資　料　編

目　　次

発表資料

HITACHI
Inspire the Next

国内におけるシーサート活動

～官民連携を通じたサイバー犯罪捜査及び被害防止対策の更なる推進に向けて～

2015/12/22

寺田真敏
Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/

1. シーサート

Hitachi Incident Response Team

Computer Security Incident Response/Readiness Teamの略

- シーサート(CSIRT)
  Computer Security Incident Response Team
  - コンピュータセキュリティにかかるインシデントに対処するための組織の総称(機能)
  - インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動

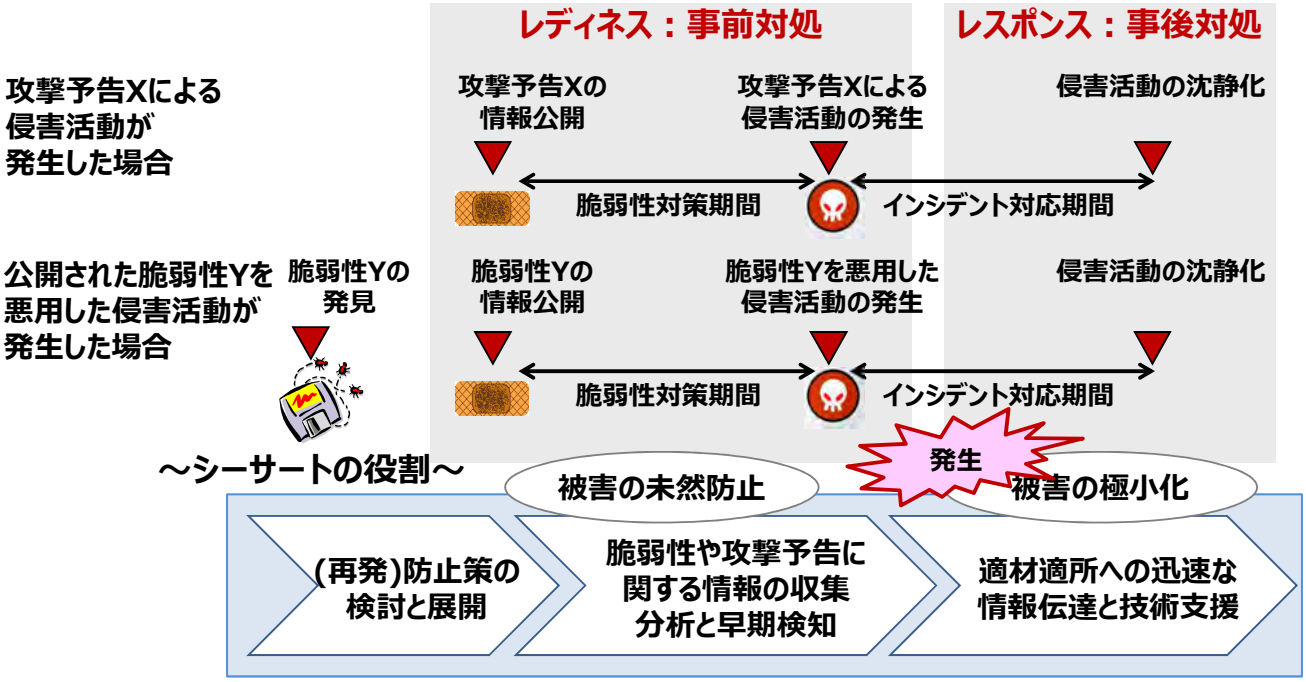
- シーサートの目的、立場(組織内での位置付け)、活動範囲、法的規制などの違いからそれぞれ各チームがそれぞれの組織において独自の活動している。

  ⇒ CSIRTに規格はなく、各組織の実態に即したCSIRTを実装
  ⇒ 1つとして同じCSIRTは存在しない

注：Cyber Security Incident Readiness Teamと呼ぶ場合もある。

1. シーサート

一般的に認識されているシーサートの役割



1. シーサート

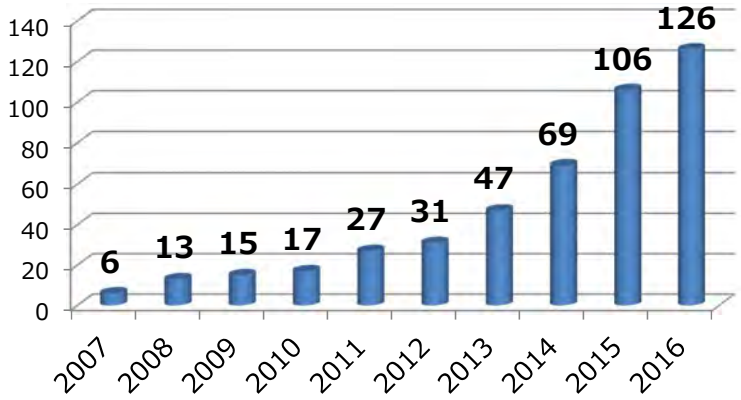
より高度なシーサート連携が求められてきている

年代	特徴	被害の模式図
2000年 ～2001年	均一的かつ広範囲に渡る単発被害 Webサイトのページ書き換え	
2000年 ～2005年	均一的かつ広範囲に渡る連鎖型被害 ウイルス添付型メールの流布 ネットワーク型ワームの流布	異なる組織のシーサート同士がつながり、手段を共有することで問題解決を図る
2005年～	類似した局所的な被害 SQLインジェクションによるWebサイト侵害 Winny、Shareによる情報流出 フィッシング、スパイウェア、ボットなど	
2006年～	すべてが異なる局所的な被害 標的型攻撃 攻撃組織基盤化 2009年～ 攻撃組織間連携 	 異なる組織のシーサート同士がつながり、侵害活動を鳥瞰することで問題解決を図る

2. 日本シーサート協議会

日本コンピュータセキュリティインシデント対応チーム協議会

- 2007年3月設立
- 使命
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る
- 2015年12月1日現在、106チームが加盟

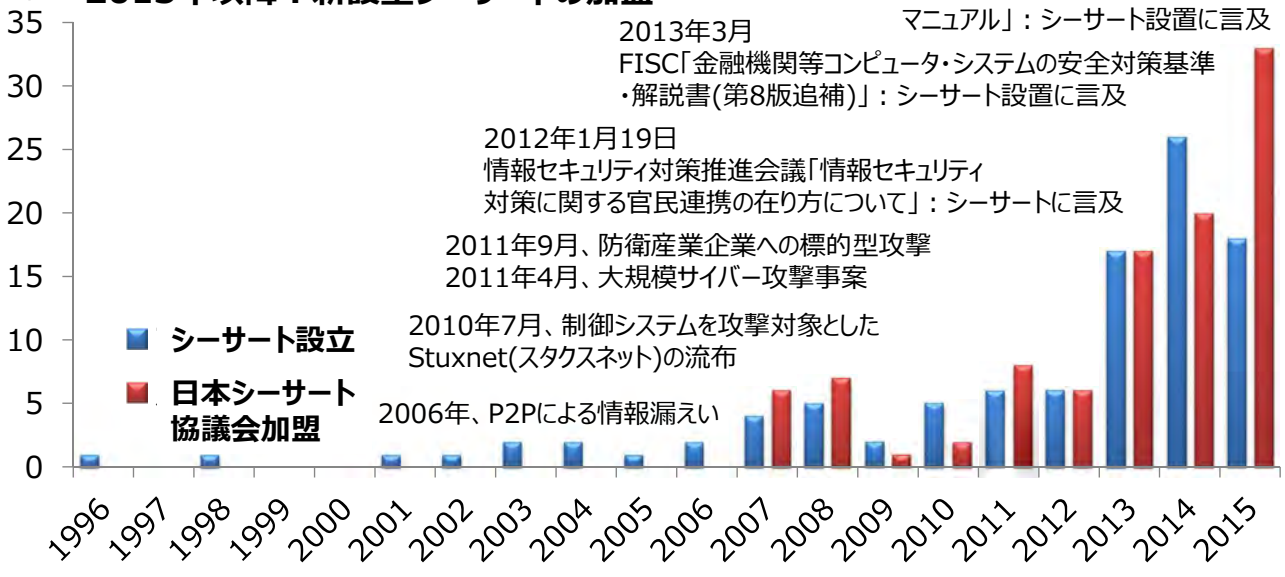


出典：日本シーサート協議会加盟組織一覧2015
http://www.nca.gr.jp/member/index.html#member_04

2. 日本シーサート協議会

シーサート設立年と日本シーサート協議会加盟年の推移

- 2012年以前：旧来型シーサートの加盟
- 2013年以降：新設型シーサートの加盟



出典：日本シーサート協議会加盟組織一覧2015
http://www.nca.gr.jp/member/index.html#member_04

2. 日本シーサート協議会

協議会活動にあたっての心構え

- **日本シーサート協議会では、『協議会の会合、メーリングリスト等』の活動において、チャタムハウスルールを適用しています。**

Chatham House Rule

The Chatham House Rule reads as follows:

> *When a meeting, or part thereof, is held under the **Chatham House Rule**, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.*

出典 http://www.chathamhouse.org/about/chatham-house-rule

出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

協議会活動にあたっての心構え

- **日本シーサート協議会では、『連絡窓口担当者(PoC: Point of Contact)の役割』を次のように定義しています。**

- ✓ **シーサート(含む、日本シーサート協議会)間の連携において、実効的な調整担当者であること。**
  - ➢ **チームEmailのメンバに登録されていること。**
  - ➢ **チームサイトURLの問合せ窓口から確実に連絡が届くこと。**
- ✓ **日本シーサート協議会においては、加盟チームの代表者であること。**
  - ➢ **加盟チームの代表者、実効的な調整担当者という立場から、日本シーサート協議会の総会議決権を行使すること。**

出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

企業におけるシーサートの役割

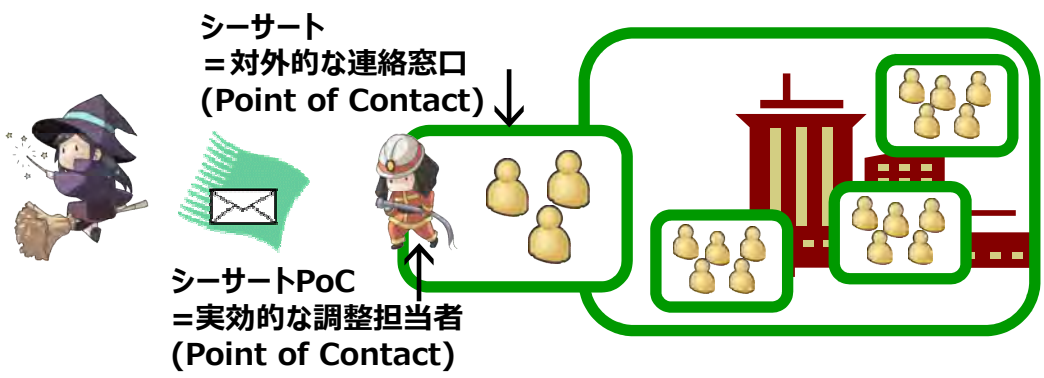
- シーサート活動から導かれる企業におけるシーサートの役割
  - 対外的な連絡窓口であること
  - 技術的な問合せに関して対応が可能であること
  - インシデントレスポンス(事後対処)だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めていること
  - 部署間を横断した組織体制をとっていること

出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

対外的な連絡窓口

- 対外的な連絡窓口が明らかになっていることの利点
  - [通知側] 脆弱性ハンドリングやインシデントハンドリングの通知先を探さずに済む。通知の背景説明を省略できる。通知をたらい回しにされない。
  - [受領側] 通知をトリガに、脆弱性ハンドリングやインシデントハンドリングをベストエフォートで動かし始めることができる。



出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

技術的な問合せに対応可

- 対外的な連絡窓口が、技術的な問合せに関しても対応可能であることの利点
  - [通知側]脆弱性ハンドリングやインシデントハンドリングの技術的な通知をたらい回しにされない。
- 連絡窓口(シーサート)に期待したい要件
  - 技術的な視点で脅威を推し量り、伝達できること
  - 技術的な調整活動ができること
  - 技術面での対外的な協力ができること

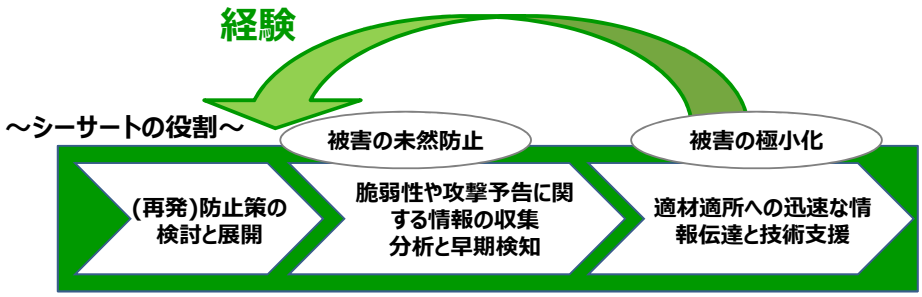
技術的な通知や依頼に対して対処してくれることを期待しているのであり、必ずしも、シーサート内に技術的な専門家が必要であるという指摘ではない。

出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

インシデントレディネス(事前対処)

- インシデントレスポンス(事後対処)などの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めることの重要性



- 経験があるからこそ、「問題解決」に向けての想像力も働く。
- 経験ができないならば、他のインシデントレスポンス(事後対処)の疑似体験を通して、「問題解決」に向けての想像力を養う。

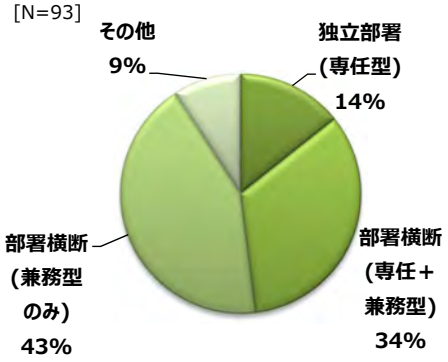
出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

2. 日本シーサート協議会

部署間を横断した組織体制

- シーサート実装の多くは、専任のシーサート要員を抱えた部署を核とした部署横断型
  - 部署間を横断した組織体制の構築、
    すなわち、組織内の横断的な協力体制整備への期待

[N=93]



サイバーセキュリティ対策の推進
特定の部署だけが頑張れば良い(お任せ)
モデルから組織全体で頑張る(連帯)モデルへ

シーサートは万能薬ではない。
組織のセキュリティ文化そのもの。

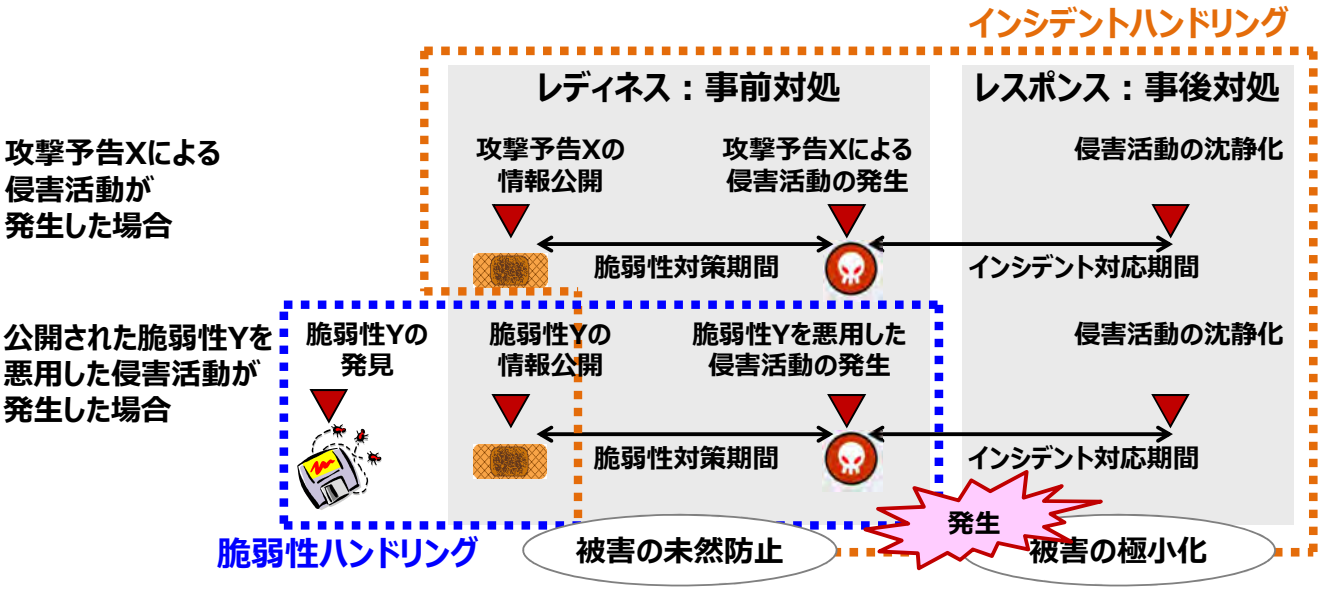
出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

3. シーサート活動の暗黙知(慣習)の明文化

脆弱性ハンドリングとインシデントハンドリング

- シーサート連携にあたっては、
  - 自身が該当組織／該当者と直接交渉
  - 調整機関を介して該当組織／該当者と間接交渉

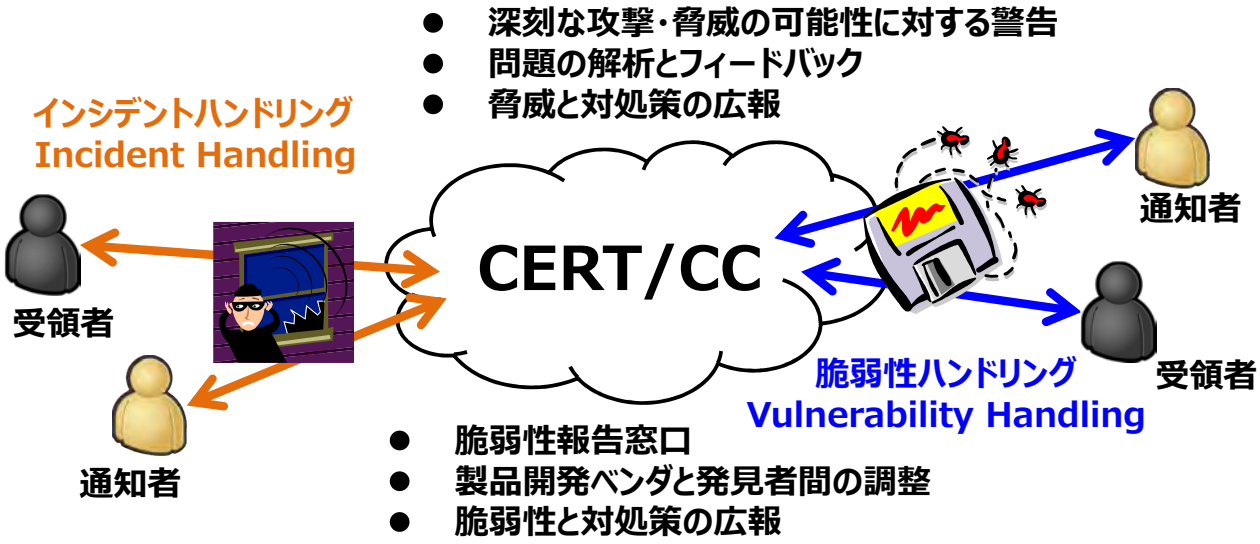
暗黙知(慣習)



3. シーサート活動の暗黙知(慣習)の明文化

脆弱性ハンドリングとインシデントハンドリング

- 脆弱性ハンドリングとインシデントハンドリングは、1988年インターネットワーム事件を契機に設立されたCERT/CCの活動がベースとなっている

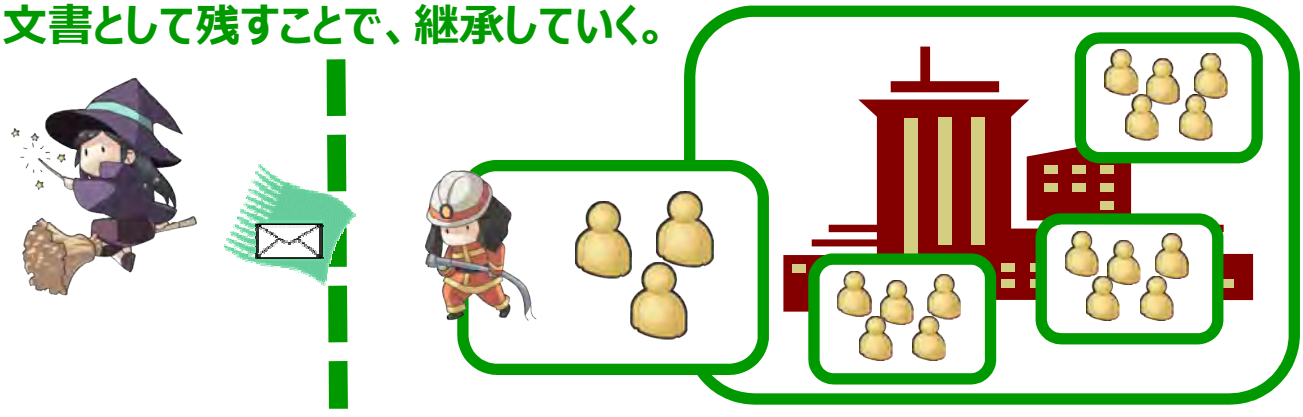


3. シーサート活動の暗黙知(慣習)の明文化

脆弱性ハンドリングとインシデントハンドリング

- {組織間の協力 x (事前対処＋事後対処)}に向けた場の整備
  ＝シーサート活動の暗黙知(慣習)の明文化

インタフェースでの手順を決め、
文書として残すことで、継承していく。



2016年01月27日@総合セキュリティ対策会議

NCFTA・JC3型官民連携の状況

－日本サイバー犯罪対策センターJC3の活動－

（一財）日本サイバー犯罪対策センターJC3
理事　　**坂　　明**

JC3 Japan Cybercrime Control Center

JC3の概要

- **法人名　　一般財団法人 日本サイバー犯罪対策センター**
  （英語名：Japan Cybercrime Control Center　略称：JC3）
- **業務開始日　平成26年11月13日**
- **目的**
  サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。
- **事業内容**
  - サイバー空間の脅威に関する情報の集約・分析
  - 研究・人材育成　　国際連携
- **米国NCFTA（JC3のモデル）の基本ポリシー**
  - “One team, one goal”
  - “F2F（Face to Face）”（直接会って）
  - “Industry First”（「民間を第一に」）
  - “Focus on what you can share and are comfortable sharing”（共有できる情報、共有しても支障のない情報にフォーカスしよう）

サイバー脅威の現状と対応

- 目的を持った執拗な攻撃
  - 情報流出
  - 経済的利益
  - 特定の目的
- 組織的・有機的・自立的な攻撃
- 攻撃主体分析とそれを踏まえた対応
  - 脅威への対応のためには、脅威の分析が重要
  - サイバー攻撃（脅威）の発生メカニズムの把握
  - 武力攻撃、テロ、犯罪、示威行動等も含め目的の把握の重要性
  - 攻撃主体は人間であり、それを踏まえた対応

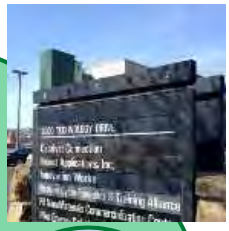
NCFTA

- NCFTA(National Cyber-Forensics & Training Alliance)は、One Team, One Goal.を掲げ、FBI等の法執行機関、民間企業、学術機関を構成員として米国に設立された非営利団体

- サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施している。設立以来300を超えるサイバー犯罪の対処に貢献している。

米国NCFTAとは

NCFTA = National Cyber-Forensics & Training Alliance



サイバー空間の脅威の深化

↓

法執行機関・民間企業・学術団体の連携による効果的対応の必要性

↓

NCFTAの設立

設立

平成9年設立
（米国ピッツバーグ）

組織

法執行機関・民間企業・学術団体を構成員とする非営利団体

目的

産学官における情報共有と協力の促進によるサイバー空間の脅威の効率的な特定、軽減及び無効化

機能

- サイバー犯罪に係る情報の集約と分析
- トレーニングの提供
（諸外国の捜査機関の捜査員が参加） 等

米国NCFTAとは

NCFTA Initiatives

CyFin 金融犯罪

The CyFin initiative is dedicated to identifying, mitigating, and neutralizing cyber threats targeting the financial services industry. As a predecessor to the initiative, the Stock-Aid initiative was started in February 2007 in an effort to provide a collaborative forum in combating online stock manipulation schemes. The "account compromise" aspect of this initiative stemmed from phishing [...]

Malware & Botnet マルウェア・ボットネット

The Malware & Botnet initiative is dedicated to better understanding the technology and identifying individuals or groups who utilize malicious code to enable crimes. The NCFTA maintains a collection of data regarding malicious code incidents, the network architecture being utilized to execute the schemes, and the communication channels implemented in these architectures. [...]

IPR Retail 知的財産権

The utilization of the Internet for the sale of counterfeit merchandise is a serious problem for US manufacturers and customers. In order to aid in the mitigation of this problem, NCFTA has partnered with the National Intellectual Property Rights Coordination Center (NIPRC) to provide comprehensive and actionable intelligence on individuals/groups involved in the distribution of [...]

Internet Fraud Alert インターネット詐欺アラート

What is Internet Fraud Alert? Internet Fraud Alert (IFA) is a system that functions as a centralized clearinghouse and alerting mechanism allowing trusted participants to report compromised credentials that have been uncovered online. Once reported, IFA will issue an alert to the relevant financial institution or other service provider indicating its customer's credentials have been [...]

Pharmacy 薬物

In order to address the serious and growing problem of illicit online pharmaceutical sales, the NCFTA established the Pharmaceutical Fraud Initiative (PFI), in partnership with the Federal Bureau of Investigation's Cyber Initiative and Resource Fusion Unit (CIRFU), and the Internet Crime Complaint Center (IC3). The purpose of this initiative is to provide a neutral forum [...]

（NCFTAウェブサイトより）

JC3設立とその活動へのニーズ

- **近年、脅威の質が変化して深刻化**
  - 国の治安や安全保障に重大な影響を及ぼしかねない状況
  - 執拗かつ組織的・有機的な攻撃と脅威の大本への対応の必要性
  - 極めて急速かつ広範に展開、国境に関係なく世界規模
  - **攻撃者を把握しこれに連携して対抗する必要性の高まり（アトリビューションの重要性）**
- **近年の脅威に対する、産業界、学術機関、法執行機関を含む官の、総力戦の流れ**

- **セキュリティ関連団体による対策検討の助言、脅威分析、注意喚起等の情報発信**
- **産学官連携の新たな枠組みが必要**
  - 各主体の対処経験を集約・分析した情報を共有
  - 脅威の大本を無効化し、以後の事案発生を防止する対応
  - 海外機関との連携、有益な情報収集と発信

産業界

強み
- 実被害の情報やそれに基づく知見を有している

弱み
- サイバー犯罪を敢行している被疑者の検挙等の脅威の大本を無効化する手段は有していない

法執行機関（警察）

強み
- 犯罪捜査等の警察活動を通じて得られる、限られた範囲でのサイバー空間の特定の脅威についての詳細な知見は有している
- 証拠の差押えや被疑者の逮捕を始めとする捜査権限の行使が可能

弱み
- サイバー空間全体を俯瞰できているわけではなく、情報の把握には限界がある

学術機関

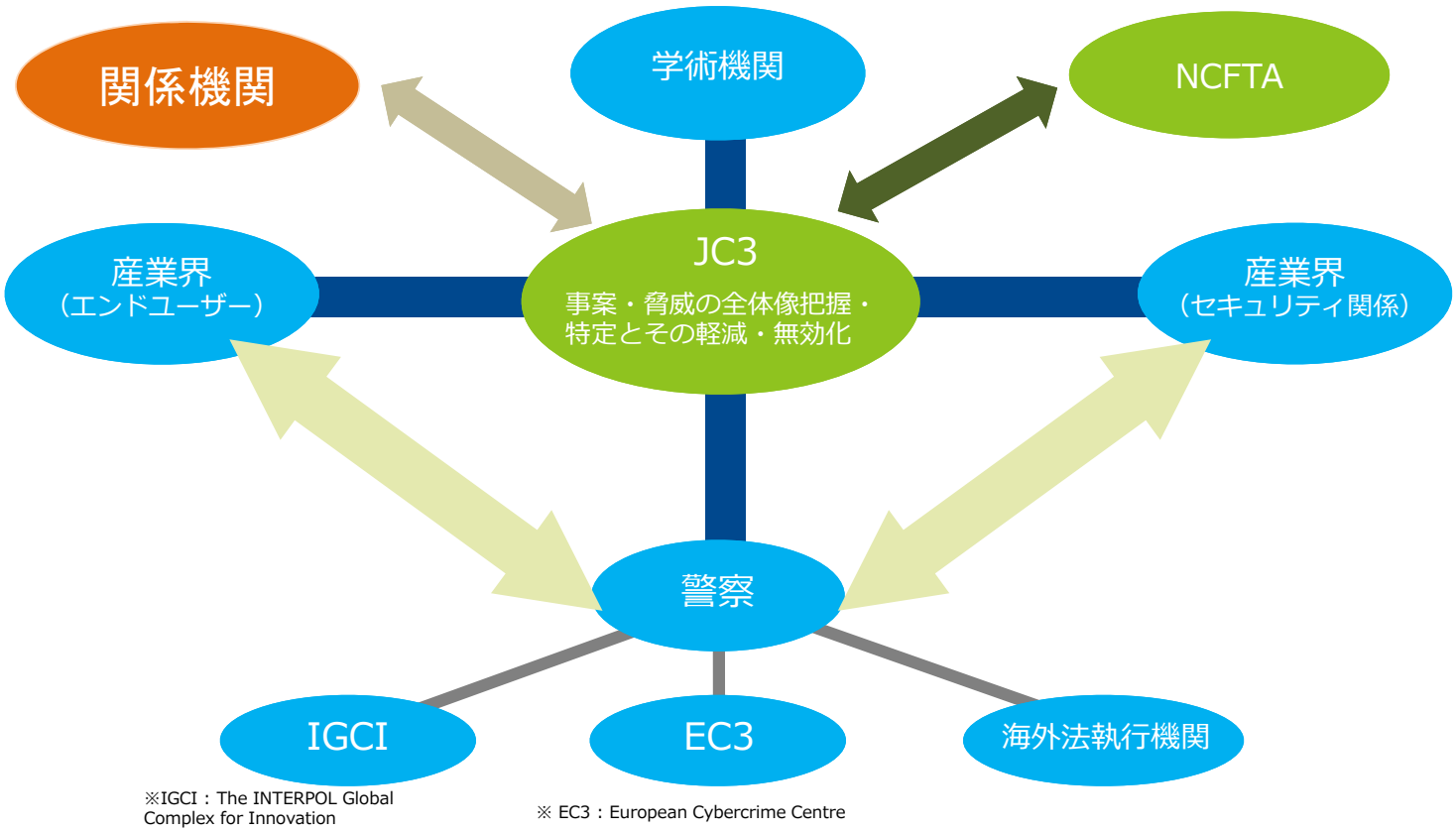
強み
- 研究成果の蓄積に基づく高度な情報通信技術や知識等を有する

弱み
- 産業界や警察との情報共有が必ずしも十分でなく、サイバー空間の脅威との「実戦」において、その真価を発揮できていない

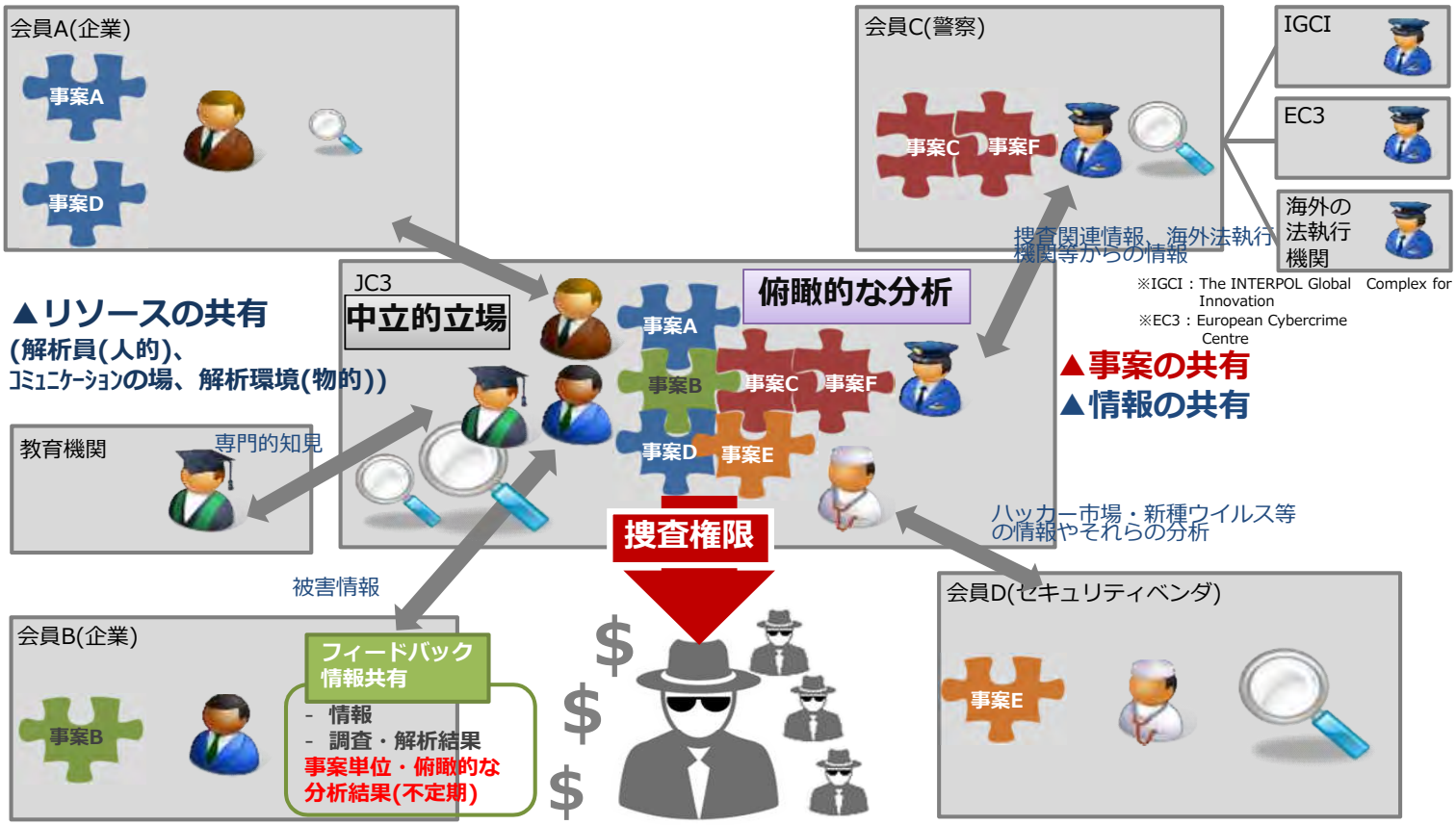
JC3設立の経緯と現在の位置付け

- **サイバーセキュリティ戦略**
  （平成２５年６月１０日　情報セキュリティ政策会議）
- **サイバーセキュリティ２０１３**
  （平成２５年６月２７日　情報セキュリティ政策会議）
- **「世界一安全な日本」創造戦略**
  （平成２５年１２月１０日　閣議決定）
- **平成２５年度総合セキュリティ対策会議報告書**
  （平成２６年１月３０日　総合セキュリティ対策会議）
- **サイバーセキュリティ２０１４**
  （平成２６年７月１０日　情報セキュリティ政策会議）
- **サイバーセキュリティ戦略**
  （平成２７年９月４日　閣議決定）
- **サイバーセキュリティ２０１５**
  （平成２７年９月２５日　サイバーセキュリティ戦略本部）
  「警察庁において、サイバー空間の脅威に対処するため、日本版NCFTAであるJC3等を通じた産学官連携を促進」

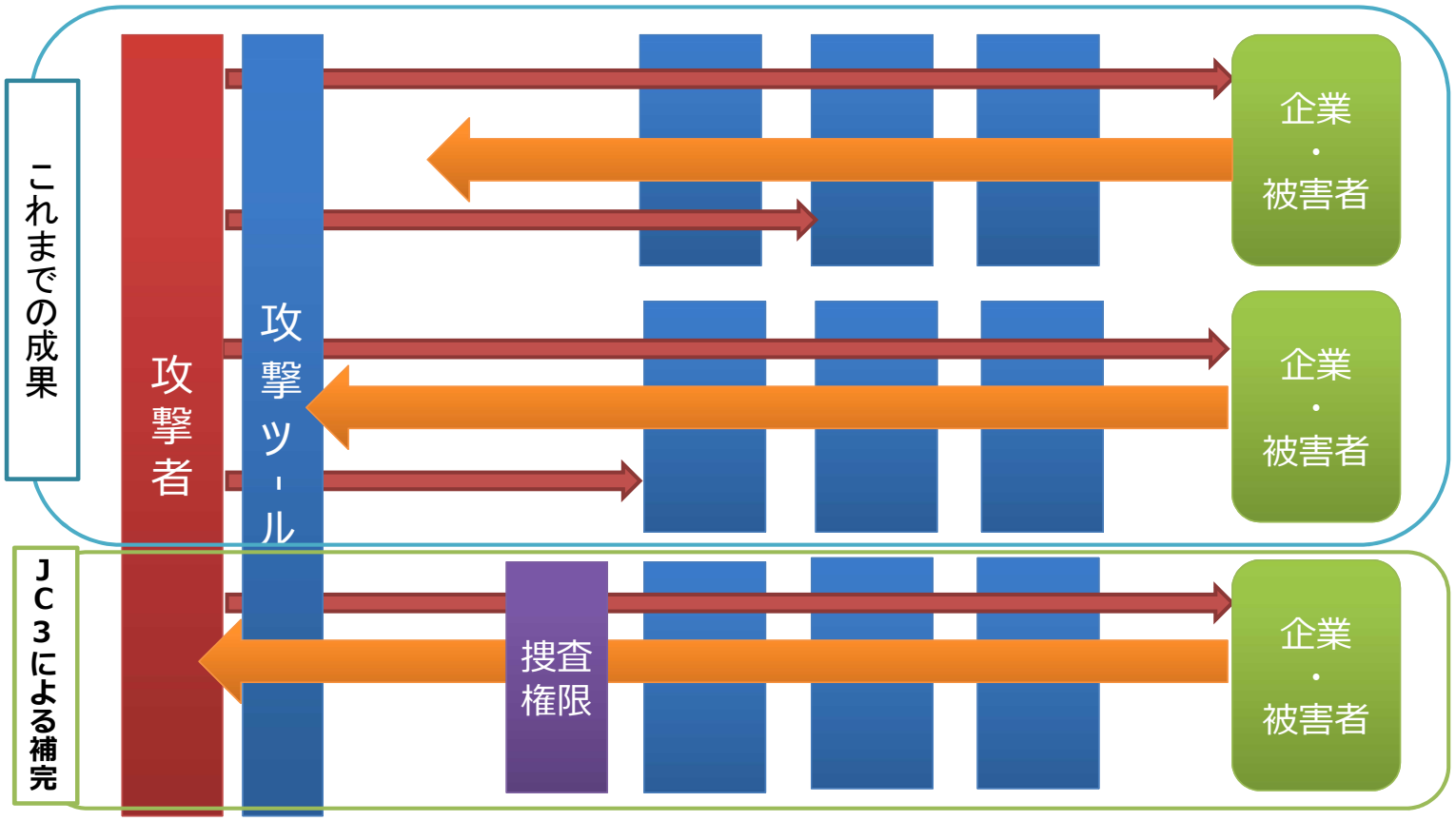
JC3における情報・知見の共有スキーム



JC3の概要～情報共有により目指す成果



JC3の役割



JC3の特徴

1. **分野（産業等）横断的な組織間連携を行うこと**
   - ✓ 特定の産業だけでなく、分野横断的に連携を行うことで、サイバー空間全体の脅威を俯瞰することを目指す
   - ✓ 産業界、学術研究機関、法執行機関（警察）による協働・他の組織との連携
2. **“Face to Face” の関係を重視していること**
   - ✓ 直接対面する場を設け、情報を共有
   - ✓ ＮＤＡ（秘密保護協定）を締結して情報共有を行い、また、直接対面して「信頼関係」を構築することにより、情報を適切に保全（＝情報の提供を促進）
3. **法執行機関（警察）が加わっていること**
   - ✓ 産学がそれぞれの特性と能力を発揮することと併せて、法執行機関にもその権限を活用してもらい、これまで分からなかった脅威の実態解明や脅威の無効化・無害化を目指す

サイバー関係情報共有のプラットフォーム

（出典:IGCI中谷局長プレゼンテーション　訳：坂）

	法執行機関など	民間	法執行機関が関与する多機関連携
国単位	IC4	FS-ISAC Telecom-ISAC	NCFTA JC3 CARA
地域	Europol J-CAT	FS-ISAC Telecom-ISAC	EC3
グローバル		FS-ISAC Telecom−ISAC	IGCI MS Cybercrime Center

米国NCFTAとの関係

- 産学官の連携の重要性の高まり
  → さまざまな形で具体的な脅威追及に向けた取組が進行
- EC3　European Cybercrime Centre
  民間企業との協定など
- IGCI
  民間からの出向者と協働しての知見共有・捜査支援
- オランダ警察
  金融犯罪対応のための警察への金融機関からの常駐体制
- JC3は、NCFTA型の協働体制では米国外で初めてのもの。
- NCFTAとの協力関係により目的の実現を推進。

NCFTAにおける情報共有

- サニタイズされたデータを共有
  - データベースシステムなど、脅威の特定・軽減・無効化につながる情報共有・蓄積のための仕組みを用意
- 情報共有の意義
  - 民間の立場から情報を共有・集約・分析し、役立てると共に、法執行機関の活動を促す。
    その際、NCFTAは、そのための活動が効果的に実施されるように、戦略的に態勢を構築
- 脅威の特定・軽減・無効化に向けた情報共有
  - 法執行機関の存在

NCFTAプレジデントのお話より

- マリア・ヴェロさんの講演録（警察學論集第67巻5号、平成26年5月、講演自体は平成25年9月）
- **NCFTAの使命と基本姿勢**
- 我々の使命を表現する言葉は、非常に短く、非常に実際的です。それは、“One Team, One Goal”です。民間企業、学術機関、法執行機関がグローバルに連携し、サイバー空間における脅威を無効化するのです。ここで言う「無効化」とは、被疑者の逮捕、資産や資金の押収を意味しています。
- サイバー犯罪を敢行する者は非常に創造性や冒険心が豊かです。新たな手口が次々に考案され、サイバー空間の脅威はますます複雑・高度化しており、我々は常に彼らから一歩遅れています。このため、犯罪被害を回避する、事後の発生を抑止するという取組だけでは、その脅威を食い止めることができません。

NCFTAプレジデントのお話より(続き)

NCFTAの使命と基本姿勢（続き）

- よって、より先制的かつ能動的に対応していくことが求められます。サイバー空間の脅威に関する情報をいち早く収集し、分析することが必要です。この点、サイバー空間の脅威には、民間－すなわち、企業と消費者が最初に接します。また、犯罪者からターゲットとされ、被害を受ける危険性が最も高いのも民間企業ですから、彼らが最も多くの情報を持っていると言えます。よって、NCFTAでは、”Industry First“（民間を第一に）を基本姿勢としているのです。
- NCFTAの本部・オフィスの双方で、産学官のメンバーが一緒に机を並べています。数歩歩けば対面で議論できるほど近くにお互いがいるからこそ、連携に必要な信頼関係が構築され、対話も進みますし、お互いに助け合うことが可能になります。NCFTAの基礎は、正にこうした信頼関係にあります。我々は、これが構築されやすくなるような環境作りに取り組んでおり、このようなコミュニケーションは、NCFTAでは日常的に行われていることなのです。

NCFTAプレジデントのお話より（続き）

NCFTAにおける脅威への対応の在り方（続き）

- 例えば、銀行で問題が発生したとの情報が一つ送られてくると、その裏に何らかの犯罪があるのではないかということで、数歩歩いて隣の机に行き、「これは変だ。これを見てくれ。」といったように、業界における見解、アナリストの意見、法執行機関の動きなどの情報をお互いに出し合って、多様な人材が即座に検討を進めていきます。
- もちろん、その際には、NCFTAとして焦点を当てるべきものであるかどうか、すなわち、時間とエネルギーとリソースを割いて対応すべきなのか、脅威の規模という点で優先順位も付けていきます。
- こうしたことが、すべてリアルタイムでなされることによって、いちはやく行動することができるのです。

JC3 Japan Cybercrime Control Center

NCFTAプレジデントのお話より（続き）

NCFTAにおける脅威への対応の在り方（続き）

- また、特定の銀行で発生している脅威が、今はその銀行のみに止まっていても、すぐに他の銀行を含めた銀行業界全体、更に製造業や流通業にも広がるといったように、業界を横断して攻撃を仕掛けてくる犯罪者もいます。
- 一つの企業又は一つの業界における被害額が１万ドルだったとしても、それが複数企業又は複数業界に渡ると被害額は大きくなります。被害金額から見れば、法執行機関は、被害額が大きければ大きいほどすぐに事件化すべきと考えますから、我々は、そうした側面からも情報収集をし、事件化を図ってもらうべきと判断したものを彼らに委ねていきます。
- もちろん、彼ら（法執行機関）も自ら情報を検証した上で、逮捕、資産の押収等適切な対処をしていくことになります。

NCFTA型の取組の特質

- **捜査権限をも活用して脅威の特定・軽減・無効化を図ることが目標であり、成果。**

- **特質**
  - 日常的な情報共有等による信頼関係の構築
  - 民間メンバーによるそれぞれの活動の展開
  - Industry First
  - どのような情報・対策が有効かの認識共有
  - 情報の集約・分析
  - 事案により具体的な協働
  - 問題事案への対処のための取組
- **取組のための体制・態勢を生成**

One Team、One Goal

- **our mission to identify, mitigate and ultimately neutralize cybercrime, threat in cyberspace.**

- **一つの目標に向かって、一丸となって**
- **サイバー脅威の特定、軽減、無効化に向けて**

米国NCFTAの成果

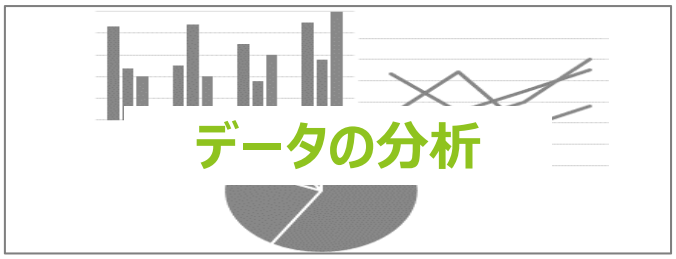
- **捜査権限をも活用して脅威の特定・軽減・無効化を図ることが目標であり、成果**

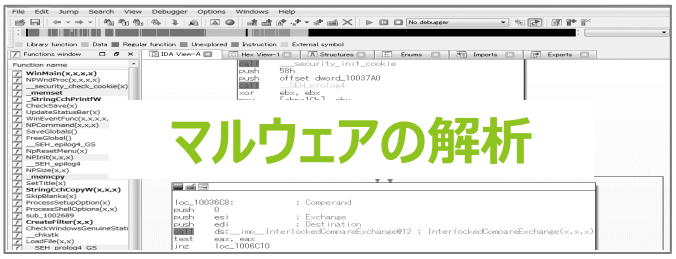
- **事件検挙**
  - 以後の事案発生を防止
  - 犯罪組織・手口の把握とそれを踏まえた対応
- **差押え**
  - 資産（被害回復にも繋がる）、攻撃リソース

- **さまざまな権限の活用**

- **情報共有による被害の防止**

JC3の活動

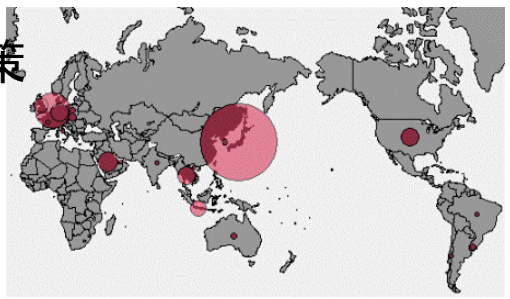




（参考）警察と民間事業者が連携した取組

- 平成27年4月、警視庁が、主に日本を標的としているとみられるネットバンキングウイルスの感染端末に関する情報を入手し世界で約8万2,000台うち国内で約4万4,000台の端末を特定したと発表。
- 日本独自としては初の大規模なボットネットテイクダウンの取組
- 「ネットバンキングウイルス無力化作戦」と名付け、セキュリティ事業者の協力を得て、ウイルス感染端末の不正送金被害を防ぐための対応策を講じている。

- 総務省の官民連携による国民のマルウェア対策支援プロジェクト（ACTIVE）と
も連携し、プロバイダ等を通じ感染端末
の利用者に対してウイルスの駆除を依頼。



JC3の活動の展開

- **脅威の実態解明に資する情報共有・分析**
  - 深い情報共有・分析による脅威の全体像の把握と対策の検討（現時点において対応上問題となっているポイントの把握も含む）
- **JC3の環境を活用した脅威の特定・軽減・無効化活動の展開**
  - 例:海外サーバー事案
- **具体的な脅威の特定・軽減・無効化活動に資する情報共有等**
  - 情報の共有・分析やJC3プラットフォームを活用した対応の展開
- **協働による能力の向上**
- **NCFTAとの連携による活動の展開**
- **さまざまな問題事象の相談対応**
  - 新たな課題となり得る問題事象について、官民で連携して対応

ありがとうございました

捜査関係事項照会等への
ヤフー株式会社の対応について

ヤフー株式会社 社長室
コーポレート政策企画本部

2016/1/27

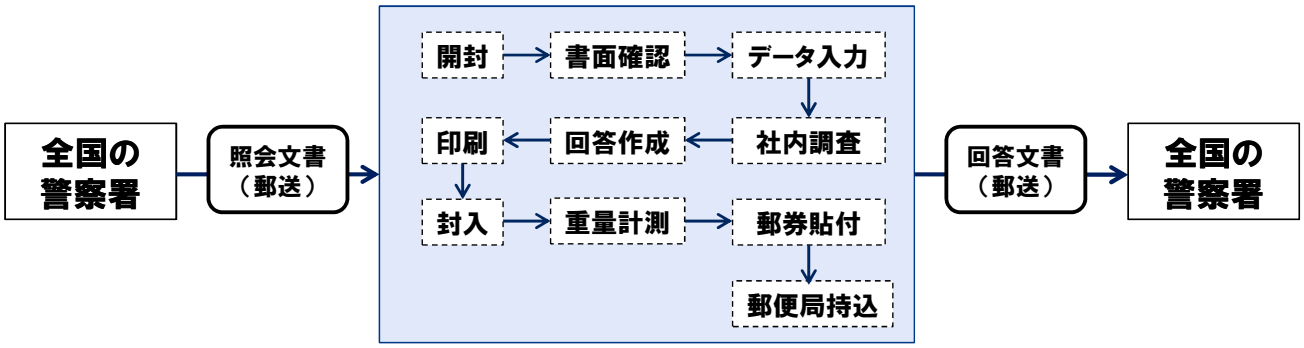
1．照会・差押え対応の現状

1－1. 照会の現状

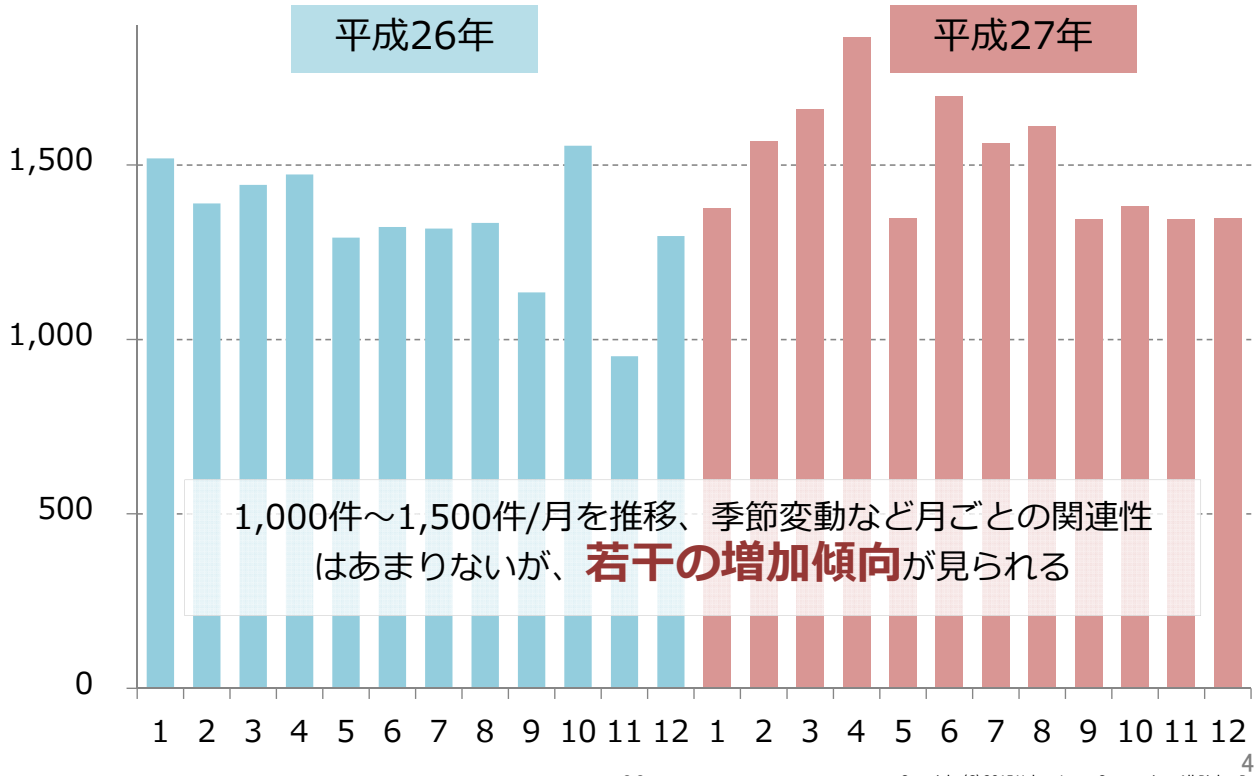
18,103 件（平成27年）

月間1,000～1,500件、6名で対応

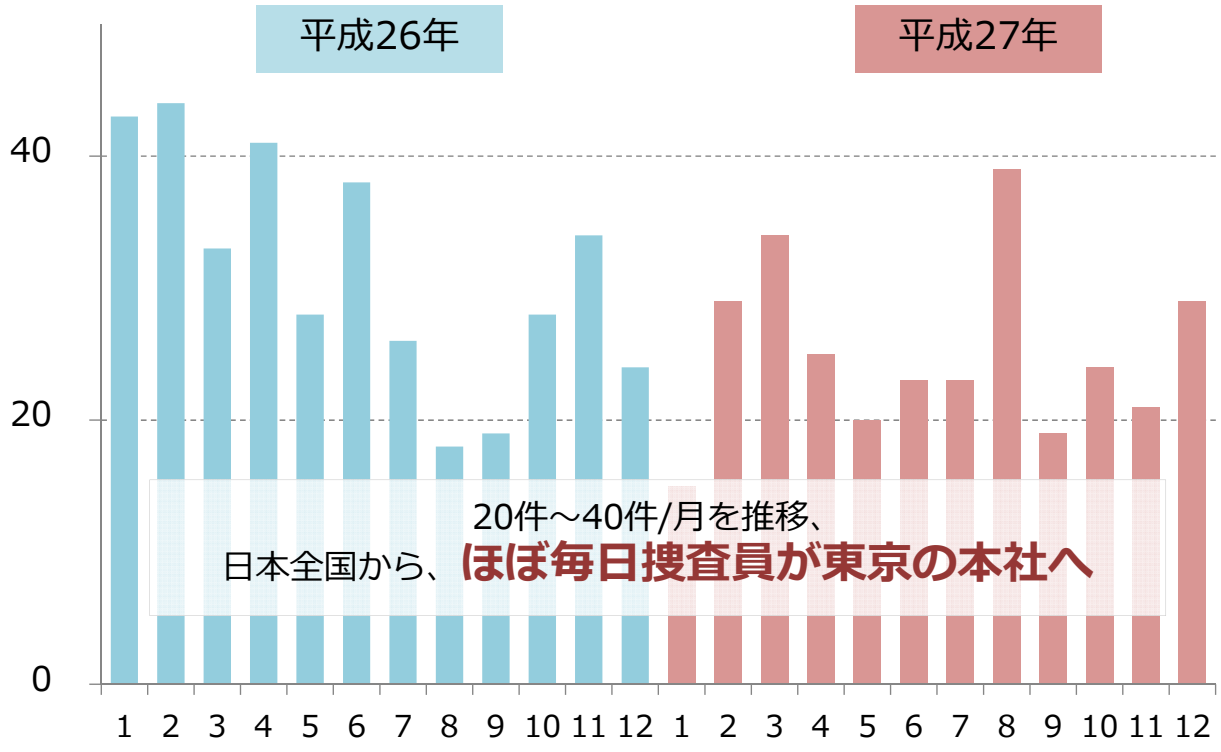
事業者内の対応



1－2. 照会件数の推移



1－3. 差押え件数の推移



2. 現状の課題、電子化のメリット

2－1. 処理スピード・量の向上

現状の課題

- 郵送作業によるタイムラグ
- 膨大なデータの取り扱いによるタイムラグ

例）事業者が膨大なログデータを紙に大量に印刷して郵送し、受け取った警察側で再度入力作業を行う　等

電子化のメリット

- リアルタイムに近い照会が可能となり捜査全体のスピードが向上
- 大量のデータの処理も容易に

2－2. 正確性、管理性の向上

現状の課題

- 郵送作業や入力作業（紙→デジタル）に伴うヒューマンエラーの発生の可能性
- 紙の情報の管理上の問題

例）紛失のリスク、アクセス状況の把握が困難　等

電子化のメリット

- ヒューマンエラーの防止
- 機械的にエラーをチェックする仕組みの導入も可能
- 紛失、対応漏れ等の解消
- 管理性の向上

例）誰がどの情報にアクセスしたかの把握、不正の排除　等

２－３．コストの低減

現状の課題

- 照会や差押えにあたる人員の人件費
- 郵送費

電子化のメリット

- コストの低減
  - 人件費（約2,000円／1件）の低減
  - 郵送費の低減

２－４．データ活用・分析

現状の課題

- 同じ内容の照会が各警察署から重複して寄せられる
- 過去に照会・回答した内容が参照・分析されにくく、その後の捜査に活用されにくい

電子化のメリット

- 蓄積される照会・回答のデータを各警察署が容易に参照可能となることで、重複した照会が不要に
- 都道府県警察が相互に捜査状況を把握することが容易になり、捜査の連携が促進される

まとめ – 電子化のメリット

- 照会の迅速化
- データ処理の効率化
- 誤記、紛失、対応漏れ等の解消
- 管理性の向上
- 都道府県警の連携促進

3. 期待する検討の方向性

- 今後も拡大・高度化が見込まれるサイバー犯罪に効果的に対処するため、現在の制度や運用に縛られることなく、将来的に必要とされる制度と電子化が併せて検討されることを期待。
- 例えば、「紙・郵送」の置き換えとしての電子化（例：照会書や令状のメール・FAX送付）ではなく、「紙」を前提とした決裁等の業務の見直し、データ活用しやすいシステムの導入等、新たな取り組みが進むことを期待。
- 一度に全ての課題に着手することは困難であるため、優先順位を定め、中長期のスケジュールを策定して着実に検討・実行が進められることが、併せて必要。

警察機関との協調による Telecom-ISAC Japanの活動について

2016年1月27日

一般財団法人日本データ通信協会
テレコム・アイザック推進会議
佐 藤 晴 樹

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Telecom ISAC Japan

Telecom-ISAC Japan の概要

Telecom-ISAC Japanの概要

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

https://www.telecom-isac.jp/

- 2002年7月に日本で最初のISACとして発足
- 通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、業界横断的な問題に対してタイムリーな対策をとる場を提供する活動を行う
- 世界に広がるサイバー空間の中で、「日本(jpドメイン)」が消失しないようサイバー脅威からネットワークを守る
- 単独では手に負えない大規模なサイバー脅威に共同で立ち向かう「互助会型」の通信事業者連携
- ビジネス競合関係にある国内大手ISPが会社の壁を越えて協力、連携するための会費会員制の民間組織

会員企業（2015年10月末現在）

緑文字はISP or 通信事業者を示す

会長：	飯塚　久夫
副会長：	中尾康二（KDDI）、山下達也（NTT コミュニケーションズ）、井手康彦（日本データ通信協会）
会員企業：(20)	日本電気株式会社、NTTコミュニケーションズ株式会社 、KDDI株式会社、株式会社NTTドコモ、株式会社インターネットイニシアティブ 、ニフティ株式会社、株式会社日立製作所、沖電気工業株式会社 ソフトバンク株式会社、東日本電信電話株式会社、西日本電信電話株式会社、日本電信電話株式会社 株式会社KDDI研究所 、ビッグローブ株式会社 、富士通株式会社、インターネットマルチフィード株式会社 NTTコムセキュリティ株式会社、エヌ・ティ・ティ・データ先端技術株式会社、ソネット株式会社 株式会社ケイ・オプティコム
アライアンスメンバー：(11)	株式会社ラック 、日本アイ・ビー・エム株式会社、トレンドマイクロ株式会社 日本マイクロソフト株式会社、株式会社サイバーディフェンス研究所 株式会社FFRI、株式会社情報通信総合研究所 一般社団法人日本ネットワークインフォメーションセンター 、BBIX株式会社 日本インターネットエクスチェンジ株式会社、NRIセキュアテクノロジーズ株式会社
オブザーバー：(5)	総務省、国立研究開発法人情報通信研究機構(NICT)、 一般社団法人日本インターネットプロバイダ協会(JAIPA) 一般社団法人テレコムサービス協会、一般社団法人電気通信事業者協会(TCA)

Telecom-ISAC JapanのWG/SiGの設置状況

WG (11)

1-1) ACCESS-WG　2007年4月設置
インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換

1-2) SoNAR-WG　2007年12月設置
ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定

1-3) DoS攻撃即応-WG　2011年10月設置
DoS攻撃への迅速な対応と複数事業者による協調対処の仕組みの検討。日本国内におけるDoS攻撃発生の、予測、早期検出、迅速かつ適切な対応の実現を目指す。

1-4) ルータ脆弱性問題-WG　2012年07月設置
危険な脆弱性を保有する特定ルータに対する具体的な対応の検討と調査を実施

1-5) 脆弱性保有ネットワークデバイス調査-WG　2013年05月設置
国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施

1-6) サイバー攻撃等への適正な対策方法検討-WG（通秘-WG）　2013年12月設置
電気通信事業の業務を整理し通信の秘密に代表される法的な整理を行うことを目的とする

3-1) 経路情報共有-WG　2005年7月設置
ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用

4-1) サイバー攻撃即応スキーム検討WG（国際サイバーWG）　2011年12月設置
マルウェアやDDoSなどの様々なサイバー攻撃情報をISP間およびセキュリティ関連機関と共有し、予知・即応可能なサイバー攻撃対応スキームを検討

4-2) ACTIVE業務推進-WG　2013年07月設置
総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す

4-3) WiFiリテラシー向上-WG　2013年09月設置
電波の有効利用（オフロード推進）を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施

6-1) サイバー攻撃対応演習-WG(CAE-WG)　2009年5月設置
電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施

SiG (1)

DNS運用者連絡会-SiG　2008年6月設置
DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換

※SiG : Special interest Group

業界全体の大規模テイクダウン活動
（Game Over Zeus，VAWTRAKの駆除）

業界全体の大規模テイクダウン活動
ACTIVEプロジェクトの取組み

■ **ACTIVE（Advanced Cyber Threats response InitiatiVE）**

- ISPなどの事業者によって、約3000万人のインターネットユーザーを対象に、マルウェア感染防止・駆除の実証実験を行う官民連携プロジェクト
- 2013年11月から開始、現在ISP12社が参画中
- 総合的なマルウェア感染対策を官民連携で実施するのは世界初の試みであり、将来的には国際連携も視野

マルウェア感染防止の取り組み

① マルウェア配布サイト等のURL情報をリスト化
② マルウェア配布サイト等にアクセスしようとする利用者に注意喚起
③ マルウェア配布サイト等の管理者に対しても適切な対策を取るように注意喚起

マルウェア駆除の取り組み

① マルウェアに感染した利用者のPCを特定
② 利用者に適切な対策を取るように注意喚起
③ 利用者は、注意喚起の内容に従いPCからマルウェアを駆除

業界全体の大規模テイクダウン活動

ACTIVEプロジェクトの体制

ISP等の通信事業者やセキュリティベンダなど35社が参画

総務省

Telecom-ISAC Japan
プロジェクト統括・推進

株式会社インターネットイニシアティブ
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社エヌ・ティ・ティピー・シーコミュニケーションズ
株式会社NTTぷらら
エヌ・ティ・ティレゾナント株式会社
株式会社ケイ・オプティコム
KDDI株式会社
ソフトバンク株式会社
ソネット株式会社
ニフティ株式会社
株式会社ハイホー
ビッグローブ株式会社
北海道総合通信網株式会社
伊賀上野ケーブルテレビ株式会社
株式会社ティエイエムインターネットサービス
株式会社グローバルネットコア
北陸通信ネットワーク株式会社
沖縄ケーブルネットワーク株式会社
NRIセキュアテクノロジーズ株式会社
NTTコム ソリューションズ株式会社
エヌ・ティ・ティ・コムチェオ株式会社
エヌ・ティ・ティ・ソフトウェア株式会社
エヌ・ティ・ティラーニングシステムズ株式会社
株式会社FFRI
株式会社カスペルスキー
キングソフト株式会社
株式会社シマンテック
株式会社セキュアブレイン
ソースネクスト株式会社
トレンドマイクロ株式会社
日本電気株式会社
日本電信電話株式会社
日本マイクロソフト株式会社
株式会社日立製作所
マカフィー株式会社

（2015年11月末現在）

業界全体の大規模テイクダウン活動

世界的なGOZボットネットテイクダウン作戦への参画

- インターネットバンキング不正送金を行うマルウェア**「Game Over Zeus」**が世界的に蔓延し、日本国内でも推定約20万台の端末が感染。セキュリティ対策に対して強い耐性を持つP2P通信を利用したボットネットを使用しており、背後には高度な技術を有する組織的な犯行グループが存在
- **米国連邦捜査局（FBI）及び欧州刑事警察機構（ユーロポール）**が中心となり、協力国の法執行機関と連携した大規模なボットネットテイクダウン作戦を展開。_日本国内では警察庁の要請のもと、総務省・Telecom-ISAC Japan が協力し、会員ISPと連携してユーザへの注意喚起・駆除活動を行った

（2014年6月）

(出典)
警察庁ウェブサイト(http://www.npa.go.jp/cyber/goz/)

作戦の内容

- C&Cサーバ・中継サーバのテイクダウン
- テイクダウンしたC&Cサーバ上で感染端末からの通信を観測し、当該ユーザへの注意喚起を行う

業界全体の大規模テイクダウン活動

VAWTRAKボットネットテイクダウン作戦への参画

- 日本国内で約4万4000台（世界で約8万2000台）にのぼるインターネットバンキング不正送金を行うマルウェア「**VAWTRAK**」の感染を確認。日本国内が占める感染台数の割合やVAWTRAKの設定ファイルから主に日本が標的とされていることが確認された。
- 対策として日本独自で行う大規模ボットネットテイクダウンの取組では**国内初**となる、ネットバンキングウイルス無力化作戦を展開。総務省・Telecom-ISAC Japan が協力し、会員ISPと連携してユーザへの注意喚起・駆除活動を行った。

（2015年4月）

(出典)総務省ホームページ
(http://www.soumu.go.jp/menu_news/snews/01ryutsu03_02000092.html)

(出典)ACTIVEホームページ
(http://www.active.go.jp/active/news/release/entry-231.html)

(出典)Telecom-ISAC Japanホームページ
(https://www.telecom-isac.jp/news/news20150410.html)

作戦の内容

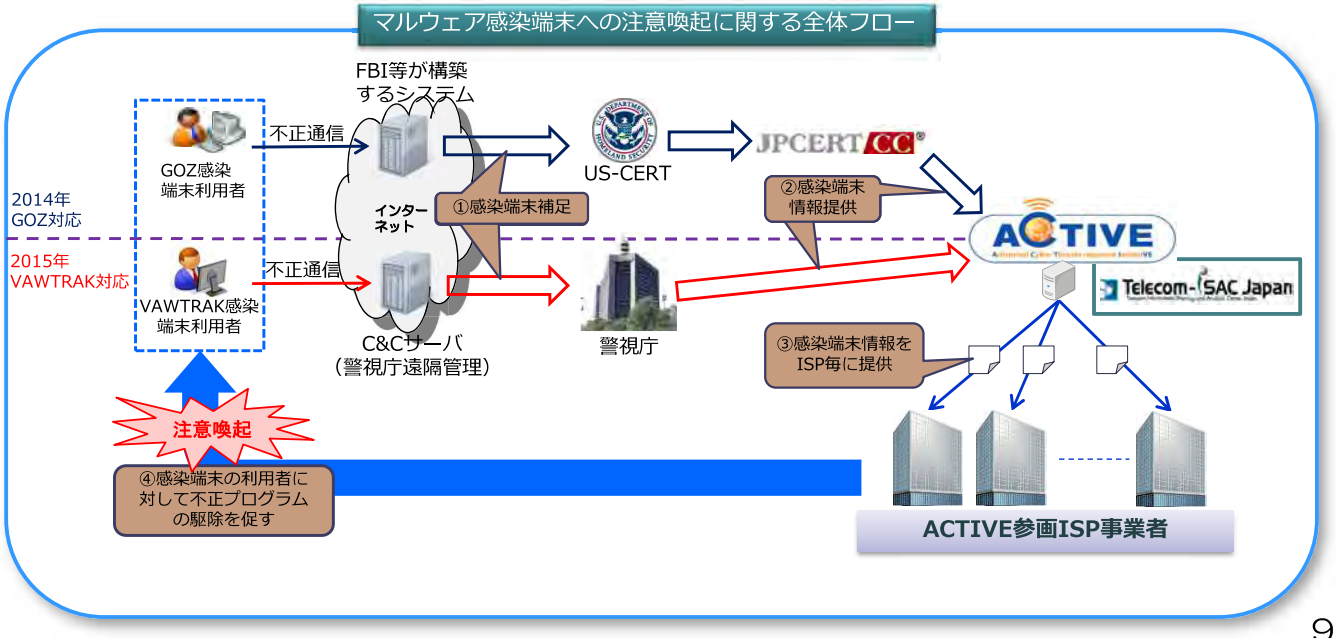
- 感染端末を利用するユーザへの注意喚起・駆除依頼の実施
- 感染端末上のVAWTRAKの無力化

8

業界全体の大規模テイクダウン活動

ACTIVE(T-ISAC-J)を通じた各ISPの取組み

- JPCERT/CCや警察などから各ISP事業者へ連絡を行うことは負担が大きいと判断し、Telecom-ISAC Japanが主管するACTIVEにて、これらの案件の窓口・とりまとめを行った。
- 感染端末への注意喚起は、「GOZ」「VAWTRAK」いずれの取組みの場合も関係各所（JPCERT/CC，警視庁）からの情報をTelecom-ISAC Japanが窓口として一元的に受け取ったのち、ACTIVEのデリバリラインを活用して各ISP事業者に対して情報提供を行っている。
- 各ISP事業者は、提供された感染端末情報を基に利用者への注意喚起および駆除依頼を実施している。



9

業界全体の大規模テイクダウン活動

警察情報によるGame Over Zeus駆除について

インターネットバンキングに係るマルウェア（Game Over Zeus）に関する作戦において得られた当該マルウェアへの感染端末に関する情報を元に、ACTIVEの取組を活用して、国内ISP事業者に対して感染者に関する情報提供を行い、各ISP事業者から利用者への注意喚起を実施。

リスト配布先：　１４の協力先に配布

	1回目	2回目	3回目	4回目	合計
JPCERT/CC からの受領数	1,320	19,482	46,718	88,001	155,521
１４協力先への送付数	839	13,028	31,725	58,647	104,239
JPCERT/CC　への返却数	481	6,454	14,993	29,354	51,282
T-ISAC-J　での対応率	63.60%	66.90%	67.90%	66.60%	67.00%

複数のISP事業者に対し、４回にわたり情報提供を行い、合計104,239の感染端末情報を提供

業界全体の大規模テイクダウン活動

警察情報によるVAWTRAK駆除について

インターネットバンキングに係るマルウェア（ VAWTRAK ）に関する作戦において得られた当該マルウェアへの感染端末に関する情報を元に、ACTIVEの取組を活用して、国内ISP事業者に対して感染者に関する情報提供を行い、各ISP事業者から利用者への注意喚起を実施。

リスト配布先：　１６の協力先に配布

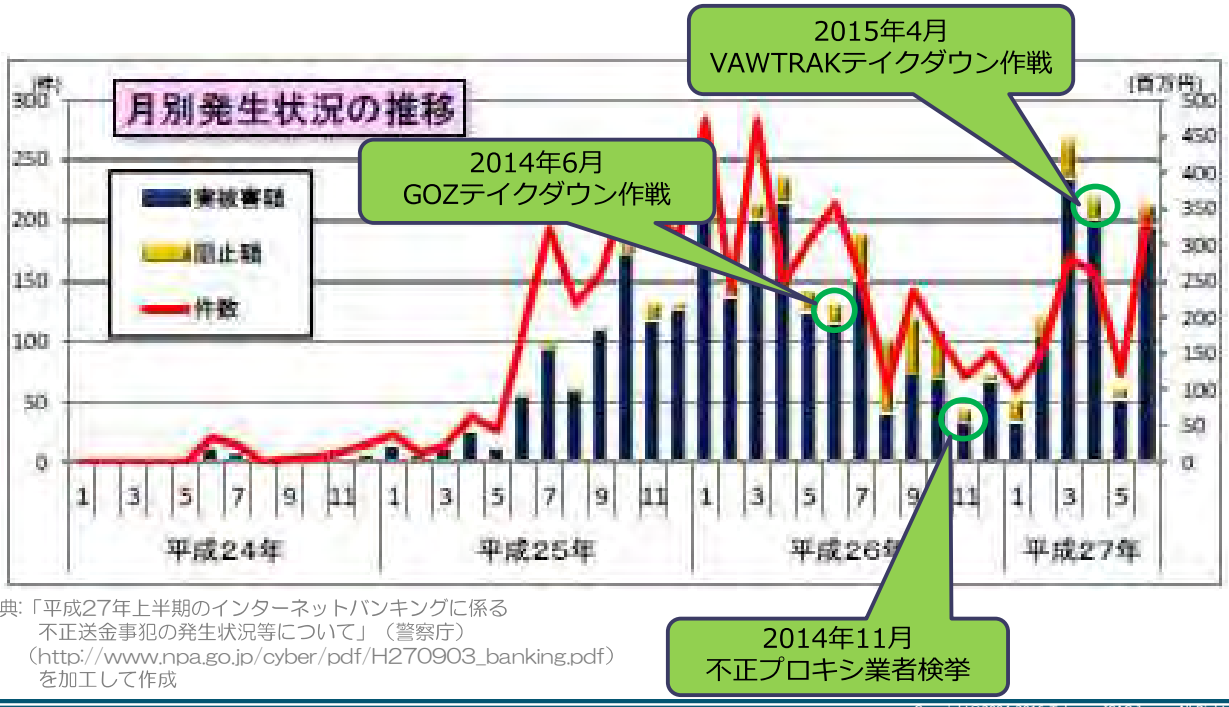
	合計
警視庁からの受領数	43,565
１６協力先への送付数	33,196
警視庁への返却数	10,369
T-ISAC-J　での対応率	76.20%

複数のISP事業者に対し、情報提供を行い、合計33,196の感染端末情報を提供

業界全体の大規模テイクダウン活動

[2015年]ネットバンキング不正送金被害

- 平成27年度（2015年）上期の被害額（実被害額）：15億4400万円（13億7500万円）
- 平成26年度（2014年）の大規模なテイクダウンや一斉検挙の取組みにより、一時的に被害額が低減したものの平成27年度上期にはまた、平成26年度上期と同一水準に戻っている。
- 上記の状況を踏まえると、今後も継続して同様な取組みを行っていく必要があると想定。

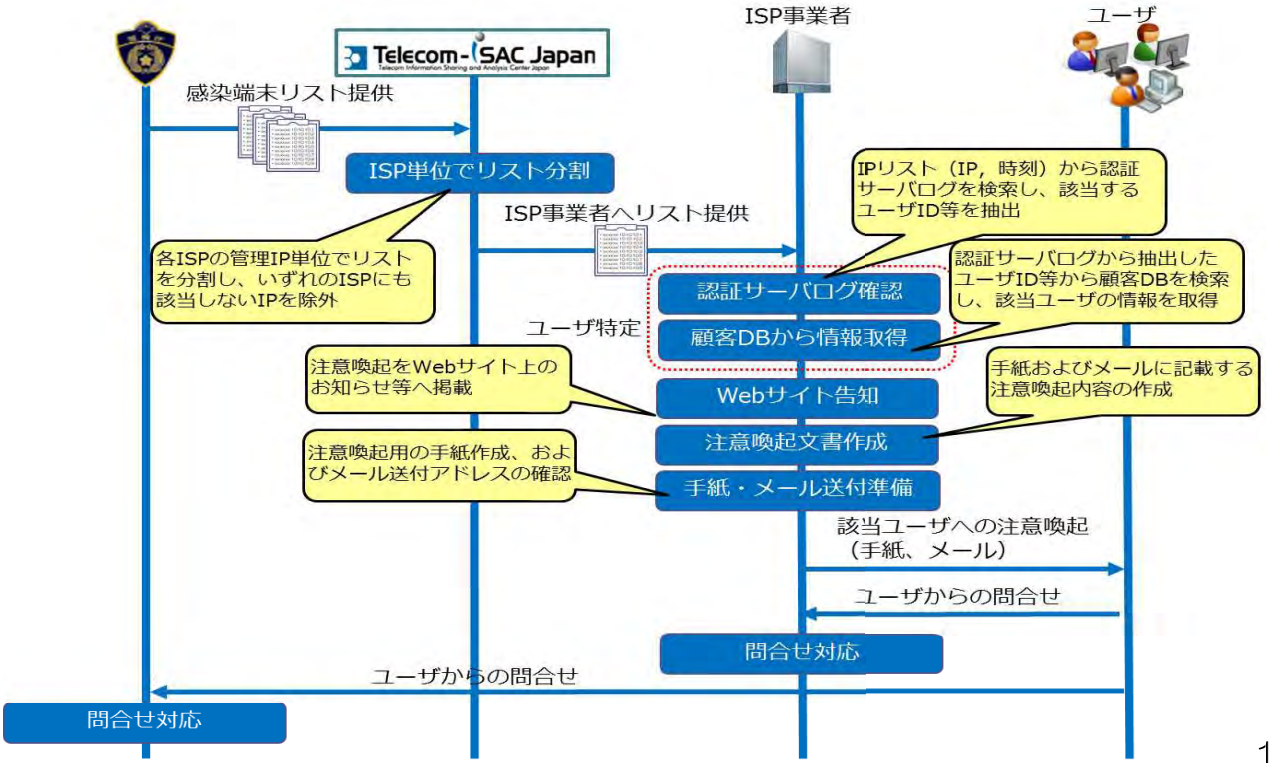


出典:「平成27年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について」（警察庁）（http://www.npa.go.jp/cyber/pdf/H270903_banking.pdf）を加工して作成

業界全体の大規模テイクダウン活動

各ISP事業者から利用者への注意喚起フロー

インターネットバンキングに係るマルウェア（ GOZ，VAWTRAK ）に関するユーザへの注意喚起においては、その対応数の多さおよび対応作業の煩雑さから、多くの作業稼動が必要。



不正プロキシサーバ業者摘発と脆弱性を有する ブロードバンドルータ問題

問題となったブロードバンドルータの脆弱性

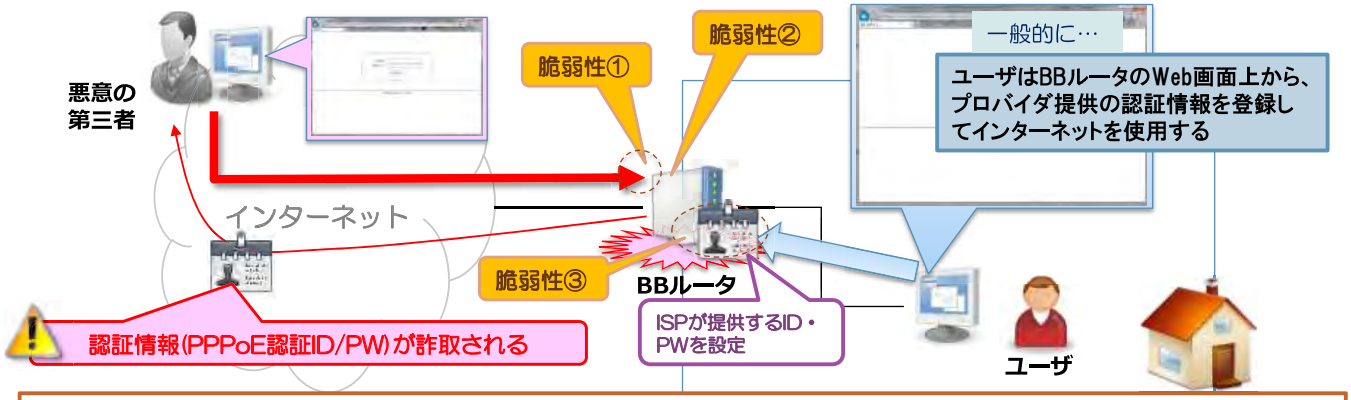
- L社製ルータ問題では、多くのNWデバイスに搭載されているWeb管理画面のID/パスワードが周知のもの、もしくは容易に推測可能であることを利用して、悪意の第三者によるWeb管理画面への不正アクセスが行われた

■問題該当機種

ロジテック株式会社「300Mbps無線LANブロードバンドルータ」
3機種

LAN-W300N/R　LAN-W300N/RS　LAN-W300N/RU2
（2009年8月発売）（2011年7月発売）（2010年2月発売）

3機種とも、
シリアルナンバーの末尾 「B」
ファームウェアバージョン 2.17

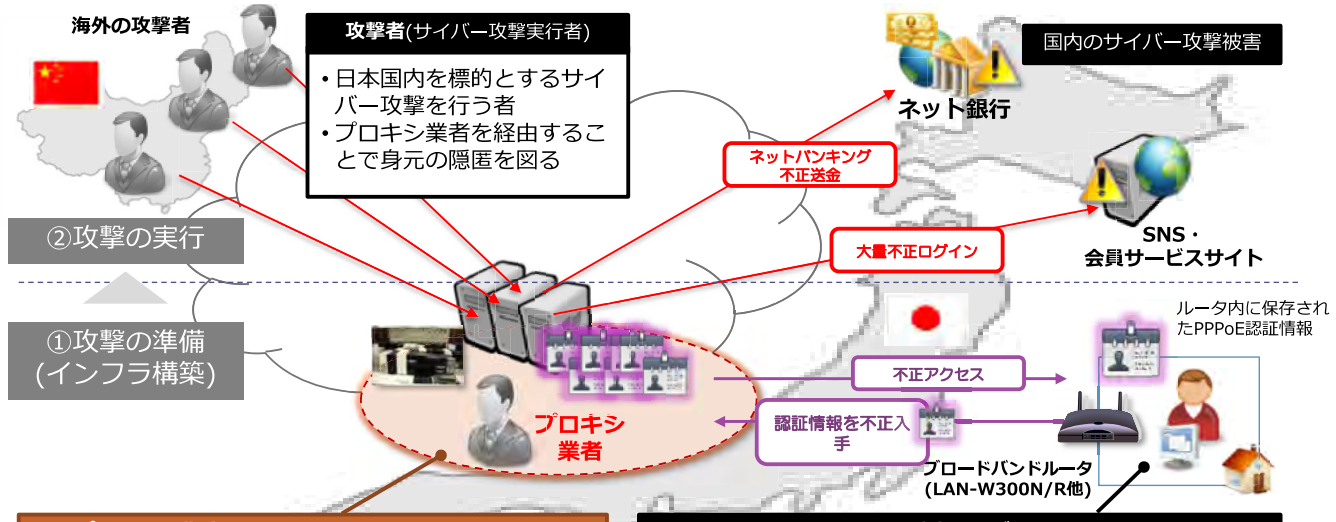


■L社ルータ問題の該当機種に実在するセキュリティ脆弱性

① WAN(インターネット)側からBBルータ管理画面へアクセス可能
② BBルータ管理画面の初期ID/PWが"admin","password"のように平易なもの
③ BBルータ管理画面上において、設定されているISP提供のPPPoEアカウント(ID/PW)情報が容易に読み取り可能な状態(平文)で保存されている

不正プロキシサーバ業者摘発と脆弱性を有するブロードバンドルータ問題

不正プロキシ事案の登場人物と全体構成



プロキシ業者(=中都商事、大光、SUNテクノ等)

- 中国など海外の攻撃者に対し、プロキシ"サービス"を提供する事業者
- プロキシサービスのインフラに、被害ユーザから窃取したPPPoE認証情報を利用した「なりすまし回線」を大量に設置し、巨大な「身元隠匿プロキシ」を構築

被害ユーザ

- 問題のロジテック社製ルータ(LAN-W300N/R他)を使用していたインターネット(NTT東西のFlet's)利用者
- プロキシ業者から行わる不正アクセスによってFlet's回線のPPPoE認証情報(認証ID/パスワード)が詐取される
- 認証情報を不正利用されていても、被害ユーザ自身の通信には影響が無い為、本人は気付かない

犯行手口

1. プロキシ業者は被害ユーザのブロードバンドルータへ不正アクセスしてアカウントを詐取。詐取情報を利用してISPへインターネット接続(PPPoE認証)することで、被害ユーザになり済ました不正接続回線を構築
2. 「1.」の回線を大量に確保したインフラを構築し、「プロキシサービス」として提供。海外の攻撃者は当サービスを利用し、身元隠匿を図った上で、日本国内のWebサイトを標的としたサイバー攻撃を実施

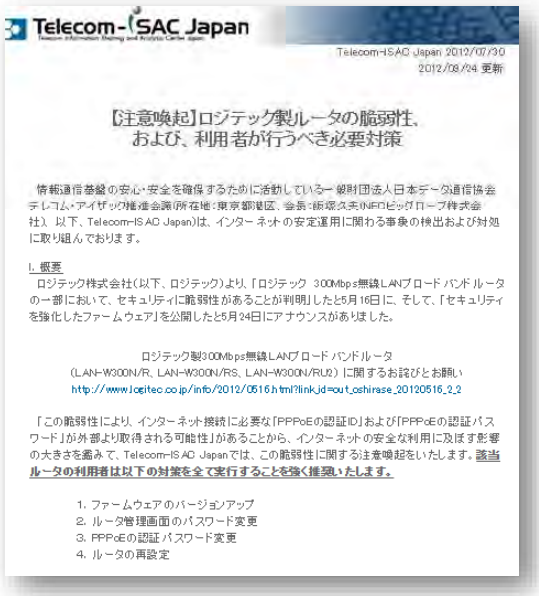
16

不正プロキシサーバ業者摘発と脆弱性を有するブロードバンドルータ問題

事件解決に向けたTelecom-ISAC Japanの取組み

- 2012年7月より、数回にわたり事件に関連するブロードバンドルータの脆弱性について注意喚起を実施し、ファームウェア更新等の対策実施をユーザ側へ促したものの、実施ユーザが一部に留まることで被害拡大が継続。
- 2013年6月からは、該当製品の所在を把握するネットワーク調査を実施し、ユーザ側へより積極的に対策実施を促す活動を展開
- 会員ISPと連携して警察側の捜査へも対応、事件全貌の解明、犯行グループの摘発へ貢献

不正利用されたルータの脆弱性に関する注意喚起(2012年)


Telecom-ISAC Japan

Telecom-ISAC Japan 2012/07/30
2012/08/24 更新

【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議(所在地:東京都港区、会長:飯塚久夫(NRIセキュアテクノロジーズ株式会社)、以下、Telecom-ISAC Japan)は、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 概要

ロジテック株式会社(以下、ロジテック)より、「ロジテック 300Mbps無線LANブロードバンドルータ」の一部において、セキュリティに脆弱性があることが判明したと5月16日に、そして、「セキュリティを強化したファームウェア」を公開したと5月24日にアナウンスがありました。

ロジテック製300Mbps無線LANブロードバンドルータ
(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2)に関するお詫びとお願い
http://www.logitec.co.jp/info/2012/0516.html?link_id=out_ishirase_20120516_2_2

「この脆弱性により、インターネット接続に必要な「PPPoEの認証ID」および「PPPoEの認証パスワード」が外部より取得される可能性」があることから、インターネットの安全な利用に及ぼす影響の大きさを鑑みて、Telecom-ISAC Japanでは、この脆弱性に関する注意喚起をいたします。該当ルータの利用者は以下の対策を全て実行することを強く推奨いたします。

1. ファームウェアのバージョンアップ
2. ルータ管理画面のパスワード変更
3. PPPoEの認証パスワード変更
4. ルータの再設定

不正利用されたルータ製品所在調査の実施(2013年)


Telecom-ISAC Japan

Telecom-ISAC Japan 2013/08/30

脆弱性保有ブロードバンドルータの状況調査および対策について

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議(所在地:東京都港区、会長:飯塚久夫、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。

I. 背景・概要

Telecom-ISAC Japanでは昨年7月30日に以下の注意喚起を行い、その状況を追い続けておりました。

【注意喚起】ロジテック製ルータ
https://www.telecom-isac.jp

その結果、本年5月頃より発生し
によって得られた情報を攻撃者が
も相談のうえ、会員企業および
援していくことにいたしました。

II. 調査内容・時期について

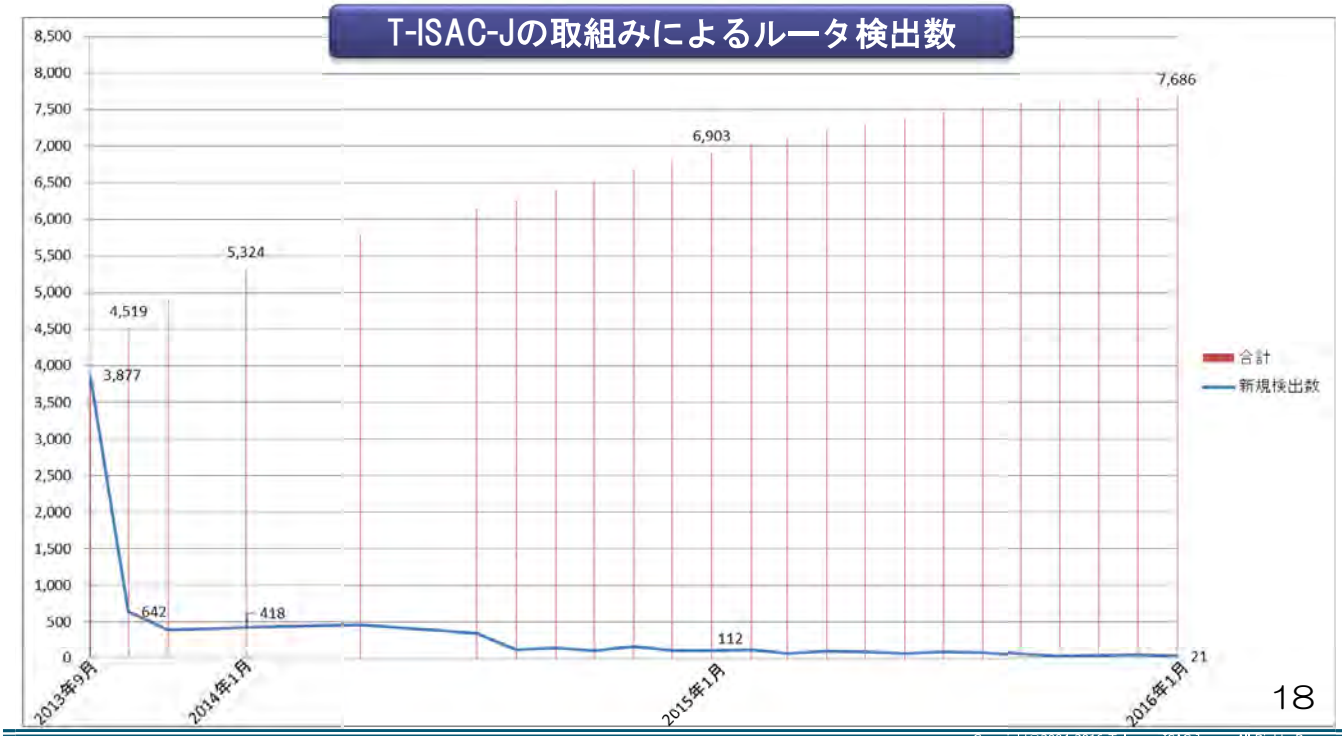
この調査は、協力要請をいた
通信コマンドで確認するもので
ようなものでは一切ありません。
また、調査の実施につきまして

17

不正プロキシサーバ業者摘発と脆弱性を有するブロードバンドルータ問題

ロジテック社該当ルータ検出数の推移

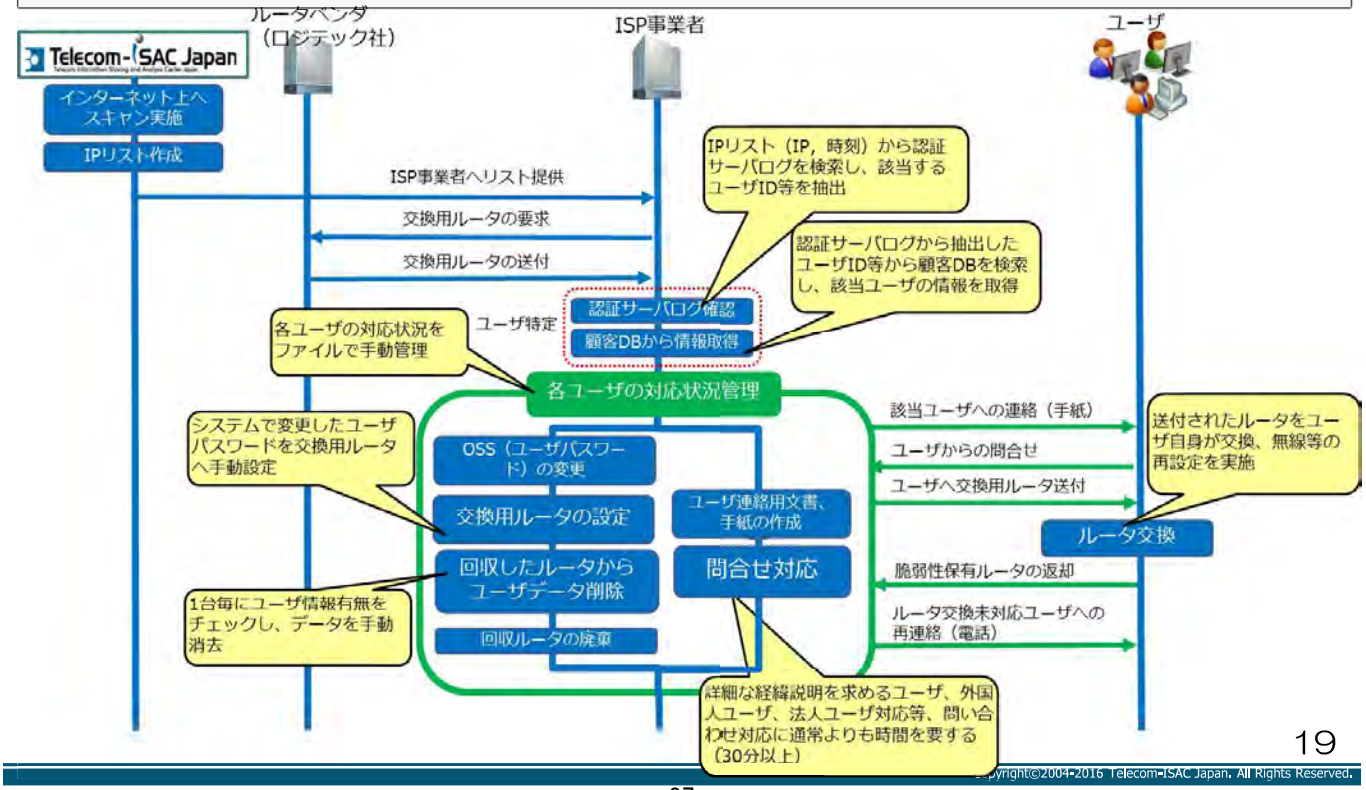
- Telecom-ISAC Japanの一部の会員企業により、2013年9月から該当ルータのファームウェアの更新、および交換の依頼を行っているが、新たに発見（新規検出）されるルータが無くならないのが現実
- 本事案のようなブロードバンドルータ問題が発生すると、その原因となる問題を完全に無くすことは極めて困難なため、このような問題がそもそも発生しないような取組みが重要



不正プロキシサーバ業者摘発と脆弱性を有するブロードバンドルータ問題

脆弱性を有するブロードバンドルータに対する注意喚起フロー

脆弱性を有するブロードバンドルータに対する注意喚起においては、その対応数の多さおよび対応作業の煩雑さから、多くの作業稼動が必要。（本対応について、一部のISPにおいて、その費用負担を当該ベンダが行うスキームを構築）



警察機関との連携に関する通信事業者の要望等について

警察機関との連携に関する通信事業者の要望等

- **警察機関からの注意喚起依頼に関する配慮・要望**
  - 警察機関とISPでの対応方法（注意喚起タイミング、IP収集方法等）の事前協議
  - ISPにおける対応内容の明確化（警察機関との役割分担の明確化）
  - 注意喚起等の施策遂行のための警察サイドにおけるユーザケア体制の構築

- **問題の原因を作った事業者、対策実施による受益者への自主的な対策推進の働きかけ**
  - 受益者（金融機関、ユーザ等）によるセキュリティ対策等に関する、自主的な対策推進の働きかけ
  - ロジテック社等、脆弱性の原因となった事業者への自主的な対策推進の働きかけ

- **警察機関からの情報共有の推進**
  - 警察機関から各ISPおよび利用者等に有益と考えられる情報の更なる共有

    ①手口、手法等、各ISPおよび利用者等の自主的な対応に繋がる情報
    ②連携して対応した事案の効果分析、結果等

一般財団法人　日本データ通信協会

テレコム・アイザック推進会議

一般財団法人 日本データ通信協会

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

https://www.telecom-isac.jp

総合セキュリティ対策会議
マイクロソフトとセキュリティ

日本マイクロソフト株式会社

片山建

2016年２月22日

Microsoft

Microsoft mission

Empower every person and every organization on the planet to achieve more

Microsoft

“地球上のすべての個人とすべての組織がより多くのことを達成できるようにする”

マイクロソフト のクラウド: 信頼できるクラウド

データはお客様のもの

データを所有し、管理するのはお客様です
マイクロソフトは、お客様のためにサービスを運営しています
マイクロソフトは、お客様に対する責任を果たしてまいります

ビルトインのセキュリティ

プライバシー・バイ・デザイン

継続的なコンプライアンス

透明性

サイバーセキュリティは経営問題

「Cyber security is a CEO issue」 *1

76%

全ネットワーク侵入件数の76% がユーザー資格情報の不正アクセスによるものです *2

200日以上

攻撃者が検出されるまでに被害者のネットワーク内に潜伏している中央値の日数は200 日を超えます

4.2億円

企業が被るデータ侵害の平均コスト *3

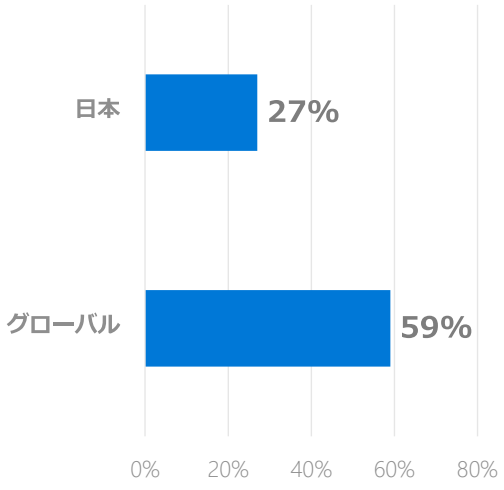
80億円+

クレジットカード会社への賠償金*4

*1 Risk and responsibility in a hyper connected world: Implications for enterprises　January 2014
*2 Verizon 2013 Data Breach Investigation Report
*3 Ponemon Institute Releases 2014 Cost of Data Breach
*4 Bloomberg　2015/8/19

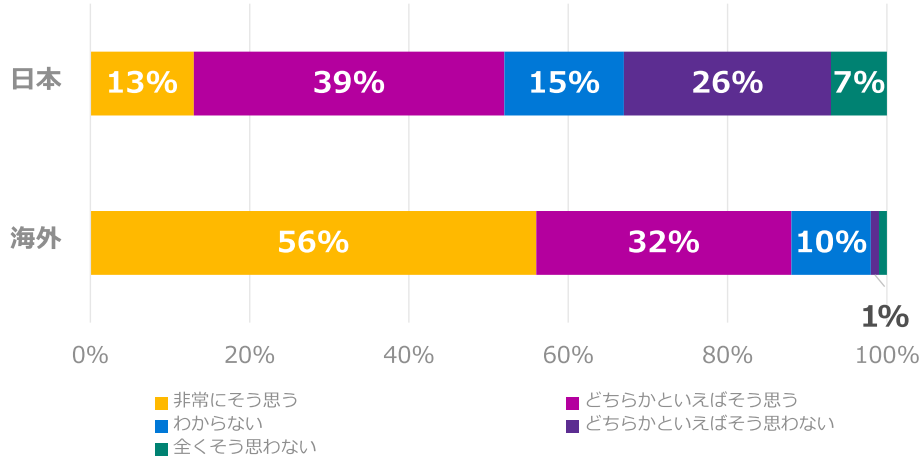
セキュリティは経営者の課題　海外比較

セキュリティ対策を推進する経営幹部がいる企業



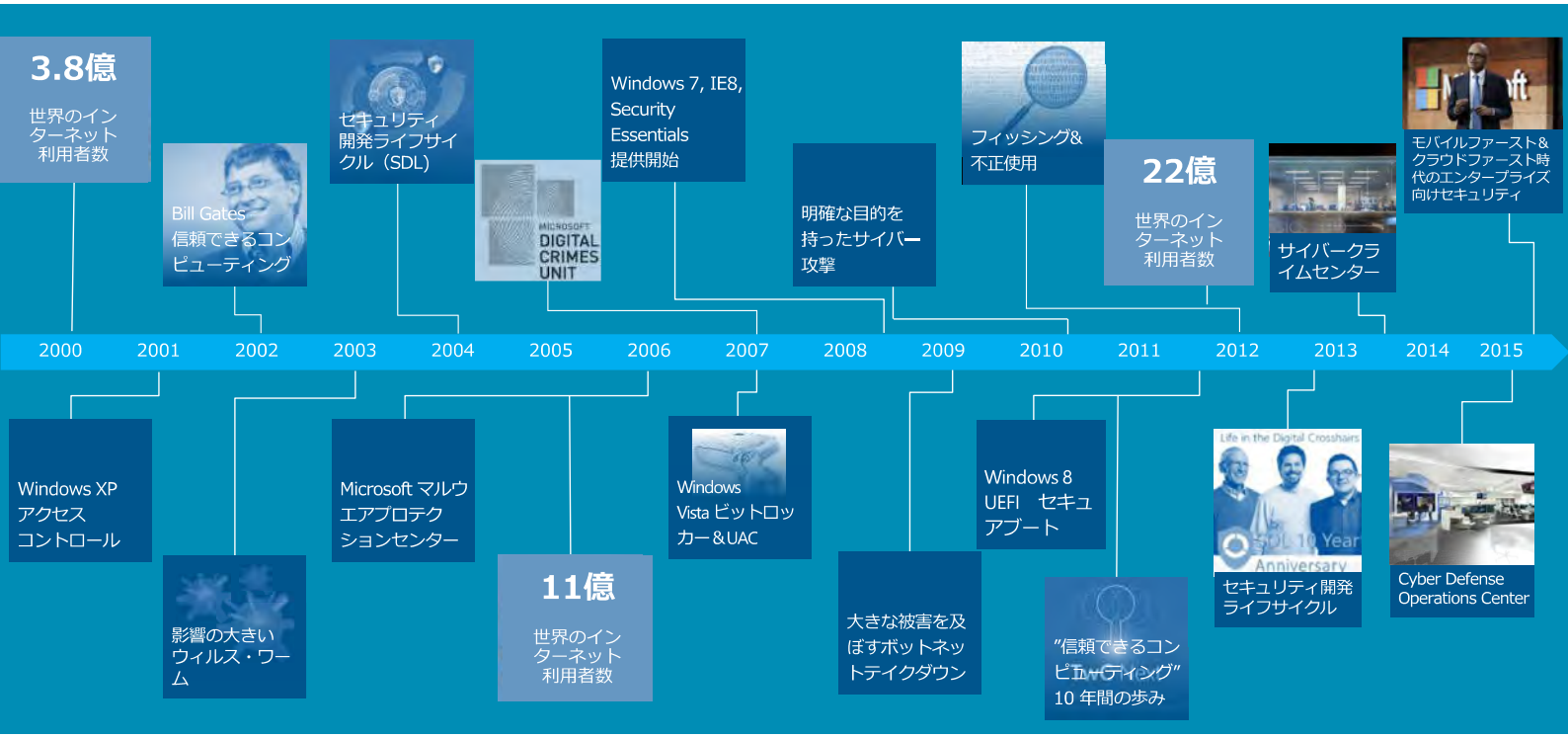
サイバー攻撃への対処を議論するレベル

問.サイバー攻撃の予防は取締役レベルで議論すべきか



経済産業省　サイバーセキュリティ経営ガイドライン（案）　2015年12月
*1 PwC「2014 Global State of Information Security Survey」
*2 KPMG [セキュリティサーベイ2013]

マイクロソフトの取り組み



保護

全エンドポイントの保護

検知

攻撃検知機能の向上、モニタリング、学習

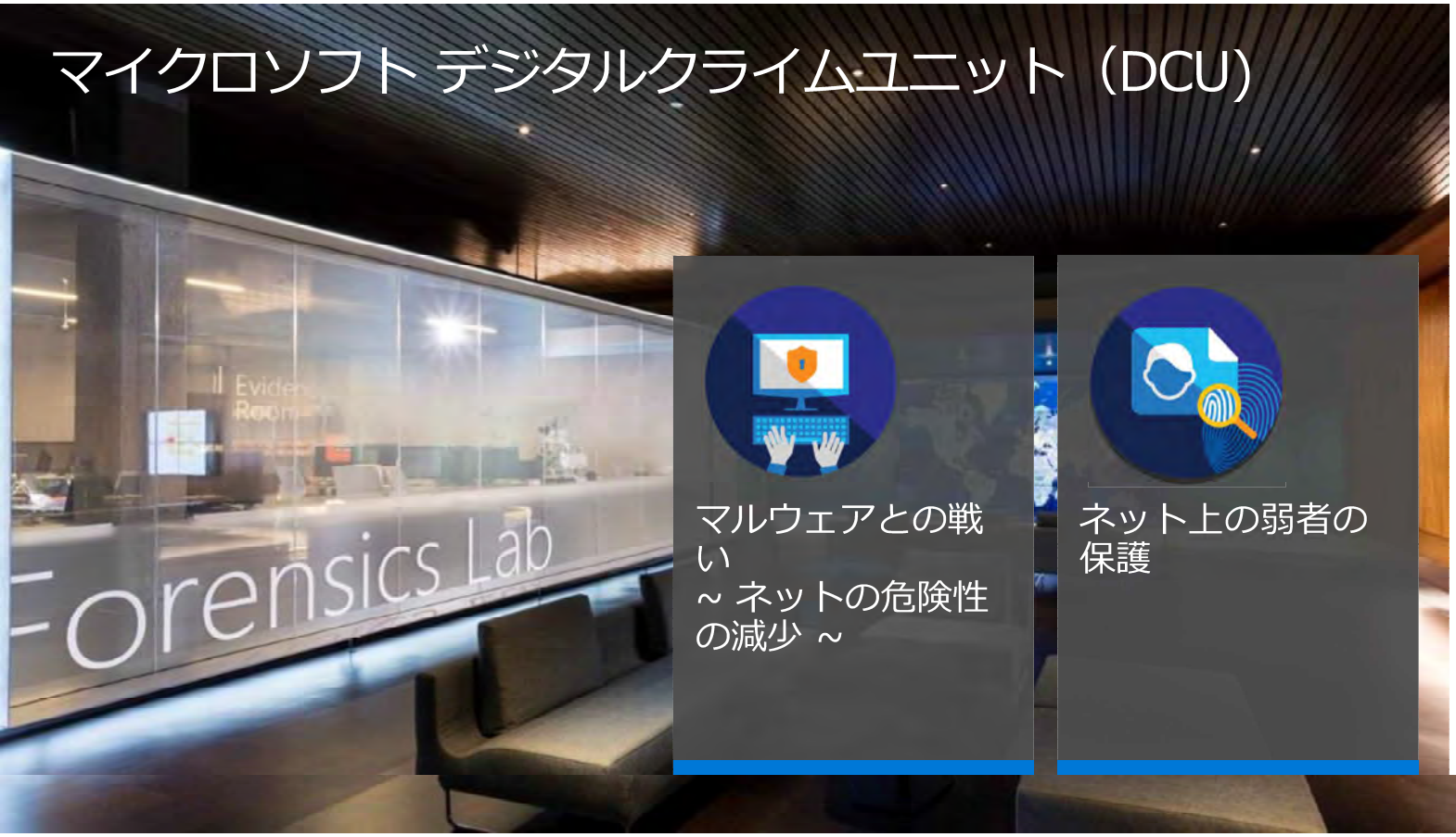
対処

セキュリティ上の脅威発見と対処のギャップを無くす

マイクロソフト　サイバー クライムセンター




マイクロソフト デジタルクライムユニット（DCU)

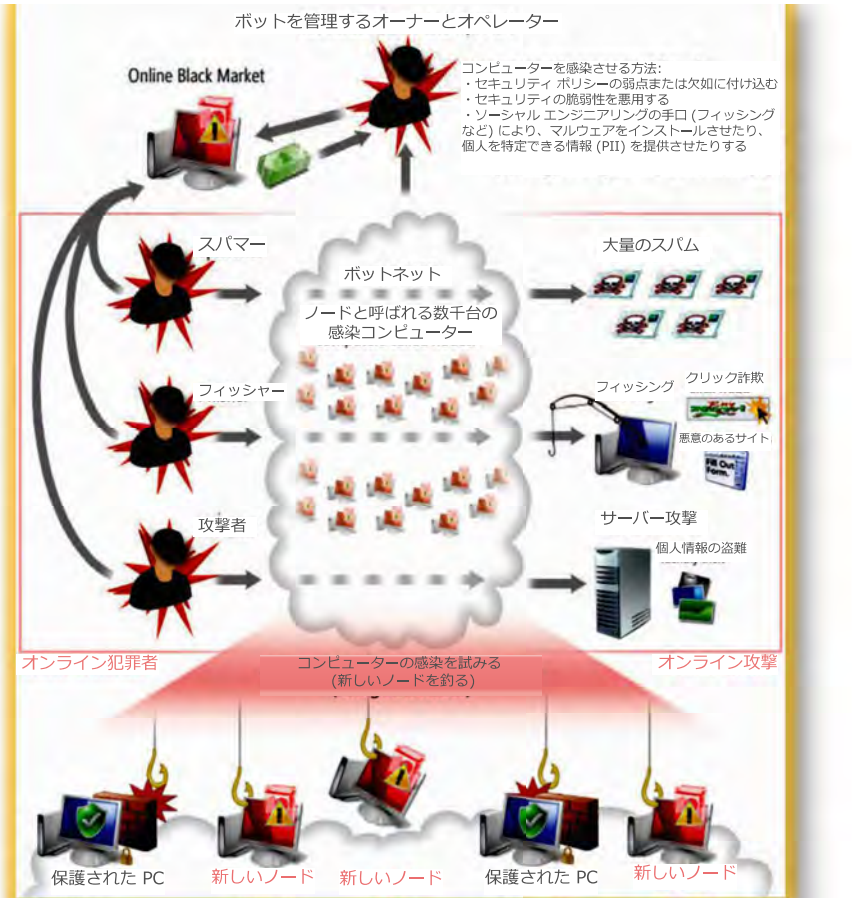


マルウェアとの戦い
～ ネットの危険性の減少 ～

ネット上の弱者の保護

ボットネット –

悪意のあるソフトウェアに感染した大量のコンピューター。サイバー犯罪者の制御のもと、あらゆる種類の犯罪活動のために、ひそかに遠隔地から操作される



DCU によるボットネット/マルウェアのテイクダウン

2010 - 2012	2013	2014	2015
Conficker 2010 年 2 月 *Botnet Worm*	**Bamital** 2013 年 2 月 広告クリック詐欺	**Game-over Zeus** 2014 年 6 月 オンライン金融詐欺	**Ramnit** 2015 年 2 月 オンライン金融詐欺
Waledac 2010 年 2 月 スパム	**Citadel** 2013 年 6 月 オンライン金融詐欺	**Jenxcus** 2014 年 6 月 金融詐欺/プライバシー	**Simda** 2015 年 4 月 マルウェア拡散
Rustock 2011 年 3 月 スパム	**ZeroAccess** 2013 年 12 月 広告クリック詐欺	**Caphaw** 2014 年 7 月 オンライン金融詐欺	
Zeus 2012 年 3 月 オンライン金融詐欺			
Nitol 2012 年 9 月 *DDOS/拡散*			

Digital Crime Consortium

-世界約30ヶ国から約500名が参加（法執行機関、政府機関、大学、セキュリティ関連企業など）
-2003年に開催されたBTF（Botnet Task Force）が前身
-世界中の産官法学が連携できるよう、成功事例の共有、情報交換、ディスカッションの場を提供
-日本からも参加

Microsoft

サイバーセキュリティの向上と捜査情報の活用

首都大学東京・法学系

星　周一郎

報告内容

１．捜査での収集情報のセキュリティ目的活用

２．サイバーセキュリティ確保への積極的措置

１．捜査での収集情報のセキュリティ目的活用

「サイバー攻撃」が刑罰法令に触れる場合

捜査機関による捜査の実施

犯人検挙・訴追に至らない場合の情報は「お蔵」

被害防止のための有益な情報……

１．捜査での収集情報のセキュリティ目的活用

捜査：被疑者の身柄確保・有罪に向けた証拠収集活動

刑事訴訟法４７条

訴訟に関する書類は、公判の開廷前には、これを公にしてはならない。但し、公益上の必要その他の事由があって、相当と認められる場合は、この限りでない。

訴訟関係人の名誉の毀損、公序良俗違反、または裁判に対する不当な影響の惹起を防止する趣旨（判例・通説）

１．捜査での収集情報のセキュリティ目的活用

訴訟関係人の名誉・公序良俗等に影響しない情報

cf. 被害防止・情報収集のための「公開捜査」

「公益上の必要その他の事由があって、相当と認められる場合」？

東京高判平成25年11月27日（判時2219号46頁）

警察活動の説明をすること自体は、警察の職務に付随し、その責務に属する行為（警察法1条・2条）

本件事件の犯人の特定、起訴に繋がらない結果となった顛末の説明は、警察の説明責任を果たす意味で必要

１．捜査での収集情報のセキュリティ目的活用

警察活動における情報の取得と管理・利用の再検討

サイバーセキュリティの向上・被害拡大防止

サイバーセキュリティの文脈における「公益上の必要その他の事由があって、相当と認められる場合」

２．サイバーセキュリティ確保への積極的措置

サイバー空間での被害防止のための積極的措置

「戸締まり用心」から積極的な被害防止への関与

「犯罪被害防止法」

２．サイバーセキュリティ確保への積極的措置

現実空間の「犯罪被害防止法」

公道上の警ら活動	個別の根拠法規のない任意活動（事実行為）
街頭防犯カメラ	設置・管理について内規による規制
交通一斉検問	公道を利用することに伴う負担（判例）
犯罪の予防・制止・立入り	警職法5条・6条に基づく警察官による行政処分
ＤＶ防止法上の被害防止	警察官による行政処分
ストーカー規制法上の警告	警察署長等による行政処分
ストーカー規制法上の禁止命令	公安委員会による行政処分
児童虐待防止法上の立入調査等	知事による行政処分
児童虐待防止法上の臨検・捜索	裁判所の許可状に基づく知事による行政処分
ＤＶ防止法上の保護命令	被害者の申立てに基づく裁判所による保護命令

２．サイバーセキュリティ確保への積極的措置

サイバー空間の「犯罪被害防止法」

社会の存立基盤（インフラ）たるサイバー空間の安全確保

ex. ボットネットのテイクダウン措置

それによって生ずる利益侵害は？

サイバー空間におけるプライバシーとは何か？

「通信の秘密」との関係？

行政法と刑事法が交錯する「間隙」

ご清聴、ありがとうございました。