



最初にお読みください

# AT-TQ2450 リリースノート

この度は、AT-TQ2450 をご購入いただき、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 3.1.2

## 2 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 **3.1.0** から **3.1.2** 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。

- 2.1 アクセスポイント起動時に NTP パケットが送信されず、起動してすぐに時刻同期ができなかったことがありましたが、これを修正しました。
- 2.2 特定のパターンを含むフレームを受信するとリポートすることがありましたが、これを修正しました。

## 3 本バージョンでの制限事項

ファームウェアバージョン **3.1.2** には、以下の制限事項があります。

### 3.1 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。
- 「VAP」画面の無線 2 (5GHz 帯) の「セキュリティ」の変更は、次のいずれかの手順で行ってください。この手順で行わないと、ピーコンが停止することがあります。
  - (1) セキュリティ設定を変更します。「無線 LAN 設定」画面の「無線 2」を「オフ」にして「適用」ボタンをクリックします。再度「無線 2」を「オン」にして「適用」ボタンをクリックします。
  - (2) 「無線 LAN 設定」画面の「無線 2」を「オフ」にして「適用」ボタンをクリックします。セキュリティ設定を変更します。再度「無線 2」を「オン」にして「適用」ボタンをクリックします。
  - (3) セキュリティ設定を変更したらアクセスポイントを再起動します。

- 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すべての VAP の「SSID のブロードキャスト」を有効にしてください。

---

## 3.2 WDS 多段接続

 [「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。

---


## 3.3 WDS

 [「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。

---


## 3.4 MAC フィルタリング

 [「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。

---


## 3.5 Managed AP

 [「リファレンスマニュアル」](#) / [「詳細設定」](#) / [「Managed AP」](#)

「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。パスフレーズの変更は可能です。

---


## 3.6 クラスタ

 [「リファレンスマニュアル」](#) / [「クラスタ」](#) / [「アクセスポイント」](#)

- クラスタ機能において、ひとつのクラスタ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。

---


### 3.7 送信 / 受信

 [「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。

---


### 3.8 SNMP

 [「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。

---

### 3.9 V.1.2.0 からのアップグレード

 [「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」

---


## 4 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.3.1.2 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.3.1.2 にアップグレードしてください。

---

### 4.1 V.1.0.0 → V.1.1.6 以降へのアップグレード

 [「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-teleasis.co.jp/>

---

## 4.2 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。

---

## 4.3 V.2.0.x→V.3.1.2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.3.1.2にアップグレードすると、無線セキュリティの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)


---

# 5 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。

---

## 5.1 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。

---

# 6 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/>