サイバー脅威の無効化のための産学官の協働
ーJC3による取組の現状ー

■一般財団法人　日本サイバー犯罪対策センター
Japan Cybercrime Control Center：JC3
■理事　坂　明

■ info@jc3.or.jp

Copyright ©JC3 All Rights Reserved.　無断転載禁止

JC3 Japan Cybercrime Control Center

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

Copyright © JC3 All Rights Reserved.　無断転載禁止

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」

Copyright © JC3 All Rights Reserved.　無断転載禁止

脅威に対する問題意識

サイバー空間をめぐる脅威の情勢（平成27年上半期・警察庁資料）

- 標的型メール攻撃の認知件数の増加
  - 警察が把握した標的型メール攻撃は1,472件、前年同期比で1,256件、581%増加
- サイバー空間における探索行為の増加
- ネットバンキングに係る不正送金事犯の被害が拡大
  - 平成27年上半期の被害額は約15億4,400万円で、前年下半期を上回り、信用金庫・信用組合等に被害が拡大

我が国におけるサイバー脅威の課題

- 経済的利益を狙った犯罪・情報窃取（侵入）を目的とした攻撃
- 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
- アトリビューションの重要性とそのための連携

Copyright © JC3 All Rights Reserved.　無断転載禁止

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

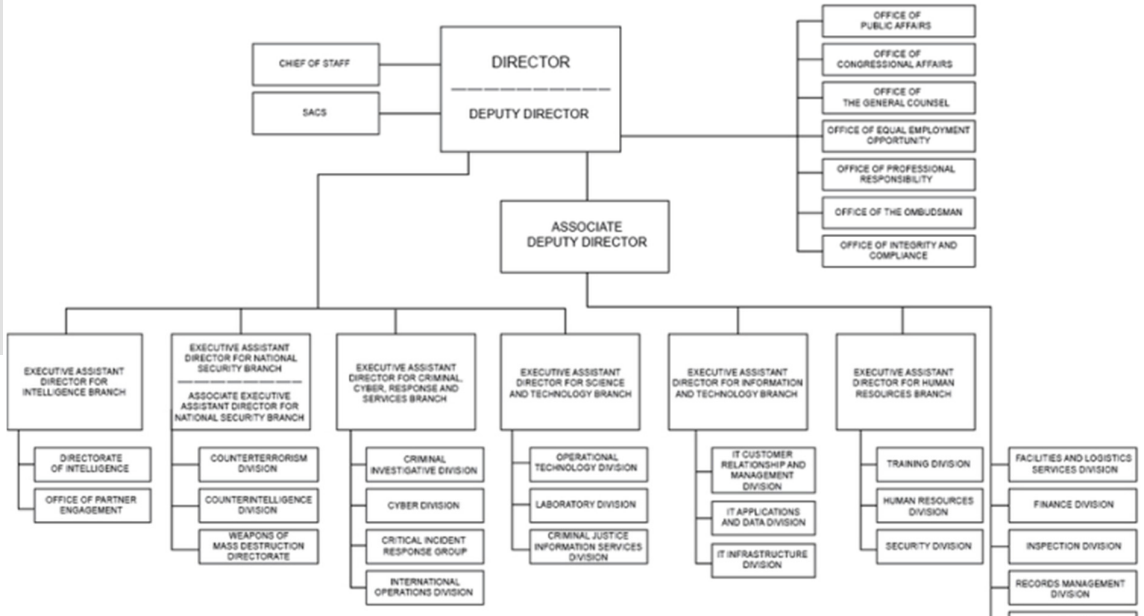
Copyright © JC3 All Rights Reserved.　無断転載禁止

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）

Copyright © JC3 All Rights Reserved.　無断転載禁止

米国NCFTAのFBIの体制

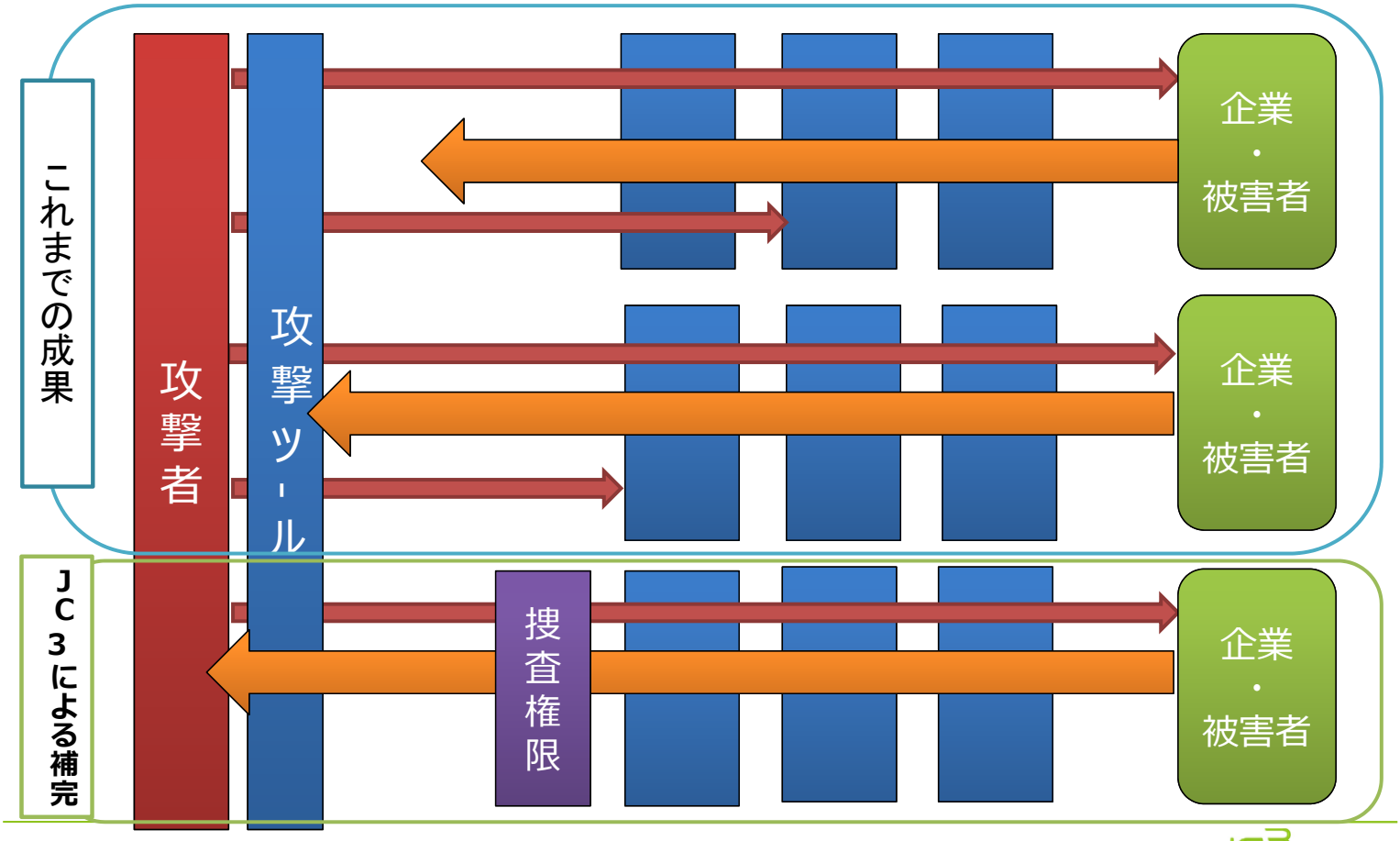


https://www.fbi.gov/contact-us/fbi-headquarters/org_chart ，2014/07/14現在

FBIのNCFTA常駐班：
Cyber Initiative and Resource Fusion Unit: CIRFU

Copyright © JC3 All Rights Reserved. 無断転載禁止

JC3の役割



Copyright © JC3 All Rights Reserved. 無断転載禁止

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

Copyright © JC3 All Rights Reserved.　無断転載禁止

米国NCFTAとの関係の強化

- **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であり、NCFTAとの協力関係は重要**

Copyright © JC3 All Rights Reserved.　無断転載禁止

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発足以前の民間企業と法執行機関との関係は、必ずしも良好とは言えませんでした。
- 法執行機関に対して消費者からのクレームや企業から犯罪被害の報告等が上がっても、彼らは一定程度の金銭的な被害規模がないと-もちろん情報は受け取りますが一捜査には乗り出しません。また、彼らは情報を機密化してしまいます。
- そのため、企業としては、法執行機関に渡した後は何も知らされず、何もできないという状況でした。
- こうしたことから、以前は、法執行機関と民間企業との間に信頼が醸成されていませんでした。民間企業は、ただでさえマスコミに自社の脆弱性等に関する情報が渡ることや企業イメージに傷がつくことを恐れている中で、法執行機関も信頼しなくなってしまったものですから、余計に情報を外に出そうとはしなくなってしまいました。
- 一方、当時、法執行機関が民間企業をどう捉えていたかというと、「民間企業は、我々に情報を渡すことを望んでいない。」と思っていたそうです。
- 民間企業は、本当は、渡したくないのではありません。労力を使い、時間とお金を割いて収集した情報を法執行機関に渡しても、彼らはその情報を受け取るだけで機密化し、当の民間企業は蚊帳の外に置かれてしまう。それで結果を聞くと「立件できない。」という繰り返しの中で、法執行機関と連携しても何も得るものはないと考えていたのです。

Copyright © JC3 All Rights Reserved.　無断転載禁止

NCFTAプレジデントのお話より（続き）

- こうした問題が解決されないまま時が過ぎていたのですが、1997年、ピッツバーグに拠点を持つ“HighTechnology Task Force”という組織を中心に、サイバー空間の脅威に対応するためには、別の角度での取組ー産学官が連携し、情報とリソースを共有すること-が必要であると認識され始めました。

- 法執行機関が、サイバー空間の脅威に対応するために必要なものすべてを持っているわけではないこと、また、脅威に対応するためには、産業界や学術界にいる特定分野の専門家が必要であること、そして、収集した情報をデータベース化するためには産学官の間に中立的な立場を作る必要があることなどに気付いたのです。

- こうした着想を基に試行錯誤を繰り返しながら、2002年、産学官のいずれにも中立的で、安全に情報を共有することが可能な仕組みを持つ組織を構築しました。それが現在のNCFTAです。

Copyright © JC3 All Rights Reserved.　無断転載禁止

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**
- **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。**

Copyright © JC3 All Rights Reserved.　無断転載禁止

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**
- **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。**

Copyright © JC3 All Rights Reserved.　無断転載禁止

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**
- **差押え**
  - 資産（被害回復にも繋がる）、攻撃リソース
- **その他権限の活用**
- **情報共有による被害の予防**

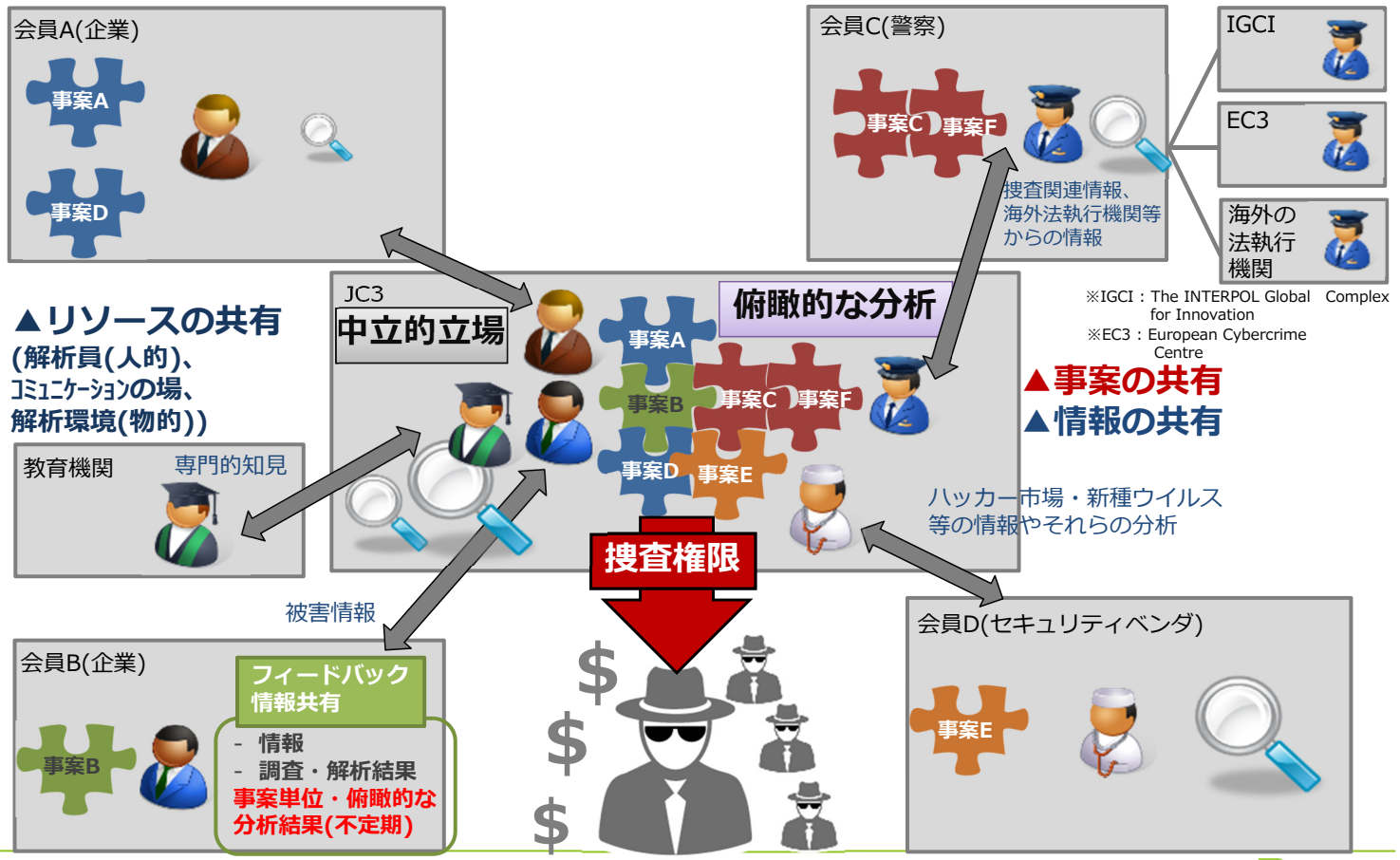
Copyright © JC3 All Rights Reserved.　無断転載禁止

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
- **取組のための新たなリソース（体制・態勢）を生成**

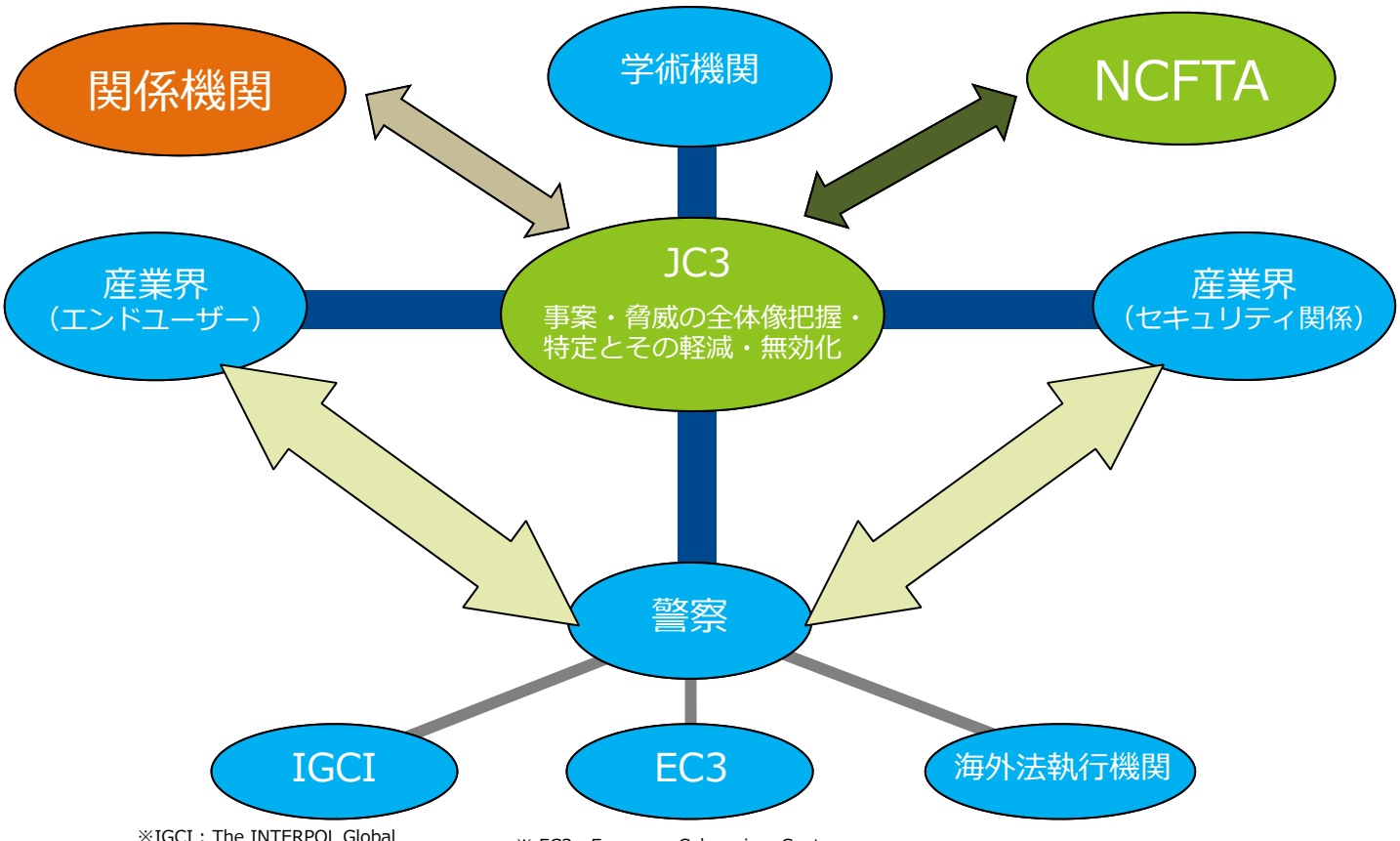
Copyright © JC3 All Rights Reserved.　無断転載禁止

JC3の概要～情報共有により目指す成果



(c) JC3 All Rights Reserved.

JC3における情報・知見の共有スキーム



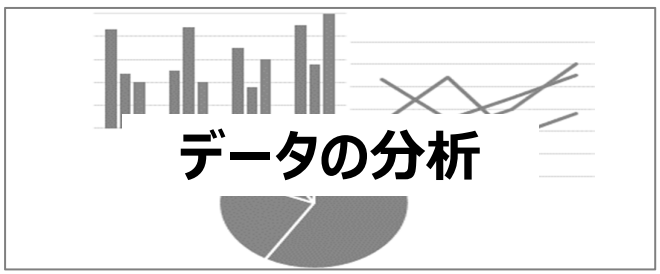
Copyright © JC3 All Rights Reserved. 無断転載禁止

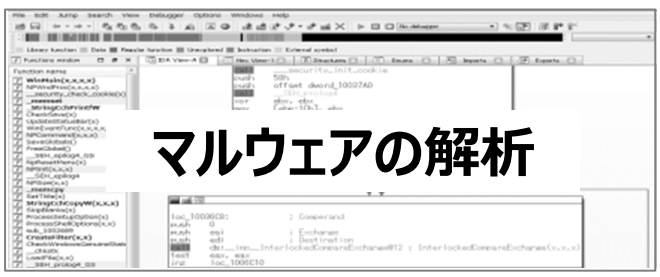
違法アダルト広告　摘発　海外サーバー利用、全国で13人逮捕

- 日本経済新聞 2015年11月27日
- 警察庁は26日、18都道府県警が海外サーバーを利用した違法なアダルト広告宣伝サイトの一斉取り締まりを25日に実施。
- 捜索は66カ所で、10都道府県警がわいせつ電磁的記録媒体陳列の疑いでサイト管理者ら13人を逮捕。
- 取り締まりには、サイバー犯罪に対処するため昨年11月に産官学で発足した一般財団法人「日本サイバー犯罪対策センター」（ＪＣ３）が初めて協力。
- 海外サーバーは匿名性が高いため、サイバー犯罪の隠れみのとして悪用されている。違法なサイトは閲覧したパソコンがウイルス感染する恐れもあることなどから、わいせつな画像を掲載したアダルト広告宣伝サイトが今回の取り締まり対象。
- 今年６月、茨城県警を中心に捜査を開始。ソフトを使って約２千のサイトを抽出し、各地の警察が捜査。
- サイトにはアダルト関連のバナー広告があり、閲覧者がクリックして会員登録や商品購入などをすると、サイト管理者は収入を得られる。
- 逮捕された13人は33～65歳で「海外サーバーなら捕まらないと思った」などと供述。

Copyright © JC3 All Rights Reserved.　無断転載禁止

JC3の活動





Copyright © JC3 All Rights Reserved.　無断転載禁止

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

Copyright © JC3 All Rights Reserved. 無断転載禁止