資料３－１

## ○　通信情報の利用

本章では、国家安全保障戦略において能動的サイバー防御の実現のための検討事項とされていた措置のうち、国内の通信事業者が役務提供する通信に係る情報（以下この提言において「通信情報」という。）の利用*について述べる。

＊同戦略では通信情報の「活用」と表現されているが、本提言では、個人情報保護法等の規定での表現にも倣い、通信情報の「利用」の語を採用する。

### ①攻撃実態の把握のための通信情報利用の制度の必要性

世界全体で政府機関や重要インフラ等を標的にしたサイバー攻撃による脅威が急速に高まりつつあり、日本でも実際に、政府機関がサイバー攻撃を受けるなどで、被害が深刻化している。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。しかも、これらボットの多くは、国外に所在すると考えられている。

このような状況では、通常の情報収集の手段では、どのような攻撃がどこから行われるかを事前に知ることが困難であり、攻撃を受ける側での防御に限界があるとともに、アクセス・無害化等の能動的な防御も難しい。そのため、被害を未然に防止するためには、通信情報を分析することにより、ボットネットワーク等の攻撃元のインフラの実態を把握し、防御を可能とすることが必須であり、特に、アクセス・無害化を行うに当たっては、今まで以上に、サイバー攻撃に関する詳細で十分な量の観測・分析の積み重ねが必要である。

通信情報の利用は、重大なサイバー攻撃が具体的に発生してからその攻撃元の実態を把握していくためだけに行われるのではなく、重大なサイバー攻撃による被害を未然に防ぐため、平時から、個別の対象を限定しない形で行われる必要があると考えられる。このため、電話番号やメールアドレスなどにより特定されて傍受令状に記載された通信手段に対して傍受を行う「犯罪捜査のための通信傍受に関する法律」（通信傍受法）のような個別的かつ司法的なコントロール*では、被害の防止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ものであり、これまで我が国では存在しない新たな制度による通信情報の利用が必要とされると考えられる。

＊憲法第３５条第２項「権限を有する司法官憲が発する各別の令状」の規定に基づくいわゆる令状主義によるコントロールを指す。なお、外国法制での「令状」あるいは「許可状」は、司法府ではなく行政府の発行するものを指す場合がある。

これは、我が国にとっては新たな挑戦となる事項であるが、先進主要国では既に、国家安全保障等の観点から通信情報を利用していると考えられ、かつ、通信情報の利用が安全保障目的のインテリジェンス活動の中核となっており、現在は、サイバー攻撃対策としても、用いられていると考えられる。この点、少なくとも米国及び英国については、サイバー攻撃対策としても成果を挙げているとの政府の公表情報があることは、特筆される。また、それ以外にも、少なくともドイツ、フランス及び豪州において、サイバー攻撃対策を含むと考えられる国家安全保障等の目的で通信情報の利用を可能とする制度が存在することが確認できる。

これらの国におけるサイバー攻撃対策の通信情報利用の手法としては、個別具体的な対象を事前に特定せずに一定量の通信情報を収集するが、その全てを分析するのではなく、通信の宛先や送受信者に関する情報など、コミュニケーションの本質的な内容ではないデータに注目す

る方法（②で「☆の方法」として参照する）が一般的にとられている</u>と考えられ、また、これを可能とするため、一定の条件の下、安全保障上の必要性等がある場合に、政府による通信情報の利用を統制しながら、利用を許容する法律が整備されている状況にある。そして、政府による通信情報の利用には、通信事業者等の協力が必要とされ、これらの国では、通信事業者等に対する法律上の義務付けが行われるとともに、政府からのコスト負担によっても、協力の実施が確保されていると考えられる。加えて、政府においても、通信情報の取得と分析について、一定の技術と能力が必要とされると考えられる。

<u>このような先進主要国の状況を踏まえると、我が国でも、</u>重大なサイバー攻撃への対策（以下「重大サイバー攻撃対策」という。）のため、<u>一定の条件の下での通信情報の利用を検討することが必要</u>である。また検討に当たっては、安全保障の観点から、海外に依存することなく日本独自の情報収集が必要と考えられることに留意すべきである。他方で国際的な観点からも、先進主要国と連携しながら通信情報を利用する*ことで日本は大きな役割を果たせると考えられるものであり、日本が重大サイバー攻撃対策の能力を高めることは、国際的にも要請されていると言えると考えられる。

＊これは、日本政府が新たな制度により利用する通信情報が無制限に他国と共有されるべきことを意味するものでは全くない。他国との情報の共有は、必要かつ合理的な程度となることが確保されるよう、制度上適切に制限されるべきである。

**②通信情報の利用の範囲及び方式**

通信情報の利用による効果と通信の秘密への影響は、利用の範囲及び方式の内容によって、変わり得る。そのため、通信の秘密を保障する憲法との関係での許容性を具体的に検討するには、まず先に、重大サイバー攻撃対策という目的を達成する観点から、通信情報の利用のあるべき範囲や方式について、検討する必要がある。その際、通信情報の分析は、問題を未然に防ぐ予防のための分析であるため、既遂行為について真実を解明することを目的とする犯罪捜査とは方法が異なり、「最初は広く、懸念が見つかったら深く」という考え方が妥当である。また、制度全体として重大サイバー攻撃対策の観点で弱点がないものとなるよう検討していくべきである。

具体的にはまず外国の通信か、国内の通信か、という観点では、<u>外国が関係する通信について、国外に日本の国家権力が及ばないこともあり、通信情報を分析する必要が特にある</u>と考えられる。<u>【Ｐ：特に、日本を経由して伝送される外国から外国への通信である「トランジット」の通信については、】先進主要国と同等の方法（①の☆の方法）の分析をできるようにしておく必要</u>がある。

分析の対象とする必要がある情報の範囲について、通信情報は、ⅰ）電気通信設備等を識別する情報、ⅱ）コンピュータ等に一定の動作をするよう指令を与える情報、ⅲ）その他機械的な情報、<u>ⅳ）個人のコミュニケーションの本質的内容に関わる情報、に主に分類できるが、このうちⅳ）は重大サイバー攻撃対策のためには特に分析する必要があるとまでは言えない</u>。すなわち、<u>メールの中身を逐一全て見るようなことは、重大サイバー攻撃対策としては適当とは言えない</u>行為である。加えて、<u>収集したデータ全てについて人間の目で判断することは不可能であり、またプライバシー保護等の観点から適切でもない。重大サイバー攻撃対策に必要な情報を取り出すため、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</u>である。

③通信の秘密との関係

通信情報の利用の範囲と方式に関する以上の結論を踏まえつつ、憲法第２１条第２項後段の通信の秘密との関係を以下検討する。

コミュニケーションの本質的内容に関わる情報は、特に分析する必要がないが、一方で、分析対象となるそれ以外の通信情報（コミュニケーションの本質的な内容ではない通信情報）も、憲法上の通信の秘密として適切に保護されなければならないものである。しかしながら、通信の秘密であっても、法律により公共の福祉のために必要かつ合理的な制限を受けることが認められているところ、具体的な制度設計の各場面において、通信の秘密との関係を考慮しつつ丁寧な検討を行うべきである。抽象的な議論のみで「許容される」あるいは「許容されない」との結論を得ることは適切ではない。

ここで参考となるのは、先進主要国での法制上の整理である。すなわち例えば英国及びドイツでは、通信情報の利用と通信の秘密又は人権との関係について、関連の判決等により、整理が図られている。したがって、先進主要国を参考にしながら、現代的なプライバシーの保護や独立機関等の議論を組み合わせるとともに、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である。その際は、英独での法的整理に鑑みると、実体的な規律とそれを遵守するための組織・手続き的な仕組み作りが必要であり、また、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。

その上で、英独に限らず先進主要国の制度を俯瞰し、通信情報の情報処理のプロセス全体で、どこにどのような統制や規律が必要となり得るか、という視点で整理した場合、情報処理のプロセスとしては、先進主要国の法律では、おおむね共通する実施過程として、準備・承認、通信事業者への措置、処理・分析、提供・共有等、保存・廃棄を認めることができると考えられ、また、独立機関による監督があることも共通している。このため、こうした仕組みを参考としながら、重大サイバー攻撃対策という我が国における今般の政策目標を踏まえつつ、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を導入していくことを考える必要がある。中でも、独立機関は重要であり、各国の司法制度等との関係や日本の他法での類例を考慮しながら、具体的な組織の在り方が検討されるべきである。また、政府における司令塔となる部門と実施を担当する部門など、独立機関以外の関係組織の役割についても明確化を図り、必要な制度的手当てを行うべきである。

なお、以上の議論は通信当事者の同意がない場合の通信情報の利用を前提としたものである。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と考えられる。その場合の同意の在り方は更に検討がされる必要があるが、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ことが方法として考えられる。またその際、規格化の一部として、通信当事者の同意のある利用であっても、独立機関の監督等のガバナンスの仕組みが用意されることが検討されるべきである。

④電気通信事業者の協力

先進主要国と同等の方法による通信情報の利用を実現していくに当たっては、その運営する

設備から通信情報を送出し政府に提供することとなる電気通信事業者の協力が必須である。

電気通信事業者の協力は通信情報の利用という通信の秘密に対する制限を伴う措置への協力となるが、これは政府の責任の下で行う公益のためのものであり、**協力を行う電気通信事業者は、社会の安全に貢献しているとして、肯定的に評価されるべきである。**社会的な非難に曝されるようなことがあってはならない。

また、通信情報の利用による重大サイバー攻撃対策という社会的に重要な施策が持続可能なものとなるよう、**電気通信事業者が直面し得る訴訟等のリスク及び通信ネットワーク運営に対する負担について、**先進主要国の例も参考にしながら、**回避策を十分に検討**していくべきである。加えて、通信ユーザの利便性低下やコスト負担が生じるようなことも避けられるべきである。

電気通信事業者の設備から通信当事者の同意なく通信情報が政府に送出されるという、通信の秘密の制約となり得る協力の是非は､行政や民間の解釈に委ねるのではなく､**法整備により、政府の責任で判断すべき**ものとすることが必要である。これをより広い視野でみれば、政府と民間の適正な連携が重要ということができるものであり、その点でも、**独立機関などのガバナンスの仕組み**を十分に考えていくべきである。

**⑤国民の理解を得るための方策とその他の検討課題等**

以上において通信情報の利用の必要性と許容性について論じたが、通信情報の利用の実現に当たっては、こうした議論のほかにも、国民の理解を得ていく観点が重要であり、そのため、**制度の在り方や制度の運用に関する透明性を確保していく視点が重要である**。「手の内」を知られないようにしなければならない必要もあり、**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**と考えられるが、例えば**定期的な報告書の公表**などの方法で、大枠の**適切な情報公開は行われるべき**である。その上で、**情報の公開が難しい部分を独立機関の監督で補う**必要があると考えられ、その意味でも、**独立機関の構成や業務の在り方が重要**である。

加えて、通信情報の利用の必要性について、固定電話からサイバースペースへの**通信の形態の変化や各国の制度の導入の経緯を説明するとともに、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ことも説明していくことで、理解を得ていくことも重要**ではないかと考えられる。また、重大サイバー攻撃対策としての通信情報の利用では、コミュニケーションの本質的内容に関わる情報までは分析しないと考えられることもあり、得られた情報は積極的に活用していくことが適切と考えられるところ、**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**とすることも重要である。

最後に、以上のほか、今後のあり得る検討課題について述べる。まず、分析の実務面については、構造化されていないデータの分析を含め、データを分析する技術・能力と設備が必要と考えられるところ、民間企業と協力することも考えられる。また、諸外国の事例を引き続き踏まえていくことが必要であり、場合によっては、継続的に検討していくことも必要ではないかと考えられる。