高度で執拗な脅威(標的型攻撃)対策の組み方

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
基盤ネットワーク研究グループ
嶋田 創

ここ2,3年の嶋田の所感

- 英語の直訳である「高度で執拗な脅威or攻撃(Advanced Persistent Threat)」を使う方が実体を表して良いと思う
  - 「標的型攻撃」と言われると、自分の所はそこまで標的にされないと安心する組織が多そう
- 「標的型攻撃」という言葉はあまり実体を表していなくなって来ている気がする
  - 特にランサムウェアを伴うようになってから、「標的を絞って攻撃」から、「初期侵入成功した後に金になりそうならば、攻撃を進行させる」というパターンも多そう
  - ランサムウェア被害は2024年に入って前年の4,5倍のペース(その後は安定)

→どの組織も「高度で執拗な脅威or攻撃」の対策は重要!

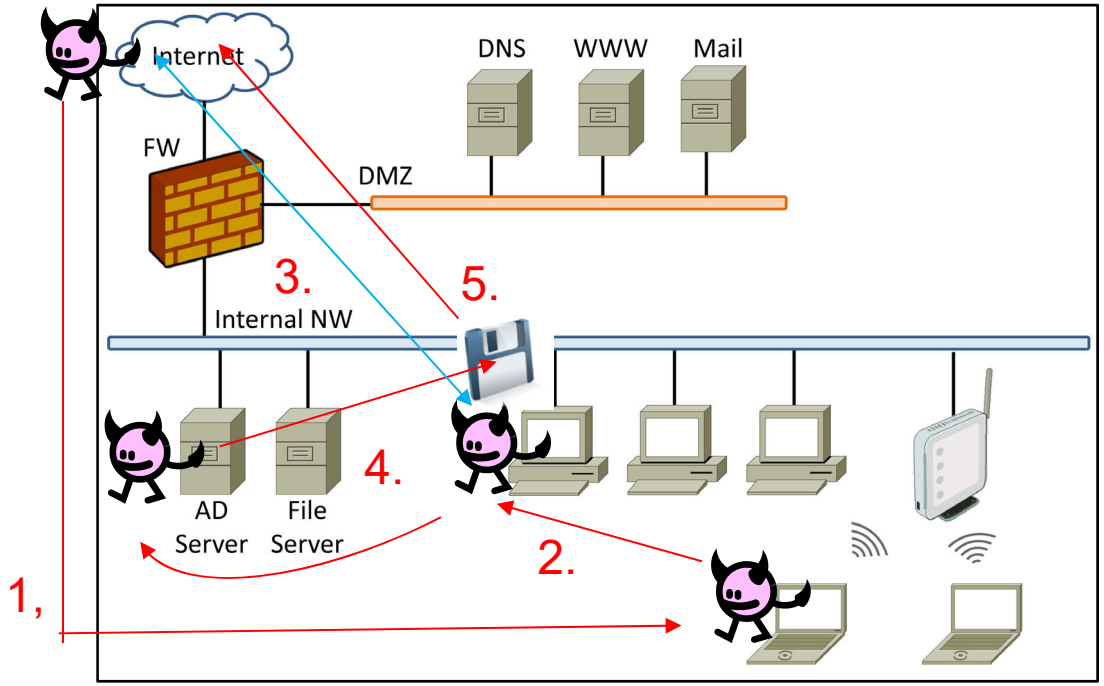
概要

- 標的型攻撃と近年の状況
- 標的型攻撃対策

標的型攻撃とその進行

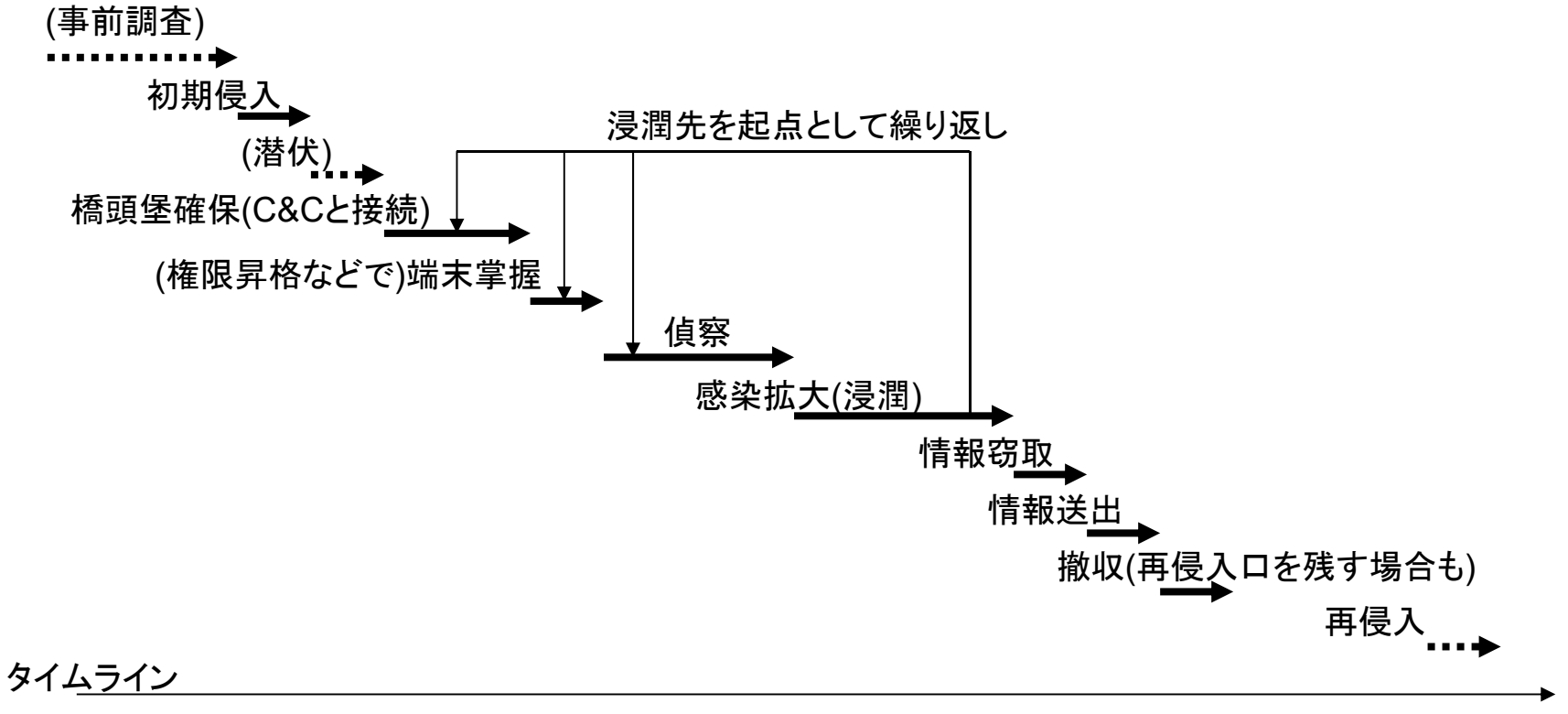
- 英語ではAdvanced Persistent Threat(高度で執拗な脅威)
  - 失敗しても何度も攻撃を試みる
- 代表的な標的型攻撃の進行
  - 侵入前に組織の内部構成を調査することもある
  - 長いものだと攻撃に数ヶ月かけることもある

1. 組織内部潜入
2. 内部での拡散
3. 外部との通信基盤構築
4. 機密情報窃取
5. 情報送出



標的型攻撃のタイムライン

- 事前調査や潜伏や再侵入は存在しないこともある
  - 個人的には、「うまく初期侵入できたから」という理由から始まる標的型攻撃が増えているのではと思っている



標的型攻撃の代表例(1/2)

三菱重工への標的型攻撃[1]

- 企業に対して大規模な標的型攻撃のリスクについて認識させた事例
- 2011/8にサーバが再起動を繰り返す原因追求中に発覚
  - 感染台数: サーバ 45台、従業員用PC 38台
  - 8種類のマルウェアを11の事業所から発見
- 発端:「原発のリスク整理」と名付けられた添付ファイルに見せかけたマルウェア
  - Adobe Flashの脆弱性を利用するマルウェア
  - 東日本大震災(2011/3)の直後かつ送信元は内閣府実在の人物の名前、メールアドレスを騙る

  →三菱重工は原発を作っている(いた)ので、受け取った人は疑いにくい

[1] https://piyolog.hatenadiary.jp/entry/20110919/1316393705

標的型攻撃の代表例(2/2)

日本年金機構への標的型攻撃[1, 2]

- 大々的にニュースになって、一般的な人にも標的型攻撃について知らしめた事例
- 2015/5/23にシステム管理会社が不審な通信を報告して発覚
- 発端: マルウェア送り込みURL付きメールのURLクリック
  - 2015/5/8に最初の1名、数日おいて他にもう1名が
  - RAT型マルウェア(Emdivi)を送り込まれ、内部感染拡大が進行
    - 当時にアンチウイルスソフトウェアの検知をすり抜けた
  - 最終的に31台のPCに感染
    - 感染PC経由で共有ファイルサーバから情報窃取された

[1] https://www.mhlw.go.jp/stf/shingi2/0000095311.html
[2] https://piyolog.hatenadiary.jp/entry/20150601/1433166675

標的型攻撃の実例(3/3)

EmEditorアップデートファイルを利用した攻撃[1]

- 攻撃対象: 名古屋大学、JAXA、ISAS、朝日新聞、農林水産省など
- 以下の様な.htaccessファイルがアップデート配布ディレクトリに置いてあった
  - 指定したIPアドレスの範囲からアップデート要求があれば別ファイルを配布

```
SetEnvIf Remote_Addr “106¥.188¥.131¥.[0-9]+” install
SetEnvIf Remote_Addr “133¥.6¥.94¥.[0-9]+” install
(… 同様に70行 …)
SetEnvIf Remote_Addr “124¥.248¥.207¥.[0-9]+” install
RewriteEngine on
RewriteCond %{ENV:install} =1
RewriteRule (.*¥.txt)$ /pub/rabe/editor.txt [L]
```

[1] https://jp.emeditor.com/general/ 今回のハッカーによる攻撃の詳細について /

個人的に勉強になると思う標的型攻撃の報告書(1/2)

- 産総研の情報システムに対する攻撃[1]
  - 研究所だけあって、50ページにも渡る詳細な報告書
    - よくぞここまで細かく公表してくれましたと感謝しかない
  - 弱いパスワードを設定したIDを外部公開システムで確認される
  - 内部システムにつながるサーバの攻略後、上記のIDを悪用される
- 海外拠点経由で侵入された三菱電機の事例[2, 3]
  - アンチウイルスソフトウェアのアップデート配信サーバの脆弱性を突いてマルウェア配布で感染拡大
    - アップデートハイジャックの亜種
  - PowerShellで組んだファイルレス型マルウェアを利用

[1] https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf
[2] https://piyolog.hatenadiary.jp/entry/2020/01/20/172436
[3] https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf

個人的に勉強になると思う標的型攻撃の報告書(2/2)

- 海外拠点とBYOD端末の2経路から侵入されたNTTコミュニケーションズの事例[1, 2]
  - 1系統は海外拠点からの侵入は、3カ国(シンガポール、タイ、米国)の営業所を経由した多ホップの侵入
    - 撤去を控えたサーバを踏み台にされた
  - もう1系統はBYOD端末(社員の私用端末)からの侵入

個人的には、企業も標的型攻撃対策に活用できるレベルの報告書を出してきてくれて嬉しい

- 個人的には、このレベルで報告書を出せる企業の方が信用できると思う

[1] https://piyolog.hatenadiary.jp/entry/2020/07/03/180308
[2] https://www.ntt.com/about-us/press-releases/news/article/2020/0702.html

その他の標的型攻撃の実例

- 大阪大学の情報機器管理者IDを窃取した事例[1]
  - 情報機器管理者IDを使って他の教職員の認証情報59人分窃取して、それを用いた不正ログインも実行
  - これを機会に脆弱性管理体制を強化[2]
- 富山大学に大学院進学希望者を装ったメールによる攻撃[3]
  - 情報を圧縮ファイルにまとめて窃取した形跡

[1] http://d.hatena.ne.jp/Kango/20171213/1513195810
[2] http://www.itmedia.co.jp/enterprise/articles/1807/17/news008.html
[3] http://d.hatena.ne.jp/Kango/20161010/1476110179

標的型攻撃とソーシャルエンジニアリングのハイブリッド(のような)

近年ではSNSで業務をアピールする人間も多々あり、SNSを通じて攻撃の初期段階が進むこともある

- SNSから仮想通貨事業者のエンジニアの割り出しと接触からの仮想通貨窃取[1]
  - SNS上でエンジニアを数人割り出して偽名でコンタクト
  - 半年以上時間をかけて交流をした上でマルウェア送り込み
- LinkedIn経由での接触からの機密情報窃取[2]
  - (進行中の案件であり、詳細は変わる可能性あり)
  - LinkedInで社名の他に研究内容を公開していた
  - 技術情報の交換と称して、機密情報を送信させた

[1] https://www.fss.jp/21180516-2/
[2] https://piyolog.hatenadiary.jp/entry/2020/10/15/180000

テレワークにおける標的型攻撃リスク (1/2)

COVID-19関係でテレワークが急速に増えたことにより、標的型攻撃を受けるリスクが高まった印象

- 雑談によるセキュリティ状況の交換が減る
  - オフラインで「怪しいメール来た」とか盛り上がったりするのは以外と重要だと思う
- テレワークで増えたVPN機器の脆弱性対応の遅れから…
  - というか、事故報告を見るとVPN機器が初期侵入口が非常に多い
  - というか、COVID-19の頃に導入されたVPN機器のメンテナンスはちゃんとされていますか?

テレワークにおける標的型攻撃リスク (2/2)

- BYODテレワークのセキュリティは?
  - 企業のセキュリティ対策ソフトウェア契約はBYODをカバーしている?
  - BYOD端末のセキュリティ上の問題を確認できる?
- インシデント発生時に追跡のための情報の不足
  - 家のブロードバンドルータのセッションログとか保存されています?
  - プライバシーの観点からも、BYOD端末や家庭内ネットワークにネットワーク・フォレンジックをするのはやりづらい…

→テレワークのVPNからの権限を一段下げるなどの工夫が欲しい

概要

- 標的型攻撃と近年の状況
- 標的型攻撃対策

(ステージが進んだ)標的型攻撃は何が痛いか?

- (当然だが)情報を窃取される
- 長期間インシデント対応者が拘束される
  - 1ヶ月以上に渡って調査している事例も多い
  - その間の新規案件の対応は大丈夫か?
- 対応の間に業務が止まる
  - 例: 産総研で1ヶ月以上ネットワーク遮断[1]
    - 2022年10現在では、政策研究大学院大学が2ヶ月ほど停止中
  - 日本年金機構も未だに過度なエアギャップを入れていると聞く
  - 近年ランサムウェアやられた大学の業務復旧も1ヶ月以上が多い

→事前に「攻撃対応と事業継続」を評価し、遮断箇所と基準を複数作る

[1] http://foxsecurity.hatenablog.com/entry/2018/03/19/090000

ポイント

- 初期侵入から基盤構築段階まではやられることは前提
- 多層防御で対応する
- 最終目的までたどり着かせなければ勝ち

- 繰り返し相手を変え手を変えて攻撃してくることを想定

事前対策

- 情報システム/ネットワーク設計
- サーバやクライアントに対する定期的な脆弱性検査
- 一般メンバへの定期的な標的型攻撃(メール)訓練
- 情報収集(脆弱性、攻撃事例)
  - 外部との情報交換体制
  - 内部への警告情報展開
- セキュリティ設計の再評価と再構築
- インシデントレスポンス体制の再評価と再構築

情報システム設計: 利用者の限定

事務作業などの定形作業が中心の部署の場合

- 利用できるアプリケーションの限定
- 利用できるウェブサイトの限定
- セキュリティの観点から、クライアント側のアプリケーション管理を行うフレームワークもある
  - アンチウイルスソフトウェアのように、クライアント側に管理ソフトウェアをインストールして
  - アプリケーションのアップデート状態も管理
  - ソフトウェア資産管理や情報漏洩対策も兼ねる

ネットワーク設計: 分離設計

- 小規模組織であっても、業務の異なる部門は別ネットワーク(VLAN設定などでサブネット)に分割する
  - 分離したネットワークの間はルーティング設定が必要
  - 例: 営業部門と開発部門のネットワークは分離
- 低価格のL3スイッチでもアクセス制御の設定はできるのがほとんど
  - ポート単位とかVLAN単位とか
- 分離したサブネット間で通信が一定量発生したらアクションを起こす設定をするとか
  - 最近のネットワークスイッチはセキュリティ対応機能が増えていたりする
    - セキュリティ機器と連動してポート遮断などもできたりする

もっとネットワーク的にガチガチなアクセス制限かけるならOpenFlowが有望

- 産業機器NWとか医療機器NWで機器からのデータは通信させたいが、規定外の通信はさせたくない用途に使えるかも
  - 例: センシングデータ入りパケットは100B-200Bの間なのでそのサイズのみ通信を許可したい →OpenFlowでそういうフローを書く
  - 規定外パケットは全てOpenFlowコントローラに投げて必要に応じて追加フローを書く形でガチガチにできるはず
- OpenFlowなどのSoftware Defined Networkはコスパが悪かったが通信量はそこそこでOKなこういう用途ならあり

- 初回講義で話した、「AIペネトレーションテストの進化で、EoL機器への脆弱性探査と攻撃が増える、ロングテールなサイバー攻撃がこの先増える」話への対策の候補
  - ECサイトでどマイナー趣味の店が成り立つECのロングテール戦略と同様のことが、サイバー攻撃で起こりうる話

定期的な脆弱性検査

- ツールを利用した定期的な脆弱性検査と対策指示
- 個人的なおすすめ
  - ウェブサーバ: OWASP ZAP
  - ネットワークサーバ全般: Nessus(個人利用は無料), OpenVAS
  - ポートのオープン状態: nmap (他の脆弱性検査ツールも多し)
  - システム内部各ソフトウェアの脆弱性情報: OpenSCAP
- 最近だとAIペネトレーションテストツールも多い(雨後の筍)
  - Artex, Cairn, Strixやそれらを連携させる(呼び出す)上位のAIエージェントとかでペネトレーションテストはまくる(はず)
    - (現時点でいろいろありすぎて嶋田はまだ実際に使えていない)
- セキュリティベンダ提供の商用な物もいろいろ

標的型攻撃訓練メール

- 対象: 全組織構成員、もしくは、特定の属性の人(役員)など
- どこがやっても、最初は10%以上がひっかかったりして、皆びっくりする傾向
- 組織外部の標的型メール差し出し元やアクセス先URLの準備に少し手間がかかるかも
  - 標的型攻撃メール訓練を実施する業者も多数出ている
  - ただし、アクセス先URLにシーケンシャルなIDを埋め込む間抜け業者もいるので注意
- フリーな物もある
  - https://github.com/fishing-cat/fishing-cat-server
  - https://github.com/gophish/gophish

情報収集

- 情報収集
  - セキュリティ関連ニュースサイト
  - IPA、JPCERT/CC、警視庁サイバー犯罪対策課などの情報
  - 後述する(CSIRTなどの)情報交換組織に加入
- 収集した情報のうち、自組織で脅威度の高く、広く共有した方が良さそうな情報は組織内展開
  - 外部がイラスト入りで親しみやすい再展開OKな情報を提供してくれるのは助かる
  - あまりしつこいとオオカミ少年になってしまうので注意

事前対策の注意点

- 全部を全力でやったら、当然、コストはうなぎのぼり
  →取捨選択は必須
- 業務フローを見て、効率の良い対応策を選択
  - 例: FA機器のみのサブネットを作成し、特定のポートの通信のみを許可するとともに、一定時間あたりの通信量でトラップをしかけた
  - 定形業務がほとんどの部門はやりやすそう
    - 例外処理は申請の形にしても対応でパンクすることは少なさそう
  - 逆に業務フローの固定されない研究開発部門などは効率の良い対応策を作成するのは難しそう

初期侵入検知

- (メール添付ファイル)
- DNSクエリログ
- IDS/ファイアウォール/ウェブプロキシログ

- このあたりは、「日に何度も更新される悪性URLや悪性IPアドレスリスト」を利用してブロックするのが基本
  - 攻撃者が1日(以下)レベルでIPアドレスを変えたりする
  - 各種セキュリティベンダがIPS/ファイアウォール向けに(有償で)提供している
- それに加えて、必要に応じて追加で自組織に対する攻撃とかのあった所をブロック
  - 必要に応じてBGPレベルなど上位レベルでブロック(ブラックホールルーティング)

検知の難しい初期侵入

- 外部に持ち出したノートPCがマルウェア感染
- USBメモリ経由で感染
  - 素の怪しいUSBメモリを挿す人は少なくても、USBストレージクラスを(隠し)持つUSB機器のマルウェア汚染というのがあるから怖い
- 保守業者がマルウェア感染PCで保守

→C&C通信などをもとに検出

- …が、DoH/ESNIなどで検知が難しくなるので怪しい低頻度通信などの振る舞い検知方向の重要性が増している

基盤構築段階での検知

- 基本はC&Cの検知
  - 普段は通信の無いIPアドレスとの通信
    - 普通は通信の無い国との通信
  - 仕事中なのにSNSなどの業務に関係無いサイトにアクセス
- 1つ見つけたら
  - 同じIPアドレスと通信している他の端末はないか
  - その端末が通信している他のC&Cらしきアドレスはないか(複数C&C)
- さらに先(侵入経路の特定)などはネットワークフォレンジック(情報ネットワーク特論[1]参照)になる

[1] https://www.net.itc.nagoya-u.ac.jp/member/shimada/infoNW2026B/index.html

基盤構築段階で泳がすのはあり?

A: ありといえばあり

- 一網打尽にしないと、他に侵入した物を使って何か悪さをされる可能性が0ではないため
  - (他感染端末への)新たな検出困難なマルウェアの更新、証拠隠滅、など
- 泳がして何をする?
  - 他に(同系統の)C&C通信が無いか確認
  - (その攻撃と並行して使われる)マルウェアの存在の調査

もちろん、リスクもある

- 泳がしている間にさらなる感染拡大をやられた
- 基盤構築段階と思ったら情報窃取も進んでいた

こんなことも想定する?

- インシデント対応者側のPCもマルウェアに感染させられた
- インシデント対応チームが連絡に使うサーバも犠牲の可能性を考えて止めることになった
  - 対応マニュアルとか入れたストレージとかも
- 対外接続回線がDoSで埋まってインシデント対応時に外部情報を参照できなくなった

→予備の連絡系統を準備しておく

- 予備のPC、予備の連絡体制(別サーバ、外部サービス)
- 予備のネットワーク回線(ISP回線、携帯電話回線)

標的型攻撃を前提としたインシデント対応に欲しい人材(もしくは役割)

- 連絡窓口(組織内、組織外)担当
- 法務(との連絡)担当
- 組織内への連絡担当
- 組織内への情報発信/教育担当
- セキュリティ関連情報収集/分析担当
- 脆弱性診断担当
- 組織内アセスメント担当
- セキュリティ戦略担当
- インシデント対応統制/管理担当
- インシデント処理担当、捜査担当(内部犯想定)
- トリアージ担当
- フォレンジック担当

各人材の動きの例(事前対応)

- 教育担当によるリテラシの向上
- 組織内アセスメント担当による業務(変化)分析
  - 必要に応じてセキュリティ戦略担当へ
- 情報収集、情報分析担当による情報収集と分析
  - 必要に応じて脆弱性診断担当、教育担当、情報発信担当へ情報展開
- 脆弱性診断担当による定期的な脆弱性診断
- セキュリティ戦略担当による次に整備/推進すべき対応の決定(と上への折衝)
- インシデント対応関係担当
  - セキュリティ機器からのインシデント発生の有無の調査
  - インシデント対応演習の実施

各人材の動きの例(インシデント対応)(1/2)

- インシデント発生
  - インシデント対応関係担当がインシデントを発見
  - 連絡窓口が外部/内部からインシデント報告をもらう
- トリアージ担当が現状の状態を分析とトリアージ案作成
- インシデント対応統制/管理担当およびインシデント処理担当による対応決定と指示
  - 複数のインシデント対応を想定
- (必要に応じて)組織内への連絡担当による関連部門との折衝
  - 部門ネットワーク/サーバ全停止など影響範囲が特に広い場合は特に重要
- (必要に応じて)フォレンジック担当による証拠保全と分析

各人材の動きの例(インシデント対応)(2/2)

- インシデント処理/捜査担当による原因のまとめ
  - 内部犯の場合は捜査
- (必要に応じて)連絡窓口からの関連外部組織への連絡
- (必要に応じて)法務担当による法務関連処理

- (終了後)組織内への情報発信/教育担当による再発防止のための情報発信/教育
- (終了後)セキュリティ戦略担当による戦略への影響の評価
- (終了後)組織内アセスメント担当による損失等の見積もりや事前対応コストの評価

インシデント対応チーム

- 前述の人材(役割)をどう確保する?
  - 1人でカバーできる範囲は限られている
  - 専任の人材をそんな数確保できない…

  →組織内の一部の人に兼任で入ってもらうこともあり
- CSIRT: Computer Security Incident Response Team
  - Computer Emergency Response Team(CERT)だったり
  - 最近は多くの組織で存在するのが当たり前になってきた
    - 後の日本CSIRT協議会の加盟数を見ると、順調に増えている
- 人材を外部サービスに頼るのもあり
  - Security Operation Center (SOC)の外部委託サービスなどと同様
  - 「週1で外部サービスの人材が来て事前対応関連の作業を行う」というサービスとか
  - 平日9-17時以外のSOC業務を依頼するとか

各担当に求められる能力

- 連絡窓口(組織内、組織外)担当
- 法務(との連絡)担当
- 組織内への連絡担当
- 組織内への情報発信/教育担当
- セキュリティ関連情報収集/分析担当
- 脆弱性診断担当
- 組織内アセスメント担当
- セキュリティ戦略担当
- インシデント対応統制/管理担当
- インシデント処理担当、捜査担当(内部犯想定)
- トリアージ担当
- フォレンジック担当

求められる能力(連絡窓口)

- 組織内外の種々の部門とやりとりできるコミュニケーション能力
- 受けた連絡や外部とのやりとりをまとめて情報戦略担当やインシデント管理担当などに送る能力
- 現状のセキュリティ問題に関する知識
  - 直接は自組織に関連しないものでも
- 既存の脆弱性に関する知識

求められる能力(法務(との連絡)担当)

- 法務のプロトコルの知識(経験)
- セキュリティに関する関連法の知識
- セキュリティに関する法的な動向の知識
- 個人情報保護や情報倫理の動向の知識
- (インシデントレスポンスに関する知識)
- (セキュリティに関する技術動向の知識)

求められる能力(組織内への連絡担当)

- 組織の各部門の情報システムに関する知識
- 組織(や各部門)のセキュリティガイドラインや遵守事項の知識
- 組織(や各部門)での折衝能力
  - インシデントのリスク把握と優先順位の説明できる能力
- インシデントレスポンスに関する知識
- 既存の脆弱性に関する知識

組織の部門の人間を巻き込む方が早そう

求められる能力(組織内への情報発信/教育担当)

- 情報を正しく伝えるコミュニケーション能力
- 情報を分かりやすく伝えるコミュニケーション能力
- 組織内での折衝能力
  - 恨みを買わないようにうまく折衝する能力
- インシデント対応チーム内での報告能力

求められる能力(セキュリティ関連情報収集/分析担当)

- 英語での情報を検索/収集できる能力
- 偽情報や誇大情報に踊らされないメディアリテラシー
- セキュリティや関連技術に関する知識
  - 偽情報や誇大情報を判別するための基礎知識
- 攻撃の動向などの知識
- 自組織の情報システムに関する知識
- 収集した情報をまとめて他担当に伝える能力
  - インシデント対応チーム内での報告能力

求められる能力(脆弱性診断担当)

- 情報システム構築に関する知識
  - OS、ネットワーク、各種(ウェブ/メール/認証/ファイル/DB)サーバ構築、など
- 自組織の情報システムに関する知識
- 脆弱性診断ツールの知識やその動向を収集する能力
- よく利用される脆弱性やそれを利用した攻撃に関する知識
- 新たなセキュリティ問題等の情報収集する能力
  - セキュリティ関連情報収集/分析担当からの報告以外にも自主的にできると良い
- インシデント対応チーム内での報告能力

求められる能力(組織内アセスメント担当)

- リスクアセスメントの評価プロセスや報告に関する知識
- セキュリティや個人情報保護関連の法律や公的規約に関する知識
  - その最新動向を調査する能力
- 組織(や各部門)のセキュリティガイドラインや遵守事項の知識
- インシデント対応チーム内での報告能力

求められる能力(セキュリティ戦略担当)

- 組織の業務のマスタープランに合わせてセキュリティ計画を立てる能力
- 組織(や各部門)のセキュリティガイドラインや遵守事項の知識
- 組織の情報システムに関する知識
- リスクマネジメントに関する知識
- セキュリティや個人情報保護関連の法律や公的規約に関する知識
- セキュリティ機器やセキュリティ関連人材を組み合わせる能力
- 経営層に戦略を説明し予算を確保するコミュニケーション能力

求められる能力(インシデント対応統制/管理担当)

- 情報システム障害の全貌を把握するための前提となる、情報システム(構築)に関する基礎知識
- 組織の情報システムに関する知識
- 情報システム停止と業務影響に関する知識と判断能力
- 経営層にインシデント対応を(噛み砕いて)説明できるコミュニケーション能力
- 標的型攻撃のフローと業務への影響の知識
- セキュリティ問題、マルウェア、攻撃の動向の知識
- 復旧も含めたインシデント対応に関する知識
- 攻撃フローと業務影響から、業務影響を考慮したインシデント対応判断を下せる能力
- インシデント対応チーム内での報告を処理する能力

求められる能力(インシデント処理担当、捜査担当)

- セキュリティ問題、マルウェア、攻撃への対応能力
- 復旧も含めたインシデント対応の能力
- 情報システム障害の全貌を把握するための前提となる、情報システム(構築)に関する基礎知識
- 組織の情報システムに関する知識
  - 運用経験があるとなお良い
- インシデント対応チーム内での報告能力

求められる能力(トリアージ担当)

- 情報システム障害の全貌を把握するための前提となる、情報システム(構築)に関する基礎知識
- 組織の情報システムに関する知識
- 情報システム停止と業務影響に関する知識
- リスクと業務影響を考えて優先順位を提示する能力
- インシデント対応チーム内での報告能力

求められる能力(フォレンジック担当)

- ネットワークフォレンジックの能力
  - ネットワーク機器からのアーティファクト抽出
- デジタルフォレンジックの能力
  - メモリやディスクからのアーティファクト抽出
- (軽い)マルウェア解析の能力
  - スクリプト、マクロ、バイナリの簡単な解析
- セキュリティ関連イベントの相関
- インシデント対応チーム内での報告能力

想定される攻撃のシナリオはどう作る?

- 過去の(外部の)インシデントを参考に作成
  - あまり細かく書かれていなかったりするので、補う
- 標的型攻撃対策の学術研究論文のシナリオを参考に作成
- MITRE ATT&CK[1]などの攻撃モデルと組織の導入機器で想定される脆弱性をもとに作成
  - 最近は、MITRE ATT&CKが攻撃モデルのデファクトスタンダードになってきている
    - ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge
  - 新しい脆弱性をMITRE ATT&CKにマッピングする研究等も多数あるので、新しい脆弱性をもとにシナリオを作りやすいと思う

[1] https://attack.mitre.org/

CSIRT間で情報交換するフレームワーク(1/3)

- FIRST(Forum of Incident Response and Security Team)
  - https://www.first.org/
  - 1990年に組織されたインシデント対応チーム情報交換用フォーラム
  - 高頻度で世界中でシンポジウムとかワークショップ(Regionalなタイトルな物も含む)を開いてor後援している
  - 教育コンテンツも提供
    - CSIRTの業務フレームワーク[1]を複数の言語で提供
    - PSIRT(製造物に関するSIRT)のガイドライン[1]も提供
- NCA(Nippon CSIRT Association)
  - http://www.nca.gr.jp/
  - こちらも日本中でワークショップを開いていたりする
    - こちらの方が、近くのCSIRTと情報交換体制を作りやすいかも
  - こちらも資料はあるが、ちょっとメンテナンスがされていない感じ

[1] https://www.first.org/education/service-framework

CSIRT間で情報交換するフレームワーク(2/3)

- 各種ISAC
  - ISAC: Information Sharing and Analysis Center
  - 主に、特定の業界において、サイバーセキュリティを含む情報セキュリティの情報交換グループ
    - 前述のFIRSTやNCAは分野を問わない感じだが、ISACは業界ごとに作られている印象
    - もちろん、分野横断の情報交換も重要
  - 例: 金融ISAC、電力ISAC、交通ISAC、通信ISAC
- CSIRTではないが、ネットワークサービス主体ならNOC(Network Operators Group)の情報交換もあり
  - 日本全体のJANOG(JApan Network Operators Group)
  - 地域NOGもいくつか(例: ChuNOG)

CSIRT間で情報交換するフレームワーク(3/3)

- NII-SOCS(Security Operation Collaboration Service)
  - Security Operation Center(SOC)ではない
  - 正式名称: 大学間連携に基づく情報セキュリティ体制の基盤構築
- セキュリティの教育が主目的
  - 各大学の技術職員などに検知、解析、対応のフローなどを教育
- まあ、実際はSOCのような業務もやっていたりはします
  - (希望を出した国立大学法人に対して)SINETの通信に対してアラートを出す形で
    - ただし、全通信を同時に見る機器性能は無く巡回開始
    - ただし、通信の中身をNII-SOCS側人員は解析しない(通信の秘密対応)
    - 特定の研究用IPアドレス領域の除外も可能
  - 各大学の技術職員の教育には、上記のアラートの自大学分を利用

経営層対策はどうする?

- 幸い、経営層向けの資料(本、雑誌記事)も増えてきている
- 経済産業省の資料
  - サイバーセキュリティ経営ガイドライン[1]
  - 付録C インシデント発生時に組織内で整理しておくべき事項(Excel形式)[2]は(Excel文化が強い多くの日本企業で?)使いやすそう
  - 経営リスクとしてのサイバーセキュリティ対策[3]
- 恐れすぎなりすぎて業務効率が悪くなりすぎないよう、必要に応じてブレーキをかけることも忘れずに
  - 「外部からの情報提供に針小棒大な反応」話はよく聞く
- (定期的に)経営層とインシデント対応フローの確認するとか
  - どこまでインシデント対応側で判断OKで、どこから経営層判断か
  - もちろん、同時に現状の世の中についてレクチャー

[1] http://www.meti.go.jp/policy/netsecurity/mng_guide.html
[2] http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_C.xlsx
[3] http://www.soumu.go.jp/main_content/000528735.pdf

標的型ランサムウェア対策(事前)

- 浸潤や情報送出対策は一般的な標的型攻撃対策と変わらない
  - 最近はVPNやRDPなどのリモートアクセス系からの侵入が特に多い
- エアギャップのある領域への定期的な複数世代バックアップ
  - 破壊された後の物をバックアップしてしまう可能性を考えて複数世代バックアップ
- 復旧手順の確認
  - システムのクリーンインストール手順の更新
  - データのリストア手順の確認
- 窃取データ公開に対する対応の事前検討
- ランサムウェア対策システムの導入
  - 不自然なストレージへのI/Oをもとに検知/ブロックして被害を部分的にするシステムなど多数あり

標的型ランサムウェア対策(事後)

- 被害範囲の確認
- 攻撃者からのオープン情報源へのアクションの確認
- 復旧前のクリーンな状態の確認
  - システム自体をクリーンインストールするのが望ましい
- クリーンな環境での最新バックアップのコピーの作成
  - 万が一のバックアップの破損への備え
- データ公開に対する対応
  - 公開されたデータで影響を受ける人や組織への対応
- 各ステークホルダー(利害関係者)への報告
  - 顧客(オンラインサービス利用者含む)、下請けもステークホルダーです

個人的には事後対応はほぼ100点満点だったランサムウェア対応事例(1/2)

タイムラインは[1]公式PDF資料と[2]の識者blogより

- 2023年7月の名古屋港コンテナ管理システムのランサムウェア対応
- 仮想化基盤からがっつり暗号化されたのに2日半で復旧
  - 警察庁資料でも1週間以内の復旧でも上位1/4
- 特に良いと感じた点
  - 比較的早期の初報と継続的な細かな報告(7/5-7/6にかけてオンラインだけで4回の報告)
    - 経緯報告も含め、今もオンラインで報告資料が見れる点も後から勉強になる点で非常に良い
  - バックアップデータに対する徹底したマルウェア確認と、発見後すぐの復旧目標の先送り判断

[1] https://meikoukyo.com/archives/3336
[2] https://piyolog.hatenadiary.jp/entry/2023/07/05/233959

個人的には事後対応はほぼ100点満点だったランサムウェア対応事例(2/2)

前ページ[1][2]よりタイムラインピックアップ

- 7/4 6:30頃 ランサムウェア起因のシステム障害発生
- 7/4 7:15頃 システム保守/開発会社に復旧依頼
- 7/4 8:15頃 サーバ再起動不可が判明
  - この時点でランサムウェアの可能性を考えている
- 7/4 14時頃 仮想化基盤からの全暗号化が判明
- 7/5 12時頃 対外発表: ランサムウェア、5日終日停止
- 7/5 21時頃 バックアップデータからもマルウェア検知で復旧目標(7/5 18時→20時→さらに)の先送り判断
- 7/6 7:15 バックアップデータ復元完了(ただし、システム上にネットワーク障害発生)
- 7/6 14:15 ネットワーク障害解消とバックアップデータとヤード在庫の整合性を確認し、復旧

嶋田の個人的な所感(1/2)

- 皆が防犯や災害対策と同じぐらいの意識で、各組織や組織員が日常的に対策を考える意識を持つようアピールしたい
  - 窃盗犯対策
  - 自然災害(火災/地震/水害)対策
  - 労働災害対策
  - (New!)サイバー犯罪(攻撃)対策
- 直近で「一般的に緩かったのを地道に要対策として浸透」させてきたものは労災対策なので、同様に地道に改善
- 難しい点は、労災対策と違って周りから見て「良くない状況にある」というのが難しい
  - しかも、サイバー攻撃は弱い所(人)を初期侵入口とした上で浸潤する要素が強いので、弱い所の改善は他と同等以上に重要

嶋田の個人的な所感(2/2)

- 一般の人に対してどう訴求するのかは何が効くのか…
  - 労災対策については現場猫なネットミームで広く知られた印象があるので、同様に何かネットミームになってくれるのが嬉しそう
    - (ネットミームの種を地道に作ってばらまいて受けるのを探す?)
- 個人的には、一般の人向けには標的型攻撃対策のGamificationを進めるのが良いのではと思ってはいるが…
  - …が、一般の人向きの感覚というのに自信が無いのが情報学系の人にとって悩みどころ(ゲーム業界を参考にできれば…?)
    - 情報学系の人だとCTFとか楽しいと思うが、一般の人に訴求するには?
  - 単純にゲーム化だけではなく、効果的な報酬は何かとかの観点とかも良いかもしれない