# 第２章

# ＜社会安全フォーラム＞

## サイバー空間の安全の確保に向けて

＜社会安全フォーラム＞
サイバー空間の安全の確保に向けて

警察政策研究センター

警察政策研究センターは、平成27年12月２日、（公財）日工組社会安全財団との共催、公益財団法人公共政策調査会、警察政策学会及び（一財）警察大学校学友会の後援により、グランドアーク半蔵門（東京都千代田区）において、社会安全フォーラム「サイバー空間の安全の確保に向けて」を開催した。

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着し、今や、サイバー空間は国民の日常生活の一部となっている。こうした中、サイバー犯罪の多発、サイバー攻撃の世界的規模での頻発など、サイバー空間における脅威は深刻化している状況にある。

警察における体制強化、日本サイバー犯罪対策センター（JC3）の設立、海外ではINTERPOL Global Complex for Innovation（IGCI）、European Cybercrime Center（EC3）の設立などサイバー空間の脅威への対応を強化しているところであるが、こういった機関の取組を参考にしながら、官民連携、国際連携の進め方やサイバー空間の脅威に対処するための法制度の在り方について論じ、安全・安心なサイバー空間の確保のために何ができるのかを討議することを目的として本フォーラムは開催されたものである。

本フォーラムでは、名和振平警察政策研究センター所長による開会挨拶の後、実務家・研究者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。

○　キンモ・ウルクニエミ氏（IGCI連携担当部門アシスタントディレクター）
　「サイバー犯罪に対抗するインターポール」
○　ベノワ・ゴダート氏（EuropolからIGCIへのリエゾン・オフィサー）
　「EC3の活動について～EU内における官民連携、国際連携を通じた取組～」
○　湯淺墾道氏（情報セキュリティ大学院大学教授）
　「サイバー空間の脅威に対処するための法制度の在り方」

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、冒頭、白井利明氏（警察庁長官官房参事官（サイバーセキュリティ担当））及び坂明氏（（一財）日本サイバー犯罪対策センター理事）による発表が行われ、その後、上記基調講演者を交え、名和所長がコーディネーターを務め、アトリビューション、ログの保存をめぐる課題、官民連携の更なる促進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、警察関係者等約280人が出席した。

## 【開会挨拶】

**警察政策研究センター所長　　名和　振平**

本日は、サイバー空間の安全確保をテーマとする社会安全フォーラムに御参加をいただき、御礼を申し上げる。

差別や排除なく誰もが容易に参加できるサイバー空間は、今や欠くことのできない経済社会の活動基盤となっている。他方、このような状況の負の側面として、サイバー犯罪やサイバーテロ、あるいはサイバーインテリジェンスによる脅威が深刻化している。国境のないサイバー空間において、これらの脅威に的確に対処していくためには国際連携が重要であることは言うまでもない。

本日のフォーラムでは、まず、国際刑事警察機構がシンガポールに開設したIGCIのキンモ・ウルクニエミ氏と欧州警察機構のベノワ・ゴダート氏から、法執行機関による国際連携の現状等について講演をしていただく。

匿名性が高く、また、国境もないサイバー空間における秩序維持には、現実空間とは異なる困難がある。また、サイバー空間における規律を検討するに際しては、情報の自由な流通を尊重することやプライバシーに配慮することも求められている。他方、あらゆるものがインターネットを介してつながるInternet of Thingsと呼ばれる状況が実現した社会では、サイバー攻撃による被害は極めて大きなものとなることが予想される。これらのことを踏まえると、サイバー空間における法制度はどのようなものであるべきだろうか。

こうした問題を考えるために、情報セキュリティ大学院大学の湯淺先生には「サイバー空間の脅威に対処するための法制度の在り方」について講演をしていただく。

講演の後には、日本サイバー犯罪対策センターの坂理事、警察庁の白井参事官にも加わっていただき、サイバー空間の安全を確保するための課題について議論をしていただく。

今日、誰もがサイバー犯罪やサイバー攻撃の脅威から無縁であると言うことはできない。本日のフォーラムが皆様のサイバー空間での安全確保に向けた実践のために有益なものとなることを期待する。

結びに、本日のフォーラムを後援していただいた公共政策調査会、警察政策学会及び警察大学校学友会の皆様に心より感謝を申し上げ、開会の御挨拶とさせていただく。

## 【基調講演①】サイバー犯罪に対抗するインターポール

ＩＧＣＩ連携担当部門アシスタントディレクター　キンモ・ウルクニエミ
編集／警察政策研究センター教授　辻　貴則

### １　インターポール

現在、私はフィンランド警察からIGCIに出向している。2013年から勤務しており、場所はシンガポールにある。本日は、インターポールが従事していること、特にサイバー犯罪との戦いについて理解を深めていただくために、組織としてのインターポールについてお話しさせていただきたい。

インターポールの思想は何も新しいものではない。モナコにおいて、インターポールの思想が最初に提唱されてから100年以上たっている。警察の幹部がモナコに集まり、警察機関が直面する問題、すなわち効果的な情報交換方法や協力モデルの構築方法について議論したのである。

インターポールのモットーは、警察機関をつなげて世界をより安全にすることである。警察機関をつなぐとは各国の警察の力を結集することであるが、最近では警察に限らず、民間部門や学術機関とも協力して犯罪対策に取り組んでいる。私達のミッションは、警察機関の国際協力を強化して、犯罪を予防し戦うことである。

インターポールでは、警察機関の国際協力を強化するため、全ての加盟国が利用できるツールやサービスを用意している。そして、警察機関間のこの強化された協力は安全な通信を確保することにより可能となっている。現在、インターポールには192か国が加盟している。実は、３週間前は190か国だったのが192か国に増えたところである。また、その他の重点分野として、警察機関やその他の関係者に訓練を提供している。

インターポールの歴史についてであるが、モナコに警察幹部が結集して最初の会議が開かれたことは先ほど申し上げた通りである。その後、1923年に各国が集まってインターポールが組織された。また、インターポールは世界に拡大を続けている。フランス・パリで始まったインターポールであるが、その後、本部、事務総局はリヨンに移され、現在は世界各国にオフィスを構えている。そして、2015年、インターポールはシンガポールに「インターポール・グローバル・コンプレックス・フォー・イノベーション（IGCI）」を設置したのである。

私は組織構成について話すのは好きではないが、今回はインターポールという組織を理解していただく上で役立つかもしれないので、お話しする。現在、インターポールの事務総長は、ユルゲン・ストックというドイツ人で昨年就任した。彼の就任後、インターポールは組織再編に取り組んでいる。インターポールは現在Interpol 2020プログラムに取り組んでいるが、これは組織としての新たな機構の導入

を目的としている。そして、組織図（省略）の中にIGCIがあるのをご覧になれると思うが、IGCIは４つある執行機関の１つであり、このことからも、サイバー組織がインターポールにおいて非常に重要な役割を果たしていることが分かると思う。

次に、各国との連携についてである。インターポールは192か国に国家中央事務局を置いている。全ての加盟国が、常時稼働しているネットワークによりつながっている。国家中央事務局だけでなく、特殊警察機関、国境検問所、空港、港もインターポールと連携している。

インターポールには地域事務局もある。本部はフランスのリヨンにあるが、南アメリカ大陸に２ヶ所ーサンサルバドルとブエノスアイレス、そしてアフリカ大陸に４ヶ所、地域事務局がある。ヨーロッパには地域事務局はないが、これは事務総局があるためである。北米にもないが、これはそこに地域事務局を置く必要性がないためである。その代わり、北米の国は事務総局の支援を受けることができる。一番新しい事務局がシンガポールに拠点を置くIGCIである。

インターポールは、ユーロポールに対して２人のリエゾン・オフィサーを派遣している。１人はサイバー犯罪、もう１人はその他の犯罪分野を担当している。また、ニューヨークにある国連とブリュッセルにある欧州連合にもリエゾン・オフィサーを送っている。

インターポールには様々な優先事項があり、この優先事項をご紹介していきたいと思う。重要分野の１つが、警察活動と法執行のための作戦支援であり、インターポールには常時支援要員が待機して、対応している。コーディネーション・センター、コミュニケーション・センターのスタッフは、インターポールの４つの公式言語である英語、フランス語、スペイン語､アラビア語でサービスを提供している。支援が必要であれば、時間に関係なくインターポールに連絡してサポートを受けることができる。

キャパシティ・ビルディング[1]は私達にとって重要である。目的は全ての国を同じレベルにすることであるが、たとえそれが無理であっても、少なくとも発展途上国と先進国の間の差を小さくすることを目指している。

インターポールの当初の原則の１つが、犯罪者に関する情報を共有し、そうした犯罪者の他国への引き渡しを強化することであったが、今もなお犯罪及び犯罪者の特定は優先事項の１つである。

続いて、法的基盤についてである。インターポールはグローバルな組織であり、非政治的組織である。インターポールはその憲章により、宗教、軍、政治に関連する犯罪への支援の提供が禁じられており、つまり、各国が協力するための政治的中立な土台を提供するのである。これは間違いなくインター

---

1　組織的な能力・基礎体力を形成・向上・構築していくこと

ポールの強みであり、これによって、インターポールは政治的に関係を持たない国同士をつなぐことができる。また、IGCI が実際に経験していることであるが、政治レベルでは交渉や議論を持つことができない国同士を実務レベルで支援することができる。これは非常に重要であり、インターポールの法務部署は、このような問題に日々取り組み、特定の分野や犯罪に対して支援を提供することができるかどうかを判断している。

既に申し上げたように、インターポールは新しい事務総長を迎え、業務に対する新たな視点も取り入れている。新事務総長は新グローバル・プログラムを導入したが、このプログラムの基礎及び根拠がどのようにしてできたかというと、インターポールが加盟国に「インターポールによる支援を期待する最も重要な分野は何か」を聞き、それに対するフィードバックを基に、テロ対策、組織的・現代型犯罪、サイバー犯罪の３領域を選んだのである。これはインターポールがより時代に対応し、応答性の高い組織になるために必要なことである。それまでのインターポールはいくつもの小さい分野を設定するものの、それら全てにリソースを配分することができなかったが、このグローバル・プログラムにより、更に集中的なアプローチをとることができるようになった。

まず、テロ対策における支援の必要性を見ていく。テロは政治的、宗教的、軍事的な動機が背景にあることが多いため、これまでインターポールでも議論されてきたが、それでも、なお、加盟国はインターポールの支援を求めている。したがって、インターポールはテロの脅威を防ぎ、それに対応するためのツール及びサービスを提供している。例えば、シリアやイラクなど危険地域に向かう外国人戦闘員の特定がある。国境検問所からインターポールのデータベースにアクセスして情報を照合することができるようにしており、テロの容疑者が特定の国や地域に向かっているという情報をインターポールがつかんだ場合、各国はその情報の提供を受けることになる。

また、海賊対策ももちろん重要分野の１つである。海賊行為に関しては、アジア地域には長い歴史があるが、現在は頻発・増加しているわけではない。ところが、アフリカ東海岸では大きな問題になっており、テロリストが海賊行為から財源を得る可能性もある。したがって、インターポールは海賊行為対策に取り組む他の国際機関に支援を提供している。

続いて、組織犯罪・現代型犯罪についてである。これに関して、各国がインターポールの支援を受ける必要性に関してはあまり説明の必要がないように思う。近年は犯罪者が簡単に移動したり、情報を交換したりできるようになり、また、犯罪者は暗号化通信を試みるようになっており、これは警察機関にとって更なる問題である。

現在ヨーロッパには、多くの人がシリアやイラクから流入してきており、利益を得ている人身売買グループや組織犯罪グループも存在する。インターポールは各国に情報を提供し、国同士をつなげ、捜査

の調整を行うことでこれを防いでいる。

また、2000年初頭よりインターポールが取り組む重要な問題の１つが、インターネット上での子供の虐待である。インターポールは、リヨンの人身売買と子供の虐待に関する副委員会に専門部署を設置しており、全ての加盟国がこの部署のデータベースを使って違法画像を検索することができ、また、インターポールは未特定画像を持つ国から情報を収集して子供達を保護している。

最後に、サイバー犯罪に関してである。国、犯罪者、市民はインターネットを利用しており、現在、世界のインターネット普及率は、私の理解が正しければ34%くらいである。裏返せば、世界でまだ多くの人がインターネットを使用していないということであり、このインターネット未利用者がインターネットを利用するようになると、彼らはインターネット上の脅威に関する情報もなく、サイバー犯罪捜査の訓練を受けた警察機関の助けもないということで問題を抱えることになる。

そこで、インターポールは、加盟国が深刻化するサイバー脅威に対応し、捜査・支援・技術的専門知識を構築するための支援をしている。それに加えて、インターポールが新たに取り組んでいることに研究、分析結果の共有がある。実用的な情報を共有したり、加盟国に訓練の機会を提供するだけでは不十分であり、出現しつつある傾向や脅威を調査する必要があるとインターポールは考えている。

インターポールには16の重点犯罪分野がある。このリストにあるものは、以前インターポールが重点的にリソースを分配していた分野である。現在、インターポールは３つのグローバル・プログラムの下でより集中的なアプローチを採用しているが、それでもこれらは重要な分野である。

まず、汚職に関してであるが、インターポールには情報を共有し、汚職に関する情報を蓄積するデータベースがある。非常に重要な分野であり、これに関しては後でもう少し詳しくお話しする。次に、金融犯罪に関してであるが、マルウェア[2]によるサイバー犯罪やクレジットカード詐欺など、金融犯罪が増えている。また、銃器もテロと密接に関係している。インターポールには、盗まれた銃器に関する情報や様々な銃器の特定方法に関する情報を蓄積する銃器データベースがある。これにより、テロ攻撃を防ぎ、捜査を支援していけたらと思っている。このほか、逃亡犯罪人の捜査もある。インターポールの赤手配書のことを聞いたことがあるかもしれないが、赤手配書とは、指名手配犯に関する情報を全加盟国間で共有するためのツールである。

続いて、インターポールのデータベースの一部を紹介する。まず、ノミナル・データベースとは個人情報のデータベースのことである。また、指名手配犯、未成年者、盗難車、指紋、DNAに関する情報もデ

---

2　コンピュータの正常な利用を妨げたり、利用者やコンピュータに害をなす不正な動作を行うソフトウェアの総称（IT用語辞典より）

ータベースには含まれる。そして、先ほど申し上げたように、子供の性的虐待画像に関するデータベースもあり、また、とても興味深いものとして、盗まれた芸術作品のデータベースもある。

インターポールは、第一にテロ集団に関する情報の共有を促進し、テロリストや潜在的脅威に関する警告を行うことで公共の安全の確保やテロ対策に取り組んでいる。テロ攻撃を未然に防ぐための早期警戒システムを持つというのがインターポールの考え方である。インターポールが受け取る情報はもちろん、加盟国から寄せられるものであり、インターポールが情報を生み出しているわけではないが、情報の分析は行う。分析の元となる情報は公開情報である場合もあるが、ほとんどが加盟国から寄せられた情報である。

次に、人身売買についてであるが、インターポールが報告するに当たって使用する標準様式がある。また、インターポールは訓練コースのほか、作戦・技術・分析の支援を行っており、現在非常に重要になっている。ヨーロッパにおいて重要となっているが、ヨーロッパに限られたことではなく、人身売買はアジアやアフリカ、そしてアメリカの一部でも問題になっている。この問題に関しては、ヨーロッパ諸国と緊密に連携しているが、ヨーロッパは人身売買、特に子供の性的虐待目的での人身売買に大きく関わっており、インターポールだけではこの問題に対応することはできない状況である。それでも、インターポールはインターネット上での大規模捜査の作戦支援を調整しており、また、近年では、自分達だけでは目的を達成できず、民間セクターの協力が必要であることを認識している。

薬物対策や組織犯罪対策は法執行機関が昔から取り組んできた分野といえる。インターポールは特に南米において、データ収集、作戦訓練を積極的に行ってきた。また、インターポールにはIRT、すなわちインシデント・レスポンス・チームがあり、作戦があれば、そのチームにインターポールのデータベースを調べさせたり、捜査を支援させることができる。

また、先ほどお話しした盗難芸術品についても、対策を行っており、インターポールは警察機関だけでなく、国立博物館や美術館とも情報共有に取り組んでいる。盗難車についても、インターポールは主に加盟国や専門家を通じた訓練や自動車メーカー、特にBMW、フォルクスワーゲン等のヨーロッパの自動車メーカーとの連携を推進している。

次に、逃亡者捜査支援についてである。インターポールは１年に１回又は２年に１回、逃亡者を特定し、引き渡す作戦を実施している。作戦名は「インフラ・レッド作戦（Operation Infra-Red）」であるが、各国と連携して情報を共有し、それぞれの国のトップ10リストに入る逃亡者を優先事項として特定し、情報をまとめ、共有することで、これまで何十か国もの加盟国において逃亡犯を逮捕してきた。つまり、インターポールは、逃亡犯に関係する情報の世界の基準点としての役割も果たしているといえ

る。

また、ヨーロッパ、アフリカにおける逃亡犯捜査支援において、インターポールは戦争犯罪捜査の訓練も提供している。特に、アフリカでは、戦争犯罪捜査の支援を行い、ヨーロッパのその他地域、旧ユーゴスラビア裁判の支援も行った。

次に、汚職に関してであるが、インターポールには盗難資産回収データベースがある。 汚職は世界の多くの地域で重大な問題になっており、インターポールは情報を共有して捜査・起訴の支援を行うことで各国に協力している。現在、70か国以上がこのネットワークに参加しており、80を超える国がこのデータベースに情報を提供しているはずである。

## 2　IGCI

ここでビデオを見ていただく。IGCI、そしてサイバー空間における私達の活動に話を移したい。

＜ビデオ上映＞

世界各国の警察は、日々、国際犯罪の新たな脅威に対応し、安全な世界を実現するために協力しなければならない。インターポールは、新たにアジアに進出することで、フランスの事務総局と世界の地域事務局を補完し、グローバル・リーチを強化した。結果として、インターポールは190の加盟国をよりよく代表する組織になった。シンガポールに拠点を置くIGCIは、国際犯罪と戦うための最新ツール、技術を備えた研究開発施設である。その最高水準の建物には指令調整センター、訓練スペース、ハイテク・デジタル研究室がある。

デジタル時代の犯罪はより攻撃的になり、また、より捕捉が難しくなってきている。一方、技術の進展により、犯罪者データへの即時アクセスなど、警察にとっての機会も大きく広がっている。イノベーションと技術はIGCIの強い味方である。イノベーション、技術の所有、研究の実戦的応用を通じて、IGCIは犯罪の脅威に直面する加盟国を支援する。

IGCIは３つの要素から構成されている。まず、IGCIは国境を越えるサイバー犯罪捜査にデジタル分野のノウハウや作戦支援を提供する。代表的施設の１つ、サイバー・フュージョン・センターはサイバー空間における脅威のリアルタイム監視と分析を行う。このセンターは、デジタル・フォレンジック[3]支援チームを派遣して現場の捜査員を支援することもできる。IGCIには、年中無休で稼働する指令調整センター（CCC）があり、これはフランスのリヨン、アルゼンチンのブエノスアイレスのCCCと連携している。CCCは緊急で警察情報が必要であったり、危機的状況に直面する加盟国の窓口である。

２つ目の構成要素は、サイバー空間の脅威に取り組むための戦略及び研究である。IGCIはインターネ

[3] 犯罪の立証のための電磁的記録の解析技術及びその手続

ット・ガバナンス・フォーラムにおいて世界の警察機関の声になっている。サイバー犯罪との闘いは、警察、研究センター、学術機関、公共部門、民間部門との密接な協力を必要としている。

３つ目の構成要素は警察官のキャパシティ・ビルディング及び訓練である。IGCI はオンライン及び実地での訓練、そして、革新的研究に基づいたサイバー訓練コースを実施している。革新的研究と技術を武器に、インターポールは国境を越えた犯罪との戦いの先頭に立ち続けることになると思われる。

ここからは私が詳細を説明したい。まず、IGCI の業務について説明し、その後、研究戦略と作戦支援に関して IGCI が行ってきたことをお話しする。最後に、IGCI の作戦部門が調整した２つの事例をご紹介する。

繰り返しになるが、まず、IGCI の歴史についてお話しする。IGCI は 2015 年に設立されたが、公式の落成式が４月だったので、まだできたばかりの組織である。作戦支援、訓練、研究はインターポールにとっても新しい分野であるが、実は、サイバー訓練はインターポールにとって新しい領域ではない。インターポールは 1983 年に最初のサイバー犯罪訓練コースを実施しており、それ以来かなりの年月がたったが、現在の規模での作戦支援は実施してこなかった。

シンガポールでは、シンガポール政府が提供する建物に拠点を置いている。シンガポール政府は、インターポール総会において IGCI をシンガポールに設置することが決まった 2010 年初頭からインターポールを支援している。

では、IGCI は、シンガポールで何をしているのだろうか。IGCI は傾向の把握、サイバー犯罪捜査班の能力向上、国際協力・サイバー作戦の支援に取り組んでいる。そして、他の分野にも共通していることであるが、サイバー分野でも警察機関をつなげている。

また、重要なこととして、私達はマルチ・ステークホルダー[4]という手法を採用している。警察機関だけではサイバー犯罪と戦えず、他組織や業界の支援が必要である。このような分野横断的なアプローチを採用する私達には３つの柱があり、それはハーモニゼーション、キャパシティ・ビルディング、そして作戦支援である。

ハーモニゼーションとは、時には加盟国間での法律のハーモニゼーションを行うこともある。また、インターポールは発展途上国におけるキャパシティ・ビルディングについてアドバイスし、支援もしており、高度な捜査法に関しても先進国を支援している。キャパシティ・ビルディングはハーモニゼーション、そして作戦支援と密接に関係している。最後の作戦支援については、年中無休で提供できるまで

4　利害関係者のこと

には至っていないが、必要があれば、担当部署が現地に出向き、惜しみない支援を提供できる。

このように、IGCIは、シンガポール国外でも活動している。しかし、インターポールは捜査権を持たない法執行機関であり、捜査を開始するのは各加盟国であるため、加盟国に入国して捜査や作戦を開始する国際管轄権をインターポールは持っていない。これは多かれ少なかれ、全ての国際法執行機関に共通することと思う。但し、インターポールは、加盟国に捜査開始を命じることはできないが、加盟国にできる限りの情報や支援を提供し、捜査開始を促すことはできる。インターポールはFBIとは異なるし、映画に出てくるインターポールとも全く異なっている。

続いて、IGCIの組織について説明する。IGCIの総局長は、皆さんご存じと思うが中谷昇さんである。中谷さんは日本の警察庁からの出向であり、IGCIを設立時から率いている。中谷さんはIGCIをゼロから立ち上げ、設立時の人員を採用している。IGCIは、彼の指揮の下で動いている。

IGCIには、まず、デジタル・クライム・センターがあり、これはサイバー犯罪捜査の作戦部門である。このセンターには、デジタル犯罪捜査支援とデジタルフォレンジック・ラボという２つの部署があり、また、デジタル犯罪捜査支援の下にサイバー・フュージョン・センターもある。

次に、サイバー・イノベーション・アウトリーチ[5]部門である。この中にも、２つの部署があり、１つは私の所属する戦略・アウトリーチ部署であり、サイバー戦略を支援し、また民間部門に接触してインターポールや加盟国への支援を取り付けている。もう１つが研究・イノベーションであり、同僚のシルヴィオ・ストリートマンが率いている。

IGCIは、サイバーやその他の分野を含めて、100人以上を雇用しているが、指令調整センターに所属するスタッフもいる。指令調整センターは世界に３つあり、リヨンとシンガポールとブエノスアイレスにある。私達は、東南アジア組織犯罪ユニットにも支援を行っている。

さて、柱の１つであるハーモニゼーションについてであるが、IGCIが従事する活動がいくつかある。まず、各国の状況やサイバー犯罪を捜査・予防する能力に関する情報を得るための国別サイバー・レビューである。次に、サイバー戦略の策定であるが、サイバー戦略の策定を必要とする国に対して手を貸したり、他の機関や組織と協働したりする。

続いて、キャパシティ・ビルディングと訓練についてであるが、IGCIは訓練コースの提供も行っている。訓練コースの一部は、世界各地で実施されており、例えば、インターネット・ガバナンス[6]、インタ

---

5　本来の意味としては、手を伸ばすこと。転じて、裾野を広げていくことという意味合いで使われている。

6　インターネットを健全に運営する上で必要なルール作りや仕組みなどを表す言葉

ーネット捜査、ダークネット[7]捜査等のコースがある。

次に、作戦支援に関しては、発表の最後に２つの事例をお話しする。コーディネートされた作戦をインターポールが各国と連携してどのように実施したかについて話をする。

サイバー・フュージョン・センターは、加盟国及び民間部門がインターポールに支援を求めたり、情報を提供するための窓口である。警察機関が学術機関、民間部門と協力して情報を提供・分析したものに基づき、加盟国が行動を取れるような実用的な情報を提供することを私たちは目的としている。これは共同作業であり、私達だけでは行うことはできない。

サイバー・フュージョン・センターは立ち上げられたばかりであり、ツールや法的な問題に取り組んでいるところであるが、民間部門から得られる情報にはどのようなものがあるだろうか。民間部門に提供できる情報にはどのようなものがあるだろうか。

通常、警察機関と民間部門の協力では、情報交換が非対称になってしまうのが問題である。つまり、民間が警察機関に情報を提供しても、警察からフィードバックを得られるとは限らないということである。情報を提供したけど、その後どうなったのかという問題である。この問題は、インターポールに限らず、ヨーロッパを含め、世界中の警察機関でずっと議論されていることであり、効果のある唯一の解決法はない。

したがって、民間部門と情報交換における信頼を築かなければならない。また、加盟国、特に加盟国の警察機関とも協力しなければならない。民間部門が、インターポールや国際警察機関に情報を提供すると、インターポールは情報の出所の国に通知し、情報の所有者を決定する必要が生じることとなるが、インターポールや国際警察機関とのこのような情報交換は非常に重要である。この情報交換なしに、私達がサイバー犯罪と戦うことはできない。

次に、フォレンジック支援についてである。デジタル・フォレンジック・ラボ（DFL）はトレンドマイクロやカスペルスキー・ラボなどの民間部門と協働している。カスペルスキー・ラボは、スタッフを１人フォレンジック・ラボに出向させてマルウェア分析をさせている。また、私達には携帯機器フォレンジックに関する専門知識もあり、インターポールから遠隔で又はスタッフを現場に送って捜査支援を行

---

7　インターネットで到達可能なグローバルIPアドレス空間のうち、どのネットワーク、コンピュータにも割り当てられていない未使用のアドレス群のこと。ダークネットは未使用のIPアドレスであり、通常はダークネットに対してパケットが送信されることは殆どないが、実際にはダークネット上で相当数のパケットが観測されるといい、その多くは不正な行為・活動に起因するものと言われている。（IT用語辞典より）

うこともできる。実際、IGCIの携帯機器フォレンジック専門家は世界各地に出向き、サイバー犯罪捜査のみならず、アジアでの殺人事件捜査やフィリピンにおける性的搾取事件などでデジタル・フォレンジックの支援を行った。

しかし、残念ながら、192か国ある全ての加盟国にデジタル・フォレンジック・サービスを提供することはできないため、このサービスを提供する際には地元職員の訓練も同時に行っている。つまり、次にフォレンジックサービスが必要になった場合、インターポールの力を借りずに自分達でフォレンジック捜査を実施することが期待されているのである。

最後に、サイバーイノベーション・アウトリーチ部署では、サイバー分野における研究支援、キャパシティ・ビルディング・訓練、戦略支援、アウトリーチを実施する。アウトリーチは、民間の技術系企業だけでなく、主要なステークホルダーに対しても行う。

### 3　研究・イノベーション

研究・イノベーション部署では、まず、サイバー研究ラボを設置している。そこでは、NEC、日本のサイバーディフェンス研究所などの民間部門と連携している。また、研究用の暗号通貨やダークネットの構築に取り組むオランダの研究機関であるTNO[8]とも協力関係にある。

サイバー能力の向上と関連して、今日、シンガポールでサイバー訓練のカリキュラムについて議論する会議が開かれている。インターポールは、現在、基礎レベル、中級レベル、上級レベルの捜査員向けのサイバー訓練のカリキュラムを作成しているところであるが、これはサイバー犯罪捜査員だけでなく、フォレンジック専門家も対象にしたものである。また、現在、世界共通で使用されるこの種のカリキュラムはない。

加えて、研究・イノベーション部署では、国別サイバー・レビュー・サービスも提供している。

インターポールには、インターポール研究ネットワーク（IRN）と呼ばれるものがあり、そこでは警察機関、官民両部門、学術機関が協働している。通常、警察機関は研究機能を持たないが、日本では警察機関においても研究の自由度が高く、かつ強力であることを嬉しく思っている。しかしながら、ほとんどの国の警察機関には研究機能がないのが現状である。

IRNが行ってきたプロジェクトとしては、まず、各国にサイバーフィーズ(Cyber feeds)を公開してきた。サイバーフィーズとは脅威や技術など、特定の情報に関する資料であるが、各国の警察機関に脅威や技術に関する情報を提供して、国内で情報を共有したり、捜査などに使用できるように公開してき

---

[8] オランダ応用科学研究機構（The Netherlands Organizations for Applied Scientific Research）

た。

また、闇サイトから収集した違法銃器に関する情報や偽造 ID・パスポート等の市場に関する情報を記載した報告書も提供した。

そして、モバイル・マルウェアやランサムウェア[9]に関する研究報告書を公開した。

TNO と連携して実施しているシミュレーションゲームについては、先週ベルギーのブリュッセルで開催された。このコースに関しては後でお話しする。

続いて、ブロックチェーン[10]について、インターポールとカスペルスキーは、ブロックチェーンにおいて特定された脆弱性に関する報告書を共同で発表した。また、この報告書は今年の Black Hat Asia 会議で発表された。

そして、私達は、捜査支援のためのツールも開発している。

インターポールは所有するこれらのツールについては、加盟国に情報を提供しているが、こういったツールを加盟国と共有することで、提供を受けた加盟国がツールをさらに改良し、情報や改良ツールをインターポールに提供してくれたらと期待している。また、私達がよく聞かれる質問に、「こういったツールを販売するのか？」というものがあるが、私達は加盟国に何も売らない。私達は全てのサービス、訓練、ツールを加盟国に無償で提供している。加盟国はインターポールに分担金を払っており、これがサービスの財源となっている。

次に、現在進行中のプロジェクトについてであるが、興味深いプロジェクトの１つがオープンソース・ダッシュボード・プロジェクトである。これは、オープンソースから情報を収集、集約、分析して加盟国に提供するシステムである。

次に、サイバーセキュリティーに関する各国の状況の週報、隔週報である。これには直ちに事件には結びつかない情報も含まれ、進行中の犯罪に関する情報を提供できるというわけではないが、それでも傾向、潜在的脅威に関する非常に重要な情報が含まれている。この情報は国内でも共有できるし、こういった情報のためのツールを来年の後半には加盟国に提供したいと思っている。

続いて、研究課題についてであるが、インターポールが研究活動を開始する際、研究分野に優先順位をつける必要があった。研究に関しては、何十もの問題や興味深い分野があったが、加盟国、民間部門、学術機関と会議をもち、インターポールにとっての課題、そして学術機関にとっての研究テーマを決めた。

---

9　感染したコンピュータが正常に利用できないよう人質に取り、復元のために対価の支払いを要求するソフトウェア（IT 用語辞典より）

10　分散型ネットワークのこと

こうして研究課題として決まったテーマについて、まずはアトリビューション[11]の進展が挙げられる。これは、もちろん警察機関にとって重要なテーマである。

次に、サイバー犯罪の評価、予測についてである。現在、多くの組織がサイバー犯罪に関する情報を集めているが、グローバル規模での全体像はつかめていない。

そして、情報交換に関する問題は100年前から存在するが、民間部門との情報交換をどのように推進するかといったことも課題の１つである。

プライバシーとセキュリティのバランスについては、捜査の解決をするだけではなくて、プライバシーとのバランスをどのように取りながら行うかという問題である。

サイバー空間における予防策の向上については、何が有効で何が有効でないかは誰もが理解するところである。

デジタルフォレンジクスについては、産業界にとって関心の高い問題であるが、この分野で警察機関を支援するような実戦的情報を提供するシステム、製品を開発できるかという課題である。

最後がサイバー犯罪学の研究である。なぜ犯罪者は罪を犯すのか、サイバー犯罪者と従来の犯罪者の間には違いがあるのかといったことであるが、サイバー分野は他の分野と比べてより複雑である。現在、インターポールはこの分野でいくつかの大学と関係を持って、研究を行っている。

そして、闇サイトにおける訓練についてである。この訓練はシミュレーションゲームであるダークリスを使用して実施されている。インターポール、TNO、カスペルスキーの共同取組であり、私達が開発した訓練ゲームである。

この訓練については、１週間理論だけを教えるのでは、人を訓練し、動機付けし、興味を維持させることは時として非常に難しくなるので、少し工夫をこらしている。この訓練は、第１回は昨年７月にシンガポールで、第２回は先週ブリュッセルで実施された。コースの前後にインターネット上での講義を実施したり、また、このコースに参加する警察官は一定のスキルを既に持っている必要があるといった特徴がある。

私達はリアルな闇サイト、つまり、Tor[12]のような非常にシンプルなネットワークをラズベリーPI[13]上に作成した。私達はラズベリーPIを数台所有しているが、このコンピュータの価格は１台30ドル程度である。つまり、この小さなコンピュータを使って、Torネットワークを作成して、安全な環境で警察官が訓

---

11
一般的にサイバー攻撃者を把握・特定して対抗措置を講ずるという意味で使われているが、法的な面では明確な定義はなされていない。

12　匿名化ソフトの名称

13　超小型コンピュータの名称

練を行えるようにした。

また、違法な物品を市場で売買するための暗号通貨ダークコイン[14]やブロックチェーン等を作成した。そうして、捜査を開始して、証拠を集めることになる。

つまり、これは、売り手、買い手、市場運営者、そして警察が参加する闇市場におけるシミュレーションゲームなのである。そして、インターポールは、オランダの研究機関であるTNOとともに、様々な市場を慎重に監視する。TNOはモニターと呼ばれるツールを持っており、Tor上の市場に関する情報を収集することができ、また、市場に限らず、あらゆるサービスを監視する。

何かを学ぶには間違いを犯す必要があり、間違いを犯さなかったということは、おそらく何も学ばなかったということになると思う。こうした安全な環境で訓練を行う警察官は、安全に間違うことから学ぶことができるのである。

次に、インターポール・デジタル・セキュリティー・チャレンジであるが、これは民間のパートナーと一緒に行っている国家チーム間の競争である。今年の年末に第１回インターポール・デジタル・セキュリティー・チャレンジを開催したいと思っていたが、残念ながら多くの会議が年末に集中しており、12月にデジタル・セキュリティー・チャレンジを開催するのは無理であると判明し、このイベントは来年の３月に延期された。

この大会では、サイバー犯罪部署の責任者、サイバー犯罪捜査官、フォレンジック支援要員から構成されるチームを競わせたいと思っている。そして、私達が作成したサイバー犯罪シナリオ、つまり、模擬サイバー犯罪シナリオの中で各チームは競う。証拠を集め、犯罪者を特定し、犯罪を解決するのがチームのタスクである。デジタル・セキュリティー・チャレンジの最後には、各チームは検察官に証拠を提出し、検察官は証拠を評価し、チームを採点し、結果を発表する。これは友好的な競争であり、国代表のチームのほか、地域代表のチーム、混成チームも出場することができる。

インターポール・デジタル・セミナーについては、民間のパートナーと一緒に行っている。特に、未来の犯罪技術については、インターポールが特に関心を持つ分野の１つであるが、民間のパートナーとは複数分野で協力しており、このセミナー終了後、レポートを作成して加盟国と共有する予定である。

### ４　能力向上

まず、能力向上プロジェクトに関してであるが、現在実施しているサイバー訓練戦略やコースカリキュラムの標準化といったことがある。

そして、加盟国の要請により行う国別サイバー・レビューであるが、法律やサイバー犯罪捜査、デジ

---

14　匿名性に特化した暗号通貨のこと

タルフォレンジックの能力について検証を行う。これは加盟国において、捜査活動や官民連携の能力に差がある場合に勧告を行えるようにするための能力差分析のようなものである。

## ５　戦略支援

まずは、戦略支援プロジェクトの中のグローバル・サイバー犯罪専門家グループについてであるが、今週の月曜と火曜に第１回のグローバル・サイバー犯罪専門家グループの会合がシンガポールで開催された。このグループには、研究、戦略、訓練、オペレーション、デジタルフォレンジックに関するサブグループがある。このグループの目的は、重点的に取り組むべき分野、サイバー犯罪と戦う上での優先順位をインターポールに勧告することであり、全ての地域の代表者が参加するものである。この２日間の会議の結果をレポートにまとめて事務総長に提出し、これに基づいて事務総長はIGCIの次のステップに関する決断を下すことになる。

また、インターネット・ガバナンスに関してはICANNと協力関係にある。ICANNはInternet Corporation for Assigned Names and Numbersの略称である。ICANNはインターネットに関する方針を立てる団体であり、インターネット自体の運営を行うわけではないが、ICANNが策定する方針の下でインターポールが動くこととなる。警察機関にとって重要なのはICANNの特定の政策や勧告に関して声を上げることである。

そして、インターネット・ガバナンスに関してのインターポールにとっての重点分野が「WHOIS」データベース（ドメインやIPアドレスの所有者のデータベース）である。「What is」、つまりモノに関する情報は手元にある場合が多いため、WHOIS情報の入手が捜査にとって重要になる。ドメインやIPアドレスの背後には誰がいるのかということである。こうしたものに対処するため、インターポール、ユーロポール、その他の警察機関は正確なWHOIS情報を入手して、捜査を支援したいと考えている。

また、2012年以降、インターポールはICANNのインターネット・ガバナンス諮問委員会にオブザーバーとして参加している。

サイバー犯罪作業部会にも、各国の代表や他の国際機関と一緒に参加している。この部会には、まず、グローバルレベルのインターポール・サイバー犯罪グループがあり、その次に、より実働的なアメリカ、ユーラシアの各地域作業部会がある。ユーラシアはアジアとヨーロッパを意味している。

## ６　アウトリーチ

ここからは実際の作戦についてお話ししていく。まずは、ストライクバック作戦についてである。フィリピンにおける性的搾取事件であり、具体的には、フィリピンの組織犯罪グループが被害者に接触し、わいせつな行為をさせてそれを録画し、脅迫し、17歳のスコットランド人少年を自殺に追い込んだ

といった事件であるが、58 人が逮捕され、彼らはその後起訴され、刑の宣告を受けた。また、250 点以上の電子装置が押収された。この捜査ではイギリス、香港、フィリピン、シンガポール等多くの国が協力した。

次に、ボットネット[15]SIMDA の捜査ではマイクロソフトと協力した。同社がボットネット SIMDA をテイクダウンするためにインターポールに協力を要請してきたのである。世界で 70 万台以上のコンピュータが感染したのだが、犯罪者グループの手口も変わってきている。

サービスとしてのマルウェアは、犯罪者グループにとって利益性の高いモデルであり、彼らはこのボットネットのサービスを使って、１つでなく複数のマルウェアの土台を作った。

ボットネット SIMDA の捜査は、複数の地域で協力して実施された。作戦はオランダ、ロシア、ルクセンブルグ、アメリカ、ポーランドとの共同であり、ある時点では、イランにも接触して話し合いを持った。先ほど話をしたが、インターポールは政治的に中立的な組織であり、ボットネットをテイクダウンするために多国間が協力したが、この種の協力は、もし協力が二国間に限られていたら不可能であったかもしれない。

捜査は進行中であり、被害者の救済も進んでいるということはお伝えしておく。また、このボットネットの背後に誰がいるのか突き止めたいと思っており、このボットネットに関して集めた証拠は現在 IGCI にて分析中である。マルウェアの分析は IGCI の専門家とカスペルスキーが共同で実施しており、今後、捜査・アトリビューションに着手したいと考えている。

捜査において、いかにして調整を行ったかということであるが、コミュニケーションはインターポールだけでなく民間のパートナーにとっても重要である。そして、この作戦では、IGCI の新能力を駆使して、国レベルでサイバー犯罪作戦を調整することができた。

学んだ教訓の１つに、プライバシーと情報収集のバランスを取る必要があるということが挙げられる。現在、私達は多くの量の情報を収集しているが、脅威に関する技術的情報であればインターポールが処理できるが、個人情報については、民間部門と協力して、個人情報の除去を行ってから、加盟国と共有する必要がある。

---

15　攻撃者の命令に基づき動作する不正プログラム（ボット）に感染したコンピュータ及びこれらのコンピュータに攻撃者の命令を送信する命令サーバから成るネットワーク

## 【②基調講演】　ＥＣ３の活動について　～ＥＵ内における官民連携、国際連携を通した取組～

Europol から IGCI へのリエゾン・オフィサー　　ベノワ・ゴダート
編集／警察政策研究センター教授　　辻　貴則

### １　ユーロポールとインターポールの間の協力関係

まず、ユーロポールのことをよくご存じでない方のために簡単に説明する。インターポールとユーロポールは協力関係にあり、使命も共有している。私達の役割は、あらゆる形態の深刻な国際犯罪及びテロリズムを防ぎ、また、警察機関を支援することである。これはインターポールも同じであるし、世界中の警察機関とも共有する役割である。

しかし、ネットワークはそれぞれ異なっている。ご存じの通り、EU には 28 の加盟国がある。EU の歴史は古く、1957 年にイタリア、フランス、ドイツ、オランダ、ベルギー、ルクセンブルグの６か国でスタートした。その後、アイルランド、イギリス、デンマークの３か国が加入し、さらに、ギリシャ、スペイン、ポルトガル、フィンランド、スウェーデン、オーストリアと少しずつ加盟国を増やしてきた。その後、10 か国を加盟国として迎えたが、その 10 か国にはマルタが含まれる。ご存じと思うが、地中海にある小さな島国である。さらに、キプロス、ブルガリア、ルーマニア、そして、昨年、一番新しいメンバーとしてクロアチアが加盟した。

これが現在の EU であり、私が所属する EC3 は EU に属する機関である。オランダ・ハーグに拠点を置くが、２年前にユーロポール内に設置された。

ユーロポールでの経験を生かして、データを処理・分析したり、それに基づき、EU 加盟国や警察機関、パートナー機関を支援して、究極的には市民の利益・安全を確保する。これは自分たちだけではできないので、ノルウェー、スイス、バルカン諸国を含むその他のヨーロッパ近隣諸国と協定を結んだ。状況は良くなってきているが、それでもまだ難しい問題である。

また、私達はアメリカとの運用協定に調印し、カナダとの運用協定にも調印した。そして、オーストラリアやヨーロッパの北側にあるアイスランド、さらに、コロンビアとも協定を結んでいる。コロンビアでは、麻薬取引が大きな問題になっているからである。私達は大きな役割を果たしているが、さらに貢献度を高めていきたいと思っており、コロンビアの当局は支援してくれている。

インターポールがメインパートナーであるということは、192 のインターポール加盟国とつながる機会を得られるということであり、これは大きな強みである。これがないと、日本を含む各国に接触するのは難しくなる。

IGCIの存在は、現在私達がカバーできていない地域、特にアジアに活動範囲を広げていく上で素晴らしい機会をもたらしてくれている。私達にとってこれは極めて重要なことであり、IGCIのユーロポール代表機関として、私達はこの広がった活動範囲から大きなメリットを得ている。

ウルクニエミさんがおっしゃったように、彼らはヨーロッパ各地に設置した支局から構成される素晴らしいネットワークを持っている。一方、私達もEUにオフィスを持っており、EU各国から得られる情報を基に、私達が何ができるのかを理解する助けになっている。

私達は様々なサービスを提供している。ウルクニエミさんがおっしゃっていたが、インターポールの大きな強みはグローバルネットワークを利用した手配書の配布であり、赤手配書はその象徴である。そして、手配書は世界に配布される。

一方、私達の主な強みは分析能力、犯罪分析である。それによって、手配書に関係するインターポールの活動やグローバルデータベースに関係するインターポールの活動を補完する。また、警察機関、ヨーロッパのパートナー、ヨーロッパ諸国にこういった分析ツールを提供することもできる。これにより捜査を実施している全ての警察機関が集めた情報を収集することができ、とても強力なツールである。

そして、構造や組織の点でもいくつかの違いがある。

私達は多機関アプローチを採用している。私のユーロポールでの役職名はフランス国家捜査サービス・ディレクターである。私はフランス国民であるが、ヨーロッパのために働いている。私が所属する機関は警察ではないが、捜査権を有している。また国によって異なるが、スペインのGuardia Civil、イタリアのGuardia di Finanza（Finaicial Guard）、Carabinieri等、様々な機関があり、捜査対象の様々な犯罪に強いインパクトを与えるべく協力して組織的に取り組んでいる。

一方、インターポールと協力する大きな利点は、先ほどの話にもあったが、「フォロー・ザ・サン」、つまり、シンガポール、リヨン、ブエノスアイレスと太陽を追いかけるように各拠点を利用することで、24時間の対応ができることである。

また、インターポールとユーロポールは協定を結んでいる。歴史はそれほどないが、しっかりとした協定である。まず、両者は2001年に運用協定を結んだ。この運用協定を通じて私達は犯罪者に関するデータを共有することができる。つまり、私達のデータとインターポールのデータベースとを照合できることとなる。インターポールは非常に多くのデータを持っており、フランス、ドイツ、イタリアなどEU加盟国の捜査官と域外の捜査官とを橋渡しできる可能性がある。

ユーロポールにはインターポールの職員が２人、リエゾン・オフィサーとして常駐している。そのうちの１人は、日本の警察庁から派遣されている日本人である。雲田さんという方であるが、私が嬉しく

思うのは、彼がこのヨーロッパ人中心の機関の部署に配属された最初のアジア人だということである。

違いはあっても、問題はない。私達の言語と皆さんの言語は異なるが、私達は同じ「言葉」を話し、同じ目的に向かい、同じゴールに向かっているので、問題はない。

次に、EC3が取り組んでいる３プロジェクトを紹介する。まずフォーカル・ポイント・サイボーグであるが、これはサイバー攻撃、サイバー侵入に焦点を当てたものである。次にフォーカル・ポイント・ターミナルであるが、これはサイバー空間におけるクレジットカード詐欺に関するプロジェクトである。最後がフォーカル・ポイント・ツインズであるが、これは子供の性的搾取に関係する捜査を支援する運用プロジェクトである。

このほかにも多くのプロジェクトがある。IGCIのプロジェクトもリストに入れているが、その意図は、私達が活発に交流していることを理解していただくためである。インターポールは私達のネットワークの一部であり、私達はインターポールがシンガポールやリヨンで実施しているプロジェクトの一部なのである。

こうしたアプローチをとることで、両者間で大きな相乗効果を生み出すことができ、警察機関に対しても多くの情報を提供できるようになる。子供の性的搾取について、例えば、私達はインターポールの信頼できるデータベースを利用できるし、私達もデータベースを持っているので、双方がうまく機能している。

業務の流れは、ユーロポールとインターポールで異なる。それほど重要なことではないが、インターポールはI-24/7というネットワークを利用している一方、私達はSIENAという自分たちのネットワークを利用している。これはSecure Information Exchange Network Applicationの略称である。重要なのは相互運用性であるが、EU加盟国でユーロポール、インターポールそれぞれに加盟している国の捜査官が同じリクエストを２回しなくても、この２つのネットワークに接触できるシステムである。そして、そのリクエストは１つの書式で行える。現在はまだ効果的なシステムとまではなっていないが、改善に取り組んでいる。

情報の照合の大切さについてはお話ししたが、ユーロポールに情報があるとして、運用協定を利用して、インターポールのデータベースと照合でき、私達の管轄にある国と情報交換したいと考えるインターポールの加盟国を特定することができるということなのである。これは双方向に言えることであり、つまり、インターポールも彼らの情報を私達のデータベースを使って照合できるのである。やや複雑に聞こえるかもしれないが、うまく機能している。

インターポールの赤手配書作戦が良い例である。これは逃亡者を世界レベルで捜査する作戦である。現在、約27,000件かそれ以上の赤手配書が発行されていると思うが、重要なのは逃亡犯の居場所を突き止めることであり、その目的で立ち上げられた作戦である。リストを入手して私達のデータベースと照

合する。初めての経験だったのだが、４人の犯罪者の居場所を突き止めることができ、結果は成功であった。これは、インターポールが持っていないデータを私達が持っていたからである。こうして機能するということが分かっていただけたと思うが、より良い形で機能するため、現在、より体系的になるよう取り組んでいる。

リエゾン・オフィサーがインターポールとユーロポールをつなげていることは先ほどお話ししたが、それに加えて、ワシントンに拠点を置くリエゾン・オフィサーが２人いる。ユーロポールのEC3にはプログラム委員会が設置されており、これにはあらゆるステークホルダーを含むが、こうした組織的なアプローチの重要性を私達は理解している。

また、インターポールが関係するプログラム委員会もあり、２日間にわたってシンガポールで開催された専門家グループにユーロポールを代表して参加できたことを嬉しく思っている。インターポールは、ヨーロッパサイバー犯罪タスクフォースのメンバーであり、ヨーロッパのサイバー犯罪部署のリーダーである。サイバー犯罪部署のリーダー28人が定期的に集まるが、インターポールも参加している。そのお礼というか、お互いに補完し合うために、私達はヨーロッパ外の組織で構成されている地域作業部会のメンバーになっており、これでEUに限定されない広い地域の全体像を得ることができる。

次に、欧州サイバー犯罪タスクフォースで私達が行っていることであるが、３つのプロジェクト、すなわちサイバー侵入、クレジットカード詐欺、子供の性的搾取である。インターポールのネットワークを使えるという強みを生かして、 南北アメリカ、ASEAN、中東、アフリカ全域に活動範囲を広げており、これも大きな成果を上げている。

そして、最終的な目的は、捜査が実施されるのがスペインであれ、オーストラリアであれ、フランスであれ、対象事件の犯罪者や犯罪者グループに関するデータを共有することである。

サイバー犯罪の分野でこういったことを行うには、民間部門と協力する必要がある。これは必須であり、難しいということは認めるが、革命的と言っていいことである。私は手元にある情報全てを秘密にするよう訓練を受けており、民間部門に接触して情報を提供してもらったとしても、こちらからその情報提供者には情報を提供することはなかった。しかし、今考えると、このやり方を検証する必要があると思う。私は決して規則を破らないが、パートナーシップ以上の協力を引き出す方法を見つけなければならない。民間部門の参加によりこの関係はさらに改善されると思う。

ここまでは、導入として、地域レベル、そして世界レベルでの私達の活動－私達はどのように相互に関係してコミュニティに貢献しているかを理解していただくために説明してきた。

## ２　EC3の活動

次のテーマに行きたいと思う。グローバル環境を念頭に置いて、EC3 に話を移したいと思うが、これが発表のメインである。

ヨーロッパで機能しても、その他の地域ではおそらく機能しないので、モデルとしてお話しするわけではない。しかし、私達はいくつかのベストプラクティスを実施することで、設立以来わずか２年間で大きな成果を上げてきたので、このベストプラクティスは他の地域にも有意義ではないかと思う。

私達はゼロからスタートしたわけではない。ユーロポールはグローバル組織として既に存在していたし、情報交換が可能な成熟レベルにあった。情報を交換するに当たっては信頼が必要であり、情報交換に関して、関係者の考えが一致している必要があるが、私達には信頼できるネットワーク情報交換システムがあり、また、情報の取扱いもしっかりとしている。情報を誰と共有するかを決めるのはあくまで情報の所有者であるが、これは重要なことである。なぜなら、提供する情報が EU 全体に配布されることはなく、その情報は協力関係を持ちたい国にのみ共有されるという理解の上で情報を提供できるからである。もちろん、ユーロポールの代表者としての私の心配は、皆が情報を共有してくれるかどうかであり、情報交換ツールを誰もが利用できるよう着実に努力する必要がある。

続いて、ユーロポールに関する数字であるが、912 人が勤務している。まもなく 150 人増員するが、これは地域のテロ対策、そして移民問題への対策によるものである。移民問題といっても、移民自体が問題なのではなく、不法移民が問題になっている。昨今の移民の流れを悪用して EU に入ろうとする人達がいて、この中にテロリストが含まれることは、残念ながら、最近の事件によって確認された。

また、ユーロポールは 40 か国をカバーし、73 の事務所を持っており、予算は 9,600 万ユーロである。そして、重要なのは、912 人のスタッフ中、200 人がリエゾン・オフィサーということである。つまり、お話しした国 28 か国全て、そしてパートナー機関がリエゾン・オフィサーをユーロポール本部に置いている。廊下を歩くと全ての地域を通過できるようなものである。それぞれの国のリエゾン・オフィサーは自国のデータベースにアクセスできるが、それにより、情報交換のスピードを高められる。そのほかに 150 人のアナリストもいる。分析は当機関の中核機能であるが、熟練したアナリストが情報の照合、データ分析、金融情報と犯罪ネットワークから得た情報の統合、全体像の把握を行い、これを捜査官が様々な事案に生かす。そして、私達は１年におよそ 73,000 件の案件を処理していく。

続いて、EC3 についてである。サイバー・セキュリティ、サイバー・ディフェンス、サイバー犯罪のあらゆる側面を考慮しながら対策を行うという決定が欧州連合によって下された。私達は指定機関、つまり、EC3 はサイバー犯罪の専門機関である。私達はギリシャを拠点にする欧州ネットワーク情報サービス機関（ENISA）と協力関係にある。ENISA はセキュリティを主に扱う機関であり、対応チームである CERT とも連携している。

一方、私達はその他の分野に重きを置く欧州の安全保障関係機関とも交流がある。私達が相手にしているのは犯罪者であるが、グローバル戦略は私達が使命を果たす上での助けとなっている。

インターネットの普及状況について、地図（省略）をご覧いただきたいが、ヨーロッパにおける普及率は高く、日本でも高い。ヨーロッパの普及率は76%であるが、ご覧のとおり、南北アメリカ大陸や、その他の地域でも増加が著しい。誰もがインターネットを利用する時代になったといえ、これは素晴らしいことである。ビジネスのために良いことであるし、革新を生み出すために良いことである。

一方、インターネットの普及は犯罪者にとっても格好の機会になっている。インターネットには多くの脆弱性が存在する。現在、27億人がインターネットを利用しており、2017年までに35億人、すなわち全人口の半分に増えると予想される。IoT[1]についてお話しすると、現在、100億台の機器がインターネットに接続されているが、規模を考えると、技術の脆弱性を悪用する可能性を犯罪者に与えてしまったといえる。インターネットは当初、多くのことを想定して設計されたが、それにセキュリティは含まれていなかった。こうして、今日、私たちが直面している課題がある。

私たちは物理的な世界からデジタルの世界に移行している。以前、私たちはリアルな世界の犯罪者を追っていた。銀行強盗犯は銃を持って実際に銀行に足を運び、そして犯行現場にいくつかの証拠を残し、私たちはそれを収集したものである。

次は、世界における収入の分布図を見ていく。当然のことであるが、犯罪者の目的はお金であり、お金を簡単に手に入れることが彼らの主な目的である。お金の多くはアメリカ、ヨーロッパ、そして日本に存在するが、それは主要銀行があるからであり、世界に散らばる犯罪者達はこのお金を狙うのである。

そして、2014年６月の作戦で監視したネットワークについて見ていくが、何が起こったのかというと、世界中から収入の多い組織や地域が攻撃を受けたのである。これが現代の犯罪様式であり、私達は今も従来型犯罪に有効なツールを使って協力を行っているが、もはや適切ではない。

サイバー犯罪は電子の速度でグローバル規模において行われる。日本から情報を得るには、刑事共助条約を利用することとなる。これは素晴らしい制度であるが、日本の当局に接触するにはいくつかのステップを踏む必要がある。例えば、私がフランスの捜査官として情報提供を要請するとして、まずフランスの行政官に要請を提出し、そしてこの行政官が大使館に提出する。大使館、外交ルートを使って大

---

[1] Internet of Things の略。コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行うこと（IT用語辞典より）

使館、日本の代表機関に到着する。日本がこの要請を受領し、当該案件の処理要請がなされ、問題がなければ、要請が処理されることとなる。但し、問題は、情報の受取が、事件発生からかなり時間が経過してからになってしまうことである。データを保存するためのツールが存在するが、こうした新しい環境下では検討する必要があるだろう。

インターネットには複数の階層があるが、今ご覧になれる部分がインデックス可能なレベル、すなわち、私達が検索エンジンでアクセスできる部分である。一般の人が利用できるものである。そしてその下の部分は深層ウェブと呼ばれており、会社などが様々な目的で使用するものであり、皆がアクセスできるものではない。私達が注目するのはさらに下の部分、ダークネットと呼ばれる部分である。先ほど話に出たTor、The Onion Routerはその良い例である。Tor[2]を介したコミュニケーションではAとBが直接接続されないネットワークを利用するので、完全な匿名コミュニケーションを可能にする。

加えて、暗号化技術というものもある。コミュニケーションは匿名であり、かつ暗号化される。私達の職務は犯罪者を追跡することなので、こういったことは非常に懸念している。犯罪者はこのようなシステムを悪用している。

また、私達は多くの困難に直面している。サイバー犯罪、これには従来型のサイバー犯罪もあれば、他の種類の犯罪を助長するサイバー犯罪もある。過激な活動ももちろん心配であり、テロ活動もそうである。国が支援する活動は対象ではないが、関心はあり、なぜなら、国レベルで使用される技術や情報がごく短時間で犯罪者によって使用されるからである。つまり一部の国では、国レベルで取得した専門知識・技術がごく短時間で組織犯罪グループにわたり、それが、こういった攻撃をより複雑にし、対応を難しくしている。

私達の主なターゲットは組織犯罪である。この種の犯罪者は様々な目的でシステムを悪用するが、主にシステムに攻撃、侵入してくる。ハッキング、トロイの木馬、マルウェア、スパイウェア、DDoS攻撃など種類には事欠かない。そして先ほどお話ししたダークネットでは匿名で暗号化された情報が行き交う。暗号化は問題である。また、仮想通貨は、マネー・ローンダリングを行う者がこのような土台を取引のために利用する。誤解してほしくないが、仮想通貨は犯罪行為に使われることを想定して設計されたものではないということである。正当な目的でも使用されるが、犯罪目的でも悪用されているのが現状である。

そして、「サービスとしての犯罪」と呼ばれるものについて話をしたい。サイバー犯罪を行うには何もハイテクを熟知している必要はない。攻撃を行うために、必要なサービスを提供する人に依頼すれば良

[2] 匿名化ソフトの名称

いのである。例えば、私が競争相手を攻撃したいなら、まず私はボットネットを数時間レンタルする。ボットネットは複数のコンピュータと接続するインフラであるので、私はこれを使ってマルウェアを配布したり、DDoS 攻撃を行ったりできる。数時間のレンタルなので、とても安く済む。誰もがインターネットを利用できてそのメリットを得られる状況にあるわけであるが、これは犯罪者もインターネットを利用できるわけで、彼らはこの状況を利用している。そして、Tor や暗号化技術を利用すれば、インターネット上で匿名性を保てる。犯罪を共同で行う人たちはお互いを知らないので、彼らの追跡は捜査官にとって極めて困難である。

例を使って考えてみたい。マルウェアを作成する本物のエキスパートであるプログラマーがいるとする。彼は、別の人に助けを依頼してマルウェアをテストする。アンチウイルス・プログラムに対するテストである。幸いなことに多くのアンチウイルス・プログラムが存在し、脅威を減らしてくれているもののテストにおいてマルウェアが検出を回避できるようなものであれば手元に戻ってくることとなり、その後、ダークマーケットの深層ウェブを経由して、そのマルウェアは配布されることとなる。

「防弾ホスティングサービス[3]」と呼ばれるものがある。犯罪者は国家間の協力がしっかりしている国に拠点を置くと 、捜査の手が自分達に及ぶリスクが高くなることから、彼らのネットワークの情報が得られにくい国に設置する傾向にある。そして、アフリカや中東やバルカン地方などに拠点を置く OCG（組織犯罪グループ）を利用して世界中にマルウェアを配布してしまうのである。グローバル現象ともいえるものである。これはリアルな脅威である。

こうしたことへの対応策として、現在、４つの主要な作戦プロジェクトが進行中であるが、先ほどそのうち３つをご紹介した。サイバー侵入、子供の性的搾取、そしてクレジットカード詐欺に関するものである。残りの１つは、サイバーインテリジェンスに関する作戦である。警察機関は、民間と密接に連携し、追加情報を入手し、さらにオープンソースを監視して状況の全体像を把握していくが、私達はその活動の調整を行っている。

また、これまで私達は ZeroAccess、Game Over ZeuS、Ramnit などいくつものボットネットを閉鎖に追い込んできた。そして、重要な事例としてお話ししたいのは私達が初めて様々な機関と連携して対応したケースである。FBI 等のパートナーと協力することで、犯罪者があらゆる商品、例えばドラッグ、武器等の販売に使用していたダークマーケットにアクセスすることができた。この作戦では、17 人を逮捕し、410 の隠されたサービスを特定、閉鎖することができた。100 万ドルのビットコインの他、現金、ドラッグ、金、銀が押収され、さらに逮捕者の家のパソコンから多くの証拠が収集された。

もう１つの例について説明すると、別の枠組の中で実施した共同作戦で、名前はダークコード作戦で

[3] 匿名化されたレンタルサーバのこと

ある。標的のこのグループは英語を話す最も活発なサイバー犯罪グループだったが、この作戦では、28人の容疑者が逮捕され、37件の家宅捜査が実施され、数多くのコンピュータが差し押さえられた。

もう１つ作戦をご紹介したい。皆で連携して取り組んだが、基本的でシンプルとはいえ多くの成果を出せたという意味で良い事例になると思う。Global Airline Action Day とインターネットで検索してみると航空会社のページがヒットすると思う。航空会社のセキュリティ部門が私達に連絡を取ってきて、詐欺被害に遭っていると言ってきた。盗難されたクレジットカード情報を利用して無料で航空券を手に入れる人がいるということである。ダークマーケットで人のクレジットカードの情報を手に入れられるということであり、犯罪者はその情報を利用して無料で旅行したのである。

そういった相談を受けたことから、「分かりました。皆で協力しましょう。私達にデータ下さい」となり、私達はクレジットカード業界と連携したのである。Visa カード、Master カードと連携したのである。

私達はデータを収集、分析して、疑わしいとされる基準に適合した人間を抽出していった。ぎりぎりのタイミングでチケットを買った人、他国の IP アドレスを使ってチケットを買った人、出身国など、様々な基準を考慮してデータを収集していった。

そして、事件着手日に私達は管理する大量の情報を世界中の警察機関に配布したのである。私達が連絡ルートを持たない国に関してはインターポールの力を借りた。インターポールが対象地域の警察機関と密接な協力関係にあるからである。最終的に、222件の不審な取引を確認することができ、130人を逮捕した。2015年６月のことである。

この130人の逮捕者全員に麻薬売買、人身売買、マネー・ローンダリングなど、何らかの前科があったのである。普通の人がオンラインでチケットを無料で手に入れようとしたのではなく、犯罪者達がシステムの脆弱性を利用して「商売」をしているのである。麻薬密売人が無料で旅行しているのである。彼らはホテルの宿泊にも同じ手口を使う。

私達は11月にもこの作戦を実施して非常に良い成果を出しており、今後もこの作戦を続けていく予定である。航空会社、クレジットカード会社、地元警察をそれぞれ結び付け、この作戦を定期的に、可能なら毎日のように実施するようにしていく必要がある。

次に、被害者特定タスクフォースについてであるが、これは子供の性的搾取に関するものである。全ての捜査官を10日間結集させ、子供の虐待に関する資料を共有し、インターポールと協力して措置をとることで25人の被害者の特定、救出にこぎつけた。

NGO とも協力したことがあり、全米行方不明・被搾取児童センター（NCMEC）は、行方不明の子供や搾取されている子供の分野で活発に活動する団体である。彼らは情報を集め、私達にその情報を提供してくれるので、それを私達は協力して照合する。ある作戦を紹介すると、監禁されていたルーマニア人の生後22カ月の性的虐待被害者を救出して、被疑者を逮捕したというようなことも行った。

続いて、J-CAT、これはJoint Cybercrime Action Taskforceの略称であるが、あらゆる専門家、情報共有に積極的な国のサイバー専門家が集結する枠組であり、非常に良い取組である。様々なアプローチを駆使して事前に情報を得ることができ、その情報を基に捜査を行うこととなる。捜査に要する時間を短縮できるのである。

そして、４つの作戦プロジェクトを補完する３つの戦略プロジェクトがあり、作戦をサポートしていく。私達は加盟国のニーズや捜査官のニーズによって動くのであるが、分析能力を駆使した支援、フォレンジック支援、戦略やアウトリーチに関わる支援を提供していくこととなる。

「インターネット上の組織犯罪の脅威評価」という資料も発出しているが、そこには今後数年で私達が直面する可能性のある脅威の概要を把握するための情報全てが含まれている。何をすべきかの優先順位を決める助けにもなる。

また、サイバー犯罪の専門家から構成される枠組みもあり、ここに警察機関関係者を招待したいと考えている。技術的情報を交換したい人全てが参加できる。ベストプラクティスを共有する枠組みである。

サイバー犯罪の予防に関しては、私達には非常にしっかりしたプログラムがある。なぜなら、捜査を実施し、その後の起訴にうまく持っていくためには、まず取り扱う犯罪の数を減らすための予防が重要だからである。

優れた意識向上プログラムもあるし、相互支援プログラムもある。また、訓練とキャパシティ・ビルディングについては、３つの主要コースがある。１つはサイバー攻撃とオープンソース情報に関するもので、主にリナックス[4]のツールを用いて実施される。もう１つは子供の性的搾取に関するコースである。最後がクレジットカード詐欺に関するコースである。EU加盟国が主な対象であるが、一部の国に対してはオープンになっており、時々、条件付きでEU外のパートナー国を受け入れている。

また、インターポールとユーロポールの合同会議を毎年開催している。次の会議は来年、シンガポールで、９月の28日、29日、30日に開催される。ユーロポールを代表して、皆さんにも是非参加していただきたいと思っている。

---

4　OSの１つ。低い性能のコンピュータでも軽快に動作するといった特徴がある。

### 3　民間部門等との連携

最後に、民間部門と連携して成し遂げたことをお話ししたいと思う。私は２年間、ユーロポールにおいてEC3のアウトリーチ戦略作成とその戦略実施の責任者を務めていた。

とても難しい仕事であった。組織犯罪グループをターゲットにしていたが、繰り返しになるが、これは自分たちだけでできることではない。民間と協働する必要があり、金融部門に関わる諮問グループを複数設置したり、マイクロソフト、カスペルスキー、トレンドマイクロなど、数多くのインターネットセキュリティ会社と40の協定を結び、大きなメリットを得た。

また、電気通信会社、インターネットサービスプロバイダとも連携しており、重要インフラ、輸送､エネルギー分野にも連携範囲を拡大している。さらに、EU加盟国のみならずEU非加盟国の警察機関との関係も確立した。EU非加盟国に対しては、インターポールを通じて接触していった。

アメリカの場合を例に取っても、FBI、シークレットサービス、入国管理機関の代表者がタスクフォースに入っており、これは素晴らしいことである。インターポールと連携し、３つの国が捜査の過程で支援してくれたような成功例もある。

私たちは、法的文書なしで情報交換することができる。JIT（Joint Investigative Team）の設置当初から協定を結んでいるからである。そして、諜報の話まで広げると、これは非常に重要なことであるが、スノーデン事件以来、諜報機関と警察機関に対する大きな誤解がある。私達は独裁的権力を持つ国家機関ではなく、私達に全ての人を監視する能力はないし、そんなことはしたくもない。犯罪者を相手にするので手一杯である。

そして、学術機関との連携についてであるが、今日は学術界から参加された皆さんを前にお話しする機会をいただけて光栄に思っている。

最後に強調したいポイントであるが、私たちには、加盟国を支援するため、警察機関を支援するためのニーズや要請がある。EU機関の指導の下で、私達は民間部門とのパートナーシップの確立を模索したところである。そして、その最初のステップは協力関係を結びたい企業の特定である。企業情報、協力したい理由、評価、得られる情報の種類、私達の能力を補完できる可能性を把握する。

企業の特定の決定は局レベルでなされ、協定が調印される。目的は進行中の全てのプロジェクトに沿ったものが設定される。作戦であれ、訓練であれ、脅威評価であれ、うまくいくかどうかを判断し、６ヶ月おきに評価を行って、協力体制を改善していくのである。これはとても効果的であり、銀行、重要インフラ、インターネットセキュリティなどの分野と連携して行っている。民間部門、公共部門、学術部門それぞれに連絡担当者が任命されている。

以上で私の発表は終わりである。この機会をいただいたことを光栄に思う。ご拝聴ありがとうございました。