情報通信システム入門セミナー

村川　猛彦

第４回：２０１０年５月１０日（月）

授業資料のWeb公開について

- 授業中に提示したいくつかの画像と，小テスト課題を取り除いています．
- 何かあってここに書かれた内容を引用したいとき，URLは以下のとおり記載してください．
  http://www.wakayama-u.ac.jp/~takehiko/20100510.pdf

本日話すこと

- 自己紹介
- 情報セキュリティの話題
  - 話題１：情報流出とその対策
  - 話題２：安全なパスワード
  - 話題３：情報の管理
  - 話題４：セキュリティの三大要素
- 小テスト

自己紹介

- 氏名: 村川猛彦（むらかわ たけひこ）
- 職名: 講師
- 担当授業: 情報処理Ⅱ，Cプログラミング基礎演習，情報ネットワーク演習，情報セキュリティ
- 研究テーマ:
  - 古典籍と呼ばれる数百年～千年前の文献をコンピュータで効率よく扱えるようにし（ディジタルアーカイブ），文学研究者や考古学ファンに親しみを持ってもらうこと.
  - 世の中の事象を，コンピュータが取り扱いやすい形に捨象，翻訳，変換すること（データモデリング）．また，蓄積されたデータから，人間にとって理解しやすい知識を引き出すこと（データマイニング）.

１年生のみなさんに要望

- ３年次の研究室配属までに
  - いい成績をとっておいてください
  - 「４年で卒業」と「大学院に進学」のどちらにするか考えておいてください
  - 「入力」と「出力」が与えられたときに，それらを結びつける「プログラム」が書けるよう，技能を磨いてください
- 卒業までに
  - C，C++，Javaから最低一つ，それ以外から一つ，プログラミング言語を習得してください
  - 英文（メール，ウェブページも）に戸惑うことのないよう，語学力と語彙を身につけてください
  - 「素材」が与えられたときに，「プログラム」を書いて，興味深い「結果」を引き出せるよう，技能を磨いてください

＜話題1＞情報漏洩・情報流出

- 事例を知るには
  - ウィキペディア（http://ja.wikipedia.org/）にアクセスし，「情報流出」で検索する．
  - セキュリティホールmemo（http://www.st.ryukoku.ac.jp/~kjm/security/memo/）にアクセスし，過去の記事を読む．

情報流出の原因と対策

- 情報流出の原因
  - リムーバブルメディア（USBフラッシュメモリなど）
  - P2Pソフトウェア（Winnyなど）
  - Web日記
  - 不注意によるメール送信
- データ管理の考え方
  - 外部に出していい情報，いけない情報について，組織内でルールを定める．
    - 研究成果は，公刊日まで，Webなどで報告しない．
    - 情報の持ち主（≠収集者，保有者）を意識する
  - 「便利だから」「念のため控えを」は流出のもと
  - 運搬・伝送方法に応じて適切に暗号化
    - 暗号化ZIP，SSH・SSLなど

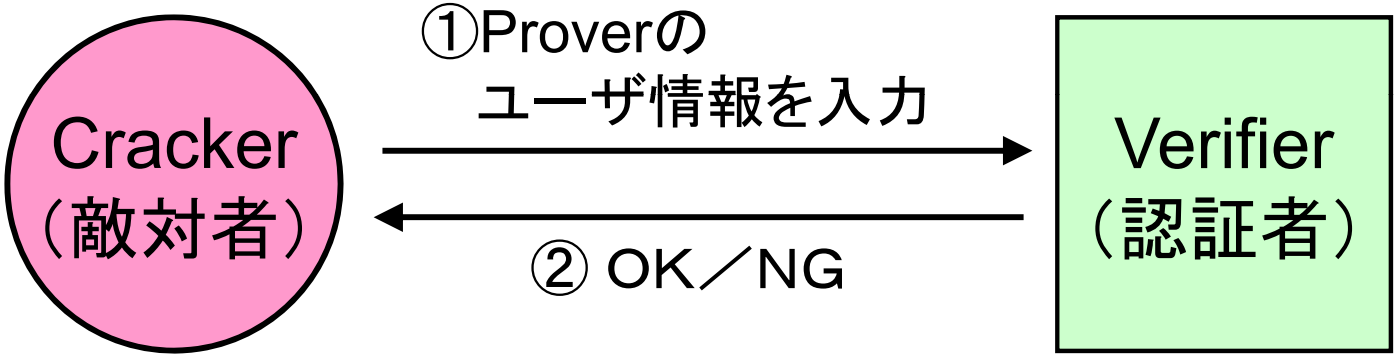
＜話題2＞ユーザ認証とパスワード

- ユーザ認証とは
  - 「個人識別情報（ユーザ名）」と「パスワード」などの組み合わせを使って，コンピュータを利用しようとしている人にその権利があるかどうかや，その人が名乗っている本人かどうかを確認すること
  - 「他人が自分の名前（ID）で入れる」では困る
- ユーザ認証のモデル

- どのようなパスワードを使用すれば安全か？

パスワード解析

- 敵対者の目標：他人の個人識別情報（ユーザ名，口座番号など）および認証方法を既知として，そこから，認証に必要なパスワードを発見すること



パスワード解析の種類

- ブルート・フォース・アタック（brute-force attack，総当り法）
  - すべてのパスワード候補を順にVerifierに送り，「当たり」が出るまで続ける
  - パスワード空間（パスワードになる値の集合）が大きいほど安全である
    - 銀行の暗証番号は，0000～9999のいずれかなので，このパスワード空間の大きさは10^4=10000
- 辞書攻撃
  - 辞書と，選ばれる傾向をもとに，パスワードを発見する
    - computer, murakawa, 20100510, takehiko2010 など
  - 見つかりやすさは，パスワード空間の大きさとは無関係
  - 辞書攻撃をするソフトウェアが存在する

パスワードの選び方

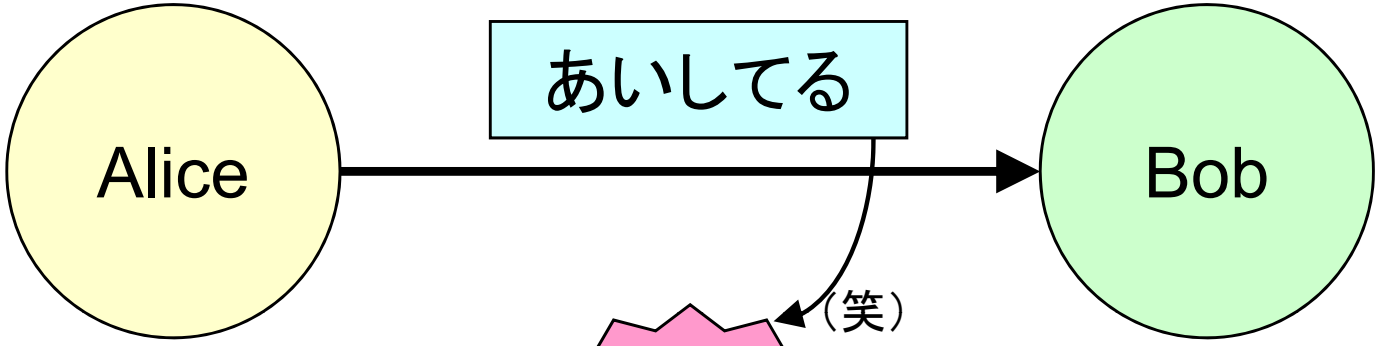
- どのようなパスワードを使用すればよいか？
  - 文字種や字数の制限があれば，それに従う
  - 学内演習室環境のパスワードでは，英数字と記号を織り交ぜて，6文字以上8文字以内にする
  - 自分は思い出しやすいものにする
    - 長ければいいってもんでもない
  - 辞書攻撃で破られるようなパスワードは使用しない
    - 個人情報や家族・恋人などの名前，生年月日，車のナンバー，電話番号など
  - パスワードをメモしない（？）
  - あちこちの認証システムで同一のパスワードにしない（？）

＜話題3＞情報の管理

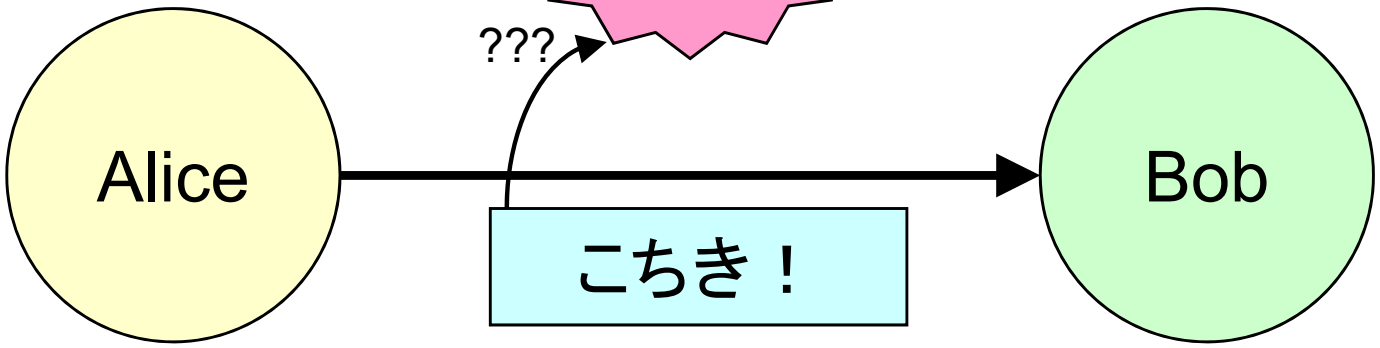
- 技術で保護・防御：暗号
- 法律で規定・抑止：個人情報保護法

暗号とは

- 暗号がないとき…



- 暗号があるとき…



暗号の方法

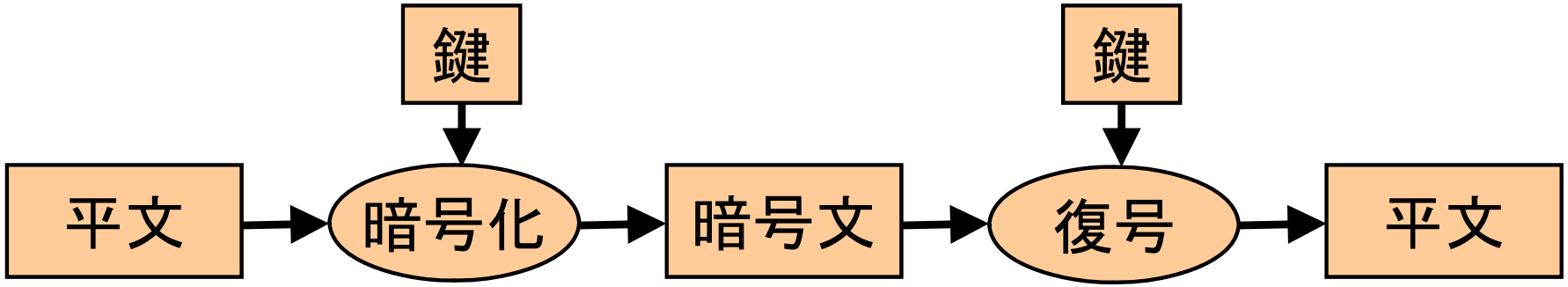
3文字ずらすだけ
（解読も容易）

シーザー暗号の例

Wagahai Ha Nekodearu

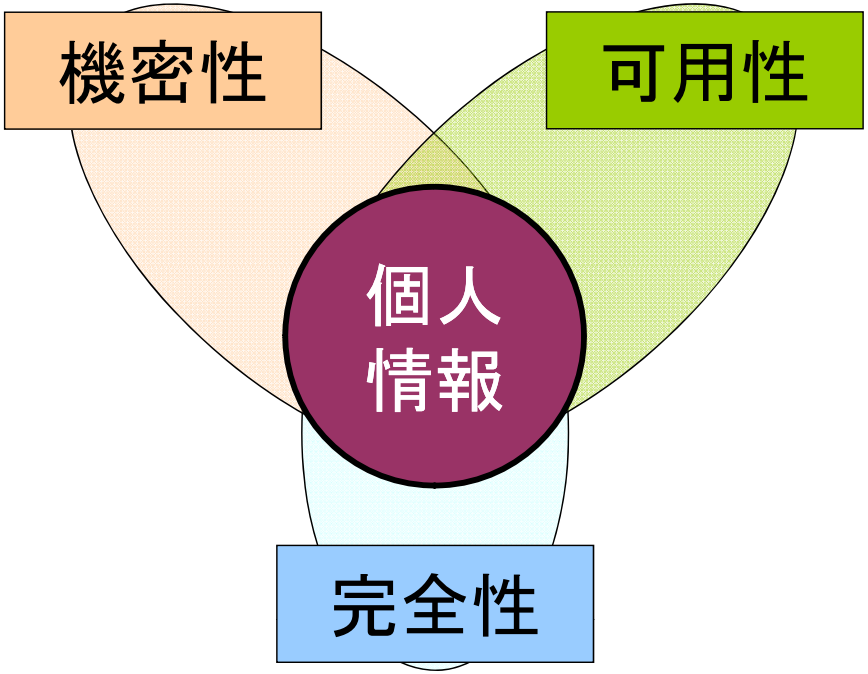
Zdjdkdl Kd Qhnrghdux

- 有名な暗号アルゴリズム（暗号の方法）
  - シーザー暗号, DES, AES, RSA など
- 現在の標準的な暗号は，
  - 暗号化：「平文」と「鍵」から「暗号文」を作る．
  - 復号：「暗号文」と適切な「鍵」から，元の「平文」を得る．
  - 解読：「暗号文」から，「平文」もしくは「鍵」を得る．
  - 「暗号文」のみから，一見しただけでは「平文」や「鍵」がわからないようにしないと！



個人情報保護法

- 目的(第1条)
  - 個人の権利と利益の保護
    - 個人情報は，データ化した企業・組織のものではなく，個人情報の本人のもの
  - 高度情報通信社会における個人情報の有用性の配慮
    - 企業・組織が，個人情報を適切に管理・使用するための方針を定める
- 反した運用をすれば，個人や事業者に罰則(懲役，罰金)が課されるほか，社会的信用を落とす．



個人情報の例

- 氏名
- 生年月日，住所，居所，電話番号，メールアドレス
- 会社における所属や職位
- 電話帳や刊行物などで公表されている個人情報
- 名刺（に記載される個人情報）

- 電子化するしないに関わらず対象
- 施行（2005年4月）の前に収集した情報も対象

個人情報とプライバシーの違い

- 個人情報保護
  - 事業者の個人情報に対する管理責任に関するもの
  - たとえていうなら，ハガキの表面（宛名）
- プライバシーの保護
  - 他人に知られたくないことを秘匿すること
  - たとえていうなら，ハガキの裏面（文面）

＜話題4＞情報セキュリティの三大要素

- 機密性（Confidentiality）…漏れない
  - 許可されている人だけが情報にアクセスできる状態
- 完全性（Integrity）…書き換えられない
  - 情報が整合性が取れて保存されている状態
- 可用性（Availability）…立入禁止にならない
  - 必要な時に情報にアクセス出来る状態

- 定性的には，この3つをすべて満たすものが「安全（secure）」で，安全にするための諸技術が「情報セキュリティ」
- 定量的に表現することもある
  - 資産価値 ＝ 機密性 ＋ 完全性
  - コスト ＜ 資産価値×攻撃成功確率　（ならば対策をとる）

機密性・完全性・可用性

- 透明の封筒に入った情報
  - 完全性を満たすが，機密性は満たさない
- ホワイトボードにあれこれ書き込む
  - 可用性を満たすが，完全性は満たさない
- どこかの本に秘密のメモを挟み，忘れてしまう
  - 機密性を満たすが，可用性は満たさない