MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定

MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーについて

レイヤ 2 およびレイヤ 3 セキュリティを組み合わせたフォールバック ポリシー メカニズムを設定できます。 MAC フィルタリングおよび Web 認証の両方が設定されているシナリオで、MAC フィルタ（RADIUS サーバ）を使用して WLAN への接続を試行する場合、クライアントが認証に失敗すると、Web 認証にフォール バックできるように認証を設定できます。 クライアントが MAC フィルタ認証をパスすると、Web 認証が省略され、クライアントは WLAN に接続されます。 この機能を使用して、MAC フィルタ認証エラーのみに基づいたアソシエーション解除を回避できます。

MACフィルタリングおよびWeb認証を伴うフォールバック ポリシーの設定（GUI）

（注） フォールバック ポリシーを設定する前に、MAC フィルタリングを有効にする必要があります。

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Web 認証に対してフォールバック ポリシーを設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Layer 3 Security] ドロップダウン リストから、[None] を選択します。

ステップ 5 [Web Policy] チェックボックスをオンにします。

（注） コントローラは、認証前にワイヤレスクライアントで送受信される DNS トラフィックを転送します。

次のオプションが表示されます。

- 認証
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

ステップ 6 [On MAC Filter Failure] をクリックします。

ステップ 7 [Apply] をクリックして、変更を確定します。

ステップ 8 [Save Configuration] をクリックして設定を保存します。

MACフィルタリングおよびWeb認証を伴うフォールバック ポリシーの設定（CLI）

（注） フォールバック ポリシーを設定する前に、MAC フィルタリングを有効にする必要があります。 MAC フィルタリングを有効にする方法については、「WLAN の MAC フィルタリングについて」の項を参照してください。

ステップ 1 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。
config wlan security web-auth on-macfilter-failure *wlan-id*

ステップ 2 Web 認証ステータスを表示するには、次のコマンドを入力します。
show wlan *wlan_id*

```
FT Over-The-Ds mode............................ Enabled
CKIP ......................................... Disabled
   IP Security................................. Disabled
   IP Security Passthru........................ Disabled
   Web Based Authentication..................... Enabled-On-MACFilter-Failure
        ACL.......................................... Unconfigured
        Web Authentication server precedence:
        1............................................ local
        2............................................ radius
        3............................................ ldap
```