

# Cisco Wireless リリース 8.10.185.0 向け Cisco Wireless Controller および Lightweight アクセスポイント リリースノート

初版 : 2022 年 9 月 19 日

最終更新 : 2023 年 3 月 30 日

## リリースノートについて

このリリースノートでは、このリリースの新機能と変更点、このリリースへのアップグレード手順、およびこのリリースの未解決の不具合と解決済みの不具合について説明します。このマニュアル内では、特に記載されていない限り、Cisco Wireless Controller をコントローラと呼び、Cisco Lightweight アクセスポイントをアクセスポイントまたは AP と呼びます。

## サポート対象の Cisco Wireless Controller プラットフォーム

このリリースでは、次のコントローラ プラットフォームがサポートされます。

- Cisco 3504 ワイヤレス コントローラ
- Cisco 5520 ワイヤレス コントローラ
- Cisco 8540 ワイヤレス コントローラ
- 次のプラットフォームの Cisco Virtual Wireless Controller (vWLC) :
  - VMware vSphere Hypervisor (ESXi) バージョン 5.x および 6.x
  - Microsoft Server 2012 以降のバージョンの Hyper-V (リリース 8.4 で導入されたサポート)
  - カーネルベース仮想マシン (KVM) (リリース 8.1 で導入されたサポート)。KVM を導入した後、リリース 8.1 より前のシスコワイヤレスリリースにダウングレードしないことをお勧めします)。
- Cisco 3504 ワイヤレスコントローラ、Cisco 5520 ワイヤレスコントローラ、および Cisco 8540 ワイヤレスコントローラのハイアベイラビリティを実現するシスコ ワイヤレス コントローラ
- Cisco Mobility Express

## サポート対象のシスコ アクセス ポイント プラットフォーム

このリリースでは、次のシスコ AP プラットフォームがサポートされます。

- Cisco Catalyst 9105 アクセス ポイント
  - C9105AXI : VID 04 以前
  - C9105AXW : VID 04 以前
  
- Cisco Catalyst 9130 アクセス ポイント
  - C9130AXE : VID 03 以前
  - C9130AXI : VID 03 以前
  
- Cisco Catalyst 9120 アクセス ポイント
  - C9120AXI : VID 07 以前
  - C9120AXE : VID 07 以前
  - C9120AXP : すべての VID
  
- Cisco Catalyst 9117 アクセス ポイント
- Cisco Catalyst 9115 アクセス ポイント
- Cisco Aironet 700 シリーズ アクセス ポイント
- Cisco Aironet 700W シリーズ アクセス ポイント
- Cisco AP803 統合アクセス ポイント
- Cisco 1100、1101、および 1109 サービス統合型ルータでの統合アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 1800 シリーズ アクセス ポイント
- Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント
- Cisco Aironet 1810W シリーズ アクセス ポイント
- Cisco Aironet 1815 シリーズ アクセス ポイント
- Cisco Aironet 1830 シリーズ アクセス ポイント
- Cisco Aironet 1840 シリーズ アクセス ポイント
- Cisco Aironet 1850 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 2800 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 Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 シリーズ 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 Aironet 1570 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 IW6300 Heavy Duty シリーズ アクセス ポイント
- Cisco 6300 シリーズ エンベデッド サービス アクセス ポイント

Cisco AP803 は、Cisco 800 シリーズ サービス統合型ルータ (ISR) 上の統合アクセス ポイント モジュールです。AP803 Cisco ISR の最小在庫管理単位 (Sku) の詳細については、次を参照してください。

<http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html>。

Cisco 1100 ISR の統合アクセスポイントの詳細については、製品データシートを参照してください。

<https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-ist/datasheet-c78-739512.html>。

特定のシスコアクセスポイントモジュールをサポートしているシスコワイヤレス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](#)」セクションを参照してください。

## リリースの新機能 8.10.185.0

今回のリリースでは、新機能は導入されていません。このリリースにおけるアップデートの詳細については、本ドキュメントの「[不具合](#)」のセクションを参照してください。



- (注) シスコワイヤレスリリース 8.10 の公開ドキュメントの全リストについては、以下のサイトでドキュメントロードマップを参照してください。<https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-810.html>

## リリース 8.10.185.0 での変更点

このセクションでは、このリリースで導入された変更および拡張機能について説明します。

### Cisco アクセスポイントの安全なデータワイプ

データワイプ機能は、NIST 800-88 データワイプ基準を満たすように強化されています。次の方法を使用して、AP からのデータをサニタイズできます。

- コントローラ
  - GUI（初期設定へのリセット）：**[Wireless] > [Access Points] > [All APs]**。AP 名をクリックし、**[Reset AP Now]** をクリックします。
  - CLI（初期設定へのリセット）：**clear ap config ap-name**

詳細については、AireOS の『[Configuration Guide](#)』を参照してください。

- AP モードボタンの使用
 

詳細については、それぞれの Cisco アクセスポイントの『[Hardware Installation Guide](#)』または『[Deployment Guide](#)』を参照してください。
- AP コンソールクリアコマンド
  - Cisco Wave 1（IOS） AP：**clear capwap ap all-config**
  - Cisco Wave 2 AP：**clear capwap ap all-config**

## ソフトウェア リリースのタイプと推奨事項

表 1: リリース タイプ

リリース タイプ	説明	利点
メンテナンス 展開 (MD)	<p>バグ修正のサポートと継続的なソフトウェア メンテナンスを提供するソフトウェア リリース。これらのリリースは、メンテナンス 展開 (MD) として分類されます。</p> <p>これらのリリースは、継続的なソフトウェア メンテナンスを含む長寿命リリースです。</p>	<p>定期的なメンテナンス リリース (MR) による安定性と長期のサポート期間を提供するソフトウェア リリースを提供します。</p>

リリースタイプ	説明	利点
早期展開 (ED)	バグ修正に加えて、新機能と新しいハードウェアプラットフォームのサポートを提供するソフトウェアリリース。これらのリリースは、早期導入 (ED) として分類されます。これらのリリースは短寿命リリースです。	最新の機能と新しいハードウェアプラットフォームまたはモジュールを導入することができます。

リリースの詳細な推奨事項については、次の場所にある『Guidelines for Cisco Wireless Software Release Migration Bulletin』を参照してください。

<http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html>。

表 2: シスコ ワイヤレス リリースのアップグレードパス **8.10.185.0**

現在のソフトウェアリリース	リリースへのアップグレードパス <b>8.10.185.0</b>
8.5.x	リリース 8.10.185.0 に直接アップグレードできます。
8.6.x	リリース 8.10.185.0 に直接アップグレードできます。
8.7.x	リリース 8.10.185.0 に直接アップグレードできます。
8.8.x	リリース 8.10.185.0 に直接アップグレードできます。
8.9.x	リリース 8.10.185.0 に直接アップグレードできます。
8.10.x	リリース 8.10.185.0 に直接アップグレードできます。

## シスコ ワイヤレス リリースのアップグレード

ここでは、シスコ ワイヤレス リリースをアップグレードする際の注意事項と制限事項およびアップグレード手順について説明します。

### 注意事項と制約事項

- 名前に「?」が付いた既存の WLAN は、このアップグレードでも引き続きサポートされません。ただし、新しい WLAN を作成するときに名前に「?」を含めることはできません。
- デフォルトの管理ユーザーログイン情報が原因で AP がコンソールをロックアウトした場合、AP コンソールにアクセスするには、コントローラ AP グローバルログイン情報をデフォルト以外のユーザー名とパスワードで設定する必要があります。
- WPA3 アップグレードとダウングレードのガイドライン：

- リリース 8.5 から 8.10 にアップグレードする場合、リリース 8.10 で有効な WPA1 AKM を使用せずに WPA1 を設定すると、アップグレード後に WPA1 設定が無効になります。
- リリース 8.10 からリリース 8.5 にダウングレードする場合、SAE 用の AKM が構成されていると、ダウングレード後に AKM 検証が失敗します。セキュリティは WPA2、AKM は 802.1X に設定されています。ただし、PMF 構成は保持されるため、エラーが発生します。
- PMF 構成と FT 構成が分離されているため、リリース 8.10 では、FT を有効状態に設定し、PMF を必須状態に設定することができます。ただし、リリース 8.5 では、この構成は無効です。したがって、リリース 8.5 にダウングレードすると、WLAN が無効になる場合があります。
- リリース 8.10 のソフトウェア ダウングレード ガイドライン：
  - リリース 8.10 ソフトウェアから Cisco コントローラをダウングレードする場合は、コントローラ構成ファイルの破損を防ぐために、リリース 8.5.151.0 以降のリリースにダウングレードすることをお勧めします。
  - リリース 8.10 で新しい国コードを設定していて、以前のリリースにダウングレードする予定の場合は、ダウングレードする前に新しい国コードの設定を削除することをお勧めします。詳細については、[CSCVq91895](#) を参照してください。
- Cisco コントローラを別のリリースにダウングレードまたはアップグレードする前に、AP または AP モードがサポートされているか確認してください。サポートされている AP のみが接続され、AP はコントローラがアップグレードまたはダウングレードされるリリースでサポートされているモードに移行されることを確認します。
- RC4 または 3DES 暗号化タイプを必要とするレガシークライアントは、ローカル EAP 認証ではサポートされません。
- リリース 8.0.140.0 または 8.0.15x.0 にダウングレードした後で以降のリリースにアップグレードするときに、複数国番号機能も設定している場合、構成ファイルが破損することがあります。以降のリリースにアップグレードしようとする、特殊文字が国のリストに追加され、構成のロード時に問題が発生します。詳細については、[CSCve41740](#) を参照してください。



(注) 他のリリース間のアップグレードおよびダウングレードでは、この問題は発生しません。

- Cisco AP に新しいソフトウェアをダウンロードした後、Cisco AP がアップグレードイメージの状態に停止する場合があります。このようなシナリオでは、コントローラを強制的に再起動して新しいコントローラ ソフトウェア イメージをダウンロードするか、新しいコントローラ ソフトウェア イメージのダウンロード後にコントローラを再起動する必要がある

ある場合があります。**reset system forced** コマンドを入力して、コントローラを強制的にリブートします。

- マルチキャストおよび IP アドレスの検証により、コントローラから一部の古い設定をダウンロードすることはできません。グローバルマルチキャストおよびマルチキャストモードのプラットフォームサポートの詳細については、『Cisco Wireless Controller Configuration Guide』の「Restrictions on Configuring Multicast Mode」の項を参照してください。
- クライアントが HTTP 要求を送信すると、コントローラはその要求を代行受信してログインページにリダイレクトします。コントローラによって代行受信された HTTP GET 要求が 2000 バイトを超えている場合、コントローラはそのパケットをドロップします。この制限に対処するために使用できる機能拡張については、不具合 ID [CSCuy81133](#) を参照してください。
- あるリリースから以前のリリースにダウングレードするときには、現在のリリースの設定が失われるおそれがあります。回避策として、バックアップサーバーに保存されている以前のコントローラ設定ファイルをリロードするか、コントローラを再設定する方法があります。
- 中間のリリースにコントローラをアップグレードする場合は、コントローラにアソシエートされているすべての AP を中間リリースにアップグレードしてから最新のコントローラソフトウェアをインストールしてください。大規模なネットワークでは、各 AP でソフトウェアをダウンロードするのに多少時間がかかる場合があります。
- FIPS が有効な場合でも、コントローラソフトウェアの新しいリリースへのアップグレードや、旧リリースへのダウングレードは実行できます。
- 最新のソフトウェアリリースにアップグレードすると、コントローラにアソシエートされている AP のソフトウェアも自動的にアップグレードされます。AP がソフトウェアをロードしている場合、アクセスポイントの各 LED は連続して点滅します。
- コントローラでは、標準の SNMP MIB ファイルがサポートされています。MIB は Cisco.com のソフトウェアのダウンロードページからダウンロードできます。
- コントローラソフトウェアは、工場ですべてのコントローラにインストールされており、リリースのアップグレード後や、AP がコントローラに参加したときには、AP に自動的にダウンロードされます。運用上の利点を最大限活用するために、利用可能な最新のソフトウェアバージョンをインストールすることを推奨します。
- ソフトウェアのアップグレードに TFTP、HTTP、FTP、または SFTP サーバーが使用できることを確認します。サーバーをセットアップするときには、次のガイドラインに従ってください。
  - TFTP サーバーで、コントローラソフトウェアリリースよりも大きなサイズのファイルがサポートされていることを確認します。このサイズのファイルをサポートする TFTP サーバーには、`tftpd32` や Cisco Prime Infrastructure 内の TFTP サーバーがあります。コントローラソフトウェアイメージをダウンロードするときに TFTP サーバーでこのサイズのファイルがサポートされていないと、次のエラーメッセージが表示されます。

「TFTP failure while storing in flash」

- ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能であるため、TFTP サーバーまたは FTP サーバーは、同じサブネット上にあっても別のサブネット上にあってもかまいません。
- コントローラのブートローダには、アクティブなプライマリ イメージとバックアップ イメージのコピーが保存されています。プライマリ イメージが破損した場合は、バックアップ イメージを使用してブートローダを起動させることができます。

バックアップ イメージが保存されている状態で、リブートの前に [Boot Options] メニューで [Option 2: Run Backup Image] を選択し、バックアップ イメージから起動されるようにします。次に、動作することが判明しているイメージでアップグレードを行い、コントローラをリブートします。

- 管理インターフェイスで NAT が有効になっている場合に、Control and Provisioning of Wireless Access Points (CAPWAP) ディスカバリ応答で送信されるアドレスを制御するには、次のコマンドを使用します。

**config network ap-discovery nat-ip-only {enable | disable}**

コマンドの詳細は次のとおりです。

**enable** : NAT IP の使用をディスカバリ応答でのみ有効にします。これはデフォルトです。このコマンドは、すべての AP が NAT ゲートウェイの外にある場合に使用します。

**disable** : ディスカバリ応答での NAT IP および非 NAT IP の両方の使用を有効にします。このコマンドは、AP が NAT ゲートウェイの内部および外部にある場合に使用します。たとえば、ローカル モードの AP と OfficeExtend AP が同じコントローラにある場合です。



- (注) AP が孤立するのを防ぐには、**config network ap-discovery nat-ip-only** コマンドに **disable** オプションを使用する前に、AP のリンク遅延を無効にする必要があります (有効にされている場合)。AP のリンク遅延を無効にするには、**config ap link-latency disable all** コマンドを使用します。

- アップグレードプロセス中にコントローラまたはいずれかの AP の電源をオフにしないでください。電源をオフにすると、ソフトウェアイメージが破損する可能性があります。多数の AP を含むコントローラをアップグレードするには、ネットワークのサイズにもよりますが、最大で 30 分かかる場合があります。ただし、同時にアップグレードされる AP 数が増加したため、アップグレードの時間が大幅に短縮されました。AP の電源は入れたままにしておく必要があります。また、アップグレード時にコントローラをリセットしてはなりません。
- 次の操作をコントローラで実行した後は、変更を有効にするためにコントローラをリブートする必要があります。

- LAG の有効化または無効化
- 証明書に関する機能の有効化 (HTTPS や Web 認証など)
- 新しいライセンスの追加、または既存のライセンスの変更



---

(注) 使用権ライセンスを使用している場合、再起動は必要ありません。

---

- ライセンスの優先度を上げます。
- HA を有効にします。
- SSL 証明書をインストールします。
- データベース サイズを設定します。
- ベンダーデバイス証明書をインストールします。
- CA 証明書をダウンロードします。
- 設定ファイルをアップロードします。
- Web 認証証明書をインストールします。
- 管理インターフェイスまたは仮想インターフェイスに変更を加えます。

## シスコ ワイヤレス ソフトウェアのアップグレード (GUI)

### 手順

---

**ステップ 1** コントローラの設定ファイルをサーバーにアップロードして設定ファイルをバックアップします。

(注) コントローラソフトウェアをアップグレードする前に、コントローラの設定ファイルをバックアップしておくことを強く推奨します。

**ステップ 2** 次の手順に従って、コントローラ ソフトウェアを入手します。

- a) ソフトウェア ダウンロード ポータル (<https://software.cisco.com/download/home>) を参照します。
- b) コントローラ モデルを検索します。
- c) [Wireless LAN Controller Software] をクリックします。
- d) ソフトウェアリリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。コントローラ ソフトウェア リリース番号をクリックします。

- [Early Deployment (ED)] : これらのソフトウェア リリースには、バグ修正ファイルだけでなく、新機能および新しいハードウェア プラットフォーム サポートが付属しています。
- [Maintenance Deployment (MD)] : これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
- [Deferred (DF)] : これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。

- ファイル名 `<filename.aes>` をクリックします。
- [Download] をクリックします。
- シスコのエンドユーザー ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- お使いのハード ドライブにファイルを保存します。
- ステップ *a* から *h* を繰り返して、他のファイルをダウンロードします。

**ステップ 3** コントローラソフトウェアのファイル `<filename.aes>` を TFTP、FTP、SFTP、または USB サーバーのデフォルトディレクトリにコピーします。

**ステップ 4** (任意) コントローラ 802.11 ネットワークを無効にします。

- (注) 使用率の高いネットワークやコントローラ、または小規模なコントローラプラットフォームでは、予防措置として 802.11 ネットワークを無効にすることをお勧めします。

**ステップ 5** [Commands] > [Download File] の順に選択して [Download File to Controller] ページを開きます。

**ステップ 6** [File Type] ドロップダウン リストから、[Code] を選択します。

**ステップ 7** [Transfer Mode] ドロップダウン リストから、[TFTP]、[FTP]、[SFTP]、[HTTP]、または [USB] を選択します。

**ステップ 8** プロンプトに従って、対応するサーバーの詳細を入力します。

- (注) 転送モードとして HTTP を選択した場合、サーバーの詳細は必要ありません。

**ステップ 9** [Download] をクリックして、ソフトウェアをコントローラにダウンロードします。

ダウンロードのステータスを示すメッセージが表示されます。

- (注) 両方のイメージで [File Type] に [Code] を選択していることを確認します。

**ステップ 10** ダウンロードの完了後、[Reboot] をクリックします。

**ステップ 11** 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。

**ステップ 12** [OK] をクリックし、変更内容を確定してコントローラをリブートします。

**ステップ 13** 802.11 ネットワークを無効にした場合は、再度有効にします。

- ステップ 14** (任意) コントローラにコントローラ ソフトウェアがインストールされたことを確認するには、コントローラ GUI の [Monitor] をクリックして、[Controller Summary] の下の [Software Version] フィールドを確認します。

## 5520 および 8540 コントローラの CIMC ユーティリティのアップグレード

AIR-CT5520-K9 および AIR-CT8540-K9 コントローラ モデルは、それぞれ Cisco UCS サーバ C シリーズの C220 および C240 M4 に基づいています。これらのコントローラ モデルには、電源、メモリ、ディスク、ファン、温度などの低レベルの物理パーツを編集またはモニターしたり、コントローラへのリモート コンソール アクセスを提供できる CIMC ユーティリティがあります。

CIMC ユーティリティを、これらのコントローラで使用することが認定されているバージョンにアップグレードすることをお勧めします。古いバージョンの CIMC がインストールされているコントローラは、FlexFlash にアクセスできずに再起動する可能性があります。その結果、製造元の証明書が使用できなくなり、SSH および HTTPS 接続に失敗し、アクセス ポイントが参加できなくなります。CSCvo33873 を参照してください。推奨されるバージョンは、CSCvo01180 警告で追跡されている脆弱性に対処します。

認定済み CIMC イメージは、次の場所で入手できます。

表 3: CIMC ユーティリティのソフトウェア イメージ情報

コントローラ	現在の CIMC バージョン	推奨される CIMC バージョン	CIMC ユーティリティのソフトウェア イメージをダウンロードするためのリンク
Cisco 5520 ワイヤレス コントローラ Cisco 8540 ワイヤレス コントローラ	2.x	3.0(4r)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)">https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)</a>  (注) TFTP、SCP プロトコルのみを使用して、ファームウェアを 2.0(13i) から 3.0(4r) にアップグレードすることをお勧めします。
Cisco 5520 ワイヤレス コントローラ Cisco 8540 ワイヤレス コントローラ	3.0 (4d)	3.0(4r)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)">https://software.cisco.com/download/home/286281345/type/283850974/release/3.0(4r)</a>

コントローラ	現在の CIMC バージョン	推奨される CIMC バージョン	CIMC ユーティリティのソフトウェアイメージをダウンロードするためのリンク
Cisco 5520 ワイヤレス コントローラ Cisco 8540 ワイヤレス コントローラ	4.0(1a)	4.0(2n)	<a href="https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)">https://software.cisco.com/download/home/286281345/type/283850974/release/4.0(2n)</a>

表 4: 4.x バージョンへのファームウェアアップグレードパス

現在のファームウェアバージョン	4.x バージョンへのアップグレードパス
2.x	3.x バージョンにアップグレードしてから、推奨される 4.x バージョンにアップグレードする必要があります。
3.x	推奨される 4.x バージョンに直接アップグレードできます。

- CIMC ユーティリティバージョン 2.x のアップグレードについては、『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.0』の「Introduction to Cisco IMC Secure Boot」のセクションを参照してください。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/cli/config/guide/3\\_0/b\\_Cisco\\_UCS\\_C-Series\\_CLI\\_Configuration\\_Guide\\_301/b\\_Cisco\\_UCS\\_C-Series\\_CLI\\_Configuration\\_Guide\\_201\\_chapter\\_01101.html#d92865e458a1635](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/3_0/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_301/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_201_chapter_01101.html#d92865e458a1635)

WebUI を使用した CIMC ユーティリティバージョン 2.x のアップグレードについては、「Updating the Firmware」セクションを参照してください。[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/gui/config/guide/3\\_0/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_for\\_HTML5-Based\\_Servers\\_301/b\\_Cisco\\_UCS\\_C-Series\\_GUI\\_Configuration\\_Guide\\_207\\_chapter\\_01101.html#task\\_C137961E9E8A4927A1F08740184594CA](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/3_0/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_for_HTML5-Based_Servers_301/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_207_chapter_01101.html#task_C137961E9E8A4927A1F08740184594CA)



- (注) WebUI メソッドを使用してファームウェアをアップグレードする場合、WebUI でプロンプトが表示されたら、[Install Firmware through Remote Server] オプションを選択する必要があります。

- CIMC ユーティリティのアップグレードの詳細については、『Cisco Host Upgrade Utility 3.0 User Guide』の「Updating the Firmware on Cisco UCS C-Series Servers」の章を参照してください。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/c/sw/lomug/2-0-x/3\\_0/b\\_huu\\_3\\_0\\_1/b\\_huu\\_2\\_0\\_13\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/3_0/b_huu_3_0_1/b_huu_2_0_13_chapter_011.html)

- [Update All] オプションを使用したファームウェアの更新

ここでは、Cisco 5520 または 8540 コントローラで CIMC ユーティリティを使用する場合について詳しく説明します。ソフトウェアおよび UCS シャーシの一般的な情報について

は、以下のサイトにある『Release Notes for Cisco UCS C-Series Software, Release 3.0(4)』を参照してください。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/release/notes/b\\_UCS\\_C-Series\\_Release\\_Notes\\_3\\_0\\_4.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html)

Cisco UCS C シリーズ ソフトウェア、リリース 4.0(2) リリースノートは以下のサイトを参照してください。

[https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/release/notes/b\\_UCS\\_C-Series\\_RN\\_4\\_0\\_2.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_RN_4_0_2.html)

表 5: リリース 4.0(2f) の解決済みの不具合

警告 ID	説明
CSCvn80088	NI-HUU は、CIFS リモート共有のパスワードの特殊文字を処理できない

表 6: リリース 3.0(4f) の解決済みの不具合

警告 ID	説明
CSCvp41543	SSH の弱い KeyExchange アルゴリズム [diffie-hellman-group14-sha1] を削除する必要がある

## 他の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 ソフトウェアと他のクライアント デバイスとの相互運用性について説明します。

次の表では、クライアント デバイスのテストに使用される設定について説明します。

表 7: 相互運用性のテスト ベッド設定

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設定タイプ
リリース	8.10.x
シスコ ワイヤレス コントローラ	Cisco 3504 ワイヤレス コントローラ
アクセスポイント	Cisco 9130、9120、および 3800 AP
無線機	802.11ax (2.4 GHz または 5 GHz)、802.11ac、802.11a、802.11n (2.4 GHz または 5 GHz)
セキュリティ	オープン、WPA3-SAE/OWE (WPA3 対応クライアント)、WPA2-PSK (WPA2-AES)、802.1X (WPA2-AES) (EAP-PEAP)

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設定タイプ
RADIUS	Cisco ISE 2.5
テストのタイプ	AP 間のアソシエーション、トラフィック (TCP/UDP/ICMP) 、

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、プリンタなどが含まれます。

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/ソフトウェアバージョン
<b>Wi-Fi 6 デバイス (携帯電話およびラップトップ)</b>	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
DELL LATITUDE 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
<b>ラップトップ</b>	
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 Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136

クライアントのタイプおよび名前	ドライバ/ソフトウェアバージョン
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
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 (18.32.0.5)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
DELL XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 (1.0.10440.0)
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。	
<b>タブレット</b>	
Apple iPad Pro	iOS 13.5
Apple iPad Air 2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 ~ 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 ~ 11ax	Intel AX201 チップセット。Driver v21.40.1.3
Microsoft Surface Pro 7 ~ 11ax	Intel Wi-Fi チップ (HarrisonPeak AX201) (11ax、WPA3)
Microsoft Surface Pro X – 11ac および WPA3	WCN3998 Wi-Fi チップ (11ac、WPA3)
<b>携帯電話</b>	
Apple iPhone 5	iOS 12.4.1

クライアントのタイプおよび名前	ドライバ/ソフトウェアバージョン
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
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 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Android 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Xperia 1 ii	Android 10
Sony Xperia xz3	Android 9.0
Xiaomi Mi10	Android 10

クライアントのタイプおよび名前	ドライバ/ソフトウェア バージョン
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android バージョン : 4.1.1
Zebra MC92N0	Android バージョン : 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
<b>プリンタ</b>	
Zebra QLn320 プリンタ	LINK OS 6.3
Zebra ZT230 プリンタ	LINK OS 6.3
Zebra ZQ310 プリンタ	LINK OS 6.3
Zebra ZD410 プリンタ	LINK OS 6.3
Zebra ZT410 プリンタ	LINK OS 6.3
Zebra ZQ610 プリンタ	LINK OS 6.3
Zebra ZQ620 プリンタ	LINK OS 6.3
<b>ワイヤレスモジュール</b>	
Intel 11ax 200	ドライバ v21.40.1.3、v21.20.1.1
Intel AC 9260	ドライバ v21.40.0
Intel Dual Band Wireless AC 8260	ドライバ v19.50.1.6

## コントローラ プラットフォームでサポートされていない主要機能

このセクションでは、各種コントローラプラットフォームでサポートされていない機能を示します。



(注) AireOS コードを実行するコントローラを使用する統合アクセス環境では、ハイアベイラビリティクライアント SSO とネイティブ IPv6 はサポートされません。

## Cisco 3504 WLC でサポートされていない主要機能

- Cisco WLAN Express セットアップの OTA プロビジョニング
- 統合アクセス モードのモビリティ コントローラ機能
- VPN 終端 (IPSec および L2TP など)

## Cisco 5520 WLC および 8540 WLC でサポートされていない主要機能

- 内部 DHCP サーバー
- 統合アクセス モードのモビリティ コントローラ機能
- VPN 終端 (IPSec および L2TP など)
- インターフェイス上でのフラグメントされた ping

## Cisco Virtual WLC でサポートされない主要機能

- Cisco Umbrella
- SD-Access
- ドメインベースの ACL
- 内部 DHCP サーバー
- Cisco TrustSec
- ローカル モードのアクセス ポイント
- モビリティまたはゲスト アンカーのロール
- 有線ゲスト
- マルチキャスト



(注) FlexConnect でローカルにスイッチングされるマルチキャストトラフィックは、同じ VLAN 上の有線およびワイヤレスの両方で透過的にブリッジングされます。FlexConnect AP は、IGMP または MLD スヌーピングに基づいてトラフィックを制限しません。

- 大規模な展開での FlexConnect 中央スイッチング



(注) • FlexConnect 中央スイッチングは、コントローラ ポートの合計トラフィックが 500 Mbps を超えない小規模な展開でのみサポートされます。

• FlexConnect ローカル スwitching はサポートされます。

- 
- Microsoft Hyper-V 展開での中央スイッチング
  - 高可用性の AP とクライアント SSO
  - PMIPv6
  - Datagram Transport Layer Security (DTLS)
  - EoGRE (ローカル スwitching モードでのみサポート)
  - ワークグループブリッジ
  - 中央スイッチングに対するクライアント ダウンストリーム レート制限
  - SHA2 証明書
  - Lync SDN API とのコントローラの統合
  - Cisco OfficeExtend アクセス ポイント

## アクセスポイントプラットフォームでサポートされていない主要機能

このセクションでは、各種 Cisco Aironet AP プラットフォームでサポートされていない主な機能を示します。Cisco Aironet Wave 2 AP および 802.11ax AP での機能のサポートの詳細については、次を参照してください。

[https://www.cisco.com/c/en/us/td/docs/wireless/access\\_point/feature-matrix/ap-feature-matrix.html](https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html)

## Cisco Aironet 1800i、1810 OEAP、1810W、1815、1830、1850、2800、3800、および 4800 シリーズの AP でサポートされていない主要機能

表 9: Cisco Aironet 1800i、1810 OEAP、1810W、1815、1830、1850、2800、3800、および 4800 シリーズの AP でサポートされていない主要機能

動作モード	<ul style="list-style-type: none"> <li>• 自律ブリッジおよびワークグループブリッジ (WGB) モード (注) WGB は Cisco Aironet 2800、3800 シリーズ AP でサポートされています。</li> <li>• メッシュモード (注) メッシュモードは、リリース 8.10.x の Cisco Aironet 1815i、1815m、1830、1850、2800、3800、および 4800 シリーズ AP でサポートされています。</li> <li>• NAT または PAT 環境の背後にある LAG</li> </ul>
プロトコル	<ul style="list-style-type: none"> <li>• 完全な Cisco Compatible Extensions (CCX) のサポート</li> <li>• Rogue Location Discovery Protocol (RLDP)</li> <li>• Telnet</li> </ul>
セキュリティ	<ul style="list-style-type: none"> <li>• ダイナミック WEP を使用した CKIP、CMIC、LEAP</li> <li>• CKIP の静的 WEP</li> <li>• WPA2 + TKIP (注) WPA + TKIP および TKIP + AES プロトコルがサポートされています。</li> </ul>
QoS	<p>Cisco Air Time Fairness (ATF)</p> <p>(注) ATF は、リリース 8.10 の Cisco Aironet 2800、3800、および 4800 シリーズ AP でサポートされています。</p>

FlexConnect の機能	<ul style="list-style-type: none"> <li>• PPPoE</li> <li>• マルチキャストからユニキャストへ (MC2UC) (注) VideoStream がサポートされています。</li> <li>• Traffic Specification (TSpec) <ul style="list-style-type: none"> <li>• Cisco Compatible Extension (CCX)</li> <li>• コールアドミッション制御 (CAC)</li> </ul> </li> <li>• VSA/レルム照合認証</li> <li>• ローカルスイッチングモードの FlexConnect を使用した SIP スヌーピング</li> </ul>
-----------------	---



(注) 現在サポートされている機能の詳細を含む Cisco Aironet 1850 シリーズ AP の技術仕様については、『[Cisco Aironet 1850 Series Access Points Data Sheet](#)』を参照してください。

## Cisco Aironet 1800i、1810 OEAP、および 1810W シリーズの AP でサポートされていない主要機能

表 10: Cisco Aironet 1800i、1810 OEAP、および 1810W シリーズの AP でサポートされていない主要機能

動作モード	Mobility Express
FlexConnect の機能	ローカル AP 認証
ロケーション サービス	データ RSSI (高速検索)

## Cisco Aironet 1830、1850、および 1815 シリーズの AP でサポートされていない主要機能

表 11: Cisco Aironet 1830、1850、および 1815 シリーズの AP でサポートされていない主要機能

動作モード	Mobility Express は Cisco 1815t AP でサポートされていません。
FlexConnect の機能	ローカル AP 認証
ロケーション サービス	データ RSSI (高速検索)

## メッシュネットワークでサポートされていない主要機能

- ローカルベースのコールアドミッション制御 (CAC)。メッシュネットワークは帯域幅ベース CAC または静的 CAC のみサポートします。
- ハイアベイラビリティ (高速ハートビートおよびプライマリディスカバリ join タイマー)
- FASTv1 および 802.1 X 認証でサブリカントとして動作する AP
- AP 参加優先順位 (メッシュ AP には固定の優先順位があります)
- ロケーションベースのサービス

## Cisco Aironet 1540 メッシュ AP でサポートされていない主要機能

- ダイナミック メッシュ バックホール データ レート。



(注) AP のブリッジデータ レートを [auto] のままにしておくことをお勧めします。

- バックグラウンド スキャン
- ノイズ耐性高速コンバージェンス

## Cisco Aironet 1560 AP でサポートされていない主要機能

- MAC 認証 FlexConnect ローカル認証
- ノイズ耐性高速コンバージェンス
- 静的 WEP

## Cisco Catalyst IW6300 Heavy Duty シリーズ AP および 6300 シリーズ エンベデッド サービス AP でサポートされていない主な機能

- MAC 認証 FlexConnect ローカル認証
- ノイズ耐性高速コンバージェンス
- 静的 WEP

## 不具合

### リリースで未解決の不具合 8.10.185.0

表 12: 未解決の不具合

ID	見出し
CSCvv81814	Cisco 1850 AP : ファームウェアアサート 0x00942D74/0x00942D79
CSCvw28085	OEAP フラッディング syslog メッセージ : 「parse_tx_bcn: Bcn payload is NULL」
CSCvx51916	C9120 でメッセージ「ASLR ENTROPY INSUFFICIENT」
CSCvy60791	9130AXI - コントローラ GUI にデュアル無線割り当て設定が存在しない
CSCwb20581	コントローラ : Emweb が原因で AireOS システムが予期せずリロードされた
CSCwc48042	Cisco Wave 2 AP は、コントローラの EAP タイムアウトに準拠していない (中央認証)
CSCwc49970	Cisco Aironet 2800、3800、4800 でチャンネル 165 が許可されない
CSCwc64201	WGB としての Cisco 9105 がパケット OTA の転送に失敗し、通信にギャップが生じる
CSCwd41463	Cisco 3800、4800 AP が IGMP メンバーシップレポートの送信を停止する
CSCwd71613	AP 9120 は、自身の BSSID を悪意のある/なりすましとして検出する
CSCwd78616	ほとんどの AP9115 Tx 電力が高く、ネイバーがないために異常な DCA チャンネル割り当てである
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、9800 デバイスは古いエントリを追跡している
CSCwd90742	AP9120AX でカーネルクラッシュが発生する (PC : rhb_del_interface+0xc)
CSCwe00848	カーネルパニック - 同期していない : 致命的な例外 9105 により予期せずランダムにリロードされる
CSCwe13020	Cisco Catalyst 9120 AP で、iPSK で無線によるダイレクトブロードキャストが送信されていない
CSCwe15203	コントローラが複数の AP の CleanAir ステータスを N/A と表示する

ID	見出し
<a href="#">CSCwe17920</a>	[IW3702] : SUNCOR ポート 9124 がセッション TO の後に WGB にトラフィックを転送しない
<a href="#">CSCwe18353</a>	C9130 AP カーネルパニッククラッシュ PC : <code>__dma_inv_range / LR: __swiotlb_unmap_page</code>
<a href="#">CSCwe22861</a>	8.10.171.0 を実行している Flex Cisco Wave 2 AP で AID リークが発生する
<a href="#">CSCwe24263</a>	C9130 でビーコンで一貫性のない Tx 電力レベルがアダプタイズされる
<a href="#">CSCwe29911</a>	Cisco 3802 FQI/NMI リセット : <code>__rmqueue &amp; get_page_from_freelist</code>
<a href="#">CSCwe30473</a>	RC キューがスタックしているため、無線ファームウェアが予期せずリロードされる
<a href="#">CSCwe30558</a>	カーネルパニックが原因で Cisco 9130 AP が予期せずリロードされる
<a href="#">CSCwe30572</a>	Cisco Wave 2 AP が iOX アプリから NAT IP をリークすることがある
<a href="#">CSCwe31030</a>	9105AXW AP のクラッシュ - NMI watchdog: BUG: soft lockup - CPU#3 stuck for 22s! [shared_printenv:10129]
<a href="#">CSCwe32005</a>	8.10.183.0 リリースソフトウェアを実行している C9130 : デジタルサイネージデバイスでのパケット損失
<a href="#">CSCwe39871</a>	9105 AP は M4 (4 ウェイハンドシェイク) 間に 20 ミリ秒かかり、クライアントトラフィックの転送を許可する
<a href="#">CSCwe41945</a>	C9130 AP 無線ファームウェアが予期せずリロードし、コアファイルが生成されない
<a href="#">CSCwe43294</a>	C9105AXW および 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 を適用しない
<a href="#">CSCwe44216</a>	カーネルパニックが原因で Cisco AP が予期せずリロードする (PC : <code>fp_reload_hw+0x30/0x44</code> )
<a href="#">CSCwe44991</a>	C9105AX AP : カーネルパニッククラッシュ
<a href="#">CSCwe45894</a>	AP がワイヤレスクライアントに IGMPv3 クエリを転送しない
<a href="#">CSCwe46834</a>	C9120AXI-E AP は、報告されているよりも高い電力で送信している

## リリース 8.10.185.0 の解決済みの不具合

表 13: 解決済みの不具合

ID	見出し
<a href="#">CSCvv96364</a>	17.3.1 を実行している 3800 AP : プロセス WCPd が予期せずリロードする
<a href="#">CSCvw20363</a>	クライアント証明書がインストールされていない場合、2800/3800 WGB が PEAP 経由で接続できない
<a href="#">CSCvx32806</a>	イメージチェックサム検証の失敗により、Cisco Wave 2 AP がブートループでスタックする
<a href="#">CSCvx80422</a>	AP が、10.128.128.127 または 10.128.128.128 宛てのパケットをドロップする
<a href="#">CSCwa48702</a>	C9130AX AP でのカーネルパニッククラッシュ
<a href="#">CSCwa68709</a>	Cisco 9115 AP がチャンネルで DFS を誤って報告する。「クリアされる予定のブロックリスト」
<a href="#">CSCwa93884</a>	アプリのアクティベーションフェーズで Cisco iOX アプリのインストールが失敗する。「アプリの起動スクリプトの作成中にエラーが発生」
<a href="#">CSCwb08291</a>	C9105AXW でクライアントが RLAN ポートを使用している場合に遅延が発生する
<a href="#">CSCwb23886</a>	Cisco 1810W : 特定のクライアントモデルでの RLAN DHCP の問題
<a href="#">CSCwb34231</a>	Cisco 9115 AP : 無線での省電力クライアント状態
<a href="#">CSCwb41815</a>	8.10 のスイッチで「cts manual」を有効にした後、AP が DHCP ACK パケットをコントローラにコピーしない
<a href="#">CSCwb51757</a>	40Mhz の 5GHz 無線での高いチャンネル使用率
<a href="#">CSCwb82694</a>	9105/9115/9120 シリーズのアクセスポイントは、順序が正しくないパケットを処理できない
<a href="#">CSCwb96560</a>	AppHost : ap-join プロファイルで USB 状態が無効になっていると、アプリのインストールが失敗する
<a href="#">CSCwc02477</a>	Cisco 9130 AP が EAP ID 要求を送信しない
<a href="#">CSCwc12918</a>	リパーリセットにより、Cisco コントローラが SNMPTask で予期せずリロードする
<a href="#">CSCwc31331</a>	C9130 アクセスポイントが run_timer_softirq で予期せずリロードする
<a href="#">CSCwc32182</a>	AP 1852 無線ファームウェアのクラッシュ

ID	見出し
<a href="#">CSCwc38912</a>	サイト/ポリシータグの変更後に Flex WLAN に参加すると、LWA クライアントがすぐに削除される
<a href="#">CSCwc55632</a>	Cisco 9124 MAP で MAP の最初のリロード後に 1562 RAP への接続に失敗する
<a href="#">CSCwc56767</a>	コマンド「show tech」を実行すると、Cisco 5520 コントローラが予期せずリロードする
<a href="#">CSCwc72194</a>	Cisco 9120 AP : 無線コアダンプ : w10: wlc_check_assert_type HAMMERING
<a href="#">CSCwc73462</a>	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ない
<a href="#">CSCwc75732</a>	ファームウェア無線が 17.3.5b コードの Cisco 4800 アクセスポイントで予期せずリロードする
<a href="#">CSCwc78435</a>	C9130AP は、アウトオブバンド DFS イベントで誤ったチャン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す
<a href="#">CSCwc81656</a>	AIR-CAP2702E-K-K9 でフラッシュファイルシステムの破損
<a href="#">CSCwc87688</a>	Cisco 9120 AP : 5 GHz 無線で非常に高いノイズレベルをランダムに示す
<a href="#">CSCwc89719</a>	無線障害（無線の復旧に失敗）が原因で AP1832 が予期せずリロードされる
<a href="#">CSCwc94898</a>	WGB AP が EAPOL 状態でスタックする
<a href="#">CSCwc99024</a>	8.10.162.0    5520 コントローラ    タスク emweb での予期しないリロード
<a href="#">CSCwd00751</a>	8.10.171 ソフトウェアリリースを実行している AP 2802 が予期せずリロードする
<a href="#">CSCwd02898</a>	C9300 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ない
<a href="#">CSCwd03803</a>	AP1815I がリブート --- PC が edma_poll か、LR が dma_cache_maint_page にある場合
<a href="#">CSCwd05593</a>	データブロック PS および AP 無線クラッシュが原因の Cisco 9120 TX STUCK
<a href="#">CSCwd06795</a>	ローカル EAP の使用時にパスワードが間違っているにもかかわらず EAP が失敗しない
<a href="#">CSCwd07551</a>	Dot1x_NW_MsgTask_7 が原因でコントローラ 5520 が予期せずリロードする
<a href="#">CSCwd08259</a>	17.3 以降を実行している AP C9120、C9115、C9105 無線ファームウェアが予期せずリロードする

ID	見出し
<a href="#">CSCwd08926</a>	ネイティブスキャンとして設定された BLE での CW9162 AP クライアント接続障害
<a href="#">CSCwd10570</a>	不正なデータレートの 9130 ビーコン - 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る
<a href="#">CSCwd19631</a>	スイッチポートで EEE が有効になっている場合、9120 AP が mGig で動作しない
<a href="#">CSCwd21996</a>	9120 アクセスポイントで CleanAir センサーが予期せずリロードする
<a href="#">CSCwd36552</a>	カーネルパニックで AP9120 が予期せずリロードされる - 同期していない : 致命的な例外
<a href="#">CSCwd37092</a>	Cisco 2800、3800、4800、1562、6300 シリーズ AP : 遅い TCP ダウンロード、8.10.181.0/17.3.6 SW での EAP-TLS の失敗
<a href="#">CSCwd37280</a>	スリープ状態のクライアントが失敗する。AireOS 外部はアイドルタイムアウト ペイロードを送信しない
<a href="#">CSCwd38925</a>	PC が wlc_key_get にあり、LR が wlc_prep_pdu にあるときに、Cisco C9105 が複数回予期せずリロードする
<a href="#">CSCwd39605</a>	カーネルパニックが原因で Cisco 9117 AP が console_unlock+0x320/0x3ac で予期せずリロードする
<a href="#">CSCwd40355</a>	8.10.171.0 を実行しているコントローラ 5520 : タスク NFV9_Task でシステムが予期せずリロードする
<a href="#">CSCwd40731</a>	カーネルパニックが原因で AP がリロードし続ける。同期は実行されず、ソフトロックアップが発生し、タスクがハングする
<a href="#">CSCwd44421</a>	コントローラが異なる 9130 AP の電波品質 AQ の正しい出力を報告しない
<a href="#">CSCwd46815</a>	Cisco 2800、3800、4800、1562、6300 シリーズ AP : MAP の背後にある有線クライアントで EAP-TLS に失敗する
<a href="#">CSCwd49166</a>	Cisco 3800 AP が常に高い QBSS 負荷を報告する
<a href="#">CSCwd55757</a>	Systemd の重要プロセスのクラッシュで Wave 2 AP が予期せずリロードする - dnsmasq-host.service が失敗した
<a href="#">CSCwd58182</a>	カーネルパニックが原因で 3800 シリーズ AP が予期せずリロードする (PC は vfp_reload_hw+0x30/0x44 にある)
<a href="#">CSCwd59921</a>	Cisco 9130 AP が EAP-TLS フレームをドロップしている
<a href="#">CSCwd60034</a>	ビーコンがスタックしているために 3800 AP 無線が予期せずリロードする

ID	見出し
CSCwd60376	C9120 AP で PC が pci_generic_config_read+0x34/0xa8 にあるときにカーネルパニックが発生する
CSCwd72847	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断続的に停止する
CSCwd74571	プロセス：解放されたパケットの再利用により、wcpd が予期せずリロードする
CSCwd77823	9130 AP 無線ファームウェアがランダムにクラッシュする
CSCwd79462	コントローラが 4800 AP モデルの電波品質 AQ の出力を正しくレポートしない
CSCwd80290	Cisco 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る
CSCwd81523	C9130 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ない
CSCwd83840	ワイヤレスクライアントが Cisco 1830 AP に接続できず、「writing to fd 27 failed!」というエラーが表示される。
CSCwd89752	「debug spectrum all enable」を実行すると、ヌルポイントが原因でワイヤレス LAN コントローラが再起動する
CSCwd91054	COS-AP で M1 ~ M4 の後に EAP_ID_REQ が暗号化されず、dot1x OKC の PMKID が更新されない
CSCwd92780	[Vanc] [9120][17.3.7.12] tx phy エラー/ucode で予期せずリロードする
CSCwe04602	AP 9120 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 秒間失敗する
CSCwe07297	無線ファームウェアのクラッシュが原因で C9120 AP がクラッシュする
CSCwe07802	Cisco 2800/3800/4800/1562 AP がアップストリーム EAP パケットをドロップする
CSCwe11476	filp_close および do_close による C9130 カーネルパニック
CSCwe14029	コントローラが 40 MHz チャンネル幅ではなく 20 MHz を誤って 9130 AP に割り当てる
CSCwe18185	箱から出したばかりの新しい C9130 (VID03) のデイズロ出荷時イメージには iox.tar.gz が含まれていない

ID	見出し
<a href="#">CSCwe19858</a>	Cisco 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する

## 関連資料

### ワイヤレス製品の比較

- 次のツールを使用して、シスコ ワイヤレス アクセス ポイントとコントローラの仕様を比較します。

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

- 製品承認ステータス :

[https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL\\_SEARCH](https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)

- 無線 LAN コンプライアンス検索 :

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

### Cisco ワイヤレス コントローラ

Cisco WLC、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。

- 特定の Cisco WLC またはアクセス ポイントのクイック スタート ガイドまたはインストール ガイド
- [Cisco Wireless Solutions Software Compatibility Matrix](#)
- [Cisco Wireless Controller Configuration Guide](#)
- [Cisco Wireless Controller Command Reference](#)
- [Cisco Wireless Controller System Message Guide](#)

すべての Cisco WLC ソフトウェアに関連するマニュアルについては、次を参照してください。

<http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html>

### Cisco Mobility Express

- [Cisco Mobility Express Release Notes](#)
- [Cisco Mobility Express User Guide](#)
- [Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide](#)

**Cisco Aironet Access Points for Cisco IOS Releases**

- [Release Notes for Cisco Aironet Access Points for Cisco IOS Releases](#)
- [Cisco IOS Configuration Guides for Autonomous Aironet Access Points](#)
- [Cisco IOS Command References for Autonomous Aironet Access Points](#)

コントローラおよびアクセス ポイント ソフトウェアで使用されるオープン ソース

コントローラおよびアクセス ポイント ソフトウェアで使用されるオープン ソースを説明するドキュメントにアクセスするには、このリンクをクリックします。

<https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html>

**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 Digital Network Architecture**

<https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html>

## 通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

## シスコバグ検索ツール

[Ciscoシスコバグ検索ツール \(BST\)](#) 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

シスコのテクニカル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。

---

【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/](http://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: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). 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)

© 2023 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。