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：B. Aboba, W. Dixon
- 論文名：IPsec-NAT Compatibility Requirements
- 出展：RFC 3715
- 2004年5月

IPsec-NAT間の互換性

渡邊研究室
030432017　今村　圭佑

目次

1.1 NAT概要

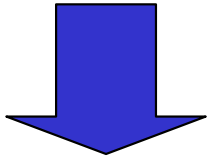
- Network Address Translation
  - ルータやデバイスに標準機能として取り付けてられている
  - ローカルアドレスとグローバルアドレスを透過的に相互変換

1.2 IPsec概要

- IPsecは、パケットを完全に運ぶ技術
- IPsecの利点
  - 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
  - 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
- 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が実現されていない
  - NATを通してIPsecを使用することができない

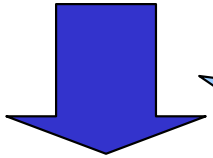
1.3 NAT透過の必要性

社内のLANなどに出張先からインターネット経由でアクセスしたい



強力な暗号化と認証を持つIPsecは極めて有効な手段

インターネットアクセスはNAT経由で接続されている場合が多い

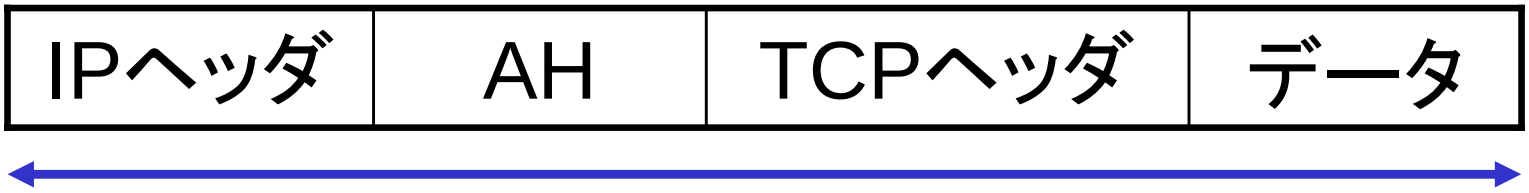


NATを越えることが出来ないため

IPsecによるリモートアクセスを使用することが出来ない

2.1 NATとIPsec間の不適合性

- IPsec AHとNAT
  - AHのパケットはトンネルモード、トランスポートモード共に、IPヘッダを認証の対象範囲に含んでいる

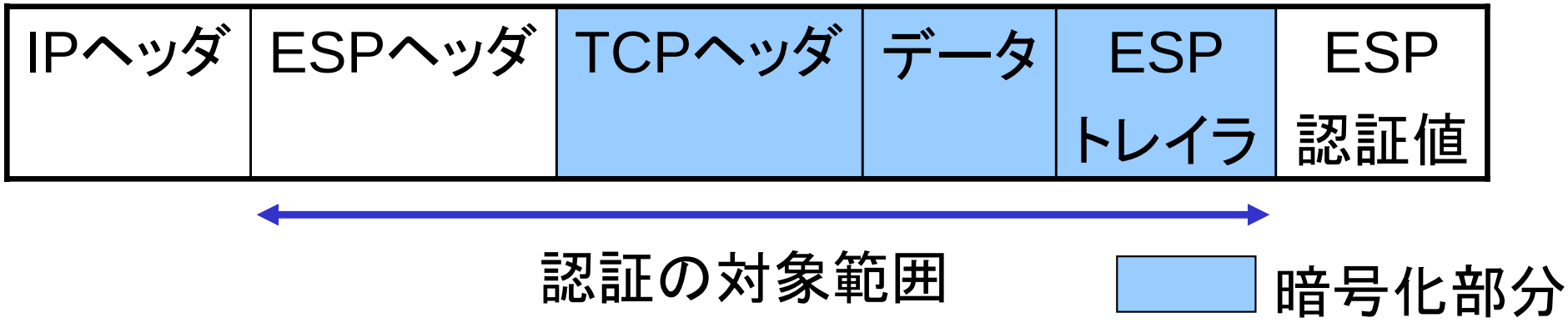


認証の対象範囲

- IPヘッダの内容を書き換えるNAT変換を行うと、AHの認証が出来ない

2.1 NATとIPsec間の不適合性

- IPsec ESPとNAT
  - NATはTCPとUDPヘッダのチェックサムを変更する

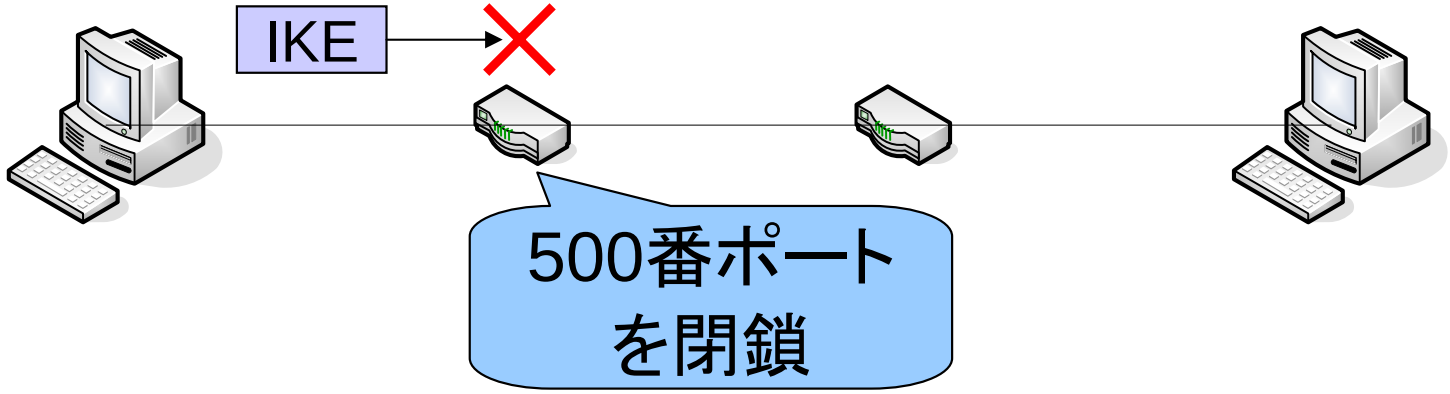


- 認証部分、暗号化部分に含まれるためTCPヘッダを変更できない

2.1 NATとIPsec間の不適合性

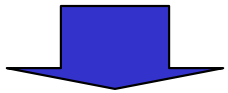
- IKE UDPポートを変更出来ない
  - IKEは、UDP500番ポートを使用する

IKEパケットがNATを通過できない

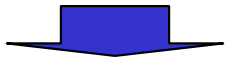


2.1 NATとIPsec間の不適合性

- 埋め込みアドレスとIKEパケットのアドレスとの不一致
  - ネゴシエーションの際に送信元IPアドレスをペイロードに埋め込み相手に送信する



送信側ノードの送信元アドレスが NAT によって変更



埋め込みアドレスと送信元アドレスの不一致

パケットが破棄されIKEネゴシエーションが中止される

3.1 解決されるべき問題

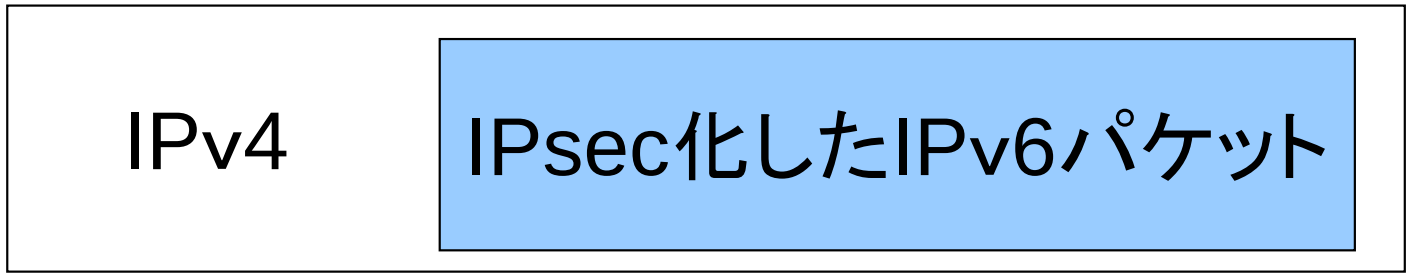
- 配備
  - IPv6が配備される前に解決する必要がある
- スケーリング
  - 何千もの機器、施設の中で適用するべきである
- モードサポート
  - トンネルモード、トランスポートモード共に適用されるべきである
- ファイアウォール互換性
  - IKEパケットを通すなどポート番号の解決
- セキュリティ
  - NAT透過を解決したことにより、セキュリティの脆弱性をもたらしてはいけない

4.1 解決策

- IPsecトンネルモード
- RSIP（Realm Specific IP）
- 6to4
- IPsec NAT-Traversal

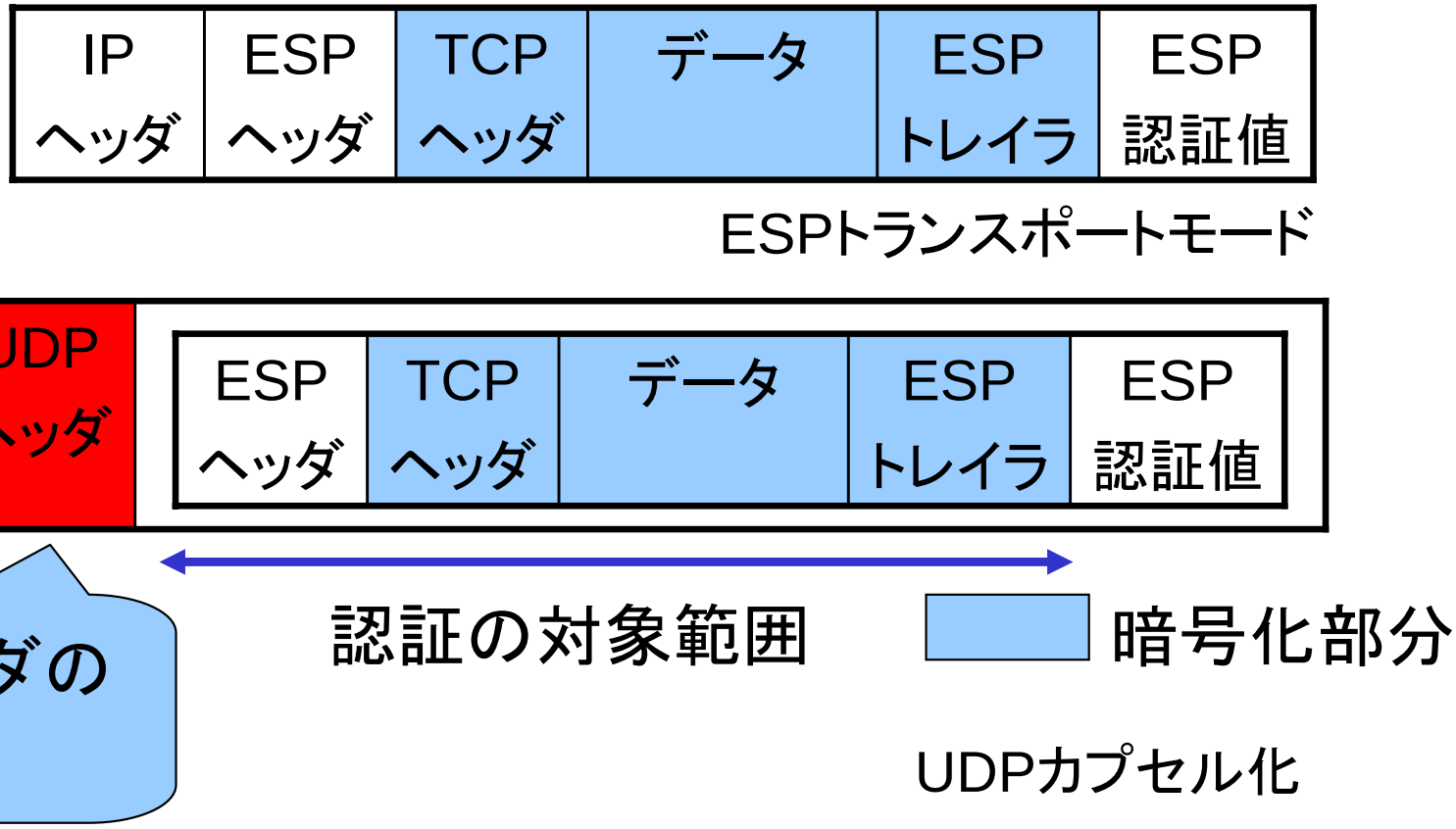
4.2 解決策～6to4～

- 6to4
  - IPsec化したIPv6のパケットをIPv4のパケットでカプセル化
  - IPsecを使用しているIPv6および6to4ネットワーク内しか使用できない
  - カプセル化によるスループットの低下
  - カプセル化部分は改ざんされる可能性がある



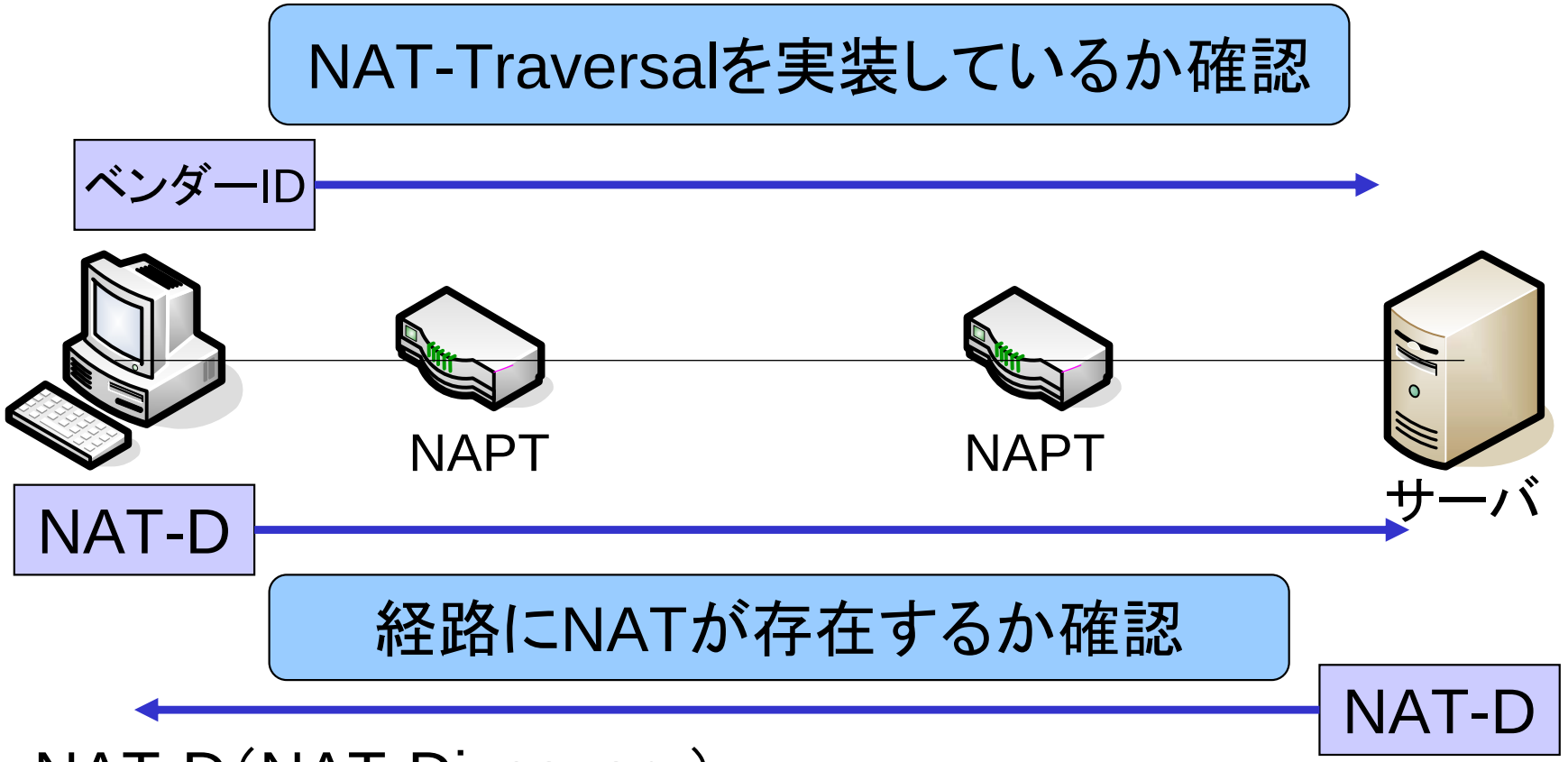
4.3 解決策～IPsec NAT-Traversal～

- IPsec NAT-Traversal
  - ESPに対するUDPのカプセル化
  - IKEヘッダの修正



4.3 解決策～IPsec NAT-Traversal～

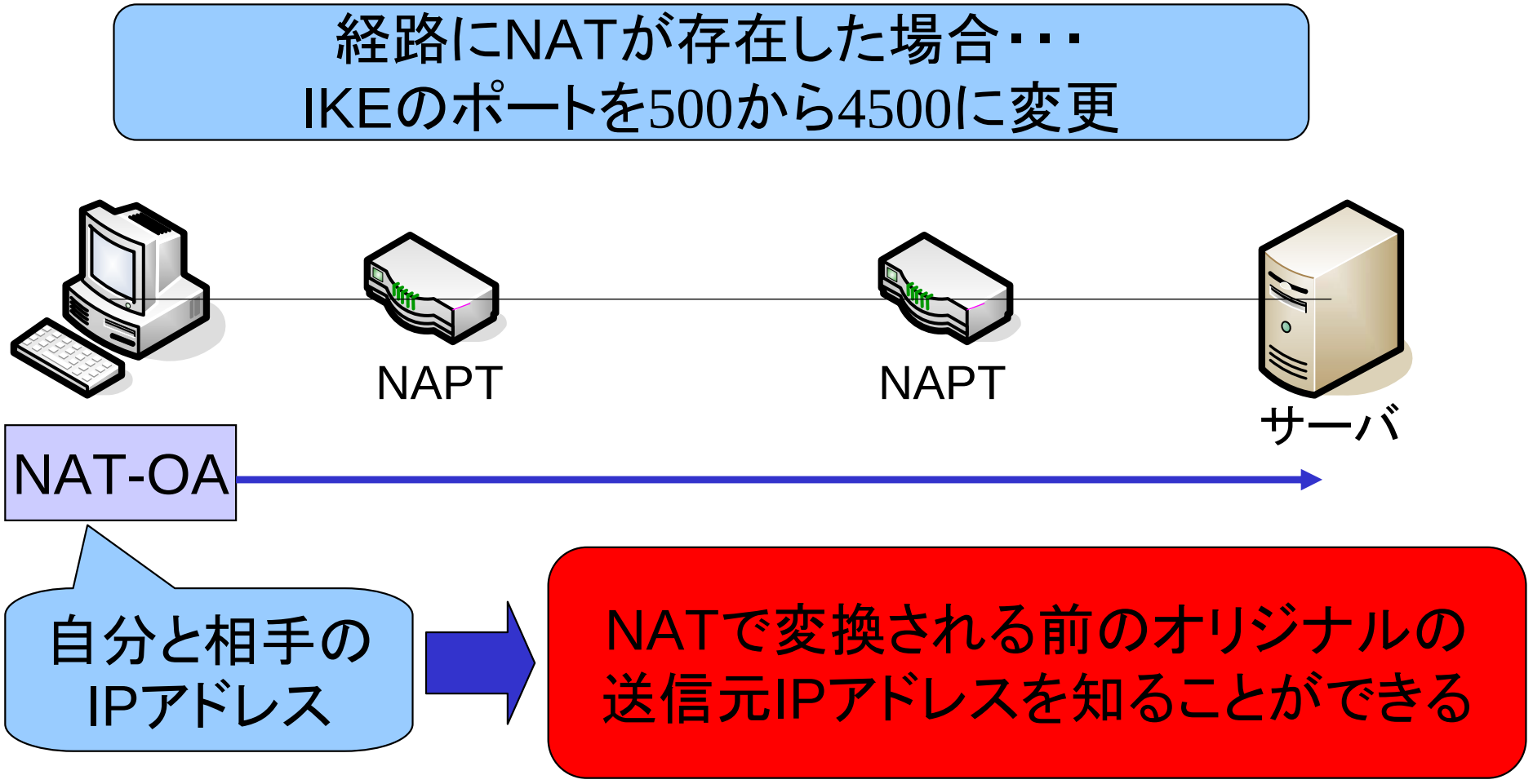
- IPsec NAT-Traversal動作



NAT-D（NAT-Discovery）
送信元IPアドレス、ポート番号のハッシュ値
宛先IPアドレス、ポート番号のハッシュ値

4.3 解決策～IPsec NAT-Traversal～

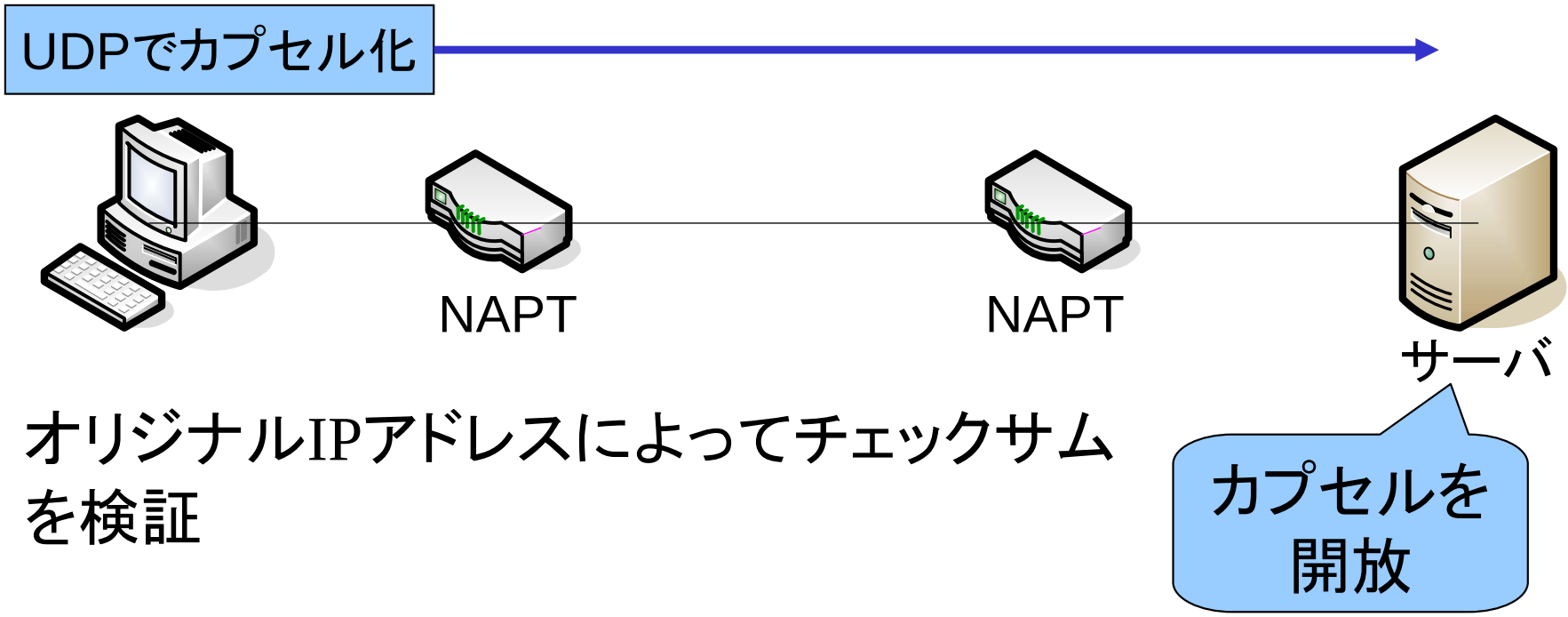
- IPsec NAT-Traversal動作



NAT-OA（NAT Original Address）

4.3 解決策～IPsec NAT-Traversal～

- IPsec NAT-Traversal動作



多くの機器でNAT-Traversalが実装されており、NAT越えの一番の解決策である

まとめ

- IPsec-NATの互換性
  - アドレス、ポートの書き換えの問題
- 解決策
  - IPsecトンネルモード
  - RSIP（Realm Specific IP）
  - 6to4
  - IPsec NAT-Traversal

参考文献

IPsec-NAT Compatibility Requirements

RFC 3715

UDP Encapsulation of IPsec ESP Packets

RFC 3948

IPsec徹底入門

著　小早川知昭

終わり