

GRE

学習内容

- 1 GREの概要と特徴
- 2 トンネリングの基本構造
- 3 GREトンネリングのトラフィックフロー
- 4 CiscoルータでのGRE基本設定
- 5 セキュリティ強化：GRE over IPsecの仕組み
- 6 ハブ & スポーク構成の設定ポイント

01 GREの概要と特徴

GREとは？ その柔軟なカプセル化技術

任意のプロトコルをIPトンネルに載せられる汎用性の高いトンネリング技術

GRE (Generic Routing Encapsulation) は、異なるプロトコルのパケットをIPパケットでカプセル化し、ネットワーク上で送信する技術

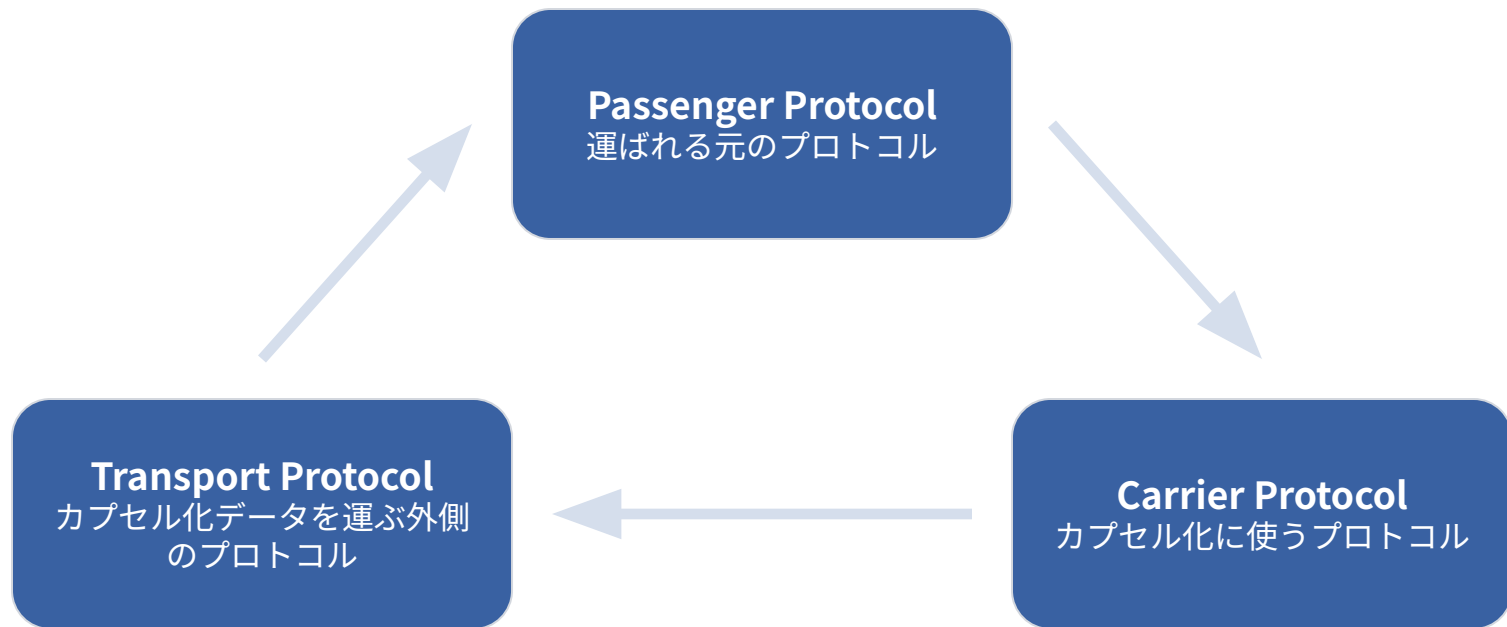
他のL2レベルのトンネル (PPTP/L2TP) に対し、GREはL3レベルのトンネリングプロトコルである

最大の特徴は「任意のプロトコル (IPX、AppleTalkなども) をIPトンネルに載せられる」という柔軟性の高さ

仮想的に直結しているように見せられるが、GRE単体では暗号化機能を持たない点に注意が必要

トンネリングを構成する3つのコンポーネント

カプセル化技術を理解するための基本要素



GREトンネリングのトラフィックフロー

パケットがルータ間でどのようにカプセル化・非カプセル化されるか

- 1 拠点LANのパケット（Private IP宛）が送信側ルータ（R2）に到着
- 2 R2がルーティングテーブルでネクストホップが**Tunnelインターフェース**であると判断
- 3 R2はパケットに**GREヘッダ**と**新しいIPヘッダ**（送信元R2 WAN IP、宛先R1 WAN IP）を追加（カプセル化）
- 4 カプセル化されたパケットがインターネットを経由して受信側ルータ（R1）に到着
- 5 R1がGREヘッダと外側のIPヘッダを外し（非カプセル化）、中のオリジナルパケットをLAN側に転送

02 GREのコンフィグレーション

トンネルインターフェースの基本設定コマンド

仮想インターフェースを作成し、トンネルの基本情報を定義する

インターフェース作成とIP設定

```
`interface tunnel number`、`ip address address mask`
```

トンネルの始点と終点の指定

```
`tunnel source address`、`tunnel destination address`
```

トンネルモードの指定

```
`tunnel mode gre ip`（省略可能）
```


GREにおけるルーティング設定の対比

スタティックルーティングとダイナミックルーティング（OSPF）の使い分け

スタティックルーティング

コマンド: `ip route [LAN NW] [Mask] tunnel 0``

設定はシンプルで容易

マルチキャストを必要としない

経路変更が多い大規模ネットワークには不向き

ダイナミックルーティング（OSPF）

トンネルI/FとLAN I/FをOSPFで`network`定義

OSPFが自動でルーティング情報を交換

GREが**マルチキャストをサポート**するため可能

大規模で動的なネットワークに適している

GREトンネルの運用と安定化

ルーティング以外の重要な設定項目

Keepalive

keepalive 5 3

トンネルの健全性監視

MTU調整

ip mtu 1476

フラグメント防止 (24B増加分吸収)

MSS調整

**ip tcp
adjust-mss 1436**

TCPセグメントの最大値制限

03

セキュリティ強化：GRE over IPsec

IPsec単体とGREの機能比較

GRE over IPsecが必要な理由を理解する

IPsec

あり

暗号化機能

なし

マルチキャスト対応

IPのみ

伝送可能プロトコル

GRE

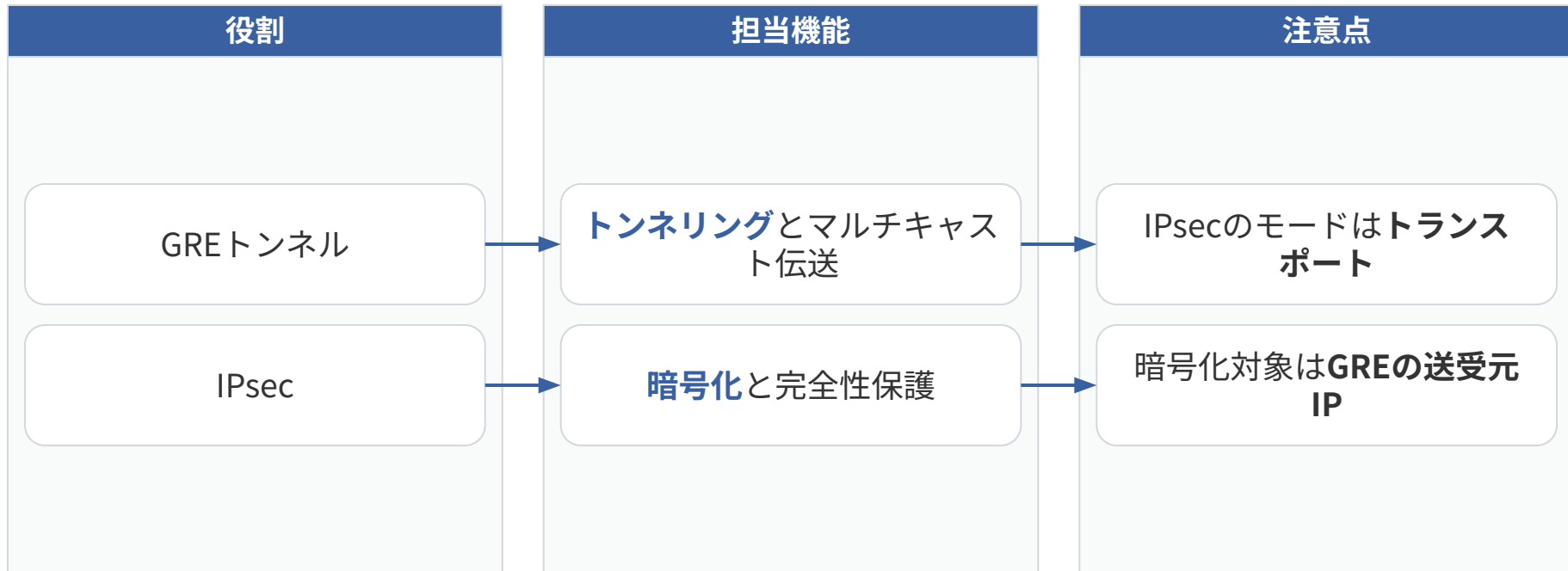
なし

あり

任意

GRE over IPsecの基本構成

IPsecをトランスポートモードで使用し二重トンネルを避ける

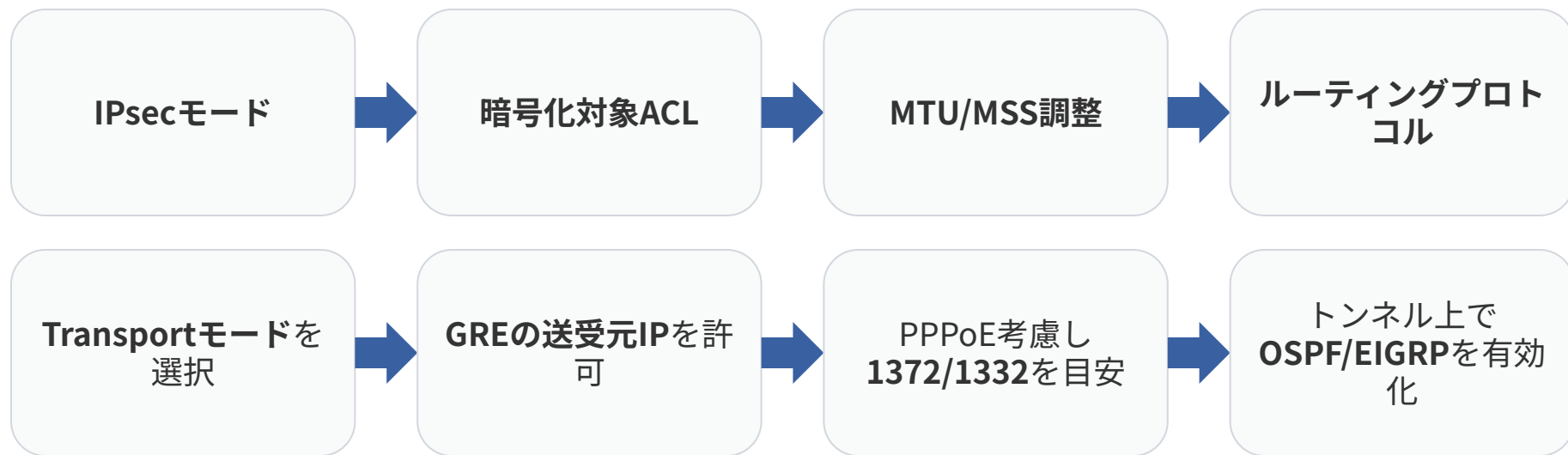


04

GRE over IPsec: ハブ & スポーク構 成

ハブ & スポーク構成の設計要点

試験で狙われる4つの必須チェックポイント



ハブ・ルータ（R1）設定のポイント

複数ピアへの対応とIPsecの分割

IKEv1鍵設定

各スポーク（R2, R3など）ごとに`crypto isakmp key`で**ピアを登録**する

GREトンネル

スポークの数だけ**Tunnelインターフェース**を作成し、それぞれに宛先を指定する

Crypto Map

複数のIPsecセッションを**Seq番号**で束ね、それぞれのピアとACLを指定する

ACL for IPsec

R2用、R3用など、**スポークごと**にGREプロトコルの許可ACLを作成する

動作確認のための検証手順

トンネル・ルーティング・IPsecの各レイヤーを確実にチェック

インターフェース状態確認

100%

OSPFネイバー形成

100%

IPsecフェーズ1確認

100%

IPsecフェーズ2確認

100%