警察政策学会資料　第120号
令和３（２０２１）年１０月

サイバー空間と警察

警察政策学会
管理運用研究部会

まえがき

管理運用研究部会では「サイバー空間と警察活動」をテーマにして、本年 8 月 16 日、四方光氏を講師とした「社会安全政策論・サイバー犯罪対策及びインターネット上の越境捜査の課題」と題した定例会、9 月 28 日、松尾庄一を講師とした「警察活動におけるコンピューティングの可能性と限界－ AI（人工知能）と PI（ポリスマンインテリジェンス＝警察官の現場の知恵)」と題した定例会をそれぞれ開催した。

本資料は、四方氏の講演を要約したものを「サイバー空間と警察－サイバー局に期待すること」と改題したうえで掲載し、松尾の講演を「警察活動における AI 導入の可能性と限界」と改題し、補論としてアンドリュー・ファンガーソン著（松尾庄一取りまとめ）の「ビッグデータ警察活動の今後のための提言」をそれぞれ掲載した。

また、令和元年７月３日の警察政策学会シンポジウム『エピソードで語る平成警察史』の際の坂明氏の講演「サイバー脅威への対応」を坂氏の許可を得て『警察政策』第 22 巻より再掲した。併せて、第 2 部「グローバル化とデジタル化への対応」（討論）の抜粋を再掲した。

令和 3 年 10 月　　松尾　庄一

目　次

サイバー空間と警察活動
― サイバー局に期待すること ―

四方　光

複雑社会の典型事例としてのサイバー犯罪

経産省系統の団体 IPA（独立行政法人情報処理推進機構）が発表している「情報セキュリティ 10 大脅威 2021」（スライド参照）は、ある意味、警察統計よりサイバー犯罪の情勢をよく表している。

情報セキュリティ 10 大脅威 2021

https://www.ipa.go.jp/security/vuln/10threats2021.htmlにより講師作成

順位	個人	組織
1位	スマホ決済の不正利用	ランサムウェアによる被害
2位	フィッシングによる個人情報等の詐取	標的型攻撃による機密情報の窃取
3位	ネット上の誹謗・中傷・デマ	テレワーク等のニューノーマルな働き方を狙った攻撃
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃
5位	クレジットカード情報の不正利用	ビジネスメール詐欺による金銭被害
6位	インターネットバンキングの不正利用	内部不正による情報漏えい
7位	インターネット上のサービスからの個人情報の窃取	予期せぬIT基盤の障害に伴う業務停止
8位	偽警告によるインターネット詐欺	インターネット上のサービスへの不正ログイン
9位	不正アプリによるスマートフォン利用者への被害	不注意による情報漏えい等の被害
10位	インターネット上のサービスへの不正ログイン	脆弱性対策情報の公開に伴う悪用増加

第１位　ランサムウェア

ウィルスに感染させてシステムダウンさせ、「回復してもらいたかったら○億円払え」と脅迫するもの。アメリカのサイバー犯罪対策上の脅威でも最も重視されている。

日米とも、警察に報告せずに闇で払っている企業もかなりあるといわれている。払わないと復旧まで相当時間がかかり、業務がストップする。しかもシステムを止める前に機密情報を抜き取り、払わないと機密情報を公開すると脅す。

第２位　標的型攻撃による機密情報の摂取

政府や防衛産業等に対するスパイ活動の一環。知り合いのメールのふりをしてウィルスを感染させる。ターゲットがどんな人と付き合いがあるか把握し、その人だとこんなメールが来そうだと思わせ、偽メールを出す。

第３位　テレワーク等のニューノーマルな働き方を狙った攻撃

テレワーク等で社員が家で使うコンピュータを乗っ取り、そこから会社のコンピュータ・ネットワークに入り込む。

第４位　サプライチェーンの弱点を悪用した攻撃

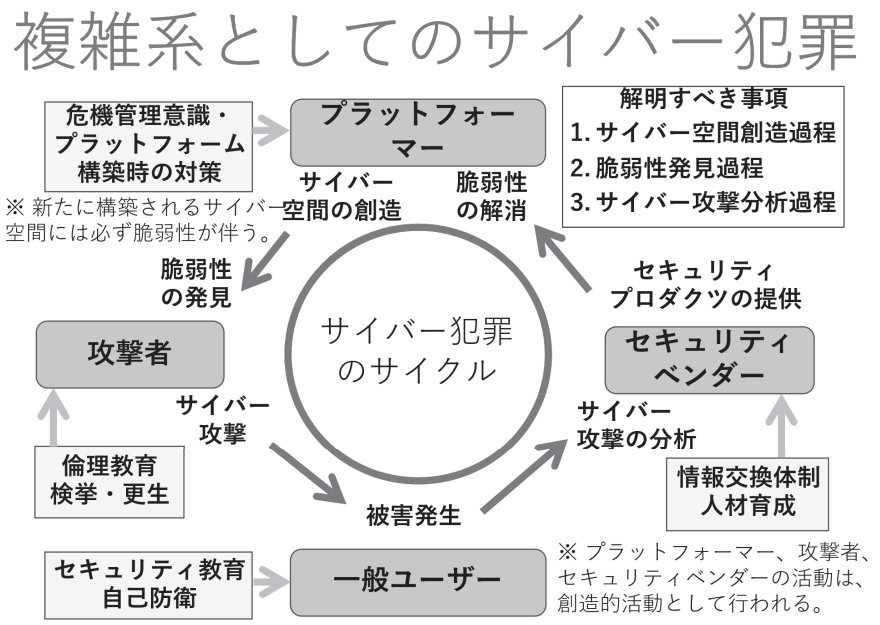
ソフト関係を含めたIT産業等、関係する企業の中でリスク管理の低いところを狙い、ウィルスを感染させ、そこからグループ全体の情報をとっていく。

第5位　ビジネスメール詐欺による金銭被害

取引先のふりをして「先日の案件のカネをこちらの口座に振り込んでほしい」などと申し向け、多額の金額をだまし取る。

サイバー犯罪の特徴

以上のような犯罪は、ビジネスの仕組みやサイバー空間の仕組みなど、何らかのリスクを伴う新たな技術の登場がきっかけになっている。なぜ、サイバー空間では次々と新しい犯罪手口が出てくるのか？　次々と生まれるサイトではリスク管理が甘くても、リスクが十分管理されないまま市場に投入される。犯罪者は目ざとくそれを見つけて儲ける。新しい仕組みが次から次にでてくるのでセキュリティベンダー等により脆弱性が十分担保されない内に、他の脆弱性を攻撃していく仕組みがある。そのプロセスを図化したのが下図。



サイバー犯罪対策における課題

サイバー空間は、産業革命に匹敵するような社会的変化が短期間に次から次へと起こっている、世の中で最も変化の激しい世界。変化への対応が一番大切になってくる。このような変化は企業家や技術者の創造性によって生じるもので、先ほど述べた近代科学が探究する普遍的法則に従うものではない。まさにサイバー犯罪は複雑系のサイバー空間が生んだ犯罪。こういうことを視野に入れながら対策を採っていかなければならないというのが第1の課題。

第2の課題は、刑事法以外の法分野も視野に入れ、なおかつ、サイバー空間は国境を越えるので国際的な枠組みが非常に大切になること。

新たに新設される警察庁のサイバー局には、こういった変化への対応を刑事法や犯罪捜査の分

野において日本社会の中でリードする存在になってもらいたい。また、国際社会での議論に迅速に参加していってもらいたい。

以上については、警察庁は現状でもそれなりにやっているが、外国から見ると今まではちょっと弱かったと思われる点もある。サイバー局ができれば変化への対応のためにどんな法制が必要なのか、その法制のためにはどんな議論があるかを把握し、その議論にもう少し積極的に参加する体制ができていくのではないか。そのためには、サイバー犯罪対策に必要な人材を育成してもらいたい。サイバー犯罪対策に必要なスキルは技術力、捜査力に加え、国際的に対応するために語学力が重要。

どういうことかというと、国際的なサイバー犯罪対策を作るときに参画したり、アメリカ等が主導するサイバー犯罪組織を検挙するための国際的プロジェクトチームに参加したりするためには、語学力が不可欠だから。これまでFBIを中心に何度か行われたプロジェクトチームに日本が呼ばれたことはない。参加するためには、捜査力と技術力だけでなく、語学力も備えた人材が不可欠。現状は、捜査力と技術力を備えた人はそこそこいるが、語学力も備えた人は数人しかいない。こういう人材を育成することで国際的なプロジェクトチームに参加できるようになることを期待する。

インターネット上の越境捜査の課題

問題の所在

インターネットの世界は国境を越えたもの。犯罪者は数か国を通ってから犯罪を行うことが多い。ところが、警察が追いかけようとするといきなり国際捜査共助をやらなければいけなくなり、それがうまくいかずにとん挫することがしょっちゅう起こる。

問題なのは、クラウド・コンピューティングが普及したこと。一般犯罪捜査においても国境を越えなければいけなくなっている。どういうことか。国内犯罪なのに、共謀している被疑者とメールでやり取りしている場合にメールを解明しようとすると、メールの情報が以前は被疑者のパソコンや携帯電話の中にあったものが、クラウド・コンピューティングの時代では、パソコンやスマホは単なる閲覧の窓口に過ぎず、データはクラウド・コンピューティングをやっている通信会社のサーバに入っている。被疑者のパソコンやスマホを押さえるだけでは、データが取れない状況が相当前から始まっている。

越境リモートアクセス

クラウド・コンピューティングに対処するために刑訴法が平成23年に改正され、「リモートアクセス」という捜査手法が認められた（刑訴法99条2項、218条2項）。その内容は、被疑者のパソコンとつながっており、被疑者が使える領域については、被疑者に対し捜索令状が出されていれば、そこの情報を引っ張ってきて複写してもよいというもの。

刑訴法99条2項

差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続してい

る記録媒体であって、当該電子計算機で作成若しくは変更をした電磁的記録又は当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されている電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる。

当時は、通信会社が設置しているサーバは国内にあると考えられていたが、マイクロソフトをはじめクラウド・コンピューティングをやっている会社のほとんどがアメリカの会社でサーバがアメリカやアイルランド等の日本国外にあることが常態となっている。最近は各国の情報はそれぞれの国に置くという動きが出ているので将来は情勢がやや変わるかもしれないが、当面はデータが外国にある状態にある。となると、改正刑訴法の条文が、外国にあるサーバの中のデータに使えるか、アクセス先が外国の場合、捜査権を海外に及ぼすこととなるので、適法な捜査として認められるのかどうかの議論、いわゆる越境リモートアクセスの問題が出てきた。しかも、この議論は、サイバー犯罪以外の一般犯罪にも妥当する。

これについての高等裁判所判決には次のようなものがある。

最初に出た平成 28 年 12 月 7 日の東京高裁判決は、差押えの対象となったパソコンをいったん押収した後で、検証許可状を得て警察署からアクセスした捜査が刑訴法の認める捜査に当たらず外国の主権を侵害する重大な違法があるとして、得られた証拠を証拠排除したが、その判断に際して外国の主権侵害のおそれもあるので採るべき捜査でなかった旨言及したもの。そのため、次の平成 30 年 9 月 11 日の大阪高裁判決が出されるまで実務上リモートアクセスは一時行われなくなったといわれている。

この大阪高裁判決は、外国の主権侵害があるといえないから適法、あるいは、外国の主権侵害があったとしても刑訴法上は違法にならないから適法という判断が出た。

3 つ目の平成 31 年 1 月 15 日の東京高裁判決は、外国の主権侵害があっても刑訴法上は違法となるものではないとの判断をした。

2 番目の大阪高裁の判決の上告審（最決令和 3 年 2 月 1 日）では基本的には OK といってくれたが、かゆいところには手が届いていない。どういうことかというと、弁護側は外国にデータがあるときには一切リモートアクセスは認められないと主張したのに対し、最高裁は「サイバー犯罪に関する条約 32 条に書いてある場合には使える」と判断した。サイバー犯罪に関する条約 32 条の b はリモートアクセスに相当する状況が念頭に置かれており、リモートアクセスの権限を持っている被疑者の任意の同意が得られる場合は OK としている。

サイバー犯罪条約 32 条 b は、他の条約締約国に蔵置されたコンピュータ・データについて、自国の領域内のコンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的かつ任意の同意がある場合には当該締約国の許可なくデータにアクセスできるとしている（上のスライド参照）

かゆいところには手が届いていないと言った理由の一つ目は、この決定は、強制捜査の令状を

サイバー犯罪に関する条約第32条

締約国は、他の締約国の許可なしに、次のことを行うことができる。

a　公に利用可能な蔵置されたコンピュータ・データにアクセスすること（当該データが地理的に所在する場所のいかんを問わない。）

b　自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。

とっていても被疑者の同意があればできるというだけ。実際、この決定後もリモートアクセスをやらない検事もいるらしい。少し訳の分かった検事はリモートアクセス令状を取ったうえで被疑者の同意を得てリモートアクセスをしているようであるが。

この決定のハードルのひとつは、サイバー犯罪に関する条約に加盟していない国の場合どうなるかということ。実際には、情報セキュリティのために（プロバイダですら）どこのサーバにあるのか分からない。実務的には、捜査共助を頼まなければいけない国すら分からない。

二つ目は、この条件に当てはまらないリモートアクセスは適法か否かには触れず、証拠排除まではしなくていいと判断していること。違法だけど証拠排除しないのか、適法なので証拠排除しないのかは言っていない。

越境リモートアクセスは、日本だけでなく世界各国が困っている問題。根底にあるのは、ある国の令状で他国のサーバに入っていいとすると、例えば中国が令状を持って堂々と日本の防衛産業企業のサーバにアクセスすることを認めることになるので、各国とも二の足を踏んでいるわけである。

そこで、私見として、通信事業者のメールサービスの場合と、会社が社員のためにアクセス権限を認めている場合とを区別することを提案したい。前者では事業者は顧客のメールの中味を見られないのだから、自国の令状があれば各国が相互に見ることができるようにすればいい。後者は社員だけでなく会社もアクセス権限を保留している場合が通常なので捜査共助でないと見られないようにする。

越境したデータのもうひとつの取り方

具体的には、警察が例えば日本のマイクロソフトに対して令状を執行し、マイクロソフトの中でデータを国境移転してもらうのである。法律的には日本国内で執行しただけということになり、法務省もできるとしているやり方。

この問題の一つは、通信事業者が国境を越えてデータ移転する時に、データを蔵置している国

の個人情報保護法が厳しく作ってあるとデータを国外に出してはいけないということになる。例えば、EU の場合、GDPR があるので多分出してはいけないとなる。このようなことを調整できるかというのが大きなハードルである。

アメリカは 2019 年クラウド法を作った。これによるとプライバシーの保護が十分である等の一定の要件を満たした国と行政協定を締結した場合には、アメリカのプロバイダから勝手に情報をもらってもよいことになる。つまり、日本の捜査機関が日本国内のプロバイダに対して令状を執行してアメリカの国内からデータ移転してもらっていいという仕組みである（行政協定締結の要件はスライド参照)。

（1）米国クラウド法
行政協定締結の要件 （クラウド法による改正法119章2523条 (b)(1)(B))

（iii）次に掲げるような国際的に認められている人権を保障する義務を保持ないし確約し（commitment）又は尊重していること。

（I）プライバシーに対する専断や不法侵害からの保護

（中略）

(iv)　データを収集、保管、利用及び共有する権限を与える手続やこれらの活動の監視など、本行政協定に基づいてデータを請求する権限を有することとなる外国政府機関を監督する法的権限と手続が明定されていること。

(v)　当該外国政府による電子データの収集と利用に関して、説明責任と適切な透明性を提供する十分な仕組を有していること。

なぜこのような法律を米国が作ったかであるが、アメリカには諸外国から国際捜査共助が山のようにきてパンクしている状況があり、いちいち共助を通さずにプロバイダに対応してもらう仕組みとして法律を作ったとのことである。

現在、アメリカはイギリスとの間で行政協定を結び、2019 年クラウド法の適用を受けている。ヨーロッパはどうするかであるが､先ほど述べた GDPR があるのがハードルになっている。さて、日本はどうするか？日本もこの行政協定を締結して 2019 年クラウド法の適用を受けられるようにしたらどうかというのが私の提案である。

ただし、アメリカと行政協定を結ぶためには次のような国内法担保措置を採らなければならない。

1　相互主義なので、アメリカがアメリカの令状を提示したときには日本国内のプロバイダがデータを提供しなければならない。ところが､最近の個人情報保護法の改正で GDPR に近い条文(外国にある第三者への提供の制限強化）がある。これが妨げにならないか。

2 「捜査機関が保有する個人情報に対する独立監督機関の設置ないし指定」の条件をどうクリアするか。

アメリカとの行政協定締結以前に、捜査機関がとったプライバシーに関する情報の蓄積に対す

る独立機関による管理がいるとの議論が別にある。警察が持つプライバシー情報蓄積の管理が適切かどうかを外部から監督するという議論である。この議論に対して、公安委員会が監督するということでいいとなれば問題はさほど大きくないが、アメリカとの行政協定締結の条件クリアのため個人情報保護委員会の監督がいるとなると別の大きな問題が生じる。

サイバー犯罪対策を有効に進めるためにはほかにも、例えば「ランサムウェア攻撃」を取締るために日本でも刑訴法の改正が必要ではないかなどの議論があるが、時間の関係で省略する。

質疑応答

○サイバー空間の定義

かっちりした定義はなく、割とざくっと考えられている。実空間だと犯罪者と被害者が交錯する場所は公共空間であることが普通。そこでの管理を安全確保のために警察がやることはそれなりにやりやすかったのではないか。ところがサイバー空間では、プラットフォーマ等の民間企業が提供している。それが国境を越えている。国、自治体が管理しにくいのがサイバー空間。なおかつ、人間が考えたものであり、新しいものが作られていく空間であり、政府機関が管理しにくい空間であることがサイバー空間の特質と考えている。

プラットフォーマとは、不特定多数の人が情報交換なりコミュニケーションのために使うようなサービスを構築して提供する事業者のこと。四方としては、プロバイダもプラットフォーマに入るものとして議論している。

○リモートアクセスとプロバイダによるデータ越境移転との関係

論者の中には、米国クラウド法での行政協定ができればリモートアクセスはいらないのではないかという人もいる。四方としては、大部分はカバーできると思うが、問題なのは誘拐など監禁場所等をすぐに解明したい等、緊急性が非常に高い場合には、プロバイダによるデータ越境移転では間に合わないのではないかと思う。なぜかというと、プロバイダに頼むと最低でも数日かかるからである。だから、緊急性が高い時にリモートアクセスをやってもいいという議論は国際的にもある。

関連する問題は、リモートアクセスの主体は捜査機関だが、ID、パスワードがないと入れない問題がある。つまり、被疑者が言わないとリモートアクセスは使えない仕組みである。最初の東京高裁判決の事案は、現場ではID、パスワードが分からなかったので、（パソコンを）警察署に持ち帰り、検証令状でやったが刑訴法では認められないとして証拠排除された。

○サイバー局新設にあたっての課題

1　サイバー局の所掌事務の対象を定義する際には、サイバー空間での安全確保のような抽象的なものにせず、一定のサイバー犯罪類型を定義して、その捜査なり、防犯なりに関することと定義するのではないか。

2　都道府県警察の枠を越える権限を警察庁に付与することについては、両者がウィンウィンの関係になるように都道府県警察ではやりたくない、やりにくいような類型の犯罪を中心にやっていくのではないか。

サイバー局が動くのは、サイバーテロやサイバーインテリジェンスのような高度な犯罪になるのではないか。これまでやってきたようなサイバー犯罪は都道府県警察が主体となって捜査するというような切り分けになるのではないか。

理論的には警察法の根本に関わる大改正なので、争点になると思うが、これまで述べたように

サイバー空間の状況が特別なので、一般犯罪とは別の仕組みが必要だというのは説得力を持つと思う。

とはいえ、都道府県警察相互の関係、警察庁と都道府県警察との連携等、警察法で手を入れないとならないところは山ほどでてくるのではないか。また、刑訴法でも、例えば、令状請求の方法、請求先裁判所等、新たに規定しなければいけないことも多くあると推測する。

3　サイバーブリング（ネット上のいじめ）やネット上の中傷などにどう取り組むかについては、犯罪に至らないあるいは形式的には名誉棄損にあたるような事案については、警察はサイバー空間に限らず人身安全関連事案は別にして消極的だが、サイバー局新設の際に、サイバーブリング等を警察の責務として取り上げることもあるかもしれない。

ただし、都道府県警察との関係では、サイバーブリング等の被害者が所在する都道府県警察が中心となって対応していくのではないか。

犯罪にならない事案をどうするのかは、警察が取り込むのではなく、これまでどおり「相談」として都道府県警察が担当して、多機関連携を推進する。また、プラットフォーマ企業がガバナンスで排除するのも一案であろう。

多機関連携については、法務省の人権擁護局のような小さな組織で対応できるかは疑問なので、例えば、知事部局の人権擁護の部署がやるというようなことも考えなければならないのかなと思う。

○サイバー局新設と捜査権限拡大

読売新聞で「捜査権限の拡大についても本格的な議論を始める必要がある」との講演者のコメントについて、研究途上ではあるが、以下のように考えている。

サイバー犯罪の情勢では詳しく述べなかったが、ランサムウェアに加え、サイバー犯罪のマルウェア等のツールを交換したりする闇サイトであるダークウェブ、それにボットネットが大きな脅威になっている。

ボットネットとは、企業や個人のコンピュータをウィルスに感染させて「部下」として使って、ウィルス、迷惑メール、フィッシングメール等を撒くなどのネットワークのことである。

これらをつぶす捜査を日本で行うためには、現在の法制ではしんどいかなと思われるので、次のようなことを考えている。

第１に、特殊な通信傍受をやってボットネットの中間管理層のC&Cサーバを見つけ、全体像を探る手法があるので、それを行うために通信傍受法を改正してサイバー犯罪を対象にする。

第２に、ダークウェブでの潜入捜査をやれるようにする。

第３に、捜査機関が犯罪者側にポリスウェアというウィルスを仕掛けることができる新しい令状の仕組みを作る。

サイバー局では、このような手法をできるようにする取組をまずやってもらいたい。警察庁はさることながら、法務省では、このような捜査手法に関する専門の担当部署がないのではないか。最高検には最近サイバー係ができたと聞いているが。法務省の尻たたきをし、諸外国と組んでオ

ペレーションをやるにはこんな権限がいるんですというようなことをサイバー局から発信してもらいたい。

○　サイバーセキュリティにおける自衛隊との連携

（質問者の発言の要旨）

「国家レベルのサイバーセキュリティは、ハイブリッド・ウォーという言葉があるように有事と平時の切れ目がない。そこで、自衛隊からサイバーセキュリティとして民間企業や自治体等に独自のルートで働きかけるということになれば、相手方に迷惑になる。警察と自衛隊が手を携えて働きかける必要がある。」

「そもそも国家レベルのサイバーセキュリティは、内閣官房で考えるべきだが、その司令塔のNISC（内閣サイバーセキュリティ センター）は機能しているか。」

ご指摘のとおり、諸外国では、情報セキュリティにおいては、捜査機関だけでなく、軍と情報機関が重要な役割を果たしている。日本では、これを刑事司法だけで対処しなければならない。

諸外国では軍も含めた情報機関の諜報活動には、情報収集活動だけでなく破壊活動も含まれている。その発想で、戦時だけでなく平常時にもサイバー攻撃が行われている。

自衛隊は、情報セキュリティに関する能力は、日本では高い方だが、憲法上の問題もあって従来自衛隊のシステムを守ることだけやってきた。防衛大綱が改正されて、日本の情報セキュリティを守る任務も付与されたが、そのための法的武器が与えられていないのではないか。

NISC は、かつては経済産業省＋旧郵政省と警察庁＋防衛省の対立があったとされ、主導権が前者にあったので守りのセキュリティしか関心がなかったが、近年はさすがに変わって、連携はある程度とれているように聞いている。

以上

警察活動における AI 導入の可能性と限界

松尾　庄一

はじめに

コンピュータの分野にはコンピューティングという言葉がある。四方教授の講演でもクラウド・コンピューティングの言葉が出てきたように、コンピュータ科学・工学では一般的に使われている。それを分かりやすく定義するのは難しいが、本講演では「コンピュータを用いた知的活動」という意味で用いたい。

「コンピュータを用いた知的活動」には、計算、分類、マッチングのような伝統的な機能に加え、最近、AI（人工知能）の機能として注目されている、認知、判断、統御も含めることとしたい。

以下、このようなコンピューティング、とりわけ AI を警察活動に積極的に導入できないかとの立場で検討してみたい。その際、警察活動の類型に分けて検討することとする。警察活動の類型化にあたっては色々な切り口があろうかと思うが、現場で重要な地位を占める職務質問に着目して類型化したい。

我が国の職務質問は、現場での警察官の観察・調査により得た情報、及び組織で共有する情報の活用によって容疑者の疑いを解明して犯罪事実を形作ることで、「何らかの犯罪を犯し…ていると疑うに足りる相当な理由」（以下「不審点」）のある者が対象となる。

不審点があるか否かは警察官の主観的判断だけでなく、「異常な挙動その他周囲の事情から合理的に判断」できる客観的根拠が必要である。なお、通常逮捕状を請求する際に求められる「相当な理由」よりも低い程度の「一応の合理性」があればよいとされる[1]。

AI を導入するといっても一律ではなく、警察活動の類型によって違えなければならないが、本講演では警察活動を「現場での警察官の観察･調査により得た情報を活用する警察活動」と「組織で共有する情報を活用する警察活動」の二つにとりあえず分け、それぞれ AI 導入の可能性を検討したい。

Ⅰ　現場での観察・調査により得た情報の活用

職務質問を中心とする警察官の現場活動[2]には､既にＮシステムとして AI が導入されているが、さらに拡大できないかが最初の問題意識である。

実際、警察官の疑いの多くは容疑者の「異常な挙動」で惹起される。

「異常な挙動」の例としては、①血痕のついた着衣を着ていること、②警察官から誰何され、または警察官の姿を見て逃げ出すこと、③証拠と思われるものを遺棄したり、破棄したりすること、④手配されている人物の年齢、身長、容貌等に似ていること、⑤着衣のポケットが不自然に膨らんでいることなどが挙げられる。

そして、警察官は次のようにカテゴライズされた推理を行う。

「血痕がついた着衣を着ているから、何らかの犯罪の犯人だろう」､「警ら中の警察官を見て横

道に入ったから、なにか犯罪に関係しているのだろう」、「パトカーを見て何かを投げ捨てたから禁制品を所持していただろう」、「付近で起きた事件で手配された犯人の特徴に当てはまるから犯人だろう」、「ポケットが膨らんでいるから凶器をもっているだろう」。

つまり、ある人物が疑わしいカテゴリー（集団）に含まれることを不審点にしている。このカテゴライズ化を AI によってできないかとの発想に進む。

適用可能な AI 技術

不審点をカテゴライズ化して不審者を発見する推論プロセスである abduction（仮説形成）のアルゴリズムが適用可能である。なお、abduction は一般的にヒューリスティクスといわれるものと似た働きをする。ヒューリスティクスとは、「確実とは言えないが多分こういうことだろう」という意味である。

実際に、開発段階であるが、カメラ画像を活用して「立入禁止地域への侵入」、「不審な物品の置き去り」等を検知するシステムがある。

Ⅱ　組織で共有する情報の活用

職務質問を実効あらしめるには、それを裏から支えるシステムが必要である。犯歴がリアルタイムで分かるシステムは、例えば、危険物であるナイフを取り上げる活動に際しても、対象者の危険性を判断する際の有力な材料になる。職務質問で疑いを強めるデータベースとして、犯歴の他に、指名手配者、車両の各データベース等が活用されている。なお、職務質問で疑いを強めるには、必ずしもシステム化されていないが、警察活動の蓄積で構築された、例えば、質問の現場が覚醒剤事犯や売春事犯の検挙例の多いホテル密集地帯、覚醒剤密売所等の情報が活用されている。

職務質問に直接関連はしないが、主として捜査や鑑識で活用される、組織で共有される情報データベースには、指紋掌紋、足跡、顔写真、手口資料等がある。

組織で共有する情報の AI 化について次のような問題意識を持つ。①犯歴、指名手配者、車両の各データベース等について、AI によってニックネームや不完全ナンバーその他の断片情報で検索できるようにできないか、②明文化されていない経験知をデータベース化できないか、③指紋掌紋の痕跡解析（鑑識）には、AI を活用した指紋自動識別システム（AFIS）が導入されているが、これ以外の分野、例えば、顔認証を用いた写真面割等に拡大できないか、④さらに、手口捜査を一歩進め、AI を活用した犯人割出し・犯行予測の犯罪プロフィリングができないか。

適用可能な AI 技術

ひと昔前には想像もできなかった方法でビッグデータの流れを仕分けることができるビッグデータ分析が適用可能である。これにより圧倒的な情報から思いもよらない隠れたパターンや見通しひらめきを導き出すことができる。

Ⅲ　行動や思考の痕跡の活用

以上二つの類型は、既存の方法で収集された情報を基にした活動類型であるが、現代社会は、

多くの人々が無自覚的にしかも克明に自らの行動や思考の痕跡をネットワークの上に残している。また、AIにセンサデバイス等が付属したコンピューティングにより人間の五感では感知できない「事実」を感知できる。これらを警察活動に活用できないかというのが、第3の問題意識である。

なお、この場合、特定の個人を丸裸にするためのデータ分析は、厳しく制限されるべきで、オープンになった情報、あるいはオープンな状況での情報を収集し、個人を特定せずに分析するものとする。オープンな情報は、不完全で断片的な記録や履歴に過ぎなくても、何万、何十万と集まることで、物象化され、統計的な価値を持ち、実に多くのことを知ることができる。

このように物象化されたり可視化されたりした人の行動や思考の痕跡を警察活動に活かせないかという発想に進む。

適用可能なAI技術

一つは、データに基づく見通しや未来の出来事の予想を行う予測分析（predictionを計測する機能）である。具体的には、ETC2.0 プローブデータやカメラ情報等を活用した道路管理や交通管理が既に一部行われているが、一歩進めて交通管制やエリア警備等の警察活動に活用する。

もう一つは、何らかの可能性がある痕跡を収集し、現実そのものを計算する機械学習アルゴリズムである。これは、現実環境にセンサリングデバイスが埋め込まれることで、様々な状況がデジタル処理が可能になり、すべてをデジタルデータとして収集するテクノロジーである。つまり、サイバー空間に現実空間と同じもの（これはデジタルツインと呼ばれる）を作り、そこでシミュレーション等のコンピューティングを行う。

デジタルツインを対象にして大規模プラントの故障を予知する故障予知システムが実用化されている。これは、プラントに埋め込まれた10万以上のセンサーによりリアルタイムでデータを集め、分析して異常値を検出することで故障を事前に検知する。このシステムの優れた点は、異常値の基準になる正常値をAIが自動で作出することである。

また、デジタルツインといえば、自動運転技術は、AIが現実の道路空間をデジタルツインとしてサイバー空間に作り上げ、そこでの操作で現実の自動車の動きを統御するものといえよう。このようにAIは複雑な現実世界の出来事をコントロールできる。

アメリカでのAIを活用した警察活動

AIを用いた警察活動は、アメリカが我が国よりはるかに進んでおり、各種アルゴリズムを積極的に開発して実装化しているのは、事実である。この理由としては、AIと並走するGAFA等のデジタル・プラットフォーム構築がアメリカの方が進んでいること、また、この後紹介する警察活動で活用されるAI技術がほとんど民間で開発されたものの購入か、民間企業との共同開発であることに加え、警察活動の概念について、我が国よりもコンピューティングに親和的であることが挙げられよう。

その一つの例として、アメリカの職務質問（stop and frisk）について、『監視大国アメリカ』（2018年）の著者のアンドリュー・ファーガソン教授は、次のように述べている[3]。

警察官の職務質問は、特定の犯罪が行われたことを証明（個別化）するものではない。職務質問での警察官の判断は、未来の行動を予想するために過去の経験に基づく一般化と直感を用いていることがわかる。警察間の判断は実際には過去の経験に基づく一般化を反映しているだけ。言い換えると、個々の容疑は実際には一般化と直感という認知的近道（ヒューリスティクス）を利用している。（一部の表現は講演者が改めた。）

これは、警察官職務執行法の条文を基にした「職務質問」の我が国の伝統的な解説に比べると論理的で、その意味でコンピューティングと親和的である。

以上を前提にして、『監視大国アメリカ』からアメリカにおける AI を活用した警察活動の例をいくつか紹介することにする。

1　不審な行動を検知する

デジタル警報システム（Digital Alert System）は、例えば、①通りに不審な荷物を残して立ち去る行為、②街角で繰り返し、頻繁に何かを手渡しするような行動、③誰かに素早く近づいてから走り去る行為を検知して直ちにアラートを発令する[4]。

2　犯罪発生場所を予測する

(1) プレドポル PredPol（Predictive Policing の略）

UCLA のジェフリー・ブランティンガム教授が開発したもので、特定の場所における犯罪、主に住宅侵入窃盗、自動車盗、車上狙いを予測するため、本来は地震の余震を推測するために開発された反復近接アルゴリズムを用いて犯罪が同様のパターンに沿っていることを突き止めた。つまり、犯罪は波紋のように伝染するものとして視覚化が可能であり、確認されたパターンを地図に示して予測できるというもの[5]。

ロサンジェルス市警本部長ウィリアム・ブラットン[6]は、前任地のニューヨーク市警本部長当時に導入した CompStat を持ち込み、またブランティンガム教授が開発したプレドポルの実験にゴーサインを出し、2011 年に一応結果が出るとブランティンガムらはすぐに商業化した。基本的には、入力データ変数を犯罪の種類、場所、犯罪発生時間に限り、データに基づいて日々変化する極めて小さな地理的範囲（約 150 メートル四方）で予測している。

わが国では、京都府警察が一部導入している。

(2) Risk Terrain Modeling（地区特性分析）

これは、リスクを高める要因を見極めようとする。

環境犯罪学を前提として、駅、ショッピングモール、駐車場等、都市環境要因と犯罪との関係を分析し、犯罪を引き寄せる場所（環境）、犯罪の起きやすい地域等、犯罪を誘発する可能性がある環境要因を特定することでリスクエリアを特定する。

Risk Terrain Modeling（地区特性分析）の手法を用いて実際に環境犯罪リスクを特定し、警察と行政との連携によってリスクを改善するための具体的な解決策が立てられている。

『警察政策』第 23 巻の野貴泰（の・たかひろ）氏著『地理的犯罪分析に関する考察』に Risk Terrain Modeling（地区特性分析）の解説が載っている。

3 「容疑者」を「割り出す」

人物予測型アルゴリズムは、犯罪を行う人物を名指しで予測するのではないが、ほかの人々と比べてそのような行動をとる可能性が高くなるリスク要因を分析してリスクのある人物を割出す。

シカゴ警察のヒートリスト（戦略的対象者リスト）は、ビッグデータテクノロジーを用いて銃撃事件の被害者になる可能性の高い人物と暴力事件を起こす可能性の高い人物をリストアップする。刑事が社会福祉士と地域社会の代表を伴って銃撃事件の被害者あるいは加害者になると予測される人物の住居を訪れ、本人及び家族に「今すぐ人生の方向転換をしなければ、未来は暗いばかりか命さえ奪われる」と告げる[7]。

4 メタデータを活用した捜査

メタデータはビッグデータの産物であり、パワフルなコンピュータが一日にアメリカを出たり入ったりする30億件の通話を高速処理している。また、メタデータはインターネットの利用、ソーシャルメディアの投稿、デジタル写真等今日行われているデジタル活動のほぼすべてから生成されている。

アメリカにおいては、電話に関するメタデータは、日常的に、かつ、行政令状により合法的に捜査に活用されている。電話に関するメタデータは、通話の内容は含まず、通話の番号、相手先、時間、日付、位置の情報等である。

これにより、例えば、テロリスト容疑者の電話番号から、直接通話した電話番号が判明するだけでなく、判明した電話番号と通話した電話番号を解明し、さらにそれと通話した電話番号を解明する。このビッグデータをAIを用いて分析することで、ある脅威が疑われる人々の間の「隠れた関係性」を明らかにできる[8]。

AIを総合的に活用した事例

アメリカでは、AI技術を個別に警察活動に活用するだけでなく、いくつかのシステムを組み合わせて活用する事例もある。次に代表的な二つの事例を紹介する。

1 ロサンジェルス警察の「即時分析緊急対応システム」

これは、ロサンジェルス警察がパランティア社と共同開発したもので、警察が保有する無数のデータを集約、分析し、普通なら見えない手がかりを導き出す。

サブシステムとして、「統合データシステム」がある。これは、署内の端末からある人物に関する車両、住宅、携帯電話、電子メールアドレス、位置、友人、仲間、家族、あるいは雇用状態を検索できる。

また、犯罪組織構成員、令状の出ている人物、その他捜査対象となりうる人物のデータベースとリンクすることで、特定の犯罪組織全員の住所や、既に知られている複数の薬物売人の行動パターンを知ることができる。

例えば、刑事がファーストネームと身体的特徴を入力すると、データベースを検索して容疑者候補リストを提示する。容疑者候補リストには、既に判明している年齢、特徴、住所、所属犯罪

組織、所有車両等が記載されている。刑事は、他の情報と照合して容疑者を割り出す。

さらに、サブシステムである「自動車ナンバー自動読み取りシステム」（N システム）に容疑者の保有車両のナンバーを入力すれば、たちどころに過去のある一定期間のロサンジェルス市内の走行経路が判明する。

緊急通報（911 番通報）が中央指令室に入ってくると、911 番での通報情報をデジタルマップに貼り付ける。中央指令室にはビッグデータネットワークが横たわっており、ネットワーク化されたシステムによって警察はより多くのデータを桁違いに高速に処理する。具体的には、中央指令室は市内に張り巡らせたモニターカメラにより、状況をモニターしながら、現場に派遣した警察官に携帯端末を通じて、当該地区の犯罪情勢、過去の銃撃事件、縄張りにしている犯罪組織、モニターカメラで撮影された現場付近の写真等、必要な情報を提供する。

日常的には、地域警察官は出勤すると、サブシステムである「犯罪予測システム」で分析された、その日の「犯罪予報」が記されたデジタルマップを受け取り、それを参考にしながらパトロールルートを決める[9]。

2　管内警戒システム (Domain Awareness System)

これはニューヨーク警察がマイクロソフト社と共同開発したもので、シティワイドのセンサーデバイス、データベース、ソフトウエア、インフラストラクチャからなるネットワークで、そこでの分析、個別の事案の関連情報等を警察官の携帯端末（約 35,000 台）やデスクトップに伝えることで警察活動に資する。

マンハッタン南端地区の公共空間をリアルタイムでモニターするために、約 9,000 台の CCTV カメラを配置している。カメラ映像は「デジタル警報システム」につながり、不審行動を発見する。

また、約 500 基の N システムが配置されマンハッタン南端地区に入ってくるすべての自動車を記録し、陸運局の車両情報、警察の指名手配者リスト、テロリストデータベースとリンクし、必要な情報が抽出できる。

「デジタル警報システム」で録画された映像は、位置、時間、日付でタグ付けされており、一度の検索で条件に一致する人物の静止画を引き出すことができる。また、容疑者の動きを追跡するために、「ニューヨーク証券取引所付近にいた赤いシャツを着ている男」等の文章を入力することによっても検索できる。

警察は現場から 150 メートル以内にあるカメラ画像を調べて、容疑者が自動車を降りたところまでさかのぼって再生できる。発見された容疑自動車は監視カメラ網に入ったところまで遡って追跡され、N システムから所有者情報あるいは盗難車両情報が引き出される。同様に逃走用の自動車も追跡され、分析される。

地域内の 1 カ月前までの映像が保存されているために、事件現場付近の過去の映像に容疑者が映っていないか分析できる。

さらに「ShotSpotter System」の高感度マイクが銃声を捉えるや否や、警察官を現場に出動させる[10]。

アメリカでのAIを活用した警察活動での問題点

このように警察の立場からは夢のようなシステムが整備されているように見えるが、もちろん問題点がないわけではない。むしろ、『監視大国アメリカ』を読むと問題点だらけとも思える。講演者なりに問題点を整理してみたい。

1　犯人を割り出す、犯行を予測するといっても、いずれも不確実性を免れないこと。これは、AIが「確実とは言えないが多分こういうことだろう」というabductionアルゴリズムを用いていることから必然的に生じる問題点である。今後、機械学習が進んで賢いAIができたとしても、精度が上がるだけである。つまり、AIは、相関関係は特定できても因果関係を正しく判断できないのである。

以上のAIの限界については、常に認識しておかなければならない。

2　予測データが示すのは問題であって解決策ではないこと。したがって、犯罪の根底にある問題と取り組む手段を伴わないAIを活用した警察活動だけでは、犯罪は完全には防止できないことになる。犯罪の根底にある社会経済問題に対処する機関・団体などと多機関連携することが必要である。

3　AIによる分析の基幹である統計分析によって真実が発見できるのはシステムが長期に安定している場合に限られること。システム自身が内発的に変化し、システムの変化の結果が偶然によって影響を受ける世界では論理実証主義の基礎となっている統計的検証がもつ意義は限られたものになる[11]。

関連して、容疑者を割り出したり、犯行場所を予測するアルゴリズムには時間的限界があること。モデルが出す予測は設定された期間によってその正確性は変化する。期間を長くとればほぼすべての予測が当たる。また、使用可能な予測を出すためには継続して最新データを収集する必要がある。特に手口については、容疑者が年をとることで、時とともに習慣が変わる可能性を認識する必要がある[12]。

4　シカゴ警察のヒートリストのような予測テクノロジーは、人種的偏見のおそれ、透明性の欠如、データの誤り、そして憲法による保護の歪曲の懸念があること。警察官が具体的な挙動ではなく、リストの対象者であるがゆえに質問することになれば、「観察と経験に基づく憲法上十分な情報を有する」という職務質問の合憲性のロジックを否定することになるだけなく、その活動からは人種的偏見と透明性の問題が生じる。

関連して、膨大な人的ネットワークから「隠れた関係性」を明らかにする、メタデータを活用した捜査は、対象となる犯罪とは無関係の、慈善事業活動への参加、政治への寄付、活動家団体との関係、あるいは雇用、友人関係等を明らかにする問題点がある。

また、電話メタデータの分析からは通話内容を調べないと得られなかったような情報が明らかになることがある。例として、架電先がアルコール、薬物、ギャンブルのような中毒に苦しむ人々のための相談電話であった場合、架けた人がこれらの中毒者であったことが推測できる[13]。

5　情報源、信頼性、検証可能性についてわからないままデータを取得し、保存すると、間違い

だらけのデータベースができあがってしまうおそれがあること。その結果がもたらす弊害は、警察への信頼を大きく損なうことになるから、個人情報を活用した警察活動では警察は情報を審査する構造を持たなければならない。情報機関は入ってくる情報を検討するために何層もの情報分析担当者を置いている[14]。

そのほか、警察官の安全を含む治安維持と住民のプライバシーの比較衡量が極めて難しいこと、住民側がプライバシーを守る自衛手段 Privacy Protects を採る可能性があることを指摘している。

ソフトターゲットテロ防止のためのエリア警備支援システム（構想）

我が国では、いくつかの AI 技術を組み合わせて活用する事例は、管見の限りではないが、講演者が東京オリ・パラでのソフトターゲットテロ防止のために考案した「エリア警備支援システム（構想）」を紹介することで、警察活動における AI 導入の可能性の議論の参考に供したい。

ソフトターゲットのテロの予防策は、オリンピックエリア等の対象地域に警戒監視のための警察官を多数配置して、テロ容疑者ないしは不審な行動を行う者（以下、「不審者」という。）を発見し、職務質問を行い、所要の措置をとることが基本である。そこで、警察官による不審者発見・追跡の警備体制を補完するため、不審者の発見・追跡を支援する「エリア警備支援システム（構想）」を考案した。その概略の仕組みは以下のとおりである。

・警戒エリアの要所に設置された多数のカメラをネットワークで接続し、オペレーションセンターに付属するデータセンターで集約して処理する。
・データセンターのサーバには、カメラの画像を処理する「不審者発見サブシステム」が組み込まれており、立入禁止地域への侵入、不審な物品の置き去り、うろつき・下見行動等を行う不審者を検知する。
・また、「ウォッチリスト照合サブシステム」が組み込まれており、テロ容疑者を含む指名手配者や「不審者発見サブシステム」で検知された不審者を発見（検知）する。

他方、現実空間では、以下の取組みが行われる。

・不審者を検知した場合、オペレーションセンターに常駐する指令員にシステムがアラートを発する
・画面の切替え、ポップアップ、映像データの記録、過去の映像データの呼出しなど、必要な種々の映像データ操作を行うための VMS「ビデオ管理システム」機能を使い、指令員は現場の警察官等に適切な指示をする。その際、不審者に関する画像を伝送する携帯端末等を活用する。
・また、「ウォッチリスト照合サブシステム」で発見（検知）した不審者を、エリア要所に設置されたカメラで追跡する。

このシステムでは、現場の警察官が的確に対応できるような指示が不可欠である。平素より司令員に対して教養・訓練を行うとともに、必要に応じて携帯端末等に画像を的確に伝送する。

検討の過程で、見当たり捜査を AI でやらせることはできないかとの問いが立てられた。結論として、「可能だが、そのためには以下のような条件をクリアする必要がある」との回答がなさ

れた。

・システムの性能を十分発揮させるために、夜間等の照明に加え、解像度やレンズ等の適切なカメラを、適切な地点に配備する必要がある。

・エリア要所に車載型カメラを、また、人流制御用レーンの出口に可搬型カメラを設置することなどによってできるだけ顔の正面画像が撮影できるようにする。

・カメラの向きやズーム量等を適切に制御する警察官の技量の向上の教養・訓練を行う。

なお、見当たり捜査とは、指名手配されている被疑者の写真を頭に叩き込み、通行者の顔の特徴と比較し、指名手配被疑者を発見する手法。どのような特徴で比較するかは、いくつかの「流派」がある。

ポリスマン・インテリジェンス（PI）

以上、アメリカの事例を参照しながら述べたように、AI を活用した警察活動は実際上かなり制約がある。その上、目まぐるしく変化する社会で、人の悪意と偶然とで生じる事案を対象とする警察活動一般を対象にするには、AI は理論上、経済上及び社会受容上なじみにくい面がある。

理論上の問題点は、前述のとおり、犯罪者の悪意によって、また、偶然によって影響を受ける現実空間では AI を活用した警察活動の意義は限られたものになること。つまり、ダイナミックに変化する対象に対しては、最終的には生身の警察官に頼らざるをえないということである。

経済上の問題点は、仮に、ニューヨーク警察の「管内警戒システム」、ロサンジェルス警察の「即時分析緊急対応システム」や「エリア警備支援システム（構想）」を実現しようとすれば莫大な費用がかかること。

「管内警戒システム」構築に 3,000 万ドルから 4,000 万ドル、「即時分析緊急対応システム」構築には建物を含め 1 億 7,000 万ドルを要した。これにシステムの維持費、システムをフルでかつ正常に機能させるためのフルタイムサポートに要する費用、ビッグデータ技術の運用と維持に従事する犯罪分析官、データ技術者等の人件費、サイバーセキュリティに要する費用がかかる[15]。これらを考えると、つい「機械の目」ではなく「警察官の目」に頼ってしまうことになる。

社会受容上の問題点は、我が国では、公共空間といえども、警察が「機械の目」を使って「監視」することについての抵抗感が強いこと。なぜ必要なのかを大方の国民に理解してもらうために制度面での検討を含めて努力しなければならない。

となると、「警察活動への AI の導入」については、AI を総合的に活用したシステムは将来の検討課題とし、当面は、「現場での警察官の観察・調査により得た情報活用」、「組織で共有する情報の活用」、「行動や思考の痕跡の活用」で述べた適用可能な AI 技術の導入に重点を置くことになろう。

その間の空白領域での警察活動はもとより、上述の「理論上の問題」から、今後とも多くの領域で警察官の能力に頼らざるを得ないことになる。

警察官の能力、とりわけ知力について、講演者は AI に対抗するものとして「ポリスマン・インテリジェンス」（PI）に着目している[16]。

PIとは、本講演においては、警察官の現場の知恵からなる熟練の技と定義することにする。

現場の知恵の活用といえば、「現場での警察官の観察・調査により得た情報…の活用によって容疑者の疑いを解明して犯罪事実を形作る」職務質問は、その典型的なものであろう。これは、学問的には、文化人類学や社会学で使われていたエスノグラフィ（Ethnography）という手法に似ている。エスノグラフィは、フィールドで生起する現象をフィールドへの参与・観察により記述し、そこから反復して出現する現象のパターンを発見、蓄積し、それらをモデル化するものである。警察においても経験的に行われてきたエスノグラフィを明示的に警察活動のツールのひとつにするべきであろう[17]。

以下、詳説する。

知恵には、文字や音声で表すことのできる明白知とそれが難しい暗黙知がある。PIはほとんどが暗黙知である。他方、警察活動は、PIによって得られた有望な推理（仮説形成作業）があってこそ成功する分野が広い。ただし、PIについては、生まれつき備わった人は少ない。したがって、その重要性の認識を踏まえて組織的な学習を推進する必要がある。

具体的には、以下のとおりである。

まず、暗黙知の外面化。これは、他のメンバーが習得するために、熟練者が暗黙知を言語や態度で表すことである。熟練者自らが自分の言葉で語りかける、勤務を通じて態度で教えるのが効果的である。

次に、暗黙知の内面化。これは、外面化された暗黙知を自分のものにする（腹に落とす）ことである。最も効果的な方法は、実務に即したOJTで熟練者の技を見よう見まねでやってみて体で覚えること。また、熟練者の経験談を聞いたり、文書にしたものを読んだりする追体験、さらにシミュレーションや訓練を通じて仮想体験する疑似体験も効果がある。

統計分析の高度化 - 警察の情報管理の高度化に向けて

これまで、主として警察活動へのAIの活用の可能性について論じてきたが、警察活動で用いられるコンピューティングには、AI技術の他に統計分析がある。

これについてもアメリカの方が進んでいる。ニューヨーク警察等には各種統計を用いた犯罪分析に基づく犯罪抑止目標を達成するために使われるシステム「コンプスタットCompStat」がある。これについては、一時期、運用において短期間の実績を競い合う件数主義になってしまい、結局タフポリシー（厳罰主義）につながったとの評価があった。しかし、タイムリーな地域分析機能や、また、犯罪情勢の短期の変化ではなく、長期の変化に着目すれば、緻密で統計変化を踏まえた犯罪対策のアプローチになると思われる。

翻って我が国では、極論すれば、対前年比の分析に終始し、犯罪等の実態が十分把握できていないきらいがある。また、現在行われている統計的手法は、一般にデータをざっくりまとめ、わかりやすい表現ができるという長所がある一方で、多数の特徴だけを残し、少数の特徴を捨てる（データの複雑な特徴を切り捨てる）ためにモデルの精度はそれほど高くないといわれている。

そこで、講演の締めくくりとして統計分析の高度化、ひいては警察の情報管理の高度化に向け

て 2 点提案したい。

1　コンピューティングによる統計分析の高度化

現在は、プログラムが利用者に入力をうながし、利用者は文字列の形式で入力を与え、プログラムはそれを読んで処理を行う、というプログラム操作が必要であるが、現場で必要な統計表をオンデマンドで作成できるようにするため、ユーザーの手元で使えるインタフェースを整備する。

また、統計分析に当たり、コード化されたデータだけでなく、いわゆる自由記述も参照できるようにしたり、また、「あいまい検索」もできるように、AI を活用した機械学習統計分析を導入する。

これにより、きめの細かい結果出力が期待できる。特に、犯罪プロファイリングは手口原紙の自由記述や犯罪統計原紙の項目を参照することで「思いもよらない」結果が期待できると思われる。

2　統計分析の可視化

現在行われている統計分析の入り口及び出口を「可視化」する。

まず、「入口」。メニュー、ダイアログボックス、アイコンなどのオブジェクトをマウスなどで指定することによりプログラムの操作を行う GUI（グラフィカル・ユーザ・インタフェース）を使うことで、マウスのクリックなどの利用者が与えた指令に応じて、例えば、自己の管内の、何層にもわたりクロスした犯罪統計表を作出することができるようになる。

次に、「出口」。見えないものを見える形に加工したり、全体傾向をわかりやすく表現したりする。例としては、①プローブによる急ブレーキのデータ（減速度、緯度経度、方位、発生日時等）の数表（数字の羅列）から、地図上に急ブレーキ多発個所を重ねる、②犯罪発生データを商業地域、住宅地域、工業地域等を示す用途地域マップに重ねることで、商業地域、住宅地域、工業地域別の犯罪統計が出力される。

こうすることで、①ではダイナミックな交通管理が行える可能性がある。また、②では、「ざっくり」した犯罪情勢の分析から、よりきめの細かい、かつ、視覚化された分析ができるようになる。

以上

1　古谷洋一編著『注釈警職法』P58

2　職務質問をめぐる警察活動について、中野目善則教授は『サイバー犯罪の捜査と捜査権の及ぶ範囲』で「現実の社会においては、不審事由が外観から判明すれば職務質問の対象となる場合もある。外観上不審事由の有無が判明しない場合でも、不審の有無を確認するための自動車検問や、チェックポイントを設けた自動車検問も許されている。また、一定のチェックポイントを通過する自動車のナンバーを自動で記録する N システムも用いられている。」と述べている。

3　アンドリュー・ファーガソン著『監視大国アメリカ』（2018 年）P199-200

4　前掲書 P136

5　前掲書 P52

6　ウイリアム・ブラットンは、1990 年代、NY 市警本部長として CompStat（computer statistics）を開発、実装した。その後、ロサンゼルス警察本部長としてプレドポルの実験にゴーサインを出した。2014 年にふたたび NY 市警本部長となり、堅固なデータ駆動型システムを導入し、マンハッタンに「リアルタイム犯罪司令部」

を構築した。
7　前掲書 P57
8　前掲書 P173
9　前掲書 P6-7
10　前掲書 P136-137
11　四方光著『システム論アプローチの立場から見た問題点』P39
12　前掲書 P295
13　前掲書 P174-175
14　前掲書 P203 等
15　前掲書 P280。なお、「エリア警備支援システム」（構想）は、途中で頓挫したため、費用算出までは至っていない。
16　この用語は平成 30 年 9 月 20 日、AI 時代における人間力の活用をテーマにしたセミナーでコーディネータの石附弘氏が提唱した。
17　四方光著『エビデンス・ベイスト・ポリシーの意義』P42-43

ビッグデータ警察活動の今後のための提言

アンドリュー・ファーガソン著
（松尾庄一取りまとめ）

アメリカでの止めることのできない最先端技術の勢いと、警察と市民の緊張関係から生じる衝突の解決策についてのアドバイスをファーガソン教授は『監視大国アメリカ』終章で展開している。以下、筆者なりに取りまとめることにする。我が国においてAI技術を積極的に導入するに当たって配慮しなければならない事柄について参考になれば幸いである。

ビッグデータ技術で何をしたいのかはっきりさせる

データ駆動型システムの最初の課題は、リスクを特定し、直面する問題解決にはどのビッグデータ技術が適しているか検討すること。犯行場所予測型システムか、容疑者割り出しシステムか、リスクのある地域を監視するシステムか、複数のデータ領域や集団や地域にまたがる「検索システム」か。

最適なビッグデータシステムの選択は、最終的には政治的決断であり、警察リソースをどこに集中させるかの選択は政治的な決定。その決定に当たり、暴力あるいは暴力的な人物を対象にすることを優先順位のトップに置くことには異論はあまりないだろうが、それ以外の決定はむずかしくなる。また、治安のために常時監視することは地域社会に受け入れられないだろうということにも異論はあまりないだろうが、この間の選択は難しい。

警察官の安全と地域社会のプライバシーの比較検討も極めて困難。ひとつの誤った推定から何の罪もない市民が銃で撃たれれば予測型警告システムそのものが危うくなるし、逆に情報がない状態も緊急事態に出動する警察官を危険にさらす（注）。

解決策として、年に一度の正式な公開の会合で、警察が将来的な技術の購入を提案し、過去の利用について説明を行うことを提案する。公開の監査並びに評価プロセスで、システムの範囲、情報源、費用を明確にし、市民の批判や懸念を議題に乗せることができる。

さらに重要なことは地域社会の意見によってリスクの背景（リスクをもたらす原因）が明らかになること。

（注）ビッグデータ技術システムが発するリアルタイム情報の利点について、ファーガソン教授は別のところで、次のように述べている。
警察官が現場に駆けつける前に現場で何が起きたのか、誰かいるのか、それは危険な人物かを指示することで、現場での適正な判断に役立つだけでなく、警察官の受傷防止に資する。
警察官による誤射殺の典型的原因は、部分的で不完全な犯罪行為の情報を無線で受けた警察官は孤立し、十分な応援もないまま容疑者に近づくこと。警察官は自分の身に危険を及ぼしそうに見える男たちに、身元も脅威の度合いも分からないまま立ち向かう。警官はほかに使えるような非致死性の武器を持っておらず、自分が感じた危険度に見合った対応をとれず、銃で射殺した。
こうした構造的なリスクの多くは、通信、警戒システムの高度化で改善することができる。

それでも、警察活動の透明性、人種の偏見、自動化への不安は、依然として警察が拭い去る必要がある。

さらに、技術の導入が単に犯罪発生件数を減らすためだけなのか、それだけでなく、それが警察官と地域社会の役に立つからなのかを検討しなければならない。ビッグデータという「流行の解決策」に頼るのは近視眼的。

ビッグデータ警察技術を推し進めようとすれば、これらの問いに答えることが第一歩。

システムに入力される正確な情報（データ）と健全な予測モデルに配慮する

ビッグデータシステムの入力情報は、予測型モデルであれば犯罪情報や犯罪統計であり、監視システムではカメラが撮影した画像、検索システムでは指紋掌紋、顔写真、犯歴等のいわゆる生データである。どのようなビッグデータシステムでも、正しい情報入力を徹底させることは、正当性、正確性、有効性にとって重要。本書では、繰り返し起きているデータの偏り、誤り、データシステムの不完全性の問題を明らかにしてきた。こうした問題は、ビッグデータシステムの正当性と信頼性を損なうおそれがある。

質の良いシステムを作るためには、信用できるデータを入力すること。その信用を築くためには「どこからデータがくるのか」「誰が集めているのか」「誰が再確認しているのか」「だれが訂正しているのか」を警察幹部が知っていなければならない。警察組織としては、データを学習、監査、クリーニングする体系を作り上げることを意味する。繰り返すと、入力情報が信用できなければ出力情報は信頼できない。

数百、数千の警察官から一日数千件のばらばらな情報を集めるシステムには、エラーが存在することは不可避。目標は、その誤った入力情報がシステム全体に害を与えないようにすること。そのためには必ず存在する誤りを（ゼロにすることはできないが）チェックする仕組みを導入すること。これが管理者が直面する最も重要な問題のひとつである。

現時点では正確性を保証する仕組みは存在しない（というのがファーガソン教授の評価）。であるのに、データ駆動型警察活動は先を急ぐあまり、すべて集めるという考え方が支配して、「すべて確認する」制度がしかれていない。警察署長は監視サミットで、「私はデータを信用しています。そしてこれが信用に値するといえる根拠となる導入済みのコンプライアンス制度です」と答えなければならない。

人間が判断するときに過ちをおかすことは不可避。その判断の上に築き上げられたビッグデータシステムもまた過ちを犯す。過ち（誤り）をゼロにすることができなくても、エラーの減少と訂正を行う仕組みと安全機能を作り上げることが信用を維持する唯一の方法。

監視システムでは、警察が情報を基に活動できるよう、システムが信用できるものでなければならない。そのために入力情報が正確でなければならないが、それがきちんと行われるためにはシステムの設計から警察幹部の関心が地域社会の関心に寄り添っていなければならない。正確さを実現させるためには、だれかが正確性の価値を訴えなければならないが、そのためには、初期の段階で、後に生じる予見可能なデータ問題について地域社会が声を上げなければならない。

予測モデルには内的妥当性、過度な一般化がないこと、時間的な限界の認識が必要

正確性以外にも、予測モデルそのものが健全で科学的に信頼できるものである必要がある。モデルは、データセット内に人種的偏見と構造的不平等が含まれる可能性を意識して設計されなければならない。これはほかのビッグデータプロジェクトでもほとんど変わらない。人間が作ったデータシステムに内在する限界を弁明するには、内的妥当性、過度な一般化、時間的な限界に目を向けなければいけないが、これらには既に対処と訂正の技術的解決方法が作られている。

内的妥当性とは、ある方法が因果関係を正しく判断できる程度を意味する。

ビッグデータは、因果関係を判断するものではない。相関関係は特定できても、因果関係の理論は単にデータ処理からは生まれない。予測型警察活動戦略が犯罪を減少させる事実は喜んでもいいが、それを犯罪減少の「原因」として売り込むべきではない。

この限界は理論の問題だけでなく、実践にも影響を及ぼす。人は相関関係を因果関係と思いがちだが、そこに過度な技術の売り込みがあると盲目的なデータ重視につながりかねない。予測型警察活動システムの弁明は、データによって不完全に支えられたものでしかない。

過度の一般化とは、ある警察での結果が必然的に別の警察にも適用できるとみなしてしまうこと。大都市で調査された研究がそれより規模の小さい都市や町でも機能するかどうかはよく考えなければならない。機能する場合もあるだろうが、特定の技術を採用する前に過度な一般化がないかどうかを問い、答えを出すことが必要である。

時間的な限界とは、モデルは予測を出すが、予測はモデルによって設定された期間によってその正確さが変化すること（松尾注。講演の中で詳しく言及している。）。

正確で信用できる入力情報と方法論を立てるには、ブラックボックスのように中身の見えない入力情報とシステムの仕組みが説明され、審査される必要がある。このためには、専門家の評価や助言が必要かもしれない。現在、そのようなことを行う法律技術コンサルタントと非営利団体が存在しており、これらなら当該ビッグデータ技術が機能するかしないかの客観的判断を提供できるだろう。さらに正式で独立した審査委員会を地域レベルで導入してもよい。

システムから出力される情報（データ）が公正である

システムから出力される情報（データ）が公正であるためには、まず、システムでどんな成果をあげたいのかはっきりさせる必要がある。犯罪率の低下、警察手続きの効率化、警察官の安全、警察官の教育、地域支援、バランスの取れた予算のいずれなのかはっきりさせる。対立する複数の目的がある場合にどのような優先順位をつけるのかはっきりさせる。

犯罪率の低下を目的とする場合、ビッグデータ警察活動は成功を計るものさしを歪めることがある。計測の容易な出力情報が、定量化の難しいものを差し置いて選ばれることがそのひとつである。

犯罪率は具体的な数値で示される。逮捕者は数えられ、地区はラベル付けされる。ところが、これらの数値が地域社会と警察の関りを正しく示しているとは限らない。悪くすると、ビッグデータの出力情報は、地域社会の住民の警察に対する信頼の問題を覆い隠してしまうかもしれない。

警察幹部は選択した計測方法が地域社会の問題を正確に反映しているかどうか自らに問う必要がある。なぜならば、犯罪を減らす一方で警察に対する信頼も失っているのなら、それは成功とはいえないから。

予算削減の時代に限られたリソースでやりくりするのは管理者にとって重要な責任の一つであるのはいうまでもない。他方、ビッグデータ技術は時間管理と人員管理の効率を上げるが、上述したように、ビッグデータ警察活動は警察の仕事のやり方を歪めるかもしれない。犯罪の減少に効果があるかどうかに関係なく、特定の区域に警察が積極的に目を向ければその区域の環境は変わるだろう。ただし、その区域での職務質問が増え、「現場尋問カード」の作成に圧力がかかれば、極端にいえば警察官はより大きな情報管理体制のデータ収取者になってしまいかねない。これは、警察の市民との関わり方を変える。

持続的な監視カメラは犯罪行為をとらえるとともに、その過程で一般市民も監視の対象にしてしまう。特定の地域に対して社会的統制活動を統制するために持続的な監視カメラが設置されるならば住民の反発を生むだろう。そのような負の感情は技術を採用した結果だと認め、警察幹部は定期的な公のフォーラムで、技術の「代償」を認め、地域社会に対して技術の価値を「弁護」できなければならない。

警察活動が公正で市民の信頼がある

ビッグデータ警察活動には、（アメリカでは）どんなに否定しても人種差別的な結果を生むリスクがある。ビッグデータシステムを採用する警察幹部は地域社会に対してどのような戦略についても人種的な影響を説明できなければならない。警察幹部は人種的に不均衡な技術の適用を避けるための確実な手段、検証、戦略を指し示さなければならない。

また、警察が犯罪を助長している根本的な環境リスクと取り組んで、犯罪を感染症のように考え、警察官を公衆衛生担当官にしようと考えているならそのビジョンには大きな疑問がある。なぜならば、ブライトデータ（注）はリスクを発見できるが、警察がそれらのリスク対策に適していると限らないから。社会問題に必要なものは社会福祉による対策であって警察活動による対策ではないと考えると、警察は特定の責任から手を引く必要があるかもしれない。

各種のビッグデータ警察活動技術の共通の特徴は、ビッグデータから犯罪行為と相関するリスク要因を特定することにある。このリスク特定技術が犯罪と取り組む警察の画期的な戦略を数多

（注）犯罪を助長している根本的な環境リスクとの取組みにおいて、「特定された社会あるいは環境リスク」を算出するためのビッグデータのことでファーガソン教授の造語。このようなビッグデータを、正確かつ目的意識がある「賢い」という意味での「ブライト」、そして隠れた問題やパターンを明らかにする「明るい」という意味での「ブライト」から「ブライトデータ」と呼んだ。
ブライトデータに対比するものとしてファーガソン教授は、「ブラックデータ」という言葉を使っている。ビッグデータ警察活動に使われるデータベースは、データの大部分が複雑なアルゴリズムの中に隠されていることから、「不透明、グロテスク」という意味での「ブラック」、データが有色人種社会に直接影響を与えることから、「人種的に符号化されている」という意味での「ブラック」、これまで法律によって明確に理解されていた部分に「法的な闇と憲法上の空白を作る」という意味での「ブラック」から「ブラックデータ」と呼んだ。

く導いてきた。しかし、これにより特定されたリスクの中には、対応は警察のみで行う必要はないものがある。他機関が行うことで同じような、場合によってはそれ以上の効果をあげることもある。

ブライトデータは、「特定された社会あるいは環境リスクに対処するに当たって、警察が本当に最適な機関なのか」と問うている。ビッグデータ技術は、リスクの予測に役立つだろうが、その構築に警察の手続きを通す必要も、警察が管理する必要がないものもあるだろう。

最近になって犯罪率が低下しているのに警察への信頼度が下がっている現象がある。人種の緊張が地域社会の信頼を覆した時には特にそうである。ビッグデータは現場での人種差別的行為を減らすためのツールであると主張するのならば、警察幹部は人種的に不均衡な技術の適用を避けるための確実な手段、検証、戦略を堂々と説明しなければならない。

人物予測型の方法には、（あらゆるリスク判定方法と同じく）差別になりかねない社会経済的な要因が含まれている。意図しない差別を避けるためには、そうした影響と計画的な修正手段をしっかりと認識することが優先されるべきである。言い換えれば、差別的な影響を回避するために、統計分析的手法の選択には慎重を期す必要がある。隠れたあるいは目に見える偏見が予測モデルに入らないようにしなければならない。

ビッグデータ警察活動は、予測データセットにおいてその焦点を個人からカテゴリー化された（集団の）疑い、あるいは場所に基づく疑いへと移している。このような容疑の一般化へのシフトは、固定観念による定型化と犯罪行為の責任を特定集団にまで広げる連座制を助長する。それは街頭での個別の容疑の基準を歪め、憲法修正 4 条の保護を弱めることになる。このことは、自分以外の人間の行為が原因で特定地域が標的になったり、自分以外の人間の行為が原因で特定集団が対象に指定されたりする可能性がある。また、単に問題のある社会ネットワークと交友があるだけで監視対象にされるおそれがある。

兄弟が犯罪組織にいる少年をみな組織の仲間とみなしたり、犯罪多発区画で生活する少女をみな容疑者としたりすべきではない。こうした一般化は、特定の疑いにおける個人の人格を無視している。憲法修正 4 条は、連帯容疑や相互に関連する容疑では自由の侵害を正当化するには不十分であるとしている。予測によって特定の集団が将来犯罪に関わることが示唆されても、（その集団の中の多くの個人は犯罪との関りを避けるのだから）そうした人々に一般化した容疑で汚名を着せてはならない。

ビッグデータ警察活動技術が説明できる、ある程度の透明性が確保されている

誤情報、偏見、歪みというテーマ、そして構造的な入力と出力の問題は、検証という解決策にたどり着く。警察活動に用いられるビッグデータ技術は継続して検証を重ねなければならない。

検証によって正確性が高まり、正当性があがり、安全性（セキュリティ）が確保できる。さらに重要なことは、その技術が検証可能であるという事実が民主主義の行政にとって欠くことのできない説明の手段になる。

実際問題として、裁判所を通して警察の行いに異議を申し立てるという法的な説明責任を追及

する形ではビッグデータ技術の発展を監督するには遅すぎる可能性がある。学者や科学者が旧式の予測システムを検証するにはそれなりの意義があるかもしれないが、実社会における説明責任としては、検証過程はいつも技術の進歩に追い越されてしまっている。予測モデルの多くは、日々変化しており、そのような動くターゲットの検証は依然として極めて難しい。警察署長がビッグデータ技術について説明する場合、「システムがどのように機能するか」や「なぜ機能するのか」に加え、「どのように検証するか」が重要になる。検証する方法が機能の仕方よりも安心感をもたらす、分かりやすい説明になる可能性がある。

システムの検証については、「どのように」あるいは「なぜ」が求められるが、これについては、独立した監査、測定基準、遵守基準があるべきだ。警察官僚にその基準に見合っているかどうかを説明する責任を課せば、どのような新技術でもその利用が成功しているかどうかが明らかになるだろう。その答えが専門家の調査に裏付けられていて、公開されており、さらに地域社会も参加していれば、すべての参加者（ステークホルダー）がその新技術に対して大きな安心感を抱ける。

警察の技術利用の影響が及ぶ人々の自主性が尊重されている

ビッグデータの魅力は、客観的で非人間的な判断に頼れるところ。ビッグデータの危険は、技術に導かれる探究の対象に人間的な要素が含まれること。他方、警察活動は（データ駆動型かどうか関係なく）人間的であり、個人の正当性や自主性という根本的問題と関わっている。つまり、データ駆動型の予測型警察活動システムでは、利用者は人間的な側面を知っておく必要がある。

人間が罪を犯し、人間が犯罪を予防し、捜査する。その行為はいずれもデータ点に変換することができる。がしかし、いずれも単なるデータとして理解すると、必ず分析で重要なことを見落とす。特にデータ駆動型警察活動では個人の特性、感情、果てはプロセスの象徴的意味さえ無視すると個人の正当性や尊厳の原則を弱めることになる。

データ依存の警察活動は個人の自主性の尊重に関わる社会的価値と対立しかねない。「個人の行動を予測する試みは、その個人を自律した人間としてではなく、予測できる物体に簡略化することのように見える」（バーバラ・アンダーウッド）。

予測型警察活動において逮捕の統計値に注目すると、容疑者の人間性を軽視することになる。例えば、警察が逮捕件数に基づいて成果を認められたり、逮捕件数を伸ばしたりするように圧力をかけられると、生産性という測定基準の陰で人間性が二の次になる。構造的には、組織上の警察活動戦略が地域社会のニーズ（人と文化）ではなく、数字、すなわち犯罪率とパターンを重視することになれば、データ主導の活動重点が地域を支援する役割より優位に立つ。

自主性軽視のリスクは、予測される要素が容疑者の手を離れた物事に関わるとさらに大きくなる。統計分析の多くの要素は容疑者自らの選択ではなく生まれつきの要因と関わっており、また、選択でさえ環境の影響を受けている可能性がある。

特に、人物予測型の方法には、前述したように差別になりかねない社会経済的な要因が含まれている。どのような技術を選択するにしても、警察は、市民の自主性を重んじ、個別の容疑に着

目すべく設計されたシステムを優先しなければならない。

まとめにかえて

本書（『監視大国アメリカ』）で取り上げた問題点は、見かけは新しい技術に基づく活動であっても古くから存在する警察活動の問題を反映している。アルゴリズムとデータ駆動型技術は新しく、ほとんどのイノベーション同様現状を打破する。けれども警察の活動にも変化が必要。ファーガソン事件後の警察の扱いに対する抗議はその時初めて始まったわけではない。いらだち、憤り、激しい怒りの声は歴史をさかのぼって、全米各地にその起源をたどることができる。

ビッグデータ警察活動はその過去を見て見ぬ振りをするために用いてはならない。技術的な可能性によって人間的な問題を回避することを信じることは空頼みである。なぜならば、いかなる新技術でも構造的体系的な社会問題を一掃してくれないから。

ビッグデータ技術の導入は、データ収集とともに、より多くの情報収集、よりよい手段、犯罪と社会問題に関するより明確な全体像が手に入るし、警察幹部は地図、図表、監視ビデオ記録でリスクを視覚化できる。これらにより警察幹部は暗闇の中を以前より深く見通すことができるのは事実である。そのために、データにもとから備わっている暗闇にいかに光を当てるかでビッグデータ警察活動の予測の適否が左右される。

また、警察幹部がリスク、入力情報、出力情報、システムの検証、市民の自主性に対して深く考察することが、ビッグデータ警察活動の成否を左右するのも事実である。本書が（アメリカの場合）次のビッグデータイノベーションに投資するかどうかの検討に資することを期待する。

以上

（本稿は、令和元年７月３日の警察政策学会シンポジウムでの講演記録を再掲した。）

サイバー脅威への対応

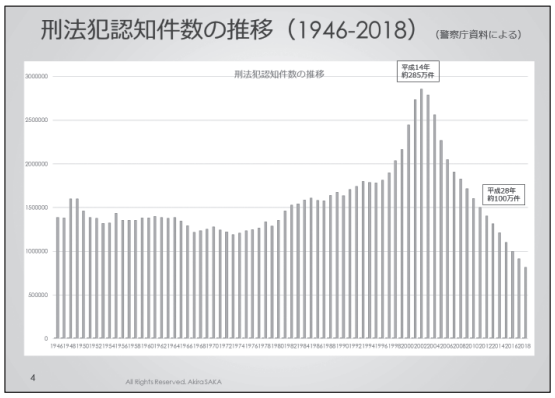
（公財）東京オリンピック・パラリンピック競技大会組織委員会 CISO　　坂　　明

それでは私から「サイバー脅威への対応」についてお話させていただきます。実は皆さんは20分なのに私だけ30分いただいております。これはなぜかというと、第２部は「グローバル化及びデジタル化への対応」というテーマで時代の変化を踏まえた検討を行うことになっているところ、サイバー脅威は当初よりグローバル化・デジタル化という特質を有しているため、第２部でお話しする内容も第１部で一体的にお話しさせていただくためです。したがいまして、第２部では、若干の補足程度のお話をさせていただくことになるかと思います。

内容としては、サイバー脅威の状況、サイバー犯罪の変遷、対応体制、国際化、サイバー犯罪の攻撃者・犯罪者像、産業界と政府・法執行機関の連携といった点をお話しし、今後に向けた対応を検討してみたいと思っております。

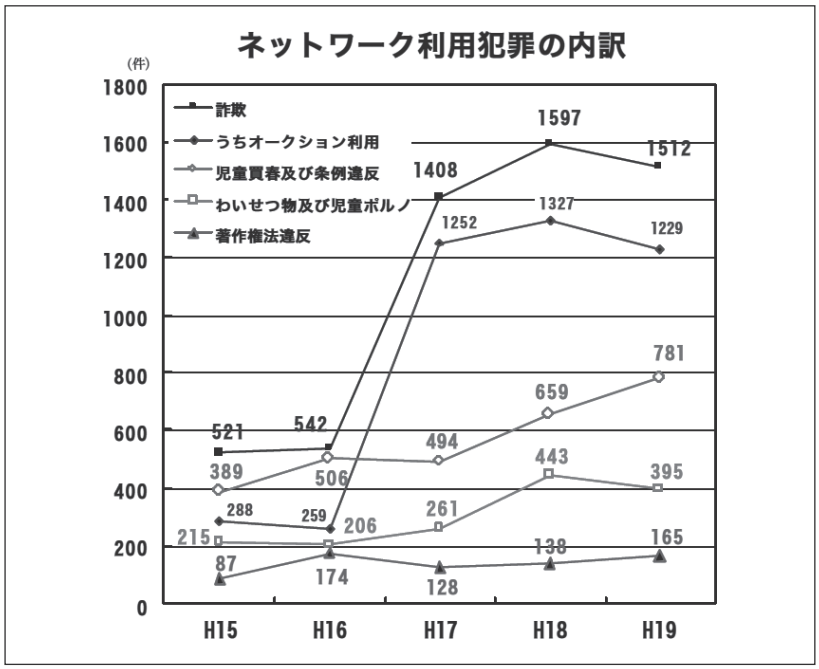
サイバー脅威の変遷

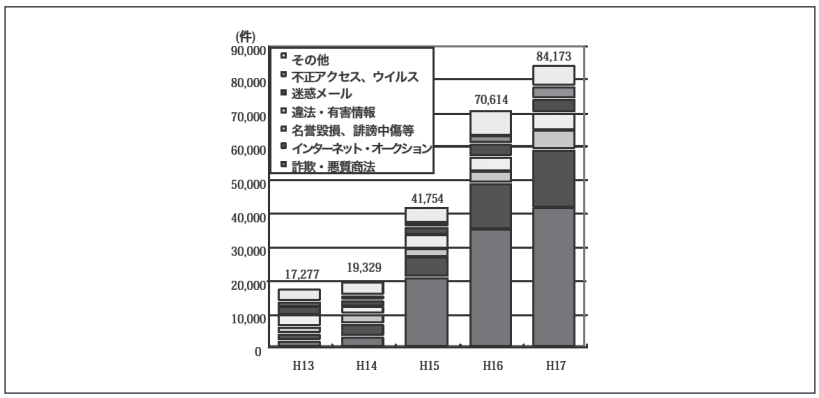
まず、サイバー脅威の状況からお話しします。この図は刑法犯認知件数の推移ということで、石附先生始め多くの方が言及されておられますが、ご覧のように平成14年をピークに減少を続けている状況です。（なお、この刑法犯認知件数を始め、以下犯罪や相談等の件数は警察庁の資料によります。）



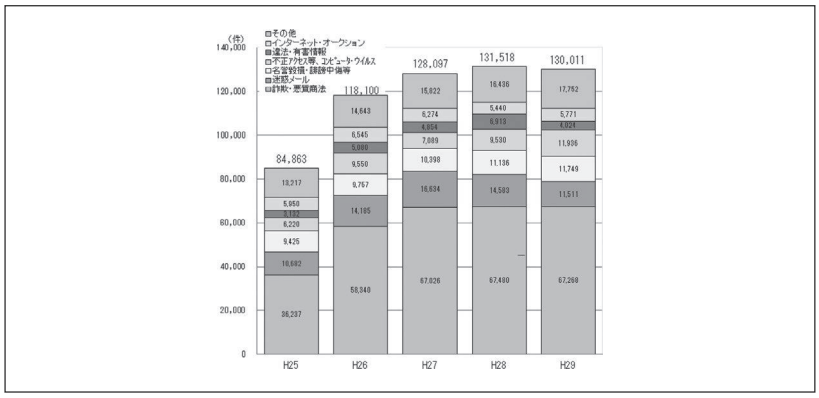
一方、サイバー犯罪ですが、図でお示ししているのはネットワーク利用犯罪の検挙の状況です。16年から17年にかけて急激に増えております。この段階で、詐欺、特にネットオークションの増加が顕著であり、比較的愉快犯の傾向の強かったサイバー犯罪が、本格的な経済的利益を狙った犯罪に変化していったことが見てとれます。

ご案内のようにサイバー犯罪というのはいろいろな犯罪の手段として使われるものですから、刑法犯としての類型及びその統計だけでは捉えることができないため、警察庁ではサイバー犯罪等に関する相談等の受理件数を毎年発表しております。先の図にありましたように検挙は17年に大きく増加していますが、相談受理件数で見ると詐欺・悪質商法とインターネット・オークションを合わせ経済的な利益を狙った犯罪が15年の段階から大きく増加しております。





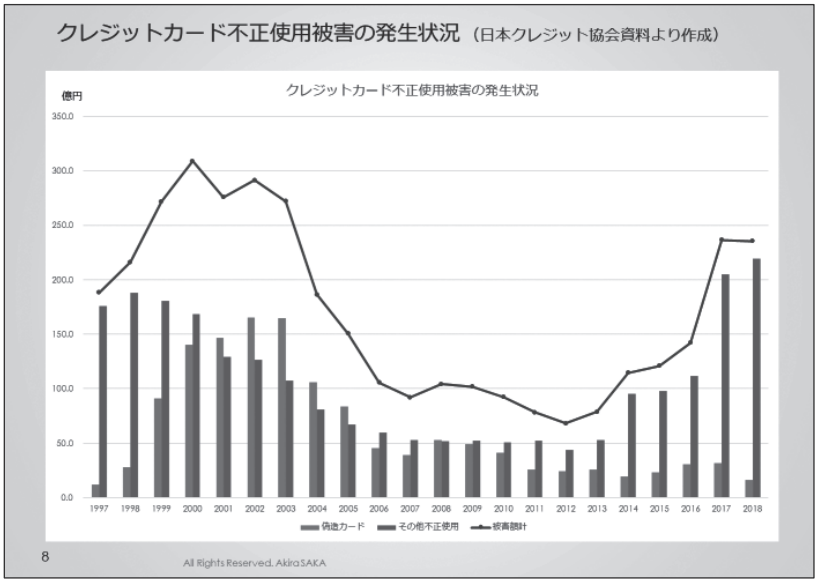
これは象徴的で、一般の犯罪では 14 年がピークで以後減少を続けていますが、サイバー犯罪はそこから増加を始めているということになります。17 年は相談等受理件数が約 8 万 4,000 件ですが、実は次の図のように、25 年は相談等受理件数が約 8 万 5,000 件です。



つまり 17 年から 25 年まではサイバー犯罪等に関する相談等受理件数は大体横ばいで推移しておりました。ところが 26 年、27 年と急激に増加していることがこの図から分かると思います。約 8 万 5,000 件から約 11 万 8,000 件に増加という状況です。この一番下の部分が詐欺・悪質商

法ですが、ここも 3 万 6,000 件から 5 万 8,000 件と大きく増えている状況です。それからその上の部分が迷惑メールです。いわゆる標的型メールのようなものも含まれていると見ていただきたいと思います。これが 25 年の 1 万件から 26 年の 1 万 4,000 件と急激に増えております。皆さん方もご記憶にあると思いますが、日本年金機構の情報流出事案が発生したのが平成 27 年 5 月です。したがいまして、15 年、16 年、17 年ぐらいに経済的な利益を狙った本格的なサイバー犯罪が急激に増加し、26、27 年あたりから経済的利益を狙った犯罪が大きく増加するとともに情報窃取を狙った標的型攻撃も広く認識されるようになった状況です。今はあらゆる形のサイバー犯罪、サイバー攻撃が高い水準で推移しているというのが実態です。

次の図はクレジットカード不正使用被害の発生状況です。日本クレジット協会の資料より作成いたしました。クレジットカード犯罪被害のピークは、一般の犯罪よりも早くて 12 年になっております。そして、近年、急激にクレジットカードの不正利用が増えており、最悪の状況に近づきつつあります。

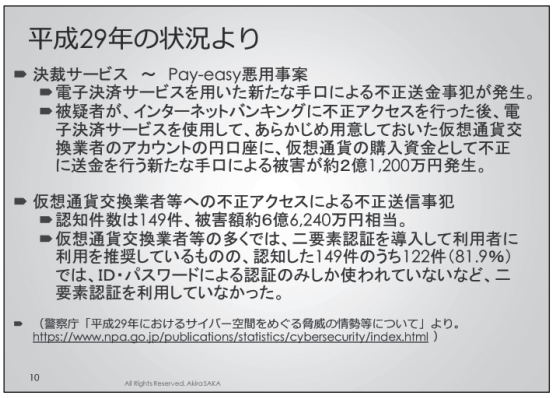


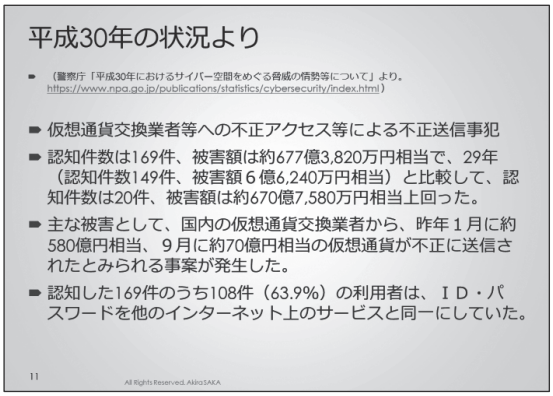
私はクレジットカード犯罪の最悪のピークの頃、警察庁生活安全局生活安全企画課セキュリティシステム対策室長をやっておりまして、クレジットカード犯罪対策も担当しておりましたが、クレジットカードには補償制度をはじめいろいろな仕組みがあり、被害が発生してもエコシステムとしてある程度維持されていたのですが、被害がこのように大きなものになってくるとそれが崩壊しかねない状況になり、関係者が一丸となっていろいろな対策を講じていた時期になります。

この図の棒グラフの左側の部分は実際の偽造カードというフィジカルなカードが出てくる犯罪と考えていただきたいと思います。棒グラフの右側の部分はその他です。その他の大きな部分は番号盗用で情報を窃取してインターネットなどで使って被害を生じさせるものです。ですから、大きな被害を出しているもの、これは 2018 年で 250 億円近くなっていますが、この被害を出しているのはサイバー犯罪としてのクレジットカードの不正利用ということになります。

このように一般の刑法犯認知件数は減少していますが、サイバー犯罪は様々な形で増加しているというのが実態であります。

さらに、最近話題の様々な決済手段、あるいは仮想通貨もサイバー犯罪の大きなターゲットになっているということは、皆さん方も報道等でご存じかと思いますが、29 年及び 30 年の状況をスライドでまとめてみました。





それから、ビジネスＥメール・コンプロマイズ、あるいはＥメールアカウントのコンプロマイズという、BEC/EAC と言われるものも大きな被害が出ています。これは関係者になりすまして金を振り込んでくれという通知を出して、お金をだまし取るというものです。

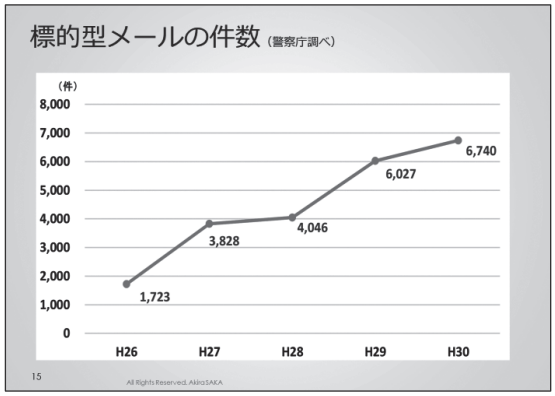
米国の IC3 が発表しているデータで被害状況を見ると、全世界では 125 億ドルという巨額の被害が発生しております。日本でも報道がありましたし、検挙事案もあります。

日本経済新聞の 18 年 9 月 5 日の「春秋」というコラムで、「日本の犯罪は 13 年連続して減り続けている。だがそれは目に見える世界の話であって、実はネット社会へと悪意が次々引っ越しているだけなのかもしれない」と書かれておりました。当時、私は「実際はどうなのだろうか、現実の犯罪というのは本当に大きな脅威であるし、本当にネットに引っ越してきているものだろうか」と半信半疑でありましたが、今、このように実態を見てみますとそのとおりかもしれないなと思うようになってきています。

サイバーインテリジェンス

サイバーインテリジェンスについてですが、こちらは情報窃取を狙う標的型メールの件数で、やはり増加している状況です。

インテリジェンスと言えば、ちょっと懐かしい話でありますが、リヒャルト・ゾルゲというス



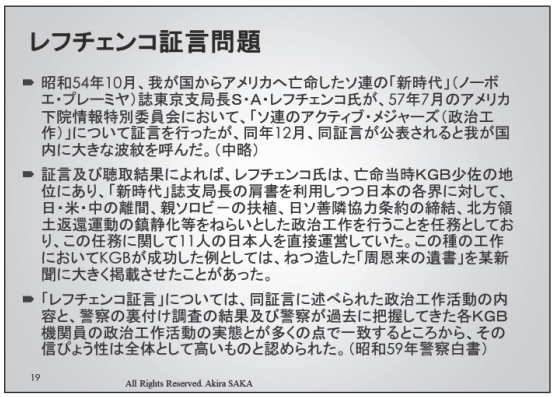
パイの関係資料を私も高校時代よく読みました。第二次大戦中に日本の上層部に食い込んで情報を窃取し、日本の南進政策を通報してソ連に勝利をもたらしたと言われております。ロシアでは国家的な英雄とされているということです。こういった諜報活動というのは当然ながら国家がやっているわけです。

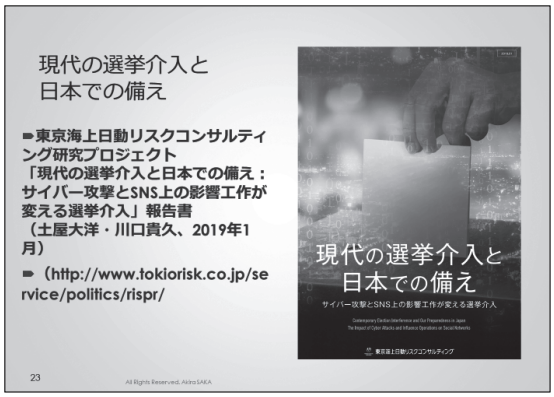
こちらはFBIの指名手配書からのものですが、2014年5月19日に、初めてこうしたステートアクターを指名手配したと書いてあります。ウエスチングハウスですから、日本とも関係の深い企業です。こちらから機密情報が盗まれたということで、中国人民解放軍幹部を指名手配しているということです。このように犯罪として扱うのは民間からの情報窃取になりますが、政府の情報も当然ターゲットになっているものと考えられます。日本にもこうした攻撃は来ているわけです。このように、一般の犯罪のみならず、諜報活動もサイバー空間で活発に行われるようになってきている。こちらも、少々懐かしい話になるかもしれませんが、ソ連時代の政治工作であるアクティブメジャーズ（偽情報の流布なども含め自国の外交政策を支援し相手国の大衆・個人・政府の意見や行動に影響を与える意図で行われる有害活動）についてのスライドです。また、その次のスライドは昭和54年のレフチェンコ証言問題についてです。

警察白書によれば、レフチェンコは「ねつ造した「周恩来の遺書」を某新聞に大きく掲載させたことがあった。」とあり、KGBの成功事例として挙げられております。

では、現在はどうかということになります。

これは、慶應SFCの土屋大洋先生、そして東京海上日動リスクコンサルティングの川口貴久





先生がまとめられた「現代の選挙介入と日本での備え」という、平成 31 年の 1 月に出されたレポートです。選挙介入は意思決定に関する影響工作になります。外国政府が対象社会を分断し、政治制度の信頼性を毀損させることを通じて政治目標を達成するための活動であり、偽情報の流布も含め、秘密工作、公然たる工作、そしてサイバー攻撃等を組み合わせたものになると論じておられます。制度への攻撃とは、選挙管理インフラに対するサイバー攻撃や、投票結果の改ざん等が代表的ですが、選挙や民主主義の信頼性を失墜させることも制度への攻撃と言えると位置付けておられます。例えば米国大統領選挙で特定の候補者に有利な投票行動に、あるいは英国の EU 離脱の国民投票のような場で特定の方向に誘導するということもあるかもしれませんが、こうした選挙や投票を混乱させることにより制度自体の信頼性を失わせるということも可能な状況になっています。プーチン大統領が 2019 年 6 月 28 日の新聞記事で「自由主義は時代おくれ」と発言したと報じられていますが、民主主義という制度自体の価値が低いものと発信しています。

近時は、中国の経済的・国際政治的・軍事的な拡大を踏まえて、中国のような体制の方が経済的にも厚生的にも効率がよいのではないか、との主張もよく耳にするところです。

こうした状況を見ると、日本警察、そして我々が守っている民主主義という価値を、サイバー攻撃によって毀損させることも可能な時代になってきていると言えるのではないかと思います。サイバー空間が「民主主義」という価値を守る上でも重要な戦場になってきているというのが今日の実態かと思います。

このように、サイバー脅威の現状は、攻撃者は、犯罪者にしても、ステートアクター（国）にしても、明確な目的を持って非常に執拗な攻撃をしてくるというものになります。その目的の内容として、情報や経済的利益、また破壊活動、更に言えば政治的な主張を展開する、データを収集する、攻撃や経済的利益のためのインフラを構築するといった様々な、しかし明確なものをもって攻撃してきているということであります。そして、犯罪者は国際的に、組織的・有機的に連携して攻撃を行い、また自立的といいますか、特定の目的に向かって、呼びかけなどに呼応した様々な主体が一斉に特定の目標を攻撃することなどもあり得るということです。

サイバー犯罪の変遷と警察の対応

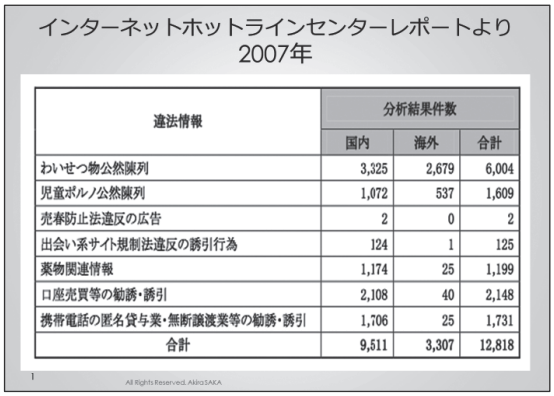
サイバー犯罪の変遷ですが、サイバー犯罪としては3つの類型を考えております。インターネットのような情報通信システムも含め情報システムに対する侵害行為。それから情報システムを利用して様々な犯罪行為を行うもの。それから青少年を守るというものが代表的ですが、環境としての情報システムに関する問題であります。大きく言えば、この順番に出現してきたところがあるかと思います。

サイバー犯罪の変遷と、警察の対応、それに対応する制度や体制についてですが四方光先生と私の名前で「サイバー犯罪とは何か」という形でとりまとめたものが角川学芸出版から平成26年12月に刊行された『仮想戦争の終わり（角川インターネット講座（13)』に収録されております。もし関心のある方はご覧いただければと思います。本日は警察関係の対策等をご紹介しますが、この本にはサイバー犯罪に関連する国の施策・制度などの関係も含めて記載しております。この論文は、実際にその政策に当たった方々にもご協力いただき、四方先生が大変活躍されてとりまとめられたものです。

これには大体26年まで書いてあるのですが、30年の警察白書もサイバー犯罪特集で非常によくまとまっておりますので、そちらをご覧になると27年以降の状況をご理解いただけるのではないかと思います。

国際化

国際化についてもいろいろなデータがありますが、ここではインターネットホットラインセンターの統計を見ていただきたいと思います。平成19年と30年の違法情報について比較していただくと、もともとサイバー犯罪は国際的なものであるところ、それが一層進展していることが一目瞭然かと思います。



インターネットホットラインセンターレポートより
2007年

違法情報	分析結果件数		
	国内	海外	合計
わいせつ物公然陳列	3,325	2,679	6,004
児童ポルノ公然陳列	1,072	537	1,609
売春防止法違反の広告	2	0	2
出会い系サイト規制法違反の誘引行為	124	1	125
薬物関連情報	1,174	25	1,199
口座売買等の勧誘・誘引	2,108	40	2,148
携帯電話の匿名貸与業・無断譲渡業等の勧誘・誘引	1,706	25	1,731
合計	9,511	3,307	12,818

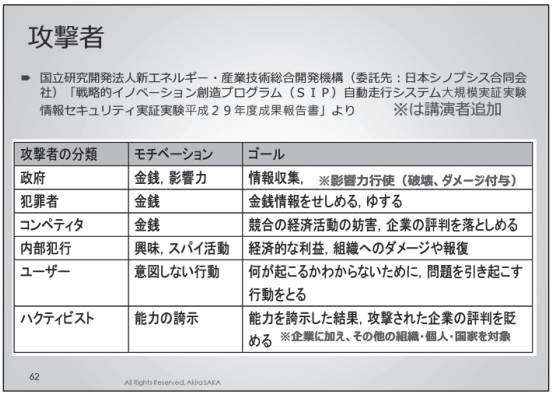
2018年　違法情報

	国内	海外	合計
わいせつ電磁的記録記録媒体陳列	2,174 件	27,911 件	30,085 件
児童ポルノ公然陳列	201 件	2,221 件	2,422 件
売春目的等の誘引	173 件	641 件	814 件
出会い系サイト規制法違反の禁止誘引行為	0 件	1 件	1 件
薬物犯罪等の実行又は規制薬物の濫用を、公然、あおり、又は唆す行為	54 件	88 件	142 件
規制薬物の広告	75 件	2,012 件	2,087 件
指定薬物の広告	2 件	11 件	13 件
指定薬物等である疑いがある物品の広告	0 件	0 件	0 件
危険ドラッグに係る未承認医薬品の広告	0 件	0 件	0 件
預貯金通帳等の譲渡等の勧誘・誘引	15 件	260 件	275 件
携帯電話等の無断有償譲渡等の勧誘・誘引	6 件	83 件	89 件
識別符号の入力を不正に要求する行為	0 件	23 件	23 件
不正アクセス行為を助長する行為	0 件	0 件	0 件
合計	2,700 件	33,251 件	35,951 件

サイバー犯罪条約も、そうしたサイバー犯罪の国境を越えるという特質を踏まえて検討・成立したものです。最近この関係で話題になっているのは越境捜査の関係です。クラウド化も随分進んで、皆様もメールサービスやリモートストレージなど様々なサービスを使っておられると思います。当然、犯罪者も利用するわけですが、サーバーが海外にあるような場合、捜査においてアクセスする場合に手続を検討する必要があります。通常の海外警察機関への協力依頼手続では間に合わない等のケースが出てきます。これにどう対応するかということが課題になっています。

攻撃者像

それから、攻撃者の分類です。次の図は、自動運転に関する情報セキュリティについての平成29年度SIPプログラムの報告書より引用しております。



攻撃者

- 国立研究開発法人新エネルギー・産業技術総合開発機構（委託先：日本シノプシス合同会社）「戦略的イノベーション創造プログラム（ＳＩＰ）自動走行システム大規模実証実験情報セキュリティ実証実験平成２９年度成果報告書」より　※は講演者追加

攻撃者の分類	モチベーション	ゴール
政府	金銭，影響力	情報収集，※影響力行使（破壊、ダメージ付与）
犯罪者	金銭	金銭情報をせしめる，ゆする
コンペティタ	金銭	競合の経済活動の妨害，企業の評判を落としめる
内部犯行	興味，スパイ活動	経済的な利益，組織へのダメージや報復
ユーザー	意図しない行動	何が起こるかわからないために，問題を引き起こす行動をとる
ハクティビスト	能力の誇示	能力を誇示した結果，攻撃された企業の評判を貶める ※企業に加え、その他の組織・個人・国家を対象

62

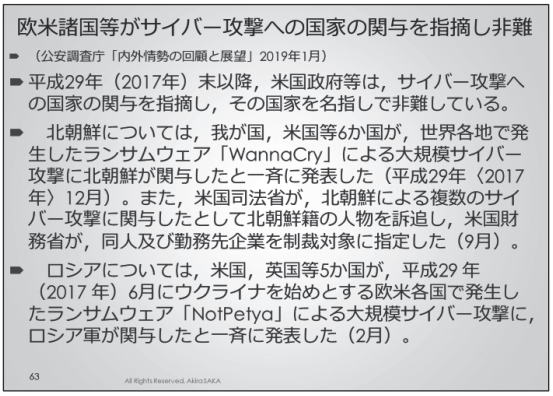
攻撃者は、政府関係、ステートアクターもこれに含まれますが、それから犯罪者、競合相手、内部犯行です。このユーザーというのは気の毒な感じもするのですが、システム管理者からするとあるのかもしれません。あるいはハクティビスト（ハッカーとアクティビスト〔活動家〕を合わせたもの）のような存在も記載されており、要するに様々な存在があります。

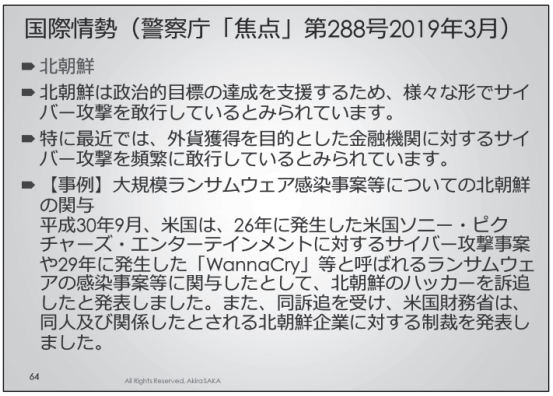
ここで考えてみたいのは北朝鮮についてです。北朝鮮のような存在は、もちろんステートアクターですし、情報窃取の能力も持っています。一方、彼らは経済的利益を得るためのサイバー犯罪も行います。

例えば「WannaCry」のようなものについても、脆弱性はもともとNSAが情報収集するために使っていたようなものを、この「WannaCry」のようなランサムウエアが使ったり、さらには

それをもうひとひねりして、「NotPetya」のようなシステムを破壊するものに使ったりするということがあります。したがいまして、ツール面でも主体の面でも、一般の犯罪とステートアクターが行うようなものが、だんだん境界が曖昧になってきていることも言えるのではないかと思います。

このような情勢に対して、以下のスライドのように公安調査庁や警察庁は警告を発しています。



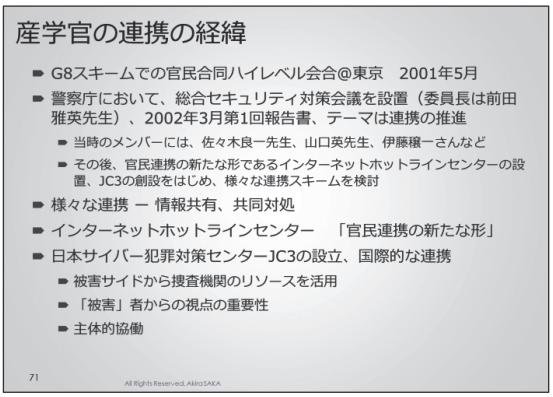


また、一般の経済的利益を狙ったサイバー犯罪について考えてみると、例えばコンピュータウイルスを悪用した不正送金事案などは、ウイルスを作成して、ウイルスを送りつけて、そのウイルスに指示して情報窃取して、その窃取した情報を使って被害者のコンピュータから金融機関のシステムにアクセスして、それから犯人が用意した口座に送金させて、それを引き出して現金化するというプロセスが発生します。つまり、まずウイルスをつくる人たちがいて、それを配る人たちがいて、送金先の口座を用意して、それに対して不正送金の実行をして、そして出し子を用意してやる。このように非常に多くの人たちが関与して犯罪が行われている。このような各存在が密接に連携し、しかも国際的に協力しながらサイバー犯罪が行われている、というのが今の実態です。

官民の連携

このようなサイバー犯罪者・攻撃者に対抗するためには、どうしたらいいのか。その鍵は官民連携であると言えます。インターネットは民間によって支えられているものですので、官民連携はサイバー犯罪対策の上でかなり早い段階から重要性が認識されておりました。その経緯につい

て次のスライドでまとめてみました。

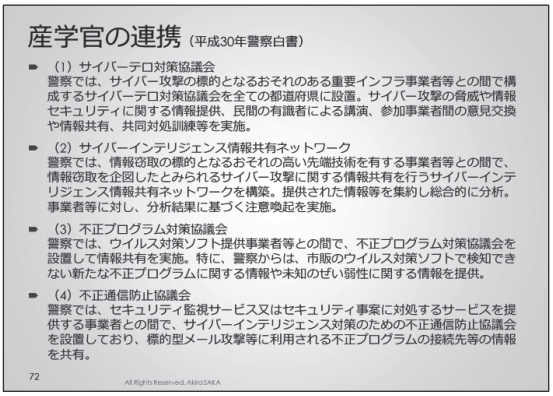


このスライドでは、2001 年（平成 13 年）から記載されていますが、政府と産業界の連携の重要性については、実際はこのかなり以前から言われており、G8 スキームでも検討され、ここにある 2001 年というのは、第 1 段階の官民連携検討のファイナルステージというか、総まとめのようなものです。サイバー犯罪対策において官民連携、つまり法執行機関と民間との連携が必要だということを G8 スキームでも議論してきて、しっかり取り組むべきだという方法論をとりまとめ、それに従って各国で対策を進めるという合意ができたのが 2001 年 5 月の東京会合と言えます。

この合意に基づき、日本では警察庁において、総合セキュリティ対策会議が設置されました。委員長には前田雅英先生がご就任されています。

この総合セキュリティ対策会議から、様々な施策も生まれております。法改正を含む制度整備にも貢献しておりますが、また、インターネットホットラインセンターのような有害情報・違法情報を民間からお寄せいただくような仕組みができ、あるいは私も理事をやらせていただいておりました日本サイバー犯罪対策センターが設立されるという形で、実際に場を同じくして官民が一緒に対策を講じていく、いわば第 2 期とも言えるような官民連携につながっていったと言えるのではないかと思います。

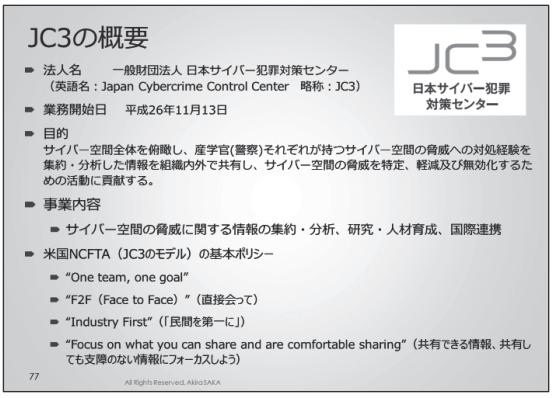
現在の官民連携の状況ですが、次の図で平成 30 年の警察白書からとりまとめたものを掲げてあります。よくまとまっているので、現在の全般的な状況を見ていただければと思います。



ここで、JC3 についてお話ししたいと思います（概要をスライドでまとめてみました）。これは NCFTA という米国の NationalCyberForensics&TrainingAlliance をモデルとしてつくられた

ものですが、米国はご案内のように連邦レベルでも捜査機関が複数ありますが、NCFTA ではそれらが一堂に集まっているとともに、民間の方々がいらっしゃって、一緒にサイバー犯罪対策を進めております。米国の NCFTA は捜査権限も活用して、脅威の特定、軽減、無効化を図ることが目標であり、成果であります。捜査機関のみならず、民間も一緒に情報を共有し様々なリソースを活用していくということです。

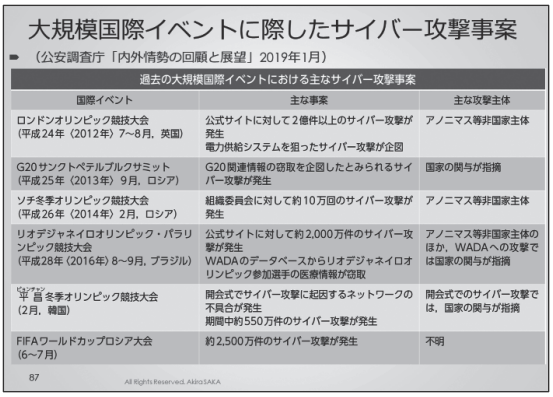
これが非常に成果を上げておりまして、日本でも取り組むべき、ということで JC3 ができましたが、ほかの国でも、例えば英国では CDA という組織もできました。さらには官民が一緒にやっていくだけではなくて、官として国際的な面も含め様々な捜査機関が場を同じくして協働していく仕組みもできつつあります。JC3 自体は 26 年から活動していますが、おかげさまで、いろいろな形での警察のご支援もあって、成果を上げつつあります。



また、少々以前の例ですが、2014 年 6 月、GameOverZeus というネットバンキングなどを狙った大規模なボットネット壊滅作戦について FBI が広報を行いましたが、多くの民間企業や関係国の法執行機関、米国政府内の協力が成果に直接結び付いたとされており、正に官民が連携して取り組まれた事案であることが分かります。この事案については、FBI・司法省に加えて、国土安全保障省（DHS）や欧州のユーロポールも同日付で広報しており、こうした機関の密接な連携も見てとれます。

今後に向けて

今後に向けてですが、まず、課題として、私も組織委 CISO として取り組んでいる、2020 年の東京オリンピック・パラリンピック競技大会の安全確保があります。



このスライドは公安調査庁の資料ですが、このようにオリンピックにも関連して様々な攻撃が行われております。多くの方々と協力して対応していくことが非常に重要であると考えております。

もう１つは、安全保障領域との関係です。最近、新聞報道でサイバーアタックについても、武力攻撃に相当するものについて、日米安保条約の対象となるという記事がありました。武力攻撃と見做し得る烈度のサイバー攻撃もあり得るということは国際的にも議論がされておりますが、問題は、そこに至らないサイバー攻撃に対してどのように対応するか、ということになります。攻撃対象としては、デモクラシー自体もあります。情報や重要インフラを含むシステムもあります。それから生命・身体・財産も当然攻撃対象になります。対応については、外交的・経済的対応も含め様々なものが考えられますが、既に国際的には例も見られるように捜査権限を活用した対策もあり得、この部分では、警察も期待されるところがあるのではないかと思います。

先ほど攻撃者という観点からステートアクターと一般犯罪者という境界が曖昧になっているという話をいたしましたが、攻撃対象から見ても、いろいろな対応から見ても、安全保障とか国家の価値といった側面から経済的利益を狙った犯罪まで、サイバー攻撃についてかなりシームレスになってきているのが実態であると思っています。

今後、サイバー脅威は、犯罪という面から見ても、国家的なオペレーションという観点から見ても、ますます高まるものと考えられ、また、攻撃や対応もシームレスになってくることを考えると、社会として、そして警察として、捜査・防犯も含めた犯罪対策にも、警備関係対策にもしっかり取り組んでいかなければいけない厳しい環境にあるということで、私のお話を終わらせていただきます。どうもありがとうございました。

（本稿は、令和元年７月３日の警察政策学会シンポジウムでの討論記録を再掲した。）

第２部　グローバル化とデジタル化への対応（討論）

警察庁の体制の整備

松尾庄一：グローバル化とデジタル化に対しては、後述するように警察庁は平成の時代に着々と体制を整備してきました。ただし、片桐さんが基調講演で述べたように、日本の警察が平成に入る以前から多数の警察官を警備対策官や警察アタッシェとして在外公館に派遣していたこと、また、情報通信局という技官集団の組織を警察庁が抱えており、コンピュータにも通暁した職員も多くいたことがグローバル化やデジタル化に的確に付いていけた理由であることは忘れてはいけないことだと思います。

組織体制については、警察法を累次改正して、平成６年の改正でグローバルな犯罪対策の推進に主導的な役割を果たすべく国際部が設置され、また、通信局が情報通信技術の飛躍的進展に対処できるよう情報通信局に名称変更されました。11年、サイバー犯罪対策の手段として「不正アクセス禁止法」が制定されると、同年の警察法改正で情報通信局の所掌事務としてサイバー犯罪に対処するため「情報解析等の情報通信技術に関すること」が追加されました。

16年には、警察庁等がつかさどる事務として、日本国の国益等に係る国際テロ等に対処するための態勢に関すること、また、国際刑事警察機構、外国の警察行政機関等との連絡に関することをそれぞれ追加しました。あわせて、刑事局に組織犯罪対策部を、警備局に外事情報部をそれぞれ設置しました。さらに、デジタル化等に対応するため、警察庁等が統轄する事務として「情報技術の解析に関する事務」を追加しました。

26年には「国際テロリスト財産凍結法」が制定され、それに要する費用が国庫支弁対象となりました。

なお、国際テロ等に対処するための権限行使に係る警察法の改正の状況は、第１部での板橋さんの報告を参照してください。

サイバー空間の特質と警察規制の在り方

松尾：ICT（InformationCommunicationTechnologyの略）の「フリー＆オープン」の原則の下、誰もがより便利でより良い空間にしようと、自由で自立した個人が競争するとともに、互いに助け合う世界観が支配するのがサイバー空間。しかし、そこは「保安官のいない西部の大平原」です。保安官、すなわち規制する公的機関がないのをいいことに好き勝手なことをするアウトローも多数います。そのことがサイバー犯罪、サイバー攻撃、さらにはサイバーテロの横行につながり、善良な人々に害をなしているのです。「フリー＆オープン」の原則があるサイバー空間だといっても、恣に発信していいわけでなく、自ずと節度というものがあるのが社会の常識ですが、その常識が通用しない連中がたくさんいるわけです。

どうしたらよいかということですが、当事者同士で法＝ルールを作り、それを逸脱する事態に対しては、別に仲間内で自主規制として規範を作る、それらによってリスクを制御するとともに、それを逸脱する者に対して何らかの制裁を加えてサイバー空間の安全・秩序を維持する

ことが、ICT 発展の歴史を見ると主流だとされています。また、サイバー空間の特質として、守るべきルールが決まればそのルールに沿ったプログラムを組めばそのとおり動きます。ルールの遵守の実効性ということでは、現実空間より確実です。したがって、社会の秩序や安全性に関して守らなければならないルールを事業者同士で決め、それをプログラムにすればよいのです。問題は、当事者のやる気ですが、これについては、社会全体としてモニターしていくことが必要だと思います。

とはいうものの、サイバー空間の下部にある現実空間（社会生活や社会インフラ）の脆弱性を突き、ICT を悪用するサイバー犯罪、さらに社会インフラや企業システムを麻痺させるサイバー攻撃やサイバーテロをより少なくし、サイバー空間をより安全に、また、秩序あるものにするためには、公共の安全と秩序を守る警察の捜査等の関与が必要です。その際、警察だけが頑張るのでなく、官学民が協力していかなければならないと思います。具体的には、最先端の ICT を活用して、①警察を含む政府の「情勢の変化を見据えた」積極的な取組、② JC3（日本サイバー犯罪対策センター）にみられるように企業・大学を含む社会が一体となった対策の推進、③国境の垣根を越えた連携の確保が必要です。

サイバー攻撃やサイバーテロへのグローバルな対応の枠組みについて、坂さんが第 1 部で紹介しているのでご参照ください。

片桐裕：サイバー空間での規制の在り方について、実務に即して私の考えを述べたいと思います。

私は警察庁生活環境課長時代にインターネットポルノ営業を規制する風営法改正に携わったことがあります。そのときにも、「無限の可能性を有するインターネットの空間は自由であるべきであり、公権力が規制を及ぼすべきではない」といった批判がありました。しかし、我々の主張は、ネット空間にも現実空間とパラレルの規制を及ぼすべきであり、現実空間で規制されることがネット空間では規制されないというのはおかしいというものでした。つまり、現実空間ではポルノビデオショップには届出が義務付けられているのに、ネット空間でポルノ映像を流す営業に何ら規制がないのはおかしいという考え方で、法改正して届出義務を課しました。これは、ネット空間のコンテンツ規制としては初めてのものだったと思いますが、国会からもマスコミからも大きな批判はなかったと記憶しています。その後、警察庁は、出会い系サイトに現実空間のテレクラ営業と同様の規制をしましたし、インターネット・オークションサイトにも現実空間の競り売り営業と同様の規制を及ぼしています。自主規制で何事もうまくいくのであればそれでもいいかもしれませんが、ネット空間はそんなに生易しいものではないと思います。ネット空間にも現実空間とパラレルの規制というのが、従来からの警察の考え方だと思います。

なお、これとの関連で、東日本大震災の時に、様々なデマ情報が飛び交いましたが、警察では、調査の結果明らかなデマと判明したものについては削除するようプロバイダーに要請しました。これについても、「ネット上の問題はネット上で解決すべきだ」との批判、つまり、ネット上の情報の真偽はネット参加者がネット上で決着をつけるべきで、公権力が立ち入るべきではないという批判がありました。しかし、非常事態においてパニックを防ぐためには、そのよ

うな考え方でいいのか、社会の混乱を防ぐため、警察はできることはすべきではないかと私は考えます。

板橋功：テロリストもインターネット、SNS を活用して、その進化を巧みに利用しています。そもそも今のテロというのは「過激化」によって起こっているわけで、何で過激化していくかというと、以前は過激なモスクで説法を受けて過激化されたのですが、今はインターネット上で過激化していくのがほとんどであります。この問題点は、モスクで過激化していく連中というのは割と目に見えます。なぜかというと、そのモスクを誰が利用しているかを把握できる。ところが、インターネット上で過激化している人間は、もう探知が不可能と言っていい。

それから、爆発物の製造方法もインターネット上でどんどん拡散しています。大学生や高校生が簡単に製造できるようになってしまっている。それから、ターゲットの選定も、グーグルストリートビューを使えば地球の反対側からでも選定できるような時代になっている。今や建物の中までインターネットで見られるような時代になっているということで、こういうものをテロリストも活用しているということであります。

松尾：インターネットで過激化するメカニズムについては、一般的なサイトからだんだん過激なサイトへ誘導していくように仕込むと、あたかも自分が見つけ出した「真理」と信じ込むのだという話を聞いたことがあります。また、インターネットでのテロ等の犯行の使嗾（指図してそそのかす意）が具体的な犯罪の教唆として罰せられないとされています。ということは、組織としての意思決定を個別的、物理的に伝える必要がなく、犯罪組織内のネットワークを把握して監視するという古典的な捜査手法は、インターネットでの使嗾に感化されて行うローンウルフ型のテロには無力と言えます。これに対しては、犯罪を知った場合は警察に通報する義務をプロバイダーに課すなどの新しい対策が必要になると思われます。

関連して、サイバー空間でのトラブルを見ると、サイバー空間ならではの特徴があります。先日、顔にぼかしが入っているが特徴ある帽子を被った人物が映っている防犯カメラの画像を見て、同様の帽子を被った人物の画像を SNS から見つけ、また、他の情報からそれが誰であるかを「特定」し、犯人は某女だと実名を SNS に投稿し、あっという間に犯人として拡散させたことがありました。投稿者の弁によると、一連の作業により、また、全身の雰囲気がよく似ていたこともあり、某女が犯人であることを「確信」していたとのことです。

捜査では、容疑者を割り出し、被疑者として特定し、被告人として裁判にかけ、有罪となって初めて法律的に犯人とされるのであり、捜査に携わった者から見れば、その確信は非常にもろいものであることはすぐに分かりますが、サイバー空間では、それが簡単に「真実」となって他人の人権を侵害する怖さがあります。

デジタル化と交通警察

矢代隆義：社会のデジタル化の視点で交通警察を眺めてみると、デジタル情報技術の進化・普及は 2 つの変化を交通警察に及ぼしており、また変化を求めていると思います。

1 つは、今警察が持っている各種の取締器材や膨大な免許データ管理、交通信号制御・交通

管制等の各種システムへの影響です。デジタル情報技術の導入により、これらの資器材やシステムは既にこれまでも大きく変化してきていますが、これからも新しいものが出てくるでしょうし、また現状の機材やシステムも機能が大幅にアップし、多様化するでしょう。

特にデジタル情報技術による交通管制の高度化は、目を見張るものがあります。交通の分野におけるデジタル情報技術の活用は、平成7年の横浜における第2回ITS世界会議以降、総称してITS（Intelligent Transport Systems）と呼ばれておりますが、警察庁は、5年に交通管制システムに多様な機能を付加するUTMS構想を策定し、走行車両の感知と併せて車載の送受信機との双方向通信機能を有する光ビーコンを導入しました。従来から交通警察は交通管理の一手段として道路交通情報の提供に力を入れていましたが、この新しく導入された光ビーコンを用い、走行中の車両の送受信機に直接交通情報を画像の形で提供できるシステムを開発しました。そして8年には、警察と道路管理者の情報収集・提供システムを統合したVICSを社会実装しています。

信号の制御方式も高度化し、8年にはセンサーで収集したデータから直接信号機の制御パラメータを算出するモデラートと呼ばれる制御方式を導入しております。その後、予測制御、進行方向別制御等の拡張機能も開発されました。また、UTMS構想に基づき、公共車両優先、現場急行支援等のいくつかの信号制御に係る交通管制システムのサブシステムも実用化されております。

初期のITSの代表的なものは、カーナビ、VICS、ETCですが、技術開発は止まることはなく、今はASV（先進安全車）を経て自動運転に関心が移っています。平成における道路交通の最大の特徴は、ITSの出現とその進展であるといえます。

もう1つは、デジタル情報技術により車社会が変化し、これに対する警察の交通管理の在り方も変わってくるということです。車社会の何が変わるかといえば、まず1つ目に、車自体が変わります。自動車のインテリジェント化がますます進み、車両の構造・装置機能は大幅に高度化します。そして、様々なレベルの自動運転が実現していきます。2つ目に自動車と外部との接続、つまりコネクトビリティが飛躍的に高まります。いわゆるコネクテッドカーが普及し、テレマティクスの活用で、車内にいながらにして社会の各システムとつながるわけであります。3つ目に、車の利用形態は、保有から使用へと移行していきます。つまり、多くの人にとって車は持たなくても利用できればよいということです。したがって、従来ですと車は自家用車にプラス、バス・タクシーという組合せであったわけですが、今後は従来のバス、タクシーに加え、タイプの異なる様々なモビリティサービスが大きく展開していきます。いわゆるMaaS（Mobility as a Service）です。そして交通社会におけるその比重が高まるわけであります。

（中略）

デジタル化・グローバル化とサイバー警察

坂　明：このシンポジウムを通じて、治安のそれぞれの分野でこれまで戦略的な官民連携施策が進められてきていることを改めて認識しました。そういう意味ではサイバー警察の方も、敵は強大ですし組織化されていますので、民間の方々のご意見も踏まえながら、一緒になって目指

すべき目標を共有し、戦略的に対策を進めていかなければいけないと改めて思ったところです。

サイバー犯罪においても、攻撃者・犯罪者の手法といいますか、手口を知らないと対策をとることが難しい面があります。さらに、国家等のステートアクターも含め、攻撃者・犯罪者は何を狙っているのかを、背景も視野に入れて理解していく必要があります。これらは、情報共有を進めてこそ分かるものがあります。その際、単に一般的に情報を共有するだけではなく、具体的に対抗するための対策面で協働するための実践的ともいえる情報共有が必要になってきます。このような取組は、国際的に見ても徐々に成果を上げつつあり、日本でも JC3 をはじめとする様々な取組がありますので、今後に期待したいと思います。

サイバー犯罪・攻撃はこれからもなくなることはありません。安易に、罪悪感なく、大きな経済的利益を手にすることができるのですから、これまでよりも更に増加することでしょう。情報や知的財産を狙った攻撃、サイバーエスピオナージにしても同様です。国家を背負い、誇りを持って一企業を攻撃してくるということもあり得ます。それを踏まえると、一人ひとりが、日常のサイバー防犯対策を心掛けるとともに、社会や公的機関がそれを支援するという、現実の犯罪への対策と同じレベルでの取組が求められていると思います。企業、公的機関、行政機関に対する犯罪・攻撃についても同様の状況があるかと思います。

2020 年のオリンピック・パラリンピックは多くの方々が力を合わせて成功のために取り組んでおられますが、サイバー対策についても同様です。日本、そして世界の多くの方々が協力してサイバーセキュリティ対策に取り組み成果を上げることでレガシーができれば素晴らしいことと考えております。私も微力ながら力を尽くしていきたいと思います。

デジタル化と生活安全警察

石附弘：生活安全警察にとってデジタル化時代の環境は、相当に厳しいものになると思います。要は、技術の進歩が速すぎて、有効な対策が打てない、そのスピードそのものが生活安全の脅威になっている、だからこそ「コミュニティ」内の情報共有や連携が必要と思います。先日、有楽町で「世界デジタルサミット」が開催され、そこでは IT 時代から既に DT（データ・テクノロジー）革命に突入ということで、時代が急激なスピードで進んでいると紹介されました。

このデジタル情報世界（デジタル空間）については、平成 30 年のダボス会議でも「サイバー攻撃」と「データの不正利用や窃取」が社会経済上のグローバルリスクとして上位を占め、警察白書でも犯罪の場となったり、犯罪に巻き込まれたりすることが、国民の体感治安不安の原因の首位に躍り出ました。デジタル空間の素晴らしい世界の裏側で想定外の脅威が生み出されています。かつてゲーテは、「光の多いところには、強い影がある」と言っていますが、影への対策が急務です。

SC の「C」（コミュニティ）の言葉はギリシャ語に由来し、その原義は「外敵（共通のリスク）に皆で手を携えて戦おう」という意味の合成語だそうです。すなわち、現下のデジタル化等の大きな環境変化の下で次々に出現する未曽有の地域課題に対して、コミュニティの成員一人ひとりが「わがこと」として知恵を出し、官民・民官・官官・民民の知恵を集め、さらには海外

の知恵も学んで、安全安心のために最善を尽くそう、また、これを脅かすリスクや危機に立ち向かって戦おうというのが、SC の原点と考えます。

視点を変えてみると、暴力団の検挙罪種においても、近年、詐欺・窃盗が増えています。先ほどからサイバー犯罪が話題になっていますが、電子キーで車を盗むとか、スマホで指紋を採るとか、防犯カメラの偽装、ストリートビュー、こういういろいろな新技術が犯罪者の側に悪用されています。

これらに対抗する予防安全の新技術とコミュニティの知恵をどう構築していくのか、その際、生活安全分野で新技術をどうやって活用していくのかを、もっと早く開発・研究・社会実装しなければいけないと思います。京都府警察で ICT を犯罪予測、防犯パトロールに使おうという動きがあります。お金はかかりますが、予防という観点からは必要不可欠な投資と考えます。

現実空間からサイバー空間への犯罪の移動

石附：人のつき合う範囲は、歴史的に見ると、家族、近隣、地域等の顔が見える関係から、だんだん相手が見えない世界での生活を余儀なくされる関係になりました。インターネットだと将来的には 100 億人相手の時代になるわけです。つまり人間は、「顔が見える世界」と「顔が見えない世界」の 2 つの異なる世界に棲む両生動物になったのではないかとの思いがします。

となると、顔が見えない世界での犯罪対策は顔が見える世界での犯罪対策とは違う側面が必要になると思います。

近年、「だまし」が学問上も実生活においてもメインテーマになってきました。「嘘や欺瞞行動に対する国際学会」がケンブリッジ大学で開かれたり、日本でも、「欺瞞的コミュニケーション研究会」が開かれたという新しい動きが出てきました。東京大学の公開講座（平成 23 年）で、「霊長類は進化するほど脳の大脳新皮質の比率が高くなり、複雑な社会的環境への適応が脳の進化を促す。だから脳の進化というのは、普通の人も善良な市民もそうですし、犯罪者も同時に進む」という話も出ました。

サイバー空間の被害、とりわけ詐欺については、顔が見えない、すなわち非対面の犯罪であり、被害回復が困難と思われます。シェイクスピアは、「詐欺は、この世からなくならないだろう。何故なら人を騙すことは楽しいからだ。したがって被害の予防もさることながら、騙された時にどうするかを考えておくことが大事だ」と警告しています。

これは、我々の子供時代の「人を見たら泥棒と思え」の安全教育を、「人を見たら詐欺犯と思え」に変えるとともに、騙された時のセーフティネットの構築が急務と思います。

坂：第 1 部でも述べたように、一般の犯罪では 14 年がピークで以後減少を続けていますが、サイバー犯罪はそこから増加を始めているとも考えられます。

つまり、現実空間での犯罪認知件数が減る一方で、まずは経済的な利益を狙った本格的なサイバー犯罪が増加し、26、27 年あたりから、情報窃取なども含めて更に増加し、現在に至っているものと思われます。

片桐：先ほど、サイバー犯罪や非対面の詐欺では、未遂のほとんどが暗数になっているというお

話をしましたが、実は未遂に限らず、被害の発生している既遂事案でも多くの未届事案があるのではないかと思います。法務省等が行っている暗数調査を見ると、特にサイバー系の犯罪で暗数が多いというデータがあります。警察は、こうした犯罪統計には現れない多くの暗数、すなわち未届け事案や未遂が存在することに留意すべきだと思います。未届け事案や未遂事案には、抑止や検挙にとって極めて有用な情報が含まれていますので、警察は、これをきちんと吸い上げて活用する努力をすべきです。先ほども述べたように、統計上の犯罪の認知件数が減ったことを喜ぶのでなく、そもそも被害が発生しないよう、検挙だけでなく抑止対策に力を入れていくべきだと思います。

（中略）

現実空間とサイバー空間の融合

坂：デジタル世界と現実世界の融合というか、一体化みたいなものが本当に進んでいると思います。昔からサイバー・フィジカル・システムといわれ、両者は密接な関係であると言われてきましたが、今や本当に一体化していると感じています。

松尾：サイバー空間と現実空間の融合を私なりにまとめると、場所を気にせず（現実空間の領域的制限を緩和し）、時間差なくリアルタイムに（時間的制限を緩和し）したいことができるようになることで、それを科学技術として促進するのがICTということです。

ディープラーニング等を用いたAI技術によって進展している自動運転技術に典型的に見られるように、現実空間をコントロールできるようになってきました。加えてIoT技術等の進展によって現実空間にセンサーが埋め込まれ、様々な状況でデジタル処理が可能になり、それが現実空間にフィードバックされて社会の役に立っています。一例を挙げると大規模プラントで製造制御のための膨大なセンサーから集まるビッグデータをAIで分析することで、正常の値（これもAIが計算します）と違うデータの振る舞いを検知し、部品が故障する前に予知し、大規模事故の発生を防止するようなことも現実にできます。

このような状況の中、ビジネスの世界では、デジタル化の加速によって、個別の企業だけでなく社会全体の生産性と利便性を高めることで社会的課題の解決につながる製品・サービス、さらには産業等を創造する動きが進んでいます。警察においても、矢代さんが指摘されたように既に交通警察では対応を開始していますが、他の分野でも対応を検討すべきところもあると思います。

デジタル化への今後の対応に関して、石附さんが別の機会に「警察官たるもの、AIではできない能力PI（Policeman Intelligence）を発揮するようにしなければならない」と述べています。デジタル化の更なる進化により人間はAIに全て置き換えられるのではないか、という考えがありますが、私はそんなことはないと思っています。例えば、人間には複雑な状況を瞬時に判断できる能力があります。自動運転を例にとれば、人間には比較的簡単にできる、横断歩道の端に立っている人が渡ろうとしているのか、車が通るのを待っているのかの判断をAIが瞬時に行うのは大変難しい。それを間違えると事故になるし、安全を重視しすぎて人影を認知したら全て止まるようにプログラムすれば至るところで渋滞が起きたり、追突されたりする

ことになりかねません。

もちろん、AIは人間には真似のできないビッグデータ処理能力があります。警察においてもAIのそのような能力は活用しつつ、PIに磨きをかけ、警察官にしかできない仕事で成果を出すようにしていかなければならないと思います。

以上

警察政策学会資料　第 120 号

サイバー空間と警察

令和 3（2021）年 10 月

編集　管理運用研究部会

発行　警察政策学会

〒 102－0093
東京都千代田区平河町 1－5－5　後藤ビル 2 階
電話（03）3230－2918・(03－3230－7520)
FAX（03）3230－7007