613-001479 Rev.Q 160502

AT-TQ2450 リリースノート

この度は、AT-TQ2450 をお買いあげいただき、誠にありがとうございます。
このリリースノートは、マニュアルに記載されていない内容や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。
最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1　ファームウェアバージョン　3.2.1

2　本バージョンで追加・拡張された項目

ファームウェアバージョン 3.1.3 から 3.2.1 へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1　SNMP トラップ /Syslog 送信機能

レーダー検出時に SNMP トラップ /Syslog 送信機能をサポートしました。
「オプション設定＞ SNMP」ページの「生成トラップ」項目において設定できます。

2.2　「ステータス＞インターフェース」ページ

「ステータス＞インターフェース」ページにおいて以下の項目を追加しました。

- 通信速度（イーサネットのリンク速度 1000/100/10）
- デュプレックスモード（イーサネットのデュプレックスモード full/half）
- 使用帯域幅（無線ページで設定されている帯域幅）
- DFS ステータス（現在の DFS の状態）

2.3　WDS の信号強度表示機能

WDS の信号強度表示機能をサポートしました。接続相手から受信した信号の強度をアイコンと数値（単位は dBm）で表示します。

2.4　Syslog

クライアントが接続を試みるときに送信される Syslog（Assoc Request）メッセージに、クライアントの信号強度を追加しました。

2.5　AT-UWC V.3.2.0

AT-UWC V.3.2.0 で管理できるようになりました。

2.6　AMF Guest node

AlliedWare Plus バージョン 5.4.6-0.1 の AMF ゲストノードをサポートしました。

3　本バージョンで仕様変更された機能

ファームウェアバージョン **3.1.3** から **3.2.1** へのバージョンアップにおいて、以下の仕様変更が行われました。

3.1　Web GUI ラベルの変更

Web GUI の「詳細設定 >VAP」のラベルを「詳細設定 >VAP/ セキュリティー」に変更しました。

3.2　「詳細設定 > 無線」

送信出力の表示を「デフォルト設定は 100%」から「最大」に変更し、「最大>強>中>弱>最弱」の中から設定できるようになりました。

4　本バージョンで修正された項目

ファームウェアバージョン **3.1.3** から **3.2.1** へのバージョンアップにおいて、以下の項目が修正されました。

4.1　「詳細設定 / イーサネット設定」ページの「DNS ネームサーバー」が「ダイナミック」に設定されている状況において、再起動後に SNMP 経由の情報取得が行えない場合がありましたが、これを修正しました。

4.2　AT-UWC 管理下で、「WDS 優先接続モード」が有効のときに「WDS 優先接続 MAC アドレス」のアクセスポイントを発見できなかった場合、「ステータス / イベント」に「Priority Connection AP not found. Disable WDS Priority Connection Mode.」のログが表示されていませんでしたが、これを修正しました。

4.3　AT-UWC 管理下で、RADIUS サーバーを使用した MAC アドレス認証を行っている環境において、アクセスポイント (AP) が AT-UWC 管理下から離れた場合、AP が RADIUS サーバーに対して意図しない MAC 認証のパケットを送信していましたが、これを修正しました。

4.4　「VAP」画面の無線 2（5GHz 帯）の「セキュリティー」の変更について、特定の手順で変更を行わないとビーコンが停止する場合がありましたが、これを修正しました。

4.5　ひとつまたは複数の VAP が有効に設定されている場合に、そのうちのひとつでも「バンドステアリング」を有効にするときは、有効に設定されている全ての VAP の「SSID のブロードキャスト」を有効にする必要がありましたが、これを修正しました。

4.6　AT-UWC 管理下で、WDS のサテライト AP に設定する WDS グループパスワードは、バックアップファイルとしてダウンロードを行ったコンフィグファイルに保存されませんでしたが、これを修正しました。

4.7　「Managed AP」画面の「パスフレーズ」を一度設定すると、設定したパスフレーズを削除することができませんでしたが、これを修正しました。

4.8 ファームウェア V.2.x.x から V.3.x.x にアップグレード、またはファームウェア V.3.x.x に V.2.x.x 以前で作成した設定ファイルをリストアしていた状態で、ファームウェア V.3.x.x で作成した設定ファイル (※) をリストアした場合に設定ファイルのリストアに失敗していましたが、これを修正しました。
※ V.3.x.x の工場出荷時設定から作成された設定ファイル

5 本バージョンでの制限事項

ファームウェアバージョン **3.2.1** には、以下の制限事項があります。

5.1 VAP

参照 「リファレンスマニュアル」/「詳細設定」/「VAP」

○ ダイナミック VLAN（WPA エンタープライズ）環境で、無線クライアントの検疫を実行するように RADIUS サーバーが設定されている場合、無線クライアントに VLAN 間ローミングが発生すると、無線クライアントの認証に失敗することがあります。

○ 無線クライアントがアクセスポイントから切断して 3 秒以内に再接続すると、RADIUS アカウンティングパケットに設定されるセッション ID が更新されません。

5.2 MAC フィルタリング

参照 「リファレンスマニュアル」/「詳細設定」/「MAC フィルタリング」

MAC フィルタリング機能の「リスト上の全てのステーションをブロックする」フィルターと WDS の併用はできません。併用すると WDS のリンクが切断されてしまいます。WDS と MAC フィルタリングを併用する場合は、「リスト上のステーションのみを許可する」を選択し、無線クライアントのリストに対向アクセスポイントの MAC アドレスを追加してください。

5.3 クラスター

参照 「リファレンスマニュアル」/「クラスター」/「アクセスポイント」
参照 「リファレンスマニュアル」/「クラスター」/「隣接アクセスポイント」

○ クラスター機能において、ひとつのクラスターに所属可能なアクセスポイント数を超える台数（17 台以上）を追加すると、画面上では 17 台目以降の情報は表示されませんが、追加したアクセスポイントでクラスターの設定が共有されたり、誤動作を起こしたりすることがあります。

○ クラスター機能は、異機種間、異なるファームウェアバージョン間での使用や、WDS 機能との併用はできません。

○ 「クラスター」/「隣接アクセスポイント」画面の「隣接アクセスポイントの表示」を「クラスターメンバーのみ」にすると、クラスターメンバーの VAP0 の SSID だけが表示されます。「クラスターメンバー以外」にすると、クラスターメンバーの VAP1 ～ 15 の SSID が表示されます。

5.4 送信 / 受信

参照「リファレンスマニュアル」/「ステータス」/「送信 / 受信」

起動の際に、VAP インターフェースの送信カウンターがカウントアップしますが、表示のみで実際にはパケットを送信していません。

5.5 SNMP

参照「リファレンスマニュアル」/「オプション設定」/「SNMP」

SNMP の設定において、「SNMP SET リクエストの許可」は未サポートです。

5.6 V.1.2.0 からのアップグレード

参照「リファレンスマニュアル」/「保守管理」/「アップグレード」

「アップグレード」画面の「切り替え」ボタンを使用して、V.1.2.0 以前のファームウェアから V.2.0.1 ～ V.2.0.8 のファームウェアへの切り替え（アップグレード）を行うと、次の項目が無効となります。切り替え後にこれらの項目を設定してください。詳細は、リファレンスマニュアルのそれぞれの項目を参照してください。

- 「詳細設定」/「無線」画面の「MCS（データレート）設定」
- 「詳細設定」/「Managed AP」画面の「WDS 運用モード」「WDS 運用時のイーサネットポート」

6 ファームウェアのアップグレードにおけるご注意

重要：アップグレード中は、本製品の無線機能が停止します。アップグレードは、必ず有線 LAN ポートに接続したコンピューターから実行してください。
また、アップグレード中は、本製品の Web 設定画面へのアクセスや、有線 LAN ポートへのトラフィック流入をできるだけ避けてください。

※ V.1.x.x から直接 V.**3.2.1** へファームウェアをアップグレードすることは未サポートです。V.2.x.x にアップグレードした後で、再度 V.**3.2.1** にアップグレードしてください。

6.1 V.1.0.0 → V.1.1.6 以降へのアップグレード

参照「リファレンスマニュアル」/「保守管理」/「アップグレード」

ファームウェア V.1.0.0 から V.1.1.6 以降へのアップグレードは、まず V.1.0.0 から V.1.1.5 にアップグレードし、引き続き V.1.1.5 から V.1.1.6 以降にアップグレードしてください。

直接、ファームウェア V.1.0.0 から V.1.1.6 以降へのアップグレードを行わないでください。これを行うと、ファームウェアが正常に更新されません。これを行ってしまった場合は、この状態から V.1.1.5 にアップグレードし、その後 V.1.1.6 以降にアップグレードしてください。

ファームウェアは、弊社ホームページからダウンロードしてください。

http://www.allied-telesis.co.jp/

6.2 V.1.1.0 ～ 1.2.0 → V.2.0.8 へのアップグレード

参照 「リファレンスマニュアル」/「保守管理」/「アップグレード」

アップグレード前の通信モードが IEEE 802.11n を含む場合、VAP のセキュリティー設定が「スタティック WEP」や「IEEE 802.1X」に設定されていると、V.2.0.8 へのアップグレードによって VAP のセキュリティー設定が「無し」に変更されます。

アップグレード前に、セキュリティー設定を「WPA パーソナル」や「WPA エンタープライズ」に変更し、それに合わせて無線クライアントのセキュリティー設定も変更してください。「スタティック WEP」や「IEEE 802.1X」には脆弱性があります。強力なセキュリティーの「WPA パーソナル」や「WPA エンタープライズ」の使用をおすすめいたします。
アップグレード後に、セキュリティー設定を「WPA パーソナル」や「WPA エンタープライズ」に変更することもできますが、一時的にセキュリティー設定が「無し」となるためおすすめいたしません。

アップグレード後も「スタティック WEP」や「IEEE 802.1X」をご使用になりたい場合は、アップグレード前に IEEE 802.11n を含まない通信モードに変更してください。

6.3 V.2.0.x → V.3.2.1 へのアップグレード

参照 「リファレンスマニュアル」/「保守管理」/「アップグレード」

無線セキュリティー設定を WPA のみで選択した状態のファームウェアを V.**3.2.1** にアップグレードすると、無線セキュリティーの WPA2 と CCMP（AES）が自動的に有効になります。（チェックを外せません）

7 マニュアルの補足

最新リファレンスマニュアルの補足事項です。

7.1 保守管理 / アップグレード

参照 「リファレンスマニュアル」/「保守管理」/「アップグレード」

V.2.0.0 以降のファームウェアでは、V.2.0.0 以降の任意のファームウェアバージョンの間でアップグレードとダウングレードが可能です。ただし、設定ファイルに下位互換性はありませんので、アップグレード後に前バージョンに戻す可能性がある場合は、アップグレードを行う前に、「保守管理」/「設定」画面で設定ファイルをバックアップしてください。

8 リファレンスマニュアルについて

最新のリファレンスマニュアル（613-001965 Rev.F）は弊社ホームページに掲載されています。本リリースノートは、上記のリファレンスマニュアルに対応した内容になっていますので、お手持ちのリファレンスマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/