

セキュリティ

セキュリティ	2
SSID のブロードキャスト	2
無線クライアントの分離	2
モード	3
なし（プレーンテキスト）	3
スタティック WEP	4
IEEE802.1x	6
RADIUS サーバーの設定	6
キーの更新	6
WPA パーソナル/エンタープライズ	7
WPA バージョン	8
暗号スイート	8
RADIUS サーバーの設定	9
キーの更新	10

セキュリティ

無線通信のセキュリティの設定を行います。

1. 「SSID のブロードキャスト」「無線クライアントの分離」を必要に応じて設定します。
2. 「モード」で暗号化の認証方式を選択してください。
3. 2.で選択した認証方式に付随する項目を設定してください。

☞ 認証方式や認証方式に付随する項目は、接続する無線クライアントと合わせてください。

4. 「適用」ボタンをクリックしてください。

SSID のブロードキャスト

SSID をブロードキャストするか否かを設定します。デフォルトは「チェックなし」です。セキュリティ対策のためには、「チェックなし」をお勧めします。

項目名	説明
チェックあり	ビーコン信号にネットワーク名を含みます。SSID が未設定であるか、ANY が設定されている無線クライアントから、本製品のネットワーク名を検出することが可能となります。
チェックなし	ビーコン信号にネットワーク名を含みません。SSID が未設定であるか、ANY が設定されている無線クライアントからは、本製品のネットワーク名を検出できません。無線クライアントを本製品に接続するためには、無線クライアントに本製品と同じ SSID を設定しておかなければなりません。

表 1:

☞ この設定は、「詳細設定」/「イーサネット設定」画面の内部ネットワークインターフェースに対して適用されます。ゲストネットワークインターフェースが有効となっている場合は、それにも適用されます。VWN（バーチャル・ワイヤレス・ネットワーク）におけるこの設定は、「詳細設定」/「VWN」画面にあります。

無線クライアントの分離

本製品に接続している無線クライアント間の通信を許可するか否かを設定します。デフォルトは「チェックなし」です。

項目名	説明
チェックあり	無線クライアント同士の通信を禁止します。
チェックなし	無線クライアント同士の通信を許可します。

表 2:

☞ WDS の接続相手となっているアクセスポイントとの通信は分離できません（相手のアクセスポイントに接続し

ている無線クライアントとの通信が可能です)。

モード

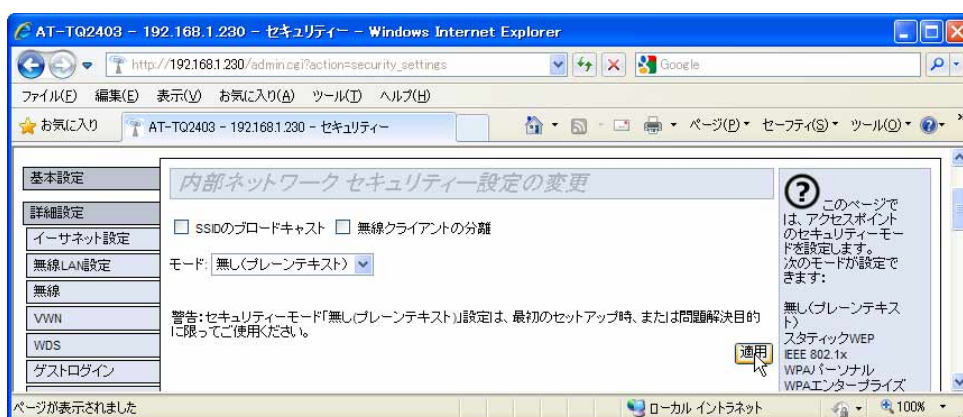
暗号化の認証方式を選択します。デフォルトは「無し（プレーンテキスト）」です。セキュリティ対策のためには、「WPA パーソナル」または「WPA エンタープライズ」をお勧めします。

項目名	説明
無し（プレーンテキスト）	認証および暗号化を行いません。誰でも自由に本製品に接続することができます。
スタティック WEP	固定キーをもとに RC4 アルゴリズムによる暗号化を行います。無線クライアント個別の認証は行いません。WEP は脆弱なため、固定キーで運用するなら「WPA パーソナル」の使用をお勧めします。
IEEE802.1x	RADIUS サーバーで無線クライアント個別の認証とキー生成を行い、本製品と無線クライアント間の通信に WEP 暗号化を行います。WEP キーは一定間隔で更新されるため、「スタティック WEP」よりは安全ですが TKIP よりは脆弱です。RADIUS サーバーをご使用になる場合は、「WPA エンタープライズ」の使用をお勧めします。
WPA パーソナル	事前共有キー（PSK）をもとに無線クライアント個別のキーを生成、本製品と無線クライアント間で認証と暗号化を行います。暗号アルゴリズムには AES または TKIP を使用します。
WPA エンタープライズ	RADIUS サーバーで無線クライアント個別のキーを生成、本製品と無線クライアント間で認証と暗号化を行います。暗号アルゴリズムには AES または TKIP を使用します。

表 3:

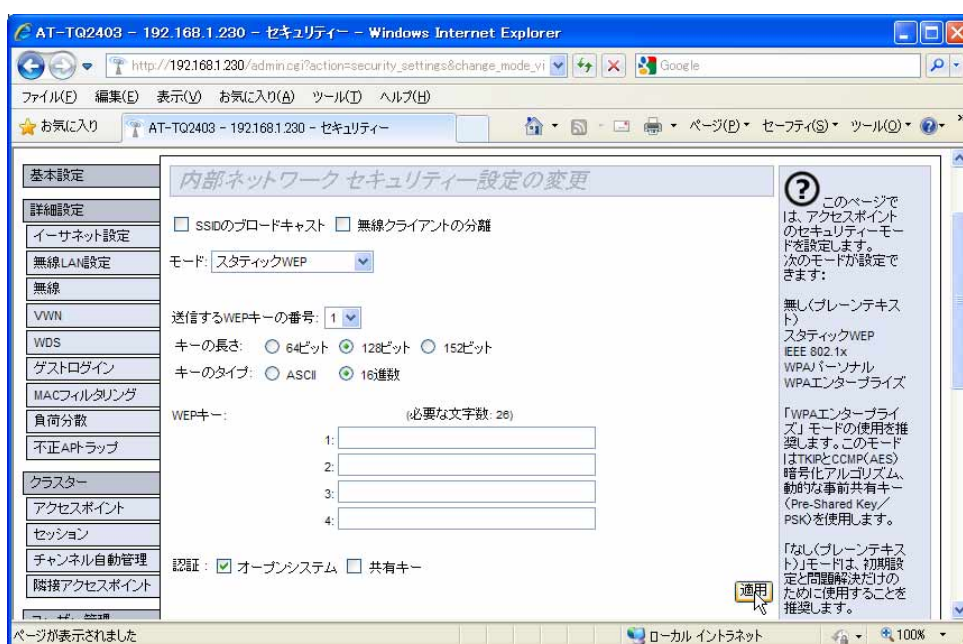
- 無線 LAN で接続しているコンピューターから本製品の設定を変更しているときにセキュリティ設定を変更すると、本製品との通信ができなくなりますのでご注意ください。設定を続ける場合は、無線 LAN カードのセキュリティ設定を本製品に合わせて変更するか、有線 LAN で接続しているネットワーク上のコンピューターから本製品にアクセスしてください。

なし（プレーンテキスト）



スタティック WEP

WEP 暗号化に関する設定を行います。



項目名	説明
送信する WEP キーの番号	1～4 の WEP キーのうち、実際に使用するキーを選択します。デフォルトは「1」です。
キーの長さ	WEP キーの強度を選択します。デフォルトは「128 ビット」です。 64 ビット 16 進数では、10 桁の WEP キーを直接入力します。

ASCII では、5 文字の半角英数記号を入力し、WEP キーを自動生成します。

128 ビット

16 進数では、26 桁の WEP キーを直接入力します。

ASCII では、13 文字の半角英数記号を入力し、WEP キーを自動生成します。

152 ビット

16 進数では、32 桁の WEP キーを直接入力します。

ASCII では、16 文字の半角英数記号を入力し、WEP キーを自動生成します。

キーのタイプ	WEP キーの生成方法を選択します。デフォルトは「16 進数」です。
	<p>ASCII</p> <p>任意の文字列から WEP キーが自動生成されます。</p> <p>入力される WEP キーの大文字・小文字は区別されます。</p>
	<p>16 進数</p> <p>16 進数 (0~9、A~F、a~f) で WEP キーを直接入力します。</p> <p>入力される WEP キーの大文字・小文字は区別されません。</p>
WEP キー	<p>「キーの長さ」と「キーのタイプ」に合わせて WEP キーを入力します。</p> <p>1~4 の 4 種類のキーを登録しておくことができます（実際に通信で使用するのはひとつです）。</p> <p>通信を行うためには、無線クライアントでも「送信する WEP キーの番号」で選択したキーと同じ WEP キーを設定する必要があります。</p>
認証	<p>通常は「オープンシステム」を選択します。</p> <p>デフォルトは「オープンシステム」です。</p> <p>セキュリティー対策のためには、「オープンシステム」にすることをお勧めします。</p> <p>オープンシステム</p> <p>無線クライアントが正しい WEP キーを持っているか否かに関係なく、任意の無線クライアントの接続を許可します。</p> <p>しかしながら、無線クライアントは接続を許可されただけであり、アクセスポイントとトラフィックの交換を行うためには、正しい WEP キーを使用してデータを暗号化/復号化しなければなりません。</p> <p>この認証アルゴリズムは、プレーンテキスト、IEEE802.1x、WPA モードでも使用されます。</p>

共有キー

無線クライアントがアクセスポイントに接続する際に、正しい WEP キーを要求します。

クライアントが誤った WEP キーを持っている場合、アクセスポイントに接続できません。

「オープンシステム」と「共有キー」の両方の選択

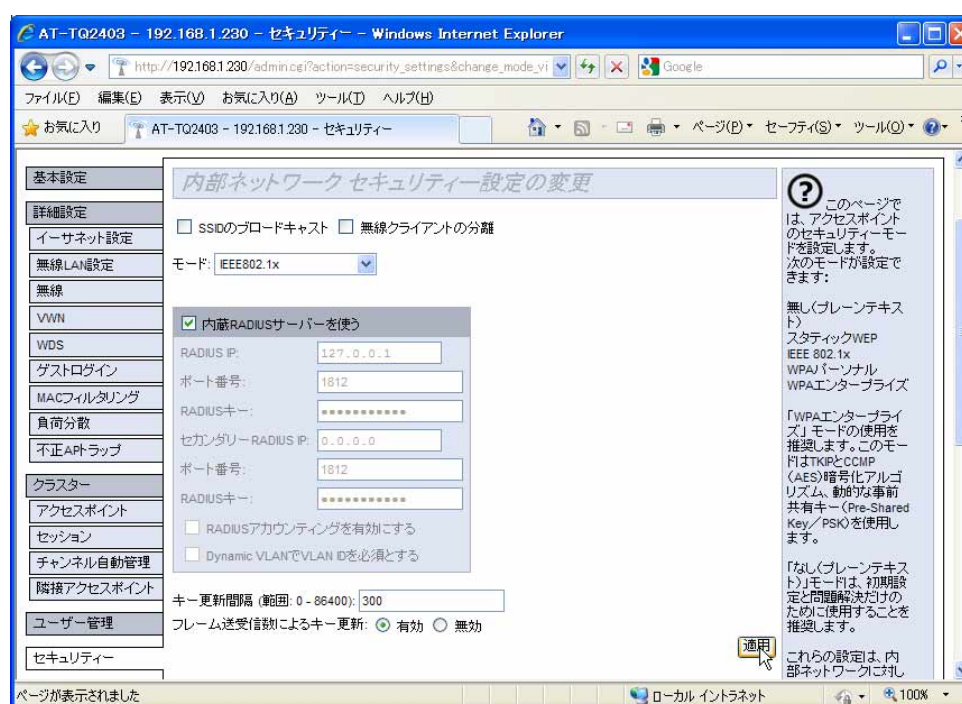
「共有キー」を使うように設定された無線クライアントは、有効な WEP キーを持っていれば、アクセスポイントに接続できます。

「オープンシステム」として WEP キーを使用するように設定された無線クライアントは（共有キーは無効）、アクセスポイントに接続できます。

表 4:

IEEE802.1x

IEEE 802.1X 認証に関する設定を行います。



RADIUS サーバーの設定

設定内容は、下の「WPA パーソナル/エンタープライズ」の「RADIUS サーバーの設定」を参照してください。

キーの更新

ブロードキャストキー（ブロードキャストフレームを暗号化する際に使用するキー）、ユニキャストキー（ユニキャストフレームを暗号化するキー、無線クライアントごとに異なります）の各々は、タイマーと送受信カウンターを持っており、次の設定に従ってこれらのキーが更新されます。

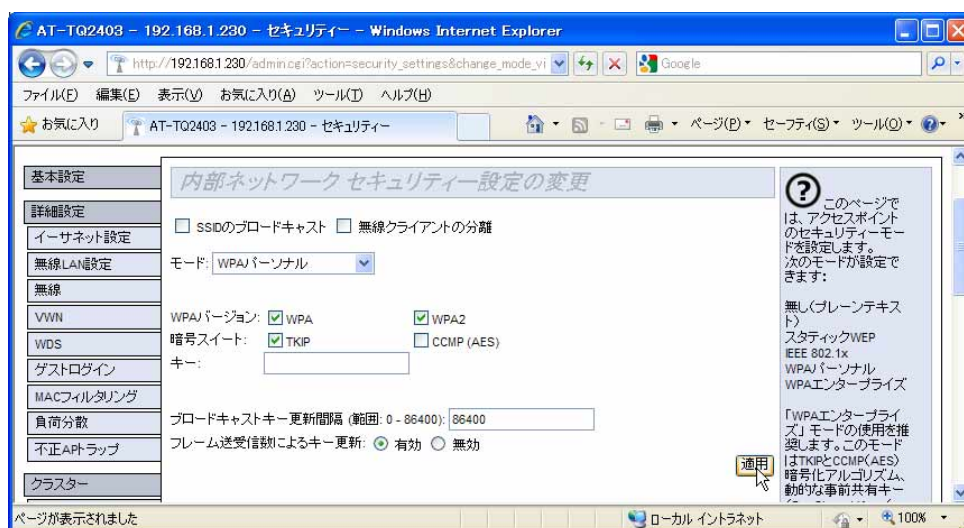
項目名	説明
キー更新間隔	ブロードキャストキーとユニキャストキーの更新間隔を 0～86400（秒）で設定します。ブロードキャストキーとユニキャストキーの更新は同時に行われます。0 を設定すると、定期的なキーの更新を行いません。デフォルトは「300」です。 キー更新が発生すると、「フレーム送受信数によるキー更新」を管理している送受信カウンターのすべりもリセットされます。
フレーム送受信数によるキー更新	送受信したフレーム数が 1,000,000 に達したときに暗号キーの更新を行うかどうかを設定します。デフォルトは「有効」です。 更新は、ユニキャストキー（無線クライアントごと）、ブロードキャストキーごとに行われます。ただし、ブロードキャストキーの更新が発生した場合、ユニキャストキーの更新も同時に行われます。キー更新が発生すると、更新されたキーの「キー更新間隔」を管理するタイマーもリセットされます。

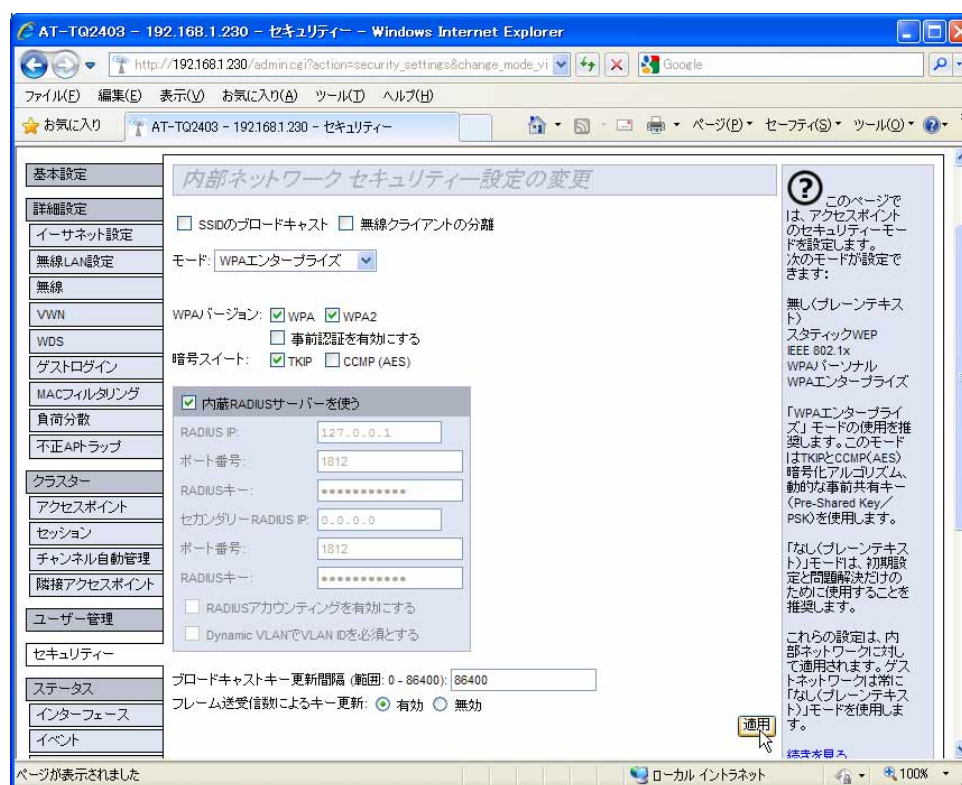
表 5:

- 再認証時間（Session-Timeout）によって再認証が発生した場合も、ユニキャストフレームの送受信カウンターがリセットされます。

WPA パーソナル/エンタープライズ

WPA 認証に関する設定を行います。





WPA バージョン

WPA の種類を選択します。WPA のみをサポートする無線クライアントと、WPA2 をサポートするものが混在する環境では両方を選択します（無線ネットワークの全体的なセキュリティは、WPA と同じレベルとなります）。デフォルトは「WPA」「WPA2」の両方です。

項目名	説明
WPA	WPA のみに対応する無線クライアントを使用する場合、「WPA」を選択します。
WPA2	WPA2 に対応する無線クライアントを使用する場合、「WPA2」を選択します。
事前認証を有効にする	<p>(WPA エンタープライズのみ)</p> <p>「チェックあり」にすると、無線クライアントが現在使用しているアクセスポイントから、対象となるアクセスポイントに、事前認証情報を中継します。これにより、無線クライアントがローミングしたときの認証をスピードアップします。この機能は、WPA2 のみで使用できます。</p>

表 6:

- 🔌 WPA は、IEEE 802.11i のドラフト段階における機能の実装です。WPA2 は、IEEE 802.11i が正式なものとなった後、IEEE 802.11i の必須機能のすべての実装です。

暗号スイート

暗号プロトコルを選択します（両方を選択することもできます）。デフォルトは「TKIP」です。

項目名	説明
TKIP	TKIP は、WEP と同様に RC4 で暗号化しますが、暗号キーは無線クライアントごとに異なったものとなり、また一定回数使用すると、新たなものに變更されます。
CCMP (AES)	米国商務省の承認した標準技術を用いた暗号化を行います。この暗号化方式は、強力なアルゴリズムを持ちます。
キー	(WPA パーソナルのみ) 暗号キーを設定します。8～63 文字の半角英数記号を入力します。大文字、小文字は区別されます。

表 7:

- 🔑 WPA 規格では、TKIP は必須項目、CCMP (AES) はオプション項目ですが、本製品では、TKIP、CCMP (AES) とも実装しています。

RADIUS サーバーの設定

項目名	説明
内蔵 RADIUS サーバーを使う	<p>認証に用いる RADIUS サーバーを選択します。</p> <p>「チェックあり」にすると、本製品内蔵の RADIUS サーバーを使用します。 「チェックなし」にすると、外部の RADIUS サーバーを使用します（外部 RADIUS サーバーの IP アドレスなどの入力が必要）。 デフォルトは「チェックあり」です。</p>
RADIUS IP	<p>プライマリーとして使用する、外部 RADIUS サーバーの IP アドレスを入力します。</p> <p>デフォルト「127.0.0.1」は、内蔵 RADIUS サーバーの IP アドレスです。 (例) 192.168.2.30</p>
ポート番号	<p>プライマリー、セカンダリーそれぞれの外部 RADIUS サーバーのポート番号を 1～65534 の範囲で入力します。デフォルトは「1812」です。アカウント用のポート番号は、「このポート番号 + 1」となります。</p>
RADIUS キー	<p>プライマリー、セカンダリーそれぞれの外部 RADIUS サーバーに接続するためのパスワードを 128 文字までの半角英数記号で入力します。</p>
セカンダリー RADIUS IP	<p>セカンダリーとして使用する外部 RADIUS サーバーの IP アドレスを入力します。</p> <p>デフォルト「0.0.0.0」のとき、セカンダリー RADIUS サーバーは無効です。</p>
RADIUS アカウンティングを有効にする	<p>「チェックあり」にすると、ユーザーを認証した外部の RADIUS サーバーを使用して、ユーザーがセッション中に使用したリソース（使用時間や送受信データの総計など）を記録することができます。</p> <p>デフォルトは「チェックなし」です。</p>
ダイナミック VLAN で VLAN ID を必須とする	<p>「チェックあり」にすると、RADIUS サーバーからの認証応答に VLAN ID が含まれていなければ、その認証要求を行った無線クライアントの通信を禁止します。</p> <p>デフォルトは「チェックなし」です。</p>

表 8:

- ☞ 本製品の内蔵 RADIUS サーバーで認証を行う場合、SP1 または SP2 を適用していない Windows Vista 内蔵サブリナントを使用した無線クライアントからは接続することができません。
- ☞ 「RADIUS IP」「セカンダリー RADIUS IP」に「999.999.999.999」のようなアドレスを設定すると、「255.255.255.255」のように設定されます。
- ☞ 「RADIUS IP」に「詳細設定」/「イーサネット設定」画面の「スタティック IP アドレス」に設定した IP アドレスを入力しないでください。

キーの更新

ブロードキャストキー（ブロードキャストフレームを暗号化する際に使用するキー）、ユニキャストキー（ユニキャストフレームを暗号化するキー、無線クライアントごとに異なります）の各々は、タイマーと送受信

カウンターを持っており、次の設定に従ってこれらのキーが更新されます。

項目名	説明
ブロードキャストキー更新間隔	ブロードキャストキーの更新間隔を 0～86400（秒）で設定します。0 を設定すると、定期的なキーの更新を行いません。デフォルトは「86400」です。 キー更新が発生すると、「フレーム送受信数によるキー更新」を管理しているブロードキャストキーの送受信カウンターもリセットされます。
フレーム送受信数によるキー更新	送受信したフレーム数が 1,000,000 に達したときに暗号キーの更新を行うか否かを設定します。デフォルトは「有効」です。 更新は、ユニキャストキー（無線クライアントごと）、ブロードキャストキーごとに行われます。ブロードキャストキーの更新が発生すると、「ブロードキャストキー更新間隔」を管理するタイマーもリセットされます。

表 9:

- 🔗 WPA エンタープライズで再認証時間（Session-Timeout）によって再認証が発生した場合も、ユニキャストフレームの送受信カウンターがリセットされます。