ネットワークの脅威に対する個人の対策

広島大学 AI・データイノベーション教育研究センター
村上 祐子

目標

情報セキュリティに留意してネットワークサービスを安全に利用するために個人が注意すべき点を指摘できるようになる

この授業で紹介すること

- インターネットに関する脅威への対策として３原則を理解する
- 個人がデータや情報を守るために適切な行動（フィッシング事例から）

キーワード

情報セキュリティ、サイバーセキュリティ、フィッシング、マルウェア

こんなことはありませんか？

From: 〇〇ショッピングサイト
1234@ooshoping.com
Date: 2022.4.14
Subject: 【重要】アカウント強制停止のお知らせ

〇〇ショッピングサイト お客様

日ごろは〇〇ショッピングサイトをご利用いただきまして誠にありがとうございます。
カスタマーのアカウントは強制停止されています。
以下のボタンをクリックしメンバーシップを確認する必要があります。

〇〇ショッピングサイト ログイン

24時間以内にご確認がない場合、お客様のアカウントの利用制限につながります。ありがとう。

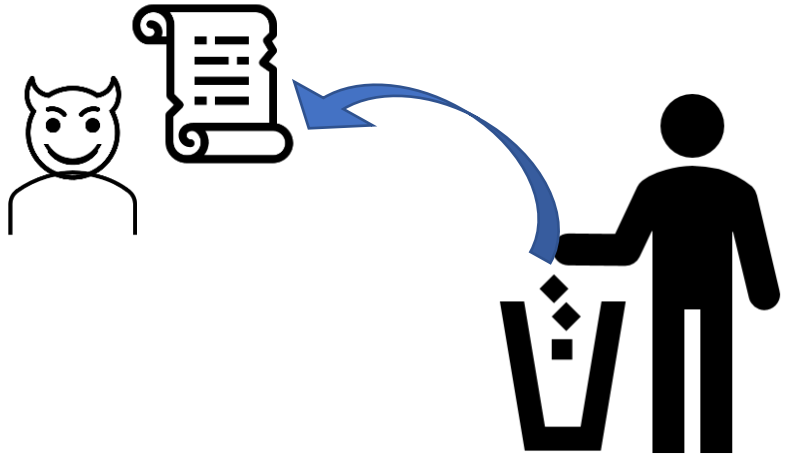
ちょっと待って！
このメールはショッピングサイトを騙った詐欺かも！

情報セキュリティ

情報セキュリティは下の３つの性質を維持すること (ISO/IEC 27000)

- 機密性：情報へアクセスが認められた人だけが情報にアクセスできる
- 完全性：情報が破壊、改ざん、消去されない状態が保持されていること
- 可用性：情報へのアクセスを認められた人だけが必要な時に情報にアクセスできる

情報セキュリティの対象になる事例

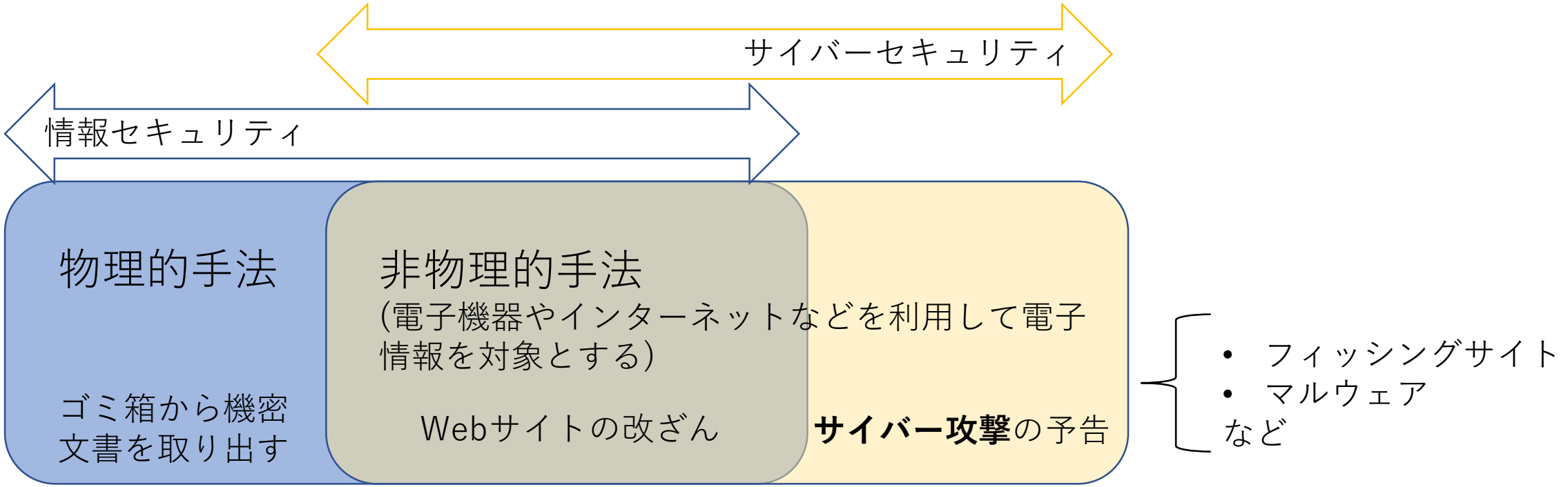


ゴミ箱から機密情報を取り出す

Webサイトの改ざん

サイバーセキュリティ

コンピュータなどの電子計算機の利用やネットワークの利用において、情報セキュリティを脅かす被害を防ぐように対策すること、またその状態を維持すること



サイバーセキュリティ初心者のための３原則

1.　ソフトウェアの更新

- ソフトウェアを更新しできる限りソフトウェアを最新の状態に保つように心がける
- 自動更新機能を有効に活用する

2.　IDとパスワードの適切な管理

- パスワードは他人に簡単に想像されないものにする
- 同じパスワードを使い回さない
- パスワードを紙などにメモする場合は他人の目につきにくいところに保管する

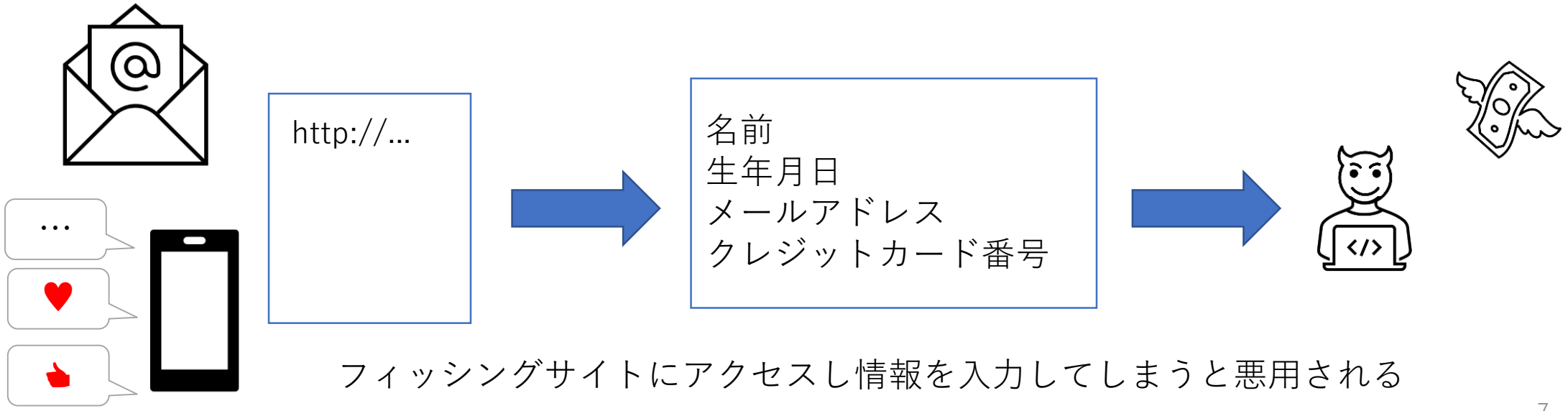
3.　ウイルス対策ソフト（ウイルス対策サービス）の導入

- コンピュータにウイルス対策ソフトを導入する
- コンピュータにどのようなウイルス対策ソフトを導入しているのか把握する

フィッシング

実在する組織や個人になりすまして、
- サービスにログインするためのユーザー名、パスワード
- クレジットカード番号

といった経済的な価値がある情報を搾取する行為



フィッシングサイトにアクセスし情報を入力してしまうと悪用される

フィッシングメールの注意点

From: ○○ショッピングサイト
1234@ooshoping.com
Date: 2022.4.14
Subject: 【重要】アカウント強制停止のお知らせ

○○ショッピングサイト お客様

日ごろは○○ショッピングサイトをご利用いただきまして誠にありがとうございます。
カスタマーのアカウントは強制停止されています。
以下のボタンをクリックしメンバーシップを確認する必要があります。

○○ショッピングサイト ログイン

24時間以内にご確認がない場合、お客様のアカウントの利用制限につながります。ありがとう。

メールアドレスに不審なところはないですか？

正しい会社名のアルファベット：ooshopping
でなければ、フィッシングメールだと疑う

- 明らかに会社名が違う
- 似ているけどちょっと違う
  (1文字間違っている、抜けがある)

日本語として読みにくいことはありませんか？

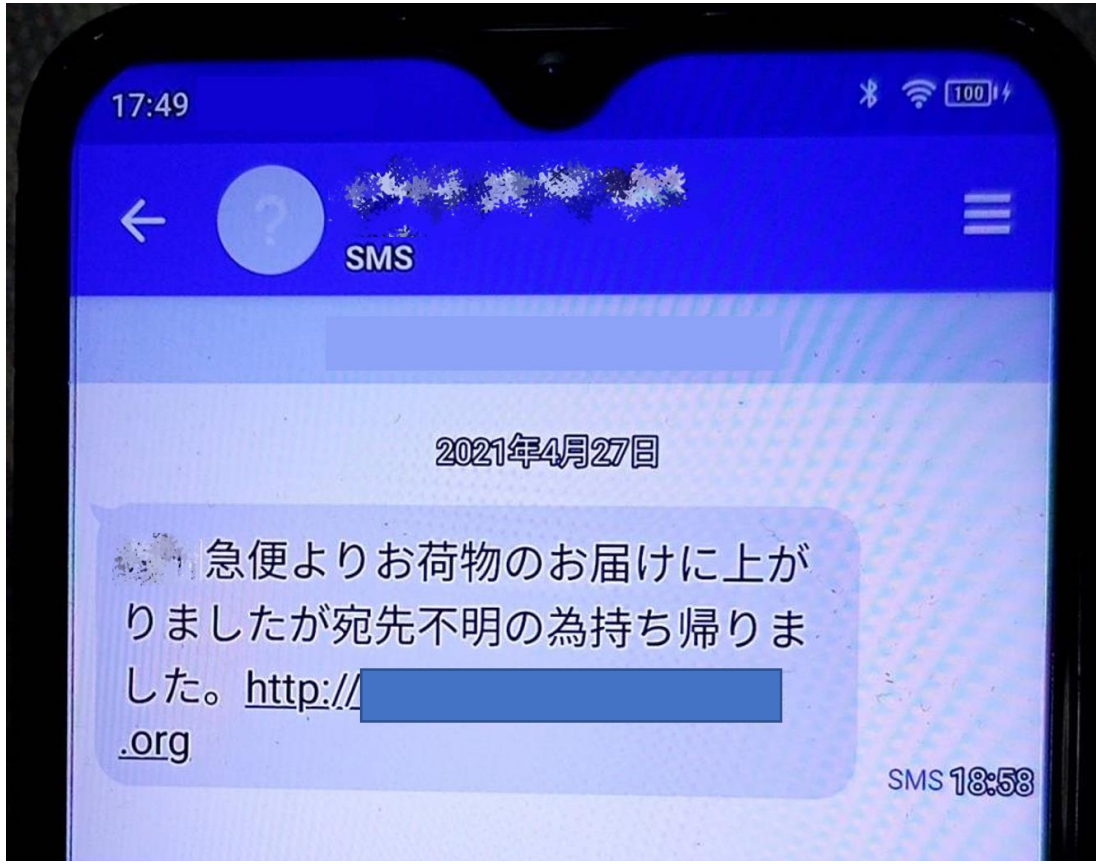
- 異なる言語が混じっている
- 文章の理解はできるが、言い回しに違和感

少しでも「あれ？」と思ったら、メールに対応しない

例題

スマートフォンに右のようなSMSが届きました。

荷物の不在通知を安全に確認したい場合にはどうしたらよいでしょうか



解説

フィッシング詐欺の一例

⚠何も確認せずにリンクをクリックしない

- 宅配業者の公式サイトにアクセスして情報収集する
  - メール, SMS等に記載されたリンクはクリックしない
  - 自分でブラウザを開いて、公式サイトにアクセスし、以下を確認する
    - フィッシングメールについての注意喚起
    - マイページなど、購入や操作履歴が確認できるページ

    身に覚えのない購入、操作履歴があればカスタマーセンターに問い合わせする

日ごろからトラブル事例を紹介しているサイト等で情報収集することが重要

例：「インターネット消費者トラブル防止キャンペーンTOP」,
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/trouble/

その他注意すべき脅威：マルウェア

デバイスに不利益をもたらす悪意のあるソフトウェアやプログラムコード

マルウェアの種類	説明・特徴
ウイルス	• 「ソフトウェアの実行」など人の操作により感染する • 感染したプログラムをもとに自己増殖し他のプログラムへ感染を拡大
ワーム	• ネットワークを通じて拡散する • 拡散に人の介入や宿主のプログラムなどは必要なし
トロイの木馬	• 無害なアプリケーションを装っており気が付きにくい • 個人情報の盗難や行動監視に長けている • 自己増殖はしない
スパイウェア	• 情報を搾取するためコンピュータ内部からインターネットに対して情報を送る
アドウェア	• 宣伝や広告収入を目的とした無料で提供されるソフトウェア • 望まない広告のしつこい表示や閲覧履歴を許諾なく外部に送信する等の迷惑行為
ボット	• 遠隔地からリモート操作できる • 不正に操作して迷惑メールの送信元として悪用されるなど
ランサムウェア	• 勝手にデバイスにインストールされファイルを暗号化 • データ復旧のために金銭を要求する

問題

授業での課題に取り組むためにWeb検索を使って調べ物をしています。あるサイトをクリックしたときに、いきなり「おめでとうございます！ゲーム機が当選しました。」と表示されました。

さらに続けて「本人確認のため、クレジットカードの情報を記載してください。」という案内と入力フォームが表示されました。

(1)これはどの種類のマルウェアに該当するでしょうか？

(2)このような表示が出た場合、どのように対処したらいいでしょうか？