業務継続と被害拡大防止を両立させる サイバー攻撃対応

高倉弘喜
国立情報学研究所

「インシデント対応＝隔離/遮断」の功罪

- ■(標的型？)サイバー攻撃によるマルウェア感染を確認
  - ● 被害状況(感染台数、感染部署、情報流出の有無)は不明
    - ◆ どのような対策が考えられるか？
- ■多くの組織で実行されるネットワーク遮断
  - ● 組織部署、もしくは、組織全体をインターネットから隔離
- ■これは正しい対応と言えるのか？
  - ● 業務(顧客サービス)が止まる
  - ● 営業機会を失う
  - ● 情報インフラが弱体化する
    - ◆ ブービートラップの可能性も
      - ➢ 日本では確認されていないが…
- ■どう対応すればいいのか？


朝日新聞デジタル ＞ 記事

産総研、ネット遮断１カ月

2018年3月16日05時00分

https://www.asahi.com/articles/DA3S13404765.html

1,300万人分のデータ持ち出し…500万人分が海外へ

■契約は800人で作業…実態は百数十人
- 800人分の作業スペース…物理的に用意できるか？
  - 一人当たり最低でも6m² → 4,800m²が必要
    - 首都圏だと家賃だけで月額2,000万円台…1.8億円の短期間契約
- 500万人分は中国の子会社へ

■契約で縛っても持ち出す奴は居る
- データは持ち出させない
  - サンプルはダミーデータ
- VPNでアクセスさせる
  - アクセス元の制限・把握
  - 大量データ持ち出しを監視する

■では、なぜこんなことに？

宇治市の個人情報持ち出し事故(1999年)の教訓はどこに？


朝日新聞 DIGITAL

トップニュース　スポーツ　カルチャー　特集・連載　オピニオン

新着　天声人語　社会　政治　経済・マネー　国際　テック&サイエンス　環境・エネルギー　地域

朝日新聞デジタル ＞ 記事　社会　事件・事故・裁判　医療・健康・福祉（アピタル）

個人情報の入力、一部を中国業者に　年金機構の委託業者

https://www.asahi.com/articles/ASL3M7QSPL3MUCLV01M.html

一因は2015年の個人情報流出事件に遡る

■年金機構をインターネットから遮断
- 100%の安全性が確認できるまで
- 端末操作の権限も一部職員に限定
  - 電話対応職員も端末がない(メモ紙のやりとり)
  - FAXやUSBメモリでの情報交換

遮断が業務フローに及ぼす影響を理解していたのか？

■100%の安全宣言を出せるのか？
- 総入れ替えしか手はない
  - パソコン、サーバ、ネットワーク装置
  - コピー機、プリンター
  - データ…と人
- 現実的には不可能
- 3年近く経っても遮断は継続
  - でも待ってくれない業務

業務継続のために却って
セキュリティレベルを下げてないか？

それでも続く、数台のマルウェア感染で全業務停止

報道日時	被害組織	感染台数	発端	原因	対応状況
2016年 6月22日	新城市	新城消防署PC2台	不明	不明	市役所を含むネットワーク遮断(6月21日～22日まで)
同日	静岡市	静岡市役所PC1台	警察からの情報提供	不審メールの開封	初期化済み(6月2日) 情報提供後インターネット接続遮断
同日	御前崎市	1台 (他感染可能性のあるPCあり)	警察からの情報提供	不明	マルウェアの駆除、初期化
同日	三豊市	市役所内PC4台	警察からの情報提供	不明	インターネット接続遮断
2016年 6月25日	群馬県	県庁内PC1台	自組織にて検知 外部より情報提供あり	ばらまき型メールの添付ファイル開封	感染詳細の調査中 詳細判明後に公表予定
同日	小山市	小中学校3校のPCがマルウェア感染	警察からの情報提供	標的型メールによると推定	感染したマルウェアは除去済み。 情報漏えいの有無について確認中。

インターネット時代における籠城戦

国立情報学研究所

5

http://d.hatena.ne.jp/Kango/searchdiary?of=1&word=%2A%5B%A5%A4%A5%F3%A5%B7%A5%C7%A5%F3%A5%C8%A4%DE%A4%C8%A4%E1%5D

全業務停止 v.s. サービス継続のジレンマ

■2016年に発生したJTB情報漏洩事件

- 3/19-24間に発生した不審通信の発生を一部見逃したのが問題なのか？

発生日	事象
3/15	攻撃メール着弾
3/18	起動不能の端末出現・NW隔離
3/19	委託監視企業よりWebサーバで複数の不審通信の報告・NW隔離と調査
3/20	調査結果はマルウェア未発見・通信先の一つを遮断
3/21	サーバでディスク容量不足発生→大容量ファイル確認・業務上不要として削除
3/24-25	複数の不審通信先を追加遮断・社内端末5台で不正通信失敗を確認
3/28	端末・サーバでのマルウェア感染を確認→詳細調査開始
4/1	概要把握→全社CSIRTによる調査開始
5/13	個人情報漏洩の可能性を認識

7日間

業務継続の是非

国立情報学研究所

6

http://d.hatena.ne.jp/Kango/20160614/1465925330#20160614f1 より抜粋

サイバー時代の籠城戦の心得

■短期決戦であること
- 情報漏洩を防止するという観点では正しい
- 営業機会を失うことによる損害額は許容範囲内か？

■備蓄が十分であること
- データの鮮度は→秒単位で賞味期限切れなものも
- 備蓄が底をつくまでに補充が受けられる見込みはあるのか？

■外界からの情報が入手できること
- 営業データ、OS・アプリの更新データ、セキュリティ情報

■良くて数日…1週間経過すると、組織内のIT系は弱体化する
- サイバー攻撃の手口は秒単位で進化する
- 籠城中に適用されるはずだったセキュリティパッチを適用できるか？

万全な対策のマイクロソフトでも…

■60万台の機器

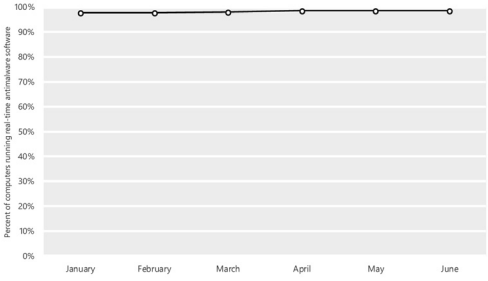
■15万人のユーザ

■100以上の国と地域

■2016年前半
- アンチウィルスソフト
  - ◆98%以上の使用率

■この規模だと
- アドウェア系: 80万件
- トロイの木馬: 35万件
- エキスプロ糸: 34万件

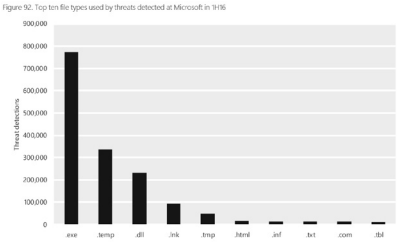
Figure 90. Percentage of computers at Microsoft running real-time antimalware software each month in 1H16



Microsoft Security Intelligence Report Volume 21

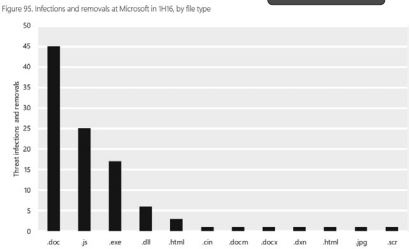
マルウェア感染を想定した対策の必要性

■ 半年で検知したマルウェア
- .exe: 78万
- .temp: 34万
- .dll: 23万



■ 感染後に検知・駆除したマルウェア
- .doc: 45件
- .js: 25件
- .exe: 17件

年々増加傾向



国立情報学研究所

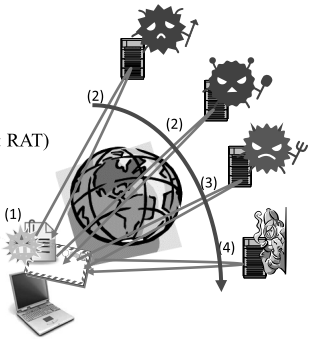
Microsoft Security Intelligence Report Volume 21

9

初期潜入後の基盤構築

■ 誤判断の誘導とステルス化

1. ダウンロード(トロイの木馬)系マルウェア
   - ◆ 感染対象機器の調査…目的のユーザなのか？
   - ◆ 感染後一般公開→駆除成功による誤判断を誘導
2. 多段ダウンロードによる追跡妨害
3. 遠隔操作マルウェア(Remote Administration Tool: RAT)
   - ◆ 組織内部に前線基地を構築
     - ➢ 脆弱性探索&攻撃
     - ➢ 標的型攻撃メールの素材収集＆送信
     - ➢ 共有サーバに悪意あるファイル設置
     - ➢ 認証サーバ(AD)を攻略
4. バックアッププログラム
   - ◆ RAT駆除等を監視→緊急連絡
   - ◆ オプションとしての破壊活動(サボタージュ)



10

国立情報学研究所

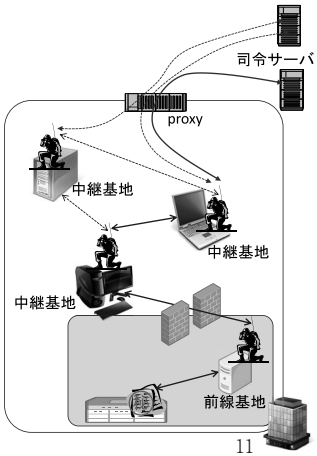
組織内部への侵食

■前線基地から徐々に内部へ侵食
- ● 前線基地を中継基地化
  - ◆ 外部接続性がない機器と外部との通信を仲介

■通信経路の多重化
- ● 司令サー・中継バサーバの多重化
- ● 組織内に張り巡らされた通信網
- ● 監視やログ記録を意識した通信手段
  - ◆ セキュリティ製品の検知回避
  - ◆ 目立たない通信
    - ➢ 木を隠すには森の中

「記録が見つからない＝被害がない」ではない！

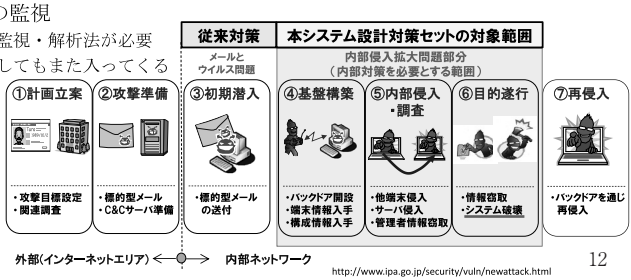
■気付いた時にはインシデント(事案)ではなくアクシデント(事態)に



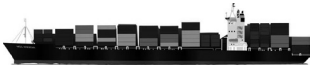
高度化する攻撃への対策

■従来対策の突破を前提とした対策が必須に
- ● 従来対策は無用という意味ではない

■内部での基盤構築、内部侵入・調査を察知し、目的遂行を阻止
- ● 内部NWの監視
  - ◆ 新たな監視・解析法が必要
  - ◆ 追い出してもまた入ってくる

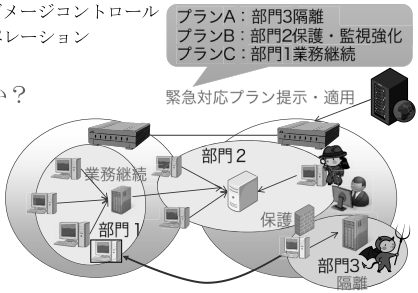


レジリエントな情報システムの構築



■情報システムの全停止は許されない時代に
- 局所的なシステム停止
  - 被害箇所の切り離し・隔離によるダメージコントロール
  - 代替措置によるデグレーデッドオペレーション
    - 業務への影響を把握

■人間がすべての指揮を執るのか？
- 人間系に対する飽和攻撃
  - パニック状態に陥るのは危険
- 一旦はプランに従って自動対応
  - 様子を見ながら適宜調整
    - 必要な情報の流れを確保
  - どこまで自動化できるかを研究



国立情報学研究所　13

CIAからAICへ

■システム全体が正常に動き続けること(Availability)　最優先事項
- 個々の情報システムの「不具合」が全体のIntegrityに影響するか？
  - 全体でみた場合、故障とマルウェア感染の区別は無い
    - 不具合は想定範囲内で制御可能なのか？　ダメージコントロール
    - 切り離しによる全体への影響は？　デグレーテッドオペレーションの可能性

■個々の部品から何らかの情報が得られること(Integrity)
- 異常値検知＆排除ができるか？
  - 福岡支店との回線が生きている…も情報

■個々のconfidentialityの優先度は一番下
- 極論だが…マルウェア感染しても使えるなら構わない

→レジリエントなシステム設計
　単一障害が致命的にならない設計(当たり前な話だが…)

国立情報学研究所　14

エリートパニックによる事態悪化の回避

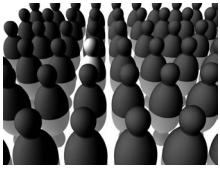
■エグゼクティブレポートとテクニカルレポートの使い分け
- 「アドウェアって何？」って上司に聞かれたら…
  - 「不要な広告表示プログラム」って言い換えれば良いやん！
    - 「不要な広告って広告になるのか？」…ツッコミ入れるとこそこかい！
      - 「不要なポスティング広告を表示するプログラム」ならどうだ！
        - **「不要とはいえ広告をセキュリティソフトが検知するのか？」…**

■一段上がるたびに「目黒のサンマ」化する報告書
- 「現場は状況を把握してるのか？」
- 「インシデント対応能力はあるのか？」
  - インシデント対応そっちのけで用語説明書の執筆会議

■どんどん遅れるインシデント対応報告
- 軽微なインシデントがアクシデント扱いに

結局、
「意味がわからん。技術用語を使え」
な指示

コストを考慮した対策の必要性

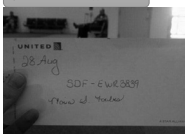


■システム全体を俯瞰する監視体制
- 膨大な情報機器と通信に対する監視
  - 平常時：全体をざっくりと俯瞰
  - 異常時：異常個所周辺を精査しつつ俯瞰も継続

■事前のアクシデント対処計画
- インシデントがシステム全体に及ぼす影響
  - 放置すれば深刻な事態に陥るのか？
  - インシデント対応(隔離)がシステム全体に及ぼす影響
- 何があっても止められない業務の運用継続
  - 通信制限、重点監視、代替手段の有無
  - 重要セグメントの構築(単独でも業務可能)

→アナログな対応の検討

停止状態の維持…

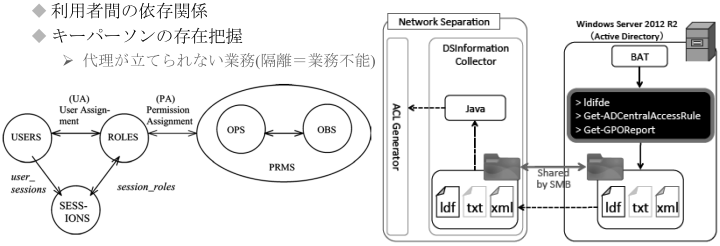


業務フローの把握…PC利用者の情報

■認証システム(Active Directoryなど)の情報を参照

■ロールベースアクセス制御の登場

- 業務フローの把握
  - 利用者間の依存関係
  - キーパーソンの存在把握
    - 代理が立てられない業務(隔離＝業務不能)

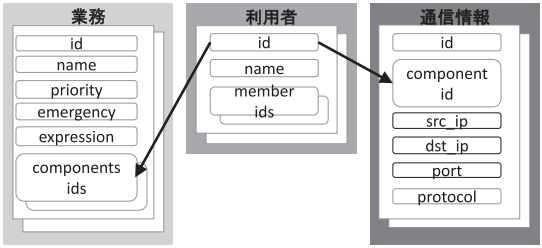


http://wiki.genexus.jp/hwiki.aspx?Role+Based+Access+Control+(RBAC%3A+ロール+ベース+アクセス制御),

業務-利用者-通信との関連性を把握

■業務を反映したアクセス制御

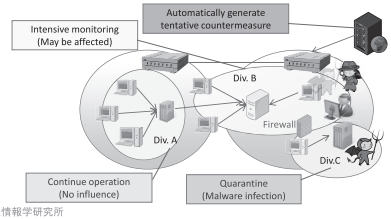
- 不要な通信を事前に遮断(予防措置、対策案の発散を防止)
- 重要な業務に使用する装置や通信の把握

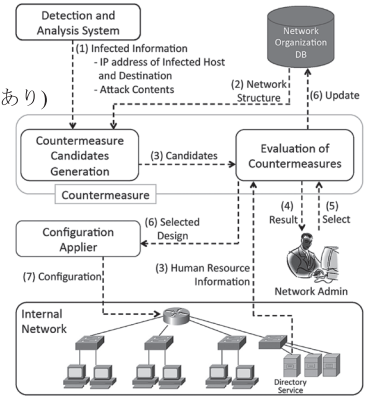


時間稼ぎによるパニック回避

■攻撃検知、ネットワーク構成情報等
- 複数の暫定対策候補を生成(事前作成もあり)

■各候補を評価
- 緩和策による効果
- 運用への影響





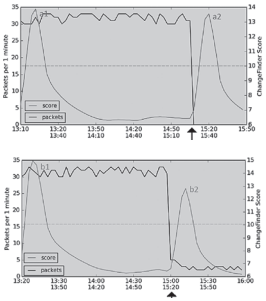
暫定対策の自動生成

■業務フローの情報に基づく
- 対策候補の効果と業務への影響度を数値化
- CSIRTと経営層が連携して最適な案を選択

候補	効果	影響度	総合判定
1. 部門A隔離(業務継続)	1.48	7.0	-0.85
2. サーバセグメント隔離	1.57	11.5	-2.26
3. 感染PC隔離(業務停止)	1.72	1.0	1.39
4. 感染PC遮断(業務継続)	1.87	0.5	1.71
5. サーバ保護	1.84	11.5	-1.99

暫定措置の効果と影響の評価

- 対策適用前後のネットワークの挙動変化を確認
  - 緩和策の効果
    - 攻撃通信を止められているか？
    - 不審通信を抑えられているか？
  - 運用継続への影響
    - 正常通信への影響度
    - 想定外の正常/不審通信の発生
- 評価結果に基づく暫定措置の更新
  - 新たな暫定措置と効果をオペレータに提示



最終的な対策が決まるまでの時間稼ぎ

コネクション番号	送信元IPアドレス	宛先IPアドレス	宛先ポート番号	想定外流量変化
Connection Number	Src IP	Dst IP	Dst port	
0	192.168.10.1	192.168.30.32	3306	
1	192.168.10.1	192.168.30.31	25	==UNEXPECTED CHANGE==
4	192.168.30.31	192.168.20.1	25	==UNEXPECTED CHANGE==

業務名	想定外業務変動率	想定内業務変動率	業務変動率	関連コネクション番号
Duty Name	Duty Unexpected Change	Duty Expected Change	Duty Change	Related Connection Number
duty0	0.25	0.25	0.5	[0, 1, 2, 5]
duty1	0.25	0.0	0.25	[2, 4, 5, 6]

21

米国の動き(1)

- DARPA Cyber Grand Challenge(2016)
  - 脆弱性検査(fuzz testing)
    - 様々なテストデータをプログラムに入力しプログラムを
    - バグを特定→攻略可能な脆弱性を探索
  - パッチプログラムの作成
    - 見つけた脆弱性に対する暫定パッチを作成する。
  - 攻撃プログラムの作成
    - 他チームのサービスプログラムを停止させる攻撃プログラムを作成
  - テストデータによる動作検証
    - 暫定パッチ適用前後での動作確認
- これを全て自動化
  - 推論エンジンを用いた攻撃開始のタイミング決定
  - 解析システム自身のクラッシュ対策
- DEF CON25 CTF(2017)へ

https://cgc.darpa.mil

22

優勝チーム(CMU)でもAIとは言えないのだが…

- ■推論システムを搭載…一世代前のAI
  - ● 人間が考えたシナリオ
  - ● 様々な条件に基づく動作指示
    - ◆ 脆弱性の可能性を発見
      - ➢ 深掘りするか？ 別の脆弱性を探すか？
        - • 推定した攻撃のインパクトに基づいて選択
    - ◆ 防御を優先するか？攻撃を選択するか？
      - ➢ 暫定パッチは副作用の確認などに時間がかかる
        - • 相手のシステムを止めた方が高得点だが…
      - ➢ 攻撃した瞬間に同じ弾が撃ち込まれるが防御できるか？
        - • 気づいていない他チームにヒントを与える可能性
    - ◆ 暫定パッチの動作検証はどうするのか？
    - ◆ 解析システム自体がクラッシュした際の自動復旧
- ■これらを全て自動化

米国の動き(2)

- ■MITRE Challenge IoT
  - ● 不正機器の発見技術
    - ◆ ただし、IoT機器やネットワーク構成には手を入れない
  - ● そのためには…
    - ◆ IoT機器ネットワークの状況把握が必須
      - ➢ 攻撃によりIoT機器が乗っ取られた場合に何が起きるのかを予測
- ■これって…
  - ● 多種多様な機器環境におけるサイバー攻撃対策
    - ◆ 常に動き回る機器…現在位置を把握できるか？
      - ➢ ノートPC、スマートフォン、PDA
    - ◆ サイバー攻撃による被害把握の必要性
      - ➢ 物理的な状態から不具合を判断できない

現在は組み込み機器
レベルではあるが...

https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot

サイバーセキュリティの研究動向(海外)

■自己免疫システム
- 未知の脆弱性の発見
  - セルフチェック
  - 攻撃手法の解析
- 暫定パッチの開発
  - IPSを用いた仮想パッチはすでに実用化
  - 暫定パッチの安全性検証

■被害状況に応じた最も効果的な対策を自動生成
- 被害拡大防止＆業務への影響を極小化
- ベストの対策ではない可能性はある
  - 人間のオペレータに考える時間を提供

国立情報学研究所

25

まとめ

■情報システムへの依存度増大
- 情報システム抜きの業務はありえない時代に
- 全面遮断による安全確保と業務停止
  - 二択しかない…という状況からの脱却

■攻撃による被害発生を前提とした対策
- 業務継続と被害拡大防止の両立

■耐性(レジリエンス)のあるサイバー攻撃対策
- ネットワークの区画化＆きめ細かいアクセス制御
  - ダメージコントロールとデグレーデッドオペレーションによる業務の継続
- 攻撃対策の事前策定
  - 想定漏れや想定外の副作用の把握
  - 自動化システムの研究開発
  - 人間の能力を超えた攻撃への備え

国立情報学研究所

26