サイバー犯罪 2021/6/11

# 情報セキュリティ論(9) サイバー犯罪 中野秀男 帝塚山学院大学非常勤講師 大阪市立大学名誉教授、堺市情報セキュリティアドバイザ

1

### 今日の話

- ▶ コンピュータ犯罪
- ▶ コンピュータウィルス
- ▶ 不正アクセスなどの事例
- 学会などでのシンポジウム
  - ▶ 電子情報通信学会、情報処理学会、白浜、越後湯沢、道後
- サイバー犯罪
  - ▶ 国/勢力と国/勢力との戦い:5軍
  - ト標的型攻撃(前回の講義)
- > 警察、裁判
- ▶ 犯罪に対する法律と判決
- ▶ サイバー犯罪で思うこと



情報セキュリティ論 サイバー犯罪 2021/6/11



帝塚山学院大学

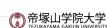
2

### コンピュータウィルス

- ▶ メールで添付ファイル(Excelやexe)が送れるようになった。
  - ▶ 1990年台前半にメールにMIME形式採用
- ▶ 最初はパソコンのデータ破壊
- 徐々にパソコンに住みついて
- ▶ 情報を外に出したり
- ▶ 遠隔から操作できるように
- ト Spyware や Adware
- Bot
- コンピュータやインターネットにある自動プログラム



情報セキュリティ論 サイバー犯罪 2021/6/11



3

サイバー犯罪 2021/6/11

### 不正アクセス等の事例(1) ► パスワードを盗る ► パソコン通信のマクロ ► メールサーバのセキュリティホール トニュースシステムのセキュリティホール ■ 踏み台攻撃 ■ 電話を調べモデムから侵入 ■ guest IDから管理者IDに入ってクラック ► トロイの木馬(古典的アタック)

1

### 不正アクセス等の事例(2)

- ▶ 電子メール爆弾と偽の発信者
- プロバイダからの偽りのメール
- ▶ デマの電子メール(hoax)
- ▶ SPAMメール(踏み台と大量DM)
- ▶「悪のマニュアル」
- ▶ クラッカーのホームページ



帝塚山学院大学

5

### 不正アクセス等の事例(3)

- ▶ WWWサーバのセキュリティホールをつく
- ▶ CGIのセキュリティ
- ▶ ファイル転送ソフトを使ったホームページの書き換え
- ▶ IE等のブラウザのセキュリティホール
- > ネットワーク・バザーでの売り逃げ
- ▶ 電子ショッピングの取り込み詐欺



情報セキュリティ論 サイバー犯罪 2021/

帝塚山学院大学

6

### 脆弱性攻撃 → バッファーオーバーフロー攻撃 → スニッフィング(パケットのキャプチャ) → DDoS攻撃(サービス不能) → ポートスキャン → パスワード・クラッキング → WEP(無線LAN)攻撃 → 市塚山学院大学 TEZURAYAMA CARUN UNIVERSITY TEZURAYAMA CARUN UNIVERSITY

7



8



q

サイバー犯罪 2021/6/11

### 情報セキュリティのシンポジウム

### > 学会

- ▶ SCIS: 電子情報通信学会
- ▶ 暗号と情報セキュリティシンポジウム(1984~)
- ▶ CSS:情報処理学会
  - コンピュータセキュリティシンポジウム



### その他のシンポジウム

- ▶ 白浜(1997~):サイバー犯罪に関する白浜シンポジウム
- ▶ 越後湯沢:情報セキュリティワークショップin越後湯沢
- ▶ 道後:情報セキュリティシンポジウム道後



10

### サイバー犯罪の特徴

- ▶ 遠隔地からの犯行
  - ▶ 例: 遠隔操作ウィルス(遠隔でかつなりすまし、または踏み台)
- ▶ 調査が難しい→アナログ犯罪より易しい?
- 訴追が難しい
  - ▶ 刑事事件につき検察官が
  - ▶ 公訴を提起し維持すること。
- ▶ 被害が甚大である
- ▶ 犯人の罪悪感が乏しい
- ▶ 処罰が軽い→みせしめの逮捕
- ▶ 愉快犯から特定目的、特定対象に
- ▶ コンピュータ犯罪からサイバー犯罪に





11

### サイバーテロ

- 重要インフラに対して、ネットワークなどを利用した電子 かな攻撃で、国民生活や社会経済活動に重大な影響を 及ぼす可能性のあるもの
- ▶ 低コスト、専門的知識、匿名、無痕跡
- ▶ 地理的制約なし、時間的制約なし
- ▶情報通信、金融、航空、鉄道、電力、ガス
- 政府・行政サービス



帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

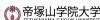
12

サイバー犯罪 2021/6/11

### サイバー犯罪の事例(1)

- ▶ 2007年4月:エストニア政府などへのウェブサイト攻撃
- ▶ 2008年8月:グルジア政府などへのウェブサイト攻撃
- ▶ 2009年7月:米国及び韓国の国防部を含む政府機関へ のウェブサイト攻撃
- ▶ 2009年I2月: Google社等への不正アクセス
- ▶ 2010年8月: イランのウラン濃縮制御システムがOSの脆 弱性を利用したウィルスに感染
- ▶ 2011年3月:韓国の国防部を含む政府機関へのウェブサ イト攻撃
- ▶ 2013年3月:韓国の複数の放送局や金融機関などの情 報システムへの攻撃

情報セキュリティ論 サイバー犯罪 2021/6/11

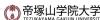


13

### サイバー犯罪の事例(2)

- ▶ 2012年8月: サウジアラビアのサウジ・アラコム社の3万 台に上るコンピュータがウィルスに感染
- ▶日本
- ▶ 2009年4月:政府機関などのウェブサイト改ざん
- ▶ 2011年9月:防衛関連企業への不正アクセス
- ▶ 2012年6月:裁判所や行政機関、大学病院などのウェブサイト への攻撃
- ▶ 2015年6月:**日本年金機構情報漏洩事件**

情報セキュリティ論 サイバー犯罪 2021/6/11



14

### 日本での体制

- ▶ サイバーセキュリティ戦略本部
  - ▶ NISC:内閣サイバーセキュリティセンター(2015年1月)
  - ▶ IT総合戦略会議、国家安全保障会議と緊密連携
- ▶各府省等
- ▶ 金融庁:金融機関
- ▶ 総務省:地方公共団体、情報通信
- ▶ 厚生労働省:医療、水道
- ▶ 経済産業省:
- ▶ 電力、ガス、化学、クレジット、石油
- ▶ 国土交通省:鉄道、航空、物流
- ▶ 文部科学省:セキュリティ教育



情報セキュリティ論 サイバー犯罪 2021/6/11



帝塚山学院大学

15

サイバー犯罪 2021/6/11

## 警察、検察、裁判所、弁護士 > 法律関係のプレイヤー > 警察 > 生活安全(局、課、係) - 検察 - 特捜 - 裁判所 - 裁判の判決は正しいか - 弁護士 - 逮捕されたら犯罪者のレッテルが - 有罪が確定するまでは - 情報セキュリティ論 サイバー犯罪 - 2021/6/11 - 市塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

16



17



18