


最近のサイバーセキュリティ情勢と デジタル・フォレンジック



情報理工学部情報システム学科
サイバーセキュリティ研究室
デジタル・フォレンジック研究会副会長
上原哲太郎

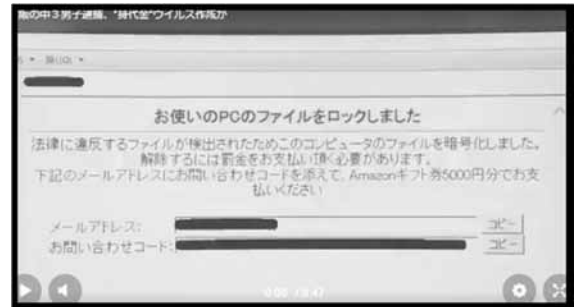


我々の情報は狙われている
常に火消しに走っているが
限界を超えている感覚

最近も大騒ぎがありました...

➤ WannaCryワーム

➤ 14歳が作った
ランサムウェア



これらのように騒ぎになるものは
技術的にはそれほど高度ではない
本当に怖いものは表に出ない

R

多様化する攻撃者像

愉快犯 思想犯

技術誇示目的

思想信条の表現

「集団暴走」

明確な目的

怨恨

金銭目的

破壊工作・諜報
そしてその演習？

R

最近メインは「金銭」「諜報」の様



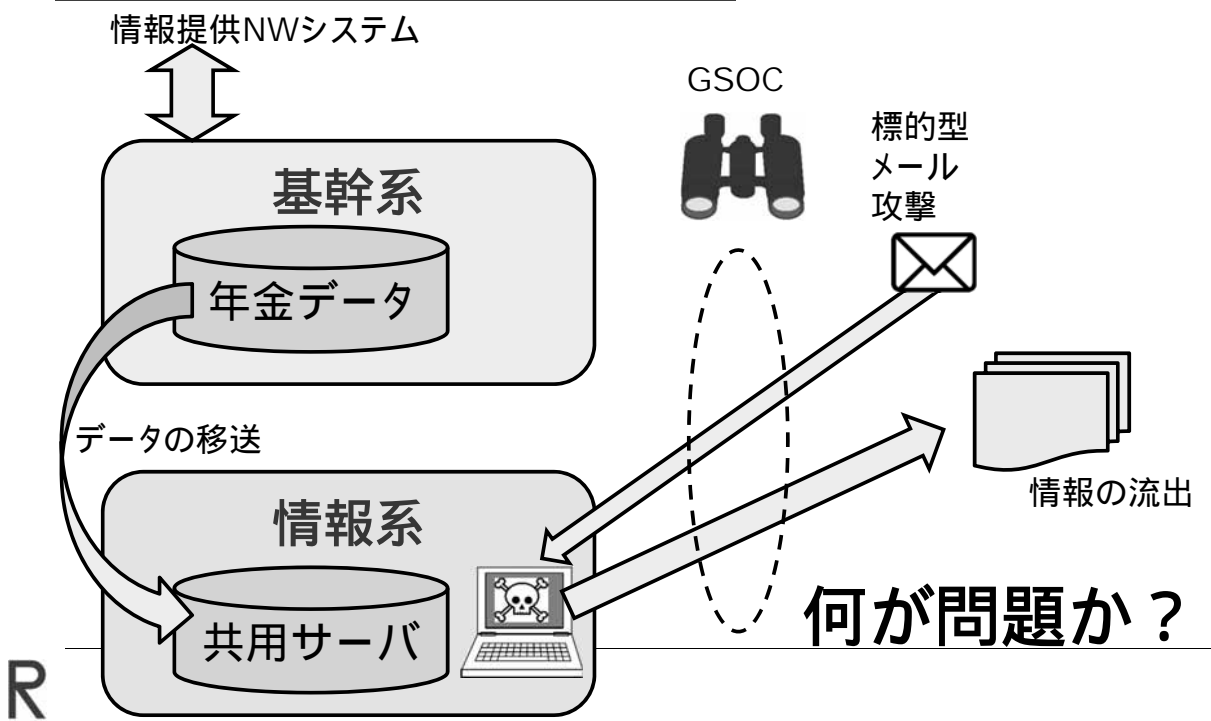
厄介な「標的型攻撃」

- 手口にはパターンがあるとはいえ多彩
 - メール、水飲み場、クラウドサービス...
- マルウェア対策があまり役立たない
 - パターンファイル系は無理
 - ふるまい検知は精度が課題

➤ 「成功するまで諦めない」

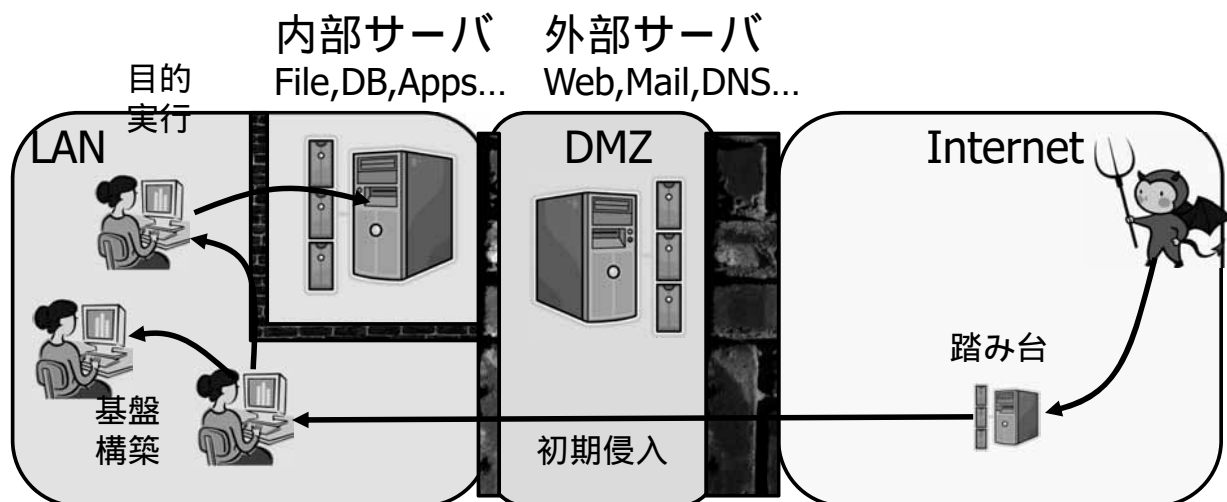
R

年金機構事件の大きな構図



R

結局このパターンは相変わらず...



情報収集 初期侵入 基盤構築 内部調査 攻撃先特定 目的実行

R

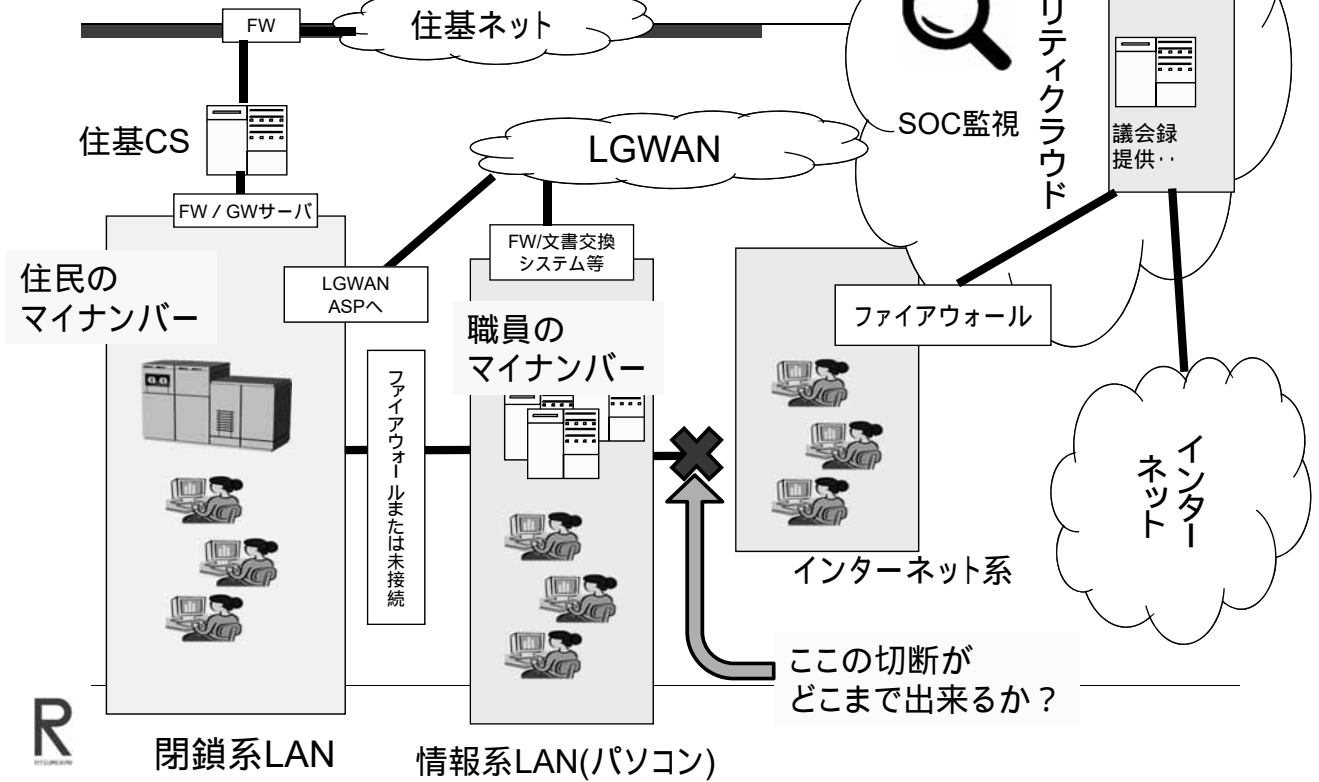
もう10年以上、この手口であらゆる情報が盗まれてきた

さすがにメールは限界ではないか？

- メールに対するさまざまな対策はあるが...
 - 発信者認証(DKIM/SPF、DMARC、S/MIME)
 - 普及に課題・UI変更や教育も課題
 - メール向けマルウェア対策
 - 特にサンドボックス製品のコストが課題
 - 添付ファイル「無害化」
 - コスト・作業効率の問題
- メールを使わない方が実は楽では？
 - ファイルのクラウドストレージを介した交換
 - 事実上の発信者認証の徹底
 - 別のメッセージング手段の確保

R

自治体は「城壁」を築いた = 「強靱化」



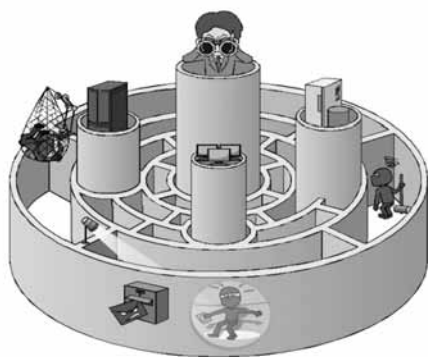
自治体情報セキュリティ強靱化モデル

- LANを基本的に三階層に分けよ
 - 住民の個人番号を扱う「基幹系システム」(A)
 - 基本的な業務を担う「情報系システム」(B)
 - インターネット直接接続の「解放系システム」(C)
- (A)と(B)の間をはっきりさせよ
- (C)は他と基本的に切り離せ
 - ただし一部データは「無害化」させて(B)へ移送可
- インターネット側の共同化を進めよ
 - 「セキュリティクラウド」計画
- インターネット側を常時監視せよ

「監視」による早期発見を中心とした対策： IPA「高度標的型攻撃」対策ガイド

「高度標的型攻撃」対策 に向けたシステム設計ガイド

～入口突破されても攻略されない内部対策を施す～



IPA 独立行政法人情報処理推進機構
セキュリティセンター

2014年9月

R

ポイントは
「侵入されないこと」
ではなく
「侵入されたことを
発見しやすい」
「侵入されても被害が
大きくなりにくい」
システムにすること

監視体制構築が課題

誰がやるの？

2017.5.28 産経新聞関西版

- 「中小向けサイバー攻撃対策 今秋にも
24時間体制の安価サービス NTT西」
 - NTT西日本が中小企業向けに、コンピューターシステムへの高度なサイバー攻撃を24時間体制で遠隔監視し、被害発生時には駆けつけて原因を突き止めるサービスを開発していることが27日分かった。(中略)NTT西は月10万円以下での提供を目指し、資金力の乏しい企業でも手が届くようにする。

今後この種の「安価な」監視サービスは増える！

しかし、監視後の「駆けつけ」は時間勝負ですよ？！

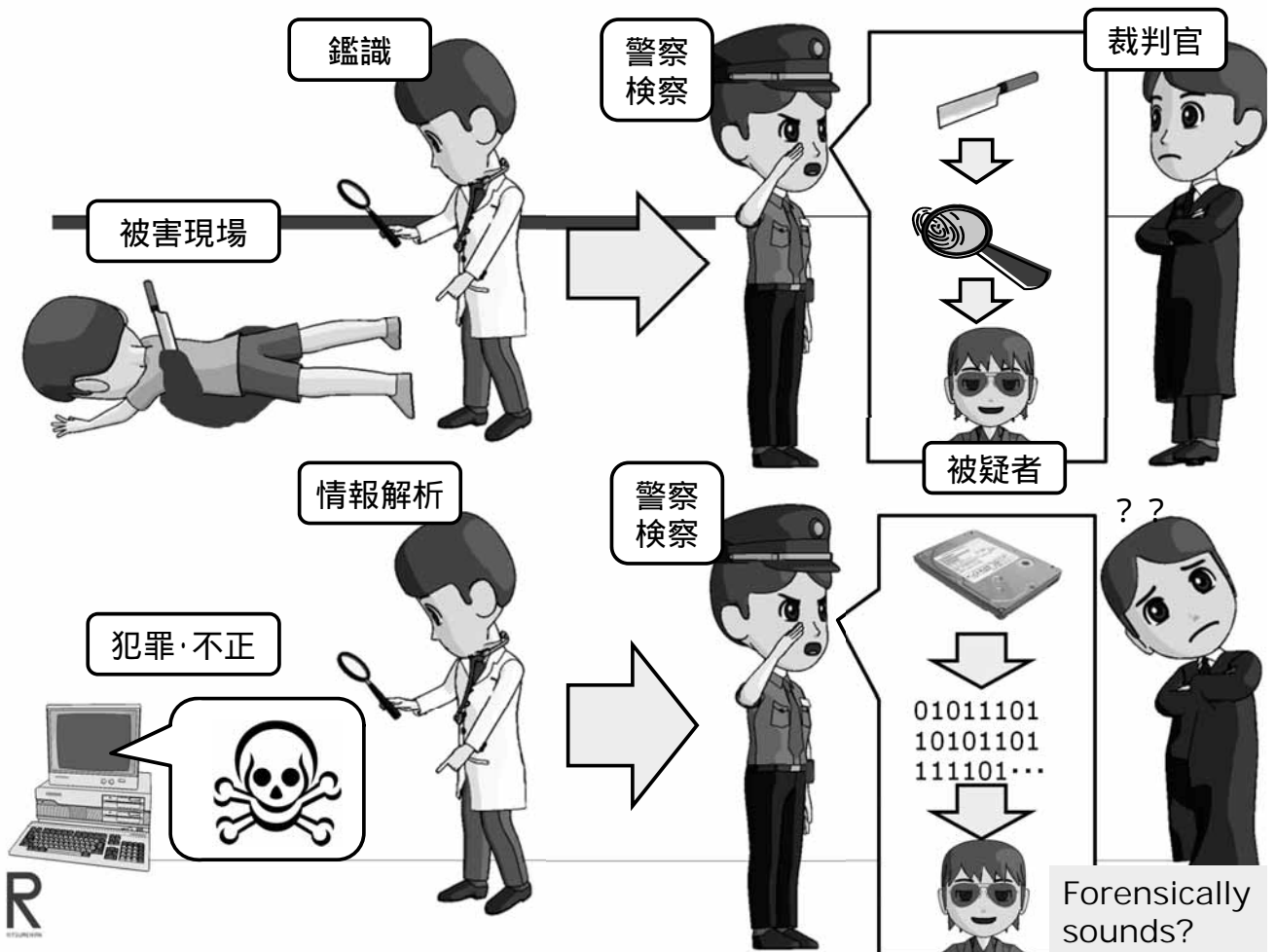
R

デジタルフォレンジックとは何か



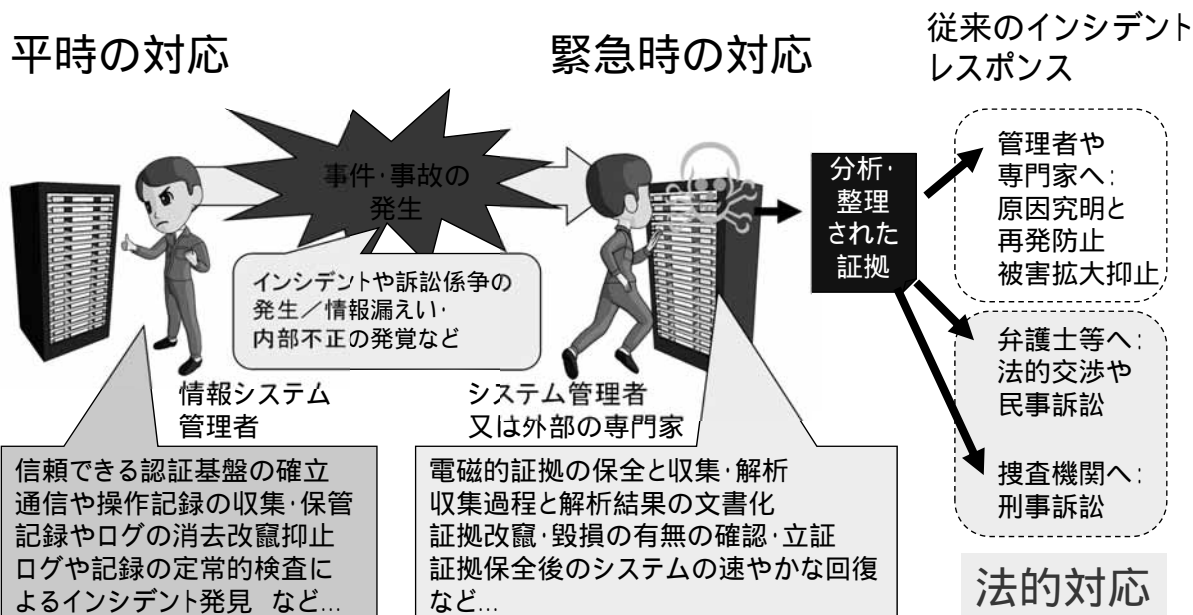
- Forensic Medicine = 法医学
Forensic Chemistry = 法化学
Digital Forensics = 情報法科学・デジタル鑑識
- 警察的な文脈ではいかにIT機器を『鑑識』して『電磁的証拠(e-Evidence)』を見つけ出すか
その『電磁的証拠』をいかに解析するか
 - 民間の文脈では組織内不正調査のための鑑識以外に、その予防策としての『記録保持』を含む
- 初動捜査では極めて重要
- ネットやPC、デジタル機器が絡むと必要

R



R

システム管理者にとっての デジタルフォレンジック



R 監視と分析はアウトソーシングできるが証拠保全は時間との戦い

だから証拠保全が大切なんだけど...

- 企業は「ファーストレスポンド」を置かないと...
 - 証拠保全できない結果、事故の詳細が失われる
 - 事故報告義務がある業種では詳細不明になれば「そもそも適切に管理されていたのか？」が問われる
- その危機感が共有できるか？
 - そのためには「証拠保全がどう役立つのか」の情報の共有が必要
 - 「情報漏洩の内容」はどう調査されるのか？
 - 適切なログがあればどのように役立つのか？