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：B. Aboba, W. Dixon

文献名：IPsec-NAT Compatibility Requirements

種類：Internet Draft

発表日：3 March 2003

IPsecとNATの互換性

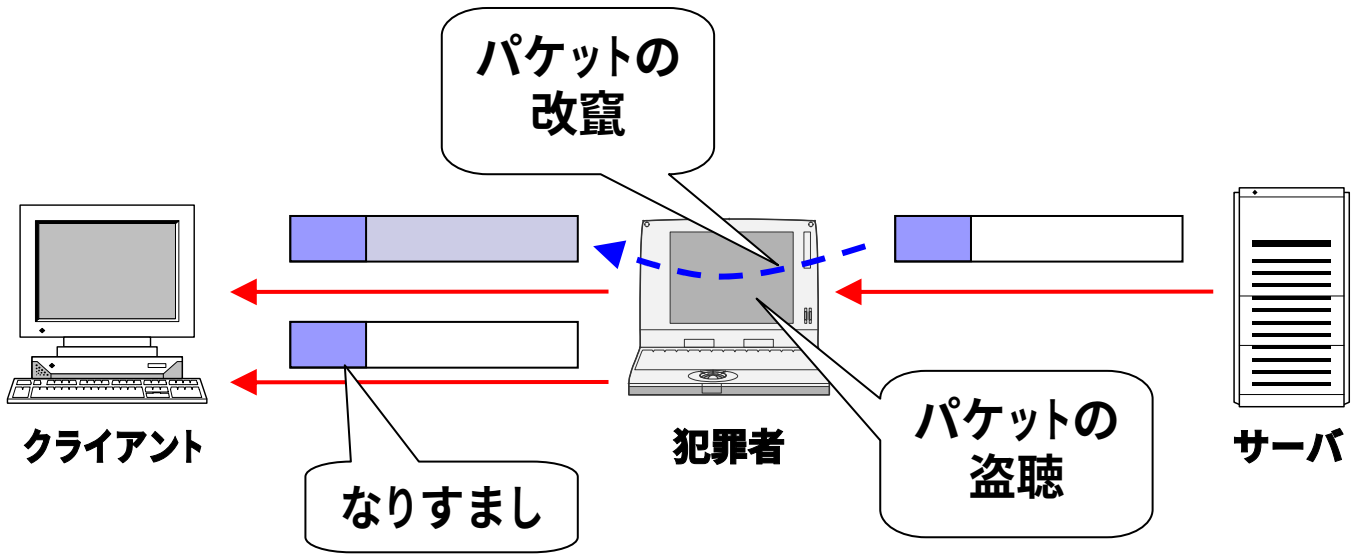
渡邊研究室
００Ｊ１２５　増田 真也

はじめに

- 全体の流れ
  1. 背景
  2. 問題点
  3. 互換性の必要条件
  4. 解決策
  5. まとめ

1．背景

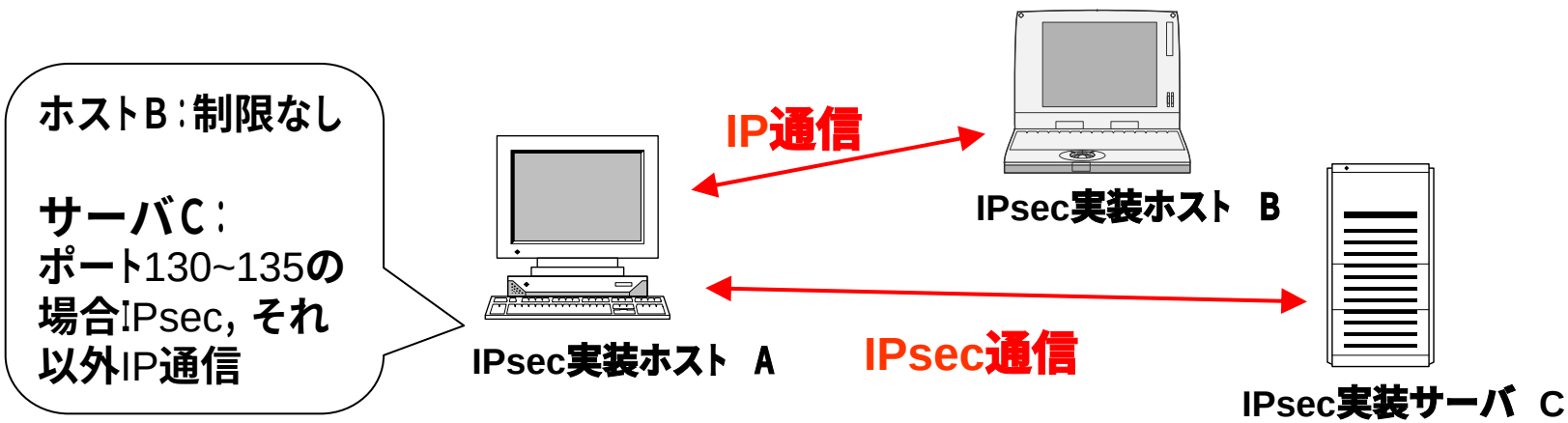
- インターネットにはセキュリティの保障がない



IPのセキュリティ上の欠点

1. 背景

- IPsecの誕生
  - IPsecの理想像
    - 全てのコンピュータがIPsecを実装
    - セキュリティレベルに応じた通信方法の自動選択
    - ユーザはIP/IPsecどちらの通信なのか意識せず利用



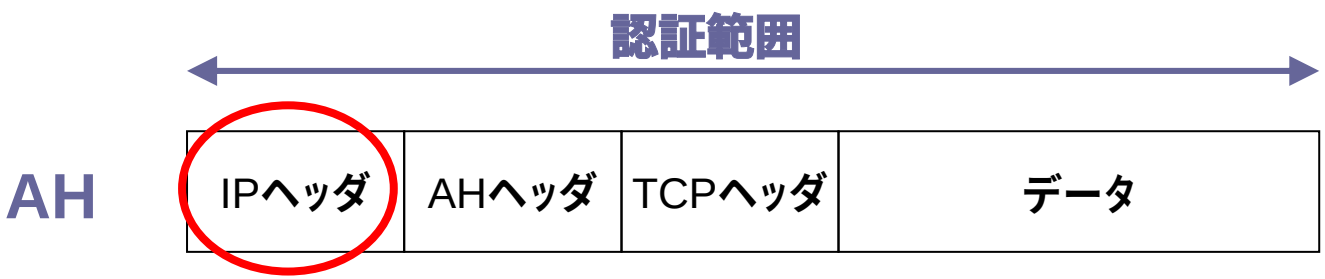
IPsecの理想像

1．背景

- 普及の弊害
  - 使い勝手が悪い（設定項目の多さ）
  - 相互接続性が悪い（複数の仕様）
  - 導入・運用コストが高い
  - 処理負荷が重い
  - 透過性に欠ける（NAT・NAPTとの相性）

2．問題点

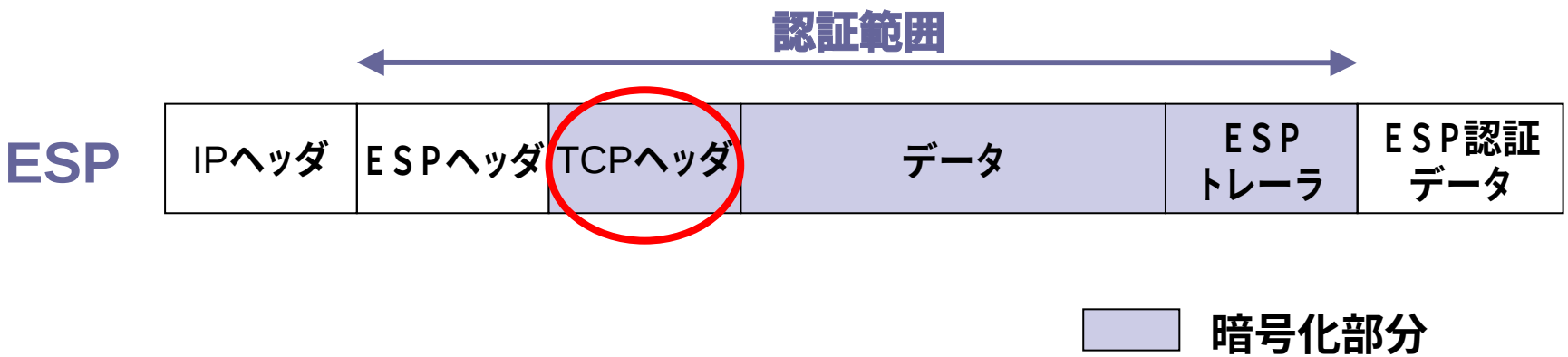
- IPsec AH と NAT
  - AHパケットのNAT通過
    → アドレス変換により認証されない



AHパケットの構造（トランスポート・モード）

2．問題点

- IPsec ESP と NAT
  - NATはTCPヘッダのチェックサムを変更する
    → 暗号化部分･認証範囲にあるTCPヘッダは変更できない



ESPパケットの構造（トランスポート･モード）

2．問題点

- IPアドレスを運ぶプロトコルとNAT
  - NATで運ぶIPアドレスも変換

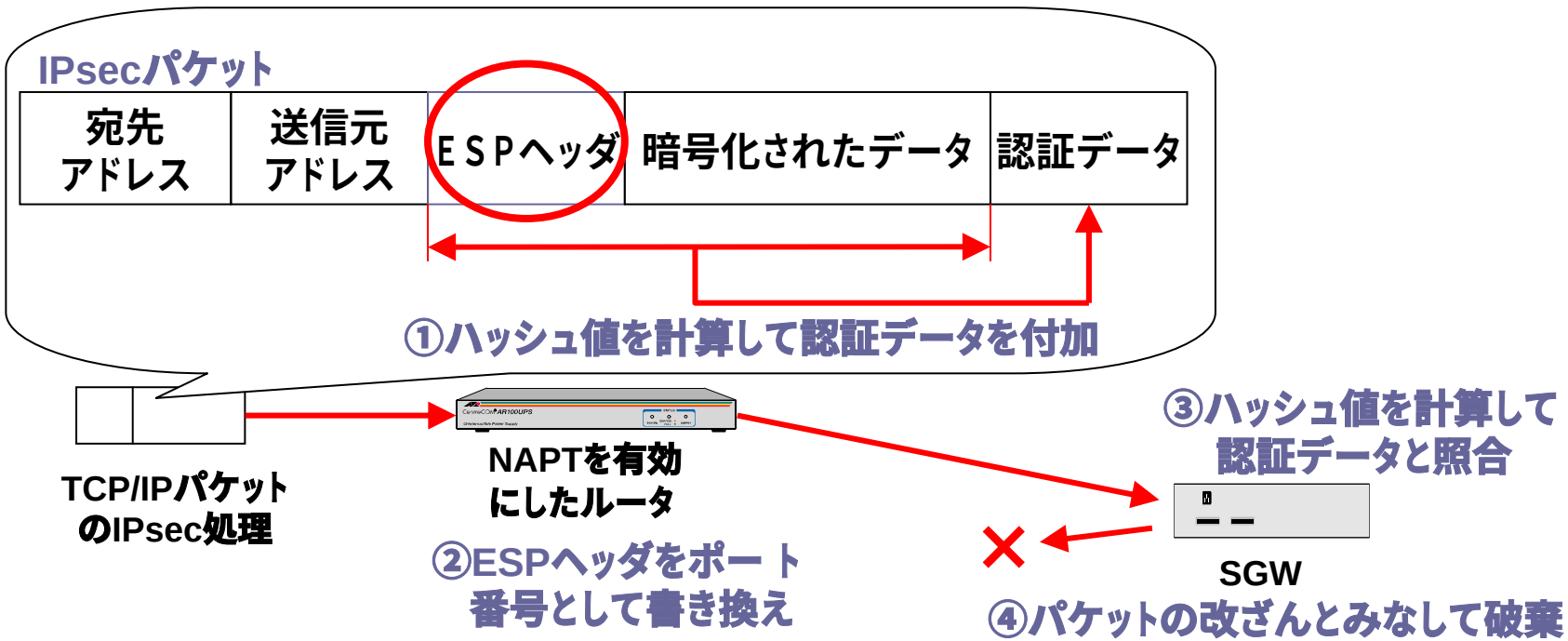
    → アドレス変換により認証されない
  - 例：FTP

    ファイル転送を行うコネクションのネゴシエーションを行う
    - ネゴシエーションで，IPアドレスとポート番号を運ぶ

      → NATで，運ぶIPアドレスも変換する必要がある

2．問題点

- ポート番号とNAPT
  - NAPTはESPヘッダをポート番号として書き換える
    → IPsecパケットは認証されない

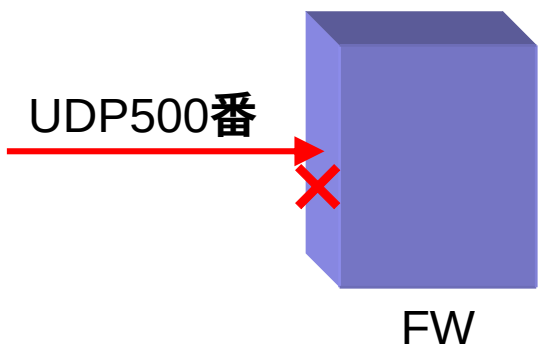


IPsecパケットがNAPTを通過できない理由

2．問題点

- IKEとポート制限
  - IKEはUDP500番ポートを使用する

    → UDP500番ポートを塞いでいる場合，IKEは使えない

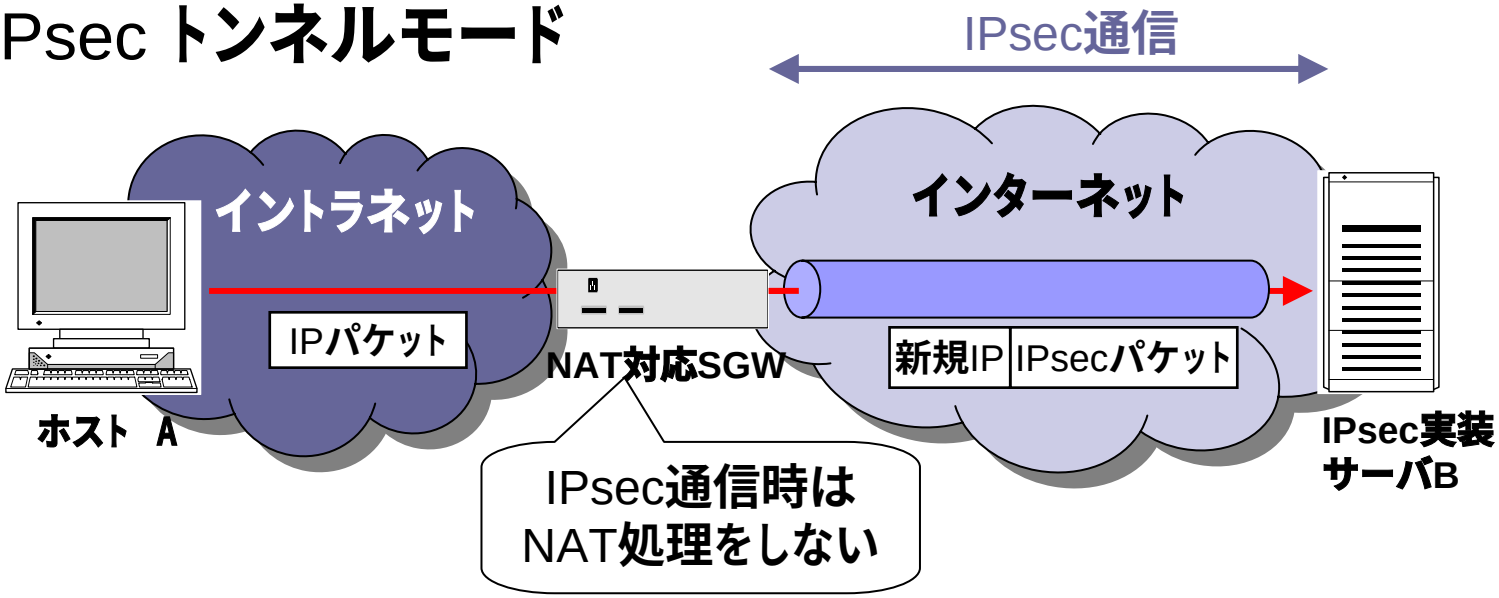


3．互換性の必要条件

- 展開
  - IPv6が普及する前に解決される必要がある
- ファイアーウォール
  - ファイアーウォールを考慮する必要がある
    → 一定したアクセスルールの作成
- スケーリング
  - 何千という通信機器から成り立っている設備の中で適用できるべきである
- セキュリティ
  - IKE, IPsecの弱点をもたらしてはならない

4．解決策

- IPsec トンネルモード

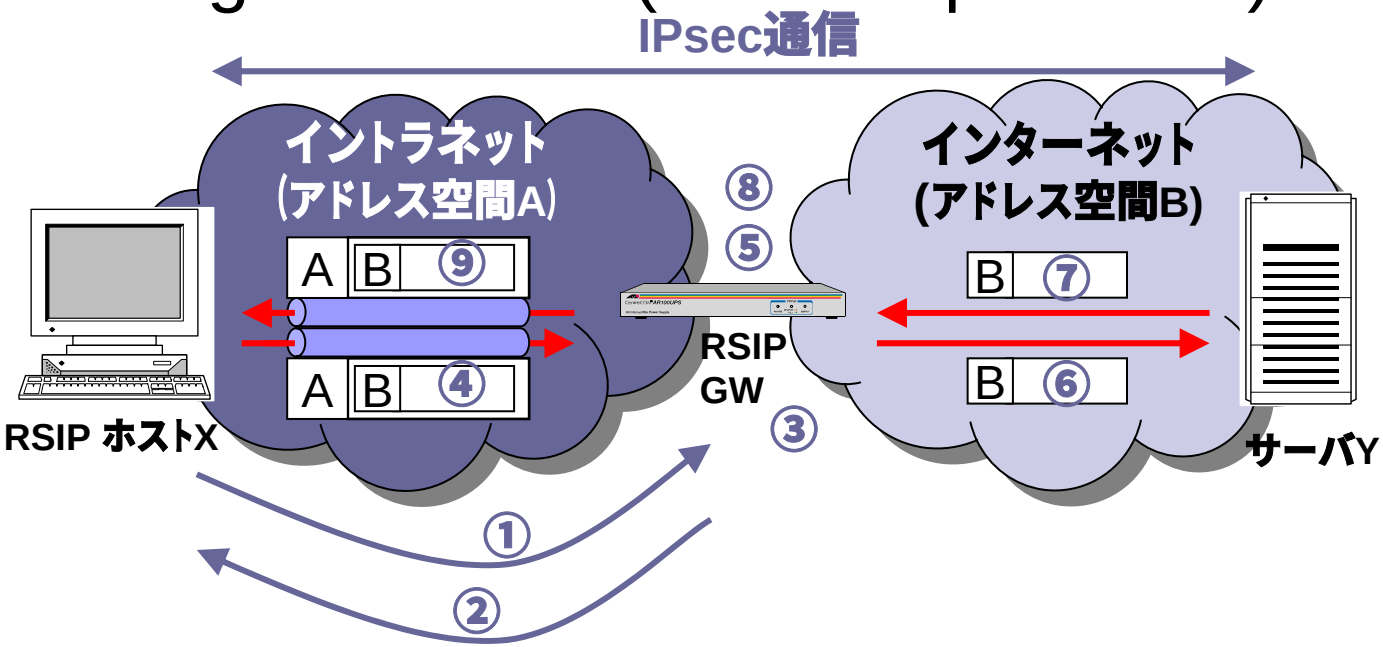


IPsecトンネルモードの概念図

- **本質的な解決策ではない**
- end-to-endのIPsec**通信ではない**
- **カプセル部分は改竄などの恐れがある**

4．解決策

- Tunneling with RSIP (Realm Specific IP)



Tunneling withRSIPの概念図

- 本質的な解決策ではない
- カプセル部分は改竄などの恐れがある

4．解決策

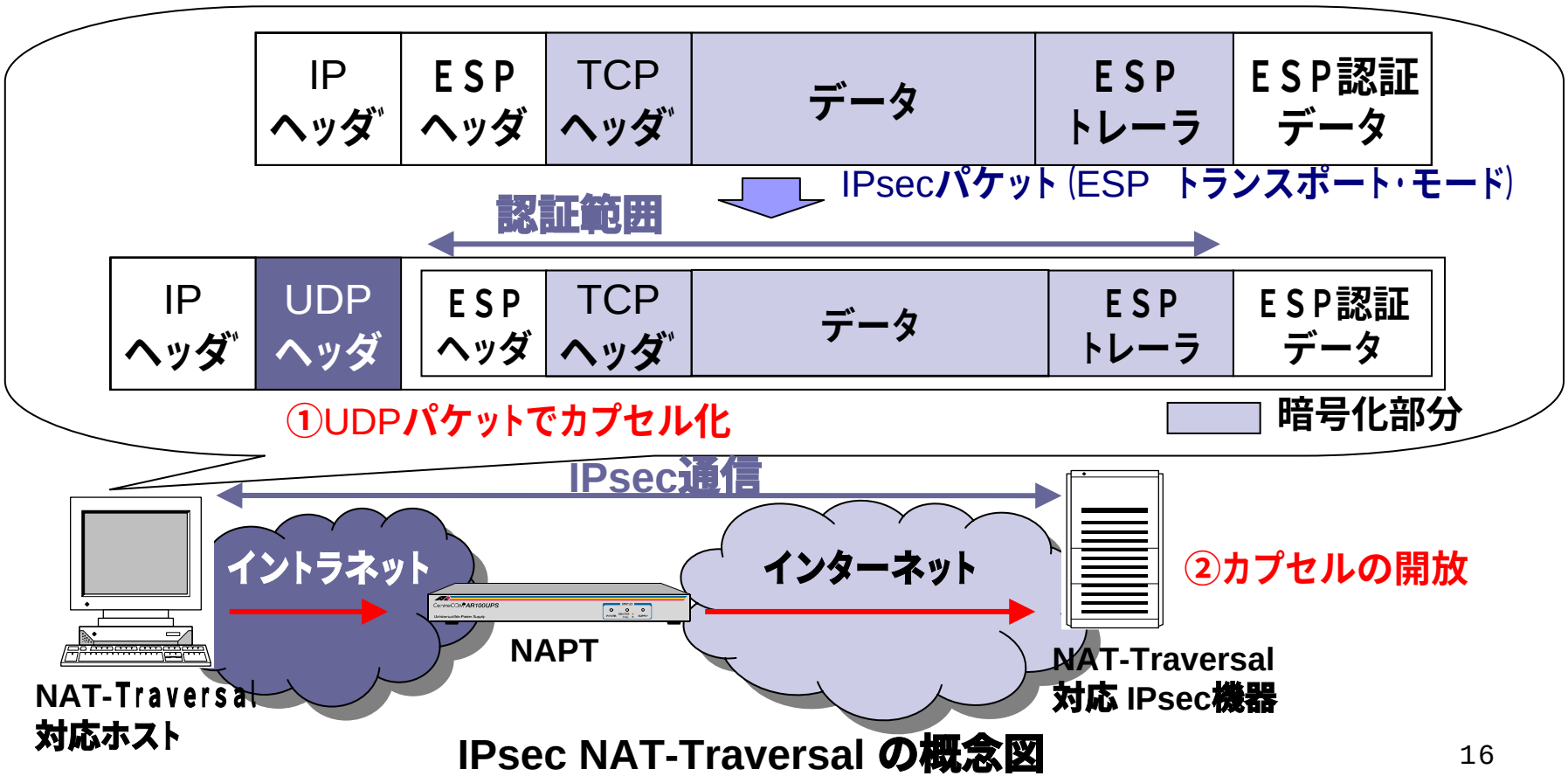
- 6to4
  - IPsecを適用したIPv6のNAT通過が可能

6to4によるカプセル化

  - IPsecを使っているIPv6，6to4ネットワーク郡に限定
  - スループットの低下
  - カプセル部分は改竄などの恐れがある

4．解決策

- IPsec NAT-Traversal
  - IPsecパケットをUDPのパケットでカプセル化



IPsec NAT-Traversal の概念図

4．解決策

- IPsec NAT-Traversal
  - **解決策の中でも本質的で，優れた手段である**
  - **カプセル部分は改竄などの恐れがある**
  - **UDPでカプセル化する理由**
    - **TCPでは，カプセル部分のTCPによる応答があるが，不要であり無駄が生じる**
    - **TCPヘッダ長が20バイトであるのに対し，UDPヘッダは最低8バイトで済む**

5．まとめ

- IPsecとNATの相性は悪い
  - アドレス･ポート番号の書き換えによる問題
- 解決策
  - IPsecトンネルモード
  - Tunneling with RSIP
  - 6to4
  - IPsec NAT-Traversal
- IPv6によるNATに依存しない通信が望ましい
  - NATが不要になると、NATで内部ネットワークを見えなくする機能が使えなくなるので危険ではないか？
    → 内部ネットワークを外から見えないようにフィルタリングや経路制御の設定をすることは、IPv6でも可能

おわり

参考文献

- “IPsec-NAT Compatibility Requirements” draft-ietf-ipsec-nat-reqts-04
- “Realm Specific IP: Protocol Specification “ RFC 3103
- “The IP Network Address Translator (NAT) “ RFC 1631
- **「マスタリングIPsec」**
  著：馬場 達也　　出版：㈱オライリー・ジャパン
- “SIP, NAT, and Firewalls”
  http://www.cs.columbia.edu/~hgs/sip/drafts/Ther0005_SIP.pdf