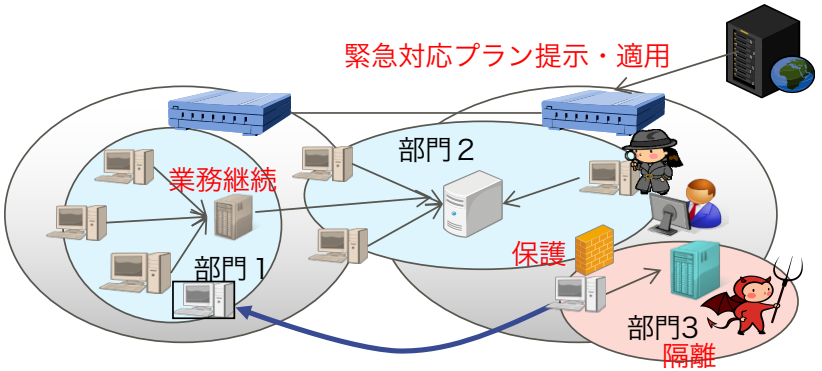
自動化の例…米国の例(2)

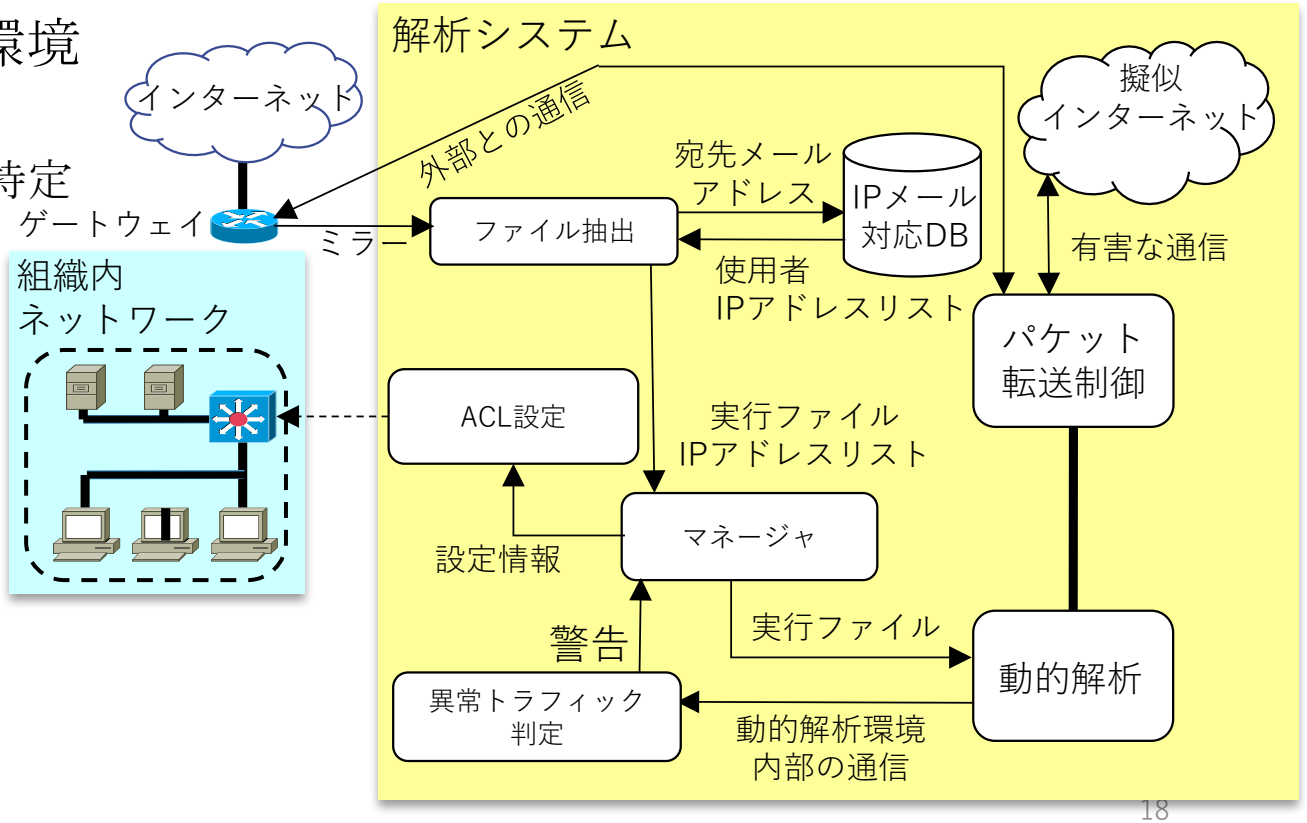
- MITRE Challenge IoT
  - 不正機器の発見技術
    - ただし、IoT機器やネットワーク構成には手を入れない
  - そのためには…
    - IoT機器ネットワークの状況把握が必須
      - 攻撃によりIoT機器が乗っ取られた場合に何が起きるのかを予測
- これって…
  - モバイルIoT機器におけるサイバー攻撃対策
    - 常に動き回るIoT機器
      - Linux制御の照準器
        - 2015年のblackhat USAで脆弱性報告
    - 当然発生するサイバー攻撃による被害

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



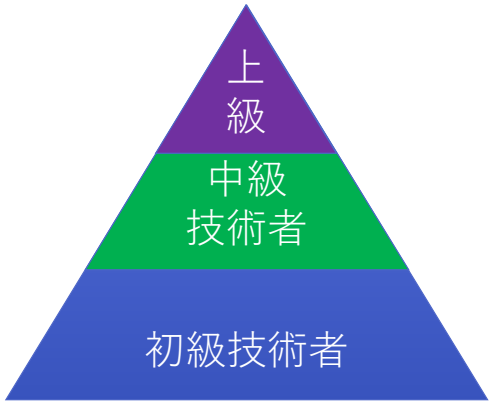


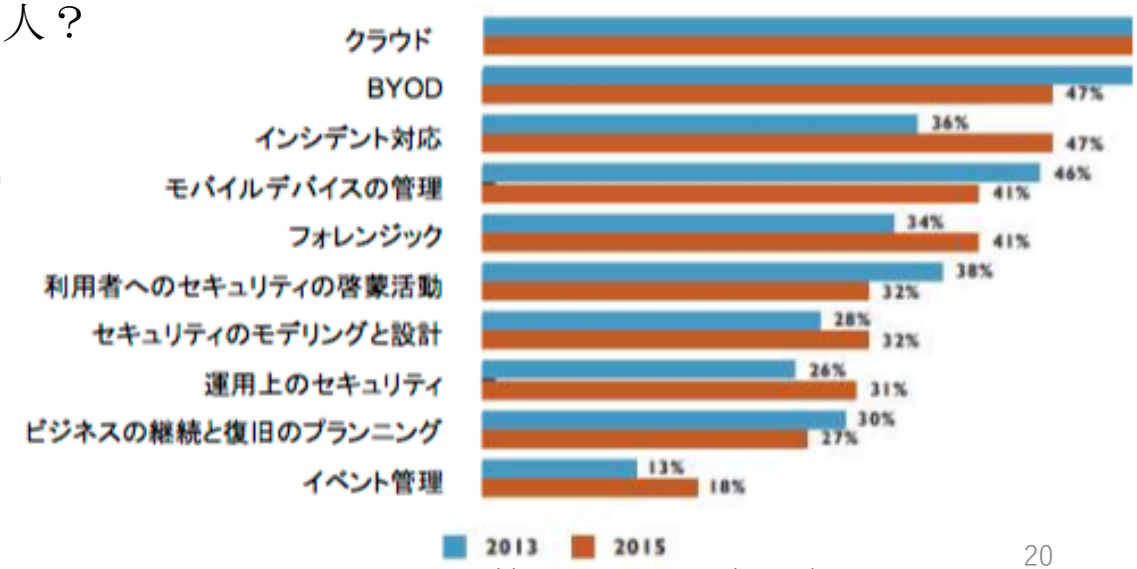
情報共有(Information Sharing)

- 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

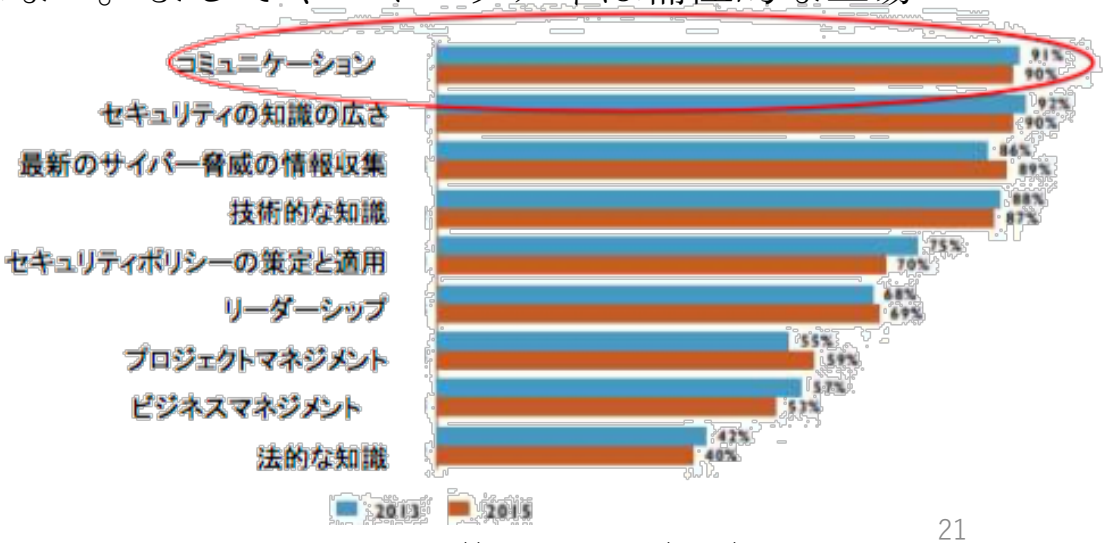




https://www.ipa.go.jp/files/000050299.pdf

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…

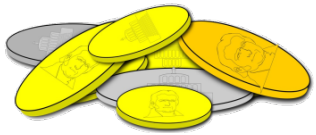


https://www.ipa.go.jp/files/000050299.pdf

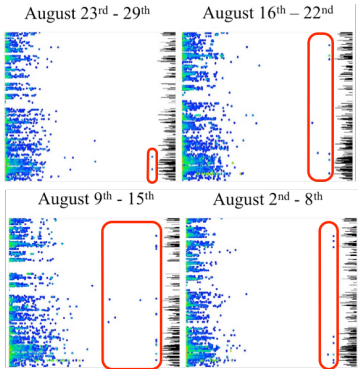
つまり本当に欲しい人は…危機管理のプロ

- 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

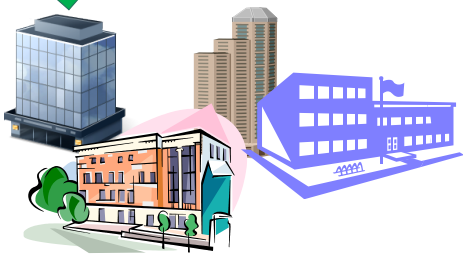
CSIRT

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

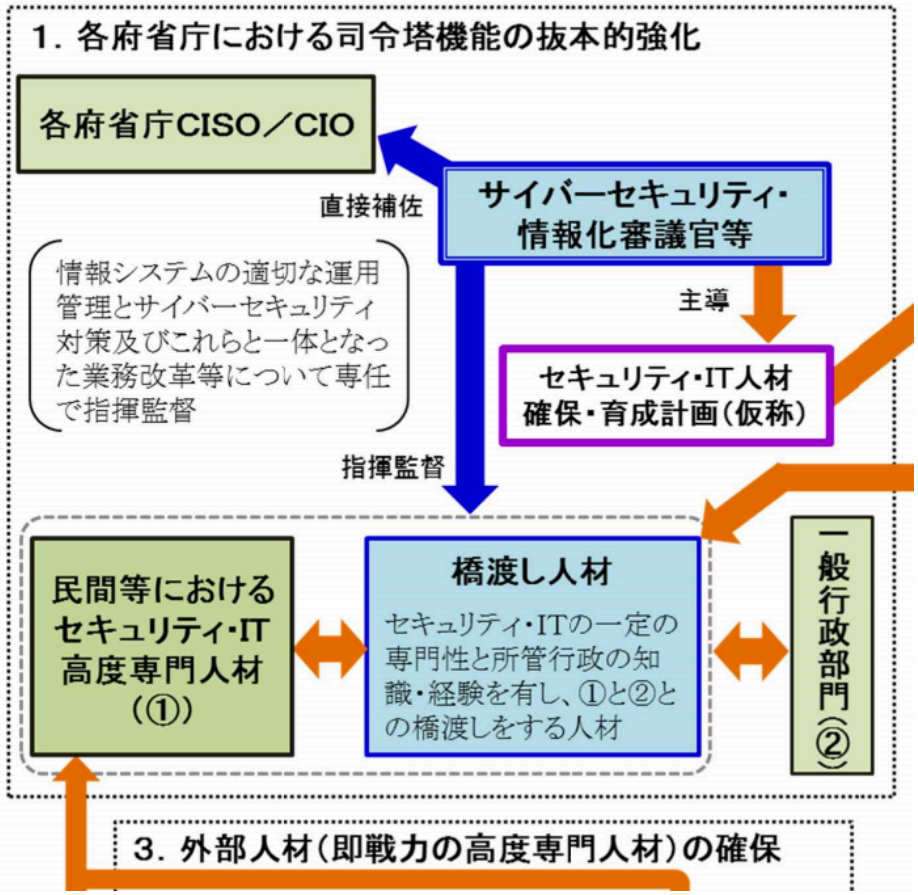
彼らのキャリアパス問題

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

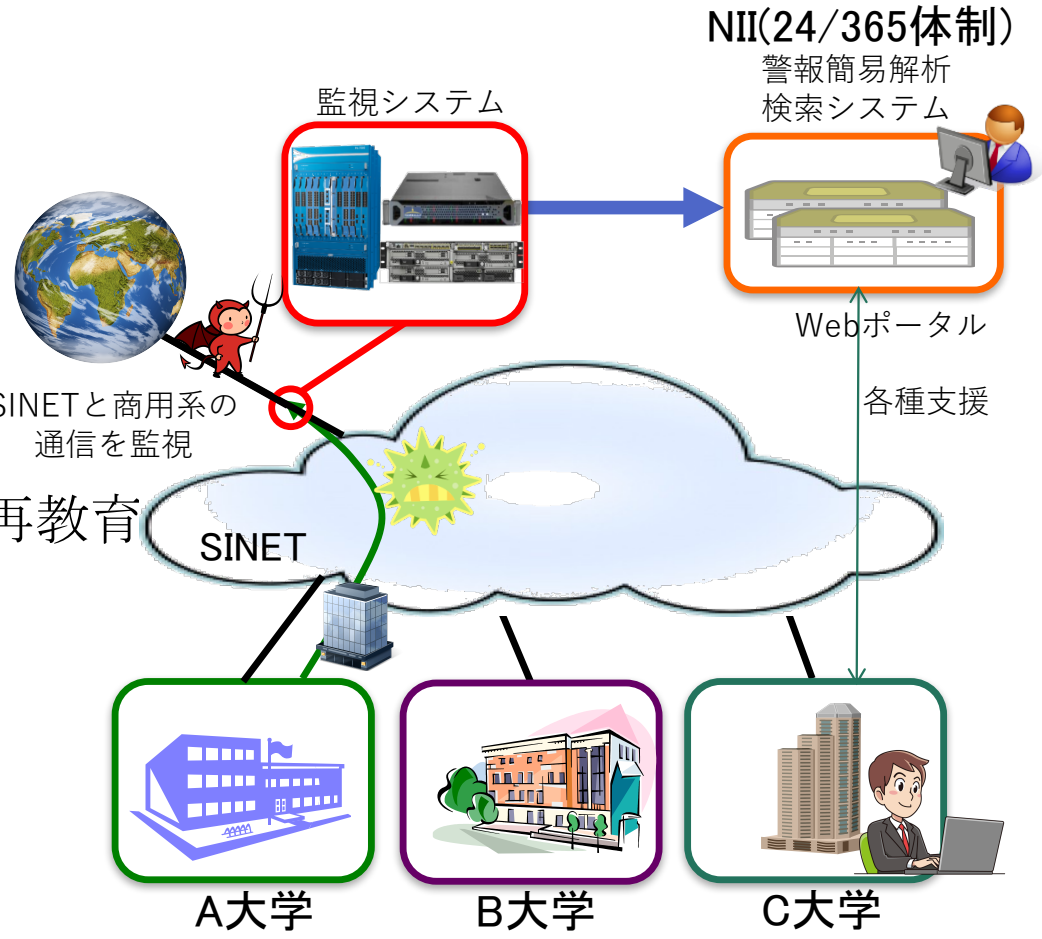


【政府機関におけるセキュリティ・IT人材の育成】
1．各府省庁における司令塔機能の抜本的強化
2．橋渡し人材（部内育成の専門人材）の確保・育成
3．外部人材（即戦力の高度専門人材）の確保
4．一般職員の情報リテラシー向上

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…