



Control and Provisioning of Wireless Access Points

- 概要 (1 ページ)
- 屋内展開の設定 (5 ページ)
- 6G 標準出力モードの AFC サポート (11 ページ)
- AP の AFC ステータスの確認 (12 ページ)
- GNSS のサポート (12 ページ)
- アンテナ切断検知について (13 ページ)
- トラブルシューティング (14 ページ)

概要

CAPWAP は、ワイヤレス LAN コントローラが複数の AP とワイヤレス LAN コントローラ (WLC) を管理し、セキュア通信トンネルを介してコントロールプレーンとデータプレーン情報を交換できるようにする IEEE 標準規格プロトコルです。

CAPWAP はレイヤ 3 でのみ動作し、AP と WLC の両方で IP アドレスの提示を必要とします。CAPWAP は、UDP ポート 5246 および 5247 で、それぞれ IPv4 および IPv6 用のトンネルを確立します。Datagram Transport Layer Security (DTLS) 暗号化により、一層セキュリティが強化されます。

DTLS は、AP と WLC 間のセキュリティを担保するプロトコルとして機能し、通信の暗号化を促進することで中間者攻撃による盗聴や改ざんを防ぎます。

デフォルトでは、DTLS は CAPWAP の制御チャンネルを保護し、AP と WLC 間のすべての CAPWAP 管理トラフィックおよび制御トラフィックを暗号化します。

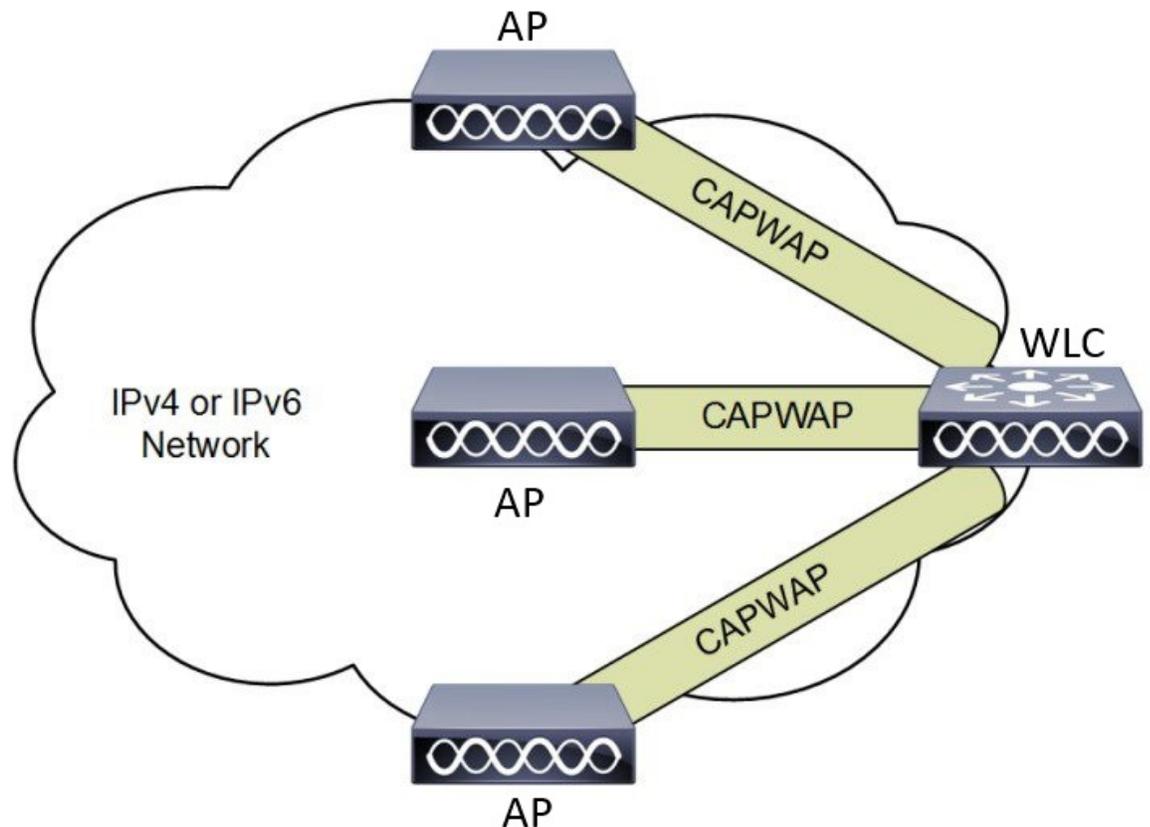
データチャンネルはデフォルトでは無効であり、AP と WLC 間を移動するクライアントデータは暗号化されません。CAPWAP データ暗号化を有効にするかどうかは任意であり、AP でアクティブ化する前に WLC に DTLS ライセンスをインストールする必要があります。

AP が DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンのみ有効となり、データプレーンの DTLS セッションは確立されません。

AP がデータ DTLS をサポートしている場合は、コントローラから新しい設定を受信した後にデータ DTLS を有効にします。AP は、ポート 5247 で DTLS ハンドシェイクを実行し、ハンドシェイクが成功すると DTLS セッションを確立します。すべてのデータトラフィック（AP からコントローラ、およびコントローラから AP）が暗号化されます。

CAPWAP によって、管理者はワイヤレスネットワーク全体を中央で一元的に管理できます。IW9165E は、コントローラとネットワーク上の他の AP 間の通信に Internet Engineering Task Force (IETF) 標準規格の CAPWAP を使用します。

図 1: WLC に接続された CAPWAP AP



Lightweight アクセス ポイントでの証明書プロビジョニング

LAP で新しい証明書をプロビジョニングするには、CAPWAP モードの間に LAP が新しい署名付き X.509 証明書を取得できる必要があります。そのために、LAP はコントローラに certRequest を送信します。コントローラは CA プロキシとして機能し、CA により署名された LAP 用 certRequest の取得を支援します。

certReq および certResponse は LWAPP ペイロードを使用して LAP に送信されます。

LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動的に再起動します。システムは、次回起動時には LSC を使用するように設定されているため、AP は join 要求の一部として LSC デバイス証明書をコントローラに送信します。join 応答の一部として、コントローラは新しいデバイス証明書を送信し、新しい CA ルート証明書を使用して受信 LAP 証明書も検証します。

次の作業

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニング機能を使用する必要があります。

AP の CAPWAP 接続について

CAPWAP を有効にすると、最初の機能として、ディスカバリフェーズが開始されます。ワイヤレス AP は、ディスカバリ要求メッセージを送信してコントローラを検索します。ディスカバリ要求を受信すると、コントローラはディスカバリ応答を返します。この時点で、この2台のデバイスの間に、CAPWAP 制御メッセージとデータメッセージを交換するための Datagram Transport Layer Security (DTLS) プロトコルを使ったセキュアな接続が確立されます。

AP は CAPWAP ディスカバリメカニズムを使用して、コントローラに CAPWAP 接続要求を送信します。コントローラは AP に CAPWAP 接続応答を送信し、AP がコントローラに接続できるようにします。AP がワイヤレスコントローラに接続すると、ワイヤレスコントローラによって AP の構成、ファームウェア、制御トランザクション、およびデータトランザクションが管理されます。

CAPWAP には、制御とデータの2つのチャンネルがあります。AP は制御チャンネルを使用して、設定メッセージの送信、イメージとクライアント鍵のダウンロード、またはコンテキストの受信を行います。現在の実装では、制御チャンネルには単一のウィンドウが設けられます。AP は、コントローラから送信されたすべてのメッセージを単一のウィンドウ内で確認する必要があります。AP は、前の制御パケットの確認応答が終わるまで、次の制御パケットを送信しません。

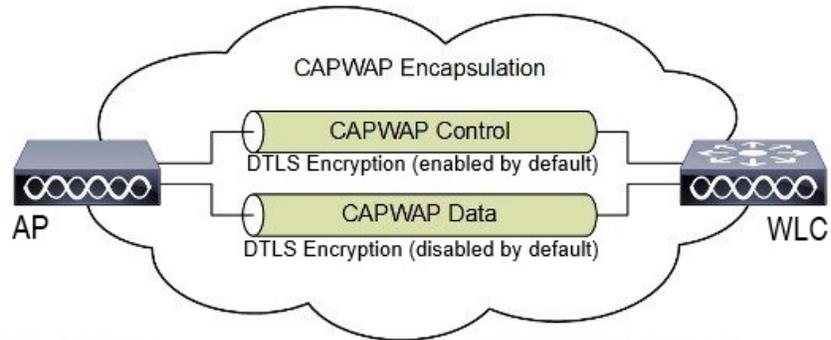
CAPWAP データチャンネルは、AP と WLC 間のユーザーデータトラフィックのカプセル化とトンネリングを担います。これにより、ユーザーデータフローの中央管理が可能になり、WLC はポリシーを適用し、Quality of Service (QoS) を適用し、ワイヤレスネットワーク全体で一貫したセキュリティ対策を確保できます。ユーザーデータは CAPWAP フレーム内でカプセル化され、AP と WLC 間で転送できるようになります。

IETF に従い、CAPWAP は2つの動作モードをサポートしています。

- **Split Media Access Control (MAC)** : CAPWAP の主要なコンポーネントの1つに、スプリット MAC という概念があります。これは、802.11 プロトコルでの動作の一部を CAPWAP AP が管理し、残りの部分を WLC が管理するというものです。

スプリット MAC モードでは、CAPWAP プロトコルがすべてのレイヤ2 ワイヤレスデータおよび管理フレームをカプセル化し、これらのデータやフレームが WLC と AP 間で交換されます。

図 2: スプリット MAC アーキテクチャ

Access Point MAC Functions:

- 802.11: Beacons, Probe Responses.
- 802.11 Control: Packet Acknowledgements and Transmission.
- 802.11e: Frame Queuing and Packet Prioritization.
- 802.11i: MAC Layer Data Encryption and Decryption.

Controller MAC Functions:

- 802.11 MAC: Management: Association Requests and Actions.
- 802.11e: Resource Reservation.
- 802.11i: Authentication and Key Management.

- **Local MAC** : ローカル MAC モードでは、データフレームをイーサネットフレームとしてローカルにブリッジまたはトンネリングできます。

ローカル MAC では、すべてのワイヤレス MAC 機能が AP で実行されます。管理フレームおよび制御フレームの処理を含む完全な 802.11 MAC 機能が AP に常駐します。

どちらのモードでも、AP はレイヤ 2 ワイヤレス管理フレームをローカルで処理してから、コントローラに転送します。

リセットボタンの設定

IW9165E では、(ブートローダがリセット信号を受信した後に) LED が赤色の点滅になると、次のリセットアクションが実行されます。デバイスの電源を入れる前に、必ずデバイスのリセットボタンを押します。

- 完全にリセットするには、ボタンを長押し (20 秒未満) します。
- 工場出荷時の状態まで完全にリセットする (FIPS フラグをクリアする) には、ボタンを長押し (20 秒以上 60 秒未満) します。

CAPWAP モードでのイーサネットポートの使用状況

Catalyst IW9165E では、2 つの 2x2 Multiple Input and Multiple Output (MIMO) と 2 つのイーサネットポート (2.5G mGig および 1G) により、最大 3.6 Gbps の物理データレートがサポートされています。

Catalyst IW9165E には、以下の内部ポートマッピングルールがあります。

- Wired0 : 802.3af、802.3at、802.3bt PoE をサポートする 1 つの mGig (2.5 Gbps) イーサネットポート。



(注) AP のローカルモードや FlexConnect モードでは、wired0 ポートは CAPWAP アップリンクポートとして使用されます。

- Wired1 : 1Gig イーサネット LAN ポート。



(注) 17.14.1 リリース以降、RLAN 機能は wired1 ポートではサポートされません。

屋内展開の設定

IW9165E は、規制ドメイン -B (米国)、-E (EU)、-A (カナダ)、-Z (オーストラリア、ニュージーランド) の屋内および屋外展開をサポートします。

デフォルトでは、AP の展開モードは屋内です。

-B ドメインでは屋外と屋内の周波数は同じです。

表 1: 無線機の 6G 出力モードの対応表

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	対応



(注) 屋外モードは屋内で使用できますが、5150 ~ 5350 MHz のチャンネルは -E の国々では屋内のみであるため、屋内モードを屋外で使用することはできません。

ワイヤレスコントローラでの AP 展開モードの設定方法については、『[Cisco Catalyst 9800 シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド](#)』を参照してください。

このコマンドは、AP の再起動を発動します。再起動後に AP がワイヤレスコントローラに登録されたら、対応する国番号を AP に割り当てる必要があります。

屋内展開の確認

WLC で屋内展開が有効になっているかどうかを確認します。

`#show ap name <AP_Name> config general | inc Indoor` コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor
      AP Indoor Mode                               : Enabled
```

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します。

```
#show ap name <AP_Name> config general | inc Indoor
      AP Indoor Mode                               : Disabled
```

AP の屋内展開のステータスを確認するには、**show controllers Dot11Radio [1|2]** コマンドを実行します。

- 屋内モードが有効になっている場合、show コマンドは次の出力を提供します。

```
Device#show controllers Dot11Radio [1|2]
...
Radio Info Summary:
=====
Radio: 5.0GHz
Carrier Set: (-Ei) ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
```



(注) コマンド出力の「-Ei」は、屋内モードが有効になっていることを示します。

- 屋内モードが無効になっている場合、show コマンドは次の出力を提供します。

```
Device#show controllers Dot11Radio [1|2]
...
Radio Info Summary:
=====
Radio: 5.0GHz
Carrier Set: (-E) ( GB )
Base radio MAC: FC:58:9A:15:B7:C0
Supported Channels:
100 104 108 112 116 120 124 128 132 136 140
```



(注) コマンド出力の「-E」は、屋内モードが無効になっていることを示します。

CLI 出力には、サポートされるチャンネルも表示されます。

AP Radio Slot

Cisco Unified Industrial Wireless ソフトウェアリリース 17.14.1 以降、Cisco Catalyst IW9165E では、2x2 5GHz Wi-Fi 専用無線機と 5 GHz および 6 GHz のデュアルバンド (XOR) 2x2 無線機が使用できます。

Catalyst IW9165E には、5G バンドと 6G バンドを切り替えるオプションがあります。5G バンドと 6G バンドを切り替えるには、次の CLI コマンドを使用します。

```
ap name <ap-name> dot11 dual-band band 6ghz/5ghz
```



- (注) デフォルトでは、管理状態は無効です。
スロット 2 の XOR 無線機は 5G に固定されています。

表 2: AP Wi-Fi 無線機アーキテクチャモード

モード	5 GHz スロット 1	5/6 GHz スロット 2
5G + 5G	5GHz 2x2:2SS (20/40/80 MHz)	5G 2x2:2SS (20/40/80/160 MHz)
5G + 6G	5GHz 2x2:2SS (20/40/80 MHz)	6G 2x2:2SS (20/40/80/160 MHz)

固定ドメインと国コードのサポート

ROW 規制ドメインにより、特定のドメインがマッピングされていないすべての国コードの製造プロセスのドメイン管理が簡素化されます。この項では、Catalyst IW9165E アクセスポイントの固定ドメインと国コードのサポートについて説明します。

サポートされている固定ドメイン

ドメイン	国番号
A	CA (カナダ)
B	US (米国)

ドメイン	国番号
E	

ドメイン	国番号
	<ul style="list-style-type: none">• AT (オーストラリア)• AT (オーストラリア)• BE (ベルギー)• BG (ブルガリア)• HR (クロアチア)• CY (キプロス)• CZ (チェコ共和国)• DK (デンマーク)• EE (エストニア)• FI (フィンランド)• FR (フランス)• DE (ドイツ)• GR (ギリシャ)• HU (ハンガリー)• IS (アイスランド)• IE (アイルランド)• IT (イタリア)• LV (ラトビア)• LI (リヒテンシュタイン)• LT (リトアニア)• LU (ルクセンブルク)• MT (マルタ)• NL (オランダ)• NO (ノルウェー)• PL (ポーランド)• PT (ポルトガル)• RO (ルーマニア)• SK (スロバキア共和国)

ドメイン	国番号
	<ul style="list-style-type: none"> • SI (スロベニア) • ES (スペイン) • SE (スウェーデン) • CH (スイス)
F	ID (インドネシア)
Q	JP (日本)
Z	<ul style="list-style-type: none"> • AU (オーストラリア) • NZ (ニュージーランド)

Catalyst IW9165 でサポートされている国コード (ROW)

ドメイン	国番号
ROW	<ul style="list-style-type: none"> • CL (チリ) • KR (韓国) • GB (英国) • VN (ベトナム)

使用している AP の各国における認可状況については、お客様にご確認いただく必要があります。認可状況および特定の国に関連する規制ドメインの確認方法。詳細については、「[Cisco Product Approval Status](#)」[英語]を参照してください。

無線アンテナ配置の設定

Catalyst IW9165E は、RP-SMA (f) コネクタで 4 つの外部アンテナをサポートしています。無線機 1 はアンテナポート 1 および 2 に接続します。無線機 2 はアンテナポート 3 および 4 に接続します。

IW9165E は、6G バンドの Self Identifiable Antenna (SIA) アンテナとの互換性があります。アンテナポート 1 および 3 では、SIA アンテナをサポートできます。アンテナの詳細については、『[Cisco Catalyst IW9165E 高耐久性アクセスポイントおよびワイヤレスクライアントハードウェア設置ガイド](#)』を参照してください。



- (注) 初めて SIA アンテナを取り付けた後は、電源を一度切ってから再度オンにする必要があります。

SIA は、アンテナ IW-ANT-OMV-2567-N および IW-ANT-OMH-2567-N のみをサポートします。

表 3: アンテナ利得 (dBm)

5 GHz スロット 1	5 GHz スロット 2	6 GHz スロット 2
3 4 7 8 10 13 15	3 4 7 8 10 13 15	7

以下の項で、SIA テストを確認するための CLI コマンドについて説明します。

コントローラの SIA ステータスを確認するには、**show ap config slots <AP>** コマンドを実行します。

```
Device#show ap config slot ap_name
show ap config slots AP2CF8.9B1C.CE78
Cisco AP Name : AP4C42.1E51.A144
Attributes for Slot 2
SIA Status      : Present (RPTNC)
SIA Product ID  : IW-ANT-OMV-2567-N
```

6G 標準出力モードの AFC サポート

Cisco Catalyst IW9165E は、自動周波数調整 (AFC) 6 GHz 標準出力モードをサポートします。標準出力 AP がシステムに接続されます。標準出力を有効にする前に、AP は AFC システムから使用可能な周波数と各周波数範囲の出力を取得する必要があります。

AFC システムは、規制機関 (米国の場合は FCC) から提供される情報に基づいて、使用可能な周波数と最大許容出力を計算します。応答がコントローラに返送され、AFC システムから返された許可チャンネルリストに基づいて標準出力チャンネルが AP に割り当てられます。

標準出力 AP は、AFC サービスを通じて調整を行います。AFC は情報にアクセスし、AP の地理位置情報とアンテナの特性に加え、AP の干渉半径をモデル化したトポグラフィック伝達マップを作成します。このマップを使用することで、最大送信電力を割り当て、チャンネル設定を調整または設定して干渉を回避できます。

表 4: 無線機の 6 GHz 出力モードの対応

AP 展開モード	6G 展開モード	屋内低出力への対応	標準出力への対応
屋内 AP	屋外	非対応	対応

送信電力の実効等方放射電力 (EIRP) は最大 36 dB に制限され、AFC サービスを通じて AP を調整する必要があります。これらの AP は、-B (米国) ドメインでは、UNII-5 (5.925 ~ 6.425 GHz) および UNII-7 (6.525 ~ 7.125 GHz) での運用が許可されます。

表 5: 6 GHz 目標出力

経路ごとの導体出力		アンテナ利得	Tx x Rx チェーン	最大 EIRP	最大 EIRP (SP/AFC)
20 ~ 80Mhz	160Mhz				
17 dBm	17 dBm	7 dBi*	2 X 2	27 dBm*	36 dBm

AP の AFC ステータスの確認

AP の AFC 要求および応答データを確認するには、**show rrm afc** コマンドを実行します。

```
Device#show rrm afc
Location Type: 1
Deployment Type: 2
Height: 129
Uncertainty: 5
Height Type: 0
Request Status: 5
Request Status Timestamp: 2023-08-31T06:20:17Z
Request Id Sent: 5546388983266789933
Ellipse 1: longitude: -121.935066 latitude: 37.512830 major axis: 43 minor axis:
  9 orientation: 36.818100
AFC Response Request ID: 5546388983266789933
AFC Response Ruleset ID: US_47_CFR_PART_15_SUBPART_E
```

現在稼働中の出力モードを確認するには、**show controllers dot11Radio 2 | i Radio** コマンドを実行します。

```
Device#show controllers dot11Radio 2 | i Radio
Dot11Radio2      Link encap:Ethernet  HWaddr 24:16:1B:F8:06:C0
Radio Info Summary:
Radio: 6.0GHz (SP)
```

GNSS のサポート

IW9165E では、全地球航法衛星システム (GNSS) がサポートされます。AP は、屋外環境に展開されたデバイスの GPS 情報を追跡し、ワイヤレスコントローラに GNSS 情報を送信します。

AP の GNSS 情報を表示するには、次のコマンドを使用します。

```
ap# show gnss info
```

AP の GPS 位置情報を表示するには、次のコマンドを使用します。

```
controller# show ap geolocation summary
controller# show ap name <Cisco AP> geolocation detail
```

アンテナ切断検知について

アクセスポイント（AP）の送信機と受信機に複数のアンテナがあると、性能と信頼性が向上します。複数のアンテナによって、受信機側でより強い信号を選択するか、個々の信号を組み合わせて受信状態が改善します。したがって、障害のあるアンテナやアンテナの物理的な破損を検出することは、APの信頼性を確保する上で重要です。

アンテナの切断検知機能は、受信機のアンテナ間における信号強度の差分に基づきます。この差分が一定期間に定義された制限を超えると、そのアンテナは問題があると見なされます。

設定した検知期間ごとに、APはアンテナの状態を伝える Inter-Access Point Protocol（IAPP）メッセージを送信します。このメッセージは、問題が検知された場合に一度だけ送信され、コントローラトラップメッセージ、SNMPトラップ、およびコントローラデバッグログに表示されます。

設定ワークフロー

1. APを設定します。
2. APプロファイルを設定します。
3. APプロファイルで機能を有効にします。
4. 機能のパラメータを設定します。
5. 設定を確認します。

ワイヤレスコントローラでのアンテナ切断検知の設定方法について詳しくは、『[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)』を参照してください。

アンテナ切断検知の確認

APのアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Controller#sh ap name AP4C42.1E51.A144 config general

Cisco AP Name      : AP4C42.1E51.A144
=====

Cisco AP Identifier      : 8c84.4292.f840
Country Code            : Multiple Countries :
US,CN,GB,HK,DE,IN,CZ,NZ
Regulatory Domain Allowed by Country : 802.11bg:-ACE^ 802.11a:-ABCDEHNSZ^
802.11 6GHz:-BEZ^
Radio Authority IDs     : None
AP Country Code         : CZ - Czech Republic
AP Regulatory Domain
802.11bg                : -E
802.11a                  : -E
MAC Address              : 8c84.4292.f840
IP Address Configuration : DHCP
IP Address               : 9.9.33.3
IP Netmask               : 255.255.255.0
```

```

Gateway IP Address           : 9.9.33.1
Fallback IP Address Being Used :
Domain                       :
Name Server                  :
CAPWAP Path MTU              : 1485
Capwap Active Window Size    : 1

```

APプロファイルのアンテナ切断検知機能の設定を確認するには、次のコマンドを使用します。

```
9800-Controller#show ap profile name ap-profile detailed
```

```

AP Profile Name: ap-profile
.
.
.
AP broken antenna detection:
  Status           : ENABLED
  RSSI threshold   : 40
  Weak RSSI        : -80
  Detection Time   : 120

```

トラブルシューティング

このドキュメントでは、アクセスポイント（AP）とワイヤレスコントローラ間の Control And Provisioning of Wireless Access Points（CAPWAP）/Lightweight Access Point Protocol（LWAPP）トンネルが切断される理由を理解するためのユースケースを紹介します。詳細については、「[コントローラからのアクセスポイントの関連付け解除のトラブルシューティング](#)」を参照してください。



(注) ソフトウェアまたはハードウェアの変更により、コマンドが動作しなくなったり、構文が変更されたり、リリースによって GUI や CLI の見た目が異なったりする場合があります。

フィードバックのリクエスト

ユーザー入力が役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始

されています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。