危機管理時における情報管理
～エリートパニックを引き起こさないために～

高倉弘喜
国立情報学研究所

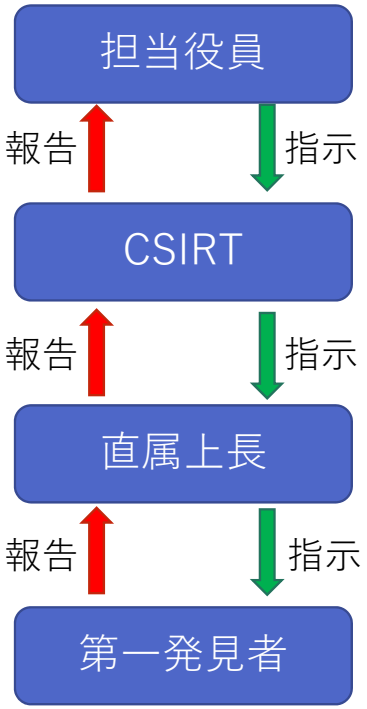
学術研究機関独特の文化

- 教育を重視、研究も重視
  - 学生という民間人の存在
    - 私物持ち込みの制限はできない
      - ノートパソコン、スマートフォン
  - 学問の自由と部局自治
    - 研究者として情報発信は当然
      - 規制に対する抵抗感
- 一方で、サイバーインシデント時には…
  - 積極的な情報開示は…隠蔽体質とも受け止められる
  - 研究者のマインドが仇に
    - 丁寧に説明すれば…
- 情報管理含めて危機管理であるという認識の欠如

サイバー攻撃への備え

- 危機管理体制の構築
  - CSIRT(Computer Security Incident Response Team)の設置
  - 緊急連絡網の整備
    - 第一発見者から担当役員まで
  - 意思決定手順の整備
    - 緊急対応を誰が判断してどう伝達するのか？
  - 関係先への連絡手順
    - 担当役員から報告？
- 伝達手段は…電子メール？電話？
- 土日・夜間はどうする？
  - 通じない報告先の存在

想定通りに事が進まない危機管理



水柱一本インシデントで轟沈する…

- 某クラウド事業者
  - 構築中だったサーバ
    - 個人情報は…なぜ無いのだ？
  - 5秒で自主的に遮断…
    - そんなありがたい裏オプション…
      独り占めとはけしからん！
- アクシデントへ
  - NHKで報道
  - 技術に偏った情報提供
    - 無かったことがあったことに…
  - 国会対応
    - 質疑時間の大部分が研究所の紹介

2015年06月09日（火）
国立情報学研究所 サーバー乗っ取られ悪用

東京にある国立情報学研究所の「サーバー」と呼ばれるコンピューターが、５日間にわたって何者かに乗っ取られ、海外の民間サイトに対するサイバー攻撃に悪用されていたことが分かりました。

誰がどこに報告するのか？

- 第一発見者/情報機器の管理者→…→担当役員
  - 直接なのか、間に連絡網の全員が挟まるべきなのか？
- 担当役員→監督官庁→NISC→セキュリティ機関
  - 伝言ゲーム問題の発生
  - 通じない技術用語 v.s. NISC/セキュリティ機関が求める技術的説明
- 不確定情報下での意思決定
  - どこまで報告すべきなのか？
    - 未確定情報は出さない → 「なんで報告しなかった？」
    - 未確定情報はその旨を添えて出す → 伝言ゲームの過程で「確定情報」に

そもそもサイバー攻撃被害はサイバー問題なのか？

エリートパニックの原因

- 全ての用語を理解して判断したがる公務員の性
  - 「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！
        - 「不要なポステイ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？」…

        どんどん疑心暗鬼に…
- 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、某所から「意味がわからん。技術用語を使え」な指示

報道機関対応

- 誰が対応する？
  - サイバーセキュリティ担当理事 or 広報担当理事
    - 押し付け合いになることも珍しくない
  - CSIRT
    - 技術屋が技術論を述べて
  - 当該部局
    - …の誰？
      - 第一発見者
        - 見つけただけで犯人扱い？
      - 管理者
        - 「攻撃者が悪い」論の展開
- 取材担当記者の違い
  - 科学部と社会部

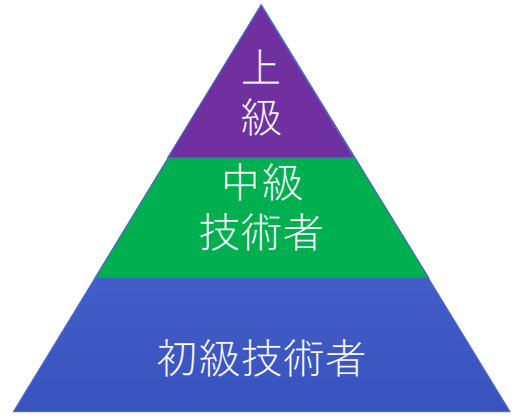
記者会見時の席順

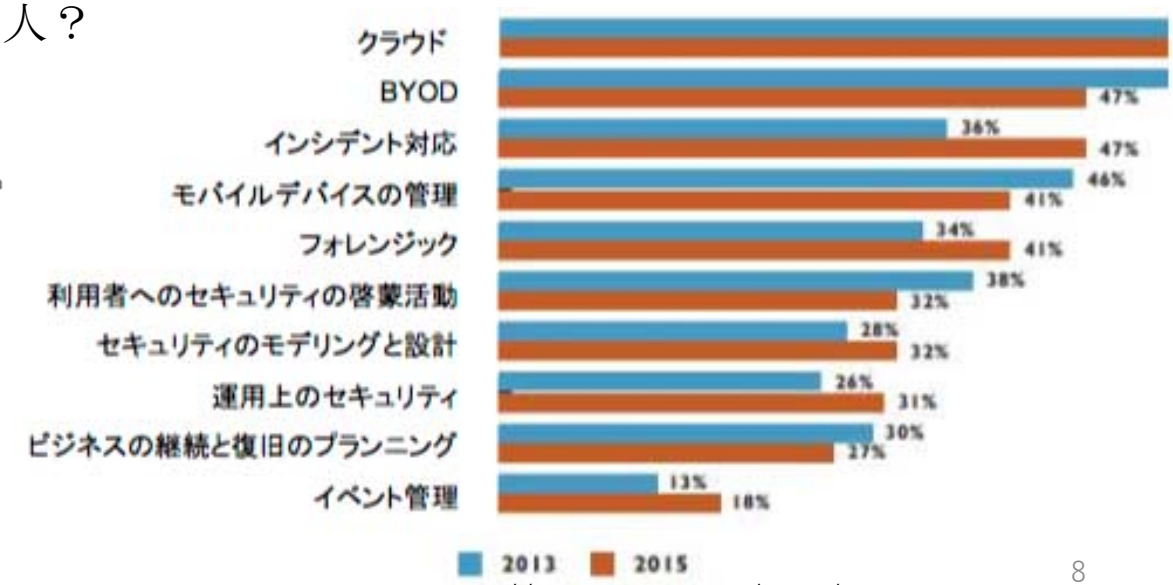
ネット中継を入れる？

研究者のマインド
「懇切丁寧に時間をかけて説明すればきっと理解してもらえる」

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(事故調査)
      - イベント管理能力とは？

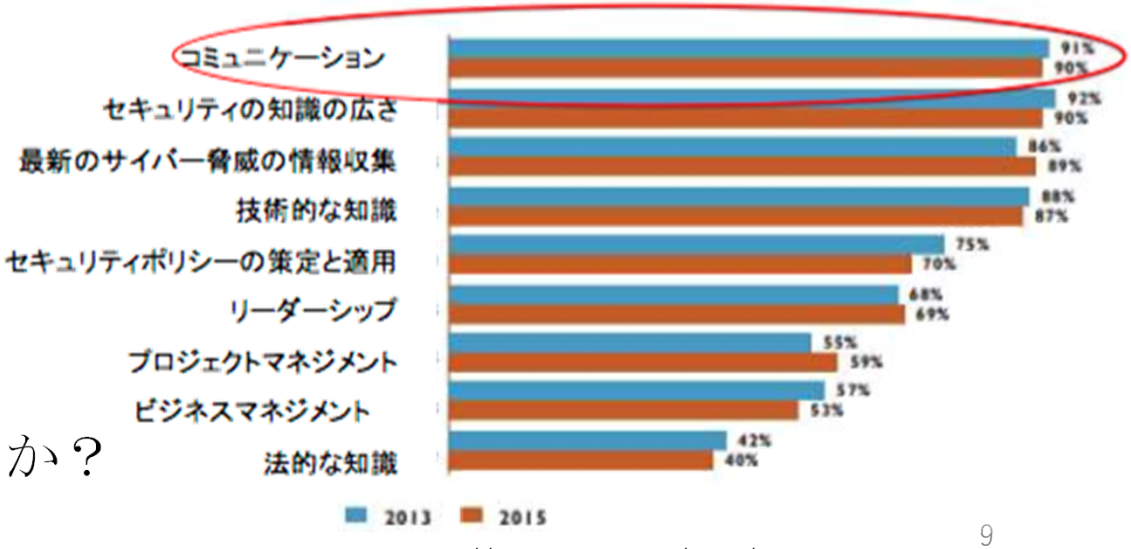




https://www.ipa.go.jp/files/000050299.pdf

組織が求める能力

- 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
    - 事実関係を究明するのがミッションのエンジニア
    - 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…技術者なのか？



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

被害発生は防げない…でも時間は止まってくれない

- 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

アクシデント化の恐怖…たった数台のマルウェア感染で

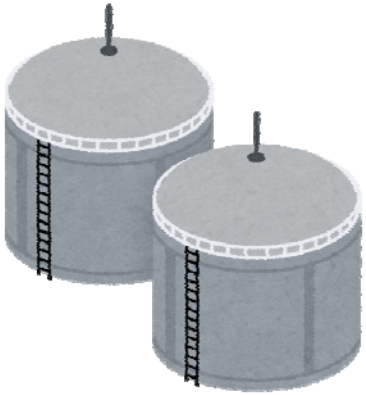
- 全ネットワーク遮断
  - 顧客サービス停止
- 年金機構でも…
  - 年金給付は継続稼働
    - 終息時期の予測不能
      - 長期の停止は人命に関わる
    - 被害の影響が及ばないことを確認
  - 個々のインシデントのトリアージ
    - アクシデントに発展するか？

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

レジリエント性が求められるIT

- IT…単なる文房具から業務支援の要へ
  - 一台のIT機器停止ですら業務への影響が…
    - マルウェアに感染したパソコン隔離(手順通り)
    - 代替パソコンの手配(手順通り)
    - 一向に届かない代替パソコン…なぜか？
- 大学だと人や設備に被害が及ぶことすら
  - 治療中の医療機器
    - 止めるか？治療を継続するか？
  - 窒素タンクの状態監視機器
    - 温度と圧力データは信用できるのか？
- 判断するのは誰の仕事か？
  - IT部門単独では動けない時代へ



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？

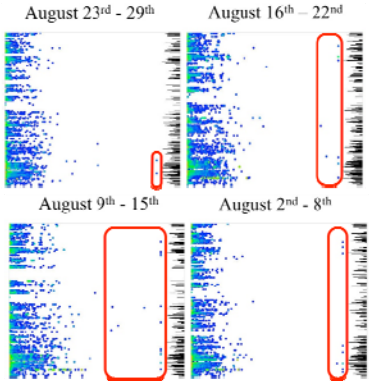
チームによる体制整備が必須

経営の知識

法律の知識

CSIRT

ネットワーク技術
セキュリティ技術
実務経験

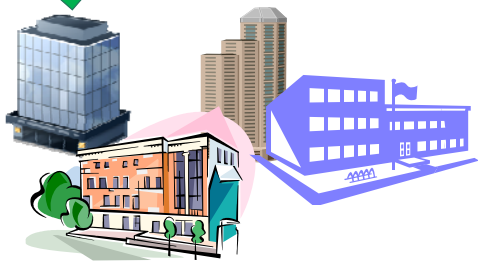


アクシデント分析と管理

戦略立案・助言
役員との意思疎通

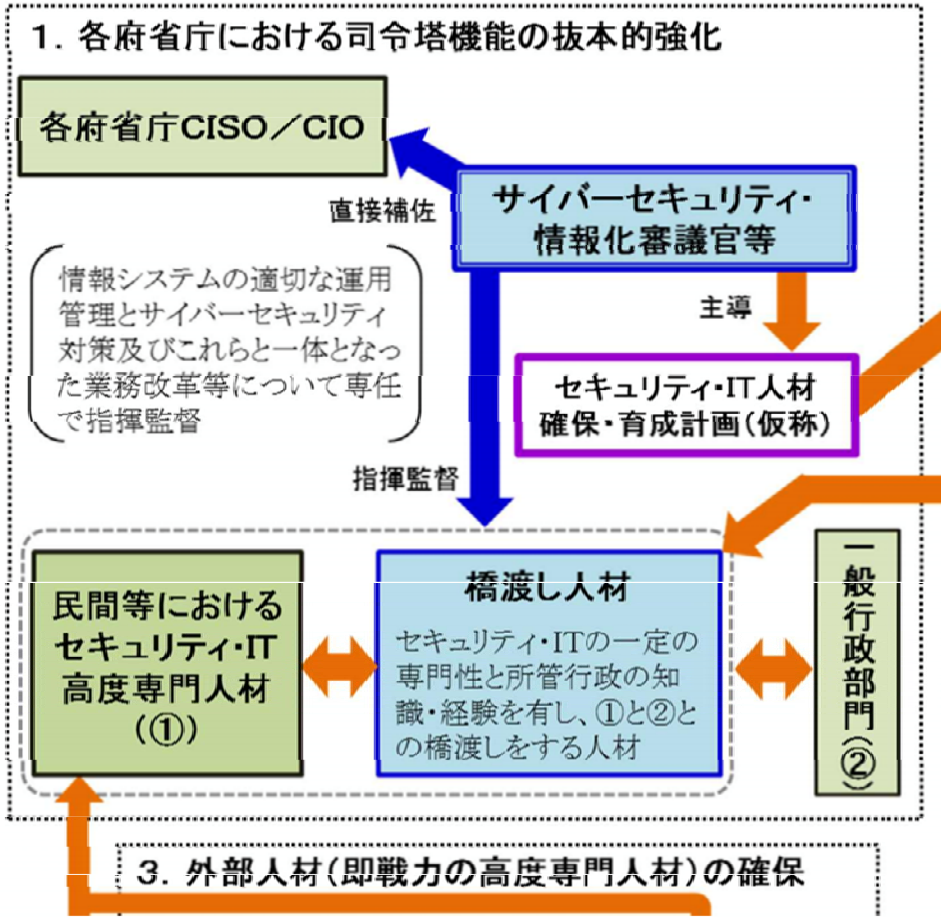
状況変化に応じた
的確な判断と指示
(トリアージ能力)

外部機関との連携



橋渡し人材の育成が急務に

- 橋渡し人材
  - インシデント対応の指揮
    - アクシデント化回避
      - 技術的知識
  - アクシデント対応の指揮
    - 関係部署との調整・情報の交通整理
- 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

まとめ

- サイバー攻撃による被害発生時
  - 迅速な原因究明・被害拡大防止・復旧
    - 専門業者との連携作業
  - 役員対応
  - 外部対応
    - 監督省庁、法執行機関、報道など
- チーム体制構築と橋渡し人材育成の必要性
  - 技術屋と経営層両方の考え方が出来る人材
  - 短時間で対応チーム規模を決定
  - 対応の長期化に備えた人材管理
    - 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…