



ファームウェアバージョン:	R4.2.0.15B001C
ハードウェアバージョン:	A1
発行日:	2019/9/9

本リリースノートには、D-Link 製アクセスポイントのファームウェア更新に関する重要な情報が含まれています。ご使用のアクセスポイントに対応するリリースノートであることを確認してください。

- 新しいアクセスポイントにインストールを行う際には、デバイス上のハードウェアバージョンの表示を確認し、ご使用のアクセスポイントがファームウェアのシステム要件を満たしていることを確認してください。ファームウェアとハードウェアの互換性についての詳細情報は、“変更履歴とシステム要件”の項を参照してください。

アクセスポイント本体に関する詳細な情報が必要な場合は“ユーザマニュアル”を参照してください。

## 目次：

変更履歴とシステム要件：	2
アップグレード手順：	2
Web GUI を使用したアップグレード	2
追加機能：	4
修正した問題点：	4
既知の問題：	4

## 変更履歴とシステム要件：

ファームウェアバージョン	リリース日付	モデル	ハードウェアバージョン
ランタイム: R4.2.0.15B001C	2019/9/9	DWL-6600AP	A1

## アップグレード手順：

**R4.2.0.9B029 以前のファームウェアからのアップグレードは、同じ手順で、必ず 2 度続けて行ってください。**

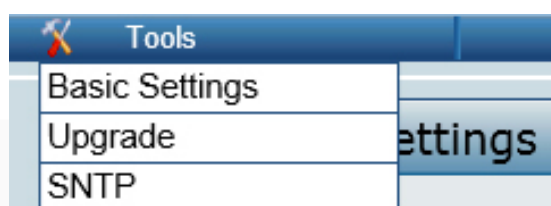
**1 回目のアップグレードのみだと、ブートオプションがセットされないためです。**

R4.2.0.9 以前の旧バージョンからファームアップする場合、ファームアップ後にファクトリリセットを行う必要があります。

ファームウェアのアップグレードは、Web GUI から行うことができます。アップグレード方法は次の「[WEB GUI を使用したアップグレード](#)」の手順に従い進めてください。

### Web GUI を使用したアップグレード

1. 本製品と設定用の PC を接続後、WEB ブラウザを立ち上げ、アドレスバーに WEB GUI の管理画面を表示します。  
※ 工場出荷時状態の IP アドレスは http://10.90.90.91 です。  
※ IP アドレスを変更している場合は、変更後の IP アドレスを入力してください。
2. WEB GUI のログイン画面が表示されたら、ユーザ名とパスワードを入力し、ログインしてください。  
※工場出荷時状態のユーザ名は「admin」、パスワードは「admin」です。
3. ログイン後、上部のメニューから「Tools」 -> 「Upgrade」の順でクリックします。



4. 「HTTP」または「TFTP」を選択します。

 A screenshot of the 'Manage firmware' page in the Web GUI. The page has a light blue header with the title 'Manage firmware'. Below the header, there is a table showing device information: Model (DWL-6600AP), Platform (dwl6600ap), and Firmware Version (4.2.0.11). Underneath the table, there is a section for 'Upload Method' with two radio buttons: 'HTTP' (selected) and 'TFTP'. Below this is a text input field for 'New Firmware Image' with a '参照...' (Browse...) button next to it. At the bottom of this section is an 'Upgrade' button. A 'Caution' note at the very bottom states: 'Uploading the new firmware may take several minutes. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the process is complete the access point will restart and resume normal operation.'

**HTTP 経由でファームウェアのアップグレードを行う場合：**

- (1) [参照]/[Browse]ボタンをクリックしてローカル PC 内のファームウェアファイルを指定 → [Upgrade]ボタンをクリックします。
- (2) 確認画面が表示されるので、「OK」をクリックします。
- (3) 経過画面が表示されますのでしばらくお待ちください。

**注意：ファームウェアのダウンロード中およびスイッチの再起動中に、電源を切らないでください。電源を切ると、起動に失敗し、起動できなくなることがあります。故障の原因となりますので、ご注意ください。**

- (4) アップグレード完了後、本製品は再起動します。  
ログインし、「Maintenance」>「Upgrade」メニューで、ファームウェアがアップグレードされたことを確認してください。
- (5) R4.2.0.9B029 以前のファームウェアからのアップグレードの場合は、続けて、さらにもう 1 回手順 (1) ～ (4) を繰り返してください。
- (6) さらに、Telnet もしくはコンソールにより、下記のコマンドの出力結果が同じバージョンになっていることを確認してください。  
bootenv -d bootver  
bootenv -d altbootver  
※どちらかのコマンドによる出力が 4.2.0.15B001C になっていない場合は、再度手順 (1) ～ (4) を繰り返してください。

**TFTP 経由でファームウェアのアップグレードを行う場合：**

- (1) [Image Filename]と[Server IP]を入力 → [Upgrade]ボタンをクリックします。
- (2) 確認画面が表示されるので、「OK」をクリックします。
- (3) 経過画面が表示されますのでしばらくお待ちください。

**注意：ファームウェアのダウンロード中およびスイッチの再起動中に、電源を切らないでください。電源を切ると、起動に失敗し、起動できなくなることがあります。故障の原因となりますので、ご注意ください。**

- (4) アップグレード完了後、本製品は再起動します。  
ログインし、「Maintenance」>「Upgrade」メニューで、ファームウェアがアップグレードされたことを確認してください。
- (5) R4.2.0.9B029 以前のファームウェアからのアップグレードの場合は、続けて、さらにもう 1 回手順 (1) ～ (4) を繰り返してください。
- (6) さらに、Telnet もしくはコンソールにより、下記のコマンドの出力結果が同じバージョンになっていることを確認してください。  
bootenv -d bootver  
bootenv -d altbootver  
※どちらかのコマンドによる出力が 4.2.0.15B001C になっていない場合は、再度手順 (1) ～ (4) を繰り返してください。

## 追加機能：

ファームウェアバージョン	追加機能
R4.2.0.15B001C	特になし

## 修正した問題点：

ファームウェアバージョン	修正した問題点
R4.2.0.15B001C	<ol style="list-style-type: none"> <li>1. リブート後に NTP サーバと同期しない問題を修正致しました。</li> <li>2. 検証 IP 及び TFTP ファイル名がコマンドインジェクション攻撃に対して脆弱である問題を修正致しました。</li> <li>3. WPA Personal (AES) を使用し、2.4GHz で長時間テストを行った際にカーネルパニックが発生する問題を修正致しました。</li> <li>4. Web Server 画面で無効なファイル名を設定した場合にエラーメッセージが表示されない問題を修正致しました。</li> <li>5. URL に"&amp;" や "?"などの特殊文字が使用されると、html コードが表示される問題を修正致しました。</li> <li>6. 5GHz を無効にした場合に、RSSI 値が減少することがある問題を修正致しました。</li> <li>7. MAC 認証でのダイナミック VLAN が動作しなくなることがある問題を修正致しました。</li> <li>8. アクセスポイントがイーサネットから受信者のいないタグ付きパケットを受信した場合に、パケットバッファを解放せずにパケットがドロップされ、メモリリークが発生する問題を修正致しました。</li> <li>9. 無線スケジューリングが機能せず、コントローラーから管理対象 AP の時間を正確に設定できない問題を修正致しました。</li> <li>10. WPA2 の脆弱性 KRACKs を修正致しました。</li> </ol>

## 既知の問題：

ファームウェアバージョン	既知の問題
R4.2.0.15B001C	<ol style="list-style-type: none"> <li>1. パスワードを使用して Web GUI にログインしパケットをキャプチャすると、実際のパスワードをデコードできてしまう問題。</li> <li>2. L2 トンネリングが機能しない問題。</li> <li>3. HTTPS ブルートフォース攻撃を防止できない問題。</li> <li>4. GUI アクセスが遅くなることがある問題。</li> <li>5. CLI から Radio ページの自動チャネルオプションを設定しても GUI に反映されない問題。</li> <li>6. Client QoS ACL 画面の Help ページにスペルミスが存在する問題。</li> <li>7. 5GHz で確立した WDS リンクでインターネット 8.8.8.8 に Ping すると 10 以上連続で Ping ロスが発生する問題。</li> <li>8. 2.4Ghz 及び 5Ghz 帯における LAN から WLAN への iperf トラフィックを処理中に、Null 値 (ゼロ) が確認される問題。</li> <li>9. SNMPv3 のユーザ名/認証タイプ/キーが CLI から設定できない問題。</li> </ol>

- |  |   |
|--|---|
|  | <ul style="list-style-type: none"><li>10. ユーザが間違ったサーバ IP で不正な SSL 証明書もしくは有効な証明書をアップロードしようとした際に正しいエラーメッセージを表示しない問題。</li><li>11. ピア設定を送信すると EmWeb がハングする問題。</li><li>12. Client QoS ACL で IPv6 : IGMP だけを許可しても失敗する問題。</li><li>13. クラスタコントローラが RADIUS-power-set AP に対して出力を変更させる問題。</li><li>14. アクセスポイントの IP アドレスが x.x.x.255 に設定されると、他のデバイスと通信できなくなる問題。<br/>対応策：アクセスポイントのアドレスの末尾を 255 にしないでください。</li></ul> |
|--|---|

**Copyright 2006-2019 D-Link Japan K.K.**