本資料について

本資料は下記文献を基にして作成されたものです．文書の内容の正確さは保証できないため，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

出版社：翔泳社

著者：小早川知昭

監修：西田晴彦

IPsec 徹底入門

発表者
渡邊研究室　01j060 瀬下 正樹

はじめに

- インターネットが普及
  - セキュリティ技術が重要
    - 特にインターネットとセキュリティ技術を利用したVPNの構築技術が重要

VPN(Virtual Private Network)

- インターネット上に仮想的な専用線空間を作り出し，拠点間を接続したネットワーク

VPNの利点

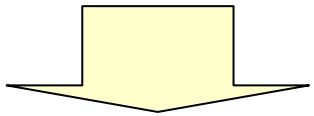
- 専用線の代わりにインターネットを利用するため安価
- 通信の暗号化による安全性の向上
- 世界中からリモートアクセスが可能

安全なVPNの構築

＜必要なセキュリティー機能＞

1. 秘密性
   - 盗聴などから通信を保護
2. 認証（本人性確認）
   - そのメッセージが本当に表示された送信元からのであることを保証
   - 通信接続の際に相手が本当に意図した本物であることを保証
3. 認証（完全性保証）
   - メッセージが改ざんされていないことを保証

4. 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する機能
5. 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/遮断する機能
6. 可用性
   - システムが常に使用できること



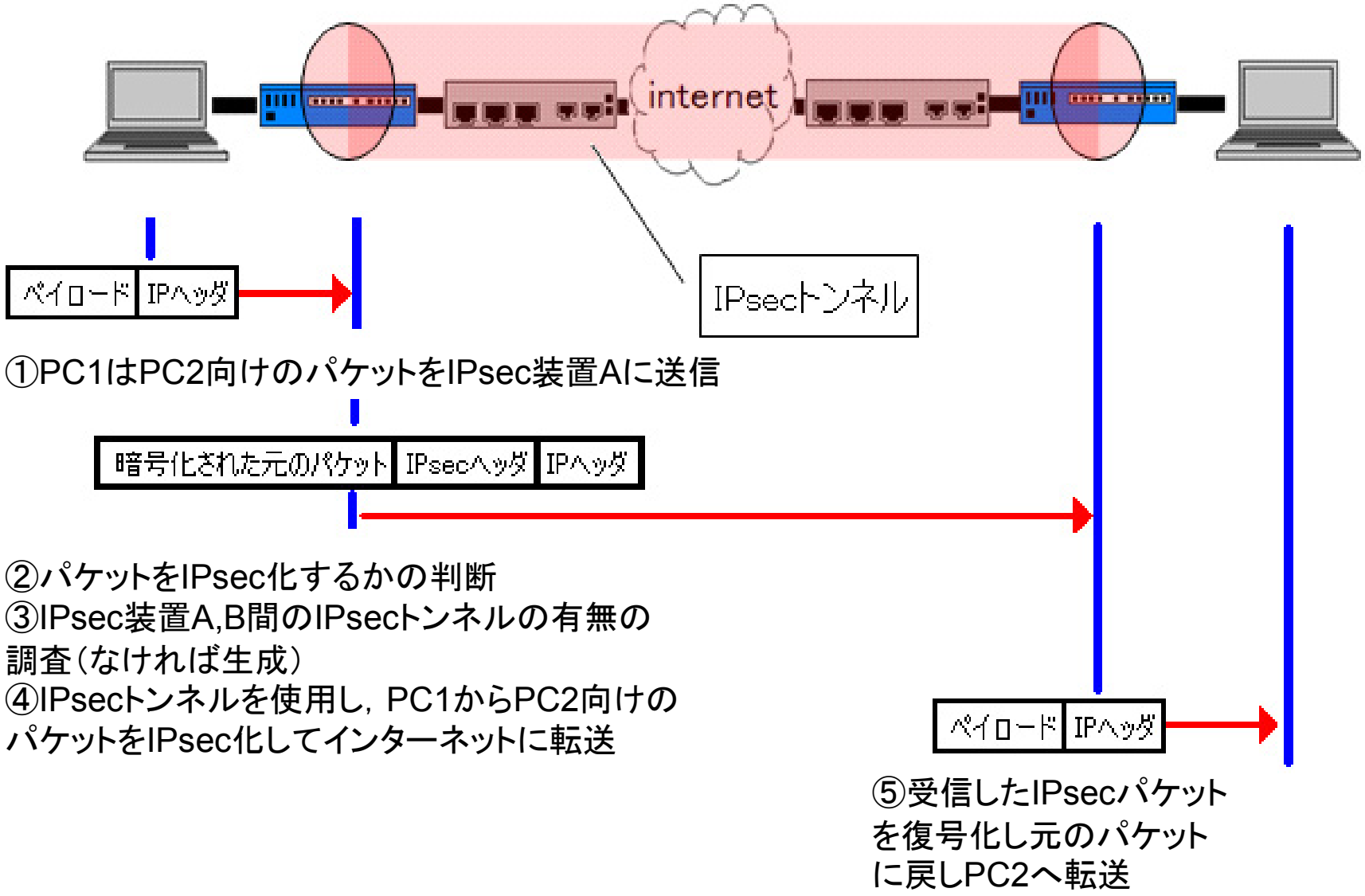
IPsec

⇒これらのセキュリティー機能をIPレイヤで実現するプロトコル

第1章　IPsec の全体像

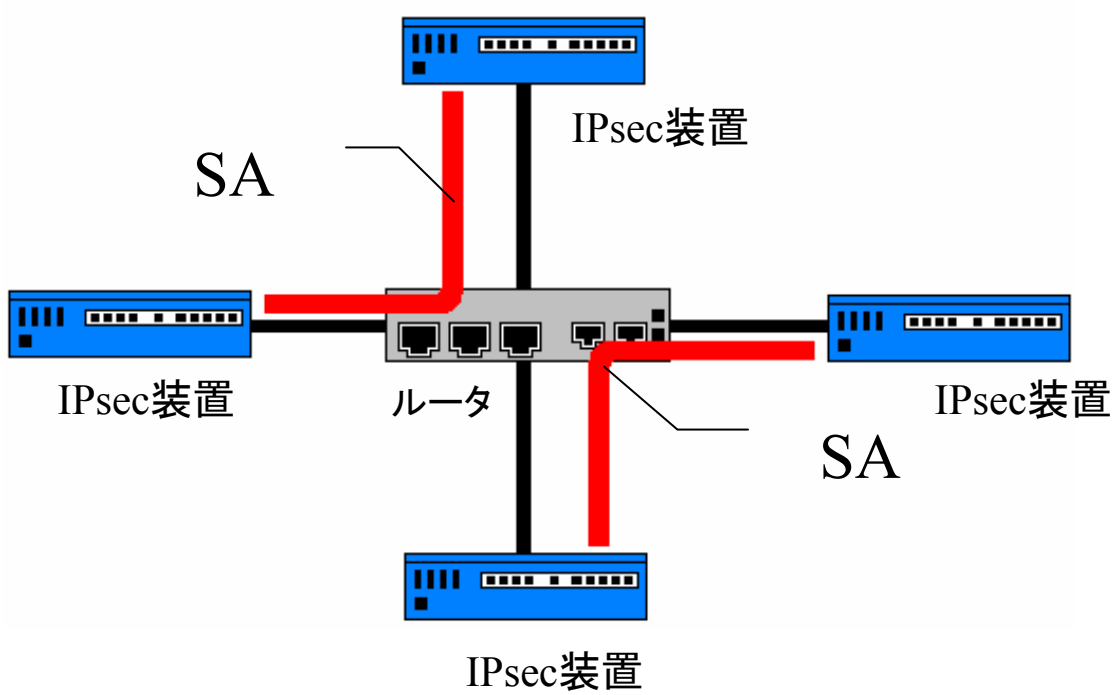
- IPsec
  - IPパケットを安全に運ぶための技術
- ■ 優れた点
  - 仕様が公開されており，また厳しい検証に耐えてきた技術で極めて安全
  - インターネットをそのまま使用
  - アプリケーションに変更を加えなくてよい
  - 標準化されている唯一のIPレイヤでのセキュリティ実現機能
- ■ 欠点
  - 複雑で理解しにくい

IPsecの動作イメージ



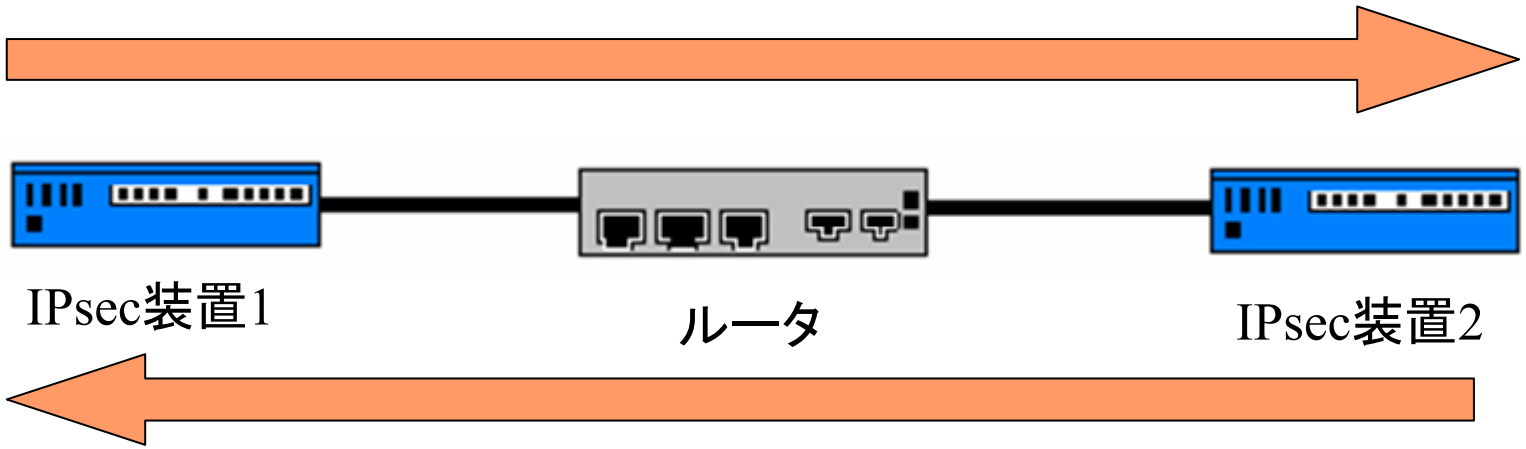
第二章　SA(Security Association)

- SA(Security Association)
  - 前スライドにおけるIPsecトンネル
  - SAはIPsec装置間で生成
  - すべてのIPsecパケットはいずれかのSAに所属して送り出される
  - パケットに暗号化などのセキュリティ機能を提供



SA(Security Association)

- SAのディレクション
  - 単方向通信可能なトンネル
  - 双方向とする場合は2つ作る



SA(Security Association)

- SAの属性の種類
  - セキュリティプロトコル
  - カプセル化モード
  - Security Parameters Index(SPI)
  - 暗号化や認証アルゴリズム
  - セレクタ

⇒属性の設定によりSAを特徴づける

SAの属性

セキュリティプロトコル

- セキュリティプロトコル
  - 暗号化や認証の違いで分けた二種類
    - ESP・・・暗号化機能と認証機能の両方
    - AH・・・暗号化機能はないが、強力な認証機能

SAの属性

カプセル化モード

- どのホストで作られ、どのホストに届けられるという観点から分類した2つのカプセル化モード
  - トンネルモード
  - トランスポートモード
- 各モードの効用的側面
  - トランスポートモードは通信の内容を秘密にする
  - トンネルモードは通信の内容ばかりか存在そのものを秘密にする

•トンネルモード

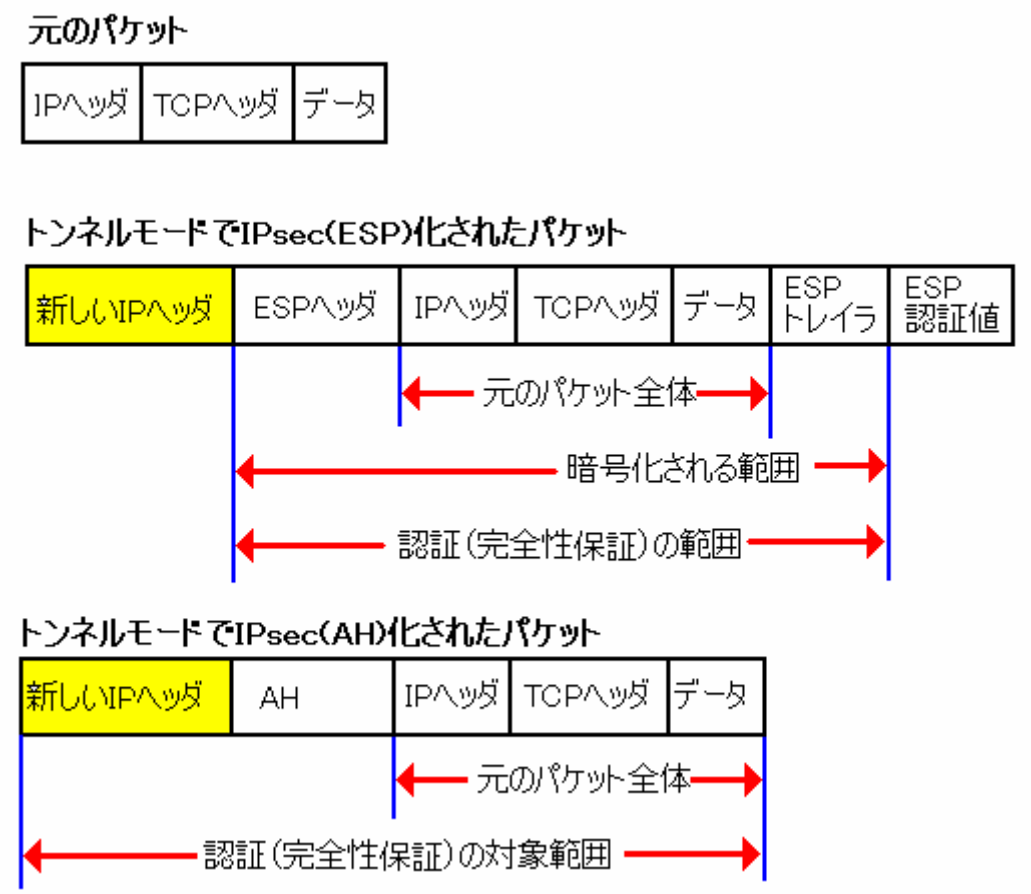
適応領域：セキュリティゲートウェイからセキュリティゲートウェイ（GWからhostまたはhostからhostも可）

• トランスポートモード

適応領域：ホストからホスト(ホスト自身がIPsec装置の機能を持っている)

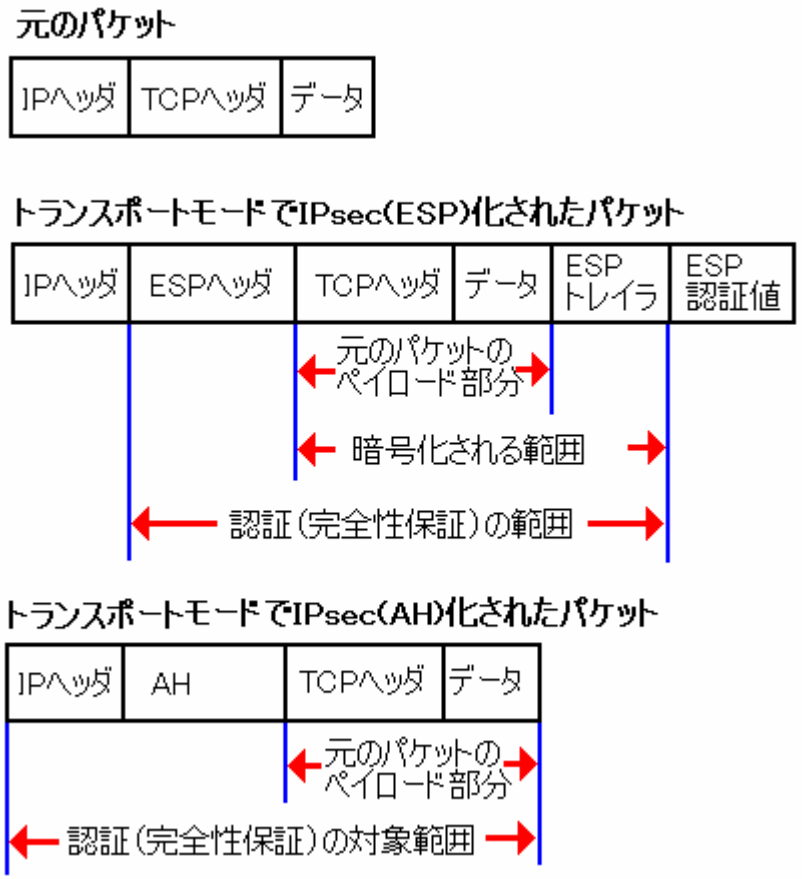
トンネルモードにおけるパケット

- トンネルモードは転送用の新しいIPヘッダを付加
- ESP、AHにより暗号化や認証範囲が異なる



トランスポートモードにおけるパケット

- 元のパケットのIPヘッダをそのまま使用
- ESP、AHにより暗号化や認証範囲が異なる



SAの属性

Security Parameters Index(SPI)

- SAを識別するための識別子
  - 実際はSPIだけではSAを識別することは不十分
    - IPsec通信相手のアドレスなどと組み合わせて使用

SAの属性

暗号化アルゴリズム

- IPsecでは使用する暗号化アルゴリズムや認証アルゴリズムをSAごとに選択することが可能
- IPsecで使用される暗号化アルゴリズムは公開鍵暗号ではなく、同じ秘密鍵を送信者と受信者で共有する対称暗号
- DESや3DESが多く使用されている

SAの属性

認証アルゴリズム

- IPsecにおける認証
  - パケットが通信経路上で改ざんされていないかを認証（完全性保証）
  - 通信相手が本物であるかどうか認証（本人性確認）
- 一方向性ハッシュ関数と呼ぶ数学的手法を用いてそれらを実現

SAの属性

セレクタ

- セレクタ
  - どのようなパケットをIPsec化するかを決定
- セレクタの種類
  - 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かUDPかなど）
  - 送信元ポートと宛先ポート
  - ユーザ名やホスト名

  =>セレクタを設定しSAのセキュリティーポリシーを決定

第三章　IKE(Internet Key Exchange)

- IKE
  - SAの自動生成、管理を行うプロトコル
    - SAを生成する場合、暗号化に使う秘密対称鍵やその他のパラメータをIPsec装置それぞれに設定することが必要
- IKEの3つの基本機能
  - Proposal交換・・・SAパラメータ決定
  - Diffie-Hellman交換・・・鍵の自動生成
  - IKE相手の認証（本人性確認）・・IKE通信相手が本物であることの確認

IKE(Interne Key Exchange)

- IKEが生成するSA
  - IKE自身が制御用に使用するSAと、パケットのIPsec化に使用するSAの2種類が存在

1. ISAKMP SA
   - IKE自身が制御信号をやりとりするために使用．実際のパケットをIPsec化して送信することはできない．双方向．
   - ISAKMP SA確立の一連の作業をPhase 1と呼ぶ
2. IPsec SA（第二章で説明してSAと同じ）
   - ISAKMP SA生成後にISAKMP SAを通して生成．実際のパケットをIPsec化して送信するSA．単方向．
   - IPsec SA確立の一連の作業をPhase 2と呼ぶ

IKEは3つの基本機能を使用し上記2種類のSAを生成する

IKEの基本機能

Proposal交換

- Proposal交換
  - SAを確立する際，装置間でSAパラメータを交換し決定
    - Proposal交換を提案する側のIPsec装置をイニシエータ，受信側をレスポンダと呼ぶ
- Proposal交換の動作概要
  - レスポンダがProposalを受信した場合，セキュリティポリシー（事前に設定しておく必要がある）に合致するProposalだけをイニシエータに返信

IKEの基本機能

Proposal交換－ISAKMP SA－

- ISAKMP SA確立(Phase 1)のためにProposal交換で決定しなければならないパラメータ
  - 暗号化アルゴリズム
  - ハッシュアルゴリズム
  - 認証方式
  - Diffie-Hellman交換に使用するパラメータ
  - Life type と Life duration

IKEの基本機能

Proposal交換－IPsec SA－

- IPsec SA確立(Phase 2)のためにProposal交換で決定しなければならないパラメータ
  - セキュリティープロトコル（ESPかAH）
  - Life type と Life duration
  - カプセル化モード（トンネルモードかトランスポートモード）
  - 暗号化アルゴリズム
  - 認証アルゴリズム
  - Diffie-Hellman交換に使用するパラメータ

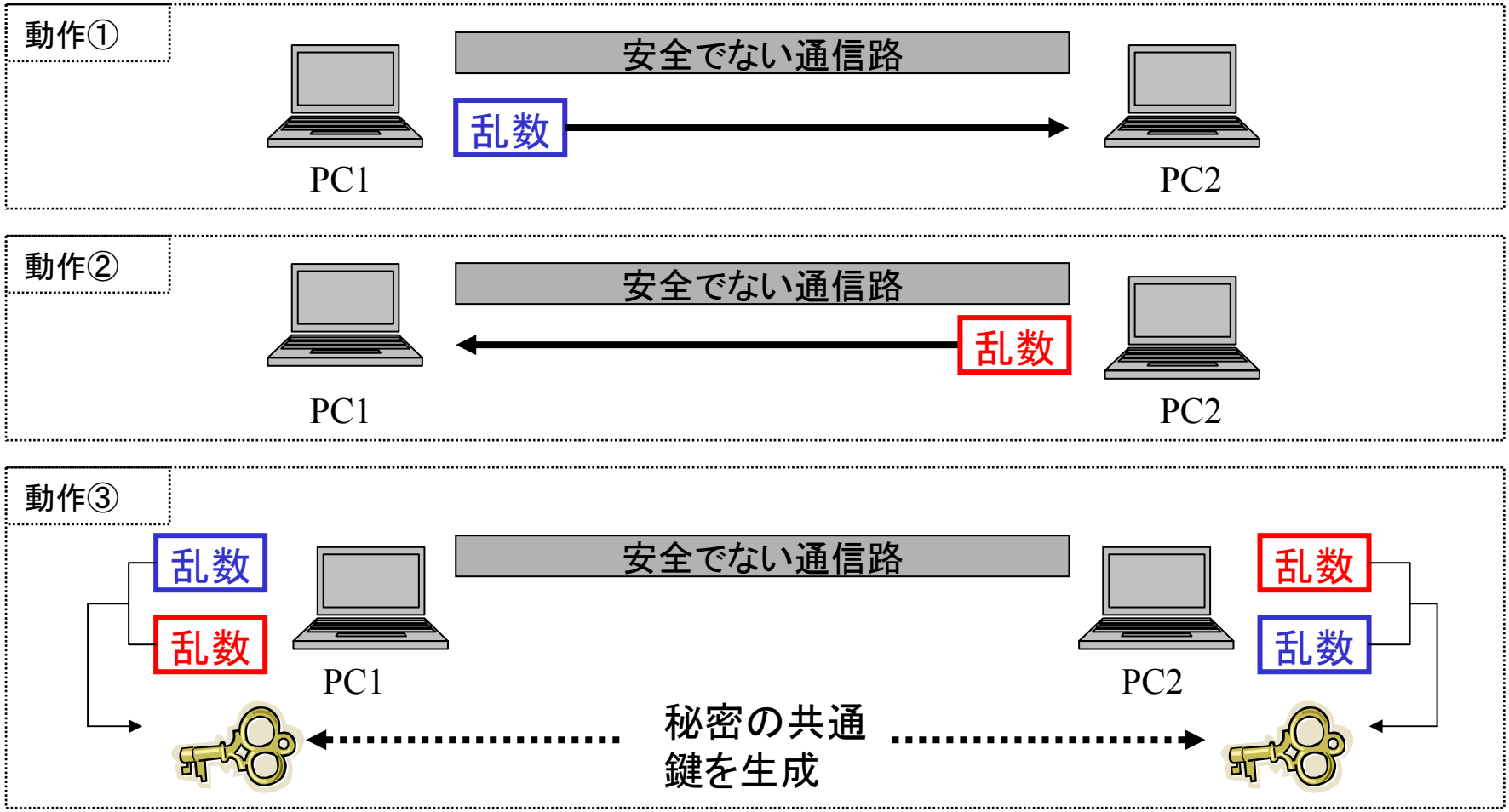
IKEの基本機能

Diffie Hellman交換

- Diffie-Helman交換
  - ある乱数を交換するだけで、安全でない通信路を使用しているのにかかわらず同一の秘密鍵を共有することができる

IKEの基本機能：Diffie-Helman交換

- Diffie-Hellman交換イメージ



IKEの基本機能

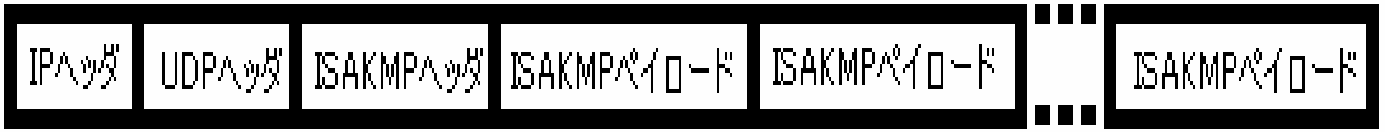
相手認証

- IKEにおける認証
  - Pre-Shared Key認証が一般的に使用される
    - Pre-Shared Key
      - パスワード認証方式
      - 通信相手と事前に共有しておく必要がある

ISAKMPについて

- ISAKMP
  - IKEで実際にやりとりするパケットフォーマットを規定しているプロトコル

- ISAKMPパケットの構成



⇒ISAKMPペイロードには色々な種類があり、目的に応じてペイロードを使い分ける

ISAKMPペイロード

- ISAKMPペイロードは
  - IKEのデータを運ぶためのペイロード
- さまざまな種類のペイロードが存在し、それらの組み合わせでISAKMPパケットを構成
  - Security Association ペイロード
  - Proposal ペイロード
  - Transform ペイロード
  - Key Exchange ペイロード
  - Identification ペイロード
  - Certificate ペイロード
  - Certificate Request ペイロード
  - Hash ペイロード
  - Signature ペイロード
  - Nonce ペイロード
  - Notification ペイロード
  - Delete ペイロード
  - Vendor ID ペイロード

ISAKMPペイロード

- Security Association(SA)ペイロード
- Proposalペイロード
- Transformペイロード
  - 上記3つのペイロードはISAKMP SAやIPsec SAを作るためProposal交換を行う際に使用

ISAKMPペイロード

- KEY Exchangeペイロード（鍵交換ペイロード）
  - Diffie-Hellman交換を行う際にDiffie-Hellman公開値を交換するのに使用
- Nonce（乱数）ペイロード
  - IKE交換を行う際に相手が実際に動作しているIPsec装置かどうかを確認するために用いられる乱数の交換に使用

ISAKMPペイロード

- Identificationペイロード
  - ID情報を交換するペイロード
    - 誰のためにそのSAをネゴシエートしようとしているかを示すために使用
- Hashペイロード
  - メッセージのハッシュ値を送信するためのペイロード
    - IKE通信を行っている通信相手が本物かの認証とISAKMPメッセージが改ざんされていないことを確認するために使用

交換タイプについて

- ISAKMPペイロードをどのように組み合わせ、どのような順番でやりとりするかという決まりを交換タイプと呼ぶ
- 交換タイプの種類
  - Main Mode
  - Aggressive Mode
  - Quick Mode

交換タイプ

Main Mode

- Main Mode
  - Phase1でISAKMP SAを確立するために使用

＜動作順序＞

1. SAペイロードを交換しSAパラメータを決定
2. 鍵交換ペイロードとNonceペイロードを交換してDiffie-Hellmanによる鍵生成
3. IDペイロードとHashペイロードを交換してお互いが本物であることを確認
4. ISAKMP SAの確立

交換タイプ

Aggressive Mode

- Aggressive Mode
  - Phase1でISAKMP SAをMain Modeより簡易に確立
    - しかしMain Modeでは暗号化されて送信されるIDペイロードが平文で送信

＜動作順序＞

1. SAペイロード，鍵交換ペイロード，Nonceペイロード，IDペイロードを送信．それの返答としてレスポンダが上記ペイロードにHashペイロードを付加したものを返信
（機能：SAパラメータの決定と鍵生成と認証の一部）
2. イニシエータがHashペイロードを送信
（機能：本人性確認の認証）
3. ISAKMP SAの確立

交換タイプ

Quick Mode

- Quick Mode
  - Phase2でIPsec SAを生成するために使用
    - 既に確立しているISAKMP SAを利用するため交換はすべて暗号化されており、わずかなパケットの交換で安全にSAを確立

＜動作順序＞

1. Hashペイロード，SAペイロード，Nonceペイロード，イニシエータ側IDペイロードとレスポンダ側IDペイロードを送信
2. レスポンダ側は同様のペイロードを返信し，最後にイニシエータがHashペイロードを送信
3. IPsec SAの確立

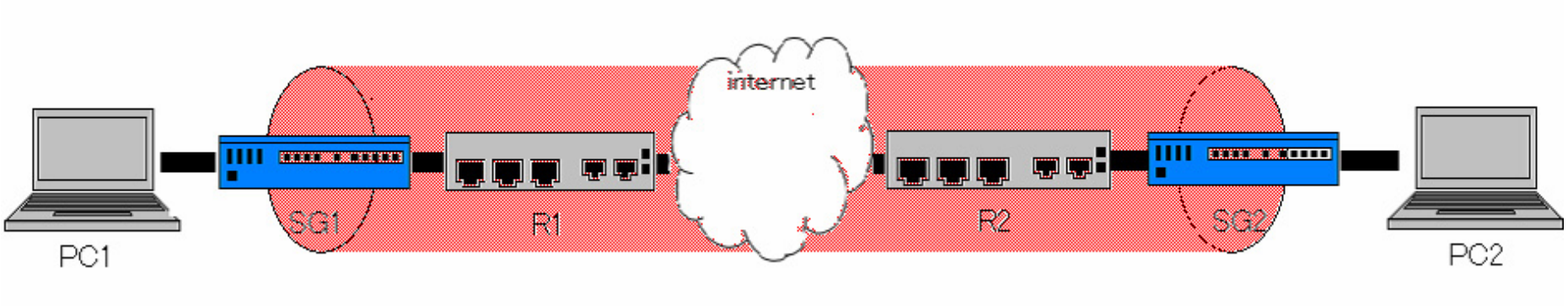
具体的なIKEの動作

各設定

- Phase 1にMain Modeを適用
- Phase 2にQuick Modeを適用
- ESPによるIPsec SAの生成
- IKE認証にPre-Shared Keyを使用

動作例に使用するシナリオ

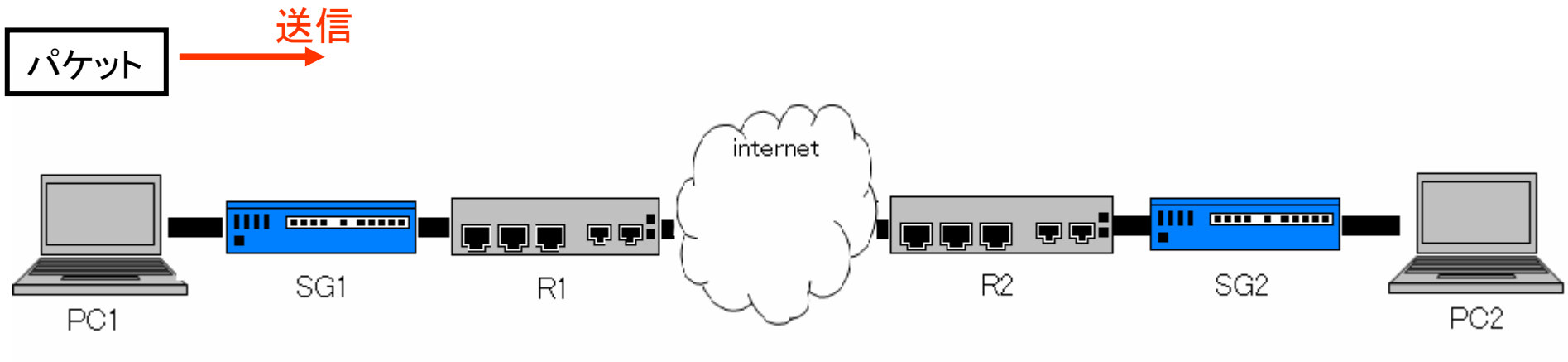
- PC1とPC2の2台のPCがそれぞれ別のネットワークに所属
- それぞれSG1とSG2というセキュリティゲートウェイを介してIPsec通信を行う



PC1からの通信

動作説明

- PC1からPC2にpingを打つ
- PC1はPC2向けのパケットをSG1に送信

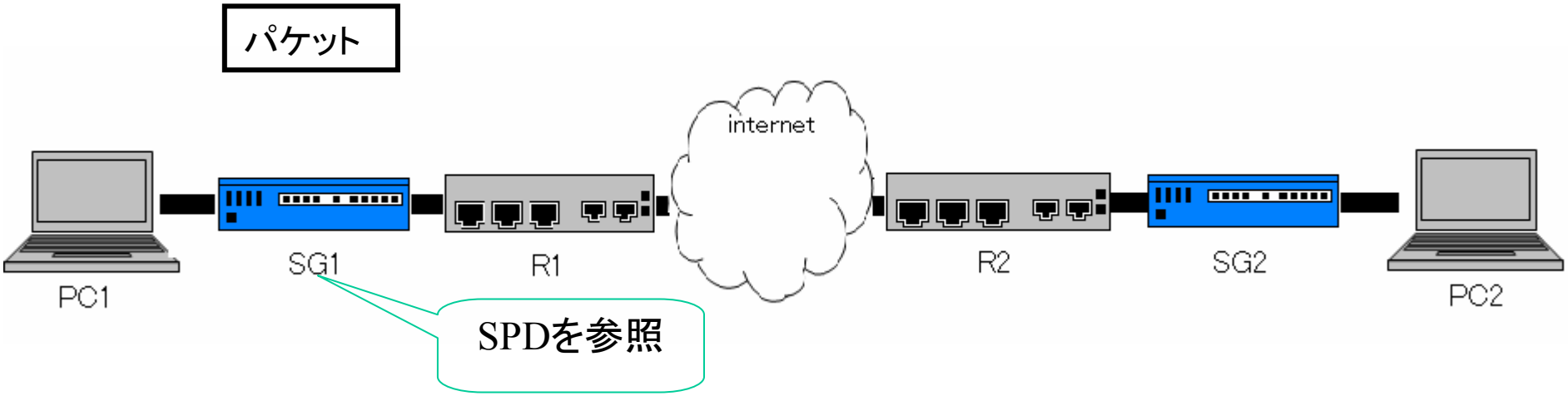


SG1におけるIPsec化の判断

動作説明

•SG1はPC1からパケットを受信

•SG1に設定されたSPDを参照する．このシナリオでは「PC1からPC2間のパケットはSG2を宛先とするトンネルモードのESPによりIPsec化、暗号化アルゴリズムは3DESを使用」というセキュリティポリシーが設定されているとする．このためSG1はセキュリティポリシーにしたがい、このパケットをIPsec化する．

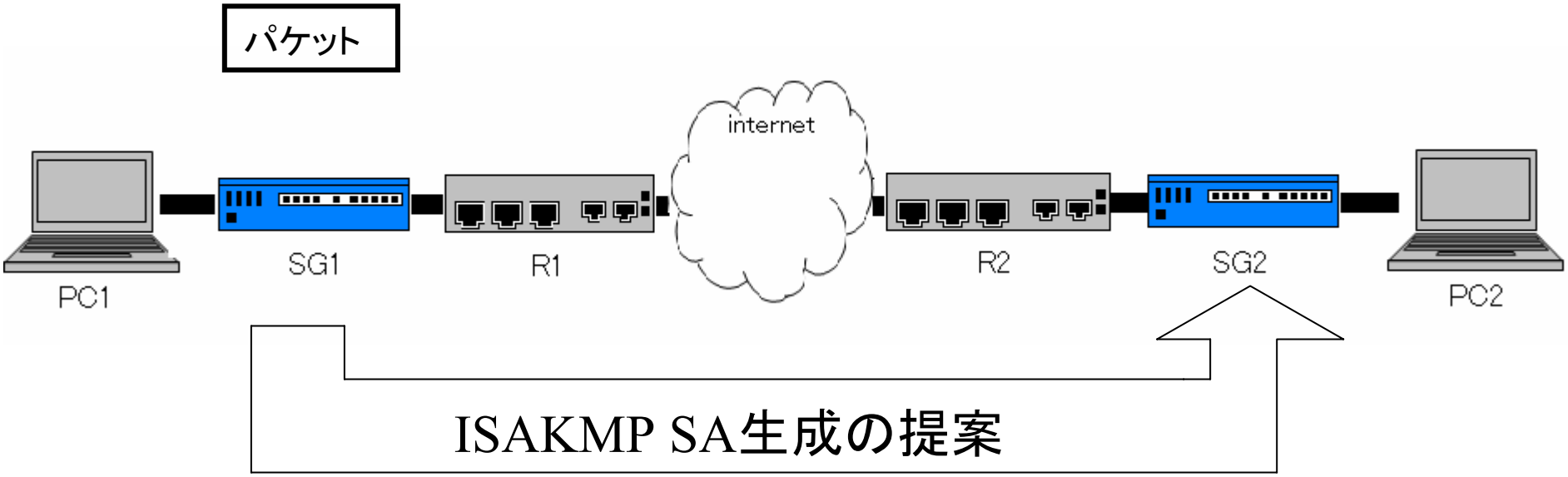


ISAKMP SA属性のネゴシエーション

動作説明

•SG1はISAKMPの生成を要求するパケットを，SG2に送信

※ISAKMPとはIKEを使用してSAを自動的に生成する場合にIKE自身が制御信号をやりとりするために使用するIKEの制御用チャネルのこと．またこのようなSA生成の要求を、Proposalと呼ぶ．

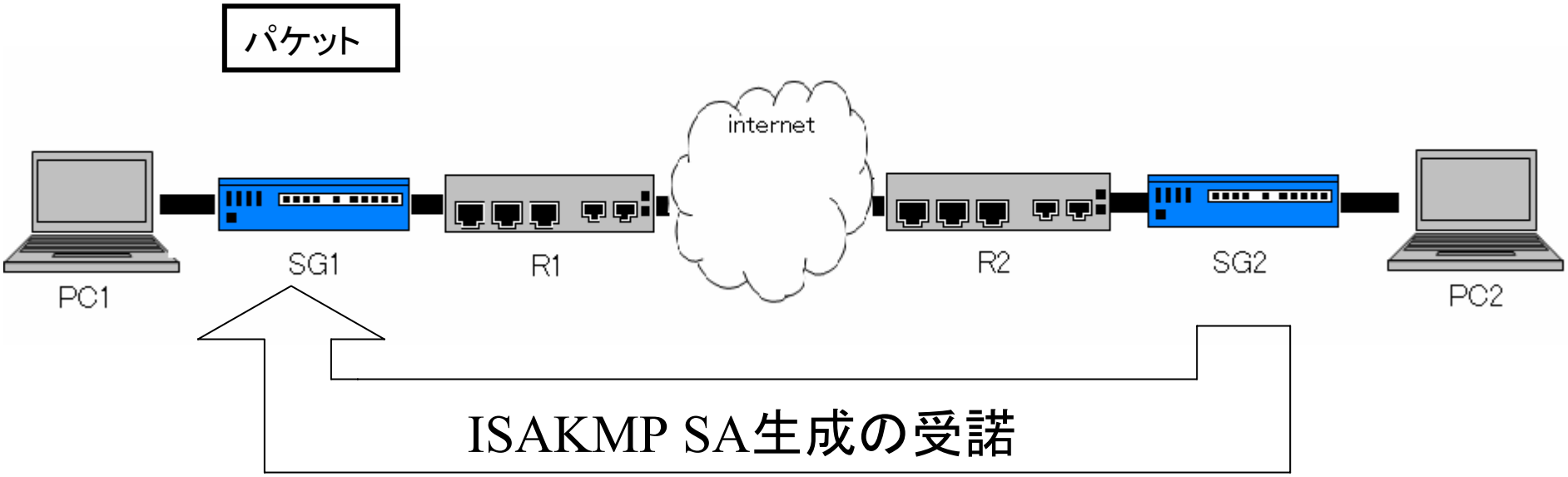


ISAKMP SA属性のネゴシエーション(続き)

動作説明

•SG2はSG1からIKEの最初のパケットとなるProposalを受信

•SG2は事前に設定してあるセキュリティポリシーからこのProposalを受諾するか判断する. セキュリティポリシーにしたがいSG2はSG1からのISAKMP SA生成のProposalを受諾し、受諾通知をSG1へ送信する.



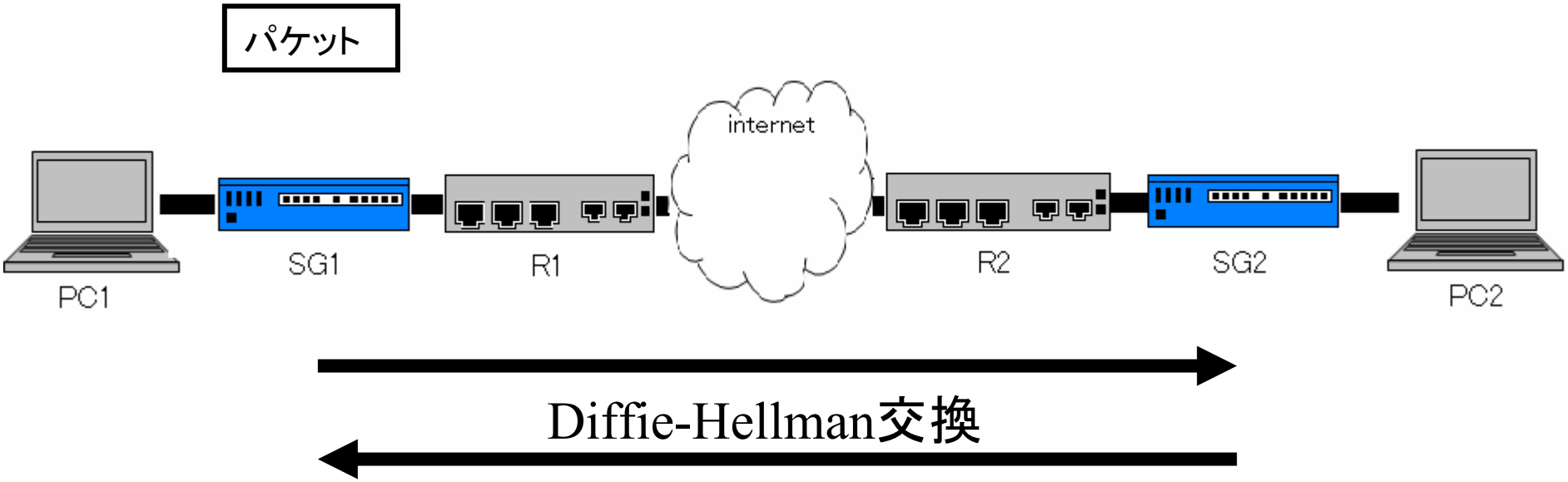
秘密対称鍵の自動生成

動作説明

•SG1はある規則に則って乱数を発生し，SG2へ乱数を送信

•SG2も同様の規則に則って乱数を発生し，SG1へ乱数を送信

•SG1とSG2は自身が送信した乱数と相手から受信した乱数を組み合わせ，公開鍵暗号技術により秘密対称鍵を生成

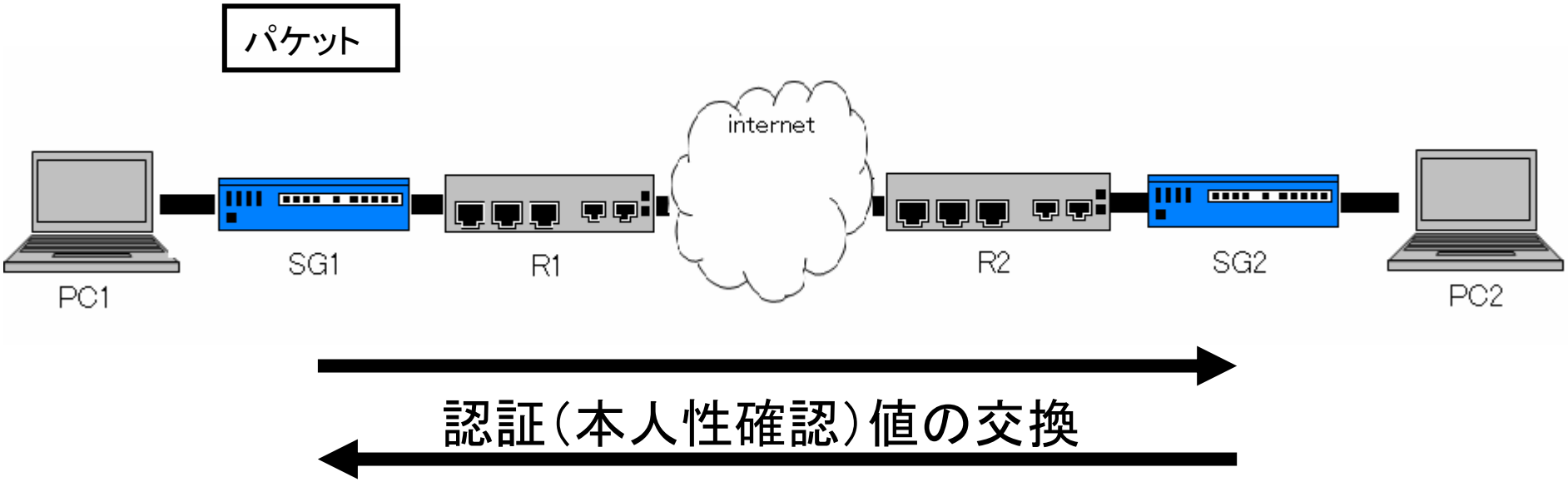


IKE相手が本物かどうかの確認

動作説明

•管理者が事前に設定しておいた秘密のパスワードを確認するためSG1とSG2はパスワードとそのほかの情報から作った認証値であるハッシュ値を交換

=>相互認証後，制御用チャネルであるISAKMP SAが確立

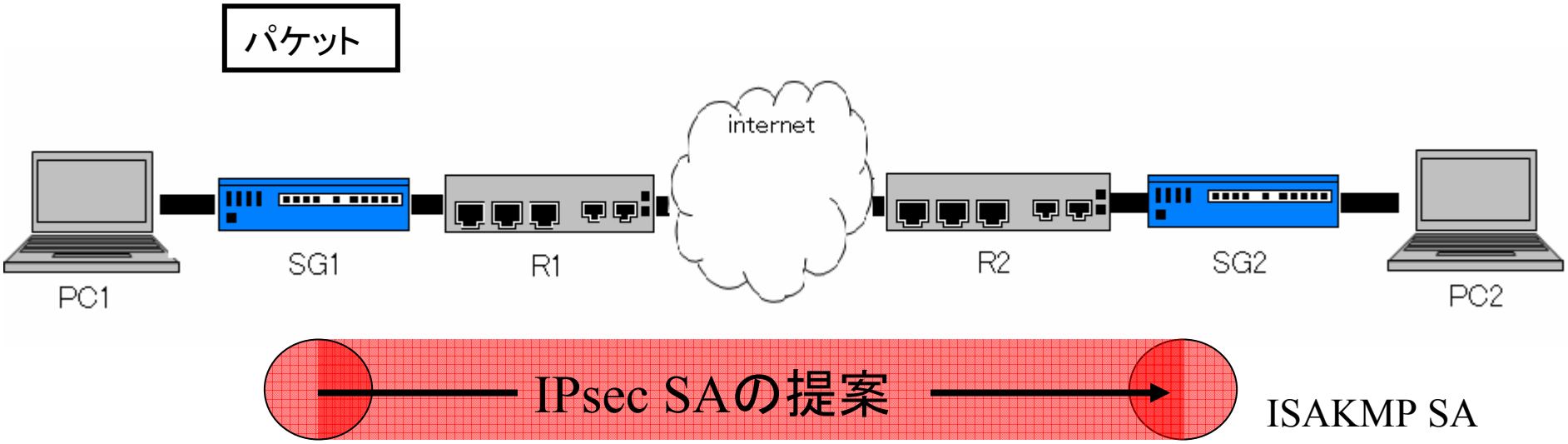


PC1からPC2へのパケットを転送するIPsec SAの提案

動作説明

•SG1は，PC1からのパケットをIPsec化するためのSA(IPsec SA)のProposalをSG2へ送信．同時に，暗号化に使用する鍵を作るための乱数も送る．

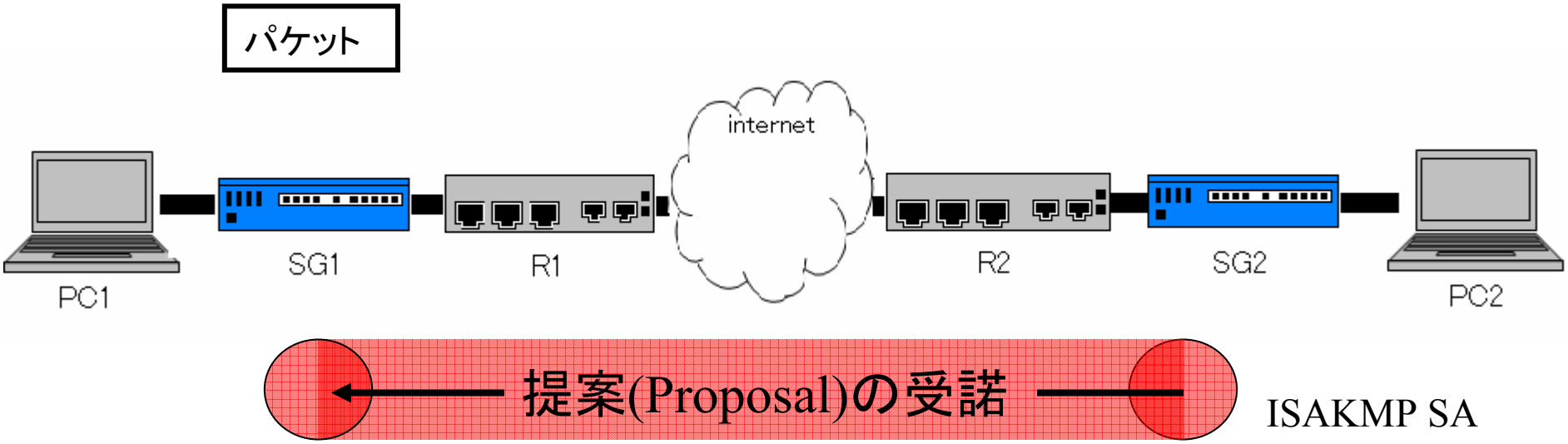
※この動作はすでに作られたISAKMP SAを通して送られるので暗号化してやりとりされる．



PC1からPC2へのパケットを転送するIPsec SAの提案

動作説明

- Proposalを受信したSG2はセキュリティポリシーを照会してProposalを受諾
- 受諾したProposalと暗号化に使用する鍵を作るための乱数などをSG1に返信



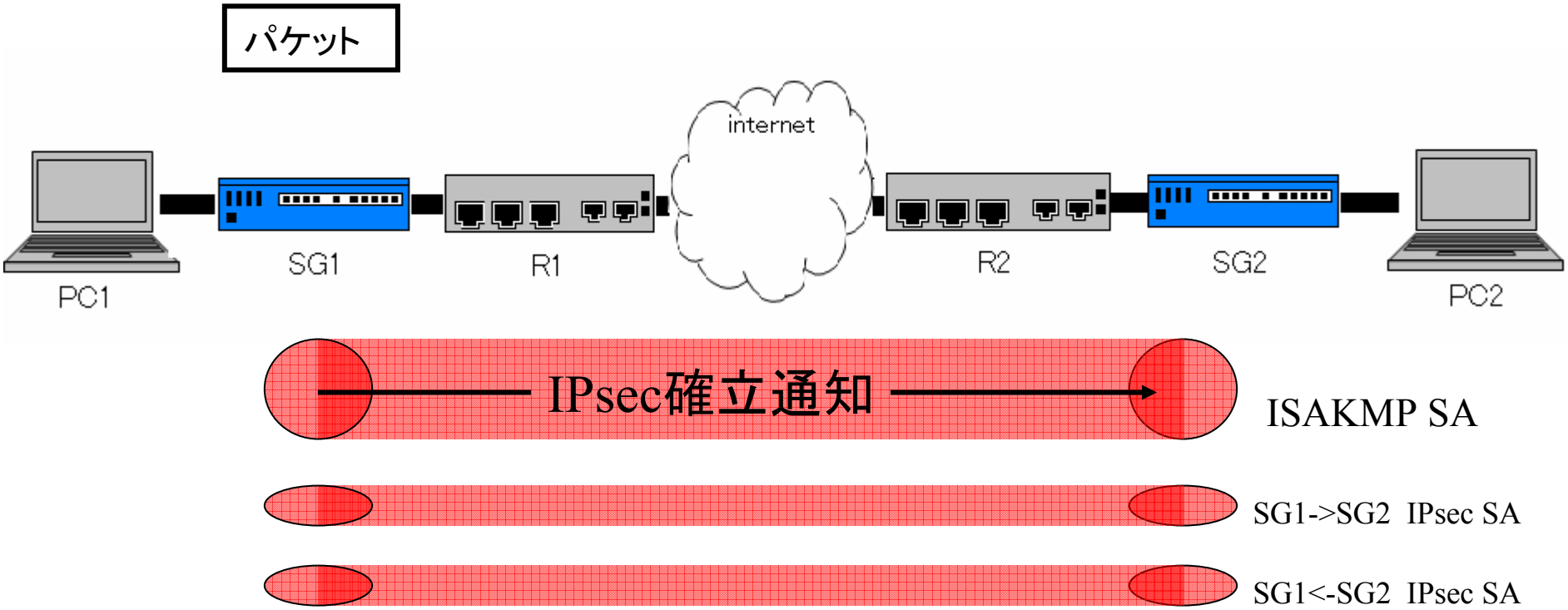
IPsec SA確立の通知

動作説明

•SG2からProposal受諾の通知を受け取ったSG1はIPsec SA を確立

•SG2へSAを確立を通知するメッセージを送信

=>制御用チャネルであるISAKMP SAと実際にユーザデータを暗号化してやりとりする
1ペア(2本)のIPsec SA が生成

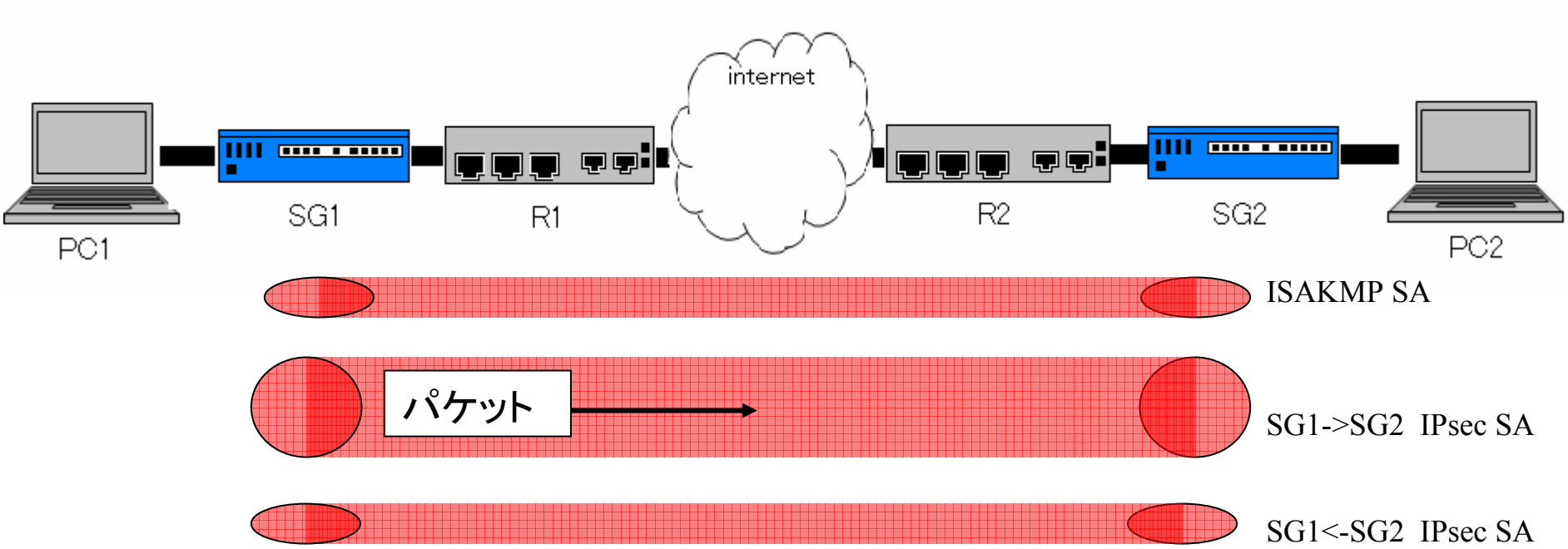


PC1からPC2へのパケットのIPsec化

動作説明

•PC1からのPingパケットをSG1は、SG1からSG2向きのIPsec SAにESP化して送信

•パケットを受信したSG2はSAのパラメータと秘密対称鍵を使用して，パケットの復号化を行いPC2へ転送



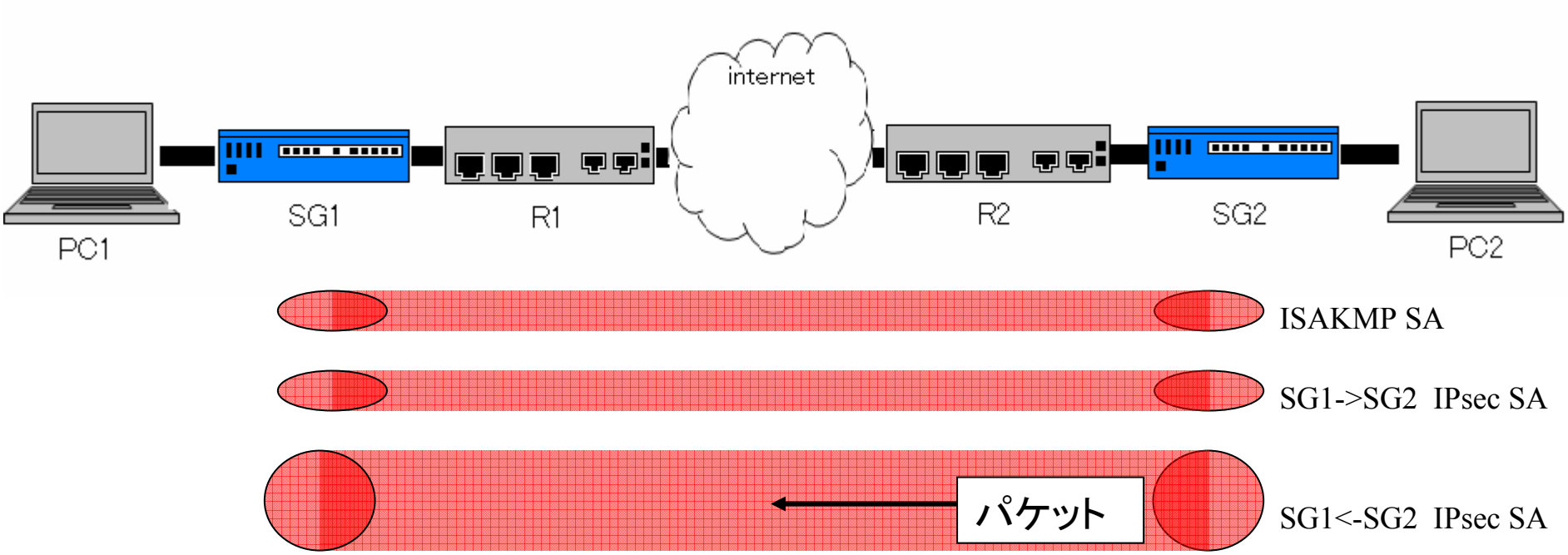
PC2からPC1へのパケットのIPsec化

動作説明

•PC2からPC1への返信を受け取ったSG2は，SG2からSG1向けのIPsec SAでこのパケットをESP化しSG1に向けて送信

このパケットを受信したSG1は復号化を行いPC1に転送

⇒ PC1はPC2からPingの返答を受信



第四章　IPsecの拡張

1. リモートアクセス
2. NAT透過拡張

以上2つのIPsecの拡張について説明

1.リモートアクセス

- IKEはリモートアクセスを想定して設計されていないため、出張先や自宅からインターネット経由で会社のVPNに接続することができない
- リモートアクセスへの妨げ
  - ユーザ認証ができない（IKEはデバイス認証）
  - VPNで使用するIPアドレスなどを動的に割り当てることができない

リモートアクセスを可能にする機能
-XAUTHとISAKMP Configuration Method-

- XAUTH
  - ユーザ名とパスワードによる認証を行うプロトコル
  - Phase1完了後にXAUTHによるユーザ認証を行う
- ISAKMP Configuration Method（モードコンフィグ）
  - ISAKMPパケットを使用してネットワーク情報を交換するための方法
  - VPN内のアドレスをノードへ動的に割り当てることが可能

⇒XAUTHとモードコンフィグを使用することでリモートアクセスが可能

2.NAT透過拡張

- NATを介してIKEは使用不可能

＜原因＞

- NATは通信を識別するためにポート番号を書き換える
  - ISAKMPパケットによるIKEは送信元、宛先ポート番号とも500番のUDPと決まっている。またIPsec化されたパケットはIPヘッダの直後にAHやESPヘッダが来るため変化させるべきポート番号が存在しない。

＜解決案＞

NATによって変化してもかまわないダミーのUDPヘッダを付加することによりNAT透過を実現

おわり