IKE

学習内容

安全なIPsec通信を支えるIKEの全体像を把握する

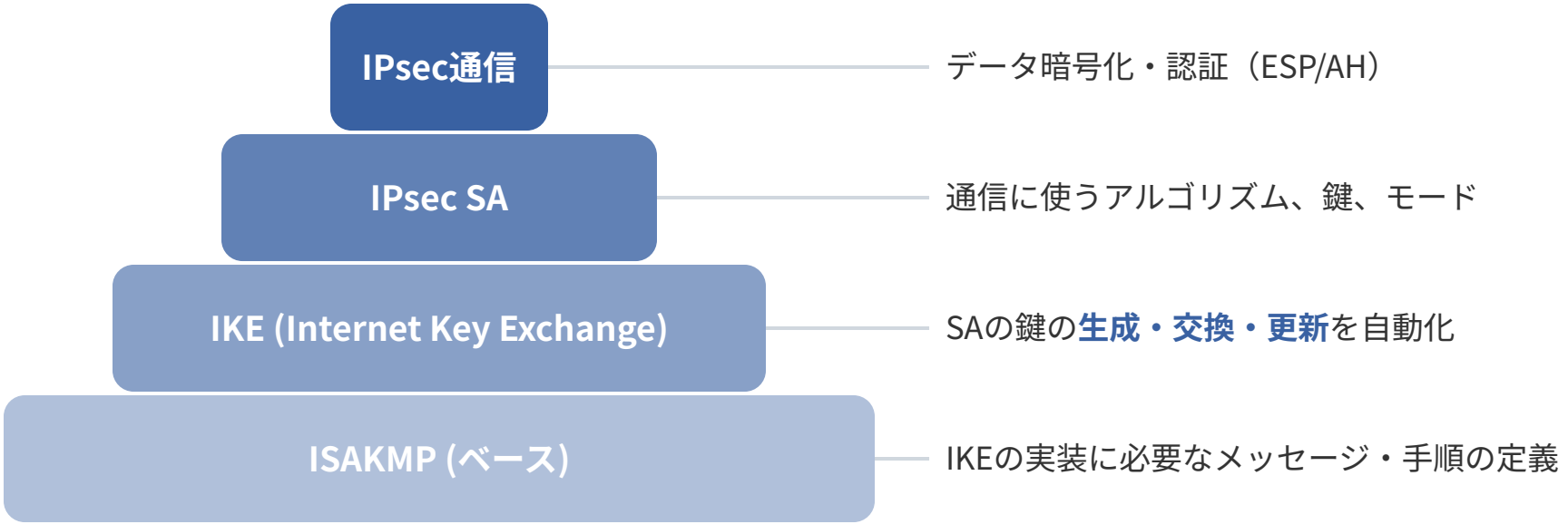
1. IKEの概要と役割
2. IKEの構造：ISAKMPメッセージ
3. IKEフェーズ1：ISAKMP SAの確立
4. IKEフェーズ2：IPsec SAの確立

01

IKEの概要と役割

IKEの役割：鍵管理の自動化

セキュリティアソシエーション（SA）を安全かつ自動で生成・更新する



IKEの動作：フェーズ1とフェーズ2

2段階のプロセスを経て、IPsec通信の準備を完了する

STEP 1	ISAKMP SAの確立
STEP 2	暗号化通信路の確立
STEP 3	IPsec SAの生成
STEP 4	IPsec通信開始

02

IKEの構造：ISAKMPメッセージ

ISAKMPメッセージの仕組み

UDP 500番ポートを利用した『最初の握手』

基本	構成
IKEの実装はISAKMPに基づき行われる	ISAKMPメッセージは**ヘッダ**と**ペイロード**から成る
UDPの**500番ポート**を利用して交換	ヘッダは通信制御情報
VPN通信の『**最初の握手**』にあたる	ペイロードは暗号方式や鍵交換パラメータ

ISAKMPヘッダの主な構成要素

メッセージ制御に必要な情報（試験で問われやすい項目）

項目	説明
Initiator Cookie	通信開始側が生成する識別子
Responder Cookie	通信応答側が生成する識別子
Exchange Type	モードの種類（Main=2, Aggressive=4, Quick=32）
Flags (Eビット)	Eビットが立つとメッセージが**暗号化済み**であることを示す

ISAKMPペイロードの代表的な種類

やり取りする内容に応じて種類が変わる（鍵交換の根幹）

SA (1)	Proposal (2)	Transform (3)
セキュリティアソシエーション情報	提案される暗号アルゴリズム	提案されたアルゴリズムの詳細

KE (4)	NONCE (10)	HASH / SIG (8/9)
鍵交換に必要な値（Diffie-Hellman）	一度きりの乱数値（リプレイ攻撃防止）	認証用のハッシュ値や電子署名

03

IKEフェーズ1：ISAKMP SAの確立

フェーズ1の2つのモードの比較

セキュリティレベルとメッセージ交換回数が異なる

Mainモード		Aggressiveモード
6回	メッセージ交換回数	3回
強固	セキュリティ	柔軟性に欠ける
遅い	処理速度	速い

フェーズ1で決定される主なパラメータ

ISAKMPメッセージの暗号化・認証の基盤を決定する

暗号化アルゴリズム

ISAKMPメッセージの暗号化方式（AES / 3DES）

ハッシュアルゴリズム

認証や鍵計算に利用（MD5 / SHA-1）

認証方式

機器の正当性確認（事前共有鍵 / デジタル署名）

04

IKEフェーズ2：IPsec SAの確立

フェーズ2：QuickモードによるIPsec SAの確立

フェーズ1のISAKMP SA上で暗号化された状態で実行される

セキュリティプロトコル (AH/ESP) の決定

暗号化/認証アルゴリズムの決定

カプセル化モード (トンネル/トランスポート) の決定

鍵のライフタイムを決定

DHグループ（PFS）の利用を決定

IPsec SAの生成・完了