平成 30 年３月 15 日

平成 29 年度サイバーセキュリティ政策会議（第４回）
発言要旨

１．　開会

２．　報告書案の説明

【事務局から、平成 29 年度サイバーセキュリティ政策会議報告書（案）「新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進」について説明】

３．　質疑応答

○（委員）　前書きの部分について、２パラグラフ目に、WannaCry に関する記述がある。この記述を残す場合、同じパラグラフの最初にあるレンタルサーバに関する一文の後に何か入れるか、WannaCry に関する記述を消すかのどちらかが良い。サイバー犯罪というのは、個人が犯罪者である愉快犯、あるグループがバックになっている経済犯、国家をバックにした犯罪の３つがある。WannaCry は、昨年 12 月、アメリカ政府、日本政府が、北朝鮮にこれを帰属したサイバー攻撃であり、国家がバックになっているサイバー攻撃であると言える。一方で、レンタルサーバに関する犯罪は、主に個人による犯罪なのではないかと思うので、その後に、国家をバックにしたサイバー攻撃である WannaCry が来るのであれば、こういった国家をバックにした攻撃があり、現在はそういう時代になっているということを書いたほうが良いのではないかという提案である。

また、捜査関係事項照会の電子化は是非進めてもらいたいと思う。これほどグローバル化が進む中で、捜査関係事項照会書を郵便で送っているのは日本だけであるので、官民連携という中で、スピードアップという観点からも、電子化を進めていくべきだと思う。

○（委員長）　１点目の指摘は、今回のテーマの１つとしてレンタルサーバを扱う理由を書いているが、それとはレベルの違う WannaCry については、もう少し詳しく注をつけて説明的なものにするべきということなのか、それとも、段

落を分けて別個のものとして扱ったほうが良いということなのか。
○（委員）　WannaCryに関する記述を残す場合、もう少し詳しく、前に説明を置くということである。一方で、WannaCryに関する記述を全て削除してしまい、レンタルサーバに関する一文の後に、例えば、昨年一年間の被害について記述するにとどめ、そのまま、次のパラグラフに移るということも考えられると思う。
　繰り返しになるが、サイバー犯罪には、個人の愉快犯、そしてグループ、さらに国家と３つのレベルがあると思うので、WannaCryの記述を残すのであれば、そういったことも認識してもらえるような記述にすることも大事なのではないかと考えているということである。
○（委員長）　サイバー犯罪には、個人の愉快犯から、国家主体のものまで様々なレベルがある中で、それらを同列に扱うのは、問題の本質が見えていないように見えてしまうのではないかという指摘は、そのとおりだと思う。
○（事務局）　指摘のとおり、内容としてつながりが悪いところがある。一方で、WannaCryの部分についても触れたいと考えており、書き方については検討させていただきたい。
○（事務局）　捜査関係事項照会の電子化については、これまでも重要なテーマの１つであった。仮想通貨に関する記述があれば、仮想通貨交換業者に対する照会の電子化の話が出てきたのだが、現在の報告書案の中でどのように記載するのが良いか、意見を踏まえて検討させていただきたい。
○（委員長）　本会議でも話が出たが、捜査関係事項照会の電子化が必要だということは共通の認識になっており、これを報告書に入れることは問題ないと思うが、一方で、どこに記述するかが難しいところである。
○（委員）　「おわりに」の最後のパラグラフが、今後に向けてといったニュアンスのパラグラフなので、そのどこかに、今後のサイバー空間の技術の発展に向けて電子化も取り入れながらといった記述や、２年前の総合セキュリティ対策会議でもあった捜査関係事項照会の電子化も含めといった記述をすることが１つの案としてあり得るのではないかと考えている。
○（事務局）　捜査関係事項照会の電子化を今回の報告書に入れることは難しい部分もあるが、オンライン化の必要性、重要性については十分認識しており、

その点は、報告書に載る載らないにかかわらず、引き続き協議させていただきたいと思っている。報告書への記載は検討させていただきたい。

○（委員）　レンタルサーバについて、弊社ではレンタルサーバという言い方は使わず、どちらかというと、利用者が資産を持たない形のサービスはホスティングという言い方をして、利用者が資産をそのままデータセンターに持ち込む形態はハウジングという言い方をしている。

最近では、新たにホスティングという領域から、クラウドというサービスが対比されるケースが多いと思うが、クラウドは利用者が好きなタイミングで好きなリソースを増やすことができるサービスである。一方で、形態としては利用者が資産を持たないということは一緒だと思っている。レンタルサーバという言葉に戻ると、最近ではあまりマスコミでも出てきていないと感じており、個人的には、昔の、おそらく 15 年ぐらい前の、いわゆる共用サーバという、1つのサーバを区切って小さく安く貸す形態が、レンタルサーバと呼ばれていたと思う。現在では、ホスティング事業、サービスや、クラウドとの対比が多いため、例えば、クレジットカードのみでリソースを借りられるサービスということで定義すれば、これらも全て入ってくると思う。

報告書案の中にもあるが、問題は本人確認が非常に弱く、クレジットカードさえあれば、誰でも借りられてしまうことであり、現在のクラウドサービスでも、そういったものが非常に多くなっているため、定義の部分を、もう少し書いたほうが、わかりやすいのではないかと感じる。レンタルサーバというと、もっと狭義になってしまうようなイメージがある。

○（委員長）　レンタルサーバについての議論のポイントは、本人確認の問題を中心に、犯罪インフラになることをどのように防ぐかという観点であるが、一方で、レンタルサーバという単語が意味するものが、ごく一部のものであるということであれば、定義を示すことやクラウドといったものも入るように、もう少し何か単語を加えるといったことはあり得ると思う。

○（委員）　ＩＴ業界を中心に考えると、パブリッククラウドの時代で、確かにハウジング、ホスティングという言葉が一般的だが、一方で、本会議の報告書で、こういう場所で犯罪が多いということを、一般に示すという点では、レンタルサーバという言葉は、はまっているようにも感じる。

○（委員）　レンタルサーバに限定した議論は、現状を考えると、少し限定し過ぎなのではないかと感じており、ホスティングサービスやクラウドを含むというイメージでよいのではないかと考えている。したがって、その定義を第１章の始めに盛り込むとともに、タイトルのレンタルサーバに、「等」を付けるといった修文が良いのではないかと考える。

○（事務局）　定義がしっかりしなければ、対象とする範囲が不明確になるので、本文に付け加える、注として書くといった形で記載する一方で、厳密に書いて狭め過ぎないよう、指摘のとおり「等」を入れた形にするという方向で検討したい。

○（委員）　レンタルサーバがテーマの１つに挙げられている趣旨は、匿名性を利用して犯罪インフラのようなものをつくってしまうということに対処していく必要があるということだと思われ、その点では、レンタルサーバという表現でもよいのではないかと思う。

○（委員長）　現実の問題として、クラウド等についても、本人確認の問題が起こっている可能性もあるので、「等」を付けつつ、具体的な定義をどこまで書き込むかは検討させていただきたいと思う。

○（委員）　仮想通貨については、現在進行形のものであり、報告書でとりまとめないこととしたことはやむを得ないと思う。

なお、前書きの３つ目の段落の最後の文は、主語がないため、加えた方が良い。

また、ボットネットに関する今後の方向性に、シンクホールの実施に向けた検討の推進という話があるが、その中で、アメリカではマイクロソフトによる民事手続によってシンクホールを行い、ドイツでは、詳細は不明だが、刑事手続きの一環としてシンクホールを行ったようだと記述があり、「それぞれの国で法体系が異なることから、それらの手続を直ちに我が国に導入することは困難である」と書かれている。ここでいう「それぞれの」は、ドイツとアメリカではなく、日本と法体系が異なるということか。外国の手続を直に日本に導入するには慎重な検討が必要であるということが言いたいのであれば、もう少しはっきり書いたほうが良いのではないかと感じる。

○（委員長）　指摘のとおり修文したい。特に、後半の指摘は、外国の手続を

そのまま持ってくることが難しいというのはそのとおりだと思うが、せっかくこういった会議の場で発表いただいているので、もう少し前向きに、十分学びつつ使えるかを考えていくといった方向性が出るように修文したいと思う。
○（委員）　ボットネット対策で、シンクホールの実施に向けた検討の推進について整理されている。この中では、随分ＪＰＲＳへの期待が大きいと感じるが、ＪＰＲＳとの話はどこまで進んでおり、どういったことを議論しているのか。

また、その続きに、総合的なボットネット対策ということが書かれている。総合的という言葉を使う場合、相当広い課題の整理がまず必要だと思っている。今回は、警察庁の施策ということで、犯罪対策に主眼を置いたとしても、防犯的な取組は必要であり、犯人検挙ももちろん必要である。レンタルサーバのほうは、どちらかというと防犯対策的な目線が中心であると思うが、ボットネットのほうは、総合対策と書かれてはいるが、犯人検挙目線であり、犯罪防止、未然防止というような観点が抜けている。2020 年に向けては、防犯的な対策のほうが、必要な面があるのではないかと思っており、そのときに行うべきボットネット対策は、今後の検討課題としてもらいたいと思う。
○（事務局）　一点目のＪＰＲＳとの協議状況については、現状、事務レベルで何度か打合せを行っているという状況であり、何らかの根拠が整理されれば、ＪＰＲＳとして、それに基づいて動くことはできるのではないかという見解をいただいているという段階である。
○（委員長）　それを踏まえてこの文章になっている。いずれにせよ、アバウトな感じの部分が残ってしまうが、書き込み過ぎることが難しい面もある。
○（事務局）　総合的という言葉は、シンクホールを含めた被疑者の検挙を目指す警察が行うこと、電気通信事業者やその他の関係者が行っていることをいろいろと組み合わせたという意味で使用している。

また、シンクホール自体が被害者への通知といったことにもつながるので、被疑者の検挙を目指すこともちろんだが、防犯にもつながると理解している。
○（事務局）　一般的に、警察の場合、まず検挙があり、それ以外に、警備、刑事、生安、交通といった各分野の施策がある。このとき、部を越えて何かを実施する場合に、総合的という言葉を使う場合がある。一方で、指摘いただい

た点では、警察の検挙だけではなく、部外のいろいろな方々の協力を得て何かを実施するというときに、よく総合的という言葉を使っている。検挙と防犯という区切りだけではなく、事業者等との協力もあるので、総合的という表現になる。そのため、警察としては、指摘の部分は、意識としてやはり「総合的」なのではないかと考えている。

○（委員長）　刑事の世界では、検挙が最大の防犯であるという言い方はよく使われる。そのため、本当はその２つを分けて考えなければならないが、連続的につながってしまうところはある。

○（委員）　総合的という言葉が入っている意味は十分理解した。一方で、警察の言う総合的という言葉を理解していない人が読むと、若干狭いという印象を受け、ある意味批判につながる可能性もあるので、書き方は検討したほうが良いと思う。

また、検挙が最大の防犯というのはそのとおりだと思うが、ボットネット対策というのは、マイクロソフトの協力があったとしても、世界的に見てそう何例も成功があるものではないので､検挙もかなりハードルが高いと考えている。取り組むことは重要だと思うが、防犯的な要素もしっかり取り込み、少なくとも日本の中で攻撃の踏み台となる端末やユーザーを減らすということの重要性を認識した上で、この取組を行うのだという書き方のほうが、受け取る側からすると、正に「総合的」という印象になるのではないかと思う。

○（委員長）　検挙と防犯の言葉がつながってしまい曖昧になるという点で、検挙が最大の防犯であると言ったが、サイバーの世界で、検挙がそう簡単にできるとは警察側も考えていないと思うし、我々も甘いものではないと思っている。その意味で、ボットネットを潰していくといったことのほうが、今の段階ではウエイトが大きく、将来的にも大きいのかもしれないとは思う。

○（委員）　前書きの部分で、技術やサービスがサイバー空間において不正に利用されている場合の、それらを提供する事業者が負う社会的責任と説明責任について書かれているが、事業者の立場からすると、過度な責任の押しつけという印象を受けるのではないかと思う。

通信事業者は、いわゆる情報の流通ということに対して責任を負っている立場であり、例えば、違法情報が流れている場合に、通信事業者がすぐに悪いと

されるのかというと、そうとまでは言えない。したがって、もちろんこうした取組に対してしっかりと対応することは当然の話だと思うが、こういった観点を踏まえた書き方にしたほうが、多くの通信事業者の立場からすれば、良いのではないかと思う。

また、レンタルサーバについても、通信事業者が全てと言えるのかというグレーの部分が出てきていることも実態であり、そういった意味で、ニュアンスが難しいところだと考えている。

○（委員）　レンタルサーバについて、先進的に不正利用対策に取り組んでいる事業者と対策が十分に行われていない事業者との間の連携という話があったが、対策が十分に行われていない事業者に加えて、規模の小さい事業者への対策も重要になると思っている。特に、不正なアップロードサーバに関しては、大手と小規模の事業者に二極分化しており、アップロード先は都内の小規模事業者が意外と多いと思う。また、１カ月程度の短期間契約が非常に多いと感じている。その中でも、特に標的型攻撃に関しては、１年間くらい遡って見る必要があるので、解約の契約情報に関しても、１年間くらい保持するように事業者へ要請していくことも有効なのではないかと思っている。

○（委員）　提供する技術・サービスが不正に利用されている事業者の社会的責任という話について、現代のＩＣＴ社会、あるいはデジタル社会において社会的インフラと言えるものを提供しているわけであるから、およそ事業者についても、社会的責任は生じると思う。一方で、そのまま記載してしまうと、先ほど指摘があったように範囲が広すぎると思うが、不正に利用されている事業者という文言で限定をかけることでバランスの良いものになっていると感じた。

○（委員長）　サイバーの世界をより良くして犯罪を防止するため、少しずつ前に進めるということだと思う。警察がまた、業界に責任をさらに押し付けるような方向で動いているというわけではなく、これまでと同じように、不正に利用されている事業者は、少なくともどれだけの対策を行っているかの説明責任は果たしてくださいということである。

○（委員）　通信業界では、アカウントの不正利用でスパムを大量にまき散らして逃げていくような悪用等、様々なことが過去起きており、現在は総務省の指導をいただき、民間でガイドラインをつくっている。

特に、アカウントの不正利用において、ユーザーを特定するといった場合に、通信の秘密との関係性において問題が生じる場合があるため、ガイドラインを整備して、円滑に対策が打てるような取組をしている。以前は、大量通信ガイドラインと呼んでいたが、今は、サイバー攻撃対象におけるガイドラインと名前を変えて運用している。

○（事務局）　不正に利用されている事業者という限定、防止を図る社会的責任という表現、さらに、被害防止策をとれというわけではなく、どのような被害対策をとっているかについて、少なくとも説明してくださいという言い方という３段階に分けて記載しているため、理解を得やすく、少なくとも過度な要求はされない形の表現になっていると考えている。

○（委員）　レンタルサーバについて、事業者によっては無償でセキュリティの機能を提供していたりするが、利用者がそのような機能を意外と知らないのではないかと感じており、今回の趣旨とは少しずれるかもしれないが、レンタルサーバ事業者による対策のところ等に、利用者に対する啓発を強化するといった文言も入れておくと良いのではないかと思う。

○（事務局）　それは事業者が啓発するということか。

○（委員）　そのとおり。契約時やトップページ、ログインページ等に広告のような形で、こういう機能がある等の悪用されないための意識付けを進めるような文言があると良いのではないかと思う。

○（事務局）　利用者に対する啓発は、先ほど議論いただいた前書き部分にも記載しており、それとのつながりもあると思うので、検討させていただきたい。

○（委員長）　こういう問題があるということを、利用者一般にアナウンスすることは良いことであり、大事なことであるが、それを義務付けるといったことは難しいので、表現は検討してもらいたい。

ここまでで発言いただいた、WannaCry の書き方や捜査関係事項照会の電子化、レンタルサーバに「等」を入れること、日本語の修正といった部分の修文は、お任せいただくこととして、基本的に、こちらを報告書として取りまとめてよいか。

（一同、異議なし。）

それでは、こういった形で、報告書は取りまとめさせていただく。

４．　各委員コメント

○（委員長）　最後に、各委員から本会議全般に関して、一言いただきたい。

○（委員）　昨今のサイバーセキュリティにおける課題については、シンクライアントを世界的に行っているところであり、米国ではグーグルが、8.8.8.8のＤＮＳを使って世界中の不正を暴きにかかっていたりする。今回の会議では、ようやく日本もサイバー犯罪に対して動き出したということを非常に感じた。引き続き、こういった議論が進んでいくと良いと思う。

○（委員）　諸般の事情で、仮想通貨に関する議論が取りまとめられなかったことは、残念ではあるが、やむを得ないと考えている。仮想通貨をめぐる議論については、今正に、最近起こった事件等を踏まえ、業界の中でどういう対応をとるべきか等の検討が始まろうとしているところである。

仮想通貨の問題は、インターネット、サイバースペースの問題が端的に現れた１つの形である。これまで我々が考えてこなかった、そういうことが多分起こらないだろうと思っていた基本的に国内に閉じていたものが、サイバースペースができたことによって、急速に一般の市民まで含めた形での国際的なつながりになってしまい、そこに、様々な攻撃の原点や被害の対象ができるなどした。全体を止めることができれば良いのかもしれないが、既に様々な形で取引等が動いてしまっている以上、それは難しい。現在、アルゼンチンでG20が開かれ、そこで、国際的な規制をどうするかという話が行われていると聞いている。そういったところでの議論を踏まえつつ、国内の対応もさらに進めていく、この会議でも、一段とそういった観点からの検討を進めてもらえればと思う。

○（委員）　今話にあったようなブロックチェーンを始め、次々とイノベーションが進んでいっている。一方で、WannaCryの話もあったが、いまだにフィッシングメールを踏んでしまう、パスワードをずっと1234にしているなど基本的なところから来る犯罪も存在しており、やはりまだまだ国内、国外問わず、サイバーハイジーンというか、対策ということについて、啓発していかなければならない。

つまり、サイバー空間における活動でベネフィットを受けていく中には、リスクがあるということを認識しなければならないということを常に啓発していかなければならないということである。今回のサイバーセキュリティ政策会議

では、防犯の点からいろいろ行っていることは重々わかるが、引き続きその啓発を行っていくとともに、日本がSociety5.0に向かっていく中で、新たな価値を創造しながらどのようにこのサイバーリスクに対応していくのかというところも日々見ながら、この会議も先に進んで行ければ良いと思う。

○(委員)　平成13年の前身となる総合セキュリティ対策会議のスタート以来、様々な検討内容について、通信業界としてもいろいろな形で取り組んできており、サイバーセキュリティの観点では、これからさらに、いろいろな官民連携が求められると思う。

今年度の内容についても､これをうまくフィードバックしていきたいと思う。

○（委員）　サイバー犯罪対策と、サイバーセキュリティ対策という言葉は、もう同じものとして扱っていかなければならないと感じている。通信事業者が犯罪対策という言葉を使うことは、過去にはあまりなかったが、最近では、それをあまり隠さずに使うようになってきている。

こういった点では、やはりこのような政策の議論に事業者が参加することは重要だと思うし、また、互いの人的関係、信頼関係を構築する上でも重要だと思っている。

また、ボットネット対策等についても、まだ将来に向けて課題を残している状況なので、こういった点も今後議論をしていきたいと考えている。

○（委員）　匿名性を利用した犯罪をどうするかということは、サイバーセキュリティを考える上で大きな課題になるが、今回、そのレンタルサーバ等に関して、これをどうするかという具体例を通して、官民連携の一層の強化という方向性が示されたのは、良いことだと思う。

また、シンクホールを実施する際に、検証令状を活用する、法の柔軟な解釈により対応するということには賛成だが、一方で、非常に固い解釈も見られるところであり、かかる人たちを今後どのように説得していくかという課題が残ると思う。

○（委員）　サイバーセキュリティ、サイバー犯罪の分野は、端的に言うと、多元方程式を解かなければならないが、それを解いている間にも新しい変数が出てきてしまうのである。これらは、一個一個変数を減らしていくしかなく、レンタルサーバの部分も、指摘があったように、範囲をどうするといったこと

もあると思うが、できることを確実に一個一個片づけていくことが、非常に重要だと思う。最低限、国内のレンタルサーバから防弾ホスティング（事務局注：サイバー犯罪者を守ることを目的とみなされるレンタルサーバ等のこと）を出さないという部分を、まずはしっかり行うということが、非常に重要なことだと思う。

また、仮想通貨に関しては、報告書に取りまとめられていないことは残念に思う。クレジットカードの犯罪が増えて、対策によって減って、インターネットバンキングの不正送金が増えて、減って、またクレジットカードが増えて、最近では、仮想通貨が悪用されているという状況である。端的に言うとこれは銀行強盗だが、これと不正送金、マネロン、大きくこの３つにどう対応していくのか、少なくとも国内の取引所に対してどういう働き掛けを行っていくのかが、課題だと思う。

○（委員）　広く官民連携を行っていくことは非常に重要だと思うが、そのとき、民間をどこまで連携に入れるのが良いのかというところを、一度はっきりさせておくほうが良いと思う。なぜなら、海外で一度、サイバー犯罪を議論する会議に出席したとき、そこで使われている官民連携の民というのが、「国家に協力する民」という定義であって、被害を受けるユーザーや他の広く一般の企業は民の対象になっておらず、少し驚いたという経験があるからである。

それでは、日本で取り組む官民連携において、どこまでの範囲で民と連携していくべきなのか、それを警察側からどう考えるのかといったときに、例えば、未然に防ぐということが重要だという視点に立ったときには、広く被害を受ける民もその連携の対象に入っていなければ、やはり議論の対象が犯罪者を検挙するというところに重きが置かれ、未然防止というところに、なかなか視点が行かないのではないかと思うのである。民間とどこまで連携していくべきか、どういう官民連携をするべきかといったところをしっかりと検討してもらいたいと思う。

○（委員）　ＤＤｏＳ攻撃をしてきているウェブカメラのような、安易なデバイスをつくっている製造事業者、ＯＳをつくっている人、サーバをつくっている人、通信を担っている人、サーバを預かっている人、あるいはそのサービスを提供している人、全ての事業者が、やはり当事者であると思う。よって、前

書き部分の事業者の社会的責任というのは、ある特定の事業者というよりは、サイバー空間を利用してビジネスをやっている事業者全てが一緒になって官民連携して、そして、何とか出ている被害を防いでいく、あるいはその当事者を排除していくという決意を持って取り組んでいくということを示すものと思っている。

引き続き、官民連携で一緒に対応していきたいと思う。

○（委員）　本会議は、公権力を行使する警察とそれに協力する民間との連携を深めていくためのものであるが、これまで常々配慮してきたことは、民の範囲と、その対策の深さということである。深すぎれば、権力の行使になってしまうが、浅くても駄目だということである。また、民の範囲という点では、アウトサイダーをどうするのかという問題が常に出てくる。協議会や業界団体等をつくっていても、常にそういうものにはアウトサイダーが存在するため、そういったところにも間接的に影響を与えるような会議でなければならないと、これまでやってきたと思う。

こういった会議の結果というのは、業界の方々、民の方々を含めて国民に受容される、受け入れられるものでなければならないため、そのバランスを考えつつ、この会議が今後も継続すれば良いと思う。

○（委員）　前身となる総合セキュリティ対策会議から出席しているが、この会議の良いところは、取りまとめた報告書の中身がきちんと実現されていくことだと思っている。法律の制度をつくるわけではないが、きちんとした官民の協力体制が１つずつ積み上がってくるところがすばらしいと思う。報告書についても、非常に工夫し、距離感を保ちながら書かれており、読み手も安心できるのではないかと思う。

官民協力の中で、民ができるもう一つのことは、こういう報告書を踏まえて官民協力をしても、どうしてもルールのほうに行かなければならないものがにじみ出てきたときに、民間側からも、そういうルールが必要だという声を上げていくことだと思う。

○（委員）　道路交通安全の分野でも、車の事故、人身事故が起こってしまうことが一番悲劇的なことで、そういう点に一番訴求力があるため、警察が中心となるが、やはり事故が起こって犯人を捕まえて処罰するだけでは足りないと

いうことで、例えば、道路の構造、車の保安基準といった点で、国交省との連携が出てくる。他にも、保険会社の対応、運転代行業の整備等、いろいろな対策があって道路交通の安全が確保できるのである。

道路交通に関しては、長い歴史もあり、また、変化のスピードもそれほど速くないため、その都度対応していけばよかったと思うが、現在、同じようなことがサイバーで起きており、これは変化が非常に激しいものであるから、いろいろな業界の方がいらっしゃる会議の場は、やはり必要になってくると、今回改めて感じたところである。さらに、総合的という言葉の意味の話もあったが、サイバーと道路交通との最大の違いは、サイバーの場合は、現実問題として、犯人検挙に結びつかないということである。この場合、その前段階の、正に警察の枠を超えた総合的な対策の必要性がより大きくなってくる。変化も速いため、常に意識の共有、すり合わせをしていかなければならない。本会議のテーマは、その一環としてのものだったと感じている。

○（委員代理）　2016年、Ｔｅｌｅｃｏｍ-ＩＳＡＣはＩＣＴ-ＩＳＡＣという形で、ＩＣＴを取り込んだＩＳＡＣ組織になった。今後は放送も通信と融合していくということである。現在、放送業界の中でも、いわゆるデジタル技術というものが、ＩＰ技術にどんどん変わっており、そういったＩＰ技術のセキュリティをどのように守ってコンテンツを安全安心に家庭に届けるのかということを日々考えている。

先日も、ある会議に参加し講演をしたが、そういった機会を捉えて、わかりやすく、セキュリティにどう対処していくかということを、どんどん啓発していくことが必要なのではないかと思っている。今後も、こういった場に参画して、情報を発信し、皆さんと共有していきたいと思う。

○（委員）　本会議では、特にシンクホールに関して、非常に興味深く考えさせていただいた。

また、ＪＰＲＳに言及したことは非常によかったと思う。引き続き、非常に難しい題材ではあるが、議論に参加していきたいと思う。

○（委員長）　基本は、いかに民の力をいただき、犯罪について、逮捕・検挙、そしてそれ以前の抑止のための力をつけていくかということである。官の力はほんの一部でしかなく、一方で、民の力を束ねるという偉そうなものでもなく、

横串を入れるという意味で、本会議は、一定の意味を持ってきたと思う。

しかしながら、総務省、経産省、金融庁といったところとの官同士の情報共有、官官連携も必要であると感じる。実際のところ、民の側は各省庁の様々な会議に参加しているが、メンバーはかなり重なっており、頭だけが違うのである。官には伝統的に縦割社会が残っているが、サイバーの世界でそのようなことを言っていては、国民の利便性や、安心・安全は守れない。

その象徴が、今回の仮想通貨の問題である。時流に乗った仮想通貨について書くほうが、報告書として良いのではないかと思う部分もあるが、どういう形でどういう報告書を出していくのが一番日本全体としてのパワーアップにつながるかという視点に立ち、このような取りまとめとなった。各省庁の連携がより緊密にならなければサイバー社会は守れないということを実感した会議であった。

５．　長官官房サイバーセキュリティ・情報化審議官挨拶

本年度のサイバーセキュリティ政策会議は、昨年 10 月 27 日の第１回会議以降、新たな傾向のサイバー犯罪等に対応するための官民連携のさらなる推進とのテーマで、官民双方が抱える課題、官民が連携した対策の今後の方向性について議論をいただいた。

各回の議論を通じて、新たな傾向のサイバー犯罪等に対する、警察及び各事業者における取組と課題等について、制度的な枠組みのあり方まで含め、大変貴重な発表、意見をいただいた。

これらを踏まえ、新たな傾向のサイバー犯罪等に対応するための官民連携の更なる推進に向けて、本日、本会議の報告書として取りまとめいただく運びとなったことを、重く受けとめている。

先ほど各先生から言及があったが、サイバーの関係は、スピードが速く、また、近年では、様々な社会全てに、サイバーが浸潤してきている。

また、官民連携については、日本の場合、民の範囲が広い。文化論に逃げることは好きではないが､それは日本の良いところなのではないかと感じている。加えて、そういった点では、各省庁の連携についても、いろいろな面で資源的に余裕がないという状況で、国全体として、資源を適正に配分して対応してい

かざるを得ない世の中になっていると認識をしている。今後も、いかなる措置を講じるかについて、関係する皆様と、実務的、具体的な検討を行っていく必要があると考えている。

今回の会議については、皆様方に、充実した議論、報告書の取りまとめをいただき、御礼を申し上げるとともに、引き続きまたいろいろな面で協力をいただければと思う。

６．　閉会