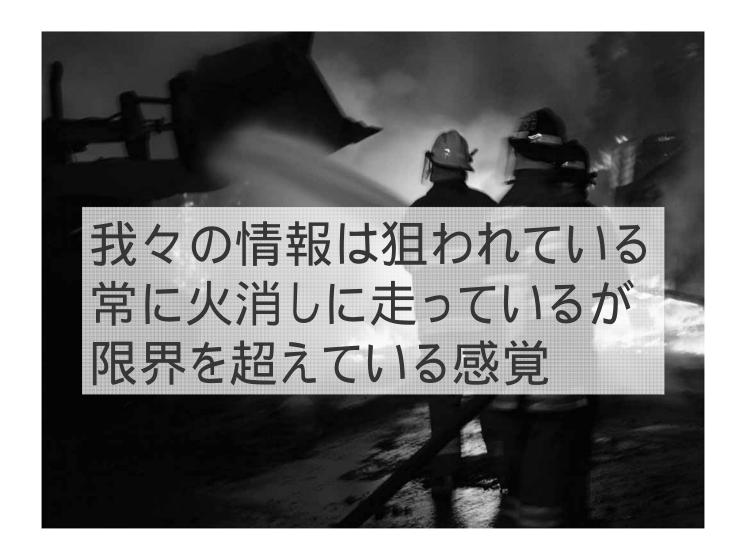
最近のサイバーセキュリティ情勢と デジタル・フォレンジック

RITSUMEIKAN

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



まずは現状を知る

- ▶ 情報セキュリティ10大脅威
 - ▶ (独)情報処理推進機構IPAが 毎年春に公表
 - ▶ 専門家の意見をまとめ 前年度起きた事件より 現状の脅威をまとめている
- ▶ 10年以上発刊されている 変遷を知るのに良い



R

結局マルウェア対策が最重要

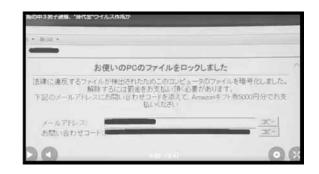
/	2006年版	2007年版	2008年版	2009年版	2010年版	2011年度	2012年版	2013年版	2014年至	2015年版	2016年至	2017年版
N	2006/3/22	2007/3/9	2008/5/27	2009/3/24	2010/3/31	2011/3/24	2012/3/22	2013/3/12	2014/3/31	2015/4/3	2016/4/27	2017/5/3
ı	「加速する経済事件化」と 今後の対策	脅威の"見えない化"が加速する!」	ますます誰む「見えない化」	攻撃手法の「多様化」が進 む	あぶり出される組織の器 点!	進化する攻撃 その対策で十分ですか?	変化・増大する脅威!	身近に思び寄る脅艦	推嫌化する情報セキュリ ティ あなたが直面している のは?	被害に遭わないために実 施すべき対策は?	個人と組織で異なる発症。 立場ことに適切な対応を	職場に迫る脅威! 家庭 に迫る脅威!? 急がは れの心構えてセキュリティ 対策を
2	http://www.ios.at.io/sequelte/sr uln/20050322 Websteamer.ht tsl		Thirthy / years, inc. go in/ second by y	http://www.ine.es.io/securits/y uln/10thrests2009.html	http://www.inces.in/securits/s uln/10thrests2010.html	tota//occasio/sessib/y uln/10thrests2011.html	http://www.iou.eu.io/securitu/v uln/10throsts2012.html	http://www.ios.as.io/securits/y uin/10thrests2012.html	http://www.ine.as.in/security/s uln/10thrests2014.html	http://www.ios.ss.io/securits/y uln/10thrests2015.html	http://www.ios.so.co/seconto/y uln/10th/esta9015.html	Mtsc://emits.zoio/secu u/win/10thmats2017.html
œ	事件化するSQL インジェ クション	施えい情報のWineyによ る止まらない流通	高まる「誘導型」攻撃の 脅威	DNSキャッシュボイズニン グの脅威 (組織への脅威:1位)	変化を続けるウェブサイト 改さんの手口	「人」が起こしてしまう情 軽温えい	機密情報が追求れる!? 新しいタイプの攻撃	クライアントソフトの 最弱性を実いた攻撃	推的型メールを用いた組織への スパイ・諸権活動	インターネットパンキング やクレジットカード情報の 不正利用	インターネットパンキング やクレジットカード情報の 不正利用	様的型攻撃による情報 進出
Q	Winny を通じたウイルス 感染による情報漏えいの 多発	表面化しづらい程的型 (スピア型)攻撃	ウェブサイトを狙った攻撃 の広まり	多様化するウイルスや ボットの感染経路 (利用者:1位)	アップテートしていないクライアントソフト	止まらない!ウェブサイト を経由した攻撃	予測不能の災害発生! 引き起こされた業務停 止	禮的型諜報攻撃の脅艦	不正ログイン・不正利用	内部不正による情報器 えい	様的型攻撃による情報 進出	ランサムウェアによる被 書
Q	音楽CD に格納された 「ルートキットに類似した 機能」の事件化	閲覧化・潜在化するポット	個常化する情報調えい	正規のウェブサイトを経 由した攻撃の猛艦 (管理者/開発者:1位)	悪質なウイルスやボット の多目的化	定番ソフトウェアの撤退 性を狙った攻撃	特定できぬ。共通思想 集団による攻撃	スマートデバイスを狙った 悪意あるアプリの横行	ウェブサイトの改ざん	様的型攻撃による環接 活動	ランサムウェアを使った 詐欺・恐喝	ウェブサービスからの個 人情報の高取
æ	悪質化するフィッシング詐欺	謝別化するセロティ攻撃	巧妙化する機能型攻撃	巧妙化する間的型攻撃 (難機への背叛:2位)	対策をしていないサーバ 製品の機器性	着われたしたスマートフォン	今もどこかで… 更新されのクライアントソフト を扱った攻撃	ウイルスを使った道場操作	ウェブサービスからのユーザー 情報の輩えい	ウェブサービスへの不正ログイ ン	ウェブサービスからの個人情 報の復取	サービス妨害攻撃によるサー ビスの停止
æ	汚物化するスパウェア	ますます多様化するフィッシン ク計数	住用できなくなった正規サイト	機能な無機に料略等方式に おける発揮 (利用者:2位)	あわせて事後対応を!強軽 能力い事件	複数の攻撃を組み合わせた 「新し4ウイブの攻撃」	止まらない!ウェブサイトを 狙った攻撃		オンラインパンキングからの不 正送金	ウェブサービスからの副客情 相の信敬	ウェブサービスへの不正ロタイ ン	内部不正による情報避えい それに伴う業務停止
a	進行が被くボント	増え続けるスパムメール	検知されにくいボット、潜在化 するコンピュータウイルス	頭導型攻撃の間在化 (管理者/開発者:2位)	被害に至づけない極的型攻撃	セキュリティ対策不確かもたら すトラブル	組々発覚、スマートフォンやタ ブレットを扱った攻撃	予期せぬ業務停止	思意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ	ウェブサイトの改ぎん	つエブサイトの改ぎん
Œ	ウェブサイトを着うだSSFの進行	減らない情報雑念い	技能エンジンからマルウェア 配位サイトに誘導	保管化する情報遅れい (経典への発展:3位)	服制4006电影	携帯電望向けウェブサイトの セキェリティ	大丈夫!?電子提明書に終 なぬ強し穴	ウェアサイトを狙った収撃	SNSへの概率な情報公開	ウェブサイトの改ぎん	審査をおり掛け会式マーケンド に始れ込んをスマートフェンア プリ	ウェブサービスへの不正のグ イン
Q	情報家司、携帯機器などの様 込みソフトウェアにひそむ聴覚 性	狙われ続ける安易なハスワード	国内製品の概報性が研究	減らないスパムメール (利用者:3位)	正規のアカウントも悪用される 背板	攻撃に気づけない他的型攻 撃	身近に弾む間の手・・・あなた の機能は大丈夫?	バスワート進出の脅威	始失や效定不備による情報 輩えい	インターネット基盤技術の悪 用	内部不正による情報量丸いと それに伴う業務停止	bT機器の機器性の存在化
ü		攻撃が急性するSQLインジェ ウンsン	減らないスパムメール	接込み製品に禁む開発性 (管理者/開発者:3位)	クラウド・コンピューティングの セキュリティ問題	クラウド・コンピューティングの セキュリティ	意ない!アカウントの使いま わしが被害を拡大!	内部犯行	ウイルスを使った詐欺・助 喝	職員性会長に伴う攻撃	巧妙・悪質化するワンクリック 請求	攻撃のビジネス化 (アンターグラウンドサービス
唯	ゼロデイ攻撃	不適切な設定のCNSサーバを 扱う攻撃の発生	組み込み製品の職務性の様 加	ユーザDとバスワードの使いま わしによる危険性 (利用者:4位)	インターネットインフラを支える プロトコルの範囲性	ミニブログサービスやSNSの利 用者を扱った攻撃	利用者情報の不適切な取扱 いによる使用失機	フィッシング哲教	サービス妨害	悪意のあるスマートフォンアブ リ	職器性対策情報の公開に伴 い公知となる職器性の感用増	インターネットパンキングやクレジットカート情報の不正利

最近も大騒ぎがありましたが...

WannaCryワーム



14歳が作った ランサムウェア



R

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

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?



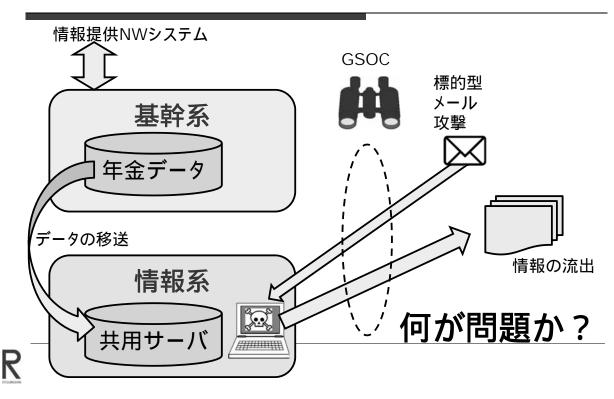
厄介な「標的型攻撃」

- ▶ 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

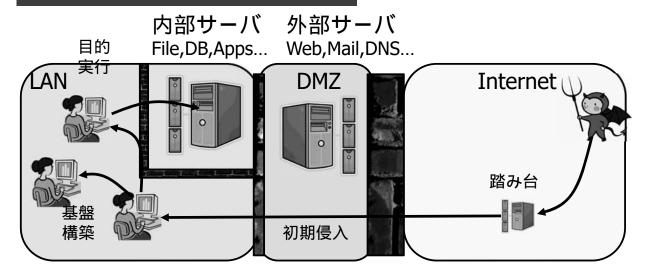
▶ 「成功するまで諦めない」

R

年金機構事件の大きな構図



結局このパターンは相変わらず...



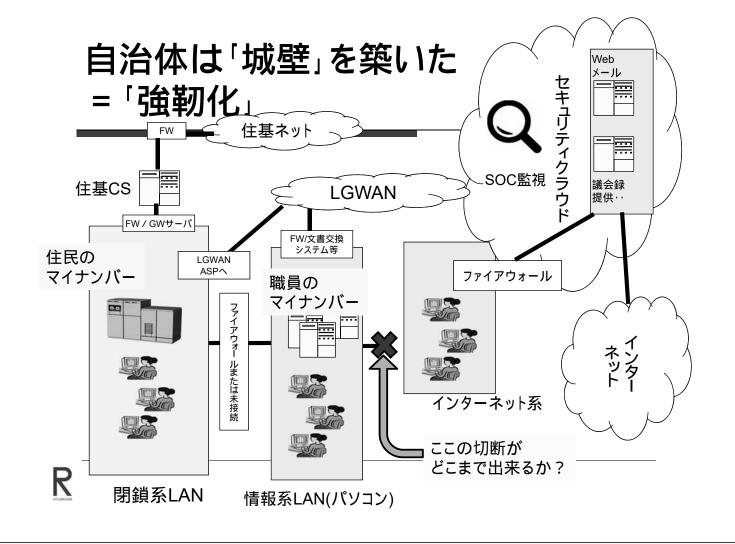
情報収集 初期侵入 基盤構築 内部調査 攻撃先特定 目的実行

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



自治体情報セキュリティ強靭化モデル

- ➤ 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



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?

R

2017.5.28 產経新聞関西版

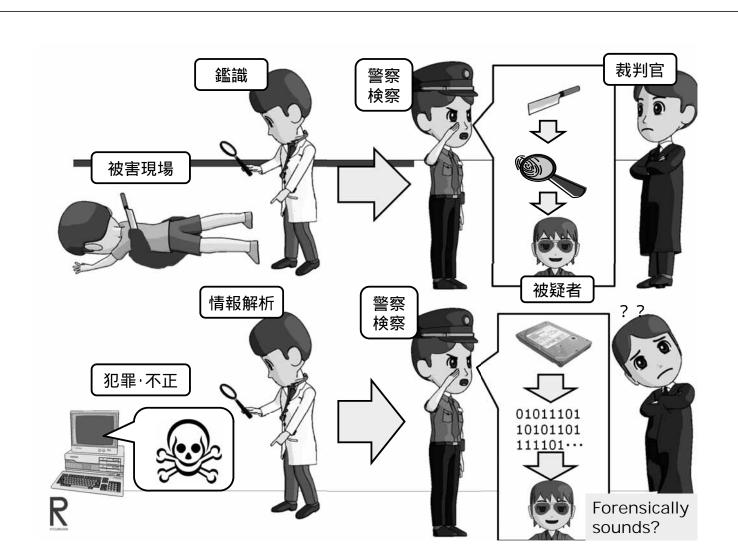
- ▶「中小向けサイバー攻撃対策 今秋にも 24時間体制の安価サービス NTT西」
 - ▶ NTT西日本が中小企業向けに、コンピューターシステムへの高度なサイバー攻撃を24時間体制で遠隔監視し、被害発生時には駆けつけて原因を突き止めるサービスを開発していることが27日分かった。(中略)NTT西は月10万円以下での提供を目指し、資金力の乏しい企業でも手が届くようにする。

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?!

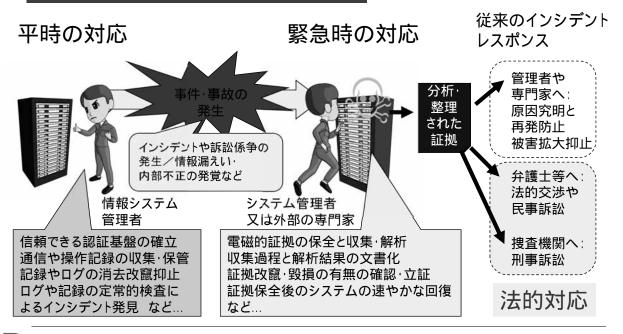
デジタルフォレンジックとは 何か

- Is blof swifelchen in recobing whose with the series in the second series of the serie
- ➤ 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



システム管理者にとっての デジタルフォレンジック



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のだけど...

- ▶ 企業は「ファーストレスポンダ」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?