2025/4/12
京都弁護士会　市民集会
攻撃は最大の防御?

能動的サイバー防御法案は、ネット監視・サイバー先制攻撃法案だ!

海渡　雄一

（弁護士　日弁連共謀罪・秘密保護法対策本部副本部長、秘密保護法対策弁護団共同代表、経済安保法に異議ありキャンペーン）

国会内で開かれた能動的サイバー防御法案を考える市民と超党派議員の勉強会。右は講師の海渡雄一弁護士＝東京・永田町で（佐藤哲紀撮影）

2.13 市民と超党派国会議員との勉強会
政府はタリンマニュアル2.0と
ドイツ連邦憲法裁判所2024年10月8日決定
をまともに検討したのか?

今日のお話

- 第1　はじめに　衆院審議のまとめと総括
- 第2　能動的サイバー防御法案によって、収集される情報はどのようなものか＝ドイツ憲法裁判所の論点ごとの判断と比較して＝
- 第3　サイバー通信情報監理委員会によってプライバシーは守れるか?
- 第4　人が分析しなければ、人権侵害が起きないのか?本当に人は不正でない仕組みなのか?
- 第6　大川原化工機冤罪事件・岐阜大垣署国家賠償請求事件名古屋高裁判決が示す公安警察組織の法遵守への根本的疑問
- 第6　サイバー攻撃と国際法　タリン・マニュアル2.0とは何か?
- 第7　無害化措置は、憲法違反の先制攻撃である。＝火遊びのような法案をつくれば大火事になりうる＝
- 第8　まとめ　2025年通常国会、能動的サイバー防御に関する法案の成立を食い止めよう

第1　はじめに　衆院審議のまとめと総括

- 政府は2022年末に改定した国家安全保障戦略で、サイバー脅威に対し「対応能力を欧米主要国と同等以上に向上させる」とした。
- サイバー空間を平時から監視し、不審な通信やサーバーを検知する、さらに重要インフラなどを狙った重大なサイバー攻撃の危険性が高い場合は、未然に攻撃者のサーバーに侵入して、マルウエアを送り込んで無害化する「能動的サイバー防御（ACD）」制度を導入するとしている。
- 政府は2024年6月7日から、このようなサイバー攻撃を未然に防ぐための「能動的サイバー防御（ACD）」制度の導入に向けた有識者会議会合を開催し、令和６年11月29日付で「サイバー安全保障分野での対応能力の向上に向けた提言」(以下「提言」と略称する)が政府に提出された。

2.7 能動的サイバー防御法案 国会提出

- 2月7日、政府は「能動的サイバー防御」を導入するための2法案を閣議決定した。
- 一つが、「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案」(サイバー被害防止法案 以下「A法案」という)、もう一つが、「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の施行に伴う関係法律の整備に関する法律案」(アクセス無害化実施法案　以下「B法案」という)である。
- 　A法案は、サイバー攻撃などによる被害の防止のための基本的な方針の策定、インフラ事業者などにサイバー攻撃を受けたことの政府への報告を義務付けること、サイバー攻撃防止のために通信情報を取得すること、通信情報の取扱いについて「サイバー通信情報監理委員会」による審査、検査について定めること、通信情報等を分析した結果の政府機関、事業者、外国政府への提供等について定めた新法である。一言でいえば、インターネット常時監視法案といえる。
- 　B法案はサイバー攻撃による重大な危害を防止するため、一定の警察官又は自衛官による無害化措置＝先制的なサイバー攻撃の根拠規定を整備し、サイバーセキュリティ基本法、警職法、自衛隊法などの関係法の改正を行う法律であり、一言でいえば、サイバー版先制攻撃法案である。

衆議院内閣委員会等における審議経過

3月19日　法案趣旨説明　審議

3月21日　審議

3月26日　審議

3月28日　参考人招致

①高見沢将林（のぶしげ）（与党推薦：軍縮会議日本政府代表部大使、元防衛省防衛政策局長）/②吉岡克成（与党推薦：横浜国大教授、情報通信専門）/③黒崎将広（立民党推薦：防衛大学校教授）/④大沢淳（？推薦：中曽根康弘世界平和研究所主任研究員）

4月2日　審議

4月3日　内閣委員会･総務委員会･安全保障委員会･連合審査会

4月4日　審議採決

4月8日　衆議院本会議採決

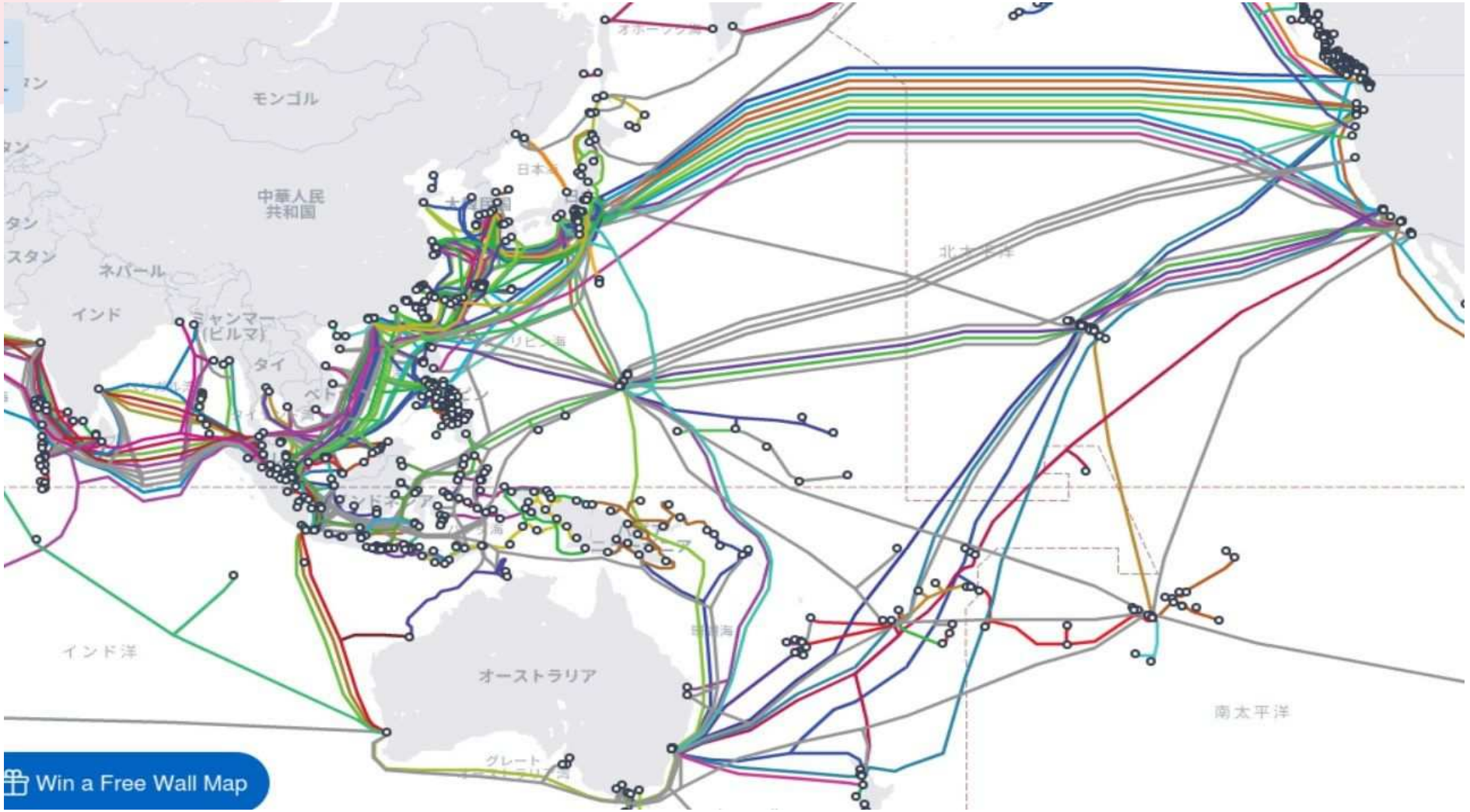
能動的サイバー防御2法案は衆院を通過へ

・　能動的サイバー防御法案は、日本国民全体のプライバシーの存立にかかわる重大な人権侵害の問われる法案である。それだけでなく、日本発の熱戦を引き起こしかねないほど、深刻な問題をはらんでいる。この問題をわかりやすく説明するためにこのQAを作成した。これは、衆院で法案が可決されようとしている段階で作成したものである。

・　4月4日午後、能動的サイバー防御法案＝ネット監視・サイバー先制攻撃二法案(A・B法案)が内閣委員会で可決された。衆院本会議でも8日の衆院本会議で採決された。

・　A法案に国会の監視機能強化、通信の秘密の尊重、三年後の見直しの三本柱とする修正案を、自民と立憲民主党を中心に、公明党、日本維新の会、国民民主党、「有志の会」などが共同提出し、この修正案が賛成多数で可決された。B法案は無修正で委員会で可決された。

日本はインターネット海底ケーブルのハブ



衆院可決の翌日の各紙


サイバー安保 危機感共有
関連法案が衆院通過 立維国賛成
基幹インフラ 国が通信監視
AI推進 国が司令塔に
IT企業の責務明示
サイバー防御法案成立へ
脆弱性修正 要請可能に
課題なお
不正閲覧 「技術的に可能」
1876円高 買い戻し

政府によるネット監視がもたらすのは、市民の沈黙・内部告発の不全

・膨大な情報を政府の中枢に吸い上げる大量監視を合法化する法案

ネット監視法案(A法案)は、サイバー攻撃防止のために事業者と締結した協定、あるいは同意なくして通信情報を取得するための法案である。政府は、収集対象となるのは海外通信に限られ、国内で完結する通信は対象としていないとする。基幹インフラ事業者や一般の通信事業者との協定に基づく通信情報の取得には、何の限定もない。情報収集は必要最低限度にとどめるという原則規定も法案にはない。

・国内通信は収集から除かれるという説明はミスリーディング

スノーデン氏が告発したアメリカのネット監視システムも、法制度上は外国通信だけを監視するとされていたが、情報機関は制約を無視して行動していた。

参考となるのが昨年10月ドイツの連邦憲法裁判所が下した判決だ。この判決は海外に関わる情報の監視のためには、国内の通信情報も含めて取得することになるが、データ削除の規定がない点を違憲判断の理由の一つとしている。政府は、ドイツは属人主義をとっているが、日本では属地主義を採用しており、問題はクリアーしているとする。この通りだとすると、国内の通信でも海外のサーバーを経由しただけで、収集の対象とされることとなり、むしろ問題はドイツより深刻だといえる。

・ネット監視は政府批判を沈黙させる

・これまで国内のネット監視は通信傍受法が根拠とされ、裁判所の令状を受ける必要があった。しかし、今回の制度では、どんな情報が政府に集められているかは、最後まで市民には明らかにされない。常に誰かに見られているという可能性があるだけで、市民は政府批判もためらい、秘密裡に公益通報することも不可能になる。人権と民主主義が、危機に瀕することとなる。

サイバー先制攻撃が、本物の戦争の引き金になる可能性がある

サイバー空間における先制攻撃が可能に

サイバー先制攻撃法案は、サイバー攻撃による重大な危害を防止するため、警察官又は自衛官によって無害化措置＝先制的なサイバー攻撃の根拠規定として、警職法と自衛隊法などを整備する。サイバー攻撃への対処には、サーバー管理者に機能停止（テイクダウン）を依頼することや、攻撃者を公表し非難するなど、他にも手段がある。ところが、B法案は、私人が行えば、不正アクセス、電磁ウィルス使用などの罪に問われる違法な行動を、警察機関や自衛隊の手で、敢行しようとしている。憲法9条に反する先制攻撃になりうる。

法案はサイバー攻撃に関する国際基準タリンマニュアルの要請を満たしていない

法案は、「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」には警察が、海外からの特に高度に組織的かつ計画的な行為が行われた場合は、自衛隊が対処する（2,4条）。しかし、サイバー攻撃に関する国際規範であるタリンマニュアルでは、「（国の）根本的な利益に対する重大で差し迫った危険」「利益を守る唯一の手段である場合」を要件とし（規則26）、「侵害の切迫性」も求められている（規則73）。しかし、法案では、個人や企業の利益を守るために海外のサーバーへの攻撃ができる。

攻撃が報復を招き、熱戦に発展する可能性は否定できない

サイバー攻撃は、正体を隠して行われる。偽情報に釣られて、攻撃対象を間違える可能性は高い。攻撃を行えば、報復が報復を呼び、偶発的にミサイル攻撃から現実の戦争へと発展する可能性も否定できない。サイバー空間においても、国際法、紛争の平和的解決の考えに沿って、サイバー攻撃を国際社会が一致して非難し、深刻化を未然に防ぐ外交関係が求められている。「気がついたら開戦」となってからでは遅いのだ。

これが修正案だ!

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案に対する修正案

〇通信の秘密の尊重(77条の2)

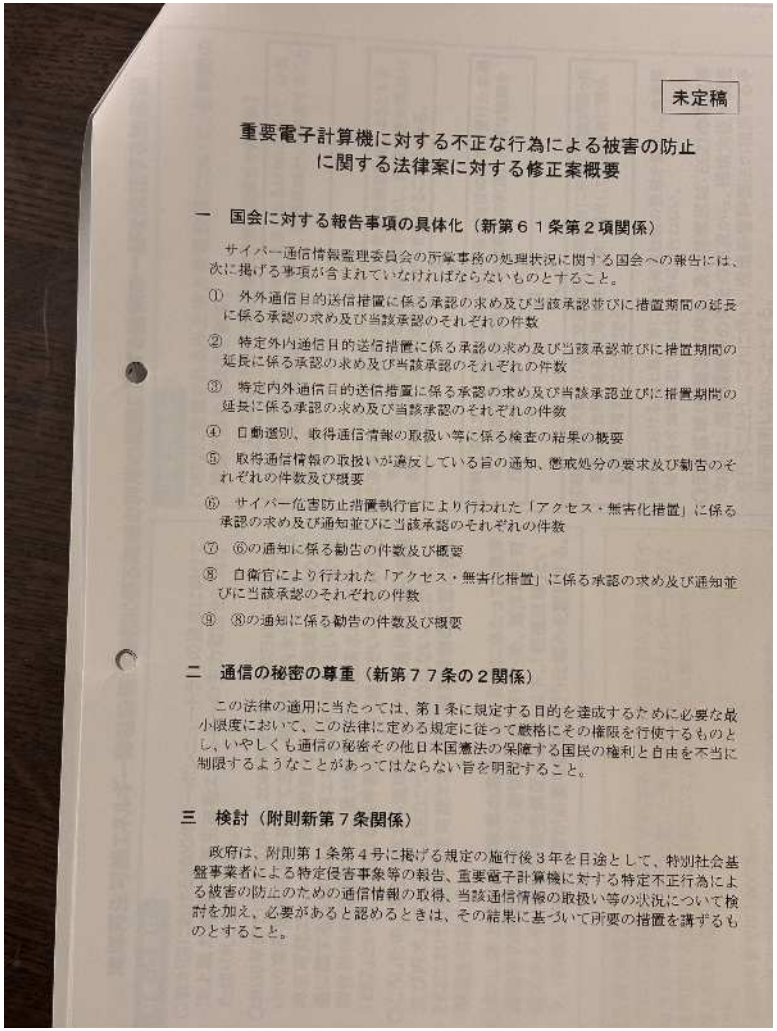
この法律の適用に当たっては第一条に規定する目的を達成するために必要な最小限度において、この法律に定める規定に従って厳格にその権限を行使するものとし、いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない

〇国会に対する報告事項の具体化(61条2項)

前項の報告には、次の各号に掲げる事項が含まれていなければならない(詳細は写真に譲る)

〇附則に次の一条を加える

検討□第七条政府は、附則第一条第四号に掲げる規定の施行後三年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。



未定稿

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案に対する修正案概要

一　国会に対する報告事項の具体化（新第６１条第２項関係）

サイバー通信情報監理委員会の所掌事務の処理状況に関する国会への報告には、次に掲げる事項が含まれていなければならないものとすること。

① 外外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

② 特定外内通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

③ 特定内外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

④ 自動選別、取得通信情報の取扱い等に係る検査の結果の概要

⑤ 取得通信情報の取扱いが違反している旨の通知、懲戒処分の要求及び勧告のそれぞれの件数及び概要

⑥ サイバー危害防止措置執行官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数

⑦ ⑥の通知に係る勧告の件数及び概要

⑧ 自衛官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数

⑨ ⑧の通知に係る勧告の件数及び概要

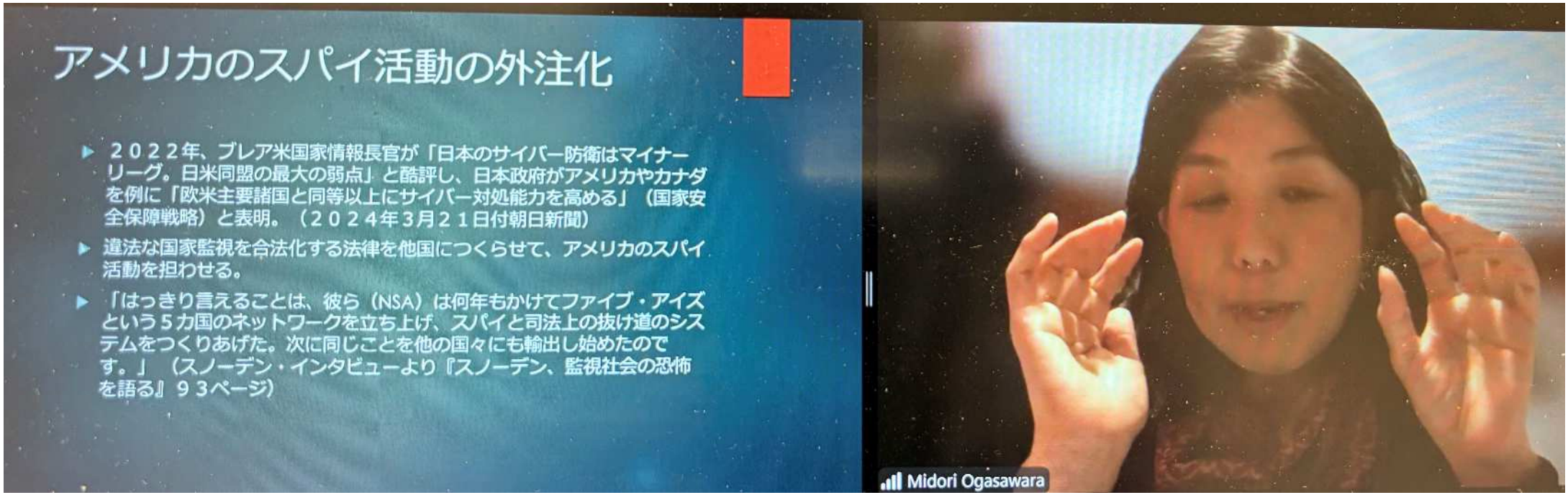
二　通信の秘密の尊重（新第７７条の２関係）

この法律の適用に当たっては、第１条に規定する目的を達成するために必要な最小限度において、この法律に定める規定に従って厳格にその権限を行使するものとし、いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない旨を明記すること。

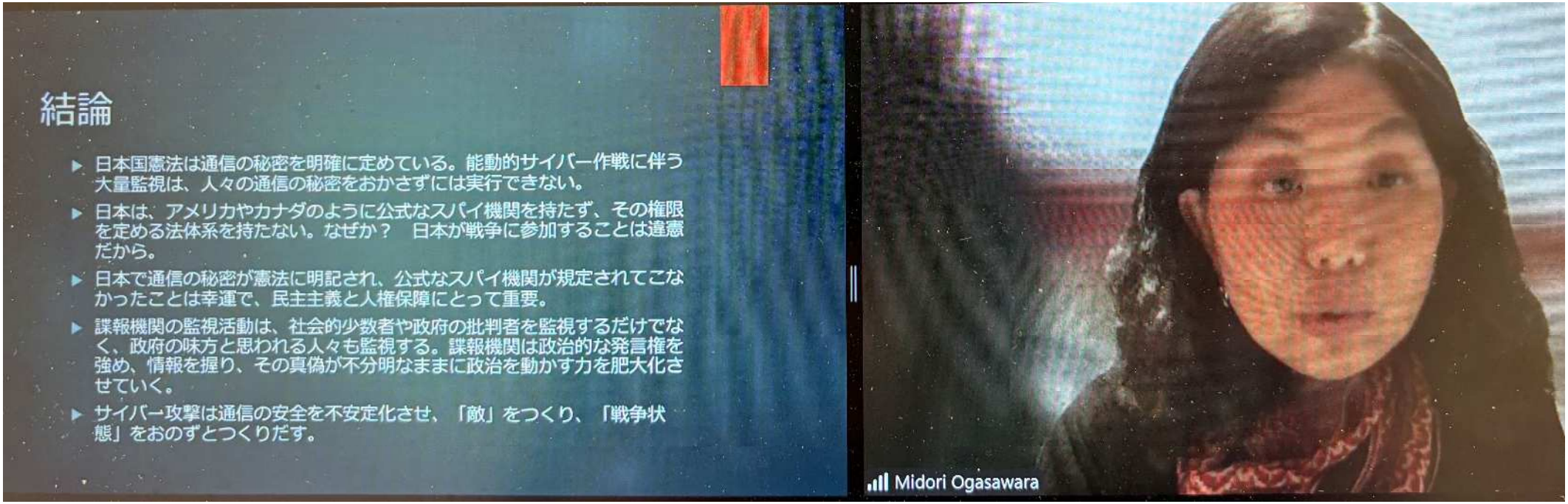
三　検討（附則新第７条関係）

政府は、附則第１条第４号に掲げる規定の施行後３年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとすること。

4.11院内緊急抗議集会
カナダからオンラインで報告したくれた小笠原みどりさん
この法案は、アメリカのスパイ活動の外注化なのだ！



・諜報機関による監視は与党政治家にまで及ぶ。
・サイバー攻撃は通信の安全を不安定化させ、「敵」を作り、「戦争状態」をおのずと作り出す。



我々は、参議院においても、この2法案の成立に反対し、闘い続ける。

- 政府は、技術的にはメールの中身まで見ることは可能と答弁した。
- 大川原化工機事件、岐阜県警大垣署国賠請求事件など、公安警察の違法捜査を断罪する判決が続いている。
- 設けられる第三者機関が、公安警察の違法な行為を効果的に止められる保障はない。
- 衆院の最終盤で、立憲民主・自民間で合意した法案の修正案でも、明らかにされるのは無害化の件数だけ、過去の海外の例を見ても明らかなように、サイバー攻撃を行った事実そのものが、経緯と対象を含めて公表される保障はない。
- この修正案では明らかに不十分であり、我々は、参議院においてもこの二法案の成立に反対し、闘いを続ける。

第2　能動的サイバー防御法案によって、収集される情報はどのようなものか

カールスルーエにある
ドイツ連邦憲法裁判所

広汎な事業者との協定に基づく情報の収集が計画されている

- まず、広汎な情報があらゆる基幹インフラ15事業者、さらにその他の広範な通信事業者との当事者協定によって取得される仕組みがつくられる。
- 「国外関係電気通信事業者」に対して、情報提供、機器の接続などの協力を求めることができ、正当な理由がない限り拒否できないと定めています(20条)。
- 基幹インフラ15事業者だけでなく、一般の電気通信役務の利用者からも、内閣総理大臣との間で、「当事者協定」を締結し、情報の提供を受ける制度がつくられる(11,12条)。そして、法案では、外内通信に係る通信情報を用いて、分析を実施し、事業者等に必要な分析結果を提供するとしている(21-31条)。
- しかし、これらの協定に基づいて提供を受ける情報については、サイバー通信情報監理委員会の承認も必要がなく、情報の種類にも制限がない。

広汎なものとなりうる当事者協定に基づく通信情報の提供(2025/2/12政府による福島みずほ議員に対する説明)

・政府に対する通信情報の提供について「事業電気通信役務の利用者」とは、**通信サービスを利用している業者を指すので、かなり広範な企業等が該当し得る。**ただし、協定を締結することが「出来る」規定なので、企業側に政府との協議に応じたり、協定を結んだりする義務はない。

・**どのような情報をどのような頻度で提供するかは政府と提供者が結ぶ協定次第だが、提供者の中には通信の種類を自前で振り分けて提供するのが困難な者もおり、外内通信とそれ以外を振り分けることを義務付けるのも難しい。結果、内内通信も含めて提供されることもあり得るが、政府は「提供されるものは全部受け取り」、その後自動選別(新法第22条)をする。**

・**政府は提供者と協定を結ぶので、情報の取得に係る制限は定めていない。政府による内内通信の取得を禁止する規定もない。提供される情報は、アプリケーションを問わない。結果、メール、LINE、SNSの投稿等、全てが提供対象になる。**

・どのような手法で情報を提供するかも協定次第。「ミラーリング」といって、通信に関する情報のコピーをリアルタイムで政府に送ることも可能。ただ、攻撃の全容を解明し、予防策を作るためには、必ずしもリアルタイムの情報共有が必須という訳ではない。

・**特定社会基盤事業者には関東キー局がすべて入っているが、さすがに取材源の秘匿の必要性から、メールを提供することは出来ないと言っている。**

事業者の同意なく情報を収集できる仕組みも整備される

- 法案第17条は国外から国内の重要な電子計算機（サーバーなど）を標的にした不正行為を防ぐために、政府が一定の通信を監視・複製できるようにするとして、サイバー通信情報監理委員会の承認を得て、国外からの通信、国内から国外への通信を監視するとしている。
- ここでは、外国間、外国・国内間の通信情報について、サイバー通信情報監理委員会の事前承認を得て取得できるとしている。「「重要電子計算機」に対するサイバー攻撃に用いられていると疑うに足りる状況のある特定の国外設備を発信元とし」ている場合と、「サイバー攻撃に用いられていると疑うに足りる状況のある特定の情報」が含まれている場合であって、これを分析しなければ、分析が著しく困難である場合に、委員会の承認を得て取得できると定めている(32条、33条)。
- 政府は、国内通信は取得できないと説明している。しかし、国内の当事者間の通信も、そのほとんどが海外のサーバーを経由するとされる。政府の説明では、海外のサーバーを経由した情報は、国内通信と定義されず、収集の対象とされる。この点は、きちんと説明されておらず、政府の説明はミスリーディングだと言える。
- また、この規定では複製の上限が通信設備の伝送容量の30%と規定しているだけで、その範囲の基準も不明、根拠も不明である。

ドイツの連邦憲法裁判所2024年10月8日決定 サイバー脅威の検知のための政府の措置の一部に違憲の判断がなされた

- 原告は国内外の人権団体
- ドイツと外国の間の通信に関する監視（以下「戦略的内外通信偵察」）を理由とした通信の秘密の制限について規定するG10法第5条第1項第3文第8号の規定並びにこの権限の行使に関連するG10法及び連邦憲法擁護庁法 の規定を対象とし、2016年に、国内外の人権団体等が連邦憲法裁判所に対し違憲の訴えを申し立てた。
- この訴えに対し、連邦憲法裁判所は、申立人の訴えの一部を認容し、2024年10月8日に、次のような内容の決定を下した。
- 連邦憲法裁判所は、他国からのサイバー脅威を早期に検知することを重要な公共の利益として認めた一方で、G10法の規定には**①内内通信の取扱いに関する規定の不備、②在外外国人の通信における私的生活形成の核心領域に関連した規定の不備、③実施記録の消去期限、④審査機関の体制**の観点から問題があると指摘している。

サイバー脅威監視が違憲とされたポイント

- ①G10法第5条第1項第3文第8号は、監視対象を内外通信に限定しているものの、戦略的内外通信偵察の際に取得したデータには、国内間でのやり取りに関するデータが含まれる場合がある（実際には大部分を占める）。しかし、同法には、同時に取得された国内間の通信データの扱いに関する規定がない。
- ②同条第2項は、私的生活形成の核心領域に影響する検索語を用いた監視を禁じている。連邦憲法裁判所はこのような領域の監視は在外外国人に対しても許されないとして、当該通信を禁止対象に含めていない同法の規定を不十分であるとしている。
- ③戦略的内外通信偵察の実施に関する記録の消去期限は、一律、記録年の翌年末まで（同項第6文）とされているが、偵察による監視措置については、措置終了後対象者に通知されることになっているため、通知の時点でこの期限が過ぎていることもあり得る。対象者の権利侵害の救済の観点から、このような場合の想定を欠く規定は問題であるとしている。
- ④現状でも監視による権利侵害の有無を審査する組織として基本法第10条委員会が整備されているが、戦略的内外通信偵察を統制する組織としては不十分な点があるとしている。具体的には、その委員を専任の職とせず名誉職としている点や委員全員には法曹資格を要求していないことが挙げられている。

国内通信は見ない
という政府の説明は信用できるか?

- 外内通信は基幹インフラ事業者等との協定に基づき、外外通信と内外通信は独立機関「サイバー通信情報監理委員会（監理委）」の承認を受け通信情報を取得できるが、国内通信は取得できないとされている。
- しかし、国内の当事者間の通信のほとんどが海外のサーバーを経由するとされている。これは、国内通信と定義されないようであり、収集の対象となる。
- その場合にも、政府が集めた情報は、人間が関与しない「自動的な方法」で選別し、IPアドレスや送受信日時など「コミュニケーションの本質」でないデータだけを分析する。メールの本文や件名など「本質的」な内容は分析対象とせず、選別段階で直ちに消去するとされている。この説明が信用できるかが問題である。

政府は、内内情報は見ないというが、内内情報も集められている

- 問題は、政府の「見ない」という約束を信ずることができるかである。
- 米情報機関で勤務していたエドワード・スノーデンが、2013年に米国家安全保障局（NSA）がテロ対策として極秘に国内外のすべての情報を収集し、自由にこれを検索して関連情報を呼び出すことができた。このXkeyscoreシステムも、もともとは外国情報だけを、令状に基づいて収集するシステムだったことを忘れてはならない。
- それ以後、米国は表向き国内の通信の傍受は行わないことになっているが、それは表向きのことである。このことを踏まえて、「サイバー安全保障有識者会議」の答申では、国内通信は取得しないとしている。しかし、この約束は守られるのだろうか。
- 政府が約束を守っていることを確実に検証できる仕組みは存在しているのだろうか。

ドイツ連邦憲法裁決定「収集された国内通信の取り扱いが決められていないことは違憲である」

- 原則として、著しく重要な公共の利益が関係するため、国際電気通信の戦略的監視を行う権限は、結果として生じる干渉の重大性にもかかわらず、それらが比例して設計されている限り、基本法第10条1項と両立する。第10条法第5条第11頁第8号は、国際電気通信の戦略的監視の限界と構造に関する要件を完全には満たしていない。
- ドイツ国民またはドイツに所在する者のみが関与する国内通信から生じるデータの削除に関する十分に具体的で明確な規定が欠けている。第10条法第5条第I項第8号が監視を国際電気通信に限定していることは事実である。しかし、このような監視を行うと、必然的に国内の通信トラフィックからデータが収集されることになります。これはパケット交換通信の場合に当てはまり、実際には国際電気通信(インターネット経由で行われるすべての通信を含む)の最大のシェアを占めています。第10条法には、国内の電気通信から偶発的に収集されたデータの取り扱いに関する規則は含まれていません。

政府の説明によると日本法は属地主義をとっているため、ドイツの問題はクリアーしているというが。

- 政府は、「ドイツは内部・外部の定義が属人主義であったので憲法裁判所が指摘する問題が生じたが、日本の法案は属地主義をとっている。外国に位置するサーバーから日本に位置するサーバーに送られるものをがいない通信と定義し、実際どのような属性の人が通信を行っているかは問わない。ドイツの問題はクリアしている。」と説明した。
- しかし、この定義によれば、内内通信として取得から除外される範囲はかなり狭くなっているのではないか。

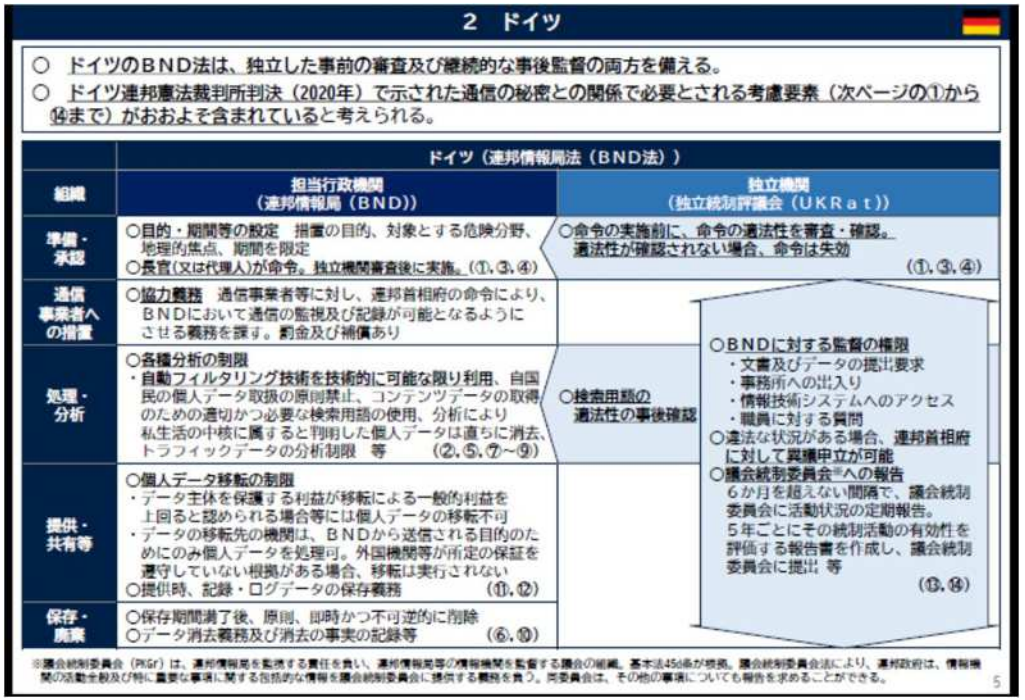
ドイツ連邦憲法裁決定「私生活の核心領域の保護が不十分である」

- 私生活の核心を保護する保護措置も同様に、十分には不十分である。私生活の核心の中での人格の自由な発達は、非常に個人的な性質の内面的な思考プロセス、反省、見解、経験を表現する可能性を包含しています。保護は、特に、監視が行われていないという合理的な期待のもとに行われる、最高水準の個人的信頼を享受している人々の間の非公開のコミュニケーションに与えられます。
- **私生活の中核からデータを標的に傍受することは、他の国に所在する人物に関しても許されません。**これは、私生活の核心に関する検索用語をそのような人物に対して使用してはならないことを意味します。第5条第2項第3文は、第10条法第5条第2項第2項と併せて、他の国に所在する者に関しては、この点に関して十分に具体的かつ明確ではない。

第3　サイバー通信情報監理委員会によってプライバシーは守れるか?

政府も認める独立の監督機関の必要性

- 能動的サイバー防御は他国の主権侵害につながりかねない、また「通信の秘密」を侵害し、プライバシーを侵害する恐れがある行為である。
- 能動的サイバー防御が許容される要件、その審査の仕組みが明確となっていなければ、人権侵害が現実化する危険性がある。
- 議論の整理では「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」「主要先進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を組み合わせ、ち密な法制度をつくりあげていく」などとされているが、裁判所による事前審査はすでに放棄されている。
- 政府資料には、ドイツの法制度について右のような説明がなされている。



2 ドイツ

○ ドイツのBND法は、独立した事前の審査及び継続的な事後監督の両方を備える。
○ ドイツ連邦憲法裁判所判決（2020年）で示された通信の秘密との関係で必要とされる考慮要素（次ページの①から⑭まで）がおおよそ含まれていると考えられる。

	ドイツ（連邦情報局法（BND法）） 担当行政機関（連邦情報局（BND））	独立機関（独立統制評議会（UKRａｔ））
組織		
準備・承認	○目的・期間等の設定　措置の目的、対象とする危険分野、地理的焦点、期間を限定 ○長官（又は代理人）が命令。独立機関審査後に実施。（①,③,④）	○命令の実施前に、命令の適法性を審査・確認。適法性が確認されない場合、命令は失効（①,③,④）
通信事業者への措置	○協力義務　通信事業者等に対し、連邦首相府の命令により、BNDにおいて通信の監視及び記録が可能となるようにさせる義務を課す。罰金及び補償あり	
処理・分析	○各種分析の制限 ・自動フィルタリング技術を技術的に可能な限り利用、自国民の個人データ取扱の原則禁止、コンテンツデータの取得のための適切かつ必要な検索用語の使用、分析により私生活の中核に属すると判明した個人データは直ちに消去、トラフィックデータの分析制限　等　（②,⑤,⑦~⑨）	○検索用語の適法性の事後確認 ○BNDに対する監督の権限 ・文書及びデータの提出要求 ・事務所への出入り ・情報技術システムへのアクセス ・職員に対する質問 ○違法な状況がある場合、連邦首相府に対して異議申立が可能 ○議会統制委員会※への報告 6か月を超えない間隔で、議会統制委員会に活動状況の定期報告。 5年ごとにその統制活動の有効性を評価する報告書を作成し、議会統制委員会に提出　等（⑬,⑭）
提供・共有等	○個人データ移転の制限 ・データ主体を保護する利益が移転による一般的利益を上回ると認められる場合等には個人データの移転不可 ・データの移転先の機関は、BNDから送信される目的のためにのみ個人データを処理可。外国機関等が所定の保証を遵守していない根拠がある場合、移転は実行されない ○提供時、記録・ログデータの保存義務　（⑪,⑫）	
保存・廃棄	○保存期間満了後、原則、即時かつ不可逆的に削除 ○データ消去義務及び消去の事実の記録等　（⑥,⑩）	

※議会統制委員会（PKGr）は、連邦情報局を監督する責任を負い、連邦情報局等の情報機関を監督する議会の組織。基本法45d条が根拠。議会統制委員会法により、連邦政府は、情報機関の活動全般及び特に重要な事項に関する包括的な情報を議会統制委員会に提供する義務を負う。同委員会は、その他の事項についても報告を求めることができる。

5

しかし、ドイツ連邦憲法裁判所は、「ドイツの監視組織は不十分」で、違憲だと述べている

- 最後に、第10条委員会が実施する独立した監視は、ごの点に関して適用される特に厳格な要件を完全には満たしていない。独立した監視は、とりわけ、戦略的な電気通信監視に関連する限られた情報と通知義務の結果として、個々のケースで法的保護を得る可能性が事実上欠如していることを補う必要があります。したがって、**司法審査に似た有能で専門的な監督が確保されなければならず、これは実質的および手続き的な観点から裁判所による審査と同等でなければならず、特に、少なくとも同等に効果的でなければなりません。**
- 第四条委員会のメンバーは、憲法で義務付けられているような主要な役職としてではなく、**補助的な立場でその職務を果たすだけでは十分ではありません。**さらに、第10条法は、第10条委員会が**司法経験を持つメンバーを含むことを保証していません。**

米NSAは、XkeyScoreは外国情報だけを収集すると大ウソをつき続けていた

・アメリカの国家安全保障局(NSA)の元職員であるエドワード・スノーデン氏がその存在を暴露したスパイのグーグルとも呼ばれるXKEYSCOREは、イギリス、メキシコ、ブラジル、スペイン、ロシア、日本などに監視施設を持ち、これらの施設を流れる通信の「全てのデータ」を収集しているといわれる。

・このシステムも、外国情報活動監視法（FISA）裁判所の承認が必要であり、外国情報だけを集めているという説明だったが、アメリカの情報機関は、このような制約を無視して行動していた。オリバーストーン監督による映画スノーデンにも適切に描かれているが、政府がXKEYSCOREの実情について国民を欺いていたことが、スノーデン氏の内部告発の最大の根拠だったのである。

・NSAのアナリストは、メール、チャット、Web閲覧履歴、音声通話、PCカメラの画像、SNS、キーログ、パスワード、さらにそれらのメタデータを含む膨大なデータを収集するデータベースを、事前の承認なしに閲覧できる。

・メールアドレスやIPアドレスなどによって、検索することが可能であり、検索結果からメール本文、SNSのチャットなどの内容を確認できるシステムとなっているのです。映画「スノーデン」をご覧になった方は、このシステムの使い方まで手に取るようにわかることでしょう。

- データの収集は通信ケーブルからのデータの抜き取り、システム管理者を狙ったハッキングなど多岐にわたる。XKEYSCOREはカナダ、ニュージーランド、イギリス、日本にも提供されている。日本では防衛省情報本部電波部に提供されている。日本国内には３箇所以上の拠点があり、５億ドル以上を日本が負担しているとされる。

サイバー通信情報監理委員会はプライバシー保護のための機関ではなく、サイバー攻撃の追認機関、情報漏洩の監視機関となる見通し

- 報道では政府から独立した第三者機関をつくるとしているが、この機関は、プライバシー侵害が起きていないかどうかを監督する機関としては設計されていない。
- 報道でも、情報の漏洩がないかを監視する組織、さらには政府がサイバー攻撃をするときに事前または事後的にこれを承認することを主要な任務としている。
- ドイツ連邦憲法裁判所は、この機関を司法的機関とせよと、命じている。裁判官を委員に入れるようなことは盛り込まれる見通しであるが、この第三が者機関は国際的な基準を満たす独立性と専門性を持ったものにはなりそうにない。

アメリカの外国諜報監視裁判所の発行する令状はラバー・スタンプである
委員会をさらに監督する機関がカナダにはあるが、法案にはない

第4　人が分析しなければ、人権侵害が起きないのか?本当に人に不正ができない仕組みなのか?

2025年(令和7年)4月9日(水曜日)　総合　2

サイバー防御法案 残る懸念

「国内間通信」拡大に含み

東証大幅反発 1876円高

不正閲覧「技術的に可能」

核心

疑問

追認

監視

能動的サイバー防御法案の論点と衆院での修正点

通信の秘密の侵害

「人が閲覧できない自動的な方法で、機械的な(有)用のみを選別し分析する」(石破茂首相)

修正　通信の秘密の尊重条文を追加

第三者機関のチェック

「独立性は担保されている」(平将明サイバー安保担当相)

修正　国会への報告事項を具体化

国際法との整合性

「海外サーバーへの侵入・監視は武力行使に当たらない」(平氏)

修正　なし

平均株価の推移

米関税の対応

外交努力指示

「人による知得を伴わない自動的な方法」とは何か

- 内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報を選別し、それ以外のものを直ちに消去するとしている(2条8項)。
- しかし、「人による知得を伴わない自動的な方法」には、取得したメタ情報に検索をかける方法が含まれるであろう。ドイツでは、この検索語の使用について、特定の用語を用いた検索を禁止しているが、今回の法案にはそのような縛りはない。

分析のために、通信情報を使う場合があることを政府は認めている。外国政府にも情報を提供する

・外国の政府に対する情報提供について(第39条関係)

・提供を行うのは、例えば国家を背景とするサイバー攻撃が起こった際にパブリックアトリビューションを行う場合。攻撃の相手となった国だけでなく、第三者もパブリックアトリビューションのエビデンスを出していると公表すれば抑止効果が高まるため、そのような共同声明を出せるようにする目的で情報提供する。

・オーストラリアがサイバー攻撃を受けた際は、それが中国を背景とするものであると、日米等8か国が共同署名した文書を発出した。

国は「不正な方法を用いてメール本文などを閲覧することは技術的に不可能ではない。」と答弁している。
問題は政府が不正をしないと信ずることができるか、不正が糺される制度となっているかどうかだ。

- 4月2日の審議で緒方林太郎議員(無所属・有志の会)の質問に対して、政府参考人の小柳氏は、「政府の職員が、取得通信情報のうちコミュニケーションの本質的内容など、法律案の要件を満たす機械的情報以外の情報を不正な方法を用いるなどして閲覧すること自体は技術的には不可能ではないというふうには思います。」
- 「ただ、本法律案では、取得した通信情報につきまして、閲覧その他、人による知得を伴わない自動的な方法により、不正な行為に関係があると認めるに足りる機械的情報のみを選別して記録し、それ以外のものを終了後直ちに消去するよう法的な義務として条文に明確に定めてございます。」
- 「この自動選別につきましては、定められた義務を履行する上で適切に選別の条件が設定されたかどうか、委員会の指定職員による継続的な検査の対象となってまいります。その検査の結果及び状況は委員会に報告をされまして、もし違反していると認められる場合には、委員会から選別を行う行政機関である内閣府に通知がされまして、通知を受けた内閣府は是正等の措置を講じなければならないこととされております。」

第5　大川原化工機冤罪事件・岐阜大垣署国家賠償請求事件名古屋高裁判決が示す公安警察組織の法遵守への根本的疑問

日本テレビ報道より

大川原化工機事件は経済安保法制定を焦る公安警察の暴走が生んだ冤罪である。

- 日本弁護士連合会：大川原化工機事件 (nichibenren.or.jp)
- 大川原化工機事件とは、そもそも犯罪が成立しない事案について、会社の代表者らが逮捕・勾留され、検察官による公訴提起が行われ、約１１か月もの間身体拘束された後、公訴提起から約１年４か月経過し第１回公判の直前であった２０２１年７月３０日に検察官が公訴取消しをしたえん罪事件である。
- ２０１３年１０月、貨物等省令が改正され、一定の要件を満たす噴霧乾燥器は兵器転用が可能になるため、これらを輸出する際に、経産省の許可を要することとなった。大川原化工機は噴霧乾燥器メーカーのリーディングカンパニーとして、法改正にあたって経産省や安全保障貿易情報センター（CISTEC）に協力してきた。

経済産業省の了承も得て、中国と韓国に噴霧乾燥機を輸出しただけなのに・・・

- 大川原化工機の噴霧乾燥機について、経済産業省は当初立件することに否定的であったが、判決では、公安警察による捜査の過程で、警視庁公安部が経済産業省の省令の解釈を立件方向で捻じ曲げていたこと、経済産業省を説得するために、専門家の供述調書として本人が話していない内容を記載されたものが作成されていたことなどが判明している。
- さらに、証人尋問では、捜査に当たった現職の警視庁の警部補が、「事件は捏造である」ことを認める証言した。
- この事件では、逮捕・勾留された技術者相嶋さんについて７たび保釈却下されていたこと、ガンの発症が判明したのちも勾留が継続され、勾留の執行停止後に死亡に至るという痛ましい悲劇を生み出した。

東京地裁判決によって断罪された
大川原化工機事件の公安・検察の捜査

- 2023年12月27日の判決で東京地方裁判所の桃崎剛裁判長は、警視庁公安部が大川原化工機の製品を輸出規制の対象と判断したことについて、「製品を熟知している会社の幹部らの聴取結果に基づき製品の温度測定などをしていれば、規制の要件を満たさないことを明らかにできた。会社らに犯罪の疑いがあるとした判断は、根拠が欠けていた」と判断し、捜査そのものが違法なものであったとしました。
- 逮捕された1人への取り調べについても、調書の修正を依頼されたのに、捜査員が修正したふりをして署名させたことを認定し、違法な捜査だとしました。
- さらに、検察捜査については、起訴の前に会社側の指摘について報告を受けていたことを挙げ、「必要な捜査を尽くすことなく起訴をした」として、起訴そのものが違法であったと判断しました。
- そして、勾留中にがんが見つかり、亡くなった相嶋静夫さんの死について、「体調に異変があった際に直ちに医療機関に受診できず、不安定な立場で治療を余儀なくされた。家族は、夫であり父である相嶋さんとの最期を平穏に過ごすという機会を、捜査機関の違法行為によって奪われた」と指摘しました。

大川原化工機の真相を白日のものとした、NHKの調査報道と公安内部からの内部告発

- NHKは、数次にわたる「“冤罪”の深層」の調査報道により、大川原化工機をめぐる不正輸出事件について、経済安保法の必要性を煽り立てるために、軍事利用とは全く無関係の噴霧乾燥機の中国への輸出を軍事技術の輸出に当たるとでっち上げていった公安警察の暴走を報じた。
- これを止められなかった検察の無力化、どのような過程をたどって“冤罪”が起きたのかを、綿密かつ広範な取材の成果を示すことによって社会に問うた。

公安警察による市民運動に対する情報収集活動が違法であると判示した名古屋高裁2024年9月13日判決

・岐阜県大垣市で計画された風力発電施設の建設を巡り、県警大垣署が住民の個人情報を収集し、業者に提供した。・名古屋高裁(長谷川恭弘裁判長)判決は2024年9月13日、一審・岐阜地裁判決を変更。情報提供に加え、情報を収集したことも「恣意（しい）的な運用がされていた」として違法性を認定、一審より増額し、原告が要求していた満額の計440万円の賠償を命じた。また、県が保有すると認められる情報の抹消も命じた。

・判決を受け、原告の一人、大垣市の住職松島勢至さん（72）は「地域の問題について意見をいう、当たり前のことが、警察から危険視される世の中ではいけない。命を守る運動がやっと認められた。うれしい」と語った。

自浄作用のない警察を信じて、すべてのプライバシーを渡したら、民主主義が成り立たなくなる

・長谷川裁判長は、憲法13条が個人情報をみだりに収集・保有されない自由も保障していることに加え、原告らの活動は平和的だったとして集会や結社、表現の自由などを保障した憲法21条にも反するとして、収集の違法性を認めた。

・さらに、恣意的とした情報収集活動について、法律の規制もなく、監督する第三者機関もないと言及した上で、「**警察内部の自浄作用が全く機能していない**」と断じた。 また、情報の抹消については、今後提供される恐れがあるとして、保有していると認められる情報の抹消を県に命じた。

憲法上の人格権としてのプライパシーを深く分析した画期的な判決

- 憲法13条は、個人の私生活上の自由が公権力の行使に対しても保障されるべきことを規定しているものであり、何人も、個人の私生活上の自由のーっとして、少なくとも、個人に関する情報をみだりに第三者に開示又は公表されない自由を有しているものと解される(最高裁20年3月6日第一小法廷判決・令和同5年3月9日第一小法廷判決)。そして、個人情報をみだりに第三者に開示又は公表(提供)されない自由のみならず、その前段階ともいえる個人情報の収集及び保有についても、個人の私生活上の自由を侵害するようなものは許されないというべきであって、そのような個人情報の収集及び保有がみだりにされない自由もまた、憲法13条により保障されているものと解すべきである。
- すなわち、私人が発信した自己の情報を公権力が広く収集L、分析しているとすると、私人が自ら情報発信すること自体を躊躇する可能性があるし、情報発信する内容についても、公権力がこれを収集していることを前提とした内容にしてしまう可能性があるのであって、いずれにせよ、私人が自らの行動に対する心理的抑制が働き、少なくとも自由な情報発信に対する事実上の制約が生じることは明らかであって、憲法で保障された表現の自由(21条1項)や内心の自由(1 9条)に対する間接的な制約になるのである。そして、公権力が、ある者の個人情報を収集しているということは、その者と接触する者の個人情報や、その者が所属する団体ないしグループ。等の情報も公権力によって収集されることになるから、そのような者との交友を避けたり、そのような者がグル~プ等に入ることを嫌ったりすることが考えられるのであって、現実的な社会生活への影響を生じさせるものといえるのである。

警察の情報収集活動がもたらす具体的な弊害を指摘

- そして、公権力が、本人の知らないまま、特定の個人に関する個人情報を、その要保護性の高低、推定的同意の有無、収集方法の強制処分性文は任意手段性の知何、正確性の有無や程度等にかかわらず、多数収集してこれらを集積し、分析し、保有するなどすれば、**当該個人の実際の人間像(人物像)とは異なる人間像がその中で形成され、これが独り歩きして、誤った個人情報に基づく措置等を行ってしまう可能性がある。**また、**保有する情報が不十分なもの(重要な意味を持つ関連情報が欠落する場合などもあり得る。)である場合は、本来であれば考慮すべき情報を考慮せずに意思決定し、それに基づく措置等を行つてしまう危険性も生じ得る**のである(部分的情報によって、当該個人に関する虚像が形成され、そのような予断に基づく意思決定がされる恐れがある。)。
- しかも、このような個人情報の収集及び保有等を警察組織が行った場合には、その利用のされ方(本件ではこの点自体も明らかではないが。)によっては、正確性を欠く情報(誤った情報、不十分な情報、最新のものではない古い情報等)に基づき、監視の対象とされたり、犯罪捜査の対象として取り上げられたりして、**.誤認逮捕等の身柄拘束が生じる可能性も否定できない**のである。
- さらには、公権力から誤った情報(部分的情報のみが提供されることも含む。)が当該個人に関係する第三者に提供されれば、当該第三者は、**誤った情報に基づく意思決定(部分的情報に基づいて虚像が形成され、これに基づいて意思決定されることも含む。)をし、当該個人に対して行動することになってしまうという弊害**も生じ得るのである。

第6　サイバー攻撃と国際法
タリン･マニュアル2.0とは何か?

・2007年に大規模なサイバー攻撃を受けたエストニアの首都タリンに、2008年にNATOサイバー防衛センターが設立された。

・同センターは、専門家が個人資格で集まり、サイバー攻撃に関する国際法ルールを作る作業を支援してきた。

・そのような作業の結果2013年に「サイバー戦に適用される国際法に関するタリンマニュアル」がまとめられた。これが、タリンマニュアル1.0(有事を対象とした規則)と呼ばれるものである。

・これを2017年にあらたに平時のサイバー活動と国際法に関して改訂したものが「サイバー行動に適用される国際法に関するタリンマニュアル2.0」である。

「越境サイバー侵害行動と国際法」の著者中村和彦氏は現職の外務省元地球規模課題審議官/国際法局長

政府も国際法・タリンマニュアルを尊重すると答弁

・この点について、平岡秀夫議員の質問に対して、政府は次のように答弁しています。「国連憲章全体を含む既存の国際法がサイバー行動にも適用されるということは、国連における議論を通じて確認をされています。

・こうした国際社会における議論を踏まえ、サイバー行動に適用される国際法に関する日本政府の基本的立場として、国連憲章全体を含む既存の国際法はサイバー行動にも適用されるとの認識を示しました。その上で、紛争の平和的解決に関しては、サイバー行動が関わるいかなる国際紛争も、国連憲章第二条３及び第三十三条に従って、平和的手段によって解決されなければならないとの考えを示しました。」(3月21日内閣委員会)

・　4月2日の審議では、上村議員の質問に対して、タリンマニュアルについて「NATOの公式見解ではないものの、この分野の議論にあたっては極めて有益なものである」と答えています。

有識者会議でもタリンマニュアルが議論の対象とされたが、提言も、法案も、これをほとんど反映したものとなっていない

- 有識者会議では、七月の審議の冒頭に、酒井啓亘早稲田大学法学学術院教授によって、「アクセス・無害化措置と国際法の関係－能動的サイバー防御（ACD）の国際法上の評価」との報告がなされている。
- このなかで、『タリン・マニュアル2.0』（2017）について、154の規則を文章化したもので、学者・実務家が作成した民間団体の成果物であるが、西側諸国をはじめとする多くの国家の共通認識とほぼ一致したものと説明されている。
- その内容は、主権；相当の注意；管轄権；国家責任法；国際人権法； 外交関係法・領事関係法；海洋法；航空法；宇宙法；国際電気通信法； 平和的解決；干渉の禁止；武力の行使；集団安全保障；武力紛争法； 占領；中立　などに及んでいる。
- しかし、提言の中に正確に反映されているとは、到底思えない。

他国の通信情報の利用・無害化措置は主権侵害となりうる

・どのようなサイバー行動が主権侵害となりうるか（ひいては違法となりうるか）について、国により、また、同じ国でも時代によって見解が異なりうる。

・例えば、ブラジルは、通信の傍受や他国領域に存在する情報システムに対するサイバー行動や域外に効果が及ぶサイバー行動は主権侵害に該当しうるとしている。

・フランスはフランスのサーバーシステムに対するすべてのサイバー攻撃又はサイバー手段を用いた方法によるフランスの領域における効果の発生は主権侵害を構成するとしている（赤堀毅外務省地球規模課題審議官（執筆当時、現在は外務審議官）著「サイバーセキュリティと国際法の基本―国連における議論を中心にー」４４頁以下）。

• 通信情報の利用・無害化措置については主権侵害、ひいては違法評価がありうることを前提に、その違法性阻却事由の存否を検討しなければならない。

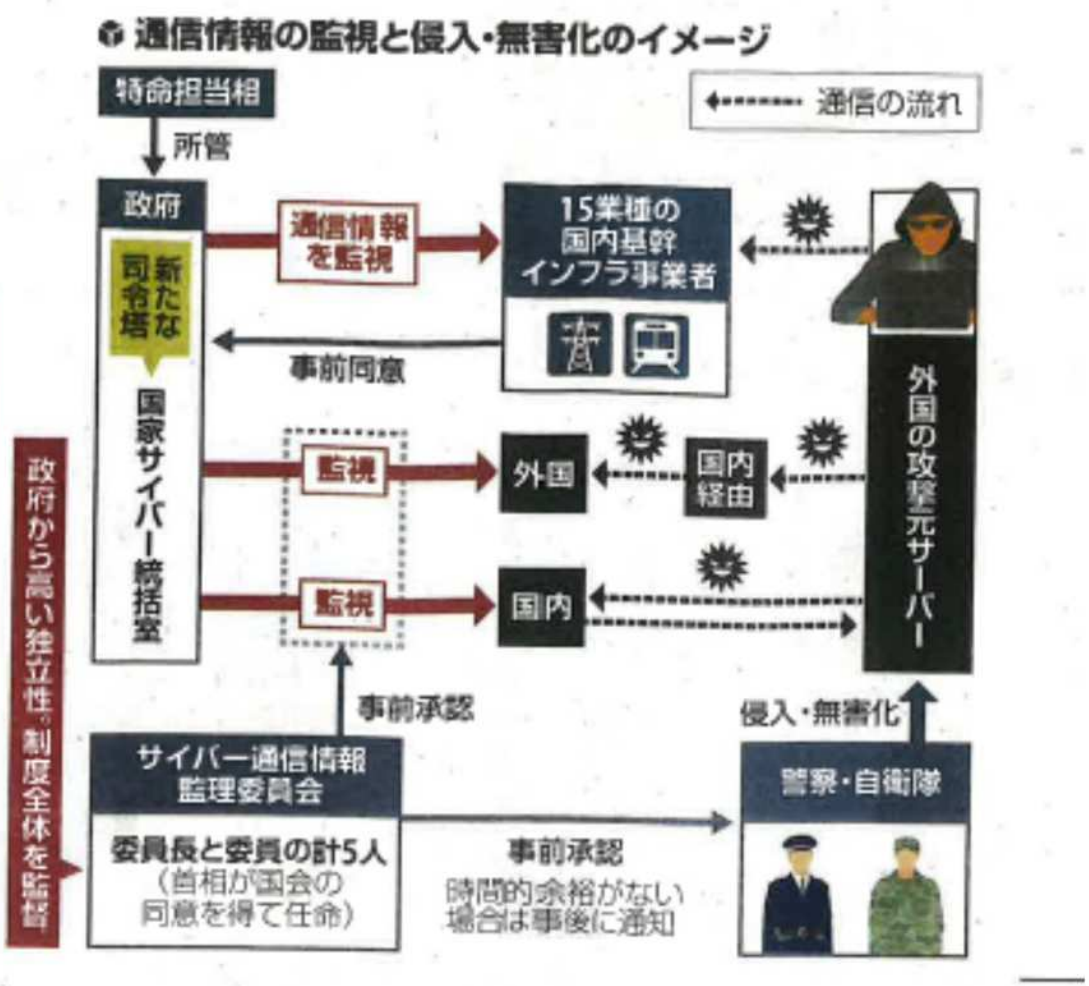
タリンマニュアル2.0の主要な条項

- 規則1　国家主権の原則は、サイバー空間において適用される
- 規則4　国家は、他国の主権を侵害するサイバー行動を行ってはならない
- 規則20 国家は、他国が自国に対して負う国際法上の義務違反への反応として、対抗措置(性質上サイバーであるか否かを問わない)をとる権限を有する。
- 規則22　対抗措置(性質上サイバーであるか否かを問わない)は、基本的人権に影響し、禁止された戦時復仇に該当し、または強行規範に反する行動を含むことはできない。対抗措置をとる国家は、外交上または領事上の不可侵に関する義務を履行しなければならない。
- 規則26 国家は、根本的な利益に対する重大で差し迫った危険を示す行為(性質上サイバーであるか否かを問わない)への反応として、そうすることが当該利益を守る唯一の手段である場合には、緊急避難を理由として行動することができる。
- 規則73　自衛の際に武力を行使する権利は、サイバー武力攻撃が発生した場合、または急迫した場合に生ずる。この権利はさらに即時性の要件に従う

タリン・マニュアル2.0によれば、重大で差し迫った危険を示す行為に対して、唯一の手段であるときに許されるとしている

- 違法性を阻却する構成として緊急避難をとりあげつつ、「重大かつ急迫した危険」、当該サイバー行動が唯一の手段であること等が要件となる。
- 「重大かつ急迫した危険」について、「危険を回避する最後の好機ー攻撃の計画が高い確度で判明」していることを要する。
- 中谷和弘他著「サイバー攻撃の国際法　タリン・マニュアル２・０の解説　増補版」１８頁（河野桂子コペンハーゲン大学政治学部研究員執筆部分）においては、刑事訴追の証拠取得のために、他国に所在するＣ２サーバーを乗っ取ってボットネットを掃討する法執行活動を主権侵害行為としている。
- タリン・マニュアル２・０規則２６（緊急避難）「国家は、根本的な利益に対する重大で差し迫った危険を示す行為（性質上サイバーであるか否かを問わない）への反応として、そうすることが当該利益を守る唯一の手段である場合には、緊急避難を理由として行動することができる」（中谷和弘他著「サイバー攻撃の国際法　タリン・マニュアル２・０の解説　増補版」３７頁）
- 「最後の好機」(規則73)、「高い確度の方法で判明」しているとの要件は中谷和弘他著「サイバー攻撃の国際法　タリン・マニュアル２・０の解説　増補版」３７～３８頁（河野桂子コペンハーゲン大学政治学部研究員執筆部分）

第7　無害化措置は、憲法違反の先制攻撃である。＝火遊びのような法案をつくれば大火事になりうる＝



2025/2/8読売新聞

アクセス・無害化のステップ（イメージ） 政府法案説明資料より

① **アクセス**：攻撃に使用されているサーバー等が持つ脆弱性を利用するなどして、
遠隔からログインを実施。

※なお、当該サーバー等が攻撃者によって現に乗っ取られているような場合には、
（攻撃者自身が自ら侵入に利用した弱点を塞ぐことをしていない限り）
非正規の侵入手段が存在するものと想定される。

↓

② **攻撃のためのプログラム等の確認**：インストールされているプログラム一覧、作動している攻撃のためのプログラム
等を確認。

↓

③ **無害化**：
当該サーバー等が攻撃に用いられないよう無害化。
（無害化の方法の例）
・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
・攻撃者が当該サーバ等へアクセスできないよう設定変更　　など

上記措置を国外にあるサーバ等に対して行う場合、主権侵害に該当するとしても、「緊急状態*」等の国際法上の法理を援用するなどして、国際法上許容される範囲内で実施。

*：緊急状態（Necessity） 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、相手国等の不可欠の利益を深刻に侵害しないといった一定の要件を 満たす場合に、違法性が阻却されるという考え方。

政府法案説明資料より

官民連携関係

- 主要国は、2010年代後半から最近にかけ、**政府からの情報提供、重要インフラ事業者による報告の義務化を制度化**

国家ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年) 重要ｲﾝﾌﾗｻｲﾊﾞｰｲﾝｼﾃﾞﾝﾄ報告法(2022年)

豪州ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年) 重要ｲﾝﾌﾗ保安法(2018年)

国家ｻｲﾊﾞｰ戦略(2022年) ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ規則(2018年)

ｻｲﾊﾞｰﾚｼﾞﾘｴﾝｽ法(2024年) ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ指令(2016年)

通信情報の利用関係

- 主要国は、**以前より、国家安全保障等の目的のために外国関係の通信情報を利用**
- 政府における通信情報の利用について **専門の独立機関が監督**

英国：調査権限法 (2016年制定)

米国：外国情報監視法 (2008年改正)

ドイツ：連邦情報局法 (2016年改正)

豪州：通信情報傍受及び アクセス法(2021年改正)

米国：Volt Typhoonによるボットネットワーク（感染ルータ群）に対する**無害化措置**（2024年）

カナダ：政府ネットワークからの情報窃取防止目的で、攻撃者の海外サーバに対する**無害化措置**（2019年以降）

英国、豪州も同様の取組を推進。

＊ 各国の法制及び実態の全てを網羅するものではない。

海外の実態は不明な部分が多い。

- 有識者会議の資料の中で、無害化の措置に関する海外の例については、アメリカとカナダの断片的な報告しかなく、その法制の裏付けや、攻撃の実際の経過など具体的な説明がほとんどない。
- 秘密裏に行われていて、資料がないと説明されている。
- したがって、その主体、手続、過誤が起きた場合の対応など、全くわからない。
- 今後、日本でも無害化が行われたとしても、衆院で可決された修正案でも、年間件数が報告されるだけで、国会にもその詳細は報告されない。

サイバー攻撃についての国際的な枠組み

・不正アクセス行為禁止法（１９９９年）、さらに は刑法改正（２０１１年）により、不正に他人のコンピューターにアクセスしてデータを書き換えたり、データを取得したりする行為、他人のコンピューターにコンピューターなどについて犯罪として処罰する規定がつくられてきた。そして、 犯罪捜査のために、リモートアクセスやサーバーへの捜索・差押などの手続きも進められるようになっている。

・国境を越えるサイバー攻撃についてサイバー犯罪から社会を保護するための国際的な協力体制を確認したヨーロッパ評議会起草のサイバー犯罪条約が２０１２年に発効し、日米など７５か国が批准している。

・２０２４年１２月には、国連サイバー犯罪条約が国連総会で採択されています。この条約の起草過程は、日米欧諸国、中国・ロシア、グローバルサウスの複雑な関係を克服して成案化された。この条約の起草はロシアが主導したものです。強権国家が反体制派の監視を目的として条約を悪用するのではないかとの懸念が米欧からは表明されている。ヒューマンライツウォッチなどの人権団体は新条約への懸念を強め、「条約は人権保護が不十分で政府のインターネットに対する監視を拡大し、世界中のジャーナリストや活動家などに対する弾圧の法的手段となる」と非難し、各国に署名・批准しないよう呼び掛けています。

・このように、サイバー犯罪に対する国際的な取り組みの枠組みについては、発展途上であるといわざるを得ませんが、国際的な合意を積み上げて、対策をしていくべき問題であることは間違いがありません。

戦略的監視と無害化は、まったく別問題
無害化は、主権侵害のサイバー攻撃であり、緊急避難の要件に該当しない限り、正当化されない

- 無害化措置のための攻撃元への侵入は、他人のサーバーへの侵入を禁止する不正アクセス禁止法や刑法に抵触し、さらに攻撃元サーバーが海外にある場合は、国際法時用の緊急避難の要件に当たらない限り、国際法上の外国に対する主権侵害に当たる(タリンマニュアル規則4)。
- サイバー攻撃を行っているサーバー国は、日本とは緊張関係を抱えている国のサイバーが用いられている例が多いと提言も述べている。
- タリンマニュアルにおいても、緊急避難に該当する場合以外は、サイバー攻撃は許されないことは、国際法の要請であるとされている。
- この点が踏まえられないと、サイバー攻撃の防止のための措置が、逆に国際紛争を拡大し、期せずして熱戦にまで発展する危惧までがある。
- 石村耕治名誉教授（白鴎大・情報法）「サイバー空間での無害化という名の先制攻撃が武力に当たるかどうか。憲法9条違反にならないのか。制度としてどう許されるのか。透明性の高い議論が必要だ」(東京新聞　7月11日)。

なぜ、私人がやれば違法な行為を国がやることができるのか？ 国際法上、そのようなことは許されるのか

- 法案は、サイバー攻撃を行おうとしている者に対して、私人が行えば、不正アクセス、電磁ウィルス使用などの刑事法上の犯罪に問われる違法な行動を、国として敢行しようとしていることになる。
- これは憲法９条に反する先制攻撃にもなりうる行動である。
- 「サイバー攻撃は時間との闘いで、『誰が背後にいるのかわからないと対処できない』という状態では国民を守ることが出来ない。そこで、警職法・自衛隊法を改正し、現在では不法行為にあたる行為を法律行為にした。自衛隊法まで改正するのは、基本的に国家を背景とする攻撃に備えるためである。」「政府が一番恐れているのは、実際の軍事行動を起こす直前にインフラを機能不全にする、もしくは軍事行動を起こさなくても社会に混乱を引き起こすことを目的にしたサイバー攻撃である。」(福島瑞穂議員に対する説明)
- しかし、法案は国家を背景とした攻撃だけを対象としておらず、日本の私企業や個人を守ることも目的としているように読める。国の存立にかかわる攻撃だけを未然に防ぐという建付けにはなっていない。

法案が無害化の措置をとれるとする場合の要件

・警察が対処する場合→法案の定める「サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、**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**」という要件は緊急避難の要件より広汎である。

・自衛隊が対処するべき場合の加重要件→「**本邦外にある者による 特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、自衛隊が対処を行う特別の必要があると認めるとき**」も、限定には役立たない。

法案は、タリンマニュアルの定めた緊急避難の要件を満たしていない

- タリンマニュアル規則26は、「国家の根本的な利益に対する重大で差し迫った危険」「利益を守る唯一の手段である場合」を要件としていた。また、タリンマニュアル73は、「侵害の切迫性」を求めている。
- 法案は、「国家の根本的利益」ではなく、個人の生命、健康、木木用の経済的利益を守る場合でも発動できるシステムとなっている。
- 法案には唯一手段性も侵害の切迫性も要件とされていない。
- 明らかに、法案の定める要件とタリンマニュアルの定める緊急避難の要件には大きな乖離がある。

無害化措置の手続への疑問

- **監理委員会が事前に承認すると説明されているが、緊急の場合は事後報告で足りるとされている。**
- **また、無害化措置は警察と自衛隊が分担して、軽微なものは警察、重大なものは自衛隊が対応するとしているが、その連絡調整の部分を内閣府が担うとされるが、その体制は明確でない。**

防衛大学校の黒崎将広教授の警告

- 3月28日の参考人質疑では、立憲民主党が推薦した、防衛大学校の黒崎将広教授は次のように述べた
- 「有識者会議の提言においても、意図せず措置を行うことで、達成しようとしていたものとは異なる結果に至った場合の対応についても、十分検討しておく必要がある。」
- 「安全保障と人権保障の適切なバランスをとり、選別対象となる機械的情報の範囲や選別基準を適宜見直していくべきである。」
- 「日本による措置を武力の行使だと批判する国が出てくる可能性は否定できず、平素から辛抱強く対外的に説明し、理解を得ていくことが課題になる」
- 「自国が国際法を誠実に履行する体制をしっかり構築しておかないと意味がありません。」

国外への無害化措置の相手を間違ったときにどのような対策をとるのか?

- 3月19日の公明党山崎正恭委員に対して内閣官房は次のように答弁している。
- 万が一にも間違いがないように、適切に判断する。
- 諸外国においても、誤った場合の対応は明らかになっていない。
- また、4月2日の立憲民主党の平岡秀夫委員に対して、外務省は、国債に違反した場合、原状回復、損害賠償、陳謝、再発防止を行う。相手国の国内法を踏まえ、個別に対応する。
- →答えになっていない。

火遊びのような法案をつくれば大火事になりうる

- 無害化措置はネットへの監視とは次元の違う問題だ。憲法９条の理念に反する先制攻撃になりうる。他国から報復を受けかねず、それはサイバー攻撃かもしれないが、ミサイル攻撃にもなりうる。
- サイバー攻撃の対処には、サーバー管理者に機能停止（テイクダウン）を依頼することや、攻撃者を公表し非難するなど、他にも手段があると指摘。「これまでそうした防御の対応を十分にしてきたのか怪しい。一足飛びに先制攻撃できるとするのは飛躍が大きすぎる。火遊びのような法案をつくれば大火事になりうる。
- 現実の戦争につながる恐れがあり、法案の全面撤回を求める。

第8　まとめ
2025年通常国会、能動的サイバー防御に関する法案の成立を食い止めよう

2014年12月　秘密保護法の制定に反対した、一万人の集会とデモ

市民の無関心と市民監視の放棄こそが、悪法を悪法として機能させる

・経済安保法・経済秘密保護法に続く能動的サイバー防御法案の提案の先には米軍の先兵として日本と中国との本物の戦争の悲劇が待っている。

・2013年に制定された特定秘密保護法、2017年に制定された共謀罪は、未だ猛威を振るうような状況になっていない。それは野党と市民が共同して大反対した記憶が残っているからだ。

・ひるがえって、経済安保法・経済秘密保護法の成立は、どれだけ市民の記憶に刻み付けられたであろうか。われわれの活動はささやかではあるが、意識的な市民の間に一定の記憶をつくることには成功した。しかし、それは明らかに不十分である。人々の記憶にも残らなかった悪法は、ただちにその正体を現すだろう。

・私たちの第一の任務は、これらの法律の問題点、人権侵害の危険性をできるかぎり広範な市民に知らせる努力を継続することである。

能動的サイバー防御法案 QA　Ver.5（4/8 改訂版）
＝能動的サイバー防御法案の本質はインターネット常時監視・サイバー版先制攻撃法案である＝
2025 年 4 月 7 日

作成　海渡雄一（弁護士・秘密保護法対策弁護団共同代表）

2025/2/13 日の市民と超党派国会議員の勉強会にて

はじめに　衆院可決に抗議し、参議院においても反対を続ける

1　2 法案は衆院を通過へ

能動的サイバー防御法案は、日本国民全体のプライバシーの存立にかかわる重大な人権侵害の問われる法案である。それだけでなく、日本発の熱戦を引き起こしかねないほど、深刻な問題をはらんでいる。この問題をわかりやすく説明するためにこの QA を作成した。これは、衆院で法案が可決されようとしている段階で作成したものである。

4 月 4 日午後、能動的サイバー防御法案＝ネット監視・サイバー先制攻撃二法案（A・B 法案）が内閣委員会で可決された。衆院本会議でも 8 日の衆院本会議で採決された。

A 法案に国会の監視機能強化、通信の秘密の尊重、三年後の見直しの三本柱とする修正案を、自民と立憲民主党を中心に、公明党、日本維新の会、国民民主党、「有志の会」などが共同提出し、この修正案が賛成多数で可決された。B 法案は無修正で委員会で可決された。

2　膨大な情報を政府の中枢に吸い上げる大量監視を合法化する法案

ネット監視法案（A 法案）は、サイバー攻撃防止のために事業者と締結した協定、あるいは同意なくして通信情報を取得するための法案である。政府は、収集対象となるのは海外通信に限られ、国内で完結する通信は対象としていないとする。基幹インフラ事業者や一般の通信事業者との協定に基づく通信情報の取得には、何の限定もない。情報収集は必要最低限度にとどめるという原則規定も法案にはない。

3　国内通信は収集から除かれるという説明はミスリーディング

スノーデン氏が告発したアメリカのネット監視システムも、法制度上は外国通信だけを監視するとされていたが、情報機関は制約を無視して行動していた。

参考となるのが昨年 10 月ドイツの連邦憲法裁判所が下した判決だ。この判決は海外に関わる情報の監視のためには、国内の通信情報も含めて取得することになるが、データ削除の規定がない点を違憲判断の理由の一つとしている。政府は、ドイツは属人主義をとっているが、日本では属地主義を採用しており、問題はクリアーしているとする。この通りだとすると、国内の通信でも海外のサーバーを経由しただけで、収集の対象とされることとなり、むしろ問題はドイツより深刻だといえる。

4　ネット監視は政府批判を沈黙させる

これまで国内のネット監視は通信傍受法が根拠とされ、裁判所の令状を受ける必要があった。しかし、今回の制度では、どんな情報が政府に集められているかは、最後まで市民には明らかにされない。常に誰かに見られているという可能性があるだけで、市民は政府批判もためらい、秘密裡に公益通報することも不可能になる。人権と民主主義が、危機に瀕することとなる。

5　サイバー空間における先制攻撃が可能に

もう一つのサイバー先制攻撃法案は、サイバー攻撃による重大な危害を防止するため、警察官又は自衛官によって無害化措置と名付けられた先制的なサイバー攻撃の根拠規定として、警職法と自衛隊法などを整備する法案である。サイバー先制攻撃法案といってよい。

サイバー攻撃の対処には、サーバー管理者に機能停止（テイクダウン）を依頼することや、攻撃者を公表し非難するなど、他にも手段がある。ところが、B 法案は、サイバー攻撃を行おうとしているものに対して、私人が行えば、不正アクセス、電磁ウィルス使用などの罪に問われる違法な行動を、国として、警察機関や自衛隊の手で、敢行しようとしている。これは憲法9条に反する先制攻撃になりうる。

6　法案はサイバー攻撃に関する国際基準タリンマニュアルの要請を満たしていない

法案は、「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」には警察が、海外からの特に高度に組織的かつ計画的な行為が行われた場合は、自衛隊が対処するとしている（2,4 条）。しかし、米欧諸国が認めるサイバー攻撃に関する国際規範であるタリンマニュアルでは、「（国の）根本的な利益に対する重大で差し迫った危険」「利益を守る唯一の手段である場合」を要件とし（規則26）、「侵害の切迫性」も求められている（規則 73）。個人や企業の利益を守るために日本の警察が海外のサーバーへの攻撃ができるように読める。

7　攻撃が報復を招き、熱戦に発展する可能性は否定できない

サイバー攻撃は、正体を隠して行われる。偽情報に釣られて、攻撃対象を間違える可能性は高い。攻撃を行えば、報復が報復を呼び、偶発的にミサイル攻撃から現実の戦争へと発展する可能性も否定できない。

サイバー空間においても、国際法、紛争の平和的解決の考えに沿って、サイバー攻撃を国際社会が一致して非難し、深刻化を未然に防ぐ外交関係を築く努力が求められている。

「気がついたら開戦」となってからでは遅いのだ。我々は、参議院においても、この 2 法案の成立に反対し、闘い続ける。

8　衆議院内閣委員会等における審議経過

3 月 19 日　法案趣旨説明　審議
3 月 21 日　審議
3 月 26 日　審議
3 月 28 日　参考人招致
①高見沢将林（のぶしげ）（与党推薦：軍縮会議日本政府代表部大使、元防衛省防衛政策局長）
②吉岡克成（与党推薦：横浜国大教授、情報通信専門）
③黒崎将広（立民党推薦：防衛大学校教授）
④大沢淳（？推薦：中曽根康弘世界平和研究所主任研究員）
4 月 2 日　審議
4 月 3 日　内閣委員会・総務委員会・安全保障委員会・連合審査会
4 月 4 日　審議採決
4 月 8 日　衆議院本会議採決

目次

Q1 能動的サイバー防御法案が国会に提案されたようですが、どんな法案なのでしょうか？

A1 私は、能動的サイバー防御法案の本質はインターネット常時監視法案・サイバー版先制攻撃法案であると思います。

国家を背景とした高度なサイバー攻撃の危険が高まっていることを理由に、2 月 7 日、政府は「能動的サイバー防御」を導入するための 2 法案を閣議決定しました。

一つが、「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案」（サイバー被害防止法案 以下「A 法案」という）、もう一つが、「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の施行に伴う関係法律の整備に関する法律案」（アクセス無害化実施法案 以下「B 法案」という）です。

A 法案は、サイバー攻撃などによる被害の防止のための基本的な方針の策定、インフラ事業者などにサイバー攻撃を受けたことの政府への報告を義務付けること、サイバー攻撃防止のために通信情報を取得すること、通信情報の取扱いについて「サイバー通信情報監理委員会」による審査、検査について定めること、通信情報等を分析した結果の政府機関、事業者、外国政府への提供等について定めた新法です。一言でいえば、インターネット常時監視法案といえます。

B 法案はサイバー攻撃による重大な危害を防止するため、一定の警察官又は自衛官による無害化措置＝先制的なサイバー攻撃の根拠規定を整備し、サイバーセキュリティ基本法、警職法、自衛隊法などの関係法の改正を行う法律であり、一言でいえば、サイバー版先制攻撃法案です。

Q2 どんな経緯で、このような法案が提案されたのでしょうか？ 米政府、米軍からの働き掛けによる制度化と考えてよいのでしょうか。

A2 伏線は 2022 年、岸田政権が策定した国家安全保障戦略です。能動的サイバー防御制度の導入は、2022 年 12 月に閣議決定された「国家安全保障戦略」において、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としたことに基づいています。その後、首班の交代がありましたが、あたかも既成事実であるかのように、法案の策定が進められてきました。

政府は、「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」を 2024 年 6 月から開催し、半年の審議を経て「サイバー安全保障分野での対応能力の向上に向けた提言」をまとめました。この提言が法案のもととなっています。

その背後にアメリカ政府からの要望がある事はほぼ明らかです。

2024 年 7 月 28 日、東京において日米安全保障協議委員会（SCC）が開催され、ブリンケン国務長官、オースティン国防長官、上川外務大臣及び木原防衛大臣が出席し、2024 年日米安全保障協議委員会声明（通称「2＋2共同声明」）を共同発表しました。

この中で、「同盟調整、指揮・統制の向上」の個別項目の5項目の最後で、サイバーセキュリティについて、次のように、言及しています。

「●日米は、相互運用性の深化を実現するため、強固なサイバーセキュリティ及び情報保 全並びに情報共

有の重要性を認識するとともに、情報共有の機会の増加、サイバーセ キュリティ、データセキュリティ及び情報保全の更なる向上並びに通信及び物理面で のセキュリティの強化を検討する。」

さらに、「日本の南西諸島における同盟活動の強化」「二国間演習、即応性及び運用の強化」「拡大抑止の強化」「ISR 協力の強化」「領域横断作戦、情報戦、人工知能（AI）に関する協力の拡大」に続く日米間の重点的協力項目の最後である 8 項において、「サイバーセキュリティ及び情報保全の強化」について、次のとおり合意しています。

「閣僚は、同盟にとって、また、同盟が未来志向の能力を開発し増大するサイバー脅威に先んじるために、サイバーセキュリティ及び情報保全が基盤的に重要であることを強調した。閣僚は、情報通信技術分野における強じん性強化のためのゼロ・トラスト・アーキテクチャの導入を通じたサイバーセキュリティ、情報保全に関する協力の深化にコミットした。閣僚は、重要インフラのサイバーセキュリティの強化の重要性について同意し、同盟の抑止力を更に強化するため、脅威に対処する防御的サイバー作戦における緊密な協力の促進について議論した。米国は、情報共有のためのより良いネットワーク防 御の実現に資するリスク管理枠組みの着実な実施を含む、国家のサイバーセキュリティ態勢を強化する日本の取組を歓迎した。閣僚は、将来の演習にサイバー防御の概念を取り入れる機会を増やすことについて議論した。閣僚は、二国間のサイバーセキュリティ及び情報保全に関する協議を通じてなされた重要な進展を称賛した。」

このように、今回の法案の提案が、米政府の強い要望によって、遂行されてきたことは明らかです。

法案の定める自衛隊による無害化の措置によって守られるシステムには米軍のシステムも含まれることが、3 月 19 日の内閣委員会における山崎議員の質問に対する答弁で次のように、確認されています。

「日米安全保障条約に基づき、我が国に所在する米軍が使用する特定電子計算機の使用が阻害された場合には、米軍の運用が妨げられることとなり、ひいては、日米の共同運用能力の低下につながり、我が国の防衛に支障が生じることになりかねません。
その上で、サイバーセキュリティーは平素から確保されることが極めて重要であることを踏まえ、我が国に所在する米軍が使用する特定電子計算機は、我が国の防衛力を構成する重要な物的手段に相当するものと評価し、新設する自衛隊法第九十五条の四における警護の対象とすることといたしました。」

Q3　法案に繰り返し出てくる重要電子計算機とは何のことですか。

A3　A 法案は、まず、重要電子計算機を定義しています。この概念が法案を理解するカギだと言えます。

まず第一に、サイバーセキュリティが害された場合に特定秘密・重要経済安保情報などの秘密の管理に重大な支障が生ずる場合、第二に、経済安保法 50 条に定められた特定社会基盤事業者が使用する電子計算機のうち、サイバーセキュリティが害された場合に特定重要設備の機能が停止・低下する恐れのあるものが指定されます。

そして、重要電子計算機からの情報漏洩などを防止するため、官民連携を図るとして、基幹インフラ 15 事業者（電気、ガス、石油、水道、鉄道、貨物自動車運送、外航通運、航空、空港、電気通信、放送、郵便、金融、クレジットカード、港湾）に、特定重要計算機を政府に届け出るこ（4 条）と、サイバー攻撃＝特定侵害事象が発生した時には、所管大臣と内閣総理大臣に届出なければならないとし、報告を義務づけています（5 条）。

第 4 条に事業者が「特定重要電子計算機の製品名及び製造者名その他の主務省令で定める事項」を届出るとされていますが「その他」で何を報告させるのかが不明です。有識者会議の提言では施設・設備・プログラム・営業の秘密に属する情報などが挙げられていましたが、それも明示されておらず、どこまでの情報が求められることになるのか予測することができません。

法案第 5 条には「特定侵害事象又は当該特定侵害事象の原因となり得る事象として主務省令で定めるものの発生を認知したときは、主務省令で定めるところにより、その旨及び主務省令で定める事項を特別社会基盤事業所管大臣及び内閣総理大臣に報告しなければならない」と定められています。ここでも、主務省令にすべてがゆだねられています。特定侵害事象の原因となり得る事象としてどのような事象が想定されているのか、完全にブラックボックス化されています。

そして、これらの届出がなされていないと考えるときには、所管大臣は届出を命ずることができるとし（6 条）、内閣総理大臣は所管大臣に意見を述べることもできるとされています（7 条）。命令に反対した時の罰則（83 条　200 万円以下の罰金）も定められています。

Q4　この法案は多くの事業者と協定を結び、これらの事業者から多くの情報を政府に吸い上げようとしているのですか。

A4　法案は、当事者の同意がなくても情報を収集できる制度を、広範に整備しようとしています。

まず、広汎な情報があらゆる基幹インフラ 15 事業者との当事者協定によって取得される仕組みがつくられます。

「国外関係電気通信事業者」に対して、情報提供、機器の接続などの協力を求めることができ、正当な理由がない限り拒否できないと定めています（20 条）。

基幹インフラ 15 事業者だけでなく、一般の電気通信役務の利用者からも、内閣総理大臣との間で、「当事者協定」を締結し、情報の提供を受ける制度がつくられました（11,12 条）。そして、法案では、外内通信に係る通信情報を用いて、分析を実施し、事業者等に必要な分析結果を提供するとしています（21-31 条）。

しかし、これらの協定に基づいて提供を受ける情報については、サイバー通信情報監理委員会の承認も必要がなく、情報の種類にも制限がありません。

法案第 12 条では特別社会基盤事業者以外の事業電気通信役務の利用者とも協定の締結が出来るとしています。しかし、どのような事業者を想定し、どのような通信情報を得るのか？ また、情報の受け渡しはどのような形で行うことを想定しているのか？ミラーリングを行うのか、一定時間通信情報をためたものを送るのか。情報の提供媒体は何か、提供される情報を外内通信に限定することは可能か。内閣総理大臣と事業者間の協定や協議にはどのような内容が求められるのか？ その狙いが全く不明で、非常に広範な情報を収集するような運用への歯止めが欠けているのです。

政府は国会議員に対する説明の中では、「どのような情報をどのような頻度で提供するかは政府と提供者が結ぶ協定次第だが、提供者の中には通信の種類を自前で振り分けて提供するのが困難な者もおり、外内通信とそれ以外を振り分けることを義務付けるのも難しい。結果、内内通信も含めて提供されることもあり得るが、政府は提供されるものは全部受け取り、その後自動選別（22 条）をする。」「政府による内内通信の取得を禁止する規定はない。」「提供される情報は、アプリケーションを問わない。結果、メール、LINE、SNS の投稿等、全てが提供対象になる。」「どのような手法で情報を提供するかも協定次第。『ミラーリング』など、通信に関する情報のコピーをリアルタイムで政府に送ることも可能である。ただ、攻撃の全容を解明し、予防策を作るためには、必ずしもリアルタイムの情報共有が必須というわけではない。」「基幹インフラ特定社会基盤事業者には関東キー局がすべて入っているが、取材源の秘匿の必要性から、メールを提供することは出来ないと言っている。」などと説明しました（2 月 10 日の政府法案担当者による福島瑞穂議員に対する説明）。

3 月 21 日の平岡議員の質問に対する答弁において、国は次のように答弁している。

「事業者協定の制度では、通信の秘密との関係も踏まえて、あくまで通信の当事者の同意に基づきその通信情報を取得をし、その上で、協定当事者のサイバーセキュリティーの確保のために必要な分析をし、その結果を協定当事者に提供することとしております。

サイバー攻撃の脅威に直面している基盤インフラ事業者等に対しては、政府から当事者協定を締結するメリットを丁寧に説明をさせていただくなどして、協定締結が促進されるように努めていきたいと考えております。」

これでは、情報収集の範囲が広汎に及ぶことの歯止めは何もないこととなります。

せめて、この当事者協定による通信情報の利用について、これを行うことを正当化する高度の必要性を要件とすべきです。

報道では、同意によらない情報収集ばかりが大きく取り上げられていますが、極めて広汎な情報が基幹インフラ 15 事業者と政府の間で即時共有される体制となると考えられるのです。

Q5　同意なしで取得される情報から、国内通信を除くという政府の説明は本当でしょうか？

A5　また、法案第 17 条は国外から国内の重要な電子計算機（サーバーなど）を標的にした不正行為を防ぐために、政府が一定の通信を監視・複製できるようにするとして、サイバー通信情報監理委員会の承認を得て、国外からの通信、国内から国外への通信を監視するとしています。

法案は、事前に当事者の同意を得ないで、通信情報が取得できる制度を定めています。国内通信を除くので、プライバシーが保護される法制度になっていると説明が繰り返されています。

ここでは、外国間、外国・国内間の通信情報について、サイバー通信情報監理委員会の事前承認を得て取得できるとしています。「「重要電子計算機」に対するサイバー攻撃に用いられていると疑うに足りる状況のある特定の国外設備を発信元とし」ている場合と、「サイバー攻撃に用いられていると疑うに足りる状況のある特定の情報」が含まれている場合であって、これを分析しなければ、分析が著しく困難である場合に、委員会の承認を得て取得できると定めているのです（32 条、33 条）。

このように、外内通信は基幹インフラ事業者等との協定に基づいて、外外通信と内外通信は独立機関「サイバー通信情報監理委員会」の承認を受けて取得できるとされているのですが、国内通信は取得できないと説明されています。

しかし、国内の当事者間の通信も、そのほとんどが海外のサーバーを経由するとされます。ところが、政府の説明では、海外のサーバーを経由した情報は、国内通信と定義されず、収集の対象とされるのです。この点は、きちんと説明されておらず、政府の説明は極めてミスリーディングだと言えます。

また、この規定では複製の上限が通信設備の伝送容量の 30%と規定しているだけで、その範囲の基準も不明、根拠も不明であり、一般通信に影響をおよぼさない保証があるのかも不明です。

Q6　この法案と同様の制度が、ドイツ連邦憲法裁判所の決定によってプライバシーを侵害する憲法違反だと判断されたと聞きましたが、どんな判断がなされたのでしょうか。

A6　ここで参考となるのが、ドイツの連邦憲法裁判所の 2024 年 10 月 8 日決定です。この決定では、サイバー脅威の検知のための政府の措置の一部について憲法違反の判断がなされています。

ドイツと外国の間の通信に関する監視（以下「戦略的内外通信偵察」）を理由とした通信の秘密の制限について 2016 年に、国内外の人権団体等が連邦憲法裁判所に対し訴えを申し立てていた事件です。

この訴えに対し、連邦憲法裁判所は、申立人の訴えの一部を認容する、違憲決定をしました。違憲とされたのは 4 点にわたります。

①G10 法第 5 条第 1 項第 3 文第 8 号は、監視対象を内外通信に限定しているものの、戦略的内外通信偵察の際に取得したデータには、国内間でのやり取りに関するデータが含まれる場合がある（実際には大部分を占める）。しかし、同法には、同時に取得された国内間の通信データの扱いに関する規定がない。

②同条第 2 項は、私的生活形成の核心領域に影響する検索語を用いた監視を禁じている。連邦憲法裁判所はこのような領域の監視は在外外国人に対しても許されないとして、当該通信を禁止対象に含めていない同法の規定を不十分であるとしている。
③情報の保有期間が短すぎ、不服申し立てに実効性がない。
④現状でも監視による権利侵害の有無を審査する組織として基本法第 10 条委員会が整備されているが、戦略的内外通信偵察を統制する組織としては不十分な点があるとしている。具体的には、その委員を専任の職とせず名誉職としている点や委員全員には法曹資格を要求していないことが挙げられている。

そして、決定は、結論として、連邦憲法裁判所は、G10 法第 5 条第 1 項第 3 文第 8 号の規定は、比例原則の観点において全面的には正当化されず、基本法第 10 条第 1 項に保障する通信の秘密を侵害すると判断し、政府に 2026 年 12 月 31 日までに、憲法違反とされた部分の制度の改訂を行うように命じたのです。

Q7　政府は、国会議員に対して、ドイツの問題はクリアしていると説明していると聞きましたが、どんな説明をしているのでしょうか。また、それは本当でしょうか。

A　この点について、政府は、国会議員への説明において、「ドイツは内部・外部の定義が属人主義であったので憲法裁判所が指摘する問題が生じたが、日本の法案は属地主義をとっている。外国に位置するサーバーから日本に位置するサーバーに送られる者がいない通信を国内通信と定義し、実際どのような属性の人が通信を行っているかは問わないので、ドイツの問題はクリアしている。」と説明しています（前記福島瑞穂議員に対する説明）。

わかりにくいですが、ドイツではドイツ市民とドイツで暮らす外国人の間での通信、国境を超えない通信は収集しないとされているのです。

しかし、この政府の説明によると、日本では、通信自体が国内で完結せず、外国のサーバーを経由する通信（ほとんどの私たちの通信はそのようなものとされています）は、の国内の日本国民や日本で暮らす外国人間の通信であったとしても、内内通信として取得から除外されるわけではないということになります。

日本政府の説明は、内内通信として取得から除外される通信はほとんどないと言っているのであり、国内の通信は政府に取得されないという政府の説明は、著しくミスリーディングなものだといえます。

Q8 ドイツの連邦憲法裁判所の判断の内容を詳しく説明してください。

A8　2024 年 10 月 8 日ドイツ連邦憲法裁判所決定（1 BvR 1743/16, 1 BvR2539/16.）が、今回日本政府が、提案している法律案と同様の法制度について判断したものです。

この決定は、信書、郵便及び通信の秘密の制限のための法律 1（以下「G10 法」。資料 3 参照）における、連邦情報庁（情報局）による「戦略的通信偵察（strategische Fernmeldeaufklärung）」に関する規定について扱ったものです。

2016 年に、国内外の人権団体等が、ドイツと外国の間の通信に関する監視（以下「戦略的内外通信偵察」）を理由とした通信の秘密の制限について規定する G10 法第 5 条第 1 項第 3 文

第 8 号の規定並びにこの権限の行使に関連する G10 法及び連邦憲法擁護庁法 2 の規定を対象として、連邦憲法裁判所に対し違憲の訴えを申し立てました。

この訴えに対して、連邦憲法裁判所は、申立人の訴えの一部を認容し、2024 年 10 月 8 日に、次のような内容の決定を下しました。

連邦憲法裁判所は、他国からのサイバー脅威を早期に検知することを重要な公共の利益として認めた一方で、G10 法の規定には①内内通信の取扱いに関する規定の不備、②在外外国人の通信における私的生活形成の核心領域 3 に関連した規定の不備、③実施記録の消去期限、④審査機関の体制の観点から問題があると指摘しています。

①G10 法第 5 条第 1 項第 3 文第 8 号は、監視対象を内外通信に限定しているものの、戦略的内外通信偵察の際に取得したデータには、国内間でのやり取りに関するデータが含まれる場合があります（実際には大部分を占める）。しかし、同法には、同時に取得された国内間の通信データの扱いに関する規定がないと指摘されています。

②同条第 2 項は、私的生活形成の核心領域に影響する検索語を用いた監視を禁じています。連邦憲法裁判所はこのような領域の監視は在外外国人に対しても許されないとして、当該通信を禁止対象に含めていない同法の規定を不十分であるとしています。

③戦略的内外通信偵察の実施に関する記録の消去期限は、一律、記録年の翌年末まで（同項第 6 文）とされていますが、偵察による監視措置については、措置終了後対象者に通知されることになっているため、通知の時点でこの期限が過ぎていることもあり得る。対象者の権利侵害の救済の観点から、このような場合の想定を欠く規定は問題であるとしています。

④現状でも監視による権利侵害の有無を審査する組織として基本法第 10 条委員会が整備されているが、戦略的内外通信偵察を統制する組織としては不十分な点があるとしています。具体的には、その委員を専任の職とせず名誉職としている点や委員全員には法曹資格を要求していないことが挙げられます。

結論として、連邦憲法裁判所は、G10 法第 5 条第 1 項第 3 文第 8 号の規定は、比例原則の観点において全面的には正当化されず、基本法第 10 条第 1 項に保障する通信の秘密を侵害すると判断しています。ただし、同裁判所は、現行規定が直ちに違憲無効となるとは判断せず、上記の問題点に関する改正が行われるまで、最長で 2026 年 12 月 31 日まで、その効力の継続を認めています。

ドイツ連邦憲法裁判所は 16 名の裁判官で構成され、女性が 9 人、男性が 7 人です。

Q9　自分はやましいことをしていないから、政府から監視されても平気ですという友人がいます。どのように、反論したらよいでしょうか。

A9　市民の間には、自分はやましいことをしていないので、政府に監視されても平気だ、サイバー攻撃から守ってもらうことの方が大事だという意見が存在しているのは確かですね。

こういう議論は、盗聴法＝通信傍受法の制定の時からありました。通信傍受法は、通信の秘密の例外として許されてきました。しかし、通信傍受のためには、一定の犯罪の捜査のために必要であるという状況があり、裁判所が令状を発していることが必要です。期間にも制限があります。

市民に対する監視は、市民の表現の自由にブレーキをかける恐れがあります。

この点については、昨年 9 月に名古屋高裁で原告の勝訴が言い渡された「岐阜県大垣警察市民監視事件」の判決が、とてもわかりやすく、そして正しいことを述べています。

市民が発信した情報を公権力が広く収集し、分析しているとすると、市民が自ら情報発信すること自体を躊躇する可能性があること、情報発信する内容についても、心理的抑制が働き、自由な情報発信に対する事実上の制約が生じることは明らかであり、憲法で保障された表現の自由（21 条１項）や内心の自由（19 条）に対する間接的な制約になるとの判断が示されているのです。

大川原化工機事件における警察・検察の違法捜査の真実を明らかにしたのも、警察、検察による違法な行為について良心ある公安警察官が行った勇気ある内部告発の力でした。しかし、政府が広汎にネット情報を集めている社会では、内部告発者は、ジャーナリストにつながる方法がありません。このような社会では、内部告発自体が成り立たなく可能性があるのです。

自分が平気ではなく、社会全体にとって、重要なコミュニケーションが成り立たなくなるということを、説明する必要があります。

Q10 スノーデン氏が告発したアメリカ政府の XKEYSCORE システムに日本政府も組み込まれているのでしょうか

A10 アメリカの国家安全保障局（NSA）の元職員であるエドワード・スノーデン氏がその存在を暴露したスパイのグーグルとも呼ばれる XKEYSCORE は、イギリス、メキシコ、ブラジル、スペイン、ロシア、日本などに監視施設を持ち、これらの施設を流れる通信の「全てのデータ」を収集しているといわれます。

このシステムも、外国情報だけを集めているという説明だったのですが、アメリカの情報機関は、このような制約を無視して行動していたのです。オリバーストーン監督による映画スノーデンにも適切に描かれていますが、政府が XKEYSCORE の実情について国民を欺いていたことが、スノーデン氏の内部告発の最大の根拠だったのです。

メールやウェブ閲覧だけでなく、音声通話、PC カメラの画像、SNS、キーログ、パスワードなどまでが収集されているといいます。メールアドレスや IP アドレスなどによって、検索することが可能であり、検索結果からメール本文、SNS のチャットなどの内容を確認できるシステムとなっているのです。映画「スノーデン」をご覧になった方は、このシステムの使い方まで手に取るようにわかることでしょう。

データの収集は通信ケーブルからのデータの抜き取り、システム管理者を狙ったハッキングなど多岐にわたるといわれています。XKEYSCORE はカナダ、ニュージーランド、イギリス、日本にも提供されています。日本では防衛省情報本部電波部に提供されているとのことです。日本国内には3箇所以上の拠点があり、5億ドル以上を日本が負担しているとされます。

A 法案は、外国政府に「提供用総合整理分析情報」を提供することができるとしています（39 条）。政府は、提供を行うのは、例えば国家を背景とするサイバー攻撃が起こった際にパブリック・アトリビューションを行う場合などを想定していると説明しています。もちろん、この外国政府は、アメリカ、カナダ、イギリスなどのファイブアイズ国が含まれるでしょう。しかし、提供される情報にどのようなものまでが含まれるか、我々には予測することができないのです。

Q11 人の知得によらない方法で情報を振り分けるなら人権侵害が起きないのでしょうか

A 11 また、内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、サイバー攻撃に関係があると認めるに足りる機械的情報（2 条 8 項）を選別し、それ以外のものは直ちに消去すると説明しています（22 条 3 項）。

しかし、まず指摘しなければならないことは、この消去が確実になされているかどうかを確認する手続きが法案には規定されていないということです。

また、「人による知得を伴わない自動的な方法」には、AI による自動選別や、取得したメタ情報に特定の用語で検索をかける方法などが含まれることでしょう。ドイツでは、プライバシー保護の観点から特定の用語を用いた検索を禁止していますが、日本の法案にはそのような縛りはありません。「人による知得を伴わない」から、人権侵害が起きないという論理は子供だましのようなもので、AI による高速で大規模情報処理とセットにされることによって、むしろ人権侵害の可能性、危険性は飛躍的に高まっていると言えます。

ドイツ連邦憲法裁決定は、私生活の中核からデータを標的に傍受することは、他の国に所在する人物に関しても許されず、私生活の核心に関する検索用語をそのような人物に対して使用してはならないとし、他の国に所在する者に関して、この点に関して十分に具体的かつ明確な保障がないと決定は述べています。

このような、ドイツの憲法裁判所決定と、法案の関連については、立憲民主党の部門会議（2 月 13 日）でも問題となりました。立憲民主党の平岡秀夫議員は、政府にドイツの連邦憲法裁判所決定において違憲とされた論点について、日本の法案に即してクリアされているとする理由を書面で説明するよう求めましたが、納得できる説明はなされませんでした。

Q12 サイバー通信情報監理委員会という政府から独立した監視機関をつくるので人権侵害が起きる心配はないと政府は説明していますが、大丈夫でしょうか

A12 政府が設立する「サイバー通信情報監理委員会」が、真に独立性・実効性のあるものとなるかどうかは疑問です。

この機関は、プライバシー侵害が起きていないかどうかを監督する機関としては設計されていません。むしろ、情報の漏洩がないかを監視する組織、さらには政府がサイバー攻撃をするときに事前または事後的にこれを承認することを主要な任務としています。したがつて、国際的な基準を満たす独立性と専門性を持った、市民のプライバシー保護のための独立機関としての制度設計にはなっていないのです。

Q 13 無害化措置とは何をするのですか？ 何のために必要なのですか？

A 13 無害化とは、サイバー攻撃を行おうとしている者の攻撃を止めるため、当該サイト内にアクセスし、その機能を止めるため、コンピューター・ウィルスなどを使用して、これを止めることです。

当該サイトが、海外にある場合が主として想定されていて、他国に対して、無害化する措置は、

その主権を侵害する行動であり、緊急避難に当たらない限り、国際法違反となるものです。

B 法案は、前述したとおり、無害化措置と名付けられてはいますが、このように、国が、先制的なサイバー攻撃を行うことの根拠規定として、警職法と自衛隊法などを整備する法案となっています。警職法を根拠に、他国における警察の行動を合法化しようとしているのです。

しかし、このような法案を提案する前に、サイバー攻撃に対する対処としては、第一に防御を固めること、サーバー管理者に機能停止（テイクダウン）を依頼すること、さらに、攻撃者を公表し非難する（パブリック・アトリビューション）など、他にもいくらでも手段があります。このような制度を提案する前に、このような措置を本当にやりつくしたのかが問われなければなりません。

Q 14 サイバー攻撃に関する国際的な法規範をまとめた規則であるタリン・マニュアルとは、何ですか？ 誰がつくったものですか？

A 14 タリン・マニュアルとは、ロシアによる大規模なサイバー攻撃を受けたエストニアのタリンの街に、サイバー攻撃に関する国際法の専門家である研究者と実務家が集まって作成した民間団体の成果物です。民間団体が作成したものですが、西側諸国をはじめとする多くの国家の共通認識とほぼ一致したものであると日本政府も説明しています（中谷和弘他著「サイバー攻撃の国際法 タリン・マニュアル2・0の解説 増補版」参照）。

2013 年には「有事・ 戦時」を念頭に置いた『タリン・マニュアル 1.0』が、2017 年には「平時」を念頭に置いた『タリン・マニュアル 2.0』が、それぞれ Cambridge University Press から刊行されています。この作業には、日欧米諸国出身の専門家だけでなく、中露等出身の専門家が携わった点が注目されます。

タリン・マニュアルは、規則 1 で、「国家主権の原則は、サイバー空間において適用される」こと、規則 4 で、「国家は、他国の主権を侵害するサイバー行動を行ってはならない」ことを明示しています。法案がこの原則に従っているかどうか、極めて疑問です。

タリン・マニュアルも、規則 20 において、「国家は、他国が自国に対して負う国際法上の義務違反への反応として、対抗措置をとる権限を有する。」としていますが、規則 22 では、「対抗措置は、基本的人権に影響し、禁止された戦時復仇に該当し、または強行規範に反する行動を含むことはできない。対抗措置をとる国家は、外交上または領事上の不可侵に関する義務を履行しなければならない。」とも定め、厳しく制約しています。

そして、最も重要な規則 26 では、「国家は、根本的な利益に対する重大で差し迫った危険を示す行為への反応として、そうすることが当該利益を守る唯一の手段である場合には、緊急避難を理由として行動することができる」としています。そして、規則 73 は、このような行動には「侵害の切迫性」も求めています。

日本政府が「サイバーセキュリティに関する国連政府専門家会合最終会合（GGE）」で示している、「国連憲章を含む既存の国際法がサイバー空間に適用される」という認識は、このようなタリンマニュアルと共通するものです。このような認識に則れば、他国の主権を侵害したり、他国のインフラを破壊したり、国際法上の武力攻撃に該当する規模・効果を持ったりする可能性のある無害化＝サイバー先制攻撃は行ってはいけないということになるはずですが、日本政府は GGE で示した認識を現在も維持しているのか、それともこのような認識を転換させたのか、明らかでは

ありません。
　この点について、平岡秀夫議員の質問に対して、政府は次のように答弁しています。
「国連憲章全体を含む既存の国際法がサイバー行動にも適用されるということは、国連における議論を通じて確認をされています。
こうした国際社会における議論を踏まえ、サイバー行動に適用される国際法に関する日本政府の基本的立場として、国連憲章全体を含む既存の国際法はサイバー行動にも適用されるとの認識を示しました。その上で、紛争の平和的解決に関しては、サイバー行動が関わるいかなる国際紛争も、国連憲章第二条3及び第三十三条に従って、平和的手段によって解決されなければならないとの考えを示しました。」（3 月 21 日内閣委員会）
　また、3 月 28 日の参考人質疑では、立憲民主党が推薦した、防衛大学校の黒崎将広教授は「有識者会議の提言においても、意図せず措置を行うことで、達成しようとしていたものとは異なる結果に至った場合の対応についても、十分検討しておく必要がある。」「安全保障と人権保障の適切なバランスをとり、選別対象となる機械的情報の範囲や選別基準を適宜見直していくべきである。」「日本による措置を武力の行使だと批判する国が出てくる可能性は否定できず、平素から辛抱強く対外的に説明し、理解を得ていくことが課題になる」「自国が国際法を誠実に履行する体制をしっかり構築しておかないと意味がありません。」と述べています。
　国内での違法性の議論と国際法的な違法性の議論の間に溝があるという重要な指摘であり、参議院段階で、徹底して議論すべきポイントです。
　4 月 2 日の審議では、上村議員の質問に対して、タリンマニュアルについて「NATO の公式見解ではないものの、この分野の議論にあたっては極めて有益なものである」と答えています。

（防衛大学校の黒崎将広教授）

Q 15 なぜ、私人がやれば違法な行為を国がやることができるのか？ 国際法上、そのようなことは許されるのか

A 15　不正アクセス行為禁止法（1999年）、さらに は刑法改正（2011年）により、不正に他人のコンピューターにアクセスしてデータを書き換えたり、データを取得したりする行為、他人のコンピューターにコンピューターなどについて犯罪として処罰する規定がつくられてきました。そして、 犯罪捜査のために、リモートアクセスやサーバーへの捜索・差押などの手続きも進められるようになっています。

2013年には、サイバーセキュリテイ基本法が制定されている。事業者・教育研究機関、行政機関におけるサイバーセキュリティ対策が進められています。

国境を越えるサイバー攻撃についてサイバー犯罪から社会を保護するための国際的な協力体制を確認したヨーロッパ評議会起草のサイバー犯罪条約が2012年に発効しています。

2024年12月には、国連サイバー犯罪条約が国連総会で採択されています。この条約の起草過程は、日米欧諸国、中国・ロシア、グローバルサウスの複雑な関係を克服して成案化された。

ただ、この条約案については、人権団体から大きな懸念が表明されています。この条約の起草はロシアが主導したものです。強権国家が反体制派の監視を目的として条約を悪用するのではないかとの懸念が米欧からは表明されています。

条約はネット上の不正アクセスや児童ポルノ拡散などの犯罪捜査で国際協力のあり方を定めたほか、途上国に対するネット犯罪の取り締まりに向けた技術支援が盛り込まれている。

もともと2001年に欧州評議会が別のサイバー犯罪条約を採択し、日米など75か国が批准しているが、未批准のロシアが「西側諸国による不完全なものだ」（国連外交筋）として包括的な新条約が必要だと主張し、22年に交渉が始まった。米欧は採択の前提として、「表現の自由」の抑圧や差別につながる捜査について、協力要請を拒否できる条項を明記するよう要求し、当初、ロシアや中国は反発したが、最終的に盛り込まれています。しかし、ヒューマンライツウォッチなどの人権団体は新条約への懸念を強めています。国際人権団体ヒューマン・ライツ・ウォッチは声明で「条約は人権保護が不十分で政府のインターネットに対する監視を拡大し、世界中のジャーナリストや活動家などに対する弾圧の法的手段となる」と非難し、各国に署名・批准しないよう呼び掛けています。このように、サイバー犯罪に対する国際的な取り組みの枠組みについては、発展途上であるといわざるを得ませんが、国際的な合意を積み上げて、対策をしていくべき問題であることは間違いがありません。

このように、B 法案は、サイバー攻撃を行おうとしている者に対して、私人が行えば、不正アクセス、電磁ウィルス使用などの刑事法上の犯罪に問われる違法な行動を、国として敢行しようとしていることになります。

これは憲法9条に反する先制攻撃にもなりうる行動です。この点に関して政府は国会議員に対する説明で次のように述べています。

「サイバー攻撃は時間との闘いで、『誰が背後にいるのかわからないと対処できない』という状態では国民を守ることが出来ない。そこで、警職法・自衛隊法を改正し、現在では不法行為にあたる行為を法律行為にした。自衛隊法まで改正するのは、基本的に国家を背景とする攻撃に備えるためである。」「政府が一番恐れているのは、実際の軍事行動を起こす直前にインフラを機能不全にする、もしくは軍事行動を起こさなくても社会に混乱を引き起こすことを目的にしたサイバー攻撃である。」（前記福島瑞穂議員に対する説明）

しかし、法案は国家を背景とした攻撃だけを対象としておらず、日本の私企業や個人を守ることも目的としているように読めます。国の存立にかかわる攻撃だけを未然に防ぐという建付けになっていないのです。

Q 16 政府は、このような措置は諸外国も多くの国で実施されていると説明していますが、本当ですか

A 16 海外の実態は闇の中であると言わざるを得ません。政府は海外にもこのような例は多くあると説明し、法案の提案の根拠としています。しかし、海外の実態には不明な部分が多く、有識者会議の資料の中で、カナダやアメリカなどの断片的な説明がみられるだけです。また、秘密裏に行われていて、資料がないとも説明されているのです。

4 月 4 日の新聞「赤旗」一面に、カナダのビクトリア大学で社会学を教えておられる小笠原みどりさんのインタビュー記事が掲載されています。一面と二面に展開している大きな記事ですが、この法案制定の背後にいるのがアメリカ政府であることが説明されています。小笠原さんのお話を聞くと、カナダでも、2015 年に諜報機関に違法行為を許す C51 法＝反テロリズム法が制定され、2019 年には、国が能動的サイバー作戦を行う C59 法＝国家安全保障法が制定されたということです。この C59 法が、今回の法案にそっくりだと説明されています。

海外の実例、その主体、法的根拠、過誤が起きた場合の対応など、カナダの例の問題点も含めて、しっかりと勉強する必要があります。

この点についても、平岡議員が、立憲民主党の部門会議（2 月 13 日）で、政府が海外で行われてきたと称するサイバー攻撃への反撃の事例について、その内容とその法的な位置づけを書面で説明するよう求めました。しかし、十分な回答はなされませんでした。

Q 17 警職法、自衛隊法を改正して、警察官、自衛官が無害化措置を実施するということですが、どのような条件で措置ができるのですか。

A 17 B 法案は、警察が対処する場合には、法案の定める「サイバー攻撃又は「その疑いがある通信等を認めた場合であって、そのまま放置すれば、人の生命、身体又は人の生命、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」を要件としています（B 法案 2 条による警職法 6 条の 2 の新設）。

また、自衛隊が対処するべき場合の加重要件としては、「本邦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ものが行われた場合において、自衛隊が対処を行う特別の必要があると認めるとき」を求めています（B 法案 4 条による自衛隊法 81 条の 3 などの新設）。

この法案の定めている攻撃の要件は先に紹介したタリン・マニュアルよりはるかに広汎です。米欧諸国が認めるサイバー攻撃に関する国際規範といえるタリン・マニュアルでは「（国の）根本的利益に対する重大で差し迫った危険」「利益を守る唯一の手段である場合」を緊急避難に当たるとするための要件と定めていました。

警職法改定案の「そのまま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…加害関係電子計算機の動作に係るものをとることを命じ、又は自らその措置をとることができる」とされ、タリンマニュアル規則 26 で規定される緊急避難の要件「国家の根本的利益に対する重大で差し迫った危険」「当該利益を守る唯一の手段」を満たしていません。このように国家の緊急避難・正当防衛とかけはなれた要件に基づく無害化措置をとることは許されません。

現職の外務省国際法局長であり、京都大学で国際法学の博士号を取得している研究者でもある中村和彦氏の近著『越境サイバー侵害行動と国際法』も、189 ページから 204 ページの「考察」において、国家がサイバー行動を行う要件として、「脅かされる利益が不可欠のものであること/危険が重大であること/危険が急迫したものであること/反撃の措置が唯一の措置であること/他国の不可欠な利益を深刻に損なうものでないこと/自国が緊急事態発生に寄与していないこと」を摘示しています。

このような厳しい要件は、B 法案の中には見いだすことはできません。むしろ、B 法案では、個人や日本企業の経済上の利益を守るために、日本の警察や自衛隊が海外のサーバーに対する攻撃ができるようにしか読めないのです。

Q 18 実際に特定国を起源とするサイバー攻撃に対応して日本の警察や自衛隊が無害化の措置を講じた場合に、最悪どんな事態になりえますか？

A 18 前述したタリンマニュアルの解説は、「重大かつ急迫した危険」については「危険を回避する最後の好機ー攻撃の計画が高い確度で判明」していることを要すると述べています（前記解説37～38頁（河野桂子コペンハーゲン大学政治学部研究員執筆部分））。

有識者会議の提言は、サイバー攻撃について次のように述べていました。

「近年、サイバー攻撃は巧妙化・高度化している。具体的には、サイバー攻撃は、複雑化するネットワークにおいて、国内外のサーバ等を多数・多段的に組み合わせ、サーバ等の相互関係・攻撃元を隠匿しつつ敢行されている。また、ゼロデイ脆弱性の活用等により、高度な侵入が行われるほか、侵入後も高度な潜伏能力により検知を回避するなど、高度化している。このため、サイバー

攻撃の特徴としては、現実空間における危険とは質的に異なり、実際にある危険が潜在化し認知しにくいということが挙げられる。また、潜伏の高度化等により、攻撃者の意図次第でいつでもサイバー攻撃が実行可能であるとともに、ネットワーク化の進展により、一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれがある。」

このように、サイバー攻撃を敢行する者たちは、みずからの正体を隠して攻撃してくることが考えられるのです。

多段階のサーバーを踏み台に攻撃してくるというのは政府自身の説明でした。だとすれば、サイバー攻撃の犯人であると考えて、A 国のサーバーを攻撃したところ、実はその攻撃は A 国を偽装した B 国のサイバー部隊によるものだったということは、十分にありうることです。

このように、偽情報に釣られて、誤った対象を攻撃し、攻撃対象国の逆鱗に触れれば、偶発的にミサイル攻撃を招いてしまう危険性は架空のものでなく現実的な蓋然性があると考えられるのです。

また、日本の警察や自衛隊が無害化＝サイバー攻撃を敢行した場合に、この事実を公表するでしょうか。小倉利丸氏は、日本政府が無害化の措置をとったことを公表することはありえないだろうと指摘しています（小倉利丸「サイバースパイ・サイバー攻撃法案批判」2025 DaRa Revo 82-85 頁）。この点は、きわめて重要です。衆院の最終盤で、立憲民主・自民間で合意した法案の修正案でも、明らかにされるのは無害化の件数だけ、過去の海外の例を見ても明らかなように、サイバー攻撃を行った事実そのものが、経緯と対象を含めて公表される保障はありません。

有識者会議の提言では、「平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、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とすべき。」としている（提言11頁）。このような見解から考えれば、攻撃が反撃を呼びエスカレートしていく危険性は現実的なものといえます。

こうしたリスクは、「独立」機関による事前承認・緊急の場合の事後報告という制度では排除することができないのです。

このように、無害化のための B 法案は極めて危険で、弊害が大きすぎる法案であり、修正も困難です。A 法案も、上記に述べたように、根本的に作り直す必要があると思います。この2法案の提案は撤回されるよう強く求めたいと思います。

付録一 サイバー行動に適用される国際法に関する日本政府の基本的な立場

2021 年 5 月 28 日
外務省
サイバー行動に適用される国際法に関する日本政府の基本的な立場
（下線部は海渡による）

1. 位置づけと目的
2004 年から 2017 年までの間、国連事務総長によって任命された政府専門家からなる「国際安全保障の文脈における情報通信分野の発展に関する政府専門家グループ」（以下 GGE）が国連総会決議に基づき設置された。政府専門家のコンセンサスで作成された 2013 年及び

2015 年の報告書において、特に国連憲章全体を含む、既存の国際法がサイバー行動(1)にも適用されることが確認された。国連総会の場で両報告書がコンセンサスで承認されたことにより、この認識は、すべての国連加盟国の総意となった。2015 年の報告書において、GGE は国際法がサイバー行動にどのように適用されるかにつき、様々な重要な見解を示し、同時に、この議論が継続されるべきである旨を勧告した。第 5 回 GGE では 2017 年に報告書を採択できなかったが、国際法の適用に関する議論が十分に収斂しなかったこともその一因である。その後、2019 年から、第 6 回 GGE2 において、国際法がどのように適用されるかに関する議論が活発に行われた。本年 5 月 28 日に第 6 回 GGE(2) の報告書がコンセンサス採択された。本文書は、サイバー行動に適用される国際法に関する日本政府の現時点での基本的な立場をまとめたものである。本文書は、事務総長に第 6 回 GGE の設置を要請した決議 73/266 に明記されたマンデートに従って、事務総長によって総会に提出される GGE 報告書の付属文書に含まれることを想定して、GGE 議長の求めに応じた各国による会合への寄与として作成された。本文書において、日本政府は、国連憲章全体を含む既存の国際法がサイバー行動にも適用されることを再確認した上で、既存の国際法がどのようにサイバー行動に適用されるかについて、最も重要かつ基本的な事項を示して現時点での立場を示すものである。本文書の内容は、現在行われているものを含む 6 回の GGE(現在の GGE を含め、日本政府から 4 回にわたり政府専門家が任命された)及び 2019 年に設置されたオープンエンド作業部会(OEWG)における議論、日本政府と各国政府との二国間・複数国間協議における議論の他、NATO サイバー防衛協力センターの支援による日本等の NATO 以外の国籍を有する専門家が個人的資格で作成したタリン・マニュアル 1.0 及び 2.0 等の政府以外の研究成果や日本政府が主導したものを含むマルチステークホルダーの議論を踏まえたものである。

日本政府は、サイバー行動に適用される国際法に関して、多数の国の政府の基本的立場が公表され、国際裁判や国内裁判で国際法が援用されることによって、国際法がサイバー行動にどのように適用されるのかに関する国際的な共通認識が深まることを期待する。日本政府は、そのような共通認識が深まることによって、特に、サイバー空間におけるいかなる行動が国際法違反であるか、サイバー行動によって法益侵害を受けた被害国が、国際法上どのようなツールを用いることができるかに関する共通認識が形成されることによって、サイバー空間における悪質な行為が抑止されることを期待する(3)。日本政府は国連の場におけるものを含め、関連の議論に積極的に参加し続ける方針である。

なお、サイバー行動に適用される国際法はここで言及されているものにとどまらない。日本はサイバー犯罪に関する条約に参加しているが、サイバー犯罪に関する条約はサイバー行動に適用される重要な国際法である。また、日本が CPTPP、日米デジタル貿易協定、日英 EPA 等でルール化を進めている DFFT に関する条約上の規定も、サイバー行動の一側面に適用される、国際法の一部である。

2. サイバー行動に適用される国際法

(1)既存の国際法及び国連憲章

国連憲章全体を含む既存の国際法はサイバー行動にも適用される。

2015 年 GGE 報告書は、国家による責任ある行動に関する拘束力のない自発的な規範を

11 項目記載している。これらは、政府専門家間で少なくとも規範として履行しなければならないものとして合意された項目であるが、その中にも、国際法上の権利義務を確認したもの及び国際法上の権利義務に関連するものが含まれている。11 項目に記載があることを以て既存の国際法上の権利義務が消滅したり変更されたりすることはない。

(2)主権侵害と不干渉原則

国家は、サイバー行動によって他国の主権を侵害してはならない。また、国家は、サイバー行動によって他国の国内管轄事項に干渉してはならない。

不干渉原則については、サイバー行動が、威圧を含むニカラグア事件判決(1986 年)(4)で明確化された要件を満たす場合には違法な干渉となり得る。

一方、このような不干渉原則とは必ずしも一致しない主権侵害について、常設国際司法裁判所は、ロチュース号事件判決において、他国領域内での権力行使は国際法上禁止されると判示し(5)、パルマス島事件仲裁判決において、仲裁裁判所は「国家間の関係においては、主権とは独立を意味する。地球の一部分に関する独立とは、他のいかなる国家をも排除して、そこにおいて国家の機能を行使する権利である。」と述べている(6)。これら及びその他の判決を考慮すれば、日本政府としては、不干渉原則により禁じられる違法な干渉とは必ずしも一致しない主権侵害が存在すると考えてきている。

また、主権侵害について、国際司法裁判所(ICJ)は、ニカラグア事件判決(1986 年)において、米国による不干渉原則への違反を認定した上で、それらに加えて米国によるニカラグア領空の飛行の指示又は許可が他国の主権を侵害してはならないという慣習国際法に違反した旨を述べており(7)、また、コスタリカ・ニカラグア事件判決(2015 年)は、コスタリカがニカラグアの領域において権威を行使した証拠がないことを、コスタリカが領土一体性及び主権を侵害したとのニカラグアの主張を退ける理由として挙げている(8)。これらを踏まえれば、主権侵害は違法な干渉に当たらなくとも国際法違反を構成する場合がある
と考えられる。

医療機関を含む重要インフラに対するサイバー行動によって物理的被害や機能喪失を生じさせる行為は、場合によっては違法な干渉等にも当たり得るが、いずれにせよ主権の侵害に該当し得ると考える(9)。主権侵害と違法な干渉の関係については、第 6 回 GGE や OEWG でも様々な意見が表明されており、国家実行や今後の議論を通じて特定されることが望まれる。

(3) 国家責任

サイバー空間における国家による国際違法行為は当該国家の国家責任を伴う。国際違法行為は、国家の作為又は不作為による国際法の一次規則の定める義務に対する違反によって生じ、サイバー行動の場合にも、国家が、主権、不干渉、武力行使の禁止等の原則、民用物への攻撃禁止等の国際人道法上の諸原則及び基本的人権の尊重等の一次規則に違反した場合は国際違法行為が生ずる。

なお、以下では参考として国際法委員会(ILC)が作成した国家責任条文に言及するが、同条文は条約として採択されておらず、個々の条文が慣習国際法を反映しているか否かについては個別に精査を要する。

(a)帰属

国家による国際違法行為は、その行為が国際法上当該国に帰属しかつその行為が当該国の国際法上の義務の違反を構成する場合に存在する。
サイバー行動における帰属の議論は、法的側面、政治的側面、技術的側面がある。
サイバー空間におけるいかなる行為についても、国際法上の国家責任を追及するためには、当該行動が特定の国家に帰属するか否かを検討する必要がある。この点については、ILC 国家責任条文第 4 条から第 11 条が参考になる。一般に、サイバー行動が国家機関によって行われている場合等は、同行動は国家に帰属すると考えられる。その上で、非国家主体によるサイバー行動は原則として国家に帰属するものではないが、ILC 国家責任条文第 8 条によれば、当該行為を行うに際して事実上国の指示に基づき、又は指揮若しくは統制の下で行
動していた場合には当該国の行為と見なされると考えられる(10)。

(b)国際違法行為を行った国家の義務
サイバー行動についても、国際違法行為に関して責任を負う国家は、次のような義務を負う。まず、その行為が継続している場合には、当該違法行為を中止しなければならず、また、事情がそれを必要とする場合には、適当な再発防止の保証を与えなければならない。そして、責任を負う国は、国際違法行為により生じた被害に対して十分な回復を行わなければならない。

(c)対抗措置・緊急避難
国際違法行為に対し対抗措置をとることは、一定の条件の下で、国際法上認められている。
一般論としては、他国による国際違法行為により侵害を受けた国は、違法行為国に対し、①国際違法行為を中止する義務や②回復の義務等の履行を促すために対抗措置をとることは、一定の条件の下で、国際法上認められている。
一般国際法上、対抗措置が先行する国際違法行為と同様の手段に限定されなければならないとの制約はなく、このことは、サイバー空間における国際違法行為に対する対抗措置についても同様だと考えられる。
また、ILC 国家責任条文 25 条に示された要件に合致する場合には緊急避難を援用することも国際法上認められていると考える。

(4)相当の注意
サイバー行動についても、国家は国際法上相当の注意義務を負う。2015 年 GGE 報告書の規範 13(c)、(f)及びパラ 28(e)の後段はこの義務に関連したものである。
ICJ は、コルフ海峡事件において「領域を他国の権利に反する行為にそれと知りつつ使わせてはならないすべての国の一般的義務(every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States)」の存在に言及している(1949 年)(11)。サイバー行動との関連では、このような意味での相当の注意義務が重要である。
その上で、相当の注意義務の概念に関連して、アラバマ号事件仲裁判決(1872 年)は、中立国の相当の注意は、中立義務の不履行によって交戦当事者の一方がさらされるおそれのあるリスクと厳格に比例すると述べ(12)、また、ジェノサイド条約適用事件 ICJ 判決において、ICJ は、

ジェノサイド条約上の防止義務の性質を相当の注意義務と解していると見られ、ジェノサイドを可能な限り防止するためにジェノサイドを行いそうな主体に対して影響を与える能力を行使することが締約国の義務であるとした(13)。

サイバー行動に関する相当の注意義務に基づく領域国の義務の内容の外縁は必ずしも明確ではないが、これらの相当の注意義務の概念に関連した ICJ 判決も参照すれば、サイバー行動の重大性や、領域国の攻撃主体に対する影響力等を考慮して、当該義務の範囲を個別具体的に検討する必要があると考えられる。

上記を踏まえれば、少なくとも、例えば、他国の重要インフラを害するといった重大で有害な結果をもたらすサイバー行動について、ある国が、同国が財政的その他の支援を行っている自国の領域に所在する者又は集団がそのようなサイバー行動に関与している可能性について信頼に足る情報を他国から知らされた際には、当該者又は集団がそのようなサイバー行動を行わないように、当該情報を知らされた国が保持している影響力を行使する義務等は、上記の考え方に鑑みると、相当の注意義務に基づく当該領域国の義務に含まれると解される。

また、サイバー行動の特徴の一つとして、国家への帰属の判断が困難なことが挙げられる。この点、相当の注意義務は、国家に帰属しないサイバー行動に対しても、同行動の発信源となる領域国に対して、国家責任を追及する根拠となり得ると考えられる。たとえ国家へのサイバー行動の帰属の証明が困難な場合でも、少なくとも、相当の注意義務への違反として同行動の発信源となる領域国の国家責任を追及できる。

(5)紛争の平和的解決・武力行使の禁止・自衛権

(a)紛争の平和的解決

サイバー行動が関わるいかなる国際紛争も、国連憲章第 2 条 3 に従って平和的手段によって解決されなければならない。また、国連憲章第 33 条に従って、サイバー行動が関わるいかなる紛争でもその継続が国際の平和及び安全の維持を危くする虞のあるものについては、その当事者は、まず第一に、交渉、審査、仲介、調停、仲裁裁判、司法的解決、地域的機関又は地域的取極の利用その他当事者が選ぶ平和的手段による解決を求めなければならない。また、紛争の平和的解決のため、国連憲章第 6 章及び第 7 章に基づく安全保障理事会の権限や同憲章第 14 章及び国際司法裁判所規程に基づく同裁判所を含む他の国連機関の任務はサイバー行動に伴う紛争においても活用されるべきである。

(b)武力行使の禁止

サイバー行動であっても、一定の場合には、国連憲章第 2 条 4 が禁ずる武力による威嚇又は武力の行使に当たり得る。同条に基づき、すべての国家は、その国際関係において、武力による威嚇又は武力の行使を慎まなければならない。

日本政府は、武力による威嚇とは、一般に、現実にはまだ武力を行使しないが、自国の主張、要求を入れなければ武力を行使するとの意思、態度を示すことにより、相手国を威嚇することをいうと考えている。国際関係における武力による威嚇又は武力の行使を慎む義務はサイバー行動に関する重要な義務である。

(c)自衛権

サイバー行動が、国際連合憲章 51 条にいう武力攻撃に当たる場合には、国家は、国際連合憲章第 51 条において認められている個別的又は集団的自衛の固有の権利を行使することが

できると考えられる。

(6)国際人道法

サイバー行動にも国際人道法は適用される。

武力紛争下においては、紛争当事者の戦闘方法や手段等は規制されるが、紛争当事者によって実施されるサイバー行動も、国際人道法の規制を受ける。人道性原則、必要性原則、比例性原則、区別原則を含む国際人道法上の諸原則はサイバー空間における行為にも適用される。2015 年 GGE 報告書パラ 28(d)でこれらの原則が「確立された国際的な法的原則」であると記されているので、同報告書が既存の国際法の適用を確認していることと合わせて読めば、同報告書はこれらの原則の適用を確認していると解釈される。また、ジュネーヴ諸条約第 1 追加議定書第 49 条においては、「「攻撃」とは、攻勢としてであるか防御としてであるかを問わず、敵に対する暴力行為をいう」とされている(14)(15)。日本政府としては、サイバー行動についても、例えば軍事目標の破壊または機能停止を生じさせるものは、場合によっては国際人道法上の「攻撃」に該当し得ると考える。

国際人道法の適用に際しては、基本的に「武力紛争」の存在が前提とされている。ジュネーヴ諸条約には「武力紛争」について特段の定義は置かれておらず、ある事態が「武力紛争」と評価できるか否かについては、実際の戦闘行為の態様や各紛争当事国の意思等を総合的に検討して個別具体的に判断すべきものと考えられるが、サイバー行動の効果を考慮すれば、サイバー行動のみによって「武力紛争」が発生することはあり得ると考えられる。

サイバー行動に国際人道法が適用されることを確認することは戦闘方法や手段等の規制に資するのであり、サイバー空間の軍事化につながるとの主張は根拠がない。例えば、武力紛争下における医療機関に物理的被害や機能喪失を生じさせるサイバー行動は、国際人道法違反を構成し得る(16)と考えられ、適切に規制されるべきである。他方で、従来空間における戦闘様相と異なるサイバー空間において、戦闘員の範囲等については、国際人道法がどのように適用されるのか、今後議論していく必要がある。

(7)国際人権法

国際人権法は、サイバー行動にも適用される。個人は、サイバー行動に関して、他で享受するのと同じ人権を享受する。国際人権法に従い、国家は人権を尊重する義務がある。サイバー空間において尊重されるべき人権には市民的、政治的、経済的、社会的、文化的権利等、国際人権法上認められる全ての人権が含まれる。サイバーの文脈で特に関連するのは、プライバシー権、思想・良心の自由、表現の自由、適正手続の保障等である。2015 年 GGE 報告書のパラ 28(b)の最後の一文は以上を確認するものである。同報告書の規範 13(e)は国際人権法上の義務を一部確認するものであるが、そこに記されていない義務を変更するものではない。

注記

1 本文書において、「サイバー行動」という用語は、情報通信設備及び技術を利用した行動を意味する。

2 第 6 回 GGE の正式名称は「国際安全保障の文脈の中でサイバー空間における国家の責任ある行動を促進することに関する政府専門家グループ」である。

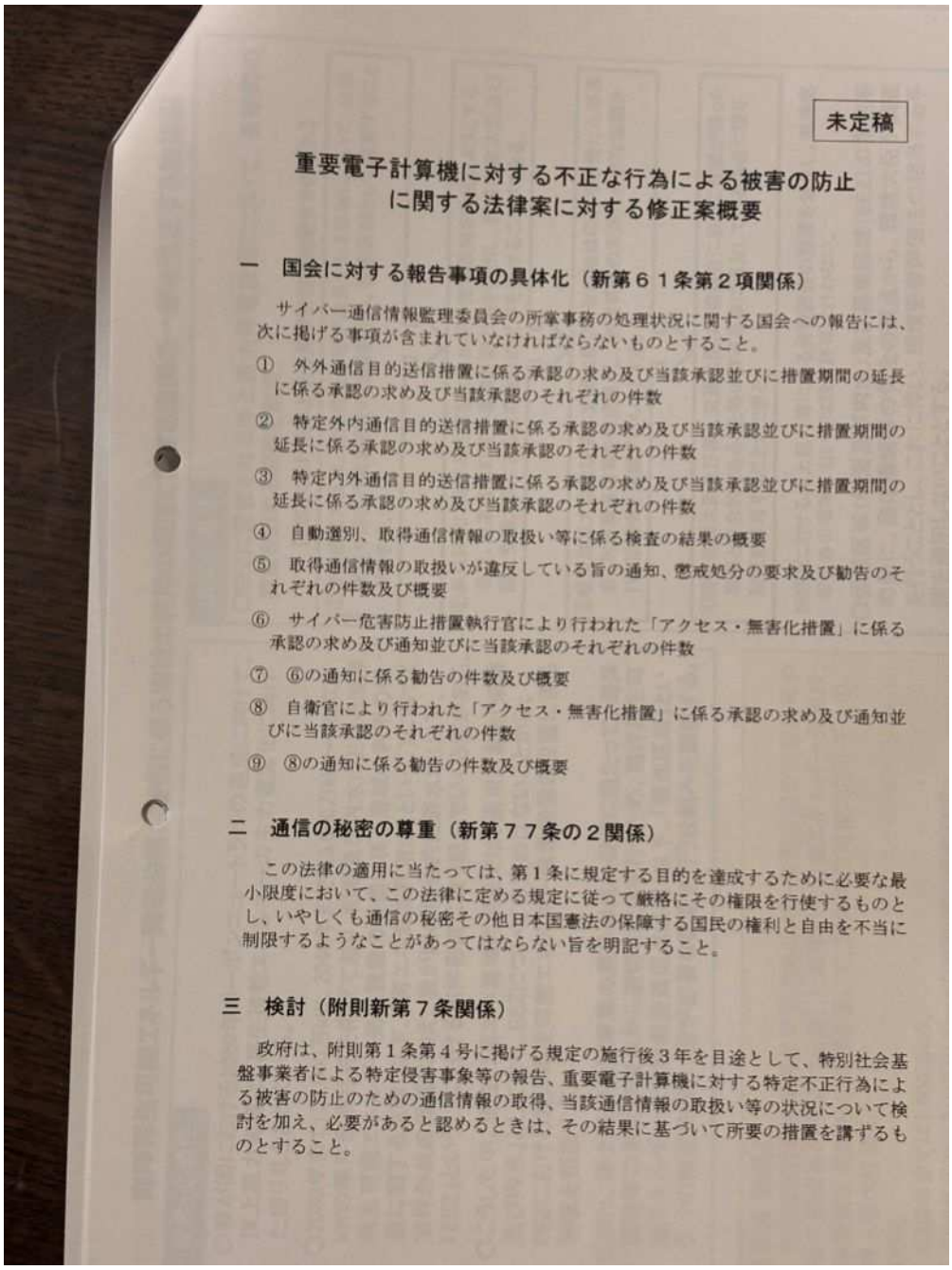
2 によって、特に、サイバー空間におけるいかなる行動が国際法違反であるか、サイバー行動に

よって法益侵害を受けた被害国が、国際法上どのようなツールを用いることができるかに関する共通認識が形成されることによって、サイバー空間における悪質な行為が抑止されることを期待する
3 「サイバー空間」という用語は、現実の空間に属しない空間の存在を意味しない。
4 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).Merits, Judgment. I.C.J. Reports 1986, p.97-98, paragraph 205.
5 The Lotus case, PCIJ, Series A, No. 10, 1927, p. 18-19.
6 Island of Palmas Case, Award, RIAA, Vol.II, p. 838.
7 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p.136-139, paragraph 292.
8 Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica), Judgment, I.C.J. Reports 2015, p. 738, paragraph 223.
9 タリン・マニュアル 2.0 は主権侵害となり得るケースとして、サイバーインフラの物理的損害が生じた場合や機能が喪失した場合にも言及している。
10 Article 8 of the ILC' s Articles on State Responsibility
11 Corfu Channel case, Judgment of April 9th, 1949: I.C.J. Reports 1949, P.22.
12 Alabama claims of the United States of America against Great Britain, RIAA, Vol XXIX, p.129.
13 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and
Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 221, paragraph 430.
14「攻撃」とは、攻勢としてであるか防御としてであるかを問わず、敵に対する暴力行為をいう(ジュネーヴ諸条約第1追加議定書第 49 条)。
15 タリン・マニュアル 2.0 では、「サイバー攻撃とは、攻勢としてであるか防御としてであるかを問わず、人に対する傷害若しくは死、又は物に対する損害若しくは破壊を引き起こすことが合理的に予期されるサイバー行動である。」とされている。
16 例えばジュネーヴ諸条約第1追加議定書第 12 条

付録二 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案に対する修正案

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案の一部を次のように修正する
〇通信の秘密の尊重(77 条の 2)
この法律の適用に当たっては第一条に規定する目的を達成するために必要な最小限度において、

この法律に定める規定に従って厳格にその権限を行使するものとし、いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない
〇国会に対する報告事項の具体化（61 条 2 項）
前項の報告には、次の各号に掲げる事項が含まれていなければならない（詳細は写真に譲る）
〇附則に次の一条を加える
　検討□第七条政府は、附則第一条第四号に掲げる規定の施行後三年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。



未定稿

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案に対する修正案概要

一　国会に対する報告事項の具体化（新第６１条第２項関係）

サイバー通信情報監理委員会の所掌事務の処理状況に関する国会への報告には、次に掲げる事項が含まれていなければならないものとすること。

① 外外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

② 特定外内通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

③ 特定内外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数

④ 自動選別、取得通信情報の取扱い等に係る検査の結果の概要

⑤ 取得通信情報の取扱いが違反している旨の通知、懲戒処分の要求及び勧告のそれぞれの件数及び概要

⑥ サイバー危害防止措置執行官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数

⑦ ⑥の通知に係る勧告の件数及び概要

⑧ 自衛官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数

⑨ ⑧の通知に係る勧告の件数及び概要

二　通信の秘密の尊重（新第７７条の２関係）

この法律の適用に当たっては、第１条に規定する目的を達成するために必要な最小限度において、この法律に定める規定に従って厳格にその権限を行使するものとし、いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない旨を明記すること。

三　検討（附則新第７条関係）

政府は、附則第１条第４号に掲げる規定の施行後３年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとすること。