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
サイバーセキュリティ研究開発センター

2016/10/28

背景…サイバーセキュリティ基本法(1)

第八条

大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

- 要は…各個に戦え！
- 必要経費は…

背景…サイバーセキュリティ基本法(2)

第十三条

国は、国の行政機関、独立行政法人及び特殊法人等におけるサイバーセキュリティに関し、国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関の情報システムに対する不正な活動の監視及び分析、国の行政機関におけるサイバーセキュリティに関する演習及び訓練…その他の必要な施策を講ずるものとする。

- 独法＆特殊法人に対する監視(IPAに委託)
  - 8法人に監視センサー設置＋残り78法人への情報提供
    - ✓ 初年度約75億円＋受益者負担(200万円/年)
- 「等」に国立大学法人は含まれるのか？
  - 当初はYesの流れ→しかし…

背景…サイバーセキュリティ基本法(3)

第三十一条

本部は、その所掌事務を遂行するため必要があると認めるときは、…国立大学法人の学長、大学共同利用機関法人の機構長、….であって本部が指定するものの代表者…に対して、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。

- サイバーセキュリティ戦略本部@内閣
- NISC発文科省経由でのお問い合わせの根拠
  - 協力要請なので断ること、無視することも可能ではある
- 私学や公立大は法律で縛れないにしても…
  - どうすんの？

インシデント対応からアクシデント対処へ

- インシデント対応は技術部隊(CSIRT)の仕事
  - 被害端末の隔離、被害状況の解析、感染駆除など
- アクシデントに発展するか？
  - 被害範囲の特定
  - 防衛ラインの設定
    - 稼働させ続ける機器(リスク分析も必要)
      - ✓ 年金機構でも外部との接続を継続した部門あり
    - 停止させる機器(業務への影響分析も必要)
  - アクシデント終了の復旧計画
    - 再接続の条件設定や判断

→CSIRTだけでは対応できない

学術ネットワークの特徴

- 多種多様な情報機器
  - 一般的なサーバやPC
  - モバイルディバイス
  - 実験機器
    - 大多数はWindowsやLinuxを内蔵
  - 制御機器
    - 一部はWindowsやLinuxを内蔵
- 開かれた研究環境
  - 私物端末の持ち込み
  - 研究データの持ち出し
  - 国際共同研究
- 分離/隔離ネットワークの利用が困難

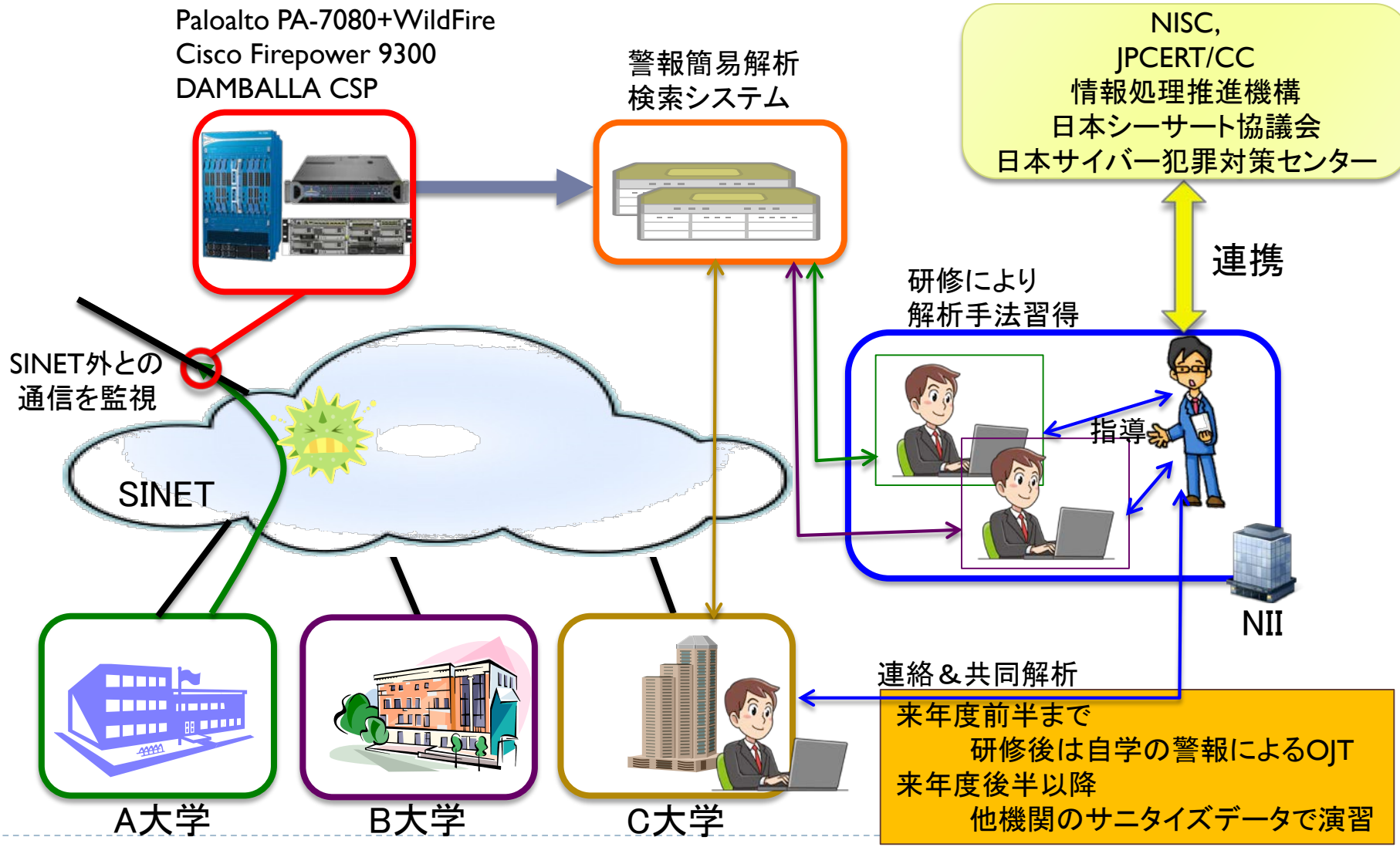




超大規模ネットワーク環境のセキュリティ対策

- SINET5による広帯域化
  - 100Gbps
  - 10～40Gbps
- 様々な接続機関…844機関
    - 国立大学法人等(86+16機関)
    - 公立･私学･高専
    - その他
  - SINET外との接続
    - 10Gbps～100Gbps
- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 初年度構築＋運営費
    - 7.8億円+受益者負担0円

NIIによるセキュリティ監視基盤の構築



巡回監視

- 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間
  - 変化点分析や機械学習による異常セッション検出

何を見るのか？

- 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

NIIでの監視手順

- 平常時
  - 警報の簡易解析の結果
    - 危険度の高い警報
    - 増加傾向にある警報
    - 攻撃成功の可能性が高い警報
      - ✓ 警報確認の際にセッション情報を閲覧
- 大学等との共同解析時
  - 大学側が閲覧を許可した警報の詳細
    - ペイロード中に含まれる文字列
      - ✓ 検知の根拠として記録

何を保存するのか？

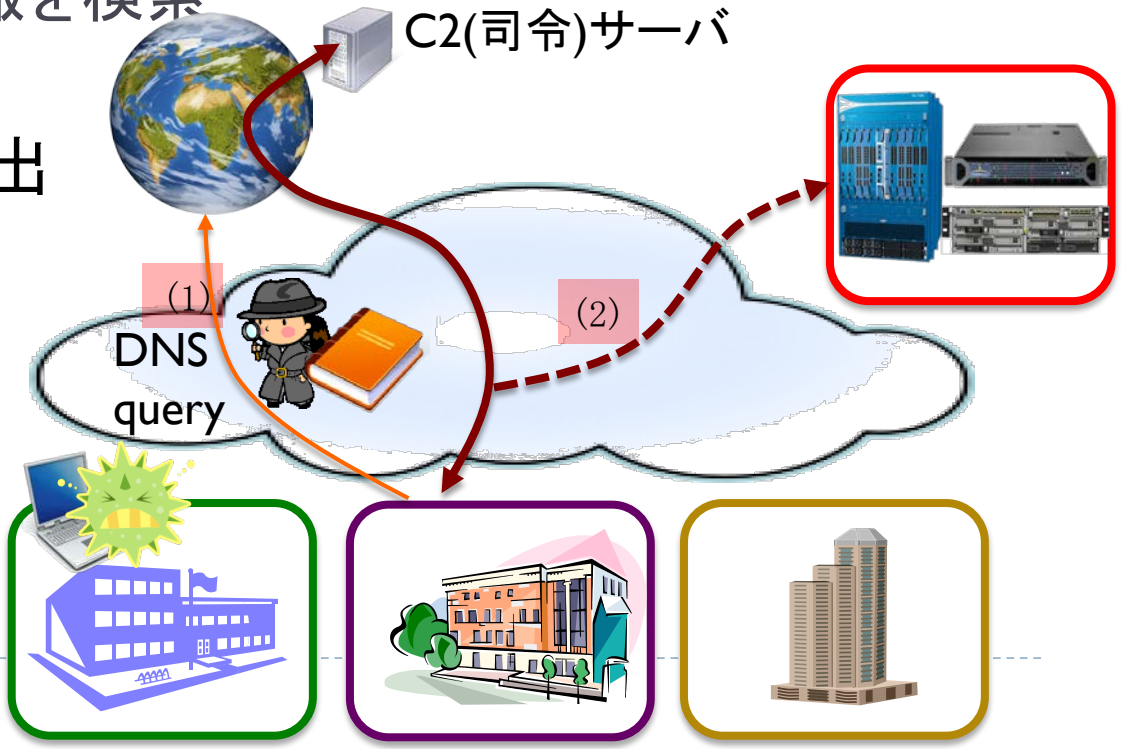
- 解析システム@NII
  - 平文として保存
    - ヘッダ情報とアプリケーション情報
  - 暗号化後に保存
    - 検知情報
      - ✓ 暗号化（復号）の鍵は毎月更新
        - 当該月の間はNIIも鍵を保持
          - NIIも閲覧することができる
      - ✓ 過去の「暗号化（復号）の鍵」
      - ✓ 暗号化してNIIで保存
        - 『暗号化された「暗号化（復号）の鍵」』の復号（取り出し）
          - 大学側でのみ可能
          - 鍵の入手後はNIIも閲覧することができる

不必要な閲覧の抑止

- 暗号化された検知情報の閲覧
  - 当該月分はNII単独で閲覧可能
  - 前月以前は大学から鍵の提供があればNIIは閲覧可能
- 主記憶への保存(残留磁気対策)
  - 大学から提供された鍵
  - 復号した検知情報
- 検知情報の閲覧
  - 閲覧記録をログとして保存
    - NII、大学両方の閲覧記録
  - 各大学向けポータルサイト
    - 閲覧記録の確認画面

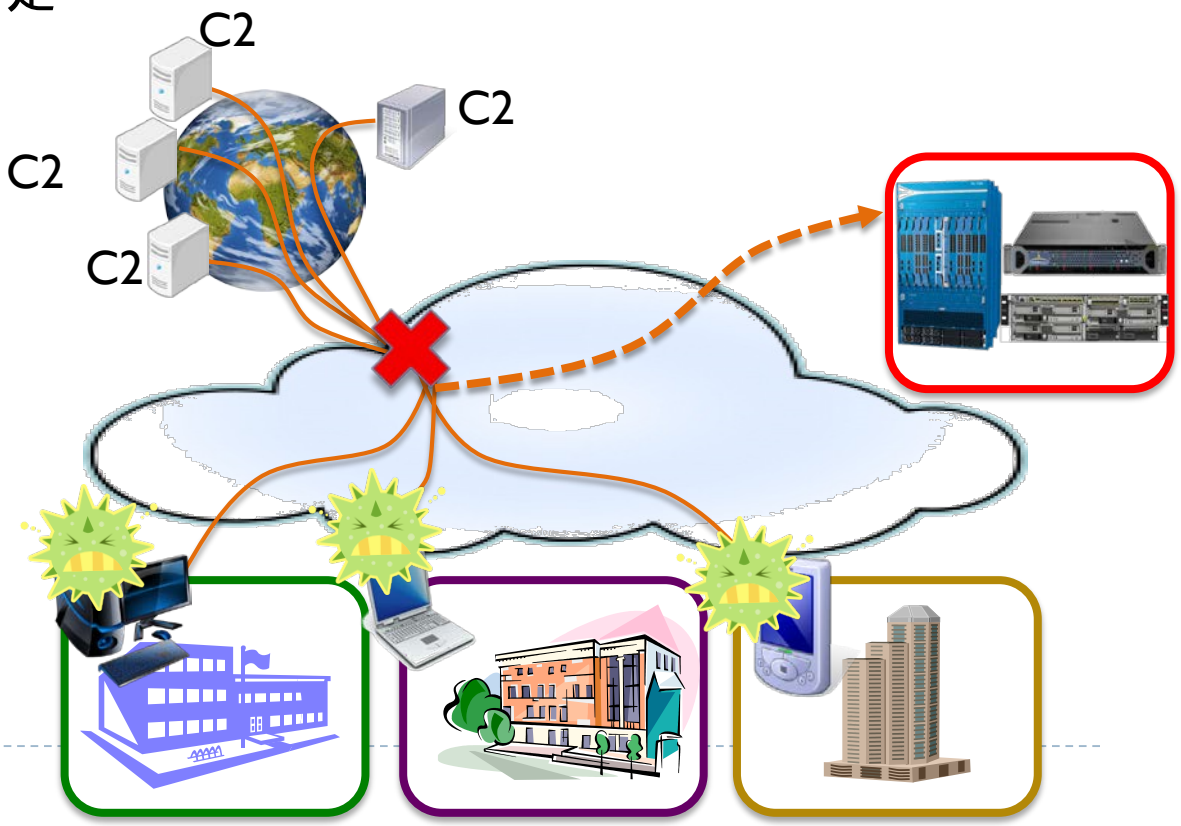
不審な通信の検知(DNS問い合わせ検知)

1. DNS queryをブラックリストと照合
2. 該当した場合、感染疑い機器がSINET内に存在
   - C2サーバとのセッション履歴を調査
     - 巡回対象でない場合：C2サーバとのセッション情報の記録開始
   - C2通信に関する警報を検索
     - 感染判定
3. 感染疑い機器を抽出



感染疑い機器に対する調査

4. **感染疑い機器の全セッションを解析**
   - 共通の接続先＆単調な通信などの特徴を確認
   - C2通信に関する警報を調査
     - 予備C2サーバの特定
- **4の繰り返し**
  - 未確認C2サーバ　C2
    - あぶり出し



辞書攻撃の検知例

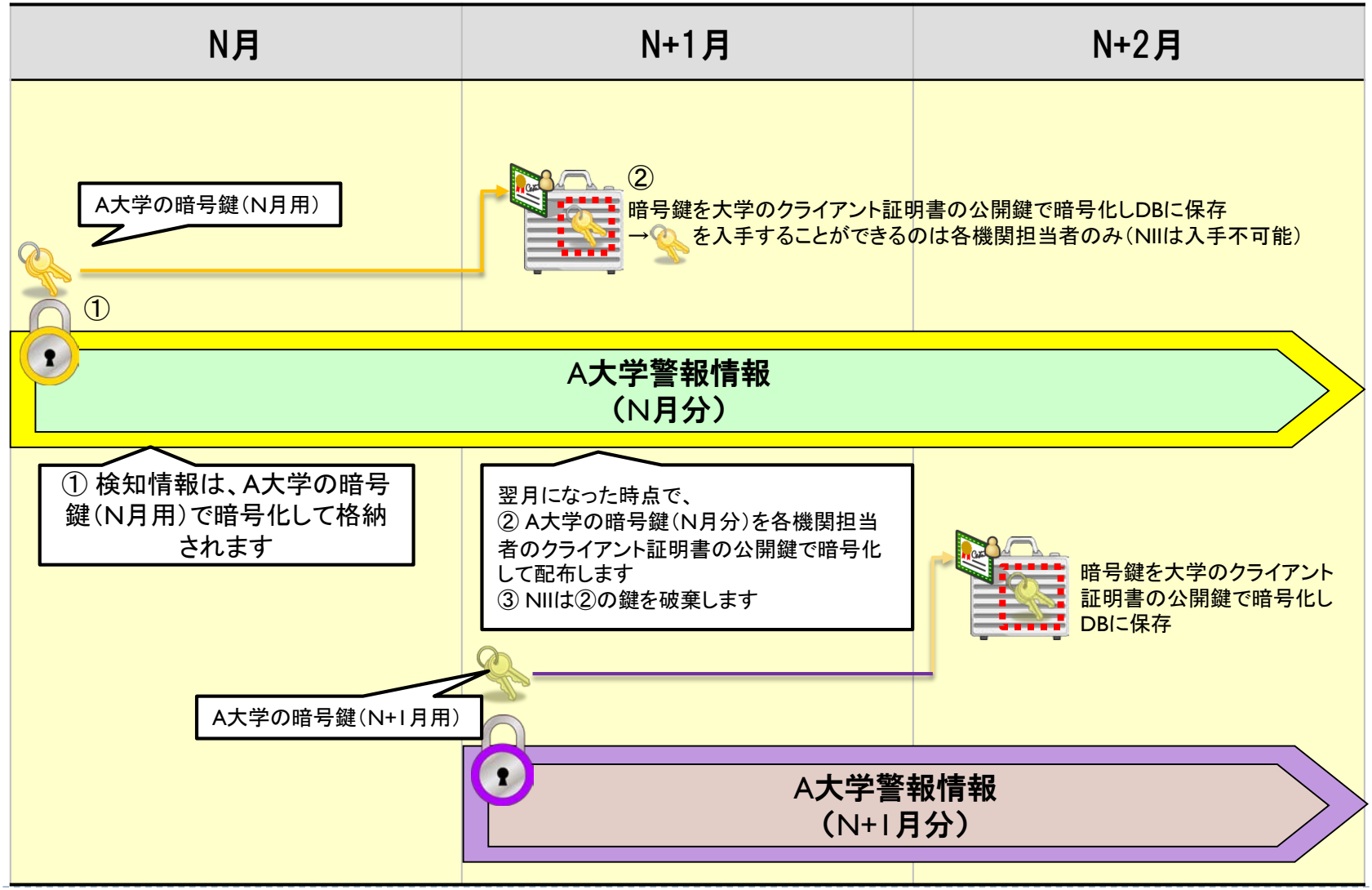
1. 辞書攻撃の警報から攻撃元IPアドレスを特定
2. 攻撃元IPアドレスでセッション情報を検索
   - セッションサイズの変動を解析
     - 平均に比べ極端に大きなセッション→侵入成功の可能性大
3. 被害機器のIPアドレスでセッション情報を検索
   - 過去に存在しない接続元
     - 辞書攻撃の平均に比べ極端に大きさセッション→追加侵入の可能性大

- 上記の事項を確認したのち、大学へ連絡

NII SOCによる監視の基本

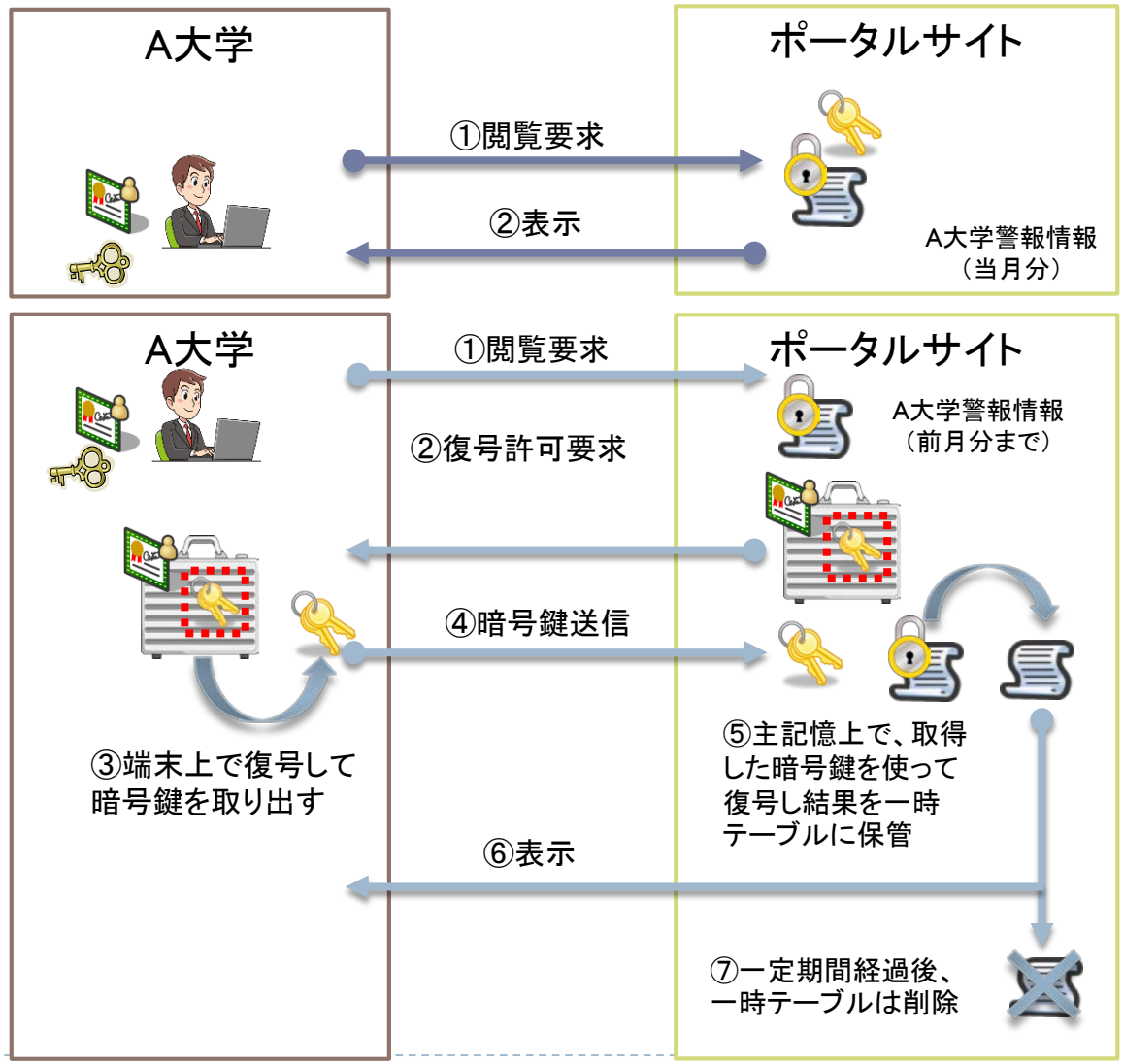
- 原則として
  - タイムスタンプ、IPアドレス、プロトコル、ポート番号、通信アプリケーションの種別、セッションサイズ等の情報を閲覧
- 「通信の内容」の扱いについて
  - 警報情報のうち、検知文字列などが含まれる項目
    - 通常の監視では検知システムの生データは閲覧しない
  - 共通鍵暗号方式の暗号鍵で暗号化して保存
    - 暗号鍵は毎月生成され、前月分以前の鍵は大学のみが保持
    - 大学の依頼を受けてNII SOCは閲覧
      - ✓ 提供された暗号鍵および復号された情報
        - 主記憶上の一時テーブルに展開
      - ✓ 閲覧ログを記録(NII SOCおよび大学担当者)
    - 完全な保護ではない

共通鍵による警報情報の暗号化

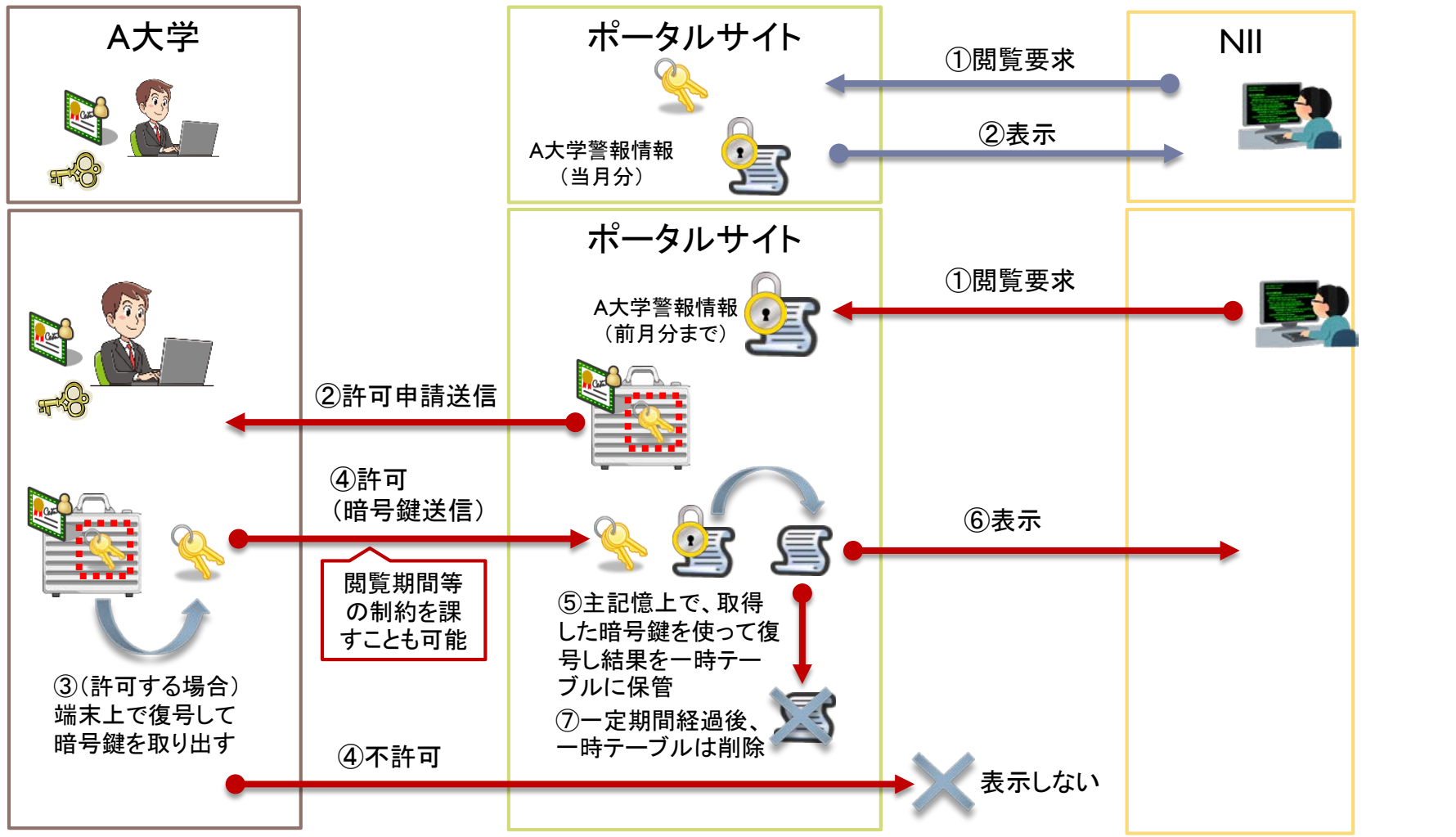


通信の内容の閲覧手順(大学側)

- 当月分のみ
  - NIIは逐次暗号化するために暗号鍵の保持が必要
  - NIIサーバで復号
- 前月以前
  - 暗号鍵の取り出しを大学に依頼
  - 許可された警報のみ主記憶上で保存
  - 一定時間経過後に削除



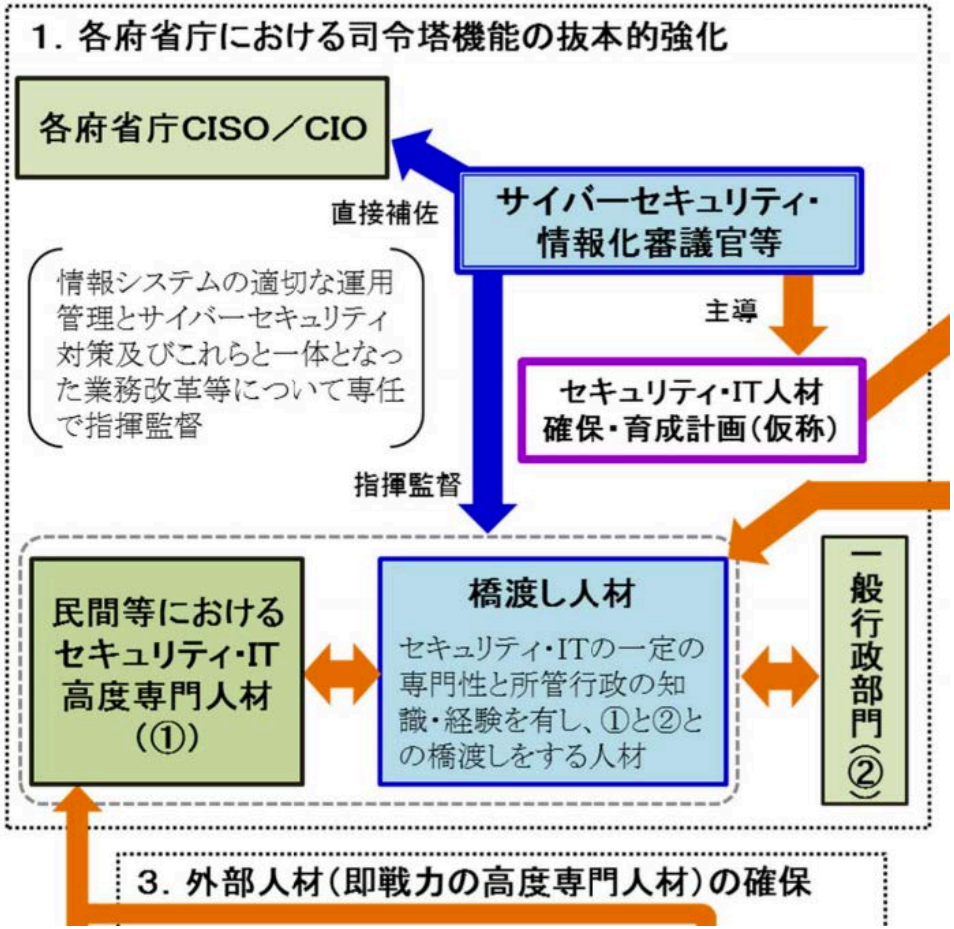
通信の内容の閲覧手順(NII側)



- いずれの場合も閲覧記録のログを保存
- 許可申請の送受信の手法は現在検討中

NII SOCでの人材育成

- 橋渡し人材
  - インシデント対応
    - 技術的知識
  - アクシデント対応
    - 経営的知識
    - その組織の歴史的背景
- 各組織での育成が必須
  - 霞ヶ関の動きは大学へ
    - 4年間で1,000人程度(全省庁)
  - 各校に数名という規模



【政府機関におけるセキュリティ・IT人材の育成】
1．各府省庁における司令塔機能の抜本的強化
2．橋渡し人材（部内育成の専門人材）の確保・育成
3．外部人材（即戦力の高度専門人材）の確保
4．一般職員の情報リテラシー向上

NII-SOCでの人財育成支援

- 各大学の技術職員のレベル向上
  - 多くの機関
    - SOC専属の教職員は稀
    - NOC担当の職員による片手間
    - そもそも技術職員が不在の機関も
- 必要な対策の選択肢を提示
  - 10パターンもない(京大、名大の経験)
    - 感染マシン、セグメント隔離…
    - 通信プロトコル制限…
- 役員向け説明能力
  - インシデント(事案)ではなくアクシデント(事態)目線で説明
    - 文科省への第一報が必要な事態なのか否か？
      - ✓ 未確定情報はなんなのか？

厚労大臣曰く
それは100件なのか？
500万件なのか？

NIIにおける職員向け研修

- 1日を想定
  - 警報閲覧ポータルサイトの使い方講習
  - 以後は各自の職場におけるOJT
- 来年度前半(予定より半年遅れで進行中)
  - 基盤センター系＋αの職員を対象とした講習
  - 各地区で大学向け講習会の開催の支援

大学側で必要な作業

- 連絡先窓口MLの設置
  - 担当教職員
  - ネットワーク運用外注先
  - セキュリティ監視外注先
  - MLのミッション
    - 連絡を受けての学内体制の整備
      - ✓ こーんな連絡が来るから、こういうことやってね。

どこまで含めるかは
各校の判断

- NII側への共同解析の依頼
  - 通常、NIIから暗号化したペイロード部分の復号は求めない
- 文科省への報告
  - NII単独では推定情報まで
- 暗号化された共通鍵の復号NIIは共通鍵自身を保持しない

正式運用に向けて

- 約款を準備
  - 運用手順や連絡体制
  - NIIに対する制限事項
    - 試行運用の結果を見ながら調整
- 警報の保存期間の明文化
  - 3ヶ月を想定
    - RAIDの保存容量の限界
    - 各大学のセキュリティポリシーとの整合性

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

2017年度半ばより
公開予定