情報セキュリティの現状と対策

情報連携統括本部情報戦略室　竹内義則

概要：

コンピュータウイルス等の情報セキュリティに対する脅威は，ますます悪質になっている．攻撃方法は，ユーザの心理の隙をつくなど洗練されてきている．この講義では，これらの攻撃から身を守るために，まず，情報セキュリティの要素である，機密性，完全性，可用性について解説し，それらに対してどのような危険があるか説明する．次に，最近の情報セキュリティの脅威の中から，心理の隙をつく受動型攻撃，脆弱なウェブサイトを狙った攻撃，巧妙化する標的型攻撃など，影響の大きいものを取り上げ，その特徴や方法を説明する．最後に，それらの脅威から身を守るために，電子メール使用時やウェブの閲覧時に気をつけることを中心とした対策を説明する．

情報セキュリティとは？

- 情報の機密性
  - 許可された者だけが情報にアクセスできること
- 情報の完全性
  - 情報および処理方法が正確であることおよび完全であること(不正に改ざんされていないこと)
- 情報の可用性
  - 許可された者が必要なときに情報または情報システムを利用できること

脅威と脆弱性

脅威
- 泥棒
- 情報漏洩
- 不正侵入
- サービス不能攻撃

脆弱性
- 鍵のかからない窓
- プログラムの不具合
- 処理能力不足

情報セキュリティの脅威（1）

- 機密性に対する脅威
  - 個人情報が漏れる、盗まれる
    - プライバシー
    - クレジットカード番号、暗証番号
  - 機密情報が漏れる、盗まれる
    - 技術情報
    - 顧客情報
    - 人事情報
    - 戦略情報

情報セキュリティの脅威(2)

- 完全性に対する脅威
  - 情報の改ざん、削除
    - ホームページの改ざん
    - ファイルの不正な削除、改ざん、追加
  - 情報システムの設定の不正変更
    - メールサーバへの侵入、設定変更:
      - スパムメール(迷惑メール)の発信、中継
    - Webサーバへの侵入、設定や内容の変更:
      - ホームページ改ざん
    - ファイルサーバへの侵入
      - ファイルの削除、改ざん

情報セキュリティの脅威（3）

- 可用性に対する脅威
  - サービス妨害（サーバへの攻撃）
    - DoS (Denial of Services) 攻撃
      - サーバに大量のデータを送り、機能停止させる攻撃
    - メールサーバ攻撃
      - メールサーバに大量のメールを送り込み、メール配信機能を停止させる攻撃
      - スパムメール（迷惑メール）
    - Webサーバ攻撃
      - Webサーバの背後にあるデータベースを攻撃

どんな危険？
---- インシデント例（１）

- 悪意、うっかりミスによる情報漏洩
  - IDとパスワードのずさんな管理によりシステムに侵入され、顧客情報が流出
  - 個人情報の入ったPCを紛失、盗難
  - 情報漏洩のおよそ8割はうっかりミスが原因

- インシデント：情報セキュリティ上の被害、損害につながる人為的事象

どんな危険？
---- インシデント例（2）

- フィッシング(Phishing)詐欺
  - おれおれ（振り込め）詐欺と同じような手口
  - 手口の例
    - 「○○カード会社です。ユーザアカウントの有効期限が近付いています。次のURLにアクセスして、更新してください。」などと書いたメール、CDなどを送りつける。
    - そのURLにアクセスすると本物そっくりに作った偽のウェブサイトに行くようにしておく。
    - クレジットカード番号、銀行預金口座番号、パスワードの入力を促し、それらを盗み、悪用する。

どんな危険？
---- インシデント例（3）

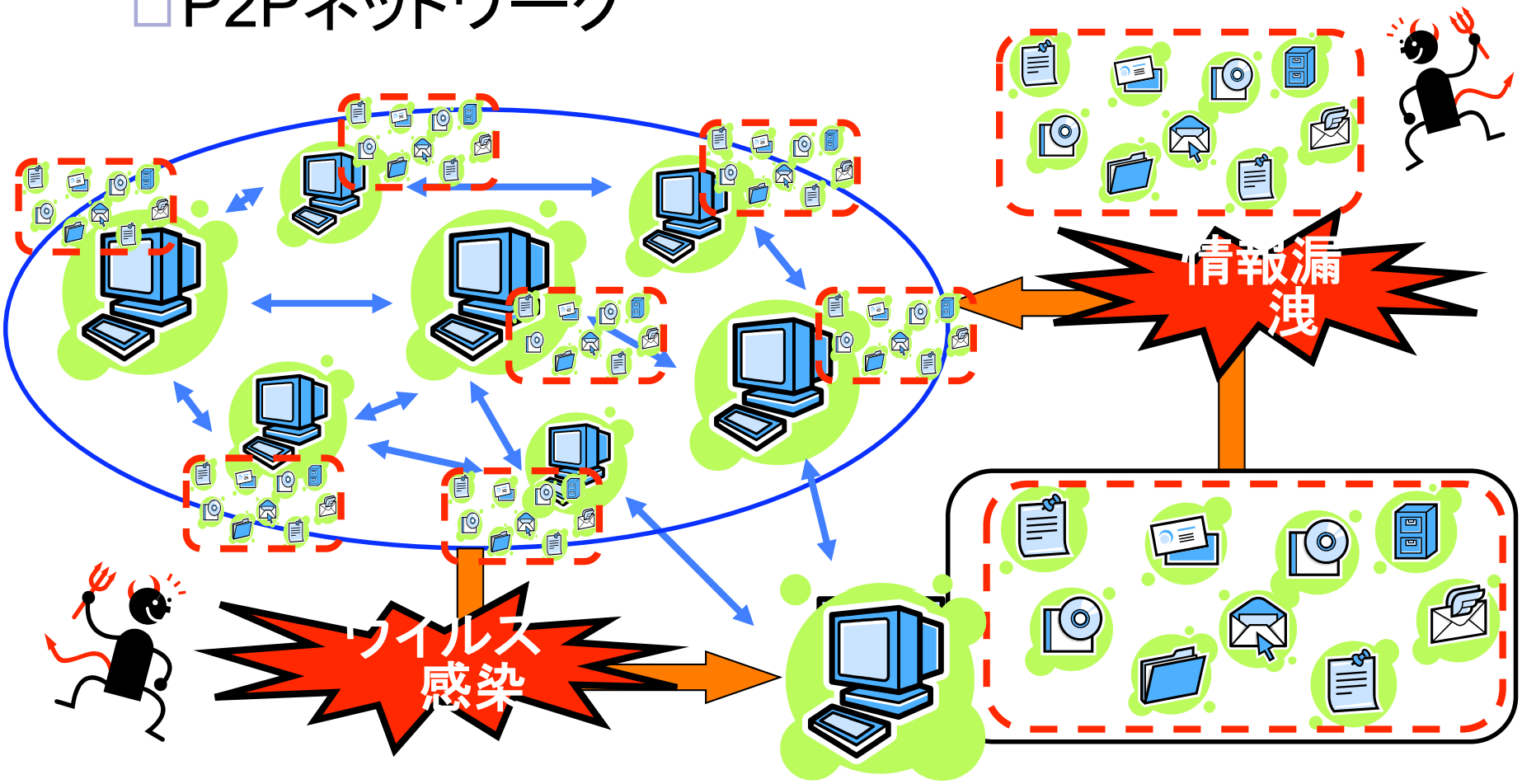
- ファーミング(Pharming)
  - フィッシング詐欺を自動化
  - DNSを書き換える
    - 書き換え前（正常）：www.nagoya-u.ac.jp 133.6.1.10
    - 書き換え後：www.nagoya-u.ac.jp xxx.xxx.xxx.xxx
  - 偽ページに誘導し，個人情報を入力させる
  - 畑に種をまいて，収穫を待つ

どんな危険？
---- インシデント例（4）

- Winnyによる情報漏洩
  - 機密情報の入ったパソコン上のWinnyがウィルスに感染し、機密情報が流出
  - 一般企業、官公庁、保険会社、銀行、電力会社など

Winnyによる情報漏洩

- P2Pネットワーク



どんな危険？
---- インシデント例（5）

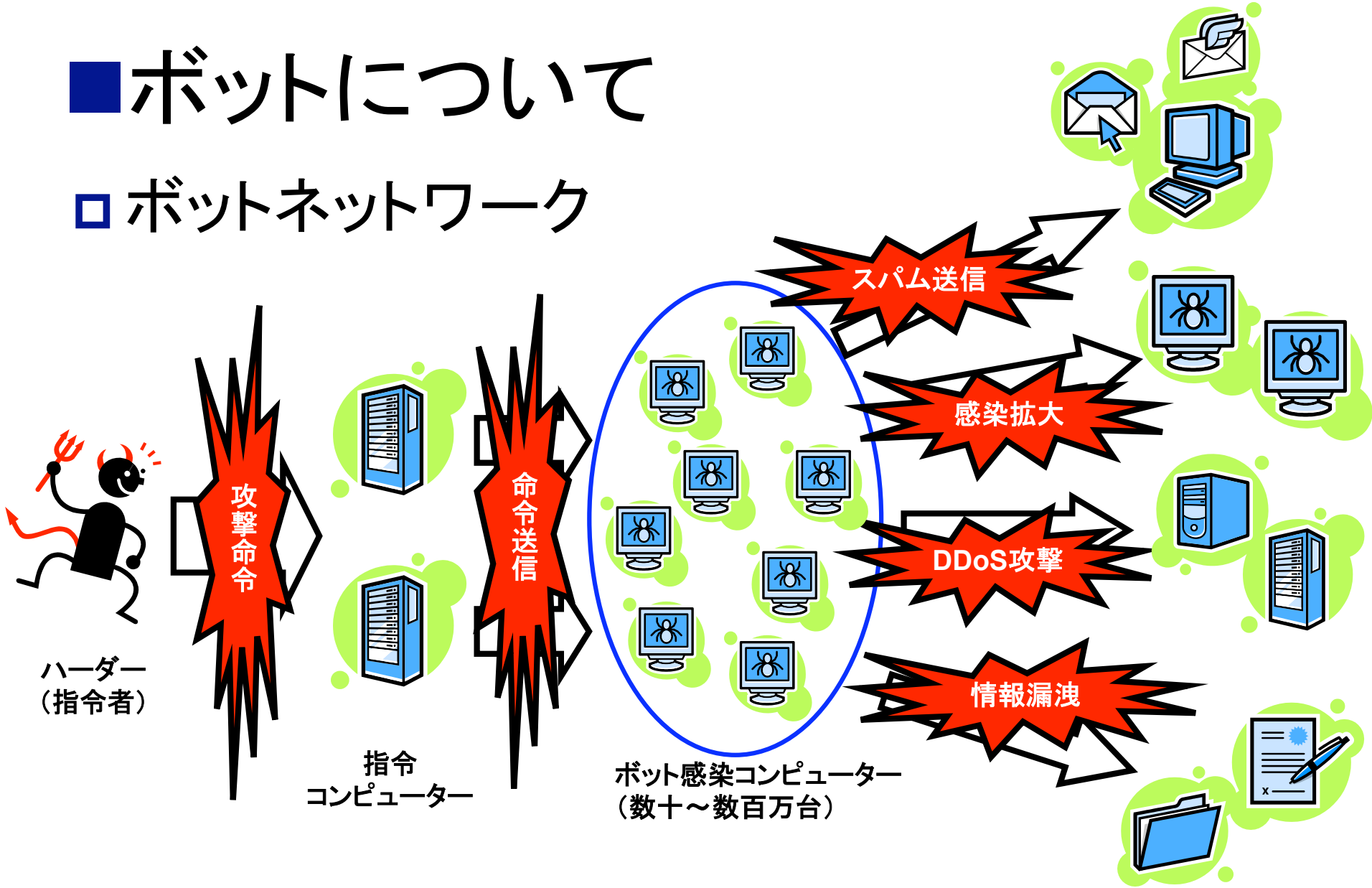
- スパイウェアによる被害
  - スパイウェアとは
    - 利用者が知らないうちにPCにインストールされ、個人情報や操作履歴などを収集し、外部に送信する（スパイ活動をする）プログラム
    - キーロガー、アドウェア、トロイの木馬
  - インターネットバンキング利用時に入力される口座番号、ログインパスワードなどをスパイウェアに盗まれて、大金を引き出された。

どんな危険？
---- インシデント例（6）

- ボットによる被害 - 2005年ごろから
  - ボットとは
    - ロボットのように外部からの指令を受けて他者を攻撃するプログラム。メールの添付ファイルや罠をしかけられたWebサイトへのアクセスにより伝染。
  - 数万台の感染PCを使って攻撃を集中させることで、企業のネットワークを利用できなくする。

ボットについて

ボットネットワーク



何に注意？
---- 情報セキュリティを脅かすもの

- コンピュータウイルス（Virus）
- メール
- ソフトウェアの脆弱性
- Winny
- 怪しげなサイト(Webページ)
- うっかり、無用心
- 個々の心構え！

何に注意？

---- ウイルスについて

- ウイルスとは、コンピュータに被害をもたらすプログラム
- メールやWebサイトなどを通じて伝染。ネットワークに繋ぐだけで感染する場合も
- 2008年はUSBメモリから感染するウイルスが猛威を振るった
- 危険度の高いものから低いものまで、多種多様（数万種類）。スパイウェア、ボットもウイルス
- 管理者の対策：メールゲートでウイルス除去、など
- 利用者の対策：以下で

何に注意？

---- メールについて

- 見知らぬ人からのメールの添付ファイルは開かない。ウィルス感染の一番の原因
- よく知っている人からでも、本文にファイルを添付することが書いてない場合は、開かない
- メールに書かれている怪しいURLを不用意にクリックしない。フィッシングに注意
- メールで個人情報や信用情報を送信しない
  - パスワード、クレジットカード番号など
- メールの暗号化や電子署名を使う

何に注意？
---- ソフトウェアの脆弱性

- ソフトウェア（OSなど）を常に最新の状態に
  - Microsoft Update（Microsoft社）
  - ソフトウェアアップデート（Apple社）
- ウイルス対策ソフトを最新の状態に
  - 情報連携統括本部のWebページ
    - 左メニューより「サイトライセンス」→「ウイルス対策」
- 信頼できないソフトウェアを使わない

何に注意？

---- 怪しいサイト

- 怪しいサイトには近づかない
  - 最近は正規サイトの改ざんも多いのでパソコンのウイルス対策はしっかりと！
- 個人情報（IDやパスワードなど）を入力するときは、ブラウザに鍵マーク が出ていること(URLがhttps://...)を確認
  - 初めてのサイトにアクセスするときは、鍵のマークをクリックして、電子証明書を見る
- 金融機関などからの緊急メールは怪しい
  - 電話等で確認

何に注意？
---- うっかり、無用心

- パスワード関連
  - IDやパスワードは他人に教えない
  - 簡単なパスワードは避ける（簡単に解析されてしまう）
  - パスワードを紙に書いておくのは危険
- メール関連
  - メール誤送信。アドレス間違い、特に、CCに注意
- 情報持ち出し
  - 個人情報の入ったパソコンを持ち出さない。紛失、盗難の危険
  - 個人パソコンに機密情報をコピーしない

何に注意？

---- 日々の心構え

- 防げない(？)攻撃
  - ゼロデイ攻撃
  - 正規サイトの改ざん
  - **完全に感染を防ぐことは無理**
- 感染の兆しを見逃さない
  - 動作が異常に遅い
  - 知らないファイルがある
- 感染後の対応が重要
  - すぐにネットワークから切り離し二次被害を防ぐ
  - バックアップ等はこまめに

不正アクセス

- ネットワークへの不正な侵入や運用しているサービスへの妨害，もしくはデータの破壊行為等を行う.
- 多くは，セキュリティホールを狙われる
  - サービス妨害（Dos攻撃、DDos攻撃）
  - データ改竄
  - メールの不正中継
  - 踏み台
  - 成りすまし
  - etc…

不正アクセス対策

- OSやソフトウェアの脆弱性を解消する
- サーバ等の不要なポートは閉じる
- ID，パスワード管理
  - 他人にID及びパスワードを教えない
  - 単純なパスワードにしない，定期的に変更する
- 無線LANのセキュリティ対策
  - 認証，暗号化
- ファイアウォールの導入
- 侵入検知システム(IDS)の導入

架空請求詐欺

- ワンクリック架空請求
  - アダルトサイトや出会い系サイトなどにパソコンや携帯電話からアクセスすると、いきなり料金請求の画面が表示される
- メールアドレスを知らせていないはずなのに、料金請求の、メールが届く
- パソコン使用時、数分おきに料金請求画面がでる

不正請求詐欺対策

- 慌てない
- 不用意に不正なサイトにアクセスしない
  - おいしい話には裏がある
- 基本的に無視
  - 問い合わせはしない
  - ひたすら無視！
  - 心配なら周りに相談する

■迷惑（スパム）メール

- 受信者の意向を無視して、無差別かつ大量に一括して送信されるメール
- 日本では大半がアダルト勧誘のURLが記されている
- フィッシング詐欺、ワンクリック不正請求を誘う等の悪質なメールも多い
- その他ねずみ講、マルチ商法、商品の販売間勧誘等
- HTML形式のメールにはWebビーコンが仕掛けられていることがある

迷惑（スパム）メール対策

- 迷惑メール対策ソフトの利用
- メーラーの迷惑対策機能の利用
  - イメージブロック機能の活用
- 本文中のURLは不用意にクリックしない
  - 配信停止等もクリックしない
- 絶対、返信はしない！基本的に無視！
- メールアドレスをむやみに公開しない
  - 画像で公開、@を他の文字に置き換える

ソーシャルエンジニアリング

- 話術や盗み聞き、盗み見などの「社会的」な手段によって、パスワードなどのセキュリティ上重要な情報を入手すること
  - 典型的な手法は、電話で情報を聞きだすこと
  - 上司やシステム管理者などになりすまして、パスワードや個人情報を聞き出す
  - オフィスから出る書類のごみをあさりパスワードや手がかりとなる個人情報を取得

ショルダーハッキング

- 肩越しに、他人が入力しているパスワードや暗証番号などを盗み見ること
  - ソーシャルエンジニアリングの手法の一つ
  - 電車の中でパソコン（携帯電話）を利用
  - 喫茶店で、大声で仕事の話をしていた
  - パソコンを開いたままトイレにいった

■ソーシャルエンジニアリング対策

- 重要書類の廃棄の際はシュレッダーにかける
  - ゴミ袋を複数に分けて廃棄，縦横カットが推奨
  - 名簿，アカウント一覧，IPアドレス一覧，ネットワーク構成等の書類は要注意
- 電話でパスワード等を聞かれた場合は本人確認を行う
  - 事前にルールを確認，パスワードは家族，友人にも教えない
- パスワード，クレジット番号等の入力時には周りに気を配る
- 座席を離れる場合はスクリーンロック，ログオフをする