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)

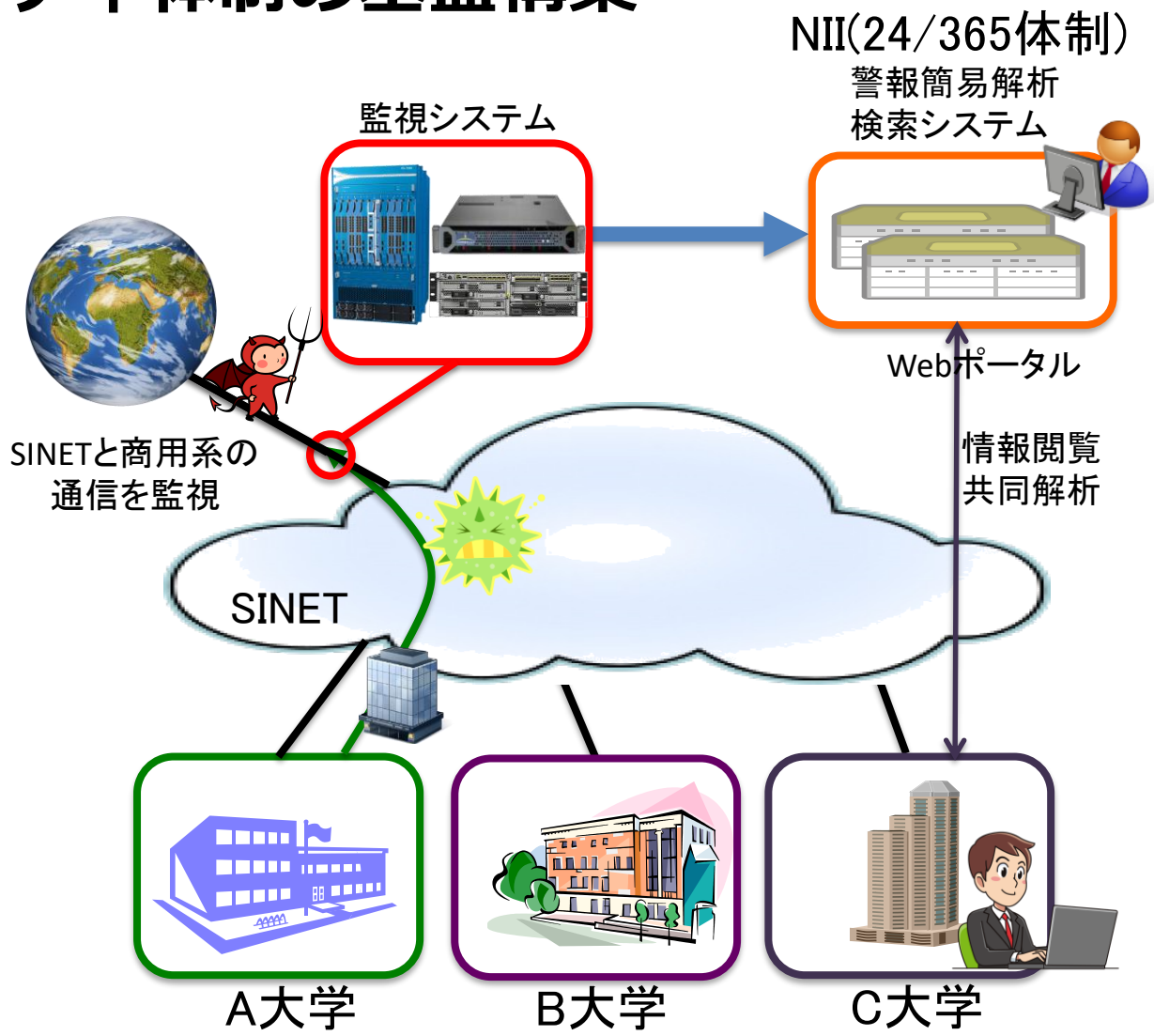
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

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)
- 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
- 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)

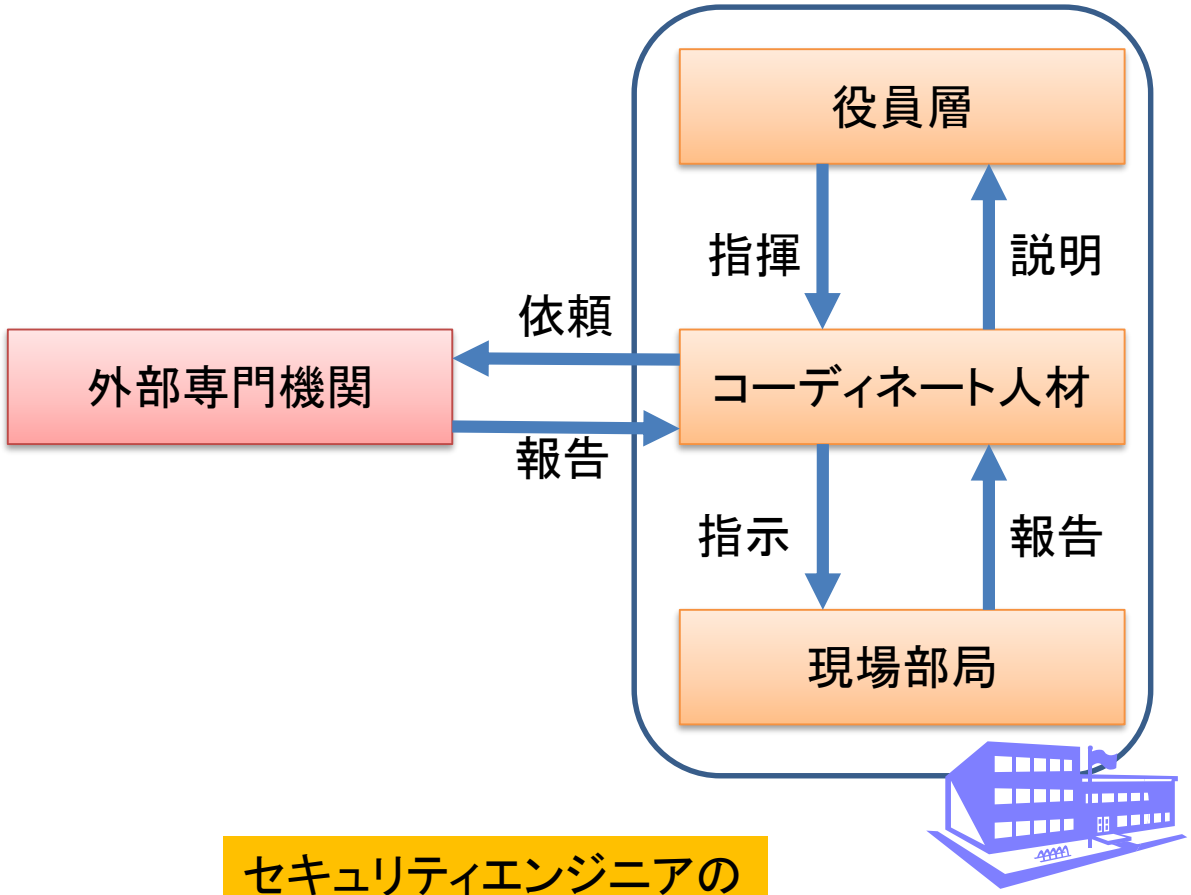
「日本再興戦略」改訂2015
(平成27年6月30日閣議決定)

- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等の運営費交付金から拠出
    - 7.8億(H28)、8億(H29)
    - H30以降は
  - 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



NII-SOCS育成する人材とは

- コーディネート人材
  - インシデント発生時
    - 外部セキュリティ専門機関との連携
    - インシデント発生現場との連携
  - アクシデント収拾時
    - 経営層へのアドバイス
    - 経営層の決定を伝達
  - 自組織での育成が必須
    - 人材を引き抜いてきても意味がない
- 中央省庁も同様の流れ
  - 担当審議官の設置
  - 橋渡し人材
    - 4年間で1,000人程度
    - 担当審議官の補佐



セキュリティエンジニアの
育成ではない

運用チームの物理環境

- 監視システム
  - 通信事業者のデータセンター内に設置
- 警報解析システム等
  - 入退室管理された隔離区画に設置
  - 平常時は無人
- 運用チーム居室
  - NII外に専用ルームを確保
    - 事務部門はNII内(SINETチームとの連携のため)
  - 入退室管理(24H/365D管理)

NII機能停止時を想定したセキュリティ運用バックアップ体制

- 別回線によるサイバー攻撃検知システムへのアクセス経路を確保
  - システムへの直接アクセスとなるため通常は機器の状態監視のみに使用
- 状況に応じてバックアップサイトとSOCの窓を遮断

巡回監視と監視対象

- 各監視システム
  - IPS機能ではNPCの実用性能は20Gbps程度
    - 2～4枚搭載
  - 対外接続線は全二重で200Gbps以上
- 全トラフィックを一括監視することは不可能
  - 監視システムの実用性能に応じて巡回監視
    - 利用申請のあったIPアドレスブロックのみ
  - シグネチャも限定
    - 最新1ヶ月分で高危険度のもの
    - Brute force攻撃系のもの
- セッションデータの取得
  - IPS機能の性能不足を補完
  - 変化点分析や機械学習による異常セッション検出

- トラフィック分散システム@SINET DC
  - 監視対象となるIPアドレスのみ
    - 全パケットを各種攻撃検知システムへ転送
- 各種攻撃検知システム@SINET DC
  - 転送された全パケット
    - ペイロード(通信の内容)の全てを検査
  - 検知した攻撃情報のみを解析システムへ転送
    - ヘッダ情報
      - タイムスタンプ、IPアドレス、プロトコル、ポート番号
    - アプリケーション情報
      - 例：Google DOC、送信・受信バイト数、継続時間
    - 検知情報
      - 例；不正サイトのドメイン名、検知文字列

» ペイロード中の該当部分のみ

監視画面の例

- **NII-SOCS運用者・大学担当者共に同一のWeb UIを使用**

- 警報160万件、2億セッションから…不自然な状態を検出

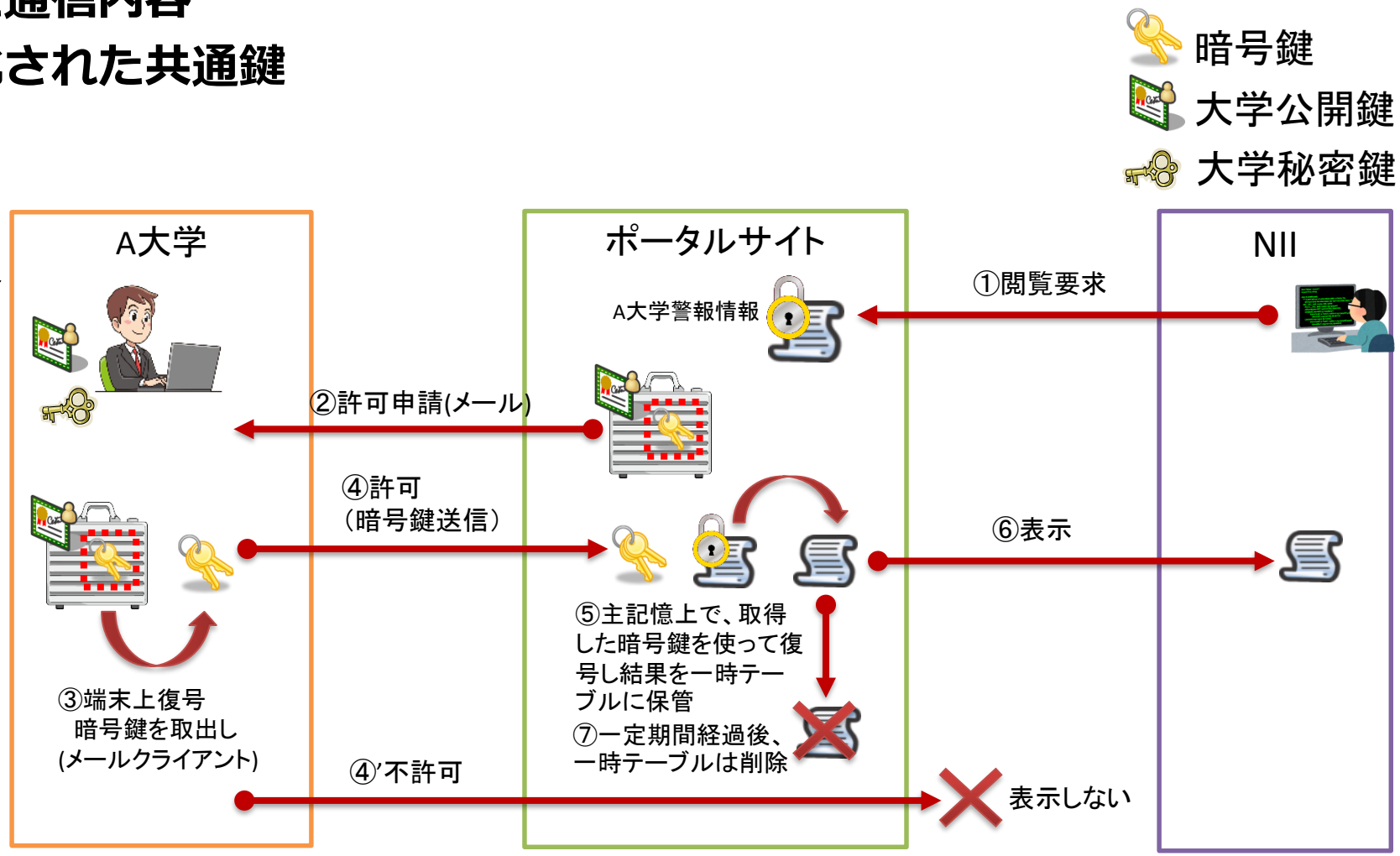
送信元IP	受信先IP	アプリケーシ	送信元ポート	受信先ポート	プロトコル	送信バイト	受信バイト	送信パケット	受信パケット
B.B.B.170	A.A.A.74	incomplete	54034	25	tcp	573	0	8	0
E.E.E.142	A.A.A.74	incomplete	53006	25	tcp	306	0	5	0
B.B.B.170	A.A.A.74	incomplete	54087	25	tcp	573	0	8	0
B.B.B.170	A.A.A.74	incomplete	54110	25	tcp	573	0	8	0
A.A.A.74	G.G.G.235	incomplete	62127	25	tcp	10179	0	23	0
A.A.A.74	H.H.H.26	incomplete	2843	25	tcp	19097	0	29	0
C.C.C.75	A.A.A.74	smtp	2742	25	tcp	608	1012	9	13
D.D.D.39	A.A.A.74	incomplete	16068	22	tcp	60	0	1	0
F.F.F.179	A.A.A.74	incomplete	18891	23	tcp	60	0	1	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	J.J.J.29	smtp	55684	25	tcp	13693	1606	25	17
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0

- 検知の根拠となった通信内容(ペイロード情報)
  - 暗号化後にDBに保存
  - 閲覧には大学の許可が必要
    - NII-SOCS単独で復号はできない
      - 法執行機関からの要請でも戻せない
        - » 「鍵は大学から受け取ってください」
    - 実装に若干の妥協はある
      - 当月分だけ技術的には解読可能
        - » 鍵をかけるためには鍵が必要
  - 閲覧記録を大学に開示
    - NII-SOCS運用担当・大学担当ともに記録
  - 取得する情報
    - URL (クラウドでの追跡に必須)
    - 添付ファイル名
    - メールの送/受信者アドレス
- 保持期間
  - 最長3ヶ月…月単位でデータ保存→破棄

攻撃先ポート	23
フラグ	0x80002000
プロトコル	tcp
アクション	alert
警報名	Mirai.Gen Command And Control Traffic(13974)
PAシグネチャID	13974
カテゴリ	any
危険度レベル	CRITICAL
方向	client-to-server
攻撃元国	Viet Nam
攻撃先国	Japan
コンテンツタイプ	
ダイジェストファイル	
ユーザエージェント	
ファイルタイプ	
X-転送	
ペイロード有無	有
ペイロード情報	閲覧

クライアント証明書による通信内容の保護と閲覧(NII側)

- **NII側**
  - 共通鍵で暗号化された通信内容
  - 大学の公開鍵で暗号化された共通鍵
- **大学作業**
  - 共通鍵の取り出し
  - 共通鍵のアップロード
- **共通鍵と復号情報**
  - 主記憶にのみ存在
  - 期限切れ時に破棄
    - HDDには保持せず

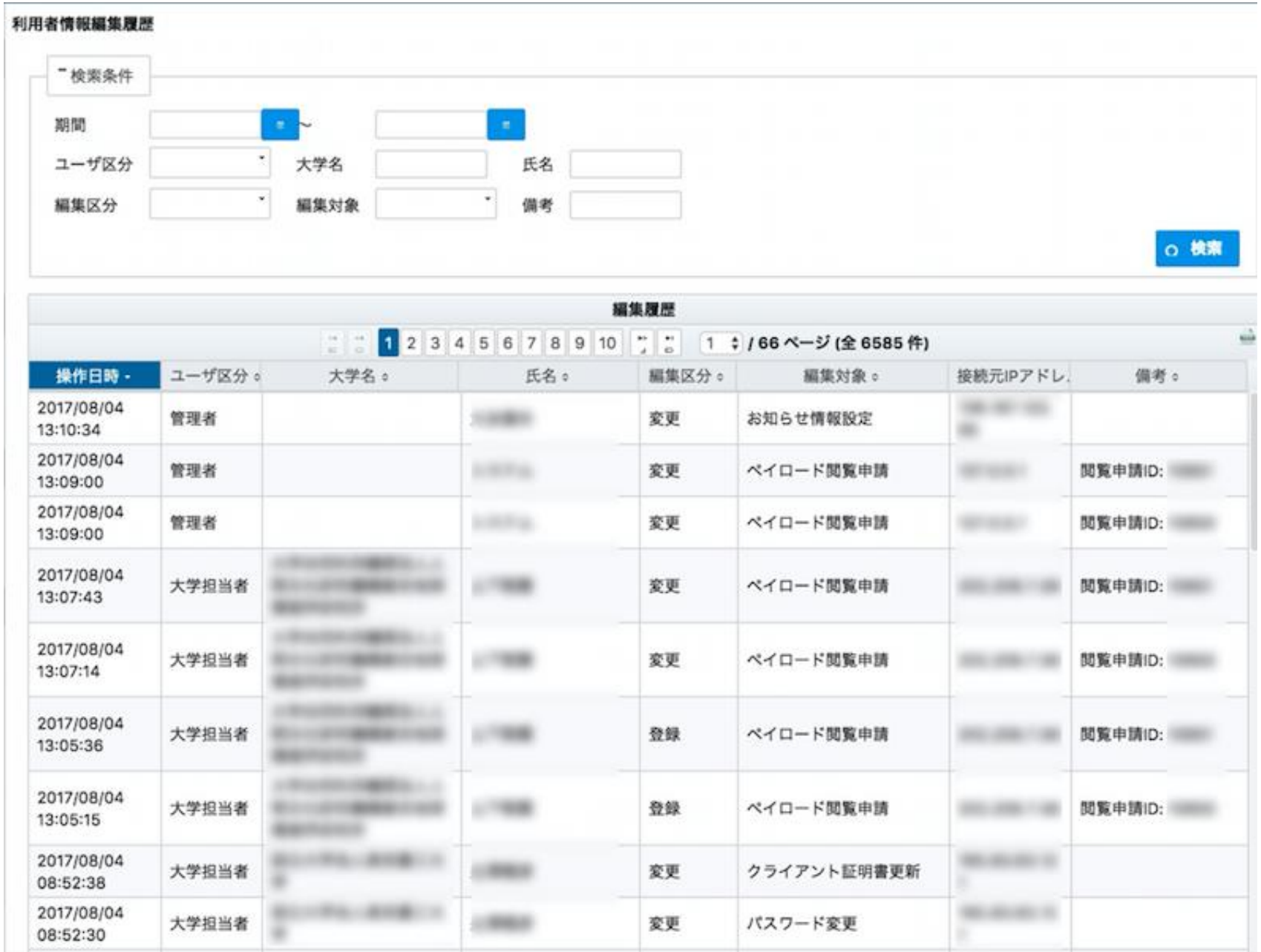


閲覧履歴の保存

通信の内容の閲覧申請記録

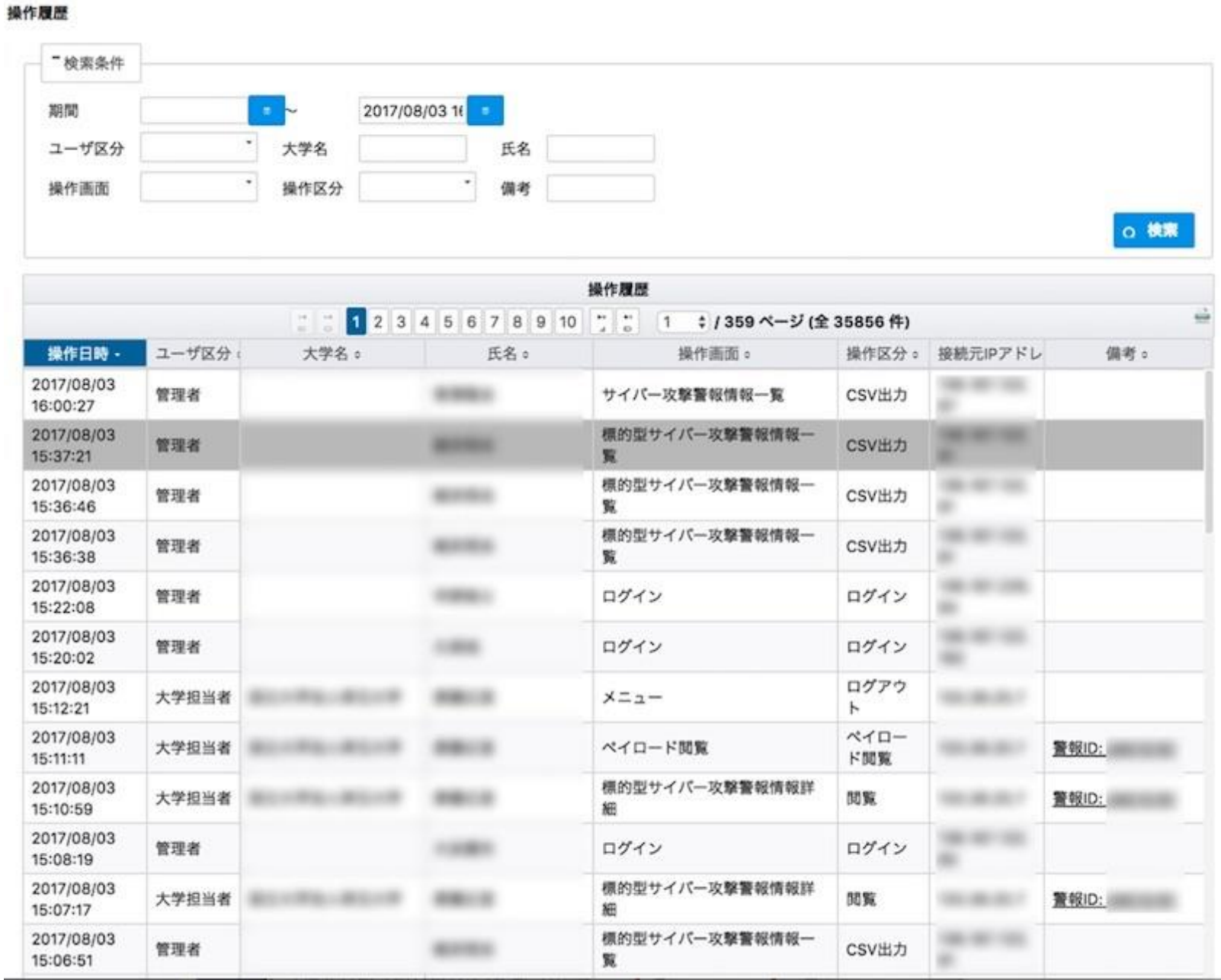
- 暗号解除の申請
  - NII→大学
  - 大学自身

  全て記録
    - 所属
    - 申請者指名
    - 対象となる警報
      - 閲覧申請IDで管理
- NII・大学の両方で同じ情報を閲覧



操作記録のログ取得

- 全ての作業歴を保存
  - 個々の警報を除く
    - 所属
    - 作業
    - 復号された警報のID
- NII・大学の両方で同じ情報を閲覧



試行運用4ヶ月間の状況

- 参加機関：74
- 通知機関：54
- 検知件数：460
  - 内訳(可能性があると判断されたもの)
    - アプリケーションの脆弱性によるもの：33件（Apache Struts2、OpenSSL、bash、ISC BIND等）
    - DNS Amp攻撃への参加：10件
    - マルウェア取得の通信、マルウェアによる通信：173件
    - 標的型サイバー攻撃の被害：6件
    - C&Cサーバーとの通信：220件
    - ルートフォース攻撃の可能性：7件
    - 辞書攻撃の可能性：4件
    - その他：7件
- 複数機関の俯瞰監視
  - 数機関の検知情報を元に，より詳細かつ正確な分析が可能
    - 例：マルウェアの初期感染から活動開始までを観察→他機関の類似事案(観戦は学外)を調査

とはいえ…
見ているだけの時間帯が圧倒的に多い

試行運用で明らかになった課題

- 誤検知
  - ペイロードの閲覧制限
  - セキュリティ製品の予防アクセス・ブラウザなどの先行アクセス
  - 推奨されないプログラムの意図した入手
  - 誤検知情報のフィードバック手段の欠如
    - 「誤検知」「通知不要」といったフィードバックがあれば…
      - でも、フィードバックがないってことは…NII-SOCSが知っていい情報か？
- 提供情報の不足
  - 多くのセキュリティ製品では攻撃の詳細情報が非開示
  - 外部セキュリティ機関とのMoUやNDAによる制限
  - 標的型サイバー攻撃察知時の情報
- 性能不足
  - 小規模・中規模大学50校程度→旧帝大も含めた74校
    - 限定的なセッション情報取得(全体の1割程度)
    - ポータルサイトの処理能力の限界

11月6日現在の参加機関：96（試行運用機関を含む）

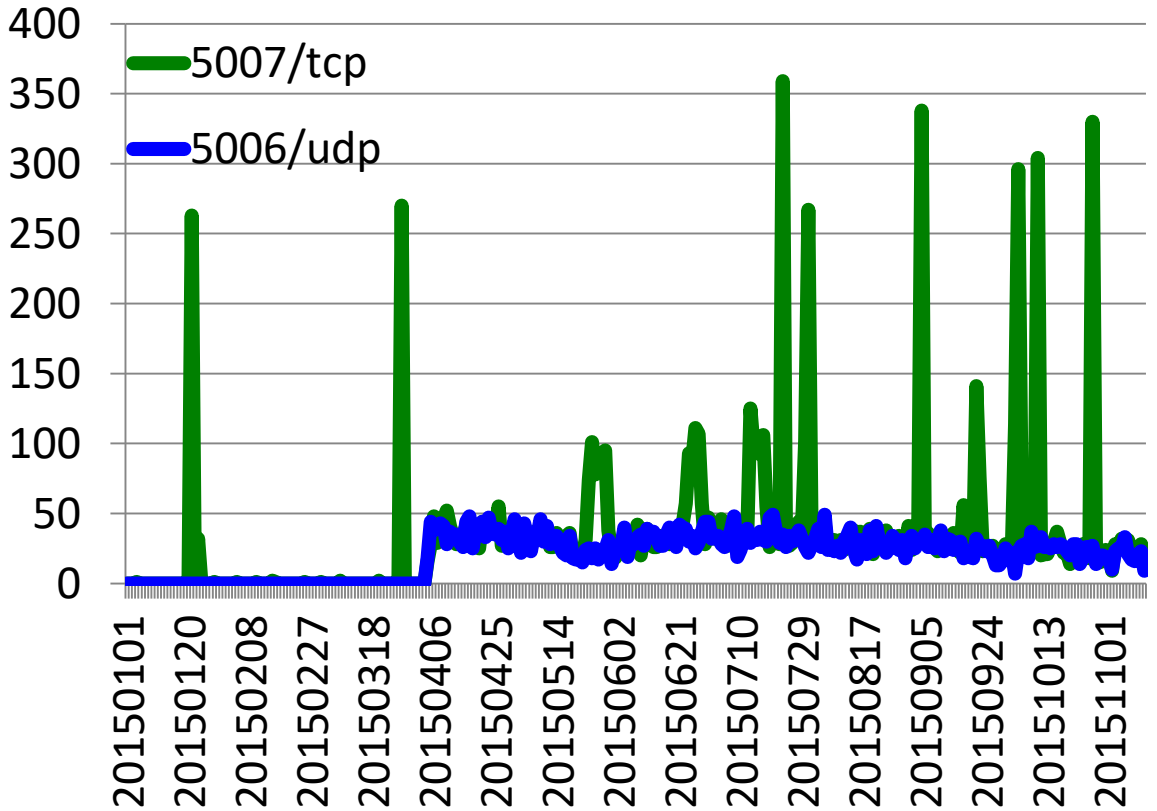
7月1日～10月31日の間の参加機関への通知情報

- 通知機関：59
- 検知件数：303
  - 内訳(可能性があると判断されたもの)
    - C&Cサーバーとの実通信の可能性：2件
    - アプリケーションソフトの脆弱性によるもの：29件
    - マルウェア感染の可能性：254件
    - 辞書攻撃の可能性：2件
    - その他（外部からの不正な攻撃の疑い　など）：16件

- 監視能力の増強
  - 現在のサンプル監視の間隔を短縮
    - 大口大学の場合、4時間に30分間だけ監視という状況も発生
- WebUIの改良
- データダウンロード用の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多し)
- 研究用データの公開
  - 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大学への提供
    - 情報不足への対応も
- 次期システム構想
  - 次期SINET対応をどうするのか？大学との意思疎通が必須
  - 現時点では、H32年度までの計画である。

一方、安全装置の無い増速は…

- 誰かが何かに気づくと急激に調査開始
  - アングラサイトでの情報(脆弱性？)
- 2種類のスキャン
  - 機器探索
    - 全方位探索
      - Shodanなどの活動が活発
  - ピンポイント系
    - 攻撃対象確認
      - 照準合わせ？
  - 変化点分析による探査動向追跡と警報



学術研究機関へのベンチマークデータの提供

- 警報情報とセッション情報
  - 一般公開
    - IPアドレス無しの単なる統計データ
  - NDAに基づく研究機関向け公開
    - IPアドレスはサニタイズ
    - 観測時間を意図的に変動
    - 警報の「通信の内容」部分は暗号化ままでハッシュ値を生成
    - KyotoData2006+準拠
- マルウェア情報
  - NDAに基づく研究機関向け公開
  - マルウェア本体+sandboxの解析結果
    - 文書ファイルなど一部は除外
  - 輸出貿易管理令の対象
    - 米国商務省による規制
    - 各機関での審査…特に留学生

IPアドレスのサニタイズ
Saltを毎月変更
/24での連続性は保証

攻撃者自身による特定作業を防止