613-001479 Rev.M 150717

Allied Telesis

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　3.1.0

2　本バージョンで追加・拡張された機能

ファームウェアバージョン **2.0.8** から **3.1.0** 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　Internet Explorer

対応 Web ブラウザーに Internet Explorer 10、11 を追加しました。

2.2　RADIUS サーバー

対応 RADIUS サーバーに Windows Server 2012 R2 を追加しました。

2.3　ファシリティー

ファシリティー選択機能をサポート。ファシリティー選択機能を使用することにより、Syslog サーバーに送信するログのファシリティーを選択できます。V.2.0.8 以前の AT-TQ2403 互換モードは本機能に統合しました。

2.4　バンドステアリング

バンドステアリング機能をサポート。バンドステアリング機能を使用することにより、5GHz 帯への接続を優先するようになり 2.4GHz 帯の混雑を解消します。

2.5　異機種間での WDS 接続

AT-TQ シリーズ（AT-TQ4600、AT-TQ4400、AT-TQ3600、AT-TQ3400、AT-TQ3200、AT-TQ2450）間での WDS 接続に対応しました。なお、WDS 接続には、次の条件を満たす必要があります。

- 同一ファームウェアバージョン
- 同一の無線チャンネル
- 同一の IEEE 802.11 無線モード（11a/n と 11a/n/ac の組み合わせは可）

2.6　クラスター、NTP

クラスター機能と NTP 機能の併用をサポートしました。

2.7 ステータス

WDS のインターフェース状態の表示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 **2.0.8** から **3.1.0** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 EAP message フレーム

参照 「リファレンスマニュアル」/ オプション設定 /SNMP

本製品が送信する EAP message フレームの ID を常時 0 から開始していましたが、セキュリティー強化のためランダムな値（0 から 255）を付与するように変更しました。

3.2 WPA バージョン、暗号スイート

参照 「リファレンスマニュアル」/ 詳細設定 /VAP

V.2.0.x で無線セキュリティー設定を WPA のみ選択していた場合に、V.3.1.0 へアップグレードすると、無線セキュリティーの WPA2 と CCMP（AES）が自動で有効になります。WPA のみ、TKIP のみの設定は本製品上では行えません。これらの設定変更は AT-UWC 管理下でのみ行えます。

3.3 QoS APSD サポート機能のデフォルト設定の変更

参照 「リファレンスマニュアル」/ オプション設定 /QoS

QoS の設定において、「APSD サポート」のデフォルト設定を「オフ」に変更しました。なお、APSD サポート機能はサポート対象外です。

3.4 パラメーターの入力文字制限の解除

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、「Read Only のコミュニティー名」、「Read/Write のコミュニティー名」、「トラップのコミュニティー名」に「"」（ダブルクオート）「'」（シングルクオート）「\」（円マークまたはバックスラッシュ）「&」「<」「>」が使用可能になりました。

3.5 AT-UWC

参照 「AT-UWC リファレンスマニュアル」/ オプション設定 /SNMP

AT-UWC 管理下での SNMP の動作をアクセスポイントの設定に従うよう変更しました。

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 **2.0.8** から **3.1.0** 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 RADIUS アカウンティングパケットに設定するセッション ID（Acc-Session-Id）が 000000-000000 固定となっていましたが、これを RFC2866 推奨の実装に修正しました。

4.2 NTP サーバーと時刻同期した際に、使用する Syslog サーバーの仕様によって出力するログメッセージが途中で改行されて表示される場合がありましたが、これを修正しました。

4.3 リンクパートナーの Pause 制御が有効と設定された状態で、有線ポートが 10M Full でリンクアップした際に、フローコントロール機能が正常に動作しない場合がありましたが、これを修正しました。

4.4 AT-TQ2450 に接続されている端末において、まれに無線切断が発生する場合がありましたが、これを修正しました。

4.5 VAP 設定画面で「ブロードキャストキー更新間隔」だけを「0」から他の値に設定変更した場合に、設定が正しく反映されず再起動が必要でしたが、これを修正しました。

4.6 MAC フィルタリング機能により接続を拒否したときに送出される SNMP トラップの atkkWiAcClient80211Spec の値が正しく表示されないことがありましたが、これを修正しました。

4.7 ごくまれに SNMP 設定を変更した際に、Coldstart Trap を送信してしまう場合がありましたが、起動時のみ送信するよう修正しました。

4.8 一旦 WDS の設定を行うと、その WDS の設定を削除しても「ステータス」/「送信／受信」ページの WDS インターフェースのステータスに「up」と表示されてしまう場合がありましたが、これを修正しました。

4.9 無線クライアントが接続していない場合でも、「送信／受信」の無線インターフェースの送信カウンターが増加していましたが、これを修正しました。

4.10 WDS リンクを構成している無線インターフェースに無線クライアントが 1 台も接続していない状態となった場合に、WDS リンク情報が削除され WDS リンクが構成できなくなることがありましたが、これを修正しました。

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 **3.1.0** 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 WDS 多段接続

参照「リファレンスマニュアル」/「詳細設定」/「WDS」

多段で WDS 構成をする場合は、3 台程度での構成を推奨します。4 台以上の多段接続は未サポートです。

AP --（WDS）-- AP --（WDS）-- AP

注意：アクセスポイント（AP）を何段も経由するとスループットが低下するため、導入の際は実環境にて事前調査を行うことを推奨します。

5.3 WDS

参照「リファレンスマニュアル」/「詳細設定」/「WDS」

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。
設定情報を筐体 A からダウンロードして筐体 B にリストアする場合は、WDS のサテライト AP に設定する WDS グループパスワードを再設定してください。

5.4 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。

5.5 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」

○ 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。

5.6 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。

5.7 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。

5.8 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.3.1.0 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.3.1.0 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「IEEE802.1X」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「IEEE802.1X」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「IEEE802.1X」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.3.1.0 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」

無線セキュリティ設定を WPA のみで選択した状態のファームウェアを V.3.1.0 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 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.D）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/