40-K9	1/10 ギガビットイーサネット SFP または SFP+ ポート（4 個）、電源スロット（2 個）。
C9800-L-C-K9	2.5/1 ギガビットポート x 4 10/5/2.5/1 ギガビット ポート x 2
C9800-L-F-K9	2.5/1 ギガビットポート x 4 10/1 ギガビット ポート x 2
CW9800H1	1 GE/10 GE SFP ポート X 8 25 GE SFP インターフェイス X 4
CW9800H2	1 GE/10 GE SFP ポート X 8 40 GE QSFP インターフェイス X 2
CW9800M	- 内蔵 1 GE/10 GE SFP ポート X 4 - 組み込み 25 GE SFP ポート X 2
CW9800L	10G/1G SFP ポート（データポート）X 2 1G 銅線（RP および SP ポート）X 2

サポートされる SFP

次の表に、サポートされる SFP モデルを示します。

表 12. サポートされる SFP モデル

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
COLORCHIP-C040-Q020-CWDM4-03B	サポート対象	—	—	—	—	—	—
DWDM-SFP10G-30.33	サポート対象	サポート対象	—	—	—	—	—
DWDM-SFP10G-61.41	サポート対象	サポート対象	—	—	—	—	—

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
FINISAR-LR - FTLX1471D3BCL (FINISAR SFP はシスコ固有ではなく、DOM などの一部の機能が正しく動作しない場合があります。)	サポート対象	サポート対象	サポート対象	—	—	—	—
FINISAR-SR - FTLX8574D3BCL	サポート対象	サポート対象	サポート対象	—	—	—	—
GLC-BX-D	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
GLC-BX-U	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
GLC-EX-SMD	サポート対象	サポート対象	—	サポート対象	サポート対象	サポート対象	—
GLC-LH-SMD	サポート対象	サポート対象	—	サポート対象	サポート対象	サポート対象	サポート対象
GLC-SX-MMD	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
GLC-T	サポート対象	—	—	—	—	—	—
GLC-TE	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
GLC-ZX-SMD	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
QSFP-100G-LR4-S	サポート対象	—	—	—	—	—	—
QSFP-100G-SR4-S	サポート対象	—	—	—	—	—	—
QSFP-40G-BD-RX	サポート対象	—	—	サポート対象	— サポート対象	— サポート対象	—
QSFP-40G-ER4	サポート対象	—	—	—	サポート対象	—	—
QSFP-40G-LR4	サポート対象	—	—	—	サポート対象	—	—
QSFP-40G-LR4-S	サポート対象	—	—	—	サポート対象	—	—
QSFP-40G-LR4-S-RF			—	サポート対象	サポート対象	サポート対象	—
QSFP-40G-CSR4	—	—	—	—	サポート対象	—	—
QSFP-40G-SR4	サポート対象	—	—	—	サポート対象	—	—
QSFP-40G-SR4-S	サポート対象	—	—	—	サポート対象	—	—
QSFP-40G-SR-BD	—	—	—	サポート対象	サポート対象	サポート対象	—
QSFP-40GE-LR4	サポート対象	—	—	—	—	—	—
QSFP-H40G-ACU7M	—	—	—	サポート対象	サポート対象	サポート対象	—

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

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-10G-AOC7M	サポート対象	サポート対象	—	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-BXD-I	—	—	—	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-BXU-I	—	—	—	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-CSR-S	—	—	—	サポート対象	サポート対象	サポート対象	—
SFP-10G-ER	サポート対象	サポート対象	—	サポート対象	サポート対象	サポート対象	—
SFP-10G-LR	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-LR-I			—	サポート対象	サポート対象	サポート対象	—
SFP-10G-LR-S	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-LR-X	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
SFP-10G-LRM	サポート対象	サポート対象	サポート対象	—	—	—	—
SFP-10G-SR	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-S	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-I	—	—	—	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-SR-X	サポート対象	サポート対象	サポート対象	—	—	—	—
SFP-10G-ZR	—	—	—	サポート対象	サポート対象	サポート対象	—
SFP-10G-ZR-I	—	—	—	サポート対象	サポート対象	サポート対象	サポート対象
SFP-10G-T-X	—	—	—	サポート対象	サポート対象	サポート対象	—
SFP-25G-CSR-S	—	—	—	サポート対象	サポート対象	サポート対象	—
SFP-25G-SR-S	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-ER-I	—	—	—	サポート対象	—	サポート対象	—
SFP-10/25G-LR-I	—	—	—	サポート対象	—	サポート対象	—
SFP-10/25G-LR-S	—	—	—	サポート対象	—	サポート対象	—
SFP-10/25G-CSR-S	—	—	—	サポート対象	—	サポート対象	—
SFP-10/25G-BXD-I	—	—	—	サポート対象	—	サポート対象	サポート対象
SFP-10/25G-BXU-I	—	—	—	サポート対象	—	サポート対象	サポート対象
SFP-H25G-CU1M	—	—	—	サポート対象	—	サポート対象	—
SFP-H25G-CU5M	—	—	—	サポート対象	—	サポート対象	—

SFP 名	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-25G-AOC1M	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-AOC2M	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-AOC3M	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-AOC5M	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-AOC7M	—	—	—	サポート対象	—	サポート対象	—
SFP-25G-AOC10M	—	—	—	サポート対象	—	サポート対象	—
SFP-H10GB-ACU10M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-ACU7M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU1.5M	サポート対象	サポート対象	サポート対象	—	—	—	—
SFP-H10GB-CU1M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
SFP-H10GB-CU2.5M	サポート対象	サポート対象	サポート対象	—	—	—	サポート対象
SFP-H10GB-CU2-5M	—	—	—	サポート対象	サポート対象	サポート対象	—
SFP-H10GB-CU2M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	—
SFP-H10GB-CU3M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU5M	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
SFP-H10GB-CU1-5M	サポート対象	サポート対象	—	サポート対象	サポート対象	サポート対象	—
Finisar-LR (FTLX1471D3BCL)	—	—	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Finisar-SR (FTLX8574D3BC)	—	—	—	サポート対象	サポート対象	サポート対象	サポート対象

光モジュール

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

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

ネットワークプロトコルとポートマトリックス

表 13. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ - ネットワークプロトコルとポートマトリックス

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	22	任意	SSH
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	23	任意	Telnet
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	80	任意	HTTP
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	任意	HTTPS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	161	任意	SNMP エージェント
任意	任意	UDP	5353	5353	mDNS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	69	69	TFTP
任意	DNS Server	UDP	53	任意	DNS
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	830	任意	NetConf
任意	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	443	任意	REST API
任意	WLC プロトコル	UDP	1700	任意	CoA パケットを受信
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5246	任意	CAPWAP 制御
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5247	任意	CAPWAP データ
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	5248	任意	CAPWAP MCAST
AP	Cisco Catalyst Center	TCP	32626	任意	インテリジェントキャプチャと RF テレメトリ

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
AP	AP	UDP	16670	任意	クライアントポリシー (AP-AP)
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	16666	16666	モビリティ制御
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	SNMP	UDP	162	任意	SNAMP トラップ
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	RADIUS	UDP	1812/1645	任意	RADIUS 認証
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	RADIUS	UDP	1813/1646	任意	RADIUS ACCT
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TACACS+	TCP	49	任意	TACACS+
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	UDP	16667	16667	モビリティ
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	NTP サーバー	UDP	123	任意	NTP
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Syslog サーバー	UDP	514	任意	SYSLOG
AP	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	HTTPS	8443	任意	アウトオブバンド AP イメージのダウンロード Cisco CleanAir スペクトル キャプチャ
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	NetFlow サーバー	UDP	9996	任意	NetFlow
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco Connected Mobile Experiences (CMX)	UDP	16113	任意	NMSP

送信元	接続先	プロトコル	宛先ポート	ソース ポート	説明
Cisco Catalyst Center	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	32222	任意	デバイス検出
Cisco Catalyst Center	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	TCP	25103	任意	テレメトリ サブスクリプション

サポート対象の AP

このリリースでは、次のシスコ AP がサポートされます。

表 14. サポート対象の AP

AP タイプ	AP 名
屋内用アクセスポイント	• Cisco Catalyst 9105AX (I/W) アクセスポイント • Cisco Catalyst 9115AX (I/E) アクセスポイント • Cisco Catalyst 9120AX (I/E/P) アクセスポイント • Cisco Catalyst 9130AX (I/E) アクセスポイント • Cisco Catalyst 9136AX アクセス ポイント • Cisco Catalyst 9162 (I) シリーズ アクセスポイント • Cisco Catalyst 9164 (I) シリーズ アクセスポイント • Cisco Catalyst 9166 (I/D1) シリーズ アクセスポイント • Cisco Wireless 9171 (I) シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9172 (I/H) シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9174 (I/E) シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9176 (I/D1) シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9178 (I) シリーズ Wi-Fi 7 アクセスポイント • Cisco Wireless 9179 (F) シリーズ Wi-Fi 7 アクセスポイント • Cisco Aironet 1815 (I/W/M/T) 、 1830 (I) 、 1840 (I) 、 および 1852 (I/E) アクセスポイント • Cisco Aironet 1800i アクセスポイント • Cisco Aironet 2800 (I/E) シリーズ アクセスポイント • Cisco Aironet 3800 (I/E/P) シリーズ アクセスポイント • Cisco Aironet 4800 (I) シリーズ アクセスポイント
屋外用アクセスポイント	• Cisco Aironet 1540 (I/D) シリーズ アクセスポイント • Cisco Aironet 1560 (I/D/E) シリーズ アクセスポイント • Cisco Catalyst Industrial Wireless 6300 Heavy Duty シリーズ アクセスポイント • Cisco 6300 シリーズ組み込みサービスアクセスポイント • Cisco Catalyst 9124AX (I/D/E) アクセスポイント • Cisco Catalyst 9163 (E) シリーズ アクセスポイント • Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty アクセスポイント • Cisco Catalyst Industrial Wireless 9165E 高耐久性アクセスポイント • Cisco Catalyst Industrial Wireless 9165D Heavy Duty アクセスポイント
統合アクセスポイント	Cisco 1100 ISR の統合アクセスポイント (ISR-AP1100AC-x、ISR-AP1101AC-x、および ISR-AP1101AX-x)

AP タイプ	AP 名
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	Cisco Wi-Fi インターフェイスモジュール (WIM) - WP-WIFI6-x

サポートされている AP チャネルと最大電力設定

Cisco AP でサポートされているアクセスポイントチャネルと最大電力設定は、アクセスポイントが販売されているすべての国のチャネル、最大電力レベル、およびアンテナゲインの規制仕様に準拠しています。Cisco IOS XE ソフトウェアリリースでサポートされているアクセスポイントの伝送値の詳細については、

https://www.cisco.com/c/ja_ip/support/wireless/catalyst-9100ax-access-points/products-technical-reference-list.html にある『Detailed Channels and Maximum Power Settings [英語]』ドキュメントを参照してください。

特定の Cisco AP モジュールをサポートしている Cisco Wireless ソフトウェアリリースの詳細については、「[Cisco Access Points Supported in Cisco Wireless Controller Platform Software Releases \[英語\]](#)」を参照してください。

関連情報

シスコ ワイヤレス コントローラ :

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

[Cisco Wireless Solutions Software Compatibility Matrix](#)

[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)

[Cisco Catalyst 9800 Series Wireless Controller Command Reference](#)

[Cisco Catalyst 9800 Series Configuration Best Practices](#)

[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。

[ハードウェア設置ガイド](#)

[All Cisco Wireless Controller software-related documentation](#)

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

[データシートリスト](#)

ワイヤレス製品の比較

[Compare specifications of Cisco wireless APs and controllers](#)

[Wireless LAN Compliance Lookup](#)

[Cisco AireOS 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 Spaces :

[Cisco Spaces ドキュメント](#)

Cisco Catalyst Center :

[Cisco Catalyst Center のマニュアル](#)

製品分析

[Cisco Enterprise Networking 製品分析に関する FAQ \(よくある質問\)](#) [英語]

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 DevNet](#) [英語] 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](#) [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

シスコバグ検索ツール

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

マニュアルに関するフィードバック

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

法的情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、シスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

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

© 2026 Cisco Systems, Inc. All rights reserved.

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。

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。