

# 本資料について

- 本資料は下記書籍を基にして作成されたものです。文章の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

書籍名：IPsec徹底入門

著者：小早川知明

発行日：2002年8月6日

発売元：翔泳社



# IPsec徹底入門

名城大学工学部  
渡邊研究室  
村橋 孝謙

# 目次

- 第1章 IPsecアーキテクチャ
- 第2章 IPsec Security Association
- 第3章 Internet Key Exchange



# 第1章

## IPsecアーキテクチャ

# はじめに

- 現在、どこからでもインターネットに接続可能になっている
- さまざまなセキュリティ機能が必要

# 身を守るべき攻撃

## ■ 受動的な攻撃

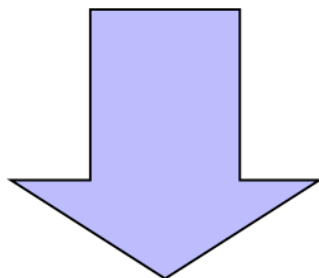
- 盗聴
- トラフィック解析

## ■ 能動的な攻撃

- なりすまし
- リプレイ攻撃
- メッセージの改ざん
- DoS攻撃

# IPsecとは

- 現在使用されているアプリケーション全てに個別にセキュリティ機能を実現することは不可能



IPレイヤにおいて、全てのIPパケットにセキュリティを提供

**IPsec**

# 必要なセキュリティ機能(1/3)

- 秘密性
- 認証(本人性確認)
- 認証(完全性保証)
- 否認不能性
- アクセス制御
- 可用性

IPsecは安全なVPNの実現するための解決策



# 必要なセキュリティ機能(2/3)

- 秘密性

- 盗聴・トラフィック解析からの保護

- 認証(本人性確認)

- 表示されたメッセージ送信元の保証
- 意図した通信相手であることの保証

- 認証(完全性保証)

- メッセージが改ざんされていないことの保証

# 必要なセキュリティ機能(3/3)

## ■ 否認不能性

- 送信者が確かにメッセージを送信したことや、受信者が確かにメッセージを受信したことを証明

## ■ アクセス制御

- 通信を行う相手やプロトコルなどによって、通信の通過・遮断を制御する

## ■ 可用性

- システムが常に使用できる

# IPsecのメリット

- VPNの各拠点にIPsec装置を置くだけで良い
- アプリケーションに変更を加える必要がない
- LAN内部の機器に暗号化等の負荷がかからない

# IPsecの実現要素

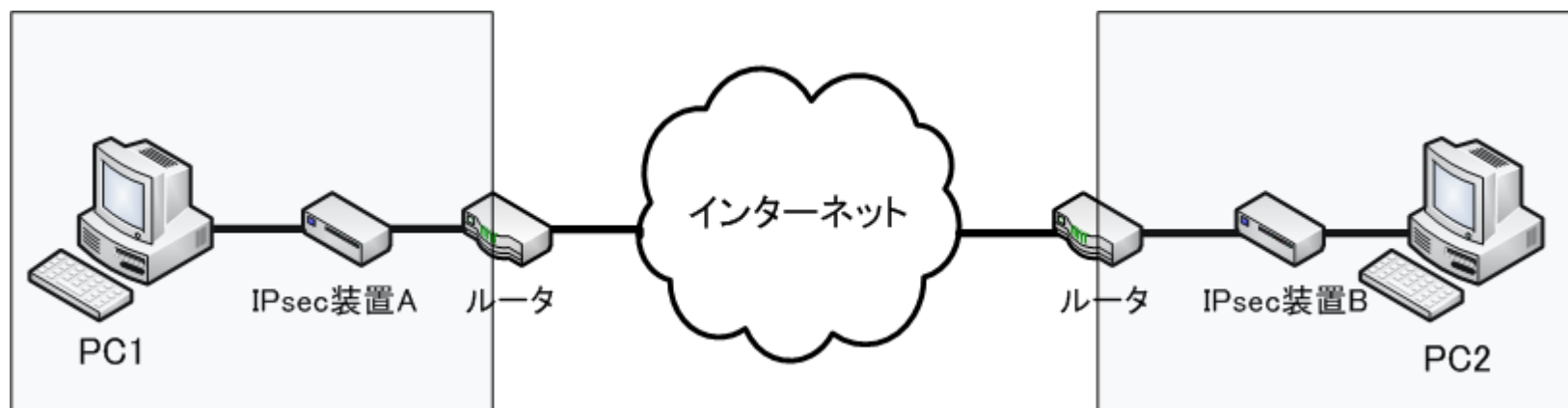
## ■ パケットのカプセル化

(セキュリティそのものを提供)

## ■ パケットの暗号化

(秘密対称鍵・IPsecコネクションの生成、管理)

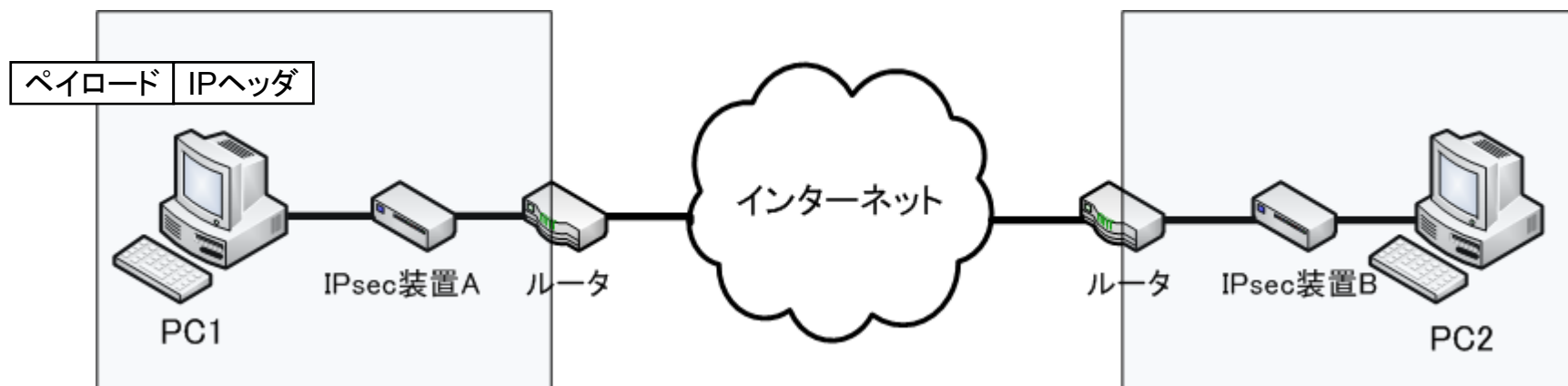
# IPsecの動作イメージ



## ■ IPsec装置Aの設定

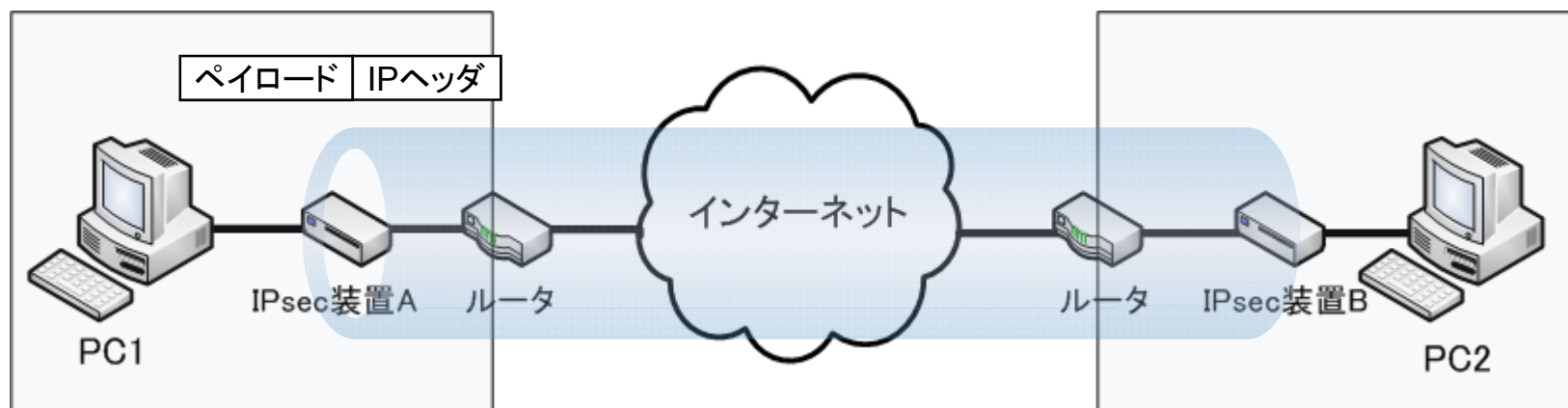
- PC1からPC2向けの packets をIPsec化してIPsec装置Bに転送

# IPsecの動作イメージ



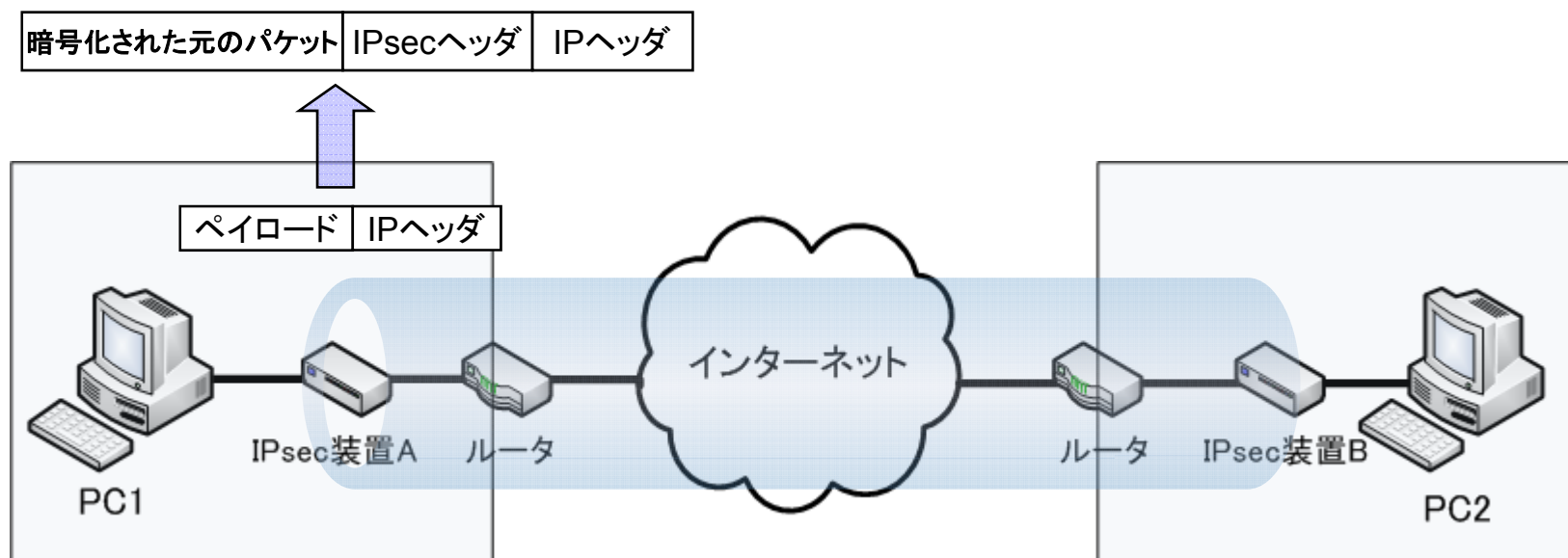
- PC1からPC2向けの packets をIPsec装置Aに送信

# IPsecの動作イメージ



- IPsecトンネルの生成、または既存のトンネルの使用

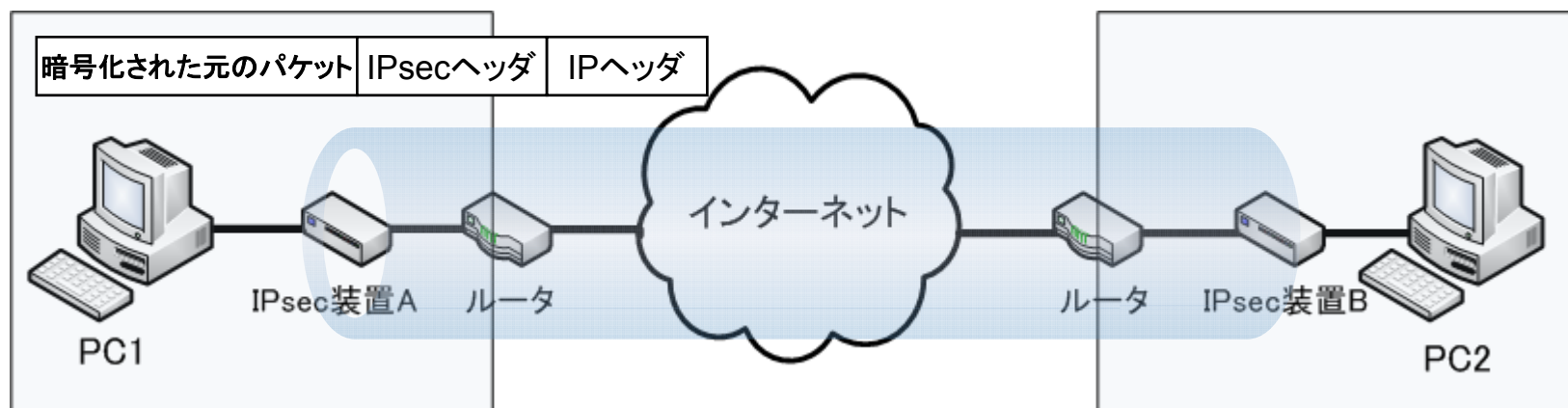
# IPsecの動作イメージ



## ■ パケットのIPsec化

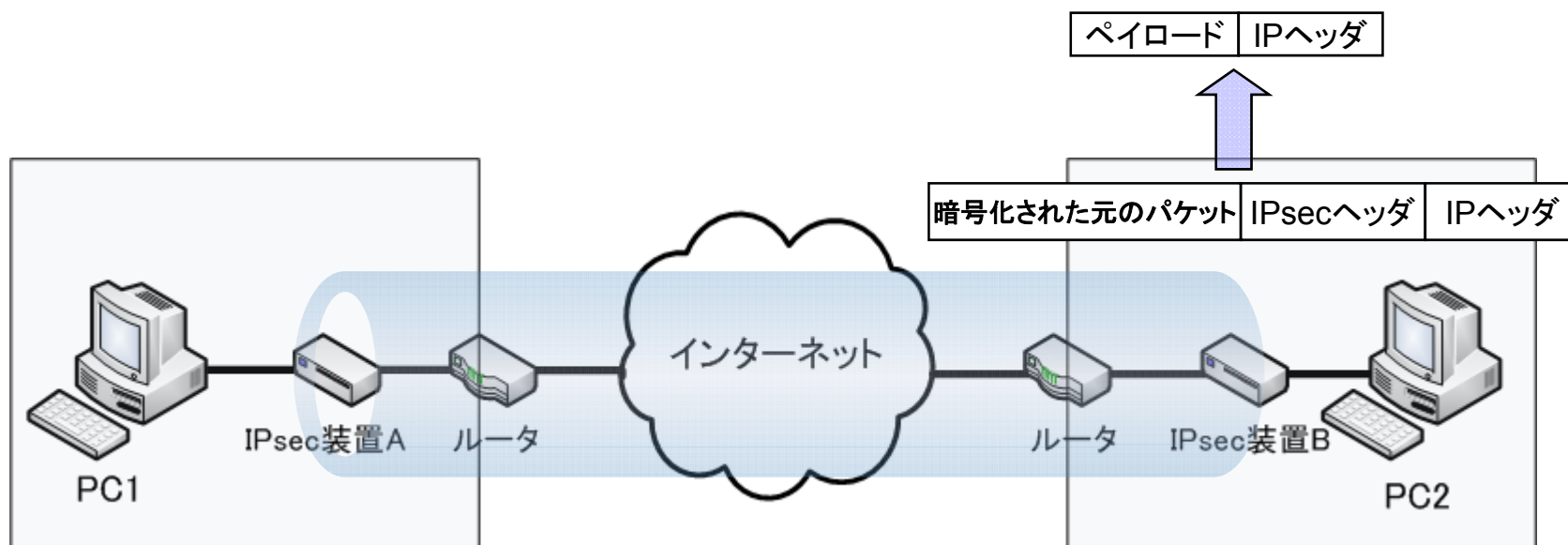


# IPsecの動作イメージ



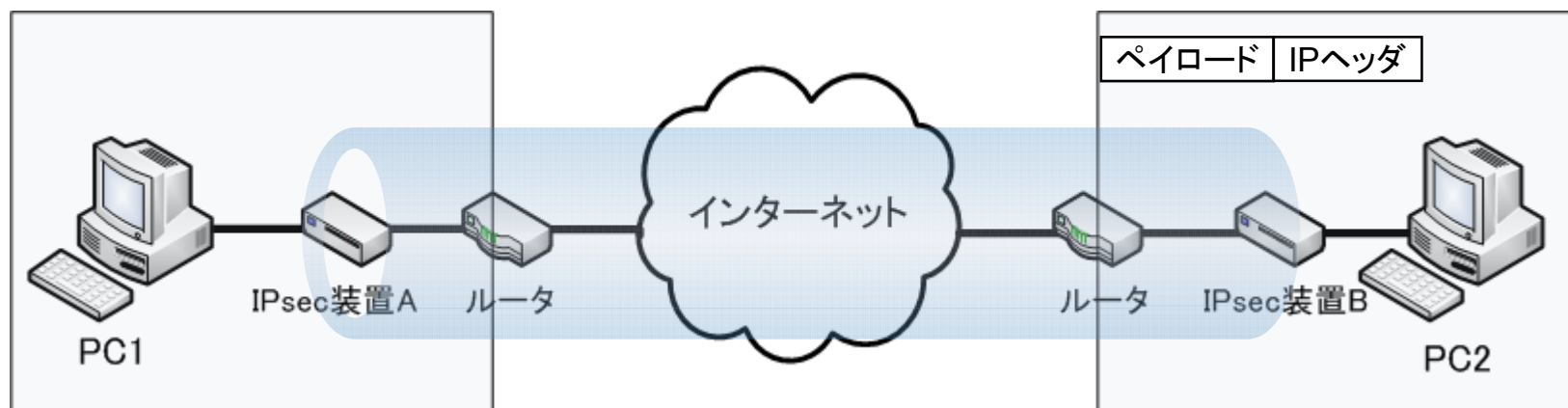
- IPsec化されたパケットをルータAに転送
- 普通のパケットとしてIPsec装置Bへ送信。

# IPsecの動作イメージ



## ■ パケットの復号化

# IPsecの動作イメージ



- PC2はPC1より送信されたパケットを受信

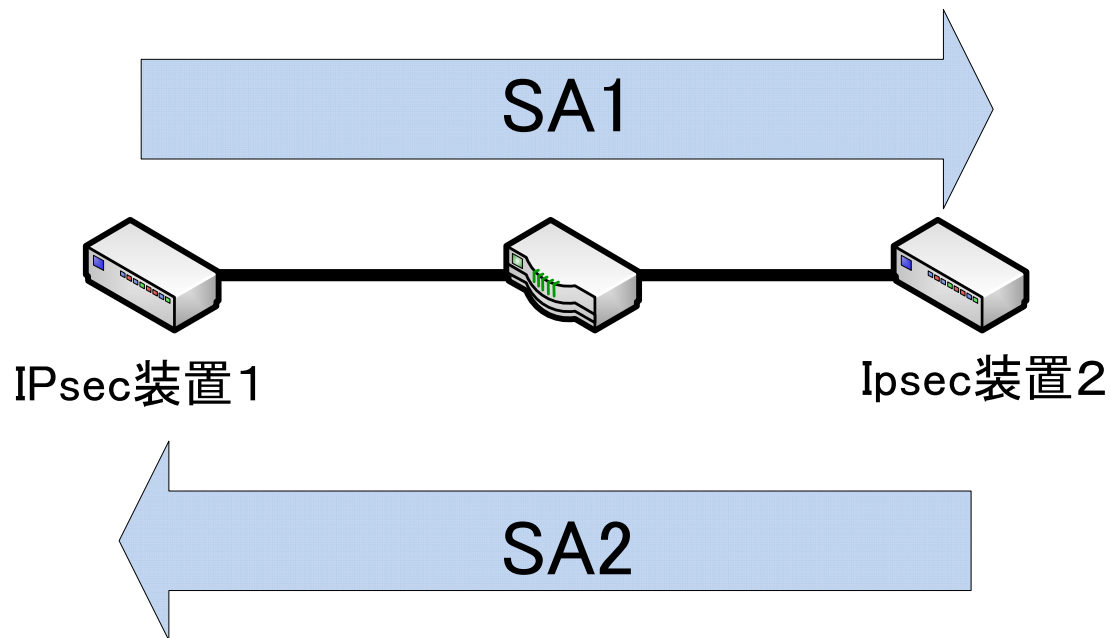
# SA (Security Association)とは (1/3)

- IPsecトンネルを正式にはSAと呼ぶ
- IPsec装置間で生成される
- すべてのIPパケットは、いずれかのSAに所属して送り出される

IPsecのセキュリティ機能は  
SAによって実現される

# SA (Security Association)とは (2/3)

- ユニディレクションである
- SAごとに独立したアルゴリズム・鍵などを持つ



# SA (Security Association)とは (3/3)

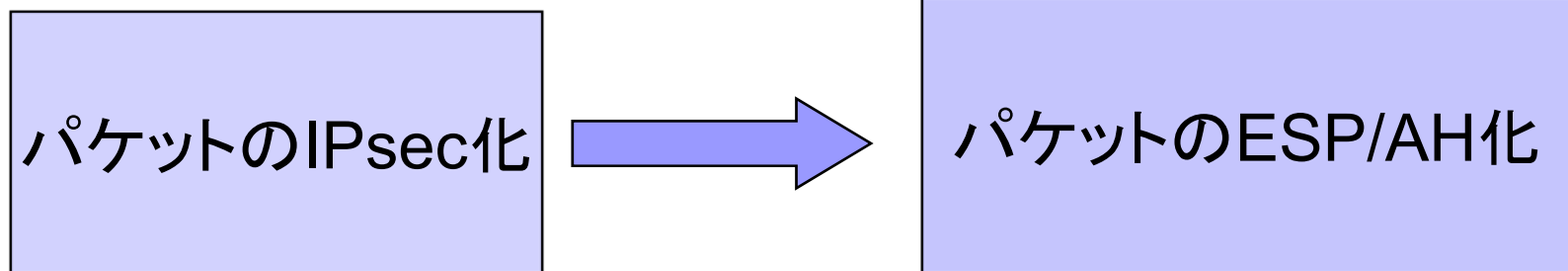
- 2種類のプロトコルを持つ

- ESP (Encapsulating Security Payload)

- パケットの暗号化機能

- AH (Authentication Header)

- パケットの改ざん検知機能



# ESPの提供するセキュリティ機能

- 秘密性
  - パケットの暗号化
- 認証(本人性確認)
  - 送信元の保証(ペイロードの改ざん防止のみ)
- 認証(完全性保証)
  - パケットが改ざんされていないことの保証
- アクセス制御
  - パケットのフィルタリング

# AHの提供するセキュリティ機能

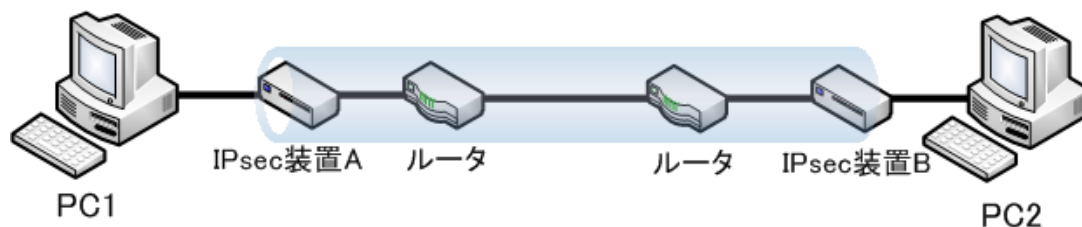
- 認証(本人製確認)
  - リプレイ攻撃の防止
  - パケット送信元を完全に保証  
( IPヘッダまで含めて認証 ESPより強力)
- 認証(完全性保証)
  - パケットが改ざんされていないことの保証
- アクセス制御
  - パケットのフィルタリング



# カプセル化モード

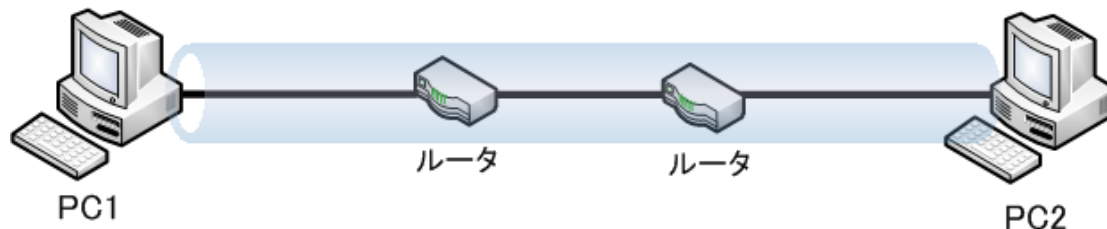
## ■ トンネルモード

- 実際に通信するホスト以外がパケットをIPsec化
- エンドツーエンドでの認証・暗号化に使用



## ■ トランスポートモード

- 通信するホスト同士が自身のパケットをIPsec化
- ネットワーク間の通信に対して認証や暗号化を行う場合に使用



# パケットのIPsec化 (ESP)

## 元のパケット

宛先 送信元	TCPヘッダ	データ
IPヘッダ		
元のパケット		

## トンネルモードでIPsec (ESP)化されたパケット

宛先 送信元	ESPヘッダ	宛先 送信元	TCPヘッダ	データ	ESP トレイラ	ESP 認証値
新しいIPヘッダ		元のIPヘッダ				
		元のパケット				
		暗号化される範囲				
		認証(完全性保証)の対象範囲				

## トランスポートモードでIPsec (ESP)化されたパケット

宛先 送信元	ESPヘッダ	TCPヘッダ	データ	ESP トレイラ	ESP 認証値
元のIPヘッダ					
		元のパケットのペイロード部分			
		暗号化される範囲			
		認証(完全性保証)の対象範囲			

# パケットのIPsec化 (AH)

## 元のパケット

宛先 送信元	TCPヘッダ	データ
IPヘッダ		
元のパケット		

## トンネルモードでIPsec (AH)化されたパケット

宛先 送信元	AH	宛先 送信元	TCPヘッダ	データ
新しいIPヘッダ		元のIPヘッダ		
認証(完全性保証)の対象範囲 ただしIPヘッダの一部転送中可変フィールドは除く				

## トランスポートモードでIPsec (AH)化されたパケット

宛先 送信元	AH	TCPヘッダ	データ
元のIPヘッダ		元のパケットのペイロード部分	
認証(完全性保証)の対象範囲 ただしIPヘッダの一部転送中可変フィールドは除く			

# カプセル化モードとプロトコル

## ■ カプセル化モード

- トランスポートモード
- トンネルモード

## ■ プロトコル

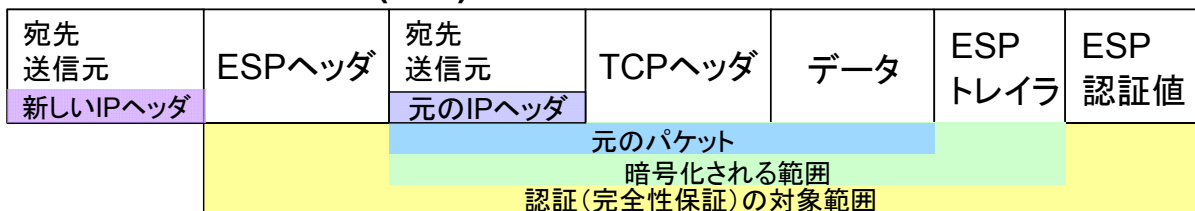
- ESP
- AH

組み合わせは自由

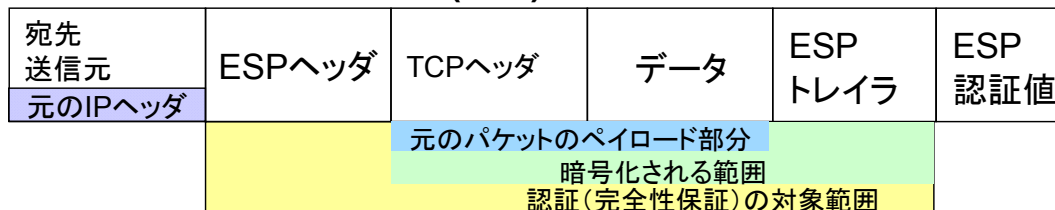
# カプセル化モードとプロトコル


- ESP単体では転送用IPヘッダの改ざんは検知不可能
  - 不要ならESPのみで十分
  - ESPで暗号化 → AHで認証
- ESPに認証(完全性保証)機能を提供
  - AHの必要性の減少

トンネルモードでIPsec (ESP)化されたパケット



トランスポートモードでIPsec (ESP)化されたパケット





# 第2章

## IPsec Security Association

# SAの属性

- セキュリティプロトコル
  - ESPまたはAH
- カプセル化モード
  - トンネルモードまたはトランスポートモード
- Security Parameters Index (SPI)
  - SAを識別するための識別子  
通信相手のアドレス等と組み合わせて使用
- 暗号化・認証アルゴリズム
  - 3DES, MD5など
- セレクタ
  - SAに流すパケットの指定

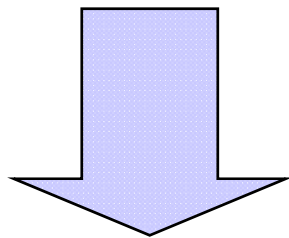
# 暗号化アルゴリズム

- IPsecでは、同じ秘密鍵を送信者と受信者で共有する  
(秘密対象鍵)
- DES,3DESが多く使用される
- ブロック暗号
  - 決められた長さのブロック単位に暗号化を行う
- CBCモード
  - 暗号化するブロックの平文と,1つ前のブロックの暗号化結果とのXOR値を暗号化する



# 認証アルゴリズム

- 認証(完全性保証)
- 認証(本人性確認)




- 一方向性ハッシュ関数により確認
  - MD5
  - SHA-1
  - HMAC (鍵付きハッシュ関数)

# セレクト

## ■ パケットをIPsec化するルールを決定

- 宛先IPアドレス
- 送信元IPアドレス
- トランスポートレイヤプロトコル(TCP,UDPなど)
- 送信元ポート,宛先ポート
- ユーザ名,ホスト名



# 第3章

## Internet Key Exchange

# IKE (Internet Key Exchange)とは

## ■ SAの自動生成・管理プロトコル

### □ SA自動生成

- IPsec通信が必要になると、オンデマンドで生成

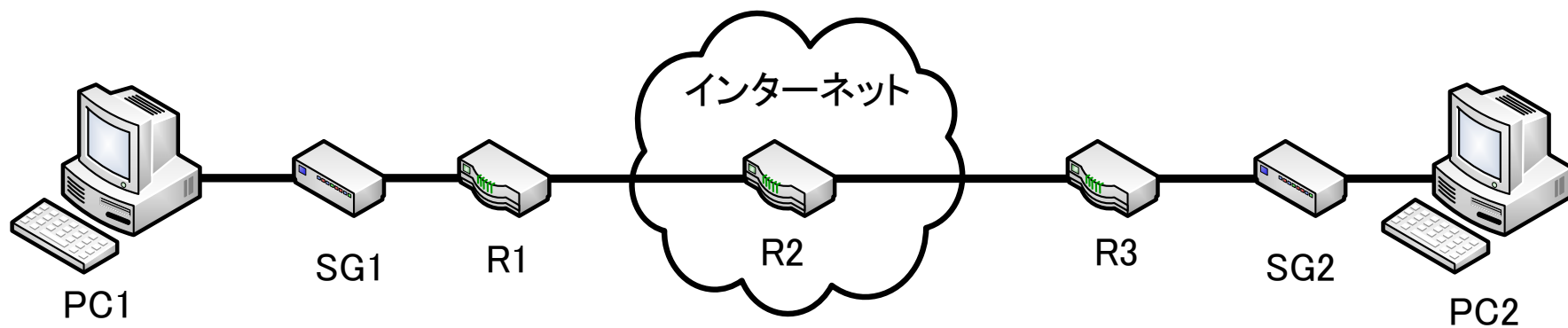
### □ SAの管理

- SAが生成されてからの期間や使用状況を監視
- SAを秘密対象鍵ごと作り直す

# IKEの基本機能

- Proposal (SA生成の要求) 交換
  - 生成するSAのパラメータをネゴシエートして決定
- Diffie-Hellman 交換
  - 生成するSAの秘密対象鍵を安全に自動生成
- IKE相手の認証 (本人性確認)
  - 通信相手が偽者でないことを確認

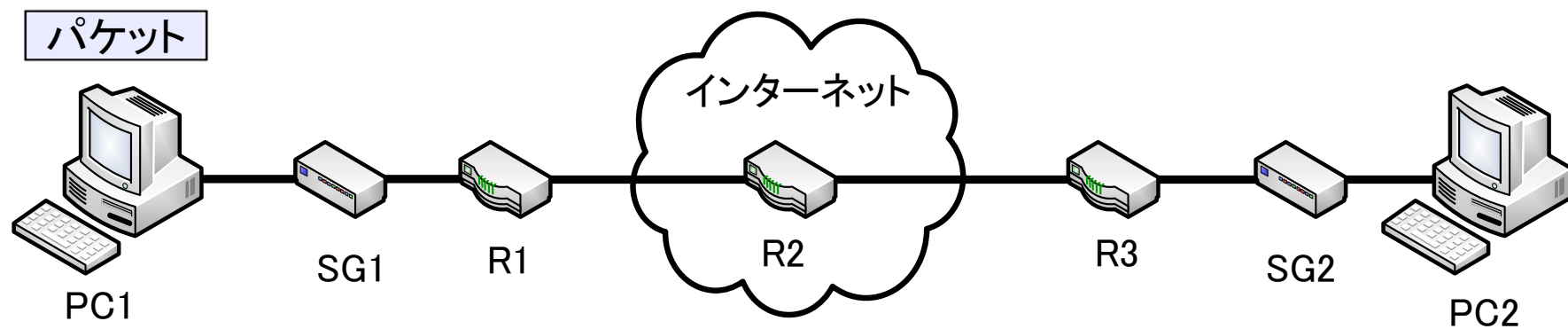
# IKE動作の典型例



- PC1がPC2へpingを打つ

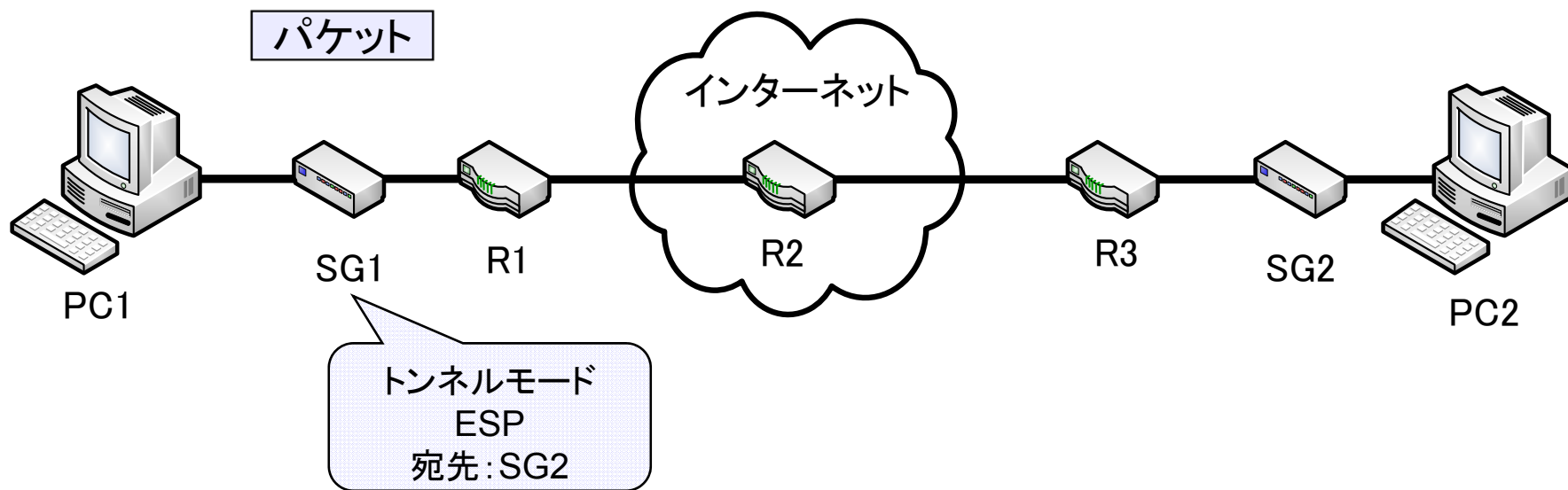
SG: セキュリティゲートウェイ  
R: ルーター

# IKE動作の典型例



- パケットをSG1に向けて送信  
(SG1: PC1のデフォルトゲートウェイ)

# IKE動作の典型例

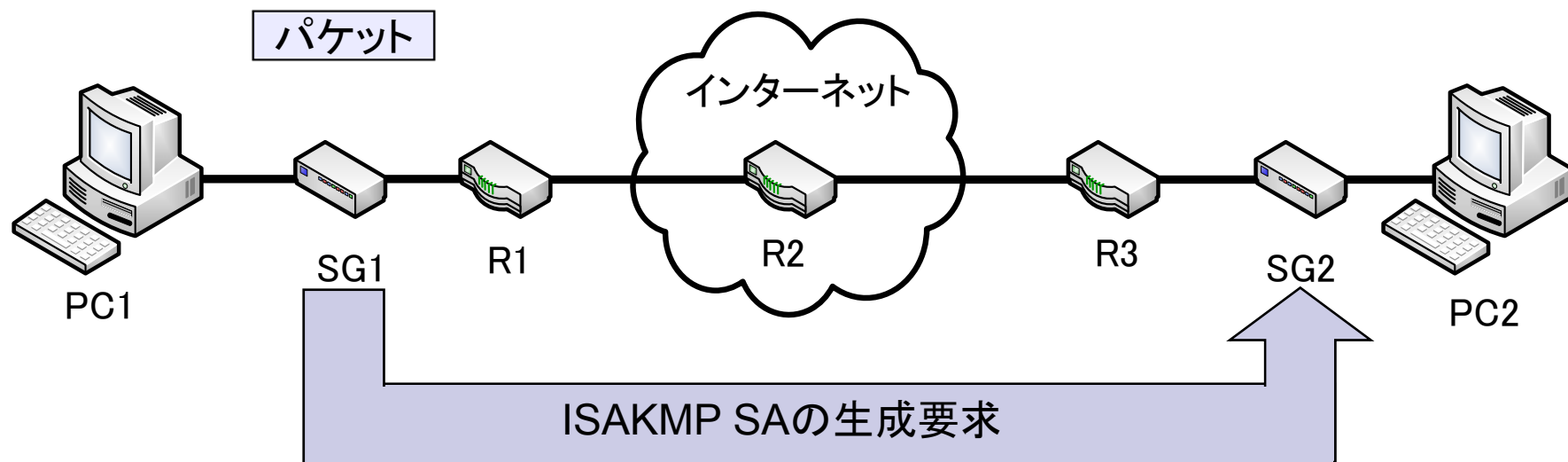


- SG1のセキュリティポリシーを参照し、IPsec化



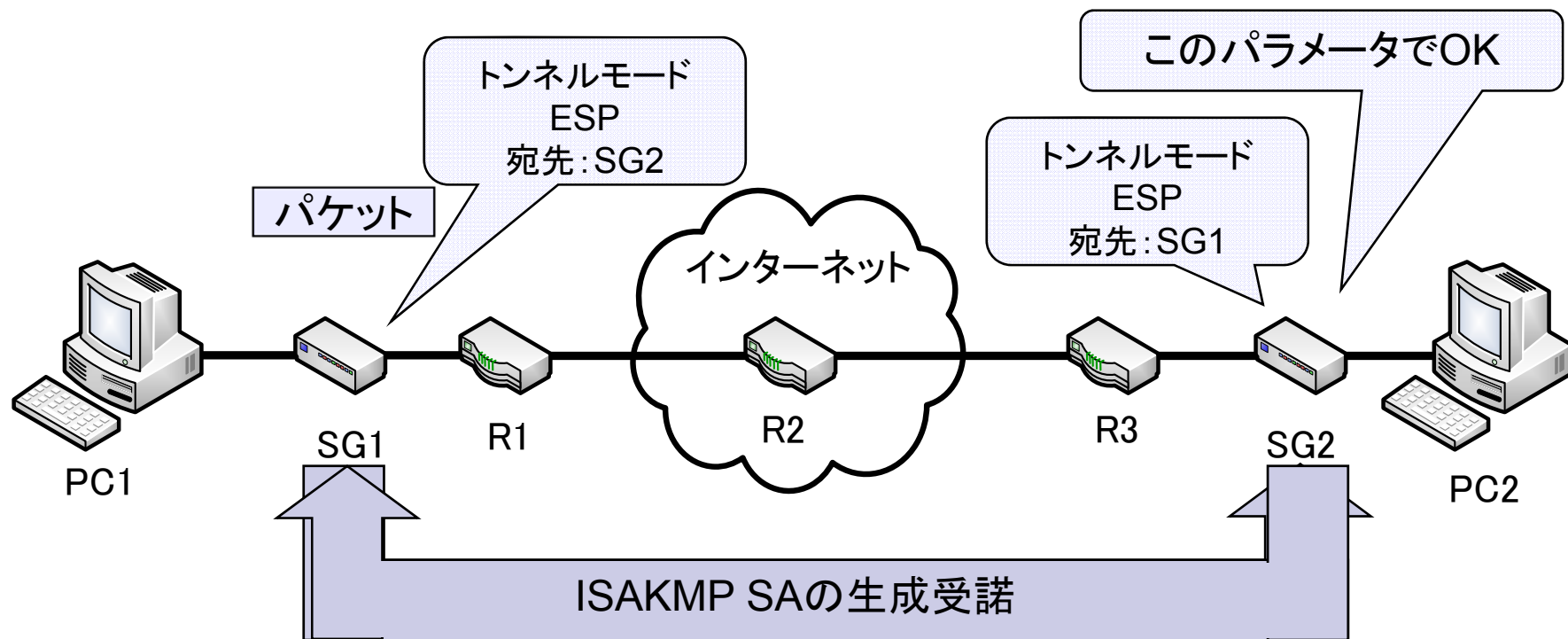
# IKE動作の典型例

ISAKMP SA:  
IKEによりSAを自動生成する際に  
IKE自身が制御信号をやり取りする  
制御用チャネル



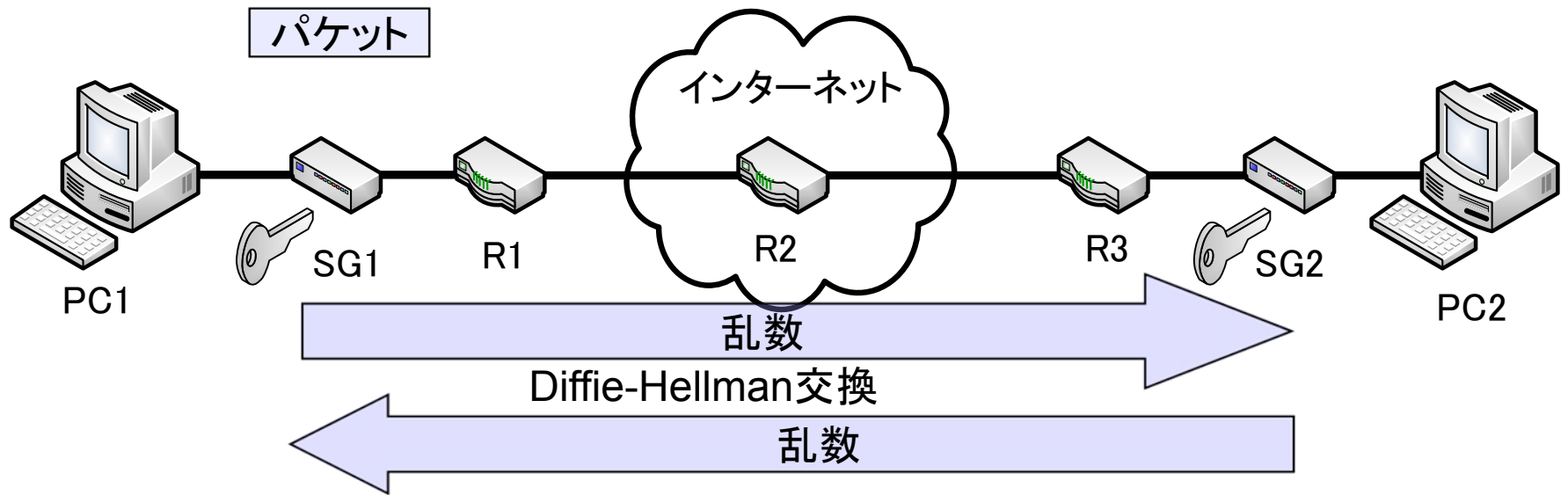
- SG1がISAKMP SAの生成要求をSG2に送信  
(Proposal)

# IKE動作の典型例



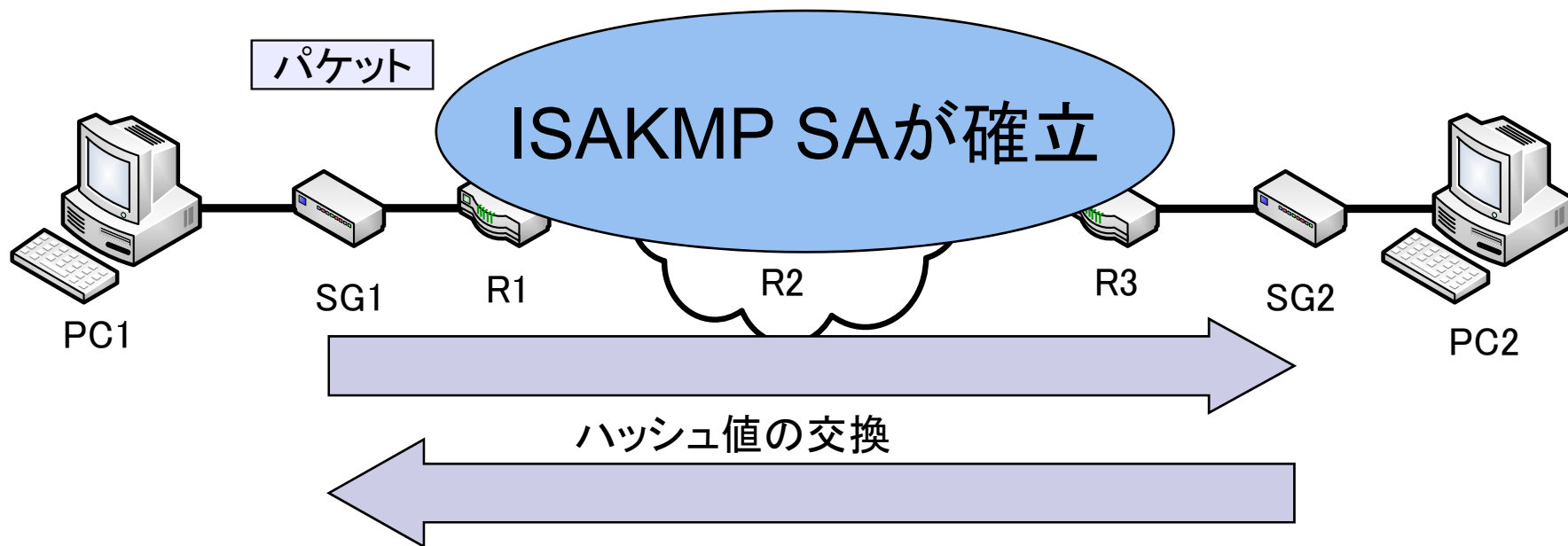
- SG1がISAKMP SAの生成要求をSG2に送信  
(Proposal)

# IKE動作の典型例



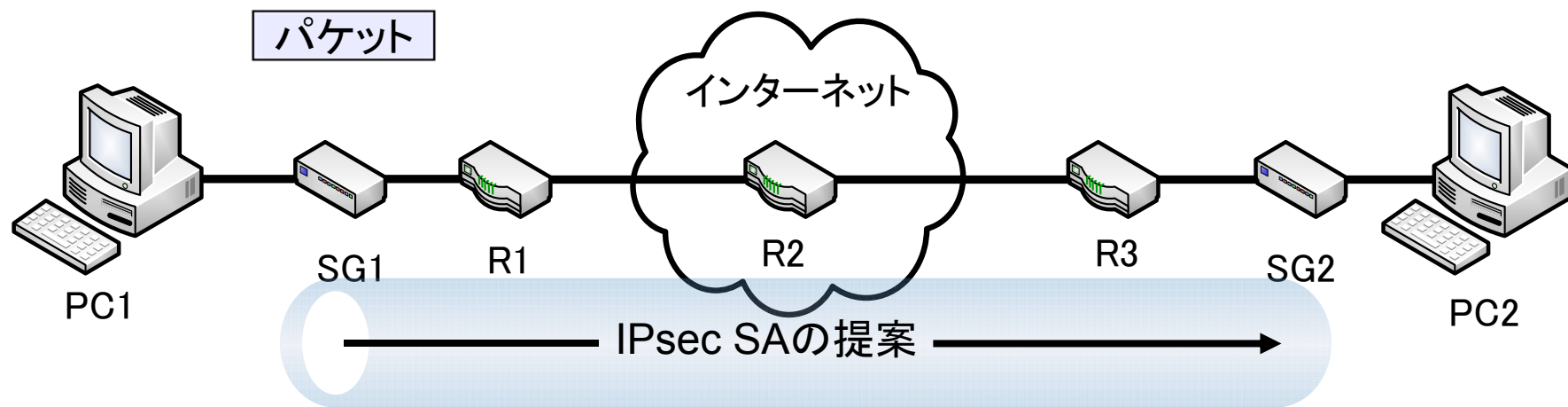
- Diffie-Hellman交換により秘密対象鍵を生成

# IKE動作の典型例



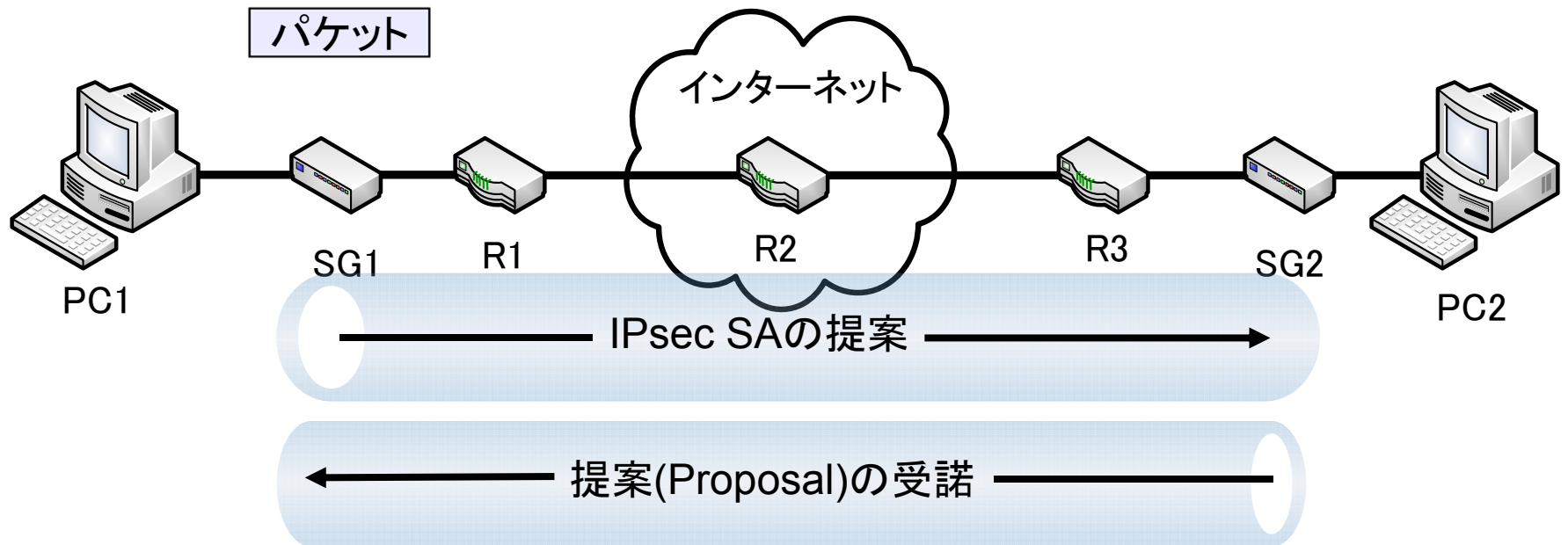
- IKE相手が本物かどうかの確認
- 認証(本人性確認)値の交換

# IKE動作の典型例



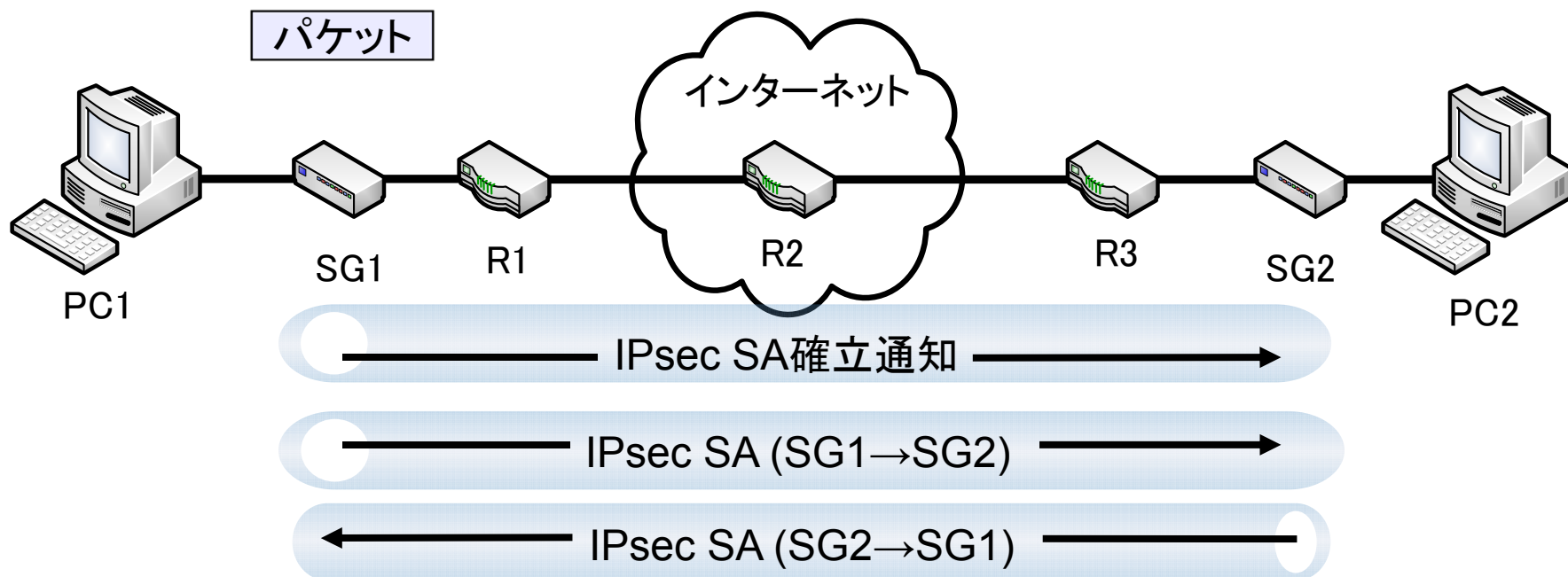
- SG1はパケットをIPsec化するためのSAのProposalをセキュリティポリシーに従ってSG2に送信
- 暗号化に使用する鍵を作るための乱数も同時に送る
- ISAKMP SAを通じているため暗号化されている

# IKE動作の典型例



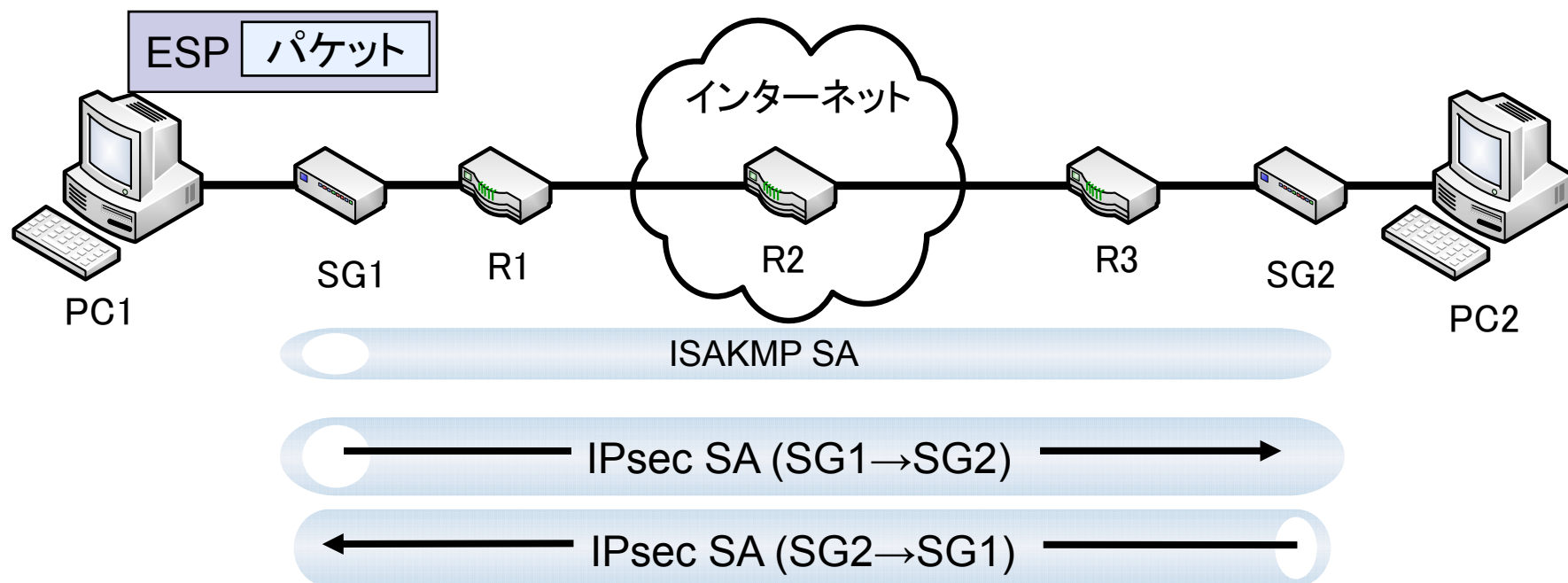
- 受諾したSAと、暗号化に使用する鍵を作るための乱数を返信

# IKE動作の典型例



- SG1よりSG2へ IPsec SA確立の通知

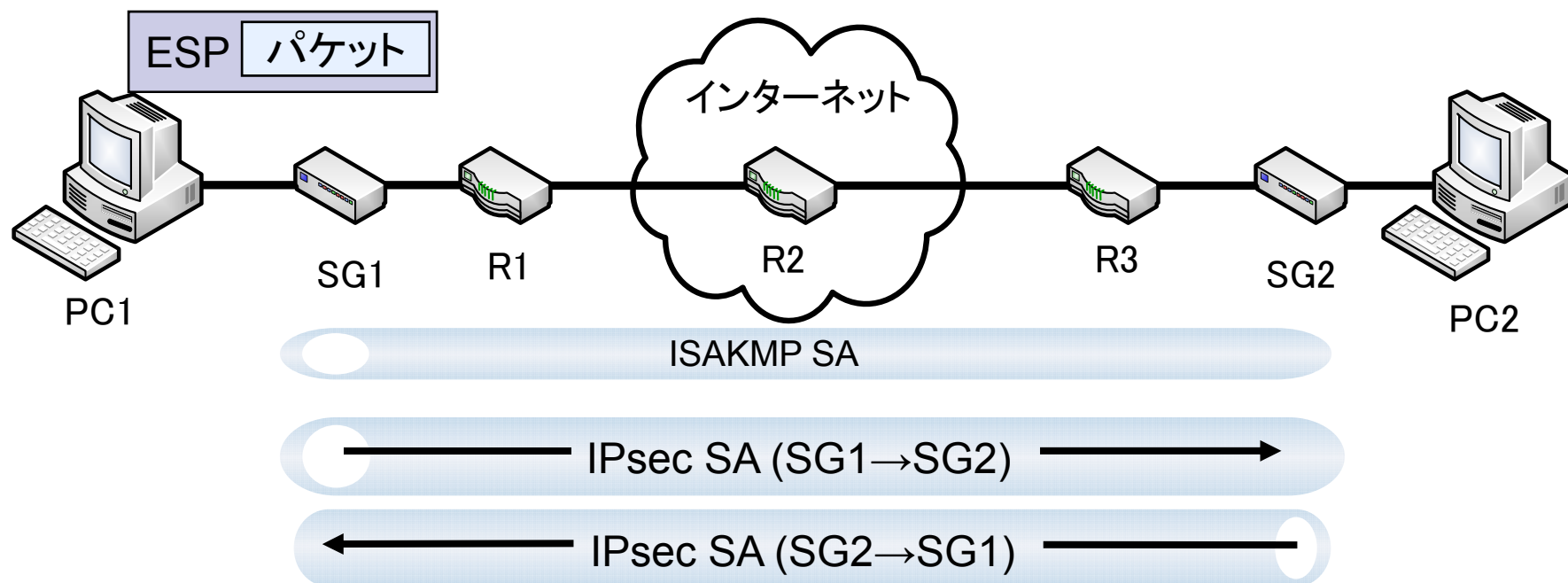
# IKE動作の典型例 (パケットのIPsec化)



- パケットをESP化

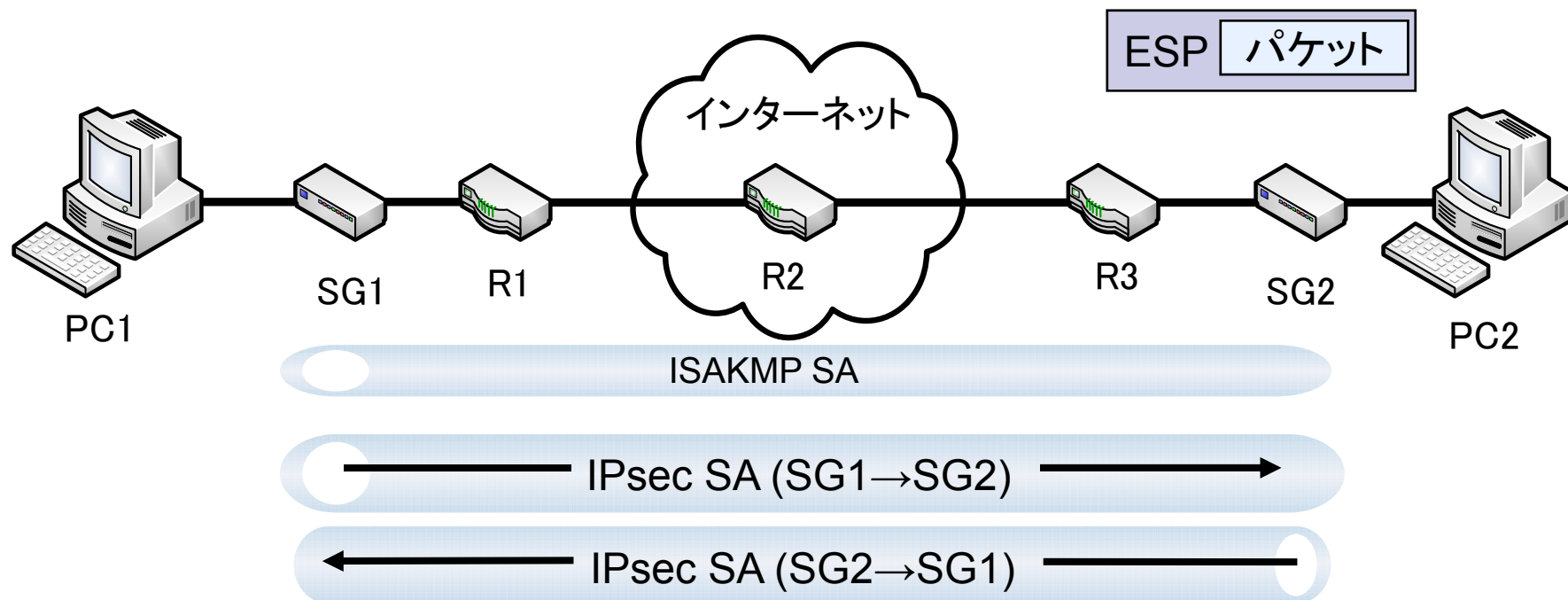


# IKE動作の典型例 (パケットのIPsec化)



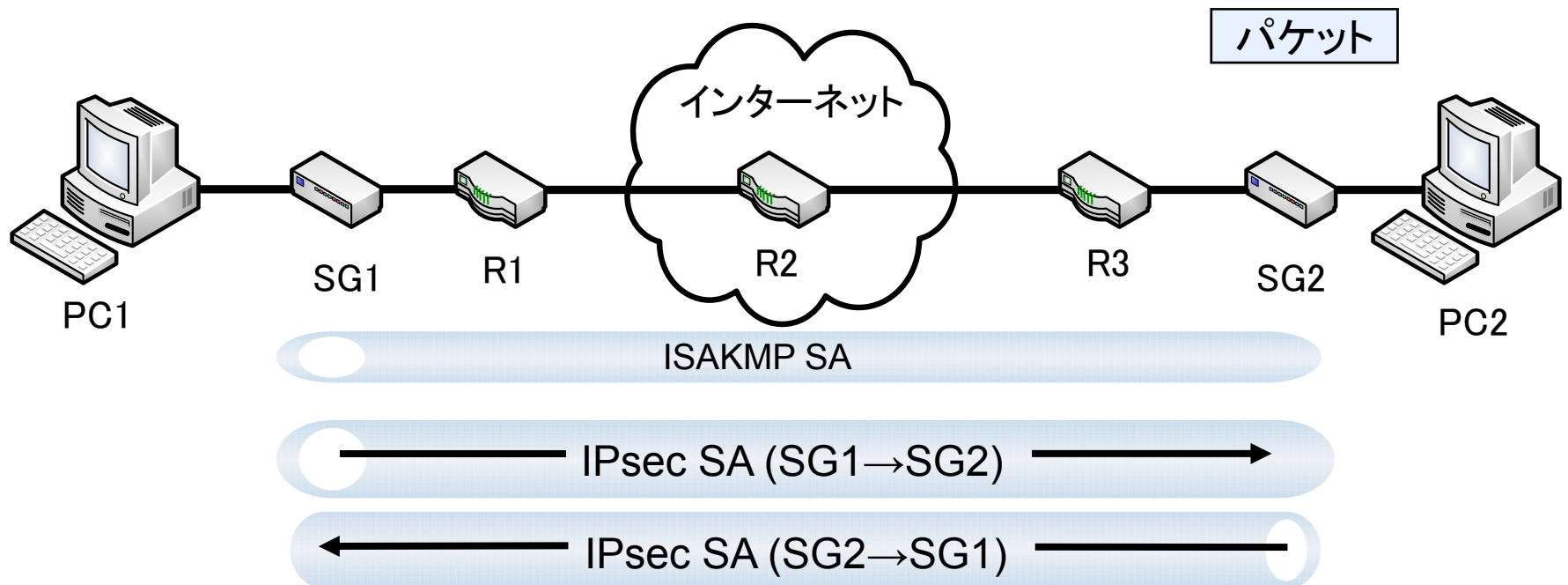
- SG1よりSG2へ ESP化されたパケットを送信

# IKE動作の典型例 (パケットのIPsec化)



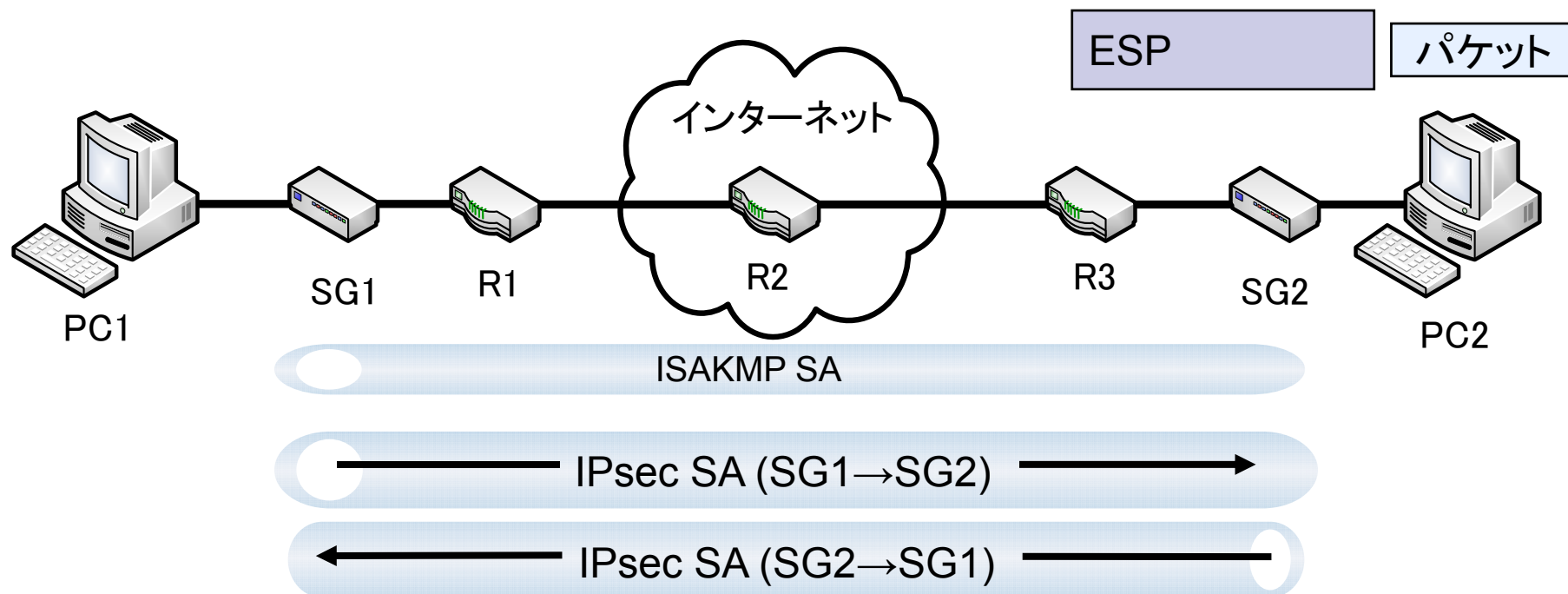
- 秘密対象鍵を用いて復号化

# IKE動作の典型例 (PC2からの応答)



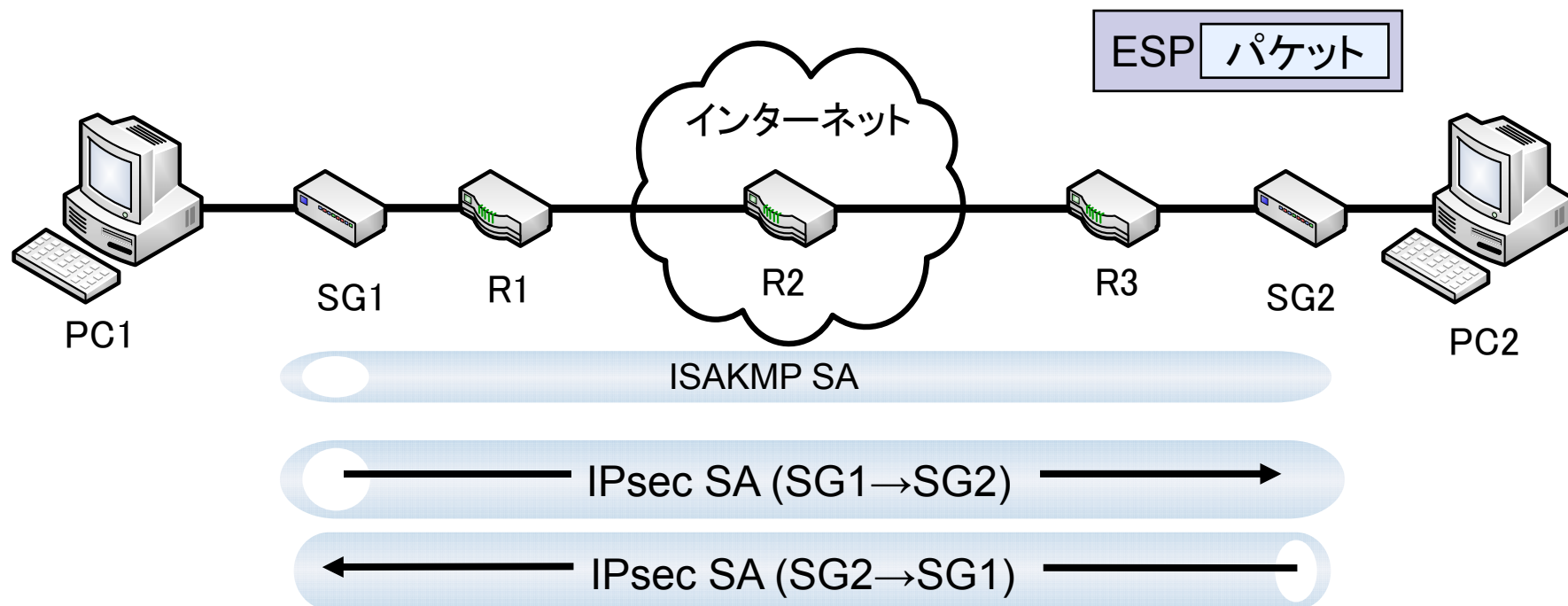
- SG1はPC2へ復号化されたパケットを送信

# IKE動作の典型例 (PC2からの応答)



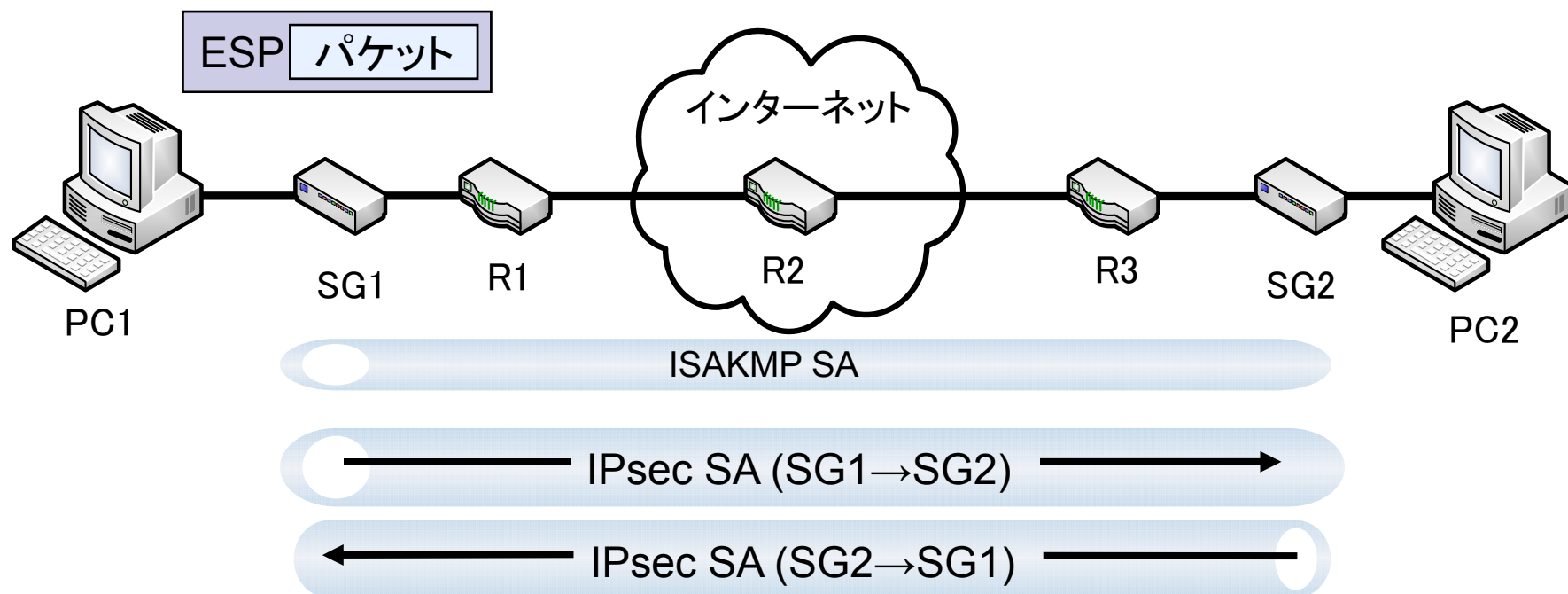
- 同様に、SG2でESP化、SG1へ送信  
SG2で復号化、PC1へ転送

# IKE動作の典型例 (PC2からの応答)



- 同様に、SG2でESP化、SG1へ送信  
SG2で復号化、PC1へ転送

# IKE動作の典型例 (PC2からの応答)



- 同様に、SG2でESP化、SG1へ送信  
SG2で復号化、PC1へ転送

# 最後に

- IPsecとは
- SA(ESP,AH)の概要
- IKEの動作例