

資料 5 - 7

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1回）
議事要旨

1. 日時

令和6年6月19日（水）8時30分から9時30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
穴戸 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
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

- おはようございます。お忙しい中、今日も御参加いただきまして誠にありがとうございます。6月7日に有識者会議第1回目を開催させていただきました。私から3つのテーマについて重点的な検討をお願いしたところでございますが、今日・明日のテーマ別の会合では、その中で通信情報の利用という点につきまして、諸外国の制度などを踏まえて、必要性それから許容性という2つの視点から集中的に御議論をいただきたいと思っております。私も時間の許す限りテーマ別会合にも出席して、皆様の御意見を拝聴したいと思っております。
- この有識者会議に対する世の中の関心は極めて高くなっております。是非皆様の活発な御議論をお願いしたいと思っております。どうぞよろしく願います。

(2) 事務局説明

事務局より、重大なサイバー攻撃とその対策の現状について、【資料2】を用いて説明があった。

(3) 有識者からのプレゼンテーション

慶應義塾大学大学院政策・メディア研究科土屋教授より、【資料3】の内容に基づき、通信情報の利用に関する国際的な状況について、以下のとおり説明があった。

- 能動的サイバー防御の起源は第二次世界大戦まで遡ることができるが、現在につながる大きな契機は911のテロ。東海岸でテロが起きた後、その日の午後にはFBIがカーニボア（Carnivore）と呼ばれるシステムを米国の主要な通信事業者の中に導入し、特定のデータをフィルタリングしてFBIに流すことで、テロリストたちの通信を監視するということが行われた。
- この後、米国人の多くも知らない中で、大規模な通信傍受が行われてきた。2005年には、AT&Tのサンフランシスコにある局舎の中で国家安全保障局（NSA）がデータを収集しているとの疑いが持ち上がった。
- これと同じ頃、『New York Times』がブッシュ政権によって大量の通信傍受が行われている疑いに関する報道を行ったところ、ブッシュ大統領はすぐに演説を行い、「American person」を含め、テロ対策のための通信傍受をNSAに許可していることを認めた。これは外国情報監視法に違反するおそれのある手法であった。
- 後に経緯が明らかになったところによると、ブッシュ大統領がNSAに何かテロを止める方法はないか問うたところ、NSAの長官だったマイケル・ヘイデンが、このようなことができれば助かると大統領に要請し、その結果、秘密の大統領令が発出され、いわゆるバルクコレクションと呼ばれる通信傍受が始まった。
- 通信傍受は2008年の大統領選挙の争点の一つとなった。オバマ候補（当時）は、自身はこれをやらないと明言していたものの、大統領選挙の途中から態度を転じた。ボブ・ウッドワードの本によると、ブッシュ政権の国家情報長官だったマイク・マッコネルは、オバマ候補に「やつらがしゃべる、われわれは耳を澄ます。やつらが動く、われわれは観察する。好機がめぐってくれば、われわれは実戦行動に出ます」と述べたという。ブッシュ政権の中で大量の通信傍受が行われ、これがテロ防止に非常に役立っているのだということをインテリジェンス側からオバマ候補に説明をし、オバマ候補はそれを受け入れ、政権が成立した後はそれを拡大させていくことになった。
- 911に関わった19人のテロリストたちがどのような通信をしていたのかを後から分析したところ、彼らは「明日試合が始まる」とか、「明日が開始時刻だ」といった言葉を、メール上で暗号化もせず、平文で交わっていたことが分かった。これは本人たちにしか意味が分からない情報であるため、収集して意味があるのかが非常に大きな議論になった。また、通話内容を聞くにしても、1分の通話を分析するには必ず

1分以上かかるため、現実の運用として難しいのではないかということが分かってきた。

- オバマ政権で創設されたサイバー軍の初代司令官に就任したキース・アレグザンダーは、「わら（データ）の山の中から針（テロリストたちの通信）を探すなら、わらの山全体が必要だ。全てを集めて保存すれば、目前に迫った攻撃のパターンと手がかりを戻って探すことができる。」と発言したように、サイバー軍では大量のデータを取得し、そして、そのコンテンツよりもメタデータと言われているものに注目していくことが始まった。メタデータの定義は、広く考えればソーシャルメディアのアカウントや銀行口座といったものも含むが、細かく言えば通信のヘッダと言われているところの情報である。メタデータの分析により、結果として後づけではあるが、9/11のハイジャックをしたテロリストたちが密接なつながりを持っていたことが分かったところ、これをテロを未然に防ぐために使うことができないかという考えの下、通信の利用が大きく始まっていった。
- 市民団体が公開した情報によると、NSAはメリーランド州にあるヘッドクォーターや全米各所にあるインターネットエクスチェンジ、海底ケーブルの陸揚げ局、人工衛星の傍受拠点から大量のデータを集め、その結果を分析することでテロを防ぐことを始めたのではないかとされている。別の研究者が公表した情報では、人工衛星やNSAの国内外の傍受拠点から集めたデータをユタ州にある東京ドーム4～5個分の敷地を持つ巨大なデータセンターの中に集め、そのデータを分析した上で、メリーランド州の本部に送り、そしてホワイトハウス、CIA、国防総省に共有しているという。
- 2013年にエドワード・スノーデンが、いわゆるプラットフォーマーと言われている米国の事業者が、NSAに協力していることを暴露した。内部文書によると、海底ケーブルの傍受を意味する「Upstream」とプラットフォーマーからの情報収集である「PRISM」の両方を用いるべしと書かれていた。
- 様々な形でのデータの収集は、当初はテロ対策に、やがてサイバーセキュリティに使われるようになってきている。
- 英国では、GCHQがフェイスブックその他のソーシャルメディアを徹底的に探しているということが指摘されている。リチャード・オールドリッチは、その著書において、米国とイギリスはスペシャルリレーションシップとよく言われるが、ロマンチックな関係では全然ない、非常にリアリズムに基づいたものだと言っている。例えば、キプロスにある中東を監視するための通信傍受拠点をイギリスが経費削減のために閉鎖しようとしたが、米国側が存続を求めた結果、米国側が中東を監視するための拠点として残されたということがあった。その時に、米国側は最新鋭の技術を提供し、イギリス側はその傍受拠点を提供するという相互依存関係が作られたことが分かっている。

- かつて、いわゆるファイブ・アイズによって、「Echelon」という人工衛星を使ったアナログ、無線通信の監視ネットワークが築かれていると言われた。しかし、通信はここ10~20年で、デジタル、有線通信に転換してきた結果、その手法も変化している。例えば、携帯電話も、手元は無線であるが、その後は光ファイバーの大きなネットワークの中に入っていくところ、携帯電話の傍受も有線ネットワークのデジタル通信を傍受することにより行われている。
- 海底ケーブル網の設置状況に鑑みると、ファイブ・アイズの空白地帯であるユーラシア大陸の北半球をどう監視していくかがファイブ・アイズの課題。日本は、ユーラシア大陸の北半球における監視に大きな役割を果たせるのではないかと思う。光ファイバーのネットワークというのは陸上線、海底ケーブルを含めてグローバルにつながっており、ここに悪い人たちもいる。この監視ネットワークをいかに築いていけるかということが重要になる。
- ファイブ・アイズの国では、シグナルインテリジェンスをやる組織がはっきりと設置されている。先進主要国では様々なインテリジェンス機関の中の一部の機能としてシグナルインテリジェンスを行うことになっており、なかなかその実態は分からないが、通信情報の取得、分析がインテリジェンス活動の中核にあることは間違いない。
- 米国のプラットフォーマーがデータをインテリジェンスに渡すのは、法律的な枠組みの中で通信事業者が協力しなくてはいけないという義務があるからだけでなく、データ取得、そして保存に関わるコストを政府側が十分に負担しているからである。
- ビッグデータと言われているものが世界中で出てきており、日々どんどん大きくなっているが、それをいかに取得し、分析をするか、そしてサンプル分析ではなくて全数分析でいかに取れるかが重要になってきている。
- 海底ケーブルにおいては大量の光信号が流れているが、当初はカプラーという光信号を分岐させる装置を使って、海底ケーブルの陸揚げ局の段階で分岐していたのではないかと聞いている。ただ、スノーデンの暴露があつてから、米国では通信事業者がそのままデータをインテリジェンスに渡すことには制限がかかるようになり、通信事業者が一定期間データを保有しておき、それを必要なときにインテリジェンス側が引き出すという措置も取られるようになってきている。
- この取得したデータをどうするかということも非常に難しい問題であり、例えば、テロリストやサイバー攻撃者は大量の動画データの中に様々な情報を隠すことも始めており、それを分析する様々な技術が必要になってくる。諸外国のインテリジェンス機関、シグント機関はこうした技術を民間と協力しながら獲得してきているところ。
- 大量に取得したデータを人間が目で見ると判断するということはほとんど不可能。機械によってどこまで処理ができるか、ヘッダ情報みたいなものを見るのだとしても、それを機械が振り分けていくときにどこまで見ていくか、「ペイロード」をどこまで見るか、見るとして機械が見ればいいのか、人間が見たら駄目なのか、事業者が見る

のか、政府が見るのか、様々な論点があり、今回の有識者会議ではこの辺の整理というのが必要になるのではないか。

- 海底ケーブルの傍受も島国である日本にとってはとても重要。海底ケーブルで入ってくるデータ、出ていくデータのほか、例えば米国から来たケーブルが一旦日本で陸揚げをされ、第三国につながるようなトランジットの場合もあるが、このような場合に米国と第三国との間の通信を見ていいのかということも一つの論点としてはあり得る。私自身は国内で完結するデータについては見る必要は今のところないと思うが、外国から来るサイバー攻撃に対処するための措置は何か考えられるのではないかと思う。
- メタデータのように処理がしやすいデータ、構造化されたデータだけでなく、非構造化されたデータ、コンピューターで処理しにくいようなデータ、あるいは例えばPDFのような文書化されたデータを分析していくという能力を日本がいかに持てるかということを考えていきたい。
- 論点としては、どんなデータをどこまで取得するか、平時と有事が切れ目なく続いている中で、いつ我々はデータが取れるか、平時から取れるのかどうか、そして通信事業者の協力なくしてはこうしたデータの収集はできないところ、通信事業者をいかに法的に守っていくかやその費用をいかに補填していくか、取得したデータを保存する設備とそれを分析する能力を、人材育成の点も含めて、いかに確保していくかというような点が挙げられる。

(4) 討議

事務局による説明や有識者からのプレゼンテーションを踏まえ、以下のような発言があった。

- 今回の取組は、非常に重要であり、かつ、一瞬だけできても駄目であって、継続的にできるかが重要である。この観点から、2点の懸念がある。
- 一つ目は、通信事業者が政府に協力する場合、海底ケーブルで上げてきたものをタップすることになると思うが、通信事業者がこうしたことを行っていることが世に知られたとき、通信事業者において訴訟対応で稼働が切迫し、負担が大きくなると継続が難しくなる。裁判の中で守られているかということに加え、それ以前のところでも考慮していただきたい。
- 二つ目は、事業者としては、海底ケーブルが陸揚げされてきたところから情報を取り出し、能動的サイバー防御を実施する行政機関に通信を引き渡すということになると思うが、可能な限り既存のネットワークに負担にならない方法でやらざるを得ない。例えば、ルーティングの設定変更となると、稼働しているシステムは、設計から何からやり直しになってしまうため、多くはタップで取り出すことになると思われる。一方で、タップで取り出す場合には、通信事業者は通信の中身をあまりいじれず、そのまま渡すことになってしまう。通信事業者が通信の中身にかかわらず行政に通信情報を提供したとき、実際に何を利用しているのかは、能動的サイバー

防御を実施している行政機関が判断しているという矛盾が生まれ、通信事業者だけが責められてしまうことを懸念。

- このように、訴訟等のリスクや、ネットワークとして負担がないようにオペレーションできるかということも含めて検討して、答えを導き出せればと思う。
- 米国では、CALEA (The Communications Assistance for Law Enforcement Act) というクリントン政権の時の法律があり、全ての米国通信事業者は、通信傍受に対応しなければならないとされていることから、そもそも通信事業者側にやる・やらないというオプションがない。また、傍受していることを対外的に言うてはいけない、やっていないと言っているということにもなっているはずである。それでも、AT&Tのように暴露されて集団訴訟になったということはあるので、訴訟から守れるようにすることは必要であり、また、国に協力する通信事業者を使いたくないといったレピュテーションリスクが生じ得ることを踏まえると、どう説明できるようにしていくか、株価を含めたレピュテーションをいかに守るかといったことも重要である。このとき、通信事業者側が選択的に通信を取り扱っていないということが重要になるように思われる。事業者に負担をかけないかたちでいかに取得できるか、かつてはカプラーで分けていただけだったので負担になっていなかっただろうが、最近の手法はものすごく負担であると思われるので、日本でそのような体制をいかに構築していくかが課題。
- 資料2スライド9枚目の各国法令の整理について、情報を取得する要件と取得後の情報を分析できる範囲が書かれているが、取得する情報の範囲について、通信の構成要素や内容でカテゴリが分かれると思うが、その辺りの内容が分かるようなら教えてほしい。

事務局より回答

- 主な対象通信の行は、各国の法律の条文において書かれているこのような通信を対象に傍受や取得をしていくという趣旨が書かれているところを抜粋したもの。メタデータまでなのかコンテンツまでなのか、どのような通信情報の種類を取得の対象にするかなどについて明確な規定がなされている例は、私どもの調査している限りでは、ない。いずれにしても、一定量の情報を取得して分析しているものと理解。
- 能動的サイバー防御の世界は、データ通信に関連する情報を、メタデータを含めて取得・分析することに意味がある。まさにサイバー防御の実効性を高めるために、メタデータにも価値があるからこそ、逆にその濫用がもたらす危険も生まれるのであって、通信内容だけでなくメタデータもしっかり保護すべき必要があるという両面を認めて、適切な規律を考えなければならない。
- これまでの通信の秘密の制約に関する通信傍受の議論は、刑事司法を念頭に、その得られた結果を犯罪捜査で使用し、裁判等で証拠として用いることに対する、個別の司法的な統制が念頭に置かれてきた。今後の検討では、通信傍受法等のこれまでの我が国の法理は前提にしつつも、問題状況に即して、現代的な個人データやプライバシーの保護、第三者機関等の議論を、世界の仕組みも参考にしながら、日本流に適切に組み合わせて、必要な情報をどこまで取得しどこまで解析・利用していくのかという実体的規律を整理し、また、その適正な規律を遵守するための組織・手

続的な仕組みづくりも必要。

- 政府と民間の適正な連携が重要。連携の名の下にどこまでも許容されるのではなく、適正な規律の下で、事業者は事業者で、政府は政府で、節度と連携を持って協力をすべきであり、だからこそ、民間事業者に対する不当な非難がないようにすることが重要と思う。こうしたことも含め、第三者機関、ガバナンスの仕組みを考えていくべき。
- 土屋先生の話では、平時・有事の切れ目がない中で、平時からデータ取得できるのかという問いかけが寄せられていた。資料を見て、また、今日話を聞いて、この領域において平時というのはあるのかというのが率直な感想である。常に有事、常に緊急事態と考えておいた方がよいのではないか。そのような領域であるという理解が必要になるのではないか。
- 鶏と卵であるが、通信情報を利用したサイバー攻撃対策を行った経験がない中で、何をどこまで見ればどのような対策が可能であるのか、それを明確に判断するのは容易ではないと思う。研究ならばインクリメンタルに行くこともあるところ、このような枠組みの中ではそれも難しいであろう。諸外国の事例を勉強し、どうしてこの範囲でデータを取っているのか、分析しているのかということをしっかり理解した上で判断していくことが必要。場合によっては、継続的に検討していくことも必要になるだろう。
- インテリジェンスの世界は、犯罪捜査の世界とは違うところがある。米国でも、FBIが主に国内での犯罪に対処するために通信を傍受しているが、インテリジェンスとは少々異なる法律に基づくものだ。インテリジェンスの目的は問題を未然に防ぐことに主眼があり、既に行われていることを証明するという点では必ずしもない。このため、犯罪捜査とは情報の取り方が異なる。
- 日本にこの分野でデータ監視の在り方を判断できるレベルの人がいないというのはそのとおりと思う。ただ、日本企業が諸外国のサイバーセキュリティ企業を買収し、従業員を派遣して経験を積ませるなどのことが行われているという事実もある。そういった人々を日本に呼び戻す、海外の企業や政府と協力する等により、ゼロから始めなくとも対応できるのではないかとも思われる。

(5) その他

事務局より、以下のとおり補足説明があった。

- 議論のスコープについて、土屋先生のプレゼンテーションは、幅広く、テロ対策、安全保障全般のためのということで、サイバーセキュリティを含む安全保障全般の議論を展開されたものと理解。一方、今回の検討は、国家安全保障戦略にあるとおり、安全保障全般ではなく、サイバー攻撃に関するものについて取得・分析することに限られてくる。このため、米国の事例よりは、範囲が狭くなるかと考えている。

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1回）
議事要旨

1. 日時

令和6年6月20日（木）8時30分から9時30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
落合 陽一	筑波大学デジタルネイチャー開発研究センター長/准教授
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
穴戸 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
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

（ゲストスピーカー）

林 紘一郎	情報セキュリティ大学院大学名誉教授
田川 義博	元情報セキュリティ大学院大学客員研究員
小西 葉子	関西学院大学総合政策学部専任講師

4. 議事概要

（1）ゲストスピーカーからのプレゼンテーション

英国の制度及び関連判決について、林氏より冒頭以下の発言があった後、田川氏より【資料2】を用いて説明があった。

(林氏冒頭発言)

- このテーマを共同研究に選んだ趣旨は、英国はインテリジェンスの母国とも言え、インテリジェンス情報の扱いをここまで幅広く規律した法律はほかにない上、議院内閣制という共通項があることで、我が国にも参考になり、EU 離脱後も欧州評議会に残るので、EU の動向も知ることができるからである。
- また、インテリジェンスの観点から補足すると、「通信の秘密」を制約する際に人権上のセーフガードが及ぶのは、原則として当該国民であるところ、外国人発着の通信やトランジット通信には、同じレベルの保障が及ぶとは限らないのが通例。今後の議論を進める上で、ともすれば忘れられがちな点であり、冒頭で注意喚起させていただく。

また、ドイツの制度及び関連判決について、小西氏より【資料3】を用いて説明があった。

(2) 討議

ゲストスピーカーからのプレゼンテーション、第1回会合における事務局説明及び有識者からのプレゼンテーションを踏まえ、以下のような発言があった(以下ゲストスピーカー小西氏を「ドイツ発表者」と、林氏及び田川氏を「英国発表者」という)。

- ドイツは緻密な制度であること、英国ではバルク令状等の工夫された制度があることが理解できた。サイバー防御に必要なものは、メールの中身を逐一見るようなものではないだろう。ドイツに倣っていうならば、コミュニケーションの具体的な内容に照準を合わせるわけではなさそうである。その意味でも、この制度は、通信の内容を扱おうとする通信傍受法とは異なるもの。
- N I S C (内閣サイバーセキュリティセンター) がサイバー攻撃を受けた事例、中国人も関係して J A X A (宇宙航空研究開発機構) がゼロデイ攻撃を受けた事例等を踏まえれば、日本においてもサイバー攻撃の被害が深刻化している実態がある。
- 欧州、米国等の各国が能動的サイバー防御の法制度を既に整えていて、日本がサイバー防御の能力を高めることが国際的に要請されていると考えられることをあわせて考えると、安全保障上の必要性の議論をこれから深め、国民の理解を得ていくことが必要。
- 通信事業者がサイバー防御に必要な情報を政府に提供するに当たって、社会の安全のために貢献していると肯定的に評価されるようにするためにも、国民の理解を高めていくことが求められる。国益、公益のために協力した事業者が訴訟リスクやレピュテーションリスクにさらされることはあってはならない。
- 重大なサイバー攻撃を未然に防ぐためには、平時から不審な動きを監視する必要がある。

あると理解。令状主義に基づく制度のみでは対応できないだろう。通信の秘密の保障と公共の福祉の両方が整合し、かつ、実効性のある防御を実現できるという緻密な法制度を、分かりやすい議論を積み上げて、作り上げていくことが必要。

- 外国人・外国人間の通信、あるいはトランジット通信については、国民あるいはそれに準じて適用される日本社会の構成員の享有する基本的人権の保護範囲には含まれず、その制約が本来的に憲法上許されるのではないかという点に基本的に同意する。
- 他方、目の前にある通信が、外国人・外国人間の通信か、日本国民間のものか、又は日本国民・外国人間のものかを、制約の前に見分けることができるか、そもそもその見分ける作業自体が一定の人権制限に当たり得るものとして、一定の防護措置、セーフガードが必要でないかどうかは、一の論点と思料。所見如何。

英国発表者より回答

- トランジットかどうか等を事前に判断するのは、難しいのではと思う。切り分け自体が第一の問題となるかもしれない。しかし、これを逆にいうと、バルク取得のような人権侵害の度合いの高いものをなぜ認めなければいけないか、ということの理由付けにもなっているという裏腹の関係でもある。
- 議院内閣制の国において、能動的サイバー防御に相当する活動を政府が行うに際して、行政内部、立法府、裁判所、これら三権による監督をどう組み合わせるかが大きな課題であり、現代的な権力分立の問題を考える上で重要な論点である。どのような組み合わせが適切か、逆に問題があるか、御教示願いたい。

英国発表者より回答

- 諸外国の制度として米国も調べているが、大統領令によって様々次々に（制度が）出てくる米国の（大統領制を採る）議会制度と比較し、議院内閣制では、議会に付され、裁判所にも服することになる。実際には英国でも司法コミッショナーという司法と行政の中間的なやり方をしているが、（制度整備は）米国的な発想にともすれば傾きがちなので、注意してくださいという趣旨であった。どのように三権の分担ができるかという議論については、もう少し注意深くやっつけていかなければいけない。
- バルク令状の発出権者は国務大臣であり、司法ではない。また、独立機関である司法コミッショナーも行政内部である。議会は広範な監督権限を有し、司法については、国内裁判所に加え、ブレグジット後も欧州裁判所の管轄になっている。よって、三権分立の建前になっている。
- バルク通信傍受は、GCHQのみが利用している安全保障全体のための通信傍受だが、サイバー防御の目的でも実施していると報告されている。

ドイツ発表者より回答

- 議会の役割は俯瞰的なもの。ドイツでは議会統制委員会がこの役目を担っているところ、選挙の結果に応じてその構成員が変わるので、個別の行政活動を統制するとい

う力を持たせることは組織上も難しいし、そのような権限を持たせる必要性も少ない。

- 行政内部の自己チェックは、当然行政で行うべき。どのようなサイバー攻撃を防止するのかといった全体的な構成の検討も、もちろん行政がやるべきこと。他方、事前の審査プロセスは、非常に強固な独立性を持った行政機関、いわゆる第三者機関がなければ、行政がその役割を果たすことは難しいと考える。
- 司法の役割として、ドイツの場合は、連邦憲法裁判所により、個別の法律が細かく違憲審査されている。しかし、日本はそうっていない。また、ドイツでは、独立機関が監督対象機関について訴えを起こす機関訴訟の在り方が話題になっている。
- ゲストスピーカーの説明資料に「介入」や「干渉」という用語が使われている。これらは、無害化のように何かを変えるといった行為も含まれるものか、単に通信データをパッシブに分析するような話なのかを教えてください。

ドイツ発表者より回答

- ドイツにおける「介入」は、基本的人権に対する介入の意味であって、通信に対して作為を加えるものではない。あくまでも、通信の情報を受け取るという趣旨である。

英国発表者より回答

- 英国における「干渉」は、interference であり通信等への干渉、ひいては人権に対する干渉ということ。
- 補足すると、Equipment Interference は、ハッキングのことである。

- ドイツに関する説明を聞き、事後審査が重要と感じた。事後審査が、どの機関で、誰がどのようにこれを行うかということが重要。また、事後に妥当性を調べようと思ったときには記録が大事になるが、記録については、どのような規定が置かれているのか。それぞれ教えてください。

ドイツ発表者より回答

- 基本法 10 条審査会も議会統制委員会もそうだが、基本的には、ドイツの情報収集機関が保有するすべての記録にアクセスできる。第三者機関であってもアクセスされると困る場合は、収集した機関側が、理由を示す必要がある。こうしたことから、第三者機関には、非常に厳しい守秘義務が課されている。
- ドイツの説明資料で、動的 IP より固定 IP の方が侵害性の低いものとされているように見受けられるが、固定の方が特定しやすいなど、逆ではないかと感じた。例えば、大学のアドレスは固定であり、公開されているので全世界に知られていて、通信対象が簡単に分かってしまう。その方が問題になってしまうのではないか。

ドイツ発表者より回答

- 御指摘はおっしゃるとおり。ただし、この部分は「通信の秘密」の侵害という視点で整理したもの。ドイツにおいては、固定 I P は「情報自己決定権」の問題として厳しく審査される。他方、「通信の秘密」の対象は通信の状況及びコミュニケーションの内容と考えられているので、固定 I P は、あくまでも「通信の秘密」という概念との関係において問題とならないということ。
- 明確かつ詳細なルールが重要ということでそのとおりと思うが、当該ルールは、ある程度事前にフィックスして運用していくものか、それともルール自体も経験を積み重ねていく中で、検証しつつ変えていく可能性があるのか、教えてほしい。

英国発表者より回答

- 法律的には、Fit for purpose が重要と申し上げたが、A I も含めて技術進歩が著しいので、どうやって法目的に合せるようにするかが重要というのが大前提である。
- 実務的には、調査権限法の下位の法令として、その Code of Practice があるので、この中で定める。明確かつ詳細なルールの中身はさらに二つあり、一つは、調査権限の内容及びその制約をどうしていくかということ。もう一つには、人権保障のための保護措置、監督、救済。こうしたものを明確かつ詳細に定めることが必要。
- 通信情報の利用のあり方についても、作用法という制度に落とし込むための議論をしなければならないと考えている。作用法にするとすることは、すなわち、誰が、何をするのかを明確にしておくということ。そのような視点から本日の議論を振り返ると、一つ目の層は、情報の収集という活動の領域であり、収集、分析、利用のそれぞれの段階について、誰が、いつ、どのような情報を収集し、どのように分析をして利用をするかという仕組み作りの議論になると思う。この点、本日の説明のなかにあった、Fit for purpose という規範等の英国法制の議論は大変勉強になった。また、どこを流れる情報なのかによってコントロールの濃淡が変わり得るということ、ドメスティックとトランジットの区別等も参考になるのではないか。もう一つの層は、情報収集活動のあり方を、第三者機関を上にかぶせる形で監視監督するという領域の議論である。この二つ目の点に関しては、本日のドイツ法制の、第三者機関の分析が参考になるものと、興味深く拝聴した。
- 本日のドイツの状況に関する説明において、基本法 10 条審査会を国家公安委員会と比較しているが、なぜこのような比較をしたのか、とくに、国家公安委員会を比較の対象としたことについて、お教え願いたい。また、ドイツにある独立統制評議会について、把握されている範囲のことでよいので、可能であればその組織や権限の内容につき、もう少し詳細に教えてほしい。

ドイツ発表者より回答

- 国家公安委員会と比較した理由は、自身の2019年論文において、国家の情報収集の統制手段に着目して第三者機関の研究をしていたため。国家の情報収集活動の個別的統制機能に着目して、同審査会と国家公安委員会を比較してみたもの。
- 2022年に設立された独立統制評議会は、新しいスタイルのもの。司法機関類似の統制機関といえば、従前、行政機関が措置を行った後、事後的に審査をすること、例えば、行政不服審査のようなものが一般的と考えられてきたが、独立統制評議会は、司法機関類似の統制機関が事前に審査を行い、行政的統制機関が事後的統制をするという特徴がある。
- 外国の例については、国内で実行を計画しているテロ対策の意味合いもあると思う。能動的サイバー防御については、場面によって法執行の主体が変わるのかと考えている。
- 海外からの通信と国内通信を分けることについては、どのように識別していくのか、今後の技術の発展状況が問題になってくる。通信技術者の実務も分からなければならない。
- どのような通信情報が必要かという点について、通信の本質的内容以外の全て、すなわちインベントリデータや、トラフィックデータなどが必要と考える。
- 取得・処理した通信情報の活用・共有の部分まで考えると、NSAが取得したデータは、NSA自体がサイバーセキュリティ機関でもあるが、どこかでCISA（米サイバーセキュリティ・インフラセキュリティ庁）等に共有しているだろう。また、GCHQがバルク令状の申請権限を有するという点から、隷下にあるNCSC（英国家サイバーセキュリティセンター）も通信情報にアクセス・活用できることが想像できる。日本では、取得した通信情報の活用や関係機関との共有はこういったプロセスになるのか。
- 独・英の第三者機関による監視・監督は、通信情報のアクセス・取得が中心のように見受けられたが、実際には情報の取得・処理・保管・活用・共有・廃棄といったライフサイクル全体に適用される必要がある。

ドイツ発表者より回答

- 連邦情報局に関しては、国内外の他の機関との共有や、共有前の処理等についても、法律上の規定がある。
- また内容を取得するときのトラフィックデータの取扱いどうするかなどについても、法律に定めがある。ドイツの第三者機関がどこまで統制しているかについては、複数の統制機関があるので、後ほどフォローできればと思う。

英国発表者より回答

- 調査権限コミッショナーは、年次報告を公表しており、MI5、GCHQなどの個別

のインテリジェンス機関に関する調査結果を掲載している。そこでは、エラーレポート、すなわちどういうエラーが何件あったか、重大なエラーについては、典型的にどういうエラーがあったかなども掲載。したがって、全てのプロセスについて監督していると考えられる。

- 他方、通信情報の扱い、特に情報の処理・活用はきわめて機微となるので、どのようなどころまでこうした監督・監視が行われているかが気になった。
- 対象とすべき通信情報は、本検討においては、外国が絡む通信を対象とするということが適切ではないかと思った。というのは、国内は日本の警察の権力が及び、捜査等が可能であるが、外国は国家権力の外なので、対策のために情報が必要ということになると考えている次第である。
- 予防及び権利保護のバランスという観点から考えると、「最初は広く、懸念が見つかったら深く」という段階が必要のようにも思われる。
- 重大な懸念に対して行うということは分かったが、重大な懸念かどうかを判断するのは、どこの機関になるのか。小西先生説明資料6ページには、『『特に深刻な』侵害の強度』というのがあるが、特に深刻なというのを判断するのはどこの機関なのか。

ドイツ発表者より回答

- 『『特に深刻な』侵害の強度』の部分は、「通信の秘密」に対してこの情報収集が「特に深刻な」侵害の強度を有するという趣旨。これとバランスを取る均衡の対象として、外国からの情報収集によって安全保障を確保するという重要な目的がある。その上で、第三者機関のコミットが重要なところ。余計な情報を取らないというところについて、たとえば独立統制評議会の一部門、すなわち司法機関に類似する統制機関による事前チェックが関係してくると思われる。
- 令状は、英国では国務大臣が発行するという点だったので、この点は分かったが、その国務大臣は、ある程度の専門的な知識を有する機関だということによい。

英国発表者より回答

- 国務大臣が令状を発出するときどのような事項を考慮するかは、調査権限法に詳細な規定がある。大臣が専門家かどうかは分からないが、実際には、その規定を見ながら判断することになるかと思う。
- なお、調査権限法の通信傍受は、国家安全保障等、最も幅広い情報を収集・分析という目的であり、サイバー防御は、その一部でしかない。実際にどう絞っているかというと、収集段階ではバルクで集めることから、セレクトアやディスクリミナントと呼ばれる選択語によって絞っていくのだろうと考えられる。
- 能動的サイバー防御の具体的な行動を行う際、誰がどのような実施計画を定めるの

か、また、そのプロセスはどうなるのか。さらに、立案された計画を実施する局面においても、情報を取得し、蓄積し、処理し、分析する。もちろんその結果を見て、新たな情報が必要かもしれないということで、さらに取得、蓄積、処理となるのかもしれない。いずれにせよ、取得、蓄積、処理、分析、分析結果の利用、外部への提供、廃棄というプロセスが考えられるし、また、統計のような形で分析した情報を広く公表することや、監視機関、あるいは国会、世論などによる統制に必要な範囲で情報を作成・加工して提供するといった作業も生じるはず。こうした、能動的サイバー防御に係る情報処理のプロセス全体で、どこにどういう規律・作業が必要となり得るか、まずは事務局で整理していただきたい。

- 同様の問題は、通信事業者内、また通信事業者間にもあるはず。これに関連する既存の取組がどういったものであり、何がどこまで可能であり、何が課題として認識されているか、新たに対応する必要があるとすれば何かなど、専門家にも聞きながら、整理していくとよいのではないか。

(3) 河野国務大臣挨拶

- 今日もお忙しい中ありがとうございました。2日間にわたり、早朝から大変活発に御議論いただきまして、感謝申し上げます。
- この通信情報の利用のテーマにつきまして、皆様の精力的な御議論を踏まえて、論点の整理に向けて、更に御検討いただきたいと思っております。今後とも御協力のほどどうぞよろしくお願い申し上げます。
- 今日御参加いただきました小西先生、林先生、田川先生、どうもありがとうございました。

以上