資料６－４

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２回）
議事要旨

1. 日時
令和６年７月26日（金）10時00分から11時15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
遠藤　信博	日本電気株式会社特別顧問
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
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

4. 議事概要
（１）事務局からの連絡
会合の冒頭、事務局より以下の連絡があった。
○ 本会議の討議テーマである「通信情報の利用」に関して、直近の一部報道において、政府として特定の方針を決定した、あるいは特定の方向で具体的検討に入ったかのような取り上げがあった。
○ 言うまでもなく、サイバー安全保障分野における新たな取組の実現のために必要となる諸方策は、本有識者会議で皆様に御議論いただいた上で決定していくべきものであり、政府として、報道にあるような内容について決定したという事実はなく、また、私ども準備室の方から報道機関に対し、そのような説明を行っているということもない。

○　皆様には、御心配をおかけしたことにつき、この場をお借りしておわびを申し上げたい。

（２）事務局説明

事務局より、【資料１】に基づき、先進主要国における通信情報利用の実施過程とその制限・監督について、【資料２】及び【資料３】に基づき、これまでの議論の整理案について説明があった。

（３）討議

有識者より、以下のような発言があった。

○　今後の法制化の局面では、各国の実施部門と監督部門との間での実際のやり取りやその課題について各国にヒアリングし、実際の運用上困っていることや上手くいっている点の情報を集めてほしい。

○　「令状主義」につき、個別的かつ司法的なコントロールでは、通信情報の利用と通信の秘密の保護という両方の目的を適切に果たすことができないという趣旨の内容を入れるとよいのではないか。（資料３の１ページ 20 行目）

○　「一定の条件の下、……政府による通信情報の利用を許容する法律が整備されている」につき、これは単に許容しているだけではなくて、いわば制限しつつ許容するという側面が当然にあるもので、権利保障をしながら同時に必要な通信情報の利用を認めるものであることをしっかり表現してほしい。（同２ページ１行目～２行目）

○　「議論を深めることで国民の理解を得ていく」につき、能動的サイバー防御に係る議論について、全て情報公開することは不可能。なればこそ、おおむねこういうことをしていると適切に情報公開し、説明責任を全体として果たしていくことで、国民が理解をし、その結果、国民としても安心できるからもう少し踏み込んでやってもよいというような形で、全体として制度の見直しも含めたプロセスを回していく視点を入れるとよい。（同２ページ５行目）

○　「機械的にデータを選別するとともに、検索条件等で絞っていくなどの工夫が必要」と記されているところは全くそのとおり。機械がやっているから通信情報の利用や分析が通信の秘密の侵害に当たらないということは、ＡＩの議論を見ても分かるとおり、人間が機械を使っている以上はあり得ない。人間が目視しているかどうかにかかわらず、通信の秘密の制限は当然に（例えば、国家が関わる場合には国家権力による制限として）存在している一方で、例えば権利侵害性が低い場合があるのではないか、濫用のおそれが少ないのではないかとかいった形で議論するのが大前提。（同２ページ 18 行目）

○　まずは広く網をかけて調べていき、色々分かっていく中で絞るという部分につき、関連性、必要性を適切に絞っていくプロセスをしっかり確立することが、法律論のみならず実効的な対策という意味でも重要。組織的にも人材の育成という観点でも重要なポイント。（同２ページ 22 行目～24 行目）

○　「通信の秘密の制限に対する通信当事者の有効な同意がある場合の通信情報の利用は、そもそも憲法上許容される」につき、命題としては正しいものだが、現実の能動的サイバー防御に関する通信の秘密に属する情報について同意に頼ることには、法的にいくつか問題あり。（同３ページ 12 行目～14 行目）

・同意の主体とは誰か。企業が通信サービスを通信事業者と契約して利用するという場合において、通信の秘密の制約に企業が同意するということはあり得るが、実際に通信を行っているのは個々の従業員や役員であることが十分あり得る。電気通信事業法上も、通信の秘密の同意として、企業を同意の主体とすることで十分か。また、憲法上の人権の観点で見たときに、利用者の通信に個々の従業員等の個人の通信が含まれることをどう整理するかは一つの論点。

・同意の撤回が起きた場合にどうするか。撤回されると、以後、新しく取得し得る情報を利用できなくなるという問題が起きる。また、既に取得した情報を利用できなくなると大変に面倒。あらかじめ同意の内容に撤回できない旨を定めておくことが求められる。

・通信の秘密の侵害に関する同意の内容とその同意の具体的中身が問題となる。サイバー防御のために求められる通信事業者の対策を利用者の同意という観点から認めて行っていくという取組は既にいろいろな形で行われ、総務省の電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会で４次にわたる取りまとめが行われ、通信の秘密の侵害を正当化し得る同意とは、伝統的には個別同意と考えられてきたが、いわゆる包括同意でも良い場合があるという整理をしてきたところ。すなわち、通信サービスは大量の通信が発生するものであるため、利用者が何について同意をするのか予測が立たないこと、また、同意した通信の秘密の内容が通信事業者等に取得されて利用されることにより、通信当事者にとって不測の権利・利益の侵害が発生し得る場合があることから、包括同意は白紙委任をするようなもので問題があるということを前提にしつつ、サイバー防御あるいはサイバーセキュリティのために必要な同意の在り方や、特定の範囲でしか同意に基づく通信の秘密は利用しないという整理を行って、これを認めてきた。今回について言うと、通信の内容の本質的部分を見ないフロー分析であり、次の段階に進むときには法的な措置を執るなど、作り込んだ状況を前提にして通信当事者が包括的な同意を行うという状況が問題になるのだろう。結局、カスタマイズされた同意ではなく、法律等で何らかの裏付けを持たせた規格化された同意を、通信利用者と通信事業者ないし政府が同意するという形にすることが適切であり、法的に、通信情報のフロー情報の取得を、通信当事者の同意なく実施する場合と、同意によって取得する場合とで、大体同じ状況になるという方向に法的に整理した方がよい。同意による場合の具体策としては、あらかじめ政府がガイドラインを定めておき、能動的サイバー防御に必要な通信の情報の利用やその範囲・限界としてイメージしているものを踏まえ、通信当事者に同意してもらう内容を規格化し、約款のような形で書き、この約款を政府が認可する。通信利用者はその認可された約款に同意をする、といったことが考えられる。また、このような法的裏付けがあると、通信情報が個人情報に該当する場合の個人データ利用につき、法令に基づいて行うという構成が取れる点でも有用。

○　「電気通信事業者……肯定的に評価されるべき」につき、電気通信事業者のこの種の取組は責務であると、国として、国民を代表する国会として、法律でしっかりとした責務規定を置くべきではないか。ただ、そのような規定を置く場合に、対象となるのは通信事業者全体なのか、一定の範囲の事業者なのか、あるいは能動的サイバー防御に協力しますといって手を挙げる事業者なのか、その範囲は今後の作り込み・正当化を含めて議論がもう一段必要。また、同意内容の国による規格化は、通信事業者の訴訟リスクを避ける観点からも有用。（同３ページ 18 行目）

○　資料２は、これまでの議論を的確にまとめており、内容的にも十分なものになっている。
○　資料１において、例えば、「処理・分析」、「提供・共有等」、「保存・廃棄」等の実施主体が明確でない。通信事業者が実施できるのは、単に情報を国の機関に引き渡すことを通信事業の機能として提供することであって、処理・分析やフィルタリング等は、通信事業者ではなく、国の機関が実施するものと理解。情報の引渡しについて、国民の同意を得て、法的にも守られる形にしていただきたい。
○　また、能動的サイバー防御について主体が分かれることにより、能動的サイバー防御として実施する内容と、その過程で通信事業者が協力して実施する内容にそごが生じ得る。そのような場合には、通信事業者が実施する内容についても、法制度上的確にカバーする必要がある。

○　本日の事務局の説明内容に同意。
○　これまで日本の法制度の中で行っていた通信傍受、すなわち、疑わしいターゲットに絞って傍受をする「ターゲティッド・コレクション」に対して、今回やろうとしていることは、ターゲットを絞らない形での情報の取得であり、なぜこれを行わなければいけなくなったかの説明が必要。
○　インターネット、サイバースペースの出現で通信の在り方はこの 20 年で大きく変わってきた。固定電話の時代には、固定電話の向こう側に誰がいるか必ずしも分からないにしても、電話番号が分かっていれば、通信傍受をやろうと思えばできることであったし、その通信の容量は非常に少なかったが、サイバースペースが出てきたことによって、匿名的な通信が大量に出現した。したがって、その通信の中に有害なものが紛れ込んでいるかもしれないのでターゲットを絞らない形での情報の取得をしなくてはいけないのだということをはっきりさせるべきで、通信の状況が変わってきたので、サイバーセキュリティの問題が生じていて、それに対応するための法制を作らなければいけないのだという説得の仕方が必要。
○　資料１につき、可能であれば５つの国の法制度がいつどのようにできたのかを強調するとよい。事務局資料には英国は 2016 年制定等と書いてあるが、ここ 20 年から 30 年ぐらいで、インターネットの普及に伴い、新たな法制度ができているということ。米国では、1978 年に外国情報監視法が制定され、ウォーターゲート事件の後は塩漬けになっていたが、９．１１テロ後のパトリオット法、2015 年のフリーダム法により、新しいサイバースペースの脅威に対応してきた。諸外国は、法制度を変えて、また、新しい制度を作って、サイバースペースの脅威に対応してきたことを強

調すると、分かりやすくなると思う。

○　トランジットについて、周辺情報にも少し目を広げていくことによって全体状況が分かりやすくなるし、周辺国、同志国、同盟国との情報共有の際にも非常に重要なツール・材料になるので、トランジットは他国と同等の分析ができるようにしておく必要があるのではないか。

○　資料３において「議論を深めることで国民の理解を得ていく」との記載があるが、国民の理解を得るには、議論の経過、つまり、どういう経過でこうなったのかを積極的に説明していくことが重要。特に、状況の転換により、大量の通信情報の確認が必要となっていることについて、十分な説明が必要。

○　国民の理解を得る方法として、一般に透明性の確保がよく言われるが、本件の性質上、その全てをつまびらかにすることになじまない。例えば、どんな情報について分析するのかを細かく言ってしまうとそれが外に漏れることになる。したがって、透明性で補えない部分を別の方法で補う必要があるところ、例えば、諸外国で行われているような独立機関による監督のように、信頼性のある独立機関による監督が担保されていることが、制度に対する国民の理解を得ることになるだろう。独立機関の構成や任務は国民の信頼の点から非常に重要である。制度に対する国民の理解が得られることが、通信事業者の協力の観点、例えば、通信事業者が実施する行為に対する肯定的な評価の点でも重要なのではないか。

○　利用者からの同意について、つまびらかにならないものについて同意をしろというのは、利用者からすると無理ではないかと思っている。また、同意構成とする場合、同意しない自由も必要となるが、本件においては同意しない場合、これを対象としないということがそぐわないという点も問題となる。そのため、同意が得られる場合に代替できると評価できるような要件・相当性を検討できるような規定を法律に設けるべきではないか。とはいえ、本件の場合、法律に具体的な要件を詳細に書き込むことは無理があると思うので、これをどう独立機関に検討してもらうのかを書き込むことが望ましいのではないか。

○　「法律」の制度にしていく観点からコメントする。

○　情報の共有に関しては、関係者に対し、明確で詳細なルールとして示すことが重要。また、独立機関の監督の仕組みも制度化しておくことが必要。

○　情報の収集・管理をめぐる責任の分配の在り方が明確になるようなルールを定め、情報管理の各プロセスの中で、情報の収集のみならず、収集した後の情報の取扱い、すなわち、収集した情報の管理・保存の在り方についても、法制度の中で明確に定めておくことが非常に重要であると考える。

○　独立機関の在り方につき、英国及びドイツの例は大変参考になるが、諸外国の仕組みや法制度を参考にするときには、法制度全体の中で、事前・事後の手続も含め、その仕組みがどうあるのかを考えなければならない。今回のテーマに関して言えば、監督機関が行う権限行使の場面だけではなく、それらの周辺にある、事前・事後にある権限統制の手続、特に、司法制度との関係を考慮に入れておく必要があるのではないか。司法的統制、すなわち、訴訟制度や裁判の仕組みは、各国で相当に

違っている。行政の権限行使をめぐる争いについても、実際に権限行使をした段階でないと争えないのか、又は、権限行使の基準を作った段階でその基準についても争うことができるのかなど、各国の制度は非常にバラエティーに富んでいると考えられる。権限行使の在り方だけではなく、権限行使（監督機関が行う権限行使も含む。）の適正性、適法性を確保するための事前・事後の手続についての各国の制度の違い、司法制度の在り方の違いなどを踏まえた議論とすべきではないか。

○　独立機関については、検討の余地があれば、諸外国の仕組みだけではなく、「日本の」情報管理の領域にあるガバナンス、組織の仕組みも考慮に入れてはどうか。例えば、公文書管理については公文書管理法に定める公文書管理委員会があり、個人情報については個人情報保護委員会がガバナンスを効かせている。また、特定秘密については、情報保全諮問会議が置かれている。それぞれの制度の特性を踏まえた相違や濃淡はあるが、ガバナンスの先行事例、独立機関の先行事例は日本の法制度の中にも色々存在しているのであるから、このようなサイバーの領域に近い位置にある諸制度も参考にしながら、日本の社会やこれまでの法制度と連続的で整合的な仕組みとして導入していくことを考える必要があるのではないか。

○　資料３に記載のとおり、通信情報の活用については、国民の理解が必要であるが、国民の理解を得るには、企業や国民に対してどのような便益があるのかを分かりやすく示すことが重要。

○　資料１を見ると、フランス・英国においては、提供・共有が限定されている印象を受けるが、これは、収集された情報がサイバー攻撃のみならず幅広い治安、テロ対策にも使われていて、通信の本質的な中身にも踏み込んでいるため、情報の提供・共有等が限定されているのではないかと推察。

○　他方、今回は、通信の本質に関する内容は必ずしも必須ではないということで、収集された通信に関する情報、機械装置に関する情報、不正なプログラムに関する情報を積極的に活用することで、企業や国民に対して便益があるとよい。情報はアクセス・無害化措置や官民連携に活用されることを期待する。ただし、秘匿性の高い情報も含まれ得るところ、先に成立した重要経済安保情報保護活用法に基づくセキュリティ・クリアランスを適切に活用し、こうしたクリアランスを持った企業にフィードバックするとともに、必要に応じてＪＰＣＥＲＴやＩＰＡを通じ、あるいは、新組織から、サニタイズした情報を国民に対して還元していくなど、最終的に企業や国民に便益がある活用、仕組みとすることが重要。

○　海外に関係する通信に限定した情報のチェックの場合、国内サーバを使用した攻撃の監視が手薄になる可能性がある。これを補おうとするならば、エンドポイントベースの攻撃監視を増強して、これの監視と通信情報を融合した攻撃監視が必要ではないか。

○　また、衛星通信は、直接ネットワークを介さずに、ある特定のところに入ってきてしまうので、これをどう監視したらいいか検討が必要ではないか。

○　これらのような海外に関係する通信を中心に情報を見ていく場合に、どのような抜けやウィークポイントがあるのかを、もう一度我々の中で確認をして、これに対す

る対応を検討していく必要がある。

（４）河野国務大臣挨拶

○　今日もお忙しい中、御参加いただきまして誠にありがとうございました。今日で２回目のテーマ別会合も一巡することができました。皆様の活発な御議論に改めて感謝申し上げたいと思います。

○　民間企業に対する大規模なサイバー攻撃が相次いでいる中で、我が国のサイバー対応能力の向上はますます急を要するものになっていると思います。世界の中で日本が弱いと捉えられないように、我々もしっかり強化していく必要があると思います。

○　引き続き、皆様には本会議の議論にも御協力いただきますようお願いを申し上げまして、今日の会議を閉じさせていただきたいと思います。本当にいつもありがとうございます。

以上