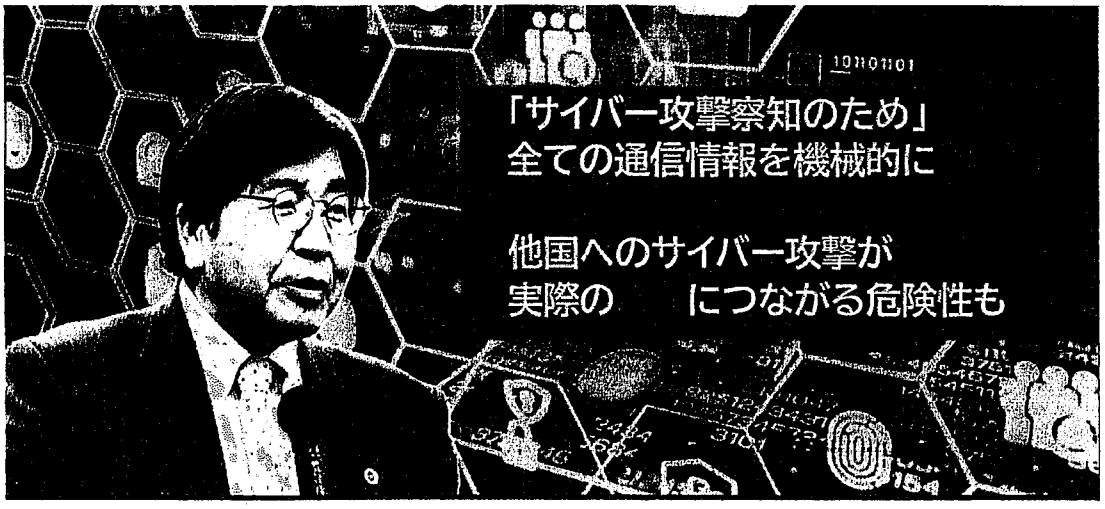
あいち総がかり行動　学習会

「能動的サイバー防御法」とは



講師：中谷雄二弁護士

2025.3.10 イーブルなごや

開始：18：00

講演：18：05～19：35

質疑：19：35～

憲法をくらしと政治にいかす　改憲NO！あいち総がかり行動
名古屋市中区大須4丁目13番46号名古屋共同法律事務所気付
052-262-7061　　090-5876-5469
メールアドレス：aichi.totalaction@gmail.com

能動的サイバー防御法案の狙いと危険性　　２０２５年3月１０日

弁護士　中谷雄二

1　能動的サイバー防御法案とは何か？

（1）サイバー防御＝サイバー攻撃から国民生活の基盤を守ること

「能動的」サイバー防御

→　他国からの攻撃の「脅威」を探索し、脅威を理由に先制的に他国に攻撃を行うこと。

（2）目的

「脅威」の探索－間違いが入る可能性　間違えた場合には、一方的な先制攻撃を日が他国に仕掛けたこととなる。

（3）方法　先制攻撃を含む点に問題－　攻撃者のサーバー等への侵入・無害化

（4）脅威の探索の手段－民間事業者の膨大な経済情報を内閣府のシステム内に取り込み官民連携の強化すでに鉄道、航空、輸送、金融、電気、ガス、水道、放送など５３社２１３事業所（基幹インフラ事業所）が契約済みで、政府と連携

－企業秘密を含む設備・プログラム・システムなどの企業情報が政府によって強権的に吸い上げて一元的に集中管理

→日本史上初の一大情報集約　官僚統制・経済統制につながりかねない危険性

（参照）法律案　概要

A　①官民連携　上記（4）

②通信情報の利用－a　基幹インフラ事業者等との協定（同意）

b　（同意によらない）通信情報の取得

c　自動的な方法による機械的情報の選別の実施

d　関係行政機関の分析への協力

e　取得した通信情報の厳格な取扱

f　独立機関による事前審査・継続的検査　等

B　アクセス・無害化措置

①警察による無害化措置

②独立機関の事前承認・警察庁長官等の指揮等（警察官職務執行法改正）＊

③内閣総理大臣の命令による自衛隊の通信防護（権限は上記を準用）

④自衛隊・在日米軍が使用するコンピュータ等の警護 等（自衛隊法改正）

2　何を懸念しているのか？

（1）戦争に結びつくのでは（軍事面）

（2）通信の秘密・プライバシー侵害の危険性→監視国家化

この間の安保法制法違憲訴訟、DNA データ等抹消事件、大垣警察市民監視事件で問題としてきた、政府の日米一体化による戦争体制作りとそのための治安体制作り＝監視国家化が結合した危険の現実化として、「能動的サイバー防御法案」が持ち出されたのではという懸念

3　日本におけるサイバーセキュリティの現状

（1）日本のサイバーセキュリティ政策

重要インフラ保護等の民政分野を中心に発展 ⇦　⇨ 軍・情報機関等が主導して政策立案

日本　　(欧米)

（2）国連の専門機関の一つ　ITU（国際電気通信連合）の国別サイバーセキュリティの　状況評価＝グローバル・サイバーセキュリティ・インデックス（GCI）

１５０か国を対象に、法制度、技術、組織、能力開発、国内外の協力関係を評価

２０２４年　GCI　法制度と組織は満点。「全ての項目で高い評価を得ている地域の　ロール・モデル」と評価

（3）他の国際機関の評価

①オーストラリア戦略研究所　サイバー成熟度調査（2017）

アジア太平洋地域の２５の国・地域において日本を２位に位置づけた。

「国際的な議論への関与、CERT（コンピュータ緊急対応チーム）の能力、インターネットの普及率」などで日本が高評価

課題：人員不足、憲法の制約、防衛産業の保護

②英国　国際戦略研究所報告書（2021．6）

米国、英国、カナダ、オーストラリア、フランス、イスラエル、日本、中国、ロシア、イラン、北朝鮮、インド、インドネシア、マレーシア、ベトナム

最も低い評価「エコシステムとして非常に良いが、インテリジェンスや攻撃的能力に欠ける」「日本は良い能力を有しているが能力開発や利用を躊躇している。」

「ハイテク産業において世界的に主導する立場にあると位置づけられる」「憲法21条の通信の秘密、憲法9条による国際紛争を解決する手段としての武力行使を放棄していることを指摘し、日本はサイバー空間における攻撃的能力が全くない」と指摘。

4　サイバー分野の安全保障への日本における重点化

（1）2006年　額賀防衛庁長官「サイバー分野における攻撃的な能力には手が回らなかった」（3月28日参議院外交防衛委員会）

2013年　安倍首相「サイバー攻撃と武力攻撃等との関係については、さまざまな議論が行われている段階であり、一概に申し上げることは困難」（3月4日衆議院本会議）

2014年　「安全保障の法的基盤の再構築に関する懇談会」報告書

「様々な主体によるサイバー攻撃が社会全体にとって大きな脅威・リスクとなっている」

「どのような場合に自衛権発動の三要件を満たすかという点や、外部からのサイバー攻撃に対処するための制度的な枠組みについて検討が必要」

2015年　中谷元防衛大臣「サイバー攻撃を仕掛けてくる場合に、そういった行為を行えば耐え難い損害を与えるんだということを明白に意識させ、そして侵略を思いとどまらせるという抑止力のためには、今までお話をしましたけれども、集団的自衛権も含めたわが国の防衛の体制をしっかり、全て法律的に対応可能とすることによってそういった場合に備える」（4月23日参議院外交防衛委員会）

＊　日米ガイドライン「日米両政府は、サイバー空間の安全かつ安定的な利用の確保に資するため、適切な場合に、サイバー空間における脅威及び脆弱性に関する情報を適時かつ適切な方法で共有する、…略…日米両政府亜、適切な場合に、民間との情報共有によるものを含め、自衛隊及び米軍が任務を達成する上で依拠する重要インフラ及びサービスを防護するために協力する。…中略…自衛隊及び日本における米軍が利用する重要インフラ及びサービスに対するものを含め、日本に対するサイバー事案が発生した場合、日本は主体的に対処し、緊密な二国間調整に基づき、米国は日本に対し適切な支援を行う。日米両政府はまた、関連情報を迅速かつ適切に共有する。日本が武力攻撃を受けている場合に発生するものを含め、日本の安全に影響を与える深刻なサイバー事案が発生した場合、日米両政府は、緊密に協議し、適切な協力行動をとり対処する」(2015. 4. 27)

2018 年　小野寺五典防衛大臣「防衛省では、中期防衛力整備計画に基づき、武力攻撃事態等において、相手方によるサイバー空間の利用を妨げることが必要となる可能性を想定しつつ、サイバー攻撃の分析機能の強化や実践的な訓練環境の整備等を行っており、その結果として、サイバー空間を通じた反撃にも対応し得る一定の知識、技能を得ております。また、わが国として、武力行使の三要件を満たす場合には、憲法上、自衛の措置としての武力の行使が許され、法理上は、このような武力の行使の一環として、いわゆるサイバー攻撃という手段を用いることは否定されないと考えます。」（4 月 12 日参議院外交防衛委員会）

2019　日米安全保障協議委員会（2+2）「サイバー攻撃を日米安全保障条約第 5 条における武力攻撃をみなし得る」と合意

2021　日本政府「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について」公表。

「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うくする虞のあるものについては、その当事者は、第一に、交渉、審査、仲介、調停、仲裁裁判、司法的解決、地域的基幹また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。」

2022. 4. 1　岸田・バイデン日米共同声明

日米軍事同盟のシームレス化、兵器の爆買い・保守・整備、兵器産業の国際分業、日米軍の一体化、米軍指揮下の自衛隊運用、国際共同兵器研究開発の推進、サイバー領域、電磁領域、スタンド・オフ防衛能力（敵基地攻撃能力、極超音速誘導弾開発）、デュアル分野（AI、量子、宇宙、海洋など）先端・新興技術分野の共同兵器開発、米英豪の安全保障（AUKUS）で、先端技術分野の軍事協力

2022. 12. 16　国家安全保障戦略　閣議決定（国家防衛戦略）

「(2) サイバー領域では、防衛省・自衛隊において、能動的サイバー防御を含むサイバー安全保障分野における政府全体での取組と連携していくこととする。その際、重要なシステム等を中心に常時継続的にリスク管理を実施する態勢に移行し、これに対応するサイバー要員を大幅増強するとともに、特に高度なスキルを有する外部人材を活用することにより、高度なサイバーセキュリティを実現する。このような高いサイバーセキュリティの能力により、あらゆるサイバー脅威から自ら防護するとともに、その能力を生かして我が国全体のサイバーセキュリティの強化に取り組んでいくこととする。 このため、2027 年度までに、

サイバー攻撃状況下においても、指揮統制能力及び優先度の高い装備品システムを保全できる態勢を確立し、また防衛産業のサイバー防衛を下支えできる態勢を確立する。今後、おおむね 10 年後までに、サイバー攻撃状況下においても、指揮統制能力、戦力発揮能力、作戦基盤を保全し任務が遂行できる態勢を確立しつつ、自衛隊以外へのサイバーセキュリティを支援できる態勢を強化する。」

2023 年　日米安全保障協議委員会（2+2）「日本の防衛産業サイバーセキュリティ基準の作成にかかる取組を含む、産業サイバーセキュリティ強化の進展を歓迎した。そして、閣僚は、情報保全に関する日米協議の下でのこれまでの重要な進展を強調した。」

2024. 11. 29　有識者会議提言

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。

ア）官民連携の強化

イ）通信情報の活用

ウ）侵入・無害化の検討を指示

5　指摘される問題点-

（1）法案の提出　手法の問題　国民民主が昨年　総論法案の提出

*束ね法案

*基本的な事項＝法律　具体的な内容は、省令に委任。

国会の形骸化-法律によって委任された省令・政令に具体化

法律による行政＝法治主義の形骸化

（2）通信の秘密、プライバシー情報の国家による機械的方法による例外なしの取得

何が監視されるのか？ー監視の対象

＊「内容は必要ない」＝除外は歯止めになるか？　＊DNA データの保管

メタ情報のみだから通信の秘密を害しない。

→通信データ（通信の開始・終了時刻、通信先、送信量、ネットワーク上のデバイス間の接続履歴、相互作用のパターン、ドキュメントやファイルの作成者、変更履歴、最終更新日時、ファイルが保存されている場所、アクセス履歴、OS のバージョン、インストールされているソフトウェア、パッチ適用状況、ターゲットとなる組織や個人の情報の収集など）＝これらは通信の秘密に当たるのではないか？

「死亡または必要がなくなったもの」＝個別判断（結局、大部分が残っていた）

「脅威」の判断のためには、内容を見なければならない。広い範囲の監視の可能性。

すべての情報が国家＝政府の下に届く仕組み

＊非識別措置-(匿名化) =24 条・一

特に必要があるときは、復元措置がとれる。プライバシー侵害の危険性を防止するものではない。

（3）監視の方法？

従前：公安警察による監視

大垣警察市民監視事件　風力発電事業の学習会を計画したことや環境問題の運動をしたこと、法

律事務所で憲法集会に関わったことが公安警察の監視の対象に警備警察全書

①視察内偵、②聞き込み、③張込み、④尾行、⑤工作、⑥面接、⑦投入（情報員が潜入）

「今日のように様々な情報通信技術の発達前のものであり、今日では、インターネット等の利用によるデーターの収集、N システム、GPS による位置情報の把握など、ここに挙げられたもの以外の多様な情報入手の手段が組み合わされて、対象とされた団体や個人の情報が対象者本人気づかれない方法で系統的に収集されているものと思われる。」（控訴審第 3 準備書面）

（4）攻撃－侵入・無害化措置

＊対象国の通信事業者の設備を無断で利用して、サイバー攻撃に関与していると疑う通信を分析し、必要な場合、取得する措置をとる（32 条）。

要件）送信元、疑うにたりる特定の機械的情報（外国の政府または国際機関、関係行政機関そのほかの関係機関から自動選別以外の方法で取得した情報であって機械的情報に相当するものを含む）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、この項の措置以外の方法では分析が著しく困難である場合において、必要と認めるときは、基準を定めて、サイバー通信情報監理委員会の承認を受けて、国外関係通信媒介中通信情報が複製され、受信用設備に送信するようにするための措置＝複製を送らせること？

「勝手に盗み見てよい」という措置を許す規定。

＊無害化措置

整備法 6 条の 2

警察庁長官→指名　サイバー危害防止措置執行官（警察庁又は都道府県警察の警察官のうちから、次項の規定による処置を適正にとるために必要な知識及び能力を有すると認められる警察官）

2 項　「情報技術利用不正行為」又はその疑いがある電磁的記録（「加害関係電磁的記録」という。）を認めた場合で、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、通信の送信元若しくは送信先である電子計算機又は加害関係電磁的記録が記録された電子計算機の管理者その他関係者に対し、加害関係電磁的記録の消去その他の危害防止のため通常必要と認められる措置とることを命じ、又は自らその措置をとることができる。

加害関係電子計算機が国外にある場合－処置は、警察庁の警察官であるサイバー危害防止措置執行官に限りできる。あらかじめ、警察庁長官を通じて、外務大臣に協議しなければならない。

3 項 サイバー危害防止措置執行官は、2 項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。

但し、機能に重大な障害を生じさせ、又は生じさせるおそれのある加害関係電気通信が現に送信されている場合その他の当該危害防止のためには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は、この限りでない。－事後承認でも可

－相手国の主権侵害－サイバー攻撃　かつて日本でも武力行使と同様に反撃可能と国会答弁されていたように、武力による反撃を招く危険性がある行為

それを形骸化必至の第三者機関の承認（事後承認可）で警察や自衛隊に実施させることの危険性

（5）実施機関－警察・自衛隊

平時　警察、有事　自衛隊

シームレス（切れ目無し）

警察に対する法的統制の脆弱性

白藤（専修大学教授）の指摘－国家公安委員会による警察の監督という警察の統制制度を全く無視した構造　警察法にかろうじて残っていた自治体警察、警察の民主化の構造の破壊？

国家警察の復活を狙っている可能性？

（6）令状なし、第三者機関による承認　サイバー通信情報監理委員会　専門職員

事後承認でも可　歯止めとなるのか？＝形骸化必至ではないのか？

重大な結果を招く危険性

権力分立がなく、**法的統制**が**脆弱**で**司法**による**事後的統制**も利かない**日本**での**権力**に**権限**を**認める法案**だということの**認識**が**重要**

きわめて**重大な影響**を**及ぼす法律**を**国民的議論**も**国会**での**十分な審議**もなく**通**そうという狙い。→**早急な反対運動**の**構築**が**必要**

以上