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-SOCS)について

NII Security Operation Collaboration Services (NII-SOCS)

- NII-SOCSの現状
- NII-SOCSの機能拡張(2020-2021年度)
- 研究用データの公開

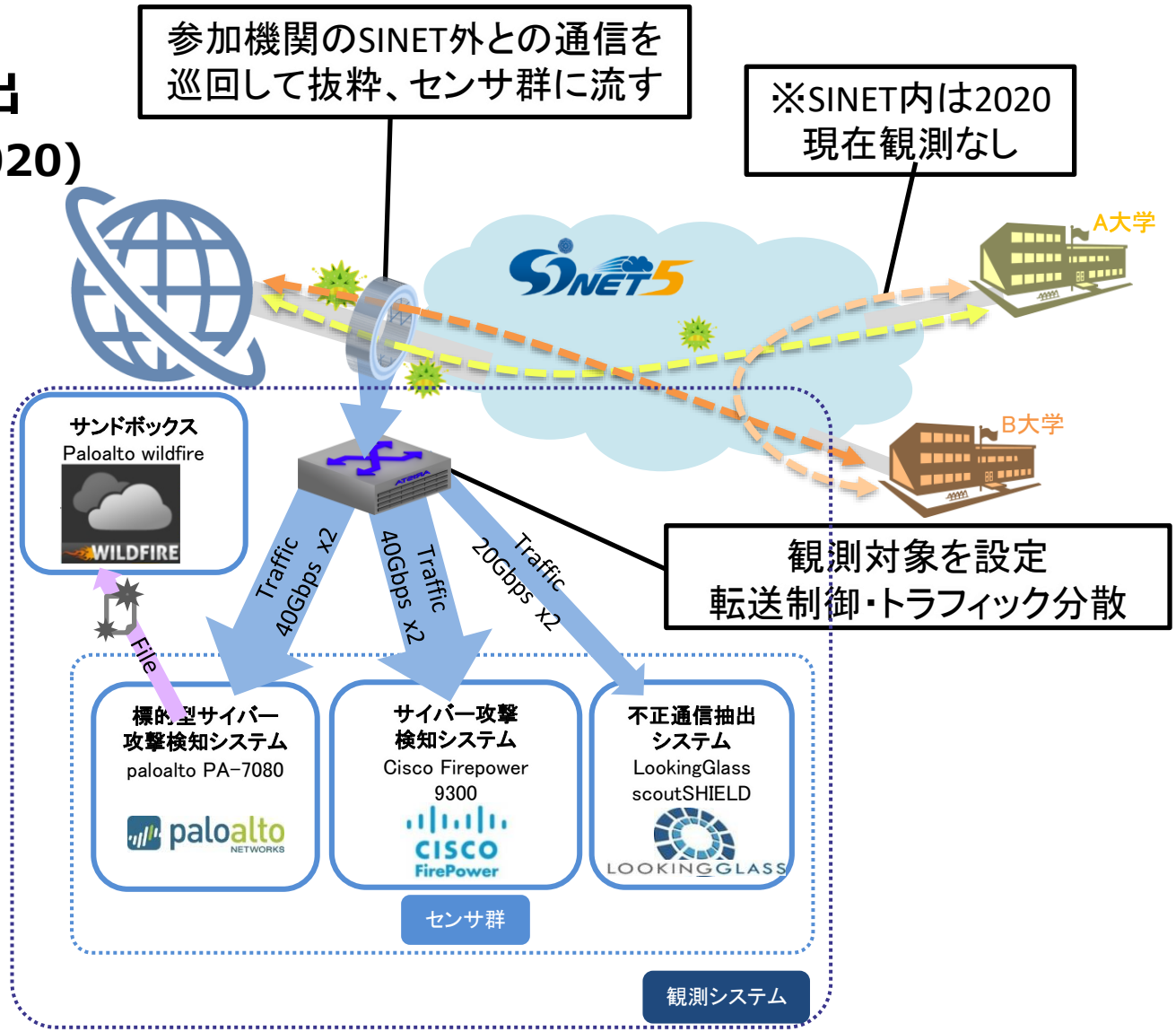
NII-SOCSの現状

大学間連携に基づく情報セキュリティ体制の基盤構築

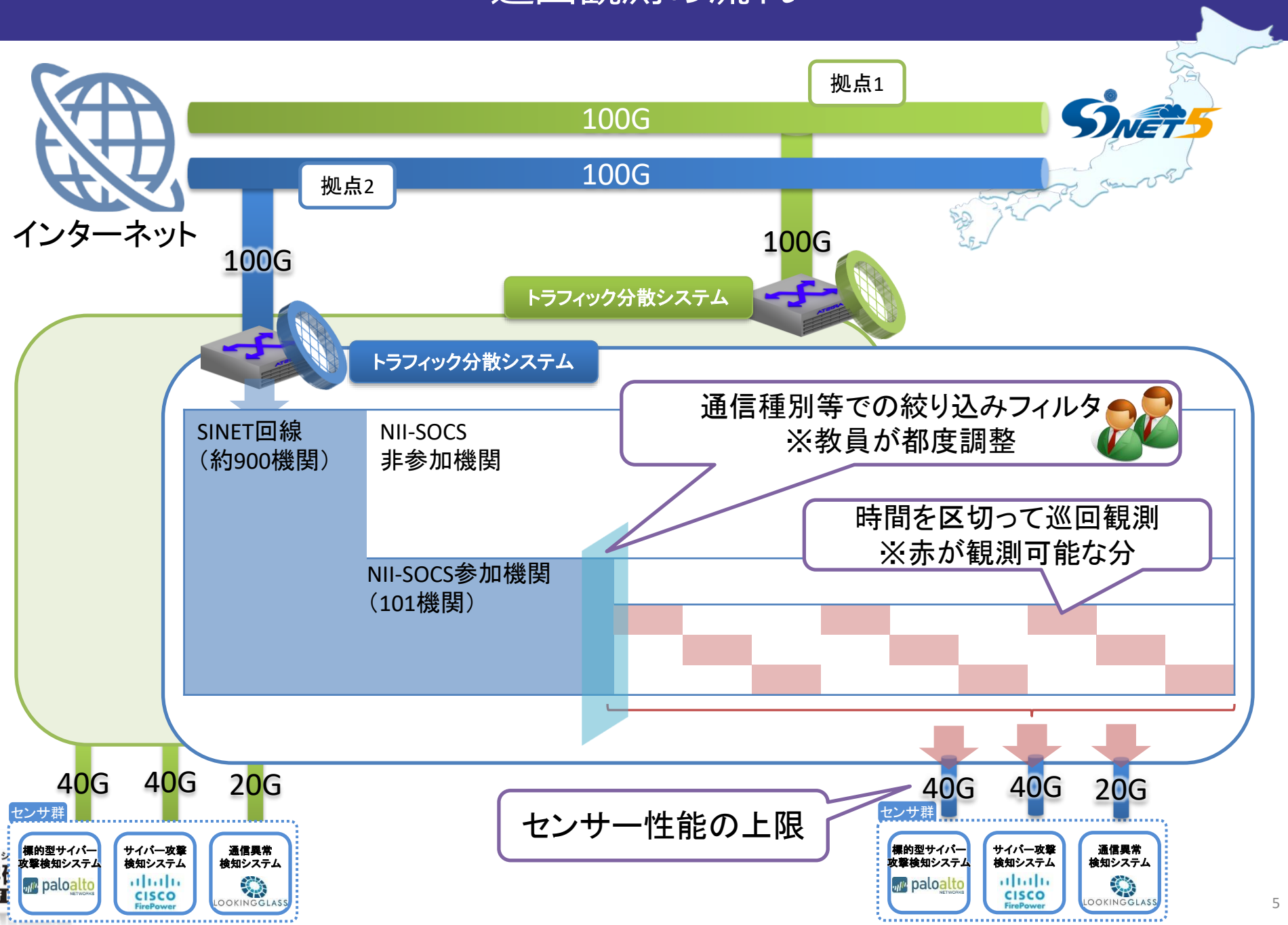
NII

◆NII-SOCSの観測体制

- ●国立大学法人等の運営費交付金から拠出
  - ■年間約8億円/約100機関の参加(2016-2020)
- ●3種類の検知システム
  - ■Sandbox搭載IDS
    - ➢paloalto PA-7080+WildFire
  - ■シグネチャベースIDS
    - ➢Cisco FirePower
  - ■不審通信抽出システム
    - ➢LookingGlass ScoutSHIELD
      - » 脅威インテリジェンスとの照合
- ●SINETと外部の通信を観測
  - ■二ヶ所
  - ■一定時間間隔で観測対象を巡回
  - ■SINET内の観測はない



巡回観測の流れ


インターネット
拠点1
100G
100G
拠点2
100G
100G
トラフィック分散システム
トラフィック分散システム
SINET回線
（約900機関）
NII-SOCS
非参加機関
NII-SOCS参加機関
（101機関）
通信種別等での絞り込みフィルタ
※教員が都度調整
時間を区切って巡回観測
※赤が観測可能な分
40G
40G
20G
センサー性能の上限
40G
40G
20G
センサ群
標的型サイバー攻撃検知システム
paloalto
サイバー攻撃検知システム
CISCO FirePower
通信異常検知システム
LOOKINGGLASS
センサ群
標的型サイバー攻撃検知システム
paloalto
サイバー攻撃検知システム
CISCO FirePower
通信異常検知システム
LOOKINGGLASS

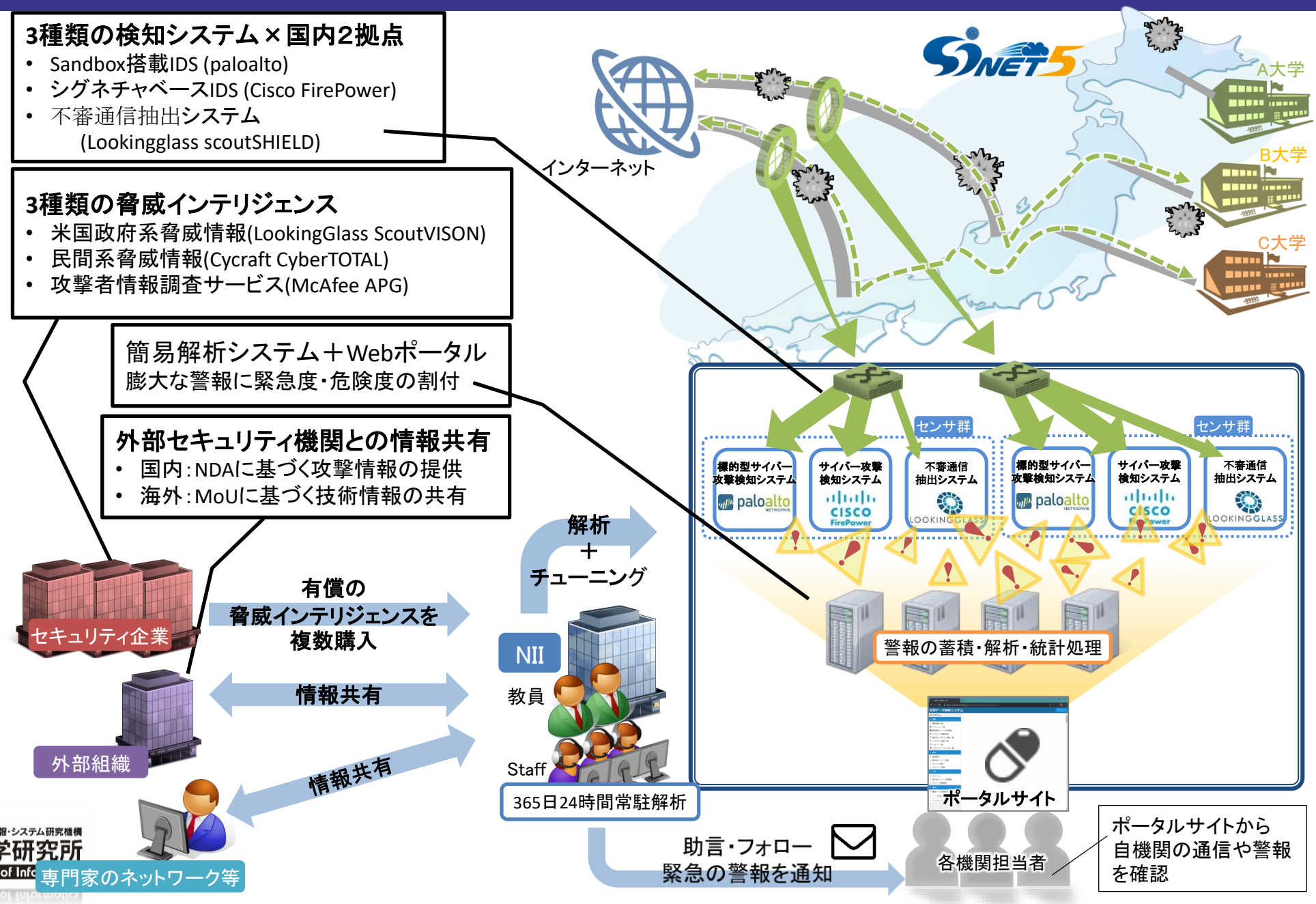
NII-SOCSの観測体制

3種類の検知システム×国内2拠点
- Sandbox搭載IDS (paloalto)
- シグネチャベースIDS (Cisco FirePower)
- 不審通信抽出システム
  (Lookingglass scoutSHIELD)

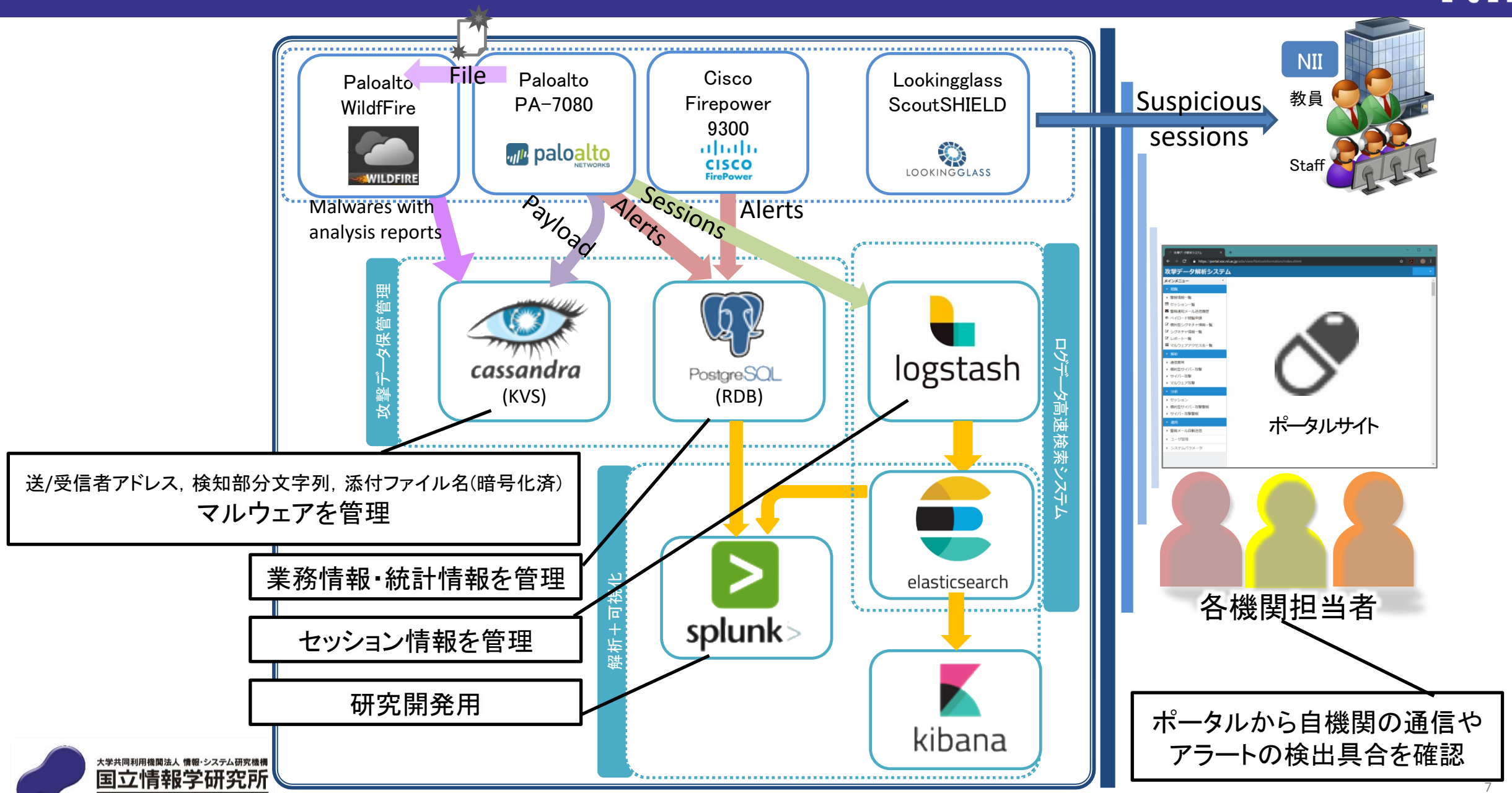
3種類の脅威インテリジェンス
- 米国政府系脅威情報(LookingGlass ScoutVISON)
- 民間系脅威情報(Cycraft CyberTOTAL)
- 攻撃者情報調査サービス(McAfee APG)

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
- 海外：MoUに基づく技術情報の共有



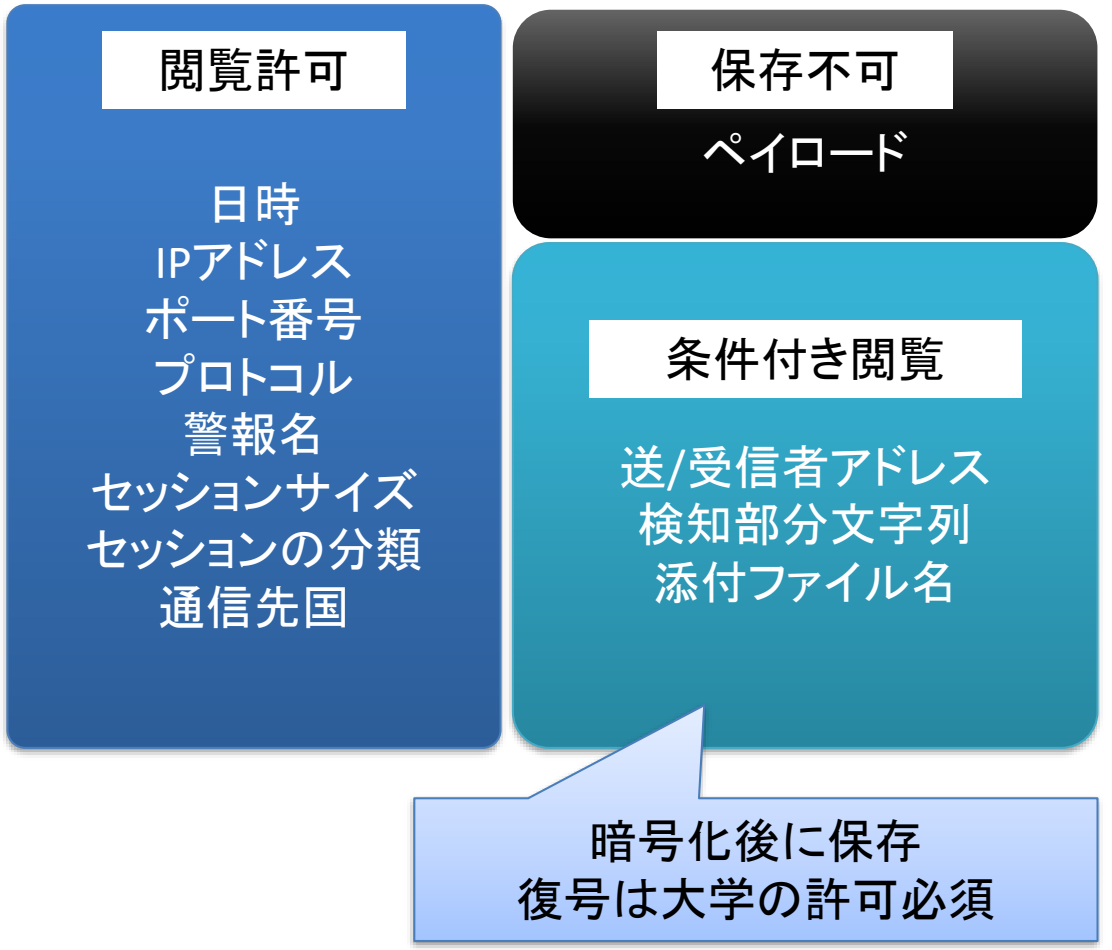
観測データの流れ


File
Paloalto
WildfFire
Paloalto
PA-7080
Cisco
Firepower
9300
Lookingglass
ScoutSHIELD
Malwares with
analysis reports
Payload
Alerts
Sessions
Alerts
攻撃データ保管管理
cassandra
(KVS)
PostgreSQL
(RDB)
logstash
ログデータ高速検索システム
解析＋可視化
splunk>
elasticsearch
kibana
Suspicious
sessions
NII
教員
Staff
ポータルサイト
各機関担当者
送/受信者アドレス，検知部分文字列，添付ファイル名(暗号化済)
マルウェアを管理
業務情報・統計情報を管理
セッション情報を管理
研究開発用
ポータルから自機関の通信や
アラートの検出具合を確認

【NII-SOCSの特徴】専門家による絞り込み作業

- ◆日々生成される膨大な情報
- ◆警報の特性に基づく絞り込み
  - ●外部専門家による分析結果
    - ■McAfee APG
  - ●脅威インテリジェンスシステム
    - ■ScoutVision, CyberTotal, Threat Grid
  - ●OSINT情報等との照合
- ◆通知は任意に選んだ1警報のみ
  - ●通知されない情報
    - ■各機関がポータルサイトで確認可能
- ◆参加機関からのフィードバック
  - ●自動絞り込みの精度向上に寄与

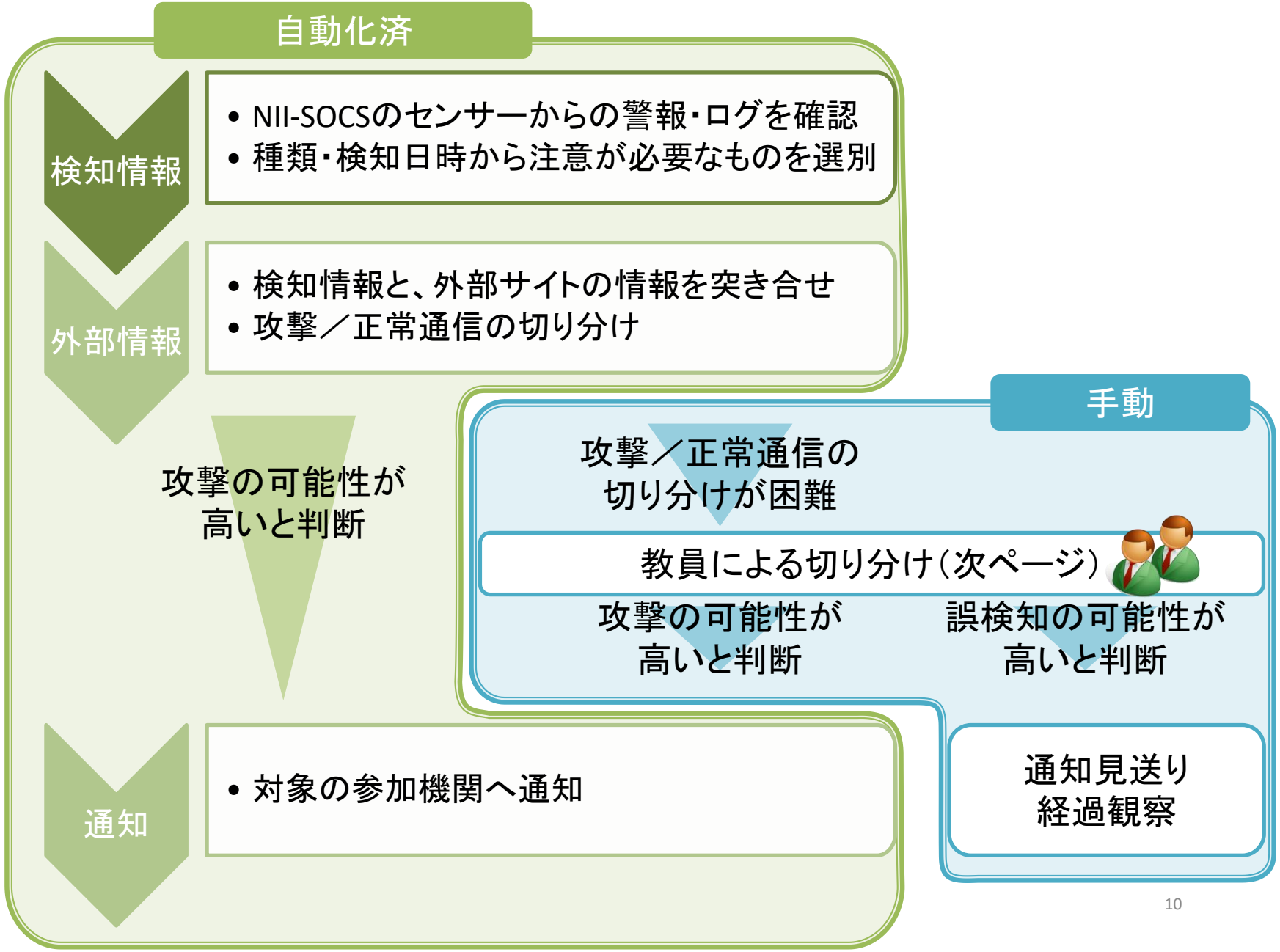
- ◆NIIは大学共同利用機関法人…国に準ずる独法
- ◆大学の構成員
  - ●教職員…国立大学なら公務員に準ずる…
  - ●学生・訪問研究者
  - ●研究を覗き見るのは…
  - ●そもそも個人所有の情報端末
- ◆憲法遵守はmust
  - ●通信の秘密
    - ■通信の中身は覗けない
  - ●財産権
    - ■無断の脆弱性診断・コマンド実行不可
- ◆通信の内容を確認せずに攻撃成否を判断
  - ●攻撃着弾後の挙動から推測
    - ■誤判定の要因の一つ



※正式運用開始後、NII-SOCSから復号依頼をした実績はない

警報・ログ通知の流れ

- ◆攻撃の可能性・被害発生の可能性を検討
  - ●通信内容を確認せずの判断
  - ●誤判断の可能性あり
- ◆自動化が可能と判断
  - ●自動通知設定
  - ●検知から通知までの時間短縮



教職員による切り分け・自動処理ルール作成

NII

- ◆脅威インテリジェンスを活用
  - ScoutVision
  - CyberTotal
  - Threat Grid
- ◆教職員による情報収集
  - OSINT情報を主として調査

新しい攻撃、正常通信と見分けがつきにくい攻撃が発生した場合、オペレータより教職員に照会

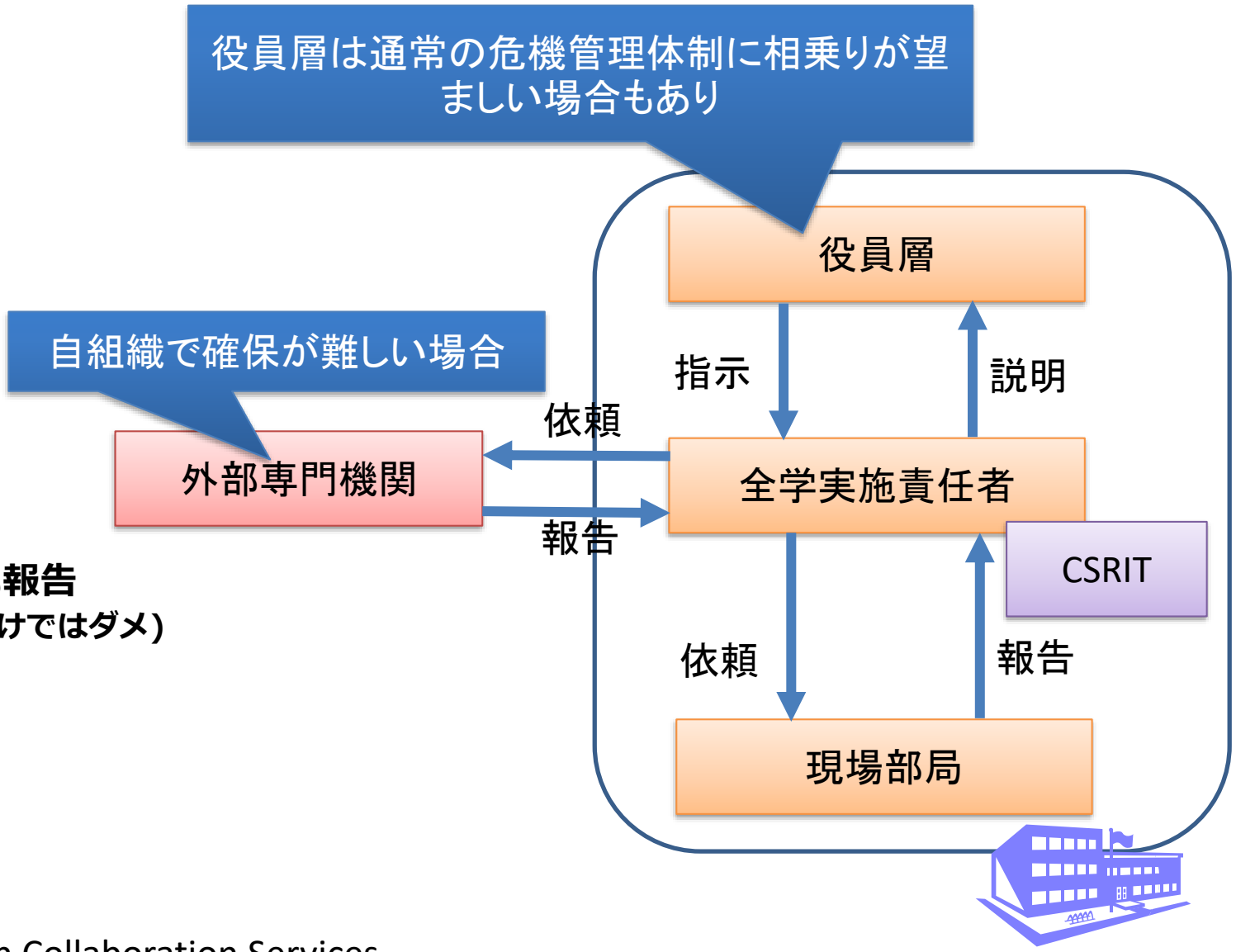
教職員が高い専門性を持って各種情報を読み解いて判断

繰り返すうちにパターン化できたものは自動化フローに組み込んでいく

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のミッション…戦略マネージメント層の育成

- ◆全学実施責任者
  - ●戦略担当
    - ■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
      - ➢CSIRTとの調整
      - ➢役員層-他との意思疎通
    - ■アクシデント時の判断
      - ➢例：認証システムでの重大インシデント
        - » 講義は？施錠管理は？
- ◆CSIRT
  - ●支援役としての役割
    - ■技術だけでなく、組織運営への影響も報告
      - ➢他部門との連携必須(パソコンを見てるだけではダメ)
- ◆自組織での人材育成が必須
  - ●学内事情に詳しくなければ動けない
  - ●キャリアパスで育成



サイバーセキュリティ人材育成

NII

- **国立大学法人等の情報セキサイバー攻撃への対処能力の高度化**
  - **SINET５の実環境による実地研修等**
- **テクニカル面よりもマネジメント面の強化に重心**

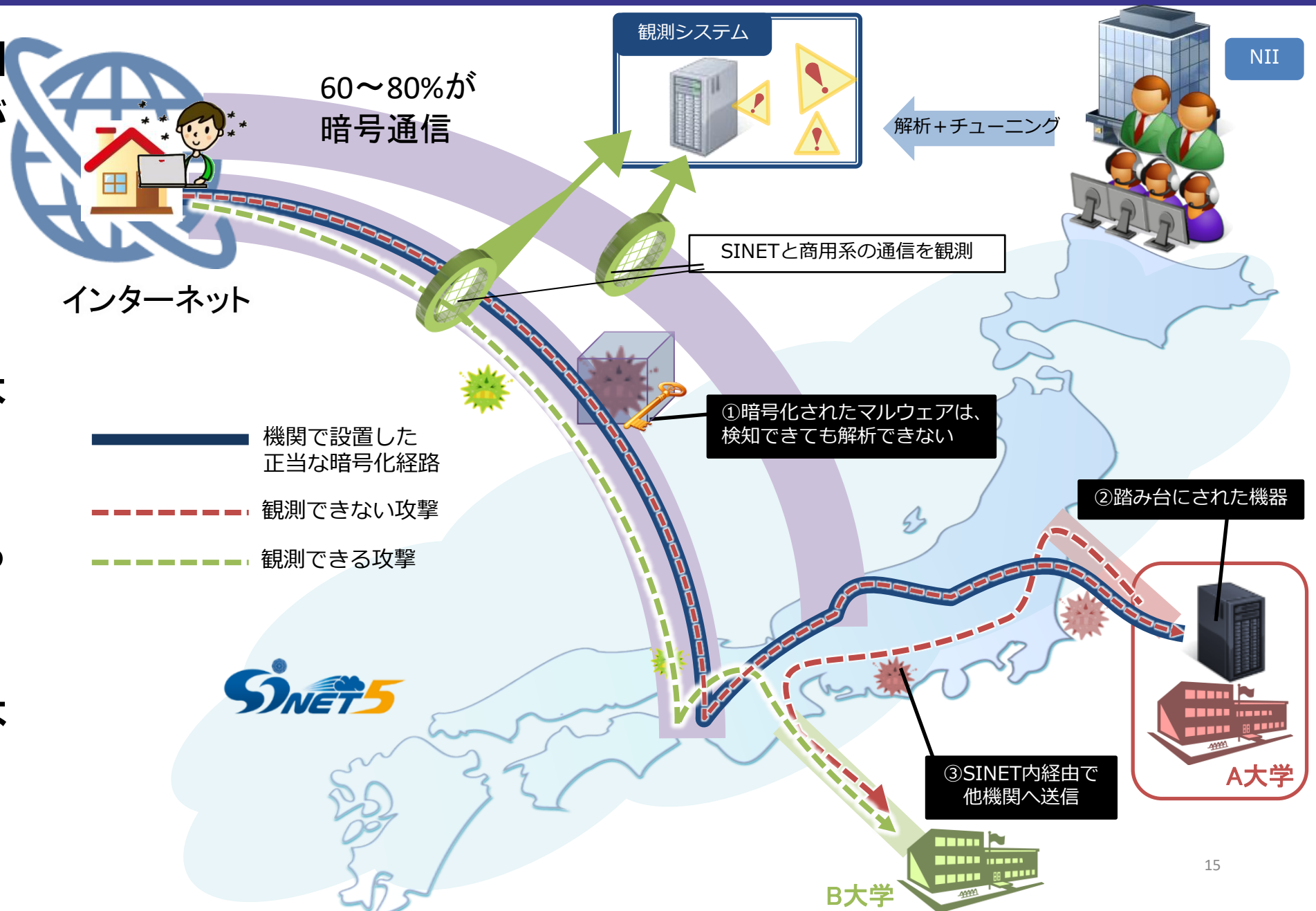
年度	研修内容	開催年月と開催数	参加機関数と参加人数
NII-SOCSコース①			
平成28年度	NII-SOCSの概要説明、Webポータルの操作説明　等	2017年3月　2回	38機関、63名
平成29年度	NII-SOCSの概要説明、Webポータルの操作説明　等	2017年4月　2回	37機関、61名
	Webポータルの操作説明及び改修内容、 NII-SOCS検知情報の事例説明　等	2018年1月　2回	13機関、30名
平成30年度	Webポータルの基本操作、サイバー攻撃手法、 警報情報の基本的な分析などの学習	2018年6-8月　4回	41機関、82名
令和元年度	Webポータルの基本操作、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	2019年6月-8月　6回	32機関、43名
令和２年度	Webポータルの基本操作、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	2020年9月　7回 (オンライン)	15機関、17名
通算			**92機関、296名**
NII-SOCSコース②			
平成30年度	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、90名
通算			**52機関、90名**
NII-SOCSマネジメント研修			
令和元年度	CSIRT・CISO向け、グループディスカッション型 インシデントマネジメント研修	2019年11-12月 2回	31機関、51名
令和２年度	CSIRT・CISO向け、グループディスカッション型 インシデントマネジメント研修	2019年12月 1回	20機関、28名
通算	通算の機関数はユニーク数です。		**42機関、79名**

NII-SOCSの機能拡張(2020-2021年度)

2020年度時点の課題

NII

- **暗号通信の増加**
  - パターン検知が困難に
- **VPN通信**
  - 活動拠点変化
    - 自宅等
  - 学内の感染拡大で初めて検知
- **SINET内攻撃**
  - 攻撃拠点となる大学
  - 他学を攻撃
  - 現状では検知は困難



2020-2021年度の観測能力拡張案

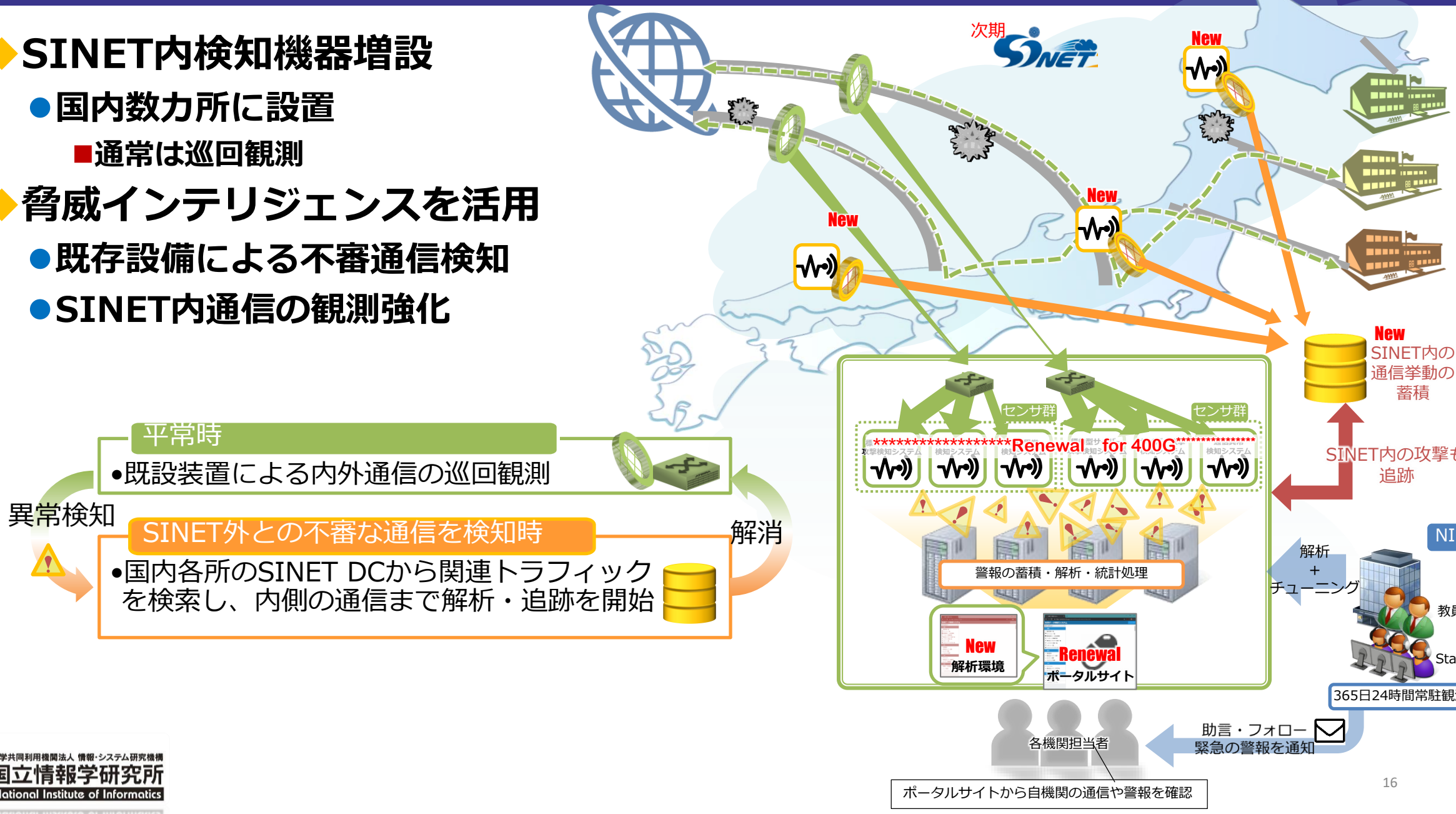
NII

◆SINET内検知機器増設

- ●国内数カ所に設置
  - ■通常は巡回観測

◆脅威インテリジェンスを活用

- ●既存設備による不審通信検知
- ●SINET内通信の観測強化



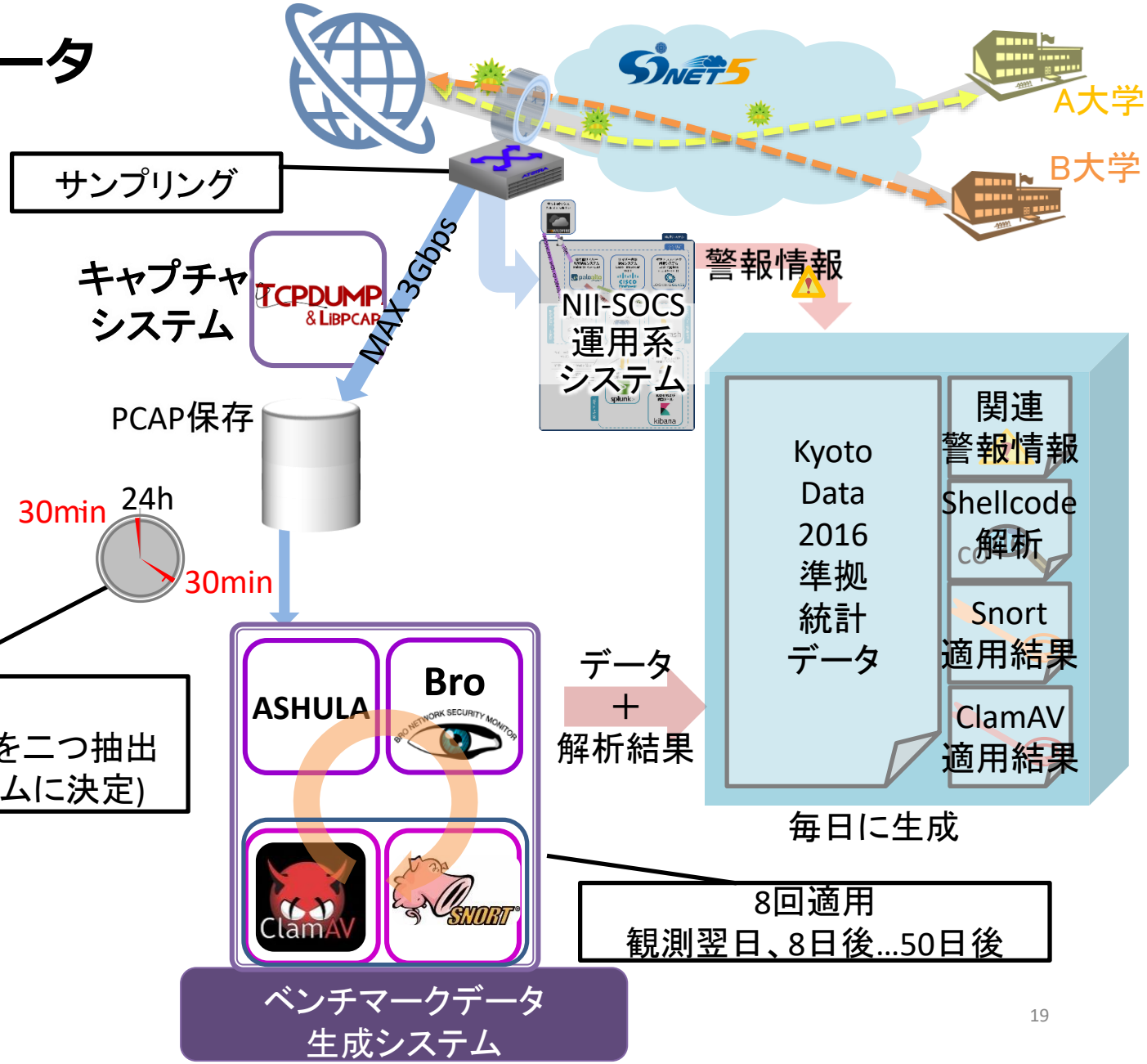
研究用データの公開

研究用データの概要

- ◆統計化・匿名化処理を施したベンチマークデータ
  - IPアドレス、ポート番号(1024以上)を匿名化
  - 各日ランダムに選んだ1時間分→00:00:00～にタイムスタンプ変更
  - 統計データ(ペイロードは含まない)
    - KyotoData2016準拠
      - 多田竜之介, 小林良太郎, 嶋田創, 高倉弘喜, NIDS評価用データセット： Kyoto 2006 Datasetの作成, 情報処理学会論文誌, No.58, Vol.9, pp.1450-1463, 2017年9月.
  - Snort/ClamAVの検知結果(7日間隔x8回: ZeroDayの正解データ)
  - 約款に基づく提供
    - https://www.nii.ac.jp/service/upload/nii-socs-benchmark-yakkanJ.pdf
- ◆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
  - 文書ファイル(MS-Office、PDF等)を除く
  - 複数機関(5機関以上を想定)で観測したもの
  - NII-SOCSで初検知のもの
  - 約款に基づく提供
    - https://www.nii.ac.jp/service/upload/nii-socs-malware-joho-dl-yakkanJ.pdf

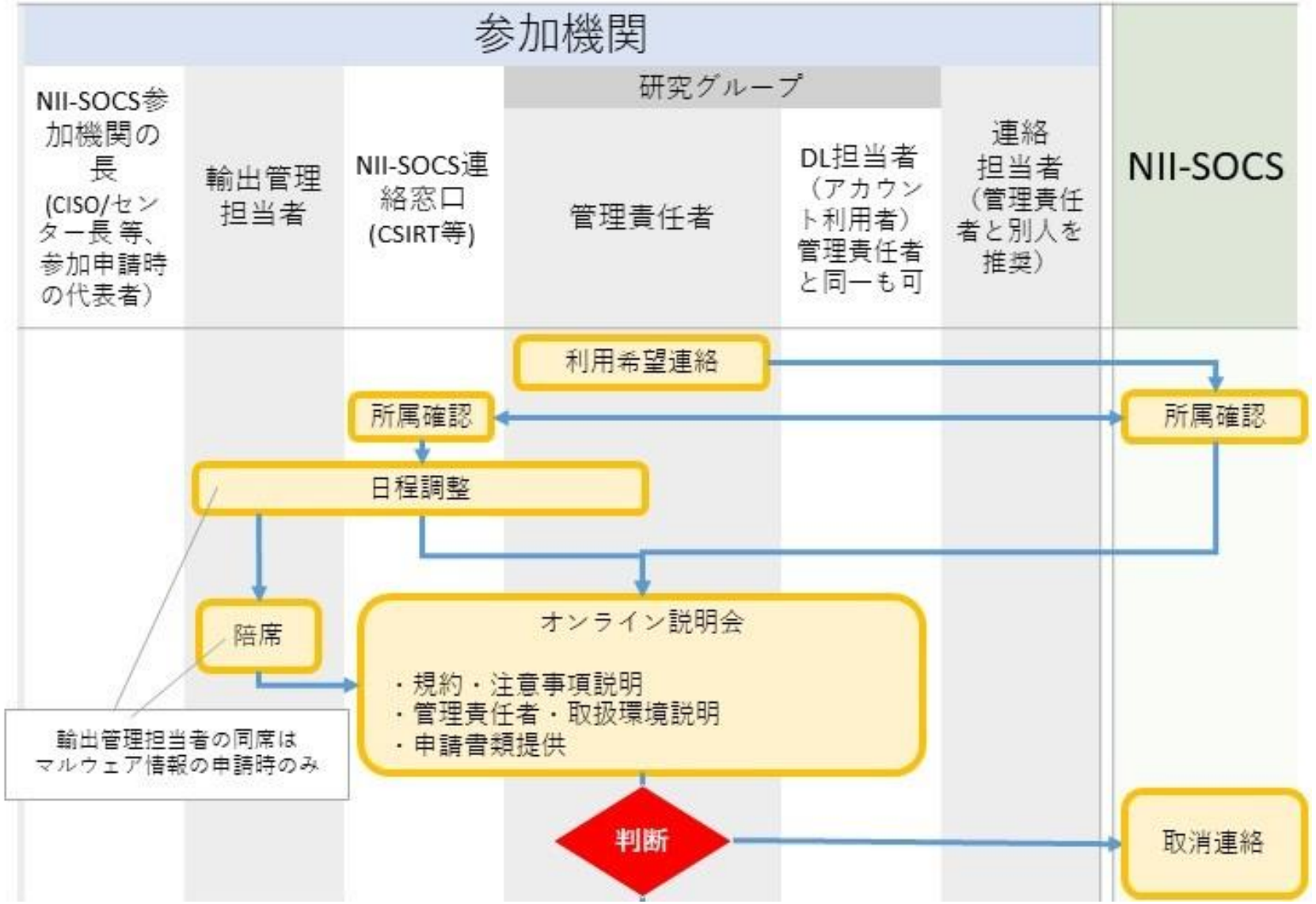
ベンチマークデータ生成の流れ

- KyotoData2016準拠の統計データ
  - SnortとClamAV
    - 観測翌日、8日後、…、50日後
      - 無償版Snortのシグネチャ提供
        - » 30日遅れる
      - Zero-day攻撃情報のラベルとなる
  - ASHULA
    - Shellcode/decoderの存在判定
  - Bro
    - トラフィック統計データ生成
- NII-SOCS観測データ



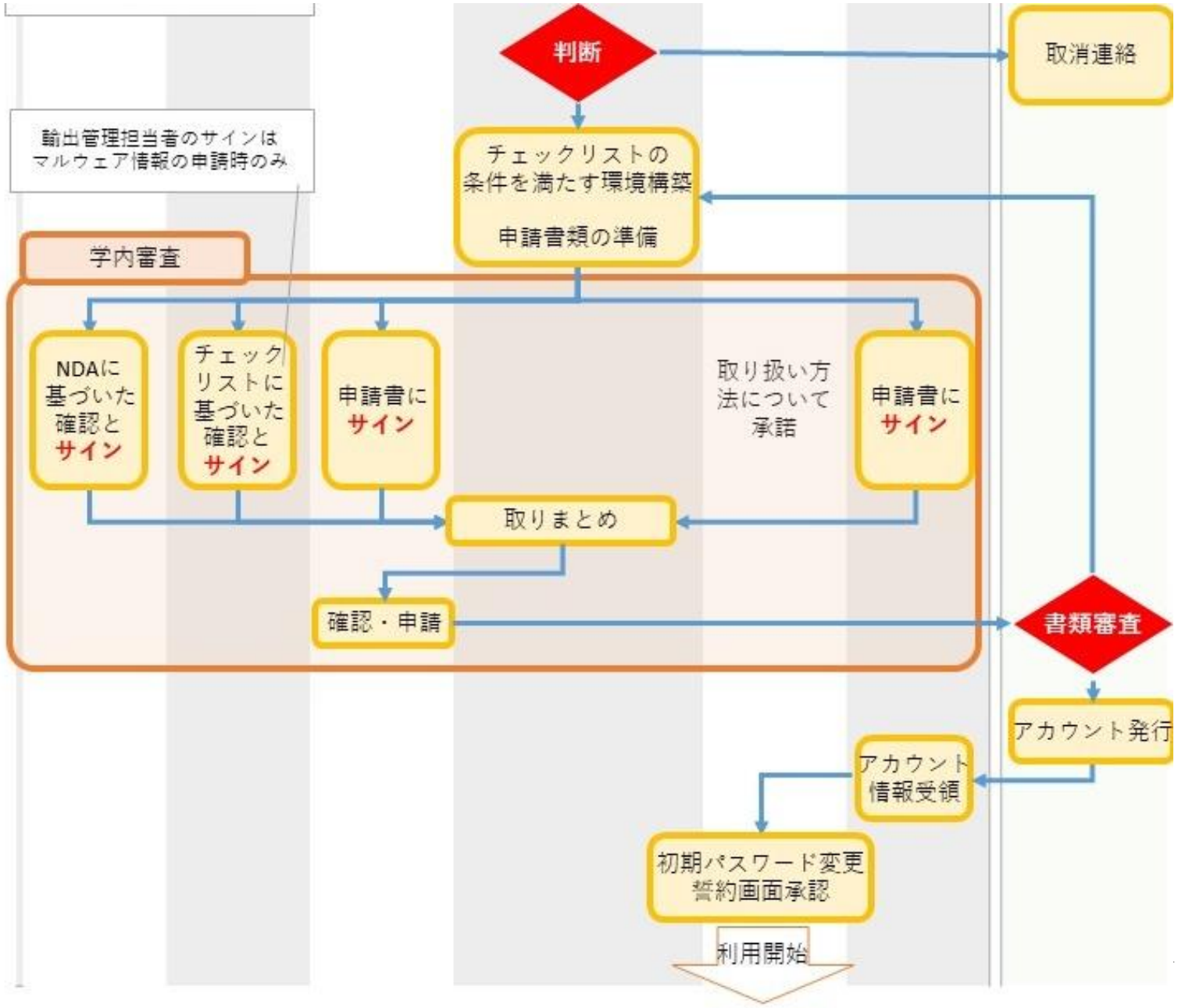
研究用データの利用申請手順(1)

- ◆利用資格の確認
  - ●NII-SOCS参加機関に所属する研究グループ
- ◆利用規約の説明
  - ●禁止事項の確認
    - ■参加機関や攻撃対象の特定や公表
  - ●マルウェアに関する特記事項
    - ■所属機関の輸出管理担当者への説明
    - ■管理体制の確認
      - ➢持ち出し防止策



研究用データの利用申請手順(2)

- チェックリストによる確認
- マルウェアについては輸出管理担当者が管理体制を確認
  - 我が国の安全保障貿易管理の対象
  - 海外製品が生成する情報
    - 製造国の輸出管理の対象
- 不適切な管理による事故は大学の責任となる



まとめ

- **NII-SOCSの現状**
  - 検知システムの換装
  - 自動処理化へ
- **NII-SOCSの機能拡張**
  - SINET内で発生する攻撃を追跡
- **研究用データの公開開始**
  - 統計化されたトラフィックデータ＋検知情報(Zero-Dayフラグ)
  - まずは参加機関に所属する研究グループへ