サイバー安保関連法案(サイバースパイ・サーバー攻撃法案)の問題点と闘いかた

小倉利丸(JCA-NET)
toshi@jca.apc.org 070-5553-5495

2025/3/16

Table of Contents

1. 法案の通称名について

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および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等に関する法律案→「[日本政府による]サイバースパイ・サイバー攻撃法案」(あるいはサイバースパイ・攻撃法案)と呼ぶ。

2．警察の軍隊化+軍隊の警察化+民間企業との連携

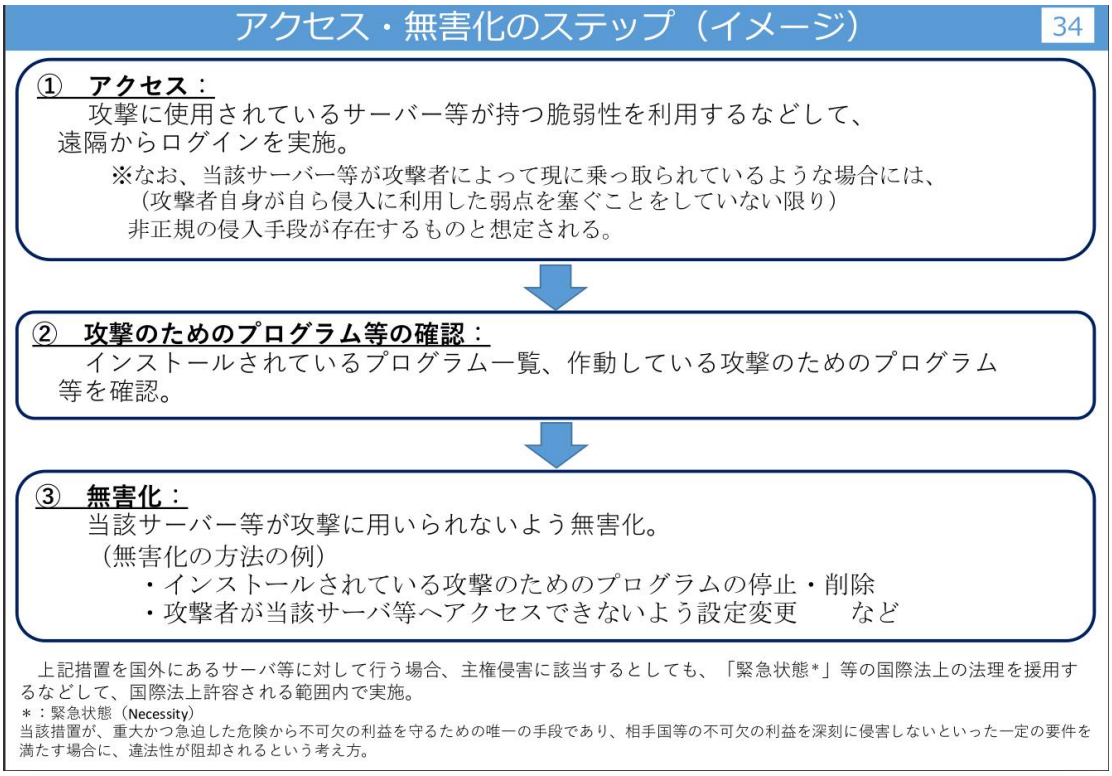
- 安保・防衛３文書の対外的な軍事安全保障。先制攻撃を含む敵基地攻撃能力との関連でのサイバー領域のスパイ・「無害化」攻撃
- 警察の役割の重視。「アクセス・無害化」の合法化を警職法に基いて整備し、新規の立法措置をとらなかった。
- 事案に応じて警察と防衛省/自衛隊の役割分担を新設の国家サイバー統括室が調整[1]

警察の軍隊化、軍隊の警察化という双方の組織性格の融合が進む危険性(警職法改正)に加えて民間企業を動員。ここでいう民間企業とは日本企業に限定されない。

2.1．法案が目指したい目標な何か

法案の説明資料：「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。[2]

基本の目的は、自衛隊、警察、政府機関や関連する民間企業による能動的サイバー防御の実施=アクセス・無害化を日本の法律上犯罪とならないように整備すること。



- 脆弱性を利用してネットを経由して侵入→「アクセス」

1 「警察・自衛隊の合同拠点新設へ□能動的サイバー防御で東京・市谷に」産経 2025/1/29 https://www.sankei.com/article/20250129-XZR6MBI3FNJH5L5JO3UD2FE7UU/ 「政府はサイバー防御の司令塔として、内閣官房に来年度、「国家サイバー統括室」を新設する。サイバー統括室が国家安全保障局 と連携し、事案の内容に応じて、攻撃元への侵入・無害化に関する警察と自衛隊の役割分担を調整する。」 国家サイバー統括室は内閣サイバーセキュリティセンター（NISC）を改組してできる組織として人員を 180 人から 230 人に増員。内閣府にはサイバー安保担当の政策統括官を配置する。(日経 2024/12/27 https://www.nikkei.com/article/DGXZQOUA278NA0X21C24A2000000/

2 内閣官房サイバー安全保障体制整備準備室「説明資料」https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

- 攻撃のためのプログラム等の確認→情報収集=スパイ行為

スパイ行為を前提として、収集した情報から「無害化」、つまりサイバー攻撃を実行する。

3．立法事実の問題点

3.1．誇張されるサイバー攻撃深刻度

法案説明資料は以下。 その下に元データを示す。

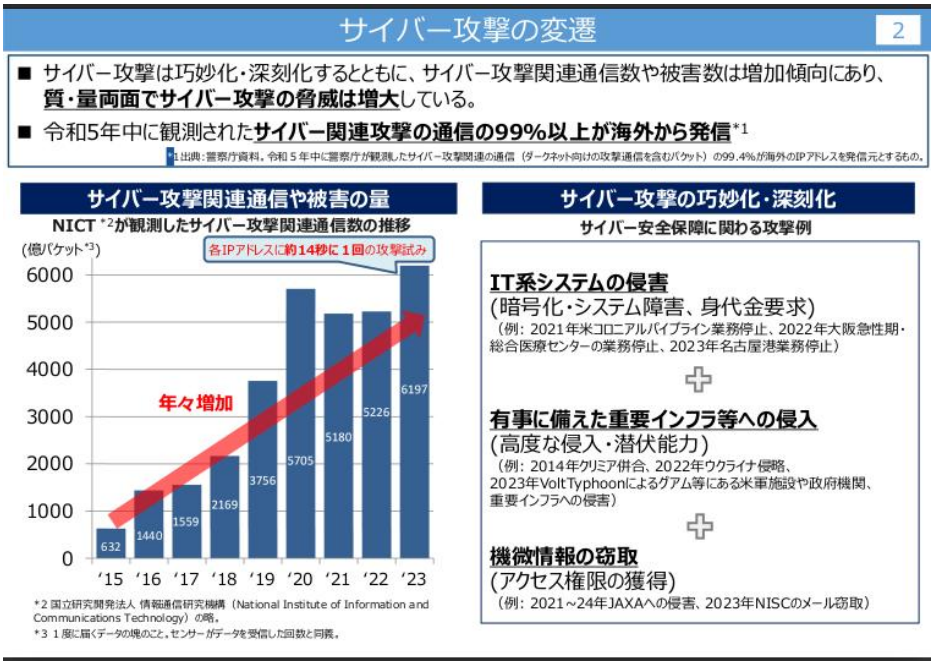


表1: 年間総観測パケット数の統計（過去 10 年間）

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレスあたりの年間総観測パケット数
2015	約 631.6 億	270,973	245,540
2016	約 1,440 億	274,872	527,888
2017	約 1,559 億	253,086	578,750
2018	約 2,169 億	273,292	806,877
2019	約 3,756 億	309,769	1,231,331
2020	約 5,705 億	307,985	1,849,817
2021	約 5,180 億	289,946	1,747,685
2022	約 5,226 億	288,042	1,833,012
2023	約 6,197 億	289,686	2,260,132
2024	約 6,862 億	284,445	2,427,977

この元データは「総観測パケット数の統計」であり攻撃数ではない。

- 攻撃数は総パケットの 4 割程度 14 秒に 1 回の攻撃：日本には通信機器が数億台は存在していることが示されていない。
- 攻撃=被害ではない。攻撃の大半は防御されている。

3.2. 実際の被害件数は？

IPA の「コンピュータウイルス・不正アクセスの届出状況」[3]の報告書によると以下のような実被害が報告されている。

- ウィルス感染：2024 年のデータでは、ウイルス届出 260 件の届出。ウイルス感染被害（実被害）15 件(ウイルス等検出数 215662)
- 不正アクセス：2024 年の不正アクセス届出は、166 件。23 年の 243 件より 77 件（約 31.7%）少ない。実被害があった届出は 132 件(全体の約 79.5%)。

など

3.3. 被害の原因：実被害届について、不正アクセスの原因別のデータ

IPA が示した「対応と対策」は、ほとんどが標的となった組織自体で対処可能なことがらであり、警察あるいは自衛隊が対処しなければならないような事態とはいえない。

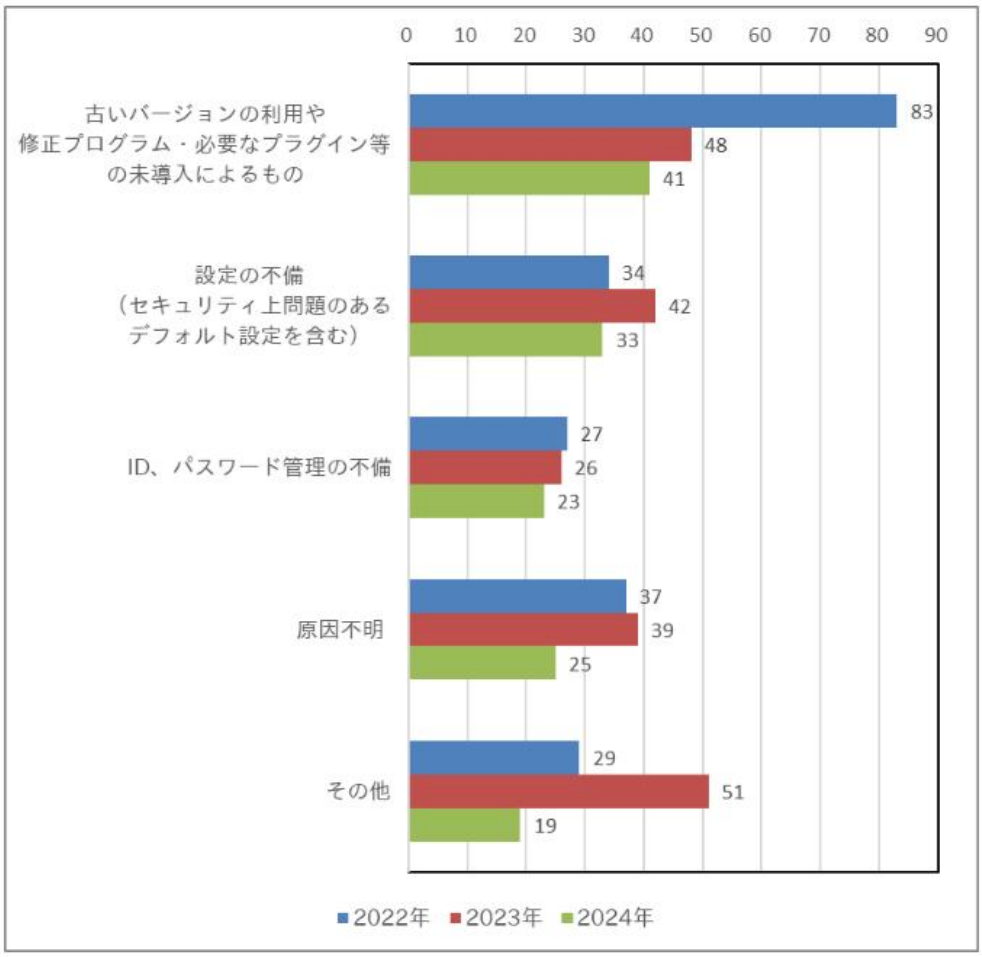
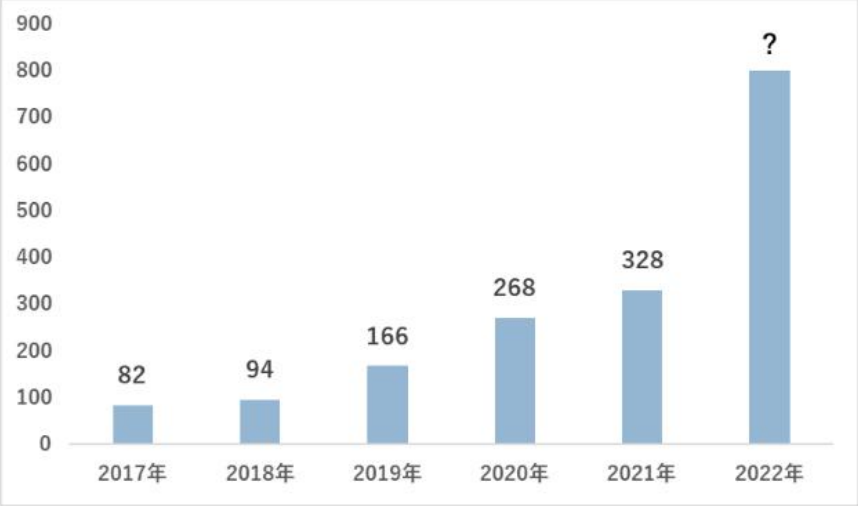


図 2-7：不正アクセス原因別件数の推移（2022～2024 年）

3 https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2024-report.pdf

報道・公表を実施する組織が年々増加していることが読み取れます。サイバー攻撃の増加もさることながら、2022年4月に施行された改正個人情報保護法の影響（被害者本人への通知が必要となったためホームページ等で公開する組織が増加したと推定）などにより、報道・公表等がなされるケースが増加していることが推測されます。



図Ⅱ-5 サイバー攻撃の公表件数の年別推移

地政学的脅威について

IPA が毎年公表している 10 大脅威のランキングで、2025 年に、はじめて「地政学的リスクに起因するサイバー攻撃」が 7 位にランキングされた。

表 1.1 情報セキュリティ 10 大脅威 2025「組織」向けの脅威の順位

順位	「組織」向け脅威	初選出年	10 大脅威での取り扱い（2016 年以降）
1	ランサム攻撃による被害	2016 年	10 年連続 10 回目
2	サプライチェーンや委託先を狙った攻撃	2019 年	7 年連続 7 回目
3	システムの脆弱性を突いた攻撃	2016 年	5 年連続 8 回目
4	内部不正による情報漏えい等	2016 年	10 年連続 10 回目
5	機密情報等を狙った標的型攻撃	2016 年	10 年連続 10 回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021 年	5 年連続 5 回目
7	地政学的リスクに起因するサイバー攻撃	2025 年	初選出
8	分散型サービス妨害攻撃（DDoS 攻撃）	2016 年	5 年ぶり 6 回目
9	ビジネスメール詐欺	2018 年	8 年連続 8 回目
10	不注意による情報漏えい等	2016 年	7 年連続 8 回目

3.4. 本当の問題はどこにあるのか

以上から

- 攻撃やスパイ活動のほとんどがセキュリティの脆弱性やセキュリティホールを狙うものである。パスワード管理を厳格にする、ソフトを最新に保つなどは、利用者やベンダーが対処するのが最速かつ確実。
- 現場のセキュリティの脆弱性やセキュリティホールへの対処は自衛隊や警察ではできない。警察や自衛隊が、当事者になりかわって措置することは、プライバシーや通信の秘密の観点からもすべきではない。
- あたかも法案が成立すればサイバー攻撃被害が防げるかのような印象操作が行なわれている。
- 地政学上のリスクの増大は政府の外交政策の失敗であり、これをスパイ行為や先制攻撃で解決することはできない。

不正アクセス、マルウェアの駆除などは当事者のセキュリティ対策によって防御できるケースが多く、警察や自衛隊の関与で解決できることはない。スパイと攻撃の目的は別にあると考える以外にない。

(結論）立法事実は意図的に水増しされており、現実問題としては立法事実は存在しないといっていい。

4. 「アクセス」=サイバースパイの問題

4.1. スパイの定義

NATO タリンマニュアル「ルール 32 – 平時におけるサイバースパイ活動」：ハーグ条約の「間諜」の定義をふまえている。

> (中略)「サイバースパイ行為」という用語は、サイバー能力を秘密裏に、または嘘の口実を使用して情報を収集する、または収集を試みる行為を指す。サイバースパイ行為には、電子的に送信または保存された通信、データ、またはその他の情報を監視、モニター、取得、または抽出するためにサイバー能力を使用することが含まれるが、これに限定されない。

日本が海外でスパイ活動を行なうことについてのは国際法上の制約は非常に低い。国内法上、自衛隊や警察のシステムへの侵入行為を合法化することが必要になる。

4.2. 法案の「スパイ」活動関連の記述例 外外通信について

法案では、「不正行為に関する実態が明らかでない」場合であっても不正行為防止のために、「サイバー通信情報監理委員会の承認を受けて」情報を収集できる。[4]不正

4 以下は外外通信の場合の条文。
> 第十七条 内閣総理大臣は、外外通信…であって、重要電子計算機に対する国外通信特定不正行為のうちその実行のために用いられる電子計算機、当該電子計算機に動作をさせるために用いられる指令情報その他の当該国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による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、かつ、この項の規定による措置以外の方法によっては当該実態の把握が著しく困難であるものに関係するものが、特定の国外関係電気通信設備…を用いて提供される事業電気通信役務が媒介する国外関係通信に含まれると疑うに足りる場合において、必要と認めるときは、当該国外通信特定不正行為に関する第二十二条第二項に規定する選別の条件を定めるための基準…を定め、サイバー通信情報監理委員会の承認を受けて、当該国外関係通信により送受信が行われる媒介中通信情報…の一部…が複製され、内閣総理大臣

行為の証拠の有無すら不明確な段階から情報収集を行うので、広範囲かつ長期にわたる情報収集=スパイ活動を想定している。

この行為は、「実態の把握」が主目的であり、コンピュータ等への侵入については、当事国の同意によらない通信情報の収集である。これらは国際法上のスパイの定義に該当する行為になる。

(結論)法案の情報収集活動の主眼が国外にあることから、この法案がスパイ活動を合法化する意図をもった法案であるとみてよい。

5. 「無害化」=サイバー攻撃の問題

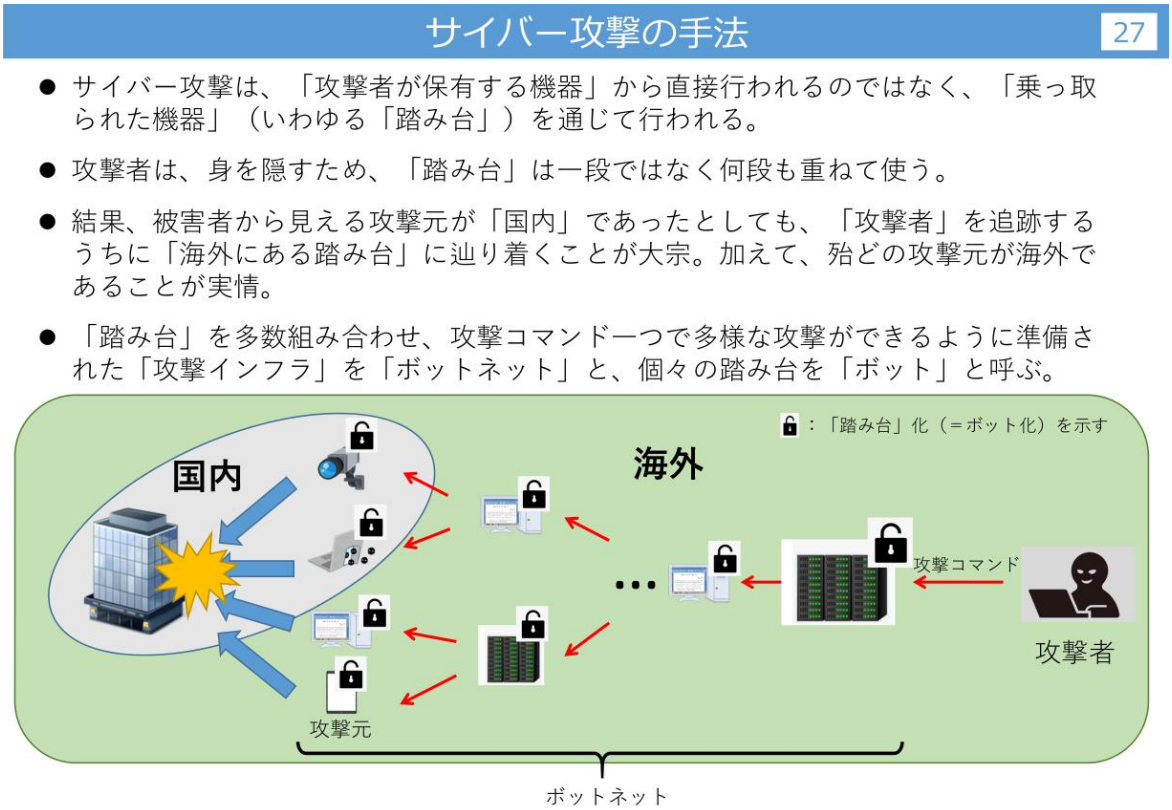
5.1. 日本への攻撃側の体制

日本国内のコンピュータ関連のシステムが攻撃を受けた場合、攻撃する側の体制は、最終的に攻撃の責任を負うべき大元が国外にあったとしても、ほぼ確実に国内に攻撃の拠点を構築する。従って、日本側が行なう「無害化」と呼ばれる攻撃は

- 国内の攻撃拠点への攻撃
- 日本国内の拠点に対して指示や命令を行なう国外の拠点への攻撃

となる。

法案が想定している攻撃手法は、国内にボットネットと呼ばれるような攻撃拠点を構築する事例などである。以下は法案の説明文書による。



の設置する設備…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。

送受信の一方が国内の場合は「外内通信」あるいは「内外通信」と呼ばれて、第 32 条、33 条に規定がある。いずれも「外外通信」とほぼ同じ規定である。

5.2. 官民連携

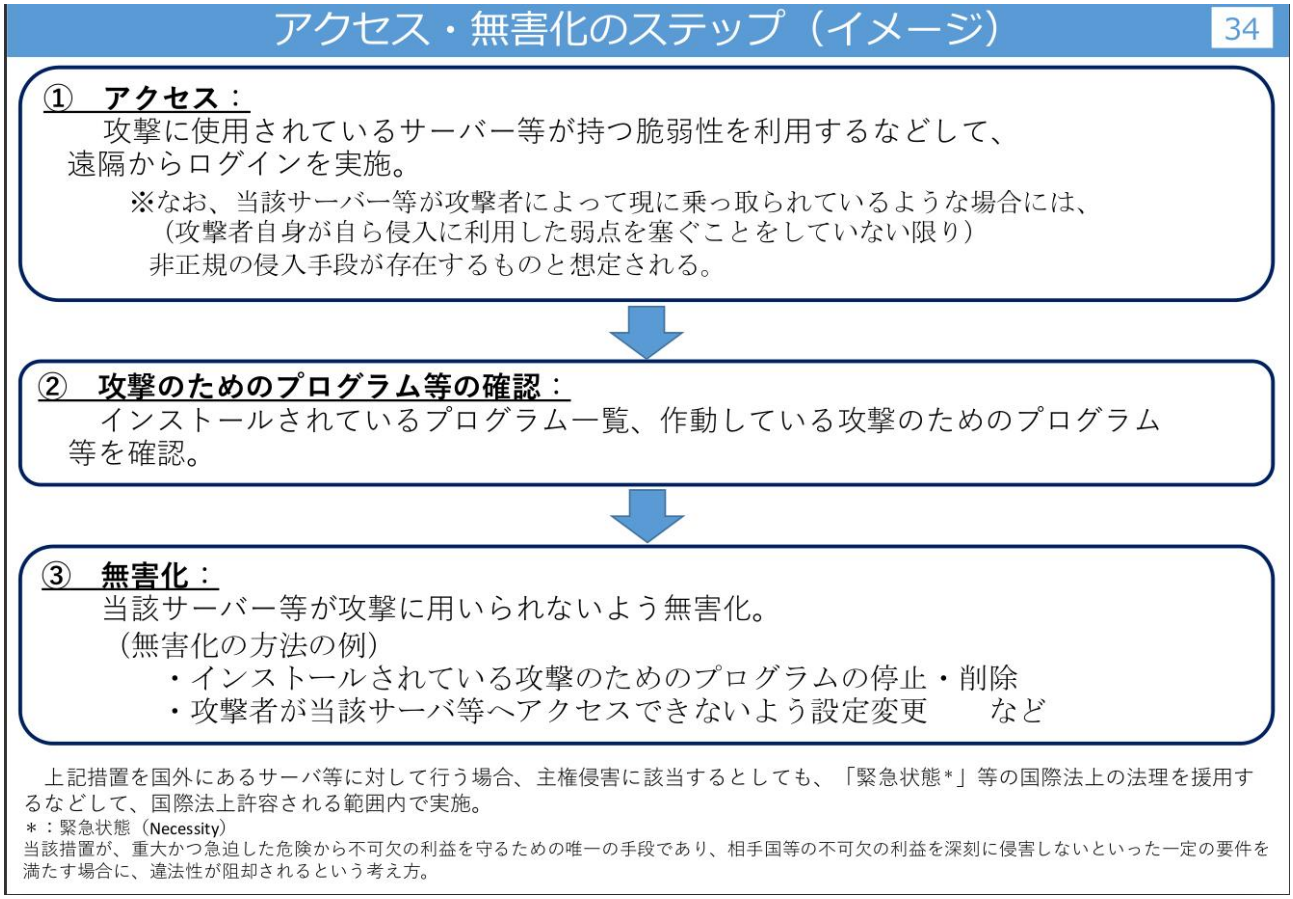
このような攻撃拠点を把握するには、国内での情報収集が必要になる。この情報収集のひとつの手段が民間の事業者からの情報提供である。これには

- 法案のなかの官民連携に基づく情報提供・共有の枠組で行なわれる場合
- 民間事業者の同意によらない通信情報の取得

があり、いずれも私たちには通知されない。通信の利用者の私たちからすると、これは、国内でのスパイ活動になりうる。

5.3. 「無害化」とは

「無害化」とは、不正行為があり放置すると重大な危害が及ぶおそれがあれば、通信事業者などに危害防止の措置を命令するか警察官(サイバー危害防止措置執行官)自らがその措置をリモートで実行できる、というもの。(改正警職法第6条、改正自衛隊法第81条)



法案では、ボットネットを構成している不正プログラムなどを仕込まれたボットの「無害化」が中心になっている。これは後述するVolt Typhoonのケースとよく似ている。

5.4. 令状主義の否定

法案はスパイ行為も「無害化」も裁判所の令状を必要としない新たな枠組を構築しようとしている。しかし、裁判所の令状によらないことになれば、令状発付に必要な証拠等が揃わない場合であっても「アクセス・無害化」が可能な枠組が可能になる。令

状は憲法が定めた基本的な手続きであり、国会は、これを無視するような違憲立法は行なえないはずだ。

5.5. 法案の影響は非常に深刻

- 日本政府が窃取しうる通信情報は、当該サーバーに直接関係しないものも含む膨大な情報になりうる。
- 長期にわたる可能性が高い。標的が「敵国」であれば、脆弱性を発見して侵入して更に可能な限り情報を収集しようとするだろう。外国の政府機関が標的の場合、相手組織は膨大であり構成員もまた多数であり、将来的に歯止めのない拡大へと向うことになる。

5.6. (事例)Volt Typhoon の場合：法案の説明文書で「無害化」の具体例として示されたケース。

米国を中心に 2021 年から活動し「無害化」まで 4 年近くがかかった。

- インターネットに接続されているルーターなどの末端のデバイスのセキュリティホールや脆弱性を突いて KV Botnet と呼ばれるマルウェアを用いて活動。
- 情報収集のみで破壊工作は確認されていない。
- 中国が後ろ盾の組織とされるが証拠は示されていない。
- 膨大な数にのぼるサポート期限が切れたルーターなどのセキュリティホールを標的にした。(適切に新規のルータに取り替えるなどすれば問題は発生しない)
- 「無害化」措置は、FBI が令状を請求して、裁判所の令状によって執行された。
- カナダ、オーストラリア、ニュージーランド、英国をあわせたファイブアイズの情報機関などとも連携。

5.7. Volt Typhoon の教訓

- 日本も同様の手口で海外でサイバースパイ・攻撃を仕掛けるにちがいない。
- 「無害化」は大元の組織を叩くものではない。
- 「無害化」と同時に、「無害化」攻撃を回避する新たな攻撃が開始された。無害化攻撃は新なサイバー攻撃のサイクルを生み出す。
- 「無害化」はサイバー領域におけるリスクを高め紛争を助長しかねない手法でしかない。
- 被害者は、警察などを待たずに対処が可能であり、警察や自衛隊などに委ねるだけが解決策ではない。

(結論)無害化によってサイバー攻撃は収束しない。むしろ新たな攻撃の応酬を招き、私たちの通信環境を国家間の紛争に巻き込むことになる。

6. そのほかの看過できない論点

6.1. 政府が参照する外国の法令はいずれも諜報機関関連の法律である

- 説明文書での諸外国の法制度への言及。ここで言及されている法律はほとんどが諜報機関に関するものばかりで、なおかつ、人権団体などから厳しく批判さ

れてきたもの。

6.2. 実空間での軍事行動との連携

法案ではほとんど対象になっていない。しかし、自衛隊のサイバー部隊を含む部隊が米軍や NATO との一体化のなかで作戦行動がとれるような枠組が存在している。この体制は、法律による新規の対応すら必要とはしていない既成事実になっているのではないか。

6.3. 国際法の不備

まだサイバー領域に関する戦争の条約はない。またサイバー戦争などの定義も合意がない。国連が策定で模索している一方で、各国は独自にサイバー領域での作戦を既に展開している。日本も米国、NATO との連携を実際に実行している。

6.4. サイバー戦争は軍隊だけでは実行できない

たとえば NATO の「ロックドシールズ 2024」の場合、防衛省のウエッブには参加組織として以下が明記されている。https://www.mod.go.jp/j/press/news/2024/04/23c.html

防衛省

内部部局、統合幕僚監部、陸上自衛隊陸上総隊司令部、陸上自衛隊システム通信団、海上自衛隊システム通信隊群、航空自衛隊作戦システム運用隊、航空自衛隊航空システム通信隊、自衛隊サイバー防衛隊、防衛研究所 他府

省等

内閣官房サイバー安全保障体制整備準備室、内閣官房サイバーセキュリティセンター（ＮＩＳＣ）、警察庁、外務省、経済産業省、情報処理推進機構（ＩＰＡ）、情報通信研究機構（ＮＩＣＴ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）、重要インフラ事業者等

日本は 2023 年、ウクライナなどとともに NATO のサイバー防衛協力センター(CCDCOE)の正式メンバーとなった。https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/

7．民衆のサイバーセキュリティは可能だ!

「サイバー攻撃」の不安が煽られている。国家安全保障の領域では、「敵」が行なう攻撃や作戦と同程度かそれ以上の能力をもった対処(攻撃など)を自軍も行なえるようにする、ということが基本の発想になる。この発想から抜けることが必要だ。そのためには不安感情の扇動に載せられないことが大切だと思う。

自分では何もできないのでは、という思い込み心理に多くの人々が支配されると、政府、とくに警察や自衛隊に頼ることなりがちだ。ミサイル攻撃への迎撃の手段をもたないことからの類推で、サイバー攻撃についても同様に、攻撃的な手段によらない防衛的な対処能力などはありえないと思い込まされている。この思い込みをまず払拭することが必要だ。とくに反戦平和運動の担い手が「政府や警察、自衛隊に依存しないでも自分たちで自分たちの通信や言論は防御できる」ということに自信を持ち、人々に警察や自衛隊に依存することの方がずっと危険な選択だということをアピールする必要がある。

7.1．政府のスパイ活動を暴露した市民たち

世界規模で起きた大きなスパイ活動として、イスラエルの企業 NSO が世界中の政府に売り込んだスパイ技術がある。Wikipedia に NSO グループの記事がある。

> NSO Group Technologies とは、スパイウェアの Pegasus などを開発している、イスラエルの企業である[1]。複数の国の政府などが顧客であり、同社が開発したスパイウェアはジャーナリストや人権活動家、企業経営者の監視に使用されている[2]。Apple や Facebook はユーザーを監視したなどとして同社に対して訴訟を起こしている[3][4]。アメリカ政府は 2021 年に、国家安全保障と外交政策上の利益に反する行為をしたとして NSO グループをエンティティリストに含め、米国企業による NSO グループの製品供給を事実上禁止した。https://ja.wikipedia.org/wiki/NSO_Group

NSO の事案は標的型と呼ばれるスパイウェアを用いたもので、スパイの対象となる人物のスマホにこの仕組みを密かにインストールする。スマホの通話盗聴、メール、マイク、カメラなどを自由にコントロールして情報を収集できてしまう。この NSO グル

ープの存在が発見されたのはアラブ首長国連邦の人権弁護士が自分のスマホにちょっとした異変を感じて、カナダのトロント大学が運営しているシチズンラボに問い合わせ、独自の調査が行なわれて、スパイウェアの身元が明かになり、これが公表されたのがきっかけで知られるようになった。[5]この大規模なスパイ活動は、各国とも官民一体となった技術協力を通じて行なわれているところが特徴的でもあり重要な点だ。米国でNSOの製品を禁じているのは、NSOに対する批判の声が世界規模で高まったことを配慮してのことだと思う。日本では小笠原みどりさんが注目して記事を書いていた[6]が、運動の側は関心をもたなかった。私も十分には取り組めていない。日本政府とNSOとの関係はいまのところ不明だ。

7.2. 市民のための自己防衛マニュアル

米国の電子フロンティア財団は独自に市民による自衛マニュアルを作成している。[7]

ここにはデモに参加する場合の注意からパスワードについての注意事項などまで、項目別に解説がある。米国の事例なので直ちに日本には適用できないところもあるが、参考になる。

実空間での安全保障での「防衛」となると、自衛のための武力行使のような薮蛇の手段をとるとか逃げるとかしかないが、サイバーでは自分たちでの防御がかなりのところまで可能だ。だから企業も小規模なサーバーの管理者もみな自前でサイバー攻撃への対処を行なうことができている。この現場の能力を軽視すべきではなく、こうした能力を国策に利用させるような体制は許してはならない。

私たちが防御の体制を構築することはどこの政府にとっても監視やスパイが困難になるので好まない。だからこそ民衆のサイバーセキュリティをきちんと実践することが大切だと思う。多くの国には有力な市民のためのサイバーセキュリティに取り組む団体がある。しかし、日本には、こうした活動を根づかせることに失敗してくたことを、ネットでの活動を担ってきた者として自戒の念を込めて反省したい。

是非共同声明の賛同団体になってください!!

(共同声明)サイバースパイ・サイバー攻撃法案(サイバー安全保障関連法案)の廃案を要求します―サイバー戦争ではなくサイバー領域の平和を

https://www.jca.apc.org/jca-net/ja/node/440

参考資料や情報

小倉のブログ

https://www.alt-movements.org/no_more_capitalism/

---

5 シティズンラボのレポートの日本語訳(機械翻訳)https://cryptpad.fr/pad/#/2/pad/view/UjG+-uMYVQToAwKCuBslbtPskrYsQonX+koLrKneMwg/ このなかにこのスパイウェアへの対処方法も記載されている。(iOSを最新バージョンにするだけですが) アムネスティの記事も参照。(機械翻訳) https://cryptpad.fr/pad/#/2/pad/view/-2on9u929fNqAyg0gVQIx-orc7hiNeg540P-Z4VJbog/

6 小笠原の下記の記事を参照。「スパイウェアに狙われるジャーナリスト⬚不都合な真実の消去に協力する企業」https://globe.asahi.com/article/14142629 「スパイ活動は国家間のフェア・ゲームか？ 被害に遭うのは個人」https://globe.asahi.com/article/14219502

7 https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/category/eff_%e8%87%aa%e5%b7%b1%e9%98%b2%e8%a1%9b%e3%83%9e%e3%83%8b%e3%83%a5%e3%82%a2%e3%83%ab/