能動的サイバー防御と通信の秘密(小倉利丸)

Table of Contents

1. 私たちが議論するときの前提となる原則について

1.1. 憲法

- 自衛権を含め、戦争、武力行使、戦力のいずれも認めるべきではない。
- サイバー領域は私たちのコミュニケーションの権利を具体的に実現するための中核的な領域である。この領域を戦争の手段にすることは、コミュニケーションの権利と両立せず、絶対に認められない。
- 能動的サイバー防御をめぐる法制化は妥協や譲歩の余地のないものであって、一切容認しないことが大切。

9条は以下である。

> **9**条
>
> 日本国民は、正義と秩序を基調とする国際平和を誠実に希求し、国権の発動たる戦争と、武力による威嚇又は武力の行使は、国際紛争を解決する手段としては、永久にこれを放棄する。
> ②　前項の目的を達するため、陸海空軍その他の戦力は、これを保持しない。国の交戦権は、これを認めない。

> **21**条
>
> 第二十一条　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
> ②　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

近藤正春内閣法制局長官は２月5日の衆院予算委員会

> 近藤政府特別補佐人　今お尋ねは、憲法第二十一条二項に規定する通信の秘密ということが中心かと思いますけれども、通信の秘密はいわゆる自由権的、自然的権利に属するものであるということから最大限に尊重されなければならないものであるということでございますけれども、その上で、通信の秘密につきましても、憲法第十二条、第十三条の規定からして、 公共の福祉の観点から必要やむを得ない限度 において一定の制約に服すべき場合があるというふうに考えております。

12、13、22、29条のように「公共の福祉」を理由とした制限がない。憲法には「公共の福祉」による制限を明記している条文と明記していない条文がある。21条は、公共の福祉に反することがあっても表現の自由や通信の秘密を保護していると解釈すべきだ。

1.2. サイバー戦争の放棄は9条では十分ではない

なによりも、サイバー領域における戦争とは何を指すのかが政府によって明確にされておらず、議論の土俵が用意されていない。

9条の諸条件はそのままではサイバー領域にあてはめることは困難で、多くの「漏れ」が生まれる。この意味で サイバー領域を自覚的にとりいれた戦争の新たな定義 、 戦争放棄の新たな定義 が不可欠である。

- 国権の発動ではなく、宣戦布告もなく、かつ、政府が主導するのでもない民間主導の戦争がありうる。
- 武力による行使や威嚇ではないが、これに代替する同等の効果をもつ行為がありうる。
- 戦力に該当しないが戦力にとって不可欠な領域がありうる。
- 交戦権に属さないが交戦権行使に不可欠な領域がありうる。

私の立場は、「自衛権」を含む一切の戦争と戦争を可能にする統治構造を認めない、という立場だ。殺傷行為そのものに加えて、たとえば以下のような 「銃後」に関わる領域を戦争概念に組込むこと が必要だ。

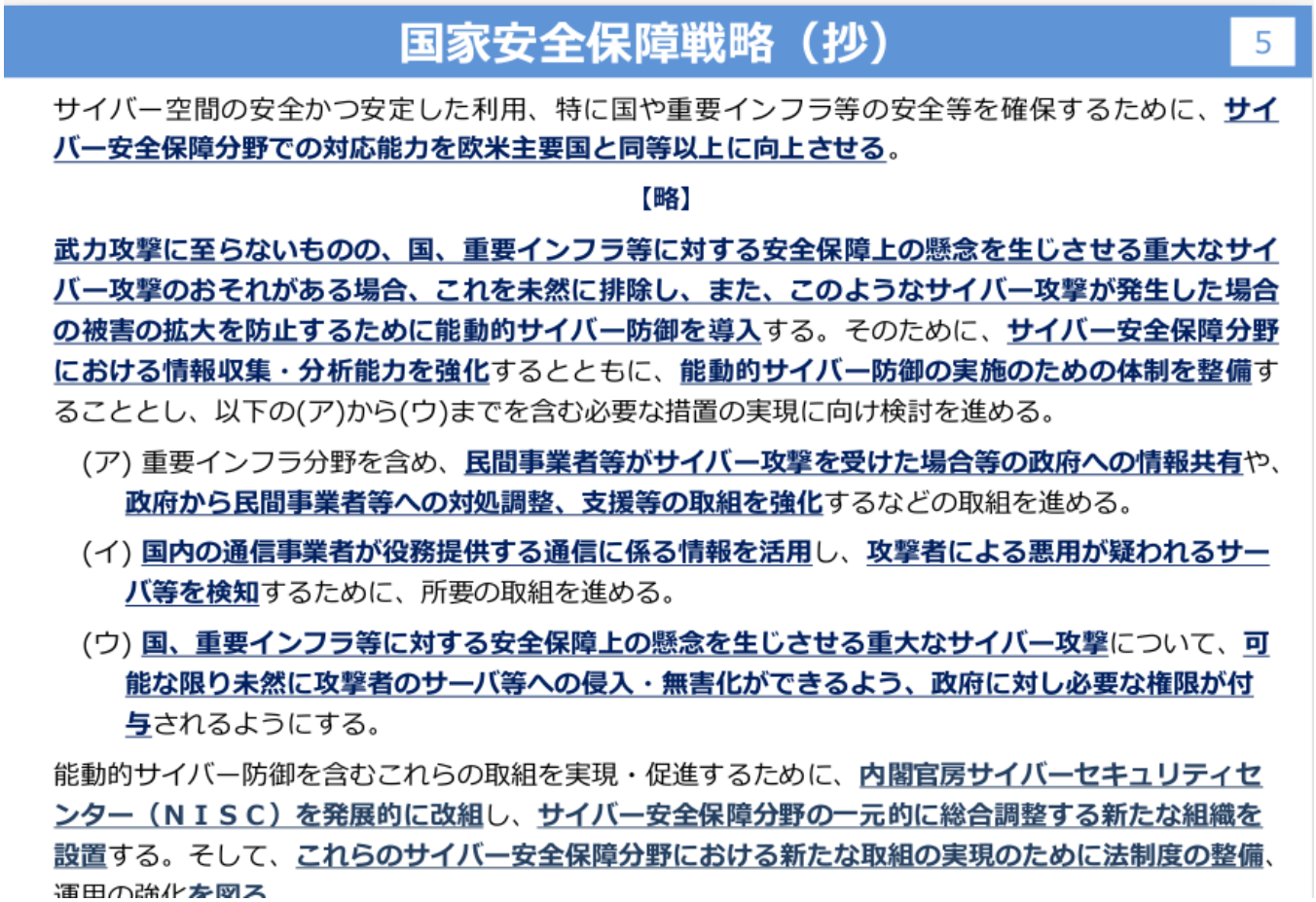
1. 将来の戦争(殺傷行為)を前提して、集団の構成員に対して、動静を把握したり、プロファイリングを行うこと。
2. 集団に対して重大な肉体的又は精神的な危害を加えること。(憎悪の扇動やヘイトスピーチ)
3. 集団に対して身体的破壊を意図して生活条件を破壊すること。(生活インフラのシステムの破壊)
4. 集団の強制的移送、排除を意図した行動をとること。
5. 愛国心やナショナリズムなど人々を個人としてではなく「国民」として束ねて動員するイデオロギーと統治の制度

2. 有識者会議に提出された内閣官房サイバー安全保障体制整備準備室の資料「サイバー安全保障分野での対応能力の向上に向けて」

資料の目次

- 国家安全保障戦略「サイバー安全保障分野での対応能力の向上」概要
- サイバー攻撃の変遷
- ウクライナに対する主なサイバー攻撃
- 最近のサイバー攻撃の動向（事前配置(pre-positioning)活動）
- 国家安全保障戦略（抄）
- 内閣サイバーセキュリティセンター（NISC）の強化
- 全体イメージ
- 主要国における官民連携等の主な取組
- 主要国における通信情報の活用の制度概要
- 現行制度上の課題

3. (スライド5) 国家安全保障戦略（抄）



国家安全保障戦略（抄）　5

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、**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**。

【略】

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化**するとともに、**能動的サイバー防御の実施のための体制を整備**することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。

(ア) 重要インフラ分野を含め、**民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への対処調整、支援等の取組を強化**するなどの取組を進める。

(イ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

(ウ) **国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃**について、**可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与**されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣官房サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組**し、**サイバー安全保障分野の一元的に総合調整する新たな組織を設置**する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、運用の強化を図る

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、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。
【略】
武力攻撃に至らないものの 、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大な サイバー攻撃のおそれがある場合、これを 未然に排除 し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために 能動的サイバー防御 を導入する。そのために、サイバー安全保障分野における 情報収集・分析能力を強化 するとともに、能動的サイバー防御の実施のための体制を整備することとし、以下の(ア)から(ウ)までを含む必要な措置の実現に向け検討を進める。
(ア) 重要インフラ分野を含め、 民間事業者等がサイバー攻撃を受けた場合 等の 政府への情報共有 や、 政府から民間事業者等への対処調整 、支援等の取組を強化するなどの取組を進める。
(イ) 国内の 通信事業者が役務提供する通信に係る情報を活用 し、 攻撃者による悪用が疑われるサーバ等を検知 するために、所要の取組を進める。
(ウ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大な サイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化 ができるよう、政府に対し必要な権限が付与されるようにする。
能動的サイバー防御を含むこれらの取組を実現・促進するために、内閣官房サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組し、サイバー安全保障分野の一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。

能動的サイバー防御の概念の定義は相変わらずあいまいなままである。関連すると思われるいくつかの概念、受動的サイバー防御、能動的サイバー攻撃、受動的サイバー攻撃、能動的防御、受動的防御などや、いくつかの言葉の組み合わせで生まれるであろう類語あるいは対語との関連が示されていない。

ポイントとなる個々のキーワードを拾い出して、これらを組み合わせて全体のイメージを作るしかない。個々のキーワードとしては、

- 欧米と同等以上
- 未然に排除
- 被害防止のための能動的サイバー防御
- 情報収集と分析力強化

- 重要インフラや民間事業者から政府への情報提供
- 政府による民間事業者への指揮命令、支援の義務化
- サーバー検知に業者の情報を活用
- サイバー攻撃に業者を動員
- NISCの組織強化と再編

重要インフラを含めた民間事業者は、政府や自衛隊によって防衛される受け身の存在でもなければ、民間に可能な「自衛」の主体に留まるのではなく、むしろサイバー攻撃に様々な方法で積極的に関与する主体として位置付けられている。サイバー領域の軍事安全保障分野が他の軍事領域と決定的に異なるのは、民間事業者が情報収集から攻撃に至るプロセス全体の主体となることなしには成り立たない、という点にある。

能動的サイバー攻撃の条件は、以下である。

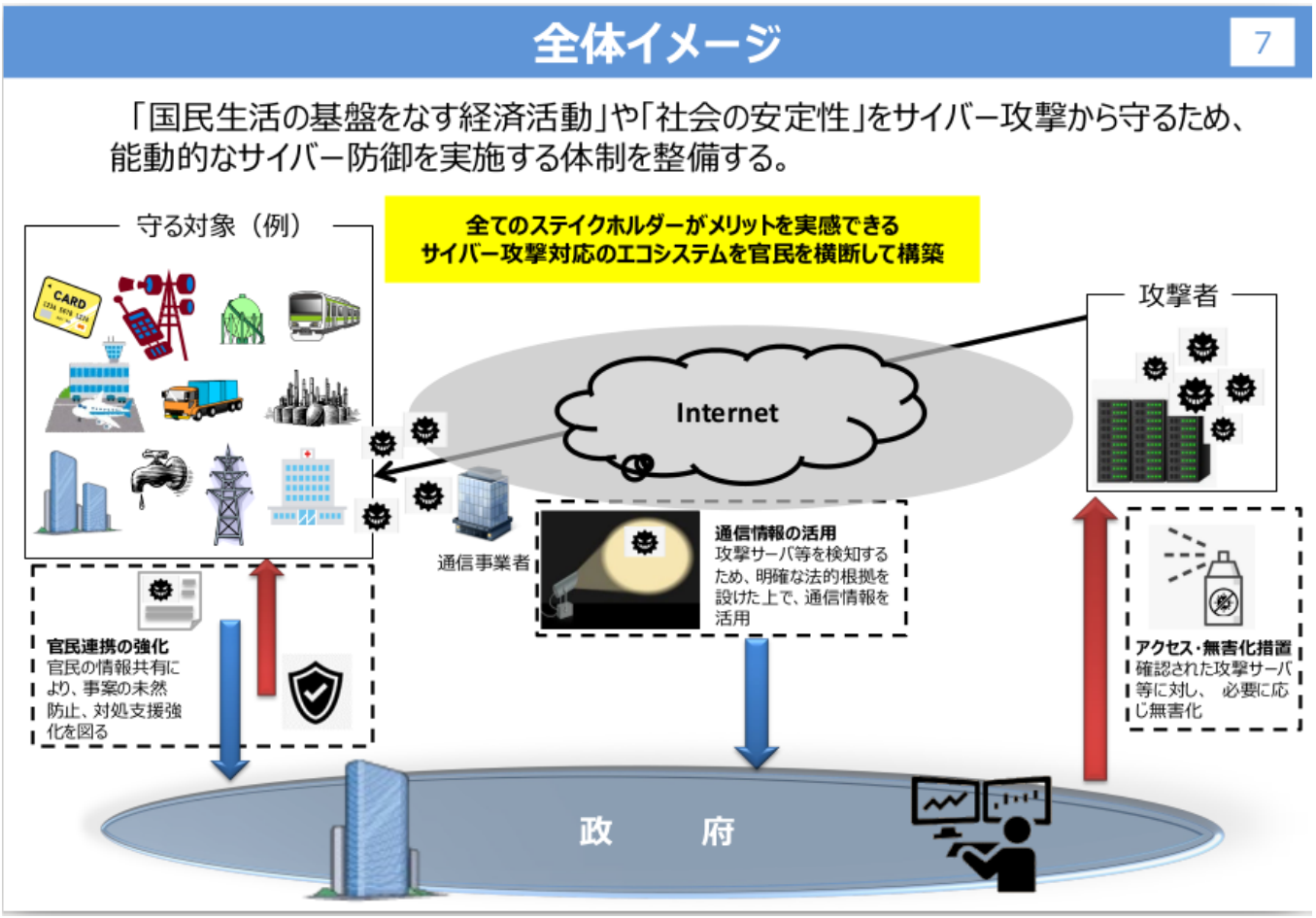
- 武力攻撃に至らない重大なサイバー攻撃のおそれ
- 安全保障上の懸念に該当し、かつ「重大」である

こうして、

- 現実の攻撃は存在しなくもよい。「懸念」「おそれ」があればサイバー攻撃を仕掛けるべきだ、という考え方は、先制攻撃そのものだ
- 導入される能動的サイバー防御の定義がないから、恣意的に運用できてしまう

  重要なことは、上記の「おそれ」「懸念」とは、実際には攻撃がない状態であっても、将来攻撃がありうると予想して先制攻撃を仕掛けることを正当化している。「おそれ」「懸念」が現実のものかどうかを立証する術はないなかで、先制攻撃を正当化する理屈だけが一人歩きする。

4. (スライド7) 全体イメージ



4.1. スライドの内容

「国民生活の基盤をなす経済活動」や「社会の安定性」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。

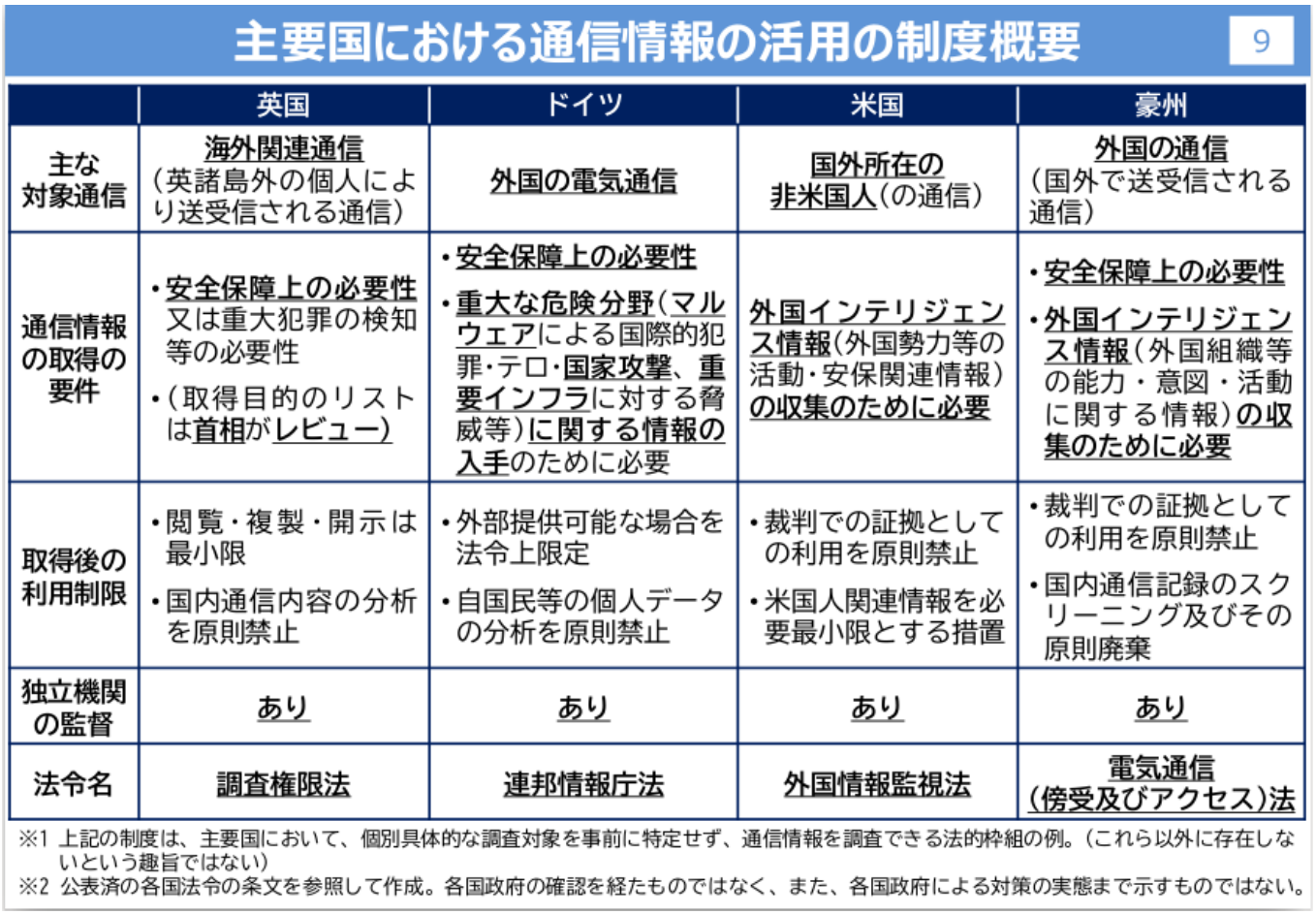
4.2. コメント

通信情報の活用として「攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を活用」とある。つまり、現行法ではカバーできない内容で「敵」とみなされるサーバーを検知するなど、現在であれば ハッキング行為や違法行為とされる活動を国家機関にのみ特権を与えて合法化 する。

サイバー攻撃の範囲は、 従来の刑事司法が担当してきたサイバー犯罪をほぼ網羅 している。「国民生活の基盤をなす経済活動」や「社会の安定性」という言い回しは、国内の 反政府運動も潜在的にターゲットにする可能性 を否定していない、ということでもある。

この図では「アクセス・無害化措置確認された攻撃サーバ等に対し、 必要に応じ無害化」という記述があるが、誰が無害化、つまり攻撃サーバへの攻撃の主体となるのかが曖昧にされている。

5. (スライド9) 主要国における通信情報の活用の制度概要



主要国における通信情報の活用の制度概要　9

	英国	ドイツ	米国	豪州
主な対象通信	海外関連通信（英諸島外の個人により送受信される通信）	外国の電気通信	国外所在の非米国人（の通信）	外国の通信（国外で送受信される通信）
通信情報の取得の要件	・安全保障上の必要性又は重大犯罪の検知等の必要性 ・（取得目的のリストは首相がレビュー）	・安全保障上の必要性 ・重大な危険分野（マルウェアによる国際的犯罪・テロ・国家攻撃、重要インフラに対する脅威等）に関する情報の入手のために必要	外国インテリジェンス情報（外国勢力等の活動・安保関連情報）の収集のために必要	・安全保障上の必要性 ・外国インテリジェンス情報（外国組織等の能力・意図・活動に関する情報）の収集のために必要
取得後の利用制限	・閲覧・複製・開示は最小限 ・国内通信内容の分析を原則禁止	・外部提供可能な場合を法令上限定 ・自国民等の個人データの分析を原則禁止	・裁判での証拠としての利用を原則禁止 ・米国人関連情報を必要最小限とする措置	・裁判での証拠としての利用を原則禁止 ・国内通信記録のスクリーニング及びその原則廃棄
独立機関の監督	あり	あり	あり	あり
法令名	調査権限法	連邦情報庁法	外国情報監視法	電気通信（傍受及びアクセス）法

※1 上記の制度は、主要国において、個別具体的な調査対象を事前に特定せず、通信情報を調査できる法的枠組の例。（これら以外に存在しないという趣旨ではない）
※2 公表済の各国法令の条文を参照して作成。各国政府の確認を経たものではなく、また、各国政府による対策の実態まで示すものではない。

5.1. スライドの内容

通信情報の取得の要件、取得後の利用制限、独立機関の監督、法令名の各項目について、英国、ドイツ、米国、オーストラリアで比較

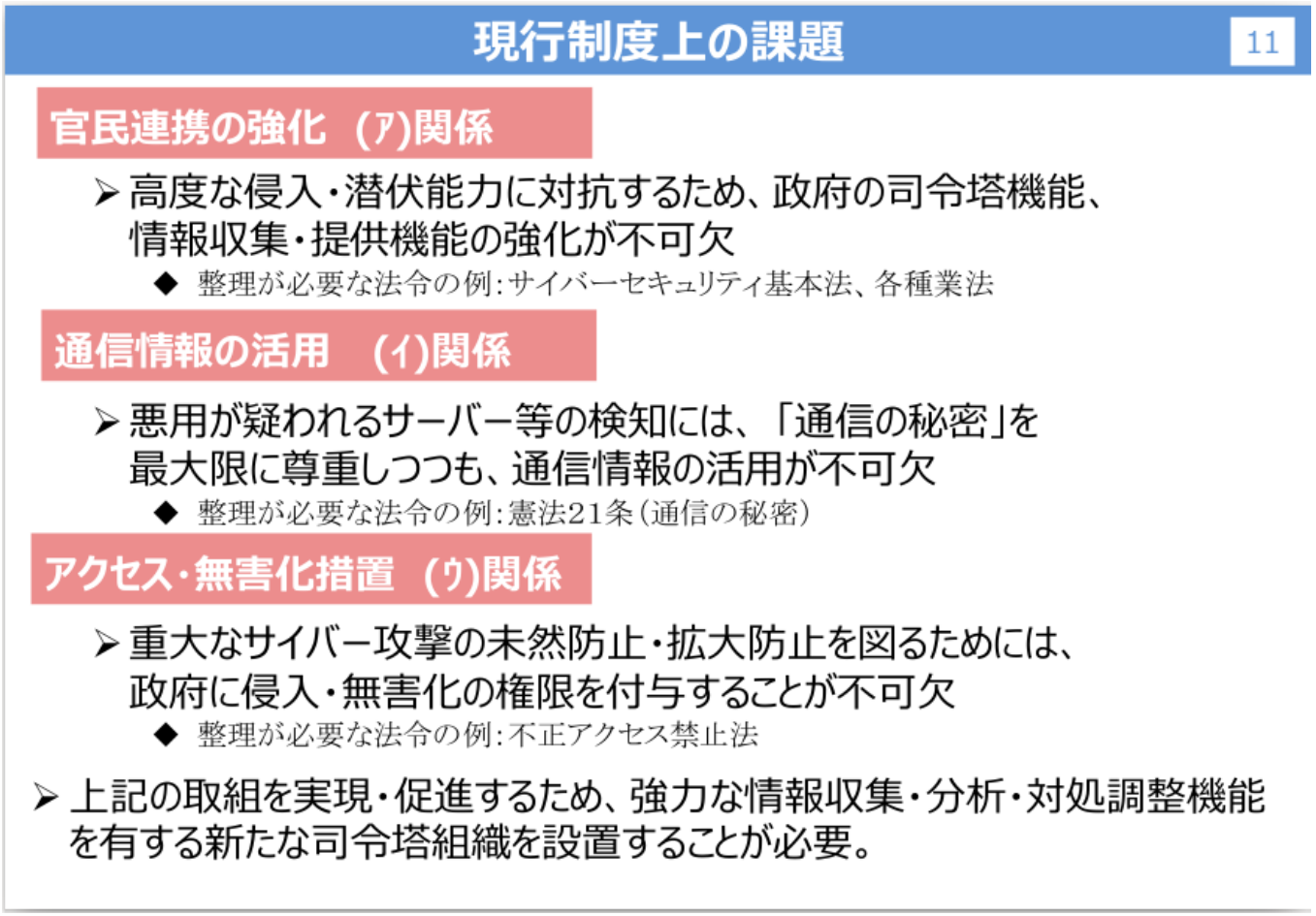
5.2. コメント

ここでいう通信情報とは、プライバシーに関わるような「通信の秘密」に該当する内容とみていい。いずれの国も 国家安全保障の必要があれば通信の秘密の侵害を合法化 している法制度があることを強調している。これに加えて 外国へのスパイ行

為(米、オーストラリア)、ドイツは重大な危険分野に関する情報入手に必要であればよい、という記述がある。ただし、英国は「国内通信内容の分析を原則禁止」、ドイツは「自国民等の個人データの分析を原則禁止」とある。また米、豪は裁判での証拠としての利用禁止とある。これをどう理解すべきか。

この整理が妥当かどうかは精査が必要である。

6. (スライド11) 現行制度上の課題



6.1. スライドの内容

官民連携の強化 (ｱ)関係
- 高度な侵入・潜伏能力に対抗するため、政府の司令塔機能、
情報収集・提供機能の強化が不可欠
- 整理が必要な法令の例：サイバーセキュリティ基本法、各種業法
通信情報の活用
(ｲ)関係
- 悪用が疑われるサーバー等の検知には、「通信の秘密」を
最大限に尊重しつつも、通信情報の活用が不可欠
- 整理が必要な法令の例：憲法２１条（通信の秘密）
アクセス・無害化措置 (ｳ)関係
- 重大なサイバー攻撃の未然防止・拡大防止を図るためには、
政府に侵入・無害化の権限を付与することが不可欠
- 整理が必要な法令の例：不正アクセス禁止法
- 上記の取組を実現・促進するため、強力な情報収集・分析・対処調整機能
を有する新たな司令塔組織を設置することが必要。

6.2. コメント

ここでは以下の二つの法制度を改悪

- 通信傍受
- 不正アクセス禁止法

特に問題になるのは憲法との関連だろう。しかし現行法の拡大解釈によって可能なことがあるはずなので法改正だけに注目すべきではない。

逆に、通信傍受やアクセス禁止を厳格に捉えるなら、能動的サイバー防御はそもそも機能しなくなることも意味している。それだけ能動的サイバー防御は深刻な政策である。

また、現行法で違法となる政策を策定し予算をつけること自体が違憲・違法行為ではないか。

この改悪を前提とした新たな「司令塔」の設置が提言されているが、内閣府と自衛隊との関連、あるいは司法警察やデジタル庁、総務省など電気通信関連省庁との関連をどう調整するのか。

論じられていない最も大切な問題：暗号化の弱体化

通信の秘密に関連して明示されていない重要な問題として、通信の暗号化に関する問題がある。通信がエンド・ツー・エンドで暗号化されてしまうと、サーバーでも経路上でも盗聴や監視が不可能になる。復号化のための高度な技術を用いるか、さもなければ、ユーザーが復号化してデータを読む行為をしている最中にこれを窃取できる仕組みを導入する必要がある。法制度としては、政府が解読できない暗号を原則禁止する、通信事業者に協力させるなどで暗号化を弱体化させることも可能 である。

こうした弱体化は、軍事が絡む国家安全保障領域を聖域として暗号化を弱体化させる特権を与えるだけでは十分ではない。軍事と非軍事が絡みあうので、 警察などもまたエンド・ツー・エンドの弱体化の重要なアクター となる。

7. スライドに欠落している重要な論点

- 軍事と非軍事が明確に区別できない領域であるために、 非軍事領域が限り無く軍事領域に引き寄せられて再定義されることになる。その結果生じる私たちの基本的な権利への侵害についての関心が皆無である。
- 日米同盟、とくに自衛隊と米軍の関係 を踏まえた記述がない
- サイバー安全保障と人権や通信の自由、プライバシーの権利などや憲法との関係で踏み込んだ記述がない。むしろこれらの権利をいかにして抑制し、憲法の規定を骨抜きあるいは 改憲をさきどり して制度化するかに関心がある。
- 民間企業への統制強化 と民間企業をむしろ主体的に国益に従属させる観点が中心になっている。
- サイバーセキュリティに関連する分野について、 各省庁の思惑や関心がバラバラ かもしれない。中核をなすデジタル庁はマイナンバーカード問題で忙殺状態のようにみえる。また サイバーセキュリティ戦略本部が2024年3月に改訂し「重要インフラのサイバーセキュリティに係る行動計画」 においては、サイバー攻撃への言及は多くみられるにもかかわらず、自衛隊への言及はなく、防衛省については一箇所のみでほとんどその意義がみられない。これに対して警察への言及がかなり多くみられる。こうした足並みの乱れとみられる事態に防衛省や軍事安全保障に関連する組織はある種の危機感をもっていてもおかしくない。

https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf

能動的サイバー防御をはじめとするサイバー領域をめぐる軍事安全保障は、政府内部ではまだ十分な合意がとれていないのではないか。内閣官房が核になった省庁横断という掛け声はあってもこれを実現できるだけの リーダーシップが内閣官房にもない と思われる。たぶん、能動的サイバー防御の有識者会議を経ての法・制度の整備によって サイバー領域の安全保障の構造が大きく変化する危険性 がある。

8. (参考)(共同声明)能動的サイバー防御と関連する法改正に反対します—サイバー戦争ではなくサイバー領域における平和を(2023年10月20日)

https://www.jca.apc.org/shiminren/?p=604

国会での議論もないままに、2022 年 12 月に安保防衛三文書が閣議決定されました。この文書に「能動的サイバー防御」という言葉が登場しました。「可能な限り未然に攻撃者のサーバー等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする」「サイバー安全保障分野における新たな取り組みの実現のために法制度の整備、運用の強化を図る」(「国家安全保障戦略」)と明記されました。サイバー領域（インターネットやコンピュータネットワークおよびこれらを用いたコミュニケーション環境のこと）において軍事を最優先させる政策は、サイバー領域全体を戦争に巻き込み、私たちのコミュニケーションの権利を根底から脅かすことになります。政府は 2023 年 1 月 31 日に、一元的サイバー安全保障体制整備準備室を内閣官房に設置し、今後必要な法改正を検討するとしました。

私たちは、サイバー領域がいわゆるサイバー戦や情報戦などの舞台となり、自衛を名目とした武力行使を含む戦争にも関与するものとなる法改正に反対します。また、サイバー領域が国籍や人種、民族、宗教、ジェンダー、価値観など様々な違いを理由に、国家や支配的な集団が憎悪や偏見、差別を扇動し、結果として自国の暴力を正当化するための場となることにも反対します。安保防衛三文書における能動的サイバー防御の考え方は、自衛隊のいわゆる敵基地への先制攻撃と関連するだけにとどまりません。サイバー領域全体を巻き込んだ情報操作や、サイバー領域全体の網羅的な監視・取り締まりの強化、いわゆる「敵」のソフトターゲット(民間人や民間の建物など警備や監視が手薄で攻撃されやすい軍事目標)を狙うなどの行動が重要な役割になります。そうした場合に、サイバー領域の戦争への加担は、自衛隊に限らず、企業、研究機関、団体、一般の市民の動員も想定されることになります。サイバー領域が戦争に巻き込まれるとき、従来の戦争で想定されている武器の他に、私たちのパソコンやスマホもまた「武器化」し、人々が容易にサイバー部隊に動員され、企業もまたサイバー領域での戦争行為に容易に加担することが可能になります。

サイバー領域を戦争に巻き込む体制が世界規模で急速に進行するなかで、私たちは、むしろサイバー領域をこれ以上戦争に加担させないための行動をとる必要を痛感しています。サイバー領域はまさに、コミュニケーションの中枢を担う領域であるからこそ、この領域を戦争のために利用したり、戦争に巻き込んだりすることは絶対に許してはなりません。むしろ私たちが希求すべきことは、サイバー領域における平和です。サイバー領域から自衛隊を含む軍隊の活動を排除するだけではなく、民間企業や私たち一人一人がサイバー戦争に加担したり、強制されたりすることを徹底して禁じる必要があります。サイバー領域が文字通りの意味で、国境を越えて、多様な民衆を相互に繋ぐコミュニケーションの場となるためにも、サイバー領域における平和が今こそ求められているのです。残念ながら日本政府の態度は、このサイバー平和とは真っ向から対立するものと言わざるをえません。岸田政権は、日本がサイバー戦争に踏み込むことを可能にするために、 障害となる憲法の保障する通信の秘密を形だけのものとしようと電気通信事業法、不正アクセス禁止法、ウイルス作成罪などを含む刑法、そして自衛隊法などの改悪を行おうとしています。 通信の秘密、表現の自由は民主主義社会の基礎です。能動的サイバー防御はこれを否定するものです。

以上、私たちは、能動的サイバー防御を合法化するための一切の法整備に反対するとともに、自衛隊、行政、民間企業によるサイバー戦争への加担に反対します。

2023 年 10 月 20 日

＜呼びかけ団体＞
JCA-NET
盗聴法に反対する市民連絡会
ATTAC Japan（首都圏）
共謀罪 NO！実行委員会
「秘密保護法」廃止へ！実行委員会
ふぇみん婦人民主クラブ
許すな！憲法改悪・市民連絡会
すべての基地に「NO！」を・ファイト神奈川

Date: 2024年6月15日
Author: 小倉利丸(toshi@jca.apc.org)
Created: 2024-06-12 水 14:47
Validate