

**Biz Box ルータ 「 RTX1210」  
ファームウェアリリースノート  
Rev. 14. 01. 11**

**RTX1210 Rev. 14. 01. 09 からの変更点**

以下のとおり機能追加・機能改善が行われました。

■機能追加

[1] L2MS で、SWX2300 および WLX202 に対応した。

ただし、Web GUI の LAN マップにおける以下の機能には未対応。

- SWX2300 の各ポートに設定されている VLAN 情報の表示
- SWX2300 の各ポートに対する VLAN の設定変更

[2] モバイルインターネット機能で、以下のデータ通信端末に対応した。

- docomo FOMA UM03-K0 専用アダプタセット
- SoftBank 403ZT

<http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/index.html>

外部仕様書をよくご確認のうえ、ご利用ください。

[3] BGP 経路強制広告機能に対応した。

[http://www.rtpro.yamaha.co.jp/RT/docs/bgp/bgp\\_force-to-advertise.html](http://www.rtpro.yamaha.co.jp/RT/docs/bgp/bgp_force-to-advertise.html)

外部仕様書をよくご確認のうえ、ご利用ください。

[4] BGP の TCP MD5 認証機能に対応した。

○TCP MD5 認証の事前共有鍵の設定

[書式]

```
bgp neighbor pre-shared-key NEIGHBOR_ID text TEXT_KEY  
no bgp neighbor pre-shared-key NEIGHBOR_ID [text TEXT_KEY]
```

[設定値及び初期値]

NEIGHBOR\_ID

[設定値] : 近隣ルーターの番号 (1...2147483647)

[初期値] : -

TEXT\_KEY

[設定値] : ASCII 文字列で表した鍵 (80 文字以内)

[初期値] : -

[説明]

TCP MD5 認証で用いる事前共有鍵を設定する。設定した事前共有鍵が一致するピア間のみ、BGP のコネクションが成立する。

- [5] Web GUI へ一般ユーザー権限 (ログインユーザー権限) でアクセスしたときに閲覧可能な画面を、ユーザーごとに設定できるようにした。

○ユーザーの属性を設定

[書式]

```
user attribute [USER] ATTRIBUTE=VALUE [ATTRIBUTE=VALUE ...]
```

```
no user attribute [USER]
```

[設定値及び初期値]

USER

[設定値] :

設定値	説明
ユーザー名	登録されているユーザー名
*radius	RADIUS 認証でログインするすべてのユーザー
*	すべてのユーザー

[初期値] : -

ATTRIBUTE=VALUE

[設定値] :

- ・ administrator: 管理者モードを使えるかどうかを示す属性

設定値	説明
on	administrator コマンドにより管理ユーザーに昇格することができる。また GUI の管理者ページへ接続すること

ができる。管理者パスワードを用いて SFTP 接続を行うことができる。

off administrator コマンドにより管理ユーザーに昇格することができない。また GUI の管理者ページへ接続することができない。管理者パスワードを用いて SFTP 接続を行うことができない。

-----  
・ connection: ルーターへのアクセス方法を示す属性

設定値	説明
off	すべての接続を禁止する。
all	すべての接続を許可する。
serial	シリアルコンソールからの接続を許可する。
telnet	TELNET による接続を許可する。
ssh	SSH による接続を許可する。
sftp	SFTP による接続を許可する。
remote	リモートセットアップによる接続を許可する。
http	GUI 設定画面への接続を許可する。

-----  
・ gui-page: ログインユーザーに対して閲覧を許可する GUI 画面の種別を示す属性 ★

設定値	説明
all	ログインユーザーでアクセスできるすべての画面の閲覧を許可する。
dashboard	ダッシュボード画面の閲覧を許可する。
lan-map	LAN マップ画面の閲覧を許可する。
config	かんたん設定画面、詳細設定画面、管理画面、CONFIG 画面および TECHINFO 画面の閲覧を許可する。

-----  
・ host: ルーターへのアクセスホストを指定する属性

設定値	説明
-----	----

IP アドレス	指定したホストからの接続を許可する。
any	すべてのホストからの接続を許可する。
インターフェース名	指定したインターフェースからの接続を許可する。

- 
- multi-session: 複数接続を許可するかどうかを示す属性

---

設定値	説明
on	同一ユーザー名による TELNET、SSH、HTTP での複数接続を許可する。
off	同一ユーザー名による TELNET、SSH、HTTP での複数接続を禁止する。

- 
- login-timer: ログインタイマーの指定

---

設定値	説明
数値 (※)	キー入力がない場合に自動的にログアウトするまでの秒数。
clear	ログインタイマーを設定しない。

※ Rev. 10.00 系以降の機種では 120..21474836 の数値を指定可能。

その他の機種では、30..2147483647 の数値を指定可能。

[初期値] :

- administrator=on
- connection=serial, telnet, remote, ssh, sftp, http
- host=any
- gui-page=all ★
- multi-session=on
- login-timer=300

[説明]

ユーザーの属性を設定する。

USER を省略した場合は、無名ユーザーの属性を設定する。

USER に\*radius を指定した場合は、RADIUS 認証でログインするすべてのユーザー

の属性を設定する。

USER にアスタリスク (\*) を指定した場合は、すべてのユーザーに対して設定を有効にする。ただし、ユーザー名を指定した設定がされている場合は、その設定が優先される。

すでに管理ユーザーに昇格しているユーザーに対して、このコマンドで administrator 属性を off に変更しても、そのユーザーは exit コマンドにより一般ユーザーに降格するか、あるいはログアウトするまでは管理ユーザーで居続けることができる。

connection 属性では、off、all 以外の値はコンマ(,)でつないで複数指定することができる。

すでに接続しているユーザーに対して、このコマンドで connection 属性または host 属性により接続を禁止しても、そのユーザーは切断するまでは接続を維持し続けることができる。

host 属性では、TELNET、SSH、SFTP 及び HTTP で接続できるホストを設定する。指定できる IP アドレスは、1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス(範囲指定)、およびこれらをコンマ(,)でつないだものである。

gui-page 属性では、all 以外の値はコンマ(,)でつないで複数指定することができる。★

本属性で設定した設定内容は、ログインユーザーとしてログインしたときのみ有効となる。管理ユーザーとしてログインした場合は、本属性の設定にかかわらず、常に GUI 上のすべての画面を閲覧する権限を持つ。★

すでに GUI に接続中のユーザーに対してこのコマンドで本属性の設定が変更された場合、次に GUI 上のページにアクセスした時点から新しい設定が反映される。★

multi-session 属性では、TELNET、SSH、HTTP での複数接続の可否を設定する。この属性を off に変更しても、シリアルと TELNET やリモートセットアップと SSH など、接続方法が異なる場合は同じユーザー名で接続することができる。

すでに複数の接続があるユーザーに対して、このコマンドで multi-session 属性を off に変更しても、そのユーザーは切断するまでは接続を維持し続けることができる。

無名ユーザーに対しては SSH、SFTP による接続を許可することができない。

無名ユーザーに対しては TELNET での複数接続はできない。

TELNET、SSH、SFTP、HTTP で接続した場合、login-timer 属性の値が clear に設定されていても、タイマ値は 300 秒として扱う。

login timer コマンドの設定値よりも、本コマンドの login-timer 属性の設定値が優先される。

[ノート]

administrator 属性を off に設定して GUI の管理者ページへの接続を制限できるのは Rev. 10.00 系以降のファームウェアである。

connection 属性に http を指定できるのは Rev. 10.00 系以降のファームウェアである。sftp を指定できるのは SRT100 Rev. 10.00.60 以降、RTX1200 Rev. 10.01.22 以降のファームウェア、および、Rev. 11.01 系以降のファームウェアである。

gui-page 属性を設定できるのは、RTX1210 Rev. 14.01.11 以降のファームウェアである。★

Rev. 10.00.31 で login-timer 属性の下限値を 30 から 120 に変更した。

本コマンドにより、すべてのユーザーの接続を禁止する、またはすべてのユーザーが管理ユーザーに昇格できないといった設定を行った場合、ルーターの設定変更や状態確認などができなくなるので注意する必要がある。

[6] IKEv2 で、CHILD SA の作成方法を変更できるようにした。

○CHILD SA 作成方法の設定

[書式]

```
ipsec ike child-exchange type GATEWAY_ID TYPE
no ipsec ike child-exchange type GATEWAY_ID [TYPE]
```

[設定値及び初期値]

GATEWAY\_ID

[設定値] : セキュリティ・ゲートウェイの識別子

[初期値] : -

TYPE : IKEv2 の CHILD SA 作成方法のタイプ

[設定値] :

設定値	説明
1	ヤマハルーターの IKEv2 の従来の動作との互換性を保持する
2	CREATE_CHILD_SA 交換を一部の実装にあわせる

[初期値] : 1

[説明]

IKEv2 の CHILD SA 作成方法を設定する。

このコマンドに対応する機種同士で接続する場合、タイプを同じ設定にして接続する必要がある。

[7] ソフトウェアの著作権情報を表示するコマンドを追加した。

また、起動時やログイン時に表示されていた著作権情報は表示されなくなった。

○ソフトウェアの著作権情報の表示

[書式]

`show copyright [detail]`

[設定値及び初期値]

`detail`

[設定値] : 条文を含めたソフトウェアの著作権情報を表示する

[初期値] : -

[説明]

ソフトウェアの著作権情報を表示する。

`detail` を指定することで、条文を含めたソフトウェアの著作権情報を表示することができる。

## ■仕様変更

[1] Lua スクリプト機能で、以下の変更を行った。

- `rt.command` 関数で、コマンド実行のログを出力するか否かを指定できるようにした。
- Lua スクリプト機能バージョンを 1.07 とした。

[2] SSH サーバー公開鍵を生成するときに、2048 ビットの鍵長を選択できるようにした。

また、セキュリティーの観点から SEED パラメーターの入力を無視するようにした。

## ○SSH サーバーホスト鍵の設定

### [書式]

```
sshd host key generate [bit=BIT] ★  
no sshd host key generate [...]
```

### [設定値及び初期値]

BIT

[設定値] : 鍵のビット長 (1024, 2048)

[初期値] : 1024

### [説明]

SSH サーバーのホスト鍵を設定する。

BIT パラメーターによって、生成する鍵のビット数を指定できる。 ★

### [ノート]

SSH サーバー機能および SFTP サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。

既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザーに対してホスト鍵を更新するか否かを確認する。

ホスト鍵の生成には、機種によって異なるが、1024 ビット鍵では数秒から数分程度、2048 ビットの鍵では数分から十数分程度の時間がかかる。 ★

TFTP で設定を取得した場合は、sshd host key generate [bit=BIT] KEY1 KEY2 KEY3 という形式で保存される。 ★

KEY1~KEY3 は、秘密鍵を機器固有の方式で暗号化した文字列である。

[3] SSH サーバー公開鍵の鍵指紋を表示するパラメーターを追加した。

## ○SSH サーバー公開鍵の表示

### [書式]

```
show sshd public key [fingerprint] ★
```

### [設定値及び初期値]

fingerprint ★

[設定値] : 鍵指紋を表示する

[初期値] : -

### [説明]

SSH サーバーの公開鍵を表示する。

fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。 ★



[4] dns host コマンドで複数のインターフェースを指定できるようにした。

○DNS サーバーへアクセスできるホストの IP アドレス設定

[書式]

```
dns host IP_RANGE [IP_RANGE [IP_RANGE...]] ★
```

```
no dns host [...]
```

[設定値及び初期値]

IP\_RANGE

[設定値] :

---

設定値	説明
1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス(範囲指定)	指定された IP アドレスを持つホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
lan	すべての LAN ポート側ネットワーク内ならば許可する
lanN	指定された LAN ポート側ネットワーク内ならば許可する (N は任意のインターフェース番号)
vlanN	指定されたポートベース VLAN インターフェースからのアクセスを許可する (N は任意の VLAN インターフェース番号)
lanN/M	指定された VLAN インターフェースからのアクセスを許可する (N は任意のインターフェース番号、M は任意のサブインターフェース番号)
none	すべてのホストからのアクセスを禁止する

---

[初期値] : any

[説明]

DNS サーバー機能へのアクセスを許可するホストを設定する。

[ノート]

any、lan、none は単独でのみ指定可能。 ★

このコマンドで LAN インターフェースを指定した場合には、ネットワークアドレスと limited broadcast address を除く IP アドレスからのアクセスを許可する。

指定した LAN インターフェースにプライマリーアドレスもセカンダリーアドレスも設定していなければ、アクセスを許可しない。

- [5] `clear log` コマンドに `saved` オプションを追加した。

このオプションを指定することで、`show log saved` コマンドを実行したときに表示されるログをクリアすることができる。

#### ○ログのクリア

##### [書式]

```
clear log [saved]
```

##### [設定値及び初期値]

`saved` ★

[設定値] : リポート直前のログをクリアする

[初期値] : -

##### [説明]

ログをクリアする。

`saved` を指定することで、`show log saved` コマンドを実行したときに表示されるログをクリアすることができる。★

- [6] ブリッジインターフェースに收容された LAN インターフェースでは QoS 機能は使用できない仕様であるため、`bridge member` コマンドによってブリッジに收容された LAN インターフェースに対して、`queue type` コマンドで `fifo` 以外を指定した場合、入力エラーとなるようにした。

また、`queue type` コマンドで `fifo` 以外が指定された LAN インターフェースを `bridge member` コマンドで指定した場合も同様に入力エラーとなる。

- [7] 温度監視によって出力される SYSLOG メッセージを以下のように変更した。

- 閾値を超えたとき

```
SYSTEM ALARM (over T1): Temperature 80 [C.]
```

- 閾値を下回ったとき

```
SYSTEM ALARM (under T2): Temperature 75 [C.]
```

- [8] Web GUI の推奨 Web ブラウザーから IE9、IE10 を除外した。

推奨 Web ブラウザーに関する詳細な情報については、以下の URL をご覧ください。

<http://www.rtpro.yamaha.co.jp/RT/FAQ/gui/browser.html>

[9] Web GUI の LAN マップのタグ VLAN 画面で、タグ VLAN を新規作成/削除したときに、DNS サーバーへアクセスできるホストの設定もそれに合わせて変更されるようにした。

[10] Web GUI の LAN マップで、LAN マップから制御できない未対応のスレーブを表すアイコンを変更した。

[11] Web GUI のかんたん設定の[基本設定]-[LAN1 アドレス]-[IPv4 アドレスの設定]、および詳細設定の[LAN]-[IPv4 アドレスの設定]で、LAN インターフェースの IP アドレスを変更するときに自動的に変更される IP アドレスとして、以下のものを追加した。

- ip keepalive コマンドで指定するキープアライブの始点 IP アドレス
- tunnel endpoint address コマンドで指定するトンネルのローカル IP アドレス

[12] Web GUI の以下の画面で、デザインやレイアウト等を修正し、視認性や操作性を改善した。

- LAN マップの一覧マップ画面のミニ一覧マップ
- かんたん設定のメニュー部分
- かんたん設定の[基本設定]-[LAN1 アドレス]-[IPv4 アドレスの設定]-[入力内容の確認]
- かんたん設定の[基本設定]-[LAN1 アドレス]-[IPv4 アドレスの設定]-[入力内容の確認]-[自動で変更されない設定の一覧]
- 詳細設定の[LAN]-[IPv4 アドレスの設定]-[入力内容の確認]
- 詳細設定の[LAN]-[IPv4 アドレスの設定]-[入力内容の確認]-[自動で変更されない設定の一覧]

[13] Web GUI のヘルプの[全般]-[その他]-[切断コード表]で、以下の切断コードの説明を追記した。

- 3000 認証失敗
- 3004 SIP サーバーの名前解決失敗
- 3020 リクエストタイムアウト
- 3503 SIP サーバー輻輳

## ■バグ修正

- [1] IPsec トンネル(※)を使用してハブ・アンド・スポーク型の VPN 構成を組んでおり、IPsec トンネルから受信したパケットを、そのままルーター内部で折り返して別の IPsec トンネルへ転送する経路が存在するとき、その経路を使用する通信に断続的に高負荷がかかり続けると SYSLOG に下記のいずれかのエラーログ (DEBUG レベル) が出力されるようになり、IPsec 通信ができなくなったり、ハングアップやリポートが発生したりすることがあるバグを修正した。

- “[SEC] Failed to enqueue the job (Job Ring 0)”
- “[SEC] Timeout waiting for the completion of the job (Job Ring 0)”

なお、ハブ拠点のルーターのみでこの問題が発生する可能性があり、一度発生すると再起動するまで IPsec 機能が動作しなくなる。また、ファストパスを無効にしている場合はこの問題は発生しない。

※IPsec トンネルは、L2TPv2/IPsec および L2TPv3/IPsec を使用するトンネルも含む。

- [2] LAN マップのメール通知機能で、本文の内容が 2048Byte を超えるメールの送信のリトライが発生したとき、リポートすることがあるバグを修正した。

- [3] URL フィルター機能で、以下の条件をすべて満たしたときに、リポートしたりブロック画面で表示される「キーワード」の一部が欠けたりすることがあるバグを修正した。

- url filter reject コマンドで reject (デフォルト値) が設定されている
- リダイレクト先のブロック画面の URL が 2048Byte を超えている

- [4] ipsec transport コマンドで、プロトコルまたは始点ポートリストのパラメーターを省略して実行したときにリポートするバグを修正した。

Rev. 14. 01. 09 で発生する。

- [5] IP マスカレードで、TCP の NAT セッション数が多いときに既存の TCP の NAT セッションが削除されると稀にリポートすることがあるバグを修正した。

ただし、nat descriptor backward-compatibility コマンドが 1 に設定されているときは本バグは発現しない。

- [6] IP マスカレードで、IP マスカレード変換セッション数制限機能によって TCP の NAT セッションの作成が制限されたとき、外側ポートが使用中のままになり、TCP セッションが新規に開始できなくなったり、メモリリークが発生したりするバグを修正した。

ただし、nat descriptor backward-compatibility コマンドが 1 に設定されているときは本バグは発現しない。

Rev. 14.01.07 以降で発生する。

- [7] PPTP で、接続処理が始動するときメモリーリークが発生するバグを修正した。
  
- [8] モバイルインターネット機能の WAN インターフェース接続で、リモートアクセスの相手にルーター自ら DHCP サーバーとして IP アドレスを割り当てる設定のとき、LAN インターフェースがリンクアップしていない状態で PPTP および L2TP/IPsec を使用したりリモートアクセス VPN 接続を受けると、DHCP サーバーの DHCP スコープ内のアドレスがすべて使用中の状態になってしまい、IP アドレスを割り当てることができなくなるバグを修正した。
  
- [9] IPsec で、以下の条件をすべて満たす場合に IPsec トンネルを経由するノーマルパスの通信が行えなくなることがあるバグを修正した。
  - LAN インターフェースまたは WAN インターフェースで DHCP によって IP アドレスを取得する設定がされている
  - 上記インターフェースをゲートウェイとして IPsec が確立する
  - トンネルインターフェースで ipsec ike local address コマンドが設定されていない
  
- [10] IPsec で、以下の条件をすべて満たす場合に IPsec トンネルを経由する通信が行えないバグを修正した。
  - ipsec ike esp-encapsulation コマンドによって ESP パケットが UDP でカプセル化される設定が有効になっている
  - UDP でカプセル化されたパケットの送信先となるゲートウェイと、ESP パケットの送信先となるゲートウェイが異なる
  - UDP でカプセル化されたパケットがファストパスで送信される
  
- [11] IPsec で、以下のすべての条件を満たす場合に、正しい設定であっても接続が確立しないバグを修正した。
  - ipsec ike negotiate-strictly コマンドが on に設定されている
  - ipsec ike encryption コマンドで aes256-cbc が設定されている
  
- [12] IKEv2 で、ipsec sa delete コマンドで IKE SA を削除するとき、ipsec ike

message-id-control コマンドが on に設定されていると対向に Delete 要求を送信しないことがあるバグを修正した。

Rev. 14. 01. 09 で発生する。

- [13] IKEv2 で、IKE SA のリキー後に ipsec sa delete コマンドで CHILD SA を削除すると、トンネルがアップしなくなることがあるバグを修正した。
- [14] L2TP/IPsec で、クライアントに対して DNS サーバー情報が通知されず、名前解決を伴う通信ができないことがあるバグを修正した。
- [15] L2TPv3 で、tunnel endpoint name コマンドによって接続先のドメイン名 (FQDN) が指定されている場合、接続処理が始動しないことがあるバグを修正した。
- [16] L2TPv3 で、トンネルの接続中に以下のコマンドによって接続先が変更された場合に、再接続に失敗することがあるバグを修正した。
  - tunnel endpoint address
  - tunnel endpoint name
- [17] データコネクト拠点間接続機能で、送信するパケットがファストパスで処理されるときに、パケットの優先度を示す IPv6 ヘッダのトラフィッククラスの値が低くなるバグを修正した。
- [18] PPTP でトンネルの端点をドメイン名 (FQDN) で指定しているとき、自機からの接続要求と相手側からの接続要求、および対応するドメイン名の IP アドレスの更新のタイミングが重なると、当該 PPTP 上の通信が行えなくなることがあるバグを修正した。
- [19] anonymous インターフェースにおいて、myname オプションを付けて pp auth username コマンドが設定されている場合と同じユーザー名とパスワードを使った複数の接続を同時に受けることができないバグを修正した。
- [20] OSPFv2 でエリア境界ルーター (ABR) として動作しているとき、バックボーンエリアに存在する AS 境界ルーター (ASBR) への経路が不正になったり、誤ったメトリック値を含むタイプ 4 の LSA (ASBR-summary-LSA) をバックボーンエリアに隣接するエリアに広告したりすることがあるバグを修正した。以下の条件に当てはまる場合に発生する。
  - バックボーンエリア側のインターフェースは DROther、隣接する他のエリア側のイ

ンターフェースは DR として動作している

- 両エリアに隣接する ABR が当該ルーター以外にも存在する
- 当該ルーターのバックボーンエリア側のインターフェースがダウンして、当該ルーターを経由していた ASBR への経路が別の ABR 経由に切り替わり、その後ダウンしていたインターフェースが再度アップした

[21] OSPFv2 で、他の OSPF ルーターから受信したタイプ 5 の LSA (AS-external-LSA) の寿命が尽きたとき、当該 LSA に含まれる外部経路は無効な経路であるにもかかわらず、有効な経路として扱われることがあるバグを修正した。

[22] OSPFv3 で、ネイバーのリンクローカルアドレスの取得に失敗することがあるバグを修正した。本バグが発現すると、該当するネイバーが広告する経路を経由した通信ができなくなり、また、show ipv6 route コマンドでその経路のゲートウェイが“-”と表示される。

[23] MLD で、MLDv2 の MLD ルーターとして動作しているとき、ソースリストが空のレポートを新規に受信すると、プロキシ情報とルーティング情報にマルチキャストグループが追加されないバグを修正した。

[24] IPv6 で PPPoE 接続をしているとき、clear status lan コマンドを実行しても show status lan コマンドで表示される IPv6 の送受信パケット数がクリアされないバグを修正した。

[25] ファストパスで、ISDN 回線/専用線、PPTP のトンネルまたはモバイルインターネットを介したデータパケットを受信したときに、ファストパスの処理対象ではないにもかかわらずフローが生成されるバグを修正した。

[26] INTEGER 型の MIB 変数で負数を取得できないバグを修正した。

[27] SNMP で、yrIfTable 配下の MIB 変数に BRIDGE1 のインターフェース番号を Index として指定すると、不正なインターフェース情報が取得されるバグを修正した。

[28] ファームウェアファイルや設定ファイルの書き込みが同時に発生したとき、書き込みが失敗する可能性を排除した。

[29] DHCP サーバー機能で、一部の DHCP リレーサーバーから受信した DHCP パケットを処理

できないバグを修正した。

Rev. 14. 01. 09 で発生する。

[30] L2MS の無線 AP に対するゼロコンフィグ機能で、以下の条件をすべて満たす場合に、工場出荷状態で起動せずファイル名が「経路.conf」のコンフィグファイルを読み込むバグを修正した。

- ap config filename コマンドが設定されていない
- ファイル名が「MAC アドレス.conf」のコンフィグファイルが存在しない
- ファイル名が「経路.conf」のコンフィグファイルが存在する

[31] 異常動作によりリブートしたときに、リブート前の SYSLOG が消えたり show status boot コマンドで表示される起動理由が“Power-on boot”になることがあるバグを修正した。

[32] SFTP 接続で、ファイルやディレクトリの情報を表示したときに不正な更新日時が表示されるバグを修正した。

[33] 以下のコマンドで PP ANONYMOUS01 の情報しか処理されていないバグを修正した。

- clear url filter external-database pp anonymous
- clear url filter pp anonymous
- show url filter
- show url filter external-database
- show url filter external-database pp anonymous
- show url filter pp anonymous

[34] clear mobile access limitation コマンドで、USB インターフェースを指定して実行しても、指定した USB ポートをバインドしている WAN インターフェースの累積のカウンター情報がクリアされず、発信制限が解除されないバグを修正した。

[35] interface reset コマンドでインターフェースに USB/SD インターフェースを指定して実行したとき、または USB バスリセットが発生したときに、デバイスが正しくリセットされないバグを修正した。

Rev. 14. 01. 09 で発生する。



- [36] show status tunnel コマンドで、L2TPv3 トンネルのインターフェースの種類が表示されないバグを修正した。
- [37] show status bgp neighbor advertised-routes コマンドの実行結果で、各パラメータの値として不正な値が出力されるバグを修正した。
- [38] 以下のコマンドのコマンドヘルプの誤記を修正した。
- show status pp
  - url INTERFACE filter コマンド
- [39] Web GUI のダッシュボードのプロバイダー接続状態ガジェットで、PPPoE 接続が切断されているときに表示されるツールチップの「接続時間」の内容が英語で表示されるバグを修正した。
- [40] Web GUI の LAN マップの一覧マップ画面で、WLX302 の VAP16 (5GHz) に接続している端末が表示されないバグを修正した。
- [41] Web GUI の LAN マップの一覧マップ画面で、SWX2200-24G が、LAN マップから制御できない未対応のヤマハスイッチの機器アイコンで表示されるバグを修正した。
- [42] WebGUI の LAN マップの機器一覧画面で、一般ユーザー権限でログインしているときに以下の CSV ファイルをダウンロードするための URL に直接アクセスすると、それぞれの CSV ファイルがダウンロードできるバグを修正した。
- 端末一覧の CSV
  - 端末マスターファイルの CSV
  - スレーブ一覧の CSV
- [43] Web GUI の LAN マップのタグ VLAN 画面で、iOS の端末から利用しているときに、VLAN の参加ポートを選択する際にポートアイコンを 2 回タップしなければならないバグを修正した。
- [44] Web GUI の LAN マップのタグ VLAN 画面で、VLAN の参加ポートを選択するときに、アップリンクポートをクリックしてもポートがアクセスポートとして選択され、上位のスレーブのアップリンクポートおよびダウンリンクポートが自動選択されないバグを修正した。

- [45] Web GUI の LAN マップのタグ VLAN 画面で、制御中のスイッチのポートに設定されているタグ VLAN を削除するときに、対象のスイッチがルーターに接続されているにもかかわらず、「ダウン中のスイッチに設定されている VLAN ID です。」と表示され削除できないことがあるバグを修正した。
- [46] Web GUI の LAN マップのタグ VLAN 画面で、VLAN の参加ポートの設定を変更したときに、アップリンクポートおよびダウンリンクポートのポートアイコンの色が正しく切り替わらないことがあるバグを修正した。
- [47] Web GUI の LAN マップのマルチプル VLAN 画面で、Web ブラウザーのウィンドウ幅が小さい状態で SWX2200-24G のマルチプル VLAN 設定を行うと、「マルチプル VLAN の設定ビュー」内のポートアイコンでウィンドウからはみ出した部分が表示されず、はみ出したポートを選択することができないバグを修正した。
- [48] Web GUI のかんたん設定の[プロバイダー接続]で、IPv6 IPoE 接続または IPv6 PPPoE 接続のプロバイダーを登録しても、設定が保存されないバグを修正した。

Rev. 14. 01. 09 で発生する。

- [49] Web GUI のかんたん設定の[VPN]-[拠点間接続]で、固定の IP アドレスが設定されている PP インターフェースを指定して IP/IP トンネルの設定を追加すると、当該 IP/IP トンネル上で正しく通信できないことがあるバグを修正した。
- [50] Web GUI のかんたん設定の以下の画面で、ユーザー名またはパスワードに以下の記号が含まれているときに、ユーザー名およびパスワードの文字列が画面上に正しく表示されないバグを修正した。
- [VPN]-[拠点間接続]-[拠点間接続 VPN]-[PPTP に関する設定]
    - アンパサンド 「&」
    - ダブルクォーテーション 「"」
    - 左アングルブラケット 「<」
    - 右アングルブラケット 「>」
  - [VPN]-[リモートアクセス]-[リモートアクセス VPN]
    - 左アングルブラケット 「<」
  - [VPN]-[リモートアクセス]-[リモートアクセス VPN]-[ユーザーの登録]
    - シングルクォーテーション 「'」

[51] Web GUI のかんたん設定の[VPN]-[リモートアクセス]で、ユーザー名とパスワードの両方に以下のいずれかの記号を使用して登録ユーザーの新規作成または追加変更を行ったときに、ユーザー名にパスワードと同じ文字列が設定されるバグを修正した。

- シングルクォーテーション「'」
- ダブルクォーテーション「"」
- ナンバー「#」
- 半角スペース「 」
- バックスラッシュ「¥」

[52] Web GUI の詳細設定の[NAT]-[NAT ディスクリプターの設定]で、変換方法として IP マスカレードを選択したときに、静的 NAT の設定の入力欄がグレイアウトするバグを修正した。

[53] Web GUI の詳細設定の[NAT]-[NAT ディスクリプターの設定]で、静的 IP マスカレードのポート番号を「外側ポート番号=内側ポート番号」の形式で指定して静的 IP フィルターの自動設定を有効にすると、設定の確定時にエラーが表示され静的 IP フィルターの設定が行われないバグを修正した。

[54] Web GUI の管理の[アクセス管理]-[ユーザーの設定]で、「接続方法の制限」の設定で「すべて許可する」を選択して設定した後にルーターを再起動して再度同設定画面を開くと、同項目の現在の設定内容として「指定した接続方法を許可する」が選択されているバグを修正した。

[55] Web GUI の以下の画面で、誤記および表記ゆれを修正した。

- LAN マップのマップ画面、タグ VLAN 画面
- かんたん設定の[基本設定]-[LAN1 アドレス]-[入力内容の確認]
- かんたん設定の[基本設定]-[LAN1 アドレス]-[IPv4 アドレスの設定]-[入力内容の確認]-[自動で変更されない設定の一覧]
- 詳細設定の[LAN]-[IPv4 アドレスの設定]-[入力内容の確認]-[自動で変更されない設定の一覧]
- ヘルプページ
  - [ダッシュボード]-[各ガジェットについて]-[システム情報]
  - [LAN マップ]-[LAN マップについて]
  - [LAN マップ]-[マップ]
  - [かんたん設定]-[基本設定]-[LAN1 アドレス]
  - [詳細設定]-[LAN]

- [管理]-[アクセス管理]

[56] OpenSSL の以下の脆弱性対応を行った。

- CVE-2015-1789 (JPCERT/CC JVNVC#91445763)
- CVE-2015-3195 (JPCERT/CC JVNVC#95113540)

IKEv2 の PKI 証明書を利用した認証 (= 「デジタル署名方式」 および 「EAP-MD5 方式」 ) を行う場合に該当する。

この脆弱性の影響により、メモリリークやリブート、ハングアップなどが発生する可能性がある。

[57] クリックジャッキング脆弱性対応を行った。  
(JPCERT/CC JVNVC#48135658)

以上