IPsecの概要

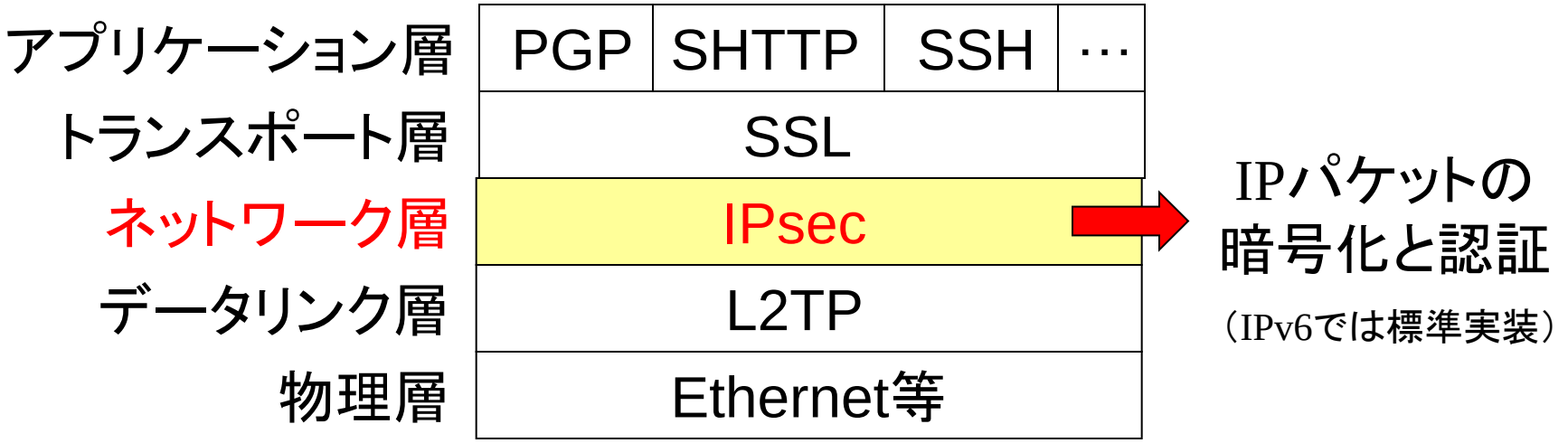
目次

1. IPsecの位置付け

2. パケットのカプセル化

3. IKE (Internet Key Exchange)

1. IPsecの位置付け



IPsec (Internet Protocol Security) =

ESP (Encapsulating Security Payload)：認証と暗号化

+ AH (Authentication Header)：強力な認証

カプセル化機能

+ IKE (Internet Key Exchange)：
通信相手の認証、ESPやAHで用いる
秘密情報（鍵）の交換

鍵およびコネクションの自動生成・管理機能

IPsecの長所と短所

○優れたインターネットVPNソリューション

－使用が公開されており、かつ多数の専門家による厳しい検証に耐えてきた技術で、極めて安全である。

－インターネットをそのまま利用できる。VPN拠点にそれぞれIPsec装置を置くだけでよい。

－IP層の処理なのでアプリケーションの変更の必要がない。

－IPsec装置をVPN拠点の出口に設けることで、LAN内部の機器には暗号化などの負担がかからない。

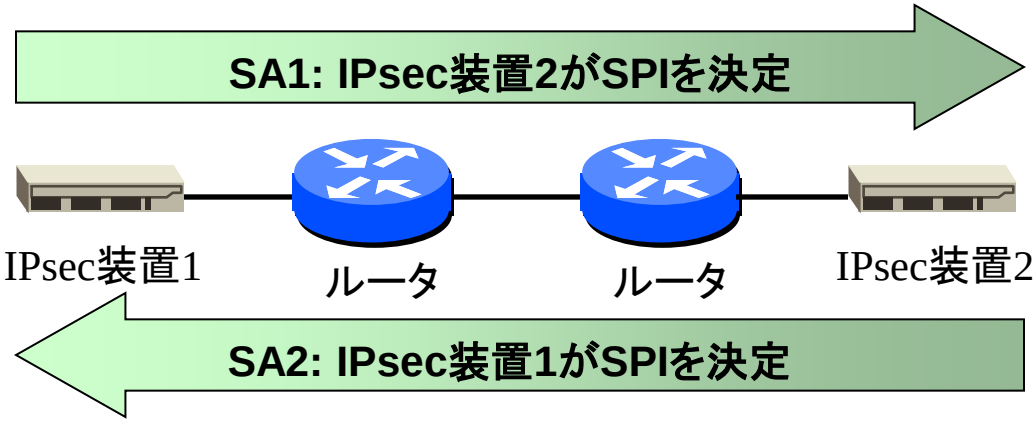
○欠点

－プロトコルが複雑すぎるために、機器への実装時に伴うバグや設定ミスによるセキュリティホールの発生が考えられる。

－異なるベンダ間で完全な相互接続性がない。

IPsec通信のコネクション

Security Association (SA)



SPI:SAの識別子

◇ IPsec装置間で生成される論理的なコネクション
◇ 一方通行、往復で二つのSAが必要
◇ SAごとに異なるセキュリティパラメータ

○ Security Association Database (SAD):
生成されているSAを管理するデータベース

SAのパラメータ

- 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
- セキュリティプロトコル: ESP/AH
- Security Parameters Index (SPI): SAの識別子
  →受信者が決める
- 暗号化アルゴリズム、認証アルゴリズム
- セレクタ: SAに通すパケットの指定
  - 宛先IPアドレス
  - 送信元IPアドレス
  - トランスポート層プロトコル
  - 送信元ポートと宛先ポート
  - ユーザ名、ホスト名

☆ SAは次の3つの値の組み合わせによって特定できる。

- SPI
- ESPかAHかの区別
- 転送用外側IPヘッダ

セキュリティポリシー

Security Policy (SP):
　　どのようなパケットをどのように処理するかのルール

○ Security Policy Database (SPD):
　　Security Policy (SP) を管理するデータベース

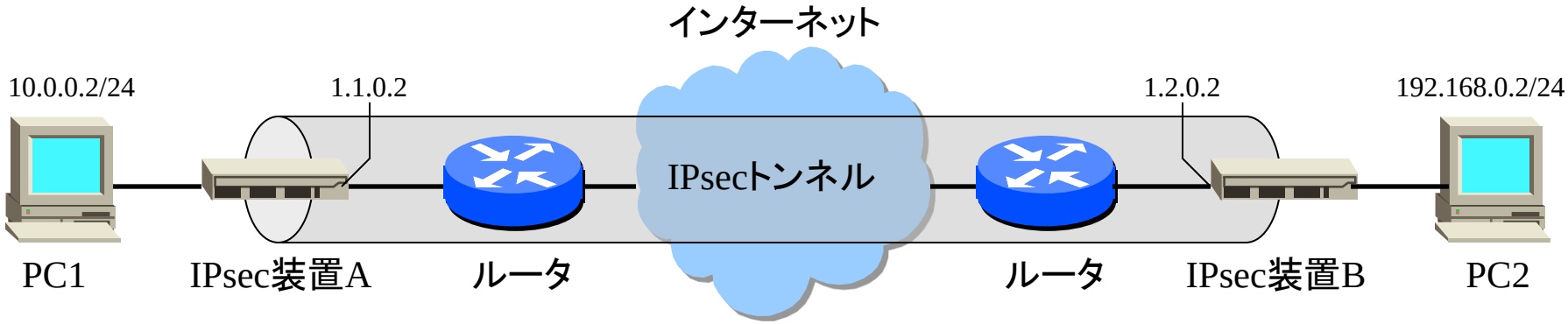
セキュリティポリシーの例

ルール番号	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	上位レイヤプロトコル
1	172.16.0.1/32	172.31.0.1/32	500	500	UDP
2	10.0.0.0/8	192.168.0.0/16	Any	Any	Any
ルール番号	動作	セキュリティプロトコル	暗号化アルゴリズム	認証アルゴリズム	カプセル化モード
1	Accept	–	–	–	–
2	IPsec	ESP	3DES	HMAC-MD5	Tunnel

2. カプセル化モード

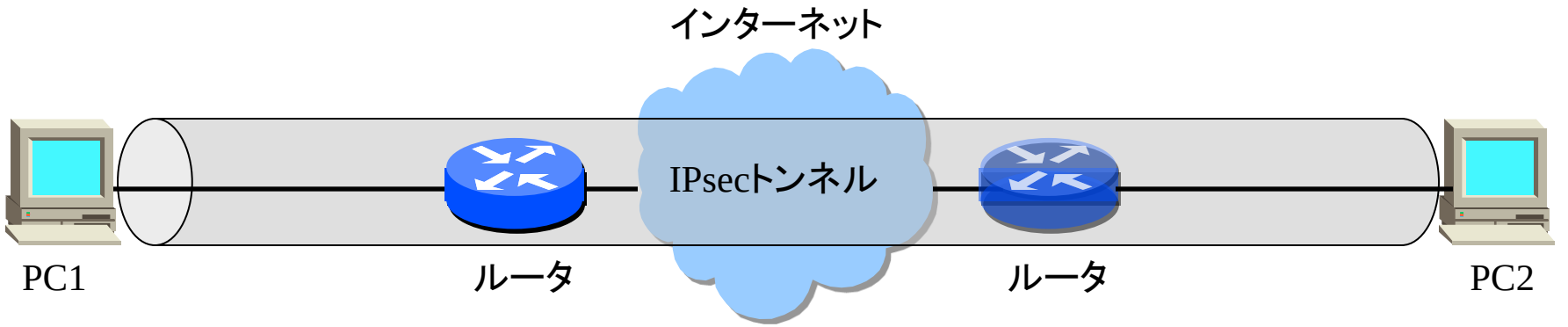
○ トンネルモード

ホスト以外が代わりにIPsec化



○ トランスポートモード

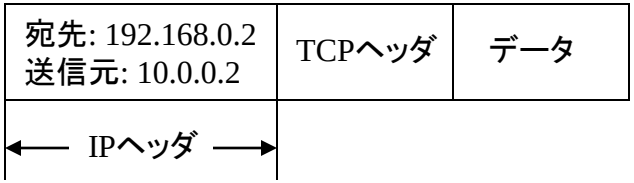
ホスト同士が自身のパケットを自身でIPsec化



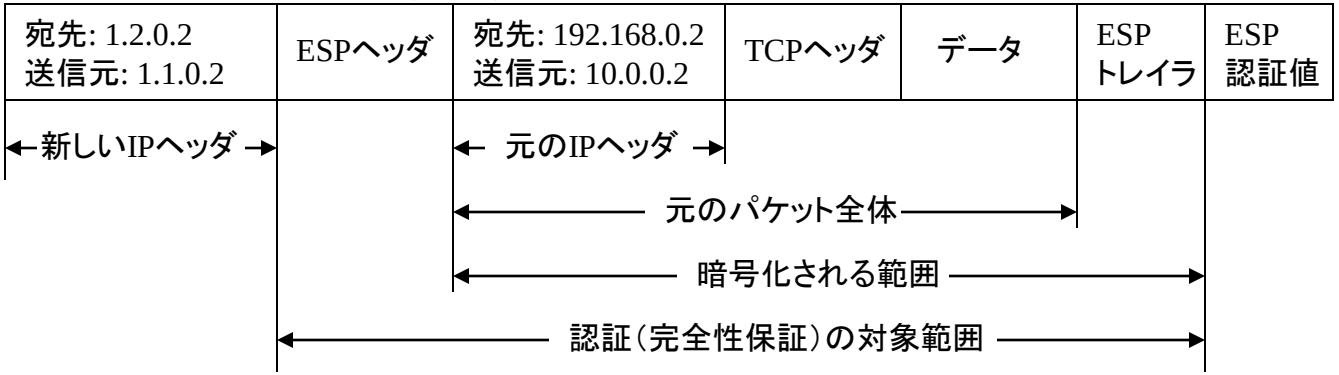
トンネルモードSA

◇ IPパケット全体の暗号化

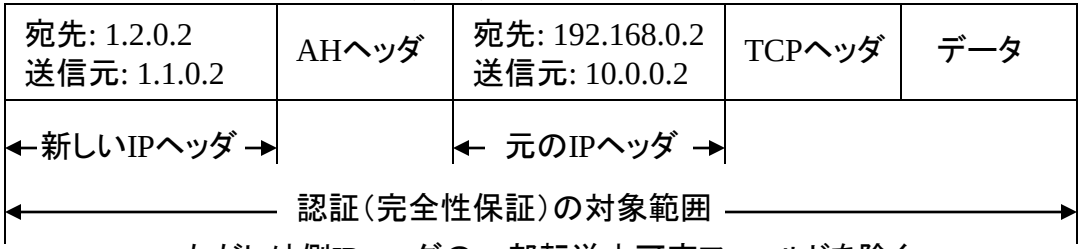
元のパケット



トンネルモードでIPsec(ESP)化されたパケット



トンネルモードでIPsec(AH)化されたパケット

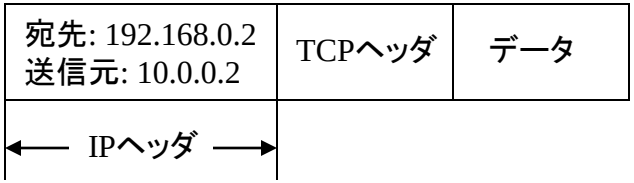


ただし外側IPヘッダの一部転送中可変フィールドを除く

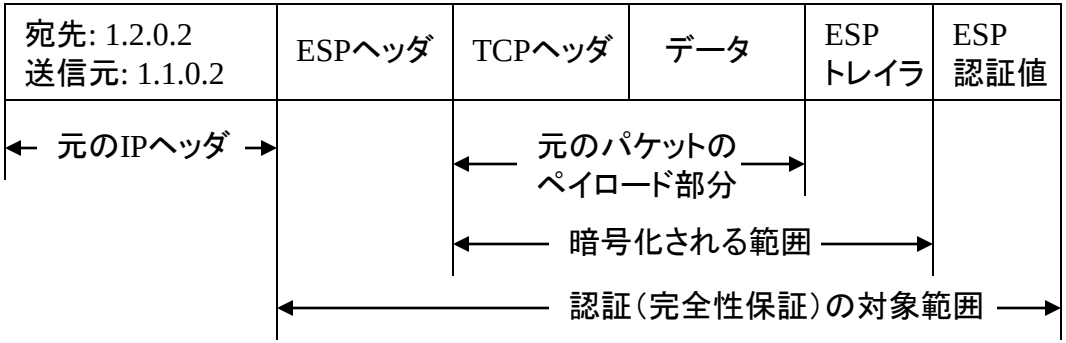
トランスポートモードSA

◇ データ部分の暗号化

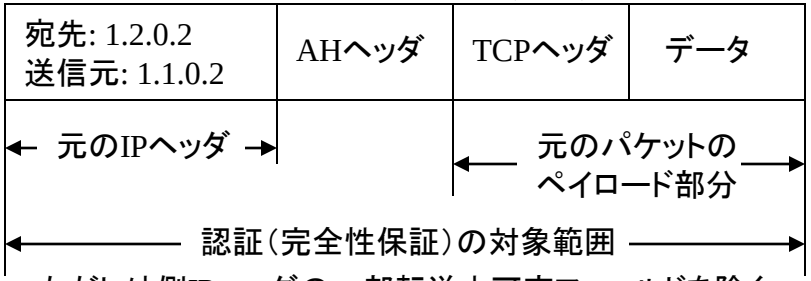
元のパケット



トランスポートモードでIPsec(ESP)化されたパケット



トランスポートモードでIPsec(AH)化されたパケット



ただし外側IPヘッダの一部転送中可変フィールドを除く

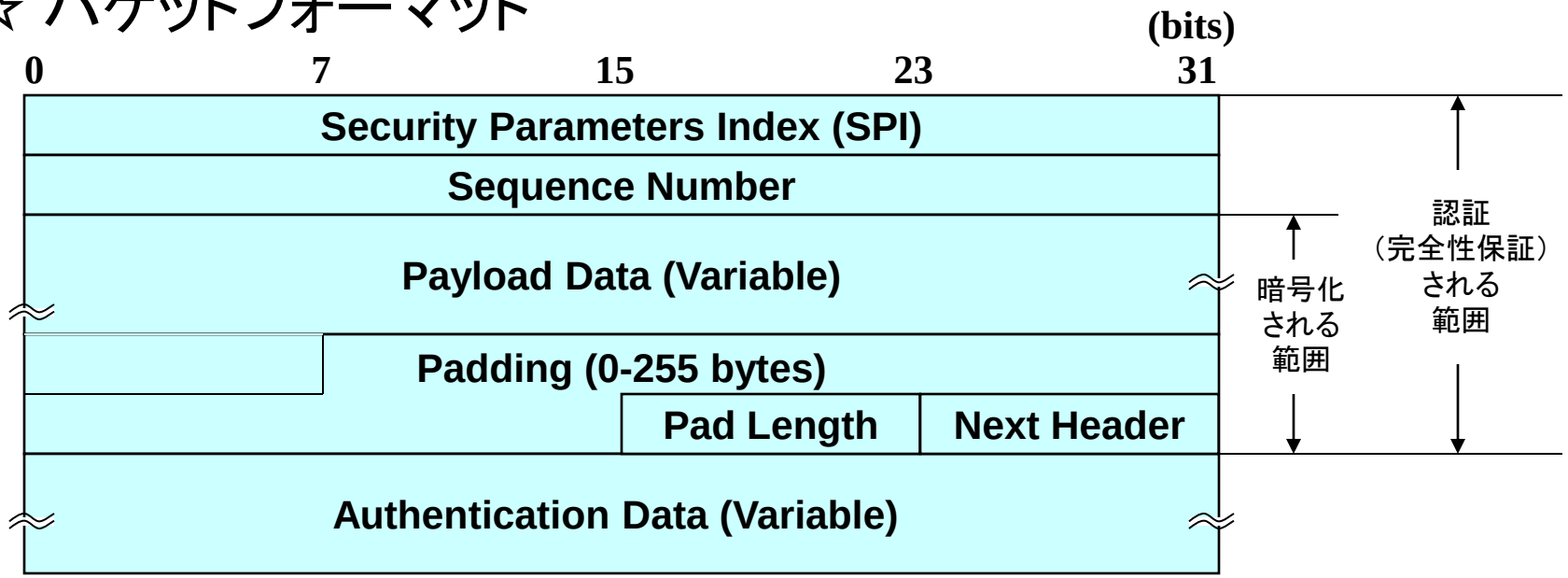
セキュリティプロトコル

	ESP (Encapsulating Security Payload)	**AH** (Authentication Header)
秘密性	元のパケットの内容を暗号化。 トンネルモードでは、元の IP ヘッダも暗号化する。	なし
認証 （本人性確認）	送信元を限定的な範囲で保証。 アンチリプレイ*機能。	送信元の完全な保証。 アンチリプレイ*機能。
認証 （完全性保証）	パケットが改ざんされていないことを保証。	パケットが改ざんされていないことを保証。
アクセス制御	設定に従ってパケットをフィルタリング。	設定に従ってパケットをフィルタリング。

＊ 以前のパケットをコピーして不正に再送するリプレイ攻撃に対する対処

ESP (Encapsulating Security Payload)

☆ パケットフォーマット



Security Parameters Index (SPI): 各IPsec装置が自身の管理しているSAを識別するために使う。
(0: 使用禁止、1~255: 予約済)

Sequence Number: アンチリプライ機能のためのカウンタ
1から始まりIPsecパケットが転送されるたびに増加していく。最大値に達したらSAは無効となる。

Payload Data: 暗号化される元のIPパケット

Padding: Payload Dataがブロックサイズの倍数になるように調整する。

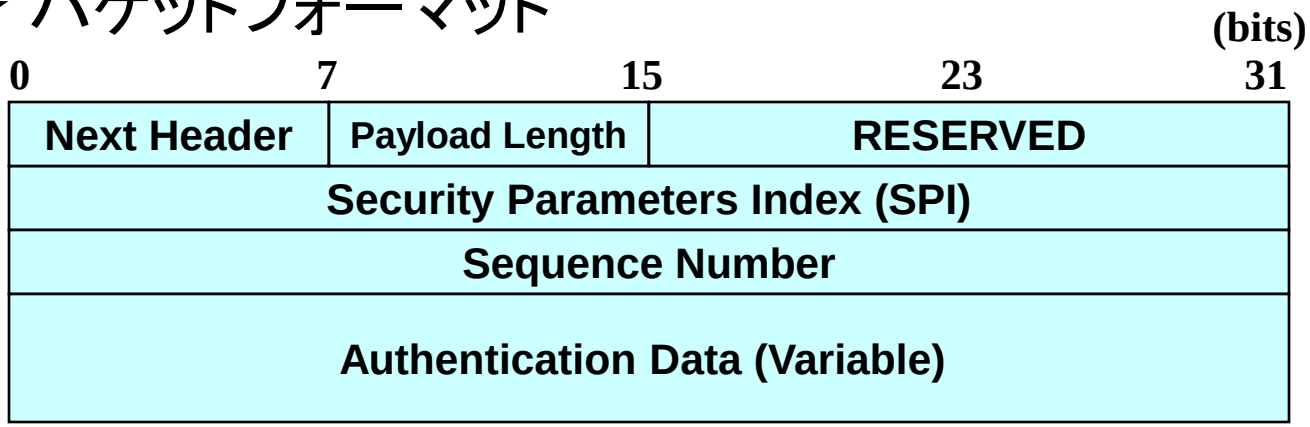
Pad Length: 0～255

Next Header: Payload Dataフィールドにあるデータの種類を指定
(IPv4のトンネルモード: 4、トランスポートモード: 6)

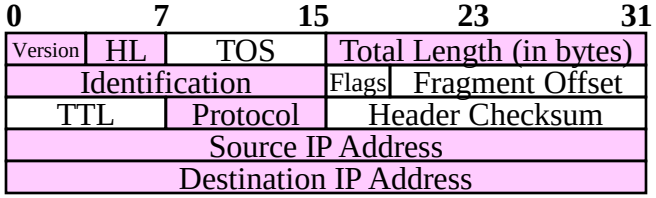
Authentication Data: SPIフィールドからNext Headerフィールドまでの Integrity Check Value (ICV、秘密対象鍵を使用して計算した対象メッセージの完全性検査用認証値)の計算結果を格納する。

AH (Authentication Header)

☆ パケットフォーマット



Next Header: AHに続くヘッダの種類を指定
(IPv4のトンネルモード: 4　　トランスポートモード: 6)
Payload Length: AH自身の長さ、ワード数（1ワード=4バイト）-2で記述、通常は4
RESERVED: すべて0
Security Parameters Index (SPI): 各IPsec装置が自身の管理しているSAを識別するために使う。
(0: 使用禁止、1~255: 予約済)
Sequence Number:アンチリプライ機能のためのカウンタ
1から始まりIPsecパケットが転送されるたびに増加していく。最大値に達したらSAは無効となる。
Authentication Data: 外側IPヘッダまで含めたパケット全体の Integrity Check Value (ICV、秘密対象鍵を使用して計算した対象メッセージの完全性検査用認証値)の計算結果を格納する。ICVの計算対象は、パケット全体から転送中に変化して予測不可能な以下のフィールドとAuthentication Dataフィールドを除いた部分。



転送中に変化しない、ICVの計算対象

転送中に変化する可能性あり、すべて0とみなして計算

暗号化アルゴリズム

○共有鍵暗号
- －DES、3DESなど

○ブロック暗号
- －ある一定長さのブロック単位で暗号化、通常ブロックサイズは64ビット
- －元の平文と同じ長さの暗号文を出力
- －IPヘッダ部分など同一のデータを繰り返し含む平文には不向き

○CBCモード (Cipher Block Chaining)
- －1つ前に暗号化したブロックの暗号文とこれから暗号化する平文のXORを計算し、そのXOR値を暗号化して出力
- －平文に規則性があっても全体としてまったく異なる暗号文が得られる。
- －最初のブロックの暗号化には、Initialization Vector(IV)を使用

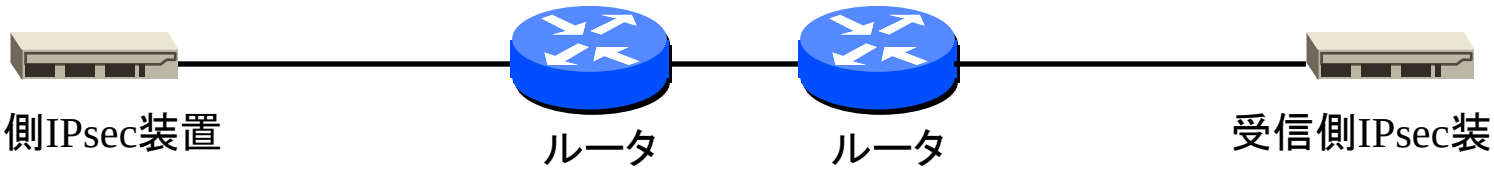
認証アルゴリズム

○認証の2つの意味
- －完全性認証: パケットが通信経路上で改ざんされていないことの認証
- －本人性確認: 通信相手が本物であるかの認証

○一方向性ハッシュ関数
- －出力から元の値を特定することが不可能
- －MD5、SHA-1など

○HMAC (Hash-based Message Authentication Code)
- －鍵付きハッシュ関数、ハッシュ関数の入力に秘密鍵を付加
- －あるメッセージの鍵付きハッシュ出力を交換することで、通信相手が同じ鍵を共有しているかどうか確認する。
- －通信経路上に鍵そのものを流さないので安全

IPsecの動作



SPD検索
セキュリティポリシー(SP)によって
パケットをIPsec化すべきかどうか決定

SA選択
SPに合致するSAがあればそれを選択
合致するSAがない場合、IKEなどの自動生成/管理
プロトコルを使用していればSAを自動的に生成し、
使用していなければパケットを破棄する。

パケットのESF/AH化
ESPヘッダ、AHヘッダ等を付加

シーケンス番号の付与
IPsecパケットを送信するたびに1ず
つ増加させる。アンチリプレイ機能有
効の場合、シーケンス番号が最大値
に達したらSAを無効化し再生成。

ESP
暗号化と
ICV計算

AH
ICV計算

パケットの分割
MTUを超えている場合

送信

セキュリティポリシー(SP)に照らし合わせ
受信パケットを受け入れ可能かどうか決定
SPDチェック

ESP/AH化される前の
元のパケットを再構築
パケットの再構築

ESPパケットのペイロード
の先頭に入っているIVを
使用して復号化
復号化

AH
ESP
通信経路上の改ざん検出
ICV検査

リプレイ攻撃対策
シーケンス番号の検査

次の3つの値の組み合わせから
・SPI
・ESPかAHかの区別
・転送用外側IPヘッダ
SAの特定

受信

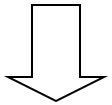
3. IKE (Internet Key Exchange)

◇手動によるSA生成:

暗号化に使う秘密対称鍵や各種パラメータをIPsec装置にそれぞれ設定する。

△問題点

・多数の通信に対応できない。
・同じ秘密対象鍵をずっと使用し続けると推定されやすくなる。
・ポート番号単位のSAを構成できない。
・…



〇SA自動生成／管理プロトコル

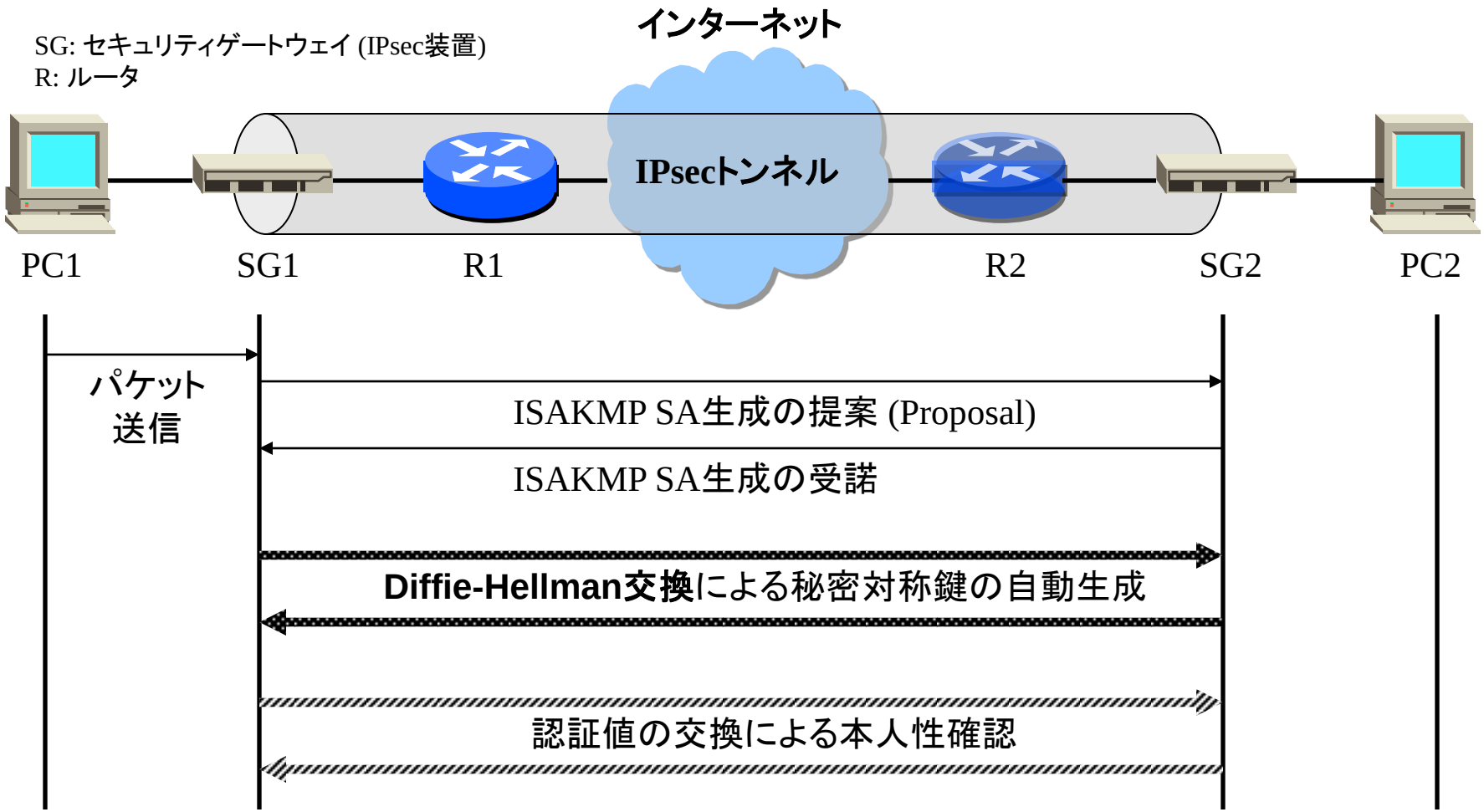
－SAの自動生成・監視・再構成、秘密対称鍵生成、パラメータ交換
－ESPやAHなどのカプセル化とは互いに独立したプロトコル

〇3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
－**Diffie-Hellman交換:** 生成するSAの秘密対称鍵を公開鍵暗号技術により安全に自動生成
－**IKE相手の認証（本人性確認）:** IKE通信相手が本物であることを確認

IKEの動作の概要 (Phase 1)

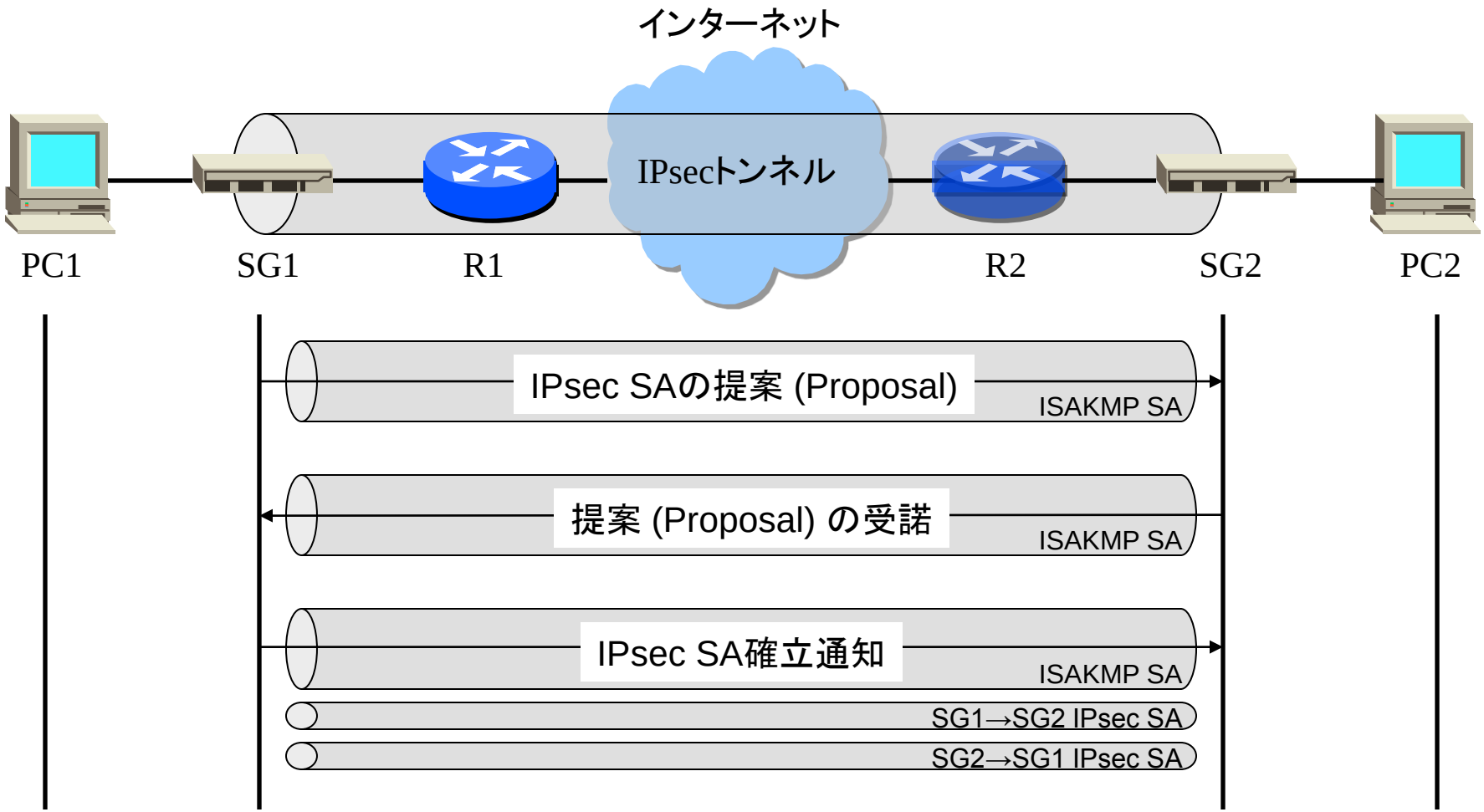
Phase 1 ー 制御用チャネルであるISAKMP* SAの確立



* ISAKMP: Internet Security Association and Key Management Protocol

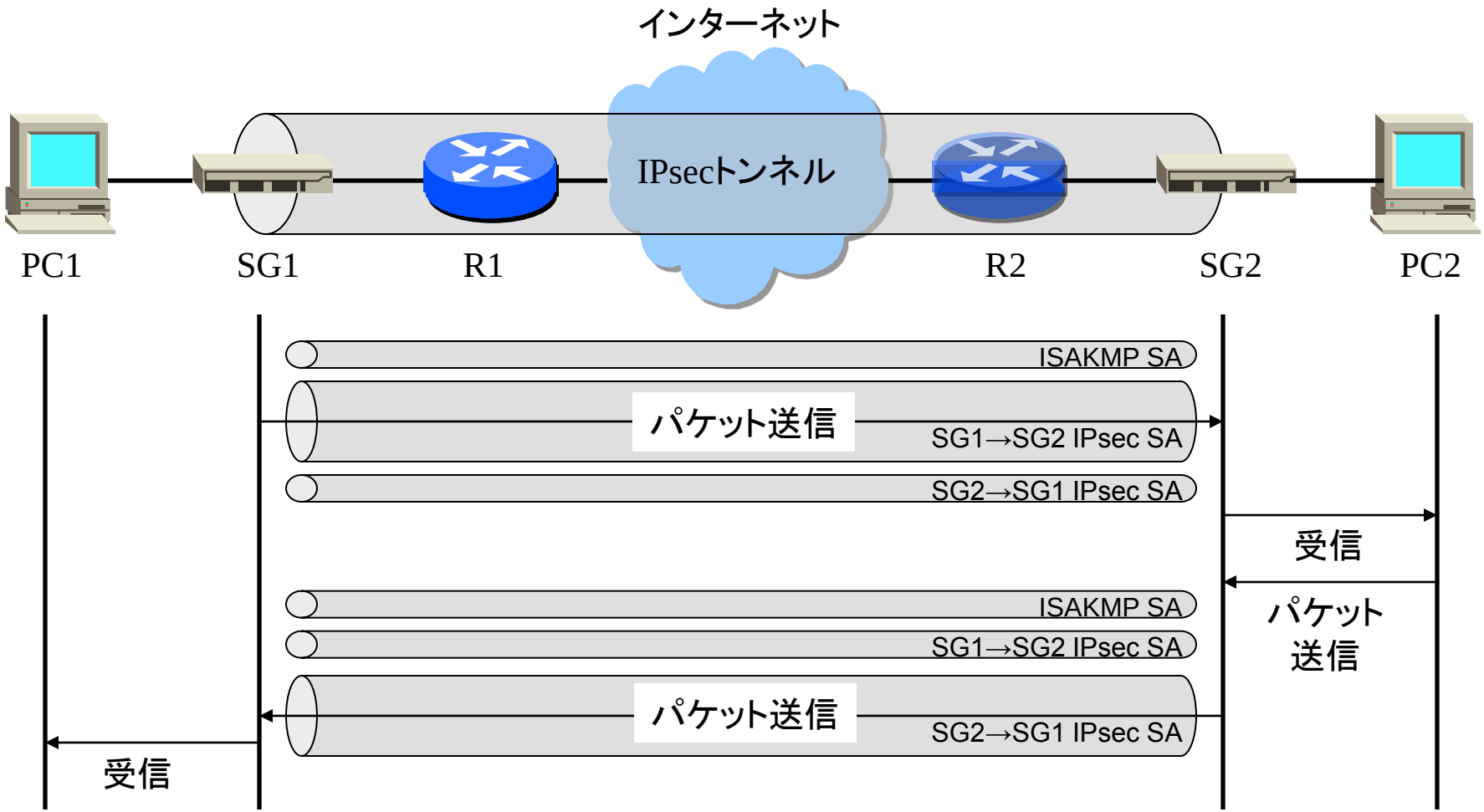
IKEの動作の概要 (Phase 2)

Phase 2 ー IPsec SAの確立



IKEの動作の概要 (IPsec通信)

IPsec通信



Proposal交換

○SAの提案とProposalの選択

－SAを確立しようとする側（イニシエータ）がSAの案をいくつか提案

－提案を受ける側（レスポンダ）は提案の中に受け入れ可能なものがある場合、1つだけ選択してイニシエータに返答

Phase 1 － ISAKMP SAの確立

☆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: DHグループ
- Life typeとLife Duration:
  ISAKMP SAの有効期間と測定方法
  （例）type: seconds, duration: 10800
  type: kilobytes, duration: 4096

Phase 2 － IPsec SAの確立

☆パラメータ

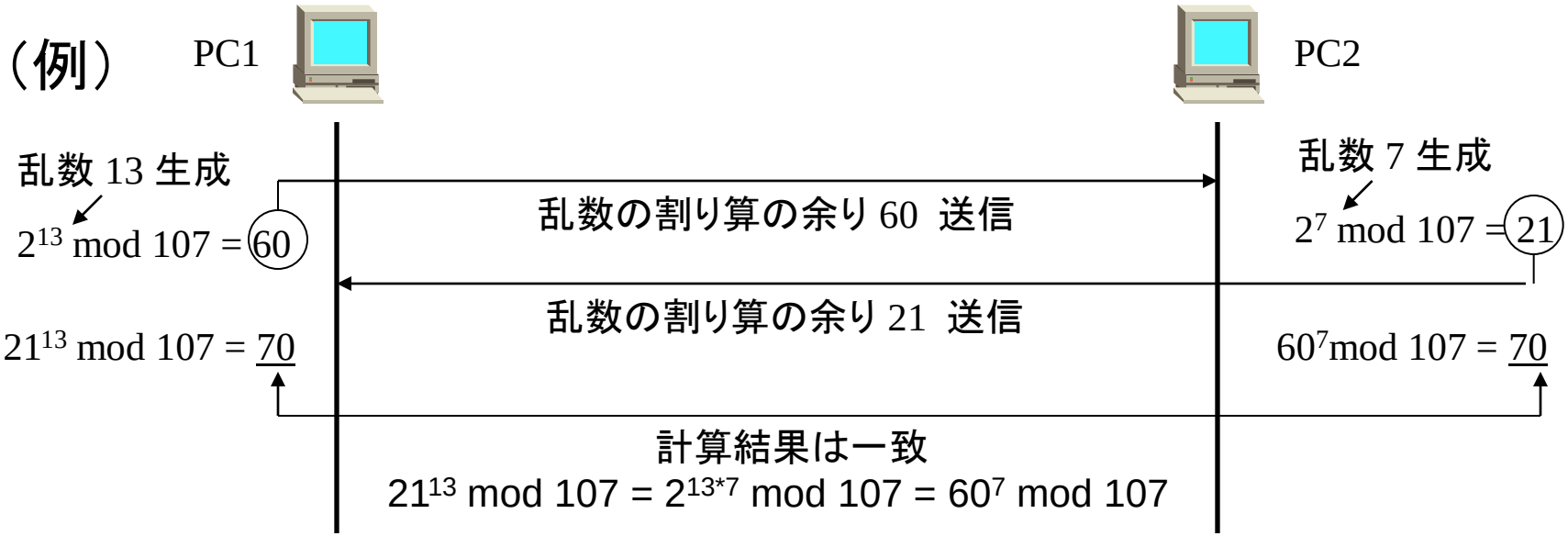
- セキュリティプロトコル
- Life typeとLife Duration
- カプセル化モード
- 暗号化アルゴリズム（ESPの場合）
- 認証（本人性確認）アルゴリズム（ESPの場合はオプション、AHの場合は必須）
- Diffie-Hellman交換に使用するパラメータ（オプション）

Diffie-Hellman交換

○秘密対称鍵の共有

－交換は安全でない通信経路を経由するが、

－盗聴者が盗み見ても鍵を推定することは非常に困難



（一般的な関係） $B^x \bmod n = g^{xy} \bmod n = A^y \bmod n$

(A,B: 乱数、n: 素数、g: nより小さい整数)

60と21の値がわかったとすると、$21^x \bmod 107 = 2^{xy} \bmod 107 = 60^y \bmod 107$
このxとyの値を見つけ出すことは、離散対数問題とよばれ、非常に難しい。

○DHグループでgとnの値を指定

－Group1: g=2, n=232桁の10進数　Group2: g=2, n=309桁の10進数

IKEにおける認証(本人性認証)方式

○3つの方式

認証方式	スケーラビリティ	簡便さ	普及度	特徴と問題点
Pre-Shared Key 認証	低	高	高	単純にいうとパスワード認証方式。 通信相手との Pre-Shared Key を事前に共有しておく必要がある。Pre-Shared Key は秘密である。
公開鍵暗号認証	中	中	低	通信相手の公開鍵を事前に設定しておく必要がある。ただし公開鍵は秘密にする必要がないため、公開鍵の配布は Pre-Shared Key の配布よりも簡単に行える。
デジタル署名認証	高	低	中	通信相手ごとに事前に鍵情報を共有する必要がないため、スケーラビィティィが高い。また CA によって証明された公開鍵を使用するため、IKE 通信相手が後に「通信をしていなかった」と嘘をつくことができない（否認不能性）というセキュリティ機能を提供できる。しかし CA の存在が必須で、採用へのハードルは高い。

ISAKMPヘッダ

☆ ISAKMPペイロードチェイニング

☆ ISAKMPヘッダフォーマット

Cookie: 通信相手が本当にIKEの実装で、通信を目的としてIKEを行っているかチェックするために使用する。IKE通信を行うIPsec装置はそれぞれ乱数を生成し、最初に交換するISAKMPヘッダのCookieフィールドにその乱数(Cookie)を入れ、相手に送信する。Cookieの交換が成功するとその後のIKE通信のすべてのヘッダに、イニシエータが送信したCookieとレスポンダが送信したCookieが付加される。通信相手が2つのCookieペアを送信してくるのを確認することで、DoS攻撃を防御する。

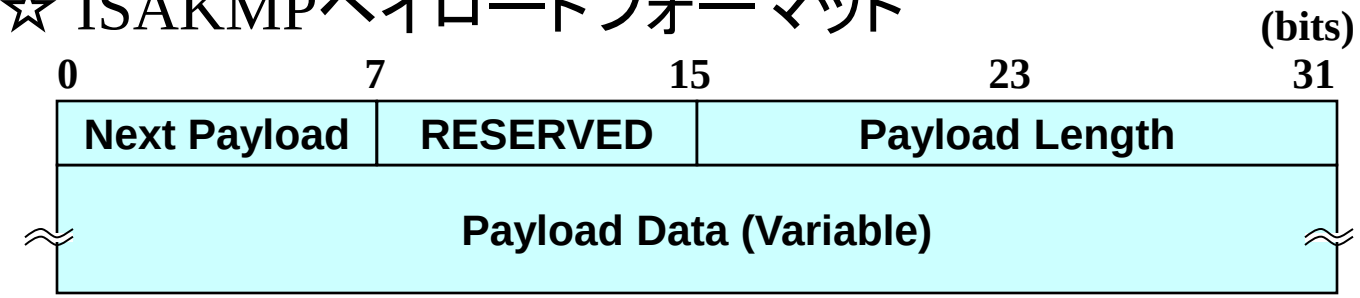
MjVer: IKEのメジャー番号　　**MnVer:** IKEのマイナー番号　　現在のバージョンは1.0

Exchange Type: ペイロードの種類　　**Flags:** パケットが暗号化されているかどうかの確認用

Message ID: 1つのISAKMP SAで複数のIPsec SAを生成することが可能であり、複数のSAのネゴシエーションを識別するために使用する。Phase 2交換用、Phase 1では常に0。

ISAKMPペイロード

☆ ISAKMPペイロードフォーマット



Next Payload: 次に続くペイロードの種類を指定、これが最後のペイロードの場合は0
RESERVED: すべて0
Payload Length: SA Proposal全体の長さをオクテット単位で指定

☆ ISAKMPペイロードの種類一覧

- Security Association Payload (SA)
- Proposal Payload (P)
- Transform Payload (T)
- Key Exchange Payload (KE)
- Identification Payload (ID)
- Certificate Payload (CERT)
- Certificate Request Payload (CR)
- Hash Payload (HASH)
- Signature Payload (SIG)
- Nonce Payload (NONCE)
- Notification Payload (N)
- Delete Payload (D)
- Vendor ID Payload (VID)

ISAKMPペイロード

☆ 主なISAKMPペイロードの内容

○Security Associationペイロード (SA)

－ISAKMP SAやIPsec SAを作るためにProposal交換を行う際に使用する。

－SAペイロードの中に、複数のProposalペイロード(P)が入り、さらにPの中に複数のTransformペイロード(T)が入る。

－ProposalペイロードはSAを提案する単位で、Transformペイロードの中に、実際にやりとりするSAのパラメータが入る。

IP: IPヘッダ　UDP: UDPヘッダ　ISAKMP: ISAKMPヘッダ

○Key Exchangeペイロード (KE)

－Diffie-Hellman公開値（DHグループ）が入る。

○Nonceペイロード (N)

－IKE交換を行う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る乱数が入る。

○Identificationペイロード (ID)

－IPアドレス、FQDNなどのID情報が入る。

○Hashペイロード (HASH)

－本人性認証、メッセージ改ざん検出に用いるハッシュ値が入る。

Exchange Type

〇Exchange Type（交換タイプ）:

どのようなペイロードをどのような順番でやりとりするかの決まり

ー **Main Mode:**

・Phase 1でISAKMP SAを確立するための標準の手順

ー **Aggressive Mode:**

・Phase 1の簡易的なISAKMP SA確立手順

・Main Modeと比べてISAKMPメッセージをやりとりする回数が少ない。

・ID情報は暗号化されない。

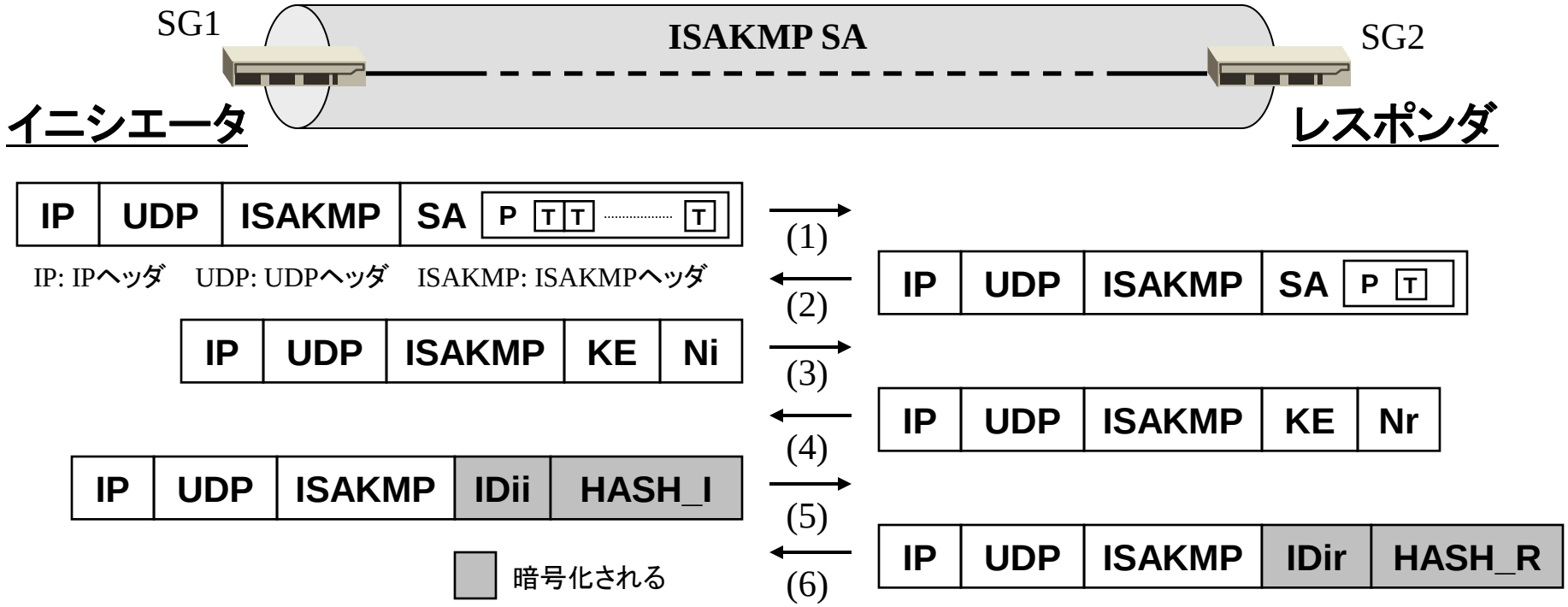
ー **Quick Mode:**

・ Phase 2で使用される唯一のモード

・すべて暗号化されており、わずかなパケットの交換でSA確立可能

IKE通信例1 - Pre-Shared KeyによるMain Mode

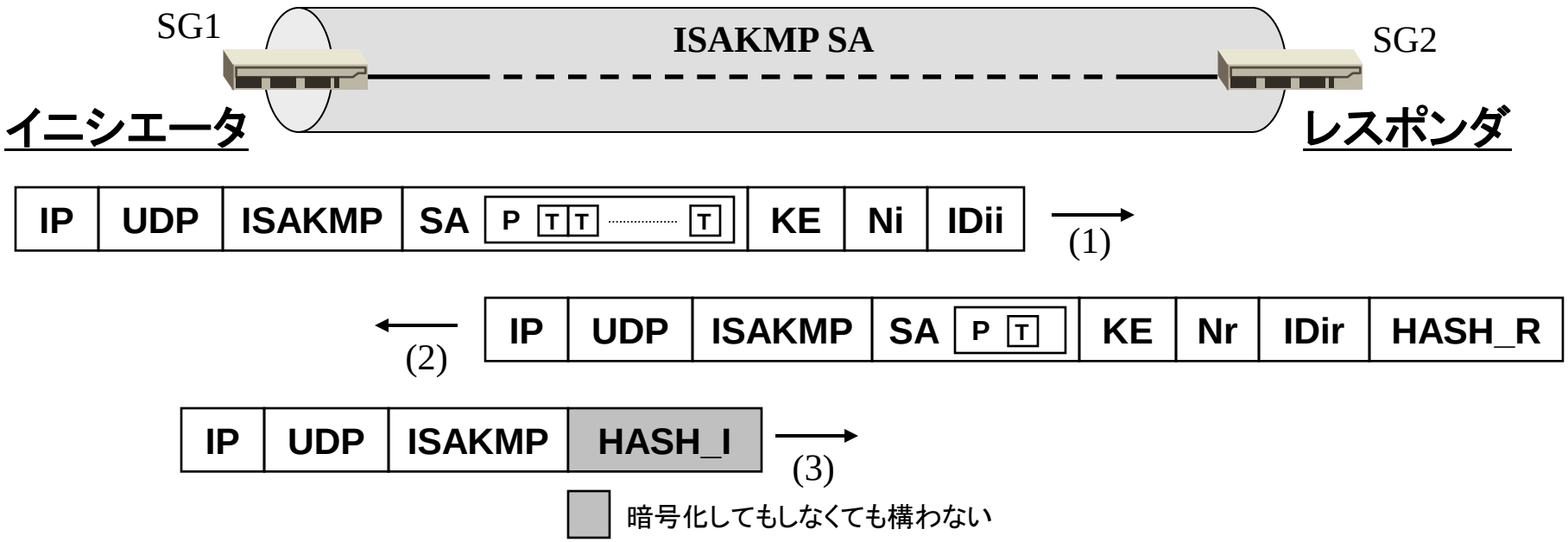
Pre-Shared Key ー あらかじめ両方のIPsec装置に共有値が設定されている必要がある。



(1) SAペイロードによりISAKMP SAのパラメータを提案
(2) 同形式のSAペイロードで、受諾可能なProposalを選択
(3)(4) Diffie-Hellman(DH)公開値と
　　Nonceによる乱数交換で秘密対称鍵生成
(5)(6) ID情報と認証情報(Hash)の交換

SA: SAペイロード
P: Proposalペイロード
T: Transformペイロード
KE: 鍵交換ペイロード
Ni: イニシエータのNonceペイロード
Nr: レスポンダのNonceペイロード
Idii: イニシエータのIDペイロード
Idir: レスポンダのIDペイロード
HASH_I:イニシエータのHASHペイロード
HASH_R:レスポンダのHASHペイロード

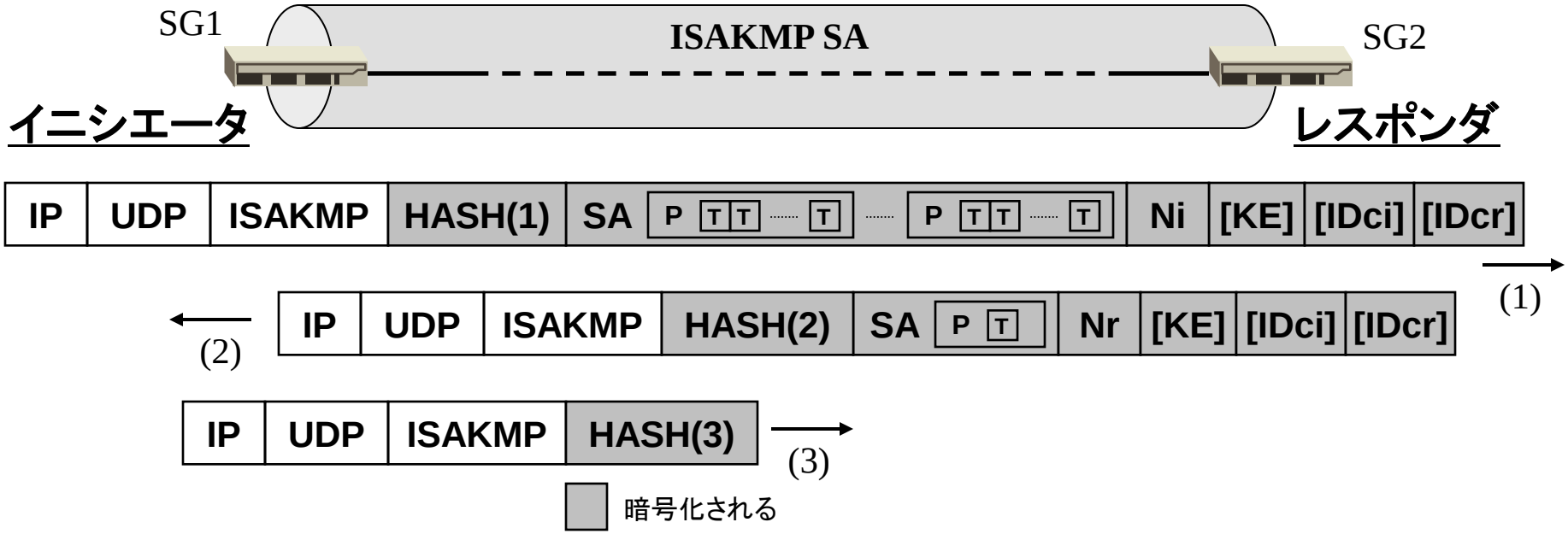
IKE通信例2 - Pre-shared KeyによるAggressive Mode



(1) ISAKMP SAのパラメータ提案、DH公開値の送信、Nonceによる乱数送信、ID情報送信を一気行う。
・ID情報は暗号化されない。
・使用するDHグループもネゴシエートできない。
(2) 受諾したProposal、DH公開値、Nonce、ID情報、Hashの送信。秘密対称鍵が生成される。
(3) イニシエータの認証情報送信

SA: SAペイロード
P: Proposalペイロード
T: Transformペイロード
KE: 鍵交換ペイロード
Ni: イニシエータのNonceペイロード
Nr: レスポンダのNonceペイロード
Idii: イニシエータのIDペイロード
Idir: レスポンダのIDペイロード
HASH_I:イニシエータのHASHペイロード
HASH_R:レスポンダのHASHペイロード

IKE通信例3 - Quick Mode



(1) IPsec SAのパラメータ提案、Nonce、
リプレイ攻撃を防ぐためのHashを送信
・生成するIPsec SAの情報が不十分な場合は両者のIDも送信
・Diffie-Hellman交換を行う場合は鍵交換ペイロードも送信
(2) 受諾したProposal、Nonce、ID情報、
リプレイ攻撃を防ぐためのHashを送信
秘密対称鍵が生成される。
(3) イニシエータの認証情報送信

SA: SAペイロード
P: Proposalペイロード
T: Transformペイロード
KE: 鍵交換ペイロード
Ni: イニシエータのNonceペイロード
Nr: レスポンダのNonceペイロード
Idci: イニシエータのIDペイロード
Idcr: レスポンダのIDペイロード
HASH(n):HASHペイロード
[ ]内はオプション

Main ModeとAggressive Mode

- Pre-Shared KeyによるMain Mode
  - セキュリティレベルは高い
  - 外出先からのVPN接続が困難

    【理由】Phase1におけるIDの種類はIPアドレスしか使用できない。
    なぜなら、最後の認証情報の交換の前にPre-Shared Keyを特定できている必要があるのに、IDペイロードは最後の交換でやりとりされるため、IDペイロードなしでIKE相手を特定してPre-Shared Keyを選択しなければならないからである。
    この制限により、外出先などではIPアドレスが動的に変化してしまい、Pre-Shared Key認証ではMain Modeを利用できないことがある。

- Pre-Shared Keyによる Aggressive Mode
  - 盗聴される可能性はMain Modeより高まる
  - IDとしてFQDNなど任意の種類を使用可能
  - Pre-Shared Key認証のほかに、ユーザ認証にXAUTHとよばれるIPsecの拡張機能を使用するのが一般的

その他の仕様

○ SAバンドル

- ESPのSAとAHのSAを組み合わせて1組として扱う
- 2つのIPsec化処理を連続して適用する

（AHとESPのトンネルモードの場合）

○ PFS (Perfect Forward Secrecy)

- ISAKMP SAの秘密対称鍵が破られると、生成されるIPsec SAの秘密対称鍵も簡単に見破られる。
- そこで、Phase 2におけるIPsec SA確立時にも、Diffie-Hellman交換を行って、IPsec SAに使用する秘密対称鍵を生成する。

バージョン情報

バージョン	作成日	内容
1.0	2003/3/14	IPsec概要
1.1	2003/4/12	一部ミス修正