セキュリティ（２）
暗号

セキュリティに使う
暗号について考えてみます

暗号とは

- データを変換して、送・受信者以外の第三者に読み書きできないようにすること
- ことば
  - 暗号化・復号化 ～ 上記の変換・逆変換のこと
  - 平文(ひらぶん) ～ 元のデータ、秘匿 ～ 隠す
  - 鍵 ～ 暗号化・復号化に用いるパラメータ

暗号システム　共通鍵 vs 公開鍵

- 共通鍵暗号 ＝ 暗号化と復号化の鍵が同じ
  - 昔からある暗号システム
  - 共通の鍵で解けるので、鍵を秘密にする
  - 鍵を通信相手に渡す(鍵配送)のが難しい
- 公開鍵暗号 ＝ 暗号化と復号化の鍵が異なる
  - '76年にデフィーらが考案、'82年にRSAが実用化
  - 暗号化・復号化の鍵の対は、互いに推測不可能
  - 一方の鍵を公開できる ⇒ 鍵配送が簡単(公開)

公開鍵暗号の利用方法

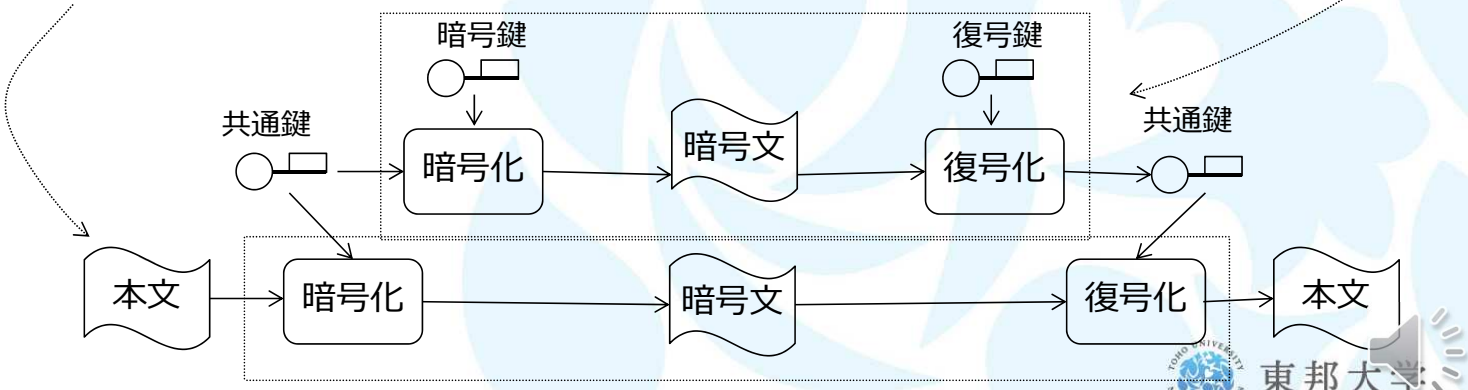
- いくつかの利用方法がある
  - メッセージの秘匿 ～ 第三者から隠す
  - 送信者の認証 (デジタル署名)
    ～ 正しい(意図した)送信者か確認
  - メッセージの改ざん検出 (データ認証)
    ～ メッセージが途中で書変えられていないか
- 公開鍵の計算は処理量が多いのが欠点

公開鍵応用 ～ メッセージ秘匿

- （教科書　図11.4）
- 受信者が(暗号・復号)鍵対を生成する
  - 一方だけを公開して(公開鍵) 送信者に知らせる
- 送信者は公開鍵によってメッセージを暗号化
  - 第三者は秘密鍵を知らないので復号できない
- 受信者は秘密鍵によって復号化できる

公開鍵応用 ～ メッセージ秘匿(続)

- 公開鍵システムの暗号化は処理量が多いので
  メッセージ全体を暗号化したくない
- 通信ごとに共通鍵暗号の鍵を生成し
  その共通鍵を公開鍵システムで交換する
- 本文は共通鍵暗号で暗号化して送る



公開鍵応用 ～ 送信者認証

- 送信者が(暗号・復号)鍵対を生成する
  - 一方だけを公開して(公開鍵) 受信者に知らせる
- 送信者は秘密鍵によってメッセージを暗号化
  - 第三者は秘密鍵を知らないので、
    書変えたものを暗号化することができない
- 受信者は公開鍵によって復号化できれば
  秘密鍵をもつ送信者であると判定できる

公開鍵応用 ～ 改ざん防止

- 送信者認証と同じ原理で、改ざん検出できる
  - 第三者は秘密鍵を知らないので、
    書変えたものを暗号化することができない
  - 大きいメッセージ全体を暗号化するので大変
- ハッシュ関数で一定長のハッシュ値を生成し、
  送信者が計算したハッシュ値と受信者の計算を比較
  - 第三者がハッシュ値を計算し直せば、改ざんできる
- ⇒ メッセージ＋共通鍵をハッシュして送る(MAC)
  - 共通鍵を知らないと正しいハッシュ値が計算できないので
    より安全

他の話題 ～ ユーザの認証（１）

- ユーザ認証 ～ あなたが本当にあなたであるのか？
- パスワード
  - 通信途中で盗まれるとダメ
- ワンタイム・パスワード ⇒ 毎回パスワードが違う
  - 時刻同期方式　時刻＋パスワードをパスワードとして使う
    システムとユーザで同じ時刻（同期）が必要
  - チャレンジ・レスポンス方式
    システムがユーザにチャレンジ情報を送り、ユーザは
    それを元に生成したパスワードを返送して認証
  - いずれも特別なデバイスを使う

他の話題 ～ ユーザの認証（２）

- ハードウェア・キー ～ ICカードキーなど
  - 携行するのが面倒
  - キー自身を盗まれるとダメ
- 生体認証 ～ 生体の一部を特徴として使う
  - 指紋、静脈パターン、虹彩 (瞳の外側) など
  - 紛失しないと言われるが、案外指紋を盗むことなどが可能
  - けがなどで無効になることがある

悪意のあるソフトウェア

- システムに対して、いろいろな攻撃がある
  - 情報を盗み出す
  - システムを破壊して企業活動などを妨害する
  - (最近) 他のシステムを攻撃するためにシステムを乗っ取る
  - (最近) システムを凍結し、解除のために金品を要求する
- 物理的攻撃(破壊など)もあるが、ここはソフトのみ
  - 最近はネットで接続されているので、そこから侵入する
  - ネット接続が無ければ、かなり問題は軽減されるが
    それでもUSBメモリ等を介して感染することもある

悪意のあるソフトウェア

キーワードのみ　教科書 p187～

- マルウェア
- トロイの木馬
- スパイウェア、キーロガー
- コンピュータウィルス・バックドア
- ワーム
- ルートキット

攻撃

キーワードのみ　教科書 p189～

- ソーシャルエンジニアリング・成りすまし・フィッシング
- サービス不能（DoS攻撃、DDoS攻撃）
- バッファオーバーラン

防御

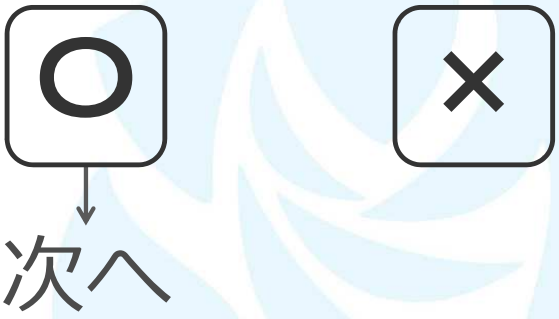
キーワードのみ　教科書 p192～

- アンチウィルスソフトウェア（ワクチン）
- ファイヤウォール、パケットフィルター
- サンドボックス

ここまでのまとめ

1. 保護　⇒　アクセス制御の考え方
   誰(主体)が、何(対象)を、どうする(操作)
   ことができるかどうか
   アクセス制御行列として表現できる
2. 実際の制御情報　～　疎な行列をうまく表現
   ケーパビリティリスト
   アクセス制御リスト

保護(アクセス制御)が何か理解できましたか？



東邦大学