8021.X 認証を使用した Web リダイレクトの設定

802.1X 認証を使用した Web リダイレクトについて

802.1X 認証が正常に完了した後に、ユーザを特定の Web ページにリダイレクトするように WLAN を設定できます。 Web リダイレクトを設定して、ユーザにネットワークへの部分的または全面的なアクセス権を与えることができます。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。 RADIUS サーバ上で、リダイレクト先のページとリダイレクトが発生する条件を指定できます。 条件には、ユーザのパスワードの有効期限が近づいている場合、または使用を継続するためにユーザが料金を支払う必要がある場合などがあります。

RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。 さらにサーバから Cisco AV ペア「url-redirect-acl」も返された場合は、指定されたアクセス コントロール リスト（ACL）が、そのクライアントの事前認証 ACL としてインストールされます。 クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。

指定された URL（たとえば、パスワードの変更、請求書の支払い）でクライアントが特定の操作を完了すると、クライアントの再認証が必要になります。 RADIUS サーバから「url-redirect」が返されない場合、クライアントは完全に認証されたものと見なされ、トラフィックを渡すことを許可されます。

（注） 条件付き Web リダイレクト機能は、802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上で条件付き Web リダイレクトを設定できます。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークに完全にアクセスできます。 RADIUS サーバでリダイレクト ページを指定できます。 RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。 クライアントは、この段階で完全に認証され、RADIUS サーバが「url-redirect」を返さなくても、トラフィックを渡すことができます。

（注） スプラッシュ ページ Web リダイレクト機能は、802.1x キー管理を使用する 802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。 事前共有キー管理は、レイヤ 2 セキュリティ方式ではサポートされません。

ワイヤレス クライアントで実行するバック エンド アプリケーションがあり、通信に HTTP または HTTPS ポートを使用したとします。 実際の Web ページが開く前にアプリケーションが通信を開始すると、リダイレクト機能が Web パススルーで機能しません。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上でスプラッシュ ページ Web リダイレクトを設定できます。

RADIUS サーバの設定（GUI）

（注） 次の手順は、CiscoSecure ACS 固有の手順ですが、その他の RADIUS サーバでも同様の手順を使用します。

ステップ 1 CiscoSecure ACS メイン メニューから、[Group Setup] を選択します。

ステップ 2 [Edit Settings] をクリックします。

ステップ 3 [Jump To] ドロップダウン リストから [RADIUS (Cisco IOS/PIX 6.0)] を選択します。

ステップ 4 [[009\001] cisco-av-pair] チェックボックスをオンにします。

ステップ 5 [[009\001] cisco-av-pair] 編集ボックスに次の Cisco AV ペアを入力して、ユーザをリダイレクトする URL を指定するか、条件付 Web リダイレクトを設定する場合は、ダイレクトが発生する条件をそれぞれ指定します。

url-redirect=http://url

url-redirect-acl=acl_name

Web リダイレクトの設定

Web リダイレクトの設定（GUI）

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 必要な 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 2] タブを選択して、[WLANs > Edit]（[Security] > [Layer 2]）ページを開きます。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[802.1X] または [WPA+WPA2] を選択します。

ステップ 5 802.1X または WPA+WPA2 に対して任意の追加パラメータを設定します。

ステップ 6 [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 7 [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 8 [Web Policy] チェックボックスをオンにします。

ステップ 9 条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを有効化するオプションとして、[Conditional Web Redirect] または [Splash Page Web Redirect] のいずれかを選択します。 デフォルトでは、両方のパラメータが無効になっています。

ステップ 10 ユーザをコントローラ外部のサイトにリダイレクトする場合、[Preauthentication ACL] ドロップダウン リストから RADIUS サーバ上で設定された ACL を選択します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

Web リダイレクトの設定（CLI）

ステップ 1 条件付き Web リダイレクト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 cond-web-redir {**enable** | **disable**} *wlan_id*

ステップ 2 スプラッシュ ページ Web リダイレクト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 splash-page-web-redir {**enable** | **disable**} *wlan_id*

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

ステップ 4 特定の WLAN の Web リダイレクト機能の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*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
...
```

WLAN ごとのアカウンティング サーバの無効化（GUI）

（注） アカウンティング サーバを無効にすると、すべてのアカウンティング動作が無効となり、コントローラが WLAN に対するデフォルトの RADIUS サーバにフォールバックしなくなります。

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 変更する 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 [AAA Servers] タブを選択して、[WLANs > Edit]（[Security] > [AAA Servers]）ページを開きます。

ステップ 4 [Accounting Servers] の [Enabled] チェックボックスをオフにします。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

WLAN ごとのカバレッジ ホールの検出の無効化

（注） カバレッジ ホールの検出は、コントローラでグローバルに有効になっています。

（注） WLAN ごとにカバレッジ ホールの検出を無効にできます。 WLAN でカバレッジ ホールの検出を無効にした場合、カバレッジ ホールの警告はコントローラに送信されますが、カバレッジ ホールを解消するためのそれ以外の処理は行われません。 この機能については、ゲストのネットワーク接続時間は短く、モビリティが高いと考えられるようなゲスト WLAN に有用です。

WLAN 上のカバレッジ ホールの検出の無効化（GUI）

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 変更する 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。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを表示します。

ステップ 4 [Coverage Hole Detection Enabled] チェックボックスをオフにします。

（注） OEAP 600 シリーズ アクセス ポイントでは、カバレッジ ホールの検出はサポートされません。

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。

WLAN 上のカバレッジ ホールの検出の無効化（CLI）

ステップ 1 カバレッジ ホールの検出を無効にするには、次のコマンドを入力します。
config wlan chd *wlan-id* **disable**

（注） OEAP 600 シリーズ アクセス ポイントでは、カバレッジ ホールの検出はサポートされません。

ステップ 2 次のコマンドを入力して、設定を保存します。
save config

ステップ 3 特定の WLAN のカバレッジ ホールの検出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*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 2
Profile Name..................................... wlan2
Network Name (SSID).............................. 2
. . .
```

```
CHD per WLAN..................................... Disabled
```