能動的サイバー防御法案の狙いと危険性

弁護士　中谷雄二

目次

1　能動的サイバー防御法案の提出理由

- 近年、国内外において国家の関与が疑われるサイバー攻撃その他のサイバー攻撃の脅威が増大していることに鑑み（①）、サイバー安全保障態勢の整備の推進に関し、基本理念を定め、国の責務等を明らかにし、及びサイバー安全保障態勢の整備の推進に関する施策の基本となる事項を定めるとともに、サイバー安全保障態勢整備推進本部を設置することにより、サイバー安全保障態勢の整備を総合的かつ集中的に推進する必要がある（②）。これが、この法律案を提出する理由である。（衆議院●サイバー安全保障を確保するための能動的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提案理由）

2　日本のサイバー攻撃の現状

①攻撃量グラフ：出典は、NITCTER（国立研究開発法バー攻撃関連通信の被害人情報通信研究機構）のダークネット観測の「年間総観測パケット数の統計」

→　ダークネットへの通信量全体をサイバー攻撃の量と誤解させている可能性

（小倉利丸「サイバースパイ・サイバー攻撃法案批判」16-17頁）

サイバー攻撃の変遷

2

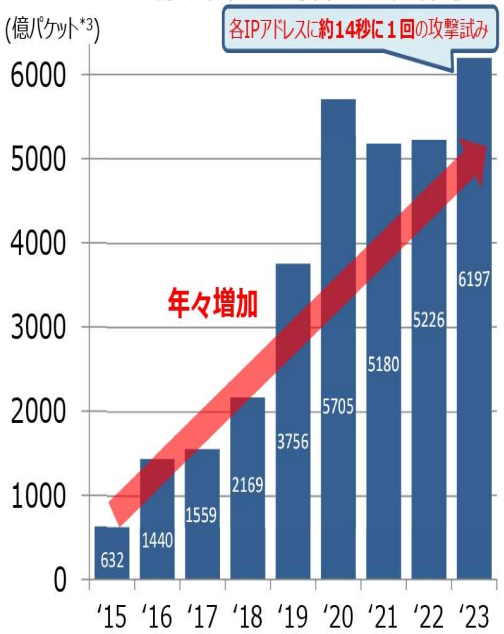
■ サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、**質・量両面でサイバー攻撃の脅威は増大**している。

■ 令和5年中に観測された**サイバー関連攻撃の通信の99%以上が海外から発信**[*1]

*1出典:警察庁資料。令和５年中に警察庁が観測したサイバー攻撃関連の通信（ダークネット向けの攻撃通信を含むパケット）の99.4%が海外のIPアドレスを発信元とするもの。

サイバー攻撃関連通信や被害の量

NICT [*2]が観測したサイバー攻撃関連通信数の推移



*2 国立研究開発法人 情報通信研究機構（National Institute of Information and Communications Technology）の略。

*3 １度に届くデータの塊のこと。センサーがデータを受信した回数と同義。

サイバー攻撃の巧妙化・深刻化

サイバー安全保障に関わる攻撃例

IT系システムの侵害
(暗号化・システム障害、身代金要求)
（例：2021年米コロニアルパイプライン業務停止、2022年大阪急性期・総合医療センターの業務停止、2023年名古屋港業務停止）

＋

有事に備えた重要インフラ等への侵入
(高度な侵入・潜伏能力)
（例：2014年クリミア併合、2022年ウクライナ侵略、2023年VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害）

＋

機微情報の窃取
(アクセス権限の獲得)
（例：2021~24年JAXAへの侵害、2023年NISCのメール窃取）

令和７年２月
内閣官房
サイバー安全保障体制整備準備室

実際の被害件数と原因推計（小倉）

サイバー攻撃の公表件数の年別推移との比較

サイバー攻撃被害の量

日本ネットワークセキュティ協会公表
サイバー攻撃数

2017年	1559億パケット	82件
2018年	2169億	94件
2019年	3756億	166件
2020年	5705億	268件
2021年	5180億	328件
2022年	5226億	
2023年	6197億	

IPA(独立行政法人情報処理推進機構)
コンピュータウイルス届出　2024年
・ウイルス感染　260件　感染被害15件
・不正アクセス　166件　実被害　132件

＊小倉前掲書15P～18P

3
サイバー攻撃被害の原因

IPAの原因別データ

小倉前掲書19頁

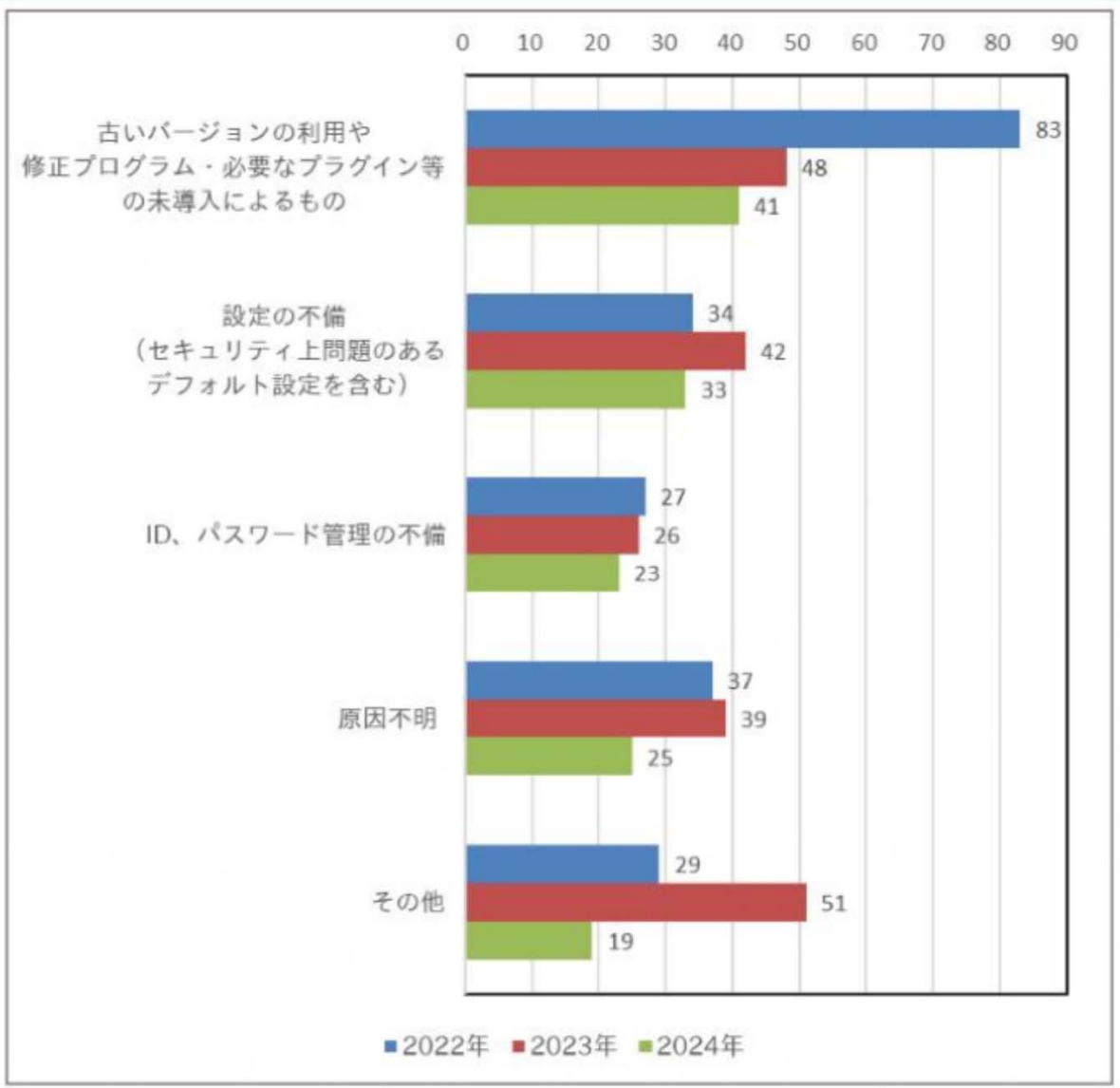


図 2-7：不正アクセス原因別件数の推移（2022～2024 年）

4　法案提出理由の検証

- １　誤解を招くサイバー被害の数
- 「脅威の増大」？
- ２　サイバー攻撃　被害の原因
- サイバー安全対策の整備の必要性に疑問
- 原因の多くは、適切なセキュリティ対策の欠如
- 例：システムのバージョンアップ
- 修正プログラムの適用
- セキュリティの設定ミス
- ＊パスワード設定の基本を守るなどによって防げるケースが
- 多い
- インシデント（アクシデントになる直前の状態）の多くが、組織内の人的なミスなどが原因。警察や自衛隊などの助けを借りずにセキュリティ対策をとりうるものが大半。

5　国連・諸外国の評価

- 1　ITU（国際電気通信連合）の国別評価
- ２０２４年　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」

- **２　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）
- **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）
- **「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

6　法案提出までの経緯

- 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
- 2015年　中谷元防衛大臣　抑止力　集団的自衛権　防衛体制を対応
- 可能とする（4月23日参議院外交防衛委員会）
- 2015年4月27日　日米ガイドライン
- 日米両政府は、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、
- 民間との情報共有…重要インフラ及びサービスを防護するために協力する。
- 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、
- …中略…米国は日本に対し適切な支援を行う。

- 2022．4．1　日米共同声明
- 2024．11．29 有識者会議提言
- 12．21　整備・推進法案（国民民主による議員立法）

- 国家安全保障戦略（令和4年12月16日閣議決定）では、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の目標を掲げ、①***官民連携の強化***、②***通信情報の利用***、③***攻撃者のサーバ等への侵入・無害化***、④***NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置***等の実現に向け検討を進めるとされた。
- 国家安全保障戦略に掲げられたこれら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、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開催（令和6年6月7日～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」を取りまとめ。

→ ***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（新法）***
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（整備法）

概　要

P7 官　民　連　携（新法）

- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告（第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

〔その他、雑則（第11章）、罰則（第12章）〕

P10 通信情報の利用（新法）

- 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（第３章）
- （同意によらない）通信情報の取得（第４章 第６章）
- 自動的な方法による機械的情報の選別の実施（第５章、第７章）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の厳格な取扱い（第23条）
- 独立機関による事前審査・継続的検査 等（第10章）

P14
- 分析情報・脆弱性情報の提供等（第８章）

P16 アクセス・無害化措置（整備法）

- 重大な危害を防止するための警察による無害化措置
- 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）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

P19 組織・体制整備等（整備法）

- 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改正）
- 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改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日 P22 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　等

7-12　情報取２つの方法①

- １　官民連携
- 罰則付の報告義務（①コンピュータ導入時、②サイバー攻撃を受けた場合）
- 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－
- 「連携」というが、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
- 　セキュリティホールの情報提供の危険性

2　通信情報の利用

①基幹インフラ事業者等との協定（同意）　12条、15条

同意は事業者の同意。事業者がプロバイダーの場合、利用者の同意なしに、個人情報提供の可能性（但し、プロバイダーとの契約時に承諾によって得たとされる危険性＝約款に「法令により情報提供が義務づけられている場合」という条項が入っている時、同意したとされる危険性）

②(同意によらない）通信情報の取得　不正行為に用いられる疑いがある場合

ⅰ　外外通信　国内設備→国外設備（送信元→送信先）

ⅱ　特定外内通信　国外設備→国内設備

ⅲ　特定内外通信　国内設備→国外設備

＊国外の大手多国籍企業（Gmail）のサービスを利用した場合や国外のVPNサービスを利用したとき外内通信に該当する可能性（全ての情報が国に取得される）

7-3 取得後の情報の扱い

- ③自動的な方法による機械的情報の選別の実施
- 機械的情報選別－脅威の判定に本文が必要では？
- ④関係行政機関の分析への協力
- **防衛大臣その他の関係行政機関の長に要請できる（27条）**
- ⑤取得した通信情報の厳格な取扱
- 不要な取得情報の抹消（22条・35条　内閣総理大臣）
- 検証なし　cf:DNAデータの扱い（資料、データ抹消）参照　6-4
- 膨大な不要なデータが保管されている。

- ⑥独立機関による事前審査・継続的検査　等
- **サイバー通信情報監理委員会（4～5人）**

参考資料

DNA型データベースの運用状況

（警察庁）

DNA型データベースの運用状況

資料1

	平成17年	平成18年	略	令和2年	令和3年	令和4年	令和4年末（総数）
登録件数（年間）	3,887	7,495		150,860	150,957	145,129	1,691,041
被疑者ＤＮＡ型記録	2,132	3,718		141,122	142,100	136,818	1,648,443
遺留ＤＮＡ型記録	1,755	3,777		7,194	6,887	7,133	27,146
変死者等ＤＮＡ型記録	－	－		468	431	393	6,088
死体ＤＮＡ型記録	－	－		112	78	97	1,377
特異行方不明者等ＤＮＡ型記録	－	－		1,964	1,461	688	7,987

	平成17年	平成18年	略	令和2年	令和3年	令和4年	令和4年末（総数）
抹消件数（年間）	65	648		14,325	12,069	14,315	215,806
被疑者ＤＮＡ型記録	0	27		2,581	2,825	3,403	92,942
（うち死亡したとき）	－	－		2,303	2,684	3,260	
（うち保管する必要がなくなったとき）	－	－		278	141	143	
遺留ＤＮＡ型記録	65	621		10,161	7,798	10,483	118,342
変死者等ＤＮＡ型記録	－	－		98	98	93	753
死体ＤＮＡ型記録	－	－		26	23	16	156
特異行方不明者等ＤＮＡ型記録	－	－		1,459	1,325	320	3,613

7－4　アクセス・無害化措置

- 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）6条の2
- 警察庁長官→サイバー危害防止措置執行官として指名された警察官
- 重大な危害が発生するおそれ　緊急の必要
- i　攻撃関係サーバ等の管理者等への措置の命令
- ii　攻撃関係サーバ等への措置（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）を自ら実施できる
- ＊海外サーバーの場合－外務大臣との協議→独立機関の承認→警察庁長官の指揮
- 原則　事前承認・特段の事由（事後通知で可）

7―5　アクセス・無害化措置②

- ③内閣総理大臣が、
- ⅰ　一定の重要な電子計算機に対するサイバー攻撃であり、
- ⅱ　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、
- ⅲ　自衛隊が対処する特別の必要があるとき
- 通信防護措置を命じた上で（第８１条の３第１項）、自衛隊の部隊等が警察と共同で措置を実施＝内閣総理大臣命令　自衛隊の通信防護
- 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）
- 内閣官房（新組織）が、国家安全保障局（ＮＳＳ）と連携しつつ、司令塔機能を発揮。警察と防衛省・自衛隊は、措置の実施主体として、内閣官房の調整の下 緊密に連携。米軍に対する攻撃についても、自衛隊が無害化措置を実施→集団的自衛権の行使にも

8-1　法案の問題点1

- １　　法案の提出　手法の問題
- 国民民主が昨年12月　整備推進法案の提出
- 政府との合意で、議員提案として提出した？
- 束ね法案（複数の法案を一括して上程）

8-2

法案の内容上の問題点

- 2　通信の秘密、プライバシーの権利の侵害
- ＊何が監視されるのか？－監視の対象（全情報が監視される危険性）
- ＊①DNAデータの扱い「内容は必要ない」というのは歯止めになるのか？

- ②大垣警察市民監視事件　法的根拠無く、市民の動静から思想、人間関係の監視まで。

3　監視手法の進化による監視国家化の深刻化

従前の監視→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

新たな手法→インターネット等の利用、Ｎシステム、ＧＰＳによる位置情報の把握、能動的サイバー防御法に基づくサイバースパイ活動の合法化

従前の秘密裏の市民監視は、辞めるのか？
警察法２条１項
「公共の安全と秩序の維持」目的の市民監視は継続し、それに新たな手法が加わる。

＊法律によるルールの無い監視行為については、野放し

8-3　法案の問題点-戦争への道を開く

- 4　侵入・無害化＝攻撃の違法性と危険性
- 　アクセス→侵入
- 　無害化→攻撃・破壊
- 　現行法における不正アクセス禁止法違反行為の合法化
- 　相手国が主権侵害・武力攻撃に匹敵する
- 攻撃と捉えた時は、反撃を受け、戦争になる。→重大な事態を招く恐れがあるのに、
- 　　第三者委員会の承認だけで良いのか？
- 　憲法9条違反では？

8-4　実施機関の問題

- 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）
- －大垣警察市民監視事件、**DNA**等抹消事件
- 警察に対する法的統制の脆弱性の一層の拡大
- ＊安保法制違憲訴訟　具体的な権利侵害がないから棄却
- 自分個人のプライバシー侵害が立証できれば、訴えられるが、日本を武力攻撃の危険にさらす行為については、国民は知ることもできず、いきなり危険になる。訴訟上の救済も求められない。
- 警察と自衛隊が守るのは、重要なインフラ・国の機関のみ
- 個人を守る意思も能力もない

8-5　手続き上の問題

- 6　裁判所による令状の必要なし、第三者機関による承認だけ
- 事後通知でも可、承認は形骸化必至
- 重大な結果を招く危険性
- 民主的手続きなしー国家公安委員会の関与は極めて限定的
- 令状を要求しても、形骸化している状況。
- 審査可能か？ー政府に忖度し、逆らえない裁判官
- 予想される、裁判所の令状を要するという修正ではダメ

9法案の狙い

- **1　法案の提出の経緯から軍事的な要請**
- **サイバー攻撃の危険性察知→能動的サイバー攻撃（先制的サイバー攻撃）＝侵入・無害化→反撃→エスカレート→武力紛争→集団的自衛権行使**として、米国と一体化した戦争に参加の恐れ

- **2　通信の秘密・プライバシー侵害の危険性→監視国家化**
- **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

10　最後に

能動的サイバー防御法案の廃案を目指した大運動の展開を！