ファームウェアバージョン：	V3.13	
製品名/ハードウェア：	DSR-1000AC	A1
	DSR-1000	B1
	DSR-500	
発行日：	2019/7/30	

本リリースノートには、DSR シリーズ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 DSR シリーズ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 DSR シリーズにインストールを行う際には、デバイス本体上のハードウェアバージョンの表示を確認し、ご使用の DSR 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。

DSR シリーズ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：

ファームウェアバージョン	リリース日付	製品名	ハードウェアバージョン
ランタイム: v3.13	2019/7/30	DSR-1000AC	A1
		DSR-1000	B1
		DSR-500	

注意事項：

1. Microsoft Windows XP は DSR ルータの USB ストレージへのアクセスに関して、制限事項があります。Windows XP 環境での制限を解除するために、D-Link ではレジストリスクリプトファイル（WinXP.reg）を提供しています。このスクリプトファイルを適用しない場合には、Windows XP から USB ストレージへのファイルのコピーはできません。（この制限は、USB ストレージから Windows XP へのファイルのコピー時には発生しません）

2. ファームウェアを新しいバージョンから古いバージョンへダウングレードする場合、アップグレードに比べてシステムのリブートに時間を要します。何らかの理由によりダウングレードを行う必要がある場合は、DSR の再起動に時間がかかることにご注意ください。また、ダウングレードによりコンフィグを維持できないことがありますので、ダウングレード後は設定を十分にご確認ください。

3. ネットワーク業界の標準的な仕様に合わせて、DHCP IP プール範囲内に DHCP 予約 IP が設定されるように対応しています。

4. RADIUS、LDAP、AD、POP3 などの外部データベースを介して SSL VPN ユーザの認証を行う場合、管理者はローカルユーザデータベースで使用しているものと同じユーザ名/パスワードでユーザアカウントを作成する必要があります。

USB ストレージへの自動バックアップ/リストアの設定に関して：

D-Link DSR ルータは、USB デバイスが挿入されている間の、設定の自動バックアップもしくはリストアに対応しています。次の情報は、バックアップ/リストアを実行するための条件となります。

1. 本ルータの設定では、USB ドライブが挿入されるとすぐに自動的に USB ドライブにバックアップを行います。既に存在する DSR ルータからのバックアップ設定ファイルを持っていない場合に、USB ドライブに、「<モデル名>_<シリアルナンバー>.cfg」という形式でバックアップファイル名が提供されます。

2. ルータのシステム LED は、バックアップ操作が開始されることを示すために橙色に 3 回点滅します。

3. USB ドライブの設定ファイルは、ユーザが手動で WEB GUI の各ページに存在する “Save Settings” ボタンをクリックし、USB ドライブに既に存在するファイルとルータのモデル名及びシリアルナンバーが一致すると更新されます。

4. リブートする場合、ルータは設定ファイル（<モデル名>_<シリアルナンバー>.cfg）が存在するかどうかを確認します。設定ファイルが検出されると、USB ドライブの設定ファイルはルータにリストアされます。正しいフォーマットの設定ファイルが接続された USB ドライブの両方に存在する場合、一番目の USB ドライブの設定ファイルをルータのリストアに使用します。

5. USB ドライブは各モデル名に対して、<モデル名>_<シリアルナンバー>.cfg のフォーマットで 1 つのみ設定ファイルを持つことが可能です。

6. USB ドライブを工場出荷時状態のルータに挿入し、リブートを行った場合、ルータに既にカスタマイズされた設定ファイルが存在しないため、バックアップファイルは保存されません。ユーザが手動で WEB GUI の各ページに存在する“Save Settings”ボタンをクリックすると、カスタマイズされた設定ファイルが USB ドライブに保存されます。

リカバリに関して：

ファームウェアのアップグレード時、またはその他の原因により製品のファームウェアが損傷した場合、次の手順でブラウザにアクセスしてください。

1. DSR の電源をオフにします。
2. リセットボタンを押した状態で電源をオンにします。
3. そのままリセットボタンを 15 秒以上押し続けます。
4. DSR が Web Recover Mode に入ります。

IP アドレスは 192.168.10.1 となりますので、接続用 PC を本製品と同じ IP セグメントに設定した上で、ブラウザから Web Recover Mode にアクセスしてください。

SSL VPN 互換性一覧：

SSL VPN 接続が可能な Windows OS、ブラウザ一覧は以下の通りです。

SSL VPN スプリットトンネル/フルトンネル	
Windows 7 (32bit)	IE 9.0/11, Firefox 47.0.1
Windows 7 (64bit)	IE 9.0
Windows 8 (32bit)	IE 10.0, Firefox 47.0.1
Windows 8 (64bit)	IE 10.0
Windows 8.1 (32bit) ※	IE 11, Firefox 47.0.1
Windows 8.1 (64bit) ※	IE 11

※「既知の問題」により、Windows8.1 上での IE11 ブラウザ経由の SSL VPN スプリットトンネル接続には対応していません。

アップグレード手順

ファームウェアのアップグレードは、WEB GUI から簡単に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。

コードの構造の変更により、R3.10 またはそれより古いファームウェアをご利用の場合は、R3.12B101H を含むそれ以降のファームウェアに直接ファームウェアアップグレードすることができません。R3.10 またはそれより古いファームをご利用の場合は、同梱の中間ファームウェアにアップグレードした後、本ファームウェアにアップグレードする必要があります。

ファームウェアのアップグレードに失敗する場合は、以下の点を確認してください。

- **デバイス画面上のハードウェアバージョンを確認してください。**
- アップグレード実施においては、以下の対応する中間ファームウェアと共通ファームウェアを選択してください。

製品名	HW	中間ファームウェア	共通ファームウェア
DSR-500	B1	DSR-500_B1_FW3.11B001E_WW	DSR-500_Bx_FW3.13_WW
DSR-1000	B1	DSR-1000_B1_FW3.11B001E_WW	DSR-1000_Bx_FW3.13_WW
DSR-1000AC	A1	DSR-1000AC_A1_FW3.11B001E_WW	DSR-1000AC_Ax_FW3.13_WW

※R3.12B101H をご利用の場合は中間ファームウェアの適用は不要です。

WEB UI を使用したアップグレード

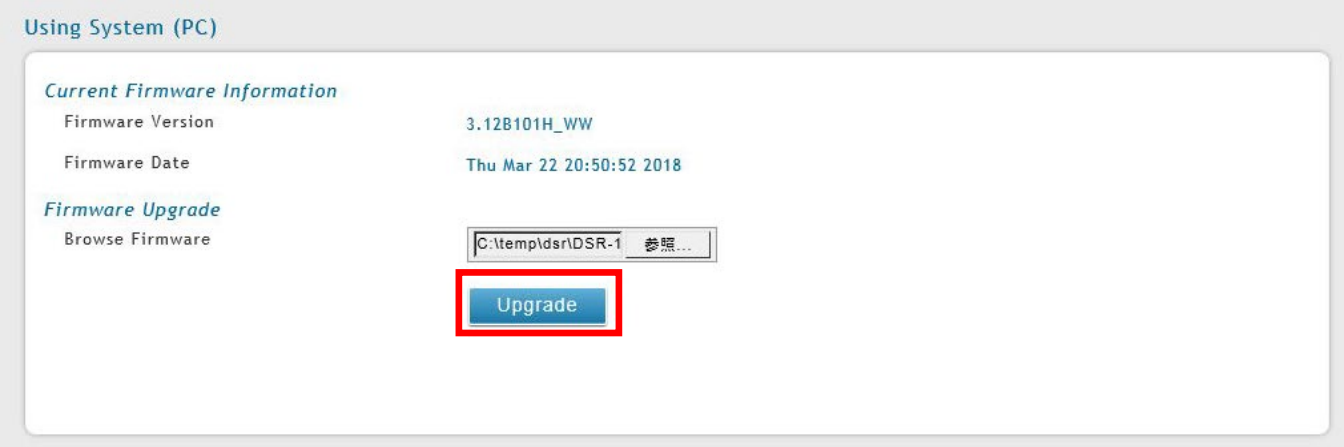
1. 本製品と設定用の PC を接続後、WEB ブラウザを立ち上げ、アドレスバーに WEB GUI の管理画面を表示します。デフォルトのシステム IP アドレスは 192.168.10.1 です。

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。デフォルトのユーザ名およびパスワードは「admin」です。

3. ログイン後、上部のメニューから、***Maintenance > Firmware > Firmware Upgrade > Using System (PC)***の順にクリックします。

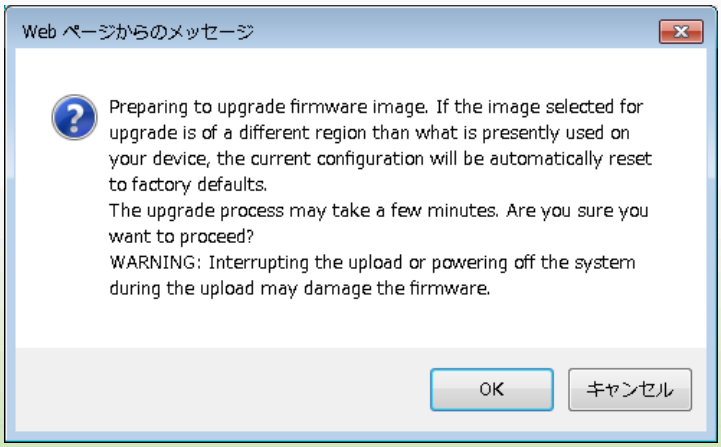
4. 「Firmware Upgrade」の「参照」ボタンをクリックします。

5. ローカルのハードディスク上に保存したファームウェアファイルを選択し、「Upgrade」をクリックします。



※R3.10 またはそれより古いファームウェアをご利用の場合は、まず R3.11B001E のファームウェアファイルを適用し、その後に R3.13 を適用する必要があります。R3.12B101H をご利用の場合は中間ファームウェアの適用は不要ですので、直接 R3.13 にアップグレードしてください。

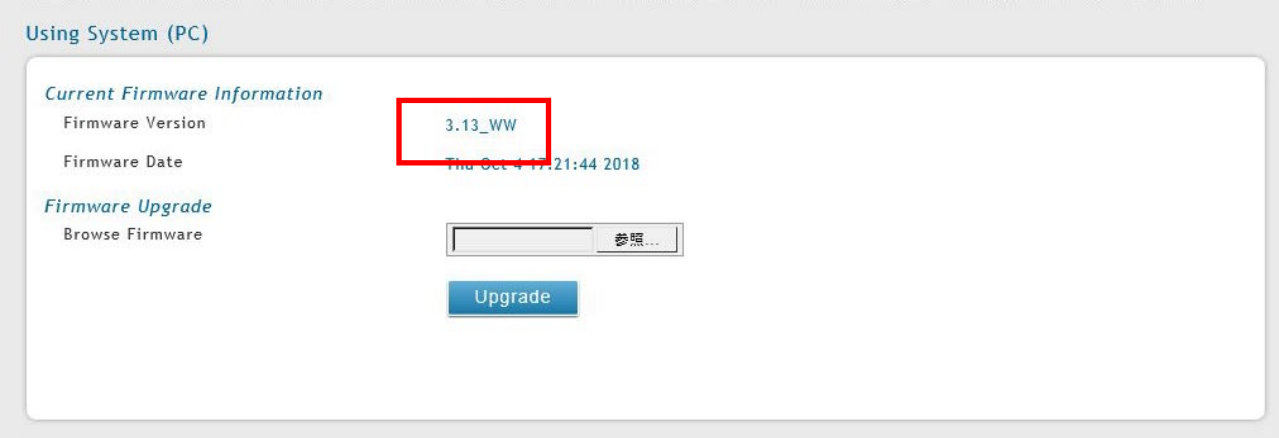
6. アップグレードの確認画面が表示されるので、「OK」をクリックします。



注意：ファームウェアのアップデート中に、電源を切らないでください。アップデート中に電源を切ると、起動に失敗し、正常に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。

7. アップグレード完了後、ログイン画面が表示されます。再度ログインし、***Maintenance > Firmware & Config > Firmware Upgrade > Using System (PC)***の順にクリックします。

8. 「Current Firmware Information」の「Firmware Version」がアップグレード後のバージョンであることを確認します。



追加機能：

ファームウェアバージョン	追加機能
V3.13	1. DDP をサポート致しました。 2. OpenVPN で手動によるトンネル接続に対応致しました。 3. WiFi 送信出力設定の単位を dbm から%に変更致しました。 4. ファイアウォールポリシーの上限数について、Inbound/Outbound で共有とし、それぞれの作成可能な最大数を拡張致しました。（Inbound/Outbound ポリシーを合わせたポリシー全体の上限数に変更はありません。） 5. OmniSSL で Win10 をサポート致しました。 6. OmniSSL ポータルレイアウト設定に対応致しました。 7. アプリケーションコントロール設定に対応致しました。 8. OmniSSL 証明書の生成において SHA2 ハッシュアルゴリズムに対応致しました。

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
V3.13	1. トラフィックセレクタから BSSID オプションを削除致しました。 2. OmniSSL トンネルの通信開始後、20 秒程度で切断・再開する問題を修正致しました。 3. スタティックルートに設定した LAN 外のサブネットをファイアウォールルールの Internal IP Address に設定できない問題を修正致しました。 4. PPTP/L2TP サーバのクライアント IP アドレスと同じサブネットで VLAN を設定できてしまう問題を修正致しました。 5. WEB コンテンツフィルタリングにおいて HTTPS の URL が正しくブロックされない問題を修正致しました。 6. OpenVPN ログが出力されない問題を修正致しました。 7. GRE 設定において、「x.x.x.0」の IP アドレスを設定できない問題を修正致しました。 8. CVE-2018-6212 の脆弱性を修正致しました。 9. CLI でスペースを含む SSID が設定できてしまう問題を修正致しました。 10. 帯域プロファイルが定義されている場合、トラフィックセレクタの作成画面で不正なパラメータが表示される問題を修正致しました。 11. L2TP トンネルの最大数が仕様に満たない問題を修正致しました。 12. Spillover モードの Max Bandwidth 設定で 100Mbps までしか設定できない問題を修正致しました。 13. 2GB のファイルを SSL VPN トンネル経由でダウンロードする際に Ping が損失する問題を修正致しました。 14. IGMP スヌーピングが動作しない問題を修正致しました。 15. プロトコルバインディングを設定している場合に WAN2 インタフェース経由で WAN1 の IP アドレスが送信される問題を修正致しました。 16. ユーザ数とユーザグループ数が仕様通りに制限されない問題を修正致しました。 17. LAN/VLAN サブネットの変更後、InterVLAN ファイアウォールウォールが適切に更新されない問題を修正致しました。 18. Stealth Mode が有効化されている場合、'zeroconf'ポートに対する UDP スキャンが Closed となる問題を修正致しました。

既知の問題：

ファームウェアバージョン	既知の問題
V3.13	1. WAN が PPTP/L2TP/PPPoE として設定されている場合、CLI で MAC アドレスが正しく表示されない問題。 2. Dashboard 画面において、WAN3 の統計が更新されない問題。 3. DSR-1000/A1 のコンフィグを B1 へ警告なしにリストアできてしまい、システムが応答不可となる問題。 4. PPTP クライアント画面においてリモートネットワークのサブネットマスクが 32 で設定されている場合、システムが再起動される問題。 5. Windows8.1（32/64bit）で IE11 ブラウザを使用した場合に SSL-VPN スプリットトンネルに対応できない問題。 6. Google Chrome v42 で Java 8 update 31 を使用している場合に SSL VPN トンネルを確立できない問題。 7. Opera v34 で SSL VPN トンネルを確立できない問題。 8. スカイプセッション終了後に UPnP Port Map List のエントリが更新されない問題。 9. Authentication server（1-3）の項目でサーバ名を設定できない問題（IP アドレスのみ可）。（制限事項） 10. WAN1 がクラシカルルーティングモードで動作しているとき、WAN2 に対してインバウンドのファイアウォールルールを追加する際に Internal IP Address 欄が表示されない問題。 11. Port Forwarding トンネル経由で Intel AMT にアクセスできない問題。 12. snmpset コマンドによりポータルが追加された場合、RADIUS_PAP 認証の SSL ポータルが外部 RADIUS_PAP ユーザでログインできない問題。 13. PPTP/L2TP サーバの IP プールが LAN 側 IP アドレスと同じサブネットに設定可能である問題。