資料1－2
AI for Scienceを支える研究データの管理・利活用と流通の在り方ワーキンググループ(第2回)
令和8年2月13日

セキュリティについて

2026年2月13日

国立情報学研究所

NII-SOCS（ニーソックス）とは？

NII-SOCS

大学間連携に基づく情報セキュリティ体制の基盤構築

NII Security Operation Collaboration Services

ネットワークを監視するSOC(Security Operation Center)とは異なる

NII-SOCS発足の経緯

- 日本年金機構の情報流出事案(2015)
  - 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→独法は第二GSOCで監視
    - 経費は各独法が負担
      - 分担額算出根拠…端末数や流量
- 大学固有の問題
  - 学生等(民間人)の通信
    - 教育研究→学生等と教職員が一体として活動→NW分割困難
    - 外部からの通信の大部分は民間(市民や民間企業)
  - 学問の自由との兼ね合い
  - 独法と比べて桁違いな端末数(学生も含めると数十万台)と流量(10-100Gbps)
- 暗号通信の比率増加(当時でも50%以上、現在90%以上)

NII-SOCSの位置付け

■サイバーセキュリティ戦略（平成30年7月27日閣議決定）
- 学術情報ネットワークを運営する機関は、国立大学及び大学共同利用機関と連携し、サイバー攻撃を観測・検知・分析するシステムを構築し、情報提供を行うとともに、監視能力の機能維持・強化及び戦略マネジメント層の育成に向けた共同研究や技術職員への研修を実施すること

■サイバーセキュリティ2024 (令和6年7月10日サイバーセキュリティ戦略本部)
- 国立情報学研究所(NII)において、引き続き国立大学法人等のインシデント対応体制を高度化するための支援を行う。
  1) NII-SOCSの監視機器を強化し、SINET外との不審通信の発見を行う。
  2) NII-SOCSが観測した警報通知、外部機関から情報提供を受けた場合、参加機関に対し最新の情報提供をいち早く行う。
  3) 情報セキュリティ担当者向け・戦略マネジメント層向けの研修を行う。

NII-SOCSのミッション

1. 重大なサイバー攻撃の検知及び情報提供
   - SINET上にサイバー攻撃を観測・検知・分析するシステムを構築し、かつ、国内外の関係機関との情報共有に基づき、国立大学法人等に攻撃の危険度や緊急度に応じた情報提供を行う。
2. サイバーセキュリティ人材の育成
   - 国立大学法人等のサイバーセキュリティを担当するCISO、管理職、CSIRT要員等の研修を実施し、サイバー攻撃への対処能力の高度化を図る。
3. 研究用データの提供（現在は参加機関のみ）

NII-SOCSで観測された
①統計化・匿名化処理を施したベンチマークデータ
②複数の大学で観測されたマルウェア(安全保障貿易管理の対象)
を研究用データとして提供する。

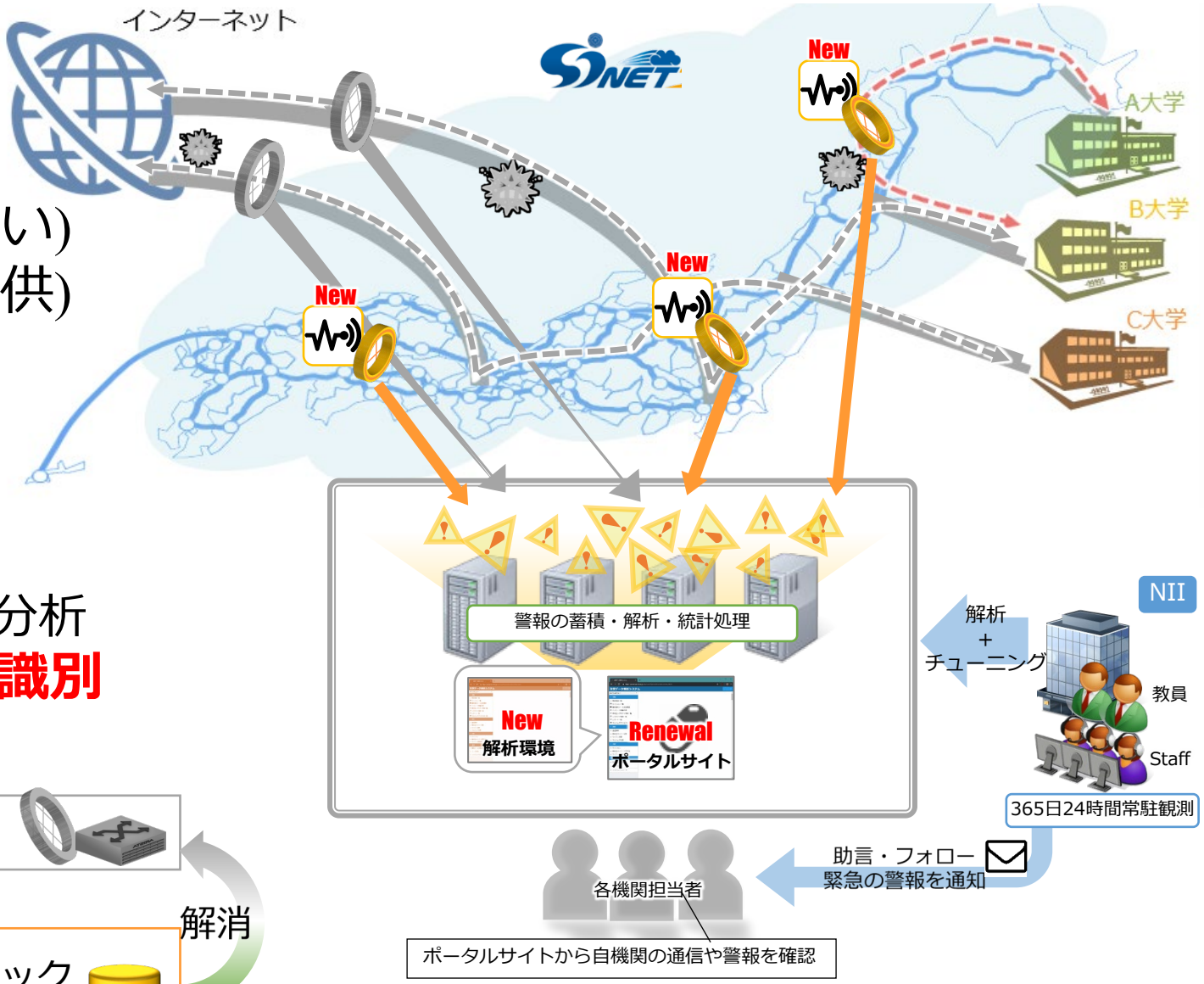
NII-SOCSの概要

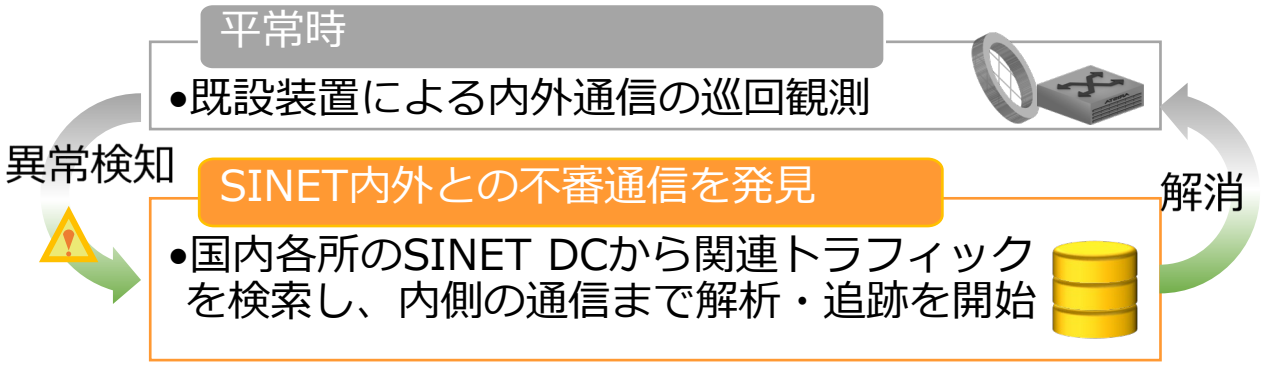
■対外観測
- ●通信挙動を分析(中身は見ない)
- ●専門情報と照合(外部から提供)

→不審通信の**発見**

■内部観測
- ●不審通信に関連する通信
  - ◆内部観測センサへ転送
  - ◆SINET内部の攻撃を追尾・分析

→攻撃の可能性がある通信を**識別**

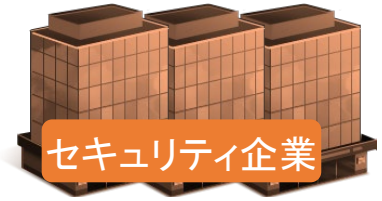




NII-SOCS
観測の流れ

- NII-SOCSから通知
- インシデント対応等は参加機関自身で実施
  (一種のOJT)

外部セキュリティ機関との情報共有
(国内・国外)



専門情報(犯罪グループ情報等)
- 民間系脅威情報(アジア)
- 民間系脅威情報(汎用)
- 民間系脅威情報(欧米)
- 攻撃者情報調査サービス

情報共有

有償情報提供

情報共有

解析
＋
チューニング

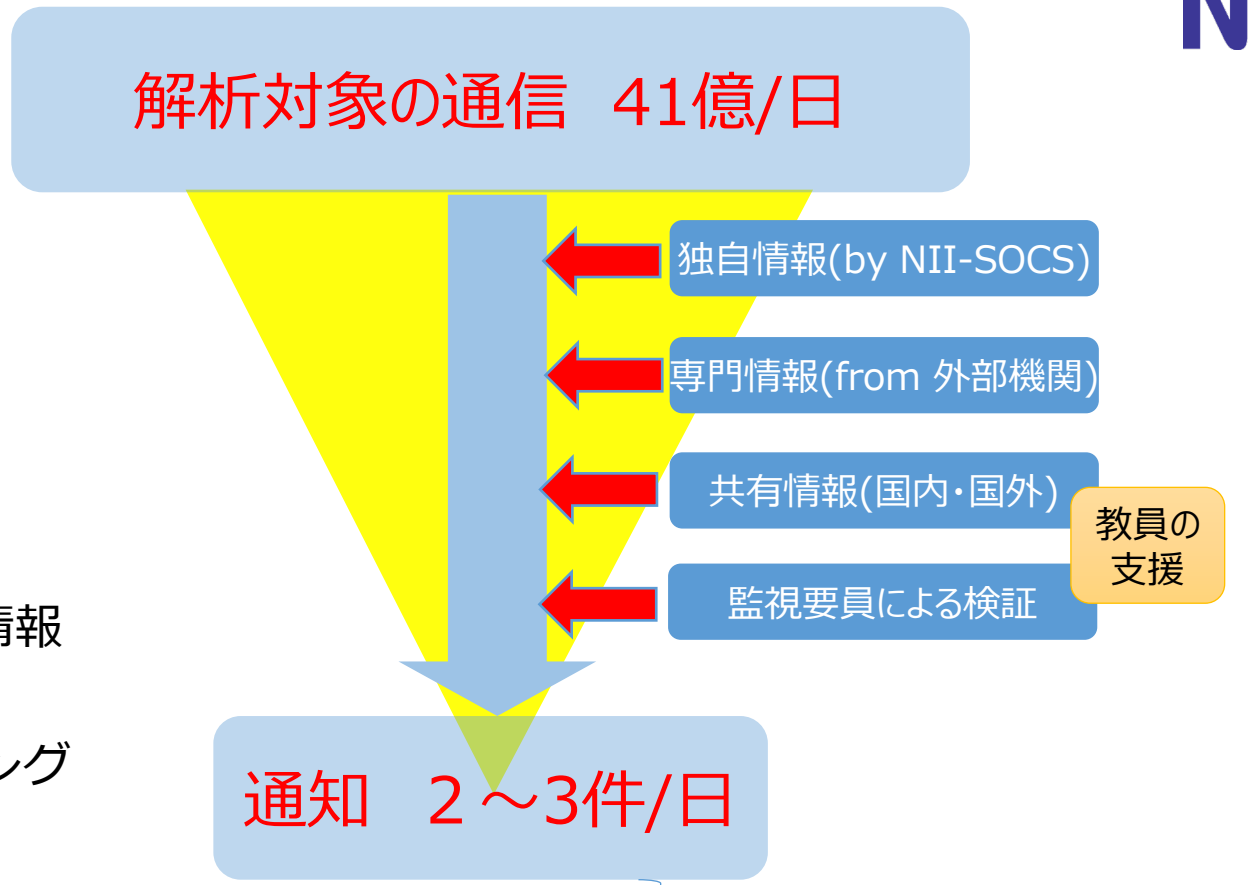
365日24時間常駐監視

助言・フォロー
緊急の警報を通知

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
通信の自動分析

- 大原則
  - 通信の中身は見ない
    - 解読できない暗号通信80-90%
    - 通信の秘密の保護(民間の通信)
- 各種情報を用いた分析
  - 自動照合
    - NII-SOCS独自の情報収集
      - マルウェア分析、SNS等からの情報
    - 外部専門組織から提供される情報
      - 攻撃関与が疑われる通信先
      - 攻撃者グループのプロファイリング
  - 手動照合
    - MoUやNDAに基づく情報共有
      - JPCERT/CC、JC3、韓国KISTI、米国CISA(提携先を介した共有)
    - 監視要員による最終チェック
    - 概ね5～30分で完了
  - AI, 機械学習での判定
- 分析完了後は完全自動処理



緊急性が高い場合は
後回し
直ちに自動処理を開始

NII-SOCSと参加機関との連携の成果

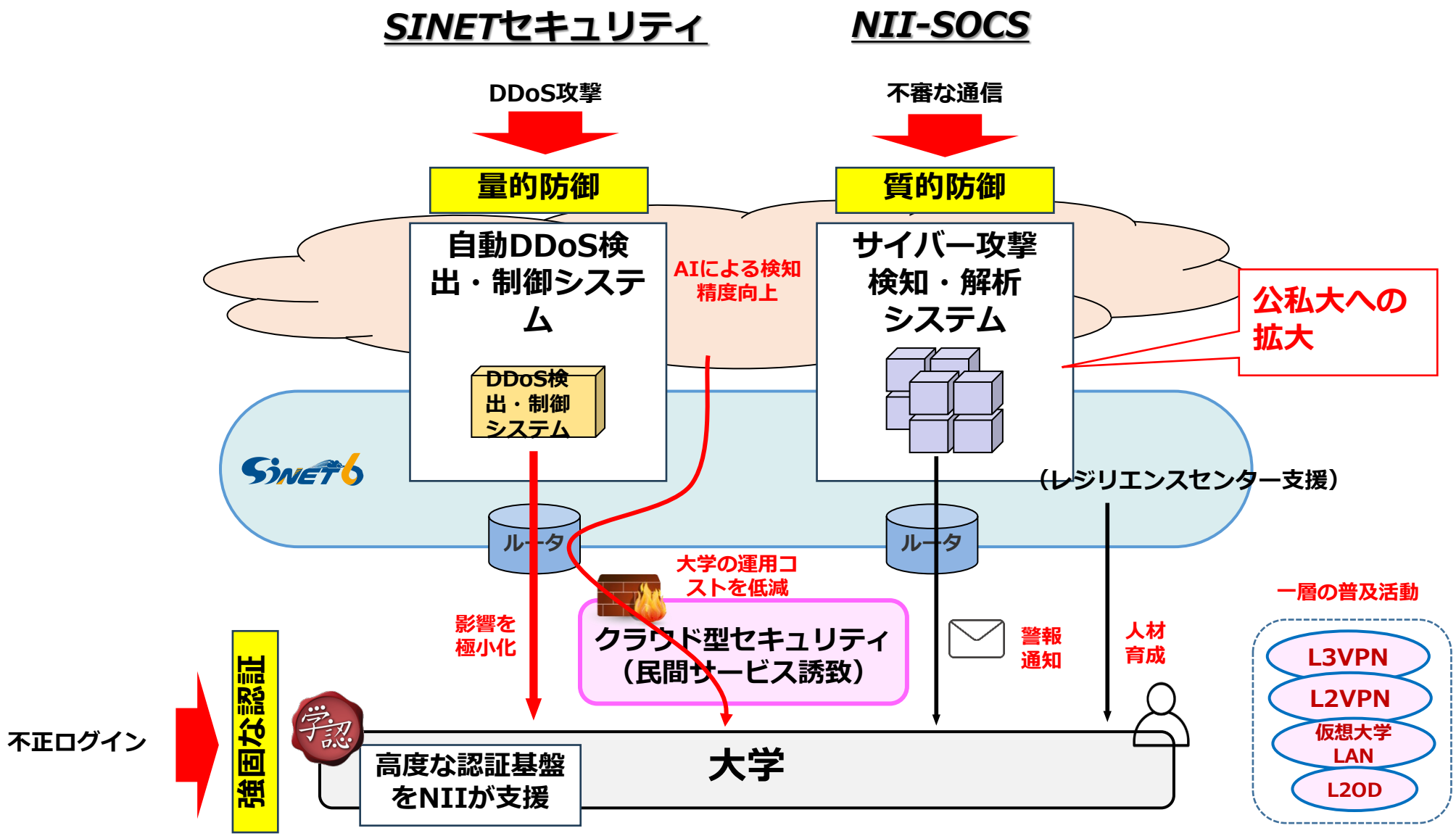
- 2017年の試行運用開始から約9年
  - 参加機関の即応力は著しく向上…放置はまず無い
- 攻撃開始前の予防措置にも対応
  - VPNサーバなどの脆弱性情報に関するの提供→被害発生前に対応
- 被害発生時の初期消火の迅速化
  - インシデントマネジメント研修などでの体験も活かす

過去６年間、スクープ記事となった情報インシデントはゼロ

インフラ面からみた次期セキュリティ（案）

NII

・SINETセキュリティとNII-SOCSを一体的に運用、希望するすべての国公私大にNII-SOCSサービス提供。



サイバー攻撃に対する耐性の強化（再掲）

- NII-SOCS機能拡張：公立・私立の希望する高等教育機関へのサービス拡張にむけた検討を進める。
- 現行の自動DDoS Mitigationは継続する。
- 非常時認証サービス代行、クラウド型ファイアウォール等、複数大学で共用する仕組み確立を推進する。