暗号化と認証

学習内容

1. 暗号化と復号の基本
2. 暗号化方式の2つの種類
3. ハイブリッド方式とSSL/TLS
4. デジタル署名と仕組み
5. デジタル証明書とPKI（公開鍵基盤）
6. 補足：RADIUSによるネットワーク認証

01

Chapter 1: 暗号化と復号の基本

暗号化と復号の基本構造

安全な通信のための「読めないデータ」への変換

暗号化：人間や機械が読める形式のデータ（**平文**）を、第三者が読めない形式（**暗号文**）に変換すること

復号：暗号文を平文に戻すこと

暗号化と復号は「**アルゴリズム（仕組み）**」と「**鍵（キー）**」の2つの要素によって成り立っている

02

Chapter 2: 暗号化方式の2つの種類

共通鍵暗号方式

暗号化と復号に「同じ鍵」を使う方式

メリットと特徴

処理が非常に速い

大量のデータを高速に暗号化・復号できる

アルゴリズム例: AES、DES、RC4

課題点

通信相手ごとに共通鍵の作成が必要

鍵の安全な受け渡しが難しい

鍵が盗まれるとデータは簡単に復号される

公開鍵暗号方式

暗号化と復号に「異なる鍵」を使う方式

メリットと特徴

暗号化に**公開鍵**、復号に**秘密鍵**を使用

公開鍵は誰にでも配布して問題ない

秘密鍵がないと復号できず**安全性が高い**

アルゴリズム例: RSA、ElGamal

課題点

処理に時間がかかる

大量データのやり取りには不向き

共通鍵暗号と公開鍵暗号の比較

特性理解が必須：速さと安全性

共通鍵暗号		公開鍵暗号
1つ（共通鍵）	使用する鍵	2つ（公開鍵/秘密鍵）
秘密に必要	鍵の交換	公開鍵は配布可
速い	処理速度	遅い
鍵管理が課題	安全性	高い

03

Chapter 3: ハイブリッド方式とSSL/TLS

ハイブリッド方式の仕組み

安全と高速性を両立させる複合技術

STEP 1 公開鍵暗号で**共通鍵**を安全に受信者へ渡す

STEP 2 受信した共通鍵を使って**データ**を暗号化

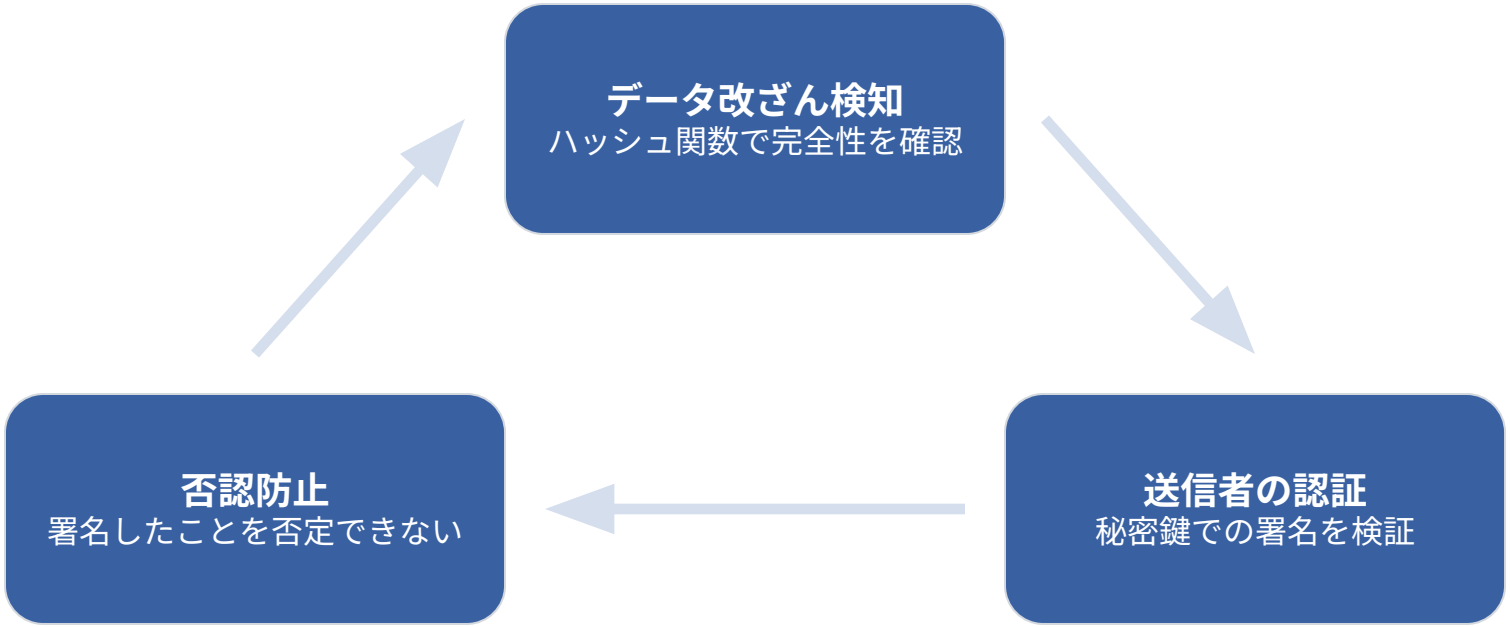
STEP 3 実際のデータ通信は処理が速い**共通鍵暗号**で行う

04

Chapter 4: デジタル署名と仕組み

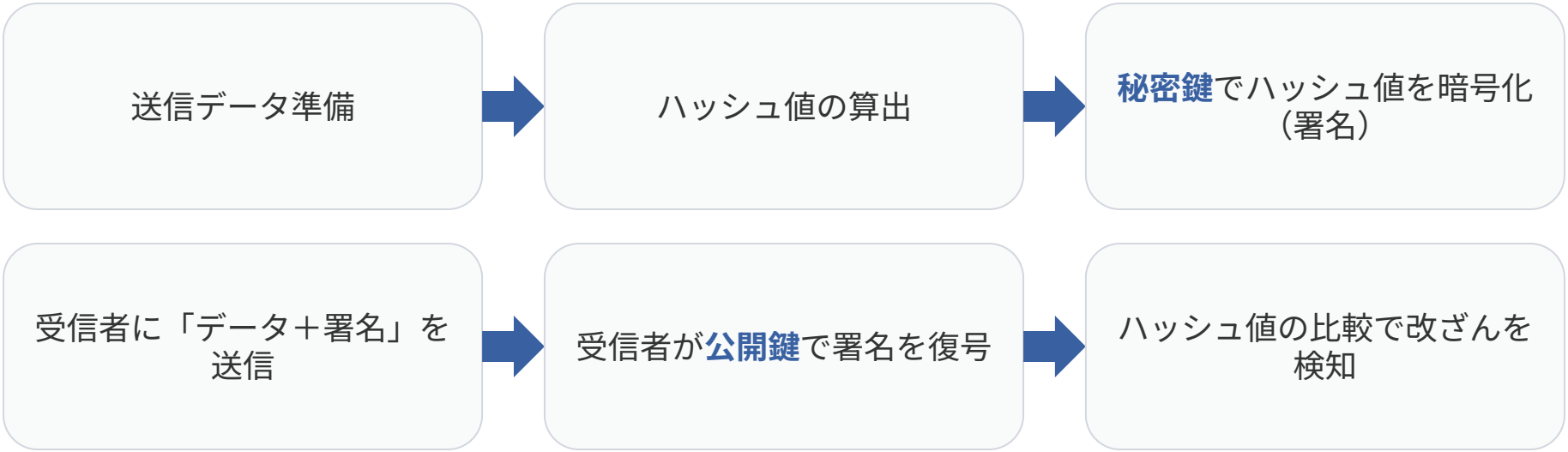
デジタル署名の2つの機能

公開鍵暗号を応用した「データの完全性」と「送信者の認証」の保証



デジタル署名の検証プロセス

送信者（秘密鍵）が署名し、受信者（公開鍵）が検証する



05

Chapter 5: デジタル証明書とPKI

デジタル証明書の役割

「公開鍵の正当性」と「所有者の身元」の保証

公開鍵の正当性保証

攻撃者による**偽の公開鍵**の配布を防ぐ

所有者の身元証明

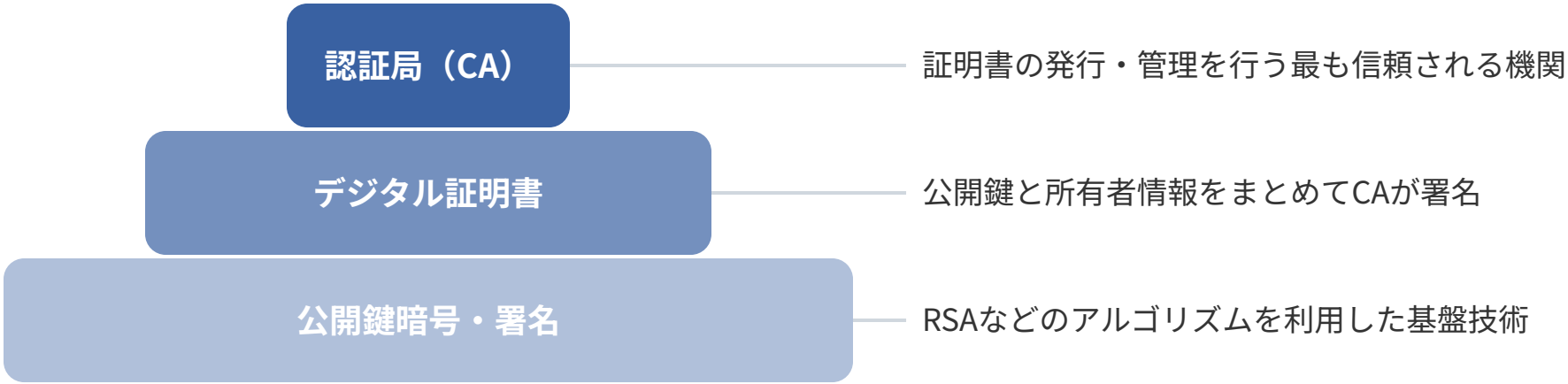
発行元である**認証局（CA）**が所有者を保証

例えるなら

デジタル署名が直筆サイン、証明書は印鑑証明書

公開鍵基盤（PKI: Public Key Infrastructure）

暗号化技術を支える社会的な仕組み全体



06

Chapter 6: 補足：RADIUSによるネットワーク認証

RADIUSによるネットワーク認証の構成

無線LANなどでのユーザー認証を支えるプロトコル