サイバー安全保障分野での対応能力の向上に向けた有識者会議
通信情報の利用に関するテーマ別会合（第３回）
議事要旨

1. 日時
令和６年８月26日（月）18時00分から19時00分までの間

2. 場所
オンライン開催

3. 出席者
（有識者）

上沼　紫野	LM虎ノ門南法律事務所弁護士
川口　貴久	東京海上ディーアール株式会社主席研究員
川添　雄彦	日本電信電話株式会社代表取締役副社長 副社長執行役員 一般社団法人 電気通信事業者協会参与 一般社団法人 ICT-ISAC理事
酒井　啓亘	早稲田大学法学学術院教授
佐々江　賢一郎	公益財団法人 日本国際問題研究所理事長
宍戸　常寿	東京大学大学院法学政治学研究科教授
篠田　佳奈	株式会社BLUE代表取締役
土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
野口　貴公美	一橋大学副学長、法学研究科教授
丸谷　浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表
村井　純	慶應義塾大学教授
山口　寿一	株式会社読売新聞グループ本社代表取締役社長
吉岡　克成	横浜国立大学大学院環境情報研究院／先端科学高等研究院教授

4. 議事概要
（１）河野国務大臣挨拶

○　今日は午後６時という遅い時間にもかかわらず、お集まりいただきましてありがとうございます。この会合は、朝だったり夜だったり本当にいろいろな時間でございますが、皆様にはお差し繰りいただいて、いつも御出席いただいておりますことに改めて御礼を申し上げたいと思います。

○　テーマ別のこの会合もいよいよ３巡目ということになります。本当に短い間に集中的、精力的に御議論いただきましたことに改めて感謝を申し上げたいと思います。

○　今回は、前回の親会でお示しいたしました議論の整理と親会における議論を基に、事務局において提言のたたき台になるものを用意させていただきました。これまでの会合と同様に闊達な御議論をしていただきたいと思います。本日も限られた時間ではございますが、どうぞよろしくお願い申し上げます。

（２）事務局説明

事務局より、資料に基づき、通信情報の利用に関する提言素案について説明があった。

（３）討議

各有識者より、以下のような発言があった。

○　今まで議論してきたことを的確にまとめていただいている。
○　107 行目辺りのパラグラフに書かれている「独立機関」について、ここでは、おそらく独立機関が政府の責任で実施される施策をしっかりと管理することで、その正当性が証明される仕組みが書かれていると思うが、これに加えて、電気通信事業者が行う範囲においても、独立機関がしっかりと見て、場合によっては、例えば、電気通信事業者に訴訟のリスクが生じたときに、独立機関からしっかりと正当に見てもらっていることが証明できるとスムーズに業務が継続できると思うので、その辺も考慮していただけるとよい。
○　141 行目の「定期的な報告書の公表」について、全てが公開できるわけではないことは皆さんの御理解のとおりだと思う。大枠の適切な情報公開は行われるべきと書かれているが、それでもやはり非公開とすべき内容もあり得るということも、国民の理解を得るためには何らかの形で記述しておくと安全ではないか。

○　67～71 行目のペンディングとされている箇所について、通信情報の利用範囲を外外に限るか、外内の同意のない利用も視野に入れるかという点は、さらに議論を深める必要があるのではないか。95 行目にあるように、通信の秘密の保障と公共の福祉を両立させて、かつ、実効性のある防御を実現することが重要であり、外外に限るよりは、外内まで対象にしたほうが実効性は高まると思われる。
○　そもそも能動的サイバー防御の目的は国民の安全な生活を守ることにあるわけで、通信情報を国民の監視に使うことは絶対にないと言い切れるはず。プライバシーは徹底して保護し、独立機関を設けて監督をし、収集したデータは人間の目で判断するわけではなく、主として機械的に処理をしていく、となっていくと思う。
○　このような制度全体の検討とかみ合わせながら、通信情報の利用範囲をどうするかを有識者会議において幅広に議論をしておく必要がある。

○　全体としてこれまでの議論を包摂し、適切にまとめていただいた。
○　67～71 行目について、ペンディングになっている節は削除をして、必ずしもトランジット通信に限定しない方針を示していただきたい。内内通信、つまり国内のドメス

ティックな通信について現段階で積極的に利用を行う必要はないと思うが、外国から国内に入ってくる通信については対象に含めるべき。無論、国内にサイバーセキュリティ脅威がないということではないと思うが、14 行目に書いてあるとおり、国外に所在するアクターというのが我々にとって一番考えなくてはいけない点であるので、ここの整合性をとるためにも、国外に所在するアクターからの通信は見るべきだ。国外に所在するアクターによるサイバー攻撃は、情報が極めて限られており、その動向をつかむためには、外から内への通信について捕捉、分析することが不可欠。サイバー攻撃の動向を未然につかんで防ぐということを今回は狙っているわけであるから、外外のトランジットに限るというのは不十分ではないか。

○ 更に言えば、国内でマルウェア等に感染したコンピューターがどこに向かって信号を出しているかを捕捉するためには、内から外への通信についても見る必要があるかもしれないため、それも対象に含めるべきである。外国勢力の協力者が国内にいる可能性も大いにあり得るし、サイバー攻撃の準備は複雑な経路を使って頻繁に行われるはずで、その動向を把握するためには、どちらか一方だけの流れを見るというのはおかしな話なのではないか。

○ 150、151 行目の「分析した情報を活用するなどして、企業・国民にとって便益がある仕組み」という表現について、それはそのとおりだと思うが、逆に分析した情報が政治的、社会的に悪用されるような使い方は決して行わないということも再確認してはどうか。例えば、仮に通信情報の取得から政治家のスキャンダルや国民の脱税等が見つかったとしても、訴追に使ったり、リークして週刊誌に流したりすることは、目的外の情報利用となるため決して行わない、ということがこの制度への信頼を高めることになる。どこまで書くかはお任せするが、国民への説明として確認しておくべき。

○ 既にサイバー攻撃で私たちの通信の秘密が侵害されている状況があるために、今回の制度、法案が検討されているということを明記すべき。

○ 今回、各委員が様々な観点で申し上げたことを整理いただき、感謝。

○ 67～71 行目のペンディングとされている箇所について、ペンディングの箇所を削除して、外内通信、すなわち、日本に入ってくるインバウンド通信と日本から出ていくアウトバウンド通信をスコープに入れることを明確化すべき。

○ 72～77 行目の分析の対象とする必要がある情報の範囲について、コミュニケーションの本質的内容以外に注目し、これらを全て活用する必要があるということには同意。重大なサイバー攻撃を防ぐために、ⅰ～ⅲを十分に活用していく必要がある。

○ ペイロードでもマルウェアのようなデータも活用の対象とすべきであり、ヘッダーとペイロード、データとメタデータについては理解を深めるという意味で注釈を入れてはどうか。

○ 152～156 行目の今後の検討課題について、非構造化データの分析も視野に入れる部分は重要な指摘。通信情報の分析に当たっては、非構造化データの分析に限定されず、他のデータとの結合や突き合わせが必要となる場合があると思うが、新しい実働組織が、経済的なインテリジェンス情報やキネティックな軍事動向に関する衛星データ等のようなオールリソースでの情報収集結果にアクセスでき、通信情報と併せて

分析できることが重要。

○ 非常に丁寧にこれまでの議論を取りまとめていただいていると思う。
○ 67～71 行目のペンディングとされている箇所について、外内、内外も対象とするよう立法措置すること自体は意味があることだと思うが、ただ削除するのは議論のやり方として若干懸念を持つ。なぜ外外だけではなく、外内、内外も必要なのかをしっかり丁寧に書くことが大事。議論の透明性のため、まずは外外が必要であるという議論をし、それから外内、内外も必要ではないかという結論に至った経緯をしっかり示していく必要がある。また、実際に独立機関を作って監視・監督するときには、外外だけであれば、外外以外のものを見ていないかという部分に監視・監督の力点が置かれるところ、外内、内外も含むということであれば、もう一段深く監視をしなければいけない、というように跳ね返ってくる。
○ 111～116 行目の「通信当事者の同意がない場合の通信情報の利用」について、ここでは電気通信事業者だけではなく、様々な通信当事者、特に重要インフラ事業者のことをひとまず念頭に置きながら議論してきたというステータスであることを踏まえ、通信当事者として誰を念頭に置いているのか追記すべき。
○ 114 行目の「制度により規格化された内容による同意を必要に応じ制度により促していく」について、少なくとも協議を一定の事業者に対して政府が求めることができるとか、協議を義務づけられるところまで踏み込んでもよいのではないか。重要インフラ事業者の中には海外の資本が一定程度入っている事業者もいるかもしれないし、株主との関係や経済合理性の観点から見て、政府との協議について、最終的に応じるにしても、二の足を踏むといったこともあり得るかもしれない。また、日本は資本主義国家であり、重要インフラも一社独占というわけではなく、複数の企業が競争しながらサービスの質・量を高めているところ、業界でまず誰が最初に政府と話をするのかという事態になるのもどうかと思われる。そういう意味で、この協議の促進については、もう少し具体的な施策があってよいのではないか。
○ 132～134 行目の独立機関のガバナンスについて、マイナンバー型のように官民両方を見る、あるいは官民の間のデータの流れが適正になされているかを見る組織であり、電気通信事業者についてもしっかり監視し、その監視・監督の結果が電気通信事業者にとって意味のあるものにするのだということをはっきりさせてもいいのではないか。
○ 145、146 行目の「通信情報の利用を通じてサイバーセキュリティが強化されることにより、通信の秘密の保護の強化が図られるという側面がある」について、通信自体が妨げられないこと、あるいは中身が他人に利用されないことにより、サイバーセキュリティが実現されることによって、通信の秘密ないし通信の秘密が前提とする通信の自由が確保され、これを国家が守っていく側面があることが書かれているが、これは重要な点かと思う。
○ 140 行目の「運用の詳細などまで全てを公開することは性質上難しい」について、これでよいと思うが、もう少し正確に言うなら、「通信の秘密を守る側面のある国家の活動であるがゆえに、手の内を全部さらしてしまうということが、活動の目的達成を阻害するところがあり、だから非公開にしなければいけない部分がある。他方で、そ

れを全部隠してしまうと、不必要な権力の濫用が行われている可能性があるので、透明性を高めていくということも同時にこの施策にとって非常に必要なことであり、その的確な両立を果たしていく」ということであり、修文される場合には御確認いただければと思う。

○ 67～71 行目のペンディングとされている箇所について、通信情報の利用の対象としては、基本的に外国から日本、日本から外国、日本を経由する外国から外国の３つとも対象になると思う。
○ 「トランジット」の定義について、委員のコンセンサスとして、外国から外国の通信が日本を経由して行われていることをトランジットと表現していると理解。専門用語としては、トランジットは、インターネット通信の場合だとＡＳトランジットを指すが、今日の議論が、例えば、ボット等を含めたサイバーセキュリティ上の脅威について、①日本が端点になっている場合、②海外が端点になっている場合、そして、③日本が中継点になっている場合を考える必要があるという論点についてであるとすると、トランジットもそうした文脈で使われる重要な言葉になるため、もう少し表現を理解しやすいようにする必要がある。
○ ボット等の踏み台が日本にあることは世界的な信頼の失墜につながるところ、きちんと対応しなければならず、それなりの説明をして、重要な課題だと表現した方がよい。

○ 有効性、実効性を能動的サイバー防御の観点から上げるという意味では、外―外だけではなく、外―内、内―外も対象にした方がよい。本当は内―内まで対象にした方が良いとも思う。
○ 「トランジット」という表現は誤解を招くおそれがある。
○ プライバシーの保護や独立機関等など色々な歯止めをかけているところ、今回の「アクティブ・サイバー・ディフェンス」という言葉に即するように、実効性を高める仕組みをどうするかを一義的に考えれば、外―外に限らず外―内、内―外も検討すべきではないか。

○ 全体として委員の意見をよく取りまとめていただいている。
○ 67～71 行目のペンディングとされている箇所について、外外の通信のほか、外内や内外の通信も対象とすべき。ただ、単にこの箇所を削除するだけではなくて、外内の通信を対象とする理由付けを付すことが望ましい。
○ 今回の検討においては、我が国が能動的サイバー防御を行うことを前提に議論がなされているが、逆に外国側から同様の措置がとられる可能性も今後出てくることを考えると、日本が攻撃の端点や中継点になっているような場合も含め、我が国の領域の中でどういうことが行われているのかということについて不断に注意を払わなければ、我が国が相当の注意を果たしていないという批判を受け、国際法上の国家責任を問われることも生じ得る。また、外国の活動との協調等の関係においても、日本でどういうことが行われているのかを説明する責任があるという観点から、対象を外外にとどめることは避けるべきだろう。

○ 97 行目以下の実体的な規律とそれを遵守するための組織・手続的な仕組み作りが必要であり、明確で詳細なルールとなるよう考慮することが適当である旨が記載されている箇所について、これはそのとおりで強く支持する。他方、こういった分野では新たな状況が生じる可能性があり、その場合にどう対応するのかを念頭に置いておかなければならない。国民の権利を制限するおそれがある場合には、法律にできるだけ特定した形でその要件が書き込まれるのが理想ではあるが、場合によっては、法律の解釈や運用で対応できるようなところを残しておくことはできないか、あるいは、どうしても新たなルールが必要となった場合、デュープロセスの観点から見直しが必要となる事情や見直しの対応をどのように判断し行っていくのかも考えなければならないだろう。近い将来、このようなことが起きるかもしれないということも目配りとしては必要なのではないか。

○ ここまでの、難しい議論を的確にまとめていただいたことに感謝。
○ 136 行目以下の透明性の確保の重要性、それにまつわる公開に関する議論について言及がなされている部分について、「情報を公開するということ」と、「情報を記録し保存しておくこと」とは異なるフェーズにあるということを今一度確認しておく必要がある。つまり、「公開ができない、または公開すべきではない、公開が難しい」情報であるとしても、サイバー領域においてどのような行政活動が行われたかをトレースするために必要になる情報や、そこで集積された情報については、きちんと管理、記録、保存し、適切な段階で必要に応じ廃棄するというプロセスを整えておくことが非常に重要である。これは行政情報一般にいえることであるが、後に行政活動がどのように行われたかを振り返り、検討するために必要な情報の保存管理、情報の取扱いに留意する必要がある。
○ 21～28 行目の通信傍受法に触れている箇所について、これは大変重要な指摘だが、「通信傍受」という単語を用いることによる議論が生じる余地があると思うので、これを読んだ人が誤解しないよう、少し丁寧に説明しておく必要がある。今回の通信情報の利用は通信傍受とは違うということが書かれていると思うが、「何が、なぜ、違うのか」を一言でもよいので説明として加えておくとよいのではないか。つまり、通信傍受法の傍受とは犯罪捜査のための傍受、つまり司法警察作用であるからこそ、捜査のターゲットが明確になっていて、しからば個別的で、なおかつ裁判所が令状を出すという意味での司法的な手続を経て行うものとされているということである。これに対して、サイバー領域の情報の収集・利用というのは、被害の未然防止や被害が生じようとしている場合に即時に対応するのにも必要となる情報の議論であって、司法的作用ではない、行政権限行使の領域に位置づけられるものを中心として議論していると整理できる。そうであるからこそ、通信傍受と相違があり、別の手だてを考えていく必要がある、と説明できるのではないか。この点が伝わるような説明が、一言でもあるとよいと考える。

○ 提言案の核となっている部分は、これまでの議論を踏まえて適切に記載いただいている。
○ 11～13 行目の「攻撃者は、攻撃元を隠蔽するため、一般利用者の通信機器をマルウ

ェアに感染させるなどして乗っ取り、これらの通信機器（ボット）を多数、多段的に組み合わせて構成された攻撃用のネットワーク（ボットネットワーク）を利用することが通常である」について、これは本当にそのとおりではあるが、実際の攻撃インフラは、一般利用者の通信機器だけでなくて、クラウドやホスティングといったようなものも大いに活用した複合的な構成になっていて、むしろどちらかというと、攻撃インフラの中で核となっているＣ＆Ｃサーバー等は、末端の機器というよりも、クラウドやホスティングサービス上で動作していることが多いと理解。

○ 用語の定義にもよるが、専門家がボットネットと聞いたときには、多数の機器を一斉に操作するタイプのサイバー脅威を想起する。その定義でのボットネットとは関わらない脅威も非常に多く、むしろ高度かつステルス性の高い、いわゆるＡＰＴのような標的型攻撃は規模が小さく、ボットネットとは対極的な脅威だと思う。最近はそれらがハイブリッド化していて、標的型でもボットネットを使う事例も出てきている。実際に 18 行目には「ボットネットワーク等」と記載されているので、ボットネットはあくまで一例であると解釈することもできるが、今回の対象とする脅威がもっと広いものであれば、少し表現を工夫してもよいと思う。

○ 濃い形でまとめていただき感謝。

○ 82 行目以下で通信の秘密との関係を書いていただいているのは大変ありがたい。本検討は決して通信の秘密を軽く見るものではなく、通信の秘密は重要だということを前提に検討していることを書くことが重要。

○ その上で、88 行目について、単純に公共の福祉のための制限というのではなく、今回守ろうとしているものが国民の安全や平穏な生活といった非常に基本的な価値なのだということを、もう少し積極的に書いてもよいのではないか。

○ 67～71 行目のペンディングとされている箇所について、自分たちの安全を守るために何を見るのかと考えたときに、外外だけだというと、一般国民としてみれば、「通信情報の利用は私たちの安全のために行うものではないのではないか」と思ってしまうのではないか。そういう意味で、内と外の間の部分も対象に入ると考えている。今回何を守ろうとしているのかという観点から検討していただけるとありがたい。

○ 146 行目に「通信の秘密の保護の強化が図られる」ことを入れていただいたのは大変ありがたいが、どう強化につながるのかがすぐには分かりづらいので、既に平穏な生活、あるいは平穏な通信が侵されているところ、それを守るために、通信情報を利用することで通信の秘密の保護が強化される、という内容を入れると、すっと頭に入ると思う。

○ 150 行目の「分析した情報を活用」について、これは非常に重要だが、活用の目的は、セキュリティ、あるいは自分たちの安全に役立つという便益の形で戻ってくるということが明確にされるとよく、この部分が「官民連携に関するテーマ別会合」にもつながることが明確になるとよい。

○ 通信情報の利用の対象として、外外、外内、内外の全てを網羅するということは理解するし、議論の透明性を確保するためにこれらを利用する理由を明確に説明すること、独立機関を設けること等をもう一段深く説明していく必要があるのではないか

という議論はそのとおりだと思う。通信当事者の有効な同意についても引き続き考えていかなければならない。

○　通信傍受法との相違について、過敏な反応を招かないよう、書き方には注意しなければならないと思う。細かく書き過ぎてはいけないし、広く包括的に書く必要があると理解。

以上