IPsec-VPN（課題と応用）

学習内容

IPsecがNAT/NAPTと共存できない理由と、その解決策となる技術

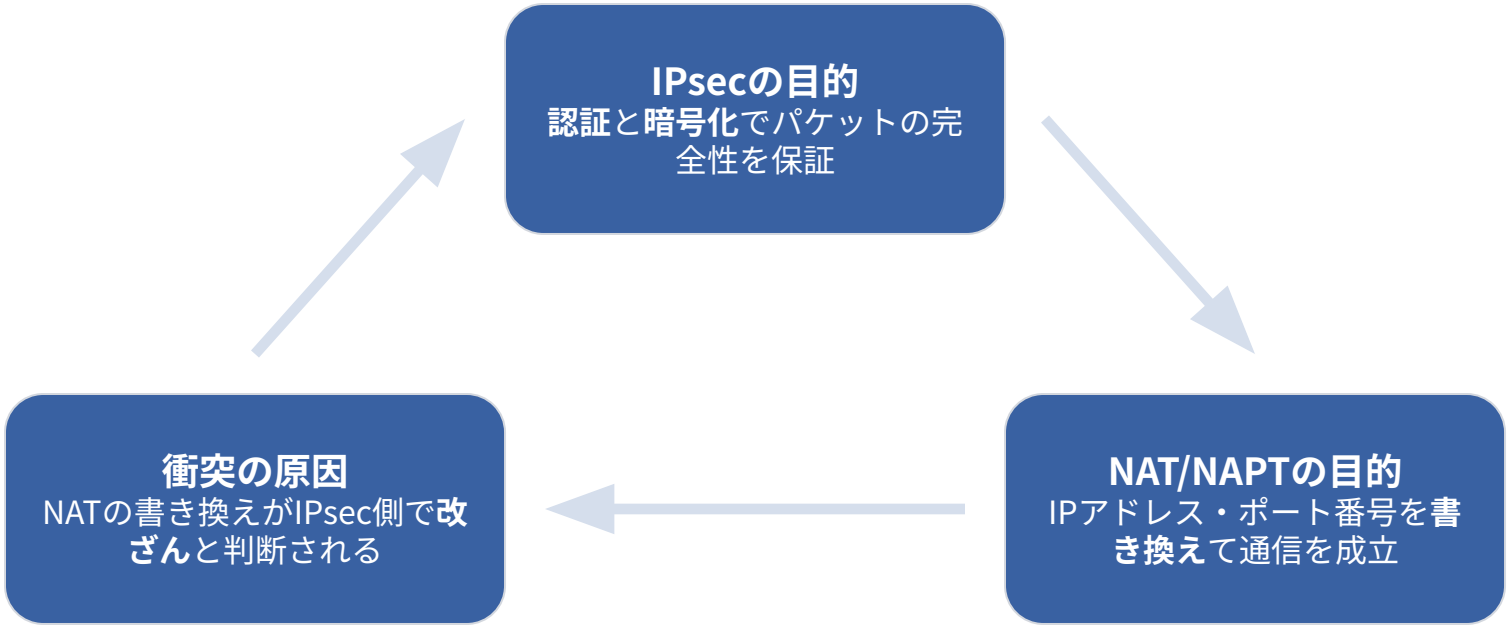
1. IPsecとNAT/NAPTの衝突のメカニズム
2. AH/ESP/IKEそれぞれの問題点
3. 解決策：NAT Traversal（NAT-T）の仕組み
4. NAT-Tを実現するIKE拡張機能
5. 応用編：動的IP環境でのIPsec-VPN接続

01

第1章：IPsecとNAT/NAPTの衝突メカニズム

なぜIPsecとNAT/NAPTは衝突するのか

パケットの「変更」がIPsecの「認証・暗号化」と矛盾



IPsec主要プロトコルにおける問題点の整理

認証範囲と暗号化範囲の違いが、NAT/NAPTの処理を妨げる

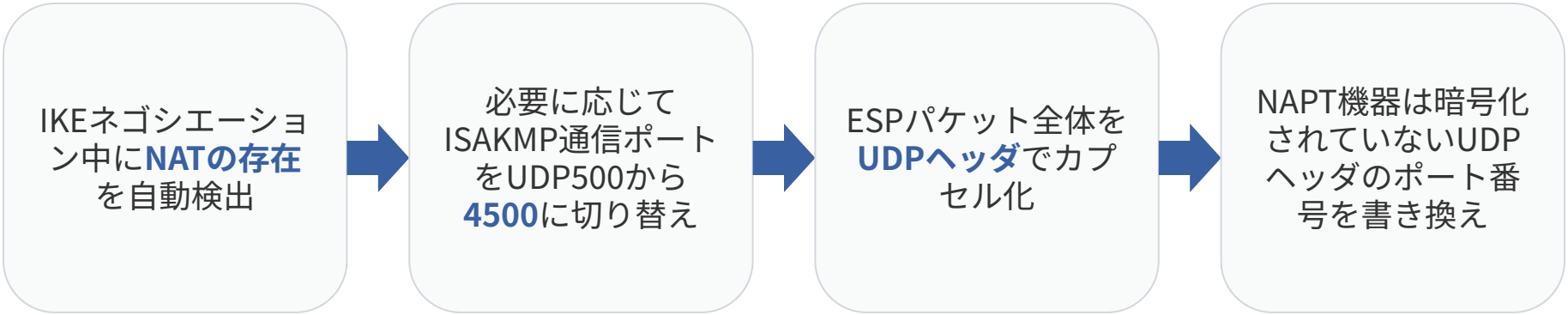
AH (Authentication Header)	ESP (Encapsulating Security Payload)	IKE (Internet Key Exchange)
IPヘッダも認証するため、NATによるIPアドレス書き換えで**認証エラー**となる。	TCP/UDPヘッダが暗号化され、NAPTに必要な**ポート番号**が読み取れない。	鍵交換にUDPの**500番**を固定で利用するため、NAPTによるポート変換が行えない。

02

第2章：解決策としてのNAT Traversal (NAT-T)

NAT Traversal (NAT-T) の仕組み

ESPパケットをUDPカプセル化し、NAPTのポート変換を可能にする



IKEフェーズ1（メインモード）でのNAT-Tネゴシエーション

NATの検出とポートの切り替えプロセス

STEP 1	Vendor ID (タイプ13) 交換でNAT-Tサポートを通知
STEP 2	NAT-D (タイプ20) ペイロードでネットワーク経路上にNAT装置の**有無**を検出
STEP 3	NAT検出後、ISAKMPポートをUDP500から**4500**に変更
STEP 4	ISAKMPヘッダとUDPヘッダの間に**Non-ESP Marker**を追加

IKEフェーズ2でのESPカプセル化の決定

ESPパケットの処理モードとオリジナルIPアドレスの伝達

Transform (タイプ3)

ESPパケットをUDPカプセル化するモード（トンネルまたはトランスポート）を決定

NAT-OA (タイプ21)

トランスポートモード利用時に**NAPT書き換え前**のオリジナルIPアドレスを伝達しチェックサムエラーを防ぐ

03

第3章：動的IPアドレス環境でのIPsec-VPN接続

動的IPアドレス環境での鍵交換モード選択

通信開始と認証IDの観点からAggressiveモードが基本となる

Mainモード	Aggressiveモード
IKEフェーズ1で**IPアドレス**を認証に使う	IKEフェーズ1で**FQDN**やユーザー名などのIDを使える
相手IPを特定できない動的IP環境では利用不可	相手IPを事前に知らなくても認証が可能となる
（※デジタル署名を使えば可能だが一般的ではない）	動的IP環境でのIPsec-VPNの**基本**