# WAPでのワイヤレスセキュリティ設定の設定

#### 概要

ワイヤレスアクセスポイント(WAP)でワイヤレスセキュリティを設定することは、ワイヤレ スデバイスのプライバシーを侵害する可能性のある侵入者や、ワイヤレスネットワークを介 して送信するデータからワイヤレスネットワークを保護するために非常に重要です。 MACフィルタ、Wi-Fi Protected Access(WPA/WPA2) Personal、およびWPA/WPA2 Enterpriseを設定して、ワイヤレスネットワークのワイヤレスセキュリティを設定できます。

MACフィルタリングは、ワイヤレスクライアントがMACアドレスを使用してネットワーク にアクセスするようにフィルタリングするために使用されます。クライアントリストは、設 定に応じて、リスト上のアドレスがネットワークにアクセスすることを許可またはブロック するように設定されます。MACフィルタリングの詳細については、ここをクリ<u>ックしま</u>す 。

WPA/WPA2 PersonalおよびWPA/WPA2 Enterpriseは、ワイヤレスネットワーク上で送信さ れるデータを暗号化してプライバシーを保護するために使用されるセキュリティプロトコル です。WPA/WPA2は、IEEE標準802.11Eおよび802.11iと互換性があります。Wired Equivalent Privacy(WEP)セキュリティプロトコルと比較して、WPA/WPA2は認証および暗 号化機能を改善しました。

WPA/WPA2 Personalは家庭用で、WPA/WPA2 Enterpriseはビジネス規模のネットワーク用 です。WPA/WPA2 Enterpriseは、WPA/WPA2 Personalと比較して、ネットワークのセキュ リティと集中制御を強化します。

このシナリオでは、WPA/WPA2パーソナル設定とエンタープライズ設定を使用してネット ワークを侵入者から保護するために、WAPでワイヤレスセキュリティを設定します。

### 目的

この記事では、ワイヤレスネットワークのセキュリティとプライバシーを向上させるために 、WPA/WPA2パーソナルおよびエンタープライズセキュリティプロトコルを設定する方法 を説明します。

**注**:この記事では、WAPでService Set Identifier(SSID)またはWireless Local Area Network(WLAN)がすでに作成されていることを前提としています。

### 該当するデバイス

- •WAP100シリーズ
- •WAP300シリーズ
- •WAP500シリーズ

### [Software Version]

- 1.0.2.14 WAP131、WAP351
- 1.0.6.5 WAP121、WAP321
- 1.3.0.4 WAP371

- 1.1.0.7 WAP150、WAP361
- 1.2.1.5 WAP551、WAP561
- 1.0.1.11 WAP571、WAP571E

## ワイヤレスセキュリティの設定

#### WPA/WPA2 Personalの設定

ステップ1:アクセスポイントのWebベースのユーティリティにログインし、[**Wireless**]>[ Networks]を選択します。

**注**:次の図では、例としてWAP361のWebベースのユーティリティを使用しています。メニ ューのオプションは、デバイスのモデルによって異なります。

_	Getting Started
	Run Setup Wizard
۲	Status and Statistics
۲	Administration
۲	LAN
ſ	Wireless
	Radio Rogue AP Detection Networks Wireless Multicast Forward

ステップ2:[Virtual Access Points (SSIDs)]領域で、設定するSSIDのチェックボックスをオンにし、[Edit]をクリックします。

注:この例では、VAP1が選択されています。

Virt	Virtual Access Points (SSIDs)								
	No.	Enable	Add New VLAN	SSID Name	Broadcast	Security	MAC Filter	Isolation	Band Steer
	0		1 🔻	ciscosb	×.	None •	Disabled •		
	- 1	2	1 🔻	Cisco_Lobby		None •	Disabled •		
	Add	E	dit Delete						
Sav	e								

ステップ3:[セキュリティ]ドロップダウンリストから[WPA Personal]をクリックします。

	VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security
	0		1 •	ciscosb	×.	None •
•	1	2	1 •	Cisco_Lobby	<b>2</b>	None 🔹
	\dd		dit Delete			None
	Auu		uit Delete			WPA Personal
						WPA Enterprise

ステップ4:チェックボックスをオンにして、WPAバージョン(WPA-TKIPまたはWPA2-AES)を選択します。同時に二つ選ぶも可なり。

- WPA-TKIP:Wi-Fi Protected Access-Temporal Key Integrity Tool。ネットワークには、元のWPAおよびTKIPセキュリティプロトコルのみをサポートするクライアントステーションがあります。アクセスポイントにWPA-TKIPのみを選択することは、最新のWi-Fi Alliance要件に従って許可されないことに注意してください。
- WPA2-AES:Wi-Fi Protected Access-Advanced Encryption Standard。ネットワーク上の すべてのクライアントステーションは、WPA2およびAES-CCMP暗号化/セキュリティ プロトコルをサポートします。このWPAバージョンは、IEEE 802.11i規格に準拠した最 高のセキュリティを提供します。最新のWi-Fi Alliance要件に従って、WAPはこのモー ドを常にサポートする必要があります。
- 注:この例では、両方のチェックボックスがオンになっています。

WPA Versions:	WPA-TKIP	WPA2-AES
Key:		(Range: 8-63 Characters)
	Show Key as Clear	ar Text
Key Strength Meter:	E	Below Minimum
Broadcast Key Refresh Rate	300	Sec (Range: 0-86400, 0 =

ステップ5:8 ~ 63文字で構成されるパスワードを作成し、[キー]フィールドに入力します。

WPA Versions:	🗹 wpa-tkip	WPA2-AES
Key:		(Range: 8-63 Characters)
Key Strength Meter:	Show Key as Clea	r Text trong

**注**:[クリアテキストとしてキ**ーを表示]ボックスをオンに**すると、作成したパスワードを表示できます。

WPA Versions:	VPA-TKIP	WPA2-AES
Key:	Str0ngPassw0rd	(Range: 8-63 Characters)
Key Strength Meter:	Chow Key as Clear	Text rong

ステップ6:(オプション)[Broadcast Key Refresh Rate]フィールドで、このVAPに関連付け られているクライアントのブロードキャスト(グループ)キーが更新される値または間隔を 入力します。デフォルトは300秒で、有効な範囲は0 ~ 86400秒です。値0は、ブロードキ ャストキーが更新されていないことを示します。

WPA Versions:	WPA-TKIP	WPA2-AES
Key:	•••••	(Range: 8-63 Characters)
	Show Key as Clear 1	Text
Key Strength Meter:	Ses	sion Key Refresh Rate
Broadcast Key Refresh Rate	300	Sec (Range: 0-86400,0 = Disable, Default: 300)

ステップ7:[Save]をクリ**ックします**。

	No.	Enable	Add New VLAN	SSID Name
	0		1 •	ciscosb
•	1	2	1 •	Cisco_Lobby
A	dd	E	dit Delete	

これで、WAPでWPA Personalが設定されました。

#### WPA/WPA2 Enterpriseの設定

ステップ1:アクセスポイントのWebベースのユーティリティにログインし、[**Wireless**]>[ Networks]を選択します。

注:次の図では、例としてWAP361のWebベースのユーティリティを使用しています。

Getting Started			
Run Setup Wizard			
<ul> <li>Status and Statistics</li> </ul>			
<ul> <li>Administration</li> </ul>			
► LAN			
Wireless			
Radio			
Rogue AP Detection			
Networks			
Wireless Multicast Forward			

ステップ2:[Virtual Access Points (SSIDs)]領域で、設定するSSIDを確認し、その下の[**Edit**]ボタンをクリックします。

l	Virtual Access Points (SSIDs)									
L		VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
L		0	2	1 •	ciscosb	×.	None •	Disabled •		
	0	1	e.	1 •	Cisco_Lobby		None •	Disabled •		
		Add	E	dit Delete						
	Save									

ステップ3:[セキュリティ]ドロップダウンリストから[WPA Enterprise]を選択します。

Virtual Access Points (SSIDs)						
	VAP No.	Enable	VLAN ID Add New VLAN	SSID Name	SSID Broadcast	Security
	0	1	1 🔻	ciscosb	1	None •
		2	1 •	Cisco_Lobby	2	WPA Enterprise 🔹
		•				None WPA Personal
						WPA Enterprise

ステップ4:WPAバージョン(WPA-TKIP、WPA2-AES、および事前認証の有効化)を選択します。

事前認証の有効化:WPA2-AESのみ、またはWPAバージョンとしてWPA-TKIPとWPA2-AESの両方を選択した場合、WPA2-AESクライアントの事前認証を有効にできます。WPA2ワイヤレスクライアントが事前認証パケットを送信するようにするには、このオプションをオンにします。事前認証情報は、クライアントが現在使用しているWAPデバイスからターゲットWAPデバイスにリレーされます。この機能を有効にすると、複数のアクセスポイント(AP)に接続するローミングクライアントの認証を高速化できます。

**注**:WPA-TKIPをWPAバージョンに選択した場合、元のWPAはこの機能をサポートしていないため、このオプションは適用されません。

ide Details					
WPA Versions:  WPA-TKIP WPA2-AES Knable pre-authentication					
<ul> <li>Use global RADIUS server settings</li> </ul>					
Server IP Address Type:    IPv4    IPv6					
Server IP Address-1:	192.168.1.101	(x000.0000.0000)			
Server IP Address-2:		(x000.0000.0000)			
Server IP Address-3:		(3000.3000.3000)			
Server IP Address-4:		(3000.3000.3000)			
Key-1:		(Range: 1 - 64 Characters)			
Key-2:		(Range: 1 - 64 Characters)			
Key-3:		(Range: 1 - 64 Characters)			
Key-4:		(Range: 1 - 64 Characters)			
Enable RADIUS Acco	unting				
Active Server:	Server IP Address-1	•			
Broadcast Key Refresh R	ate: 300	Sec (Range: 0-86400,0 = Disable, Default: 300)			
Session Key Refresh Rate	e: 0	Sec (Range: 30-86400, 0 = Disable, Default: 0)			

ステップ5:(オプション)[Use global RADIUS server settings]**チェックボックスをオフ**にして、設定を編集します。

WPA Versions: VPA-TKIP VPA2-AES				
OUse global RADIUS server settings				
Server IP Address Type:    IPv4    IPv6				
Server IP Address-1: 192.	168.1.101	(XXXX,XXXX,XXXX)		
Server IP Address-2:		(XXXX,XXXX,XXXX)		
Server IP Address-3:		(2000.2000.2000)		
Server IP Address-4:		(2000.2000.2000)		
Key-1:	•••••	(Range: 1 - 64 Characters)		
Key-2:		(Range: 1 - 64 Characters)		
Key-3:		(Range: 1 - 64 Characters)		
Key-4:		(Range: 1 - 64 Characters)		
Enable RADIUS Accounting				
Active Server:	Server IP Address-	1 💌		
Broadcast Key Refresh Rate:	300	Sec (Range: 0-86400,0 = Disable, Default: 300)		
Session Key Refresh Rate:	0	Sec (Range: 30-86400, 0 = Disable, Default: 0)		

ステップ6:(オプション)正しいサーバーIPアドレスの種類のラジオボ**タンをクリックしま** す。

注:この例では、IPv4が選択されています。

WPA Versions: VPA-TKIP VPA2-AES				
Use global RADIUS server settings				
Server IP Address Type:  IPv4  IPv6				
Server IP Address-1:	192.168.1.101	(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
Server IP Address-2:		(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
Server IP Address-3:		(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
Server IP Address-4:		(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
Key-1:	•••••	(Range: 1 - 64 Characters)		
Key-2:		(Range: 1 - 64 Characters)		
Key-3:		(Range: 1 - 64 Characters)		
Key-4:		(Range: 1 - 64 Characters)		
Enable RADIUS Accounting				
Active Server: Server IP Address-1				
Broadcast Key Refresh R	ate: 300	Sec (Range: 0-86400,0 = Disable, Default: 300)		
Session Key Refresh Rat	e: 0	Sec (Range: 30-86400, 0 = Disable, Default: 0)		

ステップ7:[Server IP Address]フィールドにRADIUSサーバのIPアドレ*スを入力*します。 **注:** この例では、192.168.1.101を使用します。

WPA Versions: VPA-TKIP VPA2-AES				
Use global RADIUS server settings				
Server IP Address Type: <a>IPv4</a> IPv6				
Server IP Address-1: 192.168.1.101	(XXXX,XXXX,XXXX)			
Server IP Address-2:	(XXXX,XXXX,XXXX)			
Server IP Address-3:	(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX			
Server IP Address-4:	(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX			
Key-1:	••• (Range: 1 - 64 Characters)			
Key-2:	(Range: 1 - 64 Characters)			
Key-3:	(Range: 1 - 64 Characters)			
Key-4:	(Range: 1 - 64 Characters)			
Enable RADIUS Accounting				
Active Server: Server IP Addres	ss-1 💌			
Broadcast Key Refresh Rate: 300	Sec (Range: 0-86400,0 = Disable, Default: 300)			
Session Key Refresh Rate: 0	Sec (Range: 30-86400, 0 = Disable, Default: 0)			

ステップ8:[Key] フィールドに、WAPがRADIUSサーバへの認証に使用するRADIUSサーバ に対応するパスワードキーを入力します。1 ~ 64文字の英数字と特殊文字を使用できます 。

**注**:キーは大文字と小文字が区別され、RADIUSサーバで設定されているキーと一致してい る必要があります。

ステップ9:(オプション)WAPと通信するネットワーク内のすべてのRADIUSサーバに対し て、ステップ7 ~ 8を繰り返します。

WPA Versions: VPA-TKIP VPA2-AES				
Use global RADIUS server settings				
Server IP Address Type:    IPv4    IPv6				
Server IP Address-1:	192.168.1.101	(X00CX00CX00C)		
Server IP Address-2:		(x000.x000.x000)		
Server IP Address-3:		(x00C300C300C)		
Server IP Address-4:		(x00C300C300X)		
Key-1:	•••••	(Range: 1 - 64 Characters)		
Key-2:		(Range: 1 - 64 Characters)		
Key-3:		(Range: 1 - 64 Characters)		
Key-4:		(Range: 1 - 64 Characters)		
Enable RADIUS Accounting				
Active Server:	Server IP Address-	1 💌		
Broadcast Key Refresh R	ate: 300	Sec (Range: 0-86400,0 = Disable, Default: 300)		
Session Key Refresh Rat	e: 0	Sec (Range: 30-86400, 0 = Disable, Default: 0)		

ステップ10:(オプション)[EnableRADIUS Accounting] チェックボックスをオンにすると 、ユーザが消費したリソース(システム時間、送信データ量)の追跡と測定が可能になりま す。 この機能を有効にすると、プライマリサーバとバックアップサーバの両方でRADIUSア カウンティングが可能になります。

WPA Versions: VPA-TKIP VPA2-AES				
Enable pre-authentication				
✓ Use global RADIUS server settings				
Server IP Address Type: <ul> <li>IPv4</li> <li>IPv6</li> </ul>				
Server IP Address-1:	192.168.1.101	(XXXX,XXXX,XXXX)		
Server IP Address-2:		(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		
Server IP Address-3:		(XXXX,XXXX,XXXX)		
Server IP Address-4:		(XXXX,XXXX,XXXX)		
Key-1:	••••••	(Range: 1 - 64 Characters)		
Key-2:		(Range: 1 - 64 Characters)		
Key-3:		(Range: 1 - 64 Characters)		
Key-4:		(Range: 1 - 64 Characters)		
Enable RADIUS Accounting				
Active Server:	Server IP Address-	1 ▼		
Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400,0 = Disable, Default: 300)				
Session Key Refresh Rat	te: 0	Sec (Range: 30-86400, 0 = Disable, Default: 0)		

ステップ11:をクリックします Save

これで、WAPでWPA/WPA2 Enterpriseセキュリティが正しく設定されました。