IPsec 対応ブロードバンドアクセスルータ

コマンドリファレンス

FITELnet-F シリーズ
（設定コマンド編）

古河電工

目次

各設定モードへの移行コマンド 6
LANインタフェース設定モード 6
PPPoEインタフェース設定モード 7
EWANインタフェース設定モード 8
BRIインタフェース設定モード 9
RIPサービス設定モード 10
OSPFサービス設定モード 11
BGPサービス設定モード 12
RIPngサービス設定モード 13
Route-MAP設定モード 14
DHCPサーバ設定モード 16
IPv6 アドレスプール設定モード 18
DHCPv6 クライアントプロファイル設定モード 19
key-chainモード 20
イベントクラス設定モード 22
イベントアクション設定モード 23
イベントマップ設定モード 24
ICMPクラス設定モード 25
クラスマップ設定モード 26
アクションマップ設定モード 27
ポリシーマップ設定モード 28
ダイヤルアップインタフェース設定モード 29
ループバックインタフェース設定モード 30
IPsecインタフェース設定モード 31
トンネルインタフェース設定モード 32
VLANインタフェース設定モード 33
電子証明書（自身のID）設定モード 34
IKEポリシー設定モード 35
VPNセレクタ設定モード 36
IPsec各種設定モード 37
IPsecログモード 38
Ethernet設定モード 39
HTTPクライアント設定モード 40
PPPoE機能 41
PPPoEを使用するための設定 41
DHCPクライアント機能 54
DHCPクライアントとして使用するための設定 54
DHCPv6 クライアント機能 60
DHCPv6 クライアント機能を使用するための設定 60
IPv6 ルーティングの設定 65
IPv6 アドレス設定 65
ICMPv6 に関する設定 69
RIPng 86

フィルタリングの設定 96
スタティックルーティングの設定 109
MTU長の設定 111
ポリシールーティング 113

IPv4 ルーティングの設定 125

IPアドレスの設定 125
RIPに関する設定 128
OSPFに関する設定 157
BGPに関する設定 206
フィルタリングの設定 249
スタティックルーティングの設定 262
ルートマップの設定 265
リゾルバの設定 281
MTU長 289
TCP MSS 291
ProxyARPの設定 293
ARP制御の設定 294
ダイレクトブロードキャストの設定 300
ICMP制御の設定 301
ポリシールーティング 303
ポリシーマップの定義 312
マルチキャストの設定 316
リミテッドブロードキャストの設定 334

IPsec機能の設定 335

IPsec基本コマンド 335
Phase1 ポリシーの設定 339
Phase2 ポリシーの設定 374
Mode-configの設定 376
トンネルルート機能の設定 385
SA-UPルート機能の設定 389
拡張認証の設定 391
VPNセレクタの設定 397
電子証明書に関する設定 417
IPsecのログ情報に関する設定 423
IPsecの各種設定 427

IP in IP機能 447

IP in IP機能 447

NAT機能 452

NAT機能 452

DHCPサーバ機能 478

DHCPサーバ機能 478

DHCPリレーエージェント機能 491

DHCPリレーエージェント機能 491

簡易DNS機能 496
簡易DNS機能の設定 496
ドメイン名によるDNS振り分け 503
ホスト名称とDNS IPアドレスの登録 504
ダイナミックDNS機能 505
サーバ機能 505
クライアント機能(ダイナミックDNS動作の設定) 509
クライアント機能（HTTPクライアントに関する設定） 511
簡易ファイアウォール機能 518
外部からの接続制御機能 518
フィルタリング機能 521
サービス制限機能 525
冗長機能 534
VRRP機能 534
イベント-アクション機能 543
宛先到達確認 554
QoS/CoS機能 581
クラスマップの定義 581
アクションマップの定義 588
ポリシーマップの定義 601
ポリシーマップの適用とキューの定義 604
L2 QoS機能 613
L2 QoS機能 613
UPnP 機能 619
UPnP 機能 619
BRIモジュール回線の選択 622
BRIモジュール回線の選択 622
ダイヤルアップ機能 623
ダイヤルアップ機能 623
HSDに関する機能 658
HSDに関する機能 658
障害監視／通知機能 664
SNMPエージェント機能 664
SYSLOGDへの障害通知機能 672
電子メールによる障害通知機能 690
NTP機能 698
SNTPクライアント機能 698
NTPサーバ機能 704
SSHサーバ機能 706

SSHサーバ機能 706
Ethernet機能 712
Ethernet機能 712
VLAN機能 721
VLAN機能 721
アクセスリスト 728
アクセスリスト 728
ループバックインタフェースの設定 739
ループバックインタフェースの設定 739
その他の機能 742
CLIの表示に関する機能 742
高速化キャッシュ機能 746

各設定モードへの移行コマンド

LANインタフェース設定モード

interface lan

LAN インタフェース設定モードに移行します。

設定例１　LAN インタフェース設定モードに移行する

```
Router(config)#interface lan 1
Router(config-if lan 1)#
```

コマンド書式

interface lan 1

パラメータ

パラメータはありません。

設定モード

基本設定モード

PPPoEインタフェース設定モード

interface pppoe

PPPoE インタフェース設定モードに移行します。
FITELnet-F シリーズ※は、24 の PPPoE インタフェースを持つことができます。PPPoE インタフェース設定モードに移行する際は、PPPoE インタフェースの番号(1～24)を指定します。

refresh コマンド後に有効になるコマンドです。

※:F80 の PPPoE インタフェース数は5つです。

設定例１　PPPoE インタフェース設定モードに移行する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#
```

コマンド書式

interface pppoe <PPPoE 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
PPPoE 番号	PPPoE ポートの番号を指定します。	1～24※	省略不可

※:F80 の場合は、1～5 になります。

設定モード

基本設定モード

EWANインタフェース設定モード

interface ewan

EWAN インタフェース設定モードに移行します。
同一物リポートで、EWAN インタフェースと、PPPoE インタフェースが共存することはできません。
両方の設定がされていると、elog に「ewan and pppoe interface duplicate set」と書かれ、インタフェースが起動しません。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN インタフェース設定モードに移行する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#
```

コマンド書式

interface ewan <EWAN 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
EWAN 番号	EWAN ポートの番号を指定します。	1～2	省略不可

設定モード

基本設定モード

BRIインタフェース設定モード

interface bri　【F100 専用コマンド】

BRI インタフェース設定モードに移行します。

設定例１　BRI インタフェース設定モードに移行する

```
Router(config)#interface bri 1
Router(config-if bri 1)#
```

コマンド書式

interface bri 1

パラメータ

パラメータはありません。

設定モード

基本設定モード

RIPサービス設定モード

router rip

RIP サービス設定モードに移行します。
RIP の各種設定を行ないます。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP サービス設定モードに移行

```
Router(config)# router rip
Router(config-rip)#
```

コマンド書式

router rip

パラメータ

パラメータはありません。

この設定を行わない場合

RIP を使用できません。

設定モード

基本設定モード

OSPFサービス設定モード

router ospf

OSPF サービス設定モードへ移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF サービス設定モードへ移行する

```
Router(config)#router ospf
Router(config-ospf)#
```

コマンド書式

router ospf

パラメータ

パラメータはありません。

この設定を行わない場合

OSPF を使用することができません。

設定モード

基本設定モード

BGPサービス設定モード

router bgp

BGP サービス設定モードに移行します。(AS 番号を指定)
BGP サービス設定モードでは、E-BGP/I-BGP のピアのアドレスや、各種アトリビュート情報を設定します。有効になる最大ピア数は、16 ピアです

refresh コマンド後に有効になるコマンドです。

設定例１　BGP サービス設定モードに移行する（自 AS 番号=64512）

```
Router (config)# router bgp 64512
Router (config-bgp)#
```

コマンド書式

router bgp〈自 AS 番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
自 AS 番号	自装置側の AS 番号を指定します。	1～65535	省略不可

この設定を行わない場合

BGP を使用できません。

設定モード

基本設定モード

RIPngサービス設定モード

router ripng

RIPng サービス設定モードへ移行します。
RIPng の各種設定を行ないます。

設定例１　RIPng サービス設定モードに移行する

```
Router(config)# router ripng
Router(config-ripng)#
```

コマンド書式

router ripng

パラメータ

パラメータはありません。

この設定を行わない場合

RIPng を使用できません。

設定モード

基本設定モード

Route-MAP設定モード

route-map

Route-map 設定モードに移行します。
Route-MAP とは、ルート情報の送受信条件や送受信先を詳細に規定しておくものです。
ルート情報の送受信条件や送受信対象を"match "で特定し、送受信するルート情報を"set "で編集します。
no route-map を指定した場合は、Route-map で設定した内容をすべてクリアします。

設定例 1　Route-map 名=map1 の Route-map 設定モードに移行する

```
Router(config)# route-map map1 permit 1
Router(config-rmap map1 permit 1)#
```

コマンド書式

route-map ｛ Route-map 名 ｝｛ permit | deny ｝〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Route-map 名	各種ルーティングプロトコルで、Route-map を指定する場合の名称になります。	-	省略不可
permit｜deny	このルートマップが許可する属性(permit)なのか、許可しない属性(deny)なのかを指定します。	permit deny	省略不可
シーケンス番号	同じルートマップ名で、複数の操作を行なう場合に、複数の属性を指定します。 ここにつける番号が、シーケンス番号です。	1～65535	省略不可

この設定を行わない場合

詳細な経路の制御を使用できない場合があります。

Route-map 詳細

Route-map の詳細について説明します。
Route-map は、ルーティングプロトコルの、各種パラメータの操作・経路情報のフィルタリングのために使用します。

例１　BGP で広告する場合は、メトリック（MED 値）を 5 としたい

FITELnet-F シリーズでは、何も指定しない場合は MED のアトリビュートを付加せずに BGP のアップデート情報を通知しますが、Route-map を利用することにより、MED アトリビュートをつけて BGP のアップデートを通知することができます。

設定モード

基本設定モード

DHCPサーバ設定モード

ip dhcp pool

DHCP サーバ設定モードに移行します。
本装置の LAN/EWAN2 インタフェースで、本装置を DHCP サーバとして使用する場合には設定が必要です。

DHCP サーバ機能と、DHCP リレーエージェント機能は共存できません。両方の設定がされている場合は、DHCP リレーエージェント機能が採用されます。

設定例　LAN インタフェースで DHCP サーバ機能を使用するために、DHCP サーバ設定モードに移行する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#
```

コマンド書式

ip dhcp pool<インタフェース名>

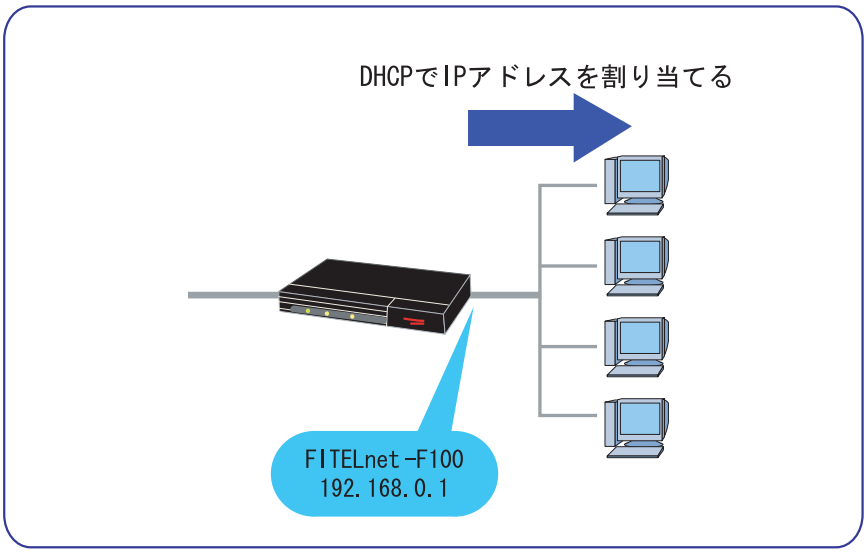
パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DHCP サーバ機能を使用するインタフェースを lan1 または ewan2 から選択します。	lan1 ewan2	省略不可

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？



DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
FITELnet-F シリーズの DHCP サーバ機能では、以下の情報を通知することができます。

・IP アドレス／サブネットマスク
・DNS サーバの IP アドレス
・デフォルトゲートウェイの IP アドレス
・ドメイン名

FITELnet-F シリーズでは、DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

IPv6 アドレスプール設定モード

address-pool ipv6 【F100/F1000 コマンド】

IPv6 のアドレスプールを指定するために、IPv6 アドレスプール設定モードに移行します。
複数設定がある場合は、プール名で sort して、一番先頭のアドレスプールのみ有効になります。

設定例１　IPv6 アドレスプール設定モードに移行する

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)#
```

コマンド書式

address-pool ipv6 〈アドレスプール名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

IPv6 アドレスプールの設定が行えません。

設定モード

基本設定モード

DHCPv6 クライアントプロファイル設定モード

ipv6 dhcp client-profile【F100/F1000 コマンド】

DHCPv6 クライアントとして動作する際の各種パラメータの設定を行う、DHCPv6 クライアントプロファイル設定モードに移行するためのコマンドです。

設定例１　DHCPv6 クライアントプロファイル設定モードに移行する

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)#
```

コマンド書式

ipv6 dhcp client-profile 〈クライアントプロファイル名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クライアント プロファイル名	設定を行う DHCPv6 クライアントプロファイル名を指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

DHCPv6 クライアントを使用することができません。

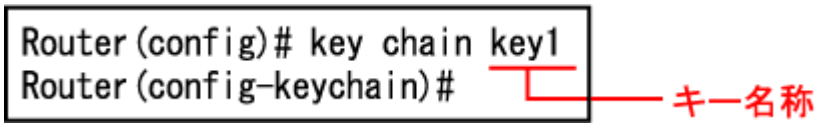
設定モード

基本設定モード

key-chainモード

key chain

RIP2 の認証を有効にするための key-chain モードに移行します。
key-chain の設定は、キー名称を指定して行ないます。key-chain モードで、キーの情報を設定し、各インタフェースの RIP2 に関する設定で、使用するキー名称を指定します。



設定例１　キー名称が"key1"である key-chain モードに移行する

```
Router(config)# key chain key1
Router(config-keychain)#
```

コマンド書式

key chain 〈キー名称〉

パラメータ

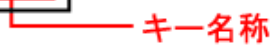
パラメータ	設定内容	設定範囲	省略時の値
キー名称	RIP2 で参照するキー(パスワード)の名称 インタフェース設定モードで参照する名称なので、わかりやすい名前にしてください。	-	省略不可

RIP2 の認証について

RIP2 では、認証キーによる認証を行い、信用できるルータからのルーティング情報であるかどうかを制御することができます。
この認証キーが異なる RIP2 の情報は、ルーティングテーブルに登録しません。

実際の RIP2 に付加される認証の情報には、以下の 2 種類があります。
・simple password （設定されたテキストの情報）
・MD5 digest （設定されたテキストから MD5 で計算されたデータ）
本装置で、RIP2 の認証を使用する場合は、RIP2 を使用するインタフェースのインタフェース設定モードの"ip rip authentication"コマンドで、key-chain で設定するキー名称を指定する形で設定します。

```
Router(config-if lan 1)#ip rip authentication key-chain key1
```



設定モード

基本設定モード

イベントクラス設定モード

event-class

イベントクラス設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントクラス設定モードに移行する

```
Router(config)#event-class 1
Router(config-event-class 1)
```

コマンド書式

event-class〈イベントクラス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントクラス番号	イベントクラス番号を指定します。	1～500※	省略不可

※:F80、F100 の場合は、1～100 になります。

設定モード

基本設定モード

イベントアクション設定モード

event-action

イベントアクション設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントアクション設定モードに移行する

```
Router(config)#event-action 1
Router(config-event-action 1)
```

コマンド書式

event-action 〈イベントアクション番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントアクション番号	イベントアクション番号を指定します。	1～500※	省略不可

※:F80、F100 の場合は、1～100 になります。

設定モード

基本設定モード

イベントマップ設定モード

event-map

イベントマップ設定モードに移行します。

設定例１　イベントマップ設定モードに移行する

```
Router(config)#event-map
Router(config-event-map)
```

コマンド書式

event-map

パラメータ

パラメータはありません。

設定モード

基本設定モード

ICMPクラス設定モード

icmp-class

ICMP クラス設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　ICMP クラス設定モードに移行する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)#
```

コマンド書式

icmp-class 〈ICMP クラス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	ICMP クラス番号を指定します。	1～500※	省略不可

※:F80、F100 の場合は、1～100 になります。

設定モード

基本設定モード

クラスマップ設定モード

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ設定モードへ移行する

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

アクションマップ設定モード

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。
ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。
また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

refresh コマンド後に有効になるコマンドです。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map <policy-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy-map-name	policy-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

ダイヤルアップインタフェース設定モード

interface dialer　【F100 専用コマンド】

dialer インタフェース設定モードに移行します。

設定例１　ダイヤルアップインタフェース設定モードへ移行する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#
```

コマンド書式

interface dialer <ISDN 接続相手シーケンス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ISDN 接続相手シーケンス番号	ISDN 接続相手を識別する番号	1～20	省略不可

設定モード

基本設定モード

ループバックインタフェース設定モード

interface loopback

ループバックインタフェース設定モードに移行します。

設定例１　ループバックインタフェース設定モードに移行する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#
```

コマンド書式

interface loopback 1

パラメータ

パラメータはありません。

設定モード

基本設定モード

IPsecインタフェース設定モード

interface ipsecif

IPsec インタフェース設定モードに移行します。

設定例１　IPsec インタフェース設定モードに移行する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#
```

コマンド書式

interface ipsecif ＜ IPsec インタフェース番号 ＞

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPsec インタフェース番号	IPsec インタフェース番号を指定します。	1～500※	省略不可

※:F80 の場合は、1～32、
　F100 の場合は、1～100 になります。

設定モード

基本設定モード

トンネルインタフェース設定モード

interface tunnel

トンネルインタフェース設定モードに移行します。

設定例１　トンネルインタフェース設定モードに移行します。

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#
```

コマンド書式

interface tunnel〈トンネルインタフェース番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トンネル インタフェース番号	トンネルインタフェース番号を指定します。	1～32	省略不可

設定モード

基本設定モード

VLANインタフェース設定モード

interface vlanif

VLAN インタフェースを登録するために、VLAN インタフェース設定モードに移行します。
VLAN インタフェースでは、属するブリッジグループや、使用する VLAN-TAG 値等の設定を行います。

設定例１　VLAN インタフェース設定モードへ移行する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)
```

コマンド書式

interface vlanif 〈VLAN インタフェース番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN インタフェース番号	VLAN インタフェース番号を指定します。	1～16	省略不可

設定モード

基本設定モード

電子証明書(自身のID)設定モード

crypto ca identity

証明書のリクエストを作成する上で、自身の情報を設定する必要があります。
本コマンドでは、証明書のリクエストを作成する上での、自身の情報を設定するために、電子証明書(自身の ID)設定モードに移行します。

設定例１　電子証明書（自身の ID）設定モードに移行する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#
```

コマンド書式

crypto ca identity

パラメータ

パラメータはありません。

設定モード

基本設定モード

IKEポリシー設定モード

crypto isakmp policy

Internet Key Exchange ポリシー(VPN ピアとのフェーズ 1 ネゴシエーション用のポリシー)のエントリを設定するために、IKE ポリシー設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　IKE ポリシー（ポリシー番号 : １）設定モードに移行する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#
```

コマンド書式

crypto isakmp policy <policy 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy 番号	IKE ポリシーの番号を指定します。 この数字の小さいポリシーを優先的に使用します。	1～500※	省略不可

※:F80 の場合は、1～32、
　F100 の場合は、1～100 になります。

設定モード

基本設定モード

VPNセレクタ設定モード

crypto map

VPN ピアとのセレクタ情報のエントリを設定する為に、VPN セレクタ設定モードに移行します。
設定の際は、セレクタ名称、シーケンス番号を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　VPN セレクタ設定モード（セレクタ名称：Tokyo）に移行する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#
```

コマンド書式

crypto map〈セレクタ名称〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	VPN セレクタの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モードで、 適用する VPN セレクタを指定しますので、わかりやすい名称にしてください。	最大 16 文字の英数字	省略不可
シーケンス番号	シーケンス番号を指定します。 既に使用したシーケンス番号と同じ番号を重複して使用すると以前設定した内容を上書きします。	1～2000※	省略不可

※:最大エントリ
F80:64 エントリ
F100:128 エントリ
F1000:2000 エントリ

設定モード

基本設定モード

IPsec各種設定モード

crypto security-association

IPsec 機能全般の、各種タイマ値等を設定するために、IPsec 各種設定モードに移行します。

設定例１　IPsec 各種設定モードに移行する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#
```

コマンド書式

crypto security-association

パラメータ

パラメータはありません。

設定モード

基本設定モード

IPsecログモード

crypto ipsec-log

"SPI no match"、"block type discard"ログ出力の抑制および、vpnlog 詳細ログ出力を制御するために IPsec ログモードに移行します。

設定例１　IPsec ログモードに移行する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#
```

コマンド書式

crypto ipsec-log

パラメータ

パラメータはありません

設定モード

基本設定モード

Ethernet設定モード

line

Ethernet インタフェースについて、速度/デュプレックス/MDI/MDI-X の設定を行なう Ethernet 設定モードに移行するためのコマンドです。

設定例１　EWAN#1 ポートの設定を行なうモードに移行する

```
Router(config)# line ewan 1
Router(config line ewan 1)#
```

コマンド書式

line〈物理インタフェース〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
物理インタフェース	設定を行なう物理インタフェースを lan 1、ewan 1、ewan 2 から選択します。	lan 1 ewan 1 ewan 2	省略不可

設定モード

基本設定モード

HTTPクライアント設定モード

http-client

ダイナミック DNS 機能に関する HTTP クライアントの設定を行なう HTTP クライアント設定モードに移行するためのコマンドです。

設定例１　HTTP クライアント設定モードに移行する

```
Router(config)# http-client 1
Router(http-client 1)#
```

コマンド書式

http-client <HTTP クライアント番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
HTTP クライアント番号	設定を行なう HTTP クライアント番号を選択します。	1～16	省略不可

設定モード

基本設定モード

PPPoE機能

PPPoEを使用するための設定

pppoe server

PPPoE 接続相手の名称を設定します。この設定は、わかりやすい名称を設定してください。
PPPoE を使用する場合は、この設定が必須になります。

設定例１　接続する相手名称を”A-Provider”に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe server A-Provider
```

コマンド書式

pppoe server〈接続相手名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
接続相手名称	PPPoE 接続相手の名称を設定します。	20 文字以内の文字列	省略不可

この設定を行わない場合

PPPoE が使用できません。

この設定は何に使われるのか？

接続相手の設定を見分けるための名称です。プロバイダに接続するためのパラメータではありません。FITELnet-F シリーズでは、同時に 5 セッションの PPPoE を設定できますので、わかりやすいように名称をつける目的の設定です。

設定モード

PPPoE インタフェース設定モード

pppoe account

プロバイダから指定されたユーザ ID とパスワードを設定します。

設定例１　ユーザ ID に f100@xxxxx.ne.jp, パスワードに f100pass を設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe account f100@xxxxx.ne.jp f100pass
```

コマンド書式

pppoe account 〈ユーザ ID〉〈パスワード〉[{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ ID	プロバイダから指定された、ユーザ ID を設定します。	127 文字以内の文字列	省略不可
パスワード	プロバイダから指定された、パスワードを設定します。	32 文字以内の文字列	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1:このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2:パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

プロバイダに接続することができません。

設定モード

PPPoE インタフェース設定モード

pppoe auth-accept

PPP の認証プロトコル(CHAP or PAP)を指定します。
通常は、プロバイダとのネゴシエーションにより決定します。プロバイダとのネゴシエーションの結果に従う場合は"auto"を指定します。
プロバイダから、認証プロトコルの指示がある場合は、認証プロトコルを指定してください。

設定例１　PPP の認証プロトコルを自動（ネゴシエーションに従う）とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe auth-accept auto
```

設定例２　PPP の認証プロトコルを PAP 固定とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe auth-accept pap
```

コマンド書式

pppoe auth-accept〈認証プロトコル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証プロトコル	認証プロトコルを chap(CHAP 固定)、pap(PAP 固定)または、auto(CHAP または PAP)から指定します。	chap pap auto	省略不可

この設定を行わない場合

auto で動作します。

設定モード

PPPoE インタフェース設定モード

pppoe interface

PPPoE インタフェースと物理ポート(EWAN 1～2)を関連づけます。
FITELnet-F シリーズ※は、24 の PPPoE インタフェースを持つことができます。

※:F80 は、5 つの PPPoE インタフェースになります。

設定例１　PPPoE 6 を EWAN 2 で使用する

```
Router(config)#interface pppoe 6
Router(config-if pppoe 1)#pppoe interface ewan 2
```

コマンド書式

pppoe interface <EWAN ポート>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
EWAN ポート	PPPoE インタフェースを割り当てる、物理ポートを指定します。 none を指定したインタフェースでは、PPPoE を使用できません。	1～2 none	省略不可

この設定を行わない場合

EWAN 1 に 1～4、EWAN 2 に 5 が関連づけられています。

設定モード

PPPoE インタフェース設定モード

pppoe service

サービス名称を設定します。通常は設定の必要はありません。
プロバイダより、サービス名を指定された場合のみ設定が必要です。

設定例１　サービス名称として xxxxx.ne.jp を設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe service xxxxx.ne.jp
```

コマンド書式

pppoe service〈サービス名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サービス名称	サービス名称を設定します。	20 文字以内の文字列	省略不可

この設定を行わない場合

設定なしとなります。

設定モード

PPPoE インタフェース設定モード

pppoe type

PPP の IP 制御プロトコルで IP アドレスのリクエストをするかしないかを設定します。
端末型接続の場合は host と設定し、IP8/IP16 のように LAN 型接続の場合は lan と設定します。

設定例１　PPPoE を LAN 型で接続する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe type lan
```

コマンド書式

pppoe type〈接続タイプ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
接続タイプ	PPPoE の接続タイプを指定します。	host lan	省略不可

この設定を行わない場合

host として動作します。

「端末型」「LAN 型」とは？

「端末型」は、IP アドレスが1つだけ割り当てられる形態、「LAN 型」は、IP アドレスが複数割り当てられる形態を表します。

設定モード

PPPoE インタフェース設定モード

pppoe ncp

PPPoE 接続時に使用する NCP を設定します。ipcp のときは IPCP を、ipv6cp のときは IPv6CP を、both のときはその両方を使用します。

設定例１　NCP に IPCP のみを接続する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe ncp ipcp
```

コマンド書式

pppoe ncp〈中継プロトコル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
中継プロトコル	PPP 上を中継するプロトコルを ipcp(IPv4)、ipv6cp (IPv6)または both(IPv4、IPv6 双方)から指定します。	ipcp ipv6cp both	省略不可

この設定を行わない場合

IPCP を使用します。

NCP とは？

NCP(Network Control Protocol)とは、PPP のオプションで、PPP を接続する両者で通信するプロトコルを規定するためにネゴシエーションするプロトコルです。
PPP は、まず LCP(Link Control Protocol)により、この PPP をどのように使用するかのネゴシエーションを行い、LCP のネゴシエーションが終了した後、どのようなプロトコルを通すかのネゴシエーション(NCP)を行ないます。

IPv4 を通すために行なう NCP を IPCP、IPv6 を通すために行なう NCP を IPv6CP といいます。
例えば、PPP を確立する相手に対して、IPCP のリクエストを送信し、確立可能のレスポンス(ACK)を受信した場合に、PPP 上で IPv4 の通信が可能になります。
ここでの設定は、PPP 上で IPv4/IPv6 のどちら(あるいは両方)の通信を行ないたいかを設定します。

設定モード

PPPoE インタフェース設定モード

ip address

PPPoE インタフェースの IP アドレスを指定します。
PPP で、アドレスを割り当てられるケースでは、設定の必要はありません。
プロバイダより、設定するアドレスを指定された場合に設定してください。

設定例１　PPPoE１の IP アドレスを 192.168.0.1 に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 192.168.0.1
```

コマンド書式

ip address <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

PPPoE インタフェース設定モード

ip name-server

プロバイダから書面で通知されている場合に、プロバイダから通知された DNS サーバの IP アドレスを入力します。書面での通知がない場合は、設定しなくてかまいません。

設定例１　プロバイダから DNS サーバの IP アドレスとして、プライマリ DNS サーバ：158.xxx.xxx.1、セカンダリ DNS サーバ：158.xxx.xxx.2 が通知された

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip name-server 158.xxx.xxx.1 158.xxx.xxx.2
```

コマンド書式

ip name-server 〈DNS アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DNS アドレス	プロバイダから通知された DNS サーバのアドレスを設定します。	IPv4 アドレス形式	省略不可

※ DNS アドレスの優先度は、入力した順に2つまで有効になります。すでに、2つ入力されている状態で3つ目以降を入力しても設定上無効となります。

この設定を行わない場合

PPP で学習できない場合は、リゾルバ・簡易 DNS 機能を使用できません。ただし、基本設定モードの ip name-server, proxydns default name-server コマンドが設定されている場合は、そちらの情報を使用します。

また、PPP で学習できた場合は、学習した DNS サーバの IP アドレスを利用します。

DNS サーバとは？

DNS は Domain Name System の略で、ホスト名から IP アドレス(またはその逆)を探し出すシステムのことです。

このシステムのために、ホスト名と IP アドレスの組み合わせデータベースが存在し、そのデータベースをもつホストのことを、DNS サーバといいます。

DNS サーバは、世界中のホストと IP アドレスの組み合わせデータベースを持っているわけではなく、自分の属するドメインの組み合わせのみを保有し、わからないホスト名のリクエストを受けた場合は、他の DNS サーバに問い合わせるという仕組みを持っています。

設定モード

PPPoE インタフェース設定モード

ip mtu

PPPoE インタフェースの MTU 長を指定します。
フレッツ ADSL または B フレッツを介して PPPoE を接続する場合は、MTU 長を 1454byte より大きくすると、通信できなくなる場合がありますので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例１　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	578～1492	省略不可

この設定を行わない場合

PPPoE インタフェースでは 1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
フレッツ ADSL、B フレッツと接続する場合、必ず経由する IP ネットワークの MTU 値が 1454byte になっています。したがって PPPoE をフレッツ ADSL や B フレッツを介して接続する場合は、この設定を 1454 以下に設定してください。

設定モード

PPPoE インタフェース設定モード

ipv6 mtu

PPPoE インタフェースの MTU 長を指定します。
フレッツ ADSL または B フレッツを介して PPPoE を接続する場合は、MTU 長を 1454byte より大きくすると、通信できなくなる場合がありますので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例１　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu 〈MTU 長〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	1280～1492	省略不可

この設定を行わない場合

PPPoE インタフェースでは 1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
フレッツ ADSL、B フレッツと接続する場合、必ず経由する IP ネットワークの MTU 値が 1454byte になっています。したがって PPPoE をフレッツ ADSL や B フレッツを介して接続する場合は、この設定を 1454 以下に設定してください。

設定モード

PPPoE インタフェース設定モード

mss

インタフェースの MSS 値を指定します。
FITELnet-F シリーズでは、TCP ヘッダオプションに含まれる MSS 値を適切な値に書き換えることができます。
パケットに書かれている値と設定値を比較して小さい方の値にします。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN の MSS 長を 1300byte にする

```
Router(config)#mss lan 1 1300
```

コマンド書式

mss 〈インタフェース名〉〈MSS 値〉
mss ipsec 〈MSS 値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24※1 ipsecif 1～500※2 tunnel 1～32 vlanif 1～16	省略不可
MSS 値	MSS 値を指定します。 off を指定した場合は、MSS 値を変更しません。 ipseif の場合は、VPN セレクタの MSS 値を指定します。※3	1240～1460※4 off	省略不可

※1:F80 の場合は、1～5 になります。
※2:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。
※3:IPsec interface 以外に提供される VPN セレクタの MSS 長の指定となります。
※4:ipsec、tunnel、pppoe の各設定値の上限は、ipsec 1420、tunnel 1440、pppoe 1452 となります。

この設定を行わない場合

各インタフェースからパケットを送出する際に、下記の値とパケットに書かれている値を比較して小さい方の値にします。通常は変更の必要はありません。

LAN interface：MTU 長 -40
EWAN interface：MTU 長 -40
PPPoE interface：MTU 長 -40
IPsec interface：MTU 長 -40
IPsec VPN selector：(送信 IF の MTU)-113
Tunnel interface：MTU 長 -40
VLANIF interface：MTU 長 -40

MSS 長とは？

MSS (Maximum Segment Size)とは、TCP で一度に伝送できるデータの最大量、最大セグメントサイズ。

設定モード

基本設定モード

DHCPクライアント機能

DHCPクライアントとして使用するための設定

dhcp-client retries infinitely

本設定により、DHCP クライアント動作においてアドレスが取得できるまでアドレス取得動作を継続します。

refresh コマンド後に有効になるコマンドです。

設定例１　アドレスが取得できるまで取得動作を継続する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#dhcp-client retries infinitely
```

コマンド書式

dhcp-client retries infinitely

パラメータ

パラメータはありません。

この設定を行わない場合

DHCPDISCOVER を 2 回リトライしても DHCPOFFER が得られない場合、アドレス取得動作を打ち切ります。

設定モード

EWAN インタフェース設定モード

ip address dhcp

EWAN インタフェースで、DHCP クライアント機能を使用する場合に指定します。
ADSL モデムで PPP を終端し EWAN 側に DHCP でアドレスを通知するようなケースや、CATV インターネット等 DHCP でアドレスを割り当てるプロバイダに契約している場合は、このモードで使用することがあります。加入している ADSL／CATV インターネットサービスに確認してください。

このモードの場合、DHCP サーバから「クライアント ID」もしくは「ホスト名」の指定を指示される場合があります。この場合は、コマンドのオプションとして指示された内容を設定してください。

設定例１　EWAN インタフェースで DHCP クライアント機能を使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address dhcp
```

コマンド書式

ip address dhcp { client-id [{ ascii | hex} <クライアント ID>] [[type <タイプ>] [hostname <ホスト名>]|[hostname <ホスト名>]]| hostname<ホスト名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
{ ascii | hex} クライアント ID	クライアント ID を ASCII または、hex で指定します。	ascii：最大 63 文字(ASCII) hex：最大 126 桁(16 進数)	クライアント ID を付けない
タイプ	クライアント ID のタイプを指定します。	0～255	クライアント ID が ASCII の場合：0 クライアント ID が hex の場合：1
ホスト名	ホスト名を指定します。	最大 63 文字	ホスト名を付けない

この設定を行わない場合

DHCP クライアント機能を使用できません。

DHCP クライアント機能とは？

DHCP プロトコルを利用して、IP アドレス等の情報を割り当ててもらい、その内容にしたがって IP 通信を行なう機能を、DHCP クライアント機能といいます。

FITELnet-F シリーズは、LAN インタフェースで DHCP サーバ機能または DHCP リレーエージェント機能が使用でき、EWAN インタフェースで DHCP クライアント機能を使用できます。

設定モード

EWAN インタフェース設定モード

ip dhcp-client dont-register-implicit-default-route

DHCP でアドレスを取得した際に、自動的にデフォルトルートの登録を行わないようにします。

設定例１　自動的にデフォルトルートの登録を行わないようにする

```
Router(config)#ip dhcp-client dont-register-implicit-default-route
Router(config)#
```

コマンド書式

ip dhcp-client dont-register-implicit-default-route

パラメータ

パラメータはありません。

この設定を行わない場合

DHCP でアドレスを取得した際に、自動的にデフォルトルートの登録を行います。

設定モード

基本設定モード

ip mtu

EWAN インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN の MTU 長を 1400byte にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	256～1500	省略不可

この設定を行わない場合

1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
標準的な Ethernet では、MTU 長は 1500byte です。

設定モード

EWAN インタフェース設定モード

ipv6 mtu

EWAN インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN の MTU 長を 1400byte にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	1280～1500	省略不可

この設定を行わない場合

1454byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
標準的な Ethernet では、MTU 長は 1500byte です。

設定モード

EWAN インタフェース設定モード

DHCPv6 クライアント機能

DHCPv6 クライアント機能を使用するための設定

address-pool enable【F100/F1000 コマンド】

本コマンドを設定することで、アドレスプールを有効にします。

設定例１　アドレスプールを有効にする

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)# address-pool enable
```

コマンド書式

address-pool enable

パラメータ

パラメータはありません。

この設定を行わない場合

アドレスプールは使用不可となります。

設定モード

IPv6 アドレスプール設定モード

address-pool ipv6【F100/F1000 コマンド】

IPv6 のアドレスプールを指定するために、IPv6 アドレスプール設定モードに移行します。
複数設定がある場合は、プール名で sort して、一番先頭のアドレスプールのみ有効になります。

設定例１　IPv6 アドレスプール設定モードに移行する

```
Router(config)#address-pool ipv6 1
Router(config-address-pool-ipv6)#
```

コマンド書式

address-pool ipv6 〈アドレスプール名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	アドレスプール名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

IPv6 アドレスプールの設定が行えません。

設定モード

基本設定モード

ipv6 address address-pool 【F100/F1000 コマンド】

アドレスプールから、/64 を切り出して、インタフェースのアドレスとして割り当てます。
アドレスプールに割り当て可能な/64 がない場合は、割り当てません(ログは出力しない)。
アドレスの割り当てが可能になったタイミングで、アドレスを割り当てます。
また、使用しているアドレスが使用禁止となった場合(例:DHCP クライアントの RENEW で異なるプレフィックスが割り当てられた等)は、アドレスを開放します。
RA により配布しているプレフィックスが使用禁止になった場合は、Valid/Preferred Lifetime を 0 とする RA を送信します。

設定例１　アドレスプール名（DHCPv6）からアドレスを割り当てる

```
Router(config)#interface lan1
Router(config-if lan1)# ipv6 address address-pool DHCPv6 prefix-length 64
```

コマンド書式

ipv6 address address-pool 〈アドレスプール名〉 prefix-length 〈プレフィックス長〉
[interface-id 〈インタフェース ID〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	/64 を切り出して割り当てるアドレスプール名を指定します。	16 文字以内の文字列	省略不可
プレフィックス長	プレフィックス長を指定します。	64	省略不可
インタフェース ID	割当先のインタフェースのアドレスを指定します。	IPv6 アドレス形式	省略不可

この設定を行わない場合

インタフェースのアドレスとして、アドレスプールを利用しません。

設定モード

LAN インタフェース設定モード
WAN インタフェース設定モード

ipv6 dhcp client【F100/F1000 コマンド】

DHCPv6 クライアント機能を指定した DHCPv6 クライアントプロファイル設定で動作させます。
DHCPv6 を動作させるインタフェースは、1 インタフェースのみになります。

設定例１　DHCPv6 クライアントプロファイル名称を DHCPv6_1 とする

```
Router(config)#interface lan1
Router(config-if lan1)# ipv6 dhcp client DHCPv6_1
```

コマンド書式

ipv6 dhcp client 〈プロファイル名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロファイル名	指定したインタフェースで DHCPv6 機能を動作させる場合の、クライアントプロファイル名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

指定しているインタフェースでは、DHCPv6 クライアントが動作しません。

設定モード

LAN インタフェース設定モード
WAN インタフェース設定モード

option-request prefix-delegation【F100/F1000 コマンド】

Prefix Delegation を要求する場合に指定します。
通知されたプレフィックスは、address-pool で指定する名称のプールに保管し、他目的(他 IF での DHCP サーバ機能等)に利用できることができます。
本コマンドが設定されている場合は、OPTION_IA_PD をつけて SOLICIT メッセージを送信します。

設定例１　通知されたプレフィックス値を保管する address-pool 名称を DHCPv6_1 とする

```
Router(config)#ipv6 dhcp client-profile dhcpv6
Router(config-ipv6-dhcp-client-prof)# option-request prefix-
delegation delegates address-pool DHCPv6_1 prefix-length 64
```

コマンド書式

option-request prefix-delegation delegates address-pool 〈アドレスプール名〉
prefix-length 〈プレフィックス値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスプール名	通知されたプレフィックス値を保管するアドレスプール名称を設定します。	16 文字以内の文字列	省略不可
プレフィックス値	プレフィックス値を指定します。	64	省略不可

この設定を行わない場合

Prefix Delegation を要求しませ。

設定モード

DHCPv6 クライアントプロファイル設定モード

IPv6 ルーティングの設定

IPv6 アドレス設定

ipv6 address

インタフェースの IPv6 アドレス(グローバル・リンクローカル)を指定します。
リンクローカルアドレスを指定しなかった場合は、EUI-64 形式のリンクローカルアドレスが自動で設定されます。
FITELnet-F シリーズでは、1つのインタフェースに4つのグローバルアドレスを指定することができます。

設定例１　プレフィックス：2002:1004::/64　EUI-64 形式で指定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 address 2002:1004::/64 eui-64
```

設定例２　リンクローカルアドレスを、fe80::1 に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 address fe80::1 link-local
```

コマンド書式

ipv6 address { <IPv6 アドレス> link-local | <IPv6 プレフィックス> [eui-64] }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	IPv6 リンクローカルアドレスを指定します。	IPv6 アドレス形式	省略不可
link-local	リンクローカルアドレスである場合に指定します。	link-local	省略不可
IPv6 プレフィックス	IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
eui-64	EUI-64 方式でグローバルアドレスを設定する場合に指定します。	eui-64	省略した場合はグローバルアドレスとして使用しません。 RA で広告するプレフィックスにのみ使用します。

最大エントリ数:30 エントリ(装置全体)

この設定を行わない場合

インタフェースに IPv6 アドレスが割り当てられません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
ループバックインタフェース設定モード

ipv6 address autoconfig

インタフェースで Stateless Address Autoconfiguration を使用し、IPv6 アドレスを自動設定します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例１　RA を受信するインタフェースを EWAN1 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 address autoconfig
```

コマンド書式

ipv6 address autoconfig [interface-id <インタフェース ID>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース ID	Stateless Address Autoconfiguration において使用するインタフェース ID を指定します。	64 ビット /xxxx:xxxx:xxxx:xxxx 型式	EUI-64 型式

この設定を行わない場合

Stateless Address Autoconfiguration によるアドレス自動割り当てを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 enable

インタフェースにグローバルアドレスを割り当てず(ipv6 address コマンドを使用しない)、リンクローカルアドレスのみで IPv6 通信を行なう(同一リンク内のみの通信)場合に指定します。

設定例１　LAN インタフェースを、リンクローカルアドレスのみで使用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 enable
```

コマンド書式

ipv6 enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 address コマンドで、IPv6 アドレスを明示的に設定しない場合、リンクローカルアドレスが割り当てられません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ICMPv6 に関する設定

ipv6 icmp error-ratelimit

本装置が、ICMP を使ってエラーを送信する際の、1 秒間に送信する最大送信パケット数を設定します。1 秒間に送信するパケット数が規定数を超過した場合に、次の 1 秒まで送信を抑止します。
0 を指定した場合、ICMP エラーメッセージおよび REDIRECT メッセージは送信されません。
エラーパケットにより、データ通信のための帯域が減ってしまうのを防ぐ機能です。

refresh コマンド後に有効になるコマンドです。

設定例１　エラーパケットを、最大 300 パケット/秒とする

```
Router(config)#ipv6 icmp error-ratelimit 300
```

コマンド書式

ipv6 icmp error-ratelimit {パケット数/秒 | unlimit}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケット数/秒	IPv6 ICMP でエラーを送信する際の 1 秒間に送信する最大送信パケット数	0～2147483647	省略不可
unlimit	ICMP エラーメッセージおよび REDIRECT メッセージのレート制限を行いません。	unlimit	省略不可

この設定を行わない場合

100 パケット/秒が設定されます。

IPv6 での ICMP エラーパケットの種類

IPv6 での ICMP エラーパケットには、以下の種類があります。

Type	内容
1	受信したパケットの宛先への中継ができない
2	パケット長が MTU 長より大きいため、転送できない
3	ホップ数が制限を越えたため、転送できない
4	IPv6 ヘッダ（拡張ヘッダを含む）が異常、もしくは未知
137	中継先を別のルータに変更したことを通知

設定モード

基本設定モード

ipv6 hop-limit

Hop limit とは、そのパケットが到達可能なホップ数です。例えば、Hop limit に"100"が設定されているパケットは、送信元のノードから、100Hop の宛先までは到達できますが、それより先のネットワークには到達できないことを意味します。

本装置では、自身から送信する IPv6 パケットの Hop limit 値、および本装置が RA を送信する場合に、RA の"current hop limit"に入れる値を設定できます。RA を受信したノードは、"current hop limit"の値を、送信する IPv6 パケットの、IPv6 ヘッダ中にある Hop limit に入れます。

設定例１　RA の current hop limit 値を、100 とする

```
Router(config)#ipv6 hop-limit 100
```

コマンド書式

ipv6 hop-limit <最大ホップ数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大ホップ数	自身または RA で通知する hop-limit 値を設定します。	1～255	省略不可

この設定を行わない場合

本装置自身が送信するパケットの Hop limit 値は 64、RA で送信する current hop limit は 0（ルータは規定しない）となります。

設定モード

基本設定モード

ipv6 hoplimit-receive-enable

受信した RA で指定されている CurHopLimit 値を有効とする場合に指定します。
有効とした場合、受信した RA に規定されている CurHopLimit 値をホップリミット値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例１　EWAN1 インタフェースから受信した RA に規定されている CurHopLimit 値をホップリミット値とする

```
Router(config)#interface ewan 1
Router(config)# ipv6 hoplimit-receive-enable
```

コマンド書式

ipv6 hoplimit-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 hop-limit コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd receive-ra

本コマンドを指定することにより、RA を受信するインタフェースとします。
同じインタフェースで、ipv6 nd send-ra が設定されている場合はログを出力し、RA の送信／受信の動作を行ないません。

設定例１　RA を受信するインタフェースを EWAN1 とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 nd receive-ra
```

コマンド書式

ipv6 nd receive-ra

パラメータ

パラメータはありません。

この設定を行わない場合

RA を受信しても無視します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd rs-delay

インタフェースが UP して最初の RS 送信までの遅延時間と次回以降の送信間隔を設定します。
ipv6 nd rs-times コマンドで指定した回数まで、設定した送信間隔で RS を送信します。
本コマンドは、ipv6 nd receive-ra コマンドが設定されている場合のみ有効となります。

設定例 1　最初に RS を送信するまでの遅延時間を 5 秒、その後 30 秒おきに送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd rs-delay 5 30
```

コマンド書式

ipv6 nd rs-delay <RS 初回送信遅延時間> <RS 送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RS 初回送信遅延時間	インタフェースが UP して最初の RS 送信までの遅延時間(単位:秒)を指定します。	0～3600	省略不可
RS 送信間隔	初回送信以降の RS 送信間隔(単位:秒)を指定します。	4～3600	省略不可

この設定を行わない場合

最初に RS を送信するまでの遅延時間 0 秒、次回以降は 4 秒おきに送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd rs-times

RS 送信開始後、RA が受信出来ない場合の RS 送信回数を指定します。
ipv6 nd rs-delay コマンドで指定した間隔で、指定した送信回数分 RS を送信します。
本コマンドは、ipv6 nd receive-ra コマンドが設定されている場合のみ有効となります。

設定例１　RS の送信回数を 10 回にとする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd rs-times 10
```

コマンド書式

ipv6 nd rs-times <RS 送信回数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RS 送信回数	RS 送信開始後、RA が受信出来ない場合の RS 送信回数を指定します。	0※～65535	省略不可

※:RS 送信回数を 0 秒に設定した場合は、RA が受信できるまで RS を送信し続けます。

この設定を行わない場合

RS の送信回数は 3 回になります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd send-ra

本装置から RA を送信するかどうかを設定します。
ipv6 nd prefix-advertisement の設定がある場合は、指定されたプレフィックス情報を通知します。
ipv6 nd prefix-advertisement の設定がない場合は、ipv6 address コマンドで設定したインタフェースに割り当てられるプレフィックスを通知します。

設定例１　RA を送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd send-ra
```

コマンド書式

ipv6 nd send-ra

パラメータ

パラメータはありません。

この設定を行わない場合

RA を送信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd ra-interval

本装置から RA を定期送信する際の、送信間隔(単位:秒)を設定します。

設定例 1　RA を 30 秒おきに送信する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ra-interval 30
```

コマンド書式

ipv6 nd ra-interval <RA の送信間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RA の送信間隔	RA を定期送信する際の送信間隔(単位:秒)	3～1800	省略不可

この設定を行わない場合

200 秒間隔で RA を送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd ra-lifetime

本装置が送信する RA のルータライフタイム値を設定します。lifetime 値は、RA を受信したノードが、RA の送信元ルータをデフォルトルータとして使用できる時間(秒)です。

設定例１　RA の lifetime を 3000 秒とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ra-lifetime 3000
```

コマンド書式

ipv6 nd ra-lifetime 〈ルータライフタイム値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータライフタイム値	RA で公開するルータライフタイム値(単位:秒)	0～9000	省略不可

この設定を行わない場合

1800 秒となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd ns-interval

本装置が、RA を送信する際に、Retrans Timer 値として通知する値を設定します。
この RA を受信したノードは、NS(Neighbor Solicitation)を再送する際、ここで指定した値(単位:m 秒)間隔で送信します。
また、本装置が NS を再送する際も、この値を使用します。

設定例 1　NS の再送間隔を 10 秒（10000m 秒）とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd ns-interval 10000
```

コマンド書式

ipv6 nd ns-interval <RA で通知する NS の再送間隔>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RA で通知する NS の再送間隔	RA で通知する NS の再送間隔および、本装置が再送信する際の送信間隔(単位:m 秒)	1000～3600000	省略不可

この設定を行わない場合

RA では 0(未指定)を通知し、FITELnet-F シリーズは 1 秒(1000m 秒)で動作します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd managed-config-flag

本装置から RA(Router Advertisement)を送信する際に、M フラグを"1"とするかどうかを設定します。このコマンドを指定した場合は、M フラグを"1"として RA を送信します。
M フラグが"1"になっている RA を受信したノードは、Stateless Auto Configuration ではなく、DHCPv6 などのアドレス自動設定(Stateful Auto Configuration)を行なう必要があります。

設定例１　M フラグをつける

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd managed-config-flag
```

コマンド書式

ipv6 nd managed-config-flag

パラメータ

パラメータはありません。

この設定を行わない場合

M フラグを"0"として RA を送信しています。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd other-config-flag

本装置から RA(Router Advertisement)を送信する際に、O フラグを"1"とするかどうかを設定します。このコマンドを指定した場合は、O フラグを"1"として RA を送信します。
O フラグが"1"になっている RA を受信したノードは、アドレス以外の情報を自動設定するために、ステートフルなプロトコルを使用する必要があります。

設定例１　O フラグをつける

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd other-config-flag
```

コマンド書式

ipv6 nd other-config-flag

パラメータ

パラメータはありません。

この設定を行わない場合

O フラグを"0"として RA を送信しています。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd prefix-advertisement

RA で通知するプレフィックスを設定します。この設定がない場合は、LAN インタフェースに割り当てられたプレフィックスを通知します。

このコマンドで通知するプレフィックスを指定する場合は、プレフィックス値のほかに、「Valid Lifetime」「Prefferd Lifetime」「onlink フラグ」「Autoconfig フラグ」も指定します。

Valid Lifetime	このプレフィックスをノードが使用する場合に、使用可能な時間(秒)
Prefferd Lifetime	このプレフィックスをノードが使用する場合に、正当な使用が問題ない時間(秒)
onlink フラグ	同一リンク上に存在することを表すフラグ
Autoconfig フラグ	このプレフィックスをノードが受信した場合に、Stateless Auto Configuration でアドレスを使用してよいかどうかを表すフラグ

設定例 1　RA で通知するプレフィックスを"2003:114::/64"に設定（Valid Lifetime:500 秒、Prefferd Lifetime:400 秒、Autoconfig フラグあり）する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd prefix-advertisement
2003:114::/64 500 400 autoconfig
```

コマンド書式

ipv6 nd prefix-advertisement <IPv6 プレフィックス> <Valid Lifetime> <Prefferd Lifetime> [onlink] [autoconfig]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 プレフィックス	RA で通知する IPv6 プレフィックスを設定します。	IPv6 プレフィックス形式	省略不可
Valid Lifetime	Valid Lifetime 値(単位:秒)を設定します。	0～4294967295	省略不可
Prefferd Lifetime	Prefferd Lifetime 値(単位:秒)を設定します。	0～4294967295	省略不可
onlink	Onlink フラグを立てる場合に指定します。	onlink	Onlink フラグを立てない
autoconfig	Autoconfig フラグを立てる場合に指定します。	autoconfig	Autoconfig フラグを立てない

この設定を行わない場合

ipv6 address コマンドで指定したプレフィックス値を RA で通知します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 nd reachable-time

本装置が送信する RA の reachable time 値を設定します。

設定例１　reachable time 値を 15000 に設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 nd reachable-time 15000
```

コマンド書式

ipv6 nd reachable-time <Reachable Time 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Reachable Time 値	Reachable Time 値を指定します(単位:m 秒)	0-3600000	省略不可

この設定を行わない場合

30000m 秒となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 ns-interval-receive-enable

受信した RA で指定されている RetransTimer 値を有効とする場合に指定します。
受信した RA で規定されている RetransTimer 値と、インタフェースに設定されている RetransTimer 値(ipv6 nd ns-interval コマンド)を比較し、小さい値をインタフェースの RetransTimer 値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例１　EWAN1 インタフェースで受信した RA で指定されている RetransTimer 値を有効とする

```
Router(config)#interface ewan 1
Router(config)# ipv6 reachable-time-receive-enable
```

コマンド書式

ipv6 ns-interval-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 nd ns-interval コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ipv6 reachable-time-receive-enable

受信した RA で指定されている Reachable Time 値を有効とする場合に指定します。
受信した RA で規定されている ReachableTime 値と、インタフェースに設定されている ReachableTime 値(ipv6 nd reachable-time コマンド)を比較し、小さい値をインタフェースの BaseReachableTime 値として使用します。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

設定例１　EWAN1 インタフェースで受信した RA で指定されている Reachable Time 値を有効とする

```
Router(config)#interface ewan 1
Router(config)# ipv6 reachable-time-receive-enable
```

コマンド書式

ipv6 reachable-time-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 nd reachable-time コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

RIPng

ipv6 prefix-list

IPv6 のプレフィックスリスト情報を設定します。
プレフィックスリストは、RIPng で広告する／広告しないプレフィックスを制御するために使用します。
本コマンドで、プレフィックス値、許可するかどうかを指定し、RIPng サービス設定モードの、distribute-list コマンドで、広告する／受け入れるプレフィックスを指定するために、本コマンドで設定したプレフィックスリスト番号を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:100::/64 を許可するプレフィックスリスト（リスト番号１）を作成する

```
Router(config)#ipv6 prefix-list 1 permit 3ffe:100::/64
```

コマンド書式

ipv6 prefix-list <リスト番号> <permit | deny > <IPv6 プレフィックス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リスト番号	プレフィックスリスト番号	1～99	省略不可
permit｜deny	許可する場合は permit、許可しない場合は deny を指定します。	permit deny	省略不可
IPv6 プレフィックス	対象となる IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

全ての IPv6 経路情報を RIPng で送受信します。

設定モード

基本設定モード

router ripng

RIPng サービス設定モードへ移行します。RIPng の各種設定を行ないます。

設定例１　RIPng サービス設定モードに移行する

```
Router(config)# router ripng
Router(config-ripng)#
```

コマンド書式

```
router ripng
```

パラメータ

パラメータはありません。

この設定を行わない場合

RIPng を使用できません。

設定モード

基本設定モード

network

RIPng サービスを提供するインタフェースをインタフェース名もしくは IPv6 アドレス形式で決定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースで RIPng を運用する

```
Router(config)#router ripng
Router(config-ripng)# network lan 1
```

コマンド書式

network ｛〈インタフェース名〉｜〈IPv6 アドレス〉｝

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	RIPng を運用するインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 vlanif 1～16	省略不可
IPv6 アドレス	RIPng を運用するインタフェースを、インタフェースの IPv6 アドレスで指定します。	IPv6 アドレス形式	

※1:F80 の場合は、1～5 になります。
※2:F100 のみ指定可能です。

この設定を行わない場合

全てのインタフェースで RIPng を運用しません。

設定モード

RIPng サービス設定モード

distribute-list

RIPng 送受信に対してフィルタリングの設定を行ないます。
ipv6 prefix-list コマンドで指定したプレフィックスの情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。
また、フィルタリング制御を行なうためのインタフェースを指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:101:220::/64 のプレフィックス情報のみを受け付ける

```
Router(config)#prefix-list 1 permit 3ffe:101:220::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 in
```

設定例２　3ffe:101:220::/64 のプレフィックス情報のみを送信しない

```
Router(config)#prefix-list 1 deny 3ffe:101:220::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 out
```

設定例３　3ffe:101:220::/64 のプレフィックス情報を、LAN からは受信しない

```
Router(config)#prefix-list 1 deny 3ffe:101:220::/64

Router(config)#router ripng
Router(config-ripng)# distribute-list prefix 1 in lan 1
```

コマンド書式

distribute-list prefix <prefix 番号> { in | out } [インタフェース名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
prefix 番号	prefix-list コマンドで指定したリスト番号を指定します。	1～99	省略不可
in | out	受信(in)／送信(out)のどちらでフィルタするかを指定します。	in out	省略不可
インタフェース名	適用するインタフェースのインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 vlanif 1～16	全インタフェースで適用

※1:F80 の場合は、1～5 になります。
※2:F100 のみ指定可能です。

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

RIPng サービス設定モード

redistribute

RIPng 以外の手段で取得した経路情報のうち、RIPng で再配布する手段を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を RIPng で再配布する

```
Router(config)#router ripng
Router(config-ripng)#redistribute static
```

設定例２　直接ルートの経路情報を RIPng で再配布する

```
Router(config)#router ripng
Router(config-ripng)#redistribute connected
```

コマンド書式

redistribute〈再配布する経路情報〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再配布する経路情報	RIPng 以外の手段で取得した経路情報のうち、RIPng で配布するものを指定します。 connected：直接経路 kernel：kernel にセットされた経路情報 static：スタティックルーティング情報	connected kernel static	省略不可

この設定を行わない場合

RIPng で受信した情報のみを広告します。

設定モード

RIPng サービス設定モード

default-information originate

自身をデフォルトルートとして、RIPng で通知するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　デフォルトルートの情報を RIP で送信する

```
Router(config)#router ripng
Router(config-ripng)#default-information originate
```

コマンド書式

default-information originate

パラメータ

パラメータはありません。

この設定を行わない場合

自身をデフォルトルートとしては通知しません。

注意

この設定は、デフォルトルートの情報を持っていないときに、RIPng でデフォルトルートを通知するかどうかの設定です。
スタティック設定でデフォルトルートを設定していたり、ルーティングプロトコルによりデフォルトルートを学習していた場合は、この設定によらずデフォルトルートの情報を RIPng で広告します。

設定モード

RIPng サービス設定モード

timers basic

RIPng に関する以下のタイマ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　定期送信間隔を 20 秒、経路情報を無効とするまでの時間を 120 秒、経路情報を RIP テーブルから削除するまでの時間を 80 秒とする

```
Router(config)#router ripng
Router(config-ripng)#timers basic 20 120 80
```

コマンド書式

timers basic 〈定期送信間隔〉〈経路情報を無効とするまでの時間〉
〈経路情報を削除するまでの時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
定期送信間隔	RIP の定期送信間隔(単位:秒)を指定します。	5～2147483647	省略不可
経路情報を無効とするまでの時間	RIP のレスポンスを受信しなくなってから、経路情報を無効とするまでの時間(単位:秒)を指定します。 指定した時間内にレスポンスを受信しないと該当経路情報は無効となり、ルーティングテーブルからは削除されます。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を無効として、RIP テーブルから削除するまでの時間(単位:秒)を指定します。 この状態では、RIP テーブルにメトリック 16 で保持されて経路が無効になった事を広告します。	5～2147483647	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
定期送信間隔	30
経路情報を無効とするまでの時間	180
経路情報を削除するまでの時間	120

設定モード

RIPng サービス設定モード

route

RIPng エントリをマニュアルで登録します。
ここで設定した経路情報は、RIPng で広告するためだけに使用されます。装置のスタティックルートとしては登録されませんので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:11::/64 の経路情報を RIPng で広告する

```
Router(config)#router ripng
Router(config-ripng)#route 3ffe:11::/64
```

コマンド書式

route <RIPng で広告する Prefix>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RIPng で広告する Prefix	RIPng で広告するプレフィックスを設定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

スタティック情報はありません。
redistribute コマンドの指定および学習した RIPng 情報のみを、RIPng で広告します。

設定モード

RIPng サービス設定モード

aggregate-address

経路情報を集約し、その情報を RIPng で通知します。通知する際は、集約後の経路情報のみを通知し、集約された元の情報は通知されません。
この機能により、RIPng で通知するプレフィックスの数を減らすことができ、ネットワークを有効に利用することができるようになります。
例えば、以下のようなケースで有効です。

EWAN 側に、3ffe:1::/64 ネットワーク、3ffe:2::/64 ネットワーク、3ffe:3::/64 ネットワーク・・・・等、1 バイト目が 3ffe であるネットワークが数多く存在する。
↓↓↓
3ffe::/8 として、LAN 側に RIPng で通知

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:100::/32 に集約して RIPng を通知します。

```
Router(config)#router ripng
Router(config-ripng)# aggregate-address 3ffe:100::/32
```

コマンド書式

aggregate-address〈集約後の IPv6 プレフィックス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
集約後の IPv6 プレフィックス	集約後の IPv6 プレフィックスを設定します。	IPv6 プレフィックス形式	省略不可

この設定を行わない場合

Aggregate しません。

設定モード

RIPng サービス設定モード

フィルタリングの設定

access-list

特定のパケットと、そのパケットの動作（中継 or 廃棄 or 学習フィルタリング）を指定します。refresh コマンド後に有効になるコマンドです。

指定したパケットは、以下の機能で使用します。

・フィルタリング（ip access-group コマンド）
・学習フィルタリング（ip access-group コマンド）
・オフセットリスト（offset-list コマンド）
・RIP/BGP で送信するメトリック値の指定（distance コマンド）
・BGP で送信する経路の指定（neighbor <IP-address> distribute-list コマンド）
・経路情報の指定（match ip address コマンド）
・NextHop の指定（match ip nexthop コマンド）
・NAT 変換前のアドレス指定（ip nat inside コマンド）
・　使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、指定したアクセスリスト番号を指定します。

refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。

この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク（Wildcard マスク）を使用して 1 エントリでアドレス範囲を指定することができます。

Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。

例）24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
　Wildcard マスクの場合：0.0.0.255
　サブネットマスクの場合：255.255.255.0

例2）ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
　Wildcard マスクの場合：0.0.0.0
　サブネットマスクの場合：255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング／学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。
本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例１　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する（許可属性）

```
Router(config)# access-list 1 permit
192.168.100.0 0.0.0.255
```

設定例２　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する（不許可属性）

```
Router(config)# access-list 100 deny ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

設定例３　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する（許可属性）

```
Router(config)# access-list 3000 permit
3ffe:110::/64 3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt
0 any eq 80
```

設定例５　学習フィルタリングを指定する（IPv4）

```
Router(config)# access-list 100 dynamic permit ip
any any
```

コマンド書式

IPv4 標準アクセスリスト（アクセスリスト番号：1～99、1300～1999）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（アクセスリスト番号：100～199、2000～2699）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence {<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（アクセスリスト番号：3000～3499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（アクセスリスト番号：3500～3999）access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> } [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>access-list 番号</td><td>それぞれの属性の番号を指定します。</td><td><table><tr><td>1～99、1300～1999</td><td>IPv4 標準アクセスリスト</td></tr><tr><td>100～199、2000～2699</td><td>IPv4 拡張アクセスリスト</td></tr><tr><td>3000～3499</td><td>IPv6 標準アクセスリスト</td></tr><tr><td>3500～3999</td><td>IPv6 拡張アクセスリスト</td></tr></table></td><td>省略不可</td></tr>
<tr><td>dynamic</td><td>学習フィルタリングを使用する場合に指定します。</td><td>dynamic</td><td>学習フィルタリングのエントリではない</td></tr>
<tr><td>{ permit | deny }</td><td>許可属性か、不許可属性かを選択します。</td><td><table><tr><td>permit</td><td>許可属性</td></tr><tr><td>deny</td><td>不許可属性</td></tr></table></td><td>省略不可</td></tr>
</table>

<table>
<tr><td>プロトコル番号</td><td>プロトコル名もしくはプロトコル番号を選択します。</td><td><table><tr><td>gre</td><td>Cisco’s GRE tunneling</td></tr><tr><td>icmp</td><td>ICMP（IPv4 拡張アクセスリスト時）</td></tr><tr><td>icmpv6</td><td>ICMPv6（IPv6 拡張アクセスリスト時）</td></tr><tr><td>ip</td><td>IP</td></tr><tr><td>ipinip</td><td>IP トンネル</td></tr><tr><td>tcp</td><td>TCP</td></tr><tr><td>udp</td><td>UDP</td></tr><tr><td>0～255</td><td>プロトコル番号を指定</td></tr></table></td><td>省略不可</td></tr>
<tr><td>any</td><td>各パラメータ（アドレスやポート番号など）で、「全て」を指定する場合は"any"を入力します。</td><td>any</td><td>–</td></tr>
<tr><td>送信元 IP アドレス</td><td>送信元アドレスを指定します。</td><td>IPv4 アドレス形式</td><td>省略不可</td></tr>
<tr><td>送信元 Wildcard マスク</td><td>送信元アドレスを範囲指定するために、Wildcard マスクを指定します。</td><td>IPv4 アドレス形式</td><td>省略不可</td></tr>
<tr><td>宛先 IP アドレス</td><td>宛先アドレスを指定します。</td><td>IPv4 アドレス形式</td><td>省略不可</td></tr>
<tr><td>宛先 Wildcard マスク</td><td>宛先アドレスを範囲指定するために、Wildcard マスクを指定します。</td><td>IPv4 アドレス形式</td><td>省略不可</td></tr>
<tr><td>host</td><td>IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。</td><td>host</td><td>–</td></tr>
<tr><td>送信元 IPv6 プレフィックス</td><td>送信元 IPv6 プレフィックスを指定します。</td><td>IPv6 プレフィックス形式</td><td>省略不可</td></tr>
<tr><td>宛先 IPv6 プレフィックス</td><td>宛先 IPv6 プレフィックスを指定します。</td><td>IPv6 プレフィックス形式</td><td>省略不可</td></tr>
<tr><td>ICMP タイプ</td><td>プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。</td><td><table><tr><td>指定できる ICMP タイプ</td></tr><tr><td>administratively-prohibited</td></tr><tr><td>alternate-address</td></tr><tr><td>conversion-error</td></tr><tr><td>dod-host-prohibited</td></tr><tr><td>dod-net-prohibited</td></tr><tr><td>echo</td></tr></table></td><td>全ての ICMP タイプ</td></tr>
</table>

		echo-reply	
		general-parameter-problem	
		host-isolated	
		host-precedence-unreachable	
		host-redirect	
		host-tos-redirect	
		host-tos-unreachable	
		host-unknown	
		host-unreachable	
		information-reply	
		information-request	
		mask-reply	
		mask-request	
		mobile-redirect	
		net-redirect	
		net-tos-redirect	
		net-tos-unreachable	
		net-unreachable	
		network-unknown	
		no-room-for-option	
		option-missing	
		packet-too-big	
		parameter-problem	
		port-unreachable	
		precedence-unreachable	
		protocol-unreachable	
		reassembly-timeout	
		redirect	
		router-advertisement	
		router-solicitation	
		source-quench	
		source-route-failed	
		time-exceeded	
		timestamp-reply	
		timestamp-request	

		traceroute ttl-exceeded unreachable ICMP タイプ値(0～255)	
ICMPv6 タイプ(IPv6)	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	ICMPv6 タイプ address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値(0～255)	全ての ICMPv6 タイプ
ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。	eq 指定するポートが対象 gt 指定するポート番号より大きいポート	全てのポート(以降設定なし)

			番号が対象	
		lt	指定するポート番号より小さいポート番号が対象	
		neq	指定するポート番号以外のポート番号が対象	
		range	ポートの範囲を指定する	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号 bgp chargen cmd daytime discard domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog tacacs tacacs-ds		全ての TCP ポート番号

		talk telnet time uucp whois www TCP ポート番号(0～65535)	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号 biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk tftp time who xdmcp UDP ポート番号(0～	全ての UDP ポート番号

		65535)	
precedence-value	precedence-value を設定します。	0～7	省略不可
precedence-named-value	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) etwork(7)	省略不可
tos-value	tos-value を設定します。	0～15	省略不可
tos-named-value	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value	dscp-value を設定します。	0～63	省略不可
dscp-named-value	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b) af43(100110b)	省略不可
ip-flag-value	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3(ワイルドカードマスク)	省略不可
tcp-flag-value	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63(ワイルドカードマス	省略不可

		ク)	
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255(ワイルドカードマスク)	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

最大エントリ数:ip access-group で関連付けた access-list に対して、最大 1024 エントリ装置全体で 1024 エントリ
ipv4, ipv6 の区別無く、装置全体で最大 1024 エントリ
各インターフェース毎の制限無く、装置全体で最大 1024 エントリ

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

ipv6 access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、LAN 送信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 access-group 1 out
```

設定例２　access-list 2 で指定したデータを、LAN からの受信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	<3000-3499> <3500-3999>	省略不可
{in | out}	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in：受信時 out：送信時	省略不可

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

PPPoE インタフェース設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
トンネルインタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。

設定例　学習フィルタリングテーブルを 16384 セッション分設定する

```
Router(config)#ip stateful max-sessions 16384
```

コマンド書式

ip stateful max-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～16384	省略不可

この設定を行わない場合

学習フィルタリングテーブルの最大数は、2048 になります。

設定モード

基本設定モード

スタティックルーティングの設定

ipv6 route

本装置の、IPv6 スタティックルートを指定します。
PPPoE や EWAN 使用する場合は、Nexthop の IP アドレスが分からないケースがありますので、Nexthop としてインタフェースを指定することもできます。
Nexthop に IPv6 アドレス(インタフェースではない)を指定した場合は、その宛先へのメトリック値を指定することができます。
デフォルトルートを指定する場合、宛先には”::0/0 ”を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　3ffe:2::/64 宛の Nexthop を 3ffe:3::1 とする場合（メトリックは指定しない）

```
Router(config)#ipv6 route 3ffe:2::/64 3ffe:3::1
```

設定例２　3ffe:2::/64 宛の Nexthop を、PPPoE1 インタフェースとする場合

```
Router(config)#ipv6 route 3ffe:2::/64 pppoe 1
```

設定例３　デフォルトルートを PPPoE１インタフェースとする場合

```
Router(config)#ipv6 route ::0/0 pppoe 1
```

設定例４　RA を送信するルータを nexthop に指定する場合

```
Router(config)#ipv6 route 0::/0 fe80:3::1 ewan 1
```

RA を送信するルータが複数存在した場合、それらを「RA 送信ルータリスト」として登録します。
RA 送信ルータリストとは、インタフェースあたり3件まで登録することができます。

コマンド書式

```
ipv6 route <宛先プレフィックス> { <NextHop> [<インタフェース名>] lan | ewan |
          pppoe | [distance] }
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先ネットワーク	スタティックルーティングの宛先 IPv6 プレフィックス	IPv4 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IPv6 アドレス	IPv6 アドレス形式	インタフェース名を設定する必要があります。
インタフェース名	NextHop に指定した場合に、その GW がどのインタフェースに存在するかの指定となります。	lan 1 ewan 1～2 pppoe 1～24※1 tunnel 1～32	NextHop の IPv6 アドレスを設定する必要があります。
lan	宛先へ到達するためのインタフェースとして指定します。 PPPoE のように、NextHop の IP アドレスが明確にわからない場合や、複数 RA を送信するルータが存在する場合に指定します。	lan 1	省略不可
ewan		ewan 1～2	
pppoe		pppoe 1～24※1	
distance	スタティックルーティングの distance 値を指定します。	2～255※2	1

最大エントリ数
F80/F100：256 エントリ（ルーティングテーブル自体は 512 エントリ）
F1000：1024 エントリ（ルーティングテーブル自体は 2048 エントリ）
※1：F80 の場合は、1～5
※2：distance 値に 255 を設定した場合、その経路情報は無効扱いとなります。

この設定を行わない場合

スタティックルーティングは設定されません。

設定モード

基本設定モード

MTU長の設定

ipv6 mtu

インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN の MTU 長を 1400byte にする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 mtu 1400
```

コマンド書式

ipv6 mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	lan 1280～1500 pppoe 1280～1492 ewan 1280～1500 tunnel 1280～1500	省略不可

この設定を行わない場合

各インタフェースにより以下のようになります。通常は変更の必要はありません。

LAN:1500
PPPoE:1454
EWAN:1454
Tunnel:1460

MTU 長とは？

MTU とは(Max Transfer Unit)の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット(IP ヘッダ＋IP ペイロード)の長さをいいます。

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
トンネルインタフェース設定モード

ipv6 mtu-receive-enable

設定しているインタフェースで、受信した RA の MTU オプションで指定されている MTU 値を有効とする場合に指定します。
有効とした場合、受信した MTU 長と、設定された MTU 長を比較し、小さい値を実際のインタフェースの MTU 長とします。
本設定を行う場合は、ipv6 nd receive-ra コマンドの設定が必要です。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 インタフェースで、受信した RA の MTU オプションで指定されている MTU 値を有効とする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ipv6 mtu-receive-enable
```

コマンド書式

ipv6 mtu-receive-enable

パラメータ

パラメータはありません。

この設定を行わない場合

ipv6 mtu コマンドの設定に従います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード

ポリシールーティング

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ設定モードへ移行します。

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 100 番もしくは 101 番にマッチするトラフィックを対象とする

```
Router(config)# class-map video-class
Router(class-map video-class)# match-any
Router(class-map video-class)# match ip access-group 100
Router(class-map video-class)# match ip access-group 101
Router(class-map video-class)# exit
```

コマンド書式

match-any

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で match-any を指定しなかった場合は以下のようになります。

```
Router(config)# class-map video-class
Router(class-map video-class)# match ip access-group 100
Router(class-map video-class)# match ip access-group 101
Router(class-map video-class)# exit
```

この場合、IP アクセスリストの 100 番にマッチ、かつ 101 番にマッチするトラフィックを対象とします。

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199、2000～2699	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan:1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16 tunnel 1～32	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
複数の match が定義された場合、定義された順に評価されます。同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。

refresh コマンド後に有効になるコマンドです。

設定例１　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

match ip input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]
match ipv6 input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

set ipv6 next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6}next-hop default が指定されている場合には、通常のルーティングが行なわれます。指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　パケット中継先を 2002:1004::1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 next-hop 2002:1004::1 distance 10
```

コマンド書式

```
set ipv6 next-hop <IP アドレス> [インタフェース※1][distance (1-255)]
set ipv6 next-hop <インタフェース※2> [distance (1-255)]
set ipv6 next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv6 アドレス形式	省略不可
インタフェース※1	NextHop にリンクローカルアドレスを設定した場合は、インタフェースの指定が必要です。	lan 1 ewan 1～2 pppoe 1～24※3	―
インタフェース※2	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	pppoe 1～24※3 tunnel 1～32	省略不可
distance	中継先の distance 値を設定します。	1～255	1
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

※3:F80 の場合は、1～5 になります。

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、クラスマップ名のアルファベット順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます(同一クラスマップ名に対しては、置換型となります)。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)# policy-map stream-service
Router(config-policy-map)# class video-class action stream-action
Router(config-policy-map)# class audio-class action stream-action
Router(config-policy-map)# exit
```

コマンド書式

class <class-map-name> action <action-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
class-map-name	class-map-name を設定します。	16 文字以内の文字列	省略不可
action-map-name	action-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。
ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。
また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

refresh コマンド後に有効になるコマンドです。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map <policy-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
policy-map-name	policy-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

```
statistics update {enable|disable}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
enable｜disable	統計情報のカウントを enable（有効）または、disable（無効）かを指定します。	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシールーティング時の NextHop 監視

ipv6 polling-interval

ポリシールーティング時に有効な中継先かどうかを判断するために、指定された中継先に対して監視パケットを送信する際の Ipv6 監視パケット(Neighbor Solicit)の送信間隔を指定します。

ARP またはネイバのキャシュテーブルの参照を行い、IPv6 では状態 ND6_LLINFO_REACHABLE ND6_LLINFO_STALE、ND6_LLINFO_DELAY、及び ND6_LLINFO_PROBE である場合に有効であると判定されます。

それ以外は、有効でないと判定されます。

有効である場合、ポリシールーティング機能では、指定された中継先への到達性があると判定し、その中継先を有効な経路と認識します。有効でない場合は、set ip next hop コマンドで設定された次の候補の判定を行います。

定変更後のリフレッシュでは変更前の監視パケット送信後、変更された指定が有効となります。

refresh コマンド後に有効になるコマンドです。

設定例 1　監視パケットの送信間隔を 10 秒にする

```
Router(config)#ipv6 polling-interval 10
```

コマンド書式

ipv6 polling-interval < 監視パケット送信間隔 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視パケット送信間隔	Ipv6 監視パケット(Neighbor Solicit)の送信間隔を指定します。	5～60	送信間隔を 5 秒に設定します。

この設定を行わない場合

監視パケットの送信間隔が 5 秒に設定されます。

設定モード

基本設定モード

IPv4 ルーティングの設定

IPアドレスの設定

ip address

インタフェースの IP アドレス、サブネットマスクを設定します。

設定例１　PPPoE１の IP アドレスを 192.168.0.１に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 192.168.0.1
```

設定例２　EWAN１の IP アドレスを 192.168.0.１、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address 192.168.0.1 255.255.255.0
```

コマンド書式

ip address〈IP アドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	インタフェースに割り当てるサブネットマスク※を設定します。	IPv4 アドレス形式	省略不可

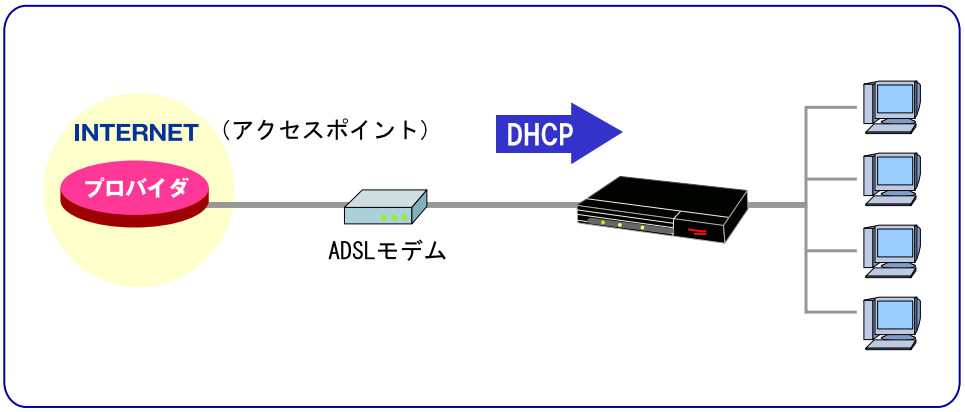
※PPPoE およびループバックインタフェースでは、サブネットマスクの指定はできません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード
トンネルインタフェース設定モード

ip address dhcp

EWAN インタフェースで、DHCP クライアント機能を使用する場合に指定します。
ADSL モデムで PPP を終端し EWAN 側に DHCP でアドレスを通知するようなケースや、CATV インターネット等 DHCP でアドレスを割り当てるプロバイダに契約している場合は、このモードで使用することがあります。加入している ADSL／CATV インターネットサービスに確認してください。



このモードの場合、DHCP サーバから「クライアント ID」もしくは「ホスト名」の指定を指示される場合があります。この場合は、コマンドのオプションとして指示された内容を設定してください。

設定例１　EWAN インタフェースで DHCP クライアント機能を使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address dhcp
```

コマンド書式

ip address dhcp client-id [[{ ascii | hex} < クライアント ID >]|[type < タイプ >]
|[hostname< ホスト名 >]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
{ ascii | hex} クライアント ID	クライアント ID を ASCII または、hex で指定します。 ascii：最大 63 文字(ASCII) hex：最大 126 桁(16 進数)	ascii hex	クライアント ID を付けない
タイプ	クライアント ID のタイプを指定します。	0～255	クライアント ID が ASCII の場合：0 クライアント ID が hex の場合：1
ホスト名	ホスト名を指定します。	最大 63 文字	ホスト名を付けない

この設定を行わない場合

DHCP クライアント機能を使用できません。

DHCP クライアント機能とは？

DHCP プロトコルを利用して、IP アドレス等の情報を割り当ててもらい、その内容にしたがって IP 通信を行なう機能を、DHCP クライアント機能といいます。

FITELnet-F シリーズは、LAN インタフェースで DHCP サーバ機能または DHCP リレーエージェント機能が使用でき、EWAN インタフェースで DHCP クライアント機能を使用できます。

設定モード

EWAN インタフェース設定モード

RIPに関する設定

network

RIP サービスを提供するインタフェースを IP アドレスまたは、インタフェースで決定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/24 のインタフェースで RIP を運用する

```
Router(config)#router rip
Router(config-rip)# network 192.168.0.0 255.255.255.0
```

設定例 2　pppoe1 のインタフェースで RIP を運用する

```
Router(config)#router rip
Router(config-rip)# network pppoe 1
```

コマンド書式

network {<IP アドレス> <ネットマスク> | インタフェース名}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP を運用するインタフェースを、インタフェースの IP アドレスで指定します。	IPv4 アドレス形式	省略不可
ネットマスク	RIP を運用するインタフェースを、IP アドレスとネットマスクの組み合わせで指定することもできます。	IPv4 アドレス形式	省略不可
インタフェース名	RIP を運用するインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

全てのインタフェースでも RIP を運用しません。

設定モード

RIP サービス設定モード

neighbor

RIP の宛先アドレスを指定します。
通常の RIP は、Version1 ではサブネットブロードキャスト(192.168.0.255 等)宛、Version2 ではマルチキャスト(224.0.0.9)宛に送信しますが、RIP を広告する相手を限定したい場合に、宛先アドレスを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP の宛先を 192.168.100.1 に限定する

```
Router(config)#router rip
Router (config-rip)# neighbor 192.168.100.1
```

コマンド書式

neighbor 〈IP アドレス〉 [source-interface 〈インタフェース名〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP の宛先を指定します。	IPv4 アドレス形式	省略不可
インタフェース名称	RIP を送信する際の送信元アドレスに使用するインタフェースアドレス。 送信元インタフェースの指定は、最大 128 エントリとなります。129 エントリ以上、送信元インタフェースを指定したエントリがある場合、129 件目以降のエントリについては、送信元エントリの指定が無効になり、実際に送信するインタフェースのアドレスが、送信元アドレスとなります。	lan 1 ewan 1～2 loopback 1 dialer 1～20※	実際に送信するインタフェース

※:F100 のみ選択可能です。

この設定を行わない場合

Version1 ではサブネットブロードキャスト(192.168.0.255 等)宛、Version2 ではマルチキャスト(224.0.0.9)宛に送信します。

設定モード

RIP サービス設定モード

ip rip receive version

PPPoE インタフェースの RIP 受信バージョン(1 or 2)を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　PPPoE1 で受信する RIP のバージョンを Version2 とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip receive version 2
```

コマンド書式

ip rip receive version 〈受信バージョン〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
受信バージョン	PPPoE で受信する RIP のバージョンを指定します。V1/V2 の両方を受信する場合は、1 2 のように2つ指定します。	1 2	省略不可

この設定を行わない場合

version コマンドで指定したバージョンとなります。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード

ip rip send version

PPPoE インタフェースの RIP 送信バージョン(1 or 2)を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　PPPoE1 で送信する RIP のバージョンを Version2 とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip send version 2
```

コマンド書式

ip rip send version <送信バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信バージョン	PPPoE で送信する RIP のバージョンを指定します。V1/V2 の両方を送信する場合は、1 2 のように2つ指定します。	1 2	省略不可

この設定を行わない場合

version コマンドで指定したバージョンとなります。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード

ip rip authentication key-chain

key chain 設定で設定した key-chain 名を指定し、PPPoE インタフェースの RIP2 のパスワード制御を行ないます。
key chain 設定では、key フレーズ／key-chain が有効な時間帯を指定することができます。
この設定が異なるルータとは、RIP2 での経路交換を行なうことができません。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP2 の認証で使用する key に、"key-rip2"を使用する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip authentication key-chain key-rip2
```

コマンド書式

ip rip authentication key-chain <key-chain 名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key-chain 名称	key chain コマンドで指定した key-chain 名称	-	省略不可

この設定を行わない場合

RIP2 の認証を行なうことはできません。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード

ip rip authentication mode

PPPoE インタフェースに RIP2 を送信する場合に、key chain 設定で定義した key フレーズをそのまま(Simple Text)で送信するか／md5 でハッシュ計算した後のデータ(Unrecognized Authentication Type)で送信するかを設定します。
そのまま送信する場合は"text"、ハッシュ計算した後のデータ(MD5 形式)で送信する場合は"md5"を指定します。この設定が異なるルータとは、RIP2 での経路交換を行なうことができません。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP2 の認証データを MD5 形式とする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip rip authentication mode md5
```

コマンド書式

ip rip authentication mode 〈認証方式〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式	RIP2 で、パスワードを送る方式を選択します。 text：Simple Text で送信する md5：MD5 形式で送信する	text md5	省略不可

この設定を行わない場合

Simple Text で送信します。

RIP2 とは？

RIP version 2 は、距離ベクタアルゴリズムをもつ、経路制御プロトコルです。
RIP version 1 とは、以下の点が異なります。
・送信する際の宛先アドレスがマルチキャスト(224.0.0.9)
・サブネットマスク情報を通知することができる
・NextHop を通知することができる
・認証データを通知することができ、認証データが異なるルータからの経路情報は有効としない。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード

ip split-horizon

インタフェースで Split-Horizon 制御を行なうかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　PPPoE インタフェースで Split-Horizon 制御を行なう

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip split-horizon enable
```

コマンド書式

ip split-horizon ＜ Split-Horizon 制御＞

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Split-Horizon 制御	Split-Horizon 制御を enable（行う）または、disabel（行わない）かどうかを指定します。	enable disable	省略不可

この設定を行わない場合

Split-Horizon 制御を行います。

Split-horizon 制御とは？

RIP 送信制御の方法です。
受信した RIP の宛先情報を、RIP を受信したインタフェースに対して送信するかどうかを規定します。Split-Horizon 制御を行なう場合は、RIP を受信したインタフェースには送信しません。
Split-Horizon 制御を行なっていないルータがネットワーク上に存在する場合、RIP で送信した情報を同じインタフェースから受信するため、そのインタフェース側にも経路が存在すると判断され、実際に送信するインタフェースが使用不可となっても、そちら側のインタフェースに経路が存在すると考えられ、データを送信してしまいます。
この機能がない場合は、経路がなくなった場合の収束が遅くなる原因となります。
Split-Horizon の拡張機能で、Split-Horizon with Poisonaous Reverse という機能があります。
この機能は、Split-Horizon のように、RIP を受信したインタフェースに同じ宛先の情報をもつ RIP を送信しないのではなく、その宛先の情報のメトリックを 16（到達不能）として RIP を送信する機能です。この機能により、さらに誤動作が防止できます。
本装置は、Split-Horizon with Poisonaous Reverse 機能をサポートしていません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
VLAN インタフェース設定モード

passive-interface

RIP の受信のみを行い、送信はしないインタフェースを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 インタフェースは、RIP の受信のみを行なう（送信しない）設定

```
Router(config)#router rip
Router(config-rip)#passive-interface ewan 1
```

コマンド書式

passive interface 〈インタフェース名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名称	RIP の受信のみを行なうインタフェースを指定します。	インタフェース名称	省略不可

この設定を行わない場合

RIP を制御するインタフェースでは、送受信を行ないます。

設定モード

RIP サービス設定モード

offset-list

access-list で指定した経路情報の送受信 RIP に対して、任意のメトリック値を加算します。
RIP 送信時は、設定したメトリック値を加算後に RIP を送信し、RIP 受信時は設定したメトリック値を加算後に経路登録を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.0/24 にマッチする経路情報の RIP 受信時に、メトリック値に 3 を加算して RIP テーブルに登録する

```
Router(config)#access-list 10 permit 192.168.100.0 0.0.0.255
Router(config)#router rip
Router(config-rip)# offset-list 10 in 3
```

コマンド書式

offset-list <access-list 番号> { in | out } <メトリック値> [インタフェース名]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	メトリック値を加算対象とするアクセスリストの番号を指定します。	1～99 1300～1999	省略不可
{in | out}	in（受信時）または、out（送信時）のどちらでメトリック値を加算するかを指定します。	in out	省略不可
メトリック値	加算するメトリック値を指定します。	0～16	省略不可
インタフェース名	適用するインタフェースのインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全インタフェースで適用

※1:F80 の場合は、1～5 になります。
※2:F100 のみ指定可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

RIP 受信時にメトリック値が 1 加算されます。

設定モード

RIP サービス設定モード

redistribute

RIP 以外の手段で取得した経路情報のうち、RIP で再配布する経路を選択し必要に応じてメトリック値等を設定します。
メトリック値を省略した場合は、"1"で配布します。
ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip rip redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を RIP で再配布する（メトリック 1）

```
Router(config)#router rip
Router(config-rip)#redistribute static
```

設定例２　BGP で取得した経路情報を RIP で再配布する。このときメトリックを 3 として配布する

```
Router(config)#router rip
Router(config-rip)#redistribute bgp metric 3
```

コマンド書式

redistribute <再配布する経路情報>[metric <メトリック値>][route-map <Route-map 名>]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>再配布する経路情報</td><td>RIP 以外の手段で取得した経路情報のうち、RIP で配布するものを指定します。
<table><tr><td>bgp</td><td>BGP で取得した経路情報</td></tr><tr><td>connected</td><td>直接経路</td></tr><tr><td>event-action</td><td>イベントアクションで追加した経路情報</td></tr><tr><td>kernel</td><td>kernel にセットされた経路情報</td></tr><tr><td>local-prot1</td><td rowspan="2">SA-UP ルート情報</td></tr><tr><td>local-prot2</td></tr><tr><td>ospf</td><td>OSPF で取得した経路情報</td></tr></table></td><td>bgp
connected
event-action
kernel
local-prot1
local-prot2
ospf
static</td><td>省略不可</td></tr>
<tr><td>メトリック値</td><td>RIP で広告する際のメトリック値を指定します。</td><td>0～16</td><td>メトリック値 1</td></tr>
<tr><td>Route-map 名</td><td>必要に応じて、適用する Route-map を指定します。</td><td>-</td><td>Route-map を適用しない</td></tr>
</table>

この設定を行わない場合

RIP で受信した情報および SA-UP ルート情報を広告します。

設定モード

RIP サービス設定モード

default-information originate

自身をデフォルトルートとして、RIP で通知するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　デフォルトルートの情報を RIP で送信する

```
Router(config)#router rip
Router(config-rip)#default-information originate
```

コマンド書式

default-information originate

パラメータ

パラメータはありません。

この設定を行わない場合

自身をデフォルトルートとしては通知しません。

注意

この設定は、デフォルトルートの情報を持っていないときに、RIP でデフォルトルートを通知するかどうかの設定です。
スタティック設定でデフォルトルートを設定していたり、ルーティングプロトコルによりデフォルトルートを学習していた場合は、この設定によらずデフォルトルートの情報を RIP で広告します。

設定モード

RIP サービス設定モード

version

装置として採用する RIP のバージョンを指定します。インタフェース毎の指定は ip rip {send/receive} version を用います。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP version 2 を使用する

```
Router(config)#router rip
Router (config-rip)# version 2
```

コマンド書式

version <RIP バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
RIP バージョン	RIP のバージョンを 1(バーション 1)、2(バージョン 2)から指定します。	1 2	省略不可

この設定を行わない場合

バージョン 2 となります。

設定モード

RIP サービス設定モード

default-metric

本装置で生成した経路情報(static の情報)を RIP で広告する際のメトリック値を設定します。ただし、デフォルトルートのメトリックについては、static 設定していたとしても"1"で広告します。

refresh コマンド後に有効になるコマンドです。

設定例１　FITELnet-F シリーズで設定したスタティックルートの情報を RIP で広告する際は、メトリック値を 5 とする

```
Router(config)#router rip
Router(config-rip)#default-metric 5
```

コマンド書式

default-metric 〈メトリック値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	スタティックルートを RIP で広告する場合のメトリック値を設定します。	1～16	省略不可

この設定を行わない場合

メトリック値は、1 で動作します。

メトリックとは？

IP パケットが通過するルータの数をメトリックといいます。
RIP で広告するメトリック値とは、その経路に到達するために、どのくらいのルータを経由しなくてはならないかを規定しています。
IPv4 では、メトリック値は 1～15 までと決められており、16 は到達不能を意味します。

通常、ルータは IP パケットを中継した際に、IP ヘッダ内にあるメトリックフィールドの値を1加算します。このようにして、メトリック値が加算され、16 になったら廃棄されます。

設定モード

RIP サービス設定モード

timers basic

RIP に関する以下のタイマ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　定期送信間隔を 20 秒、経路情報を無効とするまでの時間を 120 秒、経路情報を RIP テーブルから削除するまでの時間を 80 秒とする

```
Router(config)#router rip
Router (config-rip)#timers basic 20 120 80
```

コマンド書式

timers basic 〈定期送信間隔〉〈経路情報を無効とするまでの時間〉
〈経路情報を削除するまでの時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
定期送信間隔	RIP の定期送信間隔(単位:秒)を指定します。	5～2147483647	省略不可
経路情報を無効とするまでの時間	RIP のレスポンスを受信しなくなってから、経路情報を無効とするまでの時間(単位:秒)を指定します。 指定した時間内にレスポンスを受信しないと該当経路情報は無効となり、ルーティングテーブルからは削除されます。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を無効として、RIP テーブルから削除するまでの時間(単位:秒)を指定します。 この状態では、RIP テーブルにメトリック 16 で保持されて経路が無効になった事を広告します。	5～2147483647	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
定期送信間隔	30
経路情報を無効とするまでの時間	180
経路情報を削除するまでの時間	120

設定モード

RIP サービス設定モード

distance

同じ宛先への経路情報が複数存在した場合、どの情報を有効にするかを決定するための優先度を設定します。
例えば、スタティックルーティングで設定した情報と、RIP で受信した経路情報で、同じ宛先の情報があった場合に、どちらを優先とするかどうかの決定に使用します。
FITELnet-F シリーズでは、特定の宛先に対して、distance 値(優先度)をいくつにするかの指定もできます。さらに、どのルータから受信した RIP を対象とするかの指定もできます(ルータの限定は access-list を使用します)。
distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP の distance 値を 10 に設定する

```
Router(config)#router rip
Router(config-rip)#distance 10
```

設定例２　192.168.0.0/24 の経路情報を RIP で受信した際の distance 値を 30 に設定する

```
Router(config)#router rip
Router(config-rip)#distance 30 192.168.0.0 255.255.255.0
```

設定例３　192.168.100.0/24 上のルータから受信した 192.168.0.0/24 の経路情報は distance 値を 100 とする

```
Router(config)#access-list 1 permit 192.168.100.0 255.255.255.0

Router(config)#router rip
Router(config-rip)#distance 30 192.168.0.0 255.255.255.0 1
```

コマンド書式

distance <distance 値> [<IP アドレス> <ネットマスク> <access-list 番号>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	RIP の distance 値を指定します。	1～255	省略不可
IP アドレス	distance 値を設定する特定の宛先アドレスを指定します。	IPv4 アドレス形式	経路ごとの distance 値を指定しません。
ネットマスク	distance 値を設定するための、ネットマスク値を指定します。	IPv4 アドレス形式	経路ごとの distance 値を指定しません。
access-list 番号	distance 値を特定する、RIP 送信元ルータを指定します。	<1-99> <1300-1999>	経路ごとの distance 値を指定しません。

この設定を行わない場合

distance 値は、110 で動作します。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

RIP サービス設定モード

distribute-list

RIP 送受信に対してフィルタリングの設定を行ないます。
プレフィックスのアドレス部分が access-list コマンドで permit にマッチする情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。
また、フィルタリング制御を行なうためのインタフェースを指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.0/24 にマッチするプレフィックスのみを受け付ける

```
Router(config)#access-list 1 permit 192.168.100.0 0.0.0.255

Router(config)#router rip
Router(config-rip)# distribute-list 1 in
```

設定例２　192.168.100.0/24 にマッチするプレフィックスのみを送信しない

```
Router(config)#access-list 1 deny 192.168.100.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#router rip
Router(config-rip)# distribute-list 1 out
```

※上記の設定を行う場合は、必ず access-list コマンドで permit any を追加する必要があります。permit any を追加しないと、全てのアクセスリストの送信をフィルタしてしまいます。

設定例３　192.168.100.0/24 にマッチするプレフィックスのみを、LAN からは受信しない

```
Router(config)#access-list 1 deny 192.168.100.0 0.0.0.255
Router(config)#access-list 1 permit any
Router(config)#router rip
Router(config-rip)# distribute-list 1 in lan 1
```

設定例４　デフォルトルート（0.0.0.0/0）にマッチするプレフィックスのみを受け付ける

```
Router(config)#access-list 1 permit 0.0.0.0 0.0.0.0
Router(config)#router rip
Router(config-rip)# distribute-list 1 in
```

コマンド書式

distribute-list <access-list 番号> { in | out } [インタフェース名]

この設定を行わない場合

全てのプレフィックスを送受信します。

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	access-list コマンドで指定したリスト番号を指定します。	1～99	省略不可
in | out	受信／送信のどちらでフィルタするかを指定します※。	in：受信 out：送信時	省略不可
インタフェース名	適用するインタフェースのインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全インタフェースで適用

※1：F80 の場合は、1～5 になります。
※2：F100 のみ指定可能です。
※3：F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。
※rip distribute-list in,out 共に
・access list (permit)で指定された経路情報のみを送受信の対象とします。
・permit 指定がない経路情報はすべてフィルタします。

設定モード

RIP サービス設定モード

route

RIP エントリをスタティックで登録します。
ここで設定した経路情報は、RIP で広告するためだけに使用されます。装置のスタティックルートとしては登録されませんので注意してください。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.200.0/24 の経路情報を RIP で広告する

```
Router(config)#router rip
Router(config-rip)#route 192.168.200.0 255.255.255.0
```

コマンド書式

route〈IP アドレス〉〈ネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	RIP で広告する IP アドレスを設定します。	IPv4 アドレス形式	省略不可
ネットマスク	RIP(RIP2 のみ)で広告するネットマスクを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

スタティック情報はありません。
redistribute コマンドの指定および学習した RIP 情報のみを、RIP で広告します。

設定モード

RIP サービス設定モード

unicastrip

unicastRIP の送受信を許可するかどうかの設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　unicastRIP の送受信を許可します。

```
Router(config-rip)# unicastrip
Router(config-rip)#
```

コマンド書式

unicastrip

パラメータ

パラメータはありません。

この設定を行わない場合

unicastRIP の送受信を許可しません。

unicastRIP の動作条件

unicastRIP を送信、受信する為に必要な条件。

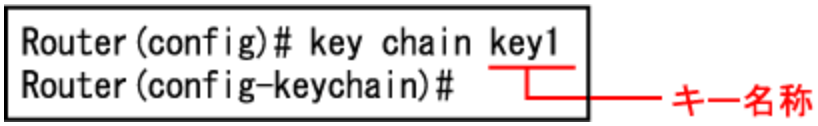
〈受信可能条件〉	unicastrip 設定がされている。
	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	受信した unicastrip の RIP バージョン(RIP1, RIP2) と、自身の RIP バージョン設定（ip rip receive version(優先)もしくは router rip の version）が一致している。
	unicastrip 送信元アドレスへの経路がルーティングテーブルに事前に存在している。
〈送信可能条件〉	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	neighbor コマンドでの unicastrip 送信先アドレスを設定されている。
	unicastrip 送信先アドレスへの経路がルーティングテーブルに事前に存在している。（RIP バージョン指定（ip rip send version 優先））

設定モード

RIP サービス設定モード

key chain

RIP2 の認証を有効にするための key-chain モードに移行します。
key-chain の設定は、キー名称を指定して行ないます。key-chain モードで、キーの情報を設定し、各インタフェースの RIP2 に関する設定で、使用するキー名称を指定します。



設定例１　キー名称が"key1"である key-chain モードに移行する

```
Router(config)# key chain key1
Router(config-keychain)#
```

コマンド書式

key chain 〈キー名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キー名称	RIP2 で参照するキー(パスワード)の名称 インタフェース設定モードで参照する名称なので、わかりやすい名前にしてください。	-	省略不可

RIP2 の認証について

RIP2 では、認証キーによる認証を行い、信用できるルータからのルーティング情報であるかどうかを制御することができます。
この認証キーが異なる RIP2 の情報は、ルーティングテーブルに登録しません。

実際の RIP2 に付加される認証の情報には、以下の 2 種類があります。
・simple password （設定されたテキストの情報）
・MD5 digest （設定されたテキストから MD5 で計算されたデータ）
本装置で、RIP2 の認証を使用する場合は、RIP2 を使用するインタフェースのインタフェース設定モードの"ip rip authentication"コマンドで、key-chain で設定するキー名称を指定する形で設定します。

```
Router(config-if lan 1)#ip rip authentication key-chain key1
                                                        キー名称
```

設定モード

基本設定モード

key <number> accept-lifetime

キーの受信時有効期限を設定します。
ここで設定した時間内であれば、RIP2 の認証キーを有効とします。<number>は、key <number> key-string コマンド、key <number> send-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例１　number=1 の受信時有効期限を"2008.9.1 12:00:00 - 2008.12.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Sep
2008 11:59:59 30 Dec 2008
```

設定例２　number=1 の受信時有効期限を"2008.9.1 12:00:00 - 無限"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Sep
2008 infinity
```

設定例３　number=1 の受信時有効期限を"2008.9.1 12:00:00 - 100 秒間"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Sep
2008 duration 100
```

コマンド書式

key <key 番号> accept-lifetime <有効開始時刻> { <有効期限> | duration <有効期間> | infinity }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key <number> key-string コマンド、key <number> send-lifetime コマンドと連携する際の番号を指定します	0～2147483647	省略不可
有効開始時刻	この鍵を受信に使用する場合の、有効開始時刻を指定します。	時:分:秒 日 月 年	3 種類のうちどれか 1 種類を指定する必要あり
duration <有効期間>	この鍵を受信に使用する場合の、有効期間(単位:秒)を指定します。	1～2147483646	
infinity	この鍵を受信に使用する場合の有効期限を、無限とします。	infinity	

この設定を行わない場合

常に使用可能です。

設定モード

key-chain 設定モード

key <number> send-lifetime

キーの送信時有効期限を設定します。
ここで設定した時間内であれば、RIP2 の認証キーをつけて送信します。
<number>は、key <number> key-string コマンド、key <number> accept-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例１　number=1 の送信時有効期限を"2008.9.1 12:00:00 - 2008.12.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Sep 2008
11:59:59 30 Dec 2008
```

設定例２　number=1 の送信時有効期限を"2008.9.1 12:00:00 - 無限"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Sep 2008
infinity
```

設定例３　number=1 の送信時有効期限を"2008.9.1 12:00:00 - 100 秒間"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Sep 2008
duration 100
```

コマンド書式

key <key 番号> send-lifetime <有効開始時刻> { <有効期限> | duration <有効期間>
| infinity }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key <number> key-string コマンド、key <number> accept-lifetime コマンドと連携する際の番号を指定します	0～2147483647	省略不可
有効開始時刻	この鍵を送信に使用する場合の、有効開始時刻を指定します。	時:分:秒 日 月 年	3 種類のうちどれか 1 種類を指定する必要あり
duration <有効期間>	この鍵を送信に使用する場合の、有効期間(単位:秒)を指定します。	1～2147483646	
infinity	この鍵を送信に使用する場合の有効期限を、無限とします。	infinity	

この設定を行わない場合

常に使用可能です。

設定モード

key-chain 設定モード

key 〈number〉 key-string

キーワードの文字列を指定します。
〈number〉は、key 〈number〉 accept-lifetime コマンド、key 〈number〉 send-lifetime コマンドと連携する際の番号です。

refresh コマンド後に有効になるコマンドです。

設定例１　number=1 のキーワードに"secret-secret"を設定する

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 key-string secret-secret
```

コマンド書式

key 〈key 番号〉 key-string 〈キーワード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
key 番号	key 〈number〉 key-string コマンド、key 〈number〉 accept-lifetime コマンドと連携する際の番号を指定します	0～2147483647	省略不可
キーワード	キーワードを指定します。	-	省略不可

この設定を行わない場合

RIP2 の認証を行なうことはできません。

設定モード

key-chain 設定モード

OSPFに関する設定

router-id

OSPF のルータ ID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF のルータ ID を 192.168.10.1 にする

```
Router(config)# router ospf
Router(config-ospf)# router-id 192.168.10.1
```

コマンド書式

router-id <ルータ ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ルータ ID	OSPF のルータ ID を設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

全インタフェースの IP アドレスのうち最大のものをルータ ID とします。

設定モード

OSPF サービス設定モード

network

OSPF エリアに含まれるネットワーク範囲を設定します。
エリアは、IP アドレスもしくは(0-4294967295)の値で指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF エリアに含まれるネットワーク範囲を、192.168.10.0/24 とします

```
Router(config)#router ospf
Router(config-ospf)#network 192.168.10.0 0.0.0.255 area 0
```

コマンド書式

network〈ネットワークアドレス〉〈マスク〉area〈エリア〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネットワークアドレス	OSPF に含まれるネットワーク範囲を指定します。	IPv4 アドレス形式	省略不可
マスク	ワイルドカードを指定します。	IPv4 アドレス形式	省略不可
エリア	エリアを IP アドレスまたは、数値で指定します。	IPv4 アドレス形式 0～4294967295	省略不可

この設定を行わない場合

OSPF エリアに含まれるネットワーク範囲を指定しません。

設定モード

OSPF サービス設定モード

OSPF 経路制御の設定

default-information originate

ルーティングテーブルにデフォルト経路(0.0.0.0/0)があれば、その情報を AS 外 LSA として配布するように設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　デフォルトルートを AS 外 LSA として配布する

```
Router(config)#router ospf
Router(config-ospf)#default-information originate
```

コマンド書式

```
default-information originate [ always] [ metric <0-16777214>] [ metric-
                                type{type-1|type-2}] [ route-map <Route-map 名>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
always	ルーティングテーブルにデフォルト経路が存在しなくても、自分自身をデフォルト経路としてアナウンスします。	always	自分自身をデフォルト経路としてアナウンスしません。
metric	メトリック値を指定します。	0～16777214	自分自身をデフォルト経路としてアナウンスします。
metric-type	メトリックタイプを指定します。	1 2	
Route-map 名	Route-map 名を指定します。	英数字	

この設定を行わない場合

メトリック値:10
メトリックタイプ:type-2
ただし、always オプションが有効な場合はメトリック値のデフォルトは 1 となります。

設定モード

OSPF サービス設定モード

default-metric

他のルーティングプロトコルで学習した経路を OSPF で再配布する際のメトリック値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　メトリック値を 30 に設定する

```
Router(config)#router ospf
Router(config-ospf)#default-metric 30
```

コマンド書式

default-metric 〈メトリック値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	他のルーティングプロトコルで学習した経路を OSPF で再配布する際のメトリック値を設定します。	0～16777214	省略不可

この設定を行わない場合

メトリック値を 20 に設定します。

設定モード

OSPF サービス設定モード

distance

OSPF の distance 値を設定します。
同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメータとなります。

refresh コマンド後に有効になるコマンドです。

設定例１　distance 値を 120 とします

```
Router(config)#router ospf
Router(config-ospf)#distance 120
```

コマンド書式

distance <distance 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	OSPF の distance 値を設定します。	1～255	省略不可

この設定を行わない場合

distance 値を 110 に設定します。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

OSPF サービス設定モード

distance ospf

external ルート、internal ルート、intra-area ルートの各 distance 値を設定します。
同じ宛先への経路を異なる手段で学習した場合に、どの情報を採用するかのパラメータとなります。

refresh コマンド後に有効になるコマンドです。

設定例１　external ルートの distance 値を 150 とします

```
Router(config)#router ospf
Router(config-ospf)#distance ospf external 150
```

コマンド書式

```
distance ospf {external <distance 値>|internal <distance 値>|intra-area
              <distance 値>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	external ルート、internal ルート、intra-area ルートの各 distance 値を設定します。	1～255	省略不可

この設定を行わない場合

distance コマンドで設定した値になります。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

OSPF サービス設定モード

neighbor

ネイバを登録します。
priority では、ネイバの優先度、poll-interval ではネイバへのポーリング間隔(単位:秒)を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.1 に対する優先度を 16 にする

```
Router(config)#router ospf
Router(config-ospf)#neighbor 192.168.0.1 priority 16
```

コマンド書式

neighbor <ip-address>[priority <優先度>] [poll-interval <ポーリング間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ip-address	ネイバを登録する IP アドレスを設定します。	IPv4 アドレス形式	省略不可
優先度	ネイバの優先度を指定します。	0～255	0
ポーリング間隔	ネイバへのポーリング間隔(単位:秒)を指定します。	1～65535	60

この設定を行わない場合

優先度:0
ポーリング間隔:60 秒

設定モード

OSPF サービス設定モード

redistribute

OSPF 以外の手段で取得した経路情報のうち、OSPF で再配布する経路を選択し必要に応じてメトリック値等を設定します。
メトリック値を省略した場合は、"1"で配布します。
ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip ospf redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例１　RIP で取得した情報を OSPF で再配布する

```
Router(config)#router ospf
Router(config-ospf)# redistribute rip
```

コマンド書式

redistribute <再配布する経路情報>[metric<メトリック値>][route-map <Route-map 名>]
[metric-type <1|2>]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>再配布する経路情報</td><td>OSPF 以外の手段で取得した経路情報のうち、OSPF で再配布するものを指定します。<table><tr><td>bgp</td><td>BGP で取得した経路情報</td></tr><tr><td>connected</td><td>直接経路</td></tr><tr><td>event-action</td><td>イベントアクションで追加した経路情報</td></tr><tr><td>kernel</td><td>kernel にセットされた経路情報</td></tr><tr><td>local-prot1</td><td rowspan="2">SA-UP ルート情報</td></tr><tr><td>local-prot2</td></tr><tr><td>rip</td><td>RIP で取得した経路情報</td></tr></table></td><td>bgp
connected
event-action
kernel
local-prot1
local-prot2
rip
static</td><td>省略不可</td></tr>
<tr><td>メトリック値</td><td>OSPF で広告する際の metric を指定します。</td><td>0～16777214</td><td>省略不可</td></tr>
<tr><td>Route-map 名</td><td>必要に応じて適用する Route-map を指定します。</td><td>-</td><td>Route-map を適用しない</td></tr>
<tr><td>1|2</td><td>OSPF の外部リンクタイプ ASBR が外部ルートをアドバタイズする場合に、どちらかを指定します。<table><tr><td>1</td><td>自 AS 内で広告される際にコスト加算する場合は、metric-type1 を指定します。</td></tr><tr><td>2</td><td>自 AS 内で広告される際にコスト加算しない場合は、metric-type2 を指定します。</td></tr></table></td><td>1
2</td><td>2</td></tr>
</table>

この設定を行わない場合

OSPF で受信した情報のみ配布します。

設定モード

OSPF サービス設定モード

summary-address

経路情報を Aggregate します。この経路を OSPF で広告しない場合は not-advertise を指定します。また、tag 値を設定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0/16 の経路情報を Tag 0 で Aggregate する

```
Router(config)#router ospf
Router(config-ospf)#summary-address 192.168.0.0 255.255.0.0 tag 0
```

コマンド書式

summary-address <ip-address> <netmask> [not-advertise] [tag <0-4294967295>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ip-address	経路情報を Aggregate する IP アドレスを指定します。	IPv4 アドレス形式	省略不可
netmask	経路情報を Aggregate する IP アドレスのネットマスク指定します。	IPv4 アドレス形式	省略不可
not-advertise	経路を OSPF で広告しない場合に指定します。	not-advertise	経路を OSPF で広告する
tag	tag 値を設定します。	0～4294967295	0

この設定を行わない場合

経路情報を Aggregate しません。

設定モード

OSPF サービス設定モード

OSPF エリア情報

area default-cost

スタブエリアにデフォルト経路をアナウンスする際のコスト値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　デフォルト経路をアナウンスする際のコスト値を 100 にする

```
Router(config)#router ospf
Router(config-ospf)#area 192.168.10.1 default-cost 100
```

コマンド書式

area〈エリア ID〉default-cost〈コスト値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IP アドレス形式	省略不可
コスト値	デフォルト経路をアナウンスする際のコスト値を設定します。	0～16777215	省略不可

この設定を行わない場合

コスト値を 1 に設定します。

設定モード

OSPF サービス設定モード

area export-list

他のエリアにアナウンスする経路をフィルタリングします。
アクセスリストにマッチしない経路はアナウンスしません。

refresh コマンド後に有効になるコマンドです。

設定例１　フィルタリングする経路をアクセスリスト番号１で指定する

```
Router(config)#router ospf
Router(config-ospf)#area 1 export-list 1
```

コマンド書式

area 〈エリア ID〉 export-list 〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
アクセスリスト番号	フィルタしたい経路を標準アクセスリスト番号でしていします。	1～99 1300～1999 10000～19999 100000～199999	省略不可

この設定を行わない場合

フィルタリングしません。

設定モード

OSPF サービス設定モード

area import-list

他のエリアからアナウンスされた経路をフィルタリングします。
アクセスリストにマッチしない経路は受け入れません。

refresh コマンド後に有効になるコマンドです。

設定例１　フィルタリングする経路をアクセスリスト番号１で指定する

```
Router(config)#router ospf
Router(config-ospf)#area 1 import-list 1
```

コマンド書式

area〈エリア ID〉import-list〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
アクセスリスト番号	フィルタしたい経路を標準アクセスリスト番号でしていします。	1～99 1300～1999 10000～19999 100000～199999	省略不可

この設定を行わない場合

フィルタリングしません。

設定モード

OSPF サービス設定モード

area nssa

OSPF エリアを NSSA(Not So Stub Area)に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　外部経路を NSSA に再配布しない

```
Router(config)#router ospf
Router(config-ospf)#area 1 nssa no-redistribution
```

コマンド書式

```
area <エリア ID> nssa [ translate-always|translate-never]
      [ no-redistribution|default-information-originate|no-summary]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
translate-always|translate-never	タイプ7LSA をタイプ5に変換して中継するかどうかを設定します。 translate-always　中継する translate-never　中継しない	translate-always translate-never	translate-always
no-redistribution	外部経路を NSSA に再配布しない場合に指定します。 ※ASBR が NSSA ABR を兼務している場合のみ	no-redistribution	タイプ5LSA を受け入れない IGRP 経路をエリア内にタイプ7として配布します。
default-information-originate	タイプ7のデフォルトルートを生成する場合に指定します。	default-information-originate	
no-summary	NSSA 完全スタブエリアを設定する場合に指定します。	no-summary	

この設定を行わない場合

OSPF エリアを NSSA に設定しません。

NSSA とは？

バックボーンでないエリアを、NSSA として設定することができます。
エリアボーダルータは、NSSA として定義したエリアへほかのエリアから学習した AS 外経路を広告しません。
NSSA を設定することで、NSSA 内では経路情報を減らし、ルータの情報の交換や経路選択の負荷を減らすことができます。

設定モード

OSPF サービス設定モード

area range

他のエリアに経路をアナウンスする際に複数の経路を 1 つの経路に集約します。

refresh コマンド後に有効になるコマンドです。

設定例 1　集約する経路の IP アドレスを 192.168.10.0/16 にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 range 192.168.0.0 255.255.0.0
```

コマンド書式

area 〈エリア ID〉 range 〈summary-address〉〈summary-address-mask〉
[substitute 〈substitute-address〉〈substitute-address-mask〉|not-advertise]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
summary-address	集約する経路の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
summary-address-mask	集約する経路のネットワークマスクを設定します。	IPv4 アドレス形式	省略不可
substitute-address	集約する経路を別のアドレスでアナウンスする場合の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
substitute-address-mask	集 約する経路を別のアドレスでアナウンスする場合のネットワークマスクを設定します。	IPv4 アドレス形式	省略不可
not-advertise	集約した経路をアナウンスしない場合に指定します。	–	–

この設定を行わない場合

経路の集約は行いません。

設定モード

OSPF サービス設定モード

area shortcut

エリアのショートカットモードを設定します。

※ospf abr-type shortcut コマンドと同時に設定して ABR タイプを shortcut モードにしておく必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　ショートカットモードを有効にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 shortcut enable
```

コマンド書式

area〈エリア ID〉shortcut〈ショートカットモード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
ショートカットモード	ショートカットモードの状態を設定します。 default：ショートカットモードをデフォルトに戻す場合に指定します。 disable：ショートカットモードを無効にする場合に指定します。 enable：ショートカットモードを有効にする場合に指定します。	default disable enable	省略不可

この設定を行わない場合

ショートカットモードを使用しません。

設定モード

OSPF サービス設定モード

area stub

OSPF エリアをスタブエリアに設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　サマリ LSA をスタブエリアにアナウンスしない

```
Router(config)#router ospf
Router(config-ospf)#area 1 stub no-summary
```

コマンド書式

area 〈エリア ID〉 stub [no-summary]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
no-summary	サマリ LSA をスタブエリアにアナウンスしない場合に指定します。	no-summary	サマリ LSA をスタブエリアにアナウンスします。

この設定を行わない場合

OSPF エリアをスタブエリアに設定しません。

スタブエリアとは？

スタブエリアには、外部経路を伝える LSA が流れません。
そのため、このエリアには ASBR を設置することはできません。
また、外部経路が伝わらないため、スタブエリアの ABR は、このエリア内にデフォルトルートをアナウンスする必要があります。

設定モード

OSPF サービス設定モード

ospf abr-type

エリア境界ルータのタイプを設定します。
オプションにより、エリア間ルートの計算の動作が異なります。

refresh コマンド後に有効になるコマンドです。

設定例１　エリア境界ルータのタイプを standard にする

```
Router(config)#router ospf
Router(config-ospf)#ospf abr-type standard
```

コマンド書式

ospf abr-type 〈ルータタイプ〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
ルータタイプ	エリア境界ルータのタイプを設定します。		cisco ibm shortcut standard	省略不可
	cisco	バックボーンエリアに隣接していて,かつバックボーンエリアの 1 台以上のルータと full ステータスとなっている場合にバックボーンエリアおよびトランジットエリアの summary lsa を計算。それ以外は全エリアの summary lsa を計算します。		
	ibm	バックボーンエリアに隣接していて,かつバックボーンエリアの 1 台以上のルータと full ステータスとなっている場合にバックボーンエリアおよびトランジットエリアの summary lsa を計算。それ以外は全エリアの summary lsa を計算します。		
	shortcut	バックボーンエリアに関しては,バックボーンエリアの 1 台以上のルータと full ステータスとなっている場合に summary LSA を計算。バックボーンエリア以外のエリアに関しては,以下のエリアに関して summary LSA を計算。 ・トランジットエリア ・ルータがバックボーンに隣接していなくて,shortcut モードが disable 以外(default or enable)のエリア ・shortcut モードが enable のエリア		
	standard	エリア間ルートの計算は,バックボーンエリアおよびトランジットエリア(Virtual Link)でのみ summary LSA を計算。		

この設定を行わない場合

ABR のタイプを standard に設定します。

設定モード

OSPF サービス設定モード

OSPF 認証の設定

area authentication

OSPF 認証機能を有効にします。
認証キーは、ip ospf authentication-key,ip ospf message-digest-key コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　エリア ID １の認証方式に MD5 を使用する

```
Router(config)#router ospf
Router(config-ospf)#area 1 authentication message-digest
```

コマンド書式

area 〈エリア ID〉 authentication [message-digest]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IP アドレスで指定します。	0～4294967295 IPv4 アドレス形式	省略不可
message-digest	OSPF 認証に MD5 を使用する場合に指定します。	message-digest	認証に MD5 を使用しない

この設定を行わない場合

OSPF 認証を行いません。

設定モード

OSPF サービス設定モード

ip ospf authentication

設定しているインタフェースで認証機能を使用するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 の認証を MD5 で行う

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf authentication message-digest
```

コマンド書式

ip ospf authentication [認証設定]

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
認証設定	認証方法を設定します。		message-digest null	simple-password で認証を行ないます。
	message-digest	MD5 で認証を行います。		
	null	simple-password で認証を行います。		

この設定を行わない場合

認証を行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf authentication-key

OSPF で認証機能を使用する場合の認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　認証キーを「ospfpaswd」にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf authentication-key ospfpswd
```

コマンド書式

ip ospf authentication-key 〈認証キー〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証キー	OSPF で認証機能を使用する場合の認証キーを設定します。	8 文字以内の英数字	省略不可

この設定を行わない場合

OSPF 認証機能で使用する認証キーを設定しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf message-digest-key

OSPF で MD5 認証機能を使用する場合の MD5 認証キーとキーID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　MD5 認証キーを「md5pswd」、キーID を 1 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf message-digest-key 1 md5 md5pswd
```

コマンド書式

ip ospf message-digest-key 〈キーID〉md5 〈認証キー〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証キー	OSPF で MD5 認証機能を使用する場合の認証キーを設定します。	16 文字以内の英数字	省略不可
キーID	OSPF で MD5 認証機能を使用する場合のキーIDを設定します。	1～255	省略不可

この設定を行わない場合

OSPF の認証機能に MD5 を使用しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

OSPF インタフェース

ip ospf hello-interval

OSPF の Hello interval を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF の Hello interval を 20 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf hello-interval 20
```

コマンド書式

ip ospf hello-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	Hello メッセージの送信間隔(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

Hello メッセージを 10 秒間隔で定期的に送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf dead-interval

OSPF の dead interval を設定します。
ここで設定した時間、OSPF の Hello を受信しなかった場合、その Neighbor をテーブルから削除します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF の dead interval を 100 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf dead-interval 100
```

コマンド書式

ip ospf dead-interval < dead interval >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dead interval	Neighbor をテーブルから削除する時間（単位：秒）を設定します。	1～65535	省略不可

この設定を行わない場合

40 秒間 Hello を受信しなかった場合にテーブルから削除します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf retransmit-interval

OSPF（Database Description および Link State Request ）の再送間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF の再送間隔を 100 秒にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf retransmit-interval 100
```

コマンド書式

ip ospf retransmit-interval 〈再送間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送間隔	Database Description および Link State Request パケットの再送間隔（単位：秒）を設定します。	3～65535	省略不可

この設定を行わない場合

5 秒間隔で送信します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf transmit-delay

設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間を設定します。
ここで設定した値が、LSA の Age に加算されます。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF の transmit delay を 10 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf transmit-delay 10
```

コマンド書式

ip ospf transmit-delay 〈中継遅延時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
中継遅延時間	設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

中継遅延時間は 1 秒になります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf cost

OSPF を使用する場合のインタフェースに割り当てるコスト値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 に割り当てるコスト値を 100 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf cost 100
```

コマンド書式

ip ospf cost 〈コスト値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
コスト値	インタフェースのコスト値を設定します。	1～65535	省略不可

この設定を行わない場合

OSPF コスト値を 1 秒で運用します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf database-filter all out

このインタフェースに新しい LSA の情報を受け付けないようにする場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　新しい LSA の情報を受け付けないようにする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf database-filter all out
```

コマンド書式

ip ospf database-filter all out

パラメータ

パラメータはありません

この設定を行わない場合

新しい LSA の情報を受け付けます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf disable all

このインタフェースで OSPF を使用しない場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　このインタフェースで OSPF を使用しないようにする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf disable all
```

コマンド書式

ip ospf disable all

パラメータ

パラメータはありません

この設定を行わない場合

OSPF を使用します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf network

OSPF インタフェースのネットワークの型を明示的に指定したい場合にこのコマンドを使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　ネットワークタイプを non-broadcast multiple access タイプに指定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# ip ospf network non-broadcast
```

コマンド書式

ip ospf network 〈ネットワークタイプ〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
ネットワークタイプ	OSPF で使用するネットワークタイプを指定します。		broadcast non-broadcast point-to-multipoint point-to-point	省略不可
	broadcast	broadcast タイプに設定します。		
	non-broadcast	non-broadcast multiple access タイプに設定します。		
	point-to-multipoint	point-to-multipoint タイプに設定します。		
	point-to-point	point-to-point タイプに設定します。		

この設定を行わない場合

broadcast タイプに設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

ip ospf priority

OSPF を使用する優先度を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF を使用するインタフェースの priority を 20 にする

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip ospf priority 20
```

コマンド書式

ip ospf priority 〈優先度〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
優先度	OSPF を使用するインタフェースの優先度を設定します。	0～255	省略不可

この設定を行わない場合

priority を 1 に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード

passive-interface

ここで指定したインタフェースには HELLO パケットの送受信を行いません。
ルータ ID 決定の際の計算の対象からも除外されます。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 で HELLO パケットの送受信を行わないようにする

```
Router(config)#router ospf
Router(config-ospf)#passive-interface ewan1
```

コマンド書式

passive-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	HELLO パケットの送受信を行わないインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24※	省略不可

※:F80 の場合は、1～5 になります。

この設定を行わない場合

HELLO パケットの送受信を行う。

設定モード

OSPF サービス設定モード

OSPF 全般の設定

compatible rfc1583

AS 外の経路について、RFC1583 互換で動作するよう設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　AS 外の経路について、RFC1583 互換で動作するようにする

```
Router(config)#router ospf
Router(config-ospf)#compatible rfc1583
```

コマンド書式

compatible rfc1583

パラメータ

パラメータはありません

この設定を行わない場合

RFC 1583 非互換で動作します。

設定モード

OSPF サービス設定モード

auto-cost reference-bandwidth

インタフェースの OSPF コスト値を自動計算する際のベースとなる値を設定します。
単位は Mbps です。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF コスト値を自動計算する際のベース値を 80 とします

```
Router(config)#router ospf
Router(config-ospf)#auto-cost reference-bandwidth 80
```

コマンド書式

auto-cost reference-bandwidth 〈ベース値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ベース値	OSPF コスト値を自動計算する際のベースとなる値を設定します。	1～4294967	省略不可

この設定を行わない場合

100Mbps に設定します。

設定モード

OSPF サービス設定モード

refresh timer

LSA リフレッシュの間隔を設定します。対象はサマリ LSA(タイプ 3,4)、AS 外 LSA 。

refresh コマンド後に有効になるコマンドです。

設定例 1　LSA リフレッシュの間隔を 30 秒にする

```
Router(config)#router ospf
Router(config-ospf)#refresh timer 30
```

コマンド書式

refresh timer 〈LSA リフレッシュの間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LSA リフレッシュの間隔	LSA リフレッシュの間隔を指定します。	10～1800	省略不可

この設定を行わない場合

LSA リフレッシュの間隔を 10 秒に設定します。

設定モード

OSPF サービス設定モード

timers spf

LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間と、SPF 計算を行ってから次の計算に入るまでのホールドタイムを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SPF 計算を開始するまでの遅延時間を 100 秒、SPF 計算を行ってから次の計算に入るまでのホールドタイムを 50 秒にします。

```
Router(config)#router ospf
Router(config-ospf)#timers spf 100 50
```

コマンド書式

timers spf <spf-delay> <spf-holdtime>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
spf-delay	LSA の更新を受信してから、実際に SPF 計算を開始するまでの遅延時間を設定します。	0～4294967295	省略不可
spf-holdtime	SPF 計算を行ってから次の計算に入るまでのホールドタイムを設定します。	0～4294967295	省略不可

この設定を行わない場合

spf-delay：5 秒
spf-holdtime：10 秒

設定モード

OSPF サービス設定モード

log-adjacency-changes

OSPF ネイバの状態遷移を slog に出力します。
出力内容は状態遷移前後のステートおよび状態遷移を引き起こしたイベントの種類です。
detail が指定された場合は、全ての状態遷移時に出力します。
detail が指定されない場合は、FULL ステートと FULL ステート以外のステートの間の遷移が発生した時のみ出力します。

refresh コマンド後に有効になるコマンドです。

設定例１　OSPF ネイバの状態遷移を slog に出力する

```
Router(config)#router ospf
Router(config-ospf)#log-adjacency-changes
```

コマンド書式

log-adjacency-changes

パラメータ

パラメータはありません

この設定を行わない場合

OSPF ネイバの状態遷移を slog に出力しません。

設定モード

OSPF サービス設定モード

virtual-link の設定

area virtual-link

Virtual-link を確立する相手のルータ ID を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　仮想リンク先の IP アドレスを 192.168.10.1 にする

```
Router(config)#router ospf
Router(config-ospf)#area 1 virtual-link 192.168.10.1
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

仮想リンクを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link authentication

設定しているインタフェースで認証機能を使用するかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　MD-5 認証機能を使用して認証する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2
authentication message-digest
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 authentication [認証設定]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
認証設定	認証方法を選択します。 message-digest：MD5 で認証を行います。 null：simple-password で認証を行います。	message-digest null	simple-password で認証を行います。

この設定を行わない場合

認証を行いません。

設定モード

OSPF サービス設定モード

area virtual-link authentication-key

Virtual-link で認証機能を使用する場合の認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　認証キーを ospfpswd に設定する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2
authentication-key ospfpswd
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 authentication-key 〈パスワード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
パスワード	認証パスワードを指定します。	最大8文字の英数字	省略不可

この設定を行わない場合

Simple-password 認証のパスワードを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link dead-interval

OSPF の dead interval を設定します。
ここで設定した時間内に OSPF の Hello を受信しなかった場合、その Neighbor をテーブルから削除します。

refresh コマンド後に有効になるコマンドです。

設定例１　20 秒間 Hello を受信しなかったらテーブルから削除する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 dead-interval 20
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 dead-interval 〈受信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
受信間隔	近接ルータをダウンと認識するまでの Hello パケット未受信間隔(単位:秒)を指定します。	1～65535	省略不可

この設定を行わない場合

40 秒間 Hello を受信しなかった場合、Neighbor をテーブルから削除します。

設定モード

OSPF サービス設定モード

area virtual-link hello-interval

Hello パケットの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　Hello パケットの送信間隔を 20 秒に設定する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 20 hello-interval 20
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 hello-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
送信間隔	Hello パケットの送信間隔(単位:秒)を指定します。	1～65535	10

この設定を行わない場合

Hello パケットの送信間隔を 10 秒に設定します。

設定モード

OSPF サービス設定モード

area virtual-link message-digest-key

Virtual-link で MD5 認証機能を使用する場合の MD5 認証キーを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　192.168.0.0/16 の経路情報を Tag 0 で Aggregate する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2 message-
digest-key 1 md5md5pswd
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 message-digest-key 〈キーID〉
md5 〈認証キー〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
キーID	キーID を指定します。	1～255	省略不可
認証キー	認証キーを指定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

認証キーを設定しません。

設定モード

OSPF サービス設定モード

area virtual-link retransmit-interval

Virtual-Link の OSPF(Database Description および Link State Request)の再送間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　OSPF の再送間隔を 100 秒に設定する

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2
retransmit-interval 100
```

コマンド書式

area 〈エリア ID〉 virtual-link 〈リモートルータ ID〉 retransmit-interval 〈再送間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
再送間隔	Database Description および Link State Request パケットの再送間隔(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

再送間隔を 5 秒に設定します。

設定モード

OSPF サービス設定モード

area virtual-link transmit-delay

Virtual-Link の LinkStateUpdate を中継するためにかかる時間を設定します。
ここで設定した値が、LSA の Age に加算されます。

refresh コマンド後に有効になるコマンドです。

設定例１　LinkStateUpdate パケットの中継遅延時間を 10 秒にする

```
Router(config)#router ospf
Router(config-ospf)#area 10.0.0.1 virtual-link 10.0.0.2
transmit-delay 10
```

コマンド書式

area〈エリア ID〉virtual-link〈リモートルータ ID〉transmit-delay〈中継遅延時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エリア ID	エリア ID を整数または、IPv4 アドレス形式で指定します。	0～4294967295 IPv4 アドレス形式	省略不可
リモートルータ ID	Virtual-link を確立する相手のルータ ID を指定します。	IPv4 アドレス形式	省略不可
中継遅延時間	設定しているインタフェースにて、LinkStateUpdate を中継するためにかかる時間(単位:秒)を設定します。	1～65535	省略不可

この設定を行わない場合

中継遅延間隔は 1 秒になります。

設定モード

OSPF サービス設定モード

BGPに関する設定

aggregate-address

経路情報を集約し、その情報を BGP で通知します。通知する際は、PATH 属性に、ATOMIC-AGGREGATE 属性、AGGREGATOR 属性(Aggregator-Origin = FITELnet-F100)をつけて通知します。summary-only を指定した場合は、集約後の経路情報のみを通知し、集約された他の情報は通知されません。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0～192.168.255.0 の経路情報を 192.168.0.0/16 に集約する

```
Router(config)#router bgp 100
Router(config-bgp)#aggregate-address 192.168.0.0 255.255.0.0
```

設定例２　設定例１と同様（ただし集約後のアドレスのみを BGP で通知する）

```
Router(config)#router bgp 100
Router(config-bgp)#aggregate-address 192.168.0.0 255.255.0.0 summary-only
```

コマンド書式

aggregate-address <IP アドレス> <ネットマスク> [summary-only]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	集約後の IP アドレス	IPv4 アドレス形式	省略不可
ネットマスク	集約後のネットマスク	IPv4 アドレス形式	省略不可
summary-only	集約後の経路情報のみを通知する場合に指定します。	summary-only	集約前の経路情報も全て通知する

この設定を行わない場合

Aggregate しません。

設定モード

BGP サービス設定モード

bgp always-compare-med

異なる自律システムに属する複数の BGP ピアから受け取った経路の MED の比較を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　MED による最適経路の比較を行なう

```
Router(config)#router bgp 100
Router(config-bgp)# bgp always-compare-med
```

コマンド書式

bgp always-compare-med

パラメータ

パラメータはありません。

この設定を行わない場合

MED の比較は行ないません。

設定モード

BGP サービス設定モード

bgp bestpath med missing-as-worst

BGP の最適経路の選択において、MED 値(MULTI-EXIT-DESCRIMINATOR)を考慮する場合に指定します。missing-as-worst を指定した場合は、MED 属性のない経路を最も適していない経路とみなします(MED 値を非優先(4294967295)として扱う)。

refresh コマンド後に有効になるコマンドです。

設定例１　MED 属性の無い経路を、非優先経路とする

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath med missing-as-worst
```

コマンド書式

bgp bestpath med missing-as-worst

パラメータ

パラメータはありません。

この設定を行わない場合

MED 属性のない経路は、MED 値の比較は行ないません。

FITELnet-F シリーズの BGP 最適経路選択

FITELnet-F シリーズの BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	FITELnet-F シリーズが生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP ＞ I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される

10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp bestpath as-path ignore

BGP の最適経路の選択において、AS パスの長さを考慮しない場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　最適経路の選択に、AS_PATH 長を考慮しない

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath as-path ignore
```

コマンド書式

bgp bestpath as-path ignore

パラメータ

パラメータはありません。

この設定を行わない場合

AS-PATH 長を考慮します

FITELnet-F シリーズの BGP 最適経路選択

FITELnet-F シリーズの BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	FITELnet-F シリーズが生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP ＞ I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される

10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp bestpath compare-routerid

BGP の最適経路の選択において、ルータ ID を考慮する場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　最適経路の選択に、ルータ ID を考慮する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp bestpath compare-routerid
```

コマンド書式

bgp bestpath compare-routerid

パラメータ

パラメータはありません。

この設定を行わない場合

ルータ ID を考慮しません

FITELnet-F シリーズの BGP 最適経路選択

FITELnet-F シリーズの BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	FITELnet-F シリーズが生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP ＞ I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される

10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

bgp default ipv4-unicast

BGP ピアと交換するアドレスファミリーのデフォルトを IPv4 とします。IPv6 をデフォルトとする場合は、disable を設定します。
disable に設定した場合で、IPv4 の経路交換を行なう場合は、neighbor activate enable コマンドで BGP ピアを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピアとの経路交換デフォルトを IPv6 とする

```
Router(config)#router bgp 100
Router(config-bgp)#bgp default ipv4-unicast disable
```

コマンド書式

bgp default ipv4-unicast〈アドレスファミリ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アドレスファミリ	BGP ピアと交換するアドレスファミリーのデフォルトを IPv4 にするかを指定します。 enable：デフォルトを IPv4 とする disable：デフォルトを IPv6 とする	enable disable	省略不可

この設定を行わない場合

IPv4 ユニキャストは交換できます。

設定モード

BGP サービス設定モード

bgp log-neighbor-changes

次のような場合に、情報を slog に出力します。
・BGP ピアとの間でセッションが確立された場合
・BGP ピアとの間でセッションが切断された場合
・BGP NOTIFICATION メッセージを送信した場合
・BGP NOTIFICATION メッセージを受信した場合

refresh コマンド後に有効になるコマンドです。

設定例１　上記タイミングでログを出力する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp log-neighbor-changes
```

コマンド書式

bgp log-neighbor-changes

パラメータ

パラメータはありません。

この設定を行わない場合

上記タイミングでのログ出力を行いません。

設定モード

BGP サービス設定モード

bgp router-id

BGP ルータ ID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP のルータ ID を 10.1.1.1 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp router-id 10.1.1.1
```

コマンド書式

bgp router-id <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP のルータ ID を指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

ルータの全インタフェースアドレスで最大のものを BGP ルータ ID とします。

ルータ ID とは？

BGP で扱う、装置の ID です。通常は、そのルータのどこか 1 つのインタフェースの IP アドレスを割り当てます。

設定モード

BGP サービス設定モード

bgp default local-preference

LOCAL-PREF 値を設定します。UPDATE メッセージで通知する全ての経路情報に関して、ここで設定した LOCAL-PREF 値をつけて通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　LOCAL-PREF 値を 200 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp default local-preference 200
```

コマンド書式

bgp default local-preference <LOCAL-PREFERENCE 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LOCAL-PREFERENCE 値	UPDATE メッセージで広告する際の LOCAL-PREFERENCE 値を設定します。	0～4294967295	省略不可

この設定を行わない場合

LOCAL-PREFERENCE 値は 100 になります。

LOCAL-PREF とは？

同じ宛先プレフィックスに対する優先度です。LOCAL-PREF 値が大きい経路情報が、優先されます。

設定モード

BGP サービス設定モード

bgp scan-time

各 BGP 経路のネクストホップに関する到達可能性の定期的なスキャンを行う間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　スキャン間隔を 5 秒に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# bgp scan-time 5
```

コマンド書式

bgp scan-time〈スキャン間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
スキャン間隔	スキャンを行なう間隔(単位:秒)を設定します。	5～60	省略不可

この設定を行わない場合

スキャン間隔は 60 秒に設定されます。

設定モード

BGP サービス設定モード

distance

特定の BGP ピアからアナウンスされた経路の distance 値を設定します。distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　access-list 番号 1 に指定したアドレスから受信した 192.168.100.0/24 の distance 値を"1"とする

```
Router(config)#router bgp 100
Router(config-bgp)# distance 1 192.168.100.0 255.255.255.0 1
```

コマンド書式

distance 〈distance 値〉〈IP アドレス〉〈ネットマスク〉[access-list 番号]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	設定している経路の distance 値を設定します。	1～255	省略不可
IP アドレス	distance 値を設定する経路情報の宛先 IP アドレスを指定します。	IPv4 アドレス形式	省略不可
ネットマスク	distance 値を設定する経路情報のネットマスクを指定します。	IPv4 アドレス形式	省略不可
access-list 番号	標準アクセスリスト番号に合致した BGP ピアからアナウンスされた経路にだけディスタンス値を適用する。	-	全ての BGP ピアから受信した情報

この設定を行わない場合

BGP のディスタンス値(distance bgp コマンドで指定)に従います。

設定モード

BGP サービス設定モード

distance bgp

EBGP／IBGP／ローカル経路について distance 値を設定します。distance 値は、値が小さいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例１　E-BGP, I-BGP, ローカル経路の distance 値を、それぞれ 30, 210, 250 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)#distance bgp 30 210 250
```

コマンド書式

distance bgp <distance 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	external(EBGP), internal(IBGP), local それぞれについて distance 値を設定します。	1～255	省略不可

この設定を行わない場合

経路	distance 値
E-BGP	20
I-BGP	200
ローカル経路	200

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

BGP サービス設定モード

neighbor activate

指定した IP アドレスを持つ BGP ピアを有効とするかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）を有効とする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 activate enable
```

コマンド書式

neighbor 〈IP アドレス〉 activate 〈BGP ピア設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
BGP ピア設定	BGP ピアを有効(enable)とするか無効(disable)とするかを設定します。	enable disable	省略不可

この設定を行わない場合

BGP ピアは有効になります。

設定モード

BGP サービス設定モード

neighbor default-originate

BGP ピアをデフォルトルートとして使うためにデフォルトルート 0.0.0.0 をネイバに送ることを許可するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）に対して、デフォルトルートの情報を送る

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 default-originate
```

コマンド書式

neighbor 〈IP アドレス〉 default-originate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

デフォルトルートを生成しません。

設定モード

BGP サービス設定モード

neighbor description

BGP ピアに名前や説明のための文字列を指定します。
この設定は相手と同じでなければいけないという決まりはありません。わかりやすい名前を設定してください。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）の名称を"IP-VPN1"とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 description IP-VPN1
```

コマンド書式

neighbor 〈IP アドレス〉 description 〈BGP ピア名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
BGP ピア名称	BGP ピアの名称を設定します。	80 文字以内の文字列	省略不可

この設定を行わない場合

設定なしとなります。BGP の経路制御に影響はありません。

設定モード

BGP サービス設定モード

neighbor distribute-list

BGP の送受信に対してフィルタリングの設定を行ないます。
access-list コマンドで指定した宛先の情報のみを受け入れる／受け入れない、または送信する／送信しないといった制御を行なうことができます。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）からは、192.168.110.0/24 の宛先情報のみを受け付ける

```
Router(config)# access-list 1 permit 192.168.110. 0.0.0.255

Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 distribute-list 1 in
```

設定例２　BGP ピア（10.0.0.1）には、192.168.110.0/24 の宛先情報のみを送信しない

```
Router(config)# access-list 1 deny 192.168.110. 0.0.0.255

Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 distribute-list 1 out
```

コマンド書式

neighbor 〈IP アドレス〉 distribute-list 〈access-list 番号〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
アクセスリスト番号	指定している BGP ピアに対して、送信する/送信しない経路情報を指定するために access-list 番号を指定します。	1～99 1300～1999	省略不可
フィルタリング	指定している BGP ピアから受信時(in)／指定している BGP ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

全てのプレフィックスを送受信します。

設定モード

BGP サービス設定モード

neighbor dont-capability-negotiate

OPEN メッセージのオプションとしてケイパビリティ交渉つけないで送信する場合に指定します。
本装置がケイパビリティ交渉を行なう際に通知するケイパビリティは、以下です。
・Multi Protocol Extension Capability (address-family ipv4 unicast/multicast)
・Route Refresh(old & new)

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）には、ケイパビリティ交渉を行なわない

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 dont-capability-negotiate
```

コマンド書式

neighbor 〈IP アドレス〉 dont-capability-negotiate

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

設定に応じてケイパビリティ交渉を行います。

ケイパビリティ交渉とは？

BGP の通信の最初に行なう OPEN メッセージで、自身がサポートするオプション機能(能力:ケイパビリティ)を相手に通知します。
これは、新しい機能やマルチプロトコル機能などの能力を通知し合うことで相手の能力を知り、無意味な UPDATE メッセージを送受信する必要がなくなるメリットがあります。
ケイパビリティ交渉を行なわない場合は、全てのオプション能力がない物(そのような UPDATE メッセージは送られてこない)として扱われます。

設定モード

BGP サービス設定モード

neighbor ebgp-multihop

BGP ピアが、E-BGP セッションであり、直接接続されていないネットワークに存在する場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）が、直接接続されていないネットワーク上にあり、E-BGP である

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 ebgp-multihop
```

コマンド書式

neighbor 〈IP アドレス〉 ebgp-multihop ［最大ホップ数］

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
最大ホップ数	BGP ピアとしてセッションを確立するための最大ホップ数を設定します。	1～255	255

この設定を行わない場合

E-BGP の場合は、直接接続されていると判断します。

注意

ebgp-multihop を指定しなくてはいけない BGP ピアの場合は、他の経路情報手段（RIP やスタティックルーティング）で、その BGP ピアへの経路を取得しておく必要があります。
取得していない場合は、BGP のセッションを確立することはできません。

設定モード

BGP サービス設定モード

neighbor maximum-prefix

BGP ピアから受け付けるプリフィック情報の最大数を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）からのプレフィックス情報の最大数を 10 に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 maximum-prefix 10
```

コマンド書式

neighbor〈IP アドレス〉maximum-prefix〈最大プレフィックス数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
最大プレフィックス数	指定している BGP ピアから受信できる最大経路情報数	1～4294967295	省略不可

この設定を行わない場合

特定のネイバに対するプリフィックス数の制限はしません

設定モード

BGP サービス設定モード

neighbor next-hop-self

この BGP ピアに対して経路を広告する場合、NextHop を自装置に書き換えて広告します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）へ広告する経路情報の NextHop を自装置に書き換えて広告する

```
Router(config-bgp)# neighbor 10.0.0.1 next-hop-self
```

コマンド書式

neighbor 〈IP アドレス〉 next-hop-self

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

NextHop を自装置に書き換えません。

設定モード

BGP サービス設定モード

neighbor override-capability

OPEN メッセージのオプションによるケイパビリティ交渉の結果を自身のケイパビリティで上書きします。refresh コマンド後に有効になるコマンドです。

neighbor strict-capability-match と同時に設定することはできません。

設定例１　BGP ピア（10.0.0.1）のケイパビリティ情報を、本装置自身のケイパビリティ情報に書き換える

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 override-capability
```

コマンド書式

neighbor 〈IP アドレス〉 override-capability

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

ケイパビリティを上書きしません。

設定モード

BGP サービス設定モード

neighbor password

TCP MD5 認証オプション(RFC2385:Protection of BGP Sessions via the TCP MD5 Signature Option)を有効にします。
また、パスワード文字列として使用する文字列を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　パスワードを secret-bgp1 として、TCP MD5 認証オプションを有効にする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 192.168.1.1 password secret-bgp1
```

コマンド書式

neighbor 〈IP アドレス〉 password 〈パスワード〉 [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
パスワード	TCP MD5 認証オプションで使用するパスワードを設定します。	25 文字以内の文字列	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。 このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1:このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2:パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

TCP MD5 認証オプションを使用しません。

共有および装置固有暗号鍵について

secret オプションを指定した場合は、F シリーズ共通の鍵を使って暗号化するのに対して、private オプションを指定した場合は、装置固有の鍵を使って暗号化します。

そのため、private オプションは secret オプションに対してセキュリティ上、優れますが保守などにより装置の入れ替えが必要となった場合に、設定内容を他の装置に適用することが出来ません。

設定モード

BGP サービス設定モード

neighbor port

BGP ピアが使用するの TCP ポート番号を指定します。
本装置が、BGP のセッションを確立するために送信する BGP パケットは、このポート宛に送信します。

refresh コマンド後に有効になるコマンドです。

設定例１　BPG ピア（10.0.0.1）の TCP ポート番号を 179 番に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 port 179
```

コマンド書式

neighbor〈IP アドレス〉port〈TCP ポート番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
TCP ポート番号	指定している BGP ピアが使用する、BGP ポート番号。	0～65535	省略不可

この設定を行わない場合

179 番を使用します。

設定モード

BGP サービス設定モード

neighbor remote-as

BGP ピアの属する AS 番号を指定します。自身の AS 番号と同じ場合は I-BGP、異なる場合は E-BGP となります。
passive を指定した場合は、相手からの OPEN メッセージがあった場合に、OPEN メッセージを送付します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）と BGP セッションを確立する（相手 AS 番号は 100）

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 remote-as 100
```

コマンド書式

neighbor 〈IP アドレス〉 remote-as 〈AS 番号〉 [passive]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
AS 番号	指定している BGP ピアの AS 番号を設定します。	1～65535	省略不可
passive	相手からの OPEN メッセージを受信してから、OPEN メッセージを送信する際に指定します。	passive	起動直後に OPEN メッセージを送信する

この設定を行わない場合

BGP の通信を行なうことができません。

設定モード

BGP サービス設定モード

neighbor route-map

BGP ピアにルートマップを適用します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）間で、受信の際に Route-map（ルートマップ名：map1）を適用する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 route-map map1 in
```

コマンド書式

neighbor 〈IP アドレス〉 route-map 〈Route-map 名〉〈フィルタリング〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
Route-map 名	適用する Route-map の Route-map 名を指定します。	-	省略不可
フィルタリング	指定している BPG ピアから受信時(in)／指定している BPG ピアへの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

Route-map 制御を行ないません。

設定モード

BGP サービス設定モード

neighbor shutdown

設定されている BGP ピアを一時的に無効にします。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）を一時的に無効にする

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 shutdown
```

コマンド書式

neighbor 〈IP アドレス〉 shutdown

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

指定している BGP ピアは有効になります。

設定モード

BGP サービス設定モード

neighbor soft-reconfiguration inbound

ネイバから受信した経路情報をルーティングテーブルとは別に保持しておく場合に指定します。
通常の BGP では、BGP ピアに対して、UPDATE メッセージを再度送付してもらうメカニズムはありません。このコマンドを指定することにより、BGP ピアからの UPDATE メッセージにより取得した経路情報を保管しておくことができます。
なお、Route-Refresh ケイパビリティを使用すると、UPDATE メッセージの再送を要求することができます。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）からの UPDATE メッセージの内容を保持する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 soft-reconfiguration inbound
```

コマンド書式

neighbor 〈IP アドレス〉 soft-reconfiguration inbound

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

フィルタリングされた経路情報は保持しません。

設定モード

BGP サービス設定モード

neighbor strict-capability-match

OPEN メッセージのオプションによるケイパビリティ交渉の際に，ネイバから未サポートのオプションを受信した場合や，自身の指定するオプションをネイバが受け入れなかった場合は，BGP コネクションを確立しないよう設定します。
neighbor override-capability と同時に設定することはできません。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）とのケイパビリティ交渉が一致しなかった場合は、BGP コネクションを確立しない

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 strict-capability-match
```

コマンド書式

neighbor 〈IP アドレス〉 strict-capability-match

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

未サポートのケイパビリティを受信しても、BGP コネクションを確立します。

設定モード

BGP サービス設定モード

neighbor timers

特定の BGP ピアの各種タイマーをセットします。
KeepAlive 送信間隔と路情報を削除するまでの時間の設定と、コネクトタイマの設定に分けて行います。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）に対応する KeepAlive の送間隔を 10 秒、BGP ピアがいなくなってから経路情報を削除するまでの時間を 30 秒とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 timers 10 30
```

設定例２　BGP ピア（10.0.0.1）に対応するコネクトタイマを 100 秒に設定する

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 timers connect 100
```

コマンド書式

neighbor〈IP アドレス〉timers｛〈KeepAlive 送信間隔〉〈経路情報を削除するまでの時間〉｜ connect〈コネクトタイマ〉｝

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
KeepAlive 送信間隔	KeepAlive 送信間隔(単位:秒)を指定します。	0～65535	省略不可
経路情報を削除するまでの時間	経路情報を削除するまでの時間(単位:秒)を設定します。	0～65535	省略不可
コネクトタイマ	BGP コネクトタイマ(単位:秒)を設定します。	0～65535	省略不可

この設定を行わない場合

タイマの内容	デフォルト値
KeepAlive 再送間隔	60 秒
経路情報を削除するまでの時間	180 秒
connect	120 秒

設定モード

BGP サービス設定モード

neighbor transparent-as

AS PATH 属性に自身の AS 番号を付加しないように設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）には、自身の AS 番号をつけない

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 transparent-as
```

コマンド書式

neighbor 〈IP アドレス〉 transparent-as

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

自身の AS 番号がつけられます。

設定モード

BGP サービス設定モード

neighbor transparent-nexthop

NEXTHOP 属性をネイバのアドレスで上書きしないように設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）には、自身を NextHop として通知しない（自分のルーティングテーブルにある NextHop を通知）

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 transparent-nexthop
```

コマンド書式

neighbor 〈IP アドレス〉 transparent-nexthop

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

自身を NextHop として通知します。

設定モード

BGP サービス設定モード

neighbor update-source

BGP セッションの確立(OPEN メッセージ)の際、BGP の送信元アドレスに割り当てる IP アドレスを指定するために、インタフェースを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）との BGP パケットの送信元アドレスに、PPPoE1 のアドレスを利用する

```
Router(config)# router bgp 100
Router(config-bgp)#neighbor A.B.C.D update-source pppoe 1
```

コマンド書式

neighbor 〈IP アドレス〉 update-source 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
インタフェース名	BGP の送信元アドレスに使用するインタフェースアドレス。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

BGP パケットを実際に送信するインタフェースになります。

設定モード

BGP サービス設定モード

neighbor version

BGP ピアとの間で使用する BGP のプロトコルバージョンを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）との BGP で使用するバージョンを"4"とする

```
Router(config)# router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 version 4
```

コマンド書式

neighbor 〈IP アドレス〉 version 〈バージョン〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。		IPv4 アドレス形式	省略不可
バージョン	指定している BGP ピアの BGP のバージョンを指定します。		4 draft	省略不可
	4	BGP バージョン 4 を指定します。		
	draft	BGP バージョン 4 マルチプロトコル拡張ドラフト版を指定します。		

この設定を行わない場合

バージョン 4 となります。

設定モード

BGP サービス設定モード

neighbor weight

BGP ピアに重み付けを設定します。
同じ宛先への複数経路を学習した場合に、どの情報(どの BGP ピアからの)を有効とするかの指針として使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）の WEIGHT 値を"65535（優先度最高）"に設定する

```
Router(config)#router bgp 100
Router(config-bgp)# neighbor 10.0.0.1 weight 65535
```

コマンド書式

neighbor 〈IP アドレス〉 weight 〈Weight 値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP ピアの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
weight 値	指定している BGP ピアからの経路情報の優先度を指定します。 優先度は、0(最低)～65535(最高)の範囲で設定できます。	0～65535	省略不可

この設定を行わない場合

他の BGP ピアを通って学習した経路ではデフォルトの weight は 0、ローカルルータによって生成された経路ではデフォルトの weight は 32768 になります。

FITELnet-F シリーズの BGP 最適経路選択

FITELnet-F シリーズの BGP では、以下の順で最適経路の選択を行ないます。

優先順位	属性	内容
1	NEXT_HOP 属性	NEXT_HOP 属性で指定された NEXT_HOP への経路がない場合は無効経路となる
2	WEIGHT 値	BGP ピアに設定した WEIGHT 値により、WEIGHT 値の大きい BGP ピアからの情報が優先される
3	LOCAL_PREF 属性	LOCAL_PREF 値の大きい経路が優先される
4	LOCAL	FITELnet-F シリーズが生成した BGP 経路が優先される
5	AS_PATH 属性	AS_PATH 長が短い経路が優先される。ただし、bgp bestpath as-path ignore コマンドが設定されている場合は、AS_PATH 長を考慮しない
6	ORIGIN 属性	ORIGIN 属性の優先度は IGP＞EGP＞incomplete
7	MED 値	MED 値の小さい経路が優先される
8	E-BGP or I-BGP	BGP のピアタイプの優先度は、E-BGP > I-BGP
9	IGP メトリック	NEXT_HOP 属性で指定された NEXT_HOP へのメトリック値が小さい経路が優先される
10	router-id	ピアの router-id 値の小さい経路が優先される。ただし bgp bestpath compare-routerid が指定されている場合に限ります。

設定モード

BGP サービス設定モード

network

BGP の経路情報として通知するプレフィックスをスタティックで登録します。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0/24 の経路情報を BGP で通知する

```
Router(config)#router bgp 100
Router(config-bgp)# network 192.168.0.0 255.255.255.0
```

コマンド書式

network〈IP アドレス〉〈ネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP を運用するインタフェースを、インタフェースの IP アドレスで指定します。	IPv4 アドレス形式	省略不可
ネットマスク	BGP を運用するインタフェースを、IP アドレスとネットマスクの組み合わせで指定することもできます	IPv4 アドレス形式	省略不可
backdoor	backdoor オプションをつけた場合は、この経路をローカル BGP 経路として扱います。ローカル BGP 経路の distance 値は、distance bgp コマンドで設定します	backdoor	External 経路、もしくは Internal 経路として扱う。(External/Internal は、BGP ピアによる)

この設定を行わない場合

自分の経路情報を通知します(redistribute コマンドの内容に従います。)

設定モード

BGP サービス設定モード

redistribute

BGP 以外の手段で取得した経路情報のうち、BGP で再配布する経路を選択し必要に応じて適用する Route-map を指定します。
ただし、経路情報に変化が無い場合は再配布が行われないため、追加した経路情報を再配布するためには、clear ip bgp redistribute コマンドを実行してください。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックで登録した経路情報を BGP で再配布する

```
Router(config)#router bgp 100
Router(config-bgp)# redistribute static
```

設定例２　RIP で取得した経路情報を BGP で再配布する

```
Router(config)#router bgp 100
Router(config-bgp)#redistribute rip
```

コマンド書式

redistribute 〈再配布する経路情報〉 [route-map 〈Route-map 名〉]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>再配布する経路情報</td><td>BGP 以外の手段で取得した経路情報のうち、BGP で再配布するものを指定します。
<table><tr><td>connected</td><td>直接経路</td></tr><tr><td>event-action</td><td>イベントアクションで追加した経路情報</td></tr><tr><td>kernel</td><td>kernel にセットされた経路情報</td></tr><tr><td>local-prot1</td><td rowspan="2">SA-UP ルート情報</td></tr><tr><td>local-prot2</td></tr><tr><td>ospf</td><td>OSPF で取得した経路情報</td></tr><tr><td>rip</td><td>RIP で取得した経路情報</td></tr></table></td><td>connected
event-action
kernel
local-prot1
local-prot2
ospf
rip
static</td><td>省略不可</td></tr>
<tr><td>Route-map 名</td><td>必要に応じて、適用する Route-map を指定します。</td><td>-</td><td>Route-map を適用しない</td></tr>
</table>

この設定を行わない場合

BGP で受信した情報のみを広告します。

設定モード

BGP サービス設定モード

フィルタリングの設定

access-list

特定のパケットと、そのパケットの動作（中継 or 廃棄 or 学習フィルタリング）を指定します。refresh コマンド後に有効になるコマンドです。

指定したパケットは、以下の機能で使用します。

・フィルタリング（ip access-group コマンド）
・学習フィルタリング（ip access-group コマンド）
・オフセットリスト（offset-list コマンド）
・RIP/BGP で送信するメトリック値の指定（distance コマンド）
・BGP で送信する経路の指定（neighbor <IP-address> distribute-list コマンド）
・経路情報の指定（match ip address コマンド）
・NextHop の指定（match ip nexthop コマンド）
・NAT 変換前のアドレス指定（ip nat inside コマンド）
・使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、指定したアクセスリスト番号を指定します。

refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。
この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク（Wildcard マスク）を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。
例1）24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合：0.0.0.255
サブネットマスクの場合：255.255.255.0
例2）ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合：0.0.0.0
サブネットマスクの場合：255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング／学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。

本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例１　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する（許可属性）

```
Router(config)# access-list 1 permit 192.168.100.0 0.0.0.255
```

設定例２　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する（不許可属性）

```
Router(config)# access-list 100 deny ip 192.168.100.0 0.0.0.255
192.168.200.0 0.0.0.255
```

設定例３　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する（許可属性）

```
Router(config)# access-list 3000 permit 3ffe:110::/64
3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt 0 any eq 80
```

設定例５　学習フィルタリングを指定する（IPv4）

```
Router(config)# access-list 100 dynamic permit ip any any
```

コマンド書式

IPv4 標準アクセスリスト（アクセスリスト番号：1～99、1300～1999）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（アクセスリスト番号：100～199、2000～2699）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence {<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（アクセスリスト番号：3000～3499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（アクセスリスト番号：3500～3999）access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> } [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	それぞれの属性の番号を指定します。	1～99、1300～1999	IPv4 標準アクセスリスト	省略不可
		100～199、2000～2699	IPv4 拡張アクセスリスト	
		3000～3499	IPv6 標準アクセスリスト	
		3500～3999	IPv6 拡張アクセスリスト	
dynamic	学習フィルタリングを使用する場合に指定します。	dynamic		学習フィルタリングのエントリではない

{ permit | deny }	許可属性か、不許可属性かを選択します。	permit: 許可属性 deny: 不許可属性	省略不可
プロトコル番号	プロトコル名もしくはプロトコル番号を選択します。	gre: Cisco's GRE tunneling icmp: ICMP(IPv4 拡張アクセスリスト時) icmpv6: ICMPv6(IPv6 拡張アクセスリスト時) ip: IP ipinip: IP トンネル tcp: TCP udp: UDP 0～255: プロトコル番号を指定	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。	any	–
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
host	IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	–
送信元 IPv6 プレフィックス	送信元 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
宛先 IPv6 プレフィックス	宛先 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
ICMP タイプ	プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。	指定できる ICMP タイプ administratively-prohibited alternate-address	全ての ICMP タイプ

		dod-host-prohibited dod-net-prohibited echo echo-reply general-parameter-problem host-isolated host-precedence-unreachable host-redirect host-tos-redirect host-tos-unreachable host-unknown host-unreachable information-reply information-request mask-reply mask-request mobile-redirect net-redirect net-tos-redirect net-tos-unreachable net-unreachable network-unknown no-room-for-option option-missing packet-too-big parameter-problem port-unreachable precedence-unreachable protocol-unreachable reassembly-timeout redirect router-advertisement router-solicitation source-quench	

		time-exceeded timestamp-reply timestamp-request traceroute ttl-exceeded unreachable	
ICMPv6 タイプ（IPv6）	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	ICMPv6 タイプ address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値（0～255）	全ての ICMPv6 タイプ

ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。	eq: 指定するポートが対象 gt: 指定するポート番号より大きいポート番号が対象 lt: 指定するポート番号より小さいポート番号が対象 neq: 指定するポート番号以外のポート番号が対象 range: ポートの範囲を指定する	全てのポート（以降設定なし）
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号 bgp chargen cmd daytime discard domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3	全ての TCP ポート番号

		sunrpc syslog tacacs tacacs-ds talk telnet time uucp whois www TCP ポート番号(0～	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号 biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk tftp	全ての UDP ポート番号

		time who xdmcp UDP ポート番号(0～65535)	
precedence-value※	precedence-value を設定します。	0～7	省略不可
precedence-named-value※	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) etwork(7)	省略不可
tos-value※	tos-value を設定します。	0～15	省略不可
tos-named-value※	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value※	dscp-value を設定します。	0～63	省略不可
dscp-named-value※	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b) af43(100110b)	省略不可

ip-flag-value※	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3(ワイルドカードマスク)	省略不可
tcp-flag-value※	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63(ワイルドカードマスク)	省略不可
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255(ワイルドカードマスク)	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

最大エントリ数:ip access-group で関連付けた access-list に対して、最大 1024 エントリ
装置全体で 1024 エントリ
ipv4, ipv6 の区別無く、装置全体で最大 1024 エントリ
各インターフェース毎の制限無く、装置全体で最大 1024 エントリ

※:これらのパラメータをフィルタリングで使用する事はできません。

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースで適用します。
フィルタリングデータは、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースで受信したパケットに適用するのか、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。(ダイヤルアップは除く)

設定例１　access-list 1 で指定したデータを、LAN 送信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、LAN からの受信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>access-list 番号</td><td>フィルタリングのデータを設定したアクセスリストの番号を指定します。</td><td><1-99>
<100-199>
<1300-1999>
<2000-2699></td><td>省略不可</td></tr>
<tr><td>{ in[interface | vpn]| out }</td><td>インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。
受信時は、さらに以下のように設定ができます。
<table>
<tr><td>in</td><td>access-list に従い制御</td></tr>
<tr><td>in vpn</td><td>自局宛 VPN 対象パケットを制御</td></tr>
<tr><td>in interface</td><td>自局宛非 VPN 対象パケットを制御</td></tr>
</table></td><td>in
out</td><td>省略不可</td></tr>
</table>

※LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
※in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。

設定例　学習フィルタリングテーブルを 16384 セッション分設定する

```
Router(config)#ip stateful max-sessions 16384
```

コマンド書式

ip stateful max-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～16384	省略不可

この設定を行わない場合

学習フィルタリングテーブルの最大数は、2048 になります。

設定モード

基本設定モード

スタティックルーティングの設定

ip route

本装置の、IPv4 スタティックルートを指定します。
PPPoE や EWAN 使用する場合は、Nexthop の IP アドレスがわからないケースがありますので、Nexthop としてインタフェースを指定することもできます。
Nexthop として EWAN インタフェースを指定できるのは、WAN 側の運用形態が DHCP クライアントの場合のみです。
この場合、"nexthop"は DHCP サーバから取得した"default gateway の IP アドレス"となります。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.1.0/24 宛の Nexthop を 192.168.2.254 とする場合

```
Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.254
```

設定例２　192.168.1.0/24 宛の Nexthop を、PPPoE1 インタフェースとする場合

```
Router(config)#ip route 192.168.1.0 255.255.255.0 pppoe 1
```

設定例３　デフォルトルートを PPPoE１インタフェースとする場合

```
Router(config)#ip route 0.0.0.0 0.0.0.0 pppoe 1
```

コマンド書式

```
ip route <宛先ネットワーク> <マスク> { <NextHop> | <インタフェース名>|
        connected { ipsecif <1-500> | null 0 } lan <1-1> | ewan <1-2> | vlan
        <1-16>}  [<distance>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先ネットワーク	スタティックルーティングの宛先ネットワークアドレス	IPv4 アドレス形式	省略不可
マスク	宛先ネットワークに対するマスク	IPv4 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IP アドレス	IPv4 アドレス形式	インタフェース名を設定する必要があります。
インタフェース名	宛先へ到達するためのインタフェース名 PPPoE のように、NextHop の IP アドレスが明確にわからない場合に指定します。	ewan 1～2 pppoe 1～24※1 tunnel 1～32	NextHop の IP アドレスを設定する必要があります。
connected ipsecif <1-500>	宛先への経路として、IPsec インタフェースを指定します。	ipsecif 1～500※2	
connected null 0	廃棄用の宛先経路情報とします	null 0	
connected lan <1-1>	宛先を LAN インタフェースの connected として扱います。	lan 1～1	
connected ewan <1-2>	宛先を EWAN インタフェースの connected として扱います。	ewan 1～2	
connected vlan <1-16>	宛先を VLAN インタフェースの connected として扱います。	vlan 1～16	
distance	スタティックルーティングの distance 値を指定します。	2～255※3	1

最大エントリ数
F80/F100:256 エントリ(ルーティングテーブル自体は 512 エントリ)
F1000:1024 エントリ(ルーティングテーブル自体は 2048 エントリ)

※1:F80 の場合は、1～5
※2:F80 の場合は、1～32、
F100 の場合は、1～100 になります。
※3:distance 値に 255 を設定した場合、その経路情報は無効扱いとなります。

この設定を行わない場合

スタティックルーティングは設定されません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

基本設定モード

ルートマップの設定

set ip next-hop

経路情報の nexthop を設定します。
BGP の場合は、NEXT-HOP 属性として設定値を通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、NEXT-HOP 属性として、192.168.100.1 をつけて送信する（ルートマップ名 : map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set ip next-hop 192.168.100.1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set ip next-hop <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP の Next-Hop 属性に設定する IP アドレスを設定します	IPv4 アドレス形式	省略不可

この設定を行わない場合

Next-Hop 属性を操作しません。

設定モード

Route-map 設定モード

set metric

経路情報の metric 値／MED 値を設定します。
BGP の場合は、MULTI-EXIT-DISCRIMINATOR 属性として設定値を通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1)には、MED 値（300）で UPDATE 情報を送信する

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set metric 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set metric <メトリック値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	RIP や BGP で使用するメトリック値/MED 値を指定します。	1～4294967295	省略不可

この設定を行わない場合

メトリック値を操作しません。

設定モード

Route-map 設定モード

set aggregator

この Route-MAP に該当した経路情報の Aggregator 属性および Aggregator AS／Aggregator Origin IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、Aggregator 属性をつけて UPDATE 情報を送信する (AggregatorAS=100、Aggregator Origin=192.168.100.1)

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set aggregator as 100
192.168.100.1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set aggregator as <AS 番号> <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS 番号	AggregatorAS の AS 番号を設定します。	1～65535	省略不可
IP アドレス	Aggregator Origin の IP アドレスを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

Aggregator 属性を操作しません。

設定モード

Route-map 設定モード

set as-path prepend

経路情報の AS-PATH 属性を追加します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、AS-PATH 属性として、300 をつけて送信する（ルートマップ名 : map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set as-path prepend 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set as-path prepend <AS 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AS 番号	AS-PATH 属性に付加する AS 番号を設定します。	1～65535	省略不可

この設定を行わない場合

AS-PATH 属性を操作しません。

設定モード

Route-map 設定モード

set atomic-aggregate

経路情報の ATOMIC-AGGREGATE 属性を追加します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、ATOMIC-AGGREGATE 属性をつけて送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set atomic-aggregate
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set atomic-aggregate

パラメータ

パラメータはありません。

この設定を行わない場合

ATOMIC-AGGREGATE 属性を追加しません。

設定モード

Route-map 設定モード

set community

COMMUNITY 属性を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、COMMUNITY 属性として"no-export"を設定する（ルートマップ名 : map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set community no-export
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set community 〈コミュニティ属性値〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
コミュニティ属性値	追加するコミュニティ属性値を設定します。		local-AS no-advertise no-export A:B	省略不可
	local-AS	NO-EXPORT-SUBCONFED コミュニティ		
	no-advertise	NO-ADVERTISE 属性		
	no-export	NO-EXPORT 属性		
	A:B	コミュニティ値を設定		

この設定を行わない場合

コミュニティ属性を操作しません。

設定モード

Route-map 設定モード

set community-additive

BGP COMMUNITIES 属性を設定します。set community が、BGP COMMUNITIES 属性の置換であるのに対し、set community-additive は追加することができます。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、COMMUNITY 属性として"no-advertise"を追加する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set community-addtive no-advertise
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set community-addtive 〈コミュニティ属性値〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
コミュニティ属性値	追加するコミュニティ属性値を設定します。		local-AS no-advertise no-export A:B	省略不可
	local-AS	NO-EXPORT-SUBCONFED コミュニティ		
	no-advertise	NO-ADVERTISE 属性		
	no-export	NO-EXPORT 属性		
	A:B	コミュニティ値を設定		

この設定を行わない場合

コミュニティ属性を追加しません。

設定モード

Route-map 設定モード

set local-preference

経路情報の LOCAL_PREF 属性および LOCAL_PREF 値を指定します。
BGP で経路を通知する際の、LOCAL_PREF 値となります。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、LOCAL_PREF (300) で UPDATE 情報を送信する

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set local-preference 300
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set local-preference <LOCAL-PREF 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LOCAL-PREF 値	指定する BGP のローカルプリファレンス値を設定します。	0～4294967295	省略不可

この設定を行わない場合

ローカルプリファレンス値を操作しません。

設定モード

Route-map 設定モード

set origin

この Route-MAP に該当した経路情報の ORIGIN 属性を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、ORIGIN 属性として"EGP"を設定する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set origin egp
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set origin <ORIGIN 属性>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ORIGIN 属性	BGP の ORIGIN アトリビュートにセットする ORIGIN 属性を指定します。 egp：EGP を設定する igp：IGPを設定する incomplete：INCOMPLETE を設定する	egp igp incomplete	省略不可

この設定を行わない場合

ORIGIN 属性を変更しません。

設定モード

Route-map 設定モード

set originator-id

Originator-ID をセットします。
Originator-ID とは、プレフィックス情報を生成したルータの IP アドレスを意味します。

refresh コマンド後に有効になるコマンドです。

設定例１　Originator-ID に、192.168.1.1 をセットする

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set originator-id 192.168.1.1
```

コマンド書式

set originator-id 〈IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	BGP の Originator-ID にセットする IP アドレスを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

Originator-ID を変更しません。

設定モード

Route-map 設定モード

set tag

AS 外部経路のタグ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　AS 外部経路のタグ値を 150 とします

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set tag 150
```

コマンド書式

set tag <タグ値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タグ値	AS 外部経路のタグ値を指定します。	0～4294967295	省略不可

この設定を行わない場合

External Route Tag には 、0 が設定されます。

設定モード

Route-map 設定モード

set weight

BGP ピアから受信した経路情報の weight 値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア（10.0.0.1）の Weight 値を 65535（最優先）にする

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#set weight 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

set weight <weight 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
weight 値	BGP の Weight 値にセットする値を設定します。 WEIGHT 値の大きい BGP ピアからの情報が優先されます。	0～65535	省略不可

この設定を行わない場合

weight 値は 0 となります。

設定モード

Route-map 設定モード

match interface

経路情報に対して、パケット送信インタフェースを特定します。
この設定は、RIP に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例１　スタティックルートについて EWAN1 から送信するもののみ RIP 広告（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match interface ewan 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router rip
Router(config-rip)#redistribute static route-map map1
Router(config-rip)#exit
```

コマンド書式

match interface〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	特定するインタフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

パケット送信インタフェースの特定を行いません。

設定モード

Route-map 設定モード

match ip address

access-list(standard)に指定した IP アドレスを特定します。
この設定は、RIP および BGP に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、"192.168.1.0"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ip address 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

match ip address <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	IP アドレスに一致する access-list 番号を指定します	1～99 1300～1999	省略不可

設定モード

Route-map 設定モード

match ip next-hop

Next-Hop を指定し、経路を特定します。
この設定は、RIP および BGP に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、Next-Hop が"192.168.10.1"の情報のみ送信する（ルートマップ名：map1）

```
Router(config)#access-list 1 permit 192.168.10.1 0.0.0.0

Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match ip next-hop 1
Router(config-rmap map1 permit 1)#exit

Router(config)#router bgp 100
Router(config-bgp)#neighbor 10.0.0.1 route-map map1 out
```

コマンド書式

match ip next-hop <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	Next-hop に一致する access-list 番号、または IP アドレスを指定します。	1～99 1300～1999 IPv4 アドレス形式	省略不可

設定モード

Route-map 設定モード

match metric

metric に一致する経路を特定します。
この設定は、RIP および BGP に対して有効となります。

refresh コマンド後に有効になるコマンドです。

設定例１　BGP ピア(10.0.0.1) には、メトリック値=3 で保持している経路情報のみ送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match metric 3
Router(config-rmap map1 permit 1)#exit


Router(config)#router bgp 100
Router(config-bgp)#redistribute connected route-map map1
```

コマンド書式

match metric <メトリック値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
メトリック値	メトリック値に一致する経路を特定します。	0～4294967295	省略不可

設定モード

Route-map 設定モード

リゾルバの設定

ip name-server

本装置で、DNS リゾルバを動作させる場合に、DNS サーバの IP アドレスを設定します。
DNS リゾルバとは、名称から IP アドレスを獲得するために、DNS サーバにリクエストをする機能です。
DNS サーバは、プライマリ/セカンダリが設定できます。コマンドでは、プライマリ・セカンダリの順に IP アドレスを入力します。

設定例　プライマリ DNS サーバに xxx.xxx.xxx.1、セカンダリ DNS サーバに xxx.xxx.xxx.2 を設定する

```
Router(config)#ip name-server xxx.xxx.xxx.1
Router(config)#ip name-server xxx.xxx.xxx.2
```

コマンド書式

ip name-server 〈DNS アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DNS アドレス	DHCP で通知するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式	省略不可

最大エントリ数:3 エントリ(ipv4,ipv6 合わせて3エントリ)

※ DNS アドレスの優先度は、入力した順に3つまで有効になります。
すでに、3つ入力されている状態で4つ目以降を入力しても設定上無効となります。

この設定を行わない場合

DNS リゾルバを使用することはできません。ただし、PPPoE や DHCP クライアント機能で、DNS の IP アドレスを学習している場合は、DNS リゾルバ機能を使用できます。

DNS リゾルバとは・・・

FITELnet-F シリーズから送信(中継ではない)データに関して、ホスト名が指定されている場合に、DNS サーバに問い合わせを行なう機能です。
FITELnet-F シリーズから送信するデータには、以下の種類があります。

・ping
・traceroute
・SMTP
・SNMP
・syslog
・telnet クライアント

があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]


Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名(www)宛の ping を実行すると、DNS サーバ(xxx.xxx.xxx.1)に問い合わせを行い、ホスト名(www.xxxxxx.ne.jp)から IP アドレス(xxx.xxx.xxx.xxx)を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名(www.xxxxxx.ne.jp)が IP アドレス(xxx.xxx.xxx.xxx)であることが確認できます。

設定モード

基本設定モード

ip name-server source-interface

DNS リゾルバを使用する場合の、DNS サーバへ送出する送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例 1　DNS サーバへ送信する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#ip name-server source-interface lan 1
```

コマンド書式

ip name-server source-interface 〈インタフェース名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DNS サーバへ送信する際の送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

DNS サーバへ実際に送信するインタフェースになります。

設定モード

基本設定モード

ip domain-name

FITELnet-F シリーズで、DNS リゾルバを動作させる場合に、ドメイン名を付加する場合に設定します。
DNS リゾルバとは、名称から IP アドレスを獲得するために、DNS サーバにリクエストをする機能です。
ここで、ドメイン名を指定した場合、DNS にて IP アドレスを解決する際、ホスト名の後にここで設定したドメイン名をつけて、DNS サーバにリクエストします。

例)
ip domain-name xxxxx.ne.jp と設定して、"ping xyz"とした場合、DNS サーバには、xyz.xxxxx.ne.jp の IP アドレスを解決するようリクエストします。

設定例　DNS リゾルバで使用するドメイン名を"xxxxxx.ne.jp"に設定する

```
Router(config)#ip domain-name xxxxxx.ne.jp
```

コマンド書式

ip domain-name 〈ドメイン名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DNS リゾルバで通知する際に付加するドメイン名称	254 文字以内の文字列	省略不可

この設定を行わない場合

DNS リゾルバ使用時に、ドメイン名を付加することはできません。

DNS リゾルバとは・・・

FITELnet-F シリーズから送信(中継ではない)データに関して、ホスト名が指定されている場合に、DNS サーバに問い合わせを行なう機能です。
FITELnet-F シリーズから送信するデータには、以下の種類があります。

- ping
- traceroute
- SMTP
- SNMP
- syslog
- telnet クライアント

があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]


Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名(www)宛の ping を実行すると、DNS サーバ(xxx.xxx.xxx.1)に問い合わせを行い、ホスト名(www.xxxxxx.ne.jp)から IP アドレス(xxx.xxx.xxx.xxx)を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名(www.xxxxxx.ne.jp)が IP アドレス(xxx.xxx.xxx.xxx)であることが確認できます。

設定モード

基本設定モード

ip resolver-cache-time

本装置で DNS リゾルバを動作させる場合に、学習した DNS 情報を保持しておく時間を設定します。

設定例１　DNS 情報を保持しておく時間を 30 秒に設定する

```
Router(config)#ip resolver-cache-time 30
```

コマンド書式

ip resolver-cache-time <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	DNS 情報を保持しておく時間(秒)	0～3600	省略不可

この設定を行わない場合

DNS 情報を保持しません。

DNS リゾルバとは・・・

FITELnet-F シリーズから送信(中継ではない)データに関して、ホスト名が指定されている場合に、DNS サーバに問い合わせを行なう機能です。
FITELnet-F シリーズから送信するデータには、以下の種類があります。

- ping
- traceroute
- SMTP
- SNMP
- syslog
- telnet クライアント

があります。
ping / traceroute を実行する場合はコマンドのオプションで、SMTP/SNMP の場合はサーバの設定にホスト名を指定しても、DNS リゾルバ機能を使用して IP アドレスを解決し、通信を行なうことができます。
DNS リゾルバで取得した IP アドレスの情報は、"show ip resolver-cache"コマンドで確認することができます。

実行例

```
Router#ping www
Sending 5, 100-byte ICMP Echos to xxx.xxx.xxx.xxx, timeout is
2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/4/10 ms

Router#show ip resolver-cache

<resolver dns table>
1th direction = [1] (name to addr)
IPv4 Address = [xxx.xxx.xxx.xxx]
Hostname = [www.xxxxxx.ne.jp]


Router#
```

ip name-server に xxx.xxx.xxx.1／ip domain-name に xxxxxx.ne.jp が設定されている場合に、ホスト名（www）宛の ping を実行すると、DNS サーバ（xxx.xxx.xxx.1）に問い合わせを行い、ホスト名（www.xxxxxx.ne.jp）から IP アドレス（xxx.xxx.xxx.xxx）を解決し、ping を送信します。
show ip resolver-cache コマンドで、ホスト名（www.xxxxxx.ne.jp）が IP アドレス（xxx.xxx.xxx.xxx）であることが確認できます。

設定モード

基本設定モード

ip resolver-retries

本装置で、DNS リゾルバを動作させる場合の、リゾルバ問合せのリトライ回数、リトライ間隔(秒)、リクエストタイムアウト(秒)、タイムアウト(秒)を指定します。

設定例１　DNS リゾルバの問い合わせを、リトライ回数 5 回、リトライ間隔 2 秒、リクエストタイムアウト 10 秒、タイムアウト 20 秒に設定する

```
Router(config)#ip resolver-retries 5 interval 2 request-timeout
10 timeout 20
```

コマンド書式

ip resolver-retries (リトライ回数) interval (リトライ間隔) request-timeout (request-timeout 時間) timeout (timeout 時間)

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	リゾルバ問い合わせ回数を設定します。	0～5	省略不可
リトライ間隔	リゾルバ問い合わせ間隔を設定します。	1～5	省略不可
request-timeout 時間	リゾルバ問い合わせリクエストタイムアウトを設定します。	1～60	省略不可
timeout 時間	リゾルバ問い合わせタイムアウトを設定します。	1～60	省略不可

この設定を行わない場合

リトライ回数 3 回、リトライ間隔) 、リクエストタイムアウト 5 秒、タイムアウト 10 秒に設定します。

設定モード

基本設定モード

MTU長

ip mtu

インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　PPPoE1 の MTU 長を 1400byte にする

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	LAN:256～1500 PPPoE:578～1492 EWAN:256～1500 BRI:253～1500(F100 のみ) VLAN:256～1500 IPsec:576～1500 Tunnel:256～1500	省略不可

この設定を行わない場合

各インタフェースにより以下のようになります。通常は変更の必要はありません。

LAN:1500
PPPoE:1454
EWAN:1454
BRI:1500(F100 のみ)
VLAN:1500
IPsec:1390
Tunnel:1480

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
BRI インタフェース設定モード（F100 のみ）
VLAN インタフェース設定モード
IPsec インタフェース設定モード
トンネルインタフェース設定モード

TCP MSS

mss

インタフェースの MSS 値を指定します。
FITELnet-F シリーズでは、TCP ヘッダオプションに含まれる MSS 値を適切な値に書き換えることができます。
パケットに書かれている値と設定値を比較して小さい方の値にします。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN の MSS 値を 1300byte にする

```
Router(config)#mss lan 1 1300
```

コマンド書式

mss〈インタフェース名〉〈MSS 値〉
mss ipsec〈MSS 値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	インタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24※1 ipsecif 1～500※2 tunnel 1～32 vlanif 1～16	省略不可
MSS 値	MSS 値を指定します。 off を指定した場合は、MSS 値を変更しません。 ipseif の場合は、VPN セレクタの MSS 値を指定します。※3	1240～1460※4 off	省略不可

※1:F80 の場合は、1～5 になります。
※2:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。
※3:IPsec interface 以外に提供される VPN セレクタの MSS 値の指定となります。
※4:ipsec、tunnel、pppoe の各設定値の上限は、ipsec 1420、tunnel 1440、pppoe 1452 となります。

この設定を行わない場合

各インタフェースからパケットを送出する際に、下記の値とパケットに書かれている値を比較して小さい方の値にします。通常は変更の必要はありません。

LAN interface：MTU 長 -40
EWAN interface：MTU 長 -40
PPPoE interface：MTU 長 -40
IPsec interface：MTU 長 -40
IPsec VPN selector：(送信 IF の MTU)-113
Tunnel interface：MTU 長 -40
VLANIF interface：MTU 長 -40

MSS 長とは？

MSS (Maximum Segment Size)とは、TCP で一度に伝送できるデータの最大量、最大セグメントサイズ。

設定モード

基本設定モード

ProxyARPの設定

ip proxy-arp

インタフェースで ProxyARP を動作させる場合に指定します。

refresh コマンド後に有効になるコマンドです。(VLAN インタフェース設定モードのみ)

設定例１　LAN インタフェースで ProxyARP 機能を動作させる

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip proxy-arp
```

コマンド書式

```
ip proxy-arp [include-default-route]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
include-default-route	デフォルトルートにヒットするあて先の ARP Request に対して、ProxyARP を行う場合に指定します。	include-default-route	デフォルトルートのみにヒットするあて先への ARP Request に対しては ProxyARP しない。

この設定を行わない場合

ProxyARP 機能が動作しません。

ProxyARP 機能とは？

自身が中継すべき相手の IP アドレスに対する ARP を受信した際に、代理にその ARP に答える機能を ProxyARP 機能といいます。
BRI インタフェースで、LAN と同一サブネットの IP アドレスを払い出すようなケースでは、ProxyARP を使用する必要があります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ARP制御の設定

ip arp 802.1p

ARP パケット(リクエスト/リプライ)の、出力時の 802.1p 値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例　ARP パケット出力時の 802.1p 値を 6 とする

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp 802.1p 6
```

コマンド書式

ip arp 802.1p <802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
802.1p 値	ARP パケット出力時の 802.1p 値を設定します。	0～7	省略不可

この設定を行わない場合

ARP パケット出力時の 802.1p 値を 0 とします。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp learning

受信した ARP により、ARP テーブルを登録するかどうかの設定をします。

refresh コマンド後に有効になるコマンドです。

設定例　ARP テーブルの登録を行わない

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp learning disable
```

コマンド書式

ip arp learning 〈登録設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
登録設定	受信した ARP により、ARP テーブルを登録するかどうかの指定をします。 enable：ARP の登録を行う disable：ARP の登録を行わない request：ARP リクエストでのみ登録を行う reply：ARP リプライでのみ登録を行う	enable disable request reply	省略不可

この設定を行わない場合

ARP リクエストおよびリプライにより、ARP テーブルの登録を行います。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp reply

ARP リクエストに応答するかどうかを設定します。
ARP テーブルで管理されている相手からのみ応答する制御を行うことにより、管理外の端末からのデータ中継を行わない制御が可能になります。

refresh コマンド後に有効になるコマンドです。

設定例　ARP テーブルに登録されている IP アドレスからの ARP リクエストにのみ応答する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp reply authorized
```

コマンド書式

ip arp reply 〈応答設定〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
応答設定	ARP リクエストに応答するかどうかを設定します。		enable disable authorized	省略不可
	enable	ARP Reply を送信する		
	disable	ARP Reply を送信しない		
	authorized	ARP テーブルに存在する IP アドレスからの ARP リクエストにのみ応答する		

この設定を行わない場合

全ての ARP リクエストに応答します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp request

ARP リクエストを送信するかどうかの設定をします。
全ての端末をスタティック ARP で管理するような場合は、ARP リクエストの送信を行わない運用が効

ip_error-ratelimit.htm

果的です。

refresh コマンド後に有効になるコマンドです。

設定例　ARP リクエストを送信しない

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip arp request disable
```

コマンド書式

ip arp request〈送信設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信設定	ARP リクエストを送信するかどうかの指定をします。 enable：ARP リクエストを送信する disable：ARP リクエストを送信しない	enable disable	省略不可

この設定を行わない場合

ARP リクエストを送信する。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ip arp static

スタティック ARP で使用する、IP アドレスと MAC アドレスの組み合わせを設定します。

refresh コマンド後に有効になるコマンドです。

設定例　IP アドレス（192.168.10.1）とＭＡＣアドレス（xxxx.xxxx.xxxx）をスタティック ARP に登録する

```
Router(config)#ip arp static 192.168.10.1 xxxx.xxxx.xxxx
```

コマンド書式

ip arp static 〈IP アドレス〉〈MAC アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	スタティック ARP で使用する、IP アドレスと MAC アドレスを指定します。	IPv4 アドレス形式	省略不可
MAC アドレス		MAC アドレス形式	省略不可

最大エントリ数：学習エントリとスタティックエントリあわせて 512 エントリ。

この設定を行わない場合

スタティック ARP を登録しません。

設定モード

基本設定モード

ip arp timeout

ARP テーブルのエージアウト時間を設定します。
ARP タイムアウト値を変更後 refresh した際は、ARP エントリを全て初期化します。

refresh コマンド後に有効になるコマンドです。

設定例　ARP のエージアウトを 30 分とする

```
Router(config)#ip arp timeout 30
Router(config)#
```

コマンド書式

ip arp timeout 〈ARP タイムアウト値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ARP タイムアウト値	ARP テーブルのエージアウト時間(単位:分)を設定します。	1～60	省略不可

この設定を行わない場合

ARP タイムアウト値を 20 分とします。

設定モード

基本設定モード

ダイレクトブロードキャストの設定

ip directed-broadcast

インタフェースのネットワークブロードキャストアドレス宛の中継パケットを、ブロードキャストパケットとして中継する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースに対して、ダイレクトブロードキャストを行う。

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip directed-broadcast
```

コマンド書式

ip directed-broadcast

パラメータ

パラメータはありません。

この設定を行わない場合

インタフェースのネットワークブロードキャストアドレス宛の中継パケットは、廃棄します。

ダイレクトブロードキャスト機能とは？

中継パケットにおいて、インタフェースのネットワークブロードキャストアドレス宛のパケットを、そのインタフェースの配下の端末に対してブロードキャスト中継する機能を、ダイレクトブロードキャストといいます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

ICMP制御の設定

ip icmp error-ratelimit

本装置が、ICMP を使ってエラーを送信する際の、1 秒間に送信する最大送信パケット数を設定します。1 秒間に送信するパケット数が規定数を超過した場合に、次の 1 秒まで送信を抑止します。
0 を指定した場合、ICMP エラーメッセージおよび REDIRECT メッセージは送信されません。
エラーパケットにより、データ通信のための帯域が減ってしまうのを防ぐ機能です。

refresh コマンド後に有効になるコマンドです。

設定例１　エラーパケットを、最大 300 パケット/秒とする

```
Router(config)#ip icmp error-ratelimit 300
```

コマンド書式

ip icmp error-ratelimit <パケット数>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケット数	IP ICMP でエラーを送信する際の 1 秒間に送信する最大送信パケット数を設定します。unlimit を指定することで、ICMP エラーメッセージおよび REDIRECT メッセージのレート制限を行いません。	0～2147483647 unlimit	省略不可

この設定を行わない場合

100 パケット/秒が設定されます。

IP ICMP エラーパケットの種類

IP ICMP エラーパケットには、以下の種類があります。

Type	内容
3	受信したパケットの宛先への中継ができない
4	資源不足のため、パケットを廃棄
5	中継先を別のルータに変更したことを通知
11	ホップ数が制限を越えたため、転送できない
12	IPv4 ヘッダ(オプションを含む)が異常、もしくは未知

設定モード

基本設定モード

ip source-quench

ICMPv4 もしくは、SourceQuench を受信した際に、TCP ウィンドウ制御に反映するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SourceQuench を受信した場合、TCP ウィンドウ制御に反映する

```
Router(config)#ip source-quench enable
```

コマンド書式

ip source-quench 〈ウィンドウ制御〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ウィンドウ制御	SourceQuench を受信した際に、TCP ウィンドウ制御に反映するかどうかを指定します。 enable：TCP ウィンドウ制御に反映する。 disable：TCP ウィンドウ制御に反映しない。	enable disable	省略不可

この設定を行わない場合

SourceQuench を受信しても TCP ウィンドウ制御に反映しません。

設定モード

基本設定モード

ポリシールーティング

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ設定モードへ移行する

```
Router(config)#class-map video-class
Router(config-class-map)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アクセスリストの 100 番もしくは 101 番にマッチするトラフィックを対象とする

```
Router(config)# class-map video-class
Router(class-map video-class)# match-any
Router(class-map video-class)# match ip access-group 100
Router(class-map video-class)# match ip access-group 101
Router(class-map video-class)# exit
```

コマンド書式

match-any

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で match-any を指定しなかった場合は以下のようになります。

```
Router(config)# class-map video-class
Router(class-map video-class)# match ip access-group 100
Router(class-map video-class)# match ip access-group 101
Router(class-map video-class)# exit
```

この場合、IP アクセスリストの 100 番にマッチ、かつ 101 番にマッチするトラフィックを対象とします。

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199、2000～2699	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。

refresh コマンド後に有効になるコマンドです。

設定例１　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

match ip input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]
match ipv6 input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16 tunnel 1～32	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(config-action-map)#
```

コマンド書式

action-map〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

set ip next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6} next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　パケット中継先を 192.168.100.1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip next-hop 192.168.100.1 distance 10
```

コマンド書式

```
set ip next-hop <IP アドレス> [distance (1-255)]
set ip next-hop <インタフェース> [distance (1-255)]
set ip next-hop connected {ipsecif <1-4> | null <0-0>} [distance (1-255)]
set ip next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	ewan 1～2 pppoe 1～24※1 dialer 1～20※2 tunnel 1～32	省略不可
connected ipsecif	宛先への経路として IPsec インタフェースを指定します。	ipsecif 1～500※3	省略不可
connected null	廃棄用の宛先経路情報とします。	null 0	省略不可
distance	中継先の distance 値を設定します。	1～255	省略不可
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、クラスマップ名のアルファベット順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます(同一クラスマップ名に対しては、置換型となります)。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)# policy-map stream-service
Router(config-policy-map)# class video-class action stream-action
Router(config-policy-map)# class audio-class action stream-action
Router(config-policy-map)# exit
```

コマンド書式

class〈クラスマップ名〉action〈アクションマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	対応づけるクラスマップ名を設定します。	16 文字以内の文字列	省略不可
アクションマップ名	対応づけるアクションマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。
ここで指定したポリシーマップを有効にするには、各インタフェース設定モードで、"service-policy input/output"コマンドで登録します。
また、自局送信をポリシールーティングする場合は、"service-policy local"コマンドで登録します。

refresh コマンド後に有効になるコマンドです。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(config-policy-map)#
```

コマンド書式

policy-map 〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	ポリシーマップ名を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

statistics update 〈カウント設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
カウント設定	統計情報のカウントを行うかどうかを指定します。 enable　統計情報のカウントを行う disable　統計情報のカウントを行わない	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシールーティング時の NextHop 監視

ip polling-interval

ポリシールーティング時に有効な中継先かどうかを判断するために、指定された中継先に対して監視パケットを送信する際の Ipv4 監視パケット(ARP)の送信間隔を指定します。

ARP またはネイバのキャシュテーブルの参照を行い、IPv4 では MAC アドレスが解決済みであったときに有効であると判定されます。

それ以外は、有効でないと判定されます。

有効である場合、ポリシールーティング機能では、指定された中継先への到達性があると判定し、その中継先を有効な経路と認識します。有効でない場合は、set ip next hop コマンドで設定された次の候補の判定を行います。

定変更後のリフレッシュでは変更前の監視パケット送信後、変更された指定が有効となります。

refresh コマンド後に有効になるコマンドです。

設定例１　監視パケットの送信間隔を 10 秒にする

```
Router(config)#ip polling-interval 10
```

コマンド書式

ip polling-interval 〈 監視パケット送信間隔 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視パケット送信間隔	IPv4 監視パケット(ARP)の送信間隔を指定します。	5～60	送信間隔を 5 秒に設定します。

この設定を行わない場合

監視パケットの送信間隔が 5 秒に設定されます。

設定モード

基本設定モード

マルチキャストの設定

igmp-proxy non-querier 【F100/F1000 コマンド】

本コマンドを設定することにより、イベントアクションが稼働した時に non-querier 状態に移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN １インタフェースに対して non-querier 状態とする

```
Router(config)#event-action 1
Router(config-event-action 1)# igmp-proxy ewan 1 non-querier
```

コマンド書式

igmp-proxy <インタフェース名> non-querier

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	non-querier 状態とするインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～16	省略不可

この設定を行わない場合

non-querier 通知をしません。

設定モード

イベントアクション設定モード

ip igmp access-group 【F100/F1000 コマンド】

各インタフェースで、マルチキャストルーティングを許可するグループアドレスをアクセスリスト番号で設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　許可するグループアドレスをアクセスリスト番号 10 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp access-group 10
```

コマンド書式

ip igmp access-group〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセスリスト番号	許可するグループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999	省略不可

この設定を行わない場合

すべてのグループアドレスを許可します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp fast-leave 【F100/F1000 コマンド】

各インタフェースで、Fast Leave を有効にするかどうかの設定をします。
複数の受信者が存在するインタフェースでは、この設定を有効にしないでください。

refresh コマンド後に有効になるコマンドです。

設定例１　Fast Leave を有効にする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp fast-leave
```

コマンド書式

```
ip igmp fast-leave
```

パラメータ

パラメータはありません。

この設定を行わない場合

Query に対して、Report メッセージがタイムアウトしてから、上流に対して Leave メッセージを通知します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp group-membership-timeout 【F100/F1000 コマンド】

マルチキャストグループに参加するインタフェース情報の保持時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　保持時間を 1500 秒とする

```
Router(config)#ip igmp group-membership-timeout 1500
```

コマンド書式

ip igmp group-membership-timeout 〈保持時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
保持時間	マルチキャストグループに参加するインタフェース情報の保持時間(単位:秒)を設定します。	30～65535	省略不可

この設定を行わない場合

保持時間を 260 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp last-membership-query-interval 【F100/F1000 コマンド】

各インタフェースで、Leave 受信後の Group Specific Query に対応する IGMP Report を受信するための待機時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　保持時間を 10 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp last-membership-query-interval 10
```

設定例 2　保持時間を 500 ミリ秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp last-membership-query-interval dsec 5
```

コマンド書式

ip igmp last-membership-query-interval [dsec] <待機時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
待機時間	Leave 受信後の Group Specific Query に対応する IGMP Report を受信するための待機時間(単位:秒)を設定します。	1～25	省略不可
dsec	待機時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

保持時間を 1 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy 【F100/F1000 コマンド】

各インタフェースで、IGMP Proxy によるマルチキャストルーティングを中継するかどうかの設定します。
Snooping および、PIM-SM に関して本装置ではサポートしていません。

refresh コマンド後に有効になるコマンドです。

設定例１　ipsec インタフェースで IGMP Proxy によるマルチキャストルーティングを中継する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp proxy
```

コマンド書式

ip igmp proxy

パラメータ

パラメータはありません。

この設定を行わない場合

マルチキャストルーティングを中継しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy-group 【F100/F1000 コマンド】

各インタフェースにおいてマルチキャストルーティングを行う際の、IGMP Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。
また、インタフェース設定モードと基本設定モードでアクセスリスト番号が重複する場合は、インタフェース設定モードが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクセスリスト番号 10 をグループアドレスとして指定する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp proxy-group 10
```

コマンド書式

ip igmp proxy-group 〈アクセスリスト番号〉 [upstream 〈インタフェース名〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセスリスト番号	グループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999	省略不可
インタフェース名	上流インタフェースに指定するインタフェースを選択します。	lan 1 ewan 1～2 ipsecif※ 1～500 vlanif 1～16	上流インタフェースを指定しません。

※: F100 の場合は、1～100 になります。

この設定を行わない場合

IGMP Proxy によるマルチキャストルーティングを中継しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp proxy-group-upstream 【F100/F1000 コマンド】

装置全体としてマルチキャストルーティングを行う際の、IGMP Proxy の動作を有効とするグループアドレスをアクセスリスト番号で指定します。
複数設定された場合には、アクセスリスト番号順にソートされます。
また、インタフェース設定モードと基本設定モードでアクセスリスト番号が重複する場合は、インタフェース設定モードが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクセスリスト番号 10 をグループアドレス、ipsecif 1 を上流インタフェースとして指定する

```
Router(config)#ip igmp proxy-group-upstream ipsecif 1 10
```

コマンド書式

ip igmp proxy-group-upstream 〈インタフェース名〉〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	上流インタフェースに指定するインタフェースを選択します。	lan 1 ewan 1～2 ipsecif※ 1～500 vlanif 1～16	省略不可
アクセスリスト番号	グループアドレスを IPv4 標準アクセスリストの中から選択します。	1～99 1300～1999	省略不可

※: F100 の場合は、1～100 になります。

この設定を行わない場合

IGMP Proxy によるマルチキャストルーティングを中継しません。

設定モード

基本設定モード

ip igmp proxy non-querier-behavior 【F100/F1000 コマンド】

Non-querier 時の動作を設定します。
2 台のルータで冗長構成を行う場合に、同一セグメント上の別ルータを Querier 状態とし本装置は Non-Querier 状態とする場合には、reject-report オプションを追加することで本装置のパケット中継を中止することができます。

refresh コマンド後に有効になるコマンドです。

設定例 1　Non-querier 時に上流に join することなくパケットの中継をしない

```
Router(config)#ip igmp proxy non-querier-behavior reject-report
```

コマンド書式

```
ip igmp proxy non-querier-behavior <Non-querier 設定>
```

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
Non-querier 設定	Non-querier 時の動作を設定します。		default reject-report no-join	省略不可
	default	上流に join し、下流は report 受付しますが、流れてきたトラヒックは廃棄し中継しません。		
	reject-report	下流からの report を廃棄し、上流に join することはなくトラヒックは流れません。		
	no-join	下流からの report は受付るが上流には join しません。		

この設定を行わない場合

上流に join し、下流は report 受付しますが、流れてきたトラヒックは廃棄し中継しません。

設定モード

基本設定モード

ip igmp querier-timeout 【F100/F1000 コマンド】

各インタフェースで、IGMP Querier の生存タイマ時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　生存タイマ時間を 100 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp querier-timeout 100
```

コマンド書式

ip igmp querier-timeout〈生存タイマ時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存タイマ時間	IGMP Querier の生存タイマ時間(単位:秒)を設定します。	60～300	省略不可

この設定を行わない場合

生存タイマ時間を 255 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp query-interval 【F100/F1000 コマンド】

各インタフェースで、IGMP Query メッセージの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　送信間隔を 100 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-interval 100
```

コマンド書式

ip igmp query-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	IGMP Querier メッセージの送信間隔(単位:秒)を設定します。	30～65535	省略不可

この設定を行わない場合

送信間隔を 125 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp query-max-response-time 【F100/F1000 コマンド】

各インタフェースで、IGMP Query 内に設定する最大応答待ち時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　最大応答時間を 10 秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-max-response-time 10
```

設定例 2　最大応答時間を 500 ミリ秒とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp query-max-response-time dsec 5
```

コマンド書式

ip igmp query-max-response-time [dsec] <最大応答待ち時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大応答待ち時間	IGMP Query 内に設定する最大応答待ち時間(単位:秒)を設定します。	1～25	省略不可
dsec	最大応答待ち時間を 100 ミリ秒単位で設定する場合に指定します。	1～255	秒単位の設定になります。

この設定を行わない場合

最大応答時間を 10 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp static-group 【F100/F1000 コマンド】

各インタフェースで、静的に登録するマルチキャストグループを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　233.0.0.1 をマルチキャストグループに追加する

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp static-group 233.0.0.1
```

コマンド書式

ip igmp static-group 〈グループアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
グループアドレス	静的に登録するマルチキャストグループを設定します。	IPv4 アドレスを設定	省略不可

この設定を行わない場合

マルチキャストグループを静的に登録しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip igmp source-interface 【F100/F1000 コマンド】

各インタフェースで、IGMP パケットソースアドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN １に IGMP パケットソースアドレスを設定する

```
Router(config)#interface ipsecif 1
Router(config-ipsecif 1)#ip igmp source-interface ewan 1
```

コマンド書式

ip igmp source-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	IGMP パケットソースアドレス設定するインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～16 loopback 1	省略不可

この設定を行わない場合

他インタフェースの IP アドレスを自動設定します。
loopback 1 -> lan -> vlan1-16 -> ewan1 -> ewan2 の順に検索し、使用できるアドレスが見つかった場合、そのインタフェースのアドレスを使用します。

設定モード

IPsec インタフェース設定モード

ip igmp version 【F100/F1000 コマンド】

各インタフェースで、IGMP Querier の動作バージョンを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　IGMP Querier の動作バージョンを１とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip igmp version 1
```

コマンド書式

ip igmp version <IGMP Querier バージョン>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IGMP Querier バージョン	IGMP Querier の動作バージョンを設定します。 1　バージョン 1 2　バージョン 2	1 2	省略不可

この設定を行わない場合

IGMP Querier の動作バージョンは 2 となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip multicast ttl-threshold 【F100/F1000 コマンド】

マルチキャスト中継時の TTL の閾値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　TTL の閾値を 10 とする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip multicast ttl-threshold 10
```

コマンド書式

ip multicast ttl-threshold <TTL>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TTL	マルチキャスト中継時の TTL の閾値を設定します。	1～255	省略不可

この設定を行わない場合

TTL の閾値を 1 に設定します。

設定モード

基本設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
IPsec インタフェース設定モード
VLAN インタフェース設定モード

ip multicast-routing proxy 【F100/F1000 コマンド】

マルチキャストルーティングを行う場合のサポートプロトコルを設定します。
Snooping および、PIM-SM に関して本装置ではサポートしていません。
refresh コマンド後に有効になるコマンドです。

設定例１　サポートプロトコルに IGMP Proxy を選択する

```
Router(config)#ip multicast-routing proxy
```

コマンド書式

ip multicast-routing proxy

パラメータ

パラメータはありません。

この設定を行わない場合

マルチキャストルーティングを行いません。

設定モード

基本設定モード

set security-association selector bypass 【F100/F1000 コマンド】

IPsecSA のセレクタ検索を行わずに中継する場合に設定します。
mcast オプションを指定することにより、マルチキャストパケットのみセレクタ検索を行わずに中継します。
ルートベース(ipsecif)を使用した IPsec でのみ有効、ポリシーベースでは無視します。

IPsec 機能を使用してマルチキャストルーティングを行う場合に設定してください。

refresh コマンド後に有効になるコマンドです。

設定例１　マルチキャストパケットのみセレクタ検索を行わずに中継する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association selector bypass mcast
```

コマンド書式

```
set security-association selector bypass [mcast]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mcast	マルチキャストパケットのみセレクタ検索を行わずに中継する場合に指定します。	mcast	全てのパケットでセレクタ検索を行わずに中継します。

この設定を行わない場合

セレクタにマッチしないパケットは破棄されます。

設定モード

VPN セレクタ設定モード

リミテッドブロードキャストの設定

ip limited-broadcast ttl

リミテッドブロードキャスト(255.255.255.255)宛の IP パケットの TTL 値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　リミテッドブロードキャストの TTL 値を 64 にする

```
Router(config)#interface lan 1
Router(config-if lan1)#ip limited-broadcast ttl 64
```

コマンド書式

ip limited-broadcast ttl ＜ TTL 値 ＞

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TTL 値	リミテッドブロードキャストの TTL 値を指定します。	1～255	省略不可

この設定を行わない場合

リミテッドブロードキャストの TTL 値は、1 となります。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

IPsec機能の設定

IPsec基本コマンド

ip mtu

IPsec インタフェースの MTU 長を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　IPsec の MTU 長を 1400byte にする

```
Router(config)#interface ipsecif 1
Router(config-if ipsecif 1)#ip mtu 1400
```

コマンド書式

ip mtu <MTU 長>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MTU 長	MTU 長を指定します。	576～1500	省略不可

この設定を行わない場合

1390byte となります。通常は変更の必要はありません。

MTU 長とは？

MTU とは（Max Transfer Unit）の略で、MTU 長とは、通常、1 パケットで運ぶことができる IP パケット（IP ヘッダ＋IP ペイロード）の長さをいいます。
標準的な Ethernet では、MTU 長は 1500byte です。

設定モード

IPsec インタフェース設定モード

linkdown-detect

LAN 側インターフェースのリンクダウンを検出するかどうかの設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN 側インタフェースのリンクダウンを検出する

```
Router(config)#inter lan 1
Router(config-if lan 1)#linkdown-detect on
```

コマンド書式

linkdown-detect 〈リンクダウン設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リンクダウン設定	物理的な LAN ポートのリンクアップ/ダウンと LAN インタフェースのアップ/ダウンを連動させるかどうかの設定を行います。 on：リンクアップ/ダウンを連動させる。 off：リンクアップ/ダウンを非連動にする。	on off	省略不可

この設定を行わない場合

LAN 側インターフェースのリンクダウンを検出しません。

設定モード

LAN インタフェース設定モード

vpn enable

IPsec 機能を使用した VPN 通信を行う場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　IPsec 機能を使用する

```
Router(config)#vpn enable
```

コマンド書式

vpn enable　[ewan] [bri]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ewan	セレクタ検索の対象とするインタフェース名を指定します。 ewan 1～2：指定した ewan のみ適用します。 all：ewan1、2 の両方に適用します。	ewan 1～2 all	LAN を除く全てのインタフェースがセレクタ検索の対象となります。
bri	セレクタ検索の対象とするインタフェースに、BRI インタフェースを指定します。	bri 1※	BRI インタフェースをセレクタ検索の対象としません。

※:F100 のみ選択可能です。

この設定を行わない場合

VPN(IPsec)は使用できません。

設定モード

基本設定モード

vpnlog enable

IPsec 機能を使用した VPN 通信動作中(SA の確立／解放)の VPN ログを残すか残さないかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SA の確立／解放を VPN ログに残す

```
Router(config)#vpnlog enable
```

コマンド書式

vpnlog enable

パラメータ

パラメータはありません。

この設定を行わない場合

SA 確立／解放の情報がログに残されません。

FITELnet-F シリーズの vpnlog とは？

FITELnetーF シリーズの IPsec 機能に関するログです。
SA を確立できなかった場合の原因究明や、改ざん・なりすまし等を検知した場合に、ログを発行します。
コンソールもしくは TELNET でログインして、vpnlog の情報を表示する場合は、show vpnlog コマンドを使用します。

設定モード

基本設定モード

Phase1 ポリシーの設定

authentication

Phase1 の認証方式を設定します。認証方式には、電子証明書(RSA)方式／Pre-shared key※の2方式があり、それぞれ拡張認証を行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

※Pre-shared key･･･一般的に「事前共有鍵」「共有秘密鍵」と呼ばれます。

設定例１　認証方式を、Pre-shared key（拡張認証なし）とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# authentication prekey
```

コマンド書式

authentication <認証方式>

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>認証方式</td><td>Pre-Shared Key による方式とするか、RSA signature の方式とするか、および拡張認証を行なうかどうかを選択します。<table><tr><td>prekey</td><td>Pre-Shared Key 認証・拡張認証なし</td></tr><tr><td>prekeyxauth</td><td>Pre-Shared Key 認証・拡張認証あり</td></tr><tr><td>rsasig</td><td>RSA signature 認証・拡張認証なし</td></tr><tr><td>rsasigxauth</td><td>RSA signature 認証・拡張認証あり</td></tr></table></td><td>prekey
prekeyxauth
rsasig
rsasigxauth</td><td>省略不可</td></tr>
</table>

この設定を行わない場合

Pre-shared key(拡張認証しない)方式を使用します。

設定モード

IKE ポリシー設定モード

encryption

Phase1 の暗号アルゴリズムを設定します。FITELnet-F シリーズの暗号アルゴリズムには、DES（56bit DES-CBC）と、3DES（168bit DES）と AES（128bit、192bit、256bit）があります。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　Phase1 の暗号化アルゴリズムを AES(128bit)方式とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#encryption aes 128
```

コマンド書式

encryption 〈暗号化アルゴリズム〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
暗号化アルゴリズム	Phase1 の暗号化アルゴリズムを指定します。 des：DES 方式 3des：3DES 方式 aes 128：AES 128bit aes 192：AES 192bit aes 256：AES 256bit	des 3des aes 128 aes 192 aes 256	省略不可

この設定を行わない場合

DES 方式を使用します。

設定モード

IKE ポリシー設定モード

group

Phase1 のネゴシエーション時に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。
このコマンドは Diffie-Hellman Group を指定します。
Diffie-Hellman Group には、1(768-bit)と、2(1024-bit)と、5(1536-bit)の 3 種類があります。
VPN ピアと設定が異なる場合は、"Group 1"で動作します。

refresh コマンド後に有効になるコマンドです。

設定例１　Phase1 のネゴシエーション時の Diffie-Hellman グループを”Group2”とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#group 2
```

コマンド書式

group <DH グループ番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ番号	Diffie-Hellman グループ番号を指定します。	1 2 5	省略不可

この設定を行わない場合

"Group 1"を使用します。

設定モード

IKE ポリシー設定モード

hash

Phase1 のハッシュアルゴリズムを設定します。FITELnet-F シリーズのハッシュアルゴリズムには、MD5 と SHA-1 があります。
この設定は、SA を確立する相手と同じ設定である必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　Phase1 のハッシュアルゴリズムを SHA-1 とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#hash sha
```

コマンド書式

hash〈ハッシュアルゴリズム〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ハッシュアルゴリズム	Phase1 のハッシュアルゴリズムを指定します。	md5 sha	省略不可

この設定を行わない場合

MD5 方式を使用します。

設定モード

IKE ポリシー設定モード

idtype-pre

Aggressive モードで、通知する ID の形式を定義します。

refresh コマンド後に有効になるコマンドです。

設定例１　Aggressive モードで通知する ID を、FQDN 形式とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#idtype-pre fqdn
```

コマンド書式

idtype-pre <ID タイプ>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ID タイプ	Aggressive モードで自身の ID を通知する際のタイプを指定します	fqdn userfqdn	省略不可

この設定を行わない場合

userfqdn(UserFQDN)を使用します。

FQDN/User-FQDN とは？

FQDN とは、Fully-qualified domain names の略です。ホスト名から全ての情報をもつドメイン名のことを言います。

User-FQDN 形式とは、電子メールアドレスの書式として使用される「ユーザ名@ドメイン名」の書式です。

Aggressive モードでは、通知する ID の形式を対向装置で受け入れ可能なものとする必要があります。

設定モード

IKE ポリシー設定モード

idtype-rsa

RSA signatures 認証の場合に、接続相手に認証してもらう自身の ID タイプを指定します。
ID タイプには、distinguished-name(DN)、ドメイン名、電子メールアドレス、IP アドレスがあります。
distinguished-name(DN)の場合は、peer-identity distinguished-name で設定した内容、ドメイン名と電子メールアドレスの場合は、peer-identity host で設定した内容、IP アドレスの場合は、peer-identity address で設定した内容と接続相手の証明書に書かれている内容を比較して認証を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　RSA signatures 認証使用時の ID タイプに電子メールを使用する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#idtype-rsa email
```

コマンド書式

idtype-rsa <ID タイプ>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
ID タイプ	RSA signatures 認証の場合に、接続相手に認証してもらう自身の ID タイプを指定。		dn domain email ip	省略不可
	dn	distinguished-name		
	domain	ドメイン名		
	email	電子メールアドレス		
	ip	IP アドレス		

この設定を行わない場合

ドメイン名を ID タイプとして接続相手に通知します。

設定モード

IKE ポリシー設定モード

ip vpn-nat pool

VPN-NAT 変換する際の、変換後の IP アドレス範囲を指定します。NAT 変換(NAT+ではない)する場合に指定する必要があります。
このコマンドでは、VPN-NAT プール名称・変換後の IP アドレス範囲(アドレス/Wildcard Mask)を指定し、ip vpn-nat inside source/destination コマンドで、使用する VPN-NAT プール名を指定します。

refresh コマンド後に有効になるコマンドです。

設定例　変換後のアドレスとして、192.168.100.0/24 を指定する（プール名：vpn-pool1）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1
192.168.100.0 0.0.0.255
```

コマンド書式

ip vpn-nat pool 〈VPN プール名〉〈変換後のアドレス〉〈Wildcard マスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN-NAT プール名	VPN-NAT プールの名称を指定します。 ip vpn-nat inside source / destination のコマンドを設定する場合に指定する VPN-NAT プール名として使用しますので、わかりやすい名称にしてください。	-	省略不可
変換後のアドレス	変換後の IP アドレスを設定します。 変換後のアドレスを範囲で指定することができます。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可
Wildcard マスク	変換後のアドレスを範囲指定するために、Wildcard マスクを指定します。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可

最大エントリ数:2 エントリ(isakmp policy 毎)装置全体で 64 エントリ

この設定を行わない場合

VPN-NAT が使用できません。

範囲指定方法

ip vpn-nat pool コマンドで IP アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。

例1) 24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い

Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0

例2) ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い

Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

設定モード

IKE ポリシー設定モード

ip vpn-nat inside source

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

LAN 側から WAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<ローカルアドレス・サブネットマスク>で指定したローカルアドレスから<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　192.168.100.0/24）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 pool vpn-pool1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1 192.168.100..0 0.0.0.255


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、ip-vpn nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 interface


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】

ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、インタフェースアドレスに集約する場合は"interface"、Mode-config 機能により取得したアドレスに集約する場合は"modeconfig"、指定したアドレスに集約する場合は"peer <ip-address>"と指定します。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24←→192.168.100.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside source static-subnet
158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】

ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】　ip-vpn nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【NAT+時】 ip-vpn nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] NAT+変換後のアドレス overload | [変換後開始ポート番号 [変換後終了ポート番号]]]
【スタティック変換】 ip vpn-nat inside source static <ローカルアドレス> <グローバルアドレス>
【NAT スタティック(一括変換)】 ip vpn-nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前(ローカルアドレス)範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後(グローバルアドレス)範囲を指定した VPN-NAT プール名を指定します。	NAT プール名	NAT の場合は省略不可
NAT+変換後のアドレス	NAT+変換後のアドレスを指定します。	interface：送信インタフェースのアドレスに変換 modeconfig：相手から割	NAT+の場合は省略不可

		り当てられたアドレスに変換 peer <IP アドレス> 設定する IP アドレスに変換	
overload	ポート変換する場合に指定	overload	ポート変換しない
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
ローカルアドレス	変換前のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
グローバルアドレス	変換後のグローバルアドレスを指定します。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換前のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
グローバルサブネット	変換後のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ数:リスト 1 エントリ(isakmp policy 毎)装置全体で 32 エントリ
スタティック 512 エントリ(装置全体)※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

設定モード

IKE ポリシー設定モード

ip vpn-nat inside destination

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

WAN 側から LAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスから<ローカルアドレス・サブネットマスク>で指定したローカルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　192.168.100.1 宛で受信したら 192.168.0.1 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static
192.168.100.1 192.168.0.1
```

【解説】

ip vpn-nat inside destination static <WAN 側アドレス> <LAN 側アドレス>となります。
これ以外のパケットを NAT 変換したい場合は、ip vpn-nat inside source コマンドを使用して、設定します。

設定例２　NAT+変換（スタティック登録）　192.168.100.1:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static
192.168.100.1 1500 192.168.0.1 80
```

【解説】

ip vpn-nat inside destination static <WAN 側アドレス WAN 側ポート番号> <LAN 側アドレス LAN 側ポート番号>となります。
これ以外のパケットを NAT+変換したい場合は、ip vpn-nat inside source コマンドを使用して、設定します。

設定例３　NAT 変換（一括変換）192.168.100.0/24←→158.xxx.xxx.xxx.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside destination static-
subnet 158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】

ip vpn-nat inside destination static-subnet <グローバルサブネット> <ローカルサブネット> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます（複数同時登録）。

例）local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】　ip vpn-nat inside destination list <access-list 番号> [開始ポート番号 [終了ポート番号]] pool <プール名> [ポート番号]
【NAT スタティック（1 対 1 変換）、NAT+スタティック時】 ip vpn-nat inside destination static <グローバルアドレス> [開始ポート番号 [終了ポート番号]] <ローカルアドレス> [ポート番号]
【NAT スタティック（一括変換）】 ip vpn-nat inside destination static-subnet <グローバルサブネット> <ローカルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前（グローバルアドレス）範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
グローバルアドレス	変換前のグローバルアドレスを指定します。	list <access-list 番号> アクセスリストで指定した IP アドレス範囲 <IP アドレス> 指定した IP アドレス modeconfig 相手から割り当てられ	省略不可

		peer <IP アドレス> / VPN ピアから指定されて設定した	
[開始ポート番号 終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後(ローカルアドレス)範囲を指定した NAT プール名を指定します。	NAT プール名	省略不可
ローカルアドレス	変換後のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
グローバルサブネット	変換前のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換後のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ数:リスト 1 エントリ(isakmp policy 毎)装置全体で 32 エントリ
スタティック 512 エントリ(装置全体)※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

設定モード

IKE ポリシー設定モード

keepalive

SA が接続されているかどうかの確認を行なうために KeepAlive を行なうかどうかを設定します。
本装置では、IKE(Internet Key Exchange security association)プロトコルの KeepAlive 機能、および ICMP による KeepAlive 機能をサポートしています。

本装置では、何も設定をしない場合、IKE の KeepAlive を行います。IKE の KeepAlive は、SA を確立する VPN ピアも IKE の KeepAlive 機能をサポートしている必要があります。

※IKE での KeepAlive は、DPD(Dead Peer Detection)および古河独自の方式をサポートしています。
対向の装置がどちらもサポートしている場合は、DPD で動作します。
対向の装置がどちらの方式もサポートしていない場合は、ICMP を使用した方法で行ってください。

ICMP による KeepAlive を行う場合は、オプションに"icmp"を指定します。ICMP による KeepAlive を行なう場合は、keepalive-icmp コマンドを指定する必要があるケースもあります。KeepAlive を行なわない場合は、"disable"を指定します。

KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

設定例１　KeepAlive を行なわない

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive disable
```

設定例２　ICMP の KeepAlive を行なう

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive icmp
```

コマンド書式

```
keepalive { always-send | response-only | icmp [always-send|traffic-based
          [always-send]]| disable}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
response-only	応答動作のみ行い、自身では KeepAlive 要求パケットを送信しません。 ※DPD もしくは、古河独自 DPD でのみ指定可能	response-only	省略不可
icmp	ICMP を利用した KeepAlive を行います。	icmp	
always-send	VPN データが送信されなくても、常に KeepAlive を送信します。	always-send	
traffic-based	送信間隔中に該当 SA の Inbound トラフィックが存在する場合には、ICMP-KeepAlive のパケットを送信しません。	traffic-based	
disable	KeepAlive 機能を使用しません。	disable	

この設定を行わない場合

IKE の keepalive でネゴシエーションを行います。
対向の装置と合意できた際に、送信間隔中に Phase2 SA で Inbound のトラフィックが無く、Outbound のトラフィックがある場合に keepalive のパケットを送信します。

設定モード

IKE ポリシー設定モード

keepalive-icmp

SA が接続されているかどうかの確認を行なうための KeepAlive を ICMP で行なう場合に、KeepAlive の宛先 IP アドレスおよび KeepAlive パケットの送信元 IP アドレスを設定します。
宛先を VPN ピア、送信元 IP アドレスを送信するインタフェースの IP アドレスとする場合は、このコマンドを設定する必要はありません。

ICMP による KeepAlive は、通常の ICMP Echo を使用していますので、宛先は TCP/IP 通信が行なえる端末であればルータでなくてもかまいません。keepalive-icmp の設定を省略した場合は宛先を VPN ピアに、送信元 IP アドレスを省略した場合はパケットを送信するインタフェースの IP アドレスを送信元にセットした KeepAlive を行ないます。

KeepAlive により、SA が使用できない状態になった場合は、SA を解放します。

refresh コマンド後に有効になるコマンドです。

設定例 1　ICMP の KeepAlive の宛先を、192.168.0.1 にする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive-icmp peer-address 192.168.0.1
```

設定例 2　ICMP の KeepAlive パケットの送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive-icmp source-interface lan 1
```

コマンド書式

keepalive-icmp peer-address 〈宛先 IP アドレス〉
keepalive-icmp source-interface 〈インタフェース名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先 IP アドレス	ICMP の KeepAlive を行なう相手の IP アドレスを設定します。	IPv4 アドレス形式	VPN ピア
インタフェース名	ICMP の KeepAlive 送信する際の、送信元アドレスに使用するインタフェースを設定します。	lan 1 ewan 1～2 dialer 1～20※ loopback 1	使用する WAN 側インタフェースの IP アドレス

※:F100 のみ選択可能

この設定を行わない場合

keepalive icmp が設定されている場合、宛先 IP アドレスは VPN ピアの IP アドレスに、送信元 IP アドレスは実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

IKE ポリシー設定モード

keepalive-icmp multi-path

IPsec 負荷分散機能使用時の ICMP の keepalive 設定を行います。
keepalive-icmp コマンドで、指定した ICMP の keepalive は、本装置のもつ経路情報に従って送信されますが、keepalive-icpm multi-path を使用すると、ICMP の keepalive パケットの NextHop を指定することができます。

IPsec 負荷分散機能では、1つの VPN ピアに対して異なる経路の SA を確立するため、ICMP の keepalive パケットも複数の経路に送信する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　ICMP の KeepAlive の Next Hop を、192.168.0.1 にする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#keepalive-icmp multi-path address 192.168.0.1
```

設定例２　ICMP の KeepAlive を送信するインタフェースを EWAN1 に設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# keepalive-icmp multi-path interface ewan 1
```

コマンド書式

keepalive-icmp multi-path { address <A.B.C.D>| <インタフェース名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address <A.B.C.D>	ICMP の KeepAlive の next hop にする IP アドレスを設定します	IPv4 アドレス形式	VPN ピア
インタフェース名	ICMP の KeepAlive を送信するインタフェースを設定します。	ewan 1～2 pppoe 1～24※	省略不可

※ F80 の場合は、1～5 になります。

この設定を行わない場合

IPsec 負荷分散機能を使用することができません。

設定モード

IKE ポリシー設定モード

keepalive-icmp redundancy

IPsec 冗長機能仕様時の ICMP の Keepalive 設定を行います。
crypto map で冗長が設定されていないときは、ルート情報に従って送信し続け、keepalive 失敗等で SA が無くなったら送信をやめます。
基本設定として、redundancy interface 設定は必ず設定されなければなりません。
また、ewan 指定時でかつ、インターフェースアドレス設定が manual 時のみ、redundancy address 設定が必要となります。

refresh コマンド後に有効になるコマンドです。

設定例１　ICMP の KeepAlive の next hop を、192.168.50.3 にする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# keepalive-icmp redundancy address 192.168.50.3
```

設定例２　ICMP の KeepAlive を送信するインタフェースを EWAN1 に設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# keepalive-icmp redundancy interface ewan 1
```

コマンド書式

keepalive-icmp redundancy {address <A.B.C.D>| interface <インタフェース名>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address <A.B.C.D>	ICMP の KeepAlive の next hop にする IP アドレスを設定します。	IPv4 アドレス形式	VPN ピア
インタフェース名	ICMP の KeepAlive を送信するインタフェースを設定します。	ewan 1～2 pppoe 1～24※1 dialer 1～20※2	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

IPsec 冗長機能を使用することができません。

設定モード

IKE ポリシー設定モード

key

Pre-Shared Key*を設定します。
文字列で指定する場合は"ascii"を指定、16 進数で指定する場合は"binary"を指定した後、Pre-Shared Key を設定します。

refresh コマンド後に有効になるコマンドです。

※Pre-Shared Key・・・一般に「事前共有鍵」「共有秘密鍵」とも呼ばれます。

設定例１　Pre-Shared Key に文字列の"secretF100"設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#key ascii secretF100
```

設定例２　Pre-Shared Key に 16 進数の"123456789abcdef"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#key binary 123456789abcdef
```

コマンド書式

```
key {ascii|binary} <Pre-shared Ke> [{secret | private}[encrypted]]
```

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>ascii | binary</td><td>Pre-shared Key を文字列(ascii)として扱うか、16 進数(binary)として扱うかを指定します。</td><td>ascii
binary</td><td>省略不可</td></tr>
<tr><td>Pre-shared Key</td><td>Pre-shared Key を設定します。</td><td>最大 64 文字の英数字</td><td>省略不可</td></tr>
<tr><td>secret | private</td><td>Pre-shared Key を暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1
<table><tr><td>secret</td><td>暗号化する際に共有暗号鍵を使用する</td></tr><tr><td>private</td><td>暗号化する際に装置固有暗号鍵を使用する</td></tr></table></td><td>secret
private</td><td>パスワードを暗号化しません</td></tr>
<tr><td>encrypted</td><td>Pre-shared Key を暗号化処理するかどうかを設定します。
このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2
secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。</td><td>encrypted</td><td>パスワードを暗号化データとして扱いません</td></tr>
</table>

※1:このオプションは、設定するとすぐに有効となり、Pre-shared Key が暗号化されて表示され encrypted オプションが自動的に付加されます。

※2:Pre-shared Key が既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

SA を確立できません。

設定モード

IKE ポリシー設定モード

lifetime

Phase1 SA の生存時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　Phase1 SA の生存時間を 1200 秒に設定する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)# lifetime 1200
```

コマンド書式

lifetime <生存時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存時間	Phase1 SA の生存時間(秒)を設定します。	60～4294967295	省略不可

この設定を行わない場合

1000 秒になります。

VPN ピアと設定が異なる場合

SA を確立しようとしている VPN ピアと、生存時間の設定が異なる場合は、次のようになります。

initiator の場合	自装置の設定値を採用します。
responder の場合	相手からの提案された値を採用します。

設定モード

IKE ポリシー設定モード

my-identity

Aggressive モードで使用する場合の自身の ID を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　自身の ID として、"F100"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#my-identity F100
```

コマンド書式

my-identity <自身の ID>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
自身の ID	Aggressive モードで使用する場合の自身の ID を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

名前はありません。

ワンポイント

PPPoE のように、IP アドレスを自動で割り当てられるようなネットワークを介している場合、VPN ピアの IP アドレスが明確に設定できないため、ID を利用して相手を確定する必要があります。
したがって、自身/相手の ID を保護する Main モードの通信を行なうことはできず、Aggressive モードでの通信を行なうことになります。

相手の設定

相手側の設定では、VPN ピアを識別する ID の設定に、ここで設定する値（設定例1では"F100"）と同じ値を設定しないと、IPsec の通信を行なうことはできません。
FITELnet-F シリーズどうしの場合は、peer-identity コマンドで設定する値と同じである必要があります。

設定モード

IKE ポリシー設定モード

nat-traversal

NAT-Traversal 機能を使用する場合に指定します。VPN ピアとの通信経路中に NAT 動作を行なうルータが存在する場合は NAT-Traversal 機能が有効です。

NAT-Traversal 機能を使用する場合は、VPN ピアに KeepAlive パケットを送信する必要があります。これは経路上の NAT ルータ上の NAT 変換テーブル情報を保つために定期的に通信データを発生させるためです。

また、このコマンドで、KeepAlive の送信間隔も指定できます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT KeepAlive の送信間隔を 20 秒とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#nat-traversal enable alivefreq 20
```

コマンド書式

```
nat-traversal enable [ alivefreq { off | <NAT KeepAlive 送信間隔> } ]
```

※alivefreq オプション時に off を設定した場合、NAT-Traversal 機能は有効ですが KeepAlive 機能は無効になります。

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
off |NAT KeepAlive 送信間隔	NAT KeepAlive の送信間隔(単位:秒)を指定します。off を指定すると、NAT KeepAlive を送信しません。	1～300 off	5

この設定を行わない場合

NAT-Traversal 機能を使用しません。

ワンポイント

NAT-Traversal 機能を使用する場合は、以下の制限があります。
・Pre-shared key での VPN 接続の場合、Aggressive mode でのサポートになります。
Main mode はサポートしていません。
・RSA Signature での VPN 接続の場合、Main mode でのサポートになります。
Phase I における ID タイプとして"IP アドレス"を使用することはできません。
ID タイプとして使用できるのは以下となります。
・Distinguished name
・Domain name
・E-Mail address
・FITELnet-F シリーズを responder 側として機能させる場合、VPN peer の IP アドレスが確定(NAT スタティックにより常に一定)していてもその IP アドレスを設定しないでください。
center(config-isakmp)#peer-identity address 158.202.x.x -> ×
center(config-isakmp)#peer-identity host f100no1 -> ○
・WAN 側アドレスが不定(フレッツ ADSL アドレス動的割当等)の場合には VPN_NAT は使用できません。

相手の設定

相手も NAT-Traversal 機能を使用する必要があります。

設定モード

IKE ポリシー設定モード

negotiation-mode

IKE(Internet Key Exchange security association) Phase1 のネゴシエーションモードを定義します。Phase1 のネゴシエーションモードには、Main モードと Aggressive モードがあります。

Main モード、Aggressive モードの特徴は、以下のとおりです。

Main モード	自身および相手の ID を保護(暗号化)することができます。ただし ID が暗号化されてしまうので、ID による相手の特定を行なうことができません。お互いの相手の特定は装置の IP アドレスになりますので、WAN 側の IP アドレスが不定の形態では、使用することができません。
Aggressive モード	自身および相手の ID により、相手を特定します。したがって、WAN 側の IP アドレスが不定の形態でも、VPN 通信を行なうことができます(どちらか一方は固定の IP アドレスが必要)。

refresh コマンド後に有効になるコマンドです。

設定例１　Main モードで接続する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#negotiation-mode main
```

コマンド書式

negotiation-mode 〈ネゴシエーションモード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネゴシエーションモード	Phase1 のネゴシエーションモードを Main モード(main)、Aggressive モード(aggressive)から選択します。	main aggressive	省略不可

この設定を行わない場合

インタフェースに IP アドレスの設定が無ければ、aggressivemode で動作します。

設定モード

IKE ポリシー設定モード

peer-identity

VPN ピアの IP アドレス、ドメイン名もしくはホスト名を設定します。
ホスト名は、Aggressive モードの Responder の場合に、相手が通知してくる ID として使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　VPN ピアの IP アドレスに、192.168.100.2 を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity address 192.168.100.2
```

設定例２　VPN ピアのホスト名として、"center"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity host center
```

コマンド書式

peer-identity address { VPN ピアの IP アドレス | ドメイン名 [v4 | v6] }
peer-identity host <VPN ピアのホスト名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアの IP アドレス	VPN ピアの IP アドレスを指定します。	IPv4 アドレス形式 IPv6 アドレス形式※1	省略不可
ドメイン名[v4 | v6]	VPN ピアをドメイン名で指定します。 ドメイン名で指定した場合は、ドメイン名の名前解決を v4、v6 のどちらかで行うか指定することができます。	ドメイン名※2 v4※3 v6※3	ドメイン名は、省略不可 v4、v6 を省略した場合は、両方で名前解決を行います。
VPN ピアの ホスト名	Aggressive モードで使用する場合の VPN ピアの ID を設定します。	最大 64 文字の英数字記号	省略不可

※1: IPv6 アドレス形式の指定は、F100/F1000 のみになります。

※2:ドメイン名として設定できる文字は、127 文字までの大文字 (A ～ Z)、小文字 (a ～ z)、数字 (0 ～ 9)、ハイフン (-) 、ドット(.)のみが設定できます。

※3:v6 の指定は、F100/F1000 のみになります。vpn enable となっているインタフェースで v4 と v6 が有効になっている場合は、v4 と v6 のどちらに名前解決させるか指定する必要があります。

この設定を行わない場合

VPN ピアのアイデンティティはありません。

相手の設定

Aggressive モードで接続する場合、相手側の設定では、VPN ピアを識別する ID の設定に、ここで設定する値（設定例 2 では"center"）と同じ値を設定しないと、IPsec の通信を行なうことはできません。FITELnet-F シリーズどうしの場合は、my-identity コマンドで設定する値と同じである必要があります。

ホスト名について

このホスト名は、Aggressive モードで Responder の場合に、相手が通知してくる ID として使用されます。

設定モード

IKE ポリシー設定モード

peer-identity distinguished-name

相手の証明書の DN(distinguished name)を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　相手の DN として、C=JP,O=furukawa,CN=honsya を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#peer-identity distinguished-name C=JP,
O=furukawa,CN=honsya
```

コマンド書式

peer-identity distinguished-name <DN>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DN	相手の DN を指定します。	最大 128 文字の英数字	省略不可

※peer-identity distinguished-name を登録する際、文字列の間にスペースを入れた形式で登録することは出来ません。スペースを省いた形式で登録してください。

この設定を行わない場合

相手を DN で認証することはできません。

設定モード

IKE ポリシー設定モード

release security-association

WAN 回線切断時に、SA(Security Association)を解放するか、そのまま残すかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　ＷＡＮ回線異常時には、ＳＡを解放する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#release security-association
```

コマンド書式

release security-association

パラメータ

パラメータはありません。

この設定を行わない場合

SA を解放せず、そのまま残します。

設定モード

IKE ポリシー設定モード

release session addr-changed

IKE パケットのソースアドレス変化の確認を行い、セッション確立時に使用していた送信元アドレスと、これから送信しようとしている IKE パケットの送信元アドレスが異なっていた場合、関連する SA (Phase 1、Phase 2 共に)をすべて削除します。
運用中に送信元アドレスが変化する構成(冗長により経路情報が変化する構成)の時に使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　IKE パケットのソースアドレス変化の確認を行う

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#release session addr-changed
```

コマンド書式

release session addr-changed

パラメータ

パラメータはありません。

この設定を行わない場合

IKE パケットのソースアドレス変化の確認を行いません。
また、変化しても SA は削除されません。

設定モード

IKE ポリシー設定モード

source-interface

送信 IKE パケットの IP ヘッダ内の送信元アドレスを指定インターフェースのアドレスに変更して送信する際の、インタフェース番号を指定します。
VRID を指定することにより、VRID にマッチする VRRP アドレスに変更して送信します。
また、VRRP ステータスが Master 以外では、IKE パケットの送信を行ないません。
SA を張っている状態で vrrp ステータスが、Master 以外に遷移した場合、PhaseI,II SA の削除を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　送信元アドレスを EWAN １インターフェースのアドレスに変更して送信する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# source-interface ewan 1
```

コマンド書式

source-interface 〈インタフェース〉〈インタフェース番号〉[VRID]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース	送信 IKE パケットの IP ヘッダ内の送信元アドレスを送信するインターフェースを指定します。	ewan vlanif	省略不可
インタフェース番号	送信 IKE パケットの IP ヘッダ内の送信元アドレスを VRRP アドレスに変更する際の、EWAN または VLANIF インタフェース番号を指定します。	ewan 1～2 vlanif 1～16	省略不可
VRID	送信 IKE パケットの IP ヘッダ内の送信元アドレスを指定インターフェースと、VRID にマッチする VRRP アドレスに変更して送信します。	1～255※	送信 IKE パケットの IP ヘッダ内の送信元アドレスを指定 EWAN インターフェースのアドレスに変更して送信します。

**※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。
ただし、各インタフェースに設定できる VRID は、2つまでになります。**

この設定を行わない場合

VRRP 機能を使用した IPsec 通信ができません。

tunnel-route

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。
この場合、VPN ピアへの NextHop も合わせて指定します。
tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。
crypto security-association モードで、設定する tunnel-route コマンドは装置に対し1つしか設定できないのに対して、本コマンドは、peer 単位で設定することができます。
本コマンドが設定されると、crypto security-association モードで設定されている tunnel-route コマンドより優先的に利用されます。

refresh コマンド後に有効になるコマンドです。

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route interface pppoe 1
```

コマンド書式

tunnel-route { address <IP アドレス> | interface <インタフェース名称>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	ewan 1 pppoe※1 1～24 dialer※2 1～20	

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。
この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。
このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IKE ポリシー設定モード

Phase2 ポリシーの設定

ipsec transform-set

Phase2 のポリシーとして、以下の情報を設定します。

暗号化方式	Phase2 の暗号化方式として、DES/3DES/AES128、192、256/暗号化しないの中から選択します。VPN ピアと同じ設定である必要があります。
認証アルゴリズム	Phase2 の認証アルゴリズムとして、HMAC-MD5/HMAC-SHA-1 の中から選択します。

FITELnet-F シリーズは、複数の Phase2 ポリシーを設定できますので、各 Phase2 ポリシーには、Phase2 ポリシー名称を設定します。

この Phase2 ポリシー名称は、実際にどのセレクタ情報に対して使用するかの指定に使用しますので、わかりやすい名称としてください。

refresh コマンド後に有効になるコマンドです。

設定例 1　Phase2 ポリシー（Phase2 ポリシー名称：P2-POLICY）として、暗号化方式：AES(256bit)、認証アルゴリズム：HMAC-SHA-1 を登録する

```
Router(config)#ipsec transform-set P2-POLICY esp-aes-256 esp-sha-hmac
```

コマンド書式

ipsec transform-set <Phase2 ポリシー名称> <暗号化方式> <認証アルゴリズム>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Phase2 ポリシー名称	Phase2 ポリシーとして、わかりやすい名称を指定します。	16 文字以内の英数字	省略不可
暗号化方式	Phase2 の暗号化方式を指定します。 esp-des：DES 方式 esp-3des：3DES 方式 esp-aes-128：AES 128bit esp-aes-192：AES 192bit esp-aes-256：AES 256bit esp-null：暗号化しない	esp-des esp-3des esp-aes-128 esp-aes-192 esp-aes-256 esp-null	省略不可
認証アルゴリズム	Phase2 の認証アルゴリズムを指定します。 esp-md5-hmac：HMAC-MD5 アルゴリズム esp-sha-hmac：HMAC-SHA-1 アルゴリズム	esp-md5-hmac esp-sha-hmac	省略不可

最大エントリ:64 エントリ

この設定を行わない場合

暗号化方式:DES、認証アルゴリズム:HMAC-MD5 で動作します

設定モード

基本設定モード

Mode-configの設定

configuration mode (isakmp policy)

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#configuration mode initiate
```

コマンド書式

configuration mode 〈制御モード〉 [skip]

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
制御モード	REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。		initiate respond	省略不可
	initiate	REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。		
	respond	SET/ACK 制御モードで動作し、set を受信待ちをします。		
skip	skip を指定することで、mode-config を省略することができます。		skip	mode-config を行います。

この設定を行わない場合

set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

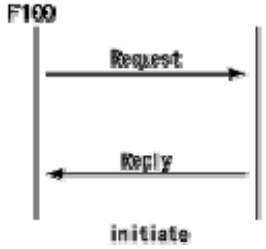
モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

1）configuration mode initiate を指定した場合

※F100 を例に説明しています。

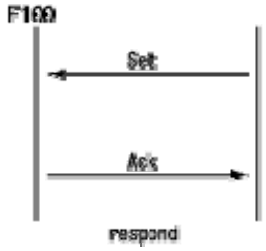
本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

※F100 を例に説明しています。

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IKE ポリシー設定モード

configuration mode (security-association)

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode initiate
```

コマンド書式

configuration mode〈制御モード〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
制御モード	REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。		initiate respond	省略不可
	initiate	REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。		
	respond	SET/ACK 制御モードで動作し、set を受信待ちをします。		

この設定を行わない場合

set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

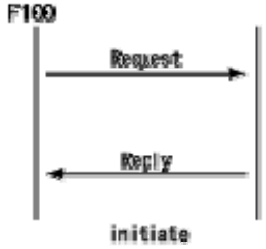
モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

1）configuration mode initiate を指定した場合

※F100 を例に説明しています。

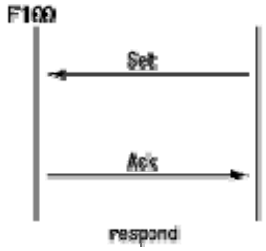
本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

※F100 を例に説明しています。

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IPsec 各種設定モード

configuration mode application-version message

configuration mode コマンドで initiate を選択した場合に、アプリケーションバージョン属性にセットする値を指定します。
respond を選択した場合は、利用しません。

refresh コマンド後に有効になるコマンドです。

設定例１　アプリケーションバージョンの値をセットする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode application-version
message fitel
```

コマンド書式

configuration mode application-version message 〈Word〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Word	アプリケーションバージョン属性にセットする値を指定します。	127 文字以内	省略不可

※ スペースも文字数としてカウントされます。
例:ＡＢＣの場合、5 文字としてカウントされます。

この設定を行わない場合

装置名と版数をセットします。

設定モード

IPsec 各種設定モード

configuration mode application-version push

configuration mode application-version message コマンドの設定があり、かつ、configuration mode コマンドで initiate が設定されている場合に、configuration mode application-version message コマンドのメッセージをセットして req パケットを送信します。

configuration mode application-version message コマンドの設定がない場合は、configuration mode application-version message コマンドのデフォルト値を使用して req パケットを送信します。

refresh コマンド後に有効になるコマンドです。

設定例１　アプリケーションバージョンに値をセットして request を送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode application-version push
```

コマンド書式

configuration mode application-version push

パラメータ

パラメータはありません

この設定を行わない場合

request パケットのアプリケーションバージョン欄を null で送信します。

設定モード

IPsec 各種設定モード

ip vpn-nat inside source

既存のネットワーク(LAN)同士を IPsec にて VPN を構築する際、互いのネットワークアドレスが重複している場合があります。
IPsec では同じネットワークアドレスの LAN を接続することが出来ません。
そのため、VPN-NAT 変換を行うことで見かけ上の重複を回避し、既存のネットワークの IP 再割り当てを行うことなく IPsec を実現します。

LAN 側から WAN 側への VPN-NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより VPN-NAT の変換ルールを、ネットワーク単位で指定することもできます。<ローカルアドレス・サブネットマスク>で指定したローカルアドレスから<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　192.168.100.0/24）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 pool vpn-pool1
Router(config-isakmp)# ip vpn-nat pool vpn-pool1 192.168.100..0 0.0.0.255


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】
ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、ip-vpn nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# ip vpn-nat inside source list 1 interface


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list 1 の部分の設定
```

【解説】
ip vpn-nat inside source <LAN 側のアドレス範囲> <WAN 側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<WAN 側のアドレス範囲>は、インタフェースアドレスに集約する場合は"interface"、Mode-config 機能により取得したアドレスに集約する場合は"modeconfig"、指定したアドレスに集約する場合は"peer <ip-address>"と指定します。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24←→192.168.100.0/24 に変換する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#ip vpn-nat inside source static-subnet
158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】

ip vpn-nat inside source static-subnet〈ローカルサブネット〉〈グローバルサブネット〉〈サブネットマスク〉となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】

ip-vpn nat inside source list〈access-list 番号〉[変換前開始ポート番号 [変換前終了ポート番号]] pool〈プール名〉[overload | [変換後開始ポート番号　[変換後終了ポート番号]]]

【NAT+時】

ip-vpn nat inside source list〈access-list 番号〉[開始ポート番号 [終了ポート番号]]　NAT+変換後のアドレス overload | [変換後開始ポート番号　[変換後終了ポート番号]]]

【スタティック変換】

ip vpn-nat inside source static〈ローカルアドレス〉〈グローバルアドレス〉

【NAT スタティック（一括変換）】

ip vpn-nat inside source static-subnet〈ローカルサブネット〉〈グローバルサブネット〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前(ローカルアドレス)範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後(グローバルアドレス)範囲を指定した VPN-NAT プール名を指定します。	NAT プール名	NAT の場合は省略不可
NAT+変換後のアドレス	NAT+変換後のアドレスを指定します。 interface　送信インタフェースの	interface modeconfig	NAT+の場合は省略不可

		アドレスに変換	peer <IP アドレス>	
	modeconfig	相手から割り当てられたアドレスに変換		
	peer <IP アドレス>	設定する IP アドレスに変換		
overload	ポート変換する場合に指定		overload	ポート変換しない
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。		1～65535	自動ポート変換
ローカルアドレス	変換前のローカルアドレスを指定します。		IPv4 アドレス形式	省略不可
グローバルアドレス	変換後のグローバルアドレスを指定します。		IPv4 アドレス形式	省略不可
ローカルサブネット	変換前のローカルアドレスを指定します。 ※ static-subnet を指定した場合は、host 部に 1 を指定しないでください。		IPv4 アドレス形式	省略不可
グローバルサブネット	変換後のグローバルアドレスを指定します。 ※ static-subnet を指定した場合は、host 部に 1 を指定しないでください。		IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。		IPv4 アドレス形式	省略不可

最大エントリ数:リスト 1 エントリ(isakmp policy 毎)装置全体で 32 エントリ
スタティック 512 エントリ(装置全体) ※isakmp policy 毎の制限はありません

この設定を行わない場合

VPN-NAT が使用できません。

設定モード

IKE ポリシー設定モード

トンネルルート機能の設定

tunnel-route（装置単位のトンネルルート）

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。

この場合、VPN ピアへの NextHop も合わせて指定します。

tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto security-association
Router(config-crypto-sa)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto security-association
Router(config-crypto-sa)#tunnel-route interface pppoe 1
```

コマンド書式

tunnel-route { address <IP アドレス> | interface <インタフェース名称> }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	ewan 1 pppoe 1～24※1 dialer 1～20※2	

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。

このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IPsec 各種設定モード

tunnel-route（VPN ピア単位のトンネルルート）

IPsec 通信において、本装置が Aggressive モードの Responder となった場合に、VPN ピアへの経路情報をテーブルに登録する場合に指定します。
この場合、VPN ピアへの NextHop も合わせて指定します。
tunnel-route の設定をした装置に crypto isakmp policy の peer-identity distinguished-name を設定すると tunnel-route が動作しません。

crypto security-association モードで、設定する tunnel-route コマンドは装置に対し1つしか設定できないのに対して、本コマンドは、peer 単位で設定することができます。
本コマンドが設定されると、crypto security-association モードで設定されている tunnel-route コマンドより優先的に利用されます。

refresh コマンド後に有効になるコマンドです。

設定例１　VPN ピアへの経路情報を登録する（NextHop は 192.168.100.1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route address 192.168.100.1
```

設定例２　VPN ピアへの経路情報を登録する（NextHop は PPPoE#1 とする）

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#tunnel-route interface pppoe 1
```

コマンド書式

```
tunnel-route { address <IP アドレス> | interface <インタフェース名称>
{ewan <1-2> | pppoe <1-24>}}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	VPN ピアへの経路情報を登録し、NextHop のアドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名称	VPN ピアへの経路情報を登録し、NextHop のインタフェースを設定します。	ewan 1 pppoe 1～24※1 dialer 1～20※2	

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

Aggressive モードの Responder の場合でも、VPN ピアへの経路情報を登録しません。

何のための設定？

Aggressive モードでは、IP アドレスではなく ID で認証できるため、Responder では IPsec のネゴシエーションが始まってから相手の IP アドレスがわかるというケースがあります。
この場合、相手（VPN ピア）の IP アドレスへの経路は、（多くの場合）デフォルトルートにしたがってしまうことになります。
このコマンドにて、まだわからない VPN ピアへの経路情報の NextHop を指定しておき、デフォルトルートとは違う経路で通信を行なうことができるようになります。

設定モード

IKE ポリシー設定モード

SA-UPルート機能の設定

sa-up route

SA-up ルートの nexthop を設定します。
これにより、IPsec SA が張られた際、その ipsec access-list の宛先 IP アドレスの経路情報をルーティングテーブル上に追加します。
（SA が消失した際は、その経路情報はルーティングテーブルから削除されます）

特に、センタ側などで 2 台構成の機器冗長も行う場合、上位で経路制御を行うルータ（又は L3 スイッチ）に対し RIP 等のダイナミックルーティングプロトコルを組み合わせ経路情報の広告のために使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　SA-up ルートの nexthop に 192.168.3.8 を指定します。

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#sa-up route address 192.168.3.8
```

コマンド書式

sa-up route <nexthop> [プロトコル] [distance]

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
nexthop	SA-up ルートの nexthop を IP アドレスまたは、インタフェースで設定します。		IP アドレス形式 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3	省略不可
	IP アドレス	SA-up ルートの nexthop をアドレスで設定します。		
	インタフェース名	SA-up ルートの nexthop をインタフェースで設定します。		
プロトコル	経路情報を広告するためのプロトコルを選択します。		local-prot1 local-prot2	rip で metric 1 で配信します。
distance	登録する経路情報の distance 値を指定します。		1～255	0

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

SA-up ルート機能を使用することができません。

設定モード

VPN セレクタ設定モード

拡張認証の設定

aaa enable

接続相手との認証に、拡張認証(Xautu)を行うかどうかを設定します。
拡張認証(Xautu)を行う場合は、相手のユーザ名・パスワードを aaa peer-name コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　拡張認証を行う

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#aaa enable
```

コマンド書式

aaa enable

パラメータ

パラメータはありません。

この設定を行わない場合

拡張認証を行いません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

設定モード

IKE ポリシー設定モード

aaa my-name

接続相手から拡張認証(Xauth)される場合の、自身のユーザ名とパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　拡張認証で使用する自身のユーザ名を"FITELnet-F100"、パスワードを"F100-pass"とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#aaa my-name FITELnet-F100 password F100-pass
```

コマンド書式

aaa my-name 〈ユーザ名〉〈パスワード〉 [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	相手から拡張認証(Xauth)される場合の相手のユーザ名を設定します。	最大 64 文字の英数字	省略不可
パスワード	相手から拡張認証(Xauth)される場合の相手のパスワードを設定します。	最大 64 文字の英数字	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1:このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2:パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

拡張認証で使用する自身の名前とパスワードはありません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

ワンポイント

相手を拡張認証する場合、相手のユーザ名・パスワードは、"aaa peer-name"コマンドで設定します。

設定モード

IKE ポリシー設定モード

aaa peer-name

相手を拡張認証(Xauth)する場合の、相手のユーザ名とパスワードを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　拡張認証で使用する相手のユーザ名を"VPN-Peer1"、パスワードを"VPN-Peer1-pass"とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#aaa peer-name VPN-Peer1 password VPN-Peer1-pass
```

コマンド書式

aaa peer-name〈ユーザ名〉〈パスワード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ユーザ名	相手から拡張認証(Xauth)される場合の相手のユーザ名を設定します。	最大 64 文字の英数字	省略不可
パスワード	相手から拡張認証(Xauth)される場合の相手のパスワードを設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

相手を拡張認証することはできません。

拡張認証とは？

IPsec では、電子証明書または Pre-shared key での認証のほかに、ユーザ名・パスワードの認証を行うことができ、これを拡張認証といいます。

ワンポイント

自分が拡張認証される場合、自分のユーザ名・パスワードは、"aaa my-name"コマンドで設定します。

設定モード

IKE ポリシー設定モード

configuration mode

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#configuration mode initiate
```

コマンド書式

configuration mode {initiate | respond} [skip]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
initiate	REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。	initiate	省略不可
respond	SET/ACK 制御モードで動作し、set を受信待ちをします。	respond	省略不可
skip	skip を指定することで、mode-config を省略することができます。	skip	mode-config を行います。

この設定を行わない場合

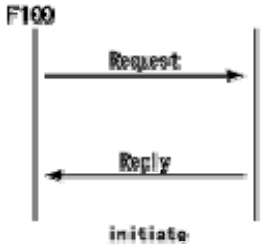
set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

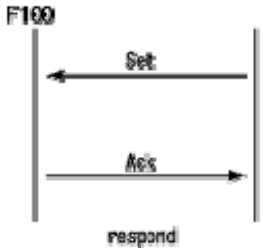
1）configuration mode initiate を指定した場合

本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2）configuration mode respond を指定した場合

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知（Set）を受けて、承認（Ack）を返します。



設定モード

IKE ポリシー設定モード

VPNセレクタの設定

anti-replay

IPsec 通信を行う場合に、使用する回線状態によりパケットの到着順序が前後するような状態が発生すると、Replay Attack 攻撃としてパケットを廃棄してしまい、スループットの低下が発生することがあります。

show vpnlog コマンドを実行して、ログに Replay Attack が表示されるようであれば、本コマンドで disable を指定する事により、スループットの改善が図れる場合があります。

通信状況に応じて disable に設定してください。

refresh コマンド後に有効になるコマンドです。

設定例１　Replay Attack 防御機能を停止して、全てのパケットを受信する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#anti-replay disable
```

コマンド書式

anti-replay <Replay Attack 設定>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Replay Attack 設定	Replay Attack に該当するパケットを破棄するかどうかの設定をします。 enable：Replay Attack に該当するパケットを破棄します。 disable：全てのパケットを受信します。	enable disable	省略不可

この設定を行わない場合

Replay Attack に該当するパケットを破棄します。

設定モード

VPN セレクタ設定モード

crypto map（基本設定モード）

VPN ピアとのセレクタ情報のエントリを設定する為に、VPN セレクタ設定モードに移行します。
設定の際は、セレクタ名称、シーケンス番号を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　VPN セレクタ設定モード（セレクタ名称：Tokyo）に移行する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#
```

コマンド書式

crypto map〈セレクタ名称〉〈シーケンス番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	VPN セレクタの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モードで、適用する VPN セレクタを指定しますので、わかりやすい名称にしてください。	最大 16 文字の英数字	省略不可
シーケンス番号	シーケンス番号を指定します。 既に使用したシーケンス番号と同じ番号を重複して使用すると以前設定した内容を上書きします。	1～2000※	省略不可

※:最大エントリ
F80:64 エントリ
F100:128 エントリ
F1000:2000 エントリ

設定モード

基本設定モード

crypto map（各インタフェース設定モード）

インタフェースに対応付ける VPN セレクタの MAP 名を定義します。
VPN セレクタは、crypto map コマンドで、VPN セレクタ設定モードに移行して、設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 インタフェースに、MAP 名（Tokyo）の VPN セレクタを対応付ける

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#crypto map mymap
```

コマンド書式

crypto map〈セレクタ名称〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セレクタ名称	crypto map コマンドで指定したセレクタ名称を指定します。	–	省略不可

この設定を行わない場合

このインタフェースでは、VPN（IPsec）を使用しません。

設定モード

EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
IPsec インタフェース設定モード

ipsec access-list

IPsec のセレクタ情報を定義します。

refresh コマンド後に有効になるコマンドです。

設定例１　全てのパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip any any
```

設定例２　192.168.100.0/24　→　192.168.200.0/24　宛のパケットを暗号化する

```
Router(config)#ipsec access-list 1 ipsec ip 192.168.100.0
0.0.0.255 192.168.200.0 0.0.0.255
```

設定例３　TCP パケットのみ暗号化する

```
Router(config)#ipsec access-list 1 ipsec tcp any any
```

設定例４　全てのパケットを暗号化しない（bypass）

```
Router(config)#ipsec access-list 64 bypass ip any any
```

コマンド書式

ipsec access-list <ipsec-access-list 番号> { ipsec | bypass | discard } <プロトコル番号> { any | local | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [eq <TCP ポート番号>] [eq <UDP ポート番号>] { any | peer | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> } [eq <TCP ポート番号>] [eq <UDP ポート番号>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipsec-access-list 番号	それぞれの属性の番号を指定します。また、この番号は、VPN セレクタの優先度としても使用されます(数字が小さいほど優先度が高い)	1～2000※	省略不可
ipsec | bypass | discard	暗号化対象とするか、透過(bypass)対象とするか、廃棄対象とするかを指定します。	ipsec 暗号化対象とする bypass 透過対象とする discard 廃棄対象とする	省略不可
プロトコル番号	プロトコル名もしくは、プロトコル番号を選択します。	icmp ICMP ip IP tcp TCP udp UDP 0～255 プロトコル番号を指定	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。 セレクタ情報として相手に通知する場合は、IPaddr=0.0.0.0 Mask=0.0.0.0 で通知します。	any	-
local	自局発信パケットを指定する場合は、"local"を指定します。	local	-
host	送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	-
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
peer	VPN ピア宛を指定する場合は、"peer"を指定します。	peer	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定しま	TCP ポート番号(0～65535)	省略不可

	す。		
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号(0～65535)	省略不可

※:最大エントリ
F80:64 エントリ
F100:128 エントリ
F1000:2000 エントリ

この設定を行わない場合

IPsec 機能を使用することはできません。

設定モード

基本設定モード

match address

暗号化するパケットを指定します。
パケットの送信元・宛先アドレスは、ipsec access-list コマンドで指定し、match address コマンドでは、採用する ipsec access-list 番号を指定します。

IPsec 冗長を行うのであれば「1st/2nd」オプションにてメイン VPN とバックアップ VPN を設定をします。
1st/2nd の 2 つの crypto map を1組設定し、セレクタ番号は同一の番号を指定します。
また、冗長で使用する crypto map は必ず、インターフェースモードにて関連付けを行なわなければなりません。

IPsec 負荷分散を行うのであれば「multi-path」オプションを設定をします。
（分散率の設定には「balance」オプションも使用します）
multi-path の 2 つの crypto map を1組設定し、セレクタ番号は同一の番号を指定します。
また、負荷分散で使用する crypto map は必ず、インターフェースモードにて関連付けを行なわなければなりません。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.0/24 <-> 192.168.200.0/24 を暗号化するパケットとして指定する

```
Router(config)#ipsec access-list 1ipsec ip 192.168.100.0
0.0.0.255 192.168.200.0 0.0.0.255

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#match address 1 1st
```

コマンド書式

match address <IPsec access-list 番号> [1st | 2nd | multi-path [balance 0-10]]]

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>IPsec access-list 番号</td><td>暗号化するパケットとして、IPsec access-list 番号を指定します。</td><td>1～128</td><td>省略不可</td></tr>
<tr><td>1st | 2nd | multi-path [balance {0-10}]</td><td>IPsec 冗長を行う場合は、1st または、2nd を選択します。
IPsec 負荷分散を行う場合は、multi-path balance {0-10}を選択します。
<table>
<tr><td>1st</td><td>IPsec 冗長機能のメイン回線を指定します。</td></tr>
<tr><td>2nd</td><td>IPsec 冗長機能のバックアップ回線を指定します。</td></tr>
<tr><td>multi-path</td><td>IPsec 負荷分散を行う場合指定します。</td></tr>
<tr><td>balance {0-10}</td><td>負荷分散時に、この SA にパケットを振り分ける割合を設定します。</td></tr>
</table></td><td>1st
2nd
multi-path
balance {0-10}</td><td>IPsec 冗長機能を使用しないセレクタになります。</td></tr>
</table>

※:最大エントリ
F80:64 エントリ
F100:128 エントリ
F1000:2000 エントリ

この設定を行わない場合

IPsec を使用できません。

設定モード

VPN セレクタ設定モード

sa-up route

IPsec 冗長機能使用する際に SA-up ルートの nexthop を設定します。
これにより、IPsec SA が張られた際、その ipsec access-list の宛先 IP アドレスの経路情報をルーティングテーブル上に追加します。
(SA が消失した際は、その経路情報はルーティングテーブルから削除されます)
特に、センタ側などで 2 台構成の機器冗長も行う場合、上位で経路制御を行うルータ(又は L3 スイッチ)に対し RIP 等のダイナミックルーティングプロトコルを組み合わせ経路情報の広告のために使用します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SA-up ルートの nexthop に 192.168.3.8 を指定します。

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#sa-up route address 192.168.3.8
```

コマンド書式

```
sa-up route {address <A.B.C.D> | interface <インタフェース名>} [local-
        prot1|local-prot2] [<distance>]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address <A.B.C.D>	SA-up ルートの nexthop をアドレスで設定します。	IP アドレス形式	省略不可
インタフェース名	SA-up ルートの nexthop をインタフェースで設定します。	ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3	省略不可
local-prot1|local-prot2	経路情報を広告するためのプロトコルを選択します。	local-prot1 local-prot2	rip で metric 1 で配信します。
distance	登録する経路情報の distance 値を指定します。	1～255	0

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

IPsec 冗長機能を使用することができません。

設定モード

VPN セレクタ設定モード

set peer

設定している crypto map が SA を確立する VPN ピアのアドレスまたはホスト名を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　設定している crypto map の VPN ピアを"192.168.1.1"に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set peer address 192.168.1.1
```

設定例２　設定している crypto map の VPN ピアを"vpnpeer1"に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set peer host VPN1
```

コマンド書式

set peer address ｛ VPN ピアの IP アドレス ｜ ドメイン名 ｝
set peer host 〈VPN ピアのホスト名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VPN ピアの IP アドレス｜ドメイン名	VPN ピアの IP アドレス、またはドメイン名※1 を指定します。 IKE ポリシー設定モードで設定した VPN ピアの IP アドレス、またはドメイン名と同じである必要があります。	IPv4 アドレス形式 IPv6※1 アドレス形式 ドメイン名※2	省略不可
VPN ピアのホスト名称	VPN ピアの名称を指定します。 IKE ポリシー設定モードで設定した VPN ピアの ID と同じである必要があります。	最大 64 文字の英数字記号	省略不可

※1:ドメイン名および IPv6 アドレス形式の指定は、F100/F1000 のみになります。

※2:ドメイン名として設定できる文字は、127 文字までの大文字 (A ～ Z)、小文字 (a ～ z)、数字 (0 ～ 9)、ハイフン (-) 、ドット(.)のみが設定できます。

この設定を行わない場合

IPsec を使用できません。

ホスト名について

このホスト名は、Aggressive モードで Responder の場合に、相手が通知してくる ID として使用されます。

設定モード

VPN セレクタ設定モード

set pfs

PFS (Perfect Forward Security)を行なう際に、Diffie-Hellman 鍵交換を使用した Oakley と呼ばれる暗号化技術を使用します。
このコマンドは Oakley Group を指定します。
Diffie-Hellman Group には、1(768-bit)と、2(1024-bit)と、5(1536-bit)の 3 種類があります。

refresh コマンド後に有効になるコマンドです。

設定例１　PFS 使用時の Oakley Group に、Group2 を使用する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set pfs group2
```

コマンド書式

set pfs 〈DH グループ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DH グループ	Diffie-Hellman グループ番号を指定します。	group1 group2 group5	省略不可

この設定を行わない場合

PFS を使用しません。

PFS とは？

Quick Mode キーが生成されるたびにキーの再交換を要求する Internet Key Exchange (IKE)の手順です。また、その際にキーの大きさ(Group1 or Group2)を指定します。
セキュリティの面では強固となりますが、キーの交換に時間がかかる欠点があります。

FITELnet-F シリーズの工場出荷時状態は、PFS を行なわない設定になっています。

設定モード

VPN セレクタ設定モード

set redundancy

メイン回線で通信が出来なくなった場合に、nexthop アドレスを使用して、バックアップ側に crypto map で関連づけれらたセレクタとピアに対してルート情報を追加します。ただし、crypto map を ewan <1-2>に設定して使用し、アドレスをマニュアルで設定しているのであれば、redundancy address 設定は必ず必要ですが、dhcp/pppoe/dialer の場合は特に設定の必要はありません。

また、delete message を設定することによりバックアップ回線からメイン回線に復帰するときに、バックアップのピアに対して、Phase1,Phase2(In/Out)の delete message を送信します。
受信側ピアは FITELnet-F シリーズ限定です。

設定例１　バックアップ時に登録する経路情報の next hop アドレスを 192.168.50.3 にする

```
Router(config)# crypto map 1
Router(config-crypto-map)# set redundancy address 192.168.50.3
```

コマンド書式

```
set redundancy {address <A.B.C.D> | delete-message-send}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address <A.B.C.D>	バックアップを行なう相手の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
delete-message-send	delete-message を送信します。	delete-message-send	省略不可

この設定を行わない場合

IPsec 冗長機能を使用することができません。

設定モード

VPN セレクタ設定モード

set redundancy distance

メイン SA 障害時に、バックアップ SA に切替わる際のバックアップ経路の distance 値を設定します。

設定例１　バックアップ時に登録する経路情報の distance 値を 10 にする

```
Router(config)# crypto map 1
Router(config-crypto-map)# set redundancy distance 10
```

コマンド書式

set redundancy distance <distance 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distance 値	バックアップ経路の distance 値を設定します。	1～255	省略不可

この設定を行わない場合

バックアップ経路の優先度が最優先となってしまうため、unicastRIP もスタティックルートも無効となります。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

VPN セレクタ設定モード

set security-association always-up

SA の確立状態を維持するかどうかを指定します。
このコマンドを設定した場合、一度確立した SA は確立し続けます。万一、SA が切断した場合は確立するまでリトライし続けます。

IPsec の Aggressive モードで運用する場合に、Initiator 側に設定しておくと効果的です。
センタ側 FITELnet-F シリーズ(固定 IP)-----拠点側 FITELnet-F シリーズ(動的 IP)
上記の環境では通常センタ側契機の VPN は張れないため、ライフタイム等で SA の消失後はセンタ側から通信が行えません。
このコマンドを使用することで拠点側より常時 SA が確立されるため、センタ側からの通信が不能になることはありません。

refresh コマンド後に有効になるコマンドです。

設定例１　SA を常時接続とする

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association always-up
```

コマンド書式

```
set security-association always-up
```

パラメータ

パラメータはありません。

この設定を行わない場合

確立した SA は、Lifetime の設定に従い解放します。

設定モード

VPN セレクタ設定モード

set security-association ipsec-src-id

Phase2 ID ペイロードの IP アドレスおよびアドレスマスクを定義します。
NAT 動作モードが”nat ”(1 対 1 変換)の場合で、変換後のアドレスが複数存在する場合に、その複数のアドレス(範囲)をこのコマンドで指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換後のアドレスが 192.168.100.0/21 になる場合

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association ipsec-src-id
192.168.100.0 0.0.0.7
```

コマンド書式

set security-association ipsec-src-id 〈IP アドレス〉〈Wildcard マスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	NAT 変換後の IP アドレス 変換後のアドレスを範囲で指定することができます。 詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可
Wildcard マスク	変換後のアドレスを範囲指定するために、Wildcard マスクを指定します。詳細は範囲指定方法を参照してください。	IPv4 アドレス形式	省略不可

この設定を行わない場合

1 つのアドレス情報でセレクタ情報を送信します。

範囲指定方法

set security-association ipsec-src-id コマンドで IP アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。

例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0

例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

設定モード

VPN セレクタ設定モード

set security-association lifetime

Phase2 SA の生存時間を設定します。
Phase2 SA の生存時間は、時間と中継データ量で指定することができます。

refresh コマンド後に有効になるコマンドです。

設定例１　Phase2 SA の生存時間を 3600 秒に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime seconds 3600
```

設定例２　Phase2 SA の生存中継データ量を 1000byte に設定する

```
Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set security-association lifetime kilobytes 1000
```

コマンド書式

set security-association lifetime { seconds 〈生存時間〉 | kilobytes 〈生存中継データ量〉 }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
生存時間	Phase2 SA の生存時間(秒)を設定します。	60～4294967295	省略不可
生存中継データ量	Phase2 SA の生存中継データ量(KB)を設定します。	1000～4294967295	省略不可

※ 時間とデータの両方を指定した場合は、時間が経過したもしくは指定したデータ量の通信が行なわれた場合(先に満了したタイミングで)に、Phase2 SA を解放します。

この設定を行わない場合

生存時間は、600 秒です。
バイト数での生存時間は存在しません。

VPN ピアと設定が異なる場合

SA を確立しようとしている VPN ピアと、生存時間の設定が異なる場合は、次のようになります。

initiator の場合	自装置の設定値を採用します。
responder の場合	自装置の設定値と相手からの提案された値を比較して、小さい方を採用します。

設定モード

VPN セレクタ設定モード

set transform-set

ipsec transform-set コマンドで設定する Phase2 の暗号化ポリシーを対応付けます。

refresh コマンド後に有効になるコマンドです。

設定例１　このセレクタにおいては、ipsec transform-set で指定した"policy1"のポリシーを使用する

```
Router(config)#ipsec transform-set policy1 esp-des esp-md5-hmac

Router(config)#crypto map Tokyo 1
Router(config-crypto-map)#set transform-set policy1
```

コマンド書式

set transform-set <Phase2 ポリシー名称>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Phase2 ポリシー名称	ipsec transform-set で設定した Phase2 ポリシー名称を指定します。	16 文字以内の英数字	省略不可

この設定を行わない場合

暗号化方式:DES、認証アルゴリズム:MD5 で動作します。

設定モード

VPN セレクタ設定モード

電子証明書に関する設定

crl-optional

証明書の有効性を CRL で確認するかしないかを設定します。

設定例１　証明書の有効性を必ず CRL で確認する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#crl-optional must
```

コマンド書式

crl-optional <CRL 設定>

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
CRL 設定	この証明書に関して、CRL を使用するかどうかを指定します。		must notuse	省略不可
	must	証明書の有効性を必ず CRL で確認します。CRL が取得できない場合は、無効と判断されます。		
	notuse	証明書の有効性を CRL で確認しません。		

この設定を行わない場合

CRL を取得(20 秒以内)できれば証明書の有効性を確認しますが、取得できなければ確認を行いません。

設定モード

電子証明書(自身の ID)設定モード

email

証明書リクエストファイルに含める電子メールアドレスを設定します。電子メールアドレスの情報を含めない場合は、設定の必要はありません。

設定例１　証明書リクエストファイルに含める電子メールアドレスとして、F100@xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#email F100@xxxxx.ne.jp
```

コマンド書式

email〈電子メールアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
電子メールアドレス	証明書リクエストファイルに含める電子メールアドレスを設定します。	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、E-Mail アドレスを含めることはできません。

設定モード

電子証明書(自身の ID)設定モード

ip address

証明書リクエストファイルに含めるIPアドレスを設定します。IPアドレスの情報を含めない場合は、設定の必要はありません。

設定例１　証明書リクエストファイルに含めるIPアドレスとして、192.168.1.1を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip address 192.168.1.1
```

コマンド書式

ip address <IPアドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPアドレス	証明書リクエストファイルに含めるIPアドレス	IPv4アドレス形式	省略不可

この設定を行わない場合

証明書リクエストファイルに、IPアドレスを含めることはできません。

設定モード

電子証明書(自身のID)設定モード

ip domain-name

証明書リクエストファイルに含めるドメイン名称を設定します。ドメイン名称の情報を含めない場合は、設定の必要はありません。

設定例１　証明書リクエストファイルに含めるドメイン名称として、xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#ip domain-name xxxxx.ne.jp
```

コマンド書式

ip domain-name 〈ドメイン名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	証明書リクエストファイルに含めるドメイン名称	最大 64 文字	省略不可

この設定を行わない場合

証明書リクエストファイルに、ドメイン名を含めることはできません。

設定モード

電子証明書(自身の ID)設定モード

name server

CRL を HTTP サーバに取りに行く場合の名前解決に使用するネームサーバーの IP アドレスを設定します。

設定例１　ネームサーバの IP アドレスを、192.168.100.1 に設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#name server 192.168.100.1
```

コマンド書式

name server〈ネームサーバの IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ネームサーバの IP アドレス	CRL を HTTP サーバに取りに行く場合の名前解決に使用するネームサーバーの IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

電子証明書(自身の ID)設定モード

query-ip

CRL を LDAP サーバに取りに行く場合の LDAP サーバの IP アドレスを設定します。

設定例１　LDAP サーバの IP アドレスを 192.168.100.2 に設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#query-ip 192.168.100.2
```

コマンド書式

query-ip <LDAP サーバの IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LDAP サーバの IP アドレス	CRL を LDAP サーバに取りに行く場合の LDAP サーバの IP アドレスを設定します。	IPv4 アドレス形式	省略不可

設定モード

電子証明書(自身の ID)設定モード

IPsecのログ情報に関する設定

multi-path 【F1000 専用コマンド】

slog に IPsec 負荷分散の状態表示(single-path または、multi-path)に関するログ情報を表示させる場合に設定します。

設定例１　IPsec アクセスリスト１に関する負荷分散のログのみを記録する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#multi-path eq 1
```

コマンド書式

multi-path {all | eq <1-2000> | gt <1-2000> | lt <1-2000> | neq <1-2000> | range <1-2000> <1-2000>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
all	全ての IPsec アクセスリストを対象とします。	all	省略不可
eq <1-2000>	指定する IPsec アクセスリスト番号を持つパスが対象となります。	1～2000	
gt <1-2000>	指定する IPsec アクセスリスト番号より大きい番号を持つパスが対象となります。		
lt <1-2000>	指定する IPsec アクセスリスト番号より小さい番号を持つパスが対象となります。		
neq <1-2000>	指定する IPsec アクセスリスト番号以外の番号を持つパスが対象となります。		
range <1-2000> <1-2000>	IPsec アクセスリストの範囲を指定し範囲内の番号を持つパスが対象となります。		

この設定を行わない場合

IPsec 負荷分散の状態表示に関するログを表示することができません。
ただし、no-path 状態はログを表示します。

※:F80/100 に関しては、デフォルトで状態表示に関するログを表示します。

設定モード

IPsec ログモード

nolog-block-type-discard

vpnlog の"block type discard ～"を抑制する設定を行います。
受信したパケットを暗号化するかどうか判断するためにセレクタ検索をする際に、下記のような場合に上記ログが記載されます。
1)マッチした ipsec access-list が discard だった場合。
2)設定された ipsec access-list にマッチしなかった場合。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

設定例１　block type discard の vpnlog を抑制する設定をする

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-block-type-discard
```

コマンド書式

nolog-block-type-discard

パラメータ

パラメータはありません

設定モード

IPsec ログモード

nolog-spi-no-match

"SPI no match ～"の vpnlog を抑制する設定を行います。
受信した ESP パケットが自装置宛にもかかわらず、パケットに格納されている SA が自装置管理下にある SA にマッチしなかった場合に出力されるログを抑制します。
このコマンドで該当するログを抑制することにより、他のログを参照しやすくすることができます。

refresh コマンド後に有効になるコマンドです。

設定例１　"SPI no match ～"の vpnlog を抑制する設定を行う

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-spi-no-match
```

コマンド書式

nolog-spi-no-match

パラメータ

パラメータはありません

設定モード

IPsec ログモード

vpnlog-detail

IKE、IPSEC ネゴの vpnlog と、keepalivefail の vpnlog 出力をピア No.ごとに設定します。
また、本コマンドを設定すると、vpnlog enable コマンドで設定した内容が有効になりません。

refresh コマンド後に有効になるコマンドです。

設定例１　keepalivefail の vpnlog 出力を全て表示する

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#vpnlog-detail all
```

コマンド書式

vpnlog-detail　[all | [<属性> <ピア番号>]

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
属性	ピア番号を範囲で指定するために、ポート属性を指定します。		all eq 1～500 gt 1～499 lt 2～500 neq 1～500 range 1～500 1～500	全パス対象に全てのログを表示します。
	all	全てのピア番号が対象となります。		
	eq※1 1～500	指定するピア番号を持つパスが対象となります。		
	gt※2 1～499	指定するピア番号より大きい番号を持つパスが対象となります。		
	lt※1 2～500	指定するピア番号より小さい番号を持つパスが対象となります。		
	neq※1 1～500	指定するピア番号以外の番号を持つパスが対象となります。		
	range※1 1～500 1～500	ピア番号の範囲を指定し範囲内の番号を持つパスが対象となります。		

※1:F80 の場合は、最大値が 32 になります。
　　F100 の場合は、最大値が 100 になります。
※2:F80 の場合は、最大値が 31 になります。
　　F100 の場合は、最大値が 99 になります。

設定モード

IPsec ログモード

IPsecの各種設定

alive

IPsec SA の KeepAlive として、ICMP を使用する場合のタイマ値/送信回数等を設定します。

設定例１　１回の KeepAlive で４つの ICMP を送信し、そのうち３つ以上応答が無かった場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3
```

設定例２　１回の KeepAlive で４つの ICMP を送信し、そのうち３つ以上応答が無い状態が３回以上続いた場合に SA の障害とみなす

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive count 4 3 fail 3
```

設定例３　ICMP の KeepAlive のタイムアウト時間を３秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive timeout 3
```

設定例４　ICMP の KeepAlive を 60 秒間隔で送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#alive freq 60
```

コマンド書式

alive count <ICMP 送信数> <ICMP 失敗数> [fail <ICMP 連続失敗回数>]
alive freq <送信間隔> [degraded-freq <送信間隔>]
alive timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP 送信数	1 回の KeepAlive で送信する ICMP の数を設定します。	1～15	省略不可
ICMP 失敗数	1 回の KeepAlive で送信した ICMP 数のうち、何個応答を受け取れなかった時に監視失敗と判定するかを設定します。	1～15	省略不可
ICMP 連続失敗回数	何回連続して ICMP 監視に失敗したら SA の障害と判定するかを設定します。	1～10	1
送信間隔	正常時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	省略不可
degraded-freq <送信間隔>	リトライ時の ICMP KeepAlive の送信間隔(秒)を設定します。	5～1000	60
timeout 時間	ICMP KeepAlive の応答待ち時間(秒)	3～60	省略不可

この設定を行わない場合

ICMP 送信数	4 回
ICMP 失敗数	3 回
ICMP 連続失敗回数	1 回
送信間隔	60 秒
degraded-freq 送信間隔	60 秒
timeout 時間	3 秒

設定モード

IPsec 各種設定モード

always-up check-interval

SA の確立状態を維持する場合の、always-up の監視間隔を指定します。
本コマンドは、set security-association always-up コマンドで、SA の確立状態を維持する設定にした場合のみ有効です。

設定例１　always-up の監視間隔を 10 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#always-up check-interval 10
```

コマンド書式

always-up check-interval 〈監視間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
監視間隔	always-up の監視間隔(秒単位)を設定します。	1～20	省略不可

この設定を行わない場合

always-up の監視間隔は 20 秒となります。

設定モード

IPsec 各種設定モード

am-3-encr

Aggressive モードによるネゴシエーションの 3 番目の ISAKMP パケットを暗号化する場合に指定します。
VPN ピアが CISCO3030 の場合は、指定が必要です。

設定例１　Aggressive モードの 3 番目のパケットを暗号化する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#am-3-encr
```

コマンド書式

am-3-encr

パラメータ

パラメータはありません。

この設定を行わない場合

Aggressive モードのネゴシエーションの 3 番目の ISAKMP パケットは、暗号化しません。

設定モード

IPsec 各種設定モード

am-3-initcont

Aggressive モードによるネゴシエーションの 3 番目の ISAKMP パケットに、INITIAL-CONTACT を送出します。

設定例１　3 番目の Aggressive パケットに INITIAL-CONTACT を送出する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#am-3-initcont
```

コマンド書式

am-3-initcont

パラメータ

パラメータはありません。

この設定を行わない場合

Aggressive の完了後に informational パケットの INITIAL-CONTACT を送出します。

設定モード

IPsec 各種設定モード

configuration mode

mode-config のネゴシエーションにおいて、REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　REQUEST/REPLY 制御で動作する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration mode initiate
```

コマンド書式

configuration mode〈制御モード〉

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
制御モード	REQUEST/REPLY 制御で動作するか SET/ACK 制御で動作するかを設定します。		initiate respond	省略不可
	initiate	REQUEST/REPLY 制御モードで動作し、自装置から req を送信します。		
	respond	SET/ACK 制御モードで動作し、set を受信待ちをします。		

この設定を行わない場合

set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

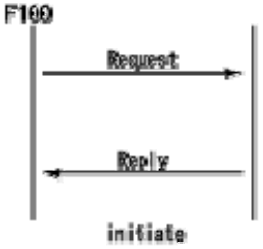
モードコンフィグの手法

モードコンフィグは、VPN 通信を行う際に Peer 同士の情報を交換する手法であり、情報交換方法は 2 パターンあります。

1）configuration mode initiate を指定した場合

※F100 を例に説明しています。

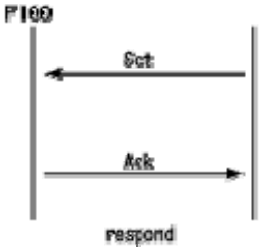
本装置はモードコンフィグのイニシエータとして動作します。
本装置から、モードコンフィグのレスポンダに対して、要求（Request）を送信して、返答（Reply）を待ちます。



2) configuration mode respond を指定した場合

※F100 を例に説明しています。

本装置はモードコンフィグのレスポンダとして動作します。
本装置は、モードコンフィグのイニシエータから通知(Set)を受けて、承認(Ack)を返します。



設定モード

IPsec 各種設定モード

configuration mode application-version message

configuration mode コマンドで initiate を選択した場合に、アプリケーションバージョン属性にセットする値を指定します。respond を選択した場合は、利用しません。

refresh コマンド後に有効になるコマンドです。

設定例１　アプリケーションバージョンの値をセットする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration application-version message fitel
```

コマンド書式

```
configuration mode application-version message <Word>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Word	アプリケーションバージョン属性にセットする値を指定します。	127 文字以内	省略不可

※ スペースも文字数としてカウントされます。
例:ＡＢＣの場合、5 文字としてカウントされます。

この設定を行わない場合

装置名と版数をセットします。

設定モード

IPsec 各種設定モード

configuration mode application-version push

configuration application-version message コマンドの設定があり、かつ、configuration mode コマンドで initiate が設定されている場合に、configuration application-version message コマンドのメッセージをセットして req パケットを送信します。
configuration application-version message コマンドの設定がない場合は、configuration application-version message コマンドのデフォルト値を使用して req パケットを送信します。

refresh コマンド後に有効になるコマンドです。

設定例１　アプリケーションバージョンに値をセットして request を送信する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#configuration application-version push
```

コマンド書式

configuration application-version push

パラメータ

パラメータはありません

この設定を行わない場合

request パケットのアプリケーションバージョン欄を null で送信します。

設定モード

IPsec 各種設定モード

crypto security-association

IPsec 機能全般の、各種タイマ値等を設定するために、IPsec 各種設定モードに移行します。

設定例１　IPsec 各種設定モードに移行する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#
```

コマンド書式

crypto security-association

パラメータ

パラメータはありません。

設定モード

基本設定モード

ikealive freq

IKE KeepAlive の送信間隔を設定します。

設定例１　IKE KeepAlive の送信間隔を 30 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive freq 30
```

コマンド書式

ikealive freq 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	IKE KeepAlive 送信間隔を設定します。	10～3600 秒	省略不可

この設定を行わない場合

送信間隔は 60 秒です。

設定モード

IPsec 各種設定モード

ikealive retry max

IKE KeepAlive のリトライ回数を設定します。

設定例１　IKE KeepAlive のリトライ回数を 3 回に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive retry max 3
```

コマンド書式

ikealive retry max 〈リトライ回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	IKE KeepAlive のリトライ回数を設定します。	1～5	省略不可

この設定を行わない場合

リトライ回数は 1 回です。

設定モード

IPsec 各種設定モード

ikealive retry timer

IKE KeepAlive のリトライ間隔を設定します。

設定例１　IKE KeepAlive のリトライ間隔を 10 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)# ikealive retry timer 10
```

コマンド書式

ikealive retry timer 〈リトライ間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	IKE KeepAlive のリトライ間隔を設定します。	2～60 秒	省略不可

この設定を行わない場合

リトライ間隔は 20 秒です。

設定モード

IPsec 各種設定モード

isakmp-negotiation

Phase1 の SA のライフタイムが満了する前に、新しい SA を確立するために Phase1 のネゴシエーションを開始します。
本コマンドでは、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。

設定例１　本装置が Initiator の場合は、ライフタイム満了の 100 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#isakmp-negotiation initiate 100
```

コマンド書式

```
isakmp-negotiation { initiate <Initiator 時のネゴシエーション開始時期> |
                     respond <Responder 時のネゴシエーション開始時期> }
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Initiator 時のネゴシエーション開始時期	自身が Initiator の SA について、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するか	1～86400	省略不可
Responder 時のネゴシエーション開始時期	自身が Responder の SA について、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するか	1～86400	省略不可

※:Phase1 の SA や Phase2 の SA を頻繁に更新するような lifetime 設定や rekey 設定は、装置負荷を高める要因となりますので行わないでください。

この設定を行わない場合

Initiator 時のネゴシエーション開始時期	90 秒前
Responder 時のネゴシエーション開始時期	30 秒前

設定モード

IPsec 各種設定モード

negotiation

本装置では、Phase2 の SA のライフタイムが満了する前に、新しい SA を確立するために Phase2 のネゴシエーションを開始します。
本コマンドでは、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するかを設定します。
この値は、本装置自身が Initiator の場合と Responder の場合で、設定値を変更することができます。

設定例１　本装置が Initiator の場合は、ライフタイム満了の 90 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation initiate 90
```

設定例２　本訴装置が Responder の場合は、ライフタイム満了の 30 秒前にネゴシエーションを開始する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#negotiation respond 30
```

コマンド書式

negotiation { initiate 〈Initiator 時のネゴシエーション開始時期〉 | respond 〈Responder 時のネゴシエーション開始時期〉 }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Initiator 時のネゴシエーション開始時期	自身が Initiator の SA について、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するか	1～255	省略不可
Responder 時のネゴシエーション開始時期	自身が Responder の SA について、ライフタイムが満了する何秒前に新しい SA のためのネゴシエーションを開始するか	1～255	省略不可

この設定を行わない場合

Initiator 時のネゴシエーション開始時期	90 秒前
Responder 時のネゴシエーション開始時期	30 秒前

設定モード

IPsec 各種設定モード

re-establish-sa rekey

Phase1 の SA の Rekey 動作を行います。

refresh コマンド後に有効になるコマンドです。

設定例１　Phase1 の SA の Rekey 動作を行う。

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#re-establish-sa rekey
```

コマンド書式

re-establish-sa rekey

パラメータ

パラメータはありません。

この設定を行わない場合

Phase1 の SA の Rekey 動作を行いません。

設定モード

IKE ポリシー設定モード

retry

ISAKMP による自動鍵交換の再送間隔(パラメータ:timer)と、最大再送回数(パラメータ:max)を設定します。

設定例１　ISAKMP による自動鍵交換の再送間隔を 20 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry timer 20
```

設定例２　ISAKMP による自動鍵交換の最大再送回数を 1 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry max 1
```

コマンド書式

retry timer 〈再送間隔〉
retry max 〈最大送信回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	ISAKMP による自動鍵交換の再送間隔(単位:秒)を設定します。	1～30	省略不可
最大送信回数	ISAKMP による自動鍵交換の最大再送回数を設定します。	1～5	省略不可

この設定を行わない場合

送信間隔	20 秒
最大送信回数	1 回

設定モード

IPsec 各種設定モード

retry guard-time

IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間を設定します。

設定例１　対向の再送パケットの受け入れ可能時間を 5 秒に設定する

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry guard-time 5
```

コマンド書式

retry guard-time（受信可能時間）

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
受信可能時間	IKE ネゴパケットの送受信において、自身が送信してから対向の再送パケットを受け入れ可能とするまでの時間(単位:秒)を設定します。	1～30	省略不可

この設定を行わない場合

受信可能時間を 1 秒に設定します。

設定モード

IPsec 各種設定モード

retry rekey-ipsec

IPsec-SA の Rekey のリトライ間隔(パラメータ:timer)と、リトライ回数(パラメータ:max)を設定します。

設定例１　IPsec-SA の Rekey のリトライ間隔を 20 秒とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec timer 20
```

設定例２　IPsec-SA の Rekey のリトライ回数を 3 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec max 3
```

コマンド書式

retry rekey-ipsec timer <リトライ間隔>
retry rekey-ipsec max {<リトライ回数>|lifetime}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	IPsec-SA の Rekey のリトライ間隔(単位:秒)を設定します。	1～30	省略不可
リトライ回数	IPsec-SA の Rekey のリトライ回数を設定します。	1～20	省略不可
lifetime	IPsec-SA の Rekey のリトライを lifetime 満了まで繰り返します。	lifetime	省略不可

この設定を行わない場合

送信間隔	retry timer コマンドで設定した間隔になります。
送信回数	retry max コマンドで設定した回数になります。

設定モード

IPsec 各種設定モード

retry rekey-ipsec negotiation

IPsec-SA の Rekey のリトライオーバー後、再度 Rekey 機能を行う場合の Rekey 回数(パラメータ:max)を設定します。

設定例１　IPsec-SA の Rekey のリトライオーバー後に再度 Rekey を行う回数を 3 回とする

```
Router(config)#crypto security-association
Router(config-crypto-sa)#retry rekey-ipsec negotiation 3
```

コマンド書式

retry rekey-ipsec negotiation {<Rekey 回数>|lifetime}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
Rekey 回数	IPsec-SA の Rekey のリトライオーバー後、再度 Rekey 機能を行う場合の回数を指定します。	1～20	省略不可
lifetime	IPsec-SA の Rekey のリトライオーバー後、lifetime 満了まで Rekey 機能を繰り返します。	lifetime	省略不可

この設定を行わない場合

Rekey を行いません。

設定モード

IPsec 各種設定モード

IP in IP機能

IP in IP機能

ip address

インタフェースの IP アドレス、サブネットマスクを設定します。

設定例１　PPPoE１の IP アドレスを 192.168.0.1 に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 192.168.0.1
```

設定例２　EWAN１の IP アドレスを 192.168.0.1、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip address 192.168.0.1 255.255.255.0
```

コマンド書式

ip address <IP アドレス> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	インタフェースに割り当てるサブネットマスク※を設定します。	IPv4 アドレス形式	省略不可

※PPPoE およびループバックインタフェースでは、サブネットマスクの指定はできません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
ループバックインタフェース設定モード
トンネルインタフェース設定モード

ip address unnumbered

指定したインタフェースに設定されている IP アドレスを使用します。
指定したインタフェースのアドレスが固定設定されていない場合は、トンネルインタフェースに使用することは出来ません。
このインタフェースからデータを送信する必要がある場合に、送信元アドレスとして使用します。

設定例１　LAN インタフェースの IP アドレスをトンネルインタフェースのアドレスに使用する

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#ip address unnumbered lan 1
```

コマンド書式

ip address unnumbered 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	指定したインタフェースに設定されている IP アドレスを使用します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 vlanif 1～16 loopback 1	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

インタフェースのアドレスを送信元アドレスとして使用しない。

設定モード

トンネルインタフェース設定モード

tunnel destination

トンネルの宛先アドレスを IPv4 アドレス形式で指定します。
tunnel source コマンドの設定とアドレスファミリを合わせてください。

設定例１　トンネルの宛先アドレスを 192.168.100.1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel destination 192.168.100.1
```

コマンド書式

tunnel destination〈宛先アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先アドレス	トンネルの宛先アドレスを設定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

トンネルの宛先アドレスを指定しません。

設定モード

トンネルインタフェース設定モード

tunnel mode

トンネルのモードを ipip(IP in IP tunneling)に設定します。

設定例１　トンネルのモードを ipip とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel mode ipip
```

コマンド書式

```
tunnel mode ipip
```

パラメータ

パラメータはありません。

この設定を行わない場合

トンネルインタフェースを使用できません。

設定モード

トンネルインタフェース設定モード

tunnel source

トンネルの送信元アドレスを IPv4 アドレス形式または、IPv6 アドレス形式で指定します。
tunnel destination コマンドの設定とアドレスファミリを合わせてください。

設定例１　トンネルの送信元アドレスを 192.168.0.1 とする

```
Router(config)#interface tunnel 1
Router(config-if tunnel 1)#tunnel source 192.168.0.1
```

コマンド書式

tunnel source〈送信元アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信元アドレス	トンネルの送信元アドレスを設定します。	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

この設定を行わない場合

トンネルの送信元アドレスを指定しません。

設定モード

トンネルインタフェース設定モード

NAT機能

NAT機能

ip nat log-table-changes

NAT 変換テーブルの作成/削除時に、slog に出力するかどうかの設定です。

refresh コマンド後に有効になるコマンドです。

設定例　NAT 変換テーブルの作成/削除時に、slog に出力する

```
Router(config)#ip nat log-table-changes
```

コマンド書式

ip nat log-table-changes

パラメータ

パラメータはありません

この設定を行わない場合

NAT 変換テーブルの作成/削除時に、slog に出力しません。

設定モード

基本設定モード

ip nat reserved-sessions

NAT 変換動作において、UPnP で要求された変換ルールや自局発着の通信のため、指定したセッション数だけ変換テーブルを予約することができます。
この設定により、NAT 変換テーブルが溢れてしまった場合でも、UPnP でポート変換を予約した通信や、DNS 問合せ等の自局発着通信が可能となります。

refresh コマンド後に有効になるコマンドです。

設定例　NAT 変換テーブルを 10 セッション分予約する

```
Router(config)#ip nat reserved-sessions 10
```

コマンド書式

ip nat reserved-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	NAT 変換動作において、予約する変換テーブルの数を設定します。	1～100	省略不可

この設定を行わない場合

変換テーブルの予約は行いません。

設定モード

基本設定モード

ip nat max-sessions

NAT 変換テーブルの総数を設定します。

設定例　NAT 変換テーブルを 16384 セッション分設定する

```
Router(config)#ip nat max-sessions 16384
```

コマンド書式

ip nat max-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	NAT テーブルの最大数を設定します。	2048～16384	省略不可

この設定を行わない場合

2048

設定モード

基本設定モード

ip nat translation finrst-timeout

TCP の FIN フラグまたは RST フラグが設定されたパケットについて NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　FIN/RST フラグが設定されたパケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation finrst-timeout 10
```

コマンド書式

ip nat translation finrst-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	FIN/RST フラグが設定されたパケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

60 秒が設定されます。

FIN フラグとは？

TCP コネクションで、コネクションを解放する場合に、FIN フラグをセットした TCP パケットを送信します。
TCP のプロトコルでは、FIN を送信した側は FIN-ACK を受信することで、TCP のコネクションの解放となります。
つまり、FIN を送信した側が FIN-ACK を受信できなかった場合、TCP コネクションの解放を行なうことができません。

FITELnet-F シリーズで NAT 機能を使用するような場合、FIN のデータは TCP の解放であり、その後このコネクションを使用してデータ通信を行なう必要がないため、他のデータに比べて NAT テーブルを長期間保持しておく必要がありません。したがって、他のデータより、タイムアウト時間を短く設定しておく運用が考えられます。

ご使用の環境に合わせて、設定変更を行なってください。

RST フラグとは？

TCP コネクションで、アプリケーションの指定により TCP コネクションを中断する場合に、RST フラグをセットした TCP パケットを送信します。

FITELnet-F シリーズで NAT 機能を使用するような場合、RST のデータは TCP の中断であり、その後このコネクションを使用してデータ通信を行なう必要がないため、他のデータに比べて NAT テーブルを長期間保持しておく必要がありません。したがって、他のデータより、タイムアウト時間を短く設定しておく運用が考えられます。

ご使用の環境に合わせて、設定変更を行なってください。

設定モード

基本設定モード

ip nat translation icmp-timeout

ICMP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　ICMP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation icmp-timeout 10
```

コマンド書式

ip nat translation icmp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	ICMP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

60 秒が設定されます。

設定モード

基本設定モード

ip nat translation tcp-timeout

TCP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　TCP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation tcp-timeout 10
```

コマンド書式

ip nat translation tcp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	TCP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

3600 秒が設定されます。

設定モード

基本設定モード

ip nat translation timeout

NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation timeout 10
```

コマンド書式

ip nat translation timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

86400 秒が設定されます。

他のコマンドとの連携

特定のパケットに対するタイムアウト時間を設定することができます。
・TCP　(ip nat translation tcp-timeout)
・TCP(FIN/RST)　(ip nat translation finrst-timeout)
・UDP　(ip nat translation udp-timeout)
・ICMP　(ip nat translation icmp-timeout)
これらが設定されている場合は、そちらのタイマに従い、特定されていないパケットについては、本コマンドの設定に従います。

設定モード

基本設定モード

ip nat translation udp-timeout

UDP について NAT/NAT+変換する場合に、装置の内部テーブルにデータをエージアウトする時間(秒)を設定します。

設定例　UDP パケットの NAT 変換タイムアウトを 10 秒に設定する

```
Router(config)#ip nat translation udp-timeout 10
```

コマンド書式

ip nat translation udp-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	UDP パケットについての NAT/NAT+変換テーブルのタイムアウト時間(秒)	1～86400	省略不可

この設定を行わない場合

300 秒が設定されます。

設定モード

基本設定モード

ip nat inside source

そのインタフェースから送信するパケットの送信元アドレスの変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source list 1 pool pool1


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
                                                ↑list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7
                                                ↑pool1 の部分の設定
```

【解説】

ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)#interface ewan 1
Router(config-if lan 1)#ip nat inside source list 1 interface


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
                                                ↑list 1 の部分の設定
```

【解説】

ip nat inside source <変換前のアドレス範囲> <変換後のアドレス範囲>となります。
<変換前のアドレス範囲>は、access-list コマンドで指定します。
<変換後のアドレス範囲>は、インタフェースアドレスに集約しますので、"interface"と指定します。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source static 192.168.0.1
158.xxx.xxx.2
Router(config-if lan 1)#ip nat inside source list 1 pool pool1
Router(config-if lan 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
                                              ↑list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7
                                              ↑pool1 の部分の設定
```

【解説】

設定例1とほぼ同じです。

違う点は、ip nat inside source static で、NAT スタティック変換をしている箇所ですが、この場合も、ip nat inside source <変換前のアドレス> <変換後のアドレス>となります。

この場合、ip nat inside destination コマンドを使用して、グローバル側→ローカル側のスタティック登録を行なう必要があります。(①の部分)

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source static-subnet
192.168.100.0 158.xxx.xxx.0 255.255.255.0
```

【解説】

ip nat inside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】

ip nat inside source list 〈access-list 番号〉[変換前開始ポート番号 [変換前終了ポート番号]] pool 〈プール名〉[overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【NAT+時】

ip nat inside source list 〈access-list 番号〉[開始ポート番号 [終了ポート番号]] interface [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【スタティック変換】

ip nat inside source static 〈変換前のアドレス〉〈変換後のアドレス〉

【NAT スタティック（一括変換）】

ip nat inside source static-subnet 〈変換前のネットワークアドレス〉〈変換後のネットワークアドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
[変換前開始ポート番号 変換前終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
interface	インタフェースのアドレスに NAT+変換します。	interface	NAT+の場合は省略不可
overload	ポート変換する場合に指定	overload	ポート変換しない
[変換後開始ポート番号 変換後終了ポート番号]	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host	IPv4 アドレス形式	省略不可

	部に 1 を指定しないでください。		
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 512 エントリ、リスト 128 エントリ

この設定を行わない場合

アドレス変換は行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
トンネルインタフェース設定モード

ip nat inside destination

そのインタフェースで受信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　158.xxx.xxx.2 宛で受信したら 192.168.0.1 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1
```

【解説】

ip nat inside destination static <変換前の宛先アドレス> 変換後の宛先アドレス>となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside destination static
158.202.232.1 1500 192.168.0.1 80
```

【解説】

ip nat inside destination static <変換前の送信元アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat inside destination static-subnet
158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】

ip nat inside destination static-subnet <変換前のネットワークアドレス> <変換後のネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat inside destination list 〈access-list 番号〉［開始ポート番号［終了ポート番号］］pool 〈プール名〉［ポート番号］

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat inside destination static 〈変換前のアドレス〉［開始ポート番号［終了ポート番号］］〈変換後のアドレス〉［ポート番号］

【NAT スタティック（一括変換）】
ip nat inside destination static-subnet 〈変換前のネットワークアドレス〉〈変換後のネットワークアドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
[開始ポート番号 終了ポート番号]	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ数:スタティック 512 エントリ、リスト 64 エントリ

この設定を行わない場合

アドレス変換は行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
トンネルインタフェース設定モード

ip nat outside source

そのインターフェースで受信するパケットの送信元アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source list 1 pool pool1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
                                                ↑list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7
                                                ↑pool1 の部分の設定
```

【解説】

ip nat outside source <変換前の送信元アドレス範囲> <変換後の送信元アドレス範囲>となります。
<変換前の送信元アドレス範囲>は、access-list コマンドで指定します。
<変換後の送信元アドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.1：～80　→　192.168.0.1：8080）

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#ip nat outside source static
192.168.0.1 80 192.168.100.1 8080
```

【解説】

ip nat outside source static <変換前の送信元アドレス　ポート番号> <変換後の送信元アドレス　ポート番号>となります。

設定例３　NAT 変換（スタティック登録）　設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static
192.168.0.1 158.xxx.xxx.2
Router(config-if lan 1)#ip nat outside source list 1 pool pool1
Router(config-if lan 1)#ip nat outside destination static
158.xxx.xxx.2 192.168.0.1

Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list
1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ←
pool1 の部分の設定
```

【解説】

設定例1とほぼ同じです。

違う点は、ip nat outside source static で、NAT スタティック変換をしている箇所ですが、この場合も、

ip nat inside source <変換前の送信元アドレス> <変換後の送信元アドレス>

となります。

この場合、ip nat outside destination コマンドを使用して、グローバル側→ローカル側のスタティック登録を行なう必要があります。(①の部分)

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside source static-subnet
192.168.100.0 158.xxx.xxx.0 255.255.255.0
```

【解説】

ip nat outside source static-subnet <変換前の送信元ネットワークアドレス> <変換後の送信元ネットワークアドレス> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】

ip nat outside source list 〈access-list 番号〉 pool 〈プール名〉

【NAT+時】

ip nat outside source list 〈access-list 番号〉［変換前開始ポート番号［変換前終了ポート番号］］ pool 〈プール名〉［変換後ポート番号］

【スタティック変換】

ip nat outside source static 〈変換前のアドレス〉［変換前開始ポート番号［変換前終了ポート番号］］〈変換前のアドレス〉［変換後ポート番号］

【NAT スタティック（一括変換）】

ip nat outside source static-subnet 〈変換前のネットワークアドレス〉〈変換後のネットワークアドレスト〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
変換前開始ポート番号 変換前終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
変換後開始ポート番号 変換後終了ポート番号	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
変換前のアドレス	変換前の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換後のアドレス	変換後の送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
変換前のネットワークアドレス	変換前の送信元アドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の送信元アドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 512 エントリ、リスト 64 エントリ

この設定を行わない場合

アドレス変換は行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
トンネルインタフェース設定モード

ip nat outside destination

そのインターフェースで受信するパケットの宛先アドレスの変換ルールを設定します。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）　192.168.0.1 宛で受信したら 158.xxx.xxx.2 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static
192.168.0.1 158.xxx.xxx.2
```

【解説】

ip nat outside destination static <変換前の宛先アドレス> <変換後の宛先アドレス>
となります。

設定例２　NAT+変換（スタティック登録）　158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#access-list 1 permit 158.xxx.xxx..2
Router(config)#ip nat pool pl-1 192.168.0.1 192.168.0.1
Router(config)#
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination list 1 1500
pool pl-1 80
```

【解説】

ip nat outside destination static <変換前の宛先アドレス　ポート番号> <変換後の宛先アドレス　ポート番号>
となります。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat outside destination static-subnet
158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】

ip nat outside destination static-subnet 〈変換前のネットワークアドレス〉〈変換後のネットワークアドレス〉〈サブネットマスク〉となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0
192.168.100.1 ⇔ 158.xxx.xxx.1
：：
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】

ip nat outside destination list 〈access-list 番号〉[変換前開始ポート番号 [変換前終了ポート番号]] pool 〈プール名〉[変換後ポート番号]

【NAT スタティック（1 対 1 変換）、NAT+スタティック時】

ip nat outside destination static 〈変換前のアドレス〉〈変換後のアドレス〉

【NAT スタティック（一括変換）】

ip nat outside destination static-subnet 〈変換前のネットワークアドレス〉〈変換後のネットワークアドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前のアドレス範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
変換前のアドレス	変換前の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
開始ポート番号 終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後のアドレス範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
変換後のアドレス	変換後の宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない

変換前のネットワークアドレス	変換前の宛先ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
変換後のネットワークアドレス	変換後の宛先ネットワークアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 512 エントリ、リスト 128 エントリ

この設定を行わない場合

アドレス変換は行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）
トンネルインタフェース設定モード

ip nat pool

NAT 変換する際の、変換後の IP アドレス範囲を指定します。NAT 変換(NAT+ではない)する場合に指定する必要があります。
このコマンドでは、プール名称・変換後の IP アドレス範囲(Start/End)を指定し、実際に NAT 変換するインタフェースで、使用するプール名を指定します。

ここで指定する範囲と、実際に NAT 変換するインタフェースの IP アドレスが重複している場合は、NAT 変換できません。

refresh コマンド後に有効になるコマンドです。

設定例　変換後のアドレスとして、158.xxx.xxx.2～158.xxx.xxx.7 を指定する（プール名：pool1）

```
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7
```

コマンド書式

ip nat pool〈プール名〉〈変換後のアドレス：先頭〉〈変換後のアドレス：最後〉

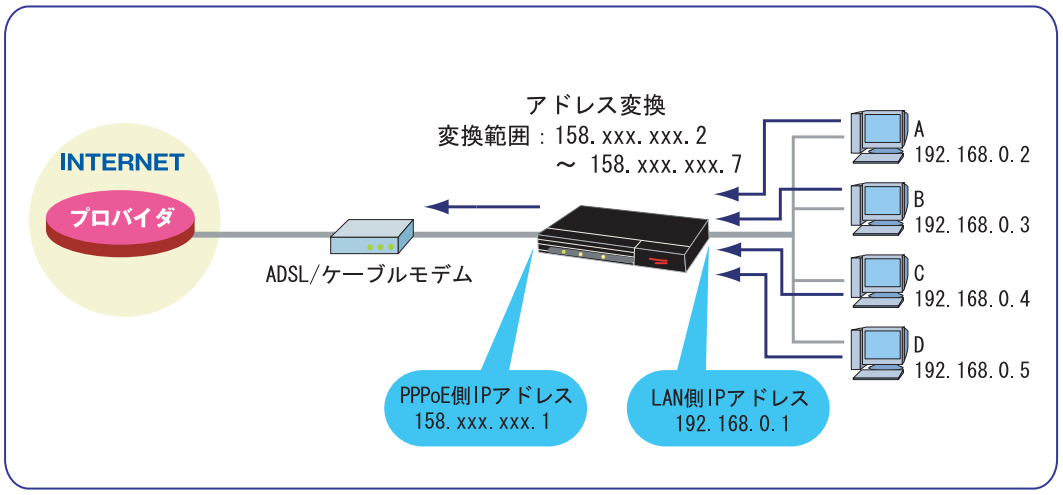
パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プール名	プールの名称を指定します。 PPPoE インタフェース設定モード/EWAN インタフェース設定モードで、NAT のコマンドを設定する場合に指定するプール名として使用しますので、わかりやすい名称にしてください。	16 文字以内の文字列	省略不可
変換後のアドレス:先頭	NAT 変換における、変換後のアドレスを範囲指定する場合の先頭アドレス	IPv4 アドレス形式	省略不可
変換後のアドレス:最後	NAT 変換における、変換後のアドレスを範囲指定する場合の最後のアドレス	IPv4 アドレス形式	省略不可

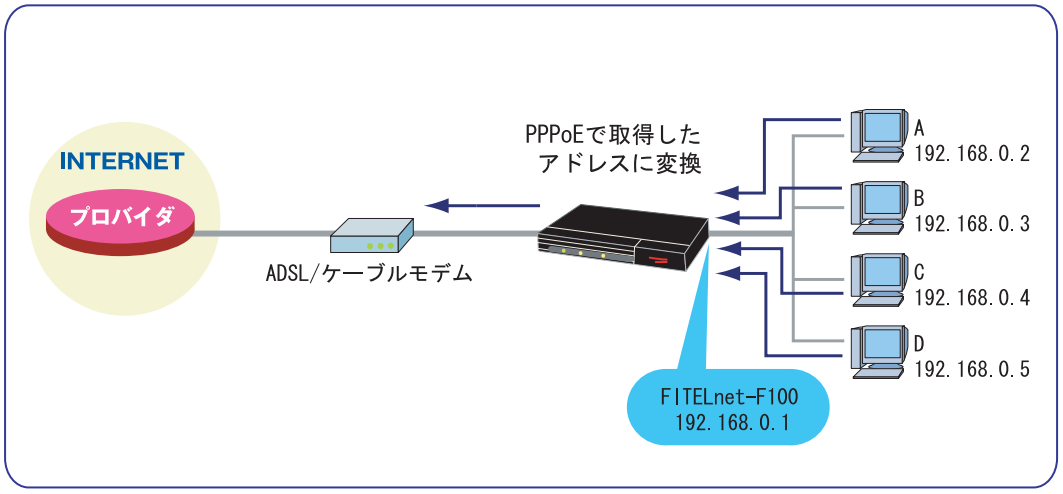
最大エントリ:8 エントリ

NAT 機能とは・・・

LAN 側にローカルアドレスを割り当てている場合、そのままのアドレスでは公共のネットワーク(インターネット等)に接続することはできません。
このような場合に、ローカルアドレスをグローバルアドレスに変換して、インターネットに接続できるようにする機能が NAT(Network Address Translation)です。
FITELnet-F シリーズでは、複数のアドレスに変換する機能を NAT 機能、1つのアドレスに集約する機能を NAT+機能と呼んでいます。
以下にイメージ図を示します。図は PPPoE を使用する例となっていますが、EWAN でも同様です。



NAT 機能



NAT+機能

他のコマンドとの連携

NAT 機能を使用するインタフェースで、NAT 機能の設定（ip nat inside コマンド）を行なう必要があります。

その際、NAT 変換後のアドレスとして、ip nat pool コマンドで指定したプール名を指定します。

設定モード

基本設定モード

DHCPサーバ機能

DHCPサーバ機能

service dhcp-server

DHCP サーバ機能を利用する場合に指定します。

設定例１　DHCP サーバ機能を使用する

```
Router(config)# service dhcp-server
```

コマンド書式

service dhcp-server

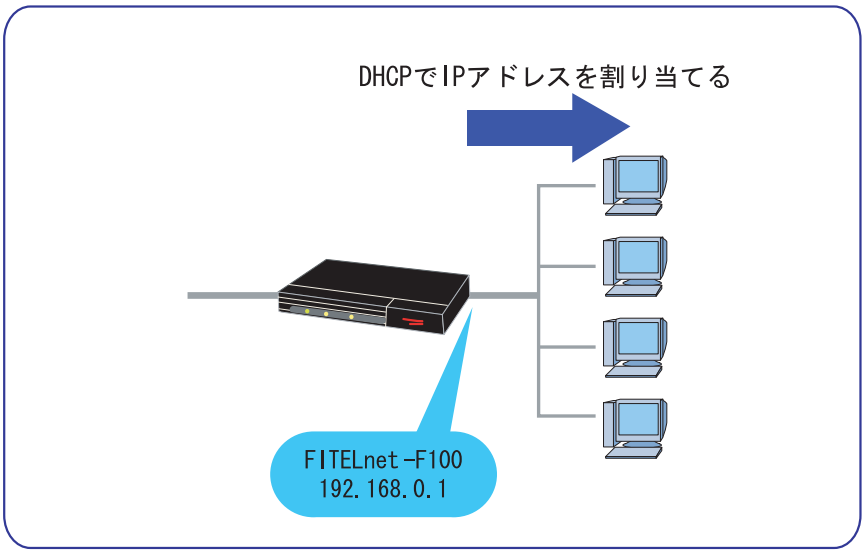
パラメータ

パラメータはありません。

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？



DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
FITELnet-F シリーズの DHCP サーバ機能では、以下の情報を通知することができます。

・IP アドレス／サブネットマスク
・DNS サーバの IP アドレス
・デフォルトゲートウェイの IP アドレス
・ドメイン名

FITELnet-F シリーズでは、DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

ip dhcp pool

DHCP サーバ設定モードに移行します。
FITELnet-F シリーズの LAN/EWAN2 インタフェースで、FITELnet-F シリーズを DHCP サーバとして使用する場合には設定が必要です。

DHCP サーバ機能と、DHCP リレーエージェント機能は共存できません。両方の設定がされている場合は、DHCP リレーエージェント機能が採用されます。

設定例　LAN インタフェースで DHCP サーバ機能を使用するために、DHCP サーバ設定モードに移行する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#
```

コマンド書式

ip dhcp pool 〈インタフェース名〉

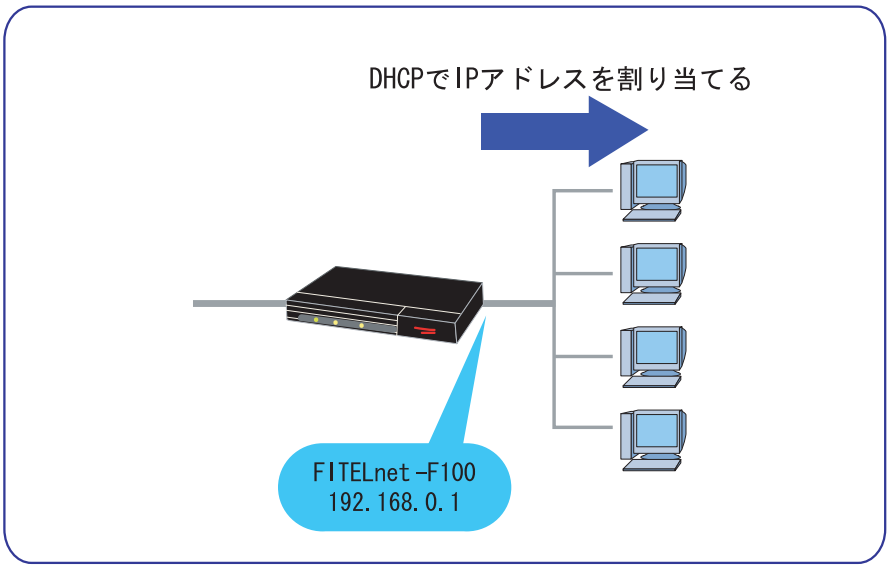
パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	DHCP サーバ機能を使用するインタフェースを lan1 または ewan2 から選択します。	lan1 ewan2	省略不可

この設定を行わない場合

DHCP サーバ機能を使用できません。

DHCP サーバ機能とは？



DHCP サーバ機能とは、DHCP(Dynamic Host Configuration Protocol)を使用して、LAN 上の端末(PC)に IP アドレスなどの情報を割り当てる機能です。
FITELnet-F シリーズの DHCP サーバ機能では、以下の情報を通知することができます。

・IP アドレス／サブネットマスク
・DNS サーバの IP アドレス
・デフォルトゲートウェイの IP アドレス
・ドメイン名

FITELnet-F シリーズでは、DHCP リレーエージェント機能もサポートしています。DHCP リレーエージェント機能は、自身がサーバになるのではなく、外部の DHCP サーバに問い合わせしなおす機能です。双方の設定がされている場合、DHCP リレーエージェント機能が有効になります。

設定モード

基本設定モード

domain-name

ドメイン名を設定します。

設定例１　DHCP で配布するドメイン名に"abc.com"を指定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#domain-name abc.com
```

コマンド書式

domain-name〈ドメイン名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DHCP で通知するドメイン名称	39 文字以内の文字列	省略不可

この設定を行わない場合

DHCP でドメイン名を通知しません。

設定モード

DHCP サーバ設定モード

dns-server

DNS サーバの IP アドレスを設定します。最大2件まで設定でき、DHCP で広告します。

設定例１　プライマリ DNS サーバに 192.168.1.100、セカンダリ DNS サーバに 192.168.1.101 を設定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#dns-server 192.168.1.100 192.168.1.101
```

コマンド書式

dns-server〈プライマリ DNS アドレス〉〈セカンダリ DNS アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ DNS アドレス	DHCP で通知するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式	省略不可
セカンダリ DNS アドレス	DHCP で通知するセカンダリ DNS サーバの IP アドレス	IPv4 アドレス形式	セカンダリ DNS を使用しない

この設定を行わない場合

DHCP で DNS サーバの情報を通知しません。

DNS サーバとは？

DNS は Domain Name System の略で、ホスト名から IP アドレス(またはその逆)を探し出すシステムのことです。
このシステムのために、ホスト名と IP アドレスの組み合わせデータベースが存在し、そのデータベースをもつホストのことを、DNS サーバといいます。

DNS サーバは、世界中のホストと IP アドレスの組み合わせデータベースを持っているわけではなく、自分の属するドメインの組み合わせのみを保有し、わからないホスト名のリクエストを受けた場合は、他の DNS サーバに問い合わせるという仕組みを持っています。

設定モード

DHCP サーバ設定モード

netbios-name-server

NetBIOS サーバの IP アドレスを設定します。最大2件まで設定でき、DHCP で広告します。

設定例１　プライマリ NetBIOS サーバに 192.168.1.200、セカンダリ NetBIOS サーバに 192.168.1.201 を設定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#netbios-name-server 10.1.1.2 10.1.1.3
```

コマンド書式

netbios-name-server〈プライマリ NetBIOS サーバアドレス〉〈セカンダリ NetBIOS サーバアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ NetBIOS サーバアドレス	DHCP で通知するプライマリ NetBIOS サーバの IP アドレス	IPv4 アドレス形式	省略不可
セカンダリ NetBIOS サーバアドレス	DHCP で通知するセカンダリ NetBIOS サーバの IP アドレス	IPv4 アドレス形式	セカンダリ NetBIOS サーバを使用しない

この設定を行わない場合

DHCP で NetBIOS サーバを通知しません。

設定モード

DHCP サーバ設定モード

default-router

デフォルトゲートウェイの IP アドレスを設定します。
但し、0.0.0.0 を設定した場合は、LAN の IP アドレスをデフォルトルータとして広告します。

設定例１　デフォルトゲートウェイの IP アドレスに 10.0.0.1 を広告する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#default-router 10.0.0.1
```

コマンド書式

default-router 〈IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で通知するデフォルトゲートウェイの IP アドレス	IPv4 アドレス形式	省略不可

この設定を行わない場合

DHCP でデフォルトゲートウェイの情報を通知しません。

デフォルトゲートウェイとは？

ルーティングテーブルにない宛先のパケットを送信する場合に、中継先としてパケットを送信するノードを、デフォルトゲートウェイといいます。
通常、パソコンはルーティングテーブルを持っていませんので、異なるサブネット宛の全てのパケットを、デフォルトゲートウェイに送ります。

言い方を替えると、デフォルトゲートウェイが設定されていないパソコンは、(ほとんど)ネットワーク機能を利用できないことになります。

設定モード

DHCP サーバ設定モード

option

本設定により、任意の DHCP 標準オプションの送信を行うことができます。
hex の後に 16 進数で任意の文字列を指定することができます。

設定例　X Window システムの Display Manager オプション（49）として、IP アドレス 192.168.1.1 を通知する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#option 49 hex c0a80101
```

コマンド書式

option 〈オプションコード〉 hex 〈オプション内容〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
オプションコード	送信するオプションコードを指定します。 4 エントリ以上指定した場合は、オプションコードの小さい順に 4 エントリが有効になります。	1～254	省略不可
オプション内容	送信する文字列を 16 進数で指定します。 全てのオプション値の合計長が 312 文字を超えた場合は、254 文字以内であっても超えたオプションは無効となります。	最大 254 文字の英数字	省略不可

この設定を行わない場合

任意のオプションは送信されません。

設定モード

DHCP サーバ設定モード

search-address

割り当て可能アドレスを立ち上がり時に調べる時の調査用の ARP に関する以下の項目を設定します。
通常の運用形態では、変更の必要はありません。

設定例１　ARP 送信回数（１回）、タイムアウト値（１秒）、アドレス検索パケット数（１６）に設定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#search-address 1 10 16
```

コマンド書式

search-address〈ARP 送信回数〉〈タイムアウト値〉〈アドレス検索パケット数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ARP 送信回数	ARP を送信する回数	1～255	省略不可
タイムアウト値	割り当て可能とするためのタイムアウト値（単位 100m 秒）	1～255	省略不可
アドレス検索パケット数	1 回の検索で送信する ARP パケット数	1～255	省略不可

この設定を行わない場合

以下で動作します。

タイマの内容	値
ARP を送信する回数	1
割り当て可能とするためのタイムアウト値（単位 100m 秒）	10
アドレス検索パケット数	16

設定モード

DHCP サーバ設定モード

allocate-address

割り当て開始アドレスの先頭値(DHCP アロケート開始アドレス)、割り当て可能な IP アドレスの個数(DHCP アロケート数)を設定します。
0.0.0.0 を指定した場合は、ホストアドレスの先頭から割り当てます。

設定例１　192.168.0.1 から 254 個分のアドレスを配布する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#allocate-address 192.168.0.1 254
```

コマンド書式

allocate-address〈IP アドレス〉〈アロケート数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で通知する IP アドレスの割り当て開始アドレス	IPv4 アドレス形式	省略不可
アロケート数	割り当て可能な IP アドレスの個数	1～255	255

この設定を行わない場合

先頭値:0.0.0.0、アロケート数:255 で動作します。

設定モード

DHCP サーバ設定モード

lease

配布する IP アドレスの有効期限を設定します。有効期限は「日」「時間」「分」もしくは「無限(infinite)」で指定します。
no 指定すると、設定を削除し、デフォルト設定値に戻します。

設定例１　リース期限を１日と１１時間２２分に設定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#lease 1 11 22
```

設定例２　リース期限を無限に設定する

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#lease infinite
```

コマンド書式

lease〈日〉〈時間〉〈分〉
　もしくは
lease infinite

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
日	DHCP で割り当てる期限(日)	0～365	省略不可
時間	DHCP で割り当てる期限(時間)	0～23	0(ただし分を設定する場合は省略不可)
分	DHCP で割り当てる期限(分)	0～59	0

パラメータ	設定内容	設定範囲	省略時の値
Infinite	DHCP で割り当てる期限を無限とする	infinite	省略不可

この設定を行わない場合

infinite となります。

設定モード

DHCP サーバ設定モード

hosttable

DHCP サーバ機能で配布する IP アドレスを端末に対して固定値を割り付けるために、端末の MAC アドレスと配布する IP アドレスの組み合わせを登録します。

設定例１　MAC アドレス 00:80:bd:f0:01:23 のホストには、10.0.0.1 を割り当てる

```
Router(config)#ip dhcp pool lan1
Router(config-dhcp-pool)#hosttable 10.0.0.1 0080.bdf0.0123
```

コマンド書式

hosttable〈IP アドレス〉〈MAC アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	DHCP で割り当てる IP アドレス	IPv4 アドレス形式	省略不可
MAC アドレス	DHCP で割り当てるホストの MAC アドレス	MAC アドレス形式	省略不可

この設定を行わない場合

固定的に IP アドレスを割り当てることはできません。

有効エントリ数

16 エントリ

設定モード

DHCP サーバ設定モード

DHCPリレーエージェント機能

DHCPリレーエージェント機能

service dhcp-relayagent

DHCP リレーエージェント機能を利用する場合に指定します。
DHCP リレーエージェント機能を使用する場合、DHCP パケットをリレーするインタフェース(DHCP サーバへの中継方向)で NAT 機能を使用することは出来ません。

設定例 1

```
Router(config)# service dhcp-relayagent
```

コマンド書式

```
service dhcp-relayagent
```

パラメータ

パラメータはありません。

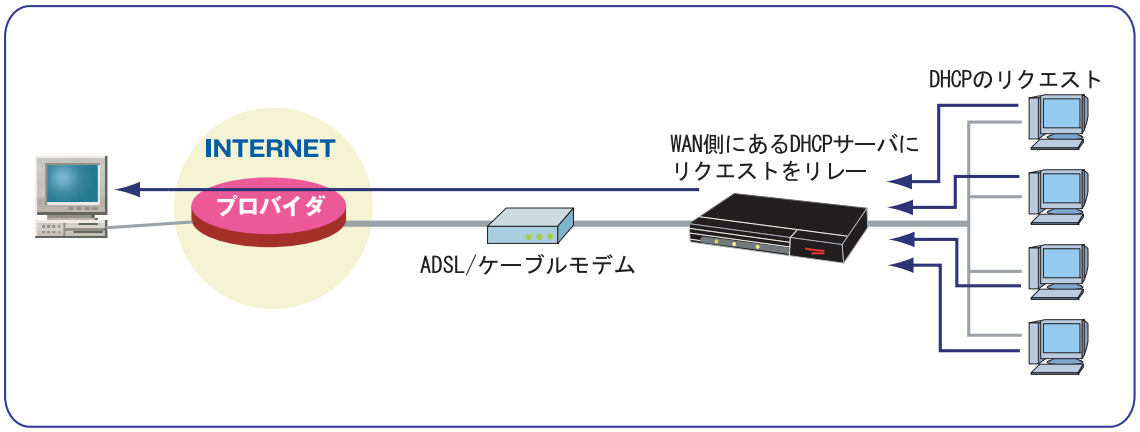
この設定を行わない場合

DHCP リレーエージェント機能を使用できません。

DHCP リレーエージェント機能とは

LAN 上の DHCP クライアントからの要求を、WAN 側にリレーし、WAN 側の DHCP サーバから割り当ててもらう機能です。

本社側で、支店の LAN 側の IP アドレスを一括で管理する場合に有効な機能です。



設定モード

基本設定モード

ip dhcp relay maxhops

DHCP リレーエージェント機能を使用する場合に、何段先までのサーバまでアクセスを許可するかを指定します。

設定例　DHCP サーバまでの許容段数を 10 とする

```
Router(config)#ip dhcp relay maxhops 10
```

コマンド書式

ip dhcp relay maxhops <HOP 数>

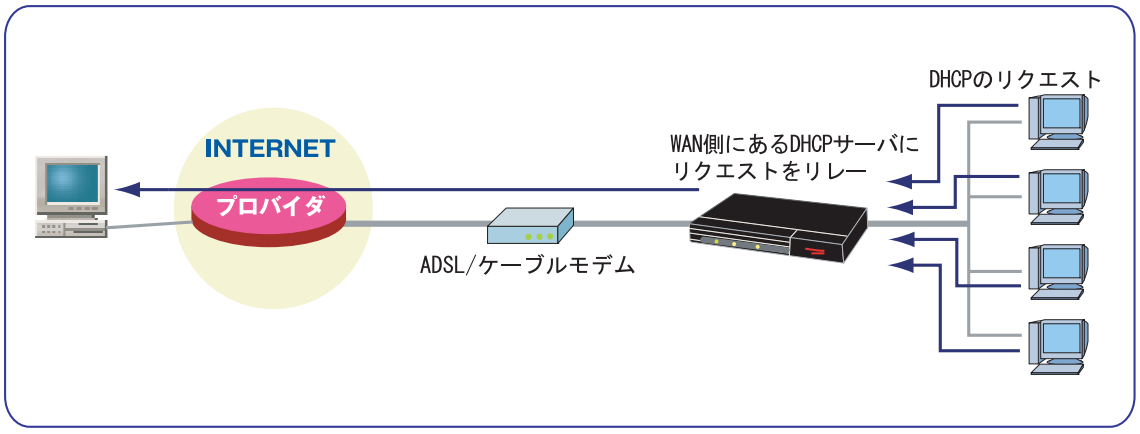
パラメータ

パラメータ	設定内容	設定範囲	省略時の値
HOP 数	何段先までのサーバまでアクセスを許可するか	1～16	省略不可

この設定を行わない場合

4 段が設定されます。

DHCP リレーエージェント機能とは？



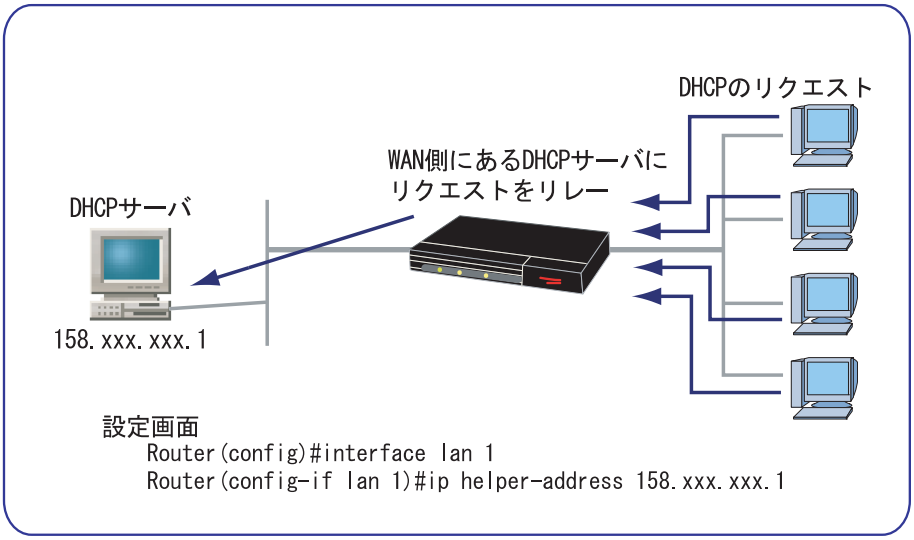
LAN 上の DHCP クライアントからの要求を、WAN 側にリレーし、WAN 側の DHCP サーバから割り当ててもらう機能です。
本社側で、支店の LAN 側の IP アドレスを一括で管理する場合に有効な機能です。

設定モード

基本設定モード

ip helper-address

FITELnet-F シリーズで、DHCP リレーエージェント機能を使用する際、リレー先の DHCP サーバを登録します。
FITELnet-F シリーズでは、最大4つまでの DHCP サーバを登録できます。



設定例１　DHCP リレーエージェント機能で問い合わせる DHCP サーバに 192.168.100.1 を設定する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip helper-address 192.168.100.1
```

コマンド書式

ip helper-address <DHCP サーバの IP アドレス> [source-interface <インタフェース名>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
DHCP サーバの IP アドレス	DHCP リレーエージェント機能でリレーする際の、リレー先 DHCP サーバの IP アドレスを指定します。	IPv4 アドレス形式	省略不可
インタフェース名	DHCP リレーする際の送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 pppoe※1 1～24 dialer※2 1～20 loopback 1 vlanif 1～16	実際に送信するインタフェース

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能

この設定を行わない場合

DHCP リレーエージェント機能を使用できません。

設定モード

LAN インタフェース設定モード
VLAN インタフェース設定モード

簡易DNS機能

簡易DNS機能の設定

proxydns mode

本装置の簡易 DNS 機能を使用するプロトコル(IPv4 or IPv6)を指定します。
双方を使用する場合は"both"を指定します。

設定例１　Ipv4、IPv6 パケットによるリクエストに対して簡易 DNS 機能を使用する

```
Router(config)# proxydns mode both
```

設定例２　IPv4 パケットによるリクエストに対して簡易 DNS 機能を使用する

```
Router(config)# proxydns mode v4
```

コマンド書式

proxydns mode〈プロトコル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロトコル	簡易 DNS 機能に対して問合せを行なう際に使用するプロトコルを指定します。 v4：IPv4 パケットによる name のリクエストに対して、代理要求/応答をする v6：IPv6 パケットによる name のリクエストに対して、代理要求/応答をする both：IPv4／IPv6 の両方のパケットでの name のリクエストに対して、代理要求/応答をする	v4 v6 both	省略不可

この設定を行わない場合

ProxyDNS 機能を使用できません。

設定モード

基本設定モード

proxydns default domain-name

proxyDNS 機能で、上流の DNS サーバに問い合わせる際につけるドメイン名を指定します。
LAN 側からの DNS のリクエスト(Query)にドメイン名がついていなかった場合、ここで設定したドメイン名をつけてサーバに問い合わせます。

設定例１　ドメイン名に furukawa.co.jp を設定する

```
Router(config)# proxydns default domain-name furukawa.co.jp
```

コマンド書式

proxydns default domain-name 〈ドメイン名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DNS のリクエストにドメイン名がついていなかった場合につけるドメイン名	-	省略不可

この設定を行わない場合

ProxyDNS 使用時に、ドメイン名を省略することはできません。

設定モード

基本設定モード

proxydns default name-server

ProxyDNS 機能を使用する場合の、DNS サーバの IP アドレスを指定します。
また、PPPoE／DHCP により、DNS アドレスを学習している場合であっても、本コマンドによる設定が優先されます。
IPv4 用の DNS サーバ／IPv6 用の DNS サーバを登録します。
アドレスを連続して入力する事により、プライマリ、セカンダリの順で DNS サーバを設定します。別のアドレスを入力すると以前入力したアドレスに上書きされます。セカンダリーのみ変更したい場合は、設定されているプライマリアドレスの後に続けて、新たにセカンダリアドレスを入力してください。

設定例１　IPｖ4 用の DNS サーバに、プライマリ：192.168.200.1／セカンダリ：192.168.200.10 を設定する

```
Router(config)# proxydns default name-server v4 192.168.200.1
192.168.200.10
```

設定例２　IPv6 用の DNS サーバに、プライマリ：2003:113::1／セカンダリ：2003:113::2 を設定する

```
Router(config)# proxydns default name-server v6 2003:113::1
2003:113::2
```

コマンド書式

proxydns default name-server {v4|v6}<プライマリ DNS アドレス>[セカンダリ DNS アドレス]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
v4|v6	DNS サーバを指定するプロトコルを選択します。 IPv4 アドレスで DNS サーバを指定する場合には v4 を使用し、IPv6 アドレスで DNS サーバを指定する場合には v6 を使用します。	v4 v6	省略不可
プライマリ DNS アドレス	Proxy DNS で使用するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ DNS アドレス	Proxy DNS で使用するセカンダリ DNS サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ DNS を使用しない

この設定を行わない場合

ProxyDNS 機能を使用できません。ただし、PPPoE や DHCP クライアント機能で、DNS の IP アドレスを学習している場合は、ProxyDNS 機能を使用できます。

設定モード

基本設定モード

proxydns default retrans-time

問い合わせパケットを中継し、それに対する応答待ち時間を設定します。
応答待ち時間経過しても応答がない場合は、再送します。

設定例１　ProxyDNS の応答待ち時間を 5 秒に設定する

```
Router(config)# proxydns default retrans-time 5
```

コマンド書式

proxydns default retrans-time 〈応答待ち時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
応答待ち時間	DNS サーバからの応答待ち時間(単位:秒)を指定します。	1～10	省略不可

この設定を行わない場合

3 秒となります。

設定モード

基本設定モード

proxydns default retry

応答パケットタイムアウトに対する再送回数を設定します。

設定例１　ProxyDNS 機能の再送を 3 回とする

```
Router(config)# proxydns default retry 3
```

コマンド書式

proxydns default retry 〈リトライ回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	DNS サーバからの応答がない場合のリトライ回数	0～10	省略不可

この設定を行わない場合

2 回となります。

設定モード

基本設定モード

proxydns default cache-time

LAN 側の端末から DNS のリクエストを受信し、proxyDNS 機能により解決した情報について、内部のテーブルに保持しておく時間を設定します。
学習した DNS 情報について、ここで指定した時間リクエストを受信しなかった場合は、該当 DNS 情報を削除します。

設定例１　PxoxyDNS のテーブルの保持時間を 60 分に設定する

```
Router(config)# proxydns default cache-time 3600
```

コマンド書式

proxydns default cache-time 〈キャッシュ時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ時間	ProxyDNS のテーブル保持時間(秒)を設定します。off を指定すると保持しません。	0～259200 off	省略不可

※ timeout 時間に、0 秒を指定すると学習した DNS 情報を保持し続けます。
　off を指定した場合は、必ず DNS サーバに問い合わせを行ないます。

この設定を行わない場合

86400 秒となります。

設定モード

基本設定モード

proxydns default source-interface

ProxyDNS 機能により、上位の DNS サーバに名前解決のパケットを送出する際の、送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例１　送信元アドレスに LAN を指定する

```
Router(config)# proxydns default source-interface lan 1
```

コマンド書式

proxydns default source-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	送信元アドレスとして指定するインタフェース	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

基本設定モード

ドメイン名によるDNS振り分け

proxydns domain

ドメイン名称とそのドメイン名称に対応する DNS IP アドレスを登録します。
別のアドレスを入力すると以前入力したアドレスに上書きされます。

設定例１　furukawa.co.jp ドメイン宛の DNS リクエストは、192.168.200.1 もしくは 2003:113::c0a8:c801 に問い合わせる

```
Router(config)# proxydns domain furukawa.co.jp v4 192.168.200.1
Router(config)# proxydns domain furukawa.co.jp v6 2003:113::c0a8:c801
```

コマンド書式

proxydns domain〈ドメイン名〉{ v4 | v6 }〈DNS アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ドメイン名	DNS リクエストのドメイン名	-	省略不可
v4 | v6	DNS サーバを指定するプロトコルを選択します。 IPv4 アドレスで DNS サーバを指定する場合には v4 を使用し、IPv6 アドレスで DNS サーバを指定する場合には v6 を使用します。	v4 v6	省略不可
DNS アドレス	DNS サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

最大エントリ数:8 エントリ

この設定を行わない場合

どのようなリクエストでも、全て固定の DNS サーバに問い合わせます。

設定モード

基本設定モード

ホスト名称とDNS IPアドレスの登録

proxydns hosts

ホスト名称と IP アドレスの組み合わせを登録することができます。本装置に DNS 要求が来た場合、このリストを参照して応答します。

設定例１　host.furukawa.co.jp の IPv4 アドレスを 192.168.100.1／IPv6 アドレスを 2003:113::c0a8:6401 に設定する

```
Router(config)# proxydns hosts host.furukawa.co.jp v4 192.168.100.1
Router(config)# proxydns hosts host.furukawa.co.jp v6 2003:113::c0a8:6401
```

コマンド書式

proxydns hosts〈ホスト名〉{ v4 | v6 }〈IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ホスト名	IP アドレスと組み合わせるホスト名を指定	-	省略不可
v4 | v6	DNS サーバの属性(IPv4 用(A レコード) or IPv6 用(AAAA レコード))を指定	v4 v6	省略不可
IP アドレス	DNS のリプライとして送信する IP アドレス(IPv4 アドレスまたは IPv6 アドレス)	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

最大エントリ数:16 エントリ(キャッシュテーブルの最大数は 64 エントリ)

この設定を行わない場合

ホスト名称とアドレスの組み合わせを持たず、全て DNS システムを使用します。

設定モード

基本設定モード

ダイナミックDNS機能

サーバ機能

ddns-server accept-fqdn type【F100/F1000 コマンド】

ダイナミック DNS サーバ機能を使用時に、受け入れを許可するレコードの内容(FQDN、アドレス種別)と、アクセスパスワード、レコードのライフタイムを設定します。
ここで指定したレコードと異なるダイナミック DNS 要求を受信しても本装置の DNS データベースには反映されません。

なお、ダイナミック DNS サーバ機能を利用する場合には、かならず HTTP サーバ機能および簡易 DNS サーバ機能を動作させるようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例 1　FQDN（host1.furukawa.co.jp）、受付アドレス種別：IPv4、アクセスパスワード"pass1"、有効時間を 300 秒とする

```
Router(config)#ddns-server accept-fqdn type v4
host1.furukawa.co.jp password pass1 lifetime 300
Router(config)#
```

コマンド書式

ddns-server accept-fqdn type {v4|v6} 〈FQDN〉 password 〈パスワード〉 lifetime 〈有効時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
v4|v6	指定する FQDN に対応するアドレスの IP バージョンを指定します。 v4　IPv4 アドレスで指定 v6　IPv6 アドレスで指定	v4 v6	省略不可
FQDN	登録要求を受け付ける FQDN を設定します。	64 文字までの英数字	省略不可
パスワード	アクセスパスワードを設定します。	32 文字までの英数字	省略不可
有効時間	有効時間を設定します。単位:秒	1～86400	省略不可

最大エントリ数:100 エントリ

この設定を行わない場合

ダイナミック DNS サーバ機能は使用できません。

FQDN とは？

FQDN とは、ホスト名.ドメイン名の形式をいいます。

ダイナミック DNS サーバの動作

本装置のダイナミック DNS サーバは、HTTP の GET リクエストを受信し CGI でレコードを登録する動作となります。

CGI プログラム名は、"(V4) cgi-bin/ddns-v4.cgi, (V6) cgi-bin/ddns-v6.cgi"です。

レコードを登録するための CGI パラメータは以下となります。

内容	CGI パラメータ	登録例
FQDN	dn	dn=host1.furukawa.co.jp
IPv4 アドレス	i4	i4=192.168.0.1
IPv6 アドレス	i6	i6=aaaa:bbbb::1
パスワード	pw	pw=pass1

注意1：i4,i6 の両方が存在しない GET リクエストの場合は、HTTP の送信元アドレスを、アドレス情報として登録します。

注意2：i4,i6 の両方が存在する GET リクエストは、エラー(403)となります。

設定モード

基本設定モード

ddns-server enable【F100/F1000 コマンド】

ダイナミック DNS サーバ機能を使用する場合に設定します。
ダイナミック DNS サーバ機能を利用する場合には、かならず HTTP サーバ機能および簡易 DNS サーバ機能を動作させるようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイナミック DNS サーバ機能を有効にする

```
Router(config)#ddns-server enable
Router(config)#
```

コマンド書式

ddns-server enable

パラメータ

パラメータはありません。

この設定を行わない場合

ダイナミック DNS サーバ機能を使用できません。

設定モード

基本設定モード

ddns-server logging address-changes【F100/F1000 コマンド】

ダイナミック DNS サーバ機能を利用時、同じ FQDN に対して、アドレスの変更があったことをログ(slog)に出力する場合に、本コマンドを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　登録アドレス変更ログを出力する

```
Router(config)#ddns-server logging address-changes
Router(config)#
```

コマンド書式

ddns-server logging address-change s

パラメータ

パラメータはありません。

この設定を行わない場合

登録アドレス変更ログを出力しません。

設定モード

基本設定モード

クライアント機能(ダイナミックDNS動作の設定)

ddns-client

ダイナミック DNS クライアントが、登録要求メッセージを送信するイベントと送信内容の設定を行います。
設定 I/F モードの IPv4/IPv6 アドレスの変化、Link 状態変化毎に実行する http-client 設定を選択します。
また、I/F アドレス状態変化の判断に一定の間隔を設ける遅延処理の設定及び、一定期間イベントが発生しない場合の定期送信を行うこともできます。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースのアドレス状態変化時に、http-client モード１に登録したメッセージを送信

```
Router(config)#interface lan 1
Router(config-if lan 1)#ddns-client address ip action http-client 1
```

コマンド書式

ddns-client　{ address { ip | ipv6 }} action http-client <http-client モード>
[delay <遅延処理設定>] [interval <定期送信間隔>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
address { ip | ipv6 }	登録要求メッセージを設定 I/F のアドレス変化、または Link 状態の変化のどちらで送信するかを指定します。 IPv4 アドレス変化時に送信する場合：address ip IPv6 アドレス変化時に送信する場合：address ipv6	address ip address ipv6	省略不可
http-client モード	送信する登録要求メッセージを選択します	1～16	省略不可
遅延処理設定	I/F アドレス状態変化の判断に一定の間隔を設ける場合に指定します。単位:秒	0～60	5 秒
定期処理間隔	一定期間、I/F アドレス状態変化が起きない場合に定期送信する場合に指定します。単位:秒	10～86400	定期送信を行いません。

この設定を行わない場合

I/F アドレスの状態変化時にメッセージを送信しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)

クライアント機能(HTTPクライアントに関する設定)

description

http-client の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　http-client の Description を HTTP-CLIENT1 とする

```
Router(config)#http-client 1
Router(http-client 1)#description HTTP-CLIENT1
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	http-client の Description を設定します。	半角英数字、記号※1	省略不可

※1:連続 254 文字まで、スペースで区切ることにより 2033 文字まで入力可能です。
ただし、show コマンド(コンフィグの表示を除く※2)で表示される文字数は、最初の 254 文字までとなります。
※2:コンフィグの表示では、2033 文字まで表示されます。

この設定を行わない場合

http-client の Description を設定しません。

設定モード

HTTP クライアント設定モード

logging

HTTP クライアントの動作において、出力するログの種別を、以下のなかから選択します。
・ログを出力しない
・エラー時のみログを出力する
・エラー時だけでなく、成功時にもログを出力する

refresh コマンド後に有効になるコマンドです。

設定例１　全てのログを出力する

```
Router(config)#http-client 1
Router(http-client 1)#logging detailed
```

コマンド書式

logging〈ログ出力レベル〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ出力レベル	ログ出力レベルを設定し出力ログを選択します。 detailed　全てのログを出力 error　エラーログのみ出力 none　ログを出力しません	detailed error none	省略不可

この設定を行わない場合

エラーログのみ出力します。

設定モード

HTTP クライアント設定モード

method

HTTP の Request-Line を指定します。HTTP の Request-Line は、以下の書式となります。
メソッド Request-URI HTTP バージョン
本装置の HTTP クライアントでは、メソッドは GET のみ指定可となります。Request-URI は、URL と CGI オプションの指定となります。
HTTP バージョンは 1.0 固定となります。

Request-URI の指定方法は、以下のとおりです。
F100 または、F1000 のダイナミック DNS サーバ宛に送信する場合は、IPv4 アドレスであれば ddns-v4.cgi、IPv6 アドレスであれば ddns-v6.cgi を指定してください。
Request-URL <CGI オプション 1> <CGI オプション値 1> <CGI オプション 2> <CGI オプション値 2> ・・・
たとえば、http://192.168.0.1/cgi-bin/ddns-v4.cgi に、dn=abc.co.jp, pw=pass1 を送りたい場合は、以下のような指定になります。
http://192.168.0.1/cgi-bin/ddns-v4.cgi dn abc.co.jp pw pass1

refresh コマンド後に有効になるコマンドです。

設定例 1　http://192.168.0.1/cgi-bin/ddns-v4.cgi に、i4=192.168.200.1 dn=abc.co.jp, pw=pass1 を送る

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.0.1/cgi-
bin/ddns-v4.cgi dn abc.co.jp i4 $i4 pw pass1
```

コマンド書式

method <番号> get url <登録要求先> [<CGI オプション> <CGI オプション値> ・・・]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
番号	シーケンス番号	1～16	省略不可
登録要求先	DDNS サーバの URL を半角で指定します。	1～254	省略不可
<CGI オプション> <CGI オプション値>	CGI オプションとその値をスペースで区切って指定します。 この組み合わせは複数指定することができます。	-	引数名、引数を指定しません。

不定アドレスの登録方法

通知したいアドレスが PPPoE のような不定アドレスのケースでは、アドレス情報としてマクロ登録を行います。
F100 でサポートしているマクロ登録は、以下の 2 つです。
$i6・・IPv6 アドレス
$i4・・IPv4 アドレス
たとえば、不定の IPv6 アドレスをダイナミック DNS 機能を利用して通知したい場合は、以下のように設定します。

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.1.1/cgi-
bin/ddns-v4.cgi dn abc.co.jp pw pass1 i6 $i6
```

どのインタフェースのアドレスを通知するかは、reference-interface コマンドで設定します。

F100 でダイナミック DNS サーバを行っている場合の登録

192.168.100.1 のアドレスを持つ F100 でダイナミック DNS サーバを動作させている場合は、以下の設定を行うことで、登録要求を行うことができます。

```
Router(config)#http-client 1
Router(http-client 1)#method 1 get url http://192.168.100.1/cgi-
bin/ddns-v4.cgi i4 10.1.1.1 pw pass1 dn F100.domain.co.jp
```

この設定を行わない場合

ダイナミック DNS サーバへ登録要求メッセージを送信しません。

設定モード

HTTP クライアント設定モード

reference-interface

method コマンドで、不定アドレス登録のためにマクロ登録を行った場合に、どのインタフェースの状態を参照するのかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースを登録要求メッセージのアドレス（IPv4/IPv6）置換時に参照する

```
Router(config)#http-client 1
Router(http-client 1)#reference-interface lan 1
```

コマンド書式

reference-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	登録要求メッセージのアドレス(IPv4/IPv6)置換時に参照するインターフェース名を指定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20※	省略不可

※:F100 のみ指定可能です。

この設定を行わない場合

インタフェースのアドレスを参照しません。

設定モード

HTTP クライアント設定モード

request-timeout

ダイナミック DNS サーバに対して送信した登録要求メッセージの応答受信待ち許容時間、およびリトライ回数を指定します。
ここで指定した時間応答を受信しなかった場合はリトライを行います。

refresh コマンド後に有効になるコマンドです。

設定例１　登録要求メッセージの応答受信待ちタイムアウト 10 秒、リトライ回数 2 回にに設定

```
Router(config)#http-client 1
Router(http-client 1)#request-timeout 10 retry 2
```

コマンド書式

request-timeout〈登録要求タイムアウト〉[retry〈リトライ回数〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
登録要求タイムアウト	ダイナミック DNS サーバに対して送信した登録要求メッセージの応答受信待ちタイムアウト時間を指定します。単位:秒	1～60	省略不可
リトライ回数	ダイナミック DNS サーバに対して送信した登録要求メッセージのリトライ回数を指定します。	0～5	リトライしません。

この設定を行わない場合

登録要求タイムアウト 10 秒、リトライしないに設定されます。

設定モード

HTTP クライアント設定モード

source-interface

登録要求メッセージの送信元アドレスをインターフェース名で設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースを登録要求メッセージの送信元アドレスとする

```
Router(config)#http-client 1
Router(http-client 1)#reference-interface lan 1
```

コマンド書式

source-interface 〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	登録要求メッセージの送信元アドレスをインターフェース名で設定します。	lan 1 ewan 1～2 pppoe 1～24 dialer 1～20※ loopback 1 vlanif 1～16	省略不可

※:F100 のみ指定可能です。

この設定を行わない場合

source-interface 指定無しで動作します。

設定モード

HTTP クライアント設定モード

簡易ファイアウォール機能

外部からの接続制御機能

remote-access limitation

パスワードを指定回数以上間違えたときにはアクセス拒否する機能の、パスワード誤りを許可する回数を設定します。0 を指定すると不正アクセス抑制を行わなくなります。

設定例１　パスワード誤り許容回数を 2 回に設定する

```
Router(config)#remote-access limitation 2
```

コマンド書式

remote-access limitation 〈パスワード誤り許容回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パスワード誤り許容回数	不正アクセスではないとみなすパスワード誤り許容回数。 この設定上の誤りがあった場合は、不正アクセスとみなし、電子メール通知／ログ出力／アクセス拒否されます。	0～5	省略不可

この設定を行わない場合

3 回となります。
4 回以上パスワードを間違えると、10 分間アクセスが拒否します。

不正アクセスが発覚した場合

不正アクセスが発覚した場合は、以下の制御が行なわれます。

●電子メールによる通知

電子メールにより、管理者宛に、不正アクセスが起こったこと、不正アクセス元の IP アドレス等の情報を通知します。

電子メール通知機能の設定は mail コマンドを使用します。

●ログ出力

slog に『Security Emergency from xxx.xxx.xxx.xxx』(xxx.xxx.xxx.xxx は不正アクセスもとの IP アドレス)と表示します。

syslog の設定がされている場合は、遠隔地の syslog サーバにリアルタイムに通知することもできます。

●アクセス拒否

不正アクセス元からのアクセスを、一定時間アクセスを制限します。アクセス制限時間の設定は remote-access time コマンドで設定します。

設定モード

基本設定モード

remote-access time

パスワードを指定回数以上間違えたときにはアクセス拒否する機能の、アクセス制限時間を設定します。

設定例１　不正アクセス発生時のアクセス制限時間を 5 分に設定する

```
Router(config)#remote-access time 5
```

コマンド書式

remote-access time 〈アクセス制限時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクセス制限時間	不正アクセスの相手に対して、アクセス制限を行なう時間(分)を設定します。	1～60	省略不可

この設定を行わない場合

10 分となります。

不正アクセスが発覚した場合

不正アクセスが発覚した場合は、以下の制御が行なわれます。

●電子メールによる通知

電子メールにより、管理者宛に、不正アクセスが起こったこと、不正アクセス元の IP アドレス等の情報を通知します。

電子メール通知機能の設定は mail コマンドを使用します。

●ログ出力

slog に『Security Emergency from xxx.xxx.xxx.xxx』(xxx.xxx.xxx.xxx は不正アクセスもとの IP アドレス)と表示します。

syslog の設定がされている場合は、遠隔地の syslog サーバにリアルタイムに通知することもできます。

●アクセス拒否

不正アクセス元からのアクセスを、一定時間アクセスを制限します。パスワード誤りの許容回数は remote-access limitation コマンドで設定します。

設定モード

基本設定モード

フィルタリング機能

ipv6 access-group

access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、LAN 送信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 access-group 1 out
```

設定例２　access-list 2 で指定したデータを、LAN からの受信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ipv6 access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	<3000-3499> <3500-3999>	省略不可
in | out	インタフェースでの受信時(in)/インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

PPPoE インタフェース設定モード
LAN インタフェース設定モード
EWAN インタフェース設定モード
トンネルインタフェース設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースで適用します。
フィルタリングデータは、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースで受信したパケットに適用するのか、各(PPPoE、LAN、EWAN、ダイヤルアップ、IPsec)インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。(ダイヤルアップは除く)

設定例１　access-list 1 で指定したデータを、LAN 送信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、LAN からの受信時に適用する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn]| out }

パラメータ

<table>
<tr><th>パラメータ</th><th>設定内容</th><th>設定範囲</th><th>省略時の値</th></tr>
<tr><td>access-list 番号</td><td>フィルタリングのデータを設定したアクセスリストの番号を指定します。</td><td><1-99>
<100-199>
<1300-1999>
<2000-2699></td><td>省略不可</td></tr>
<tr><td>{ in[interface | vpn]| out }</td><td>インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。
受信時は、さらに以下のように設定ができます。
<table>
<tr><td>in</td><td>access-list に従い制御</td></tr>
<tr><td>in vpn</td><td>自局宛 VPN 対象パケットを制御</td></tr>
<tr><td>in interface</td><td>自局宛非 VPN 対象パケットを制御</td></tr>
</table></td><td>in
out</td><td>省略不可</td></tr>
</table>

※LAN インタフェースおよび IPsec インタフェースでは、vpn を選択することはできません。
※in vpn および in interface を選択した場合、適用する access-list の宛先は、any とする必要があります。

この設定を行わない場合

該当インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
IPsec インタフェース設定モード
VLAN インタフェース設定モード
トンネルインタフェース設定モード

ip stateful max-sessions

学習フィルタリングテーブルの総数を設定します。
ここで設定する総数は、IPv4/IPv6 で使用する学習フィルタリングテーブルの総数となります。

設定例　学習フィルタリングテーブルを 16384 セッション分設定する

```
Router(config)#ip stateful max-sessions 16384
```

コマンド書式

ip stateful max-sessions 〈セッション数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
セッション数	学習フィルタリングテーブルの最大数を設定します。	2048～16384	省略不可

この設定を行わない場合

2048

設定モード

基本設定モード

サービス制限機能

console exec-timeout

コンソールでログインされている状態で、無通信監視時間を設定します。コンソールでログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#console exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#console exec-timeout off
```

コマンド書式

console exec-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	コンソールでログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間(単位:分)を指定します。 off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

60 分で自動ログアウトするようになっています。

注意！

自動ログアウト／意図的なログアウトにかかわらず、コンソールで設定した内容は記録されています。
他のユーザが TELNET でログインして、save コマンドを入力し、再起動した時点で有効となってしまいます。

設定を途中で止め、元の状態に戻すには、load コマンドを利用してからログアウトしてください。

設定モード

基本設定モード

ftp-server exec-timeout

FTP でログインされている状態で、無通信監視時間を設定します。
FTP でログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#ftp-server exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#ftp-server exec-timeout off
```

コマンド書式

ftp-server exec-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	FTP でログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間（単位：分） off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

5 分で自動ログアウトするようになっています。

設定モード

基本設定モード

ftp-server shutdown

FTP によるアクセスを拒否する場合に指定します。

設定例１　FTP のアクセスを拒否する

```
Router(config)#ftp-server shutdown
```

コマンド書式

```
ftp-server shutdown
```

パラメータ

パラメータはありません。

この設定を行わない場合

FTP によるアクセスを受け付けます。

設定モード

基本設定モード

telnet-server exec-timeout

TELNET でログインされている状態で、無通信監視時間(単位:分)を設定します。TELNET でログインされ、このコマンドで設定した時間何もコマンドの入力がなかった場合は、自動でログアウトします。

設定例 1　タイムアウト時間を 30 分に設定する場合

```
Router(config)#telnet-server exec-timeout 30
```

設定例 2　自動ログアウトさせない場合

```
Router(config)#telnet-server exec-timeout off
```

コマンド書式

telnet-server exec-timeout <timeout 時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
timeout 時間	TELNET でログインされ、オペレーションが行われなくなってから自動ログアウトするまでの時間(単位:分) off を指定すると自動ログアウトしません。	1～60 off	省略不可

この設定を行わない場合

5 分で自動ログアウトするようになっています。

注意！

自動ログアウト／意図的なログアウトにかかわらず、TELNET で設定した内容は記録されています。
コンソールや、他のユーザが TELNET でログインして、save コマンドを入力し、再起動した時点で有効となってしまいます。
設定を途中で止め、元の状態に戻すには、load コマンドを利用してからログアウトしてください。

設定モード

基本設定モード

telnet-server shutdown

TELNET によるアクセスを拒否する場合に指定します。

設定例１　TELNET のアクセスを拒否する

```
Router(config)#telnet-server shutdown
```

コマンド書式

telnet-server shutdown

パラメータ

パラメータはありません。

この設定を行わない場合

TELNET によるアクセスを受け付けます。

設定モード

基本設定モード

http-server authname【F80/F100 コマンド】

ベーシック認証及びダイジェスト認証時に使用する<REALM 値>を指定します。
この値は、HTTP クライアント側における認証画面上に認証名称として表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　REALM 値を「FITELNET」とする

```
Router(config)#http-server authname FITELNET
```

コマンド書式

http-server authname <REALM 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
REALM 値	ベーシック認証及びダイジェスト認証時に使用する REALM 値を指定します。	英数字	省略不可

この設定を行わない場合

REALM 値は空文になります。

設定モード

基本設定モード

http-server authtype digest【F80/F100 コマンド】

HTTP(Web 設定)によるベーシック認証を無効にし、ダイジェスト認証を有効にします。

refresh コマンド後に有効になるコマンドです。

設定例１　HTTP（Web 設定）のベーシック認証を無効にし、ダイジェスト認証を有効にする

```
Router(config)#http-server authtype digest
```

コマンド書式

```
http-server authtype digest
```

パラメータ

パラメータはありません。

この設定を行わない場合

HTTP(Web 設定)によるダイジェスト認証を無効にし、ベーシック認証を有効にします。

設定モード

基本設定モード

http-server digest-auth nonceage【F80/F100 コマンド】

ダイジェスト認証時に使用する<NONCE 値>の有効期間を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NONCE 値を 100 秒とする

```
Router(config)#http-server digest-auth nonceage 100
```

コマンド書式

http-server digest-auth nonceage <NONCE 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
NONCE 値	ダイジェスト認証時に使用する NONCE 値の有効期間(秒)を指定します。	1～180	省略不可

この設定を行わない場合

NONCE 値は 60 秒になります。

設定モード

基本設定モード

http-server shutdown【F80/F100 コマンド】

HTTP(Web 設定)によるアクセスを拒否する場合に指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　HTTP（Web 設定）のアクセスを拒否する

```
Router(config)#http-server shutdown
```

コマンド書式

```
http-server shutdown
```

パラメータ

パラメータはありません。

この設定を行わない場合

HTTP(Web 設定)によるアクセスを受け付けます。

設定モード

基本設定モード

冗長機能

VRRP機能

ip vrrp enable

ルータ自身が VRRP ルータとして動作するか否かを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　VRRP ルータとして動作させる

```
Router(config)#ip vrrp enable
```

コマンド書式

ip vrrp enable

パラメータ

パラメータはありません。

この設定を行わない場合

VRRP ルータとして動作しません。

設定モード

基本設定モード

vrrp address

本インタフェースで動作するルータグループの仮想 IP アドレスを指定します。
Owner を指定した場合は、IP アドレスを指定する必要がありません。
自分が Master ルータの場合であっても通常、実 IP アドレスと違うアドレスをグループの仮想 IP アドレスとして指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN の VRRP ルータアドレスを 192.168.0.254 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 address 192.168.0.254
```

コマンド書式

vrrp 〈vrid〉 address 〈VRRP ルータアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※1	省略不可
VRRP ルータアドレス	本インタフェースに対しての IP アドレスとサブネットマスクを設定します。 owner：本インタフェースの持つ IP アドレスを VRRP ルータの IP アドレスとして使用します。 IP アドレス形式：同一 VRID 値を持つ仮想ルータ間で使用される IP アドレスを設定します。	owner※2 IP アドレス形式	省略不可

※VRRP ルータアドレスに関しては、仮想 IP アドレスを参照してください。
※1:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。
ただし、各インタフェースに設定できる VRID は、2つまでになります。
※2:VRRP owner 設定を使用する場合には、同じ VRID で動作する全インタフェースで owner 設定を行ってください。
また、同じ VRID で動作する全インタフェースで一致している必要があります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

Master ルータとは？

VRID が同じグループの中で、パケットの配送を行えるのが Master です。
他のルータはバックアップとして待機し、Master に障害が発生した場合に即座に動作を引き継ぎます。

この設定を行わない場合

VRRP アドレスの設定を行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp adver-interval

本論理インタフェースで動作する VRRP ルータの ADVERTISEMENT パケットの送信間隔を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　ADVERTISEMENT パケットの送信間隔を 3 秒に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 adver-interval 3
```

コマンド書式

vrrp 〈vrid〉 adver-interval 〈送信間隔〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可
送信間隔	Advertisement パケットの送信間隔(単位:秒)を設定します。	1～30	省略不可

※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

ADVERTISEMENT パケットとは？

Master ルータから定期的に送信される稼働状態確認用のパケットです。

この設定を行わない場合

ADVERTISEMENT パケットの送信間隔を 1 秒に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp auth-type

本論理インタフェースで動作する VRRP ルータの認証方法及び認証データを設定します。
認証を行う場合は、同一グループ内で同じパスワードを使用しないとグループ形成が行えません。

本設定の text-password は、古い VRRP プロトコルとの互換性のために用意されたものであり、セキュリティレベルの向上に寄与するものではありません。通常は、auth-type none-auth でご利用ください。

refresh コマンド後に有効になるコマンドです。

設定例１　認証方式を text-password とし、認証パスワードを vrrppass とします

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 auth-type text-password vrrppass
```

コマンド書式

vrrp 〈vrid〉 auth-type 〈認証タイプ〉〈認証パスワード〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※1	省略不可
認証タイプ	パケットの認証タイプを設定します。 none-auth：認証を行なわない。 text-password：8 文字以内のテキストデータを使用して認証を行なう。	none-auth※2 text-password	省略不可
認証パスワード	認証タイプに”text-password”を指定した場合に、パスワード文字列を設定します。	8 文字以内の英数字	省略不可

※1：VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。
ただし、各インタフェースに設定できる VRID は、2つまでになります。
※2：認証タイプに none-auth を選択した場合は、認証パスワードは入力できません。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

この設定を行わない場合

none-auth が設定されます。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp preempt

本論理インタフェースで動作する VRRP ルータの Preempt mode 有効を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　VRRP ルータの Preempt mode を有効にします

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 preempt
```

コマンド書式

vrrp <vrid> preempt

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可

※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

Preempt mode とは？

Master ルータに障害が発生してバックアップルータに切り替わる場合や、Master ルータが復旧して、バックアップルータから切り替わる場合の動作を指定します。
※起動した時に、自分の優先度が一番高かった場合の動作の規定

Preempt mode が有効な場合	vrrp priority コマンドで設定した優先度で判断し、常に優先度の高いルータが Master ルータとなります。
Preempt mode が無効の場合	Master ルータに障害が発生しバックアップルータが Master ルータになった後に、最初の Master ルータが復旧したとしても、vrrp priority コマンドで設定した優先度に関係なく現在の Master ルータ(元バックアップルータ)が保持されます。

VRRP と IPsec の連携

EWAN 側で VRRP を動作させ、IPsec を動作させる場合は、以下の注意が必要です。

FITELnet-F100 などの CPE から、FITELnet-F1000 に対して IPsec の通信を行う場合、VRRP で指定した仮想 IP アドレス宛にネゴシエーションを行うことが可能です。ただし、VRRP の代表ルータに障害が発生した場合、バックアップ側のルータが IPsec 通信の継続を試みますが、暗号化されたデータを復号化するための情報がないため、通信を継続することができません。

FITELnet-F1000 で VRRP を使用し、IPsec の通信を行う場合、CPE 側で SA の監視を行う必要があります。FITELnet-F100 では、DPD（Dead Peer Detection ）などの、SA 監視機能がサポートされていますので、必ず設定するようにしてください。この SA 監視機能により、SA が切れたことを認識でき、再度ネゴシエーションを行うことができます。

また、FITELnet-F1000 の Preempt（先制）モードが ON になっていると、VRRP の優先度が高いルータが起動することにより、代表ルータの切り替えが発生するため、IPsec の SA が一時切断されます。Preempt の設定の際は注意が必要です。

この設定を行わない場合

Preempt mode は無効です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

vrrp priority

Master ルータを決定する優先度を設定します。大きい数字ほど優先度は高くなります。
この優先度は、Master ルータに障害が発生した場合に作動する順番に使用されます。
優先度が同じであった場合は、ADVERTISEMENT パケット内の IP アドレス(1)で、最も大きい値を通知したルータが Master ルータになります。

refresh コマンド後に有効になるコマンドです。

設定例１　ルータの優先度を 120 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#vrrp 1 priority 120
```

コマンド書式

vrrp <vrid> priority <優先度>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	本インタフェースで動作する VRRP ルータの VRID を設定します。	1～255※	省略不可
優先度	Master router に遷移するための優先度を設定します。	1～254	省略不可

※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

VRID とは？

VRRP 機能で使用される、VRRP ルータグループの識別子です。
VRID が同一の VRRP ルータは、同じグループに所属します。

この設定を行わない場合

ルータの優先度を 100 に設定します。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

イベント-アクション機能

イベント

event-class

ルータ冗長機能における event-class と event-action のマッピングを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントクラス番号１とイベントアクション番号１を関連づける

```
Router(config)#event-map
Router(config-event-map)# event-class 1 event-action 1
```

コマンド書式

event-class 〈イベントクラス番号〉 event-action 〈イベントアクション番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントクラス番号	関連づけるイベントクラス番号を設定します。	1～500※	省略不可
イベントアクション番号	関連づけるイベントアクション番号を設定します。	1～500※	省略不可

※:F80、F100 の場合は、1～100 になります。

この設定を行わない場合

ルータ冗長機能を使用できません。

設定モード

イベントマップ設定モード

check ip-icmp

L3ping による到達確認の ICMP-CLASS 番号(宛先)設定を行います。
本設定項目を複数設定した場合には、<ICMP-CLASS 番号>が同一のものに関しては上書きとし、<ICMP-CLASS 番号>が異なる場合には、追加設定となります。
複数の設定が合った場合には、ICMP-CLASS 番号で優先度をつけます。
例(1:優先度高い　ー　500:優先度低い)

refresh コマンド後に有効になるコマンドです。

設定例１　L3ping による到達確認の ICMP-CLASS 番号を１とする

```
Router(config)#event-class 1
Router(config-event-class 1)# check ip-icmp 1
```

コマンド書式

check ip-icmp <ICMP-CLASS 番号> [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP-CLASS 番号	L3ping による到達確認の ICMP-CLASS 番号(宛先)設定します。	1～500	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

冗長機能は使用できません。

設定モード

イベントクラス設定モード

check interface status

設定したインタフェースの状態監視を行います。
本設定項目を複数設定した場合には、インタフェース名が同一のものに関しては上書きとし、インタフェース名が異なる場合には、追加設定とします。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN1 の状態監視を行う

```
Router(config)#event-class 1
Router(config-event-class 1)# check interface status ewan 1
```

コマンド書式

check interface status〈インタフェース名〉[invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	状態監視を行うインタフェースを指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

冗長機能は使用できません。

設定モード

イベントクラス設定モード

check vrrp status vrid

本機能により、設定した VRID の VRRP 状態監視を行うことができます。
通常の設定では、Master の場合が true、Master 以外の場合が false となります。
invert 設定の場合は逆(Master が false／Master 以外が true)。

refresh コマンド後に有効になるコマンドです。

設定例１　VRID 1 の VRRP 状態監視を行う

```
Router(config)#event-class 1
Router(config-event-class 1)# check vrrp status vrid 1
```

コマンド書式

check vrrp status vrid <VRID> [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VRID	VRRP 状態監視を行う VRID を設定します。	1～255※	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

**※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。
ただし、各インタフェースに設定できる VRID は、2つまでになります。**

この設定を行わない場合

VRID の VRRP 状態監視を行いません。

設定モード

イベントクラス設定モード

dampening disable

イベントフラップダンプニング機能を使用するかどうかの設定をします。
1 回のイベントで加算されるペナルティ値は 1000、ペナルティ値の計算間隔は 15 秒です。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントフラップダンプニング機能を無効とする

```
Router(config)#event-class 1
Router(config-event-class 1)# dampening disable
```

コマンド書式

dampening disable

パラメータ

パラメータはありません

この設定を行わない場合

イベントフラップダンプニング機能は有効です。

イベントフラップダンプニング機能とは

イベントフラップダンプニング機能とは、イベントのフラッピング（ばたつき）を考慮し不安定なイベントに対してペナルティを付加することにより、一定値をこえるとそのイベントをこえる直前の状態（true or false）に固定し、ペナルティ値を下回ることで再びイベントの状態により変動できるようにする機能です。
本機能は、イベントクラスごとに設定することができます。

設定モード

イベントクラス設定モード

dampening-parameter

イベントフラップダンプニング機能の各種設定を行います。

refresh コマンド後に有効になるコマンドです。

設定例 1　半値時間を 45 分、フラッピング状態閾値を 2000、フラッピング復旧閾値を 750 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# dampening-parameter 45 2000 750
```

コマンド書式

dampening-parameter〈半値時間〉〈フラッピング状態発生閾値〉〈フラッピング復旧閾値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
半値時間	ペナルティ値の減少割合を、ペナルティ値が半分に減少するまでの時間で設定します。(単位:分)	1～45	省略不可
フラッピング状態発生閾値	フラッピング状態とみなすペナルティ値(ペナルティ値が設定値をこえた場合にフラッピング状態とみなす)を設定します。	1～65535	省略不可
フラッピング復旧閾値	フラッピング状態から復旧したとみなすペナルティ値(ペナルティ値が設定値と以下(同値を含む)になったの場合に復旧とみなす)を設定します。	1～65535	省略不可

この設定を行わない場合

半値時間:5 分、フラッピング状態閾値:20000、フラッピング復旧閾値:10000 とします。

イベントフラップダンプニング機能とは

イベントフラップダンプニング機能とは、イベントのフラッピング(ばたつき)によってアクションが多発するのを抑止するための機能です。
イベントの状態変化が発生した際にペナルティ値を累積し、フラッピング状態発生閾値を超えるとそのイベントを超える直前の状態(True もしくは False)に固定する機能です。
ペナルティ値は時間とともに減少し、フラッピング状態復旧閾値を下回ると、再びイベントの状態が変化するようになります。本機能は、イベントクラスごとに設定することができます。

設定モード

イベントクラス設定モード

description

各 event-action に Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　event-action に Description を description EVENT_ACTION 1 Main Route とする

```
Router(config)#event-action 1
Router(config-event-action 1)# description EVENT_ACTION 1 Main Route
```

コマンド書式

description <LINE>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
LINE	各 event-action に Description を設定します。	-	省略不可

※設定文字数に制限はありませんが、show event-action コマンドでの表示は 256 文字までです。

この設定を行わない場合

各 event-action に Description を設定しません。

設定モード

イベントアクション設定モード

event match-any

イベントクラスに設定されているイベント個別設定の何れかのステータスが True の場合にイベントクラスのステータスを true とします。

refresh コマンド後に有効になるコマンドです。

設定例１　L3Ping1 と L3Ping2 のどちらかが true の時 event-class を true とする

```
Router(config)#event-class 1
Router(config-event-class 1)# event match-any
Router(config-event-class 1)# check ip-icmp 1
Router(config-event-class 1)# check ip-icmp 2
Router(config-event-class 1)# exit
```

コマンド書式

event match-any

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断します。

例として、設定例 1 で event match-any を指定しなかった場合は以下のようになります。

```
Router(config)#event-class 1
Router(config-event-class 1)# check ip-icmp 1
Router(config-event-class 1)# check ip-icmp 2
Router(config-event-class 1)# exit
```

この場合、L3Ping1 が true、かつ 3Ping2 が true の時 event-class が true となります。

設定モード

イベントクラス設定モード

logging event state-change

本コマンドで、enable が設定されている場合、icmp-class、event-action、event-class の各クラスの状態変化が発生するとログを記載します。
disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change 〈ログ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード

match duration

イベントクラスにて時刻の範囲指定を行う場合に設定します。
from で指定した時刻から、to で指定した時刻までを TRUE の状態とします。
また、range minute オプションを指定することで、指定した時刻から経過時間内を TRUE 状態とする事も出来ます。

refresh コマンド後に有効になるコマンドです。

設定例１　範囲指定を 2008/02/01 0:0:0 ～ 2008/02/15 0:0:0 とする

```
Router(config)#event-class 1
Router(config-event-class 1)# match duration from 2008 2 1 to 2008 2 15
```

設定例 2　範囲指定を 2008/02/01 12:10 から 12 時間とする

```
Router(config)#event-class 1
Router(config-event-class 1)# match duration from 2008 2 1 range minute 720
```

コマンド書式

match duration from 〈年〉〈月〉 { 日 | 曜日 } 〈時〉〈分〉 to 〈年〉〈月〉 { 日 | 曜日 } 〈時〉〈分〉 [invert]

match duration from 〈年〉〈月〉 { 日 | 曜日 } 〈時〉〈分〉 range minute 〈分〉 [invert]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
年	西暦、または any を指定します。 any を指定することにより"毎年"として扱われます。	any 2000～ 2035	省略不可
月	月、または any を指定します。 any を指定することにより"毎月"として扱われます。	any 1～12	省略不可
日｜曜日	日にち/曜日、または any を指定します。 any を指定することにより"毎日"として扱われます。 また、last を指定することで月末を指定することが出来ます。	any 1～31 sun mon tue wed thu fri sat last	省略不可
時	時、または any を指定します。 any を指定することにより"毎時"として扱われます。	any 0～23	省略不可

分	分、または any を指定します。 any を指定することにより"毎分"として扱われます。	any 0～59	省略不可
range minute〈分〉	分単位で範囲を指定します。	0～ 5000000	省略不可
invert	真(true)と偽(false)の状態を反転させて通知する場合に指定します。	invert	真(true)、偽(false)をそのまま通知します。

この設定を行わない場合

イベントクラスとして時刻の範囲指定を行いません。

設定モード

イベントクラス設定モード

宛先到達確認

icmp-class

ICMP クラス設定モードに移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　ICMP クラス設定モードに移行する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)#
```

コマンド書式

icmp-class <ICMP クラス番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	ICMP クラス番号を指定します。	1～100	省略不可

設定モード

基本設定モード

address

L3ping による到達確認の宛先設定を行ないます。
本設定は同一の icmp-class 内では複数設定を行なうことはできません。
source-interface の設定がある場合には、指定したインタフェースの IP アドレスを送信元 IP アドレスとして送信します。
nexthop の設定がある場合は、続く引数がインタフェース名もしくは、IP アドレスにより動作が異なります。続く引数が、インタフェース名の場合には、インタフェース名で指定するインターフェースへ L3Ping の送信を行ないます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.1.1 宛へ LAN1 側の IP アドレスを送信元として、EWAN1 インタフェース経由で送信する

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# address 192.168.1.1 source-
interface lan 1 nexthop ewan 1
```

コマンド書式

address 〈IP アドレス〉 [source-interface 〈インタフェース名〉] [nexthop {〈インタフェース名〉|〈IP アドレス〉}]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	到達確認用の L3ping を送信する宛先の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース名	L3ping を送信する際にインタフェースを指定する場合に設定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 loopback 1 tunnel 1～32 vlanif 1～16	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。

この設定を行わない場合

冗長機能は使用できません。

設定モード

ICMP クラス設定モード

interval

L3ping の到達間隔設定を行います。
refresh によりタイマ値が変更となった場合においては、それまでのタイマ値を引き継ぎます。

refresh コマンド後に有効になるコマンドです。

設定例１　送信間隔を 120 秒、復旧と見なすまでの間隔を 60 秒とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# interval 120 restoration 60
```

コマンド書式

interval <INTERVAL> [restoration <REST-INTERVAL>]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
INTERVAL	L3ping の送信間隔を設定します。	1～2000000	省略不可
REST-INTERVAL	L3ping が復旧したと確認するまでの間隔を設定します。	1～2000000	省略不可

この設定を行わない場合

true 時 30 秒、false 時 30 秒毎に L3ping 確認を行います。

設定モード

ICMP クラス設定モード

trial

L3ping における状態遷移までの回数を設定します。
L3ping の状態が false 時に連続して<TRIAL-TIME>回疎通確認になった時点で出力状態を true とします。
また、true 時は連続して<FAIL-TIME>回疎通未確認となった時点で出力状態を false とします。
refresh により確認回数が変更となった場合においては、それまでのタイマ値を引き継ぎます。

refresh コマンド後に有効になるコマンドです。

設定例１　疎通回数１回、未疎通回数１回を確認回数とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# trial 1 fail 1
```

コマンド書式

trial <TRAIAL-TIME> fail <FAIL-TIME>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
TRAIAL-TIME	疎通確認とみなすまでの確認回数を設定します。	1～16	省略不可
FAIL-TIME	未疎通確認とみなすまでの確認回数を設定します。	1～16	省略不可

この設定を行わない場合

TRAIAL-TIME:3 回、FAIL-TIME:2 回の確認を行います。

設定モード

ICMP クラス設定モード

size

L3ping のパケットサイズを指定します。
指定したサイズは、ICMP-ECHO のデータ部サイズになります。

refresh コマンド後に有効になるコマンドです。

設定例１　パケットサイズを 256 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# size 256
```

コマンド書式

size 〈パケットサイズ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
パケットサイズ	L3ping のパケットサイズを設定します。	10～3000	省略不可

この設定を行わない場合

パケットサイズは、56 になります。

設定モード

ICMP クラス設定モード

probe

L3ping を送出する際に、複数個の ICMP メッセージを送出します。
指定パケット数のうち1パケットでも戻りがあれば成功と判断します。
また、(Layer3 タスクが)成功判断後は、残りパケットの送信しません。

refresh コマンド後に有効になるコマンドです。

設定例１　送出パケット数を 10 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# probe 10
```

コマンド書式

probe <PROBE PACKET>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
PROBE PACKET	L3ping の送出パケット数を設定します。	1～10	省略不可

この設定を行わない場合

パケット数は、2 になります。

設定モード

ICMP クラス設定モード

timeout

L3ping の送信タイムアウト時間(秒)の設定を行います。
連続送信時に最後の1パケットの送信から timeout 設定時間が経過したらタイムアウトと判断します。
refresh による即時有効コマンドですが、送信処理中の場合は、以前のタイムアウト値を使用し次の送信開始から設定されたタイムアウトを使用します。

refresh コマンド後に有効になるコマンドです。

設定例１　タイムアウトを 10 秒とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# timeout 10
```

コマンド書式

timeout 〈タイムアウト〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト	L3ping の送信タイムアウト時間(秒)の設定を行います。	1～10	省略不可

この設定を行わない場合

タイムアウトを 3 秒とします。

設定モード

ICMP クラス設定モード

logging event state-change

本コマンドで、enable が設定されている場合、icmp-class、event-action、event-class の各クラスの状態変化が発生するとログを記載します。
disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change 〈ログ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード

description

icmp-class の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　icmp-class の Description を L3PING ICMP Class Description#1 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# description L3PING ICMP Class Description#1
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	icmp-class の Description を設定します。	-	省略不可

※設定文字数に制限はありませんが、show icmp-class コマンドでの表示は 256 文字までです。

この設定を行わない場合

icmp-class の Description を設定しません。

設定モード

ICMP クラス設定モード

アクション

add ip route

経路情報の追加を行います

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.1.0 255.255.255.0 への経路を NextHop192.168.100.1 とする

```
Router(config)#event-action 1
Router(config-event-action 1)# add ip route 192.168.1.0
255.255.255.0 192.168.100.1
```

コマンド書式

add ip route 〈宛先ネットワーク〉〈マスク〉〈NextHop〉[〈distance〉] [onetime]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先 ネットワーク	スタティックルーティングの宛先ネットワークアドレス	IPv4 アドレス形式	省略不可
マスク	宛先ネットワークに対するマスク	IPv4 アドレス形式	省略不可
NextHop	宛先へ到達するための NextHop の IP アドレスまたは、インタフェースを指定します。	IPv4 アドレス形式 ewan 1～2 pppoe 1～24※1 loopback 1 dialer 1～20※2 ipsecif 1～500※3 tunnel 1～32	省略不可
distance	スタティックルーティングの distance 値を指定します。	1～255	1
onetime	true から false へ遷移時の経路情報の削除をおこなわない場合に指定します。 onetime 動作時の経路削除は装置再起動時または、該当の onetim 設定した経路を消去し即時有効させた場合に削除されます。	onetime	true から false へ遷移時の経路情報の削除を行う

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

経路情報を追加しません。

設定モード

イベントアクション設定モード

clear ipsec-session isakmp-policy

指定した ISAKMP ポリシー番号に関連する Phase 1 SA と Phase 2 SA のセッションを解放します。
true→false になった場合には、何も行いません。

refresh コマンド後に有効になるコマンドです。

設定例１　isakmp-policy 1 のセッションを解放する

```
Router(config)#event-action 1
Router(config-event-action 1)# clear ipsec-session isakmp-policy 1
```

コマンド書式

clear ipsec-session isakmp-policy <ISAKMP ポリシー番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ISAKMP ポリシー番号	セッションを解放する ISAKMP ポリシー番号を指定します。	1～500※	省略不可

※:F80 の場合は、1～32、
　F100 の場合は、1～100 になります。

この設定を行わない場合

セッションを解放しません。

設定モード

イベントアクション設定モード

description

icmp-class の Description を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　icmp-class の Description を L3PING ICMP Class Description#1 とする

```
Router(config)#icmp-class 1
Router(config-icmp-class 1)# description L3PING ICMP Class Description#1
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	icmp-class の Description を設定します。	-	省略不可

※設定文字数に制限はありませんが、show icmp-class コマンドでの表示は 256 文字までです。

この設定を行わない場合

icmp-class の Description を設定しません。

設定モード

ICMP クラス設定モード

e-mail body false-to-true

イベントアクションとして送信する電子メールの本文を設定します。
電子メールの本文は、定型文となっており、設定した内容は、定型文の最下行に追加されます。
この指定は、イベントが False→True となった場合のアクションの場合に追加されます。

refresh コマンド後に有効になるコマンドです。

設定例１　通知する電子の本文に VRRP status changes to Master. を追加する

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail body false-to-true VRRP
status changes to Master.
```

コマンド書式

e-mail body false-to-true<本文>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
本文	False->True のイベントにより送信する電子メールの本文に追加する 1 行を設定します。	最大 254 文字	省略不可

この設定を行わない場合

定型文のみ送信します。定型文は、以下の書式となります。

＜定型文例＞

```
SysDescr      : FITELnet-F100 Ver 01.30-052003 V02.03(00) 082905
IP Address    : 192.168.2.254
Time          : 2005/08/30(TUE) 12:45:18
```

設定モード

イベントアクション設定モード

e-mail body true-to-false

イベントアクションとして送信する電子メールの本文を設定します。
電子メールの本文は、定型文となっており、設定した内容は、定型文の最下行に追加されます。
この指定は、イベントが True→False となった場合のアクションの場合に追加されます。

refresh コマンド後に有効になるコマンドです。

設定例１　通知する電子の本文に VRRP status change to Backup.！を追加する

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail body true-to-false VRRP
status changes to Backup.!
```

コマンド書式

e-mail body true-to-false<本文>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
本文	True→False のイベントにより送信する電子メールの本文に追加する 1 行を設定します。	最大 254 文字	省略不可

この設定を行わない場合

定型文のみ送信します。定型文は、以下の書式となります。

＜定型文例＞

SysDescr　　: FITELnet-F100 Ver 01.30-052003 V02.03(00) 082905
IP Address　　: 192.168.2.254
Time　　: 2005/08/30(TUE) 12:45:18

設定モード

イベントアクション設定モード

e-mail subject

イベントアクションとして、電子メール通知を行う際のサブジェクトを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　通知する電子のサブジェクトを VRRP status change !!とする

```
Router(config)#event-action 1
Router(config-event-action 1)# e-mail subject VRRP status change !!
```

コマンド書式

e-mail subject 〈サブジェクト〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
サブジェクト	電子メール通知を行う際のサブジェクトを設定します。	最大 254 文字	省略不可

この設定を行わない場合

Event-action occurred on FITELnet-F100 (〈LAN 側 IP アドレス〉) True->False もしくは False->True (アクションの起動契機により変更)

設定モード

イベントアクション設定モード

logging event state-change

本コマンドで、enable が設定されている場合、icmp-class、event-action、event-class の各クラスの状態変化が発生するとログを記載します。
disable または、未設定(デフォルト)の場合は記載されません。

refresh コマンド後に有効になるコマンドです。

設定例１　event-class の状態変化が発生した場合ログを記載する

```
Router(config)#event-class 1
Router(config-event-class 1)# logging event state-change enable
Router(config-event-class 1)# exit
```

コマンド書式

logging event state-change 〈ログ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ログ設定	状態変化によりログを記載するかどうかを指定します。 enable　ログを記載する disable　ログを記載しない	enable disable	省略不可

この設定を行わない場合

状態が変化してもログを記載しません。

設定モード

イベントクラス設定モード
イベントアクション設定モード
ICMP クラス設定モード

igmp-proxy disable-upstream 【F100/F1000 コマンド】

本コマンドを設定することにより、イベントアクション稼働時に、指定したインタフェースでは IGMP Proxy の動作を無効にします。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN １インタフェースに対して、イベントアクション稼働時に IGMP Proxy の動作を無効にする

```
Router(config)#event-action 1
Router(config-event-action 1)# igmp-proxy ewan 1 disable-upstream
```

コマンド書式

igmp-proxy 〈インタフェース名〉 disable-upstream

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	イベントアクション稼働時に、IGMP Proxy の動作を有効としないインタフェースを指定します。	lan 1 ewan 1～2 ipsecif 1～500※ vlanif 1～16	省略不可

※: F100 の場合は、1～100 になります。

この設定を行わない場合

インタフェースで IGMP Proxy の動作を無効にしません。

設定モード

イベントアクション設定モード

igmp-proxy non-querier　【F100/F1000 コマンド】

本コマンドを設定することにより、イベントアクションが稼働した時に non-querier 状態に移行します。

refresh コマンド後に有効になるコマンドです。

設定例１　EWAN １インタフェースに対して non-querier 状態とする

```
Router(config)#event-action 1
Router(config-event-action 1)# igmp-proxy ewan 1 non-querier
```

コマンド書式

igmp-proxy 〈インタフェース名〉 non-querier

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	non-querier 状態とするインタフェースを指定します。	lan 1 ewan 1～2 vlanif 1～16	省略不可

この設定を行わない場合

non-querier 通知をしません。

設定モード

イベントアクション設定モード

send e-mail

イベントアクションとして、電子メール通知を行うかどうかの設定を行います。
電子メールは、イベントの true->false, false->true のどちらの場合でも送信します。
本コマンドを使用するには、電子メールによる障害通知機能(mail to コマンド)を設定する必要があります。

設定例１　イベントアクションとして、電子メール通知を行う

```
Router(config)#event-action 1
Router(config-event-action 1)# send e-mail
```

コマンド書式

send e-mail

パラメータ

パラメータはありません

この設定を行わない場合

電子メール通知を行いません。

設定モード

イベントアクション設定モード

send snmp-trap

本コマンドを指定した場合は、ステータスが activate および deactivate に遷移した際に、SNMP トラップを送信します。

設定例１　SNMP トラップを送信する

```
Router(config)#event-action 1
Router(config-event-action 1)# send snmp-trap
```

コマンド書式

```
send snmp-trap  [description]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
description	イベントアクション設定モードの description コマンドで指定した内容を、SNMP トラップに含めて通知します。	description	SNMP トラップに description を含めない

※ 詳細は、description コマンドを参照して下さい。

この設定を行わない場合

SNMP トラップを送信しません。

設定モード

イベントアクション設定モード

set ipsec-status discard isakmp-policy

イベントアクションのアクションとして、指定する ISAKMP ポリシーを利用する SA を DISCARD 状態にします。
DISCARD 状態になると、接続している IPsec-SA／IKE-SA を解放し、指定した SA との接続は行わななくなります。

refresh コマンド後に有効になるコマンドです。

設定例１　SA　１の IPsec 状態を DISCARD とする

```
Router(config)#event-action 1
Router(config-event-action 1)# set ipsec-status discard isakmp-policy 1
```

コマンド書式

```
set ipsec-status discard isakmp-policy <SA>
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SA	IPsec 状態を DISCARD にする SA を指定します。	1～100	省略不可

この設定を行わない場合

IPsec 状態を DISCARD にしません。

設定モード

イベントアクション設定モード

set policy-flag

指定したポリシーフラグ名（任意の文字列:64 文字以内）のフラグを ON にします。
複数のイベントで同じポリシーフラグを操作する設定の場合、全ての状態においてポリシーフラグが OFF になった場合に OFF となり、1つでも ON の状態が存在する場合には ON となります。

指定したポリシーフラグは、QoS 機能のクラスマップで使用します。
指定したポリシーフラグの状態で、QoS のクラス分けを行うことができます。
ポリシーフラグを使用した QoS のクラス分けは、match policy-flag コマンドで指定します。

本コマンドおよび、クラスマップ設定モードの"match policy-flag"コマンドを使用することにより、イベントが発生した場合としていない場合で、QoS やポリシールーティングの制御を変えることが可能です。
インタフェースの状態や、VRRP の状態などを検知し、柔軟に QoS やポリシールーティングの制御を変えて運用することができます。

設定例１　POLI1-FLAG のフラグを ON にする

```
Router(config)#event-action 1
Router(config-event-action 1)# set policy-flag POLI1-FLAG
```

コマンド書式

set policy-flag <ポリシーフラグ名>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーフラグ名	フラグを ON にするポリシーフラグ名を指定します。	最大 64 文字	省略不可

この設定を行わない場合

フラグを ON にするポリシーフラグを指定しません。

設定モード

イベントアクション設定モード

suspend icmp-class

icmp-class コマンドで指定した ICMP クラスの経路監視を停止します。
停止した際は、経路監視の状態は Suspend 状態となります。ただし、統計情報のクリアはせず、継続してカウントします。

suspend icmp-class コマンドを使用することで、本装置が経路監視を行う必要が無い場合（VRRP におけるバックアップルータ等）に経路監視を停止することができます。

設定例１　ICMP クラス番号 100 の経路監視を停止する

```
Router(config)#event-action 1
Router(config-event-action 1)# suspend icmp-class 100
```

コマンド書式

suspend icmp-class <ICMP クラス番号> [onetime]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ICMP クラス番号	経路監視を停止する ICMP クラス番号を指定します。	1～500※	省略不可
onetime	経路監視の停止を初回動作時のみ行います。	onetime	経路監視の停止/再開を繰り返します。

※:F80 の場合は、1～32、
　F100 の場合は、1～100 になります。

この設定を行わない場合

経路監視を停止ししません。

設定モード

イベントアクション設定モード

vrrp

vrid の Priority の変更を行います。

設定例１　vrrp：10、track：1、decrement：120 とします

```
Router(config)#event-action 1
Router(config-event-action 1)# vrrp 10 track 1 decrement 120
```

コマンド書式

vrrp <vrid> track <track_no> decrement <priority>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
vrid	変更したい vrid を指定します。	1～255	省略不可
track_no	track_no 値を設定します。 VRRP の priority 減算が4つまで設定できます。 tack 番号の重複は無効になります。(重複の場合両方とも無効) また、4つ以上の登録は無効とになります。	1～4	省略不可
priority	priority 値を設定します。	1～255※	省略不可

※:VRID の設定範囲は 1～255 ですが、1台の装置に設定できる VRID は32までとなります。ただし、各インタフェースに設定できる VRID は、2つまでになります。

この設定を行わない場合

vrid の Priority 値を変更しません。

設定モード

イベントアクション設定モード

マッピング

event-map

イベントマップ設定モードに移行します。

設定例１　イベントマップ設定モードに移行します。

```
Router(config)#event-map
Router(config-event-map)
```

コマンド書式

event-map〈イベントマップ番号〉

パラメータ

パラメータはありません。

設定モード

基本設定モード

event-class

ルータ冗長機能における event-class と event-action のマッピングを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　イベントクラス番号１とイベントアクション番号１を関連づける

```
Router(config)#event-map
Router(config-event-map)# event-class 1 event-action 1
```

コマンド書式

event-class 〈イベントクラス番号〉 event-action 〈イベントアクション番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
イベントクラス番号	関連づけるイベントクラス番号を設定します。	1～500※	省略不可
イベントアクション番号	関連づけるイベントアクション番号を設定します。	1～500※	省略不可

※:F80、F100 の場合は、1～100 になります。

この設定を行わない場合

ルータ冗長機能を使用できません。

設定モード

イベントマップ設定モード

QoS/CoS機能

クラスマップの定義

class-map

クラスマップモードに移行し、トラフィックを分類するクラシファイアを定義します。
クラスマップモードでは、match ip もしくは、match ipv6 コマンドによってトラフィックの分類条件が設定されます。
複数の条件が設定された場合、match-any の有無によって、複数の条件が OR 条件となるか、AND 条件となるかが指定されます。
IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合は、指定された条件は無視されるのではなく、不成立と判定されます。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ設定モードへ移行します。

```
Router(config)#class-map video-class
Router(class-map video-class)#
```

コマンド書式

class-map〈クラスマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラスマップ名	クラスマップ名称を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップ名によるトラフィックの分類を行いません。

設定モード

基本設定モード

match-any

同一 class-map 内で複数の match 行が記述された場合の動作を指定します。
いずれか 1 つの match 行にマッチした場合に class-map に適合したと判断します。

refresh コマンド後に有効になるコマンドです。

設定例１　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する。

```
Router(config)#class-map video-class
Router(class-map video-class)#match-any
Router(class-map video-class)#match ip access-group 2000
Router(class-map video-class)#exit
```

コマンド書式

match-any

パラメータ

パラメータはありません

この設定を行わない場合

全ての match 行にマッチした場合に、クラスマップに適合したと判断する

設定モード

クラスマップ設定モード

match ip/ipv6 access-group

クラスマップ内でマッチするトラフィックを、IP アクセスリストにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
アクセスリストの log と count は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IP アクセスリストの 2000 番をマッチするトラフィックとして設定する。

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip access-group 2000
Router(config-class-map)#exit
```

コマンド書式

match ip access-group <ext-ipv4 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}
match ipv6 access-group <ext-ipv6 アクセスリスト番号 > [input-interface {<インタフェース名> [port <ポート番号>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ext-ipv4 アクセスリスト番号	クラスマップ内でマッチするトラフィックを ext-ipv4 アクセスリスト番号で指定します。	100～199、2000～2699	省略不可
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match ip/ipv6 input-interface

クラスマップ内でマッチするトラフィックを、入力インタフェースにより設定します。
トラフィックが IPv4 パケットの場合、match ipv6 コマンドは不成立となります。逆にトラフィックが IPv6 パケットの場合、match ip コマンドは不成立となります。
同一 class-map 内で複数の match ip もしくは match ipv6 が定義された場合、定義された順に評価されます。
同一 class-map において match-any が指定されている場合には、いずれの match 行にもトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。
match-any が指定されていない場合には、いずれかの match 行にトラフィックが適合しなかった場合、該当する class-map には適合しなかったものとされます。

refresh コマンド後に有効になるコマンドです。

設定例１　トラフィックを分類するインタフェースを EWAN 1 として設定する

```
Router(config)#class-map video-class
Router(config-class-map)#match-any
Router(config-class-map)#match ip input-interface ewan 1
Router(config-class-map)#exit
```

コマンド書式

match ip input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]
match ipv6 input-interface [input-interface 〈インタフェース名〉 [port 〈ポート番号〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	クラスマップ内でマッチするトラフィックを入力インタフェースで指定します。	lan 1 ewan 1～2 pppoe 1～24※1 dialer 1～20※2 ipsecif 1～500※3 vlanif 1～16	全てのインタフェース
ポート番号	LAN インタフェースの物理ポート番号を指定します。	port 1～4	LAN インタフェースのポート番号

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

該当クラスマップにトラフィックはマッチしません

設定モード

クラスマップ設定モード

match policy-flag

QoS 変更用のフラグがセットされている、もしくはセットされていない場合の class として動作します。
イベントアクションからの通知が 1 度もない状態では、ポリシーフラグを OFF として扱います。

refresh コマンド後に有効になるコマンドです。

設定例１　QoS 変更用フラグの class を POLI1-FLAG とする。

```
Router(config)# class-map video-class
Router(class-map video-class)# match policy-flag POLI1-FLAG set
Router(class-map video-class)# exit
```

コマンド書式

match policy-flag 〈ポリシーフラグ名〉 {set|unset}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーフラグ名	QoS 変更用フラグの class をしていします。	最大 64 文字	省略不可
set|unset	QoS 変更用フラグがセットされているもしくは、されていない場合を対象とします。 set：ポリシーフラグがセットされている場合に適用 unset：ポリシーフラグがセットされていない場合に適用	set unset	省略不可

この設定を行わない場合

設定を行っていない場合は、このフラグの情報はクラスわけの情報として使用しません。

設定モード

クラスマップ設定モード

アクションマップの定義

action-map

action-map モードに移行し、トラフィックに対するアクションを定義します。
実行場所によってサポートされないアクションや、IPv4/IPv6 の違いにより設定されたコマンドが該当しないような場合、指定されたアクションは無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションマップ設定モードへ移行する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#
```

コマンド書式

action-map 〈アクションマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
アクションマップ名	アクションマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

アクションは定義されません。

設定モード

基本設定モード

drop

アクションとして、パケット廃棄を設定します。
同一アクションマップに他のコマンドが設定されていても、本コマンドが優先されます。

refresh コマンド後に有効になるコマンドです。

設定例１　アクションとしてパケット廃棄を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#drop
```

コマンド書式

drop

パラメータ

パラメータはありません

この設定を行わない場合

パケットは破棄されません。

設定モード

アクションマップ設定モード

set ip dscp

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IPv4 ヘッダに対するマーキングとして、dscp に ef を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set ip dscp ef
```

コマンド書式

```
set ip dscp {<dscp-value>|<dscp-named-value>}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp-value	dscp-value を設定します。	0～63	省略不可
dscp-named-value	dscp-named-value を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ip next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6} next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　パケット中継先を 192.168.100.1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ip next-hop 192.168.100.1 distance 10
```

コマンド書式

```
set ip next-hop <IP アドレス> [distance]
set ip next-hop <インタフェース> [distance]
set ip next-hop connected {ipsecif <1-500> | null <0-0>} [distance]
set ip next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv4 アドレス形式	省略不可
インタフェース	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	ewan 1～2 pppoe 1～24※1 dialer 1～20※2 tunnel 1～32	省略不可
connected ipsecif	宛先への経路として IPsec インタフェースを指定します。	ipsecif 1～500※3	省略不可
connected null	廃棄用の宛先経路情報とします。	null 0	省略不可
distance	中継先の distance 値を設定します。	1～255	省略不可
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

※1:F80 の場合は、1～5 になります。
※2:F100 のみ選択可能です。
※3:F80 の場合は、1～32、
　　F100 の場合は、1～100 になります。

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

set ip prec

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IPv4 ヘッダに対するマーキングとして、prec に routine を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set ip prec routine
```

コマンド書式

set ip prec {<precedence-value>|<precedence-named-value>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
precedence-value	precedence-value を設定します。	0～7	省略不可
precedence-named-value	precedence-named-value を設定します。	routine(0), priority(1) immediate(2), flash(3) flash-override(4) critical(5), internet(6) network(7)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ip tos

アクションとして、IPv4 ヘッダに対するマーキングを設定します。
対象パケットが IPv4 パケットではなかった場合、本設定は無視されます。
prec と tos は組み合わせて用いることができますが、dscp とは排他となります。
コンフィグ読み込み側での処理として、dscp が設定されている場合は dscp 設定が優先され prec と tos の設定は無効となります。
dscp が設定されていない場合のみ prec と tos の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IPv4 ヘッダに対するマーキングとして、tos に min-momentary-cost を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set ip tos min-momentary-cost
```

コマンド書式

```
set ip tos {<tos-value>|<tos-named-value}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
tos-value	tos-value を設定します。	0～15	省略不可
tos-named-value	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4), min-delay(8) ,normal(0)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ipv6 dscp

アクションとして、IPv6 ヘッダに対するマーキングを設定します。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IPv6 ヘッダに対するマーキングとして、dscp に ef を設定する。

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set ipv6 dscp ef
```

コマンド書式

set ipv6 dscp {<dscp-value>|<dscp-named-value>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dscp-value	dscp-value を設定します。	0～63	省略不可
dscp-named-value	dscp-named-value を設定します。	ef(101110b), bf(000000b) af11(001010b), af12(001100b) af13(001110b), af21(010010b) af22(010100b), af23(010110b) af31(011010b), af32(011100b) af33(011110b), af41(100010b) af42(100100b), af43(100110b)	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set ipv6 next-hop

アクションとして、パケット中継先を設定します(ポリシールーティング)。
有効な中継先のうち、distance 値がもっとも小さい中継先が有効になります。
有効な中継先のうち、もっとも distance 値が小さい中継先が同一 distance 値で複数存在する場合、config 表示で最も上の設定が適用されます。
distance 値が省略された場合のデフォルトは"1"とします。
中継先が到達不能な場合、その経路は無視されます。
個々の中継先が全て到達不能な場合、もしくは指定されていない場合、set {ip|ipv6}next-hop default が指定されている場合には、通常のルーティングが行なわれます。
指定されていない場合には、パケットは中継不能パケットとして廃棄されます。
パケットが IPv4 の場合、set ipv6 は無視されます。逆にパケットが IPv6 の場合、set ip は無視されます。
本コマンドは、I/F 受信時のサービスポリシーとして設定された場合と、自局送信時のサービスポリシーとして設定された場合にのみ有効となり、I/F 送信時のサービスポリシーとして設定された場合には無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　パケット中継先を 2002:1004::1 に distance 10 で設定する

```
Router(config)#action-map stream-action
Router(config-action-map)#set ipv6 next-hop 2002:1004::1 distance 10
```

コマンド書式

```
set ipv6 next-hop <IP アドレス> [インタフェース※1][distance]
set ipv6 next-hop <インタフェース※2> [distance]
set ipv6 next-hop default
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	中継先の IP アドレスを設定します。	IPv6 アドレス形式	省略不可
インタフェース※1	NextHop にリンクローカルアドレスを設定した場合は、インタフェースの指定が必要です。	lan 1 ewan 1～2 pppoe 1～24※3 tunnel 1～32	―
インタフェース※2	PPPoE インタフェースのように、宛先へ到達するための NextHop の IP アドレスが明確に分からない場合に設定します。	pppoe 1～24※3	省略不可
distance	中継先の distance 値を設定します。	1～255	1
default	ポリシールーティングを行わずに、通常のルーティングをおこないます。	なし	省略不可

※3:F80 の場合は、1～5 になります。

この設定を行わない場合

中継先設定は行なわれません。

（参考）他のプロトコルの distance 値

他のプロトコルの distance 値は、以下のようになっています。

プロトコル	デフォルト値	備考
スタティック	1	変更可能
直接ルート	-	変更不可
BGP(external)	20	変更可能
BGP(internal)	200	
BGP(local)	200	
RIP	120	変更可能
OSPF(external)	110	変更可能
OSPF(inter-area)	110	
OSPF(intra-area)	110	
IKE ルート	0	変更不可
SA-up ルート	0	変更可能
REDUNDANCY ルート	0	変更可能
EventAction ルート	1	変更可能
AutoConfig	0	変更不可

設定モード

アクションマップ設定モード

set ipv6 traffic-class

アクションとして、IPv6 ヘッダに対するマーキングを設定します。
対象パケットが IPv6 パケットではなかった場合、本設定は無視されます。traffic-class と dscp とは排他となります。
コンフィグ読み込み側での処理とし、dscp が設定されている場合は dscp 設定が優先され traffic-class の設定は無効になります。
dscp が設定されていない場合のみ traffic-class の設定が有効になります。
アクションが指定されなかったヘッダフィールドは、マーキングされずにそのまま転送されます。

refresh コマンド後に有効になるコマンドです。

設定例１　IPv6 ヘッダに対するマーキングとして、traffic-class の値を 5 に設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set ipv6 traffic-class 5
```

コマンド書式

set ipv6 traffic-class <traffic-class-value>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
traffic-class-value	traffic-class-value を設定します。	0～255	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

set queuing

アクションとして、CBQ もしくは PRIQ によって優先制御や帯域制御を行ないます。
指定したキュー名が定義されていない場合、設定エラーとなり、無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　stream-action に stream-que を設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)#set queuing stream-que
```

コマンド書式

set queuing <que-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
que-name	que-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

優先制御や帯域制御は行われません。

設定モード

アクションマップ設定モード

set 802.1p priority

アクションとして、Ethernet ヘッダ 802.1p Priority に対するマーキングを設定します。
アクションが指定されなかった場合、マーキングされずにそのまま転送されます。
出力インタフェースが Ethernet インタフェース(EWAN もしくは LAN)もしくは PPPoE 以外であった場合には、本設定は無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　優先度 7 で、802.1p Priority に対するマーキングを設定する

```
Router(config)#action-map stream-action
Router(action-map stream-action)# set 802.1p priority 7
```

コマンド書式

set 802.1p priority <優先度 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
優先度	Ethernet ヘッダ 802.1p Priority に対するマーキングの優先度を設定します。	0～7	省略不可

この設定を行わない場合

マーキングは行なわれません。

設定モード

アクションマップ設定モード

ポリシーマップの定義

class

クラスマップとアクションとを対応付け、クラシフィケーションされたトラフィックに対するアクションを定義します。
複数のクラスが定義された場合、クラスマップ名のアルファベット順に検索され、最初にマッチしたクラスに対するアクションのみが実行されます。
同一クラスマップ名に対しては、一つのアクションのみ記述できます(同一クラスマップ名に対しては、置換型となります)。

refresh コマンド後に有効になるコマンドです。

設定例１　クラスマップ（video-class）とアクションマップ（stream-action）を対応づける

```
Router(config)#policy-map stream-service
Router(policy-map stream-service)#
```

コマンド書式

class <class-map-name> action <action-map-name>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
class-map-name	class-map-name を設定します。	16 文字以内の文字列	省略不可
action-map-name	action-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

クラスマップとアクションとの対応は定義されません。

設定モード

ポリシーマップ設定モード

policy-map

policy-map モードに移行し、クラスマップによって分類したトラフィックに対して、どのような制御を行なうかを定義します。

refresh コマンド後に有効になるコマンドです。

設定例１　ポリシーマップ設定モードへ移行する

```
Router(config)#policy-map stream-service
Router(policy-map stream-service)#
```

コマンド書式

policy-map 〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	policy-map-name を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

ポリシーマップの設定を行うことができません。

設定モード

基本設定モード

statistics update

統計情報のカウントを行うかどうかを指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　統計情報のカウントを行う

```
Router(config)# policy-map stream-service
Router(config-policy-map)# statistics update enable
Router(config-policy-map)# exit
```

コマンド書式

statistics update 〈カウント設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
カウント設定	統計情報のカウントを行うかどうかを指定します。 enable：統計情報のカウントを行う disable：統計情報のカウントを行わない	enable disable	省略不可

この設定を行わない場合

統計情報のカウントを行いません。

設定モード

ポリシーマップ設定モード

ポリシーマップの適用とキューの定義

qos frame-length-offset

CBQ によって帯域制御が行なわれる場合、帯域計算で使用するフレーム長の補正値を指定します。
帯域計算は、適用するインタフェースごとに予め定められたフレーム構造を想定して行なわれますが、必ずしも現実と一致しない場合があるため、必要に応じて本コマンドによって補正を行ないます。
補正した結果が適用するインタフェースごとに予め定められた最小フレームサイズを下回った場合、最小フレームサイズが用いられます。最小フレームサイズについては、下記の「最小フレームサイズに関して」を参照して下さい。

refresh コマンド後に有効になるコマンドです。

設定例１　帯域計算で使用するフレーム長を 20 オフセットさせる

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos frame-length-offset increment 20
```

コマンド書式

qos frame-length-offset {increment<オフセット値> | decrement<オフセット値>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
increment	フレーム長を増加させる場合のオフセット値を設定します。	0～127	省略不可
decrement	フレーム長を減少させる場合のオフセット値を設定します。	0～128	省略不可

この設定を行わない場合

フレーム長補正は行ないません。

最小フレームサイズに関して

・IPsec-IF の場合
SIF 内部設定値 ＋ 最小フレーム長(64bytes) － FCS(4bytes)

・DIALER-IF の場合
DIALER 内部設定値

・上記以外の IF の場合
PIF 内部設定値 ＋ 最小フレーム長(64bytes) － FCS(4bytes)

インタフェースが PPP を利用する場合、PPP カプセル化処理の際にエスケープ処理が行なわれますが、帯域計算は PPP カプセル化前に行なわれるため、エスケープ処理の効果を正確に補正することはできません。
なお、PPPoE カプセル化ではエスケープ処理が行なわれないため、このような制限は発生しません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos output bandwidth

インタフェースで使用できる帯域および、QoS の方式を指定します。
帯域は、物理速度と同じ値を設定してください。
QoS 方式は、CBQ(Class-Based Queueing)／PRIQ(Priority Queueing)のどちらかを選択します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースの全帯域を 100Ｍｂｐｓとし、QoS の方式を CBQ とする

```
Router(config)#interface lan 1
Router(config-if lan 1)# qos output bandwidth 100M cbq
```

コマンド書式

qos output bandwidth 〈最大使用帯域〉〈QoS 設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
最大使用帯域	設定しているインタフェースで、全体の帯域幅(単位:bps)を設定します。 通常は、物理インタフェース速度を設定します。 kbps を示す場合は"K"、Mbps を示す場合は"M"が使用できます。 例)100kbps→"100K"、50Mbps→"50M"	範囲無し	省略不可
QoS 設定	QoS の方式を指定します。 cbq：CBQ(Class-Based Queueing)方式を指定します。 priq：PRIQ(Priority Queueing)方式を指定します。	cbq priq	省略不可

この設定を行わない場合

QoS 制御を行なわない(常にベストエフォート)。帯域幅は物理インタフェース速度。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos-que cbq

QoS 機能において、CBQ で使用するキューを定義します。
キュー名は、アクションマップにおいてキューを指定する際に参照されます。
Bandwidth で、qos bandwidth コマンドで指定した帯域の何パーセントをこのキューに割り当てるかを指定します。
borrow が指定されている場合に、親キューの帯域に余裕がある時は、その帯域を利用できることを示します。
Priority はキューからパケットを送信する際の優先度として参照され、7 が最高優先度、0 が最低優先度となります
キュー長は qlimit で指定され、あふれたパケットは廃棄されます。
red(Random EarlyDetection)が指定されている場合、TCP のパケット再送を意図し、あふれる以前の段階でランダムに廃棄が行なわれます。
default を指定すると、本キューがデフォルトキューであることを示し、action-map でキューが指定されなかったパケットがキューイングされます。
parent に"NULL"を指定すると ROOT queue を示すものとします。
delay が指定されている場合、エンキューされた時点から設定時間を超えてキューに溜まり続けたパケットは廃棄されます。
delay 指定がない場合は上記のような動作、時間でパケットを廃棄する動作は行われません。

refresh コマンド後に有効になるコマンドです。

設定例１　root-que の 10%を video-que の帯域として使用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos-que cbq video-que bandwidth 10
parent root-que
```

コマンド書式

qos-que cbq 〈キュー名〉 bandwidth 〈帯域使用率〉 parent 〈キュー名〉 [優先度][qlimit 〈キュー長〉] [delay 〈最大遅延時間〉] [borrow] [red] [default]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キュー名	CBQ のキュー名称を設定します。	16 文字以内の文字列	省略不可
帯域使用率	回線全帯域の帯域幅に対する帯域使用率(単位:%)を指定します。 IPsec インタフェースに対して帯域制御を行った場合は、送信時に EWAN 側の帯域制御も適用されます。IPsec インタフェース→EWAN の順に2段階に帯域制御されます。	1～100	省略不可
優先度	優先度を指定します。優先度が高いクラスは、優先度の低いクラスに比べ、送信処理の時間が増えます。	0～7	0

	この値が大きいほど、優先度は高くなります。		
最大遅延時間	このクラスの最大遅延時間(単位:μ 秒)を設定します。	1～999999	0
キュー長	キュー長を設定します。	1～200	50
borrow	帯域不足で送信できない場合に、親クラスに空きがあればその帯域を利用するかどうかを指定します。その帯域を利用する場合は、borrow を指定します。	borrow	親クラスの帯域を利用しない
red	キューバッファ管理方式に、RED(Random Early Detection)を使用する場合に、red を指定します。RED を使用しない場合は、キューバッファがいっぱいになってからパケットを破棄(Tail-Drop)しますが、RED を使用した場合は、キューあふれによる輻輳が発生する前にランダム破棄を開始するため、TCP のようなトラフィックを変動できるようなプロトコルでは、より早く破棄を感知できるので、通信全体でみると効率が良くなります。	red	RED を使用しない
default	デフォルトクラスの場合に指定します。デフォルトクラスは、ルートクラスに属している必要があります。	default	default 以外

この設定を行わない場合

キューは定義されません。
priority のデフォルトは 0、qlimit のデフォルトは 50。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
トンネルインタフェース設定モード

qos-que priq

QoS 機能において、PRIQ で使用するキューを定義します。
キュー名は、アクションマップにおいてキューを指定する際に参照されます。
Priority はキューからパケットを送信する際の優先度として参照され、7 が最高優先度、0 が最低優先度となります。
キュー長は qlimit で指定され、あふれたパケットは廃棄されます。RED（Random EarlyDetection）が指定されている場合、TCP のパケット再送を意図し、あふれる以前の段階でランダムに廃棄が行なわれます。
default を指定すると、本キューがデフォルトキューであることを示し、アクションマップでキューが指定されなかったパケットがキューイングされます。

refresh コマンド後に有効になるコマンドです。

設定例１　voice-que の優先度を 0、キュー長を 50 に設定する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# qos-que priq voice-que priority 0 qlimit 50
```

コマンド書式

qos-que priq 〈キュー名 〉 priority 〈優先度〉 [qlimit 〈キュー長〉] [default] [red]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キュー名	CBQ のキュー名称を設定します。	16 文字以内の文字列	省略不可
優先度	優先度を指定します。 優先度が高いキューにパケットがある間は、優先度の低いキューからパケットが送出されることはありません。この値が大きいほど、優先度は高くなります。	0～7	0
キュー長	キュー長を設定します。	1～200	50
red	キューバッファ管理方式に、RED（Random Early Detection）を使用する場合に、red を指定します。 RED を使用しない場合は、キューバッファがいっぱいになってからパケットを破棄（Tail-Drop）しますが、RED を使用した場合は、キューあふれによる輻輳が発生する前にランダム破棄を開始するため、TCP のようなトラフィックを変動できるようなプロトコルでは、より早く破棄を感知できるので、通信全体でみると効率が良くなります。	red	RED を使用しない
default	デフォルトクラスの場合に指定します。	default	default 以外

この設定を行わない場合

キューは定義されません。

設定モード

各インタフェース設定モード

service-policy

インタフェースの入出力パケットに対して、サービスポリシーを適用します。
サービスポリシーが未定義であったり、必要な定義が不足したりしている場合、エラーメッセージをelog に出力し、設定は適用されません。
インタフェースの出力パケットに対するサービスポリシーにおいては、以下のアクションは適用されず、無視されます。

refresh コマンド後に有効になるコマンドです。

設定例１　入力パケットに対して、ポリシーマップ名 pre-service を適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)# service-policy input pre-service
```

コマンド書式

service-policy〈入出力設定〉〈ポリシーマップ名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
入出力設定	入力側(input)、出力側(output)のどちらにサービスポリシーを適用するか設定します。	input output	省略不可
ポリシーマップ名	ポリシーマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

サービスポリシーは適用されません。

設定モード

各インタフェース設定モード

service-policy local

自局送信パケットに対して、サービスポリシーを適用します。
サービスポリシーが未定義であったり、必要な定義が不足したりしている場合、エラーメッセージを elog に出力し、設定は適用されません。

refresh コマンド後に有効になるコマンドです。

設定例１　自局送信パケットに対して、ポリシーマップ名 local-service を適用する。

```
Router(config)#service-policy local local-service
Router(config)#
```

コマンド書式

service-policy local〈ポリシーマップ名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポリシーマップ名	ポリシーマップ名を設定します	16 文字以内の文字列	省略不可

この設定を行わない場合

サービスポリシーは適用されません。

設定モード

基本設定モード

L2 QoS機能

L2 QoS機能

priority classification

L2 QoS を動作させる場合に指定します。
L2 QoS とは、受信データの 802.1p 値から、データを優先/非優先の判別を行い、送信時に優先データを優先的に制御する機能です。
送信制御を行う場合は、priority queuing コマンドの指定が必要です。
LAN インタフェースで動作させることが可能です。

refresh コマンド後に有効になるコマンドです。

設定例１　物理ポート２で L2 QoS 動作を行う

```
Router(config)#line lan 1
Router(config-line lan 1) priority 2 classification
```

コマンド書式

priority <port-number > classification

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
port-number	L2 QoS を動作させる物理ポート番号を指定します。	1～4	省略不可

この設定を行わない場合

優先制御をおこないません。

設定モード

Ethernet 設定モード

priority default-priority

受信したフレームが 802.1Q VLAN タグがついていなかった場合、802.1p 値をいくつで動作するかを指定します。
802.1p 値を変更することにより優先度を指定することができます。802.1p 値が大きいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例 1　ポート 2 からの受信フレームに 802.1Q VLAN タグが付いていなかった場合に、802.1p 値を 7 とする

```
Router(config)#line lan 1
Router(config-line lan 1)#priority 2 default-priority 7
```

コマンド書式

priority <port-number> default-priority <802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
port-number	指定したポート番号で 802.1p 値をいくつで動作させるかを指定します。	1～4	省略不可
802.1p 値	802.1Q VLAN タグがついていなかった場合の 802.1p 値を指定します。	0～7	省略不可

この設定を行わない場合

802.1p 値の変更を行いません。
802.1p 値は"0"として扱われます。

802.1p 値の優先度に関して

802.1p 値は、優先度を 0～7 で指定することができます。
802.1p のプライオリティレベルは、以下8段階に規定されています。

優先度	802.1p 値	プライオリティレベルの内容
高い ↑ ↑ ↑ ↑ ↓ ↓ ↓ ↓ 低い	7	予約
	6	会議型の音声
	5	会話型マルチメディア
	4	制御を必要とするアプリケーション
	3	クリティカルアプリケーション
	2	標準的なストリーム
	1	バックグラウンド
	0	ベストエフォート

設定モード

Ethernet 設定モード

priority queuing

L2 QoS の送信制御を行うポートを指定します。
送信時に、優先/非優先の判別を行い、優先データを優先的に送信します。
L2 QoS の送信制御を行う場合は、priority classification コマンドの登録も必要です。

refresh コマンド後に有効になるコマンドです。

設定例１　物理ポート２で L2 QoS の送信制御を行う

```
Router(config)#line lan 1
Router(config-line lan 1) priority 2 queuing
```

コマンド書式

priority <port-number> queuing

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
port-number	L2 QoS の送信制御を行うポートを指定します。	1～4	省略不可

この設定を行わない場合

L2 QoS の送信制御を行いません。

設定モード

Ethernet 設定モード

priority threshold

優先データとして動作するパケットを、802.1p 値で指定します。
802.1p 値が大きいほど優先度が高くなります。

refresh コマンド後に有効になるコマンドです。

設定例１　優先データとしてあつかうパケットを 802.1p 値 5 とする

```
Router(config)#line lan 1
Router(config-line lan 1) priority threshold 5
```

コマンド書式

priority threshold <802.1p 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
802.1p 値	優先データとして動作するパケットを、802.1p 値で指定します。 ここで指定した値以上の 802.1p 値を持つデータを優先データ、ここで指定した値未満の 802.1p 値を持つデータを非優先データとして扱います。 LAN インタフェースに送信する際に、送信キューの中に優先データが存在する場合は、非優先データは送信されません。	0～7	省略不可

この設定を行わない場合

802.1p 値は 4 として動作します。

802.1p 値の優先度に関して

802.1p 値は、優先度を 0～7 で指定することができます。
802.1p のプライオリティレベルは、以下8段階に規定されています。

優先度	802.1p 値	プライオリティレベルの内容
高い ↑ ↑ ↑ ↑ ↓ ↓ ↓ ↓ 低い	7	予約
	6	会議型の音声
	5	会話型マルチメディア
	4	制御を必要とするアプリケーション
	3	クリティカルアプリケーション
	2	標準的なストリーム
	1	バックグラウンド
	0	ベストエフォート

設定モード

Ethernet 設定モード(line lan モードのみ)

UPnP 機能

UPnP 機能

upnp-server access-group【F80/F100 コマンド】

UPnP 機能を利用可能な端末を、アクセスリスト番号で制限します。
permit となった端末のみ、UPnP 機能に対するアクセスやイベント受信が可能になります。
ただし、マルチキャストによるアナウンスメッセージは、本設定とは関係なく、パケット到達可能範囲の全端末が受信することができます。

refresh コマンド後に有効になるコマンドです。

設定例　アクセス番号 90 番の端末の UPnP 機能を制限する

```
Router(config)#upnp-server access-group 90
```

コマンド書式

upnp-server access-group <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	UPnP 機能の利用を制限する端末を指定します。	1～99(IPv4 標準アクセスリスト)	省略不可

この設定を行わない場合

UPnP 機能を利用する端末を制限しません。

設定モード

基本設定モード

upnp-server enable【F80/F100 コマンド】

UPnP 機能を使用する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例　UPnP 機能を使用する

```
Router(config)#upnp-server enable
```

コマンド書式

upnp-server enable

パラメータ

パラメータはありません

この設定を行わない場合

UPnP 機能を使用することができません。

設定モード

基本設定モード

upnp-server target-interface【F80/F100 コマンド】

UPnP 機能を使用するインタフェースを指定します。
UP しているインタフェースのうち、priority が最も小さいインタフェースを使用します。
ただし、同じ priority の場合には、config に表示される順となります。

refresh コマンド後に有効になるコマンドです。

設定例　PPPoE 1 を UPnP 機能を使用するインタフェースに指定する

```
Router(config)#upnp-server target-interface pppoe1
```

コマンド書式

upnp-server target-interface 〈インタフェース名〉 [〈priority〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	UPnP 機能を使用するインタフェースを指定します。	ewan 1～2 pppoe 1～24※1 dialer 1～20※2	省略不可
priority	UPnP 機能を使用するインタフェースの優先度を指定します。	0～100	50

※1:F80 の場合は、1～5 になります。
※2:F100 のみ指定可能です。

この設定を行わない場合

設定をしていないインタフェースで、UPnP 機能を使用できません。
全てのインタフェースを設定していない場合は、Connection サービスは down 状態とみなします。

設定モード

基本設定モード

BRIモジュール回線の選択

BRIモジュール回線の選択

leased-line【F100 専用コマンド】

BRI インターフェイスの動作モードを専用線にする場合に指定します。
本設定がない場合は ISDN モードで動作します。

設定例１　BRI インタフェースを HSD(128Kbps)として使用する

```
Router(config)#interface bri 1
Router(config-if bri 1) #leased-line 128
```

コマンド形式

```
leased-line {64|128}
no leased-line
```

パラメータ

パラメータはありません。

この設定を行わない場合

ISDN モードになります。

設定モード

BRI インタフェース設定モード(F100 のみ)

ダイヤルアップ機能

ダイヤルアップ機能

anonymous-call accept　【F100 専用コマンド】

発信者番号非通知の着信を受け付けるかどうかの設定をします。

refresh コマンド後に有効になるコマンドです。

設定例１　発信者番号非通知の着信を受け付ける

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#anonymous-call accept
```

コマンド形式

anonymous-call accept

パラメータ

パラメータはありません

この設定を行わない場合

dialer map、caller のいずれかに電話番号の設定がある場合は、発信者番号非通知の着信を拒否します。

設定モード

ダイヤルアップインタフェース設定モード

auto connect【F100 専用コマンド】

データ発生時に、ダイヤルアップ回線の自動発呼を行うかどうかの設定をします。

設定例１　自動発呼をおこなう

```
Router(config)#interface bri 1
Router(config-if bri 1)#auto connect on
```

コマンド形式

```
auto connect {on | off}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
on｜off	データ発生時に、自動的に接続する(on)か、接続しない(off)かを設定します	on off	省略不可

この設定を行わない場合

データ発生時に、ダイヤルアップ回線の自動接続を行います。

設定モード

BRI インタフェース設定モード(F100 のみ)

callback【F100 専用コマンド】

コールバックの設定をします。
コールバック先番号を ppp 通知、発信者番号通知、dialer に登録された番号のいずれかから選択します。
このコマンドが設定されると、コールバックしない接続はできなくなります。
また、MP 接続と併用することはできません。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

ただし、下記の状態の場合は、refresh コマンドを実行することができません。
・コールバック実行中
・発呼中
・着呼中
・切断中

設定例１　コールバック先番号を ppp 通知から選択する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#callback permit ppp
```

コマンド形式

```
callback {request {id | ppp | dialer} | permit {id | ppp | dialer}}
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
request {id | ppp | dialer}	コールバッククライアントとしての機能をパラメータから選択します。 ppp：CBCP コールバックを行います。 id：コールバック先番号を発信者番号通知で指定します。 dialer：CBCP のコールバックを行います。相手に番号を通知しません。	ppp id dialer	省略不可
permit {id | ppp | dialer}	コールバックサーバとしての機能をパラメータから選択します。 ppp：コールバック先番号を CBCP から取得します。 id：コールバック先番号を発信者番号通知で指定します。 dialer：コールバック先番号を dialer map に登録された番号から取得します。	ppp id dialer	省略不可

この設定を行わない場合

コールバック接続を行いません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

callback requestnumber【F100 専用コマンド】

コールバッククライアントにおいて、CBCP でコールバック先を指定する場合に設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　CBCP でコールバックする番号を 0312345678 に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#callback requestnumber 0312345678
```

コマンド形式

callback requestnumber <dial-string>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
dial-string	CBCP コールバックする電話番号を設定します。	10 桁以内の数字	省略不可

この設定を行わない場合

CBCP で番号を通知しません。

設定モード

BRI インタフェース設定モード(F100 のみ)

callback-responsetime【F100 専用コマンド】

コールバック要求を受けてから、コールバックを開始するまでの遅延時間を設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　コールバックを開始するまでの遅延時間を 10 秒に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#callback-responsetime 10
```

コマンド形式

callback-responsetime〈遅延時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
遅延時間	コールバックを開始するまでの時間(単位:秒)を設定します。	1～60	省略不可

この設定を行わない場合

コールバック要求の 10 秒後にコールバックします。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

callback-waittime【F100 専用コマンド】

コールバック要求を送信してから、サーバからコールバックされるまでの待ち時間を設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　コールバックされるまでの待ち時間を 12 秒に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#callback-waittime 12
```

コマンド形式

callback-waittime〈待機時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
待機時間	サーバからコールバックされるまでの待ち時間(単位:秒)を設定します。	1～60	省略不可

この設定を行わない場合

コールバックされるまでの待ち時間を 12 秒に設定します。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

called idle-timeout【F100 専用コマンド】

ダイヤルアップ接続(着信)で、ISDN 回線の無通信監視時間(秒)を設定します。
これにより、ダイヤルアップ接続後データ通信の無通信時間が設定時間を越えた際に ISDN 回線を切断します。

※データは送信・受信いずれも監視対象になります。

設定例１　無通信監視時間を 60 秒に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#called idle-timeout 60
```

コマンド形式

called idle-timeout {off | <1～3600>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
off｜<1～3600>	無通信監視時間を設定します。	off　無通信監視を行わない 1～3600	省略不可

この設定を行わない場合

着信時の無通信監視時間を 60 秒に設定します。

設定モード

BRI インタフェース設定モード(F100 のみ)

caller【F100 専用コマンド】

対向装置の電話番号を設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤルチェックする対向装置の電話番号を設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#caller 0398765432
```

コマンド形式

caller〈電話番号〉[〈サブアドレス〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
電話番号	対向装置の電話番号を設定します。	32 桁以内の数字	省略不可
サブアドレス	対向装置の電話番号のサブアドレスを設定します。	19 桁以内の数字	-

この設定を行わない場合

dialer map に番号の設定が無い場合は、発信による ISDN 回線を接続することはできません。
dialer map に番号が無い場合は、着信による接続のみ可能です。
また、発信時に発信者番号通知による相手の確認を行うことができません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

calling-number【F100 専用コマンド】

ダイヤルアップ接続で対向装置へ通知する自局の番号を設定します。
ただし間違った番号を登録した場合、網が契約者回線番号を通知します。
本設定は、着信する場合の契約者番号、ダイヤルインの設定もかねます。
サブアドレスを設定する場合は、*で区切って<dial-string>の中に記述してください。
契約者番号で着信する場合は、ダイヤル番号を特に記述せず、サブアドレスのみ記述します。

設定例１　契約者番号で着信するように設定する（サブアドレスなし）

```
Router(config)#interface bri 1
Router(config-if bri 1)# calling-number on
```

設定例２　契約者番号で着信するように設定する（サブアドレス付き）

```
Router(config)#interface bri 1
Router(config-if bri 1)# calling-number *1234
```

設定例３　ダイヤルインで着信するように設定する（サブアドレスなし）

```
Router(config)#interface bri 1
Router(config-if bri 1)# calling-number 0398765432
```

設定例４　ダイヤルインで着信するように設定する（サブアドレス付き）

```
Router(config)#interface bri 1
Router(config-if bri 1)# calling-number 0398765432 1234
Router(config-if bri 1)# calling-number 0398765432*1234
```

コマンド形式

calling-number {on | off | <dial-string> [*<subaddress>]}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
on｜off	自局の番号を通知するかどうかを設定します。	on　通知する off　通知しない	on
<dial-string> [*<subaddress>]	通知する自局の番号を設定します。	<dial-string>は 32 桁以内の数字 <subaddress>は 19 桁以内の数字	省略不可

この設定を行わない場合

自局の番号を通知します。

設定モード

BRI インタフェース設定モード(F100 のみ)

dialer flets【F100 専用コマンド】

ダイヤルアップ接続をフレッツ ISDN 用に設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤルアップ接続をフレッツ ISDN 用に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#dialer flets
```

コマンド形式

```
dialer flets
```

パラメータ

パラメータはありません。

この設定を行わない場合

フレッツ ISDN を利用することができません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

dialer interface【F100 専用コマンド】

ダイヤルアップ接続に使用するインタフェースを設定します。
本項目が設定されてないと、ダイヤルアップ接続は使用できません。
設定を削除して refresh した場合、該当する ISDN 回線が接続中の場合は強制切断します。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤルアップ接続に ISDN 回線を使用する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#dialer interface bri 1
```

コマンド形式

```
dialer interface bri 1
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
bri 1	ダイヤルアップ接続に使用するインタフェースを設定します。	bri 1	省略不可

この設定を行わない場合

ダイヤルアップ接続は、使用できません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

dialer map【F100 専用コマンド】

接続相手の IP アドレス、発呼先電話番号、対向を認証する場合の ID を設定します。
パスワードに関しては、username コマンドで設定します。
該当する ISDN 回線が接続中の場合は強制切断します。

refresh コマンド後に有効になるコマンドです。

設定例１　接続相手の IP アドレス、認証 ID、発呼先電話を設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#dialer map ip 10.1.1.1 name tokyo 0312345678
```

設定例２　接続相手から IP アドレスを割り当ててもらう場合の設定をする

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#dialer map name tokyo-ap 037777777
```

コマンド形式

```
dialer map [ip {<ip アドレス> | broadcast}] [name <username>] [<dial-string>
        [<subaddress>]]
```

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
ip {<ip アドレス> | broadcast}	接続相手の IP アドレスを設定します。	ip <ip アドレス>	IPv4 形式で設定します。	–
		ip broadcast	対向の IP アドレスを指定しません。	
name <username>	対向を認証する際の ID を設定します。	20 文字以内の文字列		–
<dial-string> [<subaddress>]	発呼先電話番号を設定します。	<dial-string>は 32 桁以内の数字 <subaddress>は 19 桁以内の数字		–

この設定を行わない場合

ダイヤルアップ接続を行いません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

forced disconnect time【F100 専用コマンド】

ダイヤルアップ接続時の強制切断タイマを設定します。
連続接続リミッタ値を設定するすることにより、設定値を超えた場合は接続を強制切断します。
設定値を超えた場合は、mail to コマンドを設定することにより電子メールで通知することもできます。
MP 接続している間は、倍にカウントされます。

refresh コマンド後に有効になるコマンドです。

※回線接続中に設定を変更して refresh した場合、タイマはそのまま保持されます。
また、強制切断のタイマが設定値を超えていた場合、接続は強制的に解除されます。

設定例１　連続接続リミッタ値を 600 分に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#forced disconnect time 600
```

コマンド形式

forced disconnect time {off | <60～1439>}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
off｜<60～1439>	ダイヤルアップ接続の強制切断タイマの設定。 off：強制切断を行いません。 60～1439：タイマ値を設定します。(単位:分)	off 60～1439	省略不可

この設定を行わない場合

連続接続時間が 600 分を超えた場合に、ダイヤルアップ接続を強制切断します。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ip address【F100 専用コマンド】

自装置の ISDN ポート側の IP アドレスを設定します。
接続相手先からアドレスを割り振ってもらう場合は「negotiated」を指定します。
refresh コマンド後に有効になるコマンドです。該当する ISDN 回線が接続中の場合は強制切断します。
また、ルート情報も変更します。

refresh コマンド後に有効になるコマンドです。

設定例１　IP アドレスを 10.1.1.1、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip address 10.1.1.1 255.255.255.0
```

コマンド書式

ip address {negotiated | <IP アドレス> <サブネットマスク>}

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
negotiated	<IP アドレス> <サブネットマスク>	ダイヤルアップ接続で使用する ISDN ポート側の IP アドレスを設定します。	negotiated	接続相手から IP アドレスを割り振ってもらう場合	省略不可
		<IP アドレス> <サブネットマスク>	IPv4 アドレス形式で設定する場合。	

この設定を行わない場合

ISDN 回線を使用したダイヤルアップ接続を行うことができません。
設定を行わない場合は、ip address negotiated として機能します。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ip access-group【F100 専用コマンド】

access-list コマンドで指定したフィルタリングデータを、dialer インタフェースで適用します。
フィルタリングデータは、dialer インタフェースで受信したパケットに適用するのか／dialer インタフェースに送信するパケットに適用するのかを指定する必要があります。

設定例１　access-list 1 で指定したデータを、dialer1 送信時に適用する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip access-group 1out
```

設定例２　access-list 2 で指定したデータを、dialer1 からの受信時に適用する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn] | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	<1-99> <100-199> <1300-1999> <2000-2699>	省略不可
{ in [interface | vpn] | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。 in: access-list に従い制御 in vpn: 自局宛 VPN 対象パケットを制御 in interface: 自局宛非 VPN 対象パケットを制御	in:受信時 out:送信時	省略不可

この設定を行わない場合

設定している dialer インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ip nat inside destination

そのインタフェースで受信するパケットの宛先アドレスの変換ルールを設定します。
合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスから<ローカルアドレス・サブネットマスク>で指定したローカルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（スタティック登録）158.xxx.xxx.2 宛で受信したら 192.168.0.1 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1
```

【解説】
ip nat inside destination static <グローバル側アドレス> <ローカル側アドレス>となります。
これ以外のパケットを NAT 変換したい場合は、ip nat inside source コマンドを使用して、設定します。

設定例２　NAT+変換（スタティック登録）158.xxx.xxx.2:ポート番号 1500 で受信したら、192.168.0.1:ポート番号 80 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside destination static
158.202.232.1 1500 192.168.0.1 80
```

【解説】
ip nat inside destination static <グローバル側アドレスグローバル側ポート番号> <ローカル側アドレスローカル側ポート番号>となります。
これ以外のパケットを NAT+変換したい場合は、ip nat inside source コマンドを使用して、設定します。

設定例３　NAT 変換（一括変換）158.xxx.xxx.xxx.0/24⇔192.168.100.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside destination static-subnet
158.xxx.xxx.xxx.0 192.168.100.0 255.255.255.0
```

【解説】
ip nat inside destination static-subnet <グローバルサブネット> <ローカルサブネット> <サブネットマスク>となります。
グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。
NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合
192.168.100.0 ⇔ 158.xxx.xxx.0

192.168.100.1 ⇔ 158.xxx.xxx.1
: :
192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT スタティック（複数指定）時】
ip nat inside destination list 〈access-list 番号〉[開始ポート番号 [終了ポート番号]] pool 〈プール名〉[ポート番号]
【NAT スタティック（1 対 1 変換）、NAT+スタティック時】
ip nat inside destination static 〈グローバルアドレス〉[開始ポート番号 [終了ポート番号]]〈ローカルアドレス〉[ポート番号]
【NAT スタティック（一括変換）】
ip nat inside destination static-subnet 〈グローバルサブネット〉〈ローカルサブネット〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前(グローバルアドレス)範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
グローバルアドレス	変換前のグローバルアドレスを指定します。	IPv4 アドレス形式	省略不可
開始ポート番号 終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	ポート変換しない
プール名	変換後(ローカルアドレス)範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	省略不可
ローカルアドレス	変換後のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
ポート番号	変換後の TCP/UDP ポート番号を指定します。	1～65535	ポート変換しない
グローバルサブネット	変換前のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換後のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 512 エントリ、リスト 64 エントリ

この設定を行わない場合

設定しているグローバル側インタフェースでは、NAT スタティック／NAT+スタティック機能を使用することはできません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）

ip nat inside source

そのインタフェースから送信するパケットの送信元アドレスの変換ルールを設定します。
NAT モードの場合と、NAT+モード(IP マスカレード)の場合で、設定のしかたが異なりますので注意してください。
パラメータ"static-subnet"を指定することにより、NAT の変換ルールを、ネットワーク単位で指定することもできます。<ローカルアドレス・サブネットマスク>で指定したローカルアドレスから<グローバルアドレス・サブネットマスク>で指定したグローバルアドレスへの変換を、<サブネットマスク>で指定した単位で一括設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　NAT 変換（192.168.0.0/24　→　158.xxx.xxx.2～158.xxx.xxx.7）

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source list 1 pool
pool1


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
←list 1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.2 158.xxx.xxx.7
← pool1 の部分の設定
```

【解説】

ip nat inside source <ローカル側のアドレス範囲> <グローバル側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<グローバル側のアドレス範囲>は、ip nat pool <pool 名>コマンドで指定します。

設定例２　NAT+変換（192.168.0.0/24　→　インタフェースアドレス）

```
Router(config)#interface ewan 1
Router(config-if lan 1)#ip nat inside source list 1 interface


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
←list 1 の部分の設定
```

【解説】

ip nat inside source <ローカル側のアドレス範囲> <グローバル側のアドレス範囲>となります。
<LAN 側のアドレス範囲>は、access-list コマンドで指定します。
<グローバル側のアドレス範囲>は、インタフェースアドレスに集約しますので、"interface"と指定します。

設定例３　NAT 変換（スタティック登録）設定例１の中で 192.168.0.1⇔158.xxx.xxx.2 のみ固定変換

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source static 192.168.0.1
158.xxx.xxx.2
Router(config-if lan 1)#ip nat inside source list 1 pool pool1
Router(config-if lan 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1 □


Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255 ←list
1 の部分の設定
Router(config)#ip nat pool pool1 158.xxx.xxx.3 158.xxx.xxx.7 ←
pool1 の部分の設定
```

【解説】

設定例1とほぼ同じです。

違う点は、ip nat inside source static で、NAT スタティック変換をしている箇所ですが、この場合も、ip nat inside source <ローカル側のアドレス> <グローバル側のアドレス>となります。

この場合、ip nat inside destination コマンドを使用して、グローバル側→ローカル側のスタティック登録を行なう必要があります。(①の部分)

設定例４　NAT 変換（一括変換）192.168.100.0/24←→158.ｘｘｘ.ｘｘｘ.0/24 に変換する

```
Router(config)#interface lan 1
Router(config-if lan 1)#ip nat inside source static-subnet
192.168.100.0 158.xxx.xxx.0 255.255.255.0
```

【解説】

ip nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>となります。

グローバル IP アドレスとプライベート IP アドレスの変換の組み合わせをスタティックに決める設定を行います。

NAT スタティックを複数行なう場合には、マスクを指定し、1 つのエントリで指定することができます(複数同時登録)。

例)local=192.168.100.0 global=158.xxx.xxx.0,255.255.255.0 と指定した場合

192.168.100.0 ⇔ 158.xxx.xxx.0

192.168.100.1 ⇔ 158.xxx.xxx.1

：：

192.168.100.255 ⇔ 158.xxx.xxx.255

コマンド書式

【NAT 時】

ip nat inside source list <access-list 番号> [変換前開始ポート番号 [変換前終了ポート番号]] pool <プール名> [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【NAT+時】

ip nat inside source list <access-list 番号> [開始ポート番号 [終了ポート番号]] interface [overload | [変換後開始ポート番号 [変換後終了ポート番号]]]

【スタティック変換】

ip nat inside source static <ローカルアドレス> <グローバルアドレス>

【NAT スタティック（一括変換）】

ip nat inside source static-subnet <ローカルサブネット> <グローバルサブネット> <サブネットマスク>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	変換前(ローカルアドレス)範囲を指定したアクセスリストを指定します。	1～99 1300～1399	省略不可
変換前開始ポート番号 変換前終了ポート番号	変換前の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
プール名	変換後(グローバルアドレス)範囲を指定した NAT プール名を指定します。	16 文字以内の文字列	NAT の場合は省略不可
interface	インタフェースのアドレスに NAT+変換します。	interface	NAT+の場合は省略不可
overload	ポート変換する場合に指定	overload	ポート変換しない
変換後開始ポート番号 変換後終了ポート番号	変換後の TCP/UDP ポート番号(範囲)を指定します。	1～65535	自動ポート変換
ローカルアドレス	変換前のローカルアドレスを指定します。	IPv4 アドレス形式	省略不可
グローバルアドレス	変換後のグローバルアドレスを指定します。	IPv4 アドレス形式	省略不可
ローカルサブネット	変換前のローカルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
グローバルサブネット	変換後のグローバルアドレスを指定します。 ※static-subnet を指定した場合は、host 部に 1 を指定しないでください。	IPv4 アドレス形式	省略不可
サブネットマスク	変換をサブネットマスクで指定した単位で一括設定します。	IPv4 アドレス形式	省略不可

最大エントリ：スタティック 512 エントリ、リスト 128 エントリ

この設定を行わない場合

設定しているローカル側インタフェースでは、NAT／NAT+機能を使用することはできません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード（F100 のみ）

lcp maxtimes【F100 専用コマンド】

LCP の再送回数の設定をします。

設定例１　LCP の再送回数を 5 回に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#lcp maxtimes 5
```

コマンド形式

lcp maxtimes〈再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送回数	LCP の再送回数を設定します。	0～255	省略不可

この設定を行わない場合

LCP の再送回数を 10 回に設定します。

設定モード

BRI インタフェース設定モード(F100 のみ)

lcp restart【F100 専用コマンド】

LCP のリスタート時間(10msec)の設定をします。

設定例１　LCP のリスタート時間を 1000msec に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#lcp restart 100
```

コマンド形式

lcp restart <リスタート時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リスタート時間	LCP のリスタート時間を設定します。	100～6000	省略不可

この設定を行わない場合

LCP のリスタート時間を 1000msec に設定します。

設定モード

BRI インタフェース設定モード(F100 のみ)

max-call【F100 専用コマンド】

ダイヤルアップ接続でリミッタが動作する1時間あたりの接続回数の設定をします。
設定値を超えた場合は、mail to コマンドを設定することにより電子メールで通知することもできます。
設定を変更して refresh した場合、リミッタが動作していれば解除し、カウンタもゼロクリアされます。

refresh コマンド後に有効になるコマンドです。

設定例１　リミッタが動作する１時間あたりの接続回数を 100 回に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#max-call 100
```

コマンド形式

max-call〈リミッタが動作する回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リミッタが動作する回数	ダイヤルアップ接続でリミッタが動作する、1時間あたりの接続回数を設定をします。 off を指定すると、接続回数の監視を行いません。	1～1000 off	省略不可

この設定を行わない場合

ダイヤルアップ接続でリミッタが動作する1時間あたりの接続回数を 40 回に制限します。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ppp authentication【F100 専用コマンド】

ダイヤルアップ接続で着信時の認証をする/しないの設定をします。また、認証する場合の認証方法を設定します。ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤルアップ接続の認証方法を chap に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ppp authentication chap
```

コマンド形式

ppp authentication〈認証方式〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
認証方式	ダイヤルアップ着信時の認証する/しないの設定を行います。また、認証する場合の方法を設定します。 pap：pap 方式で認証します chap：chap 方式で認証します off：認証しません	pap chap off	省略不可

この設定を行わない場合

ダイヤルアップの着信認証を行いません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ppp bap holdtime【F100 専用コマンド】

MP 接続状態に移行してから、このコマンドで指定した時間は回線の使用率にかかわらず、MP 接続状態を維持します。
設定時間の単位は秒(秒刻みでのみ可能)です。秒未満での単位は切り捨てになります。

設定例 1　MP 接続に移行してから、60 秒間 MP 接続状態を維持する

```
Router(config)#interface bri 1
Router(config-if bri 1)#ppp bap holdtime 60
```

コマンド形式

ppp bap holdtime <MP 接続維持時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
MP 接続維持時間	MP 接続状態に移行してから、指定した時間は回線使用率にかかわらずに MP 接続を維持します。	10～2550	省略不可

この設定を行わない場合

MP 接続状態に移行してから回線使用率にかかわらず 150 秒間は、MP 接続を維持します。

設定モード

BRI インタフェース設定モード(F100 のみ)

ppp bap threshold【F100 専用コマンド】

MP 接続時の負荷分散条件の設定します。
ppp bap threshold 0 0 で発呼時には、常に 2b 使用することができます。ただし、この設定でも 1b だけで着信した場合は、自分からは 2 本目を発呼することはできません。

設定例１　回線仕様率が 90%を超えた場合 MP 接続開始、60%未満で MP 接続停止する

```
Router(config)#interface bri 1
Router(config-if bri 1)#ppp bap threshold 90 60
```

コマンド形式

ppp bap threshold <負荷分散条件>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
負荷分散条件	MP 接続時の負荷分散条件を設定します。MP 接続を開始する使用率、MP 接続を停止する使用率の順で設定します。	0～90	省略不可

この設定を行わない場合

回線使用率 90%で MP 接続開始、回線使用率 60%で MP 接続を停止します。

設定モード

BRI インタフェース設定モード(F100 のみ)

ppp hostname【F100 専用コマンド】

ダイヤルアップ接続でインタフェースに bri を選択した場合に、接続相手に送信する自分の認証用ユーザ名、パスワードを設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　接続相手に送信する、認証用ユーザ名、パスワードを設定する

```
Router(config)#ppp hostname tokyo password eigyou
```

コマンド形式

ppp hostname <hostname> password <password> [{secret | private}[encrypted]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
hostname	ダイヤルアップ接続相手送信する、自分の認識ユーザ名を設定します。	127 文字以内の文字列	省略不可
password	ダイヤルアップ接続相手送信する、自分の認識パスワードを設定します。	32 文字以内の文字列	省略不可
secret | private	パスワードを暗号化する際に共有暗号鍵を使用するか、装置固有暗号鍵を使用するかを指定します。※1 secret：暗号化する際に共有暗号鍵を使用する private：暗号化する際に装置固有暗号鍵を使用する	secret private	パスワードを暗号化しません
encrypted	パスワードを暗号化処理するかどうかを設定します。このオプションを付加することにより、パスワードは暗号化済みと判定されます。※2 secret または、private と組み合わせて使用するため、secret、private の指定が無い場合は、encrypted を指定することは出来ません。	encrypted	パスワードを暗号化データとして扱いません

※1:このオプションは、設定するとすぐに有効となり、パスワードが暗号化されて表示され encrypted オプションが自動的に付加されます。
※2:パスワードが既に暗号化済みの場合は、このオプションを指定する必要があります。

この設定を行わない場合

接続相手に、認識ユーザ ID、パスワードを送信しません。

設定モード

基本設定モード

ppp multilink【F100 専用コマンド】

ISDN 回線を 1b のみ使用するか、MP 接続するかを指定します。
MP 接続で接続認証を行う場合は、ppp authentication で認証方式を必ず pap に設定してください。

※MP 接続とコールバック機能を併用することはできません。

設定例１　ISDN 回線 MP 接続で使用する

```
Router(config)#interface bri 1
Router(config-if bri 1)#ppp multilink
```

コマンド形式

ppp multilink

パラメータ

パラメータはありません。

この設定を行わない場合

MP 接続をおこないません。

設定モード

BRI インタフェース設定モード(F100 のみ)

recvidletimer【F100 専用コマンド】

called idle-timeout コマンドで、ダイヤルアップ接続(着信)の、ISDN 回線の無通信監視時間(秒)を設定した際に、無通信監視対象として、ISDN 側からの受信パケットを除く場合に設定します。

設定例１　ISDN 側からの受信パケットを無通信監視対象から外す

```
Router(config)#interface bri 1
Router(config-if bri 1)# recvidletimer on
```

コマンド形式

recvidletimer on

パラメータ

パラメータはありません。

この設定を行わない場合

ISDN 側からの受信パケットも無通信監視対象とします。

設定モード

BRI インタフェース設定モード(F100 のみ)

username【F100 専用コマンド】

ダイヤルアップ接続でインタフェースに bri を選択した場合に、接続相手を認証する際に使用する認証用ユーザ名、パスワードを設定します。
ISDN 回線が接続状態の時に設定を変更し refresh した場合、接続状態は保持されます。

refresh コマンド後に有効になるコマンドです。

設定例１　接続相手を認証する際に使用する、認証用ユーザ名、パスワードを設定する

```
Router(config)# username osaka password shiten
```

コマンド形式

username <username> password <password>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
username	ダイヤルアップ接続で接続相手を認証する際に使用する認証ユーザ名を設定します。	20 文字以内の文字列	省略不可
password	ダイヤルアップ接続で接続相手を認証する際に使用するパスワードを設定します。	32 文字以内の文字列	省略不可

最大エントリ数:20 エントリ

この設定を行わない場合

ダイヤルアップ接続で接続相手認証を行いません。

設定モード

基本設定モード

HSDに関する機能

HSDに関する機能

ip address【F100 専用コマンド】

自装置の HSD インタフェースの IP アドレスを設定します。
unnumberd インタフェースとする場合は、LAN のアドレスと同じ値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　IP アドレスを 10.1.1.1、サブネットマスクを 255.255.255.0 に設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip address 10.1.1.1 255.255.255.0
```

設定例 2　unnumbered インタフェースとする（LAN 側 IP アドレス：192.168.0.1/24）

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip address 192.168.0.1 255.255.255.0
```

コマンド書式

ip address {negotiated | <IP アドレス> <サブネットマスク>}

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
negotiated | <IP アドレス> <サブネットマスク>	HSD インタフェースの IP アドレスを設定します。		negotiated IPv4 アドレス形式	省略不可
	negotiated	接続相手から IP アドレスを割り振ってもらう場合		
	<IP アドレス> <サブネットマスク>	IPv4 アドレス形式で設定する場合。		

この設定を行わない場合

HSD を使用したルーティングを行うことができません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

ip access-group【F100 専用コマンド】

access-list コマンドで指定したフィルタリングデータを、dialer インタフェースで適用します。
フィルタリングデータは、dialer インタフェースで受信したパケットに適用するのか／dialer インタフェースに送信するパケットに適用するのかを指定する必要があります。

設定例１　access-list 1 で指定したデータを、dialer1 送信時に適用する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip access-group 1out
```

設定例２　access-list 2 で指定したデータを、dialer1 からの受信時に適用する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in [interface | vpn] | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	<1-99> <100-199> <1300-1999> <2000-2699>	省略不可
{ in [interface | vpn] | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。 in: access-list に従い制御 in vpn: 自局宛 VPN 対象パケットを制御 in interface: 自局宛非 VPN 対象パケットを制御	in:受信時 out:送信時	省略不可

この設定を行わない場合

設定している dialer インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

lcp keepalive【F100 専用コマンド】

HSD 回線使用時に、相手ルータの状況を確認するために、LCP Echo による KeepAlive を行う場合に指定します。KeepAlive を行わない場合、相手ルータが電源断等により生存しなくなった場合に、本装置が相手ルータがいなくなったことを判別できないため、HSD にデータを送信しつづけてしまいます。

HSD の障害時には、別経路にて迂回するようなシステムを構築する場合は、この設定を行ってください。

refresh コマンド後に有効になるコマンドです。

設定例１　LCP Echo による KeepAlive を行う

```
Router(config)#interface dialer 1
Router(config-if dialer 1)# lcp keepalive
```

コマンド形式

lcp keepalive〈送信間隔〉retry〈再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信間隔	LCP Echo フレームの送信間隔(単位:秒)を指定します	10～120	60 秒間隔
再送回数	LCP Echo の応答がない場合に行う再送の回数を指定します。ここで指定した回数応答がなかった場合は、相手ルータの異常と判断し、HSD インタフェースを使用不可とします。	0～10	2 回

この設定を行わない場合

LCP Echo による KeepAlive を行いません。

設定モード

ダイヤルアップインタフェース設定モード(F100 のみ)

lcp maxtimes【F100 専用コマンド】

LCP の再送回数の設定をします。

設定例１　LCP の再送回数を 5 回に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#lcp maxtimes 5
```

コマンド形式

lcp maxtimes〈再送回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
再送回数	LCP の再送回数を設定します。	0～255	省略不可

この設定を行わない場合

LCP の再送回数を 10 回に設定します。

設定モード

BRI インタフェース設定モード(F100 のみ)

lcp restart【F100 専用コマンド】

LCP のリスタート時間(10msec)の設定をします。

設定例１　LCP のリスタート時間を 1000msec に設定する

```
Router(config)#interface bri 1
Router(config-if bri 1)#lcp restart 100
```

コマンド形式

lcp restart <リスタート時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リスタート時間	LCP のリスタート時間を設定します。	100～6000	省略不可

この設定を行わない場合

LCP のリスタート時間を 1000msec に設定します。

設定モード

BRI インタフェース設定モード(F100 のみ)

障害監視／通知機能

SNMPエージェント機能

snmp-server community

SNMP マネージャとして登録したホスト以外からの GET/SET リクエストに対する処理方法を指定します。このコマンドでは、以下の指定を行なうことができます。

・コミュニティ名
・GET/SET リクエストに対する処理（GET のみに応答:ro／GET/SET に応答:rw）
・アクセスを許可するホストの指定

SNMP マネージャを登録する場合は snmp-server host コマンドを使用します。

設定例１　コミュニティ名を"public"に設定する

```
Router(config)# snmp-server community public
```

設定例２　コミュニティ名を"public"に設定し、Read-Only とする（SET リクエストには応答しない）

```
Router(config)# snmp-server community public ro
```

設定例３　コミュニティ名を"public"／Read-Only に設定し、アクセスを許可するホストは access-list 番号１に従う

```
Router(config)# snmp-server community public ro 1
```

コマンド書式

snmp-server community <コミュニティ名> [ro | rw] <access-list 番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
コミュニティ名	SNMP の通信を行なう際のコミュニティ名	32 文字以内の文字列	省略不可
ro| rw	Read Only(ro)もしくは Read/Write(rw)を指定する。	ro rw	ro
access-list 番号	アクセスを許可するホストを指定するために指定するアクセスリスト番号 IPv4 アドレス: 1～99 IPv6 アドレス: 3000～3499	1～99 3000～3499	全ホストからの SNMP アクセス可能

最大エントリ数:5 エントリ

この設定を行わない場合

snmp-server host コマンドで指定した SNMP マネージャ以外のホストからの SNMP には応答しません。

設定モード

基本設定モード

snmp-server enable traps

送信する SNMP トラップの種類を指定します。
SNMP マネージャ毎に異なる種類のトラップを送信したい場合は、snmp-server host コマンドで、送信するトラップを指定します。

設定例１　標準トラップのみ送信する

```
Router(config)# snmp-server enable traps snmp
```

コマンド書式

snmp-server enable traps［トラップの種類］

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
トラップの種類	送信するトラップの種類を指定します。 snmp：標準トラップを送信します。 config：拡張とラップを送信します。 event：イベントトラップを送信します	snmp config event	全てのトラップを送信します。

この設定を行わない場合

トラップを送信できません。

設定モード

基本設定モード

snmp-server host

SNMP マネージャを登録します。SNMP サーバの登録では、
・SNMP サーバの IP アドレス
・コミュニティ名
・SNMP のバージョン(V1 or V2c)
・送信するトラップの種類
を指定します。
SNMP マネージャは、8 件まで登録することができます。

設定例１　SNMP サーバ（IP アドレス=10.0.0.1、コミュニティ名：public、SNMP バージョン V2c、標準トラップのみ通知）を登録する

```
Router(config)#snmp-server host 10.0.0.1 public v2c snmp
```

コマンド書式

snmp-server host〈マネージャの IP アドレス〉〈コミュニティ名〉[v1 | v2c]〈トラップの種類〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
マネージャの IP アドレス	SNMP マネージャの IP アドレスを指定	IPv4 アドレス形式	省略不可
コミュニティ名	SNMP の通信を行なう際のコミュニティ名	32 文字以内の文字列	省略不可
v1 | v2c	SNMP のバージョンを指定	v1:SNMPv1 v2c:SNMPv2 (Community Based)	SNMPv1
トラップの種類	送信するトラップの種類を指定します。 snmp 標準トラップを送信します。 config 拡張トラップを送信します。 event イベントトラップを送信します	snmp config event	snmp-server enable traps の設定に従う

最大エントリ数:8 エントリ

この設定を行わない場合

GET/SET は、snmp-server community の設定に従います。
トラップを送信することはできません。

設定モード

基本設定モード

snmp-server source-interface

SNMP のトラップを送出する際の送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例１　SNMP のトラップを送出する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#snmp-server source-interface lan 1
```

コマンド書式

snmp-server source-interface〈インタフェース名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	SNMP のトラップを送出する際の送信元 IP アドレスとして使用するインタフェースアドレスを指定します。	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

SNMP のトラップを実際に送信するインタフェースの IP アドレスになります。

設定モード

基本設定モード

snmp-server name

この装置の名称を設定します。
通知されたテキストは、system グループの sysName に設定されます。装置の名称は 32 文字までです。

設定例１　この装置の名前を"FITELnet-F100#1"に設定する

```
Router(config)# snmp-server name FITELnet-F100#1
```

コマンド書式

snmp-server name〈装置の名前指定 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
装置の名前指定	この装置の名称を指定します。	32 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

snmp-server contact

この装置の管理者を設定します。
通知されたテキストは、system グループの sysContact に設定されます。管理者名は 32 文字までです。

設定例１　この装置の管理者を"root@fitelnet-f100"に設定する

```
Router(config)# snmp-server contact root@fitelnet-f100
```

コマンド書式

snmp-server contact〈管理者名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
管理者名	この装置の管理者を指定します。	32 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

snmp-server location

この装置の設置場所を設定します。
通知されたテキストは、system グループの sysLocation に設定されます。設置場所名は 64 文字までです。

設定例１　設置場所を"Honsha（本社）"に設定する

```
Router(config)# snmp-server location Honsha
```

コマンド書式

snmp-server contact〈設置場所名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
設置場所指定	この装置の設置場所を指定します。	64 文字以内の文字列	省略不可

この設定を行わない場合

指定なしになります。

設定モード

基本設定モード

SYSLOGDへの障害通知機能

logging-level elog

elog を syslog で送信する際の、ログ出力レベルを設定します。
elog を syslog で送信したい場合は、本コマンドで、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　elog の出力レベルを 3（ERR）とする

```
Router (config)# logging-level elog 3
```

コマンド書式

logging-level elog <出力レベル値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	elog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7	省略不可

この設定を行わない場合

elog をレベル4(WARNING)で出力します。

出力エラーレベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下8段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった(ぐらい緊急度が高い)
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnetーF シリーズの elog とは？

本装置で発生している中／軽度のエラー情報のメッセージです。
このメッセージが発生した場合は、本装置を含むネットワーク環境をご確認ください。
コンソールもしくは TELNET でログインして、elog の情報を表示する場合は、show elog コマンドを使用します。

設定モード

基本設定モード

logging-level slog

slog を syslog で送信する際の、ログ出力レベルを設定します。
slog を syslog で送信したい場合は、本コマンドで、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　slog の出力レベルを 4(WARNING)とする

```
Router(config)# logging-level slog 4
```

コマンド書式

logging-level slog 〈出力レベル値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	slog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7	省略不可

この設定を行わない場合

slog をレベル5(NOTICE)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下8段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった(ぐらい緊急度が高い)
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnetーF シリーズの slog とは？

本装置の slog では、本装置に TELNET や FTP でアクセスがあった場合の情報や、インタフェースの UP/DOWN 情報等のメッセージです。
コンソールもしくは TELNET でログインして、slog の情報を表示する場合は、show slog コマンドを使用します。

設定モード

基本設定モード

logging-level flog

flog を syslog で送信する際の、ログ出力レベルを設定します。
flog を syslog で送信したい場合は、本コマンドで、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　flog の出力レベルを 3（ERR）とする

```
Router (config)# logging-level flog 3
```

コマンド書式

logging-level flog 〈出力レベル値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	flog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7	省略不可

この設定を行わない場合

flog を syslog で送信しません。

出力エラーレベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下8段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnetーF シリーズの flog とは？

本装置で、log オプション付きのアクセスリスト（dynamic 設定のものは除く）でフィルタリング対象となったパケットをロギング（Filtering Log）することができます。

設定モード

基本設定モード

logging-level tlog

tlog を syslog で送信する際の、ログ出力レベルを設定します。
tlog を syslog で送信したい場合は、本コマンドで、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　tlog の出力レベルを 2（CRIT）とする

```
Router(config)# logging-level tlog 2
```

コマンド書式

logging-level tlog 〈出力レベル値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	tlog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7	省略不可

この設定を行わない場合

tlog をレベル3(ERR)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下8段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった(ぐらい緊急度が高い)
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnet-F シリーズの tlog とは？

本装置で発生している重度のエラー情報のメッセージです。
このメッセージが発生した場合は、本装置を含むネットワーク環境をご確認ください。また、必要があれば、本装置を再起動する等の処置をしてください。
コンソールもしくは TELNET でログインして、tlog の情報を表示する場合は、show tlog コマンドを使用します。

設定モード

基本設定モード

logging-level vpnlog

vpnlog を syslog で送信する際の、ログ出力レベルを設定します。
vpnlog を syslog で送信したい場合は、本コマンドで、syslog level コマンドで指定したレベル以上のレベル値を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　vpnlog の出力レベルを 5（NOTICE）とする

```
Router(config)# logging-level vpnlog 5
```

コマンド書式

logging-level vpnlog 〈出力レベル値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
出力レベル値	vpnlog の出力レベル値を設定します。 また、none を指定すると elog を送信しません。	0～7	省略不可

この設定を行わない場合

vpnlog をレベル6(INFO)で出力します。

出力レベルとは？

syslog のメッセージでは、レベルという領域が規定されています。
通常は、メッセージを受信した管理者が、どのような緊急性のあるメッセージなのかを把握するために利用します。
syslog のレベルは、プロトコルにより以下8段階に規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった（ぐらい緊急度が高い）
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnet-F シリーズの vpnlog とは？

本装置の IPsec 機能に関するログです。
SA を確立できなかった場合の原因究明や、改ざん・なりすまし等を検知した場合に、ログを発行します。SA の確立／解放を vpnlog に残す場合は、vpnlog enable コマンドを設定します。
コンソールもしくは TELNET でログインして、vpnlog の情報を表示する場合は、show vpnlog コマンドを使用します。

設定モード

基本設定モード

syslog sending

syslog サーバにログ情報を送信するかどうかを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG サーバにログ情報を通知する

```
Router(config)# syslog sending
```

コマンド書式

syslog sending

パラメータ

パラメータはありません。

この設定を行わない場合

ログ情報を、syslog サーバに送信しません。

設定モード

基本設定モード

syslog level

ログ情報を syslog で通知する際の出力制限レベル(0～7)を設定します。
ここで設定したレベル値以上の緊急度をもつレベルのログ情報を syslog サーバに通知します。

refresh コマンド後に有効になるコマンドです。

設定例１　Debug(7) レベル以上の緊急度をもつログ情報を SYSLOG で通知する

```
Router (config)# syslog level 7
```

コマンド書式

syslog level〈レベル番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
レベル番号	syslog で通知する際の出力制限ラベル値。	0～7	省略不可

この設定を行わない場合

レベル番号 7 になります。

SYSLOG のレベルとは？

syslog のレベルとは、ログメッセージの緊急度を表します。
RFC3164 では、以下のように規定されています。

レベル名	レベル番号	メッセージの内容・緊急度
EMERG	0	システムが利用できなくなった(ぐらい緊急度が高い)
ALERT	1	早急に対応しなくてはならない
CRIT	2	緊急状態
ERR	3	エラー発生状態
WARNING	4	注意が必要
NOTICE	5	お知らせ程度
INFO	6	情報
DEBUG	7	デバッグメッセージ

FITELnet-F シリーズのレベル値設定

本装置では、各種ログ（elog/slog/tlog/vpnlog）毎にレベル値を設定します。
各種ログのレベル値の設定は、logging level コマンドで行ないます。

設定モード

基本設定モード

syslog server

syslog サーバホストの IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG サーバに、192.168.100.1 を設定する

```
Router(config)# syslog server 192.168.100.1
```

コマンド書式

syslog server 〈SYSLOG サーバ〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SYSLOG サーバ	syslog を通知するサーバの IP アドレスを指定	IPv4 アドレス形式 IPv6 アドレス形式	省略不可

最大エントリ数:1 エントリ

この設定を行わない場合

ログ情報を、syslog サーバに送信しません。

設定モード

基本設定モード

syslog facility

ログ情報を syslog で通知する際のファシリティコード番号(0～23)を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG のファシリティ値を”local0″に設定する

```
Router(config)# syslog facility 16
```

コマンド書式

syslog facility <ファシリティコード番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ファシリティコード番号	syslog のファシリティ値を指定します。	0～23	省略不可

この設定を行わない場合

ファシリティコード番号 1 になります。

SYSLOG のファシリティとは？

syslog のファシリティとは、ログメッセージの種類を表します。
一般的には、どのような状況でログが発生したかを表す番号として指定されます。
RFC3164 では、以下のように規定されています。(OS により捕らえ方が同じように見えるファシリティ値もあります)

コード番号	ファシリティ	コード番号	ファシリティ
0	kernel message	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by syslogd	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 3 (local3)
8	UUCP subsystem	20	local use 4 (local4)
9	clock daemon	21	local use 5 (local5)
10	security/authorization messages	22	local use 6 (local6)
11	FTP daemon	23	local use 7 (local7)

syslog を通知した場合、サーバ側ではファシリティ毎に保存するファイルを変えるというような運用方法も可能となります。

設定モード

基本設定モード

syslog format bsd

本装置が送出する syslog メッセージのフォーマットを BSD タイプ（PRI 部、HEADER 部、MSG 部からなるファーマット）とします。
フォーマットは、(facility*8)+level で算出されるプライオリティ値、タイムスタンプ、ホスト名、ログのタイプ、シーケンス番号、アップタイム、TID、ログ ID、メッセージ本体の順になります。
本コマンドは、elog メッセージ、flog メッセージ、slog メッセージ、tlog メッセージ、vpnlog メッセージが対象となります。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG メッセージのフォーマットを BSD タイプとする

```
Router (config)# syslog format bsd
```

コマンド書式

```
syslog format bsd
```

パラメータ

パラメータはありません。

この設定を行わない場合

syslog メッセージのフォーマットは、プライオリティ値、シーケンス番号、アップタイム、タイムスタンプ、TID、ログ ID、メッセージ本体の順になります。

設定モード

基本設定モード

syslog source-interface

syslog パケット送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SYSLOG 送信時の送信元アドレスに、LAN インタフェースの IP アドレスを使用する

```
Router(config)# syslog source-interface lan 1
```

コマンド書式

syslog source-interface〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	syslog を通知する際のパケットの送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

syslog パケットを実際に送信するインタフェースになります。

設定モード

基本設定モード

電子メールによる障害通知機能

mail server

mail 通知機能が電子メールを送信する際のメールサーバを指定します。複数行入力することにより 3 つまで有効, 4 つ以上は無視されます。
また先に入力したサーバが優先されます。メールサーバはホスト名と IP アドレスを設定できます。
電子メールで以下の内容を通知することができます。

・不正アクセスがあった場合
・冗長機能で到達不能／復旧を感知した場合
・時刻指定リセット機能により装置の再起動が起こった場合
・ISDN 自動切断機能が作動もしくは警告状態になった場合

設定例１　メールサーバの IP アドレスを 192.168.100.1 に設定する

```
Router(config)#mail server 192.168.100.1
```

コマンド書式

mail server 〈SMTP サーバの IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SMTP サーバの IP アドレス	電子メールを送信するための SMTP サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名形式 のいずれか	省略不可

最大エントリ数:3 エントリ

この設定を行わない場合

電子メールによる通知を行ないません。

不正アクセスとは？

FITELnet-F シリーズでは、TELNET または FTP によりログインされる場合に、規定回数以上パスワード誤りが発生した場合、不正アクセスと判断します。

冗長機能とは？

FITELnet-F シリーズでは、複数の回線を利用して、バックアップ形態を形成することができます。
例）
通常は FTTH を使用し、FTTH 側で通信ができなくなった場合に、ADSL 回線に切り替えて通信する。

FITELnet-F シリーズでは、このようにバックアップを使用して通信を継続する機能を『冗長機能』といいます。

時刻指定リセット機能とは？

FITELnet-F シリーズでは、FTP で"RESETAT"ファイルを送ることにより、"RESETAT"ファイル内に記載されている指定時刻に装置を再起動することができます。
例）
2003.4.1 12:00:00 に SIDE-A のファームウェア/SIDE-A の設定ファイルで起動する場合
↓
RESETAT ファイルに、以下のように記述して、FITELnet-F シリーズに FTP で送信する
reset at 12:00 1 Apr 2003 SIDE-A.frm SIDE-A.cfg

ISDN 自動切断機能とは？

FITELnet-F100（BRI オプション）では、ISDN 回線に関して、異常課金を防ぐ機能として、連続接続を許容する時間・1 時間あたりに発信できる許容回数を指定し、指定時間/回数以上の呼確立がある場合は、呼確立を停止する機能があります。
この状態になった（作動）場合および規定時間/回数の 90%を超えた（警告）場合に、電子メールで通知します。

電子メールで通知する情報

【不正アクセスの場合】
Subject：[RAAS] Illegal Connect Request on FITELnet-F100(装置の IP アドレス)

SysDescr	装置名称　バージョン
IP Address	装置の IP アドレス
Application	不正アクセスを検知したアプリケーション
Sender	不正アクセスを行なったホストの IP アドレス
Time	不正アクセスを受けた時間

【時刻指定リセット機能の場合】
Subject:[RAAS] Auto Reset on FITELnet-F100(装置の IP アドレス)

SIDE-A/SIDE-B	SIDE-A.frm、SIDE-B.frmの情報 VALID/INVALID:使用可能/仕様不可(壊れている) ACTIVE/INACTIVE:使用中のファームウェア／待機中のファームウェア 各ファームウェアのバージョン情報
SIDE-A/SIDE-B	SIDE-A.cfg、SIDE-B.cfg の情報 ACTIVE/INACTIVE:使用中の設定情報／待機中の設定情報 LAST SAVE:最後に保存された日時
reset at	次に起動する時間・適用ファームウェア・適用設定情報

【ISDN 自動切断機能の場合】
Subject:[RAAS] Call Limitter Started on FITELnet-F100(装置の IP アドレス)

SysDescr	装置名称　バージョン
IP Address	装置の IP アドレス
Target Name	自動切断した相手の名称
Target ISDN Address	自動切断した相手の ISDN 番号／サブアドレス
Limitter Mode	自動切断の種類(時間(Continuance) or 回数(Calling count))
Current	現在の接続時間もしくは接続回数
Status	作動(bomberd) or 警告(Warning)
Time	到達不能／復旧を検知した時間

なお、電子メールの差出人(From:)は、いずれのケースでも、"Router Auto Administration System"となります。

設定モード

基本設定モード

mail from

メールの送信元アドレスを設定します。

設定例１　メールの送信元アドレスとして"F100@xxxxx.co.jp"を指定する

```
Router(config)# mail from F100@xxxxx.co.jp
```

コマンド書式

mail from〈送信元メールアドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
送信元メールアドレス	メール通知機能で送信する電子メールの From に入れるメールアドレス	-	省略不可

この設定を行わない場合

From には、何も設定されません。
その結果、メールでの通知機能も働きません。

設定モード

基本設定モード

mail to

メールの送信先アドレスを設定／解除します。
複数行入力することにより、5 つまで指定可能です。
また、電子メール通知機能で通知する種類を以下の中から選択します。

種類	電子メール送信タイミング	オプション
不正アクセス	不正アクセスを認識したタイミング	invader
自動再起動	ファームウェアの自動再起動がおこったタイミング	filemaintenance
ISDN 自動切断※1	規定時間/回数以上の呼確立があったあるいは 規定時間/回数の 90%を超える呼確立があったタイミング	limiter
IPsec 冗長機能	経路が障害発生しバックアップ経路へ切り替わった時 障害発生していたメイン経路が復旧し切り戻った時	redundancy
IPsec 負荷分散機能	経路が障害発生した時 経路が復旧した時	multi-path
イベントアクション	イベントアクション機能のアクションにメール通知を指定し、そのアクションに対応するイベントの状態変化が発生した場合。 イベントアクション機能のメール通知については、send e-mail コマンドを参照してください	event-action

※1:F100 のみ選択可能です。

設定例１　メールの宛先アドレスを admin@xxxx.co.jp に設定する（送信種類：不正アクセス、IPsec 冗長機能）

```
Router(config)#mail to admin@xxxx.co.jp invader redundancy
```

コマンド書式

mail to〈宛先メールアドレス〉[電子メールの種類]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
宛先メールアドレス	メール通知機能で送信する電子メールの To に入れるメールアドレス	−	省略不可
電子メールの種類	電子メールにて通知するメッセージの種類	invader filemaintenance limiter※ redundancy multi-path event-action のいずれかもしくは複数	全ての種類のメールを通知する

※:F100 のみ選択可能です。
最大エントリ数:5 エントリ

この設定を行わない場合

電子メールによる通知を行ないません。

設定モード

基本設定モード

mail server

mail 通知機能が電子メールを送信する際のメールサーバを指定します。複数行入力することにより 3 つまで有効, 4 つ以上は無視されます。
また先に入力したサーバが優先されます。メールサーバはホスト名と IP アドレスを設定できます。

設定例１　メールサーバの IP アドレスを 192.168.100.1 に設定する

```
Router(config)#mail server 192.168.100.1
```

コマンド書式

mail server 〈SMTP サーバの IP アドレス〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
SMTP サーバの IP アドレス	電子メールを送信するための SMTP サーバの IP アドレス	IPv4 アドレス形式 IPv6 アドレス形式 ホスト名形式 のいずれか	省略不可

最大エントリ数:3 エントリ

この設定を行わない場合

電子メールによる通知を行ないません。

設定モード

基本設定モード

mail source-interface

SMTP パケット送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

設定例１　SMTP パケットの送信元アドレスに LAN の IP アドレスを使用する

```
Router(config)# mail source-interface lan 1
```

コマンド書式

mail interface〈インタフェース名〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	SMTP パケットの送信元アドレスとしてつけるインタフェース	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

実際にパケットを送信するインタフェースの IP アドレスになります。

設定モード

基本設定モード

NTP機能

SNTPクライアント機能

sntp retry

タイムサーバからの応答がなかった場合のリトライ間隔およびリトライ動作時間を設定します。
リトライ間隔は"sntp retry interval"コマンドで、リトライ動作時間は"sntp retry keepalive"コマンドで設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　SNTP のリトライ間隔を 100 秒に設定する

```
Router(config)#sntp retry interval 100
```

設定例２　SNTP のリトライ動作時間を 10 分（600 秒）に設定する

```
Router(config)#sntp retry keepalive 600
```

設定例３　SNTP のリトライをしない

```
Router(config)#sntp retry interval off
```

コマンド書式

sntp retry interval <リトライ間隔>
sntp retry keepalive <リトライ時間>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ間隔	SNTP サーバから応答がなかった場合のリトライ間隔（単位：秒）を指定します。リトライを行わない場合は、off を指定します。	16～1024 off	省略不可
リトライ時間	リトライ継続時間（秒）。この時間経過したら、リトライ動作を終了する。	64～1024	省略不可

この設定を行わない場合

リトライ間隔	64 秒
リトライ時間	1024 秒

設定モード

基本設定モード

sntp schedule

サーバに問い合わせるスケジュールを指定します。
ここで設定するスケジュールは、以下の項目です。
・本装置の起動時に問い合わせを行なうかどうか？
・何時間おきに問い合わせを行なうか／何時に問い合わせを行なうか？

本装置起動時に問い合わせを行なう場合は、boot を指定します。
次に問い合わせを行なう間隔もしくは時間の設定は"interval"もしくは"time"で設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　本装置の起動時に問い合わせを行い、起動後は 1 時間おきに問い合わせる

```
Router(config)#sntp schedule boot interval 1
```

設定例２　本装置の起動時には問い合わせを行なわず、起動後は毎日 12:00 に問い合わせを行なう

```
Router(config)#sntp schedule time 12:00
```

コマンド書式

sntp schedule [boot] interval hour < 問い合わせ間隔 >
sntp schedule [boot] interval sec < 問い合わせ間隔 >
sntp schedule [boot] time < 問い合わせ時刻 >

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
boot	装置起動時に SNTP で時刻の問い合わせを行なうかどうか行なう場合に、boot を指定する	boot	装置起動時には問い合わせを行なわない
問い合わせ間隔	SNTP サーバに時刻を問い合わせる間隔（単位：時間） hour 指定の場合は、1～65534 sec 指定の場合は、16～16384 ※0 または、off を指定した場合は、問い合わせを行いません。 ※hour および sec を省略した場合は、単位が時間（hour）となります。	off（リトライしない） もしくは 0～65535	省略不可
問い合わせ時刻	SNTP サーバに時刻を問い合わせる時刻（時：分） 毎日この時刻に、に SNTP サーバに時刻を問い合わせる ※0:0 を指定した場合は、問い合わせを行いません。	0:0～23:59	省略不可

この設定を行わない場合

起動時問い合わせ	しない
問い合わせ間隔	1 時間

設定モード

基本設定モード

sntp server

接続するタイムサーバ(プライマリ,セカンダリ)の IP アドレスを設定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SNTP サーバ（プライマリ：192.168.100.1、セカンダリ：192.168.100.2）を設定する

```
Router(config)#sntp server 192.168.100.1 192.168.100.2
```

設定例 2　SNTP サーバ（プライマリ：3ffe:b80:bf::1、セカンダリ：3ffe:b80:bf::2）を設定する

```
Router(config)#sntp server 3ffe:b80:bf::1 3ffe:b80:bf::2
```

コマンド書式

sntp server〈プライマリ SNTP サーバ〉 [〈セカンダリ SNTP サーバ〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プライマリ SNTP サーバ	プライマリの SNTP サーバを指定	IPv4 アドレス形式 IPv6 アドレス形式	省略不可
セカンダリ SNTP サーバ	セカンダリの SNTP サーバを指定	IPv4 アドレス形式 IPv6 アドレス形式	セカンダリ SNTP サーバを使用しない

この設定を行わない場合

SNTP 機能を使用できません。

設定モード

基本設定モード

sntp source-interface

SNTP 送出の際の送信元 IP アドレスとして使用するインタフェース名を指定します。

refresh コマンド後に有効になるコマンドです。

設定例 1　SNTP を送信する際の送信元アドレスに LAN インタフェースの IP アドレスを使用する

```
Router(config)#sntp source-interface lan 1
```

コマンド書式

sntp source-interface〈インタフェース名 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース名	SNTP パケットの送信元アドレスに使用するインタフェースアドレス	lan 1 ewan 1～2 loopback 1 vlanif 1～16	省略不可

この設定を行わない場合

SNTP を実際に送信するインタフェースになります。

設定モード

基本設定モード

NTPサーバ機能

ntp-server enable

NTP サーバ機能を使用する場合に設定します。
NTP サーバ機能は、上位 NTP サーバから時刻情報を受信していなくても利用可能ですが、時刻の精度が本装置の内蔵時計の精度となってしまうため、SNTP クライアント機能の設定を行ない、上位 NTP サーバから時刻情報を受信するようにしてください。

refresh コマンド後に有効になるコマンドです。

設定例１　NTP サーバ機能を使用する

```
Router(config)#ntp-server enable
```

コマンド書式

ntp-server enable

パラメータ

パラメータはありません

この設定を行わない場合

NTP サーバ機能を使用できません。

設定モード

基本設定モード

ntp-server stratum

本装置で NTP サーバ機能を使用する際の Stratum 値を設定します。
Stratum 値とは、NTP サーバの階層を示すもので、Stratum1 が最上位の階層になります。

refresh コマンド後に有効になるコマンドです。

設定例１　Stratum 値を 2 に設定する

```
Router(config)#ntp-server stratum 2
```

コマンド書式

ntp-server stratum <stratum 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
stratum 値	NTP の Stratum 値を指定します。	1～15	省略不可

この設定を行わない場合

Stratum 値を1とします。

設定モード

基本設定モード

SSHサーバ機能

SSHサーバ機能

ip scp server enable

Secure Copy の機能を有効にします。
本装置の SCP サーバ機能を使用すると、ファームウェアファイル／設定ファイルを、暗号化して転送することができます。
SCP サーバ機能を使用する際は、ssh-server enable が必要です。

refresh コマンド後に有効になるコマンドです。

設定例１　SCP 機能を有効にする

```
Router(config)#ip scp server enable
```

コマンド書式

```
ip scp server enable
```

この設定を行わない場合

SCP サービスは動作しません

設定モード

基本設定モード

ssh-server access-group

本装置にアクセスする SSH クライアントを、指定したアクセスリストに従いフィルタリングします。permit と判断されたときのみアクセスを許可します。
ただし、設定がない場合、及び該当アクセスリストがない場合は フィルタリング機能自体が働かず全てのアクセスを許可します。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.0.0/24 のネットワークのホストからのアクセスのみを許可する

```
Router(config)# access-list 10 permit 192.168.0.0 0.0.0.255
Router(config)# ssh-server access-group 10
```

設定例２　3ffe:110::/64 のネットワークのホストからのアクセスのみを許可する

```
Router(config)# access-list 3000 permit 3ffe:110::/64
Router(config)# ssh-server ipv6 access-group 3000
```

コマンド書式

ssh-server [ipv6] access-group 〈アクセスリスト番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ipv6	IPv6 アクセスリスト番号を使用する場合に指定します。	ipv6	IPv6 アクセスリスト番号を指定できません。
アクセスリスト番号	アクセスリストで、アクセスを許可する SSH クライアントを指定し、その番号をここで指定します	1～99 3000～3499	省略不可

この設定を行わない場合

すべての SSH アクセスを許可します

設定モード

基本設定モード

ssh-server authentication-retries

SSH の認証失敗時のリトライ回数を指定します。

設定例１　SSH の認証失敗時のリトライを 5 回まで許容する

```
(config)#ssh-server authentication-retries 5
```

コマンド書式

ssh-server authentication-retries 〈リトライ回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リトライ回数	SSH の認証失敗時のリトライを許容する回数を指定します。	0～5	省略不可

この設定を行わない場合

SSH 認証リトライ回数:3 回

設定モード

基本設定モード

ssh-server enable

SSH サーバを動作させる場合に指定します。
本装置は SSH version1 のみをサポートしています。また、暗号化アルゴリズムは、DES-CBC／3DES-CBC をサポートしています。
また、generate key ssh でホスト固有鍵を生成しておく必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　SSH サーバを動作させる

```
Router(config)#ssh-server enable
```

コマンド書式

ssh-server enable

パラメータ

パラメータはありません

この設定を行わない場合

SSH サーバ機能は動作しません。

設定モード

基本設定モード

ssh-server exec-timeout

無通信監視時間(単位:分)を設定します。自動ログアウトをさせない場合は 0 分を指定します。

refresh コマンド後に有効になるコマンドです。

設定例１　TELNET では、5 分間入力がない場合は自動ログアウトする

```
Router(config)# ssh-server exec-timeout 5
```

コマンド書式

ssh-server exec-timeout 〈無通信監視時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
無通信監視時間	無通信監視時間(単位:分)。 ここで設定した時間なにも入力がない場合は、自動的にログアウトします。 off を指定すると自動ログアウトを無効とします。	1～60 off	省略不可

この設定を行わない場合

5 分間入力がない場合はログアウトします

設定モード

基本設定モード

ssh-server response-timeout

SSH のネゴシエーションにおいて、SSH クライアントからの応答待ち時間を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　60 秒間応答がない場合は セッションを切断する

```
Router(config)# ssh-server response-timeout 60
```

コマンド書式

ssh-server response-timeout 〈タイムアウト時間〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
タイムアウト時間	SSH クライアントからの応答待ち時間(単位:秒)。 ここで設定した時間クライアントからの応答がない場合、SSH セッションを解放します。	1～120	省略不可

この設定を行わない場合

SSH タイムアウト値:120 秒

設定モード

基本設定モード

Ethernet機能

Ethernet機能

hardware macaddress conventional

全てのポートで同一の MAC アドレスを使用するためのコマンドです。
本装置には、装置 MAC アドレス(MAC アドレス 1)とそれとは別にもう一つの MAC アドレス(MAC アドレス 2)が割り当てられています。

設定例１　全てのポートで同一の MAC アドレスを使用する

```
Router(config)# hardware macaddress conventional
Router(config)#
```

コマンド書式

hardware macaddress conventional

パラメータ

パラメータはありません。

この設定を行わない場合

LAN と EWAN2 に MAC アドレス1、EWAN1 に MAC アドレス 2 が割り当てられます。

※:PPPoE に関しては、それぞれ関連づけられた EWAN ポートの MAC アドレスになります。

設定モード

基本設定モード

line

Ethernet インタフェースについて、速度/デュプレックス/MDI/MDI-X の設定を行なう Ethernet 設定モードに移行するためのコマンドです。

設定例１　EWAN#1 ポートの設定を行なうモードに移行する

```
Router(config)# line ewan 1
Router(config line ewan 1)#
```

コマンド書式

line〈物理インタフェース〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
物理インタフェース	設定を行なう物理インタフェースを lan 1、ewan 1、ewan 2 から選択します。	lan 1 ewan 1 ewan 2	省略不可

設定モード

基本設定モード

linkdown-detect

物理的な LAN ポートのリンクアップ/ダウンと LAN インタフェースのアップ/ダウンを連動させるかどうかの設定を行います。
interface lna 1 で linkdown-detect on と設定することにより、LAN ポートを使用する VLAN インタフェースにもこの設定が適用されます。

refresh コマンド後に有効になるコマンドです。

設定例１　論理的な LAN インタフェースのアップ/ダウンと LAN ポートのリンクアップ/ダウンを連動させる

```
Router(config)#inter lan 1
Router(config-if lan 1)#linkdown-detect on
```

コマンド書式

linkdown-detect 〈リンクダウン設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
リンクダウン設定	物理的な LAN ポートのリンクアップ/ダウンと LAN インタフェースのアップ/ダウンを連動させるかどうかの設定を行います。 on：リンクアップ/ダウンを連動させる。 off：リンクアップ/ダウンを非連動にする。	on off	省略不可

この設定を行わない場合

物理的な LAN ポートのリンクアップ/ダウンに関わらず、LAN インタフェースは常にアップ状態となります。
ただし、「ip vrrp enable」が設定されており、かつ LAN または LAN のポートとして使用する VLAN インタフェースに VRRP の設定がある場合は、物理的な LAN ポートのリンクアップ/ダウンと連動します

設定モード

LAN インタフェース設定モード

mac access-list

MAC アドレスによるフィルタリングを行う場合の MAC アクセスリストの設定を行います。
使用方法は、まず本コマンドで MAC アドレスを指定した後、mac access-group コマンドで指定した MAC アクセスリスト番号を指定します。
mac access-list は、番号順に適用されます。
また、同じ番号の mac access-list に複数行の設定をした場合は、上の行から適用されます。

refresh コマンド後に有効になるコマンドです。

設定例１　MAC アクセスリストに、MAC アドレス 1122.3344.5566 を許可属性として設定する

```
Router(config)# mac access-list 1 permit 1122.3344.5566
```

設定例２　MAC アクセスリストに、全ての MAC アドレスを不許可属性として設定する

```
Router(config)# mac access-list 1 deny any
```

コマンド書式

```
mac access-list <mac access-list 番号> remark<コメント>
mac access-list <mac access-list 番号> permit <MAC アドレス> [log] [count]
mac access-list <mac access-list 番号> deny {<MAC アドレス>|any} [log] [count]
```

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	設定する MAC アクセスリスト番号を指定します。	1～512	省略不可
permit	設定する MAC アクセスリストに許可属性を与える場合に指定します。	permit	省略不可
deny	設定する MAC アクセスリストに不許可属性を与える場合に指定します。	deny	省略不可
MAC アドレス	MAC アドレスを H.H.H の形式で設定します。MAC アドレスが、11.22.33.44.55.66 の場合は、1122.3344.5566 となります。	MAC アドレス形式	省略不可
any	deny を指定した場合は、MAC アドレスの代わりに any を指定することにより、全ての MAC アドレスを指定することができます。	any	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。	count	カウントを行いません。

コメント	MAC アクセスリストに付けるコメントを指定します。	240 文字までの半角英数字、記号	省略不可

この設定を行わない場合

MAC アドレスによるフィルタリングを行いません。

設定モード

基本設定モード

mac access-group

mac access-list コマンドで指定したフィルタリングデータを、各インタフェースで適用します。
フィルタリングデータは、各インタフェースで受信したパケットに適用するのか／各インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　mac access-list 1 で指定したデータを、EWAN 1 送信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 1 out
```

設定例２　mac access-list 2 で指定したデータを、EWAN 1 からの受信時に適用する

```
Router(config)#interface ewan 1
Router(config-if ewan 1)#mac access-group 2 in
```

コマンド書式

mac access-group <mac access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
mac access-list 番号	フィルタリングデータを設定した MAC アクセスリストの番号を指定します。	1～512	省略不可
{ in | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。	in out	省略不可

この設定を行わない場合

MAC アドレスによるフィルタリングを行いません。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード

shutdown

物理的にポートを停止させる場合に指定します。
本コマンドでポートを停止させた場合、該当するポートはリンクアップしなくなります。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN インタフェースのポート１をリンクアップしない状態にする

```
Router(config)#line lan 1
Router(config-line lan 1)#shutdown 1
```

設定例１　EWAN#2 インタフェースをリンクアップしない状態にする

```
Router(config)#line ewan 2
Router(config-line ewan 2)#shutdown 1
```

コマンド書式

shutdown〈ポート番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN インタフェースには、4 つのポートがあるので、その番号を指定します。 EWAN インタフェースの場合は、"1"を指定します。	1～4	省略不可

この設定を行わない場合

LAN および EWAN インタフェースが使用可能です。

設定モード

Ethernet 設定モード

speed-duplex

Ethernet の通信速度/デュプレックス(全二重 or 半二重)を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN（ポート番号 4）の通信速度を、100Mbps/Full デュプレックス（全二重）に設定する

```
Router(config)#line lan 1
Router(config-line lan 1)# speed-duplex 4 100-full
```

コマンド書式

speed-duplex〈インタフェース番号〉〈 通信速度とデュプレックス 〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
インタフェース番号	LAN インタフェースには、4 つのポートがあるので、その番号を指定します。 EWAN インタフェースの場合は、"1"を指定します。	1～4 1	省略不可
通信速度とデュプレックス	設定している Ethenet インタフェースの通信速度／デュプレックスを設定します。 10-full：10Mbps/Full デュプレックス 10-half：10Mbps/Half デュプレックス 100-full：100Mbps/Full デュプレックス 100-half：100Mbps/Half デュプレックス auto：AUTO ネゴシエーション	10-full 10-half 100-full 100-half auto	省略不可

この設定を行わない場合

AUTO ネゴシエーションで動作します。

設定モード

Ethernet 設定モード

sw

Ethernet の MDI/MDI-X を設定します。

refresh コマンド後に有効になるコマンドです。

設定例１　LAN（ポート番号 4）を、MDI-X に設定する

```
Router(config)#line lan 1
Router(config-line lan 1)# sw 4 mdi-x
```

コマンド書式

sw〈ポート番号〉〈MDI 設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	LAN インタフェースには、4 つのポートがあるので、その番号を指定します。 EWAN インタフェースの場合は、"1"を指定します。	1～4	省略不可
MDI 設定	設定している Ethernet インタフェースの MDI/MDI-X を設定します。 mdi：MDI ポート mdi-x：MDI-X ポート auto：自動切換	mdi mdi-x auto	省略不可

この設定を行わない場合

自動切換で動作します。

MDI/MDI-X とは？

Ethernet ポートにおいて、DTE として使用するポートを"MDI ポート"、DCE として使用するポートを"MDI-X ポート"といいます。

通常の NIC は MDI ポート、HUB は MDI-X ポートで運用されています。

ストレートケーブルを使用する場合、相手が MDI である場合は自分は MDI-X、相手が MDI-X である場合は自分は MDI でなくてはなりません。

接続相手が自動切換の装置の場合は、本装置では自動切換にしないようにしてください。Ethernet が使用できない場合があります。

設定モード

Ethernet 設定モード

VLAN機能

VLAN機能

bridge-group

設定している VLAN インタフェースで使用するブリッジグループ番号を指定します。
この設定により、VLAN インタフェースと、ブリッジグループのひも付けを行うことができます。

設定例１　VLAN インタフェースで使用するブリッジグループを１番とする

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1) bridge-group lan 1 1
```

コマンド書式

bridge-group lan 1 <ブリッジグループ番号>
bridge-group ewan <1-2>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ブリッジグループ番号	ブリッジグループ番号を指定します。	0～15	省略不可

この設定を行わない場合

インタフェースを使用することができません。

設定モード

VLAN インタフェース設定モード

ip access-group

access-list コマンドで指定したフィルタリングデータを、VLAN インタフェースで適用します。
フィルタリングデータは、VLAN インタフェースで受信したパケットに適用するのか／VLAN インタフェースに送信するパケットに適用するのかを指定する必要があります。

refresh コマンド後に有効になるコマンドです。

設定例１　access-list 1 で指定したデータを、VLAN1 送信時に適用する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)#ip access-group 1 out
```

設定例２　access-list 2 で指定したデータを、VLAN1 からの受信時に適用する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)#ip access-group 2 in
```

コマンド書式

ip access-group <access-list 番号> { in | out }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	フィルタリングのデータを設定したアクセスリストの番号を指定します。	<1-99> <100-199> <1300-1999> <2000-2699>	省略不可
{ in | out }	インタフェースでの受信時(in)／インタフェースからの送信時(out)のどちらでフィルタリングするのかを指定します。 受信時は、さらに以下のように設定ができます。	in：受信時 out：送信時	省略不可

この設定を行わない場合

設定している VLAN インタフェースでは、IP パケットフィルタリングを使用しません。

IP フィルタリングについて

指定したパケット以外は中継しないといったように、セキュリティ強化のため使用する機能です。

設定モード

VLAN インタフェース設定モード

ip address

VLAN インタフェースの IP アドレスとサブネットマスクを指定します。

設定例１　VLAN インタフェースの IP アドレスを 158.ｘｘｘ.ｘｘｘ.1 に設定する

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1)#ip address 158.202.232.2 255.255.255.0
```

コマンド書式

ip address 〈IP アドレス〉〈サブネットマスク〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	サブネットマスクを設定します。	IPv4 アドレス形式	省略不可

設定モード

VLAN インタフェース設定モード

vlan bridge-group

ブリッジグループ番号を指定します。この設定により、物理ポートとブリッジグループのひも付けを行うことができます。
LAN ポートのみ指定することができます。

設定例１　VLAN 機能で使用する物理ポート１番と、ブリッジグループ５番をひも付ける

```
Router(config)#line lan 1
Router(config-line lan 1) vlan 1 bridge-group 5
```

コマンド書式

vlan 〈ポート番号〉 bridge-group 〈ブリッジグループ番号〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	物理ポート番号を指定します。	1～4	省略不可
ブリッジグループ番号	ブリッジグループ番号を指定します。	0～15	省略不可

この設定を行わない場合

ブリッジグループ番号=0 で動作します。

設定モード

Ethernet 設定モード

vlan egress-tagging

送信フレームに対して、802.1Q TAG ヘッダを付加させるか除去させるかを指定します。
802.1Q TAG ヘッダを付加しない場合、tagVLAN 機能を使用することはできません。
なお、受信フレームに関しては、802.1Q TAG ヘッダある/なしに関わらず、受信することができます。

設定例１　VLAN ポート 1 から送信するフレームに対して 802.1Q TAG ヘッダを付加します

```
Router(config)#line lan 1
Router(config-line lan 1) vlan 1 egress-tagging always
```

コマンド書式

vlan 〈ポート番号〉 egress-tagging 〈TAG 設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	物理ポート番号を LAN ポートの場合 1～4、EWAN ポートの場合 1 で指定します。	1～4	省略不可
TAG 設定	優先度タグを付加するか、しないかを指定します。 always：パケットに優先度タグを付加して送信します。 never：パケットに優先度タグを付加しないで送信します。	always never	省略不可

この設定を行わない場合

全てのパケットは、タグを除去された状態で送信されます。

設定モード

Ethernet 設定モード

vlan-id

このインタフェースで扱うタグフレーム ID 値を指定します。
この値は、接続する相手(L2 スイッチなど)と同じである必要があります。

設定例１　送信する VLAN-ID を 1 とします

```
Router(config)#interface vlanif 1
Router(config-if vlanif 1) vlan-id 1
```

コマンド書式

vlan-id <VLAN-ID 値>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
VLAN-ID 値	インタフェースで送信する際の VLAN-ID を指定します。	1～4094	省略不可

この設定を行わない場合

インタフェースを使用することができません。

設定モード

VLAN インタフェース設定モード

vlan port-vlan

ポート VLAN を使用するかどうかと、VLAN-ID を指定します。
ポート VLAN で使用する場合、TAG ヘッダのついていないデータを受信した場合は、設定した VLAN-ID として VLAN インタフェースを利用します。

設定例１　ポート VLAN を使用するポートを物理ポート 1 番、VLAN-ID を 10 とします

```
Router(config)#line lan 1
Router(config-line lan 1) vlan 1 port-vlan 10
```

コマンド書式

vlan 〈ポート番号〉 port-vlan 〈VLAN-ID 値〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ポート番号	物理ポート番号を指定します。	lan 1～4 ewan 1	省略不可
VLAN-ID 値	ポート VLAN で使用する VLAN-ID を指定します。	1～4094	省略不可

この設定を行わない場合

ポート VLAN を使用することができません。

設定モード

Ethernet 設定モード

アクセスリスト

アクセスリスト

access-list

特定のパケットと、そのパケットの動作(中継 or 廃棄 or 学習フィルタリング)を指定します。refresh コマンド後に有効になるコマンドです。

指定したパケットは、以下の機能で使用します。

・フィルタリング(ip access-group コマンド)
・学習フィルタリング(ip access-group コマンド)
・オフセットリスト(offset-list コマンド)
・RIP/BGP で送信するメトリック値の指定(distance コマンド)
・BGP で送信する経路の指定(neighbor <IP-address> distribute-list コマンド)
・経路情報の指定(match ip address コマンド)
・NextHop の指定(match ip nexthop コマンド)
・NAT 変換前のアドレス指定(ip nat inside コマンド)
・使用方法は、まず本コマンドでパケットを指定した後、上記機能を使用するモードで、指定したアクセスリスト番号を指定します。refresh コマンド後に有効になるコマンドです。

アクセスリスト番号について

本装置のアクセスリスト番号は、以下の規定があります。

アクセスリスト番号	名称	設定内容
1～99、1300～1999	IPv4 標準設定	IPv4 送信元アドレス指定
100～199、2000～2699	IPv4 拡張設定	IPv4 送信元／宛先アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定
3000～3499	IPv6 標準設定	IPv6 送信元／宛先アドレス指定
3500～3999	IPv6 拡張設定	IPv6 送信元アドレス指定 プロトコル番号指定 送信元／宛先ポート番号指定

指定パケットの動作指定について

指定したパケットを中継対象とするか、廃棄対象とするかを指定します。中継対象とする場合は permit、廃棄対象とする場合は deny を指定します。
この指定が必要なのは、フィルタリング／経路情報の指定／NextHop の指定のためにアクセスリストを指定する場合のみです。他の用途で指定する場合は permit を指定してください。

IP アドレス範囲指定

アクセスリストコマンドで IPv4 アドレスを指定する場合、マスク(Wildcard マスク)を使用して 1 エントリでアドレス範囲を指定することができます。
Wildcard マスクは、サブネットマスクとは書式が異なりますので注意してください。Wildcard マスクとサブネットマスクは、"1"と"0"の判別が逆になります。
例1)24bit マスクを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い
Wildcard マスクの場合:0.0.0.255
サブネットマスクの場合:255.255.255.0
例2)ホストを、Wildcard マスクで表現する場合と、サブネットマスクで表現する場合の違い

Wildcard マスクの場合:0.0.0.0
サブネットマスクの場合:255.255.255.255

ポート番号の指定

IPv4/IPv6 拡張設定では、TCP/UDP 上位ポート番号を指定することができます。この指定は、フィルタリング／学習フィルタリングの指定のためにアクセスリストを指定する場合に効果があります。他の用途で指定する場合は、標準設定でアクセスリストを指定してください。

学習フィルタリング

インターネットの常時接続で使用する場合、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN 側からのインターネット接続に対する応答データ以外はフィルタリング(廃棄)することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス(Web 等)はできなくなります。(アクセスを許可するアドレスを限定することはできます)
ただし、VPN からの受信に関してはフィルタリングを行いません。
本装置で、学習フィルタリングを使用する場合は、access-list コマンドの属性で、"dynamic"を指定します。

設定例１　IPv4 標準アクセスリストに、192.168.100.0/24 を設定する（許可属性）

```
Router(config)# access-list 1 permit
192.168.100.0 0.0.0.255
```

設定例２　IPv4 拡張アクセスリストに、src=192.168.100.0/24 dst=192.168.200.0/24 を設定する（不許可属性）

```
Router(config)# access-list 100 deny ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

設定例３　IPv6 標準アクセスリストに、src=3ffe:110::/64 を dst=3ffe:111::/64 を設定する（許可属性）

```
Router(config)# access-list 3000 permit
3ffe:110::/64 3ffe:111::/64
```

設定例４　IPv6 拡張アクセスリストに、src=any srcport=any dst=any dstport=80 を設定する（不許可属性）

```
Router(config)# access-list 3500 deny tcp any gt
0 any eq 80
```

設定例5　学習フィルタリングを指定する(IPv4)

```
Router(config)# access-list 100 dynamic permit ip
any any
```

コマンド書式

IPv4 標準アクセスリスト（アクセスリスト番号：1～99、1300～1999）
access-list <access-list 番号> { permit | deny } { any | <送信元 IP アドレス> <送信元 Wildcard マスク> }[log][count]

IPv4 拡張アクセスリスト（アクセスリスト番号：100～199、2000～2699）
access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | host <送信元 IP アドレス> | <送信元 IP アドレス> <送信元 Wildcard マスク> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | host <宛先 IP アドレス> | <宛先 IP アドレス> <宛先 Wildcard マスク> } [ICMP タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [[precedence {<precedence-value>|<precedence-named-value>}] [tos {<tos-value>|<tos-named-value>}]| [dscp {<dscp-value>|<dscp-named-value>}]] [ip-flag {<ip-flag-value>|<ip-flag-value:wildcard mask>}][log] [count]

IPv6 標準アクセスリスト（アクセスリスト番号：3000～3499）
access-list <access-list 番号> { permit | deny } { any | <送信元 IPv6 プレフィックス> } { any | <宛先 IPv6 プレフィックス> } [count]

IPv6 拡張アクセスリスト（アクセスリスト番号：3500～3999）access-list <access-list 番号> { [dynamic] permit | deny } <プロトコル番号> { any | <送信元 IPv6 プレフィックス> } [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] { any | <宛先 IPv6 プレフィックス> } [ICMPv6 タイプ] [<ポート属性> <TCP ポート番号>] [<ポート属性> <UDP ポート番号>] [tcp-flag {<tcp-flag-value>|<tcpflag-value:wildcard-mask>}] [traffic-class <traffic-class-value>|dscp {<dscp-level>|<dscp-name>}] [flow-label <flow-label-value>][count]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
access-list 番号	それぞれの属性の番号を指定します。	1～99、1300～1999	IPv4 標準アクセスリスト	省略不可
		100～199、2000～2699	IPv4 拡張アクセスリスト	
		3000～3499	IPv6 標準アクセスリスト	
		3500～3999	IPv6 拡張アクセスリスト	
dynamic	学習フィルタリングを使用する場合に指定します。	dynamic		学習フィルタリングのエントリではない
{ permit | deny }	許可属性か、不許可属性かを選択します。	permit	許可属性	省略不可

		deny 不許可属性	
プロトコル番号	プロトコル名もしくはプロトコル番号を選択します。	gre Cisco's GRE tunneling icmp ICMP(IPv4 拡張アクセスリスト時) icmpv6 ICMPv6(IPv6 拡張アクセスリスト時) ip IP ipinip IP トンネル tcp TCP udp UDP 0～255 プロトコル番号を指定	省略不可
any	各パラメータ(アドレスやポート番号など)で、「全て」を指定する場合は"any"を入力します。	any	-
送信元 IP アドレス	送信元アドレスを指定します。	IPv4 アドレス形式	省略不可
送信元 Wildcard マスク	送信元アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
宛先 IP アドレス	宛先アドレスを指定します。	IPv4 アドレス形式	省略不可
宛先 Wildcard マスク	宛先アドレスを範囲指定するために、Wildcard マスクを指定します。	IPv4 アドレス形式	省略不可
host	IPv4 拡張アクセスリストで、送信元/宛先アドレスとしてホストアドレスを指定する場合につけます。	host	-
送信元 IPv6 プレフィックス	送信元 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
宛先 IPv6 プレフィックス	宛先 IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
ICMP タイプ	プロトコル番号で"icmp"を指定した場合に、対象とする ICMP タイプを指定します。	指定できる ICMP タイプ administratively-prohibited alternate-address conversion-error dod-host-prohibited	全ての ICMP タイプ

		echo	
		echo-reply	
		general-parameter-problem	
		host-isolated	
		host-precedence-unreachable	
		host-redirect	
		host-tos-redirect	
		host-tos-unreachable	
		host-unknown	
		host-unreachable	
		information-reply	
		information-request	
		mask-reply	
		mask-request	
		mobile-redirect	
		net-redirect	
		net-tos-redirect	
		net-tos-unreachable	
		net-unreachable	
		network-unknown	
		no-room-for-option	
		option-missing	
		packet-too-big	
		parameter-problem	
		port-unreachable	
		precedence-unreachable	
		protocol-unreachable	
		reassembly-timeout	
		redirect	
		router-advertisement	
		router-solicitation	
		source-quench	
		source-route-failed	
		time-exceeded	

		timestamp-request traceroute ttl-exceeded unreachable	
ICMPv6 タイプ（IPv6）	プロトコル番号で"icmpv6"を指定した場合に、対象とする ICMPv6 タイプを指定します。	ICMPv6 タイプ address-unreachable administratively-prohibited dest-unreachable echo-reply echo-request erroneous-header-field hop-limit-exceeded-in-transit multicast-listener-done multicast-listener-query multicast-listener-report neighbor-advertisement neighbor-solicitation no-route-to-destination packet-too-big parameter-problem port-unreachable reassembly-time-exceeded redirect router-advertisement router-solicitation time-exceeded unrecognized-next-header unrecognized-option ICMPv6 タイプ値（0～255）	全ての ICMPv6 タイプ
ポート属性	ポート番号を範囲で指定するために、ポート属性を指定します。 ※gt、lt を使用する場合、指定す	eq 指定するポートが対象	全てのポート（以降設定なし）

	るポート番号は対象範囲に含まれません。	gt: 指定するポート番号より大きいポート番号が対象 lt: 指定するポート番号より小さいポート番号が対象 neq: 指定するポート番号以外のポート番号が対象 range: ポートの範囲を指定する	
TCP ポート番号	プロトコルで"tcp"を指定した場合に、対象とする TCP ポート番号を指定します。	TCP ポート番号 bgp chargen cmd daytime discard domain echo exec finger ftp ftp-data gopher hostname ident irc klogin kshell login lpd nntp pim-auto-rp pop2 pop3 smtp sunrpc syslog	全ての TCP ポート番号

		tacacs tacacs-ds talk telnet time uucp whois www TCP ポート番号(0～65535)	
UDP ポート番号	プロトコルで"udp"を指定した場合に、対象とする UDP ポート番号を指定します。	UDP ポート番号 biff bootpc bootps discard dnsix domain echo isakmp mobile-ip nameserver netbios-dgm netbios-ns netbios-ss ntp pim-auto-rp rip snmp snmptrap sunrpc syslog tacacs tacacs-ds talk tftp time who	全ての UDP ポート番号

		xdmcp UDP ポート番号(0～65535)	
precedence-value※	precedence-value を設定します。	0～7	省略不可
precedence-named-value※	precedence-named-value を設定します。	routine(0) priority(1) immediate(2) flash(3) flash-override(4) critical(5) internet(6) etwork(7)	省略不可
tos-value※	tos-value を設定します。	0～15	省略不可
tos-named-value※	tos-named-value を設定します。	min-momentary-cost(1) max-reliability(2) max-throughput(4) min-delay(8) normal(0)	省略不可
dscp-value※	dscp-value を設定します。	0～63	省略不可
dscp-named-value※	dscp-named-value を設定します。	ef(101110b) bf(000000b) af11(001010b) af12(001100b) af13(001110b) af21(010010b) af22(010100b) f23(010110b) af31(011010b) af32(011100b) af33(011110b) af41(100010b) af42(100100b) af43(100110b)	省略不可
ip-flag-value※	ip-flag-value を設定します。	0～3、もしくは、0～3:0～3(ワイルドカードマスク)	省略不可

tcp-flag-value※	tcp-flag-value を設定します。	0～63、もしくは、0～63:0～63(ワイルドカードマスク)	省略不可
traffic-class-value	traffic-class-value を設定します。	0～255、もしくは、0～255:0～255(ワイルドカードマスク)	省略不可
flow-label	flow-label を設定します。	0～1048575	省略不可
log	パケットフィルタリング機能において該当条件(行単位)にヒットしたパケットが、フィルタリングログに記録されます。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	log	フィルタリングログを記録しません。
count	統計情報としてフィルタにヒットしたパケット数、バイト数を表示します。 ※dynamic 指定の場合、学習した学習フィルタにヒットしたパケットは記録しません。	count	カウントを行いません。

最大エントリ数:ip access-group で関連付けた access-list に対して、最大 1024 エントリ
装置全体で 1024 エントリ
ipv4, ipv6 の区別無く、装置全体で最大 1024 エントリ
各インターフェース毎の制限無く、装置全体で最大 1024 エントリ

※:これらのパラメータをフィルタリングで使用する事はできません。

この設定を行わない場合

access-list を使用した機能を使用できません。

設定モード

基本設定モード

access-list remark

アクセスリストに対して、コメントを記述することができます。
記述した内容は show access-list で表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　192.168.100.1 からのアクセスを拒否しているコメントを付ける

```
Router(config)#access-list 100 remark Reject access from 192.168.100.1
Router(config)
```

コマンド書式

access-list 〈access-list 番号〉 remark 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
access-list 番号	コメントを付けるアクセスリスト番号を指定します。	1～3999※	省略不可
文字	コメントを入力します。	240 文字までの半角英数字、記号	省略不可

※:access-list 番号の設定範囲に関しては、access-list コマンドを参照してください。

設定モード

基本設定モード

ループバックインタフェースの設定

ループバックインタフェースの設定

interface loopback

ループバックインタフェース設定モードに移行します。

設定例１　ループバックインタフェース設定モードに移行します。

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#
```

コマンド書式

interface loopback 1

パラメータ

パラメータはありません。

設定モード

基本設定モード

ip address

ループバックインタフェースの IP アドレスを指定します。
サブネットマスクは、自動的に 255.255.255.255 に設定されます。

設定例１　ループバックの IP アドレスを 192.168.0.1 に設定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ip address 192.168.0.1
```

コマンド書式

ip address <IP アドレス>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可

この設定を行わない場合

ループバックインタフェースに、IP アドレスが割り当てられません。

設定モード

ループバックインタフェース設定モード

ipv6 address

ループバックインタフェースの IPv6 アドレス(グローバル・リンクローカル)を指定します。
リンクローカルアドレスを指定しなかった場合は、EUI-64 形式のリンクローカルアドレスが自動で設定されます。
FITELnet-F シリーズでは、1つのインタフェースに4つのグローバルアドレスを指定することができます。

設定例１　プレフィックス：2002:1004::/64　EUI-64 形式で指定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ipv6 address 2002:1004::/64 eui-64
```

設定例２　リンクローカルアドレスを、fe80::1 に設定する

```
Router(config)#interface loopback 1
Router(config-if loopback 1)#ipv6 address fe80::1 link-local
```

コマンド書式

ipv6 address { <IPv6 アドレス> link-local | <IPv6 プレフィックス> [eui-64] }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
IPv6 アドレス	IPv6 リンクローカルアドレスを指定します。	IPv6 アドレス形式	省略不可
link-local	リンクローカルアドレスである場合に指定します。	link-local	省略不可
IPv6 プレフィックス	IPv6 プレフィックスを指定します。	IPv6 プレフィックス形式	省略不可
eui-64	EUI-64 方式でグローバルアドレスを設定する場合に指定します。	eui-64	省略した場合はグローバルアドレスとして使用しません。RA で広告するプレフィックスにのみ使用します。

最大エントリ数:30 エントリ(装置全体)

この設定を行わない場合

ループバックインタフェースでは、IPv6 アドレスが割り当てられません。ただし、PD を使用してインターネットと接続する場合は、設定の必要はありません。

設定モード

ループバックインタフェース設定モード

その他の機能

CLIの表示に関する機能

alias

よく発行するコマンドや、長くて入力が面倒なコマンドを、alias コマンドで簡単化して登録しておきます。
このコマンドは、入力完了した時点で有効になります。

設定例 1　show interface lan 1 コマンドの alias 名を、"shlan"とする。

```
Router(config)# alias shlan show interface lan 1
```

コマンド書式

alias 〈alias 名〉〈コマンド〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
alias 名	コマンドを簡単化する際の名称	-	省略不可
コマンド	簡単化するコマンド	-	255

この設定を行わない場合

コマンドの省略形は使用できません。

設定での注意事項

注意1: FITELnet-F シリーズのコマンドを alias 名に使用しないでください。
【設定してはいけない例】
alias save save /var/card1a/config/boot.cfg
“save”というコマンド名は FITELnet-F シリーズのコマンドであるため、このように設定してはいけない。

注意2: すでに設定してある alias のコマンド名を、alias 名に使用しないでください。
【設定してはいけない例】
alias aaa bbb
alias bbb aaa
“bbb”というコマンド名はすでに alias 登録されているため、このように設定してはいけない。

設定モード

基本設定モード

description

各インタフェースに対して、コメントを記述することができます。
記述した内容は show interface で表示されます。

refresh コマンド後に有効になるコマンドです。

設定例１　ダイヤルアップインタフェースにコメントを付ける

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#description backup line
```

コマンド書式

description 〈文字〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
文字	コメントを入力します。	240 文字までの半角英数字、記号	省略不可

設定モード

LAN インタフェース設定モード
PPPoE インタフェース設定モード
EWAN インタフェース設定モード
VLAN インタフェース設定モード
ダイヤルアップインタフェース設定モード(F100 のみ)
IPsec インタフェース設定モード
ループバックインタフェース設定モード
トンネルインタフェース設定モード

shutdown

設定を残したままでインタフェースを停止させる場合に指定します。

refresh コマンド後に有効になるコマンドです。(VLAN インタフェース設定モードのみ)

設定例１　LAN インタフェースを一時的に使用できない状態にする

```
Router(config)#interface lan 1
Router(config-if lan 1)#shutdown
```

コマンド書式

shutdown

パラメータ

パラメータはありません。

この設定を行わない場合

インタフェースが使用可能です。

設定モード

LAN インタフェース設定モード
EWAN インタフェース設定モード
PPPoE インタフェース設定モード
BRI インタフェース設定モード(F100 のみ)
ダイヤルアップインタフェース設定モード(F100 のみ)
VLAN インタフェース設定モード
トンネルインタフェース設定モード

hostname

プロンプトを設定します。
このコマンドは、入力完了した時点で有効になります。

refresh コマンド後に有効になるコマンドです。

設定例　プロンプトを"F100#1"に設定する

```
Router(config)#hostname F100#1
F100#1Router(config)#
```

コマンド書式

hostname 〈プロンプト文字列〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
プロンプト文字列	プロンプトに使用する文字列を設定します。	16 文字以内の文字列	省略不可

この設定を行わない場合

"Router"となります。

設定モード

基本設定モード

高速化キャッシュ機能

flow-cache ip

パケット中継を、flow キャッシュを用いて高速に実行します。

refresh コマンド後に有効になるコマンドです。

設定例１　flow キャッシュを使用しない

```
Router(config)#flow-cache ip disable
```

コマンド書式

flow-cache ip〈キャッシュ設定〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
キャッシュ設定	flow キャッシュを使用するかどうかの指定をします。 enable：flow キャッシュを有効にする disable：flow キャッシュを無効にする	enable disable	省略不可

この設定を行わない場合

flow キャッシュを使用します。

設定モード

基本設定モード

索引

A

aaa enable..... 391
aaa my-name..... 392
aaa peer-name..... 394
access-list..... 96, 249, 728
access-list remark..... 738
action-map..... 27, 118, 309, 588
add ip route..... 563
address..... 555
address-pool enable..... 60
address-pool ipv6..... 18, 61
aggregate-address..... 95, 206
alias..... 742
alive..... 427
allocate-address..... 488
always-up check-interval..... 429
am-3-encr..... 430
am-3-initcont..... 431
anonymous-call accept..... 623
anti-replay..... 397
area authentication..... 179
area default-cost..... 169
area export-list..... 170
area import-list..... 171
area nssa..... 172
area range..... 174
area shortcut..... 175
area stub..... 176
area virtual-link..... 198
area virtual-link authentication... 199
area virtual-link authentication-key 200
area virtual-link dead-interval.... 201
area virtual-link hello-interval... 202
area virtual-link message-digest-key 203
area virtual-link retransmit-interval 204
area virtual-link transmit-delay... 205
authentication..... 339
auto connect..... 624
auto-cost reference-bandwidth..... 194

B

bgp always-compare-med..... 207
bgp bestpath as-path ignore..... 210
bgp bestpath compare-routerid..... 212
bgp bestpath med missing-as-worst.. 208
bgp default ipv4-unicast..... 214
bgp default local-preference..... 217
bgp log-neighbor-changes..... 215
bgp router-id..... 216
bgp scan-time..... 218
bridge-group..... 721

C

callback..... 625
callback requestnumber..... 627
callback-responsetime..... 628
callback-waittime..... 629
called idle-timeout..... 630
caller..... 631
calling-number..... 632
check interface status..... 545
check ip-icmp..... 544
check vrrp status vrid..... 546
class..... 121, 312, 601
class-map..... 26, 113, 303, 581
clear ipsec-session isakmp-policy.. 565
compatible rfc1583..... 193
configuration mode..... 395, 432
configuration mode application-version message..... 380, 434
configuration mode application-version push..... 381, 435
configuration mode(isakmp polcy)... 376
configuration mode(security-association)..... 378
console exec-timeout..... 525
crl-optional..... 417
crypto ca identity..... 34
crypto ipsec-log..... 38
crypto isakmp policy..... 35
crypto map..... 36, 398, 399
crypto security-association.... 37, 436

D

dampening disable..... 547
dampening-parameter..... 548
ddns-client..... 509
ddns-server accept-fqdn type..... 505
ddns-server enable..... 507
ddns-server logging address-changes 508
default-information originate. 92, 140, 159
default-metric..... 142, 160
default-router..... 485

description.... 511, 549, 562, 566, 743
dhcp-client retries infinitely..... 54
dialer flets..... 634
dialer interface..... 635
dialer map..... 636
distance..... 144, 161, 219, 220
distance ospf..... 163
distribute-list..... 89, 146
dns-server..... 483
domain-name..... 482
drop..... 589

E

email..... 418
e-mail body false-to-true..... 567
e-mail body true-to-false..... 568
e-mail subject..... 569
encryption..... 340
event match-any..... 550
event-action..... 23
event-class..... 22, 543, 580
event-map..... 24, 579

F

flow-cache ip..... 746
forced disconnect time..... 637
ftp-server exec-timeout..... 526
ftp-server shutdown..... 527

G

group..... 341

H

hardware macaddress conventional... 712
hash..... 342
hostname..... 745
hosttable..... 490
http-client..... 40
http-server authname..... 530
http-server authtype digest..... 531
http-server digest-auth nonceage... 532
http-server shutdown..... 533

I

icmp-class..... 25, 554
idtype-pre..... 343
idtype-rsa..... 344
igmp-proxy disable-upstream..... 571
igmp-proxy non-querier..... 316
ikealive freq..... 437
ikealive retry max..... 438
ikealive retry timer..... 439
interface bri..... 9
interface dialer..... 29
interface ewan..... 8
interface ipsecif..... 31
interface lan..... 6
interface loopback..... 30, 739
interface pppoe..... 7
interface tunnel..... 32
interface vlanif..... 33
interval..... 556
ip access-group 259, 522, 639, 659, 722
ip address 48, 125, 419, 447, 638, 658, 723, 740
ip address dhcp..... 55, 126
ip address unnumbered..... 448
ip arp learning..... 295
ip arp reply..... 296
ip arp request..... 297
ip arp static..... 298
ip dhcp pool..... 16, 480
ip dhcp relay maxhops..... 493
ip dhcp-client dont-register-implicit-default-route..... 57
ip directed-broadcast..... 300
ip domain-name..... 284, 420
ip helper-address..... 494
ip icmp error-ratelimit..... 301
ip igmp access-group..... 317
ip igmp fast-leave..... 318
ip igmp group-membership-timeout... 319
ip igmp last-membership-query-interval..... 320
ip igmp proxy..... 321
ip igmp proxy non-querier-behavior. 324
ip igmp proxy-group..... 322
ip igmp proxy-group-upstream..... 323
ip igmp querier-timeout..... 325
ip igmp query-interval..... 326
ip igmp query-max-response-time.... 327
ip igmp source-interface..... 329
ip igmp static-group..... 328
ip igmp version..... 330
ip limited-broadcast ttl..... 334
ip mtu..... 50, 58, 289, 335
ip multicast ttl-threshold..... 331
ip multicast-routing proxy..... 332
ip name-server..... 49, 281
ip name-server source-interface.... 283

ip nat inside destination..... 641
ip nat inside destination(PPPoE)... 465
ip nat inside source..... 644
ip nat inside source(PPPoE)..... 461
ip nat log-table-changes..... 452
ip nat max-sessions..... 454
ip nat outside destination..... 472
ip nat outside source..... 468
ip nat pool..... 475
ip nat reserved-sessions..... 453
ip nat translation finrst-timeout.. 455
ip nat translation icmp-timeout.... 457
ip nat translation tcp-timeout..... 458
ip nat translation timeout..... 459
ip nat translation udp-timeout..... 460
ip ospf authentication..... 180
ip ospf authentication-key..... 181
ip ospf cost..... 187
ip ospf database-filter all out.... 188
ip ospf dead-interval..... 184
ip ospf disable all..... 189
ip ospf hello-interval..... 183
ip ospf message-digest-key..... 182
ip ospf network..... 190
ip ospf priority..... 191
ip ospf retransmit-interval..... 185
ip ospf transmit-delay..... 186
ip polling-interval..... 315
ip proxy-arp..... 293
ip resolver-cache-time..... 286
ip rip authentication key-chain.... 133
ip rip authentication mode..... 134
ip rip receive version..... 131
ip rip send version..... 132
ip route..... 262
ip scp server enable..... 706
ip source-quench..... 302
ip split-horizon..... 135
ip stateful max-sessions..... 261, 524
ip vpn-nat inside destination..... 350
ip vpn-nat inside source..... 347, 382
ip vpn-nat pool..... 345
ip vrrp enable..... 534
ipsec access-list..... 400
ipsec transform-set..... 374
ipv6 access-group..... 106, 521
ipv6 address..... 65, 741
ipv6 address address-pool prefix-length 62
ipv6 address autoconfig..... 67
ipv6 dhcp client..... 63
ipv6 dhcp client-profile..... 19
ipv6 enable..... 68
ipv6 hop-limit..... 70
ipv6 hoplimit-receive-enable..... 71
ipv6 icmp error-ratelimit..... 69, 301
ipv6 mtu..... 51, 59, 111
ipv6 mtu-receive-enable..... 112
ipv6 nd managed-config-flag..... 79
ipv6 nd ns-interval..... 78
ipv6 nd other-config-flag..... 80
ipv6 nd prefix-advertisement..... 81
ipv6 nd ra-interval..... 76
ipv6 nd ra-lifetime..... 77
ipv6 nd reachable-time..... 83
ipv6 nd receive-ra..... 72
ipv6 nd rs-delay..... 73
ipv6 nd rs-times..... 74
ipv6 nd send-ra..... 75
ipv6 ns-interval-receive-enable..... 84
ipv6 polling-interval..... 124
ipv6 prefix-list..... 86
ipv6 reachable-time-receive-enable.. 85
ipv6 route..... 109
isakmp-negotiation..... 440

K

keepalive..... 353
keepalive-icmp..... 355
keepalive-icmp multi-path..... 357
keepalive-icmp redundancy..... 358
key..... 359
key <number> accept-lifetime..... 152
key <number> key-string..... 156
key <number> send-lifetime..... 154
key chain..... 20, 150

L

lcp keepalive..... 661
lcp maxtimes..... 648, 662
lcp restart..... 649, 663
lease..... 489
leased-line..... 622
lifetime..... 361
line..... 39, 40, 713
linkdown-detect..... 336, 714
log-adjacency-changes..... 197
logging..... 512
logging event state-change... 551, 561, 570

logging-level elog..... 672
logging-level flog..... 676
logging-level slog..... 674
logging-level tlog..... 678, 680
logging-level vpnlog..... 680

M

mac access-group..... 717
mac access-list..... 715
mail from..... 693
mail server..... 690, 696
mail source-interface..... 697
mail to..... 694
match address..... 403
match duration..... 552
match ip address..... 278
match ip next-hop..... 279
match ip/ipv6 access-group... 115, 305, 583
match ip/ipv6 input-interface 117, 307, 585
match metric..... 280
match policy-flag..... 587
match-any..... 114, 304, 582
max-call..... 650
method..... 513
mss..... 52, 291
multi-path..... 423
my-identity..... 362

N

name server..... 421
nat-traversal..... 363
negotiation..... 441
negotiation-mode..... 365
neighbor..... 130, 165
neighbor <ip-address> activate..... 222
neighbor <ip-address> default-originate..... 223
neighbor <ip-address> description.. 224
neighbor <ip-address> distribute-list..... 225
neighbor <ip-address> dont-capability-negotiate..... 226
neighbor <ip-address> ebgp-multihop 227
neighbor <ip-address> maximum-prefix..... 228
neighbor <ip-address> next-hop-self 229
neighbor <ip-address> override-capability..... 230
neighbor <ip-address> port <0-65535>..... 233
neighbor <ip-address> remote-as <1-65535>..... 234
neighbor <ip-address> route-map.... 235
neighbor <ip-address> shutdown..... 236
neighbor <ip-address> soft-reconfiguration inbound..... 237
neighbor <ip-address> strict-capability-match..... 238
neighbor <ip-address> timers..... 239
neighbor <ip-address> transparent-as..... 240
neighbor <ip-address> transparent-nexthop..... 241
neighbor <ip-address> update-source 242
neighbor <ip-address> version {4 | draft}..... 243
neighbor <ip-address> weight..... 244
neighbor password..... 231
netbios-name-server..... 484
network..... 88, 128, 158, 246
nolog-block-type-discard..... 424
nolog-spi-no-match..... 425
ntp-server enable..... 704
ntp-server stratum..... 705

O

offset-list..... 137
option..... 486
option-request prefix-delegation.... 64
ospf abr-type..... 177

P

passive-interface..... 136, 192
peer-identity..... 366
peer-identity distinguished-name... 368
policy-map..... 28, 122, 313, 602
ppp authentication..... 651
ppp bap holdtime..... 652
ppp bap threshold..... 653
ppp hostname..... 654
ppp multilink..... 655
pppoe account..... 42
pppoe auth-accept..... 43
pppoe interface..... 44
pppoe ncp..... 47
pppoe server..... 41
pppoe service..... 45
pppoe type..... 46

priority classification..... 613
priority default-priority..... 614
priority queuing..... 616
priority threshold..... 617
probe..... 559
proxydns default cache-time..... 501
proxydns default domain-name..... 497
proxydns default name-server..... 498
proxydns default retrans-time..... 499
proxydns default retry..... 500
proxydns default source-interface.. 502
proxydns domain..... 503
proxydns hosts..... 504
proxydns mode..... 496

Q

qos frame-length-offset..... 604
qos output bandwidth..... 606
qos-que cbq..... 607
qos-que priq..... 609
query-ip..... 422

R

recvidletimer..... 656
redistribute..... 91, 138, 166, 247
re-establish-sa rekey..... 442
reference-interface..... 515
refresh timer..... 195
release security-association.. 369, 370
release session addr-changed..... 370
remote-access limitation..... 518
remote-access time..... 520
request-timeout..... 516
retry..... 443
retry guard-time..... 444
retry rekey-ipsec..... 445
retry rekey-ipsec negotiation..... 446
route..... 94, 148
route-map..... 14
router bgp..... 12
router ospf..... 11
router rip..... 10
router ripng..... 13, 87
router-id..... 157

S

sa-up route..... 389, 405
search-address..... 487
send e-mail..... 573
send snmp-trap..... 574
service dhcp-relayagent..... 491
service dhcp-server..... 478
service-policy..... 611
service-policy local..... 612
set 802.1p priority..... 600
set aggregator..... 267
set as-path prepend..... 268
set atomic-aggregate..... 269
set community..... 270
set community-additive..... 271
set ip dscp..... 590
set ip next-hop..... 265, 310, 591
set ip prec..... 593
set ip tos..... 594
set ipv6 dscp..... 595
set ipv6 next-hop..... 119, 596
set ipv6 traffic-class..... 598
set local-preference..... 272
set metric..... 266
set origin..... 273
set originator-id..... 274
set peer..... 406
set pfs..... 408
set policy-flag..... 576
set queuing..... 599
set redundancy..... 409
set redundancy distance..... 410
set security-association always-up . 412
set security-association ipsec-src-id
..... 413
set security-association lifetime .. 415
set security-association selector
bypass..... 333
set tag..... 275
set transform-set..... 416
set weight..... 276
shutdown..... 718, 744
size..... 558
snmp-server community..... 664
snmp-server contact..... 670
snmp-server enable traps..... 666
snmp-server host..... 667
snmp-server location..... 671
snmp-server name..... 669
snmp-server source-interface..... 668
sntp retry..... 698
sntp schedule..... 700
sntp server..... 702
sntp source-interface..... 703
source-interface..... 371, 517

speed-duplex..... 719
ssh-server access-group..... 707
ssh-server authentication-retries.. 708
ssh-server enable..... 709
ssh-server exec-timeout..... 710
ssh-server response-timeout..... 711
statistics update..... 123, 314, 603
summary-address..... 168
suspend icmp-class..... 577
sw 720
syslog facility..... 686
syslog format bsd..... 688
syslog level..... 683
syslog sending..... 682
syslog server..... 685
syslog source-interface..... 689

T

telnet-server exec-timeout..... 528
telnet-server shutdown..... 529
timeout..... 560
timers basic..... 93, 143
timers spf..... 196
trial..... 557
tunnel destination..... 449
tunnel mode..... 450
tunnel source..... 451
tunnel-route..... 372, 387

U

unicastRIP..... 149
upnp-server access-group..... 619
upnp-server enable..... 620
upnp-server target-interface..... 621
username..... 657

V

version..... 141
vlan bridge-group..... 724
vlan egress-tagging..... 725
vlan port-vlan..... 727
vlan-id..... 726
vpn enable..... 337
vpnlog enable..... 338
vpnlog-detail..... 426
vrrp..... 578
vrrp address..... 535
vrrp adver-interval..... 537
vrrp auth-type..... 538
vrrp preempt..... 540
vrrp priority..... 542

- 本書は改善のため事前連絡なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権その他の権利について、弊社はその責を負いません。
- 無断転載を禁じます。
- Copyright© 2005-2009 FURUKAWA ELECTRIC CO., LTD. All rights reserved.

発行責任：古河電気工業株式会社
130-B0369-AH02-N
2009.8