世界規模で展開されるサイバー攻撃を見据えた新たな対策運用

高倉弘喜
国立情報学研究所

今回の内容

- 変化しない・するサイバー環境
- 長期戦化するサイバー攻撃対処
- 道具マニアからの脱却と相手側戦略の見定め
- 想定すべき見えない状況
- 今後の人材育成

変化しないサイバー環境

- 情報機器の長寿命化
  - 現在も現役で活躍中のWindows XP

制御システムの1ユニット

http://www.comparestoreprices.co.uk/coffee-makers/jura-impressa-f90-bean-to-cup-machine.asp

長寿命化による副作用

- 桁あふれ問題
  - 常時電源onの想定漏れ？
  - WiFi保守などの新技術導入の副作用？
- 常時通電のIoT機器
  - 新たに見つかる桁あふれ問題
  - バグの蓄積
- 先を見越したUpdate計画
  - いつもの更新ができない？

    不具合発生を予備回避

B787のPFDでの
GPS rollover

ボーイング７８７型機、248日継続通電で電力停止の恐れ＝米当局

2015年 05月 1日 09:51 JST

記事を印刷する | ブックマーク | 1ページに表示

おすすめ 408 ツイート 693 チェック 1 +1 15

1 of 1 [Full Size]

トップニュース

- 6年ぶり国共トップ会談、習総書記は中台の対等な対話呼び掛け

［３０日　ロイター］ - 米連邦航空局（ＦＡＡ）は、航空機大手ボーイング(BA.N: 株価, 企業情報, レポート)の７８７型機を運航する航空会社に対し電力系統のスイッチを定期的に切るよう指示すると明らかにした。７８７型機は２４８日間継続して通電されると、出力調整装置が発電機を停止する可能性があるという。

ＦＡＡは、急に電力が停止した場合、航空機が制御不能になる危険があると説明した。

http://jp.reuters.com/article/topNews/idJPKBN0NM2Y420150501

https://twitter.com/ChinaAvReview/status/1114802018919411712

「隔離NWは大丈夫」神話

- 外界とのデータ交換は必要
  - 重要なデータほど外部で利活用
    - ストレージの肥やしデータは不要
  - 定期保守
- セキュリティソフトの限界
  - 検知パターン数の制限
    - 現実的な検査時間の確保
    - アプライアンスの場合
      - CPU、メモリ、ストレージ
  - 古いマルウェアは検知対象外
    - イマドキそ感染するPCは居ない
    - 隔離NW内の情報機器は？？？

TOP > セキュリティ > サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を...

セキュリティ

関連カテゴリー： マネジメント

サンフランシスコ市交通局、ランサムウエア攻撃を受けて地下鉄を無料に

2016/12/01

シェア 0 ツイート

John Ribeiro IDG News Service

同交通局のシステムがランサムウエアの攻撃を受けたのは11月25日からだった。報道によると、駅に設置されたコンピューターの画面には、「You Hacked, ALL Data Encrypted（お前をハッキングし、すべてのデータを暗号化した）」というメッセージが表示された。

交通局は、パートナー企業の米Cubic Transportation Systemsの協力のもと、念のための措置として、市営地下鉄の駅で券売機と自動改札口を11月25日から27日朝まで停止した。結果的に、この間は無料で地下鉄に乗ることができた。

https://tech.nikkeibp.co.jp/it/atcl/idg/14/481709/120100278/?ST=cio-security&P=2

変化するサイバー環境

- 5Gなどの次世代無線通信規格
  - 回線の物理距離が伝送遅延に大きく影響
    - モバイル端末–基地局間：短い遅延(数十μs)
    - 基地局–サーバ間：極めて長い遅延(数十ms)
  - 通信成立後の高速化手法は数多く存在
    - 通信成立直後の伝送遅延の短縮は困難
    - ミッションクリティカルな環境では使いにくい
- Fog/Edgeコンピューティング
  - もちろんCloudコンピューティングとの併用
  - 街角に置かれるFog/Edgeシステム
    - 物理セキュリティの問題
      - 盗難→解析→クローンや偽システム
  - SDNの活用
    - 通信がどこを通るのかわからない

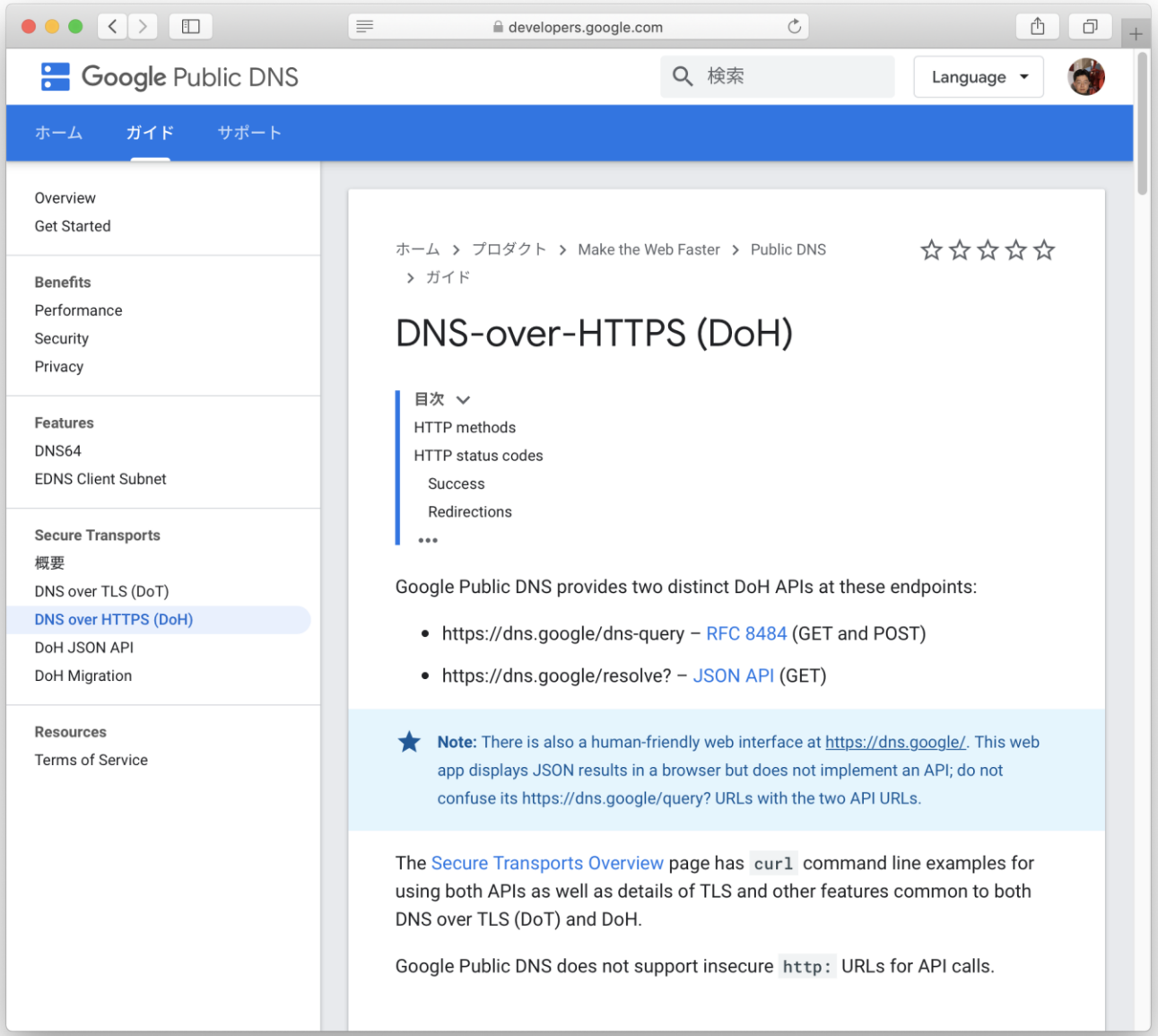
もっとも…
部品転売が懸念
されるけど

変化するネットワーク環境

- 全人類https化へ
  - DNS over HTTPS(DoH)まで登場
  - 通信経路上でのDeep Packet Inspectionが困難に
- 新たな監視手法が必要に
  - MITM的手法で解決？
  - EDR(Endpoint Detection and Response)対応？

→いずれも監視に必要なコンピュータリソースが急増

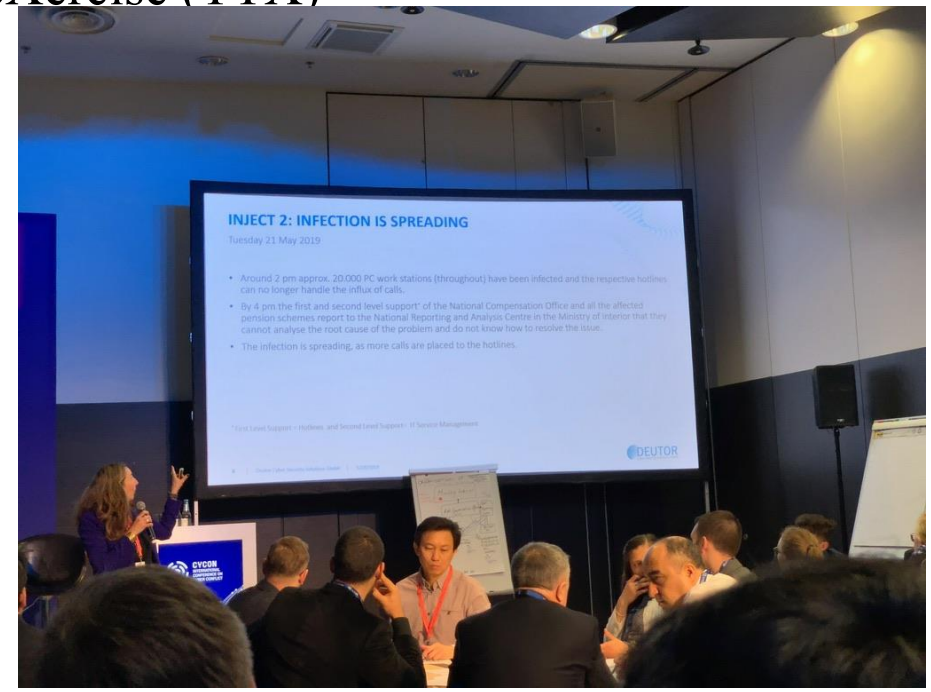
Endpointの全ログを解析するか？



https://developers.google.com/speed/public-dns/docs/doh

長期化する攻撃対処

- Cyber War Game: State-sponsored cyber-attack on a critical infrastructure
  - 2019年開催のCyCONのワークショップの一つ
    - モデレータ：Dr. Stefanie Frey and Michael Bartsch
    - 参加者：政府関係、重要インフラ事業者、法執行機関、IT企業、国際規模の企業、その他社内専門家
    - 1グループ6名程度で実施するTable Top eXercise (TTX)



演習の内容

- 基本情報：
  - 某国の人口、地理的位置、地政、軍事同盟、貿易関係、etc
    - 年金受給者の規模(海外在住者の割合)
    - 英文の3ページものの資料 (3～5分で概要理解)
- 状況開始：

5/20 0800

5/20 110 … 電話殺到

5/21 140

5/21 1000: 年金本部 内務員
未だ原
内務省

5/22 年
国家
年金支給(5/23)は不可能

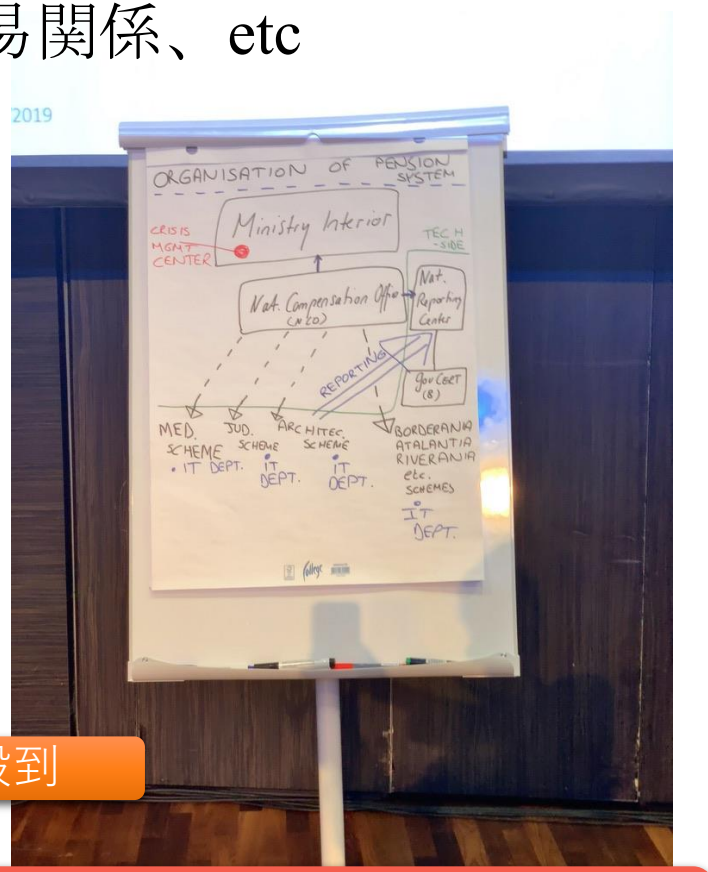
5/22 GovCERT発表
「障害」の要因不明・分析不能

5/24 マスコミ報道
年金システムでサイバー攻撃　179万人に影響

5/24 年金受給者の問い合わせ電話殺到

5/24 年金受給者@海外から大使館への問い合わせ殺到

5/26 Twitter
政府が保有電力株売却を検討してるらしい



5/26 電力株大暴落
直後、海外から大量買い注文

数日から数週間を要する初期対処

- 暫定情報からどこまでを想定するか？
  - 誤報の存在
  - 逐次入ってくる訂正情報
  - 炎上による副作用
- Influence operationの存在
  - 誰が何の目的で？
- 冷静沈着な初期対応
  - 必須となる人員交代
    - 連続する24時間勤務は不可能
- 適切かつ簡潔な引き継ぎ文書
  - 3～5分もの

わざと炎上させるのも作戦

- ダメージコントロールの一つ
  - 世間の注目を別のところに引きつける
  - 守りたいものは何か？
    - 情報機器やデータですか？
    - 運用ですか？
      - 早期の復旧ですか？
- 数ヶ月後にやってくる後始末
- 大炎上を回避できるか？
  - エリートパニックを誘発させない
  - うまく火消しができるか？

【独自】三菱電機にサイバー攻撃　防衛などの情報流出か

三菱電機 不正アクセス被害 個人情報や企業機密流出の可能性

2020年1月20日 10時50分　IT・ネット

重要な情報は流出していない

https://www.jiji.com/jc/d4?p=ssn141&d=d4_gra
https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html?fbclid=IwAR343j_338OvfPqNKaNL29X_Xe0q58YJcsvNW-yNBCvGc_9T2vwNX_OnzfE
https://www3.nhk.or.jp/news/html/20200120/k10012251691000.html?utm_int=news-new_contents_latest_relation_002

武器マニアからの脱却

ミリオタの品評会になってないか？

- Emotetによる大量攻撃

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

  - Wordファイルのため修正が容易
    - 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
  - 検知パターンの生成ができない→ユーザが開封してしまう

攻撃者の真の意図は？

- 本格的攻撃の前に監視系を潰すのは定石
  - Sandbox
    - GW型sandboxで解析
      - 直ちに新種マルウェアと判定
        - 内部への侵入をブロック
        - 検知パターンを生成→Endpoint Protectionに情報提供
          - 人が開封する間に駆除
      - 直ちにマルウェア判定できないものも存在
        - 着弾時にはC2未整備
        - Sandboxの解析回避
      - 数日間は繰り返し解析
        - マルウェア判定時に「一昨日のメール開くな」はできない
        - 被害発生の確認→被害範囲の特定→攻撃影響の封じ込め

一切機能しない

インフラへのサイバー攻撃

- ウクライナの電力会社で被害
  - 停電はした…
- けど現地では
  - それほどの騒ぎにならず
- 不安定な電力事情
  - 週に何度も停電
- ロシアとの紛争
  - サイバーだけじゃない妨害攻撃
  - 1960年代のインフラ by ソビエト
    - 裏口知り放題
    - アナログ通信(電波)での制御

NEWS 2017.07.27 THU 11:00

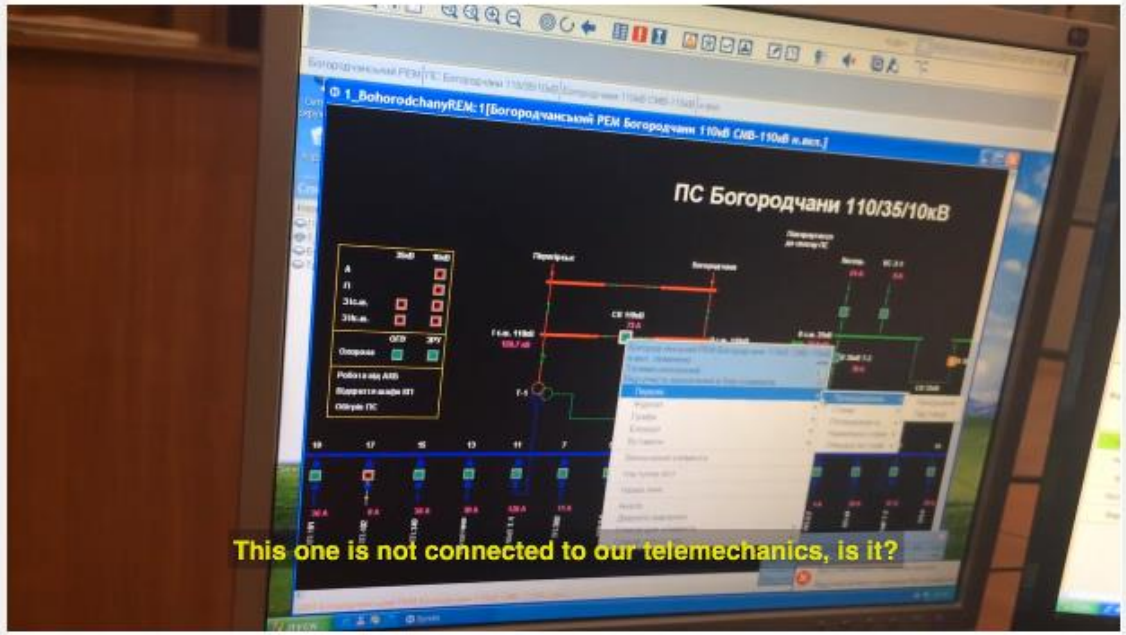
電力会社のPCがハッカーに乗っ取られる決定的瞬間――サイバー攻撃で大停電が起きたウクライナでカメラが捉えた（動画あり）

ウクライナで相次いでいるサイバー攻撃による停電。『WIRED』US版は、ハッカーが2015年に電力会社のパソコンに侵入し、遠隔操作する様子を捉えた映像を入手した。その恐るべき手口とは。

VIDEO BY WIRED US
TEXT BY ANDY GREENBERG
TRANSLATION BY HIROKI SAKAMOTO/GALILEO

WIRED(US)

ツイート いいね！ 803 シェア B! ブックマーク 55



https://wired.jp/2017/07/27/video-hackers-take-over-power-grid-computer/

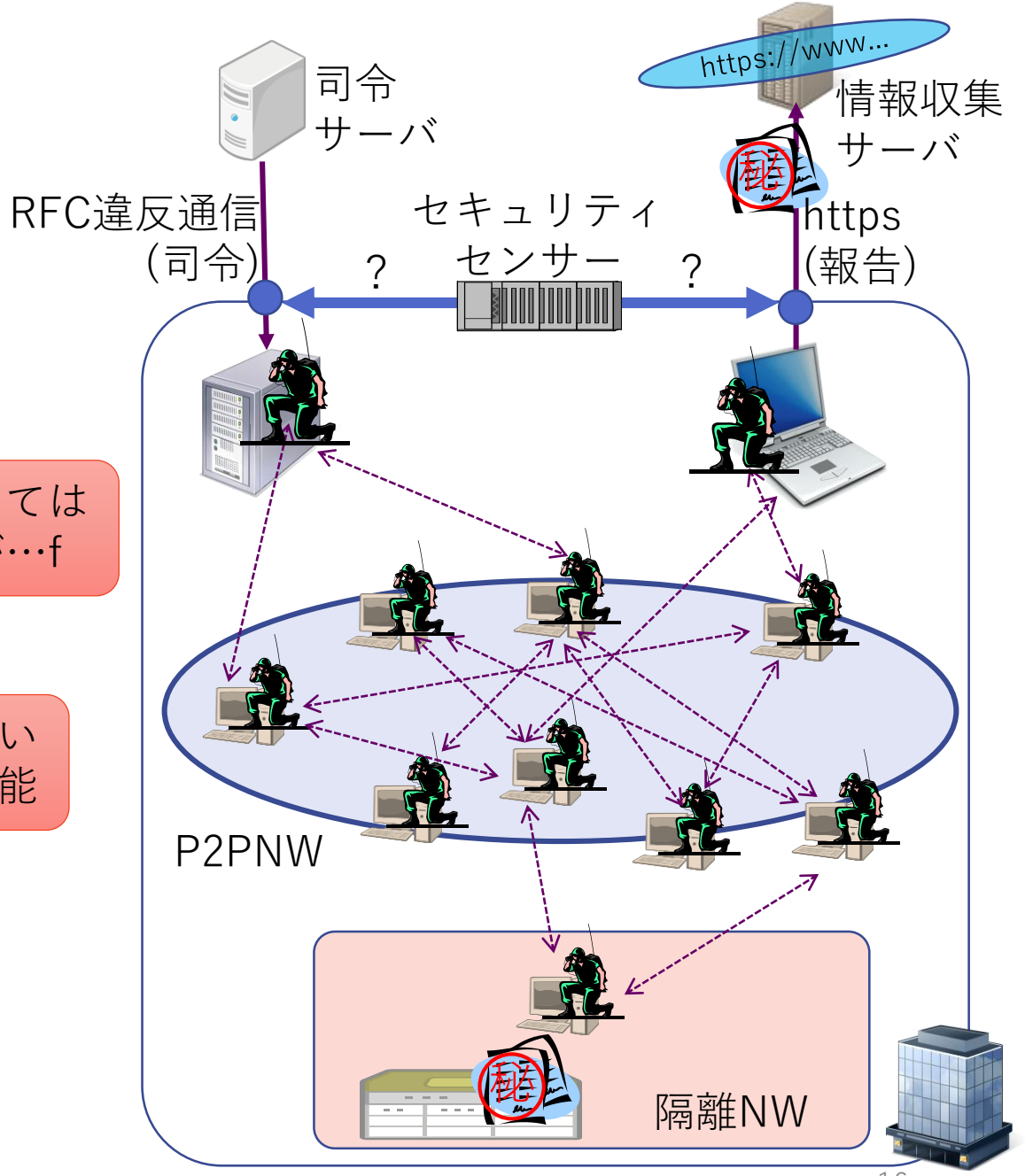
見えない攻撃を想定した対処

- Zero-day攻撃はもはや常識
  - セキュリティ侵害を想定した対応
- RFCを無視した通信
  - 例：SYNパケットのみ
    - 謎のペイロード存在
    - 通信不成立→センサーの監視対象外
- 暗号通信の活用
  - https, VPN, onion routing…
- 標的組織内の通信網を構築
  - 侵入成功後は直ちに横展開
  - P2Pを導入
    - 司令と報告が別経路

SYN floodとしては検知できるが…f

暗号を解かない限りは解析不能

内部NWの監視必要？



見えない被害の発生…セキュリティ製品の検知回避

■成立しない通信を使った情報流出

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	8	0
A.A.A.74	G.G.G.235	incomplete	62127	25	tcp	10179	0	23	0
A.A.A.74	H.H.H.26	incomplete	2843	25	tcp	19097	0	29	0
C.C.C.75	A.A.A.74	smtp	2742	25	tcp	608	1012	9	13
D.D.D.39	A.A.A.74	incomplete	16068	22	tcp	60	0	1	0
F.F.F.179	A.A.A.74	incomplete	18891	23	tcp	60	0	1	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	J.J.J.29	smtp	55684	25	tcp	13693	1606	25	17
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	402	0	6	0
A.A.A.74	I.I.I.6	incomplete	28576	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0
A.A.A.74	K.K.K.83	incomplete	17520	25	tcp	60	0	1	0

大学側

スキャン

特定不能

あり得ない
片方向通信

メール送信

Tor通信か？ 25/tcpで？

見えない攻撃を想定できないセキュリティ機器

- SYNを使った情報持ち出し
  - SYNパケットのみではセッション不成立
    - DPI実行せず
  - 毎秒数千パケットならSYN Floodで検知できるかも
    - イマドキSYN Flood検知してますか？
    - もちろん、毎分数パケットの低レート送信
- 防御側の手の内を知り尽くした攻撃者

RFC違反やんか！

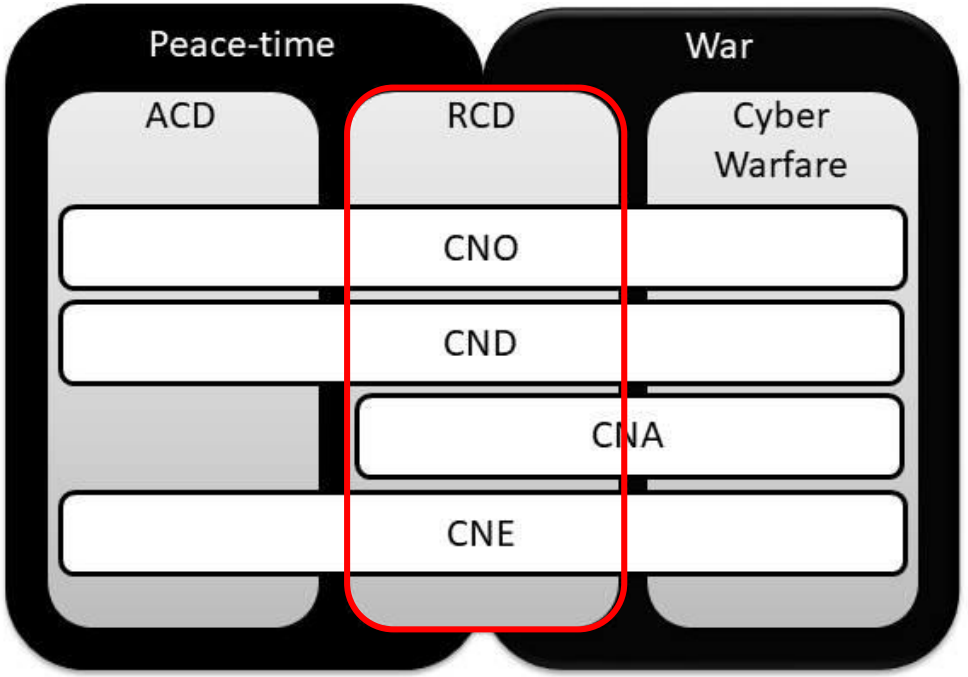
犯罪者が法律守るんだったら…

人材育成の方向性

- 存在しない平時と想定できない有事
  - グレーゾーン事態を想定
- Active Cyber DefenseからResilient Cyber Defenseへ　抗堪性のある防御
  - Computer Network Operation
  - Computer Network Defense
  - Computer Network Exploitation

  ＋Computer Network Attack
- 反撃の可能性を検討
  - ただし制限付き

ミリオタ的な発想ではあるが…



https://digi.lib.ttu.ee/i/?12015

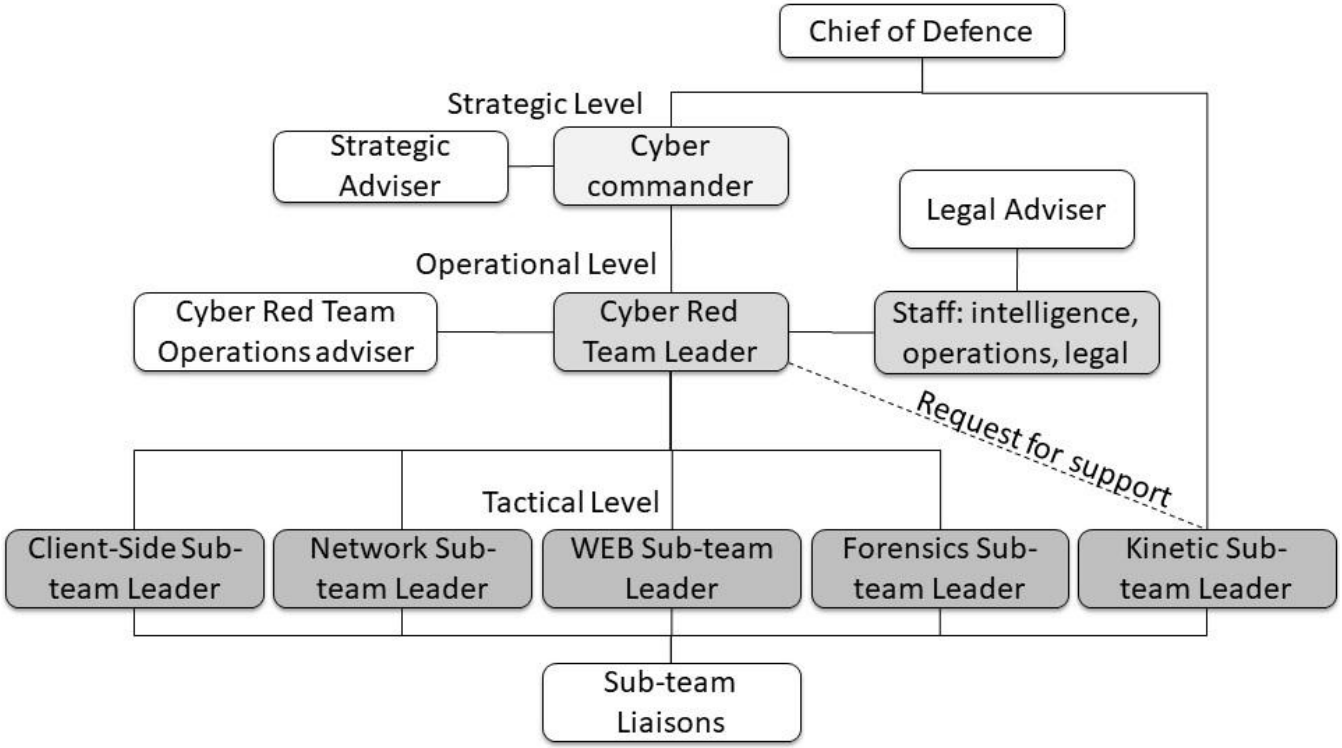
高度な攻撃対応

- 追い出してもすぐ戻ってくる
  - さらに進化して…下手すりゃステルス化して
  - 居ないのでなく見えていない可能性
    - 見えていた方が良いという考え方もある
- 可能であれば泳がせるという選択肢もある
  - 米国NIST SP800-61 rev.2 (3.3.1節)
    - Sandboxに誘導して攻撃者の挙動を観察
      - 攻撃者の背景、目的、技量を推測
  - 欺瞞攻撃(防御側による)　制限付き攻撃の例
    - Honeynetの活用
      - 攻撃を受けたネットワークを丸々再現 on VM
    - お土産(偽ドキュメントやビーコン付きドキュメント)を用意
      - 罠に気づくグループ or 間抜けなグループかの見極め

グレーゾーン事態を想定したRCD

重要なのはコミュ力

- サブチームによる作業の分担
  - 数名ずつの少数精鋭
  - それぞれ異なる目標設定
- サブチーム間の連携
  - チームリーダによる統括
  - リエゾンによる情報共有
- 必須の法律アドバイザ
  - 防御のためとはいえ法律遵守
- そのための訓練も
  - 教官向け訓練プログラム？



https://digi.lib.ttu.ee/i/?12015

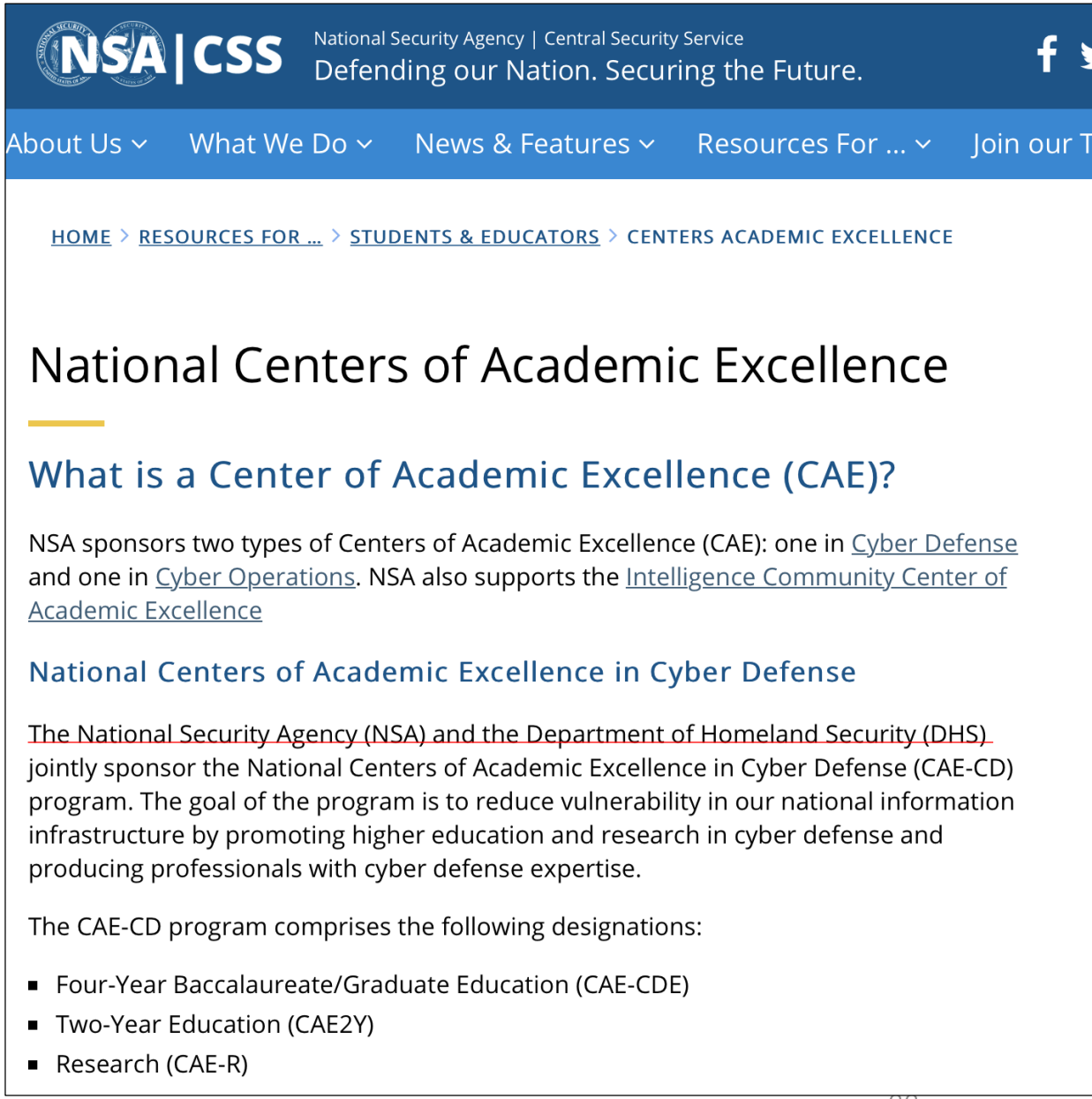
米国の状況

- 急速に進むNSAと連携する大学
  - Centers of Academic Excellence
    - Cyber Defense
      - NSAとDHSの共同スポンサー
    - Cyber Operations
      - NSAも支援するNICE

National Centers of Academic Excellence in Cyber Operations

NSA's CAE in Cyber Operations (CAE-CO) program supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation, and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation.

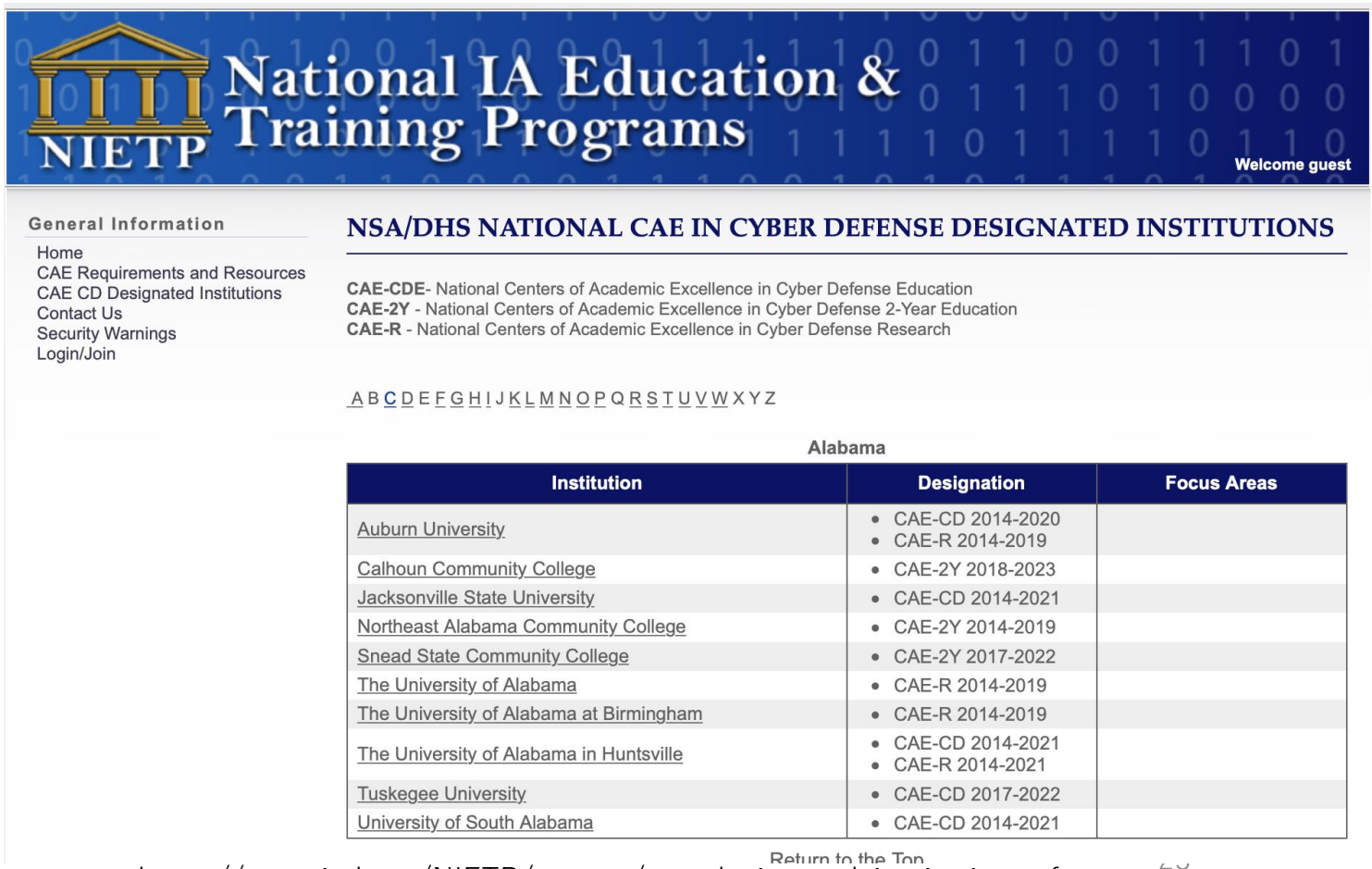
The CAE-CO program is a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.



https://www.nsa.gov/resources/students-educators/centers-academic-excellence/#defense

どんどん増加する参加大学

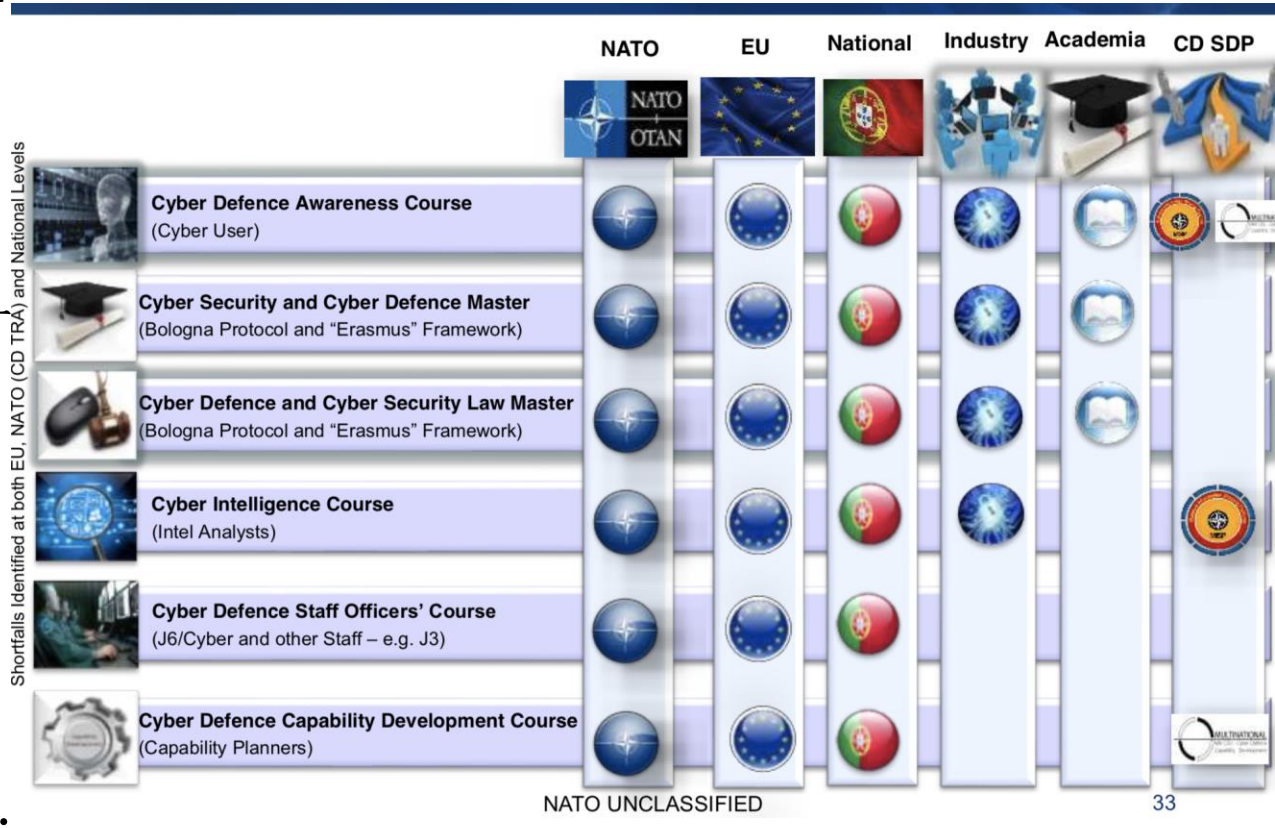
- Cyber Defense
  - もはや数えられないほどに…
  - カリキュラムは公開
    - 認定取得に必須
  - 講義内容もほぼ公開
  - 実習の一部は非公開
- Cyber Operation
  - 参加校は限られている
  - カリキュラムは非公開
    - 具体的な内容は不明
      - 学内にも
      - 建物も制限区画



https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

EU/NATOでも類似の動き

- MultiNational Cyber Defense Education & Training (MN-CD E&T)
- 背景には
  - 一般大学と軍の大学の基準合わせ
    - 学部・学科認定
      - 最低品質保証
        - 必須科目の内容
          - 選択科目は評価対象外
        - どんけつの学生のインタビュー
          - 必要最小限の知識を確認
- 一枚岩ではない
  - ドイツ：国防に対する距離感
  - イタリア：サイバーテロなら
  - フランス：米国主導に違和感
  - イギリス：海洋国家の考え方と…



http://enadciber.eb.mil.br/images/V_Seminario/palestras/2_AGO_17_6_Multinational_Cyber_Defence_Education_and_Training_Project.pdf

自動対処を見据えた人材育成

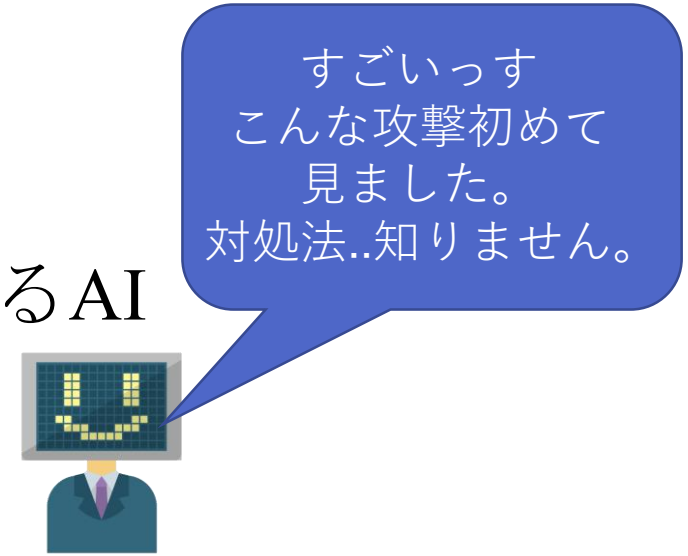
- サイバー攻撃を未然に防ぐソリューションの乱立
  - AIとか人工知能とかを駆使
    - AIが得意なのは膨大な学習データに基づく正解判定
    - 過去に存在しない状況を正しく判定できるか？
- 初期侵入～横展開への対応
  - 大部分はツールによる自動攻撃
    - 既知の攻撃・想定される攻撃シナリオに準拠
      - 発見は既存技術で可能
        - IDSの検知ルール
      - 未知攻撃も被弾直後に解析可能 (秒単位)
        - IPSによる通信遮断
          - 仮想パッチ

- …を出し抜こうとする攻撃者たち…

意図性を有する攻撃

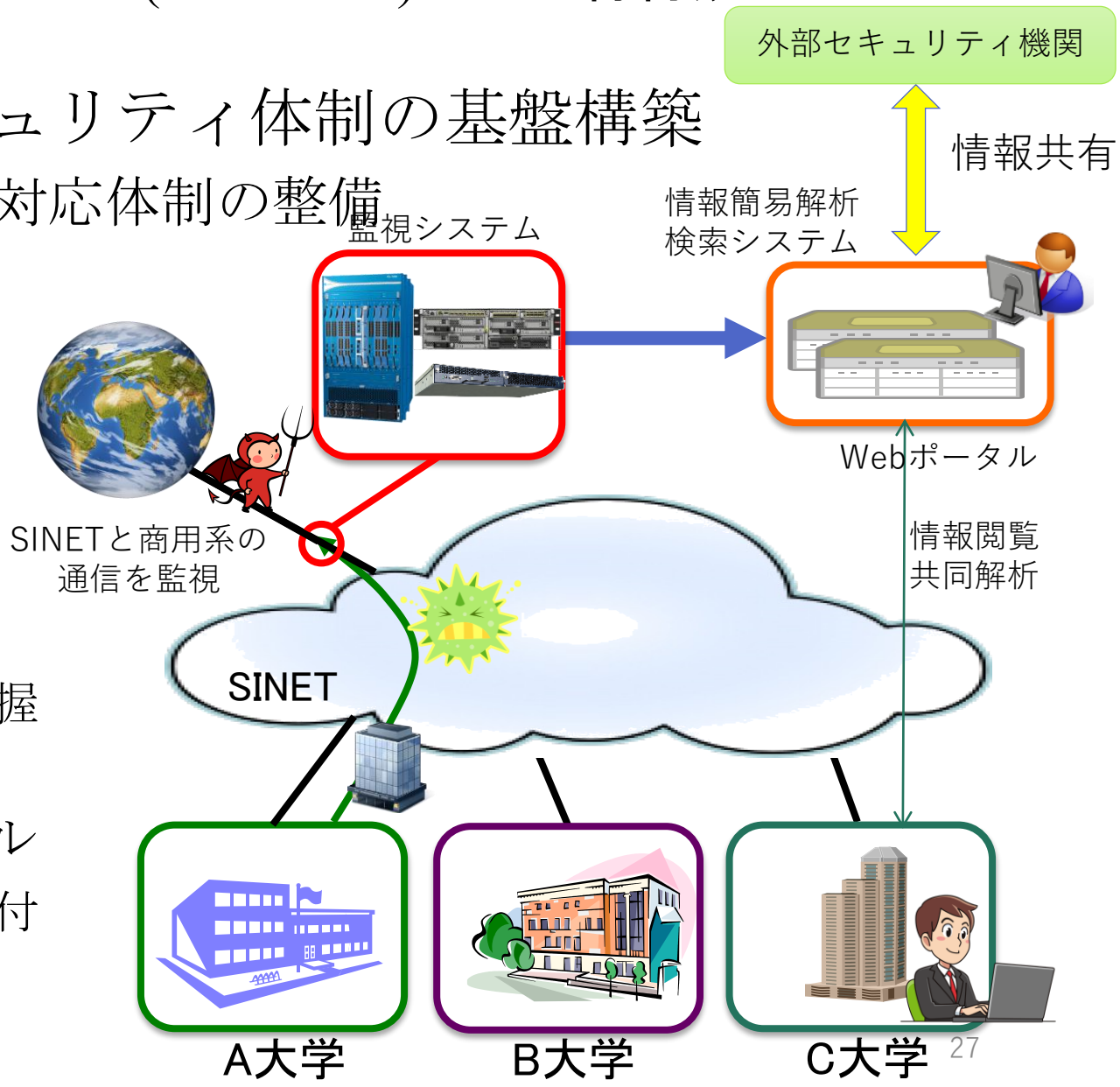
- 目的がある以上、追い出しても再度やってくる
- 繰り返すうちに高度化する…
  - 居なくなったのではなく見えなくなっただけ
- 攻撃者の目的や意図の把握が重要
  - 気付いていることを悟らせない防御
  - ダメージコントロール可能であれば
    - 観察する
    - 罠を仕掛ける

- 学習データにないイレギュラー状況を検知するAI
  - あとは人の出番
  - AIを相棒にできるセキュリティエンジニア



NII-Security Operation Collaboration Services (NII-SOCS)での人材育成

- 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8億円で100機関…(？)
    - 24/365体制での監視
  - 3種類の監視システム
    - Paloalto, Cisco FirePower, 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
      - M社 AGP
  - 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
  - 国内外との情報共有



NII-SOCSの対象…見えない攻撃

- 発見
  - 不審な活動の把握
    - 既知攻撃も検知する
      - 警報が出てる攻撃→対応済みのはず…なので対象外
    - 誤検知も多い
- 識別
  - 本当に未知の攻撃か？
    - 一定時間の挙動観測で判断
      - 脅威情報に基づく攻撃性、リスクレベル、被害範囲の推定
- 対処要請
  - 各大学へ通知
  - 対応状況を観察

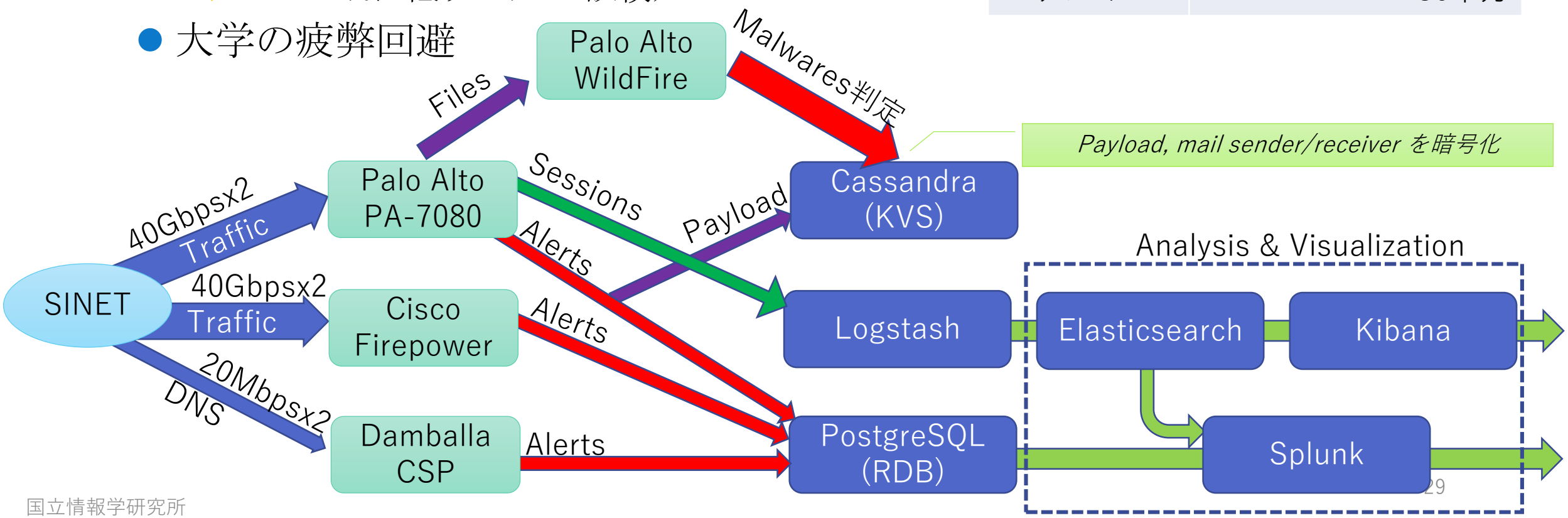
この間の遅延短縮が課題

被害拡大を生暖かい目で
見守ることも重要

NII-SOCSでの警報・セッションの自動処理

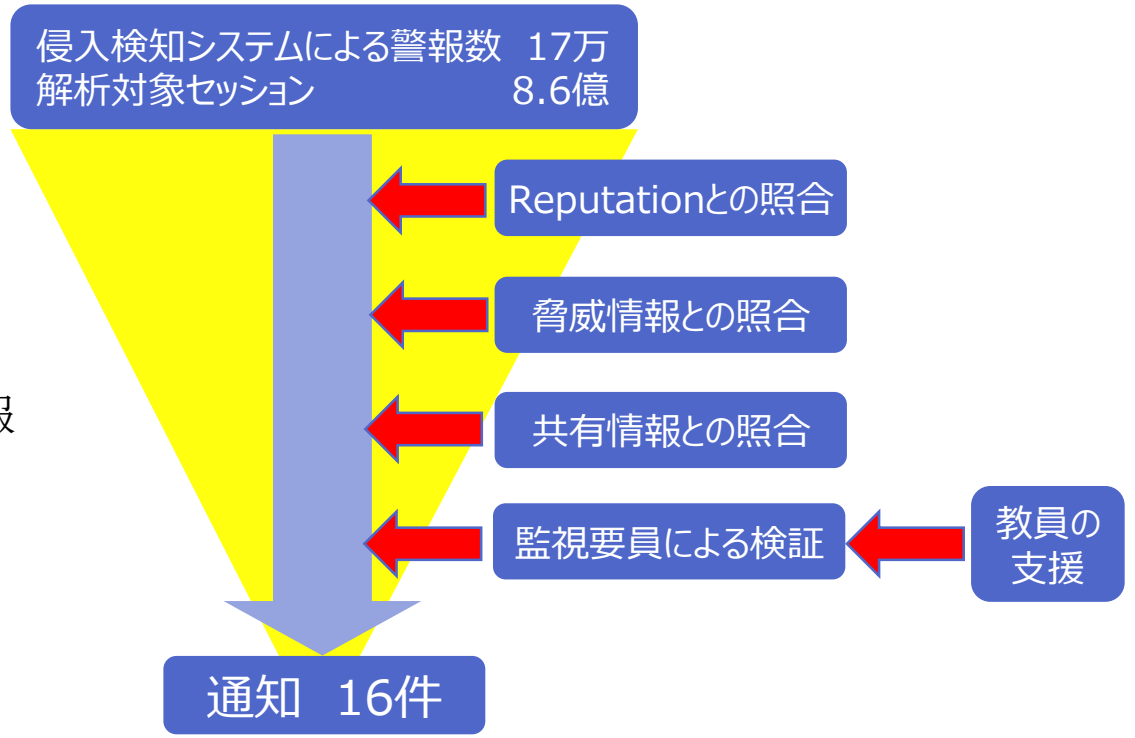
- 1日あたりの分析量
  - 17万警報
  - 8.6億セッション
    - 99.99…%は低リスク or 誤検知
  - 大学の疲弊回避

センサー	警報数/セッション数
Palo Alto	8万
Cisco	6万
Damballa	3万
セッション	86千万



警報･セッションの自動分析

- 警報・セッション情報
  - 各種情報の分析
    - 異なる脅威情報とのクロスチェック
      - 脆弱性の有無、過去の事故歴
      - Twitterで指摘されたドメイン名
      - 当該ドメイン/割当IPアドレスの脅威情報
      - Sandboxの解析結果
        - 複数で確認できたもののみ採用
    - 概ね5～30分で完了
      - 人による検証が一番時間がかかる
      - 状況によっては人の検証は事後とする
        - 夜間は人手も足りて無いし
  - 緊急性・危険度の高いものを抽出
    - 通知したものによる調査→危機管理の演習を兼ねる



まとめ

- 変化しない情報機器
  - 頑張っても撲滅は困難(OA機器ですら)
- 変化するサイバー環境
  - 次世代ネットワーク、コンピューティング環境への対応
- 長期戦化するサイバー攻撃対処
  - 要員の適切な配備と運用
- 道具マニアからの脱却と相手側戦略の見定め
  - 敵側武器の品評会やって仕方がない
- 想定すべき見えない状況
  - ルール無視の無差別格闘術に立ち向かうには
- 今後の人材育成
  - 定式化しつつある人材育成と自動化への対処