

第2章

＜警察政策フォーラム＞

サイバー空間の脅威への対策における
新たな展開 ～産学官連携への期待～

<警察政策フォーラム>

サイバー空間の脅威への対策における新たな展開 ～産学官連携への期待～

警察政策研究センター

警察政策研究センターは、平成 25 年 9 月 26 日、公益財団法人公共政策調査会、警察政策学会及び一般財団法人警察大学校校友会の後援により、グランドアーク半蔵門（東京都千代田区）において、警察政策フォーラム「サイバー空間の脅威への対策における新たな展開～産学官連携への期待～」を開催した。

近年、サイバー空間は、めざましい進化を遂げているが、それに伴い、サイバー空間の脅威もまた増大している。こうした脅威への抜本的な対策が求められている中、情報セキュリティ政策会議（議長：内閣官房長官）における「サイバーセキュリティ戦略」（平成 25 年 6 月 10 日同会議決定）など¹において、産業界、学界、そして官界といった各主体間のこれまでの個別事案ごとの協力関係ではなく、各主体が一体となってサイバー空間の脅威へ対処するという趣旨の下、「日本版 NCFTA の創設」が掲げられたところである²。

このように、サイバー空間における脅威への対策は、今、新たな展開を見せつつあるが、サイバー空間は、組織レベルから個人レベルに至るまで多様な利害関係者から成り立っており、新たな取組に当たっては、可能な限り多くの者の理解を得ながら進めていくことが望ましい。

本フォーラムは、上記の点を踏まえ、産学官連携の具体的な在り方の議論の前提として、産・学・官それぞれの主体に着目し、これまでのサイバー空間の現状におけるそれぞれの課題、また、それを打開するための対処方策としての産学官連携について、各主体のニーズ、各主体が持つ他の主体への期待、あるいは留意点等を切り口として、警察の各部門のみならず内外の実務家や研究者、企業関係者等が議論し、広く情報を共有した上で、サイバー空間に関係するすべての方々に向けて発信することを目的として開催されたものである。

本フォーラムでは、佐々木真郎警察政策研究センター所長による開会挨拶の後、有識者 3 名による基調講演が行われた。講演者及び講演タイトルは、次のとおりである。

- マリア・ヴェロ氏（Natal Cyber-Forensics & Training Alliance CEO 兼理事長）

「サイバー空間の脅威に対処するための連携の在り方」

- 田中英彦氏（情報セキュリティ大学院大学学長、同教授）

「産学官連携によるサイバー空間の安全性確保～犯罪に強い社会の実現のために～」

- 近藤邦夫氏（日本電気株式会社執行役員）

「『産』から見た産学官連携について～情報セキュリティソリューションベンダーの期待と役割～」

また、これらの基調講演の後のパネルディスカッション（討論）では、同佐々木所長がコーディネーターを務め、冒頭、2 名のパネリストによる発表が行われた。発表者及び発表テーマは、以下のとおりである。

- 星周一郎氏（首都大学東京都市教養学部法学系教授）

「サイバー空間の脅威に対する情報共有組織の意義」

¹ 同戦略のほか、同戦略に基づき 2013 年度及び 2014 年度に実施する具体的な取組の重点をまとめた「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決定）においても、「日本版 NCFTA の創設」が掲げられている。

² なお、「日本版 NCFTA の創設」は、本フォーラム開催後の同年 12 月、犯罪対策閣僚会議において策定された「『世界一安全な日本』創造戦略」（平成 25 年 12 月 10 日閣議決定）中、「1 世界最高水準の安全なサイバー空間の構築」の「（2）民間事業者等の知見の活用」においても掲げられている。

○ 緒方禎己氏（警察庁生活安全局情報技術犯罪対策課長）

「警察におけるサイバー犯罪対策」

両名による発表の後、上記基調講演者を交え、産学官連携に係るニーズや期待、留意点等について活発な議論が行われ、盛会のうちに終了した。

なお、本フォーラムには、大学研究者、企業関係者、報道機関、関係機関、警察関係者等、約 350 名が出席した。

【開会挨拶】

警察政策研究センター所長 佐々木真郎

警察政策研究センターでは、日本警察のシンクタンクとしてフォーラムを年に数回開催し、今後の警察政策の展開を議論する場を設けている。今回、「サイバー空間の脅威への対策における新たな展開～産学官連携への期待～」をテーマとした趣旨について一言御説明させていただく。

近年、サイバー空間は、めざましい進化を遂げており、それに伴い、サイバー空間の脅威もまた増大している。こうした脅威への抜本的な対策が求められている中、政府の「サイバーセキュリティ戦略」などにおいて、産業界、学术界、そして官界といった各主体間のこれまでの個別事案ごとの協力関係ではなく、各主体が一体となってサイバー空間の脅威へ対処するという趣旨の下、「日本版 NCFTA の創設」が掲げられたところである。

このように、サイバー空間における脅威への対策は、今、新たな展開を見せつつあるが、サイバー空間は、本日御参加いただいた皆様も御存知のとおり、組織レベルから個人レベルに至るまで多様なステークホルダー（利害関係者）から成り立っており、新たな取組に当たっては、可能な限り多くの皆様の理解を得ながら進めていくことが望ましい。

そこで、本フォーラムでは、産学官連携の具体的な在り方の議論の前提として、産・学・官それぞれの主体に着目し、これまでのサイバー空間の現状におけるそれぞれの課題は何か、また、それを打開するための対処方策としての産学官連携について、各主体のニーズとは何か、各主体はどのようなことを他の主体に期待するのか、あるいは留意すべき点は何かなどについて、警察の各部門のみならず内外の実務家や研究者、企業関係者等が議論し、広く情報を共有した上で、サイバー空間に関係するすべての方々に向けて発信しようというものである。

今回は、米国から NCFTA の最高責任者でおられるマリア・ヴェロ氏、情報セキュリティ大学院大学学長の田中英彦教授、日本電気株式会社執行役員の近藤邦夫氏を基調講演者としてお迎えすることができた。

マリア・ヴェロ氏は、米国の名だたる企業において実績を重ねる傍ら、産学官における情報共有と協力を促進し、三者が一体となって各種取組を進めている NCFTA (Natal Cyber-Forensics & Training Alliance) の発足当初からボードメンバー（理事）の一人として組織の立ち上げに御尽力され、現在その最高責任者として御活躍されている。本日は、米国におけるサイバー空間の脅威の現状や NCFTA 発足の経緯、意義などにつき御講演をいただく。

田中教授は、情報工学を御専門とされ、また、情報セキュリティ大学院大学学長として、情報セキュリティの人材育成に携わっておられる立場から、サイバー空間の脅威への実効性ある対処方策の在り方や、人材育成の在り方などについて御講演をいただく。

近藤執行役員は、まさにサイバー空間の脅威の最前線に立つ、日本を代表するグローバル企業としてのお立場から、企業におけるサイバーセキュリティの現状やその取組の在り方などについて御講演をいただく。

この外、パネルディスカッションにおいては、星周一郎首都大学東京都市教養学部教授、緒方禎己警察庁生活安全局情報技術犯罪対策課長をパネリストとしてお迎えしており、それぞれ刑事政策・刑事法学の立場、あるいは我が国のサイバー犯罪対策の担当者としての立場から、それぞれ貴重なお話を賜る。

このように、多様な分野の御専門の基調講演者・パネリスト、そして御参加いただいた皆様における御議論により、本フォーラムが、我が国におけるサイバー空間の脅威への対策、その新たな展開に向けた取組の一助となれば、望外の幸せである。

【基調講演①】サイバー空間の脅威に対処するための連携の在り方

NCFTA (National Cyber-Forensics and Training Alliance) CEO 兼理事長 マリア・ヴェロ

<編集> 警察政策研究センター教授 渡辺 幸次

はじめに

皆様にお目にかかれて大変光栄に思います。

近年、社会全般にわたってサイバー空間の脅威が高まっています。国家・市民、友人・家族のいずれもターゲットとされるおそれがあり、いかなる個人・組織もその脅威を免れることはできません。サイバー空間の脅威に対する我々の取組には、今、抜本的な変革が求められているのです。

仮想空間・現実空間の双方において、我々の生活やビジネスを凌駕しているサイバー犯罪には、いかなる境界も存在していません。これに対処するためには、我々も同様に、いかなる境界も超えていかなければなりません。法執行機関である政府、民間企業、そして学術機関による「産・学・官」が連携し、サイバー空間の脅威に関する情報を共有するとともに、取組に必要な人的・物的・財政的資源（以下、単に「リソース」という。）を共有していくのです。しかも、これらは国を超えて共有していく必要があります。そうしたことを実行して初めて、サイバー空間の脅威への対策は万全と行うことができるのではないのでしょうか。

本日は、私がCEO兼理事長を務めているNCFTA (The National Cyber- Forensics and Training Alliance) について、組織の概要や設立の背景、これまでの成果等を御紹介します。

1. NCFTAの構成について

NCFTAは、ペンシルベニア州のピッツバーグに本部を置いているほか、ウエストバージニア州のフェアモントにも小規模のオフィスを構えています。

パートナーとして、政府からは、国家・地方の別を問わず、多種多様な法執行機関が参画しています。また、我々は、国外の法執行機関ともパートナーシップを結んでいます。その数は増加し、また、その内容も発展し続けているところです。

民間企業からは、世界でも上位に当たる様々な企業—インターネット・サービス・プロバイダ、アンチウイルスベンダーはもとより、銀行や証券会社等の金融機関、クレジットカード会社のほか、エネルギー産業、小売業、製造業、流通業等多様な業界に属する企業—が横断的に参画しており、その数は、現在も着実に増加しています。サイバー空間の脅威に対処するためには、一緒になって戦わなければならないということを認識しているからこそ、このようなパートナーシップが増えているのだと思います。

2. 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、非常に实际的です。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。ここにいる「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步遅れています。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。

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、民間一すなわち、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常に取り組んでおり、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。

3. NCFTA設立の背景～官民連携の障害～

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一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点、「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。

また、双方の連携を阻害していたものとして、人間関係の連続性がなかったことも挙げられます。法執行機関の捜査員は頻繁に異動します。ワシントンD.C.で1年半勤務すれば、また別のところへと異動してしまう。お互いを知るチャンス、信頼を醸成する時間が与えられなかったのです。

こうした問題が解決されないまま時間が過ぎていたのですが、1997年、ピッツバーグに拠点を持つ“High Technology 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—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。なお、NCFTAは、同年に内国歳入法第501条(C)(3)の適用を受けた非営利法人となっています。

4. NCFTAにおける情報共有と連携の在り方

現在、NCFTAでは、随時パートナーから情報が提供されてきますが、受け取った情報はNCFTAにおいて匿名化し、どこに帰属するかが分からない形にして分類した上で、データベース化しています。そして、データベース内の情報を分析し、現に発生している犯罪を止めるために必要な情報を、まだ犯罪が発生しているうちにタイムリーに抽出していきます。

この際、NCFTAでは、パートナーから得る情報を無理強いすることはありません。我々は、“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）という姿勢で取り組んでいます。

とはいえ、ジグソーパズルのように、ピースを一つ一つ埋めてサイバー空間の脅威の全体像を把握していくわけですから、当然、そのために様々な情報が必要となります。ひょっとしたら、パートナーの誰かがピースの一つを持っているかもしれません。また、本人がさほど重要ではないと考えていたその情報の一欠片が、脅威の全体像を埋めるパズルの最後のピースになるかもしれません。一見して価値の低そうに見える情報についても共有していくことにより、こうした事態にも備えることができます。また、そうであればこそ、情報は一方通行ではなく、双方向で共有していくことが重要なのです。

人的資源の共有については、長年協力をしてくれている個人がNCFTAの職員として勤務しているほか、パートナーである民間企業からの派遣社員や大学のインターン、そして法執行機関からも人材を受け入れています。また、“Subject Matter Experts”という、特定分野の専門家も設定・配置しています。責任感の強い、多様な人材を集めて情報を共有するとともに、規則や約束事を遵守し、共有される情報を適切に管理することによって、サイバー空間の脅威に対処する上で必要な情報、知見、ツールが増えていくのです。

法執行機関の職員は、所属本部を拠点にしつつNCFTAに参画しています。もちろん、担当捜査員は3年～8年は異動しません。常に同じ人と話すことができる、隣の机に行けば同じ人が座っているということが、組織間の信頼関係の醸成に役立っています。また、一般的に言えることですが、本人にとっても、経験は長ければ長いほど良いと言えます。我々と一緒にサイバー犯罪と戦う経験が長いほど、情報分析能力の向上や脅威を特定するためのノウハウが多く得られることになるからです。

5. 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、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。

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ますが、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、彼らも自ら情報を検証した上で、逮捕、資産の押収等適切な対応をしていくことになります。

さらに、新しい脅威が発生したときで、「何か動きがあるように思われるものの、その脅威に関する情報が少ない。」といった場合には、法執行機関はもとより、他のNCFTAのパートナーである民間企業や大学等に「脅威レポート」として、早期に情報を流していきます。その脅威に対する対処を少しでも先制的に、予防的に取ることができるよう、我々は警鐘を鳴らすとともに、更に情報収集をしていくのです。

6. サイバー犯罪の情勢に応じたプログラムの整備

NCFTAには、様々なプログラムがあり、各プログラムを更に具体的なイニシアティブに分類し、取組を進めています。この場で一つ一つの詳細については割愛しますが、ここでは最近になって確立した「マルウェアプログラム」について触れたいと思います。

今やマルウェアやボットネットは、非常に高度化しており、全く検出されない状態で被害をもたらし得るようになっていきます。これらはIPアドレスや企業秘密、個人情報を窃取したり、他のコンピュータに感染させるために攻撃を仕掛けたりします。企業機密や各種のイノベーションに関わる情報の漏洩は、米国経済に深刻な影響を及ぼし、我々の技術革新や財産を損なうことにつながります。

我々は、常にマルウェアを監視しています。C&Cサーバ¹がどこにあるか、つまり、誰がこのネットワークを支配しているのかという点に着目し、ハイレベルの被疑者を捕まえることを重視しています。犯罪インフラを解体するためには、「モグラたたき」をしても仕方ありません。小者を捕まえても仕方がないのです。大物を捕まえないければ、彼らは「おもちゃ」を別のところに持って行って、同じ犯罪を始めるだけですから。

この点については、哲学的に様々な考え方があります。米国の企業の中には、犯罪インフラの解体には取り組まずに、ボットネットを解体してくれさえすれば良いという意見があります。しかし、それだけでは、検挙を免れた犯罪者はその仇を討つため、マルウェアを変形させる方法を学び、新たな戦略を作り、更に賢くなって再び我々の前に立ち上がるようになってしまいます。また、社会へのアピールとして、小者であってもきちんと捕まえ、プレスリリースを出して「悪い奴を捕まえた。」と言ってほしいという意見もあります。しかし、その後どうなるかという点、以前よりもっとひどい手口で犯罪が行われ、前よりはるかに大きな脅威が出現してしまうことになってしまうのです。

7. オープンソースの活用とデータベース化

NCFTAでは、インターネット上のソーシャルメディアからも多くの情報を得ています。マスメディアで何かが取りざたされると、それが気に食わない人はすぐに攻撃に出ますから、誰も安全ではありません。我々は、ソーシャルメディアの中で何が話題になっているかを常にモニターしており、一つ一つは点に過ぎませんが、これらの点を結んで線にし、将来の脅威を予測しています。

例えば、動物実験を行っている会社が気に食わない、ある政治的なつながりが気に食わない、トウモロコシの遺伝子操作をしている会社が気に食わない、そういう人たちはすぐに攻撃に出ます。我々はソーシャルメディアの中で人々が何をしているか、どんなことが話題になっているかを見て、被害に遭いそうな、攻撃されそうな人たちに警告を発することもしているのです。

また、NCFTAのアナリストたちは、オープンソースから様々な情報を入手します。我々のデータベースには11年以上に渡り、多くのデータが蓄積されています。サイバー空間において高度な技術を持つ犯罪者は、お金や

¹ Command and Control server の略。攻撃者の命令に基づき動作するコンピュータ・ウイルスに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

企業秘密を盗むことが非常に上手ではありますが、そうした者でも、最初はミスをして自分の実名を使ってしまうとか、実際の住所を使ってしまうということがあります。こうしたものをデータベース化しておけば、後々大いに活用することができるのです。

8. サイバー空間の脅威に対応するための国際連携の在り方

NCFTAは、常にパートナーシップの発展を追求しています。脅威はグローバルであって、あらゆる国から迫ってくるわけですから、自分の国だけを見ているのでは不十分です。もちろん、国によって、協力的な国もあれば手をつけられないほど非協力的な国もありますが、我々は、これまでに34か国以上の法執行機関、民間企業、学術機関と協力関係を築いてきました。

また、NCFTAでは、毎年90日間ほど、世界各国を対象にしたインターンシップを開催しています。ここでは、各国の法執行機関の参加を募り、NCFTAが、サイバー空間の脅威として何を見ているのか、どのような事件を扱っているのかなどを知ってもらうとともに、実際に協働作業を行います。その過程で、互いに友情をはぐくみ、信頼関係を構築していきます。改めて申し上げるまでもなく、この信頼関係こそがNCFTAの基盤です。

このようなインターンシップの参加国は、2011年は6 か国、2012年は11か国、今年は日本を始め16か国に上っています。来年は20か国以上の参加が期待されています。

国際連携についても、お互い顔を知ると非常に助かります。電話をかけるだけで、出た人が協力してくれるのです。もちろん、国ごとの法的な手続は踏まなければなりませんが、少なくとも気軽に電話をかけて、問題点に関する認識を共有し、具体的な対応を始めることはできます。必要な書類作業は、後でフォローアップしていけば良いのですから。

インターンの参加者は、本国に帰っても我々に連絡をしてくれます。「こういう情報が欲しい。」といった要請を受ければ、もちろん、我々は必要な情報を提供しますし、対応の仕方が分からないという場合にも協力していきます。こうした取組を行っているからこそ、NCFTAは成功しているのだと考えています。

9. NCFTAの米国における評価

本日お集まりの皆さんも、NCFTA の話を聞くのは初めてという方が多いのではないのでしょうか。我々は、できるだけ目立たないように、換言すれば、犯罪者のターゲットにならないように活動をしているためです。

とはいえ、NCFTAの活動は米国内でも高く評価されています。例えば、オバマ大統領は、2009 年、米国のサイバーセキュリティ政策に関する評価書²の中で、NCFTAは産学官連携の模範であると語っていますし、今年に入ってから、FBIのロバート・ミュラー長官（当時）が、会見の中で官民連携のモデル例としてNCFTAを取り上げています³。

10. NCFTAの取組による成果例

² CYBERSPACE POLICY REVIEW Assuring a Trusted and Resilient Information and Communications Infrastructure (http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf) P18 参照。本報告書は、オバマ氏が2009年1月の大統領就任後、60日間で米国の情報セキュリティ政策を再調査するよう指示したことを受けて作成されたものである。

³ 同氏の会見の概要は、FBIのホームページにて公表されている。
(<http://www.fbi.gov/news/stories/2013/february/the-cyber-threat-planning-for-the-way-ahead/the-cyber-threat-planning-for-the-way-ahead>)

NCFTAは、本年上半期において、パートナーに対して100件弱の脅威レポートを提供し、法執行機関に対しては300件以上の通報と、約40件の被疑者検挙に貢献しました。こうした活動の過程で押収した資産や、被害を未然に防止した詐欺の被害金額の総額は、数千万ドル相当と考えています。

これまで扱った個別事件の成功例についても若干触れます。まずは、NCFTAのインターンシップに参加しているある東欧の国を舞台とした、自動車オークション関連の詐欺事件です。その国は、この種の詐欺で成り立っている都市もあって問題となっていました。我々が情報を収集・分析して法執行機関に渡したことによって、7つの組織犯罪の首領を検挙することができました。しかも、この事件では、当時はあり得ないと思われていた米国への犯罪人引渡しまで行われました。NCFTAのインターンシップで培われた信頼関係が活かされたのです。この事件が成功した時は、虚偽の自動車オークションのネット広告が激減し、詐欺の被害発生も減りました。このほか、バタフライボットネットの事件においても、我々は情報を法執行機関に提供し、各国において被疑者の検挙に至っていますし、DDoS攻撃に関する事件でも情報の収集で成果を収めています。

また、直近で扱った事件として、模倣品のエアバッグがあります。エアバッグは、インターネット上でも売られており、修理工場の中には、そうしたネット上の安価なエアバッグを買うところもあるのですが、本事件の対象となったエアバッグは、機能しないのです。それどころか、その中に小型の金属が入っていて、自動車事故等でエアバッグが作動すると、細かい金属が飛び散り、それによって死亡することもあるというものです。

我々は情報を集め、今年に入ってから法執行機関の捜査に協力をしています。本事件において、既に同機関では30件弱の事件を立件し、約250億ドルの犯罪収益の押収と250個以上のエアバッグの差押えをすることができました。事件検挙につながったということで、我々にとっても非常に大きな成果でした。米国ばかりでなく、世界各地で売られていたので、多くの人がこれで救われたと考えています。

さらに、我々の最近の取組の一つを御紹介すると、“Pay day loan scheme” —犯罪者が会社などに電話をして「債務を返済しないと電話ができないようにしてやる。」などと脅し、応じないとインターネット経由でその会社に電話をどんどんかけてきて、その会社の電話回線を麻痺させるような行為一への対応を行っています。

同様の行為によって、緊急の対応センター、病院、警察等への電話がつながらなくなる事態もあり得るので、これは国家安全保障上の脅威でもあります。我々は、電話会社や法執行機関と連携するとともに、電話会社やセキュリティベンダーに対して、これを防ぐ技術的な仕組みが構築できないかを検討しているところです。

11. 組織犯罪のサイバー化への対応

我々の大きな関心事項に、サイバー空間を経由して犯罪収益がどこに行っているのかということがあります。米国だけで数十億ドルが犯罪収益として国外に流出し、複数の国に移されています。NCFTAでは、米国内のみならず、世界中で起きているサイバー関連の詐欺の被害額がどれぐらいで、それがどこに移されているのかについても調べています。

現実空間における従来型の犯罪とサイバー犯罪は重なってきています。サイバー空間で対処する我々にとっては、シカゴのギャングは街角には立っていません。彼らは、建物の中に入り、キーボードを使って仕事をしています。今や、彼らにとってはサイバー空間で犯罪を行う方が安全であり、その方がより多くの金を手に入れることができるのです。米国では犯行の手口がますます巧妙化し、犯罪収益は拡大しています。非常に重大な問題です。

犯罪収益がどこに行っているかを考える際に重要なのは、組織犯罪という視点です。ただ、サイバー犯罪には、組織の継ぎ目がありません。例えば、虚偽の信用情報やボットネットを必要とすればどこからでも買うことができるなど、犯行に必要な道具はサイバー空間を通じていつでも入手することができます。また、あらゆる専門技術も金さえ払えば手に入れることができます。それらを用いて自分たちを組織化した上で、ターゲットに攻撃を行うといったように、犯罪組織におけるサイバー犯罪は、非常に巧妙化・複雑化されています。

そして、最悪なことに、そのようにして奪われたお金の一部が、人身取引、売春、児童の搾取、スパイ活動、マネーローンダリング、高齢者からの金銭搾取といった、この場にいる全員が関わりたくないと思うような、更に重大な犯罪の資金として使われているのです。

我々は力を結集し、このような組織犯罪と戦わなければなりません。サイバー犯罪によって収益を上げ、その犯罪収益が更に重大な犯罪に使われている点から見ても、我々是一緒になって、こうした犯罪から社会を守らなければならないのです。

しかし、過去の歴史や私の経験からも言えることですが、こうしたサイバー空間の脅威は、企業、組織、官公庁、法執行機関のどこであれ、単独で太刀打ちすることはできないことは明らかです。全員が一緒でなければならないのです。日本では、今、「日本版NCFTAの創設」に向けて検討を始めていると聞いています。我々は、お互いがパートナーとして協力し合うべきです。お互いがより賢く、より強くなるために、国境を越えて強い協力関係を築いていかなければならないと考えています。

12. 最後に

サイバー空間に脅威を与える者には国境がありません。脅威と無関係なものは存在せず、脅威から被害を免れる人も存在しません。サイバー空間を悪用してお金を儲けることができる限り、何であれ、誰であれ標的になる可能性があります。我々はこうした脅威に対し、グローバルな視野を持ってアプローチしていかなければならないのです。

そのためにどうすべきか。犯罪者たちに目を向けると、情報を共有し、互いの専門性を共有しています。犯罪の手口やノウハウも共有しています。脆弱なターゲットがどこにいるのかについての情報や攻撃に必要な技術も共有しています。

我々も同じことをしなければなりません。民間企業である「産」、学術機関である「学」、そして法執行機関としての「官」が連携してリソースを共有し、より強く、より良好な関係を築かなければなりません。パズルを埋めるために必要なピースを共有し、サイバー空間の全体像を把握して、犯罪者が誰で、何をターゲットとしているのかを突き止めなければなりません。我々は、彼らよりも効果的に動き、彼らが行うサイバー犯罪に先行しなければならないのです。

我々は戦略を練り、常に世界中の国々との連携を模索していますが、信頼に値しないような相手と連携するつもりはありません。我々は、日本のように、信頼に値する十分な評価を持ち、問題の深刻さを認識し、この戦いに挑もうとしているパートナーと連携をしていきたいのです。

いかなる国も、企業も、また個人も、サイバー空間の脅威に対し、単独では太刀打ちできないからこそ、情報とリソースを共有し、一緒になって戦わなければなりません。そして、我々は、この戦いに勝利しなければならないのです。

御静聴いただきありがとうございました。

【基調講演②】産学官連携によるサイバー空間の安全性確保 ～犯罪に強い社会の実現のために～

情報セキュリティ大学院大学学長 田中 英彦

1. サイバー空間の安全性確保（はじめに）【図1～3】

これから、少しお時間をいただいております。ポイントは、「対策の実効化に向けて」ということですが、中身に進む前に感想のようなところから入りたいと思います。

サイバー空間の安全性確保を考えてみますと、もちろん犯罪に強い社会を作らなければなりません。犯罪が起きにくい、または起きててもすぐに対策がなされる状況を作らなければならないわけです。

ただ、それを実現するためには、様々な対策を実施していかなければならないし、多様な犯罪事象に対応するための活動もしていかなければならないし、国際的な連携も必須だと思います。

全米工学アカデミー（National Academy of Engineering）で、現代において解決することが非常に困難とされる問題をまとめた“GRAND CHALLENGES for Engineering”¹というものがありますが、この中に「サイバー空間の安全性の確保（Secure cyberspace）」とあります。安全なサイバー空間を作ることがいかに難しく、チャレンジングなものであるかを端的に示すものだと思います。

2. 情報時代の犯罪【図4、5】

情報時代の犯罪にはどういう特性があるのか。非常にシンプルな感想ですが、まず、「道具の変化」ということが言えると思います。手紙や電話という道具から、インターネットによるメールに変わりました。次に、道具の変化によって、人々の意識が変わってきます。文書を盗むという誰でも悪いことだと思いますが、コピーをするという犯罪意識が薄れてきます。また、「手紙を送る」から「メールを送る」になると、1万通でも楽に、そしてタダで送ることができるようになります。

また、面と向かっての会話は一過性のものですが、送信データは消えません。面前で話したことは相手の記憶の中以外には残りませんが、メールは一旦送るとあちこちにコピーされてずっと存在し続けます。それが後々犯罪につながることもありますよね。

こうした情報時代にあっては、攻撃側は多くの隅を突くことができる一方、防御側はあらゆる可能性をチェックせねばならず、非常に辛い立場に立たされていると言えるでしょう。

サイバー犯罪の歴史を動機面に着目して整理すると、最初は愉快犯が自らの力の誇示のために行っていたものが、次に金銭を目的とするようになり、仕事でサイバー犯罪をするプロ集団が出現し始めました。それから、「ハクティビスト」と呼ばれる思想問題や国際問題を主眼とする者たちにも利用されてきました。そして、最近では、色々な人たちがスマホを使っているの、それがすぐサイバー犯罪につながるような状況にもなっています。

3. 情報時代における問題と組織的対策の在り方【図6～14】

(1) 変化への対応～ソフト・ローからハード・ローへ～

そうした状況の下での対策ですが、まずは「変化」へ対応しなければなりません。従来のサイバーがなかった時代から、サイバーが当たり前の時代、むしろサイバー中心の時代の中で、犯罪に対応していくように組織を変えなければなりません。そのために人の対応、組織構造も変えなければならない。対応する各部門の方々

の知識も作り直さなければならない。これは、設備面も同様です。

また、新しい技術がどんどん変化していくわけですから、それに追従して行くことも必要であり、そのためには民間との協力が不可欠となります。

さらに、犯罪形態が変化している情報時代にあつては、それを踏まえて「何が犯罪か」に関しての再定義も必要のように思えます。ただ、最初はソフト・ローで臨み、その後にハード・ローというかたちで取り組んでいくことが重要だと思います。

(2) これからの警察への「期待」～世界に冠たる「新しいおまわりさん」の実現を～

私の勝手な期待ではありますが、「これからの警察への期待」ということを考えてみました。

情報時代には集中と分散で対応することが重要です。インターネット、スマホ等様々専門的に対応することは当然あるとは思いますが、それ以外に、従来から存在し、我々の身近にあつて物理的安心感を与えるもの、それはポリスボックス（交番）です。この存在は、サイバー時代でも役立つのではないかと思いますし、その安心感は重要だと思っています。

警察は、世界に冠たる「新しいおまわりさん」になっていかなければならない。もちろん、犯罪への対応能力は色々あると思いますが、サイバー犯罪に対し、すべての人が専門家になるわけではありませんから、難しいことをつなぐことのできるような人をあちこちに置いておく。情報問題の駆け込み寺のように、「交番・駐在所+Web」といった発想もあるでしょうし、「民」からの自主的な情報発信をうまく使っていくのも重要ではないかと思います。

(3) サイバー情報の一元化を

米国のセキュリティ政策は昔から色々ありました。中でも、官民連携については、昔から非常に強力なものがあります。もちろん、日本も色々な対策を講じてきました。しかし、サイバー犯罪に関しては、米国に比べて、まだ、しっかりした対応が取られていないように思えます。

ところで、犯罪とは直接には関係しませんが、最近の話題に行政手続番号法（マイナンバー制度）があります。これは、様々なデータを番号でリンクして、解析していくときの基本になるものです。上手に言えば大変強力になると言われていますが、個人情報の保護には、理論的限界があるということを申し上げたいと思います。いくら「これをやってはいけない。」と決めても、データとデータをリンクさせて、禁止した情報を知ることが完全になくすのは無理です。法律で決めるさじ加減が、理論的ゼロを満たすものではありませんので、そこを運用においてうまく作っていかねばなりません。

クラウドについても同様です。例えば、米国企業のクラウドデータに日本からも自由にアクセスできるわけですが、現状では、そのクラウドデータの帰属をどう捉えるかについて統一されたルールがありません。米国とEUではそれぞれ異なる捉え方をしています。よって犯罪に関係するデータがクラウドであった場合、そのクラウドを持つ企業が従うべきルールや検査機関が捜査を行う際に対象となるクラウドデータへのアクセスに関して、国際的対応の在り方も問題になってきます。

こうしたことから、サイバー情報の一元化が重要となってきます。国際的にもそうであるし、国内的にもサイバー情報に対して統一性が必要であり、統一された基準を継続して使っていくということです。もちろん、そのための法律の整備も必要でしょう。「インテリジェンス」という言葉が、こういう話しにはよく出てきますが、そうした考え方に基づいての統制が必要です。単にインターネットの分析をするというだけではなく、犯罪につながる分野のインテリジェンスを考慮しながら、情報の統制を行っていくことが必要です。

また、そうした分野を公共・民間・防衛に分けて、それらの分野の区分を明確にした上で、お互い連携する

という仕組みはもちろん必要でしょうし、それに対応するマンパワーの量も質も当然求められてくるでしょう。

お隣の韓国では、公共・民間・国防の分野に区分して協調しています。民間の韓国インターネット振興院(KISA)が中核となって、95%以上の情報を把握しています。こうした例も我が国にとって参考になるのではないのでしょうか。

4. 対策の実効化に向けて【図15～35】

(1) 情報共有のために

ア 産学官における情報共有

さて、これからが本題ですが、対策の実効化に向けて考えてみたいと思います。

まずは、情報共有です。情報共有の必要性は言うまでもないでしょうが、産学官は、それぞれ活動している分野が違うので、把握している情報も異なります。よって、そうした異なる特性を利用することが必要になってくるわけです。また、サイバー犯罪は、どの主体にとってもあまねく「犯罪」ですから、一部に閉じた性質のものではありません。連携の意義は、そういうところにあります。

過去を見ても、これまで警察は犯罪の専門家でありましたし、これからもそうだろうと思います。しかし、サイバーの技術、サイバー犯罪ということになると、警察は、必ずしも専門家ではなく、民間をリードする立場にはありません。技術が発達していくのは民間の方が早いわけで、それと協力するのは当然必要になってくるでしょう。

イ 情報共有のインセンティブ

産学官で情報を共有することについて、どういうインセンティブがあるかを考えてみると、まず、当然ながら、「官」にとっては、広い情報源をリアルタイムに得ることができるため、コスト性能比が良いという点があります。また、新たな分析手法を得たり、新たな分析手法に関わり人材育成が可能となったりもするでしょう。それに、社会の認知が共有できるという点も挙げられます。「官」だけで閉じてしまい、クローズドで何をしているか分からないということでは認知が進みません。

「民」と「学」については、安全を享受すること、そのために官の捜査に協力するということが挙げられます。

個別に見ていくと、まず、「学」にとっては、現場情報を使った対策研究ができます。大学にいる人間にとって、サイバー対策を研究するのはとても面白いことですし、若い人たちも大変興味を持ちます。しかしながら、現状では、研究対象とするデータについて、現場のものを見ることはできません。「サイバー犯罪はこういうものだろう。」と、勝手に想像して対策を考えていくのが基本となっており、これでは隔靴搔痒でうまくいきません。上手に仕組みを作り、共有できれば大変嬉しいと考えております。

次に「民」、企業にとっては、企業等への攻撃に対して協力して対応することができるようになりますし、分析手法や対応システムなどに関するニーズを得ることができます。それから「官」との情報共有が契機となって、民間組織間の情報共有を行うことができるようになります。普通であれば、競争している競合相手の会社とは、直接的な情報共有はしませんが、「官」が一緒になっているところには自分たちのメリットもあるし、情報の提供ができる。そういう形で民間組織間の情報共有が可能になる。これはとても嬉しいところでしよう。

現場情報がいかに嬉しいかという例として、NISCの研究者が私どもと協力して行ったものを御紹介します。

文書を添付メールで送る際、その中にマルウェアが入っていることがよくありますが、それが標的型攻撃の

契機になるので、文書が感染していることを判断するのはとても大切です。ところがマイクロソフトのOffice文書に対して、一般の検証機能では38.8%と、既存のソフトではあまり検出できない状況にあります。しかし、現場情報を上手にを使って研究すると98.5%の検知率が達成できるのです。PDF文書も同様です。最近のデータですが、悪性のPDFファイルについて、99.4%の検知率を達成しています。これは、現場の情報を使うことがいかに重要であるかのサンプルの一つと言えるでしょう。

ウ 情報共有に係る留意点

情報共有は嬉しいことですが、同時に留意しなくてはならない点もあります。

まずは、官民が情報共有の思惑についてアンバランスが生じないようにすることです。官にはある種の威力がありますし、民には善意ももちろんありますが、メリットを勘案する必要もあるでしょう。そうしたことを踏まえて成果を駆動させていく必要があります。

元の情報源と提供する情報との関係にも留意する必要があります。アクセス権について言えば、提供側が「自分はこのを出せる」というかたちで判断して出し、出した後は共有し、そこでインターフェースを切ることが考えられるでしょう。また、プライバシー問題は、技術を使ったり匿名化をしたり色々なことをしていく必要があります。ただ、民が自主提供する情報は嬉しいですね。自主提供だからこそ、使いやすいわけですから。

また、信頼関係の構築にも気を留めていく必要があります。情報共有は、信頼関係がベースとなりますから、明示的なメンバー間の人的信頼関係が非常に重要です。

エ 情報共有の在り方

共有の在り方に関しては色々議論があろうかと思います。日本ではまだ経験がないわけですから。しかし、NCFTAの経験などを参考にしながら、私たちはこれから作らなければならない。その際、協力している事実オープンにして、それ以外のことは、NDA²を結ぶなりしてしっかり保たなければいけないというのも考え方としてあるでしょう。

そうしたことを前提にして、データの共有形態の在り方を書いてみました。【図23】の上は、左の組織から右の組織にデータを渡し、渡し切った後は、使うのは自由というかたちでの情報共有の仕方です。同じ図の下はそうではなく、左の組織から共有組織にデータを渡し、その中で関係者が集まって分析して結果を出すというかたちでの共有の仕方です。こちらは、上と異なり、データをそのまま渡して後は知らないということではありません。よりセンシティブな情報を共有し、より立ち入った共有形態における共有の仕方は、こちらが適しているのではないかと思います。NCFTAはこちらの形態という気がいたします。

【図24】では、左から情報が入ってくるのですが、情報は、ネットワークで入ってきたり人から入ってきたりします。様々な機器を用いてそのログを取る、何か処理をする、あるいは人による分析をするというようなことをどんどん進めていって、レポートを作成します。その際に、官の力と民の広さで情報収集を上手にやっていくのです。関係者である警察や民間企業が目的に合わせて分析をしていく。こうした作業を行っていく中で、適当なところで分析の目的に応じたインターフェースができるという気がしています。

(2) 情報共有における基本問題

ア 情報に対する様々な制約について

次に、情報共有における基本問題を考えてみたいと思います。

情報については、様々な制約がありますが、一つは、情報収集における制約です。

例えば、不正アクセス防止法について、何か不正アクセスがあったときにその事実を報告として受ける形で

の情報収集というのは努力義務となっています。これは、提供してもらえると嬉しいという類いの規制であり、ほとんど規制がないようなものです。

また、情報分析という観点からの制約を考えますと、明治時代からある、信書の秘密というものもあります。封筒の中を見てはいけない、誰から誰へというのが書いてある表面は良いが、その中を見てはならないというものです。この点、通信になると電気通信事業法で同様に制限されていますが、現在の通信の実態は、法が想定している範囲よりもっと広がっています。

情報の保護に係る制約についても、例えば、個人情報保護法で決まっているのは、法の定義に書いてあるように、情報が暗号化によって秘匿化されているかどうかを問いません。これは、実に引かかるポイントです。いくら暗号化してしっかりしたUSBに情報を入れていても、落としたら情報漏洩となってしまう。これは実態を踏まえたとき、本当に漏洩なのだろうかと思うのです。もちろん、漏洩とされては大変ですから、落とさないように一生懸命頑張るわけです。落としたら大変なことになると。しかし、これは無意味な管理強化のような気がします。

その他、ビッグデータからの脅威として、リンクが容易になることによって個人が特定されやすくなるというところもあるでしょう。

イ ログ取得問題・信書問題について

ログの問題も同様です。電気通信事業法でログをとること、特に完全なログを取っておくのはとてもコストがかかります。ログを義務化すること自体、事業者にとってみれば大変重いことです。しかし、ログはやはり役立つものですから、何らかの形で、インセンティブとともに義務化をするといったような、そういうアプローチも必要ではないかと思います。

また、信書問題についても、現在は物理的な回線の上でメッセージが送られる時、物理的なその源と宛先はログとして取ることができますが、中身の分析はできません。実は物理的な送受信の上にISPが関与してデータを送っています。しかも、更にその通信にはLINEのような色々なアプリケーションが載っていて、誰かと誰かの間でメッセージ授受が行われています。

このように、通信というのは様々な階層構造³をしていますから、どこの階層における通信をチェックするのかを意識する必要があるのですが、上位層の方は全然チェックできていないのが現状です。しかし、欲しいのは上位層の通信という可能性もありますので、物理的な一番下だけのログで済ませてしまうのも困るわけです。こうしたことからしても、時代に適合していない可能性があります。

ウ 問題の現状と解決に向けて

こうした問題があるので、解決に向けての要請があります。「信書の秘密をどうにかしてほしい。」「暗号化の秘匿化機能を考慮してほしい。」といった、収集と解析性に関する問題を解決しなければなりません。データを集めるだけでなく、それを解析して必要なデータを取り出すことができなければなりません。あまりにも秘匿化して、名前も何も分からないようにして収集していたのでは解析には使えませんから、個人情報を保護しつつ、解析性をキープできるように、両方をうまくバランスさせなければなりません。

ただ、それは技術的には可能ではないかと思われます。

従来は、「適当なバランスを探してください。」というところで法律が終わっています。しかし、それは実際問題の解決になっていないという気がします。私は、技術として、そうした限界を破る両立性も実現可能であるということを申し上げたい。また、技術を考慮した新しい世代の法制があると便利ではないだろうかとも思うのです。

【図30】のように、例えば手紙であれば、表面は封書で、書かれた中身は封書内です。この点、メールでは、それ以外に制御情報などが付いています。文書の中にも、S'、D' とあるように、宛て先が更に存在しているかもしれない。実はそこをうまく使うと有用なことがあります。中身は見なくても、制御情報を見るだけでマルウェア判断に使えるなど、色々なことができます。内容とは無関係に、犯罪情報をチェックできる可能性があるのです。

暗号化問題に対しては、JNSA⁴の「組織で働く人間が引き起こす不正・事故対応WG」の主査である甘利康文氏が現実的方法⁵を提言しています。「暗号化していても（記憶媒体を）落としたらだめだ。」ということに対して、暗号等により秘匿化されていた場合は、紛失が起こっても漏洩事故とはみなさないという案です。その前提には、運用が適切にされている場合という条件もありますが、基本はこのようになってほしいと思います。そうすると管理がとても楽になり、無意味な管理強化をしないで済みます。実質面から見てしっかりと守ることが出来ているわけですから。そうした面におけるインターフェースを作してほしいと思います。情報漏洩は数だけはたくさん発生していますが、それが実質的に見ても被害を出しているのかどうか、その辺りを見た方が良いのではないかと思います。

(3) データベースの構築の在り方について

「個人情報をたくさん集め、ビッグデータとして分析して結果を出す。」というデータベースを作る場合ですが、個人情報に対しては提供してもらうときにポリシーを書いてもらい、ポリシー付きで提供し、それを集めてデータベースを作る。もちろん、情報は完全に暗号化し、外からアクセスしても分からないようにします。

しかし、欲しい情報については解析性をキープします。【図31】で処理装置とありますが、欲しい情報の定義を入力して解析すると、その結果データだけが出てきます。しかし、個人情報はキープできる。ポリシーはキープする。こういったシステムは、技術的には実現出来るのです。保護が困難に思えるという理由だけで、広すぎる保護範囲を設定するのもどうかという気がいたします。

消費者がネットにアクセスして何かを買うという行動をしたとき、その「買った」という情報を集め、その人が一般的に何を買いたいかを分析して、その人に宣伝会社が関連する広告を送るという仕組みがありますね。これに対し、これまでは「個人の嗜好が暴露されるから嫌だ。」ということになっていたのですが、これも上手にやると、その人向きの宣伝情報は確かに個人消費者に届けることができ、しかも誰がその情報、どういう指向を持っていたかについては広告主たちには分からないという仕組みを作ることができます。

このように、技術的には色々なことができるのです。

(4) サイバー対応力の強化のために

データベースのほかにも、サイバー犯罪のために色々なことをやらなければなりません。

重要施設には、通信、電力等以外にも、水道や交通など直接電気通信に関係ないインフラがありますが、そういうインフラも、コントロールには電気通信を使っています。そのコントロール部分だけは区別して重要な通信基盤であることを指定してコントロールすることが必要です。

また、サイバー犯罪に対する対応力を強化することも大事です。サイバー対応力を強化するためには、防御に偏せずリスクを許容するとともに、実質被害を発生させないようにすることが重要ですが、リスクの許容については、防犯カメラの経験は有効ではないかと思います。

防犯カメラは、今はたくさん入っていて、とても役立っています。しかし、防犯カメラが入ってくる前、例えばロンドンでたくさん入った時にどういう反応があったかということ、個人の活動が暴露されるといって嫌がったわけです。しかし、今は非常に多用されている。そのメリットが見えてきたおかげで、そういうことは言

われないわけです。ネットもそうなってほしいと思います。実際の犯罪や抑止効果がはっきりすると、ネットの情報についても、提供が楽になってくるのではないかと思います。

5. 日本版NCFTA創設に向けて【図36～42】

(1) 日本版NCFTAの目的と機能について

日本版NCFTAは、官民でメンバーを派遣し、サイバー犯罪に対応する実務機能として、民間との接点になります。

従来は、サイバー犯罪に対応する実務機能がありませんでした。もちろん、現在、日本には、インターネットに関する監視組織はあります。しかし、それはサイバー犯罪を抑止しているのではなくて、モニターして「こうなっている。」という情報を提示することが主目的です。日本版NCFTAは、そうではなくて、サイバー犯罪に対応するということにもその目的があるべきでしょう。

その機能としては、色々な情報を集めるわけですが、警察本体からも情報をもらうというかたちも必要です。その上でのフォレンジックス、インテリジェンス分析などが中心になるかと思います。

(2) 情報の共有、保護に対する制度の在り方について

制度的なことを考えてみますと、産学官の情報共有に対する制度は、あまりきっちり定められていないのが現状です。情報共有制度をうまく活用したいと思っても、法律がまだ追いついていない。よって、公私協働型の政策手法を取り入れていくことが必要だと思います。

法律よりも、ガイドラインやその他のソフト・ローを使いながら実効性を持たせるという方向性があります。サイバーに関する技術や状況は変化が激しい。ものすごく変化が激しい場合には、情報の利活用に対してハード・ローで規制内容を記述していくのは大変であり、難しいでしょう。むしろ産業界の自主規制で行い、自主規制ではうまくいかないところを国家が法律で規制していく。この辺りのバランスをうまく作る方が良いような気がします。

諸外国での状況を見ますと、米国はビッグデータを利活用したいと考えていて、EUはプライバシー保護重視に傾いています。日本では、最近になって色々な動きがありますね。

ただ、サイバー犯罪に関しては情報自体の保護が必要です。情報は財産です。情報を盗んでも犯罪にならないのでは困るわけですから、企業秘密が財産として保護され、それを盗んだら犯罪になるということについて、何らかの検討が必要ではないかと思います。

(3) 情報セキュリティに関する研究の必要性

従来、情報セキュリティ産業がそれほど大きくなかったからかもしれませんが、一般企業も含め、総合的なセキュリティ意識が希薄ではなかったかと思います。確かに情報セキュリティは新聞紙上を賑わせてはいますが、それだからといってお金を出して企業を守るためにサポートすると言われると、そこまで至っていない。例えば、企業内にセキュリティ担当者を設置することを推奨する、企業内システム基盤のセキュリティレベル維持を推奨するなど、何らかのサポートが必要ではないかと思います。

情報セキュリティに関しては、国家安全保障のために研究は不可欠です。完全に技術を外から輸入するだけでできるかと言われると、残念ながらそこまでの交渉力はないし、サイバー空間の脅威は激しく動くので、困難であると思います。よって、情報セキュリティに関する研究を自分たち自ら行うことは、必要だと思います。

また、ICチップなどもそうですが、一つのチップにどんどん色々な機能が入ってきており、中身が分からなくなってきました。スマホなど、1チップになってしまうと中身に何が入っているか分かりません。インター

フェースの端子を見ても、何が入っているか分からない。そうなると、犯罪捜査のときの証拠固めのときに活用しようとしても限界が出てくるわけですから、こうした「ブラック・ボックス化」への対応も必要ではないかと思います。何かの端子を出しておくなど、規制することが国際的にできると良いと思います。

これはサイバーにおける政策の全体構造ですが、社会の常識の上にサイバー組織があり、その上に新しい情報のセキュリティ制度を築いて、生き生きとした情報社会を実現する、このような構造ではないでしょうか。

6. 関係人材の育成【図43～48】

(1) 様々な人材が必要

しかし、こういうことをするのにには人材が不足しています。残念ながら、現状では何万人も不足しています。一般市民、官民全体の専門家、さらにはエキスパート、トップガン、たくさんの人たちが必要です。セキュリティ計画・対応、監視・情報収集・分析、インシデント、インテリジェンス、情報法制等専門知識による分類、国内治安、国際対応、国防、重要インフラ、一般企業、セキュリティ企業、NPO等組織の役割による分類、それぞれに応じて様々な人々が必要です。

育成プログラムについても、人材育成レベルと種別に応じて、教育・訓練組織を使うことや、警察地方組織間の切磋琢磨競争を設けることや若い人材の獲得等色々なものが必要になると思います。

教育内容も同様です。教育・訓練組織を利用するとしても、リテラシーから始まり専門情報に至るまで色々な情報が必要です。質的な面からは、特に現場経験が重要になってきます。人材育成を進めるためのインセンティブとしては、やはり、若い人材発掘に公的な補助をすることが重要と考えます。例えばバウチャー制度なども有効ではないかと思います。バウチャーをもらうと、無料で高等教育を受けることができるようになります。その代わり、受けた後の3年間はセキュリティの官・民の機関で働くなどという制度設計をすれば、若い人たちはお金がなくてもそちらを志すことができますし、実務能力の育成にも役立ちます。

また、CTF⁶のように、サイバーの深いところに入っていくような技術に関しては、若い人たちに適性があります。喜んで楽しんで生き生きとやる人たちを育てて、引っ張り上げていくことが必要ではないかと思います。

¹ “GRAND CHALLENGES for Engineering” (2008) の内容については、以下のホームページで公表されている。
(<http://www.engineeringchallenges.org/>)

² Non-Disclosure Agreement の略。秘密保持契約のこと。

³ コンピュータネットワークにおいてデータをやり取りするには、同一のプロトコル（データをやり取りする形式・手順）に基づく必要があるが、ネットワーク設計においては、概念上、プロトコルを機能的に分割し、階層（レイヤー）として整理している。プロトコルレイヤーのモデルとしては、ISO（国際標準化機構）が提唱し、プロトコルを7つの階層に整理した「OSI参照モデル」が最も一般的である。OSI参照モデルについては、独立行政法人情報処理推進機構（IPA）ホームページ「オープンソフトウェア：OSS人材育成：OSSモデルカリキュラムV2」にある「ネットワークアーキテクチャに関する知識（基礎レベル）の学習ガイダンス」を参照。
(<http://www.ipa.go.jp/files/000018486.pdf>)

⁴ Japan Network Security Associationの略。特定非営利活動法人日本ネットワークセキュリティ協会のこと。

⁵ 甘利康文「「記録媒体紛失」による情報漏洩事故を減らす現実的方法について」『JNSA Press第36号』（2013年9月）を参照。なお、同氏の論文は、JNSAホームページ（<http://www.jnsa.org/>）から入手可能。
(http://www.jnsa.org/jnsapress/vol36/2_kikou.pdf)

⁶ Capture The Flag の略。情報セキュリティ分野において技術を競う手法の一つ。世界で多くの大会が行われている。我が国でも、特定非営利活動法人日本ネットワークセキュリティ協会が「SECCON 2013」を主催している（「SECCON 2013」については、同協会ホームページ（<http://www.jnsa.org/seccon/>）を参照。）。

【講演資料】

産学官連携によるサイバー空間の 安全性確保 - 犯罪に強い社会の実現のために -

田中 英彦
情報セキュリティ大学院大学
2013年9月26日

図 1

目 次

1. サイバー空間の安全性確保
2. 情報時代の犯罪
3. 問題と組織的対策
 - 変化対応、米国政策、日本政策、クラウド域外アクセス、政府内対応、対応組織例
4. 対策の実効化に向けて
 - 情報共有、サイバ対応力強化、制度の考察、情報自体の保護、企業育成と研究開発、政策の全体構造
5. 人材育成
 - 必要人材、プログラム、教育内容、育成の実効化

図 2

1. サイバー空間の安全性確保

- 犯罪に強い社会
 - 情報犯罪が起こり難い、起こっても対策が直ぐされるという状況の醸成
- それを可能にするために
 - 対策：制度設計、組織設計、情報システム、対応人材の手当、社会の意識とリテラシ
 - 対応活動：情報収集、分析、対処、防御、管理
 - 国際対応：ネット社会は越境容易、不可欠

図 3

2. 情報時代の犯罪

- 道具の変化
 - 電話、手紙 → インターネット、スマホ、クラウド
- 意識の変化
 - 文書を盗む → コピーする(犯罪意識希薄)
 - 手紙を送る → メールを送る(1万通容易、只)
 - 紙の情報 → スマホ内に在る情報
 - 情報は紙から → 情報はネットから
 - 本(IP) 有料 → インターネットで無料
 - 数日の時間差(移動) → 数秒の時間差(ネット)
 - 会話は一過性 → 送付データは消えず、後に問題源
- 攻撃側と防御側の立場
 - 攻撃側有利、多くの隔(変更容易)を突くことができる
 - 防御側は、あらゆる可能性をチェックする必要

図 4

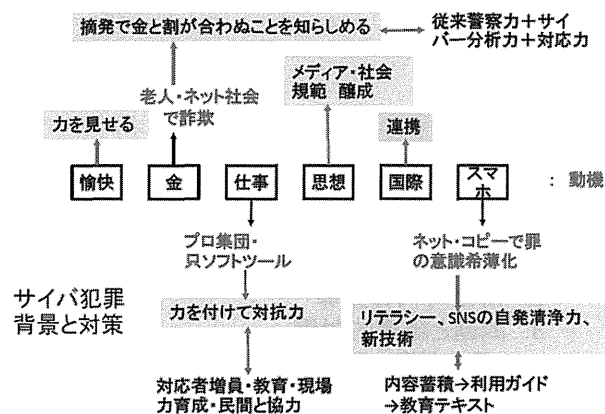


図 5

3. 問題と組織的対策

- ① 変化への対応
- ② 米国の政策
- ③ 日本の政策
- ④ クラウド域外アクセス問題
- ⑤ サイバー情報一元化
- ⑥ サイバー対応組織例

図 6

① 変化への対応

- 犯罪のサイバー化に適応する
 - － 可能な組織構造：人の展開とネット化の融合
 - － 犯罪対応部門の、犯罪変化に追従した知識の醸成と、設備の更新（現場ツールの必要性）
 - － 新技術に追従する民間との協力関係を築く
- 法制への対応基本
 - － 犯罪の再定義：情報時代の犯罪を踏まえ、ガイドライン等ソフトローの対応でリード
 - － 適切なタイミングでハードローへの反映

図 7

これからの警察への期待

- 情報時代に集中と分散で対応
 - － インターネット、スマホ利用の情報犯罪に専門的対応、情報の新技術や動向に民間との連携
 - － 従来の近くに居る物理的安心感
- 世界に冠たる「新しいおまわりさん」へ
 - － 犯罪対応能力：犯罪判断、初期対応、専門員へ繋ぎ
 - － 専門対応網は、ローカルと集中の組み合わせ
 - － 駐在所+Web：情報問題駆け込み寺、情報対応町の専門コミュニティとのリンク（ネット時代の人連携：論理＋物理）
 - － 怪しいメールなどを民が自主収集する機構
- 証拠保全機能
 - － フォレンジック能力向上

図 8

② 米国の情報セキュリティ政策

- 政府の取り組み
 - － 2009全米サイバーセキュリティイニシアティブ、2011連邦CS R&D戦略計画
 - － 2013.1 DODサイバー司令部(2010設置)の増強(900→4,900)、防衛だけでなく攻撃を目的とした編成
- 情報に関する官民連携：国家安全保障との関係で連携重視
 - － 2008US Cyber Challenge：官民共同人材育成プログラム
 - － 2012情報共有と安全性保護に向けた国家戦略
 - － 官民連携CS R&Dセンター、情報共有分析センタ
 - － 政府機関間、CERT、NOC、分野別連携の枠組み
 - － 官民パートナーシッププログラム、司法・インテリジェンスの情報連携
- 関連法案状況
 - － 2012, 2013重要インフラのセキュリティ強化は監視強化懸念で廃案、脅威情報の共有はプライバシー懸念で廃案
 - － 2013.2 官民連携制度策定中、2013.6 スノーデン問題
 - － 2013.7 情報セキュリティへのインセンティブ検討中

図 9

③ 日本の政策

- ・ 情報セキュリティ政策会議と内閣官房情報セキュリティセンター
 - － 公私パートナーシップの強化、政府組織・重要インフラ・ビジネスと個人
- ・ 政府機関の基盤
 - － 政府CISO、セキュリティ緊急支援チームCYMAT、政府横断的情報収集・分析システムGSOC
- ・ 総務省：PRACTICEプロジェクト
 - － サイバー攻撃に対し、先取対応研究と実施テスト計画、共有データ：国内で捕獲されたサイバー攻撃情報、他パートナー国の同種情報、DAEDALUSデータ
 - － 結果：攻撃類似性、攻撃の振る舞い兆候
- ・ 経済省
 - － サイバー情報共有イニシアティブ、電力、ガス、化学、石油、の5業界、39参加組織でサイバー攻撃情報共有実運用中、サイバー攻撃解析協議会
- ・ 警察庁、防衛省
 - － 情報技術解析課、サイバー防衛隊
- ・ 国際連携
 - － 日米、日英、ASEAN：サイバーインシデント対応協力、重要インフラ防護国際連携、意識啓発協力、人材育成協力、サイバー空間上国際的行動規範作り

図10

行政手続き番号法

- ・ 2013年5月31日成立
 - － 諸制度連携の第一歩：社会保障、税、防災
 - － リンク評価の考え方整理等、多くの課題
 - － 特定個人情報保護評価活動を通したプライバシーの適切な実効保護レベルの模索
 - ・ レベルは使用経験により変わる。分らないことから来る恐れと現実(なんとなく不安感vs実被害vs利用価値)
 - － 諸データを突き合わせることはサイバー対策の中核で、必要に応じそれを可能とすることは必要
- ・ Oエラー問題
 - － 保護の有効性限界と法的切り分けの意味認識

図11

④ クラウドデータ域外流出問題

- ・ 米国：愛国者法、外国情報監視法(FISA)の修正法
 - － 当局が米国のクラウド企業に対し米国市民以外のデータを提出するよう強制可能
- ・ EU：EUデータ保護指令の改正作業
 - － 2012開始。第42条 修正案(反FISA条項)
 - － EU監督当局の明示的な許可なく、第三国が域内の個人情報にアクセスすることを禁じる
- ・ 方向性
 - － 情報はクラウドに集められる。捜査時、そこへのアクセス可能性は重要事項：国内vs国際対応
 - － 国際的クラウド企業は、どちらかに背くので板挟み
 - － 方向案：EU側に立つ。個人情報制御権原則。全世界集中は不経済。論理的に一つ、物理的に分散も案。

図12

⑤ サイバー情報一元化

- ・ サイバー情報の一元化
 - － 対国際、対国内にも統一性が必要。継続性と法律整備、省庁所掌明確化
 - － リスク・インテリジェンスに基づく統制：専従のサイバーセキュリティ調整官
 - － 公共・民間・防衛の3分野区分と連携
- ・ サイバー部門強化
 - － 情報収集・分析・対応、人材(量、質)と設備の強化
 - － 情報流通の種類(電子、人・紙、インテリジェンス)

図13

⑥ サイバー対策組織例(韓国)

- ・ 公共・民間・国防の3分野に区分し協調
 - － 公共：国家情報院、安全行政、金融委員会、検察、警察
- ・ 民間：韓国インターネット振興院 KISA
 - － モニタと対応、民間が95%以上
 - － 機関連携：3分野間、通信業者、セキュリティ会社、国際
 - － インターネット24時間モニタリングと対応
 - － DDoS防御サービス：サイバー待避所構築、ゾンビPC検知・通知・治療
 - － 国内全Web HP(200万)のコード点検(3回/日)・遮断・悪性コード削除措置、相談センター運営
- ・ 連携：3分野間
 - － 悪性コード共有、事故分析資料共有、事故移管、調査協力

図14

4. 対策の実効化に向けて

- a. 情報共有
- b. サイバー対応力の強化
- c. 制度の考察
- d. 情報自体の保護
- e. 企業育成と研究開発
- f. 政策の全体構造

図15

a. 情報共有

- ① 情報共有連携の必要性
- ② 留意点
- ③ 情報共有の在り方
- ④ 情報共有の基本問題
- ⑤ 問題の現状と解決に向けて

図16

①情報共有連携の必要性

- 得意不得意分野:産官学
 - 民間活動/警察活動/教育研究活動
 - 企業実務現状/犯罪情報/研究情報
- 異なる特性の利用
 - 市場状況/捜査力/第三者意見
- 連合の意義
 - 異なる観点からのデータ集結
 - 思考形態の異なる分析の利用
- 過去と今後
 - 犯罪の専門性、IT技術発達で、今後は民間と重なり、協力必要

図17

情報共有のインセンティブ

- 官:安全を与え、協力享受
 - 広い情報源を実時間で得る(コスト性能比が良い)
 - 新しい分析手法を得る
 - 新分析手法に関わり人材育成できる
 - 社会の認知を得やすい
- 民・学:安全享受、捜査協力
 - 官の権限・手法で、通常得難い現場情報を入手
 - 新しい分析手法や対応システムのニーズを得る
 - 人材育成のニーズを享受できる
 - 官との共有が契機で、民間組織間情報入手
 - 官の協力で共有機構の維持が容易
 - 公への協力というボランティア精神が満たされる

図18

文書へのマルウェア埋め込み ー 現場(NISC)情報の威力例 ー

- 文書に実行ファイルを埋め込む
 - ー メールなどに添付し標的型攻撃に利用増加
- MS文書
 - ー MS 文書ファイルの場合、文書ファイルサイズや構造情報を検査、悪性文書ファイルを検知
 - ー 98.5%の検知率、一般のファイル検証機能の率は38.8%
 - ー Microsoft Office 2010 のファイル検証機能の検知率91.0%
- PDF文書
 - ー PDF文書ファイルの場合、従来PDFファイル中のJavaScript 等不正なコード検知手法で20%以下の検知率
 - ー 悪性PDF ファイルには構文解釈ができない部分、表示内容と関係しない部分が含まれる等の特徴があり、それを検査
 - ー 悪性PDF ファイル164 個に対し、99.4%検知

図19

②情報共有の留意点

- 官民間情報収集思惑のアンバランス
 - ー 官の威力、善意とメリット勘案:成果駆動
- 元の情報源と提供情報との関係
 - ー アクセス権、知的財産権:持込み者が解決
 - ー プライバシー問題:情報匿名化*、他の技術
 - ー 民の自主提供情報:真贋判定、仕組み
- 信頼関係の構築と情報管理
 - ー 共有機構の明示的メンバ間の人的信頼関係ベース
 - ー 機密対策、情報漏洩、外部からの攻撃対策

図20

共有情報

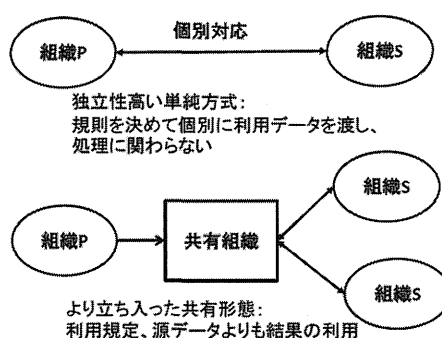
- メンバ提供情報
 - ー 産:個別企業からの脅威情報
 - ー 学:研究成果、知見
 - ー 官:捜査・犯罪関連情報
- 一般市民からの提供情報
 - ー 収集形態とパスを構築、産とも連携
 - ー 自主的提供の犯罪関連情報:従来に加えe-110番
- 情報の種類
 - ー 実時間生データ:光ファイバ、IX、メッセージ
 - ー 生でなくとも可能な対策は多い、生は民の自主協力情報
 - ー 機器ログ等、モニタ状況結果、email/文書/画像/chat
 - ー SOC、脆弱性データ、ハッカー関連情報、サイバー攻撃ケース、ハッキング手法・ツール、統計、評価結果

図21

③ 情報共有の在り方

- オープン化
 - 協力している事実はオープンにする
 - 情報共有原則と、定期的活動報告を公開
 - 第三者機関等、外部意見を受けて検討する体制整備
 - 民の自主協力情報の活用
- 情報の扱い
 - 扱う情報自体は秘密を原則：NDA
 - ステークホルダー間の情報アクセス権の明確な規定
 - 人の信頼がベース
- 情報共有の形態
 - 情報に依存する共有形態

図22



様々な情報共有形態の利用: データ依存

図23

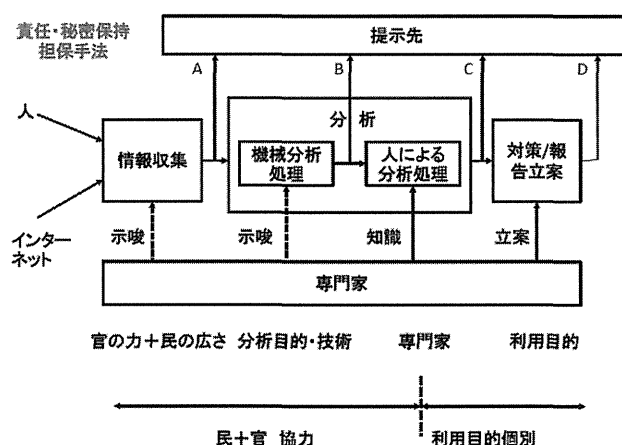


図24

情報共有のメカニズム

- 民間と官のインタフェース
 - － 民間組織に、官の特定者が関与。相互にNDA
 - － DBを官または民の特定者が特定目的に応じて利用
 - － DB内蓄積は、情報提供者の必要に応じ匿名化など措置
- 情報共有の有効性とプライバシー保護
 - － データ単位の広いアクセス権設定+利用目的の規定
 - － 護るはプライバシー、個人情報保護はその一手段、絶対視は共有の実効性を無くす可能性
 - － 利用目的の記述で最終インタフェースを定める

図25

④ 情報共有における基本問題

- 情報収集における制約: 収集
 - － サーバ管理: 不正アクセス防止法は努力義務
 - － ログ取得の制約: 電気通信の範囲、収集要請と協力による
 - － インシデント届出は努力義務なので情報が蓄積されない。IPAも、提供蓄積に留まる
 - － 現状では、官が一般モニタリングをすることは困難
- 信書の秘密からの制約: 分析
 - － 送り元、宛先情報のみ利用可能、内容の利用禁止
- ビッグデータからの脅威問題
 - － リンクで個人特定問題: 匿名化は一手段、絶対視は不可

図26

ログ取得問題

- 義務化拡大のみでは困難
 - － コストが膨大。インセンティブ(対策費、税制)が必要
 - － セキュリティ対策にはログも必要、主体的に守る推奨。サービス品質など他の形に転化
 - － 重要インフラの中でも電気・通信は、情報に絡むので、他のインフラと区別した扱いが必要
- ログ取得
 - － 米国では、インシデント時、消さないことを求めることが出来るが、既に消去済には対応できない
 - － 電気通信事業法の枠には、上位層サービスが入らない。規制無し。今後は通信とサービスが融合、ある程度の規制をかけることの是非を検討すること要す
 - － 「信書の扱い」の時代に沿った書き直し

図27

信書問題

- 従来: 信書の秘密、SD+C の内SDはログ有
- 今後: 通信の新たな枠組み、レベル構造

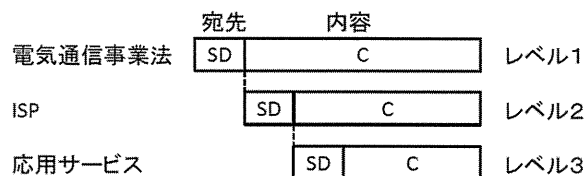


図28

⑤ 問題の現状と解決に向けて

- 要請
 - － 信書の秘密問題の新時代対応
 - － 情報収集と、それへの十分な解析性の保証
 - － プライバシー問題対処に、個人へ情報制御権を付与
 - － ビッグデータからの不安感除去
- 対応
 - － 従来の議論: 対立問題に対し「バランス」論理に留まり抜本的解決になっていない
 - － 技術: 限界を破る両立性を実現可能
 - － 技術を考慮した新世代法制の構築が必要
 - － 民からの自主的協力による情報提供の活用

図29

「信書の秘密」の情報時代に向けた再検討

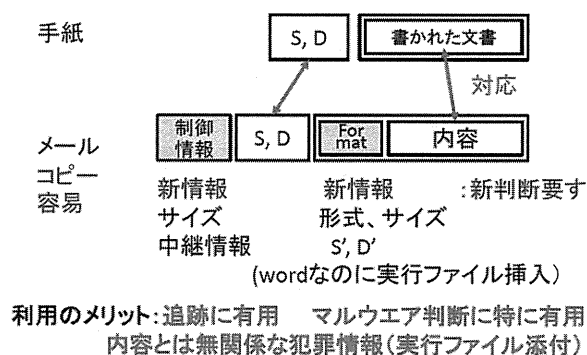


図30

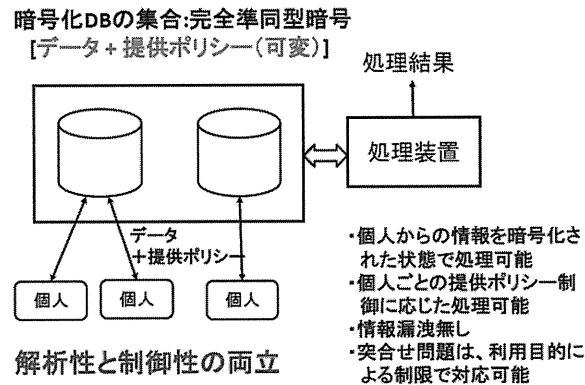


図31

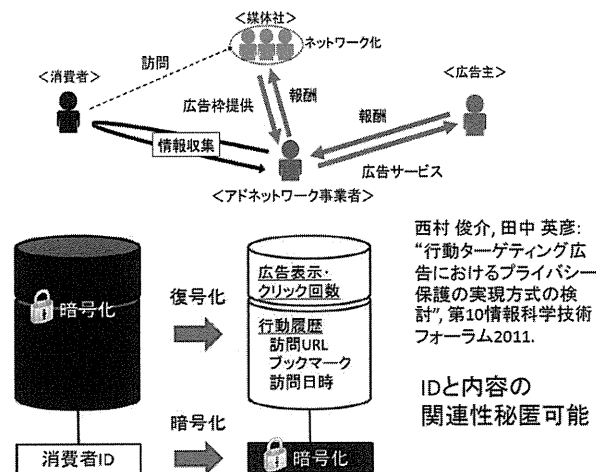


図32

新しい情報セキュリティ技術

- ・セキュアネットワーク
 - －トレーサブル、利用者保証、希望参加ベース
- ・セキュアシステム
 - －プログラム限定、セキュアOS、IO限定、セキュアPU
 - －常時モニタリング
- ・暗号の多用
 - －管理容易、高速符号化・復号化
- ・未知の脅威分析
 - －実時間検知(Black List, 振る舞い)、プロファイリング
- ・ビッグデータの活用
 - －マルウェア、攻撃事例、犯罪事例、個人情報利用
 - －アクセス履歴から有効な推奨広告: プライバシーと処理両立

図33

セキュリティデータベース上の処理

- 様々な処理
 - FW/IDS/UTMにおける処理
 - ログ分析:ログ間関連付け(SIEM)
 - DoS検出・対応、C&Cサイト発見
 - サイバー攻撃プロファイリング:国内外の侵害事故を定型化し管理、新ハッキング攻撃手法及び道具分析、関連機関・ホワイトハッカーの分析結果収集
 - 侵害事故関連性分析:事故間悪性コードの関連性分析、攻撃手法の類似性分析、時系列分析による攻撃間関連分析

図34

b. サイバー対応力の強化

- 防御に偏せず最低限のリスクを許容し、対処策を講じ、実質被害を発生させない
- 重要施設に対する情報通信基盤施設
 - 区別して指定と管理、通信+電力等
- 円滑な初期対応のための現場確認と技術支援のための法的根拠作成
- 国内外の関連機関との協調体制強化
- APT等進化サイバー攻撃の予測及び迅速対応可能システム構築
- 専門人材の拡充、必要設備の強化

図35

日本版NCFTA

- メンバ構成
 - 官(警察、他)、民間企業、大学、が派遣
- 機能
 - 他と連携して情報収集:GSOC, NISC, 警察、民間SOC, ウイルスベンダ、IPA等
 - 民間からの一般情報提供経路
 - 解析・対応・Forensics等実務を担当
 - 実務に携わることでOJT機能:senior/junior
- 経費支援
- 運営
 - 情報の扱い、人の責任、第三者対応

図36

c. 制度の考察

- 情報共有制度の現状
 - － コンピュータウイルスや脆弱性情報、インシデント情報などの報告制度、義務無しで十分に活用されず
 - － 現状は、限られた分野内でのインシデント情報共有
 - － 実時間の情報共有体制が無い
 - － 情報共有制度の積極活用が必要
- 今後の対応
 - － 公私協働型の政策手法の導入
 - － 法よりも、ガイドラインや第三者認証等のソフトロー、企業組織規律、実効性を持たせる

図37

情報共有の為の制度検討

- 公私協働型の政策手法の利点
 - － 変化と進化を続ける情報の利活用に、政府規制で詳細記述は不可能、望ましくない
 - － 主は、イノベーションの詳細知識を有する産業界の自主規制(柔軟性、当事者知識反映)
 - － 自主規制に完全委任はリスクと限界: プライバシー等
 - － 共同規制(corregulation)、自主規制の利点を生かし、リスクや限界を政府が法制度で補完
- 情報共有に関わる法制度と再検討
 - － プライバシー、知的財産、セキュリティ政策、情報公開法制、不法行為責任、刑事法(犯罪捜査時のデータ保持・開示措置)
 - － 共同規制利用促進に必要な法改正
 - － 国際的制度比較と理解

図38

諸外国の状況と日本

- EUと米国
 - － ビッグデータ利活用を先導する米国や、プライバシー保護重視のEUで、共同規制手法を重視したルール形成進行中
- 我が国
 - － プライバシー保護の第三者機関(特定個人情報保護委員会)の設立を含めた行政組織の変革
 - － 法実装の検討中: プライバシーインパクト評価の在り方と利用、個人特定可能性からプライバシーへ
 - － これらに加え、自主規制の強化に基づくイノベーションを促進する政策手法を

図39

d. 情報自体の保護

- 国
 - 秘密保全法案計画中、特定秘密と厳罰化
- 民間
 - 企業秘密保護: ノウハウとイノベーションは、最重要資源だが、国際的サイバー攻撃、モバイルが脅威に
 - 現状: 不正競争防止法、厳密秘密管理と立証必要
 - 情報そのものの営業秘密保護目的の現実的法案と国際対応が必要
 - まずはガイドライン、企業組織規律、から始め、企業情報の保護監査及び公示制度の可能性検討
 - サイバーセキュリティ産業活性化施策: クラウド、モバイル、ビッグデータに向けて

図40

e. 企業育成と研究開発

- 企業
 - 情報セキュリティ産業は小規模(日本76億/世界1900億ドル)、セキュリティ向上に振興・活性化の支援整備
 - 一般企業は情報セキュリティ意識希薄、企業内セキュリティ担当者設置推奨、基盤のセキュリティレベル規制
- 技術と制度の研究開発
 - 国家安全保障(交渉力)、独自技術、技術の囲い込み、長期的視点、チップのブラックボックス化対応(forensics)
 - 若者に夢を提供
- 国際問題
 - 国際協力、官民連携情報共有政策の国際連携
 - 国際企業へ国内法の適用可能性検討

図41

f. 政策の全体構造

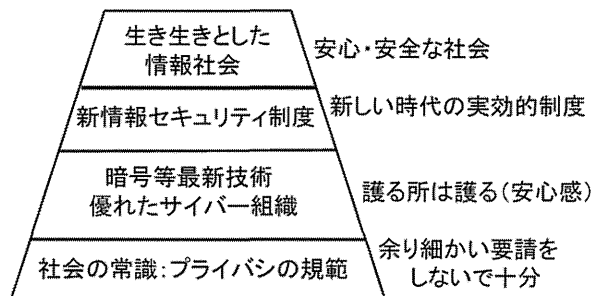


図42

5. 関係人材の育成

- 国内の情報セキュリティ人材不足
 - 産学官、すべて育成を行うことが必要
- 官側人材不足への対応
 - 様々な人材
 - 人材養成プログラム: 量と質
 - 教育内容と組織: 産・学・官連携
 - 人材育成の実効化: 産・学・官連携

図43

様々な必要人材

専門知識による分類

- セキュリティ計画・対応責任者
- 監視、情報収集、分析専門家
- インシデント対応マネージャ
- インテリジェンス専門家
- 現場対応者: Forensics
- 情報法制専門家
- 技術研究・開発者
- 国際連携対応者: 情報、協力
- 教育用人材: 専門家育成、リテラシー教育

組織内役割による分類

- 国内治安
- 国際対応
- 国防
- 公的機関
- 重要インフラ
- 企業
- 教育組織
- セキュリティ企業
- NPO

図44

我が国に求められるセキュリティ人材育成

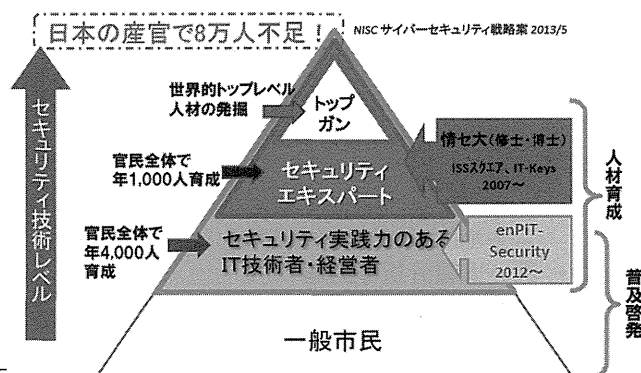


図45

人材育成プログラム

- 育成人材レベルと種別に応じた中長期戦略と実行計画の策定
 - － 教育組織(継続教育含む)・資格・訓練場
 - － 地方組織間の切磋琢磨形態醸成
 - － 若い専門人材の獲得
- 量的拡大
 - － 中央＋地方、遍く教育
- 質の向上
 - － 人材獲得経路の拡大、OJT、CTFの参加・開催
 - － 大学院：外部世界との交流、広い基礎＋専門知識、研究経験

図46

教育内容と組織

- 教育組織の利用
 - － 一般リテラシ、警察庁全体を対象
 - － 情報分野人材：情報セキュリティ基礎講座
 - － サイバー専門家：大学院、専門企業、変化に合わせた専門教育・継続教育、プロアクティブな対応人材の提供、研究
 - － 現場経験：インターン、Challenge Based Learning
- 教育内容
 - － 専門人材：技術(ネットワーク、システム、暗号)、フォレンジック、情報法制、管理法
 - － 実習：侵入・攻撃、分析・対応、経験の重要性

図47

人材育成の実効化

- 進めるためのインセンティブ
 - － 若い人材発掘に公的補助
例：バウチャー制度と活用：卒業後3年働く(インターン)
 - － 警察内専門人材キャリアパスの形成
- 連携
 - － 産・官・学 情報共有・解析の場(NCFTA)構築
 - － 各地にボランティア組織形成：ITふくろう博士
- 深い情報分析専門家
 - － 若い人材に適性、また惹きつける魅力
 - － CTFなどによる分野活性化と人材発掘
 - － 地方の各部隊間の競争大会

図48

【基調講演③】「産」から見た産学官連携について～情報セキュリティソリューションベンダーの期待と役割～

日本電気株式会社執行役員 近藤 邦夫

1. はじめに【図1、2】

今日御参加いただいている方々を拝見いたしますと、同業の方や専門の方が大勢いらっしゃると思うところ、このような大それたタイトルでお話しするのはおこがましい気がしますが、少しでも皆様のお役に立てればと思い、お話をさせていただきます。

2. サイバー攻撃の現状【図3～8】

(1) サイバー攻撃の脅威～企業の視点から～

サイバー攻撃の現状は、ほとんどの皆様が御存じかと思いますが、産業の立場で考えると、実は幾つかの側面があります。

攻撃を受けることで、一つは、企業情報が盗まれてしまうという問題があります。また、二つは、最近あるような、スキャナを乗っ取るような攻撃をされると、業務やサービスが停止することもあります。これらは企業にとって非常に大きな被害を与え、お客様の信用を失うことにもつながります。

そして、三つは、企業がお客様からお預かりしている情報が世の中に流れてしまうという問題です。このポイントは一今までの二つはどちらかというと企業は被害者の立場でしたが一被害者イコール加害者になってしまうという、非常に大きな問題となるという点です。

そうした中で、お客様の情報をお預かりしているようなタイプの企業は、サイバーに関わる意識が強いですし、情報公開に対する迅速さや、サイバーを防げないものとしてどういう対応をするかというアクティビティを非常に強く行っています。

ただ、それが機密情報という話になってくると、盗まれたことを知らせない方が良いのではないかと、あるいは一気付かないということもあるとは思いますが一これを公表することの方が、企業のレピュテーションを失わせ、企業にとって競争戦略上不利になるのではないかと考えてしまう傾向があります。そうすると、こういった情報は出てこない可能性があるというのが、もしかしたら企業が持っている一つの特性ではないかとも思います。

ただ、企業のアクティビティとしてもう一つ申し上げるとすれば、それは、産学官連携の中で企業として技術を提供しながら、一緒になってサイバーに強い社会を創っていかうというのではないのでしょうか。

(2) サイバー攻撃の変化と特徴

NECは、企業の力をもってお客様にシステム等を提供する中で、いかにこういうものを強靱にしていくか、いかにお客様の価値が失われないようにしていくかという立場にあります。

最近発生したサイバーの攻撃は皆さん御存じだと思いますが、対象については、政府機関、自治体、企業、大学・研究機関、あらゆる活動をしているところが狙われています。また、情報の価値が高いのか、それともなかなか対策が取れていないのかはわかりませんが、同じところが何度も狙われるということもあります。

こうした傾向の中で、サイバー攻撃がどのように変化しているか。従来の攻撃は、一部の有名な官公庁に集中していて、攻撃者もどちらかというと愉快犯といったところがあったと思いますが、近年はあらゆる機関に対象が広がっており、攻撃者もプロになっています。攻撃側が非常に大きなコミュニティを持っているので、

情報交換のスピードが速く、あっという間に手口が改良されていくわけです。

こういう中で我々是对応していかなければなりません。技術が高度になり、攻撃の変化も早く、被害が非常に甚大になってきています。こうした特徴に対し、我々は、一つの組織の限界を知らなければいけない。一つの組織で知ることができる情報は非常に限られています。これを早く、多くの人が共有することが必要だと思います。

(3) 我々が取り組むべきテーマ～「情報・知見の共有」「人材育成」「技術開発」～

対策に必要な情報が不足するというのは、これは民間の非常に辛いところですが、自分たちのお客様に被害があったときは、そこに入って我々は御相談を受けてやっていきます。ただ、そのお客様の持っているデータの先を見ていこうとすれば、法律の壁があって見えなくなってしまう。お客様に対してどこまで我々が貢献することが出来ているのかは、非常に頭の痛い問題です。

また、少ない情報、浅い情報から、対策技術の開発も遅れてきます。そして、圧倒的にこうしたことができる人材が不足しているという問題もあります。

こういった観点から、私どもが取り組むべきテーマは「情報・知見の共有」「人材育成」「技術開発」の三点ではないかと思います。産学官が力を合わせれば、有効に対応できるのではないのでしょうか。

また、言うまでもなくサイバーは国境がなく世界に広がります。日本人は安心・安全を考える上で、周りに海があり閉じられた空間だという見方をどうしてもしてしまいますし、サイバーにおいてもそうだと思います。先入観がなかなか消えていません。

しかし、これら三点は、いずれもグローバルに考えていかなければならない領域です。世界と情報交換をしていく上でも、グローバルトップを狙っていかないと、必要な情報が入ってきません。我々が狙っていくのは、グローバルの中で存在感のある「技術開発」であり、「人材」であり、「情報・知見」であると思います。

3. 現在の取組状況【図9～14】

NECが連携している取組について、公的な取組を含めて御紹介すると、例えばJ-CSIP¹があります。この目的は、参加組織で検知されたサイバー攻撃の情報をIPA（独立行政法人情報処理推進機構）に集約して共有するというものです。

主な参加機関ですが、多くの省庁の機関が参加しており、民間も5つの業界で構成されています。また、間接的ですが、学術機関もこの中に入っていて、御助言をいただいていると理解しています。

昨年（2012年）の活動実績を申し上げますと、寄せられた情報が246件、共有された件数が160件でした。これは、多いと思うか少ないと思うか。ほとんどの皆さんは少ないと思われるでしょうが、これは、冒頭にお話したような企業のレピュテーションの問題が原因の一つではないかと想像しています。

一方、海外での取組に目を向けますと、こうした産学官の連携による取組がアメリカは非常に進んでおり、日本は10年ぐらい遅れています。例えば、米国のジョージタウン大学では、“International Engagement on Cyber 2013”²というフォーラムが実施されています。ここでは、それぞれの産学官の役割が非常に明確に現れています。連携における主な役割として、産業界は「現場の視点」や「技術開発」、学術界は「法律」や「科学技術」、そして政府は「政策・法整備」といった論点で、コーディネートする仕組みづくりを含めて行っていると理解しています。

とはいえ、我が国でも、JNSA³が主催している「セキュリティ・コンテスト」などが―“DEF CON”⁴に遅れて何年にもなりますが一日本でもできるようになってきました。ようやく、有用な人材をこの中から発掘できる

ようになってきたかと思います。

4. 産学官連携の在り方【図15～20】

(1) 産学官の連携プロセス

産学官の連携の在り方は、「日本版NCFTA」を念頭に話をさせていただくことにします。まずは、「官」が主導して産・学・官の「連携の場」を新たに整備する必要があると思います。官でないとできないことがあるのです。先ほど、民間が非常に辛いという話をした（2. (3)参照）のは、情報にどこまでアクセスできるのかという点に限界があるからでしたが、実データをどうやって我々が得ていくか、それを技術開発に生かしていくかを考えたとき、どうしても機密情報や、被害者が受けている情報に関する捜査情報などが技術開発のために必要になってくるという局面があります。こういうものを取り扱う性質上、官側に主導していただくのが必要ではないかと思います。

そういう中で情報を集約し、分析・知見化をして、それを実際に使えるような形でフィードバックしていくところが全体のプロセス、流れになってくるというのは異論のないところだと思います。

(2) 情報集約について

情報の集約に関しては、基本的なアクティビティの基点は、攻撃を受けている被害者を含めて産業界が中心になると思います。現場で起きているサイバー攻撃に係るリアルタイムの情報、実際の情報を情報集約の場に提供することが、産業界の一つの役目になってくるでしょう。

ただ、そうした情報を色々なステークホルダーがいる連携の場に、我々産業界は出すことができるか。そこが大きなポイントではないかと思っています。

一つの解決策としては、クライテリア（規範）を定め、それに従い強制的に出すというのがあるとは思いますが。ただ、強制的に出すということに関しても、やはり何らかのルールがないと企業は動きにくいわけですから、情報を出して問題のない場にしていける、信頼を構築していくことが、企業が情報を出していくための重要な施策になってくると思います。

また、こうしたアクティビティをやっていくことにより、国外からも情報が得られるということもあります。米国のNCFTAでは、色々な国と連携をされています。その輪に我々が入る際、その先頭に立つ部分は、官の色々な取決めになってくると思っています。

そして、学の役割は、こういった活動をする上での法的なバックグラウンドや科学的な知見などを持ち寄ってやることでしょう。

(3) 情報分析・知見化について

集約された情報を分析・知見化するところですが、集約された情報の中で機密データ等にはマスキングが必要となります。また、知見化していくのに必要な情報形式を規格化していくことも必要です。こうした作業を実現させるのにも相当な技術開発が必要となります。役に立つ情報を残して、役に立たない情報を消す。それによって企業におけるトレードシークレットを守る。この部分の情報開発も今後の大きな課題でしょう。ただ、こうしたことを仕組みの中に盛り込んでいくことが重要であり、それを産学官でやっていくということだと思います。

こういう形で企業の機密を担保できれば、民間も情報を出しやすくなってくると思いますが、その上での技術開発という観点で、分析の知見化や必要な技術・専門的な人材をこの仕組みに入れていくのは、産業界の一つの大きな役割だと思います。

なお、技術開発が産学官連携におけるコミュニティの中で出来るとすれば、IPR[®]の取扱いもルールとして考えていただくことが、健全な開発をし、技術の出し惜しみをしないことにつながってきますから、こういった論点も考えていただければと思います。

また、この中で「学」の分野は、分析・知見化に関わる技術をお互いに高めていくということで、この協力の輪を速く回す、強い信頼関係を作ることが非常に重要となるでしょう。

(4) フィードバックについて

このように、集約、分析・知見化した情報を、それぞれがフィードバックしていきます。

「官」としては、国家安全保障や犯罪の撲滅・追跡に使われると思いますし、また、犯罪の予防という観点で色々な注意喚起についても、この中の情報を使ってやっていただきたい。

我々の安心・安全を警察の方々に守っていただいている中で、時々「この地区ではこんな犯罪が多い。」といったニュースが流れます。例えば、随分昔の話ですが、「ピッキングがこの地区ではこれだけ発生しているから気をつけてください。」といった情報などがありました。脅威の全体像を把握した上で、犯罪を未然に防いでいくことは、この活動の中でも重要なポイントだと思います。

「産」では、技術開発や人材育成に情報を生かしていき、事業に活用していきます。

また、研究対象としてリアルなデータが入ってくる「学」の分野においても、非常に大きなデータになります。人材育成の観点からも、そうしたデータが使える、知見が使えるというのは非常に重要なことだと思います。

まとめると、産学官連携の仕組みづくりをしていく中で、「産」としては、知見やノウハウを持ち帰り、人材育成にも活用していきたい。技術開発の種を持ち帰って技術開発に活用していく。ただ、これを持ち帰っているだけでは、新しい技術が生まれない可能性もあります。持ち帰って出てきたものは連携の場にお返しするのが、進化を早める一つのやり方だと思っています。そのための保護が先ほどお願いをした部分です。

「官」への期待は非常に大きく、これを回すためには官側の役割は非常に大きいと思います。

「学」に対する期待では、高度な専門人材の提供が一番大きな役割であると思います。

ただ、これはお願いでもあります。人材育成に関しては、人材が働ける場所を作るための施策も必要だと思っています。学生は、世の中でどういうところに就職できるかということに非常に敏感で、就職希望ランキングで企業は一喜一憂します。サイバーの優秀な人材が入ってくる環境を作るということは、社会に出て活躍できる場が整備されているということでなければなりません。この部分に関しても、産学官が協力して、そうした土壌を創っていくべきだと思っています。

但し、そういう中で一つの障害になるのがコストの面です。サイバーに対するセキュリティ技術を入れていくというのは、どうしてもコストを上積みしなければならないわけです。

例えば、官公庁の色々なシステムにおいても、入札ということで非常に厳しいコスト競争を我々は日々やっていますが、サイバーを載せるときにどれだけ強固なものにしていくか、というのがきちんと決まっていないと、コストが乗せにくいのです。

一応、ガイドラインもありますが、そこを「企業は絶対にその技術を入れなければいけない。」というように、もう少し堅い形にしていくと、それを受け取る側のお客様にしても、それを扱える人たちが必要となります。そうなってくると、サイバー人材の活躍する場が保障されてくるので、こうしたことも、是非、人材育成とともに考えていただきたいと思います。

5. NECの取組【図21～27】

(1) 基本方針

NECの取組を少し宣伝させていただきますと、私どもNECは今年度から、社会ソリューション事業に注力しようということで、事業をこちらの方向にフォーカスしています。社会ソリューション事業とは何かということですが、端的に言えば、ICTを埋め込んだ社会インフラは、すべてある種の社会ソリューション事業と捉えています。

今はすべてのものにICTが入っていると言っても過言ではありません。こうしたものがサイバー攻撃を受けると、社会的な被害は非常に大きくなります。我々の生活に不可欠な社会インフラが攻撃されると、社会が麻痺します。我々は、そうした事態にもなり得る分野において、製品をお納めしてはならないわけです。よって、そうした事態に対してきちんとした対応をしていかなければならないということが、私どものサイバーセキュリティに対する取組の根幹の一つになっています。

それに対応して、幾つかのアクティビティを行っています。まず、対策・ノウハウの知見化や技術開発の活動例として、サイバーセキュリティ・ファクトリーを御紹介させていただきます。次に、サイバー対策に対するリテラシーの向上については、「CYDER」という、実践的な防御演習に参画させていただいており—実は演習そのものは昨日から始まったものですが—この点について御紹介させていただきたいと思います。そして、国際化が進むサイバー攻撃・犯罪への対応という点では、インターポールと提携を進めておりますので、この点について簡単に御紹介させていただきます。

(2) サイバーセキュリティ・ファクトリー

まず、サイバーセキュリティ・ファクトリーについてですが、これは、サイバー攻撃対策のソリューションやサービスの開発拠点を構築し、国内のセキュリティ専門会社と連携してサイバーテストレンジとして活動する中で、技術やノウハウを蓄積・共有化していこうというものです。NEC一社ではできないようなことを、皆で力を合わせてやっていきたいという考え方に立脚しています。

取組としては、官公庁・企業に入ってくるサイバー攻撃に関わる対策の導入・運用を支援していきます。また、ノウハウを蓄積していき、進化していくソリューションとサービスをやっていきます。

また、サイバーファクトリーで蓄積して共有化したナレッジ・運用ノウハウ・監視モデルを、技術開発・人材育成にフィードバックしていきますが、これは、私どもを含めて五つの会社で運営しており、この中にサイバーテストレンジを置いて、我々が提供できるソリューションの中で、様々なプロダクト、様々な技術がどう親和性を持ってうまく使えるのか、どう実効性を発揮できるのか、こういったところを検証できるツールとしてやっていこうというものです。

(3) CYDER (Cyber Defense Exercise with Recurrence)

次にCYDERですが、これは、総務省の「サイバー攻撃解析・防御モデル実践演習」の実証実験プロジェクトとして、官民参加型のサイバー攻撃に対する実践的な防御演習を実施するというものです。

「民」の側では、NTTコミュニケーションズがこの仕事を統括しており、防御モデルの部分を担当されています。また、日立製作所が解析の部分を担当され、私どもは演習の部分の構築・実施をさせていただいているものです。

演習については、受講者が2名から4名のチームでシナリオに沿って演習をしていきます。演習1回が2日間で、正しく産官学連携という形で取組がなされています。今後、こうしたものも、日本版NCFTAと連携して使われてくることになると思っています。

(4) インターポールとの提携

インターポールとの提携についてですが、昨年12月にストラテジック・パートナーとして提携し、サイバー犯罪についてのセキュリティ対策を一緒に強化していくことになりました。来年10月にシンガポールにIGCI¹と呼ばれる組織が構築されますが、この中にデジタルセキュリティの一つとしてサイバーがテーマとして入っています。

IGCIには、様々な脅威を分析して加盟国に情報を発信したり、犯罪捜査の支援をしたりする“Cyber Fusion Centre”や、加盟国の依頼に基づきマルウェア等を解析したり、ノウハウを蓄積して新たな捜査手法を開発する“Digital Forensic Lab”、そして、このラボで開発された捜査手法をトレーニングする施設などが予定されています。

こうした機能を持つことで、インターポールに加盟している各国において、セキュリティホールができないようにしていくことが一つの目的ではないかと理解しています。

こうした提携の趣旨は、私どもNECだけではなく、NECを含む企業体がインターポールを支援し、一緒になってサイバー犯罪に対して取り組んでいこうというものです。今後こうした形は、ますます加速していくと思います。日本においても、グローバルに通用する取組に対して産業界も参加していきたいと思うので、是非御指導いただきたいと思います。

¹ Initiative for Cyber Security Information sharing Partnership of Japanの略。サイバー共有イニシアティブのこと。J-CSIPの概要については、独立行政法人情報処理推進機構（IPA）のホームページで公表されている。（<http://www.ipa.go.jp/J-CSIP/index.html>）

² 同フォーラムの概要については、ジョージタウン大学のホームページで公表されている。（<http://lsgs.georgetown.edu/events/InternationalEngagementonCyber2013/Page>）

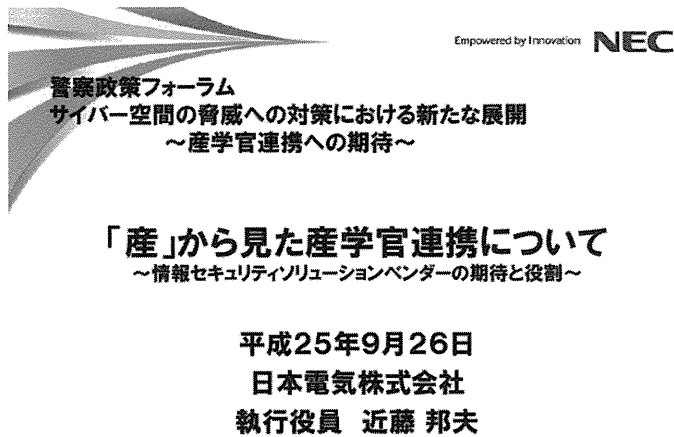
³ Japan Network Security Associationの略。特定非営利活動法人日本ネットワークセキュリティ協会のこと。

⁴ 米国で毎年開催されている大規模なセキュリティイベントのこと。

⁵ Intellectual Property Rights の略。知的財産権のこと。

⁶ The INTERPOL Global Complex for Innovation の略。

【講演資料】



Empowered by Innovation **NEC**

警察政策フォーラム
サイバー空間の脅威への対策における新たな展開
～産学官連携への期待～

「産」から見た産学官連携について
～情報セキュリティソリューションベンダーの期待と役割～

平成25年9月26日
日本電気株式会社
執行役員 近藤 邦夫

図 1

目次

1. サイバー攻撃の現状
2. 現在の取り組み状況
3. 産・学・官連携の在り方
4. NECの取り組み

図 2 Page 1 © NEC Corporation 2013 Empowered by Innovation **NEC**

1. サイバー攻撃の現状

- ・「サイバー」とは、ICTによって形成される情報空間と、そこで供される業務やサービスシステムの空間
- ・「サイバー攻撃」とは、上記の空間において、データの窃取、改ざん、破壊や、システムを機能不全に陥らせたりすること

図 3 Page 2 © NEC Corporation 2013 Empowered by Innovation **NEC**

1.1 サイバー攻撃の脅威 ～企業の視点～

- サイバー攻撃は「情報」「信用」を奪い、「業務」を停止させる

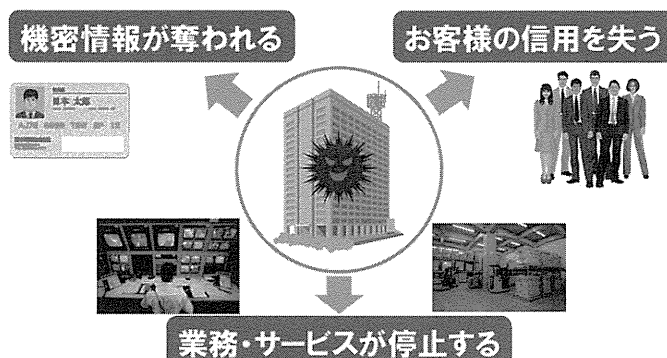


図 4 Page 3 © NEC Corporation 2013 Empowered by INFORMATION NEC

1.2 最近発生した主要なサイバー攻撃

- 攻撃の対象は政府、自治体、企業、大学・研究機関など全てがターゲット
- 特定の組織が複数回攻撃を受けるケースもある

公表時期	攻撃された企業・組織	概要
2012年9月	政府等(日本)	日本の公的機関や企業のウェブサイトがサイバー攻撃を受け、計19のサイトで閲覧障害や改ざんが確認された。
2012年10月	大学(各国)	ハッカー集団が、日本の5大学を含む世界の100大学のサーバから盗んだ情報12万件をインターネットに掲載したと公表した。
2012年12月	企業(日本)	マスコミの社内システムが不正アクセスを受け、同社が試験的に作成したデータが一時的に閲覧できる状態にあった。
2013年1月	地方自治体(日本)	地方自治体でウェブサイトの更新に必要なIDとパスワードが何らかの方法で盗まれ、海外のサーバから不正アクセスを受けた。
2013年3月	政府(日本)	中央省庁が運営するウェブサイトが改ざんされた。閲覧者のパソコン内の情報が盗まれた可能性があると発表した。
2013年4月	国際機関	サーバが攻撃を受け、情報が漏えいした可能性あり。同機関は2012年11月にも攻撃を受けている。
2013年5月	企業(日本)	ID管理サーバが攻撃を受け、最大2200万件のユーザIDが流出した可能性あり。同社は4月にも攻撃を受けている。
2013年7月	企業(日本)	約1,500万回の不正アクセスがあり、約2万回の不正ログイン。

図 5 Page 4 © NEC Corporation 2013 出典：平成25年版情報通信白書(NECで一部追記) Empowered by INFORMATION NEC

1.3 サイバー攻撃の変化と特徴

- 攻撃側において、攻撃ツールや最新情報が流通するコミュニティが存在
- 複数/多数が協力して、速いスピードで技術や手法が高度化

	従来の攻撃	近年の攻撃
攻撃対象	有名企業・一部の官公庁など	全ての企業、官公庁、公共・教育・研究機関など
攻撃者	個人(主にアマチュア)	組織・国家(プロ化) 国際的なネットワークを保有
攻撃手法の変化	変化は緩やか	組織犯のため変化が速い
目的	技術的興味、自己顕示	利益・金銭目的、諜報など
被害・損失	サービス低下、イメージ悪化	損害賠償、社会的信頼失墜、組織活動にダメージ

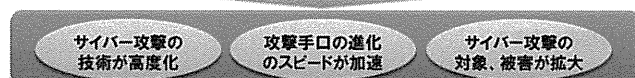
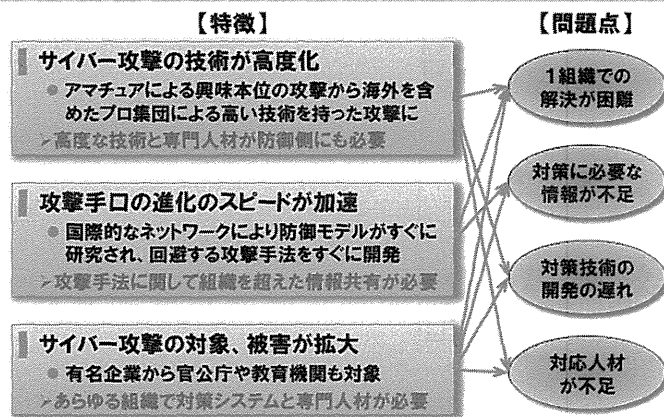


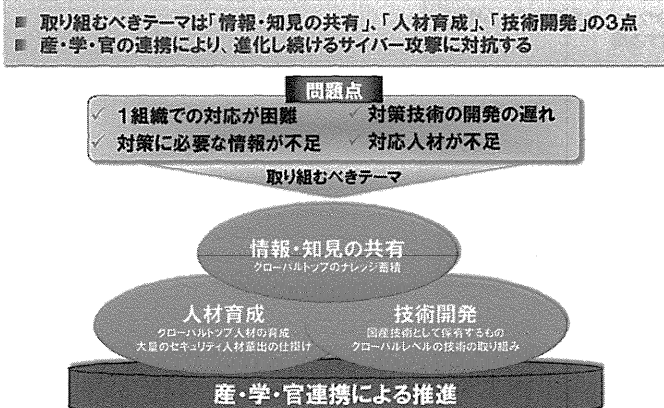
図 6 Page 5 © NEC Corporation 2013 Empowered by INFORMATION NEC

1.4 サイバー攻撃の特徴



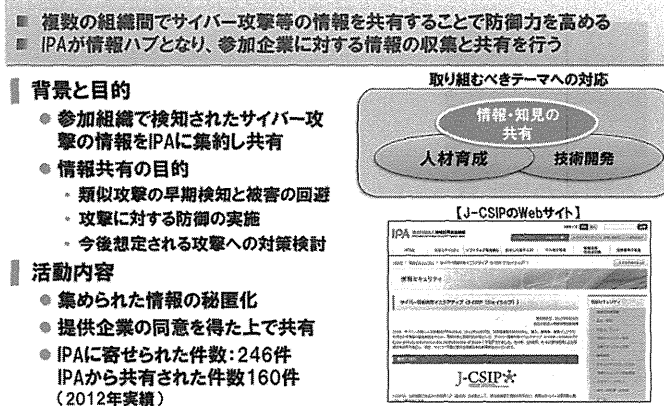
Page 6 © NEC Corporation 2013 Empowered by Innovation NEC

1.5 取り組むべきテーマ



Page 7 © NEC Corporation 2013 Empowered by Innovation NEC

2.1 サイバー情報共有イニシアティブ(J-CSIP)①



Page 9 © NEC Corporation 2013 Empowered by Innovation NEC

2.1 サイバー情報共有イニシアティブ(J-CSIP) ②

産

官

- 公的機関であるIPAがハブとなって複数業界の参加企業の情報のとりまとめを行っている(2011年10年発足)
- 5業界39組織が参加し(13年4月時点)、攻撃情報の報告・共有に協力している

主な参加機関

- IPA
- 経済産業省
- NISC(内閣官房情報セキュリティセンター)
- JPCERT/CC
- 5業界(重要インフラ機器製造業界、電力業界、ガス業界、化学業界、石油業界)

連携における主な役割

- 「産」…攻撃情報の報告
- 「官」…攻撃情報の収集・加工・共有

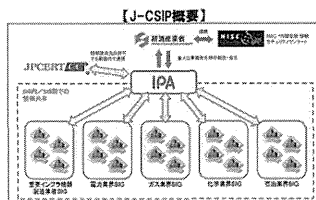

<http://www.ipa.go.jp/security/J-CSIP/>

図 10

Page 10 © NEC Corporation 2013

Empowered by INNOVATION NEC

2.2 International Engagement on Cyber 2013 (米 ジョージタウン大) ①

産

学

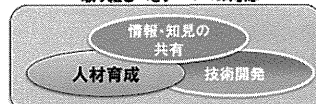
官

- サイバー領域における国際連携を目指すジョージタウン大学主催のフォーラム
- 法律と科学とグローバルセキュリティの観点で議論する場

背景と目的

- 各国政府、大学、産業の対話を促し、連携を図る
- 安心して利用できるサイバー環境の実現に向けて、国際基準と技術開発の方向性の策定を目指す

取り組むべきテーマへの対応



【International Engagement on Cyber ConferenceのWebサイト】



議論の内容

- 危機時のコミュニケーション
- サイバースペースにおける国際法の適用可能性

2011年3月から年1回開催

<http://isgs.georgetown.edu/events/InternationalEngagementonCyber2013/>

図 11

Page 11 © NEC Corporation 2013

Empowered by INNOVATION NEC

2.2 International Engagement on Cyber 2013 (米 ジョージタウン大) ②

産

学

官

参加機関

- ジョージタウン大学(主催)
 - ・ The Institute for Law, Science and Global Security
- ホワイトハウス、各国政府機関
 - ・ ロシア、エストニア、ハンガリー、カナダ、ドイツ、イスラエル、英国、NATOなど
- インターポール
- 企業、セキュリティベンダー



Dr. Catherine Lotrionte, Director,
Institute for Law, Science and
Global Security, Georgetown ※

連携における主な役割

- 「産」…現場の視点、技術開発の視点で参加
- 「学」…法学と科学を両輪とするセキュリティ議論の場を設定するとともに、学術的な貢献
- 「官」…政策・法整備の観点で議論



NEC講演

<http://isgs.georgetown.edu/events/InternationalEngagementonCyber2013/>

図 12

Page 12 © NEC Corporation 2013

Empowered by INNOVATION NEC

2.3 セキュリティ技術コンテスト:SECCON 2013 ①

- 学生から社会人まで参加できる日本最大の「ハッカー大会」
- セキュリティ技術者の育成とスキルの高度化を目指す

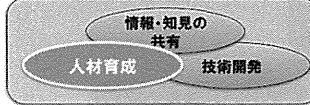
背景と目的

- 攻撃や防御の能力を競うコンテスト
- セキュリティ技術者の育成とスキルの高度化が目的
- 2012年の学生向け「SECCON」に、経産省の社会人向け「CTFチャレンジジャパン」が融合（現在は年齢制限なし）

施策の内容

- 参加者は攻撃と防御に関する幅広いスキルが必要
- 全国9か所の地方大会を経て、2014年3月に全国大会予定
- 400名以上が参加見込み

取り組むべきテーマへの対応



【SECCONの開催案内】



13

Page 13 © NEC Corporation 2013

Empowered by INNOVATION NEC

2.3 セキュリティ技術コンテスト:SECCON 2013 ②

- 多数の政府機関等が後援として活動をバックアップしている
- 複数の企業や団体が協賛という形で運用費用を支援している

主な参加機関

- 【主催】日本ネットワークセキュリティ協会(NPO)
- 【後援】情報セキュリティ政策会議、総務省、文科省、経産省、警察庁、NICT、IPA、JIPDEC、経団連
- 【協賛】NRIセキュアテクノロジーズ、ラック、NEC、など

連携における主な役割

- 「産」…運営費用の協賛、参加者の輩出
- 「学」…会場の提供、参加者の輩出
- 「官」…NPOを通じた場の提供

【協賛企業一覧】



【後援政府機関一覧】



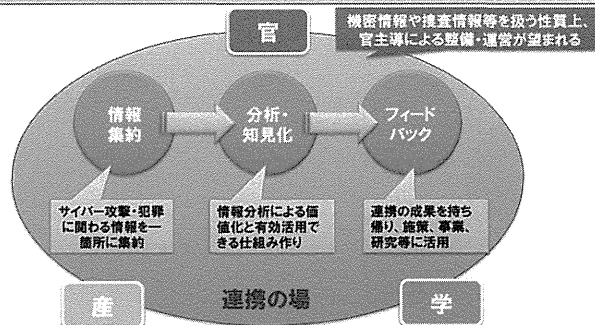
14

Page 14 © NEC Corporation 2013

Empowered by INNOVATION NEC

3.1 産・学・官の連携プロセス

- 官が主導して産・学・官の「連携の場」を新たに整備
- 「連携の場」では「情報集約」、「分析・知見化」、「フィードバック」の3つのプロセスで連携を推進



15

Page 15 © NEC Corporation 2013

Empowered by INNOVATION NEC

3.2 産・学・官の連携の進め方① ～情報集約～

- 産・学・官が互いの強味を集結し、サイバー攻撃・犯罪に関連する情報を集約
- ただし、ただ単に情報を共有しただけでは活用できるレベルにはならない

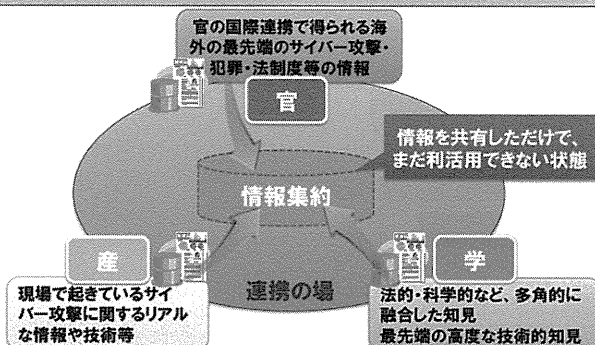


図 16 Page 17 © NEC Corporation 2013 Empowered by Innovation NEC

3.2 産・学・官の連携の進め方② ～分析・知見化～

- 『官』: 収集した情報を安心・安全に共有するための仕組み作り(標準規格化)
- 産と学は、情報を分析・知見化するための製品・技術と専門人材を提供
- 分析・知見化によりサイバーセキュリティ対策としての活用が可能に

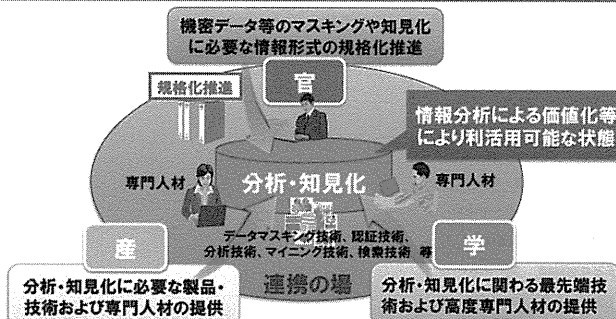


図 17 Page 18 © NEC Corporation 2013 Empowered by Innovation NEC

3.2 産・学・官の連携の進め方③ ～フィードバック～

- 官は「情報・知見」を活用し、サイバー対策、法制度・施策等の整備を推進
- 産と学は連携活動の成果を持ち帰り、技術開発、研究開発と人材育成に活用

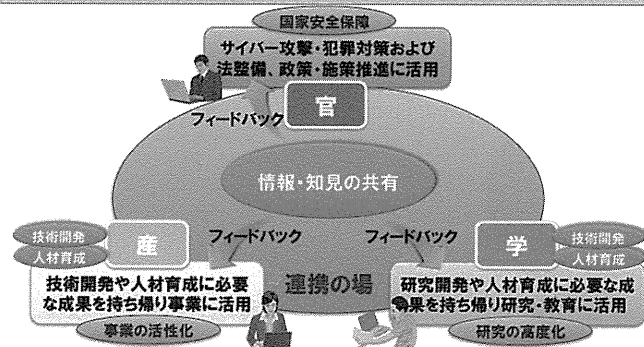


図 18 Page 19 © NEC Corporation 2013 Empowered by Innovation NEC

3.3 産から見た産・学・官連携の推進モデル

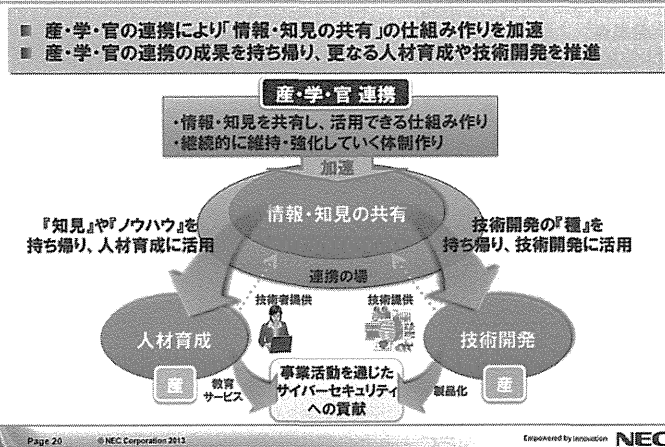


図 19

3.4 産・学・官連携への期待

官への期待

- 連携における各種障壁をクリアする「連携の場」づくりの主導
- 国際連携の推進によるグローバルな機微情報・知見の収集
- 情報形式の規格化や関連法整備など、政策・施策との連動

学への期待

- 法的・科学的知見等が多角的に融合した先端的な知見の創出
- 分析・知見化に必要な先端技術の提供
- 高度な専門人材の提供

産の役割

- 現場で起きているサイバー攻撃に関するリアルな情報の提供
- 情報分析・知見化に必要な技術・製品、専門人材の提供
- 連携の成果を活用した更なる技術開発の推進

図 20

4.1 NECの取り組みの基本方針

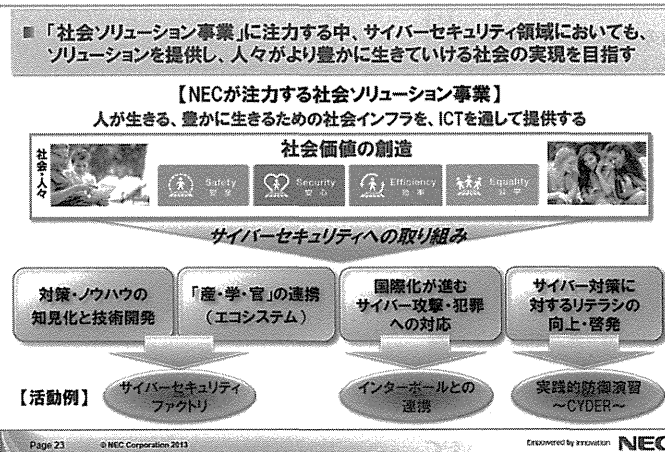


図 21

4.2 サイバーセキュリティ・ファクトリー①

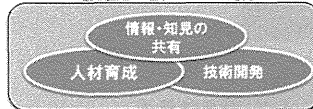
産

- サイバー攻撃対策ソリューションおよびサービスの開発拠点
- 国内セキュリティ専門会社と連携したサイバーテストレンジとして活動し、技術やノウハウを蓄積・共有化

取り組みの概要

- 官公庁や企業などにおけるサイバー攻撃対策の導入・運用を支援
- サイバー攻撃情報を収集・分析し、対応に必要な技術・ノウハウを創出・蓄積
- 日々進化する脅威に対応する、新たなソリューションとサービスを開発

取り組むべきテーマへの対応



【サイバーセキュリティ・ファクトリー イメージ図】

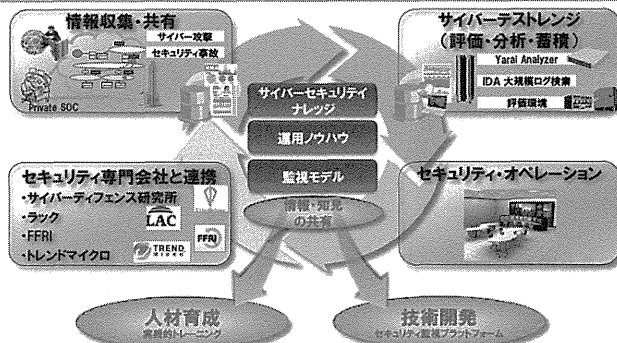


サイバーテストレンジ：ICTシステムおよび製品がサイバー攻撃を受けた際の、攻撃耐性、有用性を検証・評価し、改善等を実施するための環境および体制

4.2 サイバーセキュリティ・ファクトリー②

産

- サイバーセキュリティファクトリーで蓄積／共有化したナレッジ、運用ノウハウ、監視モデルを『技術開発』、『人材育成』にフィードバック



4.3 実践的防御演習 ～CYDER～①

産

学

官

- 官公庁や企業のLAN管理者にサイバーセキュリティの演習を提供する実証実験
- 産学官の連携によりセキュリティ人材を育成

取り組みの目的

- 総合力の高い情報システム管理者の育成（総務省受託事業）

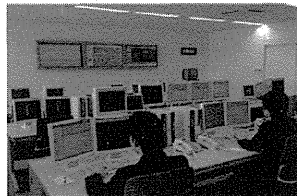
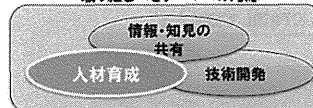
実施期間

- 2013年7月～2014年3月

実施内容

- 受講者は2～4名のチームで参加
- 大規模LANの疑似環境で標的型攻撃を体験
- 演習は2日間（1日目AM：講義、PMと2日目：実習と発表）

取り組むべきテーマへの対応



※CYDER…“Cyber Defense Exercise with Recurrence”は、「継続的に実施する実践的なサイバー防御演習」という意味です

4.3 実践的防御演習 ～CYDER～②

産 学 官

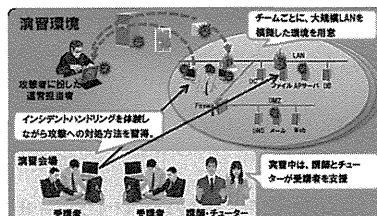
- 官民参加型のサイバー攻撃に対する実践的な防御演習を実施するもの
- 総務省の「サイバー攻撃解析・防御モデル実践演習の実証実験」プロジェクトにおいて、NTTコミュニケーションズ(統括、「防御モデル」、日立製作所(「解析」担当)、NEC(「演習」の構築・実施)をそれぞれ担当

プロジェクトに関わる主な組織

- 総務省
- NEC
- 北陸先端科学技術大学院大学
- サイバーディフェンス研究所
- 情報通信研究機構(北陸StarBED)

連携における主な役割

- 「産」…演習シナリオの作成、演習環境の構築、運営
- 「学」…演習シナリオの作成・評価
- 「官」…産学官を交えた大規模な人材育成環境の実現



25

Page 27 © NEC Corporation 2013

Empowered by Innovation NEC

4.4 インターポールとの提携①

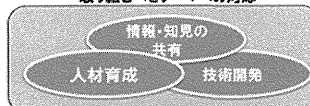
産 官

- インターポール(国際刑事警察機構)とNECがグローバルなサイバーセキュリティ対策で提携(2012年12月)
- 互いの強みを結集し、さらに複雑化、高度化するサイバー犯罪などへのセキュリティ対策を強化

概要

- 2014年10月「The INTERPOL Global Complex for Innovation (IGCI)」をシンガポールに新設
- IGCIは、サイバー犯罪に関する研究開発・トレーニング・捜査支援の活動拠点
- インターポール加盟各国へ最先端のサイバーセキュリティ対策を開発し、提供

取り組むべきテーマへの対応



IGCIの全貌(イメージ)

<http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation>

26

Page 28 © NEC Corporation 2013

Empowered by Innovation NEC

4.4 インターポールとの提携②

産 官

IGCIが実現する3つの機能

- Cyber Fusion Centre
 - ・ 膨大な脅威情報を調査・分析し、加盟国に情報を発信
 - ・ サイバー犯罪捜査の支援
- Digital Forensic Lab
 - ・ 加盟国からの依頼にもとづき、マルウェア等を解析
 - ・ 特徴等のノウハウを蓄積し、新たな捜査手法の開発を実施
- トレーニング
 - ・ ラボで開発された新たな捜査手法をトレーニングするための施設
 - ・ 各国の政府等の要員を対象に演習を実施



INTERPOL Secretary General Ronald K. Noble氏とNEC 社長



Cyber Fusion Centre (イメージ)

27

Page 29 © NEC Corporation 2013

Empowered by Innovation NEC