

INFONET - VP100

VPNボックス コマンドマニュアル

古河電気工業株式会社

ご注意

この装置の耐用年数は6年です。それ以降の使用は弊社にご相談ください。

この装置の修理可能期間は、製造終了後6年間とさせていただきます。

本マニュアルには、「外国為替及び外国貿易管理法」に定める戦略物資関連技術が含まれています。従って、本マニュアルを輸出する場合には、同法に基づく許可が必要とされます。なお、本マニュアルを廃棄する場合は、完全に粉砕して下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

INFONET-VP100 VPN ボックス コマンドマニュアル

目次

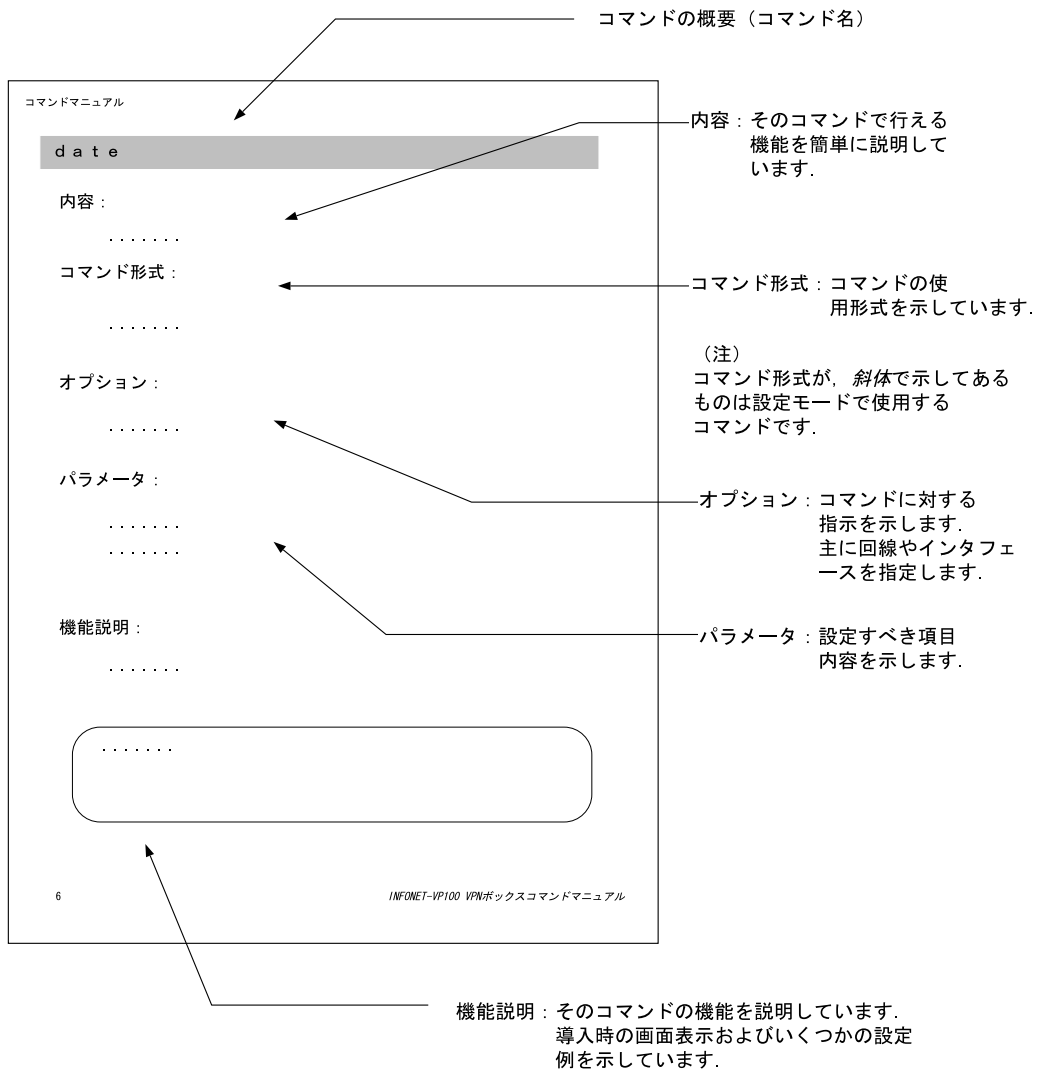
本書の見方.....	vi
autologout.....	1
clog.....	2
configuration.....	4
date.....	5
dhcpstat.....	6
display.....	7
elog.....	8
exit.....	9
flog.....	10
ftrace.....	11
gatetable.....	13
help.....	14
hereis.....	15
ipinterface.....	16
iproute.....	17
llog.....	18
more.....	19
natinfo.....	20
password.....	22
ping.....	23
reset.....	24
rgrpstat.....	28
stip.....	29
stsystem.....	31
tlog.....	33
traceroute.....	34
vlog.....	35
vpncertinfo.....	36
vpncrlget.....	37
vpnlog.....	38

コマンドマニュアル

vpnsainfo	39
vpnselectorinfo	41
vpnstat	43
clogcontrol	45
dhcpserver	47
exit	49
flogcontrol	50
help	51
hostname	52
hosttable	53
identifier	54
ifaccept	55
ifpropagate	56
interface	57
ipfiltering	59
ipripstatic	62
iprouting	63
manager	65
more	66
nat	67
natnotrans	69
natplusstatictable	70
natport	71
natrang	72
natstatictable	73
rgrpparam	74
rgrptable	75
rtcontrol	77
snmp	79
syslogcontrol	80
syslogtable	81
trustgateways	83
vpn	84
vpncert	85

vpncertparam.....	86
vpncertreq.....	87
vpngenkey.....	88
vpnikepolicy.....	89
vpnopt.....	90
vpnparam.....	91
vpnpeer.....	92
vpnpolicy.....	94
vpnselector.....	96

本書の見方



また、コマンド形式で使用される記号の意味は以下の通りです。

記号	記号の意味
[]	[] 内の項目は省略してもよい
	で区切られた項目のうちどれかを選択する
	スペースを表す
	リターンキーの入力を示す
< >	< > 内で示される内容を表す項目を表す
{ }	{ } 内の項目は省略できない
,	, で区切られた項目のうち複数の選択が可能
...	前述の項目を繰り返し設定することが可能

autologout

```
autologout [off | <logout time>]
```

【内容】

オートログアウト機能のする / しないの設定 . オートログアウトする場合のタイムアウト時間を設定します .

【オプション】

なし

【パラメータ】

off	オートログアウトを「しない」を設定します .
<logout time>	オートログアウトを「する」を設定し , その時のタイムアウト時間を指定します . 設定範囲は , 0 ~ 240 (分) . 「0」は「off」を示します . 工場出荷時の設定は 5 分です .

【機能説明】

装置に「login」をしている状態で一定時間入力が行われないと , 自動的にログアウトします . この時 , 設定中の項目はすべて無効になります .

ここで設定した <logout time> は , 新たにローカルや telnet , ftp でログインしたときに有効になります .

ftp でのログインに対して "off" は機能しません . ftp でのログインに限って "off" の場合は 5 分でログアウトします .

パラメータ指定がない場合は現在の状態を表示します .

【注意】

FTP によりリモートからアクセスされている間は , このコマンドは使用できません .

clog

c l o g [-c|-n]

【内容】

装置内で廃棄されずに送受信または中継された IP パケットのログを表示します。

【オプション】

-c	ログをクリアします (clog, flog の両方がクリアされます)。
-n	ログを新しい情報から順に表示します。
なし	ログを古い情報から順に表示します。

【パラメータ】

なし

【機能説明】

通信ログはコマンド clogcontrol によって ON/OFF の制御ができます。

通信した IP パケットに関する以下の情報が表示されます。

・通信タイプとインタフェース：

SEND, {private|public} (送信時), RECV, {private|public} (受信時),

FWD, {private|public}|{private|public} (中継時)

更に、上位プロトコルによって以下の内容が表示されます。

UDP:

・プロトコル名：UDP

・<送信元 IP アドレス>:<ポート番号> -> <送信先 IP アドレス>:<ポート番号>

TCP:

・プロトコル名：TCP

・フラグ:S(Syn), F(Fin), A(Ack), P(Push), U(Urgent), R(Reset)

・<送信元 IP アドレス>:<ポート番号> -> <送信先 IP アドレス>:<ポート番号>

ICMP:

・プロトコル名：ICMP

・<送信元 IP アドレス> -> <送信先 IP アドレス>

・メッセージタイプ

・コード

その他

・プロトコル名：protocol<IP の上位のプロトコル番号>

・<送信元 IP アドレス> -> <送信先 IP アドレス>

【表示例】

```
SEND private,UDP:192.52.150.100:1000 -> 192.52.150.1:2000  
RECV public,ICMP:192.52.150.1 -> 192.52.150.100,type8,code0  
FWD public>private,protocol2:192.52.150.1 -> 192.52.150.100  
FWD private>public,TCP(SA):192.168.2.1:2000 -> 192.52.151.1:1000
```

configuration

configuration

【内容】

ルータの設定を行うためのコンフィグレーションモードへ移行します。
コンフィグレーションモードに移らない限り、ルータの設定はできません。

【オプション】

なし

【パラメータ】

なし

【機能説明】

このコマンドによってコンフィグレーションモードに移行する場合、コンフィグレーションパスワードの入力が必要となります。ただし、ログインの際に、コンフィグレーションパスワードを入力していた場合には、ここでのパスワードの入力は必要ありません（問い合わせは行われません）。

コンフィグレーションモードに移行するとプロンプトが「conf#」に変わります。

date

date [YYMMDD. hhmss | hhmss | YYMMDD.]

【内容】

装置に設定されている現在時刻を表示します。または、装置に現在時刻を設定します。

【オプション】

なし

【パラメータ】

YY	年 (00 ~ 99 ただし1999 ~ 2098)
MM	月 (01 ~ 12) 2桁
DD	日 (01 ~ 31) 2桁
.	日付データと時刻データを分けるセパレータ。日付のみの指定の時にも必要。
hh	時 (00 ~ 23) 2桁
mm	分 (00 ~ 59) 2桁
ss	秒 (00 ~ 59) 2桁

【表示例】

```
#date
990115.101530 (123 20:23:30)
#
```

【機能説明】

パラメータを指定しない場合は現在の時刻と装置起動時からの経過時間を表示します。

例では、現在時刻が1999年1月15日10時15分30秒、装置起動時からの経過時間が123日と20時間23分30秒であることを示しています。

dhcpstat

```
dhcpstat [-{[a][s][S]}]
```

【内容】

DHCP サーバの動作時の情報を表示します。オプション省略時は "-sS" が指定された場合と同じになります。

【オプション】

a	ARPの結果，存在を確認できたIP端末
s	動的にアドレスを割り当てたIP端末
S	静的に割り当てている（保持している）IP端末

【パラメータ】

なし

【機能説明】

DHCP サーバ機能が ARP により認識した（既に利用済みの）IP アドレス（a）、IP 端末からの IP アドレス取得要求に対して DHCP サーバ機能が自動配布した IP アドレス（s）、設定（hosttable コマンド）により割り付けが決められている IP アドレス（S）を表示します。表示は IP 端末とのペアで表示し、IP 端末は MAC アドレスで表わします。

「割り付けが決められている IP アドレス（S）」に関しては、前もって設定により決められた内容となりますので実際に使用されているかの判断にはなりません。

内部的に「割り付けが決められている IP アドレス（S）」が「ARP により認識した（既に利用済みの）IP アドレス（a）」とぶつかった場合は、現況優先により「ARP により認識した（既に利用済みの）IP アドレス（a）」の内容を表示します。

これにより「割り付けが決められている IP アドレス（S）」があるはずにも関わらず、このコマンドにて表示されない場合は、既にその IP アドレスは使用されていると判断できます。

display

display [all]

【内容】

設定情報として装置に保存されている構成定義情報の内容を表示します。

【オプション】

なし	全ての設定を表示します。
all	設定および現在の情報をすべて表示します。

【パラメータ】

なし

【機能説明】

装置に保存されている、ルーティングに関する設定情報を表示します。

ルーティングに関する設定情報を見たい場合は、ログインした状態で（プロンプトが#の状態）コマンドを入力します。この時はファームウェア情報と共に装置に保存されているルーティングに関する設定が表示されます。

【メモ】

ファームウェア情報は hereis コマンドで表示される内容と同じです。設定内容の表示は、コンフィグレーションモードにおける各設定コマンド毎にそのコマンドで表示される内容が表示されます。

【注意】

FTP によりリモートからアクセスされている間は、このコマンドは使用できません。

elog

`elog [-c | -n]`

【内容】

エラーログを表示します。

【オプション】

-c	エラーログをクリアします。
-n	エラーログを新しい情報から順に表示します。
なし	エラーログを古い情報から順に表示します。

【パラメータ】

なし

【機能説明】

装置全体の中度 / 軽度エラー情報として、

” 通し番 装置稼働時間 日付 タスク ID ログ ID エラーコード ログメッセージ ”

の表示およびクリアを行います。

【メモ】

エラーログの最大ログ件数は 64 件です。64 件以上のログは、最も古いログから上書きしていきます。

exit

exit

【内容】

現在がログイン状態の場合、ログインプロンプトに戻ります。

現在がコンフィグレーションモードの場合、それを終了し、ログイン状態へ戻ります。

【オプション】

なし

【パラメータ】

なし

【機能説明】

装置からログアウトします。また現在のモードがコンフィグレーションモードの場合、それを終了し、ログイン状態へ戻ります。

コンフィグレーションモード時に設定内容を変更した場合は、ログイン状態に戻る時にその内容を装置に保存しようとしています。

保存が必要な時は "configuration modified. save OK? (y/n):" と表示されますので、"y" を入力してください。"n" を入力すると、設定してきた内容は無効となり、コンフィグレーションモードに入る前の状態に戻ります。

"y" と入力し、設定モードを終了したら reset コマンドを入力することにより装置をリセットします(リセットを行わないと変更した内容が装置に対して有効になりません)。“n” と入力し、装置に設定内容を保存しないでコンフィグレーションモードを終了したときは、装置をリセットする必要はありません。

flog

f l o g [-c|-n]

【内容】

IP フィルタリングにより廃棄されたパケットのログを表示します。

【オプション】

-c	ログをクリアします (clog, flog の両方がクリアされます)。
-n	ログを新しい情報から順に表示します。
なし	ログを古い情報から順に表示します。

【パラメータ】

なし

【機能説明】

コマンド flogcontrol により本ログ機能の ON/OFF の制御ができます。

廃棄が生じた場所によって以下の3種類のメッセージの内の1つが最初に表示されます。

RECV recv from{private|public}:

本装置宛の IP パケットを受信時に廃棄が行われました。

最後の文字列は廃棄されたパケットの受信インタフェースを示します。

FWD recv from{private|public}:

IP パケットを中継する際、受信時に廃棄が行われました。

最後の文字列は廃棄されたパケットの受信インタフェースを示します。

FWD send to{private|public}:

IP パケットを中継する際、送信時に廃棄が行われました。

最後の文字列は廃棄されたパケットの送信インタフェースを示します。

更に、廃棄された IP パケットの上位層プロトコルに依存した情報が表示されます。

表示される内容は clog のものと同様です。

【表示例】

```
RECV recv from public,UDP:192.52.150.1:1000 -> 192.52.150.100:2000
FWD recv from public,protocol2:192.52.150.1 -> 192.52.150.100
FWD send to private,TCP(S):192.52.151.1:1000 -> 192.168.2.1:2000
```

ftrace

```
f t r a c e [-{s|p|d|c}] [mac|ip|ike|esp] [<MAC frame>|<IP frame>]
    MAC frame: {off|{[remote=<mac address>] [local=<mac address>]
                [broadcast]}} port={private,public}}
    IP frame : {off|{[dst=<ip address>[,<ip address mask>]]
                [dstport=<port no.>[,<port no.>]]
                [src=<ip address>[,<ip address mask>]]
                [srcport=<port no.>[,<port no.>]]
                [prot={tcp/udp|icmp|tcp|udp|all|<protocol no.>}}
                [rcvif={private,public}]}}
```

IPSEC IKE: {off|on}
 IPSEC ESP: {off|on}

【内容】

中継するパケット等のデータをトレースします。

【オプション】

-s	トレース開始 (トレースデータの設定はできません)
-p	トレース停止 (同上)
-d	トレース表示 (同上)
-c	トレースクリア (同上)
なし	トレースデータの設定

【パラメータ】

トレースの対象とするフレームタイプを選択します。複数のフレームタイプを指定することはできません。

mac	トレースの対象としてMACフレームを指定します。
ip	トレースの対象としてIPパケットを指定します。
ike	トレースの対象としてIPSEC IKEのフレームを指定します。
esp	トレースの対象としてIPSEC ESPのフレームを指定します。

<MAC フレーム指定> : 以下のパラメータで指定します。

```
{off|{[remote=<MAC アドレス>] [local=<MAC アドレス>]
[broadcast]}} port={private,public}}
```

コマンドマニュアル

< IP フレーム指定 > : 以下のパラメータで指定します .

```
{off|{[dst=< IP アドレス > [, < IP アドレスマスク > ]]  
  [dstport=< ポート番号 > [, < ポート番号 > ]]  
  [src=< IP アドレス > [, < IP アドレスマスク > ]]  
  [srcport=< ポート番号 > [, < ポート番号 > ]]  
  [prot={tcp|udp|icmp|tcp|udp|all| < プロトコル番号 > }]  
  [recvif=private,public]
```

off トレースの対象から IP フレームをはずします .
それ以外の項目 IP フレームモードを指定すると同時に内容を指定します .
 内容に関しては , ipfiltering コマンドと同じです .

< IPSEC IKE フレーム指定 > : 以下のパラメータで指定します .

```
{off|on]  
  off                    トレースの対象から IPSEC IKE フレームをはずします .  
  on                     IPSEC IKE フレームをトレースの対象とします .
```

< IPSEC ESP フレーム指定 > : 以下のパラメータで指定します .

```
{off|on]  
  off                    トレースの対象から IPSEC ESP フレームをはずします .  
  on                     IPSEC ESP フレームをトレースの対象とします .
```

【機能説明】

フレームトレースの開始 (-s), 終了 (-p), 表示 (-d), 消去 (-c) ができます . トレースの対象とするフレームを設定したいときは , オプションを付けずに設定してください . オプションやパラメータの指定がない , コマンド名のみの入力時は現在の状況を表示します .

gatetable

gatetable

【内容】

gatedテーブルの内容を表示します。

コマンド形式：

gatetable

【オプション】

なし

【パラメータ】

なし

【機能説明】

gatedテーブルの内容として次の内容をエントリー毎に表示します。

ルーティング情報を得た手段 (other, local, rip)

other 下記以外

local スタティック登録

rip RIPで学習

宛先 IP アドレス IP アドレスマスク

宛先に到達するために送信するゲートウェイの IP アドレス

経路タイプ (local, remote)

local 直接ルート等の自装置内の経路を示します

remote 自装置以外の経路を示します

メトリック値

help

[help | ?] [-l | < command >]

【内容】

指定コマンドの usage を表示します .

【オプション】

-l	コマンドが投入された時のモードで使用できるすべてのコマンドの usage を表示します . モードにはログイン状態 (ログインモード) と コンフィグレーションモードがあります .
----	--

【パラメータ】

< command >	usage を表示させたいコマンド名
-------------	--------------------

【機能説明】

オプションやパラメータの指定がない場合は , コマンドが投入された時のモードで使用できるすべてのコマンド名だけを表示します .

hereis

hereis

【内容】

装置固有の識別子を表示します。

【オプション】

なし

【パラメータ】

なし

【機能説明】

装置を識別する内容として次を表示します。

description (装置名 / 装置版数 / ファームウェア版数と作成日 / 装置の MAC アドレス)

node (装置名称)

manager (管理者名)

location (装置設置場所)

description の内容は装置やインストールしたファームウェアで固定となります。

ipinterface

ip interface [-[private]][public]

【内容】

IPルーティングのインタフェースの情報を表示します。

【オプション】

-[private][public]	表示する回線を指定します。 private PRIVATE LAN 回線 public PUBLIC LAN回線
--------------------	--

【パラメータ】

なし

【機能説明】

IP インタフェースの情報として次の内容をインタフェース毎に表示します。ただし、ダウンしているインタフェースに対しては表示を行いません。

インタフェースのステータス	(up, down)
インタフェースタイプ	(broadcast, point to point)
インタフェースアドレス	
インタフェースの IP アドレスサブネットマスク	
ブロードキャストアドレス	
リモートアドレス	(PUBLIC LAN のみ)
リモートサブネットマスク	(PUBLIC LAN のみ)

iproute

`iproute`

【内容】

IPルーティングのルーティング情報を表示します。

【オプション】

なし

【パラメータ】

なし

【内容】

IPルーティングテーブルの内容として次の内容を表示します。

ルーティング情報を得た手段 (other , local , rip, netmsg)

other	下記以外
local	スタティック登録
rip	RIPで学習
netmsg	RIP2で学習

宛先 IP アドレス IP アドレスマスク

宛先に到達するために送信するゲートウェイの IP アドレス

経由するインタフェース

経路タイプ (direct , indirect)

direct	直接ルート等の自装置内の経路を示します
indirect	自装置以外の経路を示します

llog

`llog [-{c|n}] [-[private][public]`

【内容】

ラインログを表示します。

【オプション】

<code>-c</code>	ラインログをクリアする。
<code>-n</code>	ラインログを新しい情報から順に表示する。
<code>-[private][public]</code>	表示する回線を順に指定します。 private PRIVATE LAN 回線 public PUBLIC LAN回線
なし	すべての回線のラインログを古い情報から表示する。

【パラメータ】

なし

【機能説明】

回線に関するロギングとして次の項目を表示します。

通し番号

装置稼働時間

日付

回線種別

エラーコード

ログメッセージ”

【メモ】

ラインログの最大ログ件数は回線毎に 20 件です。20 件以上のログは、最も古いログから上書きしていきます。

more

`more [on|off|<lines>]`

【内容】

表示サスペンド機能を制御します。

【オプション】

なし

【パラメータ】

off	moreを「無効」に設定します。
on	moreを「有効」に設定します。
<lines>	moreを「有効」に設定し、その時の有効表示行数を指定します。 設定範囲：0～255 工場出荷時：23行

【機能説明】

表示サスペンド機能(MORE表示)の有効/無効を設定します。パラメータの指定が無い時は現在の状態を表示します。

表示をサスペンドするまでの表示行数を<lines>で指定します。行数の指定を行うと自動的に機能が「有効」となります。行数に0を指定すると装置デフォルト(23行)を設定します。

natinfo

`natinfo {nat|natp} [private=<ipaddress>]`

【内容】

NAT / NAT +plus 機能のアドレス変換情報を表示します。

【オプション】

なし

【パラメータ】

<code>nat natp</code>	nat , nat+plusを選択します。
<code>private=<ipaddress></code>	指定したアドレスへの変換情報の詳細を表示します。

【機能説明】

NAT +plus 機能を使用している時のアドレス変換情報として PRIVATE LAN 側の送信元 IP アドレスと PUBLIC LAN 側の変換後 IP アドレスの組と ,それに対応する宛先 IP アドレス , PRIVATE LAN 側の送信元ポートと PUBLIC LAN 側の変換後ポートの組と ,それに対応する宛先ポートを表示します。

実際の表示は次のフォーマットとなります。

PRIVATE LAN 側送信元 IP アドレス (PUBLIC LAN 側変換後 IP アドレス) 宛先 IP アドレス
PRIVATE LAN 側送信元ポート (PUBLIC LAN 側変換後ポート) 宛先ポート

“宛先 IP アドレス” を指定した場合は ,指定したアドレスへの詳細変換情報として次のように表示します。

PRIVATE LAN 側送信元 IP アドレス (変換後 IP アドレス) 宛先 IP アドレス
プロトコル番号
PRIVATE LAN 側送信元ポート (PUBLIC LAN 側変換後ポート) 宛先ポート
エージアウトタイマ (カウントダウンタイマ)
ステータス (1:有効, 2:PRIVATE LAN 側より FIN 受信, 3:PUBLIC LAN 側より FIN 受信を or で表示)

```
#natinfo natp
```

	private		global		remote		
no	(IP address	port)	port	(IP address	port)	protocol	timer(sec)
1	192.52.150.2	1230	1230	203.139.160.69	53	UDP	285
2	192.52.150.2	1231	1231	207.46.130.150	80	TCP	45
3	192.52.150.2	1232	1232	207.46.130.150	80	TCP	3585
4	192.52.150.2	1233	1233	207.46.130.150	80	TCP	45

password

password [-c]

【内容】

ログインおよびコンフィグレーションパスワードの登録 / 変更を行います。

【オプション】

-c	設定を行うためのモードに移行する場合のパスワード (コンフィグレーションパスワード) を設定する場合に使用します。
----	---

【パラメータ】

なし

【機能説明】

オプション指定がない場合はログインパスワードを、指定がある場合はコンフィグレーションパスワードを設定します。

パスワードは最大 8 文字の ASCII データで指定します。大文字小文字は違う文字として判断します。

FTP によりリモートからアクセスされている間はこのコマンドは使用できません。

【注意】

パスワードが第三者に知られるとリモートから設定を変えられてしまう危険性があります。パスワードの管理はしっかりとしてください。

【メモ】

パスワードを忘れてしまった場合は、reset-d コマンドを利用して設定内容をお買い求め時の状態に戻してください。

ping

`ping` [`< IPaddress >`]

【内容】

IP 接続の確認を行います。

【オプション】

なし

【パラメータ】

<code>< IPaddress ></code>	エコーテストの対象とする IP ホストアドレスを指定します。
----------------------------------	--------------------------------

【機能説明】

接続確認したい相手の IP アドレスを入力することにより IP 接続の確認ができます。

reset

reset [-d]

【内容】

装置の再起動を行います。

【オプション】

-d	パスワードを含む全ての設定項目を、工場出荷時の設定に戻してからリセットします。
----	---

【パラメータ】

なし

【機能説明】

装置のリセットを行います。設定を変更した場合は、必ずリセットを行ってください（変更した設定内容はリセット後有効になります）。

リセット時、-d を指定した場合はコンフィグレーションパスワードの入力が必要です。

オプション"-d" を指定してリセットを行った後のルーティングに関する設定を display コマンドで見ると次のようになります。

【注意】

この内容はファームウェアのバージョンアップにより変更される場合があります。

ルーティングに関する設定

```
#disp
hereis
description: 'INFONET-VP100' A V01.01 1999.12.13 (00:00:0e:87:c0:11)
node      :
manager   :
location  :

date
990114.231609 (0 00:11:15)

hostname
nameserver: off
netbiosserver: off
domainname:
```



```

default gateway:

identifier
node      :
manager   :
location  :

interface
<ip routing interface>
<PRIVATE>
broadcast
address:192.52.150.100 subnet:255.255.255.0 broadcast:192.52.150.255
<PUBLIC>
down

rtcontrol
<rip(ip) control>
<PRIVATE>
sendinterval:30(sec) send:rip1 rcv:riplrip2 metric:0 ageout:180(sec)
<PUBLIC>
sendinterval:30(sec) send:rip1 rcv:riplrip2 metric:0 ageout:180(sec)

iprouting
off proxyarp:shortcut filtering:off rip:on ifaccept:exclude ifpropagate:exclude

trustgateways
*** empty table

ifaccept
*** empty table

ifpropagate
*** empty table
ipripstatic
*** empty table

ipfiltering(forward)
*** empty table

ipfiltering(discard)
*** empty table

snmp
on authtrap:on

manager

```

コマンドマニュアル

```
1:0.0.0.0 public r
2:empty
3:empty
4:empty

dhcpserver
on sendarpnum:16 arptimeout:10 sendarpcount:1
  gateway:on      allocateaddr:0.0.0.0 allocatewidth:254

hosttable

syslogcontrol
off

syslogtable
0.0.0.0 err:off warning:off info:off facility:1

nat
off
  t1=1440 t2=5 t3=60 t4=1 t5=1 t6=60 t7=1

natstatictable
*** empty table

natrange
*** empty table

natnotrans
*** empty table

natplusstatictable
*** empty table

natport
*** empty table

vpn
off

vpnpeer
*** empty table

vpnpolicy
*** empty table

vpnselector
*** empty table
```

```
vpnopt
off

vpnparam
retrytimer:20(sec) max retry time:1
newsai: 90(sec) newsar: 0(sec)
phase1 sa lifetime:0(sec)
```

rgrpstat

r g r p s t a t

【内容】

【オプション】

なし

【パラメータ】

なし

【表示例】

```
#rgrps
id: 1 ---設定にて有効な VRRP-ID
macaddress: 00:00:5e:00:01:01 ---代表 MAC アドレス
status: initialize ---現在の状態(Master or Backup or
Initialize)
priority: 255 ---この ID における自分の priority
ipaddress: 192.52.150.100,192.52.119.241 ---代表 IP アドレス
Private-LAN,Public-LAN
advertisement timer: 1 ---ネゴ結果の公告パケット送信間隔
(Master 時は己の設定、Backup 時
は Master の設定)
preempt: on ---この ID における自分の preempt
uptime(sec): ---- ---Master になってからの経過時間
(Master のみ表示)
become master count: 0 ---過去、Master になった回数
advertise receive: 0 ---正常な公告パケット受信個数
error advertise receive: 0 ---間違っている公告パケット受信個数
#
```

stip

s t i p

【内容】

IP ルーティングに関する統計情報を表示します。

【オプション】

なし

【パラメータ】

なし

【機能】

IP ルーティングの統計情報として次の項目を表示します。

IP パケット統計情報

ICMP パケット統計情報

UDP パケット統計情報

TCP パケット統計情報

RIP パケット統計情報

項目毎の内容

< IP >

総入力 IP パケット数	in packet
廃棄された入力パケット数	in discard packet
IP ヘッダエラー受信パケット数	in header errors packet
IP アドレスエラー受信パケット数	in address error packet
送信要求パケット数	out request packet
内部資源不足のため廃棄された送信要求パケット数	out discard packet
フォワーディングの必要のある受信パケット数	forward packet
送信経路がないため廃棄された送信要求パケット数	no route packet

コマンドマニュアル

< ICMP >

受信 ICMP パケット数 (エラー含む)	in message packet
受信 ICMP エラーパケット数	in error packet
送信 ICMP パケット数 (エラー含む)	out message packet
送信 ICMP エラーパケット数	out error packet

< UDP >

受信 UDP データグラム数	in datagram packet
受信エラーUDP データグラム数 (チェックサムエラー等)	in error packet
受信エラーUDP データグラム数 (不正宛先ポート)	no port packet
送信 UDP データグラム数	out datagram packet

< TCP >

受信 TCP セグメント数	in segment packet
送信 TCP セグメント数	out segment packet
受信エラーTCP セグメント数 (チェックサムエラー等)	in error packet
受動オープンした回数	passive open count

< RIP >

受信 RIP パケット数	in packet
送信 RIP パケット数	sent packet
送信 RIP 要求パケット数	out request packet
受信 RIP リプライパケット数	in reply packet
「triggered update」した回数	flash update packet
送信エラーパケット数	send error packet
受信エラーパケット数	bad receive packet

stssystem

stssystem

【機能】

現在の CPU 負荷率とメモリ使用率を表示します。CPU 負荷率については最新の 5 秒, 1 分, 5 分の負荷率(%) を表示し, メモリ使用率については mbuf 使用率(%), mcb 使用率(%), isakmp のメモリ使用率(%), network のメモリ使用率(%) を表示します。(network のメモリ使用率は VPN 機能に関して使用している値を表示)

【オプション】

なし

【画面表示】

(1) 表示項目

表示項目は以下に示すものであります。

- 1.最新の 5 秒間の平均 CPU 負荷率(%)
- 2.最新の 1 分の平均 CPU 負荷率(%)
- 3.最新の 5 分の平均 CPU 負荷率(%)
- 4.mbuf 使用率(%)
- 5.mcb 使用率(%)
6. isakmp メモリ使用率(%)
- 7.network メモリ使用率(%)

1 ~ 3 の項目については装置ブート後 5 分以内は "Not Enough Data" と表示され, 値が表示されません。(データが不足しているため)

【表示例】

・装置ブート後 5 分以上経過しているとき

```
#stssystem
CPU LOAD
5sec:60%      1min:55%      5min:54%
MEMORY USAGE
mbuf:20%      mcb:8%         isakmp:1%      network:2%
#
```

コマンドマニュアル

- ・ 装置ブート後 5 分以内のとき

```
#stsystem
CPU LOAD
Not Enough Data
MEMORY USAGE
mbuf:13%      mcb:0%      isakmp:0%      network:0%
#
```


tlog

`tlog` [-c|-n]

【内容】

トラップログを表示します。

【オプション】

-c	トラップログをクリアします。
-n	トラップログを新しい情報から順に表示します。

【パラメータ】

なし

【機能説明】

装置全体の重度障害情報として次の項目を表示します。

通し番号, 装置稼働時間, 日付, タスク ID , ログ ID , エラーコード, ログメッセージ

【メモ】

トラップログの最大ログ件数は 32 件です。32 件以上のログは、最も古いログから上書きしていきます。

traceroute

```
traceroute [-m <max_ttl>]
           [-p <port#>] <ip address>
```

【内容】

目的の宛先までの経路（ルータ）を調べます。

【オプション】

-m	<最大検索経路数>の指定．検索する経路数を指定します．指定の経路数以上の調査は行いません． 工場出荷時は32です．
-p	<ポート番号>の指定．経路数を調べるときに使用するポート番号を指定します． 工場出荷時は33434です．

【パラメータ】

< ip address >	調べる先のIPアドレス
----------------	-------------

【機能説明】

<宛先 IP アドレス> に向けて調査用のデータパケットを送信することで，途中の各ルータの IP アドレスとそこまでの到達時間（m 秒）を表示します．調査用のデータパケットは途中のルータ毎に 3 回ずつ送信していき，時間も各々 1 回毎の結果を表示します．また，ルータから正常に通知がない場合は，時間表示が以下のように変わります．

原因	表示内容
タイムアウト（3 秒）	*
TTL が 1 以下発生	!
HOST UNREACHABLE 発生	! H
NETWORK UNREACHABLE 発生	! N
PROTOCOL UNREACHABLE 発生	! P
SOURCE ROUTE FILED 発生	! S
FRAGMENTATION NEEDED 発生	! F

vlog

vlog [-c | -n]

【内容】

イベントログを表示します。

【オプション】

-c	イベントログをクリアします。
-n	イベントログを新しい情報から順に表示します。
なし	イベントログを古い情報から順に表示します。

【パラメータ】

なし

【機能説明】

装置の機能的障害や回線状態の変化に含まれない事象のログ表示を目的として

” 通し番 装置稼働時間 日付 タスク ID ログ ID エラーコード ログメッセージ ”

の表示およびクリアを行います。

【メモ】

イベントログの最大ログ件数は 64 件です。64 件以上のログは、最も古いログから上書きしていきます。

vpncertinfo

vpncertinfo [cert|crl]

【内容】

証明書, CRL を表示します。

【オプション】

cert	証明書を表示します。
crl	CRLを表示します。
なし	証明書, CRLの両方が表示されます。

【パラメータ】

なし

【表示例】

```
vpncertinfo cert
[1]   Subject:xxx   --- サブジェクト(証明書の所有者)
Issuer:xxx         --- 発行者
Serial Number:xxx  --- シリアル番号
Validity: yyyy.mm.dd hh:mm:ss - yyyy.mm.dd hh:mm:ss --- 有効期間
Domain Name:xxx   --- サブジェクトのドメイン名
IP Address:x.x.x.x --- サブジェクトの IP アドレス
CRL DistPoint:xxx --- CRL 配布点(CRL が置かれている場所)
Key Usage:xxx     --- 鍵の使用用途
Email Address:xxx --- サブジェクトの Email アドレス

vpncertinfo crl
[1]   Issuer:xxx   --- 発行者
This Update:xxx   --- 更新日時
Next Update:xxx   --- 次回更新日時
```

vpncrlget

vpncrlget

【内容】

CRL(Certificate Revocation List : 証明書取り消しリスト)を取得します。CRLは、通常次のアップデート日時が決まっているため、CRLを使用するときにアップデート日時が過ぎていたら自動で新しいCRLを取得しますが、この操作では手動でCRLを取得することができます。

【オプション】

なし

【パラメータ】

なし

【表示例】

```
#vpncrlget
[1]      http://xxxxxx
[2]      CN=xx,O=xx,C=xx
Select no:1
Retreiving CRL http://xxxxxx ...
ok
#
```

vpnlog

vpnlog [-c|-n]

【内容】

VPN に関するログを表示します。

【オプション】

-c	ログをクリアします。
-n	ログを新しい情報から順に表示します。
なし	ログを古い情報から順に表示します。

【パラメータ】

なし

【機能説明】

VPN に関するログ

" 通し番 装置稼働時間 タスク ID ログ ID エラーコード ログメッセージ "

の表示およびクリアを行います。

【メモ】

- ・ イベントログの最大ログ件数は 64 件です。64 件以上のログは、最も古いログから上書きしていきます。
- ・ vpnlog を採取するためには、vpnopt コマンドで、"vpnlog=on" に設定しておく必要があります。

vpnsainfo

vpnsainfo [ike|ipsec]

【内容】

ike が指定されれば IKE SA を表示し、ipsec が指定されれば IPSEC SA を表示します。
省略された場合は IPSEC SA を表示します。

【オプション】

なし

【パラメータ】

ike	IKE SAを表示します。
ipsec	IPSEC SAを表示します。

【表示例】

・IPsecSA が存在するとき

```

IKE SA
[1] xxx.xxx.xxx.xxx 相手名前
  <--> xxx.xxx.xxx.xxx 自身名前
  <I> Aggressive Mode XAUTH pre-shared key DES MD5
  Lifetime:86400secs Current:0secs
[2] xxx.xxx.xxx.xxx
  <--> xxx.xxx.xxx.xxx
  <R> Main Mode UP pre-shared key DES SHA
  Lifetime:172800secs,4000000kbytes Current:123456secs,123456kbytes
IPSEC SA
current insa:2
current outsa:1
[1] xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx 0 0 --- 宛先
  <--> xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx 0 0 --- 送信元
peer:xxx.xxx.xxx.xxx 相手名前
<I> UP ESP DES HMAC-MD5 PFS:off Lifetime:28800secs
O-SPI:12345 Current:1234secs
  out packet :123 error packet :0
I-SPI:67890 Current:1234secs
  in packet :89 auth packet :89
  decrypt packet :89 discard packet :0
  replay packet :0 auth error packet :0
[2] xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx TCP 100
  <--> xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx TCP 0
peer:xxx.xxx.xxx.xxx 相手名前
<I> UP ESP DES HMAC-SHA PFS:on Lifetime:86400secs,2000000kbytes
O-SPI:1357 Current:3333secs,3456kbytes
  out packet :34 error packet :0
I-SPI:67893 Current:3333secs,1234567kbytes
  in packet :12345 auth packet :12345
    
```

コマンドマニュアル

```
decrypt packet :12345 discard packet :0  
replay packet :0 auth error packet :0
```

- ・ IPsecSA が存在しないとき

```
#vpnsainfo  
IPSEC SA  
current insa :0  
current outsa :0
```


vpnselectorinfo

vpnselectorinfo [`<selectorid>` | all]

【機能】

指定されたセクタ ID<selectorid>についての selector 情報（設定情報，統計情報）を表示します。

指定された ID のセクタが設定されていないときは "No Entry" を表示する。all が指定されたときは設定されている全セクタについて表示します。また，引数が省略された場合は全セクタについて表示します (all と同じ)。

【オプション】

selectorid	参照したいセクタ ID を指定する引数。指定した ID のセクタが設定されていればそのセクタに関する情報が表示され，設定されていない場合は "No Entry" と表示されます。この値の範囲は 1~1000 であり，この範囲を超えると "***range error xxx" が表示されます。
all	設定されている全セクタに関する情報を表示します。セクタが一つも設定されていないときは "***empty table" が表示されます。
なし	all を指定したときと同じ

【画面表示】

(1) 表示項目

セクタ情報については以下のものが表示されます。

1. セクタ ID
2. dst IP アドレス，アドレスマスク
3. src IP アドレス，アドレスマスク
4. プロトコル
5. dst ポート
6. src ポート
7. type
8. Peer IP アドレス/PeerName
9. Sa 確立回数（ブート後の合計）
10. Sa 確立時間（ブート後の合計）
11. 受信 Octet 数（ブート後の合計）
12. 送信 Octet 数（ブート後の合計）

1~8 の項目についてはセクタに設定されている値が (conf#vpnselector コマンドによる表示と同じ書式で) 表示されます。9~12 の項目（統計情報）については type=ipsec 以外

(type=bypass/discard)のときは常に0が表示されます。

(2) 表示例

・セレクト ID=1 を指定したとき

```
#vpnselectorinfo 1
id: 1 dst:158.202.232.82 255.255.255.255 src:158.202.233.127 255.255.255.255
  prot:all dstport:all srcport:all
  type:ipsec peer:158.202.232.82
  totalsa:2 totalsatime:1200(sec)
  inoctet:145376 outoctet:4313936
```

・all を指定したとき

```
#vpnselectorinfo all
id: 1 dst:158.202.232.82 255.255.255.255 src:158.202.233.127 255.255.255.255
  prot:all dstport:all srcport:all
  type:ipsec peer:158.202.232.82
  totalsa:2 totalsatime:1200(sec)
  inoctet:145376 outoctet:4313936
id: 2 dst:192.168.1.1 255.255.255.255 src:158.202.233.127 255.255.255.255
  prot:all dstport:all srcport:all
  type:ipsec peer:192.168.1.1
  totalsa:0 totalsatime:0(sec)
  inoctet:0 outoctet:0
id: 30 dst:all src:all
  prot:all dstport:all srcport:all
  type:bypass peer:
  totalsa:0 totalsatime:0(sec)
  inoctet:0 outoctet:0
#
```

vpnstat

vpnstat

【内容】

現在設定されている VPN の統計情報を表示します。

【オプション】

なし

【パラメータ】

なし

【機能説明】

VPN の統計情報の表示を行います。

以下に表示内容を示します。

PI send packet	Phase I 送信パケット数
PI receive packet	Phase I 受信パケット数
PI discard packet	Phase I 廃棄パケット数
PI decrypt error packet	Phase I 復号化エラーパケット数
PI hash error packet	Phase I ハッシュエラーパケット数
PI exchange fail	IKE SA 確立エラー数
PI exchange success	IKE SA 確立数
xauth send packet	拡張認証 送信パケット数
xauth receive packet	拡張認証 受信パケット数
xauth discard packet	拡張認証 廃棄パケット数
xauth exchange error	拡張認証 失敗数
xauth exchange success	拡張認証 成功数
PII send packet	Phase II 送信パケット数
PII receive packet	Phase II 受信パケット数
PII discard packet	Phase II 廃棄パケット数
PII decrypt error packet	Phase II 復号化エラーパケット数
PII hash error packet	Phase II ハッシュエラーパケット数
PII exchange fail	IPsec SA 確立エラー数
PII exchange success	IPsec SA 確立数
notify send packet	Notify メッセージ送信数
notify receive packet	Notify メッセージ受信数
other ISAKMP send packet	その他の ISAKMP パケット送信数
other ISAKMP receive packet	その他の ISAKMP パケット受信数
VPN discard packet	VPN 廃棄対象パケットとして廃棄したパケット数
ESP send packet	ESP 送信パケット数

コマンドマニュアル

ESP receive packet	ESP 受信パケット数
ESP discard packet	ESP 廃棄パケット数
ESP replay error packet	ESP リプレイアタックされたパケット数
ESP auth error packet	ESP 認証エラーパケット数
ESP send error	ESP 送信失敗数

clogcontrol

```
clogcontrol [on|off|
            [add [prot={tcp|udp|icmp|other|all}]
                [type={send[, {private|public|all}] | recv[, {private|public|all}]
                | fwd[, {private|public|all}]>{private|public|all}] | all]]]
            |[delete [prot={tcp|udp|icmp|other|all}]
                [type={send[, {private|public|all}] | recv[, {private|public|all}]
                | fwd[, {private|public|all}]>{private|public|all}] | all]]]
```

【内容】

装置内で廃棄されずに送受信または中継された IP パケットのログ機能の ON/OFF を制御します。

【オプション】

なし

【パラメータ】

on	ログ機能を有効にします。
off	ログ機能を無効にします。
add	ログ対象となるパケットのタイプを追加します。
delete	ログ対象となるパケットのタイプを削除します。
prot={tcp udp icmp others all}	パラメータに add または delete が指定された時の対象となるパケットのプロトコルを指定します。 無指定の場合は「all」となります。 設定範囲：tcp,udp,icmp,others,all tcp TCP パケットを指定します。 udp UDP パケットを指定します。 icmp ICMP パケットを指定します。 others 上記以外のパケットを指定します。 all すべてのプロトコルを指定します。 *TCP を指定した場合、記録されるのは SIN または FIN フラグが立っているパケットのみとなります。 工場出荷時：なし
type={send[, {private public all}] recv[, {private public all}] fwd[, {private public all}]>{private public all}] all}}	パラメータに add または delete が指定された時の対象となるパケットの通信方向を指定します。 無指定の場合は all ととなります。 設定範囲：

	<p>send[, {private public all}] 装置が各インタフェースへ送信したパケットログを記録します。インタフェースの指定がないまたは all の場合は両方のインタフェースへ送信されたパケットのログを記録します。</p> <p>recv[, {private public all}] 装置が各インタフェースから受信したパケットログを記録します。インタフェースの指定がないまたは all の場合は両方のインタフェースから受信したパケットのログを記録します。</p> <p>fwd[, {private public all}]>{private public all} 装置がフォワードしたパケットのログを記録します。フォワードパケットの受信インタフェース、送信インタフェースの順で指定します。 送受信インタフェースの指定がない時には装置がフォワードした全てのパケットのログを記録します。 *注意:送受信インタフェースは片方だけの指定はできません。</p> <p>all 装置が送信、受信、フォワードした全てのパケットのログを記録します。 工場出荷時：なし</p>
--	--

【機能説明】

パラメータが無指定の場合は、現在の設定内容を表示します。

記録されたログは clog コマンドで表示できます。

dhcpserver

```
dhcpserver [[off|on] [gateway={on|off}]
            [sendarpnum=< times >] [arptimeout=< 100msec >]
            [sendarpcount=< times >] [allocateaddr=< IP address >]
            [allocatewidth=< number >]]
```

【内容】

DHCP サーバの動作について設定します。

【オプション】

なし

【パラメータ】

off on	DHCP サーバ機能を利用する / しないを選択します。 工場出荷時：off
gateway={on off}	DHCP サーバを利用するとした時、LAN インタフェースのアドレスをデフォルトゲートウェイ通知をするか / しないかを選択します。 工場出荷時：on
sendarpnum=< times >	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対象アドレス件数（ARP 単位）を設定します。 設定範囲：1～255 工場出荷時：16
arptimeout=< 100msec >	同上の調査時に割り当て可能とする為のタイムアウト値（ARP タイムアウト）を設定します。 設定範囲：1～255 工場出荷時：10
sendarpcount=< times >	同上の調査時に調査用の ARP を送信する回数（ARP リクエスト送信回数）を設定します。 設定範囲：0～255 工場出荷時：1
allocateaddr=< IP address >	割り当て開始 IP アドレスの先頭値（DHCP アロケート開始アドレス）を設定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
allocatewidth=< number >	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。 設定範囲：1～255 工場出荷時：100

【機能説明】

DHCP サーバ機能が "on" の時 "allocateaddr" から始まり, "allocatewidth" で示される分の IP ホストアドレスを割り当てます .

例外として "allocateaddr" が 0.0.0.0 の場合は, LAN インタフェースに設定された IP アドレスが属するネットワーク番号内の最初のホストアドレスから "allocatewidth" で示される分の IP ホストアドレスを割り当てます .

「IP アドレス」が割り当て可能かどうかは ARP によりチェックしますが (ARP の応答がタイムアウトした内容を配信可能アドレスとします), まずは装置立ち上がり時に "sendarpnum" 分のアドレスを "sendarpcount" 回送信した結果を反映します .

装置運用中に "sendarpnum" 分のアドレスを使い切った場合には, 配信要求毎に ARP の交換を行い調査した結果を割り当てます .

exit

exit

【内容】

現在がログイン状態の場合、ログインプロンプトに戻ります。

現在がコンフィグレーションモードの場合、それを終了し、ログイン状態へ戻ります。

【オプション】

なし

【パラメータ】

なし

【機能説明】

装置からログアウトします。また現在のモードがコンフィグレーションモードの場合、それを終了し、ログイン状態へ戻ります。

コンフィグレーションモード時に設定内容を変更した場合は、ログイン状態に戻る時にその内容を装置に保存しようとしています。

保存が必要な時は "configuration modified. save OK? (y/n):" と表示されますので、"y" を入力してください。"n" を入力すると、設定してきた内容は無効となり、コンフィグレーションモードに入る前の状態に戻ります。

"y" と入力し、設定モードを終了したら reset コマンドを入力することにより装置をリセットします(リセットを行わないと変更した内容が装置に対して有効になりません)。“n” と入力し、装置に設定内容を保存しないでコンフィグレーションモードを終了したときは、装置をリセットする必要はありません。

flogcontrol

`flogcontrol` [on|off]

【内容】

IP フィルタリングにより廃棄されたパケットのログ記録の ON/OFF を行います。

【オプション】

なし

【パラメータ】

on	ログ機能を有効にします。
off	ログ機能を無効にします。

【機能説明】

パラメータが無指定の場合は、現在の設定内容を表示します。

記録されたログは `flog` コマンドで表示できます。

help

[help | ?] [-l | < command >]

【内容】

指定コマンドの usage を表示します .

【オプション】

-l	コマンドが投入された時のモードで使用できるすべてのコマンドの usage を表示します . モードにはログイン状態 (ログインモード) と コンフィグレーションモードがあります .
----	--

【パラメータ】

< command >	usage を表示させたいコマンド名
-------------	--------------------

【機能説明】

オプションやパラメータの指定がない場合は , コマンドが投入された時のモードで使用できるすべてのコマンド名だけを表示します .

hostname

```
hostname [nameserver=< IPaddress >[,< IPaddress >]]
        [netbiosserver=< IPaddress >[,< IPaddress >]]
        [domainname=[domain name]]
        [defaultgw=<IPaddress>]
```

【内容】

DHCP で通知する各種情報を設定します。

【オプション】

なし

【パラメータ】

nameserver=< IPaddress >[,< IPaddress >]	DHCP 通知項目としてネームサーバの IP アドレスを登録します。 ", "で区切られた左側の IP アドレスが優先的（プライマリ）に利用されます。 設定範囲：プライマリ IP アドレス，セカンダリ IP アドレス
netbiosserver=< IPaddress >[,< IPaddress >]	DHCP 通知項目として NetBios サーバの IP アドレスを最大 2 件まで登録します。 ", "で区切られた左側の IP アドレスが優先的（プライマリ）に利用されます。 設定範囲：プライマリ IP アドレス，セカンダリ IP アドレス
domainname=< domain name >	DHCP 通知項目としてドメイン名称を登録します。 設定範囲：最大 40 文字の ASCII データ
defaultgw=<IPaddress>	通知するデフォルトゲートウェイの IP アドレスを設定します。

【機能説明】

パラメータが無指定の場合は，現在の設定内容を表示します。装置導入時は未登録です。

デフォルトホスト名称の設定は 1 件のみとなります。

現状ではデフォルトホスト名称に対応する内容(nameserver ,netbiosserver ,domainname)のみが DHCP での通知対象となります。

hosttable

```
hosttable [[add mac=< MAC address > ip=< IP address >]
          [delete [all|[[mac=< MAC address >]|[ip=< IP address >]]]]]
```

【内容】

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ます。

【オプション】

なし

【パラメータ】

add	指定データの登録を指定します。
delete [all]	指定データの削除を指定します。 all 指定時は登録されているすべてのデータを削除します。
mac= < MAC address >	端末の指定としてその MAC アドレスを指定します。 設定範囲：00:00:00:00:00:00 ~ ff:ff:ff:ff:ff:ff 工場出荷時：なし
ip= < IP address >	端末に対応する IP アドレスを指定します。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：なし

【機能説明】

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ます。

端末は MAC アドレスで指定し、16 台分の IP アドレスを割り付けることができます。

identifier

```
identifier [[node=< nodename >]
           [manager=< managername >] [location=< nodelocation >]
```

【内容】

装置固有の識別子の設定を行います。

【オプション】

なし

【パラメータ】

node=< nodename >	装置名称を指定' 'を指定時は NULL の入力とし設定内容を消します。 設定範囲：最大 32 文字の英数字 工場出荷時：なし
manager=< managername >	管理者名を指定' 'を指定時は NULL の入力とし設定内容を消します。 設定範囲：最大 32 文字の英数字 工場出荷時：なし
location=< nodelocation >	装置の物理的位置を指定' 'を指定時は NULL の入力とし設定内容を消します。 設定範囲：最大 64 文字の英数字 工場出荷時：なし

【機能説明】

パラメータが無指定の場合は、現在の設定内容を示します。

hereis コマンドで確認できます。

node の内容が設定されていない状態で、hostname コマンドで「デフォルトホスト」を設定すると、その内容は node にも反映されます。

装置導入時は未登録です。

ifaccept

```
if accept [[add dst=< ipaddress > [, < ipaddressmask > ]
          [recvif={private,public}]
          |[delete {all}|[dst=[ < ipaddress > ][, < ipaddressmask > ]]]
          [recvif={private,public}]
```

【内容】

RIP パケットを受信するときに有効（あるいは無効）にするルーティング情報を設定します。

【オプション】

なし

【パラメータ】

add	指定のフィルタリングテーブルを登録します。
delete [all]	指定のフィルタリングテーブルを削除します。 「all」を指定すると全エントリを削除します。
dst=< ipaddress >	受信ルーティング情報の宛先 IP アドレスを指定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし
, < ipaddressmask >	受信ルーティング情報の宛先 IP アドレスに対するマスクパターンを指定します。省略されると 255.255.255.255 を採用します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：255.255.255.255
recvif={private,public}	受信インタフェースを指定します。 省略するとすべてのインタフェースが対象となります。 設定範囲：private,public 工場出荷時：全てのインタフェース

【機能説明】

パラメータ指定がない場合は登録されたテーブルの内容一覧を表示します。
また、IP アドレスとマスクの掛け合わせた結果適用される IP アドレスを（）内で示します。

本テーブルのモード（テーブルに設定した RIP 情報を有効として扱う / 無効として扱う）の切り替えは、iprouting コマンドで行ってください。

装置導入時、本テーブルは未登録状態です。

ifpropagate

```
ifpropagate [[add dst=< ipaddress >[, < ipaddressmask >]
             [sendif={private,public}]
             |[delete {all}|[dst=[ < ipaddress >][, < ipaddressmask >]]
             [sendif={private,public}]
```

【内容】

RIP パケットを送信するときには有効（あるいは無効）にするルーティング情報を設定します。

【オプション】

なし

【パラメータ】

add	指定のフィルタリングテーブルを登録します。
delete [all]	指定のフィルタリングテーブルを削除します。 「all」を指定すると全エントリを削除します。
dst=< ipaddress >	送信ルーティング情報の宛先 IP アドレスを指定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし
, < ipaddressmask >	送信ルーティング情報の宛先 IP アドレスに対するマスクパターンを指定します。省略されると 255.255.255.255 を採用します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：255.255.255.255
sendif={private,public}	送信インタフェースを指定します。 省略するとすべてのインタフェースが対象となります。 設定範囲：private,public 工場出荷時：全てのインタフェース

【機能説明】

パラメータ指定がない場合は登録されたテーブルの内容一覧を表示します。
また、IP アドレスとマスクの掛け合わせた結果適用される IP アドレスを（）内で示します。

本テーブルのモード（テーブルに設定した RIP 情報を有効として扱う / 無効として扱う）の切り替えは、iprouting コマンドで行ってください。

装置導入時、本テーブルは未登録状態です。

interface

```
interface [[ip] [down|{ private|public }
           [down|[addr=[< address >][,< subnetmask >]]
           [remote=[< remoteaddress >][,< remotesubnetmask >]
           |broadcast[=< broadcastaddress >]]]]]
```

【内容】

IP ルーティングの使用の有無および使用する場合のインタフェースに関する設定を行います。

【オプション】

なし

【パラメータ】

ip	IP ルーティングを使用する場合に指定します。 この項目は指定しなくても工場出荷時で有効となっています。
private public	設定を行うインタフェースを指定します。 設定範囲：private,public
down	指定インタフェースのルーティングを OFF にします。インタフェースの指定がない場合はすべてのインタフェースが対象になります。
addr= < address >	インタフェースアドレスを指定します。インタフェースタイプがポイントツーポイント PUBLIC LAN の場合は省略することができます。この場合、PRIVATE LAN 側のインタフェースアドレスが設定されます。インタフェースタイプがブロードキャスト PUBLIC LAN の場合は省略することはできません。 設定範囲：0.0.0.0 ~ 126.255.255.255 128.0.0.0 ~ 255.255.255.255 工場出荷時：private=192.52.150.100
, < subnetmask >	< address > に対するサブネットマスクを設定します。インタフェースタイプがポイントツーポイントの PUBLIC LAN の設定では設定は必要ありません。インタフェースタイプがブロードキャストの場合、新規登録時に設定が省略されると、上記の< address >がクラス A では 255.0.0.0、クラス B では 255.255.0.0、クラス C では 255.255.255.0 が設定されます。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：private =255.255.255.0

コマンドマニュアル

remote= < remoteaddress >	PUBLIC LAN の接続先インタフェースのアドレスを設定します。 本設定を行うことにより、インタフェースタイプがポイントツーポイントに指定されます。 設定範囲：0.0.0.0～126.255.255.255 128.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
, < remotesubnetmask >	< remoteaddress > のサブネットマスクを指定します。 新規登録時に設定が省略されると 255.255.255.255 が設定されます。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
broadcast [= < broadcastaddress >]	インタフェースタイプがブロードキャストの時に PUBLIC LAN 側のブロードキャストアドレスを指定します。省略時は、ホスト部がオール1のアドレスが設定されます。 設定範囲：0.0.0.0～126.255.255.255 128.0.0.0～255.255.255.255 工場出荷時：lan=192.52.150.255

【機能説明】

パラメータが無指定の場合は、現在の設定内容を示します。

装置リセット後、有効となった内容は ipinterface コマンドで確認できます。

ipfiltering

```
ipfiltering  {[-f]|-d}
              [[add dst=< ipaddress > [, < ipaddressmask > ]
               [dstport=< portnumber > [, < portnumber > ]]
               src=< ipaddress > [, < ipaddressmask > ]
               [srcport=< portnumber > [, < portnumber > ]]
               [prot={tcp/udp|icmp|tcp|udp|all| < protocolnumber > }]
               [recvif={private,public}]
               [sendif={private,public}] [full|half]]
| [delete {all|[dst=< ipaddress > ][, < ipaddressmask > ]]
         [dstport=< portnumber > [, < portnumber > ]]
         [src=< ipaddress > ][, < ipaddressmask > ]]
         [srcport=< portnumber > [, < portnumber > ]]
         [prot={tcp/udp|icmp|tcp|udp|all| < protocolnumber > }]
         [recvif={private,public}]
         [sendif={private,public}] [full|half]]}]
```

【内容】

IP パケットフィルタリングテーブルを設定します。

【オプション】

-f	フォワードフィルタリングを指定します。(一致したパケットを中継する)
-d	ディスカードフィルタリングを指定します。(一致したパケットを廃棄する)
なし	'- f 'が指定された場合と同じ。

【パラメータ】

add	指定のフィルタリングテーブルを登録します。
delete [all]	指定のフィルタリングテーブルを削除します。 「all」を指定すると全エントリを削除します。
prot={tcp/udp icmp tcp udp all < protocolnumber > }	フィルタリングの対象とするパケットのプロトコルを指定します。 無指定の場合は「all」となります。 設定範囲：tcp/udp, icmp, tcp, udp, all 工場出荷時：all
src=< ipaddress >	フィルタリングの対象とするパケットの送信元 IP アドレスを指定します。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：なし
, < ipaddressmask >	「src」に対するマスクパターンを指定します。 「すべてのアドレス」を指定する場合は0.0.0.0を指定し

	<p>ます . 設定範囲 : 0.0.0.0 ~ 255.255.255.255 工場出荷時 : なし</p>
srcport= < portnumber >	<p>フィルタリングの対象とするパケットが TCP あるいは UDP の場合 , 送信元ポートを指定します . ポート番号は範囲指定する必要があります . ここでは , 送信元フィルタリングの対象となるポートの最小ポート番号を指定します . 値が無指定の場合は 0 となります . 設定範囲 : 0 ~ 65535 工場出荷時 : 0</p>
, < portnumber >	<p>送信元フィルタリングの対象となるポートの最大ポート番号を指定します . 値が無指定の場合は 65535 となります . 設定範囲 : 0 ~ 65535 工場出荷時 : 65535 メモ TCP や UDP で使用されるポート番号は , TCP や UDP より上位に位置する各プログラム (プロセス) の識別子のことをさします . IP アドレスとポート番号の組み合わせで , データを送信するプロセスが正確に決定されます . ポート番号には , 統一的に割り当てられている番号 (ウェルノウンポート番号) と , 動的に割り当てられる番号 (テンポラリポート) の 2 種類があります .</p>
dst= < ipaddressmask >	<p>フィルタリングの対象とするパケットの宛先 IP アドレスを指定します . 設定範囲 : 0.0.0.0 ~ 255.255.255.255 工場出荷時 : なし</p>
, < ipaddressmask >	<p>「dst」に対するマスクパターンを指定します . 設定範囲 : 0.0.0.0 ~ 255.255.255.255 工場出荷時 : なし</p>
dstport= < portnumber >	<p>フィルタリングの対象とするパケットが TCP あるいは UDP の場合 , 宛先ポートを指定します . ポート番号は範囲指定する必要があります . ここでは , 宛先フィルタリングの対象となるポートの最小ポート番号を指定します . 値が無指定の場合は 0 となります . 設定範囲 : 0 ~ 65535 工場出荷時 : 0</p>
, < portnumber >	<p>宛先フィルタリングの対象となるポートの最大ポート番号を指定します . 値が無指定の場合は 65535 になります .</p>

	設定範囲：0～65535 工場出荷時：65535
recvif={ private,public }	無指定の場合は全インタフェースとなります。 設定範囲：private,public 工場出荷時：全てのインタフェース
sendif={ private,public }	送信インタフェースを指定します。 無指定の場合は全インタフェースとなります。 設定範囲：private,public 工場出荷時：全てのインタフェース
full half	指定したパケットに対する応答パケットをフィルタリングの対象とする場合は、「full」を指定します。 指定したパケットに対する応答パケットをフィルタリングの対象としない場合は「half」を指定します。無指定の場合は「full」となります。 設定範囲：full, half 工場出荷時：full

【機能説明】

パラメータ指定がない場合は登録されたテーブルの内容一覧を表示します。

IP フィルタリング機能そのものが有効なときに、このテーブル内容が利用されます。IP フィルタリング機能の ON/OFF は iprouting コマンドを参照してください。

IP フィルタリングは中継条件を満たした内容を遮断条件に照らし合わせる方法をとっています。

IP フィルタリング機能が有効であるときに、IP フィルタリングテーブルの中継側に 1 件も登録がない場合は、すべてのパケットが遮断されてしまいます。

特定のパケットだけを遮断したい場合は、すべてが中継されるような中継条件の登録もしてください。

ipripstatic

```
ipripstatic [[add {default=< ipostaddress >
               |dst=< ipaddress >[,< ipaddressmask >
               {nexthop=< ipostaddress >}
            |[delete {all|default|[dst=< ipaddress >][,< ipaddressmask >]]
               {nexthop=< ipostaddress >}]}
```

【内容】

IP スタティックルーティングテーブルを設定します。

【オプション】

なし

【パラメータ】

add	指定のスタティックテーブルを登録します。
delete [all]	指定のスタティックテーブルを削除します。 「all」を指定すると全エントリを削除します。
default = { < ipostaddress > }	デフォルトルートを設定する場合の、< ipostaddress > (中継先ルータアドレス)を指定します。
dst=< ipaddress >	ルーティング情報の宛先 IP アドレスを指定します。 デフォルトルートを指定するときは 0.0.0.0 と入力してください。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
, < ipaddressmask >	ルーティング情報の宛先 IP アドレスに対するマスクパターンを指定します。省略されると 255.255.255.255 を採用します。 デフォルトルートを指定するときは<宛先 IP ネットワークアドレス>と同様に 0.0.0.0 と入力してください。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
nexthop=< ipostaddress >	「dst」で指定された宛先へパケットを送信する場合の、< ipostaddress > (中継先ルータアドレス)を指定します。

【機能説明】

パラメータ指定がない場合は登録された有効なテーブルの内容一覧を表示します。
装置導入時は未設定です。

iprouting

iprouting

```
[[on|off] [[proxyarp={off|shortcut|any}] [filtering[={on|off}]]
[rip[={on|off}]] [ifaccept={exclude|include}]
[ifpropagate={exclude|include}]]
```

【内容】

IPルーティングを使用する場合、ProxyARP、RIPの動作モードおよびRIPパケットのフィルタリングの制御に関する設定を行います。

【オプション】

なし

【パラメータ】

[on off]	IPルーティングを使用するかどうか指定します。 設定範囲：on, off 工場出荷時：on
proxyarp = { off shortcut any }	Proxy ARPの動作モードを指定します。 off 動作しない shortcut 中継すべきアドレスのARPに答える any すべてのアドレスのARPに答える 設定範囲：off, shortcut, any 工場出荷時：shortcut
filtering [= { on off }]	IPフィルタリングを使用する場合に指定します。使用しない場合は「off」を指定します。 設定範囲：on, off 工場出荷時：off
rip[={on off}]	RIPを利用したルーティング（ダイナミックルーティング）の動作（on：する、off：しない）を指定します。「しない」とした場合、スタティックルーティングのみの動作となります。 設定範囲：on, off 工場出荷時：off
ifaccept = { exclude include }	RIPフィルタリング機能（ifaccept）の動作モードを設定します。RIPパケット受信時、インタフェース毎に有効にする（あるいは無効にする）情報を限定することができます。「exclude」とした場合、テーブル（「RIPフィルタリング（ifaccept）の設定」）に設定されているエントリに一致しないものを有効にします。「include」とした場合は一致したものを有効にします。 設定範囲：exclude, include 工場出荷時：exclude

ifpropagate = { exclude include }	RIP フィルタリング機能 (ifpropagate) の動作モードを設定します。 RIP パケット送信時、インタフェース毎に有効にする (あるいは無効にする) 情報を限定することができます。「exclude」とした場合、テーブル (「RIP フィルタリング (ifpropagate) の設定」) に設定されているエントリに一致しないものを有効にします。 「include」とした場合は一致したものを有効にします。 設定範囲：exclude, include 工場出荷時：exclude
---	--

【機能説明】

パラメータがすべて無指定の場合は、IP ルーティングの各機能に対応した設定状況を表示します。

manager

```
manager [[add <index>
        [addr=ipaddress] name=<community name>
        [mode={trw|rw|tr|r}]]
|[delete {<index>|all}]]
```

【内容】

SNMP マネージャに関する情報および動作モードを設定します。

【オプション】

なし

【パラメータ】

add <index> [delete {<index> all}]	指定のテーブルを登録および削除します。テーブルは最大4件登録できます。
addr=ipaddress	SNMP マネージャの IP アドレスを指定します。「0.0.0.0」はデフォルトマネージャ（すべての装置が本装置の SNMP エージェント機能を使用可能）のエントリを示します。省略時は、0.0.0.0 となります。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：0.0.0.0
name=<community name>	SNMP マネージャと通信する場合のコミュニティ名を英数字 32 文字以内で指定します。 設定範囲：最大 32 文字の英数字 工場出荷時：public
mode={trw rw tr r}	マネージャの動作モードを指定します。省略時は r となります。 設定範囲：trw, rw, tr, r 工場出荷時：r

【機能説明】

パラメータ指定がない場合は内容の一覧を、「マネージャホストアドレス、コミュニティ名、動作モード」の順に表示します。

more

`more [on|off|<lines>]`

【内容】

表示サスペンド機能を制御します。

【オプション】

なし

【パラメータ】

off	moreを「無効」に設定します。
on	moreを「有効」に設定します。
<lines>	moreを「有効」に設定し、その時の有効表示行数を指定します。 設定範囲：0～255 工場出荷時：23行

【機能説明】

表示サスペンド機能(MORE表示)の有効/無効を設定します。パラメータの指定が無い時は現在の状態を表示します。

表示をサスペンドするまでの表示行数を<lines>で指定します。行数の指定を行うと自動的に機能が「有効」となります。行数に0を指定すると装置デフォルト(23行)を設定します。

nat

```

n a t  [{nat|natp|off}]
        [t1=<min>] [t2=<min>] [t3=<min>] [t4=<min>]
        [t5=<min>] [t6=<min>] [t7=<min>]
    
```

【内容】

NAT+plus 機能の選択を行います。

【オプション】

なし

【パラメータ】

{nat natp off}	<p>NAT +plus 機能の使用 / 不使用とアドレス変換モードを設定します。</p> <p>nat : NAT 優先モードで NAT +plus 機能を使用します。</p> <p>natp : NATP モードで NAT +plus 機能を使用します。</p> <p>off : NAT +plus 機能を使用しません。</p> <p>また、on を指定すると natp が指定されます。</p> <p>NAT 優先モード：通常の NAT によりアドレス変換を行い、変更アドレスが残り 1 つになった時、そのアドレスで NAT+ の変換を行います。</p> <p>NAT+モード：最初から NAT+ の変換を行います。</p> <p>設定範囲：nat, natp, off</p> <p>工場出荷時：off</p>
t1=<min>	<p>NAT 動的アドレス変換テーブルエントリタイムアウト時間を設定します。</p> <p>ここで "0" を設定した場合は、タイムアウトしません。</p> <p>通常、本項目を変更する必要はありません。</p> <p>設定範囲：0 ~ 1440</p> <p>工場出荷時：1440</p>
t2=<min>	<p>NATP 動的アドレス変換テーブルエントリUDPタイムアウト時間を設定します。</p> <p>通常、本項目を変更する必要はありません。</p> <p>設定範囲：1 ~ 1440</p> <p>工場出荷時：5</p>
t3=<min>	<p>NATP 動的アドレス変換テーブルエントリTCPタイムアウト時間を設定します。</p> <p>通常、本項目を変更する必要はありません。</p> <p>設定範囲：1 ~ 1440</p> <p>工場出荷時：60</p>

t4=<min>	NATP 動的アドレス変換テーブルエントリ及び、NAT FTP テーブルエントリにおけるTCP (FIN, RST受信後) タイムアウト時間を設定します。 通常、本項目を変更する必要はありません。 設定範囲：1～1440 工場出荷時：1
t5=<min>	FTP テーブルタイムアウト時間 (PORT コマンド受信からDATA 転送まで) を設定します。 通常、本項目を変更する必要はありません。 設定範囲：1～1440 工場出荷時：1
t6=<min>	FTP テーブルタイムアウト時間を設定します。 通常、本項目を変更する必要はありません。 設定範囲：1～1440 工場出荷時：60
t7=<min>	NATP 動的アドレス変換テーブルエントリICMP タイムアウト時間を設定します。 通常、本項目を変更する必要はありません。 設定範囲：1～1440 工場出荷時：1

【機能説明】

NAT+plus 機能の有効無効を設定します。

また、パラメータ指定がない場合は内容の一覧を表示します。

natnotrans

```
natnotrans  [[add private=<ipaddress>,<ipmask>]]
            [[delete {all|private=<ipaddress>}]]
```

【内容】

変換しない LAN 側のプライベート IP アドレスを設定します。

ここで設定しないプライベートアドレスは「変換後のアドレス範囲」にしたがって NAT 変換されます。

【オプション】

なし

【パラメータ】

add	指定のIPアドレスの組み合わせを登録します。
delete {all}	指定のIPアドレスと一致する変換しないIPアドレスを削除します。「all」を指定すると全ての変換しないIPアドレスを削除します。
private=<ipaddress>	LAN 側のプライベート IP アドレスを指定します。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：なし
<ipmask>	ipaddress に対するマスクの値を設定します。設定が省略されると 255.255.255.255 が設定されます。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：255.255.255.255

【機能説明】

パラメータ指定がない場合は内容の一覧を表示します。

natplusstatictable

```

natplusstatictable [[add virtual=[< IP address >],< port No >
                    local=< IP address >,< port No >]
[delete [all|[virtual=[< IP address >],< port No >
| local=< IP address >,< port No >]]]]

```

【内容】

NAT +plus 機能に関するスタティック設定を行います。

【オプション】

なし

【パラメータ】

add	データを登録します。
delete [all]	指定データを削除します。all指定時はすべてのデータを削除します。
virtual=[< ipaddress >], < port No >	変換先IPアドレスとなるPUBLIC LANインタフェースIPアドレスとポート番号を指定します。変換先IPアドレスをダイヤルアップ接続で取得する場合は、アドレス値を省略できます。
local=< ipaddress > , < port No >	PRIVATE LAN側に存在する端末のIPアドレスと使用するポート番号を設定します。

【機能説明】

local パラメータで示される PRIVATE LAN 側アドレスとポート番号の組と virtual パラメータで示される PUBLIC LAN 側アドレスとポート番号の組との間で IP アドレス変換が行われるようにデータを登録します。

natport

```

n a t p o r t    [[add rcvport=<Port No.>
                  refport=< Port No.>]
                 [delete  [all][rcvport=< Port No.>]
                       [ refport=< Port No.>]]]]

```

【内容】

NAT +plus 機能を利用している環境で、PRIVATE LAN 側に存在するクライアント (PC) の受信用特定ポート宛にパケットを送信してくる PUBLIC LAN 側のサーバと通信を行う為に、このポート番号とサーバ宛の特定ポート番号を登録します。

【オプション】

なし

【パラメータ】

add	データを登録します。
delete [all]	指定データを削除します。all指定時はすべてのデータを削除します。
rcvport=< Port No.>	外部のサーバからのパケットをPRIVATE LAN側のクライアント (PC) で受信する時のポート番号。
refport=< Port No.>	PUBLIC LAN側のクライアント (PC) が外部のサーバにパケットを送信する時の宛先ポート番号

【機能説明】

NAT +plus 機能が有効なときに、PUBLIC LAN 側から受信したパケットの宛先アドレスを、"refport"で登録したポート宛のパケットを発行した PRIVATE LAN 側の PC の IP アドレスで置き換えます。

"refport"の決定は、一緒に"rcvport"で登録したポート番号と PUBLIC LAN 側から受信したパケットの宛先ポート番号が一致するものとします。

【注意】

"rcvport"で登録するポート番号と natplusstatictable コマンドの"local"で登録するポート番号が同じ場合、natplusstatictable コマンドで登録した内容が有効になります。複数の PC が同一のサーバに対してアクセスする場合はご利用できません。

natrange

```
natrange [[add begin=<ipaddress> end=<ipaddress>]
          |[delete {all|begin=<ipaddress>}]]
```

【内容】

NAT で変換する PUBLIC LAN 側アドレス（グローバル IP アドレス）の範囲を設定します。

【オプション】

なし

【パラメータ】

add	指定のグローバルIPアドレスの範囲を登録します。
delete {all}	指定の先頭のIPアドレスと一致するグローバルIPアドレスの範囲を削除します。「all」を指定すると全てのグローバルIPアドレスの範囲を削除します。
begin=<ipaddress>	NAT 機能で変換する PUBLIC LAN 側の IP アドレス範囲の先頭の IP アドレスを設定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし
end=<ipaddress>	NAT 機能で変換する PUBLIC LAN 側の IP アドレス範囲の最後の IP アドレスを設定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし

【機能説明】

パラメータ指定がない場合は内容の一覧を表示します。

natstatictable

```
natstatictable [[add local=<ipaddress> global=<ipaddress>]
                [delete {all|local=<ipaddress>|global=<ipaddress>}]]
```

【内容】

NATに関するスタティック設定を行います。

【オプション】

なし

【パラメータ】

add	データを登録します。
delete [all]	指定データを削除します。all指定時はすべてのデータを削除します。
local=< ipaddress >	PRIVATE LAN 側のアドレスを指定します。 local=< ipaddress > の形式での入力も可能です。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし
global=< ipaddress >	PUBLIC LAN 側のアドレスを指定します。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし

【機能説明】

指定の PRIVATE LAN 側アドレスと指定の PUBLIC LAN 側アドレスの間で変換が行われるようにデータを登録します。

rgrpparam

`rgrpparam [on|off]`

【内容】

ルータグループ化機能を動作させるか否かを設定します。

【オプション】

なし

【パラメータ】

on	動作させる
off	動作させない

rgrptable

```
rgrptable [add|delete|set]
  [add id=<vrid>
    [priority=<priority>]
    addr={owner|<address on private>,<address on public>}
    [sendinterbal=<1sec>]
    [preempt={on|off}]
  set id=<vrid>
    [priority=<priority>]
    [address={owner|<address on private>,<address on public>}]
    [sendinterval=<1sec>]
    [preempt={on|off}]
  delete[all|[id=<vrid>]
    [priority=<priority>]
    [address={owner|<address on private>,<address on public>}]
    [sendinterval=<1sec>]
    [preempt={on|off}]
```

【内容】

RGRP 機能を使用する場合は、RGRP グループに属している必要があります。
本コマンドで RGRP グループの設定を行います。

【オプション】

なし

【パラメータ】

id=<vrid>	この設定は RGRP グループを形成する他の INFONET-VP100 と同じである必要があります。 設定範囲：1～255 工場出荷時：なし
priority=<priority>	1～254：ルータの優先度（大きい数字ほど優先度は高い） 設定範囲：1～254 工場出荷時：100
address={owner <address on private>,<address on public>}	Master ルータが使用する IP アドレス。 （注）自局の Interface IP アドレスと同一の設定を行った場合、Master ルータ候補（“IP Address Owner” という）となる。 （注）複数のインタフェースにて同時に管理させたい場合、各

	<p>インタフェース毎に IP アドレスを設定する . 設定範囲 : owner , address on private , address on public 工場出荷時 : なし</p>
sendinterval=<1sec>	<p>Master ルータが送信する VRRP 公告パケットの送信間隔 (秒) 設定範囲 : 1 ~ 30 秒 工場出荷時 : 1 秒</p>
preempt={on off}	<p>他に Master ルータがいる状態で , 自分に設定された Priority の方が高い場合 , 自分を Master ルータとして公告を開始するかどうかを設定する . ただし , IP Address Owner だった場合は , この設定に拘わらず常に on となる . 設定範囲 : on , off 工場出荷時 : off</p>

rtcontrol

```
rtcontrol [[ip] [{private|public}
           [sendinterval[={< sendinterval >|off}]]
           [send[={rip1|rip2|rip1rip2|off}]] [recv[={rip1|rip2|rip1rip2|off}]]
           [metric=< metric >] [ageout[={< ageouttime >|off}]]]]
```

【内容】

IP ルーティングにおけるルーティング情報の送受信の制御に関する設定をルーティングインタフェース毎に行います。

【オプション】

なし

【パラメータ】

ip	RIPの制御を指定します。 この項目は省略しても工場出荷時で有効になっています。
private public	設定を行うインタフェースを指定します。 設定範囲：private,public 工場出荷時：全てのインタフェース
sendinterval[={< sendinterval > off}	「sendinterval」のみ指定した場合はRIP情報の定期送信を行います。< sendinterval >は定期送信の送信間隔を指定します。0秒を指定した場合は、定期送信を停止します。「off」は0秒を指定した場合と同じ意味です。 設定範囲：off, 30~255 工場出荷時：lan=30, その他=off
send[={rip1 rip2 rip1rip2 off}	RIP情報の送信をする/しないを指定します。 「off」の指定がある場合は「しない」、 「on」の場合は「する」となります。 設定範囲：on, off 工場出荷時：lan=on, その他=off
recv[={rip1 rip2 rip1rip2 off}	RIP情報の受信をする/しないを指定します。 「off」の指定がある場合は「しない」、 「on」の場合は「する」となります。 設定範囲：on, off 工場出荷時：lan=on, その他=off
metric=< metric >	インタフェースのメトリック値を指定します。 RIPの受信時、「RIPパケットに設定されたメトリック' + 1 + '本設定値」をルーティング情報として保持します。 設定範囲：0~16 工場出荷時：0

ageout[={ < ageouttime > off}]	RIP で学習したルーティング情報のエージアウト時間 (< ageouttime >) を設定します。 「off」を指定するとエージアウトは行われません。 「0」は「off」と同じ意味です。 設定範囲：off, 30 ~ 65535 工場出荷時：lan=180, その他=0
---------------------------------------	--

【機能説明】

ルーティングプロトコルを指定するパラメータ以外の省略可能なパラメータがすべて無指定の場合は、ルーティングプロトコルに対応したすべての設定状況を表示します。インタフェースの指定がある場合は指定インタフェースの設定状況を表示します。

snmp

s n m p [on|off] [authtrap[={on|off}]]

【内容】

SNMP エージェント機能の使用の有無，トラップ送信を行う / 行わないを設定します。

【オプション】

なし

【パラメータ】

on off	本装置を SNMP エージェントとして使用する / しないを指定します。 設定範囲：on, off 工場出荷時：on
authtrap[={on off}]	認証失敗時，トラップを受け付けるマネージャに対して認証失敗 トラップを送信する / しないを指定します。 設定範囲：on, off 工場出荷時：on

【機能説明】

パラメータ指定がない場合は SNMP に関する登録内容を表示します。

syslogcontrol

`syslogcontrol [on|off]`

【内容】

syslogd が作動しているサーバに , syslog 情報を送信するかどうかを設定します .

【オプション】

なし

【パラメータ】

on off	syslogd が作動しているサーバに syslog 情報を送信する / しないを指定します . 設定範囲 : on, off 工場出荷時 : off
--------	---

【機能説明】

パラメータ指定がない場合は syslog 機能の設定内容を表示します .

syslogtable

```
syslogtable [[addr=<ipaddress>] [err={tlog|off}] [warning={elog|off}]
             [info={llog,vlog,vpnlog|off}] [notice={clog,flog,|off}]
             [facility=<no>]]
```

【内容】

syslog 情報を送信するサーバのアドレスを登録します。

【オプション】

なし

【パラメータ】

addr=<ipaddress>	syslogd サーバの IP アドレスを指定します。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：なし
err={tlog off}	tlog 情報を syslog に送信するかどうかの設定。 設定範囲：tlog, off 工場出荷時：なし
warning={elog off}	elog 情報を syslog に送信するかどうかの設定。 設定範囲：elog, off 工場出荷時：なし
info={llog,vlog,vpnlog off}	llog 情報を syslog に送信するかどうかの設定。 設定範囲：llog,vlog,vpnlog,off 工場出荷時：なし
notice={clog,flog, off}	clog,flog 情報を syslog に送信するかどうかの設定。 設定範囲：clog,flog,off 工場出荷時：off
facility=<no>	syslog 情報として送信する場合のファシリティを設定します。syslog のファシリティは、通常 syslogd で定義されています。特にいくつでなくてはいけないという値はありませんが、syslogd の設定でそのファシリティで受けた syslog パケットを保存するファイル名を指定しておく必要があります。 設定範囲：0 ~ 23 工場出荷時：1

コマンドマニュアル

【機能説明】

パラメータ指定がない場合は syslogtable の設定内容を表示します。

trustgateways

```
trustgateways [[add nexthop=< iphostaddress >]
               |[delete {all|nexthop=< iphostaddress >}]]
```

【内容】

有効なルーティング情報を提供してくれるゲートウェイの IP アドレスを設定します。

【オプション】

なし

【パラメータ】

add	指定のIPホストアドレスをトラストゲートウェイアドレスとして登録します。
delete [all]	指定のIPホストアドレスと一致するトラストゲートウェイアドレスをすべて削除します。「all」を指定すると全エントリを削除します。
nexthop=< iphostaddress >	有効なルーティング情報を提供してくれるゲートウェイの IP アドレスを指定します。登録されたゲートウェイからの RIP 情報のみ有効とします。登録がない場合はすべてのゲートウェイからの RIP 情報を有効とします。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：なし

【機能説明】

有効なルーティング情報を提供してくれるゲートウェイの IP アドレスを登録および削除します。

パラメータ指定がない場合は登録された内容の一覧を表示します。

装置導入時は未設定です。

vpn

v p n [off|on]

【内容】

VPN 通信を行うかどうかを設定します。

【オプション】

なし

【パラメータ】

[off on]	VPN 通信を行うかどうかの設定。 設定範囲：off, on 工場出荷時：off
----------	--

vpncert

```
vpncert [add [root]
        |[delete {all|id=<ID>}]
```

【内容】

証明書の追加/削除を行います。

【オプション】

なし

【パラメータ】

add	証明書の追加をします。
add [root]	信頼できるRoot CAの証明書の追加をします。
delete {all id=<ID>}	証明書の削除を行います。 all：全ての証明書を削除します。 id=<ID>：指定された証明書のみ削除します。

vpncertparam

```
vpncertparam [crl={use|notuse|must}]
              [domainname=<domainname>]
              [nameserver=<nameserver>]
              [ldapservers=<ldapservers>]
```

【内容】

証明書を使用して認証を行う場合に設定します。

【オプション】

なし

【パラメータ】

crl={use notuse must}	CRL を使用する/しないの選択をします。 use: 有効な CRL を取得できれば CRL チェックを行う。 有効な CRL が取得できなければ CRL チェックは行わない。 (CRL が保存されているサーバ停止, サーバとの通信不能等) not use: CRL チェックを行わない。 must: CRL チェックを必ず行う。 設定範囲: use, notuse, must 工場出荷時: use
domainname=<domainname>	本装置のドメイン名を設定します。 RSA signatures 認証使用時の自身のIDとなります。 設定範囲: 最大64文字のASCIIデータ 工場出荷時: なし
nameserver=<nameserver>	ネームサーバIPアドレスを設定します。 証明書にCRLのURLが含まれていてHTTPでCRLを取得する場合, URLからIPアドレスを求めるためにネームサーバを使用します。 工場出荷時: なし
ldapservers=<ldapservers>	LDAPサーバIPアドレスを設定します。 CRLがLDAPサーバにおかれている場合設定します。 工場出荷時: なし

vpncertreq

```
vpncertreq [CN=<CommonName>]
           [O=<Organization>]
           [C=<Country>]
           [domainname]
           [ip]
```

【内容】

自身の証明書のリクエストメッセージを生成し、PEM フォーマットで画面に表示します。
vpncertreq コマンドは、ログイン状態で使用します。

【オプション】

なし

【パラメータ】

CN=<CommonName>	一般名を表示します。 設定範囲：最大64文字
O=<Organization>	組織名を表示します。 設定範囲：最大64文字
C=<Country>	国名（2文字の国コード）を表示します。
[domainname]	証明書パラメータ(vpncertparam)で設定したdomainnameを証明書リクエストに入れる。
[ip]	証明書パラメータ(vpncertparam)で設定したipaddr(VP100の場合はpublic interfaceに設定したIPアドレス)を証明書リクエストに入れます。

vpngenkey

vpngenkey [size=<size>]

Exist. New key pair create OK?(y/n) 鍵ペアがすでに存在する場合表示されます。

【内容】

鍵ペアを生成する際に、公開鍵のサイズを設定します。

【オプション】

なし

【パラメータ】

size=<size>	公開鍵のサイズ(bits)を指定します。 設定範囲：512 ~ 2048 省略した場合は1024になります。
-------------	--

vpnikepolicy

```
vpnikepolicy  [{add|set} id=<ID>
                [encr={des|3des}]
                [method={prekey|rsasig}]
                [group={1|2}]
                [hash={md5|sha}]]
|[delete {all|[id=<ID>]
            [encr={des|3des}]
            [method={prekey|rsasig}]
            [group={1|2}]
            [hash={md5|sha}]]]
```

【内容】

IKE ポリシー (VPN ピアとの Phase I ネゴシエーション通信用ポリシー) エントリを設定します。

【オプション】

なし

【パラメータ】

add	エントリに登録します。最大エントリ数16
id=<ID>	ポリシーエントリの識別子。 設定範囲：1～16 工場出荷時：なし
encr={des 3des}	暗号アルゴリズムを選択します。 設定範囲：des, 3des 工場出荷時：des
method={prekey rsasig}	認証方法を選択します。 設定範囲：prekey, rsasig 工場出荷時：prekey
group={1 2}	鍵計算に使用するDiffie-Hellman Groupを選択します。 設定範囲：1, 2 工場出荷時：1
[hash={md5 sha}]	ハッシュアルゴリズム。 設定範囲：md5, sha 工場出荷時：md5

vpnopt

`vpnopt [vpnlog[={on|off}]]`

【内容】

VPN 動作時にイベントを vpnlog に残すかどうかを設定します。

【オプション】

なし

【パラメータ】

on off	on : IKE SA 確立 , IPSEC SA 確立のログを残します off : ログに残しません 工場出荷時 : off
--------	---

【メモ】

vpnlog は , "vpnlog" コマンドで表示できます。

vpnparam

```
vpnparam [retrytimer=<sec>]
          [retrymax=<max retry time>]
          [newsai=<sec>]
          [newsar=<sec>]
          [p1lifesecc=<sec>]
```

【内容】

IPsec の鍵交換に関する各種タイム値を設定します。

【オプション】

なし

【パラメータ】

retrytimer=<sec>	自動鍵交換の最初の再送までの時間。単位は秒。 次の再送までの時間は前回の再送までの時間の倍の時間となる。但し、最大は30秒。 設定範囲：1～30 工場出荷時：4
retrymax=<max retry time>]	自動鍵交換の再送の最大回数。 設定範囲：1～0xffffffff 工場出荷時：2
newsai=<sec>	自身が Initiator の場合に、SA の Lifetime が満了する時間よりも指定された時間だけ前に、新しい SA を確立するために Phase1 ネゴシエーションを開始します。単位は秒。 設定範囲：1～255 工場出荷時：90
newsar=<sec>	自身が Responder の場合に、SA の Lifetime が満了する時間よりも指定された時間だけ前に、新しい SA を確立するために Phase1 ネゴシエーションを開始します。単位は秒。値が 0 となっている場合は、newsai で指定されている値-60秒だけ前に開始します。 設定範囲：0～255 工場出荷時：0
p1lifesecc=<sec>	IKE SA の Lifetime。単位は秒。 設定範囲：0, 60～0xffffffff 工場出荷時：1000

vpnpeer

```

v p n p e e r    [[{add|set} {addr=<peer ipaddress>|name=<peer name>}
                  [myname={<my name>|""}]
                  [mypasswd={<my password>|""}]
                  [key=[a,|b,]{<key>|""}]
                  [nat={off|nat|natp|peernat}]
                  [natglobal=<global ipaddress>[,<global ipaddressmask>]]
                  [idtype={domainname|ip|""}]
                  [ikepolicy={<ID>|""}]]
[delete {all|[addr=<peer ipaddress>]
        [name=<peer name>]
        [myname={<my name>|""}]
        [mypasswd={<my password>|""}]
        [key=[a,|b,]{<key>|""}]
        [nat={off|nat|natp|peernat}]
        [natglobal=<global ipaddress>[,<global ipaddressmask>]]
        [idtype={domainname|ip|""}]
        [ikepolicy={<ID>|""}]]]]

```

【内容】

VPN ピア (VPN 通信相手 .ホストもしくはルータ等のセキュリティゲートウェイ .自身と VPN ピア間でセキュアな通信を行なう) のエントリを設定します .

省略した項目についてはデフォルト値となります .

【オプション】

なし

【パラメータ】

add	エントリに登録します . 最大エントリ数500
addr=<peer ipaddress>	VPNピアのIpaddress
name=<peer name>	VPN ピアの名前 . VPN ピアが , Dial-up 接続して IPaddress を取得する場合などで , IPaddress が既知でない場合 , 名前で指定します . RSA signatures の場合は , VPN ピアの ID (名前やドメイン名) を指定します . 設定範囲 : 最大 64 文字の英数字 工場出荷時 : なし
myname=<my name>	自身の名前 . 将来拡張用のため , 特に設定する必要はありません .

	<p>設定範囲：最大 64 文字の英数字 工場出荷時：なし</p>
mypasswd=<my password>	<p>自身のパスワード。 将来拡張用のため、特に設定する必要はありません。 設定範囲：最大 64 文字の英数字 工場出荷時：なし</p>
key=[a, b,]{<key> ""}	<p>VPN ピアに依存する鍵データ。 VPN ピアと同じ値とする必要があります。 a を指定した場合 ASCII データ, b を指定した場合バイナリデータ, 省略した場合 ASCII データとみなします。バイナリデータの場合 16 進表記します。 "" を指定することにより登録を削除することができます。 設定範囲：最大 64 文字の英数字かバイナリデータ 工場出荷時：なし</p>
nat={off nat natp peernat}	<p>VPN ピア毎の NAT 動作モード。 装置としての NAT 機能使用有無の設定が「使用する」の場合に有効になり, VPN 対象データは VPN ピア毎に指定された動作モードで動作します。 nat : NAT のモード・変換アドレス等, 装置としての NAT の設定に従います。 off : NAT 変換しません。 peernat : natglobal で指定したアドレスを使用して NATP モードとして動作します。 natp : NATP モードとして動作します。 設定範囲：off, nat, natp, peernat 工場出荷時：nat</p>
natglobal=<global ipaddress> [,<global ipaddressmask>]	<p>VPN ピア毎の NAT の変換アドレス。 nat の指定が peernat の場合に有効になります。global ipaddressmask は, 将来拡張用のため, 特に設定する必要はありません。 設定範囲：0.0.0.0 ~ 255.255.255.255 工場出荷時：255.255.255.255</p>
[idtype={domainname ip ""}]	<p>RSA Signature 認証使用時の IKE Phase I ネゴシエーションにおける自身の ID タイプ。 デフォルト：なし</p>
ikepolicy=<ID> ""}	<p>vpnikpolicy の id を指定します。 省略した場合, デフォルト値 (des, prekey, group1) で動作します。 指定した ID の vpnikpolicy エントリがない(削除された等)場合, エントリは無効になります。 設定範囲：vpnikpolicy で設定した id</p>

vpnpolicy

```

v p n p o l i c y  [{add|set} id=<ID>
                    [sec=<lifetime second>]
                    [kbytes=<lifetime kbytes>]
                    [pfs={no|yes}]
                    [group={1|2}]
                    [encr={null|des|3des}]
                    [auth={null|hmac-md5|hmac-sha}]]
|[delete {all|[id=<ID>]
          [sec=<lifetime second>]
          [kbytes=<lifetime kbytes>]
          [pfs={no|yes}]
          [group={1|2}]

```

【内容】

VPN 通信のための transform(暗号・認証アルゴリズム)エントリ，ポリシーエントリを設定します。

省略した項目についてはデフォルト値となります。

【オプション】

なし

【パラメータ】

add	エントリに登録します。最大エントリ数20
id=<ID>	ポリシーエントリの識別子。 設定範囲：1～20，他のエントリと重ならないようにしてください。 工場出荷時：なし
sec=<lifetime second>	Lifetime 秒。通常は設定を変更する必要はありません。変更する場合は，VPN ピアどうして，同じ値に設定してください。 設定範囲：0(設定なし)，60～0xffffffff 工場出荷時：0
kbytes=<lifetime kbytes>	Lifetime kbytes。通常は設定を変更する必要はありません。変更する場合は，VPN ピアどうして，同じ値に設定してください。 設定範囲：0(設定なし)，1000～0xffffffff 工場出荷時：0

pfs={no yes}	yes の場合, SA 確立時新たな鍵情報を指定します。 新しい鍵情報を使用する方がセキュリティは高いが, 鍵生成に時間がかかります。 設定範囲: no, yes 工場出荷時: no
group={1 2}	PFS 使用時に使う Oakley Group。 設定範囲: 1, 2 工場出荷時: 1
encr={null des 3des}	暗号アルゴリズム。 設定範囲: null, des, 3des 工場出荷時: des
auth={null hmac-md5 hmac-sha}	認証アルゴリズム。 設定範囲: null, hmac-md5, hmac-sha 工場出荷時: hmac-md5

【機能説明】

Lifetime に関して, sec も kbytes もどちらも設定されなかった(デフォルト)場合, 28800 秒(8hour)として動作します。

vpnselector

```

vpnselector  [{add|set} id=<ID>
              dst={all|peer|<ipaddress>[,<ipaddressmask>]}
              src={all|<ipaddress>[,<ipaddressmask>]}
              [prot={icmp|tcp|udp|all|<protocolnumber>}]
              [dstport={all|<portnumber>}]
              [srcport={all|<portnumber>}]
              [type={ipsec|bypass|discard}]
              [negotype={[initon|initoff],[normal|lifetime|time]}]
              [negotime=<hhmm>]
              {peeraddr=<peer ipaddress>|peername=<peer name>}
              policy=<ID>]
|[delete {all|[id=<ID>]
         [dst={all|peer|<ipaddress>[,<ipaddressmask>]}]
         [src={all|<ipaddress>[,<ipaddressmask>]}]
         [prot={icmp|tcp|udp|all|<protocolnumber>}]
         [dstport={all|<portnumber>}]
         [srcport={all|<portnumber>}]
         [type={ipsec|bypass|discard}]
         [negotype={[initon|initoff],[normal|lifetime|time]}]
         [negotime=<hhmm>]
         {peeraddr=<peer ipaddress>|peername=<peer name>}
         [policy=<ID>}]]]

```

【内容】

VPN 対象データ(selector)エントリを設定します。
省略した項目についてはデフォルト値となります。

【オプション】

なし

【パラメータ】

add	エンTRIESに登録します。最大ENTRIES数1000
id=<ID>	VPN 対象データ(selector)ENTRIESの優先順位。値が小さい方が優先順位が高くなります。 設定範囲：1～1000 工場出荷時：なし
dst={all peer <ipaddress>[,<ipaddressmask>]}	宛先 IPaddress 範囲。 VPN ピアの IPaddress が既知でない場合は、dst=peer を指定することによって VPN ピア宛のデータを指定できます。 ipaddressmask を省略した場合 255.255.255.255 となります。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：255.255.255.255
src={all <ipaddress>[,<ipaddressmask>]}	送信元 IPaddress 範囲。 ipaddressmask を省略した場合 255.255.255.255 となります。 設定範囲：0.0.0.0～255.255.255.255 工場出荷時：255.255.255.255
prot={icmp tcp udp all <protocolnumber>}	プロトコル。 設定範囲：icmp, tcp, udp, all 工場出荷時：all
dstport={all <portnumber>}	宛先ポート番号。 設定範囲：1～65534 工場出荷時：all
srcport={all <portnumber>}	送信元ポート番号。 設定範囲：1～65534 工場出荷時：all
type={ipsec bypass discard}	IPsec 処理タイプ。 ipsec を指定すると IPsec による VPN 通信を行います。 bypass を指定すると、VPN でない通常の通信を行います。 Selector で指定されないパケットは、廃棄されます。 複数のENTRIESに該当する場合は、優先度が高い処理タイプが適用されます。 設定範囲：ipsec, bypass, discard 工場出荷時：ipsec
negotype={[initon initoff],[normal lifetime time]}	SA 確立契機を指定します。 initon の場合、起動時 SA を確立します。 lifetime の場合、トラフィックに関係なく、Lifetime 満了前に常に新しい SA を確立しておきます。 time の場合、Lifetime の設定及びトラフィックに関係なく、negotime で指定した時刻に常に新しい SA を

コマンドマニュアル

	確立します。 設定範囲：initon, initoff, normal, lifetime, time 工場出荷時：initoff, normal
negotime=<hhmm>	negotype が time の場合の SA 確立時刻。 設定範囲：0000 ~ 2359 工場出荷時：0000(0時0分)
peeraddr=<peer ipaddress> peername=<peer name>	VPN ピアエントリ。 設定範囲：vpnpeer で設定した VPN ピア IPaddress または VPN ピア名称 工場出荷時：なし
policy=<ID>	ポリシーエントリの識別子。 設定範囲：vpnpolicy で設定した id 工場出荷時：なし

INFONET-VP100 VPN ボックス
コマンドマニュアル 4 版
発行日 2000年 9月
発行責任 古河電気工業株式会社
Printed in Japan

- 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は、当社はその責を負いません。
- 無断転載を禁じます。
- 落丁・乱丁本はお取り替えいたします。