



情報セキュリティ

紹介者：福井

情報セキュリティの定義

- 情報セキュリティに関する要求事項を定めたJIS Q 27001
 - 情報セキュリティを確保するシステムである情報システムセキュリティマネジメントシステム（ISMS）がある
- 情報セキュリティは、**情報の機密性、完全性および可用性を維持すること**と定義されている
- CIAと呼ばれる
 - 機密性（Confidentiality）
 - 完全性（Integrity）
 - 可用性（Availability）

情報セキュリティ

- 機密性 (Confidentiality)
 - 認可されていない個人, エンティティまたはプロセスに対して, 情報を使用不可または非公開にする特性
- 完全性 (Integrity)
 - 資産の正確さおよび完全さを保護する特性
- 可用性 (Availability)
 - 認可されたエンティティが要求した時のアクセスおよび使用が可能である特性
- 真正性 (Authenticity)
 - 主体性または資源が, 主張どおりであることを確実にする特性
- 責任追跡性 (Accountability)
- 否認防止 (Non-Repudiation)
- 信頼性 (Reliability)

情報セキュリティの重要性

- 情報資産

- 業務に必要なこうした価値のある情報
 - ▶ 顧客情報や技術情報など形のないもの
- ISMSでは組織が持つ情報資源にとっての脅威を洗い出し，脆弱性を考慮することにより最適なセキュリティ対策を考える

- 脅威

- システムや組織に損害を与える可能性があるインシデントの潜在的要因

- 脆弱性

- 脅威が漬け込むことができる，資産が持つ弱点

不正のメカニズム

- 不正のトライアングル理論

- 人が不正行為を実行するに至るまでには，不正の3要素がそろう必要がある

- ▶ 機会

- ・ 不正行為の実行が可能，または安易となる環境

- ▶ 動機

- ・ 不正行為を行うための事情

- ▶ 正当化

- ・ 不正行為を行うための良心の呵責を乗り越える理由



攻撃者の種類

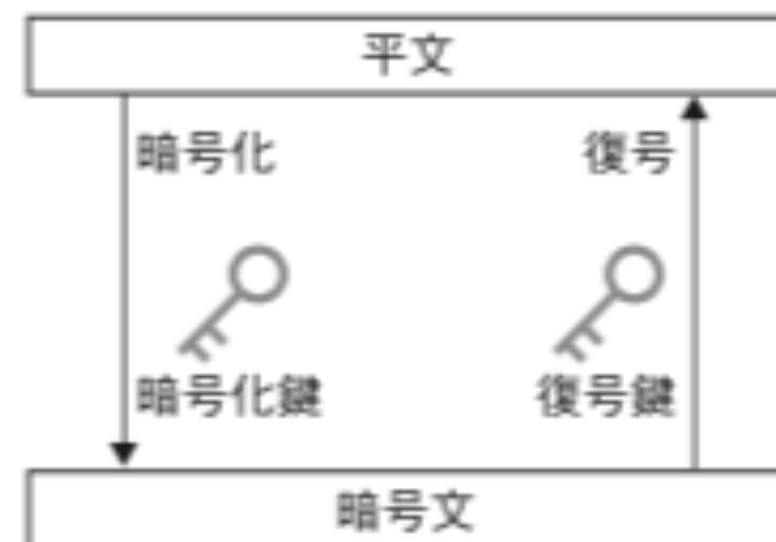
- スクリプトキディ
 - インターネット上で公開されている簡単なクラッキングツールを利用して不正アクセスを試みる攻撃者
- ボットハーダー
 - ボットを利用することでサイバー攻撃などを実行する攻撃者
- 内部関係者
 - 従業員や業務委託系の社員など、組織の内部情報にアクセスできる権限を悪用する攻撃者

攻撃者の目的

- 金銭奪取
 - 金銭的に不当な利益を得ることを目的とした攻撃
- ハクティビズム
 - 政治的・社会的な思想を基に積極的行われるハッキング活動
- サイバーテロリズム
 - ネットワークを対象に行われるテロリズム、組織や社会機能に大きな打撃を与える

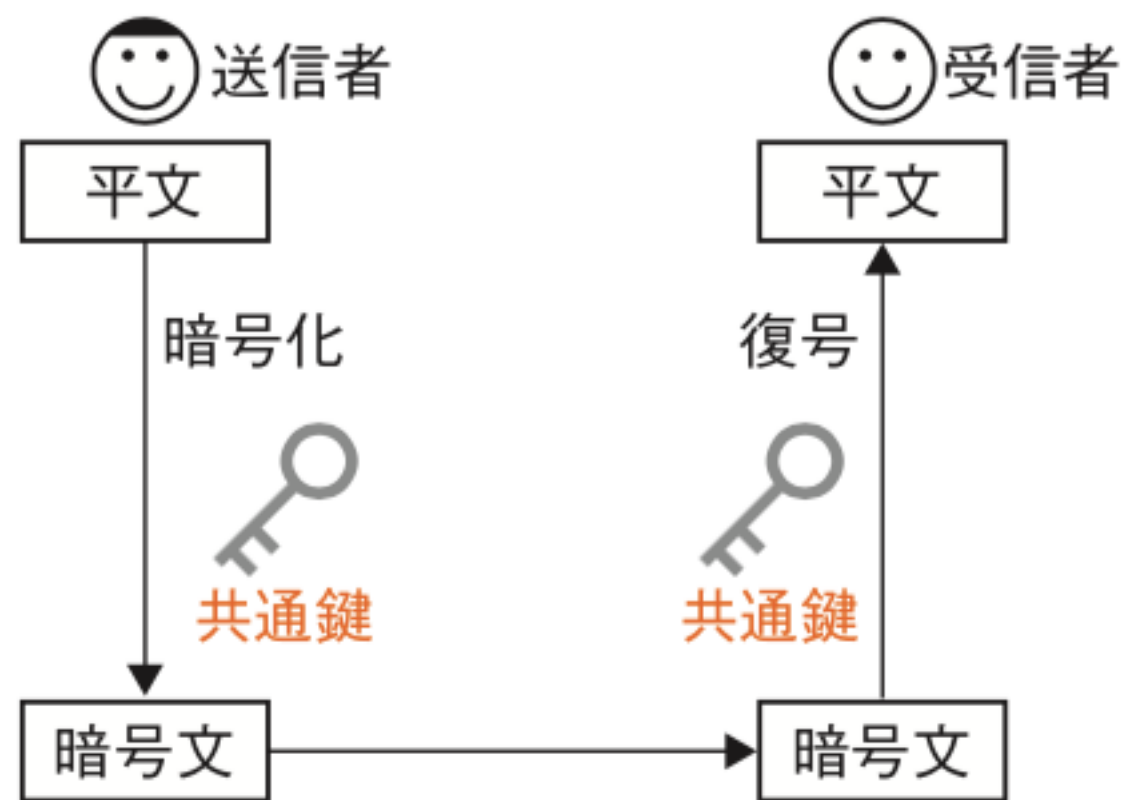
暗号化技術

- 暗号化
 - 普通の文章（平文）を読めない文章（暗号文）に変換することで、読めないようにすること
- 復号
 - 元に戻すこと
- 暗号化および復号化するのに必要なのは、暗号アルゴリズムと鍵



共通暗号方式

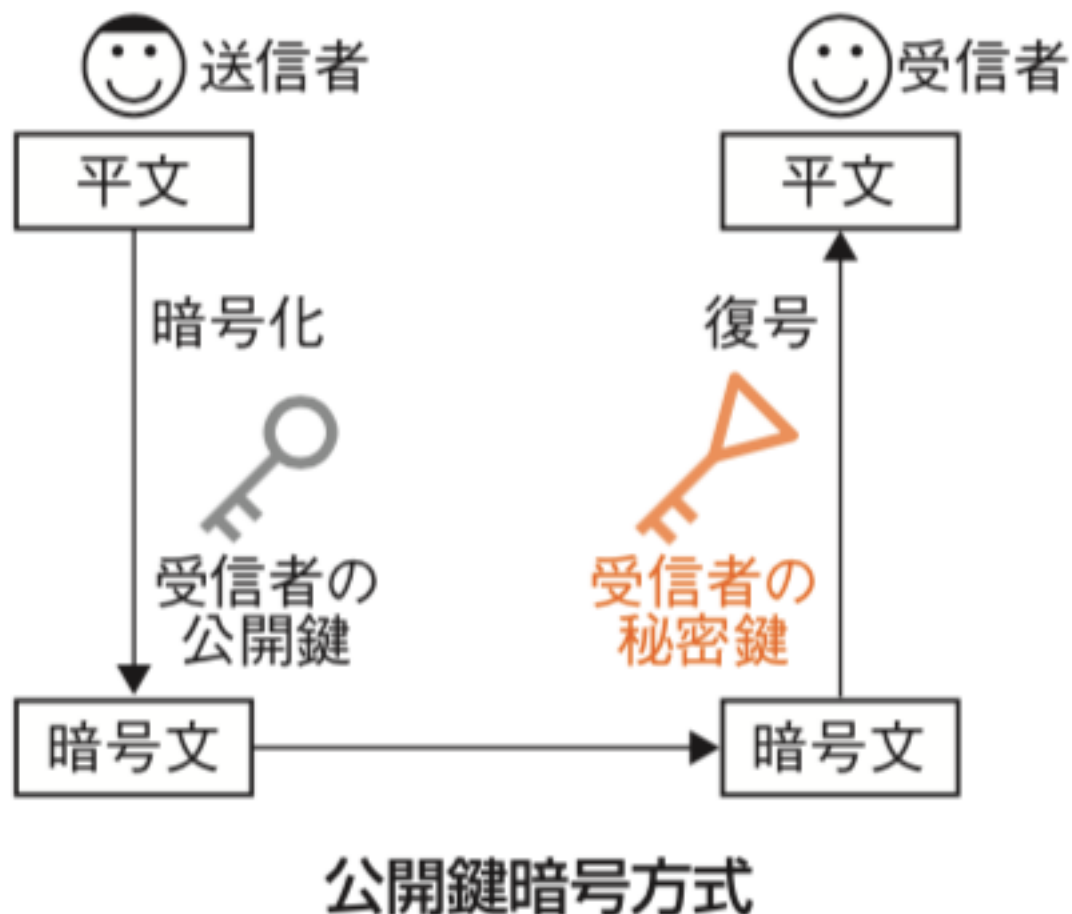
- 暗号鍵と復号鍵が共通である暗号方式
 - 共通で使用する鍵を共通化鍵
- 鍵を秘密にして共有する必要がある
- アルゴリズムが単純で高速



共通鍵暗号方式

公開暗号方式

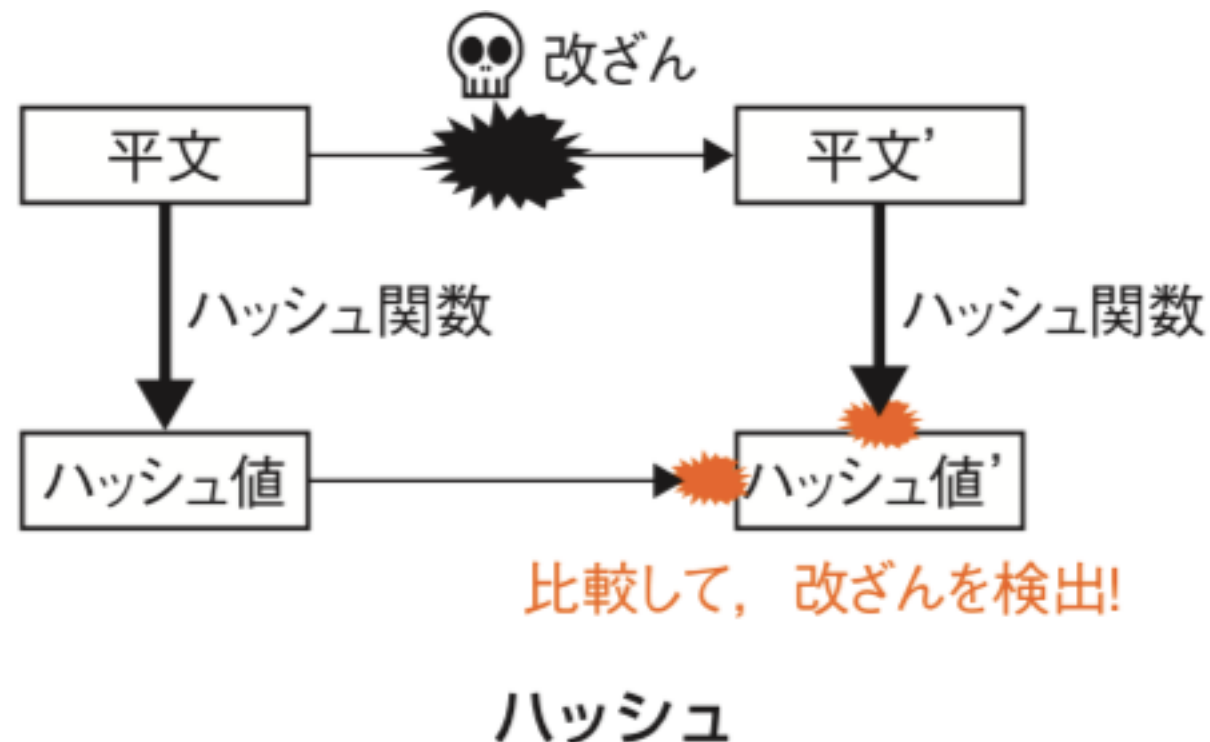
- 暗号鍵と復号鍵が異なる方式
- 使用する他人事に公開鍵と秘密鍵のペアを作る
- 公開鍵は相手に渡して、秘密鍵は自分で保管



1. 公開鍵で暗号化すると同じ人の秘密鍵で復号化できる
2. 秘密鍵で暗号化すると、同じ人の公開鍵で復号化できる

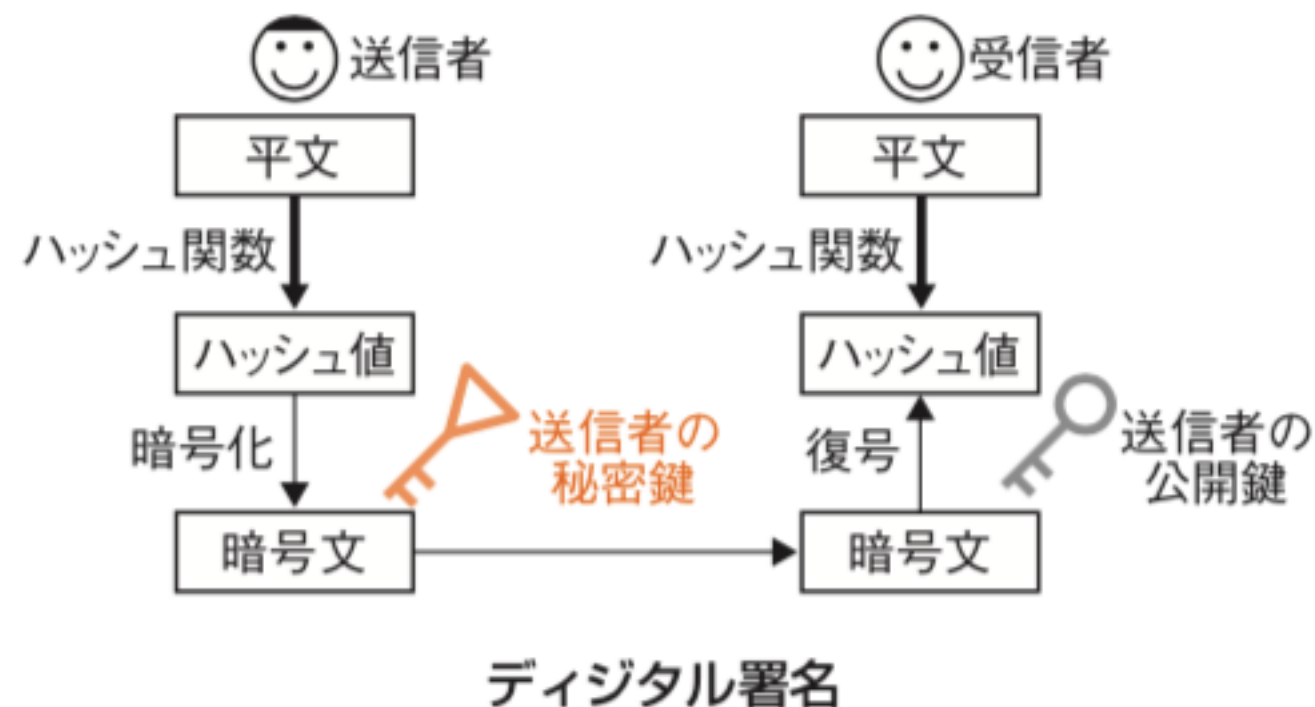
ハッシュ

- ハッシュ関数は一方向性の関数
 - 平文を変換してハッシュ値を求める
- 送りたいデータと合わせてハッシュ値を送ることで改ざん検出ができる



デジタル署名

- 公開鍵暗号方式は，暗号化以外にも使われる
 - 本人の秘密鍵を持っていることが本人であるという証明になる
 - ▶ 送信者の秘密鍵で暗号化して，受信者は公開鍵で復号化する
- デジタル署名
 - ハッシュを組み合わせることでデータの改ざんも検出できる

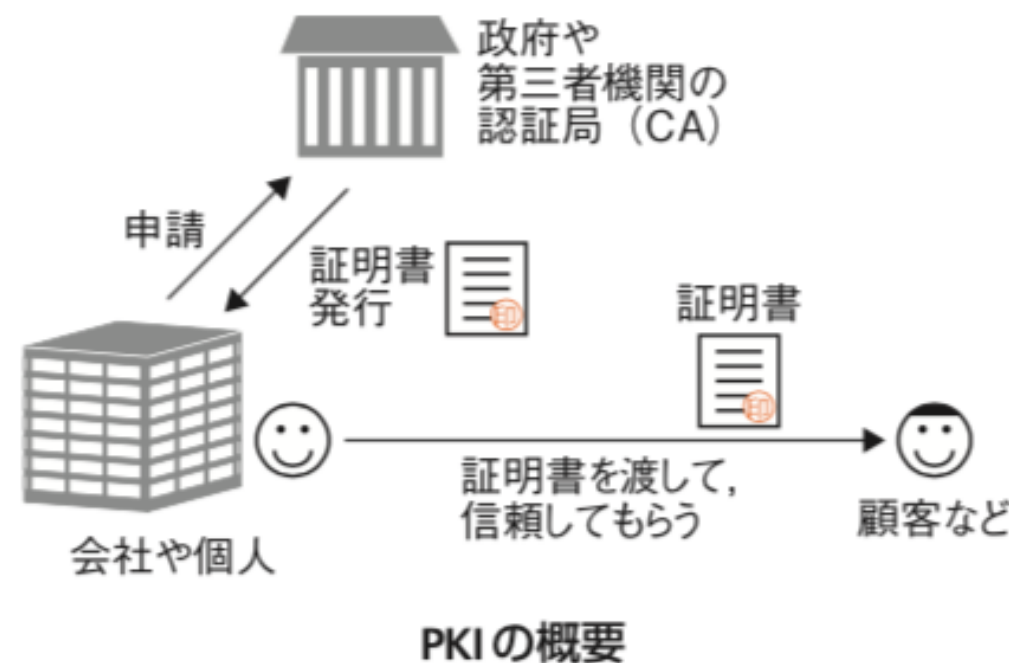


暗号アルゴリズム

- 公開鍵暗号方式
 - RSA
 - 楕円曲線暗号
- ハッシュ
 - MD5
 - SHA-1
 - SHA2
- 共通暗号方式
 - DES
 - AES
 - RC4

PKI(Public Key Infrastructure)

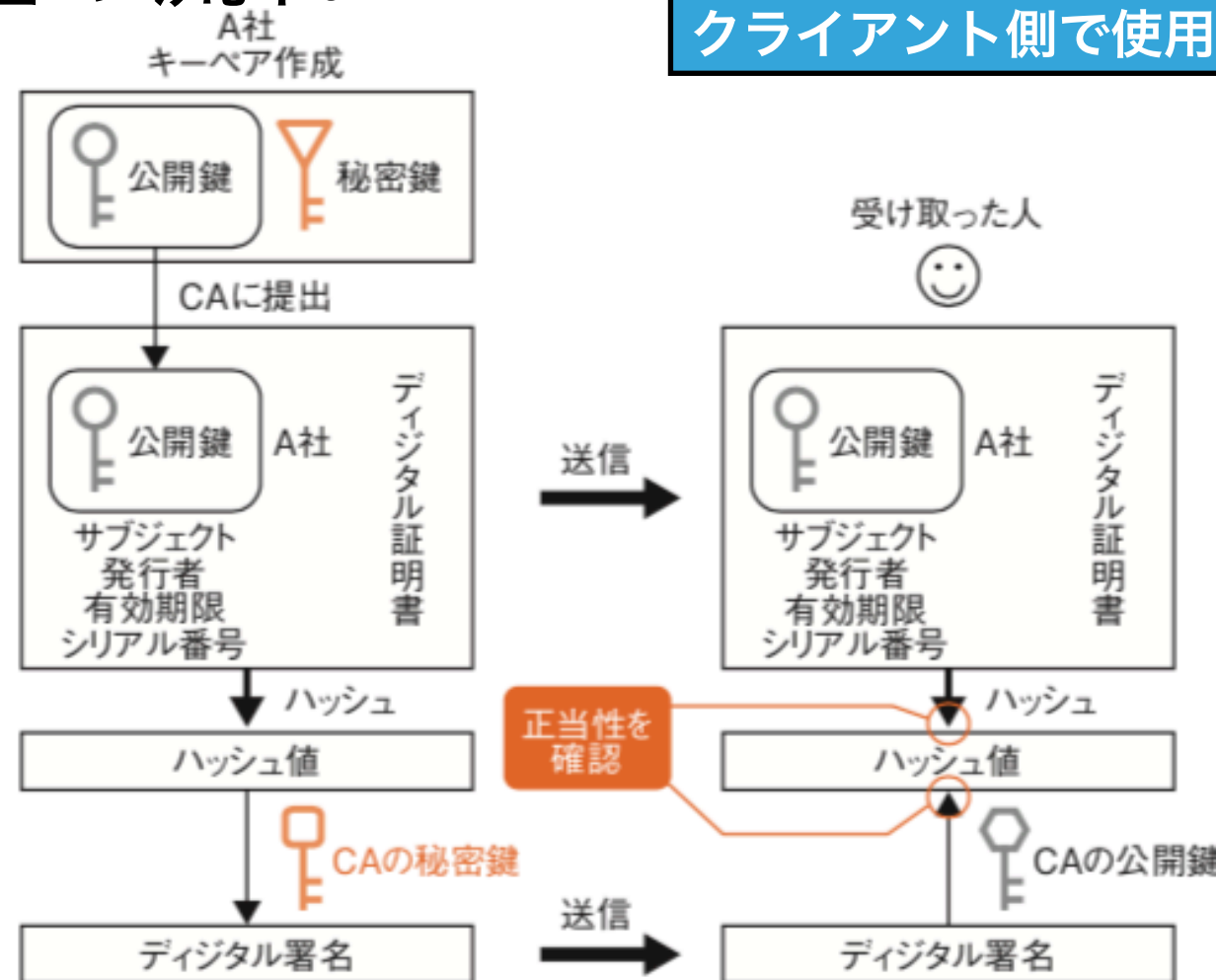
- 公開鍵暗号方式を利用した社会基盤
 - 政府や認証局（CA）に証明書を発行してもらい，身分を証明してもらう
- 政府が発行するPKI
 - 一般のPKIと区別され，政府認証基盤(GPKI)と呼ばれる



デジタル証明書

- CAがデジタル署名を行うことによって、申請した人や会社の公開鍵などの証明書の内容が正しいことを示す
- PKIの処理の流れ

・デジタル証明書の種類
サーバで使われる：サーバ証明書
クライアント側で使われる：クライアント証明書



CRLとOCSP

- デジタル証明書の有効期限内に秘密鍵が漏洩したりセキュリティ事故が起こったりしてデジタル署名の信頼性が損なわれる事がある
 - CAに申請してCRLに登録してもらう
- CRL(Certificate Revocation List)
 - 失効した証明書のリスト. CRLを確認することで証明書が有効か判断できる
- OCSP(Online Certificate Status Protocol)
 - デジタル証明書の失効情報を取得するためのプロトコル

暗号化技術の応用

- SSL/TLS
- IPsec
 - IPパケット単位でのデータ改ざん防止や秘匿機能を提供するプロトコル
- S/MIME
 - MIME形式の電子メールを暗号化し，デジタル署名を行う標準規格
 - CAを利用
- PGP
 - 電子メールの暗号方式，CAを利用しない
- SSH