

Cisco ワイヤレス コントローラおよび Lightweight アクセス ポイント用 Cisco Wireless リリース 8.9.111.0 リリース ノート

初版 : 2019 年 6 月 6 日

リリース ノートについて

このソフトウェア リリースは、Cisco Catalyst 9100 シリーズ アクセス ポイントで展開されたネットワークでのみ使用することをお勧めします。

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、シスコ ワイヤレス コントローラをコントローラと呼び、シスコの中央管理型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。

コンテンツ ハブ

最新の製品マニュアル ポータルの [コンテンツ ハブ](#) を参照してください。ここでは、ファセット検索を使用して最も関連性の高いコンテンツを検索したり、カスタマイズした PDF を参照していつでも参照したり、コンテキストベースの推奨事項を活用したりすることができます。

パーソナライズされたドキュメントエクスペリエンスを実現するには、<https://content.cisco.com/> のコンテンツ ハブから開始してください。

コンテンツ ハブでの体験のフィードバックをお送りください。

サポート対象の Cisco ワイヤレス コントローラ プラットフォーム

このリリースでは、次の Cisco ワイヤレス 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 バーチャル ワイヤレス コントローラ (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ロードしないことをお勧めします)
- Cisco 3504 WLC、Cisco 5520 WLC、および Cisco 8540 WLC のハイ アベイラビリティを実現する Cisco ワイヤレス コントローラ。
- Cisco Mobility Express ソリューション

サポート対象の Cisco 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 9120 アクセス ポイント
- 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 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



- (注)
- 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-isr/datasheet-c78-739512.html>。

特定の Cisco アクセス ポイント モジュールをサポートしている Cisco 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 8.9.111.0

このセクションでは、このリリースで導入された新機能および拡張機能の概要を簡単に説明します。



- (注)
- Cisco Wireless リリース 8.9 の公開ドキュメントの全リストについては、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-89.html>

Cisco Catalyst 9120 アクセス ポイント

Cisco Catalyst 9120 アクセス ポイントは、場所を問わず、Wi-Fi 6 (802.11 ax) 標準を超えるシームレスなワイヤレス エクスペリエンスを実現します。アクセス ポイントは、統合型のセキュリティ、復元力、運用の柔軟性を提供し、さらにネットワーク インテリジェンスを向上させます。

あらゆる規模のシスコのインテントベースネットワークで、Catalyst 9120 APは、IoTデバイスの高まる需要に応えつつ、最新のイノベーションや革新的な技術のすべてをカバーしています。

Cisco Catalyst 9120 AP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/products/collateral/wireless/catalyst-9120ax-series-access-points/datasheet-c78-742115.html>

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>	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。
早期展開 (ED)	<p>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。</p> <p>これらのリリースは短寿命リリースです。</p>	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: Cisco Wireless リリース 8.9.110.0 へのアップグレードパス

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 8.9.111.0
8.6.x	リリース 8.9.111.0 に直接アップグレードできます。

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 8.9.111.0
8.7.x	リリース 8.9.111.0 に直接アップグレードできます。
8.8.x	リリース 8.9.111.0 に直接アップグレードできます。

Cisco ワイヤレス リリースのアップグレード

ここでは、Cisco Wireless 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

- 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。
- Cisco 9100 AP で **show tech-support** コマンドを実行して、表示された結果が空である場合は、回避策として、同じアクセス ポイントからログアウトし、SSH を使用して同じアクセス ポイントに再ログインし、コマンドを実行します。詳細については、[CSCvo28881](#) を参照してください。
- 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 から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、アップグレード後にこの機能の設定は破損します。詳細については、[CSCve41740](#) を参照してください。
- 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で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。
- リリース 8.9 から以前のリリースにダウングレードする場合は、ローカル ポリシー ID が 255 を超えている、ローカル ポリシーから WLAN ID へのマッピングは、ダウングレード

後に失われます。必要に応じて、255 を超える ID を持つローカル ポリシーが使用されないように、ポリシー マッピングを変更できます。

ローカル ポリシー ID を確認するには、次のいずれかの方法を使用します。

- CLI : **show policy summary** コマンドを入力します。
 - GUI : **[Security] > [Local Policies]** に移動します。[Policy List] ページで、ポリシー ID がポリシー名とともに表示されます。
-
- 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 サーバが使用できることを確認します。サーバ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 サーバには、`tftpd32` や Cisco Prime Infrastructure 内の TFTP サーバがあります。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 サーバまたは FTP サーバ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なります。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イネーブルにします。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 の両方の使用をイネーブルにします。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 を有効化または無効化
- 証明書に關係する機能の有効化 (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の上昇
- HA の有効化
- SSL 証明書のインストール
- データベース サイズの設定
- ベンダーデバイス証明書のインストール
- CA 証明書のダウンロード
- 設定ファイルのアップロード
- Web 認証証明書のインストール
- 管理インターフェイスまたは仮想インターフェイスの変更

Cisco Wireless 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。
- 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。
 - コントローラ モデルを検索します。
 - [Wireless LAN Controller Software] をクリックします。
 - 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。

- e) ファイル名 `<filename.aes>` をクリックします。
- f) [Download] をクリックします。
- g) シスコのエンドユーザ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。
- h) お使いのハード ドライブにファイルを保存します。
- i) ステップ *a* から *k* 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、または SFTP サーバのデフォルト 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]、または [SFTP] を選択します。

ステップ 8 [IP Address] フィールドに、TFTP、FTP、または SFTP サーバの IP アドレスを入力します。

ステップ 9 TFTP サーバを使用している場合は、[Maximum Retries] フィールドの 10 回の再試行、および [Timeout] テキスト フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてこれらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を [Maximum Retries] フィールドに、ソフトウェアのダウンロードを試行する時間の合計 (秒単位) を [Timeout] フィールドに入力します。

ステップ 10 [File Path] フィールドに、ソフトウェアのディレクトリ パスを入力します。

ステップ 11 [File Name] フィールドに、ソフトウェア ファイルの名前 `<filename.aes>` を入力します。

ステップ 12 FTP サーバを使用している場合は、次の手順に従います。

- a) [Server Login Username] フィールドに、FTP サーバにログインするためのユーザ名を入力します。
- b) [Server Login Password] フィールドに、FTP サーバにログインするためのパスワードを入力します。
- c) [Server Port Number] フィールドに、FTP サーバ上のダウンロードが行われるポート番号を入力します。デフォルト値は 21 です。

ステップ 13 [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 14 ダウンロードの完了後、[Reboot] をクリックします。
- ステップ 15 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 16 [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 17 802.11 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 18 (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 3.0(4d) 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。

CIMC 3.0(4d) 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	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	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0%25284d%2529
Cisco 8540 ワイヤレス コントローラ	https://software.cisco.com/download/home/286281356/type/283850974/release/3.0%25284d%2529

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

[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

表 4: リリース 3.0(4d) で未解決の不具合

警告 ID	説明
CSCvj80941	CIMC を 3.04d にアップグレードした後、電源をリセットした後のみ UCS ベースのコントローラが起動する。
CSCvj80915	コントローラから設定されたユーザ名とパスワードを使用して CIMC GUI にログインできない。

表 5: リリース 3.0(4d) で解決済みの不具合

警告 ID	説明
CSCvd86049	<p>症状: システム イベント ログ (SEL) で PROCHOT、MEMHOT、および DMI タイムアウト関連イベントが報告されている場合、OS の動作中にシステムが稼働を停止したり、再起動したりする。</p> <p>条件: C220-M4 または C240-M4</p> <p>回避策: 回避策はありません。</p> <p>このバグ修正によって、ASPM (アクティブ電源状態管理) のデフォルトの BIOS オプションが「L1 only」から「Disabled」に変更され、ASPM 設定を変更できなくなります。この変更は、システムの安定性を向上させ、一部のシステムクラッシュシナリオを解消するために行われました。</p>

警告 ID	説明
CSCvf78458	<p>症状：システム イベント ログ (SEL) で PROCHOT、MEMHOT、および DMI タイムアウト 関連イベントが報告されている場合、OS の動作中にシステムが稼働を停止したり、再起動したりする。</p> <p>条件：C220-M4 または C240-M4</p> <p>回避策：回避策はありません。</p> <p>このバグ修正により、BIOS オプションの「Package C-State limit」のデフォルト値が C6 Retention から C0/C1 に変更され、システムの安定性が向上し、一部のクラッシュ シナリオが解消されます。</p> <p>アップグレードが完了したら、BIOS 設定をデフォルトにリセットするか、「Package C-State limit」を手動で C0/C1 に変更します。</p>

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 6: 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	8.9. x
Cisco ワイヤレス コントローラ	Cisco 5520 ワイヤレス コントローラ
アクセス ポイント	C9115AXE-B、C9117AXI-B、C9120AXI
無線機	802.11ax (2.4 GHz または 5 GHz)、802.11ac、802.11a、802.11g、802.11n (2.4 GHz または 5 GHz)
セキュリティ	Open、PSK (WPA-TKIP-WPA2-AES)、802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST)
RADIUS	Cisco ACS 5.3、Cisco ISE 2.2、Cisco ISE 2.3

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
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、プリンタなどが含まれます。

表 7: 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
ラップトップ	
ACER Aspire E 15	Windows 8.1
Acer Aspire E 15 E5-573-3870	Windows 10 Pro
Apple Macbook Air	OS Sierra v10.12.2
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 11 inch mid 2013	OS Sierra 10.12.3
Apple Macbook Air 11 inch Mid 2013	OS X Yosemite 10.10.5
Apple Macbook Air 13inch (mid 2011)	OS Sierra 10.12.4
Apple Macbook Pro OS X v10.8.5 mid 2009	OS X 10.8.5
Apple Macbook Pro Retina 13 inch early 2015	OS Sierra 10.12.6
Apple Macbook Pro Retina 13 inch late 2013	OS Sierra 10.12.4
DELL Inspiron 13-5368 Signature Edi	Win 10 Home 18.40.0.12
DELL Inspiron 15-7569	Windows 10 Home 18.32.0.5
DELL Latitude 3480	Win 10 Pro 12.0.0.307
DELL Latitude E5430	Windows 7 Professional 15.1.1.1
DELL Latitude E5430	Windows 7 Professional 15.17.0.1
DELL Latitude E6430 Dekra TB	Windows 7 Professional 6.30.223.60
DELL latitude E6840	Windows 7 Professional 6.30.223.215
DELL Latitude E7450	Windows 7 Professional 6.30.223.245
DELL Latitude Intel Centino N 6205	Win 8.1 Pro 15.18.0.1
DELL XPS 12 9250	Windows 10 Home 18.40.0.9
DELL XPS 12 v9250	Windows 10 19.50.1.6
FUJITSU Lifebook E556 Intel 8260	Windows 10 Pro 19.20.0.6
HP Chromebook Chrome OS	Chrome OS 55.028883.103
Lenovo Thinkpad Yoga 460	Windows 10 Pro 20.20.2.2

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
(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	
Amazon Kindle	Ver 6.2.2
Apple iPad 2 MC979LL/A	iOS 9.3.1
Apple iPad Air 2 MGLW2LL/A	iOS 11.4.1
Apple iPad Air 2 MGLW2LL/A	iOS 10.2.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad MD78LL/A	iOS 11.4.1
Apple iPad MGL12LL/A	iOS 9.1
Apple iPad mini 2 ME279LL/A	iOS 11.4.1
Apple iPad mini 2 ME279LL/A	iOS 12.0
Apple iPad mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad MK6L2LL/A	iOS 10.2
ET50PE エンタープライズ タブレット	Ver 5.1.1
Google Nexus 9 タブレット	Android 6.0.1
Motorola ET1 エンタープライズ タブレット	Android バージョン : 2.3.4
Samsung Galaxy Tab A SM T350	Android 5.0.2
Samsung Galaxy Tab GT N5110	Android 4.4.2
Samsung Galaxy Tab SM-P 350	Android 6.0.1
Samsung Galaxy TAB SM-P600	Android 4.4.2
Samsung Tab Pro	Samsung Android 4.4.2
Samsung Tab Pro SM-T320	Android 4.4.2
Samsung Tab SM-T520	Android 4.4.2
Toshiba TAB AT100	Android 4.0.4
Mobile Phones	
Apple iPhone 5	iOS 10.3.12
Apple iPhone 5c	iOS 10.3.3
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8 plus	iOS 12.0.1

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 8 Plus MQ8D2LL/A	iOS 12.0.1
Apple iPhone MD237LL/A	iOS 9.3.5
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone X MQA52LL/A	iOS 12
ASCOM Myco2	ビルド 2.1、Android バージョン 4.4.2
ASCOM Myco2	ビルド 4.5、Android バージョン 4.4.2
ASCOM Myco2	プラットフォーム バージョン 10.1.0
ASUS Nexus 7	Android 6.0
AT100	Android 4.0.4
Cisco CP 7925G-EX	1.4.8.4
Cisco CP 7926G	1.4.8.4
Cisco CP 7926G	1.4.5.3
Cisco CP 8821	rootfs8821.11-0-3ES2-1
Google Pixel	Android 8.1.0
HTC One 6.0	Android 5.0.2
HTC PI39100	Android 7.5
Huawei MATE9 Pro LON-L29	Android 7.0
Huawei MediaPad X1 7.0	Android 4.4.2
Huawei P7-L10	Android 4.4.2
LG D855	Android 5.0
Motorola ET1 エンタープライズ タブレット	Android 2.3.4
Motorola ET50PE エンタープライズ タブレット	Android 5.1.1
Motorola MC75A	OEM バージョン 02.37.0001
Motorola MC9090	Windows Mobile 6.1
Motorola MC9090G	OEM バージョン 1.35
Moto X (第 2 世代)	Android 5.0
Nokia Lumia 1520 0268	Windows 10
Nokia Lumia 925.5	Windows 8.1
One Plus One	Android 4.3
Samsung Galaxy Mega GT-i9200	Android 4.4
Samsung Galaxy Note 3 - SM-N9005	Android 5.0

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
Samsung Galaxy Note4 edge	Android 6.0.1
Samsung Galaxy S10.P.1.4	Android 9
Samsung Galaxy S4	Android 4.2.2
Samsung Galaxy S4	Android 4.2.2
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 GT 19500	Android 5.0.1
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S6	Android 6.0.1
Samsung Galaxy S7	Android 6.0.1
Samsung Galaxy S8	Android 7.0
Samsung S7 SM-G930F	Android 7.0
Samsung SM-P600	Android 4.4.2
Samsung SM-T520	Android 4.4.2
Spectralink 8440	Android 5.0.0.1079
Spectralink 8742	Android 5.1.1
Spectralink 8742	Android 5.1.1
Spectralink 8744	Android 5.1.1
Spectralink 9553	Android 8.10.0
Symbol MC40	Android バージョン 4.4.4
Symbol MC40N0 EZ	Android バージョン : 4.1.1
Symbol MC55A	Windows 6.5
Symbol MC 7090	OEM バージョン 03.33.0000
Symbol MC92N0	Android バージョン 4.4.4
TC510K	Android 6.0.1
TC8000	Android 4.4.3
Zebra TC510K	Android バージョン : 6.0.1
Zebra TC520K	Android バージョン : 8.1.0
Zebra TC57	Android バージョン : 8.1.0
Zebra TC700H	Android バージョン : 4.4.3
Zebra TC75	Android バージョン : 4.4.3
Zebra TC8000	Android バージョン : 4.4.3

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
Zebra TC8000	Android バージョン : 5.1.1
Zebra WT6000	Android バージョン 5.1.1
Drager M300	
Drager Delta	
プリンタ	
Zebra QLn320 プリンタ	バージョン : V 68.20.15ZP41800
Zebra ZQ620 プリンタ	V 85.20.15

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、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
- 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
- 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機能を示します。

Cisco Catalyst 9120 AP でサポートされていない主要機能

表 8: Cisco Catalyst 9120 シリーズ 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"> • ダウンリンク 高効率 MU-MIMO • アップリンク MU-MIMO • ダウンリンク OFDMA • アップリンク OFDMA • BSS カラーリング • ワークグループブリッジ (WGB) モード • メッシュ モード • Mobility Express • Web セキュリティ アプライアンス (WSA) センサー • ターゲット起動時間 (TWT)
-------	---

Cisco Catalyst 9117 AP でサポートされていない主要機能

表 9: Cisco Catalyst 9117 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"> • ダウンリンク 高効率 MU-MIMO • アップリンク MU-MIMO • ダウンリンク OFDMA • アップリンク OFDMA • BSS カラーリング • Mobility Express • ターゲット起動時間 (TWT)
-------	---

Cisco Catalyst 9115 AP でサポートされていない主要機能

表 10: Cisco Catalyst 9115 シリーズ 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"> • ダウンリンク 高効率 MU-MIMO • アップリンク MU-MIMO • ダウンリンク OFDMA • アップリンク OFDMA • BSS カラーリング • Mobility Express • RF チャネル幅 80+80 MHz
-------	--

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

Cisco Aironet Wave 2 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/controller/technotes/8-7/b_feature_matrix_for_802_11ac_wave2_access_points.html。

表 11: 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"> • 自律ブリッジおよびワークグループブリッジ (WGB) モード • メッシュ モード • NAT または PAT 環境の背後にある LAG
プロトコル	<ul style="list-style-type: none"> • 完全な Cisco Compatible Extensions (CCX) のサポート • Rogue Location Discovery Protocol (RLDP) • Telnet

セキュリティ	<ul style="list-style-type: none"> • ダイナミック WEP を使用した CKIP、CMIC、LEAP • CKIP の静的 WEP • WPA2 + TKIP <p>(注) WPA + TKIP および TKIP + AES プロトコルがサポートされません。</p>
QoS	Cisco Air Time Fairness (ATF)
FlexConnect の機能	<ul style="list-style-type: none"> • Split Tunneling • PPPoE • マルチキャストからユニキャストへ (MC2UC) <p>(注) VideoStream がサポートされません。</p> <ul style="list-style-type: none"> • Traffic Specification (TSpec) <ul style="list-style-type: none"> • Cisco Compatible Extension (CCX) • コールアドミッション制御 (CAC) • VSA/レルム照合認証 • 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



(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 12: 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 13: 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 ディスカバリ要求タイマー)
- 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
- Static WEP

注意事項

未解決の不具合

表 14: 未解決の警告

警告 ID 番号	説明
CSCvb70551	Cisco Wave 2 AP がカーネルパニックにより再起動し、非同期になる：メモリ不足
CSCvj48316	AP3700：プロセス「QoS stats process」により、予期しないリロードが発生する
CSCvj61869	WPA2+802.1x SSID を使用する 702w AP での 20 ～ 30 Mbps ダウンリンク速度
CSCvm63975	特定の国が同時に有効になっている場合、Cisco コントローラの設定が失われる
CSCvm65411	FC71 コードを使用した Cisco 2700 AP 無線のリセット
CSCvm68341	Cisco コントローラは、重複する中間アカウントングパケットを ISE に送信する
CSCvm81901	Cisco 3800 AP がクライアントフレームを認識しない
CSCvm93785	[Client update cache from write handler] をクリックすると、Cisco 2800、3800 AP が予期せずリロードする
CSCvn03560	Cisco 702 AP で復号化エラーが発生する
CSCvn15777	Cisco 5508 コントローラは、emWeb プロセスで CPU 使用率が高いと予期せずリロードする
CSCvn17267	702AP：WGB が「parent lost: Too many retries」でルート AP から接続を解除、AP がオフチャネルの場合に RTS
CSCvn27144	802.11ac MCS パラメータを復元できない
CSCvn37957	アソシエーション応答 FT 802.11r を送信している Cisco コントローラの FTIE が保存されていない
CSCvn56211	Cisco 702W AP 無線のリセット、トレースバック、およびその他の無線バッファエラー
CSCvn62176	Cisco 3802 シリーズ AP は、UNII-1 チャンネルを使用している場合にクライアントを関連付けることができない

警告 ID 番号	説明
CSCvn69015	ローカルモードの Cisco Wave 2 AP は、有線インターフェイスからレイヤ 2 マルチキャスト制御トラフィックを転送する
CSCvn99809	AID 調査中に PAK スケジューラが処理される
CSCvo28881	AP9115、9117 : show tech-support は空で、セクション見出しのみ示される
CSCvo50532	Cisco 1572 AP で「nokey」エラーが報告される
CSCvo55603	Cisco 4800 シリーズ アクセス ポイントは、Cisco 94xx スイッチに接続されている場合 UPoE 電力を要求しない
CSCvo71753	AP 側 : CTS でインラインタギングを有効にすると、マルチキャストトラフィックが機能しなくなる
CSCvo74306	Cisco 1815W AP : ユーザごとの BW 契約が Web ポリシーで機能しない
CSCvo87937	ATF + MU-MIMO を使用した 2800/3800/4800/1560 AP での「FW クラッシュ」リロード
CSCvp00688	EFT <TUD> : Cisco 2800、3800 AP 無線が予期せずリロードする
CSCvp03798	Wave1 AP : メモリ フラグメンテーション「Net Background」により、FlexConnect のローカル EoGRE が予期せずリロードする
CSCvp11765	ワイヤレスクライアントは、再起動するまで、Cisco 1830 AP にアソシエートできない
CSCvp18422	8.5.135.0 を実行している Cisco コントローラは、taskname spamApTask6 で予期せずリロードする
CSCvp21915	アソシエーションと EAPOL-M2 フレーム間の RSN IE の長さが一致しない
CSCvp58062	ビーコン スタック FW のハングによる Cisco 1815 AP の無線コア ダンプ
CSCvp88088	AP9117 : FW クラッシュ @whal_recv_recovery.c:834 (RX_BACKPRESSURE_MONITOR_BUF_EMPTY) (SF 04035754)

解決済みの不具合 (p.11)

表 15: 解決済みの不具合 (p.11)

警告 ID 番号	説明
CSCvj69298	RPE/ダブルビットエラーが原因でデータプレーンが予期せずリロードする
CSCvk70379	8.5_Cisco コントローラに古いクライアントが存在する

警告 ID 番号	説明
CSCvk79765	apstatEngineMsgQ MSGQ_RUNNING_HIGH または MSGQ_SEND_FAILED キュー使用率の問題
CSCvm65360	外部 Web 認証ログインが成功した後、Cisco コントローラは内部 Web 認証ログインページにリダイレクトされる
CSCvm90337	「無線障害（無線の復旧に失敗）」が原因で Cisco 18xx AP が予期せずリロードされる
CSCvm91854	systemDb の破損によって Cisco 8540 コントローラがアクセス不能になる
CSCvn74948	ウォッチドック プロセス sxpd で Cisco AP が予期せずリロードする
CSCvn87656	QCA ドライバ @ click_packet_type_event_hook のコンテキストで Cisco Wave 2 AP が予期せずリロードする
CSCvn98214	Cisco 1830 AP : WGB アソシエーション中に WGB が参加していない core-radio1FW が検出される
CSCvn98598	FT 802.1X クライアントは、ME マスター AP/N+1 コントローラのフェールオーバー後に認証できない
CSCvo26556	コマンド「config network ssh host-key use-device-certificate-key」で WLC が予期せずリロードする
CSCvo28124	一部のシナリオでは、ローカル スイッチング WLAN が中央スイッチングに変更される
CSCvo48363	GUI でマルチキャストの MGID を表示すると、Cisco コントローラが予期せずリロードする
CSCvo48759	AP は理由コード 7（アソシエートされていない STA からクラス 3 フレームを受信）でアソシエートされたクライアントの認証を解除する
CSCvo90764	AP4800 : 複数の場所で AP の定期的な予期しないリロードが検出される
CSCvo98569	Cisco Wave 1 AP : EoGRE アップストリーム/ダウンストリーム パケットのドロップが flex ローカル EoGRE で確認される
CSCvp07442	Cisco コントローラがタスク「tplusTransportThread」で予期せずリロードする
CSCvp07829	4800 AP の CDP 状態を切り替えると、AP がオフになり、スイッチに Ieee PD と表示される
CSCvp26465	AireOS HA : モビリティ ハッシュ キーが AireOS で同期されない

警告 ID 番号	説明
CSCvp36496	AP がリロードしてコントローラに再参加した後に、ビームフォーミング設定がデフォルトに戻る
CSCvp41629	スロット 0 が 5 GHz に切り替わった後、802.11bg の規制ドメインが -A に変更される
CSCvp52994	WLC が AAA VLAN の学習に失敗し、2 回目の Add Mobile で Central Switched VLAN を送信できない
CSCvp57188	Cisco 4800 AP では、8.8.X.X コードの kmalloc-512 および 1024 kmalloc でメモリリークが発生する

関連資料

ワイヤレス製品の比較

- 次のツールを使用して、Cisco 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

- 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 モビリティ サービス エンジン

[Cisco モビリティ サービス エンジン マニュアル](#)

Cisco Connected Mobile Experiences

[Cisco Connected Mobile Experiences マニュアル](#)

マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『[What's New in Cisco Product Documentation](#)』を参照してください。

新しく作成された、または改訂されたシスコのテクニカルコンテンツをお手元で直接受け取るには、『[What's New in Cisco Product Documentation](#)』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

【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: [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)

© 2019 Cisco Systems, Inc. All rights reserved.