Biz Box ルータ「N1200」
ファームウェアリリースノート
Rev.10.01.39

Rev.10.01.39

以下のとおり機能追加・機能改善が行われました。

1. 本バージョンで追加された項目

（1）フレッツ光ネクストにおけるインターネット(IPv6 IPoE/IPv6 PPPoE)接続に対応した。

（2）自動ファームウェアアップデート機能に対応した。

（3）GUI からモバイルインターネット接続を設定できるようにした。

（4）SNMPv3 で VACM に対応した。

（5）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 L-02A
- docomo L-05A
- docomo L-08C
- docomo L-02C(※1)
- EMOBILE D01HW
- EMOBILE D02HW
- EMOBILE D21HW
- EMOBILE D22HW
- EMOBILE D23HW
- EMOBILE D12LC
- EMOBILE D11LC
- EMOBILE D31HW
- EMOBILE D32HW
- EMOBILE D33HW
- EMOBILE D41HW
- EMOBILE GD01
- KDDI DATA03(※2)
- KDDI DATA07
- NTT コム MF111
- NTT コム MF121
- NTT コム MF110
- NTT コム MF120
- SoftBank C01LC
- SoftBank C02HW
- SoftBank 004Z
- SoftBank C01SW

- SoftBank C02LC
- SoftBank C02SW
- WILLCOM HX006ZT
- WILLCOM HX008ZT
- WILLCOM HX001IN
- WILLCOM HX003ZT
- WILLCOM HX002IN
- WILLCOM HX004IN
- IIJ モバイル 110FU
- IIJ モバイル 120FU(TypeD)
- IIJ モバイル 120FU(TypeDS)
- IIJ モバイル D22HW(TypeE)
- IIJ モバイル D22HW(TypeES)
- 日本通信 MF636-BKIC(I・Care3G)
- 日本通信 MF626-BKIC(I・Care3G)
- 日本通信 BM-DC1-500M(b-mobile Doccica)
- 日本通信 BM-DL3-150H(b-mobile 3G)

※1 … docomo L-02C のファームウェアバージョンを V10b 以降にする必要がある。

※2 … 本来 DATA03 は、WiMAX と CDMA の両エリアで使用可能なデータ通信端末だが、今回の対応では、CDMA エリアでの利用が可能となるようにした。WiMAX を利用した通信には対応していない。

(6)モバイルインターネット機能で、PIN コード設定端末を利用できるようにした。

〇携帯端末に入力する PIN コードの設定

[書式]

mobile pin code INTERFACE PIN

no mobile pin code INTERFACE [PIN]

[設定値及び初期値]

INTERFACE

[設定値] :

設定値	説明
usb1	USB1 インタフェース

[初期値] : -

PIN

[設定値] : PIN コード

[初期値] : -

[説明]

USB インタフェースに接続する携帯端末の使用に PIN コードを必要とする場合に、用いる PIN コードを設定する。

携帯端末が PIN コードを必要としない場合には、本コマンドの設定に関係なく携帯端末を使用することができる。

[ノート]

PIN コードを利用する場合は、予め携帯端末の接続ユーティリティ等を使用して SIM カードに PIN コード

を登録する必要がある。ルーターでは SIM カードに PIN コードを登録することはできない。
SIM カードに登録された PIN コードと本コマンドの設定が一致せず、3 回連続して失敗すると、携帯端末は自動的にロック(PIN ロック)される。PIN ロックがかかるとルーターでは解除できない。携帯端末の接続ユーティリティにて PIN ロック解除コードを入力する必要がある。

（7）SNMP でデータ通信端末の情報取得と電波強度トラップ送信に対応した。
トラップについては yrIfMobileStatusTrap を送出する。このトラップは、ルーターが電波強度を取得した時に snmp trap mobile signal-strength の設定と一致した場合に送出される。

〇電波強度トラップを送信するか否かの設定
[書式]
snmp trap mobile signal-strength SWITCH [ANTENNALEVEL]
no snmp trap mobile signal-strength [SWITCH [ANTENNALEVEL]]
[設定値及び初期値]
SWITCH:トラップの送信設定
[設定値] :

設定値	説明
on	トラップを送信する
off	トラップを送信しない

[初期値] : off
LEVEL:アンテナ本数の閾値
[設定値] :

設定値	説明
0.3	アンテナ本数
省略	省略時は圏外

[初期値] : -
[説明]
モバイル端末の電波強度トラップを送信するか否かを設定する。
自動/手動に関わらず、ルーターが電波強度を取得した時にトラップ送信が許可されており、電波強度のアンテナ本数が閾値以下であった場合にトラップが送信される。

（8）L2TP/IPsec に対応した。
制限事項については以下の通り。
・L2TP 単体での機能は提供しません。L2TP/IPsec のみサポートします。
・リモートアクセス VPN のサーバーとして動作します。クライアントとしては動作しません。
・LAN 間接続 VPN には対応していません。
・L2TP パケットの最初の待ち受けは UDP のポート番号 1701 が使用されます。変更することはできません。
・IKEv1 にのみ対応しており、IKEv2 は使用できません。

・グローバル IP アドレスが付与されない 3G 網からでも L2TP/IPsec 接続を利用することができます。(NAT トラバーサルを用いた L2TP/IPsec 接続に対応)
・L2TP/IPsec の anonymous 接続と PPTP の anonymous 接続を併用することができます。
・L2TP/IPsec によって確立した L2TP トンネルを経由するパケットはファストパスで処理されます。
ただし、以下の条件に合致するパケットはノーマルパスで処理されます。
-フラグメントされているパケット
-フラグメントする必要があるパケット
-PP インタフェースで CCP による圧縮をする必要があるパケット
-PP インタフェースで VJC(Van Jacobson 圧縮)をする必要があるパケット
・L2TP/IPsec 接続の PPP 認証では、PAP または CHAP を用いた RADIUS 認証を利用することができます。

(9)IPsec のハッシュアルゴリズムとして SHA-256 に対応した。
また暗号アルゴリズム AES-CBC において鍵長 256bit に対応した。

〇IKE が用いる暗号アルゴリズムの設定
[書式]
ipsec ike encryption GATEWAY_ID ALGORITHM
no ipsec ike encryption GATEWAY_ID [ALGORITHM]
[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] : -
ALGORITHM
[設定値] :

設定値	説明
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES128-CBC
aes256-cbc	AES256-CBC ★

[初期値] : 3des-cbc
[説明]
IKEv1 として動作する際に用いる暗号アルゴリズムを設定する。始動側として働く場合に、本コマンドで設定されたアルゴリズムを提案する。応答側として働く場合は本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。ただし、ipsec ike negotiate-strictly コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。
[ノート]
IKEv2 で暗号アルゴリズムを折衝する際は、本コマンドの設定にかかわらず動的に決定される。具体的に、始動側として働く場合はサポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は、提案されたものからより安全なアルゴリズムを選択する。

AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

※IKEv2 でのみ AES192-CBC をサポート

〇IKE が用いるハッシュアルゴリズムの設定

[書式]

ipsec ike hash GATEWAY_ID ALGORITHM

no ipsec ike hash GATEWAY_ID [ALGORITHM]

[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] : -

ALGORITHM

[設定値] :

設定値	説明
md5	MD5
sha	SHA-1
sha256	SHA-256 ★

[初期値] : sha

[説明]

IKEv1 として動作する際に用いるハッシュアルゴリズムを設定する。始動側として働く場合に、本コマンドで設定されたアルゴリズムを提案する。応答側として働く場合は本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。

ただし、ipsec ike negotiate-strictly コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。

[ノート]

IKEv2 では、IKEv1 のハッシュアルゴリズムに相当する折衝パラメータとして、認証アルゴリズム(Integrity Algorithm)と PRF(Pseudo-Random Function)がある。

ただし、これらのパラメータを折衝する際は、本コマンドの設定にかかわらず動的に決定される。

具体的に、始動側として働く場合はサポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は、受け取った提案から以下の優先順位でアルゴリズムを選択する。

- 認証アルゴリズム

  HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

- PRF

  HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

〇SA のポリシーの定義

[書式]

ipsec sa policy POLICY_ID GATEWAY_ID ah AH_ALGORITHM [local-id=LOCAL-ID]
[remote-id=REMOTE-ID] [anti-replay-check=CHECK]

ipsec sa policy POLICY_ID GATEWAY_ID esp ESP_ALGORITHM [AH_ALGORITHM]

[anti-replay-check=CHECK]

no ipsec sa policy POLICY_ID [GATEWAY_ID]

[設定値及び初期値]

POLICY_ID

[設定値] : ポリシーID(1..2147483647)

[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] : -

AH_ALGORITHM : 認証アルゴリズム

[設定値] :

設定値	説明
md5-hmac	HMAC-MD5
sha-hmac	HMAC-SHA-1
sha256-hmac	HMAC-SHA2-256 ★

[初期値] : -

ESP_ALGORITHM : 暗号アルゴリズム

[設定値] :

設定値	説明
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES128-CBC
aes256-cbc	AES256-CBC ★

[初期値] : -

LOCAL-ID

[設定値] : 自分側のプライベートネットワーク

[初期値] : -

REMOTE-ID

[設定値] : 相手側のプライベートネットワーク

[初期値] : -

CHECK

[設定値] :

設定値	説明
on	シーケンス番号のチェックを行う
off	シーケンス番号のチェックを行わない

[初期値] : on

[説明]

SA のポリシーを定義する。この定義はトンネルモードおよびトランスポートモードの設定に必要である。この定義は複数のトンネルモードおよびトランスポートモードで使用できる。

LOCAL-ID、REMOTE-ID には、カプセル化したいパケットの始点/終点アドレスの範囲をネットワークアドレスで記述する。これにより、1 つのセキュリティ・ゲートウェイに対して、複数の IPsec SA を生成し、IP パケットの内容に応じて SA を使い分けることができるようになる。

CHECK=on の場合、受信パケット毎にシーケンス番号の重複や番号順のチェックを行い、エラーとなるパケットは破棄する。破棄する際には debug レベルで

[IPSEC] sequence difference

[IPSEC] sequence number is wrong

といったログが記録される。

相手側が、トンネルインタフェースでの優先/帯域制御を行っている場合、シーケンス番号の順序が入れ替わってパケットを受信することがある。その場合、実際にはエラーではないのに上のログが表示され、パケットが破棄されることがあるので、そのような場合には設定を off にするとよい。

IKEv2 として動作する場合、AH_ALGORITHM、及び ESP_ALGORITHM パラメータは効力を持たず、これらのアルゴリズムは折衝時に動的に決定される。

具体的に、始動側として働く場合はサポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は、受け取った提案から以下の優先順位でアルゴリズムを選択する。

- 認証アルゴリズム

  HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

- 暗号アルゴリズム

  AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

  ※IKEv2 でのみ AES192-CBC をサポート

また、IKEv2 では LOCAL-ID、REMOTE-ID パラメータに関しても効力を持たない。

[ノート]

双方で設定する LOCAL-ID と REMOTE-ID は一致している必要がある。

(10)IKEv2 で、CREATE_CHILD_SA 交換に対応した。

なお、対向側の本製品が本リビジョンより古い場合、自機から鍵交換を始動しても接続できない。
データコネクトを利用した拠点間接続で、IPsec 方式で接続する場合も同様である。

(11)RADIUS を使用したログインユーザーの管理機能を追加した。

制限事項は以下の通り。

・RADIUS アカウンティングには対応していません。

・無名ユーザーの認証に RADIUS サーバーを使用することはできません。

(12)DiffServ ベース QoS に対応した。

(13)リブートログ保存機能に対応した。

(14)HTTP リビジョンアップ機能において、HTTP リダイレクトに対応した。

http revision-up url コマンドで指定された URL への HTTP 要求に対して、以下のステータスコードが応答として返された場合には HTTP ヘッダー内の"Location:"で指定された URL を用いて HTTP リビジョンアップを行う。

〇HTTP ステータスコード

- HTTP1.0 301 Moved Permanently
- HTTP1.1 301 Moved Permanently
- HTTP1.0 302 Moved Temporarily
- HTTP1.1 302 Found
- HTTP1.1 307 Temporary Redirect

〇対応したリビジョンアップ手段

- http revision-up go コマンドの実行
- ダウンロードボタン押下

(15)RIPng による経路の優先度を設定するコマンドを追加した。

〇RIPng による経路の優先度の設定

[書式]

ipv6 rip preference PREFERENCE

no ipv6 rip preference [PREFERENCE]

[設定値及び初期値]

PREFERENCE

[設定値] : RIPng による経路の優先度(1..2147483647)

[初期値] : 1000

[説明]

RIPng による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。

RIPng とスタティックなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

[ノート]

静的経路の優先度は 10000 で固定である。

（16）DNS フォールバック動作をルーター全体で統一することができるようにした。

〇DNS フォールバック動作をルーター全体で統一するか否かの設定

[書式]

dns service fallback SWITCH

no dns service fallback

[設定値と初期値]

SWITCH

[設定値] :

設定値	説明
on	DNS フォールバック動作を IPv6 優先に統一する
off	DNS フォールバック動作は機能ごとにまちまちである

[初期値] : off

[説明]

DNS フォールバック動作をルーターのすべての機能で統一するか否かを設定する。

DNS でホスト名を IP アドレスに変換する場合、IPv4/IPv6 いずれかを DNS サーバーに先に問い合わせ、アドレスが解決できない場合に他方のアドレスを問い合わせる動作を、DNS フォールバックと呼ぶ。ルーター自身が問い合わせる場合、IPv4 を優先するか IPv6 を優先するかは機能ごとにまちまちであった。具体的には、以下の機能では DNS フォールバック動作では IPv6 が優先されるが、その他の機能では IPv4 が優先されている。

- HTTP リビジョンアップ機能
- HTTP アップロード機能

このコマンドを on に設定すると、ルーターのすべての機能で IPv6 が優先されるようになる。

[ノート]

DNS リカーシブサーバーとして、LAN 内の PC 等の問い合わせを上位の DNS サーバーに転送する際には、PC 等の問い合わせ内容をそのまま上位サーバーに転送するため、DNS フォールバックの動作も PC 等の実装がそのまま反映され、このコマンドの設定には影響を受けない。

（17）インタフェースのカウンター情報をクリアするコマンドを追加した。

〇インタフェースのカウンター情報のクリア

[書式]

clear status INTERFACE

clear status pp PNUM

clear status tunnel TUNNEL_NUM

[設定値及び初期値]

INTERFACE

[設定値] : LAN インタフェース名

[初期値] : -

PNUM

[設定値] : 相手先情報番号

[初期値] : -

TUNNEL_NUM

[設定値] : トンネルインタフェース番号

[初期値] : -

[説明]

指定したインタフェースのカウンター情報をクリアする。

(18)DNS キャッシュの内容を表示するコマンドを追加した。

○DNS キャッシュの内容を表示する

[書式]

show dns cache

[説明]

DNS キャッシュの内容を表示する。

(19)SIP 着信時にユーザー名を検証するか否かを設定するコマンドを追加した。

○SIP 着信時にユーザー名を検証するか否かの設定

[書式]

sip arrive address check SWITCH

no sip arrive address check [SWITCH]

[設定値及び初期値]

SWITCH

[設定値] : 'on' or 'off'

[初期値] : on

[説明]

SIP の着信時にユーザー名が正常か否かを検証する設定をする。

2 本バージョンで仕様変更された機能

（1）PPTP で、パケットの圧縮タイプとして MPPE を設定した場合、CCP Reset-Request 送信後に CCP Reset-Ack が返ってこなくても、FLUSHED bit がセットされた compressed パケットを受信することにより CCP Reset-Ack 受信時と同様の処理を行うようにした。

（2） ipv6 INTERFACE address コマンドでアドレスのタイプ（'unicast'、'anycast'）を設定できるようにした。

〇インタフェースの IPv6 アドレスの設定

[書式]

ipv6 INTERFACE address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
ipv6 INTERFACE address auto
ipv6 INTERFACE address dhcp
ipv6 pp address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
ipv6 pp address auto
ipv6 pp address dhcp
ipv6 tunnel address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
ipv6 tunnel address auto
ipv6 tunnel address dhcp
no ipv6 INTERFACE address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
no ipv6 INTERFACE address auto
no ipv6 INTERFACE address dhcp
no ipv6 pp address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
no ipv6 pp address auto
no ipv6 pp address dhcp
no ipv6 tunnel address IPV6_ADDRESS/PREFIX_LEN [ADDRESS_TYPE]
no ipv6 tunnel address auto
no ipv6 tunnel address dhcp

[設定値及び初期値]

INTERFACE
[設定値] : LAN インタフェース名、LOOPBACK インタフェース名
[初期値] : -

IPV6_ADDRESS
[設定値] : IPv6 アドレス部分
[初期値] : -

PREFIX_LEN
[設定値] : IPv6 プレフィックス長
[初期値] : -

ADDRESS_TYPE ★
[設定値] :

設定値	説明
unicast	ユニキャスト
anycast	エニーキャスト

[初期値] : unicast

auto : RA で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード

[初期値] : -

dhcp : DHCPv6 で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード

[初期値] : -

[説明]

インタフェースに IPv6 アドレスを付与する。

[ノート]

このコマンドで付与したアドレスは、show ipv6 address コマンドで確認することができる。
複数の LAN インタフェースでアドレスを自動で設定する機能を利用することができる。
具体的には、RA で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能と、DHCPv6 で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能が利用できる。
これらを設定する場合、デフォルト経路は最後に設定が完了したインタフェースに向く。
LOOPBACK インタフェースを指定した場合は、auto、dhcp、ADDRESS_TYPE は指定できない。

（3）ipv6 INTERFACE rtadv send コマンドで以下のオプションを指定できるようにした。

- adv-retrans-time
- adv-cur-hop-limit

〇ルーター広告の送信の制御

[書式]

ipv6 INTERFACE rtadv send PREFIX_ID [PREFIX_ID...] [OPTION=VALUE...]

ipv6 pp rtadv send PREFIX_ID [PREFIX_ID...] [OPTION=VALUE...]

no ipv6 interface rtadv send [...]

no ipv6 pp rtadv send [...]

[設定値及び初期値]

INTERFACE

[設定値] : LAN インタフェース名

[初期値] : -

PREFIX_ID

[設定値] : プレフィックス番号

[初期値] : -

OPTION=VALUE : NAME=VALUE の列

[設定値] :

NAME	VALUE	説明
m_flag	on、off	managed address configuration フラグ。ルーター広告による自動設定とは別に、DHCPv6 に代表されるルーター広告以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。
o_flag	on、off	other stateful configuration フラグ。ルーター広告以外の手段により|IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。
max-rtr-adv-interval	秒数	ルーター広告を送信する最大間隔(4-1,800 秒)
min-rtr-adv-interval	秒数	ルーター広告を送信する最小間隔(3-1,350 秒)
adv-default-lifetime	秒数	ルーター広告によって設定される端末のデフォルト経路の有効時間(0-9,000 秒)
adv-reachable-time	ミリ秒数	ルーター広告を受信した端末が、ノード間で確認した到達性の有効時間(0-3,600,000 ミリ秒)
adv-retrans-time	ミリ秒数	ルーター広告を再送する間隔(0-4,294,967,295 ミリ秒)
adv-cur-hop-limit	ホップ数	ルーター広告の限界ホップ数(0-255)
mtu	auto、 off、 バイト数	ルーター広告に MTU オプションを含めるか否かと、含める場合の値の設定。auto の場合はインタフェースの MTU を採用する。

[初期値]

m_flag = off

o_flag = off

max-rtr-adv-interval = 600

min-rtr-adv-interval = 200

adv-default-lifetime = 1800

adv-reachable-time = 0

adv-retrans-time = 0

adv-cur-hop-limit = 64

mtu = auto

[説明]

インタフェースごとにルーター広告の送信を制御する。送信されるプレフィックスとして、ipv6 prefix コマンドで設定されたものが用いられる。また、オプションとして m_flag および o_flag を利用して、管理するホストがルーター広告以外の自動設定情報をどのように解釈するかを設定することができる。オプションでは、送信するルーター広告の送信間隔や、ルーター広告に含まれる情報の設定を行うこともできる。

(4)ipv6 prefix コマンドの preferred-lifetime オプションと valid-lifetime オプションで設定できる値の範囲を以下のように変更した。

変更前:60-15552000

変更後:0-4294967295(=0xFFFFFFFF)

（5）ping6 コマンドでパケットサイズ、送信元アドレス、送信間隔を指定できるようにした。

〇ping6 の実行

[書式]

ping6 [-s LENGTH] [-c COUNT] [-sa SOURCE] [-w WAIT] DESTINATION

ping6 [-s LENGTH] [-c COUNT] [-sa SOURCE] [-w WAIT] DESTINATION%SCOPE_ID

ping6 [-s LENGTH] [-c COUNT] [-sa SOURCE] [-w WAIT] DESTINATION
INTERFACE

ping6 [-s LENGTH] [-c COUNT] [-sa SOURCE] [-w WAIT] DESTINATION pp
PEER_NUM

ping6 [-s LENGTH] [-c COUNT] [-sa SOURCE] [-w WAIT] DESTINATION tunnel
TUNNEL_NUM

[設定値及び初期値]

LENGTH

[設定値]： データ長(1..65535)

[初期値]：64

COUNT

[設定値]： 実行回数(1..21474836)

[初期値]：Ctrl+c キーが入力されるまで繰り返す

SOURCE

[設定値]： 始点 IPv6 アドレス

[初期値]： ルーターのインタフェースに付与されたアドレスの中から選択する

WAIT

[設定値]： パケット送信間隔秒数(0.1..99.9)

[初期値]：1

DESTINATION

[設定値]： 送信する宛先の IPv6 アドレス、または名前

[初期値]：-

SCOPE_ID

[設定値]： スコープ識別子

[初期値]：-

INTERFACE

[設定値]：LAN インタフェース名

[初期値]：-

PEER_NUM

[設定値]： 相手先情報番号

[初期値]：-

TUNNEL_NUM

[設定値]：トンネルインタフェース番号

[初期値]：-

[説明]

指定した宛先に対して ICMPv6 Echo Request を送信する。

スコープ識別子は、show ipv6 address コマンドで表示できる。

COUNT パラメータを省略すると、Ctrl+C キーを入力するまで実行を継続する。
-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-wオプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

（6）ping コマンドで送信可能なデータサイズの最小値を 1 に変更した。

（7）DHCPv6 クライアント機能で、Inform-Request を送信できるように変更した。

〇DHCPv6 の動作の設定

[書式]

ipv6 INTERFACE dhcp service TYPE
ipv6 INTERFACE dhcp service client [ir=VALUE]
ipv6 pp dhcp service TYPE
ipv6 pp dhcp service client [ir=VALUE]
ipv6 tunnel dhcp service TYPE
ipv6 tunnel dhcp service client [ir=VALUE]
no ipv6 INTERFACE dhcp service
no ipv6 pp dhcp service
no ipv6 tunnel dhcp service

[設定値及び初期値]

INTERFACE

[設定値] : LAN インタフェース名

[初期値] : -

TYPE

[設定値] :

設定値	説明
off	DHCPv6 を使わない
client	クライアント
server	サーバー

[初期値] : off

VALUE ★

[設定値] :

設定値	説明
on	クライアントとして動作する時、Inform-Request を送信する
off	クライアントとして動作する時、Solicit を送信する

[初期値] : off

[説明]

各インタフェースにおける DHCPv6 の動作を設定する。

(8)DHCPv6 サーバー機能で、上位のサーバーからプレフィックスなどの情報を取得するまでルーター配下の端末からの Inform-Request に応答しないようにした。

また、Inform-Request に応答できる場合には、Domain Search List(24)、SNTP Servers(31)オプションに上位サーバーから取得した情報を応答するようにした。

(9)DHCPv6 クライアント機能で、Request、Inform-Request の要求オプションリストに Domain Search List(24)、SNTP Servers(31)を設定するようにした。

(10)DHCPv6-PD プロキシ機能で、取得したプレフィックスを基に複数のプレフィックスを動的に生成した場合、インタフェース毎に異なるプレフィックスを配布できるようにした。

なお、DHCPv6-PD で取得したプレフィックス長が、配布するプレフィックス長より短い場合のみ上記動作となる。

(11)DHCP サーバー機能で、1～49、62～254 のオプション番号を dhcp scope option コマンドで設定できるように変更した。

○DHCP オプションの設定

[書式]

dhcp scope option SCOPE_NUM OPTION=VALUE

no dhcp scope option SCOPE_NUM [OPTION=VALUE]

[設定値及び初期値]

SCOPE_NUM

[設定値]: スコープ番号(1..65535)

[初期値]: -

OPTION

[設定値]:

・オプション番号(1..49,62..254)またはニーモニック ★

・主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

[初期値]: -

VALUE: オプション値

[設定値]:

・値としては以下の種類があり、どれが使えるかはオプション番号で決まる。例えば、'router','dns','wins_server'は IP アドレスの配列であり、'hostname','domain'は文字列である。

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット整数の配列	2 オクテット整数をコンマ(,)で並べたもの
4 オクテット整数	0..2147483647
IP アドレス	IP アドレス
IP アドレスの配列	IP アドレスをコンマ(,)で並べたもの
文字列	文字列
スイッチ	"on","off","1","0"のいずれか
バイナリ	2 桁十六進数をコンマ(,)で並べたもの

[初期値]: -

[説明]

スコープに対して送信する DHCP オプションを設定する。dns server コマンドや wins server コマンドなどでも暗黙のうちに DHCP オプションを送信していたが、それを明示的に指定できる。また、暗黙の DHCP オプションではスコープでオプションの値を変更することはできないが、このコマンドを使えばそれも可能になる。

[ノート]

no dhcp scope コマンドでスコープが削除されるとオプションの設定もすべて消える。

(12)IPv4 ファストパスのフローを消すタイミングを、フローの生成時刻からの一定時間経過後から、当該フローを利用するパケットの最終通過時刻からの一定時間経過後に変更した。なお、一定時間とは ip flow timer コマンドで設定されている時間を指す。

(13)IPv4 over IPv6/IPv6 over IPv6 の IPsec トンネルで、一つの SA でノーマルパスとファストパスの双方でパケットを送信しているときに、ノーマルパスのパケットに ESP のシーケンス番号を付与してから実際にそれを送信するまでの間に、ファストパスのパケットの処理が進んでしまい、ノーマルパスのパケットが追い越されてしまった際に、追い越されてしまう数によっては受信側でのアンチリプレイチェックによりノーマルパスでのパケットが破棄されてしまうことがあった。そのため、ノーマルパスでのパケットを実際に送信する直前に再度シーケンス番号の確認を行い、必要であればシーケンス番号を付け直すように変更した。

(14)IKEv2 で以下の仕様変更をした。

- IKEv2 で送信するリクエストの SA プロポーザルにおいて、DH グループを提案する際にサポート可能なグループを全て含めるようにした。
- ipsec ike nat-traversal コマンドのオプションで'force=on'と指定した場合、IKE_SA_INIT 交換から UDP4500 番ポートを使用して鍵交換を始動するようにした。
- SYSLOG の出力内容の一部を変更、追加した。

なお、対向側の本製品が本リビジョンより古い場合、自機から鍵交換を始動しても接続できない。
データコネクトを利用した拠点間接続で、IPsec 方式で接続する場合も同様である。

(15)EAP-MD5 認証で証明書要求ペイロードを送信できるようにした。

○EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定

[書式]

ipsec ike eap send certreq GATEWAY_ID SWITCH

no ipsec ike eap send certreq GATEWAY_ID [SWITCH]

[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] : -

SWITCH

[設定値] :

設定値	説明
on	送信する
off	送信しない

[初期値] : off

[説明]

EAP-MD5 認証方式の場合、始動側のセキュリティ・ゲートウェイから送信する IKE_AUTH 交換に、証明書要求(CERTREQ)ペイロードを含めるか否かを設定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

(16)データコネクトサービスを利用した拠点間接続で、追加番号による拠点間接続をできるようにした。

○NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定

[書式]

tunnel ngn interface LAN

no tunnel ngn interface [LAN]

[設定値及び初期値]

LAN

[設定値] :

設定値	説明
auto	自動設定
LAN インタフェース名	LAN ポート

[初期値] : auto

[説明]

NGN 網を介したトンネルインタフェースで使用する LAN インタフェースを設定する。

auto に設定した時はトンネルインタフェースで設定した電話番号を利用して、使 用する LAN インタフェースを決定する。

追加番号を使用する場合に設定する。

(17)データコネクトサービスを利用した拠点間接続で、特定の帯域での着信のみ許可する設定ができるようにした。

〇NGN 網を介したトンネルインタフェースの帯域の設定

[書式]

tunnel ngn bandwidth BANDWIDTH [arrivepermit=SWITCH]

no tunnel ngn bandwidth [BANDWIDTH arrivepermit=SWITCH]

[設定値及び初期値]

BANDWIDTH

[設定値] :

設定値	説明
64k	64kbit/s
512k	512kbit/s
1m	1Mbit/s

[初期値] : 1m

SWITCH ★

[設定値] :

設定値	説明
on	帯域の設定と一致しない着信も許可する
off	帯域の設定と一致した着信のみ許可する

[初期値] : on

[説明]

NGN 網を介したトンネルインタフェースの帯域を設定した値にする。

帯域の設定が一致しない着信について、arrivepermit オプションが off の場合は着信せず、on の場合は着信する。

[ノート]

通信中の変更は無効である。

(18)show account コマンドでデータコネクト接続の料金情報を表示するようにした。

また、データコネクト拠点間接続設定毎の料金情報も表示できるようにした。

表示される料金情報はあくまでも目安で、2011 年 7 月現在の料金表を参考に通信時間と接続帯域からルーター内部で計算しているため、実際に請求される料金とは異なる場合がある。

〇データコネクトのアカウントの表示

[書式]

show account ngn data

[説明]
データコネクトの発着信回数や料金情報を表示する。

〇TUNNEL アカウントの表示
[書式]
show account tunnel [TUNNEL_NUM]
[設定値及び初期値]
TUNNEL_NUM
[設定値]： 相手先情報番号
省略時、選択されている相手について表示する
[初期値]：－
[説明]
指定したデータコネクト接続設定がされているトンネルインタフェースについて発着信回数や料金情報を表示する。
発信回数、着信回数は切断時にカウントされる。
料金情報は再起動によりクリアされる。
account threshold コマンドで設定される閾値を超えたか否かの計算には、データコネクト分の料金は含まれない。

〇データコネクトのアカウントのクリア
[書式]
clear account ngn data
[説明]
データコネクトのアカウントをクリアする。

〇TUNNEL アカウントのクリア
[書式]
clear account tunnel [TUNNEL_NUM]
[設定値及び初期値]
TUNNEL_NUM
[設定値]： 相手先情報番号
省略時、選択されている相手について表示する
[初期値]：－
[説明]
指定したデータコネクト接続設定がされているトンネルインタフェースに関するアカウントをクリアする。

(19)SIP の OPTIONS リクエストに対して応答をしないように変更した。

(20)PAP 認証で、Msg-Length フィールドのない PAP を受理するように変更した。

(21)OSPF で、セカンダリアドレスを使用できるようにした。

(22)起動時のコンフィグ設定において sshd host key generate コマンドを読み込む際、SSH の暗号化された RSA 秘密鍵と DSA 秘密鍵の復号に失敗した場合には RSA 秘密鍵と DSA 秘密鍵を再生成するようにした。
この変更によって秘密鍵が再生成される場合には、起動時間が 30 秒程度長くなる。

(23)SFTP 接続で、techinfo を取得できるようにした。

techinfo は system ディレクトリ内に配置されており、TFTP 同様にファイル名を"techinfo"とすることで show techinfo コマンドの出力結果と同じものを取得することができる。

(24)SFTP 接続で system ディレクトリ内を表示する場合、exec ファイルのファイル名にリビジョン番号を付加するようにした。

exec ファイルの操作は従来通り"exec"として扱うことができる。

(25)外部メモリ内のファームウェアで起動しているときに SFTP 接続でリビジョンアップする場合は、起動中の外部メモリ内のファームウェアを更新するようにした。

(26)外部メモリ関連のコマンドで、ファイル名／ディレクトリ名、及びフルパスに指定可能な文字数制限を変更した。

〇対象コマンド

- external-memory config filename
- external-memory exec filename
- external-memory batch filename
- external-memory syslog filename
- external-memory statistics filename prefix
- copy config
- copy exec
- copy
- save
- make directory
- rename
- show file list
- 外部メモリへのリダイレクト

ファイル名／ディレクトリ名に指定可能な最大文字数を半角 99 文字、フルパスに指定可能な最大文字数を半角 246 文字に変更した。("usb1:"などのプレフィックスは含まない)

但し、一部のコマンドに関しては以下の制限がある。

- external-memory syslog filename コマンドについては、指定されたファイル名からバックアップファイル名を決定して作成する必要があるため、以下に制限される。
  - 暗号化しない場合は、拡張子を除いて半角 95 文字までとする。
  - 暗号化する場合は、拡張子を除いて半角 90 文字までとする。
- external-memory batch filename コマンドについては、実行結果ファイル名を決定して作成する必要があるため、以下に制限される。
  - 実行結果ファイル名を指定しない場合は、バッチファイル名に指定可能な最大文字数は拡張子を除いて半角 91 文字までとする。
  - 実行結果ファイル名を指定した場合、バッチファイル名で指定したパスと合わせて半角 246 文字までとする。
- external-memory statistics filename prefix コマンドで指定可能な統計情報のファイル名のプレフィックスの文字数を"usb1:"などのプレフィックスを含めずに半角 15 文字とする。(従来まではプレフィックスを

含む 15 文字）

- make directory コマンドで、指定可能なフルパスは、半角 243 文字までとする。
- rename および copy コマンドで、ディレクトリ指定の場合に指定可能なフルパスは、半角 243 文字までとする。

(27)lan type コマンドの macaddress-aging オプションで、エージング時間を指定できるようにした。

〇LAN インタフェースの動作タイプの設定

[書式]

lan type INTERFACE_WITH_SWHUB SPEED [PORT] [SPEED [PORT]...]
[OPTION=VALUE...]

lan type INTERFACE_WITH_SWHUB OPTION=VALUE

lan type INTERFACE_WITHOUT_SWHUB SPEED [OPTION=VALUE...]

lan type INTERFACE_WITHOUT_SWHUB OPTION=VALUE

no lan type INTERFACE [...]

[設定値及び初期値]

INTERFACE_WITH_SWHUB

[設定値] : スイッチングハブを持つ LAN インタフェース名

[初期値] : -

INTERFACE_WITHOUT_SWHUB

[設定値] : スイッチングハブを持たない LAN インタフェース名

[初期値] : -

INTERFACE

[設定値] : LAN インタフェース名

[初期値] : -

SPEED

[設定値] :

設定値	説明
auto	速度自動判別
1000-fdx	1000BASE-T 全二重
100-fdx	100BASE-TX 全二重
100-hdx	100BASE-TX 半二重
10-fdx	10BASE-T 全二重
10-hdx	10BASE-T 半二重
省略	省略時は auto

[初期値] : auto

PORT : スイッチングハブのポート番号

[設定値] : 省略時は全ポート

[初期値] : -

OPTION=VALUE : オプション機能

[設定値] :

・mtu

インタフェースで送受信できる最大データ長

・auto-crossover

オートクロスオーバー機能

設定値	説明
on	オートクロスオーバー機能を有効にする
off	オートクロスオーバー機能を無効にする

・macaddress-aging ★

MAC アドレスエージング機能

設定値	説明
秒数	エージング時間
off	MAC アドレスエージング機能を無効にする

・port-based-ks8995m/port-based-option

LAN 分割機能、ポート分離機能

設定値	説明
divide-network	LAN 分割機能を有効にする
split-into-split_pattern	ポート分離機能を有効にする
off	LAN 分割機能、ポート分離機能を無効にする

・speed-downshift

速度ダウンシフト機能

設定値	説明
on	速度ダウンシフト機能を有効にする
off	速度ダウンシフト機能を無効にする

・energy-saving

省電力機能

設定値	説明
on	省電力機能を有効にする
off	省電力機能を無効にする

[初期値]:

・mtu=1500

・auto-crossover=on

・macaddress-aging=300

・port-based-ks8995m/port-based-option=off

・speed-downshift=on

・energy-saving=on

[説明]

指定した LAN インタフェースの速度と動作モードの種類、およびオプション機能について設定する。

スイッチングハブを持つ LAN インタフェースについては、ポート毎に速度と動作モードを指定できる。

・mtu

インタフェースで送受信できる最大データ長を指定する。データ長には MAC ヘッダと FCS は含まれない。また、タグ VLAN 時のタグ長(4 バイト)も含まれない。

指定できるデータ長の範囲は 64～1500 の範囲となる。

インタフェースの mtu を設定して、かつ、ip mtu コマンドまたは ipv6 mtu コマンドが設定されずデフォルトのままの場合、IPv4 や IPv6 での mtu としてはインタフェースの mtu が利用される。一方、ip mtu コマンドまたは ipv6 mtu コマンドが設定されている場合には、インタフェースの mtu の設定にかかわらず、ip mtu コマンドまたは ipv6 mtu コマンドの設定値が mtu として利用される。インタフェースの mtu も含めてすべて設定されていない時には、デフォルト値である 1500 が利用される。

・オートクロスオーバー機能

LAN ケーブルがストレートケーブルかクロスケーブルかを自動的に判定して接続する機能。この機能が有効になっていると、ケーブルのタイプがどのようなものであるかを気にする必要が無くなる。

・MAC アドレスエージング機能

スイッチングハブを持つ LAN インタフェースでのみ利用できる。

スイッチングハブが持つ MAC アドレステーブル内のエントリを、一定時間で消去していく機能。この機能を off にすると、一度スイッチングハブが記憶した MAC アドレスは自動的に消去されないのはもちろん、clear switching-hub macaddress コマンドを実行しても消去されない。エントリが消去されるのは、この機能を有効にした時だけになる。

本機では、設定値に秒数を指定することができる。指定できる秒数の範囲は 1～86400 の範囲となる。ただし、コマンドの設定値と実際に消去されるまでの時間に誤差が生じる場合がある。

MAC アドレステーブルには最大で 8192 個のエントリを格納できる。

・LAN 分割機能

スイッチングハブを持つ LAN インタフェースでのみ利用できる。

LAN 分割機能には基本機能と拡張機能がある。

基本機能では、スイッチングハブの各ポートが個別の LAN インタフェースとして動作する。各インタフェースにはそれぞれ個別の IP アドレスを付与でき、その間でのルーティングも可能になる。

拡張機能では、スイッチングハブの各ポートを自由に組み合わせて 1 つの LAN インタフェース(VLAN インタフェース)とすることができる。

同一の VLAN インタフェースに所属するポート間はスイッチとして動作する。

基本機能における LAN インタフェースのインタフェース名は元のインタフェース名にピリオドとポート番号をつなげることで表される。

拡張機能では、LAN インタフェースのインタフェース名として vlan1、vlan2、vlan3…(VLAN インタフェース)を使用する。基本機能とは異なり、VLAN インタフェースは特定のポートと関連付けられてはいない。

vlan port mapping コマンドを用いて、スイッチングハブの各ポートがどの VLAN インタフェースに所属

するかを設定することで、分割方法を自由に変更することができる。同時に使用できる VLAN インタフェースは vlan1～vlan8 の範囲となる。
LAN 分割機能を有効にした場合、lan1 インタフェースに対する設定は、lan1.1(基本機能の場合)もしくは vlan1(拡張機能の場合)に引き継がれる。
LAN 分割で使用する LAN インタフェースの MAC アドレスは元の LAN インタフェースの MAC アドレスに一致する。

・ポート分離機能
スイッチングハブを持つ LAN インタフェースでのみ利用できる。
スイッチングハブのポート間での通信を禁止しつつ、ルーターを経由した通信は可能にする機能。
通常は、スイッチングハブの各ポートは他のポートと制限無く通信できるが、ポート分離機能を利用すると、ポートをグループに分離し、グループ内の通信およびルーターとの通信はそのまま可能だけれども、他のグループのポートとは通信できないようになる。
LAN 分割機能とは異なり、ポート分離機能によって LAN インタフェースが増減することはない。分離されたポートはすべて同じ LAN インタフェースとして認識され、同一の IP アドレスを持つ。
同一 LAN インタフェースにおけるプライマリアドレスのネットワークとセカンダリアドレスのネットワーク間の通信はルーターを経由するので、他のグループとの通信も可能である。

・速度ダウンシフト機能
on に設定すると 1000BASE-T で使用できないケーブルを接続された時に、速度を落としてリンクを試みる。

・省電力機能
on に設定すると使用していない LAN ポートで消費電力を抑えることができる。

[ノート]
本コマンドの実行後、LAN インタフェースのリセットが自動で行われ、その後に設定が有効となる。

(28)不正アクセス検知機能で Unknown IP protocol として検知するプロトコル番号を 143 以上に変更した。

(29)ntpdate コマンドおよび、SNTP サーバー機能で、IPv6 に対応した。
SNTP サーバー機能では、グローバルユニキャストアドレスである IPv6 アドレスからのアクセスのみ対応している。

(30)Lua スクリプト機能の rt.syslog 関数で入力するログ文字列にタブ文字が使用できるようにした。

(31)show techinfo コマンドの結果に以下のコマンドを追加した。
- show ip route summary
- show ipv6 route summary
- show status heartbeat2

(32)WAN インタフェースおよび L2TP/IPsec の追加に伴い、SNMP のインタフェース番号を変更した。

タグ VLAN を使用せず、LAN1 を LAN 分割機能で分割もしていない場合

Index	インタフェース	備考
1～3	LAN1～LAN3	
4	WAN1	
5	BRI1	
6～105	PP01～PP100	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
106～228	PP Anonymous	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
229～328	Tunnel01～100	snmp yriftunneldisplayatmib2 on 設定時に MIB2 の範囲でも有効
329	NULL	
330～338	Loopback01～09	
339	Mobile1	Rev.10.01359 以降で使用可能
100,000,000～ 199,999,999	スイッチ 1～	snmp yrifswitchdisplayatmib2 on 設定時に MIB2 の範囲でも有効

タグ VLAN を使用するか、もしくは LAN1 を LAN 分割機能で分割している場合

Index	インタフェース	備考
1	LAN1(VLAN1)	
2～3	LAN2～LAN3	
4	WAN1	
5～11	VLAN2～VLAN8	
12～43	LAN1/1～ LAN1/32	
44～75	LAN2/1～ LAN2/32	
76～107	LAN3/1～ LAN3/32	
108	BRI1	
109～208	PP01～PP100	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
209～331	PP Anonymous	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
332～431	Tunnel01～100	snmp yriftunneldisplayatmib2 on 設定時に MIB2 の範囲でも有効
432	NULL	
433～441	Loopback01～09	
442	Mobile1	Rev.10.01.35 以降で使用可能
100,000,000～ 199,999,999	スイッチ 1～	snmp yrifswitchdisplayatmib2 on 設定時に MIB2 の範囲でも有効

（WAN インタフェース及び L2TP/IPsec 追加前の Index 値）

タグ VLAN を使用せず、LAN1 を LAN 分割機能で分割もしていない場合

Index	インタフェース	備考
1～3	LAN1～LAN3	
4	BRI1	
5～104	PP01～PP100	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
105～197	PP Anonymous	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
198～297	Tunnel01～100	snmp yriftunneldisplayatmib2 on 設定時に MIB2 の範囲でも有効
298	NULL	
299～307	Loopback01～09	
308	Mobile1	Rev.10.01.35 以降で使用可能
100,000,000～ 199,999,999	スイッチ 1～	snmp yrifswitchdisplayatmib2 on 設定時に MIB2 の範囲でも有効

タグ VLAN を使用するか、もしくは LAN1 を LAN 分割機能で分割している場合

Index	インタフェース	備考
1	LAN1(VLAN1)	
2～3	LAN2～LAN3	
4～10	VLAN2～VLAN8	
11～42	LAN1/1～ LAN1/32	
43～74	LAN2/1～ LAN2/32	
75～106	LAN3/1～ LAN3/32	
107	BRI1	
108～207	PP01～PP100	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
208～300	PP Anonymous	snmp yrifppdisplayatmib2 on 設定時に MIB2 の範囲でも有効
301～400	Tunnel01～100	snmp yriftunneldisplayatmib2 on 設定時に MIB2 の範囲でも有効
401	NULL	
402～410	Loopback01～09	
411	Mobile1	Rev.10.01.35 以降で使用可能
100,000,000～ 199,999,999	スイッチ 1～	snmp yrifswitchdisplayatmib2 on 設定時に MIB2 の範囲でも有効

（33）GUI から HTTP リビジョンアップ機能の項目を削除した。

3 本バージョンで修正された項目

（1）RIPv2 で不正な経路を受信すると、その経路を破棄せずに経路テーブルに取り込んだり、リブートしたりするバグを修正した。本修正により、不正な経路を受信した場合、下記に示すようなログが DEBUG レベルの SYSLOG に出力される。

Received illegal IP route X.X.X.X/X.X.X.X from X.X.X.X by RIPv2

（2）正常な SIP パケットを短い時間に大量に受信するとメモリリークしてリブートすることがあるバグを修正した。

（3）LOOPBACK インタフェース、または NULL インタフェース宛に IPv6 パケットを送信するとリブートするバグを修正した。

（4）不正なフォーマットの DNS パケットを受信すると、その後の動作が不安定になり、リブートしたりハングアップしたりすることがあるバグを修正した。

（5）不正なフォーマットの ICMPv6 パケットを受信するとリブートすることがあるバグを修正した。

（6）ルーターを端点とする TCP の通信が行われると、稀にリブートすることがあるバグを修正した。
データコネクトサービスを利用したリモートセットアップ実行時に本バグが発生することを確認している。

（7）mail server pop コマンドで認証パスワードを指定せずに設定するとリブートすることがあるバグを修正した。

（8）OSPF で広告可能な外部経路として取り込まれている静的な経路について以下の条件を満たす設定を連続して 1 秒以内に行うとリブートすることがあるバグを修正した。
- 該当する経路のマスク長を短くした経路を追加する
- 該当する経路のゲートウェイを、ダウンしているトンネルインタフェースまたは経路が存在しない IP アドレスに変更する

（9）BGP で 24 対地以上のネイバと接続した状態で bgp configure refresh コマンドを実行するとリブートするバグを修正した。
この修正に伴い、bgp neighbor コマンドを 32 個までしか設定できないようにした。

（10）ip filter dynamic timer コマンドを設定した状態で動的フィルターが最大セッション数に達すると、リブートすることがあるバグを修正した。

（11）ip pp remote address コマンドが設定された PP インタフェースが接続中のとき、GUI の[インタフェース]ページの「詳細」ボタンまたは「状態」ボタンを押すと、リブートすることがあるバグを修正した。

（12）SFTP 接続で、接続してから数分後にリブートすることがあるバグを修正した。

（13）SFTP 接続で、system ディレクトリ下へファイルを PUT した場合に不正なメモリ解放を示すログが出力されたり、リブートしたりすることがあるバグを修正した。

（14）内部データベース参照型 URL フィルター機能で、フラグメントされた HTTP リクエストを受信した場合、先頭以外のパケットを先に受信するとリブートするバグを修正した。

(15)内部データベース参照型 URL フィルター機能で、"/.."を含む URL を参照すると、正しく解析できなかったり、リブートしたりすることがあるバグを修正した。

(16)ルーターに TELNET で接続しているとき、ルーターからの文字出力と TELNET クライアントからのコネクション切断が重なると、稀に CPU 使用率が 100%に達したまま下がらなくなり、リブートすることがあるバグを修正した。

(17)dhcp client hostname コマンドや dhcp client client-identifier コマンドを設定した状態で show status dhcpc コマンドを実行すると、リブートすることがあるバグを修正した。
　また、dhcp client hostname コマンドでホスト名に 128 文字以上を指定したときに表示されるエラーが不適切だったバグを修正した。

(18)ディレクティッドブロードキャスト宛の MagicPacket を受信したとき、ディレクティッドブロードキャストと同じサブネットの IP アドレスが設定された LAN インタフェースにおいて以下の設定がされているとリブートするバグを修正した。
- ip INTERFACE intrusion detection out on
- ip INTERFACE wol relay broadcast/unicast

(19)モバイルインターネット機能で、SoftBank C01SW または SoftBank C02SW をバックアップとして利用した場合、バックアップから復旧した後に、ルーターがリブートすることがあるバグを修正した。
　また、切断する際に不要な USB バスリセットが発生することがあるバグを修正した。

(20)GUI の[保守]-[コマンドの入力]ページから、半角スペースや「&」「"」「>」「<」を含む文字列をコマンドとして実行すると、リブートしたりルーターの動作が不安定になったりするバグを修正した。
　これらの文字を HTML のマークアップ表現に変換した後の文字列長が 2048 バイト以上になる場合に問題が発生する。

(21)データ通信端末を挿入した状態での起動や挿抜で、ごく稀にシステムがハングアップすることがあるバグを修正した。

(22)以下の条件をすべて満たす場合に、キーボードからシリアルコンソールに文字入力をしているとシリアルコンソールがハングアップすることがあるバグを修正した。
- ip routing process fast
- QoS の設定がある
- ファストパス対象外のパケットの送信負荷が高くパケットロスしている

(23)IPsec のファストパス通信中に稀にルーターがハングアップすることがあるバグを修正した。

(24)queue class filter コマンドを上書きした場合および、no queue class filter コマンドで設定を削除した場合に、メモリリークするバグを修正した。

(25)SFTP 接続で RTFS 領域または外部メモリへファイルを書き込む場合、書き込みに失敗するとメモリリークすることがあるバグを修正した。

(26)OSPF で、下記に示すようにエリア全体の認証が有効になっているがそのエリアに属するインタフェースの設定に認証鍵の指定がない場合、本来送信しない Hello パケットを送信しようとしてメモリリークが発生するバグを修正した。

(MD5 認証の設定誤りの例)

ip lan1 ospf area backbone	× md5key がない
ip lan2 ospf area backbone md5key=1,abc	○ 正しい
ospf area backbone auth=md5	

(プレーンテキスト認証の設定誤りの例)

ip lan1 ospf area backbone	× authkey がない
ip lan2 ospf area backbone authkey=abc	○ 正しい
ospf area backbone auth=text	

(27)SSH サーバー機能で、接続／切断を繰り返しているとメモリリークするバグを修正した。

(28)TELNET や SSH で接続しコマンドを実行したとき、コマンドが完了する前に TELNET や SSH のセッションを切断するとメモリリークするバグを修正した。

(29)ipv6 INTERFACE dhcp service コマンドで、入力したコマンドがエラーとなったときメモリリークするバグを修正した。

(30)DHCPv6 クライアント機能で、サーバーから情報を取得するときにメモリリークするバグを修正した。

(31)RA プロキシの設定をしているとき、RA を受信するとメモリリークするバグを修正した。
メモリリークが発生すると、show ipv6 route summary コマンドまたは show ipv6 route detail コマンドを実行したとき、同じ宛先に対する implicit 経路や temporary 経路が複数個表示されていた。

(32)FAT16 のアロケーションユニットサイズ 64KB でフォーマットされた外部メモリにアクセスするとメモリが不正に解放されるバグを修正した。

(33)SFTP 接続で RTFS 領域のルートディレクトリを対象として特定のファイル名のファイルの読み出しや書き込みなどの操作を行った場合、メモリの二重解放が起きるバグを修正した。
以下の条件で本バグは発生する。
- USB メモリがアタッチされている場合にファイル名が"u", "us", "usb" であるファイルを操作した場合
- SD カードがアタッチされている場合にファイル名が"s", "sd" であるファイルを操作した場合

(34)フラグメントされた特定サイズの IPv6 パケットを受信したとき、パケットが破棄されてしまうバグを修正した。
最後のフラグメントパケットを破棄していたため、パケット全体も破棄されてしまっていた。

(35)フラグメントされた ICMPv6 パケットが転送されないことがあるバグを修正した。

(36)IP ヘッダーに不正なタイムスタンプオプションが含まれているパケットを受信したとき、IP オプションフィールドを不当に書き換えてしまうことがあるバグを修正した。

(37)IPv6 マルチキャストパケットが以下の条件でファストパス処理されないバグを修正した。
- LAN 分割機能で分割された LAN インタフェースにおいて IPv6 マルチキャストパケットを受信した場合
- VLAN インタフェースにおいて IEEE802.1Q タグが付加された IPv6 マルチキャストパケットを受信した場合

(38)OSPF でタイプ 5(AS External)LSA の Link State ID を決定するときに、複数の Link State ID とバッティングした場合に正しく経路が広告されないことがあるバグを修正した。

(39)RIPng の優先度が他より低い場合に、RIPng で通知された経路と同一の宛先に対する経路が ipv6 route コマンドで静的に設定されると、当該経路情報が RIPng によって通知されなくなっても hide 状態でルーティングテーブルに残り、さらに静的経路が削除されると本来は無効(hide 状態)であるべき RIPng によって通知された経路が有効になってしまうバグを修正した。

(40)経路指定がある RIP リクエストを受信した場合、コンソールに"free[xxx:yy]: illegal address～" というエラーログが出力されるバグを修正した。
本製品ではこのようなリクエストを送信することはないため、本製品間で RIP による経路交換を行う場合は発生しない。

(41)VLAN インタフェースに対して PPPoE の設定をしているとき、PPPoE 経由の通信が発生すると、その後の動作が不安定になることがあるバグを修正した。

(42)IPCP で IP アドレスを取得し、コネクションを切断した後、ソースアドレスが 0.0.0.0 のパケットを受信すると破棄するバグを修正した。

(43)anonymous 接続で名前によるルーティングを設定している場合、PPP の LCP セッション確立後に LCP Configure Request が再送されると、PPP セッションの切断後にその相手先へ接続できなくなる可能性を排除した。

(44)侵入検知機能で、IP ヘッダー、IP ヘッダーオプション、フラグメント、ICMP、UDP、TCP に関する侵入検知がインタフェースから出て行くパケットについて動作していないバグを修正した。

(45)モバイルインターネット機能で、電波受信レベルが取得できないことがあるバグを修正した。

(46)モバイルインターネット機能で、網側からの接続切断直後の再接続が、発信規制により 1 分程度できないことがあるバグを修正した。

(47)モバイルインターネット機能で、接続中に pp disable コマンドまたは no pp bind コマンドを実行すると切断できなくなるバグを修正した。

(48)モバイルインターネット機能で、網からの切断処理が正しく行われないことがあるバグを修正した。

(49)モバイルインターネット機能で、一部のデータ通信端末で電波状態が悪化したときに電波受信レベルの取得を繰り返すと、電波状態が回復した後も接続できなくなることがあるバグを修正した。

(50)ISDN の呼制御処理で異常時の処理が正しく行われないことがあるバグを修正した。

(51)UPnP で、NOTIFY の送信間隔が CACHE-CONTROL(max-age=1800s)と同じ 30 分であったのを、規格に合わせてその半分の 15 分となるように修正した。

(52)IPv6 の IPsec 接続で、プロトコルタイプに AH を指定したとき、トランスポートモードで通信できないバグを修正した。

(53)IKEv2 で、一部の鍵交換のパケットがロスすると、トンネルがつながらなくなることがあるバグを修正した。

(54)IKEv2 で、CHILD SA の削除を通知する Delete ペイロードに含める SPI 値がリクエストとレスポンスで互いに逆となっているバグを修正した。

(55)データコネクトサービスを利用した拠点間接続で、自動切断タイマーが無効になることがあるバグを修正した。

(56)VRRP で、仮想ルーターの IP アドレスとして VRRP グループに所属する VRRP ルーターのうちの 1 台の IP アドレスを利用する場合、マスタールーターのシャットダウンによりバックアップルーター経由の経路に切り替わった状態だとバックアップルーター配下の端末の通信が行えなくなることがあるバグを修正した。

(57)一つの宛先ネットワークに対して複数のゲートウェイが存在するとき、最初のゲートウェイが ip INTERFACE vrrp shutdown trigger コマンドの route 形式の nexthop で設定した IP アドレスでなかった場合に、2 番目以降のゲートウェイに nexthop で設定した IP アドレスが存在していても VRRP をシャットダウンしてしまうバグを修正した。

(58)VRRP で ip INTERFACE vrrp コマンドを再設定すると、優先度 255 のマスタールーターが、コンフィグで設定された優先度のバックアップルーターになってしまうバグを修正した。
　また、VRRP を設定しているインタフェースで IP アドレスを再設定しても、VRRP に設定した IP アドレスが反映されないバグを修正した。

(59)VRRP でマスタールーターが切り替わった直後に ARP request を受信すると、マスタールーターのみが reply を返すべき ARP request(仮想 IP アドレスに対する ARP request など)に対しても、旧マスタールーターが reply を返すことがあるバグを修正した。

(60)RA を送信するとき、パケットの送信元 IPv6 アドレスとして不正なアドレスが選択されることがあるバグを修正した。

(61)DHCPv6-PD 機能で、プレフィックス情報取得後に Reconfigure メッセージを受信したとき、要求された動作に移行しないことがあるバグを修正した。

(62)DHCPv6 クライアント機能で、優先度が小さい DHCPv6 サーバーに Reqeust を送信していたバグを修正した。

(63)ngn type コマンドを設定していないインタフェースで DHCPv6-PD クライアントの設定をしているとき、DHCPv6-PD メッセージで不要なオプションを設定し送信してしまうバグを修正した。

(64) DHCPv6-PD クライアントを設定している場合、show status ipv6 dhcp コマンドで Vender Specific Information を取得していないときでも表示するバグを修正した。

(65) RADIUS 機能で、ルーターから RADIUS サーバーに送出される Access-Request および Accounting-Request に含まれる NAS-Port-Type 属性の値が、着信ポートの種類によらず常に ISDN Sync (2) となっているバグを修正した。
着信ポートの種類と、対応する NAS-Port-Type 属性の値は以下の通りである。
- ISDN 同期通信の場合 : ISDN Sync (2)
- PIAFS の場合 : PIAFS (6)
- それ以外 (PPTP など): Virtual (5)

(66) PPP ならびに IPsec XAUTH の認証やアカウンティングで RADIUS を使用する場合、Access-Request、Accounting-Request の再送処理中に再接続を行うと、不正なパケットが送信されたりパケットの送信間隔が設定値よりも短くなったりするバグを修正した。

(67) 以下の機能で、RADIUS を使用して PAP でパスワード認証を行う場合、パスワードの長さが 17 文字以上あると認証できないバグを修正した。
- PPP
- IPsec XAUTH

(68) RADIUS 機能で ISDN 接続による認証を行う場合、PP 切断時にルーターから RADIUS サーバーに送出される Accounting-Request に含まれる NAS-Port 属性と Calling-Station-Id 属性の値が不正になるバグを修正した。

(69) ルーターに設定しているパスワードの長さが 32 文字で、かつ暗号化してある場合、パスワード認証において、最初の 32 文字が正しいパスワードと一致する 33 文字以上の文字列を入力すると、認証に成功してしまうバグを修正した。
以下の場合にパスワードは暗号化される。
- login password コマンドで encrypted を指定した場合
- administrator password コマンドで encrypted を指定した場合
- login user コマンドでユーザーを登録した場合

(70) ルーターのコンソールから IPv6 アドレス宛に対する telnet コマンドや rdate コマンドなどの TCP アプリケーションを実行したとき、通信できないことがあるバグを修正した。

(71) 起動直後から以下の機能が使用できないことがあるバグを修正した。
- TFTP
- SNMP(snmp host コマンドが設定されているとき)

(72) TFTP で'config'宛に設定ファイルを PUT すると、設定ファイルの内容によってはそれ以降、TFTP が使えなくなることがあるバグを修正した。

(73) SFTP 接続で外部メモリへのファイルの書き込みを行う場合、存在しないディレクトリ配下へファイルを書き込もうとすると SFTP 接続が切断することがあるバグを修正した。

(74)SFTP 接続で、INFO レベルの SYSLOG に表示される以下のログにおいて、ユーザ名が正しく表示されないことがあるバグを修正した。

- [SFTPD] Login succeed: IP アドレス ユーザ名 as administrator
- [SFTPD] Login succeed: IP アドレス ユーザ名 as login user
- [SFTPD] Logout: ユーザ名
- [SFTPD] Get ファイル名 succeed by ユーザ名
- [SFTPD] Put ファイル名 succeed by ユーザ名
- [SFTPD] Get ファイル名 failed by ユーザ名
- [SFTPD] Put ファイル名 failed by ユーザ名

(75)vlan INTERFACE 802.1q コマンドが 1 つでも設定されていると、LAN インタフェースがリンクダウンした際に、対応するすべてのタグ VLAN インタフェースに対する linkdown トラップが送出されるバグを修正した。

(76)トンネルインタフェースに対する SNMP の MIB 変数 ifMtu に、ip tunnel mtu コマンドの設定値が反映されないバグを修正した。

(77)SNMP で、yrIfTunnelDisplayAtMib2 にアクセスできないバグを修正した。

(78)SNMP Get リクエストで tcpConnTable 以下の MIB 変数にアクセスできないバグを修正した。

(79)モバイルインターネット機能の PP インタフェースで、ifOperStatus 以下の MIB 変数が正しく表示されないバグを修正した。

また、送受信数のカウンターがカウントアップされないバグを修正した。

(80)外部メモリに保存する SYSLOG ファイル名の拡張子に ″.bak″ を指定したときのエラーメッセージを適切なメッセージに変更した。

(81)save コマンドにて設定ファイルを暗号化して外部メモリに保存したとき、不正なデータが書き込まれることがあるバグを修正した。

(82)メール送信機能で、メール送信処理中に突然メールサーバーからコネクションを切断されると、以下の不具合が発生することがあるバグを修正した。

- CPU 使用率が 100%に達し、その状態が継続する
- その後のメール送信が行われなくなる
- 管理者権限が必要なコマンドが正常に実行できなくなる

(83)メール送信機能で、メール送信処理中にメールサーバーから 1600 バイト以上のデータを受信すると、CPU 使用率が 100%に達したまま下がらなくなるバグを修正した。

(84)トリガによるメール通知機能で、Subject を半角スペースと全角文字を混ぜた文字列で設定したとき、正しく MIME エンコードできないバグを修正した。

(85)カスタム GUI で、コマンド実行結果の文字列に不要な改行が挿入されないようにした。従来は 1 行あたりの文字数が console columns コマンドの設定値に到達した時点で改行が挿入されていたが、スクリプトで処理しやすくするため、本来の終端位置以外では改行されないようにした。

(86)カスタム GUI で、マルチバイト文字を含むコマンドを実行すると、実行結果が文字化けするバグを修正した。
/custom/execute に対してマルチバイト文字を POST した場合は、当該文字を UTF-8 として解釈するようにした。

(87)queue INTERFACE type コマンドの設定が priority または shaping になっている LAN インタフェースで、wol send コマンドを実行しても Magic Packet が送出されないバグを修正した。

(88)LAN 分割機能を設定したとき、以下のコマンドの入力形式の"lan1"が不正に分割されたインタフェースに変換されてしまうバグを修正した。
- lan port-mirroring lan1
- snmp trap link-updown separate-l2switch-port lan1

(89)bgp export filter コマンドの preference オプションが動作しないバグを修正した。

(90)bgp import filter コマンドおよび bgp export filter コマンドで、ip_address/mask パラメータを指定していなくても、オプションパラメータを指定するとエラーにならないバグを修正した。

(91)disconnect user コマンドで、以下のバグを修正した。
- "disconnect user (ユーザー名)/http"を実行した場合に、HTTP で接続しているすべてのユーザーの接続が切断される
- "disconnect user (ユーザー名)/http(接続番号)"を実行した場合に、ユーザー名が一致しなくても該当する接続番号の接続が切断される
- GUI の[保守]-[コマンドの入力]ページからコマンドを実行した場合に、自身の接続を切断できてしまう

(92)ユーザー名と接続種別を指定して disconnect user コマンドを実行した場合、当該ユーザーが login user コマンドで登録されていても、ログインしていないと「指定されたユーザー名は登録されていません」というエラーメッセージが表示されることがあるバグを修正した。

(93)no ethernet INTERFACE filter コマンドで、フィルター番号が 3 つ以上指定されていると削除できないバグを修正した。

(94)user attribute コマンドを用いて、すべてのユーザーに対する administrator 属性を off に設定しても、個別のユーザーに対する当該コマンドの設定が存在しない場合は、SFTP において管理権限でログインできるバグを修正した。

Rev.10.01.26 以降で発生する。

(95)login user コマンドでユーザー名が 32 文字であるユーザーを作成している状態で、GUI の認証画面において、最初の 32 文字が設定値と一致する、33 文字以上の文字列をユーザー名として入力した場合に、パスワードが正しければログインできてしまうバグを修正した。

(96)auth user group コマンドで、"ユーザ ID-ユーザ ID" という形式でユーザ ID を設定できないことがあるバグを修正した。

(97)ipv6 filter コマンドの tcpflag オプションが動作しないバグを修正した。

(98)ipv6 INTERFACE prefix コマンドで、auto や dhcp が設定できてしまうバグを修正した。

(99)以下のコマンドで、local-addr オプションに 0.0.0.0 や :: が設定できてしまうバグを修正した。

- cooperation bandwidth-measuring remote
- cooperation load-watch remote

また、オプションを重複して指定してもエラーにならないバグも修正した。

(100)ip INTERFACE vrrp コマンドで、advertise-interval/down-interval の各パラメータを重複指定してもエラーにならないバグを修正した。また、priority/preempt/auth の各パラメータを重複指定したときのエラーメッセージが不適切であったため、適切なメッセージに修正した。

(101)queue class filter コマンドで mapping パラメータと cos パラメータを同時に設定できないバグを修正した。

(102)dhcp scope option コマンドで、設定値が 4 オクテット整数型のオプションを設定するとき、範囲外の値が設定できてしまうバグを修正した。

(103)以下のコマンドで半角スペースや「'」「#」を含むパスやファイル名などを指定した場合、設定が正しく保存されなかったり、正しく表示されないバグを修正した。

- external-memory batch filename
- external-memory config filename
- external-memory exec filename
- external-memory statistics filename prefix
- external-memory syslog filename
- operation button function download execute lua

(104)リダイレクト文字「>」を含んだコマンド文字列を show config コマンドで表示させたとき、表示されたコマンド文字列をコピー＆ペーストすると、コマンド実行エラーとなるバグを修正した。
リダイレクト文字「>」を含んだコマンド文字列は、「"」で括って表示するように修正した。

(105)grep コマンドで「$」を指定したとき、パターンに一致する行があるにも関わらず何も表示されないバグを修正した。

(106)console prompt コマンドで長い文字列を指定している際、その後に表示されるはずのサフィックスの表示が途切れてしまうバグを修正した。

(107)プロンプトの文字数（末尾の空白 1 文字を含む）と入力したコマンドの文字数の合計が 4095 文字を超えている状態で Ctrl+E を押下すると、カーソルの位置が終端に移動しないバグを修正した。

(108)show status vlan コマンドの実行結果が正しく表示されないことがあるバグを修正した。

(109)show status dhcpc コマンドの表示結果の誤記を修正した。

(110) show techinfo コマンドの実行結果で、show status ngn 以降の表示がされないバグを修正した。

Rev.10.01.26 以降で発生する。

(111) 以下のコマンドのコマンドヘルプの誤記を修正した。

- account threshold
- auth user group
- bgp neighbor
- bgp export filter
- bgp import filter
- external-memory config filename
- external-memory exec filename
- ip INTERFACE ospf area
- ip stealth
- ipv6 INTERFACE address
- ipv6 prefix
- ipv6 stealth
- ospf area network
- tunnel ngn bandwidth

(112) GUI の[ログインユーザーの設定]ページで、半角スペースや「'」「"」「#」「¥」を含む文字列を暗号化してログインパスワードに設定した場合、ログインパスワードが正しく設定されないバグを修正した。

Rev.10.01.26 以降で発生する。

(113) GUI のウィザードから暗号化したパスワードを設定するとき、パスワードに半角スペースや「'」「"」「#」「¥」を含む文字列を登録すると、入力した文字列とは別 の文字列がパスワードに設定されてしまうバグを修正した。

(114) GUI の[保守]-[コマンドの入力]ページ、またはカスタム GUI から show status user コマンドを実行した場合、自分自身のユーザー情報の先頭にアスタリスク (*) が付かないバグを修正した。

(115) GUI の以下のページで、「&」などの HTML として文字参照される文字列がコマンドとして正しく設定されなかったり、外部メモリ内のファイル名に使用されていると、正しく表示できなかったり、意図した設定にならないバグを修正した。

- [保守]ページ
- [保守]-[ファームウェアファイルのコピー]ページ
- [保守]-[ファームウェアファイルのコピー]-[ファイルの一覧]ページ
- [保守]-[外部デバイスの設定]ページ
- [保守]-[外部デバイスの設定]-[ファイルの一覧]ページ

(116) GUI の以下のページで、「'」を含むファイル名のファイルを選択できないバグを修正した。

- [保守]-[ファームウェアファイルのコピー]-[ファイルの一覧]ページ
- [保守]-[外部デバイスの設定]-[ファイルの一覧]ページ

（117）GUI のウィザードから「CATV インターネット、または PPPoE を用いない端末型接続」の WAN 側 IP アドレスを指定して登録すると、正しく設定できたにも関わらず、設定完了画面で ″設定が正常に完了しませんでした。″ と表示されてしまうバグを修正した。

（118）GUI の[保守]-[コマンドの入力]ページから、HTML タグを含む文字列をコマンドとして実行した場合、実行結果の表示が乱れることがあるバグを修正した。

（119）GUI の[保守]-[コマンドの入力]ページ、もしくはカスタム GUI から、4096 文字以上の文字列をコマンドとして実行すると、それ以降 GUI およびカスタム GUI のいずれにもアクセスできなくなるバグを修正した。

（120）GUI のウィザードの一部で、不正な入力でページ遷移した際に表示されるエラー画面で HTML 文法エラーや javascript エラーが発生するバグを修正した。