

Revision : 15.00.22

Release : Apr. 2021, ヤマハ株式会社

NVR700W Rev.15.00.22 リリースノート

---

○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以降のファームウェアへ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](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.15.00.19 からの変更点

---

## ■脆弱性対応

[1] OpenSSLの以下の脆弱性対応を行った。

- CVE-2020-1971(JPCERT/CC JNVU#91053554)

[2] Web GUIの以下の脆弱性対応を行った。

- CVE-2021-20843 (JPCERT/CC JNVU#91161784)

- CVE-2021-20844 (JPCERT/CC JNVU#91161784)

## ■機能追加

[1] L2MSで以下の機種に対応した。

- SWX3220-16MT

- SWX3220-16TMs

- SWX2322P-16MT

- SWX2320-16MT

- SWX2110P-8G

- SWX2110-16G

- SWX2110-8G

- SWX2110-5G

- WLX413

- UTX200

- UTX100

[2] YNOエージェント機能で、LAS (ログ分析サービス) 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ください。

[3] 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。

- SoftBank A002ZT

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

外部仕様書をよくご確認ください。

[4] IPv6のフラグメントパケットを再構成するために保持しておく時間を設定できるようにした。

○IPv6のフラグメントパケットを再構成するために保持しておく時間を設定

[書式]

ipv6 reassembly hold-time TIME

no ipv6 reassembly hold-time [TIME]

[設定値及び初期値]

TIME

[設定値]

秒数 (1 ... 60)

[初期値]

60秒

[説明]

IPv6のフラグメントパケットを再構成するために保持しておく時間。

設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。

コマンド実行時にすでに保持していたパケットについては変更しない。

[5] トンネルQoSで、トンネルインターフェースのデフォルトクラスを設定できるようにした。

○デフォルトクラスの設定

[書式]

```
queue tunnel default class CLASS
```

```
no queue tunnel default class [CLASS]
```

[設定値及び初期値]

- CLASS

[設定値] : クラス (1..16; RTX5000、RTX3500 の場合は 1..100)

[初期値] : 2

[説明]

インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[6] IPv6で、近隣キャッシュの最大エントリー数を変更できるようにした。また、近隣キャッシュの最大エントリー数の初期値を256から1024へ変更した。

○近隣キャッシュの最大エントリー数の設定

[書式]

```
ipv6 INTERFACE neighbor cache max entry NUM
```

```
no ipv6 INTERFACE neighbor cache max entry [NUM]
```

[設定値及び初期値]

INTERFACE

[設定値]

LANインターフェース名、ONUインターフェース名

[初期値]

なし

NUM

[設定値]

最大エントリー数 (256…20480)

[初期値]

1024

[説明]

インターフェースごとに近隣キャッシュの最大エントリー数を設定する。

近隣キャッシュのエントリー数が、設定した最大エントリー数に達した場合は、古い近隣キャッシュを削除する。

本コマンド実行時、現在の近隣キャッシュのエントリー数が最大エントリー数を超える場合は、古い近隣キャッシュを削除する。

[7] IPv6 RAプロキシ機能で、RDNSSオプションに対応した。

○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、DHCP6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。

rdnss                rdnss、off、dhcpv6    ルーター広告にRDNSSオプションを含めるか否かと、含める場合の値の設定。  
rdnssの場合はRAのRDNSSオプションで割り当てられたサーバー群を通知する。 ★

-----  
[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
- rdnss = rdnss ★

[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。

[8] DPIの識別結果のキャッシュを表示するコマンドと削除するコマンドを追加した。

○識別結果のキャッシュの表示

[書式]

```
show dpi cache
```

[説明]

アプリケーションの識別結果のキャッシュをIPv4/IPv6アドレスに分けて、0-9、a-zの順に表示する。TTLは分' 秒" のフォーマットで表示する。

○識別結果のキャッシュのクリア

[書式]

```
clear dpi cache
```

[説明]

アプリケーションの識別結果のキャッシュをクリアする。

[9] VoIP機能で、発番号情報なしのSIP着信に対して、着信動作を設定できるようにした。

○発番号情報なしSIP着信機能の設定

[書式]

```
analog sip arrive without-calling-number PORT TYPE [OPTION [OPTION [OPTION]]]  
no analog sip arrive without-calling-number PORT
```



## [設定値及び初期値]

PORT

[設定値]:

1 : TEL1 ポート

2 : TEL2 ポート

[初期値]:

TYPE

[設定値]:

permit : 発番号情報なしSIP着信を許可する

reject : 発番号情報なしSIP着信を拒否する

[初期値]: permit

OPTION

[設定値]:

all : すべての着信を対象にする

public-telephone : 本設定を公衆電話からの着信に限定する

rejected-by-user : 本設定をユーザによる通知拒否の着信に限定する

service-unavailable : 本設定を表示圏外からの着信に限定する

[初期値]: all

## [説明]

SIP着信に対して、指定したTELポートの発番号情報なしの着信を、指定した非通知理由により許可するか否かを選択する。

## [ノート]

ナンバー・ディスプレイサービスの契約が必要。

[10] BGP機能でMED属性が付与されていない経路のデフォルトのMED値を設定するコマンドを追加した。

○BGPの最適経路選択におけるMED属性が付加されていない経路のデフォルトのMED値

の設定

[書式]

```
bgp default med MED
```

```
no bgp default med [MED]
```

[設定値及び初期値]

MED

[設定値] : 0 .. 2147483647

[初期値] : 2147483647

[説明]

BGPの最適経路選択で、MED属性が付加されていない経路に対するデフォルトのMED値を設定する。

本コマンドが設定されていない場合、MED属性が付加されていない経路は最大のMED値（2147483647）を持つことになり、優先度は最低となる。

本コマンドの設定は、MED属性が付加されている経路には影響しない。

[11] Web GUIのダッシュボードの[Live]に、UTXセキュリティーガジェットを追加した。

UTXセキュリティーガジェットでは、UTX100/UTX200から取得したセキュリティーレポートの概要を確認できる。

[http://www.rtpro.yamaha.co.jp/RT/docs/dashboard\\_ver2/index.html](http://www.rtpro.yamaha.co.jp/RT/docs/dashboard_ver2/index.html)

外部仕様書をよくご確認のうえ、ご利用ください。

## ■仕様変更

[1] Web GUIで、Internet Explorer11のサポートを終了した。

詳細および最新の推奨ブラウザについては、以下のURLをご覧ください。

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

[2] IPIPトンネルで、L2TP/IPsecおよびL2TPv3に対応した。

ただし、IPv6 IPoE + IPv4 over IPv6 接続のサービスでは、契約形態により制限があるため、以下の技術資料をご確認のうえ、ご利用ください。

[http://www.rtpro.yamaha.co.jp/RT/docs/#ipoe\\_46](http://www.rtpro.yamaha.co.jp/RT/docs/#ipoe_46)

[3] show ipv6 neighbor cacheコマンドで、インターフェースを指定して表示できるようにした。また、エントリー数のみを表示できるようにした。

○近隣キャッシュの表示

[書式]

show ipv6 neighbor cache [INTERFACE] ★

show ipv6 neighbor cache [INTERFACE] summary ★

[設定値及び初期値]

INTERFACE ★

[設定値]

LANインターフェース名、ONUインターフェース名

[初期値]

なし

[説明]

近隣キャッシュの状態を表示する。インターフェース名を指定した場合、そのインターフェース経由で得られた近隣キャッシュの状態のみ表示する。

summaryを指定した場合、近隣キャッシュのエントリー数のみ表示する。

[4] clear ipv6 neighbor cacheコマンドで、インターフェースを指定して消去できるようにした。

## ○近隣キャッシュの消去

### [書式]

```
clear ipv6 neighbor cache [INTERFACE] ★
```

### [設定値及び初期値]

INTERFACE ★

#### [設定値]

LANインターフェース名、ONUインターフェース名

#### [初期値]

なし

### [説明]

近隣キャッシュを消去する。インタフェース名を指定した場合、そのインタフェース経由で得られた近隣キャッシュのみ消去する。

[5] OCNバーチャルコネクトサービスで、通信を安定化させるために以下を変更した。

- ルーター起動時、MAPルールの処理を開始してから取得を行うまでの待機時間を3秒から8秒へ変更した
- 固定IP契約で、起動時にルーターが保持しているMAPルールのプレフィックスと受信したプレフィックスが一致しない場合に、MAP-Eルールの取得するタイミングを1～10分後から15～20分後へ変更した
- 動作中にプレフィックスが変更された場合に、MAP-Eルールの取得するタイミングを3秒後から15分後へ変更した

[6] OCNバーチャルコネクトサービスの固定IP契約で、起動時にルーターが保持しているMAPルールのプレフィックスと受信したプレフィックスが一致しない場合でも、トンネルがアップするよう変更した。

[7] IPv6でNGN網を介したリナンバリングが発生したとき、または、マルチプレフィックスになったとき、直後に配下の端末が持つ優先度の低いプレフィックスを無効にす

るよう変更した。

[8] IPv6でNGN網を介したリナンバリングが発生したとき、LANインターフェースがリンクダウンしないバグを修正した。

[9] DHCPサーバー機能で、特定の機器でDHCPNAKが認識できなかったのを、認識できるようにした。

[10] 以下のコマンドで、始点IPアドレスおよび終点IPアドレスにmap-eを指定できるようにした。

- ip filterコマンド
- ip filter dynamicコマンド
- ipv6 filterコマンド
- ipv6 filter dynamicコマンド

○IPパケットのフィルタの設定

[書式]

```
ip filter FILTER_NUM PASS_REJECT SRC_ADDR[/MASK] [DEST_ADDR[/MASK] [PROTOCOL  
[SRC_PORT_LIST [DEST_PORT_LIST]]]
```

```
no ip filter FILTER_NUM [PASS_REJECT]
```

[設定値及び初期値]

FILTER\_NUM

[設定値] : 静的フィルタ番号 (1..21474836)

[初期値] : -

PASS\_REJECT

[設定値] :

-----

設定値	説明
-----	----

---

pass 一致すれば通す ( ログに記録しない )  
pass-log 一致すれば通す ( ログに記録する )  
pass-nolog 一致すれば通す ( ログに記録しない )  
reject 一致すれば破棄する ( ログに記録する )  
reject-log 一致すれば破棄する ( ログに記録する )  
reject-nolog 一致すれば破棄する ( ログに記録しない )  
restrict 回線が接続されていれば通し、切断されていれば破棄する ( 破棄する場合のみログに記録する )  
restrict-log 回線が接続されていれば通し、切断されていれば破棄する ( ログに記録する )  
restrict-nolog 回線が接続されていれば通し、切断されていれば破棄する ( ログに記録しない )

---

[初期値] :-

SRC\_ADDR : IPパケットの始点IPアドレス

[設定値] :

- IPアドレス
  - A.B.C.D (A~D: 0~255もしくは\*)
  - 上記表記でA~Dを\*とすると、該当する8ビット分についてはすべての値に対応する
  - 間に - を挟んだ2つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
  - , を区切りとして複数設定することができる。
- FQDN
  - 任意の文字列 (半角255文字以内。 / : は使用できない。 , は区切り文字として使われるため、使用できない)
  - \* から始まるFQDNは \* より後ろの文字列を後方一致条件として判断する。例えば \*.example.co.jpは

www.example.co.jp、mail.example.co.jpなどと一致する

・,を区切りとして複数設定することができる。

・map-e ★

・MAP-Eのマッピングルールにより生成されたグローバルIPv4アドレスを表すキーワード ★

・\*(すべてのIPアドレスに対応)

[初期値]:-

DEST\_ADDR: IPパケットの終点IPアドレス

[設定値]:

- ・src\_addrと同じ形式
- ・省略した場合は一個の\*と同じ

[初期値]:-

MASK: IPアドレスのビットマスク (SRC\_ADDRおよびDEST\_ADDRがネットワークアドレスの場合のみ指定可)

[設定値]:

- ・A.B.C.D (A~D: 0~255)
- ・0xに続く十六進数
- ・マスクビット数
- ・省略時は0xffffffffと同じ

[初期値]:-

PROTOCOL: フィルタリングするパケットの種類

[設定値]:

- ・プロトコルを表す十進数 (0..255)
- ・プロトコルを表すニーモニック

icmp 1 ICMP/パケット

tcp 6 TCP/パケット

udp 17 UDP/パケット

ipv6 41 IPv6/パケット

gre 47 GRE/パケット

esp 50 ESPパケット

ah 51 AHパケット

icmp6 58 ICMP6パケット

- 上項目のカンマで区切った並び (5個以内)
- 特殊指定

---

設定値	説明
-----	----

---

icmp-error	TYPEが3、4、5、11、12、31、32のいずれかであるICMPパケット
------------	--

icmp-info	TYPEが0、8~10、13~18、30、33~36のいずれかであるICMPパケット
-----------	--

tcpsyn	SYNフラグの立っているtcpパケット
--------	---------------------

tcpfin	FINフラグの立っているtcpパケット
--------	---------------------

tcprst	RSTフラグの立っているtcpパケット
--------	---------------------

established	ACKフラグの立っているtcpパケット内から外への接続は許可するが、外から内への接続は拒否する機能
-------------	---

tcpflag=VALUE/MASK	TCPフラグの値とMASKの値の論理積 (AND)
--------------------	---------------------------

tcpflag!=VALUE/MASK	が、VALUEに一致、または不一致であるTCPパケットVALUEとMASKは0xに続く十六進数で0x0000~0xffff
---------------------	---

*	すべてのプロトコル
---	-----------

---

- 省略時は \* と同じ。

[初期値] :-

SRC\_PORT\_LIST : PROTOCOLに、TCP(tcp/tcpsyn/tcpfin/tcprst/established/tcpflag)、UDP(udp)のいずれかが含まれる場合は、TCP/UDPのソースポート番号。PROTOCOLがICMP(icmp)単独の場合には、



ICMPタイプ。

[設定値] :

- ポート番号、タイプを表す十進数
- ポート番号を表すニーモニック (一部)

ftp 20,21

ftpdata 20

telnet 23

smtp 25

domain 53

gopher 70

finger 79

www 80

pop3 110

sunrpc 111

ident 113

ntp 123

nntp 119

snmp 161

syslog 514

printer 515

talk 517

route 520

uucp 540

submission 587

- 間に - を挟んだ2つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10個以内)
- \* (すべてのポート、タイプ)

- ・省略時は \* と同じ。

[初期値] :-

DEST\_PORT\_LIST

[設定値] : PROTOCOLに、TCP(tcp/tcpsyn/tcpfin/tcprst/established/  
tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDPの  
デスティネーションポート番号。PROTOCOLがICMP(icmp) 単独の  
場合には、ICMPコード

[初期値] :-

[説明]

IPパケットのフィルタを設定する。本コマンドで設定されたフィルタは  
ip filter directed-broadcast、ip filter dynamic、ip filter set、  
ip forward filter、ip fragment remove df-bit、ip INTERFACE rip filter、  
ip INTERFACE secure filter、およびip routeコマンドで用いられる。

[ノート]

restrict-log及びrestrict-nologを使ったフィルタは、回線が接続されている  
時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに  
有効である。

例えば、時計を合わせるためのNTPパケットがこれに該当する。ICMPパケットに  
対して、ICMPタイプとICMPコードをフィルタでチェックしたい場合には、  
PROTOCOLには'icmp'だけを単独で指定する。

PROTOCOLが'icmp'単独である場合にのみ、SRC\_PORT\_LISTはICMPタイプ、  
DEST\_PORT\_LISTはICMPコードと見なされる。

PROTOCOLに'icmp'と他のプロトコルを列挙した場合にはSRC\_PORT\_LISTと  
DEST\_PORT\_LISTの指定はTCP/UDPのポート番号と見なされ、ICMPパケットとの比  
較は行われぬ。

また、PROTOCOLに'icmp-error'や'icmpinfo'を指定した場合には、  
SRC\_PORT\_LIST とDEST\_PORT\_LISTの指定は無視される。

PROTOCOLに'\*'を指定するか、TCP/UDPを含む複数のプロトコルを列挙している  
場合には、SRC\_PORT\_LISTとDEST\_PORT\_LISTの指定はTCP/UDPのポート番号と見

なされ、パケットがTCPまたはUDPである場合のみポート番号がフィルタが比較される。パケットがその他のプロトコル (ICMPを含む) の場合には、SRC\_PORT\_LISTとDEST\_PORT\_LISTの指定は存在しないものとしてフィルタと比較される。

src\_addrおよびdest\_addrはIPアドレスとFQDNとmap-eを混合することも可能。src\_addrおよびdest\_addrにFQDNを指定することによって、固定IPアドレスではないサーバーや1つのFQDNに対して複数の固定IPアドレスを持つサーバーを対象にしたフィルタリングを行う事が出来る。FQDNを使用する場合、ルーター自身がDNSリカーシブサーバーとして動作し、ルータ配下の端末は、DNSサーバーとして本機を指定する必要がある。

src\_addrおよびdest\_addrへのFQDNの指定はNVR700W Rev.15.00.10 以降、NVR510 Rev.15.01.13 以降のファームウェアで指定可能。

指定したFQDNに一致する通信が発生した場合、設定したFQDNに該当するIPアドレスの情報が保持される。保持される期間は、ip filter fqdn timerコマンドで指定できる。

src\_addrおよびdest\_addrへのmap-eの指定はNVR700WはRev.15.00.22以降のファームウェアで指定可能。 ★

## ○動的フィルタの定義

### [書式]

```
ip filter dynamic DYN_FILTER_NUM SRCADDR[/MASK] DSTADDR[/MASK] PROTOCOL [OPTION ...]
```

```
ip filter dynamic DYN_FILTER_NUM SRCADDR[/MASK] DSTADDR[/MASK] filter FILTER_LIST [in FILTER_LIST] [out FILTER_LIST] [OPTION...]
```

```
no ip filter dynamic DYN_FILTER_NUM
```

### [設定値及び初期値]

DYN\_FILTER\_NUM

[設定値] : 動的フィルタ番号 (1..21474836)

[初期値] :-

SRCADDR

[設定値] : 始点IPアドレス

- ip filterコマンドのsrc\_addrと同じ形式
- 省略した場合は一個の \* と同じ

[初期値] : -

DSTADDR

[設定値] : 終点IPアドレス

- SRCADDRと同じ形式
- 省略した場合は一個の \* と同じ

[初期値] : -

MASK : IPアドレスのビットマスク (src\_addrおよびdest\_addrがネットワークアドレスの場合のみ指定可)

[初期値] : -

PROTOCOL : プロトコルのニーモニック

[設定値] :

- echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/  
whois/dns/domain/
- tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/  
ms-rpc/
- netbios\_ns/netbios\_dgm/netbios\_ssn/imap/snmp/snmptrap/bgp/  
imap3/ldap/
- https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
- ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
- ping/ping6/tcp/udp

以下のニーモニックは設定できますが、動的フィルタとして動作しません

- dhcpc/dhcps/dhcpv6c/dhcpv6s

[初期値] : -

FILTER\_LIST

[設定値] : ip filterコマンドで登録されたフィルタ番号のリスト

[初期値] : -

## OPTION

[設定値]:

- syslog=SWITCH

on コネクションの通信履歴をSYSLOGに残す

off コネクションの通信履歴をSYSLOGに残さない

- timeout=time

time データが流れなくなったときにコネクション情報を解放する

までの秒数

[初期値]: syslog=on

### [説明]

動的フィルタを定義する。第1書式では、あらかじめルーターに登録されているアプリケーション名を指定する。

第2書式では、ユーザーがアクセス制御のルールを記述する。キーワードの filter、in、outの後には、ip filterコマンドで定義されたフィルタ番号を設定する。

filterキーワードの後に記述されたフィルタに該当するコネクション(トリガ)を検出したら、それ以降inキーワードとoutキーワードの後に記述されたフィルタに該当するコネクションを通過させる。

inキーワードはトリガの方向に対して逆方向のアクセスを制御し、outキーワードは動的フィルタと同じ方向のアクセスを制御する。

なお、ip filterコマンドのIPアドレスは無視される。pass/rejectの引数も同様に無視される。

プロトコルとしてtcpやudpを指定した場合には、アプリケーションに固有な処理は実施されない。

特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。

### ○IPv6フィルタの定義

[書式]

```
ipv6 filter FILTER_NUM PASS_REJECT SRC_ADDR[/PREFIX_LEN] [DEST_ADDR[/PREFIX_LEN]  
[PROTOCOL [SRC_PORT_LIST [DEST_PORT_LIST]]]]
```

```
no ipv6 filter FILTER_NUM [PASS_REJECT]
```

[設定値及び初期値]

FILTER\_NUM

[設定値] : 静的フィルタ番号 (1..21474836)

[初期値] : -

PASS\_REJECT

[設定値] : フィルタのタイプ (ip filterコマンドに準ずる)

[初期値] : -

SRC\_ADDR

[設定値] : IPパケットの始点IPアドレス

- IPv6アドレス
  - 静的または動的IPv6アドレス
  - , を区切りとして複数設定することができる。
- map-e ★
  - MAP-Eのマップルールにより生成されたグローバルIPv6アドレスを表すキーワード ★

[初期値] : -

PREFIX\_LEN

[設定値] : プレフィックス長

[初期値] : -

DEST\_ADDR

[設定値] : IPパケットの終点IPアドレス

- SRC\_ADDRと同じ形式
- 省略した場合は一個の \* と同じ

[初期値] : -

PROTOCOL : フィルタリングするパケットの種類 (ip filterコマンドに準ずる)

[設定値]:

-----

設定値 説明

-----

icmp-nd 近隣探索に関するパケットの指定を示すキーワード。  
(TYPEが133、134、135、136のいずれかであるICMPv6パケッ  
ト)

icmp4 ICMPv4パケットの指定を示すキーワード

icmp ICMPv6パケットの指定を示すキーワード

icmp6

-----

[初期値]:-

SRC\_PORT\_LIST

[設定値]:TCP/UDPのソースポート番号、あるいはICMPv6タイプ  
(ip filterコマンドに準ずる)

[初期値]:-

DEST\_PORT\_LIST

[設定値]:TCP/UDPのデスティネーションポート番号、あるいはICMPv6コー  
ド

[初期値]:-

[説明]

IPv6のフィルタを定義する。

○IPv6動的フィルタの定義

[書式]

ipv6 filter dynamic DYN\_FILTER\_NUM SRCADDR[/PREFIX\_LEN] DSTADDR[/PREFIX\_LEN] PROTOCOL

[OPTION ...]

ipv6 filter dynamic DYN\_FILTER\_NUM SRCADDR[/PREFIX\_LEN] DSTADDR[/PREFIX\_LEN] filter

FILTER\_LIST [in FILTER\_LIST] [out FILTER\_LIST] [OPTION ...]

no ipv6 filter dynamic DYN\_FILTER\_NUM [SRCADDR ...]

[設定値及び初期値]

• DYN\_FILTER\_NUM

[設定値] : 動的フィルタ番号 (1..21474836)

[初期値] : -

• SRCADDR

[設定値] : 始点IPv6アドレス

- ipv6 filterコマンドのsrc\_addrと同じ形式
- 省略した場合は一個の \* と同じ

[初期値] : -

• PREFIX\_LEN

[設定値] : プレフィックス長

[初期値] : -

• DSTADDR

[設定値] : 終点IPv6アドレス

- SRCADDRと同じ形式
- 省略した場合は一個の \* と同じ

[初期値] : -

• PROTOCOL : プロトコルのニーモニック

[設定値] :

- echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time  
/whois/dns/domain/dhcps/
- dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp  
/ntp/ms-rpc/
- netbios\_ns/netbios\_dgm/netbios\_ssn/imap/snmp/snmptrap/bgp  
/imap3/ldap/
- https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
- dhcpcv6c/dhcv6s/ms-sql/radius/l2tp/pptp/nfs/msblast  
/ipsec-nat-t/sip/



- ping/ping6/tcp/udp

[初期値] :-

- FILTER\_LIST

[設定値] : ipv6 filterコマンドで登録されたフィルタ番号のリスト

[初期値] :-

- OPTION

[設定値] :

- syslog=SWITCH

on コネクションの通信履歴をsyslogに残す

off コネクションの通信履歴をsyslogに残さない

- timeout=TIME

time データが流れなくなったときにコネクション情報を解放する  
までの秒数

[初期値] :

- syslog=on

- timeout=60

## [説明]

IPv6の動的フィルタを定義する。第1書式では、あらかじめルーターに登録されているアプリケーション名を指定する。

第2書式では、ユーザーがアクセス制御のルールを記述する。キーワードのfilter、in、outの後には、ipv6 filterコマンドで定義されたフィルタ番号を設定する。

filterキーワードの後に記述されたフィルタに該当するコネクション(トリガ)を検出したら、それ以降inキーワードとoutキーワードの後に記述されたフィルタに該当するコネクションを通過させる。

inキーワードはトリガの方向に対して逆方向のアクセスを制御し、outキーワードは動的フィルタと同じ方向のアクセスを制御する。

なお、ipv6 filterコマンドのIPアドレスは無視される。pass/rejectの引数も

同様に無視される。

ここに記載されていないアプリケーションについては、filterキーワードを使って定義することで扱える可能性がある。

特にsnmpのように動的にポート番号が変化しないプロトコルの扱いは容易である。tcpかudpを設定することで扱える可能性がある。特に、telnetのように動的にポート番号が変化しないプロトコルはtcpを指定することで扱うことができる。

src\_addrおよびdest\_addrはIPv6アドレスとmap-eを混合することも可能 ★

src\_addrおよびdest\_addrへのmap-eの指定はNVR700W Rev.15.00.22以降で指定可能。 ★

[11] Web GUIの以下で、OCNバーチャルコネクトサービス 固定IP1契約の設定時に設定されるLuaスクリプトを変更した。

- 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]

[12] Web GUIの詳細設定の[LAN]-[IPアドレス]で、IPアドレスを手動で設定するとき、その他の設定のIPアドレスを自動で変更する範囲の初期値を以下のように変更した。これに伴い、設定項目の表示順序を変更した。

- 変更前：DHCPで払い出すIPアドレスの範囲のみ変更する
- 変更後：設定に含まれるIPアドレスをすべて変更する

[13] SNMPで、内蔵無線WAN機能の標準MIBに対応した。併せて、内蔵無線WANインターフェースの情報をMIB2の範囲で表示するか否かを設定するコマンドを追加した。

○内蔵無線WANインターフェースの情報をMIB2の範囲で表示するか否かの設定

[書式]

```
snmp yrifwwandisplayatmib2 SWITCH
```

```
no snmp yrifwwandisplayatmib2
```

## [設定値及び初期値]

SWITCH

[設定値]:

設定値	説明
-----	----

-----+-----

on	!MIB 変数 yrlfWwanDisplayAtMib2 を "enabled(1)" とする
----	--

off	!MIB 変数 yrlfWwanDisplayAtMib2 を "disabled(2)" とする
-----	---

[初期値]: off

## [説明]

MIB変数yrlfWwanDisplayAtMib2の値をセットする。このMIB変数は、内蔵無線WANインターフェースをMIB2の範囲で表示するかどうかを決定する。

[14] Web GUIのLANマップのSWX2210/SWX2210Pシリーズの[ポートの設定]ダイアログで、QoSの設定項目にポート優先度を追加した。

## ■バグ修正

[1] IKEv2でPKI証明書を利用した認証を行うとき、ペイロードの不一致により接続できない場合にリポートすることがあるバグを修正した。

[2] IKEv2を使用してIPsecトンネルを確立している場合、SAの更新処理が行われるときにリポートやハングアップすることがあるバグを修正した。

[3] IPv6でマルチポイントトンネルが確立すると、その後の動作が不安定になり、リポートすることがあるバグを修正した。

Rev.15.00.16以降で発生する。

[4] 以下のコマンドを実行したとき、リポートすることがあるバグを修正した。

- syslog execute command
- no syslog execute command

[5] bgp importコマンドで、不正なオプションを入力した時にリブートすることがあるバグを修正した。

[6] トンネルテンプレート機能を使用して生成した大量のIPsecトンネルで、IKEキープアライブパケットの到達性がない状態が続くとリブートすることがあるバグを修正した。

Rev.15.00.07以降で発生する。

[7] IPsecトンネルの接続数が多いとき、ipsec refresh saを実行するとリブートすることがあるバグを修正した。

[8] 全ノードマルチキャストアドレス(ff02::1)、および全ルーターマルチキャストアドレス(ff02::2)宛のパケットを送信するとき、リブートすることがあるバグを修正した。

Rev.15.00.07で発生する。

[9] IPv6機能で、複数のインターフェースにipv6 rtadv sendコマンドを設定し、RAでプレフィックスの更新通知を受信するとリブートする可能性があるバグを修正した。

Rev.15.00.17以降で発生する。

[10] Web GUIのLANマップで、Webブラウザの複数のタブやウィンドウでそれぞれ異なるインターフェースのLANマップ画面を同時に開いているとき、インターフェース間でスレーブを移動したのちにツリービューから当該スレーブを選択すると、リブー

トしたり状態が正常に表示されなかったりすることがあるバグを修正した。

Rev.15.00.03以降で発生する。

[11] 大量のユーザーがWeb GUIへ同時にログインしたとき、リポートすることがあるバグを修正した。

[12] Anonymousインターフェースを選択した状態でshow status netvolante-dns ppコマンドを実行するとリポートするバグを修正した。

[13] schedule atコマンドで、TIMEに時刻形式以外のパラメーターを指定したntpdateコマンドが設定されているとき、Web GUIの以下のページを開くとリポートすることがあるバグを修正した。

- かんたん設定の[基本設定]-[日付と時刻の設定]

- 管理の[本体の設定]

[14] LANマップで端末監視が有効のとき、消失端末情報が内部的に蓄積し続けリポートする可能性があるバグを修正した。

ただし、この現象は確認されていない。

[15] Web GUIのダッシュボードでVPN接続状態（リモートアクセス）ガジェットを表示させながらpp auth usernameコマンドを設定するとリポートすることがあるバグを修正した。

[16] Flash ROMアクセス中にごく稀にハングアップすることがある不具合を修正した。

[17] 不正な多重タグパケットを受信したとき、ハングアップすることがあるバグを修正した。

[18] DHCPサーバー機能で、DHCP DISCOVERを一度に大量に受信したとき、ハングアップすることがあるバグを修正した。

Rev.15.00.14以降で発生する。

[19] `httpd service off`コマンドが設定されているとき、`disconnect user`コマンドを実行すると、ハングアップすることがあるバグを修正した。

[20] IKEv2のIPsecトンネルにおいて、`ipsec ike keepalive use`コマンドでICMP Echo以外のキープアライブ方式を設定している場合、IKE SAの更新処理が行われる度にメモリーリークが発生するバグを修正した。

[21] `ipsec transport`コマンドを設定するとメモリーリークが発生するバグを修正した。

[22] IPv6プレフィックスのRAの有効寿命が尽きたとき、メモリーリークが発生するバグを修正した。

[23] YNOエージェント機能で、YNOマネージャーのファームウェア更新機能によってファームウェアを更新したとき、YNOマネージャーのジョブの実行結果に更新前のリビジョンが表示されるバグを修正した。

[24] TELポートが起動後497日以降に使えなくなる可能性を排除した。

[25] 複数のルーティングプロトコルから同一の経路を受信しているとき、`bgp export`コマンドでルーティングテーブルに取り込まない設定になっているBGP由来の経路が`show ip route detail`コマンドの結果に表示されることがあるバグを修正した。

[26] `ospf export from ospf`コマンドが設定されているとき、BGPで受信した経路が`bgp`

exportコマンドの設定どおりにルーティングテーブルに取り込まれないことがあるバグを修正した。

[27] 複数のルーティングプロトコルから同一の経路を受信しているとき、OSPFの優先度が最も高く設定されていると、他のルーティングプロトコル由来の経路をbgp importコマンドの設定どおりにBGPに取り込むことができないことがあるバグを修正した。

[28] YNOエージェント機能で、以下のいずれかの状態でルーターが起動すると、"[YNO\_AGENT] internal error"がDEBUGレベルのSYSLOGに出力されるバグを修正した。

- yno useコマンドがon、かつyno access codeコマンドが設定されている
- yno useコマンドがon、かつyno zero-config idコマンドが設定されている

[29] YNOエージェント機能で、以下のバグを修正した。

- 発生したアラームが正常にYNOマネージャーに通知されないことがある
- 発生したアラームが重複してYNOマネージャーに通知されることがある

[30] YNOエージェント機能で、YNOマネージャーでアクセスコードを変更したときYNOマネージャーに接続済みのルーターに変更したアクセスコードが適用されないことがあるバグを修正した。

[31] YNOのGUI Forwarder経由で、Web GUIの詳細設定の[プロバイダー接続]から既存の設定で「IPv4 over IPv6 トンネルの設定」を「使用する」に変更すると、正常にページ遷移が行われないバグを修正した。

[32] マルチポイントトンネルインターフェースのアドレスがゲートウェイに指定されている静的経路が、対象のトンネルの切断時に消失し、トンネルが再確立しても復元せずに当該経路の通信ができなくなるバグを修正した。

Rev.15.00.17以降で発生する。

- [33] IKEv2デジタル署名方式の認証によるIPsec接続で、RSA鍵長2048ビットの証明書を利用すると接続が確立しないことがあるバグを修正した。
- [34] IKEv2のレスポnderとして動作しているとき、イニシエーターからIDr無しのIKE\_AUTHを受信した場合に認証エラーとなり、IKEv2の接続ができないことがあるバグを修正した。
- [35] IKEv2のレスポnderとして動作しているとき、イニシエーターからのIKE\_SA\_INITを2回以上受信すると、IKE\_AUTH以降の処理で不正な値のresponderSPIを送信して接続できないことがあるバグを修正した。
- [36] L2TP/IPsecおよびL2TPv3/IPsecにおいて、tunnel disableコマンドが設定されているときに接続できてしまうバグを修正した。
- [37] 既に受信したことのあるRAと同じRAを再受信したとき、パケットロスが発生することがあるバグを修正した。
- [38] IPマスカレード機能では、PPTPで使用されるGREパケットはIPヘッダ一部の書き換えと共にGREヘッダ一部を書き換えるが、PPTPの通信パケットとは認識されないGREパケットのGREヘッダ一部を不当に書き換えることがあるバグを修正した。
- [39] L2MSでスタック1台構成、かつ、スタックIDが1以外のスレーブが接続されているとき、認識できないスレーブとして検出されるバグを修正した。
- [40] IPマスカレード機能で、TCP, UDP, ICMP, GRE以外のプロトコルのNATエントリーが存在するとき、当該プロトコルの外から内向きのパケットを受信すると不要なNAT



エントリーが登録されることがあるバグを修正した。

Rev.15.00.17で発生する。

[41] インターフェースIDが::1の動的IPv6アドレスが割り当てられたとき、ネットボランチDNSが使用できないバグを修正した。

[42] 動的フィルター機能で、ファストパスが有効かつNATまたはIPマスカレードが適用される通信において、動的フィルターセッションの戻り方向の通信が発生しているにもかかわらず、当該セッションがタイムアウトで削除されることがあるバグを修正した。

[43] 動的フィルター機能で、ファストパスが有効かつNATまたはIPマスカレードが適用される通信において、動的フィルターセッションの削除に連動して、対応するファストパスのフローが削除されないバグを修正した。

[44] RAプロキシ配下のLANインタフェースで、RA受信により生成したIPv6アドレスが、暫定IPv6アドレスのままになることがあるバグを修正した。

Rev.15.00.17以降で発生する。

[45] メール通知機能で、SMTP認証を有効にしたとき一部のメールサーバーに対してメールを送信できないバグを修正した。

[46] DHCPサーバー機能で、DHCP REQUESTメッセージのOptionにEndが入っていないとき、不正な値をOptionの値として取得してしまうことがあるバグを修正した。

[47] LAN分割時に、ファストパスでIPv6マルチキャストパケットを送信できないバグを

修正した。

[48] トンネルQoSで、ファストパス経由のパケットはトンネルインターフェースのクラス分け設定に従うのに対し、ノーマルパス経由のパケットはトンネルの送出インターフェースとなっている物理インターフェースのクラス分け設定に従ってしまい、ファストパスとノーマルパスでクラス分け結果が異なるバグを修正した。

[49] OCNバーチャルコネクトサービスで、接続中の回線を動的IP契約から固定IP契約へ切り替えたとき、IPマスカレードで利用するポートの範囲が更新されないバグを修正した。

[50] ファストパスで、ip tos supersedeコマンドの設定値によるtosフィールドの書き換えが行われない事があるバグを修正した。

IPヘッダのサービスタイプが設定値と同じパケットによってファストパスのフローが作られたときに、そのフローを利用するがサービスタイプが違うパケットについて書き換えが行われていなかった。

[51] dhcp scope optionコマンドで、オプション番号252の設定値をバイナリで入力したとき、show config コマンド実行時に余分な文字列が表示されることがあるバグを修正した。

[52] show status mobile signal-strengthコマンドで、不正なキーワードを入力してもエラーが表示されないバグを修正した。

[53] dhcp scope optionコマンドで、オプション値に特殊文字（?#|>¥"(空白)）を含む文字列を設定したとき、コンソール上で正しく設定内容が表示されないバグを修正した。

[54] showコマンドの表示中にログインタイマーが満了しても、showコマンドの実行結果

の表示が止まらず、ログアウトされないバグを修正した。

[55] 動的フィルターの適用されたインターフェースで受信したIPv4フラグメントパケットにおいて、再構成のために保持しておく時間がip reassembly hold-timeコマンドの設定値に従っていないバグを修正した。

[56] nat descriptor masquerade incomingコマンドで、actionパラメーターがthroughまたはforwardに設定されているとき、TCP、UDP、ICMP、GRE以外のパケットを外から内向きに転送すると、不要なNATエントリーが登録されることがあるバグを修正した。

[57] no ipsec tunnelコマンドで、policy\_idオプションに整数以外が指定できるバグを修正した。

これにより、ipsec tunnelコマンドが意図せず削除されトンネルがダウンすることがなくなる。

[58] IPマスカレード機能で、UPnPのポートマッピングのリクエストまたはFTPのPASV/PORTコマンドに応じたNATエントリーの作成および削除が行われると、以後TCP以外のセッションまたはFTPセッションで正常に通信ができなくな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。

Rev.15.00.17以降で発生する。

[59] show arpコマンドのカウント数が不正な値になることがあるバグを修正した。

[60] httpd serviceコマンドをonとoffに繰り返して設定した場合、Web GUIへログインできなくなることがあるバグを修正した。

[61] SNMP機能で、snmp yriftunneldisplayatmib2コマンドをonに設定すると、標準MIBの内蔵無線WANのインターフェース番号に不正な値が表示されるバグを修正した。

[62] console characterにen.asciiが設定されているとき、show ipv6 addressコマンド実行時に表示される括弧が文字化けするバグを修正した。

Rev.15.00.17で発生する。

[63] 以下のコマンドで、無効なポート番号を設定できるバグを修正した。

表示上の問題であり、機能には影響はない。

- ip filterコマンド
- ipv6 filterコマンド
- ipsec transportコマンド
- queue class filterコマンド

[64] Web GUIにログインしているとき、httpd serviceコマンドをonからoffに設定すると、ログインタイマー満了後にユーザーがログアウトされないバグを修正した。

[65] Web GUIの以下のページでプロバイダーの設定を追加したとき、dns hostコマンドがdns host lan1に上書きされ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]

[66] Web GUIのかんたん設定の[VPN]-[リモートアクセス]で、L2TP/IPsecの認証鍵にスペースや「|」「#」「¥」などの特殊文字が含まれている状態でリモートアクセスのユーザーを追加したとき、正しく設定されないバグを修正した。

[67] Web GUIのLANマップの設定[マスターモード時の動作設定]-[端末の管理]-[下記無線AP配下の端末の更新間隔]で、対象の機種一覧にWLX212が記載されていないバグ

を修正した。

[68] Web GUIのLANマップで、タグVLANの設定を追加または変更したとき、dns hostコマンドにタグVLANのインターフェースが重複して設定されることがあるバグを修正した。

[69] Web GUIのLANマップの[一覧マップ]で、L2MSのマスターとして動作しているときに、スレーブルーターに接続されているスレーブのリンク速度が正しく表示されないことがあるバグを修正した。

[70] Web GUIの管理の[アクセス管理]-[各種サーバーの設定]-[SSH/SFTP を使用したアクセス]で、利用できないアルゴリズムが表示されるバグを修正した。

[71] Web GUIのかんたん設定の[アプリケーション制御]-[フィルターと経路]で、すべての経路を「アプリケーションごとの振り分けをしない」に変更したとき、デフォルト経路が削除されないことがあるバグを修正した。

[72] Web GUIのかんたん設定の[アプリケーション制御]-[フィルターと経路]で、デフォルトゲートウェイに設定されていないインターフェースを経路に設定したとき、設定されたインターフェースのプロバイダー設定が、かんたん設定および詳細設定の[プロバイダー接続]のページに表示されなくなるバグを修正した。

[73] Web GUIの以下のページで、IPv6 IPoE(DHCP)接続の「v6プラス」固定IPサービスを設定したとき、不正な内容が設定されてIPv4で通信できなくなるバグを修正した。

- 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]

[74] Web GUIのかんたん設定の[YNOエージェント]で、半角カタカナが含まれている文字列を設定しようとする、すでに設定されているyno useコマンドとyno access

codeコマンドが削除されるバグを修正した。

[75] Web GUIのダッシュボードの[Live]の各ガジェットで、URLを直接Webブラウザに指定したときに正常に表示されないバグを修正した。

Rev.15.00.16以降で発生する。

[76] Web GUIのダッシュボードのヘルプで、[概要]-[Liveの使い方]-[警告表示]の表にファンについての記載があるバグを修正した。

[77] Web GUIのかんたん設定の[プロバイダー接続]でプロバイダー接続の新規設定を行うとき、インターフェースの選択ページで初期選択されているラジオボタンに応じたパンくずリストが表示されないバグを修正した。

[78] Web GUIの以下のヘルプページで、誤記を修正した。

- 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]

[79] コマンドヘルプの誤記を修正した

---

## ■更新履歴

Apr. 2021, Rev.15.00.22 リリース

May. 2021, 誤記修正

Jul. 2021, バグ修正[6]文面修正

Nov. 2021, 脆弱性対応[2] 追加

以上