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-F120

（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

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-F120 は、5 つの 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（1～5）を指定します。

refresh コマンド後に有効になるコマンドです。

※：同一物理ポートで、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。

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 <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
PPPoE 番号	PPPoE ポートの番号を指定します。 PPPoE1～4 が物理ポート EWAN1 に、 PPPoE5 が物理ポート EWAN2 で使用できます。	1～5	省略不可

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。

refresh コマンド後に有効になるコマンドです。

※：同一物理ポートで、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。

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

モバイルインタフェース設定モード

interface mobile

mobile インタフェース設定モードに移行します。

設定例1　モバイルインタフェース設定モードに移行する

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

コマンド書式

interface mobile 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します。

```
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

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。
refresh コマンド後に有効になるコマンドです。
有効になる最大ピア数は、１６ピアです。

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-F100 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。
FITELnet-F120 の LAN/EWAN2 インタフェースで、FITELnet-F120 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 lan 1
Router(config-dhcp-pool)#
```

コマンド書式

ip dhcp pool { lan 1 | ewan 2 }

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
lan1 ｜ ewan2	DHCP サーバ機能を使用するインタフェースを選択します。	lan 1	LAN インタフェースで使用する	省略不可
		ewan 2	EWAN2 インタフェースで使用する	

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-F120 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-F120 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。

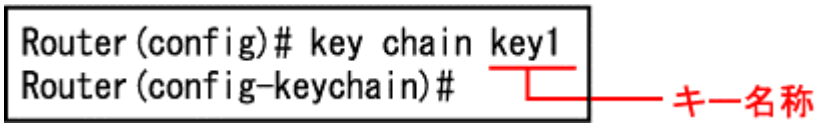
設定モード

基本設定モード

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
```

キー名称

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

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に移行する

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

コマンド書式

interface dialer〈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
接続相手シーケンス番号	接続相手を識別する番号	1～4	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。	1～4	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。
ポリシーの番号を 1 ～32 の範囲で指定してください。
refresh コマンド後に有効になるコマンドです。

設定例1 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。	1～32	省略不可

最大エントリ：32 エントリ

設定モード

基本設定モード

VPNセレクタ設定モード

crypto map

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。
ポリシーの番号を 1 ～32 の範囲で指定してください。

refresh コマンド後に有効になるコマンドです。

設定例1　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 ～64	省略不可

最大エントリ：64 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。
refresh コマンド後に有効になるコマンドです。

設定例1 IPsec ログモードに移行する

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

refresh コマンド後に有効になるコマンドです。

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選択します。	lan 1	LAN インタフェース（SW-HUB 4 ポート）	省略不可
		ewan 1	EWAN#1 ポート	
		ewan 2	EWAN#2 ポート	

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 〈PPPoE 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
PPPoE 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-F120 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 f120@xxxxx.ne.jp, パスワードに f120pass を設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#pppoe account f120@xxxxx.ne.jp f120pass
```

コマンド書式

pppoe account〈ユーザ ID〉〈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 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

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	プロバイダとの PPP 認証プロトコルを指定します。 auto…自動、プロバイダとのネゴシエーション結果に従います pap…PAP 固定 chap…CHAP 固定	auto pap chap	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 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

端末型接続（host）か、LAN 型接続（lan）かを選択します。OCN ADSL アクセス IP8/IP16「フレッツ」プランのように、複数のアドレスが割り当てられる契約の場合は LAN 型を選択します。

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…インタフェースアドレスが 1 つ割り当てられている場合 lan…インタフェースアドレスが複数割り当てられている場合	host lan	省略不可

この設定を行わない場合

”端末型”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。
「端末型」と「LAN 型」では、IPCP を確立するためのネゴシエーションにおいて、自身の IP アドレスとして相手に通知するアドレスが異なります。

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 <NCP>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
NCP	PPP 上を中継するプロトコル（IPv4, IPv6）を指定します。 ipcp…IPv4 を中継する ipv6cp…IPv6 を中継する both…双方を中継する	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 158.xxx.xxx.1 に設定する

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

※：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

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。

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。

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

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

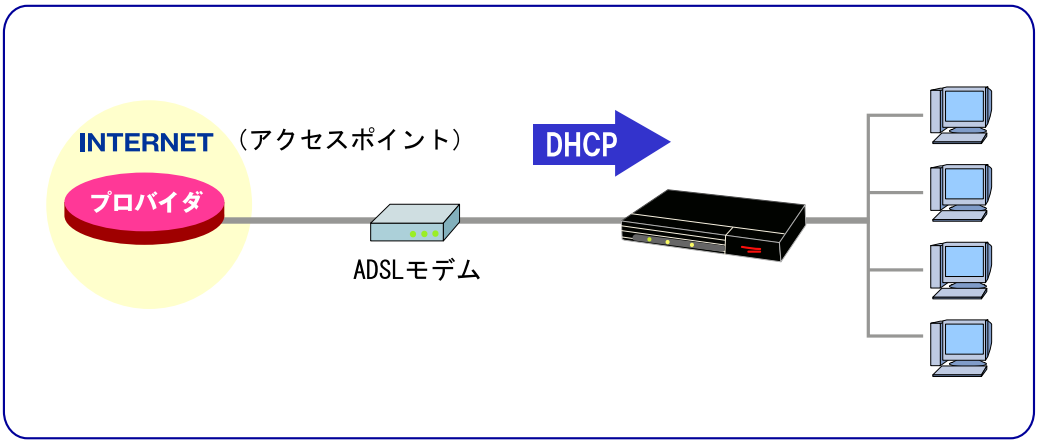
DHCPDISCOVER を 2 回リトライしても DHCPOFFER が得られない場合、アドレス取得動作を打ち切ります。

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、プロバイダから「クライアント ID」もしくは「ホスト名」を指定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 >}[type < タイプ >] | [hostname< ホスト名 >]]

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>{ ascii | hex}
クライアント ID</td><td>クライアント ID を ASCII または、hex で指定します。</td><td><table><tr><td>ascii</td><td>最大 63 文字 (ASCII)</td></tr><tr><td>hex</td><td>最大 126 桁 (16 進数)</td></tr></table></td><td>クライアント ID を付けない</td></tr>
<tr><td>タイプ</td><td>クライアント ID のタイプを指定します。</td><td>0～255</td><td><table><tr><td>クライアント ID が ASCII の場合</td><td>0</td></tr><tr><td>クライアント ID が hex の場合</td><td>1</td></tr></table></td></tr>
<tr><td>ホスト名</td><td>ホスト名を指定します。</td><td>最大 63 文字</td><td>ホスト名を付けない</td></tr>
</table>

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-F120 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 mtu

EWAN インタフェースの MTU 長を指定します。

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

1500byte 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。

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

1500byte 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 ルーティングの設定

IPv6 アドレス設定

ipv6 address

LAN 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-F120 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

LAN インタフェースでは、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

ipv6 enable

LAN 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

ICMPv6 に関する設定

ipv6 nd send-ra

FITELnet-F120 が送信する 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あるいは、PD で取得した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

ipv6 nd ra-interval

FITELnet-F120 が 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 秒おきに 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

ipv6 nd ra-lifetime

FITELnet-F120 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

ipv6 nd ns-interval

FITELnet-F120 が、RA を送信する際に、Retrans Time 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) を定期送信する際、ここで指定した値（単位：m 秒）間隔で送信します。
また、FITELnet-F120 が NS を定期送信する際も、この値を使用します。

設定例1 NS の定期送信間隔を 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
RA で通知する NS の定期送信間隔	RA で通知する NS の定期送信間隔および、FITELnet-F120 自身が定期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-F120 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

ipv6 nd managed-config-flag

FITELnet-F120 が、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

ipv6 nd other-config-flag

FITELnet-F120 が、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

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、あるいは PD で取得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

ipv6 nd reachable-time

FITELnet-F120 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

15000～45000m 秒の間の、ランダムな値となります。

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 icmp error-ratelimit

FITELnet-F120 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。
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。

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>

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

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。

エラーメッセージ名称	内容
Destination Unreachable Message.	受信したパケットの宛先への経路が存在しない
Packet Too Big Message	パケット長が、MTU 長より大きいため、転送できない
Time Exceeded Message	ホップ数が 0 のパケットを受信したため、転送できない
Parameter Problem Message	IPv6 ヘッダ（オプション含む）が異常または未知

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。

FITELnet-F120 では、FITELnet-F120 自身から送信する IPv6 パケットの Hop limit 値、および FITELnet-F120 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

FITELnet-F120 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

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。

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 or 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称もしくは IPv6 アドレス形式で決定します。

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 { <インタフェース名称> | <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
インタフェース名称	RIPng を運用するインタフェース名称を指定します。	インタフェース名形式	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	

この設定を行わない場合

どのインタフェースでも 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。

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 } [インタフェース名称]

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／送信のどちらでフィルタするかを指定します。	in 受信時 out 送信時	省略不可
インタフェース名称	適用するインタフェースのインタフェース名称を指定します。	インタフェース名形式	全インタフェースで適用

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	省略不可
		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	

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

自身がデフォルトルート情報を持っていない場合でも、RIP テーブルにデフォルトルートを登録して RIP で通知できるようにします。
refresh コマンド後に有効になるコマンドです。

設定例1　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

デフォルトルートを通知しません。

設定モード

RIPng サービス設定モード

timers basic

RIPng に関する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 30 秒、経路情報を削除するまでの時間を 180 秒、経路情報を一時到達不能にするまでの時間を 120 秒とする

```
Router(config)#router ripng
Router(config-ripng)#timers basic 30 180 120
```

コマンド書式

timers basic〈定期送信間隔〉〈経路情報を削除するまでの時間〉〈経路情報を一時到達不能にするまでの時間〉

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	定期送信間隔（単位：秒）を設定します。	5～2147483647	省略不可
経路情報を削除するまでの時間	経路情報を削除するまでの時間（単位：秒）を設定します。	5～2147483647	省略不可
経路情報を一時到達不能にするまでの時間	経路情報を一時到達不能にするまでの時間（単位：秒）を設定します。	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
経路情報を削除するまでの時間	180
経路情報を一時到達不能にするまでの時間	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。

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

FITELnet-F120 では、常にインターネットに接続しており、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。
FITELnet-F120 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>][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>][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	全ての ICMP タイプ

		conversion-error	
		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	

		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-advertisment 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	全てのICMPv6 タイプ

		ICMPv6 タイプ値（0～255）	
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	全ての TCP ポート番号

		pop3 smtp sunrpc syslog 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	全ての UDP ポート番号

		talk tftp time who xdmcp UDP ポート番号（0～65535）	
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。

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（PPPoE、LAN、EWAN）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）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）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、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

ipv6 access-group 〈アクセスリスト番号〉{ 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
アクセスリスト番号	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

スタティックルーティングの設定

ipv6 route

FITELnet-F120 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 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。

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
```

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>] [distance] | pppoe <1-5>}

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	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。 NextHop にリンクローカルアドレスを指定した場合に、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。	インタフェース名形式	NextHop の IPv6 アドレスを設定する必要があります。
distance	スタティックルーティングの distance 値を指定します。	2～255※	1
pppoe	宛先へ到達するためのインタフェースとして PPPoE インタフェースを指定します。	1～5	省略不可

最大エントリ数：63 エントリ（ルーティングテーブル自体は 300 エントリ）
※：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

ipv6 mtu

インタフェースの MTU 長を指定します。

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。	LAN：1280～1500 PPPoE：1280～1492 EWAN：1280～1500 MOBILE：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
MOBILE：1500

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
モバイルインタフェース設定モード

IPv4 ルーティングの設定

IPアドレスの設定

ip address

PPPoE 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。
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 158.xxx.xxx.1/24 に設定する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip address 158.xxx.xxx.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

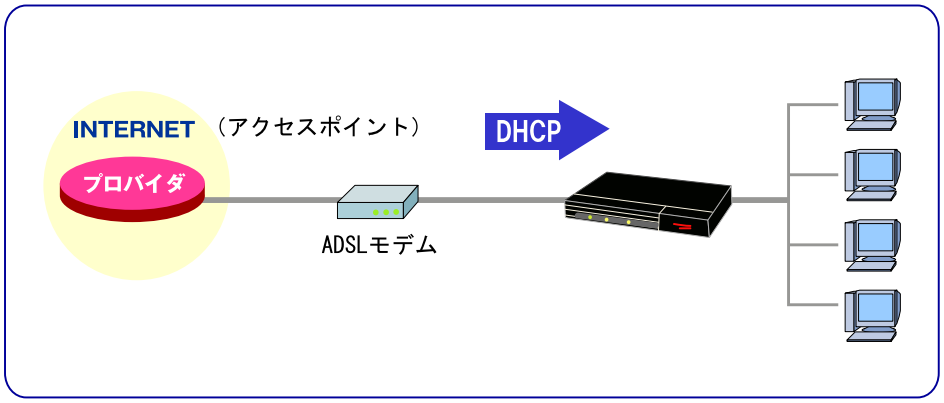
パラメータ	設定内容	設定範囲	省略時の値
IP アドレス	インタフェースに割り当てる IP アドレスを設定します。	IPv4 アドレス形式	省略不可
サブネットマスク	サブネットマスクを設定します。	IPv4 アドレス形式	省略不可

設定モード

PPPoE 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} < client-id >]
ip address dhcp [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} < client-id >	DHCP サーバから指定された、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
ホスト名	DHCP サーバから指定された、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-F120 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

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します。

```
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

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、インタフェース名称で決定します。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> | lan <1-1> | ewan <1-2> | pppoe <1-5>}

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
lan	RIP を運用するインタフェースを、lan1～1 に指定します。	1～1	省略不可
ewan	RIP を運用するインタフェースを、ewan1～2 に指定します。	1～2	省略不可
pppoe	RIP を運用するインタフェースを、pppoe1～5 に指定します。	1～5	省略不可

この設定を行わない場合

ど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 lan 1]

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
[source-interface lan 1]	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	-	実際に送信するインタフェース

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 { 1 | 2 } { 2 | 1 }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
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 or 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

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 { 1 | 2 } { 2 | 1 }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
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 or 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

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	254 文字の英数字	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

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 { text | md5 }
```

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
text ｜ md5	RIP2 で、パスワードを送る方式を選択します。	text	Simple Text	省略不可
		md5	MD5	

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

ip split-horizon

PPPoE 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。
Split-Horizon 制御を行なう場合は"enable"、行なわない場合は"disable"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　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 { 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	Split-Horizon 制御を行なうかどうかを指定します。	enable：制御を行なう disable：制御を行なわない	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 Poison 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。
FITELnet-F120 は、Split-Horizon with Poison 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

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 { lan <1-1> | ewan <1-2> | pppoe <1-5> }

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
lan	RIP の受信のみを行なうインタフェースを lan に指定します。	1	省略不可
ewan	RIP の受信のみを行なうインタフェースを ewan に指定します。	1～2	省略不可
pppoe	RIP の受信のみを行なうインタフェースを pppoe に指定します。	1～5	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 〈アクセスリスト番号〉{ in | out }〈メトリック値〉[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
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 1～5 dialer 1～20 vlanif 1～16	全インタフェースで適用

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>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>static</td><td>スタティックルーティング情報</td></tr></table></td><td>bgp
connected
kernel
local-prot1
local-prot2
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 { 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
バージョン	RIP のバージョンを指定します。	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

FITELnet-F120 が生成した経路情報（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。

FITELnet-F120 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 30 秒、経路情報を無効とするまでの時間を 180 秒、経路情報を削除するまでの時間を 120 秒とする

```
Router(config)#router rip
Router (config-rip)#timers basic 30 180 120
```

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 で保持されて広告されます。	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-F120 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）。
refresh コマンド後に有効になるコマンドです。

distance 値は、値が小さいほど優先度が高くなります。

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> <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
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。
アクセスリスト番号	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
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

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。
access-list コマンドで指定したアクセスリスト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。

設定例1　192.168.100.0/24 のアクセスリスト情報のみを受け付ける

```
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 のアクセスリスト情報のみを送信しない

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

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 のアクセスリスト情報を、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)#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 〈アクセスリスト番号〉{ in | out } [インタフェース名称]

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
アクセスリスト番号	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 受信時 out 送信時	省略不可
インタフェース名称	適用するインタフェースのインタフェース名称を指定します。	インタフェース名形式	全インタフェースで適用

※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。

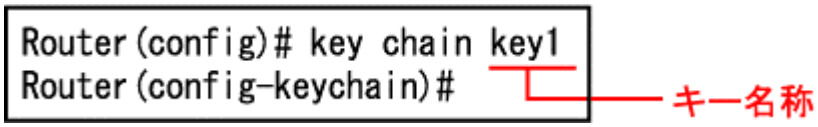
<受信可能条件>	unicastrip 設定がされている。
	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	受信した unicastrip の RIP バージョン(RIP1, RIP2) と、自身の RIP バージョン設定 (ip rip receive version(優先)もしくは router rip の version) が一致している。
	unicastrip 送信元アドレスへの経路がルーティングテーブルに事前に存在している。
<送信可能条件>	network コマンドで RIP サービスを動作させるインターフェース指定されている。
	neighbor 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)
FITELnet-F120 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"2003.4.1 12:00:00 - 2003.4.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 accept-lifetime 12:00:00 1 Apr
2003 11:59:59 30 Apr 2003
```

設定例2　number=1 の受信時有効期限を"2003.4.1 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 Apr
2003 infinity
```

設定例3　number=1 の受信時有効期限を"2003.4.1 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 Apr
2003 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"2003.4.1 12:00:00 - 2003.4.30 11:59:59"とする

```
Router(config)#key chain key-chain-1
Router(config-keychain)# key 1 send-lifetime 12:00:00 1 Apr 2003
11:59:59 30 Apr 2003
```

設定例2　number=1 の送信時有効期限を"2003.4.1 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 Apr 2003 infinity
```

設定例3　number=1 の送信時有効期限を"2003.4.1 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 Apr 2003
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
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

BGPに関する設定

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。
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

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-F120）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。
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-F120 の BGP 最適経路選択

FITELnet-F120 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-F120 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-F120 の BGP 最適経路選択

FITELnet-F120 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-F120 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-F120 の BGP 最適経路選択

FITELnet-F120 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 値の小さい 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-F120 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 { 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	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 とするかどうかを指定します。	enable	IPv4 とする	省略不可
		disable	IPv6 とする	

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 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 に設定します。

```
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-PREF 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 <scan-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
scan-time 値	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

scan-time 値は 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ディスタンス値を設定します。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> [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
distance 値	設定している経路のディスタンス値	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
アクセスリスト番号	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ディスタンス値を設定します。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 <external> <internal> <local>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
<external> <internal> <local>	external(EBGP), internal(IBGP), local それぞれについてディスタンス値を設定します。	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
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

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。
有効とする場合は"enable"、無効とする場合は"disable"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 { 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
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
enable | disable	指定している BGP ピアが有効か無効化を指定します。	enable 有効 disable 無効	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

自身がデフォルトルート情報を持っていない場合でも、ネイバにデフォルトルート情報を通知するようにします。
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)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

パラメータはありません。

この設定を行わない場合

デフォルトルートを通知しません。

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 〈アクセスリスト番号〉 { 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
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アクセスリスト番号を指定します。	1-99 1300-1999	省略不可
in | out	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 受信時 out 送信時	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。refresh コマンド後に有効になるコマンドです。
FITELnet-F120 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)

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

パラメータはありません。

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

```
Rouer(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

パラメータはありません。

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、FITELnet-F120 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

パラメータはありません。

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 port <0-65535>

BGP ピアが使用するの TCP ポート番号を指定します。
FITELnet-F120 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> { 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
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
{ in | out }	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 受信時 out 送信時	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。

設定例1 BGP ピア(10.0.0.1)に対応する KeepAlive の送信間隔を 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 20
```

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 送信間隔	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
インタフェース名称	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。	インタフェース名形式	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。
4 は BGP バージョン 4, draft は BGP バージョン 4 マルチプロトコル拡張ドラフト版を表します。
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

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-F120 の BGP 最適経路選択

FITELnet-F120 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-F120 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>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><tr><td>static</td><td>スタティックルーティング情報</td></tr></table></td><td>connected
kernel
local-prot1
local-prot2
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。

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

FITELnet-F120 では、常にインターネットに接続しており、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。
FITELnet-F120 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>][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>][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>

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

		conversion-error	
		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	

		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	全てのICMPv6 タイプ

		ICMPv6 タイプ値（0～255）	
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	全ての TCP ポート番号

		pop3 smtp sunrpc syslog 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	全ての UDP ポート番号

		talk tftp time who xdmcp UDP ポート番号（0～65535）	
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。

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

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)#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 〈アクセスリスト番号〉{ 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
アクセスリスト番号	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 ※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。	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

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
IPsec インタフェース設定モード

スタティックルーティングの設定

ip route

FITELnet-F120 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 <1-4> | null 0 } } [<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	インタフェース名称を設定する必要があります
インタフェース名称	宛先へ到達するためのインタフェース名称 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する	ewan 1～2 pppoe 1～5 dialer 1～4	NextHop の IP アドレスを設定する必要があります。
connected ipsecif <1-4>	宛先への経路として、IPsec インタフェースを指定します。	ipsecif <1-4>	
connected null 0	廃棄用の宛先経路情報とします	null 0	
distance	スタティックルーティングの distance 値を指定します。	2～255※	1

最大エントリ数：128 エントリ（ルーティングテーブル自体は 300 エントリ）
※：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
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

設定モード

基本設定モード

マルチルーティングの設定

multiroute static

マルチルーティングの経路情報テーブルを登録します。

設定例1　192.168.50.0/24 発のデータは、PPPoE#1 に送信する

```
Router(config)#multiroute static 192.168.50.0 0.0.0.255 any pppoe 1
```

設定例2　192.168.100.0/24 宛のデータは、PPPoE#2 に送信する

```
Router(config)#multiroute static any 192.168.100.0 0.0.0.255 pppoe 2
```

設定例3　SMTP（ポート 25/tcp）のデータは、NextHop=192.168.100.1 に送信する

```
Router(config)#multiroute static any any port 25 25 nexthop 192.168.100.1
```

設定例4　URL が、www.furukawa.co.jp 宛のデータは、PPPoE#5 に送信する

```
Router(config)#multiroute static any url www.furukawa.co.jp pppoe 5
```

コマンド書式

multiroute staic { 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〉 } { any | url 〈宛先 URL〉 | host 〈宛先 IP アドレス〉 | 〈宛先 IP アドレス〉〈宛先 Wildcard マスク〉 } [port 〈宛先先頭ポート番号〉 [〈宛先最終ポート番号〉]] { nexthop 〈IP アドレス〉 | 〈インタフェース名称〉 } [preference 〈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
any	送信元／宛先アドレスの設定において、「全て」を指定する場合は"any"を入力します。	any	-
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
宛先 URL	宛先 URL を指定します。	64 文字以内の文字列	省略不可
宛先先頭ポート番号	マルチルーティング対象とする宛先ポート番号の先頭の値を指定します。	0～65535	全てのポート番号
宛先最終ポート番号	マルチルーティング対象とする宛先ポート番号の最後の値を指定します。	0～65535	宛先先頭ポート番号が指定されていない場合は、全てのポート番号 宛先先頭ポート番号が指定されている場合は、そのポート番号のデータのみ
インタフェース名称	データを送信するインタフェースの名称を指定します。	インタフェース名称（LAN、EWAN 以外）	省略不可
nexthop〈IP アドレス〉	nexthop の IP アドレスを指定します。	IPv4 アドレス形式	
優先度	同じデータの指定が、複数のテーブルに存在した場合の優先度を指定します。 値が小さいほど、優先度は高くなります。	0～31	0

最大エントリ数：32 エントリ

この設定を行わない場合

マルチルーティング機能を使用することはできません。

マルチルーティングとは？

通常のデータ通信では、経路テーブルにしたがって、データ中継を行ないますが、特定のデータだけは経路テーブルでなく、別の経路からデータ中継を行ないたいケースで、マルチルーティング機能を使用します。

例えば、フレッツサービスで提供されているフレッツスクエアを利用するような場合に便利な機能です。

・通常のデータは、デフォルトルート（例えば PPPoE1）で通信するが、フレッツスクエアの場合は PPPoE2 を使用して通信を行なう。

このような場合は、設定例４のように、

```
multiroute static any url www.flets pppoe2
```

と設定し、PPPoE2 の設定で、ユーザ ID：guest@flets／パスワード：guest と設定することにより、設定変更なしでフレッツスクエアを利用できます。

設定モード

基本設定モード

multiroute exclusive

multiroute static コマンドで指定したマルチルーティングテーブルのなかで、このデータだけは通常ルーティングテーブルに従い中継をするという場合に、通常ルーティングするデータを登録します。

設定例2　192.168.50.0/24 発のデータは、PPPoE#1 に送信するが、192.168.50.1 発のデータは、通常ルーティグする

```
Router(config)#multiroute static 192.168.50.0 0.0.0.255 any pppoe 1
Router(config)#multiroute exclusive host 192.168.50.1 any
```

設定例2　192.168.100.0/24 宛のデータは、PPPoE#2 に送信するが、192.168.100.254 宛のデータは、通常ルーティングする

```
Router(config)#multiroute static any 192.168.100.0 0.0.0.255 pppoe 2
Router(config)#multiroute exclusive any host 192.168.100.254
```

コマンド書式

multiroute exclusive { 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〉} { any | url 〈宛先 URL〉 | host 〈宛先 IP アドレス〉 | 〈宛先 IP アドレス〉〈宛先 Wildcard マスク〉} [port 〈宛先先頭ポート番号〉 [〈宛先最終ポート番号〉]]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
any	マルチルーティング対象外とする送信元／宛先アドレスの設定において、「全て」を指定する場合は"any"を入力します。	any	-
host	マルチルーティング対象外とするマルチルーティング対象外とする送信元/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	マルチルーティング対象外とする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	マルチルーティング対象外とする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	マルチルーティング対象外とする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	マルチルーティング対象外とする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
宛先 URL	マルチルーティング対象外とする宛先 URL を指定します。	64 文字以内の文字列	省略不可
宛先先頭ポート番号	マルチルーティング対象外とする宛先ポート番号の先頭の値を指定します。	0～65535	全てのポート番号
宛先最終ポート番号	マルチルーティング対象外とする宛先ポート番号の最後の値を指定します。	0～65535	宛先先頭ポート番号が指定されていない場合は、全てのポート番号 宛先先頭ポート番号が指定されている場合は、そのポート番号のデータのみ

最大エントリ数：16 エントリ

この設定を行わない場合

マルチルーティングテーブルに登録したデータは、全て設定に従います。

マルチルーティングとは？

通常のデータ通信では、経路テーブルにしたがって、データ中継を行ないますが、特定のデータだけは経路テーブルでなく、別の経路からデータ中継を行ないたいケースで、マルチルーティング機能を使用します。

例えば、フレッツサービスで提供されているフレッツスクエアを利用するような場合に便利な機能です。

- 通常のデータは、デフォルトルート（例えば PPPoE1）で通信するが、フレッツスクエアの場合は PPPoE2 を使用して通信を行なう。

  このような場合は、設定例４のように、

  ```
  multiroute static any url www.flets pppoe2
  ```

  と設定し、PPPoE2 の設定で、ユーザ ID：guest@flets／パスワード：guest と設定することにより、設定変更なしでフレッツスクエアを利用できます。

設定モード

基本設定モード

ルートマップの設定

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-F120 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

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。

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。

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。

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。

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。

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。

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-EXPORT-SUBCONFED コミュニティ	省略不可
		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。

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-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	local-AS no-advertise no-export A:B	省略不可

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。

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。

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	省略不可
		igp	IGP を設定する	
		incomplete	IMCOMPLETE を設定する	

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。

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 weight

BGP ピアから受信した経路情報の weight 値を設定します。

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

インタフェースを特定します。
この設定は、RIP および BGP に対して有効となります。
ここで指定したインタフェースに対してどのような処理をするかの設定となります。

refresh コマンド後に有効になるコマンドです。

設定例1　RIP で直接ルートの情報を LAN インタフェースにのみ送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match interface lan 1
Router(config-rmap map1 permit 1)#exit


Router(config)#router rip
Router(config-rip)#redistribute connected route-map map1
```

設定例2　BGP で直接ルートの情報を LAN インタフェースのみ送信する（ルートマップ名：map1）

```
Router(config)#route-map map1 permit 1
Router(config-rmap map1 permit 1)#match interface lan 1
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 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	特定するインタフェース名称を指定します。	インタフェース名形式	省略不可

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 〈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	IP アドレスに一致するアクセスリスト番号を指定します	-	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。
各経路情報のうち、指定した Next-Hop の情報をもつ経路情報に対してどのような処理をするかの設定となります。

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 〈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	Next-hop に一致するアクセスリスト番号を指定します	-	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。
ここで指定したメトリック値をもつ経路情報に対してどのような処理をするかの設定となります。

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

FITELnet-F120 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-F120 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-F120 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 domainname 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 domain-name

FITELnet-F120 で、DNS リゾルバを動作させる場合に、ドメイン名を付加させたい場合に設定します。
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 domainname 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 リゾルバで通知する際に付加するドメイン名を"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。

設定モード

基本設定モード

ip resolver-cache-time

FITELnet-F120 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（単位：秒）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）	0～60	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

MTU長

ip mtu

インタフェースの MTU 長を指定します。

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 IPsecIF：576～1500 MOBILE：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
IPsecIF：1390
MOBILE：1500

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
IPsec インタフェース設定モード
モバイ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 長を指定します。
FITELnet-F120 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。

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〉〈off | 設定値〉
mss ipsec 〈off | 設定値〉

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 1～5 ipsecif 1～4		省略不可
ipsec	VPN セレクタの MSS 長を指定します。	off	mss 値を変更しません	省略不可
off ｜ 設定値	MSS 長を指定します。	設定値	1240～1460※	

※：ipsec と pppoe の設定値の上限は、ipsec 1420、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

MSS 長とは？

MSS (Maximum Segment Size)とは、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。

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。

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

ICMP制御の設定

ip source-quench

ICMPv4 の 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 {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	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：反映する disable：反映しない	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

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

IPsec機能の設定

IPsec基本コマンド

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 { <1～2>| all }][mobile 1]

パラメータ

パラメータ	設定内容		設定範囲	省略時の値
[ewan { <1～2>| all }][mobile 1]	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 all mobile 1	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。
	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。		
	mobile 1	mobile に適用します。		

※：対象とする EWAN ポートを利用する PPPoE インタフェースにも適用されます。

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-F120 の vpnlog とは？

FITELnetーF120 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

パラメータ	設定内容	設定範囲		省略時の値
認証方式	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。	prekey	Pre-Shared Key 認証・拡張認証なし	省略不可
		prekeyxauth	Pre-Shared Key 認証・拡張認証あり	
		rsasig	RSA signature 認証・拡張認証なし	
		rsasigxauth	RSA signature 認証・拡張認証あり	

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-F120 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 3des	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)の 2 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 or 2	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-F120 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 認証使用時の Phase 1 における自身の ID タイプを指定します。
電子証明書には、以下の情報が格納されております。

電子メールアドレス	電子証明書所有者の電子メールアドレス	email
ドメイン名	電子証明書所有者の存在するドメインの名称	domain
IP アドレス	電子証明書所有者の端末の IP アドレス	ip

この情報のうち、どの情報を通知するかを選択します。
電子証明書の情報は使用せずに、任意の文字列を ID タイプとする場合は、DN (Distinguished Name) 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　RSA signatures 認証使用時の ID タイプに「email」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 認証に使用する ID タイプを指定します。	email domain ip dn	省略不可

この設定を行わない場合

domain-name 値を使用します。

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-NAT 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。

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。

コマンド書式

【NAT 時】　ip vpn-nat inside source list〈アクセスリスト番号〉[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〈アクセスリスト番号〉[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〉

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	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	NAT+の場合は省略不可
		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	IPv4 アドレス形式		省略不可

	を指定します。		
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

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。
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。

コマンド書式

【NAT スタティック（複数指定）時】　ip vpn-nat inside destination list 〈アクセスリスト番号〉[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]

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	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〈アクセスリスト番号〉：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たアドレス peer〈IP アドレス〉：VPN ピアから指定されて設定した IP アドレス	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。	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

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。
FITELnet-F120 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。

FITELnet-F120 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。
対向の装置がこれらの方式を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 | icmp [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
always-send | response-only | icmp [always-send] | disable	KeepAlive 機能を指定します。	icmp	ICMP を利用した KeepAlive を行なう	省略不可
		disable	KeepAlive 機能を使用しない	
		always-send	VPN データが送信されなくても、常に KeepAlive を送信します	
		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	

この設定を行わない場合

IKE の KeepAlive を行なう。

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 <lan 1>

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	IPv4 アドレス形式	VPN ピア
<lan 1>	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アドレス	lan 1：LAN インタフェースの IP アドレスを使用する	使用する WAN 側インタフェースの IP アドレス

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、FITELnet-F120 のもつ経路情報に従って送信されますが、keepalive-icmp 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>| interface {ewan <1-2> | pppoe <1-5>}}

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	IPv4 アドレス形式		VPN ピア
interface {ewan <1-2> | pppoe <1-5> }	ICMP の KeepAlive を送信するインタフェースアドレス	ewan <1-2>	EWAN を指定します	省略不可
		pppoe <1-5>	pppoe を指定します	

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。
cyrpto 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 {ewan <1-2> | pppoe <1-5> }}

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	IPv4 アドレス形式		VPN ピア
interface {ewan <1-2> | pppoe <1-5> }	ICMP の KeepAlive を送信するインタフェースアドレス	ewan <1-2>	EWAN を指定します	省略不可
		pppoe <1-5>	pppoe を指定します	

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

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。

※Pre-Shared Key･･･一般に「事前共有鍵」「共有秘密鍵」とも呼ばれます。

refresh コマンド後に有効になるコマンドです。

設定例1 Pre-Shared Key に文字列の"secretF120"設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#key ascii secretF120
```

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 Key>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
ascii | binary	Pre-shared Key を文字列として扱うか、16 進数として扱うかを指定します。	ascii：文字列として扱う binary：16 進数として扱う	省略不可
Pre-shared Key	Pre-shared Key を指定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

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、"F120"を設定する

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#my-identity F120
```

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 "F120"）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-F120 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。
※FITELnet-F120 では IPsec 時に IKE KeepAlive を行います（初期値）

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-Traversal 機能を使用する。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。	1～300	送信間隔を設定します。	5
		off	使用しない	

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-F120 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 f120no1 -> ○

・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指定します	main	Main モード	省略不可
		aggressive	Aggressive モード	

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 アドレスもしくは名称を設定します。
名称は、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 ピアの名称として、"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〉
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 アドレスを設定します。	IPv4 アドレス形式	省略不可
VPN ピアのホスト名称	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	省略不可

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-F120 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

VPN ピアにおける証明書 SubjectName 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　証明書 SubjectName に、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

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
distinguished-name	VPN ピアにおける証明書の SubjectName を指定します。	-	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

電子証明書に、SubjectName を含め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 を消去しません。

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	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 インタフェース番号を指定します。	1～2	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 となりますが、１台の装置で有効となる VRID は２つまでとなります。同一の VRID を複数のインターフェースに適用することは可能です。

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。

設定モード

IKE ポリシー設定モード

tunnel-route

IPsec 通信において、FITELnet-F120 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 <1-5>}}

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 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
interface <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 1～2 pppoe 1～5	

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-F120 では、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 を登録します。

```
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 128 ビット esp-aes-192…AES 192 ビット esp-aes-256…AES 256 ビット esp-none…暗号化しない	esp-des esp-3des esp-aes-128 esp-aes-192 esp-aes-256 esp-none	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

IPsec の通信を行なうことができません。

設定モード

基本設定モード

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、FITELnet-F120 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。
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 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。	インタフェース名称	

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、FITELnet-F120 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 <1-5>}}

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 1～2 pppoe 1～5	

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 {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：EWAN を指定します。 pppoe 1～5：PPPoE を指定します。 dialer 1～4：ダイヤルアップを指定します。 Ipsecif 1～4：Ipsecif を指定します。	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：経路情報を広告す	rip で metric 1 で配信します。

		local-prot2	
distance	スタティックルーティングの distance 値を指定します。	1～255	0

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-F120"、パスワードを"F120-pass"とする

```
Router(config)# crypto isakmp policy 1
Router(config-isakmp)#aaa my-name FITELnet-F120 password F120-pass
```

コマンド書式

aaa my-name〈ユーザ名〉password〈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）される場合の自身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）される場合の自身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

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

接続相手を拡張認証（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）される場合の自身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）される場合の自身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

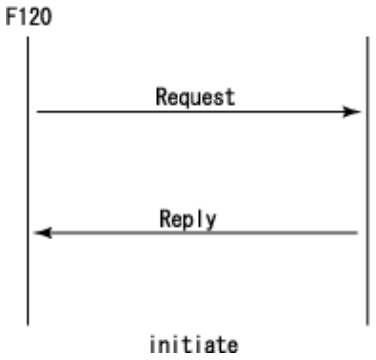
set-ack モードで動作し、set の受信待ちをします。
Mode Config を使用する場合は、ip vpn-nat inside source コマンドで modeconfig で割り当てられた NAT+変換する設定を行う必要があります。

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。

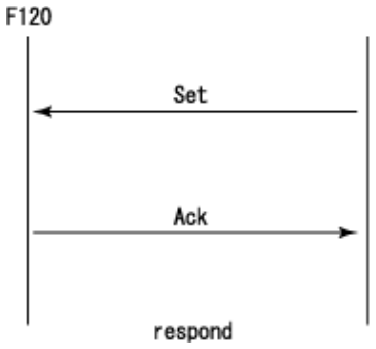
1）configuration mode initiate を指定した場合

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

ダイヤルアップ接続で AIR-EDGE を使用した場合、4x や 8x パケット方式のように複数のチャンネルを使って通信すると、パケットの到着順が前後することがあり、IPsec 通信においては 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 {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	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。	省略不可
		disable	全てのパケットを受信します。	

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

aaa peer-name

相手を拡張認証する場合の、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	相手を拡張認証する場合の相手のユーザ名を設定します。	-	省略不可
パスワード	相手を拡張認証する場合の相手のパスワードを設定します。	-	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

crypto map

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ます

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

最大エントリ：64 エントリ

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
モバイル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

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-アクセスリスト番号〉{ 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-アクセスリスト番号	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）	1～64	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	省略不可

		bypass: 透過対象とする discard: 廃棄対象とする	
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す。	TCP ポート番号（0～65535）	省略不可
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：64 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 アクセスリスト番号を指定します。

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 アクセスリスト番号> [1st | 2nd | multi-path [balance 0-10]]

パラメータ

パラメータ	設定内容	設定範囲		省略時の値
IPsec アクセスリスト番号	暗号化するパケットとして、IPsec アクセスリスト番号を指定します。	1～64		省略不可
1st | 2nd | multi-path [balance {0-10}]	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。	1st	IPsec 冗長機能のメイン回線を指定します。	IPsec 冗長機能を使用しないセレクタになります。
		2nd	IPsec 冗長機能のバックアップ回線を指定します。	
		multi-path	IPsec 負荷分散を行う場合指定します。	
		balance 0-10	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。	

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

set peer

設定している crypto map が SA を確立する VPN ピアの IP 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>
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	VPN ピアの IP アドレスを指定します。 IKE ポリシー設定モードで設定した VPN ピアの IP アドレスと同じアドレスである必要があります。	IPv4 アドレス形式	省略不可
VPN ピアのホスト名	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 IP アドレスと同じアドレスである必要があります。	-	省略不可

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。
group1 は 768-bit Diffie-Hellman、group2 は 1024-bit Diffie-Hellman 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 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	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-F120 では、工場出荷時は、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 security-association always-up

SA の確立状態を確保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 F120（固定 IP）-----拠点側 F120（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
```

※ 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。

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

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。	-	省略不可

この設定を行わない場合

IPsec を使用することはできません。

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 で関連づけられ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-F120 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
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

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

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

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 { must | notuse}

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>must | notuse</td><td>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：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。</td><td>must
notuse</td><td>省略不可</td></tr>
</table>

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

電子証明書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　電子証明書に含める電子メールアドレスとして、F120@xxxxx.ne.jp を設定する

```
Router(config)#crypto ca identity
Router(config-ca-identity)#email F120@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	電子証明書に含める電子メールアドレスを設定します。	-	省略不可

この設定を行わない場合

電子証明書に、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

電子証明書に含める 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　電子証明書に含める 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	電子証明書に含める 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

電子証明書に、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

電子証明書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　電子証明書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	電子証明書に含めるドメイン名称	-	省略不可

この設定を行わない場合

電子証明書に、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

CA との認証を行うためののネームサーバーの 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	CA との認証を行なうためのネームサーバの IP アドレスを指定します。	IPv4 アドレス形式	省略不可

設定モード

電子証明書（自身の ID）設定モード

query-ip

CA との認証を行うための 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	CA との認証を行なうための LDAP 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

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

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。
refresh コマンド後に有効になるコマンドです。

設定例1 IPsec ログモードに移行します。

```
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

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。

設定例1　192.168.0.1 の block type discard を制御する設定をします。

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-block-type-discard 192.168.0.1
```

コマンド書式

crypto ipsec-log 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。

設定例1 "SPI no match ～"の vpnlog を抑制する設定を行います。

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#nolog-spi-no-match
```

コマンド書式

crypto ipsec-log 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。

設定例1　keepalivefail の vpnlog 出力を全て表示します。

```
Router(config)#crypto ipsec-log
Router(config-ipsec-log)#vpnlog-detail all
```

コマンド書式

crypto ipsec-log 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	全てのピア番号が対象となります	全パス対象に全てのログを表示します。
		eq 1～32	指定するピア番号を持つパスが対象となります。	
		gt 1～31	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 2～32	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 1～32	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 1～32 1～32	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。	

設定モード

IPsec ログモード

IPsecの各種設定

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：A B C 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

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]

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

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。

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します。

```
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

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。
設定する内容は以下です。

内容	パラメータ	備考
１回の KeepAlive で送信する ICMP の数 また、そのうち応答を受け取れなかったときに SA の障害と判定する数	count	送信数を１番目のパラメータに SA の障害とみなす数を２番目のパラメータに設定する
ICMP KeepAlive の送信間隔（秒）	freq	
ICMP KeepAlive の応答待ち時間（秒） この時間をこえて応答がなければ応答なしとみなす	timeout	

設定例1　1 回の KeepAlive で4つの ICMP を送信する、そのうち3つの応答を受け取れなかった場合に 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　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3　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>
alive 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	1～15	省略不可
ICMP 失敗数	1 回の KeepAlive で送信した ICMP 数のうち、応答を受け取れなかったときに SA の障害と判定する数	1～15	省略不可
送信間隔	ICMP KeepAlive の送信間隔（秒）	5～1000	省略不可
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
送信間隔	60 秒
timeout 時間	3 秒

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

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 FITELnet-F120 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

FITELnet-F120 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、FITELnet-F120 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 FITELnet-F120 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 FITELnet-F120 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
再送間隔	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

NAT機能

NAT機能

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 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-F120 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-F120 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-timeou)
・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(PPPoE)

LAN 側から PPPoE 側への 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、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 pppoe 1
Router(config-if pppoe 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 <LAN 側のアドレス範囲> <PPPoE 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。
<PPPoE 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 pppoe 1
Router(config-if pppoe 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 <LAN 側のアドレス範囲> <PPPoE 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。
<PPPoE 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 pppoe 1
Router(config-if pppoe 1)#ip nat inside source static 192.168.0.1
158.xxx.xxx.2
Router(config-if pppoe 1)#ip nat inside source list 1 pool pool1
Router(config-if pppoe 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 〈LAN 側のアドレス〉〈PPPoE 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、PPPoE→LAN 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 pppoe 1
Router(config-if pppoe 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 〈ローカルネットワークアドレス〉〈グローバル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> [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。	NAT プール名	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
ローカルネットワークアドレス	変換前のローカル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
グローバルネットワークアドレス	変換後のグローバル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	IPv4 アドレ	省略不可

	た単位で一括設定します。	ス形式	

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 PPPoE 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

PPPoE インタフェース設定モード

ip nat inside source(EWAN)

LAN 側から WAN 側への 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、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 ewan 1
Router(config-if ewan 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 <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 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 ewan 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 <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 ewan 1
Router(config-if ewan 1)#ip nat inside source static
192.168.0.1 158.xxx.xxx.2
Router(config-if ewan 1)#ip nat inside source list 1 pool pool1
Router(config-if ewan 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 〈LAN 側のアドレス〉〈WAN 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、WAN→LAN 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 ewan 1
Router(config-if ewan 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 〈ローカルネットワークアドレス〉〈グローバル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>［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 <ローカルネットワークアドレス><グローバル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（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。	NAT プール名	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
ローカルネットワークアドレス	変換前のローカル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
グローバルネットワークアドレス	変換後のグローバル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

設定している EWAN 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

EWAN インタフェース設定モード

ip nat inside source(ダイヤルアップ)

LAN 側から WAN 側への NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モードの場合で、設定のしかたが異なりますので注意してください。

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 dialer 1
Router(config-if dialer 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 <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 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 dialer 1
Router(config-if dialer 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 <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 dialer 1
Router(config-if dialer 1)#ip nat inside source static
192.168.0.1 158.xxx.xxx.2
Router(config-if dialer 1)#ip nat inside source list 1 pool
pool1
Router(config-if dialer 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〈LAN 側のアドレス〉〈WAN 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、WAN→LAN 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 pppoe 1
Router(config-if pppoe 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〈ローカルネットワークアドレス〉〈グローバル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> [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 <ローカルネットワークアドレス> <グローバル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（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。	NAT プール名	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
ローカルネットワークアドレス	変換前のローカル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
グローバルネットワークアドレス	変換後のグローバル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

設定している dialer 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

ダイヤルアップインタフェース設定モード

ip nat inside destination(PPPoE)

PPPoE 側から LAN 側への 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、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 pppoe 1
Router(config-if pppoe 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1
```

【解説】
ip nat inside destination static 〈PPPoE 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 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 pppoe 1
Router(config-if pppoe 1)#ip nat inside destination static
158.xxx.xxx.2 1500 192.168.0.1 80
```

【解説】
ip nat inside destination static 〈PPPoE 側アドレス PPPoE 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 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 pppoe 1
Router(config-if pppoe 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〈グローバルネットワークアドレス〉〈ローカル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（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。	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	1～65535	ポート変

	す。		換しない
グローバルネットワークアドレス	変換前のグローバル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
ローカルネットワークアドレス	変換後のローカル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 64 エントリ

この設定を行わない場合

設定している PPPoE 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

PPPoE インタフェース設定モード

ip nat inside destination(EWAN)

WAN 側から LAN 側への 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、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 ewan 1
Router(config-if ewan 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1
```

【解説】
ip 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 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 ewan 1
Router(config-if ewan 1)#ip nat inside destination static
158.202.232.1 1500 192.168.0.1 80
```

【解説】
ip 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 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 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〈グローバルネットワークアドレス〉〈ローカル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〈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〈グローバルネットワークアドレス〉〈ローカル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（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。	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

グローバルネットワークアドレス	変換前のグローバル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
ローカルネットワークアドレス	変換後のローカル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 64 エントリ

この設定を行わない場合

設定している EWAN 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

EWAN インタフェース設定モード

ip nat inside destination(ダイヤルアップ)

LAN 側から WAN 側への 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、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 ewan 1
Router(config-if ewan 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 <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 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 ewan 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 <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 ewan 1
Router(config-if ewan 1)#ip nat inside source static
192.168.0.1 158.xxx.xxx.2
Router(config-if ewan 1)#ip nat inside source list 1 pool pool1
Router(config-if ewan 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 〈LAN 側のアドレス〉〈WAN 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、WAN→LAN 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 ewan 1
Router(config-if ewan 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 〈ローカルネットワークアドレス〉〈グローバル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>［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 <ローカルネットワークアドレス><グローバル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（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。	NAT プール名	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
ローカルネットワークアドレス	変換前のローカル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
グローバルネットワークアドレス	変換後のグローバル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

設定しているダイヤルアップ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

ダイヤルアップ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〉

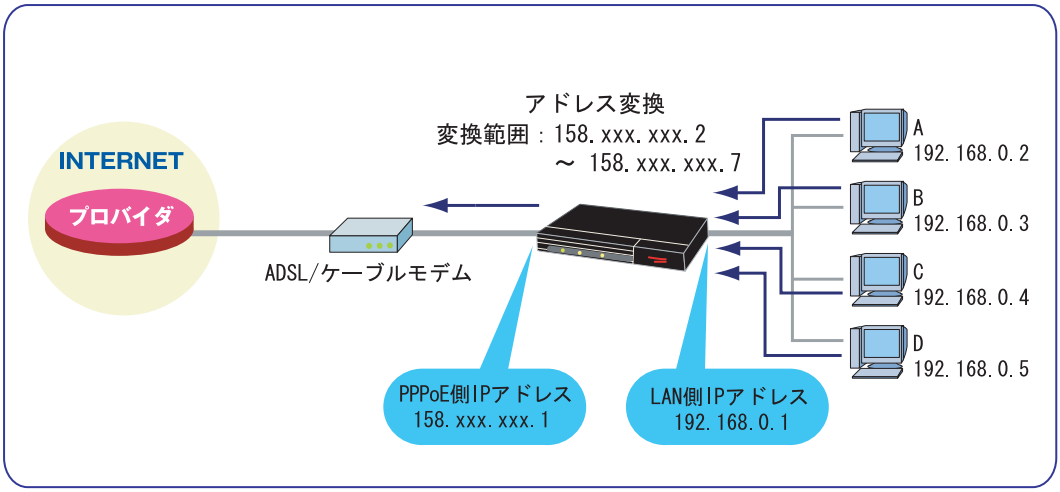
パラメータ

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。	-	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

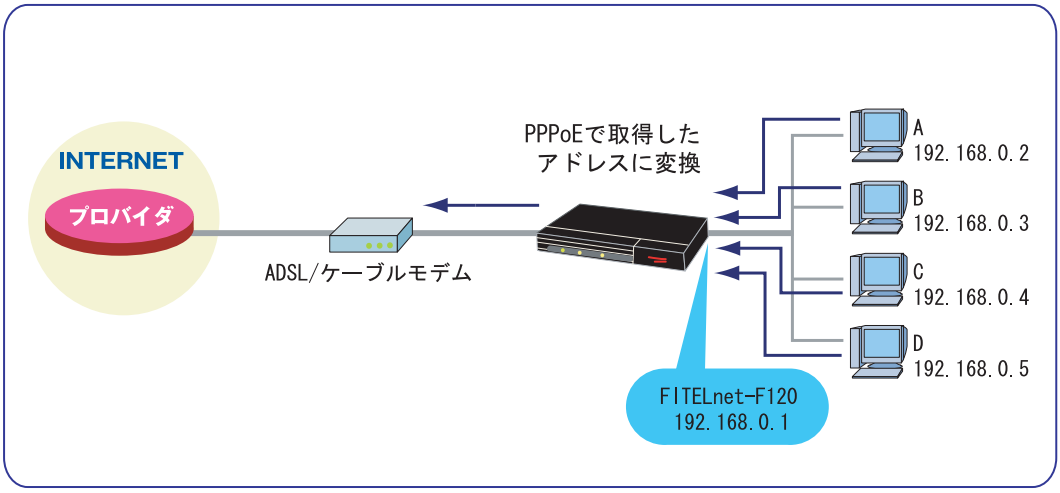
最大エントリ：8 エントリ

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-F120 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

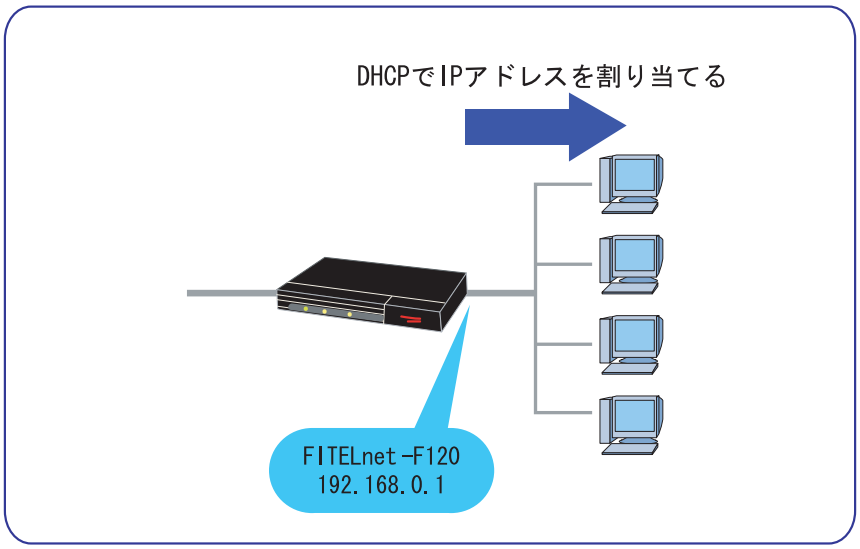
パラメータ

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-F120 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-F120 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-F120 の LAN/EWAN2 インタフェースで、FITELnet-F120 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 lan 1
Router(config-dhcp-pool)#
```

コマンド書式

```
ip dhcp pool { lan 1 | ewan 2 }
```

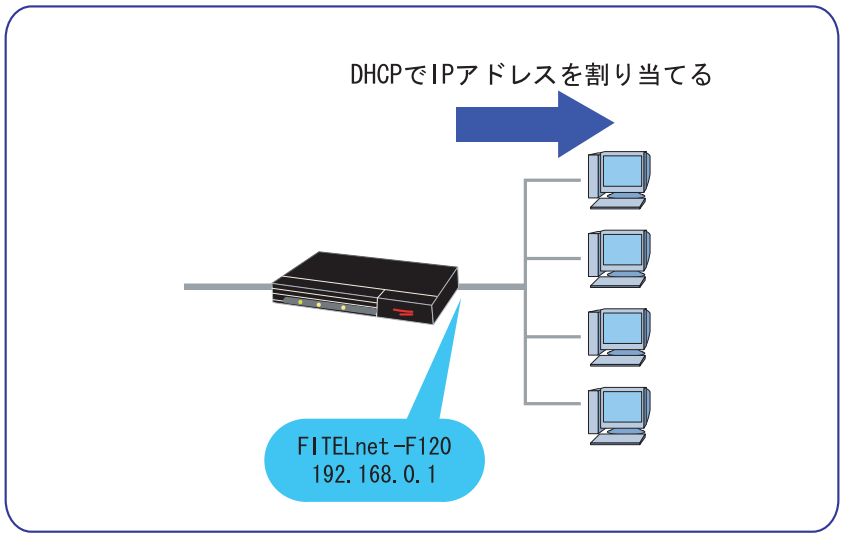
パラメータ

パラメータ	設定内容	設定範囲		省略時の値
lan 1 | ewan 2	DHCP サーバ機能を使用するインタフェースを選択します。	lan 1	LAN インタフェースで使用する	省略不可
		ewan 2	EWAN2 インタフェースで使用する	

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-F120 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-F120 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

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。

設定例1

```
Router(config)# service dhcp-relayagent
```

コマンド書式

service dhcp-relayagent

パラメータ

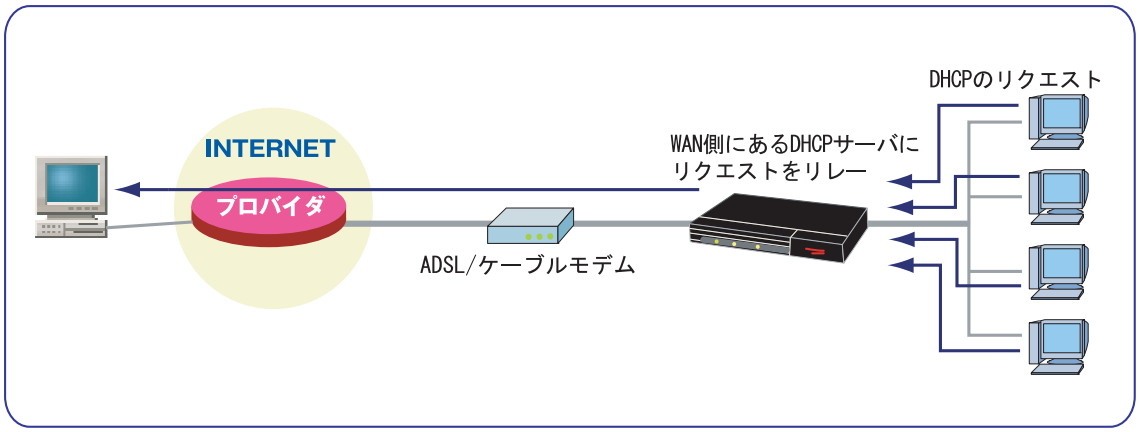
パラメータはありません。

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>

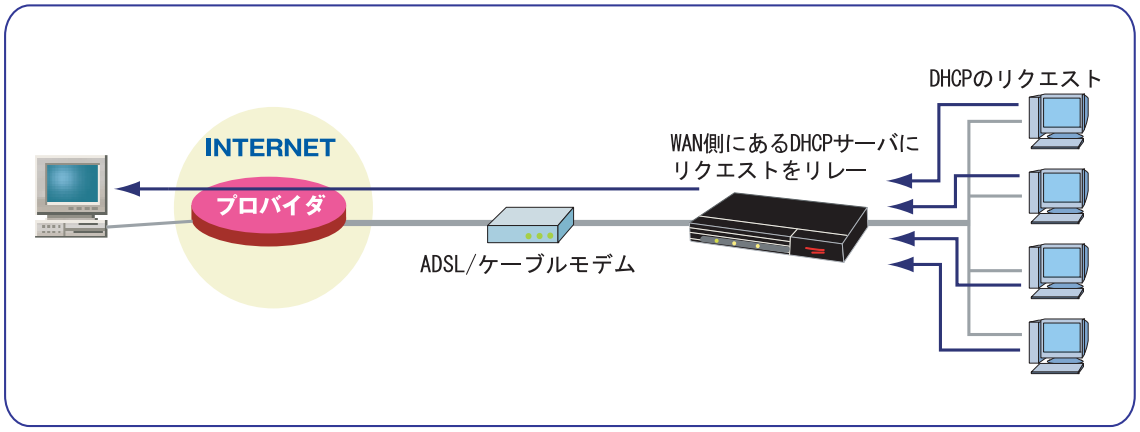
パラメータ

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？



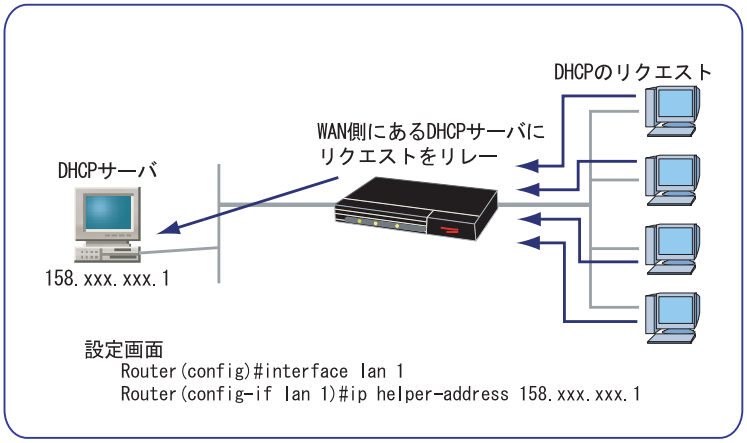
LAN 上の DHCP クライアントからの要求を、WAN 側にリレーし、WAN 側の DHCP サーバから割り当ててもらう機能です。
本社側で、支店の LAN 側の IP アドレスを一括で管理する場合に有効な機能です。

設定モード

基本設定モード

ip helper-address

FITELnet-F120 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-F120 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 lan 1]

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
[source-interface lan 1]	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	-	実際に送信するインタフェース

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

簡易DNS機能

簡易DNS機能の設定

proxydns mode

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 とも、簡易 DNS 機能を使用する

```
Router(config)# proxydns mode both
```

設定例2 IPv4 のみ簡易 DNS 機能を使用する

```
Router(config)# proxydns mode v4
```

コマンド書式

proxydns mode { v4 | v6 | both}

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 | both	ProxyDNS が動作するプロトコル （IPv4 or IPv6）を指定。 両方のプロトコルで動作する場合は both	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 or v6	省略不可
プライマリ DNS アドレス	ProxyDNS で使用するプライマリ DNS サーバの IP アドレス	IPv4 アドレス形式もしくは IPv6 アドレス形式	省略不可
セカンダリ DNS アドレス	ProxyDNS で使用するセカンダリ DNS サーバの IP アドレス	IPv4 アドレス形式もしくは 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(単位：秒)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 サーバからの応答を待つ時間（秒）	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 60
```

コマンド書式

proxydns default cache-time {off | <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	ProxyDNS のテーブル保持時間（秒）	0～259200	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〈インタフェース名称〉〈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
インタフェース名称	送信元アドレスとして指定するインタフェース	lan 1	省略不可
インタフェース番号	送信元アドレスとして指定するインタフェース番号	1	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

ip resolver-cache-time

FITELnet-F120 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（単位：秒）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）	0～60	省略不可

この設定を行わない場合

60 秒が設定されます。

DNS リゾルバとは・・・

FITELnet-F120 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-F120 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 domainname 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

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〉

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。

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
DNS アドレス	DNS サーバの IP アドレス	IPv4 アドレス形式または IPv6 アドレス形式	省略不可

最大エントリ数：8 エントリ

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。FITELnet-F120 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〉

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。

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	ホスト名	-	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 アドレス形式または 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）

設定モード

基本設定モード

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

IPパケット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（PPPoE、LAN、EWAN）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）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）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、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 〈アクセスリスト番号〉{ 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
アクセスリスト番号	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

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。（モバイルは除く）

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 〈アクセスリスト番号〉{ 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
アクセスリスト番号	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 ※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。	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
モバイルインタフェース設定モード

学習フィルタリング機能

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、PPPoE インタフェースで適用します。
フィルタリングデータは、PPPoE インタフェースで受信したパケットに適用するのか／PPPoE 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、PPPoE1 送信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip access-group 1 out
```

設定例2　access-list 2 で指定したデータを、PPPoE1 からの受信時に適用する

```
Router(config)#interface pppoe 1
Router(config-if pppoe 1)#ip access-group 2 in
```

コマンド書式

ip access-group 〈アクセスリスト番号〉 { 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
アクセスリスト番号	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 PPPoE 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

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（単位：分）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）	1～60 off：自動ログアウトしない	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（単位：分）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）	1～60 off：自動ログアウトしない	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）	1～60 off：自動ログアウトしない	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

QoS/CoS機能

QoS／CoS機能

qos 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。

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 bandwidth 100M cbq
```

コマンド書式

qos bandwidth <最大使用帯域> [cbq | priq]

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
cbq | priq	QoS の方式を指定します。	cbq CBQ 方式 priq PRIQ 方式	QoS 制御を行なわない（常にベストエフォート）

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。

CBQ とは？

CBQ は、Class-Based Queueing の略です。
キューイングを行なう際の処理に、データの指定された帯域にクラス分けし、その帯域の優先順位に従って送信処理を行なう方式です。
CBQ では、階層的なクラス構造を指定でき、キューを無駄なく使用できる構造になっています。

詳細は、用語集の「CBQ」を参照してください。

PRIQ とは？

PRIQ は、Priority Queueing の略です。
送信キューを、「優先キュー」・「通常キュー」・「非優先キュー」の３つにわけ、送信処理を区別します。
送信処理は、「優先キュー」にデータがある場合は常に優先キューの送信処理を行い、「優先キュー」にデータがなくなると「通常キュー」からの送信処理を行い、「通常キュー」からもデータがなくなると「非優先キュー」の送信処理を行ないます。したがって、「優先キュー」にデータがある間は、「通常キュー」「非優先キュー」のデータの遅延がおこったり、廃棄されたりする場合があります。

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

qos-class cbq

CBQ(Class-Based-Queueing)のキュー構造を指定します。CBQ では次のような階層構造をとります。

root クラス
　├control クラス
　├任意のユーザ定義クラス(例:DATA-CLASS)
　└default クラス

□さらに下位の階層も定義できます

root クラスは、論理的に回線全体を示すクラスです。
control クラスは、制御パケット用のクラスです。デフォルトで ICMP、IGMP、RSVP 等が割り当て済みです。
default クラスは、どのクラスにも該当しないパケットのクラスです。

なお、帯域制御(CBQ)を有効にするためには、root、control、default の 3 つのクラスを設定することが必要です。

FITELnet-F120 ではユーザ定義クラスとして、各インタフェース毎に 16 クラス、装置全体で計 64 クラスまでクラス分けすることができます。
また、各クラスに優先度を設定し送信処理に優先度を付けることもできます。

設定例1　WAN インターフェースの帯域制御を設定します

```
ROOT-CLASS
        ├CONTROL-CLASS (5%)
        ├DATA-CLASS (75%)
        └DEFAULT-CLASS (20%)
```

root クラスを設定（帯域は 100%）

```
Router(config)#interface wan 1
Router(config-if ewan 1)# qos-class cbq ROOT-CLASS bandwidth 100
parent NULL
```

control クラスの帯域を親クラスの帯域(ROOT-CLASS)の 5%とする

```
Router(config)#interface wan 1
Router(config-if ewan 1)# qos-class cbq CONTROL-CLASS bandwidth
5 parent ROOT-CLASS control
```

データクラスの帯域を親クラス(ROOT-CLASS)の帯域の 75%とする

```
Router(config)#interface wan 1
Router(config-if ewan 1)# qos-class cbq DATA-CLASS bandwidth 75
parent ROOT-CLASS
```

※別途、クラス名「DATA-CLASS」についてルールの定義が必要です（qos-filter 参照）default クラスの帯域を親クラス(ROOT-CLASS)の帯域の 20%とする

```
Router(config)#interface wan 1
Router(config-if ewan 1)# qos-class cbq DEFAULT-CLASS bandwidth
20 parent ROOT-CLASS default
```

設定例2　設定例1の DATA-CLASS の下層に TCP データ用の「TCP-CLASS」を設定します

```
ROOT-CLASS
        ├CONTROL-CLASS
        ├DATA-CLASS
        │        └TCP-CLASS (70%)
        └DEFAULT-CLASS
```

DATA-CLASS の下層に TCP データ用の「TCP-CLASS」を置き、帯域を親クラス（DATA-CLASS）の 70%とする。
帯域不足の場合、親クラスに空きがあればその帯域も利用する。

```
Router(config)#interface wan 1
Router(config-if ewan 1)# qos-class cbq TCP-CLASS bandwidth 70 parent DATA-
CLASS borrow
```

コマンド書式

qos-class cbq 〈クラス名〉 bandwidth 〈帯域使用率〉 parent 〈親クラス名〉
[priority 〈優先度〉] [delay 〈最大遅延時間〉] [borrow] [red]
[default] [control]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
クラス名	CBQ のクラス名称を設定します。	-	省略不可
帯域使用率	親クラスに対する帯域使用率（単位：%）を指定します。	1～100	省略不可
親クラス名	親クラス名を指定します。設定しているクラスが、ルートクラスに属する場合は NULL を記述します。	-	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。 この値が大きいほど、優先度は高くなります。	0～2	0
最大遅延時間	このクラスの最大遅延時間（単位：m 秒）を設定します。この時間経過しても送信されない場合は廃棄されます。	1～9999	0
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	省略不可
control	コントロールクラスの場合に指定します。コントロールクラスは、ルートクラスに属している必要があります。	control	省略不可

この設定を行わない場合

CBQ 方式の QoS 制御を行なうことはできない。

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

qos-class priq

PRIQ のキュー構造を指定します。
PRIQ では、クラス名および『優先キュー』（優先度 2）、『通常キュー』（優先度 1）、『非優先キュー』（優先度 0）を指定します。

※必ずしも 3 つのキューを指定する必要はありません。
※いずれかひとつを default クラスに設定する必要があります。

設定例1　優先キューの設定

```
Router(config)# interface ewan 1
Router(config-if ewan 1)# qos-class priq HIGH-class priority 2
```

※別途、クラス名「HIGH-class」についてルールの定義が必要です（qos-filter コマンドを参照）

設定例2　デフォルトクラスを非優先キューとする

```
Router(config)# interface ewan 1
Router(config-if ewan 1)# qos-class priq LOW-class priority 0
default
```

※別途、クラス名「LOW-class」についてルールの定義が必要です（qos-filter コマンドを参照）

コマンド書式

qos-class priq <クラス名> priority <優先度>[qlimit <キュー限度値>]
[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
クラス名	PRIQ のクラス名称を設定します。	-	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。 この値が大きいほど、優先度は高くなります。	0～2	0
キュー限度値	キューにためることができるパケット数を指定します。	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	red	RED を使用しない

	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。		
default	デフォルトクラスの場合に指定します。 qos filter に適用されなかったデータをどのような優先度で処理するかを指定する場合に使用します。	default	デフォルトクラス以外

この設定を行わない場合

PRIQ 方式の QoS 制御を行なうことはできない。

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

qos-filter

CBQ/PRIQ のクラスに適用されるパケットの種類を、アクセスリストを利用して指定します。
アクセスリストは、IPv4/IPv6 拡張アクセスリストを使用します。

設定例1　access-list 番号 100 で指定したパケットを、クラス名"tcp-class"に適用させる。

```
Router(config)#interface lan 1
Router(config-if lan 1)#qos-filter tcp-class access-group 100
```

コマンド書式

qos-filter 〈クラス名〉 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
クラス名	CBQ/PRIQ のクラス名称を設定します。 クラス名称は、qos-class cbq コマンド、もしくは qos-class priq コマンドで設定します。	-	省略不可
アクセスリスト番号	CBQ/PRIQ のクラスに適用されるパケットの種類を、アクセスリスト番号で指定します。	100～199 2000～2699 3500～3999	省略不可

この設定を行わない場合

CBQ/PRIQ 方式の QoS 制御を行なうことはできない。

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

VRRP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。※2 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。	省略不可

※1：VRID の設定範囲は 1～255 となりますが、１台の装置で有効となる VRID は２つまでとなります。同一の VRID を複数のインターフェースに適用することは可能です。

※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。

※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。

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

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 となりますが、１台の装置で有効となる VRID は２つまでとなります。同一の VRID を複数のインターフェースに適用することは可能です。

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

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。※2 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。	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 となりますが、１台の装置で有効となる VRID は２つまでとなります。
同一の VRID を複数のインターフェースに適用することは可能です。
※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

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

※1：VRID の設定範囲は 1～255 となりますが、1 台の装置で有効となる VRID は 2 つまでとなります。
同一の VRID を複数のインターフェースに適用することは可能です。

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-F120 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-F120 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 や F120 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-F120 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

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

※１：VRID の設定範囲は 1～255 となりますが、１台の装置で有効となる VRID は２つまでとなります。
同一の VRID を複数のインターフェースに適用することは可能です。

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

UPnP機能

UPnP機能

upnp-server access-group

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。

設定例　アクセス番号 90 番の端末の UPnP 機能を制限する場合

```
Router(config)#upnp-server access-group 90
```

コマンド書式

upnp-server 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	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

FITELnet-F120 で UPnP 機能を使用する場合に設定します。

設定例 UPnP 機能を使用する場合

```
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

UPnP 機能を使用するインタフェース指定します。
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。

設定例 UPnP 機能を使用するインタフェースを PPPoE1 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〉[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
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 1～5 dialer 1～4	省略不可
優先度	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

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

モバイル機能

モバイル機能

auto connect

データ発生時に、モバイル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　自動発呼を行うように設定します。

```
Router(config)#interface mobile 1
Router(config-if mobile 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、自動的に接続するかどうかを設定します	on	自動接続する	省略不可
		off	自動接続しない	

この設定を行わない場合

データ発生時に、モバイル回線の自動接続を行います。

設定モード

モバイルインタフェース設定モード

caller

接続先アクセスポイントの電話番号を設定します。
refresh コマンド後に有効になるコマンドです。

設定例1　W01K を使用して接続する場合は、*99**24# に設定します

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#caller *99**24#
```

設定例 2　AX510N を使用して接続する場合は、057057XXXX##XX に設定します

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#caller 057057XXXX##XX
```

コマンド形式

caller <AP 電話番号>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
AP 電話番号	接続するアクセスポイントの電話番号を設定します。	32 桁以下の英数字・記号	省略不可

この設定を行わない場合

発信によるモバイル回線の接続ができません。

設定モード

ダイヤルアップインタフェース設定モード

card out-strings init

本コマンドを設定することにより、モデムカードを初期化するための文字列を任意に指定することができます。
通常はファームウェアが個別に保持している適切な文字列が使用されますので、本コマンドを設定する必要はありません。

設定例1 モデムカードに対して初期化文字列※を設定する。

```
Router(config)#interface mobile 1
Router(config-if mobile 1)#card out-strings init ATE0V1Q0&C1&D2
```

※初期化の内容は、下記を参照してください。

設定内容	AT コマンド例
コマンドエコー制御 カードに対して送信したコマンドを、装置側にエコーバックしない設定	E0
リザルトコード形式 リザルトコードを文字形式に設定	V1
リザルトコード表示制御 リザルトコードを表示する設定	Q0
DCD 制御 DCD 信号をデータリンク確立時のみ ON にする設定	&C1
DTR 制御 DTR 信号を ON から OFF に制御した場合に回線を切断する設定	&D2

コマンド形式

card out-strings init 〈初期化文字列〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
初期化文字列	モデムカードを初期化するための文字列を設定します。	最大 64 文字の英数字	省略不可

この設定を行わない場合

ファームウェアが個別に保持している適切な文字列が送信されます。

設定モード

モバイルインタフェース設定モード

forced disconnect cumulative-time

1ヶ月で許可する累積許容時間を指定します。
累積許容時間がここで設定した値を超えた場合は、現在接続中であれば切断し、以降の発信動作を停止します。
calender set コマンドや、SNTP 機能により、現在時刻の内容に、月が進む変更があった場合は、課金リミッタの状態を初期化します。

・毎月 1 日の 0:0:0 に、課金リミッタ情報はクリアされます。
その際、発信が制限されている状態も解除されます。
・現在の状況は、show limiter cumulative-time status コマンドで確認できます。
・発信が制限されている場合は、clear forced disconnect cumulative-time mobile で解除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。

※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　1ヶ月の累積許容時間を 2000 分に制限する

```
Router(config)#interface mobile 1
Router(config-if mobile 1)#forced disconnect cumulative-time 2000
```

コマンド形式

forced disconnect cumulative-time 〈累積許容時間〉 [〈プレアラート値〉]

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
累積許容時間	1ヶ月の接続累積許容時間（分）を設定します。 off を指定することで制限を無効にします。	off 60～2400	省略不可
プレアラート値	設定した累積許容時間に対して、警告を発する値（単位：%）を設定します。 warning-only を指定することで、累積許容時間を超えた場合に警告と共にログを残しますが、回線は接続されたままになります。	warning-only 1～99	設定値の90%で警告状態となります。

この設定を行わない場合

累積許容時間を制限しません。

設定モード

モバイルインタフェース設定モード

forced disconnect packet

1 日（24 時間）で送受信を許可するパケット数を指定します。
送受信パケット数がここで設定した値を超えた場合は、現在接続中であれば切断し、以降の発信動作を停止します。
forced disconnect cumulative-time コマンドとは異なり、発信制限がかかると、自動では解除されません。
発信制限は、clear forced disconnect packet mobile status コマンドにより解除できます。

- 現在の状況は、show limiter packet コマンドで確認できます。
- 発信が制限されている場合は、clear forced disconnect packet で解除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。

※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　24 時間の送受信パケット数を 75000 パケットに制限する

```
Router(config)#interface mobile 1
Router(config-if mobile 1)#forced disconnect packet 75000
```

コマンド形式

forced disconnect packet〈上限パケット数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
上限パケット数	1 日（24 時間）で送受信を許可するパケット数を指定します。off を指定することによりパケット数の制限が無くなります。 ※このパケット数は、ルータ内部で算出している数値であり、目安です。	off 1～ 4294967294	省略不可

この設定を行わない場合

送受信を許可するパケット数を制限しません。

参考

1 パケットは、128 バイトのユーザデータとして算出しています。

設定モード

モバイルインタフェース設定モード

idle-timer send

送信データに関する無通信監視時間（秒）を設定します。
ここで指定した時間送信データがない場合は、ダイヤルアップ接続を切断します。

設定例1　送信データに関する無通信監視時間を 60 秒に設定します。

```
Router(config)#interface mobile 1
Router(config-if mobile 1)#idle-timer send 60
```

コマンド形式

idle-timer send　{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>	送信データに関する無通信監視時間を設定します。	off	無通信監視を行いません。	60
		1～3600		

この設定を行わない場合

FITELnet-F120 が送信するデータが 60 秒間ない場合は、ダイヤルアップ回線を切断します。

設定モード

モバイルインタフェース設定モード

idle-timer receive

受信データに関する無通信監視時間（秒）を設定します。
ここで指定した時間受信データがない場合は、ダイヤルアップ接続を切断します。

設定例1　受信データに関する無通信監視時間を 60 秒に設定します。

```
Router(config)#interface mobile 1
Router(config-if mobile 1)#idle-timer receive 60
```

コマンド形式

idle-timer receive　{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>	受信データに関する無通信監視時間を設定します。	off	無通信監視を行いません。	60
		1～3600		

この設定を行わない場合

FITELnet-F120 が受信するデータが 60 秒間ない場合は、ダイヤルアップ回線を切断します。

設定モード

モバイルインタフェース設定モード

ip address

自装置のモバイルポート側の 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。該当するモバイル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 〈モバイルポート側 IP アドレス〉

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>モバイルポート側
IP アドレス</td><td>モバイル接続で使用するモバイルポート側の IP アドレスを設定します。
<table><tr><td>negotiated</td><td>接続相手から IP アドレスを割り振ってもらう場合</td></tr><tr><td>IPv4
アドレス形式</td><td>IP アドレス、サブネットマスクの順で設定します。</td></tr></table></td><td>negotiated
IPv4 アドレス形式</td><td>省略不可</td></tr>
</table>

この設定を行わない場合

モバイル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

モバイ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、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 〈アクセスリスト番号〉 { 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
アクセスリスト番号	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

モバイルインタフェース設定モード

ip nat inside destination

WAN 側から LAN 側への NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モードの場合で、設定のしかたが異なりますので注意してください。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 dialer 1
Router(config-if dialer 1)#ip nat inside destination static
158.xxx.xxx.2 192.168.0.1
```

【解説】
ip 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 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 dialer 1
Router(config-if dialer 1)#ip nat inside destination static
158.202.232.1 1500 192.168.0.1 80
```

【解説】
ip 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 nat inside source コマンドを使用して、設定します。

コマンド書式

【NAT スタティック（複数指定）時】　ip nat inside destination list 〈アクセスリスト番号〉[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]

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	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。	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

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、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

モバイルインタフェース設定モード

ip nat inside source

LAN 側から WAN 側への NAT 変換ルールを設定します。
NAT モードの場合と、NAT+モードの場合で、設定のしかたが異なりますので注意してください。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 dialer 1
Router(config-if dialer 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 <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 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 dialer 1
Router(config-if dialer 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 <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 dialer 1
Router(config-if dialer 1)#ip nat inside source static 192.168.0.1
158.xxx.xxx.2
Router(config-if dialer 1)#ip nat inside source list 1 pool pool1
Router(config-if dialer 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 〈LAN 側のアドレス〉〈WAN 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、WAN→LAN のスタティック登録を行なう必要があります。（①の部分）

コマンド書式

【NAT 時】　ip nat inside source list 〈アクセスリスト番号〉[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〉[変換後開始ポート番号] ［変換後終了ポート番号]]

【NAT+時】　ip nat inside source list 〈アクセスリスト番号〉[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〉

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	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	NAT プール名	NAT の場合

	囲を指定した NAT プール名を指定します。		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

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 dialer 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

モバイルインタフェース設定モード

lcp maxtimes

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 mobile 1
Router(config-if mobile 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

モバイルインタフェース設定モード

lcp restart

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 mobile 1
Router(config-if mobile 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 3000msec に設定します。

設定モード

モバイルインタフェース設定モード

max-call

ダイヤルアップ接続で 1 時間あたりの発呼回数制限の設定します。
設定値を超えた場合は、mail to コマンドを設定することで電子メールで通知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　1 時間あたりの発呼回数を 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〈発呼回数〉

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
発呼回数	ダイヤルアップ接続で 1 時間あたりの発呼回数制限の設定をします。 off を指定するとで、発呼回数制限の監視が無効になります。	1～1000	省略不可

この設定を行わない場合

モバイル接続で 1 時間あたりの発呼回数を 40 回に制限します。

設定モード

モバイルインタフェース設定モード

ppp account

ダイヤルアップ接続でインタフェースに mobile 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。
refresh コマンド後に有効になるコマンドです。

設定例1　ユーザ ID に f120@xxxxx.ne.jp, パスワードに f120pass を設定する

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ppp account f120@xxxxx.ne.jp
f120pass
```

コマンド形式

ppp account <username> <password>

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
hostname	モバイル接続相手送信する、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	モバイル接続相手送信する、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

この設定を行わない場合

ダイヤルアップ接続を行うことができません。
W01K カードを装着している状態で、SMS 着信によるコールバックのみを行う場合は、設定不要です。

設定モード

ダイヤルアップインタフェース設定モード

ppp account-sms

SMS 着信時の、認証パスワードを設定します。SMS リクエストメッセージの自由領域に指定した認証パスワードが、ここで設定した認証パスワードと同じ場合に、コールバック動作を行います。
refresh コマンド後に有効になるコマンドです。

※W01K カードを装着している場合に有効なコマンドです。

設定例1　SMS 着信の認証パスワードとして、sms-pass を設定する。

```
Router(config)#interface dialer 1
Router(config-if dialer 1)#ppp account-sms sms-pass
```

コマンド形式

ppp account-sms〈認証パスワード〉

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

自由領域に認証パスワードが指定されていない場合は、コールバックを行います。

設定モード

モバイルインタフェース設定モード

recvidletimer

called idle-timeout コマンドで、モバイル接続（着信）の、モバイル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、モバイル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 モバイル側からの受信パケットを無通信監視対象から外します。

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

モバイル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

モバイ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。該当するモバイル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　dialer1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 dialer 1
Router(config-if dialer 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

設定しているモバイルインタフェースが使用可能です。

設定モード

モバイルインタフェース設定モード

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]〈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
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 もしくは rw	ro
アクセスリスト番号	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	1～99：IPv4 用 3000～3499：IPv6 用	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

SNMP トラップを送信する場合に指定します。FITELnet-F120 では、パラメータにより、標準トラップ（MIBII）のみ送信・拡張 MIB のみ送信を指定することもできます。

パラメータ	送信するトラップの種類
snmp	標準トラップのみ送信
config	拡張トラップのみ送信
指定しない	全てのトラップを送信

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-manager 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	標準トラップのみを送信するか、拡張トラップのみを送信するかを指定します	snmp（標準トラップ） もしくは config（拡張トラップ）	標準トラップ/拡張トラップの両方を送信

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	標準トラップのみを送信するか、拡張トラップのみを送信するかを指定します	snmp（標準トラップ）もしくは config（拡張トラップ）	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-TRAP 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称を指定します。

設定例1 トラップ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)#snmp-server source-interface lan 1
```

コマンド書式

snmp-server source-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	SNMP Trap 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	省略不可

この設定を行わない場合

トラップ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

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-F120#1"に設定する

```
Router(config)# snmp-server name FITELnet-F120#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-f120"に設定する

```
Router(config)# snmp-server contact root@fitelnet-f120
```

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
設置場所名	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 {<エラーレベル値>| none}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エラーレベル値	elog の主力エラーレベル	0～7	省略不可
none	elog を送信しません	none	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F120 の elog とは？

FITELnetーF120 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、FITELnet-F120 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 {<エラーレベル値>| none}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エラーレベル値	slog の主力エラーレベル	0～7	省略不可
none	slog を送信しません	none	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F120 の slog とは？

FITELnet-F120 の slog では、FITELnet-F120 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 {<エラーレベル値>| none}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エラーレベル値	flog の主力エラーレベル	0～7	省略不可
none	syslog を送信しません	none	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F120 の flog とは？

FITELnet-F120 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 {<エラーレベル値>| none}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エラーレベル値	tlog の主力エラーレベル	0～7	省略不可
none	tlog を送信しません	none	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-F120 の tlog とは？

FITELnetーF120 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、FITELnet-F120 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、FITELnet-F120 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 {<エラーレベル値>| none}

パラメータ

パラメータ	設定内容	設定範囲	省略時の値
エラーレベル値	vpnlog の主力エラーレベル	0～7	省略不可
none	vpnlog を送信しません	none	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-F120 の vpnlog とは？

FITELnetーF120 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-F120 のレベル値設定

FITELnet-F120 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	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 16 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 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称を指定します。

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	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	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
・もしくは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
・モバイル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-F120 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-F120 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 ADSL を使用し、ADSL 側で通信ができなくなった場合に、モデム回線に切り替えて通信する。

FITELnet-F120 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-F120 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-F120 に FTP で送信する
reset at 12:00 1 Apr 2003 SIDE-A.frm SIDE-A.cfg

モバイル自動切断機能とは？

FITELnet-F120 では、モバイル回線に関して、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-F120(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

【冗長機能の到達不能／復旧の場合】
Subject：[RAAS] Pathcheck Error on FITELnet-F120(装置の IP アドレス)

[1]	Layer3 監視のシーケンス番号です。
pathchkipaddr	Layer3 監視先の IP アドレス（設定値）を表示します。

status	Layer3 監視経路の状態を表示します。経路に問題がない場合は"Normal"、経路に問題がある場合は"Error"と表示されます。
fail	経路の障害とみなすパケット数（設定値）のうち、いくつのパケットを受け取れなかったかを表示します。 上記画面例では、4 つのパケットを受け取れなかった場合に障害とみなすという設定に対し、現在 2 つのパケットを受け取れていないことを意味します。
success	障害復旧とみなすパケット数（設定値）のうち、いくつのパケットを受け取れたかを表示します。 上記画面例では、10 個のパケットを受け取れた場合に障害復旧とみなすという設定に対し、現在 3 つのパケットを受け取れていることを意味します。
route	この Layer3 監視パケットの NextHop（設定値）を表示します。
PingTrial	1 回の Layer3 監視で送信するパケットの個数(設定値）を表示します。
PathChkInterval	経路監視パケットの定期送信間隔を表示します。
PathChkcount	いくつの L3 監視パケットの応答を、受け取れなかった場合に、経路の障害と判断するかの個数を表示します。
RestChkInterval	経路異常時の経路監視パケットの定期送信間隔を表示します。
RestChkcount	経路の障害時に、いくつの L3 監視パケット（応答）を受け取れた場合に、経路の障害が復旧したと判断するかの個数を表示します。
backup network	バックアップを利用するデータの情報を表示します。
destination	宛先アドレス（範囲）を表示します。
1st/2nd	メイン経路のインタフェース／バックアップ経路のインタフェースを表示します。
Time	冗長機能のステータス変更時刻

【時刻指定リセット機能の場合】

Subject：[RAAS] Auto Reset on FITELnet-F120(装置の IP アドレス)

SIDE-A/SIDE-B	SIDE-A. ｆ ｒｍ、SIDE-B. ｆ ｒｍ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

【モバイル自動切断機能の場合】
Subject：[RAAS] packet limiter: alerted-90/bombarded on FITELnet-F120(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
Interface	Mobile 1
Configuration	上限パケット数
Status	作動（bomberd） or 警告（Alert）
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"F120@xxxxx.co.jp"を指定する

```
Router(config)# mail from F120@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
モバイル自動切断	規定パケット数以上の送受信データがあったあるいは規定パケット数の 90%を超える送受信データ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

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 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

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 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称を指定します。

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	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	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

SNTP機能

SNTP機能

sntp

SNTP を有効にします。

設定例1　SNTP 機能を使用する

```
Router(config)#sntp
```

コマンド書式

sntp

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

SNTP 機能を使用できません。

SNTP 機能とは？

現在時刻を取得するプロトコルです。（Simple Network Time Protocol）
FITELnet-F120 は、外部の SNTP サーバから現在時刻を取得することができます。SNTP サーバとしては動作しません。

設定モード

基本設定モード

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。

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	off（リトライしない） もしくは 64～1024	省略不可
リトライ時間	リトライ継続時間。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。
・FITELnet-F120 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？

FITELnet-F120 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。

設定例1　FITELnet-F120 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　FITELnet-F120 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 < 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） ※0 を指定した場合は、問い合わせを行いません	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。

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
```

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	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	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称を指定します。

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	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	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

SSH機能

SSH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

```
(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。

```
(config)# access-list 10 permit 192.168.0.0 0.0.0.255
(config)# ssh-server access-group 10
```

コマンド書式

ssh-server 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	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	アクセスリスト番号	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 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

```
(config)#ssh-server enable
```

コマンド書式

ssh-server enable

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

```
(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。	1～60 off：自動ログアウトしない	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 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 秒間入力がない場合は セッションを切断する

```
(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

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。
refresh コマンド後に有効になるコマンドです。

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選択します。	lan 1	LAN インタフェース（SW-HUB 4 ポート）	省略不可
		ewan 1	EWAN#1 ポート	
		ewan 2	EWAN#2 ポート	

設定モード

基本設定モード

linkdown-detect

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　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 {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	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かどうかの設定	on：連動 off：非連動	省略不可

この設定を行わない場合

論理的な LAN インタフェースのアップ/ダウンに関わらず、LAN ポートは常にリンクアップ状態となります。
ただし、ip vrrp enable コマンドが設定されている場合は、論理的な LAN インターフェースのアップ/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

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。	LAN インタフェース：1～4 EWAN#1, EWAN#2 インタフェース：1	省略不可
通信速度とデュプレックス	設定している Ethernet 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	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 〈インタフェース番号〉〈mdi | mdi-x | auto〉

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。	LAN インタフェース	1～4	省略不可
		EWAN#1,EWAN#2 インタフェース	1	
mdi | mdi-x | auto	設定している Ethenet インタフェースの MDI/MDI-X を設定します。	mdi	MDI ポート	省略不可
		mdi-x	MDI-X ポート	
		auto	自動切換	

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

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）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

FITELnet-F120 では、常にインターネットに接続しており、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。
FITELnet-F120 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>][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>][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 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	省略不可
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

		conversion-error	
		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	

		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	全てのICMPv6 タイプ

		ICMPv6 タイプ値（0～255）	
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	全ての TCP ポート番号

		pop3 smtp sunrpc syslog 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	全ての UDP ポート番号

		talk tftp time who xdmcp UDP ポート番号（0～65535）	
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。

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

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-F120 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-F120 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

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"F120#1"に設定する場合

```
Router(config)#hostname F120#1
F120#1(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

索引

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

- 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。
-

発行責任：古河電気工業株式会社
130-B0401-AH01-D
2008.10