

帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(7)  
ソーシャルアタック  
-特に標的型攻撃-

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ー


1 情報セキュリティ論 ソーシャルアタック 2020/6/19

1

今日の話

- ▶ 情報セキュリティの変遷
- ▶ 最近の情報セキュリティの考え方
- ▶ ソーシャルアタック
- ▶ 標的型攻撃
  - ▶ 定義と目的
  - ▶ 攻撃者
  - ▶ インシデント事例
  - ▶ ソーシャルエンジニアリング
- ▶ 標的型攻撃メール
- ▶ 参考にした本

▶ 2 情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

2

## 情報セキュリティの変遷

### ▶ 歴史的に

- ▶ 1980年ぐらいまでは暗号(慣用暗号)
- ▶ 公開鍵暗号の登場で電子署名などビジネスや暮らしに
- ▶ 1990年代のインターネットの普及でセキュリティが重要に

### ▶ 今

- ▶ 国や企業を狙ったインシデントが
- ▶ コンピュータ犯罪からサイバー犯罪へ
- ▶ 国と国などとのサイバー攻撃合戦(第5軍)
- ▶ 標的型攻撃/標的型攻撃メール



▶ 3

情報セキュリティ論 ソーシャルアタック 2020/6/19

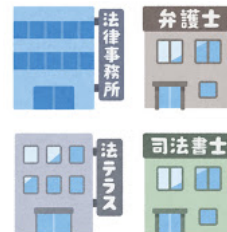


帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

3

## 最近の情報セキュリティの考え方

- ▶ セキュリティ原理主義者に対して
- ▶ IT/ICTを最大限に使うためのセキュリティ
  - ▶ 投資
  - ▶ それ以上は犯罪という切り分け
- ▶ プライバシは世界の流れも
  - ▶ 米:トラッキング禁止(Do Not Track)
  - ▶ 欧:忘れてもらう権利(Right to be forgotten)
    - ▶ →消去権
  - ▶ IT/ICTも世界のレベルで動いている
- ▶ 法律がIT/ICTに追付いてきた
  - ▶ 有罪と無罪を切り分ける法律と裁判
- ▶ IoT時代のセキュリティ



▶ 4

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

4

## ソーシャルアタック

- ▶ ソーシャルアタック
  - ▶ 個人へのアタック
  - ▶ ソーシャルメディアツールを使ったアタック
- ▶ ショルダーアタック
  - ▶ パスワードや暗証番号やスマホのパスコードの覗き見
- ▶ 偽の電話やメール(標的型メール)
  - ▶ 個人情報を聞く
- ▶ ソーシャルエンジニアリング
  - ▶ 情報収集
  - ▶ 誰かになりすます



▶ 5

情報セキュリティ論 ソーシャルアタック 2020/6/19



5

## 標的型攻撃(1)定義と目的

- ▶ 組織はそこそこ強くなったので、まず弱い個人から攻めよう
- ▶ 定義
  - ▶ 明確な意志と目的をもった人間が、特定のターゲットに対して、特定の目的で行う、サイバー攻撃の一種
  - ▶ 欧米ではAPT(Advanced Persistent Threat)
- ▶ 目的
  - ▶ 政治的活動(Anonymous, WikiLeaks)
  - ▶ サイバー犯罪
  - ▶ サイバーテロ
  - ▶ サイバー戦争(サイバー空間は第5の戦場)
  - ▶ 業務妨害(DDoS攻撃によるサーバ停止)
  - ▶ 政治的駆け引き
  - ▶ 個人的な動機による攻撃



▶ 6

情報セキュリティ論 ソーシャルアタック 2020/6/19



6

## 標的型攻撃(2)目的(続)

- ▶ **サイバー犯罪**
  - ▶ オンラインバンクを利用しての不正送金
    - ▶ 最近は二重認証の方向へ
  - ▶ フィッシング詐欺
  - ▶ ランサムウェア(Ransomware)による脅迫:身代金ウイルス
  - ▶ 個人情報の売買
  - ▶ DDoS攻撃
- ▶ **個人的な動機による攻撃**
  - ▶ 愉快犯
  - ▶ 恨みつらみ
  - ▶ サイバーストーカー



▶ 7

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

7

## 標的型攻撃(3)攻撃者

- ▶ **政府、軍関係者**
- ▶ **民間企業**
  - ▶ アングラ企業
  - ▶ ライバル会社を攻撃
- ▶ **マフィア、反社会勢力**
- ▶ **学生**
- ▶ **その他**
  - ▶ ネットストーカー
  - ▶ 上司や女性社員のPCにRAT(遠隔操作ツール)



▶ 8

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

8

### 標的型攻撃(4)インシデント事例と標的型メール

- ▶ RAT(遠隔操作ツール)がPCに
  - ▶ メールやメッセージのURLのクリックで
  - ▶ 届いたUSBをPCに
- ▶ 標的型メール
  - ▶ 個人情報の収集
    - ▶ Facebook, Twitter, 検索エンジンで写真、住所、勤務先情報を
  - ▶ 攻撃するPCが標的
  - ▶ RATを組み込ませる
  - ▶ パスワードやアドレス帳などを入手
  - ▶ 接続元の隠蔽工作
  - ▶ 破壊



▶ 9

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

9

### 標的型攻撃(5)ソーシャルエンジニアリング

- ▶ 狙われる情報
  - ▶ 氏名
  - ▶ メールアドレス
  - ▶ 会社名
  - ▶ 役職
  - ▶ 人間関係
- ▶ 「なりすましメール」
- ▶ SNSやウェブから情報を



▶ 10

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

10

## 標的型攻撃(6)標的型メール

### ▶ 実体

- ▶ 業務連絡を装ったメール
- ▶ 取引先を装ったメール
- ▶ 冠婚葬祭を装ったメール
- ▶ 時事ニュースを装ったメール
- ▶ 人材募集を装ったメール
- ▶ グリーティングカードを装ったメール



### ▶ 不正プログラムの実行

- ▶ 添付ファイル
- ▶ URLのクリック(不正サイトへの誘導リンク)

▶ 11

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

11

## 参考にした本

- ▶ 「標的型攻撃/セキュリティガイド」岩井博樹(ラック)
  - ▶ Softbank Creative, 2013年3月
- ▶ 「ソーシャル・エンジニアリング」Christopher Hadnagy
  - ▶ 日経BP, 2011年



▶ 12

情報セキュリティ論 ソーシャルアタック 2020/6/19



帝塚山学院大学  
TEZUKAYAMA GAKUIN UNIVERSITY

12