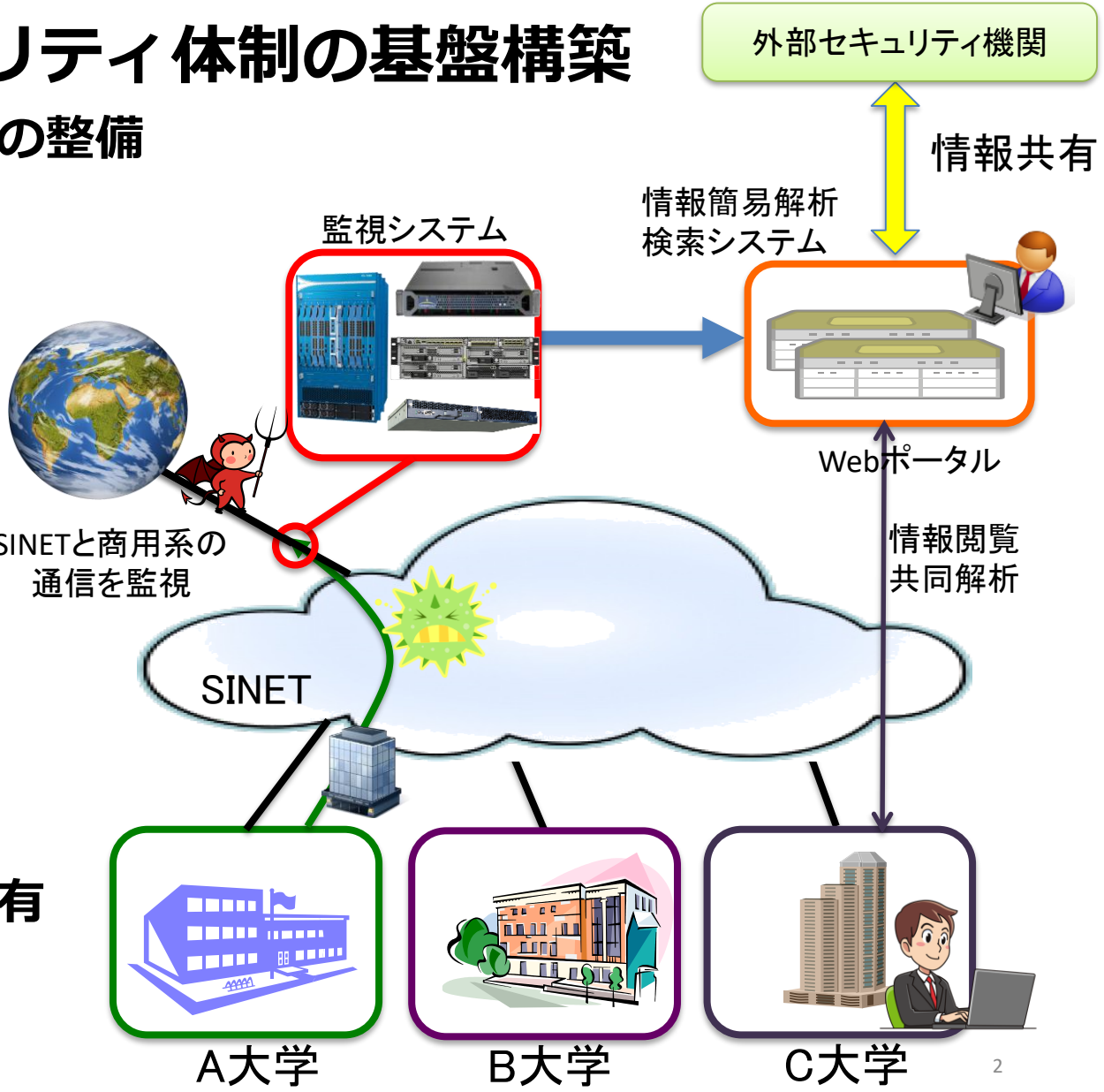
大学間連携に基づく情報セキュリティ体制の基盤構築の状況と課題

NII Security Operation Collaboration Services (NII-SOCS)

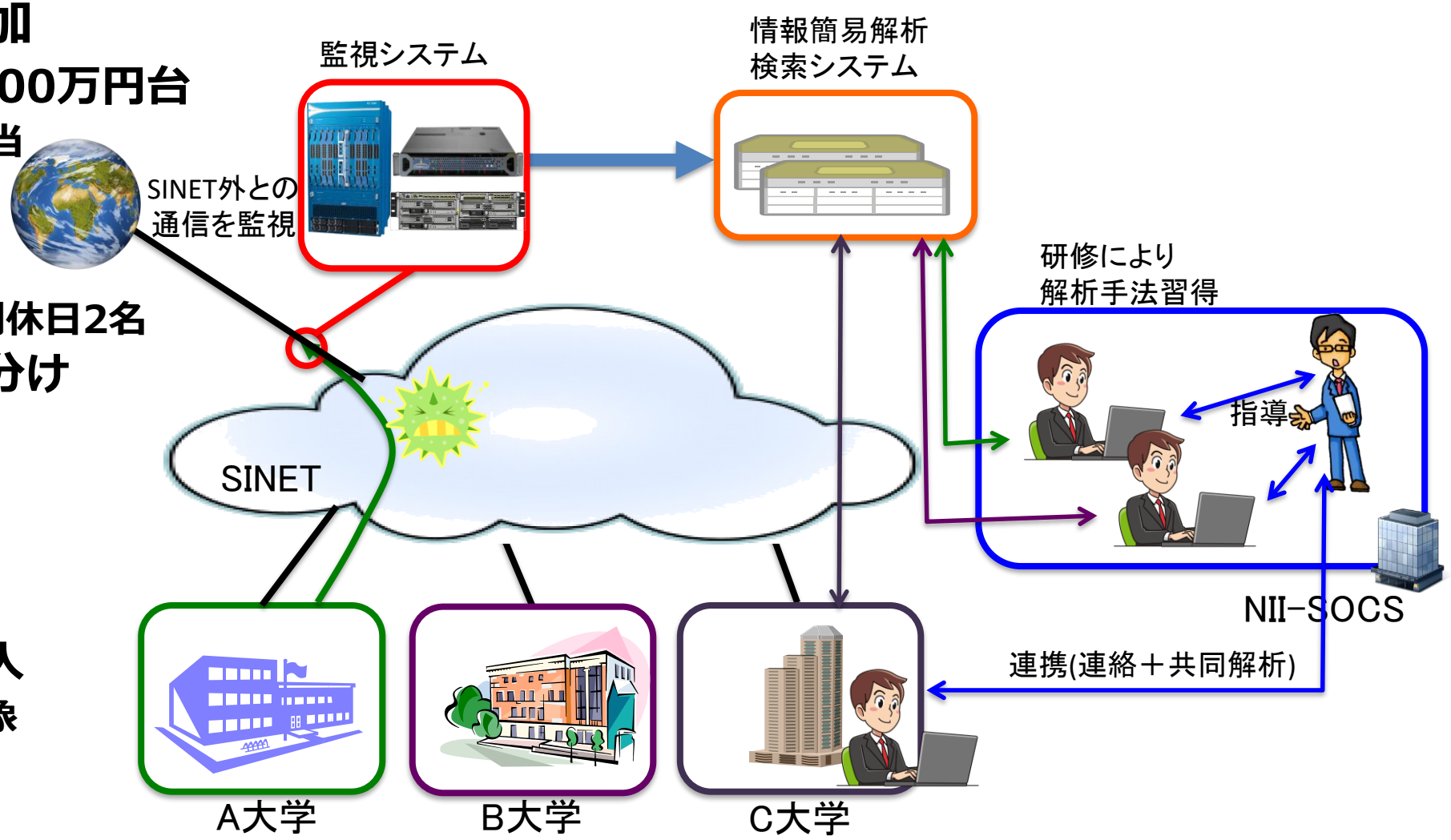
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等のインシデント対応体制の整備
    - 年間約8億円
      - 2021までは継続の予定
  - 4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)
    - Reputation情報(LookingGlass)
  - 脅威情報サービスの利用
    - サイバー攻撃の背景や危険度の把握
  - 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
  - 国内・国外セキュリティ機関との情報共有



NII-SOCSの仕組み

- 100機関以上の参加
  - 1機関あたり年額700万円台
    - 大手SOCの月額相当
- 警報監視
  - 24/365体制
    - 平日日中4人、夜間休日2名
  - 簡易解析結果の仕分け
    - 60万警報/日
    - 6億セッション/日
  - 情報収集
- インシデント連絡
  - 自動処理を一部導入
    - 典型的な攻撃を対象
    - 迅速性を重視



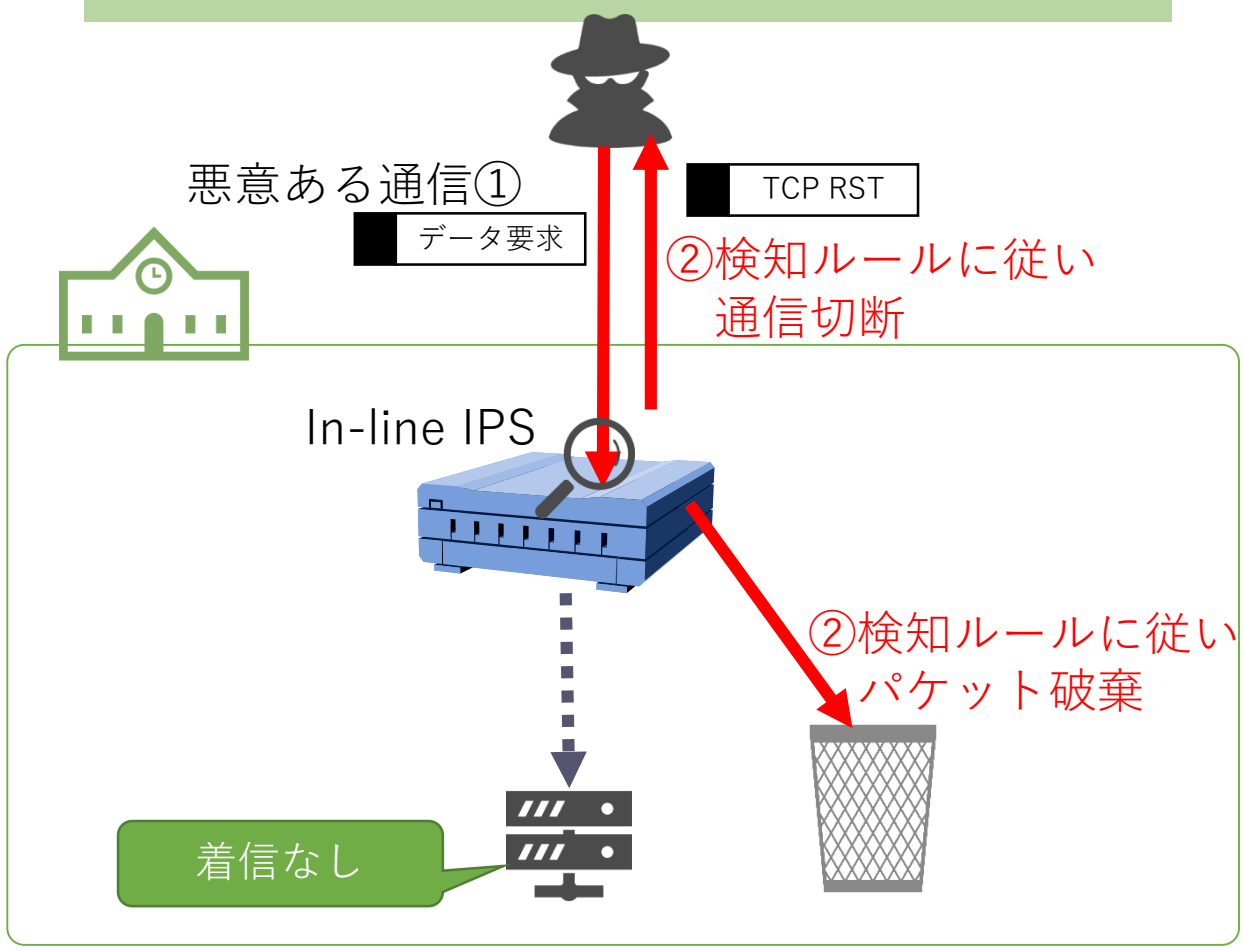
今年度の実施項目

- 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(既存センサの弱点対策)
  - 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
  - 週次・月次レポート
    - 判定：相対順位ではなく、月当たりの通知件数に基づく
  - 警報情報ダウンロード用のAPIの提供
  - 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)
- 研究目的でのNII-SOCSデータ活用
  - 各機関のセキュリティポリシーで認められているか？
  - NII-SOCS導入機器の評価はメーカとの契約違反
- 研究用データの公開(現在準備中)
  - トラフィック統計データと一部のマルウェア

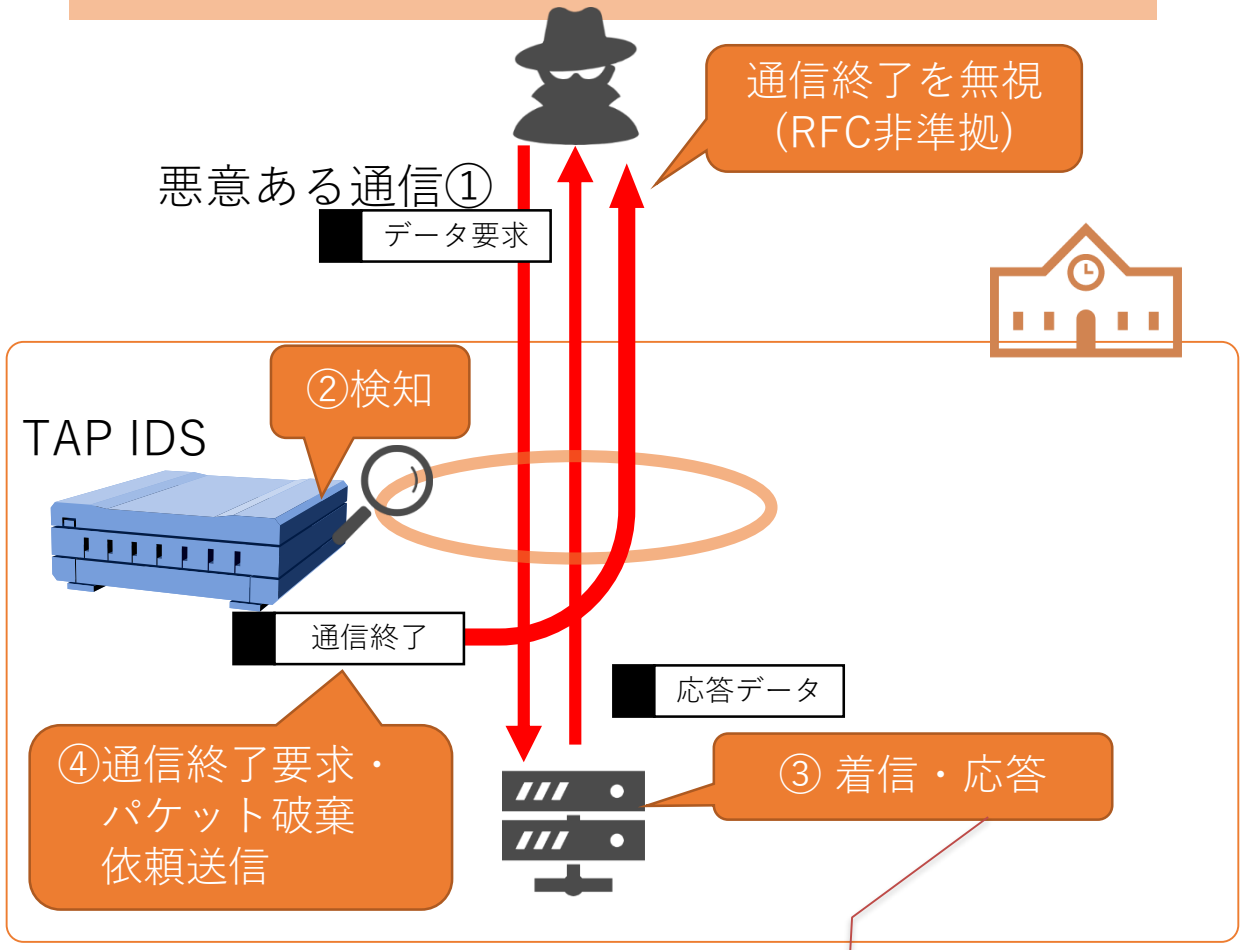
マルウェアの厳格な管理と輸出貿易管理令遵守

IDS TAPモードでの通信遮断の注意点

In-line構成での通信遮断



TAP構成での通信遮断

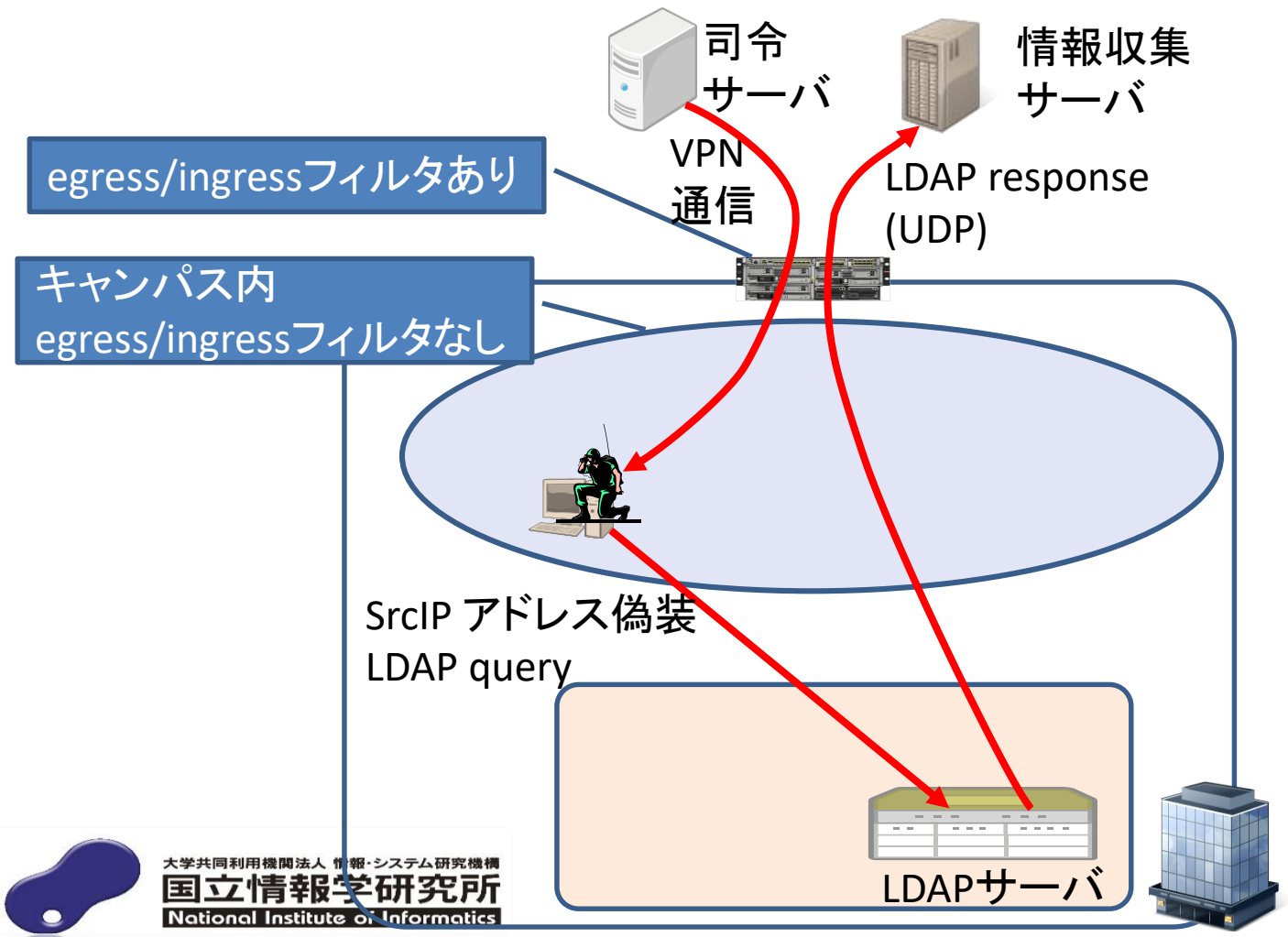


一般に通信遮断処理はソフトウェア処理(ハードウェア処理のルータに比べ10倍以上の処理遅延)
③よりも先に④を送れる場合、大学側機器にも通信遮断要求を送る必要
攻撃者が④を受信してもRFCを守らずパケットを破棄

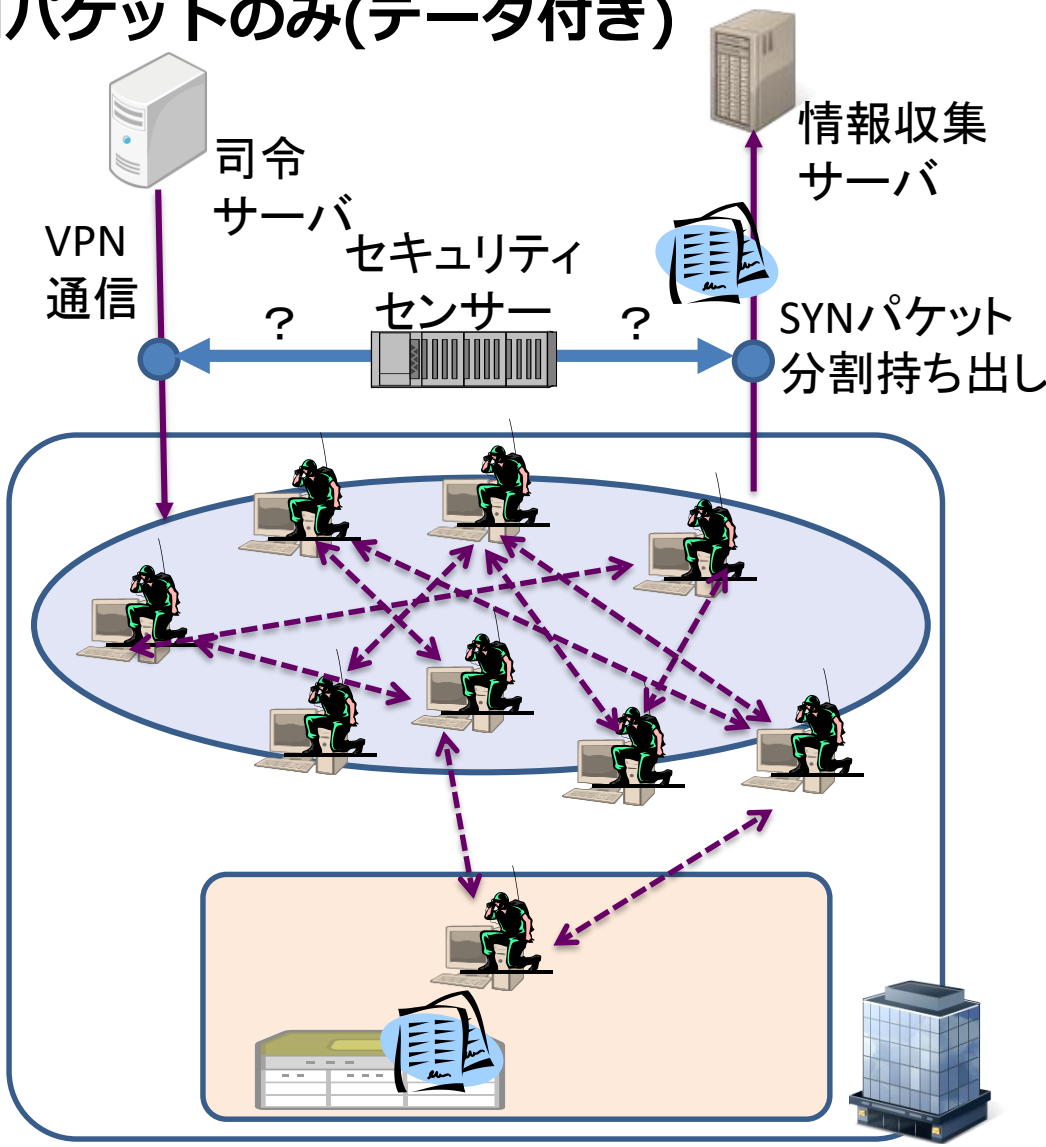
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

データ持ち出しの事例

- VPN等の暗号通信
- 送信元IPアドレス偽装
  - UDPの利用

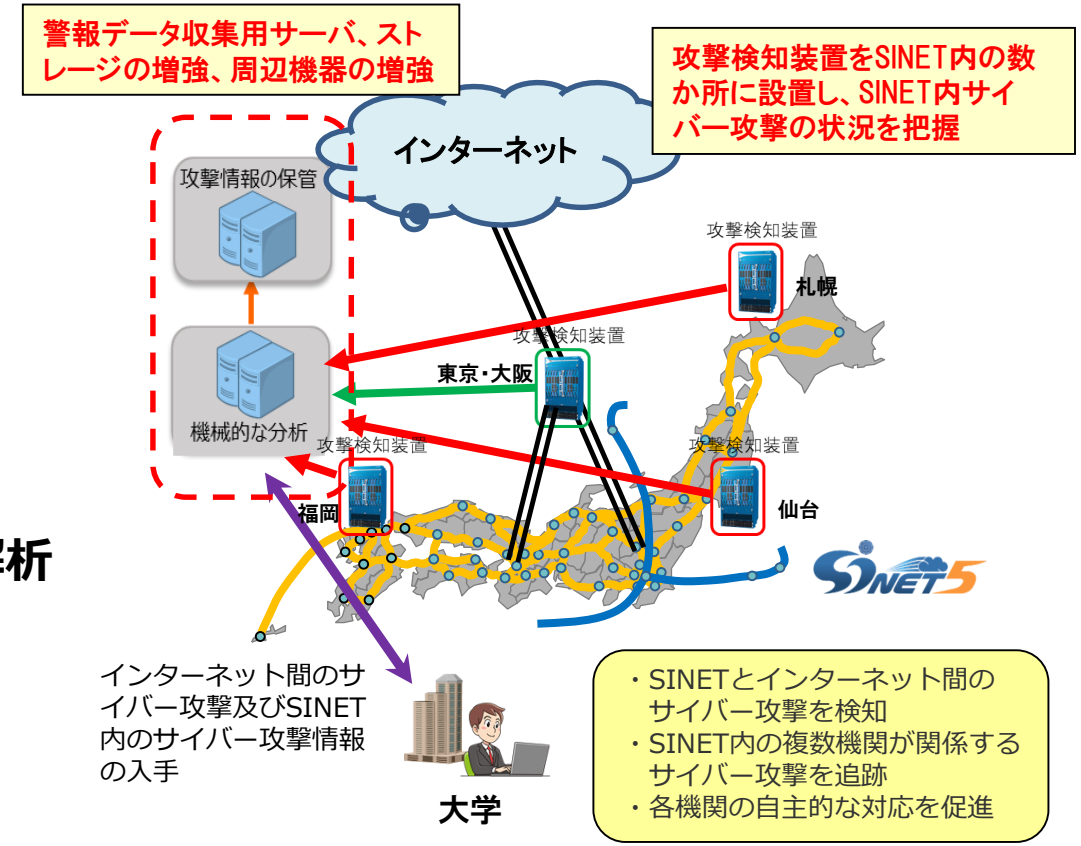


- RFC無視の通信
  - SYNパケットのみ(データ付き)



第2期計画を模索中...

- 現セキュリティ監視装置の強化
  - 次期SINETに対応するため
- SINET内にセキュリティ監視装置を新設
  - 2～4箇所を想定
  - SINET内のサイバー攻撃を検知可能に
  - SINET外との不審な通信を検知
    - 国内各所のSINET DCから関連トラフィックを転送し解析
    - 巡回監視



マルウェアEmotetによる攻撃

NII

- Emotetによる大量攻撃
  - Wordファイルのため修正が容易
    - 一文字変えればハッシュ値が異なる
      - メタデータの変更
    - Sandboxで未解析のファイルとして解析
      - 偽のC2サーバへの接続
- ターゲット機関のsandbox
  - 解析数に制限がある場合
    - 1分あたりの解析数や1日あたりの解析数
  - 制限を超えると偽C2サーバへの接続停止
    - 外部からsandbox解析停止を確認
- 本命の対象者への攻撃メール
  - Sandboxでの解析を受けない
  - 検知パターン/検知ハッシュ値の生成ができない→ユーザが開封してしまう

NII-SOCSサンドボックスでの解析
の
90%以上がターゲット機関

Sandboxの使い方
検知パターン/検知ハッシュ生
成
ユーザの開封前に発見・駆除