2025/2/13
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

能動的サイバー防御法案は、インターネット常時監視法案・サイバー版先制攻撃法案だ!

海渡　雄一

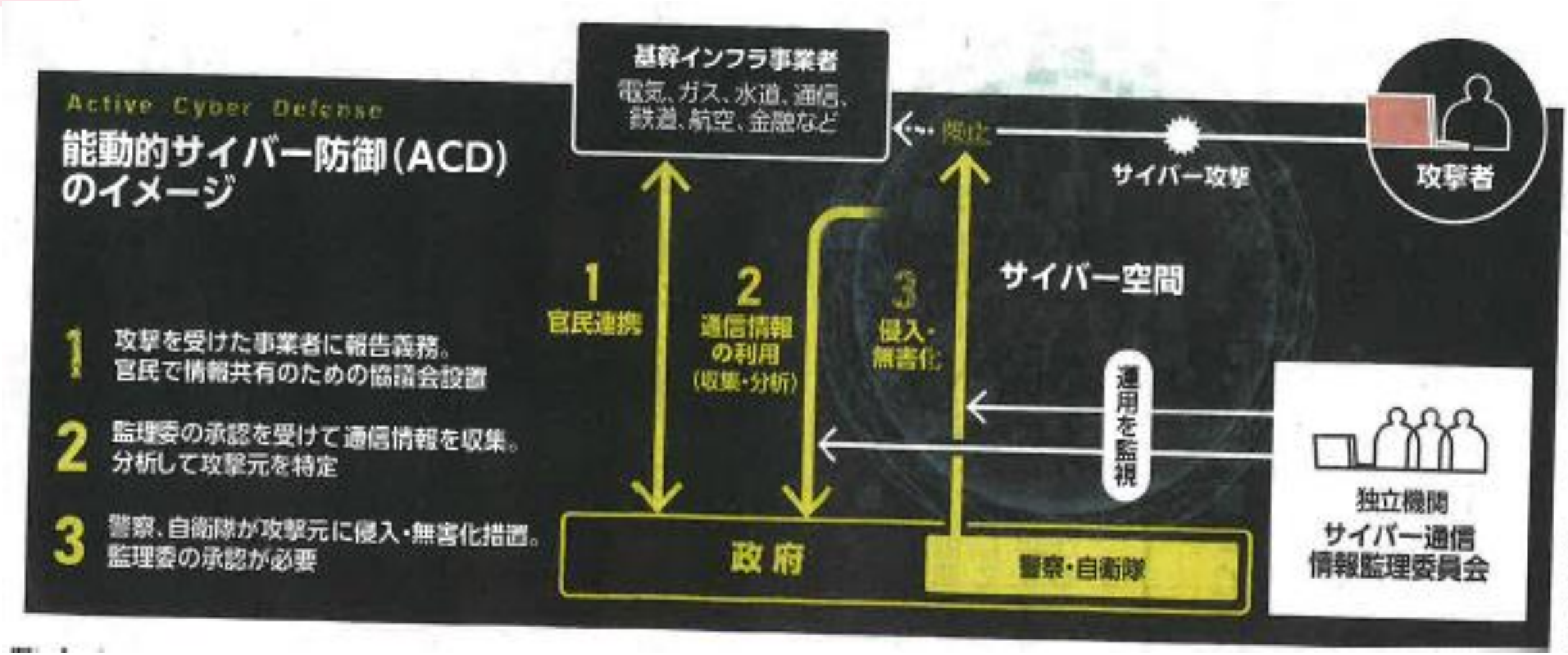
（弁護士　秘密保護法対策弁護団
共同代表・経済安保法に異議あり
キャンペーン）

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　能動的サイバー防御法案って、なに？　本当に必要なの?
- 第2　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3　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4　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5　情報の分析・整理とは何を行うのか?
- 第6　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7　大川原化工機冤罪事件の公安捜査が示す警察組織の法遵守への根本的疑問
- 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

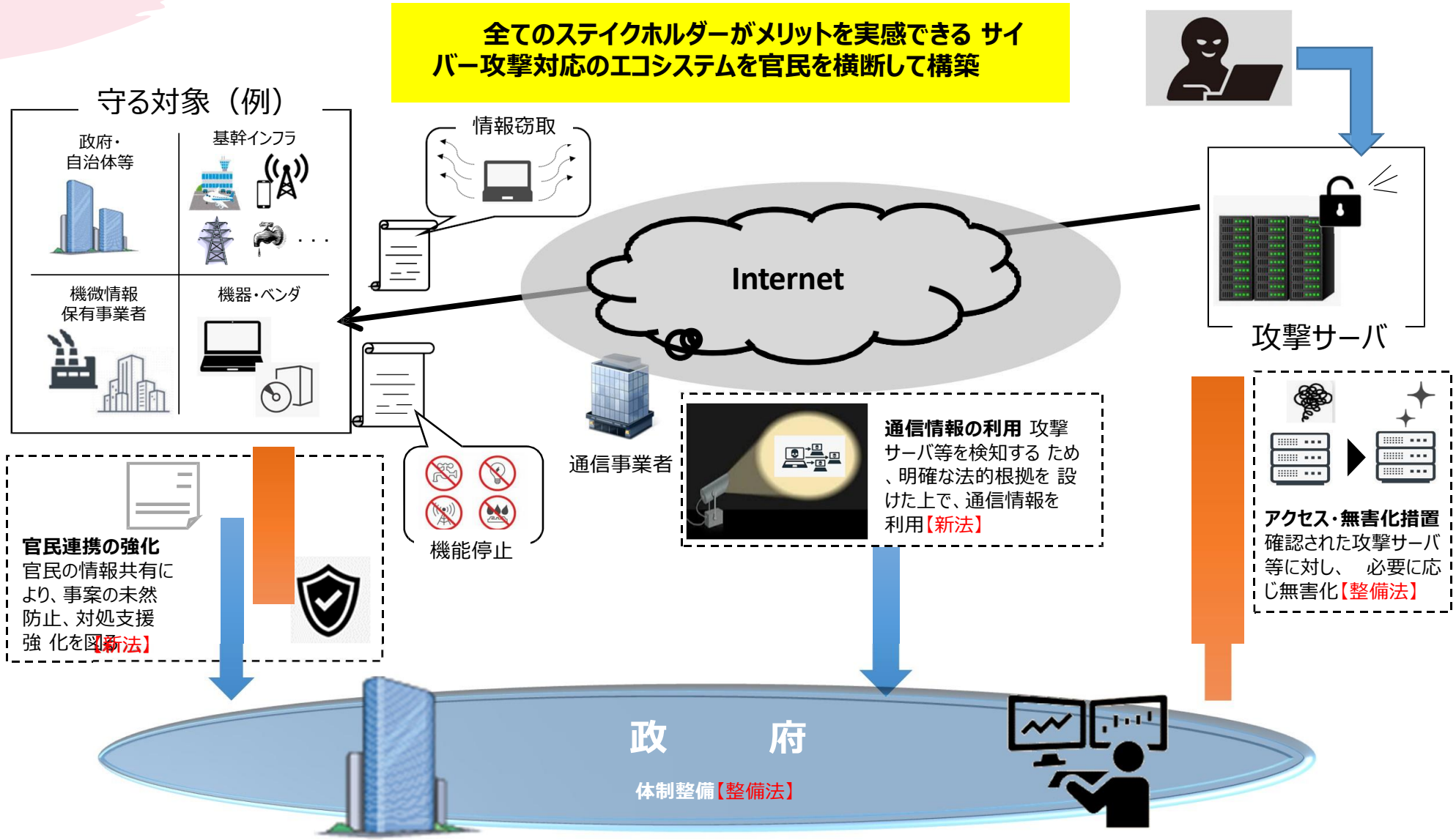
第1　能動的サイバー防御法案って、なに?
本当に必要なの?



朝日新聞　2025年2月8日

政府法案説明資料より

「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。



基幹インフラ事業者とは

政府法案説明資料より

経済安全保障推進法

国民生活及び経済活動の基盤となる「特定社会基盤役務」の安定的な提供を確保するため、国が規制対象となる「特定社会基盤事業」「特定社会基盤事業者」「特定重要設備」を指定。

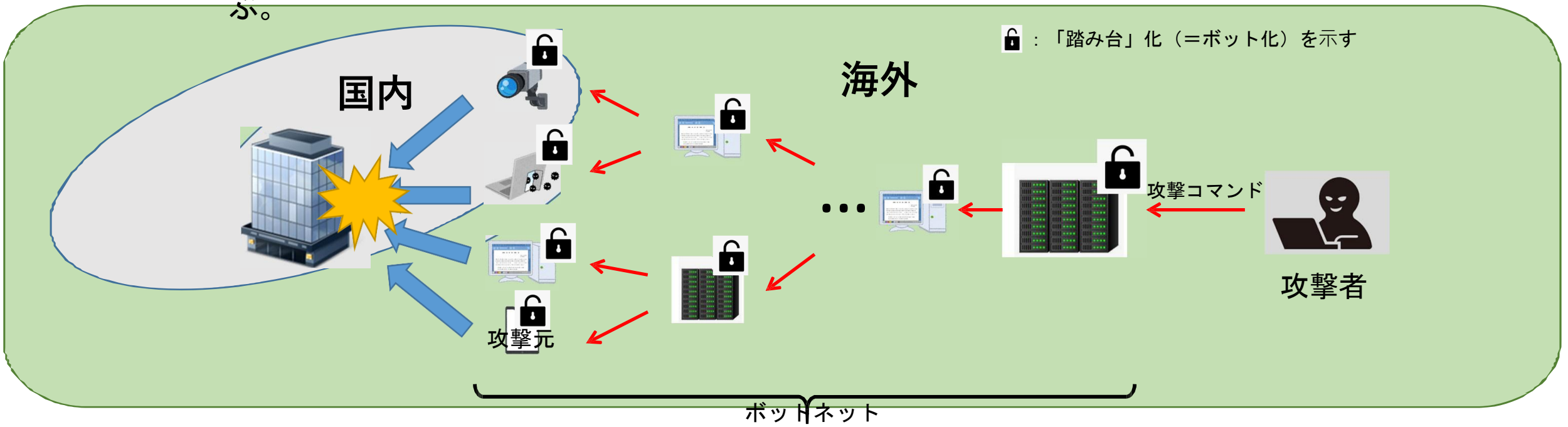
- ✓ **「特定社会基盤役務」**：国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの
- ✓ **「特定社会基盤事業」**：対象１５事業（下表参照）のうち、特定社会基盤役務の提供を行うものとして政令で定めるもの
- ✓ **「特定社会基盤事業者」**：特定社会基盤事業を行う者のうち、その使用する特定重要設備の機能が停止し、又は低下した場合に、その提供する特定社会基盤役務の安定的な提供に支障が生じ、これによって国家及び国民の安全を損なう事態を生ずるおそれが大きいものとして主務省令で定める基準に該当する者
- ✓ **「特定重要設備」**：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

基幹インフラ制度の対象事業（特定社会基盤事業）　（計２１３者）

①電気（４４者）	②ガス（２５者）	③石油（１８者）
④水道（２３者）	⑤鉄道（５者）	⑥貨物自動車運送（３者）
⑦外航海運（３者）	⑧航空（２者）	⑨空港（６者）
⑩電気通信（１０者）	⑪放送（６者）	⑫郵便（１者）
⑬金融（５９者）	⑭クレジットカード（８者）	⑮港湾（未施行）

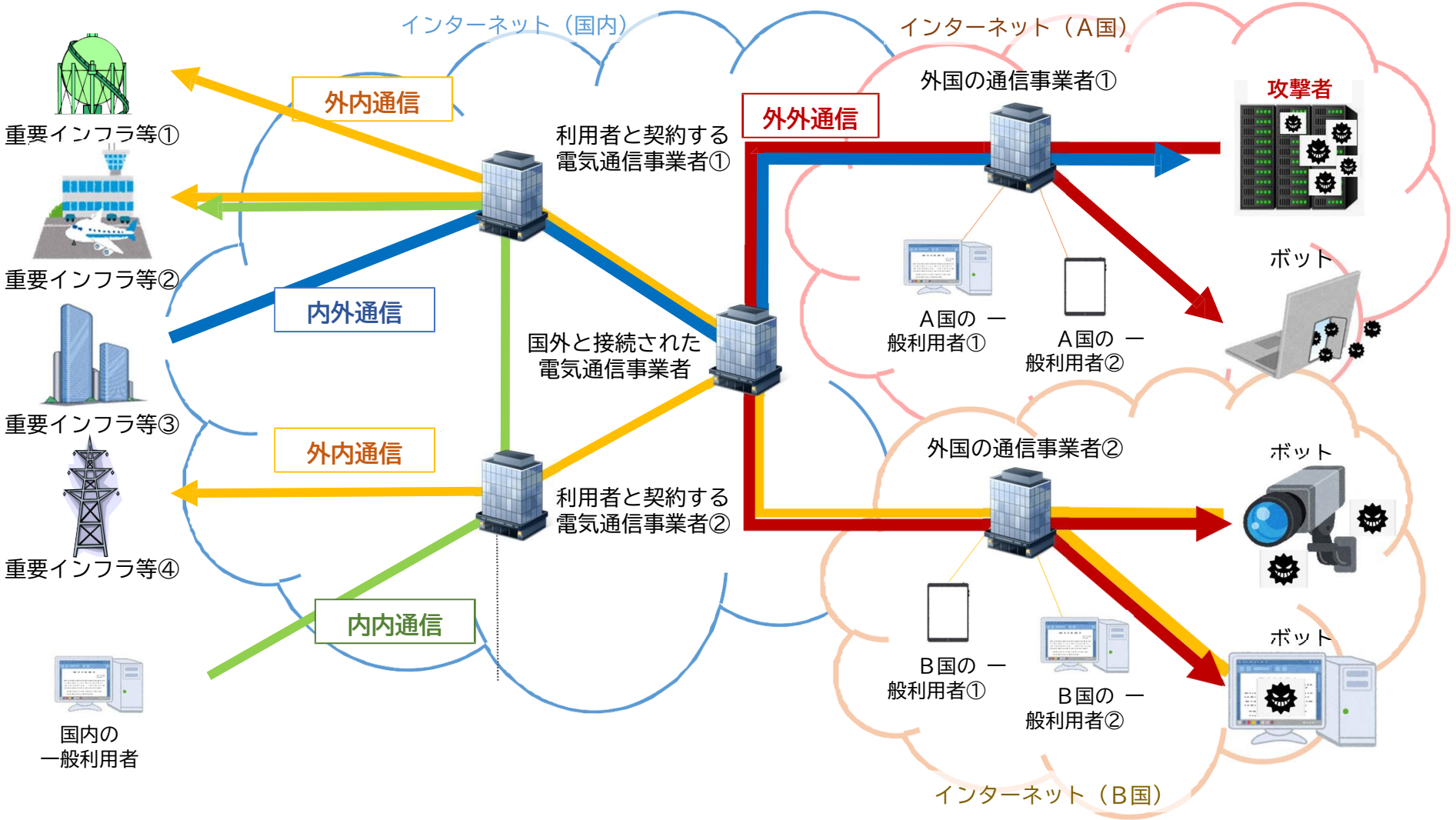
※ 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）
※ 内閣府「特定社会基盤事業者として指定した者（令和６年10月17日時点）」から作成
※ サイバーセキュリティ基本法の「重要社会基盤事業者（重要インフラ）」とは別概念

- サイバー攻撃は、「攻撃者が保有する機器」から直接行われるのではなく、「乗っ取 られた機器」（いわゆる「踏み台」）を通じて行われる。
- 攻撃者は、身を隠すため、「踏み台」は一段ではなく何段も重ねて使う。
- 結果、被害者から見える攻撃元が「国内」であったとしても、「攻撃者」を追跡する　うちに「海外にある踏み台」に辿り着くことが大宗。加えて、殆どの攻撃元が海外で あることが実情。
- 「踏み台」を多数組み合わせ、攻撃コマンド一つで多様な攻撃ができるように準備さ れた「攻撃インフラ」を「ボットネット」と、個々の踏み台を「ボット」と呼ぶ。



国外が関係する通信、関係しない通信

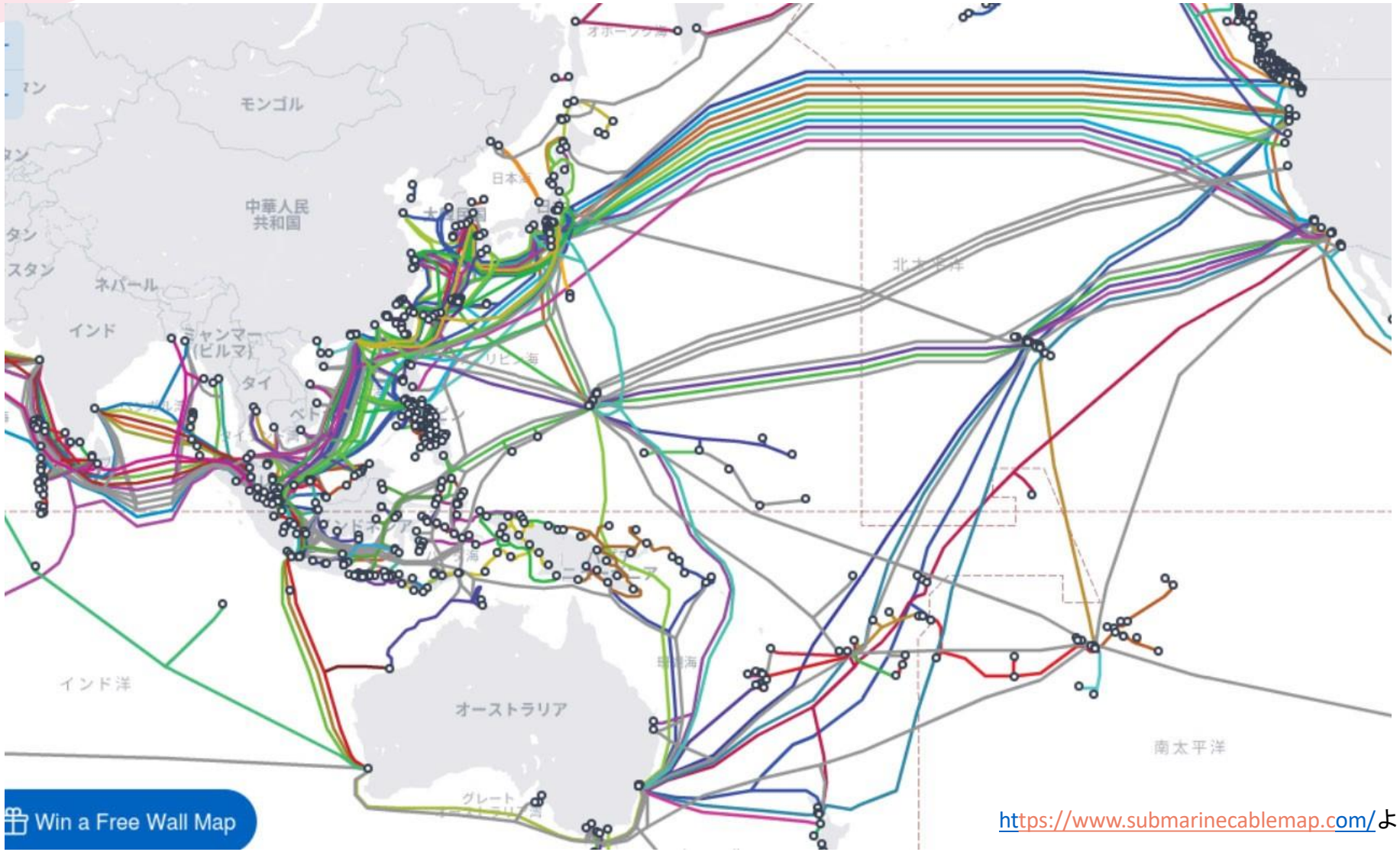
政府法案説明資料より



物理的な「インターネットのインフラ」

- 米国＝アジア間の通信は「太平洋を横断する海底ケーブル」を経由
- また日本が太平洋横断ケーブルの「ハブ」になっている

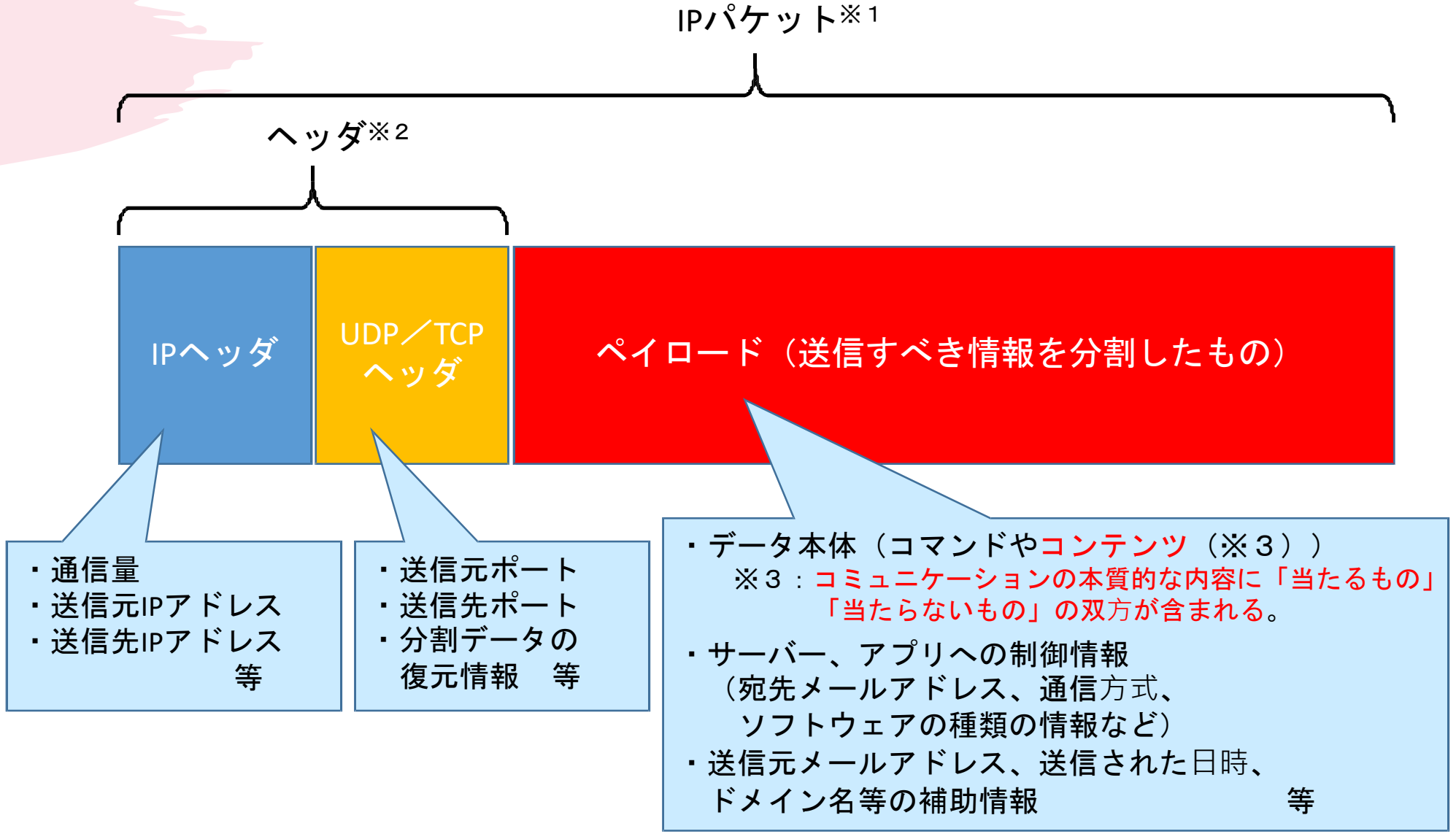
≒　太平洋を横断する殆どの通信が「日本乗換」



https://www.submarinecablemap.com/より

インターネットを流れるデータの構造

政府法案説明資料より



※１：IPパケット自身に「受信日時」は含まれないが、いわゆる「ログ保存時」にその瞬間の日時を「受信日時」として記録

※２：「フロー情報」、「メタデータ」の語は、上記「ヘッダ」を指すことが多い

コミュニケーションの本質的な内容ではない情報の例

コミュニケーションの 本質的な内容に **当たらない例**	○ 送受信日時　2024.04.01 12:00:04 ○ ＩＰアドレス　103.23.145.84 ○ 通信量　20kB ○ ポート番号　80 ○ コマンド　POST/ A3fe e3844A7D35300734D2BA HTTP/1.1 ○ プロトコル（通信方式）　HTTP / SSL / SMTP ○ ソフトウェアの種類　Mozilla/4.0(…Trident/7.0;NET4.0c;…)… ○ ドメイン名　cas.go.jp ○ メールアドレス　hogehoge@example.com （個人情報保護の観点から、個人を識別することができないように加工することが必要）
コミュニケーションの 本質的な内容に **当たる例**	× 電子メールの本文・件名 × 添付ファイルの内容・名称 × ＩＰ電話の通話内容 × Ｗｅｂサイトに掲載されている文章、画像

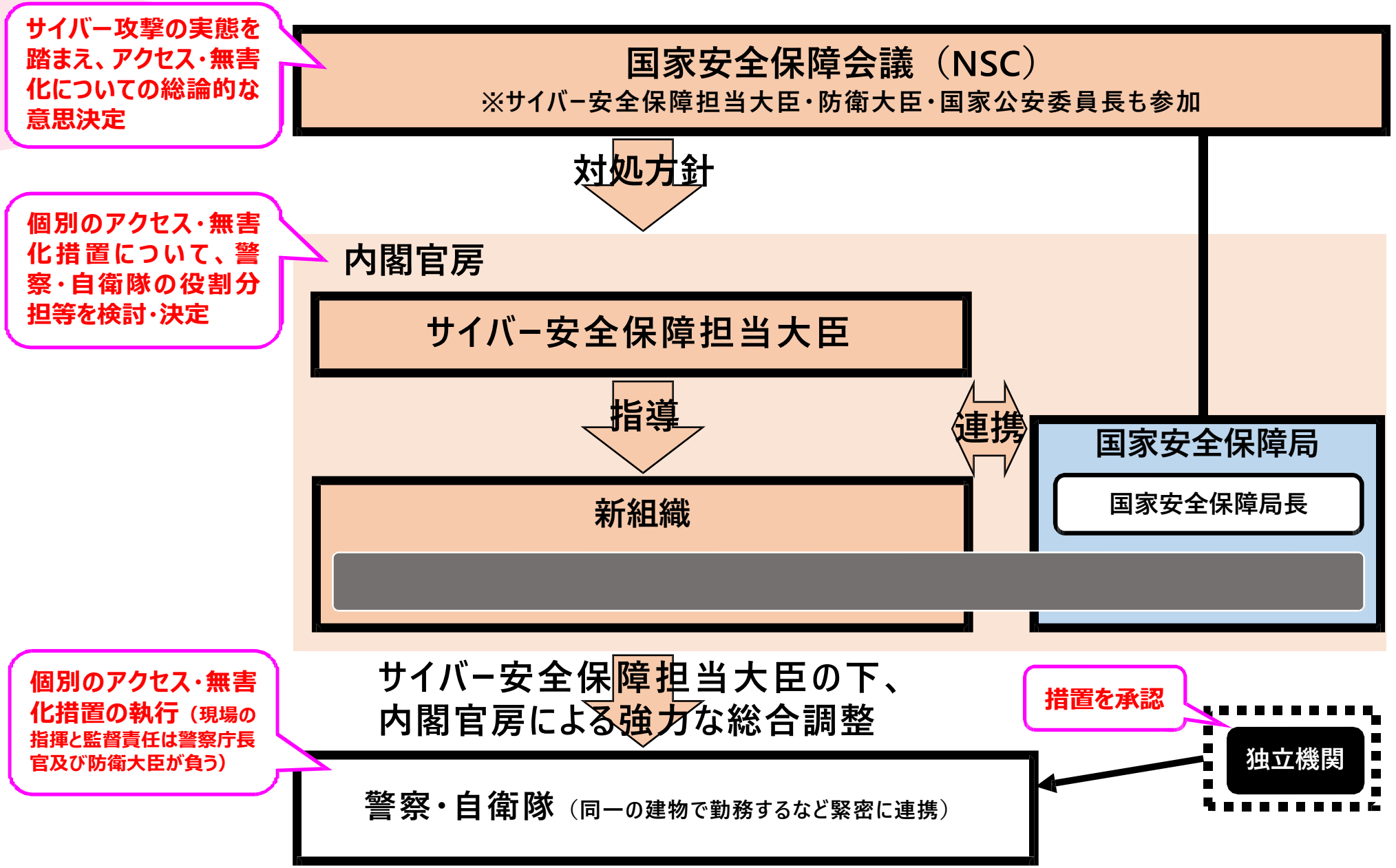
政府法案説明資料より

黄色ハッチ部が「コミュニケーションの本質的内容」に相当。

番号	通信情報の内容	説明
1	From: hanako1@example.jp	送信者メールアドレス
2	To: taro2@cas.go.jp	宛先メールアドレス
3	Subject: 重要書類の送付について（至急）	件名
4	Date: 2012/03/25 10:37	送信日時
5	Return-Path: <mail-system@example.jp>	送信元メールアドレス （システムエラー時の返信先）
6	Received: from mail.cas.go.jp ([198.51.100.3]) by aa00bb01.cas.go.jp id <20120325103715817.****.****60@aa00bb01. cas.go.jp >; Sun, 25 Mar 2012 10:37:15 +0900	受信側組織内の伝送の記録
7	Authentication-Results: cas.go.jp; spf=pass reason=policy; sender-id=pass reason=policy	受信側メールサーバでの 迷惑メール判定結果
8	Received: from example.jp (mail. example.jp [203.0.113.1]) by cas.go.jp with ESMTP id D098B19 for <taro2@cas.go.jp>; Sun, 25 Mar 2012 10:37:15 +0900 (JST)	送信側メールサーバから 受信側メールサーバへの伝送の記録
9	Received: from hnkwinpc ([192.0.2.6]) by mail.example.jp with ESMTP id D098A05; Sun, 25 Mar 2012 10:37:03 +0900 (JST)	送信側組織内の伝送の記録
10	Message-ID: <IMTw1fOIffff0KsJ@example.jp>	送信側で付した番号
11	MIME-Version: 1.0 Content-Type: multipart/alternative ; boudary= "_Part_28873_0A61" Content-Transfer-Encoding: 7bit	本文の符号化の方式
12	内閣官房サイバー準備室　御中 お世話になっております。 添付の至急ご確認をお願いします。 oo花子　拝	本文 （実際には符号化されて伝送。 左欄は復号化後の内容。以下同じ。）
13	重要書類.docx	添付ファイル名 （技術的には本文の一部）
14	これは重要書類です。直ちに保存して、なるべく多くの方に共有をお願いします。 よろしくお願いします。 84 a7 f3 9b 61 c1 08 99 27 1d 44	添付ファイルの内容 （技術的には本文の一部）

不正なコマンド
（通常は表示されない）

受信側メールサーバ等が追加する情報


サイバー攻撃の実態を踏まえ、アクセス・無害化についての総論的な意思決定
国家安全保障会議（NSC）
※サイバー安全保障担当大臣・防衛大臣・国家公安委員長も参加
対処方針
個別のアクセス・無害化措置について、警察・自衛隊の役割分担等を検討・決定
内閣官房
サイバー安全保障担当大臣
指導
連携
国家安全保障局
国家安全保障局長
新組織
サイバー安全保障担当大臣の下、内閣官房による強力な総合調整
個別のアクセス・無害化措置の執行（現場の指揮と監督責任は警察庁長官及び防衛大臣が負う）
措置を承認
独立機関
警察・自衛隊（同一の建物で勤務するなど緊密に連携）

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。

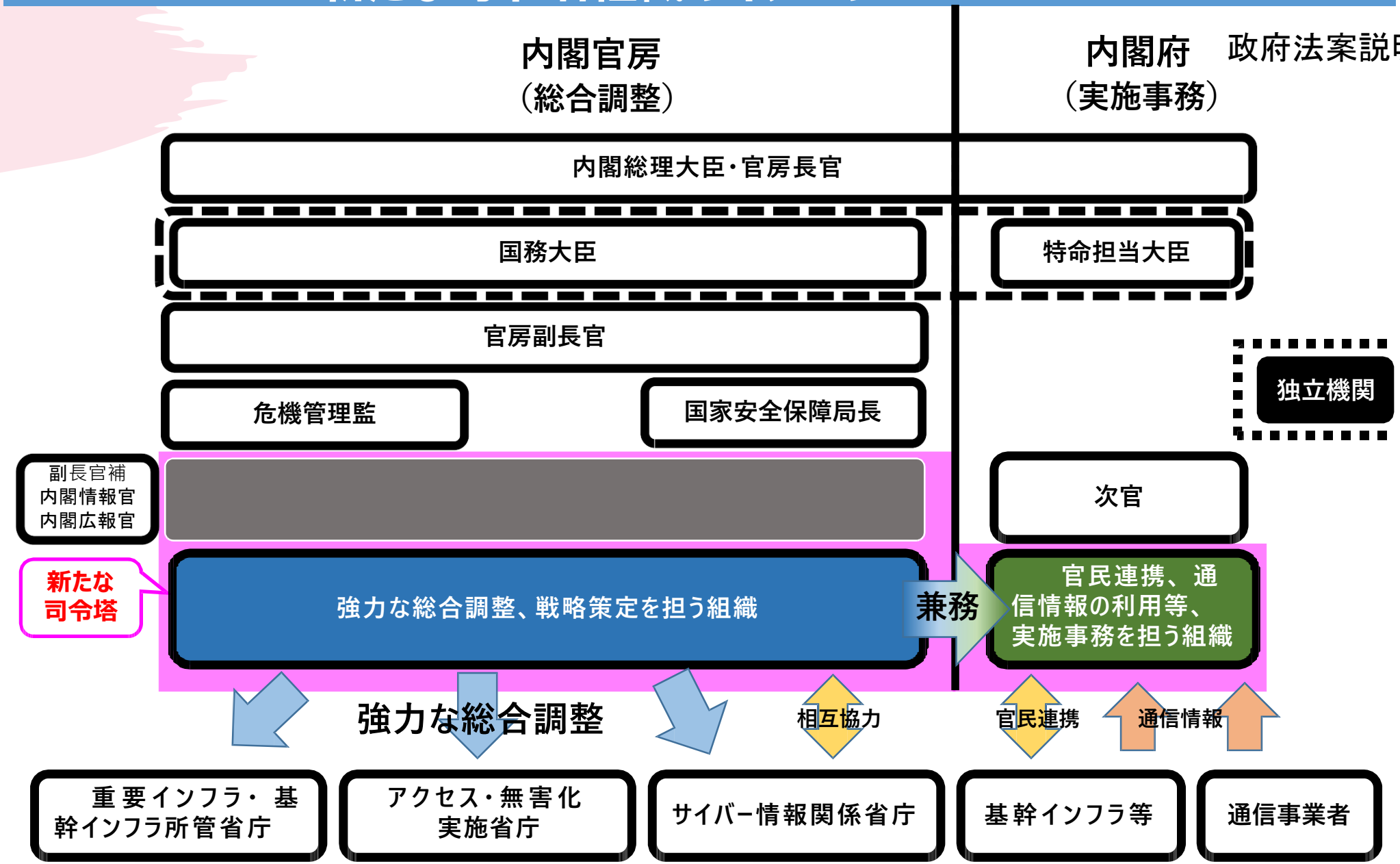
国際法の緊急避難の要件に従うと説明資料には書かれているが。

- 「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。」

- しかし、法案の定める要件が、タリンマニュアルの緊急避難の要件に適合していないことは後述する通り。

新たな司令塔組織のイメージ

政府法案説明資料より



相次ぐサイバー攻撃とその被害　Ⅰ

- 米国では2021年、同国最大規模の石油パイプライン企業コロニアル・パイプラインが身代金目的でマルウエア（悪意のあるプログラム）を送り込む「ランサムウエア攻撃」の被害に遭い、五日間にわたり稼働を停止した。このサイバー攻撃は、犯罪者グループDarkSideによって行われ、DarkSideは440万ドルの身代金を要求するとともに、身代金が支払われなかった場合、搾取した約100GBのデータを漏洩させると二重の脅迫をした。コロニアル・パイプラインは、身代金を支払ったとされるが、FBIが、その大半は差し押さえたとされている。

- 日本でも2022年にはトヨタ自動車系メーカーが攻撃を受け、トヨタの国内工場が稼働を停止した。

- 2023年7月には名古屋港のコンテナ搬出入を管理するシステムがターゲットとされた。

相次ぐサイバー攻撃とその被害　Ⅱ

- 宇宙航空研究開発機構（JAXA）も、一年間に４回のサイバー攻撃で情報漏えいがあったことを2024年７月に発表した。

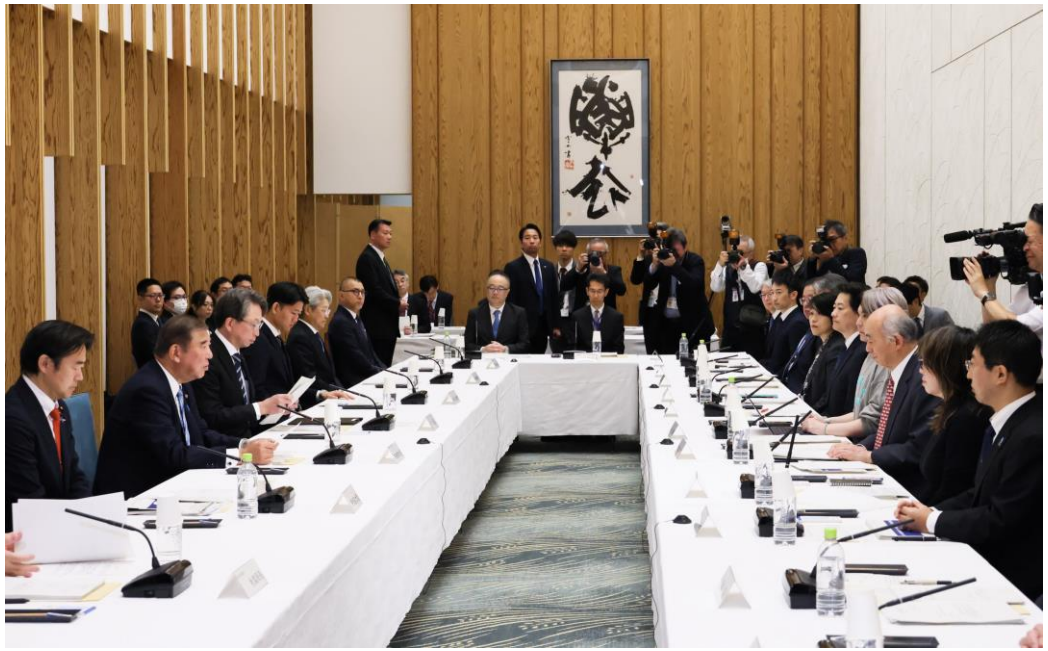
  •最近では、角川書店に対するサイバー攻撃(ロシアのハッカー集団が声明を発表している)によって、同書店の業務が長期にわたって停止した。KADOKAWAグループのサーバーでアクセス障害が起きたのは2024年6月8日。1カ月がたっても収束せず、グループ各社で多岐にわたる被害が生じたとされる。サイバー攻撃が、企業活動や市民生活に甚大な影響を与えることが改めて示された。

能動的サイバー防御とは何か?

- 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。
- そして、提言に基づいて、2025年

時系列

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提出



2024/11/29 官邸HPより

- 2024年11月29日「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」という)
- 2024年12月21日　国民民主党が議員立法として、サイバー安全保障を確保するための「能動的なサイバー防御等に係る態勢の整備の推進に関する法律案」を衆議院に提出
- 2025年１月下旬「重要電子計算機の被害の防止に関する法律案」を閣議決定し、通常国会に提出する予定
- あわせて警察と自衛隊に無害化措置を行う権限を与えるため、関連法をまとめて改正する整備法案も、提出へ

なぜ、このような制度必要なのか、そもそも許されるものなのかという前提が説明されていない

- 能動的サイバー防御制度は広範なインターネット情報を収集分析することを不可避とする制度であり、不審なサーバーの検知や攻撃者を特定するための通信記録の監視や解析は、**憲法21条が保障する通信の秘密に抵触し、プライバシーの侵害につながる可能性がある。**このような、大きな弊害をもたらす危険性のある制度を導入することを不可避とする立法事実の説明がなされていない。
- さらに、サイバー攻撃に対する対策の基本は、侵入を防ぐためのシステムの防御であり、攻撃によって食い止めるという方法は、その効果も不確実であり、他国の主権侵害行為を含み、紛争を拡大する危険性がある。
- このような制度の導入が国際法の下で、どのような要件の下で許容されうるのかが、十分検討される必要がある。

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。

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。

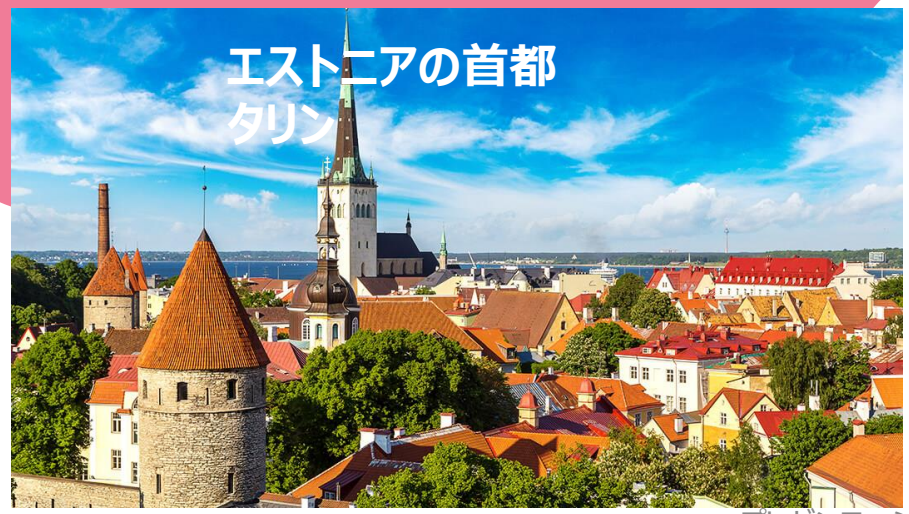
サイバー脅威監視が違憲とされたポイント

- 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。

決定は、違憲と判断しつつ、制度の早期改正を促した

- 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る。
- 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る。

第2　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

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―」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。

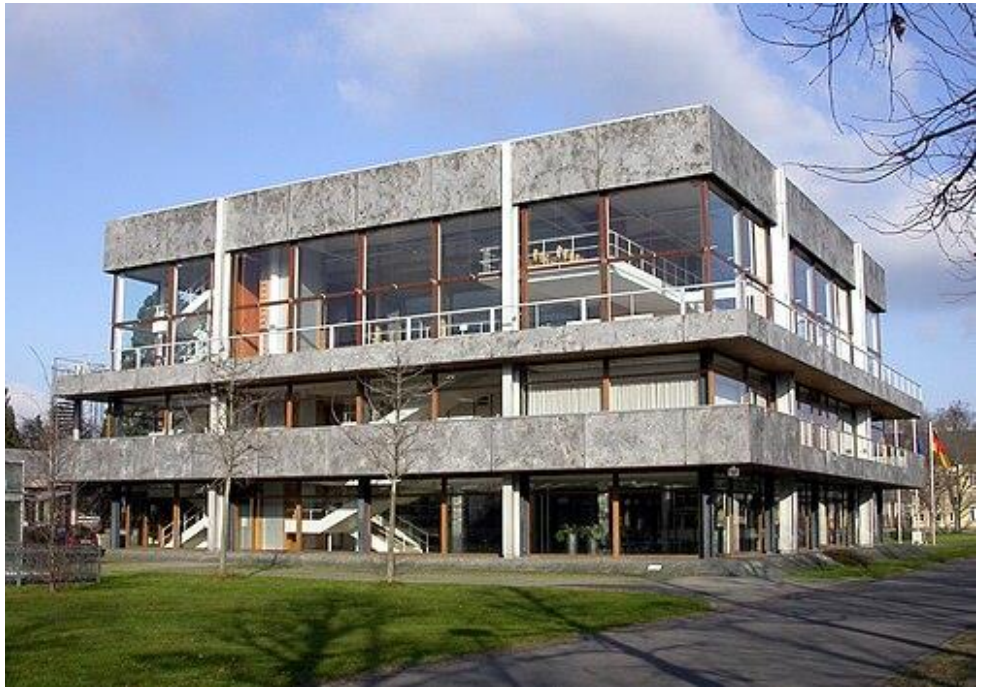
タリンマニュアル2.0の主要な条項

- 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3　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＝



カールスルーエにある
ドイツ連邦憲法裁判所

我が国に対する**サイバー攻撃の実態を把握するため、通信情報を利用し、分析**。これらについては、独立機関がチェック。制度設計に当たっては、**「通信の秘密」に十分配慮**

基幹インフラ事業者等との協定（同意）に基づく通信情報の取得

（新法第３章関係）

- 内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得（このうち、外内通信に係る通信情報を用いて分析を実施、当該事業者に必要な分析結果を提供）

（同意によらない）通信情報の取得

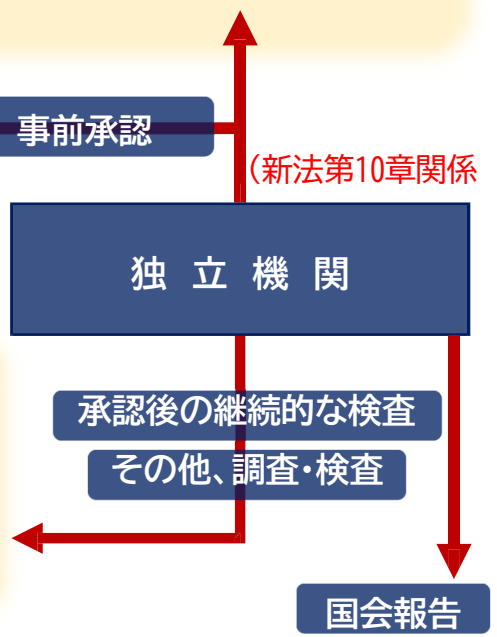
【外外通信の分析】

- 内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得（新法第４章関係）

【外内通信又は内外通信の分析】

- 内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得（新法第６章関係）

（※）外外通信：国内を経由し伝送される国 外**から国外への通信**
外内通信：国外から国内への通信 内
外通信：国内から国外への通信



自動的な方法による機械的情報の選別の実施（新法第２条第８項、第５章、第７章関係）

- 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

（それ以外のものを直ちに消去）

※ 機械的情報とは、アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報

※ その他、「関係行政機関の分析への協力」（新法第27条関係）、「取得した通信情報の厳格な取扱い」（新法第23条関係）等を規定

政府説明資料より

（同意によらない）通信情報の取得（新法第４章、第６章）

（外外通信の分析のための取得） 内閣総理大臣は、外外通信であって、他の方法ではその実態の把握が著しく困難であるサイバー攻撃に関係するものが、特定の電気通信設備により伝送されていると疑うに足りる状況がある場合には、サイバー通信情報監理委員会の承認（☆１）を受けて、当該電気通信設備から通信情報が送信されるようにする措置（☆２）をとることができることとする。（第17条、第18条）

（外内通信又は内外通信の分析のための取得） 内閣総理大臣は、外内通信又は内外通信であって、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外国設備と送受信し、又は当該状況のある機械的情報が含まれているものの分析をしなければ被害防止が著しく困難であり、他の方法ではこれらの通信の分析が著しく困難である場合には、サイバー通信情報監理委員会の承認（☆１）を受けて、これらの通信が含まれると疑うに足りる外国関係通信を伝送する電気通信設備から通信情報が送信されるようにする措置（☆２）をとることができることとする。（第32条、第33条）

☆１　委員会は承認の求めがあった場合において、理由があると認めるときは、遅滞なく承認する。

☆２ ここで送信されるものは、国外関係通信、すなわち、外外通信、外内通信及び内外通信であるが、自動選別を行うことにより、それぞれ分析に必要なものが選別されることになる。

調査すべき情報の選別（新法第２条第８項、第５章、第７章）

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、対象とすべき通信のうち機械的情報（☆）であって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状況があるものを、承認を受ける際に定めた基準に基づき選別した後、それ以外のものを直ちに消去する措置を講ずることとする。（「自動選別」）（第22条、第35条）

☆　アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報（第２条第８項）

取得情報の利用･共有について(第23条･29条関係)(政府による福島みずほ議員に対する説明)

- 第23条第4項で目的外利用の規定を設けているのは、「特定被害」ではない被害(「重要電子計算機」以外のコンピューターに対する攻撃等)の防止等に提供された情報を活用できるようにするため。
- 第29条で情報提供の対象とされている「その他の者」については、特段の限定はない。基幹インフラ事業者並みの秘密保持に関する合意をした相手には情報を渡せるような規定になっている。例えば、既に行われたサイバー攻撃と同様の攻撃の対象になると考えられる相手に予防策を教える場合等が想定される。
- 第29条に基づいて提供される情報は、自動選別によって取り出されたものの内、「提供したとしてもその通信の当事者の通信に係る権利利益の保護に支障を生ずるおそれがない」ものだけ取り出したもの。
- 取得情報を犯罪捜査等に活用したいという行政機関もあるが、そのようなことが出来ないよう、自動選別で人の目に触れない形で選別を行い、通信の中身は全部自動的に消去する(ただし、メールアドレスは発信者の特定に関わるので消さない)。

政府説明資料より

当事者協定（同意）に基づく通信情報の取得（新法第３章）

内閣総理大臣は、基幹インフラ事業者その他の電気通信役務の利用者との協定に基づき、当該利用者が送受信する通信情報の提供を受けることとする（この通信情報のうち、外内通信に係る通信情報を用いてサイバーセキュリティ確保のための分析を行うとともに、当該利用者のサイバーセキュリティの確保のため必要な分析結果を提供することとする）。（第11条～第13条）

☆内閣総理大臣及び基幹インフラ事業者は、相互に、相手方に対し、協定締結のための協議の求めをすることができることとし、相手方は、正当な理由がない限り、協議に応じなければならないこととする（協定はあくまで任意）。

☆　前ページの「調査すべき情報の選別」（自動選別）は、協定に基づき取得した通信情報についても実施。

関係行政機関の分析への協力（新法第５章第27条）

内閣総理大臣は、自動選別又は選別後の通信情報の分析をするために必要があると認めるときは、防衛大臣その他の関係行政機関の長に対し、必要な協力を要請できることとし、要請を受けた関係行政機関の長は、その所掌事務に支障を生じない限度において、協力を行うものとする。（第27条）

取得した通信情報の厳格な取扱い（新法第５章第23条）

内閣総理大臣は、取得した通信情報について、自動選別を行う場合を除き、選別前の通信情報を自ら利用し、又は提供してはならないこととする。選別後の通信情報についても、関係行政機関に分析協力を要請する場合、アクセス・無害化を行う行政機関に提供する場合等を除き、提供してはならないこととする。（第23条）

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((新法第12条関係)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、がいない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。

政府説明資料より

独立機関の設置等（新法第10章）

○　通信情報の利用の適正確保のため、サイバー通信情報監理委員会（いわゆる３条委員会）を置くこととする。　（第46条）

○　委員会に、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、無害化措置に際しての審査・承認等の事務を行わせることとするほか、通信情報を保有する機関に対する勧告等の権限を付与する。
（第63条～第68条）

○　委員会は、委員長及び委員４人をもって組織する。また、委員長及び委員は、専門的知見を有する者等から両議院の同意を得て、内閣総理大臣が任命する。　（第50条）

○　また、同委員会は、その所掌事務の処理状況について、国会に報告するとともに、その概要を公表しなければならないこととする。　（第61条）

罰則の整備（新法第12章）

・通信情報を取り扱う行政職員による、通信情報の不正な利用・漏えいの行為
　データベース提供については、４年以下の拘禁刑又は200万円以下の罰金
　⇨ その他は、３年以下の拘禁刑又は100万円以下の罰金　（第79条、第81条）

・通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為
　⇨ ３年以下の拘禁刑又は150万円以下の罰金　（第80条）

・その他の行政職員及び協議会の事務の従事者による秘密の不正な利用・漏えいの行為
　⇨ ２年以下の拘禁刑又は100万円以下の罰金※官民連携関係　（第82条）　等

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るのだろうか。
- 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。

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。

戦略的電子監視による干渉の深刻さ

戦略的電子監視による、プライバシー侵害の深刻さについてのドイツ連邦憲法裁判所決定

- 戦略的電気通信監視は、特に、そのような監視が特定の根拠を必要とせずに誰に対しても使用でき、監視によって追求される特定の目的によってのみ制限されることを考えると、特定の深刻な干渉をもたらす手段です。
- 通信技術の現在の現実と、それが通信に与える影響の重要性を考えると、通信技術は非常に普及しています。
- 問題となっている権限に起因する干渉の深刻さは、連邦憲法裁判所が1999年に国際通信を対象とする戦略的監視措置に関する決定で取り上げた権限の深刻さを大幅に上回っています(連邦憲法裁判所の判決、Entscheidungendes Bundesverfassungsgerichts -BVerfGE (Entscheidungen des Bundesverfassun gsgeri chts)100, 313)。
- 同時に、諜報機関が利用できる分析の可能性も広がっています。正式な検索用語を使用することが可能になったため、戦略的通信監視は、個人を対象とした通信監視により密接に類似しています。

ドイツ連邦憲法裁判所も、監視(無害化は含まない)の必要そのものは認めている

- ドイツ連邦共和国にとって外交政策や安全保障政策の観点から重要な他国からのサイバー脅威を早期に検出することには、非常に大きな公共の利益があり、重要なデジタルインフラや同様に重要なITシステムの保護には非常に大きな公共の利益があります。ドイツでは、ITシステムに対する国際的なサイバー攻撃の割合が高く、増加し続けています。国際的なサイバー攻撃によって引き起こされる潜在的な損害は、非常に甚大です。社会、経済、行政、政治のデラタル変革を考えると、生活のほぼすべての側面が、適切に機能し、安全なデジタルインフラストラクチャにますます依存しています。憲法上の機関や憲法秩序の他の必要な要素も、その任務を遂行するためにITシステムの使用にますます依存するようになっています。
- 重要なデジタルインフラや同様に重要なITシステムに対する国際的なサイバー攻撃は、社会を不安定化させることを目的としており、憲法秩序、連邦や州の存在と安全、生命、身体、自由を危険にさらす可能性があります。社会のデジタル変革を考えると、水やエネルギーの供給、輸送、医療など、重要かつ重要な分野のITインフラに対する国際的なサイバー攻撃の危険性は、武力攻撃に匹敵するレベルに達する可能性があり、これは、法第10条第5条第H頁第3文第1号において、戦略的な電気通信監視の正当な根拠として常に認識されてきました。

しかし、有識者会議提言における収集の対象から外内、内外通信、さらには関連する内内通信も確実に除外されるとは限らない

- 通信情報の利用による効果と通信の秘密への影響は、利用の範囲及び方式の内容によって、変わり得る。
- その際、通信情報の分析は、問題を未然に防ぐ予防のための分析であるため、過去になされた行為について真実を解明することを目的とする犯罪捜査とは方法が異なり、「最初は広く、懸念が見つかったら深く」という考え方が妥当である。
- また、制度全体として重大サイバー攻撃対策の観点で弱点がないものとなるよう検討していくべきである。
- 具体的にはまず国外の通信か、国内の通信か、という観点では、攻撃用のインフラを構成するボットやC2 サーバの多くは国外に所在することから、国外が関係する通信について、通信情報を分析する必要が特にある。
- そして、多くが国外所在と考えられるそうした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（国内を経由して伝送される国外から国外への通信）」については、先進主要国と同等の方法（コミュニケーションの本質的な内容ではないデータに注目する方法）の分析をできるようにしておく必要がある。
- 加えて、国外に所在する潜在的な攻撃者から国内に対して攻撃がなされるという状況を踏まえ、「外内通信（国外から国内への通信）」及び「内外通信（国内から国外への通信）」についても、被害の未然防止のために必要な分析をできるようにしておくべきと考えられる。
- このうち、国外からの攻撃に関係する通信が含まれる「外内」通信だけでなく「内外」通信まで分析する必要性が想定されるのは、例えば、国内でマルウェア等に感染したコンピュータが国外の攻撃元に通信を送信している場合である。
- また、外内通信及び内外通信の分析は、我が国への国際的な信頼の失墜につながり得る、国内の領域にボット等が所在し攻撃の一端となるような事例の発生の未然防止や、国際社会における国内の領域で行われている行為の説明責任を果たすことにもつながるものである。

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。

メールの中身を逐一見ることは適当でないとしつつ、メールの中身は見てはならないとは提言は述べていない

- 分析の対象とする必要がある情報の範囲について、通信情報は、ｉ）電気通信設備等を識別する情報、ii）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、iii）その他機械的な情報、iv）個人のコミュニケーションの本質的内容に関わる情報、に主に分類できるが、このうちiv）は重大サイバー攻撃対策のためには特に分析する必要があるとまでは言えない。すなわち、メールの中身を逐一全て見るようなことは、重大サイバー攻撃対策としては適当とは言えない行為である。
- 加えて、収集したデータ全てについて人間の目で判断することは不可能であり、またプライバシー保護等の観点から適切でもない。重大サイバー攻撃対策に必要な情報を取り出すため、機械的にデータを選別するとともに、検索条件等で絞っていくなどの工夫が必要である。

- なお、ｉ）からiii）に当たる、特に分析する必要があると考えられる情報（コミュニケーションの本質的な内容ではない通信情報）は、いわゆる「メタデータ」に限られるものではないと考えられる。

メタデータしか収集しない、外国との通信だけを監視するというのは本当か？

- 内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得し、このうち、外内通信に係る通信情報を用いて分析を実施し、事業者に必要な分析結果を提供するとされている。基幹インフラ事業者が政府に提供する情報そのものには、何でも含まれるのではないか。そして、この情報については任意に提供を受けたものであるからだろうが、必要なもの以外はすぐに消去するという規定もない。
- そして、内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得できる。
- さらに、内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得することができる。これらの情報にも内内通信は含まれている。

「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。

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ぜん。**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。

「文書の保存期間が、効果的な保護を受けるには短すぎる」

- さらに、国際電気通信の戦略的監視に関する文書の保存期間が短すぎる。第10条法第5条第21頁第6文は、文書が記録された年の翌暦年の終わりに文書を削除しなければならないと規定しています。
- この期間は、影響を受ける人々が効果的な法的保護を受けるには短すぎます。厳格な期限は、影響を受ける人々の通知を規定する規定とはまったく関連していません。通知は、それぞれの措置が恒久的に終了した場合にのみ行われます。その時点では、ログデータがまだ存在するという保証はありません。

ドイツ連邦憲法裁判所　法廷と裁判官

第4　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?

2025/1/26 読売新聞予測報道

政府説明資料より

独立機関の設置等（新法第10章）

○　通信情報の利用の適正確保のため、サイバー通信情報監理委員会（いわゆる３条委員会）を置くこととする。　（第46条）

○　委員会に、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、無害化措置に際しての審査・承認等の事務を行わせることとするほか、通信情報を保有する機関に対する勧告等の権限を付与する。
（第63条～第68条）

○　委員会は、委員長及び委員４人をもって組織する。また、委員長及び委員は、専門的知見を有する者等から両議院の同意を得て、内閣総理大臣が任命する。　（第50条）

○　また、同委員会は、その所掌事務の処理状況について、国会に報告するとともに、その概要を公表しなければならないこととする。　（第61条）

罰則の整備（新法第12章）

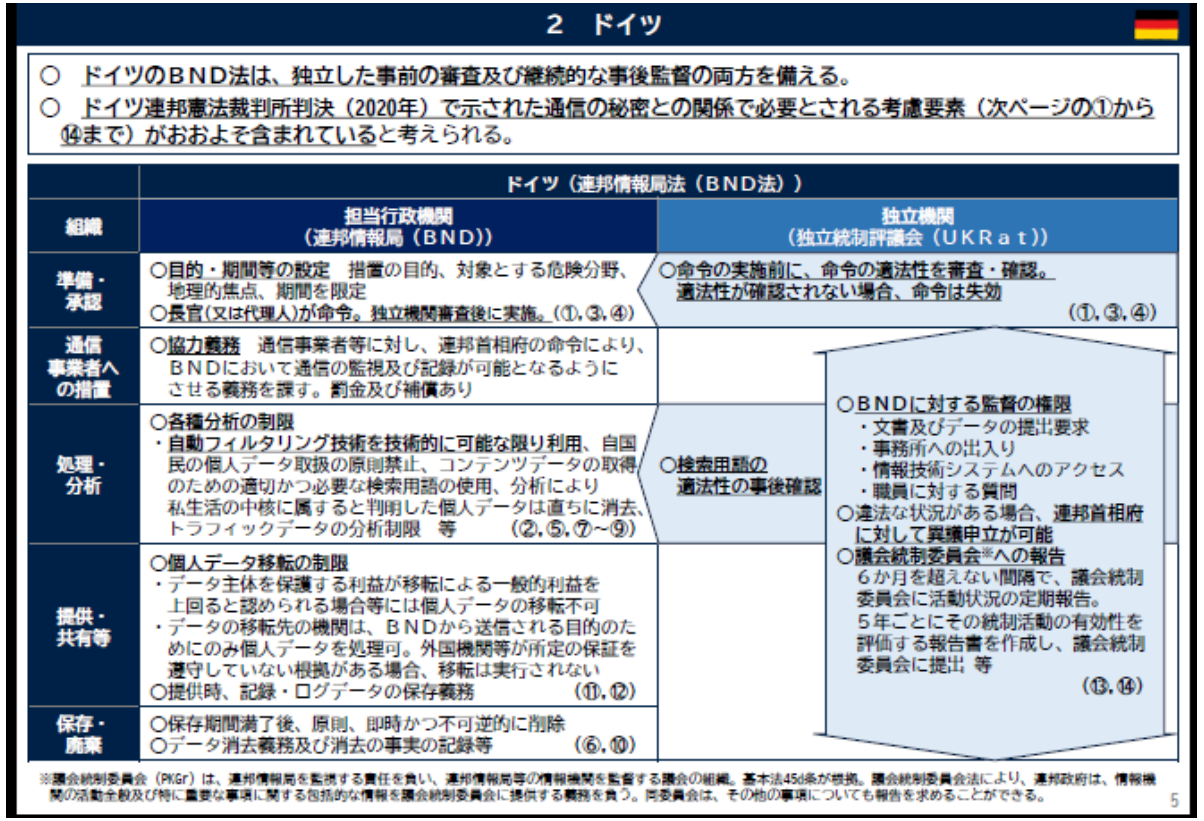
・通信情報を取り扱う行政職員による、通信情報の不正な利用・漏えいの行為
　データベース提供については、４年以下の拘禁刑又は200万円以下の罰金
　⇨ その他は、３年以下の拘禁刑又は100万円以下の罰金　（第79条、第81条）

・通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為
　⇨ ３年以下の拘禁刑又は150万円以下の罰金　（第80条）

・その他の行政職員及び協議会の事務の従事者による秘密の不正な利用・漏えいの行為
　⇨ ２年以下の拘禁刑又は100万円以下の罰金※官民連携関係　（第82条）　等

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
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）	

○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）

※議会統制委員会（PKGr）は、連邦情報局を監視する責任を負い、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

イギリスでも、情報収集は認められるが、独立の監督機関が設けられている。

- 英国では、海外からの通信を対象に、安全保障上の必要や重大犯罪の検知を目的にした情報収集が認められている。
- この権限は情報機関が大臣に申請して大臣が許可状を発行する(1994年情報機関法第5条)。
- 取得した情報の閲覧や複製などは必要最小限に制限され、独立の監督機関として調査権限コミッショナーが設置されている(2016年調査権限法229条)。


英情報機関・秘密情報部（MI6）の本部＝ロンドンで1月24日、篠田航一撮影

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、こ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。**

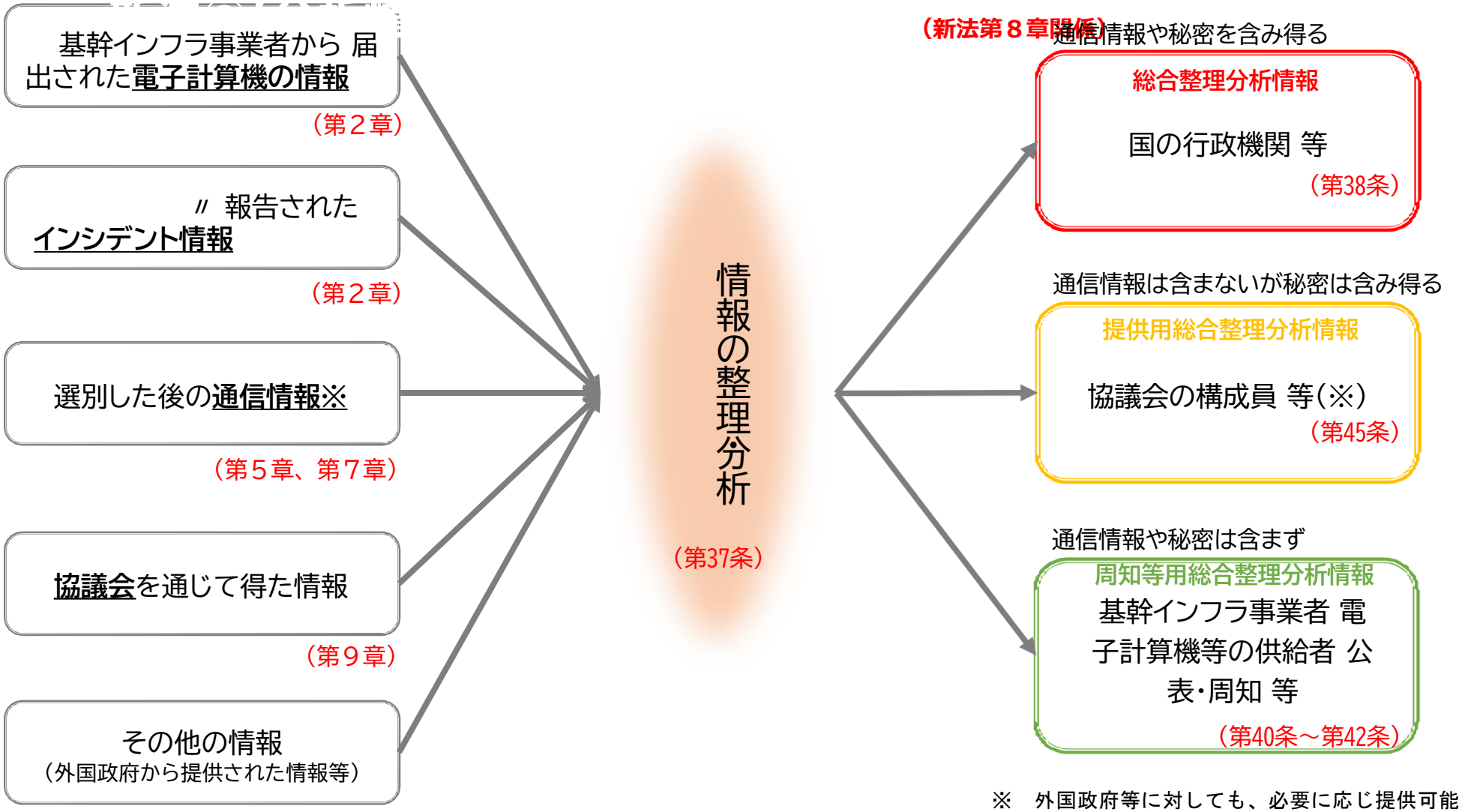
サイバー通信情報監理委員会はプライバシー保護のための機関ではなく、情報漏洩の監視機関となる見通し

- 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。おそらく、間もなく姿を現す法案では、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。

能動的サイバー防御法案は、防御という名のサイバー攻撃を合法化し、市民の「通信の秘密」を侵害し、市民監視のシステム構築につながりかねない

- 能動的サイバー防御の制度は二つに分け、ネットの監視の部分と無害化の措置をとるとされる部分に分けて議論をする必要がある。
- ネット監視の部分は、ドイツ連邦憲法裁判所の決定を参考に、プライバシー侵害の起きない制度設計について、見直すべきことを主張していくべきであろう。
- 制度の必要性にも根本的に疑問があるが、世界のすう勢だとして、仮にこのような制度を導入するとしても、プライバシーの侵害を防止し、深刻な国際紛争の発生を回避するためには、明快な承認要件と独立機関による事前審査と継続的な事後監督の制度を備えることは、最低限の要件であり、法案はいったん撤回したうえで、再検討すべきである。

第5　情報の分析・整理とは何を行うのか?



※　外国政府等に対しても、必要に応じ提供可能。
（第28条、第39条）

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。

政府説明資料より

分析情報の提供等（新法第８章）

○　内閣総理大臣は、基幹インフラ事業者によるインシデント報告等に係る情報を含め、取得した情報を整理・分析し、その情報を、サイバーセキュリティ確保のため、アクセス・無害化を行う行政機関その他関係行政機関に提供するものとする。また、内閣総理大臣は、必要がある場合には、外国の政府等に対し、分析情報を提供することができることとするほか、事業所管大臣も、必要がある場合にはその情報を基幹インフラの事業者に提供することができることとする。（第37条～第40条）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止に必要な情報を公表・周知する。（第41条）

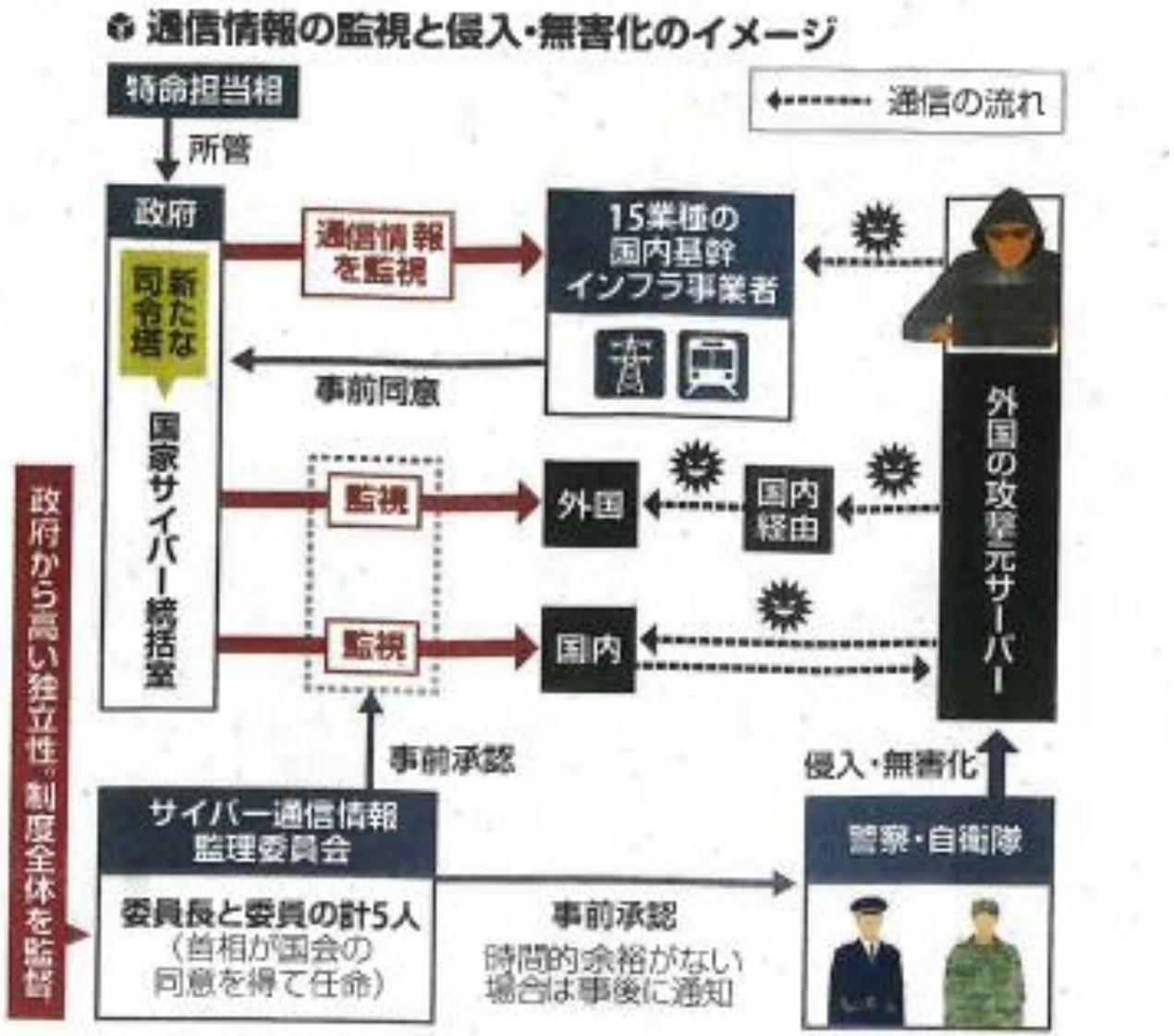
（再掲）　内閣総理大臣及び電子計算機等供給事業所管大臣（☆１）は、重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知したときには、当該電子計算機等の供給者（☆２）に対し情報を提供することができることとする。（第42条第１項）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。（第45条）

罰則の整備（新法第12章）

・行政職員及び協議会構成員等による秘密の不正な利用・漏えいの行為
　⇨　２年以下の拘禁刑又は100万円以下の罰金　（第82条）

第6　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

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。

政府法案説明資料より

サイバー攻撃による重大な危害を防止するため の**警察・自衛隊による措置** 等を可能とし、その際の**適正性を確保するための手続** を新設

警　　察

（警察官職務執行法第6条の2関係）

- 措置の主体は、警察庁長官が指名した警察官に限定
- 措置を実施する場面は、

① サイバー攻撃に用いられる電気通信等を認めた場合で

② そのまま放置すれば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

- 措置の内容は、

① 攻撃関係サーバ等の管理者等への措置の命令

② 攻撃関係サーバ等への措置(※)を自ら実施

(※)インストールされている攻撃のためのプログラムの停止・削除など

- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、警察庁長官等の指揮

（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：事後通知）

申請 ↓　↑ 承認

防衛省・自衛隊

（自衛隊法第81条の3・第91条の3・第95条の4関係）

- 内閣総理大臣が次の場合に通信防護措置を命じた上で、自衛隊の部隊等が措置を実施（新たな行動類型）（警察と共同対処）

① 一定の重要な電子計算機に対するサイバー攻撃であり

② 外国政府を背景とする主体による高度な攻撃と認められるものが行われ

③ 自衛隊が対処する特別の必要(※)があるとき

(※)自衛隊が有する特別な技術又は情報が必要不可欠であるなど

- 自衛隊及び日本に所在する米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官が、緊急の必要があるときに無害化措置を実施
- 措置を実施する場面・措置の内容は、警察と同様
- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、防衛大臣の指揮

（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：事後通知）

申請 ↓　↑ 承認

内閣官房(※)の調整の下で緊密に連携

独　立　機　関

（※）アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮。

政府法案説明資料より

アクセス・無害化措置（警察官職務執行法（警職法）第６条の２）

○ 警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、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は、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、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こととする。

○ 処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、警察庁の警察官のみが処置をできることとし、あらかじめ、警察庁長官を通じて、外務大臣と協議しなければならないこととする。

○ サイバー危害防止措置執行官が、上記の処置をとる場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならないこととする。
　ただし、サイバー通信情報監理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ないこととし、当該処置後速やかに、当該処置についてサイバー通信情報監理委員会に通知しなければならないこととする（同委員会は、必要に応じ勧告を実施）。

○ サイバー危害防止措置執行官は、措置の実施について、警察庁長官又は都道府県警察本部長の指揮を受けなければならないこととする。

（※）アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮。

政府法案説明資料より

アクセス・無害化措置（自衛隊法第81条の３、第91条の３及び第95条の４）

○ 内閣総理大臣は、一定の重要電子計算機（☆１）に対する攻撃であって、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（☆２）と認めるときは、当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができることとする（新たな行動類型の創設）。

☆１　国の行政機関等、地方公共団体、基幹インフラ、一定の防衛産業の重要な電子計算機。
☆２　☆１の電子計算機がサイバー攻撃を受け、国家及び国民の安全を著しく損なう事態が生じるおそれが大きく、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、国家公安委員会から要請又はその同意がある場合。

○ 通信防護措置をとるべき旨を命ぜられた部隊等は、警察と共同して当該通信防護措置を実施することとする。

その際、改正警職法を準用し、処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、上記処置をとる当該部隊等の自衛官は、あらかじめ、防衛大臣を通じて、外務大臣と協議しなければならないこととする。 また、上記処置をとる当該部隊等の自衛官は、あらかじめ、防衛大臣を通じて、サイバー通信情報監理委員会の承認を得なければならないこととする。ただし、同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ないこととし、当該処置後速やかに、当該処置について同委員会に通知しなければならないこととする（同委員会は、必要に応じ勧告を実施）。

さらに、当該部隊等の自衛官は、措置の実施について、防衛大臣の指揮を受けなければならないこととする 。

○ 自衛隊又は日本国にあるアメリカ合衆国の軍隊が使用する一定の電子計算機をサイバー攻撃から職務上警護する自衛官についても、同様に改正警職法の権限を準用することとする。

政府法案説明資料より

能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる**内閣官房新組織の設置** 等、**政府を挙げた取組を推進するための体制を整備**(内閣官房(司令塔・総合調整)と内閣府(実施部門)が一体となって機能)

サイバーセキュリティ戦略本部の強化

(サイバーセキュリティ基本法第26条・第28条・第30条・第30条の2関係)

- サイバーセキュリティ戦略本部の改組

  サイバーセキュリティ戦略本部を

  ・本部長:内閣総理大臣
  ・本部員:全ての国務大臣

  とする組織に改組

  ※ 有識者から構成される「サイバーセキュリティ推進専門家会議」を設置

- サイバーセキュリティ戦略本部の機能強化

  サイバーセキュリティ戦略本部の所掌事務に

  ・ 重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成
  ・ 国の行政機関等におけるサイバーセキュリティの確保の状況の評価

  を追加

内閣サイバー官の設置

(内閣法第19条の2及び第16条関係)

- サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を内閣官房に新設

※1 内閣サイバー官は、国家安全保障局次長を兼務

※2 内閣サイバーセキュリティセンター(NISC)の改組は政令で実施予定

内閣府特命担当大臣の設置等

(内閣府設置法第4条・第9条関係)

- 官民連携や通信情報の利用に関する事務を内閣府の所掌事務に追加
- これら事務を掌理する内閣府特命担当大臣の設置が可能

政府法案説明資料より

サイバーセキュリティ戦略本部の改組（サイバーセキュリティ基本法第28条、第30条及び第30条の2）

サイバーセキュリティ戦略本部について、内閣総理大臣を本部長、全ての国務大臣を本部員とする組織に改組するとともに、有識者から構成されるサイバーセキュリティ推進専門家会議を設置する。

サイバーセキュリティ戦略本部の機能強化（サイバーセキュリティ基本法第26条）

サイバーセキュリティ戦略本部の所掌事務を見直し、

- 重要社会基盤事業者等のサイバーセキュリティ確保に関する国の基準の作成
- 国の行政機関等におけるサイバーセキュリティの確保の状況の評価　等

をその所掌事務に追加することとする。

（独）情報処理推進機構（IPA）における事務の追加（情促法第51条）

新法の制定及び戦略本部の機能強化に伴い、（独）情報処理推進機構の事務に（新法第11章）

- 情報の整理分析及び被害防止に必要な情報の周知等の事務（内閣総理大臣からの委託）
- 重要社会基盤事業者等のサイバーセキュリティの確保の状況の調査（戦略本部からの委託）

を追加することとする。（サイバーセキュリティ基本法第31条）

（国研）情報通信研究機構（NICT）における事務の追加（NICT法第14条）

戦略本部の機能強化に伴い、（国研）情報通信研究機構の業務に、国等の情報システムに対する不正な活動の監視及び分析に係る事務（戦略本部からの委託）を追加することとする。

（サイバーセキュリティ基本法第31条）

政府法案説明資料より

内閣府における所掌事務の追加等（内閣府設置法第４条、第64条）

新法の制定に伴い、内閣府の所掌事務に新法に関する事務（☆）を追加するとともに、同府に、サイバー通信情報監理委員会を置くこととする。

☆　新法に基づく重要電子計算機に対するサイバー攻撃による被害の防止に関する事務（「官民連携の強化」及び「通信情報の利用」に関する部分）

内閣府特命担当大臣の設置（内閣府設置法第４条、第９条）

新法の施行に伴い、内閣府設置法を改正することにより、新法に関する事務を掌理する内閣府特命担当大臣を置くことができることとする。

内閣サイバー官の新設（内閣法第19条の２、第16条）

○ 内閣官房に、サイバーセキュリティの確保に関する事務等を掌理する内閣サイバー官（次官級の特別職）一人を新たに置くこととする。

○　国家安全保障局次長を３人に増やすこととし、内閣サイバー官をもつて充てることとする。

☆　内閣サイバーセキュリティセンター（ＮＩＳＣ）の改組については、政令改正において措置する予定。

政府法案説明資料より

その他所要の改正（整備法第１条、第３条、第８条から第11条まで、第14条及び附則第５条）

新法の施行に伴い、その他以下の法律を改正。 国家公務員法、特別職の職員の給与に関する法律

、行政機関が行う政策の評価に関する法律 等(※)

（※）情報通信技術を活用した行政の推進等に関する法律、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律、産業競争力強化法、情報通信技術を利用する方法による国の歳入等の納付に関する法律、デジタル庁設置法

• 施行期日（新法附則第１条、整備法附則第１条）

- 【新法】一部を除き、公布の日から起算して１年６月を超えない範囲内において政令で定める日
  - ☆ サイバー通信情報監理委員会の設置については１年を超えない範囲内において政令で定める日、通信 情報の利用については一部を除き２年６月を超えない範囲内において政令で定める日。

- 【整備法】新法の施行の日
  - ☆ サイバーセキュリティ戦略本部の改組、内閣サイバー官の設置等については、６月を超えない範囲内 において政令で定める日から施行。

海外の実態も不明な部分が多い。

- 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、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。
- ぎりぎり、ドイツ連邦憲法裁判所の判断枠組みに沿って、戦略的監視は認めるとしても、無害化の措置は削除すべきだ。

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（白鷗大・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)。

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。
- 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。

無害化についてⅠ
(政府による福島みずほ議員に対する説明)

- 無害化を行わなければならない理由は、サイバー攻撃は様々なサーバーを経由して行われるため、攻撃の大本にたどり着くことが出来ないから。そこでボットネットを辿り、出来るだけ上流にあるコマンドサーバーを無力化することが必要になる。
- 国内のサーバーが踏み台にされていれば、そのサーバーを提供している事業者の協力を得ることになる。
- ボットネットの中で踏み台にされるサーバーは、「乗っ取られている」ものなので、それを無力化しても、乗っ取った張本人がその無力化は不正だ、先制攻撃だ、等と名乗りを上げることは考えられない。ただし、無力化が、その対象となったサーバーが存在する国の主権を侵害すると言われる可能性はある。
- 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。

無害化についてⅡ
(政府による福島みずほ議員に対する説明)

- 今行われているサイバー攻撃は、実験のようなもの。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。
- まずはサイバー攻撃に対する防御力を高めることが大切だが、防御をするにも限界がある。仮に防御が出来ても、それをすることで本来の業務が困難になったり、コストがかかりすぎたりする場合がある。そのため無力化が必要になる。
- 警察官が無力化を行う場合、その主体は「サイバー危害防止措置執行官」に限られ、しかも警察庁長官(または都道府県警本部長)の指揮を受けて動く。警察は単独でアクセス無害化を行うことはあり得るが、自衛隊は必ず警察と共に行う。
- アクセス無害化は、外国の場合は情報機関(例えばイギリスの政府通信本部GCHQ)が行っている場合もある。無害化は、乗っ取られたサイバーの穴を見つけ、そこから内部に侵入すれば実行可能。

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、緊急の場合は事後承認とされている。
- 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。

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。

専門家の冷静な見方
八田真行　駿河台大学経済経営学部教授

- 能動的サイバー防御は海外ではプロアクティブ・サイバー・ディフェンスと呼ばれ、米国や英国などで政策となっています。
- インターネットやAIなど様々な形でサイバー空間が物理インフラのような現実世界にも影響するようになった現在、サイバー防御能力の向上が必要なのは確かですし、昔から「攻撃は最大の防御」とも言いますが、個人的には**リスクの割にあまり有効ではないのではないか**と思います。
- プライバシー侵害への懸念もさることながら、そもそも**メタデータの収集で分かることは限られていますし（宛先だけでは小包の中身が分からないのと同じ）、偽情報に釣られて偶発的に（本物の）戦争が起きることもあり得る**でしょう。また、以前米国CIAからの流出資料（Vault 7）が明らかにしたように、**情報機関がゼロデイ脆弱性を秘匿することで、サイバー紛争がエスカレーションするという可能性も否定できません。**いずれにせよ、前提として事前に相当なインテリジェンス人材の育成が必須だと思われますが、そこまでの準備が今の日本にあるのでしょうか。

第7　大川原化工機冤罪事件の公安捜査が示す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。

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制度の新設に反対の声をあげていく

- 対象となる通信の絞り込み、内内通信の除外　確実に除外できる仕組み
- 私的領域の核心部分に係る情報を取得させない 「見ない」のではなく、そもそも確実に取得させない仕組みが必要
- 独立第三者機関が、真の独立性、専門性を持った歯止めとなるような制度設計を確保する
- ドイツ連邦憲法裁判所の判例、諸外国の監督機関に倣った制度の作り込みが必要だ
- 無害化措置の部分は、立法事実も不明であり、手続きが不明確であり、国際法的な検討、厳格な手続き保障も不足している。
- 法案から削除するべきである。

戦略的監視については、要件の厳格化がない限り法案反対/無害化措置については全面撤回を

- 通常国会では、国民民主党提案の「能動的なサイバー防御等に係る態勢の整備の推進に関する法律案」と政府提案による「重要電子計算機の被害の防止に関する法律案」と無害化措置についての整備法案(名称未定)が審議される。
- 国会では、制度の必要性、海外の制度との比較、限定の要件、ドイツ連邦憲法裁判所の2024年10月の決定内容に即した審議を積み重ね、法案の撤回を求めよう。
- 少なくとも、戦略的監視については、要件の厳格化がない限り法案反対を貫こう。
- 無害化措置については全面撤回を求めよう。