目次

概要

このドキュメントでは、ワイヤレス LAN のコントローラ（WLC）でサポートされるレイヤ 2 およびレイヤ 3 のセキュリティ メカニズムの互換性マトリクスを示します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight AP および Cisco WLC の設定に関する基本的な知識
- Lightweight AP Protocol（LWAPP）に関する基本的な知識
- Wireless Security Solutions についての基本的な知識

使用するコンポーネント

このドキュメントの情報は、ファームウェア バージョン 7.0.116.0 が稼働する Cisco 4400/2100 シリーズ WLC に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Cisco Unified Wireless Network のセキュリティ ソリューション

Cisco Unified Wireless Network ではレイヤ 2 およびレイヤ 3 セキュリティ方式がサポートされます。

- レイヤ 2 セキュリティ
- レイヤ 3 セキュリティ（WLAN 向け）またはレイヤ 3 セキュリティ（ゲスト LAN 向け）

レイヤ 2 セキュリティは、ゲスト LAN ではサポートされていません。

ワイヤレス LAN コントローラでサポートされる各種レイヤ 2 およびレイヤ 3 セキュリティ方式を次の表に示します。 これらのセキュリティ方式は、WLAN の [WLANs] > [Edit] ページの [Security] タブでイネーブルにできます。

レイヤ 2 セキュリティのメカニズム		
パラメータ		**説明**
レイヤ2セキュリティ	なし	レイヤ 2 の選択はありません。
	[WPA+WPA2]	Wi-Fi Protected Access をイネーブルにするには、この設定を使用します。
	802.1X	802.1x 認証をイネーブルにするには、この設定を使用します。
	スタティック WEP	スタティック WEP 暗号化をイネーブルにするには、この設定を使用します。
	[Static WEP + 802.1x]	スタティック WEP パラメータと 802.1x パラメータの両方をイネーブルにするには、この設定を使用します。
	CKIP	Cisco Key Integrity Protocol（CKIP）をイネーブルにするには、この設定を使用します。 AP モデル 1100、1130、および 1200 では機能しますが、AP 1000 では機能しません。 この機能が動作するためには、Aironet IE を有効にする必要があります。 CKIP によって暗号キーが 16 バイトに拡張されます。
MACフィルタリング	MAC アドレスに基づいてクライアントをフィルタリングする場合に選択します。 [MAC Filters] > [New] ページで MAC アドレスを使用してクライアントをローカルに設定します。 そうでない場合は、RADIUS サーバのクライアントを構成します。	
レイヤ 3 セキュリティのメカニズム（WLAN 向け）		

パラメータ		説明
レイヤ3セキュリティ	なし	レイヤ 3 セキュリティは選択されません。
	IPSec	IPSec をイネーブルにするには、この設定を使用します。 IPSec を実装する前に、ソフトウェアが使用できるかどうかと、クライアント ハードウェアの互換性を確認する必要があります。 **注**IPSec をイネーブルにするには、オプションの VPN/Enhanced Security Module（暗号プロセッサ カード）が装着されている必要があります。 [Inventory] ページでコントローラにこれが装着されていることを確認します。
	VPN パススルー	VPN パススルーをイネーブルにするには、この設定を使用します。 **注**このオプションは、Cisco 5500 シリーズ コントローラおよび Cisco 2100 シリーズ コントローラでは使用できません。 ただし、ACL を使用してオープンな WLAN を作成することで、Cisco 5500 シリーズ コントローラまたは Cisco 2100 シリーズ コントローラでこの機能を複製できます。
Web Policy	Web ポリシーをイネーブルにするには、このチェックボックスをオンにします。 コントローラは、認証前にワイヤレス クライアントとの間で DNS トラフィックを転送します。 **注**[Web Policy] は、[IPSec] オプションまたは [VPN Pass-Through] オプションと組み合わせて使用することはできません。 次のパラメータが表示されます。 • 認証か。このオプションを選択する場合、ユーザはユーザ名 および パスワードのためにクライアントを無線ネットワークに接続している間プロンプト表示されます。 • パススルーか。このオプションを選択する場合、ユーザはユーザ名 および パスワード 認証なしでネットワークに直接アクセスできます。 • 条件付き Web リダイレクトか。このオプションを選択する場合、ユーザは特定の Webページに	

	802.1X 認証が正常に完了した後条件付きでリダイレクトすることができます。 リダイレクト ページ、および、RADIUS サーバでリダイレクトを実行する条件を指定できます。 • スプラッシュ ページ Web リダイレクトか。このオプションを選択する場合、ユーザは特定の Webページに 802.1X 認証が正常に完了した後リダイレクトされます。 ユーザは、リダイレクト後、ネットワークにフル アクセスできます。 RADIUS サーバでスプラッシュ Web ページを指定できます。 • MAC フィルタ失敗か。有効 Web 認証 MAC フィルタ失敗。
事前認証ACL	クライアントとコントローラ間のトラフィックに使用する ACL を選択します。
[Over-ride Global Config]	[Authentication] を選択すると表示されます。 [Web Login Page] で設定されたグローバル認証の設定を上書きするには、このボックスをオンにします。
[Web Auth type]	[Web Policy] と [Over-ride Global Config] を選択した場合に表示されます。 Web 認証タイプを選択します。 • 内部 • [Customized (Downloaded)] ログイン ページか。ドロップダウン リストからログイン ページを選択して下さい。ログイン障害 ページか。Web 認証が失敗した場合クライアントに表示する ログイン ページを選択して下さい。Logout ページか。システムからクライアントにときユーザログ 表示する ログイン ページを選択して下さい。

	• External（外部サーバへリダイレクト） URL ?外部サーバの URL を入力します。
[Email Input]	[Passthrough] を選択すると表示されます。 このオプションを選択すると、ネットワークへの接続時に電子メール アドレスの入力が求めれられます。

レイヤ 3 セキュリティのメカニズム（ゲスト LAN 向け）		
パラメータ		**説明**
レイヤ 3 セキュリティ	なし	レイヤ 3 セキュリティは選択されません。
	Web 認証	このオプションを選択すると、ネットワークへのクライアントの接続時にユーザに対してユーザ名とパスワードの入力が求められます。
	Web パススルー	このオプションを選択すると、ユーザとパスワードによる認証を行わずにネットワークに直接アクセスできます。
事前認証 ACL		クライアントとコントローラ間のトラフィックに使用する ACL を選択します。
[Over-ride Global Config]		[Web Login Page] で設定されたグローバル認証の設定を上書きするには、このボックスをオンにします。
[Web Auth type]		[Over-ride Global Config] を選択すると表示されます。Web 認証タイプを選択します。 • 内部 • [Customized (Downloaded)] ログイン ページか。ドロップダウン リストからログイン ページを選択して下さい。ログイン障害ページか。Web 認証が失敗した場合クライアントに表示する ログイン ページを選択して下

	さい。Logout ページか。システムからクライアントにときユーザログ 表示する ログイン ページを選択して下さい。 • External (外部サーバへリダイレクト) URL ?外部サーバの URL を入力します。
[Email Input]	[Web Passthrough] を選択すると表示されます。 このオプションを選択すると、ネットワークへの接続時に電子メール アドレスの入力が求めれられます。

注コントローラ ソフトウェア リリース 4.1.185.0 以降では、CKIP はスタティック WEP でのみ使用できます。 Dynamic WEP での使用はサポートされていません。 したがって、ダイナミック WEP で CKIP を使用するように設定されたワイヤレス クライアントは、CKIP 用に設定されているワイヤレス LAN にアソシエートできません。 CKIP なしでダイナミック WEP を使用する (安全性がより低い) か、または TKIP または AES で WPA/WPA2 を使用する (安全性がより高い) ことを推奨します。

ワイヤレス LAN コントローラ レイヤ2 か。 レイヤ3 セキュリティ 互換性 マトリックス

ワイヤレス LAN のセキュリティを設定するときには、レイヤ 2 およびレイヤ 3 のセキュリティ方式を組み合わせて使用できます。 ただし、レイヤ 2 セキュリティ方式と組み合わせて使用できない レイヤ 3 セキュリティ方式があります。 次の表に、ワイヤレス LAN のコントローラでサポートされるレイヤ 2 およびレイヤ 3 のセキュリティ方式の互換性マトリクスを示します。

レイヤ 2 セキュリティのメカニズム	**レイヤ 3 セキュリティのメカニズム**	**互換性**
なし	なし	有効
[WPA+WPA2]	なし	有効
[WPA+WPA2]	Web 認証	Invalid
[WPA-PSK/WPA2-PSK]	Web 認証	有効
[WPA+WPA2]	Web パススルー	Invalid
[WPA-PSK/WPA2-PSK]	Web パススルー	有効
[WPA+WPA2]	条件付き Web リダイレクト	有効
[WPA+WPA2]	スプラッシュ ページ Web リダイレクト	有効

[WPA+WPA2]	[VPN-PassThrough]	有効
802.1X	なし	有効
802.1X	Web 認証	Invalid
802.1X	Web パススルー	Invalid
802.1X	条件付き Web リダイレクト	有効
802.1X	スプラッシュ ページ Web リダイレクト	有効
802.1X	[VPN-PassThrough]	有効
スタティック WEP	なし	有効
スタティック WEP	Web 認証	有効
スタティック WEP	Web パススルー	有効
スタティック WEP	条件付き Web リダイレクト	Invalid
スタティック WEP	スプラッシュ ページ Web リダイレクト	Invalid
スタティック WEP	[VPN-PassThrough]	有効
[Static-WEP+ 802.1x]	なし	有効
[Static-WEP+ 802.1x]	Web 認証	Invalid
[Static-WEP+ 802.1x]	Web パススルー	Invalid
[Static-WEP+ 802.1x]	条件付き Web リダイレクト	Invalid
[Static-WEP+ 802.1x]	スプラッシュ ページ Web リダイレクト	Invalid
[Static-WEP+ 802.1x]	[VPN-PassThrough]	Invalid
CKIP	なし	有効
CKIP	Web 認証	有効
CKIP	Web パススルー	有効
CKIP	条件付き Web リダイレクト	Invalid
CKIP	スプラッシュ ページ Web リダイレクト	Invalid
CKIP	[VPN-PassThrough]	有効

関連情報

- Wireless LAN Controller と Lightweight アクセス ポイントの基本設定例
- Wireless LAN Controller (WLC) への Lightweight AP (LAP) の登録

- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0.116.0
- Wireless LAN Controller (WLC) に関する FAQ
- テクニカルサポートとドキュメント - Cisco Systems