攻撃者への「アクセス・無害化措置」明記
欠如したままの欧米水準のシギント機関
「サイバー対処能力強化法」の全貌と課題

米軍と共同訓練を行う自衛隊サイバー防衛隊。今後、攻撃者のサーバ等へのアクセス・無害化措置が強化される（防衛省）

去る５月16日、日本のサイバー安全保障分野での対応能力向上を目的とした「サイバー対処能力強化法及び同整備法」が国会で可決成立した。同法の成立自体は大きな前進であるものの、欧米先進国並みのサイバーセキュリティ対応になるまでには課題が多く残されている。その課題を探り、今後の改正に当たって何が必要かを考える。

〈元内閣衛星情報センター次長〉**茂田 忠良**

政府は本年（二〇二五年）二月、「サイバー対処能力強化法案及び同整備法案」を国会に提出し、五月一六日に国会で可決成立した。本法律は我が国のサイバー安全保障分野での対応能力向上を目的としたもので、その内容は①官民連携、②事業者の保有する通信情報の利用、③攻撃者のサーバ等へのアクセス・無害化措置、④内閣サイバー官の新設など組織・体制の整備の四点から構成されている。

この背景には、二〇二二年一二月に政府が閣議決定した「国家安全保障戦略」がある。同戦略は、サイバー空間に関して「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」こととし、そのため「能動的サイバー防御」を導入し、「重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に必要な権限が付与されるようにする」と記載している。本法律は、本戦略実現の一環であり、一部報道では、「これで日本のサイバーセキュリティ対応が欧米水準になる」とする記事もある。そこで、本法律によって我が国のサイバー対応能力が欧米水準に達すると言えるのか。法律の骨子を紹介すると共に、本法律に対する評価と今後の課題を述べてみたい。

なお、本稿は、衆議院内閣委員会での審議内容も分析資料としている。

1　本法律案の骨子

法律は、「重要電子計算機に対する不正な行為による被害の防止に関する法律」（新法）と「新法の施行に伴う関係法律の整備等に関する法律」（整備法）の二つ(1)からなり、その骨子は次の通りである。

（1）官民連携（新法）

基幹インフラ事業者(2)がサイバー攻撃を受けた場合等の政府への情報共有や、政府からの民間事業者等への情報共有、対処支援等の官民連携の取組を強化するとして、次の主な施策を定めている。

○基幹インフラ事業者は、特定の重要電子計算機を導入した時は、製品名等を所管大臣に届け出る（新法第２章）。

○基幹インフラ事業者は、不正アクセス行為などのインシデント情報等を、所管大臣と内閣総理大臣に報告する（新法第２章）。

○内閣総理大臣は、情報共有と対策のための協議会を設置し、基幹インフラ事業者や電子計算機等のベンダー等を構成員に加える（新法第９章）。

○内閣総理大臣や所管大臣は、電子計算機等の脆弱性を認知した時は、電子計算機等のベンダー等に対して情報を提供するなど対応を強化する（新法第８章）。

（2）事業者の保有する通信情報の利用（新法）

我が国に対するサイバー攻撃の実態を把握するため、通信情報を利用して、分析する。具体的には次の通り。

○内閣総理大臣は、基幹インフラ事業者等との任意のサイバーセキュリティに関する協定に基づき通信情報を取得し、このうち外国からの通信を分析して、当該事業者に分析結果を提供する（新法第３章）。

○内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、サイバー通信情報監理委員会の承認を得て通信情報を取得する（新法第４章、第６章）。

○取得する通信情報は、ＩＰアドレスや指令情報などの機械的情報に限定される。機械的情報は人による知得を伴わない自動的方法によって選別され、それ以外の情報は消去される（新法第５章、第７章）。

○通信情報の利用の適性確保のため、サイバー通信情報監理委員会を設置する（新法第10章）。

（3）攻撃者のサーバ等へのアクセス・無害化措置（整備法）

サイバー攻撃による重大な危害を防止するための警察・自衛隊による措置を可能とし、その際の適正性を確保する手続を新設する。次の通り。

○警察庁長官が指名する警察官は、サイ

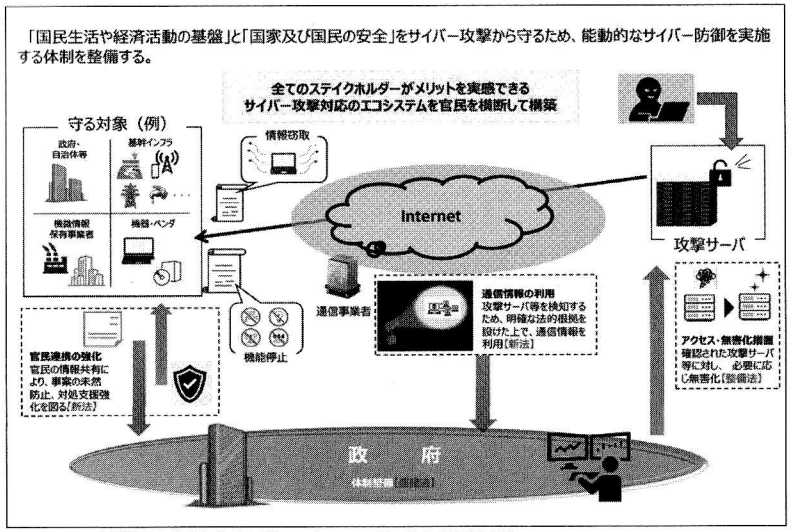
バー攻撃に用いられる電気通信等を認めた場合に、「そのまま放置すれば、人の生命、身体または財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは」、危害防止措置（インストールされている攻撃のためのプログラムの停止・削除など）を執ることができる。（警察官職務執行法第6条の2新設）。

○この措置を執る場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならない。但し、加害電気通信が現に送信されている場合その他危害防止のために承認を得るいとまがないと認める特段の事由がある場合には、事後通知で可（同上）。

○危害防止処置の対象となる電子計算機が国外に設置されている可能性がある場合には、あらかじめ外務大臣との協議が必要（同上）。

○内閣総理大臣は、攻撃が、国外にある者による特に高度に組織的かつ計画的な行為と認められる場合において、（自衛隊が有する特別の技術または情報が必要不可欠であるなど）自衛隊が対処を行う特別の必要があると認めるときは、通信防護措置を命ずることができる（自衛隊法第81条の3新設）。その際の権限は、警察官職務執行法を準用する（自衛隊法第91条の3新設）。

○自衛隊または在日米軍の使用する一定の電子計算機をサイバー攻撃から職務上警護する自衛官についても、改正警職法の権限を準用する（自衛隊法95条の4新設）。



サイバー対処能力強化法案のイメージ（内閣官房）

（4）内閣サイバー官の新設など組織・体制の整備（整備法）

能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる内閣官房新組織の設置等、政府を挙げた取組を推進するための体制を整備するとして、次の強化策が示されている。

○サイバーセキュリティ戦略本部の改組強化：本部長を官房長官から総理大臣に格上げし、本部員を特定の大臣から全ての国務大臣に拡大する。さらに「サイバーセキュリティ推進専門家会議」

を設置する（サイバーセキュリティ基本法第28条、第30条、第30条の2の改正新設等）。

○内閣サイバー官（国家安全保障局次長兼務）を新設し、サイバーセキュリティの総合調整等に当たらせる（内閣法第19条の2新設）。

2　総合的評価

さて、本法律の制定で、我が国のサイバー対応能力が欧米水準になると言えるであろうか。

結論から言えば否であり、欧米水準と比べると不十分であり、課題も多く残されている。

しかし、我が国のサイバーセキュリティの現状を前提とすれば、とにかく本法律が制定されたこと自体が大きな前進であると評価すべきであろう。日本の政治状況など諸条件を勘案すれば、現在、制定可能な法律であったというべきもので、不十分で課題が多く残されていても仕方がないと言える。

法律は制定後の運用実績を見て今後改正を重ねていく必要がある。政府は国会審議で、本法律はサイバー対処能力強化の「第一歩である」（サイバー安全保障担当大臣）とか、「不断の見直しが必要」（内閣総理大臣）と述べる(3)など、将来の法律改正に含みを持たせる答弁をしており、本法律の不十分性は十分認識していると考えられる。今後の逐次改正、改良を期待したい。それでこそ、本法律の意義が大きなものとなろう。


サイバー対処能力強化法及び同整備法の成立後に開催された第43回サイバーセキュリティ戦略本部（内閣官房）

それでは、以下、本法律案では不十分な点や将来の課題を述べていきたい。先ず欧米諸国、特に米国と我が国の基礎的条件の違いについて述べ、次に法律案に即して、個別の課題を見ていきたい。

3　我が国に不足する基礎的条件

本法律自体の評価以前の課題として、我が国のサイバーセキュリティにおいては、米国と対比して、不足する二つの基礎的条件があることを指摘しておきたい。それは、サイバーセキュリティに関与するシギント機関の不在とプラットフォーマーの不在である。

（1）サイバーセキュリティに関与するシギント機関の不在

我が国に欠ける基礎的条件の一つは、サイバーセキュリティに関与する「シギント（信号諜報）機関」である。シギントとは、インターネット上を含む通信や

電波、信号の傍受で得た情報を利用するインテリジェンス活動のことであり、シギントは国家の安全保障や電子戦を含む軍事技術とも密接に結びついている。そして、シギント活動はサイバーセキュリティのため重要な要素でもあるが、残念ながら、本法律案検討のための政府有識者会議の議事録を読んでも、ほとんどシギントに対する言及が見られない。

英国のシギント機関、GCHQ の本部（MoD of UK）

（ア）UKUSA諸国のシギント機関の係わり

世界最強のインテリジェンス同盟にUKUSAがある。第二次世界大戦において、米英両国は対日独伊戦争を遂行するため、シギントでも緊密に協力した。この協力が大きな成果を上げたため、その協力関係を戦後も継続することとしたが、それが通称「UKUSA」と呼ばれるシギント同盟である。英UKと米USA両国の協定を基軸として、その後カナダ、オーストラリア、ニュージーランドが加わった。この五か国のシギント機関は密接に協力して、ワールドワイドに活動する世界最強のインテリジェンス同盟を構築してきたのである(4)。

UKUSA同盟は、サイバー空間を含め世界中に及ぶ強大な情報収集力を持ち、同盟参加五か国のサイバーセキュリティをバックアップしている。米国を除く四か国では、サイバーセキュリティを所管しているのは、全てシギント機関である。例えば、英国ではシギント機関である政府通信本部（GCHQ）に「ナショナル・サイバー・セキュリティ・センター」という組織が附置され、同機関が政府のサイバーセキュリティの主管組織となっている。また、カナダ、豪州、ニュージーランドも同様に、サイバーセキュリティの主管組織は、それぞれのシギント機関に附置されている。

他方、米国では国家安全保障庁（NSA）という国家シギント機関があるが、二〇世紀におけるインテリジェンス機関に対する不信という過去の経緯があり、サイバーセキュリティ全体の主管官庁は、NSAではなく、国土安全保障省傘下のサイバーセキュリティ・社会基盤安全保障庁（CISA）という組織である。ところが、サイバー空間についてはNSAが突出した技術力と情報力を持っているため、二〇一九年にNSAは「サイバーセキュリティ総局」を設置して、自らサイバーセキュリティに対する取組を強化すると共に、CISAを支援している。また、サイバー関連の事件では、NSAがFBIによる捜査を支援している。

（イ）シギント機関はサイバーセキュリティに不可欠

UKUSA諸国でシギント機関がサイバーセキュリティに深く関与している理由は、一言で言えば、シギント機関がハッカー組織でもあるからである。もちろんシギントとはハッキングだけではなく、無線通信も含む多様な通信の傍受解読をしている。

ところが、二〇〇〇年前後からサイバー空間が極めて重要な情報空間となってきたため、NSAは一九九七年にTAOというハッキング専門部署を設置して、情報収集のためにサイバー空間を開拓してきた。おそらくNSAのTAOが世界最強のハッカー組織であろう。このように、シギント組織はサイバー空間で情報収集を行い、ハッキングも行っているので、攻撃側の手口が分かる。攻撃方法を知って初めて効果的な防禦も可能となるのである。したがって、サイバーセキュリティにおいても、シギント組織による支援が必要なのは当然である。

米国のシギント機関、NSA の本部（NSA）

ところで、一部にハッキングとは「天才ハッカー」のような傑出した人材が行っているイメージがある。しかし、NSAのTAOはどちらかというと「装置・技術産業」であり、そのためのシステムを世界中に設置している。協力企業やUKUSA諸国やいわゆるサードパーティー諸国と協力関係を構築して、インターネット回線から情報を吸い上げている。NSAは世界中でサイバー空間を監視するトータルなシステムを構築しているからこそ、高いハッキング能力を持っているのである。逆に言うと、サイバー防禦でも、そうしたシステムを使ってハッカーの脅威情報を把握することによって、ハッカー集団によるサイバー攻撃を事前に察知することが可能となるのである。

少し古い資料であるが、二〇〇七年時点での「米国シギント・システム戦略的任務リスト」という機密資料が漏洩されている。その中ではNSAの任務として、①コンピュータ・ネットワーク防禦支援、②コンピュータ・ネットワーク攻撃支援、③外国諜報諸機関によるサイバー脅威活動の解明が、明示されている(5)。

（ウ）アトリビューション支援

シギント機関による具体的なサイバーセキュリティ支援では、攻撃を受けた際の攻撃者の特定（アトリビューション）への貢献がある。

例えば、二〇一四年に米国のソニー・ピクチャーズ・エンタテインメントが北朝鮮から大規模なサイバー攻撃を受けた際には、攻撃発覚後一か月程でFBIが

北朝鮮の犯行と断定している。このアトリビューションではNSAが支援しており、NSAの看板プログラム「エックスキースコア」というシステムが貢献している。

「エックスキースコア」は、本来は情報収集のためのシステムで、世界中の主要収集拠点に設置されたデータの一次記憶装置であり、かつ分析支援システムである。これが同時に、アトリビューションにも活用できるのである。かつてNSAの職員であったエドワード・スノーデンが、二〇一三年に大量の情報を漏洩したが、漏洩資料の中に「X-Keyscore for Cybersecurity」という表題のプレゼン資料があり、サイバーセキュリティにおけるエックスキースコアの活用方法を説明している。また、スノーデン自身もサイバー攻撃に対するアトリビューションでエックスキースコアを使ったことがあると述べている(6)。

この他にも、「宝地図」や「プリズム」など活用できるシギントのシステムがあり、NSAは、これらを活用してアトリビューションに貢献しているのである。

(エ) 脅威情報の事前把握

また、サイバー防禦では脅威情報の事前把握が重要であるが、シギント機関は各種の手法で脅威情報を事前に収集している。エドワード・スノーデンによる漏洩資料によると、二〇一三年の時点で既に次のような対策を取っていた(7)。

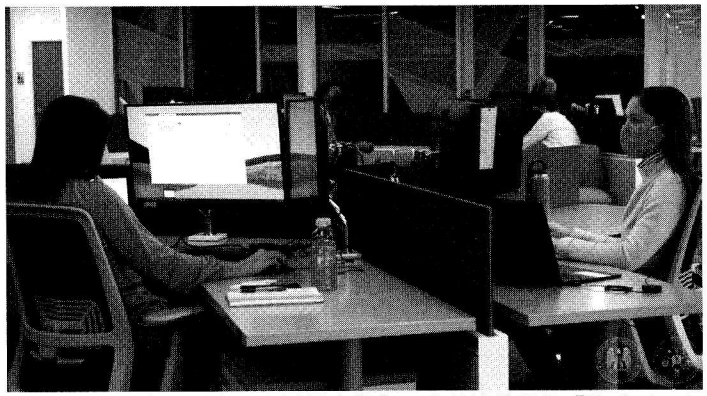
○「イオンブルー」：世界のインターネット通信網に設置したハッカー通信の探知センサー。カナダのシギント機関である通信安全保障局（CSE）がUKUSA諸機関の協力を得て設置したもので、二〇一〇年時点で世界二〇〇か所以上に設置していた。

○「ラブリーホース」：ダークウェブ上のハッカーのブログやチャットから、ハッカーの動向に関する情報を自動的に収集し分類して、分析官が使用できるようにしたシステム。英国のGCHQが開発した。現在、イスラエルや韓国、台湾系などの民間企業が、このようなダークウェブの情報を収集分析して販売しているが、シギント機関は既に一五年前にシステム化していたのである。

○「C-CNE（Counter-Computer Network Operation）」：ハッカー集団をハッキングしてその脅威（ウィルスなどの技術情報や攻撃目標、入手情報など）を解明するシギント活動である(8)。NSAは二〇一三年時点で中露などの二八のハッカー集団をハッキングして脅威情報を収集し、ハッカー集団に対して対策を講じていた(9)。

なお、二〇二三年のワシントンポスト紙の報道によれば、二〇二〇年秋にNSAは防衛省のコンピューターシステムが中国人民解放軍によってハッキングされているのを探知し、米政府はこれを日本政府に警告したという。これは、NSAがC-CNEによって浸透した人民解放軍系のハッカー集団のコンピュータの中に、防衛省の機密情報を発見したものと推定できる。

以上、簡潔に述べたが、NSAはじめUKUSAシギント諸機関のサイバーセキュリティにおいて果たす役割は大きなものであり、将来的には、我が国のシギント機関の抜本的強化とサイバーセキュリティへの関与を議論すべきであろう。



NSAが2020年に設立した民間企業との官民連携組織「サイバーセキュリティ協働センター」の内部（NSA）

(2) 巨大プラットフォーマーの不存在

米国と対比して我が国に欠けるもう一つの基礎的条件は、巨大プラットフォーマーの存在である。

米国にはグーグル、アマゾンウェブサービス、マイクロソフトといった巨大プラットフォーマーがある。彼らは世界中に及ぶ彼らのプラットフォームから、日々、脅威情報などを収集している。その上でNSAと密接に協力している。二〇二〇年にNSAは本部ビルの隣に民間企業との官民連携組織「サイバーセキュリティ協働センター」を設立した。二〇二三年夏の時点でIT企業など約五〇〇社が参加している。そこでサイバーセキュリティに関する技術的知見について実務的な情報交換をしている。NSAがシギント活動から得た機密の知見と、民間企業が収集した脅威情報と専門技術を総合しており、サイバーセキュリティ対策の拠点となっている。NSA本部は秘密保持のため原則的に民間企業の人は入れないため、近くに民間企業用の専門家と協働するためのビルを建設したのである。

残念ながら、日本には巨大プラットフォーマーが存在しない上、シギント機関と民間企業の密な情報交換もない。初期条件で既に大きなハンディキャップを背負っているのである。法律だけを見ても、この基礎的条件の違いは分からない。この点を押さえた上で、次に本法律の今後の課題について、国会審議も踏まえて法律案に即して論じていきたい。

4 アクセス・無害化措置の課題

先ず、注目を集めている、いわゆるアクセス・無害化措置について論じる。

本法律では、このアクセス・無害化措置について、どこまで実効性ある手段が提供されているのかが、分かり難い。例えば警察によるアクセス・無害化措置については、警察官職務執行法第6条の2（新設）では、サイバー攻撃に用いられる電気通信等を認めた場合に、「そのまま放置すれば、人の生命、身体または財産に対する重大な危害が発生するおそれがあるため緊急の必要があるとき」に無

害化措置を実行できることになっている。

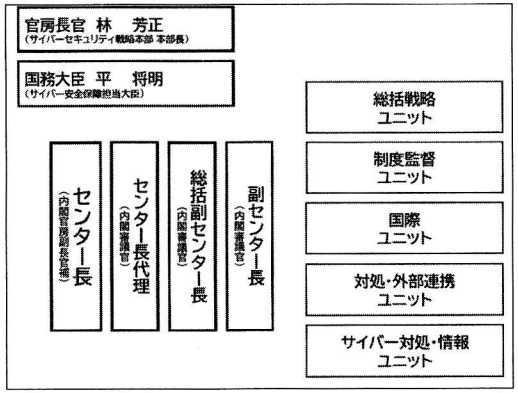
では、どうやって「緊急の必要」の要件に合致するか認定するのであろうか。事前に情報がなければ、被害が発生する前にその認定はできないはずである。事前の脅威情報がなければ、攻撃されて被害を受けてから初めて分かることになる。どの集団がどのような手段を使ってどの標的を攻撃しようとしているかを、いかに事前に解明するかが重要である。そのような脅威情報を事前に解明できれば、実際に攻撃を受け被害が発生する前に無害化することが可能となる。しかし、解明できないならば、攻撃を受け多大な被害が発生してからでないと、「緊急の必要」があるかどうか分からない。

すなわち、緊急の必要が生じるかどうかも含め、事前に脅威情報を解明しておかなければ、いざというときに無害化できない。国家安全保障戦略がいう「未然に攻撃者のサーバ等への侵入・無害化」はできないのである。つまり、当方から先にハッカー集団のサーバをハッキングして、ハッカー集団の持つマルウェアなどの技術情報、攻撃しようとしている標的などの作戦情報などを事前に把握して初めて、甚大な被害を受ける前に攻撃を阻止することができるのである。

ところで本法律では、無害化措置（警察による危険防止措置、自衛隊による通信防護措置）については規定されているが、そのためのアクセスとアクセス要件についての規定はない。衆議院内閣委員会の審議でもアクセスに限った要件の議論は見られなかった。仮に無害化措置の要件「そのまま放置すれば、人の生命、身体または財産に対する重大な危害が発生するおそれがあるため緊急の必要があるとき」に初めてアクセスの努力をできると解釈するならば、アクセス・侵入は即時にはできないのであるから、実効性のない規定となってしまう。そこで、合理的に解釈するならば、ハッカー集団のサーバ（及びハッカー集団が支配するサーバ）へのアクセスは、無害化措置を適切に行うための正当な事前の準備行為、すなわち正当業務行為（刑法35条）であると解釈して、普段から行う必要があるだろう。そうでなければ、無害化措置も絵に描いた餅となってしまう。

また、本法律では、加害サーバが国外にある可能性のある場合に無害化措置を実行するには、外務大臣と協議し、更にサイバー通信情報監視委員会の承認を受ける必要がある。しかし、無害化措置を実行するのは「緊急の必要があるとき」である。その時に大臣協議や委員会承認の時間的余裕があるのだろうか。

国会審議における政府答弁(10)によれば、無害化措置の手続は、「先ず国家安全保障会議四大臣会合で対処方針を定め、次にサイバー安全保障担当大臣の指導の下に内閣サイバーセキュリティセンター（NISC）の(11)後継組織（新NISC）が国家安全保障局と連携して総合調整を行い、その後に実施主体である警察または自衛隊が個別の無害化措置を行う」という。また、実際の無害化措置は、相手のサーバをインターネットにアクセスできなくするとか、攻撃コマンドを送れなくするというもので、破壊的なものにはならないとされている（政府答弁(12)）。



現在の内閣サイバーセキュリティセンターの編成
（内閣官房）

このような無害化措置には、本手続で十分であろう。外務大臣協議では、無害化措置が国際法上の許容範囲か否かを協議するとされているが、そもそも、無害化措置は国際的には生成途上のものであるので、国内法のように確立した判例や解釈が存在するわけではない。外務省の関与は、四大臣会合や国家安全保障局を通じた調整で十分であろうし、サイバー通信情報監視委員会の関与は事後報告で十分ではないだろうか。

ちなみに、二〇一八年以前の米国では、国外に対する秘匿の無害化措置は、インテリジェンス機関の「秘密工作」に該当したが、秘密工作には大統領決裁が必要であり、その前段で国家安全保障会議（NSC）を経由（そのための関係省庁調整）する必要があるため、サイバーセキュリティ対策では機能しなかった。そこで、（無害化措置等を）「伝統的軍事活動」と定義し直すことによって、実施要件を下げて実施できるようにした。つまり、武力の行使に至らないものは、国防長官の権限、実質的にサイバー司令官＝NSA長官権限とすることにより、サイバーセキュリティのための無害化措置の実行を容易にしたのである(13)。この経緯と対比すると、外務大臣との事前協議や通信情報監視委員会の事前承認は過重な手続規定であろう。

5　事業者の保有する通信情報の利用の課題

(1)「選別後通信情報」の限定性

本法律では、政府が通信事業者から取得して分析対象とする通信情報は「選別後通信情報」、すなわち人による知得を伴わない自動的な方法によって、「不正行為に関係があると認めるに足りる状況」の「機械的情報」（IPアドレス、指令情報等の意思疎通の本質的な内容ではない情報）のみを選別し、それ以外は直ちに消去する措置を講じたものとされる（「自動選別」）。この限定の下で、どれだけ有効なサイバーセキュリティ対策ができるのか、疑問である。

結局「選別後通信情報」とは、既知の加害サーバとの通信や既知のマルウェアを含む通信に限定されてしまうだろう。つまり、未知のマルウェアは探知できない。新しいマルウェア情報を入手しても、過去の通信情報に遡って検索することもできない。また、メールに添付されたPDFファイルに仕込まれたマルウェアを探知できるのであろうか。

さらにハッカー通信には、ハッキングしたサーバから入手する機密情報が含まれる。しかし、機密情報は機械的情報には含まれないであろうから、機密情報が

漏洩しているかどうかについては、国内の通信事業者から得た通信情報からは知り得ないこととなる。先に紹介したNSAのエックスキースコアは、機械的情報に限定せずに通信内容を収集しているので、ハッカー集団のアトリビューションにも有効なのであるが、我が国の場合の有効性は限定的なものとなろう。

二〇二三年五月に米連邦捜査局（FBI）は、ロシアの諜報機関であるロシア連邦保安庁（FSB）（旧ソ連国家保安委員会〈KGB〉）のセンター16内のハッカー組織が使用する「スネイク」というマルウェアを感染コンピュータ多数から除去する作戦を実施したが、「スネイク」によるハッカー通信は、HTTPやTCPなどの正常通信を偽装した暗号通信であり、その探知は困難を極めたとされている。そのため、その解明には、「スネイク」型マルウェアが発見されて以来二〇年近い年月を要している(14)。このような高度なマルウェアによるハッキングを、本法律の枠組で探知し得るのであろうか。疑問である。

さらに、本法律は、外外通信についてまで、分析対象を「機械的情報」に限定しているが、外外通信の秘密は日本国民の人権とはほとんど関係がないと見られるので、これは過剰な限定である。

以上は、将来の改正時の検討課題であろう。

なお、内々通信は本法律による収集分析の対象外であるが、本法律制定後は、当然、攻撃側は日本国内のサーバを経由するなどして探知の回避措置をとるであろうから、近い将来、内々通信に関する情報収集の必要も認識されるであろう。

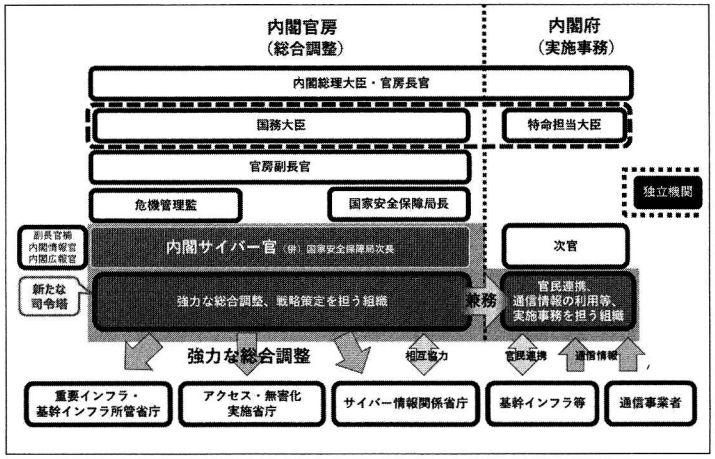
(2)「選別後通信情報」の使用目的の限定

このように「選別後通信情報」のデータ項目自体が限定的であるが、さらにその使用目的も、被害防止目的に限定されている（新法23条2項）。かつ、国会審議における政府答弁(15)によれば、本法律の目的は被害防止という行政目的であるので、「選別後通信情報」は犯罪捜査には使用しないとしている。

しかしながら、逮捕起訴を含む犯罪捜査によって加害行為を鎮圧するのは、まさに被害拡大防止を含む被害防止目的に適うのであるから、犯罪捜査には使用しないとの解釈には疑問を抱かざるを得ない。

最近、サイバー攻撃の激化に対抗して、国際的に協力して対処する事例が増加している。国際共同捜査を行い、共同でパブリック・アトリビューションをしたり、参加国の一部が指名手配をしたり訴追したりするのである。著名な事例では、二〇二四年七月に発出されたサイバーセキュリティの国際アドバイザリーがある。これは、中国海南省の国家安全庁傘下のハッカー集団「APT40」の脅威に対して、豪州が中心となって注意を喚起したものであるが、共同署名国には米英加ニュージーランドのUKUSA加盟国に加えて、日本、韓国、ドイツも加わっており、注目を集めた。このアドバイザリーはパブリック・アトリビューションの一種である。これより先、二〇二一年にも米英とEU諸国はAPT40のパブリック・アトリビューションを行い、同時に米国司法省がAPT40メンバー四人を起訴している。

このように、サイバーセキュリティの国際協力においては、パブリック・アトリビューションや、起訴という犯罪捜査も総合して行うものである。しかし、我が国が「選別後通信情報」を犯罪捜査には使用しないという立場であるならば、新法第28条（外国の政府等に対する選別後通信情報の提供）の規定の解釈としては、他国による起訴や捜査利用の可能性がある限り他国には提供しないということになろう。そのようなことで国際協力が成り立つのであろうか。



新たな司令塔機能のイメージ（内閣官房）

さらに万が一、我が国が他国と交戦状態となり防衛出動が下令された場合には、「選別後通信情報」を、自衛隊部隊は新法の枠組（公共の秩序の維持）の中では使用できるが、武力の行使、すなわち破壊的結果をもたらすサイバー攻撃のためには使用できないという解釈にならざるを得ないであろう。国家がその生存を賭けて持てる資源を総動員して戦うべき時に、そのような使用目的的の制限を付して、良いのであろうか。

また、国会審議における政府答弁(16)によれば、アクセス無害化措置の過程で得た情報の犯罪捜査での使用は想定していないという。米国司法省による起訴状などの資料を見ると、米国はまさにハッカー集団のサーバにアクセスしてハッカー集団を解明して、これに基づいて起訴していると推定できるが、我が国はハッカー集団を解明して起訴したりする意図はないと表明していることとなる。これも不可解である。

6 官民連携の課題

官民連携では、不正アクセス行為などのインシデント情報を所管大臣と内閣総理大臣に報告する対象事業者が、一五業種の基幹インフラ事業者に限定されている。医療機関などは含まれておらず、報告義務を負う事業者の範囲が狭すぎるのではないかと危惧する声も聞くが、当初は限定されていても仕方がないと考える。対象事業者の拡大は将来の課題であろう。

むしろ本法律で気になるのは、基幹インフラ事業者が提出するインシデント情報の報告先である。以前から所管官庁や個人情報保護委員会など、政府の報告先がいくつもあり、これでは煩雑であり、

政府の報告窓口を一本化して欲しいという要請があったが、この法律は依然として、事業の主管官庁など複数の報告先があり、報告窓口の一本化が実現していない。国会審議では報告様式を統一し煩雑さを軽減するとしているが、それでは不十分ではないか。報告窓口の一本化も将来の課題であろう。

もっとも、窓口一本化の前提には、窓口となる組織機関の力量が課題となる。内閣官房のNISC後継の新NISCがどのような組織になるかはまだ明らかではないが、その専門能力や事務量など十分な力量の確保が課題であろう。UKUSA諸国のうち米国以外の英加豪ニュージーランドがシギント機関の附置機関にサイバーセキュリティを所管させているのも、限られた専門人材を有効に活用しようという意図であろう。

7 政府の組織・体制の整備の課題

組織・体制の整備では、サイバーセキュリティ戦略本部の改組強化、「サイバーセキュリティ推進専門家会議」の設置、内閣サイバー官の新設が掲げられている。今後、事務局であるNISCが改組されて強化される予定であるが、重要なのは、NISC後継組織（新NISC）が、真の専門家集団となる人事をどのように構築していくかであろう。NISCは現在、生抜き職員がずっといるわけではなく、多くの官庁からの二年間程度の出向者や一年から数年の任期制職員が大多数を占めていると見られる。そこで、真の専門家集団になるような人事をどのように構築して行くのかという課題がある。

日本の公務員の人事制度は、一つの役職の任期が短いため、どうしても専門性が高まらず、また知識経験の蓄積が不十分な傾向にある。人事の課題に正面から取り組む必要があろう。

8 最後に

以上論じたように、今回の「サイバー対処能力強化法及び同整備法」は、多くの課題を残す法律であり、これで欧米水準のサイバー対応能力が構築できるとは到底言えないであろう。

しかしそれでも、本法律は、我が国のサイバーセキュリティ対策において大きな前進である。残された課題は、制定後の運用実績を見て改正を重ねていけば良いのであり、そうしてこそ本法律の意義が大きなものとなろう。

ところで、課題を残す法律制定の背景には、我が国における人権の理解の在り方が横たわっている。一部の学識者は、憲法が保障する「通信の秘密」と国家権力を対置して、「通信の秘密」という人権を必死で守ろうとする。

しかし、現代社会のサイバーセキュリティは、国民の豊かで安全で自由な生活を確保するため不可欠な社会基盤である。すなわち、外国インテリジェンス機関がサイバー空間を通して、我が国の機密情報を容易に窃取し、情報工作によって世論を分断できるようでは、外交の場で不利益を被るのみならず、我が国の国家体制の弱体化や民主政治に混乱が生じ、引いては、国民の人権を守るべき国家の枠組自体が危うくなる。また、サイバー攻撃によって基幹インフラ企業が機能不全に陥れば、国民生活に直接的な被害が生じる。さらに、企業に対するハッキングによって、優れた先端科学技術や企業秘密が流出し続ければ、民間企業の競争力が低下して、国民生活が貧困化してしまう。あるいは、ランサムウェア攻撃やインターネット詐欺などのサイバー犯罪が横行し適切に取り締まれなければ、国民生活が犯罪の脅威に晒される。つまり、サイバーセキュリティとは、豊かで安全で自由な国民生活という人権を守るための重要な社会基盤なのである。

一方、「通信の秘密」も大切な人権であるが、これを教条的に掲げれば、それは、犯罪のための通信の秘密の擁護に陥ってしまうこととなる。

「通信の秘密」という人権も、サイバーセキュリティによって守られるべき国民の豊かで安全で自由な生活も、共に重要な人権である。したがって、この両者の人権を守るためには、サイバーセキュリティ確保のための各種の施策が、どのような状況でどのように「通信の秘密」を侵害するおそれがあるのか、それは豊かで安全で自由な国民生活を守るために許容できる範囲のものなのかを、具体的に検討する必要がある。

そうなれば、「通信の秘密」を教条的に掲げた不毛な議論も終りを告げるであろう。

【注】

(1)内閣官房、国会提出法案（第217通常国会）、https://www.cas.go.jp/jp/houan/217.html

(2)基幹インフラ事業者（＝「特定社会基盤事業者」）とは、経済安全保障推進法第50条第1項に規定する事業者で、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航海運、航空、空港、電気通信、放送、郵便、金融、クレジットカード、港湾の一五業種で、医療機関などは含まれない。

(3)衆議院内閣委員会。四月四日、市村浩一郎議員の質問に対する平サイバー安全保障担当大臣の答弁、及び、今井雅人議員の質問に対する総理大臣答弁。

(4)シギントについての概説書としては、茂田、江崎道朗（共著）『シギント』（ワニブックス、二〇二四年）参照。

(5)茂田「米国国家安全保障庁の実態研究」（警察政策学会資料第82号、二〇一五年）三〇頁

(6)茂田「サイバーセキュリティとシギント機関～NSA他UKUSA諸機関の取組～」（情報セキュリティ総合科学第11号、二〇一九年）六四・六六頁。

(7)茂田「米国ACD・Defend Forwardとシギント機関の役割～日本『能動的サイバー防御』と対比して～」（警察政策学会資料第134号「国家安全保障に関する諸論考」、二〇二四年）三四・三六頁

(8)茂田、前掲「米国国家安全保障庁の実態研究」九五・九六頁。

(9)米国におけるActive Cyber Defenseとは、本来このような脅威情報を事前に把握した上で、自己のネットワークとインターネットの接続点において対抗手段を設置するものであり、代表的なシステムとしてはTutelageが知られている。茂田、前掲「米国ACD・Defend Forwardとシギント機関の役割」三五・三六頁参照。

(10)衆議院内閣委員会。四月二日、藤岡たかお議員の質問に対する小柳内閣官房審議官答弁、四月四日、橋本幹彦議員の質問に対する平大臣答弁など。

(11)内閣サイバーセキュリティセンターNational Center of Incident Readiness and Strategy for Cybersecurity

(12)衆議院内閣委員会。四月三日、赤嶺政賢議員の質問に対する平大臣答弁。

(13)茂田、前掲「米国ACD・Defend Forwardとシギント機関の役割」四一・四三頁。

(14)米司法省、"Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service," Justice News, 9 May 2023

(15)衆議院内閣委員会。四月二日、平岡秀夫議員の質問に対する小柳内閣官房審議官答弁。

(16)衆議院内閣委員会。四月四日、塩川鉄也議員の質問に対する警察庁サイバー警察局長答弁。