

コンピュータ基礎(13)

9章 9.1-9.3 情報セキュリティ
10章 10.2 情報システムの信頼性

この章で学習すること

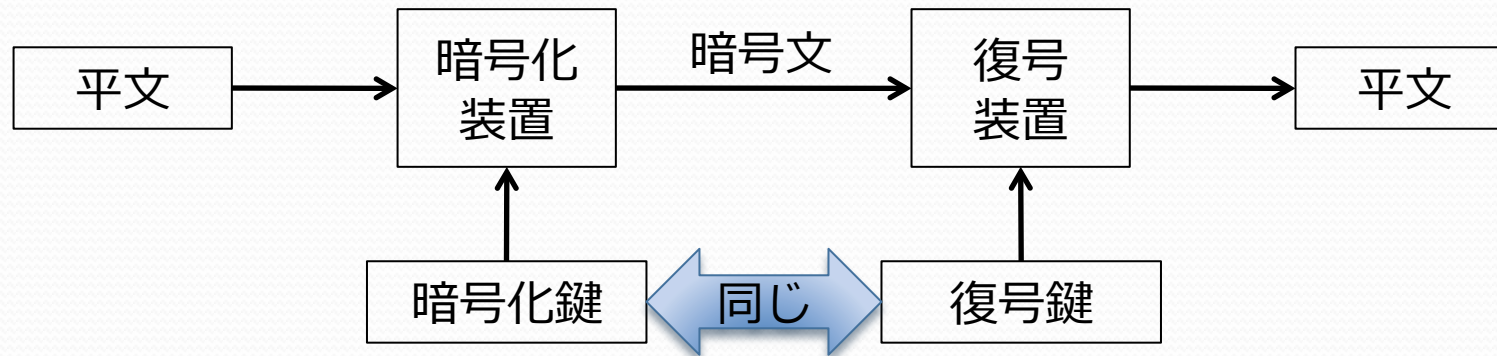
- 9.1 情報セキュリティの概念
 - セキュリティと脅威について
- 9.2 情報セキュリティに関する技術
 - 暗号化（共通鍵暗号, 公開鍵暗号）
 - 認証, デジタル署名
- 9.3 情報セキュリティ管理
 - リスク管理・分析, リスクの種類
- 10.2 情報システムの信頼性
 - RASIS（信頼性, 可用性, 保守性, 完全性, 安全性）
 - 稼働率の計算（MTBF, MTTR と稼働率）

情報セキュリティとは？

- セキュリティを考えるための要素
 - 保護すべきもの（データ，システム）
 - 保護すべきものを脅かすもの（脅威）
 - 保護すべきものを守る手段（セキュリティ）
- 脅威の種類
 - 自然災害・天災（地震，台風，洪水など）
 - 火災
 - 破壊（建物・コンピュータ・データを故意に壊す）
 - 不正行為（コンピュータ犯罪，改ざん，盗聴，なりすまし，漏えい，複製，抹消など）
 - 過失（ミスによる様々な損失）
 - いたずら（侵入やコンピュータウィルスなど）



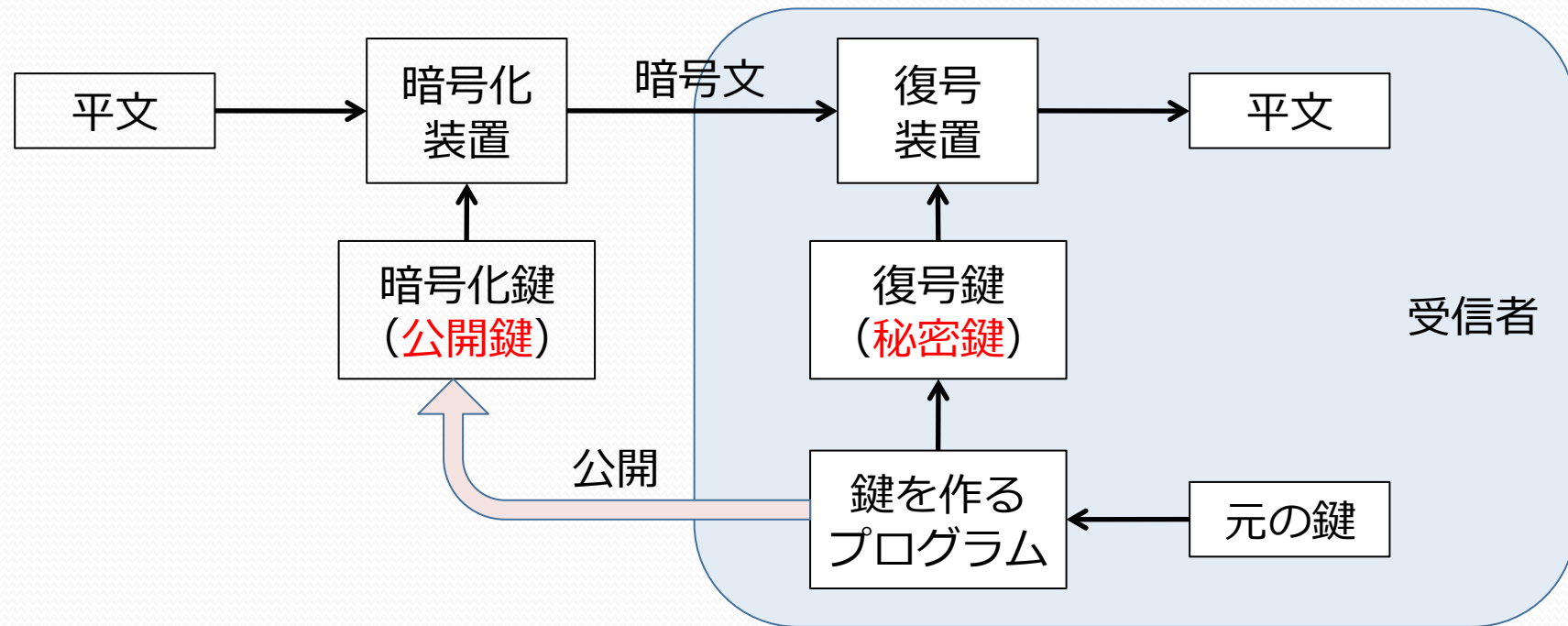
暗号化(1)



- **共通鍵暗号方式**

- 暗号化鍵と復号鍵が同じ
- お互いの持つ鍵を秘密にしておく必要がある
 - 鍵を相手へ「**秘密に**」届ける方法が問題となる。
もし鍵が漏れると、他人が復号できてしまう
(メッセージを読まれてしまう)。
- 通信相手が増えると、鍵がその分増えてしまう。

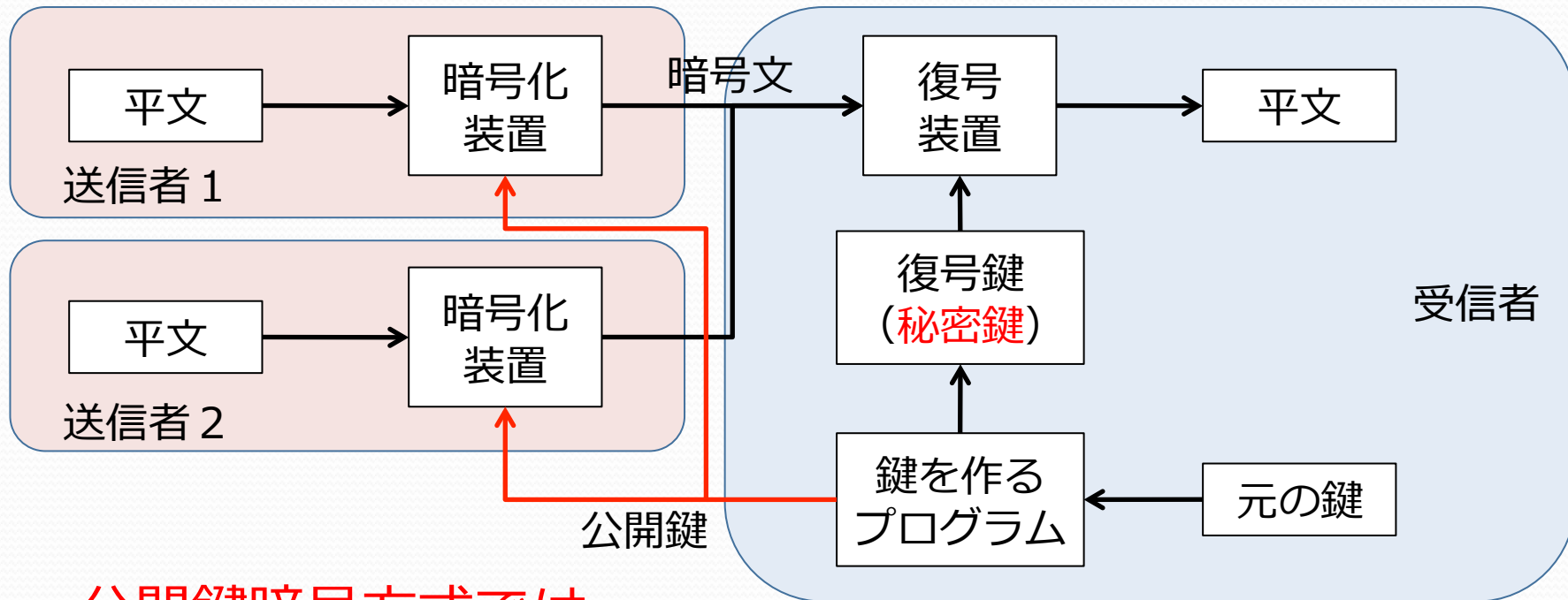
暗号化(2)



- **公開鍵暗号方式**

- 2個セットの鍵を作成し、暗号化鍵を**公開**する
- 復号鍵は受信者から外に出ないので、復号鍵 (秘密鍵) を盗まれる危険性が低く、安全性が高い

暗号化(3)



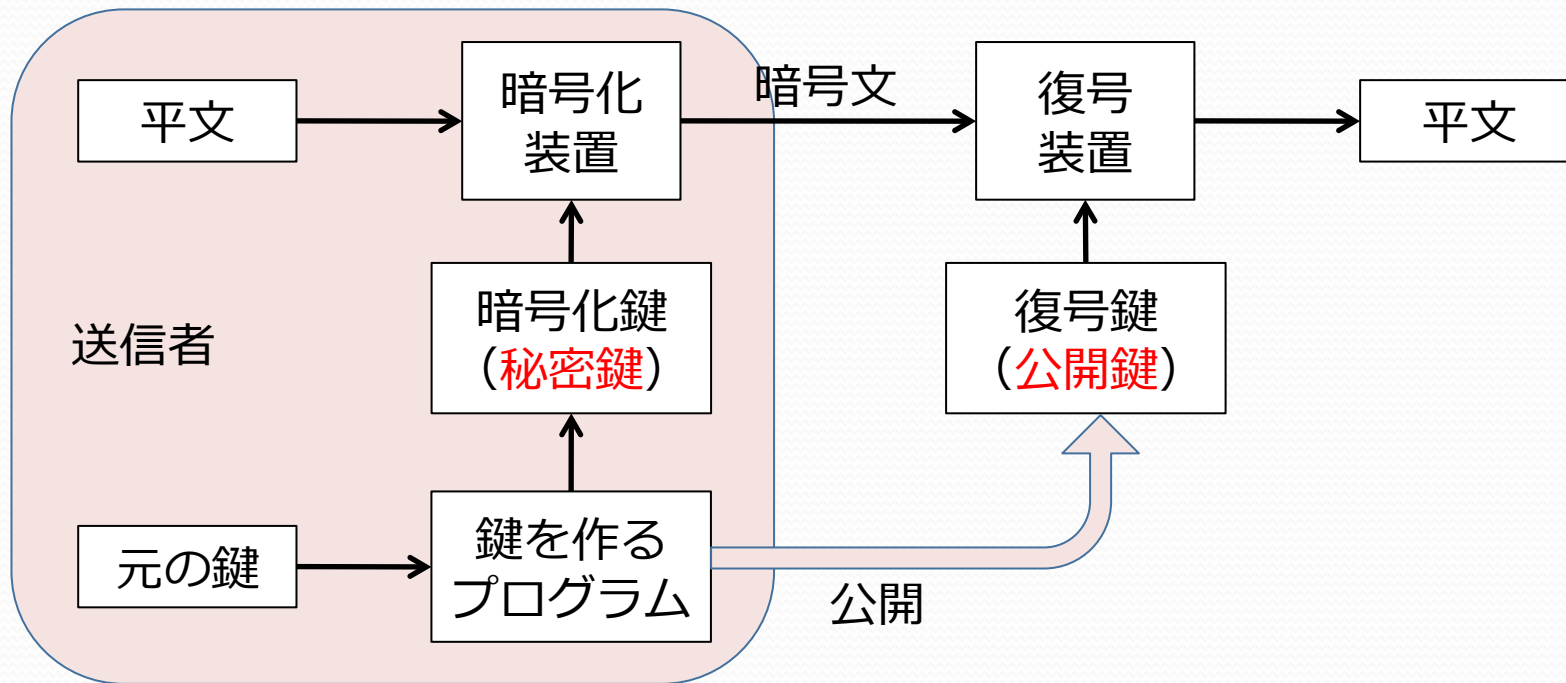
- **公開鍵暗号方式では**

- 複数の送信者が同じ鍵でそれぞれ秘密のメッセージを送信できる。受信者以外は復号出来ない

- **問題点**

- 公開鍵を入手すればだれでも送信できるので、送信者を特定できない（偽情報を送ることができてしまう）
- 他人が受信者になりすまして、偽の鍵を公開して情報を盗み出す危険がある→認証局の必要性

デジタル署名



- デジタル署名

- 復号鍵をあらかじめ公開しておく。誰でも復号できる。
- 暗号化鍵は秘密なので、他人が同じ暗号データを作ることができない (本人が作ったデータであることが確か)

情報セキュリティ管理

- リスク管理とは、将来発生しうるリスクを想定し、これに対する対策を考えること。
- リスク管理は、以下の2つに分類できる。
 - **リスクコントロール**：リスクがもたらす損失を最小にするために事前に施される対策。以下は例。
 - リスク回避：そもそもリスクが発生することをしない。
例：危ない橋は、渡らない。
 - リスク分散：リスクを分けることでリスクを軽減させる。
例：2つの橋に半分の人数ずつ渡らせて全滅を避ける
 - **リスクファイナンス**：リスクが発生した時の、回復のための資産手当の方法。
 - リスク保有：損失にあてる資金を予め用意しておく。
例：貯金しておく。
 - リスク移転：他者に責任を移転する。
例：保険をかける。

リスクの種類

- 純粋リスク

- 単に損失をもたらすもの。
例：ハードディスクの故障。
自然災害。悪意による攻撃。

- 投機的リスク

- 利益と損失のどちらか一方をもたらすもの。
例：新しい商品を売り出す。
売れば利益が得られるが、外れると大損・・・
研究開発に力を入れる。
新発見があればよいが、なければ無駄・・・

試験では投機的リスクをとらないように！
(ヤマを張る，不正行為をする，・・・)

信頼性を向上させる技術

- 冗長化（多重化）

- 最小限のシステムでなく，冗長な（余裕のある，無駄のある）設計で，故障時に代替がきくようにする
- 例：データを二箇所保存する，複数の計算機で計算して多数決を取る，など

- フェイルセーフ(fail safe)

- 故障したときに，常に安全側に壊れる設計。
 - 例：信号機は壊れると常に赤が点灯するようになっている

- フールプルーフ(fool-proof)

- 人的ミスを前提に，ミスしにくい設計にする。
 - 例：ファイル削除をするときに警告を出す。
ブレーキを踏んでいないとエンジンがかからない

情報システムの信頼性とは？

- 情報セキュリティに関する用語(RASIS) 10.2章
 - **R**eliability(信頼性) : 情報システムが障害なく動作すること (故障しないこと)
 - **A**vailability (可用性) : 使いたい時に, いつでも使えること (正しく動いている時間の割合が長いこと)
 - **S**erviceability (保守容易性) : 障害の検出, 診断, 切離しなどの再構成がしやすいこと (修理しやすいこと)
 - **I**ntegrity (保全性, 完全性) : データの破壊・損失がなく, もし起きても修復できること (間違えないこと)
 - **S**ecurity (安全性) : 不正アクセスが出来ないように保護されていること (データが盗み見られないこと)

システムの稼働率

- 信頼性の尺度 : **MTBF** (平均故障間隔)
 - Mean Time Between Failures
- 保守性の尺度 : **MTTR** (平均修理時間)
 - Mean Time To Repair
- **稼働率** : システムが動いている時間の割合.



- MTBF : T_1, T_2, \dots の平均
- MTTR : R_1, R_2, \dots の平均
- **稼働率**
$$\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$