情報通信ネットワーク
第14回

理工学部情報科学科
松澤　智史

本日のコンテンツ

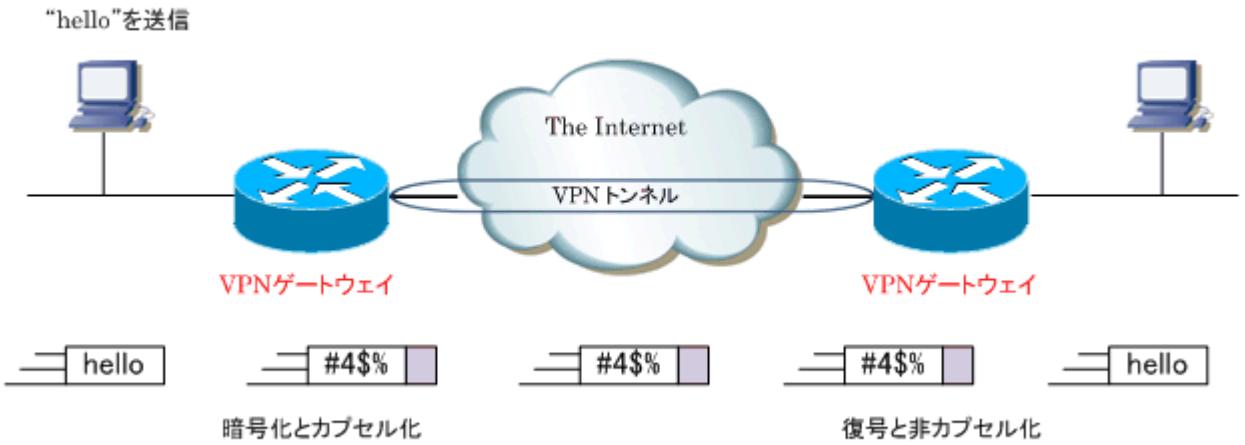
- LANに関する技術
  - VPN
    - カプセル化とトンネリング
    - IPSec
    - 暗号アルゴリズム
  - ファイアウォール
  - IDS,IPS
- その他の暗号プロトコル
  - TLS/SSL

VPN(Virtual Private Network)

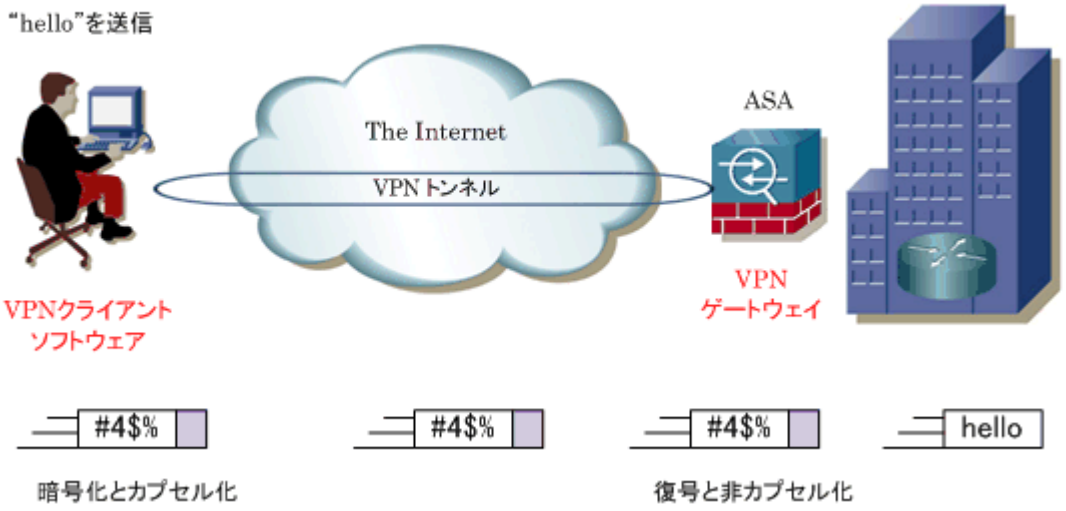
- 仮想的なプライベートネットワーク接続
- インターネットVPN
  - インターネットなどの公衆網を利用したVPN
- IP-VPN
  - 通信事業者が提供するIPネットワークを利用したVPN

VPNの接続形態

- サイト間VPN



- リモートアクセスVPN



VPNを構成する技術

- トンネリング（カプセル化）
  - ある通信プロトコルに他の通信プロトコルのヘッダを付加する（カプセル化）
  - ある通信プロトコルの環境の上に、異なる通信プロトコルを透過的に流す

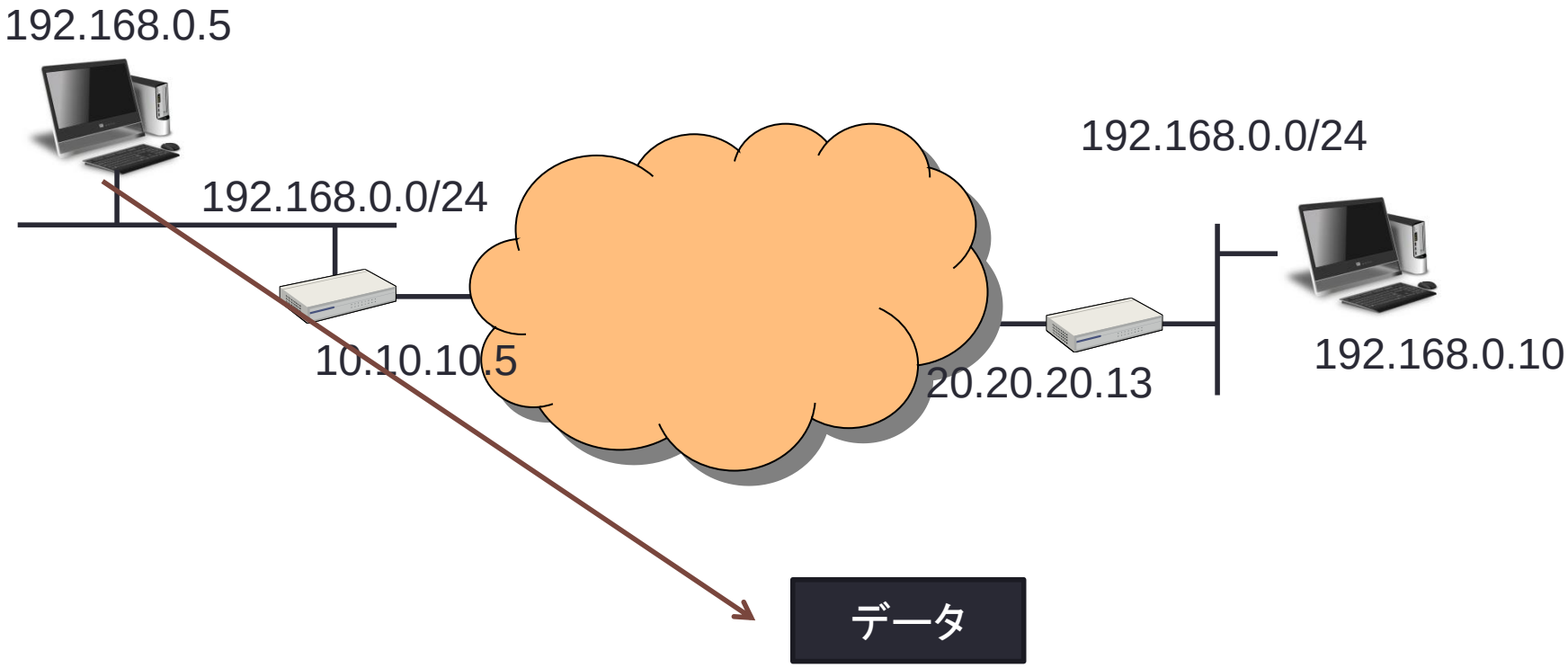
- 暗号
  - 共通鍵暗号
  - 公開鍵暗号
  - 鍵交換

トンネリングとカプセル化

カプセル化

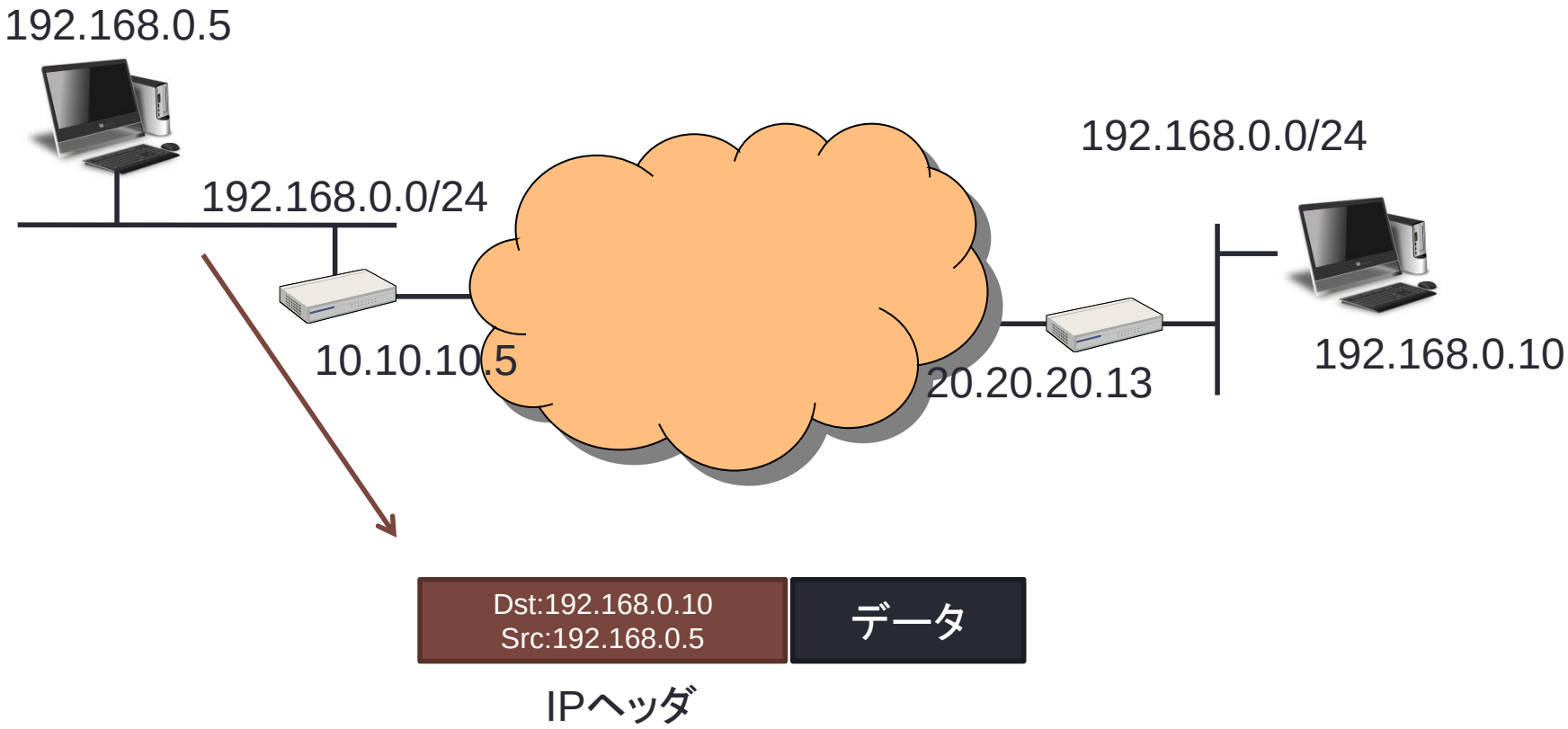
トンネリング

もう少し詳しくみていこう



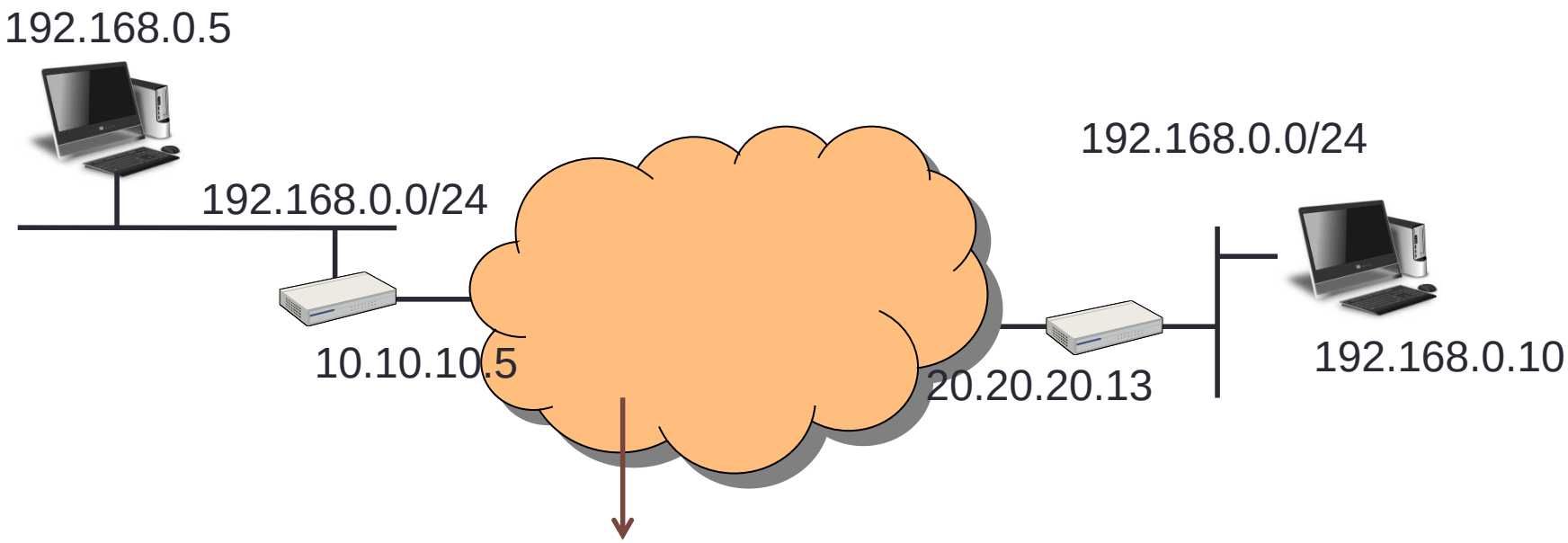
物理的に異なる位置に同じネットワークを構成したい

もう少し詳しくみていこう



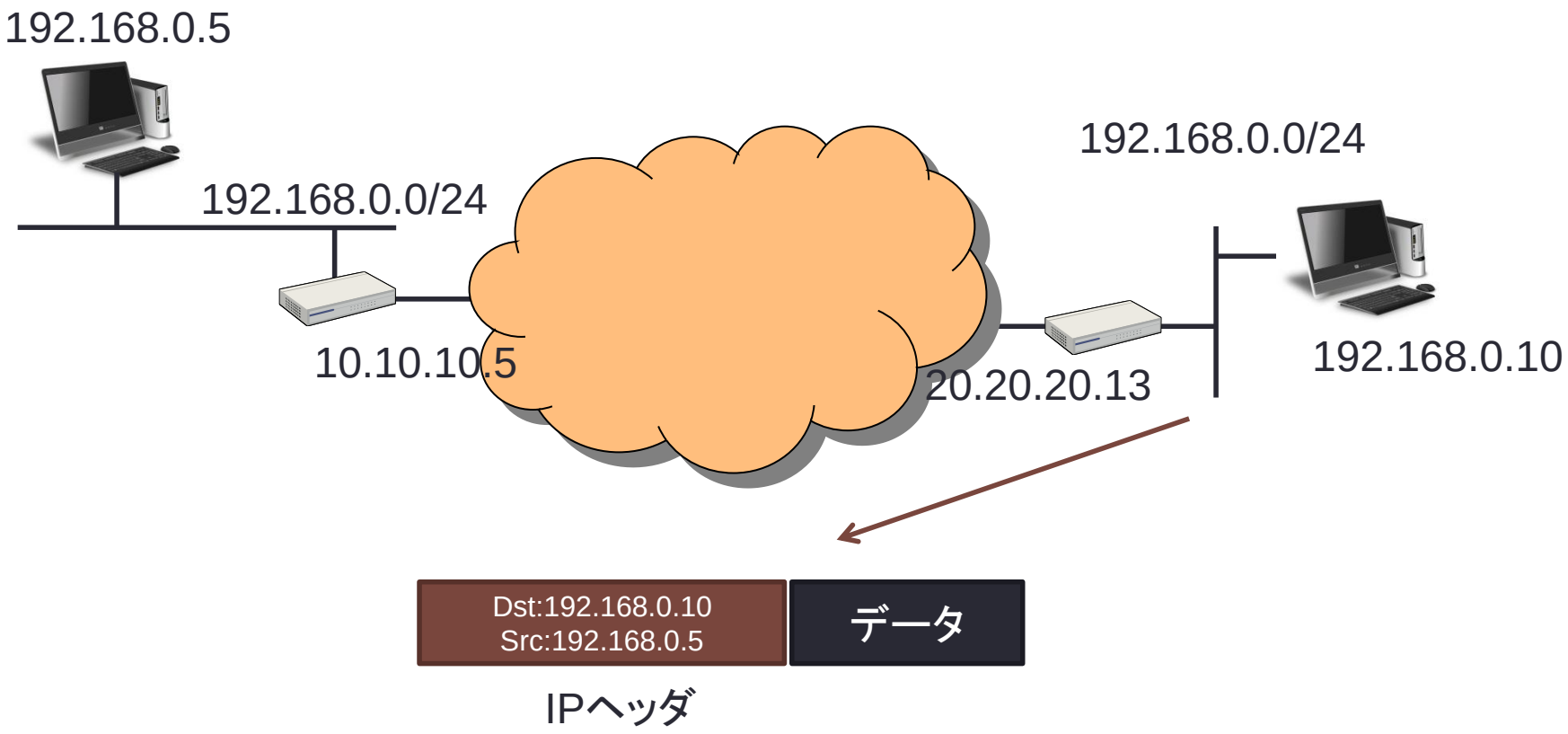
物理的に異なる位置に同じネットワークを構成したい

もう少し詳しくみていこう



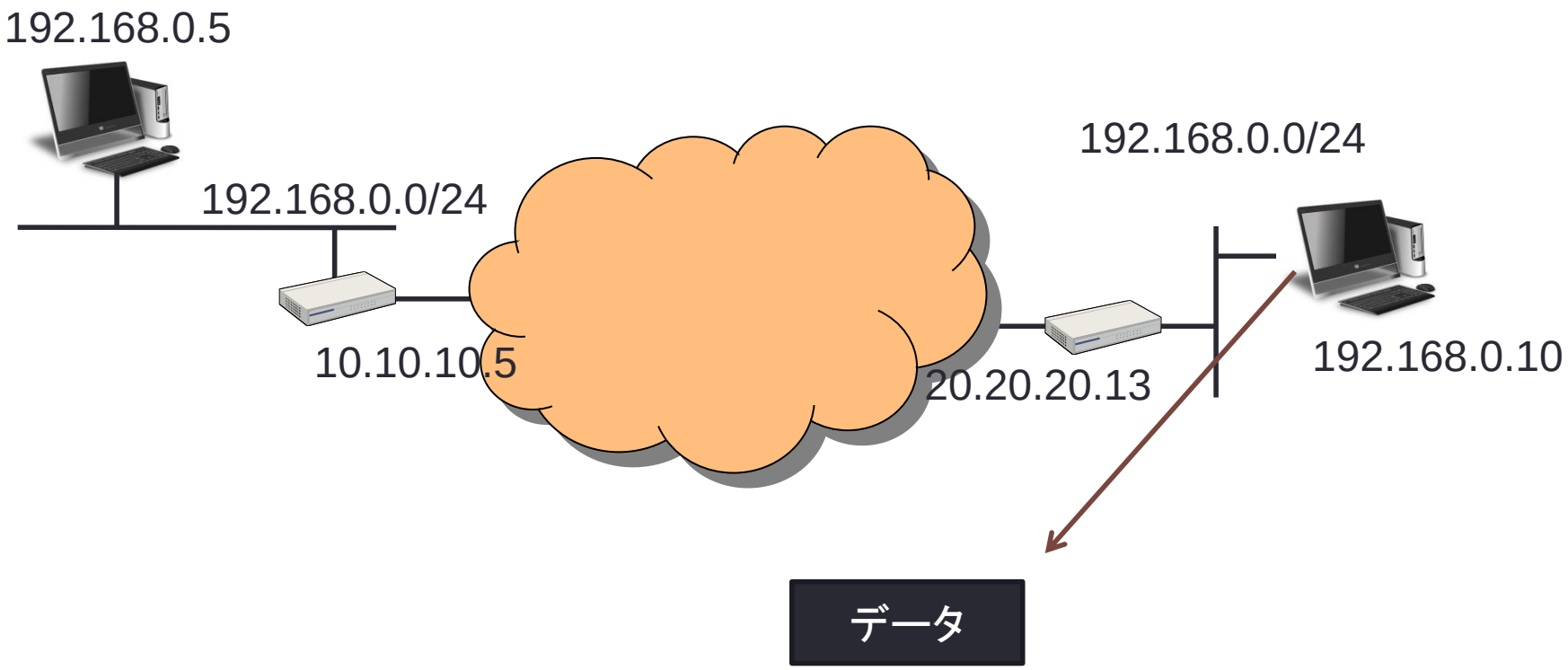
物理的に異なる位置に同じネットワークを構成したい

もう少し詳しくみていこう



物理的に異なる位置に同じネットワークを構成したい

もう少し詳しくみていこう



物理的に異なる位置に同じネットワークを構成したい

トンネリング用のプロトコル

プロトコル	層	マルチキャスト可	暗号可
IPsec	L3 (IP)	×	○
GRE	L3 (IP,他)	○	×
L2TP	L2 (PPP) L3(IP,他)	○	×

IPSec

- ネットワーク層でデータを保護するためのアーキテクチャ
- VPNはIPSec利用例の1つ
- 機能
  - 通信内容の秘匿
  - 通信相手の認証
  - 通信内容の改ざん検出
- IPSec プロトコル
  - AH(Authentication Header)
    認証，改ざん検知が可能なプロトコル
  - ESP(Encapsulating Security Payload)
    秘匿，改ざん検知が可能なプロトコル
  - IKE(Internet Key Exchange)
    鍵交換プロトコル

IPSecで使用されるアルゴリズム

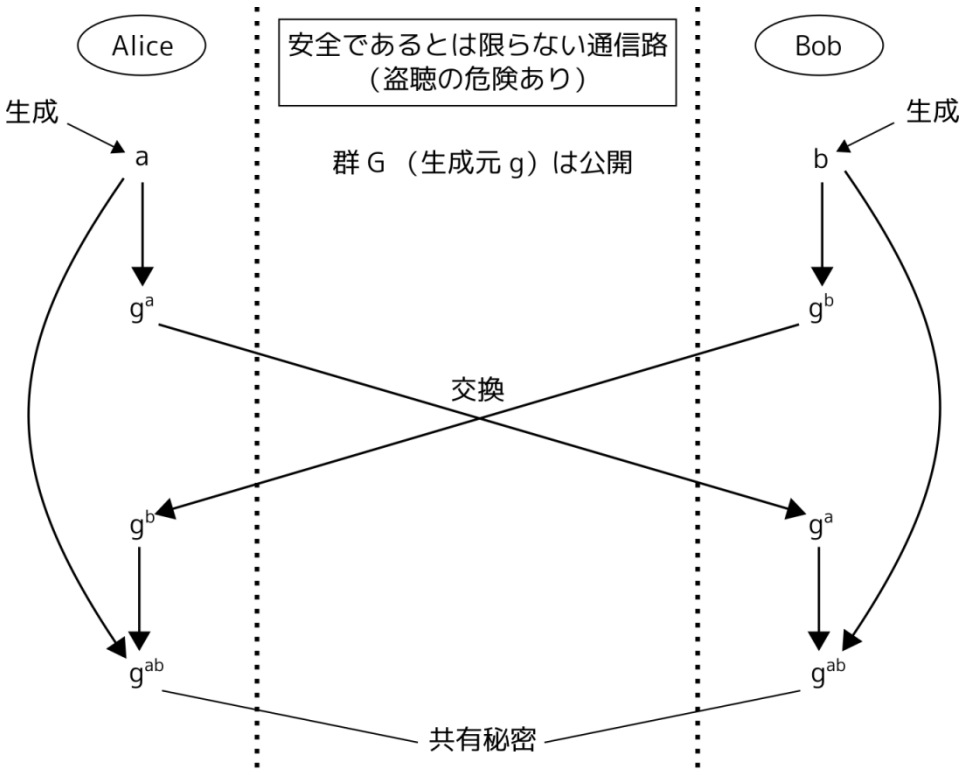
- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

IPSecで使用されるアルゴリズム

- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

Diffie-Helman

- 前提(離散対数問題)
  - $h = g^x \pmod p$ gは群Gの生成元，pは素数
  - gとhが既知であってもxを求めるのは容易ではない
- アルゴリズム



IPSecで使用されるアルゴリズム

- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

Elgamal暗号

- $GF(p)$のpと生成元gを選ぶ
- xをZ_p^*からランダムに選ぶ (秘密鍵)
- $h = g^x$とする.
- (p, g, h)を公開しxを秘密鍵とする
- 平文$m \in Z_p^*$において, $r \in Z_p^*$とし, 暗号文c_1とc_2を

$$c_1 = g^r, c_2 = m \times h^r$$ と計算する

- 暗号文$c_1, c_2 \in Z_p^*$において暗号文mを

$$m = c_2 \times (c_1^x)^{-1}$$ と計算する

IPSecで使用されるアルゴリズム

- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

RSA

- 素数pとqを選ぶ,$n = p * q$とする(pとqは互いに素)
- $\gcd(e, (p-1)(q-1)) = 1$となるeを選ぶ
- $ed = 1\ mod\ (p-1)(q-1)$となるdを選ぶ(秘密鍵)
- (n, e)を公開鍵とする

- 平文$m \in Z_p^*$において暗号文cを

$$c = m^e mod\ n$$ と計算する

- 暗号文$c \in Z_p^*$において暗号文mを

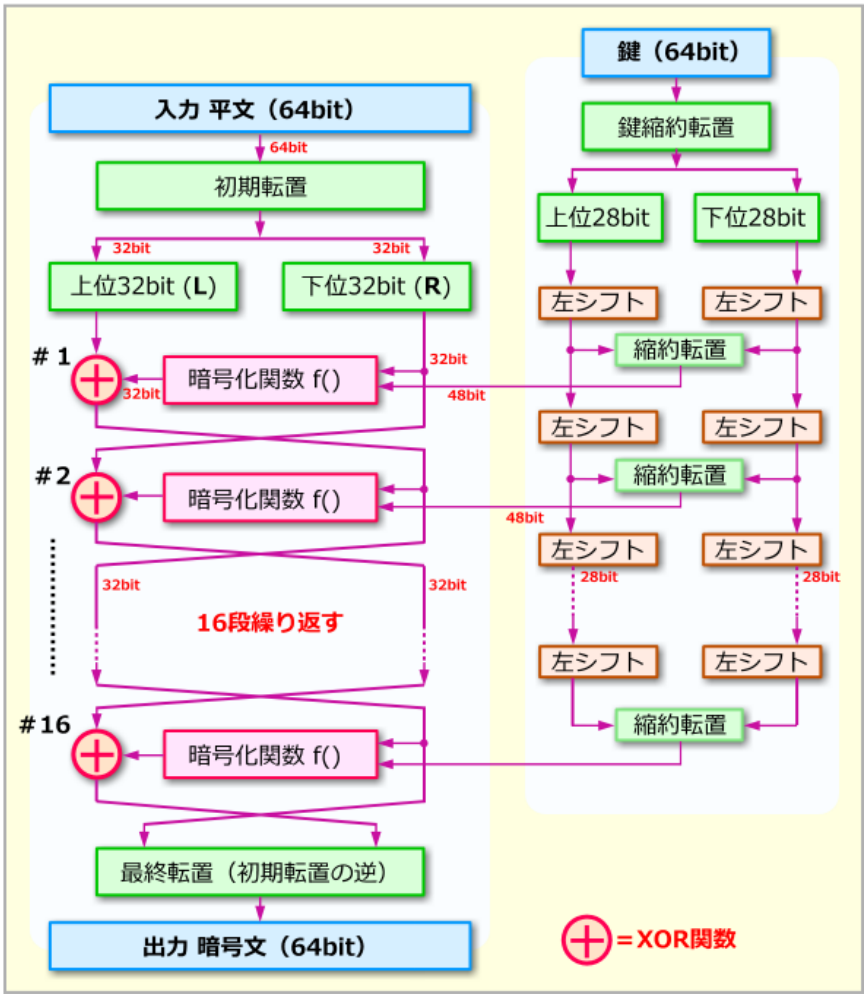
$$m = c^d mod\ n$$ と計算する

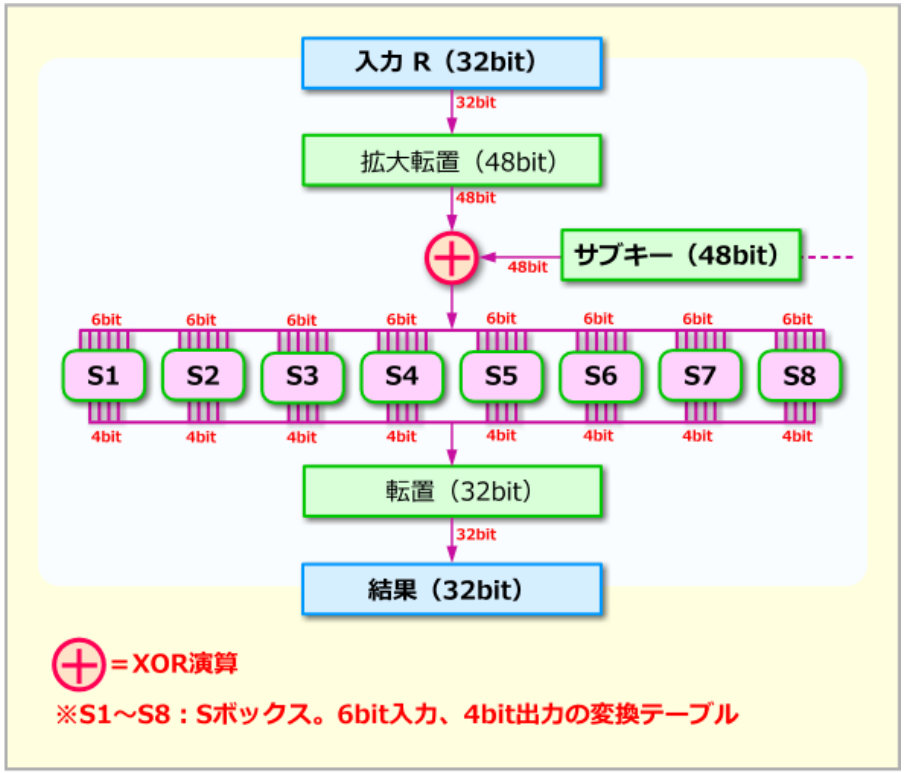
IPSecで使用されるアルゴリズム

- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

DES(Data Encryption Standard)

- 共通鍵を使って転置，シフト，XORを繰り返す



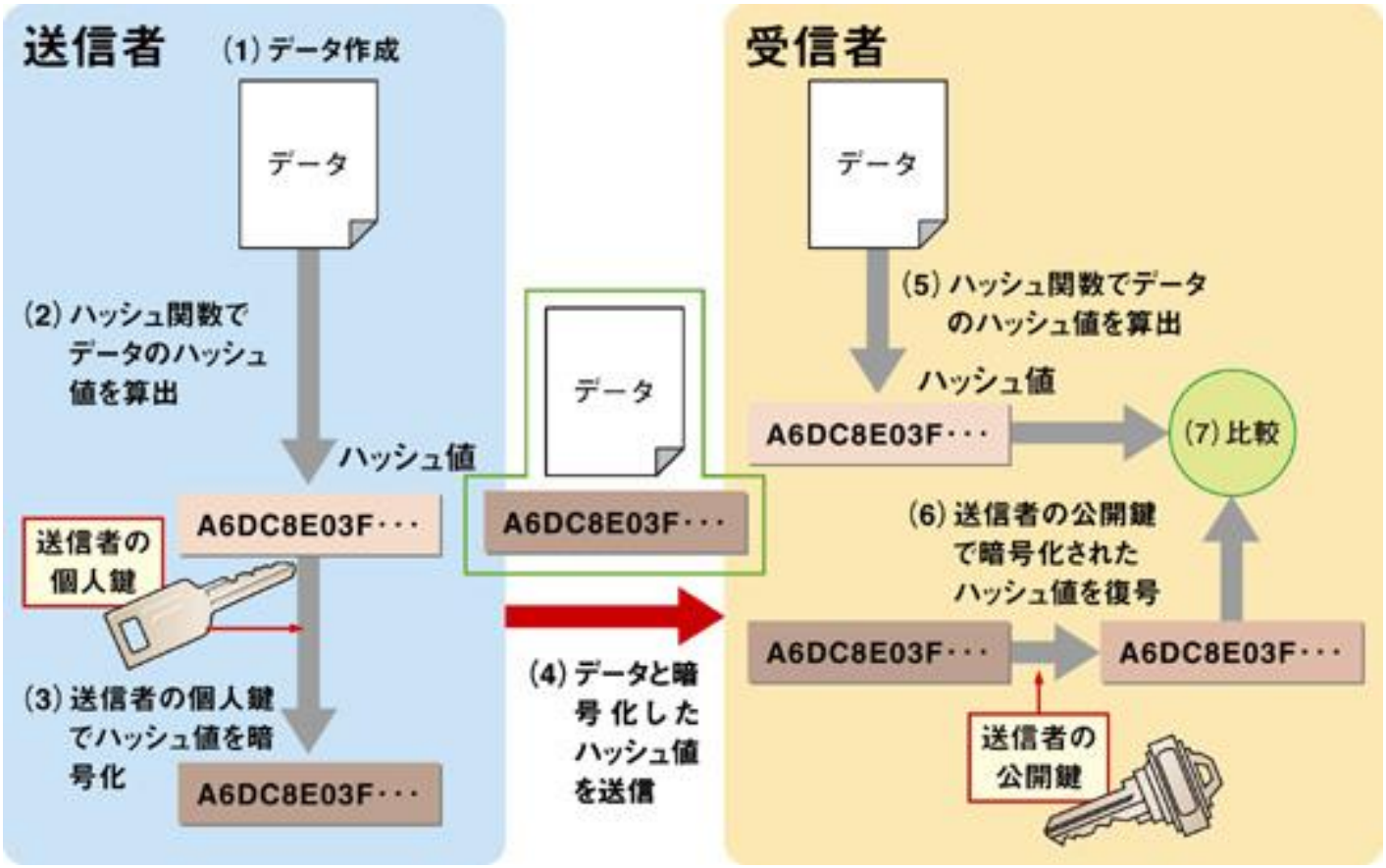


IPSecで使用されるアルゴリズム

- 鍵交換（IKE)
  - Diffie-Hellman
- 暗号化
  - 公開鍵暗号
    - Elgamal, RSA
  - 共通鍵暗号
    - DES, 3DES, AES
- デジタル署名
  - RSA, DSA

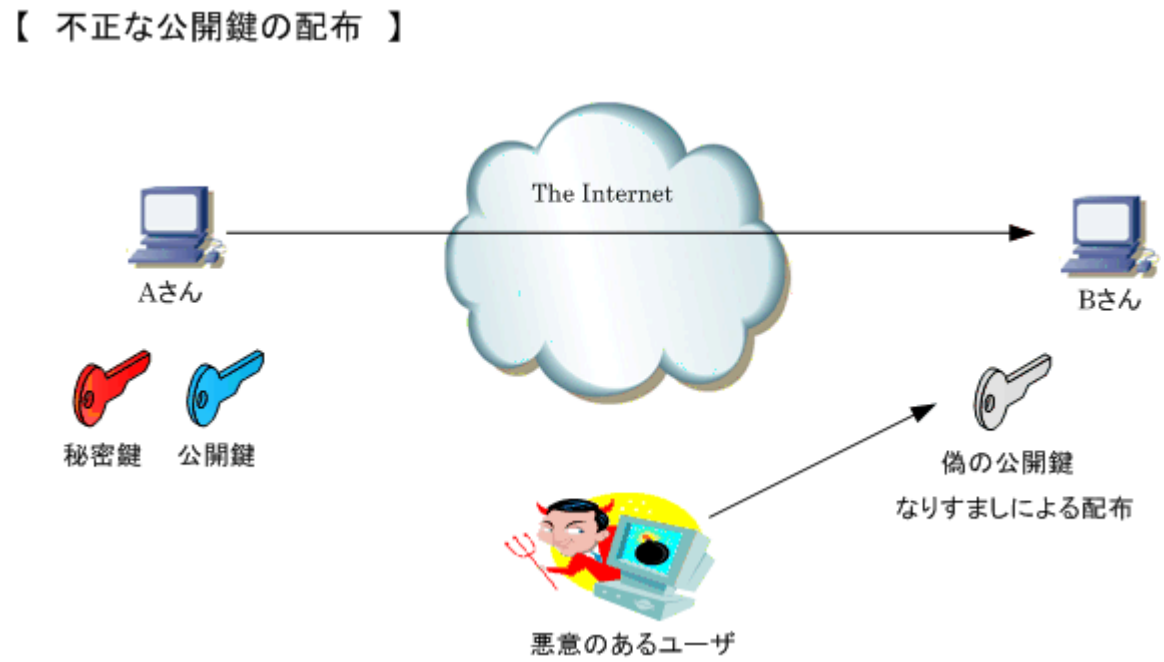
デジタル署名(電子署名)

- 公開鍵暗号とハッシュを用いて改ざんを防止する
- 秘密鍵で暗号化し，公開鍵で復号する(公開鍵暗号とは逆)



デジタル認証

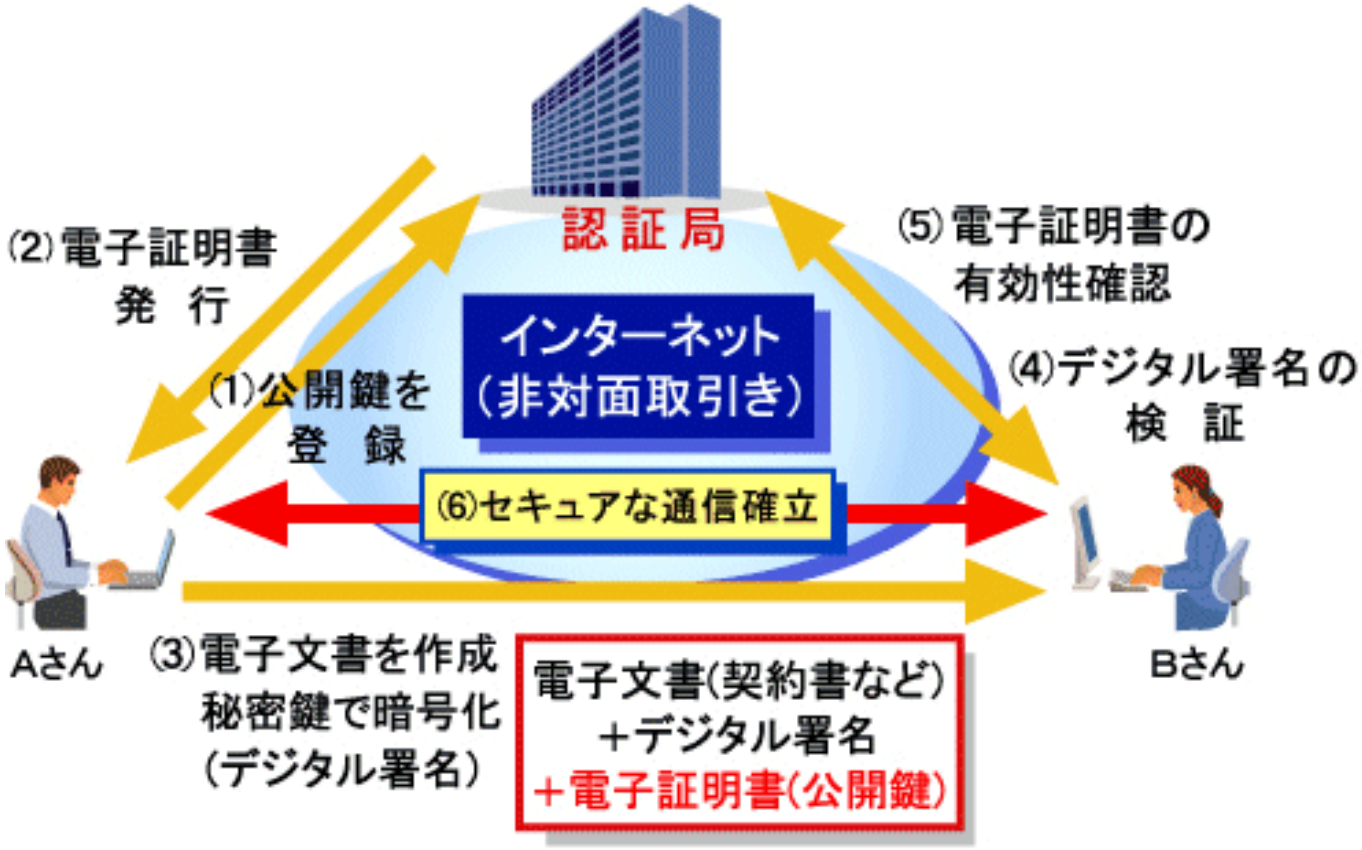
- デジタル署名を用いて階層的に認証を行う方法



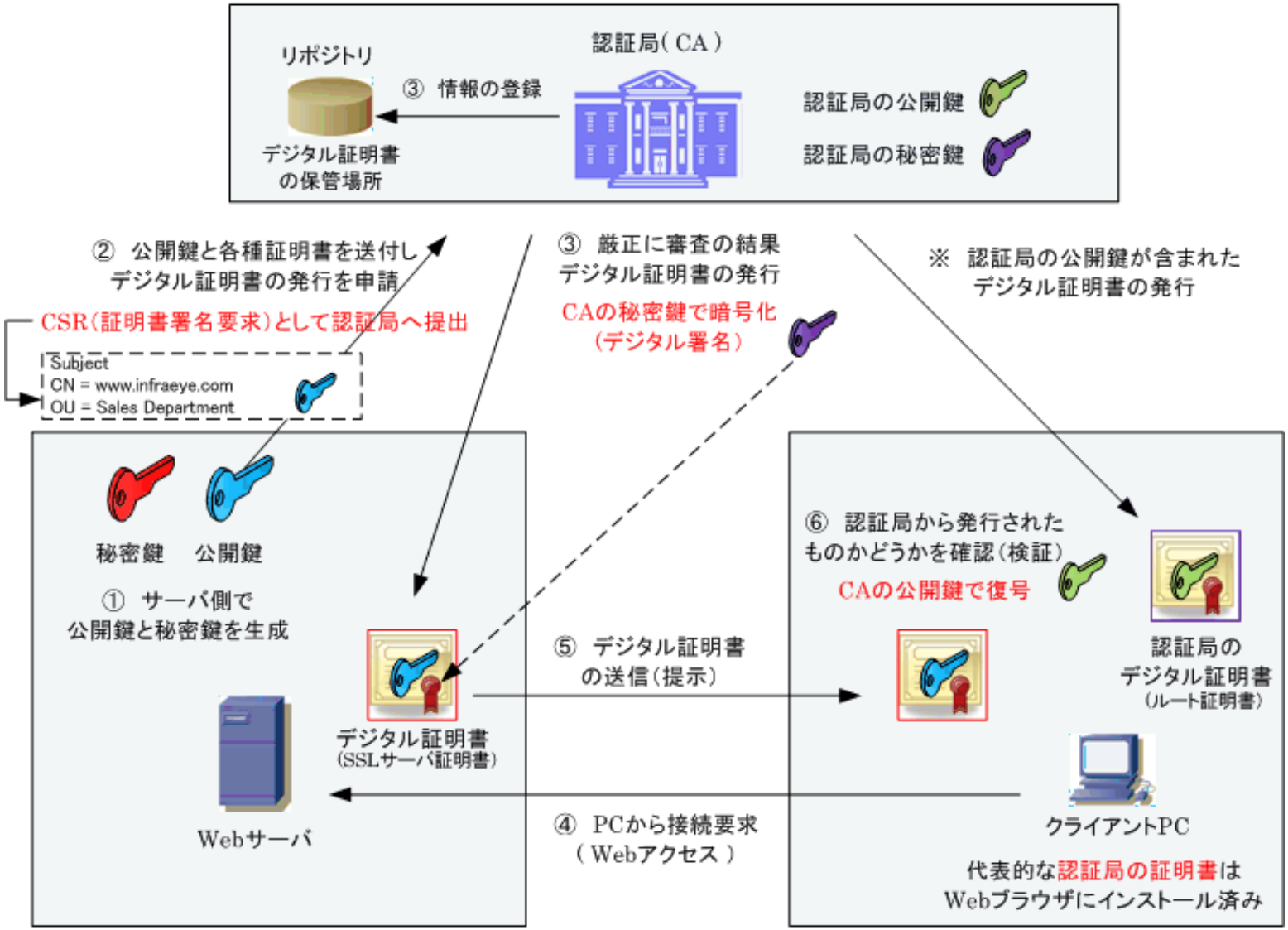
このケースはデジタル署名だけでは防げない

デジタル認証の仕組み

- CA(Certification Authority)と呼ばれる認証局のデジタル署名を受けたデジタル証明書(電子証明書)を使用する

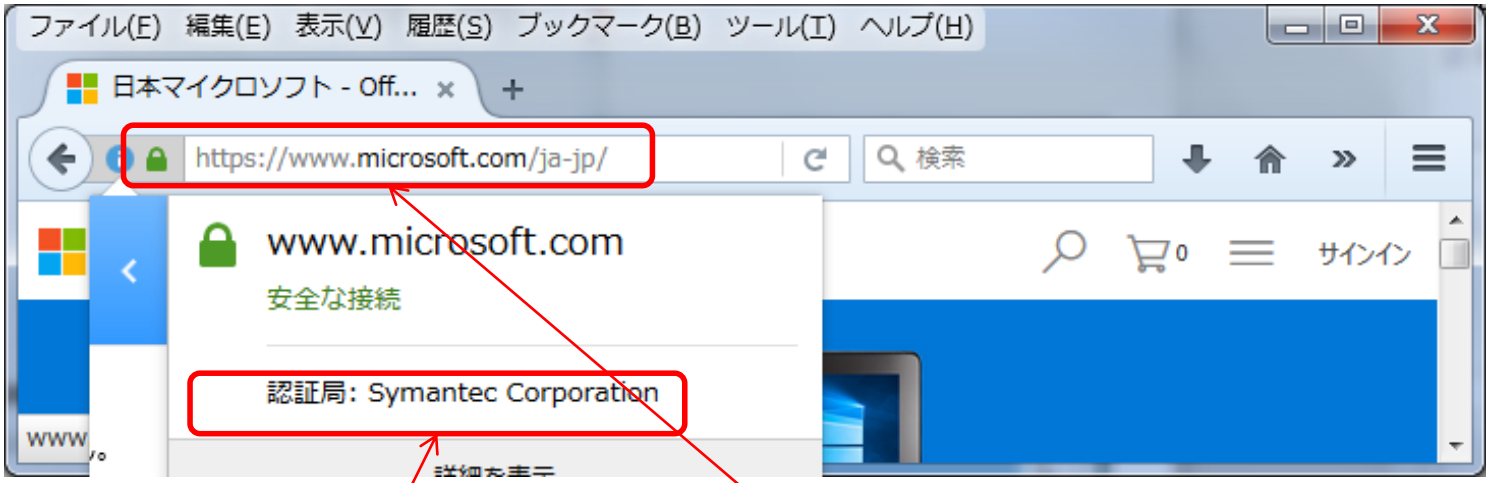


【 デジタル証明書を使用したデジタル署名の仕組み 】



http://www.infraexpert.com/study/security6.html

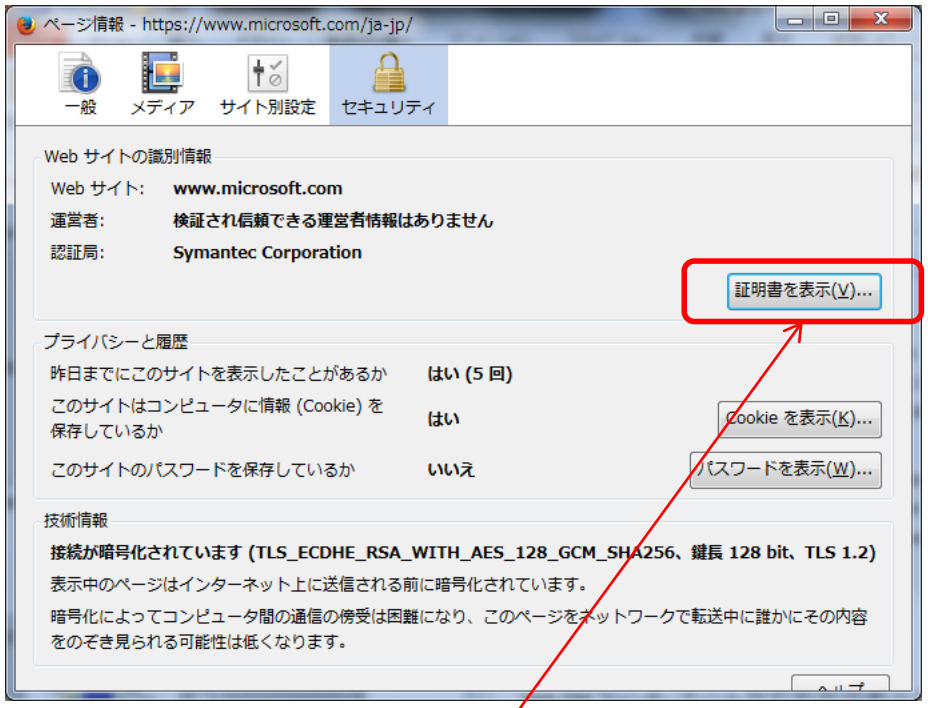
証明書を確認してみよう



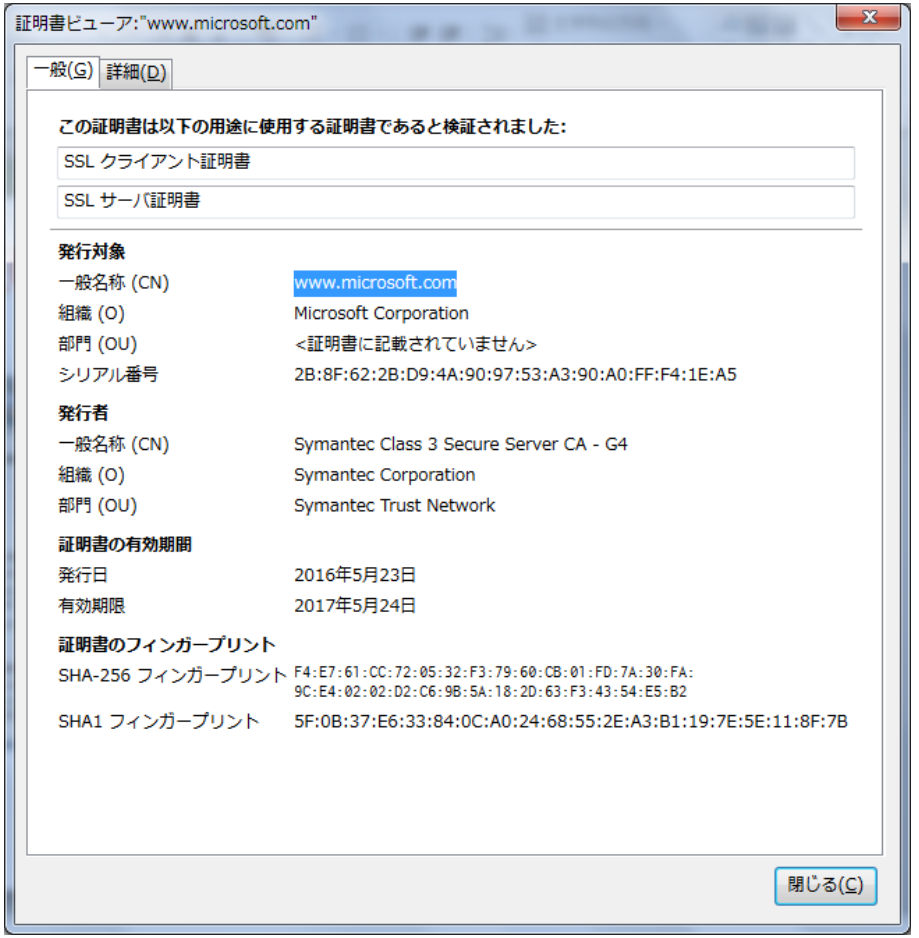
どのCAから認証を受けているか確認

https SSLが使われている通信
鍵マークをクリック(Firefox)

証明書を確認してみよう



証明書を表示

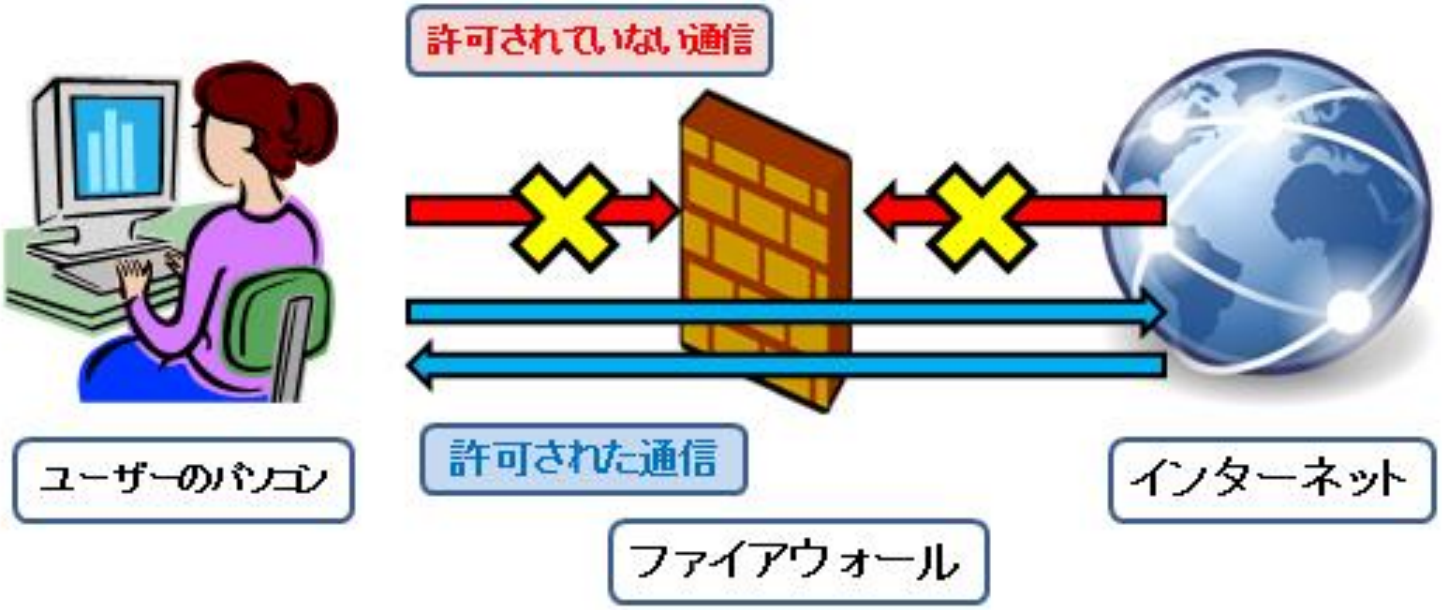


VPNまとめ

- カプセル化を行いトンネリングで拠点間のデータ転送を行う
- トンネルプロトコルとしてIPSecなどが使われる
- IPSecはセキュリティのフレームワークで，
  鍵交換，暗号化(秘匿，認証，改ざん検知)が行える

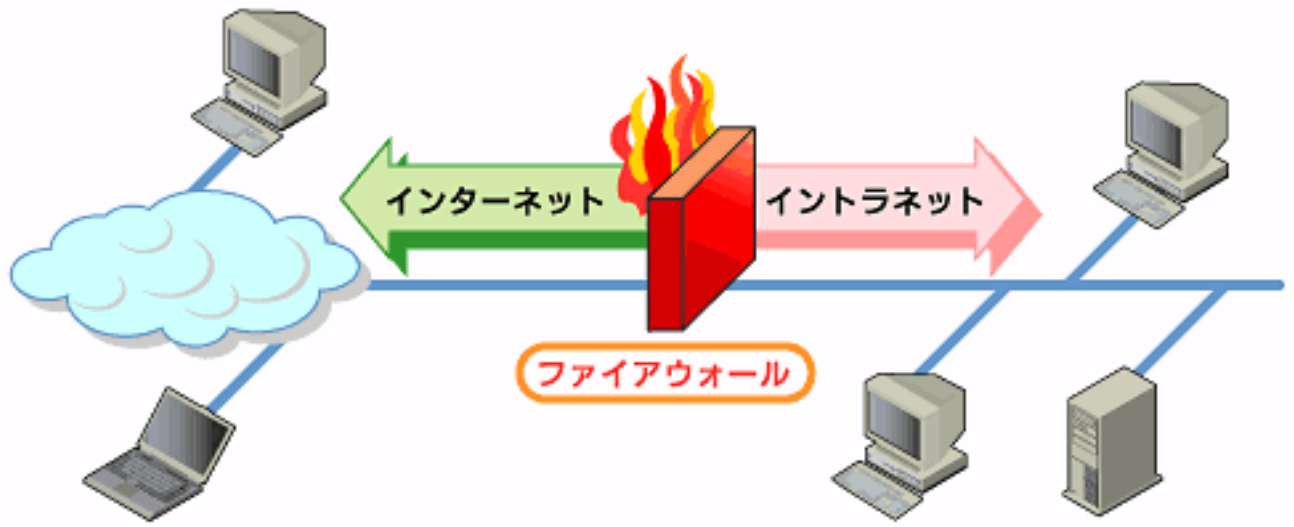
ファイアウォール

- 不審な通信を遮断するソフトウェア
- パケットフィルタリング型
  - IPアドレス，ポート番号で通過の判断を行う
- アプリケーションゲートウェイ型
  - 特定のアプリケーションの通信内容を見て通過の判断を行う



ファイアウォールの設置場所

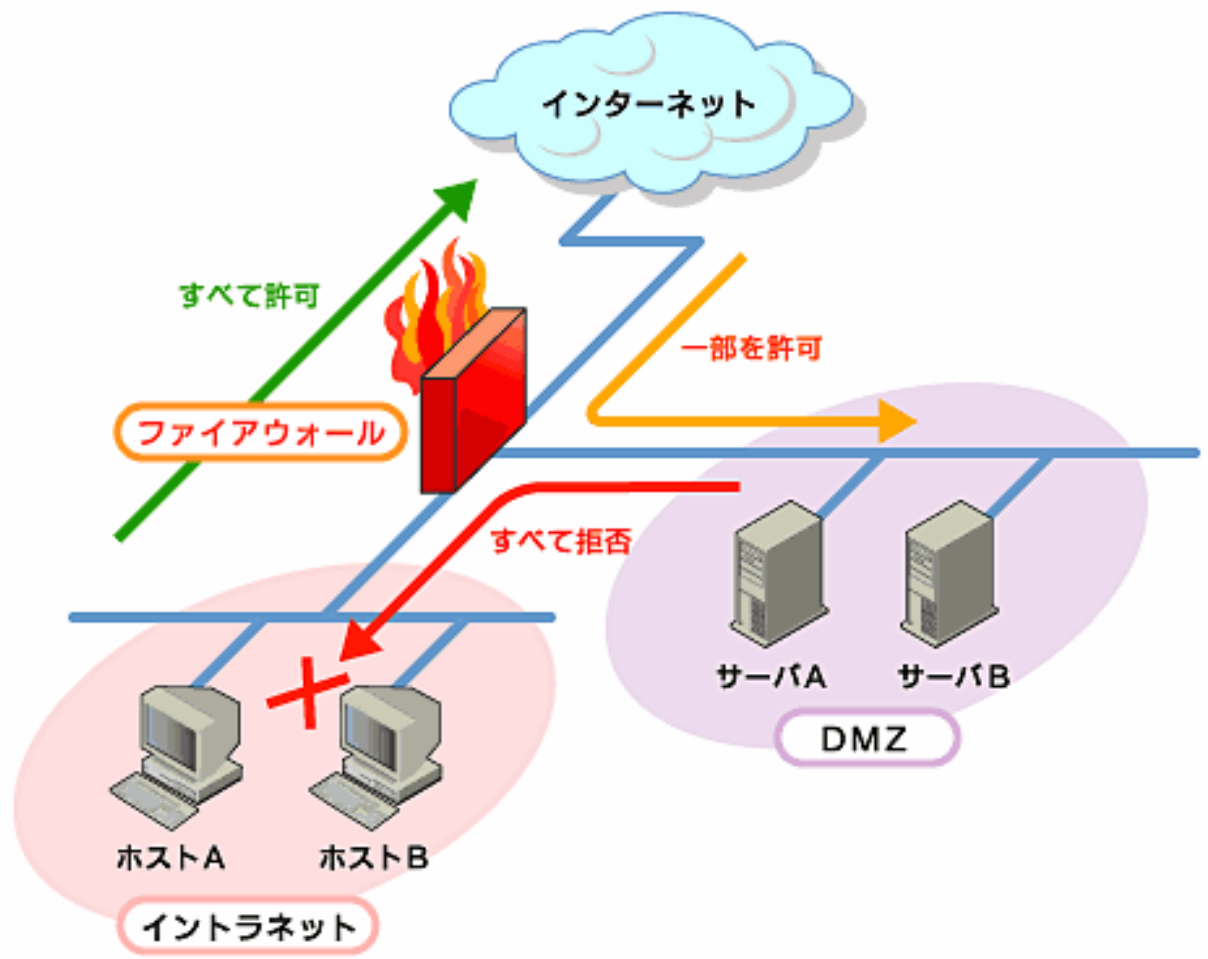
- 一般的には内部ネットワーク（イントラネット）と外部ネットワークとの境界に置く



- ただしこの場合，公開したいサーバなどの機器がある場合に不便となる

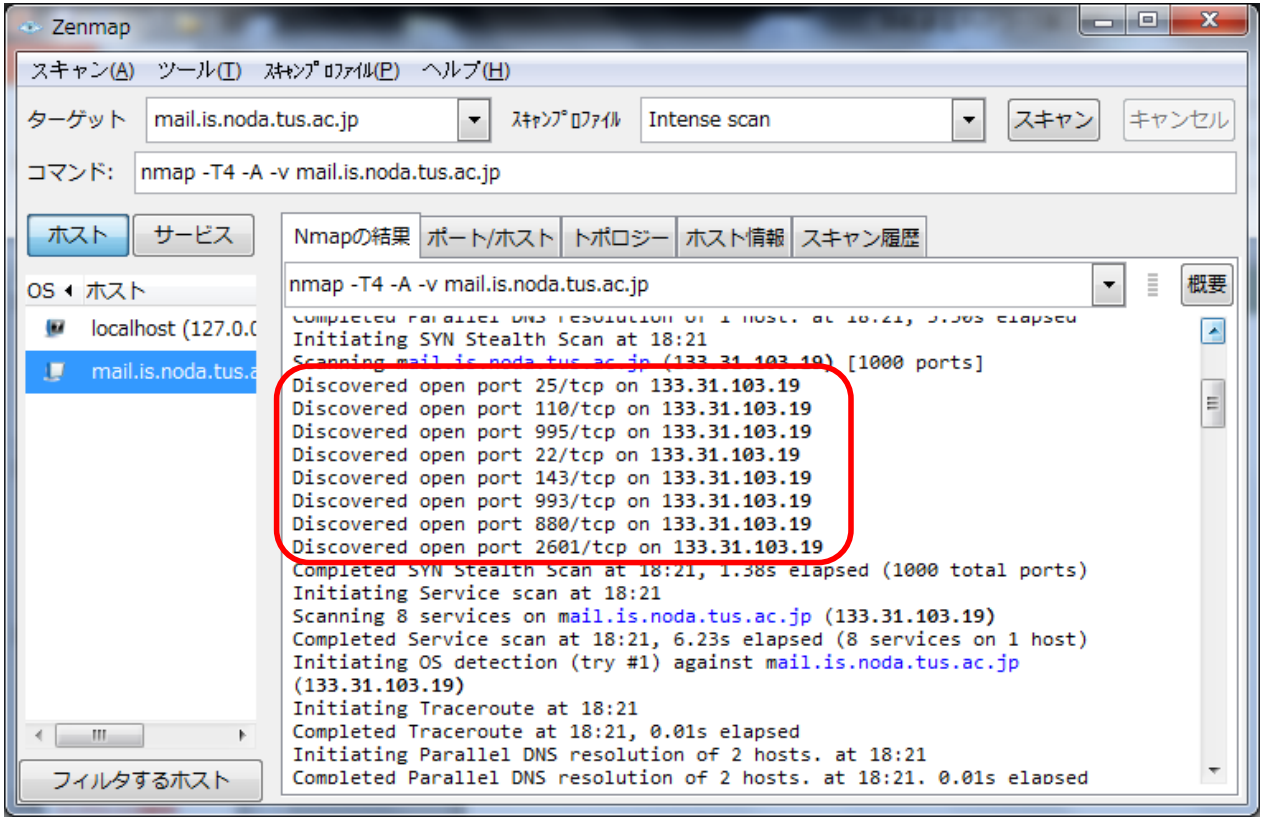
ファイアウォールの設置場所

- DMZ(DeMilitarized Zone)を設ける



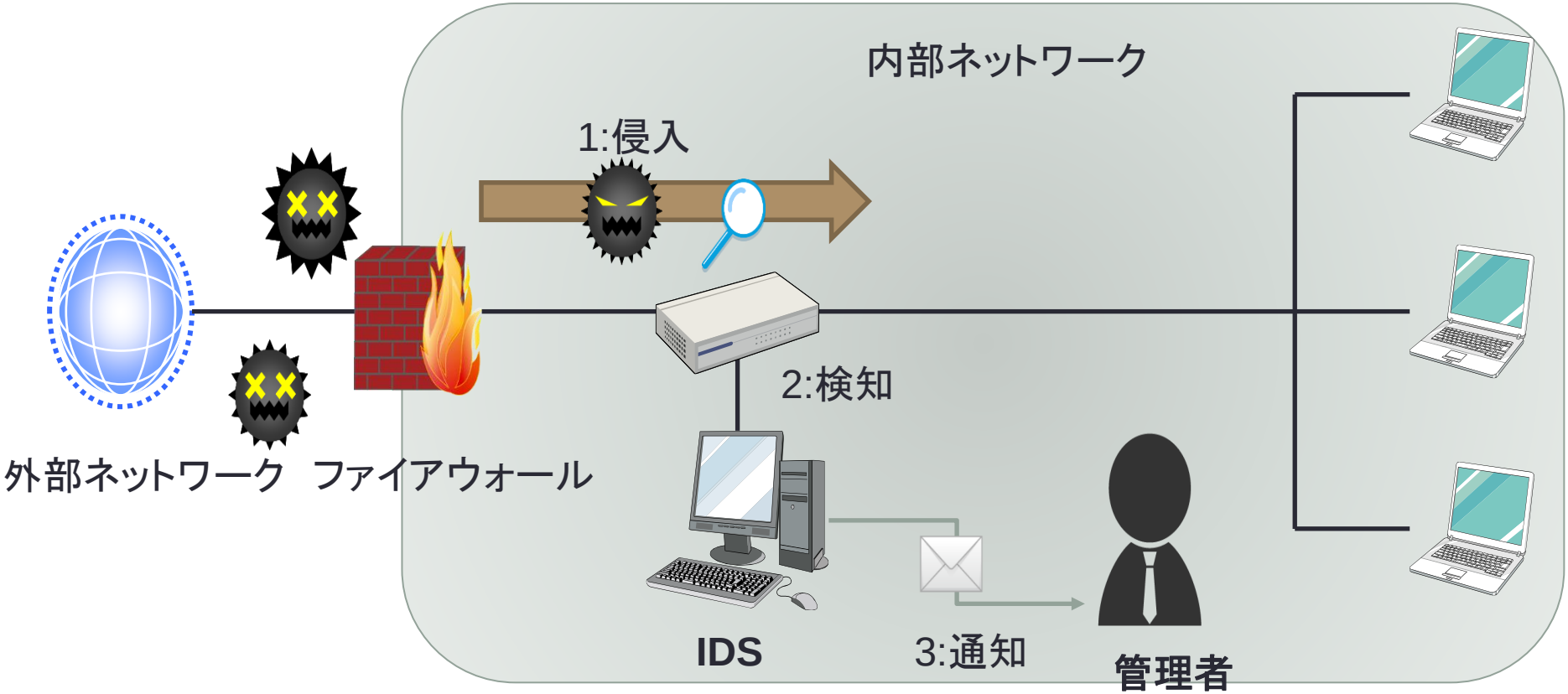
ツール: nmap

- ポートスキャンツール
- 動作しているポート番号をチェックする
- https://nmap.org/download.html



IDS(Intrusion Detection System)

- 侵入検知システム
- 不正な侵入や攻撃を検知すると管理者に通知するシステム
- 検知方法からシグネチャ型とアノマリ型に分類される



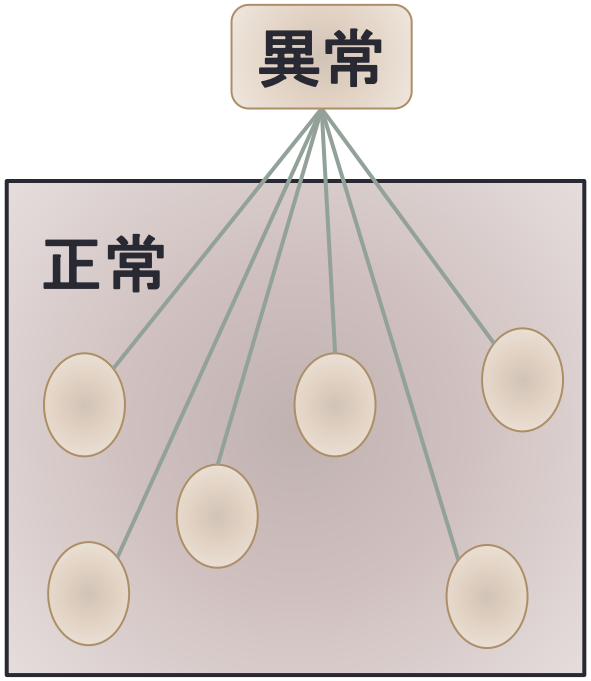
IDSの種類

- シグネチャ型
  - 不正な侵入や攻撃の特徴データ(シグネチャ)をあらかじめ定義しておき
    シグネチャと一致したものを脅威として検知する
  - 既知の攻撃しか対応できない

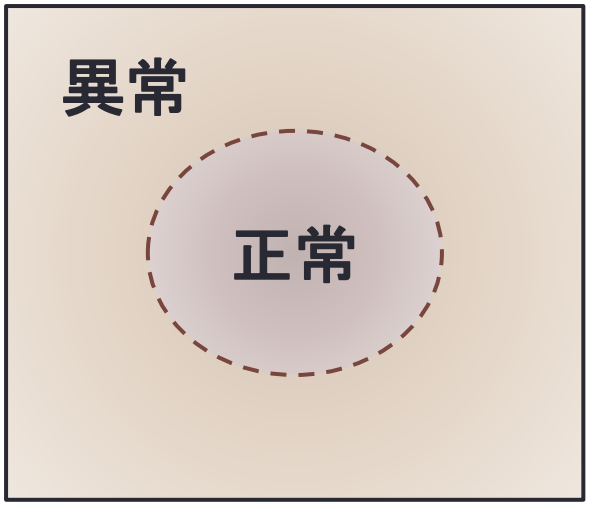
- アノマリ型
  - 監視対象の正常な状態をあらかじめ定義しておき
    これと大きく異なった状態となった場合に異常として検知する
  - 未知の攻撃にも対応することができる

IDSの種類

- 検知方法



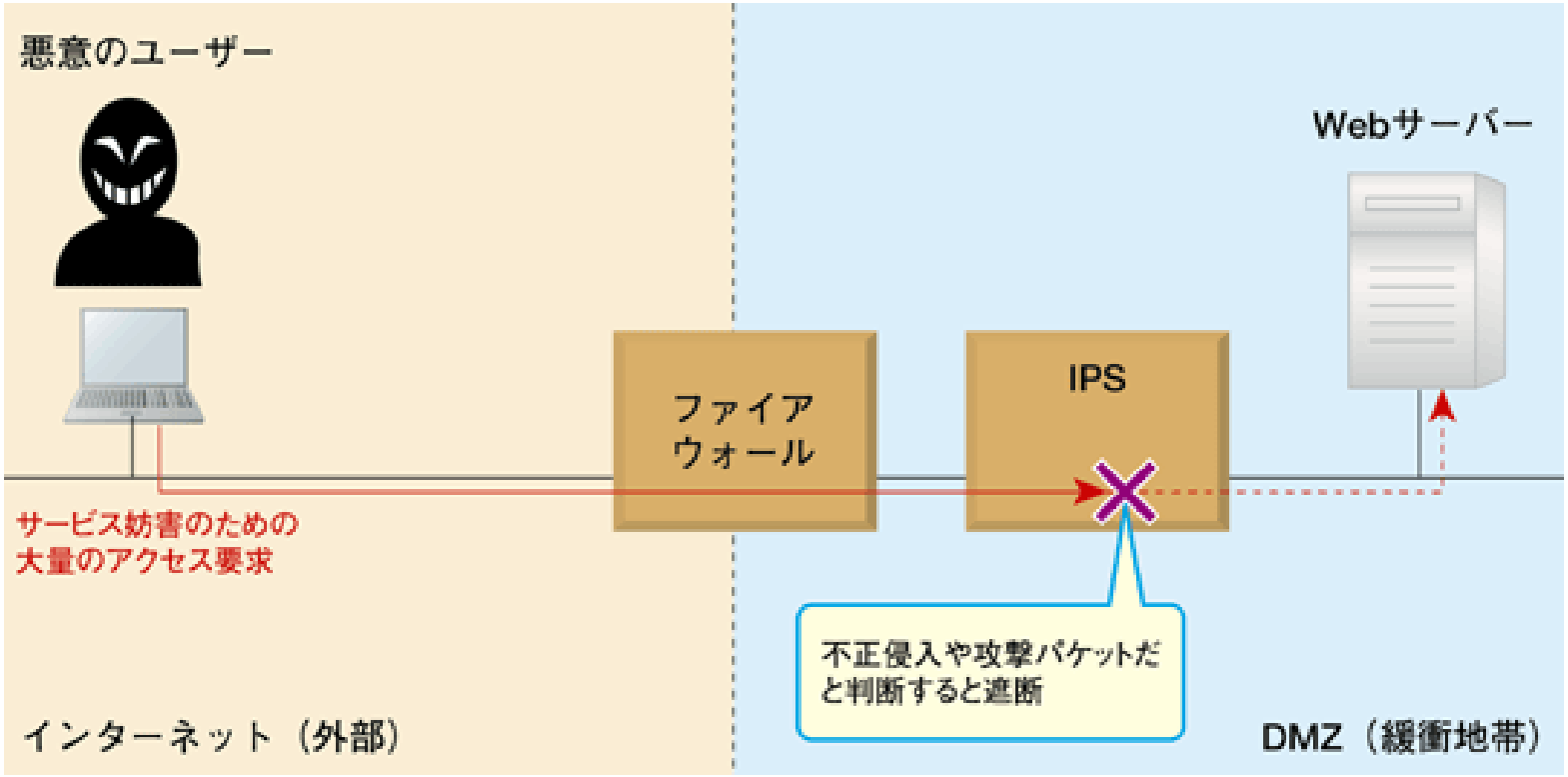
シグネチャ型



アノマリ型

IPS（Intrusion Prevention System）

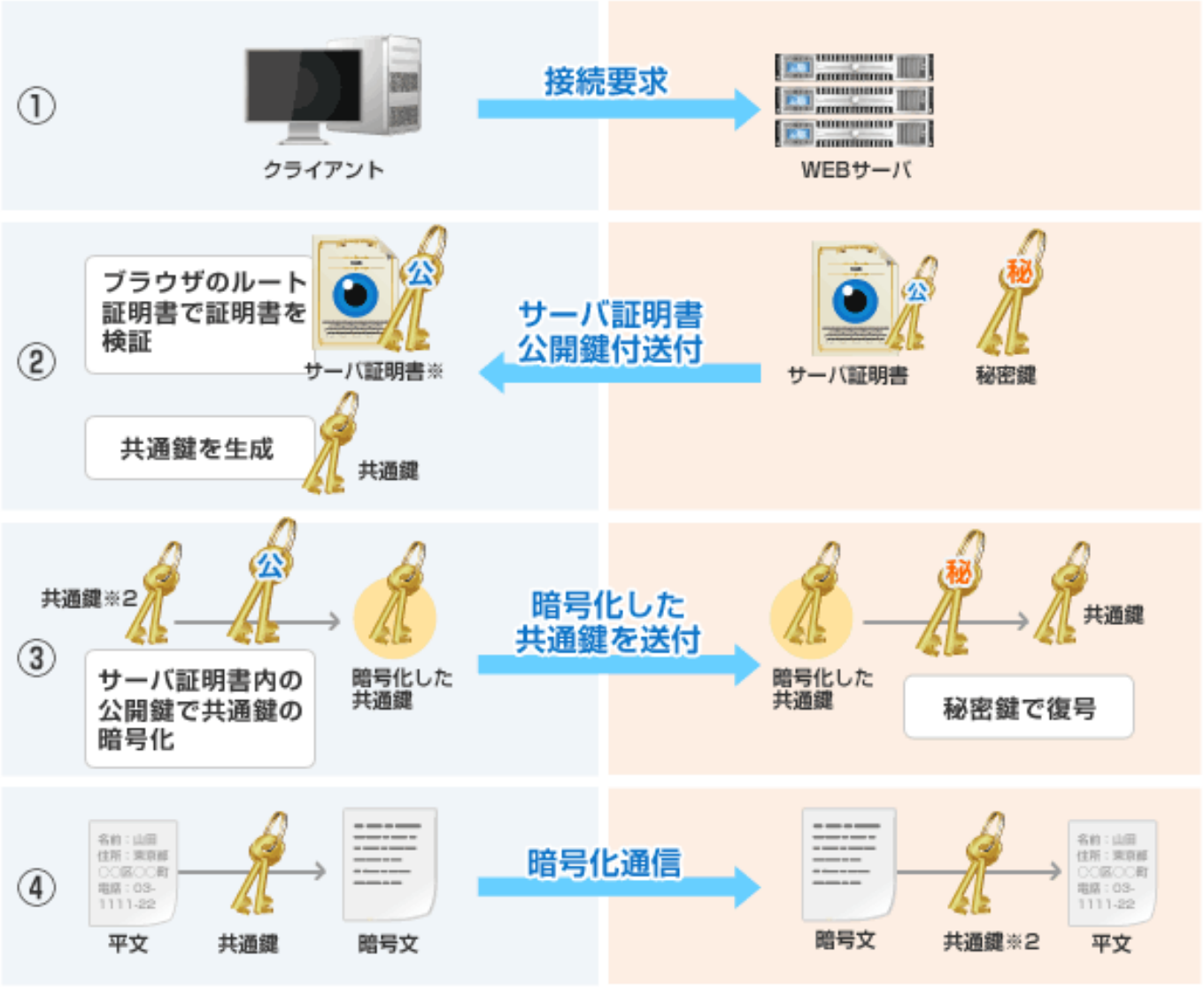
- IDSと同様の働きをするが管理者に通知ではなく
  防御策を実行するシステム



TLS/SSL

- 正式名：Transport Layer Security/Secure Sockets Layer
- トランスポート層(TCP)の上で動作する暗号プロトコル
- 暗号アルゴリズムはIPSecと同様に選択可能
- TLS1.0はSSL3.0の後継バージョン

TLS/SSLの動作


①
クライアント
接続要求
WEBサーバ
②
ブラウザのルート証明書で証明書を検証
公
サーバ証明書※
サーバ証明書公開鍵付送付
公
サーバ証明書
秘
秘密鍵
共通鍵を生成
共通鍵
③
共通鍵※2
公
サーバ証明書内の公開鍵で共通鍵の暗号化
暗号化した共通鍵
暗号化した共通鍵を送付
暗号化した共通鍵
秘
共通鍵
秘密鍵で復号
④
名前：山田
住所：東京都○○区○○町
電話：03-1111-22
平文
共通鍵
暗号文
暗号化通信
暗号文
共通鍵※2
名前：山田
住所：東京都○○区○○町
電話：03-1111-22
平文

今回のまとめ

- VPN
  - カプセル化を行いトンネリングで拠点間のデータ転送を行う
  - トンネルプロトコルとしてIPSecなどが使われる
  - IPSecは鍵交換，暗号化(秘匿，認証，改ざん検知)などが行える
- ファイアウォール
  - パケットフィルタ型とアプリケーションゲートウェイ型がある
- IDS,IPS
  - 通信異常を検出し，管理者に通知する(IDS) or 防御策を実行する(IPS)
- TLS/SSL
  - IPSecとは異なり，TCP上で動作する暗号プロトコル