基礎研レポート

サイバー対処能力強化法の成立

能動的サイバー防御

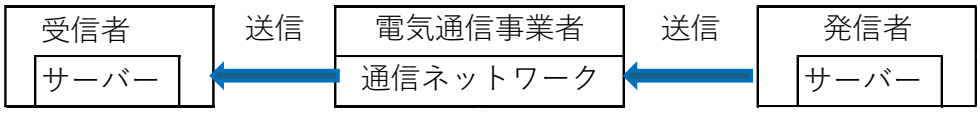
取締役 保険研究部 研究理事　**松澤　登**
(03)3512-1866　matuzawa@nli-research.co.jp

1――はじめに

サイバー対処能力強化法（以下、強化法）は、重要電子計算機への不正行為を防止するための法律および関連法の整備法を含み、2025 年 5 月 16 日に国会で成立した。このうち、同法律（以下、「強化法」）と警察官職務執行法（警職法）と自衛隊法を解説する。

今回制定・改正された強化法等はコンピューターウイルスなどのサイバー攻撃に対して、政府が情報を収集・分析し、分析結果を事業者等に提供すること、および実害が発生する以前に対処することを定めたものである。強化法が想定するサイバー攻撃は図表 1 の図示する通りであり、攻撃主体（図表 1 の発信者）が通信ネットワークを介して受信者側に攻撃を仕掛けるといったものである。強化法等では、特に国外から国内に対して攻撃がなされるものを想定している。これはサイバー攻撃のうち 99.4%が国外からのものとされる実態調査結果に基づいている[1]。

【図表 1】サイバー攻撃



国外からのサイバー攻撃については、組織的な攻撃が行われているという指摘がある。そのため、強化法等では国外から送信されたサイバー攻撃について情報収集・分析し、その結果を利用・提供する体制が構築される。そのうえで必要があれば、まずは警察が対応し、有事の場合は自衛隊が出動するという仕組みになっている（後述）。ここには自衛権の行使という側面もある。

この点、強化法等の立法の基礎となった有識者会議報告「サーバー安全保障分野での対応能力の向

[1] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf　参照。

上に向けた提言」では、重大なサイバー攻撃が国家の安全保障上の懸念であると明記された。これを受け、官民ともに「常に有事である」という危機意識を持って対応が求められている[2]。

なお、強化法等はテクニカルな用語や規定の仕方が多く、一見しただけでは容易には理解しがたい規定内容になっている。したがって、内容については幹の部分のみに焦点を当てるとともに、条文を大幅に簡略化するなど文章を工夫している点に注意していただきたい。

2――目的･定義･基本計画

1｜目的

強化法の目的についてだが、強化法 1 条では、具体的な目的として、以下の①～⑤が定められている。強化法が定義している特殊な用語が多いが、これらは後述する。

①重要電子計算機に対する特定不正行為による被害の防止のための基本的方針の策定
②特別社会基盤事業者による特定侵害事象等の報告の制度
③重要電子計算機に対する国外通信特定不正行為による被害の防止のための通信情報の取得
④当該通信情報の取扱いに関するサイバー通信情報監理委員会による審査および検査
⑤当該通信情報を分析した結果の提供

これを要約すると、強化法では、政府が同意の下で情報提供を受け、あるいは自発的に情報を取得したうえで、分析し、その結果を関係行政機関あるいは関係事業者に提供することが目的として定められている。　そのうえで警職法により警察が、自衛隊法により自衛隊がそれぞれ一定の要件のもと対処することになる。

2｜定義

(1) サイバーセキュリティ

まず、サイバーセキュリティであるが、これはサイバーセキュリティ基本法 2 条に定められたものをいう（強化法 2 条 1 項）。サイバーセキュリティ基本法 2 条を要約すると、情報システムがサイバー攻撃の脅威から十分に隔離され、安全性が維持管理されることをサイバーセキュリティとしている。

(2) 重要電子計算機

強化法の適用対象となるのが「重要電子計算機」であるが、概略すると以下のもののうち、政令で定めるものとされている（強化法 2 条 2 項）。

①政府（地公体含む）の保有する電子計算機のうち、防衛あるいは経済安全保障にかかわるもの
②特定社会基盤業者（下記に記載）が使用する電子計算機のうち一定のもの
③その他重要情報を保有する事業者が使用する電子計算機のうち一定のもの

上記②でいう特定社会基盤業者とは経済安全保障推進法（経済政策を一体的に講ずることによる安全保障の確保の推進に関する法律）50 条 1 項に定めるものをいう。同法においては電気事業者やガス事業者、水道業者、石油精製業などがある。ただし、強化法の対象となるのはこのうち政令で定める

[2] https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf　参照。

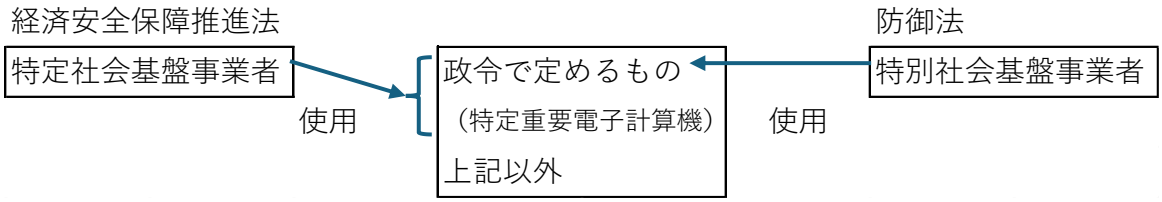
一定のもの（(3)で後述）を使用する事業者（＝特別社会基盤事業者）に限定されている。

上記③の重要情報を保有する事業者については、提言(4p)によれば「重要インフラ事業者」[3]および機微情報を保有する事業者が指定されることとされている。サイバーセキュリティ基本法では、保険会社が「重要インフラ事業者」として指定されており、生命保険会社は重要情報を保有する事業者と指定されることが想定される。

(3)特別社会基盤事業者

少し複雑だが、強化法の対象となる特別社会基盤事業者（提言では「基幹インフラ事業者」と表記）とは、上記(2)②でいう、特定社会基盤事業者が使用する電子計算機のうち、サイバー攻撃によって特定重要設備[4]の機能が停止・低下するおそれのあるものとして政令で定めるもの（これを「特定重要電子計算機」という）を使用するものと定義されている。したがって、特定社会基盤事業者のうち、特別社会基盤事業者となるものと、ならないものがある（図表 2）。

【図表 2】特別社会基盤事業者（イメージ）



(4)特定不正行為

強化法は「特定不正行為による被害の防止」を目的としているが、特定不正行為は以下のア）～ウ）を指す（強化法 2 条 4 項）。

ア）正当な理由なく、他人の電子計算機で不正指令電磁的記録作成等[5]をする行為（刑法 168 条の 2 第 2 項）

イ）不正アクセス行為[6]（2 条 4 項）

ウ）サイバーセキュリティを害することを通じて、信用および業務を害する罪（刑法 233 条～234 条の 2）[7]を犯す行為

---

[3] 提言でいう重要インフラ事業者とは、サイバーセキュリティ基本法 3 条 1 項でいう重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者）を指す。具体的には、「重要インフラのサイバーセキュリティに係る行動計画」で規定されている。

[4] 「特定社会基盤事業の用に供される設備、機器、装置又はプログラムのうち、特定社会基盤役務を安定的に提供するために重要であり、かつ、我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして主務省令で定めるもの」と定義されている（経済安全保障推進法 50 条 1 項）。省令では社債、株式の振替等に係るシステムが指定されている（内閣府・法務省・財務省関係経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づく特定社会基盤事業者の指定等に関する命令 1 条）。

[5] 「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」を人の電子計算機において実行することを指す。

[6] 本法に関連するのは特に「電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為」（2 条 4 項 3 号）であろう。

[7] 具体的には、信用毀損および業務妨害(233 条)、威力業務妨害(234 条)、電子計算機損壊等業務妨害(234 条の 2)である。

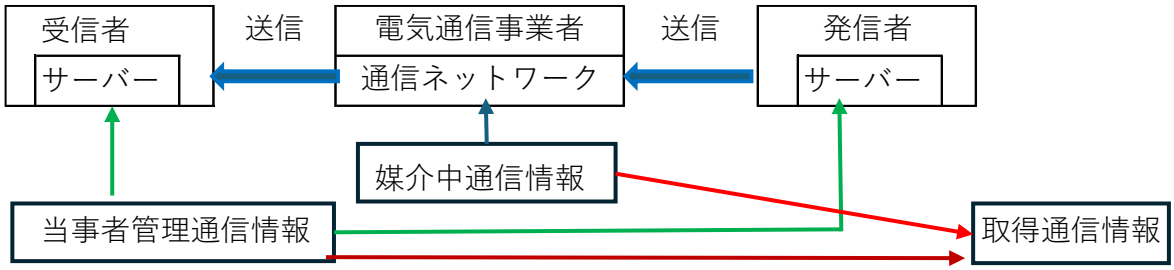
(5)特定侵害事象

強化法の対象となるのは特定侵害事象（＝サイバー攻撃）である。特定侵害事象とは、重要電子計算機（上記（3））に対する特定不正行為（上記(4)）により、当該重要電子計算機のサイバーセキュリティ（上記（1））が害される事象を言う（強化法2条5項）。

(6)通信情報

通信情報は三つのものが定められている。まず、通信中であって電気通信事業者が管理するものを「媒介中通信情報」といい、送信または受信される情報であって、送信者又は受信者が管理するものを「当事者管理通信情報」、そしてこれら二つの情報を複製して内閣総理大臣に提供されたものを「取得通信情報」という（強化法2条6項。図表3）。

【図表3】通信情報



(7)国外通信特定不正行為

国外にある電気通信設備を送信元とする電気通信の送信により行われる特定不正行為（上記(4)）をいう。すなわち強化法では国外発信のサイバー攻撃が主な適用対象となっている。

(8)機械的情報

強化法では、政府がサイバー攻撃に係る情報を取得することができるが、通信の具体的内容まで踏み込むこととはされていない。利用等できるのは、以下の三つに限られる（強化法2条8項）。

ⅰ)送信元または送信先を示す情報であるIPアドレス

ⅱ）電子計算機に動作をさせる指令を与える電磁的記録に記録された情報（指令情報）

ⅲ）その他通信内容にかかわらないものであって内閣府令で定めるもの

(9)通信情報保有機関

通信情報保有機関とは、ア）内閣府、イ)選別後通信情報(後述5の3)の分析に協力をする行政機関・外国政府・国際機関（強化法27条3項、36条)、被害防止のために選別後通信情報を提供された行政機関（強化法31条1項・2項。警察・自衛隊等)、ウ）選別後通信情報を整理または分析した情報を提供された行政機関(38条1項・2項)を指す。すなわち、政府が収集した情報を保有する行政機関を指す。

3｜基本方針

内閣総理大臣はサイバー攻撃による被害防止のための基本方針を作成し、閣議決定しなければならない（強化法3条)。方針に定められるのは、たとえば重要電子計算機に対する特定不正行為による被

害の防止に関する基本的な事項(2 項 1 号)などである[8]。

4｜コメント

上述の通り、保険会社はサイバーセキュリティ基本法で「重要インフラ事業者」として指定されていることから、強化法では「重要情報を保有する事業者」として法が適用されることとなるものと考えられる。

保険会社が重要情報を保有する事業者と指定された場合には、①当事者協定の締結（強化法 12 条、ただし特別社会基盤事業者に対して規定されている協議の求めおよび協議に応ずる義務(強化法 11 条 2 項）に相当する規定の適用はない)、②保有する重要電子計算機の被害が想定されるときに通信目的措置（通信情報を内閣総理大臣が取得する措置）の対象となること、③周知総合整理分析情報（後述 6 の 1）の提供先となること（強化法 41 条）が挙げられる。これらは後述する。

3――特別社会基盤事業者等

1｜特定重要電子計算機の届出

特別社会基盤事業者（上記 2 の 2 の(3)）が、特定重要電子計算機（上記 2 の 2 の(2)）を導入したときは、省令に定めるところにより、特別社会基盤事業所管大臣（金融業が指定された場合においては金融庁長官[9]）に届け出る必要がある（強化法 4 条 1 項、74 条 2 項)。届出事項に変更があった場合にも届出が必要である（強化法 4 条 3 項)。特別社会基盤事業所管大臣はこれら届出があった場合には内閣総理大臣に通知する(強化法 4 条 2 項、4 項)。

特別社会基盤事業者は特定重要電子計算機に係る特定侵害事象(上記 2 の 2 の (5))および当該特定侵害事象の原因となる事象として、省令で定めるものを認知したときには、特定社会基盤事業所管大臣および内閣総理大臣に報告する必要がある(強化法 5 条)。すなわち、サイバー攻撃を受けた際の報告義務がある。

そのほか、届出・報告に係る特定社会基盤事業所管大臣の命令権（強化法 6 条)、助言指導権（強化法 10 条）などが規定されている。

2｜当事者協定

(1)外内通信情報

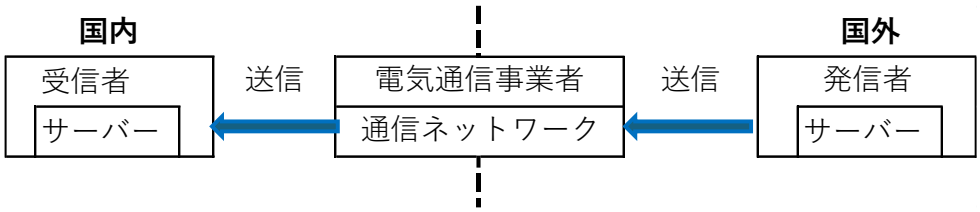
強化法 3 章で規定している当事者協定は、図表 4 でいう通信情報に係るものである。これは国外の IP アドレスから国内の IP アドレスに送信される情報で、強化法では外内通信情報と定義されている（強化法 11 条)。

---

8 このほか、当事者協定(強化法 13 条)の締結に関する基本事項(2 号)、通信情報保有期間における通信情報の取扱いに関する基本事項(3 号)、報告等情報などの整理および分析(強化法 37 条)に関する基本事項(4 号)、総合整理分析情報の提供に関する基本事項(5 号)、協議会（強化法 45 条）に組織に関する基本事項(6 号)、およびその他必要な事項(7 号)がある。

9 強化法第 2 章（特定重要電子計算機の届出等。本条も含む）および 40 条 1 項等の権限は金融庁長官に委任するものとされている（強化法 74 条 2 項)。金融庁長官はさらに権限を財務局長等に委任できる(3 項)。

【図表 4】外内通信情報

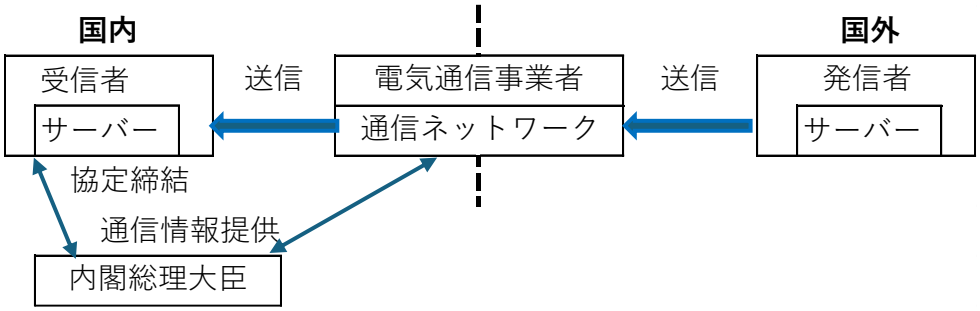


(2) 特別社会基盤事業者との協定締結

内閣総理大臣は特別社会基盤事業者（上記 2 の 2 の(3)）との間で、外内通信情報の提供を受け、分析し、その結果（「個別分析情報」という）をその特別社会基盤事業者に提供することを内容とする協定を締結することができる（強化法 11 条 1 項）。協定締結は義務ではないが、内閣総理大臣又は特別社会基盤事業者は相互に協定締結の協議を求めることができるとされ、当該求めを受けた相手方は協議に応じなければならない（強化法 11 条 2 項）。

また、本条で定める協定の内容として、媒介中通信情報（上記 2 の 2 の(6)、電気通信事業者が保有する情報）を内閣総理大臣に対して複製して送信することを定めるようとするときは、内閣総理大臣、特別社会基盤事業者、電気通信事業者による三者協定としなければならない（強化法 11 条 3 項、図表 5）。

【図表 5】三者協定



なお、内閣総理大臣は特別社会基盤事業者との協定締結に同意したときであって、特別社会基盤事業者からでは当事者管理通信情報（上記 2 の 2 の(6)）を取得することが困難な場合においては、電気通信事業者に対して当事者協定を締結することについて協議を求めることができる。この場合、電子通信事業者は協議に応じなければならない（強化法 13 条）。

(2) 特別社会基盤事業者以外の事業者との協定締結

内閣総理大臣は事業電子通信役務（＝電気通信事業者の通信サービス（強化法 2 条 6 項））の利用者（特別社会基盤事業者を除く）との間で上記(2)と同様の協定を締結することができる（強化法 12 条 1 項）。ただし、協議を求めることと、その協議に応ずる義務規定は存在しない。なお、上記三者協定の規定は本条の協定にも準用される（強化法 12 条 2 項）。電気通信事業者との協議規定（協議に応ずる義務を含む）の適用も同様である（強化法 13 条）。本条によって特別社会基盤事業者以外の事業者からも広く情報収集が可能になる。

(3)内閣総理大臣の情報取得

内閣総理大臣は当事者協定の定めるところに従い、当事者協定の協定当事者を通信の当事者とする通信情報の提供を受けることができる（強化法 15 条）。

3｜コメント

本項で述べたところは提言(2p)にある政府からの「高度な攻撃に対する支援・情報提供」となる部分である。提言はまた「『平時・有事』の区別なく、状況に応じて、政府が率先して情報提供し、官民双方向の情報共有を促進すべき」とする。さらに提言では「高度な侵入・潜伏能力を備えた攻撃に対し、事業者等が具体的な行動がとれるよう、攻撃者の動向を踏まえつつ、専門的なアナリスト向けの技術情報に加え、経営層が判断を下す際に必要な、攻撃の背景や目的なども共有されるべき」としている。

そして提言（5p）では「被害を防止するためには、通信情報を分析し(中略)、攻撃用のインフラの実態を把握し、防御を可能にすることが必須であり、特にアクセス・無害化を行うにあたっては、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」とする。

このような情報観測・分析の前提として、政府が情報収集をする必要がある。ただ、政府が通信情報を取得するにあたっては、「通信の秘密は、これを犯してはならない」（憲法 21 条 2 項）との整合性を取らなければならない。強化法が民間事業者からの通信情報取得の主たる方法として定めているのは、当事者協定である。これは通信の主体からその同意の下で情報を取得するものである。媒介中の通信情報についても、受信者の同意の下、さら電気通信事業者の同意を得て、取得することができる。

憲法 21 条 2 項を遵守するため、協定の締結そのものを義務化することはせず、当事者協定締結に向けた協議を求め、その場合は協議をする義務があるだけにとどまっている。

なお、後述の通り、取得した通信情報は自動選別によって、通信内容が削除された状態で行政において記録・利用されることとなる。自動選別前の情報の利用は原則として禁止されており、選別後通信情報にも厳格な利用制限がある。

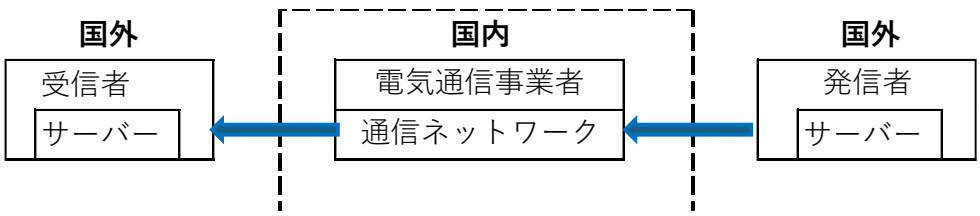
4――外外通信目的送信措置

1｜措置の内容

(1)総論

本項で述べる規制が適用されるのは、図表 6 の通り、国外 IP アドレスから国外 IP アドレスに送信されるもので国内設備を用いて媒介されるもの（外外通信という）である。

【図表 6】外外通信

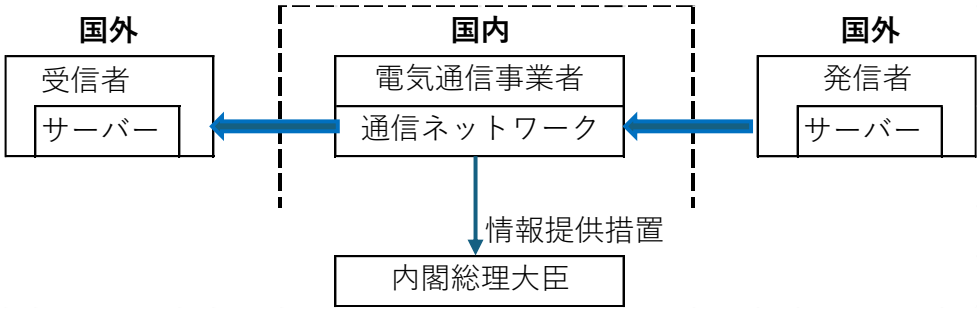


後述(2)の通り、外外通信のうち、サイバー攻撃の可能性が高いものについて、電気通信事業者から内閣総理大臣が通信情報を受領できることが定められている。

(2)外外通信目的送信措置

内閣総理大臣は、外外通信のうち、重要電子計算機に対する国外通信特定不正行為（上記2の2の(7)）のうち、一定のものについて、サイバー通信情報監理委員会（強化法46条、以下、「委員会」）の承認を受けて、電気通信事業者の媒介中通信情報（上記2の2の(6)）を複製し、内閣総理大臣の設置する設備に送信させる措置を取ることができる（強化法17条1項）。ここでいう一定のものについては、①電子計算機に対する指令情報の実態が明らかでないために重要電子計算機の被害防止が著しく困難であり、かつ②この送信措置以外では実態把握が著しく困難であるものに関連するものが、外外通信に含まれると疑うに足りるものをいう（図表7）。

【図表7】外外通信目的送信措置



この措置にあたっては自動選別基準（強化法22条2項（後述）で規定。IPアドレスと指令情報による基準。「外外通信選別条件設定基準」という）を定め、委員会の承認を受ける必要がある。

(3)委員会の承認

委員会は上記(2)で述べた承認の求めがあった場合において、その求めに理由があると認めるときは、遅滞なく承認をするものとされ、同委員会は措置の実施および取得情報の取扱いに関して、適当と認める条件を付すことができる（強化法18条）とされる。

2｜コメント

提言(6p - 7p)では、「多くが国外所在と考えられる攻撃用のインフラの実態把握が必要であることに鑑み、まず『外外通信』について」「通信の宛先や送受信に関する情報及び通信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など、コミュニケーションの本質ではないデータに注目する方法」による分析をできるようにしておく必要があるとする。

ここで対象とするのは外外通信であって、サイバー攻撃であると疑われ、実態把握が困難であると、被害防止が十分に図れないものである。世界中のサイバー攻撃情報（送信元情報・指令情報）の収集・分析は、被害防止に不可欠である。

ただ、世界中と言っても国内事業者が関与しないと収集は困難であることから、国内の電気通信事業者が媒介するものに限定されている。そして、上記の外内通信における当事者協定と異なるのは、

送受信者ともに国外に所在するため、通信の当事者の同意を得ることができないことである。この点、外外通信目的送信措置では、委員会の承認を得ることとし、行政の恣意的な運用の防止策としている。

5――取得情報の取扱い

1｜対象となる不正行為

強化法 21 条が定める「対象不正行為」とは、①内閣総理大臣が当事者協定に基づき取得した外内通信情報（上記 3 の 2 の(1)）については、重要電子計算機にかかる国外通信特定不正行為（上記 2 の 2 の(7)）および協定当事者が使用する電子計算機にかかる特定不正行為（上記 2 の 2 の(4)）を言い、また②内閣総理大臣が外外通信目的送信措置（上記 4）によって取得した通信情報については、18 条の承認（上記 4 の(3)）に係る国外通信特定不正行為を言う。後述 5 の 2 の通り、取得した通信情報のうち「対象不正行為」にかかる情報のみを自動選別にかけて記録することなる。

2｜自動選別の実施

内閣総理大臣は当事者協定に基づき取得した通信情報と、外外通信目的送信措置により取得した通信情報について、他人により知覚されない自動的な方法で以下の要件を満たす機械的情報（上記 2 の 2 の(8)）のみを選別（「自動選別」という）して記録することが求められる（強化法 22 条 1 項、図表 8）。

【図表 8】自動選別（イメージ）

つまり内閣総理大臣は未加工の情報を受領するが、通信情報の内容に踏み込まない範囲まで削ったうえで記録することが求められる。これは、憲法 21 条 2 項に基づく通信の秘密の保護を目的として設けられた規定である。

本項でいう要件とは、①当事者協定によって取得した通信情報は外内通信によるものであること、または②外外通信目的送信措置によって取得した通信情報は、外外通信によって送受信が行われたものであることのいずれかであり、かつ③取得通信情報に係る対象不正行為（上記 5 の 1）に関係があると認められるものであること、である（強化法 21 条 1 項各号）。ここで、③の認定にあたっては、ⅰ）対象不正行為に関係すると認められる送信元の IP アドレス、ⅱ）対象不正行為の実施に用いられるものと認められる指令情報、ⅲ）その他対象不正行為の探索が容易になると認められる情報、のうち、二つ以上を理由とするものでなければならない（強化法 22 条 2 項）。

自動選別終了後、選別された情報以外のすべてを消去する（強化法 22 条 3 項）。

3｜利用及び提供の制限

内閣総理大臣は自動選別前の情報を国外通信特定不正行為による被害防止目的（「特定被害防止目的」という）以外では利用・提供してはならず（強化法 23 条 1 項）、後述する限られた場合を除き、自動選別後の通信情報（「選別後通信情報」という）を利用・提供してはならない（強化法 23 条 2 項・3 項）。

内閣総理大臣が利用・提供できるのは以下の通りである（強化法 23 条 4 項）。

①当事者協定によって取得した選別後通信情報について、当事者の同意を得て利用・提供する場合
②防衛大臣等その他の行政の長に協力を要請した場合において選別後通信情報を提供する場合、および選別後通信情報を保護する十分な措置を講じている外国政府・国際機関に提供する場合
③委員会に対して強化法の定める承認を求める場合
④委員会による検査の場合および資料提出要求・実地調査の場合

内閣総理大臣は、電子メールアドレスのドメイン名（@の右側）以外の、個人を識別できる可能性の高い情報について、特定の記述を変換するなどして個人識別ができないようにする措置（「非識別化措置」という）を講じなければならない（強化法 24 条 1 項）[10]。

4｜その他の重要な規定

内閣総理大臣は選別後通信情報の分析を行うために必要があるときは、防衛大臣その他の行政機関の長に対して、専門的知識を有する職員による技術援助、自動選別等の実施に用いる電子計算機の貸与その他の必要な協力を要請することができる（強化法 27 条 1 項）。この場合、内閣総理大臣はこれらの行政機関に対して選別後通信情報を提供することができる（同条 3 項）。

次の行政機関の長が特定被害防止目的（上記 5 の 3）達成のため必要があると認めるときは、それぞれ各号に定める行政機関に対して選別後通信情報を提供することができる（強化法 31 条 1 項）。

一　国家公安委員会⇒警察庁
二　警察庁⇒国家公安委員会または都道府県警察
三　都道府県公安委員会⇒都道府県警察
四　都道府県警察⇒警察庁または都道府県公安委員会

また、次の行政機関の長が特定被害防止目的（上記 5 の 3）達成のため必要があると認めるときは、警職法（本改正で定められるサイバー危害防止措置執行官に関する規定。自衛隊法で準用する場合を含む）の処置に関する事務の必要な範囲内で、それぞれ各号に定める行政機関に対して選別後通信情報を提供することができる（強化法 31 条 2 項）。

一　警察庁⇒委員会（上記 4 の(2)）または防衛省
二　防衛省⇒委員会または警察庁
三　都道府県警察⇒委員会

[10] なお、特に必要があると認められるときは、特定記述を復元するなど個人が識別できるようにする措置（「再識別化措置」という）を講ずることができる。

5｜コメント

ここでは当事者協定および外外通信目的送信措置によって内閣総理大臣が取得した通信情報の取扱いについて規定している。上述(3 及び 4)の通り、当事者協定による外内通信情報はサイバー攻撃かどうかを問わず一律に、外外通信目的送信措置では、実態不明で被害防止のため実態把握の必要があるものについて情報収集を行うこととされている。

強化法ではこれら情報のうち、送信元情報や指令情報に照らしてサイバー攻撃と認められるものだけ自動選別にかける。自動選別にかけられなかった取得通信情報および自動選別ではじかれた取得通信情報の中身については削除される。残った記録においてもメールアドレスのドメイン名以外の個人情報に該当しかねない部分について非識別化措置をとることとされる。

さらに選別後通信情報の利用方法も限定され、かつ行政機関への提供および行政機関間の提供も法定の範囲内に限定されている。このように取得通信情報の取扱いは、通信の秘密に配慮しつつ、サイバー攻撃への的確な対応を可能とする枠組みでとされている。

6――特定外内通信目的送信措置・特定内外通信目的送信措置

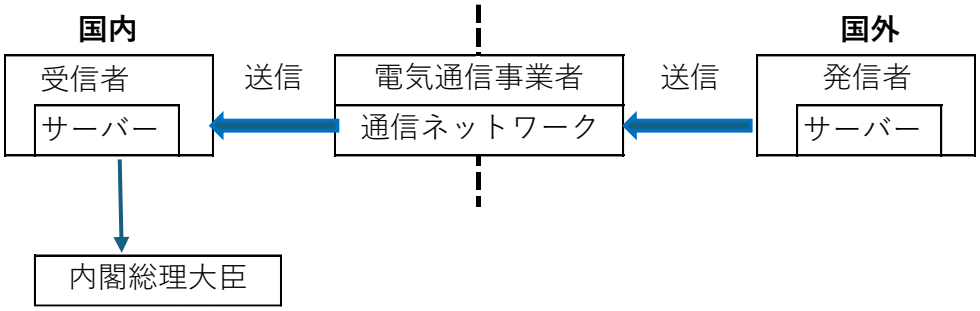
1｜特定外内通信目的送信措置・特定内外通信目的送信措置

(1) 特定外内通信目的送信措置

外内通信情報は上記 3 の 2 の通り、当事者協定で事業者や電気通信事業者との協定を通じて、通信情報を取得される。これに加えて強化法では、上記 4 で述べた外外通信目的送信措置と同様の措置を外内通信目的送信措置としてとることができるとする。

具体的には、内閣総理大臣は、サイバー攻撃を行っていると疑うに足りる状況のある特定の国外設備を送信元とするか、あるいはサイバー攻撃を行っていると疑うに足りる機械的情報が含まれている外内通信情報（あわせて「特定外内通信」という）の分析をしなければ、重要電子計算機の被害を防止することが著しく困難であり、本条の定める措置以外では分析が著しく困難であるときは、委員会（上記 4 の（2））の承認を受けて、特定外内通信を複製し、受信用設備に送信される措置を取ることができる（強化法 32 条、図表 9）。

【図表 9】特定外内通信目的送信措置（イメージ）

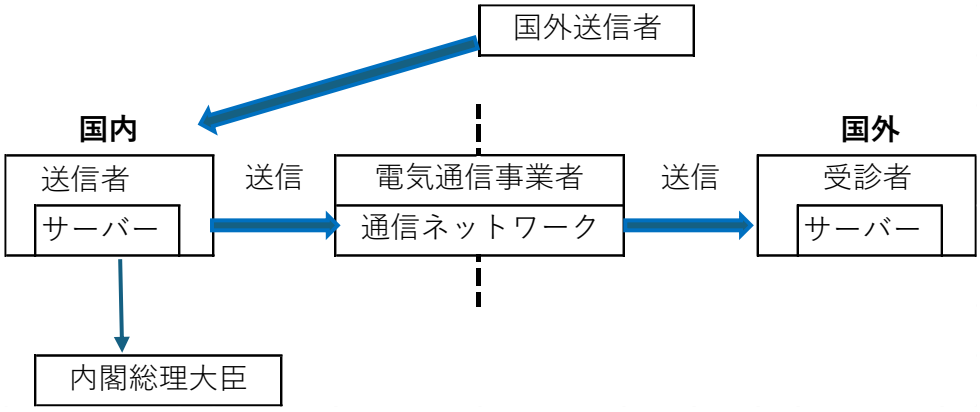


(2) 特定内外通信目的送信措置

内外通信については、当事者協定の範囲外であり、本条(強化法 33 条)により情報を取得するルート

以外はない。強化法では内外通信を定義し、IP アドレスから判断して国内設備から国外設備に送信されると認められる電気通信をいうとしている。ただし、この内外通信は、①国外通信特定不正行為に用いられていると疑うに足る状況にある国外設備を転送元のもともとの発信元としているか、あるいは②その国外通信特定不正行為に用いられていると疑うに足りる状況のある機械的情報が含まれているものに限定されている(「特定内外通信」という)。つまり単純に日本が発信元というのではなく、元の通信情報が海外から来たものという制限がかかっている（図表 10)。

【図表 10】特定内外通信目的送信措置



そして本条では、特定内外通信の分析をしなければ、重要電子計算機への被害を防止することが著しく困難であり、かつ本条に定める措置以外では分析が著しく困難であるときに、委員会の承認を受けて、国外にある電気通信設備によって媒介される国外関係通信媒介中通信情報が複製され、受信用設備に送信されるようにするための措置を講ずることができるとする（強化法 33 条)。

すなわち、国外からサイバー攻撃の「踏み台」として国内の設備が利用されている場合に、それを阻止することに主眼がある。

2｜特定外内通信目的送信措置・特定内外通信目的送信措置による取得通信情報の取扱い

特定外内通信目的送信措置・特定内外通信目的送信措置による取得通信情報に関する「対象不正行為」とは、いずれも国外通信特定不正行為（上記 2 の 2 の(7)）を指す。つまり国外が発信元であるサイバー攻撃に限定されている。

取得通信情報については、外内通信情報等と同様に自動選別を行わなければならない（強化法 35 条)。上記 5 の 2 と同様の規定が置かれている。

3｜コメント

強化法の建付けとしては、外内通信に関して、受信者の同意を得る当事者協定が本則とされている。しかし、強化法の定める要件において、他に手段がないときに内閣総理大臣は受信者から情報を一方的に取得する措置をとることができるとされた。受信者の同意を得ない代わりに、委員会の承認が要求されている。

他方、内外通信に関しては、ここで定める通信目的送信措置が唯一の手段である。ただし、内外通

信と言っても、条文にある通り、国外からの送信をきっかけに国内から送信されるものに限定されている。国内の送信者は悪意ある主体ではないことを前提としていると考えられる。いわゆる「踏み台」となった送信者も含むであろう。内外通信目的送信措置に関しても、国内の送信者の同意を得ないことから、委員会の承認が求められている。

7――強化法におけるその他の重要項目

1｜内容

(1)総合整理分析情報の提供等

内閣総理大臣は強化法に基づき受領した情報および選別後通信情報は被害防止を目的とした有効利用のため整理分析を行うものとされる（強化法 37 条）。この整理分析結果（「総合整理分析情報」という）は行政機関（強化法 38 条）、外国の政府等（強化法 39 条）、特別社会基盤事業者（強化法 40 条）に提供することができる。また内閣総理大臣が必要と認めるときには、重要電子計算機を使用する者等に対して「周知等用総合整理分析情報」を提供し、あるいは公表できる（強化法 41 条）。

また、総合整理分析情報に基づいて電子計算機あるいはプログラムの脆弱性を認知したときは、電子計算機の供給者等に情報提供し、あるいは公表することができる（強化法 42 条）。

(2)協議会

内閣総理大臣は、内閣総理大臣および関係行政機関の長により構成される重要電子計算機に対する特定不正行為（上記 2 の 2 の(4)）による被害の防止のための情報共有及び対策に関する協議会（「協議会」という）を組織する(強化法 45 条 1 項)。協議会には重要電子計算機の利用者、電子計算機等供給者その他の内閣総理大臣が認める者を構成員とすることができる(強化法 45 条 2 項)。

(3)サイバー通信情報監理委員会(委員会)

内閣府にサイバー通信情報監理委員会（委員会）を置くこととされる(強化法 46 条)。委員会の主な権限として、外外通信目的送信措置をとるときの承認（強化法 17 条。上記 4 の(2)）、特定外内通信目的送信措置をとるときの承認（強化法 32 条。上記 5 の 1 の(1)）、特定内外通信目的送信措置をとるときの承認（強化法 33 条、上記 5 の 1 の(2)）、サイバー危害防止措置執行官が危害防止のための措置を取るときの承認（警察官職務執行法（以下、「警職法」）6 条の 2 第 4 項）、治安出動を命ぜられた自衛隊の通信保護措置を講ずる時の承認（自衛隊法 89 条 1 項で準用する警職法 6 条の 2 第 4 項）といった権限がある。また内閣総理大臣の行う自動選別・記録措置、非識別化措置、再識別化措置に関する検査権(強化法 63 条 1 項)、そのほか通信情報保有期間における取得通信情報の取扱いに関する検査権（強化法 63 条 2 項）がある（強化法 48 条）。

委員長を含む委員は 4 名で組織され、ⅰ）裁判官であったものなど法律の専門家、ⅱ）サイバーセキュリティまたは情報通信技術に関して専門知識・経験ならびに高い識見を有する者で構成される。

2｜コメント

強化法において、政府が特別社会基盤事業者等に提供するサイバー攻撃に関する情報は「総合整理分析情報」とされており、重要電子計算機を使用する者等を含め広めに情報提供するときには「周知

用総合整理分析情報」を提供することとされている。提言(2p)では、サイバー攻撃に関する「情報は広く、一般的に注意喚起されるべき性質のものである」一方で、「政府のインテリジェンス情報や企業秘密に関わるものも存在する」とする。したがって情報のうち「特に漏洩により我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティクリアランス[11]制度を活用する等適切な情報管理と情報共有を両立する仕組みを構築すべき」とされている。総合整理分析情報の提供先が限定されている背景にはこのような考えが存在する。

また、提言(3p)では、強化法で新たな情報共有枠組みを設けることとされ、これが上述の協議会である。

さらに委員会の設置は政府に対して情報提供を求める際に、通信の秘密との整合性を図る鍵となる組織体であり、提言(8p)において、「実体的な規律とそれを遵守するための組織・手続き的な仕組みづくりが必要」とされる部分に対応するものである。さらに委員会に関連して、提言（9p）では「電気通信事業者の設備から政府への情報通信の送出の適正性が確保され、同時に協力する電気通信事業者の直面しうるリスクの軽減につながりうるような監督のあり方を含め、独立機関などのガバナンスの仕組みを十分考えていくべき」としている。

8――警察官職務執行法・自衛隊法

1｜警察官職務執行法

警察庁長官は必要な知識・能力を有すると認められる者をサイバー危害防止措置執行官（以下、「執行官」）として指名する（警職法 6 条の 2 第 1 項）。

執行官のとることのできる措置は警職法 6 条の 2 に規定がある。それは以下の通りである。

（発動要件）

・情報技術を用いた不正行為（「情報技術利用不正行為」という）に用いられる電気通信、もしくはその疑いがある電気通信（あわせて「加害関係電気通信」という）、または情報技術利用不正行為に用いられる電磁的記録（「加害関係電磁的記録」という）を認めた場合であって、

・これを放置すれば人の生命、身体又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

（対象）

・加害関係電気通信の送信元若しくは送信先である電子計算機、又は加害関係電磁的記録が記録された電子計算機（総称して「加害関係電子計算機」という）の管理者その他関係者に対し、

（措置）

・加害関係電子計算機に記録されている加害関係電磁的記録の消去その他の危害防止のため通常必要と認められる措置であって、

・電気通信回線を介して行う加害電子計算機の動作にかかるものをとることを命じ、又は、自らその

[11] セキュリティクリアランスとは漏洩すると日本の安全保障に支障を来すおそれがある国の情報を指定し、民間も含めて国が信頼性を確認した人に限ってアクセスできるようにする制度である。
https://www3.nhk.or.jp/news/html/20250516/k10014806811000.html

措置をとることができる（ここまで2項）。

（国外の加害関係電子計算機）

・加害関係電子計算機が国内にあると認める相当な理由がない場合には、サイバー危害防止措置執行官に限り、2項の措置をとることができる。この場合、外務大臣と協議しなければならない（3項）。

（委員会の承認）

・2項の措置をとる場合にはあらかじめ委員会の承認を得なければならない（4項）。ただし、危害の防止のために委員会の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この限りではない（4項但書）。

・4 項但書に基づいて、委員会の承認を得なかった場合には、とった措置について速やかに委員会に通知する（9項）。

・9 項に基づく通知を受けた委員会は必要があるときは、処置事務の適正な実施を確保するために、必要な措置を命ずることができる（10項）。

2｜自衛隊法

自衛隊法83条の3に基づいて、内閣総理大臣は自衛隊に対して通信防護措置（後述）をとるべき旨を命ずることができる。具体的には以下の通りである。

（発動要件）

・重要電子計算機に対する特定不正行為（強化法2条4項。上記2の2の（4））であって

・本邦外にある者による特に高度で組織的かつ計画的な行為と認められるものが行われた場合において、

・重要電子計算機に特定重大支障（重要電子計算機の機能が停止・低下し、容易に回復できない支障が生じ、これによって国家及び国民の安全を著しく損なう事態が生ずるもの）が生ずるおそれが大きいと認められ、特定重大支障の発生を防止するために自衛隊が有する特別の技術又は情報が必要不可欠であり、かつ国家公安委員会からの要請又はその同意があることにより自衛隊が対処を行う特別の必要があると認められるとき、

（措置）

・部隊等が特定不正行為による重要電子計算機への被害を防止するために必要な電子計算機の動作に係る措置であって

・電気通信回線を介して行うもの（「通信防護措置」という）をとるべき旨を命ずることができる（ここまで1項）。

（重要電子計算機に関する限定）

・重要電子計算機は強化法2条2項（上記2の2の(2)）に定めるものだが、3号（その他重要情報を保有する事業者が使用する電子計算機）については、防衛生産基盤強化法に定める一定のものという限定が付されている（2項）。

（措置の実施）

・部隊等は警察庁又は都道府県警察と共同して通信防御措置を実施する（3項）。

（協議）

・通信防御措置を命ずる場合には、あらかじめ、防衛大臣と国家公安委員会との間で協議をし、対象となる重要電子計算機や措置内容等について定める(4 項)。

3｜コメント

本項で述べた警職法、自衛隊法の規定は、サイバー攻撃に関する被害防止のための措置を警察及び自衛隊にも認めるものである。

提言(10p)では、、「武力攻撃事態に至らない状況下において、重大なサイバー攻撃による被害の未然防止・拡大防止を目的とした、攻撃者サーバー等へのアクセス・無害化を行う権限を政府に付与することは必要不可欠」であるとする。そして、「新たな制度の目的が、被害の未然防止・拡大防止であることを踏まえると、インシデントが起こってから令状を取得し、捜査を行う刑事手続では十全な対処ができないと考えられ、新たな権限執行には、緊急性を意識し、事象や状況の変化に臨機応変に対処可能な制度とする必要がある」とする。そして、警察と自衛隊とがそれぞれ警職法・自衛隊法の定める要件のもと権限を行使するにあたっては、「武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度の構築が必要」とする提言(11p)の趣旨に沿うものである必要がある。

また、警察・自衛隊の権限が海外に及ぶ点について、提言(12p)では、「他国の主権侵害に当たり得るものである場合であっても、国際法上の違法性が阻却される場合がある。 その違法性阻却事由として」は、「『緊急状態（Necessity)』（中略）が援用しやすいものと考えられる」とする。ここで緊急事態とは「当該措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、当該行為が相手国又は国際共同体の不可欠の利益を深刻に侵害せず、状態の発生に寄与していない場合に違法性阻却が認められるという考え方」とする。

ここでいう緊急状態は民法・刑法でいう緊急避難に類似した考え方で、人身事故を避けるために不可欠な行動として物品を破壊したような場合に、犯罪や不法行為の違法性が阻却される場合を指す。

9――おわりに

外国から国内に行われるというサイバー攻撃の特殊性があるため、警察及び自衛隊の権限行使が外国に及ぶことが定められているが、その国際法上の合法性が問題となる。

国会でもこの点についての質問がなされ、参考人の証言によれば、武力行使が緊急状態（緊急避難）で合法化できるかどうかは説が分かれているとのことである。そして強化法が定めるのは武力行使に至らない域外のアクセス・無害化措置であるとし、この場合であれば緊急状態で認められるとの説明があった[12]。

ここでは警察につき考えるとすると、これまでは国際捜査共助[13]によらない国外にあるサーバーに対する捜索差押さえであっても、捜索差押許可状に基づくものであれば、開示権限者の明確な同意に

[12] 衆議院内閣委員会令和 7 年 3 月 28 日議事黒崎参考人発言
[13] 日本が 2012 年に加入したサイバー犯罪条約によるもの。同条約では①データがオープンアクセスに供されている場合、および②データの開示権限を持つ者の合法的かつ任意の同意が得られる場合に捜査機関のリモートアクセスが認められるとしている。

よらなくとも違法とは言えない（最高裁決定令和３年２月１日）という判例があった。この最高裁決定では「条約に拠らないリモートアクセスが果たして主権侵害にあたるのか、主権侵害にあたらないとすればそれはどのような場合かを明確にする必要がなお残されている[14]」との評価がある。

強化法は少なくとも国内において、主権侵害にあたらない場合を明確にしたと言える。もっとも強化法が国際法的にみて他国の執行管轄権を侵害するかどうかは、他国の司法権の判断するところによる。

強化法では単なる捜索差押だけではなく、措置をとることまで認めている。この点、国会答弁からは、自制的な権限行使こそが国際的に認められるために必要であり、かつそのことを認知されるよう国際的に説明していくことが重要としている。

したがって、本法の施行にあたっては、今後も実務における運用状況の検証および国際社会との協調が重要である。国民への周知や透明性確保にも留意すべきであろう。

[14] 竹内真理「リモートアクセス操作と国家主権」ジュリスト 1570 号(2022 年 4 月) p 248 参照。