Revision : 15.00.24

Release : Mar. 2023, ヤマハ株式会社

NVR700W Rev.15.00.24 リリースノート

〇ファームウェアのリビジョンアップを行う前に必ずお読みください

Rev.15.00.11より前のファームウェアからリビジョンアップを行う際には以下の点にご注意ください

Rev.15.00.11では以下の変更をしています。

「NVR700W Rev.15.00.11 リリースノート」より、

http://www.rtpro.yamaha.co.jp/RT/docs/relnote/Rev.15.00/relnote_15_00_11.txt

[1] 本機にアクセスするときのセキュリティーを強化した。

(8) 工場出荷状態の設定にtelnetd host lanコマンドを追加した。

Rev.15.00.11以降のファームウェアを使用して工場出荷状態からプロバイダーを設定すると、上記のコマンドが設定されているため遠隔からTELNETでログインができなくなります。
遠隔からTELNETでログインをする場合はtelnetd hostコマンドの設定を変更してください。

Rev.15.00.23 からの変更点

■機能追加

[1] YNOのLASで、機器統計情報の送信に対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/yno/agent/las/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[2] BIGLOBE IPv6オプションに対応した。

http://www.rtpro.yamaha.co.jp/RT/docs/biglobe/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[3] IKEv2で、Configuration Payloadに対応した。
この変更により、AndroidとiOSの端末でIKEv2を使ったリモートアクセスVPN接続が
可能になる。

http://www.rtpro.yamaha.co.jp/RT/docs/ipsec/ikev2_ras/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[4] コマンドラインからOSPF、BGP、OSPFv3を設定したとき、configure refreshコマンドの実行を促す注意喚起メッセージを表示するようにした。

[5] コマンドラインから以下を設定したとき、再起動を促す注意喚起メッセージを表示するようにした。

- パケットバッファーの設定
- NATの動作タイプの変更

[6] IPヘッダーおよびIPv6ヘッダーのDSフィールドを書き換えるコマンドを追加した。

〇IPパケットのDSフィールドの書き換えの設定

[書式]

ip dscp supersede ID DSCP FILTER_NUM [FILTER_NUM_LIST]

no ip dscp supersede ID [DSCP]

[設定値及び初期値]

・ID

[設定値] : 識別番号 (1..65535)

[初期値] : -

・DSCP

[設定値] :

・書き換えるDSCP値 (0..63)

・以下のニーモニックが利用できる

・cs1/cs2/cs3/cs4/cs5/cs6/cs7/af11/af12/af13/af21/af22/af23/af31/af32/af33/af41/af42/af43/ef

[初期値] : -

・FILTER_NUM

[設定値] : 静的フィルターの番号 (1..21474836)

[初期値] : -

・FILTER_NUM_LIST

[設定値] : 静的フィルターの番号 (1..21474836) の並び

[初期値] : -

[説明]

IP パケットを中継する場合に DS フィールドを指定した値に書き換える。

識別番号順にリストをチェックし、filter_num リストのフィルターを順次適用していく。そして、最初にマッチした IP フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。

reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

ip tos supersede コマンドの設定と本コマンドの設定で条件が同じ場合、本コマンドの設定が優先される。

[ノート]

NVR700W は Rev.15.00.24 以降で使用可能。

〇IPv6パケットのDSフィールドの書き換えの設定

[書式]

ipv6 dscp supersede ID DSCP FILTER_NUM [FILTER_NUM_LIST]

no ipv6 dscp supersede ID [DSCP]

[設定値及び初期値]

・ID

[設定値] : 識別番号 (1..65535)

[初期値] : -

・DSCP

[設定値] :

・書き換えるDSCP値 (0..63)

・以下のニーモニックが利用できる

・cs1/cs2/cs3/cs4/cs5/cs6/cs7/af11/af12/af13/af21/af22/af23/af31/af32/af33/af41/af42/af43/ef

[初期値] : -

・FILTER_NUM

[設定値] : 静的フィルターの番号 (1..21474836)

[初期値] : -

・FILTER_NUM_LIST

[設定値] : 静的フィルターの番号 (1..21474836) の並び

[初期値] : -

[説明]

IPv6 パケットを中継する場合に DS フィールドを指定した値に書き換える。

識別番号順にリストをチェックし、filter_num リストのフィルターを順次適用していく。そして、最初にマッチした IPv6 フィルターが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DS フィールドが書き換えられる。

reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

[ノート]

NVR700W は Rev.15.00.24 以降で使用可能。

[7] ipsec ike durationコマンドで、古くなったSAの寿命を強制的に短縮する時間を設定できるようにした。

〇SAの寿命の設定

[書式]

ipsec ike duration SA GATEWAY_ID SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME] ★

no ipsec ike duration SA GATEWAY_ID [SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]] ★

[設定値及び初期値]

・SA

[設定値] :

設定値　　説明

---

ipsec-sa (もしくは child-sa)　IPsec SA (CHILD SA)

isakmp-sa (もしくは ike-sa)　ISAKMP SA (IKE SA)

[初期値] : -

・GATEWAY_ID

[設定値] : セキュリティー・ゲートウェイの識別子

[初期値] : -

・SECOND

[設定値] : 秒数(300..691200)

[初期値] : 28800

・KBYTES

[設定値] : キロ単位のバイト数(100..100000)

・REKEY : SAを更新するタイミング

[設定値] :

設定値　説明

70% - 90%　パーセント

off　　更新しない(SAパラメーターでisakmp-sa (ike-sa) を指定した

ときのみ設定可能)

[初期値] : 75%

・DEL_TIME

[設定値] : 古くなったSAの寿命を強制的に短縮する時間(1..691200) ★

[初期値] : -

[説明]

各 SA の寿命を設定する。

KBYTES パラメーターを指定した場合には、 SECOND パラメーターで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。

KBYTES パラメーターは SA パラメーターとして ipsec-sa (child-sa) を指定したときのみ有効である。SA の更新は KBYTES パラメーターに設定したバイト数の75%を処理したタイミングで行われる。

REKEY パラメーターは SA を更新するタイミングを決定する。例えば、 SECOND パラメーターで 20000 を指定し、 REKEY パラメーターで75%を指定した場合には、SA を生成してから 15000 秒経過したときに新しい SA を生成する。

REKEY パラメーターは SECOND パラメーターに対する比率を表すもので、KBYTES パラメーターの値とは関係がない。

SA パラメーターで isakmp-sa(ike-sa) を指定したときに限り、REKEY パラメーターで 'off' を設定できる。このとき、 IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、 ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作するIKEのバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1

  始動側として働く場合に、このコマンドで設定した寿命値が提案される。

  応答側として働く場合は、このコマンドの設定に関係なく相手側から提案された寿命値に合わせる。

  また、 ISAKMP SA に対する REKEY パラメーターを off に設定した場合、その効果を得るためには、次の2点に注意して設定する必要がある。

1. IPsec SAよりもISAKMP SAの寿命を短く設定する。
2. ダングリングSAを許可する。すなわち、 ipsec ike restrict-dangling-sa
コマンドの設定をoffにする。

- IKEv2

IKEv2ではSA寿命値は折衝されず、各セキュリティー・ゲートウェイが独立して管理するものとなっている。従って、確立されたSAには、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティー・ゲートウェイの方がSA更新のタイミングが早ければ、 SAはその分早く更新されることになる。

forced-reductionオプションに時間を指定すると、SAを更新した際に古くなった既存のSAの寿命を強制的に設定値に変更し、消滅までの時間を早めることができる。 ★
ただし、KBYTESパラメーターを指定したIPsec SAについては、このキーワードの有無に関わらず古くなった時点で寿命を30秒に短縮する。また、IKEv1では寿命が設定値よりも短い場合は変更しない。 ★

ISAKMP SA (IKE SA)の寿命がIPsec SA (CHILD SA)の寿命より先に尽きた場合は、ISAKMP SA (IKE SA)の寿命値をIPsec SA (CHILD SA)の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在するSAの寿命値は変化せず、新しく作られるSAにのみ、新しい寿命値が適用される。

[ノート]

forced-reductionオプションは以下の機種およびリビジョンで使用可能。
NVR700Wは Rev.15.00.24以降で使用可能。

[8] bgp export filterコマンドのpreferenceオプションが比較するBGP経路の種別を

変更するコマンドを追加した。

〇BGPで受信した経路に対するbgp export filterのpreferenceオプションを使用した
経路選択プロセスの動作を設定 ★

[書式]

bgp export route selection rule RULE

no bgp export route selection rule [RULE]

[設定値及び初期値]

・RULE

[設定値] : ebgp-only, all

設定値　　説明

---

ebgp-only　　eBGPで受信した同じ宛先の経路を比較
対象とする。

all　　全てのBGPで受信した同じ宛先の経路を
比較対象とする。

[初期値] : ebgp-only

[説明]

BGP で同じ宛先の経路を複数の相手から受信した際、一方を選択するための優先度による比較対象を設定する。

本コマンドの設定により bgp export filter コマンドの preference オプションで比較する経路の種別が変更される。

RULE に ebgp-only を設定した場合、eBGP で受信した経路にのみ preference による比較が働く。このため、iBGP で受信した経路では、preference による比較は働かない。

RULE に all を設定した場合、全ての BGP で受信した経路に preference による

比較が働く。このため、eBGP と iBGP で受信した経路間でも、preference による比較が働く。

従来 iBGP で受信した経路は eBGP で受信した経路よりも低い優先度の経路として扱われていたが、RULE に all を指定することで iBGP で受信した経路の優先度を eBGP で受信した経路よりも高くすることが可能になる。
また、bgp export filter コマンドの preference は Local Preference よりも高い優先度であるため、iBGP 経路同士の場合にもより柔軟にネットワークを設計することが可能になる。

本コマンドに対応していないリビジョンでは、RULE が ebgp-only のときの動作をする。

[ノート]

RTpro"BGP-4 仕様[http://www.rtpro.yamaha.co.jp/RT/docs/bgp/index.html]" に掲載している "コマンドで設定した優先度による比較" で比較する経路種別を制御することができる。
eBGP と iBGP 間で同じ宛先の経路を受信する環境下で特定の経路を優先するよう制御したい場合、本コマンドを設定することで実現できる。

NVR700W は Rev.15.00.24 以降で使用可能。

[9] ipv6 routeコマンドで、ゲートウェイにRAにて決定されるデフォルトゲートウェイの指定を追加した。

〇IPv6の経路情報の追加

[書式]

ipv6 route NETWORK gateway GATEWAY [PARAMETER] [gateway GATEWAY [PARAMETER]]

no ipv6 route NETWORK [gateway...]

[設定値及び初期値]

・NETWORK

[設定値]

設定値　　説明

IPv6 アドレス/プレフィックス長　送り先のホスト

default　　デフォルト経路

[初期値] : -

・GATEWAY : ゲートウェイ

[設定値] :

・IP アドレス % スコープ識別子

・pp PEER_NUM [dlci=DLCI] : PP インターフェースへの経路。

"dlci=dlci" が指定された場合は、フレー

ムリレーの DLCI への経路

・PEER_NUM

・相手先情報番号

・anonymous

・pp anonymous name=NAME

設定値 説明

---

name　PAP/CHAP による名前

・dhcp INTERFACE

設定値　説明

INTERFACE DHCP にて与えられるデフォルトゲートウェイを使う場

合の、DHCP クライアントとして動作する LAN インターフェース名、ブリッジインターフェース名(送り先がDefaultの時のみ有効)

・ra INTERFACE ★

設定値　説明

INTERFACE　RA にて決定されるデフォルトゲートウェイを使う場合の、RAクライアントとして動作する LAN インターフェース名、ブリッジインターフェース名(送り先がDefaultの時のみ有効)

・tunnel TUNNEL_NUM : トンネルインターフェースへの経路

・LOOPBACK インターフェース名、NULL インターフェース名

[初期値] : -

・PARAMETER : 以下のパラメーターを空白で区切り複数設定可能

[設定値]

設定値 説明

---

metric メトリックの指定

METRIC　・METRIC

・メトリック値 (1..15)

・省略時は 1

hide　出力インターフェースが LAN インターフェース、または PP インターフェース、TUNNEL インターフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

[初期値] : -

[説明]

IPv6 の経路情報を追加する。LAN インターフェースが複数ある機種ではスコープ識別子でインターフェースを指定する必要がある。インターフェースに対応するスコープ識別子はshow ipv6 address コマンドで表示される。

LAN インターフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

なお LOOPBACK インターフェース、NULL インターフェースは常にアップ状態なので、hide オプションは指定はできるものの意味はない。

[ノート]

RTX1220、RTX1210、RTX830、RTX810 では、PP インターフェースの dlci= オプションは指定できない。

GATEWAY に ra を指定できるのは、RTX1500 / RTX1100 / RT107e Rev.8.03.92以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.24 以降、および、Rev.11.01 系以降のすべてのファームウェアである。

gateway に ra を指定できるのは、NVR700W Rev.15.00.24 以降のファームウェアである。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[10] Web GUIのかんたん設定および詳細設定の[プロバイダー接続]-[IPv4 over IPv6 トンネルの設定]で、以下のサービスに対応した。

- transix
- v6 コネクト
- クロスパス (Xpass)

■仕様変更

[1] DPI機能で、DPIシグネチャーの容量増大に対応するためにDPIシグネチャーの形式を
Ver. 1.1系に変更した。
これ以降、Ver. 1.0系のDPIシグネチャーは読み込めない。
Ver. 1.0系のDPIシグネチャーを読み込もうとした場合はDPI機能が有効にならない。

以下の設定を入れている場合はご注意ください。
- dpi signature download urlコマンドを使用して、DPIシグネチャーの読み込み先
URLを変更
- external-memory dpi signature directoryコマンドを使用して、シグネチャーを
保存する外部メモリーのディレクトリーを設定

http://www.rtpro.yamaha.co.jp/RT/docs/dpi/index.html

外部仕様書をよくご確認のうえ、ご利用ください。

[2] Luaスクリプト機能で、rt.httprequest関数のHTTPリクエスト設定テーブルのurlフィールドの最大文字数を半角255文字から半角2048文字に変更した。

[3] RAプロキシーで、RAによるプレフィックスのpreferred lifetimeが残り60秒になったとき、RSを送出するようにした。

[4] モバイルインターネット接続機能で、モバイル端末をアタッチした際に、自局番号の取得に一定回数失敗したとき、自局番号を取得せずにインターネットに接続できるようにした。

自局番号を取得しない場合、show status usbhost コマンドにて、ダミーの自局番号"----------"が表示される。

[5] show dpi application detailコマンドで、シグネチャーのアプリケーションの説明がマルチバイト文字だった場合には、ヤマハの「Ysig Book」ページへ誘導するメッセージを表示するようにした。

DPIで識別可能なアプリケーション一覧(Ysig Book)については、以下のURLをご覧ください。

http://www.rtpro.yamaha.co.jp/RT/signature/ysig_book/index.html

[6] ipsec ike durationコマンドのKBYTESパラメーターを以下のように変更した。
- 最大値を100000から2147483647に変更
- 初期値なしから2000000に変更

この修正により、初期値で2GBのバイト寿命を持つため、IPsec SA (CHILD SA) が古くなったとき、forced-reductionオプションの設定がない場合でも、自動的に秒寿命が30秒に短縮される。

またバイト寿命の最大値が2,147,483,647KBの機種が始動側になる場合は、相手側機器がバイト寿命の最大値が2,147,483,647KBの機種ではないとき、バイト寿命を必ず2GB以下に設定する必要がある。

〇SAの寿命の設定

[書式]

ipsec ike duration SA GATEWAY_ID SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]

no ipsec ike duration SA GATEWAY_ID [SECOND [KBYTES] [rekey REKEY] [forced-reduction=DEL_TIME]]

[設定値及び初期値]

・SA

[設定値] :

設定値　　説明

---

ipsec-sa (もしくは child-sa)　IPsec SA (CHILD SA)

isakmp-sa (もしくは ike-sa)　ISAKMP SA (IKE SA)

[初期値] : -

・GATEWAY_ID

[設定値] : セキュリティー・ゲートウェイの識別子

[初期値] : -

・SECOND

[設定値] : 秒数(300..691200)

[初期値] : 28800

・KBYTES

[設定値] : キロ単位のバイト数

設定値　　説明

100..2147483647　キロ単位のバイト数 (NVR700W Rev.15.00.24以降のファームウェア) ★

100..100000　キロ単位のバイト数 (その他のファームウェア) ★

off　　設定しない ★

[初期値] :

- 2000000 (NVR700W Rev.15.00.24以降のファームウェア) ★

- off (その他のファームウェア) ★

・REKEY : SAを更新するタイミング

[設定値] :

設定値　説明

70% - 90% パーセント

off　更新しない(SAパラメーターでisakmp-sa (ike-sa) を指定したときのみ設定可能)

[初期値] : 75%

・DEL_TIME

[設定値] : 古くなったSAの寿命を強制的に短縮する時間(1..691200)

[初期値] : -

[説明]

各 SA の寿命を設定する。

KBYTES パラメーターを指定した場合には、 SECOND パラメーターで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。KBYTES パラメーターは SA パラメーターとして ipsec-sa (child-sa) を指定したときのみ有効である。SA の更新は KBYTES パラメーターに設定したバイト数の75%を処理したタイミングで行われる。また、IPsec SA (CHILD SA) が更新されたとき古くなった既存の IPsec SA (CHILD SA) の寿命が 30 秒以上である場合は、寿命が 30 秒に短縮される。★

REKEY パラメーターは SA を更新するタイミングを決定する。例えば、 SECOND パラメーターで 20000 を指定し、 REKEY パラメーターで75%を指定した場合には、SA を生成してから 15000 秒経過したときに新しい SA を生成する。 REKEY パラメーターは SECOND パラメーターに対する比率を表すもので、 KBYTES パラメーターの値とは関係がない。

SA パラメーターで isakmp-sa(ike-sa) を指定したときに限り、REKEY パラメーターで 'off' を設定できる。このとき、 IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、 ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作するIKEのバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

・IKEv1

始動側として働く場合に、このコマンドで設定した寿命値が提案される。
応答側として働く場合は、このコマンドの設定に関係なく相手側から提案された寿命値に合わせる。

また、 ISAKMP SA に対する REKEY パラメーターを off に設定した場合、
その効果を得るためには、次の2点に注意して設定する必要がある。

1. IPsec SAよりも ISAKMP SA の寿命を短く設定する。
2. ダングリングSAを許可する。すなわち、ipsec ike restrict-dangling-sa
   コマンドの設定を off にする。

NVR700W または、RTX1300、vRX が始動側になる場合は、最大で
2147483647 KB のバイト寿命値を相手側へ提案可能であるが、相手側機器が
NVR700W および、RTX1300、vRX 以外の場合は 2 GB を超えるバイト寿命値を正しく認識できないため、NVR700W および、RTX1300、vRX 以外の機種と接続する場合は必ず 2 GB 以下に設定する必要がある。 ★

・IKEv2

IKEv2 では SA 寿命値は折衝されず、各セキュリティー・ゲートウェイが
独立して管理するものとなっている。従って、確立された SA には、常に
このコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティー・ゲートウェイの方が SA 更新のタイミングが早ければ、 SA はその分早く更新されることになる。

forced-reduction オプションに時間を指定すると、SA を更新した際に古くなった既存の SA の寿命を強制的に設定値に変更し、消滅までの時間を早めることができる。ただし、IPsec SA (CHILD SA) で KBYTES パラメーターにバイト寿命値を指定している場合は、DEL_TIME パラメーターで 31 秒以上の値を設定していても、短縮される値は 30 秒となる。また、IKEv1 では寿命が設定値よりも短い場合は変更しない。

ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、 ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在するSAの寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

[ノート]

forced-reduction オプションは以下の機種およびリビジョンで使用可能。

NVR700W は Rev.15.00.24以降で使用可能。

[7] ipsec ike local idコマンド、およびipsec ike remote idコマンドを設定したとき、SAの削除およびIKEの初期化を行うようにした。

[8] tunnel templateコマンド実行時に進捗状況を示すメッセージを出力するようにした。

[9] Web GUIのかんたん設定の[プロバイダー接続]および詳細設定の[プロバイダー接続]で接続種別にIPv6 IPoE接続を選択したとき、以下のIPv4 over IPv6トンネルを設定できるようにした。

- BIGLOBE
  - IPv6 オプション
  - IPv6 サービス (IPIP)

[10] Web GUIの以下のプロバイダー接続の設定時に設定されるLuaスクリプトのインデントを削除した。スクリプトの動作に変更はない。

- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]
  - OCNバーチャルコネクト 固定IP1契約
  - 「v6プラス」固定IPサービス

[11] 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

[12] Web GUIの以下のページで、「v6プラス」固定IPサービスを設定したとき、トンネルインターフェースのMTUの値を1280から1460へ変更した。

- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]

[13] Web GUIのかんたん設定、および詳細設定の[プロバイダー接続]ページで、v6プラスとOCNバーチャルコネクトの表記を一部変更した。

[14] Web GUIの詳細設定の[プロバイダー接続]のヘルプで、「1.概要」の「IPv6 IPoE接続」に説明を追記した。

[15] WebGUIのヘルプにWLX222に関する記述を追加した。

■バグ修正

[1] LANインターフェースやトンネルインターフェースなどの複数のインターフェースで同時にキープアライブがダウンしたとき、リブートすることがあるバグを修正した。

[2] system packet-bufferコマンドを設定して再起動すると、リブートを繰り返すことがあるバグを修正した。

Rev.15.00.17以降で発生する。

[3] pp selectコマンドで接続先を選択している状態、またはswitch selectコマンドでスイッチを選択している状態のときに、tunnel enable/disableコマンドの設定変更やloadコマンドで設定を読み込むと、トンネル接続の設定が正しく反映されなかったり、リブートすることがあるバグを修正した。

[4] 以下のコマンドにより外部メモリーに統計情報を保存する設定がされているとき、ごく稀にリブートすることがあるバグを修正した。
- external-memory statistics filename prefixコマンド
- statisticsコマンド

[5] LANマップで、端末情報が大量に蓄積された状態で新規端末を検出すると、メモリーリークが発生することがあるバグを修正した。

Rev.15.00.21以降で発生する。

[6] Web GUIの詳細設定の[メール通知]-[登録されているメールサーバーの一覧]で、メールサーバーの設定をするとメモリーリークが発生するバグを修正した。

[7] モバイルインターネット接続機能で、SIMカードが正しく認識されていない場合でも、syslogに"found SIM card"と出力するバグを修正した。

Rev.15.00.23以降で発生する。

[8] マルチポイントトンネルで、トンネルの切断後にクライアントが再接続処理を開始しないことがあるバグを修正した。

[9] OSPFとBGPで、自分側アドレスが設定されており相手側アドレスが設定されていないトンネルインターフェースをゲートウェイとする経路を広告できないバグを修正した。

[10] Web GUIのLANマップの接続機器ビューと[一覧マップ]で、SWX2220-10NT/SWX2221P-10NTのポート10配下に端末もしくはL2MSエージェントが接続されているとき、ポート10のVLAN設定を表示するべき箇所にポート9のVLAN設定が表示されるバグを修正した。

[11] DPIが一度もアクティベートしていないときに、DPIを用いたフィルター型ルーティングを使用すると、以下の機能が使用できないバグを修正した。

- DPI
- YNO
- ネットボランチDNS

[12] OCNバーチャルコネクト 固定IP8/16契約で、以下の条件をすべて満たす場合に、MAP-Eトンネルに設定されたグローバルIPv6アドレスが更新されずIPv4通信ができなくなるバグを修正した。

- MAP-EトンネルにIPマスカレードの設定がない
- NGN網を介したリナンバリングが発生した

[13] IPv6機能で、DHCPv6のIRに対するReplyを連続で受信したとき、DNSサーバー情報が取得できないバグを修正した。

[14] LANマップで、端末情報が蓄積された状態で端末管理機能を一旦無効にしてから有効にした場合、検出できる端末の数が減少するバグを修正した。

Rev.15.00.21以降で発生する。

[15] HTTPリビジョンアップ機能で、ファームウェアを更新したときに出力されるログの誤記を修正した。

[16] SNMPで、SERIALポートからのログイン情報を表す以下のMIB変数がSFTPからのログアウトを契機に不当に変更されるバグを修正した。

- yrfLoginSerial
- yrfLoginStatus
- yrfLoginUser

[17] フィルター型ルーティングまたはパケット転送フィルターを使用しているとき、ルーターからtelnetコマンドやrdateコマンドなどを実行すると、通信できないバグを修正した。

[18] コマンドヘルプで、表示する文字列が不当に改行されることがあるバグを修正した。

[19] bgp export filterコマンドで、preference パラメーターによる経路選択が正常に動作しないことがあるバグを修正した。

[20] tunnel templateコマンドで以下のコマンドが展開されないバグを修正した。

- ipsec ike backward-compatibilityコマンド
- ipsec ike mode-cfg methodコマンド
- ipsec ike negotiation receiveコマンド

[21] 以下のコマンドで、不正なオプションを設定することができるバグを修正した。

- dns severコマンド
- dns sever dhcpコマンド

- dns sever ppコマンド
- dns sever pdpコマンド
- dns sever selectコマンド

[22] ip INTERFACE intrusion detectionコマンドで、オプションに誤った文字列を指定したとき、エラーが表示されないバグを修正した。

[23] Web GUIの以下のプロバイダー接続で各設定項目に長い文字列を設定したとき、インターネットに接続できないことがあるバグを修正した。
- OCNバーチャルコネクト 固定IP1契約
- 「v6プラス」固定IPサービス

[24] Web GUIの以下のページで、LAN分割時に、IPv4 over IPv6トンネルの設定ができてしまうバグを修正した。
- かんたん設定の[プロバイダー接続]
- 詳細設定の[プロバイダー接続]

[25] Web GUIの管理の[保守]-[CONFIGファイルの管理]-[CONFIGファイルのインポート]で、末尾に改行コードがないコンフィグファイルをインポートしたとき、最終行の設定内容が反映されないバグを修正した。

[26] Web GUIの[詳細設定]-[プロバイダー接続]で、IPv4 over IPv6トンネルの設定を「使用する」から「使用しない」に変更したとき、IPv4 over IPv6 トンネルの設定が削除されないバグを修正した。

[27] Web GUIの以下のページで、プライマリーDNSサーバーのみアドレスを指定して設定すると、不正なセカンダリーDNSサーバーのアドレスが設定されるバグを修正した。
- かんたん設定の[プロバイダー接続]
  - 内蔵無線WWAN接続

- モバイル接続(イーサネット方式)

[28] Web GUIの以下のページで、8桁のフィルター番号を設定したとき、1の位が表示されないバグを修正した。
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv4 フィルターの一覧]-[インターフェースへの適用の設定]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv4 フィルターの一覧]-[インターフェースへの適用の設定]-[入力内容の確認]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv6 フィルターの一覧]-[インターフェースへの適用の設定]
- 詳細設定の[セキュリティー]-[IPフィルター]-[適用されている IPv6 フィルターの一覧]-[インターフェースへの適用の設定]-[入力内容の確認]

[29] 以下のプロバイダー接続を設定しているとき、Web GUIのかんたん設定からVPN接続の設定をしても接続できないバグを修正した。
- BIGLOBE IPv6サービス(IPIP)
- OCNバーチャルコネクト 固定IP1/8/16契約
- transix IPv4接続(固定IP)
- v6 コネクト IPv4 over IPv6 接続 (IPIP)
- 「v6プラス」固定 IP サービス
- クロスパス (Xpass) 固定 IP1/8/16契約

[30] Web GUIの以下のページで、VLANインターフェースに[DHCP、または固定IPアドレスに接続]を指定して固定IPを設定したとき、WAN側IPアドレスが表示されないバグを修正した。
- かんたん設定の[プロバイダー接続]の「設定内容の確認」
- 詳細設定の[プロバイダー接続]-[設定内容]
- 詳細設定の[プロバイダー接続]-[設定内容]-[基本設定]-[入力内容の確認]

[31] 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。

- 詳細設定の[内蔵無線 WAN]-[ファームウェアの更新]-[ネットワーク経由でファームウェアを更新]-[ファームウェア更新の実行]
- 管理の[本体の設定]-[DOWNLOADボタンの設定]-[ソフトウェアライセンス利用規約]
- 管理の[保守]-[ファームウェアの更新]-[ネットワーク経由でファームウェアを更新]-[ファームウェア更新の実行]

[32] Web GUIのLANマップの以下のページの入力欄で、全角文字が使用できないバグを修正した。

- [機器一覧]-[端末一覧]
- [機器一覧]-[端末情報DB]

Rev.15.00.23以降で発生する。

[33] Web GUIの詳細設定の[DNSサーバー]-[DNSサーバー機能の基本設定]ページで、「DNSサーバー機能を使用する(リカーシブサーバー)」を設定したとき、dns serviceコマンドの初期値が明示的に設定されるバグを修正した。

[34] Web GUIのかんたん設定の[プロバイダー接続]で、IPv6 PPPoE接続を設定したとき、ppp ipcp msext onコマンドが設定されないバグを修正した。

[35] Web GUIの管理の[保守]-[コマンドの実行]で、入力できないコマンドが入力できてしまうことがあるバグを修正した。

[36] Web GUIの[管理]-[保守]-[コマンドの実行]のヘルプページの実行できないコマンド一覧に、以下のコマンドを追記した。

- administrator passwordコマンド
- administrator password encryptedコマンド
- copyコマンド
- copy execコマンド
- deleteコマンド
- delete execコマンド
- execute batchコマンド
- lessで始まるコマンド
- login passwordコマンド
- login password encryptedコマンド
- make directoryコマンド
- password reenterコマンド
- renameコマンド
- rtfs formatコマンド
- rtfs garbage-collectコマンド
- scpコマンド
- sshコマンド
- sshd host key generateコマンド
- '|' でgrepを連結したコマンド
- '|' でlessを連結したコマンド

[37] Web GUIの管理の[保守]-[コマンドの実行]で、以下のコマンドが入力できないバグを修正した。

- administrator radius auth コマンド
- ssh encrypt algorithm コマンド
- ssh known hosts コマンド

[38] Web GUIの以下のページで、誤記を修正した。

- LANマップの[マップ]-[機器詳細と設定]

- ヘルプページ

- LANマップの[詳細]-[マップ]

[39] コマンドヘルプの誤記を修正した。

■更新履歴

Mar. 2023, Rev.15.00.24 リリース

以上