アクセス ポイント通信プロトコルの使用

アクセス ポイント通信プロトコルについて

Cisco Lightweight アクセス ポイントは、IETF 標準 Control and Provisioning of Wireless Access Points Protocol（CAPWAP）を使用してネットワーク上のコントローラおよび他の Lightweight アクセス ポイントと通信します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、コントローラによる無線アクセス ポイントの集合の管理を可能にします。 CAPWAP は、次の理由でコントローラに実装されます。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- コントローラにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

LWAPP を使用可能なアクセス ポイントは CAPWAP コントローラを検出して join することができ、CAPWAP コントローラへの変換はシームレスです。 たとえば、CAPWAP 使用時のコントローラ ディスカバリ プロセスおよびファームウェア ダウンロード プロセスは、LWAPP 使用時のものと同じです。 例外として、レイヤ 2 の展開は CAPWAP ではサポートされません。

CAPWAP コントローラおよび LWAPP コントローラは、同じネットワークで展開が可能です。 CAPWAP を使用可能なソフトウェアでは、アクセス ポイントは CAPWAP を実行するコントロー

ラでも LWAPP を実行するコントローラでも join できます。 Cisco Aironet 1040、1140、1260、3500、および 3600 シリーズ アクセス ポイントは唯一の例外であり、これらは CAPWAP のみをサポートし、CAPWAP を実行するコントローラにのみ join します。 たとえば、1130 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにも LWAPP を実行するコントローラにも join できますが、1140 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにのみ join できます。

次に、アクセス ポイント通信プロトコルについて従う必要がある注意事項を示します。

- LWAPP を使用するアクセス ポイントからのトラフィックのみ許可するようファイアウォールが設定されている場合は、ファイアウォールのルールを変更して CAPWAP を使用するアクセス ポイントからのトラフィックを許可する必要があります。
- CAPWAP UDP ポート 5246 および 5247（LWAPP UDP ポート 12222 および 12223 と同等のポート）が有効になっており、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト（ACL）がコントローラとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。

アクセス ポイント通信プロトコルの制約事項

- 仮想コントローラ プラットフォームでは、クライアントごとのダウンストリーム レート制限は FlexConnect 中央スイッチングでサポートされません。
- レート制限は、どの方向からでも CPU 宛てのすべてのトラフィックに適用されます（無線または有線）。 コントローラにトラフィックをレート制限するデフォルトの **config advanced rate enable** コマンドでコントローラが常に実行し、サービス拒絶（DoS）攻撃から保護することを推奨します。 Internet Control Message Protocol（ICMP）エコー応答のレート制限をテスト目的で停止する **config advanced rate disable** コマンドを使用できます。 ただしテスト完了後、**config advanced rate enable** コマンドを再適用することを推奨します。
- コントローラが適切な日時で設定されていることを確認してください。 コントローラに設定されている日時がアクセス ポイントの証明書の作成日とインストール日に先行すると、アクセス ポイントはコントローラに join しません。

データ暗号化の設定

Cisco 5500 シリーズ コントローラにより、データグラム トランスポート層セキュリティ（DTLS）を使用してアクセス ポイントとコントローラの間で送信される CAPWAP コントロール パケット（および、オプションとして CAPWAP データ パケット）の暗号化が可能です。 DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。 CAPWAP コントロール パケットとはコントローラとアクセス ポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。 CAPWAP コント

ロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。 アクセス ポイントが 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 プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

（注） Cisco WLC は、ゲートウェイのスタディック設定のみをサポートします。 そのため、ゲートウェイの IP アドレスを変更する ICMP リダイレクトは考慮されません。

データ暗号化のためのガイドライン

- Cisco 1130 および 1240 シリーズのアクセス ポイントはソフトウェアベースの暗号化で DTLS データ暗号化をサポートしています。
- Cisco 1040、1140、1250、1260、1530、1550、1600、1700、2600、2700、3500、3600、および 3700 シリーズのアクセス ポイントはハードウェア ベースの暗号化で DTLS データ暗号化をサポートします。
- Cisco Aironet 1552 および 1522 屋外アクセス ポイントはデータ DTLS をサポートしています。
- DTLS データ暗号化は、Cisco Aironet 700 シリーズ アクセス ポイントではサポートされていません。
- DTLS データ暗号化は OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。 ほとんどのアクセス ポイントは会社のビルディング内の安全なネットワークにおいて展開されるため、データの暗号化は必要ありません。 反対に、OfficeExtend アクセス ポイントとコントローラの間のトラフィックは安全でないパブリック ネットワークを経由するため、これらのアクセス ポイントではデータの暗号化はより重要です。 データの暗号化が有効な場合、トラフィックはアクセス ポイントで暗号化されてからコントローラに送信され、また、コントローラで暗号化されてからクライアントに送信されます。
- 暗号化はコントローラおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- シスコのユニファイド ローカル ワイヤレス ネットワーク環境では、Cisco 1130 および 1240 アクセス ポイントで DTLS を有効にしないでください。有効にすると、重大なスループットの低下が発生し、AP が使用できなくなるおそれがあります。

  OfficeExtend アクセス ポイントの詳細は、『OfficeExtend Access Points』を参照してください。
- コントローラを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- データ DTLS のアベイラビリティは次のとおりです。

- Cisco 5500 シリーズ コントローラは、2 個のライセンスのオプションで使用可能です。ライセンスおよびデータ DTLS を使用するのにライセンスを必要とする他のイメージなしでデータ DTLS を使用可能にします。 「Cisco 5500 シリーズ コントローラ用 DTLS イメージのアップグレードまたはダウングレード」の項を参照してください。 DTLS のイメージとライセンス付き DTLS のイメージは、次のとおりです。

  ライセンス付きの DTLS：AS_5500_LDPE_x_x_x_x.aes

  ライセンスなしの DTLS—AS_5500_x_x_x_x.aes

- Cisco 2500、Cisco WiSM2、Cisco 仮想ワイヤレス コントローラ：デフォルトでは、これらのプラットフォームに DTLS は含まれていません。 データ DTLS をオンにするには、ライセンスをインストールする必要があります。 これらのプラットフォームには、データ DTLS を無効にした 1 つのイメージがあります。 データ DTLS を使用するには、ライセンスが必要です。

  データ DTLS が含まれていない Cisco 仮想ワイヤレス コントローラの場合、コントローラの平均スループットは約 200 Mbps です。 データ DTLS を使用するすべての AP を使用すると、コントローラの平均スループットは約 100 Mbps になります。

- コントローラにデータ DTLS のライセンスがなく、コントローラに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- Cisco 5508 シリーズ コントローラを使用しているロシア以外のお客様はデータ DTLS ライセンスを必要としません。 ただし、Cisco 2500 シリーズ コントローラ、Cisco 8500 シリーズ コントローラ、WISM2 および Cisco 仮想ワイヤレス コントローラを使用しているすべてのお客様は、データ DTLS 機能をオンにするためにデータ DTLS ライセンスが必要です。

Cisco 5500 シリーズ コントローラ用 DTLS イメージのアップグレードまたはダウングレード

ステップ 1 アップグレード操作は、最初の試みで失敗し、警告はライセンス付きの DTLS イメージへのアップグレードを行うと元に戻せないことを示します。

（注） ステップ 1 の後にコントローラをリブートしないでください。

ステップ 2 次のアップデートでは、ライセンスが適用され、イメージが正常に更新します。

DTLS イメージへまたは DTLS イメージからのアップグレード時のガイドライン

- ライセンス付きのデータ DTLS イメージがインストールされると、通常のイメージ（ライセンスなしのデータ DTLS）をインストールできません。

- ライセンス付き DTLS イメージから別のライセンス付き DTLS イメージにアップグレードできます。
- 通常のイメージ（DTLS）からライセンス付きの DTLS イメージへのアップグレードは、2 ステップ プロセスで行います。
- **show sysinfo** コマンドを使用して、イメージのアップグレードの前後に LDPE イメージを確認できます。

データ暗号化の設定（GUI）

Cisco 5500 シリーズ コントローラに基本ライセンスがインストールされていることを確認します。ライセンスがインストールされると、アクセス ポイントのデータ暗号化を有効化できます。

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2 暗号化を有効にするアクセス ポイントの名前をクリックします。

ステップ 3 [Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます。

ステップ 4 このアクセス ポイントでデータ暗号化を有効にする場合は [Data Encryption] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。 デフォルト値はオフです。

（注） データ暗号化モードに変更するには、アクセス ポイントをコントローラに再 join する必要があります。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

データ暗号化の設定（CLI）

（注） DTLS ライセンスのないイメージでは、**config** または **show** コマンドは使用できません。

コントローラの CLI を使用してコントローラ上のアクセス ポイントの DTLS データ暗号化を有効にする手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ暗号化を有効または無効にします。
config ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

デフォルト値は [disabled] です。

（注） データ暗号化モードに変更するには、アクセス ポイントをコントローラに再 join する必要があります。

ステップ 2 アクセスポイントおよび接続しているクライアントの切断を確認するよう求めるプロンプトが表示されたら、**Y** と入力します。

ステップ 3 **save config** コマンドを入力して、設定を保存します。

ステップ 4 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示します。
show ap link-encryption {**all** | *Cisco_AP*}

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセスポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。

ステップ 5 すべてのアクティブな DTLS 接続の概要を表示するには、次のコマンドを入力します。
show dtls connections

（注） DTLS データ暗号化に問題が生じた場合は、**debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} コマンドを入力して、すべての DTLS メッセージ、イベント、トレース、またはパケットをデバッグします。

ステップ 6 次のコマンドを入力して、AP とコントローラの間の DTLS 接続用の新しい暗号スイートを有効にします。
config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

ステップ 7 次のコマンドを入力して、DTLS 暗号スイートの概要を表示します。
show ap dtls-cipher-suite

CAPWAP の最大伝送単位情報の表示

コントローラ上の CAPWAP パスの最大伝送単位（MTU）を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

以下に類似した情報が表示されます。

```
Cisco AP Identifier............................. 9
Cisco AP Name................................... Maria-1250
Country code.................................... US  - United States
Regulatory Domain allowed by Country............ 802.11bg:-A     802.11a:-A
AP Country code................................. US  - United States
AP Regulatory Domain............................ 802.11bg:-A    802.11a:-A
Switch Port Number ............................. 1
MAC Address..................................... 00:1f:ca:bd:bc:7c
IP Address Configuration........................ DHCP
IP Address...................................... 1.100.163.193
IP NetMask...................................... 255.255.255.0
CAPWAP Path MTU................................. 1485
```

CAPWAP のデバッグ

次のコマンドを使用して、CAPWAP デバッグ情報を取得します。

- **debug capwap events** {**enable** | **disable**}：CAPWAP イベントのデバッグを有効または無効にします。
- **debug capwap errors** {**enable** | **disable**}：CAPWAP エラーのデバッグを有効または無効にします。
- **debug capwap detail** {**enable** | **disable**}：CAPWAP の詳細のデバッグを有効または無効にします。
- **debug capwap info** {**enable** | **disable**}：CAPWAP 情報のデバッグを有効または無効にします。
- **debug capwap packet** {**enable** | **disable**}：CAPWAP パケットのデバッグを有効または無効にします。
- **debug capwap payload** {**enable** | **disable**}：CAPWAP ペイロードのデバッグを有効または無効にします。
- **debug capwap hexdump** {**enable** | **disable**}：CAPWAP 16 進数ダンプのデバッグを有効または無効にします。
- **debug capwap dtls-keepalive** {**enable** | **disable**}：CAPWAP DTLS データ キープアライブ パケットのデバッグを有効または無効にします。

コントローラ ディスカバリ プロセス

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してコントローラを検知してから、コントローラに CAPWAP join request を送信します。 これに対し、コントローラはアクセス ポイントに CAPWAP join response を返し、アクセス ポイントはコントローラに join できるようになります。 アクセス ポイントがコントローラに join すると、コントローラによってアクセス ポイントの構成、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。

次に、コントローラ ディスカバリ プロセスの注意事項を示します。

- LWAPP から CAPWAP へのアップグレード パスおよび CAPWAP から LWAPP へのダウングレード パスがサポートされます。 LWAPP イメージを持つアクセス ポイントは、LWAPP でディスカバリ プロセスを開始します。 LWAPP コントローラを検出すると、LWAPP ディスカバリ プロセスを開始してコントローラに join します。 LWAPP コントローラが見つからない場合は、CAPWAP でディスカバリを開始します。 1 つのディスカバリ タイプ（CAPWAP または LWAPP）でディスカバリ プロセスを開始した回数が最大ディスカバリ カウントを超えてもアクセス ポイントが discovery response を受信しない場合は、ディスカバリ タイプはもう一方のタイプに変更されます。 たとえば、アクセス ポイントが LWAPP でコントローラを検出できない場合、CAPWAP でディスカバリ プロセスを開始します。

- アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してコントローラに再 join します。
- コントローラが CAPWAP discovery response で送信する IP アドレスを設定するには、**config network ap-discovery nat-ip-only** {**enable** | **disable**} コマンドを使用します。
- アクセス ポイントをネットワークでアクティブにするには、コントローラがそのアクセス ポイントを検出する必要があります。 Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。
  - Layer 3 CAPWAP または LWAPP ディスカバリ：この機能は、アクセス ポイントとは異なるサブネット上で有効化でき、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IPv4 アドレスと IPv6 アドレスのどちらかと UDP パケットが使用されます。
  - CAPWAP マルチキャスト ディスカバリ：ブロードキャストが IPv6 アドレス内に存在しません。 アクセス ポイントは、すべてのコントローラのマルチキャスト アドレス（FF01::18C）に CAPWAP ディスカバリ メッセージを送信します。 コントローラは、同じ L2 セグメント上に存在する AP のみから IPv6 ディスカバリ要求を受け取り、IPv6 ディスカバリ応答を返します。
  - ローカルに保存されているコントローラの IPv4 または IPv6 アドレス ディスカバリ：アクセス ポイントがすでにコントローラにアソシエートされている場合は、プライマリ、セカンダリ、およびターシャリ コントローラの IPv4 または IPv6 アドレスがアクセス ポイントの不揮発性メモリに保存されます。 今後の展開用にアクセス ポイントにコントローラの IPv4 または IPv6 アドレスを保存するこのプロセスは、「アクセス ポイントのプライミング」と呼ばれます。
  - オプション 43 を使用した DHCP サーバ ディスカバリ：この機能では、DHCP オプション 43 を使用して、コントローラの IPv4 アドレスをアクセス ポイントに提供します。 Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。 DHCP オプション 43 の詳細については、「Using DHCP Option 43 and DHCP Option 60」の項を参照してください。
  - オプション 52 を使用した DHCP サーバ ディスカバリ：この機能は、DHCP オプション 52 を使用して、AP が接続先のコントローラの IPv6 アドレスを検出できるようにします。 DHCPv6 メッセージの一部として、DHCP サーバは IPv6 アドレスをコントローラ管理に提供します。
  - DNS の検出：アクセス ポイントでは、ドメイン ネーム サーバ（DNS）を介してコントローラを検出できます。 CISCO-LWAPP-CONTROLLER.*localdomain* または CISCO-CAPWAP-CONTROLLER.*localdomain* への応答としてコントローラの IPv4 アドレスと IPv6 アドレスを返すように DNS を設定する必要があります。ここで、*localdomain* はアクセス ポイント ドメイン名です。

    アクセス ポイントは、DHCPv4/DHCPv6 サーバから IPv4/IPv6 アドレスと DNSv4/DNSv6 の情報を受信すると、DNS に接続して CISCO-LWAPP-CONTROLLER.*localdomain* または CISCO-CAPWAP-CONTROLLER.*localdomain* を解決します。 DNS がアドレスまたはアドレスの両方が IPv4 アドレスまたは IPv6 を含むかもしれないコントローラの IP アドレスのリストを受信すると、アクセス ポイントはコントローラに検出要求を送信します。

コントローラ ディスカバリ プロセスの制約事項

- ディスカバリ プロセスでは、1040、1140、1260、3500、および 3600 シリーズ アクセス ポイントはシスコの CAPWAP コントローラのみをクエリーします。 LWAPP コントローラに関するクエリーは送信されません。 これらのアクセス ポイントで LWAPP と CAPWAP コントローラの両方に対するクエリーを送信する場合は、DNS を更新する必要があります。
- コントローラが現在の時刻に設定されていることを確認してください。 コントローラをすでに経過した時刻に設定すると、その時刻には証明書が無効である可能性があり、アクセス ポイントがコントローラに join できない場合があります。

アクセス ポイントのコントローラへの join の確認

コントローラを交換する場合、アクセス ポイントが新しいコントローラに join していることを確認する必要があります。

アクセス ポイントのコントローラへの join の確認（GUI）

ステップ 1 次の手順で、新しいコントローラをマスター コントローラとして設定します。

a) [Controller] > [Advanced] > [Master Controller Mode] の順に選択し、[Master Controller Configuration] ページを開きます。

b) [Master Controller Mode] チェックボックスをオンにします。

c) [Apply] をクリックして、変更を確定します。

d) [Save Configuration] をクリックして、変更を保存します。

ステップ 2 （任意）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。

ステップ 3 アクセス ポイントを再起動します。

ステップ 4 すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定するには、[Master Controller Configuration] ページで [Master Controller Mode] チェックボックスをオフにします。

アクセス ポイントのコントローラへの join の確認（CLI）

ステップ 1 次のコマンドを入力して、新しいコントローラをマスター コントローラとして設定します。

config network master-base enable

ステップ 2 （任意）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。

ステップ 3 アクセス ポイントを再起動します。

ステップ 4 次のコマンドを入力して、すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定します。
config network master-base disable