本資料について

- 本資料は下記論文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．

- 著者：小早川　知明
- 論文名：IPsec徹底入門
- 発表日：2002年8月6日

IPsec徹底入門

発表者

渡邊研究室　030432017　今村　圭佑

目次

- 第一章　IPsecアーキテクチャ
- 第二章　IPsec Security Association
- 第三章　IKE (Internet Key Exchange)

第一章　IPsecアーキテクチャ

1.1 インターネットと攻撃方法

- インターネットが普及
  - セキュリティ技術が必要
- 攻撃方法
  - 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

1.2 必要なセキュリティ機能

1. 秘密性
   - 盗聴やトラフィック解析からの保護
2. 認証（本人性確認）
   - メッセージが表示された送信元からであることを保障
   - 通信の際に相手が意図した人物であることを保障
3. 認証（完全性保障）
   - メッセージが改ざんされていないことを保障

1.2 必要なセキュリティ機能

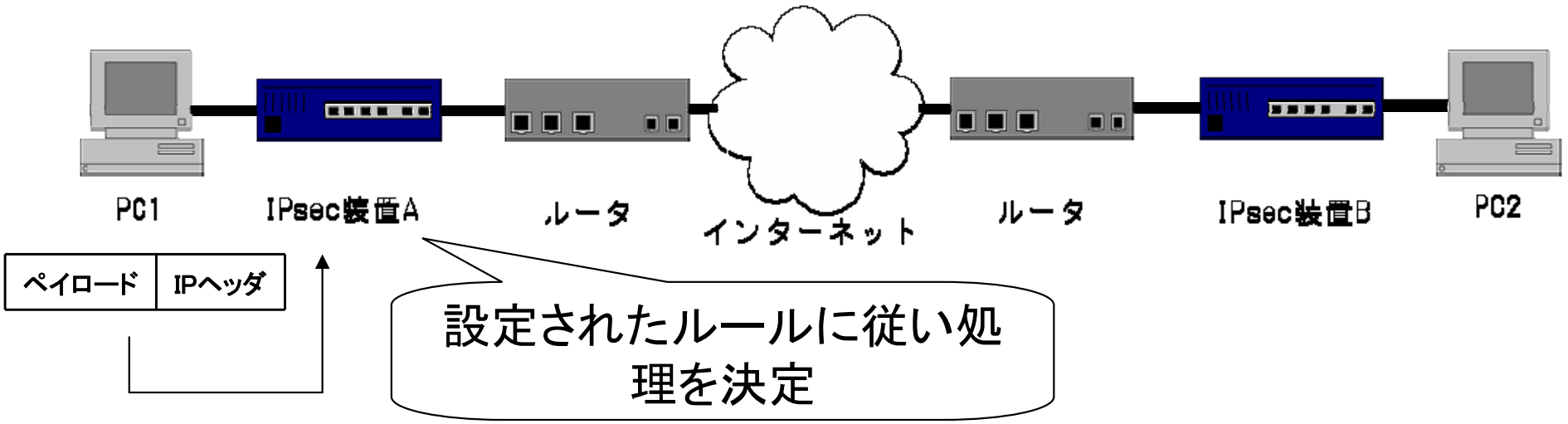
4. 認否不能性
   - 送信者がメッセージを送信したことや、受信者がメッセージを受信したことを証明
5. アクセス制御
   - 通信を行う相手やプロトコルなどによって、通信の通過／遮断を制御する機能
6. 可用性
   - システムが常に使用できること

1.3 IPsecとは

- IPパケットを完全に運ぶための技術

- IPsecの利点
  - 仕様が公開されており、専門家による厳しい検証に耐えてきた技術で、極めて安全
  - VPN拠点それぞれにIPsec装置があればよく、インターネットをそのまま使用できる
  - IP通信にセキュリティ機能が提供されるため、アプリケーションに変更を加えることなく使用できる
  - 標準化されているIPレイヤでのセキュリティ実現機能
- IPsecの欠点
  - プロトコルが複雑で理解しにくい
  - 異なるベンダのIPsec装置間で完全な相互接続性が実現されていない

1.4 IPsec動作イメージ

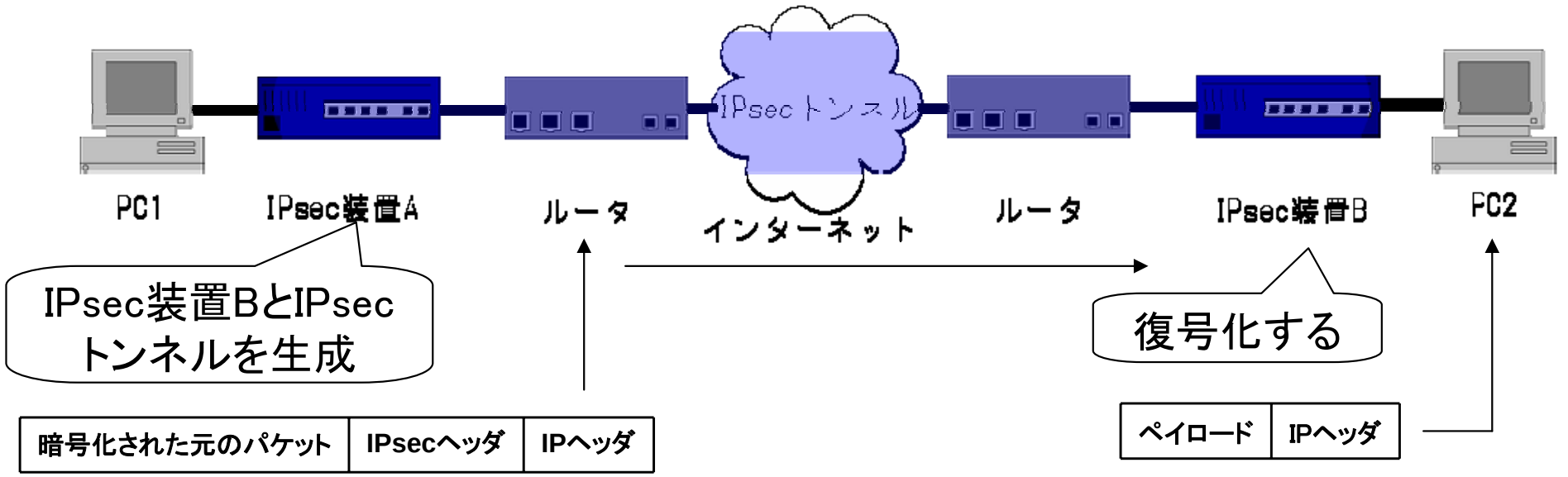


1、PC1はPC2向けのパケットをIPsec装置Aに送信

2、IPsec装置Aに設定されたルールに従い、パケットをどのように処理するか決定

3、IPsec装置Aは、IPsec装置BとIPsecトンネルが確立されているか調べ、IPsecトンネルがなければ生成し、あればそのトンネルを使用する

1.4 IPsec動作イメージ



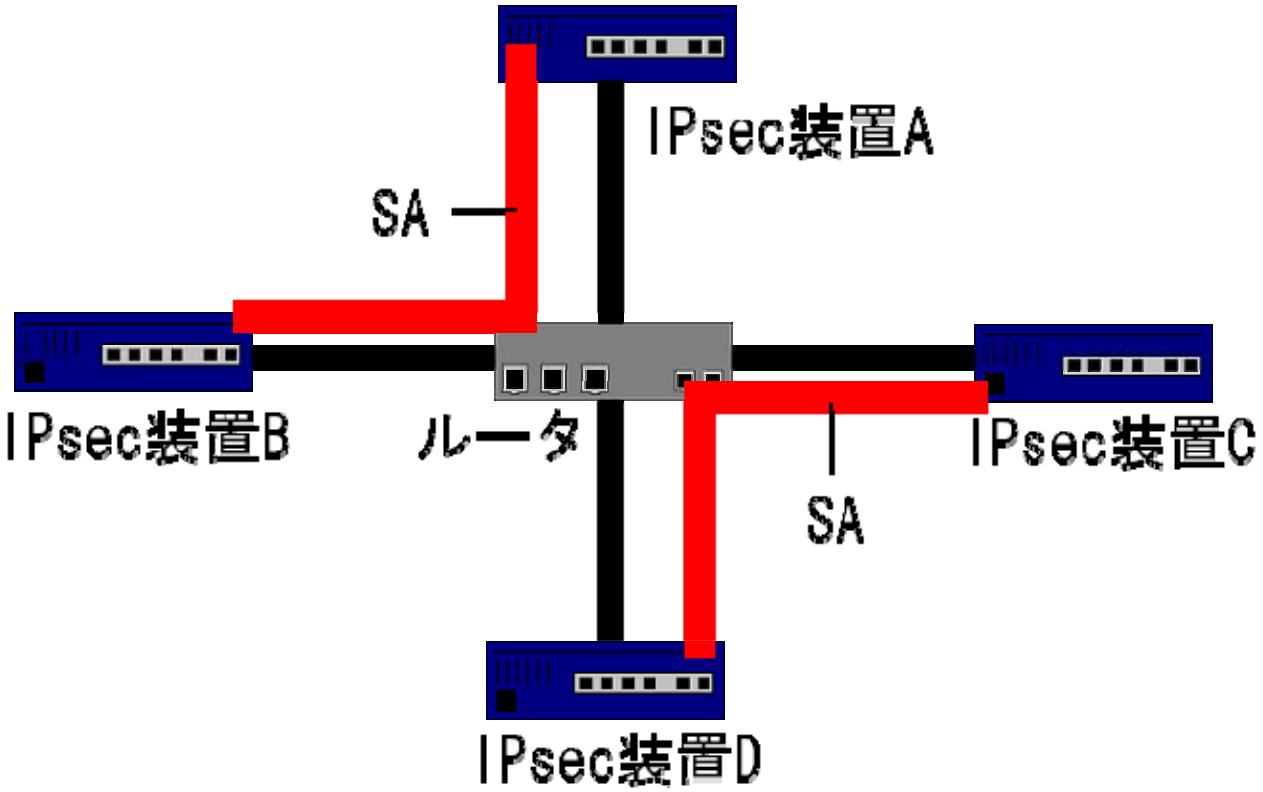
4、IPsec装置Aは、IPsecトンネルを使用しパケットを転送

5、インターネット上の中継ルータは通常のIPパケットとして
ルーティングする。

6、IPsec装置Bはパケットを受信し、パケット復号化後
元のパケットを取り出してPC2に転送する。

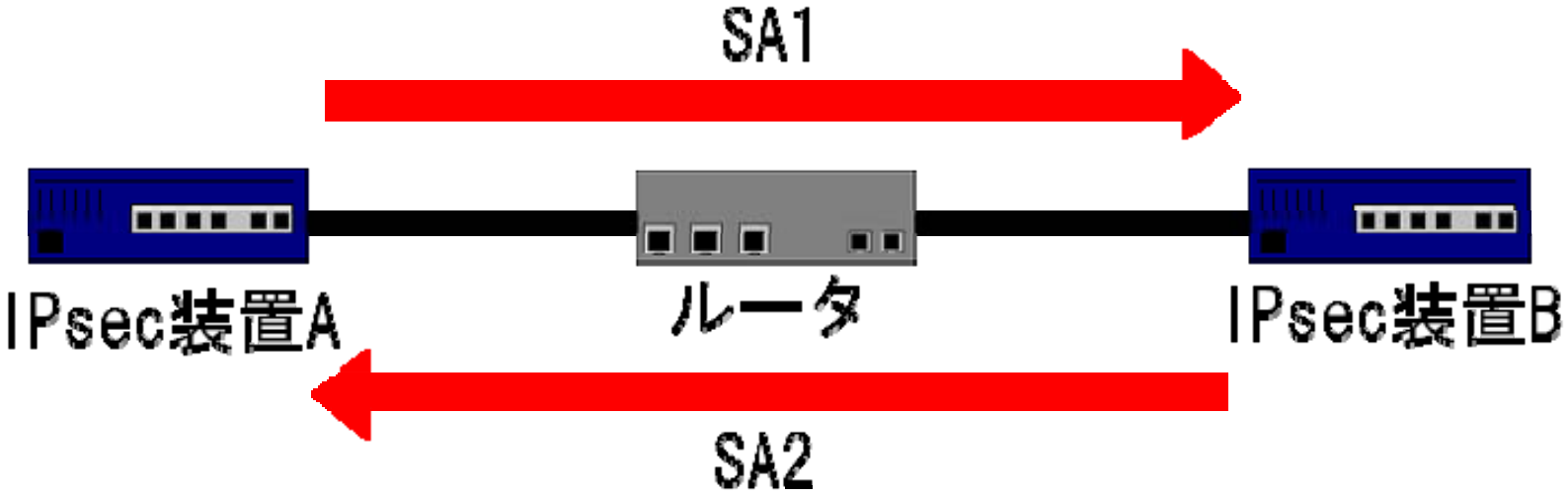
1.5 SAとは

- SA (Security Association)
  - IPsec装置間で生成される
  - 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



1.5 SAとは

- SAのディレクション
  - SAはユニディレクション(一方通行)のコネクション
  - 双方向の通信のためには、行きと帰りの2本のSAが必要



- 暗号化や認証アルゴリズム、使用する鍵などは、IPsecごとに独立

1.6 セキュリティプロトコル

- SAには種類があり、ESPとAHなどがある
- ESP (Encapsulating Security Payload)
  - パケット暗号化機能
- AH (Authentication Header)
  - パケットの改ざん検知機能

1.6 セキュリティプロトコル

- ESPの提供するセキュリティ機能
  - 秘密性：元のパケットを暗号化
  - 認証（本人性確認）：限定的な範囲で保障
  - 認証（完全性保障）：パケットの改ざんがないことを保障
  - アクセス制御：パケットのフィルタリングが可能
- AHの提供するセキュリティ機能
  - 秘密性：提供されない(盗聴者は中身を見ることが可能)
  - 認証（本人性確認）：本人であることを保障
  - 認証（完全性保障）：パケットの改ざんがないことを保障
  - アクセス制御：パケットのフィルタリングが可能

ESPはAHに比べ秘密性が高いが、本人性確認機能が弱い
AHは、強力な認証機能を備えているが、秘密性が弱い

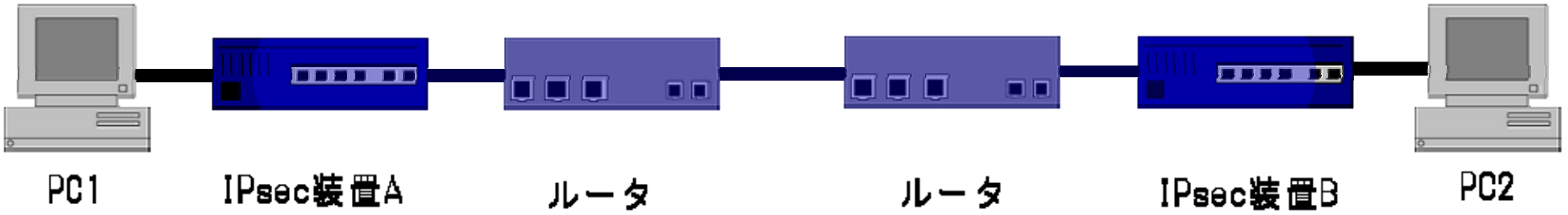
1.7 トンネルモードとトランスポートモード

- トンネルモード
  - 通信の内容ばかりか存在そのものを秘密にする
- トランスポートモード
  - 通信の内容を秘密にする

1.7 トンネルモードとトランスポートモード

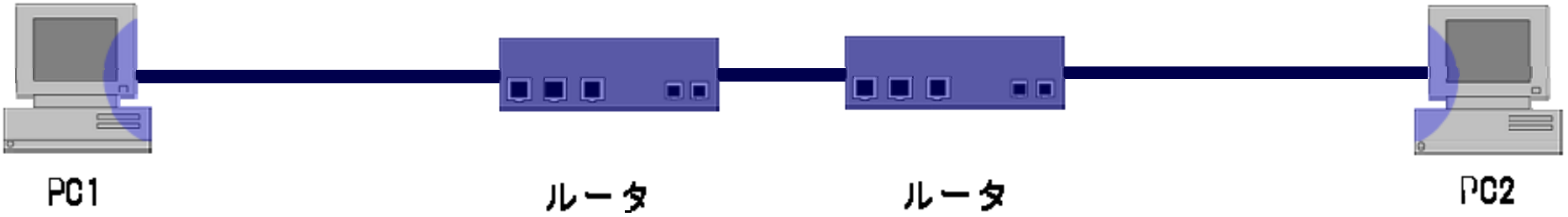
トンネルモードSA

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



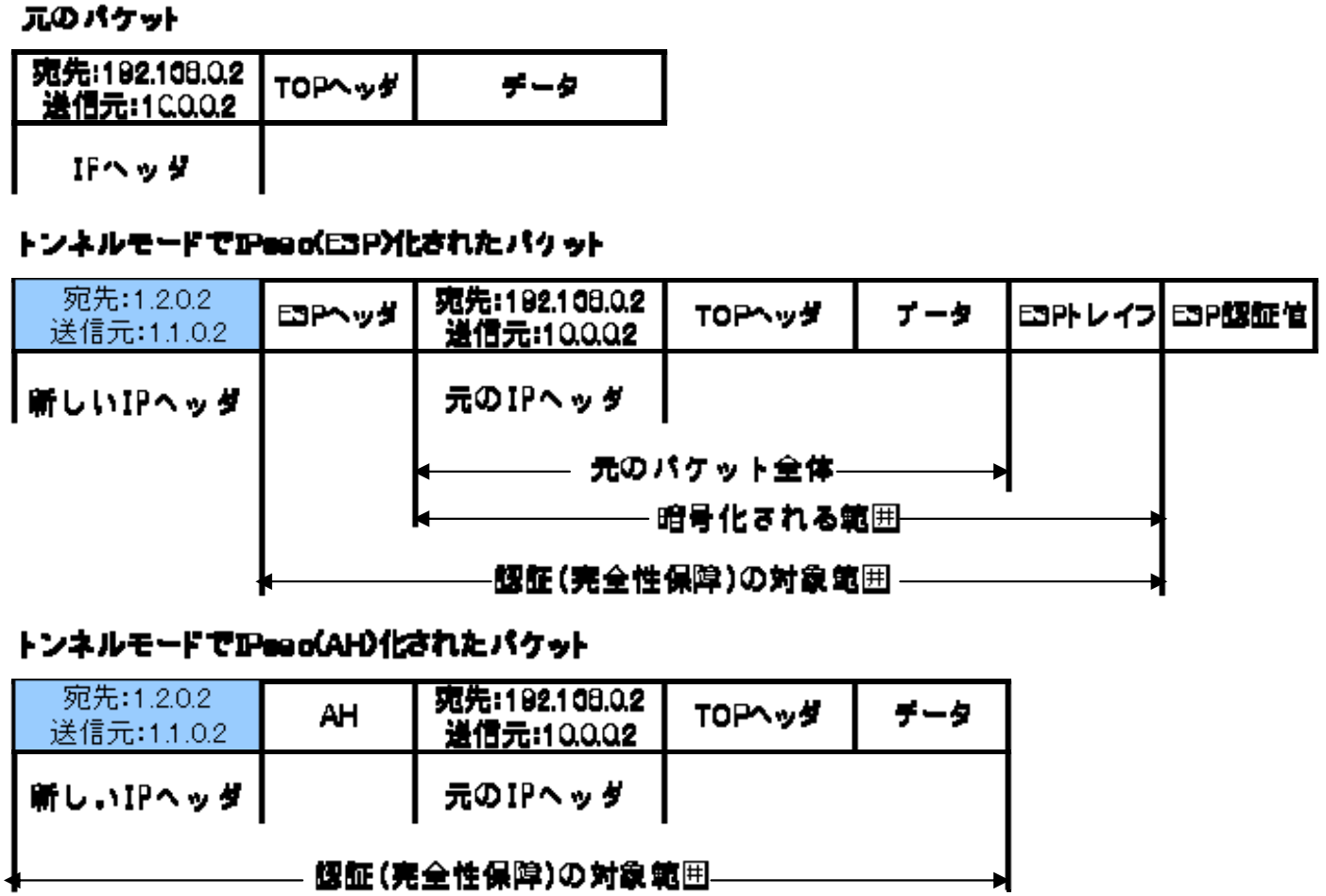
トランスポートモードSA

エンド・ツー・エンドで認証や暗号化を行う場合に使用



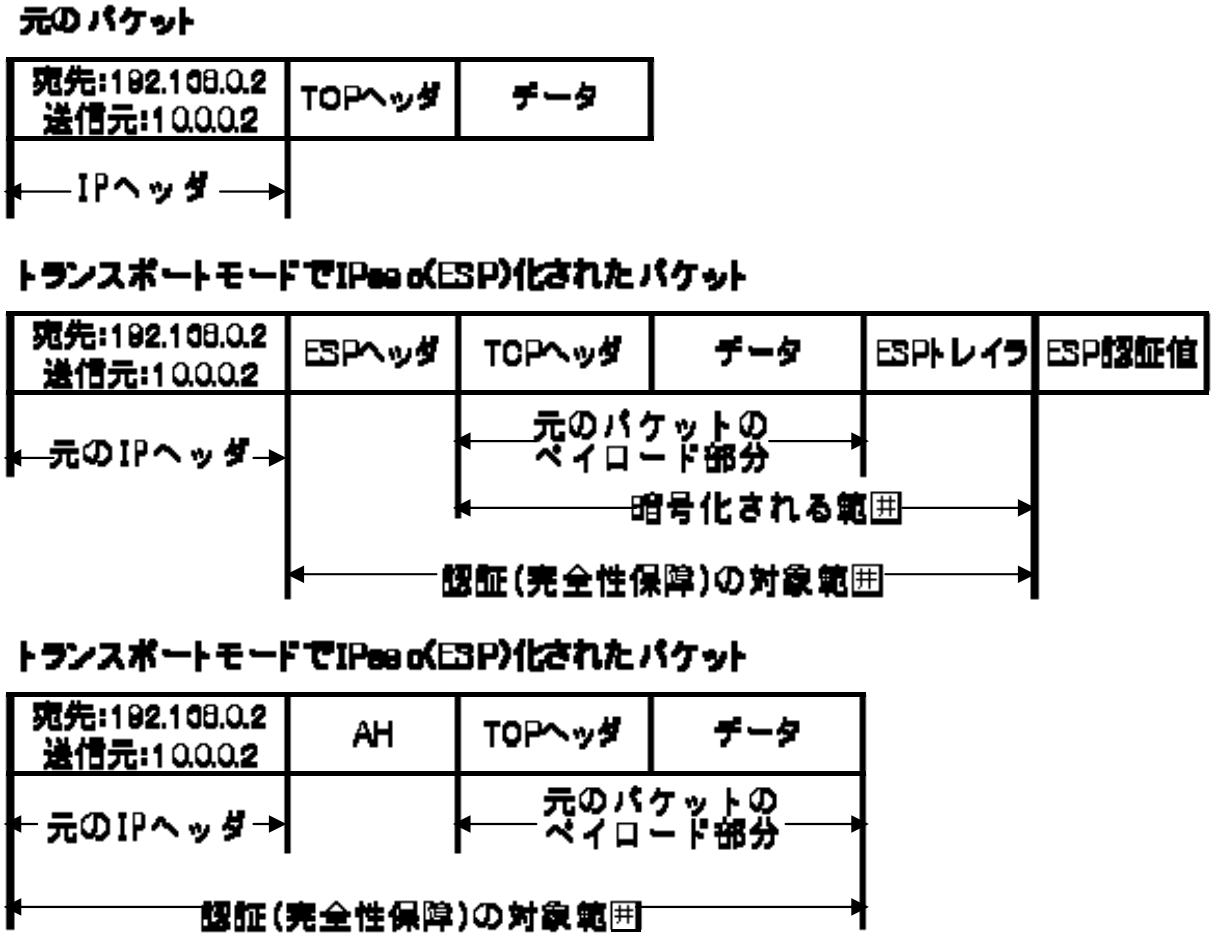
1.7 トンネルモードとトランスポートモード

- トンネルモードのパケット
  - 元のパケットをIPヘッダから丸ごと暗号化する



1.7 トンネルモードとトランスポートモード

- トランスポートモードのパケット
  - 元のIPヘッダをそのまま転送用IPヘッダとして使用し、元のパケットのペイロード部分だけを暗号化



第二章　IPsec Security Association

2.1 SAの属性

- 基本的なSAの属性
  - セキュリティプロトコル
    - SAがESPで処理されるか、AHで処理されるか
  - 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か
  - SPI (Security Parameters Index)
    - SAを識別するための識別子
  - 暗号化や認証(完全性保障)アルゴリズム
    - どのような暗号化アルゴリズムを使用するか
  - セレクタ
    - SA毎にどのようなパケットを流すべきか

2.2 暗号化アルゴリズム

- IPsecで使用する暗号化アルゴリズムや認証アルゴリズムはSAごとに選択可能
  - ブロック暗号
  - CBCモード
- 暗号化アルゴリズムは公開暗号ではなく、同じ秘密鍵を共有する対象暗号である
- DESや3DESが多くの製品で実装されよく使用されている

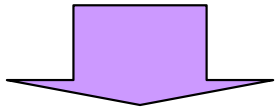
2.3 認証アルゴリズム

- 認証の種類
  - 完全性保障：パケットが通信経路上で改ざんされていないかを保障
  - 本人性確認：通信相手が本物であるかどうかの認証
- 一方向性ハッシュ関数と呼ばれる手法でチェックサムなどを用い、確認する
  - MD5
  - SHA-1
  - HMAC

2.4 セレクタ

- IPパケットがIPsec化されるルール

- 異なるセキュリティ機能を持つSAが複数ある場合
  - セキュリティポリシー
    - TCPパケットは通す
    - UDPパケットは通す
    - 上記のパケット以外と通さない

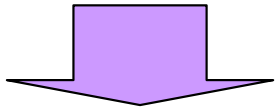


IPsecではこれらを詳細に規定

第三章　IKE (Internet Key Exchange)

3.1 IKE概要

- IKE（Internet Key Exchange）
  - SA自動生成
    - IPsec通信が必要になると、IKEがオンデマンドでSAを生成し、IPsec通信が可能になる
  - 管理プロトコル
    - SAが生成されてからの期間や使用状況を監視し、秘密対称鍵を自動生成する



IKEは、運用、セキュリティの両面からみて、IPsecには必須

3.1 IKE概要

- 3つの基本機能
  - Proposal交換
    - 生成するSAのパラメータをネゴシエートして決定する機能
  - Diffie-Hellman交換
    - 生成するSAの秘密対称鍵を、公開暗号技術により安全に自動生成する機能
  - IKE相手の認証(本人性確認)
    - IKE通信している相手が本物であることを確認する機能

3.2 IKEの基本機能

- Proposal交換
  - SAの提案
  - Proposalの選択
- Proposal交換で決定されるパラメータ
  - ネゴシエートされるパラメータ
    - 暗号化アルゴリズム
    - ハッシュアルゴリズム
    - 認証（本人性確認）方式
    - Diffie-Hellman交換に使用するパラメータ
    - SAのLife TypeとLife duration

3.2 IKEの基本機能

- 暗号化アルゴリズム
  - ISAKMP SAを暗号化するために使用する暗号化アルゴリズム
  - 3DES-CBCやDES-CBCなどから1つ指定
- ハッシュアルゴリズム
  - 各種認証に使用するハッシュアルゴリズム
  - SHA-1やMD5などから1つ指定
- 認証（本人性確認）方式
  - IKE通信相手の認証方式
  - Pre-Shared Key認証、デジタル署名認証など

3.2 IKEの基本機能

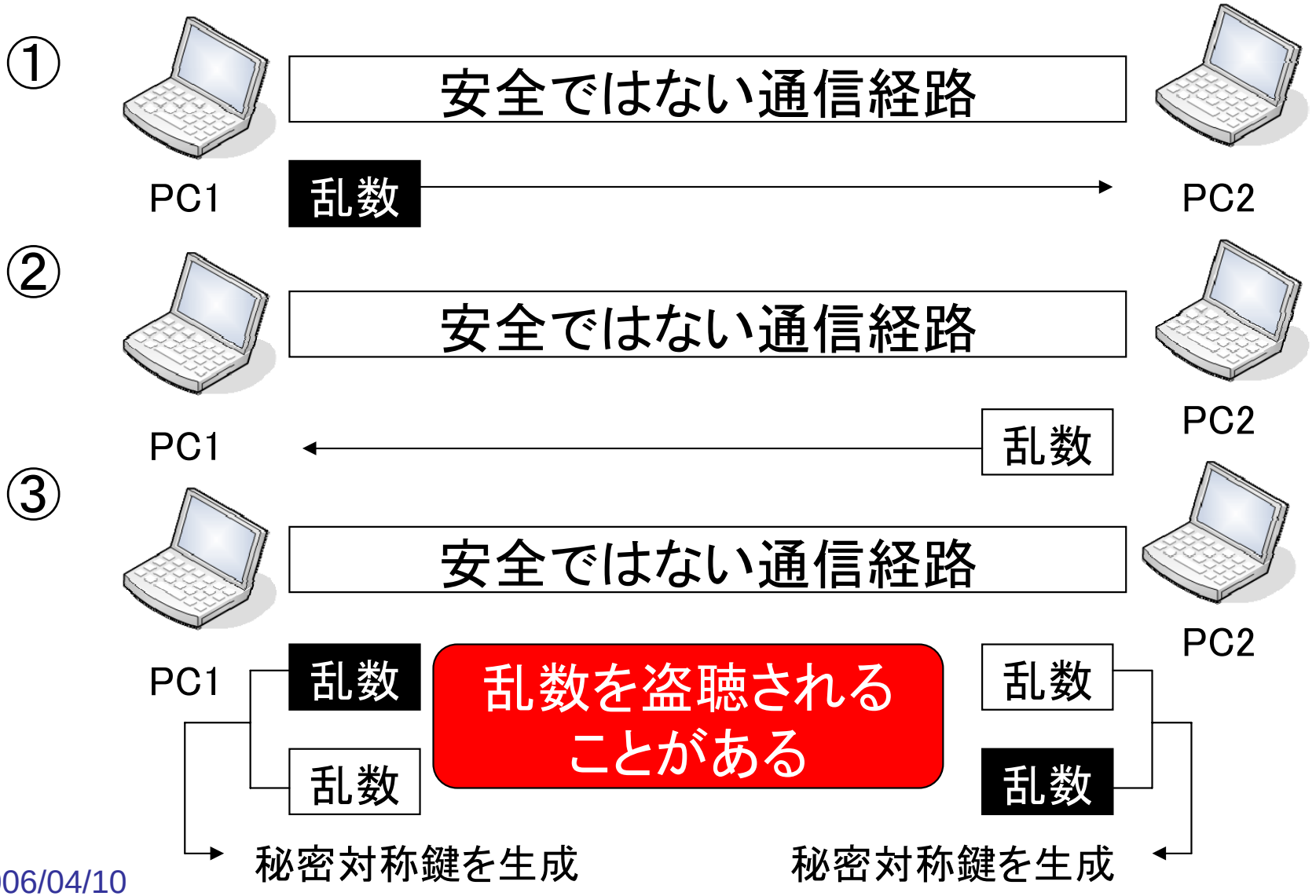
- Diffie-Hellman交換に使用するパラメータ
  - Diffie-Hellman交換をする前に、条件を決めておく必要がある
  - DHグループ1、2、5などから選択
- SAのLife TypeとLife duration
  - ISAKMP SAの有効期限と想定方法を指定

3.2 IKEの基本機能

- Diffie-Hellman交換
  - お互いが乱数を交換することで、安全でない通信経路を使用するにもかかわらずまったく同一の秘密の鍵を共有出来る

3.2 IKEの基本機能

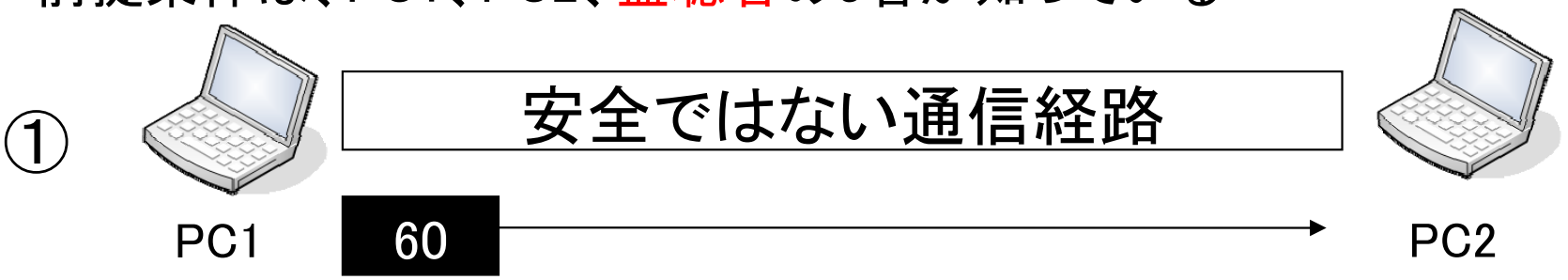
Diffie-Hellman交換



3.2 IKEの基本機能

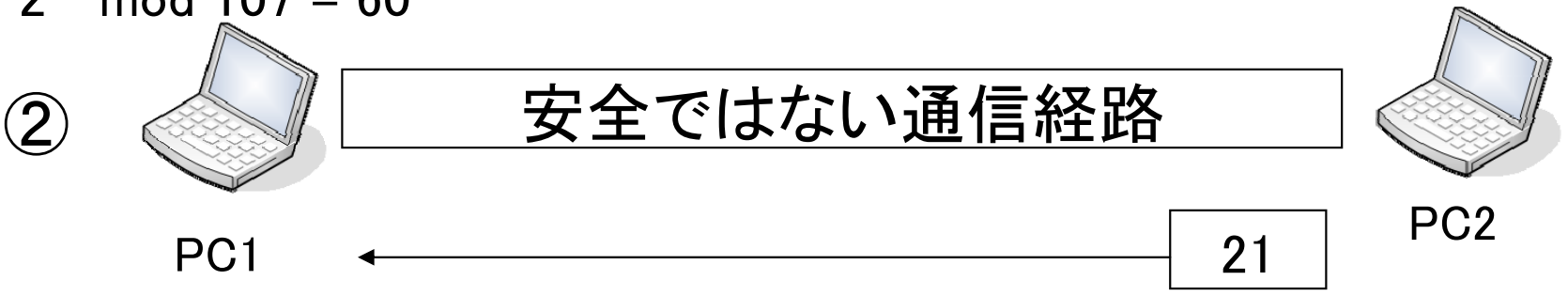
Diffie-Hellman交換の例

事前に2と107という数字はDiffie-Hellman交換の前提条件として使用する
前提条件は、PC1、PC2、盗聴者の3者が知っている



PC1は乱数を作成：13

$2^{13} \bmod 107 = 60$



PC2は乱数を作成：7

$2^{7} \bmod 107 = 21$

3.2 IKEの基本機能

PC1

PC2

PC1はPC2から送られてきた21
と自分で作った乱数13を使用

$21^{13} \bmod 107 = 70$

PC2はPC1から送られてきた60
と自分で作った乱数7を使用

$60^{7} \bmod 107 = 70$

2つの値は一致し、70という数字を共有することが出来る

盗聴者は、前提条件の2と107、また盗聴した21、60を知っている
70を求めるには・・・

$21^{X} \bmod 107 = 2^{XY} \bmod 107 = 60^{Y} \bmod 107$

安全でない通信経路を使用しても秘密対称鍵が共有可能

3.2 IKEの基本機能

- IPsec通信相手の認証（本人性確認）
  - Pre-Shared Key認証
  - 公開鍵暗号認証および改良型公開鍵暗号認証
  - デジタル署名認証
- Pre-Shared Key認証
  - パスワード認証方式
  - IKE通信でパスワードを相互に確認して認証する

3.3 ISAKMP

- ISAKMP (Internet Security Association and Key Management Protocol)
- ISAKMPパケット
  - ISAKMPペイロードにはいろいろな種類がある
  - 目的に応じて使用する

3.4 ISAKMPペイロード

- ISAKMPペイロード
  - Security Associationペイロード
  - Proposalペイロード
  - Transfrom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ペイロード

3.5 交換タイプ

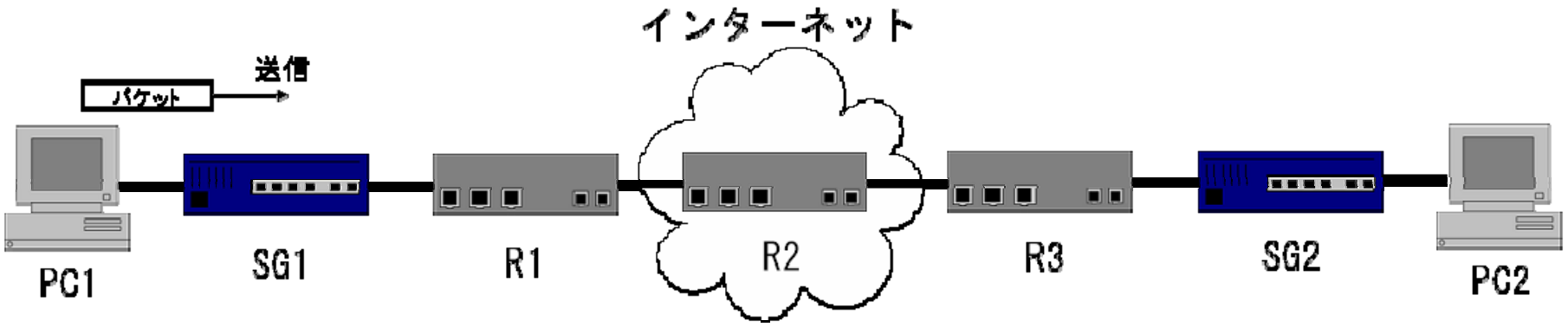
- Main Mode
  - ISAKMP SAの確立のために使用
- Aggressive Mode
  - ISAKMP SAをMain Modeより簡単に確立
- Quick Mode
  - IPsec SAを生成するために使用

3.6 具体的なIKEの動作

PC1からの通信

PC1はPC2にpingを打つ

PC1はPC2向けのパケットをSG1に送信する



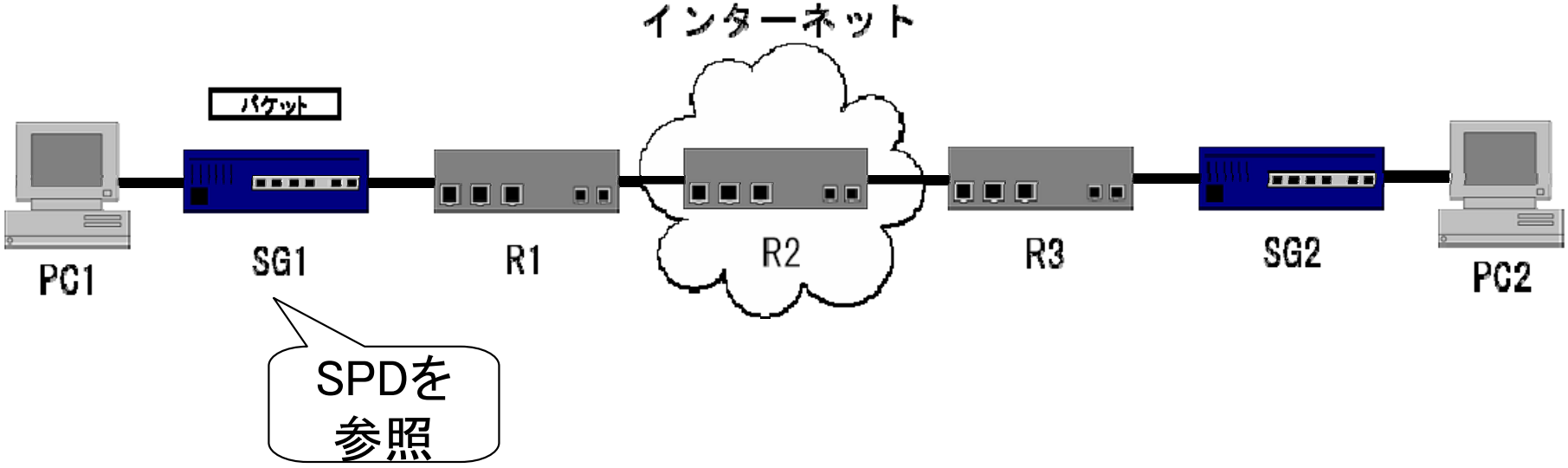
SG：セキュリティゲートウェイ

R：ルータ

3.6 具体的なIKEの動作

SG1におけるIPsec化の判断

SG1はPC1からのパケットを受信
SG1に設定されたセキュリティポリシー(SPD)を参照し、
このパケットをどのように処理するか判断する
今回は、SG1に「PC1と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化する」というセキュリティ
ポリシーに従い、このパケットをIPsec化する



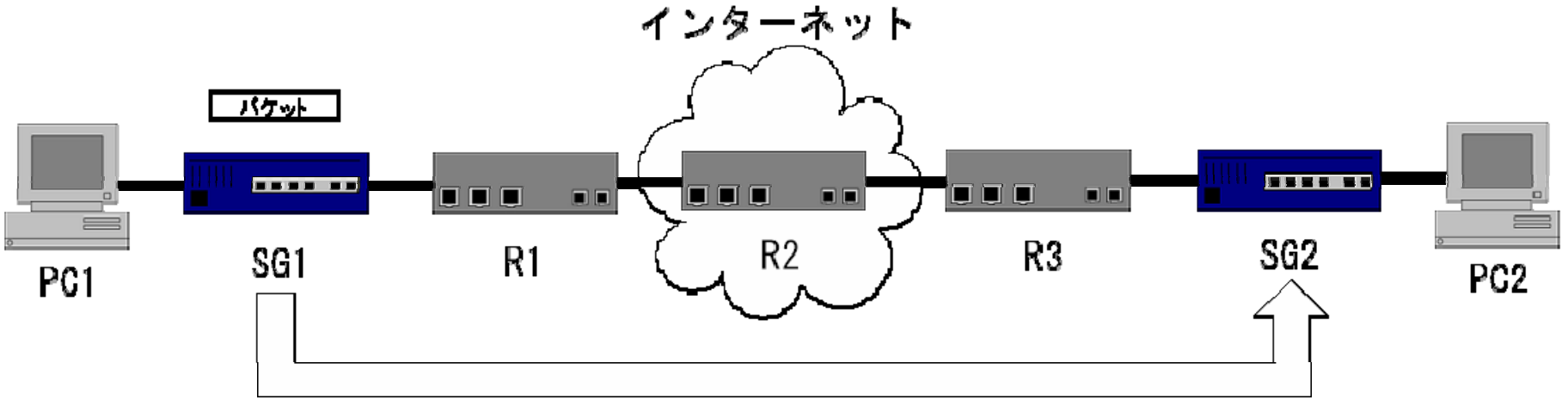
3.6 具体的なIKEの動作

ISAKMP SA属性のネゴシエーション

SPDの設定通りにSG1は、IKEのやりとりをSG2と開始する

ISAKMP SAの生成を要求するパケットを、SG2に送信

ISAKMP SAとは、IKEを使用してSAを自動生成する場合に、IKE自身が制御信号をやりとりするために使用する制御チャンネル

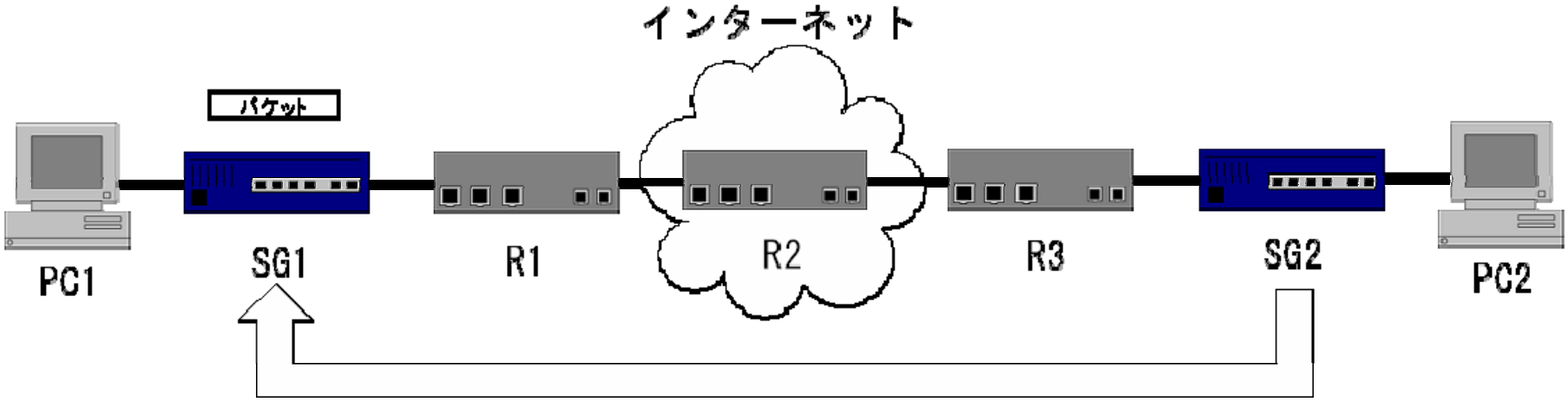


ISAKMP SA生成の提案

3.6 具体的なIKEの動作

ISAKMP SA属性のネゴシエーション

SG2はSG1からIKEの最初の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を受諾してよいか判断する
SG2はセキュリティポリシーにしたがって、ISAKMP SA生成のProposalを受託し、受託通知をSG1に送る

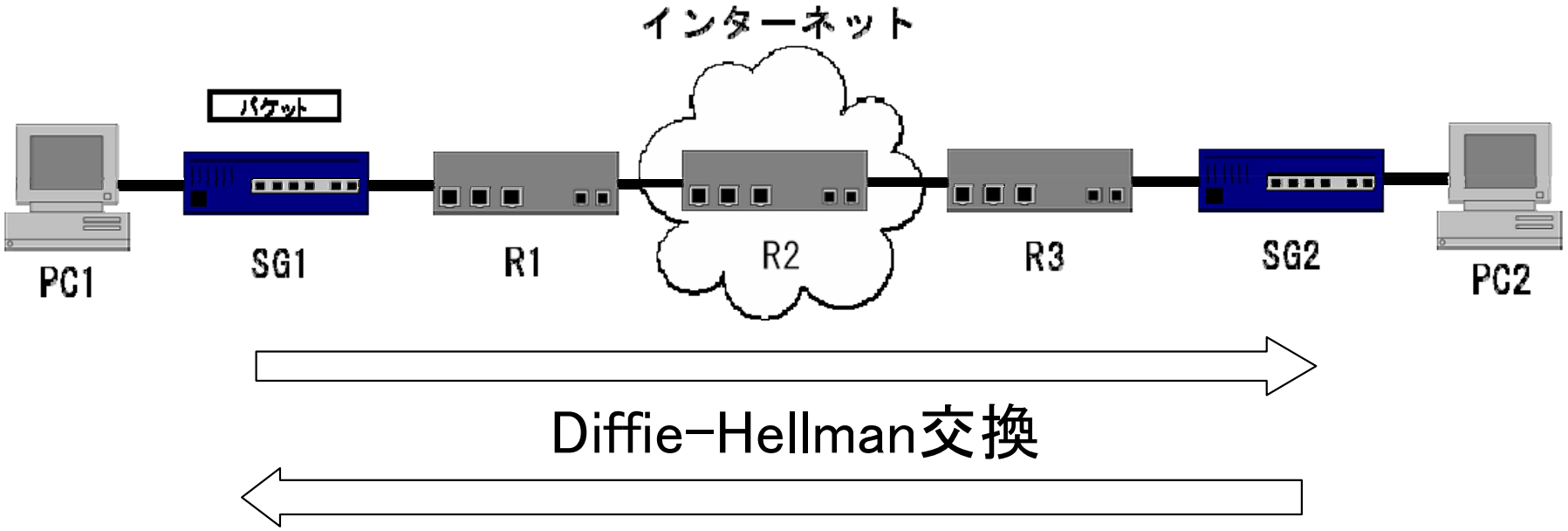


ISAKMP SA生成の受託

3.6 具体的なIKEの動作

秘密対称鍵の自動生成

SG1は規則に従って乱数を発生し、SG2へ送信する
SG2も同様に乱数をSG1に送信する
SG1、SG2は2つの乱数を組み合わせ、公開鍵暗号技術により秘密対称鍵を生成する

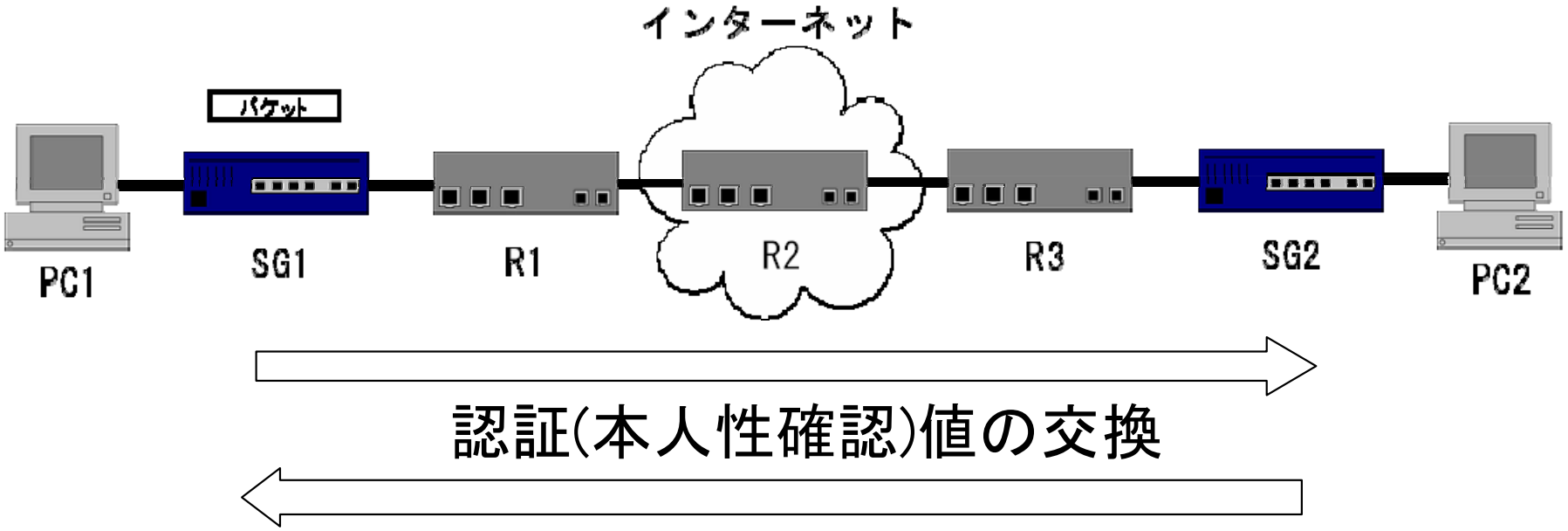


3.6 具体的なIKEの動作

IKE相手が本物かどうかの確認

SG1は、事前に設定した秘密のパスワードとその他の情報から作った認証(本人性確認)値であるハッシュ値をSG2に送信する
SG2も同様にSG1へ向けハッシュ値を送信し交換が成立する

相互認証が完了した後、ISAKMP SAの確立が完了

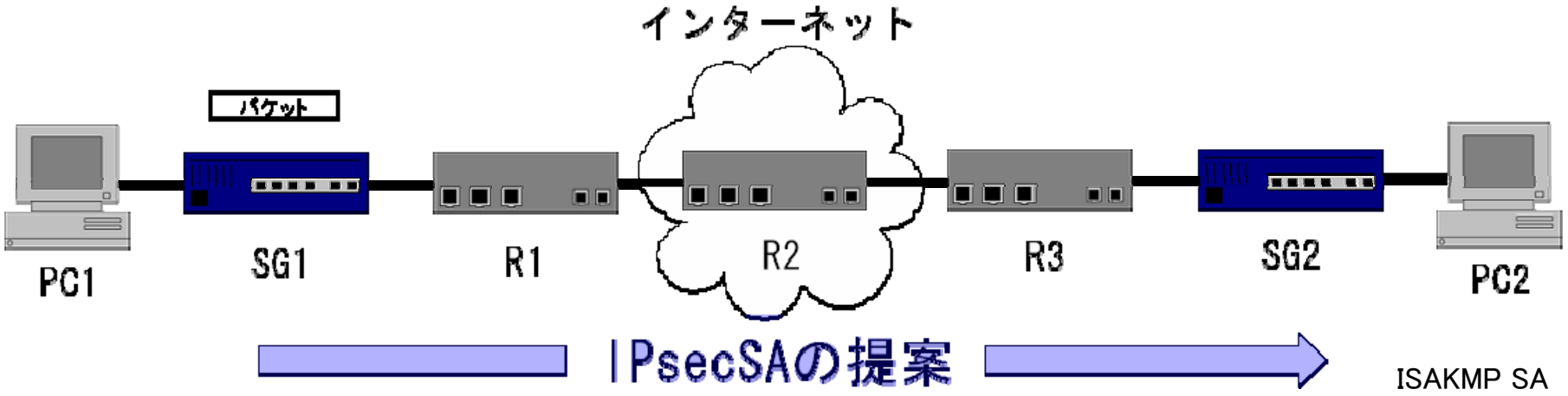


3.6 具体的なIKEの動作

PC1からPC2へのパケットを転送するIPsec SAの提案

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

上記のパケットはISAKMP SAを通して
送られるので暗号化されている

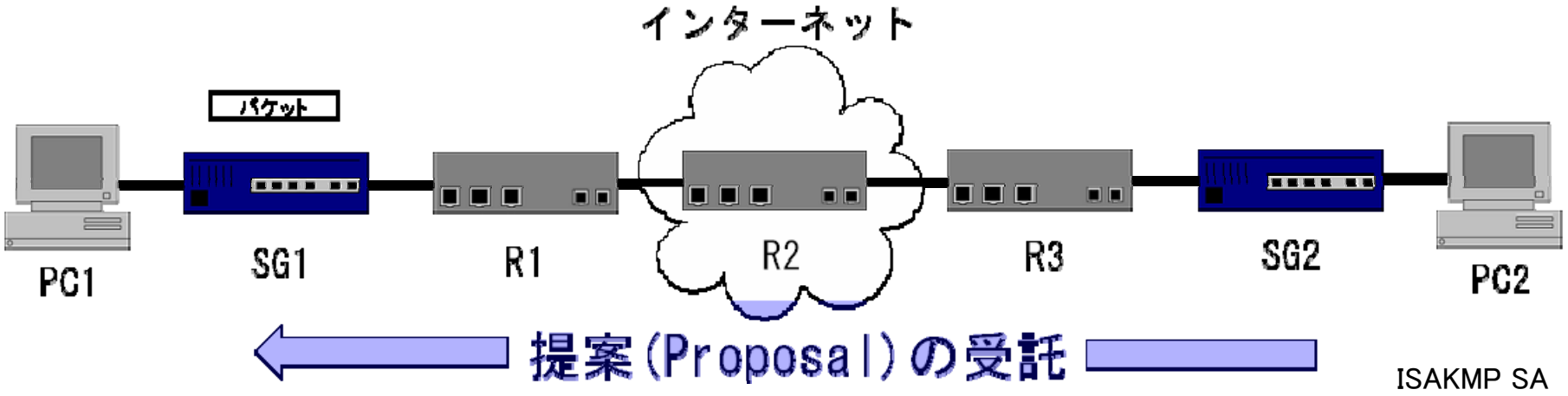


3.6 具体的なIKEの動作

Proposalの受諾

SG2は、セキュリティポリシーを照会して、Proposalを受託
受託したProposalと暗号化に使用する鍵を作るための乱数をSG1に送信

上記のパケットはISAKMP SAを通して
送られるので暗号化されている

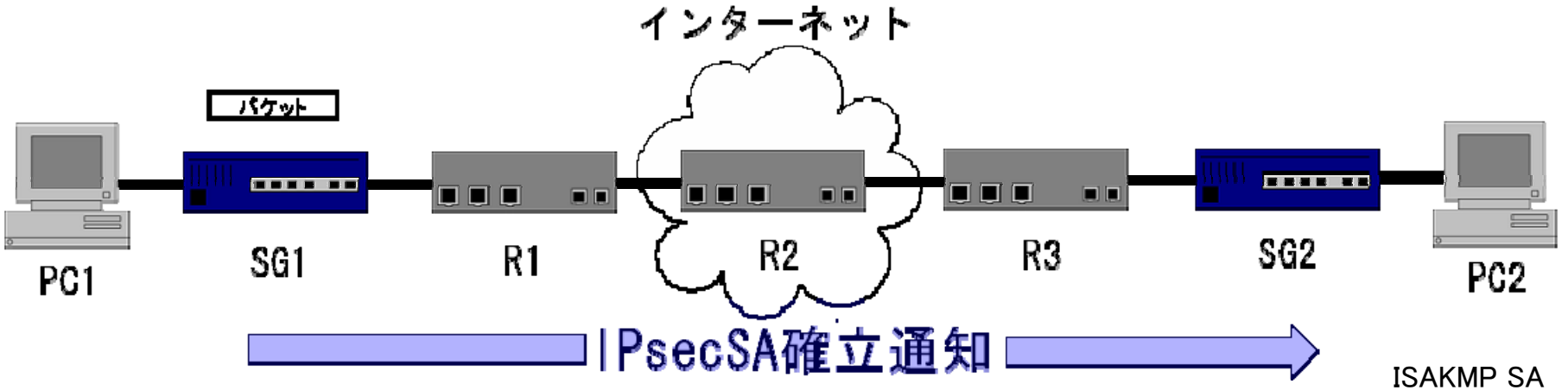


3.6 具体的なIKEの動作

IPsec SA確立の通知

SG2からProposal受諾の通知を受け取ったSG1はIPsec SAを確立し、SG2にSAの確立を通知する

制御用チャンネルISAKMP SAと、データを暗号化してやりとりするIPsec SAが完成



ISAKMP SA

SG1→SG2 IPsec SA

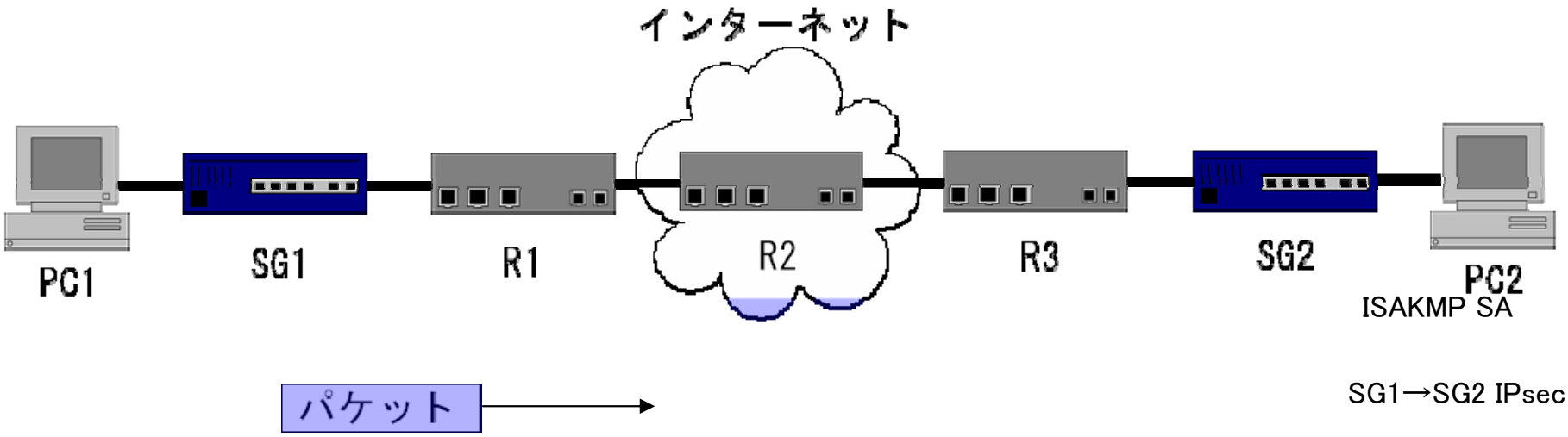
SG2→SG1 IPsec SA

3.6 具体的なIKEの動作

PC1からPC2へのパケットIPsec化

SG1は、SG1からSG2向きのIPsec SAにpingパケットをESP化して送信

途中のR1、R2、R3にとってIPsecパケットはSG1からSG2へのパケットにしか見えないため、通常のIP転送を行う



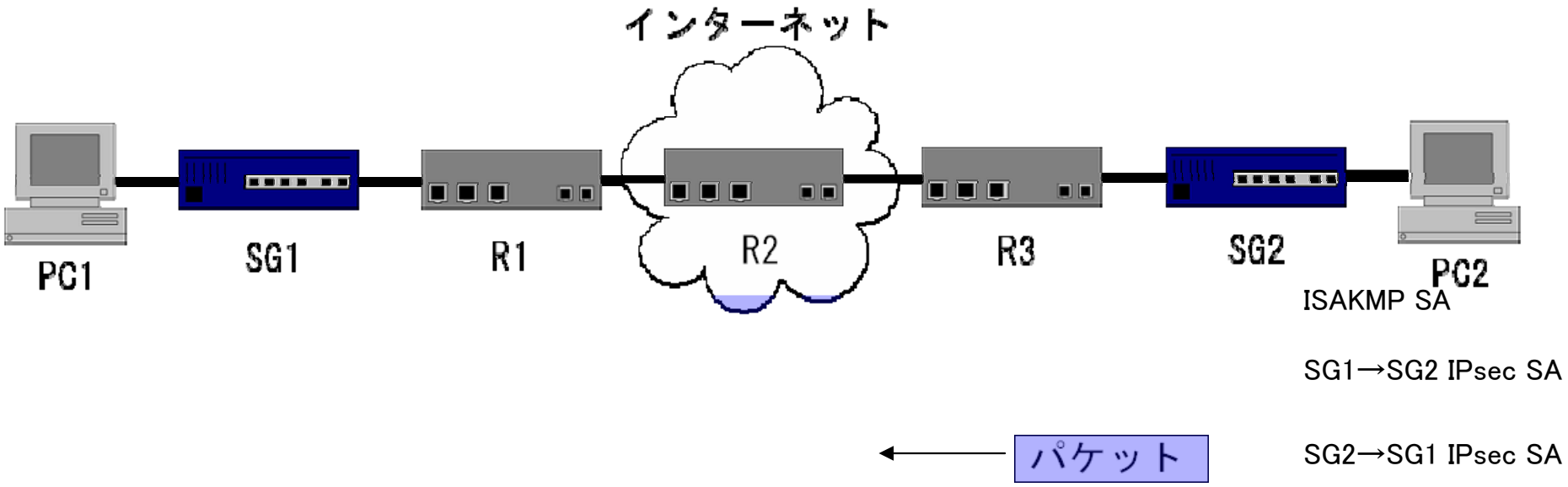
3.6 具体的なIKEの動作

PC2からPC1へのパケットIPsec化

SG2は、セキュリティポリシーに設定してある情報から、SG2からSG1向けのIPsec SAでパケットをIPsec化すべきとわかる

SG2からSG1向けのIPsec SAでパケットをESP化し、SG1へ送る

PC1はPC2からpingの返事を受信



むすび

- IPsecのアーキテクチャ
- IPsec SAの説明
- Diffie-Hellman交換の説明
- IKEの動作

参考

IPsec徹底入門　2002年8月6日　初版

著者　小早川　知明

おわり