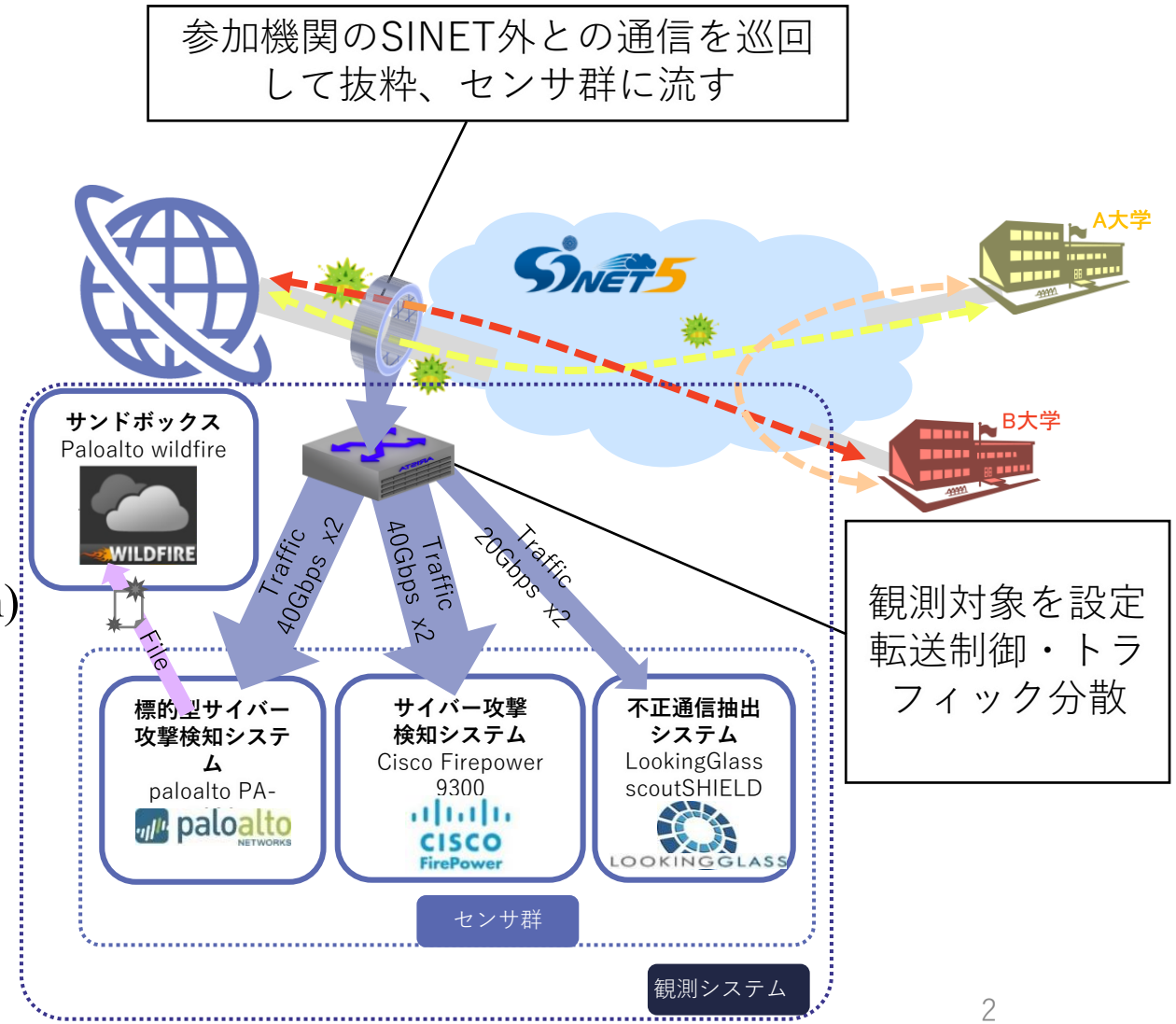
NII-SOCSの運用で見えるサイバー攻撃の変化

高倉弘喜
国立情報学研究所

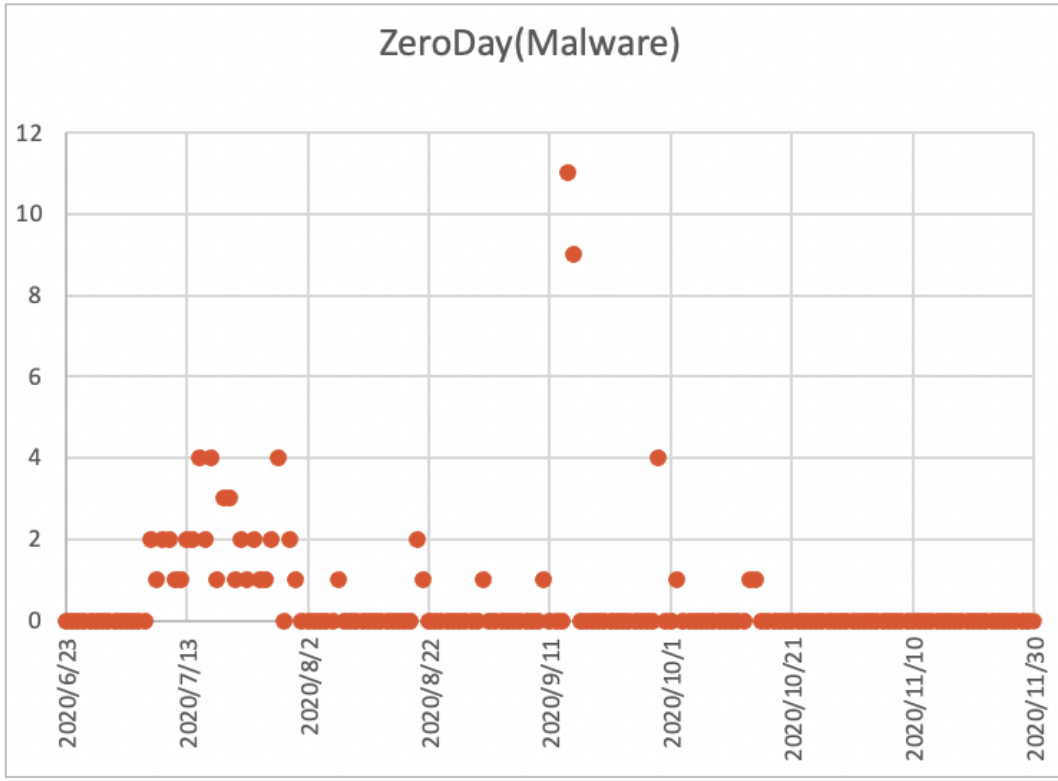
NII-SOCSの観測体制(現在)

- 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(2016-2021)
- 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
  - 米国政府系脅威情報(LookingGlass scoutVision)
  - 民間系脅威情報(CyCraft CyberTOTAL)
  - 民間系脅威情報(Recorded Future)
  - 民間系脅威情報(Cisco Threat Grid)
  - 攻撃者情報調査(McAfee APG)
  - オープンソース系(Twitter、Shodan)
  - その他独自収集(業務委託先、教職員独自)



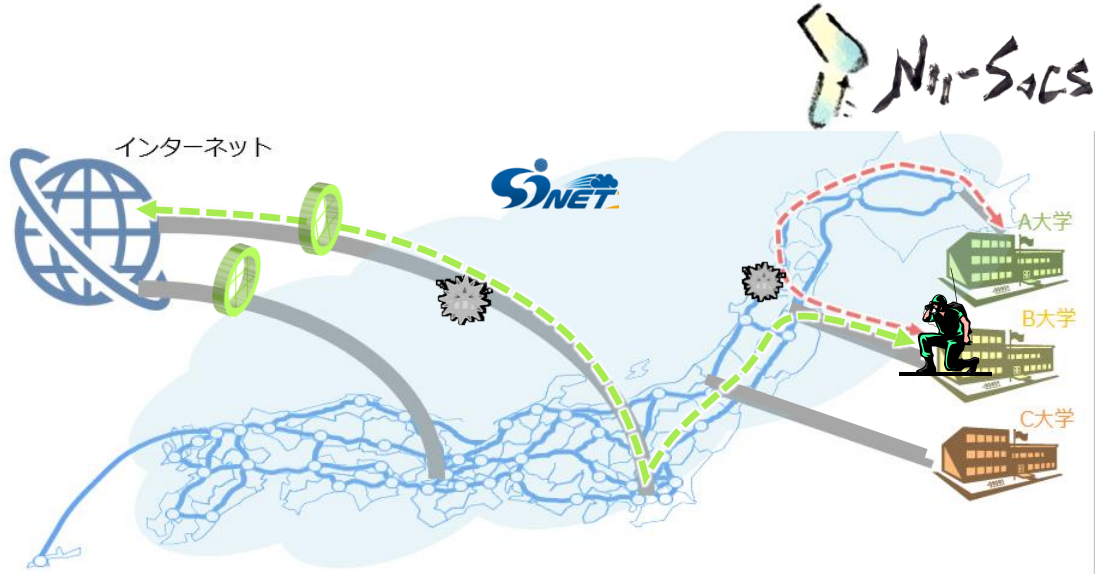
遅延起爆型マルウェアに備えた検査用保存食(検食)

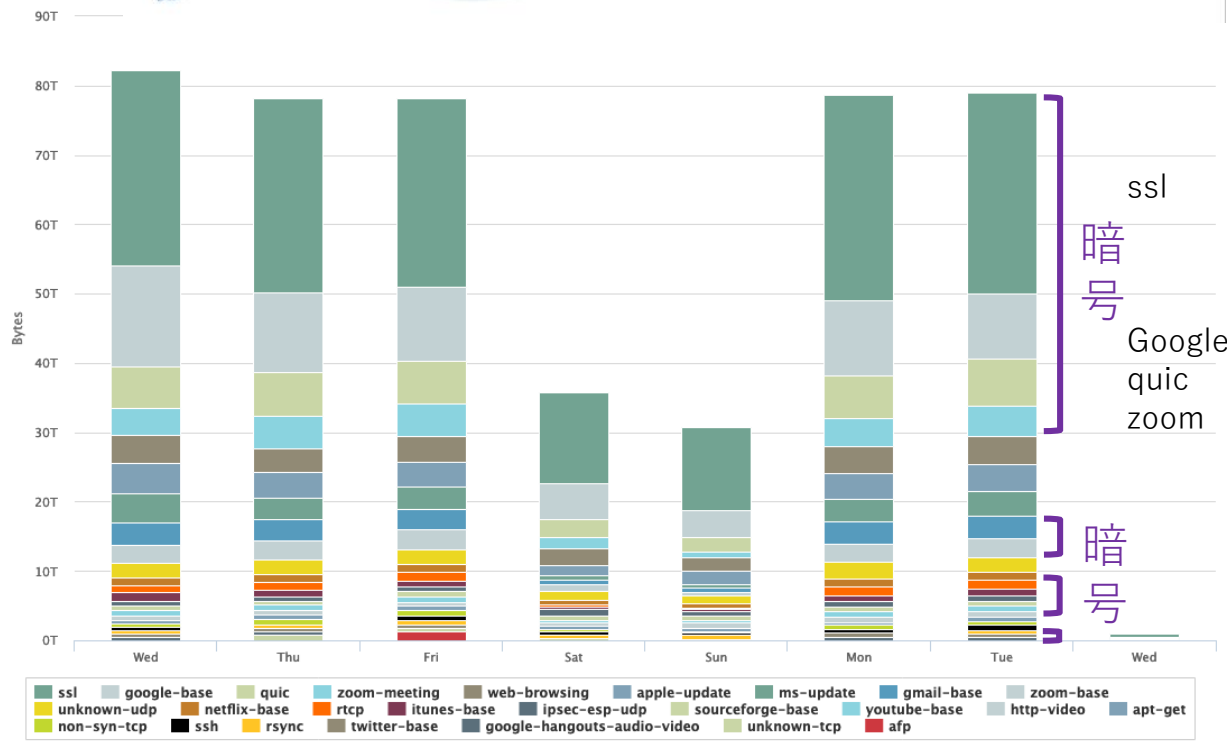
- マルウェア到着から活動開始までに数日から数週間の遅延
  - サンドボックスでの解析時には発症しない→破損ファイルと判定
  - Emotet系の事例
    - 7月に遅延起爆型の連続着弾…少種類
    - 9月に遅延起爆型の種類増加…短期集中攻撃
      - 状況判断に活用…使われ方が変わった？
- 短期保存
  - 運用系サンドボックス(Full capture)
    - 判定が微妙→〇日間保管(メーカ標準設定)
    - 毎日の動的解析とAntiVirus検査
      - 数日後マルウェア判定
- 長期保存
  - 研究ベンチマーク系でサンプル採取
    - 57日間保管
      - 観測翌日、以降毎週8回の検査(ClamAV)



暗号通信の比率急増

- 観測対象の80%以上が暗号通信
  - 100Gbps(現状)→400Gbps(SINET6)
    - 暗号を解きながらの解析は不可能
- 既存技術単独の攻撃検知
  - ほとんど見えなくなっている
  - 暗号開始前のやり取りで識別
- 2020年の状況
  - 暗号通信が全体の70%を占める
    - ssl、Google、quic、zoomなど

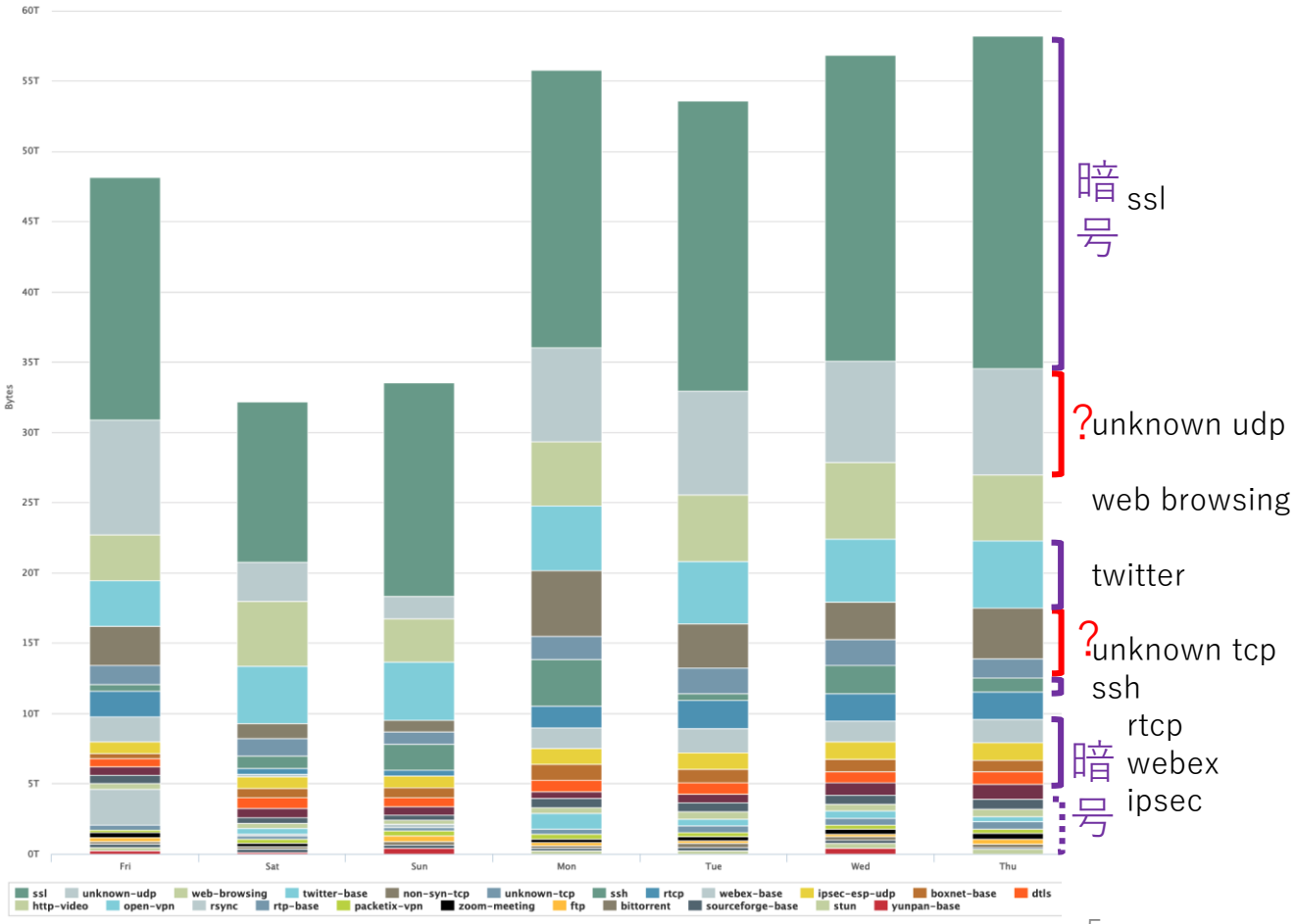




2021年の状況→脅威インテリジェンス活用へ

- 正体不明のUDP・TCP通信の増大
  - 暗号開始前のやり取りの取りこぼし
    - 通信プロトコルや通信先判定失敗
    - センサーの限界に近づいている？
  - 正規の通信手順を無視
    - 最近のマルウェアに多い
    - 大量の正規通信に紛れ込ませる
- 検知センサー
  - 正規の通信手順を想定
    - 手順無視

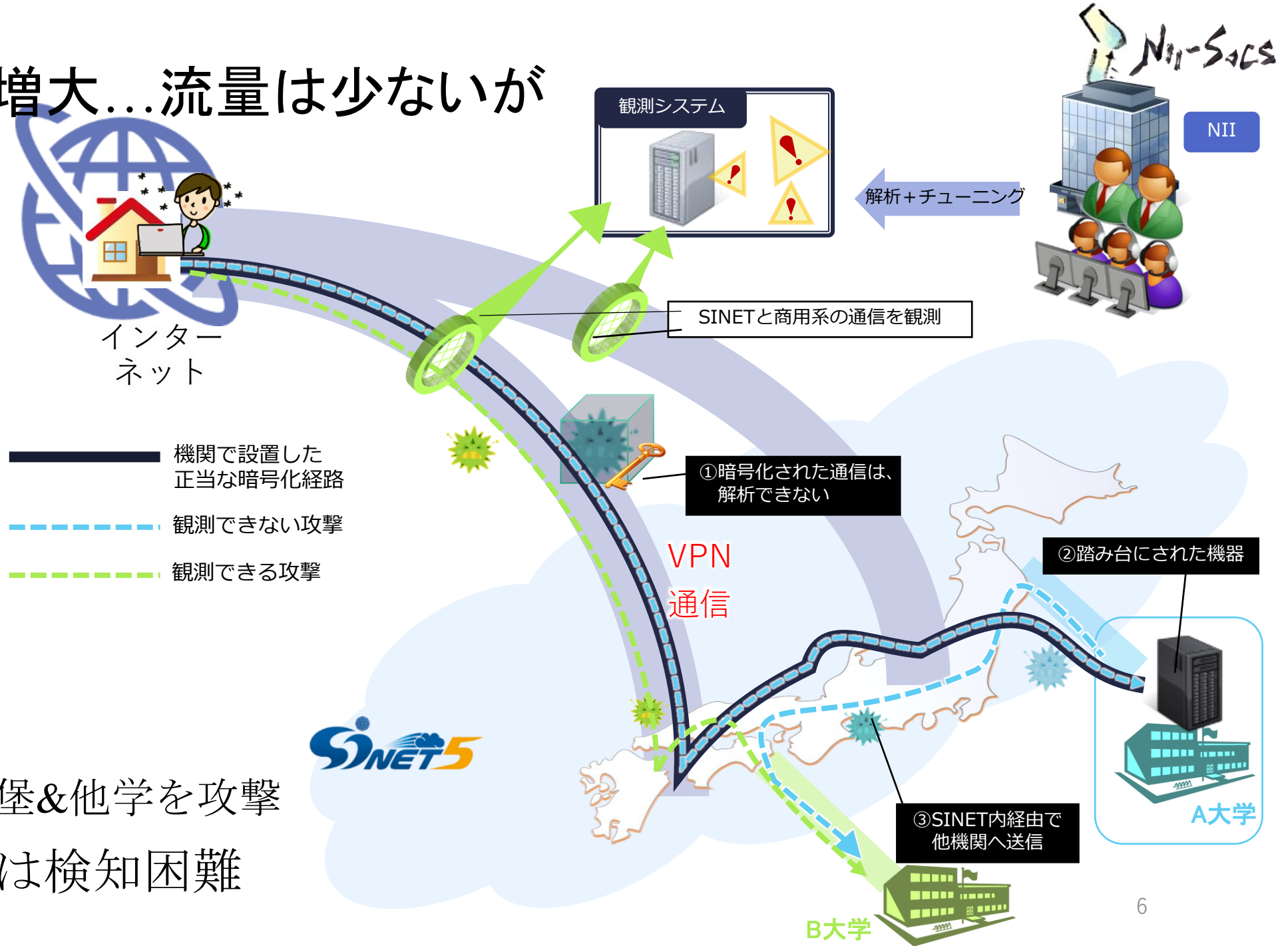
    →通信できないはず→観測対象外
- 不審な通信に注視した観測
  - 脅威インテリジェンスの活用



VPN通信の増大…流量は少ないが

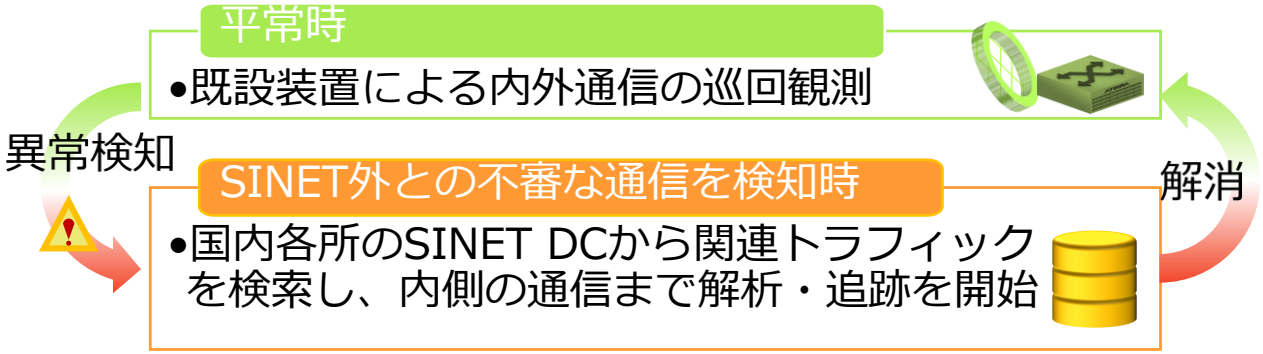
- 最近の攻撃傾向
  - VPNに便乗
  - 国内外企業の多くの事故事例の起点
- 活動拠点
  - 自宅や滞在先

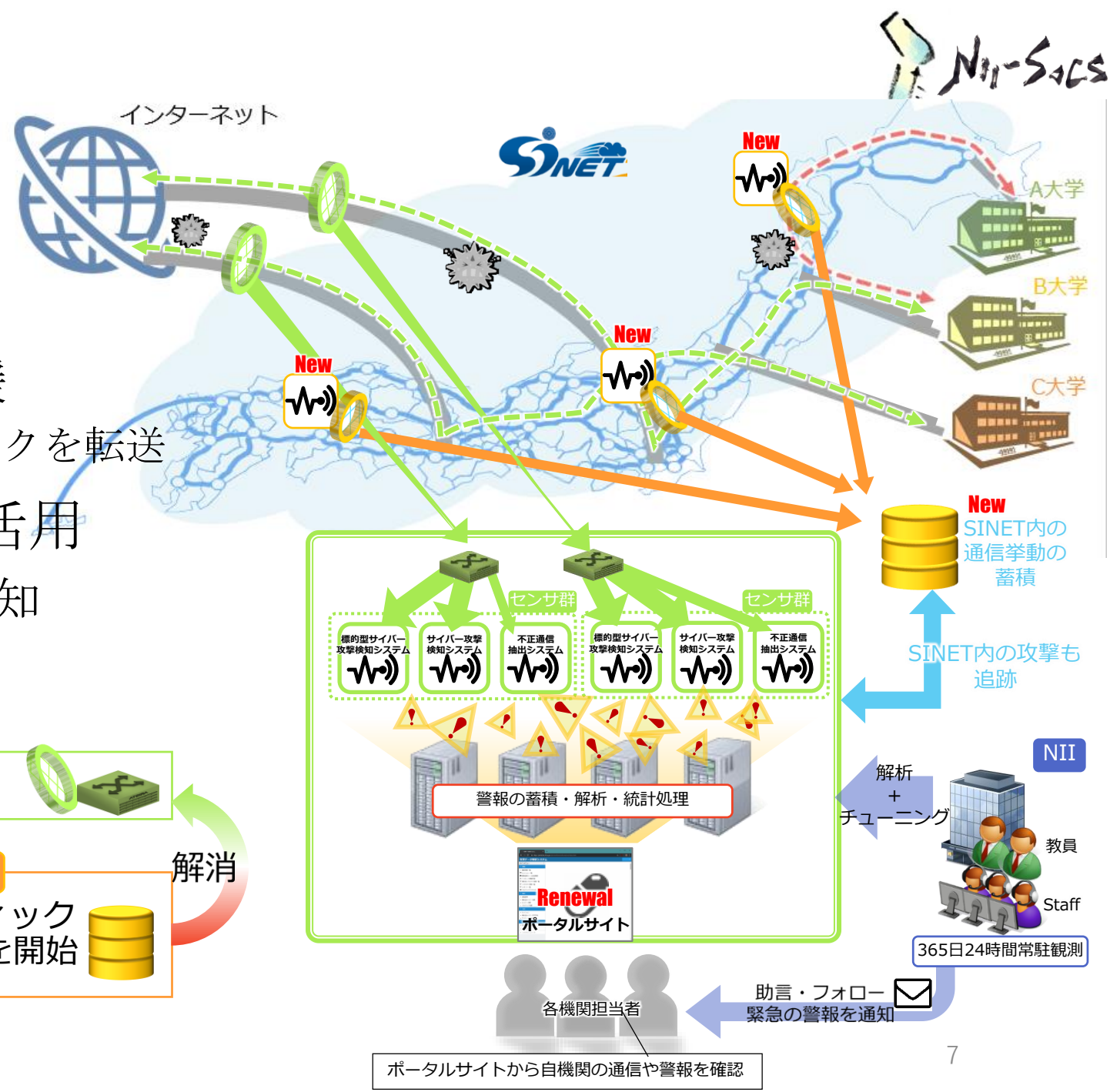
  →SINETの外
- SINET内攻撃
  - 大学内に橋頭堡&他学を攻撃
- 現NII-SOCSでは検知困難



能力拡張(R2年度補正)

- SINET内観測機器増設
  - 国内数カ所に設置
  - SINTE6の新機能による支援
    - SINET内の任意のトラフィックを転送
- 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３０分×２回　→　00:00:00～,12:00:00～　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

適切なサイバー攻撃観測のお願い

- 脅威インテリジェンスや外部機関からの連絡
  - 大学設置のサイバー攻撃観測装置(ハニーポットやDarknet)に関する情報
  - 当該装置に対する妨害計画謀議の情報
  - 当該装置による攻撃活動の情報
    - 攻撃先が他者が運用するサイバー攻撃観測装置となっている事例も
- 攻撃者グループ間の情報交換やオープンソース脅威情報で指摘
  - DoS/DDoS攻撃や偽攻撃が集中
    - 「観測装置が模倣している」実機への攻撃と比べ、著しい挙動の乖離を観測
  - オープンソース脅威情報は半永久的に存在
    - 妨害攻撃の長期間化
    - 撤去後もネットワークセグメントの利用困難
- 不自然なハニーポットやDarknetの運用
  - 運用状況を機関のCIO、CISOが把握していただきたい

https://www.nii.ac.jp/service/nii-socs/20210614.html

今後のNII-SOCSの体制…自動化の促進と新たな対策

1. 情報の相関性から情報の確度と攻撃のリスクを確認
2. 戦略策定
   - なにをどこから守るのか？
3. 作戦立案
   - 状況変化に臨機応変な対応できるか？
   - 限られた資金・人を効率的に運用するための見積
     - 何日間を想定するか？
       - 暫定対処完了までに1ヶ月かかることも珍しくない
     - 資材の備蓄は何日分あるか？
     - 補給は確保できているか？
     - 円滑な引き継ぎはできるか？
       - 1ヶ月の長期戦でもバテない体制の整備

高リスク攻撃が想定される場合

NII-SOCSのコロナ対応
昨年
1月大量備蓄開始
2月在宅勤務演習
3月在宅勤務へ順次移行
4月100%在宅勤務体制導入
今年
現在 50%/~100%在宅体制

高騰する資材単価…50%up
見込めない入荷…200日後