警察政策学会資料　第124号
令和４（２０２２）年８月

サイバー空間における安全安心の確保

警察政策学会
管理運用研究部会
情報技術犯罪対策研究部会

まえがき

我が国の犯罪情勢は、20年前の平成14年(2002年)の刑法犯認知件数約285万件が、昨年（令和3年）には約56万件と、ピーク時の5分の1になった。統計上は、日本は「世界一安全な国」に戻ったといえる。これを受け、政府広報室の「治安に関する世論調査」（令和3年12月～4年1月）によれば、「日本は安全・安心の国か」との問いに85.1％の人が「そう思う」、「どちらかと言えばそう思う」と回答している。ちなみに同じ質問に対する回答は、5年前（平成29年）が80．2％、10年前（平成24年）が59．７％であった。

ところが、同じ世論調査で、「ここ10年で日本の治安はよくなったか」という問いに対し、54.5％の人が、「悪くなった」「どちらかといえば悪くなった」と回答している。なぜこのようなことになるのだろうか。

その答えのヒントになると思われるのが、「自分や身近な人が被害に遭うかもしれないと不安に思う犯罪等は何か」という問いに対して、

○特殊詐欺や悪質商法などの犯罪　52.6％、

○不正アクセスやフィッシング詐欺等のサイバー犯罪52.3％

との回答が最も多かったこと。不安に思う犯罪として、サイバー犯罪よりも多かった特殊詐欺も、非対面の電話というツールを使っていること、また、悪質商法のかなりの部分がインターネットを舞台にしていることを考えると、これらも広い意味ではサイバー犯罪といえる。となると、国民が被害に遭うかもしれないと不安に思う犯罪は圧倒的にサイバー犯罪ということになろう。つまり、サイバー犯罪への不安が体感治安を悪化させているといえる。

なお、同調査では「日本社会の治安をどう思うか」との問いに対して最も多い回答（64.4％）が「偽の情報を含め、様々な情報がインターネットで氾濫し、それが容易に手に入るようになった」ことであった。つまり、3分の2の国民がサイバー空間での「アノミー（無規範状態や無規則状態)」を憂いていることがわかる。

関連して、同じ世論調査での「自分や身近な人が犯罪に遭うかもしれないと不安になる場所は？」との問いに、「インターネット空間」と答えた人が、「路上」、「繁華街」を抑えて第一位となっている（統計数字は、それぞれ、53.9％、50.7％、

47.9％）。ちなみに、10 年前の調査では、①「繁華街」（53.7％）、②「道路上」（53.6％）に次いで、③「インターネット空間」（41.9％）であった。

これらを総合すると、サイバー犯罪は、平成の後半から令和にかけて、減少を続ける一般犯罪を尻目に増加を続けているというのが、サイバー犯罪の研究者やサイバー犯罪の取締に当たる実務家の率直な印象であろう。

ところで、サイバー空間について、筆者はこの分野に本格的に関心を持ち始めた数年前に、①「保安官のいない西部の大平原」、②能力のある若い人が自由に羽ばたける「戦後の闇市」のような空間との描写に共感した。前者は文字どおり、警察等の取締機関がない世界、後者は、諸般の理由で警察が弱体化していた世界であり、それをいいことに好き勝手をするアウトローが多数存在していたともいえる。そして、その延長で、現在、サイバー犯罪、サイバー攻撃、サイバーテロやその準備行為の横行につながり、善良な人々に害をなしているといえるのではないだろうか。

このような状態に対してどうしたらよいのだろうか。

サイバー空間をもたらした ICT の発展の歴史を振り返ると、ほとんど規制のない中でプレイヤーたちの競争と自己規制で秩序を作ってきた。これに対して、警察は早い時期からまず、行政面では、「サイバー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サイバー空間で規制されないのはおかしい」という立場をとり、実際に現実空間のポルノショップに課されている届出義務を、インターネットでポルノ映像を流す営業に課す法改正を行った。また、捜査面では、当事者の自主規制だけに頼るのではなく、警察等の捜査機関の一定の関与が必要との立場をとり、取締を行ってきた。

これらが、今般の「サイバー空間にも現実空間と同等の安全安心を確保する」ことを目的にした警察制度の改正につながったと理解している。6 月 9 日のフォーラムは、警察の新しい体制についての期待や課題を論じることを目的に開催したもので、本資料はその結果をとりまとめたものである。

松尾　庄一

目　次

サイバー空間における社会安全政策

四方　光

私が与えられた題は「サイバー空間における社会安全政策」なので、最初に社会安全政策論とはどのような理論であるのか紹介し、その観点からサイバー空間、サイバー犯罪の特徴を述べた上で、サイバー犯罪に関して今後検討すべき課題２点について話をする。

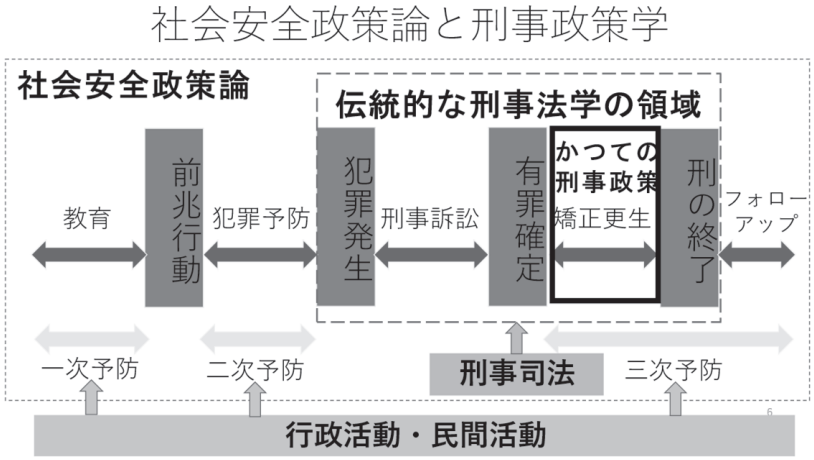
１　社会安全政策論とは

社会安全政策論は、私の師匠である故渥美東洋中央大学名誉教授と警察政策学会、警察政策研究センターが一緒になって構築した犯罪対策論。渥美先生は、犯罪者処遇論に限られない欧米で議論されているような総合的な犯罪対策を日本でも興そうという観点があったと思うし、警察は、警察幹部の暗黙知を理論化するという目的があり、それらが合致してできたものと理解している。

既存の学問である刑事政策との相違を見ると、刑事政策を含む刑事法学は、伝統的には犯罪が発生してから刑の終了までを扱った学問であるといえる。これは近代法の侵害原理に従って、犯罪という他者への侵害行為があった後に国家機関が個人に強制的に介入でき、その介入が正当化されるのは刑の終了までという理解が背景にあったものと考えられる。

しかし、DV、ストーカー、児童虐待等の犯罪の問題の重要性が認識されるようになり、被害者が死亡したり、重傷障害を負ったりした後に犯人を検挙して刑罰を与えたとしても誰もハッピーではないではないか、被害が生じる前兆が分かったのであれば未然防止すべきではないかという、至極まっとうな国民世論と、平成の半ば、刑法犯認知件数が未曽有の増加を見せ、刑事司法という後追いの対応では対処が追い付かないようになったことにより、犯罪予防の重要性が認識されるようになった。

さらに近年では、刑が終了して刑務所から出所しても、泊るところも仕事もなくやむを得ずホームレスをしてついにはまた犯罪を犯す者が意外に大勢いる、何らかの福祉的、医療的なサービスを適切に提供すれば再犯を防止できる者がかなりいるのではないか、したがって再犯防止のた



めには刑の終了後も一定の関与をしていくべきではないかという議論がなされるようになってきている。

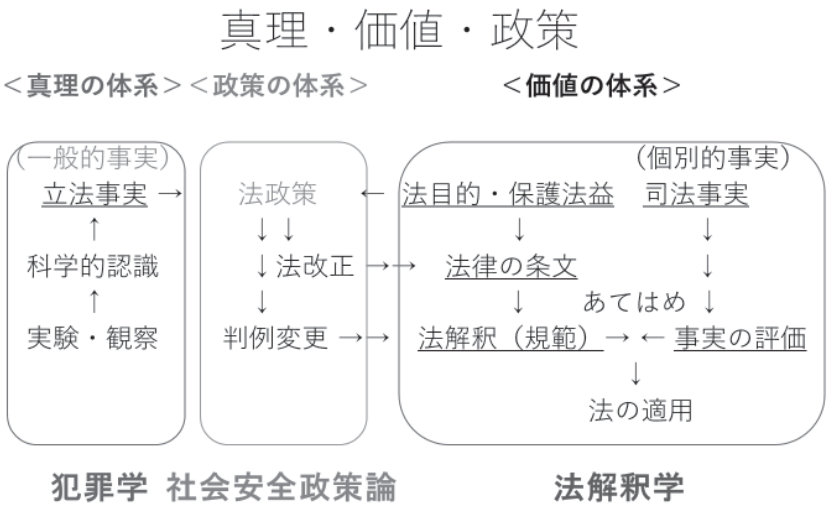
社会安全政策論は、こういう議論をもう 20〜30 年も前からしてきた。

社会安全政策論では、政策の基礎になる事実関係を科学的に把握するということも重視してきた。伝統的な法解釈学では、法の目的や保護法益といった法的価値に照らして法の条文を解釈し、それによって定立された規範に、法の適用対象となる個別の事実（司法事実）があてはまるかという議論をしてきた。

これに対し、立法などの政策を論じる社会安全政策論は、立法事実や政策の基礎となる事実、すなわち単なる個別の事実ではなく今後適用すべき法律や政策の基礎となる事実であるから今後当面の間は妥当する事実関係、一種の社会法則の認識を重視している。日頃立法に従事している霞が関の官僚にとっては立法事実が重要であることは当然のことだが、法解釈学では現実の事実関係を法理論の中に取り入れる理論的枠組みが明示的に整備されているわけではない。

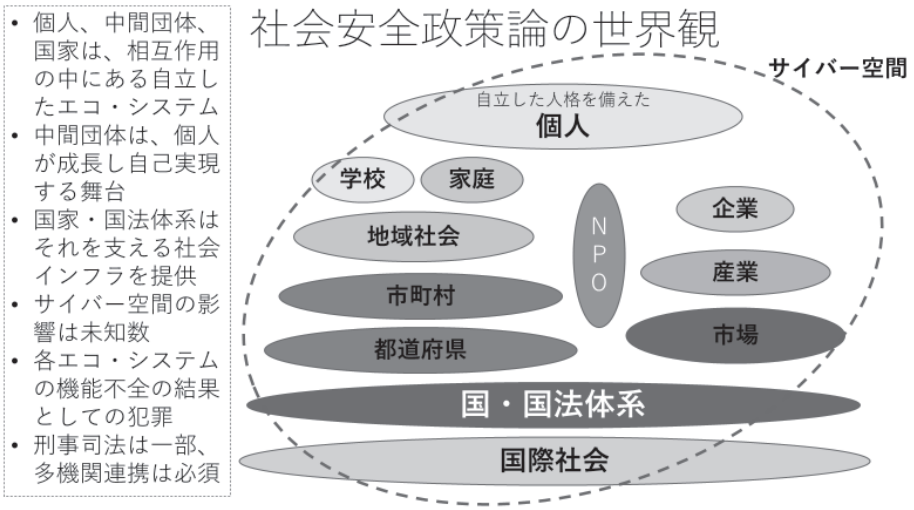
社会安全政策論は、このような事実関係をできれば科学的に認識すべきと考える。もっとも、物理学を理想とする近代科学の方法によって法的事象をよく把握できるのかという問題はあるが、この点は本日は時間の関係で割愛したい。

そのように現実の事実関係を把握した上で、法的価値に照らして何が改善すべき問題であるのかを特定し、うまく改善するための立法技術、政策的な技術を提案するのが、政策論としての社会安全政策論。



さらに、社会安全政策論は、警察幹部の暗黙知がそうであるように、犯罪対策を研究する理論ではあるが、目の前の犯罪事象だけを見るのではなく、社会全体の仕組を見て、その中でどのように犯罪事象が生じるのかという視点を持っている。

各自自立してその尊厳が尊重されるべき存在である個人が、家庭・学校・地域社会の構成員としてその中で成長し、やがて企業等の組織を舞台にして活躍し、自己実現を達成する。また、家庭・学校・地域社会を支える存在として自治体があり、企業が活動する場として市場がある。さらにそれらの土台を形成するのが国家や国法体系であると考えることができる。

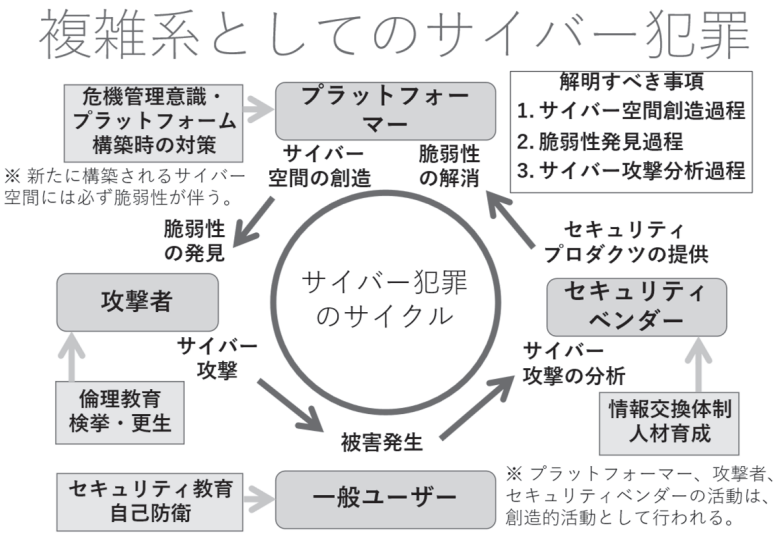


２　サイバー空間・サイバー犯罪の特徴

スライドにおいて点線で囲んだところが、サイバー空間。サイバー空間は、現実空間の諸階層に対して横断的に大きな影響を与える人間や企業の新たな活動空間となっているが、いまだその在り方や影響は十分には解明されておらず、その解明が急がれている。

サイバー空間は、急速に変化する。このような急速な変化の比喩として、「ドッグイヤー」という言葉がしばしば使われる。犬の寿命は人間の７分の１なので、年月が流れるスピードは人間の７倍早い、同様にサイバー空間は現実空間の７倍の速さで進展しているという趣旨である。

このようなサイバー空間の変化は、プラットフォーマーやICT技術者など人間の創造力によって内発的に生じるもので、偶然や歴史法則によって生じるものではない。これまでの現実世界における産業の進展も人間の創造力によってなされてきたが、このことはサイバー空間において顕著である。サイバー空間では、技術革新が価値を生むので、プラットフォーマーやICT技術者などは、利益を確保するためには次々に新たな技術を生み出し、市場に提供し続けなければならない。このようにサイバー空間の進化は、「ドッグイヤー」のスピードで内発的、継続的に生じるようにそのメカニズムの中に組み込まれている。



そうすると、新技術を生み出すプレッシャーに晒されているプラットフォーマーやICT技術者などは、脆弱性がまったくない完璧な商品やサービスを開発する余裕はなく、多少の脆弱性を抱えたまま次々に市場に投入しなければならない。サイバー犯罪の犯罪者は、このような新たな脆弱性を次々に見つけて、被害者から不当な利益を得る手法を生み出す。これに対し、認知された被害をもとにセキュリティベンダーが脆弱性への対処方策を考案するが、それを待つまでもなく新たな脆弱性を抱えた新たな技術が市場に提供され、犯罪者は新たな手口を発見できるようになる、ということが繰り返されている。

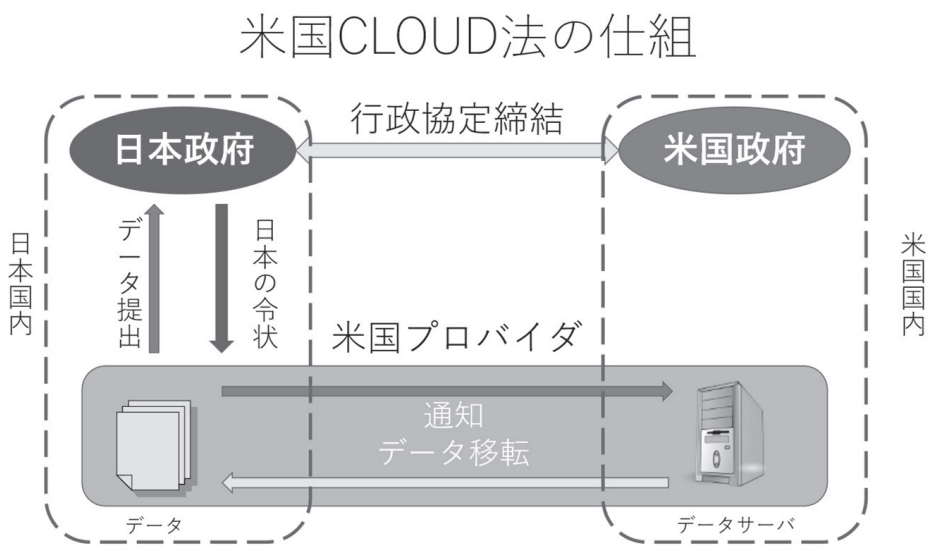
そこで、第一に、サイバー犯罪対策においては、サイバー空間やサイバー犯罪の変化への迅速な対応が重要になるし、第二に、サイバー空間の変化による人間の生活様式の変化への影響は、犯罪者・被害者・犯罪機会にどのような影響をもたらすのかを解明する必要がある。

3　課題（1）：技術的変化に対応した迅速な法整備

サイバー犯罪対策における我が国の現行法の課題を端的に述べると、①国境の壁が越えられない、②サイバー空間の秘匿性を打破できない、③これらの課題を解決する海外の取組に日本が追い付いていないということが挙げられる。

具体的には、米国クラウド法行政協定の締結、ポリスウェア等の捜査手法の導入、グルーミング処罰規定の導入等が、今後の課題になろうかと思う。

クラウド法は、捜査機関が国境を越えようとすると大変な時間がかかるので、国際企業たるプロバイダにおいてデータを国境を越えて移転してもらおうというもの。イギリスとオーストラリアが既にこの行政協定を締結している。もっとも、個人情報の海外移転という観点からは問題がないわけではないので、相手国が十分な個人情報保護法制を有していることが行政協定締結の要件となっている。EUのGDPRのようにアメリカより厳しい個人保護法制を有している場合には行政協定を締結しづらいという問題が生じるが、捜査上必要な情報の越境取得はEUも含め大半の国で問題になっていることなので、EUでも情報取得の必要性は認識されている。



サイバー犯罪対策における重要課題として、ボットネットという一度に大量の通信を行うことができる犯罪ツールや、サイバー空間の闇市場というべきダークウェブを取り締まることが挙げられる。秘匿性の高いサイバー空間においてこれらを検挙するためには、ポリスウェアなど犯罪者特定のための技術的手段を用いることが不可欠。アメリカでは、NIT 令状という既存の令状の枠組みのなかで技術的手段（Network Investigative Techniques）を用いることができることとなっており、他方ドイツでは刑事訴訟法の改正によって同様のことを行うことができるオンライン捜索という捜査手法が導入されている。

我が国では、警察庁にサイバー警察局が設置され、関東管区警察局にサイバー犯罪特別捜査隊が設けられて、今後の捜査の進展が期待されているが、このような先進的な捜査の道具が与えられなければ、欧米先進国並みの成果をあげることは難しいかもしれない。我が国でも、今後このような捜査手法の導入を検討すべきだろう。

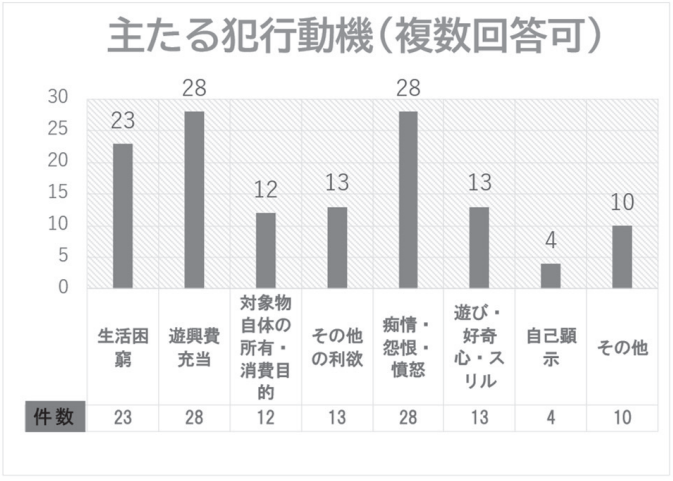
また、サイバー空間を舞台にした児童の性的搾取は、我が国だけでなく世界中で問題となっている。中でも、SNS において性的な目的を秘して児童に接近しようとするいわゆるグルーミングが多くの国で問題となっており、グルーミング行為を規制する法律が多くの国々で制定されている。中には、犯罪者の目的が児童の性的搾取であれば、実在する児童に対する誘惑等でなくても（おとり捜査官に対するものであっても）処罰の対象とする規定を定めている国もある。

我が国でも法制審議会で議論がなされているようだが、実効性のある規定の早期の制定が待たれる。

４　課題（２）：人間の生き方の変化への対応

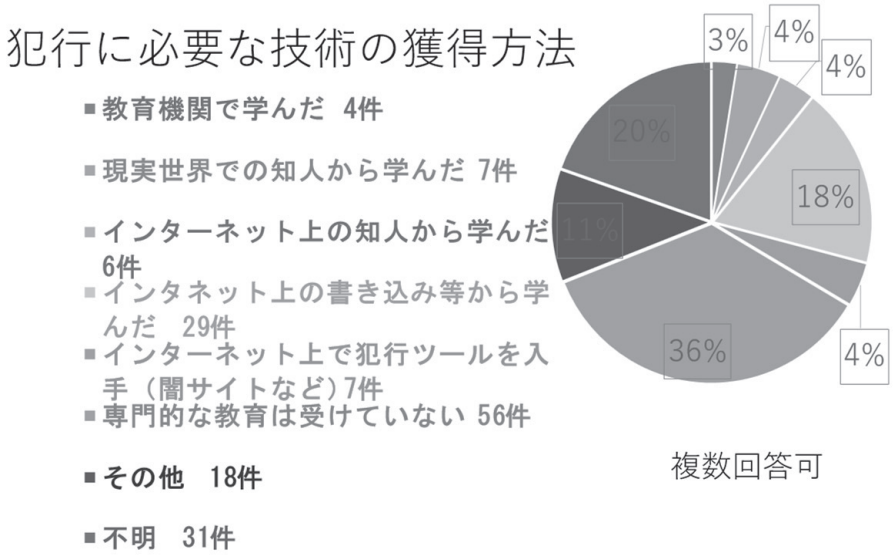
近年刑法犯認知件数が年々減少していることは皆さんご存知のとおりだが、少年の刑法犯検挙人員も急速に減少している。その速度は少子化の速度を超えており、少年人口 10 万人当たりの検挙人員（刑法犯少年人口比）も減少して、成人のそれに近い値になっている。実は、10 代半ばの男子少年の非行少年人口比が他の年生層より高いのは世界的に見られてきた現象であり、成長発達という人類共通の過程で少なからぬ少年に見られる現象と考えられてきた。

にもかかわらず、非行少年人口比が大幅に減少しているということは、少年の成長発達の過程



が変化しているのか、あるいは少年非行が潜在化しているのかのいずれかである可能性があり、いずれに対してもサイバー空間の登場と発展はその原因となっている可能性がある。

サイバー空間の出現と発展は、犯罪者、被害者、犯罪機会という犯罪の３要素それぞれに大きな影響を与えている可能性があり、早急な解明が望まれる。



上記のスライドは、2021 年に、過去 3 年間（2018・2019・2020）に 40 歳未満の者が犯した不正アクセス禁止法違反／コンピュータ・電磁的記録対象犯罪（警察が報道発表したもの）について、警察政策研究センターの協力を得て、四方と矢作由美子先生が行った、道府県警本部担当者への質問紙調査の結果の抜粋。

これによれば、①技術力を示すような動機は少なく、利益目的の犯行が多かった、②情報技術について高等教育を受けたのではなく、犯行の方法をインターネットを通じて独学で学んでいる、③簡単な犯罪であればサイバー犯罪を行うためのツールは既に国内にも出回っており、新世代の非行少年が「楽して儲ける手段」としてサイバー犯罪を行っている可能性があることが示唆されている。

５　まとめ

以上述べたことをまとめると、

- サイバー犯罪は、人間社会の内発的発展による変化が最も顕著に表れる分野であること。
- サイバー犯罪対策では、実体法、手続法、政策的対処いずれにおいても迅速な対応が重要であること。
- サイバー空間の連続的変化が、人間の人格や社会構造に及ぼす影響を解明する必要性があること。
- 政府や学会は、上記課題に対応できるリソースを用意する必要があること。

がいえるのではないかと思う。

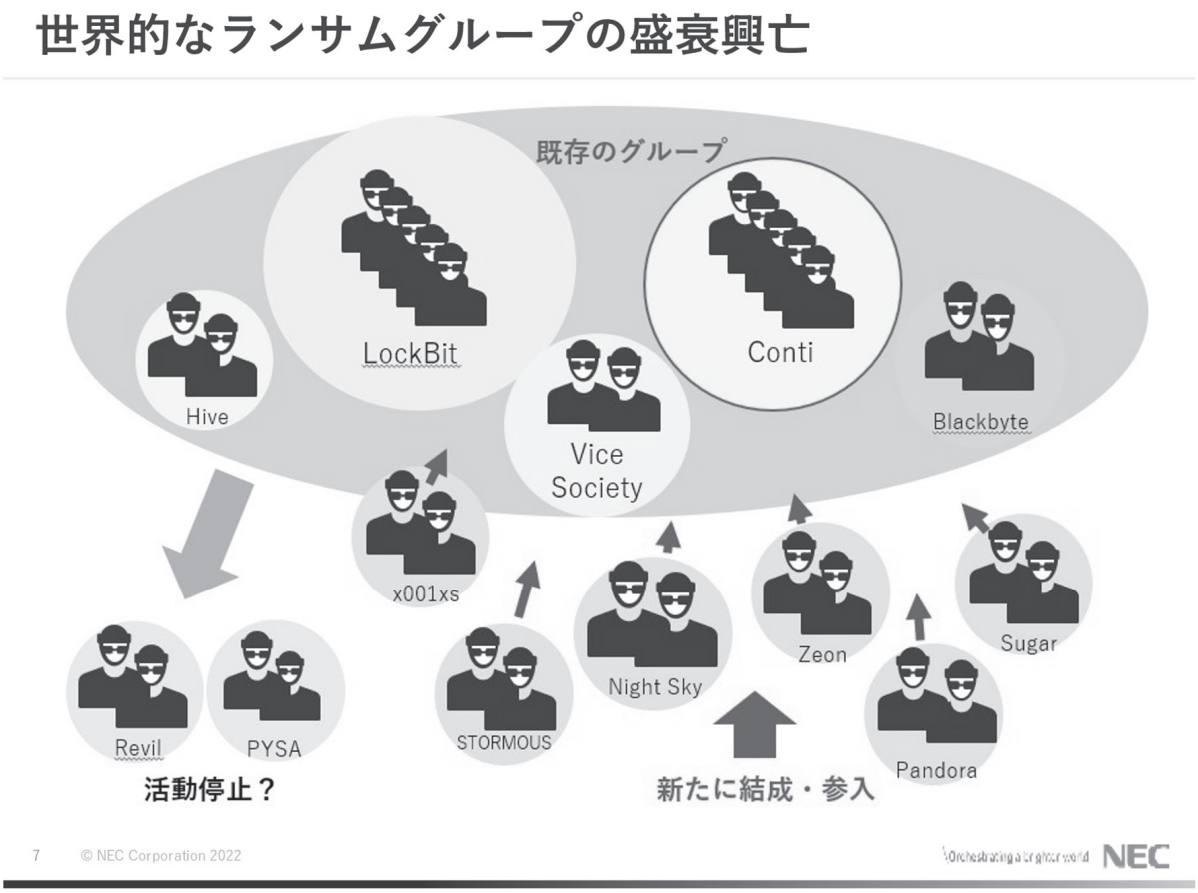
最新情勢から読み解くサイバー犯罪の近未来像と対策

木村　公也

サイバー犯罪の最新情勢

次のスライドは世界的なランサムグループの盛衰興亡を図式化したものである。現在、全世界で多くの被害を出している標的型ランサムウェアで最大グループの LockBit に次ぐ Conti は２年前に確認され、現在、全世界で多くの被害を出している標的型ランサムウェアに関連するグループである。二重脅迫（暗号化、公開）を行う悪質なグループだが、最近、ウクライナ侵攻に関し、特別軍事侵攻賛成派と戦争反対派が対立して内部分裂した。

特別軍事侵攻賛成派はロシアが中心の多数派、反乱側は少数派と思われるが、業務で使用していた６万件のチャットデータを公開、流出させ、ランサムウェアグループの高度な組織化と分業が判明した。



インターネットが登場し、素性を明かさないまま協働することが可能となったため、サイバー空間における犯罪組織では犯罪の分業が進んでいる。犯罪の全体像が見えないため、なかには違法行為の認識なく、犯罪組織に加担しているケースもある。

元々、見知らぬ者同士であるため、組織への帰属意識は希薄で、今回の情報流出でも捜査の手が身辺に及ぶことを恐れ、組織から距離をとる者も出始めており、それらがまた小さな犯罪グループを作って、再びランサムウェア攻撃の業界に参入する動きがあり離合集散を繰り返している。

なお、IT 大国とも言われるウクライナに関するエピソードであるが、従前から、コンピュータ・ウィルスは、どこからやってくるのか関心がもたれていたが、出元を遡っていく追跡は難しいことから、通信系プログラムとしてのウイルスの発信先の動向を調査すると、ウクライナを含む東欧が関連していると思われることがあった。

ウイルスの多くは通信系プログラムである。標的型攻撃以外の感染活動は、ウイルスを広範囲にばらまくため、犯罪者にとって、あらかじめ誰にうまく感染させることができるのかを知ることができない。だから、多くの場合、感染に成功したウイルス側から、犯罪者たる BOSS に「今、自分（ウイルス）は何番の IP アドレスが割り振られた PC に感染している」と連絡するように設計されている。（なお、最近のウイルスは自分自身が解析環境に置かれていることを認識し、動きを止めてしまうことも確認されているので、これらの調査は慎重にやる必要がある。）

私は、以前、複数のウイルスが感染後どこに連絡しようとするのかを調べたことがあった。当初、ネット人口が多い米国や中国ではないかと想像していたが、結果はこれらの大国に比して人口が圧倒的に少ないウクライナが多く、驚いた。今回の Conti の分裂騒動から考えると、ウクライナの周辺国の犯罪者がウクライナの脆弱性のあるサーバを乗っ取り、踏み台にしていたのではないかと思われる。

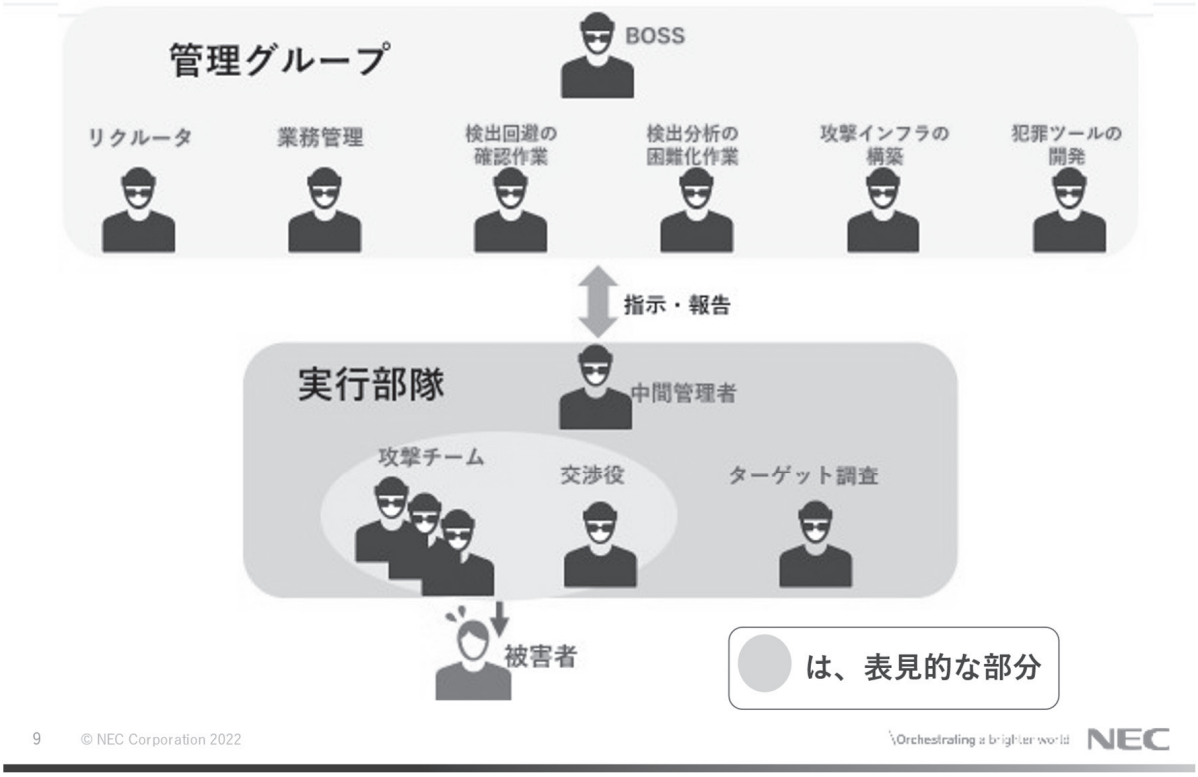
なお、東欧には、以前から、IT マフィアとか、IT ギャングなどと呼ばれる犯罪組織が横行していることは知られていた。なぜ、東欧に集中しているのかという理由は定かではないが、サイバー攻撃やセキュリティの技術の発展と戦争は密接に関係しており、また犯罪と経済状態も密接に関係しているため、絶え間なく紛争があり、経済的にも苦しい社会環境が続いた東欧で、技術的な知識を持つ一部の犯罪グループが核となり、一攫千金をもくろむ中で徐々に分派していったのではないかと思われる。また、複数の言語が話される地域において、ロシア語という共通言語の存在も犯罪組織の形成に寄与した可能性も考えられる。

サイバー犯罪組織、犯罪インフラ企業の現状

ランサムウェアを収益ツールとする犯罪グループの図式は次のスライドのとおり。

大きな特徴としては、実行部隊と管理グループに分かれていること。

実行部隊は、ターゲット調査、攻撃チーム、交渉役からなり、「中間管理者」が統括する。その上に、報告を受けて指示したり、犯罪ツールの開発、攻撃インフラの構築、エンジニアのリクルート等を行う管理グループがあり、BOSS が統括する。このように、中間管理者を設けることにより、万一、実行部隊が摘発された場合でも、管理グループに捜査の手が直接及ばないようにしている。

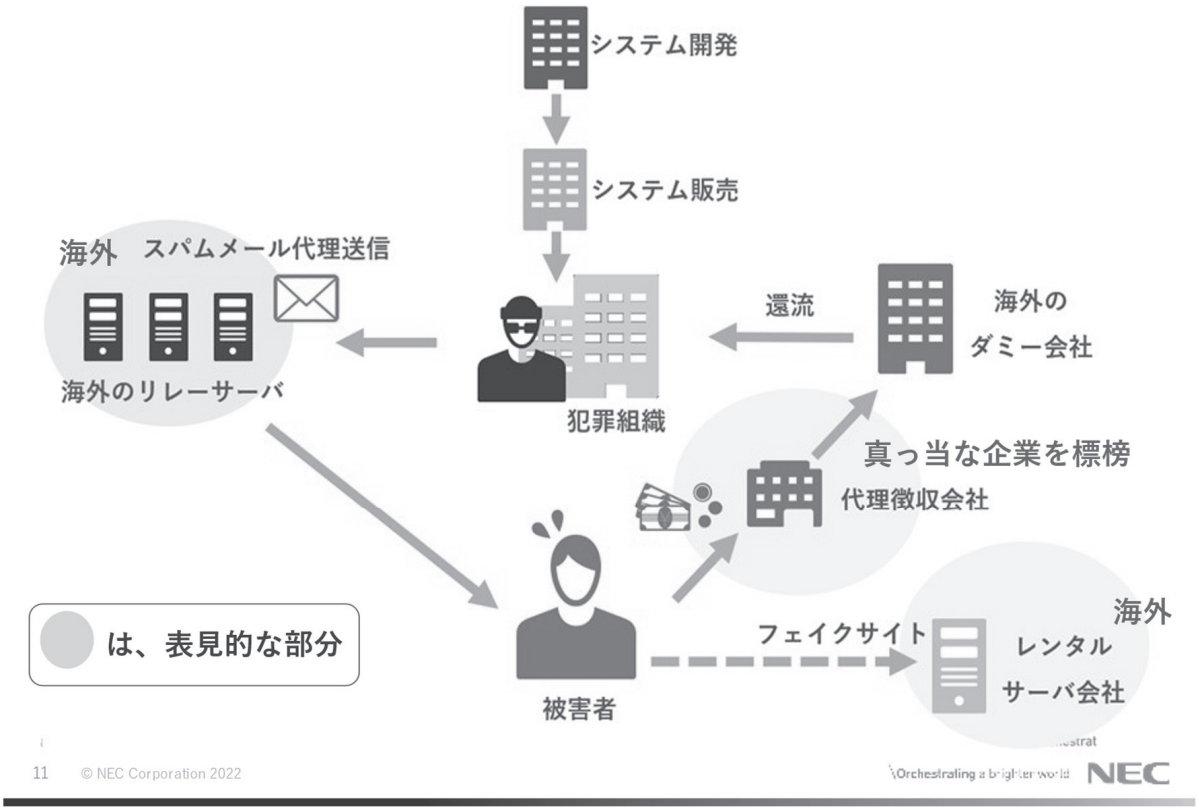


我が国を舞台にしたランサムウェア攻撃の実例をもとに、分業の実際を紹介する。彼らの中にはターゲットを探すのを仕事としているターゲット調査役がいる。ターゲット調査では、「ここなら○千万円なら払うが、それ以上要求すると警察に相談するだろう」と、コンプライアンス等の状況を見て、被害者の支払い能力を値踏みする。また、中には、経営者の性格まで調査して交渉役にアドバイスする場合もある。

我が国のサイバー犯罪組織の仕組み

我が国の一般的なサイバー犯罪組織の仕組みは以下のとおりである。

海外に拠点を置くスパムメール代理送信企業、海外のレンタルサーバ会社が運営するフェイクサイトの詐取金やオンラインカジノの賭け金等を代理徴収する「代理徴収会社」等の犯罪インフラ企業が犯罪組織と連携してサイバー犯罪を敢行している。



サイバー犯罪組織の特徴をまとめると、次のとおり。

まず、① IT を用い、分業と効率的な犯罪収益の確保を実現する、②巨額の不正な資金を短期間で獲得する。この過程で新規参入者、再犯者が続出していることは後述する。

次に、③表向きは普通の会社と見分けがつかず、目立たず、特に、④日本では取締りが低調でアダルトビジネスのような保護価値が低い事案をあえて狙い、⑤他の犯罪の影に隠れ、ほぼノーマークで急成長している。

さらに、⑥海外のランサムグループのように、巨大化、巧妙化、悪質化したり、⑦海外拠点で完全犯罪のシステムをビジネス化（B to B）しており、これらの結果、捜査困難領域（デッドゾーン）が拡大している。

以下、実際の事例に基づき、やや詳細に解説する。

代理徴収会社は、犯罪組織から離れている犯罪インフラ企業。彼らはまっとうな企業を標ぼうしているので、警察の捜査の手が及ぶと「当社のサービスがそんなことに使われていたのですか。知りませんでした。」ととぼけながら、さっさと逃げる。

また、異性の動向を監視するストーカー用ソフトを、ぼけ老人の徘徊防止や迷子防止と装って販売していた例もある。会社自体は、ぼけ老人の徘徊防止とＨＰ上では説明しているが、それでは売れないので、第三者になりすましたり、アルバイトを雇って、「これって彼女の動向の監視もできるよね」などと煽ったうえで、本来の機能を宣伝するというような手口もある。

また、海外の犯行ツールを犯罪組織がリースしている例もある。ネットカジノについて、マスコミでは海外でのオンラインカジノなどと説明しているのを見かけるが、これは正確ではない。正確には、海外のオンラインカジノのシステムをリースしている日本の胴元のサイトでのオンラインカジノであり、胴元も顧客も日本にいるので賭博罪が完全に成立している。

さらに、仲間を人柱にした人間ファイアーウォールのような仕組みもある。例えば、犯行ツールを直接借りる（使う）サイトを仮に「直営店」と名付ける。そこに賭客であったり、詐欺の被害者が出てくる。この直営店がその犯行ツールを仲間に又貸しすると、フランチャイズ店のようなものがたくさんできる。そこがこの犯行ツールを使って犯罪を実行するとそれぞれに被害者が出てくる。いくつかのフランチャイズ店のひとつに警察の捜査の手が及ぶと、直営店は逃げ、海外に拠点を移したりして、また新たな犯罪組織を作る。

まとめると、元々、犯罪性向を持っている人間が、インターネットを使って分業と効率的な金儲けの方法を知るとそこに手を出す。これらは他の犯罪に隠れてノーマークで成長していくという特徴があり、後ろで糸を引いている連中は安全で儲かる仕組みとなっている。また、捕まった人間もここに戻ってしまうというのもサイバー犯罪の特徴のひとつ。再犯者が続出するのである。

表向きは普通の会社と変わらず、目立たない犯罪企業が、取締りが低調で保護価値が低い事案をあえて狙う。

具体的には、

○　過激な映像を見せると誘いかけて、実はそうではなく、平易な写真を見せた上で、高額の利用料を取り立てる

○　利用した覚えがない、あるいは利用したかどうか自分でも曖昧なサイトの利用料金を取り立てる

○　チャットロボットを相手にチャットさせ、本当に異性に出会えるかと勘違いさせて交渉をじらし、高額な利用料を請求する

といったような例がある。

つまり、犯罪組織のメインの罪種としては、通常のアダルトサイトとかいうようなものではなく、家族や警察に相談しにくい性的なことを餌に、詐欺をしたりお金を脅し取ったりするというケースが多い。

今のところは警察に盾突いてどうこうしようというわけではなく、波風立てずに平穏に金を儲けたいというのが日本のサイバー犯罪組織の特徴である。もちろん、一般人に対しては、騙したり、脅したりして金をとるが、「金返せ」と怒鳴りこんだり、警察が入ってくるとすぐ返金に応じるような特徴がある。しかし、海外での犯罪動向が数年遅れて日本に入り込んでくる傾向がある。日本には、これらの犯罪組織の素地、土壌があるので、今回のようなランサムウェアグループのような大儲けできるシステム、アイデアが出てくると、すぐに乗り換え、先鋭化し、日本のサイバー犯罪組織が、巨大化、巧妙化、悪質化するおそれがあるということは、認識しないとい

けない。

さらに進むと、犯罪組織が海外に拠点を移し、BtoB ビジネス（一般消費者でなく、ビジネスをしているものに対するビジネス）、つまり、犯罪者が被害者に対して何かをするというよりも、犯罪を行っている連中に対してビジネスをするという「完全犯罪」のようなシステムが出来上がる。

こうなると、警察がいくら頑張っても捜査困難領域（デッドゾーン）が拡大し、検挙できなくなる。

サイバー犯罪対策

対策の提案に移る。

その前提として、警察は、過去、社会の構造変化から生まれた巨悪をいかにして駆逐したのかを振り返る。

社会の構造変化が投げかけた犯罪捜査への影響をまとめてみた。

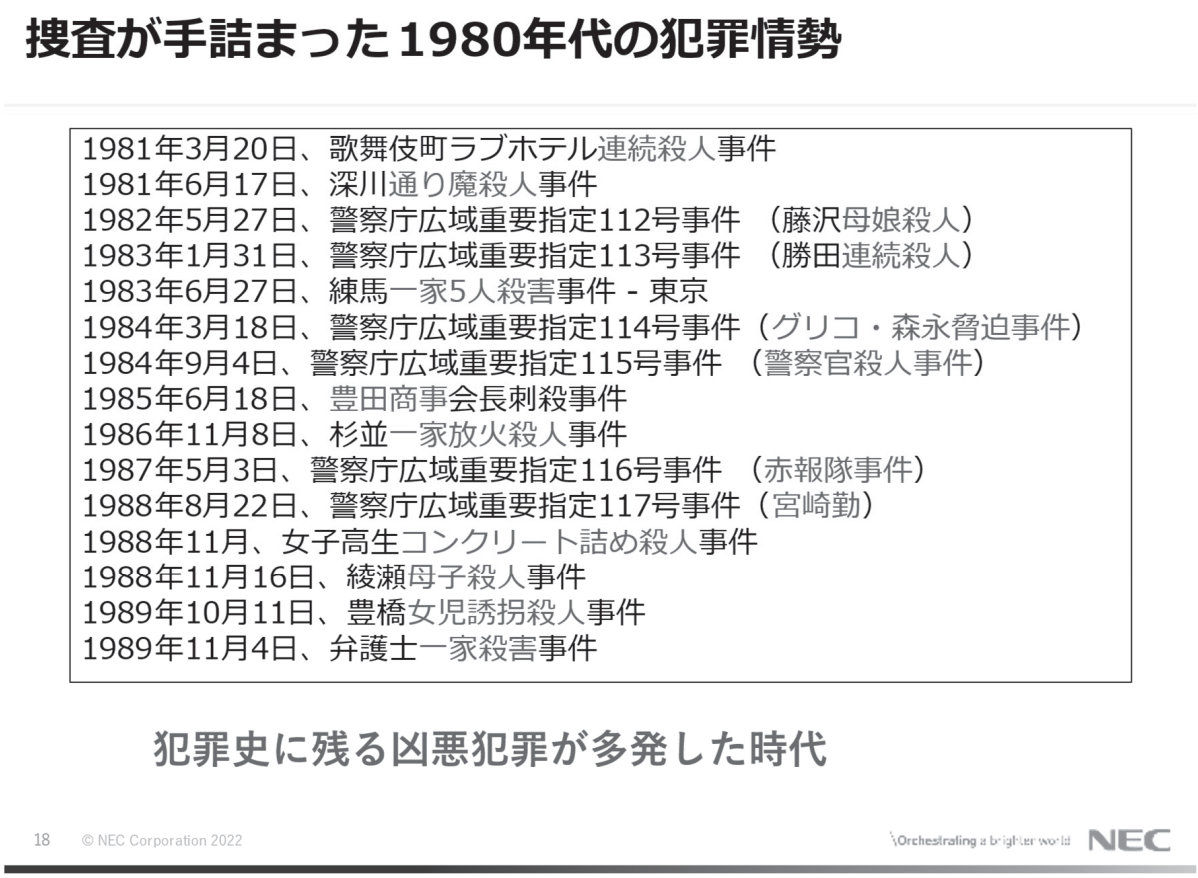
明治、大正、昭和戦前期は、犯行現場中心の捜査、言い換えると現場第一の捜査で、早期に周囲を固めて犯人を捕捉することが主流だった。

昭和戦後期は、モータリゼーションによるスピード化と電話網の発展によって捜査エリアが飛躍的に拡大した。私が拝命した昭和 50 年代の通達では「都市化、モータリゼーションによって捜査環境が著しく悪化」というのがいつもの枕詞であった。

平成に入るころになると、サイバー空間という概念上の空間が出てきて、犯罪は国境を軽々と超えるのが当たり前になった。

また、「境界線」があいまいになった。例えば、ある殺人事件が発生すると、「規制線」を引いて、その中で「しらみ潰し」「総当たり」の捜査をするという常道が通用しなくなったことが一つの例。このような問題が残されたまま、現在の令和の時代に入り、サイバー犯罪のさらなる高度化、国際化につながった。

少し時間を遡り、モータリゼーション等で捜査が手詰まった 1980 年代の犯罪情勢をみることにする。次のスライドは、1980 年代の、犯罪史に残るような、身震いする重要凶悪犯罪の一覧表である。



この中でも、1984 年（昭和 59 年）に発生した、怪人 21 面相によるグリコ森永事件は捜査の手詰まりを象徴する事件だった。

この発端は、入浴中の大手菓子メーカーの社長を猟銃で脅して誘拐するという、我が国では見られなかった事件であった。その後、さまざまな犯罪が行われ、約 16 年間、捜査員延べ 130 万人を動員し、捜査対象が 12 万 5 千人に達するものであったが、2000 年に、殺人未遂、誘拐、放火、強迫等 28 件すべての時効が成立した。警察にとっても苦い終わり方をした事件であった。

私自身も、毒入りチョコが置かれるかもしれないというので、24 時間、コンビニに張り込んだ経験がある。

この事件は、我が国初の劇場型犯罪で、国民を巻き込み、警察を揶揄しながら行われた特異な事件であった。

しかし、今、同じようなことが起きたらすぐに捕まるといえる。なぜかといえば当時の警察と今の警察は違うからである。

官民連携による先端技術の導入

サイバー犯罪対策の提言に戻る。

その１は、官民連携による先端技術の導入。

平成になってからの警察は、①高度な緊急指令システム、情報ネットワークシステムがある、②警察無線のデジタル化（当時の警察はアナログ無線で、一般の人も傍聴できた。）があり、また、

③防犯ビデオが普及したことなどにより、それまでの捜査の手詰まり感は払しょくされた。

ところで、ここに挙げたシステム、機材はいずれも官民連携による先端技術の導入である。言い換えると、官民連携による先端技術の導入が、手詰まりを払拭した原動力であった。

しかし、サイバー犯罪捜査では、犯行現場における「しらみ潰し」「総当たり捜査」という従来の基本的な捜査手法が著しく困難になった。

具体的には、サイバー犯罪は、ほとんどがリモート犯罪で、そもそも犯人は被害発生場所にはいないため、捜査範囲が著しく拡大したこと、重要な証拠が広範囲に点在し、クラウドの発展により文字通り世界中に拡散したこと。このために、犯行現場をいくら探しても犯人に至る情報は得られなくなった。クラウドでは管理者自身でもデータが世界のどこにあるかわからなくなった。

また、デジタル証拠は何かに化体させないと人の目では認識できず、また、そのデータもテラ単位が普通で、印刷すると何億行にもなることが多い。つまり、人力では証拠を解析することができなくなった。

私は現在、先端技術導入に貢献したNECで勤務し、時にはサイバー犯罪の捜査に先端技術を導入するよう現場の警察とやりとりしているが、サイバー犯罪捜査にとっては官民連携した令和の先端技術の導入が重要だと実感している。

捜査環境改善に向けた議論

その２は、四方先生の話にもあったが、捜査環境の改善に向けた議論を進めること、具体的には、諸外国との足並みを合わせる社会のコンセンサス作りである。

サイバー犯罪に関しても、日本の捜査環境は厳しいものがある。

新聞記事の見出しを見ても次のようなお叱りを受けている。例えば、「GPSを活用した位置把握は問題である」とか、「照会によるカード情報の捜査協力要請はダメだ」と言われる。しかし、すべて令状で対応しなければならないとなると、検挙はますます難しくなる。また、本人の承諾がないスマホのロック解除が問題視されているが、本人が承諾しないから高いお金を払ってロック解除しなければならない。そのツケは国民が払っている。

海外のシンポジウムに参加してみると、サイバー犯罪捜査の困難化、手詰まり感は各国共通だが、おとり捜査、ワイヤータッピング、潜入捜査による摘発事例を堂々と発表し、聴衆も当然視しているのに驚いた。サイバー犯罪は、このような特殊な捜査手法でなければ捕まえることができないという社会のコンセンサスが出来上がっている。日本でこういうことをやるといえば、「とんでもない」となったのではなかろうか。

ところが、最近、我が国の潮流にも少し変化が見られるようになった。2021年7月4日付けの日経新聞「スキあり、サイバー捜査網！」では、サイバー捜査では欧米と格差があること、従来型の捜査では限界があることなどに触れ、40か国超で導入されているポリスウェアの導入を我が国でも考えなければならないと警鐘を発してくれた。

サイバー局が発足した今こそ、捜査環境改善に向けた議論を始める好機ではないか。

以上

サイバー犯罪の取締に当たって留意すべき倫理問題

河島　茂生

■はじめに

私の専門は、メディア研究や情報倫理であり、研究の大義を「情報環境を良くすること」と位置づけて活動している。

情報倫理の「倫理」（エシックス）は、一般的に説教臭いイメージをもたれることが多く、「･･･してはならない」という戒め・説教と同じだとよく勘違いされる。あるいは、個人の心のもちようであると捉えられることもある。しかし、実はそうではなく語源は「慣習」「習わし」という意味で、これはモラルの語源も意味は同じである。日本語の「倫理」という言葉をみても、倫は「なかま」、理は「すじみち」という意味である。したがって倫理を考えるというのは、「秩序を考える」ということであり、これからどのような秩序を作っていくかを考えていくということである。

このあたりは、警察法の第一条で書かれている「個人の権利と自由を保護し、公共の安全と秩序を維持するため、民主的理念を基調とする」ということと相通ずるといってよい。

■背景

今日的問題の背景としては、司会の松尾庄一氏が著書『変化の時代』（立花書房、2009）で述べているように都市化・グローバル化が起きたことがある。個々人の多様化も起きた。さらにそれらに加えて、ICT の高度化・ネットワーク化・遍在化も起きた。

コンピュータ技術が高度化し、それらが通信で結ばれ、至るところにビデオカメラ等を含めたセンサーが配置されている。この ICT の高度化・ネットワーク化・遍在化は、まったくもって衰えず、今後もデジタル空間は拡大の一途をたどり、現実空間のなかにまだらにひろがり、ときには現実空間と一体化して、現実空間を引っ張っていくことになると推察される。

松尾氏が「保安官のいない西部の大平原」「戦後の闇市」という言葉を引かれていたことと同様だが、かつては「サイバースペース独立宣言」などのように、サイバースペースは「これまでとは全く違う新しい空間で、規制など入れなくとも民主的で輝かしい空間となる」といった考え方がそれなりに幅をきかせた面はあった。しかし、これまでインターネット上で起きた誹謗中傷や詐欺、知的財産の侵害などを考えると、そんな悠長なことは言っていられないと考えられるようになってきた。

こうした状況をきちんと直視していたからこそ、四方光先生は早くからサイバー犯罪の研究に取り組み、木村公也氏は現場で実際に取締に当たってきたのだろう。また、こうした背景に対応するために、今回、サイバー警察局やサイバー特別捜査隊が作られたのだと捉えている。

■ビッグデータ・人工知能（AI）

10 年ほど前「ビッグデータ」という言葉が流行り、いまもデータの活用が盛んに言われている。このビッグデータに加え、計算機パワーの向上と人工知能（AI）の機械学習アルゴリズムの工夫が合わさって、帰納的プログラミングが活発化し、これまでコンピュータがうまく扱えなかったデータまで解析できるようになってきた。すでに多くの分野で AI 技術が使われているが、ディープフェイク（AI のディープラーニングを使って嘘の画像や動画を作って拡散すること）も増えている。

■ AI の倫理

一般的に技術は、倫理的な議論を引き起こすことがある。技術の社会的影響が増していくにつれて、さまざまな学協会が倫理綱領等を作ってきた。こうした取り組みは、日本でも 1990 年代以降、本格化している。

AI についても同じで、AI の影響が広く深く社会に入り込むことが想定されたため、AI 関連の原則、ガイドライン、報告書、提言等が積極的に作られ、これまで数百も公開されてきている。これら数百ある原則等は、共通点がかなりあり、「個人の尊重」「公平性」「説明可能性」「プライバシーの保護」「安全性とセキュリティ」などが共通している。

AI を開発し利活用する企業の側でも、倫理方針を立てるケースが増えてきている。企業の AI 倫理指針は、「企業のビジョン」と「ほかの AI 倫理原則等」を突き合わせて作るが、AI 倫理指針は目指すべき大きな方向性を示し抽象的に設定する。実践のためには、それを細かなプロセスに具体化していくことが要請される。AI 倫理のガバナンスやマネジメントをしていくということである。倫理委員会を設置したり、e- ラーニング教材を使って研修を実施したり、あるいはアセスメントシートを活用したり、AI 可視化ツールを利用したりしている。

■ソフトロー／ハードロー

AI 関係のガバナンスは、全体としては原則や標準、ガイドラインといった緩やかなソフトローで進められてきた。もちろん医療や自動運転車の分野など、人命に直接的に関わるリスクの高い領域はハードロー（法的拘束力のある法令）にせざるをえない面があった。したがって個別の分野にフォーカスして、その分野の必要性に応じてハードローでやっていくという流れだった。しかし 2021 年 4 月に「欧州 AI 規制法案」が出て、流れが変わり、徐々にハードローの流れが強くなってきている。

■欧州 AI 規制法案

欧州の AI 規制法案は、まだ案であり、AI の定義など少なからず変更が予想されるが、現時点の案に基づきつつ実際の事例にも触れながら簡単に説明する。現時点では、リスクを 4 段階に分けて、それぞれのレベルに応じた規制が提案されている。容認できないリスク・高リスク・ローリスク・最小のリスクの 4 段階である。

まず容認できないリスクとしては、政府による個人のスコアリングや、法執行機関による公共空間でのリアルタイムの生体識別が禁止とされている。例外的扱いは行方不明児童の捜索やテロ行為の防止などに使う場合である。

たとえば、政府が抗議活動を行っている不特定多数を高精細のビデオカメラで撮影して顔のデータをデータベースに入れ込み、それを多くの場所で実施して照合すると、政府による監視が過度に進み巨大な権力が生まれる。その権力に従わない人はスコアも下げるようにすると、人々が抗議活動すらできなくなる事態が想定されてしまう。

Black Lives Matter を受け、2020 年 6 月に Amazon 社や Microsoft 社は、AI の顔認識の技術を警察に提供しないことに決めた。顔識別の技術は、以前から男性より女性の精度が低く、白人よりアフリカ系の人たちに対して精度が低いことが指摘されており、2020 年にはミシガン州でアフリカ系の男性が誤認逮捕される問題が起きている。また、中国では少数民族の監視などに顔識別の技術を使っているという指摘がある。

次の高リスクのレベルには、医療機器などの AI の規制が入っており、HR Tech などによる利用も入っている。AI を使った人物評価はよくある使用法だが、世界的に有名な AI プログラムを自分の会社の人事査定に使ったら労使紛争に発展してしまった例もある。

限定的リスクのレベルについては、さきほど触れたディープフェイクなどがここに入る。音声合成 AI によって、本物そっくりの声が合成され詐欺が行われた事例も発生している。

■監視選別社会

監視選別社会（スコア社会）について簡単に触れておきたい。日本は、いまのところ、かなり抑制が効いているが、スコア社会化が進むと大きな社会的問題が引き起こされかねない。

AI 等を使ったシステムを使ってすでに自分のスコアを出した経験のある参加者もいるだろうが、スコアの計算方法が相当不透明で、間違ったデータが入り込んでいても気づかない算出方法になっている。

これは、偏差値とはまったく違っている。偏差値の弊害も唱えられて久しいが、偏差値は、明々白々な計算式を使って計算に用いられたデータの範囲も明確である。対して AI によるスコア算出は、計算式もよく分からず、使われているデータについてもよく分からない。しかし、それがコンピュータを使って出された数値であるがゆえ、客観的であるかのような様相を帯びてしまう。

データ自体に間違いがあるケースもあるが、たとえデータが正しくとも、それを誤って識別してしまうケースもある。たとえば、新型コロナウイルスの接種券の OCR ラインについても、数字の誤識別があり 1% ほどの誤りが出た。数字の自動識別は、かなり安定性があって普及した技術だが、それでも誤りがゼロにはならない。ほかのデータについても誤りは出る。間違ってもそれほど大きな問題にならない対象に対してであればよいかもしれない。しかし人を評価する際に、どのようなデータが分析にかけられているかも分からず、内部のメカニズムも不透明で、かつ誤っているかどうかも定かではないというのは大きな問題であるといわざるをえない。

スコア社会化には人間の平等性に対する懸念もつきまとう。国際的な AI 倫理の議論でも、公

平性が必ずといってよいほど入れられている理由である。さきほど見た欧州 AI 規制法案でも、政府がスコア化を行う場合には容認できないリスクに挙げられていた。

スコア社会は、全方位的に個人を格付けする。学歴や年収だけでなく、年齢、職業、性格、趣味、買い物、家族構成、SNS の利用などが計算に組み入れられる。そのいわば全人的なスコアが倍の差になっているとき、人は皆、平等であるという考え方を社会的に堅持できるだろうか。これまで人類は時間をかけて、ようやく一人ひとりは平等であるという考え方に辿り着いてきた。しかし、その考え方が瓦解してしまいかねない。

ここで規範的な論を離れ、スコア社会化に関する一般的な意見をみてみたい。2019 年に私が河井大介氏と行った調査結果を示す（注 1）。

AI による人物評価への信頼度は、現時点では半々である（表 1）。AI による人物評価は、「AI がこう判定しているから」などと判断の理由を AI に責任転嫁して自分の判断の言い訳を行い自分で責任を取ることを回避するような危険性があるが、現時点なら「AI の言っていることは当てにならず間違いが多い」という意見にも賛同が集まる状況である。

表 1　AI による人物評価への信頼度

問　AI は、人間よりも正しく人物評価を下せると思いますか。（単一回答）

正しく下せると思う	ある程度正しく下せると思う	あまり正しく下せるとは思わない	正しく下せるとは思わない
2.1％	46.1％	38.0％	12.5％

無回答 1.3％

けれども、将来は分からない。今後、さらに収集するデータの種類や量が増えていくと、将来は AI による人物評価の信頼性が上がっていくことがありえる。また、これまでの HR Tech の報道をみると、すでに AI の判定にすでに依存しはじめていることが窺いしれる。

「自分の点数が出たときに、どのような人・組織であれば見られてもよいか」という質問については、親子や夫婦であればおよそ半数の人がみられてもよいと考えており、その次にみられてもよいのが国や警察という回答分布になった（表 2）。国や警察への信頼が比較的厚いことが見て取れる。

表 2　点数をみられてもよい対象

問　AI の計算により、自分の点数が出るとします。どのような人・組織であれば、その点数を見られてもよいでしょうか。（複数回答可）

親子　51.5％	採用担当　14.9％
夫婦　49.3％	賃貸関係者　8.0％
親子・夫婦以外の家族　11.1％	国　24.9％
友人　7.2％	自治体　11.2％
恋愛対象の相手　6.4％	警察　19.6％

勤務先の人事担当　13.0％	その他　12.7％

無回答 4.7％

続いては、自分の点数への納得感に関する項目である（表 3）。やはり自分の点数が高い場合には納得する比率が増し、低い場合には納得しない比率が増している。ただし点数が高い場合でも、納得する比率と納得しない比率は同程度である。

表 3　自分の点数への納得感

問　AI の計算により、自分の点数が出るとします。その点数は、少なからず自分の人生に影響します。しかし、その計算手順や読み込んだデータは公開されません。ほかの人よりも点数が高い場合、そのことに納得しますか。（単一回答）

とても納得する	ある程度納得する	どちらともいえない	あまり納得しない	まったく納得しない
2.4％	29.9％	36.3％	21.8％	8.3％

無回答 1.3％

問　AI の計算により、自分の点数が出るとします。その点数は、少なからず自分の人生に影響します。しかし、その計算手順や読み込んだデータは公開されません。ほかの人よりも点数が低い場合、そのことに納得しますか。（単一回答）

とても納得する	ある程度納得する	どちらともいえない	あまり納得しない	まったく納得しない
1.1％	17.8％	31.9％	36.6％	11.2％

無回答 1.3％

また自分の点数を算出する変数として抵抗のあるデータはなにかという質問については、病歴は当然のこととして、SNS の利用内容や友人関係を変数とすることに対して抵抗感が示されている（表 4）。昨年、報道された記事によると警察庁は、SNS の公開データを AI で解析して人物の相関図を作成しているということだが、このアンケート結果をみるかぎり、それなりに一般の人たちが抵抗感を抱くことが予想される。

表 4　自分の点数の算出のための変数

問　AI の計算により、自分の点数が出るとします。その点数は、少なからず自分の人生に影響します。AI による計算の際、どのようなデータが読み込まれることに抵抗がありますか。（複数回答可）

性別　16.9％	年収　30.7％
人種　22.2％	宗教　21.8％
自分の病歴・家族の病歴　33.7％	学歴　27.1％
身長　17.8％	職歴　22.3％

顔　28.9％	犯罪の有無　16.7％
姿勢、振る舞い　16.2％	趣味　25.2％
年齢　14.1％	SNS の利用内容（友達、投稿内容）　35.5％
婚姻関係の有無　23.3％	友人関係　34.2％
生活保護を受けた経験の有無　19.9％	その他　5.1％

無回答 1.1％

他者の点数を算出するのに必要なデータとしては、いまの履歴書や面接で分かる項目に支持が集まっている（表 5）。一方、他の人の点数をはじきだすために SNS の利用内容をデータとして使うことは、それほど必要と考えられていない。SNS の利用は、匿名かつ複数アカウントであることも多く、良からぬことをするときはそのときしか使わずすぐにアカウントを変えている現状があるため、このような結果になっていると推察される。

表 5　他者の点数の算出のための変数

問　AI の計算により、他の人の点数が出るとします。その点数は、少なからず他の人の人生に影響します。AI による計算の際、どのようなデータが読み込まれると正しい点数が出ると思いますか。（複数回答可）

性別　41.4％	年収　38.5％
人種　24.4％	宗教　20.4％
自分の病歴・家族の病歴　36.3％	学歴　48.6％
身長　22.3％	職歴　51.5％
顔　21.0％	犯罪の有無　65.5％
姿勢、振る舞い　46.1％	趣味　27.8％
年齢　49.8％	SNS の利用内容（友達、投稿内容）　22.5％
婚姻関係の有無　27.1％	友人関係　25.2％
生活保護を受けた経験の有無　28.3％	その他　8.8％

無回答 0.3％

監視選別社会の話を締めくくるにあたって、計算によって人を評価することの限界を確認しておきたい。

詳しくは『未来技術の倫理』（河島茂生、勁草書房、2020）を参照してもらいたいが、人は、自らで細胞を作りながら、免疫系や神経系、そして身体と一体となった心を自ら内部で作り出し、環境を認知して変化している。その結果、人は不確実性を帯びている。この意味での不確実性は、機械の内部の変動性とは本質的に違う。

たとえば野球では、ドラフト候補選手たちを 100 項目以上に細分化して数値化し、スカウティングの精度を上げようと努力している。しかし、それでもドラフト 1 位の選手がまったく活躍しなかったり、育成出身の選手が日本代表となっていたりすることもしばしばある。これだけコンピュータ技術で投手の球の回転数や手から球を離す位置などを細かく計測していても、次のシー

ズンに活躍できるかどうかまったく分からない。

それだけ人は不確実性があり、そのときどきでそれぞれの人が内部で環境を認知し、生きている。コンピュータによって人を全面的に計算しつくすというのはかなり難しい。計算によってある人が将来、「必ず」犯罪を犯すことを導き出すことは、いまの技術の動向をみるかぎり、たとえできるようになるにしても、かなり先だと予想される

ロンブローゾの骨相学など、古くから私たちは「未来の犯罪行為を予測したい」という欲望をもっており、よく映画やドラマの題材にもなる。最近は、コンピュータ技術を使って未来の犯罪行為を予想する試験的開発も行われるようになってきた。けれども、近いうちに未来犯罪予測の欲望が満たされるのは難しいといえる。

前に述べたように、未来予測ではなく現状の人物評価であっても、AI はそれなりに間違ったり偏りのある結果を算出する。そのため警察であれば、AI だけに限らず DNA 鑑定や指紋の調査なども引き続き重要な意義をもっている。もちろん、『AI ×クリエイティビティ』（河島茂生・久保田裕、高陵社書店、2019）でも書いているように、違和感（ちょっと妙だといった感覚）などの身体感覚もきわめて重要である。しかし、生身の身体感覚だけでは限界があるため、私たちの能力を拡張するためにテクノロジーを利用する。指紋の照合や DNA 鑑定などと同じく、人間の能力を拡張するテクノロジーとして AI を使えばよい。ただし、そのようにテクノロジーを使いつつも、最終的には人のことは人が決めるという覚悟をもって判断していく必要がある。

■ロボット

これからのことを考えるなら、まだまだ開発が難しい点があるものの、スマートロボットの時代が本格的に来ることを想定しなければならない。

自動運転車も、ロボットカーと言われるようにロボットの一種だと考えると、とてつもなく大きな社会的影響がある。AI はソフトウェアのみだが、ハードウェアを伴ったスマートロボットの時代は、生身の身体に直接的にダメージが与えられかねないため「安全性」（Safety）がより強調される。警察が犯人をきちんと特定して処罰できなければ、クラッキングが後を絶たず、海外からの犯罪も多発する恐れが高いとなると、結果的にロボット社会が立ち上がらなくなってしまいかねない。

■メタバース

過剰気味に語られているメタバースも、CPS（Cyber-Physical System）やデジタルツインのように、実空間と連動したりリアル都市を模して作られたりすることがある。そのため知的財産権などは、メタバースでも課題になるし、実画像を元に 3D アバターも作られてしまい、なりすましも横行すると思われる。

また、たとえ実空間を模さなくとも、しばしば人は、自身のアバターに愛着をもち、サイバースペースの場所にも愛着をもつ。実空間と同じような問題が生じてくると予想される。

スマートロボットと同じく、いますぐメタバースの時代が来るわけではないが、いずれくる未来

として想定しておく必要がある。

■最後に

警察は、民間よりも、より厳密な倫理規範が求められるだろうが、ある業務を実施するか否かを迷ったときは、エシックテストが使える。可逆性テストや徳テスト、危害テスト、公開テスト、専門家テストなどである。

なお、こうしたエシックテストを実施する場合は、その組織自体の偏りについて留意したほうがよい。たとえば警察の場合、警察官の女性の比率が 10％を割り込んでいることから、男性目線に陥りがちだと推察される。警察官同士だけで妥当であると判断しても、社会全体でみるといびつに受け止められることが出てきかねない。

時間の関係上、いくつかの論点は省略したが、たとえ警察であっても一組織だけではとても太刀打ちできない課題が山積しており、組織横断的なレベルでの責任についてより焦点を当てて取り組むことが欠かせない。ここでいう責任には、問題が起きたときに取る責任だけでなく、よい未来を作っていく責任も含まれている。

データの取り扱い等にあたっては、企業がいかに法やガイドラインなどをみながら活動しているか参照することで、警察にとっても学ぶことが少なくないと考えられる。

注

(注) 2019 年の社会調査は、筆者と河井大介との共同調査であり、中央調査社のマスターサンプルに対する郵送調査（督促はがき 1 回）を行った。このマスターサンプルは電子住宅地図を利用した層化三段無作為抽出法に基づいて依頼を受けた個人が登録されているものであり、調査会社が保有する調査パネルのなかでも偏りが小さく、代表性が高いと考えられる。調査対象は、マスターサンプルのうち日本全国に居住する者で、20 歳以上 59 歳以下の男女である。調査対象者は性別と年齢層（10 歳刻み）で母集団比例の割付を行ったうえで、予測回収率をもとに重みづけを行い、地域（7 地域）と都市規模（3 段階）で層化無作為抽出された 1300 人で、回答者は 623 人であった。発送・返送期間は、2019 年 1 月～同年 2 月である。回答者の内訳は、男性 311 人 (49.9%)、女性 312 人（50.1%）であり、年齢別でみると 20 歳代 132 人（21.2%)、30 歳代 138 人（22.2%)、40 歳代 210 人（33.7%)、50 歳代 138 人（22.2%)、60 歳代 5 人（0.8%）である。なお調査対象者は 59 歳までであったが、調査期間中に 60 歳代になった人が 5 名いた。

質疑応答

（質問者）サイバー空間の安全は国家安全保障と切り離せない。社会安全政策論をサイバー空間に適用する際に国家安全保障の視点をどのように位置づけているか。

四方光　社会安全政策論においては、これまでテロ対策までは視野に入っていたと認識しているが、国家安全保障まで認識していたかと問われるとそうでなかったかもしれない。

ただ、サイバー攻撃といわれているものにおいては、国家を背景にした破壊工作、戦争の前哨戦との境界がなくなってきたといわれているので、ご指摘の点も視野にいれていかなければいけない問題だと感じている。

松尾庄一　サイバー犯罪がサイバー空間だけでなく、現実空間で行動、活動と融合している面がある。木村さんは別の機会に「サイバー犯罪の手口として、風俗的なことをダシにして詐欺や恐喝をするというのがほとんどだ」と言われたが、具体的な手口についてご教示願いたい。

木村公也　発表では、「サイバー犯罪にはアダルト的なものが多い」と言ったが、今、はやっているものとして「サポート詐欺」がある。どういうことかといえば、アダルトサイトをみていると、実際には感染していないのに、ウィルスに感染したような画面が出てくる。慌ててそこのサイトのヘルプデスクに連絡すると「サポートデスクです。こういうふうにして、ああいうふうにして下さい」と言ってお金をとる手口がある。あるいは、予防と称して、必要のないソフトを高額で売りつけるものもある。

もうひとつが、女性になりすまして男性に近づき、「お互いにからだを見せ合いっこしましょう」といって写真のやりとりをしている間に、アドレス帳のデータを全部抜き、「裸の写真をアドレス帳の全員に送る」といって恐喝するような手口もあった。

ほかにも、決して出会うことのない「出会わない系」という手口もある。チャットロボット相手にのめりこみ、ポイントを 100 万円近くだまし取られるケースもある。周りの人や警察に相談できないことをダシにして儲けているというのが、日本のサイバー犯罪には多い。

（質問者）ランサムウェアによりデータがブロックされたときに、犯人の要求に応じて身代金を支払うことについての考えは？

木村　大変難しい質問。元警察官としては、犯罪組織にお金を支払うことは、次の被害者を生んでしまうからよくない、あるいはランサムウェア攻撃が続発するのは、お金になるから、儲かるからで、身代金を支払うのは、彼らに肥やしを与えるからよくないということになるだろう。

しかし、報告でもふれたが、病院が狙われ、業務用のデータがブロックされると、患者の命にかかわることにもなり、経営者としては身代金を払ってでも一刻も早く復旧したいという気持ちが強い。そういうところに「けしからんから絶対だめだ」というのは酷。

物ごとのバランスを考えて、苦渋の選択を考えて判断することは認めなければならないと思う。

松尾　河島先生はご著書『AI 倫理』（西垣通先生との共著）で、「ある特性値のデータをもつ人物

を把握してグループ分けするプロファイリングは、深刻な差別や冤罪を招くおそれがあるので慎重な配慮が必要とされる。」と述べられている。

他方、警察としては、暴力団を念頭に置くと分かりやすいが、捜査員の目と耳で集めた情報に基づき、捜査員の頭で分析して「ある特性値のデータをもつ人物」を容疑者群としてグループ分けして、犯罪捜査や予防に活用しているのは事実。そのような中で、一見無関係なビッグデータの間に有意な相関関係を見出すのに優れたAIを活用して、たとえば、今まで知らなかった犯罪者のネットワークを浮かび上がらせたいと願うのは、もっともだと思う。それについてのご意見、また、肯定する場合にも、警察として特に留意すべき事項があればご教示願いたい。

河島茂生　まず大きな前提を確認しておきたい。世界人権宣言や日本国憲法第十四条では、人種等の差別を禁止しており、倫理学においても自由平等主義は、一人ひとりの平等を唱えている。報告で述べたように欧州AI規制法案では政府による個人のスコアリングは禁止とされているが、もし警察が日本に居住する人を対象としてスコアリングするならば、それは国内だけでなく国際的にも大きな非難を浴びるに違いない。AIを使ってさまざまなデータの相関関係が見られるからといって、収集できるデータ――人種等の生物学的特性を含む――をすべて読み込ませてスコアリングするというのは批判を免れえない。例えば犯罪顔を見分けるAIを開発し、犯罪顔に分類された人を捜査対象とするといったことは避けるべきだ。

もちろん、犯罪が起きた後で、ビデオカメラに映った顔や身体を見分けるためにAIを使って解像度を上げたり身長を推定したりするのに使うのは問題ではない。ただしAIを使っても必ずしも正解にたどり着けるわけではなく、ときには差別的な判定や誤った推定になることは念頭におかなければならない。

松尾　河島先生の報告やただいまの話を聞いて、警察の領域以外からサイバー犯罪を取り締まる側の倫理問題を論じるのは重要なことだと実感した。

他方、4月1日からサイバー警察局やサイバー特捜隊がスタートしており、実績をあげていくことも国民から期待されている。警察への新体制への希望なり注文があれば聞かせてほしい。

河島　今後、コンピュータの高度化・ネットワーク化・遍在化により、実にさまざまなデータが手に入るようになるが、公的機関として許されるデータ収集・利活用なのかをエシックテストなどをもとに考えてもらいたい。

今回の組織改正のようなものは、評価できる点もあれば、当然、評価できない点も出てくる。四方先生や木村様の話を聞き、今後、捜査権限等が焦点となってくることを確認することができた。

四方　私は新体制はいい仕事をしてくれるのではないかと思っている。ただ、そのためには課題もいくつかある。最大の課題は、外国の捜査機関と連携した共同捜査が行えるかということ。そ

のためにはサイバー犯罪に関する知識、捜査能力、それに語学という三つの能力が必要だと思っている。そのうち、知識、捜査能力については、木村さんのような人材が育っていることは評価してよいが、英語ができて外国の捜査員と対等にわたりあえる人材はまだまだ少ない。サイバー警察局にはそういう人材をより多く育成することを期待している。

他方で、報告でも触れたが、サイバー犯罪捜査に有効な捜査権限が乏しいが、サイバー局ではそれがより切実になることから、法務省等とも連携して捜査権限拡大についても検討すればいい仕事につながるのではないか。

以上

警察政策学会資料　第 124 号

サイバー空間における安全安心の確保

令和 4（2022）年 8 月

編集　管理運用研究部会
　　情報技術犯罪対策研究部会

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