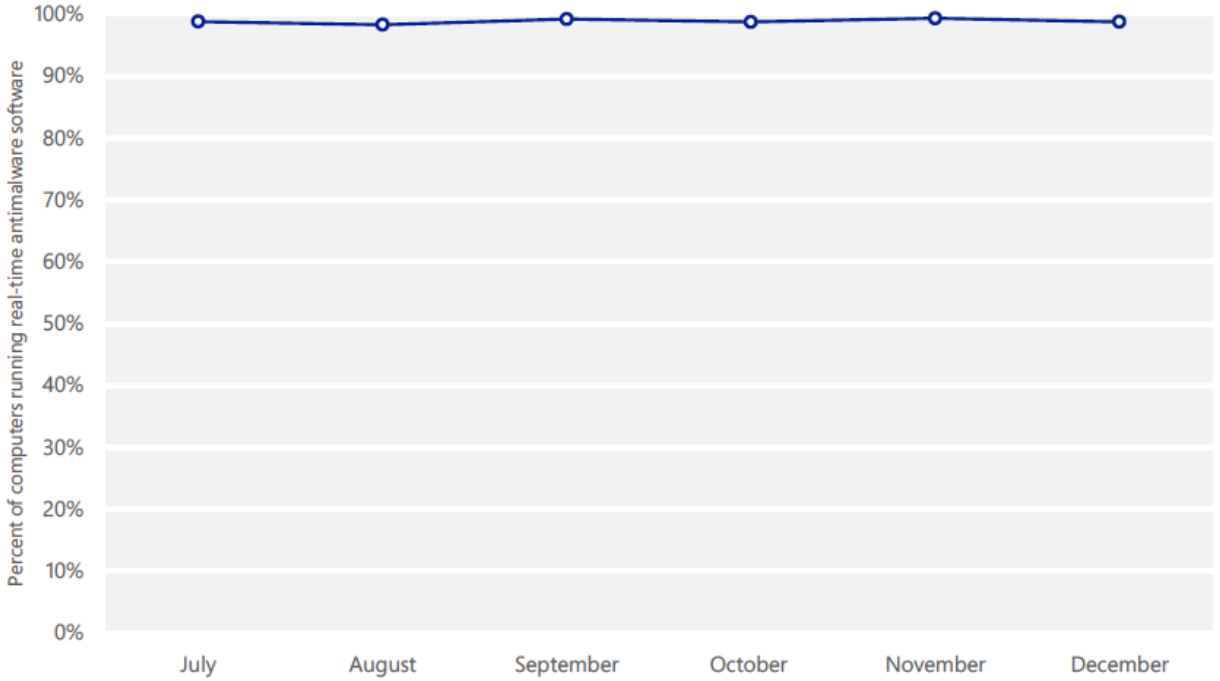
サイバー攻撃被害を軽減するための研究開発と人材育成の動向

高倉弘喜
国立情報学研究所

万全な対策...

- マイクロソフト
  - 60万台の機器
  - 15万人のユーザ
  - 100以上の国と地域
- 2015年後半
  - アンチウィルスソフト
    - 98%以上の使用率
  - アドウェア系: 100万件
  - トロイの木馬: 50万件
  - エキスプロ糸: 30万件

Figure 100. Percentage of computers at Microsoft running real-time antimalware software each month in 2H15



Microsoft Security Intelligence Report
Volume 20 | July through December, 2015

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: 80万(21万)
  - .dll: 60万(3万)
  - .temp: 30万(5万)
- 感染後に検知したマルウェア
  - .exe: 16件(111)
  - .temp: 9件(1)
  - .doc: 4件(番外)

括弧は2014後半

Figure 102. Top ten file types used by threats detected at Microsoft in 2H15

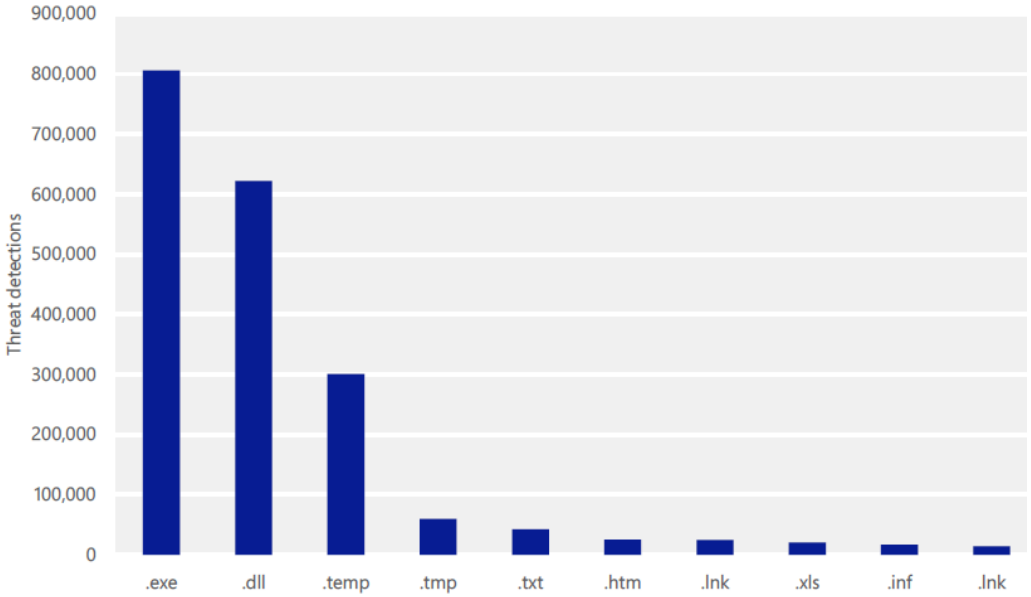
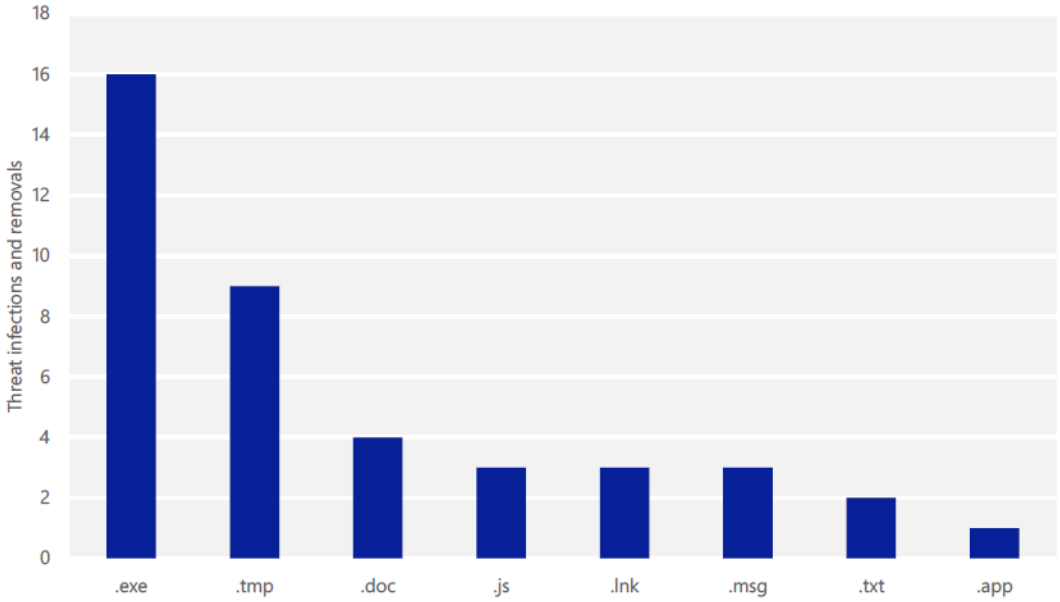


Figure 105. Infections and removals at Microsoft in 2H15, by file type



これでも対応が遅い…のか？

- 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

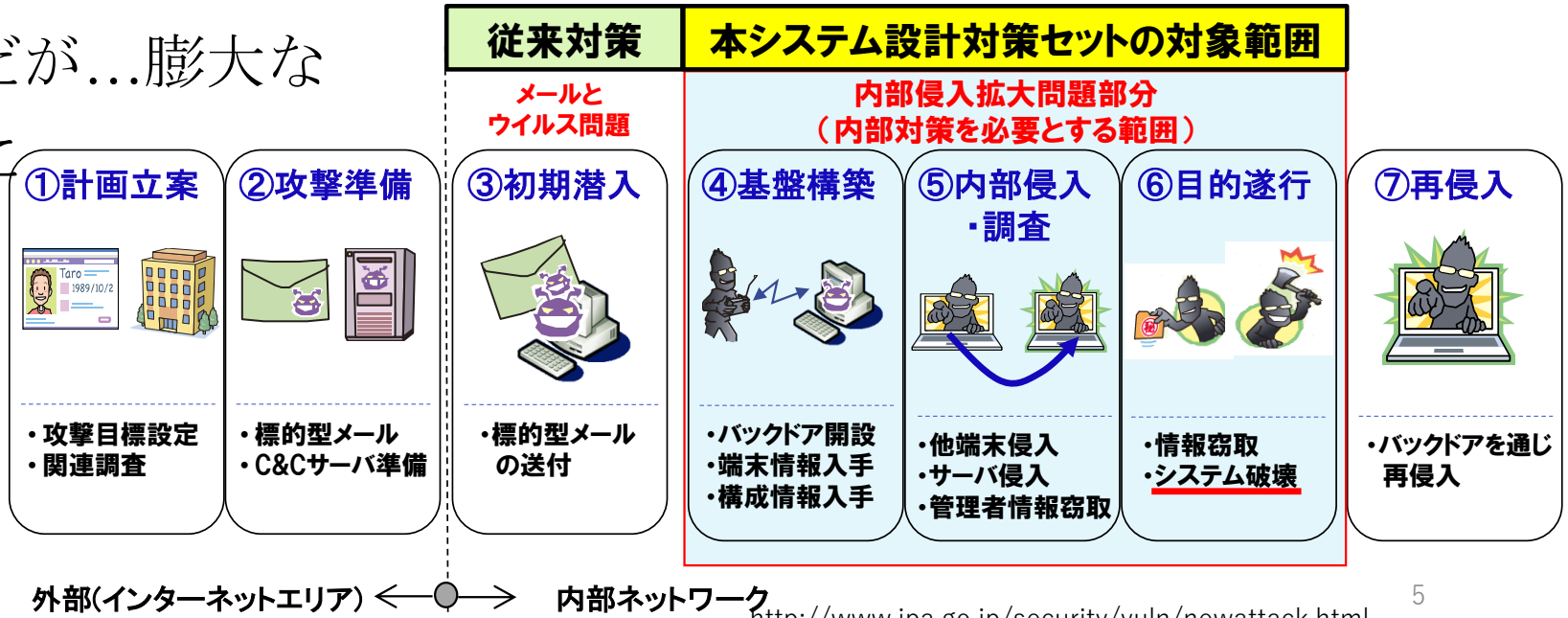
7日間

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

答えが分かった後で、目的遂行を許した責任を問われても…

- 不審通信が存在するのにマルウェアが見つからない
  →未知マルウェアの感染を疑うべき
- 謎の大容量ファイル、複数の不審通信の発生
  →マルウェアによる基盤構築や内部浸入・調査を疑うべき

そりゃそうだが…膨大な無関係情報に埋没した…



http://www.ipa.go.jp/security/vuln/newattack.html

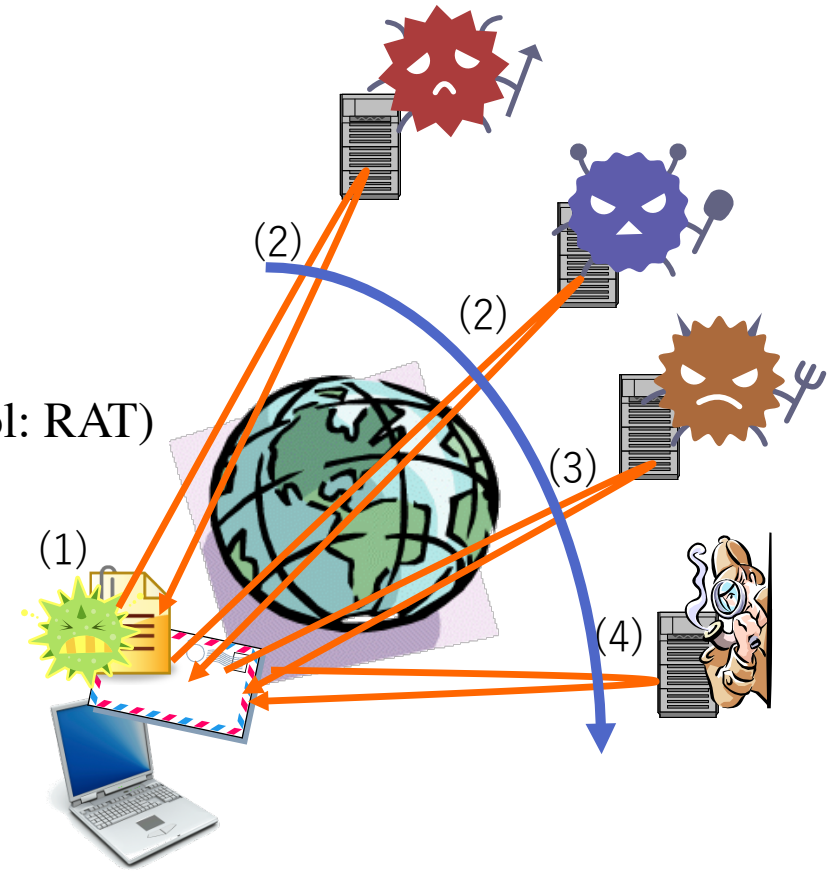
困難なインシデントの全貌把握

- 業務を装ったメール
  - いつもの相手先担当名、いつもの文面、いつもの添付書類
  - 添付書類やリンク先の無害化で対策するしかない？
    - 不自然な文面なら疑うべきなのか？…富山大情報漏洩事件
- 不審通信先の発見・調査
  - 膨大な不審通信先情報
    - 深刻な事態を招く通信先の炙り出せるのか？
  - クラウド活用の普及
    - 攻撃指令サーバもクラウドを活用
  - 通信先発見がスタート地点ではない
    - 発見以前は「情報がない」という情報をどう考えるか？
- 謎の大容量ファイル
  - バグによるコアダンプの可能性も想定(運用優先 v.s. セキュリティ優先)

初期潜入後の基盤構築

■誤判断の誘導とステルス化

1. トロイの木馬
   - ◆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を阻止
   - ◆指定通りの手順か？何人めの感染か？
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

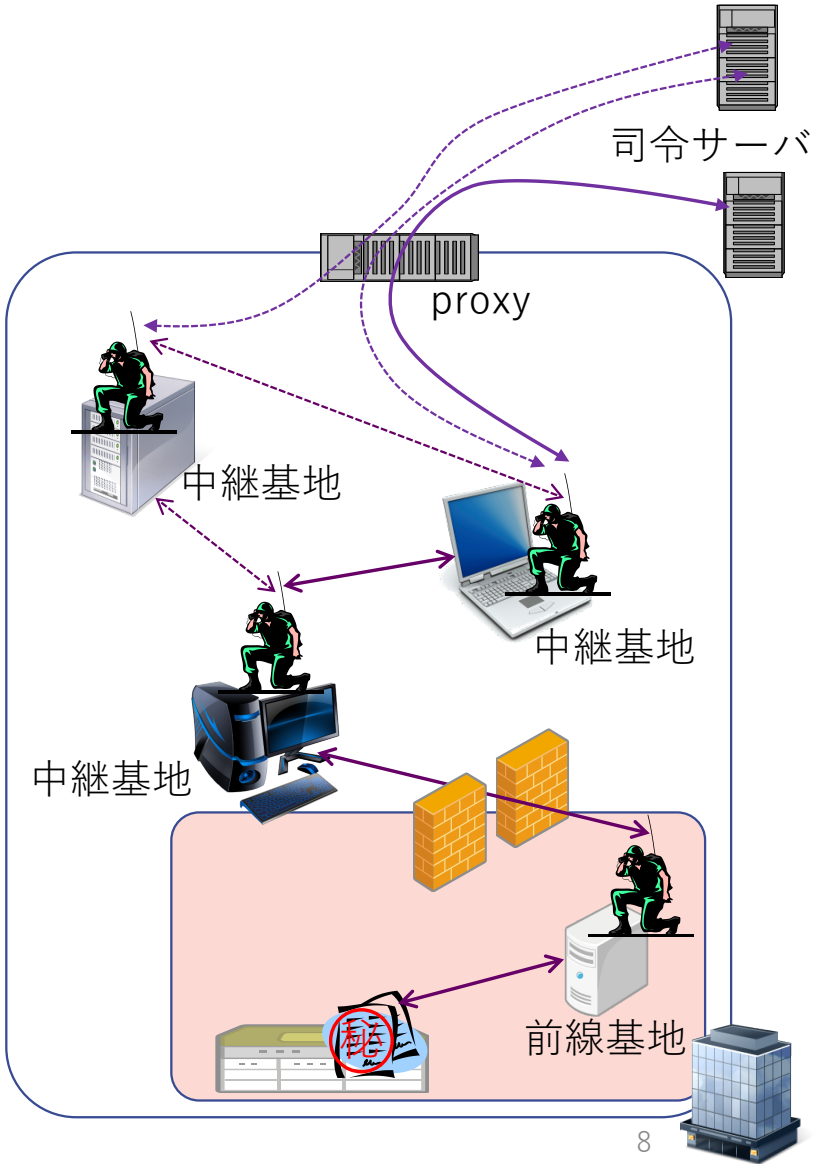


組織内部への侵食

- 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



アクシデント化の恐怖…たった数台のマルウェア感染で

- 全ネットワーク遮断
  - 顧客サービス停止
- 年金機構でも…
  - 年金給付は継続稼働
    - 終息時期の予測不能
      - 長期の停止は人命に関わる
    - 被害の影響が及ばないことを確認
      - 100%の安全宣言？
      - 永久に復旧できない
- 個々のインシデントのトリアージ
  - アクシデントに発展するか？

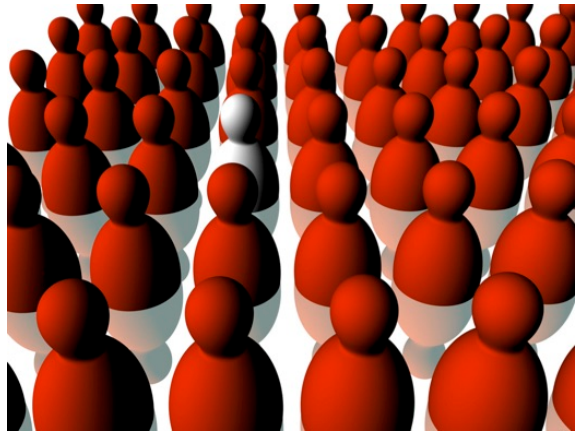
報道日時	被害組織	感染台数	発端	原因	対応状況
2016年6月22日	新城市	新城消防署PC2台	不明	不明	市役所を含むネットワーク遮断(6月21日～22日まで)
同日	静岡市	静岡市役所PC1台	警察からの情報提供	不審メールの開封	初期化済み(6月2日) 情報提供後インターネット接続遮断
同日	御前崎市	1台 (他感染可能性のあるPCあり)	警察からの情報提供	不明	マルウェアの駆除、初期化
同日	三豊市	市役所内PC4台	警察からの情報提供	不明	インターネット接続遮断
2016年6月25日	群馬県	県庁内PC1台	自組織にて検知 外部より情報提供あり	ばらまき型メールの添付ファイル開封	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ものと推定	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。

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

全体を俯瞰したインシデント対応とアクシデント体制

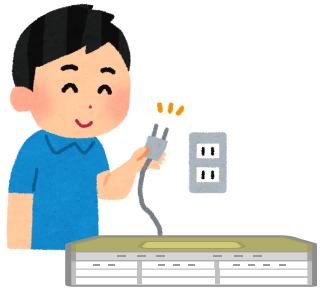
- IT…単なる文房具から業務支援の要へ
  - 闇雲に見張れば良いというものではない → 毎年何十億円かかるのやら…
    - 組織内の全てのネットワーク装置で監視＆自動解析
    - 24/365の有人監視によるインシデント対応
- 侵入を前提とした効率的な監視体制
  - 全体俯瞰による状況把握(各種ツールの登場)
    - 不審な外部通信や見慣れない組織内通信の確認
    - 初動対応：記録の欠落や矛盾の発見
  - トリアージによる判断
    - 単発のインシデント or 業務に影響するアクシデント

    CSIRTの仕事はここまで
- アクシデント確認時の体制切り替え
  - CSIRTによる戦略立案と経営層による判断

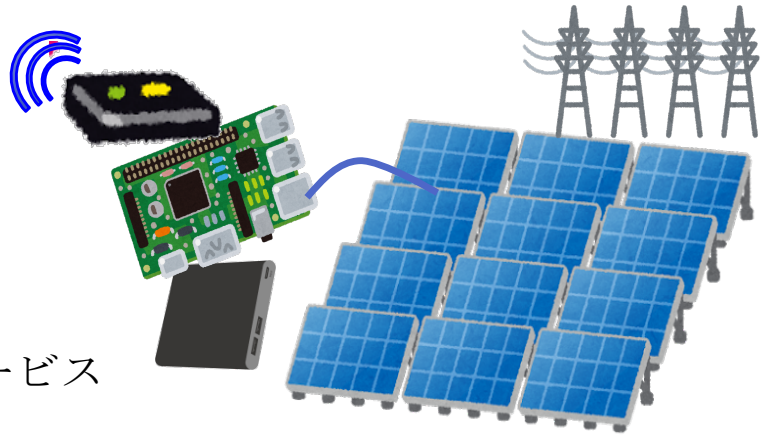


多種多様化する情報機器…IoT時代

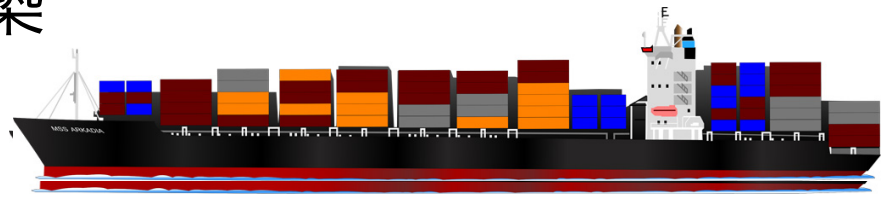
- セキュリティ軽視なIoT技術導入
  - 低価格で高機能を実現
    - 拡張性に余裕のないハードウェアリソース
      - セキュリティパッチ適用という概念がない
    - その割に長い製品寿命…10年以上も珍しくない
- 単純な通信プロトコル故の…
  - バレたあとの暗号化？
    - 選択的平文攻撃
      - しかも、パターンはごく少数
- 大量導入によるコスト効果が裏目に
  - 設置後の改修作業のコスト
    - 450万台のWebカメラのfirmware無償更新サービス
      - 回収＆再設置費用は？



FW/IDS/VPN

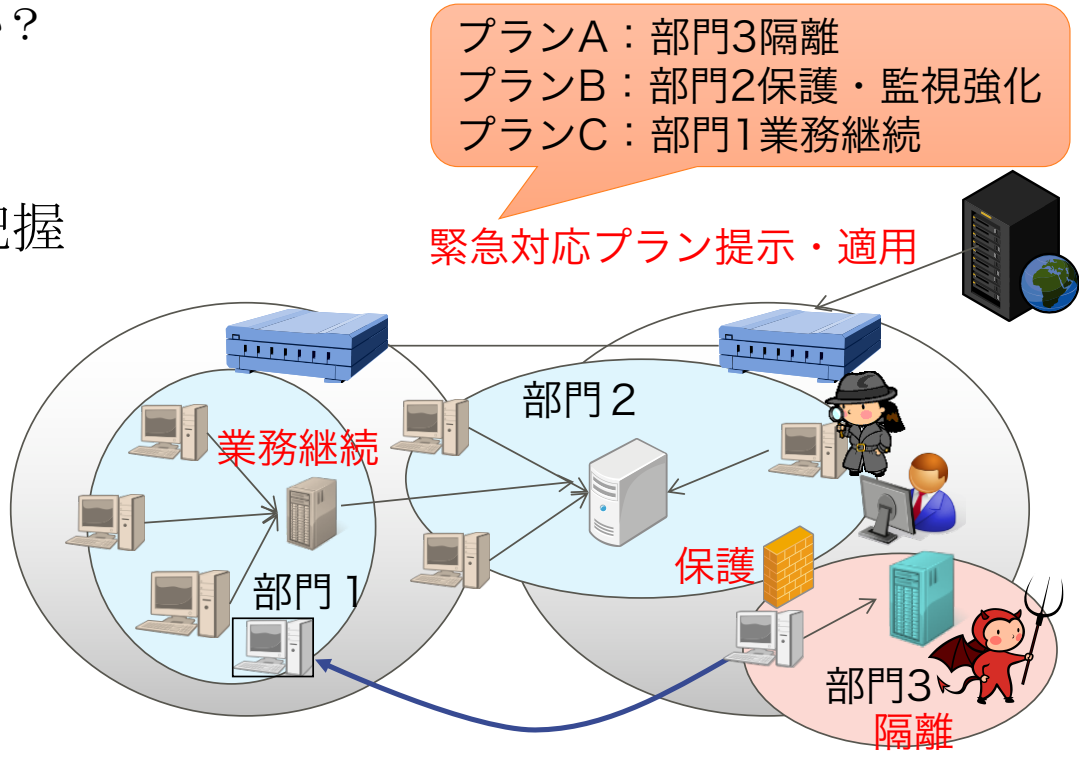


レジリエントな情報システムの構築



- ITの全停止は許されない時代に
  - 隔離による業務全体への影響を確認
    - 認証系やサーバ系は継続利用可能か？
    - 他部門との情報伝達手段は？
    - 組織外との通信の必要性は？
  - 停止による業務全体への影響を把握
    - 他部門で代行可能な業務か？
      - 必要なデータや情報機器は？
  - 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
    - パニック状態で悩むのは危険

で、誰が指揮を執るのか？

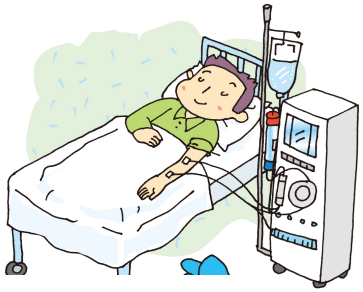


事前に立案するアクシデント対応(ダーメージコントロール)

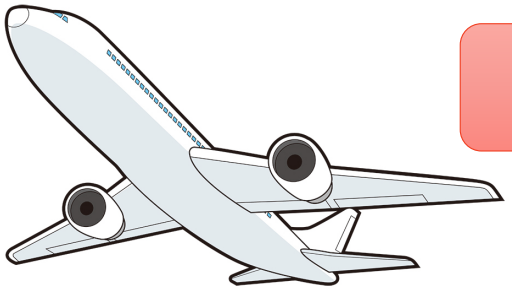
- 情報システム単体ではなく業務単位で事前に考えておく
  - デグレーデッドオペレーション(縮退運転)を検討

アクシデント発生でパニクっている時には判断できない

    - 止められない業務
      - 情報システムが止まっても継続
        - 担当者が張り付いてでも、後で巻き戻し作業が入ってもシステム運用継続
          - 集中治療室



    - 止めてほしくない業務
      - 代替策の有無(アナログなものでも良い)
        - システム停止も選択肢の一つ
          - 手書き搭乗券
    - 止めるしかない業務
      - 代替策がない
        - 業務停止(経営判断が必要)
          - 重量管理システム



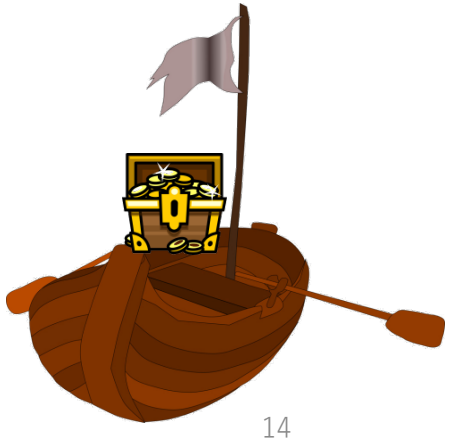
自動対応を謳う製品の登場

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「部品」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？
    - センサーまでの回線が生きている…も情報
- 個々の「部品」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…)

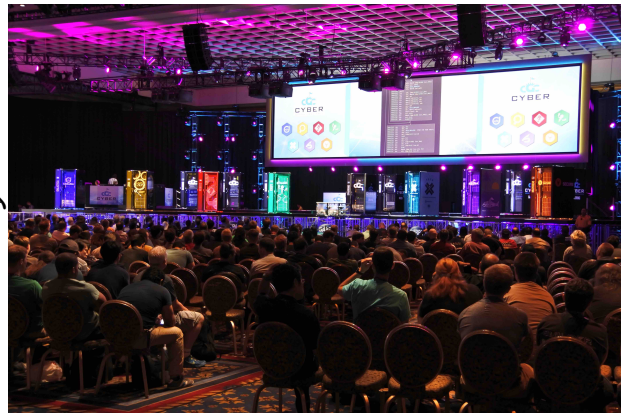


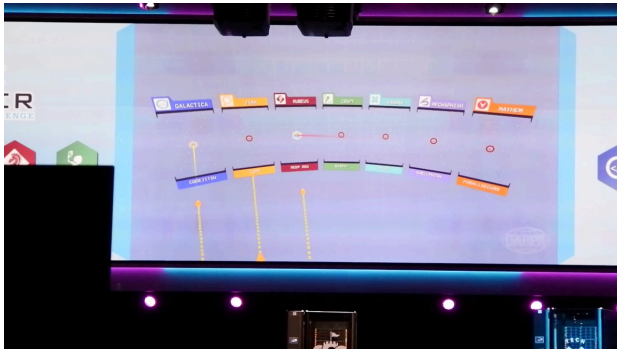
サイバーセキュリティ関連技術の動向

- 自動化の流れ
  - 推論システムや機械学習技術の活用
    - AIはまだまだこれから
  - 脆弱性自己検出・自動防御(自動攻撃)
  - 被害機器と規模の特定
- インテリジェンス情報
  - ただし民間向けインテリジェンス情報の限界
    - それでも膨大な玉石混交情報の精査
      - リスク評価(自組織に対する)
      - 対策立案
    - アナリストが必要
- 100%の安全確認ができない現状
  - 技術的なマインドでは判断不能→経営的判断が必要に

自動化の例…米国の例(1)

- DARPA Cyber Grand Challenge
  - 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
    - 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…今は小規模ソフトが限界とはいえ…
  - 推論システムを用いた攻撃のタイミング決定
  - 解析システム自身のクラッシュ対策





https://cgc.darpa.mil

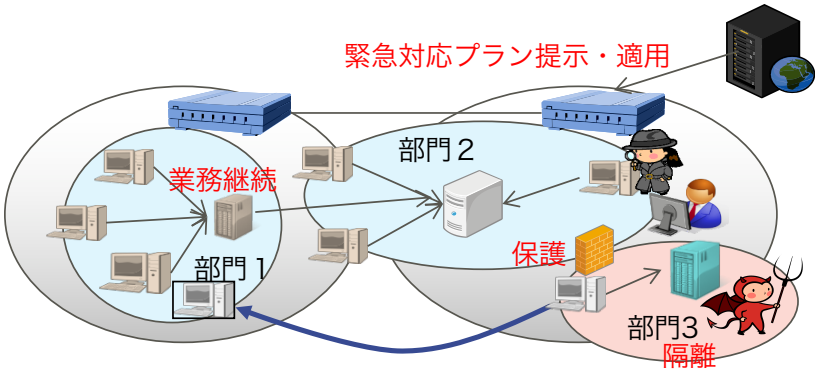
自動化の例…米国の例(2)

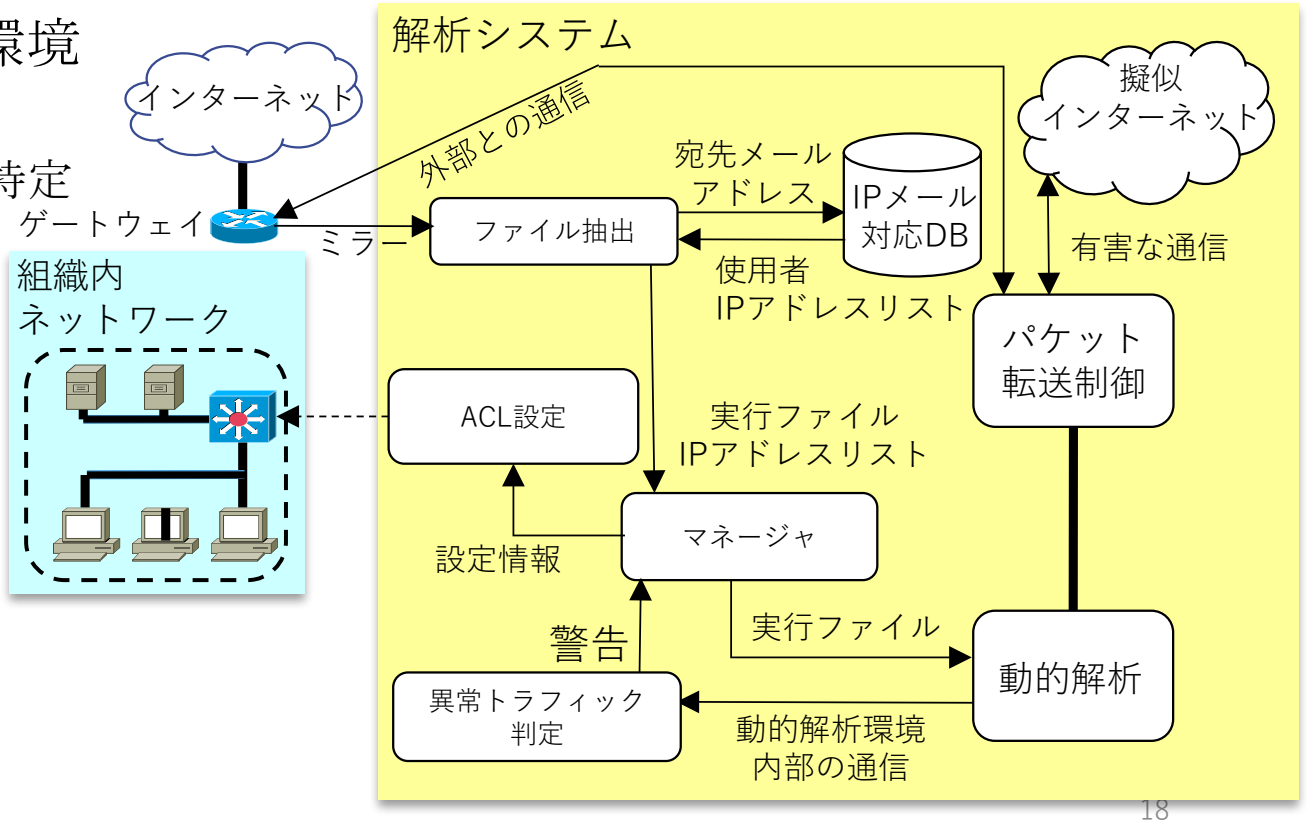
- MITRE Challenge IoT
  - 不正機器の発見技術
    - ただし、IoT機器やネットワーク構成には手を入れない
  - そのためには…
    - IoT機器ネットワークの状況把握が必須
      - 攻撃によりIoT機器が乗っ取られた場合に何が起きるのかを予測
- これって…
  - モバイルIoT機器におけるサイバー攻撃対策
    - 常に動き回るIoT機器
      - Linux制御の照準器
        - 2015年のblackhat USAで脆弱性報告
    - 当然発生するサイバー攻撃による被害

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

手前味噌な例

- 被害状況に応じたインシデント対応
  - 業務継続と被害軽減の両立を自動化
  - 組織内NW全体の模擬環境
    - マルウェア活動を追跡
    - 感染範囲・攻撃目標を特定
    - 攻撃状況に応じた対策
  - 対策による副作用確認
    - 業務効率の変化を注視



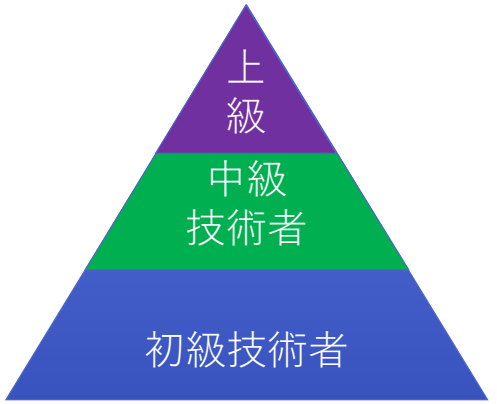


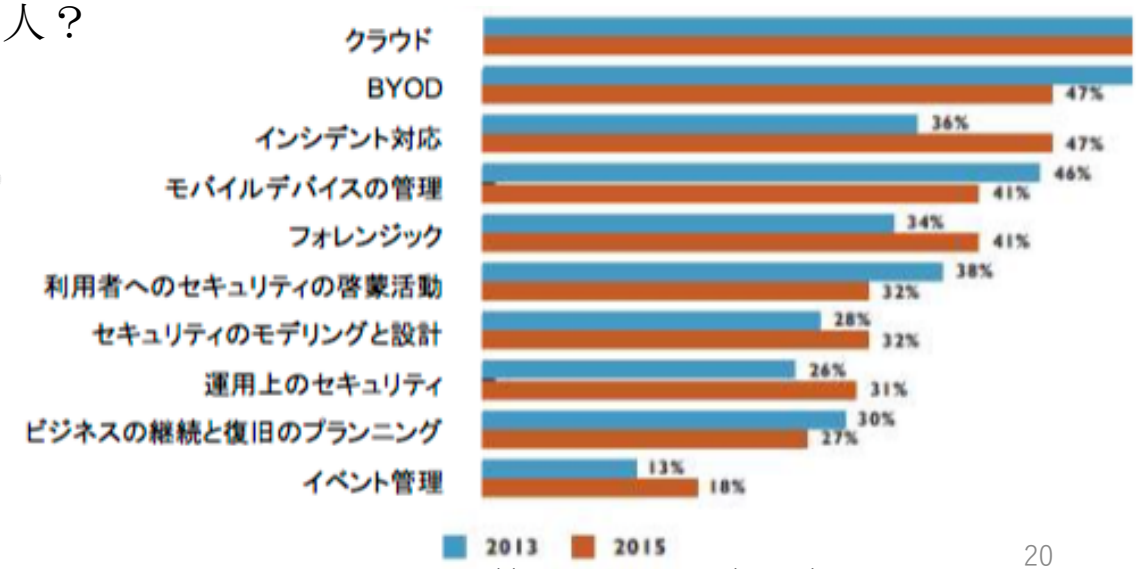
情報共有(Information Sharing)

- 米国での情報共有
  - 被害企業から提供される情報
  - **政府機関(FBI, CIA, DHS)が収集する情報**
    - 匿名化等をほとんど施さずに政府系から降ってくる
  - 業界によっては役職(担当)ごとに存在する横串型ISAC
- 膨大な共有情報の分析と対応
  - 各社や各員の責任
    - 情報提供を受けていたにも拘らず適切な…なときの罰則の存在
  - 1社あたり数千人のセキュリティエンジニア・アナリストの採用
- 我が国で同じ規模のコストがかけられるか？
  - 法制度の問題
  - とはいえ、米国との連携の流れ

サイバーセキュリティ人材に求められる能力とは？

- よく言われる
  - サイバーセキュリティ人材不足は本当なのか？
  - 上級、中級、初級技術者とは何者なのか？
    - 教育でステップアップするものなのか？
  - 能力不足って、何の能力が不足しているのか？
    - 分野的には…なんでもできる人？
      - フォレンジック
      - イベント管理能力

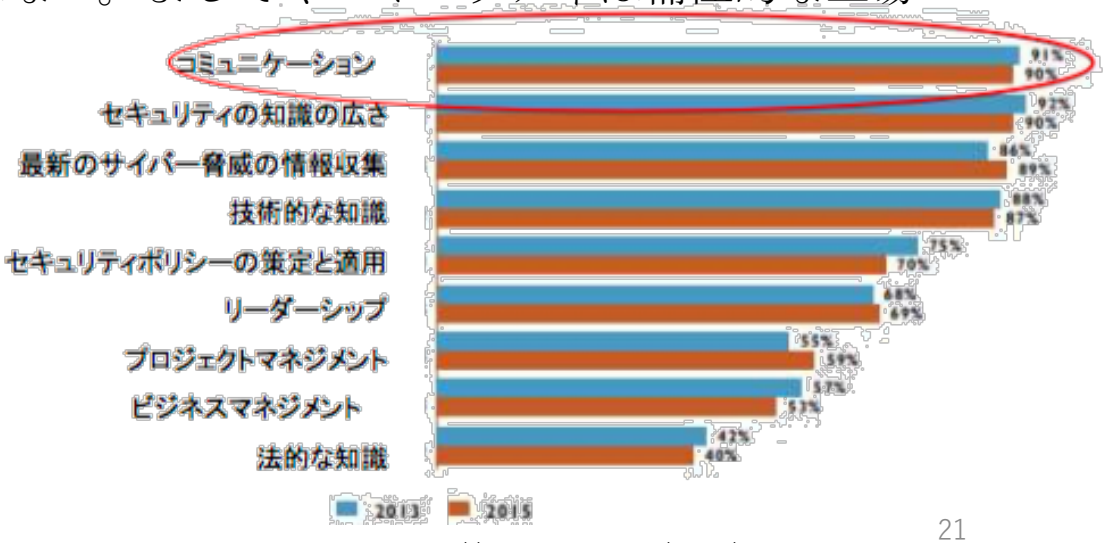




https://www.ipa.go.jp/files/000050299.pdf

企業が求める能力

- 実はコミュ力
  - 技術用語から役員用語への翻訳…これが一番難しい
    - 事実関係だけに興味があるエンジニア
    - 経営への影響だけに興味がある役員
  - 関係部門との調整
    - 情報システムは業務そのものではない。ましてやセキュリティは補佐的な立場
      - 停止や縮退による影響把握
      - 影響緩和策を議論
- マネジメント能力
  - それセキュリティですか？
- 広大な知識が必要
  - 技術、法律、経営…

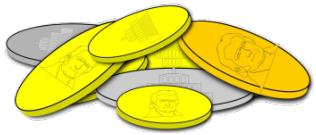


https://www.ipa.go.jp/files/000050299.pdf

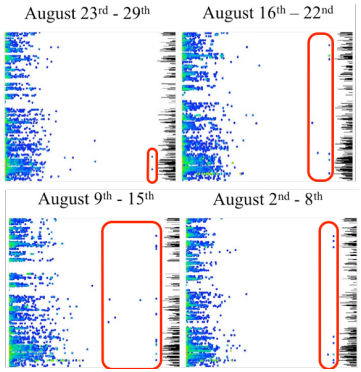
つまり本当に欲しい人は…危機管理のプロ

- スーパーマン？
  - 技術屋ではないことは確か
  - 社内に居るか？
  - 社外から呼ぶ？
    - 社内事情に詳しい部外者って誰？

法律の知識



経営の知識



アクシデント分析と管理

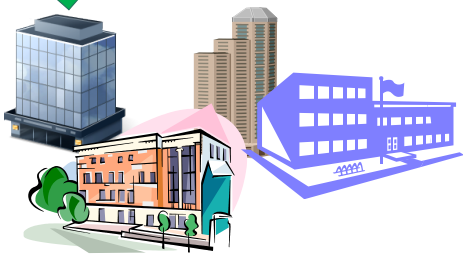
CSIRT

ネットワーク技術
セキュリティ技術
実務経験

戦略立案・助言
役員との意思疎通

状況変化に応じた
的確な判断と指示
(トリアージ能力)

外部機関との連携



人材育成...韓国の場合

- 知られているのは...
  - 120名から10名を選抜
    - 座学による学習
    - 演習による実践経験
    - 最終認定によるTop Gun
  - 各段階に応じた就職先の斡旋
- ただし
  - 高経験の上級技術者
    - 教育で育てられる
    - 素質は重要だが
  - 戦略立案能力の修得
    - 数年では養えない

認定10名

教育120名以上

競技30名

参謀(指揮官候補)育成は別パス

目立つことはない

- 陸海空軍から下士官を毎年4名選抜し修士課程へ
  - 2名 米国
    - CMU、スタンフォード、MIT、士官学校
  - 2名 日本
    - 早稲田、防大、名古屋
  - 学習目的
    - 若手セキュリティエンジニアの思考パターン
    - アクシデント発生時の対応手順の修得
- 帰国後一定の研修後
  - Top Gun卒業生達の指揮
  - サイバー部隊の司令官を補佐
  - 退役して民間のサイバーセキュリティ部門管理職へ

職人気質のエンジニアを
使いこなすための実務経験

必ずしもサイバー技術に
精通している必要はない

欧米企業におけるサイバー
セキュリティ管理職と同じ

日本のセキュリティ人材育成の課題

- 正義のハッカー育成に注力
  - ある意味一匹狼の大量生産
    - 得意な課題には飛びつくが…
      - 苦手な課題は後回し…ログの目視確認とか…
      - 新たな技術への適応
    - チームプレーは大の苦手
      - 全体を俯瞰した自身の立ち位置理解が難しい
    - コミュニケーション能力の問題
- 指揮官(橋渡し)人材不足が顕在化
  - 技術知識＋
    - 法律、経営、
    - 戦略立案・遂行
    - 技術者の人心掌握
    - 顧客対応能力…忍耐力

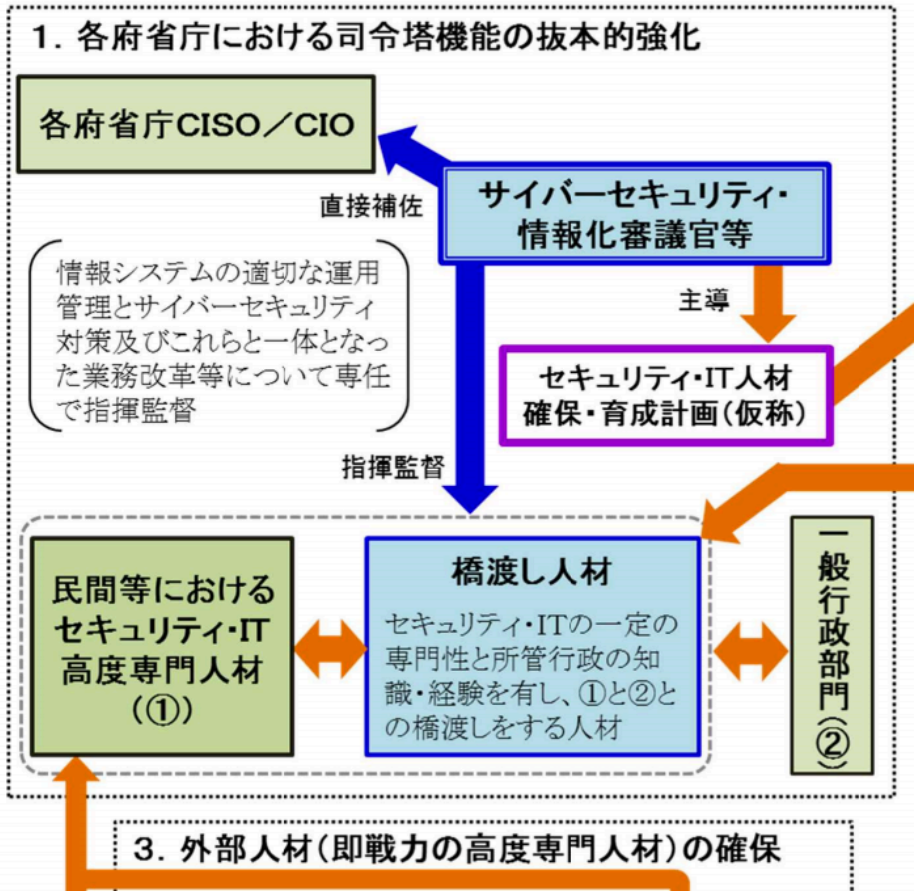
彼らのキャリアパス問題

愛せキュ無罪な発想にまで…

座学や演習だけでは修得困難

橋渡し人材の育成が急務に

- 橋渡し人材
  - インシデント対応
    - 技術的知識
  - アクシデント対応
    - 経営的知識
    - その組織の歴史的背景…さらに無茶な
- 組織で育成するしか無い
  - 霞ヶ関でも自力育成に舵を
    - ただし専門知識の習得は専門機関に委託
      - 民間セキュリティ企業、国の機関、大学
    - 4年間で1,000人程度

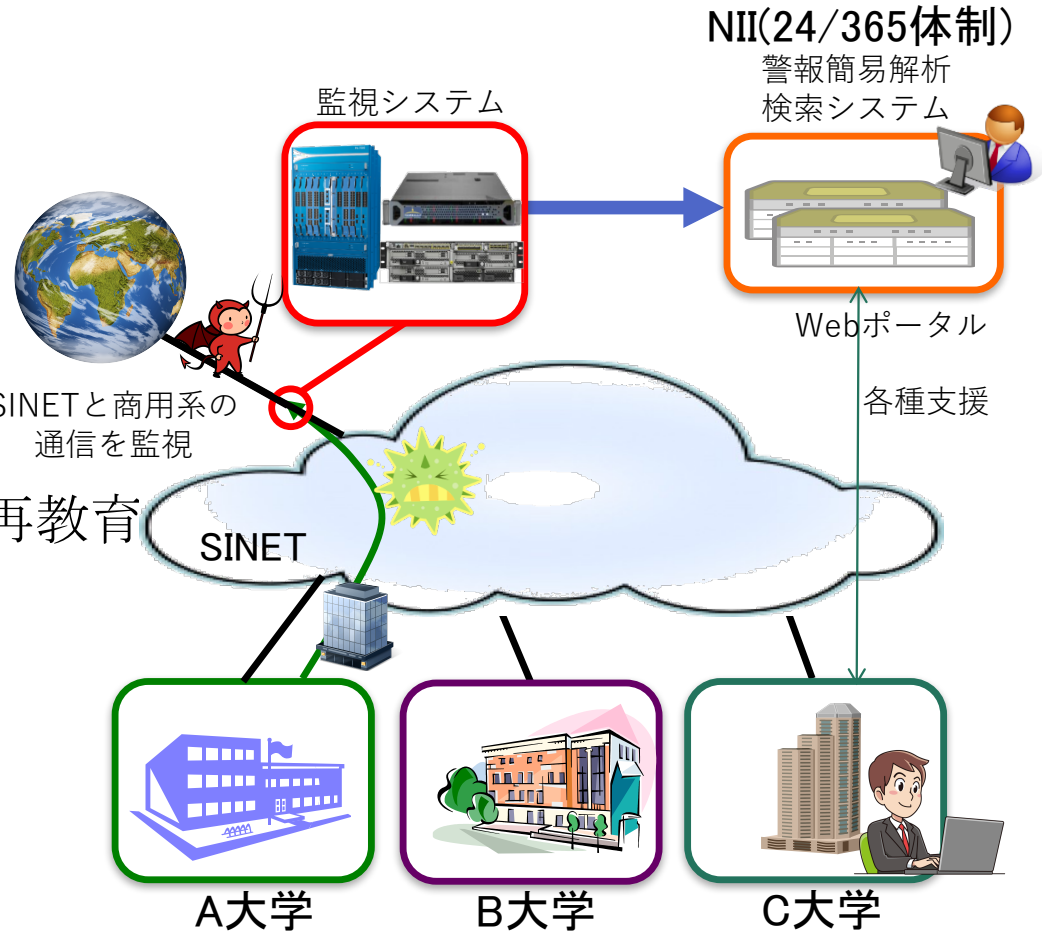


【政府機関におけるセキュリティ・IT人材の育成】
1．各府省庁における司令塔機能の抜本的強化
2．橋渡し人材（部内育成の専門人材）の確保・育成
3．外部人材（即戦力の高度専門人材）の確保
4．一般職員の情報リテラシー向上

http://www.nisc.go.jp/active/kihon/pdf/jinzai_kyoka_hoshin.pdf

大学も橋渡し人材の育成へ

- 大学ごとに異なる組織文化
  - 学問の自由を保証
    - (ある程度)開かれたネットワーク環境
  - 職員ではない学生や滞在者の存在
    - 外部専門家の採用だけでは難しい
- 組織内部での人材育成
  - 学内のネットワークエンジニアの再教育
    - サイバーセキュリティの知識
    - 大学経営の視点からの判断
    - 役員への助言
  - 視野の広い学生教育
    - 危機管理を意識した○○学



まとめ

- 高度化するサイバー攻撃対策
  - 攻撃によるインシデント発生を前提とした対策
    - アクシデントに至る前に極力阻止
    - アクシデント発展確認時の速やかな体制変更(指揮権をCSIRTから経営陣へ)
- レジリエントな情報システム構築
  - ダメージコントロール＋デグレーデッドオペレーション
- 橋渡し人材育成の必要性
  - 単なる技術屋ではない
    - むしろ技術屋ではない場合も(新たな技術の登場＋AIC的な判断)
  - 技術屋と経営層両方の考え方が出来る人材
    - 借りてこれるものではない
    - ある程度は自組織での養成が必須に…