Management Frame Protection

管理フレーム保護（MFP）について

管理フレーム保護（MFP）は、アクセスポイントとクライアント間で送受信される管理メッセージに対するセキュリティを確保します。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。

  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。

インフラストラクチャ MFP は、デフォルトで無効になっており、システム全体で有効にできます。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 ポイント認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。

- 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。

サポートされるアクセスポイントモデル

Cisco MFP は、次の AP モデルでサポートされています。

- Cisco Aironet 2802、3802、および 4802 シリーズ アクセスポイント
- Cisco Aironet 2800、3800、4800、1560 シリーズ アクセスポイント
- すべての Cisco IOS アクセスポイント

サポートされないアクセスポイントモデル

Cisco MFP は、次の AP モデルではサポートされていません。

- Cisco Aironet 1800 および 1900 シリーズ アクセスポイント
- Cisco 802.11ax アクセスポイント

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。
- 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。
- OEAP 600 シリーズ アクセスポイントでは、MFP はサポートされません。
- 802.11ax 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 が無効にされているか、オプションである場合は、非 CCXv5 クライアントが WLAN にアソシエートされる可能性があります。
- 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。
- キーは乱数ジェネレータを使用して生成されますが、SHA に変更することによってキーを改善できます。
- 各 BSSID の MFP キーはサポートされていません。

管理フレーム保護の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps mfp** 例： `Device(config)# wireless wps mfp`	管理フレーム保護を設定します。

	コマンドまたはアクション	目的

ステップ 3	**wireless wps mfp** {**ap-impersonation** | **key-refresh-interval**}
	例：
	`Device(config)# wireless wps mfp ap-impersonation`
	`Device(config)# wireless wps mfp key-refresh-interval`
		AP の偽装検出（または）MFP キーの更新間隔を時単位で設定します。
		key-refresh-interval：MFP キーの更新間隔を時単位で設定します。有効な範囲は 1 ～ 24 です。デフォルト値は 24 です。

ステップ 4	**end** 例： `Device(config)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 **EXEC** モードに戻ります。

管理フレーム保護の設定の確認

管理フレーム保護（MFP）機能が有効かどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary
Client Exclusion Policy
  Excessive 802.11-association failures   : unknown
  Excessive 802.11-authentication failures: unknown
  Excessive 802.1x-authentication         : unknown
  IP-theft                                : unknown
  Excessive Web authentication failure    : unknown
  Failed Qos Policy                       : unknown

Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

MFP の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless wps mfp summary
Management Frame Protection
  Global Infrastructure MFP state : Enabled
  AP Impersonation detection      : Disabled
  Key refresh interval            : 15
```

MFP の統計情報の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless wps mfp statistics
BSSID          Radio DetectorAP                        LastSourceAddr Error
Count     FrameTypes

aabb.ccdd.eeff a     AP3800                            aabb.ccdd.eeff Invalid MIC     10
        Beacon, Probe Response
                                                                     Invalid MIC     20
        Beacon, Probe Response
```

アクセスポイントが MFP の検証と保護をサポートしているかどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps mfp ap summary
AP Name                          Radio MAC              Validation           Protection
-------------------------------------------------------------------------------------------
AP002A.1087.CBF4                 00a2.eefd.bdc0           Enabled               Enabled

AP58AC.78DE.9946                 00a2.eeb8.4ae0           Enabled               Enabled

APb4de.3196.caac                 4c77.6d83.6b90           Enabled               Enabled
```