巧妙化するサイバー攻撃に対するタメージコントロール

高倉弘喜
国立情報学研究所

多様化する攻撃先

- 攻撃の目的が諜報活動へ
  - もちろん金銭目的の攻撃も継続中

国家機密情報、ソースコード、メールアーカイブ、交渉計画、新規油田・ガス田開発に関する詳細な調査結果、ドキュメントストア、契約書、システム設計図面など

業種	攻撃数
航空宇宙・防衛	41組織
エネルギー関係	34組織
金融	26組織
ソフトウェア産業	19組織
法律関係	17組織
メディア・出版	17組織
情報通信	14組織

出典：Mandiant M-Trends

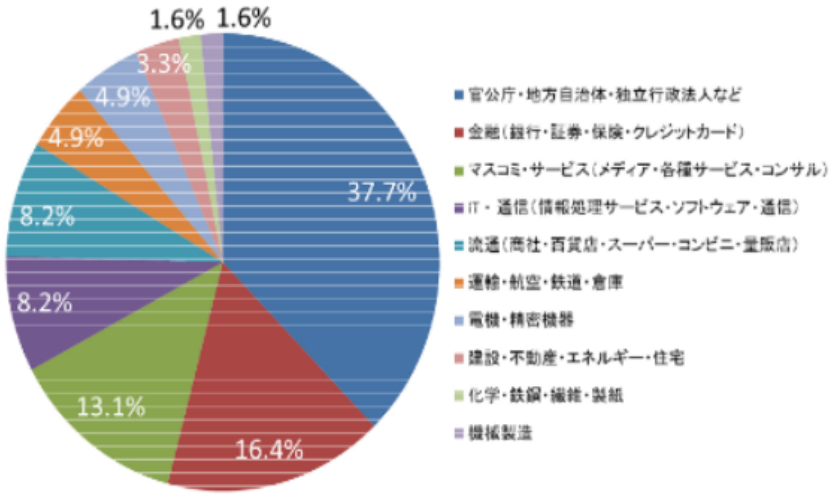


図 31 標的型メール攻撃のターゲットとなった組織の業種別割合

（Tokyo SOC 調べ：2013 年 1 月 1 日～2013 年 6 月 30 日）

出典：「東京SOC情報分析レポート 2013上半期」
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2013_h1.pdf

オンラインバンキングを狙った攻撃

- マルウェア検知件数の増加

出典：「PWS:Win32/Zbot」の国内検出数推移（グラフ：日本MS）

増加するゼロデイ攻撃

- 2013年IPA集計
  - 対策が存在しない状態での攻撃開始

公開	ゼロデイ脆弱性	影響を受ける製品
1月	CVE-2012-4792	MS Internet Explorer
	CVE-2013-0422	Orackle Java
2月	CVE-2013-0437	Orackle Java
	CVE-2013-0633	Adobe Flash Player
	CVE-2013-0634	
	CVE-2013-0030	MS Internet Explorer
	CVE-2013-0640	Adbe Reader、Adobe Acrobat
	CVE-2013-0641	
	CVE-2013-0504	Adobe Flash Player
	CVE-2013-0643	
	CVE-2013-0648	
3月	CVE-2013-1493	Oracle Java
5月	CVE-2013-1347	MS Internet Explorer
6月	CVE-2013-1331	MS Office
7月	CVE-2013-3660	Windowsカーネル
	CVE-2013-4854	ISC BIND
10月	CVE-2013-3893	MS Internet Explorer
	CVE-2013-3897	MS Internet Explorer
11月	CVE-2013-3906	MS Office
	CVE-2013-3918	Internet Explorer Active X

ゼロデイ脆弱性の件数
・2012年→14件
・2013年→22件

OSよりアプリケーションへの
ゼロディ脆弱性が増加

ゼロディ攻撃ツール開発販売を
生業とする企業まで登場

Drive by download攻撃の急増

- 正規Webサイト
  - 広告でマルウェア配布サイトへ誘導
  - 各種脆弱性を衝かれてマルウェアインストール
- 多くの場合でゼロディ攻撃
  - Anti-virusなどでの検知困難
  - 利用者に気付かれることなく
  - C2(司令)サーバへの接続
    - さらなるマルウェアダウンロード
      - ✓ 多重化のため

表１　ドライブ・バイ・ダウンロード攻撃に悪用された Adobe Flash Player の脆弱性
(Tokyo SOC 調べ：2015 年 1 月 1 日～2015 年 12 月 31 日)

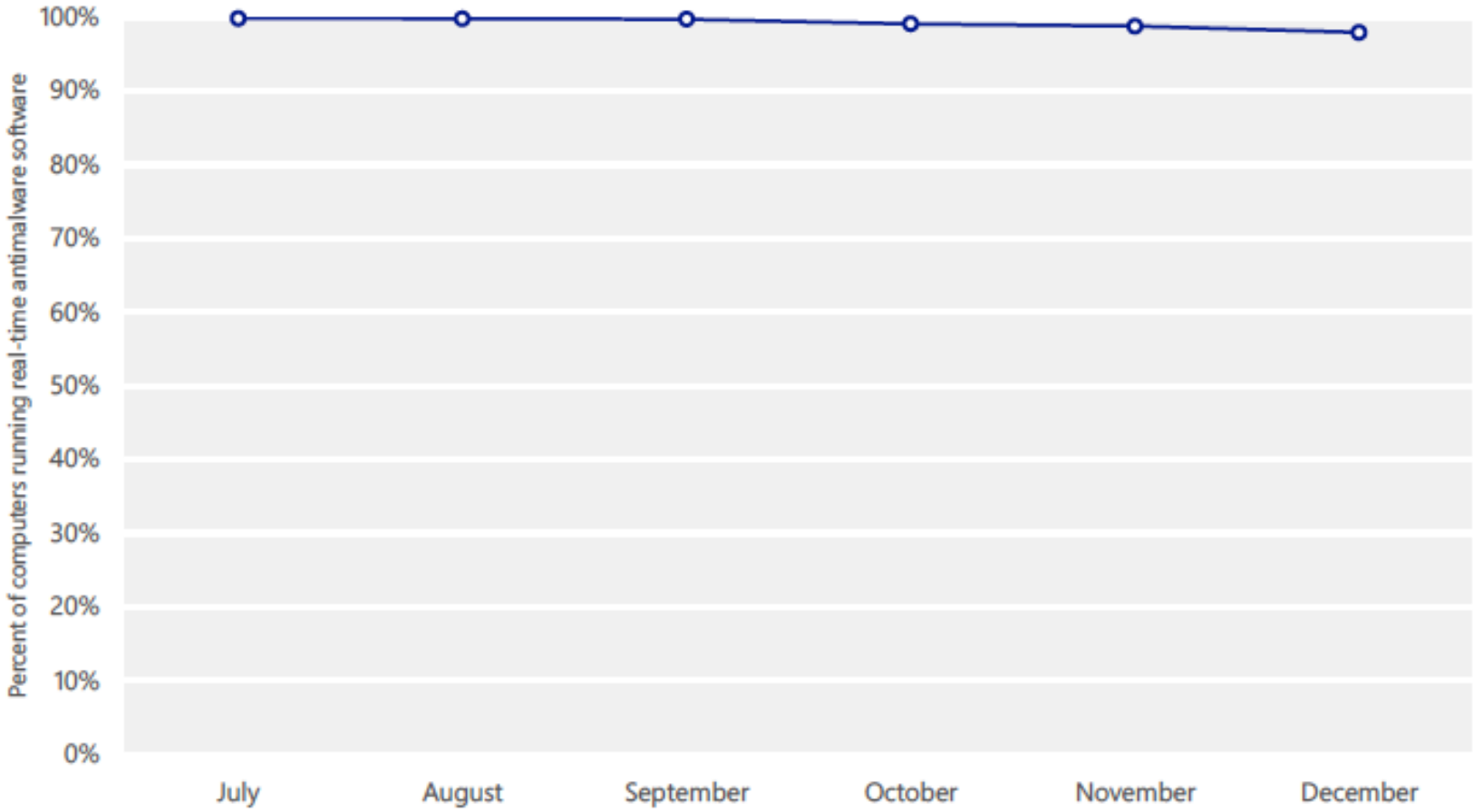
公開月	脆弱性識別番号	ゼロデイ脆弱性
2015 年 1 月	CVE-2015-0310 (APSB15-02)	✔
2015 年 1 月	CVE-2015-0311 (APSA15-01/APSB15-03)	✔
2015 年 2 月	CVE-2015-0313 (APSA15-02/APSB15-04)	✔
2015 年 3 月	CVE-2015-0336 (APSB15-05)	
2015 年 4 月	CVE-2015-3043 (APSB15-06)	✔
2015 年 4 月	CVE-2015-0359 (APSB15-06)	
2015 年 5 月	CVE-2015-3090 (APSB15-09)	
2015 年 6 月	CVE-2015-3104 (APSB15-11)	
2015 年 6 月	CVE-2015-3105 (APSB15-11)	
2015 年 6 月	CVE-2015-3113 (APSB15-14)	✔
2015 年 7 月	CVE-2015-5119 (APSA15-03/APSB15-16)	✔
2015 年 7 月	CVE-2015-5122 (APSA15-04/APSB15-18)	✔
2015 年 8 月	CVE-2015-5560 (APSB15-19)	
2015 年 10 月	CVE-2015-7645 (APSA15-05/APSB15-27)	✔
2015 年 12 月	CVE-2015-8446 (APSB15-32)	
2015 年 12 月	CVE-2015-8651 (APSB16-01)	✔

出典：「東京SOC情報分析レポート 2015下半期」
http://www-935.ibm.com/services/jp/ja/it-services/soc-report/

マイクロソフト社ですら…

- 60万台以上、ほぼ100%のアンチウイルスソフト稼働率

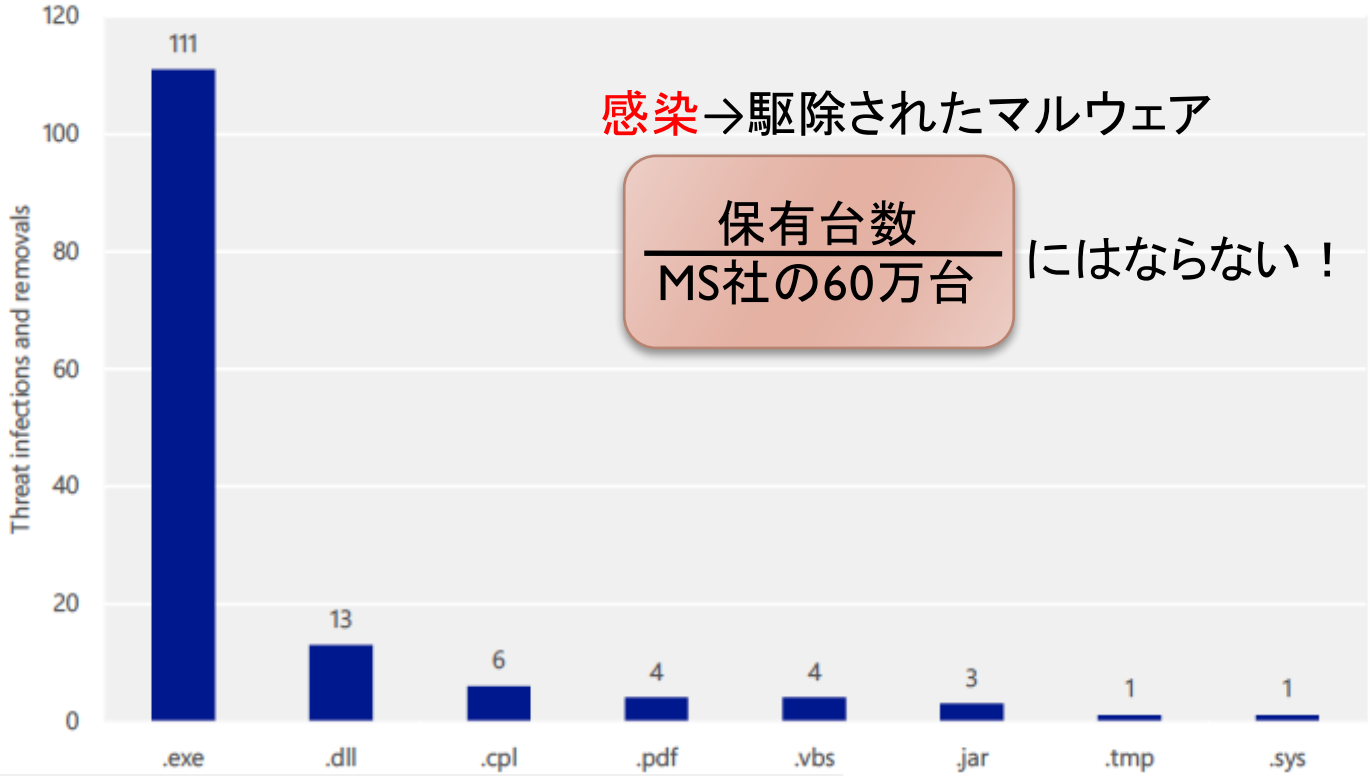
Figure 65. Percentage of computers at Microsoft running real-time antimalware software in 2H14　2014年後半



http://www.microsoft.com/security/sir/default.aspx

結果として…

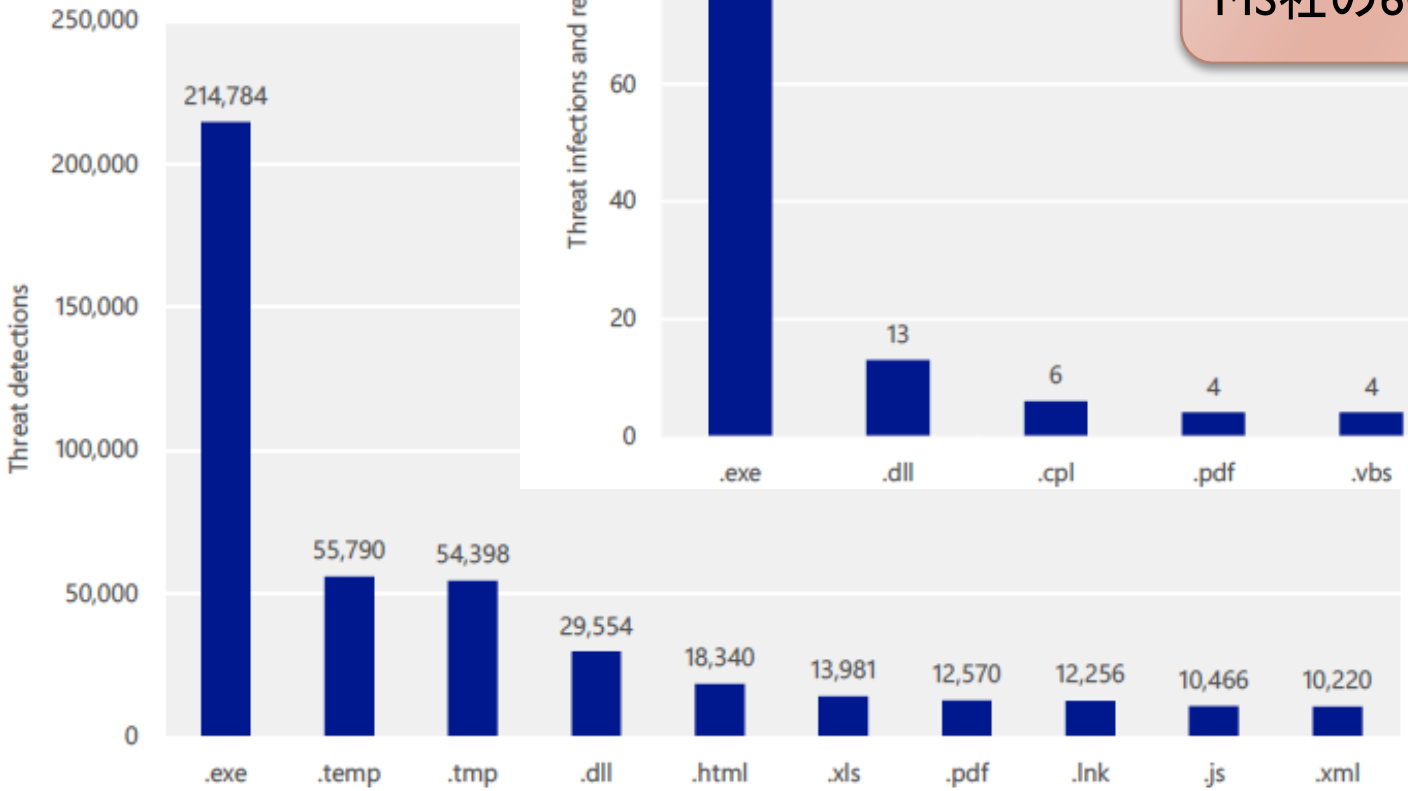
Figure 70. Infections and removals at Microsoft in 2H14, by file type



感染→駆除されたマルウェア

保有台数 / MS社の60万台 にはならない！

Figure 67. Threat detections at Microsoft in 2H14,



検知したマルウェア

http://www.microsoft.com/security/sir/default.aspx

見えない攻撃

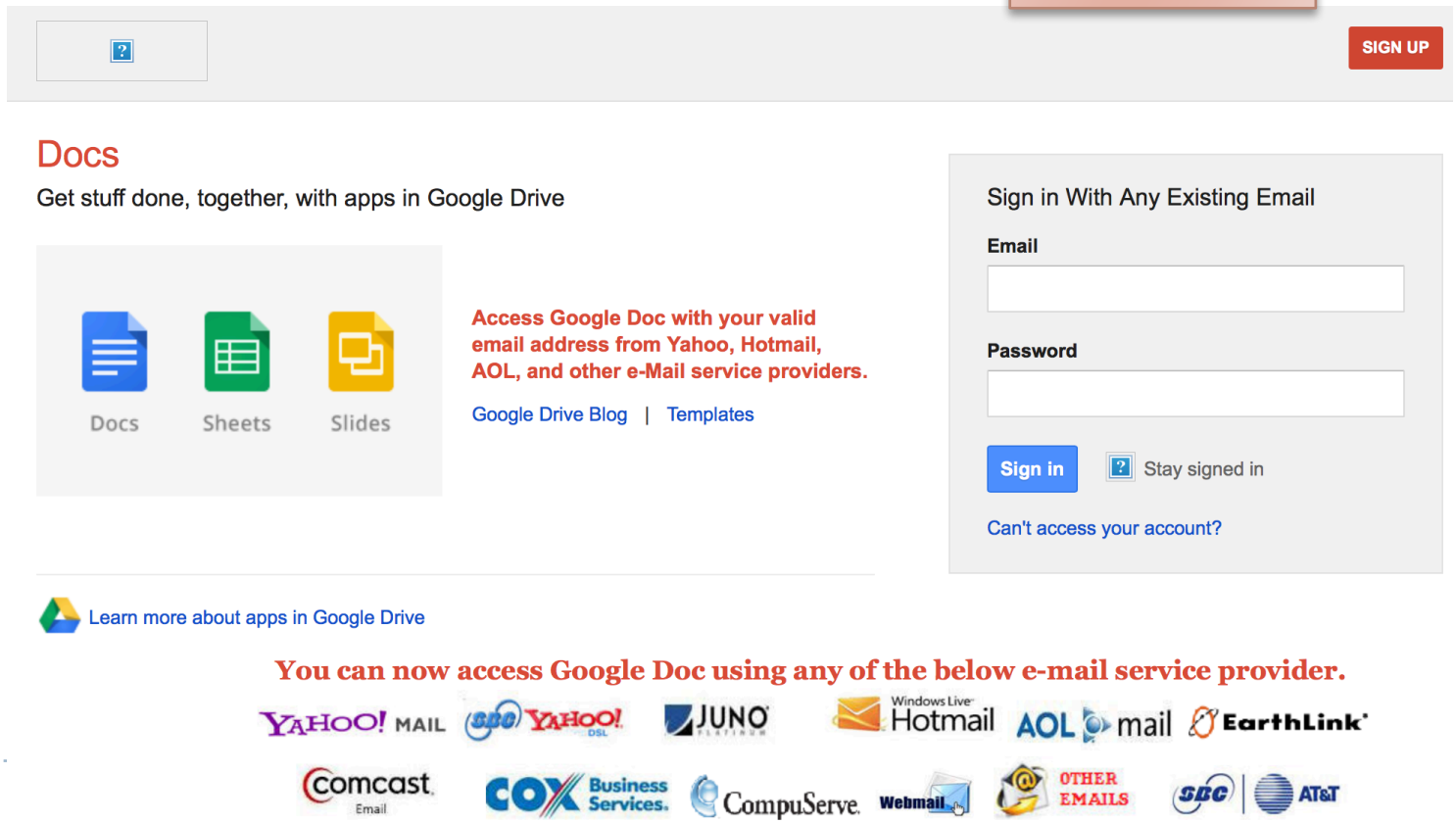
- Anti-virus/spam素通り

リンク先は

- 偽GoogleDocs
  - セッションログ調査
    - Email/Passwordを入力したと推定される挙動
    - 他と明らかに異なる挙動を示した機器

      本命？

一桁多い
セッション数



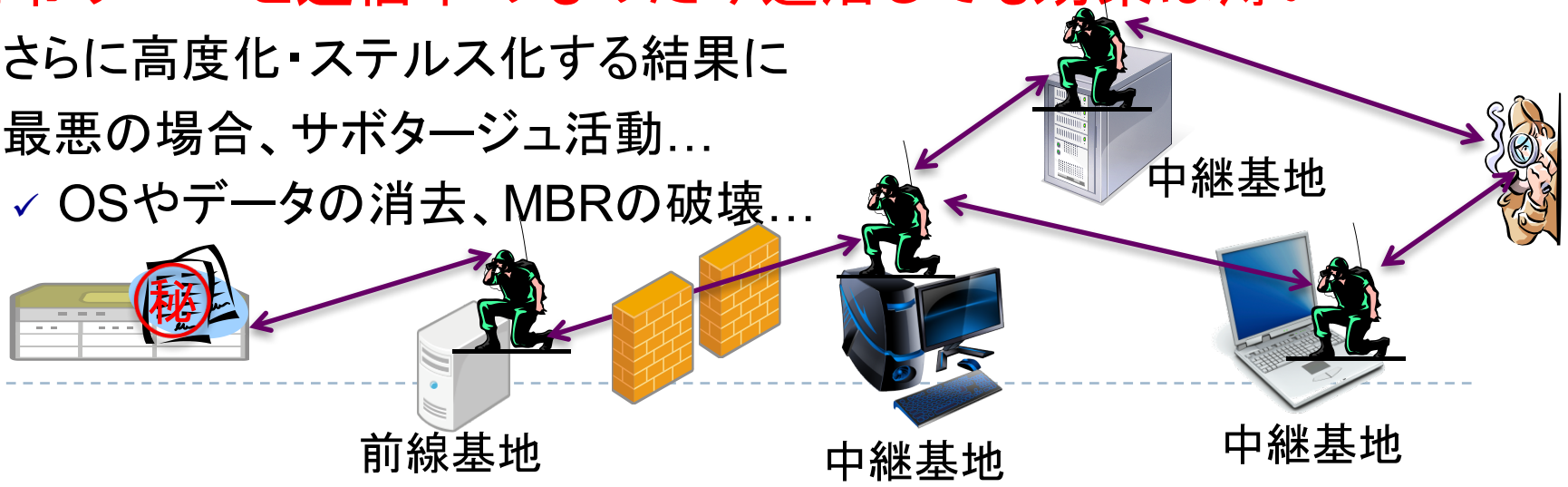
ステルス攻撃…検知不能

- 1回目 (5/8)
  - 悪意あるURL付きメール
    - クリック後直ちに外部と通信(直ちに検知)
    - 4時間後：感染PC隔離特定、当該URL遮断
- 2回目 (5/18)
  - 同一URL→外部との通信ブロック
- 3回目 (5/18, 19)
  - 誰も悪意あるURLクリックせず
- 4回目 (5/20)
  - 別の悪意あるURL付きメール
    - 1台のPC感染 → 数時間後：6台のPCに感染
- 情報漏洩 (5/21-23)
  - 21台のPCにより情報持ち出し(勤務時間中)
- 全ネットワークの切断…ただし一部を除く
  - アクシデント対処→判断基準は？

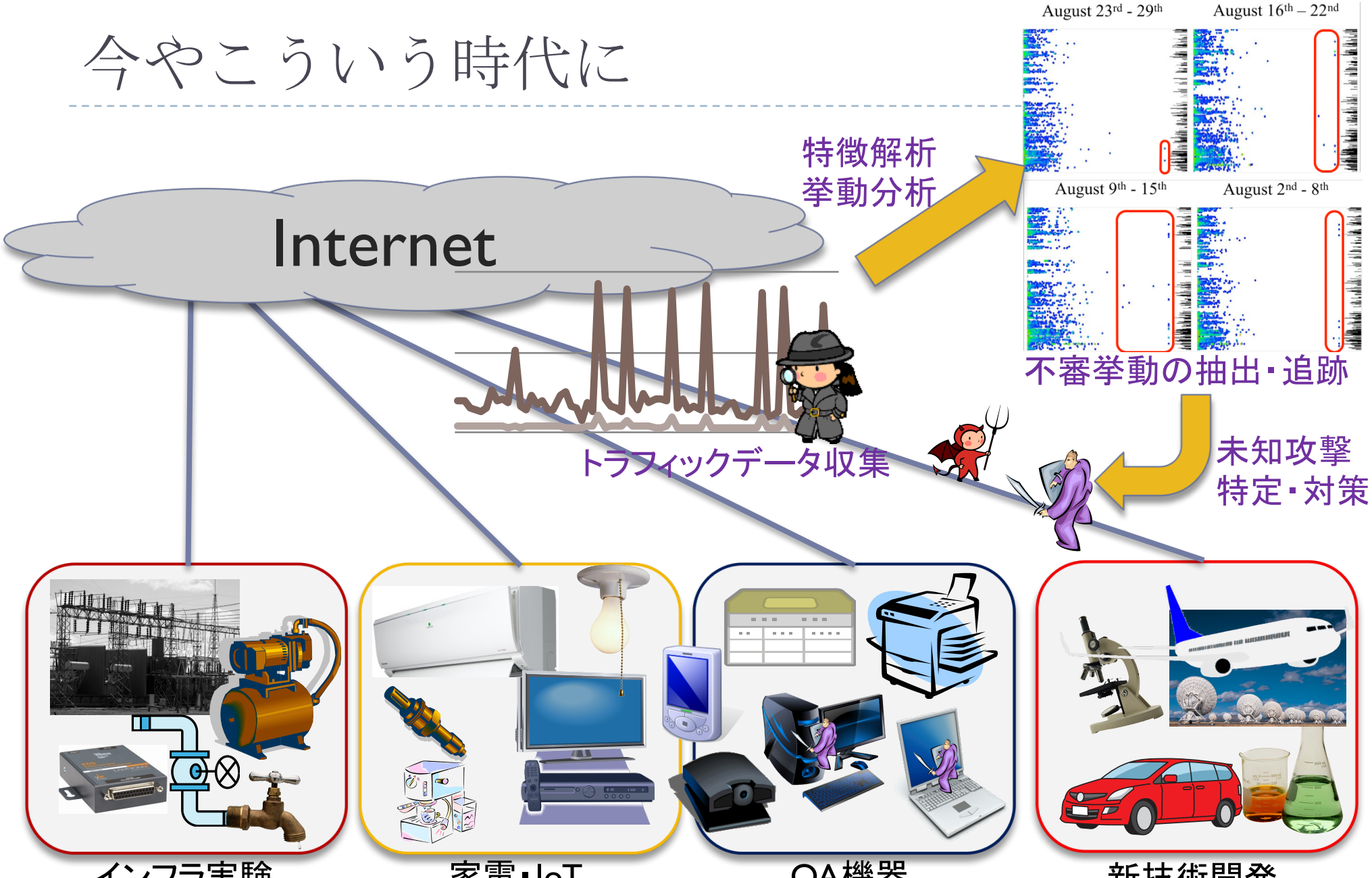
日本年金機構
Japan Pension Service

高度サイバー攻撃の特徴

- わざと目立つような攻撃の水面下で…
  - 本命に対するマルウェア感染攻撃
    - いつもの通信相手の乗っ取り
    - いつもの文面＋いつもの添付ファイル(ただしオマケ付き)
- 広範囲な感染被害を想定
  - 組織内に張り巡らされた感染機器ネットワーク
    - 多数の待機機器、通信経路多重化、マルウェア多重感染…
  - 司令サーバと通信中のものだけ退治しても効果は薄い
    - さらに高度化・ステルス化する結果に
    - 最悪の場合、サボタージュ活動…
      - ✓ OSやデータの消去、MBRの破壊…

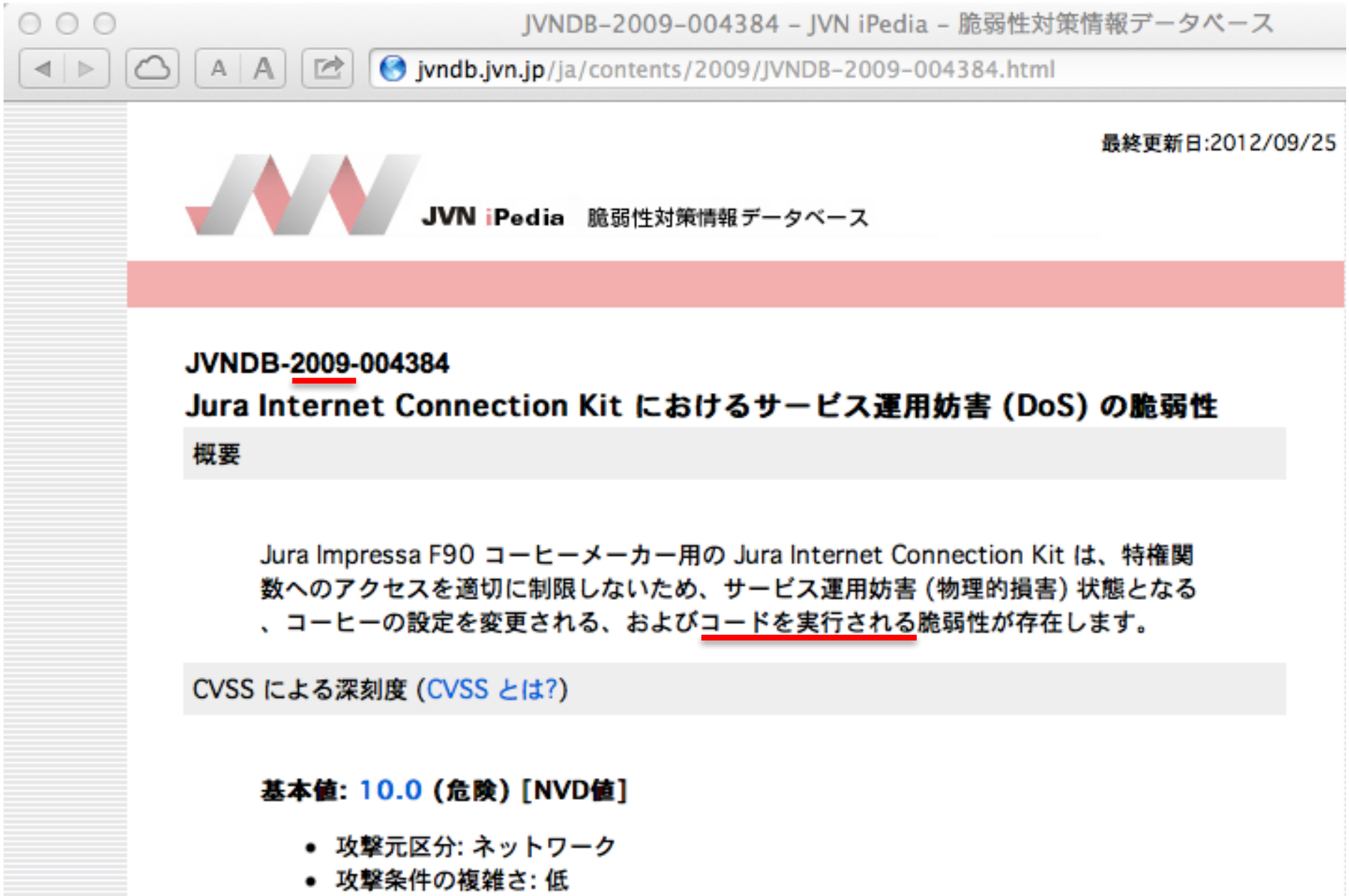


今やこういう時代に


Internet
特徴解析
挙動分析
August 23rd - 29th
August 16th – 22nd
August 9th - 15th
August 2nd - 8th
不審挙動の抽出・追跡
未知攻撃
特定・対策
トラフィックデータ収集
インフラ実験
家電・IoT
OA機器
新技術開発

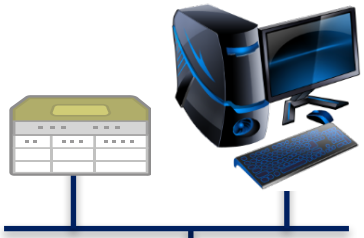
http://www.comparestoreprices.co.uk/coffee-makers/jura-impressa-f90-bean-to-cup-machine.asp

汎用化が進んだ結果...
意外なものにまで発生する脆弱性



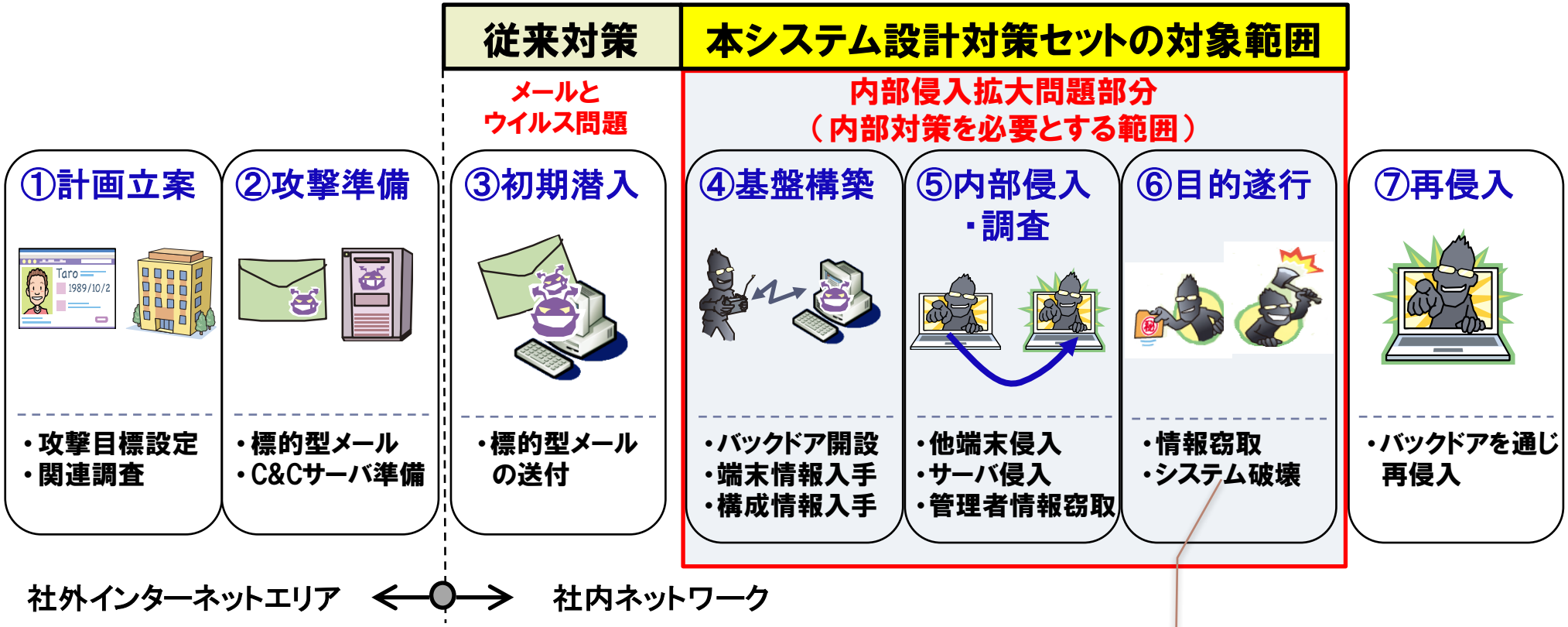
単発のインシデントに右往左往…からの脱却

- 止められないコンピュータの存在
  - 制御する対象が稼働し続ける限りは…
- サイバー攻撃による異常と故障による異常
  - 全体で見たらどちらも同じ
  - 一つのセンサー故障したらアウト？
    - 異常データからわかる事実もある
- 全体としての機能維持
  - 従来とは異なる考え方が必要
  - インシデント対応から
    アクシデント対処へ
    - ダメージコントロール
    - 縮退運用



侵入を前提とした対策の必要性

by IPA



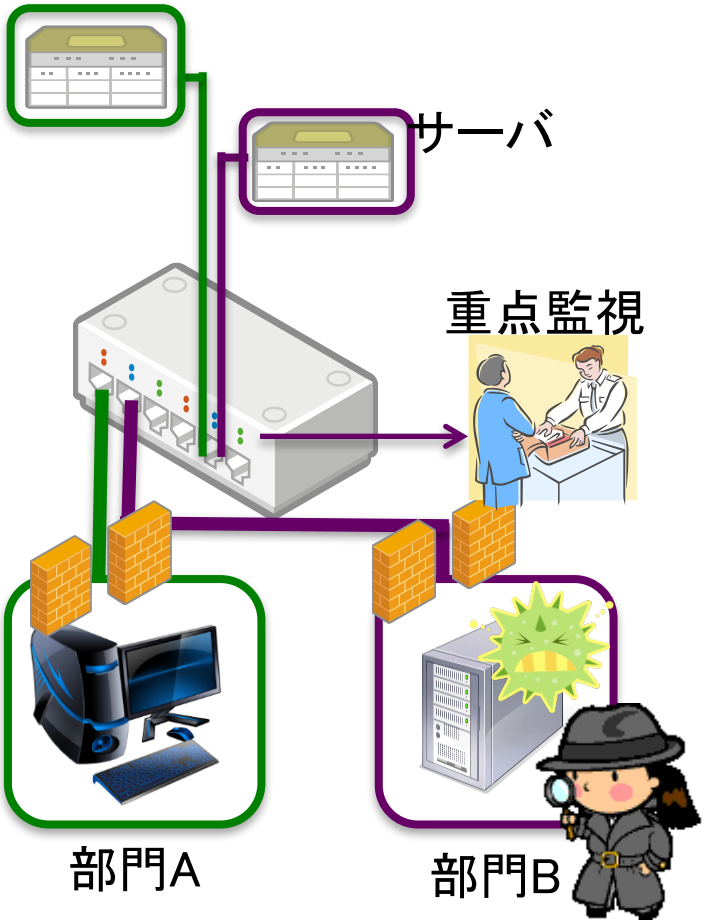
- 内部ネットワークでの対策必須
  - 解析対象のトラフィック量増大
  - 新たな解析手法が必要に
  - 中央省庁に加え独法でも対応が求められることに…

情報窃取
システム破壊

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

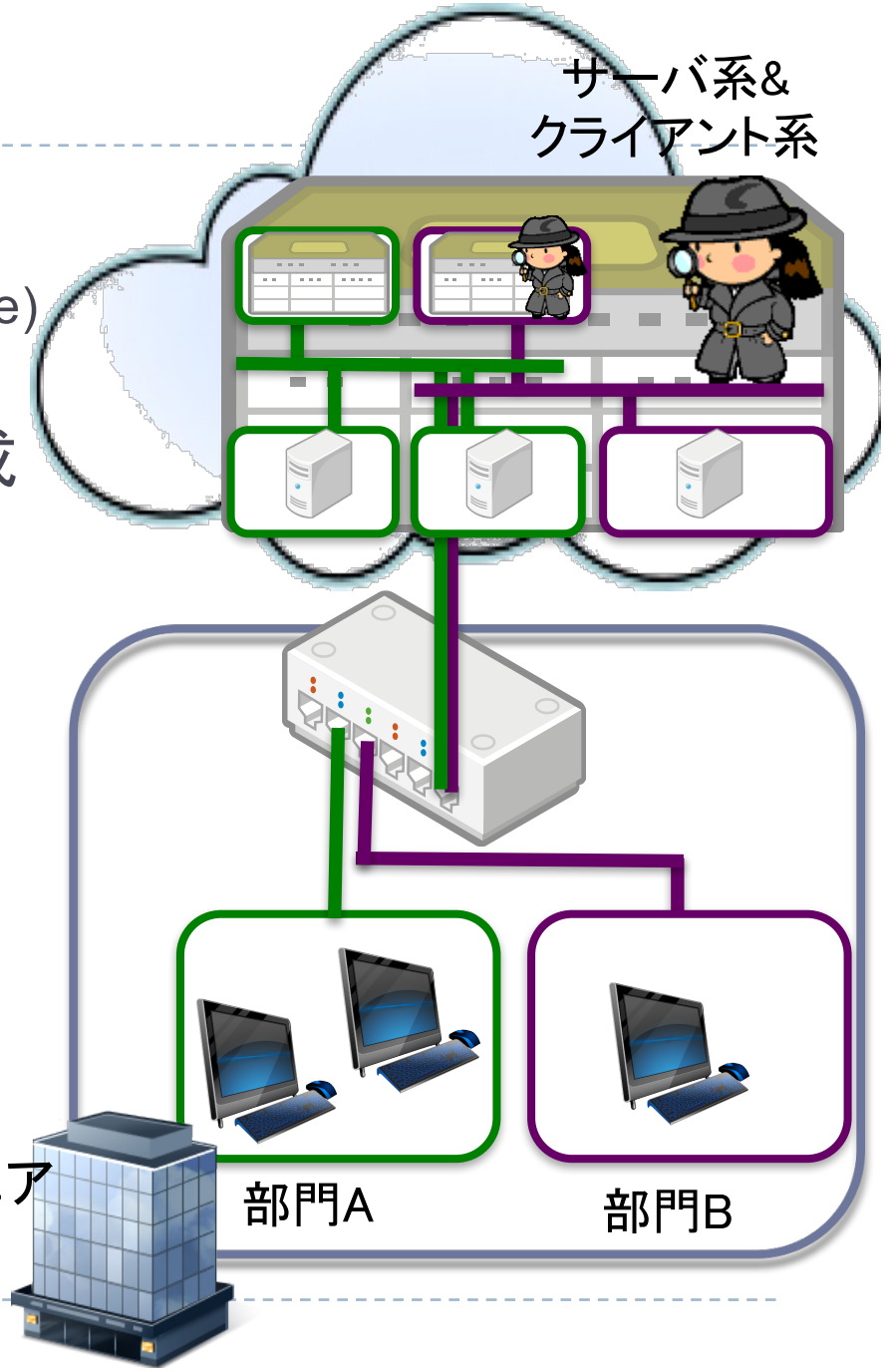
内部攻撃に備えたネットワーク構築

- ネットワーク分割とアクセス制御
  - 部門NWでのFW構築
  - 存在しないはずの通信を禁止
    - アクセス数をカウントするACLでも良い
- 部門NWをざっくりと監視
  - 部門間を跨ぐ通信
    - 通常であれば極わずか
    - 通常時に疎だった通信の急増
      - ✓ 設定ミス
      - ✓ 偵察活動の可能性
        - 重点監視のトリガー
          - 専門家召喚
  - 解析対象のトラフィック量を削減
    - 「対策」の低コスト化

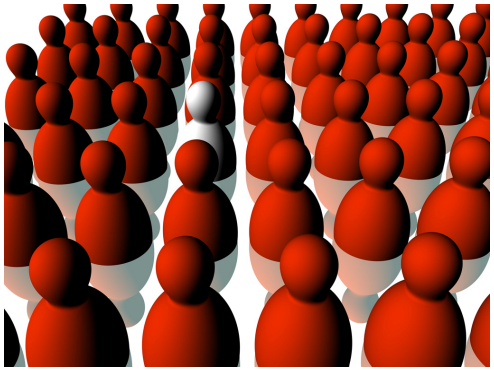


仮想化技術の導入

- 部署内への侵入阻止
  - VDI導入(Virtual Desktop Infrastructure)
    - サーバだけじゃなくクライアントも
  - proxy上でWebコンテンツ再構成
    - 添付ファイルもproxy上で展開
- トラフィック監視の集約
  - 標的型対策は内部監視必須
    - Server – client間
    - Client – client間
  - DC内での監視
    - VLAN間通信監視の容易化
    - Proxyのsandbox化
      - ✓ sandbox内で発症しないマルウェア
  - 迅速なインシデントレスポンス



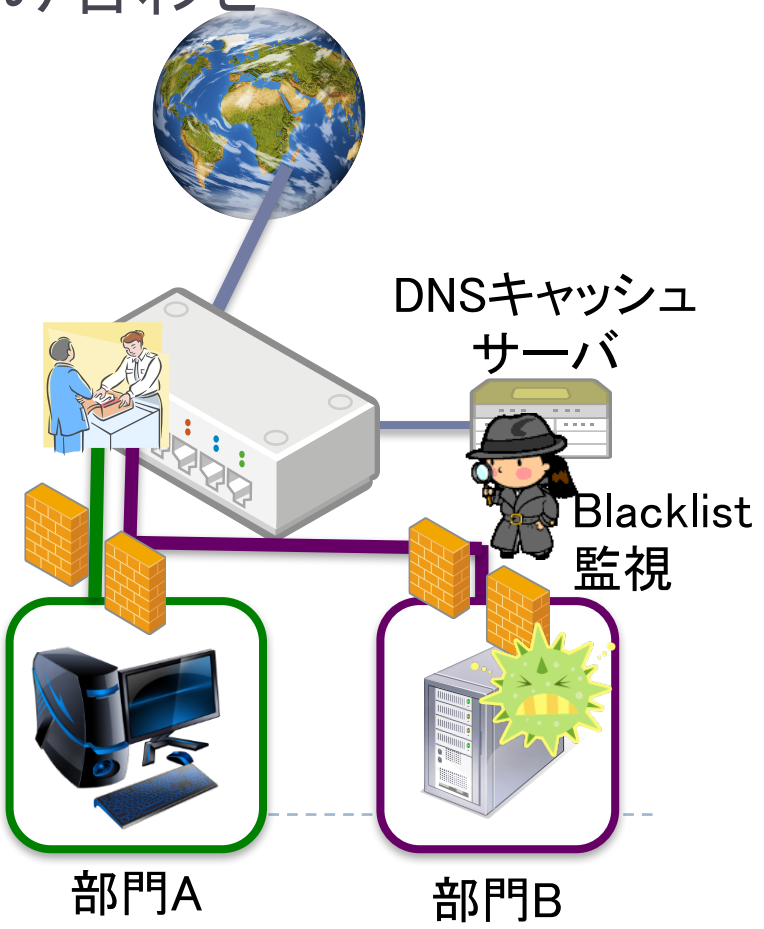
全体を俯瞰したサイバー攻撃の存在察知



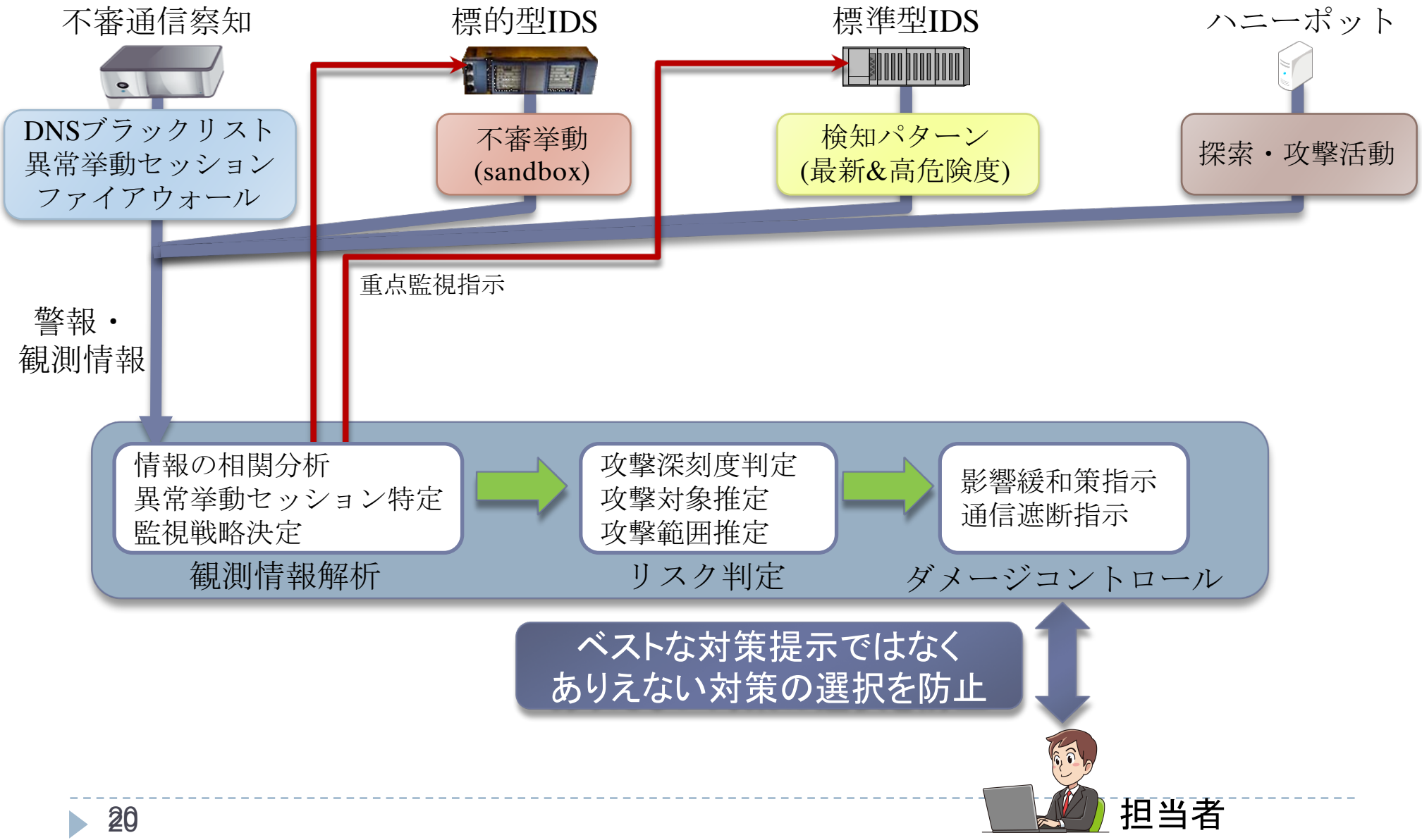
- 組織内ネットワークのサンプル監視
  - 不自然な挙動を示す通信の有無
    - 通信を行っている機器の特定
      - ✓ 潜伏期間中は通信頻度は極めて低い
    - 関連する機器の通信挙動の調査
- サイバー攻撃の疑いが濃厚
  - 被害発生機器と類似の通信挙動の有無を調査
    - 感染端末は複数台、を疑う(バックアップ機の存在)
- 縮退運用
  - 被害発生が局所的→その部分だけを隔離
    - 隔離処置後、異常な挙動を示す機器の有無を調査
  - 攻撃目標の推定→目標機器の保護
    - 被害発生部分からのアクセスを禁止＆その他のアクセスも精査
- 実は…監視カメラの不審者探しと同じアイデア

従来対策の統合による攻撃存在の察知

- IDSによる検知
  - 新規追加された検知ルール
  - 最近見かけなかった検知ルール
  - 複数の検知ルールだが有りえない組み合わせ
    - 不自然な誤検知
- Firewall
  - 禁止された通信の試み(内部から)
- 囮アカウント＆ハニーポット
- DNS監視
  - Blacklist情報を活用
- 目的
  - ステルス攻撃の尻尾を掴む



攻撃検知と解析の流れ


不審通信察知
標的型IDS
標準型IDS
ハニーポット
DNSブラックリスト
異常挙動セッション
ファイアウォール
不審挙動
(sandbox)
検知パターン
(最新&高危険度)
探索・攻撃活動
重点監視指示
警報・
観測情報
情報の相関分析
異常挙動セッション特定
監視戦略決定
観測情報解析
攻撃深刻度判定
攻撃対象推定
攻撃範囲推定
リスク判定
影響緩和策指示
通信遮断指示
ダメージコントロール
ベストな対策提示ではなく
ありえない対策の選択を防止
担当者

全体俯瞰によるセキュリティ対策技術開発

- 被害拡大の防止
  - 予想される被害範囲特定
- 可用性の維持
  - 継続させるべき業務特定

- 総合判断によるアクシデント対処
  - 重要情報の保護
  - 局所的な封じ込め
  - 可用性の確保との両立

早期対応の失敗 → 業務へ影響大

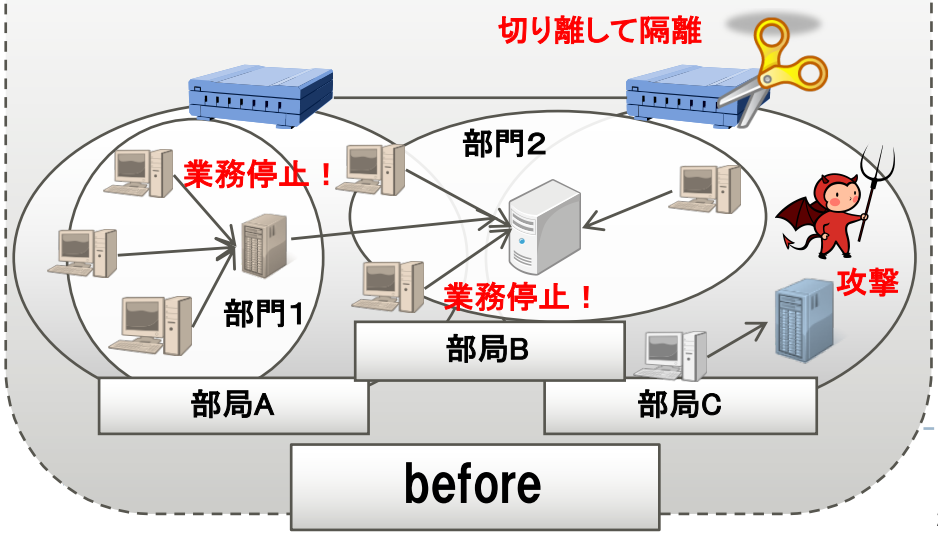
インシデントに振り回された対応

◆緊急対応プラン
- 不可能なプラン、プラン不在の組織多数

◆被疑/NW情報機器
- 選択肢は隔離のみ、機器の状況把握が困難

◆復旧手順
- BCPを考慮しないプラン

→結果的に対処放置 or 全面遮断



BCPを意識したアクシデント対処

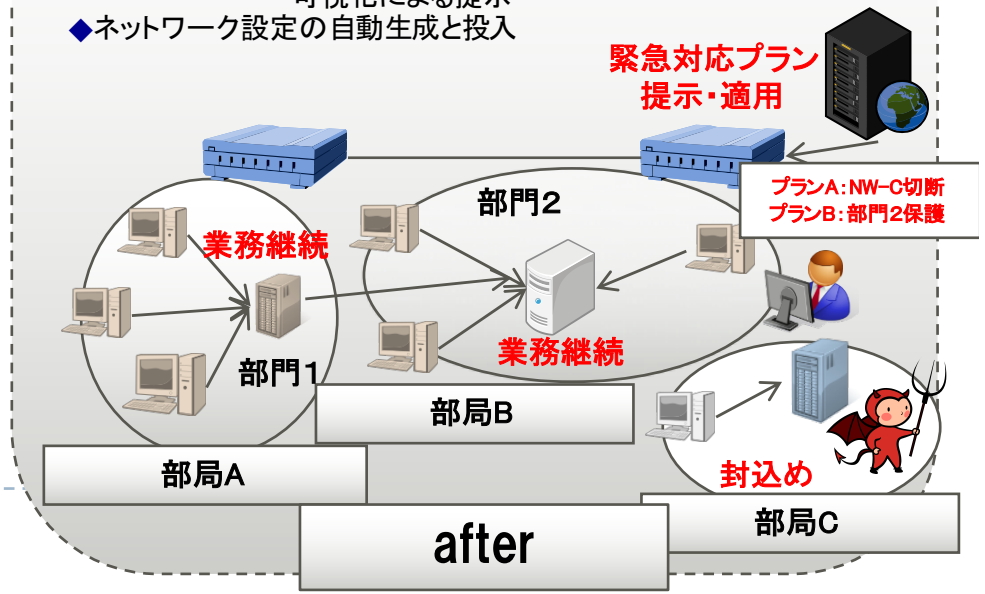
緊急対応の自動化/復旧支援

◆緊急構成情報の記述法
- 被疑機器/NWの重要度を定義、自動処理と影響評価を実現

◆緊急対応プランの自動生成と評価
- 緊急ポリシを処理((3)から提供)、設定後の変化や影響度を評価、段階的な強化/緩和プラン

可視化による提示

◆ネットワーク設定の自動生成と投入



進化する対策技術

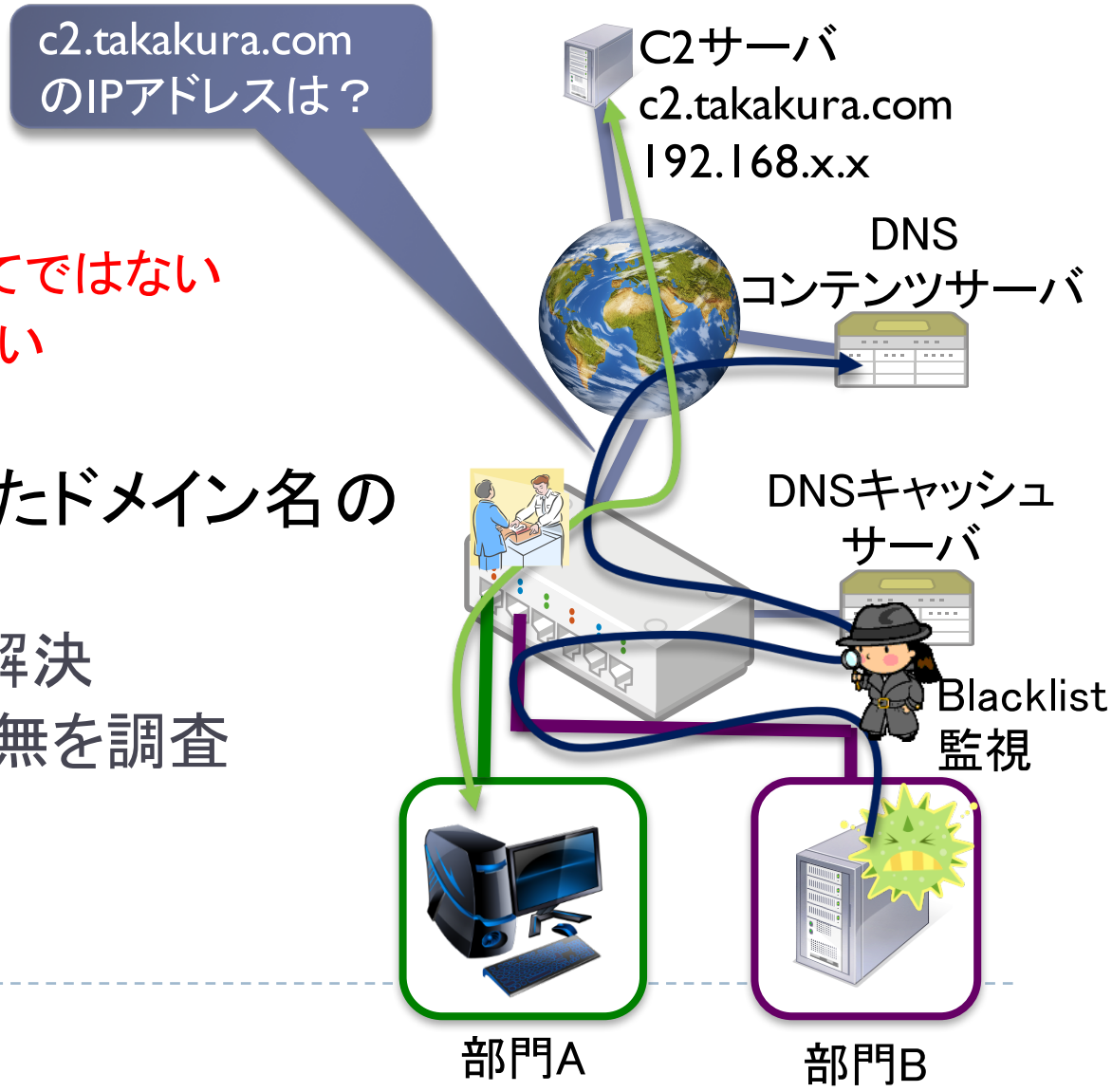
- 攻撃検知手法
  - 理論と現実の限界
    - ベンチマークデータでは99.9…9%の検知性能＆0.0…1%の誤報
    - 実際には20%の検知性能と30%の誤報
      - ✓ 相手が次にどの駒を取ってどこに置くか？
- 海外ベンダーの動向
  - 攻撃の方向把握
    - ○○先生が狙われているらしい
      - ✓ 相手が狙っている駒はどれなのか？
        取られそうになったら阻止する…全員で猛タックルするのか？
- 今後の研究課題
  - 攻撃対象の事前保護
    - ○○先生が狙われているなら…
      - ✓ どう保護すべきなのか？

AI技術活用？

不審な通信の検知(DNS blacklistの場合)

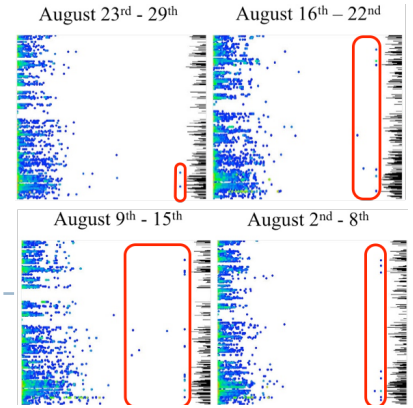
- アクシデント対処の注意点
  - 通信経路多重化
  - 指揮系統多重化
  - 潜伏中のマルウェア
    - 今見えているものが全てではない
    - 感染機器は本命ではない

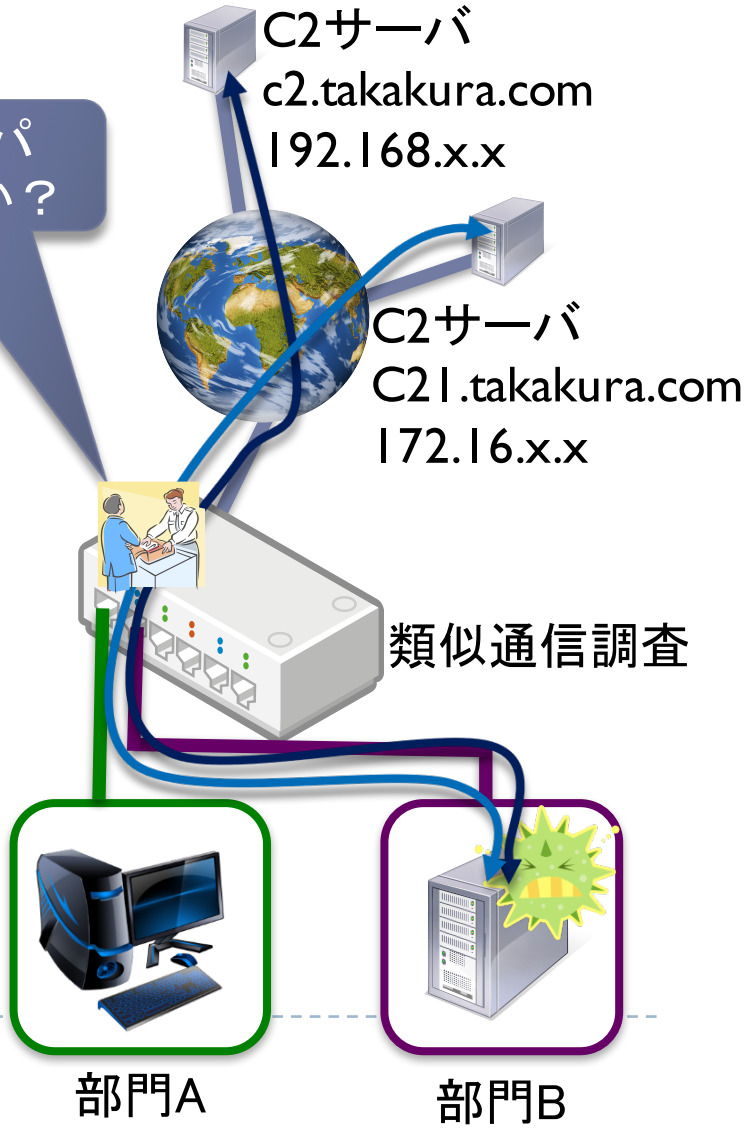
1. Blacklistに登録されたドメイン名の解決要求を検知
   - 内部のマシンが名前解決
   - C2サーバとの通信有無を調査
     - 感染疑い機器の特定



被疑端末の挙動調査

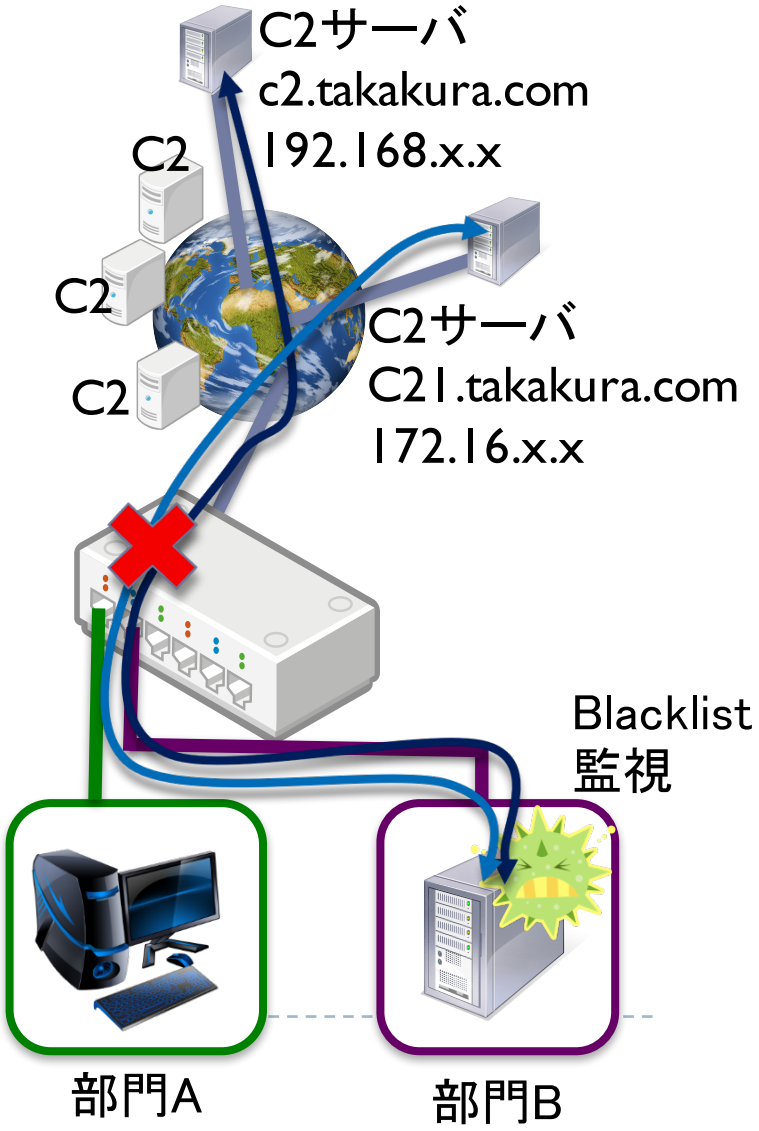
1. 被疑機器と外部との通信を精査
   - さらなる不審な通信パターンを抽出
     - Sandboxによる挙動調査
2. 類似する通信を調査
   - アクセス挙動の類似性判定
     - 潜伏中のマルウェアの洗い出し
       - ✓ 潜伏中でも定時交信がある
3. 攻撃目標の推定
   - どの方向に向かっているか？
   - 重要情報の存在？





封じ込めとダメージコントロール

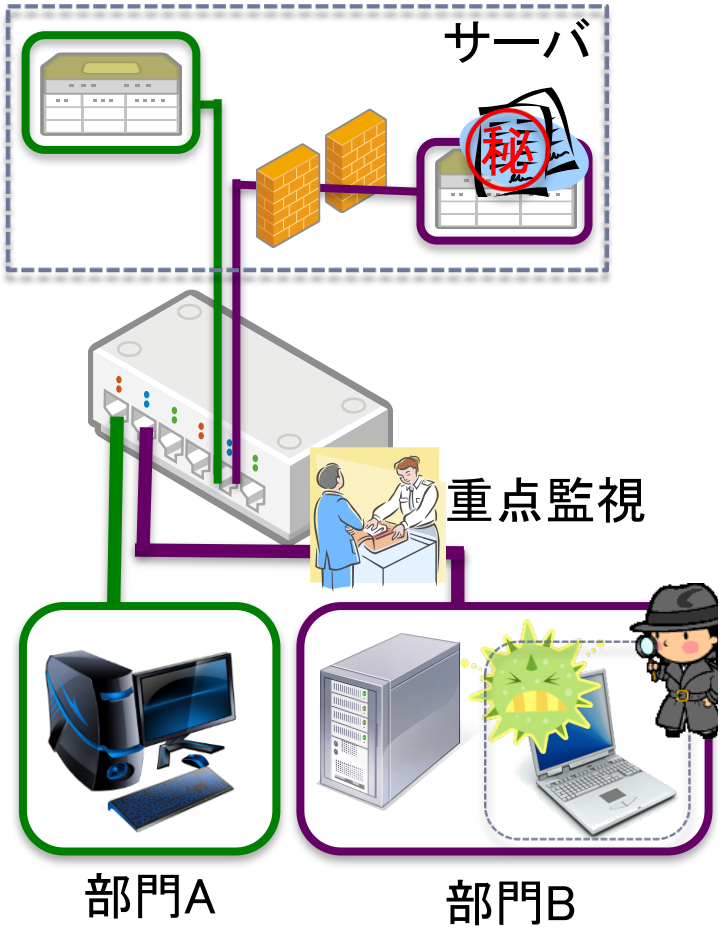
- 封じ込め
  1. C2サーバ全てとの通信を遮断
  2. 全体の通信挙動を観察
  - 予備C2サーバへの接続試み
- ダメージコントロール
  - アクシデント全体を俯瞰した対応
    - リスク要因の高いものから順に対応
      - ✓ 機器の重要度も考慮
    - 被害の深刻化や拡大防止が優先
      - ✓ 状況次第で重要度の低いものは放棄
    - 要保護機器の警護強化＆破壊阻止
  - 再攻撃への備え(リソース配置)



ダメージコントロールをかけながらの
臨機応変な運用

縮退運用による機能維持

- 未感染機器のみのセグメント
  - 継続利用(重要情報アクセス許可)
  - 感染機器からの保護
    - 臨時のアクセス制御
- 感染(疑い)機器の存在するセグメント
  - 原則はネットワークからの切り離し
  - 機器の重要度を考慮
    - 業務に不可欠など
  - 業務継続とリスク緩和のバランス
    - セグメント内通信限定
    - 感染機器を監視下に
    - インターネットとの通信禁止
- 重要情報の保護
  - 感染機器からの直接/間接の到達を排除



まとめ

- サイバー攻撃の高度化
  - 攻撃の完全阻止は困難
  - 攻撃によるアクシデント発生を前提とした対策
- 新たな対策手法の必要性
  - ネットワーク分割＆アクセス制御
  - 各種監視による攻撃の兆候察知
    - 監視対象の絞り込み＆精査による状況把握
  - ダメージコントロール＆縮退運用
    - アクシデントの状況に応じた動的な対策適用
      - ✓ 対策適用と並行した状況把握
    - 業務継続を意識した縮退運用
      - ✓ アクシデントの影響がない or 僅かな箇所は運用継続
      - ✓ 攻撃の目標をいかに保護するか？
      - ✓ 影響はあるが重要度が高い箇所は様子を見つつ運用継続