令和３年９月 21 日

令和３年度サイバーセキュリティ政策会議（第１回）
発言要旨

１　開会

２　サイバーセキュリティ・情報化審議官挨拶

昨年度のサイバーセキュリティ政策会議においては、新型コロナウイルスの感染拡大を契機とするデジタル化の加速により、サイバー空間は全国民が参画し、重要な社会経済活動が営まれる、これまで以上に重要かつ公共性の高い場へと変貌を遂げていく中、増大するサイバー空間の脅威について幅広く御議論いただいた。

近々策定予定である政府の次期サイバーセキュリティ戦略においても、サイバー空間の公共空間化に伴い、実空間と同様の安全安心の確保が求められており、攻撃者との非対称な状況を看過せず、環境・原因の改善に正面から取り組んでいく旨の記述がなされるなど、国が責任を持って関与していく方向性が打ち出された。正にサイバー空間における国の役割はターニングポイントを迎えていると考えている。

その一方で、本年５月に発生した米国のパイプライン事業者に対するランサムウェア攻撃では、市民生活や経済活動に多大な影響を生じており、日本国内においても警察庁として把握しているランサムウェア被害の件数が大幅に増加している。また、これに加えて、政府機関・研究機関等に対するサイバー攻撃が多数発生するなど、サイバー空間の脅威は極めて深刻な情勢が続いている。

このような厳しい情勢に対し、米国ではランサムウェア攻撃に対処するため司法省が中心となった官民タスクフォースの設置や、その攻撃への対応をテロ攻撃と同等に引き上げるなどの措置を実施しているほか、ユーロポール主導の Emotet ネットワークの壊滅に見られるように、有志国による国際共同オペレーションの積極的な展開なども進められている。このような中、我が国においても、より積極的な連携・関与が不可欠であることは、言を俟たない。

そこで、昨年度の政策会議でも御議論いただいたが、警察の総力を結集し、体制を抜本的に強化するため、令和４年度に警察庁にサイバー局を、関東管区警察局に国の捜査部隊としてサイバー隊を設置する組織改正の概算要求を提出している。

このサイバー局等新組織の目指すところは、サイバー空間に限定された安全安心の確保にとどまるものではない。内閣府が行っている世論調査においても、日本について誇りに思うこととして、長年にわたり最上位に「治安のよさ」があげられるなど、世界一安全な日本はかけがえのない社会の財産である。

新しい組織は、生活安全局、刑事局、警備局等既存の局とも連携し、サイバー空間上での様々な対策だけでなく実空間における取組とも連動することにより、デジ

タル化が進み、実空間・サイバー空間の両者が一体不可分となった新しい社会においても、これまで以上の安全安心を国民の皆様にお届けすることを目指している。

この目標は非常に高く、警察の中の議論だけでは真に実効性のある政策を打ち出すことは難しく、有識者の皆様に幅広く多様な視点から御議論・御指導いただくことが不可欠であると認識している。

そのため、令和３年度サイバーセキュリティ政策会議は、「サイバー局と新組織において取り組む政策パッケージ」をテーマとした。

委員の皆様においては、新組織に求められる役割、取組等について、多様な観点から自由に御議論いただき、忌憚なく御意見を賜るようお願い申し上げる。

３　委員長挨拶

審議官からお話があったように、新しい組織について議論することが本年度サイバーセキュリティ政策会議の中心となる。これまで、この会議の前身である総合セキュリティ対策会議時代も含めて、サイバーセキュリティ対策を取り扱ってきたが、その内容も大きく変わってきたと思う。初めは重要インフラをいかに守るかというところに重点が置かれていたが、現在では、国民への直接的な被害も非常に深刻となってきており、公共空間化したサイバー空間をいかに守るかということが重要な課題となってきている。

また、これまでは国民を国内の犯罪者による攻撃からどう守るかを考えてきたわけだが、最近では、国家を背景とする攻撃等も発生しており、より大きな枠組みで対応することが必要とされていると思う。

さらに、デジタルやAI等の先端技術の進展も著しい中、国民は国が専門性を持って対応することを期待していると思う。警察に限っても、人材をいかに結集し、どの様に有効に運用していくのかが求められる、大きな転換点に来ているのだと思う。

この点、今回の警察庁組織改正構想は、警察庁自体がある種の執行機関的な対処能力を持つという、警察の長い歴史の中でも大きな転換なのだと思う。日本警察の強さは、地域に根差した各都道府県警察であり、地域住民の心にまでおりていく対応が非常に大事である一方、先ほど申し上げたようないろいろな要請の中で、国家の組織として統一的・合理的にどう動いていくか考えていく必要がある。

その検討における重要なポイントは、最後は国民の安心・安全にどう資するか、国民が納得してくださるのかというところに帰着すると思う。そのためにも、多様な分野からお集まりいただいた委員の皆様の忌憚のない御意見を伺い、今後の警察庁のサイバー政策がよりよいものとなるように協力していきたい。

4　特別委員講演

【特別委員から、「安全なデジタル社会の創生」について講演】

5　事務局説明

【事務局から、「新組織における施策の方向性（案）」について説明】

6　討議

委　　員：　昨年度のサイバーセキュリティ政策会議では、特に「サイバーハイジーン」の重要性について申し上げた。今回は、事務局説明においても官民連携や民間からのインプットという話があったが、「マルチステークホルダー」というキーワードが非常に重要になってくると思う。

委員長からも国家を背景とするサイバー攻撃が最近多くなっていると触れておられたが正にそのとおりである。国連のＧＧＥ（政府専門家会合）からも色々なレポートが発表されているが、各国においてマルチステークホルダーの観点から対応を進めることが重要ということで、検討の際の重要なキーワードの１つになると思う。

委　　員：　事務局説明資料のⅣ「地域を支える多様なチャネルの発掘・活性化」について、ＣＳＩＲＴ活動を行っていると、最近は、大学等の学術機関とも連携する場面が出てきているが、協力に関して、学術機関等のどういったところに期待されているのか。

また、高校生、大学生の中には、トップガンには至らないが、専門知識を持つ中間層は結構いると思う。そういった方々に対して期待することなどあれば伺いたい。

事 務 局：　リテラシー教育については、より身近な学生の方から行った方が、トップガン人材が行うよりも小・中学生に対して分かりやすい説明ができることもあると思う。先ほどの事務局説明の中で佐世保高専の事例も紹介させて頂いたが、そのほかにも身近な例として、特殊詐欺対策において、警察官が小学校・中学校に行き、「家に帰ったら、自分のおじいちゃん、おばあちゃんに、詐欺の電話に気をつけるようにお話をしてね」という話をして、より身近な方から働きかけてもらうという取組も行っている。サイバーセキュリティに係るリテラシー教育についても、専門知識をある程度持つ学生の方に、小・中・高校生のところに行っていただいて、何が問題になっているか、とるべき対策等についてお話していただくことも有効であると考えている。

委　　員：　今後どういった形で広げていけばいいのか、ＣＳＩＲＴに活動等も

含め、いろいろな形で情報提供・連携のようなことを考えていければと思う。

委　　員：　事務局説明資料のＶ－１について、各種サービスを提供している事業者等に対する被害実態の情報提供があげられているが、資料全体を通して「被害」という語がサイバー攻撃そのものによる被害のみを指している様に感じられる。直接的な被害だけでなく、攻撃により流出した情報が悪用されるといった二次被害という側面も考える必要があると思う。警察から被害実態に係る情報提供をいただくことはありがたいが、二次被害の実態については、逆にもう少し民間から吸い上げるようにしていただきたい。

オンラインマーケットプレイス協議会において、実務上の課題について意見交換する中で、不正なクレジットカードによる被害がＥＣ事業者全体にとって非常に大きな課題になっている。自衛の対策として、３Ｄセキュア等で認証を強化することや、チャージバック保険等での対応も行っているが、事業者としては警察に犯人を捕まえてほしいという期待がある。

しかし、事業者が不正なクレジットカードによる被害を受けた際に、警察に通報してもなかなか話も聞いてくれず、捜査に動いてくれそうな感じがせず、期待できないということで通報もしなくなったという声も多数ある。

この様な被害は普通の詐欺によるものであり、サイバー局としての関心からは外れるかもしれないが、どこから不正なカード情報等を入手したか、ルートをたどっていくと、サイバー攻撃を行った者が利用するダークマーケットにつながる可能性もあるかもしれないし、手口情報の共有だけでも意味があるのではないかと考えている。

事業者等が二次被害に遭ったときの情報を活用していただけるのであれば、ＥＣ業界としては喜んで情報提供をしたいと思うので、サイバー局に窓口を設けていただけるとありがたい。

また、最近は、ｅコマースだけでなく、フードデリバリーサービスや、それを利用する飲食店にも不正カードの被害が及んでいるようなので、そういったところで何が起こっているかということも情報収集するようにして頂ければと思う。

事 務 局：　現場でなかなか話を聞いてもらえないということがあるとしたら、大変申し訳ない。他方で、警察では、御指摘いただいた不正クレジットカードを利用した犯罪に対する捜査を非常に重視しているところであり、また、対策という観点からも、事業者の方から実態について教

えていただくことを大変重視している。

実際、不正クレジットカードに係る被害は全国で発生しているところであり、多くの都道府県警察が連携した共同捜査により、不正クレジットカードを使った犯行手口を研究し、突き上げ捜査等を実施している。不正クレジットカード等に係る被害に遭った際には、警察本部のサイバー犯罪対策課に積極的に御相談いただきたい。

また、犯行手口を検証し、対策を打つことにも努めており、未然防止というリスクコミュニケーションについても今後しっかりと取り組んでまいりたい。

委 員 長： 情報収集を基に捜査を広げていくことは重要。今回の報告書の中でも、具体的にサイバー空間を通じて国民の安全安心をどう前進させるかについても考えていただきたい。

委　　員： 人材育成について、日頃肌で感じていることとして、サイバーセキュリティ人材の地域格差というようなものがあると思っている。サイバー局・サイバー隊創設により、人材を増やしていくということにも期待するが、高度な人材を地域に配置した上で機動的に活用するというところで、地域格差がなくなっていくことも期待している。

また、官民連携について、官と民という関係だけでなく、制度設計を行う側と技術を扱う側という関係における連携や融合といったことも必要ではないかと思う。例えばＳＭＳ認証について資料に例示されているが、ＳＭＳは信頼できるということで制度設計をして、認証の手段として使っていたが、現状は、認証代行等によって認証の穴が生じてしまっており、業界団体に対し、データＳＩＭに係る本人確認の協力をお願いしているということかと思う。こういったことは、イタチごっこになりがちである。例えば、ＳＭＳ認証を使ってもいいものと、犯罪に悪用されるから駄目なものといった色分けをシステム開発側も含めて共同で考えていくことが、全体として安全を確保するためには必要になってくるのではないかと思う。サイバー局の中でも、技術と制度、あるいはガバナンスの観点から民間等との協働をいかに進めて行くのかという点も必要になるかと思う。

事 務 局： 警察の中でも高度な技術的知見を持った集団もあれば、高度な捜査能力を持った集団、地域社会と密接な接点を持つ集団など様々な特性を持った部署がマルチステークホルダー的に存在しており、これらを融合することにより安全を確保していくための組織をしっかり作ろうということが、サイバー局設置に向けた検討の最初の出発点であった。

サイバーの世界での対応は、技術・制度のどちらかのみを考えても駄目であり、国民の方々の生活の実態を知らなくても駄目である。警察の中での様々な知見とそれぞれの得意分野を融合し、民間事業者・学術機関等とも連携を持ち、一緒に知恵を出し合っていくことによって安全を守っていくことが重要。これは新しい組織が設置されるのを待たず、今からそういった問題意識を持って、取組を進めていこうと考えているので、引き続き御指導等をお願いしたい。

委　　員：　今日の資料については、いろいろ検討していて、非常によくできていたと思う。そういう意味では、方針としては出来たわけで、これから実態としてどうやっていくかということが課題になると思う。

最近はクラウド化が進み、クラウド業者自体がセキュリティサービスを担っていく、あるいはそのインフラを提供するＳＡＳＥ（Secure Access Service Edge）を展開していく中でそれらをベースにして、様々なコントロールがなされていくようになってくることを考えると、クラウド業者とどういった協力をして犯罪を防止していくか、あるいは、被疑者の逮捕等への道を開いていくかが重要であると認識しているが、その辺りの考えはどうか。

事 務 局：　クラウド化の進展に伴い業界との対話は大変重要になっていると考えている。卑近な例では、上半期の脅威情勢にも掲載している事例であるが、クラウド上のＩＤ、パスワードを保管したものが窃取された可能性がある事案を確認している。

御指摘いただいた点は、クラウド化の進展が政府機関を含めてこれからますます進んでいく中で、今後のサイバー局・サイバー隊にとって大変重要であり、しっかりと取り組んでまいりたい。

委 員 長：　警察に限っても、デジタルトランスフォーメーションを進める中で、情報をどこに集約して、どの様に安全性を担保するのかなどは引き続き大きな課題となっていると認識。また、政府全体でも、クラウドの使い方として海外企業のものに依拠することに関して相当議論があったと伺っている。国全体のセキュリティの問題としても、今御指摘いただいた点は非常に重要であり、警察としても検討を進めていただければと思う。

委　　員：　サイバー空間のみで完結するフィッシング詐欺のような事例だけではなく、サイバー空間からリアル空間におびき出して特殊詐欺を展開する様な事例が非常に増えてきている。具体的には、ウェブサイトの検索結果から誘導して、電話といった伝統的な媒体へ移行してテクニカルサポート詐欺、特殊詐欺等を敢行している。犯罪者側は、デジタ

ルトランスフォーメーションを既に実現していて特殊詐欺等を行っているという現状がある中で、サイバー局・サイバー隊においては従来の縦割りを打破し、他部局と連携をして、特殊詐欺といった話であっても、サイバーの領域が深く関わっている部分では対応いただきたいと思っているが、その辺りの考え方について伺いたい。

事 務 局：　御指摘は正に組織改正の核となる部分である。会議冒頭でもお話ししたが、新しい組織はサイバー空間に限定された安全を確保するものではないと考えている。従来の様にサイバー犯罪・サイバー攻撃だけに対応すれば良いということではなく、サイバー空間と実空間が一体不可分となったデジタル社会全体における安全を確保することまで到達して、初めて新たな組織をつくる意味があると思っている。

繰り返しになるが、今回の組織改正では、生活安全局と警備局のサイバー関連機能を集めるというだけではなく、刑事局で取り扱っているビジネスメール詐欺等を含めて、サイバー空間だけでは完結しない犯罪についても新組織のスコープに入れていく。

一方、サイバー隊の関与については、既存の組織と密接に連携しながら進めて行くこととなるので、個別の事案毎の判断となる。スコープを明確に決めきるということは考えていない。

事 務 局：　サイバー犯罪については、単にサイバー空間にとどまるものではなく、そこから実空間に移ってくるものも多くあり、実態として、全国共同捜査等で対応する事案の中でもかなりの割合を占めている。

特殊詐欺の様な事案についても、「ネットワーク利用犯罪」に関するものであれば、サイバー事案として現在も対応させていただいている。

また、刑事部門が行っている捜査について、現在もサイバー部門が技術支援を行っており、サイバー局が発足した後も、支援をしっかりやっていきたいと思う。

委　　員：　事務局説明資料のⅢ－１「警察に対する通報・相談の促進」に関連して、セキュリティに係るサービスを提供する中で、お客様の社内における内部犯行の疑いの相談を数多く受けている。相談を受けた段階では、被害の実態が定かではなく確固たる証拠等が分かっていない事例も多々あるが、このようなケースは、相談先がないと認識しているところ、今後、このような事案があった場合には、警察で相談対応をしていただけるのか。

また、資料Ｖ－２「民間の知見活用や情報の共有等連携のさらなる推進」について、官民連携に係る施策が記載されているが、弊社でも

人事交流をはじめ、情報共有をさせていただいているところ、この次の段階ということであれば、サイバー局の一部の業務について民間委託するということは考えられるか。

事 務 局：　被害実態が定かではないが、内部犯行の疑いがあるというものについても、都道府県警察に相談窓口を設けているので、御相談いただければと思う。また、民間委託については既に一定程度行っている。例えば、ＩＨＣ（インターネット・ホットラインセンター）の取組がある。平成 18 年から、ＩＨＣでは、わいせつ情報、児童ポルノ情報、薬物情報等を認知・通報いただいて、保護・削除の依頼を実施している。こういった定型的な部分であれば、民間になじむというところもあるので、どのようなものが適切なのかというのは、一つ一つ議論をしながらということにはなろうかと思うが、今後、サイバー局と民間との連携という中で、しっかりと議論をしていきたい。

委　　員：　インターネットの現状などを考えると、今回のサイバー局設置を含めた新組織への移行というのは、非常に重要。また、本日の説明資料の方向性については、全く異論がない。その上で、事務局説明資料Ⅲ－１に関連して、サイバー犯罪等発生時において、捜査における警察と事業者の連携対応について、今後具体的にどうなっていくのか、各事業者、通信業界としても、やはり非常に関心のあるところであり、早めに情報を提供する必要があると考える。

　具体的には、サイバー隊と都道府県警察の役割等が、これまでと比較してどうなっていくのか。この点については、早めに情報提供いただきたいと考えており、会議の中でもしっかりと議論ができればと考えている。また、例えば、特に関連する業界等に対する説明会などを実施するということも検討をしていただき、トラブルなくスムーズな対応を行うことが重要だと思う。

事 務 局：　サイバー隊と都道府県警察の役割分担については、これからまだ詰めなければといけない部分があるが、事業者の皆様とも意見交換を図り、実際に事案が発生した際に具体的にどうしていくのかという点を分かりやすく御説明できるように今後検討してまいりたい。

委　　員：　今回の組織改正については非常に前向きに捉え、評価している。その一方で、取材等に対応する中で、サイバーの世界で警察の力が大きくなることに対して、懸念を持つ向きもある感じも受けなくはない。

　法執行の部分とインテリジェンスの部分が重なっているところに、サイバー局が創設されることにある種の懸念を感じている方々に今回の組織改正をどう説明していくかは大きな課題ではないかと思う。

また、インテリジェンスの部分が法執行の部分にどう重なってくるのか、あるいは重なってこないのか。本来であれば、インテリジェンスとの間には壁があるべきだと思うが、壁をつくることで捜査がやりにくくなる部分というのも当然あると思う。その区分けをどう説明していくかが課題ではないかと思う。

事 務 局：　御指摘のような懸念が存在することは認識しており、丁寧に説明を行っていく必要があると考えている。インテリジェンスは、サイバー空間に関連した脅威を払拭し、安全を確保していく上では避けて通れない部分であるが、その一方で非常にデリケートなものであり、その取扱いには十分に注意することを心してかからなければいけないと考えている。国民の皆様に誤解が生じないように丁寧に説明をしていきたい。

委　　員：　グローバルな感覚では、事務局説明資料のⅡ－１の二国間・多国間連携の強化や、Ⅱ－２にある国際共同オペレーションについては、説明にもあったように、関係構築が重要である。最終的には、やはり人と人、個人と個人の信頼関係ということが非常に重要になってくる。

一日や二日といった短期間、リエゾンが出向くことですぐに関係が構築できる訳ではなく、５年１０年といった長い時間を要する可能性もある。こういった中で、中長期的な計画をどのように立てていらっしゃるのかお伺いしたい。また、人事配置についても、官公庁では一般的に２年に一度程度の頻度で人事異動があるところ、セキュリティ関係やグローバル関係の業務に関しては、長年担当していただくことで信頼関係が生まれ、力を発揮できることもある。そういった人材の回し方、キャリアパスについても、中長期的にどのような計画があるのかお伺いしたい。

事 務 局：　国際連携あるいは国際共同オペレーション等を実施する上で、人と人とのつながりというのは非常に重要。日本は国際的な窓口のつくり方だけでなく、人事異動のサイクルが非常に短いという問題がある。国際会議等においても、日本を除く諸外国は皆顔見知りであったり、あるいは１０年以上在任されている方もいる。そういう国は必然的に発言力も高まってくる。また、国際共同オペレーションを実施していく上でも、知らない人間にはなかなか情報が来ないのが現実だと思う。

新組織の国際的な窓口については、一定程度、長期間そのポストに配置されるような人事を考えている。これまで以上に進化した国際連携、国際協調を行っていきたいと考えている。

委　　員：　国際連携対応について、課題として「国際共同オペレーションの端緒となり得る日常的な情報交換等を行う、実務者レベルでの関係の構築が十分でない」、「各国で強みとしている技術等を実務者レベルで十分に情報共有していると言えず、具体的な連携方策の検討に支障を生じている」とされているが、施策を進める上で、現在どのような状態にあって、それを解決するためにはどういう方策をとり、どこまで到達しようと考えているのかをお伺いしたい。

事 務 局：　国際的なサイバー犯罪、組織的なサイバー犯罪に関して、各国と様々なやり取りをしているが、取組は緒に就いたばかりであり、恒常的に情報交換をできているというわけではない。相手方のニーズをとらえ、どういった情報を的確に出していくかについて、今まさに試行錯誤をしている段階である。

その中で、サイバー局・サイバー隊の設置に際しては、ある程度恒常的な人的関係を構築し、国レベルでの関係づくりを進めるということが大事だと考えている。

また、都道府県警察では、各企業との関係も構築しているところ、しっかり初動捜査を行い、情報を国で吸い上げ、海外に対してしっかり提供していくことにも取り組んでいきたい。

委　　員：　９月 20 日の日経新聞の１面に、各国において、被害企業がランサムウェアの身代金をどのぐらい払ったかという記事が掲載された。身代金の支払いに巻き込まれる可能性は今後も高まっていく。特にコロニアル・パイプライン社の事件では、コロニアル・パイプライン社、ＦＢＩ、ホワイトハウスまで巻き込んだ連携が上手くいき、１週間程度で混乱は解消されたと考えている。日本でも同じようなことが発生し得ると思われるので、特定の業者に関しては、サイバー局において、企業の担当者と平時から意見交換をする場を設けた方が良いと思う。平時からの意見交換を行っていれば、被害に遭ったときに、すぐ相談ができる。犯罪情報の収集という意味でも役に立つ上、企業としても早く立ち直ることができる。こういう場を用意いただけるとありがたい。

また、地域連携について、様々な取組が既に行われている。それらが独立した動きにならないようにすることが重要であるので、警察庁の取組についても、関連団体との連携をお願いしたい。

事 務 局：　現時点でも重要インフラ事業者、金融機関等との間では協議会を設けたり、協定を結んで協力関係を構築するという活動を行っているところ。サイバー局設置後もこういった地域に根差した活動は大事であ

り、サイバー局ではさらに声かけをして、様々な事業者の方に協定を結んでいただいたり、情報提供等を行わせていただいたりして、関係を構築していきたい。単に協定を１回結べば終わりではなく、きちんと担当者との顔つなぎができるようにという活動を進めていきたい。

委　　員：　新組織の施策を決める上で実態把握が非常に重要。警察庁では、これまでもサイバー空間の脅威の情勢等を広く一般にも公表されているが、サイバー空間の脅威は、物理的な制約がない分、非常に短時間に攻撃されるなど物理的な犯罪に比べても乱高下が激しい、そういった特徴があると考えている。

一定の範囲では暗数が生じることもやむを得ないが、できる限り広く被害実態が見えてこないと、どういった政策・取組に力を入れていく必要があるかが見えてこないと思う。

組織改正を機に、警察でもデジタル化が進んでいくと思うので、最前線の警察署－警察本部－警察庁というルートの中で、スピーディーな形で事案の把握ができるようにすることや、企業等への適時適切な情報提供・情報共有がなされることが大事であると考えている。

委 員 長：　今後、非常にタイトなスケジュールの中で、具体的な肉づけをしていかなければいけないので、第２回では、早速、その中身について事務局から発表いただきたい。その際には、本日各委員から御指摘のあった点、例えば、脅威に係る実態の把握、官民の任務分担・連携、国家安全保障、地域住民の気持ちの汲み上げ等を踏まえて進めていただきたい。

また、時間がタイトなので、事務局から早めに情報を委員に提供していただきたい。委員の皆様からも、要望等があれば事務局に出していただいて、それに対応するというキャッチボールをする中で有効に時間を使っていくようお願いする。

７　閉会