VPN

学習内容

1. VPNの基本概念とメリット
2. VPNの種類と接続形態
3. VPNの安全性を支える技術
4. プロトコルの比較と試験の重要ポイント

01

VPNの基本概念とメリット

VPNとは：公衆網で専用線のような安全性を実現する技術

Virtual Private Network（仮想専用ネットワーク）の仕組み

VPNは、インターネットなどの公衆回線上に「**仮想的な専用回線**」を構築する技術

暗号化と**トンネリング**により、第三者からの盗聴・改ざんを防ぎ安全な通信を実現

高額な**専用線**や広域イーサネットに比べ、大幅に**WAN接続コスト**を削減できる

IPsecなどのセキュリティ技術を組み合わせ、安全性を確保しながら企業の拠点間通信（WAN）を低コストで実現

VPNのコア技術：安全性を支える二大要素

トンネリングと暗号化により、機密性の高い通信路を構築

データを読めない形に変換し、盗聴・改ざんを防止

公衆網の上に仮想的な専用回線（トンネル）を構築

通信相手の身元確認と適切なアクセス権の付与

02

VPNの種類と接続形態

【比較】VPNの主要な種類

インターネットVPNとIP-VPN（MPLS-VPN）の対比

インターネットVPN	IP-VPN（MPLS-VPN）
公衆回線（インターネット）を利用	通信事業者の**閉域IP網**を利用
IPsecや**SSL/TLS**を用いて暗号化	**MPLS**を用いて経路情報を管理
低コストで導入しやすい	インターネットを経由せず、高品質で安定
回線の混雑状況に品質が左右される	インターネットVPNよりコストが高くなる

インターネットVPNの2つのプロトコル

暗号化技術による分類

IPsec-VPN	SSL-VPN
IPsecを利用し、ルータやVPNゲートウェイ間で通信を暗号化	**SSL/TLS**を利用し、Webブラウザや専用クライアントで安全な接続を実現

インターネットVPNの2つの接続形態

用途による利用シーンの違い

サイト間VPN（拠点間）

企業の**複数拠点**を**ルータ同士**で接続する方式。ルータが暗号化を処理する

リモートアクセスVPN

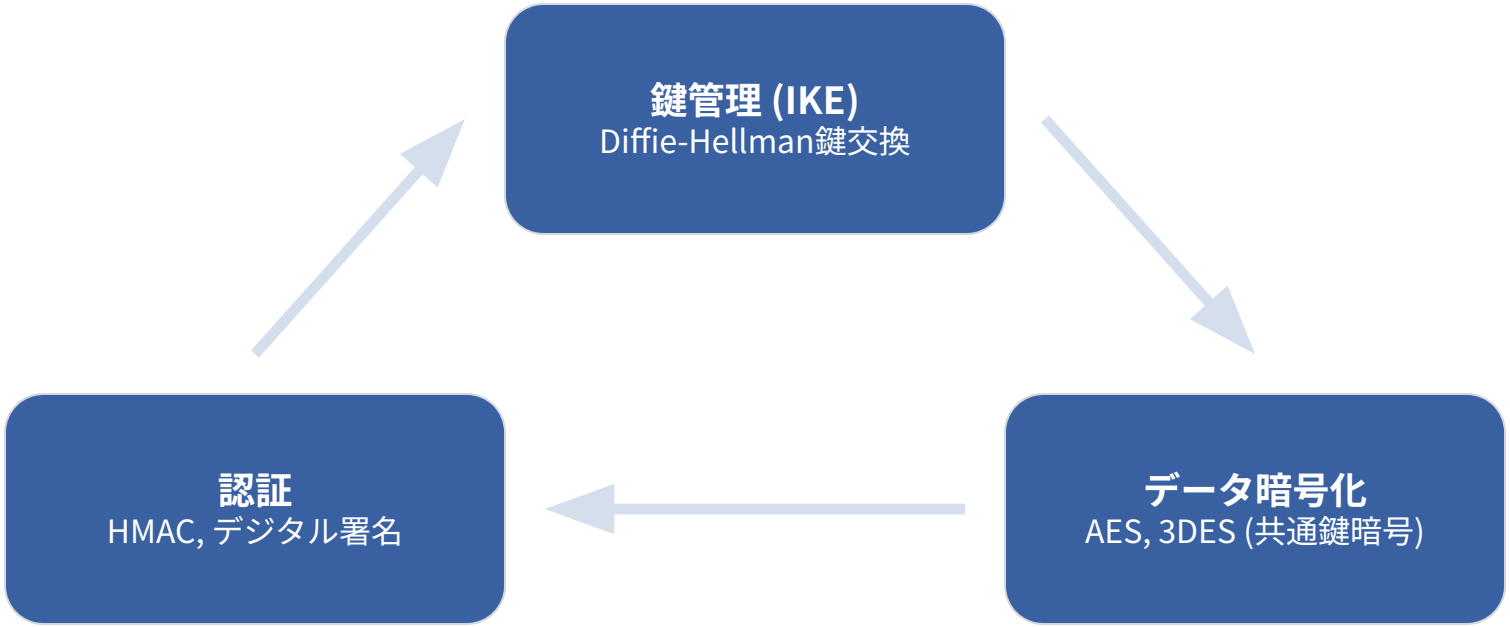
外出先や自宅のPCから**社内ネットワーク**へ安全に接続する方式。テレワークで多用

03

VPNの安全性を支える技術

IPsecを構成するセキュリティの基本要素

VPNの安全性を担保する4つの要素



【試験対策】暗号化方式の分類と特徴

共通鍵暗号と公開鍵暗号の対比

共通鍵暗号（対称暗号）		公開鍵暗号（非対称暗号）
1つ（共通鍵）	鍵の数	2つ（公開鍵/秘密鍵）
高速	処理速度	低速
AES、3DES、RC4	代表例	RSA、ElGamal
実データの暗号化	主な用途	鍵交換、デジタル署名

鍵管理と改ざん検知の重要用語

IPsecにおける役割の整理

Diffie-Hellman鍵交換

鍵交換方式

共通鍵の安全な共有

ハッシュ関数

改ざん検知

データの整合性保証

HMAC

認証

共通鍵を用いた認証

デジタル署名

認証

公開鍵を用いた送信者確認

04

プロトコルの比較と試験の重要ポイント

【比較】主要なVPNプロトコル

マルチキャスト対応と暗号化機能の有無

プロトコル	伝送プロトコル	マルチキャスト対応	暗号化
IPsec	IP	×	○
GRE	IP	○	×
L2TP	UDP/IP	○	×

GRE over IPsec：ルーティング利用時の鉄則

IPsecの弱点を補完する組み合わせ技術

IPsec単独では**マルチキャスト通信**をトンネルできない

OSPFやEIGRPなどのルーティングプロトコルを拠点間で利用するには**マルチキャスト対応**が必要

GRE（Generic Routing Encapsulation）はマルチキャストを扱えるが暗号化機能がない

解決策として、GREでマルチキャスト対応のトンネルを作り、それを**IPsecで暗号化**する（GRE over IPsec）

CCNAで問われるVPN重要テーマまとめ

必ず押さえるべき知識の整理

VPNの基本

専用線のような安全性を公衆網で実現（トンネリングと暗号化）

分類

インターネットVPN（低コスト・低品質）とIP-VPN（高コスト・高品質）の対比

プロトコル

IPsec（暗号化○、マルチキャスト×）とGRE（暗号化×、マルチキャスト○）