I P s e c

T10:IPSec ～技術概要とセキュアなネットワークの実現手法～

第一部 IPsecの基本とリモートアクセスへの応用

2003/12/3

新日鉄ソリューションズ株式会社
基盤ソリューション事業部
マーケティング部
松島 正明

Agenda

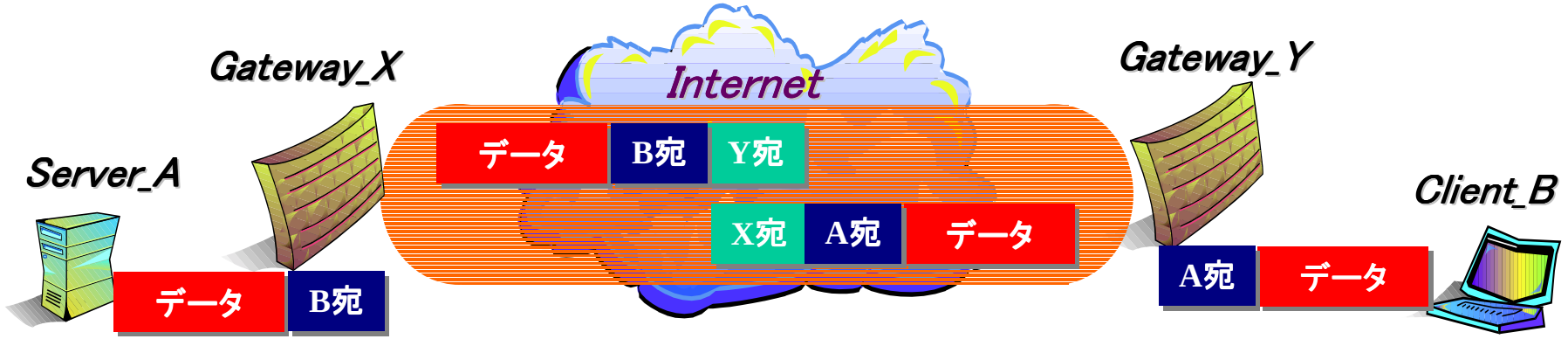
- IPsecの基本
- IKE(Internet Key Exchange)の概要
- IKE Phase1ネゴシエーションの詳細
- IKE Phase2ネゴシエーションの詳細
- Remote Access環境への対応
- Remote Accessの新たな手法 ～SSL VPN～

IPsecの基本

INTERNET WEEK 2003
2 - 5 December 2003 Yokohama / パシフィコ横浜

VPNとは

- Virtual Private Network
  - 仮想私設網/仮想自営網
    - Publicなネットワークをあたかも私設(自営)のネットワークのように使用するための技術
    - 私設ネットワークに見せかけるために、トンネリング技術を使用
    - VPN ≠ 暗号技術ではない。

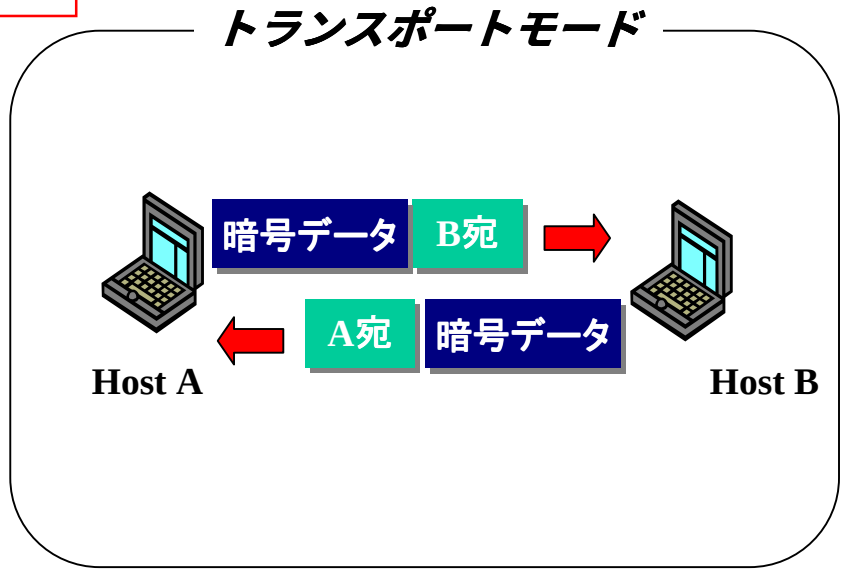


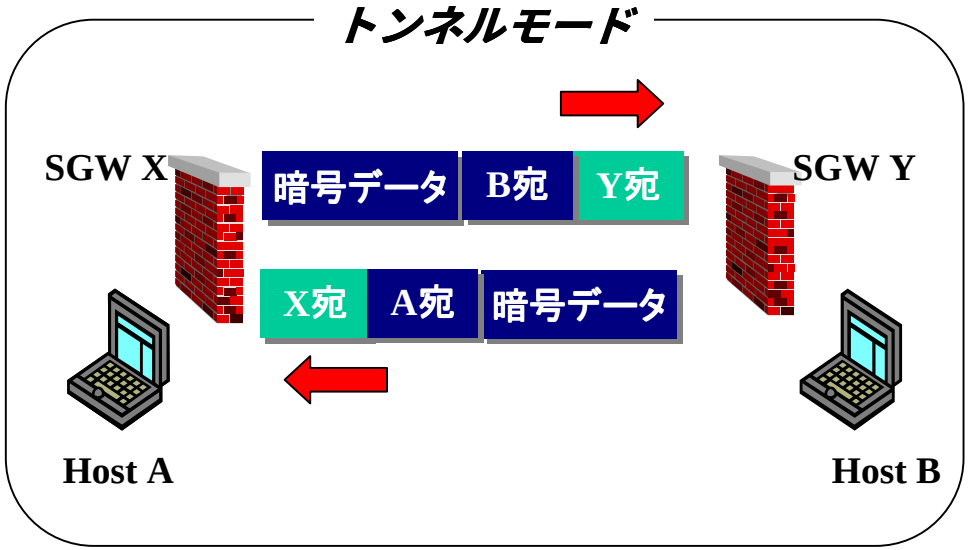
IPsec（IP Security Protocol）

- IPsecとは
  - IPにセキュリティ機能を持たせるためのプロトコル
  - 暗号と鍵管理を分離して標準化
  - 2つのモードと2つのヘッダ形式がある
  - IPv4とIPv6の両方で使用可能な技術
- セキュリティ機能
  - 認証
    - 鍵管理プロトコル（IKE）の相互認証機能
    - IPsec通信時のHMAC-MD5/HMAC-SHA1による認証機能
  - 改竄防止
    - IPsec通信時のHMAC-MD5/HMAC-SHA1による改竄防止機能
  - 暗号
    - DES-CBCによる暗号化（ほとんどが3DESをサポート）

2つのモード

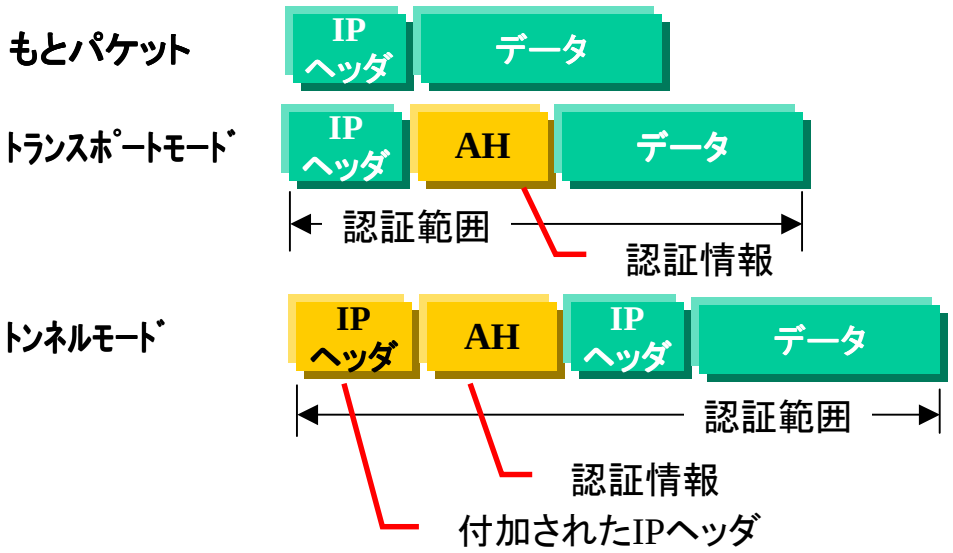
- トランスポートモード
  - データ部分だけが暗号/認証の対象
- トンネルモード
  - 元のIPパケットに新たなIPヘッダを付加する。元のIPパケットすべてが暗号/認証の対象

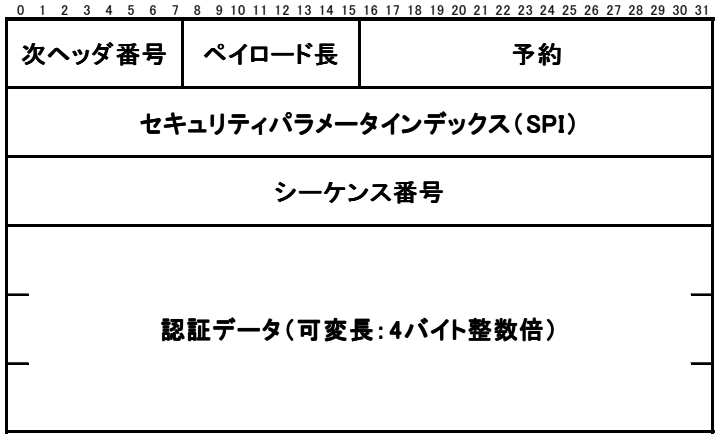




2つのヘッダ

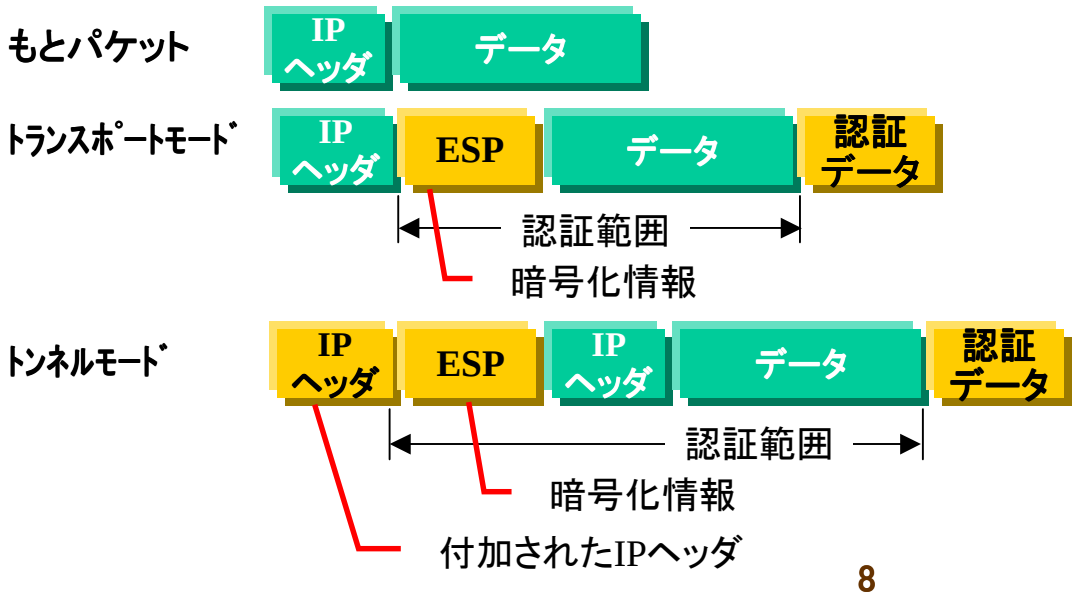
- AH(Authentication Header)
  - RFC2402
  - IP Protocol No = 51
  - 提供する機能
    - 送信元の認証と、データの完全性を確保
    - リプレイ攻撃防御機能(オプション)

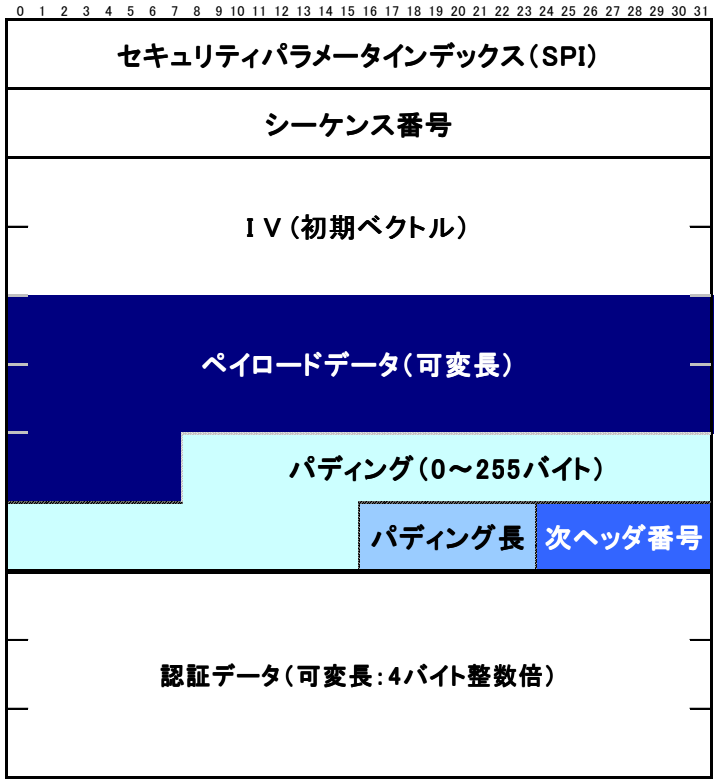




2つのヘッダ

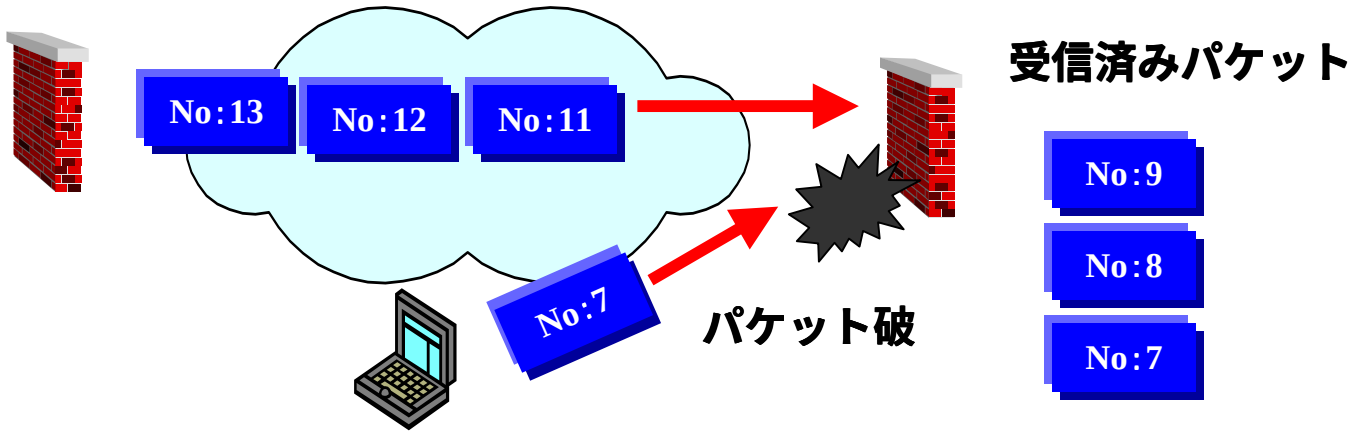
- ESP(Encapsulating Security Payload)
  - RFC2406
  - IP Protocol No = 50
  - 提供する機能
    - データの機密性(暗号)
    - 送信元認証とデータの完全性を確保
    - リプレイ攻撃防御機能





リプレイ攻撃防御機能

- リプレイ攻撃
  - 通信内容を記録しておき、あとで再生する攻撃
- IPsecのリプレイ攻撃に対する機能
  - 受信パケットのシーケンス番号を確認し、重複している場合は、そのパケットを破棄
  - シーケンス番号の確認は、リプレイ防御ウィンドウで行う。
  - シーケンス番号は32bit、一巡した場合はSAを無効とする。



IPsecのセキュリティポリシー

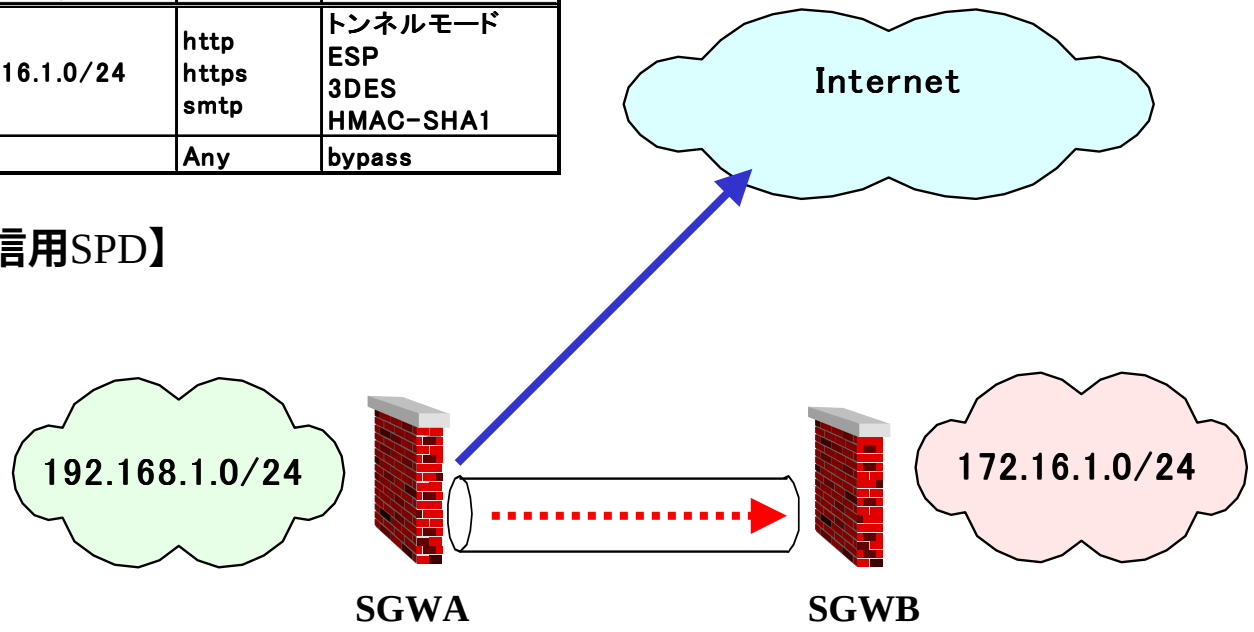
- セキュリティポリシー
  - IPパケットトラフィックに対し、IPsecを適用するルールを定義
    - パケット破棄（discard）
    - パケット通過（bypass）
    - IPsec適用（apply）
- セキュリティポリシーデータベース（SPD）
  - IPsecデバイスで設定されるセキュリティポリシーを格納するデータベース
  - 送信用と受信用の2つのデータベースを使用する。

IPsecのセキュリティポリシー

- セレクタ
  - セキュリティポリシーを定義する情報
  - 一般的には、送信元、宛先、プロトコル等を定義する。

順序	セレクタ			処理
	送信元	宛先	プロトコル	
1	192.168.1.0/24	172.16.1.0/24	http https smtp	トンネルモード ESP 3DES HMAC-SHA1
3	Any	Any	Any	bypass

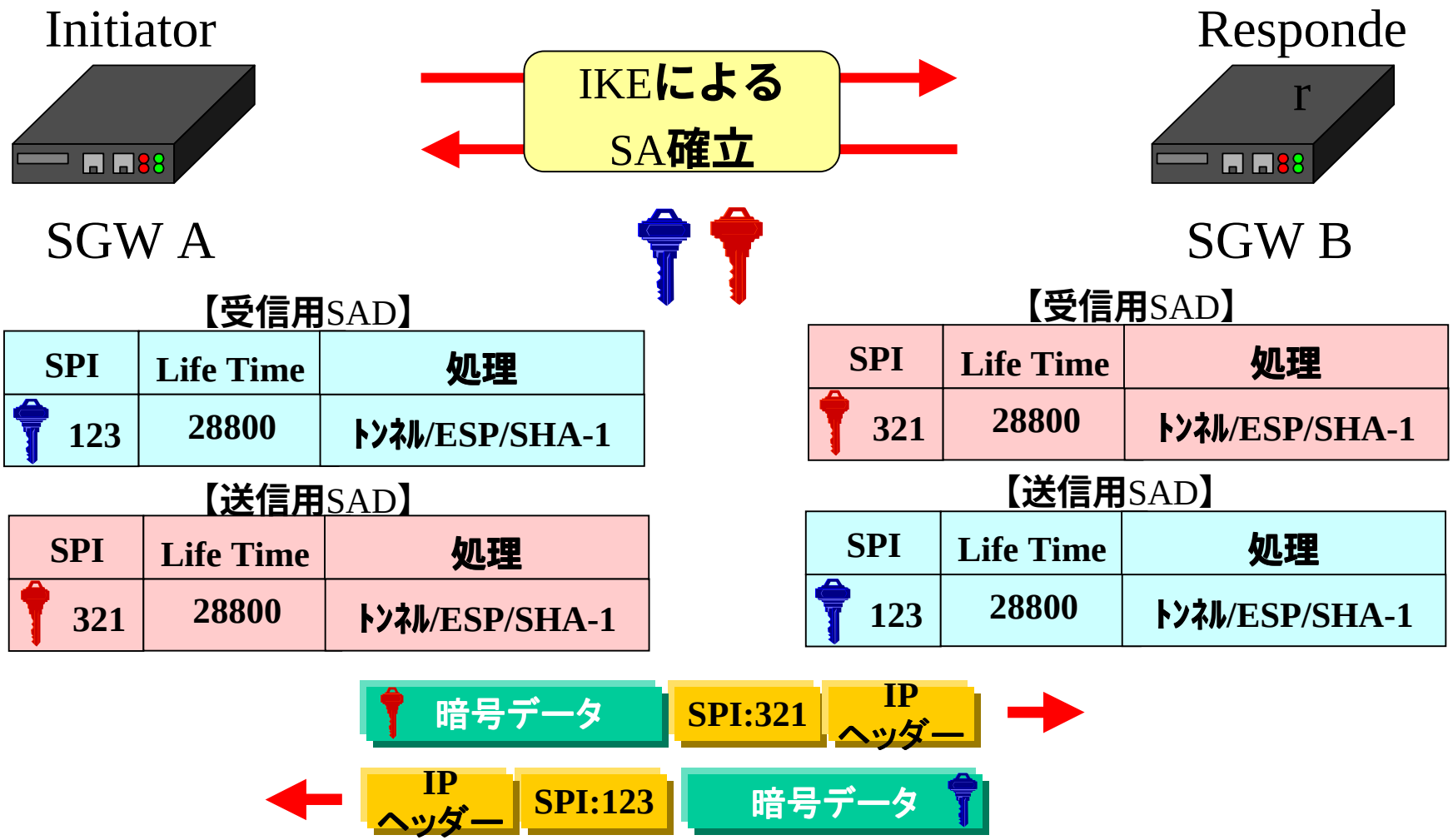
【SGWAの送信用SPD】



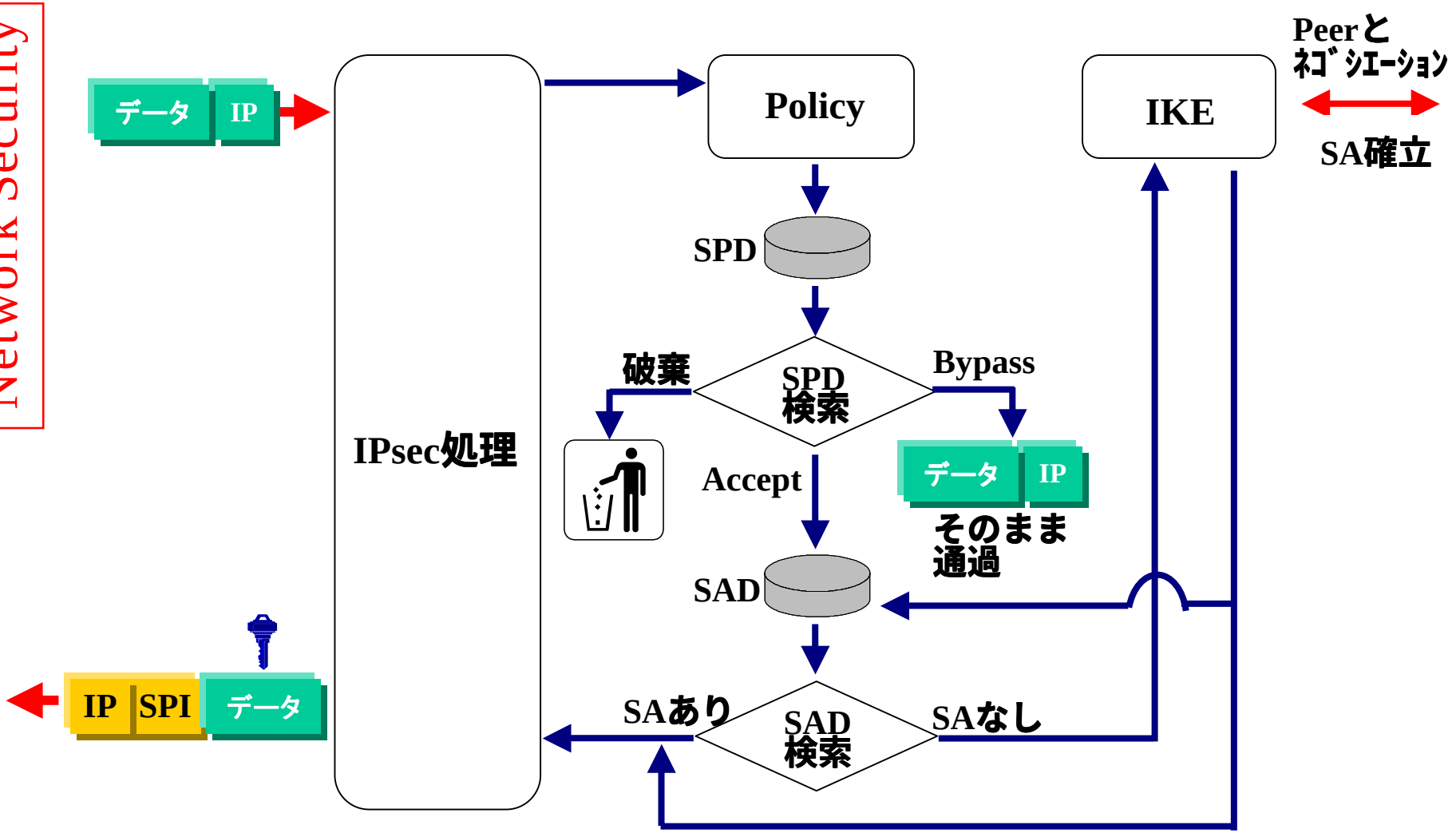
Security Association

- Security Association(SA)
  - 2者間でIPsec通信を実施する際に必要となる、暗号鍵情報や使用する暗号・認証アルゴリズム情報
  - IPsecのSAは送信用　と受信用のSAがある。
  - SAには有効期限がある。
  - IKEがSAを確立する。
- SPI（Security Parameter Index）
  - SAを検索するための識別子
- SAD（Security Association Database）
  - 確立したSAを格納しておくデータベース
  - 送信用と受信用の2つのデータベースを使用する。

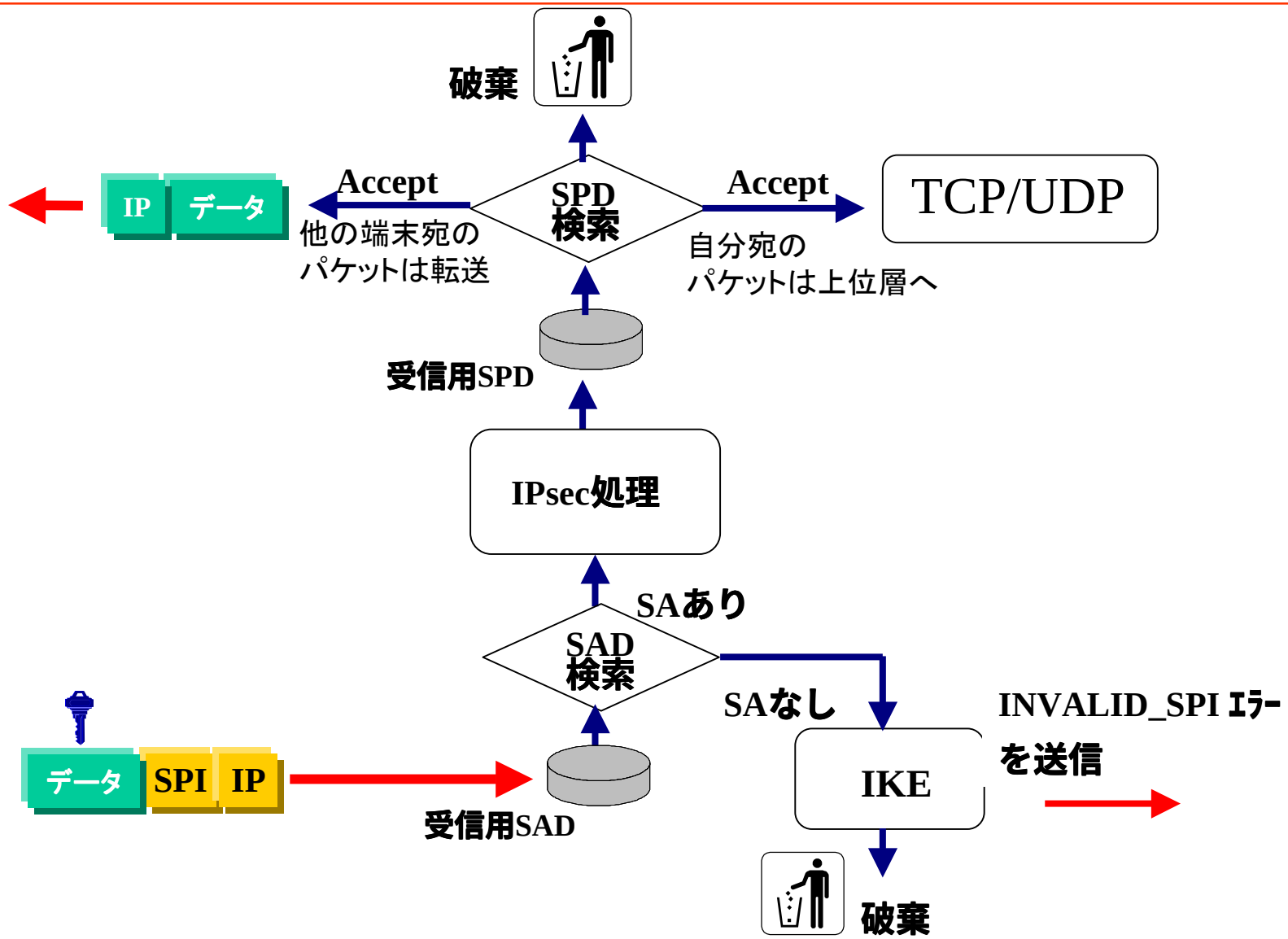
SA，SPI，SADの関係



IPsec処理の流れ（送信時）



IPsec処理の流れ（受信時）



IKE(Internet Key Exchange)の概要

IKEの役割

- IKEの提供する機能
  - 認証
    - 秘密鍵(SA)を共有する相手を認証する。
    - 認証方式は下記の4種類
      - 既知共有秘密鍵(Pre-Shared Secret Key)認証方式
      - デジタル署名認証方式
      - 公開鍵暗号認証方式
      - 改良型公開鍵認証方式
  - SAの確立と管理
    - IPsec通信に先立ち、秘密鍵(SA)を確立する。
    - 有効期間を管理(有効期間が切れる前に再度SA確立)

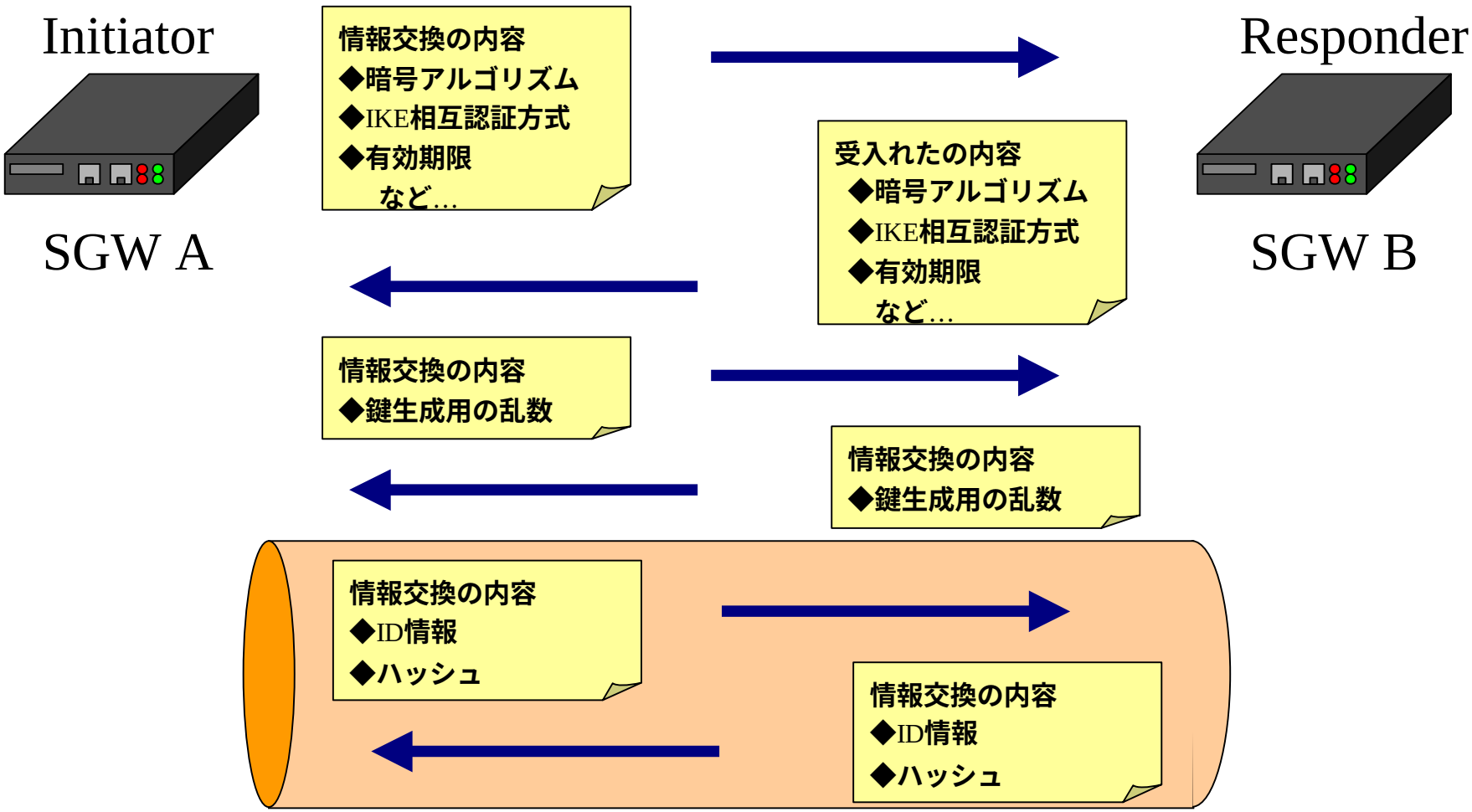
IKEの機能

- Phase1
  - 役割
    - ISAKAMP SAの確立
      - ISAKAMP SAの折衝
      - 共有秘密鍵の生成
      - 認証
    - Phase2（IPsec SA）を安全に生成するための通信路の確立
  - 2つのモード
    - メインモード
      - 計6回のメッセージ送受信で、ISAKMP SAを確立
      - 実装必須
    - アグレッシブモード
      - 計3回のメッセージ送受信で、ISAKMP SAを確立
      - 実装はオプション

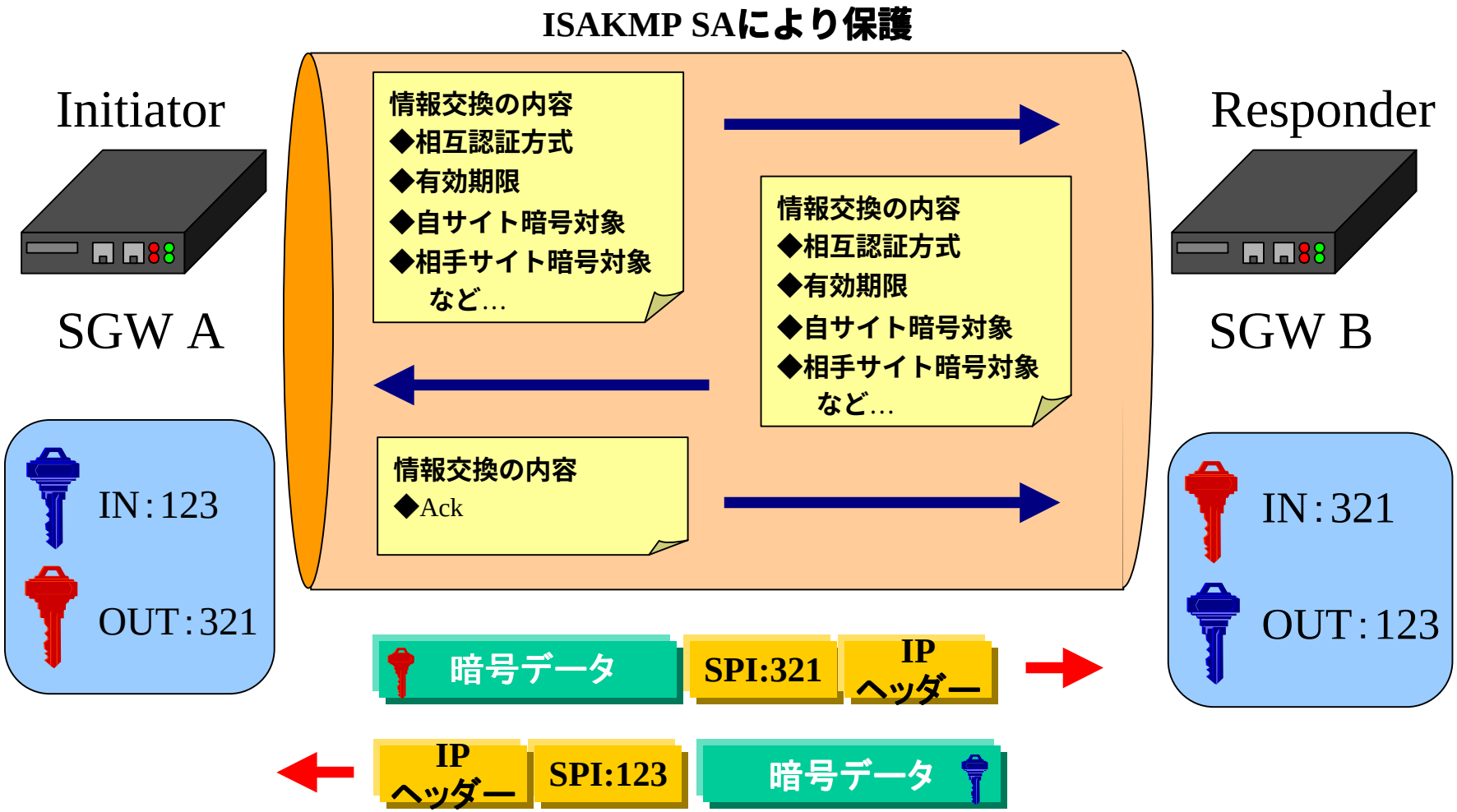
IKEの機能

- Phase2
  - 役割
    - IPsec SAの確立
      - セキュリティプロトコルの折衝
      - 共有秘密鍵の生成
  - モードは1つ
    - クイックモード
      - 計3回のメッセージ送受信で、IPsec SAを確立

IKEの動作（Phase1）



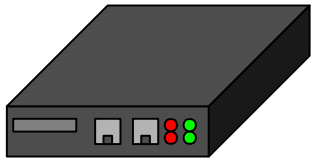
IKEの動作（Phase2）



IKE Phase1ネゴシエーションの詳細

パラメータ折衝(Pre-Shared Key)

Initiator



SGW A

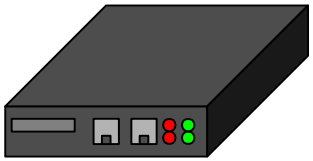
◆暗号アルゴリズム：3DES
◆Hashアルゴリズム：SHA1
◆認証方式　　：Pre-Sh
◆DHグループ　　：5
◆有効期限　　：24H

◆暗号アルゴリズム：DES
◆Hashアルゴリズム：MD5
◆認証方式　　：Pre-Sh
◆DHグループ　　：1
◆有効期限　　：24H

IKE SAを確立するために使用するパラメータを提案

（複数提案可能）

Responder



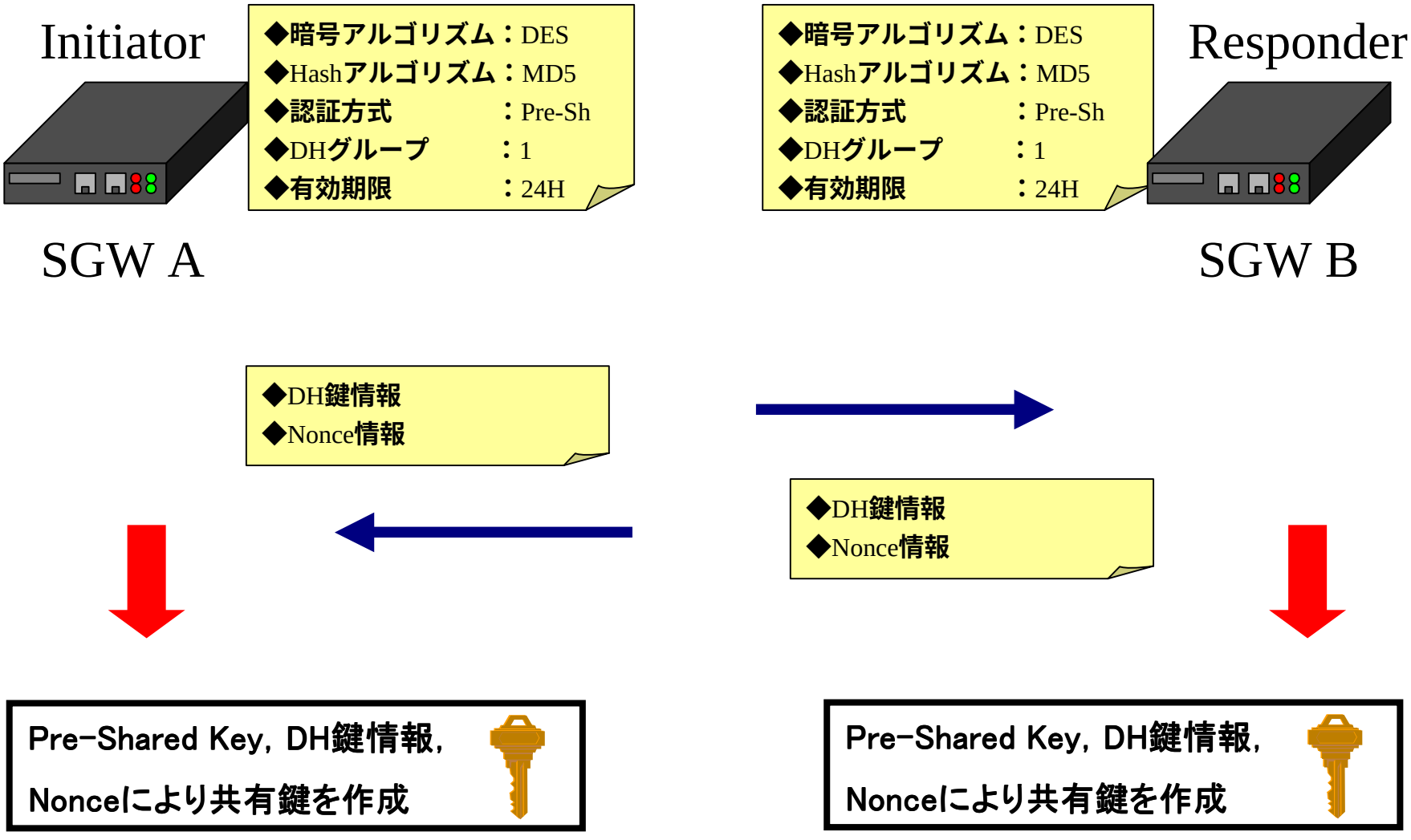
SGW B

受入れたパラメータを回答

（複数回答不可）

◆暗号アルゴリズム：DES
◆Hashアルゴリズム：MD5
◆認証方式　　：Pre-Sh
◆DHグループ　　：1
◆有効期限　　：24H

鍵材料の交換(Pre-Shared Key)



認証 Ini → Res (Pre-Shared Key)

SKEYIDを作成

SKEYID=PRF(pre-shared secret key,Ni | Nr)

認証に使用されるHASH_I

HASH_I=PRF(SKEYID,g^i|g^r|CKY_I|CKY_R|SAp|ID_I)

◆ID情報
◆HASH

→ データ復号化した後、IDとHASH_Iを取出す。

SKEYIDを作成

SKEYID=PRF(pre-shared secret key,Ni | Nr)

認証に使用されるHASH_I

HASH_I=PRF(SKEYID,g^i|g^r|CKY_I|CKY_R|SAp|ID_I)

受信したHASH_Iと計算したHASH_Iと一致したら、鍵交換とInitiatorの認証が成功したことになる

PRF：疑似乱数関数
Ni：InitiatorのNonce情報／Nr：responderのNonce情報
g^xy：DHによって作成された共有鍵
g^i:：InitiatorのDH公開情報／g^r：ResponderのDH公開情報
CKY_I：Initiatorのｸｯｷｰ情報／CKY_R：Responderのｸｯｷｰ情報
SAp：SAﾍﾟｲﾛｰﾄﾞ情報

認証 Res → Ini (Pre-Shared Key)

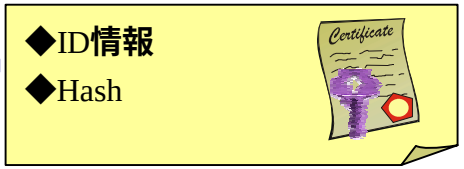
SKEYIDを作成

SKEYID=PRF(pre-shared secret key,Ni | Nr)

認証に使用されるHASH_I

HASH_R=PRF(SKEYID,g^i|g^r|CKY_I|CKY_R|SAp|ID_R)

データ復号化した後、IDとHASH_Iを取出す。



SKEYIDを作成

SKEYID=PRF(pre-shared secret key,Ni | Nr)

認証に使用されるHASH_I

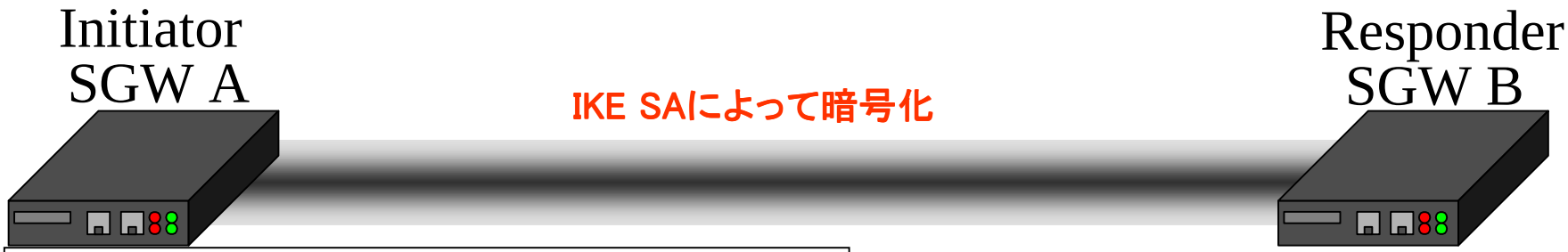
HASH_I=PRF(SKEYID,g^i|g^r|CKY_I|CKY_R|SAp|ID_I)

受信したHASH_Iと計算したHASH_Iと一致したら、鍵交換とResponderの認証が成功したことになる

PRF：疑似乱数関数
Ni：InitiatorのNonce情報／Nr：responderのNonce情報
g^xy：DHによって作成された共有鍵
g^i:：InitiatorのDH公開情報／g^r：ResponderのDH公開情報
CKY_I：Initiatorのｸｯｷｰ情報／CKY_R：Responderのｸｯｷｰ情報
SAp：SAﾍﾟｲﾛｰﾄﾞ情報

IKE Phase2ネゴシエーションの詳細

パラメータ提案



認証済み鍵素材

SKEYID_d = PRF(SEYID , g^xy | CKY-I | CKY-R | 0)
SKEYID_a = PRF(SEYID , SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = PRF(SEYID , SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Phase2 のStage1で使用するHASH1

HASH1 = PRF (SKEYID_a, M-ID | SA | Ni [| KE] [| IDci | IDcr])

◆暗号アルゴリズム：3DES
◆認証アルゴリズム：SHA1
◆DHグループ　　：5
◆有効期限　　：8H

◆暗号アルゴリズム：DES
◆認証アルゴリズム：MD5
◆DHグループ　　：1
◆有効期限　　：8H

IPsec SAを確立するために使用するパラメータを提案

認証情報として、HASH1
共有鍵作成のため、DH公開情報
乱数情報も合わせて送信

パラメータ選択

受信したHash1の認証確認

Phase2 のStage2で使用するHASH2

HASH1 = PRF (SKEYID_a, M-ID | Ni | SA | Nr [| KE] [| IDci | IDcr])

受入れたパラメータを回答

認証情報として、HASH2
共有鍵作成のため、DH公開情報
乱数情報も合わせて送信

◆暗号アルゴリズム：DES
◆認証アルゴリズム：MD5
◆DHグループ　　：1
◆有効期限　　：8H

IPsec SAの確立

◆暗号アルゴリズム：DES
◆認証アルゴリズム：MD5
◆DHグループ　　：1
◆有効期限　　：8H

◆暗号アルゴリズム：DES
◆認証アルゴリズム：MD5
◆DHグループ　　：1
◆有効期限　　：8H

受信したHash2の認証確認

Phase2 のStage3で使用するHASH3
HASH1 = PRF (SKEYID_a, 0 | M-ID | Ni | Nr)

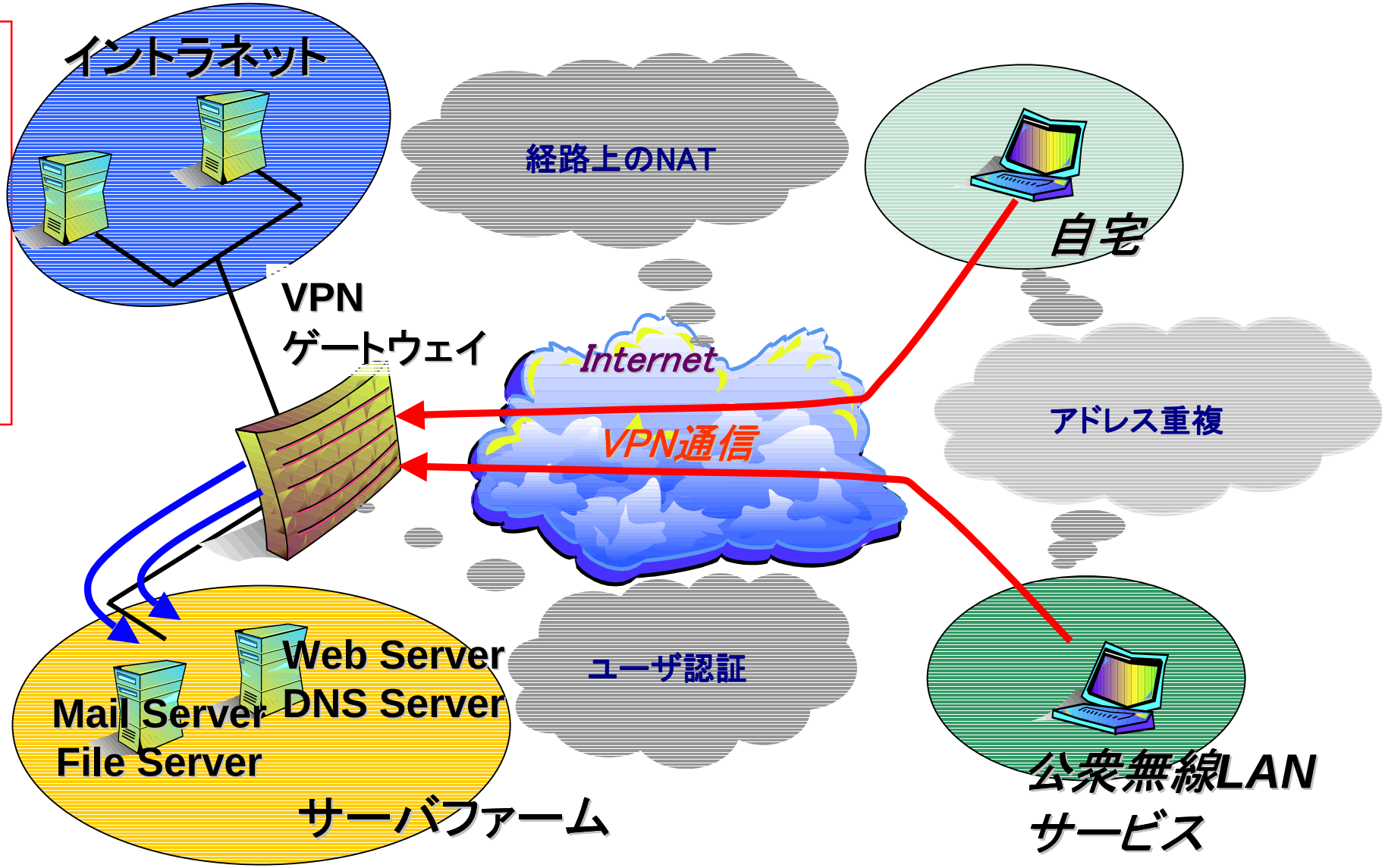
Initiatorの生存証明のために
Hash3を送信

受信したHash3の認証確認

Remote Access 環境への対応

INTERNET WEEK 2003
2 - 5 December 2003 Yokohama / パシフィコ横浜

IPsecを リモートアクセス環境で使うと…

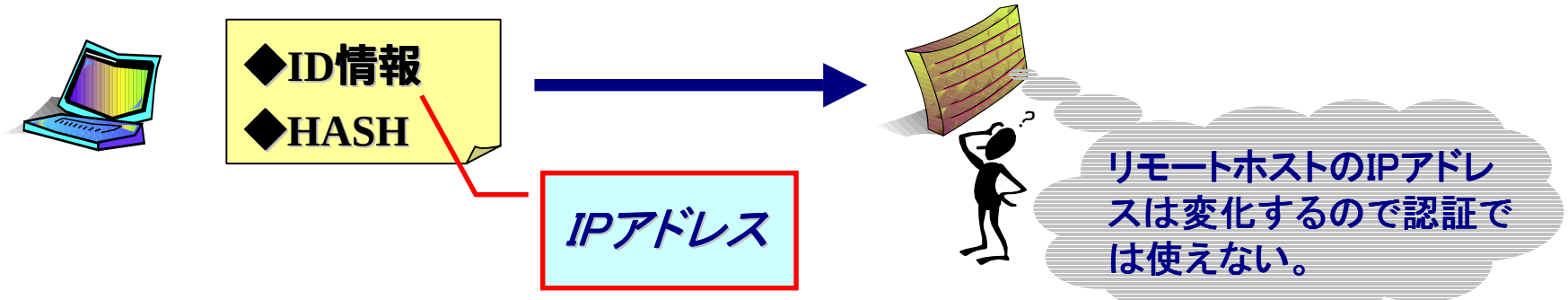


IPsecを リモートアクセス環境で使うと…

- 検討すべき問題点
  - 認証に関する問題
    - リモートユーザを認証するためのしくみ
  - NATに関する問題
    - 多くの公衆無線LANサービスはPrivate IPアドレスのため、経路上にNAT機器が介在する
  - IPアドレスに関する問題
    - Private IPアドレスの重複
  - フラグメントに関する問題
    - VPNゲートウェイでフラグメント化されたパケットがVPNクライアントまで到達しない

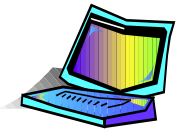
認証に関する問題

- 問題点1
  - ゲートウェイ間のIPsec通信で最も使用されている、Mainモードで Pre-Shared認証を使用する方法はリモートクライアントでは使用できない。
- 原因
  - MainモードのPre-Sharedでは、認証の際に通信相手のIPアドレス情報を使用する。リモートクライアントはIPアドレスを固定できないため、MainモードのPre-Sharedは使用できない。

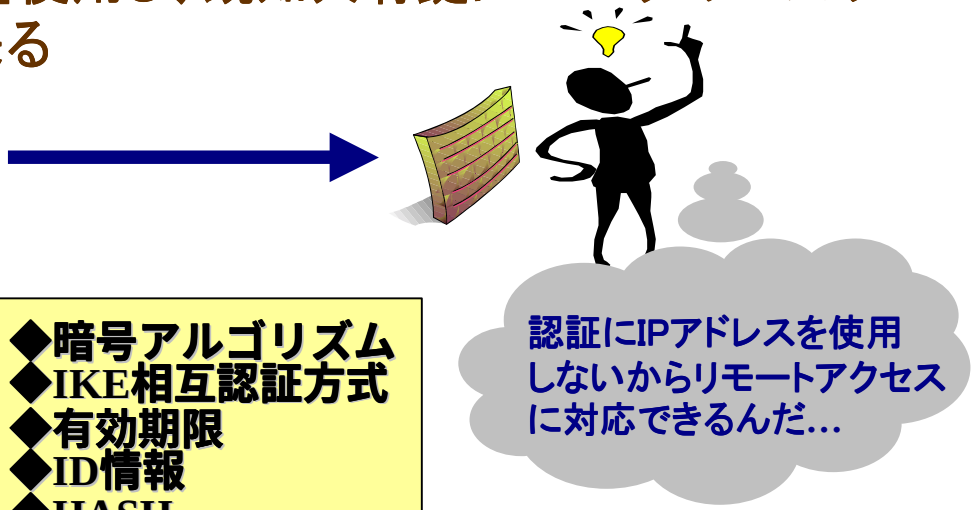


認証に関する問題

- 解決策
  - Aggressiveモードを使用する。
    - ID情報にIPアドレスを使用しなくても良い
    - ID情報にユーザ情報を使用し、既知共有鍵にユーザのパスワードを使用する事が出来る



◆暗号アルゴリズム
◆IKE相互認証方式
◆有効期限
◆ID情報



ユーザ情報

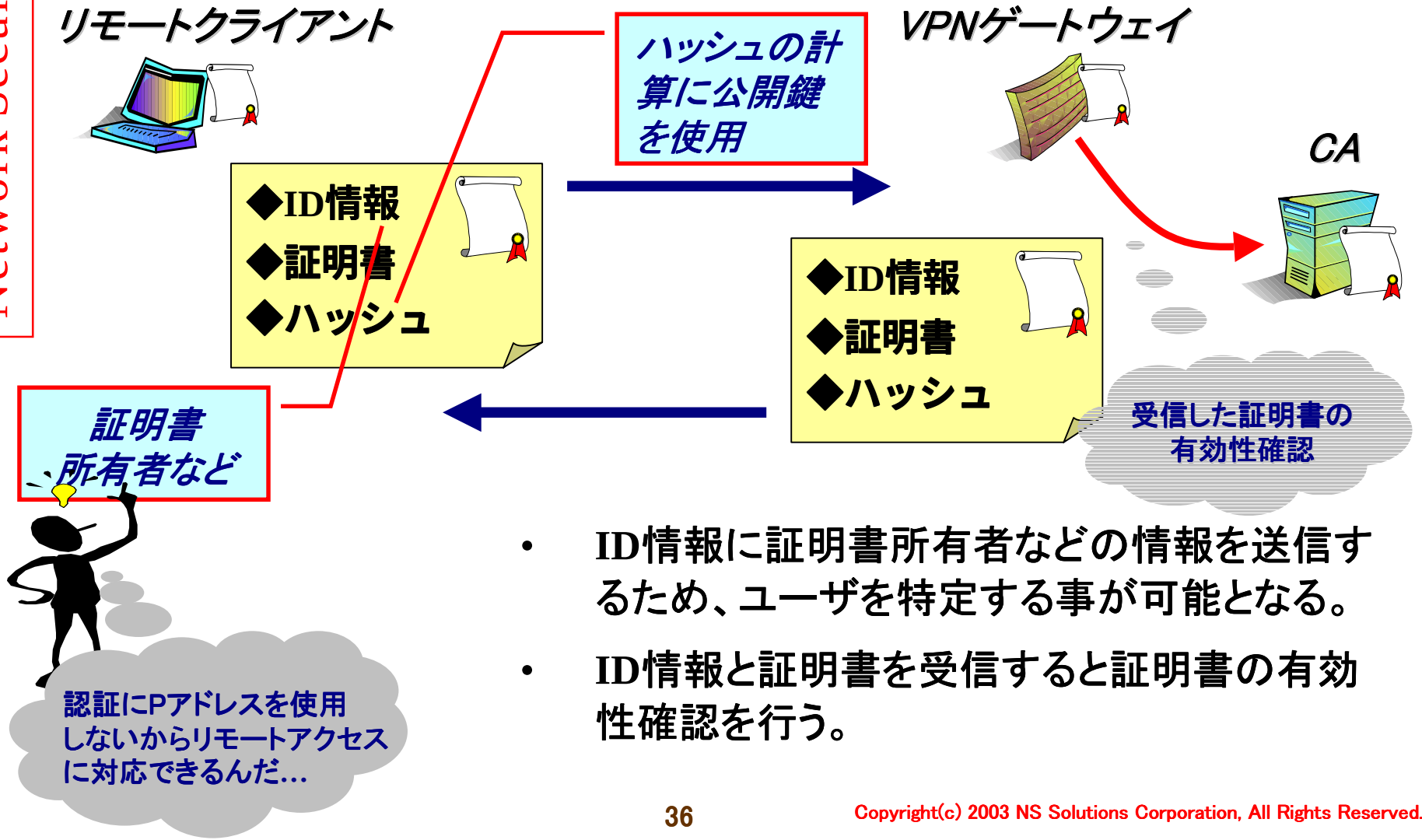
◆暗号アルゴリズム
◆IKE相互認証方式
◆有効期限
◆ID情報
◆HASH

◆暗号アルゴリズム
◆IKE相互認証方式
◆有効期限
◆ID情報
◆HASH

HASH計算時にユーザのパスワードを使用

認証に関する問題

- 解決策　電子署名認証方式

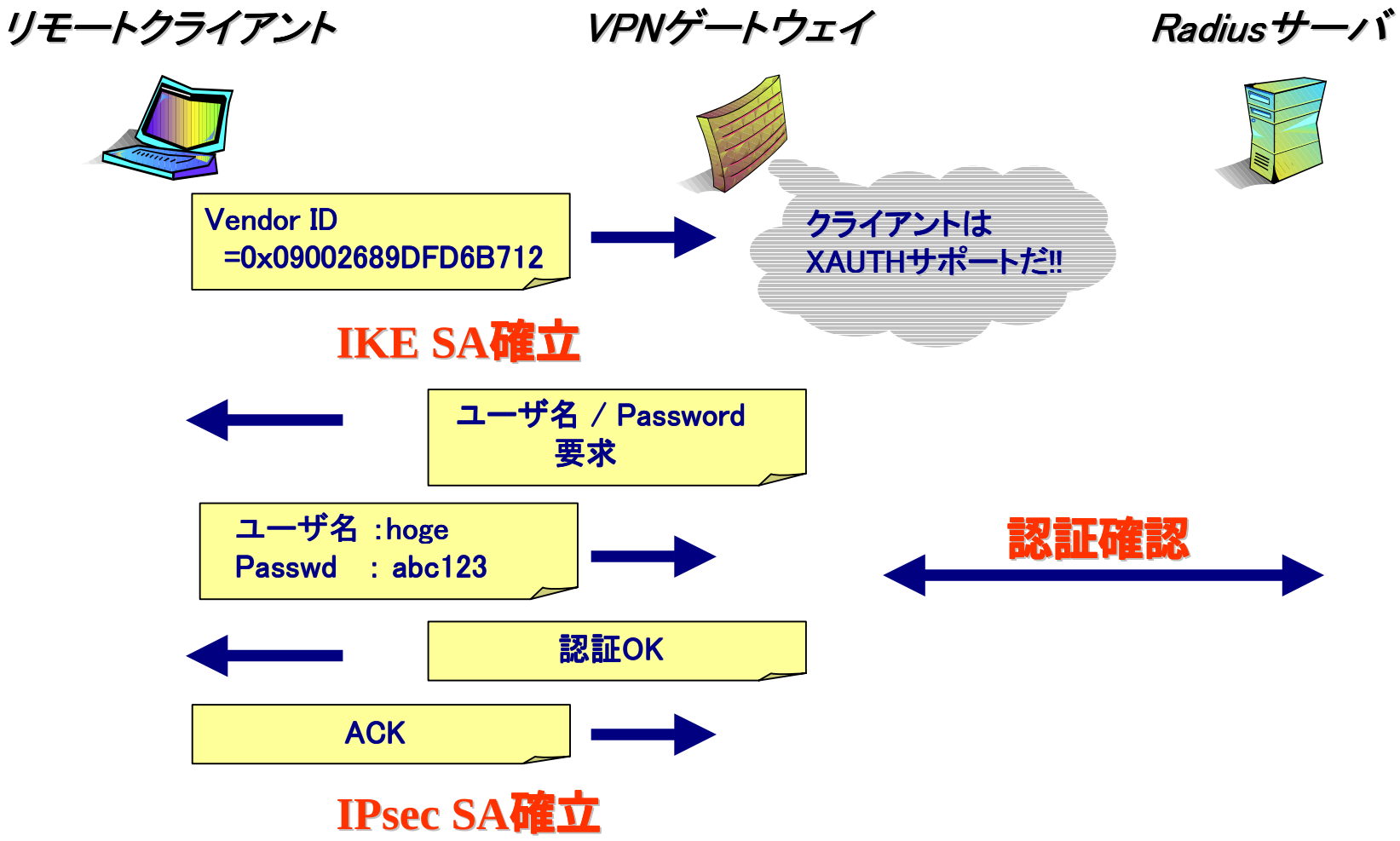


- ID情報に証明書所有者などの情報を送信するため、ユーザを特定する事が可能となる。
- ID情報と証明書を受信すると証明書の有効性確認を行う。

認証に関する問題

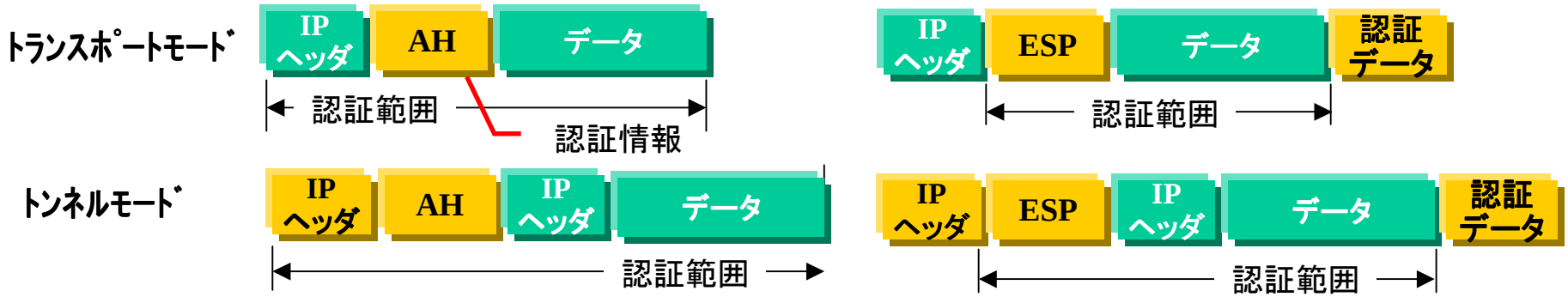
- 問題点2
  - IPsecは基本的に、リモートユーザを認証する機能を持っていない。
- 対応策
  - XAUTHまたは、Hybrid Authをサポートした製品を使用する。
    - XAUTH, Hybrid AuthともInternet DraftからExpire
    - ただし、多くのIPsec機器およびClientソフトはXAUTHをサポートしている
    - Hybrid Authをサポートしている製品は少数
    - XAUTH, Hyblid Auth ともに、Radius, One Time Password, S/Keyなどが使用可能

認証に関する問題
～XAUTH使用時のﾈｺﾞｼｴｰｼｮﾝ～



NATに関する問題

- 問題点
  - AHは、IPヘッダが認証範囲に入っているため、NATには対応できない。
  - ESPは、IPヘッダのすぐ後に、ESPヘッダがあるため、NAPT（Network Address Port Translation）に対応できない。（1対1のNATには対応可能）

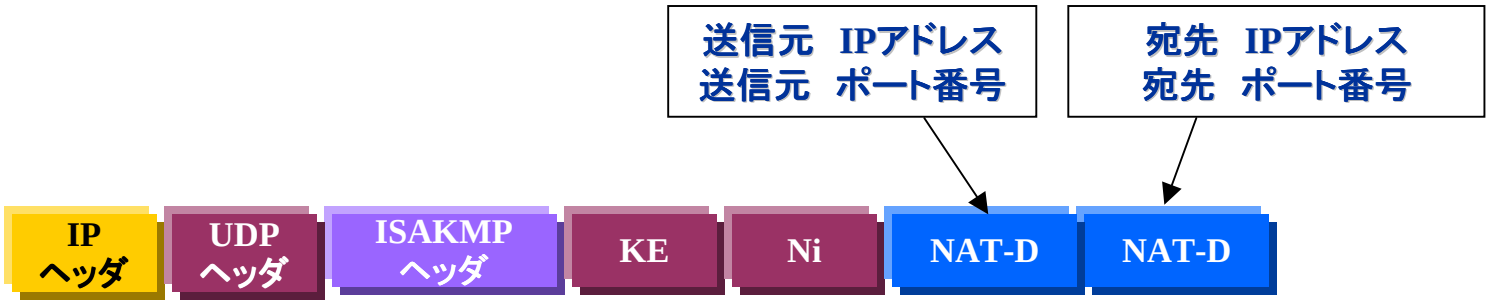


AHはIPヘッダが認証範囲にふくまれるからNATがダメなんだ

ESPのトンネルモードはIPヘッダ直後にESPヘッダが来るからNATがダメなんだ

NATに関する問題

- 解決策
  - NAT Traversal（NAT-T）をサポート製品を使用する。
    - イニシエータはNAT-Dペイロードに始点IPアドレス/ポート番号・終点IPアドレス/ポート番号を埋め込んで送信する。レスポンダはNAT-Dペイロードの中のデータと実際のIPアドレス・ポートを比較してNATの有無を検知する

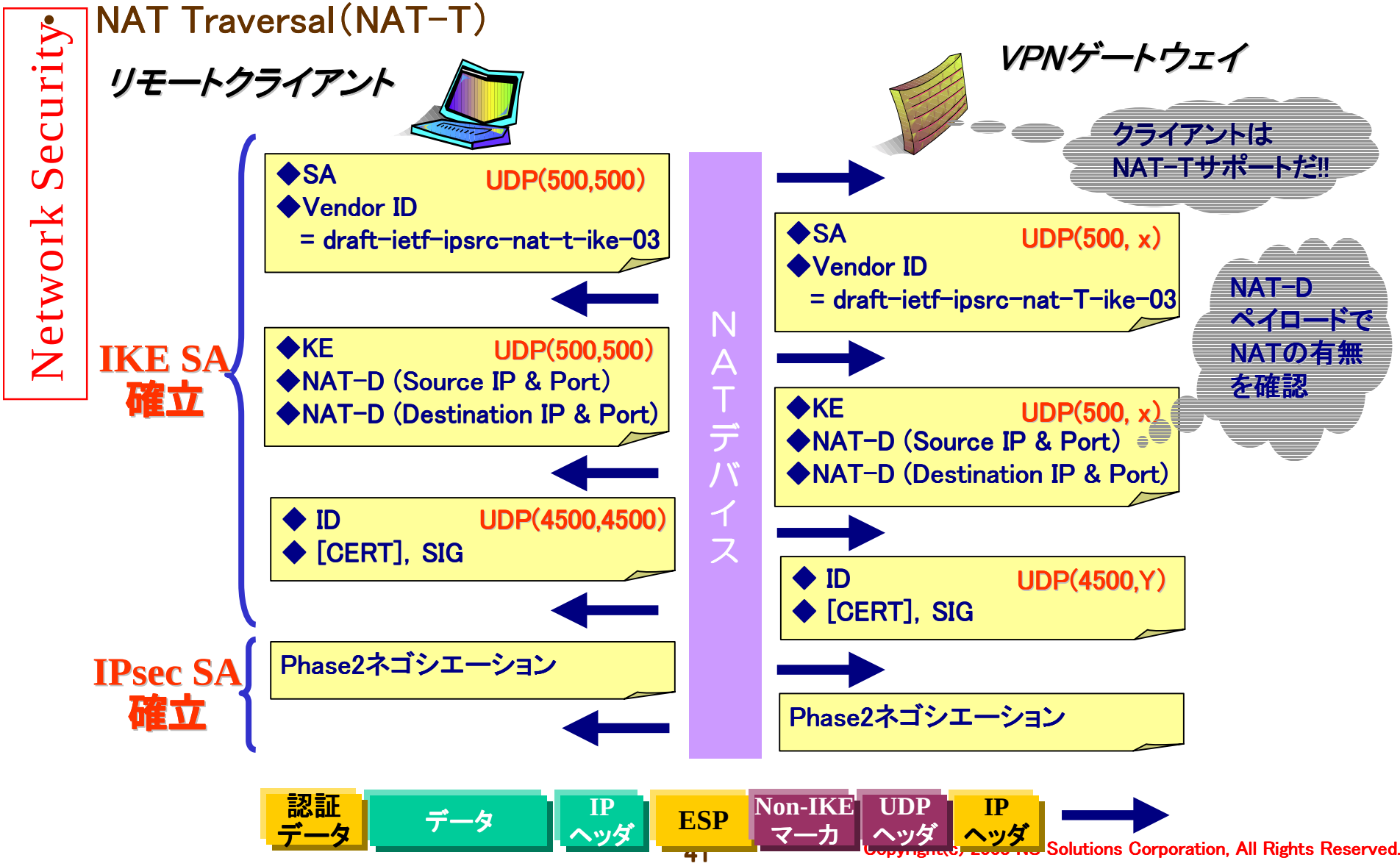


    - IPsecパケットは、『UDP Encapsulation of IPsec Packet』でUDP Encapsulationされる。
    - NAT-Tのドラフトバージョンが異なると、NAT-T対応製品同士でも接続は不可能（要注意!!）

NATに関する問題

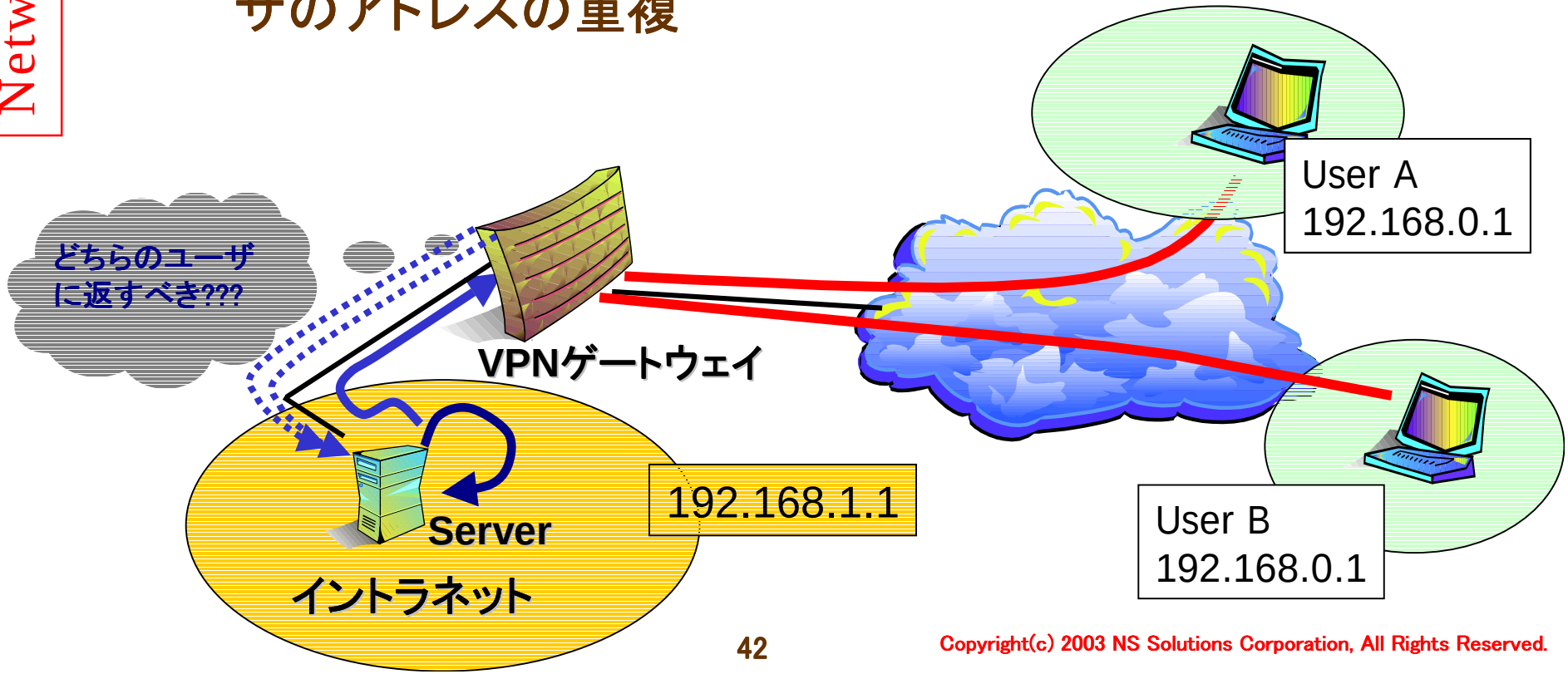
Network Security

NAT Traversal（NAT-T）



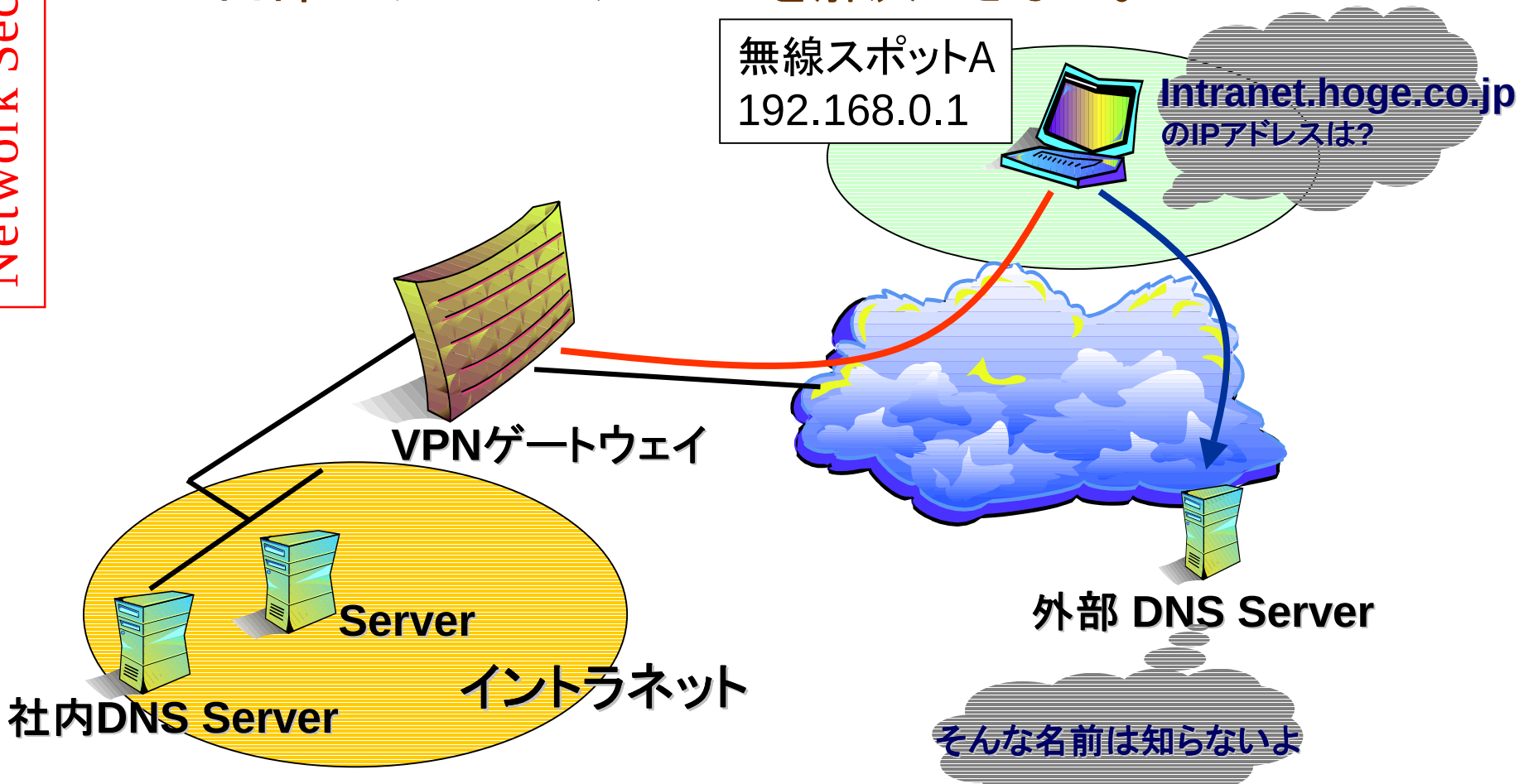
IPアドレスに関する問題

- 問題点
  - リモートアクセスユーザのアドレスと、社内のネットワークの重複
  - リモートアクセスユーザAとリモートアクセスユーザBユーザのアドレスの重複



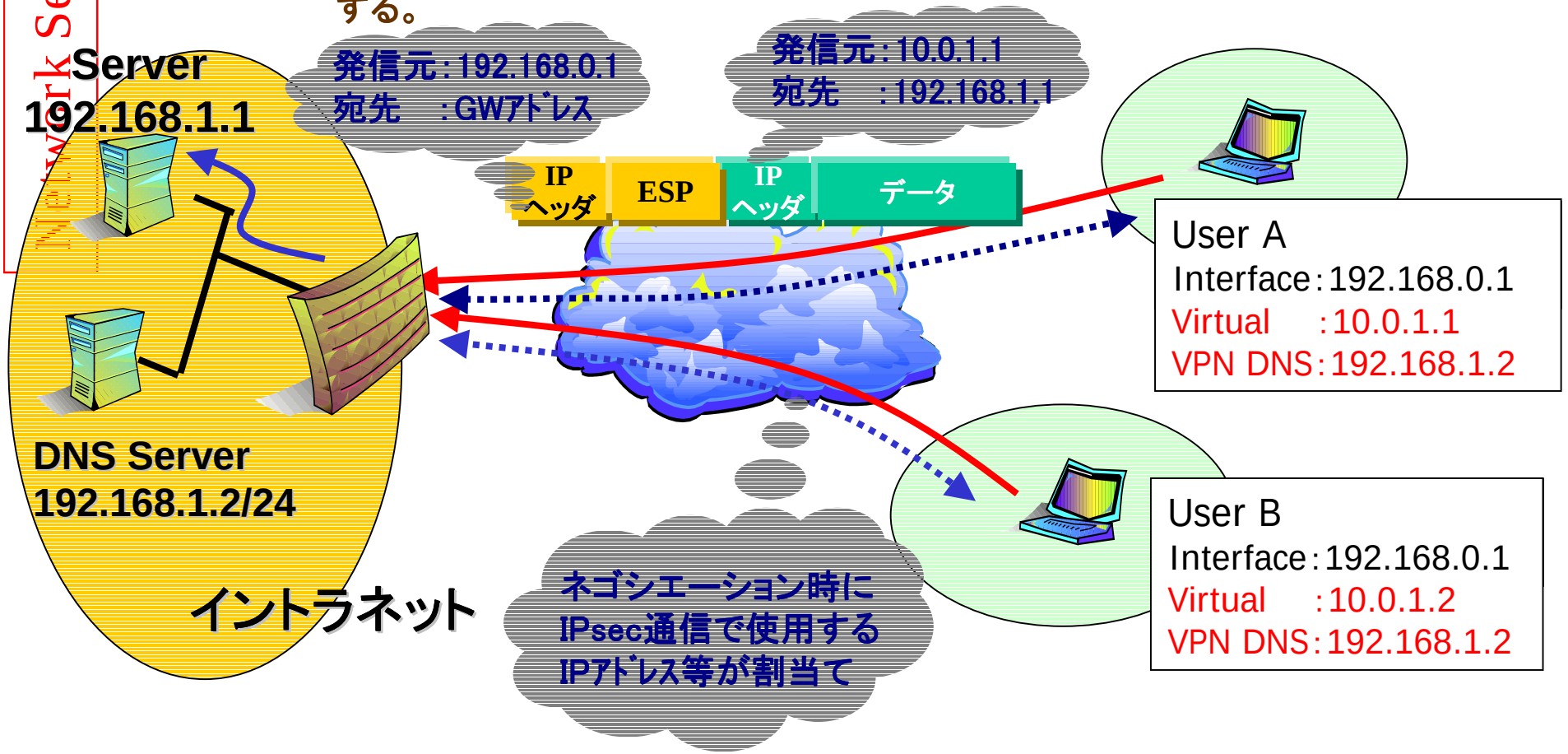
IPアドレスに関する問題

- 外部のDNSサーバを参照してしまう
  - 内部のサーバのアドレスを解決できない。



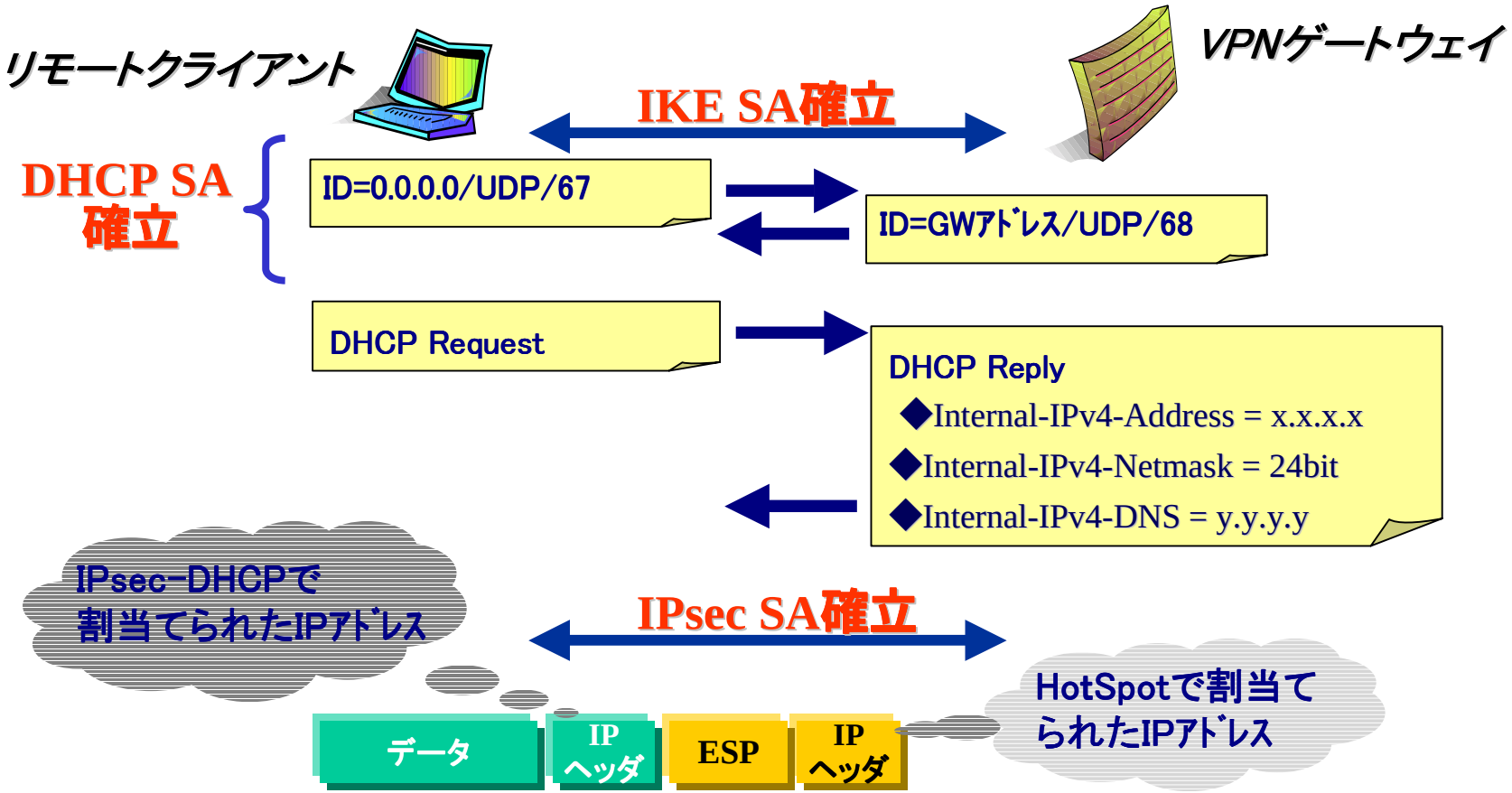
IPアドレスに関する問題

- 解決策
  - VPNゲートウェイから、VPN通信用のIPアドレスを割当てる。
    - IPsec-DHCPまたは、ISAKMP Configuration Methodをサポートする製品を使用する。



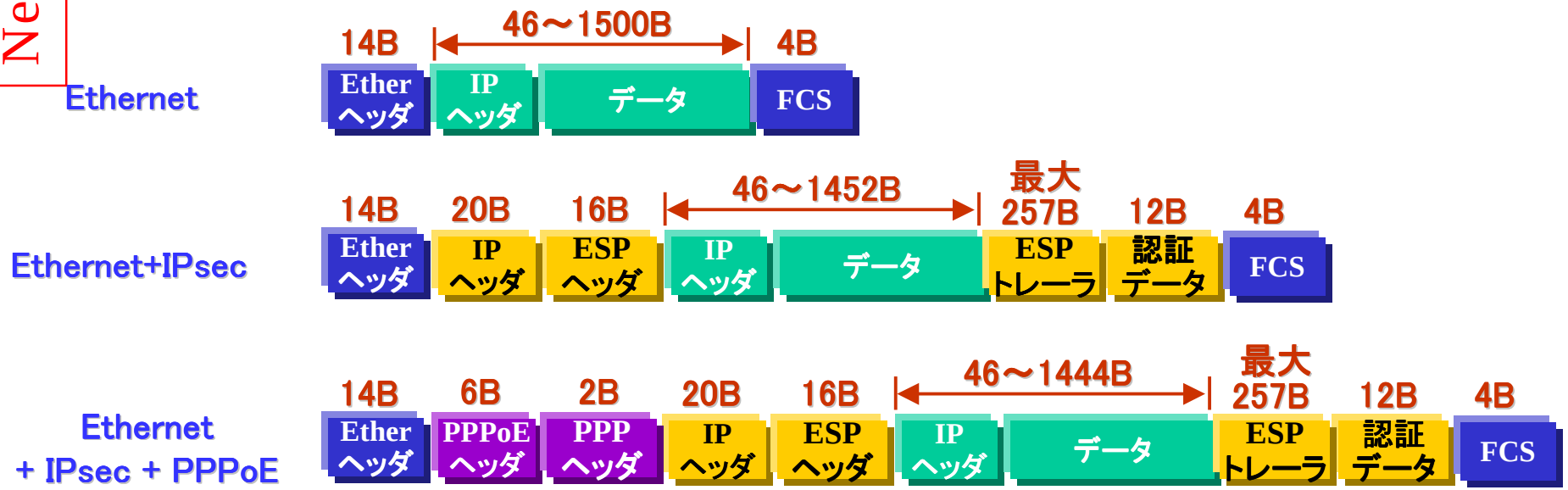
IPアドレスに関する問題

- IPsec-DHCP
  - 2003年 1月 RFC 3456で標準化
  - Phase2でDHCP用のSAを確立する。

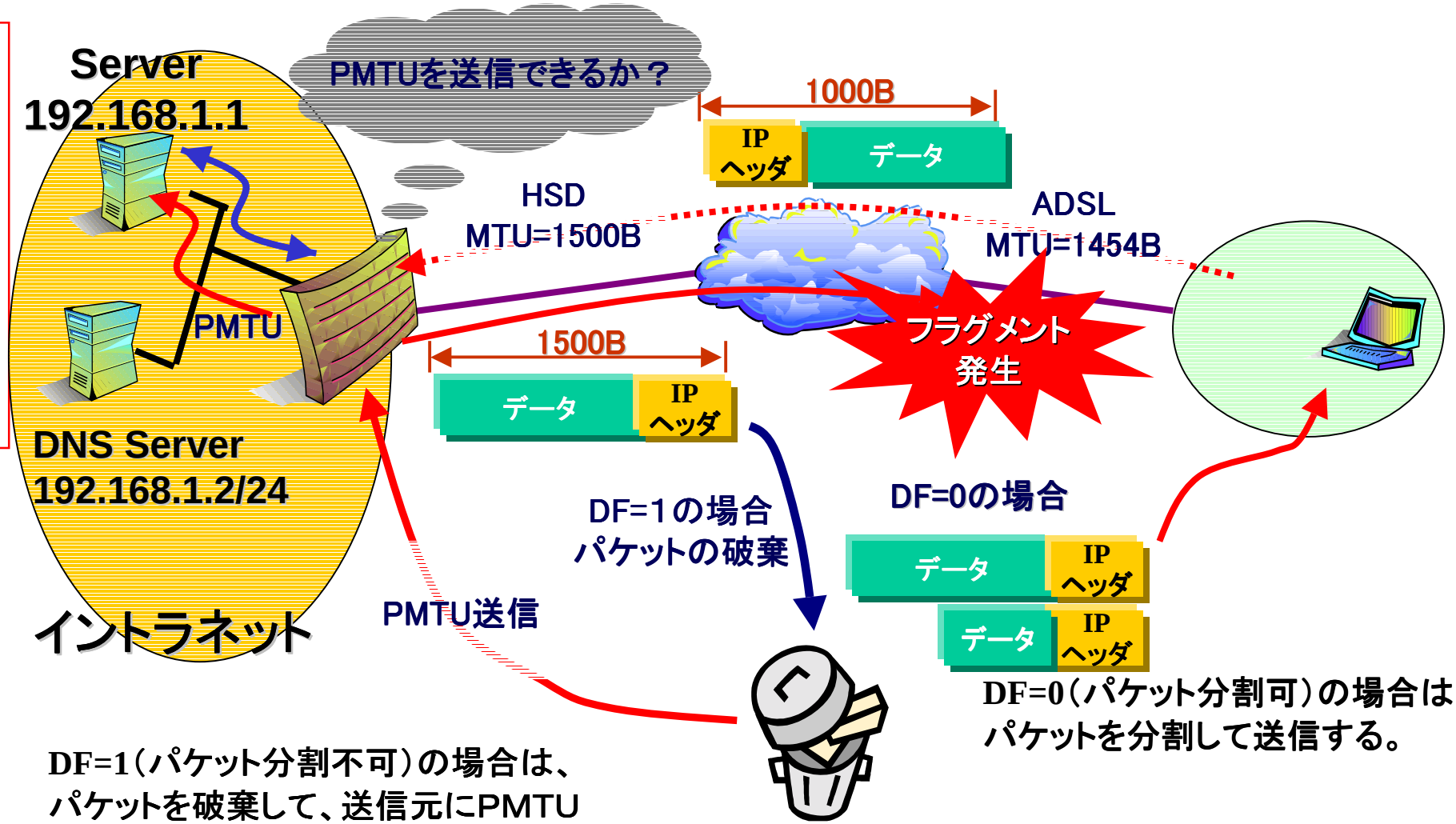


フラグメントに関する問題

- フラグメントに関する問題
  - IPsec使用により、ヘッダ等の情報追加でMTUを越える可能性が高くなる。
  - HotSpotではADSLが多く使用されているので、PPPoEヘッダ等の追加もあるので、更にフラグメントが発生し易い状態になる。



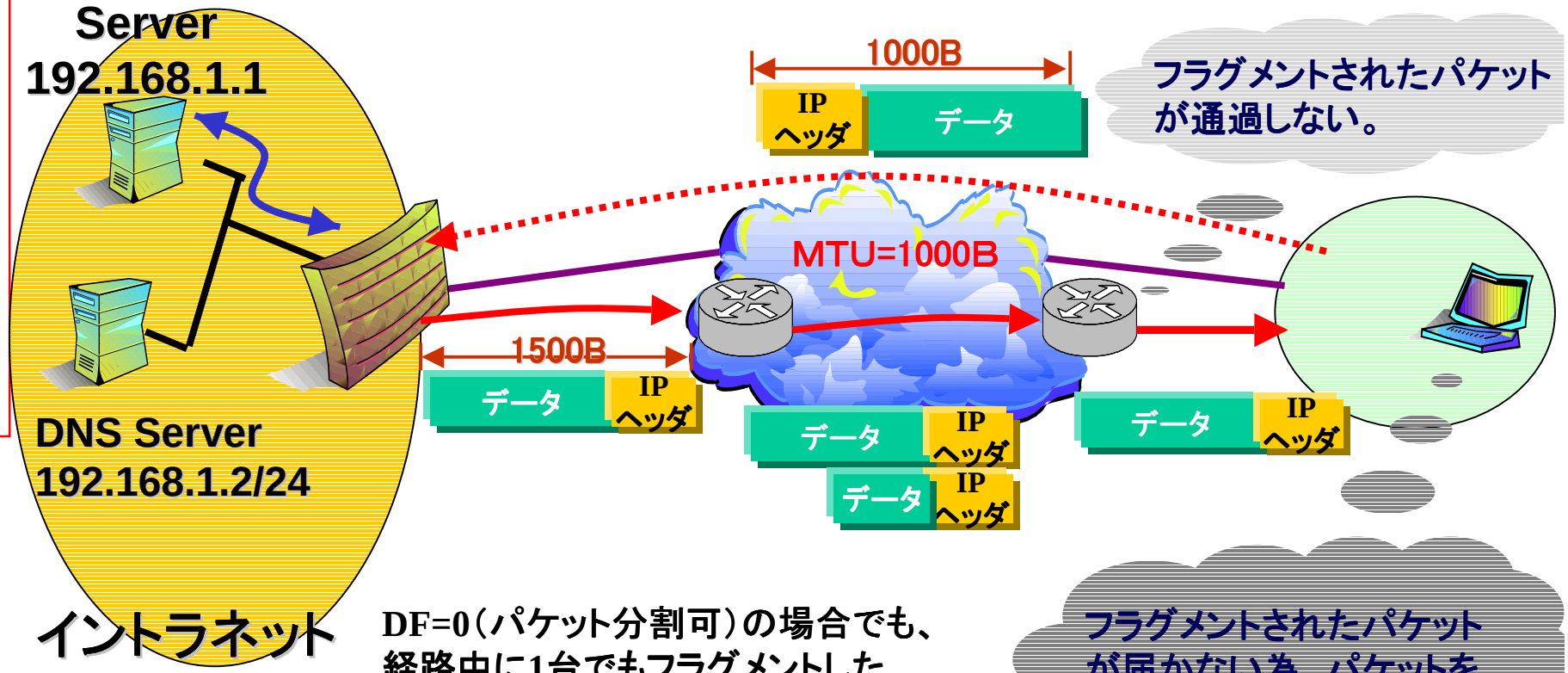
フラグメントに関する問題



DF=1（パケット分割不可）の場合は、パケットを破棄して、送信元にPMTUを送信する。

DF=0（パケット分割可）の場合はパケットを分割して送信する。

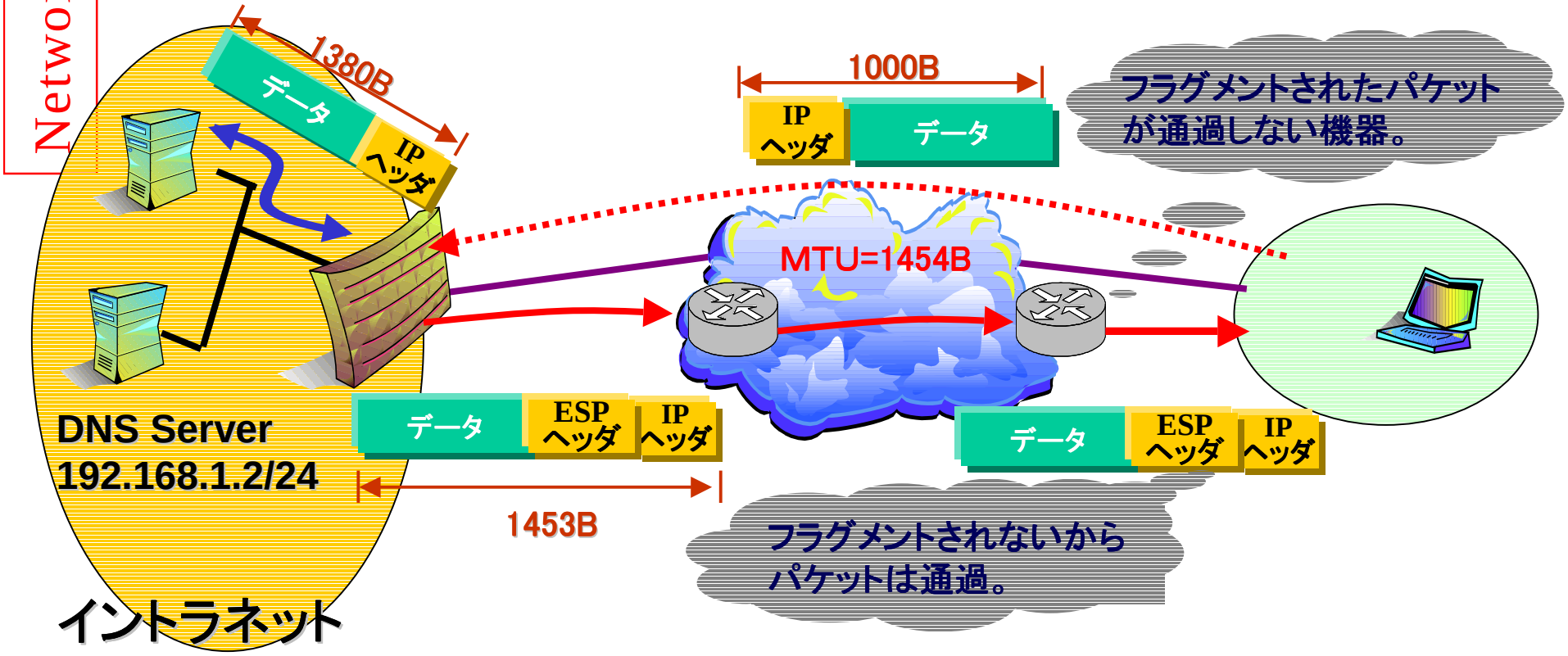
フラグメントに関する問題



DF=0（パケット分割可）の場合でも、経路中に1台でもフラグメントしたパケットを通過させられない機器があると、クライアント側からみると通信不能状態となる。

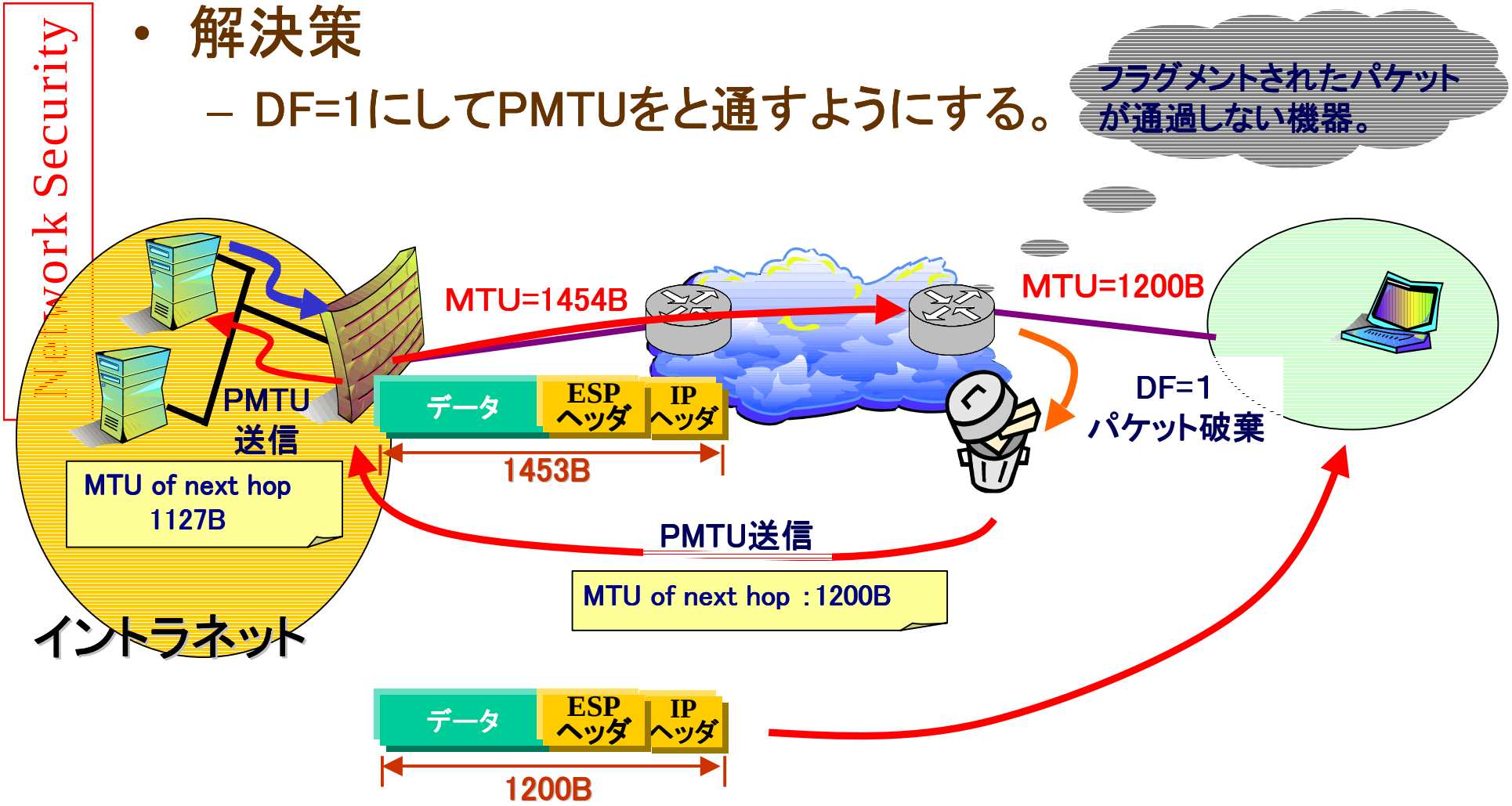
フラグメントに関する問題

- 解決策
  - サーバ側のMTUサイズを調整する
  - 経験では1380B程度に設定すればフラグメントによる通信障害の大半は回避できる



フラグメントに関する問題

- 解決策
  - DF=1にしてPMTUをと通すようにする。



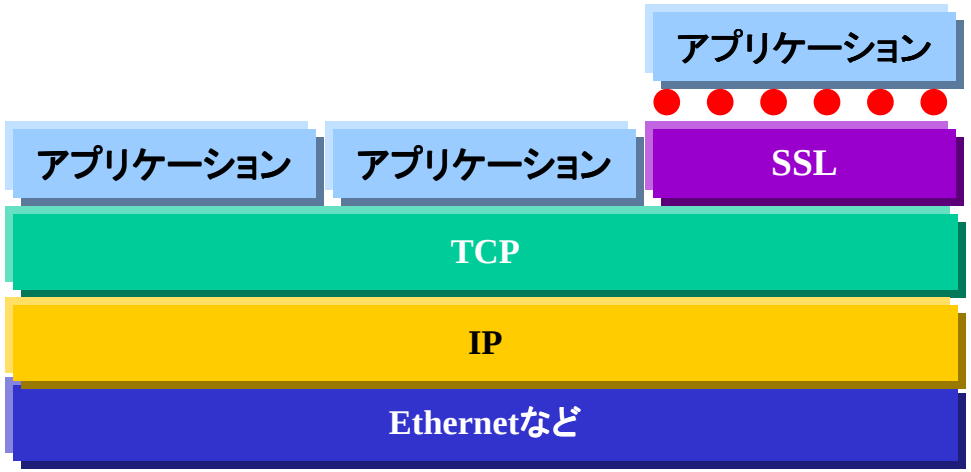
リモートアクセス使用時のまとめ

- VPN構築において留意すべき点
  - 認証は何を使うか？XAUTHやHybrid Authに対応しているか？
  - NAT-Traversalに対応しているか？
  - IPsec-DHCPに対応しているか？
  - 経路上にIKEをふさぐようなデバイスがないか
  - フラグメントが起きて通信できないような場合は予めサーバ側のMTUを小さくしておく。
    またICMPのPMTUを通すようにしておく。
  - クライアントのデスクトップセキュリティ
    - ウイルスその他の攻撃に遭った場合、それをそのまま会社に持ち込む可能性も考えられる

Remote Accessの新たな手法 ～ SSL VPN ～

SSLとは？

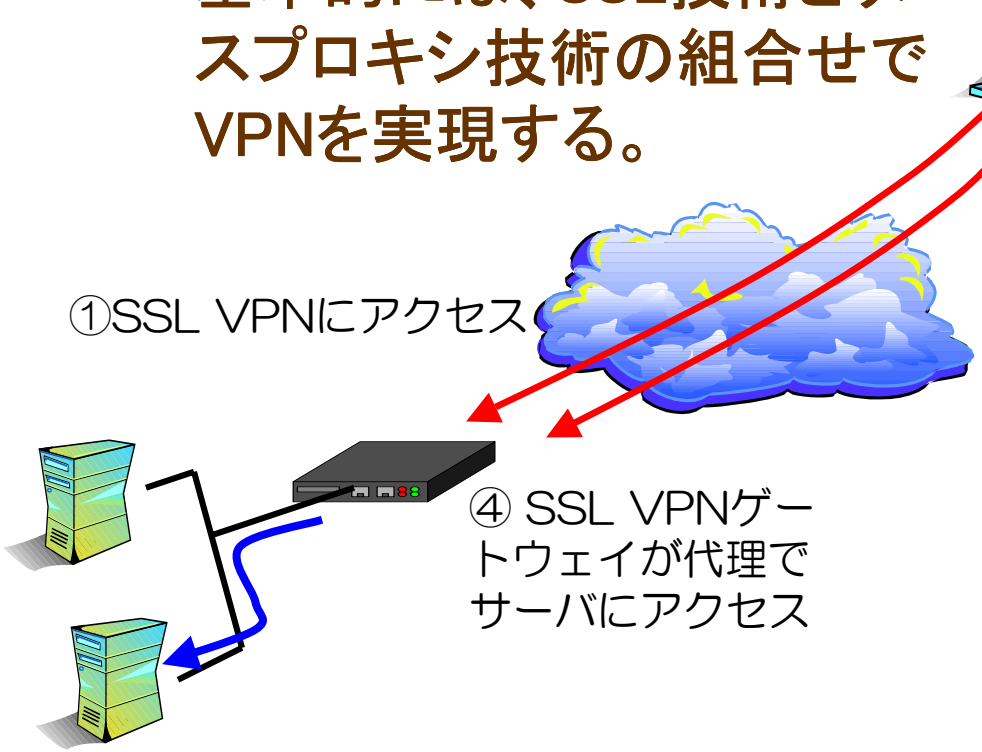
- Secure Socket Layer
  - TCP通信を安全に行うための機能を提供
    - 暗号化　　:RC4,DESなどの暗号機能
    - 相互認証　　:通信する相手を認証する機能
    - メッセージ認証:通信中のデータ改竄を検知する機能
  - 実装はアプリケーションに依存する。



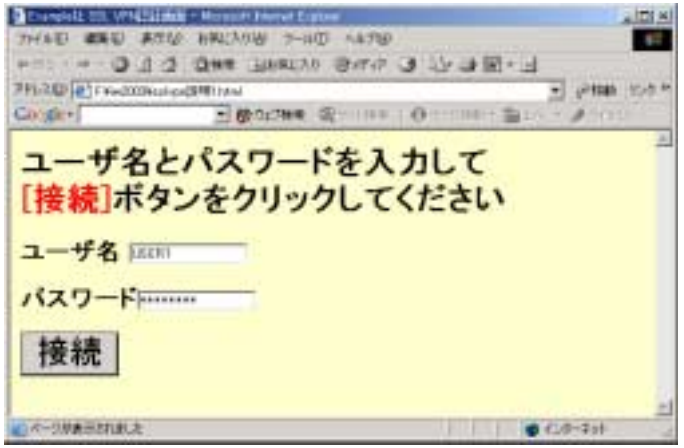
SSLのAPI

SSL VPN

- SSL VPNとは？
  - SSLを利用してVPNを実現する技術
  - 基本的には、SSL技術とリバースプロキシ技術の組合せでVPNを実現する。



② 認証画面が表示され
認証情報を入力



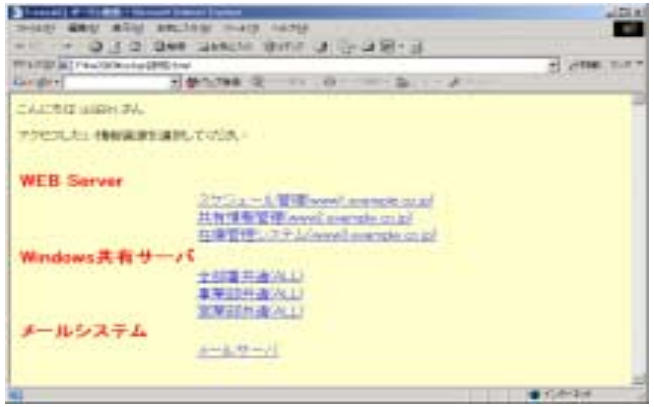
③ ポータル表示されたアクセス可能なリソースから任意のリソースを選択

非SSLアプリへの対応

- リバースプロキシー方式
  - WEBブラウザだけを使用してアクセスする
  - 多くの製品は、WEBとWindowsファイル共有が使用可能
- ポートフォワード方式
  - Javaアプレットをダウンロードし、社内リソースへの通信をSSL化して転送する。
  - TCP固定ポートのアプリケーションが使用可能
- SSLトンネル方式
  - 専用クライアントを使用して、社内リソースへの通信をSSL化して転送する。
  - TCP/UDP問わずほとんどのアプリケーション使用可能

ポートフォワード方式

① ポータルから非SSL対応アプリを選択。



② Javaアプレットを自動的にダウンロードし起動する。

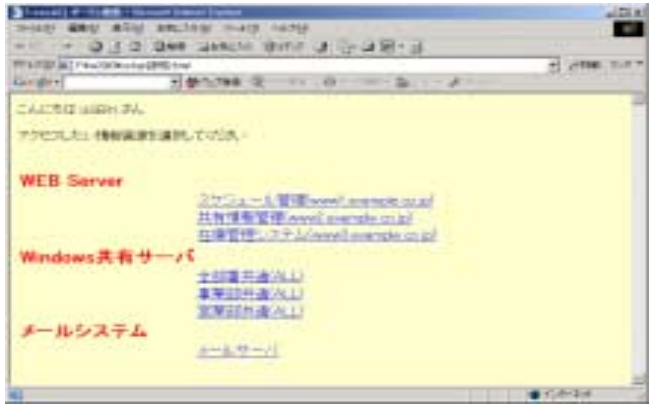
③ Javaはポートフォワード機能と、選択されたサーバのアドレスをhostsファイルに追加する。

④ 選択したリソースへのアクセスを開始すると、hostsファイル参照により、クライアント自身（Javaが受取る）宛に通信を行う。

④ 社内リソース宛の通信を受信したJavaは通信をSSL化してSSL VPNゲートウェイに転送

SSLトンネル方式

① ポータルから非SSL対応アプリを選択。



② 初めての場合はActiveXで自動的にクライアントアプリケーションをインストール

③ クライアントアプリケーションにより仮想インターフェースが設定される。

④ 選択したリソースへのアクセスを開始すると、その通信は仮想ドライバがSSL化しSSL VPNゲートウェイに転送する。

SSLトンネル時のパケットの構成

SSL VPN導入の注意点

- 社内に居る時と、社外に居るときで操作が変わる。
  - すべてのリソースをポータル経由でアクセス
    - メール本文記述のURLや、クライアントPCのブックマークを使用して直接リソースにアクセスできない。
- クライアントアプリケーション
  - クライアントアプリケーションがインストールされる際には、Administrator権限が必要となる
- 証明書の検証
  - クライアント証明書の検証が行われない製品が多い
    - SSLの標準では証明書の検証が行われないため、SSL VPNゲートウェイの実装も証明書の失効検証が行われない製品が多い。
- アクセス制御について
  - アクセス制御の設定変更が有効になるタイミングが製品によって異なる。
    - 製品によっては、アクセス制御の設定変更時に全てのセッションが切断されることがある。

IPsec vs SSL VPN

	IPsec	SSL VPN
対応端末	OS依存	SSL対応WEBブラウザが稼動すればプラットフォームに依存しない。携帯電話やPDAもOK
対応アプリケーション	IP上で稼動するアプリケーション	製品依存
使い勝手	リソースへのアクセスはローカル環境と同様のオペレーションで可能	リソースへのアクセスはポータル経由
ネットワーク環境依存	NAT-Tや、IPsec-DHCPでほぼ解決しているが、MTU問題が若干残る	NATや名前解決の問題は発生しない。
アクセス制御	IPアドレス単位で実施	リソース単位で実施 （例えばURL単位やフォルダ単位）
費用	小規模の場合、SSL VPNより割安 大規模の場合、SSL VPNより割高になる可能性が高い	小規模の場合、IPsec VPNより割高 大規模の場合、IPsec VPNより割安になる可能性が高い

現状では、使用したい端末とアプリケーションとのバランスを考慮してVPN技術を選択することが、失敗しないリモートアクセスVPNに繋がる

ありがとうございました。

商標について

•本文記載の会社名および製品名は、それぞれ各社の商標又は登録商標です。