# 実インシデント対応による高等教育機関のサイバーセキュリティ管理体制の強化

高倉弘喜
国立情報学研究所

# サイバー攻撃の深刻化

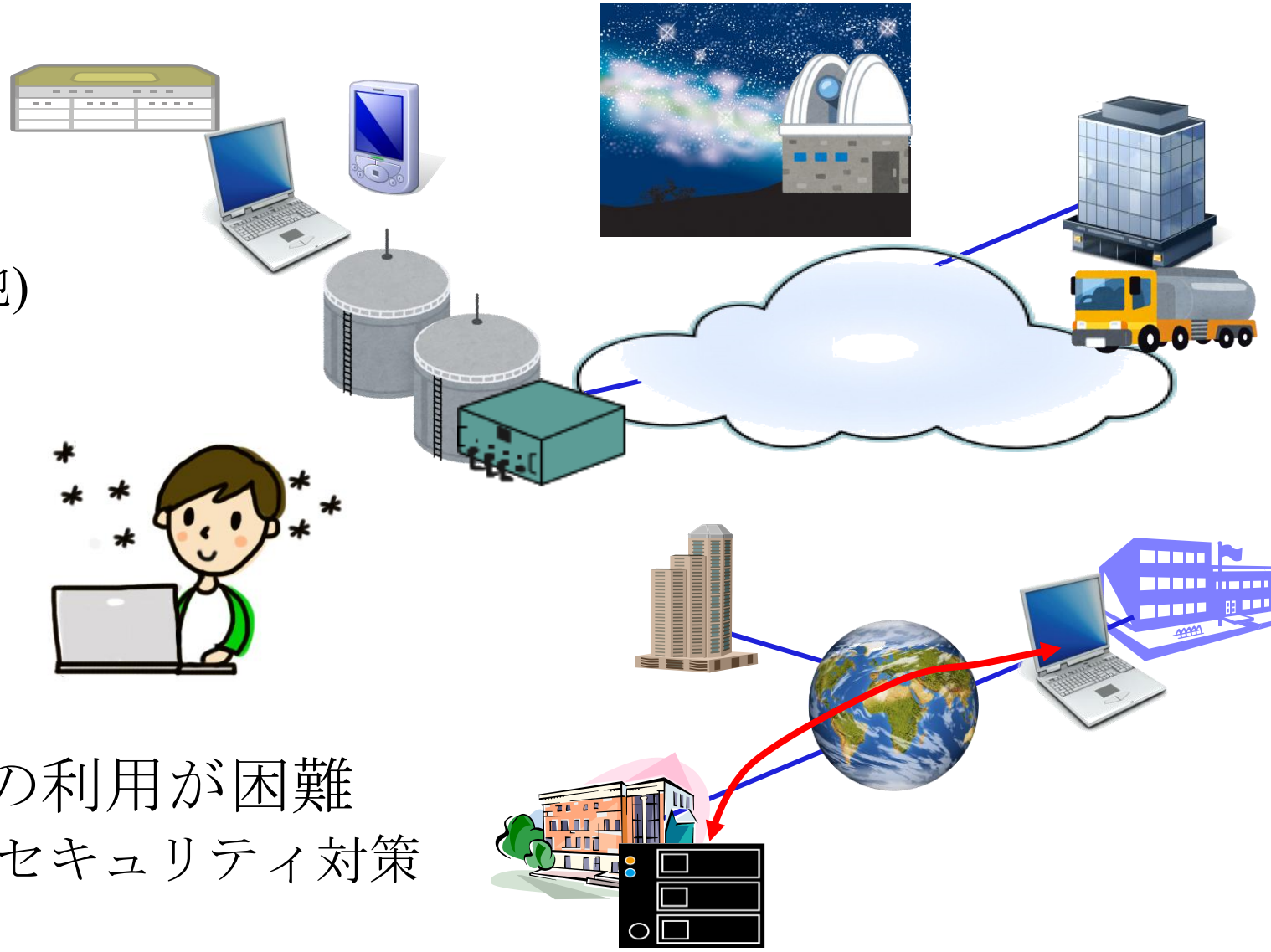
- 学術研究機関も標的
  - 研究者の保持するデータ
    - 様々な知財
      - 次世代における産業の礎
    - 間接的に安全保障に関連する
      - 海洋
      - 航空・宇宙
      - 原子核物理
      - 文系分野でも
        - 経済、歴史、言語…



https://www.sankei.com/politics/news/180412/plt1804120003-n1.html
http://tech.nikkeibp.co.jp/it/atcl/column/16/020800033/020800001/

# 学術機関の特徴…多種多様な接続機器

- 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
  - 観測・実験機器(超遠隔地)
  - センサー
    - 遠隔監視/管理が一般的
- 開かれた教育研究環境
  - 私物端末の持ち込み
  - 国際共同研究
    - 研究データの共有
- 分離/隔離ネットワークの利用が困難
  - という状況でのサイバーセキュリティ対策

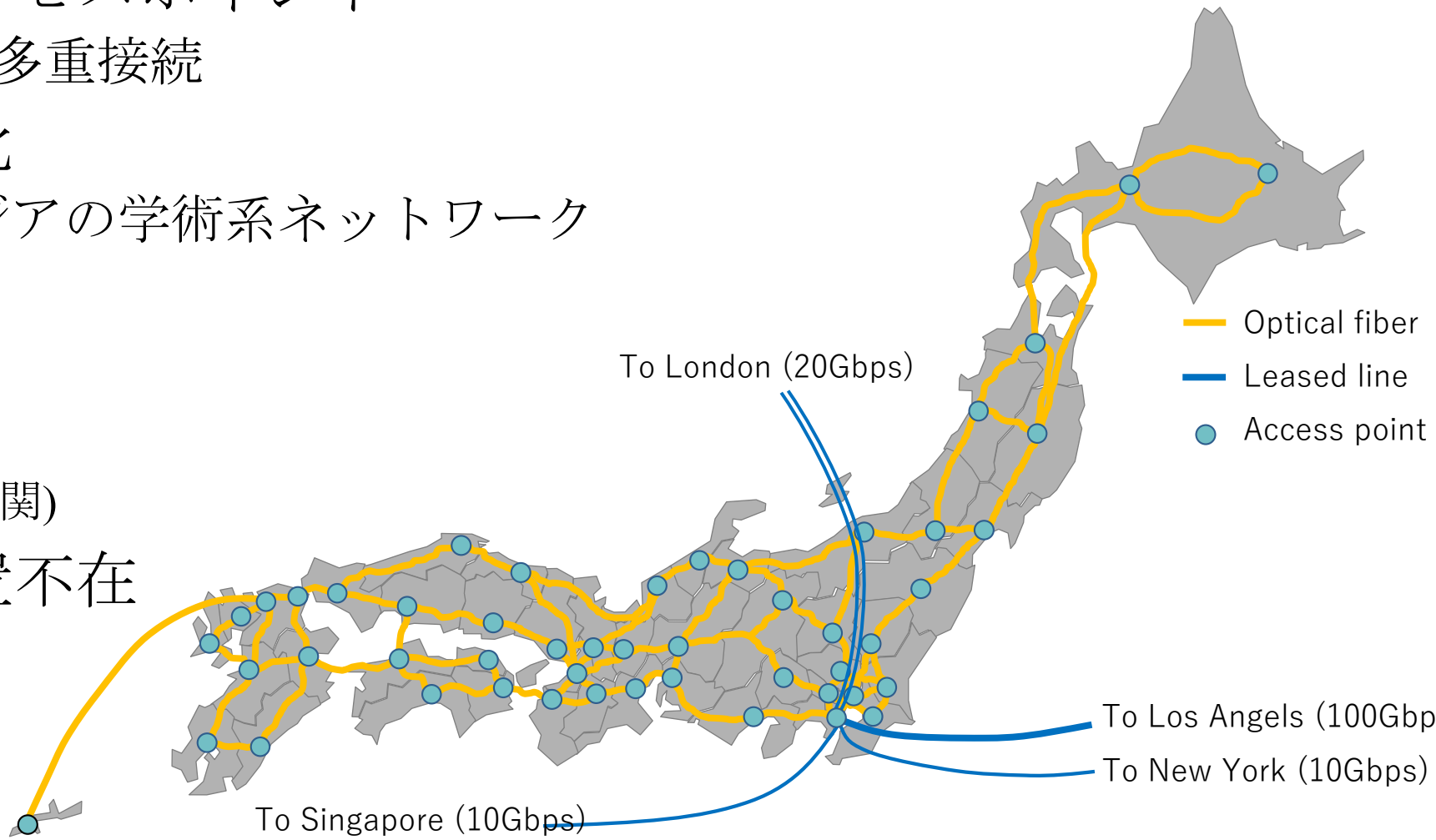


# 学術機関故の悩み…広帯域ネットワーク接続

- 国内50箇所のアクセスポイント
  - 100Gbps回線での多重接続
- 海外線の広帯域化
  - 米国、欧州、アジアの学術系ネットワーク
- 大学の接続帯域
  - 817機関
    - 100Gbps (16機関)
    - 10-40Gbps (101機関)
- セキュリティ装置不在

↓

NII-SOCS発足へ



# NII-Security Operation Collaboration Services(NII-SOCS)の経緯

## ■サイバーセキュリティ基本法

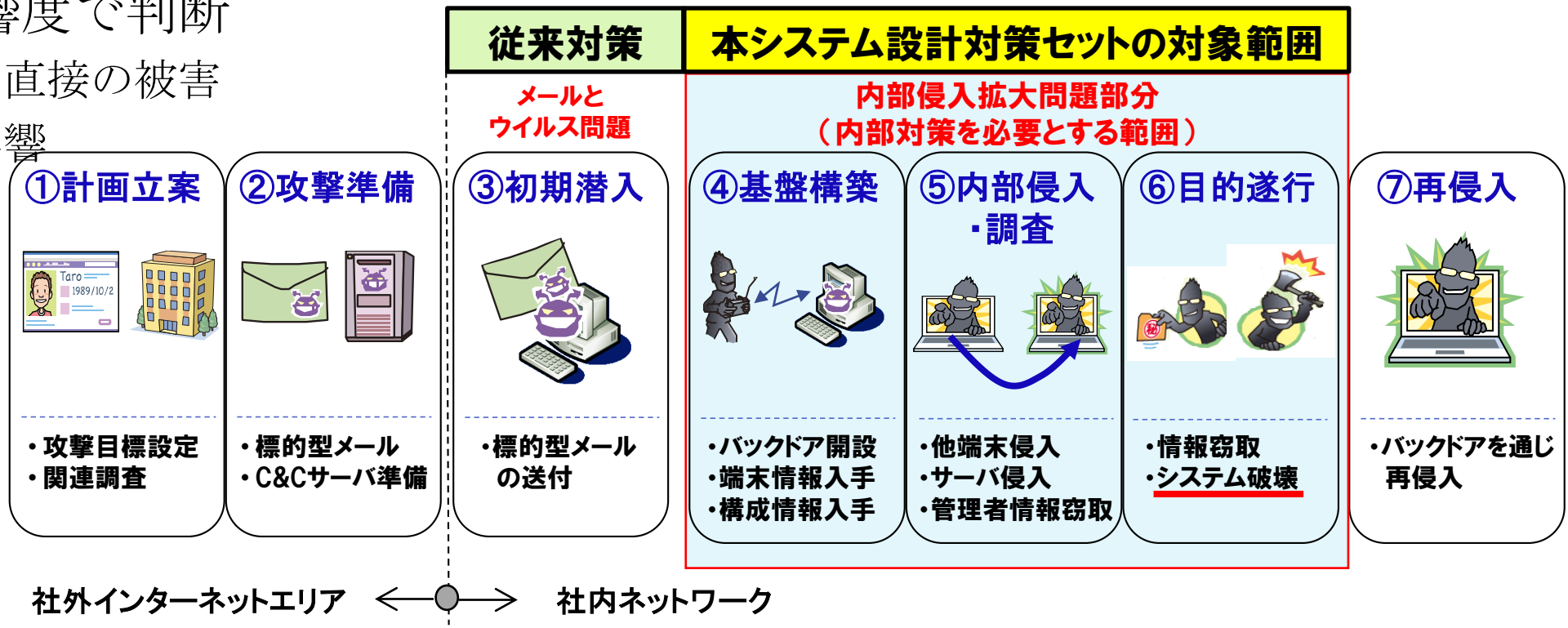
- **第八条**　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
- **第三十二条**　本部は、その所掌事務を遂行するため必要があると認めるときは…国立大学法人の学長、大学共同利用機関法人の機構長…に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。

…と言われても…

# インシデント対応からアクシデント対処へ

- 基盤構築や内部侵入・調査段階の発見対処
  - 目的遂行の阻止
- 単体のインシデントで右往左往しない
  - 組織への影響度で判断
    - 攻撃による直接の被害
    - 業務への影響
- アクシデント
  - 業務停止
  - 人的・金銭的被害発生

機械的対処では対応不能に




http://www.ipa.go.jp/security/vuln/newattack.html

# エリートパニックによる事態悪化

- エグゼクティブレポートよりテクニカルレポートを求める経営
  - 「アドウェアって何？」って役員に聞かれたら…
    - 「不要な広告表示プログラム」って言い換えれば良いやん！
      - 「不要な広告って広告になるのか？」…ツッコミ入れるとこそこかい！
        - 「不要なポスティング広告を表示するプログラム」ならどうだ！
          - 「不要とはいえ広告をセキュリティソフトが検知するのか？」…そこじゃなくて…
- 一段上がるたびに「目黒のサンマ」化する報告書
  - 「現場は状況を把握してるのか？」
  - 「インシデント対応能力はあるのか？」
    - インシデント対応そっちのけでサイバー用語辞転の執筆会議
- どんどん遅れるインシデント対応
  - 軽微なインシデントがアクシデントに


結局、NISCなどからお電話
「意味がわからん。技術用語を…」

# エリートパニックが引き起こす典型パターン

- (標的型？)サイバー攻撃によるマルウェア感染を確認
  - 被害状況(感染台数、感染部署、情報流出の有無)は不明
    - どのような対策が考えられるか？
- 多くの組織で実行されるネットワーク遮断
  - 組織部署、もしくは、組織全体をインターネットから隔離
- これは正しい対応と言えるのか？
  - 業務が止まる
    - 教育機関の場合、授業が止まる
  - 情報インフラが弱体化する
    - ブービートラップの可能性も
      - 日本では確認されていないが…
- 先の見えない籠城戦になっていないか？

# サイバー時代の籠城戦の心得

- 短期決戦であること
  - 情報流出を防止するという観点では正しい
  - 良くて数日…1週間経過すると、組織内のIT系は弱体化する
    - サイバー攻撃の手口は秒単位で進化
    - 籠城中に見つかった脆弱性対策は？
- 備蓄が十分であること
  - データの鮮度は→秒単位で賞味期限切れなものも
    - 籠城中に発生する損害は許容範囲内か？
- 情報収集は可能か？
  - 備蓄が底をつくまでに補充が受けられる見込みはあるのか？
    - 教務データ、OS・アプリの更新データ、セキュリティ情報
      - ➢ 有害なものを排除できるか？

あらかじめ出口戦略を定めておく

# IT依存度が急速に高まる大学

- 見えない攻撃にどう対処するのか？
  - 重要なのはインシデント対応、それとも、事業継続？
- CIAからAICへ
  - 大学の事業が継続できること(Availability)
    - そもそもインシデントによるシステム停止と故障によるシステム停止の違いは？
    - 重要システムの故障でも事業継続… ダメージコントロール
  - 情報が得られることも重要(Integrity)
    - 異常データを吐く機器が特定可能
      - データ破棄 or 参考値として使える デグレーテッドオペレーションの可能性
        - NWは生きていることが分かる…も情報
  - 個々の機器のconfidentialityはそこそこでよい

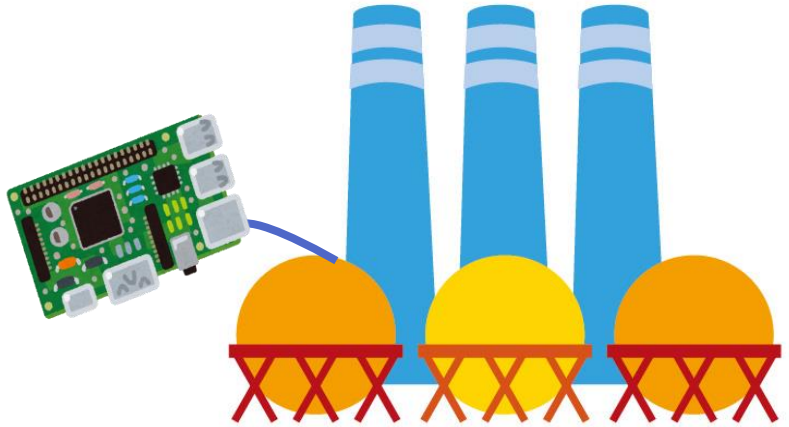
レジリエントな情報システムの設計

# 難易度が上がるサイバー攻撃対応

- これまでは…CIA (蟻一匹通すな!)
  - マルウェア感染、サーバ乗っ取り
    - 直ちに遮断・隔離
      - セキュリティ First!
  - パソコン１台なくなったってどーってことはない
    - 予備機の1台くらいあるだろう

Confidentiality
Integrity
Availability

- 最近はAICへ (擦り傷、大したことない!)
  - IT系を先に遮断・隔離をすると制御不能に…
  - セキュリティの前にセーフティ
    - 物理現象(化学反応)は急には止まれない！
    - 停止状態を維持するための情報システム
- 攻撃による被害予想と対処による副作用
  - バランス感覚のある対処能力が必要に



そもそもそんなモノをネットに繋ぐなんて…

# 事前に立案する要領・手順や人による対策

- 情報システム単体ではなく業務単位で事前に考えておく
  - アクシデントに至った状況下での適切な判断は困難
    - エリートパニックによる思考停止→全面遮断
- ダメージコントロールを想定した業務体制
  - ある研究室でマルウェア感染
  - 教務システムでマルウェア感染
  - 認証システムへの不正アクセス

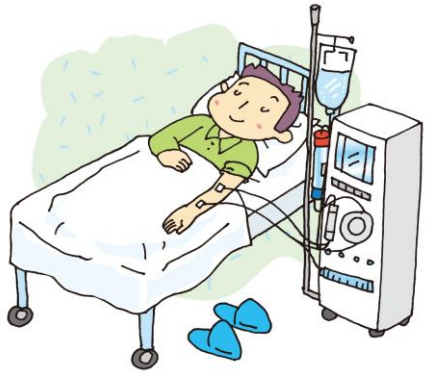
リスクレベルに応じた対応

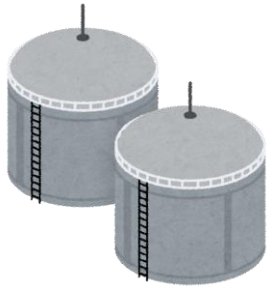
- デグレーデッドオペレーション(縮退運転)を検討
  - 止められない
  - 止めたくない
  - 止めるしかない

停止による影響を考慮

# 止められない情報システム

- 運用停止による影響が甚大
  - 人命に関わるもの(医療機器、危険物の管理)
    - 手動操作が困難
- ダメージコントロール
  - 運用継続による被害拡大防止
    - 防衛ラインの設定(Standalone運用は可能か)
- デグレーデッドオペレーション
  - サイバー攻撃による異常動作も想定
    - 担当者が張り付いてでも運用
    - 後で巻き戻し作業が入っても業務継続
    - 緊急停止機能の確認
    - 代替手段の確保





判断基準・手順のマニュアル化

# 止めたくない情報システム

- 運用停止による影響大
  - 講義
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 情報システム停止も想定
    - 手動による業務継続
      - 手書き出席票
    - 情報取得を諦めるのもアリ
      - 全員出席とみなす

利用者の不利益回避

http://www.dailymail.co.uk/news/article-2194960/United-Airlines-Computers-passengers-given-handwritten-boarding-passes.html
https://tech.nikkeibp.co.jp/it/atcl/idg/14/481709/120100278/?ST=cio-security&P=2

# 止めるしかない情報システム

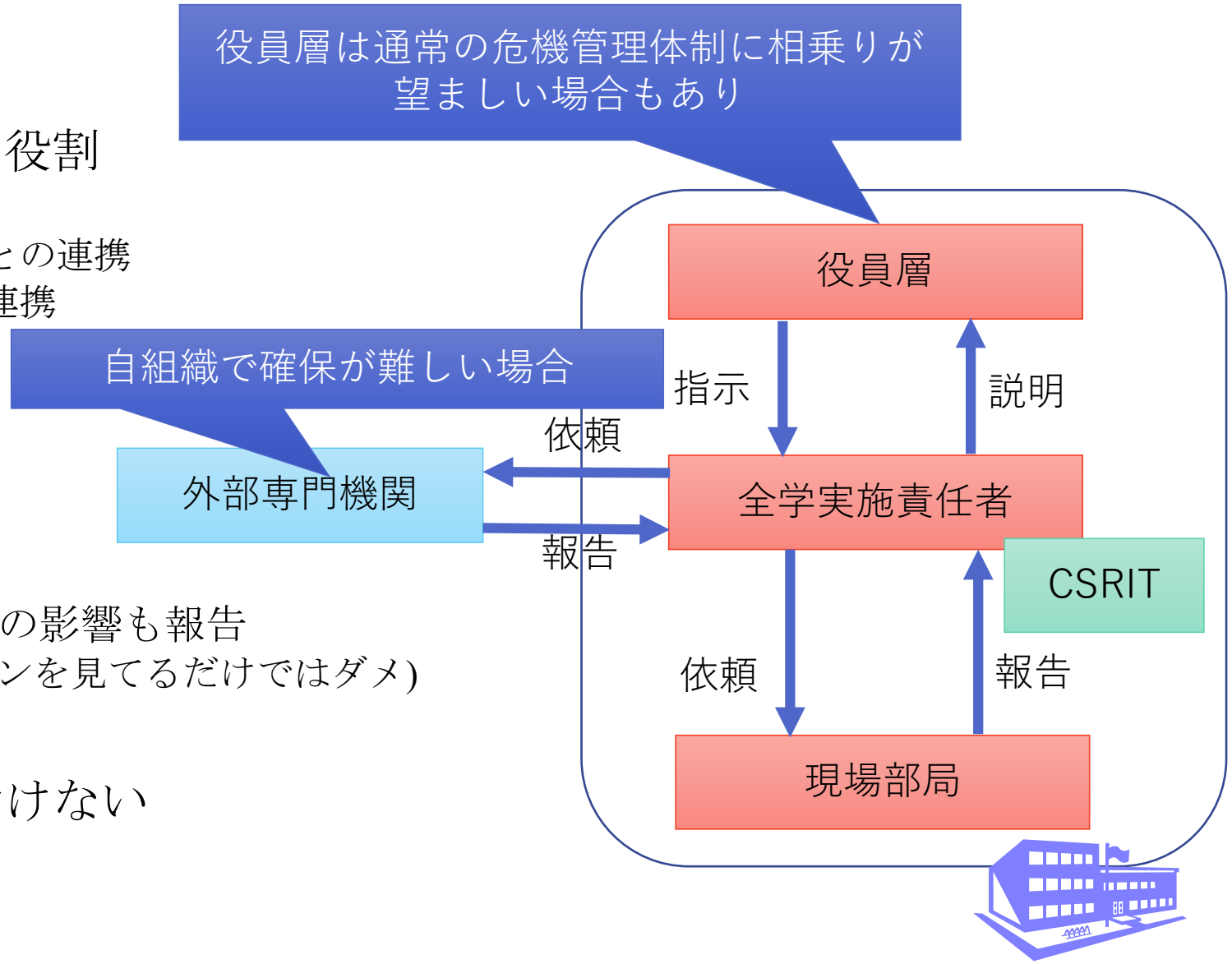
- 代替手段がない
- 手動操作は不可能
  - Single Point of Failure(SPF)の存在を把握
    - 経営陣が知っていることが重要
    - 現場判断で停止させないことがベスト
- ダメージコントロール
  - システム停止の影響範囲を極小化
- デグレーデッドオペレーション
  - 多くの場合重要システムなので…

SPFは極力回避


https://toyokeizai.net/articles/-/39544
https://ja.wikipedia.org/wiki/コンテナ#/media/File:Unloading_JAL_747.jpg

# 戦略マネージメント層の育成

- 全学実施責任者
  - 戦略マネージメントとしての役割
    - 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
      - アクシデント化を阻止
- 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



# 今後…本当に欲しい人材は

## ■おそらく技術だけのエンジニアは不要となる

- 今後数年間は…
  - SOCへの外注が進む…次期NII-SOCSの雲行きが…
  - セキュリティマネージメント層
    - ネットワークとセキュリティに詳しくなくてもよい
    - インシデント/アクシデントがBCPに及ぼす規模を想定できることが重要

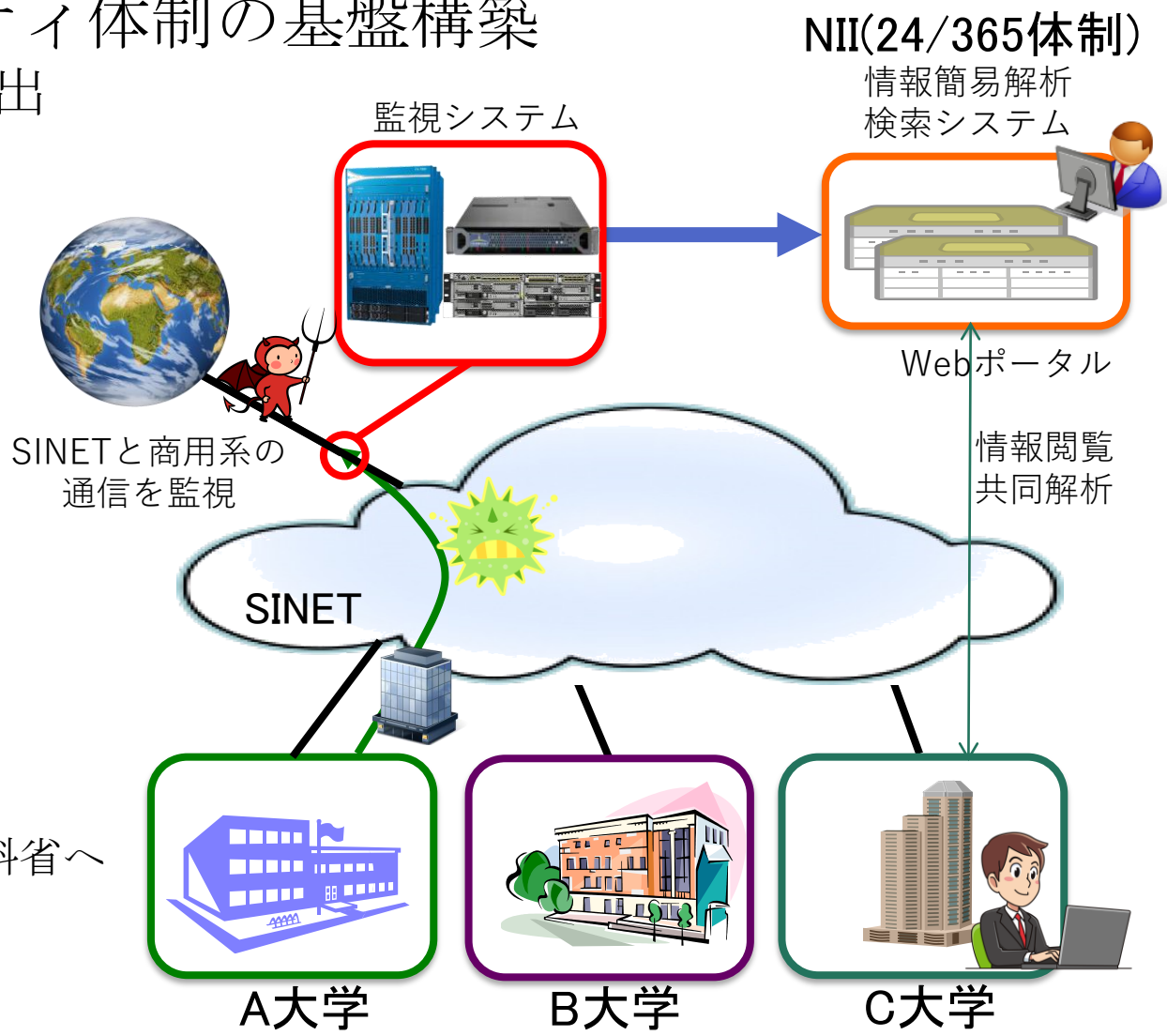
パソコン触ったことがない人でも務まる…

- 急速に進むAI化&自動化
  - 雑魚はAIが片付けてくれる
  - 自己免疫機構
    - 攻撃検知と同時に検知パターンや暫定パッチを自動生成

- それでも残る人による判断
  - 自動対処はあくまでも人が判断する時間を確保するため
  - 暫定パッチ提供の可否・タイミング

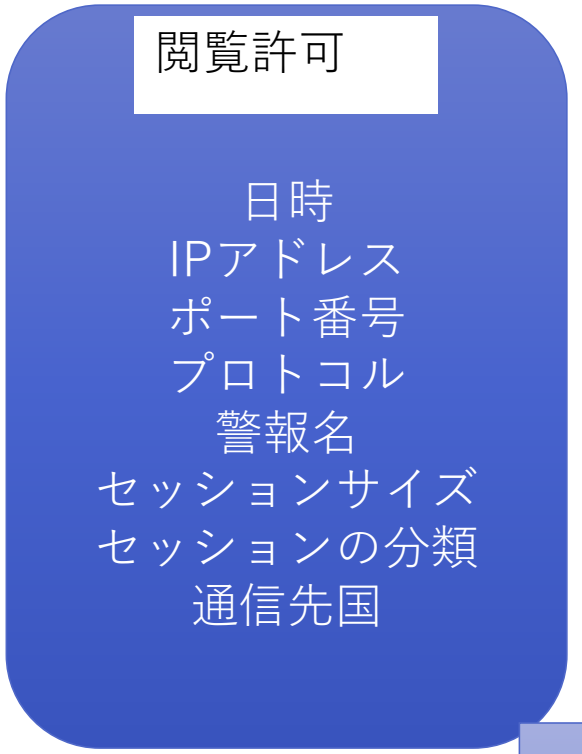
# NII-SOCSの構築と運用

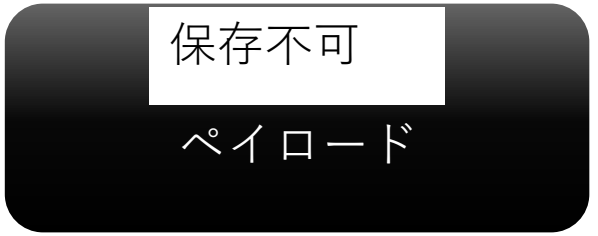
- 大学間連携に基づく情報セキュリティ体制の基盤構築
  - 国立大学法人等の運営費交付金から拠出
    - 7.8億(2016)、8億(2017)、8億(2018)
      - 2021までは継続の予定
  - 3種類の監視システム
    - Sandbox搭載IDS (paloalto)
    - シグネチャベースIDS (Cisco FirePower)
    - DNSトラフィック監視 (Damballa CSP)
  - 簡易解析システム＋Webポータル
    - 膨大な警報に緊急度・危険度の割付
  - 外部セキュリティ機関との情報共有
    - 国内：NDAに基づく攻撃情報の提供
      - 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

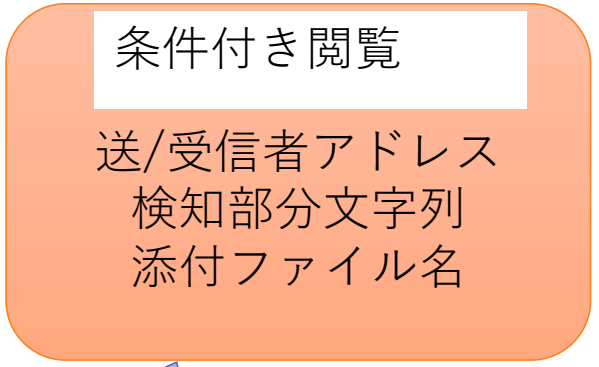


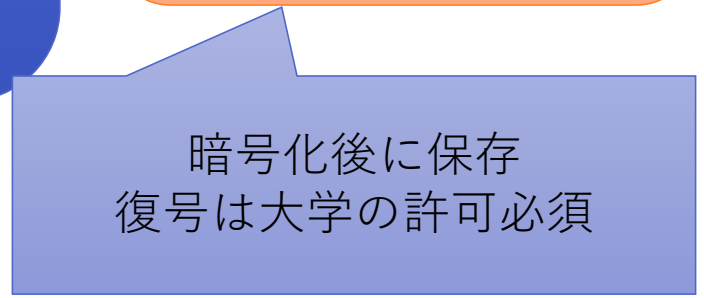
# NII-SOCSの制限

- 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



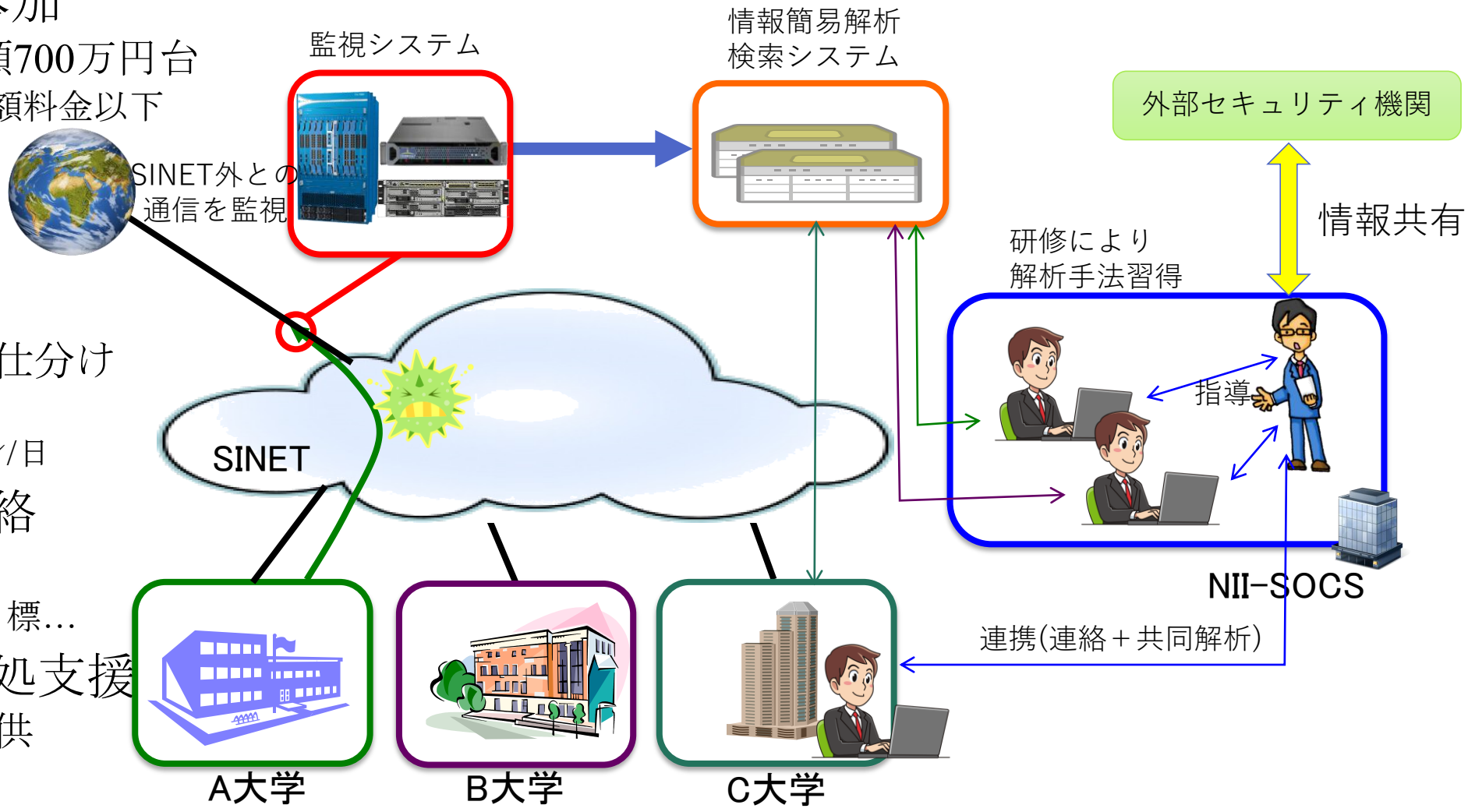



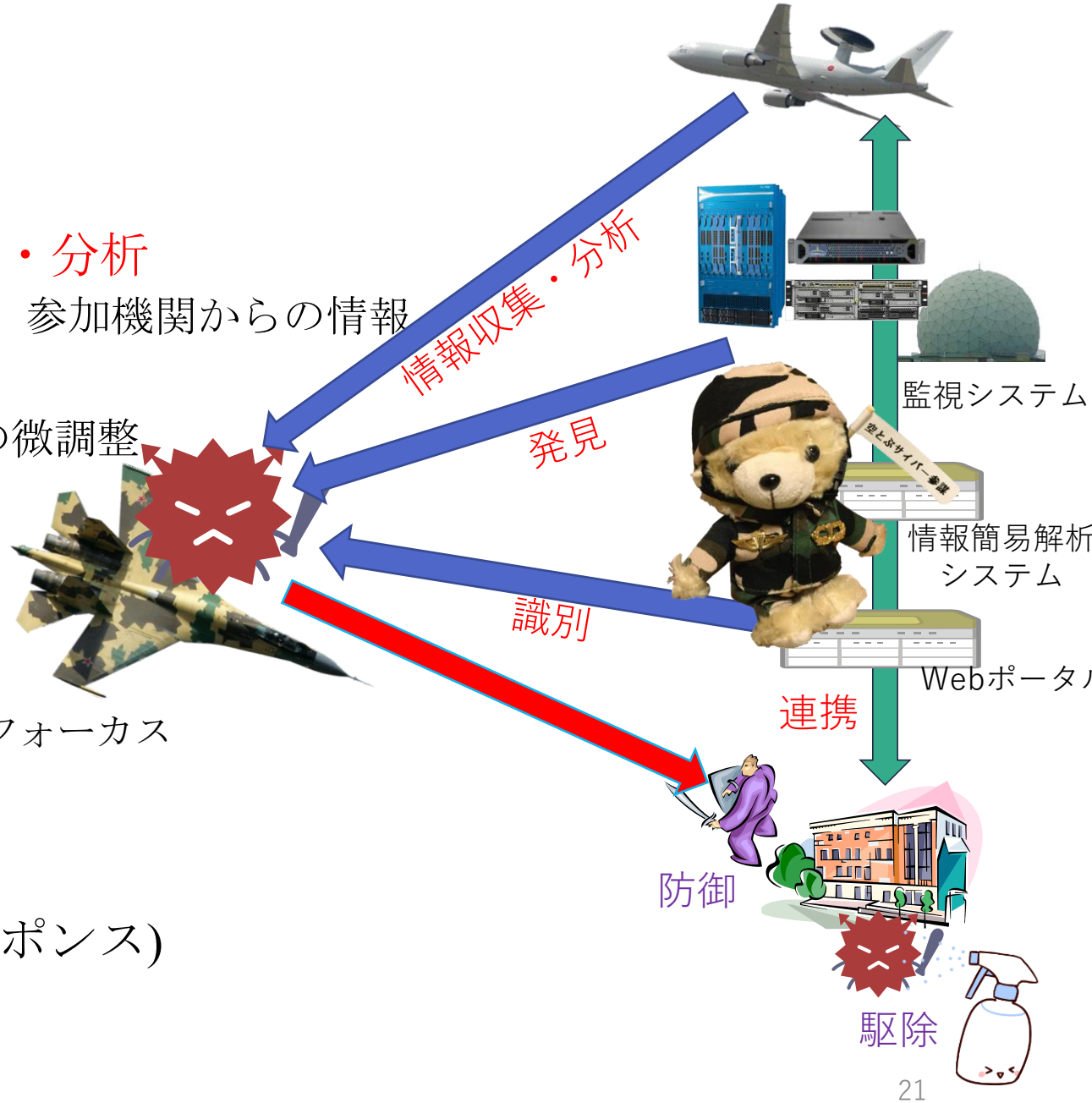
# NII-SOCSの仕組み

- 100機関以上の参加
  - 1機関あたり年額700万円台
    - 大手SOCの月額料金以下
- 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
- インシデント連絡
  - 大学へ連絡
    - 週1件程度を目標…
- アクシデント対処支援
  - 必要な情報の提供



# NII-SOCSの作業の流れ

- サイバー攻撃への初動対応
  - 早期警戒情報(インディケータ)の収集・分析
    - 国内・国外のセキュリティ機関、民間、参加機関からの情報
  - サイバー攻撃の発見
    - IDS、サンドボックス、ハニーポットの微調整
  - サイバー攻撃の目標と脅威度の識別
    - 各種情報との照合
    - 攻撃先の分布状況や攻撃手法の解析
    - 被害推定
      - Zero Day攻撃など被害が大きいものにフォーカス
  - 参加機関と連携
- 参加機関
  - 現場対応(予防措置/インシデントレスポンス)
    - 防御や駆除



# 主な仕事は情報の入手

- 国内外のセキュリティ機関との連携
  - Sinkholeの分布状況
    - アクセス状況(マルウェア感染の特定)
  - Honeypot/darknetの分布情報
    - ノイズ情報の削除
  - Scannerの分布情報
    - 探査活動の追跡
- 探査活動の監視
  - ShodanやRapid7による探索活動
    - 日によって大きく偏る。
      - 思ったより少ないメジャープロトコル…すでに探索済みだし…
      - 何かを探している…誰が？
    - 深掘り探索もある
      - バージョン番号や設定などを確認…なぜ知りたい？

| 回数 | ポート番号／プロトコル |
|---|---|
| 639317 | 81/tcp |
| 638848 | 102/tcp |
| 637993 | 444/tcp |
| 637040 | 2222/tcp |
| 636701 | 82/tcp |
| 636534 | 9000/tcp |
| 636482 | 6666/tcp |
| 358167 | 80/tcp |
| 351648 | 443/tcp |
| 345561 | 53/udp |
| 324982 | 8080/tcp |
| 320330 | 3749/tcp |
| 320149 | 25/tcp |
| 320007 | 4782/tcp |

# 公開情報の入手

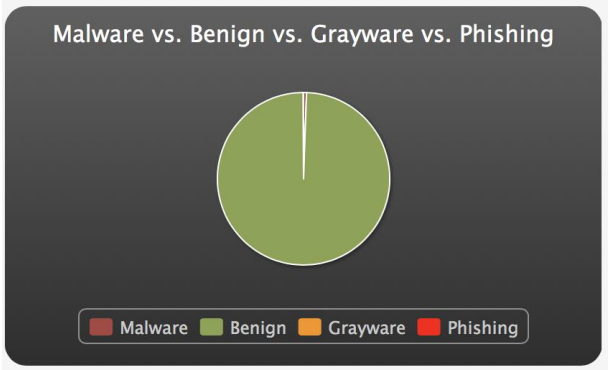
- SNS(関係者のtweet)
- サイバーに関わるニュース
  - 今は仮想通貨が旬

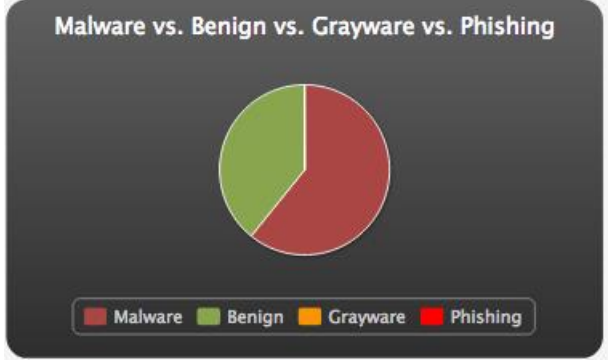
https://jp.reuters.com/article/china-bitcoin-idJPKBN1F50PH

http://nakayoshi-togi.com/post/1466

# NII-SOCSの運用実績

- いかに絞り込むか?
  - 膨大なデータ
    - 60万警報/日
    - 6億セッション/日
- 概ね30分以内の通知
- 9割を占める
  - マルウェア系
    - 半自動処理
- 残り1割
  - 絞り込み
  - 目視による監視

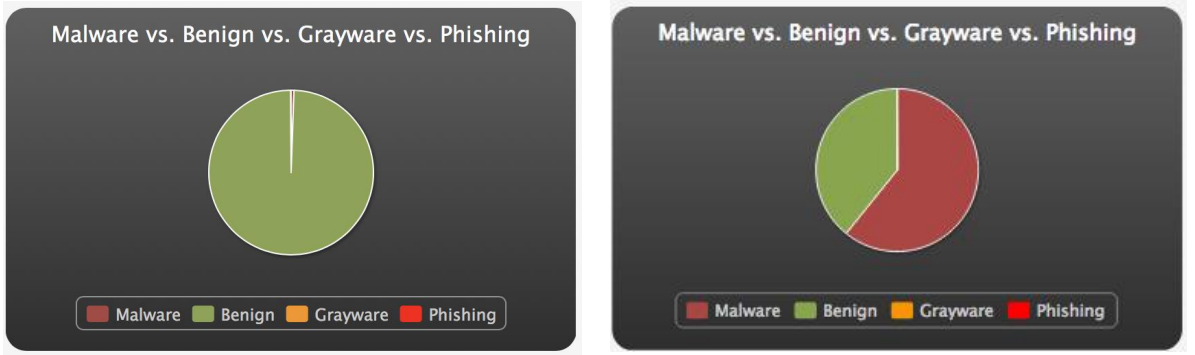



| 中項目 | | 累計 (2018/4/1~9月末) |
|---|---|---|
| 通知件数 | | 3617 |
| | 分類１：マルウェア感染の可能性 | 2760 |
| | 分類２：アプリケーションソフトの脆弱性によるもの | 225 |
| | 分類３：C&Cサーバーとの実通信の可能性 | 480 |
| | 分類４：ブルートフォース攻撃の可能性 | 0 |
| | 分類５：辞書攻撃の可能性 | 0 |
| | 分類６：標的型サーバー攻撃に関与している可能性 | 0 |
| | 分類７：man-in-the-middle 攻撃 | 0 |
| | 分類８：DNS Amp 攻撃への参加 | 0 |
| | 分類９：その他 | 152 |
| 誤報件数 | | 2 |

# 使える手を駆使する攻撃者

- バラマキ型攻撃の減少
  - メール添付・水飲み場型
    - ともに減少傾向
    - 来るときは大挙して来るが…
      - Sandbox検知で90%以上は数分で対応
        - Reputationによる通信ブロック
        - AVの検知パターン生成
          - ユーザが開封する前に間に合えば…
- コスパを重視した攻撃へ移行
  - ファイル共有サービスの活用など
    - よく考えたら不自然ではあるのだが…
      - Reputationでのブロックは困難
      - httpsはトラフィック監視では検知不能
      - 検知パターンの生成も困難




通常期 v.s. 繁忙期 (1時間あたりの割合)
NII-SOCSでの観測事例

〇〇委員各位

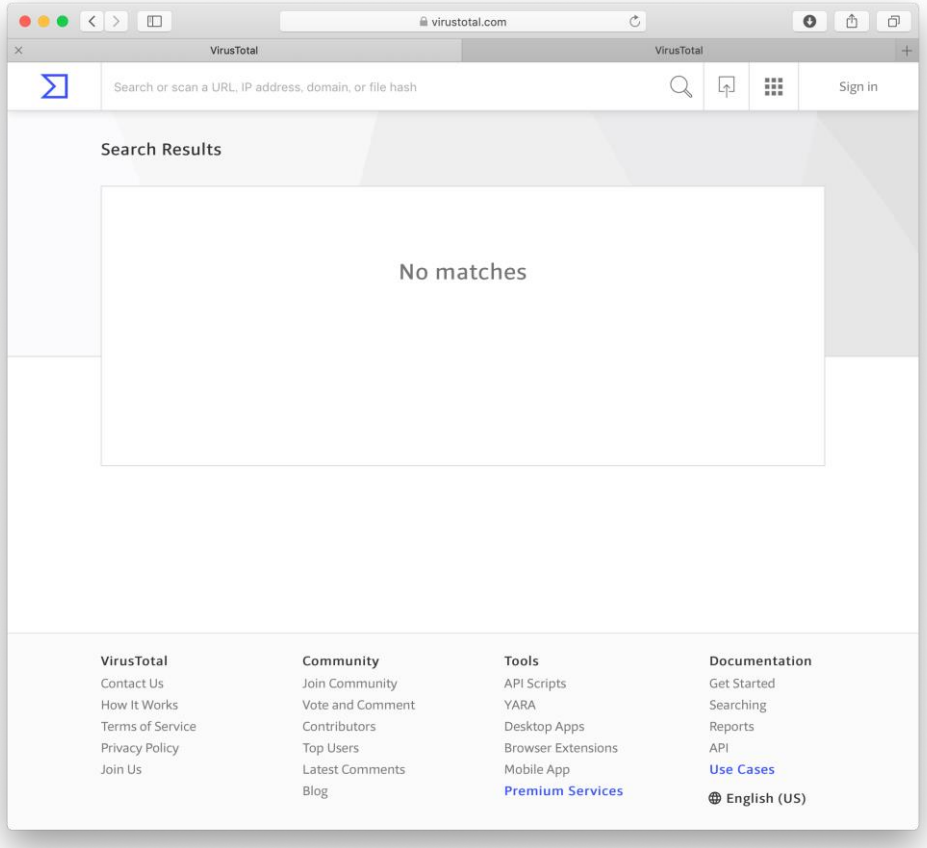
平成30年度の方針については、dr●pboxのファイルをご確認いただきますようお願い申し上げます。
https://www.dr●pbox.com/**********

ご不明な点がございましたら、当方までご連絡ください。

〇〇省 〇〇局….
〒100 - xxxx 東京都千代田区霞が関x-x-x
電話: 03-xxxx-xxxx

# NII-SOCSの運用方針

- 最近の攻撃のみ監視
  - 古い脆弱性を狙った攻撃
    - 情報収集目的での検知
      - 古い攻撃の大量発生→未知攻撃の可能性
- マルウェア
  - Sandboxによる検知
    - 通知は大手セキュリティソフト未検知のもののみ
      - 伝えられるのはハッシュ値のみ
      - 来年度からはマルウェア検体の提供も開始するが…
        - 懸念されるVirusTotalへの脊髄反射upload
- よくある誤対応
  - セキュリティソフトで検知されませんでした
    - それは当然
  - なので被害なしと判断します
    - それは大丈夫か？




一定期間経過観察
異常検知→再通知

# 挙動の違いによる被害推定

- 追加ダウンロードの可能性あり
  - 関係機関へ通知

| Date | Src IP | Dst IP | Src Port | Dst Port | Protocol | Sent(byte) | Rec. (byte) | Src Country | Dst Country |
|---|---|---|---|---|---|---|---|---|---|
| 2018/5/◯ 09:19:28 | A.B.C.D | W.X.Y.Z | 49940 | 80 | tcp | 2283 | 353460 | Japan | Russian Federation |
| 2018/5/◯ 18:26:14 | E.F.G.H | W.X.Y.Z | 64464 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 19:07:37 | E.F.G.H | W.X.Y.Z | 50368 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 16:53:14 | E.F.G.H | W.X.Y.Z | 58072 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 17:45:15 | E.F.G.H | W.X.Y.Z | 61838 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 18:15:39 | E.F.G.H | W.X.Y.Z | 64279 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 19:59:12 | E.F.G.H | W.X.Y.Z | 53316 | 80 | tcp | 1154 | 23532 | Japan | Russian Federation |
| 2018/5/◯ 16:41:48 | E.F.G.H | W.X.Y.Z | 57399 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |
| 2018/5/◯ 18:04:36 | I.J.K.L | W.X.Y.Z | 63829 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |
| 2018/5/◯ 19:37:44 | I.J.K.L | W.X.Y.Z | 52110 | 80 | tcp | 307 | 14466 | Japan | Russian Federation |

# 最も警戒するもの…見えない被害の発生

- 検知パターンなし
  - 6億セッション/日から不審な動きを特定

大学側

スキャン

特定不能

| 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 | | |
| A.A.A.74 | G.G.G.235 | incomplete | 62127 | 25 | tcp | 10179 | 0 | | |
| A.A.A.74 | H.H.H.26 | incomplete | 2843 | 25 | tcp | 19097 | 0 | | |
| C.C.C.75 | A.A.A.74 | smtp | 2742 | 25 | tcp | 608 | 1012 | | |
| D.D.D.39 | A.A.A.74 | incomplete | 16068 | 22 | tcp | 60 | 0 | | |
| F.F.F.179 | A.A.A.74 | incomplete | 18891 | 23 | tcp | 60 | 0 | | |
| A.A.A.74 | I.I.I.6 | incomplete | 28576 | 25 | tcp | 402 | 0 | | |
| A.A.A.74 | I.I.I.6 | incomplete | 28576 | 25 | tcp | 60 | 0 | | |
| A.A.A.74 | J.J.J.29 | smtp | 55684 | 25 | tcp | 13693 | 1606 | | |
| A.A.A.74 | K.K.K.83 | incomplete | 17520 | 25 | tcp | 402 | 0 | | |
| A.A.A.74 | I.I.I.6 | incomplete | 28576 | 25 | tcp | 60 | 0 | | |
| A.A.A.74 | K.K.K.83 | incomplete | 17520 | 25 | tcp | 60 | 0 | | |
| A.A.A.74 | K.K.K.83 | incomplete | 17520 | 25 | tcp | 60 | 0 | | |

NII-SOCSのサンドボックスにおいて、他機関のマルウェア受信を検知し、

https://www.virustotal.com/ja/file/a8

のマルウェアもしくはその亜種による通信先を把握しました。これを元に調査したところ、以下の接続試行を確認しました。

セッションID：

また、貴学側IPアドレスに関して以下の期間

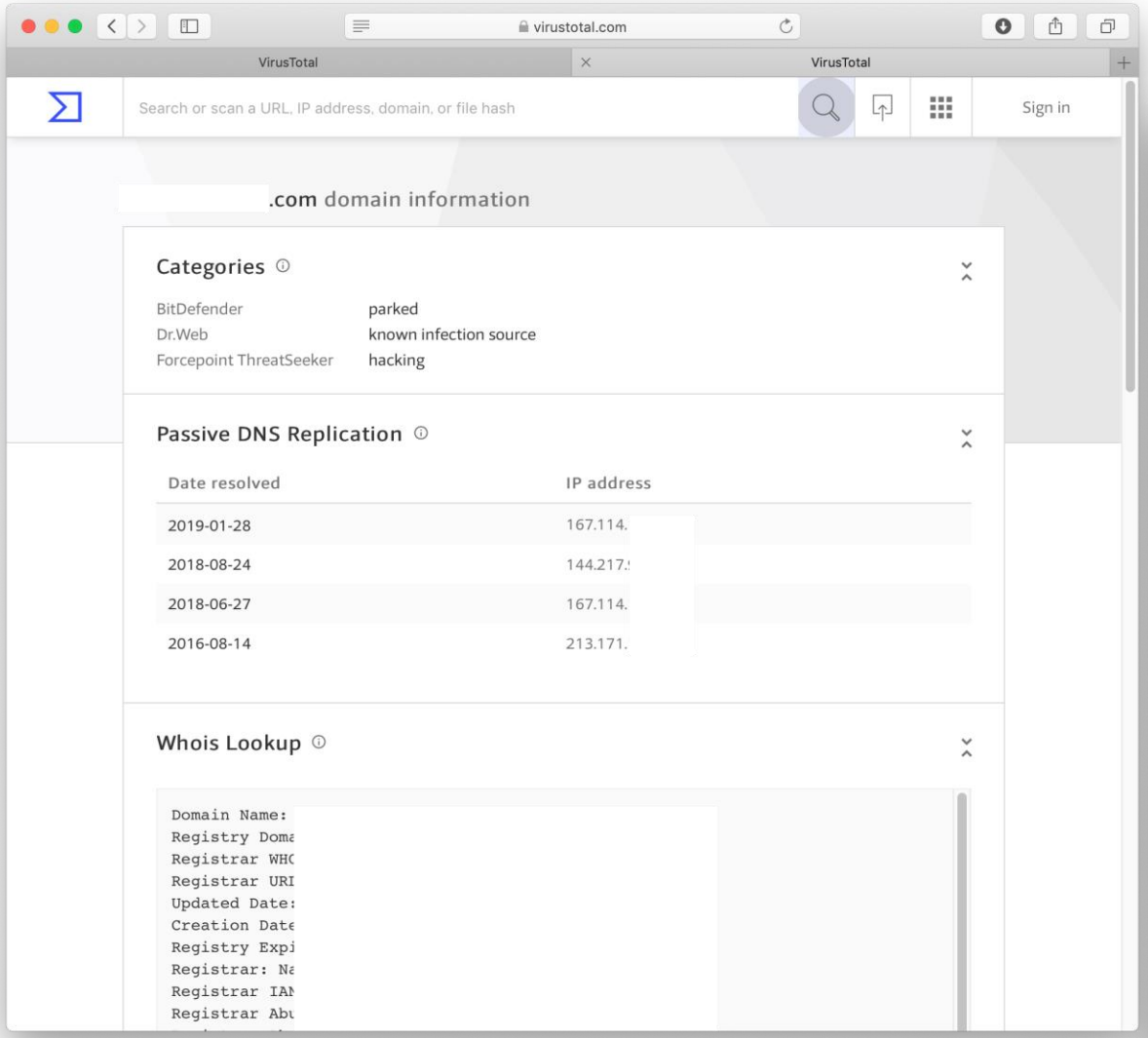
2017 - 2017

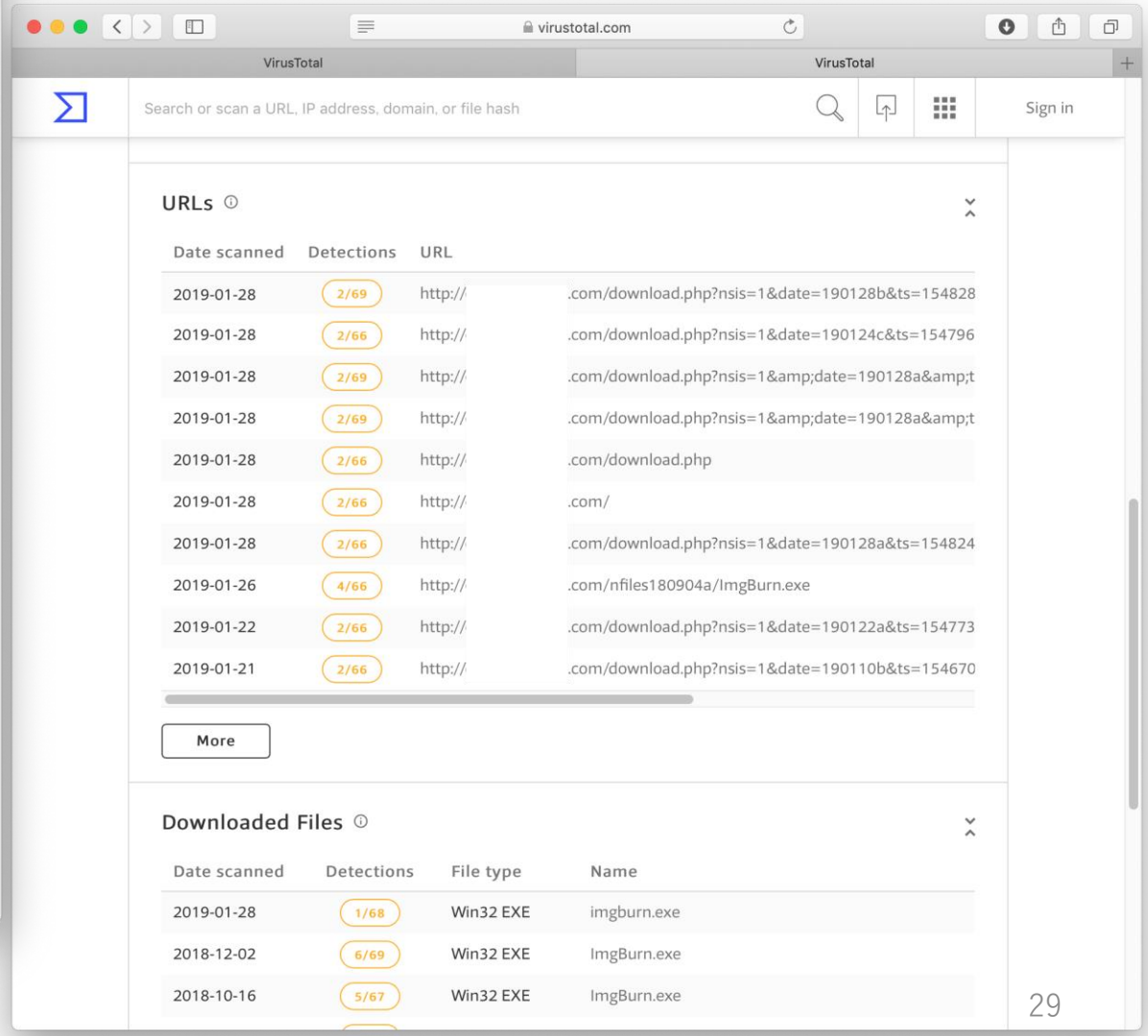
のセッションを確認したところ、問題となる通信先以降に、imcompleteの中に、セッション不成立にも関わらず一方的にパケットを送信し続けている現象、および、送信バイト数と送信パケット数の比較から、正規のSYNパケットにしては1パケットあたりの送信バイト数が大きいと思われるものが観測されています。

このため、お手数をおかけしますが、上記時間帯に接続ができないWebサイトへのアクセスを繰り返したか、当該機器の利用者に確認をいただけませんでしょうか？

Tor通信か？ 25/tcpで？

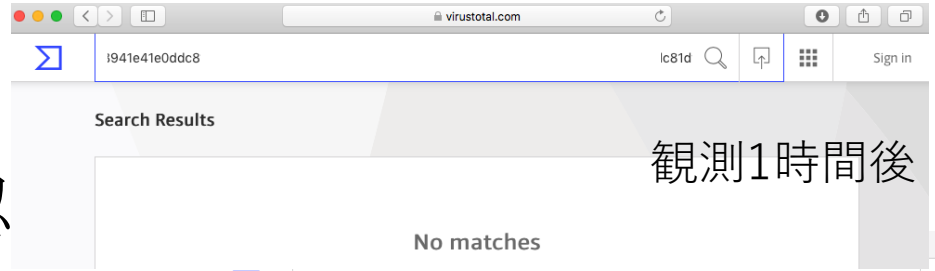
# 配布元ドメインを調査

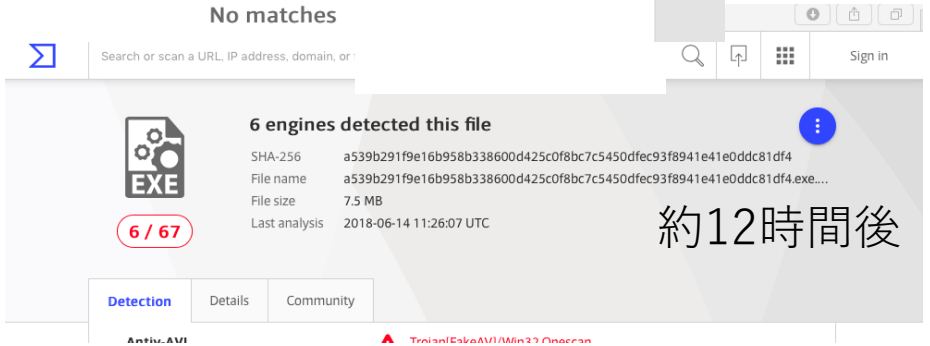

virustotal.com
VirusTotal
VirusTotal
Search or scan a URL, IP address, domain, or file hash
Sign in
.com domain information
Categories
BitDefender parked
Dr.Web known infection source
Forcepoint ThreatSeeker hacking
Passive DNS Replication
Date resolved IP address
2019-01-28 167.114.
2018-08-24 144.217.
2018-06-27 167.114.
2016-08-14 213.171.
Whois Lookup
Domain Name:
Registry Doma
Registrar WHO
Registrar URI
Updated Date:
Creation Date
Registry Expi
Registrar: Na
Registrar IAN
Registrar Abu

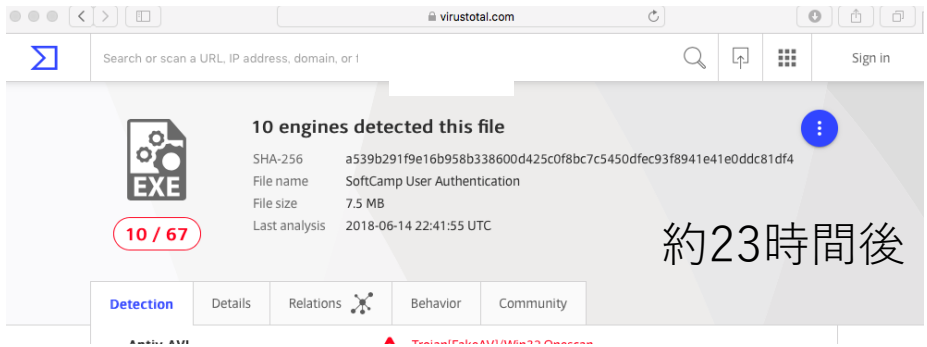

virustotal.com
VirusTotal
VirusTotal
Search or scan a URL, IP address, domain, or file hash
Sign in
URLs
Date scanned Detections URL
2019-01-28 2/69 http:// .com/download.php?nsis=1&date=190128b&ts=154828
2019-01-28 2/66 http:// .com/download.php?nsis=1&date=190124c&ts=154796
2019-01-28 2/69 http:// .com/download.php?nsis=1&date=190128a&t
2019-01-28 2/69 http:// .com/download.php?nsis=1&date=190128a&t
2019-01-28 2/66 http:// .com/download.php
2019-01-28 2/66 http:// .com/
2019-01-28 2/66 http:// .com/download.php?nsis=1&date=190128a&ts=154824
2019-01-26 4/66 http:// .com/nfiles180904a/ImgBurn.exe
2019-01-22 2/66 http:// .com/download.php?nsis=1&date=190122a&ts=154773
2019-01-21 2/66 http:// .com/download.php?nsis=1&date=190110b&ts=154670
More
Downloaded Files
Date scanned Detections File type Name
2019-01-28 1/68 Win32 EXE imgburn.exe
2018-12-02 6/69 Win32 EXE ImgBurn.exe
2018-10-16 5/67 Win32 EXE ImgBurn.exe

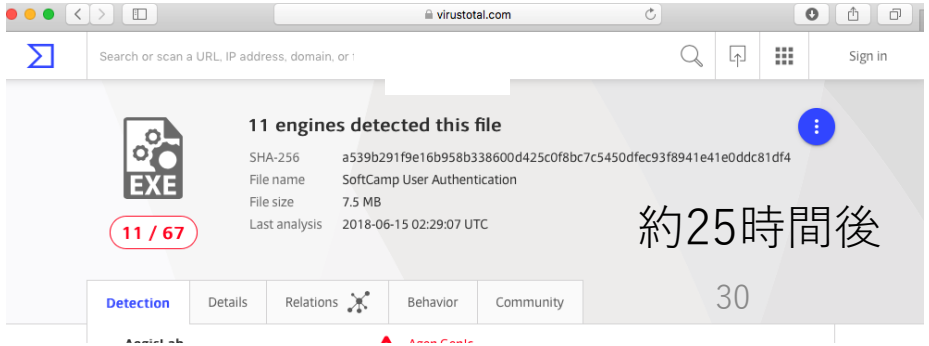
# 標的型攻撃への事例

- NII-SOCSで数名にのみ着弾確認
  - 月に数度は観測
- 採取時は未知マルウェア
  - 検知AV 0は当たり前
    - そもそもサンプルとして上がっていない
- 半日程度で検知が始まるが…
  - サンプルファイルを提供したのは誰か？
    - サンプルがなければ検知パターンが作れない
- 遅々として向上しない検知カバー率
  - 1件のみのサンプル提供
  - 各社サンドボックスからのアクセス回避
    - 緊急度と悪性度の判断しにくい



# 用心深い攻撃者との心理戦

- 攻撃メール送信から数時間はC2サーバ不在
  - ドメイン名解決不能、404エラーなど
    - セキュリティ製品の先読みチェックを回避？
    - 感染マシンからの接続試行は継続するので問題はない
- マルウェア提供先を選別
  - 特定のIPアドレス以外からのアクセス
    - ファイル提供せず
      - 大手セキュリティベンダー/攻撃対象組織のsandboxのIPアドレスを把握
  - 想定IPアドレスからのアクセス
    - マルウェア提供
    - 数回のアクセス後はファイル消去
      - 防御側の追跡を振り切る？
- 断片的な情報から攻撃者の意図を推定

# まとめ

- 日々進化するサイバー攻撃
  - 手口のステルス化、被害の深刻化
- 高等教育機関の悩み
  - 多種多様な情報機器・制御機器が混在
    - 近未来のIoT環境なのかもしれない
- エリートパニックをいかに防ぐか？
  - 出口戦略を見据えた籠城戦の必要性
  - AICという考え方へ移行
  - そのためのサイバーセキュリティマネージメント層育成
- NII-SOCSの実事例
  - 技術的な判断はNII-SOCS
  - 経営判断は各機関

] サイバー攻撃対処自動化を見据えた人材育成