# 情報セキュリティ
# 情報セキュリティ技術の活用

情報の科学　第１９回授業

03ネットワークがつなぐコミュニケーション

対応ファイル：19exp18.xls（前回）

# 情報セキュリティ対策

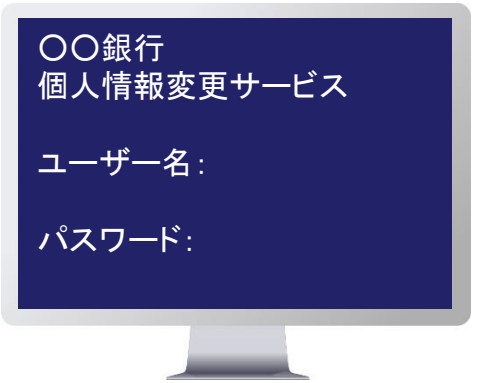
- 技術的な側面
  - 機器やソフトウェア等を用いて対策
- 人的・組織的な側面
  - 利用者の教育や啓発を行うことによる対策
- 法的な側面
  - 不正アクセス禁止法などによる対策

# SSL（P.78）

- ハイブリッド暗号の1つで、「https://」で始まる
- 重要な情報をやりとりする時には確認を！

# フィッシング詐欺

本物のサイト




②アクセス

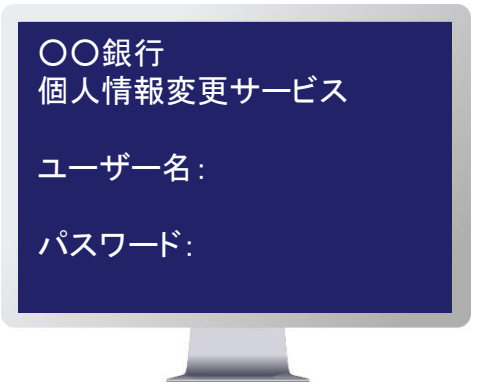
①ニセ
メール

〇〇銀行より

あなたのアカウントが凍結されました！
すぐに以下にアクセスを！

http://www.usonosaite.com/account/・・

ニセのサイト




③ニセのサイトから情報ゲット

# 認証技術による対策（P.73）

- パスワードの運用
- いろいろな認証技術
  - 生体情報（指紋・静脈など）
  - 記憶情報（パスワード、パターンなど）
  - 所持情報（スマートフォン、トークン）
- 二要素認証、二段階認証

# 認証技術の例1（パターン）

- パターンを覚える
  - スマートフォンのロック解除

# 認証技術の例2

- 二段階認証

http://www.google.co.jp/intl/ja/landing/2step/#tab=how-it-works

- パスワードカード（トークン）

http://www.jp-bank.japanpost.jp/direct/pc/security/token/dr_pc_sc_token.html

# 認証技術の例3

- 合言葉

# 認証技術の例4

- ソフトウェアキーボード
  - キーロガーに有効

# 情報セキュリティ対策（つづき）

- 技術的な側面
  - 機器やソフトウェア等を用いて対策
- 人的・組織的な側面
  - 利用者の教育や啓発を行うことによる対策
- 法的な側面
  - 不正アクセス禁止法などによる対策

# 情報セキュリティの3要素（P.72）

- 機密性・完全性・可用性

# ソーシャルエンジニアリング

- 盗み見たり、ある人物を装うなどして、社会的な手段で不正に情報を得ること。

# ソーシャルエンジニアリング

- 2011年のある企業による調査結果
  - 「脅威（＝恐ろしくおびやかす存在）」と認識
    - ９７％（セキュリティ担当者）
    - ８６％（ITセキュリティ担当者）
  - 実際に攻撃にあった：４３％
  - 被害にあっていないと確信：１６％
  - 攻撃にあったかどうかわからない：４１％

# 情報セキュリティ対策（つづき）

- 技術的な側面
  - 機器やソフトウェア等を用いて対策
- 人的・組織的な側面
  - 利用者の教育や啓発を行うことによる対策
- 法的な側面
  - 不正アクセス禁止法などによる対策

# 不正アクセス禁止法（p.72）

- 「不正アクセス行為の禁止等に関する法律」
  - 他人のIDやパスワードを勝手に利用したら犯罪
  - 偶然知ってしまっても利用したらダメ
  - 正規の手段以外でネットワークに入る事も犯罪
    - 1年以下の懲役または50万円以下の罰金
  - 他人のID・パスワードを周りに教えても犯罪
    - 30万円以下の罰金