管理フレーム保護の設定

管理フレーム保護について

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。 MFP は、インフラストラクチャとクライアント サポートの両方を実現します。

- インフラストラクチャ MFP：DoS 攻撃を引き起こしたり、ネットワーク上で過剰なアソシエーションやプローブを生じさせたり、不正なアクセスポイントとして介入したり、QoS と無線測定フレームへの攻撃によりネットワーク パフォーマンスを低下させたりする敵対者を検出することにより、管理フレームを保護します。 インフラストラクチャ MFP は、フィッシング インシデントを検出および報告するための迅速かつ効果的な手段を提供するグローバル設定です。

  インフラストラクチャ MFP は特に、アクセス ポイントによって送信され（クライアントによって送信されたのではなく）、次にネットワーク内の他のアクセス ポイントによって検証される管理フレームに、Message Integrity Check Information Element（MIC IE; メッセージ整合性情報要素）を追加することによって、802.11 セッション管理機能を保護します。 インフラストラクチャ MFP はパッシブです。 侵入を検知し報告しますが、それを止めることはできません。

- クライアント MFP：認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多くの一般化した攻撃が効力を発揮することのないようにします。 認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを悪化させます。

  具体的には、クライアント MFP は、アクセス ポイントと CCXv5 クライアント間で送受信される管理フレームを暗号化します。その結果、スプーフィングされたクラス 3 管理フレーム（つまり、アクセスポイントと、認証およびアソシエートされたクライアントとの間でやり取りされる管理フレーム）をドロップすることにより、アクセスポイントとクライアントの両方で予防措置をとることができます。 クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP は、最も一般的な種類のサービス拒否攻撃から、クライアントとアクセス ポイント間のセッションを保護します。 また、セッションのデータ フレームに使用されているのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。 アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

  クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしており、TKIP または AES-CCMP のいずれかを使用して WPA2 をネゴシエートする必要があります。 EAP または PSK は、PMK を取得するために使用されます。 CCKM およびコントローラのモビリティ管理は、レイヤ 2 およびレイヤ 3 の高速ローミングのために、アクセス ポイント間でセッション キーを配布するのに使用されます。

  （注） ブロードキャスト フレームを使用した攻撃を防ぐため、CCXv5 をサポートするアクセス ポイントでは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントおよびアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄する必要があります。

  インフラストラクチャ MFP は、クライアント MFP 対応でないクライアントに送信された無効なユニキャスト フレームと、無効なクラス 1 およびクラス 2 管理フレームを引き続き検出および報告するため、クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足するものであると言えます。 インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

  インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- 管理フレーム保護：アクセス ポイントは、送信される各管理フレームに MIC IE を追加することによってフレームを保護します。 フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。 MFP は、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。

- 管理フレーム検証：インフラストラクチャ MFP では、アクセス ポイントによって、ネットワーク内の他のアクセス ポイントから受信する各管理フレームが検証されます。 MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。 MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能するように、すべてのコントローラでネットワーク タイム プロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントで異常が検出されるとコントローラに通知されます。コントローラでは、受信した異常イベントが集計され、その結果が SNMP トラップを使用してネットワーク管理システムに報告されます。

（注） クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効化されており、システム全体で無効化できます。 以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント許可が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はシステム全体で無効になります。インフラストラクチャ MFP がグローバルに有効化されると、選択した WLAN に対してシグニチャの生成（MIC を送信フレームに追加する）を無効にでき、選択したアクセス ポイントに対して検証を無効にできます。

クライアント MFP は、WPA2 に対して設定された WLAN 上でデフォルトで有効にされています。選択した WLAN 上で無効にすることも、必須にする（その場合、MFP をネゴシエートするクライアントのみがアソシエーションを許可されます）こともできます。

管理フレーム保護の制約事項

- Lightweight アクセス ポイントでは、インフラストラクチャ MFP はローカル モードおよび監視モードでサポートされます。アクセス ポイントがコントローラに接続しているときは、FlexConnect モードでサポートされます。 クライアント MFP は、ローカル モード、FlexConnect モード、およびブリッジ モードでサポートされます。
- OEAP 600 シリーズのアクセス ポイントでは、MFP はサポートされません。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでの使用のみがサポートされています。
- クライアント MFP が無効にされているか、オプションである場合は、非 CCXv5 クライアントは WLAN にアソシエートできます。
- スタンドアロン モードの FlexConnect アクセス ポイントで生成されるエラー レポートは、コントローラに転送することはできず、ドロップされます。

管理フレーム保護の設定（GUI）

ステップ 1 [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[AP Authentication Policy] ページを開きます。

ステップ 2 [Protection Type] ドロップダウン リストから [Management Frame Protection] を選択して、コントローラに対してインフラストラクチャ MFP をグローバルに有効にします。

ステップ 3 [Apply] をクリックして、変更を確定します。

（注） 複数のコントローラがモビリティ グループに含まれている場合は、インフラストラクチャ MFP に対して設定されているモビリティ グループ内のすべてのコントローラ上で、ネットワーク タイム プロトコル（NTP）サーバを設定する必要があります。

ステップ 4 コントローラに対してインフラストラクチャ MFP をグローバルに有効にしたあと、次の手順を実行して、特定の WLAN にクライアント MFP を設定します。

a) [WLANs] を選択します。

b) 目的の WLAN のプロファイル名をクリックします。 [WLANs > Edit] ページが表示されます。

c) [Advanced] を選択します。 [WLANs > Edit]（[Advanced]）ページが表示されます。

d) [MFP Client Protection] ドロップダウン リストから、[Disabled]、[Optional]、または [Required] を選択します。 デフォルト値は [Optional] です。 [Required] を選択した場合、MFP がネゴシエートされている場合（つまり、WPA2 がコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 に対して設定されている場合）のみ、クライアントはアソシエーションを許可されます。

（注） Cisco OEAP 600 では MFP はサポートされません。 [Disabled] または [Optional] を選択してください。

e) [Apply] をクリックして、変更を確定します。

ステップ 5 [Save Configuration] をクリックして設定を保存します。

管理フレーム保護の設定の表示（GUI）

コントローラの現在のグローバル MFP の設定を表示するには、[Security] > [Wireless Protection Policies] > [Management Frame Protection] の順に選択します。 [Management Frame Protection Settings] ページが表示されます。

このページでは、次の MFP 設定が表示されます。

- [Management Frame Protection] フィールドは、インフラストラクチャ MFP がコントローラでグローバルに有効化されているかどうかを示します。
- [Controller Time Source Valid] フィールドは、コントローラの時刻が（時刻を手動で入力することにより）ローカルで設定されているか、外部ソース（NTP サーバなど）を通じて設定されているかを示します。 時刻が外部ソースにより設定されている場合、このフィールドの値は「True」です。時刻がローカルで設定されている場合、このフィールドの値は「False」で

す。時刻ソースは、モビリティ グループ内の複数のコントローラのアクセス ポイント間の管理フレーム上のタイムスタンプの検証に使用されます。

- [Client Protection] フィールドは、クライアント MFP が個別の WLAN に対して有効化されているかどうかと、オプションまたは必須のいずれであるかを示します。

管理フレーム保護の設定（CLI）

- 次のコマンドを入力して、コントローラに対してインフラストラクチャ MFP をグローバルに有効または無効にします。
  config wps mfp infrastructure {enable | disable}
- 次のコマンドを入力して、特定の WLAN でクライアント MFP シグニチャを有効または無効にします。
  config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

  クライアント MFP を有効にしてオプションの **required** パラメータを使用すると、MFP がネゴシエートされている場合のみ、クライアントはアソシエーションを許可されます。

管理フレーム保護の設定の表示（CLI）

- 次のコマンドを入力して、コントローラの現在の MFP の設定を表示します。
  show wps mfp summary
- 次のコマンドを入力して、特定の WLAN の現在の MFP の設定を表示します。
  show wlan wlan_id
- 次のコマンドを入力して、特定のクライアントに対してクライアント MFP が有効になっているかどうかを表示します。
  show client detail *client_mac*
- 次のコマンドを入力して、コントローラの MFP 統計情報を表示します。
  show wps mfp *statistics*

（注） 実際に攻撃が進行中でない限り、このレポートにデータは含まれません。 ここに示すさまざまなエラーの種類の例は、図示のみを目的としています。 この表は 5 分ごとにクリアされ、データはネットワーク管理ステーションに転送されます。

管理フレーム保護の問題のデバッグ（CLI）

- MFP に関する問題が発生した場合は、次のコマンドを使用します。
  debug wps mfp ? {**enable** | **disable**}

  ここで、? は、次のいずれかを示します。

client：クライアント MFP メッセージのデバッグについて設定します。

capwap：コントローラとアクセス ポイント間の MFP メッセージのデバッグについて設定します。

detail：MFP メッセージの詳細なデバッグについて設定します。

report：MFP レポートのデバッグについて設定します。

mm：MFP モビリティ（コントローラ間）メッセージのデバッグについて設定します。