

# 大学間連携による サイバーセキュリティ体制の強化

高倉弘喜  
国立情報学研究所

# サイバー攻撃の目的の変化

## ■ 真の目的

- 情報持ち出しは本来の目的のための下準備
- 情報機器を麻痺させる or 破壊することではない  
→ サイバー攻撃により相手の能力を削ぐこと

## ■ CyCON\* Table Top Exercise(TTX)のお題

- 攻撃者の本当の目的に気づけたか?
  - ◆ お手軽な方法で目標達成
  - ◆ サイバー攻撃の影響範囲はサイバー空間に留まらない

## ■ 防御側の考え方も変わらざるを得ない

- 被害範囲の推定
- 防衛ラインの設定
- (部分的な)運用継続の可否判断

年金事務所のマルウェア感染



電力会社の株価暴落



電力会社の経営権奪取

守りたいものは何か？

DoS攻撃回避のためWebサーバを停止？

# サイバー攻撃の巧妙化...の例

## ■ 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

SYN floodとしては  
検知できるが...

## ■ 暗号通信による司令

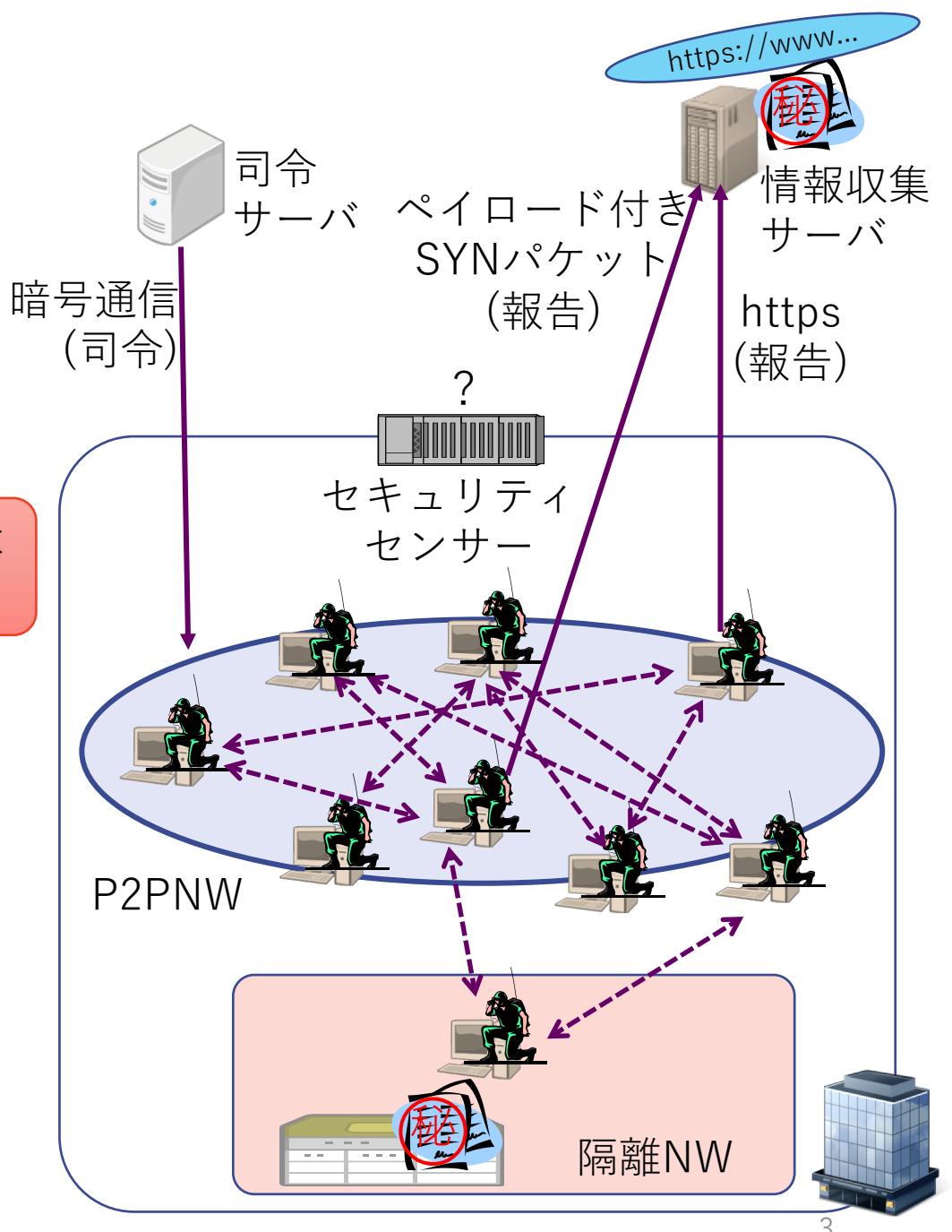
- https, VPN, onion routing...

暗号を解かない  
限りは解析不能

## ■ 標的組織内で通信網を構築

- 侵入成功後の横展開
  - 司令と報告は別経路

内部NWの  
監視必要？



# セキュリティ侵害の発生を想定したセキュリティ対策

## ■ 攻撃や情報流出の可能性

- 検知できなくて当たり前

## ■ 海外の動きは...

- セキュリティ装置のMITM化

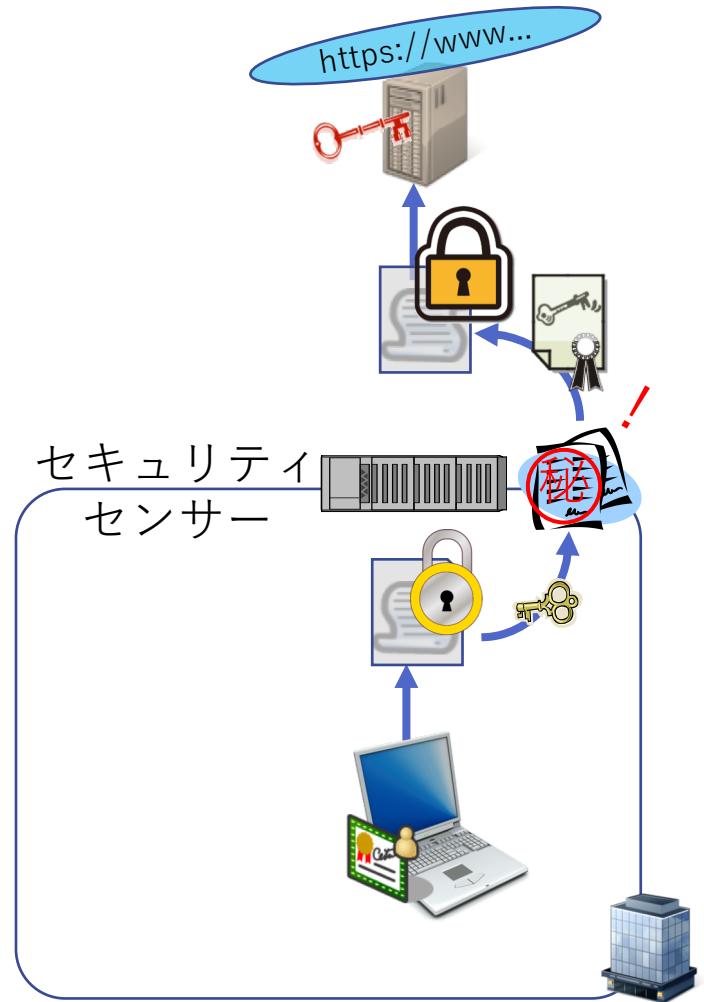
- ◆ 暗号通信を復号+平文内容を検査+再暗号化
  - コスパ問題...小規模NWなら
  - セキュリティセンサーによるオレオレ証明書
    - プライバシ問題...職場なら
    - 装置そのものが攻撃の対象に...ミイラ取りが...

- 暗号を解かずにセキュリティ侵害発生を検知

- ◆ 暗号通信の挙動から不審なものを...

## ■ 実用レベルには...

→脅威インテリジェンスの活用



# レジリエンスのあるサイバー攻撃対応



## ■ 情報システムの全停止は許されない時代に

### ● 局所的なシステム停止

- ◆ 被害箇所の切り離し・隔離によるダメージコントロール
- ◆ 代替措置によるデグレーデッドオペレーション
  - 業務への影響を把握

プランA：部門3隔離  
プランB：部門2保護・監視強化  
プランC：部門1業務継続

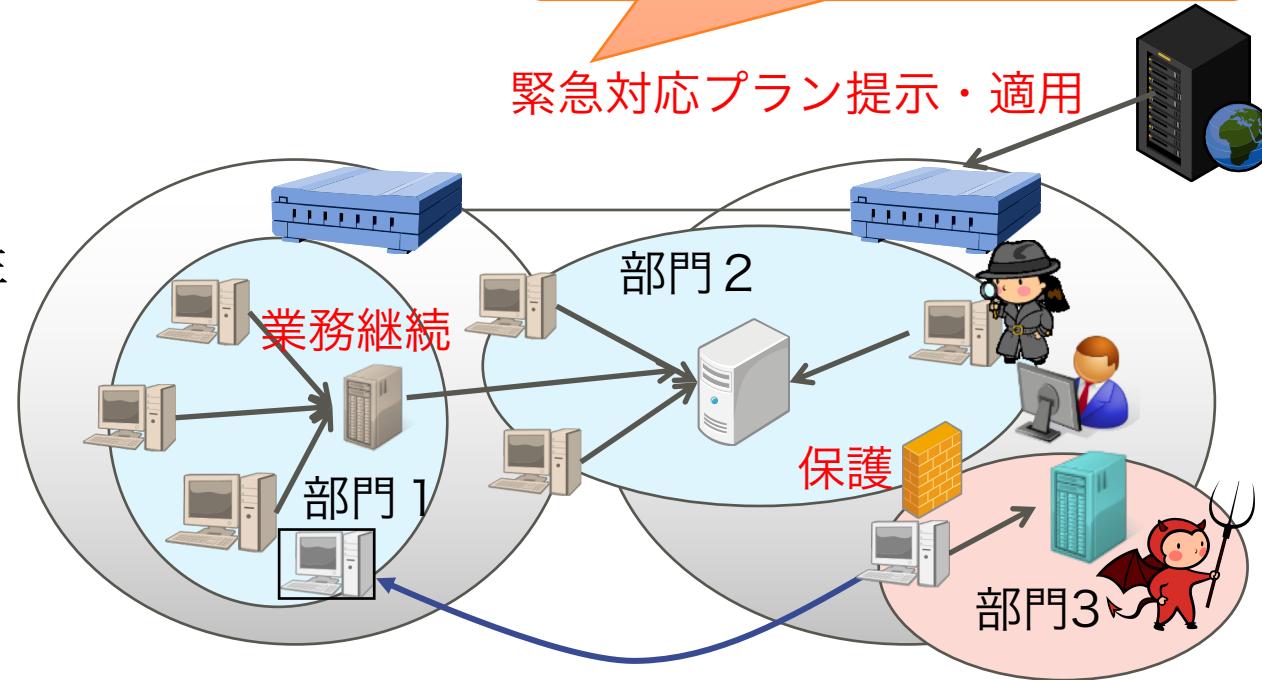
## ■ 人間がすべて判断するのか？

### ● 人間系に対する飽和攻撃

- ◆ エリートパニック状態に陥る危険性

### ● 自動対応による暫定措置

- ◆ 様子を見ながら適宜調整
  - 必要な情報の流れを確保
- ◆ これも研究段階



# 現状では、高度な攻撃には高度な体制が必要

## ■ サブチームによる作業分担

- 数名ずつの少数精銳
- 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

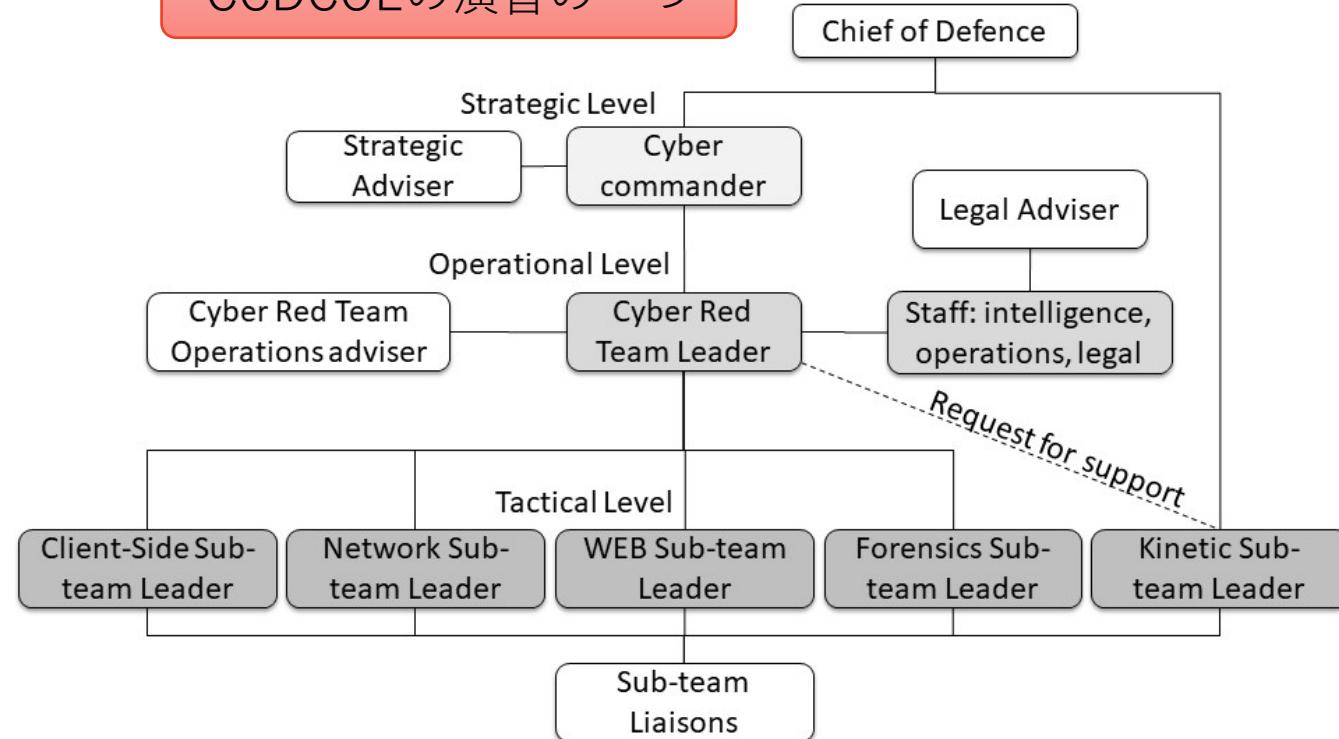
- 防御のためとはいえ法令遵守

## ■ そのための訓練も

- 統制のとれたチームプレー  
ができる人材の育成が急務

## ■ 次世代技術の動向は注視

CCDCOEの演習の一つ



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

一匹狼が活躍する時代から…



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

## ■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

- 4種類の監視システム

- ◆ Paloalto, Cisco FirePower,  
Damballa CSP, LookingGlass

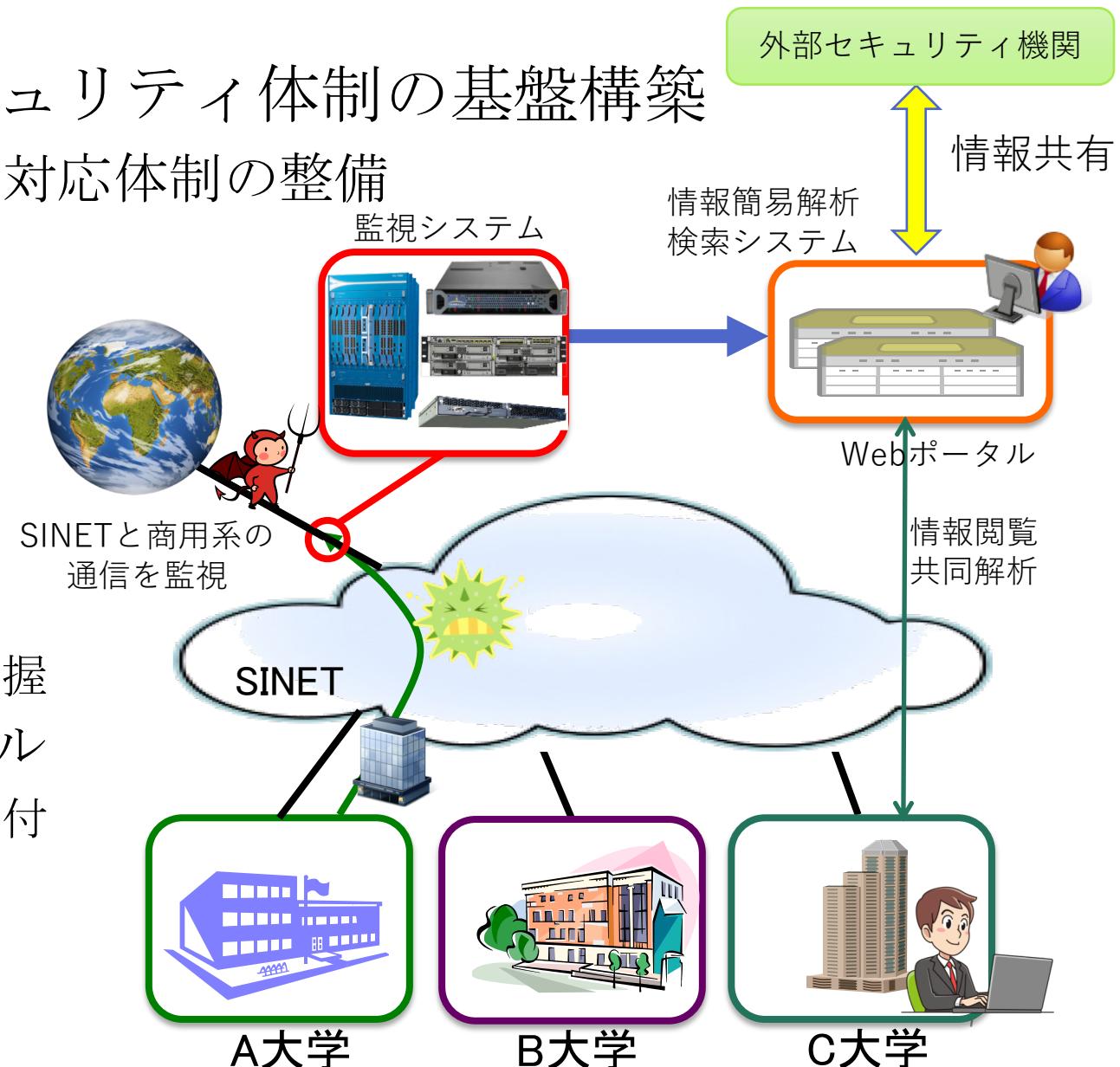
- 脅威情報サービスの利用

- ◆ 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

警報はトリガーではない

## ■ 識別

- 本当に未知の攻撃か?
  - ◆ 関連すると思われるセッションの挙動分析で判断
    - 警報が出ることはほとんどない
    - 脅威情報に基づく攻撃性、リスクレベル、被害範囲の推定

この間の遅延短縮が課題

## ■ 対処要請

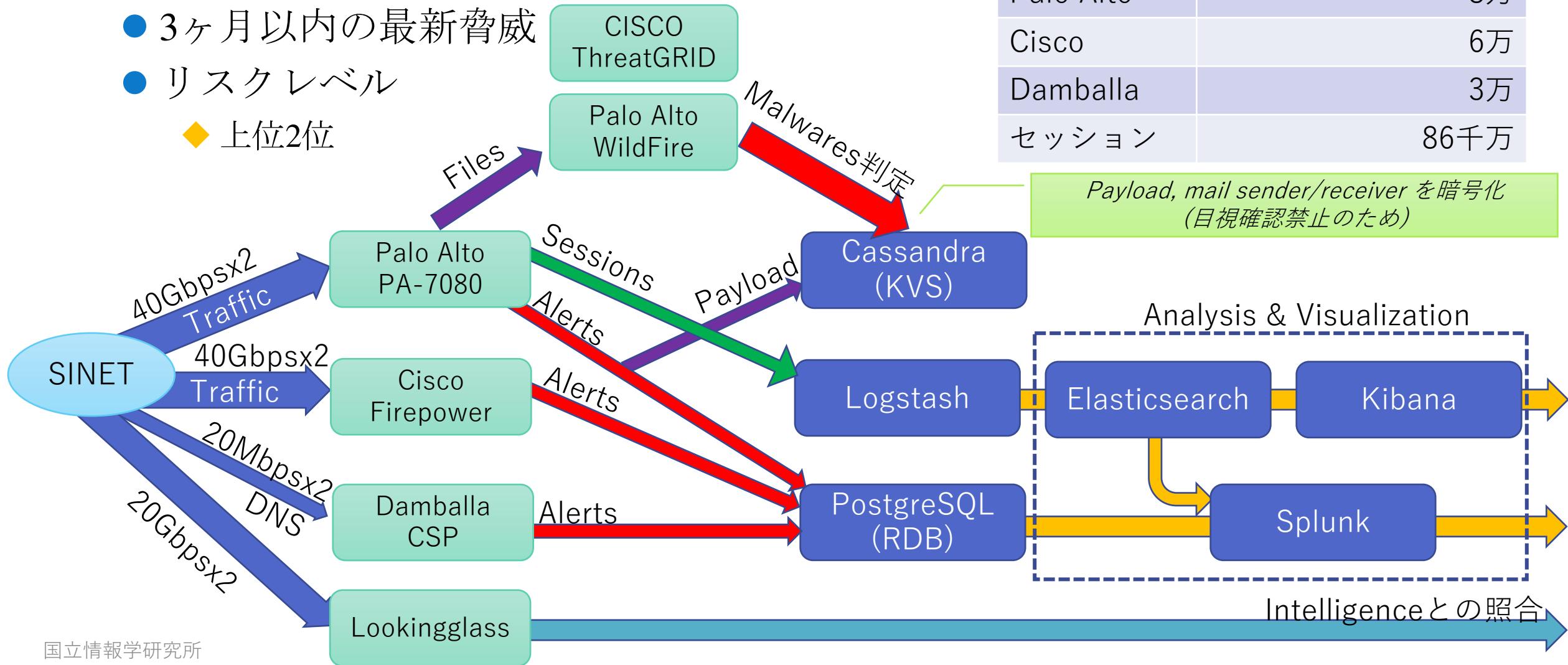
- 各大学へ通知
- 対応状況を観察
  - ◆ 状況に応じたトリアージ判定
  - ◆ 致命傷事態の回避

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

## ■ 警報

- 3ヶ月以内の最新脅威
- リスクレベル
  - ◆ 上位2位



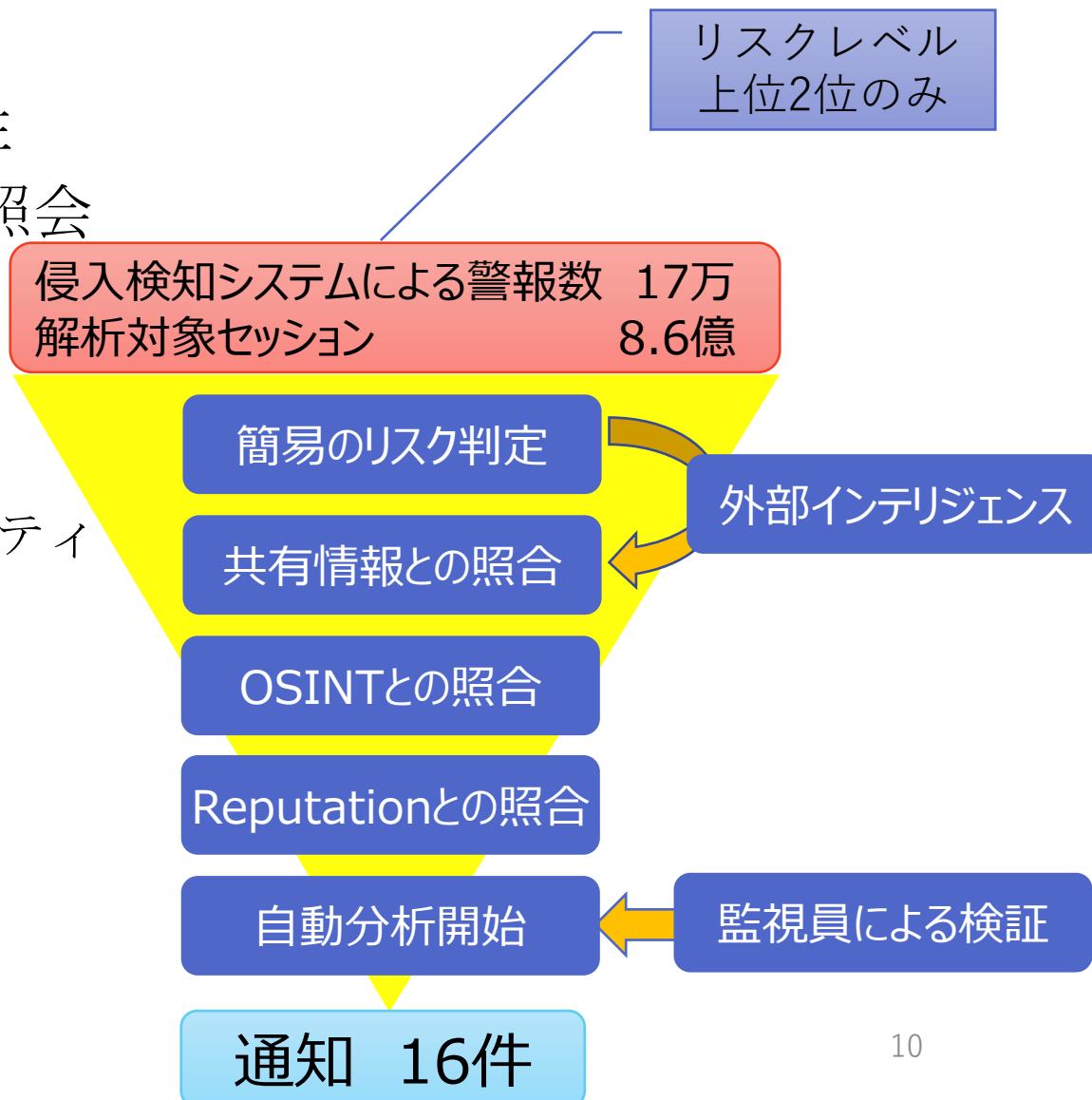
# 警報・セッションの自動分析(1)

## ■ 簡易分析によるリスク判定

- Zero-dayの可能性、被害発生の可能性
- 場合により外部インテリジェンスへ照会

## ■ 共有情報との照合

- NII-SOCS参加機関からの情報
- 国内外連携先からの情報
  - ◆ JPCERT/CC, IPA, NISCサイバーセキュリティ協議会, ....
  - ◆ 各個の入手情報
- 外部インテリジェンスの情報
  - ◆ Alien vault (AT&T Cybersecurity), ETPRO(Proofpoint), AIS(DHS NCCIC)...
  - ◆ A●P(M社)
- 時間がかかる場合は後で反映



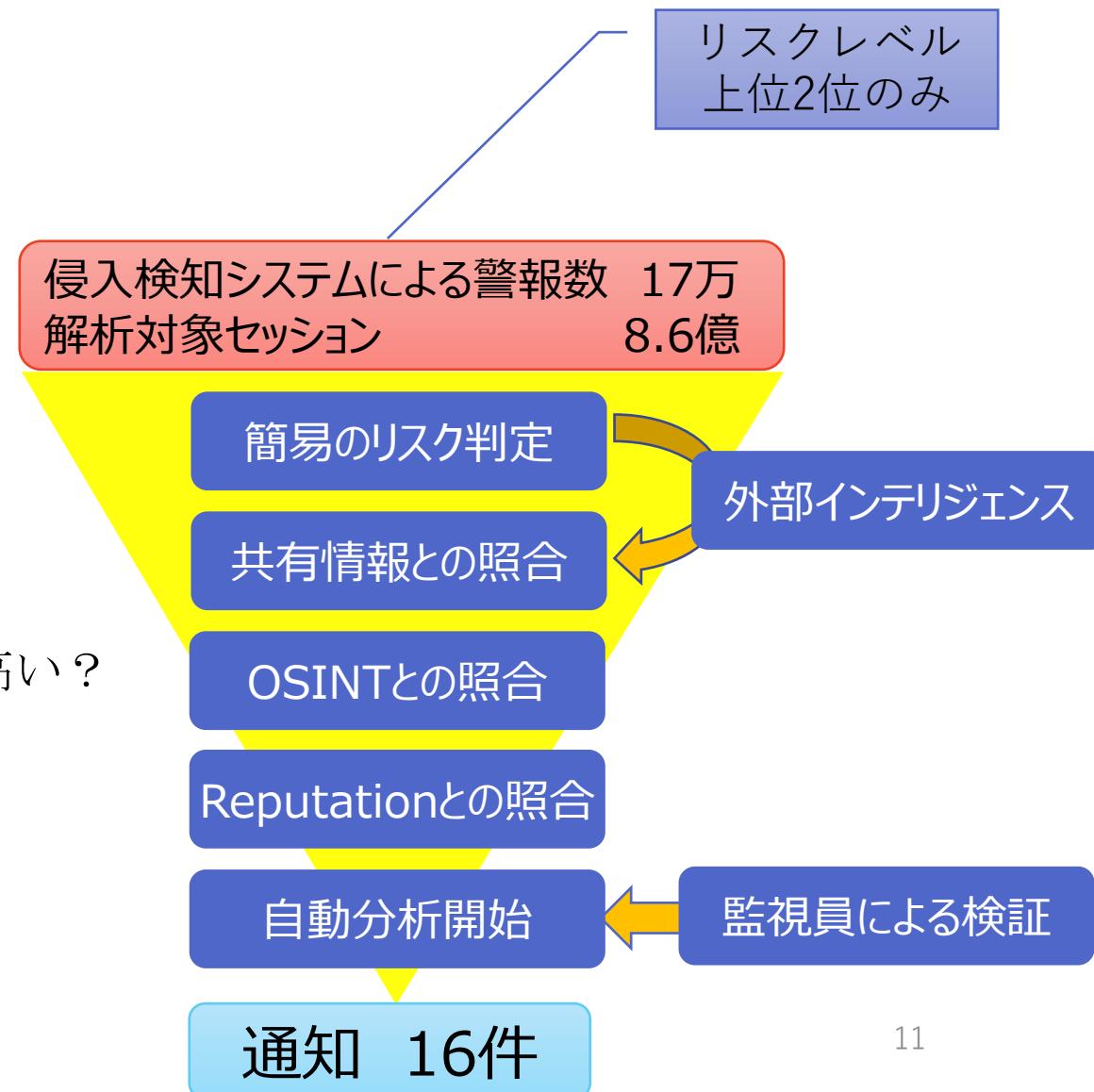
# 警報・セッションの自動分析(2)

## ■ OSINTとの照合

- SNSやブログの情報検索
- 国内セキュリティ情報検索
  - ◆ 日本限定の攻撃の察知
- SHODAN, VirusTotal等の確認
  - ◆ 狙われたシステムに関する情報収集
  - ◆ マルウェアの新規性と危険度を推定

## ■ Reputationとの照合

- 複数サンドボックスの動的解析を比較
  - ◆ 商用&無償それぞれを活用
  - ◆ それぞれで挙動が大きく異なる→本気度高い?
- C2のIPアドレスを特定
  - ◆ C2 DNS/IPアドレスのリスク度確認
  - ◆ DNS名に対するIPアドレスの変遷を追跡
- DarkWebの自力調査



# 警報・セッションの自動分析(3)

## ■ 各種情報の照合作業

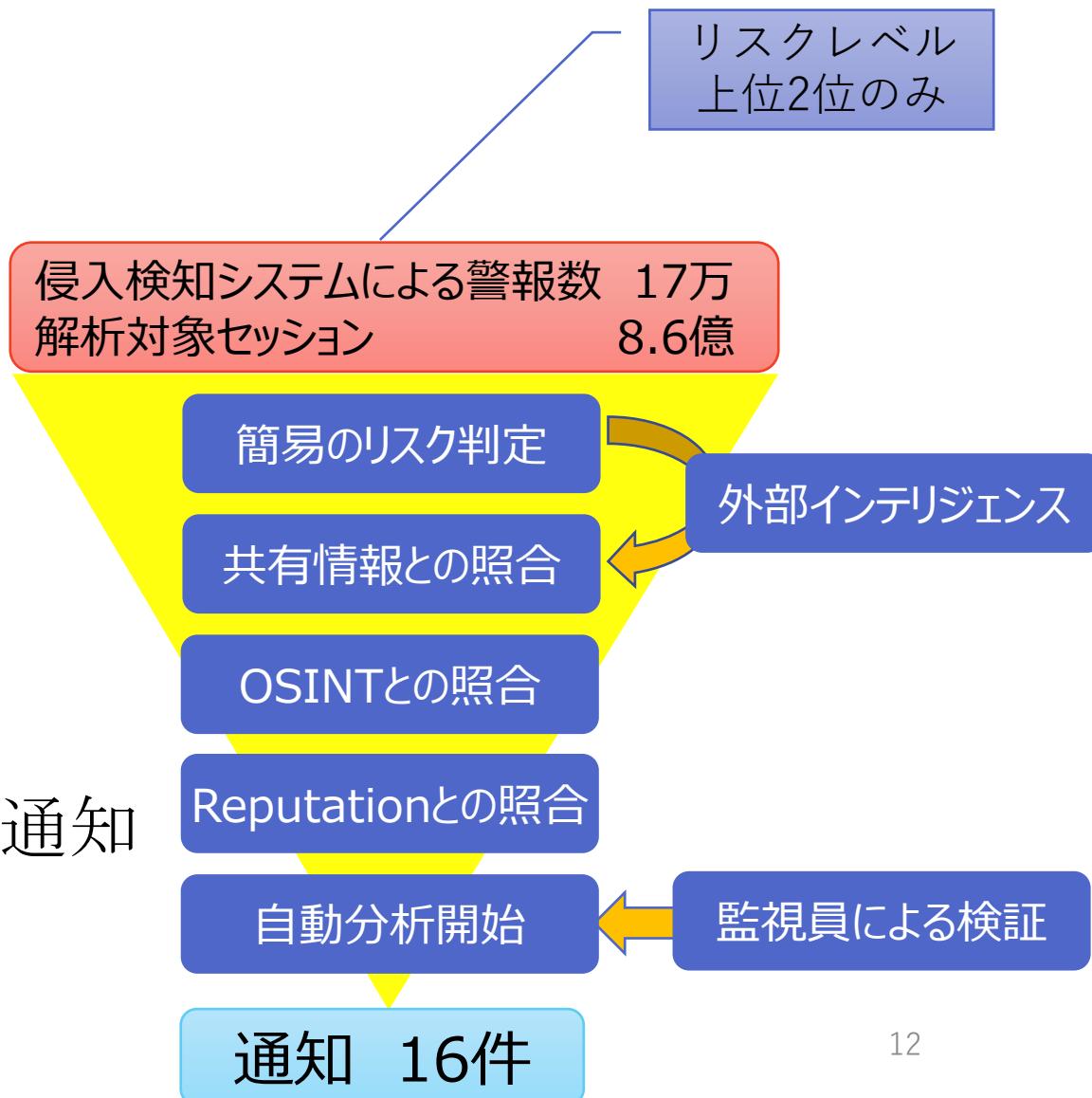
- 全て自動化
  - ◆ 情報の構造分析と必要情報の抽出

- 概ね5分で完了

## ■ 人による照会や検証

- 外部インテリジェンス照会
- 監視員による検証
- DarkWebの自力調査
  - ◆ 一番時間がかかる

→緊急性・危険度に応じて暫定でも通知



# リスク分析

- 目標：各大学へ高リスク攻撃情報を週1件程度通知
  - 大多数は数ヶ月に1件程度

capture_time	source_ip	duration	concurrency	City	Country	days_since_last_activity	threatscore	visitor_type
2019-04-18 06:41:10.255								
2019-04-18 06:46:46.075	7.166	335.82	11	Paris	France	76	6	1
2019-04-18 23:48:57.268								
2019-04-18 23:51:47.804								
2019-04-18 23:51:50.31								
2019-04-18 23:52:46.389		231.424	8		France			
2019-04-18 23:52:48.692								
2019-04-18 07:25:08.639								
2019-04-18 07:27:13.298	153	124.659	12	Walnut	United States			
2019-04-18 01:49:17.555								
2019-04-18 01:57:14.052	0.60	476.497	7	Provo	United States			
2019-04-18 04:51:32.017								
2019-04-18 04:51:42.83								
2019-04-18 04:51:43.531	228	11.514	6		Ghana			
2019-04-18 16:04:19.496								
2019-04-18 16:04:20.097								
2019-04-18 16:10:04.075	3.62	344.779	17		Ukraine			
2019-04-18 16:10:04.275								
2019-04-18 01:43:19.711								
2019-04-18 01:43:39.536								
2019-04-18 01:51:13.301	5.82	473.59	8	Algemesi	Spain			



# リスクレベルに応じたインシデントレスポンス

## ■ 緊急性の高いものから対応

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

# マルウェアの脅威分析

## ■ 標的型攻撃メール

- 数度観測

- ◆ 数名への着弾確認

- 複数のsandboxで挙動分析

- ◆ 発症後に通信するC2を特定

- 被弾PCでのマルウェア発症を調査
- Sandboxと異なる挙動の特定

- NII-SOCS解析時は未知マルウェア

- ◆ そもそもサンプルとして上がっていない
- ◆ その後の推移

- 被弾機関へのサンプルupload自粛要請
- サンプルuploadを確認(誰が?)
- カバー率の状況を注視

→マルウェアの危険度を推定



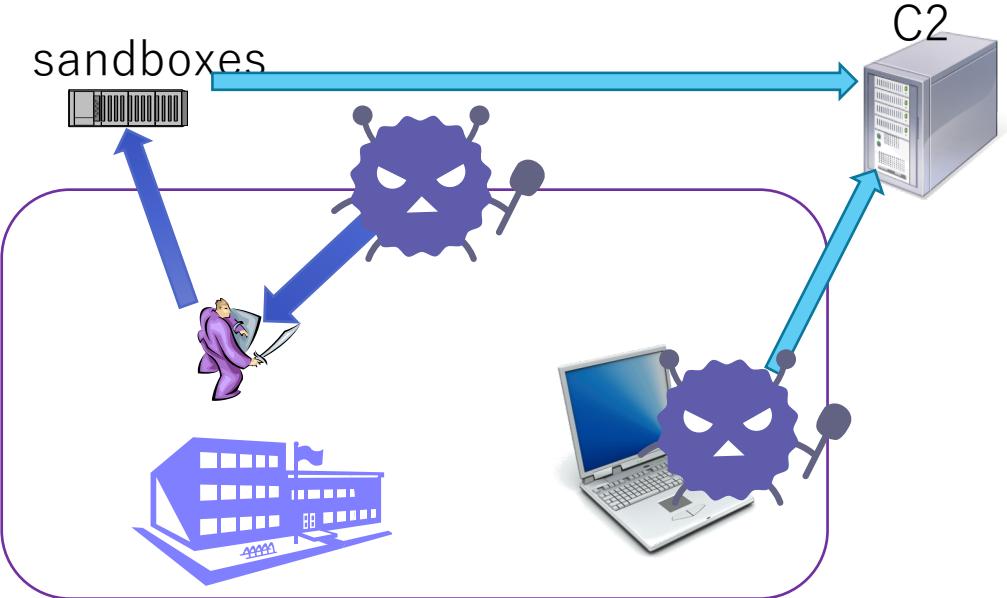
# 類似挙動の追跡

## ■多くの機器

- 学外感染
  - ◆ 自宅、出張先、モバイルルータ...
  - ◆ マルウェア感染時は確認不能

## ■ Sandboxでの解析結果

- C2サーバの特定
  - ◆ 複数のsandboxが同じC2を指しているか？
- 同じ挙動を示す機器のあぶり出し
  - ◆ 感染済みbut未発症のPCの特定
    - C2サーバへのkeep alive通信を特定



virustotal.com

Search or scan a URL, IP address, domain, or file hash

37 engines detected this file

SHA-256: ac81ec77b9d67db7a62c5c4a4b9eeecd2c2bbddfc  
File name: 職場あて.xls  
File size: 61 KB  
Last analysis: 2018-05-15 14:35:09 UTC  
Community score: -97

Detection	Details	Behavior	Community
Ad-Aware	⚠ VB:TrojanDownloader.JUGR		
AegisLab	⚠ W97M.Gen!		
AhnLab-V3	⚠ XLS/Downloader		4

# 各種情報の共有

## ■ インシデント情報共有の課題

- 情報提供による二次被害発生の懸念
  - ◆ NDAなどで縛られてはいるが... 疑心暗鬼なのは仕方がない
- 組織としての情報共有 v.s. 担当者間の情報共有
  - ◆ 事務方が分かる用語の利用
  - ◆ 決済のたびに丸められる技術情報
  - ◆ 担当の独断で情報が出せるか？

## ■ 海外の場合

- 政府機関が情報収集
  - ◆ 法的義務付けがある場合も
  - ◆ 匿名化等をほとんど施さずに共有
    - 提供情報に基づく情報分析や遮断を自動で実施する製品
- 業界によっては役職(担当)ごとに存在する横串型ISAC

# 各種情報によるクロスチェック

## ■ サイバー攻撃の目的、攻撃性、侵害時リスクの把握

### ● 攻撃者のターゲットを推定

- ◆ 攻撃者のプロファイリング
- ◆ 攻撃対象のプロファイリング
- ◆ 攻撃の目的と手段

- 情報の持ち出しだけではない
- 業務妨害目的だってある

### ● 被害範囲と拡大状況の推定

- ◆ 被害は1大学か？複数大学か？
- ◆ 被害が広がりつつあるのか？

- 感染疑いはあるが発症していない？
- 発症した場合の確認手段はあるか？

### ● ダメージコントロール不能になる前に対策開始

# 脅威情報の鮮度と精度

## ■ 有償情報でも...

- 不正確情報・誤報は含まれる
- 我々に影響のない情報多数
  - ◆ 一方で多国籍組織な大学
  - ◆ 日本限定の情報だけでは不十分
- 深刻な攻撃情報の調査は月単位

## ■ 攻撃者に騙されるsandboxやハニーポット

- 偽C2サーバ情報に振り回される

## ■ OSINT情報の精度はさらに低い

- 鮮度は高いが

## ■ DarkWeb

- 見つけられたとしても極わずか...
  - ◆ その情報はリスクが高いか？

○

億件パスワード情報漏洩

364229	3	13	2018	1practicing.com.txt
76914	3	13	2018	1anyconference.org.txt
76919	3	13	2018	1anyconference.org.txt
7200	3	13	2018	1botanyconference.org.txt
7200	3	13	2018	2015.botanyconference.org.txt
17729	3	13	2018	2017.botanyconference.org.txt
150060	3	13	2018	210.212.144.213.txt
3100293	3	13	2018	211026.myam.us.txt
227200	3	13	2018	216.38.51.242.txt
112821401	3	13	2018	2Games.com .txt
1431417	3	13	2018	35fg.net.txt
75931	3	13	2018	35map.com.txt
1694123	3	13	2018	3DSISO.com.txt
77486	3	13	2018	3ziko.pl_normalized.txt
189824	3	13	2018	45-rpm-records.ad-bazaar.com.txt
465993	3	13	2018	52.11.102.112.txt
566877	3	13	2018	52.66.141.39_normalized.txt
91661	3	13	2018	525.tw_normalized.txt
44859	3	13	2018	5forty3.in.txt
20453	3	13	2018	64.17.172.33.txt
75720	3	13	2018	69.174.243.24.txt
677626	3	13	2018	95.110.213.190.txt
16866	3	13	2018	96.0.100.127.txt
29183899	3	13	2018	ALternos.org.txt
147886242	3	13	2018	Aipai.com.txt
147886242	3	13	2018	Alpari.com.txt
14336873	3	13	2018	AndroidForums.com.txt
4811080	3	13	2018	Anime-Planet.net.txt
2299792	3	13	2018	AnimuTank.com.txt
4117602	3	13	2018	AutoCentrum.pl .txt
345036	3	13	2018	AutoHotKey.com.txt
7835547	3	13	2018	Avast.com .txt
3286000	3	13	2018	BCWars.com.txt
98917	3	13	2018	BTCF.fi .txt
3132383	3	13	2018	BTUN.net .txt
842314578	3	13	2018	Badoo.com .txt
865198	3	13	2018	BigBomber.com .txt
5668236	3	13	2018	Bi .txt
41849	3	13	2018	Bit .txt
1825460	3	13	2018	Bit .txt

古すぎる  
一時利用でテキトーにつけたPW

# NII-SOCSがハブとなる情報共有

## ■ NII-SOCS

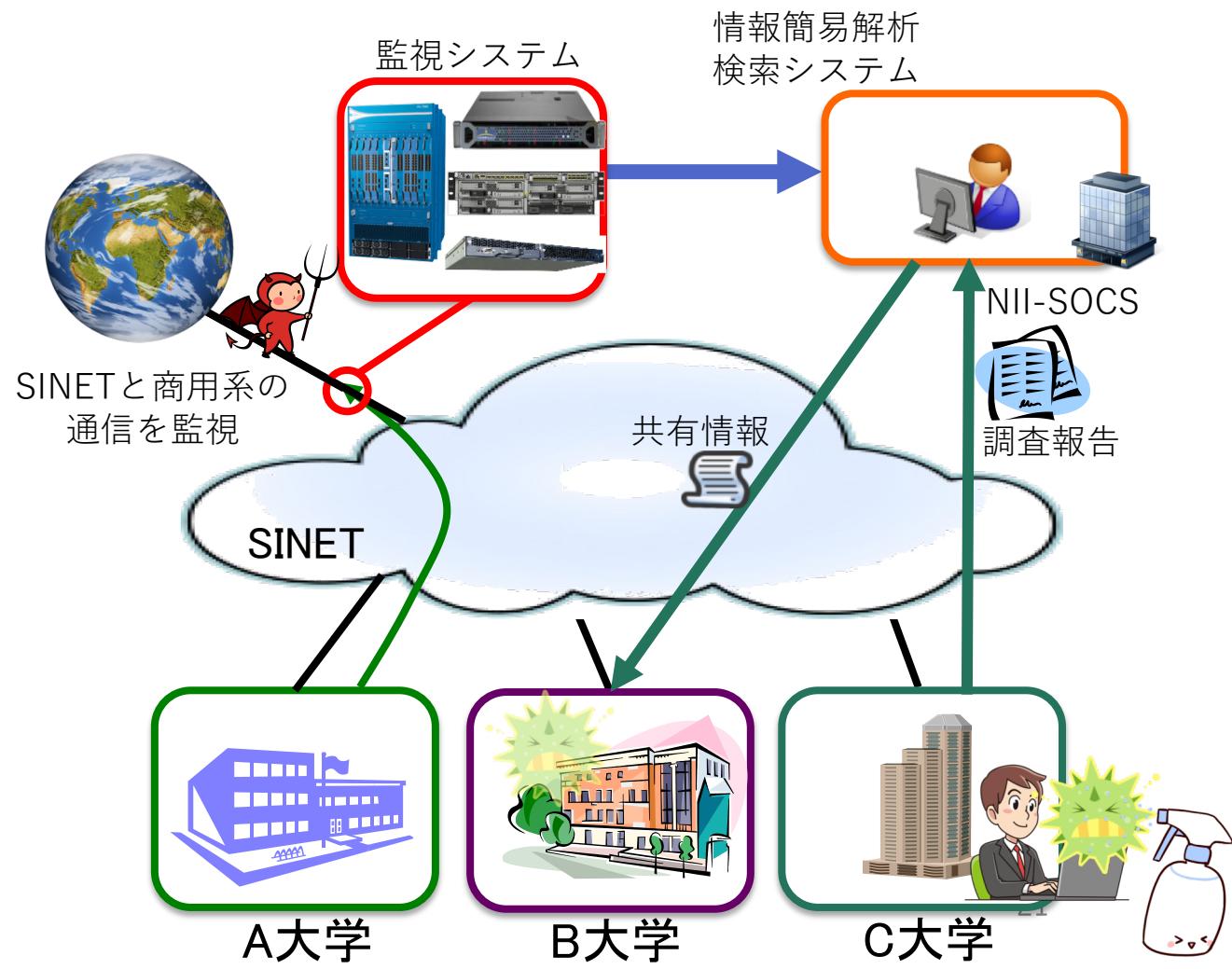
- 警報情報とセッション情報を保持

## ■ 被害発生機関

- 調査報告を提出(任意)
  - ◆ マルウェア感染の経緯
  - ◆ 改ざんされたファイル
  - ◆ 確認された通信先
  - ◆ 送られた(と推定される)情報

## ■ 情報共有

- 組織名を匿名化
- 報告中の個人情報を匿名化
  - ◆ Takakura\_PC...といった情報
- 類似事象が観測された機関のみ
  - ◆ 大規模な場合は同報対応



# 共有情報の例

## ■被害の確認と状況調査

- 想定される被害
- 調査のポイント
  - ◆ 推定される感染マルウェア
  - ◆ 他機関から提供された情報

連絡させていただきました

接続先ドメイン名：

接続先IPアドレス：

ですが、他機関から、  
・暗号化された文字列  
・何らかの制御を行なっていると推定される文字列  
・PCのメーカー名やシリアル番号と推定される文字列  
などが送信されているとの報告がありました。

これらの情報から調査したところ、

[https://www.symantec.com/security\\_response/writeup.jsp?](https://www.symantec.com/security_response/writeup.jsp?)

もしくは、これに類するマルウェアに感染している可能性があると判断されます。本件につきましては、新たな情報が入り次第お知らせ致します。

### [セッション情報]

対象日時：2018/1/...

セッションID：

接続先IPアドレス：

接続元IPアドレス：

不正な通信と思われる状況を確認しましたので、お知らせいたします。  
この通信先IPアドレスについては

<https://www.virustotal.com/#/ip-address/>  
<https://cymon.io/>

マルウェアの接続先情報

可能な場合はOSINT情報  
へのリンクを添付

参加機関間の  
情報共有

# 大学間の情報共有の促進

## ■ NII-SOCS

- 文科省の指揮下にある組織
  - ◆ 誤解ではあるが
- 大学との適度な緊張感の維持
  - ◆ ナアナアな関係の回避

## ■ NII-SOCSと対峙する大学側コミュニティ

- NII-SOCSには報告しづらい情報の共有
  - ◆ 誤検知や誤判断の情報
  - ◆ より踏み込んだインシデントの詳細情報

## ■ NII-SOCSの本来の目的

- 大学の独り立ち
  - ◆ 互助組織によるサイバーセキュリティ能力の向上

# まとめ

## ■ サイバー攻撃の目的の変化

- 目的に応じた
  - ◆ 戦略に基づく作戦立案
  - ◆ 作戦遂行としてのサイバー攻撃対処

## ■ ダメージコントロールによるレジリエントな攻撃対処

## ■ 警報によらないサイバーセキュリティ

- 脅威情報をトリガーとする分析
- インシデントのリスク判定と判定に応じた対処

## ■ 脅威情報そのものの真贋判定

- 正しい場合...重要情報か否か

## ■ 様々な情報共有によるサイバー攻撃耐性の向上