CHAPTER 26

Management Frame Protection

このマニュアルでは、Management Frame Protection（MFP; 管理フレーム保護）の設定方法について説明します。

Management Frame Protection の概要

Management Frame Protection は、アクセス ポイント（AP）とクライアント ステーション間を通過する管理メッセージのセキュリティを確保します。MFP は、インフラストラクチャ MFP およびクライアント MFP という 2 つの機能コンポーネントから構成されています。

インフラストラクチャ MFP は、インフラストラクチャのサポートを提供します。インフラストラクチャ MFP は、ブロードキャストやダイレクト管理フレームで Message Integrity Check（MIC; メッセージ完全性チェック）を利用します。このチェックは、不正なデバイスや Denial-of-Service （DoS; サービス拒絶）攻撃を検出するのに役立ちます。クライアント MFP は、クライアントのサポートを提供します。

クライアント MFP は、WLAN に対する一般的な攻撃の多くが効力を持たないようにすることでスプーフされたフレームから認証されたクライアントを保護します。

Management Frame Protection が動作するには、Wireless Domain Services（WDS; 無線ドメイン サービス）が必要です。MFP は Wireless LAN Solution Engine（WLSE）で設定されますが、AP および WDS で MFP を手動で設定することもできます。

（注） WLSE がない場合、MFP は検出された侵入を報告できず、効果が制限されてしまいます。WLSE が存在する場合、WLSE から設定を行う必要があります。

完全に保護するには、Simple Network Time Protocol（SNTP）の MFP AP も設定する必要があります。

クライアント MFP は、AP と Cisco Compatible Extension バージョン 5（CCXv5）対応のクライアント ステーション間で送信されたクラス 3 管理フレームを暗号化し、AP およびクライアントの両方が、スプーフされたクラス 3 管理フレーム（つまり、認証および関連付けが行われた AP とクライアント ステーション間で受け渡される管理フレーム）を廃棄して予防措置を講じることができるようにします。クライアント MFP は、IEEE 802.11i で定義されたセキュリティ メカニズムを利用してクラス 3 ユニキャスト管理フレームを保護します。再アソシエーション要求の Robust Security Network Information Element（RSNIE）の STA でネゴシエートされたユニキャスト暗号スイートは、ユニキャスト データおよびクラス 3 管理フレームの両方の保護に使用します。ワークグループ ブリッジ モード、リピータ モード、または非ルートブリッジ モードの AP がクライアント MFP を使用するには、Temporal Key Integrity Protocol（TKIP）または Advanced Encryption Standard-Cipher Block Chaining Message Authentication Code Protocol（AES-CCMP）のいずれかのネゴシエーションを行う必要があります。

ユニキャスト管理フレームの保護

ユニキャスト クラス 3 管理フレームは、データ フレームに使用されるのと同様の手法で AES-CCMP または TKIP のいずれかを適用することにより保護されます。暗号化が AES-CCMP または TKIP で、鍵管理が Wi-Fi Protected Access バージョン 2（WPA2）の場合に限り、クライアント MFP が自律 AP でイネーブルになります。

ブロードキャスト管理フレームの保護

ブロードキャスト フレームを使用した攻撃を回避するために、CCXv5 をサポートする AP ではブロードキャスト クラス 3 管理フレームを放出しません。クライアント MFP がイネーブルの場合、ワークグループ ブリッジ モード、リピータ モード、または非ルートブリッジ モードの AP はブロードキャスト クラス 3 管理フレームを破棄します。

暗号化が AES-CCMP または TKIP で、鍵管理が WPA2 の場合に限り、クライアント MFP が自律 AP でイネーブルになります。

ルート モードのアクセス ポイントのクライアント MFP

ルート モードの自律 AP は、混合モードのクライアントをサポートします。暗号スイート AES または TKIP が WPA2 とネゴシエートする CCXv5 対応のクライアントでは、クライアント MFP がイネーブルになります。クライアント MFP は、CCXv5 に対応していないクライアントをディセーブルにします。デフォルトでは、クライアント MFP は AP 上の特定の Service Set Identifier（SSID; サービス セット ID）のオプションになります。SSID 設定モードで Command Line Interface（CLI; コマンドライン インターフェイス）を使用することにより、クライアント MFP をイネーブルまたはディセーブルにできます。

クライアント MFP は特定の SSID で必須またはオプションとして設定できます。クライアント MFP を必須の要素として設定するには、鍵管理に WPA2 mandatory を使用して SSID を設定します。鍵管理が WPA2 mandatory でない場合、エラーメッセージが表示され、CLI コマンドが拒否されます。クライアント MFP を必須の要素とし、鍵管理を WPA2 に設定している場合に鍵管理を変更しようとすると、エラーメッセージが表示され、CLI が拒否されます。オプションとして設定されている場合、SSID が WPA2 対応のときにクライアント MFP がイネーブルになります。それ以外の場合は、クライアント MFP がディセーブルになります。

クライアント MFP の設定

AP がルート モードのクライアント MFP を設定するには、次の CLI コマンドを使用します。

- **ids mfp client required**

  この SSID 設定コマンドは、特定の SSID でクライアント MFP を必須の要素としてイネーブルにします。このコマンドが実行されると、dot11radio インターフェイスがリセットされます。また、このコマンドは SSID が WPA2 mandatory に設定されていることを前提としています。SSID が WPAv2 mandatory に設定されていない場合、エラーメッセージが表示され、コマンドが拒否されます。

- **no ids mfp client**

  この SSID 設定コマンドは、特定の SSID でクライアント MFP をディセーブルにします。このコマンドが実行されると、dot11radio インターフェイスがリセットされます。

- **ids mfp client optional**

  この SSID 設定コマンドは、特定の SSID でクライアント MFP をオプションとしてイネーブルにします。このコマンドが実行されると、dot11radio インターフェイスがリセットされます。SSID が WPA2 対応の場合、この特定の SSID に対するクライアント MFP がイネーブルになります。それ以外の場合は、クライアント MFP がディセーブルになります。

- **show dot11 ids mfp client statistics**

  このコマンドは、dot11radio インターフェイスの AP コンソール上にクライアント MFP の統計を表示する場合に使用します。

- **clear dot11 ids mfp client statistics**

  このコマンドは、クライアント MFP の統計をクリアする場合に使用します。

- **authentication key management wpa version {1 | 2}**

  このコマンドは、特定の SSID に対する WPA 鍵管理に使用する WPA のバージョンを明示的に指定する場合に使用します。

インフラストラクチャ MFP の設定

インフラストラクチャ MFP を設定するには、イネーブル EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ids mfp generator**	AP を MFP ジェネレータとして設定します。イネーブルに設定した場合、AP が伝送する各フレームに Message Integrity Check Information Element（MIC IE; メッセージ完全性チェック情報要素）を付加することにより、AP は管理フレームを保護します。フレームのコピー、変更、または再生を試みると、MIC が無効となり、MFP フレームを検出（検証）するように設定されている受信 AP によって不一致が報告されます。AP は WDS のメンバである必要があります。
ステップ 3	**dot11 ids mfp detector**	AP を MFP 検出器として設定します。イネーブルに設定した場合、AP は他の AP から受信する管理フレームを検証します。AP が有効かつ予測された MIC IE が含まれないフレームを受信した場合、WDS に不一致を報告します。AP は WDS のメンバである必要があります。
ステップ 4	**sntp server** *server IP address*	SNTP サーバの名前または IP アドレスを入力します。
ステップ 5	**end**	イネーブル EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

WDS を設定するには、WDS のイネーブル EXEC モードを開始し、次の手順を実行します。

	コマンド	説明
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ids mfp distributor**	WDS を MFP ディストリビュータとして設定します。イネーブルに設定した場合、WDS は MIC IE の作成に使用されたシグニチャ キーを管理し、WDS はジェネレータと検出器の間でシグニチャ キーをセキュリティ保護された状態で転送します。
ステップ 3	**end**	イネーブル EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。