# IPsec

# 学習内容

1. IPsecの概要と役割
2. 動作レイヤーとTLS/SSLとの比較
3. 構成プロトコル（AH・ESP・IKE）の詳細
4. 通信モード（トランスポート・トンネル）の比較
5. SAとSPD：セキュリティ情報の管理

01

# IPsecの概要と役割

# IPsecとは：公開ネットワークでの安全な通信

ネットワーク層で動作し、暗号化と認証でセキュアな通信を実現

IPsecは、インターネットなどの**公開ネットワーク**上で安全な通信を確立する仕組み

**ネットワーク層**（IP層）で動作し、データ保護を行う

主な役割は、データの**暗号化**（盗聴防止）と**認証**（改ざん防止・なりすまし防止）

IPsecを利用した**VPN**（仮想プライベートネットワーク）は、拠点間接続やリモートアクセスに広く利用される

# 動作レイヤーによるSSL/TLSとの違い

IPsecは幅広い通信を保護、SSL/TLSはアプリケーションに特化

| IPsec | SSL/TLS |
| --- | --- |
| **ネットワーク層**（レイヤー3）で動作 | **セッション層**（レイヤー5）で動作 |
| TCP/UDPなど上位層のプロトコルに**依存しない** | HTTPやSMTPなど**特定のアプリケーション**に限定される |
| IP通信であれば**全てを保護**できる | アプリケーションごとの**設定が必要** |
| 主にVPNや**OSレベル**の通信で利用 | 主にWeb通信（HTTPS）やメールで利用 |

02

# IPsecを構成する主要プロトコル

# IPsec構成プロトコルの役割と識別番号

AH、ESP、IKEの機能とIPプロトコル番号を整理

| プロトコル名 | 主な役割 | IPプロトコル番号/ポート |
| --- | --- | --- |
| AH (Authentication Header) | パケットの**改ざん防止**（認証機能のみ）。暗号化は行わない | **IPプロトコル番号 51** |
| ESP (Encapsulating Security Payload) | パケットの**暗号化**と**改ざん防止**（認証）。データ部分を守る | **IPプロトコル番号 50** |
| IKE (Internet Key Exchange) | 通信相手と安全に**鍵を交換**するための仕組み | **UDPポート番号 500** |

# AHとESPの仕組み：セキュリティパラメータの共有

両者に共通する重要な識別子 SPIとリプレイ攻撃対策のSequence Number

**SPI（Security Parameters Index）**

どの**セキュリティ設定**（SA）を使うかを識別する

**Sequence Number**

パケットの連番。**リプレイ攻撃**（盗聴パケットの再送）を防ぐ

**Authentication Data**

パケットが改ざんされていないかを確認する**認証用の値**

03

# 通信モードの理解（トランスポート vs. トンネル）

# IPsec 2つの通信モードの比較

保護対象の違い：ホスト間はトランスポート、拠点間はトンネル

## トランスポートモード

元の**IPヘッダはそのまま**利用

暗号化・認証の対象は**データ部分**（ペイロード）のみ

主にIPsecを実装した**ホスト同士**の通信に利用

## トンネルモード

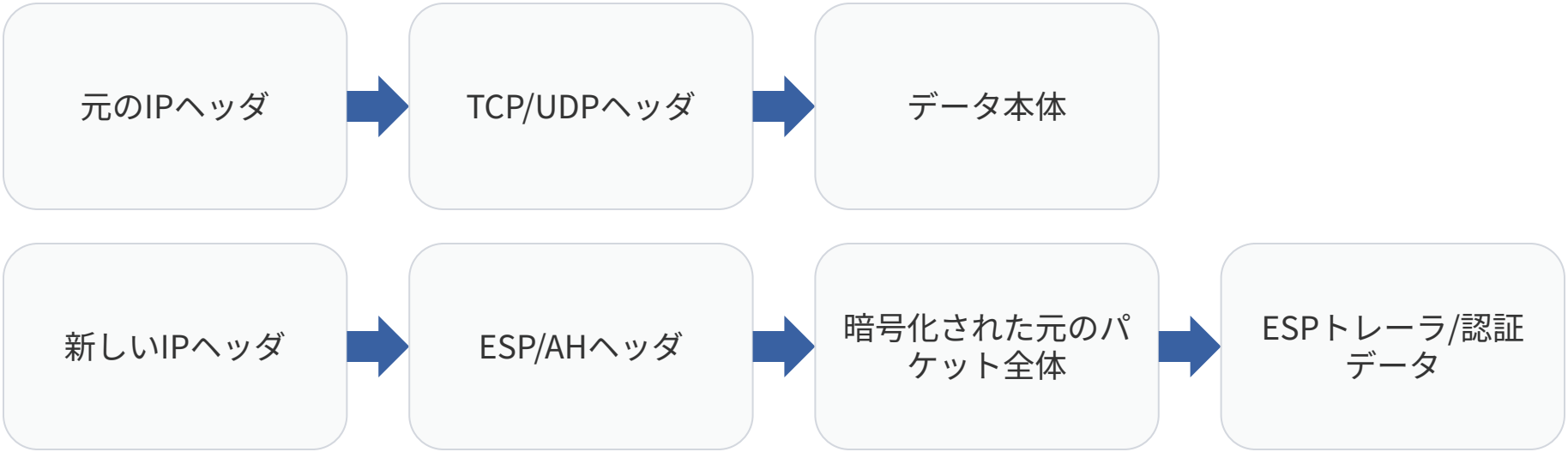
元のIPヘッダごと**全体を暗号化**

**新しいIPヘッダ**を付加して送信

主に**VPNルータ同士**の拠点間通信に利用

# トンネルモードのデータ構造イメージ

元のパケット全体をESP/AHで包み、新しいIPヘッダを付与

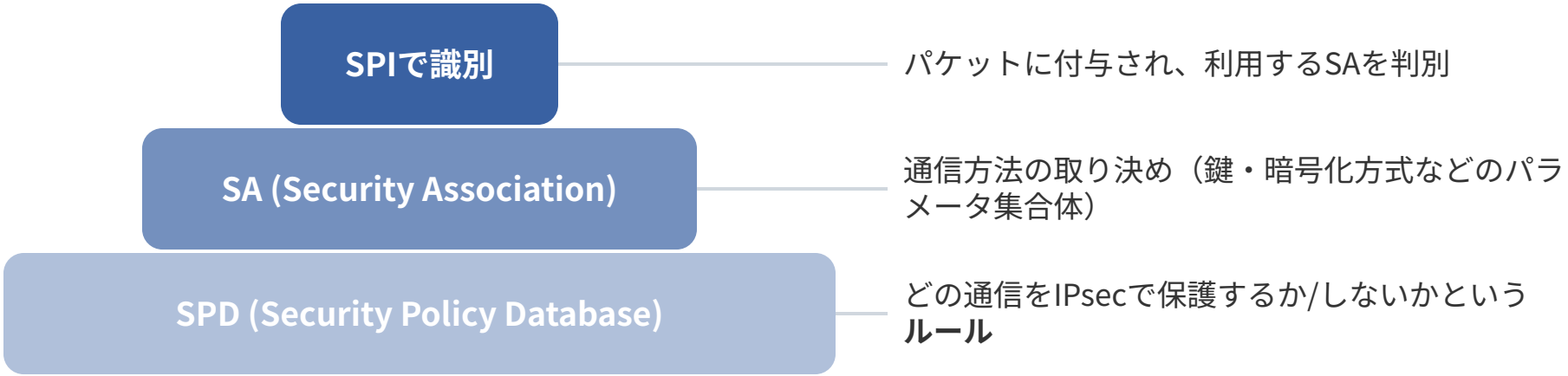


04

# セキュリティ情報の管理（SAとSPD）

# IPsec通信の鍵となる管理機構

ポリシー（SPD）に基づいてSAが確立され、通信が行われる



# SA（Security Association）の性質

一方向のコネクションであり、SPIで識別される

SAは、IPsec通信を行うための**暗号化方式**や**鍵**などのパラメータ集合体

SAは**一方向**の通信に対して設定される（双方向には最低2つ必要）

パケットヘッダの**SPI**（Security Parameters Index）によってSAが識別される

SAの情報はSAD（Security Association Database）に保存・管理される

# SPDの役割：通信の振り分け

どの通信にセキュリティを適用するかを決定するデータベース

対象通信の指定

**どのIPアドレス間、どのポート番号の通信か**

ACL（アクセスリスト）で表現される

ポリシーの決定

**IPsec適用 / IPsec不適用 / 破棄**

通信のセキュリティ処理を規定