



SonicOS 7

内部無線

管理者ガイド

SONICWALL®

# 目次

<b>状況</b> .....	<b>4</b>
WLAN 設定 .....	4
WLAN の統計 .....	5
WLAN 利用状況 .....	6
ステーション状況 .....	6
<b>設定</b> .....	<b>8</b>
デバイス サポート .....	9
コンプライアンス .....	9
FCC U-NII の新しい規則への準拠 .....	9
RED 遵守 .....	9
無線接続を使用する場合の考慮事項 .....	9
最適な無線パフォーマンスのための推奨事項 .....	10
アンテナの調整 .....	10
無線ノード数の強制 .....	11
MAC フィルタ リスト .....	11
無線の設定 .....	11
アクセス ポイント .....	11
無線 WDS ステーション .....	16
アクセス ポイントおよび WDS ステーション .....	18
<b>セキュリティ</b> .....	<b>21</b>
認証について .....	21
WEP 設定の構成 .....	23
WPA3/WPA2/WPA PSK 設定の構成 .....	24
WPA3/WPA2/WPA EAP 設定の構成 .....	25
<b>詳細</b> .....	<b>27</b>
ビーコンと SSID の制御 .....	28
グリーン アクセス ポイント .....	28
無線に関する詳細設定 .....	29
設定可能な使用するアンテナ .....	30
<b>MAC フィルタ リスト</b> .....	<b>31</b>
展開に関する考慮事項 .....	32
MAC フィルタ リストの設定 .....	32
<b>IDS</b> .....	<b>33</b>
アクセス ポイントの IDS .....	33

悪意のあるアクセス ポイント .....	33
IDS の設定 .....	34
検出されたアクセス ポイント .....	35
ネットワークでのアクセス ポイントの許可 .....	36
<b>仮想アクセス ポイント .....</b>	<b>37</b>
無線仮想 AP 設定タスクリスト .....	37
仮想アクセス ポイント プロファイル .....	39
仮想アクセス ポイント スケジュールの設定 .....	39
仮想アクセス ポイント プロファイル 設定 .....	39
ACL 強制 .....	42
仮想アクセス ポイント .....	43
VAP 一般設定 .....	43
VAP 詳細設定 .....	43
仮想アクセス ポイント グループ .....	44
仮想アクセス ポイント グループの有効化 .....	44
<b>SonicWall サポート .....</b>	<b>45</b>
このドキュメントについて .....	46

# 状況

① | **補足:**「内部無線状況」ページは無線プラットフォームにのみ適用されます。

「デバイス > 内部無線 > 状況」ページでは、無線通信機およびクライアントステーション情報を含んだ無線ネットワークの状況情報が提供されます。

「内部無線状況」ページには、以下のテーブルが表示されます。

- [WLAN 設定](#)
- [WLAN の統計](#)
- [WLAN 利用状況](#)

## WLAN 設定

「内部無線状況」ページには、内蔵無線の設定情報をリスト化した「WLAN 設定」テーブルが表示されます。「WLAN 設定」テーブルの設定可能項目はすべて、対応する設定ページへのハイパーリンクになっています。

### WLAN 設定

WLAN 設定	値
WLAN	「有効 (動作中)」または「無効 (停止中)」の設定を構成するには、「編集」リンクをクリックして「内部無線 > 設定」ページを開いてください。
SSID	無線ネットワークの識別のためのサービス セット識別子 (SSID) を構成するには、「編集」リンクをクリックして「内部無線 > 設定」ページを開いてください。
プライマリ BSSID	無線セキュリティ装置の MAC アドレス/シリアル番号
プライマリ IP アドレス	無線インターフェースの IP アドレス
プライマリ サブネット マスク	無線サブネットのネットマスク
規制地域	北米の装置の場合は「FCC - 北米」 日本の装置の場合は「MCK - 日本」 北米以外の装置の場合は「ETSI - 欧州」
チャンネル	無線信号の送信のために選択するチャンネル番号を構成するには、「編集」リンクをクリックして「内部無線 > 設定」ページを開いてください。

無線伝送速度	無線データ転送速度で、「最良」またはいくつもの可能な Mbps 単位の数値から選択します。これを構成するには、「編集」リンクをクリックして「内部無線 > 詳細」ページを開いてください。
無線伝送能力	現在の無線信号転送の電力レベルで、「最大出力」またはその他のいくつかの設定から選択します。これを構成するには、「編集」リンクをクリックして「内部無線 > 詳細」ページを開いてください。
プライマリ セキュリティ	無線のユーザ認証に使用する暗号化設定、または「無効」から選択します。これを構成するには、「編集」リンクをクリックして「内部無線 > セキュリティ」ページを開いてください。
MAC フィルタ リスト	クライアント無線デバイス (MAC アドレス) の許可リストと拒否リストの両方またはどちらかが「有効」あるいは「無効」であることを示します。これを構成するには、「編集」リンクをクリックして「内部無線 > MAC フィルタ リスト」ページを開いてください。
無線ゲスト サービス	「有効」または「無効」ゲスト サービスの有効化または無効化は「オブジェクト > ゾーン」で、ゾーンを編集してダイアログの「ゲスト サービス」画面の設定を更新して行うことができます。
侵入検知	「有効」または「無効」これを構成するには、「編集」リンクをクリックして「内部無線 > IDS」ページを開いてください。
無線ファームウェア	無線カードのファームウェア バージョン
参加ステーション	無線セキュリティ装置に参加しているクライアントの数と、その装置がサポートしている無線参加の最大数です。
無線モード	現在の無線転送のモードで、以下を含みます。 <ul style="list-style-type: none"> <li>• 種別 - 「2.4GHz」または「5GHz」無線周波数帯</li> <li>• プロトコル - 「802.11 a」、「b」、「g」、「n」、「ac」、または「/」で表されるそれらの組み合わせ</li> <li>• 「混在」または「単一」- 複数プロトコルが無線でサポートされている場合は「混在」、無線モードが特定の単一のプロトコルのデバイスとしか接続しないよう構成されている場合は「単一」</li> </ul> これを構成するには、「編集」リンクをクリックして「内部無線 > 設定」ページを開いてください。

## WLAN の統計

「内部無線状況」ページの「WLAN の統計」テーブルには、装置の無線通信と無線クライアントデバイスとの間で WLAN 経由で送信および受信するすべてのトラフィックが表示されます。「WLAN の統計」列には記録されたトラフィックの種別、「受信」列には受信したトラフィック、「送信」列には送信したトラフィックが表示されます。

### WLAN の統計

無線統計	受信/送信
正常フレーム	受信および送信し、許可されたフレームの数。
不良フレーム	破棄されたフレームの数。
正常バイト	正常フレームの合計バイト数。
管理フレーム	受信および送信された管理フレームの数。

制御フレーム	受信および送信された制御フレームの数。
データフレーム	受信および送信されたデータフレームの数。

## WLAN 利用状況

「内部無線状況」ページの「WLAN の利用状況」テーブルには、SonicWall 無線セキュリティ装置に接続している無線クライアントの履歴が表示されます。

### WLAN 利用状況

無線利用状況	値
参加	無線セキュリティ装置に接続した無線クライアントの数。
不参加	無線セキュリティ装置から切断された無線クライアントの数。
再参加	以前に接続していて再接続した無線クライアントの数。
認証	認証された無線クライアントの数。
非認証	切断された認証済みクライアントの数。
破棄されたパケット	破棄されたパケットの数。

## ステーション状況

「内部無線状況」ページの「ステーション状況」タブには、無線セキュリティ装置に現在参加している無線クライアントデバイスの情報が表示されます。

### ステーション状況

無線情報	説明
ステーション	無線クライアント デバイスの名前
MAC アドレス	クライアント デバイスの無線ネットワークカードのハードウェア アドレス
ベンダー	クライアント ステーションを製造したベンダー
SSID	クライアント ステーションが接続されている無線のサービス セット識別子 (SSID)
認証済	クライアント認証の状況
参加済	クライアント ステーションと SonicWall 無線装置の間の無線参加状況
参加 ID	セキュリティ装置によって割り当てられた参加 ID
信号	無線信号の強度
接続速度	クライアント ステーションと無線装置の間の接続速度。通常は Mbps 単位。
タイムアウト	セッションの残り秒数

---

無線情報	説明
構成	<p data-bbox="467 264 1319 297">クライアントステーションを制御するオプションで、以下のようなものがあります。</p> <ul data-bbox="467 331 1319 676" style="list-style-type: none"><li data-bbox="467 331 1319 432">•  - このステーションにセキュリティ装置への接続を許可し、MACフィルタの許可リストに追加します。</li><li data-bbox="467 465 1319 566">•  - このステーションをセキュリティ装置から遮断し、MACフィルタの拒否リストに追加します。</li><li data-bbox="467 600 1319 676">•  - このステーションをセキュリティ装置からログアウトさせ、参加解除します。</li></ul>

---

## 設定

SonicWall 無線セキュリティ装置は、装置に関する無線設定を構成するためのページを「[デバイス](#) > [内部無線](#) > [設定](#)」のみで提供します。

SonicWall 無線セキュリティ装置は、IEEE802.11a、IEEE 802.11ac、IEEE 802.11b、802.11g、および 802.11n という無線プロトコルをサポートしており、無線伝送でデータを送信します。これらの無線伝送は一般に Wi-Fi として知られています。SonicWall 無線セキュリティ装置は、アクセス ポイント、セキュア無線ゲートウェイ、および、NAT や VPN の柔軟な開始と停止が可能なステートフル ファイアウォールという 3 つのネットワークコンポーネントを組み合わせ、全面的に安全な無線ファイアウォールを提供します。この組み合わせにより、無線セキュリティ装置は、ネットワークセキュリティを損なうことなく無線の柔軟性を実現します。

通常、無線セキュリティ装置は、無線 LAN のアクセス ポイントになり、LAN 上のコンピュータのセントラル アクセス ポイントの役割を果たします。また、1 つのブロードバンド接続をネットワーク上のコンピュータと共有します。無線セキュリティ装置はファイアウォール保護も提供するので、インターネットからの侵入者はネットワーク上のコンピュータやファイルにアクセスできません。これは、ネットワーク上のコンピュータ間で共有している DSL 回線や T1 回線などの“常時稼働”接続にとって特に重要です。

ただし、無線 LAN は他の無線ネットワークから“傍受”されやすいので、無線 LAN には無線セキュリティポリシーを確立する必要があります。無線セキュリティ装置では、無線クライアントはファイアウォールのアクセス ポイントレイヤに接続します。有線ネットワークに接続を直接ブリッジする代わりに、無線トラフィックはまず保護された無線ゲートウェイレイヤへ渡され、クライアントはそこでユーザレベル認証で認証される必要があります。ゲスト サービスと MAC フィルタリストへの無線アクセスは無線セキュリティ装置によって管理されます。すべてのセキュリティ条件を満たすと、無線ネットワークトラフィックは以下のいずれかの配信システムを通過できます。

- LAN
- WAN
- WLAN 上の無線クライアント
- DMZ または Opt ポート上のその他のゾーン
- VPN トンネル

### トピック:

- [デバイス サポート](#)
- [コンプライアンス](#)
- [無線接続を使用する場合の考慮事項](#)
- [アンテナの調整](#)
- [無線ノード数の強制](#)
- [MAC フィルタリスト](#)
- [無線の設定](#)

# デバイス サポート

SonicOS でサポートされる無線ネットワーク セキュリティ装置 (ファイアウォール):

- TZ570W
- TZ500W
- TZ400W
- TZ350/350W
- TZ300W
- SOHO W
- SOHO 250/250W

## コンプライアンス

無線デバイスを特定の国や地域で販売・使用するには、さまざまな必要条件を遵守する必要があります。SonicWall 無線デバイスに関する利用認可と制限の最新情報については、<https://www.sonicwall.com/ja-jp/support/technical-documentation> で対象製品の技術文書を参照してください。デバイスごとに、固有の規制文書、または関連情報を提供する『クイックスタートガイド』があります。

## FCC U-NII の新しい規則への準拠

SonicOS 6.2.5.1 以降では、FCC U-NII (Unlicensed -National Information Infrastructure) の新しい規則 (Report and Order ET Docket No. 13-49) が TZ シリーズおよび SOHO 無線装置でサポートされます。動的周波数選択 (DFS) に関する FCC の新しい規則に準拠するために、TZ シリーズまたは SOHO 無線装置は DFS バンドのレーダー信号を検出してレーダー信号との干渉を回避します。

- ① **補足:** FCC の新しい規則に準拠したファームウェアを使用して製造された TZ シリーズおよび SOHO 無線装置は、SonicOS 6.2.5.1 以降でのみサポートされています。

## RED 遵守

SonicOS 6.5 以降では、TZ シリーズおよび SOHO 無線装置は無線デバイス指令 (RED) をサポートしています。RED (2014/53/EU) は、安全性、衛生、電磁的適合性および電波スペクトルの効率的な使用に対する重要な必要事項を規定しています。

## 無線接続を使用する場合の考慮事項

無線接続を有線接続と比較して検討する際には、インフラおよび環境に対する利点と欠点を考慮してください。

モビリティ	ネットワークの大多数はラップトップコンピュータですか？ 無線接続は有線接続より移動性に優れています。
利便性	無線ネットワークでは、各コンピュータをケーブルでつないだり、コン

	<p>コンピュータケースを開けてネットワークカードをインストールしたりする必要がありません。</p>
速度	<p>ネットワーク速度が重要な場合は、無線接続よりイーサネット接続を使用することを検討してください。</p>
到達範囲	<p>ネットワーク環境に物理的な障害物や干渉要素が多い場合、無線ネットワークは適さない可能性があります。</p>
セキュリティ	<p>無線伝送の持つ無制約な性質上、無線ネットワークには本質的なセキュリティ問題があります。ただし、無線セキュリティ装置はファイアウォールであり、その NAT 機能でセキュリティを提供しており、WPA または WPA2 を使用してデータ伝送を保護できます。</p>

## 最適な無線パフォーマンスのための推奨事項

最適な無線パフォーマンスのために、SonicWall は以下を推奨します。

- 無線セキュリティ装置は、目的のネットワークの中心近辺に配置します。こうすることによって、近隣の無線ネットワークから傍受される可能性も低減できます。
- 無線セキュリティ装置と PC やラップトップなどの受信ポイントの間の壁や天井の数を最小限にします。
- 無線セキュリティ装置は、できる限り、他の無線コンポーネントから直線で結ばれる位置に配置するようにします。無線コンポーネント同士が直接見える位置にあると、最高のパフォーマンスが得られます。
- 建築構造によっても無線パフォーマンスに違いが出ることがあります。
  - 無線セキュリティ装置は、壁や暖炉など大きくて隙間のない物体の近くに置かないようにします。
  - 無線セキュリティ装置をコンピュータケース、モニター、装置など金属製の物の近くに置くと、そのユニットのパフォーマンスが低下することがあります。
  - 金属製フレーム、窓ガラス用 UV カット フィルム、コンクリート造または石造の壁、金属塗料などの近くに無線セキュリティ装置を設置した場合も、信号強度が低下することがあります。
- 建物の上階では、無線セキュリティ装置を高い場所に設置すると、障害物を回避してパフォーマンスを向上させることに役立ちます。
- 近隣の無線ネットワークや無線デバイスによって、無線セキュリティ装置の信号強度、速度、到達範囲が影響を受けることがあります。
- コードレス電話、ラジオ、電子レンジ、テレビなどのデバイスによって、無線セキュリティ装置に干渉が発生する可能性もあります。

## アンテナの調整

無線セキュリティ装置のアンテナを調整して、無線受信状態が最もよくなるようにします。まず、アンテナをまっすぐ上に立て、それから必要に応じて調整します。無線セキュリティ装置の真下など、一部、相対的に受信状態の悪い領域があります。アンテナを別の無線デバイスに直接向けても、受信状態の向上にはつながりません。干渉が発生する可能性があるため、アンテナを金属製のドアや壁の近くに配置しないでください。

# 無線ノード数の強制

WLAN に接続しているか、SonicWall GroupVPN 経由で接続しているユーザは、SonicWall 無線ネットワーク装置でノード数の強制に加算されません。LAN および Opt ポート上の非無線ゾーンのユーザのみ、ノード数制限に加算されます。

「ステーション状況」テーブルには、接続されているすべての無線ノードが表示されます。

# MAC フィルタリスト

SonicWall 無線セキュリティ装置のネットワークプロトコルは、ネイティブの MAC アドレス フィルタリング機能を提供します。MAC アドレス フィルタリングを有効にすると、802.11 レイヤでフィルタリングが行われ、無線クライアントは認証と無線アクセスポイントへの参加ができなくなります。認証と参加なしにはデータ通信は行えないので、クライアントが無線ネットワークカードの Mac アドレスをネットワーク管理者に提示するまではネットワークへのアクセスは許可されません。

# 無線の設定

無線装置は、アクセスポイント、無線クライアントブリッジ、またはアクセスポイントとステーションとしてセットアップできます。

## 802.11 無線アンテナの設定を構成するには、以下の手順に従います

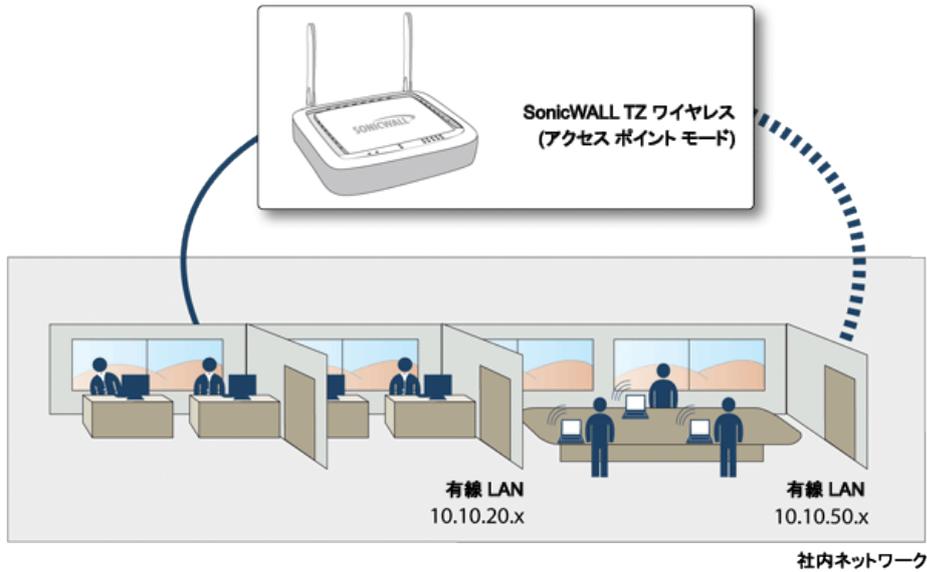
1. 「デバイス > 内部無線 > 設定」に移動します。
2. 装置に実行させたい「無線の役割」を選択します。
  - ① | **重要:** モードを変更すると、クライアントが切断され、再起動が必要になります。
  - ① | **補足:** どの「無線の役割」を選択したかに応じて、ページ内のオプションの表示は変わります。

以下のセクションでは、個々の「無線の役割」オプションに対する構成方法について説明します。

- [アクセスポイント](#)
- [無線 WDS ステーション](#)
- [アクセスポイントおよび WDS ステーション](#)

# アクセスポイント

「無線の役割」として「アクセスポイント」を選択した場合、SonicWall を下図に示すような無線クライアントに対するインターネット/ネットワークゲートウェイとして構成することになります。



#### トピック:

- アクセスポイント無線の設定
- 無線仮想アクセスポイント

## アクセスポイント無線の設定

- ① **重要:** 無線装置をアクセスポイントとして設定する場合、無線運用者は、該当する地域の電波を管轄する関係団体または機関により発布されているすべての法令や規制を遵守する責任を負います。

1. 「デバイス > 内部無線 > 設定」に移動します。
2. 「無線の役割」フィールドで、「アクセス ポイント」をドロップダウン メニューから選択します。

3. 「WLAN を有効にする」オプションをオンにして有効にします。これによって、モバイル ユーザにクリーンな無線アクセスを提供できます。WLAN 無線は既定では無効になっています。
4. 「スケジュール」フィールドで、ドロップダウン メニューから WLAN 無線をアクティブにする時間を選択します。「スケジュール」リストには、「オブジェクト > 一致オブジェクト > スケジュール」ページで作成および管理するスケジュール オブジェクトが表示されます。既定値は「常に有効」です。
5. 「国コード」フィールドには、アクセス ポイントが使用される国を選択してください。国コードは、どの規制地域の管轄で無線を利用するかを決定します。
6. 「無線モード」フィールドには、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。無線セキュリティ装置では、次のモードがサポートされています。

- ① **ヒント:** 802.11n クライアントだけを対象に最適なスループット速度を実現するために、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。
- 802.11n/a/ac 混在 - 802.11a、802.11ac、および 802.11n のクライアント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。
  - 「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する場合は、このモードを選択します。

無線モード	定義
2.4GHz 802.11n/g/b 混在	802.11b、802.11g、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。
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。

無線モード	定義
2.4GHz 802.11g/b 混在	802.11g と 802.11b 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両方の種別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。
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を選択できます。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 802.11n/a 混在	802.11a と 802.11n のクライアント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。
5GHz 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する場合は、このモードを選択します。
5GHz 802.11a のみ	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。
5GHz 802.11n/a/ac 混在	802.11a、802.11n、および 802.11ac のクライアント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。
5GHz 802.11ac のみ	スループットを向上させたい場合に選択してください。

「無線の設定」セクションの残りのオプションは、選択した無線モードに応じて表示が変化する場合があります。

#### トピック:

- [802.11n の無線設定](#)
- [802.11a/b/g の無線設定](#)
- [802.11ac の無線設定](#)

## 802.11n の無線設定

「無線モード」フィールドが 802.11n のみ、または 802.11n を含む混在モードに設定された場合、以下のオプションを構成します。

① | **補足:** 設定する構成の種別に応じて、実際に表示されるオプションは多少変わる場合があります。

無線帯域	802.11n の無線帯域を設定します。
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。このオプションは既定の設定です。
標準 - 20 MHz チャンネル	802.11n 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。このオプションを選択すると、「標準チャンネル」ドロップダウンメニューが表示されます。
標準チャンネル	既定値は自動であり、装置は信号の強度と整合性に基づいて最適なチャンネルを設定します。オプションで、規制地域内の単一のチャンネルを選択することもできます。特定のチャンネルを選択すると、エリア内の他の無線ネットワークとの干渉を防ぐのにも役立ちます。
広域 - 40 MHz チャンネル	802.11n 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。このオプションを選択すると、「プライマリチャンネル」および「セカンダリチャンネル」ドロップダウンメニューが表示されます。
プライマリチャンネル	既定値は自動であり、特定のプライマリチャンネルを指定することもできます。
セカンダリチャンネル	このドロップダウンメニューの設定は、プライマリチャンネルでの選択によって決まります。 <ul style="list-style-type: none"> <li>• プライマリチャンネルを「自動」に設定すると、セカンダリチャンネルも「自動」に設定されます。</li> <li>• プライマリチャンネルを特定のチャンネルに設定すると、セカンダリチャンネルはそのプライマリチャンネルとの干渉を防ぐ最適なチャンネルに設定されます。</li> </ul>
ショートガード間隔を有効にする	サポートされている場合、これを有効にすると送信/受信速度が向上します。802.11ac/n モードにのみ適用されます。
凝集 (アグリゲーション) を有効にする	802.11n フレーム集約を有効にすることによって、複数のフレームを結合してオーバーヘッドを減らしスループットを向上させます。802.11ac/n モードにのみ適用されます。
WDS AP を有効にする	WDS クライアントがこのアクセスポイントに接続できるようにします。
SSID	既定値は、sonicwall- に BSSID の最後の 4 文字を付加したもの (例: sonicwall-C587) になります。SSID は、32 文字以内の任意の英数字に変更できます。

- ① **ヒント:** 「ショートガード間隔を有効にする」オプションと「凝集 (アグリゲーション) を有効にする」オプションを選択すると、スループットを若干向上させることができます。どちらも、信号強度が高く干渉がほとんどない最適なネットワーク条件において、最も効果的です。最適とは言えない条件下 (干渉がある、信号強度が低いなど) のネットワークでは、これらのオプションが原因で伝送エラーが発生することがあるので、スループット向上効果は得られません。

## 802.11a/b/g の無線設定

「無線モード」フィールドが 802.11a のみ、802.11g/b 混在、802.11a のみ、または 802.11g のみに構成された場合、以下のオプションの設定が表示されます。

チャンネル	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。このオプションは既定の設定です。オプションで、規制地域内の単一のチャンネルを選択することもできます。
WDS AP を有効にする	WDS クライアントがこのアクセスポイントに接続できるようにします。
SSID	既定値は、sonicwall- に BSSID の最後の 4 文字を付加したもの (例: sonicwall-C587) になります。SSID は、32 文字以内の任意の英数字に変更できます。

## 802.11ac の無線設定

802.11ac のみに無線通信機を構成すると、次のオプションが表示されます。

- 無線帯域ドロップダウンメニュー - 広域 - 80 MHz チャンネルのサポートを許容する、802.11ac 無線の帯域を設定します。
- 「チャンネル」ドロップダウンメニュー - チャンネルを選択します。
  - 「自動」- 無線セキュリティ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。「自動」は既定のチャンネル設定であり、この設定では、選択されている動作中のチャンネルが右側に表示されます。これ以外に、規制地域内のチャンネルを明示的に定義することもできます。
  - 特定のチャンネル。

## 無線仮想アクセスポイント

無線仮想アクセスポイントを使用する場合、「無線仮想アクセスポイント」セクションのドロップダウンメニューから「仮想アクセスポイントグループ」を選択してください。または、定義済の VAP グループを選択することもできます。

すべてのアクセスポイント設定が終了したら、「適用」を選択して設定を保存します。

## 無線 WDS ステーション

無線装置は、別の SonicWall 無線デバイスまたは SonicPoint アクセスポイントにインターネット/ネットワークアクセスを提供します。「無線 WDS ステーション」モードを「無線の役割」として選択すると、物理的に離れている場所の間で、長くてコストのかかるイーサネットケーブル接続を必要とすることなく、保護されたネットワーク通信ができるようになります。

- ① **補足:** 無線仮想アクセスポイントの使用中は、装置を無線 WDS ステーションとして使用することはできません。

## 無線の設定

1. 「デバイス > 内部無線 > 設定」に移動します。
2. 「無線の役割」フィールドで、「無線 WDS ステーション」をドロップダウンメニューから選択します。

The screenshot shows the 'Wireless Mode' configuration page. At the top, 'Wireless Role' is set to 'Wireless WDS Station'. Below that, 'Wireless Interface as WAN' is disabled. The 'Wireless Setup' section includes: 'WLAN Enable' (checked), 'SSID' (sonicwall-593C), 'Wireless Mode' (2.4GHz 802.11n/g/b Mixed), 'Short Guard Interval Enable' (checked), 'Aggregation Enable' (checked), and 'Wireless Client Connectivity Enable' (unchecked). A 'ping First Remote IP' field is set to 0.0.0.0. The 'Wireless Tuning' section includes: 'Use Antenna' (External), 'Transmit Power' (Maximum), 'Fragmentation Size (Bytes)' (2346), and 'RTS Threshold (Bytes)' (2346). Buttons for 'Cancel', 'Apply', and 'Restore Defaults' are at the bottom.

3. 「WAN としての無線インターフェース」オプションをオンにして、無線インターフェースを WAN として使用します。既定値は無効です。
4. 「無線の設定」セクションで、「WLAN を有効にする」オプションをオンにして有効にします。無線 WDS ステーションモードでは、無線が有効になるとアクセスポイントではなくクライアントとして動作し、クライアントに対する無線アクセスは提供しません。WLAN 無線は既定では無効になっています。
5. 以下のオプションを選択します。

SSID	既定値は、sonicwall- に BSSID の最後の 4 文字を付加したものの (例: sonicwall-C587) になります。SSID は、32 文字以内の任意の英数字に変更できます。
ショートガード間隔を有効にする	サポートされている場合、これを有効にすると送信/受信速度が向上します。802.11ac/n モードにのみ適用されます。
凝集 (アグリゲーション) を有効にする	802.11n フレーム集約を有効にすることによって、複数のフレームを結合してオーバーヘッドを減らしスループットを向上させます。802.11ac/n モードにのみ適用されます。
無線クライアント接続性確認と自動再接続を有効にする	定期的に、ユーザが定義した IP アドレスに ping を行うことで無線クライアント接続性を確認します。接続が失われている場合、自動再接続を実行します。
ping 先リモート IP	前に接続性確認を有効にしていた場合、ping を実行する先のリモート IP アドレスを入力します。 ① <b>重要:</b> 指定した IP アドレスが ping を返すことを確認してください。

## 無線に関する詳細設定

無線に関する詳細設定を行うには、以下の手順に従います:

1. 「使用するアンテナ」を設定します。既定値は**最良**です。
2. ドロップダウンメニューから、「電波出力」を選択します。
  - 「最大出力」は、最も強い信号を WLAN に送信します。例えば、建物間で信号を送信する場合は、「最大出力」を選択します。
  - 「1/2 出力 (-3 dB)」は、同じビル内のオフィス間に推奨されます。
  - 「1/4 出力 (-6 dB)」は、短距離の通信に推奨されます。
  - 「1/8 出力 (-9 dB)」は、比較的短距離の通信に推奨されます。
  - 「最小」は、非常に短い距離の通信に推奨されます。
3. 「断片化のしきい値 (バイト)」を指定します。最小値は **256**、最大値は **2346** です。既定値は最大値です。
4. 「RTS しきい値 (バイト)」を設定します。最小値は **1** で、最大値は **2346** です。既定値は最大値です。
5. 「適用」を選択して設定を保存します。  
① | **補足:** 「既定の設定への復元」をクリックすると、工場出荷時の既定の設定に戻すことができます。

## アクセスポイントおよび WDS ステーション

802.11 プロトコルを通じて 2 つ以上のホストが接続される場合で、接続を確立するには距離が遠すぎる場合、無線リピータがその間をブリッジします。

SonicWall 無線セキュリティ装置には、アクセスポイントモードとブリッジモードがあります。「アクセスポイントおよび WDS ステーション」モードで動作中は、1 つの仮想アクセスポイントがステーションとして作成されて、別のアクセスポイントに接続できます。他の仮想アクセスポイントは通常のアクセスポイントとして動作します。つまり、装置を「アクセスポイントおよび WDS ステーション」に構成すると、リピーターモードで動作します。このモードでは、仮想アクセスポイントが WAN インターフェースとして使用する仮想インターフェースを設定することもできます。

**無線モード**

無線の役割 アクセス ポイントとステーション ⓘ

**無線設定**

① ユーザは、該当する地域の電波を管轄する関係団体または機関により発布されているすべての法令及び規制項目を遵守する責任を求められます。

WLAN を有効にする  ⓘ

スケジュール 常に有効

規制地域 MKK - Japan

国コード Japan-JP

無線モード 2.4GHz 802.11n/g/b 混在

WDS AP を有効にする  ⓘ

SSID sonicwall-593C

**無線仮想アクセス ポイント**

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-- ⓘ

**ステーション設定**

ステーションモードを有効にする

AP SSID

AP 認証種別 オープン

事前共有鍵

VLAN ID VLAN ID の選択

無線インターフェースを WAN として使用する

キャンセル
適用

## アクセス ポイント および WDS ステーションの無線設定

① **重要:** 無線装置をアクセス ポイントとステーションとして設定する場合、無線運用者は、該当する地域の電波を管轄する関係団体または機関により発布されているすべての法令や規制を遵守する責任を負います。

1. 「デバイス > 内部無線 > 設定」に移動します。
2. 「無線の役割」フィールドで、「アクセス ポイントとステーション」をドロップダウン メニューから選択します。
3. 「WLAN を有効にする」をオンにして有効にします。これによって、モバイル ユーザにクリーンな無線アクセスを提供できます。WLAN 無線は既定では有効になっています。
4. 「スケジュール」フィールドで、ドロップダウン メニューから WLAN 無線をアクティブにする時間を選択します。「スケジュール」リストには、システムが提供するオプションに加えて、「オブジェクト > 一致オブジェクト > スケジュール」ページで作成および管理するスケジュール オブジェクトが表示されます。既定値は「常に有効」です。
5. 「国コード」フィールドには、アクセス ポイントが使用される国を選択してください。国コードは、どの規制地域の管轄で無線を利用するかを決定します。
6. 「無線モード」フィールドには、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。
7. 「WDS AP を有効にする」オプションをオンにして有効にします。WDS クライアントがこのアクセス ポイントに接続できるようにします。
8. 「SSID」フィールドが正しく入力されているか確認してください。既定値は、sonicwall- に BSSID の最後の 4 文字を付加したもの (例: sonicwall-C587) になります。SSID は、32 文字以内の任意の英数字に変更できます。
9. 「適用」を選択して設定を保存します。

## 無線仮想アクセスポイント

無線仮想アクセスポイントを使用する場合、「無線仮想アクセスポイント」セクションのドロップダウンメニューから「仮想アクセスポイントグループ」を選択してください。または、定義済の VAP グループを選択することもできます。

すべてのアクセスポイント設定が終了したら、「適用」を選択して設定を保存します。

## ステーション設定

ステーション設定を構成するには、以下の手順に従います：

1. 「ステーションモードを有効にする」をオンにして有効にします。
2. 表示されるフィールドに **AP SSID** を入力します。
3. ドロップダウンメニューから「**AP 認証種別**」を選択します。以下から選択します。
  - オープン
  - WPA2 - 自動 - PSK
  - WPA3 - PSK
4. **事前共有鍵**を入力します。
5. ドロップダウンメニューから「**VLAN ID**」を選択します。
6. 「無線インターフェースを WAN として使用する」をオンにして有効にします。
7. 「**適用**」を選択して設定を保存します。

## セキュリティ

「デバイス > 内部無線 > セキュリティ」ページでは、無線装置の認証と暗号化設定を構成します。選択した認証の種別に応じて、異なるオプションが表示されます。

### トピック:

- [認証について](#)
- [WEP 設定の構成](#)
- [WPA3/WPA2/WPA PSK 設定の構成](#)
- [WPA3/WPA2/WPA EAP 設定の構成](#)

## 認証について

認証種別は以下のテーブルで説明されています。

### 認証種別

種別	機能と用途
WEP (Wired Equivalent Protocol)	<ul style="list-style-type: none"> <li>• データを無線ネットワーク経由で保護します。</li> <li>• SonicWall 装置を通過後には保護はありません。</li> <li>• 伝送するデータに対して最小限の保護を提供します。</li> <li>• 暗号化に静的な鍵を使用します。</li> <li>• 旧式のデバイス、PDA、無線プリンタで有用です。</li> <li>• 高い水準のセキュリティが必要な配備には推奨できません。</li> </ul>
WPA (Wi-Fi Protected Access)	<ul style="list-style-type: none"> <li>• 高いセキュリティ (TKIP を使用)</li> <li>• 信頼性の高い企業の無線クライアントで使用</li> <li>• Windows ログインを使用したトランスペアレントな認証</li> <li>• 一般にクライアントソフトウェアは不要</li> <li>• RADIUS などのユーザを認証する認証プロトコルが別途で必要です。</li> <li>• 動的鍵を使用します。</li> </ul> <p>① <b>補足:</b> このオプションは、内部設定ページで有効にした場合にのみ表示されます。</p>
WPA2 (Wi-Fi Protected Access, v2)	<ul style="list-style-type: none"> <li>• 最高のセキュリティ (AES を使用)</li> <li>• 信頼性の高い企業の無線クライアントで使用</li> </ul>

種別	機能と用途
	<ul style="list-style-type: none"> <li>• Windows ログインを使用したトランスペアレントな認証</li> <li>• 場合によってクライアントソフトウェアをインストールする必要があります。</li> <li>• 802.11i WPA/WPA2 EAP 認証モードをサポートします。</li> <li>• 最初のログイン後のバックエンド認証はなし（より高速なローミングが可能）</li> <li>• 鍵の保存と生成に関して2つのプロトコルをサポートします。PSK（事前共有鍵）拡張認証プロトコル（EAP）です。</li> </ul> <p>① <b>補足:</b> EAP のサポートは、アクセスポイントモード（「デバイス &gt; 内部無線 &gt; 設定」ページで選択）においてのみ使用できます。ブリッジモードでは使用できません。</p>
WPA2-自動	<ul style="list-style-type: none"> <li>• WPA2 セキュリティを使用して接続を試みます。</li> <li>• 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。</li> </ul>
WPA3	<ul style="list-style-type: none"> <li>• WPA3 は、個人および企業ネットワーク用 WPA3 セキュリティ規格です。</li> <li>• モデム セキュリティアルゴリズムとより強固な暗号スイートを使用して、Wi-Fi セキュリティを向上します。</li> <li>• 鍵の保存と生成に関して、PSK（事前共有鍵）、EAP（拡張認証プロトコル）、OWE（Opportunistic Wireless Encryption）をサポートします。</li> </ul>
WPA3/WPA2	<ul style="list-style-type: none"> <li>• WPA3 セキュリティを使用して接続を試みます。</li> <li>• クライアントが WPA3 に対応していない場合、接続は既定で WPA2 に設定されます。</li> </ul>
WPA3-EAP-192B	<ul style="list-style-type: none"> <li>• WPA3-Enterprise によって提供される 192 ビット セキュリティモードは、適切な組み合わせの暗号化ツールが使用され、WPA3 ネットワーク内で整合性のあるセキュリティ基準を設定することを確実にします。</li> <li>• 拡張認証プロトコル（EAP）を使用します。</li> </ul>

# WEP 設定の構成

認証種別として WEP オプションの 1 つが選択されている場合、以下のオプションを設定できます。

暗号化モード

認証種別 WEP - 両方 (オープンシステムと共有鍵)

WEP 暗号化設定

既定の鍵 第 1 鍵

鍵登録  英数字  16 進数字 (0 ~ 9、A ~ F)

第 1 鍵 [ ] なし ⓘ

第 2 鍵 [ ] なし ⓘ

第 3 鍵 [ ] なし ⓘ

第 4 鍵 [ ] なし ⓘ

キャンセル 適用

無線装置に WEP 認証を構成するには、以下の手順に従います：

1. 「デバイス > 内部無線 > セキュリティ」ページに移動します。
2. 「認証種別」ドロップダウンメニューで、適切な認証種別を選択します。
  - **WEP - 両方 (オープンシステムおよび共有鍵)** (既定): 各フィールドで同一の鍵を使用している場合、「既定の鍵」の割り当ては重要ではありません。
  - **オープン**: オープンシステム認証では、ファイアウォールは ID を検証せずに無線クライアントのアクセスを許可します。すべての Web 暗号化設定は、グレー表示されて選択できません。
  - **「WEP - 共有鍵」**: WEP を使用し、認証を許可する前に無線クライアントに共有鍵が配布されている必要があります。「共有鍵」を選択した場合は、「既定の鍵」の割り当てが重要です。
3. 「既定の鍵」ドロップダウンメニューで、既定にする鍵として、「第 1 鍵」、「第 2 鍵」、「第 3 鍵」、または「第 4 鍵」を選択します。
4. 「鍵登録」オプションで、鍵が「英数字」か「16 進数字(0-9, A-F)」かを選択します。
5. 鍵は、指定されたフィールドに 4 つまで入力できます。各鍵について、**64 ビット**、**128 ビット**、**152 ビット**のいずれかを選択します。ビット数が多いほど、鍵は安全になります。個々の種別の鍵について、何文字が必要かについては以下のテーブルを参照してください。

## 鍵種別

鍵種別	WEP - 64 ビット	WEP - 128 ビット	WEP - 152 ビット
英数字	5 文字	13 文字	16 文字
16 進数字 (0 ~ 9、A ~ F)	10 文字	26 文字	32 文字

6. 「適用」を選択します。

# WPA3/WPA2/WPA PSK 設定の構成

認証種別として WPA PSK オプションの 1 つが選択されている場合、以下のオプションを設定できます。

暗号化モード

認証種別 WPA2-PSK

EAPOL 設定

EAPOL バージョン V2

WPA3/WPA2/WPA 設定

暗号化種別 AES

グループ鍵の更新 無効

事前共有鍵 (PSK) 設定

パスワード パスワードの入力...

キャンセル 適用

無線装置に設定済の共通鍵を使用する WPA 認証を構成するには、以下の手順に従います：

1. 「デバイス > 内部無線 > セキュリティ」ページに移動します。
2. 「認証種別」ドロップダウンメニューで、適切な認証種別を選択します。
  - **WPA2-PSK**: WPA2 と設定済認証鍵を使用して接続します。
  - **WPA2-自動-PSK**: 自動的に WPA2 と設定済認証鍵を使用しての接続を試行し、クライアントが WPA2 に対応していない場合には WPA にフォールバックします。
  - **WPA3-PSK**: WPA3 と設定済認証鍵を使用して接続します。
  - **WPA3/WPA2-PSK**: 自動的に WPA3 と設定済認証鍵を使用しての接続を試行し、クライアントが WPA3 に対応していない場合には WPA2 にフォールバックします。
3. 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 (既定)** - バージョン 2 を選択します。バージョン 1 よりセキュリティは強化されますが、無線クライアントによってはサポートしていない場合があります。
  - **V1** - バージョン 1 を選択します。
4. 「WPA3/WPA2/WPA 設定」セクションで、以下の設定を指定してください。
  - **暗号化種別** - TKIP を選択します。*Temporal Key Integrity Protocol (TKIP)* は、パケット単位で鍵の整合性を適用するためのプロトコルです。ただし、安全性は比較的 low、スループットも下がります。AES と自動も暗号化種別のオプションです。
  - **グループ鍵の更新** - SonicWall セキュリティ装置が鍵をいつ更新するかを指定します。秒数で指定した間隔の後で新しいグループ鍵を生成するには、「**タイムアウトごと**」を選択します。これが既定です。静的鍵を使用する場合は「**無効**」を選択します。
  - **間隔** - 「**グループ鍵の更新**」フィールドで「**タイムアウトごと**」を選択した場合は、WPA が新しいグループ鍵を自動的に生成するまでの秒数を入力します。既定値は **86400** 秒です。「**グループ鍵の更新**」で「**無効**」を選択した場合は、このオプションは表示されません。
5. 「**パスフレーズ**」フィールドに、鍵の生成に使用するパスフレーズを入力します。
6. 「**適用**」をクリックして設定を保存して適用します。

# WPA3/WPA2/WPA EAP 設定の構成

認証種別として WPA EAP オプションの 1 つが選択されている場合、以下のオプションを設定できます。

暗号化モード	認証種別	WPA2 - EAP
EAPOL 設定	EAPOL バージョン	V2 ⓘ
WPA3/WPA2/WPA 設定	暗号化種別	AES
	グループ鍵の更新	無効
拡張認証プロトコル (EAP)	RADIUS サーバ再試行回数	4
	再試行間隔 (秒)	0
	RADIUS サーバ 1 IP	ⓘ
	ポート	1812 ⓘ
	RADIUS サーバ 1 パスワード	ⓘ
	RADIUS サーバ 2 IP	ⓘ
	ポート	1812 ⓘ
	RADIUS サーバ 2 パスワード	ⓘ
	キャンセル	適用

無線装置に WPA 認証を構成するには、以下の手順に従います

- 「デバイス > 内部無線 > セキュリティ」ページに移動します。
- 「認証種別」ドロップダウンメニューで、適切な認証種別を選択します。
  - WPA2 - EAP: WPA2 および拡張認証プロトコル (EAP) を使用して接続します。
  - WPA2 - 自動 - EAP: 自動的に WPA2 と拡張認証プロトコルを使用しての接続を試行し、クライアントが WPA2 に対応していない場合には WPA にフォールバックします。
  - WPA3 - EAP: WPA3 および拡張認証プロトコル (EAP) を使用して接続します。
  - WPA3/WPA2 - EAP: 自動的に WPA3 と設定済認証鍵を使用しての接続を試行し、クライアントが WPA3 に対応していない場合には WPA2 にフォールバックします。

① **補足:** EAP は、アクセスポイントモードにおいてのみサポートされています。クライアントブリッジモードではサポートされません。
- 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。
  - 「V1」: LAN バージョン 1 経由の拡張認証プロトコルを選択します。
  - 「V2」: LAN バージョン 2 経由の拡張認証プロトコルを選択します。バージョン 1 よりセキュリティは強化されますが、無線クライアントによってはサポートしていない場合があります。

4. 「WPA3/WPA2/WPA 設定」セクションで、以下の設定を指定してください。

- **暗号化種別** – TKIP を選択します。Temporal Key Integrity Protocol (TKIP) は、パケット単位で鍵の整合性を適用するためのプロトコルです。ただし、安全性は比較的 low、スループットも下がります。AES と自動暗号化種別のオプションです。
- **グループ鍵の更新** – SonicWall セキュリティ装置が鍵をいつ更新するかを指定します。秒数で指定した間隔の後で新しいグループ鍵を生成するには、「**タイムアウトごと**」を選択します。これが既定です。静的鍵を使用する場合は「**無効**」を選択します。
- **間隔** – 「**グループ鍵の更新**」フィールドで「**タイムアウトごと**」を選択した場合は、WPA が新しいグループ鍵を自動的に生成するまでの秒数を入力します。既定値は **86400** 秒です。「**グループ鍵の更新**」で「**無効**」を選択した場合は、このオプションは表示されません。

5. **拡張認証プロトコル (EAP) の設定** セクションでは、以下の設定を指定してください。

- 「**RADIUS サーバ再試行回数**」: サーバによる認証の試行回数を入力します。既定値は 4 です。
- 「**再試行間隔 (秒)**」: サーバが次の再試行まで待つ時間を入力します。既定値は 0 (間隔を置かない) です。
- **RADIUS サーバ 1 IP とポート**: プライマリ RADIUS サーバの IP アドレスとポート番号を入力します。
- **RADIUS サーバ 1 パスワード**: Radius サーバにアクセスするためのパスワードを入力します。
- **RADIUS サーバ 2 IP とポート**: セカンダリ RADIUS サーバがある場合は、その IP アドレスとポート番号を入力します。
- **RADIUS サーバ 2 パスワード**: Radius サーバにアクセスするためのパスワードを入力します。

6. 「**適用**」をクリックして WPA3/WPA2 EAP 設定を適用します。

## 詳細

詳細設定では、無線装置のための広範囲な機能をカスタマイズできます。このページは、ファイアウォールがアクセスポイントとして動作している場合にのみ使用できます。

**ビーコンと SSID 制御**

ビーコンに SSID を載せない

ビーコン間隔 (ミリ秒)

**グリーン アクセス ポイント**

グリーン AP を有効にする  ⓘ

グリーン AP タイムアウト

**無線詳細設定**

<p>Short Slot Time を有効にする <input type="checkbox"/></p> <p>受信に使用するアンテナ <input type="text" value="最良"/></p> <p>電波出力 <input type="text" value="最大出力"/></p> <p>プリアンプル長 <input type="text" value="長い"/></p> <p>断片化のしきい値 (バイト) <input type="text" value="2346"/></p> <p>RTS しきい値 (バイト) <input type="text" value="2346"/> ⓘ</p> <p>DTIM 間隔 <input type="text" value="1"/></p>	<p>参加タイムアウト (秒) <input type="text" value="300"/></p> <p>クライアント最大参加数 <input type="text" value="128"/></p> <p>データ速度 <input type="text" value="最良"/></p> <p>保護モード <input type="text" value="自動"/></p> <p>保護速度 <input type="text" value="11 Mbps"/></p> <p>保護種別 <input type="text" value="CTS のみ"/></p>
--	---

既定の設定への復元

### トピック:

- [ビーコンと SSID の制御](#)
- [グリーン アクセス ポイント](#)
- [無線に関する詳細設定](#)
- [設定可能な使用するアンテナ](#)

# ビーコンとSSIDの制御

ビーコンとSSID制御

ビーコンにSSIDを載せない

ビーコン間隔 (ミリ秒)

ビーコンとSSIDの制御を構成するには、以下の手順に従います:

1. 「デバイス > 内部無線 > 詳細」ページに移動します。
2. 「ビーコンにSSIDを載せない」オプションをオンにします。これにより、SSID名のブロードキャストを抑制し、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、許可されていない無線クライアントによってその無線SSIDが認識されるのを防ぐことができます。この設定は既定で無効になっています。
3. 「ビーコン間隔」の値をミリ秒単位で入力します。間隔を短くすると、ビーコンフレームがネットワークを無線接続にいつそう頻繁に通知するので、パッシブスキャンの信頼性と速度が向上します。既定の間隔は200ミリ秒です。
4. 「適用」をクリックして変更を適用します。「既定の設定への復元」をクリックすると、工場出荷時の既定の設定に戻ります。

# グリーンアクセスポイント

グリーンアクセスポイント

グリーンAPを有効にする  ⓘ

グリーンAPタイムアウト

電力効率を構成するには、以下の手順に従います:

1. 電力効率を高めるには、「グリーンAPを有効にする」オプションを選択します。この設定はデフォルトで無効になっています。
2. 「グリーンAPタイムアウト」フィールドにタイムアウト時間を指定します。既定値は200です。
3. 「適用」をクリックして変更を適用します。「既定の設定への復元」をクリックすると、工場出荷時の既定の設定に戻ります。

# 無線に関する詳細設定

無線詳細設定	
Short Slot Time を有効にする	<input type="checkbox"/>
受信に使用するアンテナ	最良
電波出力	最大出力
プリアンブル長	長い
断片化のしきい値 (バイト)	2346
RTS しきい値 (バイト)	2346
DTIM 間隔	1
参加タイムアウト (秒)	300
クライアント最大参加数	128
データ速度	最良
保護モード	自動
保護速度	11 Mbps
保護種別	CTS のみ

無線に関する詳細設定を構成するには、以下の手順に従います

- 「Short Slot Time を有効にする」オプションをオンにして、802.11g トラフィックのみを利用する場合のパフォーマンスを高めま。802.11b は Short Slot Time に対応していません。この設定はデフォルトで無効になっています。
- 「受信に使用するアンテナ」ドロップダウン メニューから、無線セキュリティ装置がデータの送受信に使用するアンテナを選択します。アンテナ選択のより詳細については、「[設定可能な使用するアンテナ](#)」を参照してください。既定は「最良」です。
- 「電波出力」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。
  - 「最大出力」は、最も強い信号を WLAN に送信します。例えば、建物間で信号を送信する場合は、「最大出力」を選択します。
  - 「1/2 出力 (-3 dB)」は、同じビル内のオフィス間に推奨されます。
  - 「1/4 出力 (-6 dB)」は、比較的短距離の通信に推奨されます。
  - 「1/8 出力 (-9 dB)」は、比較的短距離の通信に推奨されます。
  - 「最小」は、非常に短い距離の通信に推奨されます。
- 「プリアンブル長」ドロップダウン メニューから、「短い」または「長い」を選択します。無線ネットワークでの効率化とスループット向上のため、「短い」をお勧めします。既定は「長い」です。
- 「断片化のしきい値 (バイト)」を指定します。最小値は 256、最大値は 2346、既定値は **2346** です。  
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。この値を大きくすると、フレームが配信されるときオーバーヘッドは小さくなりますが、失われたり壊れたりしたフレームは破棄して再送信する必要があります。
- RTS しきい値 (バイト) を、RTS に対して送信するよう指定します。最小値は 1、最大値は 2347、既定値は **2346** です。  
このフィールドには、パケット送信の前に送信する RTS のパケットサイズのしきい値をバイト単位で設定します。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。ネットワークのスループットが低い場合、または再送信されるフレームの数が多い場合は、RTS しきい値を小さくして RTS クリーニングを有効にします。
- DTIM (Delivery of Traffic Indication Message) 間隔を、「DTIM 間隔」フィールドで指定します。最小値は 1、最大値は 256、既定値は 1 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 を送信する前に待つビーコンフレーム数を指定します。DTIM 間隔の値を大きくすると、電力をいっそう効果的に節約できます。

8. クライアント参加の秒数を、「**参加タイムアウト(秒)**」フィールドに入力します。既定値は **300** 秒で、設定可能な範囲は 60～36000 秒です。ネットワークが非常にビジーの場合、このフィールドの秒数を増やすことによって、タイムアウトを長くできます。
9. このプロファイルを使用する SonicPoint ごとに「**クライアント最大参加数**」を入力します。最小値は 1、最大値は 128、既定値は **128** です。この設定によって、同時に無線接続できるステーションの数が制限されます。
10. 「**データ転送**」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**」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。あるいは、**1 Mbps ~ 54 Mbps** の転送速度を手動で選択することができます。
11. 「**保護モード**」ドロップダウンメニューから、保護モードを選択します。「**なし**」、「**常に**」、「**自動**」のいずれかを選択します。

保護により競合を減らすことができます。特に、2 つの SonicPoint が重複している場合に有効です。ただし、パフォーマンスが低下する場合があります。通常は、「**自動**」が最善の設定です。SonicPoint が重複している場合にのみ有効になるためです。
12. 「**保護速度**」をドロップダウンメニューから選択します。「**1 Mbps**」、「**2 Mbps**」、「**5 Mbps**」、または「**11 Mbps**」を選択します。保護速度は、保護モードが有効になっているときの転送速度です。速度が遅いほど保護レベルは高くなりますが、データ伝送速度は遅くなります。
13. 「**保護種別**」ドロップダウンメニューから、無線接続の確立に使用されるハンドシェイクの種類として、「**CTS のみ**」(既定)または「**RTS と CTS**」を選択します。

① | **補足:** 802.11b トラフィックと互換性があるのは **CTS** だけです。
14. 「**適用**」をクリックして変更を適用します。「**既定の設定への復元**」をクリックすると、工場出荷時の既定の設定に戻ります。

## 設定可能な使用するアンテナ

無線 SonicWall セキュリティ装置には、ダイバーシティモードで動作する 5 dBi のデュアル アンテナが採用されています。ダイバーシティモードの既定の実装では、1 つのアンテナが送信用に使用され、両方のアンテナが受信アンテナとして使用できるようになっています。セキュリティ保護された無線装置の両方のアンテナに無線信号が届くと、信号の強度と整合性が評価された後、受信した中で最善の信号が使用されます。2 つのアンテナの選択処理は動作中は一定であり、常に可能な限り最善の信号が提供されます。外部の (ゲインが高く単一指向性の) アンテナを使用できるよう、使用するアンテナの設定は無効にできます。

SonicWall NSA 220 および 250M 無線セキュリティ装置では、3 つのアンテナが使用されます。「使用するアンテナ」は既定で「**最良**」に設定されており、これらの装置ではこの設定のみを使用できます。

「**受信に使用するアンテナ**」の設定は、無線セキュリティ装置がデータの送受信に使用するアンテナを決定します。規定値の設定は**最良**です。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無線セキュリティ装置によって自動的に選択されます。

## MAC フィルタ リスト

無線ネットワークにより、無線セキュリティ装置に対する無線クライアントの認証や参加を防ぐ、ネイティブな MAC フィルタ機能が提供されます。WLAN 上で MAC フィルタを強制すると、無線クライアントは無線ネットワークカードの MAC アドレスを提出しなければなりません。SonicOS 無線 MAC フィルタリストにより、あなたの無線ネットワークへのアクセスを許可または拒否をするクライアントのリストを構成できます。MAC フィルタリング無しでは、無線ネットワークに入るための SSID および、その他のセキュリティパラメータを知っていれば、どのような無線クライアントでも無線ネットワークに「押し入る」ことができます。

以下に、一般的な 284 MAC フィルタリストの配備シナリオを示します。



# 展開に関する考慮事項

MAC フィルタ リストを展開する場合は、以下を考慮します。

- SonicPoint-N 装置の場合、この機能ではゲートウェイが MAC フィルタ リスト設定を保存する必要があります。
- SonicWall TZ シリーズ装置の内部無線の場合、MAC フィルタ リスト設定を保存するために VAP 構造にいくつかメンバーを追加する必要があります、また、ドライバに構成を設定するために機能全体を修正する必要があります。
- 仮想アクセス ポイントは独自の MAC フィルタを構成することもできますし、「デバイス > 内部無線 > MAC フィルタ リスト」ページで構成されたグローバル設定を継承することもできます。

## MAC フィルタ リストの設定

MAC フィルタ リストを構成するには、以下の手順に従います：

1. 「デバイス > 内部無線 > MAC フィルタ リスト」ページに移動します。
2. 「MAC フィルタ リストを有効にする」をクリックします。この設定はデフォルトで無効になっています。
3. 「許可リスト」ドロップダウン メニューから、許可したいアドレス グループを選択します。「すべての MAC アドレス」（既定）、「既定 ACL 許可グループ」、または個別に作成したグループです。
4. 「拒否リスト」ドロップダウン メニューから、拒否したいアドレス グループを選択します。MAC アドレスなし（既定）、既定 ACL 拒否グループ、または個別に作成したグループです。
5. 許可または拒否リストに新しいアドレス オブジェクトを追加するには、「許可リスト」または「拒否リスト」いずれかのドロップダウン メニューから「MAC アドレス オブジェクト グループの作成...」を選択します。



- a. 「名前:」テキスト フィールドに、新しいグループの名前を入力します。
  - b. 左側の列で、許可または拒否するグループあるいは個別のアドレス オブジェクトを選択します。Ctrl キーを押しながらクリックすると、一度に複数の項目を選択できます。
  - c. 右矢印をクリックして、項目をグループに追加します。
  - d. 「保存」をクリックします。アドレスが、ドロップダウン メニューの選択肢として表示されます。
6. 「適用」を選択します。

## IDS

無線侵入検知サービス (IDS) を使用すると、SonicWall 無線セキュリティ装置のセキュリティ機能が大幅に向上します。一般的な不正無線アクティビティの大半を認識し、対応策を講じることもできます。無線 IDS は、次の 3 つの種類のサービスで構成されています。

- シーケンス番号分析
- アソシエーションフラッド検出
- 悪意のあるアクセスポイントの検出

## アクセスポイントのIDS

無線セキュリティ装置の「無線の役割」が「アクセスポイント」モードに設定されていると、3種類の WIDS サービスをすべて使用できますが、悪意のあるアクセスポイント検出は既定によりパッシブモードで機能します（選択されている動作チャンネルのみで他のアクセスポイントビーコンのフレームをパッシブにリッスンします）。「スキャン」を選択すると、「無線の役割」が即座に変更されて無線セキュリティ装置はアクティブスキャンを実行できるようになり、関連する無線クライアントに対する接続がしばらく失われることがあります。「アクセスポイント」モードの間は、アクティブに関連付けられているクライアントがない場合、またはクライアントの接続が中断する可能性があっても問題ない場合にも、「スキャン」機能を使用する必要があります。

## 悪意のあるアクセスポイント

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）アクセスポイントの導入を許す環境が形作られています。具体的には、悪意のあるデバイスへの無意識的な接続や、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、多種多様な脅威が生み出されています。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。

セキュリティ装置は、ネットワークへのアクセスを試みる可能性のある、悪意のあるアクセスポイントを認識することによって、この脆弱性を緩和できます。そのためには、802.11a、802.11g、802.11n チャンネルすべてでのアクセスポイントのアクティブスキャンと、単一の動作チャンネルでのビーコンアクセスポイントの（アクセスポイントモードでの）パッシブスキャンという2つの方法が使用されます。

# IDS の設定

IDS スキャンの実行をスケジュールするには、「IDS スキャンを予定する」ドロップダウンメニューから、スケジュールを選択または作成します。

- 無効 – これは既定です。選択するとIDS スキャンは行われません
- スケジュールの作成 – 「スケジュールの追加」ダイアログが表示され、このセクションで説明する個別のスケジュールを作成できます。
- 勤務時間
- 月-火-水-木-金 08:00 から 17:00
- 時間外
- 土-日 00:00 から 24:00
- 月-火-水-木-金 17:00 から 24:00
- 月-火-水-木-金 0:00 から 8:00
- 週末時間
- AppFlow 報告時間
- 日-月-火-水-木-金-土 00:00 から 24:00
- アプリケーション可視化報告時間
- TSR 報告時間
- 日-月-火-水-木-金-土 00:00 から 00:01
- クラウド バックアップ時間
- 日-月-火-水-木-金-土 02:00 から 03:00
- ゲスト サイクル クォータ更新
- 日-月-火-水-木-金-土 00:00 から 00:15

新しいスケジュールを追加するには、以下の手順に従います：

1. 「IDS スキャンを予定する」フィールドで、**新しいスケジュールの作成**を選択します。

2. 「スケジュール名」を入力します。
3. スケジュール種別で、次のいずれかを選択します。
  - 「1回」では、1 回だけのイベントをスケジュールします。「1回」セクションのフィールドだけが入力可能になります。
    - 「1回」セクションでは、ドロップダウンメニューを使用してIDS スキャンの開始と終了の時刻をスケジュールします。
  - 「繰り返し」では、繰り返しイベントをスケジュールします。「繰り返し」セクションのフィールドだけが入力可能になります。

- スキャンの「曜日」を選択します。
  - 24 時間形式で「開始時刻」を入力します。
  - 24 時間形式で「終了時刻」を入力します。
  - 「追加」をクリックして、これらのパラメータをスケジュール リストに追加します。
  - リストから項目を削除するには、反転表示させて削除アイコンをクリックします。すべて削除アイコンをクリックすると、スケジュール リストが消去されます。
- 「混在」では、混在イベントをスケジュールします。すべてのフィールドが入力可能になります。
4. 「保存」をクリックして、スケジュールをドロップダウン メニューに追加します。

## 検出されたアクセスポイント

アクティブ スキャンは、無線セキュリティ装置の起動時、およびテーブルの上部にある「スキャン」がクリックされるたびに実行されます。装置は環境をスキャンして、近辺にある他の無線デバイスを特定します。テーブルの上の「補足」には、検出されたアクセスポイント数と、最後のスキャンからの経過時間が、日数、時間数、分数、秒数で表示されます。

「検出されたアクセスポイント」テーブルのエントリを再表示するには、「更新」をクリックします。直ちにスキャンを実行するには、「スキャン」をクリックします。

① **重要:** アクセスポイント モードで動作している時に「スキャン」機能を使用すると、サービスがしばらく中断します。この中断は次のようなものです。

- 非永続的でステートレスなプロトコル (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。それが問題になる場合は、アクティブなクライアントがなくなるまで、または中断する可能性があってもかまわないときまで待ってから、「スキャン」を使用してください。

「検出されたアクセスポイント」の表には、すべての SonicPoint または個別の SonicPoint で検出できるすべてのアクセスポイントについての情報が表示されます。

フィールド	説明
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	アクセスポイントの無線 SSID です。
チャンネル	アクセスポイントで使用される無線チャンネルです。
認証	認証の種別です。
暗号	使用する暗号です。
ベンダー	アクセスポイントの製造元です。SonicPoint で示される製造元は SonicWall または Senao のどちらかです。
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。通常は 54 Mbps です。
許可	許可されたアクセスポイントのアドレス オブジェクト グループにアクセスポイントを追加するには、「許可」列の編集アイコンをクリックします。

## ネットワークでのアクセスポイントの許可

無線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、動作を許可できるものとして無線セキュリティ装置により識別されるまでは、Rogue (悪意の侵入者) とみなされます。アクセスポイントを承認するには、承認アイコンをクリックしてください。

# 仮想アクセスポイント

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。仮想アクセスポイントでは、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、単一の内部無線通信機に適用することができます。

VAP を使用する利点は、以下のとおりです。

- **無線チャンネルの節約** - チャンネルの競合を避けて単一の物理アクセスポイントをさまざまな目的に使用できるようにすることで、重複したインフラストラクチャの構築を防止します。空港などの公共スペースでは、複数のプロバイダが標準になりつつあります。空港内では、FAA ネットワーク、1 つ以上の航空会社ネットワーク、そして 1 つ以上の無線 ISP をサポートする必要があるかもしれません。けれども、米国とヨーロッパでは 802.11b ネットワークで 3 つの使用可能な (重複していない) チャンネルしかサポートできませんし、フランスと日本では 1 つのチャンネルしか使用できません。それらのチャンネルが既存のアクセスポイントで利用された後、追加のアクセスポイントはお互いに干渉し合い、パフォーマンスが落ちることになります。VAP は単一のネットワークを多様な目的に使用できるようにすることで、チャンネル数を節約します。
- **「無線 LAN インフラストラクチャの最適化」** - 重複したインフラストラクチャを構築せずに、複数のプロバイダの間で同じ無線 LAN インフラストラクチャを共有することにより、WLAN の設置と保守にかかる費用を引き下げます。

## トピック:

- [無線仮想 AP 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](#)
- [仮想アクセスポイントグループの有効化](#)

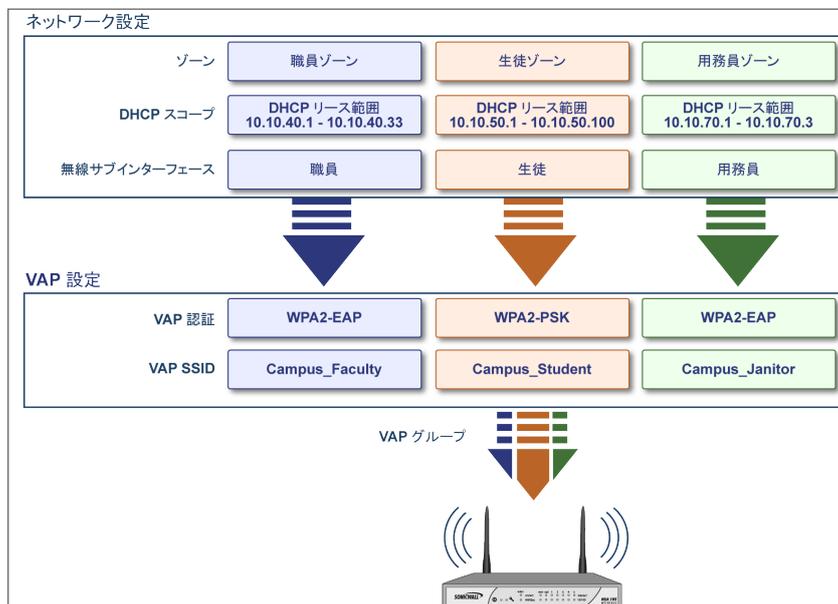
## 無線仮想 AP 設定タスクリスト

無線 VAP を配備するには、いくつかのステップから成る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、以下のステップの概要を説明します。

1. **ネットワークゾーン** - ネットワークゾーンは VAP 設定の重要部分です。作成した各ゾーンは、それぞれの個別的なセキュリティ設定とアクセス制御設定を持つことになります。複数のゾーンを作成し、無線サブネット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 セットアップガイド』の「オブジェクト > 一致オブジェクト > ゾーン」を参照してください。

2. **無線インターフェース - W0 インターフェース** (およびその WLAN サブネット) は SonicWall ネットワークセキュリティ装置と内部無線通信機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、それから無線通信機に転送されます。無線インターフェースの詳細については、『SonicOS システム セットアップガイド』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 対象の既定の範囲は、ほとんどのユーザーにとって必要以上に配備されます。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などです。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 セットアップガイド』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** - VAP 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** - VAP 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 および無線サブネット名が構成されます。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** - VAP グループ機能では、単一の内部無線通信機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。詳細については、「[仮想アクセスポイントグループ](#)」を参照してください。
7. **VAP グループを内部無線通信機に割り当てる** - VAP グループが内部ワイヤレス無線機に適用され、複数の SSID を通じてユーザが使用可能になります。詳細については、「[仮想アクセスポイントグループの有効化](#)」を参照してください。



# 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。VAP 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>内部無線>仮想アクセスポイント>仮想アクセスポイントプロファイル」で行います。プロファイル名を選択して編集アイコンを選択するか、「追加」をクリックして新しい仮想アクセスポイントプロファイルを作成します。設定の完了後、「適用」を選択します。

- ① **ヒント:** この機能は、複数の仮想アクセスポイントが同じ認証方法を共有する場合にすばやく設定を行ううえで特に便利です。

## 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](#)

## 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>内部無線>仮想アクセスポイント>仮想アクセスポイントプロファイル」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設定を行うには、以下の手順に従います:

1. 「デバイス>内部無線>仮想アクセスポイント>仮想アクセスポイントプロファイル」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. 「仮想アクセスポイントプロファイル設定」グループで、「無線種別」を設定します。既定では「無線内部通信」になります。VAP アクセスに内部無線機を使用する場合は、既定値のままにしてください。(これが現在サポートされてい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よいでしょう。
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
共有	WEP 暗号化認証設定では、共有鍵が使用されます。
両方	共有鍵が構成されていなければ、公開ネットワークと同じです。 共有鍵が構成されていれば、公開認証でデータトラフィックは暗号化されていることとなります。
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-自動-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。認証に事前共有鍵を使います。
WPA2-自動-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。
WPA3-OWE	WPA3 は、個人および企業ネットワーク用 WPA セキュリティ規格です。モデムセキュリティアルゴリズムとより強固な暗号スイートを使用して、Wi-Fi セキュリティを向上します。Opportunistic Wireless Encryption (OWE) を使用します。
WPA3-PSK	WPA3 は、個人および企業ネットワーク用 WPA セキュリティ規格です。モデムセキュリティアルゴリズムとより強固な暗号スイートを使用して、Wi-Fi セキュリティを向上します。認証に事前共有鍵を使います。
WPA3-EAP	WPA3 は、個人および企業ネットワーク用 WPA セキュリティ規格です。モデムセキュリティアルゴリズムとより強固な暗号スイートを使用して、Wi-Fi セキュリティを向上します。拡張認証プロトコル (EAP) を使用します。
WPA3/WPA2-PSK	WPA3 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 WPA3 に対応していない場合、接続は既定で WPA2 に設定されます。認証に事前共有鍵を使います。
WPA3/WPA2-EAP	WPA3 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 WPA3 に対応していない場合、接続は既定で WPA2 に設定されます。拡張認証プロトコル (EAP) を使用します。
WPA3-EAP-192B	WPA3-Enterprise によって提供される 192 ビットセキュリティモードは、適切

な組み合わせの暗号化ツールが使用され、WPA3 ネットワーク内で整合性のあるセキュリティ基準を設定することを確実にします。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。

6. 「最大クライアント数」フィールドには、この仮想アクセスポイントに対して許容される同時クライアント接続の最大数を選択します。
7. 「VAP WDS (Wireless Distribution System) を有効にする オプション」をオンにして有効にします。既定では、このオプションはオフになっています。
8. 「802.11b クライアントの接続を許可する」オプションをオンにして有効にします。既定では、このオプションはオフになっています。

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。

- 「両方」または「共有」を選択した場合の設定に関しては、「[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を選択した場合の設定に関しては、「[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) を使用するオプションを選択した場合の設定に関しては、「[WPA-EAP > WPA2-EAP 暗号化の設定](#)」を参照してください。

## WEP 暗号化の設定

仮想アクセスポイントプロファイルの作成時に「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」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。

## WPA-PSK > WPA2-PSK 暗号化の設定

仮想アクセスポイントプロファイルの作成時に、「認証種別」ドロップダウンメニューで、事前共有鍵が必要なオプション (WPA2-PSK または WPA2-自動-PSK) を選択した場合、「WPA/WPA2-PSK 暗号化設定」と呼ばれる設定が表示されます。

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。以下のフィールドに値を入力します。

フィールド名	説明
パスフレーズ	PSK ベースの認証で接続するときにユーザが入力する共有パスフレーズ
グループ鍵交換間隔	グループ鍵が有効な時間間隔。既定値は 86400 秒です。この値を小さく設定すると、接続の問題が生じる可能性があります。

## WPA-EAP > WPA2-EAP 暗号化の設定

仮想アクセスポイントプロファイルの作成時に、「認証種別」ドロップダウンメニューで、EAP が必要なオプション (WPA2-EAP または WPA2-自動-EAP) を選択した場合、「RADIUS サーバの設定」と呼ばれるセクションが表示さ

れます。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。

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。
グループ鍵交換間隔	WPA/WPA2 グループ鍵が更新される時間間隔 (秒数) を入力します。既定値は 86400 です。

## 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。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。

MAC フィルタリストの強制化を有効にする、以下の手順に従います:

1. 「**MAC フィルタリストを有効にする**」オプションをオンにして有効にします。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。
2. 「**グローバル ACL 設定を使用する**」オプションをオンにして有効にします。これによって、仮想アクセス ポイントに、SonicWall ネットワーク セキュリティ装置の既存の MAC フィルタリスト設定が関連付けられます。このオプションを有効にした場合は、許可/禁止リストを編集できなくなることに注意してください。
3. 「**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。この方法の詳細については、『*SonicOS ポリシー ガイド*』を参照してください。
4. 「**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。この方法の詳細については、『*SonicOS ポリシー ガイド*』を参照してください。
5. 設定の完了後、「**適用**」を選択します。

# 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 および無線サブネット名が構成されます。仮想アクセスポイントの構成は「デバイス > 内部無線 > 仮想アクセスポイント > 仮想アクセスポイントオブジェクト」で行います。



## VAP 一般設定

仮想アクセスポイントの一般設定は、以下の手順に従います

1. 「デバイス > 内部無線 > 仮想アクセスポイント > 仮想アクセスポイントオブジェクト」ページに移動します。
2. 既存の仮想アクセスポイントの設定を編集するには、そのアクセスポイントに対する編集アイコンをクリックします。新しいアクセスポイントを作成するには、「追加」をクリックします。
3. 「名前」フィールドにアクセスポイントのわかりやすい名前を入力します。
4. 「SSID」フィールドに一意的な名前を入力します。この名前は、パケットヘッダに添付される一意の識別子になります。最大 32 文字の英数字で、大文字と小文字は区別されます。
5. ドロップダウンメニューから VLAN ID を選択します。
6. 「仮想アクセスポイントを有効にする」オプションをオンにして有効にします。
7. 必要に応じて、権限のない無線クライアントから無線 SSID を確認できなくする場合は、「SSID 抑制を有効にする」オプションをオンにします。オンにした場合、SSID 名のブロードキャストを抑制し、プローブ要求への応答を無効にします。
8. 「適用」を選択します。

## VAP 詳細設定

「詳細設定」では、仮想アクセスポイントの認証と暗号化設定が構成できます。表示されるオプションは、仮想アクセスポイントプロファイルを定義した時と同じです。

仮想アクセスポイントの詳細設定は、以下の手順に従います:

1. 「デバイス > 内部無線 > 仮想アクセスポイント > 仮想アクセスポイントオブジェクト」ページに移動します。
2. 既存の仮想アクセスポイントの設定を編集するには、そのアクセスポイントに対する編集アイコンをクリックします。新しいアクセスポイントを作成するには、「追加」をクリックします。
3. 「詳細」を選択します。
4. 「仮想アクセスポイントプロファイル設定」の見出しで、「プロファイル名」をドロップダウンメニューから選択します。そのプロファイルのすべての設定が、プロファイルから自動で入力されます。

5. プロファイルを使用しない場合、「プロファイル名」を「プロファイルなし」のままにして、「**仮想アクセスポイントプロファイル**」の説明に従って残りのフィールドを入力します。
6. 「**適用**」を選択します。

## 仮想アクセスポイントグループ

仮想アクセスポイントグループ機能では、単一の内部無線通信機に適用する複数の 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** > **内部無線** > **仮想アクセスポイント** > **仮想アクセスポイントグループ**」タブで行います。

- ① **補足:** 仮想アクセスポイントグループを作成するには、複数の仮想アクセスポイントが設定されていることが必要です。アクセスポイントが 1 つしかない場合、自動的に既定のグループである内部 AP グループに追加されます。

仮想アクセスポイントグループの有効化は、以下の手順に従います:

1. 「**デバイス** > **内部無線** > **仮想アクセスポイント** > **仮想アクセスポイントグループ**」タブに移動します。
2. 既存の仮想アクセスポイントグループの設定を編集するには、そのアクセスポイントに対する**編集**アイコンをクリックします。
3. 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ます。
4. グループからオブジェクトを削除するには、「**仮想 AP グループメンバー**」リストからオブジェクトを選択し、左矢印ボタンをクリックします。
5. 設定の完了後、「**適用**」を選択します。

## 仮想アクセスポイントグループの有効化

仮想アクセスポイントを構成して VAP グループに追加した後、そのグループを内部無線に適用してユーザが利用可能にしなければなりません。

グループを利用可能にするには、以下の手順に従います:

1. 「**デバイス** > **内部無線** > **仮想アクセスポイント**」に移動します。
2. 「**無線仮想アクセスポイントグループ**」タブで、有効にする内部 AP グループの三角アイコンをクリックします。
3. **編集**アイコンをクリックし、「**仮想アクセスポイントを有効にする**」を選択します。
4. 「**適用**」を選択して設定を更新します。

## 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 内部無線 管理者ガイド  
更新日 - 2021 年 1 月  
ソフトウェア バージョン - 7  
232-005660-10 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