

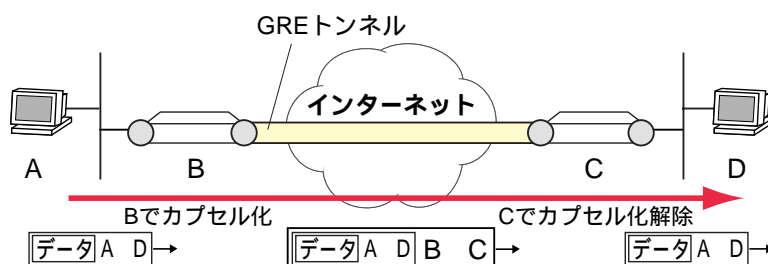
GRE

概要・基本設定	2
設定手順	2
設定例	4
基本設定	4
IP NAT との併用	5
ファイアウォール NAT との併用	6
コマンドリファレンス編	9
機能別コマンド索引	9
ADD GRE	10
DELETE GRE	12
DISABLE GRE	13
ENABLE GRE	14
PURGE GRE	15
RESET GRE	16
SET GRE	17
SHOW GRE	18

概要・基本設定

GRE (Generic Routing Encapsulation) は、任意のネットワーク層プロトコルパケットを、別のネットワーク層プロトコルパケットに包み込んで送信する汎用のトンネリングプロトコルです。

本製品では、IP パケットを別の IP パケットでカプセル化することにより、プライベート IP アドレスで運用している LAN 同士をインターネット経由で接続することが可能です。



GRE は設定がシンプルでわかりやすいところが特徴ですが、他のトンネリングプロトコル (L2TP や IPsec のトンネルモード) と比べて、以下の欠点があります。

- IP パケットしかトンネリングできない。
- トンネルの両端のルーターの IP アドレスが固定されていなくてはならない。L2TP や IPsec は、片側のアドレスが不定でも (若干の制限があるものの) 使用できる。
- セキュリティー機能がない

使用するネットワークの構成や要件に応じて、どのトンネリングプロトコルを使用するかを選択してください。一般的に、IPX や AppleTalk のトンネリングが必要なら L2TP を、IP だけのトンネリングでセキュリティ機能が必要なら IPsec (ESP) を、IPX や AppleTalk のトンネリングでセキュリティが必要なら L2TP と IPsec (ESP) の併用を考えるとよいでしょう。

設定手順

GRE の設定は IP フィルターとよく似ています。各ルーターで以下の設定を行います。

1. GRE フィルターを作成し、トンネリングするパケットの条件を指定します。始点・終点 IP アドレスの組み合わせで指定する方法と、受信インターフェースで指定する方法があります。たとえば、次のような指定が可能です。
 - 192.168.10.0/24 から 192.168.20.0/24 へのパケットをトンネリング
 - LAN 側インターフェース (eth0) で受信したパケットをトンネリング
2. 同じく GRE フィルターで、カプセル化したパケットの送信先 (トンネルの終点) を指定します。具体的には、対向ルーターの IP アドレスを指定します。こちらのルーターから到達できるアドレスでなくてはなりません。
3. 手順 1、2 の設定内容 (GRE フィルター) を、トンネル対象パケットの受信インターフェースに適用します。設定内容を IP インターフェースに適用しないと GRE の設定は有効になりませんのでご注意ください。

4. GRE モジュールを有効化します。

以下、実際にコマンド例を示しながら解説します。

GRE モジュールはデフォルトでは無効になっています。有効にするには ENABLE GRE コマンド (14 ページ) を使います。

```
ENABLE GRE ↵
```

トンネリングするアドレスの範囲を指定するには、ADD GRE コマンド (10 ページ) を使います。GRE フィルターには 1 ~ 100 の任意の番号を付けます。たとえば、192.168.10.0/24 192.168.20.0/24 のパケットをカプセル化して、対向ルーター 2.2.2.2 に送る場合は、次のようにします。

```
ADD GRE=1 SOURCE=192.168.10.0 SMASK=255.255.255.0
DESTINATION=192.168.20.0 DMASK=255.255.255.0 TARGET=2.2.2.2 ↵
```

次のように複数の条件を同時に指定することもできます。これにより、複数拠点をインターネット経由で結ぶことも可能です。たとえば、192.168.10.0/24 192.168.20.0/24 のパケットを 2.2.2.2 へ、192.168.10.0/24 192.168.30.0/24 のパケットは 3.3.3.3 へ送る場合は、次のようにします。

```
ADD GRE=1 SO=192.168.10.0 SMASK=255.255.255.0 DEST=192.168.20.0
DMASK=255.255.255.0 TARGET=2.2.2.2 ↵
ADD GRE=1 SO=192.168.10.0 SMASK=255.255.255.0 DEST=192.168.30.0
DMASK=255.255.255.0 TARGET=3.3.3.3 ↵
```

また、特定の IP インターフェースで受信したパケットすべてをカプセル化したい場合は、SOURCE/SMASK、DESTINATION/DMASK の代わりに INTERFACE パラメーターを使用します。このときアドレスは指定できません。たとえば、eth0 で受信したすべてのパケットをカプセル化して、対向ルーター 2.2.2.2 に送る場合は、次のようにします。

```
ADD GRE=1 INT=eth0 TARGET=2.2.2.2 ↵
```

GRE フィルターの設定を変更するには、SET GRE コマンド (17 ページ) を使います。このコマンドは ENTRY パラメーターが必須です (SHOW GRE コマンド (18 ページ) で確認できます)。

```
ADD GRE=1 ENTRY=1 TARGET=2.2.2.1 ↵
```

GRE フィルターを IP インターフェースに適用するには、SET IP INTERFACE コマンド (「IP」の 321 ページ) の GRE パラメーターを使います。GRE の設定はインターフェースに適用して初めて効果を持ちます。通常、GRE フィルターはトンネリング対象パケットを受信するインターフェースに適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

GRE フィルターの設定を確認するには、SHOW GRE コマンド (18 ページ) を使います。

```
SHOW GRE ↵
```

GRE モジュールの状態を確認するには、SHOW GRE コマンド（18 ページ）の GENERAL オプションを使います。

```
SHOW GRE GENERAL ↓
```

IP インターフェースに適用されている GRE フィルターは、SHOW IP INTERFACE コマンド（「IP」の 392 ページ）で確認できます。GRE フィルターが適用されていれば、「GRE」欄にフィルター番号が表示されます。

```
SHOW IP INT ↓
```

```
SHOW IP INT=eth0 ↓
```

GRE フィルターからエントリを削除するには、DELETE GRE コマンド（12 ページ）を使います。

```
DELETE GRE=1 ENTRY=1 ↓
```

```
DELETE GRE=1 ENTRY=ALL ↓
```

IP インターフェースから GRE フィルターの適用を解除するには、SET IP INTERFACE コマンド（「IP」の 321 ページ）の GRE パラメーターに NONE を指定します。

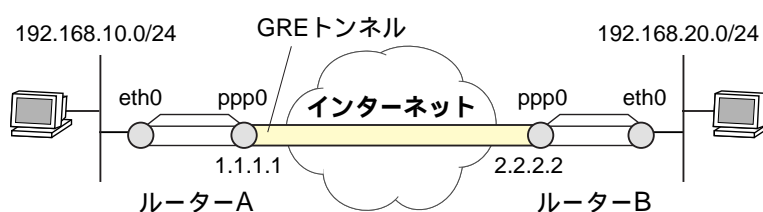
```
SET IP INT=eth0 GRE=NONE ↓
```

GRE モジュールを無効にするには、DISABLE GRE コマンド（13 ページ）を使います。

```
DISABLE GRE ↓
```

設定例

GRE トンネリングを用いて、2 つのプライベートネットワークを接続する設定例をいくつか示します。ここでは、次のような構成を想定します。ルーター A、B とも、WAN 側（ppp0）インターフェースにグローバルアドレスが固定的に割り当てられているものとします。なお以下の例では、IP の設定までは完了しているものと仮定しています。



基本設定

プライベート LAN 間の通信だけを行う設定です。NAT の設定がされていないため、プライベート LAN からインターネットにはアクセスできません。

ルーター A

1. GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

2. ローカル LAN (192.168.10.0/24) からリモート LAN (192.168.20.0/24) へのパケットをカプセル化してルーター B (2.2.2.2) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.10.0 SMASK=255.255.255.0 DEST=192.168.20.0
    DMASK=255.255.255.0 TARGET=2.2.2.2 ↵
```

3. GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

ルーター B

1. GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

2. ローカル LAN (192.168.20.0/24) からリモート LAN (192.168.10.0/24) へのパケットをカプセル化してルーター A (1.1.1.1) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.20.0 SMASK=255.255.255.0 DEST=192.168.10.0
    DMASK=255.255.255.0 TARGET=1.1.1.1 ↵
```

3. GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

IP NAT との併用

上記の基本設定に IP NAT (レンジ NAT) の設定を追加して、プライベート LAN 間だけでなく、それぞれのプライベート LAN からインターネットにもアクセスできるようにします。

ルーター A

1. GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

2. ローカル LAN (192.168.10.0/24) からリモート LAN (192.168.20.0/24) へのパケットをカプセル化してルーター B (2.2.2.2) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.10.0 SMASK=255.255.255.0 DEST=192.168.20.0
    DMASK=255.255.255.0 TARGET=2.2.2.2 ↵
```

- GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

- IP NAT モジュールを有効にします。

```
ENABLE IP NAT ↵
```

- ローカル LAN 側ホストのプライベート IP アドレスを、ppp0 のグローバルアドレスに変換するダイナミック ENAT の設定を行います。

```
ADD IP NAT IP=192.168.10.0 MASK=255.255.255.0 GBLINT=ppp0 ↵
```

ルーター B

- GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

- ローカル LAN (192.168.20.0/24) からリモート LAN (192.168.10.0/24) へのパケットをカプセル化してルーター A (1.1.1.1) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.20.0 SMASK=255.255.255.0 DEST=192.168.10.0  
DMASK=255.255.255.0 TARGET=1.1.1.1 ↵
```

- GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

- IP NAT モジュールを有効にします。

```
ENABLE IP NAT ↵
```

- ローカル LAN 側ホストのプライベート IP アドレスを、ppp0 のグローバルアドレスに変換するダイナミック ENAT の設定を行います。

```
ADD IP NAT IP=192.168.20.0 MASK=255.255.255.0 GBLINT=ppp0 ↵
```

- この設定では、NAT 用グローバルアドレスとして ppp0 のインターフェースアドレスを使っているため、ルーター A、B は外部からの Ping に応えません。接続性をテストするときなどにはご注意ください。詳細は「IP」の「レンジ NAT」をご覧ください。

ファイアウォール NAT との併用

上記の基本設定にファイアウォール NAT の設定を追加して、プライベート LAN 間だけでなく、それぞれのプライベート LAN からインターネットにもアクセスできるようにします。

GRE とファイアウォールを併用するときは、次のポイントに注意してください。

- 対向ルーターからの GRE パケットがファイアウォールで遮断されないよう ALLOW ルールを設定する

- プライベート LAN 間のパケットにファイアウォール NAT が適用されないよう NONAT ルールを設定する

ルーター A

1. GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

2. ローカル LAN (192.168.10.0/24) からリモート LAN (192.168.20.0/24) へのパケットをカプセル化してルーター B (2.2.2.2) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.10.0 SMASK=255.255.255.0 DEST=192.168.20.0
    DMASK=255.255.255.0 TARGET=2.2.2.2 ↵
```

3. GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

4. ファイアウォールとダイナミック ENAT の基本設定をします。

```
ENABLE FIREWALL ↵
CREATE FIREWALL POLICY=net ↵
ENABLE FIREWALL POLICY=net ICMP_F=ALL ↵
DISABLE FIREWALL POLICY=net IDENTPROXY ↵
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE ↵
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC ↵
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0 ↵
```

5. 外側インターフェースで受信した GRE パケットを NAT の対象からはずします。

```
ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=ppp0 PROT=GRE ↵
```

6. 内側インターフェースで受信したパケットのうち、トンネリング対象のパケットを NAT の対象からはずします。

```
ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=eth0 PROT=ALL
    IP=192.168.10.1-192.168.10.254 REM=192.168.20.1-192.168.20.254 ↵
```

ルーター B

1. GRE モジュールを有効にします。

```
ENABLE GRE ↵
```

2. ローカル LAN (192.168.20.0/24) からリモート LAN (192.168.10.0/24) へのパケットをカプセル化してルーター A (1.1.1.1) に送る GRE フィルター「1」を作成します。

```
ADD GRE=1 SO=192.168.20.0 SMASK=255.255.255.0 DEST=192.168.10.0
    DMASK=255.255.255.0 TARGET=1.1.1.1 ↵
```

- GRE フィルター「1」を eth0 に適用します。

```
SET IP INT=eth0 GRE=1 ↵
```

- ファイアウォールと ENAT の基本設定をします。

```
ENABLE FIREWALL ↵
CREATE FIREWALL POLICY=net ↵
ENABLE FIREWALL POLICY=net ICMP_F=ALL ↵
DISABLE FIREWALL POLICY=net IDENTPROXY ↵
ADD FIREWALL POLICY=net INT=eth0 TYPE=PRIVATE ↵
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC ↵
ADD FIREWALL POLICY=net NAT=ENHANCED INT=eth0 GBLINT=ppp0 ↵
```

- 外側インターフェースで受信した GRE パケットを NAT の対象からはずします。

```
ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=ppp0 PROT=GRE ↵
```

- 内側インターフェースで受信したパケットのうち、トンネリング対象のパケットを NAT の対象からはずします。

```
ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=eth0 PROT=ALL
    IP=192.168.20.1-192.168.20.254 REM=192.168.10.1-192.168.10.254 ↵
```


コマンドリファレンス編

機能別コマンド索引

一般コマンド

ADD GRE	10
DELETE GRE	12
DISABLE GRE	13
ENABLE GRE	14
PURGE GRE	15
RESET GRE	16
SET GRE	17
SHOW GRE	18

ADD GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

```
ADD GRE=gre-number SOURCE=ipadd [SMASK=ipadd] [DESTINATION=ipadd]
    [DMASK=ipadd] TARGET=ipadd [ENTRY=entry-id]
ADD GRE=gre-number
    INTERFACE=interface TARGET=ipadd [ENTRY=entry-id]
```

gre-number: GRE フィルター番号 (1~100)

interface: IP インターフェース名 (eth0、ppp0 など)

ipadd: IP アドレスまたはネットマスク

entry-id: エントリー番号 (1~)

解説

GRE フィルターにトンネリング対象パケットの条件を追加する。

GRE トンネリングを行うには、GRE フィルターを定義して、IP インターフェースに適用する必要がある。

パラメーター

GRE GRE フィルター番号

SOURCE トンネリング対象パケットの始点 IP アドレス。SMASK と組み合わせて範囲指定が可能。

SMASK SOURCE に対するネットマスク。

DESTINATION トンネリング対象パケットの終点 IP アドレス。DMASK と組み合わせて範囲指定が可能。

DMASK DESTINATION に対するネットマスク。

TARGET GRE パケットの送信先アドレス。トンネルの終点となる対向ルーターの IP アドレスを指定する

ENTRY GRE フィルター内のエントリー番号。

INTERFACE トンネリング対象トラフィックの受信 IP インターフェース。INTERFACE を指定した場合、指定したインターフェースで受信した IP パケットはすべてトンネリングの対象となる。SOURCE、SMASK、DESTINATION、DMASK とは同時に指定できない。

例

192.168.10.0/24 から 192.168.20.0/24 へのパケットをカプセル化し、対向ルーター 2.2.2.2 に送信する GRE フィルター「1」を作成する。

```
ADD GRE=1 SO=192.168.10.0 SMA=255.255.255.0 DEST=192.168.20.0
    DMA=255.255.255.0 TARGET=2.2.2.2
```

関連コマンド

DELETE GRE (12 ページ)

SET GRE (17 ページ)

SHOW GRE (18 ページ)

DELETE GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

DELETE GRE=*gre-number* ENTRY={*entry-id*|ALL}

gre-number: GRE フィルター番号 (1 ~ 100)

entry-id: エントリー番号 (1 ~)

解説

GRE フィルターからトンネリング対象パケットの条件 (エントリー) を削除する。

パラメーター

GRE GRE フィルター番号

ENTRY GRE フィルター内のエントリー番号。ALL を指定した場合は、すべてのエントリーが削除される。

関連コマンド

ADD GRE (10 ページ)

SET GRE (17 ページ)

SHOW GRE (18 ページ)

DISABLE GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

DISABLE GRE

解説

GRE モジュールを無効にする。デフォルトは無効。

関連コマンド

ENABLE GRE (14 ページ)

ENABLE GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

ENABLE GRE

解説

GRE モジュールを有効にする。デフォルトは無効。

関連コマンド

DISABLE GRE (13 ページ)

PURGE GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

PURGE GRE

解説

GRE の設定情報をすべて削除する。

備考・注意事項

ランタイムメモリー上にある GRE 関連の設定がすべて削除されるため、運用中のシステムで本コマンドを実行するときは十分に注意すること。

関連コマンド

RESET GRE (16 ページ)

RESET GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

RESET GRE

解説

GRE モジュールをリセットする。

DISABLE GRE コマンド、ENABLE GRE コマンドを実行するのと等しい。

関連コマンド

DISABLE GRE (13 ページ)

ENABLE GRE (14 ページ)

SET GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

```
SET GRE=gre-number ENTRY=entry-id [SOURCE=ipadd] [SMASK=ipadd]
    [DESTINATION=ipadd] [DMASK=ipadd] [TARGET=ipadd]
SET GRE=gre-number
    ENTRY=entry-id [INTERFACE=interface] [TARGET=ipadd]
```

gre-number: GRE フィルター番号 (1~100)

entry-id: エントリー番号 (1~)

ipadd: IP アドレスまたはネットマスク

interface: IP インターフェース名 (eth0、ppp0 など)

解説

GRE フィルターの設定を変更する。

パラメーター

GRE GRE フィルター番号

ENTRY GRE フィルター内のエントリー番号

INTERFACE トンネリング対象パケットの受信 IP インターフェース。INTERFACE を指定した場合、指定したインターフェースで受信した IP パケットはすべてトンネリングの対象となる。SOURCE、SMASK、DESTINATION、DMASK とは同時に指定できない。

SOURCE トンネリング対象パケットの始点 IP アドレス。SMASK と組み合わせて範囲指定が可能。

SMASK SOURCE に対するネットマスク。

DESTINATION トンネリング対象パケットの終点 IP アドレス。DMASK と組み合わせて範囲指定が可能。

DMASK DESTINATION に対するネットマスク。

TARGET GRE パケットの送信先アドレス。トンネルの終点となる対向ルーターの IP アドレスを指定する

関連コマンド

DELETE GRE (12 ページ)

SET GRE (17 ページ)

SHOW GRE (18 ページ)

SHOW GRE

カテゴリー：GRE / 一般コマンド

対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

SHOW GRE [=gre-number] [GENERAL]

gre-number: GRE フィルター番号 (1～100)

解説

GRE モジュールの設定、および、GRE フィルターの設定を表示する。

パラメーター

GRE GRE フィルター番号。省略時はすべての GRE フィルターに関する情報が表示される。

GENERAL GRE モジュールの一般情報が表示される。GRE フィルター番号と同時に指定することはできない。

入力・出力・画面例

```

Manager > show gre

-----
GRE      Entry   Interface   Source          Destination      Target
          Source Mask      Dest. Mask      Match
-----
   1      1      -           192.168.10.0    192.168.20.0    172.31.28.186
          255.255.255.0    255.255.255.0          2536
          Requests:      2536          Translations:      2536
-----

Manager > show gre general

GRE General Informations
-----
Status ..... Enabled
greInPkts ..... 2458

```

GRE	GRE フィルター番号
Entry	フィルターエントリー番号
Interface	トンネリング対象パケットの受信インターフェース名。「-」は未指定を示す

Source	トンネリング対象パケットの始点 IP アドレス
Source Mask	Source に対するネットマスク
Destination	トンネリング対象パケットの終点 IP アドレス
Dest. Mask	Destination に対するネットマスク
Target	GRE パケットの送信先 IP アドレス
Match	条件に一致した IP パケットの数
Requests	条件に一致するかチェックした IP パケットの数
Translations	条件に一致し GRE パケットでカプセル化された IP パケットの数

表 1:

Status	GRE モジュールの有効・無効
greInPkts	GRE パケット受信数 (受信後カプセル化を解除し、プライベート LAN に転送したもの)

表 2: GENERAL オプション

関連コマンド

ADD GRE (10 ページ)

DELETE GRE (12 ページ)