



ファームウェアバージョン :	V3.12B101H	
製品名/ハードウェア :	DSR-1000AC	A1
	DSR-1000	B1
	DSR-500	
発行日 :	2018/7/6	

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 :	2
注意事項 :	2
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 :	2
リカバリに関して :	3
SSL VPN 互換性一覧 :	3
アップグレード手順	3
WEB UI を使用したアップグレード	4
追加機能 :	6
コマンドラインインタフェースの変更点 :	6
修正した問題点 :	7
既知の問題 :	9

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: v3.12B101H	2018/7/6	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。

本ファームウェア (R3.12) 以降、ハードウェア共通のファームウェアをサポートしています。このような仕様の変更に伴い、R3.12 にアップグレードするには、まず R3.11B001E を適用し、その後に R3.12B101H を適用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。

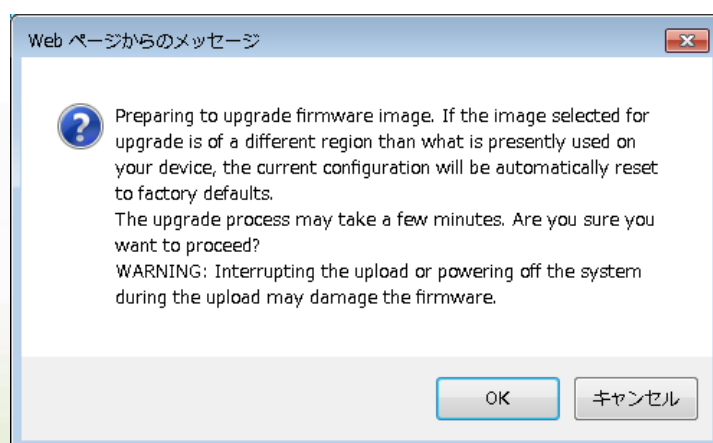
製品名	HW	中間ファームウェア	HW 共通ファームウェア
DSR-500	B1	DSR-500_B1_FW3.11B001E_WW	DSR-500_Bx_FW3.12B101H_WW
DSR-1000	B1	DSR-1000_B1_FW3.11B001E_WW	DSR-1000_Bx_FW3.12B101H_WW
DSR-1000AC	A1	DSR-1000AC_A1_FW3.11B001E_WW	DSR-1000AC_Ax_FW3.12B101H_WW

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。ここでは、まず R3.11B001E のファームウェアファイルを指定します。

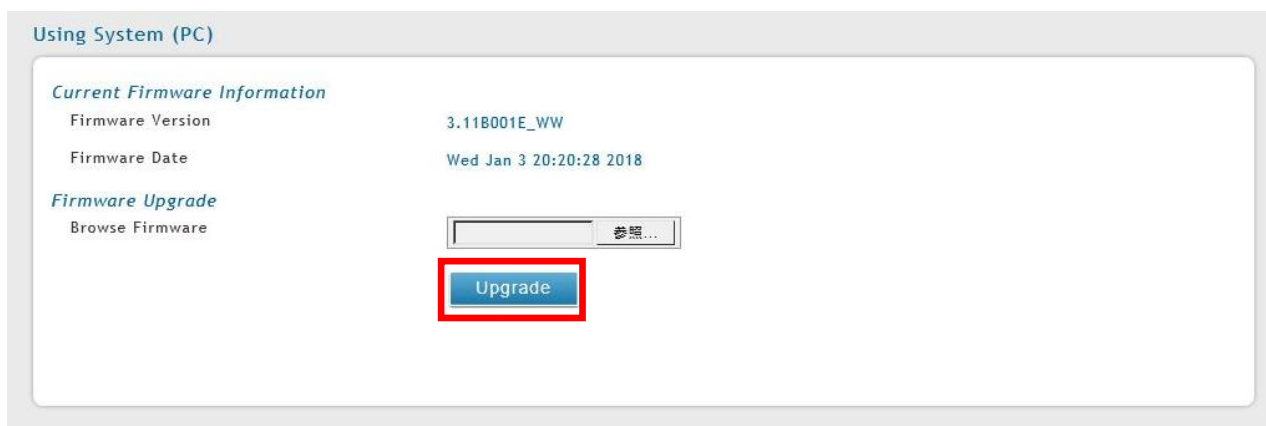


6. アップグレードの確認画面が表示されるので、「OK」をクリックします。



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。

- 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 > Firmware Upgrade > Using System (PC)**の順にクリックします。
- 「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。



- 手順 3～手順 7 を繰り返し、R3.12B101H のファームウェアファイルを適用します。アップグレード後、WebGUI のファームウェアバージョンが R3.12B101H になってい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
V3.12B101H	<ol style="list-style-type: none"> 1. OpenVPN Certificates 機能を追加致しました。 2. IPv6 VLAN 設定に対応致しました。 3. サービスルート管理機能を追加致しました。本機能では、VLAN/IPSec ベースの RADIUS 認証設定を行うことができます。 4. DHCP リースクライアントリストでホスト名を表示するように対応致しました。 5. Radius Accounting 設定を追加致しました。本機能では、Interim-Update 設定を行うことができます。 6. IPv6 WAN設定の PPPoE モードにおいて、DHCPv6 クライアントに対する「Stateful DHCPv6 with Prefix Delegation」の認証タイプに対応致しました。 7. PPTP/L2TP クライアント設定の「Auto Dial」を「Auto Connect」という名称に変更致しました。 8. URL Filtering ACL 機能を追加致しました。本機能では、IP アドレス範囲によるホワイトリスト/ブラックリストを設定することができます。 9. 帯域制御を有効にしている場合のスループットを改善致しました。 10. トラフィック管理でセッション数による制限に対応致しました。 11. URL フィルタリングの設定でワイルドカードに対応致しました。 12. Web コンテンツフィルタリングで HTTPS に対応致しました。 13. ログ出力内容を改善致しました。 14. WAN インタフェースでジャンボフレームに対応致しました。 15. OpenVPN において、ユーザ、証明書、TLS の混合認証に対応致しました。

コマンドラインインタフェースの変更点：

ファームウェアバージョン	変更点
V3.12B101H	<ol style="list-style-type: none"> 1. net vlan コマンドで IPv6 設定に対応致しました。 2. show net vlan configuration で IPv6 表示に対応致しました。 3. net lan ipv6 コマンドでプリフィックス委譲の設定に対応致しました。 4. net radvd configure コマンドで VLAN 指定による設定に対応致しました。 5. RADVD Pool コンフィグレーションモードで VLANID の設定に対応致しました。 6. show vpn openvpn コマンドで証明書の Subject Name、Server Name、Client Name の表示に対応致しました。 7. vpn openvpn コマンドで証明書の追加に対応致しました。

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
V3.12B101H	<ol style="list-style-type: none"> 1. ワイヤレス設定のデフォルトプロファイルで、Radio Mode 項目が表示されない問題を修正致しました。(DSR-1000AC のみ) 2. WCF ライセンスをアクティブ化した後、タイムゾーンを変更できない問題を修正致しました。 3. Classical Routing モードにおいて、VPN エラー619 により PPPoE WAN の PPTP トンネルを確立できない問題を修正致しました。 4. Wireless Clients 画面において、接続クライアントの周波数帯域が 5GHz/2.4GHz でではなく Radio 1/Radio 2 と表示される問題を修正致しました。(DSR-1000AC のみ) 5. Traffic Selector 設定画面で IP アドレスに「0.0.0.0」を入力できてしまう問題を修正致しました。 6. VPN エラー628 により PPPoE WAN の PPTP トンネルを確立できない問題を修正致しました。 7. システムログ表示において、出力ログの Severity を error から Information に変更致しました。 8. WAN 側に配置された RADIUS サーバを設定できない問題を修正致しました。 9. DHCP リレー機能が Classical Routing モードにおいて動作しない問題を修正致しました。 10. ログを有効化している場合、ログ生成時に Web GUI が遅くなる問題を修正致しました。 11. WAN 側の IP アドレスと URL を使用して Web GUI に接続できない問題を修正致しました。 12. WAN モードの変更ができず、エラーメッセージが表示される場合がある問題を修正致しました。 13. Captive Portal にログインした後、HTTPS 画面にリダイレクトされない問題を修正致しました。 14. GUI または CLI による IPSec PSK 設定において、ダブルクォテーション、バックスラッシュ、スペースを除く文字記号をサポート致しました。 15. PPPoE 接続の WAN 通信において Reconnect Mode を「On demand」に設定した場合、正常に動作しない問題を修正致しました。 16. System Check におけるルート表示でスタティックルートが表示されない場合がある問題を修正致しました。 17. ロードバランシングモードにおいて、WAN1 が再接続した際に WAN2 が再度スタンバイ状態にならない問題を修正致しました。 18. WAN1 と WAN2 で同じ VLAN ID を設定できない問題を修正致しました。 19. NTP 有効化時、WiFi のスケジューリング機能が正しく動作しない問題を修正致しました。 20. カスタム NTP サーバが選択したタイムゾーンと同期されない問題を修正致しました。 21. PPTP/L2TP サーバ設定において、クライアントの IP アドレス範囲に含まれる最大 IP アドレス数を 26 個から 16 個に修正致しました。 22. USB ポートで 2TB HDD に接続できない問題を修正致しました。 23. LAN DHCP 予約 IP アドレスの既存エントリの編集により、別のエントリと同じホスト名に設定できてしまう問題を修正致しました。 24. ログが適切に更新されない問題を修正致しました。 25. Approved URL 画面で CSV ファイルがアップロードされない場合がある問題を修正致しました。 26. ロールバックの際に Rollover WAN が UP しない問題を修正致しました。 27. SNMPv3 トラップが送信されない問題を修正致しました。 28. 再起動またはログの有効化後に L2TP over IPSec 接続が切断される問題を修正致しました。 29. コンフィグファイルのサイズが大きい場合にリストアが失敗する問題を修正致し

- ました。
30. WAN の自動ロールオーバーが動作しない問題を修正致しました。
 31. システムログが新しい順に表示されない問題を修正致しました。
 32. OpenVPN と OmniSSL 接続で定義済みのネットワークに接続できない問題を修正致しました。
 33. L2TP over IPsec VPN 接続の AD 認証または NT ドメイン認証が動作しない問題を修正致しました。
 34. ダッシュボード画面の Traffic Overview タブで「Detail」ボタンをクリックできない問題を修正致しました。
 35. CVE-2017-14491 の脆弱性を修正致しました。
 36. SSID トランクモードにおいてタグなしのインタフェースから無線クライアントに接続できない問題を修正致しました。
 37. IPsec クライアントが NAT デバイスの配下に存在する場合にトラフィックの損失が発生することがある問題を修正致しました。
 38. WAN モードが Load Balancing に設定されている場合に IPsec トンネル経由で DUT LAN インタフェースに到達できない問題を修正致しました。
 39. OpenVPN Settings 画面でカスタム OpenVPN ネットワークが設定されている場合、ユーザ定義の OmniSSL サーバポリシーが動作しない問題を修正致しました。
 40. WAN の PPPoE 設定において、ユーザ名とパスワードに 16 文字以上を設定できない問題を修正致しました。
 41. デフォルトの VLAN IP ネットワークを変更後、Web 管理画面に接続できなくなる場合がある問題を修正致しました。
 42. デバイス起動時にケーブルが差し込まれると、WAN がリンクダウン状態となる場合がある問題を修正致しました。
 43. WAN2 インタフェースに対して IP エイリアスが設定できない場合がある問題を修正致しました。
 44. Approved/Blocked URL でスラッシュ記号「/」に対応していない問題を修正致しました。
 45. IPv6 LAN 接続で Web 画面に接続できない問題を修正致しました。
 46. 外部認証サーバ (Active Directory、NT Domain、LDAP サーバ) を使って、PPTP 及び L2TP VPN トンネル接続を確立できない問題を修正致しました。
 47. “show system log viewLogs”コマンドがが正しく動作しない問題を修正致しました。
 48. 同じリモートネットワークが設定された複数の IPsec ポリシーが存在する場合、そのうちの 1 つのポリシーは必ず有効となり、全てを無効化することはできない問題を修正致しました。
 49. IPsec トンネルモードで DNS サーバを設定できない問題を修正致しました。
 50. NAT の keep alive 時間の最大値を 3600 に修正致しました。
 51. IPS 機能が有効の場合に TeamViewer による接続が許可されない問題を修正致しました。
 52. CVE-2014-0195、CVE-2014-0224、CVE-2016-2183、CVE-2014-3566 の脆弱性を修正致しました。
 53. 特定の VLAN を追加しない場合にキャプティブポータルが動作しない問題を修正致しました。
 54. NAT 配下において、Aggressive モードで IPsec 接続を確立できない問題を修正致しました。
 55. スタティックルートのプルダウンメニューで WAN インタフェースが表示されない場合がある問題を修正致しました。
 56. ログ表示において、「Clear All」をクリックした後にログの上限が仕様よりも小さく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
V3.12B101H	<ol style="list-style-type: none"> 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。 IGMP スヌーピングが動作しない問題。 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。 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。 Opera v34 で SSL VPN トンネルを確立できない問題。 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。 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)。 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。 Port Forwarding トンネル経由で Intel AMT にアクセスできない問題。 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。 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。 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。 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。 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。 BSSID 環境では帯域制御のトラフィックセクタが動作しない問題。

Copyright 2006-2018 D-link Japan K.K.