



SonicOS 7

アクセスポイント

管理者ガイド

SONICWALL®

目次

設定	5
アクセス ポイントの同期	6
プロビジョニングの概要	6
プロビジョニング プロファイルの作成/変更	7
プロビジョニング プロファイルの追加/編集 - はじめに	8
プロビジョニング プロファイルの一般設定	9
プロビジョニング プロファイルの 5GHz/2.4GHz 無線の基本設定	10
プロビジョニング プロファイルの 5GHz/2.4GHz 無線の詳細設定	22
プロビジョニング プロファイルの WIDP のセンサー設定	28
プロビジョニング プロファイルのメッシュ ネットワーク設定	28
プロビジョニング プロファイルの 3G/4G/LTE WWAN 設定	30
プロビジョニング プロファイルの Bluetooth LE 設定	32
アクセス ポイントプロファイルの削除	33
製品特有の設定に関する注意事項	33
アクセス ポイントの管理	34
アクセス ポイントオブジェクトの削除	34
アクセス ポイントオブジェクトの再起動	35
アクセス ポイントオブジェクトの変更	35
ファームウェアの管理	36
ファームウェアの管理について	36
最新の SonicWall ファームウェアの入手	37
特定の URL からのファームウェアのダウンロード	38
ファームウェアをアクセスポイントにアップロードする	38
フロアプランの表示	40
フロアプランの管理	41
フロアプランの選択	41
フロアプランの作成	41
フロアプランの編集	41
測定用尺度の設定	42
アクセスポイントの管理	42
利用可能なデバイス	43
追加されたアクセスポイント	43
アクセスポイントの削除	43
画像としてエクスポート	44
コンテキストメニュー	44

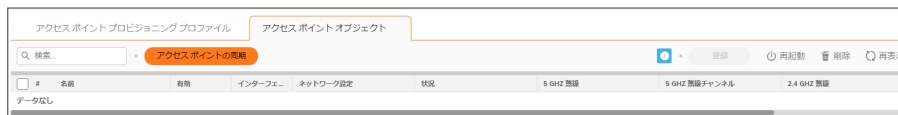
ステーション状況	45
侵入検知サービス	46
アクセスポイントのスキャン	47
アクセスポイントの許可	48
高度なIDP	49
プロファイルで無線IDP を有効にする	49
無線IDPの設定	50
KRACK スニッファ パケットの表示	51
パケットキャプチャ	53
仮想アクセスポイント	54
VAP を設定する前に	56
VAP のニーズを確定する	56
セキュリティ設定を確定する	56
サンプル ネットワーク定義	57
前提条件	57
VAP 設定ワークシート	57
アクセスポイント VAP 設定タスクリスト	58
仮想アクセスポイントプロファイル	59
仮想アクセスポイントスケジュールの設定	60
仮想アクセスポイントプロファイル設定	60
RADIUS サーバと RADIUS アカウント	61
WPA-PSK > WPA2-PSK 暗号化の設定	63
WEP 暗号化の設定	63
ACL 強制	63
リモート MAC アドレス アクセス制御の設定	64
仮想アクセスポイント	65
「一般」タブ	65
「詳細」タブ	66
仮想アクセスポイントグループ	66
RF 監視	68
前提条件	69
RF 監視の要約	69
802.11 一般フレーム設定	70
802.11 管理フレーム設定	70
802.11 データ フレーム設定	71
検出された RF 脅威ステーション	72
警戒リストへの脅威ステーションの追加	73
RF 監視の活用法	74
センサー ID の使用による RF 脅威の場所の判別	74
RSSI の使用による RF 脅威の近接性の判別	75

RF 解析	77
RF 解析の選択	77
RF 環境	77
SonicWall アクセスポイントにおける RF 解析の使用	78
RF スコアとは	79
チャンネル使用率に関するグラフと情報	79
過負荷チャンネルの表示	80
RFA 高干渉チャンネル	81
RF スペクトラム	82
FairNet	84
サポート対象プラットフォーム	85
FairNet の機能	85
管理インターフェースの概要	85
FairNet の設定	86
Wi-Fi マルチメディア	88
WMM アクセス種別	88
アクセス種別へのトラフィックの割り当て	90
ファイアウォール サービスとアクセス ルールの指定	90
VLAN タグ付け	90
Wi-Fi マルチメディア パラメータの設定	91
WMM の設定	91
アクセス ポイントの WMM プロファイルの作成	92
3G/4G/LTE WWAN	93
Bluetooth LE デバイス	94
BLEスキャンデータの表示	94
無線リソース管理	96
無線リソース管理の設定	96
動的チャンネル選択の設定	98
SonicWall サポート	100
このドキュメントについて	101

設定

無線アクセスポイントを提供するうえで最も効率的な方法は、SonicOS ファイアウォールに自動的にアクセスポイントを検出させて、既定プロファイルのうちの 1 つを使用することです。SonicOS には、SonicWall アクセスポイントの各世代に合わせて 1 つずつ、合計 4 つの既定プロファイル (SonicPointN、SonicPointNDR、SonicPointACe/ACi/N2、SonicWave) が提供されています。これらはそのまま使用することも、設定に合わせてカスタマイズすることもできます。SonicWall アクセスポイントの種類に基づいて、新規のプロファイルを作成することもできます。

「デバイス > アクセスポイント > 設定」ページには、情報メッセージが表示され、利用可能なアクセスポイントのファームウェアバージョンが示されます。



アクセスポイントプロファイルは、「アクセスポイントプロビジョニングプロファイル」タブに表示されます。各プロファイルを編集するか、新しいプロファイルを追加できます。

「アクセスポイントオブジェクト」タブには、接続されたアクセスポイントの設定が表示されます。また、それらを編集したりその他のアクションを実行したりするための編集アイコンがあります。

① **補足:** 無線 LAN を無効にすると、すべてのアクセスポイントと無線関連のページが消えます。ゾーン種別から無線ゾーンが削除されます。また、既存の WLAN ゾーンやオブジェクトを一切編集できなくなります。

トピック:

- [アクセスポイントの同期](#)
- [プロビジョニングの概要](#)
- [プロビジョニングプロファイルの作成/変更](#)
- [アクセスポイントの管理](#)

アクセスポイントの同期

「デバイス>アクセスポイント>設定」ページの上にある「アクセスポイントの同期」をクリックして、SonicWall 装置から WLAN ゾーンへクエリを発行します。接続されているすべてのアクセスポイントが、それぞれの現在の設定と統計を装置に報告します。同時に SonicOS は、新規に接続されてファイアウォールにまだ登録されていないアクセスポイントの存在を特定しようと試みます。

- ① **補足:** このボタンを選択すると、すべてのアクセスポイントに対してポーリングが行われますが、それらに設定がプッシュされることはありません。

プロビジョニングの概要

SonicPoint/SonicWave プロビジョニング プロファイルは、分散無線アーキテクチャ全体で複数のアクセスポイントの設定とプロビジョニングを行うための拡張性を備え、高度に自動化された方法を提供します。

SonicPoint/SonicWave プロファイルの定義には、2.4GHz および 5GHz の無線設定、SSID、動作チャンネルなど、SonicWall アクセスポイントで構成できるすべての設定が含まれます。

アクセスポイントプロファイルを定義し終えたら、そのプロファイルを実無線ゾーンに適用することができます。各無線ゾーンを、それぞれ 1 つのアクセスポイントプロファイルを使用して構成することができます。1 つのプロファイルを任意の数のゾーンに適用することもできます。その後、アクセスポイントがゾーンに接続すると、そのゾーンに割り当てられたプロファイルを使用して自動的にプロビジョニングされます。

アクセスポイントを最初に接続して電源を入れると、工場出荷時の既定の設定が割り当てられます (IP アドレス: 192.168.1.20、ユーザ名: admin、パスワード: password)。初期化時に、アクセスポイントは通信相手となる SonicOS デバイスを探します。SonicOS デバイスを起動すると、そのデバイスも SonicWall ディスカバリプロトコルを介してアクセスポイントを検索します。アクセスポイントと通信相手の SonicOS デバイスが互いに検出する場合、両装置間で暗号化されたデータ交換により通信が実行されます。その際、関連する無線ゾーンに割り当てられたプロファイルを使用して、新たに追加されたアクセスポイント装置が自動的にプロビジョニングされます。

プロビジョニングプロセスの一環として、SonicOS は検出されたアクセスポイントに一意の名前を割り当て、その MAC アドレス、インターフェース、検出されたゾーンを記録します。プロファイルの一部の場合、アクセスポイントが WPA-EAP をサポートするために認証サーバと通信できるように、IP アドレスを自動的に割り当てることもできます。SonicOS は、該当するゾーンに関連付けられたプロファイルを使用して、2.4GHz および 5GHz の無線設定を構成します。

プロファイルに変更を行っても、すでにプロビジョニングされて動作状態にある装置には影響しません。動作しているアクセスポイントに対して設定変更を行う方法は 2 通りあります。

- 手動設定変更による方法
単一または小規模な変更を行う場合に適しています。とりわけ、個々のアクセスポイントで、そのゾーンに割り当てられたプロファイルとは異なる設定が必要なときに適した方法です。
- プロビジョニング解除による方法
アクセスポイントを削除することにより、その装置に対するプロビジョニングが有効に取り消されます。当該装置の設定はクリアされ、相手の SonicOS デバイスとの間で新規にプロビジョニングプロセスが自動的に行われる状態になります。この方法はゾーンのプロファイルを更新または変更し、その変更内容を伝播するように設定する場合に便利です。アクセスポイントでファームウェアを更新したり、単に複数のアクセスポイントを一定の制御されたやり方で自動的に更新したりするときに、この方法が使用できます。すべてのアクセスポイントを一度に変更すると、サービスに混乱が生じる可能性があるためです。

プロビジョニングプロファイルの作成/変更

「デバイス>アクセスポイント>設定」ページで、個別のオブジェクトだけでなく、プロビジョニングプロファイルの構成と管理を行うことができます。任意の数のプロファイルを追加することができます。

- ① **補足:** SonicPoint AC とは、SonicPoint ACe/ACi/N2 のことです。SonicPoint は、すべての SonicPoint デバイスを指します。SonicWave とは、SonicWave 432e/432i/432o/224w/231c/231o を指します。SonicPoint AC は、SonicOS 6.2.2 以降を実行する装置でサポートされますが、SonicWave デバイスは SonicOS 6.5 以降でサポートされます。

「デバイス>アクセスポイント>設定」ページに移動します。「SonicPoint/SonicWave プロビジョニングプロファイル」セクションに、4つの既定 SonicOS プロファイルと共に、作成した個別プロファイルが表示されます。既定のプロビジョニングプロファイルを変更する場合、プロファイルにマウスカーソルを重ね、**編集アイコン**をクリックし、適切な変更を行ってください。

#	名前	選択ゾーン	5 GHz 無線	5 GHz 無線チャンネル	2.4 GHz 無線	2.4 GHz 無線チャンネル
1	SonicPointN	WLAN	SSID: sonicwall-C9F0 Mode: 5GHz n/a only	Band: Auto Channel: Auto	SSID: sonicwall-C9F0 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto
2	SonicPointNDR	WLAN	SSID: sonicwall-C9F0 Mode: 5GHz n/a only	Band: Auto Channel: Auto	SSID: sonicwall-C9F0-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto
3	SonicPointACeACiN2	WLAN	SSID: sonicwall-C9F0 Mode: 5GHz n/a/b/c	Band: Auto Channel: Auto	SSID: sonicwall-C9F0-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto
4	SonicWave	WLAN	SSID: sonicwall-C9F0 Mode: 5GHz n/a/b/c	Band: Auto Channel: Auto	SSID: sonicwall-C9F0-1 Mode: 2.4GHz n/g/b	Band: Auto Channel: Auto

- ① **重要:** SonicPoint/SonicWave プロビジョニングプロファイルの作成または変更はすべての種類のアクセスポイントを通じて同様であるため、このセクションでは SonicWave デバイスに対して新規プロファイルを追加する方法を確認します。一般的な手順に対して重大な違いがある場合には注記して、このセクションの後の方で詳細を説明します。

- ① **補足:** SonicWave が提供するプロビジョニングプロファイルは削除することができません。したがって、対応する**削除アイコン**は淡色表示になって無効になっています。

「新規プロファイルの追加」オプションには、類似の設定をグループ化した複数の画面があります。手順は、それらの画面に合わせてグループ化されています。

トピック:

- [プロビジョニングプロファイルの追加/編集 - はじめに](#)
- [プロビジョニングプロファイルの一般設定](#)
- [プロビジョニングプロファイルの 5GHz/2.4GHz 無線の基本設定](#)
- [プロビジョニングプロファイルの 5GHz/2.4GHz 無線の詳細設定](#)
- [プロビジョニングプロファイルの WIDP のセンサー設定](#)
- [プロビジョニングプロファイルのメッシュネットワーク設定](#)
- [プロビジョニングプロファイルの Bluetooth LE 設定](#)
- [アクセスポイントプロファイルの削除](#)
- [製品特有の設定に関する注意事項](#)

プロビジョニング プロファイルの追加/編集 - はじめに

新しいプロファイルを追加するには、以下の手順に従います

1. 「デバイス>アクセスポイント>設定>アクセスポイントプロビジョニングプロファイル」ページに移動します。
2. 「新しいプロファイルの追加」ドロップダウンで、作成するプロファイルの種別を選択します。この例では、「SonicWave プロファイル」が選択されています。

① | **補足:** 既存のプロファイルを変更するには、更新したいプロファイルの**編集**アイコンをクリックします。

SonicWave プロファイルの追加

< 一般 5GHz 無線基本 5GHz 無線詳細 2.4GHz 無線基本 2.4GHz 無線詳細 センサー メッシュネットワーク 3G/4G/LTE WW >

一般設定

有効

設定を保持 編集

RF 監視を有効にする

LED を有効にする

低電力モードを有効にする

PoE 出力

名前開始文字列

国コード: United States-US

EAPOL バージョン v2

帯域誘導モード 無効

仮想アクセスポイント設定

5GHz 無線仮想アクセスポイントグループ -- 仮想アクセスポイントオブジェクトグループの... ①

2.4GHz 無線仮想アクセスポイントグループ -- 仮想アクセスポイントオブジェクトグループの... ①

動的 VLAN ID の割り当て

5GHz 無線で動的 VLAN ID 割り当てを有効にする 編集

2.4GHz 無線で動的 VLAN ID 割り当てを有効にする 編集

OK キャンセル

プロビジョニング プロファイルの一般設定

「一般」画面でオプションを構成するには、以下の手順に従います

1. 「SonicWave 設定」を設定します。

オプション	動作
有効	選択すると、SonicWave アクセス ポイントが有効になります。既定で、このオプションは有効になっています。
設定を保持	選択すると、装置が次に再起動されるまでカスタマイズした設定が保持されます。「編集」オプションが有効になると、「設定を保持」ダイアログが表示されます。どの設定を保持する必要があるかをカスタマイズできます。
RF 監視を有効にする	選択すると、無線 RF 脅威のリアルタイム監視と管理が有効になります。
LED を有効にする	選択すると、SonicWave LED が有効になります。このチェックボックスにチェックを入れないまま（既定値）にしておくと、LED は無効のままになります。
低電力モードを有効にする	選択すると、SonicWave が低電力モードで動作することを許可します。電源が標準の 802.3at PoE ではない場合に使用します。
名前開始文字列	名前の先頭部分で使用する文字列を所定のフィールドに入力します。
国コード	ドロップダウン メニューから、アクセス ポイントを配備する国の国コードを選択します。
EAPoL バージョン	ドロップダウン メニューから EAPoL バージョンを選択します。V2 の方がセキュリティが向上することに注意してください。
帯域誘導モード	ドロップダウン メニューから帯域誘導モードを選択します。以下のオプションがあります。 無効、自動、5GHz を優先、または 5GHz を強制 。

2. 仮想アクセス ポイント設定を設定するには、以下の手順に従います。
 - a. 「5GHz 無線仮想 AP グループ」で、ドロップダウン メニューから仮想アクセス ポイントオブジェクトグループを選択します。
 - b. 「2.4GHz 無線仮想 AP グループ」で、ドロップダウン メニューから仮想アクセス ポイントオブジェクトグループを選択します。

3. 一般設定が見えるまで下にスクロールします。

The screenshot shows a configuration window with three sections:

- 動的 VLAN ID の割り当て**: Two toggle switches for enabling dynamic VLAN ID assignment on 5GHz and 2.4GHz wireless networks. Each has a '編集' (Edit) button.
- L3 SSLVPN トンネル設定**: Fields for 'SSLVPN サーバ' (Server), 'ユーザ名' (Username), 'パスワード' (Password), and 'ドメイン' (Domain). A radio button for '自動再接続' (Auto-reconnect) is currently off, with a note: 'L3 SSLVPN を構成するには、次に移動します: SSL VPN > クライアント設定。' (To configure L3 SSLVPN, move to: SSL VPN > Client settings).
- 管理者設定**: Fields for '名前' (Name) and 'パスワード' (Password).

Buttons for 'OK' and 'キャンセル' (Cancel) are at the bottom right.

4. 「動的 VLAN ID の割り当て」を設定します。
「動的 VLAN ID の割り当て」でオプションを有効にするには、「オブジェクト > 一致オブジェクト > ゾーン」で WLAN ゾーンを、「ネットワーク > システム > VLAN 変換」で VLAN インターフェースを作成する必要があります。
5. SSL VPN トンネル設定の構成
 - a. テキストフィールドに **SSL VPN サーバ**名または IP アドレスを入力します。
 - b. SSL VPN サーバ用の **ユーザ名** をフィールドに入力します。
 - c. SSL VPN サーバ認証用の **パスワード**を入力します。
 - d. **ドメイン** 名をフィールドに入力します。
 - e. 「**自動再接続**」オプションを選択して有効にします。
 - f. レイヤ 3 SSL VPN を構成する場合、「**SSL VPN > クライアントの設定**」をクリックし、適切な設定を定義してください。
6. 「**管理者設定**」を設定します。
 - a. ネットワーク管理者の **ユーザ名**を入力します。
 - b. ネットワーク管理者の **パスワード**を入力します。

プロビジョニング プロファイルの 5GHz/2.4GHz 無線の基本設定

さまざまな種類のアクセスポイントで、5GHz 無線と 2.4GHz 無線の基本設定は似ており、わずかな違いしかありません。この違いについては各ステップで説明します。ただし、一般設定で VAP グループが選択されていた場合、さまざまなオプションが表示されます。

以下のトピックでは、「5GHz/2.4GHz 無線の基本」画面の設定について説明します。

トピック:

- 無線設定
- 無線セキュリティ
- 保護された管理フレーム (PMF オプション)
- ローカル RADIUS サーバと EAP 認証バランスについて
- RADIUS サーバの設定
- ACL 強制
- リモート MAC アドレス アクセス制御の設定

無線設定

5GHz 無線/2.4GHz 無線の基本設定を構成するには、以下の手順に従います:

1. 「5GHz 無線の基本」または「2.4GHz 無線の基本」を選択します。



2. 「無線を有効にする」をオンにすると、このプロファイルでプロビジョニングされたすべてのアクセスポイントで無線帯域が自動的に有効になります。このオプションは、既定では選択されています。
3. 「無線を有効にする」ドロップダウンメニューで、無線をオンにする時間のスケジュールを選択するか、新しいスケジュールを作成します。既定は「常に有効」です。
4. 「モード」ドロップダウンメニューから適切な無線モードを選択します。

無線モードの選択肢

5GHz 無線基本	2.4GHz 無線基本	定義
5GHz 802.11n のみ	2.4GHz 802.11n のみ	802.11n クライアントだけが無線ネットワークにアクセスできます。この制限付き無線機モードでは、802.11a/b/g クライアントは接続できません。
5GHz 802.11n/a 混在	2.4GHz 802.11n/g/b 混在 (SonicPoint AC/NDR の既定)	802.11a および 802.11n (5GHz 無線) または 802.11b、802.11g、および 802.11n (2.4GHz 無線) のクライアントを同時にサポートします。無線ネットワークが複数の種類のクライアントで構成されている場合は、このモードを選択してください。
5GHz 802.11a のみ (SonicPoint NDR の既定)		802.11a クライアントだけが無線ネットワークにアクセスする場合は、このモードを選択します。

2.4GHz 802.11g のみ	無線ネットワークが 802.11g クライアントだけで構成されている場合は、802.11g パフォーマンスを向上させるためにこのモードの選択をお勧めします。このモードを選択すると、802.11b クライアントの参加を防ぐこともできます。
5GHz 802.11ac/n/a 混在 (SonicWave および SonicPoint AC の既定)	802.11ac、802.11a、および 802.11n のクライアントを同時にサポートします。無線ネットワークが複数の種類のクライアントで構成されている場合は、このモードを選択してください。
5GHz 802.11ac のみ	802.11ac クライアントだけが無線ネットワークにアクセスできます。この制限付き無線モードでは、他のクライアントは接続できません。

- ① **ヒント:** 802.11n クライアントのみ 最適なスループット速度をお求めの場合、SonicWall では「**802.11n のみ**」無線モードをお勧めします。複数の無線クライアント認証の互換性を維持するには、「**802.11n/g/b 混在**」無線モードを使用してください。
- 802.11ac クライアントだけを対象に最適なスループット速度をお求めの場合、SonicWall では「**802.11ac のみ**」無線モードをお勧めします。「**802.11ac/n/a 混在**」無線モードは、複数無線クライアント認証互換性の用途で使用します。
- ① **補足:** 「**802.11n 5GHz/2.4GHz 無線設定**」で使用可能なオプションは、選択したモードによって変わります。無線通信の構成モードによって、以下のようになります。
- 802.11n をサポートするモードの場合は、「無線帯域」、「プライマリチャンネル」、「セカンダリチャンネル」、「ショートガード間隔を有効にする」、「アグリゲーションを有効にする」のオプションが表示されます。
 - 802.11n をサポートしないモードの場合は、「チャンネル」オプションのみが表示されます。
5. 「SSID」フィールドに、このプロファイルを使用する各アクセスポイントの SSID として認識可能な文字列を入力します。これが、利用可能な無線接続のクライアント一覧に表示される名前になります。
- ① **ヒント:** 組織内のすべての SonicPoint または SonicWave で同じ SSID を共有していれば、ユーザがアクセスポイント間でローミングを行うときに無線接続の維持が容易になります。
6. それ以外のモードの場合は、「無線帯域」ドロップダウンメニューから無線帯域を選択します。
- ① **補足:** 「モード = 5GHz 802.11a のみ」の場合、「無線帯域」オプションは利用不可です。
- 「自動」- 装置は信号の強度と整合性に基づいて、無線動作に最適なチャンネルを自動的に検出および設定できます。一つが選択された場合、「プライマリチャンネル」と「セカンダリチャンネル」も「自動」に設定しなくてはなりません。このオプションは既定の設定です。
 - 「標準 - 20MHz チャンネル」- 無線が標準 20MHz チャンネルのみを使用するように指定します。
 - 「広域 - 40 MHz チャンネル - 「5GHz 802.11a のみ」が「無線帯域」で選択されている場合を除いて、すべてのモードで利用可能です。無線が広域 40MHz チャンネルのみを使用するように指定します。
 - 「広域 - 80 MHz チャンネル」- 「5GHz 802.11ac/n/a 混在」または「5GHz 802.11ac のみ」が「無線帯域」として選択されている場合のみ利用可能で、5GHz 無線が広域 80MHz チャンネルのみを使用するように指定します。（「モード」が「5GHz 802.11n のみ」、「5GHz 802.11n/a 混在」、または「5GHz 802.11a のみ」のときは使用できません。）

7. チャンネルを、モードおよび無線帯域オプションの選択に合わせて選択してください。

モード	無線帯域	チャンネル
5GHz 802.11n のみ	自動	「プライマリチャンネル」と「セカンダリチャンネル」フィールドの既定値は自動です。
	標準 - 20 MHz チャンネル	「自動」または「標準チャンネル」ドロップダウンメニューで指定された無線チャンネルの1つを選択します。
	広域 - 40 MHz チャンネル	「自動」または「プライマリチャンネル」の無線チャンネルの1つを選択します。「セカンダリチャンネル」は自動的に「自動」に定義されます。
5GHz 802.11n/a 混在	自動	「プライマリチャンネル」と「セカンダリチャンネル」フィールドの既定値は自動です。
	標準 - 20 MHz チャンネル	「自動」または「標準チャンネル」ドロップダウンメニューで指定された無線チャンネルの1つを選択します。
	広域 - 40 MHz チャンネル	「自動」または「プライマリチャンネル」の無線チャンネルの1つを選択します。「セカンダリチャンネル」は自動的に「自動」に定義されます。
5GHz 802.11a のみ	(オプションはありません)	「自動」または「チャンネル」ドロップダウンメニューで指定された無線チャンネルの1つを選択します。
5GHz 802.11ac/n/a 混在	自動	「チャンネル」フィールドの既定値は自動です。
	標準 - 20 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューで指定された無線チャンネルの1つを選択します。
	広域 - 40 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューの無線チャンネルのいずれかを選択します。
	広域 - 80 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューの無線チャンネルのいずれかを選択します。
5GHz 802.11ac のみ	自動	「チャンネル」フィールドの既定値は自動です。
	標準 - 20 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューで指定された無線チャンネルの1つを選択します。
	広域 - 40 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューの無線チャンネルのいずれかを選択します。
	広域 - 80 MHz チャンネル	「自動」または「チャンネル」ドロップダウンメニューの無線チャンネルのいずれかを選択します。

8. 「ショートガード間隔を有効にする」を選択して有効にします。ガード間隔を短くすることによって、無線転送速度を上げます。無線クライアントもこれをサポートしていることを確認し、互換性の問題が発生しないようにしてください。
9. 「アグリゲーションを有効にする」を選択して有効にします。単一の伝送で複数のデータフレームを送信することにより、無線スループットを上げます。無線クライアントもこれをサポートしていることを確認し、互換性の問題が発生しないようにしてください。

無線セキュリティ

- ① **補足:** SonicOS インターフェースは、状況に応じて表示が変わります。「一般」画面で VAP グループが選択されている場合、「無線セキュリティ」セクションは飛ばせるように表示されません。

無線セキュリティオプションを設定するには、以下の手順に従います

1. 無線セキュリティセクションまでスクロールします。これらのオプションは、選択した**認証種別**によって変化します。

無線セキュリティ

認証種別

WEP 鍵のモード

既定の鍵

鍵登録

第 1 鍵

第 2 鍵

第 3 鍵

第 4 鍵

無線セキュリティ

認証種別

暗号化種別

グループ鍵交換間隔 (秒)

PMF オプション

パスワード

無線セキュリティ

認証種別

WEP 鍵のモード

既定の鍵

鍵登録

第 1 鍵

第 2 鍵

第 3 鍵

第 4 鍵

無線セキュリティを構成するには、以下の手順に従います

1. 「無線セキュリティ」セクションで、「認証種別」をドロップダウンメニューから選択します。
① **補足:** 使用可能なオプションは、選択した設定の種別によって変わります。「WPA2 - EAP」オプションを選択すると、「RADIUS サーバの設定」セクションが表示されます。
2. 以下のテーブルを参考にして、残りの設定を定義します。

無線セキュリティのための WEP 設定

WEP の説明		
認証種別	WEP 鍵のモード	設定
WEP (Wired Equivalent Privacy) は、Wi-Fi 無線ネットワークセキュリティ用の規格です。公開システムで、認証のため情報を交換し、その後データを暗号化します。共有キーは共有鍵を使って認証します。		
WEP - 両方 (オープン システムおよび共有鍵)	WEP 鍵モード = なし	残りの設定はグレー表示になっていて選択できません。
	WEP 鍵のモード = 64 ビット、128 ビットまたは 152 ビット。ビット数が、WEP 鍵の強度を表します。	<ul style="list-style-type: none">• 「既定の鍵」フィールドでは、既定値の鍵 (最初に試行した鍵) を選択してください。第 1 鍵が既定値です。• 「鍵登録」フィールドでは、鍵を「英数字」とするか「16 進数字 (0 ~ 9、A ~ F)」とするか選択してください。• 第 1 鍵、第 2 鍵、第 3 鍵、第 4 鍵のフィールドに、データを転送する際に使用する暗号化鍵を入力します。
WEP - オープン システム		残りの設定はグレー表示になっていて選択できません。
WEP - 共有鍵	WEP 鍵のモード = 64 ビット、128 ビットまたは 152 ビット。既定値は 152 ビットです。	<ul style="list-style-type: none">• 「既定の鍵」フィールドでは、既定値の鍵 (最初に試行した鍵) を選択してください。第 1 鍵が既定値です。• 「鍵登録」フィールドでは、鍵を「英数字」とするか「16 進数字 (0 ~ 9、A ~ F)」とするか選択してください。16 進数字が既定値です。• 第 1 鍵、第 2 鍵、第 3 鍵、第 4 鍵のフィールドに、データを転送する際に使用する暗号化鍵を入力します。

WPA2 無線セキュリティ設定

説明	
認証種別	設定
WPA および WPA2 (Wi-Fi Protected Access) は、無線デバイスの保護のためのより新しいプロトコルです。「WPA2 - 自動」オプションの 1 つを選択しておくこと、デバイスで WPA2 が有効になっていない場合には WPA プロトコルを使用します。	
WPA2 - PSK	<ul style="list-style-type: none">• ドロップダウンメニューから「暗号化種別」を選択します。オプションには、「AES」(既定)、「TKIP」、「自動」

認証種別	説明
	<p>があります。</p> <ul style="list-style-type: none"> グループ鍵交換間隔を秒数で設定します。既定値は 86400 です。 SonicWaveの場合、ドロップダウンメニューから「PMF オプション」を選択します。「保護された管理フレーム (PMF オプション)」を参照してください。 公開共有鍵の パスフレーズ を定義します。
WPA2 - EAP	<ul style="list-style-type: none"> SonicWaveの場合、ドロップダウンメニューから「認証バランス方式」を選択します。「ローカル RADIUS サーバと EAP 認証バランスについて」を参照してください ドロップダウンメニューから「暗号化種別」を選択します。オプションには、「AES」(既定)、「TKIP」、「自動」があります。 グループ鍵交換間隔を秒数で設定します。既定値は 86400 です。 SonicWaveの場合、ドロップダウンメニューから「PMF オプション」を選択します。「保護された管理フレーム (PMF オプション)」を参照してください。
WPA2 - AUTO - PSK	<ul style="list-style-type: none"> ドロップダウンメニューから「暗号化種別」を選択します。オプションには、「AES」(既定)、「TKIP」、「自動」があります。 グループ鍵交換間隔を秒数で設定します。既定値は 86400 です。 SonicWaveの場合、ドロップダウンメニューから「PMF オプション」を選択します。「保護された管理フレーム (PMF オプション)」を参照してください。 公開共有鍵の パスフレーズ を定義します。
WPA2 - AUTO - EAP	<ul style="list-style-type: none"> SonicWaveの場合、ドロップダウンメニューから「認証バランス方式」を選択します。「ローカル RADIUS サーバと EAP 認証バランスについて」を参照してください。 ドロップダウンメニューから「暗号化種別」を選択します。オプションには、「AES」(既定)、「TKIP」、「自動」があります。 グループ鍵交換間隔を秒数で設定します。既定値は 86400 です。 SonicWaveの場合、ドロップダウンメニューから「PMF オプション」を選択します。「保護された管理フレーム (PMF オプション)」を参照してください。

保護された管理フレーム (PMF オプション)

「認証種別」の設定が WPA2 オプションのいずれかであるとき、「PMF オプション」設定を使用できます。「PMF オプション」設定は、SonicOS 6.5.2 以降の SonicWave プロファイルでサポートされています。この機能は、無線管理フレームの保護のための IEEE 802.11 標準に対する IEEE 802.11w-2009 修正をサポートします。また、Protected Management Frames (PMF) 標準としても知られています。

「無線セキュリティ」の下にある「PMF オプション」ドロップダウンメニューから、次の設定のいずれかを選択できます。

- **無効** - このサービスは有効化されません。クライアントは PMF なしで接続します。
- **有効** - このサービスは、無線クライアントではオプションです。クライアントは、クライアント設定に基づいて、PMF の有無にかかわらず接続できます。
- **必須** - クライアントは、PMF を有効化しないと接続できません。

802.11i 修正により**データ** フレームは保護されますが、認証、認証解除、関連付け、解離、ビーコン、プローブなどの管理フレームは、ネットワーク サービスのセッションを開始または破棄するために無線クライアントで使用されます。暗号化して機密性を高めることができるデータトラフィックとは異なり、これらのフレームはすべてのクライアントが聞き取り、理解する必要があるため、オープンまたは暗号化されていない状態で送信する必要があります。これらのフレームは暗号化できませんが、攻撃から無線媒体を保護するために偽装防御を実施する必要があります。たとえば、攻撃者がクライアントの MAC アドレスを取得すると、AP の名前でクライアントに不参加要求を送信したり、クライアントの名前で AP に再参加要求を送信したりできます。いずれの状況でも、クライアントはログオフされません。

802.11w 修正は、Protected Management Frames (PMF) サービスによって保護されている堅牢な**管理**フレームのセットに適用されます。これには、関連付け解除フレーム、認証解除フレーム、堅牢なアクションフレームが含まれます。802.11w は、特定の管理フレームのみを保護し、アクセスポイントとクライアント間の通信に影響を与えません。802.11w が有効になるのは、アクセスポイントとクライアントの両方で 802.11w が有効になっているときのみです。

802.11w には次のメリットがあります。

機密性	ユニキャスト管理フレームを暗号化する: データフレームと同じ PTK を使用する 前もって暗号化されていないフレーム ヘッダーを追加認証データ (AAD) で保護する 拡張 AES-CCM でユニキャスト管理フレームを処理する 独立した受信シーケンスカウンタ (RSC) でリプレイ攻撃を防御する
グループアドレス指定フレーム保護	ブロードキャスト/マルチキャスト整合性プロトコル (BIP) は、ブロードキャストとマルチキャストの整合性を保護し、リプレイ攻撃を防ぎ、ブロードキャスト/マルチキャスト攻撃のなりすましからクライアントを保護します。ブロード/マルチキャスト管理フレームの場合: WPA 鍵ハンドシェイク中に受信した新しい Integrity Group Temporal Key (IGTK) を使用する 新しいアルゴリズム: Broadcast Integrity Protocol (BIP) 新しい情報要素: 管理 MIC IE でシーケンス番号 + 暗号化ハッシュ (AES128-CMAC ベース) を使用
接続保護	セキュリティアソシエーション (SA) クエリは、再参加要求のスプーフィングによってクライアントがオフラインにされることを防ぐことができます。

ローカルRADIUS サーバと EAP 認証 バランスについて

この機能は SonicOS 6.5.2 で導入されました。この機能を使用すると、選択した SonicWave 内でローカル SonicWave アクセス ポイントがローカル RADIUS 認証サービスを提供できるようになります。なお、この機能は、ネイティブ LDAP システムや Active Directory などの企業ディレクトリ サービスと統合されます。このシナリオでは、SonicWave はクライアントに EAP 認証を提供し、認証システムと認証サーバの両方として同時に機能します。再接続時の動作を高速化するために、LDAP キャッシュと TLS キャッシュがサポートされています。

この機能を構成するためには、以下が必要です:

- WLAN ゾーンにインターフェースがあって、そこでサブネットに 1 つ以上のローカル RADIUS サーバを構成すること。これらは SonicWave ローカル RADIUS サーバです。
- WLAN ゾーンの構成に関連して「RADIUS サーバ」画面の「ローカル RADIUS サーバを有効にする」オプションを選択すること。このオプションは、この機能を有効にするかどうかを制御します。
- SonicWave プロファイルに関連して「無線の基本」画面で以下を設定すること:
 - いずれかの WPA2-EAP を「認証種別」で選択
「RADIUS サーバの設定」セクションが表示され、ローカル RADIUS サーバ設定を構成できます。
「RADIUS サーバの設定」を参照してください。
 - 「認証バランス方式」でいずれかの「ローカル RADIUS サーバ」オプションを選択



最初にローカル RADIUS サーバ - このオプションを選択すると、クライアントが認証を試みたとき、最初にローカル RADIUS サーバが使用されます。認証に失敗すると、認証要求はリモート RADIUS サーバに送信されます。

リモート RADIUS サーバのみ - リモート RADIUS サーバのみを認証に使用します。

ローカル RADIUS サーバのみ - ローカル RADIUS サーバのみを認証に使用します。

フェイルオーバー メカニズムとしてのローカル RADIUS サーバ - リモート RADIUS サーバがダウンすると、ローカル RADIUS サーバが自動的に使用されます。

- NAT ポリシー、アクセス ルール、アドレス グループ、RADIUS プール - 自動的に構成されます。

SonicWave でローカル RADIUS サーバを有効にすると、NAT ポリシーとアクセスルールが自動的に作成されます。SonicOS NAT モジュールにはフェイルオーバーと負荷分散の機能があるため、RADIUS サーバ プールがサポートされています。ローカル RADIUS サーバが構成された追加的な SonicWave をこのプールに追加できます。複数のローカル RADIUS サーバによって、フェイルオーバー メカニズムが提供され、ネットワーク パフォーマンスが最適化されます。

「ローカル RADIUS サーバを有効にする」オプションやその他の項目の設定は、「オブジェクト > 一致オブジェクト > ゾーン」から WLAN ゾーンを構成するときに使用可能となる「RADIUS サーバ」画面で行われます。この画面には、インターフェースあたりの RADIUS サーバ数、サーバポート、クライアントパスワード、TLS キャッシュ、および LDAP または Active Directory アクセス設定を設定するためのオプションがあります。SonicWave でローカル RADIUS サーバを有効にすると、構成されている RADIUS サーバポートとクライアントパスワードがその SonicWave で使用されます。

- ① **補足:** SonicWave DNS サーバは、LDAP サーバまたは Active Directory サーバドメインの名前を解決する必要があります。

「インターフェースあたりのサーバ数」オプションは、このゾーンの特定インターフェースの配下にあるローカル RADIUS サーバ数を制御します。この値を増やすと、RADIUS プールに追加できる SonicWave が増えます。最小値は 1 で、最大値は WLAN ゾーン内のインターフェースあたりの SonicWave の最大数と等しくなります。このオプションで構成する値は、接続されている SonicWave の数よりも小さいので、ローカル RADIUS サーバとして構成した特定の SonicWave は固定されません。

「ローカル RADIUS サーバ TLS キャッシュを有効にする」オプションが有効になっている場合、クライアントとサーバは TLS セッションの鍵をキャッシュし、これを使用してクライアントの認証要求と RADIUS サーバの応答の間の時間的な遅延を減らすことができます。クライアントは高速再接続も実行できます。有効にすると、「**キャッシュの継続期間**」オプションでキャッシュ項目の保存時間数を設定できます。キャッシュの持続時間は、1 時間から 24 時間の範囲で指定できます。

セキュリティ装置の起動時に、「ローカル RADIUS サーバを有効にする」が WLAN ゾーンで有効になっていると、アドレスオブジェクト、RADIUS プール、NAT ポリシー、およびアクセス ルールが作成されるはずですが、RADIUS プールの名前、インターフェース名と「Radius Pool」の組み合わせです。たとえば、X2 Radius Pool のようになります。RADIUS サーバとして動作する SonicWave の新しいアドレスオブジェクトが自動的に作成されます。これは、SonicWave のインターフェース名と MAC アドレスに基づいて名前が付けられます。たとえば、X2 18:b1:69:7b:75:2e のようになります。利用可能なシートがあれば、このアドレスオブジェクトは RADIUS プールに追加されます。

「ローカル RADIUS サーバを有効にする」が無効になっている場合、SonicWave アドレスオブジェクト、RADIUS プール、NAT ポリシー、およびアクセス ルールは削除されます。また、restApi による削除コマンドが RADIUS プール内の SonicWave に送信され、ローカル RADIUS サーバは停止します。

WLAN ゾーンが編集されると、NAT ポリシーとアクセス ルールは削除され、再作成されます。「ローカル RADIUS サーバを有効にする」が無効になっていない限り、RADIUS プールは常に存在します。

インターフェースが変更された場合、インターフェースがまだ WLAN ゾーンにバインドされていると、NAT ポリシー、アクセス ルール、および RADIUS プールは削除され、再度作成されます。

RADIUS サーバの設定

「WPA2-EAP」または「WPA2-AUTO-EAP」を「無線セキュリティ」セクションで選択した場合、「RADIUS サーバの設定」セクションが表示され、RADIUS サーバによる認証鍵の生成に関する設定を行うことができます。サーバはこのために、また、SonicWall 装置と通信できるよう構成されていなくてはなりません。

RADIUS サーバ設定を構成するには、以下の手順に従います:

1. 「RADIUS サーバの設定」をクリックします。「RADIUS サーバの設定」ダイアログが表示されます。このダイアログ上のオプションは、SonicPoint/SonicWave の種別によって異なります。



2. 「再試行」フィールドに、他の RADIUS サーバにフェイルオーバーする前に、ファイアウォールが接続を試行する回数を 1 ~ 10 の数値で入力します。
3. 「再試行間隔」フィールドに、次の再試行まで待つ時間を 0 ~ 60 秒で入力します。既定値は 0 で、間隔を置かずに再試行することを意味します。
4. 以下のテーブルの説明に従って、RADIUS サーバの設定を定義します。

RADIUS 認証サーバの設定

オブジェクトの説明

サーバ 1
RADIUS 認証サーバの名前/場所
サーバ IP

サーバ 1
RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信するポート。既定のポートは 1812 です。
サーバ 1 ポート

サーバ 1
RADIUS サーバ用のシークレット パスワード
サーバ 1
パスワード

サーバ 2
バックアップ RADIUS 認証サーバの名前/場所
サーバ 2
RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信するポート。既定のポートは 1812 です。
サーバ 2
ポート

サーバ 2
バックアップ RADIUS 認証サーバ用のシークレット パスワード
サーバ 2
パスワード

5. RADIUS サーバを課金のために使用量を追跡するために利用するのであれば、RADIUS アカウントサーバをセットアップしてください。

RADIUS アカウントサーバ設定

オプション	説明
サーバ 1 IP	RADIUS 認証サーバの名前/場所
サーバ 1 ポート	RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信

	するポート。
サーバ 1 パスワード	RADIUS サーバ用のシークレット パスコード
サーバ 2	バックアップ RADIUS 認証サーバの名前/場所
サーバ 2 ポート	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信するポート。
サーバ 2 パスワード	バックアップ RADIUS 認証サーバ用のシークレット パスコード

- NAS 識別子を RADIUS サーバに送信するには、「**NAS 識別子の種別**」ドロップダウン メニューから種別を選択します。
 - 含まない(既定)
 - SonicPoint の名前**
 - SonicPoint の MAC アドレス**
 - SSID** – SSID オプションが選択されている場合、RADIUS 認証メッセージと RADIUS アカウントメッセージの両方がアクセス ポイントまたは SSID を伝送します。
- NAS の IP アドレスを RADIUS サーバに送信するには、「**NAS IP アドレス**」フィールドにアドレスを入力します。
- 「OK」をクリックします。

ACL 強制

各アクセス ポイントは、個別のアクセス制御リスト (ACL) をサポートして、より効率的な認証制御を提供できます。この ACL 機能は、現在 SonicOS で利用可能な無線 MAC フィルタ リストと同時に動作します。この ACL 強制機能を使って、ユーザは MAC フィルタ リストを有効/無効にする、許可リストを設定する、そして拒否リストを設定することが可能です。

MAC フィルタ リストの強制化を有効にするには、以下の手順に従います

- 「**MAC フィルタ リストを有効にする**」オプションをオンにします。MAC フィルタ リストが有効な場合、他の設定項目も設定できるように表示されます。
- 「**許可リスト**」で、ドロップダウン メニューからオプションを選択します。どの MAC アドレスにアクセスを許可するかを指定します。
アクセスさせたい MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。詳細は、『SonicOS ポリシー』を参照してください。
- 「**拒否**」リストで、ドロップダウン メニューからオプションを選択します。どの MAC アドレスからのアクセスを拒否するかを指定します。
アクセスさせたくない MAC アドレスを集めて新しいアドレス オブジェクト グループを作成する場合、「**MAC アドレス オブジェクト グループの作成**」を選択してください。詳細は、『SonicOS ポリシー』を参照してください。
- 「**MIC 失敗 ACL ブラックリストを有効にする**」オプションをオンにします。
- MIC 失敗頻度のしきい値** を、1 分間の回数に基づいて設定します。既定値は 3 です。

リモート MAC アドレス アクセス制御の設定

このオプションでは、RADIUS サーバによる、MAC ベースの認証ポリシーに基づく無線アクセス制御を強制することができます。

無線アクセス制御を許可するには、以下の手順に従います:

1. 「リモート MAC アクセス制御を有効にする」オプションをオンにします。
2. 「構成」をクリックします。
3. 構成済みでない場合、RADIUS サーバを「RADIUS サーバの設定」の説明に従ってセットアップします。
4. 「OK」をクリックします。

プロビジョニング プロファイルの 5GHz/2.4GHz 無線の詳細設定

これらの設定は、無線帯域の動作に影響します。SonicPoint/SonicWave は 2 種類の内蔵無線を搭載しています。そのため、両帯域での送受信を同時に行うことができます。

「5GHz 無線の詳細」画面には、「2.4GHz 無線の詳細」画面と同じオプションに加えて、その他のオプションがあります。これらの画面は、さまざまなアクセス ポイント モデルで類似しています。相違点については、必要があれば手順の中で示します。

5GHz 無線/2.4GHz 無線の詳細設定を構成するには、以下の手順に従います：

1. 必要に応じて、「5GHz 無線の詳細」または「2.4GHz 無線の詳細」を選択します。
2. 「ビーコンに SSID を載せない」場合にはこのオプションをオンにします。こうすると、SSID が無線 SSID 名の通知の代わりにマルチ SSID ビーコンを送信するようにします。マルチ SSID ビーコンを送信すると、接続する SSID を無線クライアントに強制的に知らせることができます。このオプションは既定でオフになっています。
3. 「IDS スキャンを予定する」ドロップダウン メニューから、IDS (侵入検知サービス) スキャンのスケジュールを選択します。

無線接続が破棄されるという不都合を最小限に抑えるために、無線ネットワークの需要が比較的少ない時間を選択します。「スケジュールの作成」を選択して独自のスケジュールを作成したり、既定の設定である「無効」を選択してこの機能を無効にしたりすることができます。

- ① **補足:** IDS は、無線の脅威からネットワークを保護するためのさまざまな侵入検知機能を備えます。この機能によって、許可されたアクセスポイント、RF 媒体、有線ネットワークで構成される WLAN インフラに対する攻撃が検知されます。許可されている有効な AP は、WLAN インフラに属するアクセスポイントとして定義されます。アクセスポイントは、SonicPoint、SonicWave、またはサードパーティのアクセスポイントです。
4. 「**転送速度**」ドロップダウンメニューから、データが送受信される速度を選択します。「**最良**」(既定)では、電磁波妨害やその他の要因を考慮したうえで、その地域で利用できる最適な速度が自動的に選択されます。
 5. 「**電波出力**」ドロップダウンメニューから、電波出力を選択します。電波出力は SonicPoint の範囲に影響します。
 - **最大出力** (既定)
 - **1/2 出力 (-3 dB)**
 - **1/4 出力 (-6 dB)**
 - **1/8 出力 (-9 dB)**
 - **最小**
 6. SonicPoint NDR を設定する場合は、「**使用するアンテナ**」ドロップダウンメニューから、「**最良**」(既定値)を選択します。

「**使用するアンテナ**」設定は、アクセスポイントがデータの送受信に使用するアンテナを決定します。「**最良**」を選択すると、強度が最も高く、劣化していない信号を受信したアンテナがアクセスポイントによって自動的に選択されます。
 7. 「**ビーコン間隔(ミリ秒)**」フィールドに、無線 SSID ビーコンを送出する間隔をミリ秒単位で入力します。最小間隔は 100 ミリ秒 (既定値)、最大間隔は 1000 ミリ秒です。
 8. 「**DTIM 間隔**」フィールドに、DTIM 間隔をミリ秒で入力します。フレーム数の最小値は 1 (既定値)、最大値は 255 です。

マルチキャストパケットを受信する 802.11 省電力モードのクライアントに対し、「**DTIM 間隔**」は、DTIM (Delivery Traffic Indication Message) を送信する前に待つビーコンフレーム数を指定します。
 9. SonicPointNDR を設定する場合、「**断片化のしきい値(バイト)**」フィールドに、ネットワークで許容する断片化データのバイト数を入力します。

断片化のしきい値は、最大フレームサイズを制限します。フレームサイズを制限すると、フレーム送信に要する時間が短くなるため、フレームが破損する確率が低下します (その代わりに、データオーバーヘッドは高くなります)。無線フレームの断片化は、RF 干渉が存在する場所や、無線通信範囲の電波が弱い場所において、信頼性とスループットを向上させます。しきい値が低いほど、より細かく断片化されます。最小値は 256 バイト、最大値は 2346 バイト (既定値) です。
 10. 「**RTS しきい値(バイト)**」フィールドに、パケット送信の前に送信する RTS (Request to Send: 送信要求) のパケットサイズのしきい値をバイト単位で入力します。

RTS を送信すると、クライアントが同じアクセスポイントの範囲内にあるが互いの範囲内にあるとは限らないという状況で、無線の衝突が生じないようにすることができます。しきい値の最小値は 256 バイト、最大値は 2346 バイト (既定値) です。
 11. 「**クライアント最大参加数**」フィールドに、このプロファイルを使用する各アクセスポイントに、この無線で同時にサポートさせたいクライアントの最大数を入力します。クライアント数の最小値は 1、最大値は 128、既定値は 32 です。
 12. 「**ステーション無動作タイムアウト(秒)**」フィールドに、無線クライアントの無動作の最大時間を秒単位で入力します。この時間が経過すると、アクセスポイントはその無線クライアントを期限切れにします。最小値は 60 秒、最大値は 36000 秒、既定値は 300 秒です。
 13. 「**2.4GHz 無線の詳細**」画面の設定を行う場合は、そのウィンドウに固有の以下の設定を定義してください。そうでなければ次のステップに進んでください。

オプション	設定
プリアンブル長	ドロップダウン メニューから次のいずれかを選択します。 <ul style="list-style-type: none"> 長い (既定) ショート
保護モード	ドロップダウン メニューから次のいずれかを選択します。 <ul style="list-style-type: none"> なし 常に有効 自動
保護速度	ドロップダウン メニューから次のいずれかを選択します。 <ul style="list-style-type: none"> 1 Mbps (既定) 2 Mbps 5 Mbps 11 Mbps
保護種別	ドロップダウン メニューから次のいずれかを選択します。 <ul style="list-style-type: none"> CTS のみ (既定) RTS と CTS
Short Slot Time を有効にする	クライアントによる不参加と再参加を迅速に行えるようにします。このオプションを指定すると、アクセス ポイントがパケットを LAN にリレーする前に待機する時間を短くすることによって、802.11n/g 無線帯域上のスループットを上げることができます。

802.11b クライアントの接続を許可しない ターボ G モードを使用する (したがって 802.11b クライアントの接続を許可しない) 場合に、これを使用します。このオプションを指定すると、無線接続が 802.11g と 802.11n のクライアントのみに制限されます。

- 「WMM (Wi-Fi マルチメディア)」ドロップダウン メニューで、WMM プロファイルをこのプロファイルに関連付けるかどうかを選択します。
 - 無効 (既定)
 - WMM プロファイルの作成
 - 構成済みの WMM プロファイル
- 「WDS AP を有効にする」オプション ボックスをオンにします。これを利用すると、複数のアクセス ポイントを使用して、以前のような各アクセス ポイントを接続する有線バックボーンを必要とせずに、無線ネットワークを拡大できるようになります。
- 「グリーン AP を有効にする」を選択して、アクセス ポイント無線がスリープ モードに入ることを許可します。これによって、アクティブに接続するクライアントが存在しない場合の電力が抑えられます。いずれかのクライアントが接続を試みると、アクセス ポイントは直ちに最大出力モードに入ります。緑の AP は、5GHz 無線と 2.4GHz 無線の各無線に対してそれぞれ個別に設定できます。
- 「グリーン AP タイムアウト」フィールドに、アクティブな接続が存在しない場合にスリープ モードに入るまでにアクセス ポイントが待機する時間を入力します。この遷移時間の範囲は 20 ~ 65535 秒で、既定値は 20 秒です。
- SonicWave または SonicPoint ACe/ACi/N2 プロファイルを設定する場合は、「RSSI を有効にする」チェック ボックスをオンにして RSSI しきい値を有効にします。信号強度がしきい値を下回るクライアントは、アクセス ポイントによって関連付けが解除されるため、より近いアクセス ポイントに関連付けられます。このオプションは、既定では選択されていません。

19. 「RSSIを有効にする」が選択されている場合は、しきい値を負の値として「RSSIしきい値 (dBm)」フィールドに入力します。既定値は -95 dBm です。RSSIしきい値の詳細については、「RSSIしきい値の設定」を参照してください。
20. SonicWave デバイスを設定する場合、「エアタイムフェアネスを有効にする」オプションをオンにしてください。

この機能は、既定では無効になっています。有効にすると、5GHz 帯を使用できるデバイスに対して 5GHz 帯を使用させます。通常、5GHz 帯の方がトラフィックが少なく、干渉も少ないためです。信号強度または信号品質が 2.4GHz 帯の方が良好である場合、トラフィックはそちらの帯域を使用させます。目的は、両方の帯域を最も有効な方法で使用することです。
21. 「IEEE802.11r 設定」で、「IEEE802.11rを有効にする」をオンにして、安全で高速ローミングを有効にします。「IEEE802.11rを有効にする」が選択されている場合は、その他のオプションを選択できます。
 - DS を介した FT の有効化 - DS を介した高速移行を有効にします。
 - IEEE802.11r 混合モードを有効にする - 混合モードでの高速移行を有効にします。これらのオプションの詳細については、「安全で高速なローミングのための IEEE802.11r 設定」を参照してください。
22. 「IEEE802.11k 設定」で、「近隣レポートを有効にする」をオンにして、近隣についての情報の収集を有効にします。このオプションは、既定では選択されていません。「動的無線管理のための IEEE802.11k 設定」を参照してください。
23. 「IEEE802.11v 設定」で、「BSS 移行管理を有効にする」をオンにして、クライアントがアクセスポイントにクエリを送信した場合にアクセスポイントが音声クライアントに特定のアクセスポイントへの移行を要求できるようにします。このオプションは、既定では選択されていません。「動的環境管理のための IEEE802.11v 設定」を参照してください。
24. 「IEEE802.11v 設定」で、「WNM スリープモードを有効にする」をオンにして、非アクセスポイントステーションが指定の時間だけスリープすることをアクセスポイントに通知できるようにします。このオプションは、既定では選択されていません。「動的環境管理のための IEEE802.11v 設定」を参照してください。

RSSIしきい値の設定

エリア全体に適切な WiFi カバレッジを提供するために複数のアクセスポイントが必要とするほど大きいエリアでは、WiFi クライアントが最も近いアクセスポイントを検出して移動することが期待されます。残念ながら、多くの WiFi クライアントは、通常はより良い選択である近くのアクセスポイントに移動するのではなく、関連付けられた元のアクセスポイントに固執する傾向があります。これはスティッキ動作と呼ばれ、低い RSSI (受信信号強度インジケータ) と高い SNR (信号対雑音比) をもたらします。クライアントが移動する元のアクセスポイントから離れるほど、その RSSI は弱くなり、SNR は悪くなります。再送信が発生し、動的なレートシフトが発生し、クライアントははるかに低いデータレートで通信します。データレートが低いと、同じ情報を転送するための通信時間が長くなり、チャンネル使用率が高くなります。理想的には、クライアントは最も近いアクセスポイントにローミングし、結果として生じる RF スペースは誰にとってもより良いものになります。

SonicOS 6.5.2 以降では、RSSIしきい値がサポートされています。クライアントがアクセスポイントから見て一定の RSSI レベルに達すると、アクセスポイントはクライアントから切り離され、クライアントはより近いアクセスポイントに関連付けられます。RSSIしきい値は設定可能です。

RSSI 測定値は、アンテナおよびケーブルレベルで損失が発生した後のデバイスで受信した信号の相対的な品質を表します。RSSI 値が高いほど、信号は強くなります。負の値で測定した場合、ゼロに近い値は通常、より良い信号を意味します。例として、-50 dBm は非常に良好な信号であり、-75 dBm はかなり妥当であり、-100 dBm はまったく信号がありません。

安全で高速なローミングのための IEEE802.11r 設定

IEEE 802.11 WiFi の多くの実装の有効範囲はわずか数百メートルであるため、通信を維持するには、移動中のデバイスがあるアクセスポイントから別のアクセスポイントにハンドオフする必要があります。自動車環境では、5～10 秒ごとにハンドオフが起こる可能性があります。

ハンドオフは現在の標準で既にサポートされています。802.11 でのハンドオフの基本アーキテクチャは、802.11r を使用しても使用しなくても変わりません。モバイル デバイスは、ハンドオフするタイミングとハンドオフするアクセスポイントの決定を完全に任せられます。802.11 の初期の頃、ハンドオフはモバイル デバイスにとってはるかに簡単なタスクでした。デバイスが新しいアクセスポイントとの接続を確立するために必要なメッセージは 4 つだけです (クライアントから以前のアクセスポイントに送信される可能性のあるオプションの「I'm leaving」メッセージ [認証解除および不参加パケット] もカウントする場合は 5)。しかし、802.1X 認証を備えた 802.11i や、アドミッション コントロール要求を備えた 802.11e または WMM などの追加機能が標準に追加されたため、必要なメッセージの数は劇的に増加しました。これらの追加メッセージが交換されている間、音声通話からのトラフィックを含むモバイル デバイスのトラフィックは処理できず、ユーザが経験する損失は数秒に及ぶ可能性があります。一般的に、エッジネットワークが音声コールに導入する遅延または損失の最大量は 50 ミリ秒です。

802.11r は、セキュリティとサービス品質のためにハンドオフプロセスに追加された追加の負荷を取り除いて、元の 4 メッセージ交換の状態に戻します。この方法では、ハンドオフの問題は解消されませんが、少なくとも現状に戻ります。

802.11r 標準で現在想定されている主なアプリケーションは、標準のセルラー ネットワークの代わりに (またはそれに加えて) 無線インターネット ネットワークで動作するように設計された携帯電話による Voice over IP (VOIP) です。

動的無線管理のための IEEE802.11k 設定

「5GHz または 2.4GHz 無線の詳細」画面の「IEEE802.11k 設定」セクションには、「近隣レポートを有効にする」オプションがあります。このオプションを有効にすると、802.11 標準の IEEE802.11k 改正で定義されているように、アクセスポイントが無線測定値を収集します。

近隣レポート要求は、クライアントからアクセスポイントに送信されます。アクセスポイントは、クライアントが再参加する既知の候補である隣接アクセスポイントに関する情報を含む近隣レポートを返します (クライアントがそうすることを選択した場合)。したがって、近隣レポート要求/レポートペアにより、クライアントは、現在関連付けられているアクセスポイントの近隣アクセスポイントに関する情報を収集できます。この情報は、ローミング中に新しい接続点の潜在的な候補の識別として使用される場合があります。

近隣レポート要求/レポートの利点は次のとおりです。

- **スキャンの高速化** – クライアントが時間のかかるスキャン アクティビティ (アクセスポイントを積極的にローミングするか、ビーコンのすべてのチャンネルを受動的にリスンする) に関与する代わりに、クライアントはそのリストを既知の利用可能な近隣に絞り込むことができます。これは、クライアントが複数の WLAN をリスンできる高密度環境で特に役立ちます。
- **クライアントの電力消費を削減** – スキャン (特にアクティブ スキャン) にかかる時間もクライアントのバッテリー電力は消費されます。近隣レポートはローミング前に情報を提供するため、消費される電力が少なくなる可能性があります。
- **WLAN エアタイムのより効率的な使用** – アクティブ スキャンは、クライアント リソース (CPU、メモリ、無線など) の観点から時間がかかるだけでなく、エアタイムも消費します。たとえば、近隣を認識していないクライアントは、いわゆるワイルドカードプローブ要求に関与する可能性があります (一部のクライアントはこれをバーストします)。このシナリオでは、通常、プローブ要求をリスンするすべてのアクセスポイントがプローブ応答を生成します。つまり、単一のクライアントの場合、N 個のアクセスポイントが N 個のプローブ応答を生成します。複数のクライアントがワイルドカードプローブを行う場合、クライアントが近隣要求を使用し

ていないという理由だけで、RF 環境が管理トラフィックですぐに汚染される可能性があります。これは、WLAN 全体に悪影響を及ぼします。

動的環境管理のための IEEE802.11v 設定

802.11v は、IEEE802.11 無線ネットワーク管理 (修正 8) を指します。これは、無線ネットワークに接続しているときにクライアント デバイスを構成できるようにするための IEEE 802.11 標準の修正です。WNM (無線ネットワーク管理) をサポートするステーションは、情報を相互に (アクセス ポイントと無線クライアント間で) 交換することで、無線ネットワークの性能を向上できます。802.11v により、クライアント デバイスは RF 環境を含むネットワークトポロジに関する情報を交換することが可能になり、各クライアント ネットワークを認識させたり、無線ネットワークの全体的な性能向上を促進したりすることができます。

ステーションは WNM プロトコルを使用して操作データを交換し、各ステーションがネットワークの状態を認識できるようにして、ステーションがネットワークのトポロジと状態をより認識できるようにします。WNM プロトコルは、ステーションが共存干渉の存在を認識し、ステーションがネットワーク条件に基づいて RF パラメータを管理できるようにする手段を提供します。

ネットワーク状態に関する情報の提供に加えて、WNM は位置情報の交換、同じ無線インフラストラクチャでの複数の BSSID 機能のサポート、グループ アドレス指定フレームの効率的な配信のサポート、WNM スリープ モード (STA が AP からフレームを受信せずに長時間スリープできる) の有効化の手段も提供します。

BSS 最大アイドル期間管理は、SonicWall SonicPoint によってサポートされています。SonicWave は、無線ネットワークの性能を向上させるために、さらに 2 つの WNM サービスをサポートしています。

- **BSS 移行管理を有効にする** - アクセス ポイントは、特定のアクセス ポイントへの移行を音声クライアントに要求したり、ネットワーク負荷分散または BSS 終了により、音声クライアントに一連の優先アクセス ポイントを提案したりすることができます。これにより、音声クライアントは、そのクライアントがローミングするときに移行先となる最適なアクセス ポイントを識別できます。

BSS 移行機能は、個々の音声トラフィックの負荷を ESS 内のより適切な関連ポイントに (移行を介して) シフトすることにより、ネットワーク内の音声クライアントのスループット、データレート、および QoS を改善できます。

802.11v BSS 移行管理要求は、クライアントに提供される提案です。クライアントは、提案に従うかどうかを独自に決定できます。

BSS 移行管理は、次のフレーム種別を使用します。

- **クエリ** - 関連アクセス ポイントが BSS 移行機能をサポートしていることを示す場合、BSS 移行管理をサポートする音声クライアントが BSS 移行候補リストをその関連アクセス ポイントに要求することで、クエリフレームが送信されます。
- **要求** - BSS 移行管理をサポートするアクセス ポイントは、BSS 移行管理クエリフレームに BSS 移行管理要求フレームで応答します。
- **応答** - 応答フレームが音声クライアントによってアクセス ポイントに返され、移行を受け入れるか拒否するかが通知されます。
- **WNM スリープ モード** - 非アクセス ポイントステーションがすべての配信 DTIM (Delivery Traffic Indication Message) ビーコン フレームをリッスンする必要がなく、GTK/IGTK (Group Temporal Key/Integrity Group Temporal Key) の更新を実行しない非アクセス ポイントステーション用の拡張省電力モードです。

WNM スリープ モードは、非アクセス ポイントステーションがアクセス ポイントに指定の時間だけスリープすることを通知できるようにします。これにより、非アクセス ポイントステーションは電力消費を削減し、ステーションがアクセス ポイントとの間で送受信するトラフィックがない間、関連付けられたままになります。

① **重要:** WNM-Sleep モードが有効で、ステーションが WNM-Sleep モードをサポートしている場合は、鍵再インストール攻撃 (Key Reinstallation Attack) を回避するためにステーションを更新します。

プロビジョニング プロファイルの WIDP のセンサー設定

「センサー」画面では、「無線侵入検知と防御 (WIDP)」モードを有効または無効にできます。SonicOS 6.5.3 以降では、SonicWave 装置はアクセス ポイントとしても、SonicWall ネットワークに接続された不正アクセス ポイントを検知するセンサーとしても機能します。



以前のリリースでは、このオプションが選択されると、アクセス ポイントまたは仮想アクセス ポイントの機能は自動的に無効になります。

センサー画面オプションを構成するには、以下の手順に従います

1. 「WIDP センサーを有効にする」を選択すると、アクセス ポイントは WIDP センサーとして動作します。このオプションは、既定では選択されていません。
2. アクセス ポイントが WIDP センサーとして動作する時間のスケジュールをドロップダウン メニューから選択するか、「新しいスケジュールの作成...」を選択して別の時間を指定します。既定は「常に有効」です。

プロビジョニング プロファイルのメッシュ ネットワーク設定

この機能は、大規模なカバー エリア全体にスケラブルで安全な無線ネットワーク インフラストラクチャを提供します。この機能を利用して、SonicWave アクセス ポイントを配備および管理できます。

トピック:

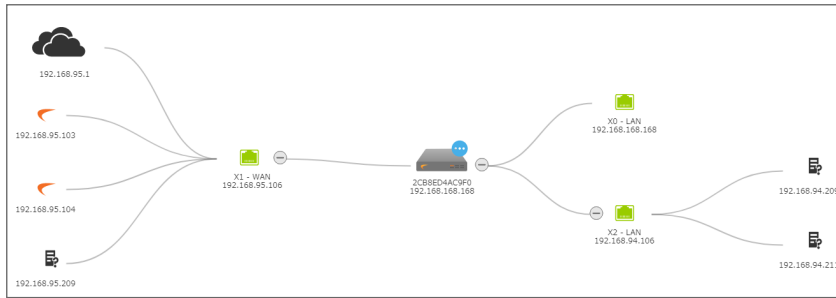
- [メッシュ ネットワークのセットアップ](#)
- [マルチホップ メッシュ ネットワークの有効化](#)
- [アクティブ/アクティブ クラスタリング フルメッシュ](#)

メッシュ ネットワークのセット アップ

メッシュ ネットワークをセットアップするには、以下の手順に従います

1. 「マルチホップ メッシュ ネットワークの有効化」の説明に従って、ファイアウォールの SonicWave プロファイルでメッシュを有効にします。
2. イーサネット ケーブルによって、各 SonicWave をこのファイアウォールに接続します。
3. SonicWave の状態が「利用可能」になったら、その装置からケーブルを外します。
4. 1 つの SonicWave をファイアウォールに接続したままにします。
5. 切断した SonicWave を、所定の場所に移動します。
6. すべての SonicWave の電源を入れます。

7. ネットワークを表示するには、「デバイス>アクセスポイント>トポロジ表示」に移動します。



マルチホップ メッシュ ネットワークの有効化

マルチホップ メッシュ ネットワークを有効にするには、以下の手順に従います

1. 「デバイス>アクセスポイント>設定」ページに移動します。
2. 「アクセスポイントプロビジョニングプロファイル」をクリックします。
3. SonicWave プロファイルの編集アイコンをクリックします。「SonicWave プロファイルの編集」ダイアログが表示されます。
4. 「メッシュネットワーク」を選択します。



5. メッシュ ネットワークに使用する無線を選択します。
 - 5GHZ 無線
 - 2.4GHZ 無線
6. SonicPointAC の無線帯域メッシュを有効にするには、「メッシュを有効にする」を選択します。
7. 「メッシュ SSID」に、WLAN ネットワークの SSID を入力します。
8. 「メッシュ PSK」に、事前共有鍵を入力します。
9. 「メッシュ RSSI しきい値」に、しきい値を入力します。既定値は **-80** です。
10. 「OK」をクリックします。

アクティブ/アクティブ クラスターリングフルメッシュ

アクティブ/アクティブ クラスターリングのフルメッシュ設定は、アクティブ/アクティブ クラスターリングの設定オプションを強化したもので、ネットワーク内のあらゆる単一障害点を回避します。ファイアウォールをはじめとするすべてのネットワーク デバイスは、完全な冗長化のために連携されます。フルメッシュでは、デバイス (セキュリティ装置/スイッチ/ルータ) であればリンクであれば、一切の単一障害点が展開に存在しないことが保証されます。すべてのデバイスは、接続先のデバイスに二重に配線されます。フルメッシュによるアクティブ/アクティブ クラスターリングは、実現可能な最高レベルの可用性と高いパフォーマンスを提供します。下のテーブルを参照してください。

- ① **重要:** セキュリティ装置のアップストリーム側ネットワーク内にあるルータは、Virtual Router Redundancy Protocol (VRRP) 向けにあらかじめ構成されている必要があります。
フル メッシュ配備では、ポート冗長化が有効かつ実現されている必要があります。

アクティブ/アクティブ クラスタリング フル メッシュのメリット

コア ネットワーク内に単一障害点が存在しない	アクティブ/アクティブ クラスタリング フルメッシュ配備では、セキュリティ装置だけでなく、コア ネットワーク全体にわたって単一障害点が存在しません。パス上のスイッチ、ルータ、セキュリティ装置に同時に障害が発生した場合でも、トラフィックフローの代替パスが必ず利用できるため、最高レベルの可用性を実現できます。
ポート冗長化	アクティブ/アクティブ クラスタリング フルメッシュでは、各クラスタ ノード内の HA 冗長化や、クラスタ内のノード レベルの冗長化に加え、冗長ポートも利用します。ポート冗長化では、プライマリ ポートに障害が発生した場合、バックアップリンクがトランスペアレントな形で処理を引き継ぎます。この場合、デバイスレベルのフェイルオーバーは必要ありません。

プロビジョニング プロファイルの 3G/4G/LTE WWAN 設定

- ① **補足:** USB モデムを設定しない場合、このセクションはスキップできます。

この機能は、SonicWave デバイスのように無線アクセス ポイントを使用するファイアウォール装置に、追加の無線 WAN ソリューションを提供するものです。USB モデム デバイスを SonicWave に接続すると、ダイヤルアップ動作を行ってインターネットに接続します。接続すると、SonicWave はファイアウォールの WWAN デバイスとして機能し、WAN アクセスを提供します。

モデムを最初に設定する場合、このオプションの自動発見機能を利用するために、ウィザードを使用することができます。

トピック:

- [3G/4G/LTE WWAN プロファイルの手動設定](#)
- [3G/4G/LTE WWAN ウィザードの使用](#)
- [複数の USB モデム間の負荷分散の設定](#)

3G/4G/LTE WWAN プロファイルの手動設定

3G/4G/LTE WWAN プロファイルを手動で構成したり、手動で変更したりするには、以下の手順に従ってください。

モデムを WWAN として手動で構成するには、以下の手順に従います:

1. 「3G/4GWWAN」をクリックします。



2. 「3G/4G/LTE モデムを有効にする」オプションをオンにします。
3. WAN VLAN インターフェースへの関連付けドロップダウンメニューから VLAN インターフェースを選択します。
ドロップダウンメニューにインターフェースが表示されない場合は、定義する必要があります。詳細については、『SonicOS 6.5 システム セットアップ』の「ネットワーク>システム>インターフェース」セクションを参照してください。
① **補足:** VLAN インターフェースを構築する場合、ゾーンを WAN ゾーンにして、親インターフェースをアクセスポイントが接続されている物理インターフェースにしてください。
3G USB モデムについては、IP 割当を静的に設定して、プライベート IP アドレスを割り当ててください。「ゲートウェイ」と「DNS サーバ」フィールドは空白のまま残します。
4G と QMI モデムについては、IP 割当を DHCP に設定します。
4. 「接続プロファイル」セクションで、「接続プロファイルを有効にする」オプションをオンにします。
① **補足:** 従来の 3G/4G モデムには、ダイヤルアップ用の接続プロファイルを必要とするものがあります。
5. 「国」フィールドには、アクセスポイントが配備される国を選択してください。
6. ドロップダウンメニューからサービスプロバイダを選択します。
7. ドロップダウンメニューから「プラン種別」を選択します。選択によって、他のフィールドが自動的に生成されます。
8. 必要があればユーザ名とパスワードを適切なフィールドに入力します。
9. 画面上のすべての設定が完了したら、「OK」を選択します。

3G/4G/LTE WWAN ウィザードの使用

ウィザードを使ってモデムを構成するには、以下の手順に従います:

1. 「3G/4GWWAN」をクリックします。
2. 一番下までスクロールし、「3G/4G/LTE ウィザード」を選択します。
3. 「次へ」ボタンを選択します。
4. 「VLAN インターフェース」をドロップダウンメニューから選択するか、「新しい VLAN インターフェースの作成」のオプションをオンにします。

新しい VLAN インターフェースの作成を選択する場合は、残りのフィールドが有効化されます。要求されたデータを入力します。

- ① **補足:** 「IP 割当」を「DHCP」に設定すると、「IP アドレス」、「サブネット マスク」、「デフォルト ゲートウェイ」のフィールドは入力不可になります。

5. 「次へ」ボタンを選択します。
6. 「国」フィールドには、アクセスポイントが配備される国を選択してください。
7. ドロップダウンメニューから「サービスプロバイダ」を選択します。
8. ドロップダウンメニューから「プラン種別」を選択します。選択によって、他のフィールドが自動的に生成されます。
9. 必要があればユーザ名とパスワードを適切なフィールドに入力します。
10. 「次へ」ボタンを選択します。
11. 再度「次へ」を選択して、設定を反映します。

複数のUSBモデム間の負荷分散の設定

複数の SonicPoint/SonicWave および複数の 3G/4G モデム (それぞれ最低 2 台) が使用可能な場合、これらの SonicPoint/SonicWave およびモデムの複数のペア間で負荷分散を実行できます。

複数の 3G/4G モデムを使用して負荷分散を構成するには、以下の手順に従います:

1. 手動で、または 3G/4G/LTE ウィザードを使用して、SonicPoint/SonicWave と 3G/4G モデムの各ペアに一意の VLAN を割り当てます。
2. これらの VLAN インターフェースを「ネットワーク>システム>フェイルオーバーおよび LB」で負荷分散グループに追加します。詳細については、『SonicOS システム セットアップ』管理マニュアルを参照してください。

プロビジョニングプロファイルの Bluetooth LE 設定

SonicWave シリーズは、標準的な Bluetooth のサブセットである Bluetooth 低消費電力 (BLE) 機能を備えています。BLE を使用すると、特に iBeacon 対応装置に非常に近接している場合、スマートフォン、タブレット、SonicWall モバイルアプリケーション、その他の SonicWaves などの他のデバイスを SonicWave アクセスポイントに簡単に接続できます。BLE は位置推定も提供します。

iBeacon はアップルが開発したプロトコルです。さまざまなベンダーが、近くの携帯電子デバイスに識別子をブロードキャストする iBeacon 互換の BLE デバイスを製造しています。このテクノロジーにより、スマートフォン、タブレット、その他のデバイスは、iBeacon の近くにいるときにアクションを実行できます。

Bluetooth 低消費電力設定を有効にして構成するには、以下の手順に従います:

1. 「デバイス>アクセスポイント>設定」ページに移動します。
2. 「アクセスポイントプロビジョニングプロファイル」をクリックします。
3. SonicWave の編集アイコンを選択します。「SonicWave プロファイルの編集」ダイアログが表示されます。
4. 「Bluetooth LE」を選択します。



5. BLE アドバタイズメントを有効にするには、「アドバタイズメントを有効にする」をオンにします。このオプションは、既定では選択されていません。このオプションを有効にすると、「iBeacon を有効にする」オプションが

使用可能になります。

① | **補足:** BLE アドバタイズメントを有効にすると、2.4G 無線周波数に影響または干渉する可能性があります。

6. BLE デバイスが識別子をブロードキャストするように iBeacon を有効にするには、「**iBeacon を有効にする**」を選択します。このオプションは、既定では選択されていません。従属するフィールドが使用可能になります。

7. フィールドに情報を入力します。

- **UUID** – UUID の 36 文字を入力します。例を以下に示します。

51b9d455-6a32-426c-b5cc-524181c24df3

- **メジャー** – 同じ地理的グループで有効な ID を入力します。有効な範囲は 0 ~ 65535 で、既定値は 0 です。

- **マイナー** – 同じ地理的グループのセカンダリ ID を入力します。範囲は 0 から 65535 で、既定値は 0 です。

① | **ヒント:** 異なる UUID を使用して異なる地理的グループを識別し、メジャーおよびマイナー オプションを使用して地理的グループ内の領域を識別します。たとえば、1 つの建物に BLE を使用して複数の SonicWave 装置を展開し、これらの SonicWave 装置に同じ UUID を設定したとします。同じフロアの SonicWave 装置は、同じメジャー番号を持ちますが、同じフロアの異なる場所では異なるマイナー番号を持ちます。このように、お使いになっているモバイル デバイスの近くには SonicWave 装置がありません。

8. 「OK」をクリックします。

アクセスポイント プロファイルの削除

① | **補足:** 事前定義されているプロファイルは削除できません。削除できるのはユーザが追加したのだけです。

個々のプロファイルまたはプロファイルのグループの削除は、「**デバイス > アクセスポイント > 設定**」ページの「**アクセスポイントプロビジョニングプロファイル**」セクションで行えます。

- 1 つのアクセスポイントプロファイルを削除するには、以下の手順に従ってください。
 1. マウスカーソルをアクセスポイントプロファイルに重ね、「**削除**」をクリックします。確認メッセージが表示されます。
 2. 「OK」をクリックします。
- 1 つ以上のアクセスポイントプロファイルを削除するには、以下の手順に従います。
 1. 削除するアクセスポイントの名前の横にあるチェックボックスをオンにします。
 2. 「**削除**」アイコンをクリックします。確認メッセージが表示されます。
 3. 「OK」をクリックします。

製品特有の設定に関する注意事項

SonicPoint の設定手順は、対象の SonicPoint がシングル無線 (SonicPointN) デバイスであるか、デュアル無線 (SonicWave、SonicPoint AC、SonicPoint NDR) デバイスであるかによって若干異なります。

アクセスポイントの管理

「SonicPoint / SonicWave オブジェクト」セクションには、接続されたアクセスポイントの設定が表示されます。また、それらを編集したりその他のアクションを実行したりするためのアイコンがあります。

このテーブルには、アクセスポイントに構成された以下の値が表示されます。

列	説明
#	行参照番号
名前	アクセスポイントの名前
インターフェース	アクセスポイントが接続されているファイアウォール インターフェース番号とゾーン
ネットワーク設定	アクセスポイントの IP アドレス、MAC アドレス、および管理指定
状況	利用可能、応答なし、またはその他のアクセスポイント状態
5GHz 無線	この無線、周波数、および 802.11 プロトコルのアクセスポイント SSID (MSSID) 名
5GHz 無線チャンネル	帯域設定、チャンネル、および無線状態 (有効、アクティブなど)
2.4GHz 無線	この無線、周波数、および 802.11 プロトコルのアクセスポイント SSID (MSSID) 名
2.4GHz 無線チャンネル	帯域設定、チャンネル、および無線状態 (有効、アクティブなど)
3G/4G/LTE	3G、4G、または LTE の有効/無効状態とバインディング情報
有効	アクセスポイントが有効な場合に選択
SSH	アクセスポイントへの SSH アクセス用のボタン

トピック:

- [アクセスポイントオブジェクトの削除](#)
- [アクセスポイントオブジェクトの再起動](#)
- [アクセスポイントオブジェクトの変更](#)

アクセスポイント オブジェクトの削除

個々のアクセスポイントまたはアクセスポイントのグループの削除は、「デバイス > アクセスポイント > 設定」ページの「アクセスポイントオブジェクト」セクションで行えます。

- 1つのオブジェクトを削除するには、以下の手順に従います。
 1. マウスカーソルを重ね、**削除**アイコンをクリックします。確認メッセージが表示されます。
 2. 「OK」をクリックします。
- 1つ以上のオブジェクトを削除するには、以下の手順に従います。
 1. 削除するオブジェクトの横にあるチェックボックスを選択します。
 2. **削除**アイコンをクリックします。確認メッセージが表示されます。
 3. 「OK」をクリックします。

アクセスポイント オブジェクトの再起動

個々のアクセスポイントまたはアクセスポイントのグループの再起動は、「デバイス>アクセスポイント>設定」ページの「アクセスポイントオブジェクト」セクションで行えます。

- 1つのオブジェクトを再起動するには、以下の手順に従います。
 1. 再起動するアクセスポイントの名前の横にあるチェックボックスをオンにします。
 2. 「再起動」をクリックします。確認メッセージが表示されます。
 3. 再起動の種別を選択します。
 - 再起動(既定) - 構成したプロファイル設定で再起動します。
 - 工場出荷時の状態で再起動 - 工場出荷時の設定で再起動します。
- △ **注意:** このオプションを選択すると、アクセスポイントプロファイルが工場出荷時の既定値で上書きされます。
4. 「OK」をクリックします。

アクセスポイント オブジェクトの変更

アクセスポイントオブジェクトの変更は、「デバイス>アクセスポイント>設定」ページで行えます。

1. 変更するオブジェクトにマウスカーソルを重ね、編集アイコンをクリックします。
 2. 変更したい設定を変更します。
 3. 「OK」を選択して新しい設定を保存します。
- ① **補足:** ネットワーク装置が自動発見プロセスを実行すると、新しい SonicPoint/SonicWave アクセスポイントが自動的に追加されます。

ファームウェアの管理

「デバイス>アクセスポイント>ファームウェアの管理」ページには、最新の SonicPoint/SonicWave ファームウェアを入手し、それを使用してアクセスポイントを更新する方法が表示されます。

ファームウェア管理

Q 検索...

ファームウェアイメージ	バージョン	状況	ビルド日
SonicPoint-N	sw_spn_eng_5.8.0.1.7.bin.sig	●	該当なし
SonicPoint-NDR	sw_spn_eng_7.8.0.1.7.bin.sig	●	該当なし
SonicPoint-Ni/Ne	sw_spn_eng_6.8.0.1.7.bin.sig	●	該当なし
SonicPoint-ACe/ACi/NZ	sw_spn_eng_9.0.1.5.9.bin.sig	●	該当なし
SonicWave-432e/432i/432e	sw_spw_eng_9.1.3.0.46.bin.sig	●	該当なし
SonicWave-231c/224w/231o	sw_spw_eng_9.2.3.0.46.bin.sig	●	該当なし

ダウンロード URL

SonicPoint-N イメージの URL を手動で指定する

SonicPoint-Ni/Ne イメージの URL を手動で指定する

SonicPoint-NDR イメージの URL を手動で指定する

SonicPoint-AC イメージの URL を手動で指定する

SonicWave-432e/432i/432e イメージの URL を手動で指定する

SonicWave-231c/224w/231o イメージの URL を手動で指定する

キャンセル 適用

トピック:

- [ファームウェアの管理について](#)
- [最新の SonicWall ファームウェアの入手](#)
- [特定の URL からのファームウェアのダウンロード](#)
- [ファームウェアをアクセスポイントにアップロードする](#)

ファームウェアの管理について

「ファームウェアの管理」テーブルには、現在のアクセスポイントファームウェアイメージの状況を表示し、新しいファームウェアを取得してアクセスポイントにアップロードするためのボタンがあります。

列	説明
ファームウェアイメージ	ファームウェアイメージのアクセスポイントの種別を表示します。
バージョン	アクセスポイントが一致させる必要がある、ファイアウォールでサポートされているファームウェアバージョンを表示します。新しいバージョンの APファームウェアが提供されると、ファイアウォールがそれに対応していれば、「バージョン」項目に表示され、接続後にアクセスポイントが新しいバージョンに自動的に更新されま

	す。
状況	初期状態で、すべてのファームウェアの状況は、「ダウンロードが必要」となっています。別のファームウェアイメージがファイアウォール バッファにアップロードされると、準備完了を示すチェックマークに変わります。
ビルド日	アップロードされたファームウェアが作成された日付を表示します。
動作	2つのアイコンがあります。 <ul style="list-style-type: none"> ● ファームウェアのアップロード - クリックすると、ダウンロードしたファームウェアがファイアウォール バッファにアップロードされます。上記の「バージョン」で説明したように、サポートされている新しい APファームウェアはアクセスポイントに自動的にプッシュされます。ファームウェアを既に動作状態にあるアクセスポイントにプッシュするには、内部設定を使用する必要があります。内部設定の使用については、SonicWall サポートにお問い合わせください。 ● ファームウェアのリセット - クリックすると、ダウンロードされたファームウェアイメージがバッファから削除されます。

このページの「ダウンロード URL」セクションでは、HTTP を介して特定の場所から アクセスポイントファームウェアイメージをダウンロードすることができます。これにより、SonicWall サポートが提供する公式リリース前のバージョンなど、代替のファームウェアをロードできます。

最新の SonicWall ファームウェアの入手

SonicWall から最新版のファームウェアを入手するには、以下の手順に従います

1. 「デバイス > アクセスポイント > ファームウェアの管理」ページに移動します。
2. 「ファームウェアの管理」テーブルで、目的のアクセスポイントにマウスカーソルを重ね、編集（ファームウェアのアップロード）アイコンをクリックします。

ファームウェア イメージ	バージョン	状態	ビルド日
SonicPoint-N	sw_spt_eng_5.8.0.1.7_bin.sig	●	該当なし
SonicPoint-NDIR	sw_spt_eng_7.8.0.1.7_bin.sig	●	該当なし
SonicPoint-NiNe	sw_spt_eng_6.8.0.1.7_bin.sig	●	該当なし
SonicPoint-Ace/ACLIN2	sw_spt_eng_9.0.1.5.9_bin.sig	●	該当なし
SonicWave-4320/432/432e	sw_spw_eng_9.1.3.0.46_bin.sig	●	該当なし
SonicWave-2310/224w/2310	sw_spw_eng_9.2.3.0.46_bin.sig	●	該当なし

3. 「ファームウェアのアップロード」ダイアログボックスで、software.sonicwall.com リンクを選択します。

ファームウェアのアップロード

● 新しいファームウェアをアップロードすると、既存の「アップロードされたファームウェア」のイメージは上書きされます。

最新のファームウェアは、software.sonicwall.com で入手できます。ローカルディスクに最新のファームウェアをダウンロードし、このダイアログを使用して SonicWall 装置にアップロードします。「参照」、「ファイルの選択」などのボタンを使用して、アップロードするファームウェアファイルを選択します。

ファームウェア ファイルは、.sig 拡張子の付いた「sw_firmware.sig」のような名前になっています。

ファームウェア ファイル

4. `sw_firmware.sig` などのファイルは、Downloads フォルダなどの既定の場所に保存されます。

特定の URL からのファームウェアのダウンロード

URL の場所を手動で指定し、そこからファームウェアイメージをダウンロードしてアクセスポイントで使用できます。

イメージの URL を指定するには、以下の手順に従います:

1. 「デバイス > アクセスポイント > ファームウェアの管理」に移動します。
2. 「ダウンロード URL」セクションまでスクロールします。
3. ダウンロードするイメージの種別オプションをオンにします。フィールドが使用可能になります。

ダウンロード URL

SonicPoint-N イメージの URL を手動で指定する http://

SonicPoint-Ni/Ne イメージの URL を手動で指定する

SonicPoint-NDR イメージの URL を手動で指定する

SonicPoint-AC イメージの URL を手動で指定する

SonicWave-432o/432i/432e イメージの URL を手動で指定する

SonicWave-231c/224w/231o イメージの URL を手動で指定する

キャンセル 適用

4. フィールドにイメージの場所の URL を入力します。

http://

5. 「適用」を選択します。ファイルはファイアウォールバッファに保存されます。

ファームウェアをアクセスポイントにアップロードする

ローカルに保存されたファームウェアイメージファイルをアクセスポイントにアップロードできます。保存されるファイルは、公式の SonicWall ファームウェアバージョン、または手動で指定した URL からダウンロードされたファームウェアイメージです。

ファームウェアイメージをアクセスポイントにアップロードするには、以下の手順に従います:

1. 次のいずれかを実行して、ファームウェアイメージを取得し、ローカルワークステーションに保存します。
 - 「最新の SonicWall ファームウェアの入手」の説明に従って、公式の SonicWall バージョンをダウンロードします。
この手順では、ローカルコンピュータにイメージファイルを保存した後、「ファームウェアのアップロード」ダイアログにとどまります。
 - 「特定の URL からのファームウェアのダウンロード」の説明に従って、手動で指定した URL からファームウェアイメージをダウンロードします。
2. ファームウェアイメージをアップロードする場合は、目的のアクセスポイント種別の行の「動作」の下にある「ファームウェアのアップロード」を選択して、「ファームウェアのアップロード」ダイアログ ボックスを開きます。software.sonicwall.com へのリンクを使用してイメージファイルをダウンロードした場合、ダイアログは既に開いています。

3. 「ファームウェアのアップロード」ダイアログで、「参照」を選択し、保存されたイメージに移動して選択します。「ファームウェアのアップロード」ダイアログに、ファームウェア イメージ名が表示されるようになります。
4. 「ファームウェアのアップロード」ダイアログで、「アップロード」を選択します。

ファームウェアイメージは、セキュリティ装置のバッファにアップロードされます。アップロード中、「状況」にアップロードの割合が示されます。

アップロードが完了すると、「バージョン」列に新しいファームウェア バージョンが表示されます。アクセスポイントが接続されている場合は、ファームウェアバージョンが自動的にプッシュされ、「状況」の表示がファームウェアイメージの準備完了を示すチェックマークに変わり、「ビルド日」にイメージの作成日付が表示されます。現在、アクセスポイントは新しいファームウェアを実行しています。
5. ダウンロードしたファームウェアをバッファから消去するには、「ファームウェアのリセット」をクリックします。「状況」インジケータと「ビルド日」は既定の表示に戻ります。

フロアプランの表示

「デバイス>アクセスポイント>フロアプラン表示」ページでは、SonicOS ユーザーインターフェースから多数の SonicWave および SonicPoint デバイスをより視覚的な方法で管理できます。また、物理的な位置とリアルタイムの状況も追跡できます。

フロアプラン表示機能は、既存の SonicOS 無線アクセスポイント管理スイートに対するアドオンです。実際の無線配備環境をリアルタイムで図示し、新規の配備による無線通信範囲を推定する上で役立ちます。FPMV はまた、コンテキストメニューから、アクセスポイント統計の確認、リアルタイムのアクセスポイント状態監視、アクセスポイント構成、アクセスポイント除去、さらに RF 範囲の表示まで提供する、ワンストップのコンソールです。

次の図は、標準的なフロアプラン表示の例です。



トピック:

- [フロアプランの管理](#)
- [アクセスポイントの管理](#)

フロアプランの管理

フロアプラン表示機能には、フロアプランを表示、追加、編集する多くの方法があります。このセクションでは、最も通常のを説明します。

トピック:

- [フロアプランの選択](#)
- [フロアプランの作成](#)
- [フロアプランの編集](#)
- [測定用尺度の設定](#)

フロアプランの選択

「デバイス>アクセスポイント>フロアプラン表示」ページに移動し、左上の ≡ (フロアプランリスト) アイコンをクリックして、表示するフロアプランを選択します。

フロアプランの作成

フロアプランを作成するには、以下の手順に従います

1. 「デバイス>アクセスポイント>フロアプランの表示」ページに移動します。
2. + アイコンをクリックします。「新規フロアプランの追加」ダイアログが表示されます。

フロアプランの追加

フロアプラン名

説明

階数

フロアプランファイル

3. プランを説明するフィールドに入力します。
4. 「OK」をクリックします。

フロアプランの編集

フロアプランを編集するには、以下の手順に従います

1. 「デバイス>アクセスポイント>フロアプランの表示」ページに移動します。
2. 「Edit(編集)」アイコンをクリックします。「フロアプランの編集」ダイアログが表示されます。

次のフロアプランの編集: [新しいフロ...

フロアプラン名

説明

画像の幅

画像の高さ

縮尺

フロアプラン ファイル


フロアプランデバイス

🔍 + 🗑

<input type="checkbox"/> 名前	MAC アドレス	モデル
データなし		
総数: 0 件		

- 必要に応じてフィールドを変更します。
- 「OK」をクリックします。


リスト上のプランを編集するには、以下の手順に従います

- 「デバイス > アクセスポイント > フロアプランの表示」ページに移動します。
-  (フロアプランリスト) アイコンをクリックします。
- 編集するフロアプランのチェックボックスを選択し、**編集**アイコンをクリックします。「フロアプランの編集」ダイアログが表示されます。
- 必要に応じてフィールドを変更します。
- 「OK」をクリックします。

測定用尺度の設定

実際の距離 (フィート) と、フロアプランの図を構成しているピクセルの関係を示すために、測定縮尺を設定する必要があります。この数値は、RF範囲の推定の支援にも使用できます。

測定用尺度を設定するには、以下の手順に従います

- 「デバイス > アクセスポイント > フロアプランの表示」ページに移動します。
- ページ左下の  (測定距離と領域) アイコンにマウスカーソルを重ね、「測定の新規作成」オプションをクリックします。
- 測定の作成を開始するには、アクセスポイントをマップに追加して「測定終了」をクリックします。

アクセスポイントの管理

アクセスポイントの状況が色で表示されます:

● オンライン ● オフライン ● ビジー

個々のアクセスポイントは、「フロアプラン表示」ページで管理できます。

トピック:

- 利用可能なデバイス
- 追加されたアクセスポイント
- アクセスポイントの削除
- 画像としてエクスポート

利用可能なデバイス

展開に利用可能なアクセスポイントが、「利用可能なデバイス」リストに表示されます。通常、リストは右上隅に表示されます。角にある「x」をクリックすると閉じることができます。リストを表示するには、「アクセスポイント > フロアプラン表示 > フロアプラン情報」をクリックします。

これらのアクセスポイントをフロアプランにドラッグアンドドロップして、配備したい場所に置くことができます。作業が終わったら、必ず「プランの保存」を行ってください。

① | **補足:** 既にフロアプランに追加されているアクセスポイントは、このパネルには表示されません。

追加されたアクセスポイント

配備されたアクセスポイントは、「追加されたアクセスポイント」リストに表示されます。リストは通常左上隅に表示されますが、ドラッグアンドドロップで任意の場所に移動できます。角にある「x」をクリックすると閉じることができます。

これらのアクセスポイントをフロアプランにドラッグアンドドロップして、別の場所に置くことができます。また、プランから削除することもできます。作業が終わったら、必ず「プランの保存」を行ってください。

① | **補足:** 既にフロアプランに追加されているアクセスポイントは、このパネルには表示されません。

アクセスポイントの削除

すべてのアクセスポイントを削除するには、以下の手順に従います

1. 「デバイス > アクセスポイント > フロアプラン表示」に移動します。
2. 「詳細」オプションをクリックします。
3. 「現在のフロアプランからすべての追加されたアクセスポイントを削除する」を選択します。

画像としてエクスポート

フロアプランの画像をエクスポートするには、以下の手順に従います

1. 「デバイス>アクセスポイント>フロアプランの表示」ページに移動します。
2. 「詳細」オプションをクリックします。
3. 「画像としてエクスポート」を選択し、画像形式を選択します。
4. 後でアクセスできる場所に保存します。

コンテキストメニュー

さまざまなコンテキストメニューを動作させるために、マウスを利用できます。

- フロアプランのアクティブなアクセスポイントの上にマウスポインタを重ねると、ID、状況、クライアント数、稼働時間を含む、アクセスポイント情報をポップアップ表示します。
- アクセスポイントをクリックすると、RF範囲が表示されます。
- アクセスポイントをダブルクリックすると、リアルタイム監視ウィンドウが表示されます。
- アクセスポイントを右クリックすると、コンテキストメニューが表示されます。コンテキストメニューは、編集、統計の表示、監視状況その他のオプションがあります。

ステーション状況

「ステーション状況」ページでは、各アクセスポイントの状況が報告されます。

テーブルには、各アクセスポイントに接続されている無線クライアントに関する項目が個別に表示されます。テーブルのセクションはアクセスポイント別に分かれています。アクセスポイントごとに、現在接続されているクライアントがすべて表示されます。

左上隅の「再表示」ボタンを選択すると、一覧が更新されます。

侵入検知サービス

Rogue (悪意の侵入者) アクセスポイントは、無線セキュリティに対する最も深刻かつ油断のならない脅威の1つです。一般に、ネットワーク上での使用が許可されていないアクセスポイントは、悪意のあるアクセスポイントとして認識されます。保護されていないアクセスポイントの利便性や可用性と、ネットワークへの追加のしやすさによって、Rogue (悪意の侵入者) デバイスの導入を許す環境が形作られています。多種多様な脅威が生み出されています。

- 悪意のあるデバイスへの無意識的な接続
- 保護されていないチャンネルを介した機密データの転送
- LAN リソースへの不要なアクセスなど、

これは特定の無線デバイスのセキュリティ不足ではなく、無線ネットワーク全体のセキュリティの脆弱性を示しています。

ファイアウォールでは、侵入検知サービス (IDS) によって、一般的な不正無線アクティビティの大半を認識して対応策を講じることができるようになり、そのセキュリティ機能が大幅に向上します。IDS は、802.11a、802.11g、および 802.11n 無線帯域をスキャンすることによって検出できるアクセスポイントをすべて報告します。

「デバイス > アクセスポイント > IDS」ページには、ファイアウォールとその関連アクセスポイントによって検出されるデバイスがすべて報告され、正当なアクセスポイントを承認することができます。



次の表に、「IDS」ページに表示される「検出されたアクセスポイント」テーブルと項目を示します。

テーブルの列または項目	説明
項目	
再表示	画面を再表示して、ネットワーク内のアクセスポイントの最新の一覧を表示します。
すべてスキャン	すべてのアクセスポイントを呼び出し、接続されたデバイスを特定する作業を開始する。
表示形式: アクセスポイント	複数のアクセスポイントがある場合は、「アクセスポイント」ドロップダウンメニューで個々のデバイスを選択することも、また、すべてのアクセスポイントが見たい場合は「すべてのアクセスポイント」を選択することもできます。
「検出されたアクセスポイント」テーブル	
アクセスポイント	アクセスポイント名は、「すべての SonicPoint」が「表示形式: アクセスポイント」ドロップダウンメニューで選択されている場合にのみ表示されます。

MACアドレス (BSSID)	検出されたアクセスポイントの無線インターフェースの MACアドレスです。
SSID	デバイスの無線 SSID です。
種別	デバイスによって使用される無線帯です。2.4 GHz または 5 GHz です。
チャンネル	デバイスで使用される無線チャンネルです。
認証	認証種別です。
暗号	暗号モードです。
製造元	アクセスポイントの製造元です。
信号強度	検出された無線信号の強度です。
最高速度	アクセスポイントの無線で利用できる最高転送速度です。
許可	編集アイコンを選択すると、許可されたデバイスのアドレスオブジェクトグループにデバイスが追加されます。

トピック:

- [アクセスポイントのスキャン](#)
- [アクセスポイントの許可](#)

アクセスポイントのスキャン

アクティブスキャンは、セキュリティ装置の起動時に実行されます。起動後にスキャンを命令した場合、無線クライアントの接続は数秒間切断されます。スキャンはトラフィックに次のように影響します。

- 非永続的で処理状態を把握しないプロトコル (HTTP など) には悪影響を及ぼしません。
- 永続的な接続 (FTP などのプロトコル) の場合は、接続状態が悪くなるか、切断されます。
- WiFiSec 接続は、クライアントが切断に気付かないように自動的に再確立され、再開される必要があります。

△ **注意:** 「すべてスキャン」をクリックすると、スキャン実行中に動作中の無線クライアントすべてが切断されます。サービス中断が問題になる場合は、SonicWall セキュリティ装置がアクセスポイントモードにある間はスキャンを命令しないことをお勧めします。アクティブなクライアントがなくなるまで、または一時的な切断であれば許容されるようになるまで待ちます。

スキャンを実行するには、以下の手順に従います:

1. 「デバイス > アクセスポイント > IDS」ページに移動します。
2. 「表示形式」で: 「アクセスポイント」ドロップダウンメニュー (テーブルの最上部) で、すべてのデバイスをスキャンするには「すべてのアクセスポイント」を選択し、単一のデバイスをスキャンするには特定のアクセスポイントを選択します。
3. テーブルの上部で:
 - すべてのアクセスポイントをスキャンする場合には、「すべてスキャン」をクリックします。
 - アクセスポイントだけをスキャンする場合、「表示形式: アクセスポイント」ドロップダウンメニューからアクセスポイントを選択し、「一アクセスポイントのスキャンを実行」のドロップダウンメニューで、「両方の無線のスキャン」、「無線 (2.4GHz) のスキャン」または「無線 (5GHz) のスキャン」オプション

のいずれかを選択します。



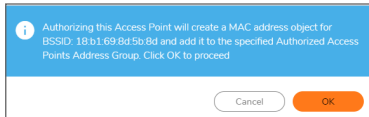
4. スキャンを実行することを確認します。

アクセスポイントの許可

セキュリティ装置によって検出されたアクセスポイントは、その動作を許可するようにセキュリティ装置が構成されるまでは、Rogue (悪意の侵入者) と見なされます。

アクセスポイントを許可するには、以下の手順に従います:

1. 「デバイス > アクセスポイント > IDS」ページに移動します。
2. 許可するアクセスポイントの「許可」列にある編集アイコンを選択します。確認ダイアログが表示されます。



3. 「OK」をクリックします。
4. アクセスポイントの MAC アドレスが追加されたことを確認して、承認が成功したことを確認してください。(詳細については、「SonicOS システムセットアップ」を参照してください)

高度なIDP

高度な侵入検知と防御 (IDP)、または無線侵入検知と防御 (WIDP) は、電波スペクトルを監視して、許可されていないアクセスポイントの存在を検知 (侵入検知) し、管理者設定に基づいて自動的に防止策を実行 (侵入防御) します。アクセスポイント上で高度なIDPを有効にすると、無線機能は専用のIDPセンサーとして機能します。

△ | **注意:** SonicWallアクセスポイント無線で高度なIDPを有効にすると、アクセスポイント機能は無効になり、すべての無線クライアントが切断されます。

SonicOS の無線侵入検知と防御は、SonicPoint と SonicWave アクセスポイントに基づいており、SonicWall ゲートウェイと連係します。この機能は、これらのアクセスポイントを、SonicWall ネットワークに接続している許可されていないアクセスポイントを検知するための専用 WIDPセンサーとして使用します。これには、KRACK Man-in-the-Middle アクセスポイントの検知が含まれます。

△ | **注意:** WIDP センサーとして構成された SonicPoint N は、アクセスポイントとして機能できません。

アクセスポイントが悪意のあるアクセスポイントとして特定されると、その MACアドレスが「すべての悪意のあるアクセスポイント」アドレスオブジェクトグループに追加されます。

トピック:

- [プロフィールで無線IDPを有効にする](#)
- [無線IDPの設定](#)
- [KRACK スニッファ パケットの表示](#)

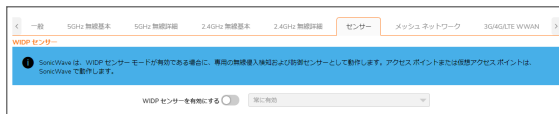
プロフィールで無線IDPを有効にする

スキャンのスケジュールを設定するなど、アクセスポイントプロフィールで無線侵入検知と防御を有効にできます。アクセスポイントプロフィールの詳細については、「[アクセスポイント > 設定](#)」ページの「[プロビジョニングプロフィールの作成/変更](#)」を参照してください。

アクセスポイントプロフィールで高度な無線IDP スキャンを有効にするには、以下の手順に従います:

1. 「[デバイス > アクセスポイント > 設定](#)」ページの「[SonicPoint/SonicWave プロビジョニングプロフィール](#)」セクションに移動します。
2. 目的のインターフェースの **編集** アイコンを選択します。
3. **センサー** を選択します。
① | **ヒント:** 「**センサー**」画面は、すべての SonicPoint または SonicWave プロフィールで同じです。

4. 「WIDP センサーを有効にする」を選択します。ドロップダウンメニューが使用可能になります。



5. ドロップダウンメニューから、IDPスキャンに対する適切なスケジュールを選択するか、「スケジュールの作成」を選択して個別スケジュールを作成します。
注意: SonicPoint/SonicWave 無線で高度なIDP スキャンを有効にすると、そのアクセスポイント機能は無効になり、すべての無線クライアントが切断されます。
6. 「OK」をクリックします。

無線IDPの設定

無線 IDP 構成を行うには、以下の手順に従います:

1. 「デバイス > アクセスポイント > 高度なIDP」ページに移動します。



2. 「無線侵入検知と防御を有効にする」を選択して、装置による悪意のあるアクセスポイント (KRACK Man-in-the-Middle アクセスポイントを含む) の検索を有効にします。このオプションは、既定では選択されていません。従って、選択すると他のオプションが選択可能になります。
補足: ① 検出されたすべてのアクセスポイントが、「デバイス > アクセスポイント > IDS」ページの「検出されたアクセスポイント」テーブルに表示され、許可する任意のアクセスポイントを承認できます。
3. 「許可されたアクセスポイント」に対して、許可されたアクセスポイントに割り当てるアドレスオブジェクトグループを選択します。既定では、これは「すべての許可されたアクセスポイント」に設定されます。
補足: ① SonicPoint N には、アクセスポイントモードの仮想アクセスポイント (VAP) は作成されません。ステーションモードの VAP が 1 つ作成され、IDSスキャンの実行、および保護されないアクセスポイントへの接続とプローブ送信に使用されます。
4. 「悪意のあるアクセスポイント」に対して、許可されていないアクセスポイントに割り当てるアドレスオブジェクトグループを選択します。既定では、これは「すべての悪意のあるアクセスポイント」に設定されます。

5. どの AP を悪意があるか判別するための以下の 2 つのオプションから 1 つを選択します (同時に 2 つとも有効にすることはできません)。
 - 「許可されていないアクセスポイントを「悪意のあるアクセスポイントリスト」に追加する」は、検出されたすべての許可されていない AP を (それらがお使いのネットワークに接続しているかどうかにかかわらず)、自動的に Rogue リストに割り当てます。
 - 「接続された許可されていないアクセスポイントを「悪意のあるアクセスポイントリスト」に追加する」は、許可されていない AP がお使いのネットワークに接続している場合のみ、それらを Rogue リストに割り当てます。以下のオプションによって、IDP が接続された悪意のある AP を検出する方法が決まります。両方を選択することができます。
 - 接続された悪意のあるアクセスポイントを検知するために ARP キャッシュ検索を有効にする – 高度な IDP は、クライアント MAC アドレスを ARP キャッシュから検索します。それが発見されて、接続している AP が許可されていない場合に、その AP は悪意として分類されます。
 - 接続された悪意のあるアクセスポイントを検知するためにアクティブ監視を有効にする – SonicPoint/SonicWave が疑わしいデバイスに接続して、ファイアウォールのすべての LAN、DMZ、WLAN インターフェースにプローブを送信します。ファイアウォールがこれらのプローブのいずれかを受信した場合に、その AP は悪意として分類されます。
6. 許可リストの中にはないが管理されているアクセスポイントと同じ SSID を持つデバイスを Rogue リストに追加するには、「Evil Twin (偽装アクセスポイント) を「悪意のあるアクセスポイントリスト」に追加する」を選択します。
7. Rogue リストと一致する送信元 IP アドレスを持つ受信トラフィックをすべて破棄するには、「悪意のあるアクセスポイントとそれに参加するクライアントを不参加にする」を選択します。「悪意のある装置の IP アドレス」ドロップダウンメニューで、次のいずれかを実行します。
 - 「すべての悪意のあるデバイス」(既定)、または作成済みのアドレスオブジェクトグループを選択します。
 - 「IP アドレスオブジェクトグループの作成」を選択して、新しいアドレスオブジェクトグループを作成します。「アドレスオブジェクトグループの追加」ウィンドウが表示されます。
8. 悪意のあるアクセスポイントとの間の通信を停止するために、クライアントに認証解除メッセージを送信するには、「悪意のあるアクセスポイントと関連クライアントを不参加にする」を選択します。
9. 「KRACK MITM AP からクライアントを不参加にする」を選択して、KRACK 防御機能を有効にします。有効にすると、SonicWave は定期的に KRACK Man-in-the-Middle アクセスポイントをチェックし、関連付けられているクライアントを検知すると、そのクライアントを KRACK MITM アクセスポイントから積極的に切り離します。
10. 「適用」を選択して変更を保存します。

KRACK スニッファパケットの表示

「無線侵入検知と防御を有効にする」オプションが有効になっていると、SonicWave は無線環境を定期的にスキャンして KRACK Man-in-the-Middle アクセスポイントおよびそれと情報を交換しているすべてのクライアントを検索します。KRACK は、Key Reinstallation Attack (鍵再インストール攻撃) の頭字語です。

KRACK MITM 攻撃は、実際のアクセスポイントと同じ MAC アドレスを持つ別のチャンネルで実際のアクセスポイントを複製します。KRACK MITM アクセスポイントが検知されると、SonicWave は KRACK MITM と同じチャンネルで監視インターフェースを開き、チャンネル上のパケットを一定期間スニффイングします。MITM アクセスポイントに関連付けられている無線クライアントがあり、「KRACK MITM AP からクライアントを不参加にする」オプションが有効に

なっている場合、そのクライアントは MITM アクセスポイントから切り離されます。次のいずれかのイベントが発生すると、「監視」>「ログ」>「システムログ」ページでログメッセージが報告されます。

- KRACK MITM アクセスポイントが検知された
- MITM アクセスポイントと通信しているクライアントが検知された
- クライアントが MITM アクセスポイントから切り離された

スニффイングは KRACK 検知プロセス中に行われるため、キャプチャされたパケットは SonicWave のバッファに保存されます。下の画像は、複数の SonicWave からの KRACK スニッフアの結果を示しています。



#	名前	インターフェース	状態	ゾーン	IP	MAC
データなし						

KRACK プロセスを分析するには、SonicWave のダウンロードアイコンをクリックして、パケットデータをファイル `krackSniffer_[SonicWave 名].cap` にエクスポートします。ここで `[SonicWave 名]` は SonicWave の名前です。次に、ファイルを開き、Wireshark または別の PCAP アナライザツールで調査します。

パケット キャプチャ

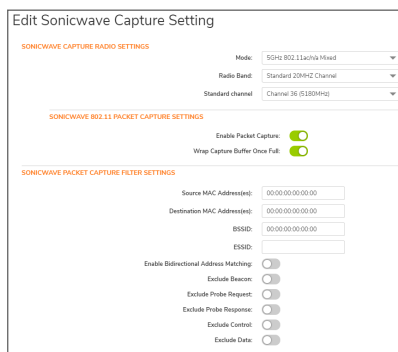
「デバイス>アクセスポイント>パケットキャプチャ」機能は、クライアントから無線データを収集し、読解可能なファイルとして出力するために使用できる、詳しい無線トラブルシューティング種別を提供します。この機能は SonicWave アクセスポイントでサポートされています。

- ① **補足:** スキャン無線のアンテナは 1 x 1 なので、一部のデータフレームはハードウェアの制約によりスキャン無線でキャプチャできません。

「パケットキャプチャ」ページには、SonicWave の状況、キャプチャされたパケットの数、パケットバッファのサイズが表示されます。右側で SonicWave にマウスカーソルを重ね、各 SonicWave のキャプチャ設定を構成します。



構成ダイアログでモード、帯域、およびチャンネルを構成し、特定のチャンネルの無線パケットをキャプチャすることができます。最大で 5 つまで送信元および送信先 MAC アドレスを構成できます。構成したい SonicWave の編集アイコンをクリックします。



構成した SonicWave 無線のいずれかのデータをキャプチャするには、「パケットキャプチャ」ページで当該行の「ダウンロード」をクリックします。キャプチャファイルには、“wirelessCapture_[SW名].cap” という形式で名前が付きます。ここで、SW名は、SonicWave の名前です。ファイルの読み取りには Wireshark™ を使用できます。

仮想アクセスポイント

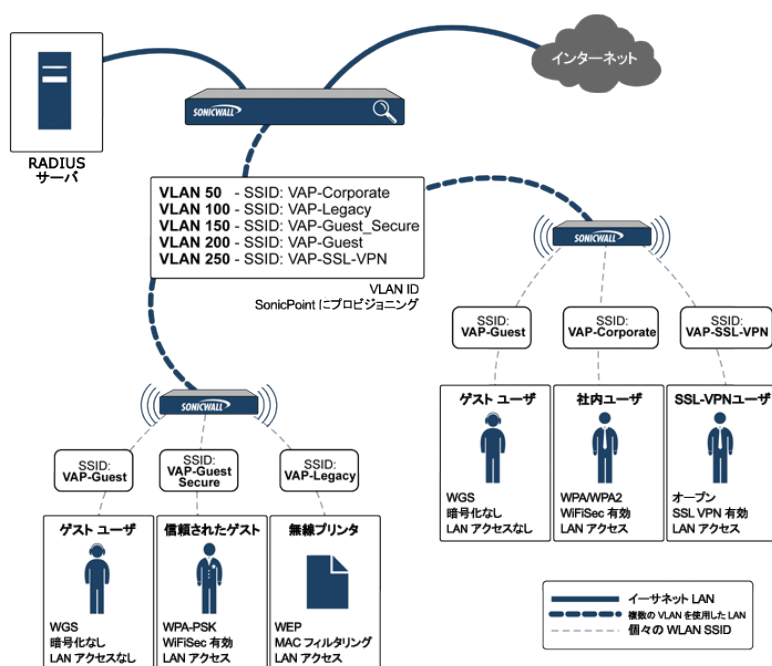
- ① **補足:** 仮想アクセスポイントは、SonicWall NSA 装置と共に無線アクセスポイントを使う場合にサポートされません。

仮想アクセスポイント (VAP) とは、単一の物理アクセスポイントを多重インスタンス化したものです。それ自身を複数の別個なアクセスポイントとして見せます。無線 LAN クライアントからは各仮想 AP が個別の物理 AP のように見えますが、実際には 1 つの物理 AP しか存在しません。VAP では、単一の物理インターフェース上で複数の個別設定をセットアップすることにより、無線ユーザアクセスとセキュリティの設定を制御できます。これらの個別構成は、それぞれ別々の (仮想) アクセスポイントとして機能し、またグループ化して、単一の内部無線通信機に適用することができます。

SonicWall VAP 機能を使用すると、一意の基本サービスセット識別子 (BSSID) とサービスセット識別子 (SSID) が含まれるメディアアクセスコントロール (MAC) プロトコルレイヤの標準である IEEE 802.11 規格に準拠しています。そのため、単一の物理アクセスポイントデバイスの単一の無線周波数フットプリント内で無線ネットワークサービスをセグメント化できます。

VAP では、単一の物理インターフェース上で複数の個別設定をセットアップすることにより、無線ユーザアクセスとセキュリティの設定を制御できます。これらの個別設定は、それぞれ別々の (仮想) アクセスポイントとして機能し、またグループ化して、同時に単一または複数の物理アクセスポイントに適用することができます。

仮想アクセスポイントの設定



VAP には次の利点があります。

- VAP ごとに個別のセキュリティ サービス設定 (GAV、IPS、CFS など) を持たせることができます。
- ゾーンレベルで構成したアクセスルールを使って、各 VAP からのトラフィックを容易に制御できます。
- それぞれに別々のゲスト サービスまたはライトウェイト ホットスポット メッセージング (LHM) 設定を適用することができ、アクセスポイントの共通セットで複数のゲスト サービスプロバイダの表示を容易にすることができます。
- 帯域幅管理やその他のアクセスルール ベース制御を容易に適用することができます。

トピック:

- [VAP を設定する前に](#)
- [アクセスポイント VAP 設定タスクリスト](#)
- [仮想アクセスポイント プロファイル](#)
- [仮想アクセスポイント](#)
- [仮想アクセスポイントグループ](#)

VAP を設定する前に

仮想アクセスポイントを設定する前に、オプションにどのようなものがあり、何ができるのかを理解する必要があります。

トピック:

- [VAP のニーズを確定する](#)
- [セキュリティ設定を確定する](#)
- [サンプル ネットワーク定義](#)
- [前提条件](#)
- [VAP 設定ワークシート](#)

VAP のニーズを確定する

VAP の構成方法を決定するときは、まず以下のような通信ニーズについて検討してください。

- 何種類の無線ユーザをサポートする必要があるか。
- それらの種類の無線ユーザをどのように保護するか。
- 選択したセキュリティ設定をサポートするために必要なハードウェアとドライバを無線クライアントが持っているか。
- 無線ユーザはどんなネットワークリソースと通信する必要があるか。
- それらの無線ユーザの中に他の無線ユーザと通信する必要のあるユーザはいるか。
- それらの種類の無線ユーザの各々にどんなセキュリティサービスを適用したいか。

セキュリティ設定を確定する

セキュリティの必要条件を理解したら、次にゾーン（およびインターフェース）と、ユーザに対して最も効果的に無線サービスを提供できる VAP を定義します。以下は、特定の種類のユーザを定義する方法の例です。

- **社内無線** - 信頼度の高い無線ゾーン。WPA2-AUTO-EAP セキュリティを使用します。WiFiSec (WPA) を実行します。
- **WEP & PSK** - 信頼度が中程度の無線ゾーン。これは 2 組の仮想 AP およびサブインターフェースで構成されます。1 つは旧式の WEP デバイス(無線プリンタ、旧式のハンドヘルド デバイスなど) 用で、もう 1 つは WPA-PSK セキュリティを使用する来訪クライアント用です。
- **ゲスト サービス** - 内部ゲスト サービス ユーザ データベースを使用します。
- **LHM** - 外部 LHM 認証バックエンド サーバを使用するように構成したライトウェイト ホットスポット メッセージング対応ゾーン。

サンプル ネットワーク定義

以下のリストは、確実に適切なアクセスができるようにする前に、どのように仮想アクセス ポイントを構成するかの可能性のある方法の一例を示します。

- **VAP#1、社内無線ユーザ** – 普通はオフィスにいるユーザの集まりで、接続が認証されて安全であれば、すべてのネットワークリソースへの完全なアクセスが許されるべき人たちです。これらのユーザはすでにネットワークのディレクトリ サービスである Microsoft Active Directory に属しています。これはインターネット認証 サービス (IAS) を通じて EAP インターフェースを提供します。
- **VAP#2、旧式の無線デバイス** – WEP 暗号化にしか対応していない旧式の無線デバイスの集まり (プリンタ、PDA、ハンドヘルド デバイスなど)。
- **VAP#3、来訪パートナー** – オフィスを頻繁に訪れ、一部の信頼されたネットワークリソースおよびインターネットにアクセスする必要のあるビジネス パートナー、クライアント、および関連会社の人たち。これらのユーザは会社のディレクトリ サービスに属していません。
- **VAP#4、ゲストユーザ** – インターネットなどの信頼されていないネットワークリソースへのアクセスのみを許したい来訪クライアントです。一部のゲスト ユーザには、一時的で簡単なユーザ名とパスワードが与えられます。
- **VAP#5、頻繁なゲスト ユーザ** – ゲスト ユーザと同じですが、バックエンド データベースを通じて一時的でないゲストアカウントが与えられます。

前提条件

仮想アクセス ポイントを設定する前に、以下に注意してください。

- 各 SonicWall アクセス ポイントが、仮想アクセス ポイントに対して明示的に有効にする必要があります。確認するには、「デバイス > アクセス ポイント > 設定」ページに移動します。「SonicPoint/SonicWave プロビジョニング プロファイル > 一般設定: 有効」オプションの編集アイコンをクリックし、VAP を有効にします。
- アクセス ポイントのプロビジョニングが行われるようにするには、アクセス ポイントを SonicWall ネットワークセキュリティ装置上の WLAN ゾーンにリンクする必要があります。
- VAP と共に VLAN を使用するときは、物理アクセス ポイントの検出パケットと配布パケットにタグ付けされないようにする必要があります (ファイアウォール上の VLAN サブインターフェースにネイティブに終端されている場合を除く)。
- また、アクセス ポイントによって VLAN タグが付けられた VAP パケットが、ネットワーク上の中間デバイス (VLAN 対応スイッチなど) によって変更されずに (カプセル化されず、二重カプセル化もされずに) 配信されるようにする必要があります。
- アクセス ポイントの最大数制限は、SonicWall セキュリティ装置に応じて異なります。

VAP 設定ワークシート

下の表は、VAP 設定に関する一般的な検討事項とソリューションを示しており、実際の設定内容を記入するための空欄もあります。

VAP 設定ワークシート

質問	例	ソリューション
どれだけの種類の無線	社内無線、ゲスト アクセス、来訪パー	異なる VAP の必要数を把握します。必

ユーザをサポートする必要はあるか。	トナー、無線デバイスは、すべて一般的なユーザタイプで、それぞれ固有の VAP を必要とする。	要な各 VAP についてゾーンと VLAN を構成します。
	実際の設定内容:	
各 VAP で何人のユーザをサポートする必要があるか。	会社の構内に 100 人の従業員がいて、全員が無線機能を使用する。	少なくとも 100 個のアドレスを提供するように訪問者ゾーンの DHCP スコープを設定します。
	会社の構内に無線機能を使用できる 20~30 人の訪問者がよく来訪する。	少なくとも 25 個のアドレスを提供するように訪問者ゾーンの DHCP スコープを設定します。
	実際の設定内容:	
異なる種類の無線ユーザをどのように保護するか。	社内 LAN リソースにアクセスできる社内ユーザ。	WPA2-EAP を構成します。
	インターネット アクセスのみに限定されたゲストユーザ。	ゲスト サービスを有効にしますが、セキュリティ設定は構成しません。
	社内 LAN 上の旧式の無線プリンタ。	WEP を構成し、MAC アドレスフィルタを有効にします。
	実際の設定内容:	
ユーザはどんなネットワークリソースと通信する必要がありますか。	社内 LAN とすべての内部 LAN リソース (他の WLAN ユーザも含む) へのアクセスを必要とする社内ユーザ。	社内ゾーンでインターフェース間通信を有効にします。
	インターネット アクセスを必要とするが、他の WLAN ユーザとの通信は許可すべきでない無線ゲスト。	ゲストゾーンでインターフェース間通信を無効にします。
	実際の設定内容:	
ユーザにどんなセキュリティサービスを適用したいか。	完全な SonicWall セキュリティスイートで保護すべき社内ユーザ。	SonicWall のすべてのセキュリティサービスを有効にします。
	社内 LAN 上にいないので、配慮する必要のないゲストユーザ。	SonicWall のすべてのセキュリティサービスを無効にします。
	実際の設定内容:	

アクセスポイント VAP 設定タスクリスト

アクセスポイント VAP を展開するには、いくつかの構成手順を実行する必要があります。このセクションでは、関連するステップの概要を説明します。

1. **ネットワークゾーン** - ゾーンは VAP 設定の重要部分です。作成した各ゾーンは、それぞれに個別のセキュリティ設定とアクセス制御設定を持つこととなります。複数のゾーンを作成し、VLAN サブインターフェースを通じて単一の物理インターフェースに適用することができます。ネットワークゾーンに関する詳細は、『SonicOS システム セットアップ』の「オブジェクト > 一致オブジェクト > ゾーン」に関するセクションを参照してください。
2. **インターフェース (または VLAN サブインターフェース)** - インターフェース (X2、X3 など) は SonicWall ネットワークセキュリティ装置と物理アクセスポイントの間の物理接続を表します。個々のゾーン設定はこれらのインターフェースに適用され、それからアクセスポイントに転送されます。無線インターフェースの詳細については、『SonicOS システム セットアップ』の「ネットワーク > システム > インターフェース」に関するセクションを参照してください。

3. **DHCP サーバ** – DHCP サーバはリースされる IP アドレスを指定された範囲（「スコープ」と呼ばれる）内のユーザに割り当てます。DHCP スコープの既定の範囲は、たいていの SonicPoint 配備のニーズにとって過大なものです（たとえば、30 個のアドレスしか使用しないインターフェースに対して 200 個のアドレスというスコープ）。そのため、利用可能なリース スコープを使い果たさないように、DHCP 範囲は気をつけて設定する必要があります。DHCP サーバ設定の詳細については、『SonicOS システム セットアップ』の「ネットワーク > システム > DHCP サーバ」に関するセクションを参照してください。
4. **仮想アクセス ポイント プロファイル** – 仮想アクセス ポイント プロファイル 機能では、必要に応じて新しい無線仮想アクセス ポイントに簡単に適用できる無線設定プロファイルを作成できます。詳細については、「[仮想アクセス ポイント プロファイル](#)」を参照してください。
5. **仮想アクセス ポイント オブジェクト** – 仮想アクセス ポイント オブジェクト 機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および VLAN ID が構成されます。詳細については、「[仮想アクセス ポイント](#)」を参照してください。
6. **仮想アクセス ポイント グループ** – 仮想アクセス ポイント グループ 機能では、単一のアクセス ポイントに同時に適用する複数の仮想アクセス ポイント オブジェクトをグループ化することができます。
7. **仮想アクセス ポイント グループをアクセス ポイント プロファイル無線に割り当てる** – プロビジョニング プロファイルでは、新しいアクセス ポイントのプロビジョニング時に VAP グループを適用できます。
8. **WEP 鍵を割り当てる (WEP 暗号化のみ)** – WEP 鍵の割り当てでは、新しいアクセス ポイントのプロビジョニング時に WEP 暗号化鍵を適用できます。WEP 鍵はアクセス ポイントごとに構成されます。つまりアクセス ポイントに割り当てられた WEP 対応の仮想アクセス ポイントは、すべて同じセットの WEP 鍵を使用しなければなりません。4 つまでの鍵を定義できます。WEP 対応の VAP は、この 4 つの鍵を独立に使用できます。WEP 鍵の構成は、「[デバイス > アクセス ポイント > 設定](#)」ページで個々の物理的アクセス ポイントまたはアクセス ポイント プロファイルに対して行います。

仮想アクセス ポイント プロファイル

仮想アクセス ポイント プロファイルを使用すると、アクセス ポイント設定をあらかじめ構成して、プロファイルに保存することができます。仮想アクセス ポイント プロファイルにより、新しい仮想アクセス ポイントに簡単に設定を適用することができます。仮想アクセス ポイント プロファイルの構成は「[デバイス > アクセス ポイント > 仮想アクセス ポイント](#)」ページの「[仮想アクセス ポイント プロファイル](#)」セクションで行います。

仮想アクセス ポイント グループ					
仮想アクセス ポイント オブジェクト					
仮想アクセス ポイント プロファイル					
検索					
+ 追加 削除 再表示					
名前	種類	状態	種類	最大クライアント数	
1	openprof	SonicPoint/SonicWave	オープン	なし	16

既存の VAP プロファイルを構成するには、そのプロファイルに対する**編集**アイコンを選択します。新しい VAP プロファイルを追加するには、**追加**アイコンをクリックします。

① | **補足:** 表示されるオプションは、他のオプションの選択内容によって変わります。

トピック:

- [仮想アクセス ポイント スケジュールの設定](#)
- [仮想アクセス ポイント プロファイル設定](#)
- [ACL 強制](#)
- [リモート MAC アドレスアクセス制御の設定](#)

仮想アクセス ポイント スケジュールの設定

個々の仮想アクセス ポイントは固有のスケジュールを持つことができます。拡張により、個々のプロファイルも専用に定義されたスケジュール設定を持つことができます。

スケジュールを仮想アクセス ポイント プロファイルに関連付けるには、以下の手順に従います。

1. 「デバイス > アクセス ポイント > 仮想アクセス ポイント」に移動します。
2. 新しいプロファイルを作成するには「追加」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して編集アイコンをクリックします。
3. 「VAP スケジュール名」フィールドで、スケジュールをドロップダウン メニューから選択します。

仮想アクセス ポイント プロファイル設定

仮想アクセス ポイント プロファイルを設定するには、以下の手順に従います

1. 「デバイス > アクセス ポイント > 仮想アクセス ポイント」に移動します。
2. 新しいプロファイルを作成するには「追加」を選択し、既存のプロファイルを編集するには仮想アクセス ポイント プロファイルを選択して編集アイコンをクリックします。
3. 「無線種別」を設定します。アクセス ポイントを仮想アクセス ポイントとして使用する場合、既定で「SonicPoint/SonicWave」に設定されます（現在のところサポートされる唯一の無線種別です）。
4. 「プロファイル名」フィールドに、この仮想アクセス ポイント プロファイルのわかりやすい名前を入力します。後でこのプロファイルを新しい VAP に適用するときにわかりやすく、覚えやすい名前にするとういでしょう。

5. 「認証種別」をドロップダウンメニューから選択します。以下のオプションから選択します。

認証種別	定義
オープン	認証方法を特定しない。安全でないアクセスです。
共有	共有鍵が認証に使用され、基本的なセキュリティが確保されます。
両方	保護されない共有アクセス。
WPA2-PSK	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。認証に事前共有鍵を使います。
WPA2-EAP	信頼性の高い企業の無線クライアントで使用される、最良のセキュリティです。Windows ログインを使用したトランスペアレントな認証。Fast Roaming 機能をサポートします。拡張認証プロトコル (EAP) を使用します。
WPA2-AUTO-PSK	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。認証には事前共有鍵を使用します。
WPA2-AUTO-EAP	WPA2 セキュリティを使用して接続を試行します。クライアントが WPA2 に対応していない場合、接続は既定で WPA に設定されます。拡張認証プロトコル (EAP) を使用します。

選択された認証種別に基づいて、「ユニキャスト暗号」フィールドが表示されます。

① | **補足:** ページに表示される設定は、選択したオプションに応じて異なります。

選択された「認証種別」に応じて、仮想 アクセス ポイント プロファイルの追加/編集ページには、追加のオプションのセクションが表示されます。

選択した内容によって次の手順が異なります。

- **オープン:** RADIUS 設定に関する「[RADIUS サーバと RADIUS アカウント](#)」を参照してください。
- **両方または共有:** 設定に関する詳細は、「[WEP 暗号化の設定](#)」を参照してください。
- **事前共有鍵 (PSK) を必要とするオプション:** 設定に関する詳細は、「[WPA-PSK > WPA2-PSK 暗号化の設定](#)」を参照してください。
- **拡張認証プロトコル (EAP) を必要とするオプション:** 設定に関する詳細は、「[RADIUS サーバと RADIUS アカウント](#)」を参照してください。

RADIUS サーバと RADIUS アカウント

「認証種別」ドロップダウンで選択したすべてのオプションに対して、RADIUS サーバを設定することができます。この設定が定義されると、鍵の生成および認証に外部の 802.1x/EAP 対応 RADIUS サーバを利用します。以下のフィールドに値を入力します。

RADIUS サーバの設定を行うには、以下の手順に従います。

フィールド名	説明
RADIUS サーバ再試行回数	アクセスを拒否するまでにユーザが認証を試行できる回数を入力します。既定値は 4 です。
再試行間隔 (秒)	再試行が有効な期間を入力します。既定値は 0 です。

RADIUS サーバ 1	RADIUS 認証サーバの名前/場所を入力します。
ポート	プライマリ RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信するポートを入力します。
RADIUS サーバ 1 パスワード	プライマリ RADIUS サーバ用のシークレット パスコードを入力します。
RADIUS サーバ 2	バックアップ RADIUS 認証サーバの名前/場所を入力します。
ポート	バックアップ RADIUS 認証サーバがクライアントおよびネットワーク デバイスと通信するポートを入力します。
RADIUS サーバ 2 パスワード	バックアップ RADIUS 認証サーバ用のシークレット パスコードを入力します。

RADIUS アカウント サーバの設定を行うには、以下の手順に従います。

フィールド名	説明
サーバ 1 IP	プライマリ RADIUS サーバの IP アドレスを入力します。
ポート	プライマリ RADIUS アカウント サーバがクライアントおよびネットワーク デバイスと通信するポートを入力します。
サーバ 1 パスワード	プライマリ RADIUS アカウント サーバ用のシークレット パスコードを入力します。
サーバ 2 IP	バックアップ RADIUS サーバの IP アドレスを入力します。
ポート	バックアップ RADIUS アカウント サーバがクライアントおよびネットワーク デバイスと通信するポートを入力します。
サーバ 2 パスワード	バックアップ RADIUS アカウント サーバ用のシークレット パスコードを入力します。
NAS 識別子の種別	<p>ドロップダウン メニューから NAS 識別子種別を選択します。以下のオプションがあります。含まない (既定)、アクセス ポイント名、アクセス ポイント MAC アドレス、SSID。</p> <p>「SSID」オプションが選択されている場合、RADIUS 認証メッセージと RADIUS アカウントメッセージの両方で VAP SSID が伝送されます。</p>
NAS IP アドレス	NAS システムの IP アドレスを入力します。
グループ鍵交換間隔	グループ鍵の有効時間を秒単位で入力します。この時間が経過すると、グループ鍵が強制的に更新されます。既定値は 86400 秒です。(24 時間)

WPA-PSK > WPA2-PSK 暗号化の設定

「**認証種別**」ドロップダウンで事前共有鍵が必要なオプション（「**WPA2-PSK**」または「**WPA2-AUTO-PSK**」）を選択した場合、「**WPA/WPA2-PSK 暗号化設定**」と呼ばれるセクションが表示されます。これらの設定が定義されると、事前共有鍵が認証に使用されます。

暗号化を設定するには、以下の手順に従います：

1. 「**パスフレーズ**」フィールドにパスワードを入力します。
2. リモート MAC アクセス制御を有効にしている場合は、「**RADIUS サーバと RADIUS アカウント**」に移動して、RADIUS 設定をセットアップしてください。

WEP 暗号化の設定

前の手順の「**認証種別**」ドロップダウンメニューで「**両方**」または「**共有**」を選択した場合、「**WEP 暗号化の設定**」と呼ばれるセクションが表示されます。WEP 設定は、物理アクセス ポイントを共有する仮想アクセス ポイント間で共有されます。

暗号化を設定するには、以下の手順に従います：

1. 「**暗号化鍵**」フィールドで、「**第 1 鍵**」、「**第 2 鍵**」、「**第 3 鍵**」、または「**第 4 鍵**」をドロップダウンメニューから選択します。
2. リモート MAC アクセス制御を有効にしている場合は、「**RADIUS サーバと RADIUS アカウント**」に移動して、RADIUS 設定をセットアップしてください。

ACL 強制

各仮想アクセス ポイントは、個別のアクセス制御リスト (ACL) をサポートして、より効率的な認証制御を提供できます。この無線 ACL 機能は、現在 SonicOS で利用可能な無線 MAC フィルタリストと同時に動作します。この ACL 強制機能を使って、ユーザは MAC フィルタリストを有効/無効にする、許可リストを設定する、そして拒否リストを設定することが可能です。

各 VAP は個別の MAC フィルタリスト設定を持つ、またはグローバル設定を使うことが可能です。グローバル設定が有効な場合は、SonicWave、SonicPoint-N/ SonicPointNDR/ SonicPoint Ni/Ne、SonicPoint または SonicPoint-N 装置は、既定でこれらの設定を使います。仮想アクセス ポイント (VAP) モードでは、このグループの各 VAP が同一 MAC フィルタリスト設定を共有します。

ACL 強制の設定

オプション	説明
MAC フィルタリストを有効にする	特定のデバイスからのトラフィックを許可または禁止することによって、アクセス制御を行います。既定では、このオプションは選択されておらず、このセクションのすべてのオプションがグレー表示で利用できない状態になっています。
グローバル ACL 設定を使用する	グローバル ACL 設定を使用します。

	<p>① 補足: 仮想アクセスポイントごとの ACL サポートは、SonicPointN によってのみサポートされています。1 つの仮想アクセスポイントが SonicPoint/SonicWave によって使用されている場合、グローバル ACL 設定が既定で適用されます。</p>
許可リスト	<p>MAC アドレスグループを選択すると、そのグループ内の MAC アドレスを持つすべてのデバイスからのトラフィックが自動的に許可されます。</p> <ul style="list-style-type: none"> 新しい MAC アドレスオブジェクトグループの作成 すべての MAC アドレス <p>① 補足: 「許可リスト」には「すべての MAC アドレス」を設定することを推奨します。</p> <ul style="list-style-type: none"> 既定の SonicPoint/SonicWave ACL 許可グループ ユーザ定義の MAC アドレスオブジェクトグループ
拒否リスト	<p>ドロップダウンメニューから MAC アドレスグループを選択すると、そのグループ内の MAC アドレスを持つすべてのデバイスからのトラフィックが自動的に拒否されます。</p> <p>① 補足: 拒否リストが適用された後で、許可リストが適用されます。</p> <ul style="list-style-type: none"> 新しい MAC アドレスオブジェクトグループの作成 MAC アドレスなし 既定の SonicPoint/SonicWave ACL 拒否グループ <p>① 補足: 「拒否リスト」には「既定の SonicPoint/SonicWave ACL 拒否グループ」を設定することを推奨します。</p> <ul style="list-style-type: none"> ユーザ定義の MAC アドレスオブジェクトグループ

リモート MAC アドレスアクセス制御の設定

- ① **補足:** このセクションは、「認証種別」として「WPA2-EAP/WPA2-AUTO-EAP」が選択されている場合は表示されません。

オプション	説明
リモート MAC アドレスアクセス制御を有効にする	リモート RADIUS サーバで MAC ベースの認証ポリシーに基づく無線アクセス制御を強制するには、このオプションを選択します。既定では、このオプションはオフになっています。

- ① **補足:**「認証種別」として「WPA2-EAP/WPA2-AUTO-EAP」以外を選択した場合は、「リモート MAC アクセス制御を有効にする」を選択すると、「RADIUS サーバの設定」セクションが表示されます。

仮想アクセスポイント

VAP 設定機能では、一般 VAP 設定をセットアップできます。VAP 設定により、SSID および VLAN ID が構成されます。仮想アクセスポイントの構成は「デバイス>アクセスポイント>仮想アクセスポイント」ページで行います。

仮想アクセスポイントグループ		仮想アクセスポイントオブジェクト		仮想アクセスポイントプロファイル					
名前	SSID	VLAN ID	認証	モード	最大クライアント数	SSID 隠蔽	有効	動作中	
1	vapobject1	1888	0	オープン	なし	16	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

既存の VAP を構成するには、その VAP に対する「編集」アイコンを選択します。新しい VAP を追加するには、「追加」をクリックします。

トピック:

- 「一般」タブ
- 「詳細」タブ

「一般」タブ

仮想アクセスポイントの編集: vapobject1

一般 詳細

仮想アクセスポイント一般設定

名前: vapobject1

SSID: 1888

VLAN ID: VLAN ID なし

仮想アクセスポイントを有効にする:

SSID 隠蔽を有効にする: ①

キャンセル 適用

「一般」タブで以下の機能を設定します。

仮想アクセスポイントの一般設定

機能	説明
名前	VAP のニックネームを作成します。
SSID	この VAP を使用するアクセスポイントの SSID 名を入力します。この名前は、利用可能なアクセスポイントを検索するときに、無線クライアントのリストに表示されます。
VLAN ID	VLAN をサポートしているプラットフォームを使用するときは、この VAP に関連付ける VLAN ID をオプションで選択できます。選択した VLAN から、この VAP のための設定が引き継がれます。
仮想アクセスポイントを有効にする	この VAP を有効にします。このオプションは、既定では選択されています。

SSID 抑制を有効にする

SSID 名のブロードキャストを抑止し、プローブ要求への応答を無効にします。このオプションをオンにすると、不正な無線クライアントから SSID を確認できなくなります。このオプションは、既定では選択されていません。

動的 VLAN ID 割り当てを有効にする

このオプションをオンにすると有効になります。動的 VLAN を有効にできるのは、認証種別が EAP の場合のみです。

「詳細」タブ

The screenshot shows the configuration page for a VAP object named 'vapobject1'. It is divided into several sections:

- 仮想アクセスポイントスケジューラ設定:** VAP スケジュール名: 常に有効
- 仮想アクセスポイントプロファイル設定:** 無線種別: SonicPoint/SonicWave, プロファイル名: プロファイルなし, 認証種別: オープン, ユニキャスト暗号: なし, 最大クライアント数: 16, VAP WDS を有効にする:
- リモート MAC アドレスアクセス制御設定:** リモート MAC アクセス制御を有効にする:
- ACL 制御:** MAC フィルタ リストを有効にする: , グローバル ACL 設定を使用する:

Buttons at the bottom: キャンセル, 適用

詳細設定では、特定の仮想アクセスポイントに対して、認証と暗号化の設定が構成できます。ユーザが作成したプロファイルからこれらの設定を引き継ぐには、**プロファイル名**を選択します。「**仮想アクセスポイントを追加または編集する**」ウィンドウの「**詳細**」タブは、「**仮想アクセスポイントプロファイルを追加または編集する**」ウィンドウと同じなので、認証と暗号化の設定の詳細については、「**仮想アクセスポイントプロファイル**」を参照してください。

仮想アクセスポイントグループ

仮想アクセスポイントグループ機能は、SonicWall NSA 装置で利用できます。この機能ではアクセスポイントに同時に適用する複数の VAP オブジェクトをグループ化することができます。仮想アクセスポイントグループの構成は「**デバイス > アクセスポイント > 仮想アクセスポイント**」ページで行います。

#	名前	種別	認証	暗号	最大クライアント数
1	openprof	SonicPoint/SonicWave	オープン	なし	16

仮想アクセスポイントグループを追加するには、以下の手順に従います:

1. 「**デバイス > アクセスポイント > 仮想アクセスポイント**」ページに移動します。
2. 新しいプロファイルを作成するには「**追加**」を選択し、既存のプロファイルを編集するには仮想アクセスポイントプロファイルを選択して**編集**アイコンをクリックします。



3. 「仮想 AP グループ名」フィールドに入力します。
4. オブジェクトをグループに追加するには、「使用可能な仮想 AP オブジェクト」リストから追加したいオブジェクトを選択して、右矢印をクリックし、「仮想 AP グループのメンバー」に移動させてください。
5. オブジェクトを選択して左矢印を使用し、オブジェクトをグループから削除します。
6. 「適用」をクリックして設定を保存します。

RF 監視

現在の 802.11 ベースの無線ネットワークデバイスで使用されている無線周波数 (RF) 技術は、侵入者の格好のターゲットになっています。管理下に置かずに放置すると、無線 (および有線) ネットワークは RF デバイスが原因で、サービス妨害 (DoS) からネットワークセキュリティ侵害まで、外部のさまざまな脅威にさらされる可能性があります。SonicWall 無線アクセスポイントの安全性確保を支援するため、SonicWall は、無線ネットワークや有線ネットワークの現在の操作を中断することなく脅威の検出を支援します。

SonicOS RF 監視には、SonicPoint の無線周波数トラフィックのリアルタイムの脅威監視および管理機能が用意されています。リアルタイムの脅威管理機能の他に、SonicOS RF 監視では、システムを利用して RF 脅威およびトラフィック統計を中央で一括収集して、SonicWall セキュリティ装置のゲートウェイから直接、RF 機能を簡単に管理することができます。

「デバイス > アクセスポイント > RF 監視」ページでは、RF シグネチャタイプの選択、検出された RF 脅威ステーションの表示、検出された脅威ステーションの警戒リストへの追加を、すべて 1 か所で行うことができます。

The screenshot shows the configuration interface for RF monitoring. It includes sections for summary, general frame settings, management frame settings, and data frame settings, each with various controls and status indicators.

トピック:

- [前提条件](#)
- [RF 監視の要約](#)
- [802.11 一般フレーム設定](#)
- [802.11 管理フレーム設定](#)
- [802.11 データフレーム設定](#)
- [検出された RF 脅威ステーション](#)
- [警戒リストへの脅威ステーションの追加](#)
- [RF 監視の活用法](#)

前提条件

RF 監視を適用するには、使用可能なすべての アクセスポイントで RF 監視オプションを有効にする必要があります。最も簡単な方法は、アクセスポイントのプロファイルを更新して、そのプロファイルを該当するアクセスポイントに適用することです。RF 監視機能のオプションを見つけるには、以下の手順に従います：

1. 「デバイス > アクセスポイント > 設定」ページに移動します。
2. 更新したいプロファイルの **編集** アイコンをクリックします（または、新しいプロファイルを作成する場合は、「新しいプロファイルの追加」ドロップダウンメニューから「SonicPoint/SonicWave 種別」を選択します）。
3. 「一般設定」グループの「有効」オプションを選択します。



プロファイルのセットアップの詳細については、『SonicOS 接続』管理マニュアルの「プロビジョニング プロファイルの作成/変更」を参照してください。

RF 監視の要約

「RF 監視の要約」パネルは、RF 監視の対象として構成されたアクセスポイントに関するデータを表示します。

そこには、検出された RF 脅威の数と、**測定間隔**設定が赤色で表示されます。「測定間隔」は、フィールドに新しい数値を入力することでリセットできます。既定値は **300** 秒です。必ず「適用」をクリックして設定を保存してください。



「アクセスポイント」リンクをクリックすると、「デバイス > アクセスポイント > 設定」ページに移動して、プロファイルやオブジェクトの設定を編集できます。

802.11 一般フレーム設定

802.11 一般フレーム設定パネルは、一般脅威の総数と、長期間を有効にするオプションを表示します。



「長期間」オプションを選択し、「適用」をクリックすると、「長期間」が有効になります。RF 帯域を 14 のチャンネルにばらばらに分割することで電波を共有します。各デバイスは、指定された（短い）時間、チャンネルを予約し、いずれか 1 つのデバイスがチャンネルを予約している間、他のデバイスはそのチャンネルをブロードキャストに利用できないと認識します。長期間攻撃は、このプロセスを悪用して、多くの RF チャンネルを非常に長期に亘って確保し、事実上、正当な無線トラフィックが空きブロードキャスト チャンネルを見つけることができないようにするものです。既定では、このオプションはオフになっています。

802.11 管理フレーム設定

「802.11 管理フレーム設定」パネルは、管理フレーム設定を構成します。また、各設定の脅威数を表示します。



いずれかの設定を有効にするには、そのオプションのラジオボタンをオンにします。既定では、すべて有効になっています。「適用」を選択して設定を保存します。これらの設定の説明を下の表にまとめました。

名前	説明
管理脅威の総数	管理脅威の総数を表示します。
管理フレーム フラッド (洪水)	DoS 攻撃のこのバリエーションは、管理フレーム (参加要求や認証要求など) を使って無線アクセスポイントでフラッドを発生させて、偽の要求で管理テーブルを満杯にしようとします。
ヌル プローブ 応答	無線クライアントがプローブ要求を送信すると、攻撃者はヌル SSID を含む応答を送り返します。この応答を受け取ると、一般的な無線カードやデバイスの多くは応答を停止します。
ブロードキャストの非認証	DoS の一種であるこの攻撃は、無線クライアントに大量の偽の認

名前	説明
	証解除フレームを送信することで、これらのクライアントがアクセスポイントで常に認証解除と再認証を繰り返す状態を引き起こします。
不正な SSID を持つ有効なステーション	この攻撃では、Rogue (悪意の侵入者) アクセスポイントが信頼できるステーション ID (ESSID) のブロードキャストを試みます。BSSID が無効であっても、クライアントはそのステーションを信頼できるアクセスポイントと見なす可能性があります。一般に、この攻撃の目的は、信頼できるクライアントから認証情報を取得することにあります。
Wellenreiter 検出	Wellenreiter は、攻撃者が周囲の無線ネットワークから情報を取得する場合によく使われるソフトウェアアプリケーションです。
アドホックステーション検出	アドホックステーションとは、実際のアクセスポイントとユーザとの橋渡しをすることで無線クライアントへのアクセスを提供するノードです。アドホックステーションは実際のアクセスポイントと同じ SSID を持つ場合があるので、無線ユーザはだまされて、実際のアクセスポイントではなくアドホックステーションに接続します。これにより、アドホックステーションは接続クライアントがアクセスポイントとの間で送受信する無線トラフィックをインターセプトすることができます。

802.11 データフレーム設定

「802.11 データフレーム設定」パネルは、データフレーム設定を構成します。また、各設定の脅威数を表示します。



いずれかの設定を有効にするには、そのオプションのラジオボタンをオンにします。「適用」を選択して設定を保存します。既定では、「関連付けのないステーション」オプションのみが有効ではなく、それ以外は有効です。これらの設定の説明を下の表にまとめました。

名前	説明
データ脅威の総数	データ脅威の総数を表示します。

名前	説明
関連付けのないステーション	無線ステーションはアクセスポイントに参加する前に認証を試みるので、未参加のステーションが未参加を続けた状態でアクセスポイントに大量の認証要求を送信することによってDoSが引き起こされる可能性があります。
NetStumbler 検出	一般に、無料のインターネットアクセスと、興味深いネットワークを検出するのに使用されます。NetStumbler は、GPS レシーバおよびマッピングソフトウェアと連動して無線ネットワークの場所を自動的に特定します。NetStumbler も、攻撃者によって周囲の無線ネットワークから情報を取得する目的に使用されます。
EAPOL パケットフラッド	WPA および WPA2 認証メカニズムでは、Extensible Authentication Protocol over LAN (EAPOL) パケットが使用されます。これらのパケットは、ほかの認証要求パケットと同様に、無線アクセスポイントで無制限に受信されるので、これらの大量のパケットが原因で無線ネットワークへの DoS が引き起こされる可能性があります。
脆弱な WEP IV	WEP セキュリティメカニズムは、WEP キーと、Initialization Vector (IV) というランダムに選択された 24 ビットの数値を使って、データを暗号化します。ランダムな IV 数が弱いと WEP キーの復号化が簡単になるので、この種の暗号化はネットワーク攻撃者のターゲットになります。

検出された RF 脅威ステーション

「検出されたRF脅威ステーション」タブには、検出されたRF脅威ステーションの情報が表示されます。脅威ステーションについては、検出されたすべてのステーションを表示するか、警戒リストグループに含まれるステーションだけを表示できます。これは「**表示形式: ステーション**」ドロップダウンメニューの内容に基づき選択できます。

以下の表は、「脅威ステーション」テーブルに表示されるデータの説明です。

名前	説明
項目	ログに記録された脅威の総数を表示します。矢印ボタンでページを移動することができます。
表示形式: ステーション	一覧に表示するステーションの種別を選択します。 <ul style="list-style-type: none"> 検出されたすべてのステーション ウォッチリストグループに含まれるステーションのみ
#	エントリの参照番号。
MACアドレス	項目を MAC アドレスによって並べ替えます。これは RF 脅威ステーションの物理アドレスです。
種別	項目を脅威ステーションから受信した無線信号のタイプによって並べ替えます。
ベンダー	項目をベンダー別に並べ替えます。これは脅威ステーションの製造元 (MAC アドレスによって判別) です。

名前	説明
RSSI	項目を SonicWave が報告した受信信号の強度によって並べ替えます。この項目は、「センサー」項目と共に、RF 脅威デバイスの実際の物理的な場所を三角測量する場合に役立ちます。
速度	項目を脅威ステーションの転送速度 (Mbps) によって並べ替えます。
暗号化	項目を脅威ステーションでの無線信号の暗号化 (「なし」または「暗号化」) によって並べ替えます。
RF脅威	項目を最新の RF 脅威によって並べ替えます。
更新時刻	項目をこのログレコードが作成/更新された時刻によって並べ替えます。
センサー	項目をこの脅威を記録した SonicWave の ID によって並べ替えます。この項目は、「RSSI」項目と共に、RF 脅威デバイスの実際の物理的な場所を三角測量する場合に役立ちます。
コメント	脅威に関するコメントを追加するためのテキストボックスを表示します。
構成	検出されたステーションの警戒リストを構成します。

- ① **ヒント:** ログ採取した脅威統計を使って、RF 脅威デバイスのおおよその場所を見つけることができます。RF 管理の脅威統計の使用法に関する実践的なヒントおよび情報については、「[RF 監視の活用法](#)」を参照してください。

警戒リストへの脅威ステーションの追加

RF 監視の検出された脅威ステーションの「警戒リスト」機能では、無線ネットワークに対する脅威の警戒リストを作成することができます。警戒リストは、「[検出された RF 脅威ステーション](#)」リストの結果にフィルタを適用するために使用されます。

警戒リストにステーションを追加するには、以下の手順に従います

1. 「デバイス > アクセスポイント > RF 監視」ページに移動し、「[検出された RF 脅威ステーション](#)」タブを選択します。
2. 警戒リストに追加したい脅威ステーションに対応する編集アイコンをクリックします。確認ダイアログが表示されます。
3. 「OK」を選択して警戒リストにステーションを追加します。
4. 警戒リストに間違っただけのステーションを追加してしまった場合や、リストから削除したいステーションがある場合は、削除したい脅威ステーションに対応する削除アイコンを選択します。

① **ヒント:** 1 つ以上の脅威ステーションを警戒リストに追加した後、「[ウォッチリストグループに含まれるステーションのみ](#)」を「表示形式」ドロップダウンメニューから選択して、リアルタイム ログにこれらのステーションだけが表示されるように結果を絞り込むことができます。
5. 「適用」を選択します。

RF 監視の活用法

このセクションでは、WiFiの脅威発生源を検出するために収集したRF監視データの活用法について説明します。RFデータを使って脅威を検出する場合、無線信号は多くの要因の影響を受けることに注意してください。

- 信号強度は距離の適切な指標になるとは限りません。
壁、無線の干渉、デバイスの出力、さらに周囲の湿度や温度などでさえ、障害として無線デバイスの信号強度に影響を与えることがあります。
- MACアドレスは、必ずしも恒久的とは限りません。
一般に、MACアドレスはデバイス種別や製造元の適切な指標になるものの、このアドレスは変更が可能であり、なりすましに悪用されることもあります。また、RF 脅威の発行者が、複数のハードウェア デバイスを自在に操っている可能性もあります。

トピック:

- センサー ID の使用による RF 脅威の場所の判別
- RSSI の使用による RF 脅威の近接性の判別

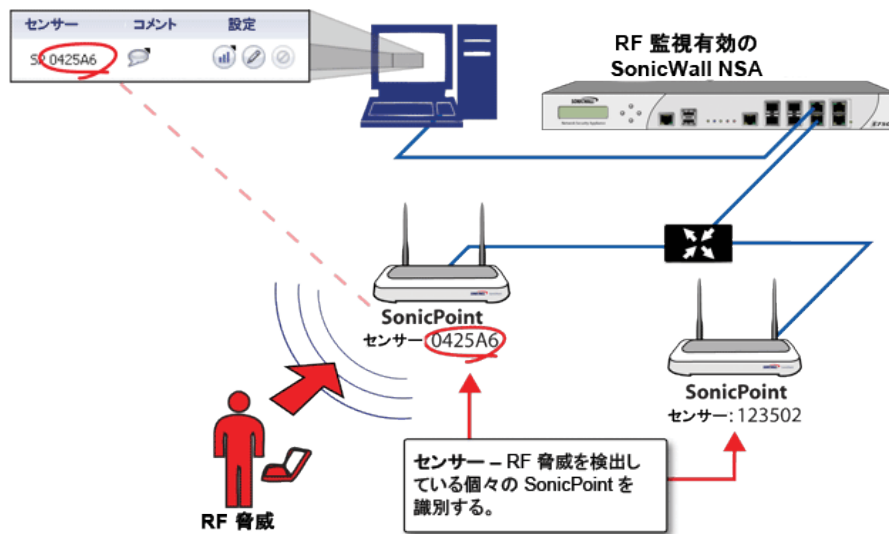
センサー ID の使用による RF 脅威の場所の判別

「検出された RF 脅威ステーション」テーブルの「センサー」フィールドは、どのアクセスポイントが特定の脅威を検出しているかを示します。アクセスポイントのセンサー ID と MAC アドレスを使って、脅威を検出しているアクセスポイントの場所を簡単に判別することができます。

① **ヒント:** アクセスポイントの場所と MAC アドレスをきちんと記録しておくことは一般的に良い習慣ですが、このセクションの作業には特に役立ちます。

1. 「デバイス > アクセスポイント > RF 監視」ページに移動します。
2. 「検出された RF 脅威ステーション」テーブルで、ターゲットの RF 脅威を検出している SonicPoint/SonicWave の「センサー」を探して、その番号を記録します。
3. 「デバイス > アクセスポイント > 設定」ページに移動します。
4. 「SonicPoint/SonicWave オブジェクト」テーブルで、ステップ 2 で記録したセンサー番号と一致するアクセスポイントを探します。
5. そのアクセスポイントの **MAC アドレス**を記録します。
6. この MAC アドレスを使用して、アクセスポイントの物理的な位置を探します。
RF 脅威は、このアクセスポイントのサービス対象範囲内にあると考えられます。

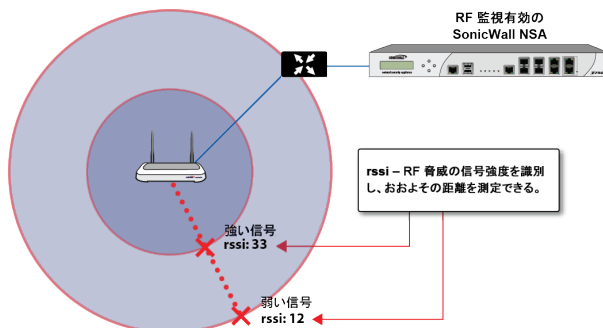
センサーIDの使用によるRF脅威の場所の判別



RSSIの使用によるRF脅威の近接性の判別

このセクションは、「センサーIDの使用によるRF脅威の場所の判別」で説明した内容に基づいています。「検出されたRF脅威ステーション」テーブルの「RSSI」フィールドは、RF脅威を検出している特定のアクセスポイントの位置での信号強度を示します。

RSSIの使用によるRF脅威の近接性の判別



「RSSI」フィールドを利用することで、RF脅威とその脅威を検出しているアクセスポイントとの近接性を簡単に判別することができます。一般に、RSSIの数値が高いほど、脅威はアクセスポイントに近接していることを意味します。

① **重要:** 壁が無線信号の障壁となることを忘れてはなりません。非常に弱いRSSI信号は、RF脅威が非常に遠く離れた場所にあることを意味する場合もあるものの、距離は近いが部屋や建物の外部の場所に脅威があることを示している可能性もあります。

1. 「デバイス>アクセスポイント>RF監視」ページに移動します。
2. 「検出されたRF脅威ステーション」テーブルで、ターゲットのRF脅威を検出しているアクセスポイントの「センサー」と「RSSI」を探して、それらの数値を記録します。
3. 「デバイス>アクセスポイント>設定」ページに移動します。

4. 「**SonicPoint/SonicWave オブジェクト**」テーブルで、ステップ2で記録したセンサー番号と一致するアクセスポイントを探します。
5. その SonicPoint/SonicWave の **MAC アドレス**を記録します。
6. この MAC アドレスを使用して、SonicPoint/SonicWave の物理的な位置を探します。
一般に、RSSIが高い場合は、脅威が SonicPoint/SonicWave に近接していることを示します。RSSIが低い場合は、RF 脅威との間に障害があるか、距離が離れていることが考えられます。

RF 解析

RF 解析は、管理対象の SonicWall アクセスポイント、およびその他のすべての近隣無線アクセスポイントでの無線チャンネルの利用状況を把握するために使用する機能です。このセクションでは、SonicWall SonicOS の RF 解析機能を使用して、無線アクセスポイント装置を最大限に有効利用する方法を説明します。

- ① **補足:** SonicWall RF 解析では、サードパーティのアクセスポイントを解析してその統計値を RF データに取り込むこともできますが、そのためには SonicWall ファイアウォールで管理されている SonicWall アクセスポイントが少なくとも 1 つ存在しなければなりません。

RF 解析の選択

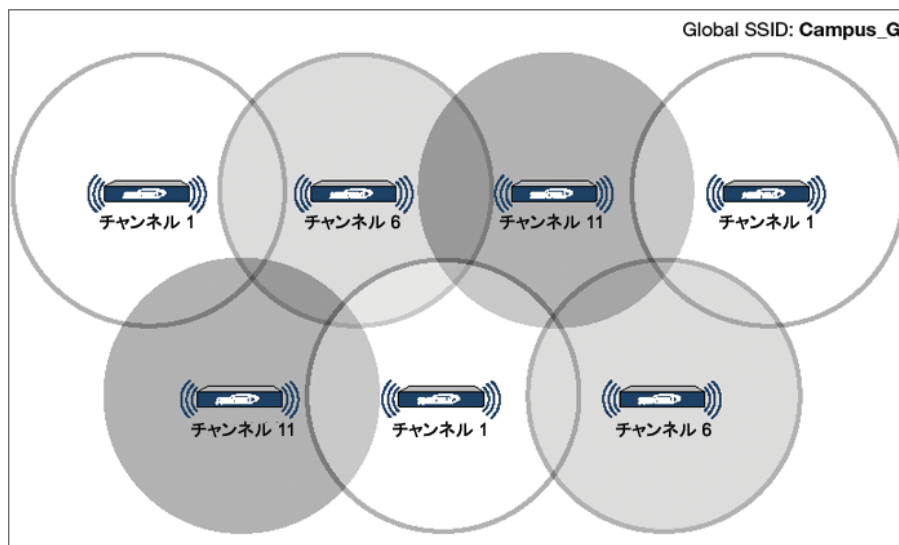
無線インフラの配備とメンテナンスはネットワーク管理者にとって気が重い仕事です。パフォーマンスが上がらない、接続性が悪いといった無線に関わる問題に無線ネットワークの管理者はたびたび直面しますが、皮肉にもそうした問題は、たいてい無線機の設定を解析して適切に調整するだけで解決できます。

RFA は、こうした無線に関する潜在的な問題を認識するためのツールです。RFA が扱う 2 つの主な問題は、チャンネルの過負荷と隣接チャンネルの SonicWall アクセスポイント干渉です。RF 解析は、運用中のアクセスポイントごとに RF スコアを算出し、データを表示することで、問題のある RF 環境で動作しているアクセスポイントを特定できるようにします。

RF 環境

IEEE 802.11 では ISM 2.4 GHz 帯と 5 GHz 帯のデバイスが規格の対象とされていますが、現在配備されている無線デバイスのほとんどは 2.4 GHz 帯を使用します。各チャンネルの占有帯域幅は 20 MHz で、利用可能な 11 チャンネルのうち 3 チャンネルだけが重複していません。米国では、チャンネル 1、6、および 11 が非重複チャンネルです。多数の SonicWall アクセスポイントを配備するときは、ほとんどの場合、この 3 チャンネルが使われます。

SONICPOINT の手動によるチャンネル選択



2.4GHz 帯は全体が 3 つの独立したチャンネル 1、6、11 に分割されます。これを理想的なシナリオで遂行するには、次の 2 点に注意する必要があります。1 つはチャンネルの割り当てで、もう 1 つは出力の調節です。ほとんどの場合、隣接する SonicPoint を異なるチャンネルに割り当てるのが最善です。SonicPoint の電波出力も注意深く監視しなければなりません。近くのクライアント同士が接続できるだけの十分な強度は必要ですが、同じチャンネル内で動作する他の SonicPoint と干渉しない範囲の出力であることも必要です。

SonicWall アクセスポイントにおける RF 解析の使用

RF 解析は、スコア、グラフ、および各種の数値に基づいて、無線に関する潜在的な問題や既存の問題をユーザーが検出して特定できるようにします。

最適なシナリオとしては、同じチャンネルで同時に動作するアクセスポイントの数をできるだけ少なくすることが望ましいわけですが、そのような状態を維持することは、特に多数のアクセスポイントを配備した環境では現実的ではありません。また、ISM 帯は一般に公開されているので、管理対象外のその他のデバイスがこの帯域で動作していることも考えられます。

トピック:

- RF スコアとは
- チャンネル使用率に関するグラフと情報
- 過負荷チャンネルの表示
- RFA 高干渉チャンネル

RF スコアとは

RF スコアは、1 から 10 の等級を範囲とする値で計算され、特定のチャンネルの全般的な状態を示すために用いられます。スコアの値は、それが大きいほど RF 環境の状態がよいことを意味します。スコアの値が小さい場合は、注意が必要です。



SonicWall の無線ドライバが報告する信号強度 (RSSI 値) からの式で、1 から 100 までの等級を範囲とする先行 RF スコアを求めることができます。

$$rfaScore100 = 100 - ((rssiTotal - 50) * 7 / 10)$$

簡略化: $rfaScore100 = -0.7 * rssiTotal + 135;$

この rfaScore100 から次のように最終スコアが求められます。

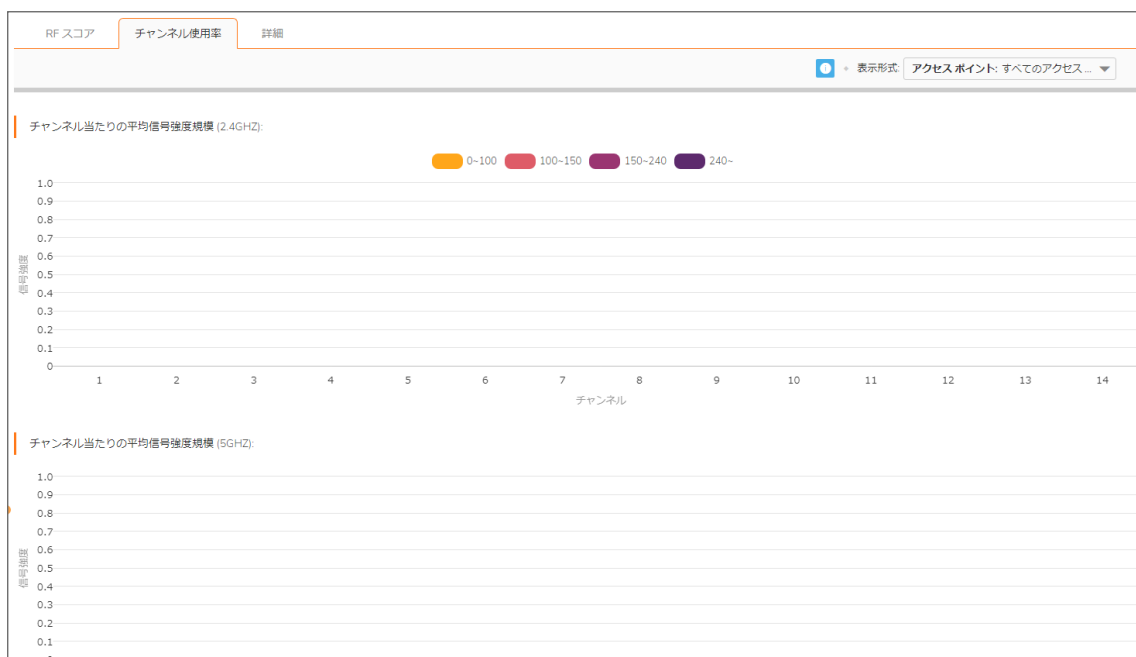
- RFA スコアが 96 より大きければ、10 と報告する。
- RFA スコアが 15 より小さければ、1 と報告する。
- その他のスコアは、1 から 10 の間に収まるように 10 で割った値の小数点以下を切り捨てて求めます。

SonicOS インターフェースには、SonicWall アクセスポイントが使用しているチャンネルに関する RF スコアが表示されます。

① **補足:** この機能は、SonicPoint がどのチャンネルで動作しているかという情報に基づいています。チャンネル番号がわからない場合、RF スコアは利用できなくなります。

チャンネル使用率に関するグラフと情報

接続中のすべての SonicPoint におけるチャンネルの利用状況を表示する手段として弊社が考案したのが、チャンネル使用率グラフです。



チャンネルごとに2つのカラーバーが表示されます。各カラーバーの頭頂部の数値は、そのチャンネルで特定の問題を検出した SonicWall アクセスポイントの数です。起動時に SonicWall アクセスポイントは利用可能なすべてのチャンネルに対してIDS スキャンを実行し、RF 解析はそれらのスキャンの結果を解析して、各チャンネルで発生する可能性のある問題を特定します。

例を以下に示します。10 台の SonicWall アクセスポイントが接続されていて、そのうちの6台がチャンネル11を過負荷状態であると判定した場合は、紫色のカラーバーの頭頂部の値が6になります。また、8台の SonicWall アクセスポイントがチャンネル6を重度に干渉されていると判定した場合は、青色のカラーバーの頭頂部の値が8になります。チャンネルに問題がなければ値0が表示されます。

① **補足:** ここにはチャンネル12、13、14が表示されていますが、これらのチャンネルが使われていない国もあります。しかし、それでもこれらのチャンネルは監視されます。不法な無線妨害を試みる人物がチャンネル12、13、14のいずれかに無線妨害器を設置して、それ以下のチャンネルに対してDoS (Denial of Service) 攻撃を仕掛ける可能性があるためです。

過負荷チャンネルの表示

RF 解析は同一チャンネルで動作するアクセスポイントの数が4を超えたことを検出すると警告を発します。信号強度とは関係なく、RF 解析はそのチャンネルを過負荷として報告します。

過負荷チャンネル



検出された各アクセスポイントに関する情報: SSID、MAC、信号強度、チャンネルです。信号強度には、「dBm」と「パーセント値」の2つの値が表示されます。

RFA 高干渉チャンネル

同一チャンネルで動作するアクセスポイントは干渉を起こす可能性があります。また、隣接チャンネル（チャンネル番号の差が5より小さいチャンネル）で動作するアクセスポイントも相互に干渉する可能性があります。

RFAは、特定の SonicPoint の周辺で、番号の相対距離が5より小さい範囲にあるチャンネルで動作する AP の数が5を超えていることを検出すると、警告を発します。信号強度とは関係なく、RFAはそれらのチャンネルを高干渉チャンネルとして報告します。

高干渉チャンネル

RF スコア	チャンネル使用率	詳細
同一チャンネルで動作している AP によって過負荷をかけられたチャンネル		同一チャンネル及び隣接チャンネルで動作している AP によって重畳に干渉したチャンネル
<input type="text" value="検索"/>		
#	アクセスポイント	
データなし		
分析		

検出された各 AP に関する情報は、SSID、MAC、信号強度、チャンネルです。信号強度には2つの値が表示されます。1つは dBm 値で、もう1つは % 値です。

RF スペクトラム

Wi-Fi デバイス、Bluetooth 無線技術、防犯カメラを広く使用すると、スペクトル干渉が増加し、パフォーマンスが低下します。SonicOS は、以下の機能を提供します。

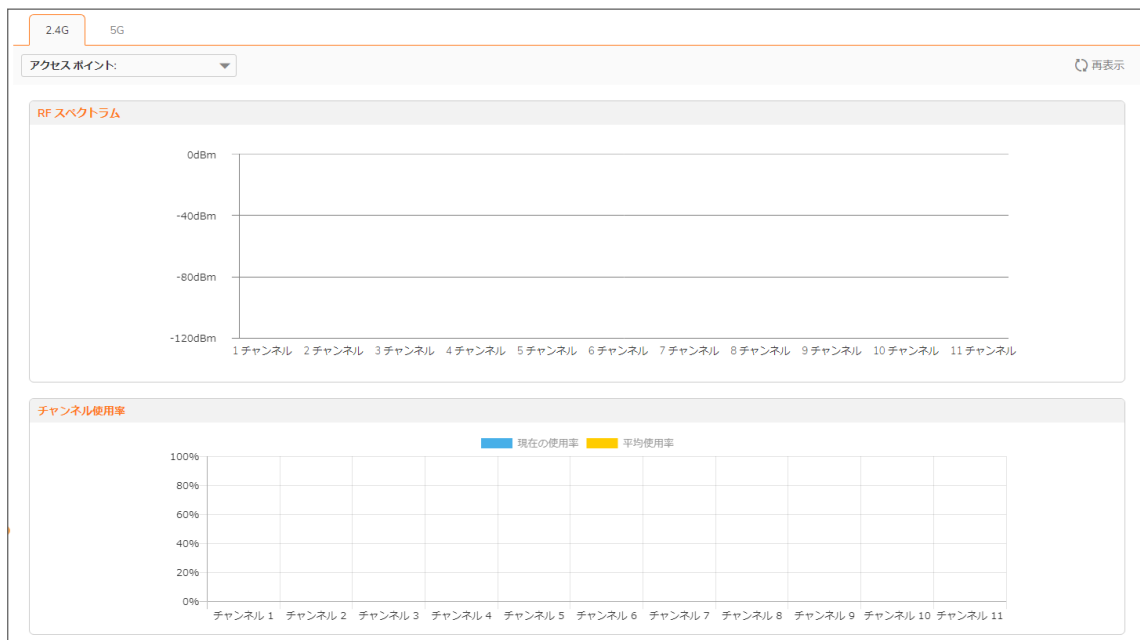
- 自動 RF チャンネル干渉検出。
- RF 環境のより深い層でトラブルシューティングを行い、それに応じて無線設定を調整する強力なツール。

問題のトラブルシューティングを支援するには、「デバイス > アクセスポイント > RF スペクトラム」ページに移動します。

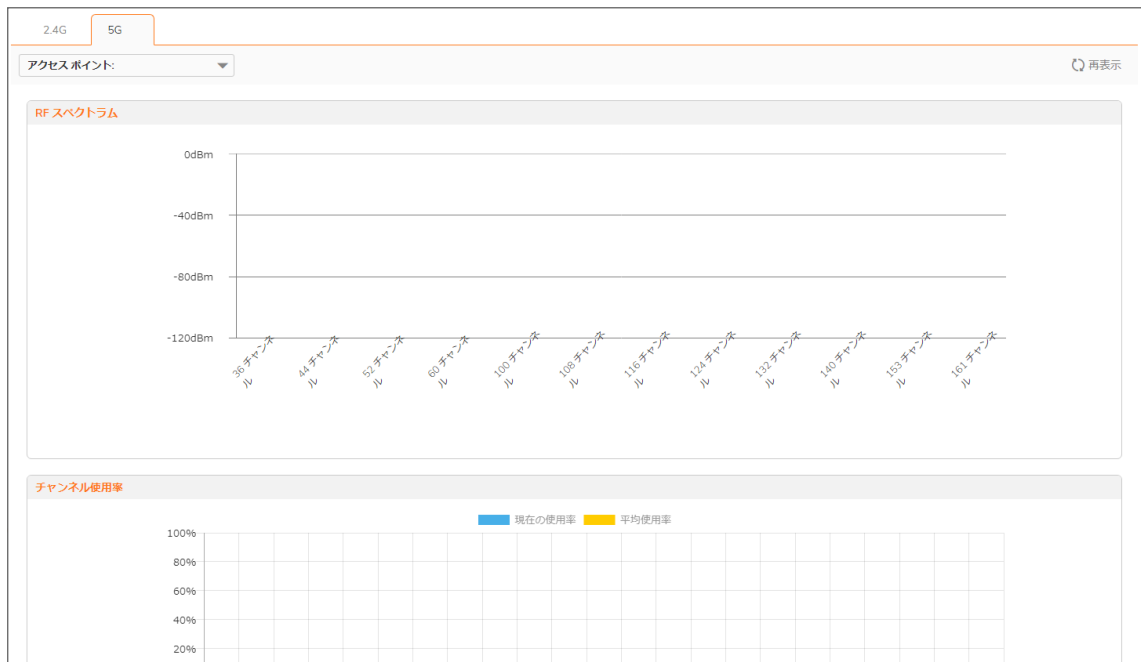
RF チャンネル干渉を監視するには、以下の手順に従います：

1. 監視する帯域幅 (2.4G または 5G) を選択します。
2. パフォーマンス低下または干渉検出の分析を行うアクセスポイントを「アクセスポイント」ドロップダウンメニューから選択します。

2.4G の例



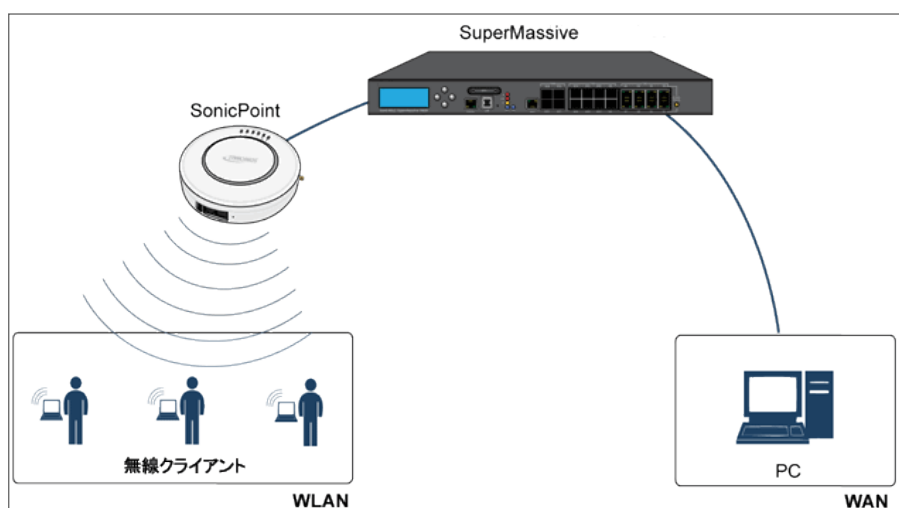
5G の例



FairNet

FairNet機能は、関連する無線クライアントの帯域幅を制御してクライアント間で帯域幅が公平に振り分けられるようにする機能で、ネットワーク管理者が簡単に使えるツールです。管理者は、すべての無線クライアント、特定の IP アドレス範囲、または個々のクライアントに対して FairNet の帯域幅制限を構成することで公平性とネットワーク効率を向上させることができます。

以下に、典型的な FairNet トポロジの例を示します。



ラップトップまたは PC に IEEE802.11b/g/n 無線ネットワーク インターフェース コントローラを装備する必要があります。

トピック:

- [サポート対象プラットフォーム](#)
- [FairNet の機能](#)
- [管理インターフェースの概要](#)
- [FairNet の設定](#)

サポート対象プラットフォーム

FairNet 機能は現在、次の装置モデルでサポートされています。

- SonicWall TZ シリーズ
- SonicWall NSA シリーズ
- SonicWall E-Class NSA シリーズ

FairNet の機能

Distributed Coordination Function (DCF) は、個々のクライアントが媒体にアクセスするとき等しい機会が得られるようタイミングの公平性を実現します。ただし、すべての無線クライアントの間でのステーション単位のデータトラフィックの公平性を保証することはできません。FairNet 機能は既存の 802.11 DCF 上に実装され、フローの数や方向とは関係なく、無線クライアントの間での公平な帯域幅を保証します。

トラフィック制御機能は、(キューの長さが限界に達した場合やトラフィックが速度制限を超えた場合に) パケットをキューに入れるか破棄するかを判断します。パケットをどの順序で送信するか判断する(特定の packets を優先する場合など)、パケットの送信を遅らせせる(発信トラフィックの速度を制限する場合など)といったことも行います。トラフィック制御がパケットを送信用に解放した後、デバイスドライバがそのパケットを補足し、ネットワークで放出します。

管理インターフェースの概要

FairNet 表示の要素を、以下のテーブルで説明します。

名前	説明
FairNet を有効にする	FairNet 機能を有効にします。
FairNet ポリシー	「FairNet ポリシー」テーブルの見出しで、「FairNet ポリシー」テーブルのすべてのポリシーを選択または選択解除します。ポリシーのリストでポリシーを個別に選択することもできます。
方向	各ポリシーの方向を表示します。方向は、次のように区分されます。 <ul style="list-style-type: none">• アップリンク• ダウンリンク• 両方
開始 IPアドレス	IPアドレス範囲の始点を表示します。
終了 IPアドレス	IPアドレス範囲の終点を表示します。
最低速度 (kbps)	クライアントに保証される最低帯域幅です。最低速度は 1Kbps です。
最高速度 (kbps)	クライアントに保証される最大帯域幅です。最大速度は 54000Kbps です。
インターフェース	FairNet ポリシーの適用先のインターフェースを表示します。これはアクセスポイントが接続する管理ファイアウォールのインターフェースです。
有効	このチェックボックスをオンにすると、選択された FairNet ポリシーが有効になります。

名前	説明
構成	編集アイコンが選択された場合に、既存の FairNet ポリシーを編集します。特定の FairNet ポリシーを削除するには、削除アイコンをクリックします。
追加	特定の IPアドレスまたはアドレス範囲について FairNet ポリシーを追加します。「Fairnet ポリシーの追加」ダイアログが表示されます。
削除	選択した FairNet ポリシーを削除します。
適用	直前の構成の設定を適用します。
キャンセル	構成の設定の変更を取り消します。

FairNet の設定

このセクションでは、FairNet の設定例を示します。

FairNet で両方向の帯域幅を広く構成するには、以下の手順に従います

1. 「デバイス > アクセスポイント > FairNet」ページに移動します。
2. 追加アイコンをクリックします。「Fairnet ポリシーの追加」ダイアログが表示されます。

FairNet ポリシーの追加

ポリシーを有効にする

方向 両方向 ▼

開始 IP アドレス

終了 IP アドレス

最低速度 (kbps)

最高速度 (kbps)

インターフェース ▼

3. 「ポリシーを有効にする」オプションをオンにします。これは、既定で選択されています。
4. 「方向」ドロップダウンメニューから、「両方向」を選択します。これでポリシーはコンテンツのアップロードとダウンロードを行うクライアントに適用されます。これは、既定で選択されています。
5. 「開始 IP アドレス」フィールドに、FairNet ポリシーの開始 IP アドレス (例えば、172.16.29.100) を入力します。
6. 「終了 IP アドレス」フィールドを選択し、FairNet ポリシーの終了 IP アドレス (例えば、172.16.29.110) を入力します。

① **ヒント:** この IP アドレス範囲は、WLAN インターフェースに関して構成されたサブネット上になければなりません。
7. 「最低速度 (kbps)」フィールドに、FairNet ポリシーの最小帯域幅を入力します。最小値かつ既定値は 100Kbps、最大値は 300Mbps (300,000Kbps) です。
8. 「最高速度 (kbps)」フィールドに、FairNet ポリシーの最大帯域幅を入力します。最小値かつ既定値は 100Kbps、最大値は 300Mbps (300,000Kbps) です。ただし、通常の設定は 20Mbps です。

9. 「**インターフェース**」ドロップダウンメニューから、アクセスポイントの接続先のインターフェース（例えば、「X2」）を選択します。
10. 「**OK**」をクリックします。FairNet ポリシーが「FairNet ポリシー」テーブルに追加されます。
11. 「**FairNet ポリシー**」テーブルで、FairNet ポリシーを有効にします。
12. 「**適用**」を選択します。

Wi-Fi マルチメディア

SonicOS アクセスポイントは、Wi-Fi マルチメディア (WMM) をサポートし、無線 IEEE 802.11 ネットワーク上で帯域幅を大量に使用する VoIP、Wi-Fi 電話機上の VoIP、マルチメディアトラフィックなどのアプリケーションのサービス品質 (QoS) エクスペリエンスを高めめます。

WMM は IEEE 802.11e 規格に基づく Wi-Fi Alliance の相互通信認証です。WMM では、以下の 4 つのアクセス種別に基づいてトラフィックに優先順位を付けます。

- 音声型 – 最も優先順位が高い
- 映像型 – 2 番目に優先順位が高い
- 最大努力型 – 3 番目に優先順位が高い (電子メールやインターネット サーフィンなどのアプリケーションを想定)
- バックグラウンド型 – 4 番目に優先順位が高い (印刷など、遅延の影響を受けにくいアプリケーションを想定)

① | **補足:** WMM は保証されたスループットを提供しません。

SonicWall 無線クラウド管理サポートは、SonicWave アクセスポイントにも利用できます。SonicWave を中央ファイアウォールに接続して管理する必要はありません。ネットワークに接続することにより、スタンドアロンで展開できます。このアプリケーションは、新しいモバイル アプリケーションでクラウドを介して管理できる無線サービスを提供します。

トピック:

- [WMM アクセス種別](#)
- [アクセス種別へのトラフィックの割り当て](#)
- [Wi-Fi マルチメディア パラメータの設定](#)
- [アクセスポイントの WMM プロファイルの作成](#)

WMM アクセス種別

それぞれのアクセス種別には自身の伝送キューがあります。トラフィックには、アプリケーションまたはファイアウォールのいずれかから提供されるサービス種別 (ToS) 情報に基づいて適切なアクセス種別が割り当てられます。SonicWall セキュリティ装置は、アクセスルールまたは VLAN タギングのいずれかを介して ToS を割り当てます。

以下の表に、WMM アクセス種別と 802.1D ユーザ優先順位の対応関係を示します。

Wi-Fi マルチメディアのアクセス種別

優先順位	ユーザ優先順位 (802.1D)	802.1D の指定	WMM アクセス種別 (AC)	WMM AC 指定 (情報)
最低	1	BK	AC_BK	バックグラウンド型
↓	2	—	AC_BK	バックグラウンド型
	0	BE	AC_BE	最大努力型
	3	EE	AC_BE	最大努力型
	4	CL	AC_VI	映像
	5	VI	AC_VI	映像
	6	VO	AC_VO	音声
最高	7	NC	AC_VO	音声

WMM は、拡張型分散チャンネル アクセス (EDCA) と呼ばれるプロセスによってトラフィックに優先順位を付けます。WMM は、アクセス種別ごとに異なる “バックオフ” 時間を定義してトラフィックに優先順位を付けます。WMM バックオフ時間は、以下の 2 つのパラメータで定義されます。

- **Arbitration Inter-Frame Space (AIFS)** – 無線チャンネルが無動作状態になってから、AC がチャンネルへのアクセスのネゴシエーションを開始できるようになるまでの時間間隔。
- **Contention Window (CW)** – ランダムなバックオフ時間のとり得る値の範囲。ランダムなバックオフ時間を指定する時間の範囲。CW は最小値と最大値で定義されます。
 - **Minimum contention window size (CWMin)** – CW の長さの最初の上限。AC は 0 ~ CWMin までのランダム時間待機してから伝送を試みます。優先順位の高い AC にはそれだけ短い CWMin が割り当てられます。
 - **Maximum contention window size (CWMax)** – CW の上限。競合が発生した場合、AC は CW のサイズを 2 倍にして (最大 CWMax まで) 伝送を再度試みます。CWMax は CWMin よりも大きい必要があります。

一般に、優先順位の高い AC には、AIFS、CWMin、CWMax の値が小さく設定されます。

① **補足:** AIFS、CWMin、および CWMax の測定単位は、使用されている 802.11 規格のスロット時間の倍数です。802.11b の場合、1 スロットは 20 マイクロ秒です。802.11a と 802.11g の場合、1 スロットは 9 マイクロ秒です。

アクセスポイントとステーション (SonicWall セキュリティ装置) にそれぞれ異なる WMM パラメータが構成されます。以下のテーブルに、アクセスポイントと SonicWall セキュリティ装置の既定の WMM パラメータを示します。

アクセスポイントの既定の WMM パラメータ

WMM アクセス種別 (AC)	WMM AC 指定 (情報)	CWMin	CWMax	AIFS
AC_BE(0)	最大努力型	4	6	3
AC_BK(1)	バックグラウンド型	4	10	7
AC_VI(2)	映像	3	4	1
AC_VO(3)	音声	2	3	1

SONICWALL セキュリティ装置の既定の WMM パラメータ

WMM アクセス種別 (AC)	WMM AC 指定 (情報)	CWMin	CWMax	AIFS
AC_BE(0)	最大努力型	4	10	3
AC_BK(1)	バックグラウンド型	4	10	7
AC_VI(2)	映像	3	4	2
AC_VO(3)	音声	2	3	2

アクセス種別へのトラフィックの割り当て

WMM はアクセスポイントに対して、複数の優先順位アクセス種別に対して複数のキューを実装するように要求しています。アクセスポイントは、アプリケーションまたはファイアウォールが提供する IP データ内のサービス種別 (TOS) 情報に基づいて、トラフィック種別を区別します。SonicWall セキュリティ装置は、WMM アクセス種別に以下の 2 つの方法でトラフィックを割り当てます。

- ファイアウォール サービスとアクセス ルールの指定
- VLAN タグ付け

ファイアウォール サービスとアクセス ルールの指定

特定のポートを使用するサービスに優先順位を付けて、適切な伝送キューに入れます。例えば、ポート 2427 に送信される UDP トラフィックをビデオ ストリームとみなすことができます。「オブジェクト > サービス > サービス オブジェクト」ページでユーザ定義サービスを追加します。詳細は、『SonicOS ポリシー』を参照してください。

新しいサービスに対して少なくとも 1 つのアクセス ルールが「ポリシー > ルールとポリシー > アクセス ルール」ページで追加されている必要があります。例えば、そのようなサービスが LAN ゾーン上のステーションから WLAN ゾーン上の無線クライアントに対して実行される場合は、アクセス ルールを「ルールの追加」ウィンドウで構成できます。「ルールの追加」ウィンドウの「トラフィックシェイピング」タブでは、明示的な DSCP 値が定義されます。

後に、送信先ポート 2427 で UDP プロトコルを使用してパケットがファイアウォールを通してアクセスポイントに送信されるたびに、それらの TOS フィールドはアクセスルール内の QoS 設定に従って設定されます。

VLAN タグ付け

SonicWave、SonicPoint N および AC では、同一の VLAN ID を使用して VLAN と接続するように仮想アクセスポイントを構成できるため、仮想アクセスポイントを介した VLAN 内の優先順位付けが可能です。VLAN トラフィックに対する優先順位はファイアウォール アクセスルールを通して設定可能です。

ファイアウォール アクセスルールは、例えば 2427 番ポートに向けられた UDP サービスに対する優先順位を設定するのと同様ですが、送信元と送信先は WLAN から WLAN へのルールであるため、WLAN サブネットのような VLAN (VAP を介した VLAN) インターフェースで構成します。詳細は、『SonicOS ポリシー』を参照してください。

Wi-Fi マルチメディア パラメータの設定

既定では、単一の WMM プロファイルが SonicWall セキュリティ装置に構成され、パラメータは 802.11e 規格の値に設定されます。

トピック:

- [WMM の設定](#)
- [アクセス ポイントの WMM プロファイルの作成](#)

WMM の設定

WMM 設定をカスタマイズするには、以下の手順に従います:

1. 「デバイス > アクセス ポイント > Wi-Fi マルチメディア S」ページに移動します。
2. WMM プロファイルを変更するには、そのプロファイルに対する編集アイコンを選択します。あるいは、新しい WMM プロファイルを作成する場合は、追加アイコンをクリックします。

アクセス種別	CWMin	CWMax	AIFS
AC_BE(0)	4	6	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	1
AC_VO(3)	2	3	1

アクセス種別	CWMin	CWMax	AIFS
AC_BE(0)	4	10	3
AC_BK(1)	4	10	7
AC_VI(2)	3	4	2
AC_VO(3)	2	3	2

3. 新しい WMM プロファイルを作成する場合は、「プロファイル名」を入力します。既定の名前は、wmmDefault です。
4. パラメータを変更して、WMM プロファイルをカスタマイズします。デフォルトの WMM パラメータ値はウィンドウに自動入力されます。これらの種別に関する詳細は、「[Wi-Fi マルチメディアのアクセス種別](#)」テーブルを参照してください。

① **補足:** WMM プロファイルを構成するときに、コンテンション ウィンドウのサイズ (CWMin/CWMax) と、AIFS (フレーム送信間隔) を構成できます。これらの値は、アクセス ポイント (SonicPoint-N) とステーション (ファイアウォール) 上の AC_BK、AC_BE、AC_VI、AC_VO の各優先順位に対して、個別に構成可能です。

5. 「割付」タブを選択して、アクセス種別と DSCP 値の割付をカスタマイズします。

アクセス種別	DSCP
AC_BE(0)	1
AC_BK(1)	8
AC_VI(2)	40
AC_VO(3)	48

6. 割付優先順位レベルを DSCP 値に対応付けることができます。既定の DSCP 値は、「ポリシー>ルールとポリシー>アクセスルール>ルールの追加>トラフィックシェイピング」タブの値と同じです。
7. 「OK」をクリックします。

アクセスポイントの WMM プロファイルの作成

「デバイス>アクセスポイント>Wi-Fi マルチメディア」ページは、パラメータと優先順位マッピングを含む WMM プロファイルを構成する方法を提供します。

詳細については、「[WMM の設定](#)」を参照してください。

WMM プロファイルの削除

1 つの WMM プロファイルを削除するには、そのプロファイルの「構成」列の削除アイコンをクリックします。

複数の WMM プロファイルを削除するには、削除するプロファイルの横にあるチェックボックスをオンにしてから、テーブル上部の削除アイコンをクリックします。


3G/4G/LTE WWAN

アクセスポイントに接続された 3G/4G/LTE デバイスがあれば、「デバイス>アクセスポイント>3G/4G/LTE WWAN」ページでそのデバイスに対する監視情報が提供されます。

最初のパネルは接続データとモデム状況を提供し、2 番目のパネルにはデバイスの信号強度をグラフィック表示します。

パネルでデータを更新するには、「更新」をクリックします。

3G/4G/LTE デバイスがアクセスポイントで検出されない場合、「デバイス>アクセスポイント>3G/4G/LTE WWAN」ページに以下のメッセージが表示されます。

SONICPOINT/SONICWAVE 3G/4G/LTE 設定	
	SonicPoint/SonicWave は WAN 接続を提供するために 3G/4G/LTE デバイスに接続できます。
SONICPOINT/SONICWAVE 3G/4G/LTE 状況	
データなし	

Bluetooth LE デバイス

SonicWave 432 および 200 シリーズの装置は、Bluetooth 低消費電力 (BLE) をサポートするようになりました。Bluetooth 低消費電力とは、標準の Bluetooth 装置と同程度の通信範囲を維持しつつ、消費電力とコストを大幅に削減する、無線パーソナルエリアネットワーク技術です。Bluetooth 低消費電力 (BLE) は、特に iBeacon 装置に近接している場合に、スマートフォン、タブレット、SonicWall モバイル アプリケーション、および他の SonicWave などの他のデバイスが SonicWave アクセスポイントに簡単に接続できるようにする標準的な Bluetooth のサブセットです。BLE は、位置推定と、より簡単な SonicWave 設定も提供します。

- ① **補足:** iBeacon はアップルが開発したプロトコルです。さまざまなベンダーが、近くの携帯電子デバイスに識別子をブロードキャストする iBeacon 互換の BLE デバイスを製造しています。このテクノロジーにより、スマートフォン、タブレット、その他のデバイスは、iBeacon の近くにいるときにアクションを実行できます。

BLE スキャンデータの表示

「デバイス > アクセスポイント > Bluetooth LE」ページには、近くの Bluetooth Low Energy (BLE) デバイスに関する情報が表示されます。ページ上部の「アクセスポイント」ドロップダウンリストから、1 つの SonicWave または「すべてのアクセスポイント」を選択することにより、表示を制御できます。

下のテーブルには、近くの BLE デバイスからスキャンされた情報が表示されます。使用可能な場合、列には次の情報が表示されます。

列	説明
#	テーブル行の参照番号。
アクセスポイント名	BLE デバイスをスキャンするアクセスポイント (SonicWave) の名前。
デバイス名	BLE デバイスの名前。
MAC アドレス	デバイスの一意的ハードウェアアドレス。
ベンダー	デバイスの製造元。
RSSI	負の数 (dB) で表される、BLE デバイスの受信信号強度インジケータ。数値が大きいく (ゼロに近い) ほど、信号は強くなります。
UUID	BLE デバイスの一意的識別子である近接 UUID。ちょうど 36 個の、16 進文字とハイフン。 すべてゼロには設定しないでください。
Major (重度)	BLE デバイス グループ内の上位の ID。有効な値は 0~65535 です。 0x0000 = 設定解除。

列	説明
Minor(軽度)	BLE デバイスグループ内の下位の ID。有効な値は 0~65535 です。 0x0000 = 設定解除。
電源	BLE デバイスの電力レベル (dBm)。これは、スキャンされたデバイスの測定電力です。Apple で定義されたある方法と同等の方法で複数の RSSI サンプルを平均化することにより計算されます。

無線リソース管理

このセクションでは、SonicOS における無線リソース管理および動的チャンネル選択で利用可能な設定について説明します。

- ① **補足:** 無線リソース管理は、SonicWave 231c、231o、432e、432i、432o などの専用スキャン無線を持つ SonicWall アクセスポイントでサポートされます。RRM 機能は、SonicWave 224w および SonicPoint ではサポートされません。

トピック:

- [無線リソース管理の設定](#)
- [動的チャンネル選択の設定](#)

無線リソース管理の設定

無線リソース管理の設定は、「デバイス>アクセスポイント>無線リソース管理」ページで行うことができます。

無線リソース管理基本設定

無線リソース管理 (RPM) を有効にする

ステーション品質のしきい値 (1 ~ 50) ①

無線品質のしきい値 (1 ~ 50) ①

動的チャンネル選択 (DCS) 設定

DCS モード グローバル ローカル ①

2.4GHz 無線 DCS スキーム ①

5GHz 無線 DCS スキーム ①

無線リソース管理基本設定

オプション名	説明
無線リソース管理 (RPM) を有効にする	このオプションを有効にすると、「ステーション品質のしきい値」と「無線品質のしきい値」の設定が有効になります。このオプションは、既定では無効になっています。

オプション名	説明
ステーション品質のしきい値(1～50)	<p>無線クライアントの接続状況を追跡・評価するための、1～50の健全性指標です。指標値が高いほど、無線ステーションはより高いデータ速度で接続されており、パケット損失が少ないことを意味します。</p> <p>ステーションの品質が構成されたしきい値を下回ると、無線クライアントは切断されます。</p> <ul style="list-style-type: none"> 最小値 = 1 最大値 = 50 既定値 = 20
無線品質のしきい値(1～50)	<p>電波帯の利用状況を追跡・評価するための、1～50の健全性指標です。指標値が高いほど、無線帯域の利用率が低く、パケット損失が少ないことを意味します。</p> <p>無線品質が構成されたしきい値を下回ると、無線送信電力が低下します。</p> <ul style="list-style-type: none"> 最小値 = 1 最大値 = 50 既定値 = 20

無線リソース管理の設定を構成するには、以下の手順に従います

1. 「デバイス>アクセスポイント>無線リソース管理」ページに移動します。
2. 「無線リソース管理(RPM)を有効にする」オプションを選択し、この機能を有効にします。
3. 「ステーション品質しきい値(1-50)」について、1～50の値を入力するか、既定の設定値20を受け入れます。
 指標値が高いほど、無線ステーションはより高いデータ速度で接続されており、パケット損失が少ないことを意味します。ステーションの品質が構成されたしきい値を下回ると、無線クライアントは切断されます。
4. 「無線品質しきい値(1-50)」について、1～50の値を入力するか、既定の設定値20を受け入れます。
 指標値が高いほど、無線帯域の利用率が低く、パケット損失が少ないことを意味します。無線品質が構成されたしきい値を下回ると、無線送信電力が低下します。
5. 「適用」を選択します。

動的チャンネル選択の設定

動的チャンネル選択の設定は、「デバイス>アクセスポイント>無線リソース管理」ページで行うことができます。

無線リソース管理基本設定

無線リソース管理 (RPM) を有効にする

ステーション品質のしきい値 (1 ~ 50) ⓘ

無線品質のしきい値 (1 ~ 50) ⓘ

動的チャンネル選択 (DCS) 設定

DCS モード グローバル ローカル ⓘ

2.4GHz 無線 DCS スキーム ⓘ

5GHz 無線 DCS スキーム ⓘ

動的チャンネル選択 (DCS) 設定

オプション名	説明
DCS モード	「DCS モード」は、チャンネルの自動選択のために、2つの設定をサポートします。 <ul style="list-style-type: none">「グローバルモード」- ファイアウォールは、すべての SonicWave からの情報に応じて、すべての SonicWave に適切なチャンネルを割り当てます。「ローカルモード」- SonicWave は、自分自身の情報を元に最適なチャンネルを見つけます。
2.4GHz 無線 DCS スキーム	2.4GHz または 5GHz 無線 DCS スキームオプションは以下の通りです。
5GHz 無線 DCS スキーム	<ul style="list-style-type: none">セーフモード - SonicWave は、クライアントが接続されていない場合のみ、より適切なチャンネルに切り替えます。これは、保守的なモードです。安定モード - SonicWave は、バックグラウンドで定期的により適切なチャンネルを探します。これは、中間のモードです。高速モード - SonicWave は、現在のチャンネルでノイズ/干渉が強くなったら、すぐにより適切なチャンネルに切り替えます。これは、積極的なモードです。 既定は、「セーフモード」です。

動的チャンネル選択の設定を構成するには、以下の手順に従います

- 「デバイス>アクセスポイント>無線リソース管理」ページに移動します。
- 「DCS モード」について、「グローバル」または「ローカル」を選択します。

「グローバル」を選択すると、ファイアウォールは、すべての SonicWave から受信した情報に応じて、すべての SonicWave に適切なチャンネルを割り当てます。「ローカル」を選択すると、SonicWave は、自分自身の情報を元に最適なチャンネルを見つけます。

3. 「2.4GHz 無線 DCS スキーム」について、以下のいずれかを選択します。

- **セーフモード**

SonicWave は、クライアントが接続されていない場合にのみ、より良いチャンネルに切り替えます。これは、保守的なモードです。

- **安定モード**

SonicWave は、バックグラウンドで定期的により良いチャネルを探します。これは、中間のモードです。

- **高速モード**

SonicWave は、現在のチャンネルでノイズ／干渉が高くなったら、すぐにより良いチャンネルに切り替えます。これは、積極的なモードです。

4. 「5GHz 無線 DCS スキーム」について、以下のいずれかを選択します。

- **セーフモード**

SonicWave は、クライアントが接続されていない場合にのみ、より良いチャンネルに切り替えます。これは、保守的なモードです。

- **安定モード**

SonicWave は、バックグラウンドで定期的により良いチャネルを探します。これは、中間のモードです。

- **高速モード**

SonicWave は、現在のチャンネルでノイズ／干渉が高くなったら、すぐにより良いチャンネルに切り替えます。これは、積極的なモードです。

5. 「適用」を選択します。

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、次の URL を開きます:

<https://www.sonicwall.com/ja-jp/support>

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- 次のサイトでコミュニティフォーラムのディスカッションに参加したり、その内容を閲覧したりする:
<https://community.sonicwall.com/technology-and-support>
- ビデオ チュートリアルを視聴する。
- <https://mysonicwall.com> にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: <https://www.sonicwall.com/ja-jp/support/contact-support>

このドキュメントについて

- ① | **補足:** メモアイコンは、補足情報があることを示しています。
- ① | **重要:** 重要アイコンは、補足情報があることを示しています。
- ① | **ヒント:** ヒントアイコンは、参考になる情報があることを示しています。
- △ | **注意:** 注意アイコンは、手順に従わないとハードウェアの破損やデータの消失が生じる恐れがあることを示しています。
- △ | **警告:** 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS アクセス ポイント 管理者ガイド

更新日 - 2021 年 3 月

ソフトウェア バージョン - 7

232-005634-10 Rev B

Copyright © 2022 SonicWall Inc. All rights reserved.

本文書の情報は SonicWall およびその関連会社の製品に関して提供されています。明示的または暗示的、禁反言にかかわらず、知的財産権に対するいかなるライセンスも、本文書または製品の販売に関して付与されないものとします。本製品のライセンス契約で定義される契約条件で明示的に規定される場合を除き、SONICWALL および/またはその関連会社は一切の責任を負わず、商品性、特定目的への適合性、あるいは権利を侵害しないことの暗示的な保証を含む(ただしこれに限定されない)、製品に関する明示的、暗示的、または法定的な責任を放棄します。いかなる場合においても、SONICWALL および/またはその関連会社が事前にこのような損害の可能性を認識していた場合でも、SONICWALL および/またはその関連会社は、本文書の使用または使用できないことから生じる、直接的、間接的、結果的、懲罰的、特殊的、または付随的な損害(利益の損失、事業の中断、または情報の損失を含むが、これに限定されない)について一切の責任を負わないものとします。SonicWall および/またはその関連会社は、本書の内容に関する正確性または完全性についていかなる表明または保証も行いません。また、事前の通知なく、いつでも仕様および製品説明を変更する権利を留保し、本書に記載されている情報を更新する義務を負わないものとします。

詳細については、次のサイトを参照してください: <https://www.sonicwall.com/ja-jp/legal>

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: <https://www.sonicwall.com/ja-jp/legal>

オープンソースコード

SonicWall Inc. では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープンソースコードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、「SonicWall Inc.」を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request

Attn: Jennifer Anderson

1033 McCarthy Blvd

Milpitas, CA 95035