

# 情報セキュリティと認証技術

情報 I 第15回授業

03情報通信ネットワークのしくみ

対応ファイル: 22exp14.xls (前回)

# 復習

- インターネットは、世界中の人が集まる場所
- インターネット上は、「ハガキ」程度のセキュリティ
- 悪意をもった人も中には存在
- それぞれの「しくみ」に応じたセキュリティ対策が必要！
- 悪意の「手口」を理解し、「身を守る」方法につなげる！

# 情報セキュリティ対策の3つの側面

- 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

# 無線LANのセキュリティ(P.181)

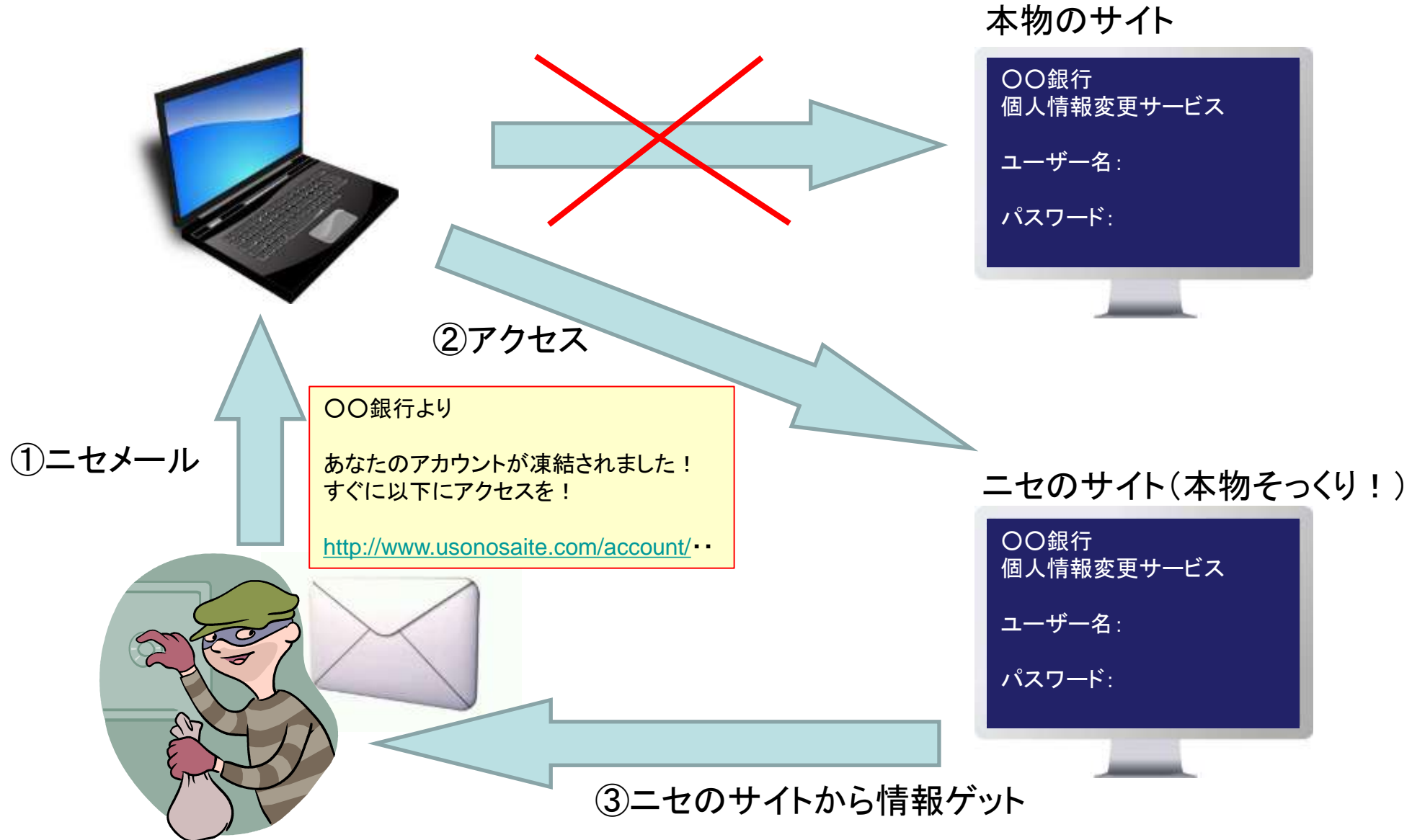
	WEP	WPA	WPA2	WPA3
特徴	最初の規格 現在は 非推奨	WEPの 改良版	WPAの 改良版	WPA2の 改良版
主な 暗号化方式	WEP	TKIP	CCMP (AES)	CCMP (AES)
暗号化の 強度	×(弱い)	×(弱い)	○(強い)	◎(より強い)

Wi-Fi接続には、「暗号化キー(鍵)」が設定され、キーを知らない端末が勝手に接続できないようになっている。

# SSL (P.181)

- ハイブリッド暗号の1つで、「https://」で始まる
- 現在はバージョンアップし、「TLS」などとも言われる。
- 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



# 認証技術による対策(P.176)

- 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)





# 認証技術の例2

- 二要素認証

1. IDなどを入力

会員サイトへ

ユーザIDを入力

3. パスワードとセキュリティコードを入力

ユーザID

パスワード

セキュリティコード

4. 認証完了

会員サイトへ  
ようこそ！

2. 登録携帯にSMS等でセキュリティコードを配信



記憶情報(パスワード)と所持情報(スマートフォン)の二要素で認証

# 認証技術の例3

- 二段階認証

1. ID・パスワードなど  
を入力

ユーザID

パスワード

2. あらかじめ登録した  
「合言葉」を入力

質問: あなたの好きな場所は?

回答

3. 認証完了

〇〇銀行

記憶情報(パスワード)の後、さらに  
記憶情報(合言葉)の二段階で認証

# 認証技術の例4

- ソフトウェアキーボード
  - 「キーロガー」に対応

# 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.176)

- 機密性
  - パスワードの設定
  - 立ち入り禁止区域の設定
- 完全性
  - デジタル署名
- 可用性
  - ディスクの多重化(RAID)
  - 無停電電源装置(UPS)

# 情報セキュリティポリシー

- 情報システムごとに3要素をそれぞれ評価し、対策を立てる
  - 例) Aシステム 機密性:A 完全性:A 可用性:B
  - Bシステム 機密性:C 完全性:B 可用性:C など
- 「コンピュータ」だけではなく、情報そのものの扱いも定める
  - 例えば、「USBフラッシュメモリに保存しない」「外部持出禁止」など
- 定期的にチェックし、内容に不備がないかを確認する
  - 「ルールを厳格に守ること」も大切だが、「安全を確保」することが目的
  - 定期的に見直し、必要に応じて状況に合わせて変更する
    - 「実施不可能」なルールは意味がない
- トラブルが起きた時の対策なども定められることが多い

# ソーシャルエンジニアリング

- 盗み見たり、ある人物を装い電話で聞き出すなどして、社会的な手段で不正に情報を得ること。
  - ショルダーハッキング、トラッキング、なりすまし電話、なりすましメールなど
  - 多くの不正アクセスの「入り口」となる
  - 組織での脅威第1位「標的型攻撃」にて多用される

# 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

# 【復習】不正アクセス禁止法

(平成25年改正)

- 主な内容(詳細は下部の総務省リンクにて)
  - 三年以下の懲役または百万円以下の罰金
    - 他人のID・パスワードで「なりすまし」ログオン
    - セキュリティホールを突くなどして不正にログオン
  - 一年以下の懲役または五十万円以下の罰金
    - 不正目的で他人のID・パスワードを不正に取得
    - 他人のID・パスワードを別の人に教える
    - 不正目的で不正取得した他人のID・パスワードを保管
    - 本物に似せたサイトに誘導しID・パスワードを騙し取る(いわゆる「フィッシング」)

総務省「国民のための情報セキュリティサイト」

[https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/security/basic/legal/09.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/09.html)

# まとめ

## 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
  - 巧妙化する犯罪や技術の進歩に対応する法律の整備

→ あらゆる側面からの対策・対応の必要性