大学間連携に基づく情報セキュリティ体制の基盤構築

国立情報学研究所
NII SOCS(NII SECURITY OPERATION COLLABORATION SERVICES)

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

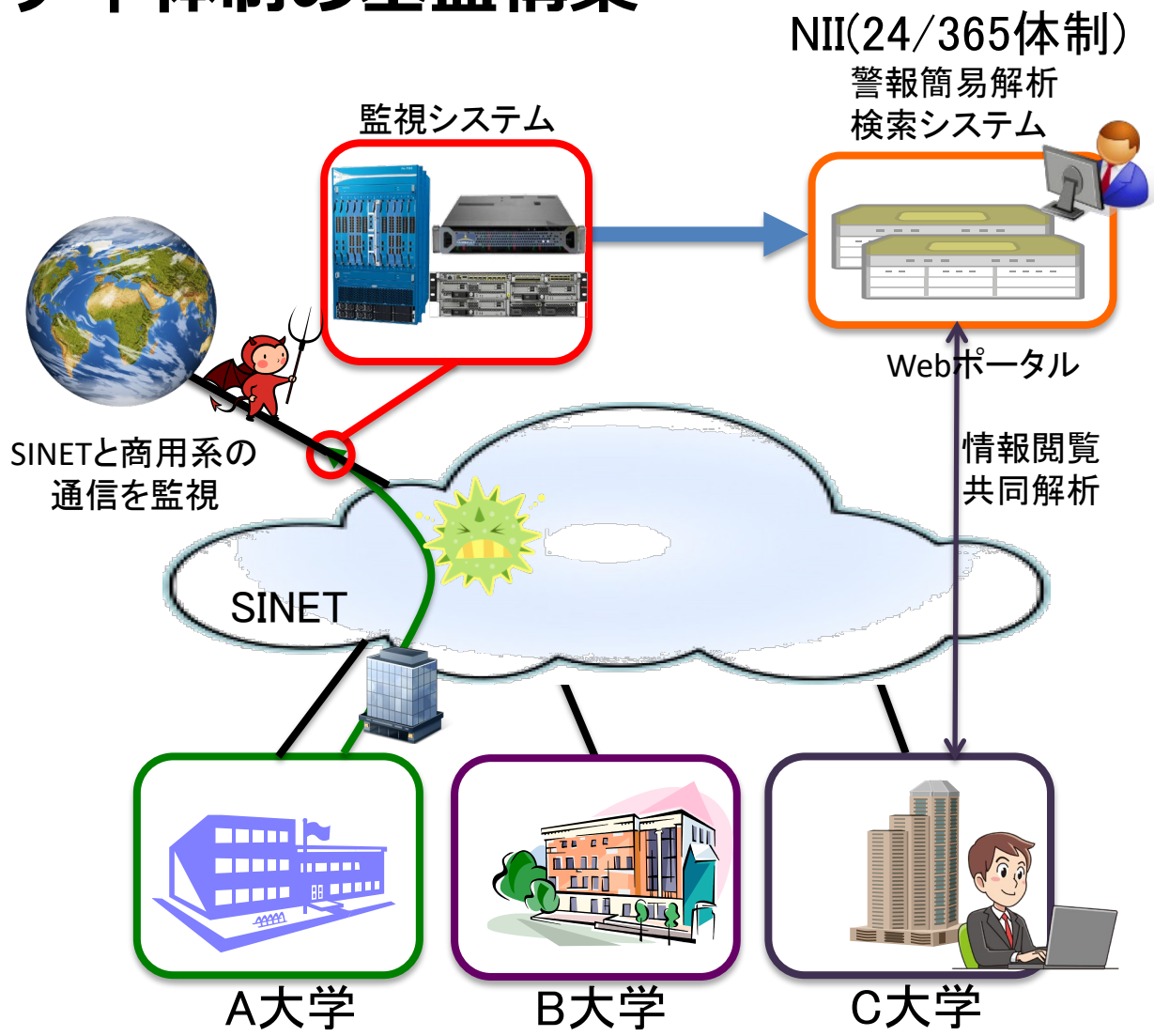
NII-SOCS発足の経緯

- サイバーセキュリティ基本法における国立大学への要請(第32条)
  - 2018年秋国会で改正案審議(主に、オリパラ対応…)
- 中央省庁に加え、独立行政法人や府省庁と一体となり公的業務を行う特殊法人等を、内閣サイバーセキュリティセンター(NISC)の制度に基づく監視・監査の対象に追加する。
  →独法は第2 GSOCで監視

「日本再興戦略」改訂2015
(2015年6月30日閣議決定)

- 国立大学法人固有の問題
  - 学生(民間人)の通信が混在
    - 学生と教職員でネットワーク論理分割が必須となるが…非現実的
  - 学問の自由との兼ね合い
  - 監視経費は各法人に請求(端末数、流量に比例)
    - 研究系独法と比べても桁違いな大学
      - 構成員数(端末数)、対外接続帯域
- 国立大学法人は自主的な対策強化へ
  - セキュリティ監視能力ではなく、インシデント対応能力の向上(5年計画)

- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等の運営費交付金から拠出
    - 7.8億(2016)、8億(2017)、8億(2018)
      - 機能強化と予算圧縮を常に意識
  - 3種類の監視システム
    - Sandbox搭載IDS (paloalto)
    - シグネチャベースIDS (Cisco FirePower)
    - DNSトラフィック監視 (Damballa CSP)
  - 簡易解析システム＋Webポータル
    - 膨大な警報に緊急度・危険度の割付
  - 外部セキュリティ機関との情報共有
    - 国内：NDAに基づく攻撃情報の提供
      - サイバー攻撃拠点のNIIへの事前通知
      - NIIは通信の有無のみを回答
        - » セキュリティ機関：NISC経由で文科省へ
        - » NII：大学に直接通知
    - 海外：MoUに基づく技術情報の共有



２０１８年４月～９月末までの通知件数

中項目		累計 (2018/4/1～9月末)
通知件数		3617
	分類１：マルウェア感染の可能性	2760
	分類２：アプリケーションソフトの脆弱性によるもの	225
	分類３：C&Cサーバーとの実通信の可能性	480
	分類４：ブルートフォース攻撃の可能性	0
	分類５：辞書攻撃の可能性	0
	分類６：標的型サーバー攻撃に関与している可能性	0
	分類７：man-in-the-middle 攻撃	0
	分類８：DNS Amp 攻撃への参加	0
	分類９：その他	152
誤報件数		2

研修の実施状況

研修内容	開催年月と開催数	参加機関数と参加人数
NII-SOCSの概要説明、 ポータルサイトの操作説明　等	2017年4月　2回	37機関、61名
ポータルサイトの操作説明及び改修内容、 NII-SOCS検知情報の事例説明　等	2018年1月　2回	13機関、30名
サービスポータルの基本操作、サイバー攻撃手法、警報情報の基本的な分析などの学習	2018年6-8月　4回	41機関、82名
警報情報の基本的な分析、サイバー攻撃手法、演習を含んだインシデント調査方法の学習	2018年10-12月　6回	52機関、91名（予定）

- 監視能力の増強
  - 主に、ストレージ増強＋解析ツール導入(Elasticsearchなど)
  - マルウェアダウンロード、C2サーバへの通信検知機能の強化(既存センサの弱点を埋める)
  - 脅威情報サービスの購入(DarkWebなどの調査追跡)
- ポータルサイトの改良
  - マルウェアダウウンロード機能(自組織に関するもののみ)
  - 警報情報ダウンロード用のAPIの提供
    - 研究目的でのダウンロードは禁止(セキュリティポリシーで認められない機関)
  - 情報共有ポータルサイト(参加機関同士でスキル向上)
  - 週次・月次レポート
- 研究用データの公開(2018年度末開始予定)
  - 「大学間連携に基づく情報セキュリティ体制の基盤構築」の目的の一つ
    - 研究者への研究データ提供による研究の活性化と研究成果の還元による大学の体制強化への寄与
  - 統計化・匿名化処理を施したベンチマークデータ
  - バラマキ型の新種マルウェア情報の情報セキュリティ研究者への提供
    - 参加機関へ、データ採取承諾のお願い文書送付の準備中

- 現NII-SOCSは2020年度までの運用を想定
  - 最終年度までに「インシデントが起きても粛々と対応する体制」を各機関に整える
    - ほとんどの機関がその体制はできつつあると思われる
    - インシデント発生頻度の高い機関での課題は残っている
  - 2021年度は機材撤収や次期計画への引き継ぎの年
    - 次期SINETとの連携
- 次期NII-SOCSの可能性
  - 現在のスタイルでの継続は難しい
    - 5カ年計画の約束
    - サイバーセキュリティ基本法改正の動き
  - 完全撤退は認められないことは理解
    - NII負担＋受益者負担形式への移行
      - 他省庁研究機関、公立・私立大学への対応
  - 何らかのアクションは必須
    - 現NII-SOCSは国大協から文部科学大臣への要請が原点
    - 政府関係との調整に2年はかかる(通常なら)

最悪のシナリオはNII-SOCS終了
それに備えた体力作り