まちがえ、だまされ、事故になる

人間の信頼性をどう考えるか

産業技術総合研究所

セキュアシステム研究部門　主任研究員

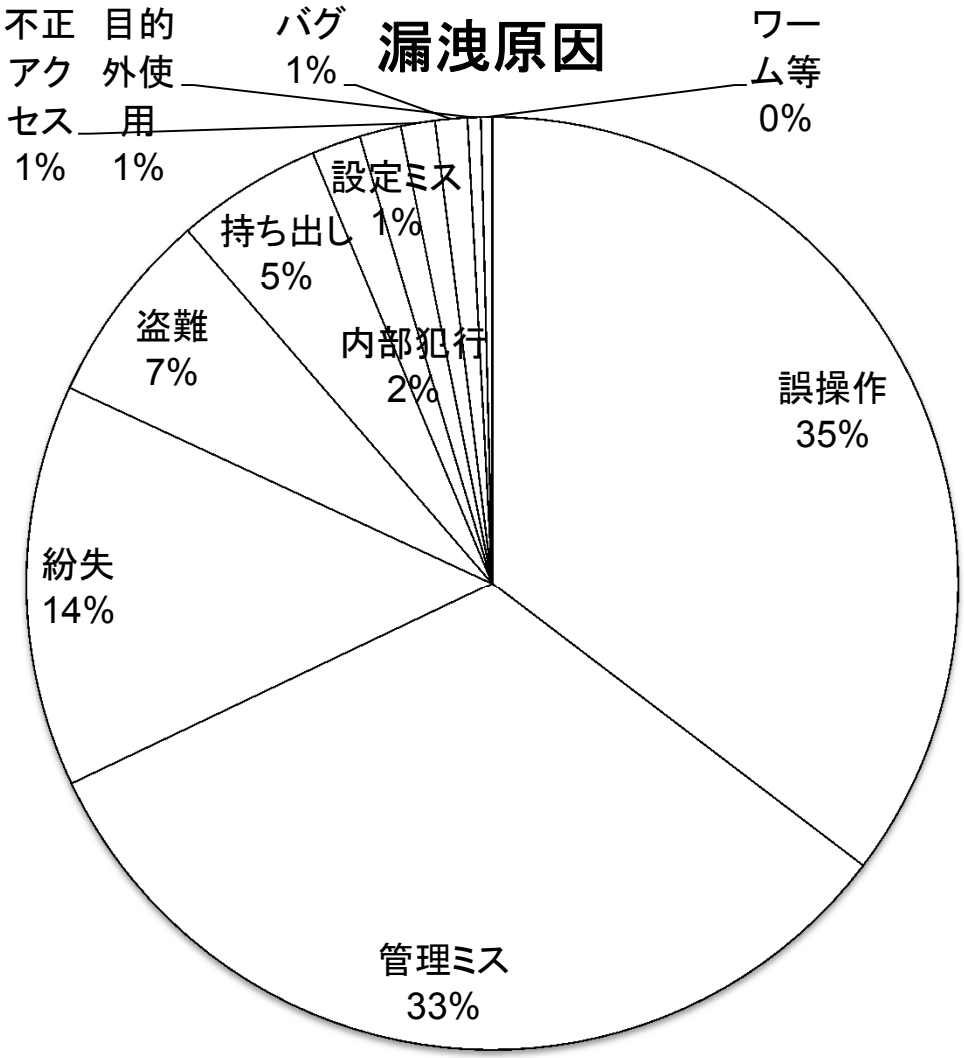
中田　亨

toru-nakata@aist.go.jp

これぞ深刻な脆弱性

- TX Overflow
- Nozomi Overflow
- Yamanote line Overflow

情報漏洩　最大の穴は「人間」

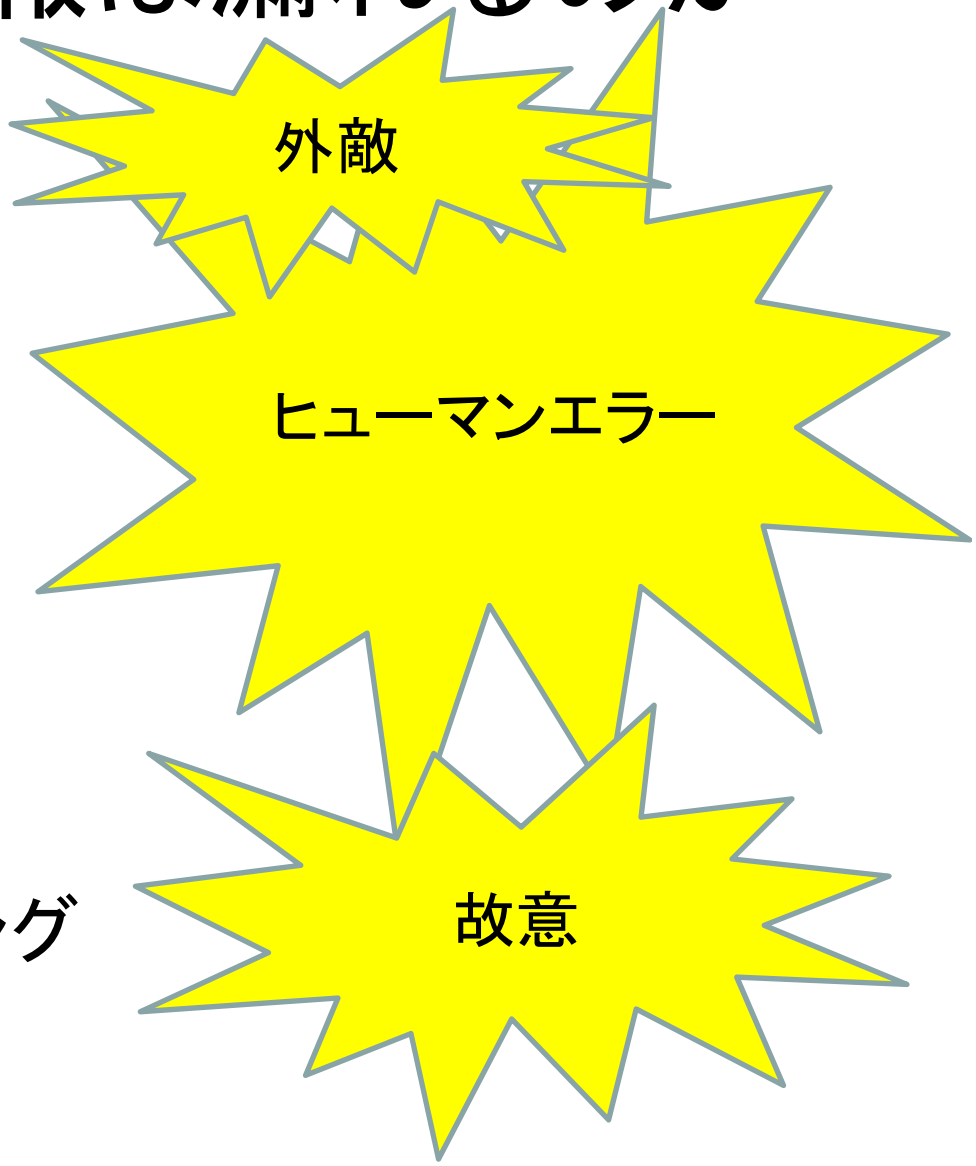


(出典：JNSA, 2011年情報セキュリティインシデントに関する調査報告書　個人情報漏えい編)

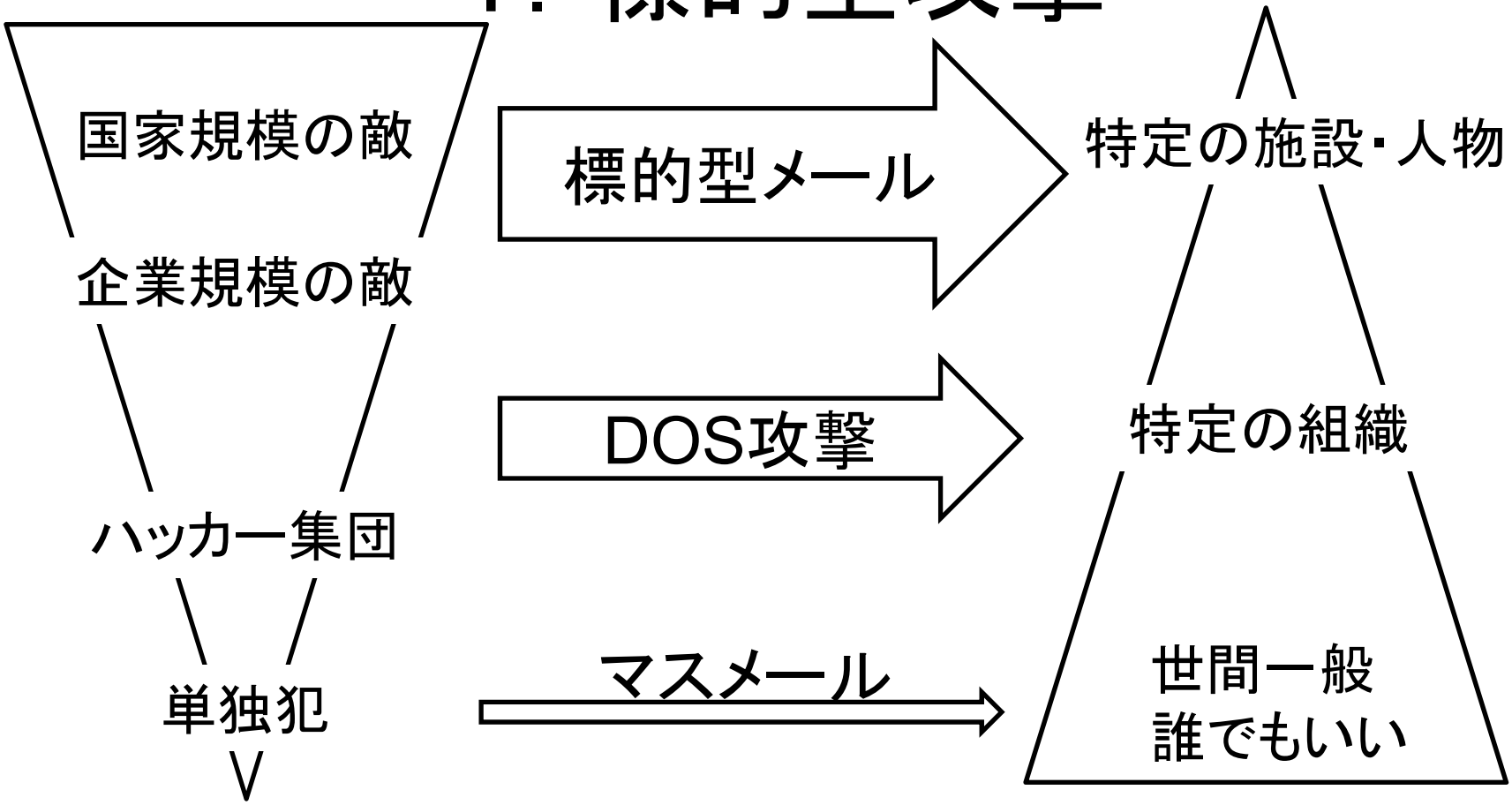
- 個人情報漏洩では、人為ミス系が圧倒的に多い
- 他のセキュリティ事故でも大半は人間のミスが原因

どのように情報は漏れるのか

- 標的型攻撃
- 情報持ち出し、紛失
- 誤送付
- 内部犯行
- ソーシャルネットワーキング(SNS)で漏らす



1．標的型攻撃



- 「敵」が巨大化している。
  - 国の基幹が標的化
- 攻撃も洗練化：流暢な日本語メール

標的型攻撃のやり方：心理戦

- 急ぎ助けて型
  - 「至急、おたくの課の〇〇さんからのファイルのパスワード教えて！」
- にせ警官型：安全の権威者のふりをする
  - 「情報セキュリティ本部です。添付を開いて報告しなさい」
  - 帝銀事件、三億円事件
- 薄味型：どうでもいい内容で警戒させない。
  - 「駐車場の車のランプが点いてます。詳しくは添付を」
  - 一番強力であるらしい。

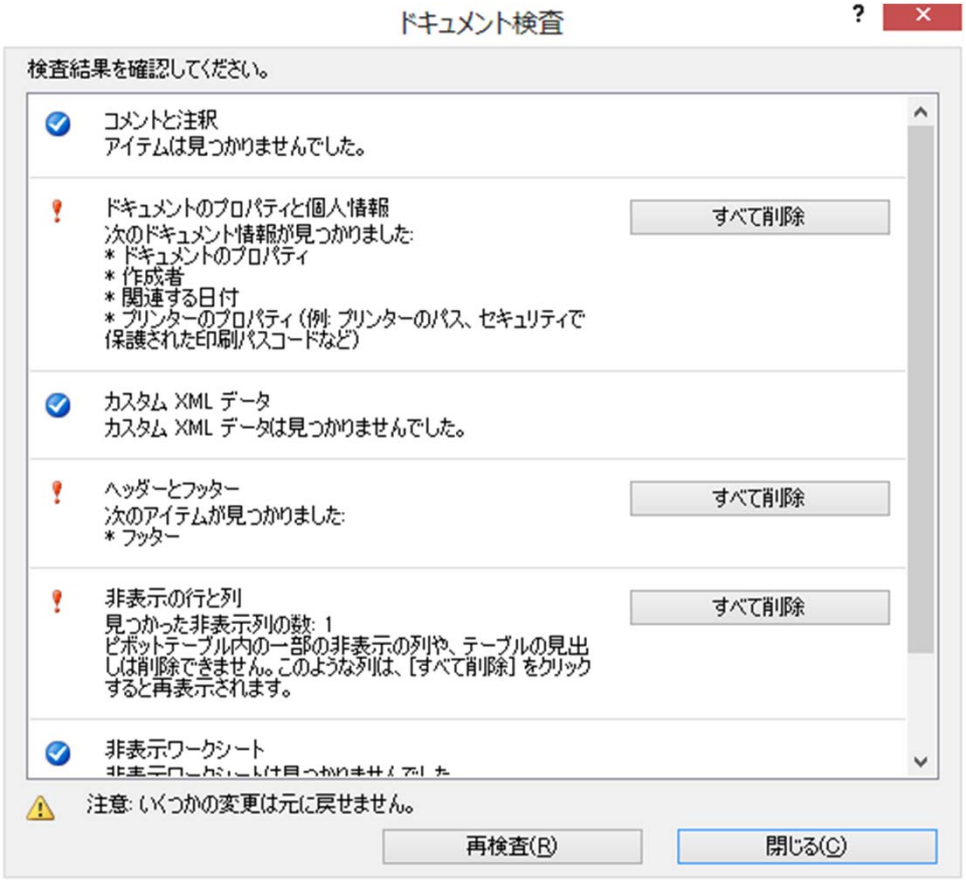
「注意力不足」というより「注意力抑制手口」

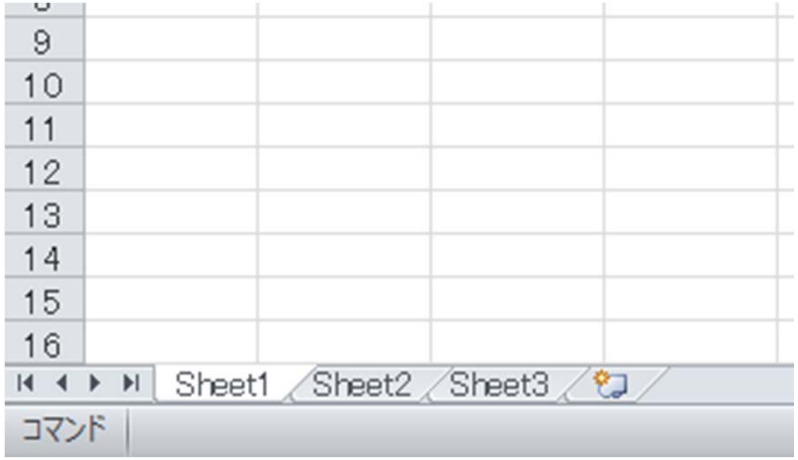
標的型攻撃を防ぐには？

- 装置的な対処：
  - フィルタリング、警告発出、exeファイル自動除去

  - 古くさい風習：「表を書くぞ！」→「ならエクセルだ！」→「マクロだ!」
- 人員的な対処
  - 教育：一度実際にひっかける「ワクチン」訓練。エクセルよりワードを使え。
  - 体制：必要最小限の人にだけ情報を扱わせる

誤送信、消し忘れ





↑エクセルの２枚目以降があぶない

←ワードの無駄情報掃除

- ファイルはひな形を用意せよ
- 前の仕事のファイルを使いまわすな。
  - 何かが残存しているぞ

“誤送神”は恐ろしい

- 9.11テロ実行犯に、事件後にビザ発給さる
- 紺屋の白袴

特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

メール誤送信に関するお詫びとご報告

このたび、当協会事務局において、セミナーに参加された方々に対し誤ったファイルを添付したメールを送信いたしました。
関係者の皆様に多大なご迷惑とご心配をお掛け致しましたことを深くお詫び申し上げます。

本件に関する経緯及び対応について、以下のとおりご報告申し上げます。

■誤送信した情報
当協会が開催しました「中小企業向け指導者育成セミナー」の受講者579名のメールアドレス一覧を記載したCSVファイル。
記載していたのはメールアドレスのみです。

■経緯
2014年2月14日　11時14分　「中小企業向け指導者育成セミナー」の受講者の内1562名にアンケートを添付し

送信する前、した後に

- する前：入念な確認が必要
  - 宛先、本文、添付ファイル
    - しかし、英字のメアドは確認しにくい
  - 無理をするな。古い手を使うな。
    - ×「BCCで一斉送信」
    - ×「ファイル輸送はなんでもメールで」
    - ×「宛名はオートコンプリートで」（新しい手だが毒）
- した後：送信取り消し機能も取り入れよう
  - 数十秒は保留待機する機能
  - 旧式のメールソフトは退役を

内部犯行

- 換金目的
  - 通販会社顧客データ漏洩事件(2004)
- 会社への対抗手段として秘密の持ち出し
  - 映画「エリン・ブロコビッチ」
- 正義感
  - スノーデン事件(2013)、外交公電Wikileaks 事件(2010)
- 自分のため
  - シマンテック社Ponemon 社共同調査(2009)
  - 退職者の53%が、退職前に社内の情報を持ち出していた
  - 82%は、情報管理について上司による監督や検査を退職前に受けず
  - 24%は、退職後も会社のシステムに入ることができた

SNSで漏らす

- 職務上の秘密を漏らす
  - 鑑識課警察官FB投稿 (2012)
- 社内・自分の不祥事を漏らす
  - 製薬会社員薬不正使用TW投稿(2011)
  - 飲食業従業員による不謹慎TW投稿は多発
- 問題になるとは認識せずに漏らす
  - ホテル従業員TW投稿「有名人がお泊りデートだ」(2011)

戦前の軍機保護法違反の例

- 軍港の詳細な図面を不法所持
  - 限られた人しか図面を見られない。
  - 不便なので、コピーを作り、関係者に配布。
  - コピーの入ったカバンを紛失。警察が発見。
- 基地建設現場を第三者に案内し詳説
  - 建設会社社長、同業者を工事に参画させたくて案内。

- ところで、この捜査情報がなぜここに、、、？

認識のズレは恐ろしい

		情報の読み手（部下）の見解	
		「この情報は重要である」	「この情報は重要ではない」
情報の持ち主（上司）の見解	「この情報は重要である」	【戸締りされた扉】 この情報は財として扱われる。	【噂の扉】 この情報は流出する。
	「この情報は重要ではない」	【ガラス張りの扉】 この情報は無断利用される。	【出入り自由の扉】 この情報は分析技術が開発されるまでは活用されない。

不一致の扉で情報の漏洩・盗難が起こる

誓約書：先に署名が（なぜか）効果的

署名：山田太郎
私は下記を誓います

- 私用メールはしません
- USBメモリは持ち込みません。
- 個人情報ファイルは登録し、所定のパスワードをかけます。

- 私用メールはしません
- USBメモリは持ち込みません。
- 個人情報ファイルは登録し、所定のパスワードをかけます。

私は上記を誓います
署名：山田太郎

まとめ：対策の刷新を

- 情報大漏洩時代が来た
  - プロによる攻撃
  - 漏れやすい道具の普及（スマホ）
  - 漏れるルートの普及（SNS)
- モノの対策
  - 定型的な事故には、対処手段が既にある
- 人材の対策
  - 不定形な事故には、リスク観・価値観の一致が必要
  - 「初期設定・無防備はオカシイ」という感覚を
- ポリシーでの対策
  - ある程度は不効率を我慢する時代に
  - 可用性と堅牢性のバランスを選択する、全社的合意を
    - 「誰でもファイルを見られる」で良いか？
    - パスワードは我流で作成・伝達・廃棄で良いか？