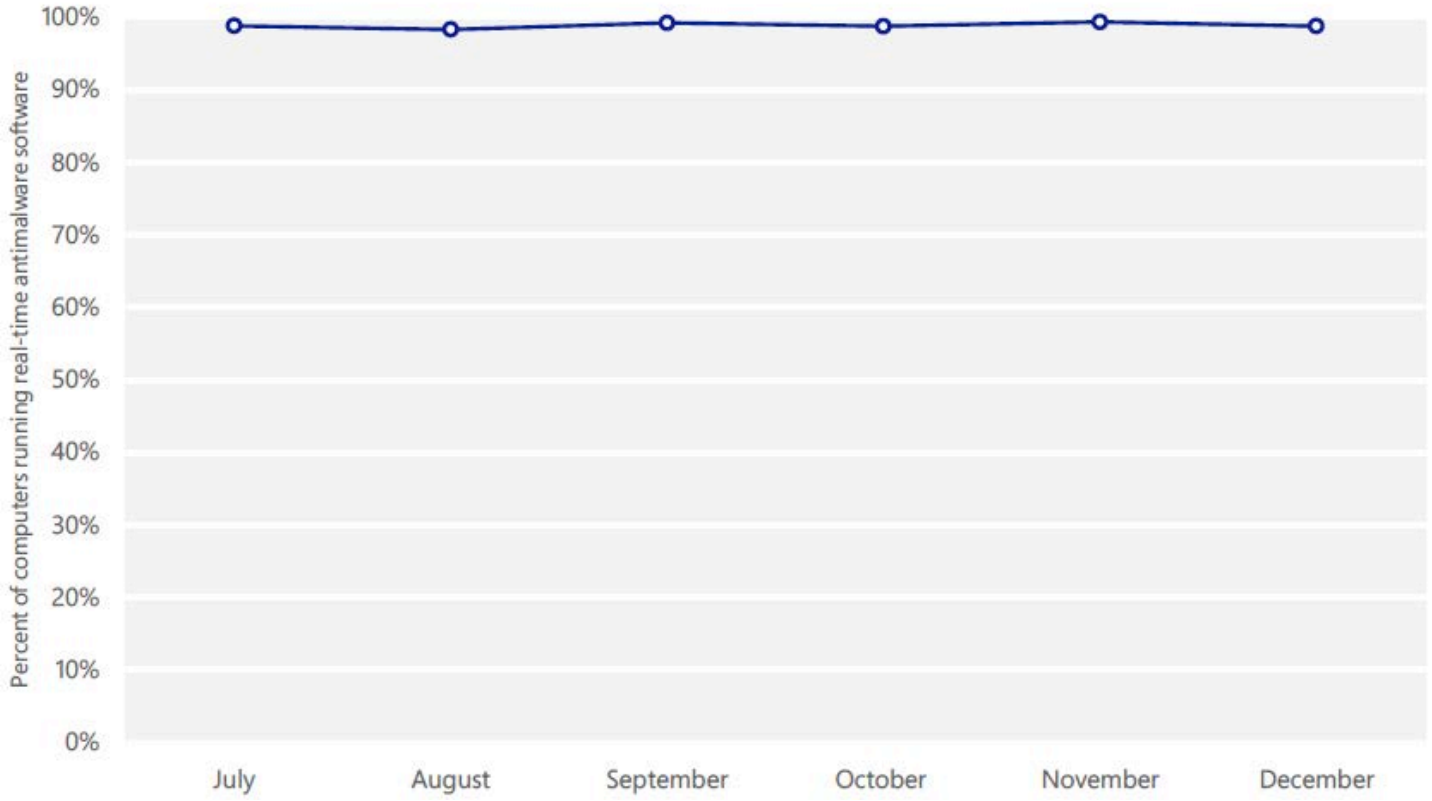
サイバー攻撃に耐性を有する情報ネットワーク
―システム全体を俯瞰したダメージコントロールの実現―

高倉弘喜
国立情報学研究所/名古屋大学

万全な対策...

- マイクロソフトの例
  - 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



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

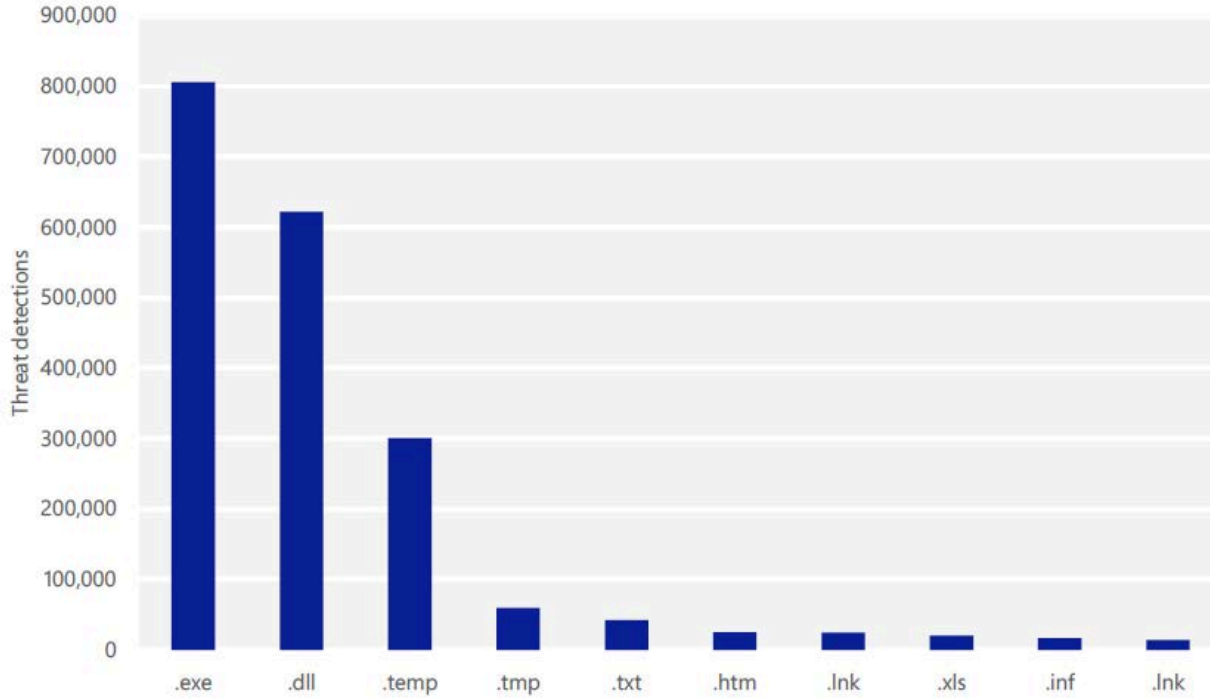
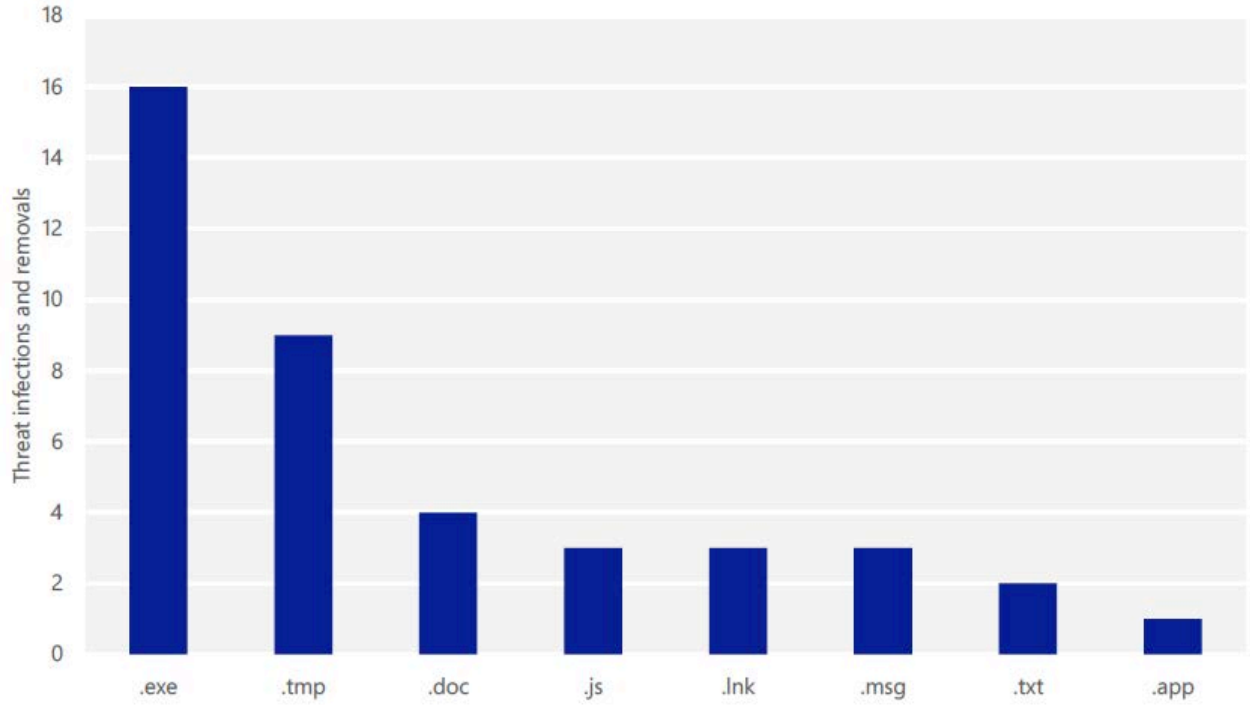
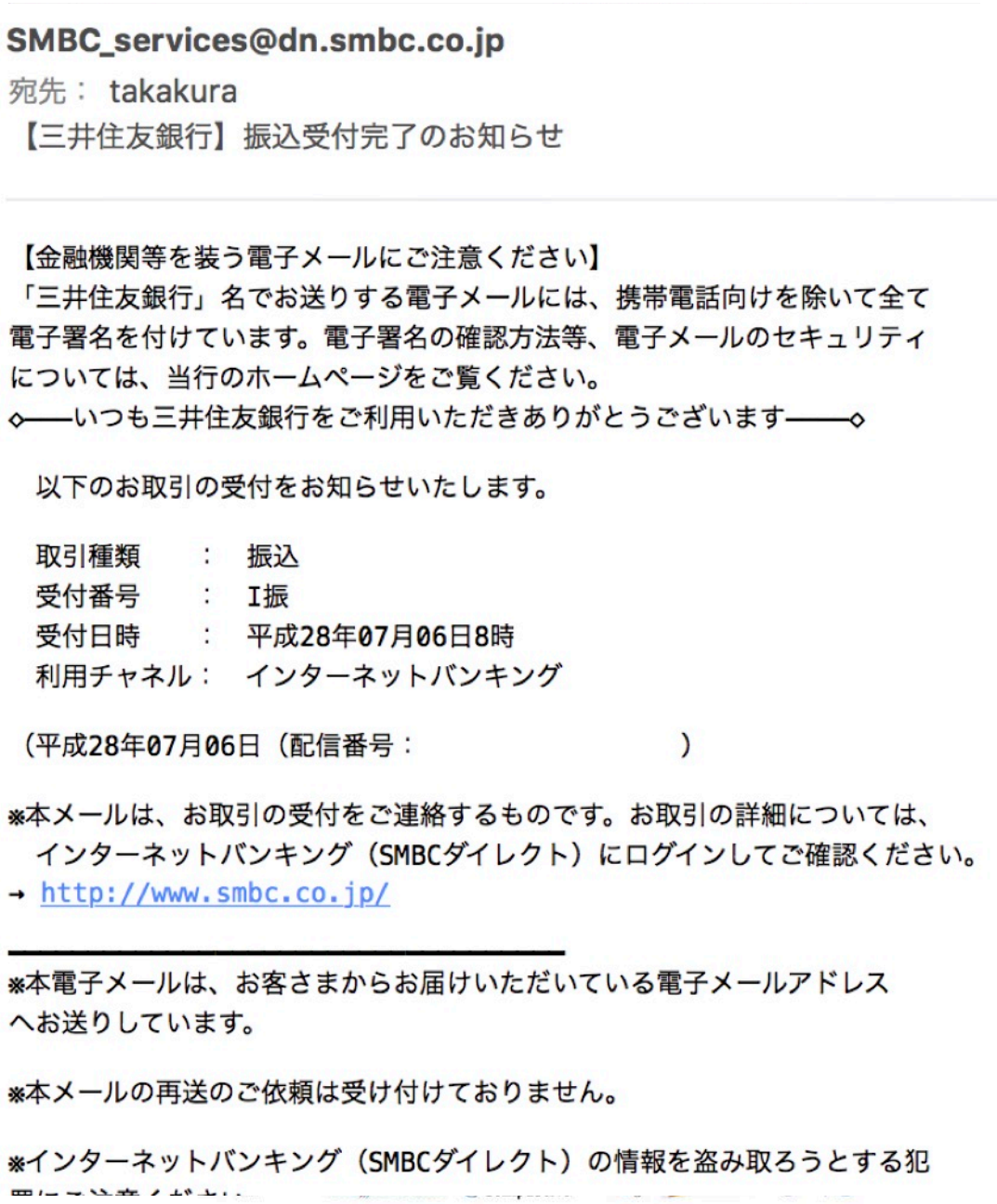


Figure 105. Infections and removals at Microsoft in 2H15, by file type



様々な感染経路

- メール
  - マルウェア添付
  - マルウェア配布Webサイトへのリンク
    - クリック or アクセスでマルウェア感染
  - 標的型攻撃では文面等に違和感がない
    - 例：JTB
  - 不自然な日本語の方が違和感がないことも
    - 大学など
- Web
  - ブラウザやプラグインの脆弱性を攻撃
    - アクセスした瞬間にマルウェア感染



SMBC_services@dn.smbc.co.jp

宛先： takakura

【三井住友銀行】振込受付完了のお知らせ

【金融機関等を装う電子メールにご注意ください】
「三井住友銀行」名でお送りする電子メールには、携帯電話向けを除いて全て電子署名を付けています。電子署名の確認方法等、電子メールのセキュリティについては、当行のホームページをご覧ください。
◇――いつも三井住友銀行をご利用いただきありがとうございます――◇

以下のお取引の受付をお知らせいたします。

取引種類　：　振込
受付番号　：　I振
受付日時　：　平成28年07月06日8時
利用チャネル：　インターネットバンキング

（平成28年07月06日（配信番号：　　）

※本メールは、お取引の受付をご連絡するものです。お取引の詳細については、
インターネットバンキング（SMBCダイレクト）にログインしてご確認ください。
→ http://www.smbc.co.jp/

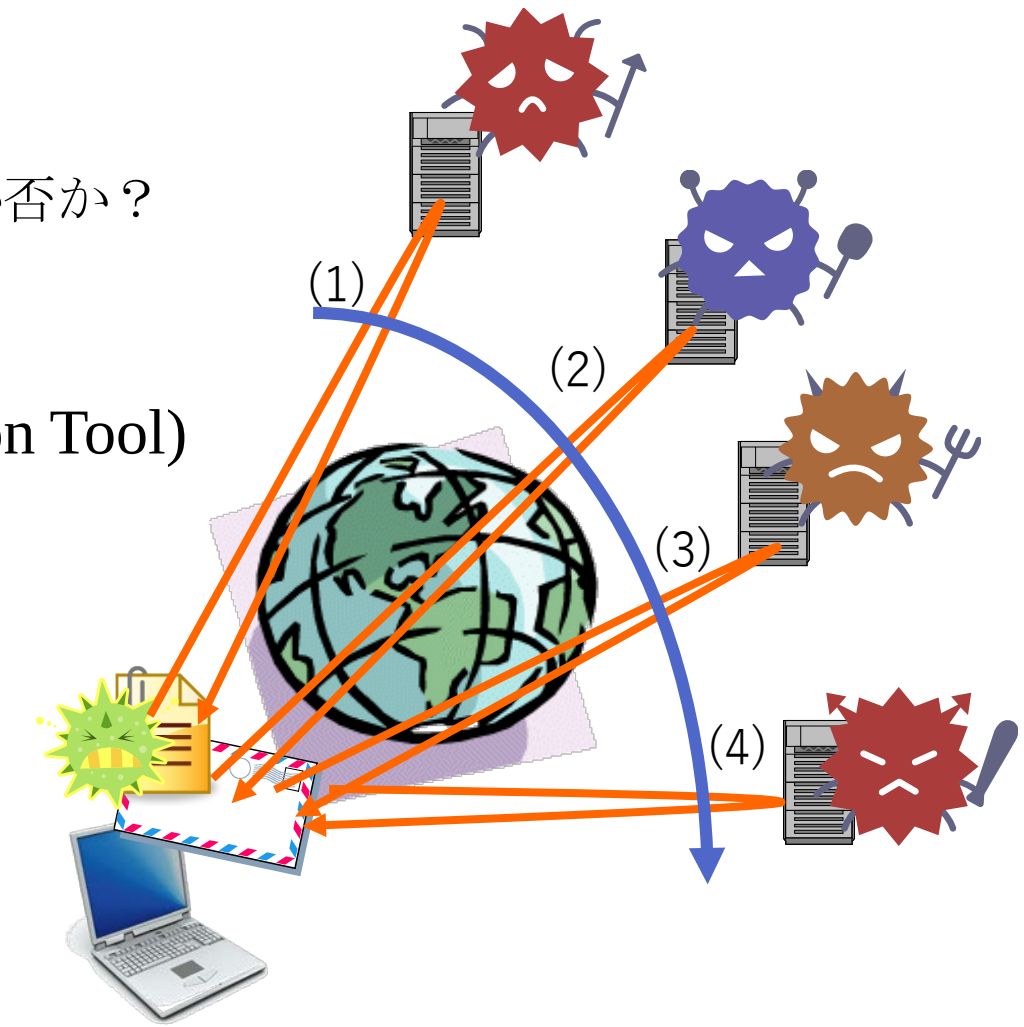
※本電子メールは、お客さまからお届けいただいている電子メールアドレスへお送りしています。

※本メールの再送のご依頼は受け付けておりません。

※インターネットバンキング（SMBCダイレクト）の情報を盗み取ろうとする犯

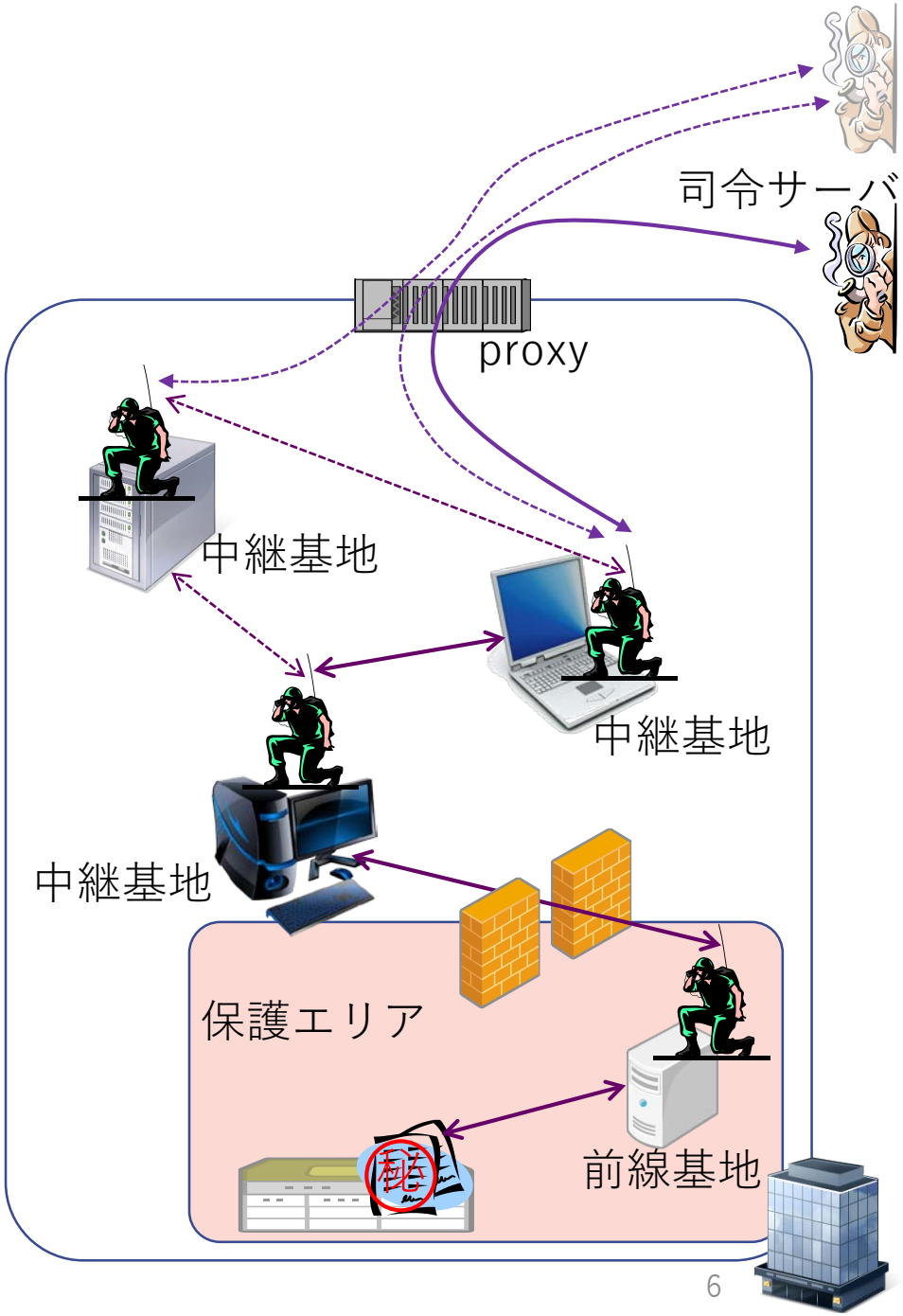
侵入後の攻略基盤構築

- 多段ダウンロードによる追跡妨害
  - ダウンローダ(トロイの木馬)
    - 感染対象機器の調査…乗っ取る価値があるか否か？
    - 感染確認後に一般公開
      - アンチウィルス駆除による誤判断を誘導
  - 遠隔操作プログラム(Remote Administration Tool)
    - 組織内部に前線基地を構築
      - 最初の任務は「偵察」
        - 脆弱性探索&攻撃
        - 標的型攻撃メールの素材収集＆送信
  - 監視プログラム
    - 防御側の動きをを監視
      - 緊急連絡
      - 「防御」に対する先回り対策



偵察から内部侵食へ移行

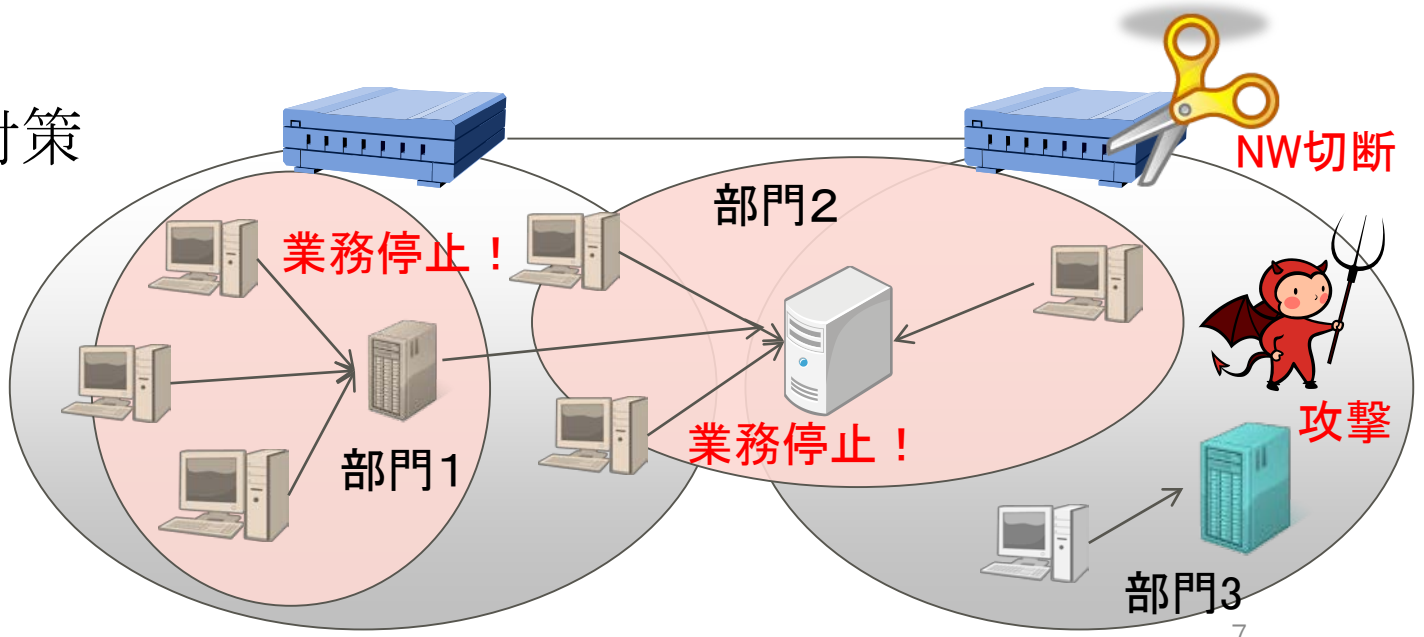
- 前線基地から徐々に内部へ侵食
  - 中継基地の構築
    - 保護エリアの機器と司令サーバの通信を仲介
- あらゆるものを多重化
  - 司令サーバ
  - 組織内の情報伝達経路
  - セキュリティ監視を意識した通信手段
    - 利用頻度の高い通信プロトコル
      - 木を隠すには森の中
    - 暗号通信
      - 解読できるのは攻撃者だけ
    - 規格外れの通信
      - 攻撃者もルールを守る必要性は…



内部ネットワーク(NW)侵食を想定しないセキュリティ対策

- 内部NWに監視ポイント無し
- 内部NWに隔壁(水密区画)なし
  - セグメント化&アクセス制御
    - 被害範囲の把握不能
    - 被害拡大の防止不能
- 攻撃者は全てお見通し
  - 導入されているセキュリティ対策
    - 検知できないマルウェア
    - 検知できない攻撃・偵察活動
- 対策プランの事前策定無し
  - エリートパニックを誘発
    - 過剰対応による全NW停止

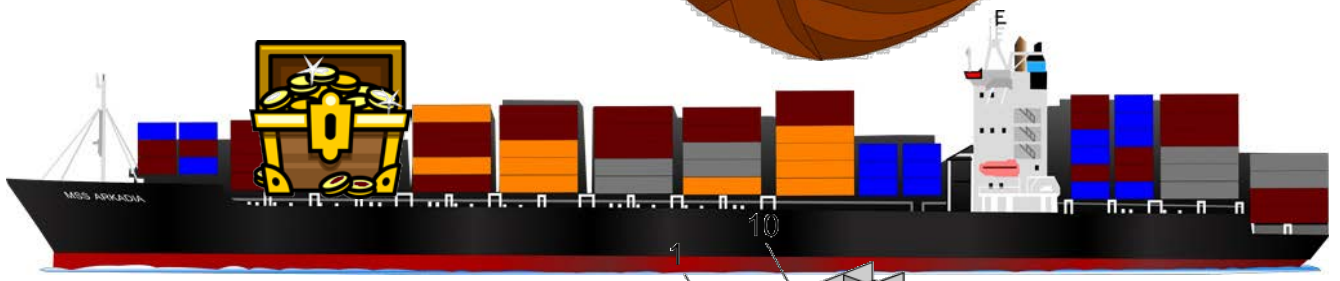
- 軽率な対応
  - 攻撃者の監視プログラムが察知
    - より慎重な活動へ移行
      - 新たな検知不能マルウェアの導入
    - データ破壊によるサボタージュ活動
      - 盗めなければ足止めする



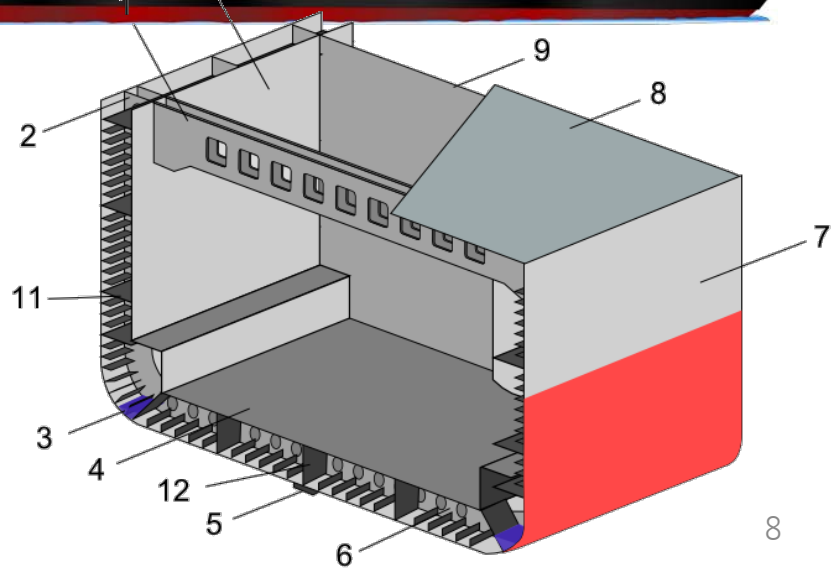
ウィルス一匹で大騒ぎ？

これはつまり…

- 水密区画のある船と手漕ぎボート位の違い
  - 手漕ぎボートに貴重品を載せて運搬？
    - 火災が起きれば一気に全焼
    - 浸水すれば…



- ダメージコントロール機能の有無
  - 浸水や火災を局所的に留められるか？
- レジリエンス(耐性)の有無
  - 区画を封鎖しても活動が継続できるか？
    - 一箇所のトラブルで全停止？



たった数台のマルウェア感染で

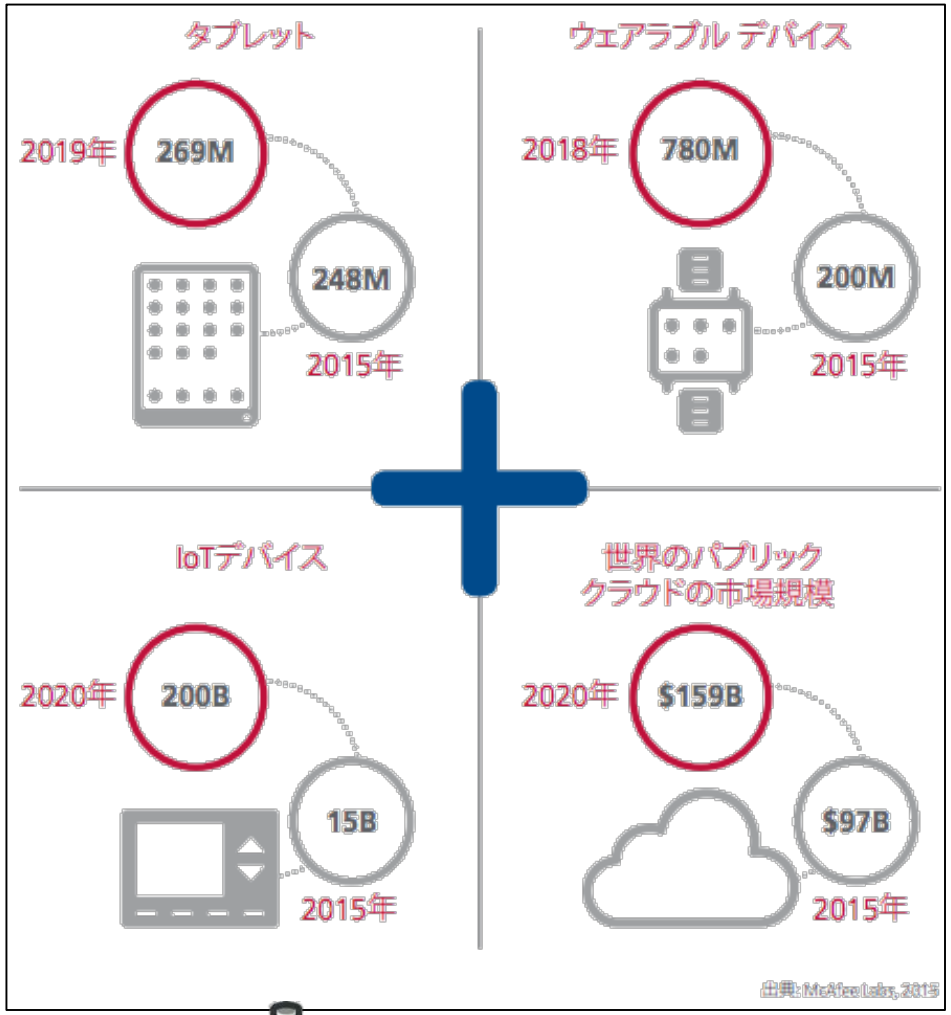
- 全ネットワーク遮断
  - 全サービスを停止
- 年金機構事故でも…
  - 年金給付は継続
    - 収束時期の予測不能
      - 長期の停止は人命に関わる
    - 被害の影響が及ばないことを確認
  - 情報機器で考えない
    - 業務で考える
      - この仕事が止まったら…

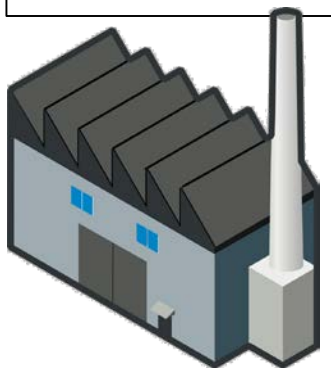
報道日時	被害組織	感染台数	発端	原因	対応状況
2016年6月22日	新城市	新城消防署 PC2台	不明	不明	市役所を含むネットワーク遮断(6月21日～22日まで)
同日	静岡市	静岡市役所 PC1台	警察からの情報提供	不審メールの開封	初期化済み(6月2日) 情報提供後インターネット接続遮断
同日	御前崎市	1台 (他感染可能性のあるPCあり)	警察からの情報提供	不明	マルウェアの駆除、初期化
同日	三豊市	市役所内 PC4台	警察からの情報提供	不明	インターネット接続遮断
2016年6月25日	群馬県	県庁内 PC1台	自組織にて検知 外部より情報提供あり	ばらまき型メールの添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

なぜ止められないのか？

- 情報システムの応用範囲の拡大
  - 止められないものの制御
    - 人命に関わるもの
    - 工場など制御対象が主であるもの
      - 情報システムが先に止まってしまっては…
        - 技術者が張り付いてでも、後で巻き戻し作業が入っても運用継続
  - アナログな代替策も重要
    - システムの運用停止を想定するか？
      - 手書き搭乗券、バネ式非常弁
  - それでもダメなら業務停止も想定
    - 経営判断が必要 (技術屋の仕事では無い)
      - 重量管理システム

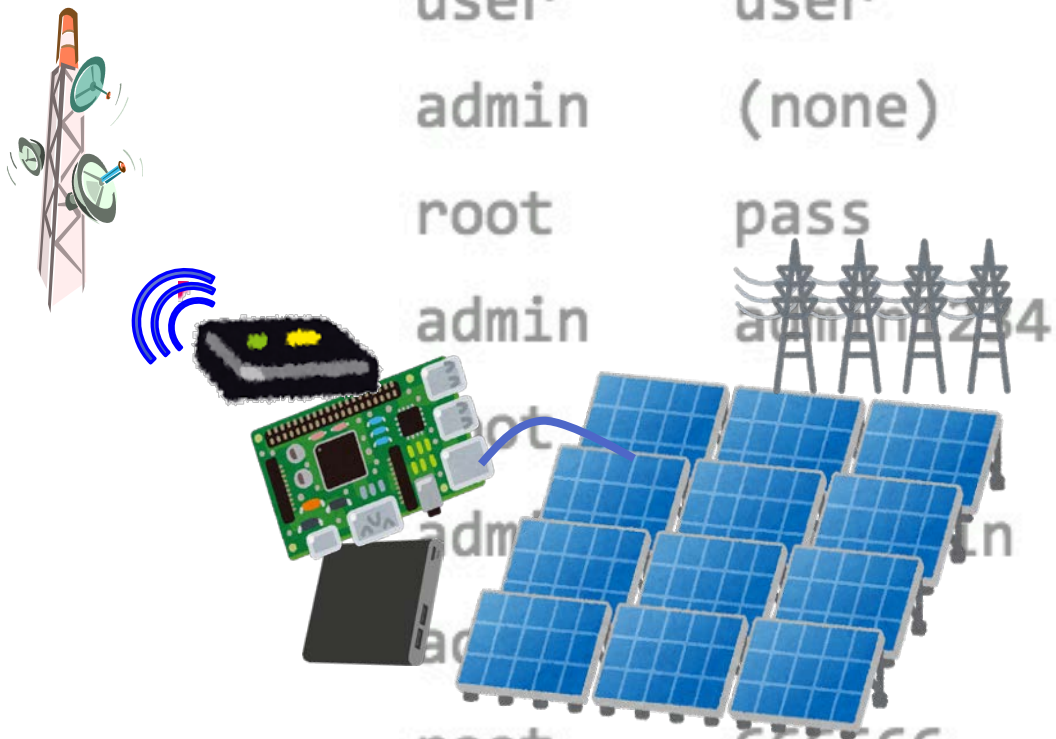




http://www.mcafee.com/jp/resources/reports/rp-threats-predictions-2016.pdf

爆発的に普及するIoT

- 避けられないインターネット利用
  - 様々な事情
    - ディバイスの製造コスト
    - 消費電力コスト
    - 設置・運用コスト
- 汎用プロトコルによる遠隔保守
  - インターネットで一般的なもの
    - プログラム開発コストを最小化
  - 脆弱な認証
    - ID=admin
    - パスワード=password



```
support   support
root      (none)
admin     password
root      root
root      12345
user      user
admin     (none)
root      pass
admin     admin1234
root      666666
root      password
```

https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/scanner.c#L123

インターネット直結されるIoT機器

- 当然探査活動は活発に
  - 狙われる様々なプロトコル
  - IoT機器の識別に便利
- Web公開されるマニュアル
  - 誰でも入手可能

133. .12

Country	Japan
Organization	National University University
ISP	National University University
Last Update	2015-10-26T10:00:53.325953
ASN	

Ports

23 5006 5007

Services

23 tcp telnet — VxWorks login:

5006 udp — Mitsubishi Q PLC

CPU: Q12DCCPU-V C 6

5007 tcp — Mitsubishi Q PLC

CPU: Q12DCCPU-V C 6

11.2 Remote Operation . . . . . .

Remote RUN (command: 1001) . . . . . .

Remote STOP (command: 1002) . . . . . .

Remote PAUSE (command: 1003) . . . . . .

Remote latch clear (command: 1005) . . . . . .

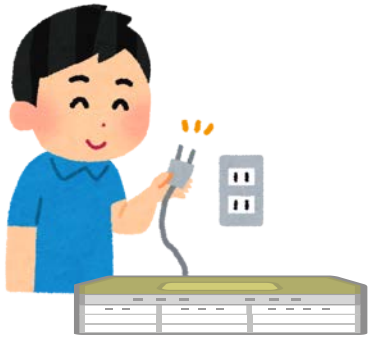
Remote RESET (command: 1006) . . . . . .

Read CPU model name (command: 0101) . .

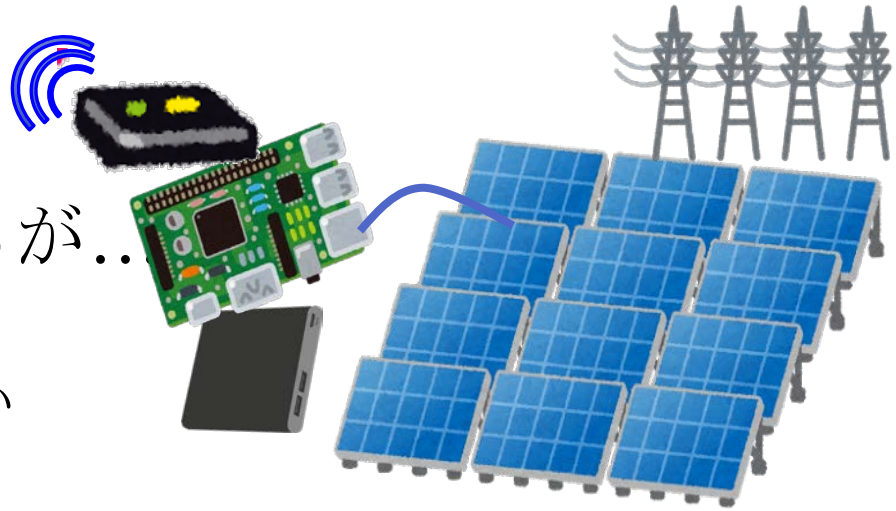
低コストゆえの悩み

- 個々のIoT装置
  - 20年前のパソコン並みのセキュリティ対策
    - セキュリティ機能を搭載する余裕がない

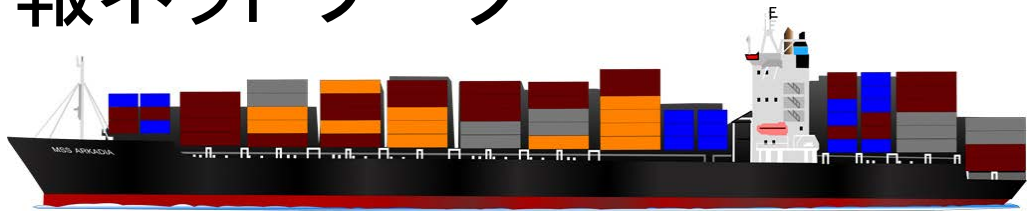
    →単体での防御性能は望めない
- 脆弱なIoT装置を保護
  - 各種セキュリティ装置の設置
    - 本体よりも高額な装置代と運用経費
    - 電力消費も桁違いに大きい
      - ➢ そもそも、そんな機材が置けるなら…
- 低コストなチップ開発は進みつつあるが…
  - 爆発的な普及に間に合わない恐れ
    - 1銭単位で求められるコスト削減との兼ね合い



FW/IDS/VPN



サイバー攻撃に対しレジリエンスな情報ネットワーク

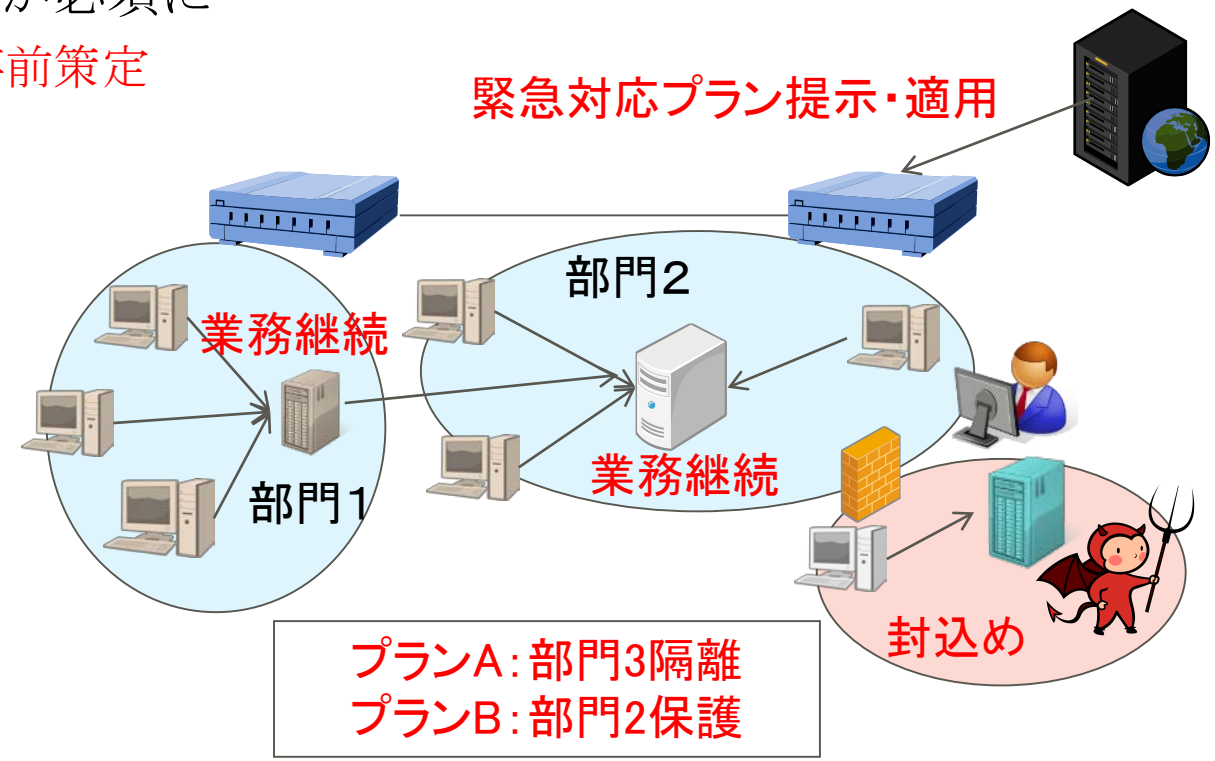


■ダメージコントロール

- ●どこで食い止めるのか？何を守るべきなのか？
  - ◆ネットワークの区画化とアクセス制御が必須に
    - ➢ 攻撃パターン毎に緊急対応プランを事前策定

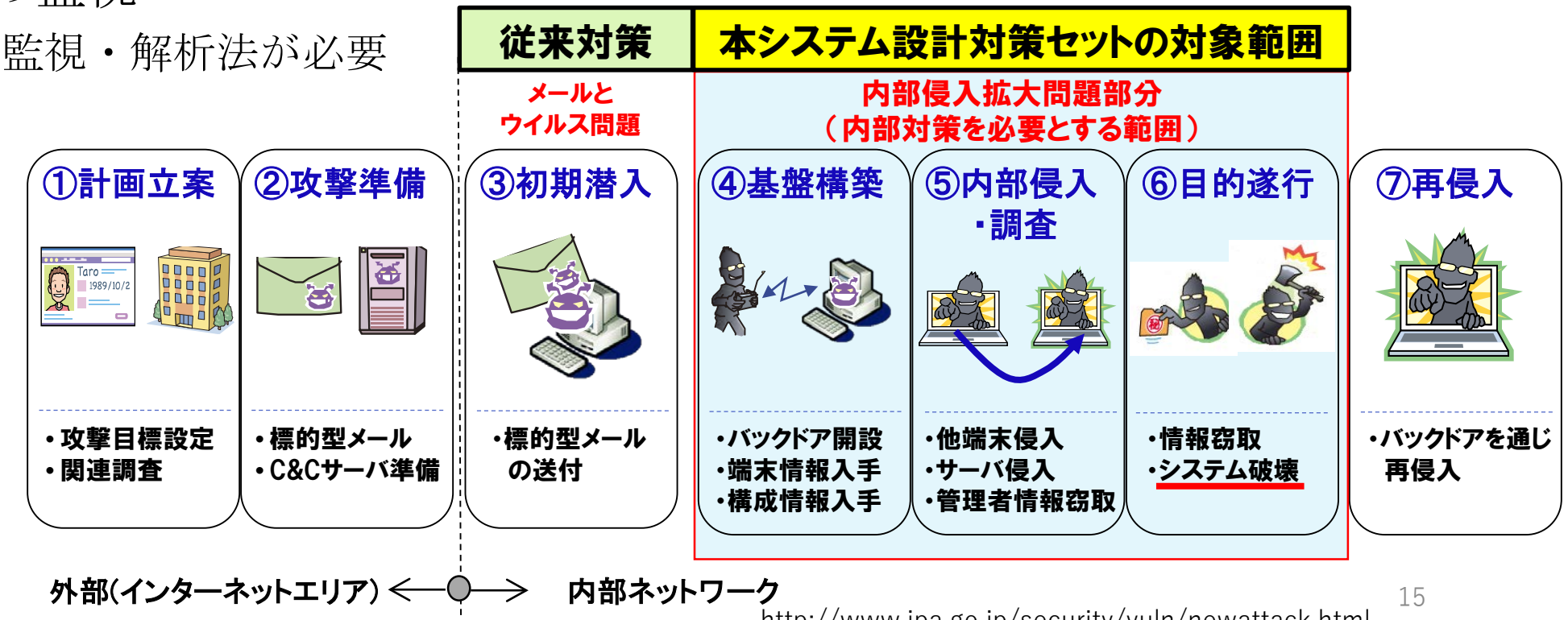
■デグレーデッドオペレーション

- ●業務継続と被害拡大防止の両立
  - ◆業務へ影響を最小化
- ●想定外の副作用を想定
  - ◆遮断できる…筈だった
    - ➢ バックアップ系が正しく稼働した
  - ◆単独で活動できる…筈だった。
    - ➢ 調達部門を隔離すれば…どうなる？
      - 業務毎に影響度を見積もり



高度化する攻撃への対策

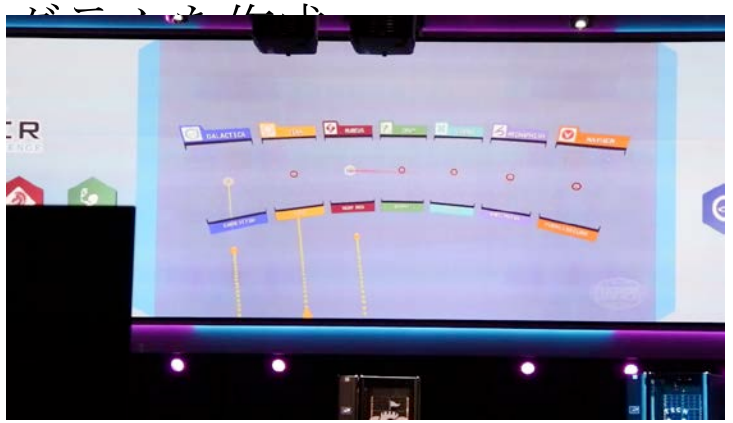
- 従来対策の突破を前提とした対策が必須に
  - 従来対策は無用という意味ではない
- 内部での基盤構築、内部侵入・調査を察知し、目的遂行を阻止
  - 内部NWの監視
    - 新たな監視・解析法が必要



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

米国の動き

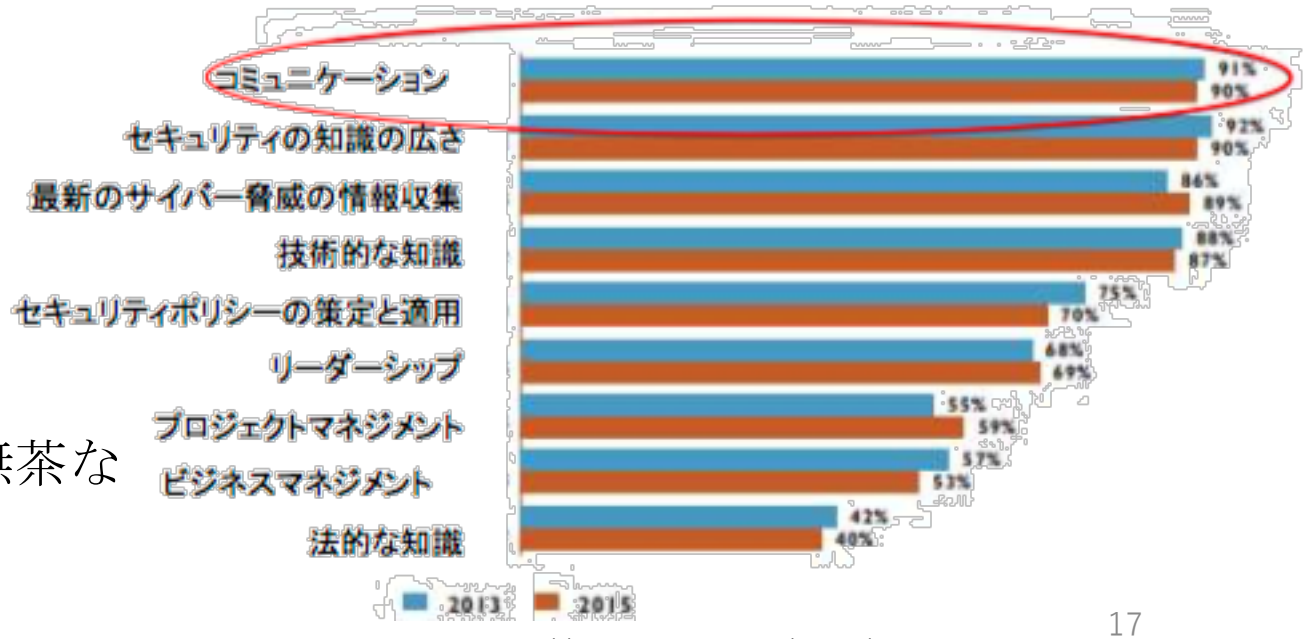
- DARPA Cyber Grand Challenge
  - 脆弱性検査(fuzz testing)
    - 様々なテストデータをプログラムに入力しプログラム
    - バグを特定→攻略可能な脆弱性を探索
  - パッチプログラムの作成
    - 見つけた脆弱性に対する暫定パッチを作成する。
  - 攻撃プログラムの作成
    - 他チームのサービスプログラムを停止させる攻撃プロ
  - テストデータによる動作検証
    - 暫定パッチ適用前後での動作確認
- これを全て自動化
  - 解析システム自身のクラッシュ対策



https://cgc.darpa.mil

橋渡し人材の確保

- セキュリティ人材の求められる能力
  - まずはコミュ力
  - 技術用語から役員用語への翻訳…これが一番難しい
  - 広大な知識が必要
    - 技術、法律、経営…万能人材？
- 橋渡し人材が要に
  - 被害発生部門との技術対応
  - 経営層への説明
  - 外部委託の必要性判断
    - 技術＋経営＋…
    - 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



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

橋渡し人材育成…韓国の場合

- 露出度が高いのは…
- 参謀(指揮官候補)育成
  - 別パス
  - 陸海空軍から毎年4名の下士官選抜
    - 留学：米国2、日本2
      - 大学、士官学校
    - 若手エンジニアの思考パターン
      - 命令すりゃ動く人たちでは無い
    - サイバー攻撃対策
      - プランの策定
      - 攻撃確認時の選択

今後求められる技術

- サイバー攻撃技術の高度化
  - 現在
    - サイバー攻撃の情勢分析
      - 弊社は攻撃対象となりうるのか？
    - 攻撃検知やマルウェア解析
      - 攻撃による被害は業務にどの程度の影響があるのか？
  - 近未来
    - 攻撃の方向性を把握
      - 攻撃者の狙いを予測
  - 今後
    - 攻撃対象の予防的保護
      - 攻撃による被害状況の把握
      - 攻撃者の最終目標を先回りで保護
        - 偽情報を掴ませて反応を観察

まとめ

- サイバー攻撃の高度化
  - 攻撃による侵入の完全阻止は困難
  - 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
      - 止められない情報システムの急増
- 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による攻撃の封じ込め(被害拡大防止)
    - デグレーデッドオペレーションによる業務の継続
  - 攻撃対策のの事前策定
    - 想定漏れや想定外の副作用の把握
- 橋渡し人材育成の必要性と新たな技術開発