令和２年 10 月 30 日

令和２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　長官官房サイバーセキュリティ・情報化審議官挨拶

本会議も前回の平成２９年度の開催から２年以上が経過したが、この間、新型コロナウイルス感染症の拡大という世界を揺るがす大きな猛威を経験し、私たちの日常生活は大きく変わった。

いわゆる「三つの密」の回避など、感染拡大を防止する新しい生活様式の定着が求められ、企業におけるテレワークの本格実施、電子決済サービスの普及など、対面が前提であった社会経済活動がサイバー空間を通じて行われるようになった。こうした動きに加え、今後は、ＡＩやビッグデータの活用、５Ｇ、ＩｏＴ機器の普及、行政手続のオンライン化など、社会のデジタル化が加速していくことが予想される。

サイバー空間の脅威情勢については、サイバー犯罪の検挙件数は昨年過去最多を更新し、インターネットバンキングの不正送金事案が急増した。また、オンライン会議システムの脆弱性を悪用したサイバー攻撃や、電子決済サービスを悪用したサイバー犯罪が多発するなど、サイバー空間をめぐる社会的・経済的環境の劇的な変化に伴い、情勢は深刻化している。

こうした我が国の社会経済活動を混乱に陥れる新たな脅威に適切に対処し、デジタル化が進展する中で、国民の安全・安心を守っていくためには、サイバーセキュリティの確保に向けた今後の官民の連携の在り方について、大局的な見地から検討することが必要である。

そのため、今年度のサイバーセキュリティ政策会議は、「生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携のさらなる推進」をテーマとした。官民の知見を結集し、今後、焦点を当てるべきサイバー空間の脅威は何かを改めて洗い出すとともに、こうした脅威への対策について、幅広い視点から御議論いただきたい。

３　委員長挨拶

審議官から話があったように、今がターニングポイントだと思う。

本会議は、従来から、国民の安心・安全をいかにサイバーの世界で守るか、官民連携をいかに進めるかということをやってきた。その基調は変わらないが、国際的な国家間のレベルの話もサイバーの世界では強くなるなど、今後どう変わるかが見

えていないところがある。

この会議では、国全体としてデジタルについてどう動いていくか、安心・安全だけでなく、サイバー世界の展開を見据えながら、忌憚のないところを御披瀝いただきたい。

セキュリティ抜きの発展はあり得ず、今後、一層サイバーセキュリティの重要性は増していくと思うので、この会を実り多いものにするためにも、よろしくお願いする。

４　令和２年度サイバーセキュリティ政策会議のテーマ及び会議の進め方について

【事務局から、令和２年度サイバーセキュリティ政策会議のテーマ及び会議の進め方について発表】

５　サイバー空間を取り巻く情勢について

【委員から、サイバー空間を取り巻く情勢について発表】

６　銀行等を狙ったフィッシングの分析とその課題

【有識者から、銀行等を狙ったフィッシングの分析とその課題について発表】

７　質疑

委　　員：　本日の発表を踏まえ、改めてサイバーハイジーン（公衆衛生）の重要性を指摘したい。先ほどのフィッシングの話でもいろいろあったが、使う側が二要素認証を使っていない、非常に単純なパスワードを使っているといった事例もある中で、サイバーハイジーンの重要性を改めて再確認していかなければいけない。

サイバー空間に接続する以上は、パッチを当てる、ソフトウェアをアップデートする、二要素認証や簡単に判別できないようなパスワードを使用する、フィッシングサイトの見分け方を知るといったことも重要だと思う。

委　　員：　有識者の講演の最後に今後の課題として、対策推進のための官民連携、特に産官学連携が重要という話があったが、全くそのとおりだと思う。大学単独でフィッシング等に係る研究をしようと思っても、実データを保有していないため事実上不可能であるという状況である。

また、講演内容は主にフィッシングサイトであったが、例えばこれと不正アクセスとをつなげて分析することができればもっといろいろなことが分かってくると思う。大学をもっと活用するための連携の枠組みをこの会議で進めることができたらと期待している。

委 員 長：　先ほど講演した有識者は、産官学の連携をより実質化するための枠組みとして出来たものであり、この会議の成果だと思う。有識者が成立した理由も、御指摘のあった点も含めて、生データでリアルなことを踏まえて動かないと、安心・安全に具体的に役に立たないことがあるためである。様々な大学なども含めて、有識者にもっと結集することが日本のためになると思う。

委　　員：　消費者保護をテーマとするような会議では、被害にあった消費者がいかに救われるか、補償してもらえるかという話や、不審なサイトの見分け方といった消費者啓発、注意喚起の話、さらには、不正利用されてしまったときに不正なアクセスを確実に遮断しないサイトが悪いといった認証の話に焦点が行ってしまう。それぞれ非常に重要な視点とは思うが、犯人を捕まえるという話が欠けてしまっていると思う。消費者の立場からすると、被害が救済され、金銭的な被害がなければそれで満足してしまうところもあり、本当に悪い人が誰かというところに思いが行かないというのは、若干問題ではないかと思う。

　そういう意味では、有識者の講演において犯人像の分析、実態解明がもっと必要だという話があったことは非常に大切なことだと思う。

　警察庁に質問であるが、犯人像が見えたとして、それでも犯人を捕まえるのは難しいというのは、どの様な問題、障害があるのか。国をまたぐという問題なのか。

事 務 局：　御指摘のとおり、データを分析することにより犯人像が浮かび上がるようになったことは大きな進歩であり、これを生かさなければならないとの思いはある。

　一方で、犯人像が浮かび上がってきた段階を、犯人を検挙するというアクションに結びつけるためには、犯罪捜査を進めていくための証拠という形に結びつけなければいけないというハードルがある。

　また、犯人が海外にいるという場合には、証拠を外国の捜査機関等に渡して捜査をしてもらう必要があるが、ほとんど何も動かないという国に対してどの様に働きかけていくのかというところも課題である。

　ただ、以前と比べ、外国で何が行われているのか、誰がやっているのかが分からないという段階からは進歩してきており、それをいかに捜査に落とし込むのかということは課題としてやっていかなければいけないと考えている。

事 務 局：　国際捜査に関して補足だが、サイバー犯罪やサイバー攻撃は、大部分といってもいいぐらいのものが国をまたいで敢行されている。国際

捜査を行う上で、当該国、関係国の協力は非常に重要であるが、協力に消極的な国も多々あるほか、サイバー攻撃の中には外国政府等が背景に存在するものも多々あるところ、その様な場合にはなおさら当該国から協力を得ることは困難であるという状況がある。

そうした中でも、関係国、友好国と協力して情報を集め、どういった国のどういった組織がこれに関与しているのかといったアトリビューション、属性付けは、ある程度可能になってきているという状況である。

これをうまく使えば外交カードとして、非常に有効に活用できるということもある。そういった意味で、このアトリビューションは非常に重要であり、それをどのように国際場裡で知らしめていくかということが、我が国の重要な課題であり、やっていかなければいけないことだと認識している。

警察、外務、防衛等関係機関の連携はこれからもさらに重要になっていくという認識で進めている。

委 員 長： この会議では一貫して、「民」でいかに被害を防ぐかという議論をしてきたが、ボールは警察にも投げられていて、犯人を何故捕まえられないのか、もう少し前に出てほしいという意識が国民にはあるので、この点については是非また議論したいと思う。

委　　員： 最近オンライン化が進み、昔であれば隣に人がいて少し相談するということができていたのが、気軽に相談できないため不審な話であってもつい信頼してしまうという話を聞く。オンラインになって、気軽に相談できなくなった部分の影響など、オンライン化という環境変化の影響をぜひ捉えていただきたい。

また、利用者側の意識について、例えばマルウェアに感染した場合であっても、マルウェアを作った犯人を直接認識できないため、犯人がいるということを忘れてしまっている。利用者側の意識を高めるには、マルウェアの存在だけではなく、それを使っている犯人たち、作っている犯人たちがいるということをもう少し意識させることもやらなければいけないと思うので、この辺りのところも啓発活動を一緒に、何らかの形でできたらと思う。

委　　員： 今の発言に関連して、行為者がいて、被害者がいるというところに加え、社会の反応も非常に重要ではないかと思う。マルウェア等により被害を受けると、被害者のリテラシー不足ばかりが責められるような社会であってはならない。行為者を責めるような社会情勢を、この会議も含めて作っていかなければいけない。サイバー空間では被害者

だけが苦しんでしまう状況がありがちであるが、行為者、被害者、そして社会という三すくみの中で健全なサイバー空間を醸成していかないといけないと考える。

委　　員：　銀行やクレジット業界等、各業界でそれぞれ具体的にきっちりマルウェアの対策を行うことは当然だと思うが、その対策の傍らで、利用者は、ＩＤやパスワード、最近であれば二段階認証等いろいろな機能を合わせ持たなければならず、非常に管理が煩雑。

事業者・利用者のいずれもコスト的な負担が非常に大きい。それぞれの業界が連携するとともに、最適・的確な本人確認・本人認証の在り方の議論を進めることが必要と思う。本人確認と本人認証は、これからのサイバーセキュリティの非常に肝になる部分である。

委 員 長：　御指摘のとおり、社会全体のデジタル化のためには、サイバー空間上においてもリアル空間と同じ様に、誰がやりとりの相手になっているのかを認識できるということが大前提になると思う。セキュリティを考えていく上で、全ての国民・業界に関係することであるため、本人認証やそのコストも含めて、議論の俎上に上げてやっていきたいと思う。

委　　員：　セキュリティやサイバー犯罪といっても非常に範囲が広いので、どの辺りを重点的にやるのかという議論も必要と思う。金銭目的の犯罪であるのか、国家スパイ、産業スパイ、あるいはテロリストの話、愉快犯等様々あるが、どの辺りを狙うのか。

また、情報のＣＩＡ（機密性、完全性、可用性）についても考えなければいけないが、完全性という課題は、これからＩｏＴが進展していくと非常に大きな影響をもつこととなるので検討が必要と思う。

さらに、ランサムウェアについても、情報を凍結するだけではなく、公開するという攻撃も増えるなど悪質化しているがどの様に対応すべきかということも検討課題であると思う。

加えて、脱はんこという動きがあるが、これはセキュリティ、特に将来的に経済犯罪に絡んでくるのではないかと思う。電子署名のやり方も、従来のいわゆる当事者型と言われているものから、最近は立会人型というものが増えてきており、必ずしも完全に本人確認等ができない仕組みのものも存在する。この状況が直ちに危ないというわけではないが、将来的にここの部分は気をつけなければいけないところだと思う。今後の課題として検討いただければと思う。

委　　員：　土屋委員の御発表の中でアトリビューションが重要という御指摘があり、また、有識者からも、犯人像のアトリビューションをしていっ

て、グループ化していくことが犯罪行為の全容把握にはかなり重要なポイントであるという御指摘があった

他方、アトリビューションの話の一例として、平昌の冬季オリンピック大会の際に、サイバー攻撃が行われ、オリンピックの運営が一部妨げられた、その主体は北朝鮮であったという報道があったが、後々になって専門家がオリンピックデストロイヤーと呼ばれているマルウェアを入手して解析したところ、北朝鮮が従来使っているような手口とは全く別のものであったという判断をしたという事例がある。

アトリビューションを明らかにしていくためには、例えばマルウェアの場合であれば、リバースエンジニアリングという高度な技術が必要になるなど、アトリビューションをしっかりしていくということに関しては、高度な技術者を育成していくことが必要であると理解している。これについて、民間ができる支援策があるのか。

委　　員：　御指摘のとおり、アトリビューションは簡単ではない。アトリビューションは、ストラテジックなレベルとオペレーションのレベルと、タクティカルなレベルと３つの層がある。タクティカルなところでは、例えばマルウェアの解析をやらなければいけないし、ＩＰアドレスの追跡という技術的なところをまずやらなければいけない。

一方で、政府レベルで攻撃の主体者を公にするといったストラテジックなレベルのアトリビューションは非常にポリティカルであり、外交的な判断をしなければいけない。問題は、その間にあるオペレーションのレベルで技術を担う人と政策を担う人の間をつないで翻訳をできる人がいないと、うまくいかない。そういう厚い人材の層を作ることができるのは、民間ではなく、政府がリソースを投入してやっていく必要がある。

米国では、捜査機関や軍、インテリジェンス機関にいる人を大学院に出して、補助金や奨学金を与えて技術を学ばせる。その後、政府の中である程度業務に就かせ、後は民間へというサイクルができている。そのため、政府の中には、常に新しい技術を持った若い人たちが入ってきて、その人たちが民間に出ていくことで、民間のサイバーセキュリティ技術も全体として上がるということをやっている。そういう人材育成をやるべきだと思う。

委 員 長：　今日、頂いたテーマについて、かなり認識が共有できたと思う。サイバーの世界では、はじめは皆さん注意して、被害に引っかからないように、こういうものは駄目ですという話ばかりだったが、徐々に作った悪い人がいて、それをどう捕まえるかという方向に、間違いなく

進んでいる点は非常に心強く思う。

８　閉会