WLCレイヤ2およびレイヤ3セキュリティの互換性マトリクス

内容

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 に関する基本的な知識

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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	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	

ング	、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を有効**にするには、オプションの VPN/Enhanced Security Module(ESM) (暗号化プロセッサカード) をインストールする必要があります。[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 Pass-Through]	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ポリシーは、IPsecまたはVPNパススルー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。 • [Authentication]：このオプションを選択すると、ワイヤレス 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。 • [Passthrough]：このオプションを選択すると、ユーザはユーザ名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。 • [条件付きWebリダイレクト(Conditional Web Redirect)]：このオプションを選択すると、802.1X認証が正常に完了した後で、ユーザを特定のWebページに条件付きでリダイレクトできます。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(Splash	

	Page Web Redirect)]：このオプションを選択すると、802.1X認証が正常に完了した後で、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。 • [On MAC Filter failure]：MAC フィルタが失敗した場合に Web 認証をイネーブルにします。
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]	[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)] [Login Page]：ドロップダウン リストからログイン ページを選択します。[Login Failure page]：Web 認証に失敗した場合にクライアントに対して表示するログイン ページを選択します。[Logout page]：ユーザがシステムからログアウトするときにクライアントに対して表示するログインページを選択します。 • 外部（外部サーバにリダイレクト）[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。
	We	このオプションを選択すると、ユーザとパス

	b パススルー	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)] [Login Page]：ドロップダウン リストからログイン ページを選択します。[Login Failure page]：Web 認証に失敗した場合にクライアントに対して表示するログイン ページを選択します。[Logout page]：ユーザがシステムからログアウトするときにクライアントに対して表示するログイン ページを選択します。 • 外部（外部サーバにリダイレクト）[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 レイヤ 3 セキュリティの互換性マトリクス

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	Invali

	Web リダイレクト	d
CKIP	[VPN-PassThrough]	有効

関連情報

- ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本設定例
- ワイヤレス LAN コントローラ（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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。