本資料について

- 本資料は下記書籍を基にして作成されたものです。文書の内容の正確さは保障できないため、正確な知識を求める方は原文を参照してください。

- 題目：ネットワークセキュリティ 【第2版】
- 著者：谷口　功
- 発行日：2005年8月22日
- 発行所：オーム社

ネットワークセキュリティ

-攻撃と防御のメカニズム-

名城大学　情報工学科
渡邊研究室
三輪亮太

ウイルスの主な感染経路

- 電子メールの添付ファイル
- 電子メールのプレビュー
- ホームページの閲覧
- インターネット接続
- ファイルのダウンロード
- 媒体（DVD、USBメモリなど）から

電子メール

- 電子メールはメッセージ伝達の中心である

  - 添付ファイルに潜むコンピュータウイルスが短期間で、広範囲に拡散する

- メリッサ
  - 50の宛先に送信
- I LOVE YOU ウイルス
  - アドレス帳のすべてのアドレスに送信

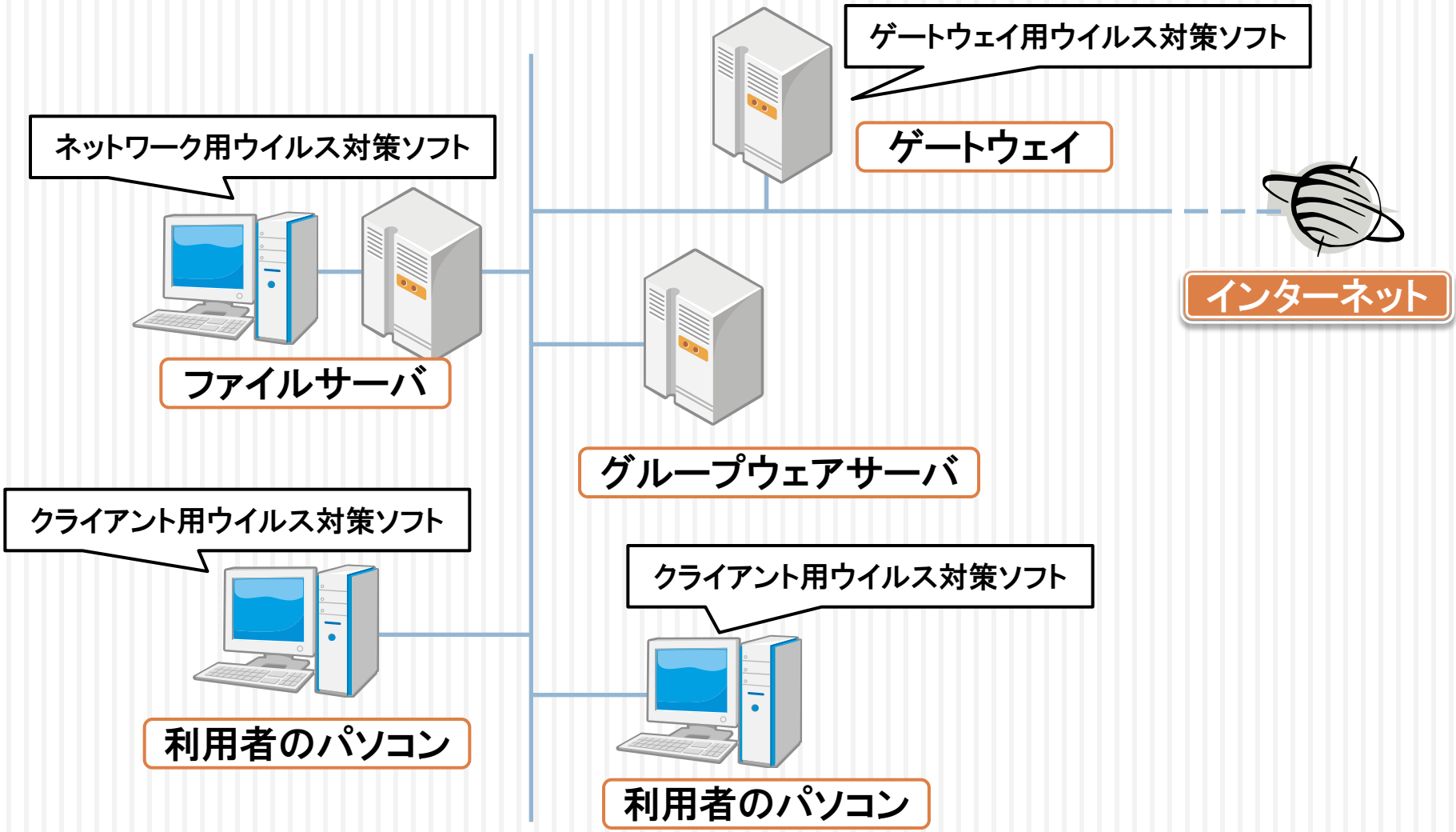
マクロウイルス

- WordやExcelなどのアプリケーションソフトに備わっている「マクロ」という簡易プログラムの仕組みを悪用したコンピュータウイルス。

- 比較的簡単に作成可能
  - ✓ インターネット上にマクロウイルス作成ツールが出回っている

- 感染が広がり易い

ウイルス対策ソフトの設置



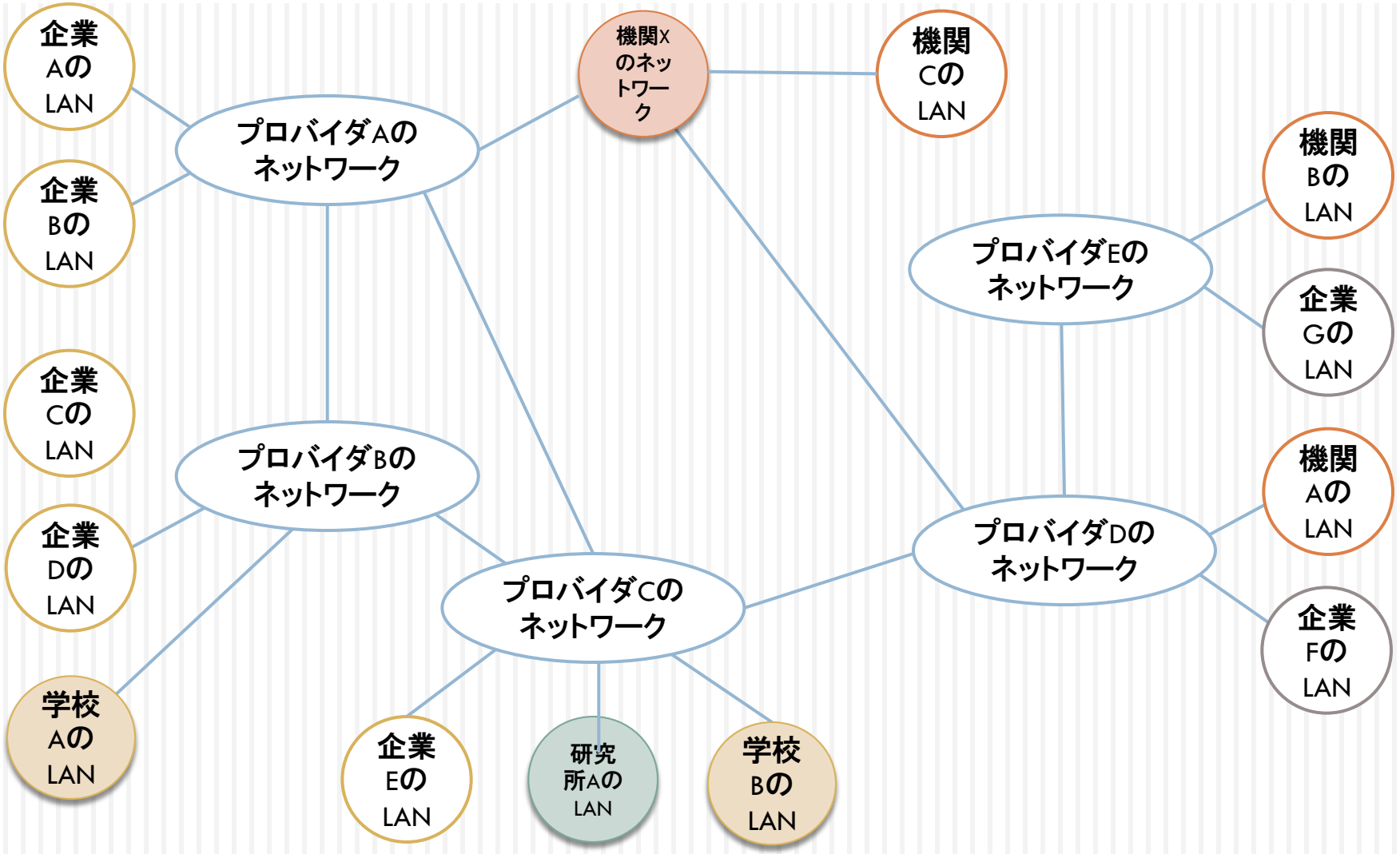
未知のコンピュータウイルス対策

- スタティックヒューリスティック法
  - コンピュータウイルスの行動パターンをあらかじめ定義情報として登録
- ダイナミックヒューリスティック法
  - ウイルス対策ソフトが、感染の疑いのあるプログラムをメモリ上で仮想的に実行して、どのように動作するか調べる

(*)ヒューリスティック

- 試行錯誤して自分で見つける技術

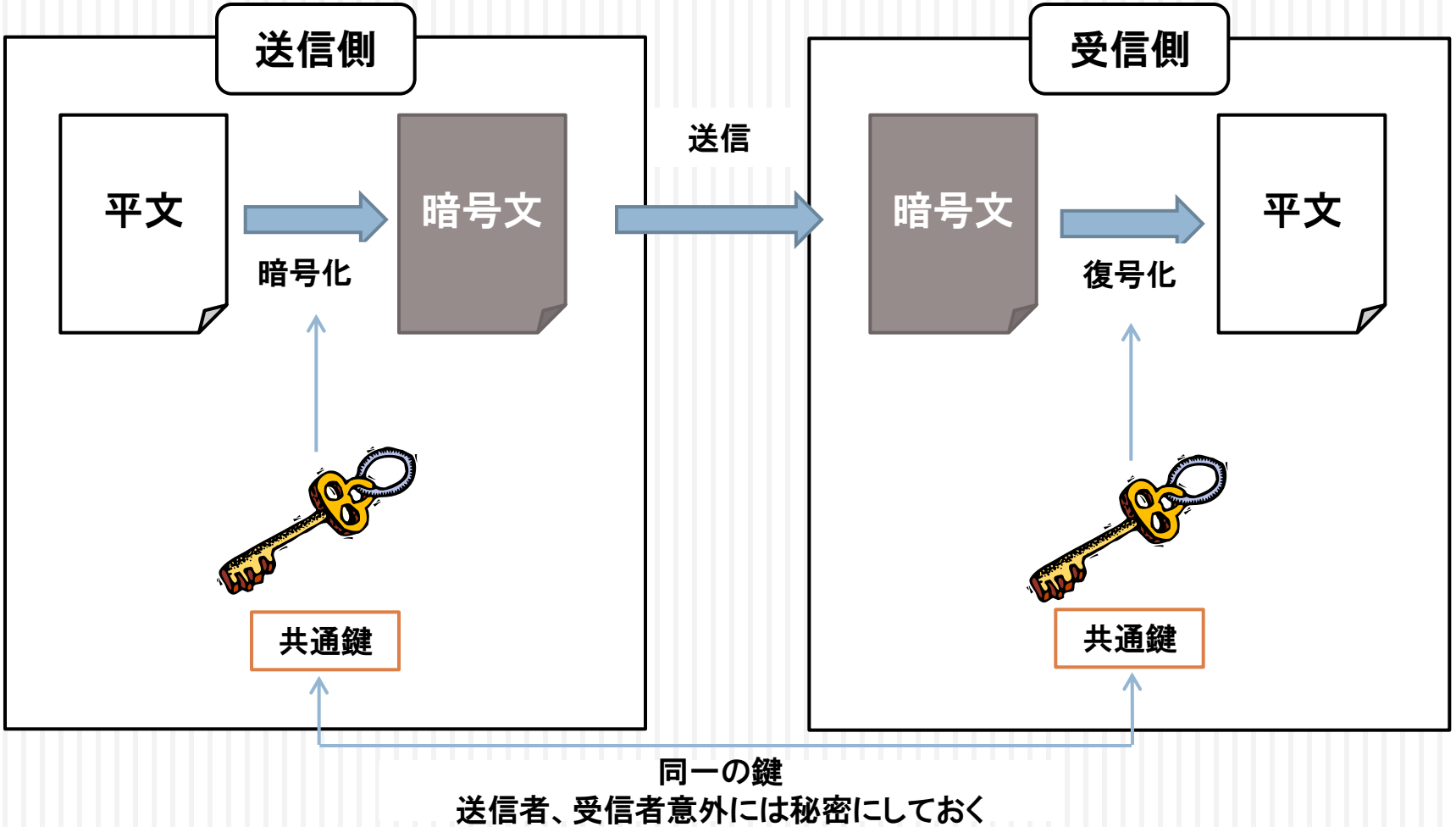
インターネットの構造


企業Aの LAN
企業Bの LAN
企業Cの LAN
企業Dの LAN
学校Aの LAN
プロバイダAの ネットワーク
プロバイダBの ネットワーク
機関Xのネットワーク
機関Cの LAN
プロバイダEの ネットワーク
機関Bの LAN
企業Gの LAN
プロバイダDの ネットワーク
機関Aの LAN
企業Fの LAN
プロバイダCの ネットワーク
企業Eの LAN
研究所Aの LAN
学校Bの LAN

ネットワーク上の脅威

- 盗聴
  - 実際には、情報のコピー
  - 電子的なデータはコピーされても痕跡が残らない
- 改ざん
  - 送信者から受信者に送信されたデータを、第三者に改ざんされる危険性

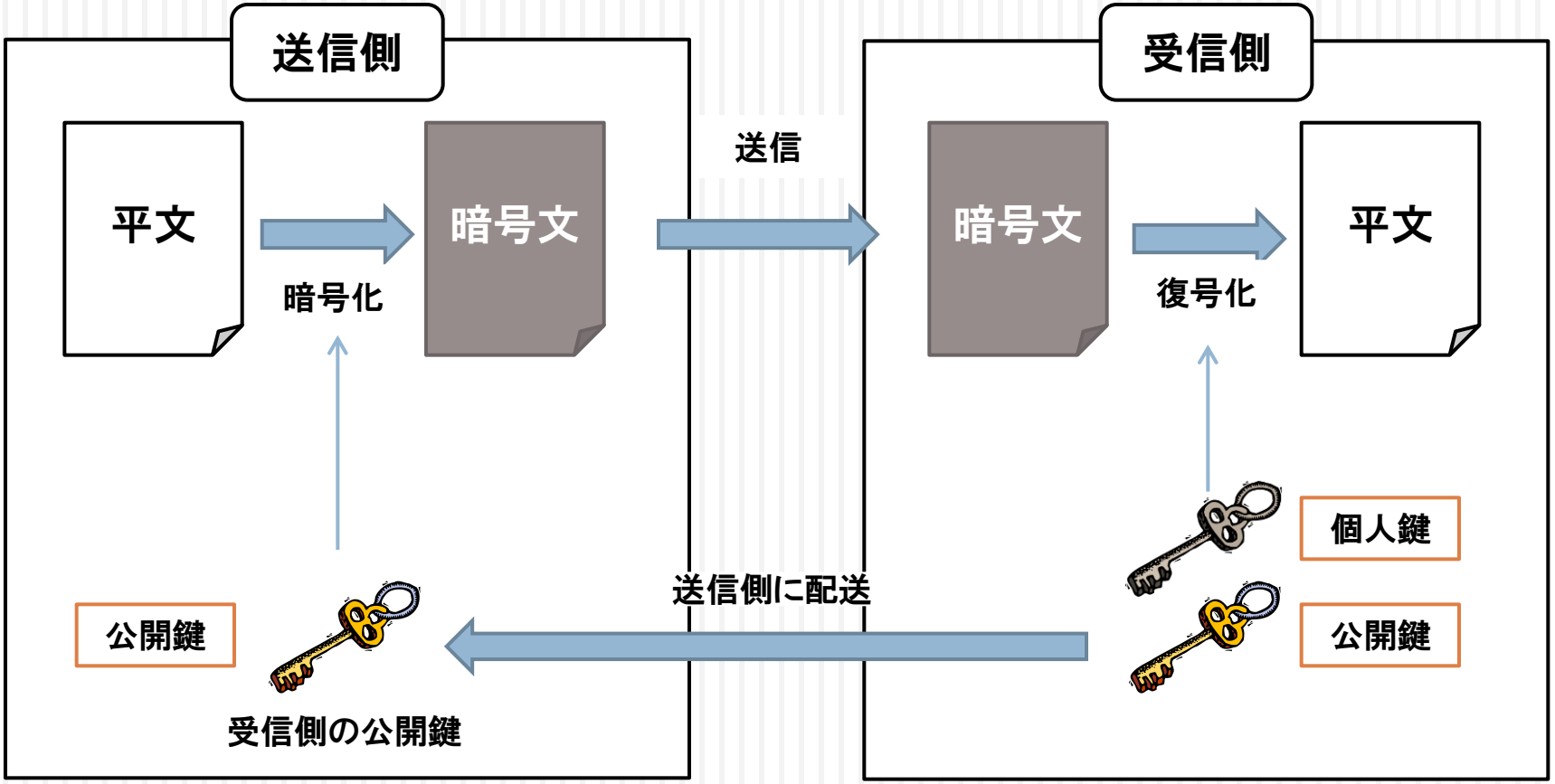
暗号化(共通鍵暗号化方式)



共通鍵暗号化方式の規格

- DES(Date Encryption Standard)
  - 1970年代はじめにIBM社が開発
  - 米国政府が標準暗号化方式として採用
- AES(Advanced Encryption Standard)
  - DESの後継規格として使用する次世代高度暗号化標準規格
- トリプルDES
  - 2つの鍵を使ってDESの処理を3回繰り返す

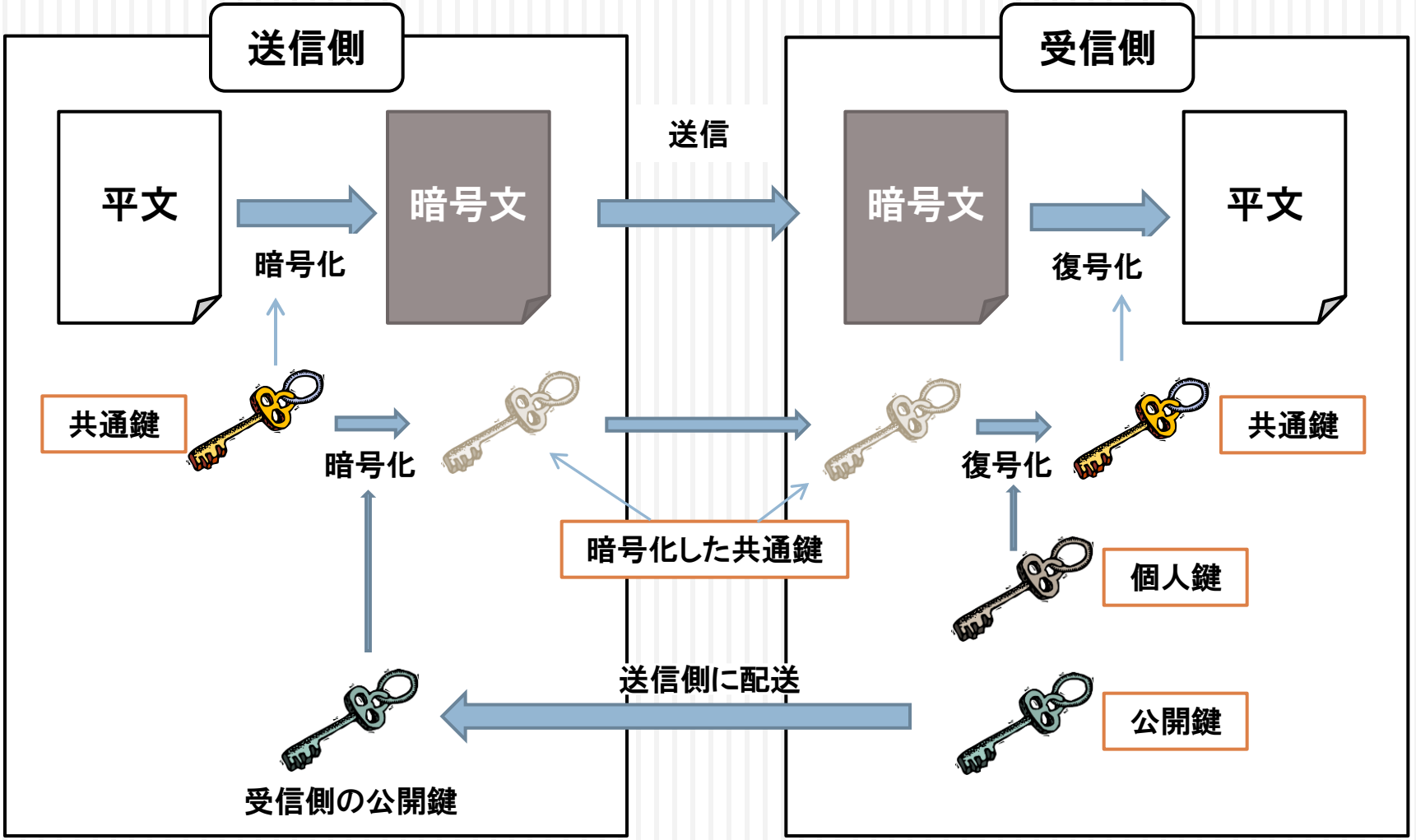
暗号化(公開鍵暗号化方式)



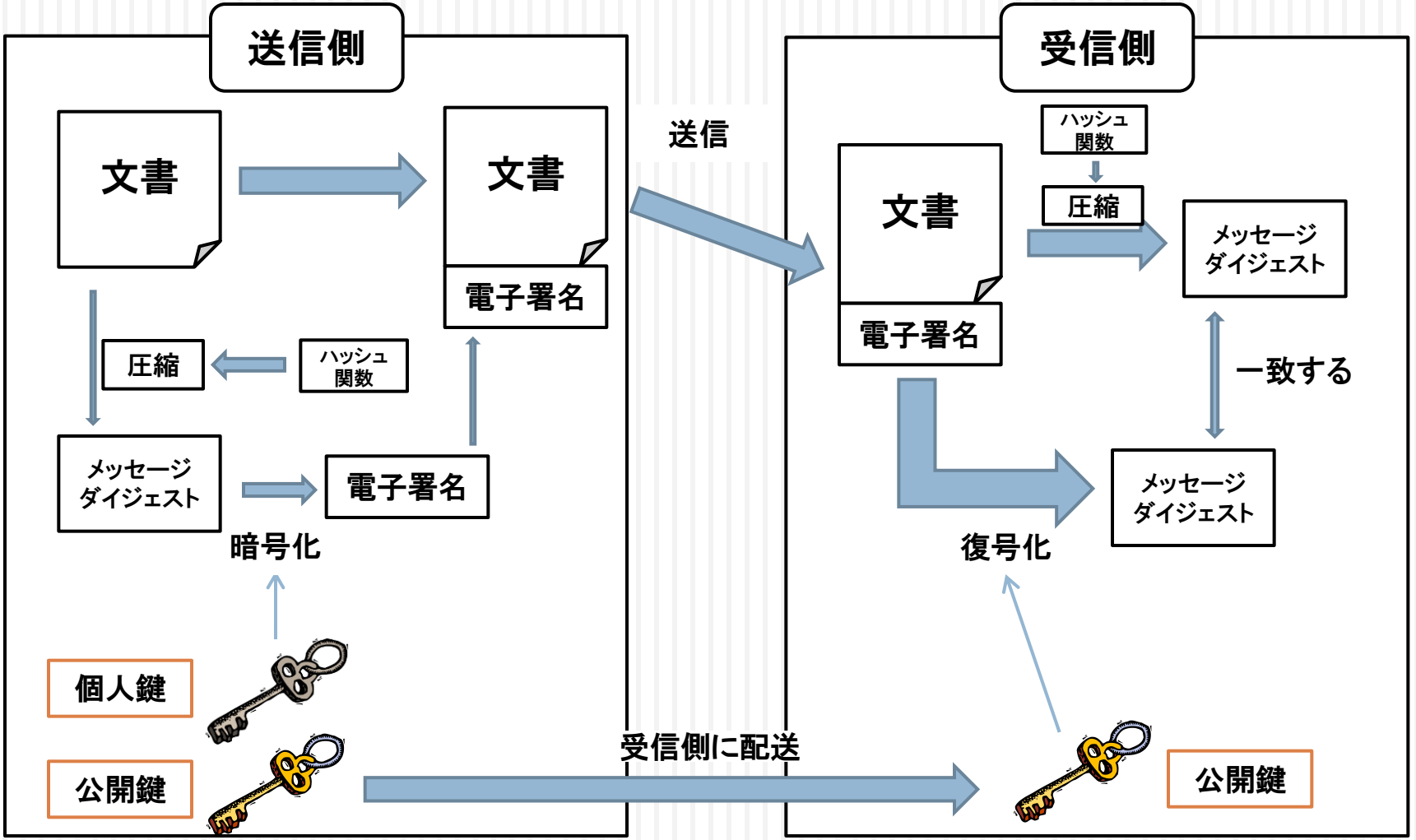
比較

	共通鍵暗号化方式	公開鍵暗号化方式
鍵の種類	共通鍵	公開鍵、個人鍵
鍵の交換	必要 （ユーザーが5人のネットワークでは鍵が10個必要、100人なら4950個必要）	不要
演算速度	速い	遅い

組み合わせ


送信側
受信側
平文
暗号化
暗号文
送信
暗号文
復号化
平文
共通鍵
暗号化
暗号化した共通鍵
復号化
共通鍵
個人鍵
送信側に配送
公開鍵
受信側の公開鍵

電子署名


送信側
文書
文書
電子署名
送信
圧縮
ハッシュ関数
メッセージダイジェスト
電子署名
暗号化
個人鍵
公開鍵
受信側に配送
受信側
文書
電子署名
ハッシュ関数
圧縮
メッセージダイジェスト
一致する
メッセージダイジェスト
復号化
公開鍵

認証機関

- CA（Certificate Authority）
  - ✓ 電子的な証明書を発行する機関
  - ✓ 発行される証明書には、CAの電子署名が添付される
  - ✓ 他には、本人情報、認証局名、証明書の有効期間などとともに、正当性を保証する公開鍵などが含まれる

オンラインショッピング

- 支払い方法
  - 銀行振込、郵便振替、代金引換、クレジットカード
- クレジットカードは危険
  - 番号を盗み取られ、悪用される恐れがある

SSL（Secure Sockets Layer）

- プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる
- 消費者～店舗間のセキュリティを確保するためにSSLが一般的に使用されている

SSL（Secure Sockets Layer）

- ブラウザに標準的に組み込まれているため、ほとんどのインターネット利用者が使用可能

SET（Secure Electronic Transavtion）

- クレジットカード決済専用のオンラインショッピング決済システム
- VISAとMasterCardが開発
- SSLと違い、店舗側が顧客のクレジットカード番号を見ることがない

SETの問題点

- なぜSETはそれほど普及していないのか？

  - ✓ SSLと違って新たにSET用ソフトウェアをインストールしなければならない
  - ✓ そのソフトウェアが高価である
  - ✓ システムの構築に技術が必要

- だが、北欧諸国では、安全性の高さからオンラインショッピングの決済手段としてすべてSETが使われている

ご清聴ありがとうございました