詳細設定

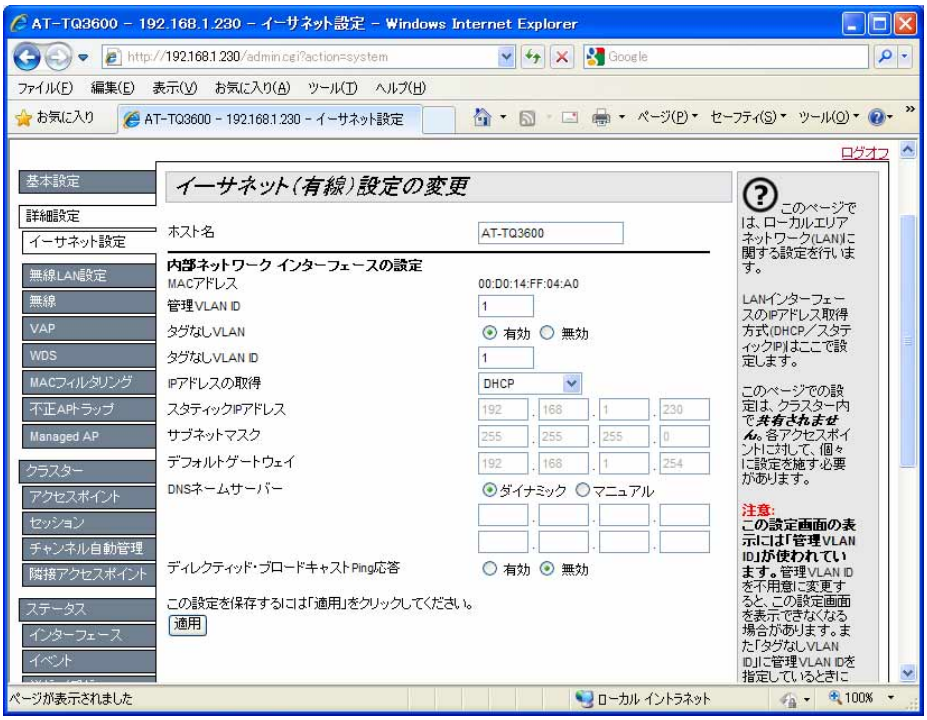
イーサネット設定 2
無線 LAN 設定 5
無線 1/2 6
無線 8
VAP 16
バーチャルアクセスポイント 16
セキュリティー 18
無し 18
スタティック WEP 19
IEEE 802.1X 21
WPA パーソナル 23
WPA エンタープライズ 24
セキュリティー 27
WDS 28
WDS 接続の設定 28
スタティック WEP 30
WPA パーソナル 30
WDS 接続の解除 31
MAC フィルタリング 32
リストへの追加 32
リストからの削除 33
不正 AP トラップ 34
リストへの追加 35
リストからの削除 35
Managed AP 36
無線コントローラーの管理下に入れる 36
無線コントローラー管理下の WDS 接続 37

イーサネット設定

イーサネットポート（インターフェース）に関連する設定を行います。

1. 必要に応じて、以下の各項目を設定してください。
2. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。



項目名	説明
ホスト名	本製品のホスト名を 1～63 文字の半角英数字とハイフンで入力してください。 先頭、末尾がハイフンのホスト名は許されません。デフォルトは製品名です。このホスト名は、Web ブラウザーのタイトルバーに表示されます。
MAC アドレス	本製品の内部ネットワークインターフェースの MAC アドレスが表示されます。
管理 VLAN ID	本製品の管理用 VLAN ID を 1～4094 で指定します。デフォルトは「1」です。 管理用 VLAN には、Web 設定画面を使用して本製品の設定を変更する設定用コンピューターを接続します。

タグなし VLAN	VLAN タグを持たないパケットの取り扱い方法を決めます。 「有効」の場合、指定した VLAN ID を持つパケットをイーサネットポートから送信するとき、タグを取り除きます。また、イーサネットポートから VLAN タグなしのパケットを受信したとき、指定した VLAN ID を持つパケットとして扱います。 デフォルトは「有効」です。
タグなし VLAN ID	管理用 VLAN ID、バーチャルアクセスポイント（VAP）の VLAN ID のうち、タグなし（UNTAGGED）にしたい VLAN の ID を指定します。 「タグなし VLAN」が「有効」のとき入力が可能です。デフォルトは「1」です（管理 VLAN ID と同じ値）。
IP アドレスの取得	「DHCP」または「スタティック IP」を選択します。 「スタティック IP」を選択した場合、「スタティック IP アドレス」「サブネットマスク」「デフォルトゲートウェイ」「DNS ネームサーバー」を入力してください。 「DHCP」を選択した場合、DHCP サーバーから IP アドレスなどを自動取得します。DNS サーバーのアドレスも自動取得する場合は、「DNS ネームサーバー」で「ダイナミック」を選択してください。DHCP サーバーからの情報の取得に失敗すると、IP アドレスは「192.168.1.230」となります。 デフォルトは「DHCP」です。
スタティック IP アドレス	本製品の IP アドレスを指定します。デフォルトは「192.168.1.230」です。
サブネットマスク	サブネットマスクを指定します。デフォルトは「255.255.255.0」です。
デフォルトゲートウェイ	デフォルトゲートウェイを指定します。デフォルトは「192.168.1.254」です。
DNS ネームサーバー	DHCP サーバーから取得した DNS サーバーのアドレスを使用するか否か。 「ダイナミック」を選択した場合、DHCP サーバーから取得したアドレスを使用します。 「マニュアル」を選択した場合、下の入力欄に「プライマリー DNS サーバー」（上側）、「セカンダリー DNS サーバー」（下側）の IP アドレスを入力します。ひとつのみ入力する場合は、上側の欄に入力してください。 デフォルトは「ダイナミック」です。
ディレクティッド・ブロードキャスト Ping 応答	ディレクティッド・ブロードキャスト Ping に応答するか否か。 「有効」はディレクティッド・ブロードキャスト Ping に応答します。「無効」は応答しません。デフォルトは「無効」です。

表 1:

✎ IP アドレスを変更すると、本製品との通信が切断されます。設定を継続する場合は、変更後の IP アドレスで Web 設定画面に再ログオンしてください。また、ナビゲーションと言語が「dropdown menu」と「English」に戻ります。変更後の IP アドレスでナビゲーションと言語を再設定してください。詳しくは、「設定画面へのアクセス」/「ナビゲーションと言語」を参照してください。

✎ 「タグなし VLAN」を「有効」に設定し、「管理 VLAN ID」と「タグなし VLAN ID」を同じ値に設定すると、設

定用コンピューターを本製品のイーサネットポートに直接接続することができます。ご購入時、それらの VLAN ID は「1」に設定されています。これらの設定を変更する場合は、ご使用になるスイッチの VLAN 設定も確認してください。

✎ ディレクティッド・ブロードキャストは、192.168.1.255 のようにホストアドレス部分がすべて「1」のアドレスに対するブロードキャストです。ディレクティッド・ブロードキャスト Ping は、ネットワーク管理ソフトウェアなどが管理対象の機器を検索するために使用することがあります。

無線 LAN 設定

無線 LAN の設定を行います。

1. 「無線 1」および「無線 2」で「オン」をクリックしてください。「オン」にすることにより、無線電波の送受信が開始されます。
2. 「モード」で希望の通信プロトコルを選択し、「無線クライアントの分離」を設定してください。
3. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ 「無線 1」または「無線 2」のどちらか一方のステータスを変更すると、もう一方の無線も一時的にリンクダウンします。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。

✎ カントリーコードは、変更できません。

✎ IEEE 802.11a、IEEE 802.11n において、W52 のチャンネル（36、40、44、48）と W53 のチャンネル（52、56、60、64）は屋外での使用が禁止されています。

✎ W53 や W56（100、104、108、112、116、120、124、128、132、136、140）において現在使用しているチャンネルで気象レーダーが検出されると、アクセスポイントはレーダーとの干渉を避けるために自動的にチャンネルを変えます。その際、新たなチャンネルを使い始める前に 1 分間ほどワッチしてレーダーが検出されないことを確認します。レーダーが検出されたチャンネルは、レーダーが検出されてから 30 分間は再使用しません（使用は許されません）。気象レーダーが検出されてから 30 分以内に、検出前のチャンネルに手動で再設定しないでください。

✎ 上記画面は、「無線 1」「無線 2」を「オン」にした状態です。デフォルトは「オフ」です。

無線 1/2

項目名	説明
無線 1/2	「無線 1」(2.4GHz 帯)、「無線 2」(5GHz 帯)の無線電波を送受信するか否か。 送受信する場合は「オン」、しない場合は「オフ」を選択します。デフォルトは「オフ」です。 この設定は「無線」画面の「ステータス」と連動します。
MAC アドレス	無線 1/2 の MAC アドレスが表示されます。
モード	「無線 1」は、「IEEE 802.11b/g」「IEEE 802.11b/g/n」「2.4GHz IEEE 802.11n」が選択可能です。 「無線 2」は、「IEEE 802.11a」「IEEE 802.11a/n」「5GHz IEEE 802.11n」が選択可能です。 この設定は「無線」画面の「モード」と連動します。
チャンネル	無線 1/2 で使用するチャンネルを選択します。「Auto」を選択すると、本製品は空きチャンネルを走査し、自動的に干渉の少ないチャンネルを選択します。「Auto」に設定されていると、本製品の起動の際にもチャンネルの自動選択が行われます。「ステータス」/「インターフェース」画面で実際に使用されているチャンネルを確認できます。デフォルトは「Auto」です。「クラスター」の「チャンネル自動管理」が有効となっている場合、「Auto」は表示されません。この設定は「無線」画面の「チャンネル」と連動します。
無線クライアントの分離	同一のバーチャルアクセスポイント(VAP)に接続している無線クライアント同士の通信を許可するか否か。許可しない場合は「チェックあり」、許可する場合は「チェックなし」にします。デフォルトは「チェックなし」です。 「チェックあり」にしても、有線ネットワークや、他のバーチャルアクセスポイントに接続している無線クライアントとは通信が可能です(ご使用になる VLAN スイッチなどにより、それらが通信ができるように設定されている必要があります)。

表 2:

✎ 「無線 1」「無線 2」の「無線クライアントの分離」のどちらか一方または両方が「チェックあり」でも、同一の VAP における「無線 1」と「無線 2」間の通信は可能です。また、この機能は WDS インターフェースには適用されません。

✎ 「無線クライアントの分離」を有効にすると、例えば公共のアクセスポイントとして運用する際、同時に接続しているユーザー間のセキュリティーを確保することができます。

✎ IEEE 802.11n を使用する場合、「オプション設定」/「QoS」画面の「Wi-Fi マルチメディア(WMM)」が「有効」(デフォルト)である必要があります。

無線

無線 1（2.4GHz 帯）、無線 2（5GHz 帯）ごとに無線電波のパラメーターを設定します。パラメーターの変更が不要な場合は、「無線 LAN 設定」画面で設定するのが簡単です。

1. 「無線」で周波数帯を選択します。

   ✎ 「1」および「2」それぞれで「適用」ボタンをクリックしてください。「適用」ボタンをクリックする前に「無線」を変更すると、施した変更内容が破棄されます。

2. 「ステータス」で選択した周波数帯の無線電波の送受信を「オン」にします。
3. 「モード」で希望の通信プロトコルを選択します。
4. 必要であれば、無線電波のパラメーターを変更します。
5. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ 「無線 1」または「無線 2」のどちらか一方のステータスを変更すると、もう一方の無線も一時的にリンクダウンします。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。

✎ IEEE 802.11a、IEEE 802.11n において、W52 のチャンネル（36、40、44、48）と W53 のチャンネル（52、56、60、64）は屋外での使用が禁止されています。

✎ W53 や W56（100、104、108、112、116、120、124、128、132、136、140）において現在使用しているチャンネルで気象レーダーが検出されると、アクセスポイントはレーダーとの干渉を避けるために自動的にチャンネルを変えます。その際、新たなチャンネルを使い始める前に 1 分間ほどワッチしてレーダーが検出されないことを確認します。レーダーが検出されたチャンネルは、レーダーが検出されてから 30 分間は再使用しません（使用は許されません）。気象レーダーが検出されてから 30 分以内に、検出前のチャンネルに手動で再設定しないでください。

✎ IEEE 802.11a、IEEE 802.11n において、屋外使用が許されている W56 のチャンネルだけを「Auto チャンネル候補」で選択し、その候補のすべてのチャンネルで気象レーダーが検出されると（候補のチャンネルのすべてが使えないと判断されると）、本製品は W52 のチャンネルを使用します。

✎ 上記画面は、「無線 1」のステータスを「オン」にした状態です。デフォルトは「オフ」です。

項目名	説明
無線	設定を行う周波数帯を選択します。 「1」は、2.4GHz 帯の無線電波の設定を行います。 「2」は、5GHz 帯の無線電波の設定を行います。
ステータス	選択した周波数帯の無線電波を送受信するか否か。送受信する場合は「オン」、しない場合は「オフ」を選択します。デフォルトは、無線 1、無線 2 とも「オフ」です。これは「無線 LAN 設定」画面の「無線 1」「無線 2」と連動します。
モード	本製品で用いる通信プロトコルを選択します。 「無線」が「1」の場合、「IEEE 802.11b/g」「IEEE 802.11b/g/n」「2.4GHz IEEE 802.11n」が選択可能です。デフォルトは「IEEE 802.11b/g/n」です。 「無線」が「2」の場合、「IEEE 802.11a」「IEEE 802.11a/n」「5GHz IEEE 802.11n」が選択可能です。デフォルトは「IEEE 802.11a/n」です。 この設定は、「無線 LAN 設定」画面の「モード」と連動します。
チャンネル	下記から無線通信で使用するチャンネルを選択します。 無線 1：Auto 1 2 3 4 5 6 7 8 9 10 11 12 13 無線 2：Auto 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 「Auto」を選択すると、本製品は空きチャンネルを走査し、自動的に干渉の少ないチャンネルを選択します。「Auto」に設定されていると、本製品の起動の際にもチャンネルの自動選択が行われます。「ステータス」/「インターフェース」画面で実際に使用されているチャンネルを確認できます。デフォルトは「Auto」です。「クラスター」の「チャンネル自動管理」が有効となっている場合、「Auto」は表示されません。この設定は「無線 LAN 設定」画面の「チャンネル」と連動します。
Auto チャンネル候補	「チャンネル」で「Auto」を選択したときに自動選択されるチャンネルの候補を設定します。「チェックあり」にすると候補になります。「チェックなし」にすると候補になりません（そのチャンネルは使用されません）。 無線 1（2.4GHz）のデフォルトは、下記のすべてが選択されています。 1 2 3 4 5 6 7 8 9 10 11 12 13 無線 2（5GHz）のデフォルトは、下記のすべてが選択されています。 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
定期チャンネル更新	定期的にチャンネル再選択を行う機能を設定します。「チェックあり」にすると、「チャンネル」で「Auto」が設定されている場合には、24 時間ごとにチャンネル再選択を行います。ただし、チャンネル再選択を行おうとしたときに無線クライアントが接続中であった場合は、再選択を 30 分延期します。デフォルトは、「チェックなし」です。

使用帯域幅（IEEE 802.11n のみ）	IEEE 802.11n では、隣接する 20MHz 帯域幅の 2 つのチャンネルを合わせて、ひとつの 40MHz 帯域幅のチャンネルとして使うことができます。 IEEE 802.11n で使用する帯域幅を「20MHz」「40MHz」から選択します。デフォルトは「20MHz」です。 「40MHz」を選択すると、より高い通信レートを得られますが、倍の帯域を使用するので空きチャンネルを減らします。
制御用チャンネル（IEEE 802.11n のみ）	「使用帯域幅」を「40MHz」に設定したとき、20MHz 帯域幅のチャンネルのみをサポートした IEEE 802.11n 無線クライアントや、従来規格の無線クライアントが使用するチャンネルです。 「上側波帯」または「下側波帯」を設定します。デフォルトは「下側波帯」です。 （注）40MHz 帯域幅のうち上側の 20MHz を上側波帯、下側を下側波帯と呼びます。
ショートガードインターバル（IEEE 802.11n のみ）	ガードインターバルとは、マルチパスの影響を効率よく除去するための冗長時間です。 「有効」にすると、無線クライアントも 400ns（ナノ秒）に対応していた場合、ガードインターバルを 400ns に短縮します。スループットは、理論値で 10%ほど良くなります。 「無効」にすると、IEEE 802.11a/g と同じ 800ns のガードインターバルを使用します。 デフォルトは「有効」です。 （注）マルチパスとは、壁や天井などで反射した電波が複数の経路をとおって受信側に届く現象です。反射した電波は、直接届いた電波より遅れるので、受信側では遅れて届いた電波の影響を防ぐ必要があります。
ビーコンに国情報を付加	ビーコンに国情報を含めるか否かを設定します。含める場合は「有効」、含めない場合は「無効」を選択してください。デフォルトは「有効」です。
プロテクション	IEEE 802.11n が従来規格（IEEE 802.11a/b/g）の機器との干渉を防ぐ信号を送信するか否か。 「Auto」は、本製品が使用するチャンネルで従来規格の機器（無線クライアントや他のアクセスポイント）を検出すると信号の送信（プロテクション）を行い、通信速度の低下を改善します。IEEE 802.11n と従来規格の機器が混在する環境では必ず「Auto」にしてください。 「オフ」は、信号の送信を行いません。IEEE 802.11n と従来規格の機器が混在している環境でこの機能をオフにすると、それらの機器の間で無線電波の干渉（コリジョン）が多発し、パフォーマンスが著しく下がります。 デフォルトは「Auto」です。 無線 1 のモード「IEEE 802.11b/g」では、IEEE 802.11b と IEEE 802.11g の干渉のプロテクションを行います。

ビーコン間隔	本製品が周期的に送信するビーコン信号の送信間隔を、20～2000 の数値（ミリ秒）で設定します。デフォルトは「100」です。
DTIM 間隔	本製品が送信するビーコンに、DTIM（Delivery Traffic Information Map）を挿入する割合を、1～255 の数値で設定します。デフォルトは「2」です。 「2」はビーコンを 2 回送信するうちの 1 回に DTIM を挿入します（DTIM を持つビーコンと持たないものが交互に送信されます）。 DTIM は、無線クライアントが省電力モードで動作しているとき、無線クライアント宛に送信すべきパケットが存在することを無線クライアントに通知します。 無線クライアントが通信可能な状態になれば、本製品は無線クライアント宛にパケットを送信します。 この値を大きくすると省電力の効果は高くなりますが、応答が悪くなります。
パケット分割しきい値	パケットを分割（Fragmentation）して送信する場合の、分割の基準となるパケットサイズを 256～2346 の偶数の数値（バイト数）で設定します。 設定した数値より大きいパケットは分割して送信します。 ただし、「2346」を設定するとパケットの分割を行いません。デフォルトは「2346」です。 通信状態が悪く、大きなパケットでは再送が発生するような環境では、送信するパケットサイズを小さくすることにより、状況が改善することがあります。 しかしながら、通常はこのサイズの変更はおすすめいたしません。
RTS しきい値	パケットを送信する前に、RTS（送信要求）パケットを送る場合の基準となるパケットサイズを 0～2347 の数値で設定します。 指定したパケットサイズより大きいサイズのパケットを送信する場合に、RTS パケットを送信します。 ただし、「2347」を設定すると RTS パケットを送信しません。デフォルトは「2347」です。 RTS しきい値を低く設定すると、頻繁に RTS パケットが送信されます。 これは、より多くの無線帯域を消費し、スループットを下げますが、通信トラフィックが多いとか、干渉を受けているネットワークにおいては、コリジョンや干渉が改善されることがあります。 しかしながら、通常はこのサイズの変更はおすすめいたしません。
最大ステーション数	本製品に接続可能な無線クライアント数を 0～200 の数値で設定します。 「0」に設定した場合、無線クライアントは接続されません。デフォルトは「200」です。
送信出力	本製品の電波出力の強度を下記から選択します。デフォルトは「100%」です。 1% 5% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

マルチキャスト送信レート	本製品にサポートさせたいマルチキャスト送信レートを下記から選択します（Mbps）。ブロードキャストやビーコンの送信もこのレートが使用されます。 「Auto」を選択すると、「レガシーレートセット」で選択されているベーシック・レートセットのうち最も低いレートを使用します。デフォルトは「Auto」です。 無線 1：54 48 36 24 18 12 11 9 6 5.5 2 1 Auto 無線 2：54 48 36 24 18 12 9 6 Auto
レガシーレートセット	通信プロトコルが IEEE 802.11n 以外の場合のレート（通信速度）を設定します。 サポート 本製品でサポートさせたいレートを下記から選択します。選択するレートにチェックをつけてください。 デフォルトは、本製品がサポートするすべての速度が選択されています。 無線 1：54 48 36 24 18 12 11 9 6 5.5 2 1 無線 2：54 48 36 24 18 12 9 6 ベーシック 本製品に接続してくるステーション（無線クライアントや他のアクセスポイント）が、本製品への接続を許されるために最低限サポートしていなければならないサポート・レートセットです。ステーションのサポート・レートセットに、このベーシック・レートセットのひとつでも欠けていると接続は許されません。一般的なステーションのサポート・レートセットはベーシック・レートセットより高いレートを含んでいるので、通常はベーシック・レートセットより高いレートで接続します。 「サポート」で選んだレートの中から選択します。選択するレートにチェックをつけてください。通常は変更の必要はありません。デフォルトは以下のとおりです。 無線 1：11 5.5 2 1 無線 2：24 12 6
MCS（データレート）設定	通信プロトコルが IEEE 802.11n の場合のレート（通信速度）を設定します。選択するインディックスにチェックをつけてください。レートとインディックスの対応は表 2 を参照してください。デフォルトは、次の 2 種類の製品とも選択可能なすべてが選択されています。

	AT-TQ2450 では（2 ストリームが可能）、インディックス 0～15 が選択可能です。 AT-TQ3600 では（3 ストリームが可能）、インディックス 0～23 が選択可能です。
ブロードキャスト/マルチキャスト速度制限	イーサネットポートで受信したブロードキャストとマルチキャストのパケットが無線 LAN で送信される際の制限を行うか否か。 行う場合は「チェックあり」、行わない場合は「チェックなし」にします。 デフォルトは「チェックなし」です。 他の機器の ARP リクエストや DHCP メッセージなど、ブロードキャストやマルチキャストは、ネットワーク上のほとんどの機器にとって自分には関係ないものです。 この機能を有効にすると、ネットワークに送信される冗長なパケットの数を制限します。また、次の 2 つの項目の入力が可能となります。
速度制限	1～50 の数値（パケット数/秒）で設定します。デフォルトは「50」です。この設定値は、無線 1 または無線 2 ごとに現在有効となっている VAP 全体で共有されます。例えば、無線 1 で 3 つの VAP が有効になっていれば、個々の VAP における制限は 50/3 となります。また、仮に 3 つの VAP に向かうパケットがそれぞれ 40 ずつあったとすると 70（=40 × 3-50）が破棄されます。
バースト時の速度制限	「速度制限」の設定値～75 の数値（パケット数/秒）で設定します。デフォルトは「75」です。 この速度制限を上回るブロードキャストとマルチキャストのトラフィックは、間欠的なバーストとなります。

表 3:

✎ IEEE 802.11n を使用する場合、「オプション設定」/「QoS」画面の「Wi-Fi マルチメディア（WMM）」が「有効」（デフォルト）である必要があります。

✎ 2.4GHz 帯（無線 1）では、拡張チャンネル側帯域で他の通信が行われていることが確認された場合、自動的に 20MHz 帯を使用した通信へと切り替わるため、一般的な環境においてチャンネルボンディング（40MHz 幅）が使用できる場面は非常にまれです。

✎ 「定期チャンネル更新」が有効となっているとき、本製品の起動直後のチャンネル更新のログは出力されません。

✎ 「プロテクション」を「オフ」にしても RTS/CTS が送出されます。

✎ サポートレートを超えるレートで送信されたパケットを受信します。

✎ AT-TQ3600 において、「MCS（データレート）設定」で 3 ストリームのインディックス 16～23 を有効にしたい場合は、インデックス 16～23 のすべてとインディックス 0～15 のうちのどれかひとつを有効にしてください。インデックス 16～23 だけを設定した場合、その設定は無効となり、インデックス 0～7 が有効となった状態で動作します。

		データレート（Mbit/s）				
		800ns		400ns		ガードインターバル
インディックス	ストリーム数	20MHz	40MHz	20MHz	40MHz	使用帯域幅
0	1	6.5	13.5	7.2	15	
1		13	27	14.4	30	
2		19.5	40.5	21.7	45	
3		26	54	28.9	60	
4		39	81	43.3	90	
5		52	108	57.8	120	
6		58.5	121.5	65	135	
7		65	135	72.2	150	
8	2	13	27	14.4	30	
9		26	54	28.9	60	
10		39	81	43.3	90	
11		52	108	57.8	120	
12		78	162	86.7	180	
13		104	216	115.6	240	
14		117	243	130	270	
15		130	270	144.4	300	
16	3	19.5	40.5	21.7	45	
17		39	81	43.3	90	
18		58.5	121.5	65	135	
19		78	162	86.7	180	
20		117	243	130	270	
21		156	324	173.3	360	
22		175.5	364.5	195	405	
23		195	405	216.7	450	

表 4: MCS インディックスとデータレート

VAP

バーチャルアクセスポイント

バーチャルアクセスポイント（VAP）は、本製品上に仮想的なアクセスポイントを作り出す機能です。VAP と VLAN を組み合わせることにより、1 台の本製品をあたかも複数のアクセスポイントが存在するかのように動作させることができます。VAP は、無線 1/2 ごとに 16 個まで作成することができます。
VAP ごとに、下記の項目をカスタマイズできます。

- VAP の有効または無効
- VLAN ID
- SSID
- SSID のブロードキャスト
- セキュリティー
- MAC フィルタリング

✎ VAP の数は、無線 1/2 ごとに 5 個以内にすることをおすすめいたします。

VAP0 は、常に有効です（無効にできません）。デフォルト設定は下記のとおりです。

- 無線 1（2.4GHz）、無線 2（5GHz）とも使用
- VLAN ID：1（「イーサネット設定」画面の「タグなし VLAN ID」に一致しています）
- SSID：allied
- SSID のブロードキャスト：する
- セキュリティー：無し
- MAC フィルタリング：適用しない

✎ 無線クライアントが VAP0 に接続できるようにするには、「無線 LAN 設定」画面で「無線 1」および「無線 2」を「オン」にする必要があります。

設定手順は、下記のとおりです。

1. 該当の VAP の「有効」にチェックを入れます。
2. 「VLAN ID」を入力します（ご使用になるスイッチの VLAN 設定が必要です）。
3. 「SSID」「SSID のブロードキャスト」「セキュリティー」「MAC フィルタリング」を設定します。これらは、「無線 1」「無線 2」で別々の設定にすることもできます。

   ✎ 「セキュリティー」の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。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。

項目名	説明
無線	設定を行う周波数帯を選択します。 「1」は、2.4GHz 帯の無線の設定を行います。 「2」は、5GHz 帯の無線の設定を行います。 「1」および「2」ごとに VAP の設定を変えることができます。
VAP	VAP（バーチャルアクセスポイント）の番号 0～15 が表示されています。
有効	該当の VAP を有効にするか否か。有効にする場合は「チェックあり」、無効にする場合は「チェックなし」にします。デフォルトは「チェックなし」です。VAP0 は常に「有効」です。
VLAN ID	該当の VAP が使用する VLAN ID を 1～4094 の数字で入力します。
SSID	該当の VAP が使用する SSID（ネットワーク名）を入力します。この SSID は指定した VLAN ID に対応づけられます。 1～32 文字の半角英数記号で入力します。 デフォルトは「Virtual Access Point 1～15」です。
SSID のブロードキャスト	該当の VAP で SSID（ネットワーク名）をブロードキャストするか否か。 「チェックあり」にすると、ビーコン信号に SSID を含みます。任意の無線クライアントの接続設定において、接続の候補として本製品の SSID が自動的に表示されます。また、無線クライアントの ANY 接続を許可します。 「チェックなし」にすると、ビーコン信号に SSID を含みません。無線クライアントの接続設定で、本製品の SSID は表示されません。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 を手入力しなければなりません。また、無線クライアントの ANY 接続を拒否します。 セキュリティー対策のためには、「チェックなし」にすることをおすすめします。デフォルトは「チェックあり」です。
セキュリティー	「無し」「スタティック WEP」「IEEE 802.1X」「WPA パーソナル」「WPA エンタープライズ」から選択します。デフォルトは「無し」です。それぞれの詳細な設定内容は別表を参照してください。 （注）「無線 LAN 設定」画面または「無線」画面で IEEE 802.11n を含む通信モードが選択されているとき、「セキュリティー」プルダウンメニューに「スタティック WEP」「IEEE 802.1X」は表示されません。 「無し」は、認証および暗号化を行いません。誰でも自由に VAP に接続することができます。 「スタティック WEP」は、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」の使用をおすすめします。

	「IEEE 802.1X」は、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」の使用をおすすめします。 「WPA パーソナル」は、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し、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」は、RADIUS サーバーで無線クライアント個別のキーを生成し、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。
MAC フィルタリング	該当の VAP に対して「MAC フィルタリング」を適用するか否か。 「適用しない」「適用する」から選択します。デフォルトは「適用しない」です。 「MAC フィルタリング」に使用する無線クライアントのリストは「MAC フィルタリング」画面で入力します。

表 5: バーチャルアクセスポイント

✎ 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ー設定を変更すると、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ー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。

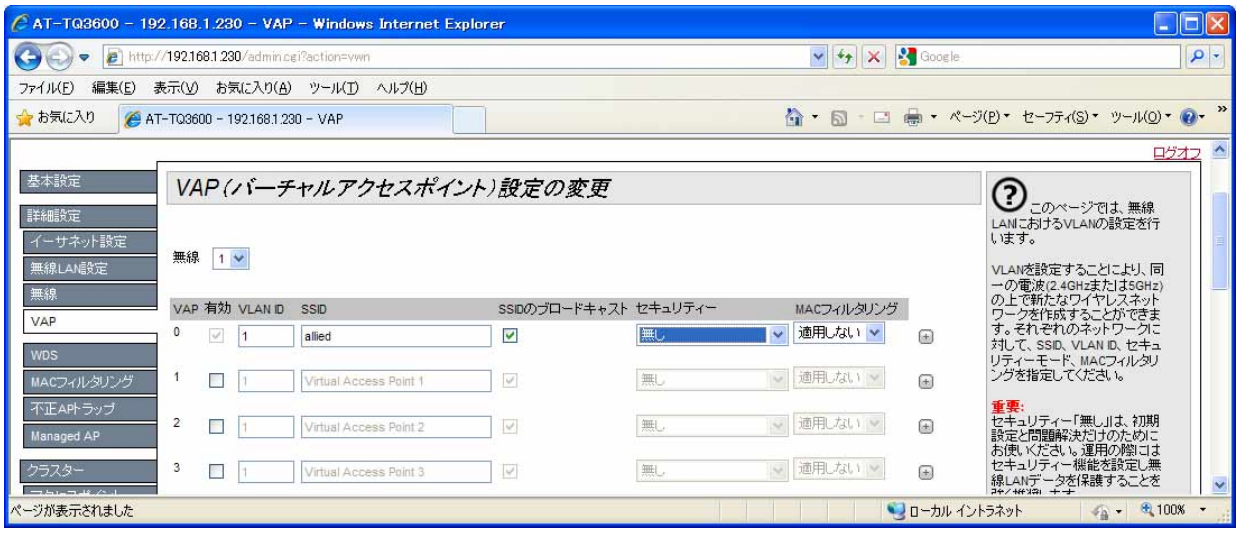
✎ 「ANY 接続」は、SSID に「ANY」を設定した、または SSID が未設定の無線クライアントによるアソシエーション（アクセスポイントと無線クライアントがお互いを認識している状態）です。アソシエーションが確立しても、キーを知らなければそのアクセスポイントを使うことはできませんが、「ANY 接続」を許したり、無線クライアントの設定時に容易に SSID を知ることができれば、接続を許したくない無線クライアントが求めるアソシエーションに応答して、不要なリソースを使う可能性があります。

✎ SNMP MIB「ifAdminStatus」の SET 操作ができません。SET は成功するように見えますが、VAP の状態は変わりません。また、設定画面で VAP の「有効」のチェックを外してもアクセスポイントを再起動するまでは該当 VAP の ifEntry が残り続けます（ifAdminStatus は down(2) が返されます）。

セキュリティー

無し

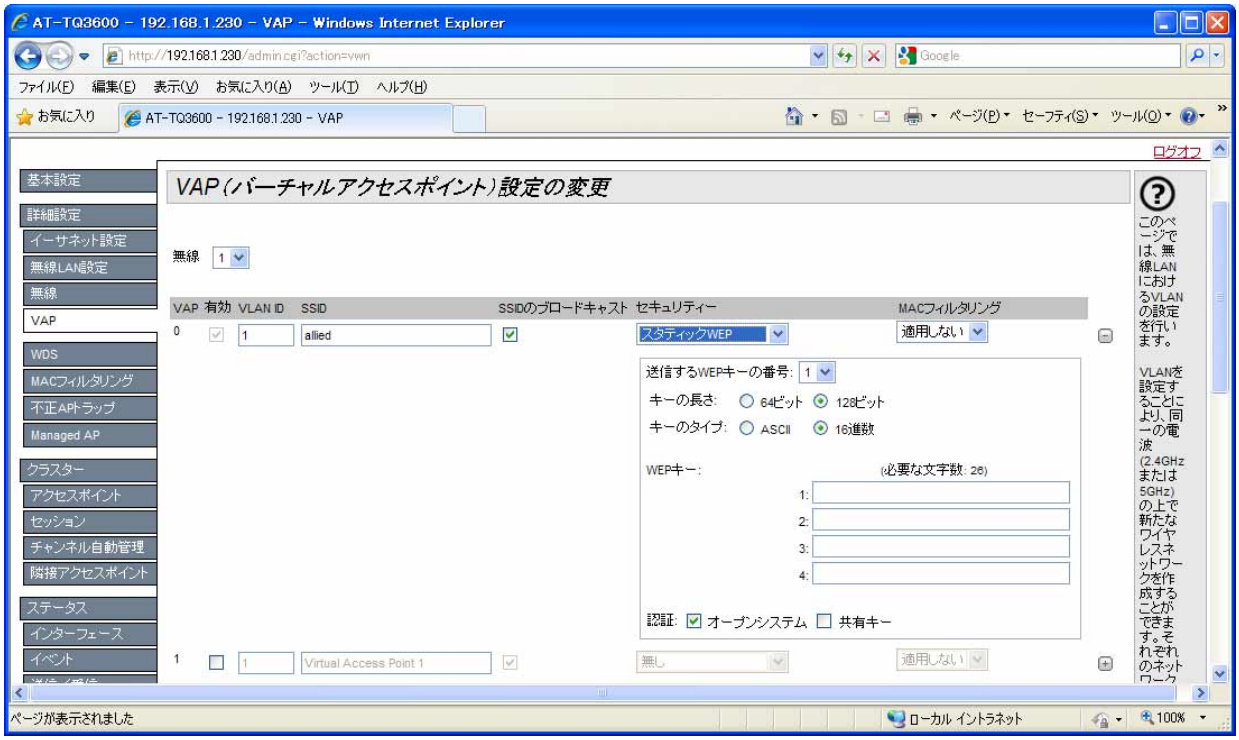
「無し」は、認証および暗号化を行いません。誰でも自由に VAP に接続することができます。ゲスト用のホットスポットを用意するなどの目的でこれを選択する場合、ネットワーク全体のセキュリティーを考慮する必要があります。



スタティック WEP

「スタティック WEP」は、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」の使用をおすすめします。

✎ 「無線 LAN 設定」画面または「無線」画面で IEEE 802.11n を含む通信モードが選択されているとき、「セキュリティー」プルダウンメニューに「スタティック WEP」は表示されません。



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。
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。 ASCII 任意の文字列から WEP キーが自動生成されます。 入力される WEP キーの大文字・小文字は区別されます。 16 進数 16 進数（0～9、A～F、a～f）で WEP キーを直接入力します。 入力される WEP キーの大文字・小文字は区別されません。
WEP キー	「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。 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）。 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。
認証	通常は「オープンシステム」を選択します。デフォルトは「オープンシステム」です。 セキュリティー対策のためには、「オープンシステム」にすることをおすすめします。 オープンシステム 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。 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。

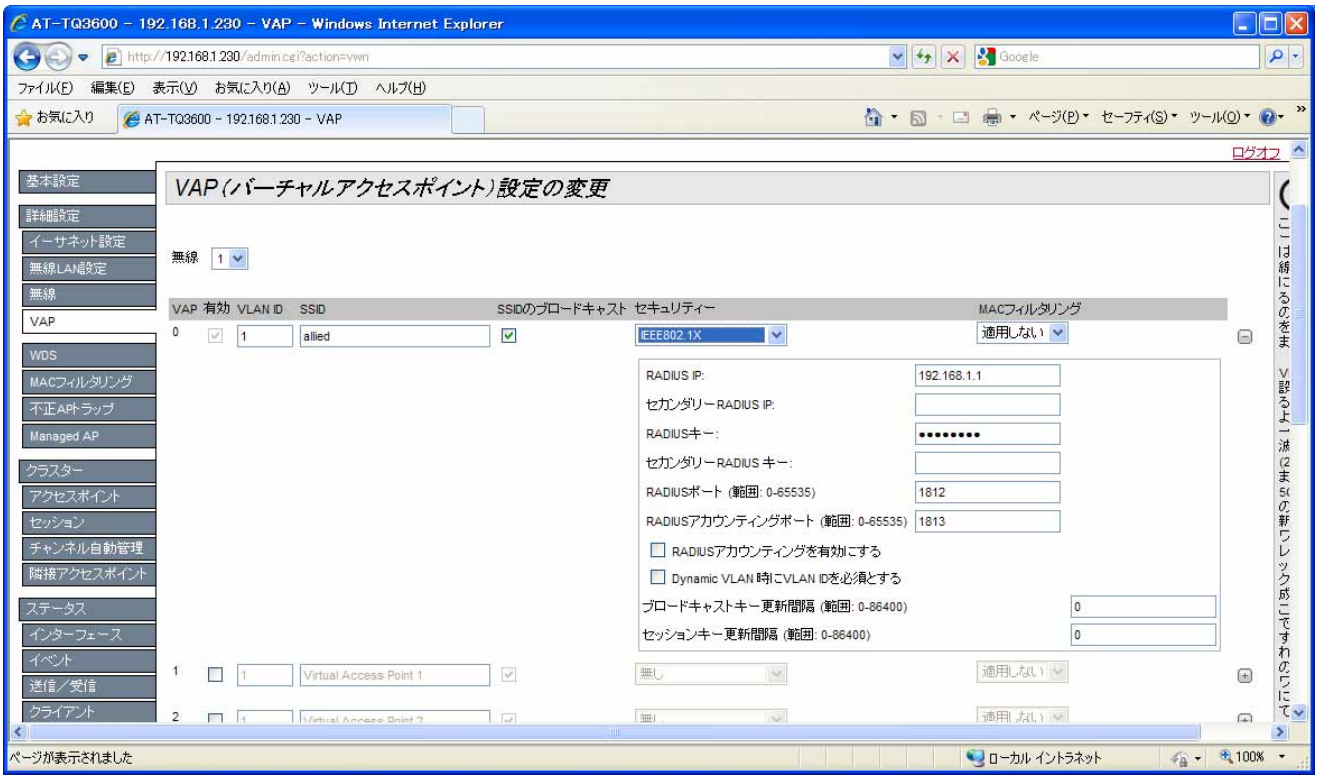
	この認証アルゴリズムは、「無し」「IEEE 802.1X」「WPA パーソナル」「WPA エンタープライズ」でも使用されます。 共有キー 無線クライアントがアクセスポイントに接続する際に、正しい WEP キーを要求します。 クライアントが誤った WEP キーを持っている場合、アクセスポイントに接続できません。 「オープンシステム」と「共有キー」の両方の選択 「共有キー」を使うように設定された無線クライアントは、有効な WEP キーを持っていれば、アクセスポイントに接続できます。 「オープンシステム」として WEP キーを使用するように設定された無線クライアントは（共有キーは無効）、アクセスポイントに接続できます。

表 6: スタティック WEP

IEEE 802.1X

「IEEE 802.1X」は、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 キーはセッションキー更新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」の使用をおすすめします。

✎ 「無線 LAN 設定」画面または「無線」画面で IEEE 802.11n を含む通信モードが選択されているとき、「セキュリティー」プルダウンメニューに「IEEE 802.1X」は表示されません。



項目名	説明
RADIUS IP	プライマリーとして使用する RADIUS サーバーの IP アドレスを入力します。 デフォルトは「192.168.1.1」です。
セカンダリー RADIUS IP	セカンダリーとして使用する RADIUS サーバーの IP アドレスを入力します。セカンダリー RADIUS サーバーを使用しない場合は空欄にします。
RADIUS キー	プライマリー 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。空白が許されます。デフォルトは「secret」です。
セカンダリー RADIUS キー	セカンダリー 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。空白が許されます。
RADIUS ポート	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 0～65535 の範囲で入力します。デフォルトは「1812」です。
RADIUS アカウンティングポート	プライマリー、セカンダリーそれぞれの外部 RADIUS サーバーのアカウンティングポートのポート番号を 0～65535 の範囲で入力します。デフォルトは「1813」です。

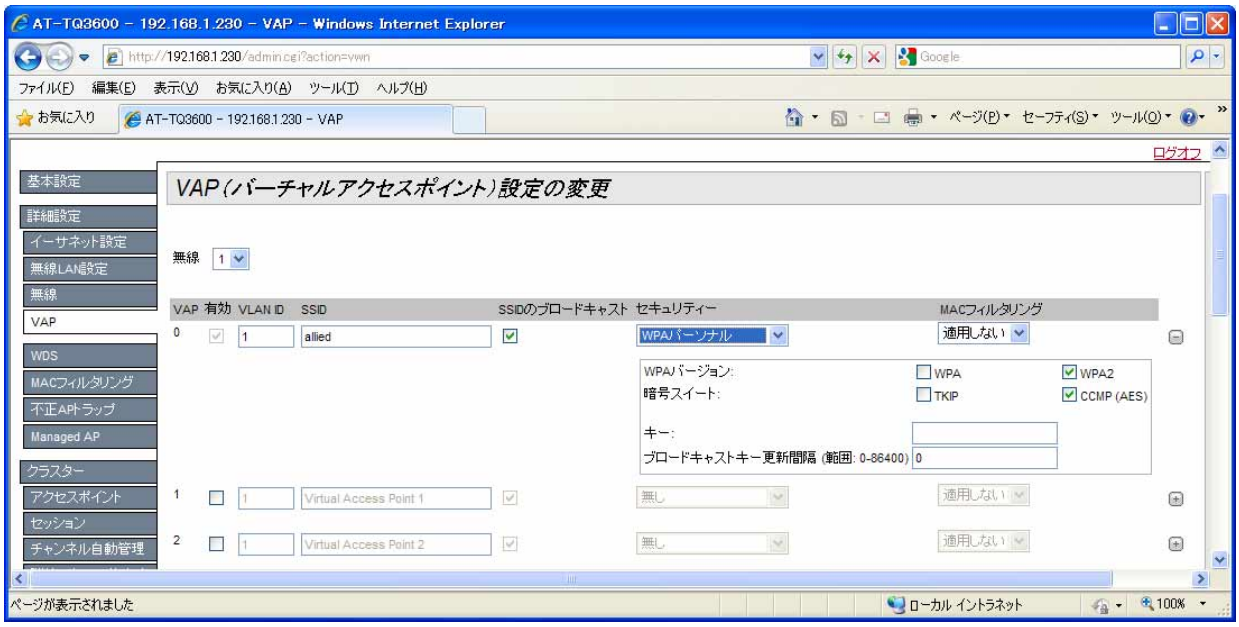
RADIUS アカウンティングを有効にする	「チェックあり」にすると、ユーザーを認証した外部のRADIUS サーバーを使用して、ユーザーがセッション中に使用したリソース（使用時間など）を記録することができます。デフォルトは「チェックなし」です。
Dynamic VLAN 時に VLAN ID を必須とする	「チェックあり」にすると、アクセスポイントがDynamic VLAN モードのときに、RADIUS サーバーからの認証応答に VLAN ID が含まれていなければ、その認証要求を行った無線クライアントの通信を禁止します。デフォルトは「チェックなし」です。
ブロードキャストキー更新間隔	VAP に接続している無線クライアントに送信するブロードキャストパケットのキーの更新間隔を設定します。 0～86400（秒）が入力できます。「0」は、キーを更新しません。デフォルトは「0」です。
セッションキー更新間隔	VAP に接続している無線クライアントの各々に送信するユニキャストのセッションキーの更新間隔を設定します。 0～86400（秒）が入力できます。「0」は、セッションキーを更新しません。デフォルトは「0」です。 キーは、セッションごとに新たに生成されますので、「WPA エンタープライズ」で CCMP（AES）のような強力な暗号を使用している場合、更新はほぼ不要です。更新間隔を短くすると、本製品の処理速度を低下させます。

表 7: IEEE 802.1X

✎ RADIUS サーバーがセカンダリーに切り替わった後、プライマリーに戻るためには次の条件が必要です。（1）本製品が、セカンダリー RADIUS サーバーはダウンしていると判断した場合（2）本製品の再起動

WPA パーソナル

「WPA パーソナル」は、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し、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。

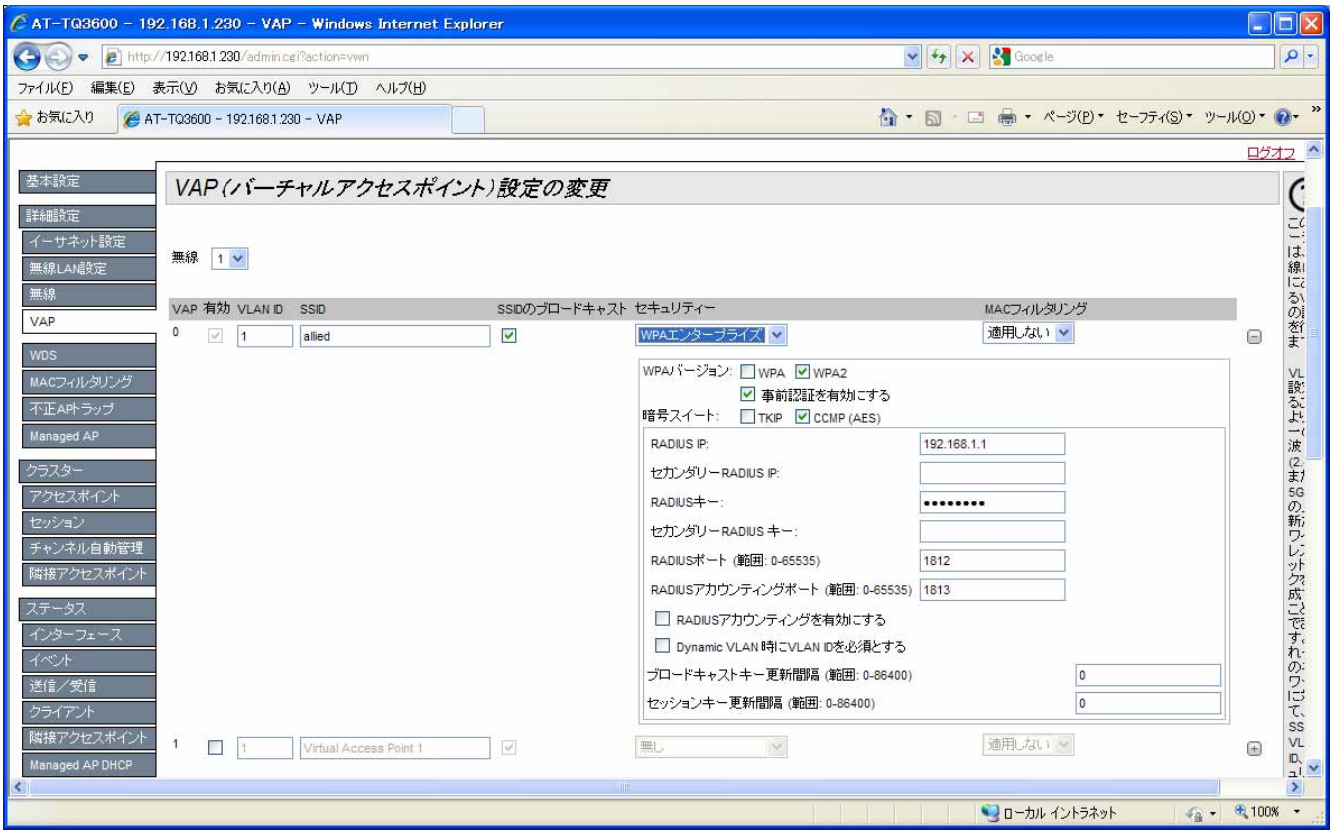


項目名	説明
WPA バージョン	次の WPA エンタープライズの項を参照してください。
暗号スイート	次の WPA エンタープライズの項を参照してください。
キー	暗号キーを設定します。8～63 文字の半角英数記号を入力します。 大文字、小文字は区別されます。
ブロードキャストキー更新間隔	VAP に接続している無線クライアントに送信するブロードキャストパケットのキーの更新間隔を設定します。 0～86400（秒）が入力できます。「0」は、キーを更新しません。デフォルトは「0」です。

表 8: WPA パーソナル

WPA エンタープライズ

「WPA エンタープライズ」は、RADIUS サーバーで無線クライアント個別のキーを生成し、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。RADIUS サーバーに関する設定の詳細は、「IEEE 802.1X」を参照してください。



項目名	説明
WPA バージョン	使用するバージョンにチェックを入れてください。デフォルトは「WPA2」です。可能であるなら「WPA2」のみを選択することをおすすめします。 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 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。 WPA と WPA2 が混在する環境では、両方を選択します。無線ネットワークから見たセキュリティーは、WPA と同じレベルになります。 （注）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。
事前認証を有効にする	「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。デフォルトでは「チェックあり」です。 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。
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「CCMP（AES）」です。 「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、新たなものに変更されます。 「CCMP（AES）」は、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。「無線 LAN 設定」画面または「無線」画面で IEEE 802.11n を含む通信モードが選択されているとき、「CCMP（AES）」をオフにすることはできません。 （注）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。

表 9: WPA エンタープライズ

セキュリティー

「VAP」を参照してください。

WDS

WDS（Wireless Distribution System）は、無線通信でアクセスポイント間をブリッジする機能です。この機能により、LAN 同士の接続や、無線サービスエリアの拡大が可能となります。

✎ イーサネットポートで受信した EAP/BPDU（L2 control）フレームは WDS 接続で転送されません。

✎ 無線コントローラーで WDS 接続を管理する場合は、この画面で何も設定しないでください。

以下の点に注意して、設定してください。

- WDS 接続の対となる 2 台のアクセスポイントのそれぞれで WDS の設定をしてください。
- 最大 4 台まで WDS 接続相手を設定することができます。
- WDS 接続を行うもの同士は、同一機種のアクセスポイントにしてください（AT-TQ2450 同士または AT-TQ3600 同士）。
- WDS 接続を行うもの同士は、同一の IEEE 802.11 モード、同一の無線チャンネルを設定してください。
- WDS で接続しているもの同士は、多重に WDS 接続することはできません（複数のリモートアドレス欄に、同一の MAC アドレスを入力しないでください）。
- WDS ブリッジ単独でも、イーサネットと WDS ブリッジの組み合わせのどちらにおいても、ループを作らない構成にしてください。

WDS と下記の機能の併用はおすすめいたしません。

- クラスター機能

  ✎ WDS 接続は、有線接続と比較して通信速度や信頼性が劣ります。クラスターで共有する情報が WDS 接続を経由してやりとりされるため、その情報共有（同期）が確実に行われない可能性があります。

WDS 接続の設定

1. 「無線」で「1」（2.4GHz 帯）または「2」（5GHz 帯）を選択します。

   ✎ 「無線」で「2」を選択する場合、W52 のチャンネル（36 40 44 48）に設定してください。W53 と W56 の周波数帯域はレーダーによっても使用されています。Auto、W53 のチャンネル（52 56 60 64）、W56 のチャンネル（100 104 108 112 116 120 124 128 132 136 140）に設定すると、レーダーとの干渉を自動的に回避する機能 DFS（Dynamic Frequency Selection）が働いたときにチャンネルが変更され、WDS 間の接続が切断されることがあります。

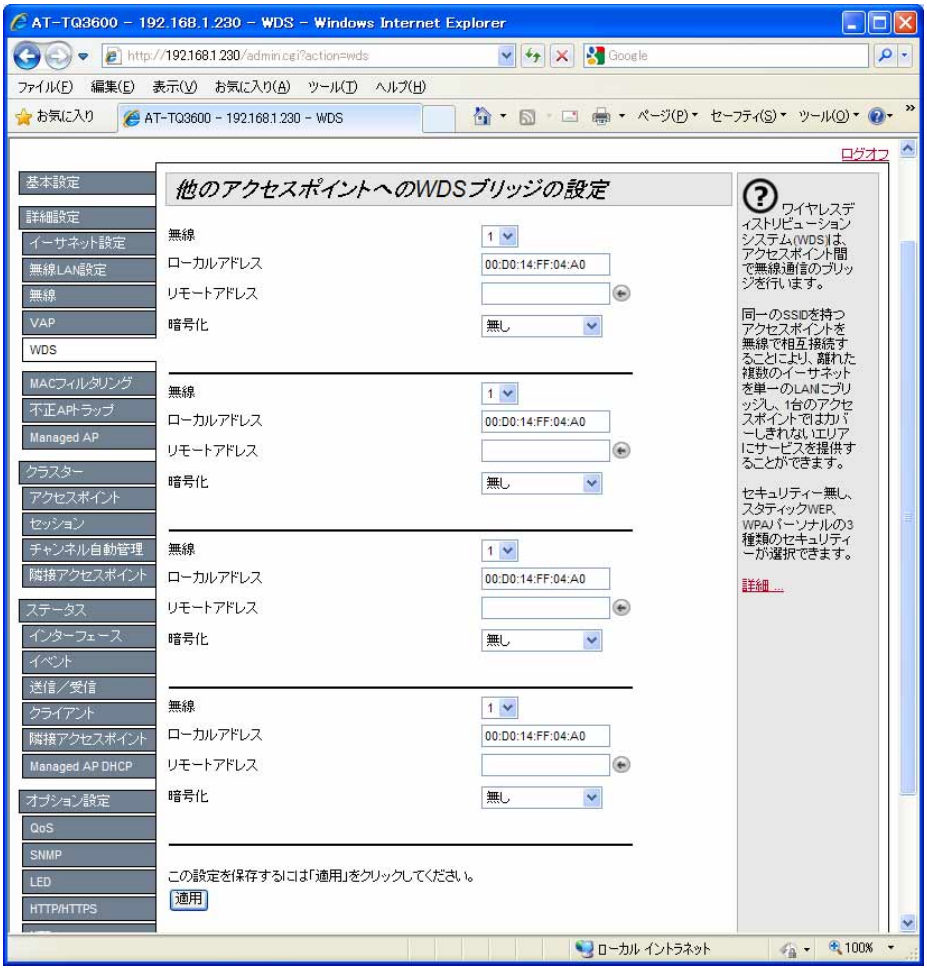
2. 「リモートアドレス」に接続相手の MAC アドレスを入力します。「隣接アクセスポイントの表示」が「有効」に設定されていれば、「←」のクリックでリストから選択できます。

   ✎ 「ステータス」/「隣接アクセスポイント」画面で「隣接アクセスポイントの表示」を有効にできます。

3. 暗号化の認証方式を選択します。「WPA パーソナル」をおすすめします。

   ✎ 「暗号化」で「WPA パーソナル」を選択する場合は、「詳細設定」/「VAP」画面でご使用になる無線帯域（1 または 2）の「VAP0」の「セキュリティー」を「WPA パーソナル」または「WPA エンタープライズ」に設定してください。

4. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。
5. 接続相手の本製品に対しても、同様に設定します。



項目名	説明
無線	WDS で使用する無線バンドを選択します。 「1」は、2.4GHz 帯の無線を使用します。 「2」は、5GHz 帯の無線を使用します。
ローカルアドレス	本製品の MAC アドレス（無線 1 の VAP0 または無線 2 の VAP0 の MAC アドレス）が表示されます。
リモートアドレス	WDS を構成する他の無線アクセスポイントの MAC アドレスを入力します。 「ステータス」/「隣接アクセスポイント」画面で「アクセスポイントの検出」が「有効」の場合、入力欄の右の「←」ボタンをクリックすると、現在動作中の通信可能なアクセスポイントの選択リストが表示されます。

	「←」はトグルボタンになっており、クリックするごとに、リストの表示、非表示が切り替わります。
暗号化	WDS の通信における暗号化の認証方式を選択します。 「無し」は、暗号化を行いません。 「スタティック WEP」は、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。個別の認証は行いません。 「WPA パーソナル」は、共通の事前共有キーをもとに個別のキーを生成、アクセスポイント間で認証と暗号化を行います。WEP よりも強度の高い暗号化が可能です。 セキュリティー対策のためには、「WPA パーソナル」にすることをおすすめします。デフォルトは「無し」です。

表 10:

✎ 「無線 LAN 設定」画面または「無線」画面で IEEE 802.11n を含む通信モードが選択されているときに、「暗号化」の「スタティック WEP」はグレイアウトして選択できません。

スタティック WEP

「暗号化」で「スタティック WEP」を選択した場合、以下の項目を入力します。WDS を構成するもう一方のアクセスポイントにも同一の設定を施します。

項目名	説明
キーの長さ	WEP キーの強度を「64 ビット」「128 ビット」から選択します。デフォルトは「128 ビット」です。
キーのタイプ	WEP キーの生成方法を「ASCII」「16 進数」から選択します。デフォルトは「16 進数」です。
必要な文字数	「キーの長さ」と「キーのタイプ」の設定に合わせて、WEP キーに入力しなければならない文字数が表示されます。
WEP キー	「キーのタイプ」が「ASCII」の場合は任意の半角英数記号で、「16 進数」の場合は 16 進数（0～9、A～F、a～f）で「必要な文字数」に表示された文字数の WEP キーを入力します。

表 11:

WPA パーソナル

「暗号化」で「WPA パーソナル」を選択した場合、以下の項目を入力します。WDS を構成するもう一方のアクセスポイントにも同一の設定を施します。

項目名	説明
SSID	WDS 接続で使用するネットワーク名（SSID）を 1～32 文字の半角英数記号で入力します。

キー	事前共有キーを 8～63 文字の半角英数記号で入力します。

表 12:

✎ 「暗号化」で「WPA パーソナル」を選択する場合は、「詳細設定」/「VAP」画面でご使用になる無線帯域（1 または 2）の「VAP0」の「セキュリティー」を「WPA パーソナル」または「WPA エンタープライズ」に設定してください。

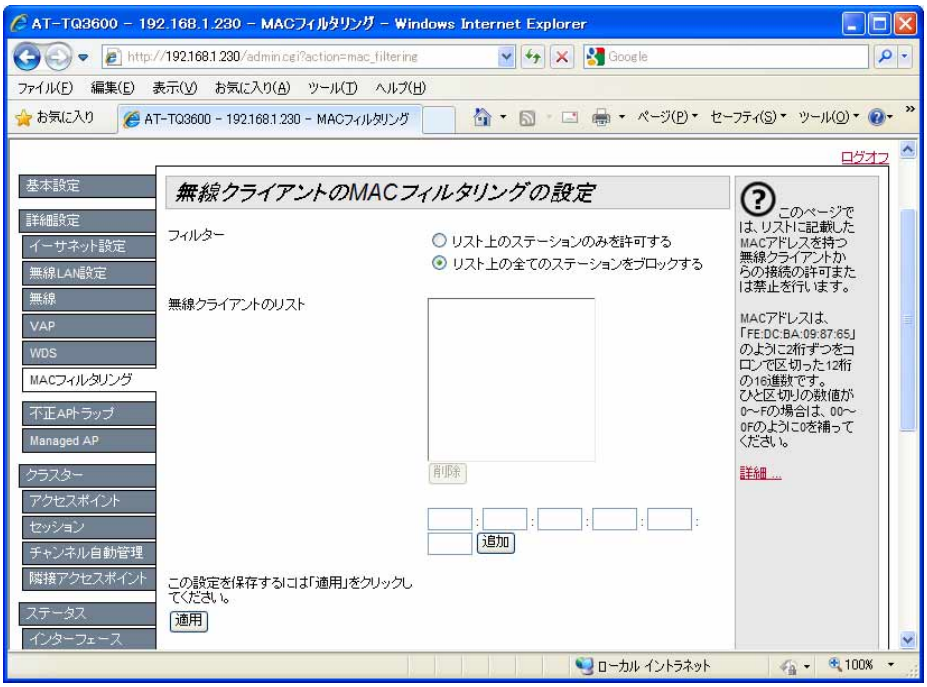
✎ WPA バージョンは WPA2、暗号スイートは CCMP（AES）です。

WDS 接続の解除

1. 「無線」で「1」（2.4GHz 帯）または「2」（5GHz 帯）を選択します。
2. 「リモートアドレス」に入力されている MAC アドレスを削除します。
3. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。
4. 接続相手の本製品に施した設定に対しても、同様にして削除します。

MAC フィルタリング

特定の MAC アドレスからの接続の許可または禁止を行うためのリストを作成します。このリストは、「VAP」画面（バーチャルアクセスポイント）で、VAP ごとに適用することができます。



項目名	説明
フィルター	「リスト上のステーションのみを許可する」は、指定した MAC アドレスからの接続のみを許可します。 「リスト上の全てのステーションをブロックする」は、指定した MAC アドレスからの接続を禁止します。 デフォルトは、「リスト上の全てのステーションをブロックする」です。
無線クライアントのリスト	フィルターを適用する MAC アドレスのリストです。1024 件まで登録できます。

表 13:

リストへの追加

1. 「無線クライアントのリスト」の下にある入力欄に MAC アドレスを 2 桁ごとに入力します。0～9、a～f、A～F が使用できます。1 桁の数値を入力した場合は、上位桁に「0」が補われます。
2. 12 桁を入力したら「追加」ボタンをクリックしてください。
3. 登録する MAC アドレスの数だけ 1～2 を繰り返してください。
4. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ 「追加」ボタンのクリックではセッションのタイマーが更新されません。たくさんのリストを追加するときは、「セッションタイムアウト」が満了する前に「適用」ボタンをクリックしてください。「セッションタイムアウト」は、「オプション設定」/「HTTP ／ HTTPS」画面で変更できます。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。

✎ マルチキャストアドレスとブロードキャストアドレスは登録できません。

リストからの削除

1. 「無線クライアントのリスト」の MAC アドレスを選択します。
2. 「削除」ボタンをクリックしてください。
3. 削除する MAC アドレスの数だけ 1～2 を繰り返してください。
4. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ 「適用」ボタンをクリックすると、変更した項目によっては、無線クライアントが一時的に切断されることがあります。アクセスポイントの設定の変更は、無線トラフィックが少ないときに行うことをおすすめします。

不正 AP トラップ

不正 AP トラップ機能は、「既知のアクセスポイントのリスト」に記述されていないアクセスポイントが検出されたとき、SNMP トラップを送信すると同時にイベントとして記録する機能です。ご購入時には、この機能は無効となっています。この機能を使用する場合は、次の手順を実行してください。

1. 「無線 1 での検出」または「無線 2 での検出」を「有効」に設定してください。
2. イベントとして記録しないアクセスポイントの MAC アドレスを設定します。手順は、下記の「リストへの追加」を参照してください。
3. 「適用」ボタンをクリックしてください。

✎ 「ステータス」/「イベント」、「ステータス」/「隣接アクセスポイント」に関連情報があります。

項目名	説明
無線 1 での検出	無線 1（2.4GHz 帯）で隣接するアクセスポイントの検出を行うか否か。検出する場合は「有効」、しない場合は「無効」を選択します。デフォルトは「無効」です。これは、「ステータス」の「隣接アクセスポイント」画面の「無線 1 での検出」と連動します。

無線 2 での検出	無線 2（5GHz 帯）で隣接するアクセスポイントの検出を行うか否か。検出する場合は「有効」、しない場合は「無効」を選択します。これは、「ステータス」の「隣接アクセスポイント」画面の「無線 2 での検出」と連動します。
検出間隔	不正アクセスポイントを検出する間隔を下記から選択します。デフォルトは「15 分」です。 15 分、30 分、1 時間、3 時間、5 時間、10 時間、1 日、1 週間、2 週間、4 週間
既知のアクセスポイントのリスト	イベントとして扱わないアクセスポイントのリストです。200 件まで登録できます。リストに何も登録されていないとき、不正 AP トラップ機能は無効になります。

表 14:

リストへの追加

1. 「既知のアクセスポイントのリスト」の下にある入力欄に MAC アドレスを 2 桁ごとに入力します。0～9、a～f、A～F が使用できます。1 桁の数値を入力した場合は、上位桁に「0」が補われます。
2. 12 桁を入力したら「追加」ボタンをクリックしてください。
3. 登録する MAC アドレスの数だけ 1～2 を繰り返してください。
4. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

✎ マルチキャストアドレスとブロードキャストアドレスは登録できません。

リストからの削除

1. 「既知のアクセスポイントのリスト」の MAC アドレスを選択します。
2. 「削除」ボタンをクリックしてください。
3. 削除する MAC アドレスの数だけ 1～2 を繰り返してください。
4. 「適用」ボタンをクリックしてください。設定は直ちに反映されます。

Managed AP

無線コントローラーの管理下に入れる

本製品は、次の 2 つのモードを持っています。

- 本製品のみで動作するモード：本製品は、単体のアクセスポイントまたはクラスターを構成するアクセスポイントとして動作します。本製品の設定は、本製品の Web 設定画面および SNMP で行います。
- Managed AP モード：本製品は、無線コントローラー（AT-UWC）の管理下で動作します。本製品の設定は、無線コントローラーで行います。本製品の Web 設定画面および SNMP は無効となります。

✎ Managed AP モードが「有効」のとき、本製品はイーサネットポートで無線コントローラーを検出し接続を試みます。接続に成功すると、本製品の Web 設定画面にはアクセスできなくなります。本製品のみで動作するモードに戻したい場合には、次の方法で無線コントローラーと接続できない状態にしてから Web 設定画面にアクセスしてください。・無線コントローラーが存在しないネットワークに本製品を移動する・無線コントローラーで対象のアクセスポイントを Standalone モードに変更する

無線コントローラーと本製品の接続を設定するには、次の 4 つの方法があります。

- 本製品に無線コントローラーの IP アドレスをスタティック登録する

✎ 本製品に無線コントローラーの IP アドレスをスタティック登録すると、それ以外の無線コントローラーの管理下に入ることはできなくなります。

- 無線コントローラーに本製品の IP アドレスを設定する
- DHCP オプションを用いて本製品に無線コントローラーの IP アドレスを通知する

✎ 「ステータス」/「Managed AP DHCP」に関連情報があります。

- 無線コントローラーと本製品を同一のサブネットに設置する（同一サブネットでは自動検出されます）

本製品に無線コントローラーの IP アドレスをスタティック登録する手順は次のとおりです。

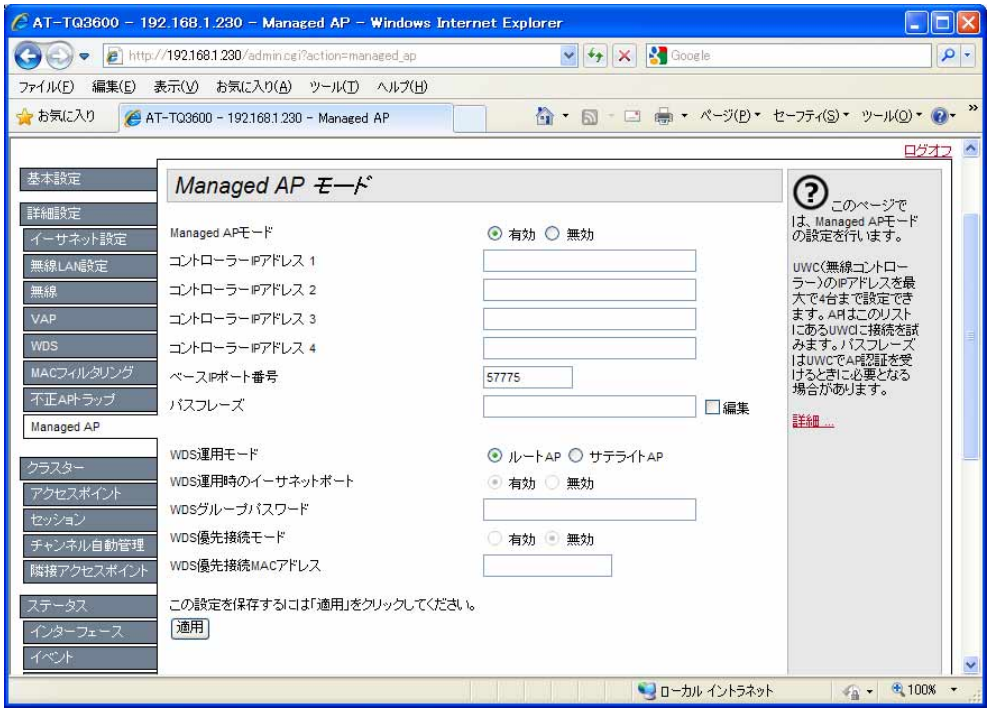
1. 「Managed AP モード」で「有効」を選択します。
2. 「コントローラー IP アドレス 1～4」を入力します。1 から順に入力してください。
3. 必要であれば「ベース IP ポート番号」を変更します。
4. 「編集」にチェックを入れ、「パスフレーズ」を入力します。

✎ 同じパスフレーズを無線コントローラーに設定しておく必要があります。パスフレーズは空欄が許されます。

5. 「適用」ボタンをクリックします。

✎ 「適用」ボタンをクリックすると、「編集」のチェックは自動的に外れます。

✎ パスフレーズの削除は、「編集」にチェックを入れて入力文字列を削除し「適用」をクリックします。



項目名	説明
Managed AP モード	無線コントローラーの管理下に入るか否か。管理下に入る場合は「有効」を、入らない場合は「無効」を選択します。デフォルトは「有効」です。
コントローラー IP アドレス 1～4	本製品の無線コントローラーとなるホスト名または IP アドレスです。4 つまで登録できます。本製品はリストの 1 から順に接続を試み、接続が成功した時点でその無線コントローラーの管理下に入ります。ホスト名（FQDN）は、64 文字までの半角英数字、ハイフン、ピリオドが使用できます。FQDN は、半角英数字で始まらなければなりません（数値で始まるホスト名が許されます）。また、末尾はハイフンかドット以外でなければなりません。（例）uwc.your.domain.com、192.168.1.1
ベース IP ポート番号	本製品が無線コントローラーとの通信に使用する TCP/UDP ポート番号です。1 から 65000 までの値を設定できます。ここで設定したポートから 10 個の連続した TCP/UDP ポート番号が使用されます。デフォルトは「57775」です（57775～57784 までを使用します）。
パスフレーズ	無線コントローラーで機器認証を受けるためのパスフレーズです。8～63 文字までの半角英数字が入力できます。入力文字は●で表示されます。

表 15:

無線コントローラー管理下の WDS 接続

無線コントローラーの管理下で WDS 接続を使用する場合は、次の項目を設定してください。

✎ 無線コントローラー管理下でWDS接続を使用する場合は、「詳細設定」/「WDS」画面で何も設定しないでください。

項目名	説明
WDS運用モード	無線コントローラーの管理下にあるアクセスポイントが次のどちらであるかを指定します。 「ルートAP」は、イーサネットポートを介して無線コントローラーと通信を行うモードです。イーサネットポート側に無線コントローラーがある場合はこちらを選択してください。無線コントローラーを使用しない場合は、必ずルートAPを選択してください。 「サテライトAP」は、WDS接続を経由して無線コントローラーと通信を行うモードです。イーサネットポート側に無線コントローラーがない場合はこちらを選択してください。このモードにすることにより、サテライトAPは接続可能なルートAPを探索して、WDS接続を確立します。これを選択すると、次の「WDS運用時のイーサネットポート」「WDSグループパスワード」「WDS優先接続モード」「WDS優先接続MACアドレス」が設定可能となります。 デフォルトは「ルートAP」です。
WDS運用時のイーサネットポート	サテライトAPが無線コントローラーの管理下に入ったとき、イーサネットポートを有効にするか否か。サテライトAPでイーサネットポートを使う場合は「有効」に、使わない場合は必ず「無効」に設定してください。デフォルトは「有効」です。ルートAPに設定されているアクセスポイントでは、この設定は常に「有効」となります。
WDSグループパスワード	サテライトAPが、WDS接続確立の際に使うWPA2パーソナル認証のパスワードです。ルートAPは、無線コントローラーの管理下に入ったとき、無線コントローラーからパスワードを得ます（無線コントローラーにパスワードを設定しておきます）。
WDS優先接続モード	「WDS優先接続モード」を「有効」にするか否か。「有効」にすると、次の「WDS優先接続MACアドレス」に入力したMACアドレスを持つアクセスポイントとのWDS接続の試行を優先することによりWDS接続確立までの時間を短縮します。「無効」にすると、探索したアクセスポイントに対して順にWDS接続を試みます。デフォルトは「無効」です。
WDS優先接続MACアドレス	サテライトAPの接続相手となるルートAPの無線インターフェースのMACアドレスを入力します。入力するMACアドレスは、WDS接続に「無線1」「無線2」のどちらを使用するかによって異なります。「ルートAP」の「ステータス」/「インターフェース」画面で確認してください。「WDS優先接続モード」が「有効」のとき、この項目は入力（変更）できます。「WDS優先接続モード」が「無効」のとき、この項目は無視されます。

表 16:

✎ 「WDS 運用モード」を「サテライト AP」に設定する前に、あらかじめ「詳細設定」/「VAP」画面の「無線 1」「無線 2」の「VAP0」の「セキュリティー」で「WPA パーソナル」を選択し「キー」を設定してください。「WDS 運用モード」を「サテライト AP」にすると、「無線 1」「無線 2」の「ステータス」が自動的に「オン」になります。「VAP0」のデフォルトはセキュリティーなしです。「VAP0」にダミーのキーを設定して、ルート AP との WDS 接続が確立するまでと、その後無線コントローラーの管理下に入るまでの間のセキュリティーを確保してください。

✎ 「WDS 運用モード」を「サテライト AP」に設定する場合は、「詳細設定」/「無線」画面の内容をデフォルトのまま変更しないでください。