警察政策学会資料　第150号
令和８（２０２６）年８月

国家諜報長官 DNI の権限
サイバー対処能力強化法及び同整備法の評価と課題
大川原化工機国賠事件・控訴審判決と
警視庁の検証報告書を読む

警察政策学会

テロ・安保問題研究部会

＜目次＞

令和８年８月

テロ・安保問題研究部会　部会長
茂田インテリジェンス研究室主宰
茂田　忠良

国家諜報長官 DNI の権限

茂田　忠良

＜目次＞

はじめに

最近、我が国では政府のインテリジェンス能力の強化に向けた動きがあり、その一環で国家情報局を設置する法律が制定された[1]。そこで、本稿では、その国家情報局長と対比されるべき米国の国家諜報長官 DNI の権限について論述したい。DNI は、諜報コミュニティの長 Head であり、且つ、国家安全保障に関するインテリジェンスについて、大統領と国家安全保障会議及び国土安全保障会議に対する首席アドバイザーであり、国家諜報計画の実施と予算執行を監督し指揮する責務を有する[2]。そして、その責務を果たすために法令によって広汎且つ詳細な権限を付与されている。

本稿では、先ず DNI 権限の法源と「国家インテリジェンス」の定義を説明した上で、根拠法令に基づいて DNI の主な権限を列挙して解説を加える。

なお、本稿では、Intelligence は「諜報」、Information は「情報」と訳して、両者を区別している。

[1] 国家情報会議と国家情報局を設置する国家情報会議設置法が、2026 年 5 月 27 日に国会で可決成立した。

[2] EO12333 Part1.3 及び合衆国法典 50 篇 3023 条（b）項など。

１　DNI 権限の主たる法源

国家諜報長官（Director of the National Intelligence：DNI）の権限に関する主たる法源は、1947 年制定の国家安全保障法（National Security Act）と 1984 年制定の大統領命令第 12333 号（EO12333）「合衆国諜報活動（United States Intelligence Activities）」である。国家安全保障法は、連邦議会が制定したインテリジェンスに関する基本法である。これに対して、大統領命令は、連邦議会が制定した法律の委任に基づくものではなく、合衆国憲法第 2 章が定める大統領の行政権に根拠を置くものであり行政各部を拘束する[3]。EO12333 はインテリジェンス活動についての基本的行政命令であり、諜報コミュニティにとっての憲法とも呼ばれている。

ところで、国家諜報長官 DNI を創設したのは、2004 年諜報改革・テロ防止法 IRTPA（国家安全保障法の改正法）である。本法は DNI を創設すると共に、諜報コミュニティ運営に必要な多くの権限を DNI に付与した。この法改正に伴い、大統領命令 EO12333 も同年 EO13355 によって改正されたが、その際の改正は必要最小限の暫定的なものに留まり、DNI の実質的な権限はそれ程強化されなかった。その後 2008 年に至って、大統領命令 EO12333 が EO13470 により大改正され、2004 年改正法の多くの権限規定を取り込むと共に新規の権限規定も追加された。DNI の権限が大統領命令の形で行政府内でも制度化され、実質的に大幅に強化されたのである。ここに至って、DNI 創設の趣旨が名実ともに実現したと言えよう[4]。

国家安全保障法と EO12333 はその後も改正されてきたが、特に国家安全保障法はしばしば改正され、その度に DNI に新しい権限が付与され、DNI の地位は強化されている。これらの改正によって、DNI は 2004 年創設当初の諜報コミュニティの調整者から、現在は諜報コミュニティ最高経営責任者（CEO）になったと言えるであろう。

２　「国家インテリジェンス」の定義

DNI は「国家インテリジェンス」の長官 Director であり、主として「国家インテリジェンス」について権限を行使しているのであるから、先ず、この用語の定義を確認しておこう。

3　大統領命令は、連邦議会の制定する法律を変更することはできず、また、法律に基づかない大統領命令は私人に対しては拘束力はないと理解されている。

4 DNI 権限論について体系的に論じた先行研究を調査すると、最重要論文として次の論文が挙げられる。小林良樹「米国インテリジェンス・コミュニティの改編―国家情報長官（DNI）制度の創設とその効果」（『国際政治』第 158 号、日本国際政治学会、2009 年、158–182 頁）。本論文は DNI 創設初期の制度的背景を整理した点では貴重であるが、2008 年 8 月の EO12333 改正（EO13470）による DNI の権限強化を分析対象に含めていない。また、NSA、NGA、NRO、DIA など国防総省傘下のインテリジェンス機関の予算を「軍諜報計画」予算に含まれるものと誤解して立論しているが、これら機関の予算の大部分を占める国家インテリジェンス任務は「国家諜報計画」予算に計上されており、DNI の予算編成権限の対象である。この「国家諜報計画」予算制度の根幹に関する誤解は、DNI の権限評価に重大な影響を与えている。従って、小林論文は 2008 年以降の DNI 権限論の基礎研究としては限定的な参考文献として位置付ける必要がある。

このほか、防衛研究所紀要を見ても、DNI の権限を主題として論じたものは見当たらなかった。

国家安全保障法 3 条（合衆国法典 50 篇 3003 条）には「国家インテリジェンス」の定義規定があり、大要次のように定義している。即ち、「国家インテリジェンス」及び「国家安全保障に関するインテリジェンス」とは、2 以上の政府機関（agency）の所掌に係わるインテリジェンスであって、米国の国家安全保障又は国土安全保障に係わるものをいう。要約すると、①2 以上の政府機関に係わる、②（国土安全保障を含む）国家安全保障に係わるインテリジェンスということになる。

更に、「国家インテリジェンス」は、諜報源の種類、収集場所の国内外を問わず、また、米国の国民・財産・利益に対する脅威、大量破壊兵器に係わるものを含むとしている。狭義の対外諜報にとどまらず、米国内におけるインテリジェンス活動や防諜活動（Counterintelligence）も含む概念であり、幅広い活動が含まれる[5]。

重要なのは、このような「国家インテリジェンス」（以下「国家諜報」）の定義は、インテリジェンスの「機能」に関する定義であって、インテリジェンス機関の所属とは関係がないことである。米国には 18 の諜報機関が存在するが、その内、国家諜報長官室や CIA が国家諜報を担当しているのは当然として、国防総省傘下の NSA、NGA、NRO、DIA、司法省傘下の FBI なども国家諜報を担当する主要機関である。そもそも、国家安全保障庁 NSA（National Security Agency）や国家地理空間諜報庁 NGA（National Geospatial-Intelligence Agency）そして国家偵察局 NRO（National Reconnaissance Office）の「N」はこれら諸機関が当初から国家諜報を主任務として発足したことを示しているのである[6]。また、国務省、エネルギー省、国家安全保障省、財務省の諜報組織も国家諜報を担当している。

他方、国家諜報の定義に含まれないものには、特定の 1 つの政府機関（agency）にしか係わりのないインテリジェンスや純粋に軍事作戦実施のためのインテリジェンスがある。NSA[7]、NGA や DIA は、国家諜報任務を負うが、同時に軍司令官の作戦支援など軍諜報任務も負っている。つまり、同一組織が国家諜報任務と軍諜報任務の両方の任務機能を有しているのである。

それでは、以下、国家安全保障法及び EO12333 の関連規定を基に、諜報コミュニティ運営のために DNI に付与された権限を見ていく。但し、法律や大統領命令で与えられた権限は広

---

5 「国家インテリジェンス」の定義は、2004 年インテリジェンス改革・テロ防止法 IRTPA で改正されて、概念が拡張された。防諜活動や米国内の活動、国土安全保障関連活動が含まれることが明確にされた。そもそも、2004 年改正法の出発点は、2001 年の 9.11 事件という米国内における大規模テロ事件であり、それを考えれば、概念の拡張は当然であろう。

6 歴代の防衛省情報本部長には、この点についての理解が不十分な方が散見される。例：外薗健一朗氏『官民軍インテリジェンス』（ワニブックス、2025 年）137-138 頁。また、同じく元情報本部長の太田文雄氏は「国防組織の情報機関の第一の顧客は、第一線の戦闘部隊」である旨を述べている（2026 年 1 月 26 日付「国基研ろんだん」2026 年 3 月 3 日閲覧。https://jinf.jp/feedback/archives/46544）。残念ながら、両者には本文記載の事実（米国では、国防省に属する諜報機関である NSA や NGA が、CIA と並んで「国家インテリジェンス」を担う主要機関であること）に対する理解不足が見られる。

7 NSA の組織名を厳密に記述すると NSA/CSS であり、その CSS（Central Security Service）部分が、軍諜報任務を負っている。

汎且つ詳細であり、全てに言及することは紙幅の関係上不可能なので、主要な権限について見ていくこととする。

３　情報アクセス権限

DNI が諜報コミュニティを運営していくためには、関係諜報機関の情報及びインテリジェンスにアクセスできることが重要である。

この点について、法 3024 条（b）項は、DNI が全ての「国家インテリジェンス」及び「国家安全保障に関連するインテリジェンス」に対してアクセス権を有すると規定している。

2008 年に改正された EO12333 は、より広く且つ強いアクセス権を定めている。即ち、DNI が、国家安全保障に関連する全てのインテリジェンスと情報、及び DNI の職務遂行上必要とされるその他全てのインテリジェンスと情報（管理運営に関する情報を含む）に対してアクセス権を有すると明記し（Part 1.3(a)）、また、関係省庁の長官に対して、これらの情報やインテリジェンスについて DNI にアクセスを提供する義務を課している（Part 1.5(a)）。つまり、DNI のアクセス権の対象がより広く（「国家インテリジェンス」以外の職務遂行上必要な情報を含む）、且つ、アクセス権に実効性を持たせるために、関係省庁の長官に対してアクセス提供の義務を明文化しているのである。

更に、EO12333 は、DNI による「国家諜報計画（NIP）」策定[8]を支援するために、関係省庁の長官に対して、DNI が必要とする全ての事業計画と予算に関する情報を提供することを義務付けている（Part 1.5(b)）。

DNI が、必要とする諜報コミュニティ内のあらゆるインテリジェンスと情報にアクセスできることは、諜報コミュニティ運営のために必要な基本中の基本であり、これを疑問の余地なく定めているのである。

４　人事権限

法 3041 条と EO12333 の Part 1.3(d)(e)は、DNI に諜報コミュニティを運営するための広汎な人事権を与えている。官僚組織において、権力の源泉は、人事と予算である。

人事権については、DNI は、各諜報機関のトップ人事について、選任に関して、同意し又は協議を受ける権限を持ち、また、罷免を勧告する権限も持っている。これらの権限が具体的にどのように行使されているか、詳細は不明であるが、官僚組織ではこれらの権限が存在すること自体が、大きな力となるのである。以下、法 3041 条と EO12333 が DNI に与えた人事権限について記述する。

---

[8] 「国家諜報計画（National Intelligence Program: NIP）」とは、国家諜報活動を指し、具体的には、国家安全保障や外交政策のために政治・経済・軍事などの幅広い情報を収集・分析し、大統領初め政府全体を支援するためのインテリジェンス活動である。これに対して、「軍諜報計画（Miliary Intelligence Program: MIP）」とは、軍司令官や軍事作戦を支援するためのインテリジェンス活動であり、国防総省が所管している。

（1）選任についての推薦対象　（法 3041 条(a)項）

次の職の選任に関しては、DNI は大統領に推薦するものとする。

○　国家諜報首席副長官

○　中央諜報庁（CIA）長官

（2）選任についての同意対象　（Part 1.3(d)、法 3041 条(b)項同旨）

次の職の選任に関しては、関係省・局の長官は DNI の同意を得るものとする。DNI が同意しない場合は、関係省・局の長官は、大統領に推薦してはならず、或いは任命してはならない。関係長官と DNI が合意に達しない場合は、直接大統領に事情を説明することができる。（任命権者は、②⑥⑧はそれぞれの長官、それ以外は大統領）。

①　国家安全保障庁（NSA）長官

②　国家偵察局（NRO）長官

③　国家地理空間諜報庁（NGA）長官

④　国土安全保障省 諜報・分析担当次官

⑤　国務省 諜報・調査（INR）担当次官補

⑥　エネルギー省 諜報・防諜担当次官補[9]

⑦　財務省 諜報・分析担当次官補

⑧　連邦捜査局（FBI）国家安全保障部門（NSB）担当次長補

（3）選任の際の協議対象　（Part 1.3(d)）

次の職の選任に関しては、関係省長官は推薦又は任命前に DNI と協議しなければならない。（実質的任命権者は全て大統領。但し、形式上、軍人の将官昇進は大統領、補職はそれぞれの長官。）

①　国防総省 諜報・保全担当次官（USD（I&S））[10]

②　国防諜報庁（DIA）長官

③　陸軍、海軍、空軍および海兵隊の諜報部門の制服組トップ

④　沿岸警備隊 諜報担当副司令官

⑤　司法省 国家安全保障担当次官補

（4）罷免の勧告権　（Part 1.3(e)）

○　DNI は、CIA 長官の罷免を大統領に勧告することができる。

○　上記（1）の職（②⑥⑧を除く）又は（2）②の職にある者の罷免又は罷免勧告について

---

[9] EO12333 には「エネルギー省 諜報・防諜局長」と記載されているが、組織改正があり名称が変更されたので、正式名称を記載した。

[10] 同じく、EO12333 には「国防総省諜報担当次官（USD（I））」と記載されているが、組織改正があり名称が変更されたので、正式名称を記載した。

は、DNI と関係省・局の長官とは協議するものとする。両者が合意に達しない場合は、それぞれが大統領に罷免を勧告することができる。

○　上記（1）②⑥⑧及び（2）①④の職にある者の罷免については、DNI と関係省・局の長官とは、協議するものとする。省の長官が罷免しない場合には、DNI はその旨を大統領に報告することができる。

○　DNI は、陸海空軍海兵隊の諜報部門トップ（（2）③）の罷免を国防長官に勧告することができる。

このように DNI は各諜報機関のトップの選任や罷免に関して大きな影響力を持っており、これが、諜報コミュニティ運営に当たっての梃となっている。

（5）人員の異動・配置転換権限

大統領命令 EO12333 で認められた人事権限の他に、2004 年改正法によって DNI に認められた人員の異動・配置転換の権限がある（法 3024 条（e）項）。この権限によって、諜報コミュニティにおける柔軟な定数管理が可能となっている。即ち、以下のように予算年度途中でも、国家諜報長官室に新しいセンターを開設したり、インテリジェンス機関の間で配置転換をしたりできる。米国のプラグマティズム、実用主義の顕れである。我が国の「静的な」定数管理制度とは大きく異なる思想である。

○　DNI は、国家諜報を実施する新しいセンターを開設した場合、開設後 1 年間、諜報コミュニティから 100 人以下の人員を異動させることができる。この場合、予算管理局長の同意を得て且つ連邦議会の関連委員会と協議の上、行う必要がある。（同項（1）号）

○　DNI は、緊急の必要や効率を高める必要がある場合は、諜報コミュニティ内で同種の業務を担当する人員の配置転換をすることができる。この場合、予算管理局長の同意を得て且つ関係省庁と定めた手続に従って行い、事後迅速に連邦議会の関連委員会に通知する必要がある。（同項（2）号）

○　DNI は、一定の必要がある場合には、国家諜報長官室の勤務員定数を 100 人増員することができる。（同項（3）号）

○　更に同項（4）号は、連邦議会は「国家安全保障上の脅威は、諜報コミュニティが予期せぬ事象に対して迅速且つ柔軟に対応する必要があり、大統領は、DNI 他の諜報コミュニティが迅速かつ効率的に対応するため、その裁量権を働かせるべきである」と認識している旨を宣言して、諜報コミュニティの臨機応変の対応を推奨している。我が国の法律では考えられない規定である。

５　予算の編成と執行権限

次に、官僚組織において、もう一つの権力の源泉である予算に関する権限を見てみよう。

即ち、DNI は、「国家諜報計画（NIP）」の策定と執行に責任を負っている。2025 会計年度

（2024 年 10 月～2025 年 9 月）の NIP 予算額は 733 億ドル、日本円にして約 11 兆円という予算を統括しており、その権限は巨大である。NIP 予算の執行機関は、国家諜報長官室、CIA、NSA、NGA、NRO、DIA、FBI などの主要インテリジェンス機関のほか、国務省、エネルギー省、国家安全保障省、財務省に及ぶ。また、金額は少ないものの各軍諜報部門でも執行しており、NIP 予算の執行は諜報コミュニティ全 18 機関に及んでいる。

また、DNI は、「軍諜報計画（MIP）」の予算策定にも参加している。MIP 予算は、軍事作戦遂行のための予算であり、国防長官の所管であるが、国家諜報も軍諜報も相互に関連しているために、DNI の参加が定められている。2025 年度の MIP 予算額は 278 億ドル（4 兆円超）である。

DNI の予算に関する権限については、法 3024 条（c）（d）項が詳細に規定しているので、同項の骨子を次に紹介する。

（1）「国家諜報計画 NIP」予算編成権限 （（c）項（1）（2）号）

NIP 予算編成では、DNI は、インテリジェンス関係省庁に予算策定の指針を発し、関係省庁からの予算提案に基づいて、年度統合予算案を策定決定して大統領に提出しなければならない。関係省庁は、DNI が予算案編成に必要な情報を提供しなければならない。

（2）「軍諜報計画 MIP」予算への関与権限 （（c）項（3）号）

DNI は、国防長官による軍諜報計画（MIP）の年度予算案の策定に参加する。また、DNI は、国家諜報計画（NIP）に含まれないインテリジェンスの年度予算の策定について指針を発する。

（3）NIP 予算執行監督権限 （（c）項（5）号）

DNI は、関係省庁の長に対して、NIP 予算の割当てと配分を指示し、その実施と執行を監督するなど、同予算の執行に責任を負う。

（4）NIP 予算の振替権限 （（d）項）

DNI は、一定の要件下に NIP 予算の費目振替や使途変更を行うことができる。一定の要件とは、関係諜報機関が所属する省の長官と協議後に、一定金額の範囲内（各省庁の NIP 予算の 5%以下且つ 1 億 5 千万ドル以下）で振替や使途変更をすることである。省の長官が同意した場合には、上記金額の制限を超えて振替や使途変更ができる。

また、国防長官は、MIP 予算の振替や使途変更を行う場合は、DNI と協議しなければならない。

上記のように、DNI は、NIP 予算の編成と執行に関する権限のみならず、MIP 予算に対しても一定の権限を保持している。それは、国家諜報と軍諜報と区分しても、その実務におけ

る境界は必ずしも明確ではなく、また、先述したように、NSA、NGA、NRO、DIA など国防総省傘下の諜報機関は、国家諜報も軍諜報も共に所掌しており、NIP 予算と MIP 予算の整合性を図る必要があるからである。

なお、DNI の法律上の予算権限は強力であるが、現実にその権限を有効に行使できるか否かは、別問題である。過去には国防総省傘下の機関である NSA、NGA、NRO、DIA などの NIP 予算を DNI が統制するには困難があったとされる。しかし 2010 年頃からは、国防総省関係の NIP 予算と MIP 予算の策定では、共同の予算策定指針を発するなど国家諜報長官室と国防省が協力して行うようになり[11]、DNI と国防総省の協力関係が円滑になってきたようである。また、予算策定において DNI の武器となったのが、後述する「国家諜報優先順位枠組」（国家の情報関心を事項別、国別に区分して 5 段階で示した機密文書）である。即ち、この枠組に照らして、各諜報機関の予算案の適否を検討することが可能となり、DNI の予算権限が行使し易くなったと言われる。

６　優先順位設定・任務付与の権限

DNI が諜報コミュニティを統合して運営していくには、コミュニティ構成機関に対して、インテリジェンス活動の目標・優先順位・指針を設定すると共に、具体的な情報収集の任務付与にも権限を及ぼす必要がある。

DNI の優先順位設定や任務付与の権限は、2004 年改正法によって DNI 創設時に規定されたが、2008 年の EO12333 改正により更に強化された（Part1.3（b）(1)(17)(18)など）。この強化規定はその後の法改正で国家安全保障法にも取り込まれた。法律も EO12333 もほぼ同文であるので、ここでは法 3024 条（f）項を基に、DNI の広義の任務付与権限を見てみよう。

① DNI は、国家インテリジェンスの適時且つ効果的な収集・処理・分析・配布を確保するため、諜報コミュニティのために目標・優先順位・指針を設定する。（法同条（f）項（1）号（A））（EO Part1.3（b)(1)同旨）

② DNI は、国家インテリジェンスの収集・分析・作成・配布についての、要求と優先順位を決定し、(収集アセットに対する)任務付与を管理指揮する。(法、同上)（EO Part1.3（b)(17)同旨）

③ DNI は、諜報コミュニティ内の、収集要求及び国家収集アセットに対する任務付与を巡る対立を解決する。（法、同上：2010 年追加）（EO 同上）

④ 国家諜報計画外のインテリジェンス活動について、助言的（収集アセットに対する）任

[11] Congressional Research Service, *Defense Primer: Budgeting for National and Defense Intelligence*, In Focus IF10524 (Washington, DC: CRS, January 6, 2025), https://www.congress.gov/crs-products/product/pdf/IF/IF10524.
—Congressional Research Service, *Intelligence Planning, Programming, Budgeting, and Evaluation (IPPBE) Process*, In Focus IF10428 (Washington, DC: CRS, March 13, 2023), https://www.congress.gov/crs-products/product/pdf/IF/IF10428

務付与を提供する。（法、同上：2014 年追加）（EO Part1.3（b)(18)）
＜上記に対する例外＞
○　大統領の指示は上記に優越する（法同条（f）項（1）号（B））。
○　国防長官と DNI が合意した計画に基づいて国防長官が任務付与をする場合（同上）。

本条は、インテリジェンス活動の目標や優先順位の設定、収集アセットに対する任務付与権限についての基本規定であり、DNI に強力な権限を与えている。しかし、これは個別の収集アセットに対する個別の任務付与に至るまで、DNI が管理していることを意味しない。そもそも、NSA にしろ、NGA にしろ、CIA にしろ、何れも巨大な諜報機関であり、それぞれ膨大な収集アセットを保持している。その個別の収集アセットに対する個別の任務付与にまで DNI が関与するのは、効率的でもなければ望ましくもない。現実に行われているのは、「国家諜報優先順位枠組」による管理である。即ち、DNI は、本条と大統領命令 12333 号（米国諜報活動）に基づき、「国家諜報優先順位枠組」（National Intelligence Priority Framework：NIPF）を定めているが、これは情報関心を事項別、国別に区分して優先順位を 5 段階で示したものである。DNI は、この NIPF 枠組に基づき、各インテリジェンス機関の優先順位の設定と任務付与が適切になされているかを、管理している。この NIPF 枠組によって、米国諜報コニュニティ全体の諜報活動が適切な方向を指向しているか管理できるのである。

但し、これには例外があり、最も重要なのは大統領の意向である。つまり、大統領の情報需要が最優先されるのである。筆者は嘗て米国某インテリジェンス機関から収集アセットに対する任務付与（tasking）の手順についてブリーフィングを受けたことがある。一般的には収集アセットに対する任務付与は、NIPF 枠組に基づき且つインテリジェンス顧客諸組織からの要求を積み上げて構築していくのであるが、大統領は例外で、大統領が知りたいと言えば、「他に如何に重要な収集目標があろうとも、大統領の情報関心が最優先される」そうである。法 3024 条（f）項（1）号（B）は正にその根拠条文である。

７　インテリジェンス配布に関する権限

DNI は、インテリジェンス情報の配布に対しても、指針を定める権限を持っている。それは前章 6 で示した①②の規定に基づくほか、EO12333 には次の規定（Part1.3（b)(9)）がある。
○　DNI は、関係省庁の長と協議の上、諜報コミュニティのため、全てのインテリジェンス及びインテリジェンス関連情報（最終形態のみならず初期収集形態を含む。）へのアクセス及び配布に関する指針を策定する（要旨）。

８　その他の権限

DNI が諜報コミュニティを統合して運営していくために、上記の他にも様々な権限が法律及び EO12333 に規定されている。その内、興味深いものを以下に列挙する。如何に DNI の

権限が確固としたものか、理解できるであろう。なお、法律と大統領命令の両者に類似の規定がある場合は、法律の規定を紹介し、大統領命令のみに規定がある場合は、その規定を紹介する。

（1）国家インテリジェンス・センターの設置と監督（法 3024 条（f）項（2）号）

DNI は、国家テロ対策センターNCTC、国家拡散対策センターNCPC、国家防諜・保全センターNCSC その他の国家インテリジェンス・センターを監督する。

DNI は、個別の諜報機関の所掌を超える諜報コミュニティ共通の課題についてインテリジェンス・センターを運営することによって、諜報コミュニティ諸機関に横櫛を通すことができるのである。なお、DNI のスタッフやこれらセンター勤務者には、給与面でのインセンティブを提供することも規定されている。（(l）項（1）号）

（2）人事政策や人事計画の策定（(f）項（3）号）

DNI は、諜報コミュティに対して拘束力ある人事政策や人事計画を策定する。それには、国家インテリジェンス・センターや他機関での勤務経験を要求或いは推奨すること、教育訓練・キャリア開発の基準を定めること、特定の職務には複数の諜報機関での勤務歴を条件とすること等が含まれる。

（3）責任検証調査（(f）項（7）号）

DNI は、諜報コミュニティ内における失敗や欠陥について、責任検証調査（accountability review）を行い、関連機関の長に対して免職を含む必要な矯正・懲罰処分を勧告する。

（4）内部脅威対策の推進（(f）項（8）（9）号）

DNI は、諜報コミュニティ内における内部脅威対策の基準を定め、防諜、保全、内部脅威対策の有効性を評価するなどして、内部脅威対策を推進する。秘密漏洩が発生した場合は、当該職員のセキュリティ・クリアランスのための背景調査や審査経緯を検証する。

（5）インテリジェンス情報の共有の推進（(g）項（1）号）

DNI は、諜報コミュニティ内において、秘密保全に配慮しつつ、インテリジェンス情報の利用可能性とアクセス性を最大限に確保する主たる責任者である。そこで、DNI は次の施策を行う。

- 秘密保全の統一基準と統一手順を定める。
- 諜報情報共有と諜報源保護という対立する２つ必要性を両立させる方針と手順を定める。
- インテリジェンス報告書の共有を推進するため、報告書フォーマットの標準化の指針を定める。

このように、DNI は DNI 自身のインテリジェンス情報へのアクセス権限以上の責任と権限、諜報コミュニティにおける情報共有を推進する責任と権限を持っているのである。

（6）IT アーキテクチャに関する権限（（g）項（1）号）

また同号は、情報共有の視点から、情報システムに関する DNI の権限も規定している。

・ IT の共通の基準や手順とインターフェースを定める。

・ 諜報コミュニティの IT アーキテクチャを開発する。

・ 国家諜報計画 NIP 予算から支出する IT アーキテクチャ全てについて執行承認権を有する。

（7）秘密情報に関する統一手順を定める権限（（j）項（1）号）

DNI は、機微区画情報（Sensitive Compartmented Information: SCI）へのアクセス許可に関する統一基準と手続を定めるほか、セキュリティ・クリアランスのための背景調査や審査が可能な限り速やかに実施されるようにする。

インテリジェンス情報の内、重要なものは、機微区画情報 SCI に指定されており、インテリジェンス機関員は職務上 SCI へのアクセス許可が必要である。DNI は諜報コミュニティにおけるセクキュリティ・クリアランス制度の管理者なのである。

（8）秘密工作の監督権（EO Part1.3(b)(3)）

DNI は、全ての進行中及び提案中の秘密工作（covert action）計画を監督し、秘密工作に関して大統領と国家安全保障会議に助言を提供する。

この規定の存在によって、DNI は諜報コミュニティ内のどの機関が実行するにせよ、機微な秘密工作の情報に必ずアクセスし監督することになる。これも DNI 権限を補強する規定である。

（9）外国諜報機関との渉外権限（EO Part1.3(b)(4)）

DNI は、外国政府や国際機関との諜報・防諜に関する取決や協定を締結し、政策を策定する。更に、諜報コミュニティ構成機関の諜報・防諜に関する対外関係の整合性と統合性を確保する。

この規定により、諜報コミュニティ構成機関と外国政府機関との関係について、DNI は常に監督する権限を有することとなる。これも重要な権限である。

９　DNI の規則制定権

DNI は、以上の各種権限を執行するために、諜報コミュニティ構成機関を拘束する規則を制定する権限を有している。規則制定権が、DNI 権限の行使においては、重要な手段となっているのである。

（1）ICD（Intelligence Community Directives：IC 指令）

DNI は、法 3024 条及び EO12333Part1.3 で与えられた権限を行使するために行政命令を発することができると理解されており（根拠条文は、法 3024 条(f)項(1)号(A)など）、ICD という名称の指令が多数発出されている。更に、ICD の下部規則として、ICPG（IC Policy Guidance：IC 政策指針）や ICPMs（IC Policy Memorandums：IC 政策覚書）がある。

ICD の幾つかを以下に例示する。ウェブサイトに開示されている ICD は 50 本以上に及ぶ[12]。DNI の規則制定権の広汎なことが理解できる。

○ ICD104「NIP 予算の策定・執行・成果評価」
○ ICD119「メディアとの接触」
○ ICD190「クリティック」（国家指導者に即時通報すべき重要情報通報システム）
○ ICD203「分析基準」
○ ICD204「国家諜報優先順位枠組」NIPF
○ ICD207「国家諜報会議」NIC
○ ICD209「ティアライン作成及び配布」（「サニタイズ」の主たる技法）
○ ICD404「行政府インテリジェンス顧客」（顧客との接触窓口など）
○ ICD405「諜報外交」（外国政府との諜報協力）
○ ICD503「IC 情報環境のリスク管理」
○ ICD700「国家諜報の保護」
○ ICD701「秘密情報の漏洩対策」
○ ICD703「機微区画情報を含む秘密情報の保護」
○ ICD704「人的保全基準及び機微区画情報へのアクセス適格性」
○ ICD710「秘密区分管理及び配布統制表示制度」
○ ICD750「防諜諸計画」

（2）SEADs（SecEA Directives：保全統括責任者指令）

DNI は、合衆国法典 50 篇 44 章（国家安全保障）の 3162a 条によって、連邦政府の保全統括責任者（Security Executive Agent: SecEA）に指定され、諜報コミュニティのみならず、政府全体の保全について責任と権限を有している。本業務に関する行政規則は SEAD と呼ばれている。一例を挙げると、セキュリティ・クリアランスの審査指針を定める SEAD4「国家安全保障審査指針」[13]などが発出されている。

---

[12] ODNI website, accessed 23 February 2026, https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

[13] ODNI website, accessed 23 February 2026, https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy

終りに

以上、米国国家諜報長官 DNI が、米国諜報コミュニティの長として、諜報コミュニティを一体的に運営していくために付与された主要な権限を見てきた。DNI の権限が、法律や大統領命令によって如何に広汎且つ詳細に規定されているか御理解いただけたであろうか。DNI は、このような広汎な権限を行使して米国の諜報コミュニティを運営しているのである。

（以上）

サイバー対処能力強化法及び同整備法の評価と課題

茂田　忠良

＜目次＞

2025 年 5 月「サイバー対処能力強化法案及び同整備法案」が国会で可決成立した。本法律は我が国のサイバー安全保障分野での対応能力向上を目的としたもので、その内容は①官民連携、②事業者の保有する通信情報の利用、③攻撃関係サーバー等へのアクセス・無害化措置、④内閣サイバー官の新設など組織・体制の整備の 4 点から構成されている。

本法律の背景には、2022 年 12 月に政府が閣議決定した「国家安全保障戦略」がある。同戦略は、サイバー空間に関して「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」こととし、そのため「能動的サイバー防御」を導入し、「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ー等への侵入・無害化ができるよう、政府に必要な権限が付与されるようにする」と記載していた。本法律は、本戦略実現の一環であり、一部報道では、「これで日本のサイバーセキュリティ対応が欧米水準になる」とする記事もあった。

しかし残念ながら、本法律制定によって我が国のサイバー対応能力が欧米水準に達するとは到底言えない。そこで、法律の骨子を紹介すると共に、本法律に対する評価と今後の課題を述べてみたい[1]。

１　本法律の骨子

法律は、「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」（通称「サイバー対処能力強化法」。以下「強化法」）と「強化法の施行に伴う関係法律の整備等に関する法律」（以下「整備法」）の二つ[2]からなる。また、これら法律の運用指針として 2025 年 12 月に、強化法については「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」（以下「基本方針」）が閣議決定され、整備法については「アクセス・無害化措置の運用に関する指針」（以下「運用指針」）が国家安全保障会議で決定されている。

法律の骨子は次の通りである。

（1）サイバー対処能力強化法

（ア）官民連携

基幹インフラ事業者[3]がサイバー攻撃を受けた場合等の政府への情報共有や、政府からの民間事業者等への情報共有、対処支援等の官民連携の取組を強化するとして、次の主な施策を定めている。

○　基幹インフラ事業者は、特定の重要電子計算機を導入した時は、製品名、製造者名等を所管大臣に届け出る（強化法第 2 章）。

○　基幹インフラ事業者は、不正アクセス行為などのインシデント情報等を、所管大臣と内閣総理大臣に報告する（強化法第 2 章）。

○　内閣総理大臣は、情報共有と対策のための協議会を設置し、基幹インフラ事業者や電子

---

[1] 本稿は、拙稿「『サイバー対処能力強化法』の全貌と課題」（『軍事研究』60 巻 8 号 92-105 頁）を基に、2025 年 12 月の閣議決定等を踏まえて、大幅に加筆修正をしたもの（分量 2 倍超）である。

[2] 内閣官房国家サイバー統括室、「サイバー安全保障に向けた取組」（2025 年 9 月）、2026 年 4 月 30 日最終閲覧。https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

[3] 基幹インフラ事業者（＝「特定社会基盤事業者」）とは、経済安全保障推進法第 50 条第 1 項に規定する事業者で、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航海運、航空、空港、電気通信、放送、郵便、金融、クレジットカード、港湾、医療の 16 業種である。

医療分野については、2021 年の徳島県つるぎ町立半田病院や 2022 年の大阪急性期・総合医療センターに対するランサムウェア攻撃など、外国からのサイバー攻撃によって被害が発生しており、2026 年 6 月に経済安全保障推進法が改正され、医療分野が追加された。

計算機等のベンダー等を構成員に加える（強化法第 9 章）。
○　内閣総理大臣や所管大臣は、電子計算機等の脆弱性を認知した時は、電子計算機等のベンダー等に対して情報を提供するなど対応を強化する（強化法第 8 章）。

（イ）事業者の保有する通信情報の利用

我が国に対するサイバー攻撃の実態を把握するため、通信情報を利用して、分析する。具体的には次の通り。
○　内閣総理大臣は、基幹インフラ事業者等との任意の協定に基づき、通信情報を取得し、このうち外国からの通信を分析して、当該事業者に分析結果を提供する（強化法第 3 章）。
○　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、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、サイバー通信情報監理委員会の承認を得て通信情報を取得する（強化法第 4 章）。＜外外通信情報の取得＞
○　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、サイバー通信情報監理委員会の承認を得て通信情報を取得する（強化法第 6 章）。＜外内・内外通信情報の取得＞
○　取得する通信情報は、（不正行為に関係がある）IP アドレスや（不正行為の実施に用いられる）指令情報などの機械的情報に限定される。機械的情報は人による知得を伴わない自動的方法によって選別され、それ以外の情報は消去される（強化法第 5 章、第 7 章）。

（ウ）サイバー通信情報監理委員会の設置

サイバー通信情報監理委員会を設置し、通信情報の取得や無害化措置（後述）についての審査・承認等を行う（強化法第 10 章）。

（2）整備法

（ア）攻撃者のサーバー等へのアクセス・無害化措置

サイバー攻撃による重大な危害を防止するための警察・自衛隊による措置を可能とし、その際の適正性を確保する手続を新設した。次の通り。
○　警察庁長官が指名する警察官は、情報技術利用不正行為（サイバー攻撃）に用いられる電気通信や電磁的記録を認めた場合に、「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」、「危害防止措置」（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・削除その他の措置）を、加害関係電子計算機の管理者等に対して執ることを命じ、又は自ら執ることができる。（警察官職務執行法第 6 条の 2 新設）。
○　この処置を執る場合には、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、加害電気通信が現に送信されている場合その他危害防止のために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、事後通知で可（同上）。
○　危害防止の処置の対象となる電子計算機が国外に設置されている可能性がある場合には、あらかじめ外務大臣との協議が必要（同上）。

○　内閣総理大臣は、攻撃が、国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場合において、（自衛隊が有する特別の技術又は情報が必要不可欠であるなど）自衛隊が対処を行う特別の必要があると認めるときは、「通信防護措置」を命ずることができる（自衛隊法第 81 条の 3 新設）。その際は、自衛隊の部隊は警察庁（又は都道府県警察）と共同して通信防護措置を実施する。その際の権限は、警察官職務執行法を準用する（同法第 91 条の 3 新設）。

○　自衛隊又は在日米軍の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、改正警職法の権限を準用する（同法 95 条の 4 新設）。

（イ）内閣サイバー官の新設など組織・体制の整備

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するとして、次の強化策が実施された。

○　サイバーセキュリティ戦略本部の改組強化：本部長を官房長官から総理大臣に格上げし、本部員を特定の大臣から全ての国務大臣に拡大する。更に「サイバーセキュリティ推進専門家会議」を設置する（改正サイバーセキュリティ基本法第 28 条、30 条、第 30 条の 2 等）。

○　内閣サイバー官（国家安全保障局次長兼務）を新設し、サイバーセキュリティの総合調整等に当たらせる（内閣法第 19 条の 2 新設）。

２　総合的評価

さて、本法律の制定で、我が国のサイバー対応能力が欧米水準になると言えるであろうか。

結論から言えば否であり、欧米水準と比べると不十分であり、多くの課題が残されている。

しかし、我が国のサイバーセキュリティの現状を前提とすれば、とにかく本法律が制定されたこと自体が大きな前進であると評価すべきであろう。我が国の政治状況など諸条件を勘案すれば、本法律が、現在、制定可能な法律であったというべきもので、不十分で課題が多く残されていても仕方がないと言える。

一方、本法律は制定後の運用実績を見て今後改正を重ねていく必要がある。政府は国会審議で、本法律はサイバー対処能力強化の「第一歩である」（平将明サイバー安全保障担当大臣）とか、「不断の見直しが必要」（内閣総理大臣）と述べる[4]など、将来の法律改正に含みを持たせる答弁をしており、本法律の不十分性は十分認識していると考えられる。今後の逐次改正、改良を期待したい。それでこそ、本法律の意義が大きなものとなろう。

それでは、以下、本法律では不十分な点や将来の課題を述べていきたい。先ず、欧米諸国、特に米国と我が国の基礎的条件の違いについて述べ、次に、法律案に即して、個別の課題を見ていきたい。

---

[4]　衆議院内閣委員会。4 月 4 日市村浩一郎議員の質問に対する平将明サイバー安全保障担当大臣の答弁、及び、今井雅人議員の質問に対する総理大臣答弁。

３　我が国に不足する基礎的条件

本法律自体の評価以前の課題として、我が国のサイバーセキュリティにおいては、米国と対比して、我が国に不足する 2 つの基礎的条件があることを指摘しておきたい。それは、サイバーセキュリティに関与するシギント機関の不在と巨大プラットフォーマーの不在である。

（1）サイバーセキュリティに関与するシギント機関の不在

我が国に欠ける基礎的条件の一つは、サイバーセキュリティに関与する「シギント（信号諜報）機関」である。シギントとは、インターネット上を含む通信や電波、信号の傍受で得た情報を利用するインテリジェンス活動のことであり、シギントは国家の安全保障や電子戦を含む軍事技術とも密接に結びついている。また、シギント活動はサイバーセキュリティのため重要な要素である。しかし残念ながら、本法律検討のための政府有識者会議の議事録を読んでも、殆どシギントに対する言及が見られない。本法律は、サイバーセキュリティ上重要なシギント活動との連携を議論せずに制定されている。

（ア）UKUSA 諸国のシギント機関の係わり

世界最強のインテリジェンス同盟に UKUSA がある。第 2 次世界大戦において、米英両国は対日独伊戦争を遂行するため、シギントでも緊密に協力した。この協力が大きな成果を上げたため、その協力関係を戦後も継続することとした。それが通称「UKUSA」と呼ばれるシギント同盟である。英 UK と米 USA 両国の協定を基軸として、その後カナダ、豪州、ニュージーランドが加わった。この 5 カ国のシギント機関は密接に協力して、ワールドワイドに活動する世界最強のインテリジェンス同盟を構築してきたのである[5]。

UKUSA シギント同盟は、サイバー空間を含め世界中に及ぶ強大な情報収集力を持ち、同盟参加 5 ヵ国のサイバーセキュリティをバックアップしている。米国を除く 4 ヵ国では、サイバーセキュリティを所管しているのは、全てシギント機関である。例えば、英国ではシギント機関 GCHQ（政府通信本部）に National Cyber Security Centre という組織が附置され、同機関が政府のサイバーセキュリティの主管組織となっている。また、カナダ、豪州、ニュージーランドも同様に、サイバーセキュリティの主管組織は、それぞれのシギント機関に附置されている[6]。

他方、米国では NSA 国家安全保障庁という国家シギント機関があるが、20 世紀におけるインテリジェンス機関に対する不信という過去の経緯があり、サイバーセキュリティ全体の

---

[5] シギントについての概説書としては、茂田、江崎道朗（共著）『シギント』（ワニブックス、2024 年）参照。更に詳しくは、茂田「米国国家安全保障庁の実態研究」（警察政策学会資料第 82 号、2015 年）（以下、茂田①）を参照されたい。

[6] 英国は 2016 年にシギント機関 GCHQ に National Cyber Security Centre を設置。カナダは 2018 年に CSE に Canadian Cyber Security Centre を設置。豪州は 2014 年に ASD に Australian Cyber Security Centre を設置し、2018 年に同センターを強化して政府のサイバーセキュリティ対策を一元化した。また、ニュージーランドは 2011 年に GCSB に National Cyber Security Centre を設置し、2017 年に強化した。

主管官庁は、NSA ではなく、国土安全保障省傘下の CISA（サイバーセキュリティ・社会基盤安全保障庁）という組織である。ところが、サイバー空間については NSA が突出した技術力と情報力を持っているため、2019 年に NSA は「サイバーセキュリティ総局」を設置して、自らサイバーセキュリティに対する取組を強化すると共に、CISA を支援している。また、サイバー関連の事件では、NSA が FBI による捜査を支援している。

（イ）シギント機関はサイバーセキュリティに不可欠

UKUSA 諸国でシギント機関がサイバーセキュリティに深く関与している理由は、一言で言えば、シギント機関がハッカー組織でもあるからである。もちろんシギント活動は、ハッキングだけではなく、無線通信も含む多様な通信を傍受し解読している。ところが、2000 年前後からサイバー空間が極めて重要な情報空間となってきたため、NSA は 1997 年には TAO というハッキング専門部署を設置して、情報収集のためにサイバー空間を開拓してきた。おそらく NSA の TAO が世界最強のハッカー組織であろう。このように、シギント組織はサイバー空間で情報収集を行い、ハッキングも行っているので、攻撃側の手口が分かる。攻撃方法を知って初めて効果的な防禦も可能となるのである。従って、サイバーセキュリティにおいても、シギント組織による支援が必要なのは当然である。

ところで、一部にハッキングとは「天才ハッカー」のような傑出した人材が行っているイメージがある。しかし、NSA の TAO はどちらかというと「装置・技術産業」であり、そのためのシステムを世界中に設置している。協力企業や UKUSA 諸国、その他の所謂サードパーティー諸国と協力関係を構築して、インターネット回線からデータを吸い上げている。NSA は世界中でサイバー空間を監視するトータルなシステム、インフラを構築しているからこそ、高いハッキング能力を持っているのである。つまり、サイバー防禦でも、シギントのインフラと能力を使ってハッカーの脅威情報を把握することによって、ハッカー集団によるサイバー攻撃を事前に察知することが可能となるのである。

少し古い資料であるが、2007 年時点での「米国シギント・システム戦略的任務リスト」という機密資料が漏洩されているが、その中では NSA の任務として、①コンピュータ・ネットワーク防禦支援、②コンピュータ・ネットワーク攻撃支援、③外国諜報諸機関によるサイバー脅威活動の解明が、明示されている[7]。

UKUSA 諸国のシギント機関は、上記のようなシギントの知見とインフラを活かして、様々な方法で各国のサイバーセキュリティ対策に貢献している。即ち、サイバーセキュリティ対策の情報提供や指導助言、教育・研究、情報システムの構築管理、事案対応、アトリビューション（攻撃者の探知特定）、積極防禦、無害化措置の支援等である[8]。

ここでは、以下、アトリビューション、脅威情報の事前把握、積極防禦の典型としての Tutelage システム、無害化支援について、簡単に説明する。

---

[7] 茂田①　30 頁。

[8] 茂田「サイバーセキュリティとシギント機関～NSA 他 UKUSA 諸機関の取組～」（情報セキュリティ総合科学第 11 号、2019 年）（以下、茂田②）58-75 頁

（ウ）アトリビューション（攻撃者の探知特定）支援

シギント機関による具体的なサイバーセキュリティ支援では、先ず、攻撃を受けた際の攻撃者の探知特定（アトリビューション）への貢献が挙げられる。

例えば、2014 年に米国のソニー・ピクチャーズ・エンタテインメントが北朝鮮から大規模なサイバー攻撃を受けた際には、攻撃発覚後 1 ヵ月程で、FBI が北朝鮮の犯行と断定している。このアトリビューションでは NSA が支援しており、NSA の看板プログラム「エックスキースコア」というシステムが貢献している。

「エックスキースコア」は、本来は、情報収集のためのシステムで、世界中の主要収集拠点に設置されたデータの一次記憶装置であり、且つ分析支援システムである。これが同時に、アトリビューションにも活用できるのである。嘗て NSA の職員であったエドワード・スノーデンが、2013 年に大量の機密情報を漏洩したが、漏洩資料の中には「X-Keyscore for Cybersecurity」という表題のプレゼン資料があり、サイバーセキュリティにおけるエックスキースコアの活用方法を説明している。また、スノーデン自身もサイバー攻撃に対するアトリビューションでエックスキースコアを使ったことがあると述べている[9]。

この他にも、「宝地図」（インターネットの詳細世界地図）や「プリズム」など活用できるシギントのシステムがあり、NSA は、これらを活用してアトリビューションに貢献しているのである。

（エ）脅威情報の事前把握

また、サイバー防禦では脅威情報の事前把握が重要であるが、シギント機関は各種の手法で脅威情報を事前に収集している。スノーデンによる漏洩資料によると、2013 年の時点で既に次のような対策を取っていた[10]。

○　「イオンブルー」：世界のインターネット通信網に設置したハッカー通信の探知センサー。カナダのシギント機関 CSE が UKUSA 諸機関の協力を得て設置したもので、2010 年時点で世界 200 ヵ所以上に設置していた。

○　「ラブリーホース」：ダークウェブ上のハッカーのブログやチャットから、ハッカーの動向に関する情報を自動的に収集し分類して、分析官が使用できるようにしたシステム。英国のシギント機関 GCHQ が開発した。

現在、イスラエルや韓国、台湾系などの民間企業が、このようなダークウェブの情報を収集分析して販売しているが、UKUSA シギント機関は既に 15 年前にシステム化していたのである。

○　「C-CNE（Counter-Computer Network Exploitation）」：ハッカー対策であるが、これは脅威国のハッカー集団のシステムをハッキングして、その脅威（ウィルスなどの技術情報、

---

[9] 茂田② 64-66 頁。

[10] 茂田「米国 ACD・Defend Forward とシギント機関の役割～日本『能動的サイバー防御』と対比して～」（警察政策学会資料第 134 号「国家安全保障に関する諸論考」、2024 年）（以下、茂田③）34-36 頁

攻撃目標や時期、既に入手した情報など)を解明するシギント活動である[11]。NSA は 2013 年時点で中露などの 28 のハッカー集団をハッキングして脅威情報を収集し、ハッカー集団に対して対策を講じていた[12]。

2023 年の報道[13]によれば、2020 年秋に NSA は防衛省のコンピューターシステムが中国人民解放軍によってハッキングされていることを探知し、米政府が日本政府に警告を発したという。これは NSA が、C-CNE によって浸透した人民解放軍系のハッカー集団のコンピュータの中に、防衛省の秘密情報を発見したものと推定できる。

（オ）Tutelage システム（積極防禦の典型）[14]

米国 NSA は、上記の脅威情報の事前把握、特に C-CNE によって解明したハッカー集団の脅威情報を基に、2009 年に Tutelage システムを構築し導入した。これは、米国国防省の情報システム NIPERNet[15]とインターネットの接続点に設置したものであるが、脅威ハッカー集団に対する C-CNE によって、マルウェアの開発準備段階で、その技術、攻撃目標や時期を解明して、接続点に攻撃が到来する前に対抗システムを配置しておくものである。NSA 漏洩資料によれば、Tutelage システムによって 2010 年には国防総省高官に対するフィッシング攻撃を阻止するなどの成果を挙げていた。

この Tutelage システム、或いはその派生型は、米国一般官庁用のシステム Einstein 3A や他の UKUSA 諸国にも導入されたとみられる。また、NSA 漏洩資料によれば、2013 年にドイツが Tutelage システムの導入に意欲を示していた。

（カ）無害化措置、無害化支援[16]

米国は、2018 年に前方防禦（Defend Forward）戦略を採用した。これは脅威がインターネットとの接続点に到達する前に、敵空間又はインターネット空間で先制的に防禦するものである。これが始まった背景は、結局 Tutelage システムなど従来の対策では不十分であったからである。C-CNE によっても全ての脅威ハッカー集団の解明は不可能であり、また、地方政府や民間インフラ等の防護も重要であるからである。考え方は、今回我が国の整備法によって規定された無害化措置と類似の措置である。

---

11 茂田① 95-96 頁。

12 次に述べる Tutelage である。

13 Ellen Nakashima, “China hacked Japan’s sensitive defense networks, officials say,” *The Washington Post*, 8 August 2023, last accessed 22 April 2026.

14 茂田② 67-72 頁、茂田③ 35-36 頁。

米国政府による Active Cyber Defense という言葉の使用は、2010 年代初めに多く見かけるが、典型例は Tutelage システムであり、脅威ハッカー集団のシステムに対する無害化措置とは別物である。無害化措置は、後述の Defend Forward 戦略の一部と位置付けられている。この点、無害化措置を、Active Cyber Defense の中心とする我が国の用語法とは異なっている。

15 Unclassified and controlled unclassified information(sensitive 情報)が扱える謂わば国防総省イントラネット。日本の横田基地を含め世界 10 カ所でインターネットと接続されている。この他、国防総省には SIPRNet（Secret まで取扱い可）と JWICS（Top Secret まで取扱い可）の情報システムがあるが、これらはインターネットとは接続されていない。

16 茂田③ 41-44 頁

国外にあるハッカー集団の無害化は、以前から NSA による「秘密工作（Covert Action）」として可能であったが、「秘密工作」の実施には大統領の個別決裁と（事後の）議会報告[17]が法律で義務付けられており、その前提として国家安全保障会議の審議を経る必要があるなど、サイバー空間における脅威集団に対して適時に対応することが困難であった。

そこで、米国は 2019 年国防授権法によって、サイバー空間における秘匿の軍事活動を、「秘密工作」には該当しない「伝統的軍事活動」[18]と定義することによって、個別の大統領決裁と議会報告を不要としたのである。この結果、「武力の行使」に該当しない一定のサイバー作戦は国防長官又は Cyber Command 司令官の権限で実施可能となった。軍事活動と定義したので、所管は米軍の Cyber Command であるが、その実施においては NSA が支援している。Cyber Command 司令官は NSA 長官が兼務しており、NSA と Cyber Command は緊密な協力関係にある。

米国が前方防禦作戦を実施した典型的な事例は、2018 年秋の Synthetic Theology 作戦である。米中間選挙で選挙介入を図ったロシアの Internet Research Center のサーバーをインターネットから遮断するなどの無害化措置を実施した。作戦権限は Cyber Command であったが、実際は NSA との合同チームで取り組んでおり、NSA が Cyber Command を支援しているのである。

米国と同様に、他の UKUSA 諸国でも、このような無害化措置、即ち、国外からのサイバー脅威に対する対抗措置にはシギント機関が貢献している。例えば、英国は 2000 人規模の National Cyber Force を創設したが、これは GCHQ と国防省が中心の組織である。また、豪州ではサイバー攻撃部署はシギント機関 ASD の内に設置されている。このようにシギント機関の役割には大きなものがある。

なお、米国 Cyber Command、英国 National Cyber Force、豪州 ASD 内の攻撃部署などのような「サイバー攻撃能力」の任務には、平時には脅威ハッカー集団の無害化が含まれるが、戦時においては正に戦争行為としてのサイバー攻撃が含まれるのである。

以上、簡潔に述べたが、NSA 初め UKUSA シギント諸機関がサイバーセキュリティにおいて果たす役割は大きなものであり、我が国においてもシギント機関の抜本的強化とサイバーセキュリティへの関与を議論すべきであろう。

---

17 この議会報告は公開で行うものではなく、通常 Gang of Eight と呼ばれる 8 人に対して秘密報告がなされる。8 人の内訳は、上下両院の与野党のトップ 4 人、上下両院の諜報委員会の与野党のトップ 4 人。正式には、下院（議長と少数党院内総務、諜報特別委員会の委員長と筆頭理事）、上院（多数党院内総務と少数党院内総務、諜報特別委員会の委員長と副委員長）である。

18 中曽根平和研究所の大澤淳氏は、サイバー脅威に対して国外で対抗措置をとる行為は、国際法上「軍隊」が実施することとされていると主張している（「サイバーでも反撃できない日本」（『産経新聞』2024 年 4 月 28 日付）。しかし、米国が「伝統的軍事活動」と定義したのは、米国内法上の都合によるものであって、国際法に基づくものではない。

（2）巨大プラットフォーマーの不存在

米国と対比して我が国に欠けるもう一つの基礎的条件は、巨大プラットフォーマーの存在である。

米国にはグーグル、アマゾンウェブサービス、マイクロソフトといった巨大プラットフォーマーがある。彼らは世界中に及ぶ彼らのプラットフォームから、日々、脅威情報などを収集している。その上で、NSA と密接に協力している。

2020 年に NSA は本部ビルの隣に民間企業との官民連携組織「サイバーセキュリティ協働センターCybersecurity Collaboration Center」を設立した。2023 年夏の時点で既に IT 企業など約 500 社が参加している。そこでサイバーセキュリティに関する技術的知見について実務的な情報交換をしている。NSA がシギント活動から得た機密の知見と、民間企業が収集した脅威情報と専門技術を総合しており、サイバーセキュリティ対策の拠点となっている。NSA 本部は秘密保持のため原則的に民間企業の人は入れないため、近くに民間企業用の専門家と協働するためのビルを建設したのである。

残念ながら、日本には巨大プラットフォーマーが存在しない上、シギント機関と民間企業の間の密な情報交換もない。初期条件で既に大きなハンディキャップを背負っているのである。法律だけを見てもこの基礎的条件の違いは分からない。この点を押さえた上で、次に本法律の今後の課題について、政府の運用方針や国会審議を踏まえて法律に即して論じていきたい。

４　アクセス・無害化措置の課題

先ず、注目を集めている所謂アクセス・無害化措置について論じる。

典型的なアクセス・無害化措置は、整備法によって新設された警察官職務執行法第 6 条の 2 によるものである。本条によれば、警察庁のサイバー危害防止措置執行官（担当警察官）[19]が、①情報技術利用不正行為（サイバー不正行為）に用いられる電気通信や電磁的記録を認めた場合であって、②「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」に、危害防止措置（不正プログラムの停止・削除など）を、加害関係コンピュータの管理者等に対して執ることを命じ、又は自ら執ることができるというものである[20]。

---

[19] 警察庁のサイバー危害防止措置執行官には、関東管区警察局サイバー特別捜査部特別対処課に属する警察官が想定されている（警察庁組織令第 48 条第 2 項、同施行規則第 134 条、第 137 条参照）。

[20] 国内におけるアクセス・無害化措置については、我が国では本条の枠組で行われるが、米国では FBI が司法手続の一環として行う慣行が確立している。即ち、マルウェアの削除や通信遮断による無害化措置が、連邦刑事訴訟規則第 41 条に基づく捜索差押として裁判所の令状を得て行なわれている。2023 年 Qakbot ボットネット、2024 年中国系 Typhoon ボットネットなど、国内の所在地不明の多数のボットネットの無害化が有名である。

なお、我が国の場合、国内における無害化措置についても、本文①のサイバー不正行為に加えて、②の「緊急の必要」要件が必要とされている。しかし、現実に①の違法状態が存在しており、且つ、サイ

さて、このアクセス・無害化措置について、その手続規定を確認した上で、課題を述べたい。

（1）アクセス・無害化措置の手続

我が国に対するサイバー攻撃の殆どが国外からのものであるので、国外に設置されている加害関係コンピュータに対するアクセス・無害化措置を前提に、その手続を整備法（警察官職務執行法第 6 条の 2）及び国家安全保障会議が決定した運用指針[21]を基に、どのような手続が想定されているのか、確認する。

① 対処方針案の作成（運用指針 2（1））

内閣官房国家安全保障局が、内閣官房国家サイバー統括室と十分に連携を図りつつ、警察庁、外務省、防衛省等と調整してアクセス・無害化措置を実施するに当たっての方針[22]を作成する。

② 国家安全保障会議における対処方針の審議（運用指針 2（2）、（3））

この際の会議員は、総理大臣、外務大臣、防衛大臣、内閣官房長官、サイバー安全保障大臣、国家公安委員長その他関係大臣となる。

③ 国家サイバー統括室による総合調整（運用指針 2（1））

対処方針に基づき、国家サイバー統括室が、サイバー安全保障担当大臣の指導の下、国家安全保障局と連携しつつ、個別のアクセス・無害化措置に係る、警察庁及び防衛省・自衛隊の役割分担等に対して総合調整を行う。

④ 外務大臣との協議（警職法第 6 条の 2 第 3 項）

担当警察官は、警察庁長官を通じて、外務大臣と協議する。

⑤ サイバー通信情報監理委員会の承認（同条第 4 項、第 5 項）

担当警察官は、危害防止措置について、サイバー通信情報監理委員会の承認を得る。但し、基幹インフラ事業者の重要電子計算機に対して（その機能に重大な障害を生じさせ、又は生じさせる虞のある）加害関係電気通信が現に送信されている場合その他、危害防止のため承認を得る暇がないと認める特段の事由がある場合は、速やかな事後通知でよい（同条第 9 項）。国会答弁によれば、「特段の事由」の要件としては、重大な危害発生の切迫性が挙げられている[23]。

バー通信情報監理委員会の承認が要件とされているのであるから、②の「緊急の必要」要件まで必要か、疑問がある。①の要件に付加する要件は、他の規定の仕方もあったのではないか。違法状態の除去は知らぬ間にマルウェアを設置された加害関係コンピュータの管理者にとっても利益となるのである。

[21] 国家安全保障会議決定 2025 年 12 月 26 日、「アクセス・無害化措置の運用に関する指針」（「運用指針」）。

[22] 対処方針については、アクセスと無害化措置についての概括的な一般方針ではなく、個別事案毎の対処方針とされる。（参照、参議院内閣委員会、2025 年 5 月 15 日奥村政佳議員の質問に対する飯島内閣審議官答弁。「アクセス・無害化措置については、…サイバー攻撃キャンペーン毎に議論をいたしまして総論的な対処方針を定める」）

[23] 重大な危害発生の切迫性を「特段の事由」の要件とする国会答弁は次の通り。即ち、「その時点でアクセス・無害化措置をとらなければ、人の生命、身体又は財産に対する重大な危害の発生を防ぐことができないという状況」であり、具体例として「サイバー攻撃により基幹インフラに現に重大な障害が発生している状況、攻撃者によるサイバー攻撃の敢行予定日時等が判明したが、既にその予定時刻が切

⑥　危害防止措置の実施（同条第 2 項）

危害防止措置のうち実際の無害化措置として想定されているのは、国会答弁[24]や政府公表資料[25]によれば、攻撃者が加害関係サーバーへアクセスできないように設定を変更するとか、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・削除するとか、攻撃者のサーバーをインターネットにアクセスできなくするとか、攻撃コマンドを送れなくするというものであって、「サーバー等に物理的被害や機能喪失等、その本来の機能に大きな影響を生じる、大きな影響が生じることは想定され」ないとしている。

⑦　危害防止措置の設備管理者への通知（同条第 8 項）

国家公安委員会規則で定めるところにより、遅滞なく、施設管理者に通知をする。但し、加害関係コンピュータに関する危害防止に支障がある場合及び管理者の所在が不明の場合は、通知は不要である。国会審議から判断すると、国外の脅威集団に対するアクセス・無害化措置の実施については、通知を行わないのが基本的な方針であると推定できる[26]・[27]。

⑧　実施報告（運用方針 2（5））

国家公安員会は、サイバー安全保障保障担当大臣と調整の上、実施したアクセス・無害化措置について国家安全保障会議に報告する。

迫している状況」が挙げられている（参議院内閣委員会、2025 年 5 月 15 日奥村政佳議員の質問に対する飯島内閣審議官答弁）。

[24] 衆議院内閣委員会、2025 年 4 月 3 日赤嶺政賢議員の質問に対する平大臣答弁。参議院内閣委員会、同年 5 月 15 日石川のりこ議員に対する平大臣答弁

[25] 国家サイバー統括室、「サイバー対処能力強化法及び同整備法について」（2025 年 9 月）、スライド 37 頁。https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

[26] 平大臣は、「サイバーセキュリティの世界は、私はこんなことをやりましたということは基本的には秘匿をされつつ、必要な時にパブリックアトリビューションでここがやったんではないかというのも、かなり戦略的にだすことになります」と答弁しているので（参議院内閣委員会、2025 年同年 5 月 15 日石川のりこ議員に対する平大臣答弁）、本項に規定する「加害関係電子計算機に関する危害防止に支障がある場合」と解釈して、通知をしない場合が多いのではないかと推定する。

また、自衛隊が行う通信防護措置（アクセス・無害化措置）についてであるが、次の政府答弁があり、これからも、通常は、国外施設の管理者には通知しない方針であると推定される。「通信防護措置の実施後、国会に報告して当該措置の内容を明らかにすることは、我が国政府がどのような事案を調査してるのか、またどの攻撃者にどのような手法を用いて措置を実施したのかどうかなど明らかになるおそれがございますので、その場合、当該措置を受けた攻撃者が自衛隊による措置であることを認知しその手法を研究して対策を講じるなど、結果的に攻撃者を利することにつながる…ので、措置の終了後の情報の取扱いについても慎重な検討が（必要で？）ある」（参議院内閣委員会、2025 年 5 月 15 日大島九州男議員に対する飯島内閣審議官答弁）。

[27] 危害防止措置の設備管理者への通知に関連して、衆議院内閣委員会で、中曽根平和研究所の大澤淳参考人は、2018 年に米政府がサンクトペテルブルグにあるサーバーに対して無害化措置を執った際には、（無害化措置の相互エスカレーションを防ぐために）、作戦実施後に作戦の目的と理由を説明した旨の発言をしている（衆議院内閣委員会、2025 年 3 月 28 日市来伴子議員の質問に対する答弁）。本件無害化措置とは Synthetic Theology 作戦と伝えられる作戦で、2018 年米国中間選挙に際して、ロシアによる選挙干渉を防ぐために、米 Cyber Command と NSA の合同チームが、サンクトペテルブルグの Internet Research Agency のサーバーをインターネットから遮断する措置（無害化措置）を実施したことを指すと考えられるが、米国政府が、本作戦の実施について公式に認めた事実は確認されていない。本作戦については秘密扱いであり、その理由は、正に相手国との相互エスカレーションを回避し、また、能力を秘匿する必要があるためと考えられる。

なお、国内に設置されている加害関係コンピュータに対するアクセス・無害化措置であって、且つ国家安全保障に関わらない場合の手続は、上記⑤⑥⑦のみである。

（2）欧米主要国と同等以上の対応能力が実現されたか？

2022 年 12 月閣議決定「国家安全保障戦略」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」、「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ー等への侵入・無害化ができるよう、政府に必要な権限が付与されるようにする」と記載されているが、残念ながら、本条によっては、欧米主要国と同等以上の無害化措置は実現できない。

その最大の原因は、本来、平時から、どの集団がどのような手段を使ってどの標的を攻撃しようとしているかについて、脅威情報を探知解明しておく必要があるが、それには、平時からハッカー集団のサーバーにアクセス（＝ハッキング）して、ハッカー集団の持つマルウェアなどの技術情報、攻撃しようとしている標的や時期などの作戦情報を事前に把握することが効果的である。しかし、本条の手続では、「緊急の必要」が生じて、初めて、攻撃者のサーバーへのアクセスを試みることができる構造（アクセスを試みても即座にアクセスする能力は担保されていない）となっているからである。

以下、課題を詳しく見ていく。

（3）アクセス要件の課題

アクセス・無害化措置の手続で注目すべきは、法律は「危害防止措置」と規定しているが、運用指針では「アクセス・無害化措置」と記述しており、無害化措置以前の加害関係コンピュータへのアクセスが、無害化措置と一体のものとして規定されている点である。従って、加害関係コンピュータに対してアクセスする要件は、「危害防止措置」「無害化措置」の要件と同一と考えざるを得ない。

危害防止措置の要件は、サイバー不正行為に用いられる電気通信・電磁的記録を認めた場合であって、且つ「そのまま放置すれば、人の生命、身体また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」である。アクセスするにも、この「緊急の必要」が要件となる。

（ア）平時からの脅威情報の事前把握は困難

既述の通り、米国 NSA は、C-CNE によって、脅威ハッカー集団のシステムにアクセス（＝ハッキング）してその脅威、即ち、ウィルスなどの技術情報、攻撃目標や時期、ハッカー集団が既に入手した情報などを解明するシギント活動を行なっている。事前にアクセスしていれば、「そのまま放置すれば、人の生命、身体また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」かどうか、脅威度の判断が容易になる。しかし、本手続では、サイバー不正行為の認知に加えて、「緊急の必要」要件を充足して初めてアクセスできるのであるから、米国のように平常から、脅威ハッカー集団のシステムにアクセスして、その脅威を把握解明することはできないこととなる。

（イ）アクセスには時間がかかる

本手続を見ると、サイバー不正行為を認知して且つ「緊急の必要」がある場合に、初めてアクセスを試みるのであるから、迅速にアクセスする必要があるのは明白である。しかし、そもそもアクセスの努力の開始、イコール、アクセス成功ではない。「緊急の必要」があるにも拘わらず、迅速にアクセスに成功できるか、課題が残るのである。

米国の漏洩資料を見ても、国家レベルのハッカーは、多くの作戦中継機（hop points）を経由し、且つハッカー端末の IP アドレスも変更されるため、ハッカー端末を特定するのに困難を極めた事例が記述されている。また、ハッカー端末を特定した後に、端末へのアクセス（＝侵入）では Man-in-the-Middle と称する高度なハッキング手法が必要であった[28]。

我が国のアクセス能力は NSA のアクセス能力よりも高いとは到底考えられないが、本法律と手続は、アクセスに必要な時間をどう想定しているのか、疑問が残る[29]。

（ウ）アクセスのための「緊急の必要」の要件とは何か

本来、サイバー不正行為を認知した場合には、即座に脅威ハッカー端末へのアクセス努力を認める必要がある。しかし、本法では更に「緊急の必要」要件が必要である。それでは、「緊急の必要」要件とは、具体的にはどのようなもので、如何にして判断するのであろうか。

「緊急の必要」要件についての政府答弁[30]では、「マルウェアに感染した IoT 機器を発見した場合で、…当該マルウェアと C2 サーバーが定期的に通信を行っていると認められるため、攻撃者の意図次第でいつでも攻撃が行われると認められる場合」を例示している。この場合は、既に C2 サーバーにアクセスして「攻撃者の意図」を解明している訳ではないので、「攻撃者の意図」は不明であるが、危害発生の切迫の可能性があれば「緊急の必要」要件を満たすと解釈していることになる。即ち、客観的な重大な危害発生の切迫性までは要件としていないと解釈せざるを得ない[31]。

ところで、一般的なランサムやボットなどのマルウェアは C2 サーバーと定期的通信が見られると言われる。しかし、有名な Volt Typhoon は、長期潜伏型で必要時にのみ低頻度の偽装通信をするだけで、定期通信を行う訳ではなく、また、同じく有名な Lockbit も通信は攻撃段階毎に断続的に発生し、定期通信を行う訳ではないとされる。つまり、C2 サーバーとの定期通信がないとしても、危害発生の切迫の可能性がない訳ではない。定期通信がない場合に、「緊急の必要」、危害発生の切迫の可能性をどのように認定するのであろうか。

運用指針では、アクセス・無害化措置を行う典型としては「サイバー攻撃キャンペーン」

---

[28] 茂田① 95 頁。

[29] 国会審議や政府資料を見ると、脅威ハッカー集団が構築しているボット網については、そもそもセキュリティに弱点があるので、アクセスが容易であろうという想定が示されているが、この議論を前提とすると、ボットではなく、攻撃の発信源や C2 サーバーに対するアクセスの難易度をどう想定しているのか、不明である。

[30] 参議院内閣委員会、2025 年 5 月 15 日片山大介議員に対する飯島内閣審議官答弁。

[31] (1)アクセス・無害化措置の手続⑤脚注で述べたように、重大な危害発生が切迫している場合には、サイバー通信情報監理委員会の事前承認ではなく事後報告で良いとされている点から判断しても、事前承認を必要とするアクセス・無害化措置については、重大な危害発生の切迫性までは必要とされていないと解釈できる。

（一定期間内において特定の主体が国・重要インフラ等の特定の組織・分野に対して特定の攻撃手法・攻撃インフラを用いて繰り返し行うサイバー攻撃活動）[32]を想定している。「サイバー攻撃キャンペーン」とはLockBitのようなランサム犯罪集団による攻撃や、Volt Typhoonのような重要インフラ等への事前侵入などを指しているとみられる。ランサム犯罪集団による攻撃では、既に各地で散発的にでも実害が発生している場合には、「緊急の必要」が認め易いであろう。他方、Volt Typhoonのような有事に備えた長期潜伏（pre-positioning）で、C2サーバーと定期通信もしない、所謂Living off the Landの場合、その探知には相当の困難[33]が予想される。そして仮に探知しても、重大な危害発生防止の「緊急の必要」をどのような論理で認定するのであろうか。Volt Typhoon型の場合は、数年にも亘る潜伏期間が想定されるが、潜伏それ自体の探知があれば、“脅威国の意図次第でいつでも戦争とサイバー攻撃が起こり得る”ので、「緊急の必要」があると解釈するのであろうか。何れにしろ、「サイバー攻撃キャンペーン」に対しても、探知してから、何時の段階からアクセス努力を開始できるのか、その場合の「緊急の必要」をどう認定するのかが、課題であろう。

他方、国家アクターが特定の個別標的を狙って攻撃をしてくる場合は、何をもって「緊急の必要」要件を認定するのか、不明である。

結局、「緊急の必要」要件は、サイバー通信情報監理委員会の判断次第であり、同委員会の責任は重い。

（エ）在るべきアクセス要件

上記のような各種の課題は、アクセスの要件と無害化措置の要件を同一としていることに起因する。そもそも、現にサイバー不正行為が行われているのにもかかわらず、その脅威の解明のためのアクセスについて、更に「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「緊急の必要」要件を課すことに意味があるとは考えられない。

立法論としては、アクセス要件と無害化措置の要件を別個に設定し、アクセス要件には「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」の要件を不要とすべきであったと考える。即ち、サイバー不正行為が行われていると認めた場合には、サイバー通信情報監理委員会の承認を得て、アクセス活動を認めるべきであろう。

現行法の運用についても、危害防止措置（＝アクセス）を実施する「緊急の必要」は幅広く認め、具体的な対処方針の中では、無害化措置の実施についてはより厳しい要件を別途設定することによって、アクセス・無害化措置が機能し易くするようにするべきではないかと考える。

（4）手続規定の煩雑さ

先述のように、米国では、外国ハッカー集団の無害化は、NSAによる「秘密工作（Covert

---

[32] 運用指針 2(1)

[33] Volt Typhoon型の探知に関しては、友好国の機関からの情報提供に多くを期待することになるのであろうか。

Action)」として可能であったが、その実施には大統領の個別決裁が必要であるなどの手続を経る必要があったため、サイバー脅威集団に対して適時に対応することが困難であった。そのため、2019 年国防授権法によって、個別の大統領決裁を不要として、国防長官又はサイバー司令官の権限で実施可能としたのである。

本条の「危害防止措置」の実施手続は、上記（1）でも見たように、2018 年以前の米国の手続よりも、更に複雑である。国家安全保障会議における対処方針の審議には外務大臣が加わっているにもかかわらず、更に、それとは別に担当警察官が警察庁長官を通じて外務大臣との協議を要するなどの手続を付加している。

今後の運用実績を見て、手続を簡素化する必要が判明すれば、法律改正を躊躇するべきではないだろう。

（5）自衛隊による無害化措置の課題

次に、自衛隊によるアクセス・無害化措置（自衛隊法第 81 条の 3「通信防護措置」）の課題を見てみよう。これは、国外からの「特に高度に組織的且つ計画的な行為」に対して自衛隊が有する「特別の技術又は情報が必要不可欠なとき」、警察と共同して実施するものである。

（ア）更に煩雑な手続規定

警察によるアクセス・無害化措置（「危害防止措置」）の手続ですら複雑であるが、自衛隊法第 81 条の 3 によるアクセス・無害化措置（「通信防護措置」）は更に煩雑である。

上記（1）③の内閣官房国家サイバー統括室による総合調整の結果、警察・自衛隊による共同対処を実施することとされた場合には、（1）③と④の間に更に次の手続が加重されることになる（運用指針 2（2））。

③－①　自衛隊による通信防護措置について、再度の国家安全保障会議での審議
（運用指針 2（2））

③－②　国家公安員会からの要請又は同意（同条第 1 項）

③－③　防衛大臣と国家公安委員会の協議（同条第 4 項）

③－④　閣議決定（運用指針 2（2））

③－⑤　内閣総理大臣による通信防護措置の命令（同条第 1 項）

このような複雑な手続で、「緊急の必要」がある時に、適時に対処できるのか、大きな課題であろう。

（イ）なぜ、閣議決定まで必要なのか

特に、上記手続では、自衛隊がアクセス・無害化措置において警察と共同対処するには、閣議決定が必要とされている。

その理由を推定すると、第 1 に、治安出動（自衛隊法第 87 条、第 81 条）との権衡が考えられる。自衛隊によるアクセス・無害化措置は、警察によるものと同様に、広義の治安活動と位置付けられている。そして、総理大臣による治安出動の下令手続としては、閣議決定が必要と解釈されているので、その対比で閣議決定を必要としたと考えられる。

しかし、治安出動命令は、自衛隊という武力に準じる実力を国内で行使する、即ち、場合によっては国民に対して殺傷能力の高い武器を向けることとなる非常の措置であって、内閣

全体の責任として行うべき最も重い決定である。

それに対して、自衛隊によるアクセス・無害化措置は、先ず、国外からの脅威に対して実施されるものであるから、治安出動とは異なり、国民に対して武器を向ける可能性は存在しない。また、同措置は、国外の脅威に対して「緊急の必要」がある時に迅速に実施すべき措置であり、且つ、その措置は脅威を無害化するだけであって、「サーバー等に物理的被害や機能喪失等、その本来の機能に大きな影響を生じる、大きな影響が生じることは想定され」ない[34]のである。更に、運用指針によれば、既に 2 回に亘る国家安全保障会議による審議を経ている上に、更に閣議決定を必要としているのである。屋上屋を架する手続としか言いようがない。

他方、閣議を経ることによって、当該アクセス・無害化措置について閣僚全員が知ることとなり、秘密保全の点でも問題がある。既述のように[35]、自衛隊による国外の脅威集団に対するアクセス・無害化措置の実施については、通知を行わない方針であると推定できるが、この方針と矛盾すると考えられる。

理由の第 2 は、内閣制度上の総理大臣の位置付けが考えられる。憲法第 72 条は、総理大臣の権能として、内閣を代表することと、行政各部を指揮監督することしか規定していない。従って、総理大臣は、あくまで内閣を代表して自衛隊に「通信防護措置」を命ずるのであって、内閣を代表して命じるからには個別の閣議決定が必要であるという論理に立っている可能性がある。しかし、この解釈運用は、学問的憲法解釈を優先して、現実の必要を軽視するものである。

従って、予め包括的な「通信防護措置の発動方針」を閣議決定で定めておいて、個別案件ではその方針の範囲で総理大臣が機動的に発動の判断をする（＝個別案件での閣議決定を不要とする）など、工夫をするべきではないかと考える。

（ウ）警察・自衛隊による共同実施の課題

自衛隊法第 81 条の 3 による「危害防止措置」（アクセス・無害化措置）は、同条第 3 項で警察と共同して実施することとされている。この場合は、警察庁長官指揮下の担当警察官と防衛大臣指揮下の担当部隊と、指揮系統が並列関係になる。

機動的な決定と行動を要する現場活動においては、指揮系統を一元化し、責任も一元化する必要があるのは常識である。二つの指揮系統間の調整を現場担当者の協力に委ねることは、混乱の元となることが危惧される。

アクセス・無害化措置の共同実施に当たっては、国家サイバー統括室で総合調整した後に 2 回目の国家安全保障会議が開催される手続になっているが、そこでは二つの指揮系統の優先関係と責任を明確にすべきである。即ち、二つの指揮系統の現場調整が迅速にできない場合には、何れの指揮系統を優先させるか（同時に、主たる結果責任を負わせるか）を、事案毎に予め決定しておくべきであろう。その場合、自衛隊が有する「特別の技術又は情報が必要不可欠なとき」に、自衛隊に「通信防護措置」を下命する趣旨からすれば、現場判断の権限と責任は、防衛大臣の指揮下の担当部隊が負い、警察の担当官は自衛隊部隊の活動を支援する

[34] 上記（1）⑤参照。
[35] 上記（1）⑦参照。

役割となることが多いのではないだろうか。

（エ）自衛隊部隊の実力

自衛隊によるアクセス・無害化措置が実施されるのは、国外からの「特に高度に組織的且つ計画的な行為」であって、且つ、自衛隊が有する「特別の技術又は情報が必要不可欠なとき」である（同条第 1 項）。

即ち、本法では、自衛隊は警察よりも高度な能力（技術・情報）を持っていることが当然の前提とされている。

さて、それでは自衛隊のサイバー防衛部隊の能力は、どれ程高いのであろうか。仄聞するところでは、自衛隊のサイバー防衛に関しては、潤沢な予算と人員が措置されているから、装備や人員面においては、警察を遥かに上回る水準を保持していることが推定される。また、訓練も十分に行われているであろう。

問題は、実戦経験である。装備と訓練だけでは精強な部隊を構築することは難しく、実戦経験と経験に基づいた訓練が重要である。サイバー空間に関して言えば、実戦とは、インターネット空間及び敵空間（標的システム）内における作戦経験である。2013 年のスノーデン漏洩情報にいう Computer Network Exploitation（CNE）、即ち、標的システムへのアクセス確保とデータ収集の経験である。これらは、正に、シギント機関の任務であり、シギント機関が最も経験を積み知見を有する分野である。そこで、米英豪を見ると、アクセス・無害化措置に当たる組織は、全て、このシギント機関の経験と能力を活用できる立場にある。米国 Cyber Command は、シギント機関 NSA の長官が司令官を兼務するなど密接な協力関係にあり、NSA の人員・経験・情報・装備を活用できる。英国 National Cyber Force は、GCHQ と国防省が中心の組織であり、人員の約半数はシギント機関である GCHQ から派遣されていると推定できる。また、豪州はシギント機関 ASD 自体が、無害化措置の主体である。このように、無害化措置の実施主体はシギント機関と密接な関係にあり、シギント機関の経験と中核人材を活用できるのである[36]。

しかし我が国には、現在、CNE を実施しているシギント組織は存在していないと考えられる[37]。このような環境において、如何にして、自衛隊のサイバー防衛部隊の能力を高めることができるか、大きな課題である。サイバー空間を主な活動空間とする国家シギント機関の必要性が痛感されるのである。

５　事業者の保有する通信情報の利用の課題

強化法によって、政府は通信事業者から、外外通信、外内通信、内外通信から、サイバー不正行為に関連する一定の通信情報を取得して、サイバー攻撃の実態を把握するとしている。

---

[36] 無害化措置の実施主体は、シギント機関と単に密接な関係を有するだけではなく、UKUSA 諸国によるシギント・インフラも活用できるのである。

[37] 肚の座った防衛大臣が、情報本部電波部門に対して刑法第 35 条の正当業務行為を適用して CNE 活動を命じる可能性が絶無とは言えないが、不正アクセス禁止法が存在する現在、先ず、有り得ないであろう。

しかし、取得する通信情報は極めて限定的であり、その使用目的も限定されている。サイバーセキュリティ対策上の課題を 2 点指摘しておきたい。

（1）「選別後通信情報」の限定性

本法律では、政府が通信事業者から取得して分析対象とする通信情報は「選別後通信情報」、即ち、人による知得を伴わない自動的な方法によって、「不正行為に関係があると認めるに足りる状況」の「機械的情報」（IP アドレス、指令情報等で、通信の意思疎通の本質的な内容ではない情報）のみを選別し、それ以外は直ちに消去する措置を講じたものとされる（「自動選別」[38]）。この限定の下で、どれだけ有効なサイバーセキュリティ対策ができるのか、疑問である。

結局「選別後通信情報」とは、既知の加害関係サーバーとの通信や既知の指令情報などのハッカー通信を含む通信情報に限定されてしまうだろう。つまり、未知のハッカー通信は探知できないし、既知のハッカー通信を含まない未知の加害関係サーバーとの通信も探知できない。新しい指令情報や加害関係サーバーに関する情報を入手しても、過去の通信情報に遡って検索することもできない。

更に実際のハッカー通信には、ハッキングしたサーバーから入手する秘密情報が含まれる。しかし、秘密情報は機械的情報には含まれないであろうから、秘密情報が漏洩しているか否かについては、国内の通信事業者から得た通信情報からは知り得ないこととなる。先に紹介した NSA のエックスキースコアは、機械的情報に限定せずに通信内容を収集しているので、ハッカー集団のアトリビューションにも有効なのであるが、我が国の場合の有効性は限定的なものとなろう。

2023 年 5 月に FBI は、ロシアの諜報機関 FSB（旧 KGB）のセンター16 内のハッカー組織が使用する「スネイク」というマルウェアを感染コンピュータ多数から除去する作戦を実施したが、「スネイク」によるハッカー通信は、HTTP や TCP などの正常通信を偽装した暗号通信であり、その探知は困難を極めたとされている。そのためその解明には、「スネイク」

---

[38] この「自動選別」によって、どれほど効果的にハッカー通信を探知できるのであろうか。

本文「3（1）（エ）脅威情報の事前把握」で紹介したが、カナダが既に 2010 年頃に導入済みの EONBLUE というサイバー脅威探知センサーがある。これはカナダ CSE が UKUSA 諸機関の協力を得て、世界のインターネット空間に設置されているシギント・インフラを活用して、サイバー脅威探知センサーを 200 以上設置したものである。

探知手法は、anomaly-based discovery と signature-based detection の二つある。anomaly-based discovery（SLIPSTREAM）プログラムは、ハッカー通信に特徴的な特異性を探知する。通信の周期性、暗号強度のレベル、或いは通信パケット内容の分析など 50 以上の特異性の検知方式によって、ハッカー通信を発見しようとしている。また、signature-based detection（SNIFFLE）プログラムは、既に解明したハッカー通信に特有な特徴点を基にハッカー通信を探知するものである。

後者の signature-based detection（SNIFFLE）プログラム部分は、我が国でも選別前の通信情報に適用すれば、ハッカー通信探知に効果が見込まれるであろうが、それは可能であろうか。
茂田③34-35 頁参照。

型マルウェアが発見されて以来 20 年近い年月を要している[39]。このような高度なマルウェアによるハッキングを、本法律の枠組で探知し得るのであろうか。疑問である。

更に、本法律は、外外通信についてまで、分析対象を「機械的情報」に限定しているが、殆どの外外通信の「通信の秘密」は日本国民の人権とは関係がないと見られる。日本国憲法が規定する「通信の秘密」は、日本国内或いは日本国民の人権を守る規定であり、世界の「通信の秘密」を守る規定ではない筈である[40]。外外通信に対する情報収集範囲の限定は、過剰な限定であろう。

以上は、将来の改正時の検討課題であろう。

なお、内々通信は本法律による収集分析の対象外であるが、本法律制定後は、当然、攻撃側は日本国内のサーバーを経由するなどして探知の回避措置をとるであろうから、近い将来、内々通信に関する情報収集の必要も認識されるであろう。

(2)「選別後通信情報」の使用目的の限定

このように「選別後通信情報」のデータ項目自体が限定的であるが、更にその使用目的も、被害防止目的に限定されている（強化法 23 条 2 項）。国会審議における政府答弁[41]によれば、本法律の目的は被害防止という行政目的であるので、「選別後通信情報」は犯罪捜査には使用しないとしている。これは、「選別後通信情報」の裁判証拠としての使用を認めないだけでなく、捜査資料として分析の対象とすること自体を否定していると考えられる[42]。しかし、この

---

[39] 米司法省、“Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia’s Federal Security Service,” *Justice News,* 9 May 2023.

[40] NSA による米国内での外外通信（米国 NSA のいう Transit 通信）の収集は、FISA（外国諜報監視法）に基づくのではなく、大統領命令第 12333 号に基づいて行われている。即ち、外外通信は、内々通信、外内通信、内外通信と同様の人権保障の対象ではないと考えられているのである。

[41] 衆議院内閣委員会、4 月 2 日平岡秀夫議員の質問に対する小柳内閣官房審議官答弁。「犯罪捜査とは、捜査機関が、犯罪があると思料するときに、事案の真相を明らかにし、刑罰法令を適用実現するため、犯人及び証拠を発見、収集、保全する手続を指すものでございまして、本法案で、通信情報を利用する目的である特定被害防止目的(一定の重大なサイバー攻撃による被害を防止する目的)とは明確に異なるものである…。したがいまして、選別後通信情報がアクセス・無害化のため警察庁等に提供された場合であっても、犯罪捜査目的が特定被害防止目的に含まれるとして選別後通信情報を利用することが認められるというようなことはな（い)」

また、参議院内閣委員会、2025 年 5 月 15 日木戸口英司議員に対する次の総理大臣答弁がある。「この法律の目的は、重要な電子計算機に対する不正な行為による被害の防止を図ること、つまり…サイバーセキュリティー対策に関するもので…、この目的の範囲を超えた利用は第 1 条に定めました法目的に反しますので、…許容されないと…考えておる…。この法目的に犯罪捜査目的が含まれることはなく、本法律案に基づく他目的利用により犯罪捜査のために通信情報を提供することも許容されない」。(参議院内閣委員会、2025 年 5 月 15 日木戸口英司議員に対する総理大臣答弁)

[42] 衆議院内閣委員会で 2025 年 4 月 2 日塩川鉄也議員の質問に対して警察庁サイバー警察局長は、次の答弁をしている。「選別後通信情報は意思疎通の本質的な内容を含まない機械的情報でありますから、そもそも刑事事件の証拠としてこれを利用することが必要となる場面は極めて限定的、例外的であろう」「仮に捜査に利用する場合には、令状を取得して選別後通信情報を差し押さえるなど、個別具体の状況に応じて、刑事訴訟法の規定に基づく厳格な手続にのっとって適切に対応することとなる」

解釈では、サイバー攻撃から国民の人権を守る上で支障が生じる上に、論理的にも疑問を抱かざるを得ない。

（ア）使用目的の限定により誰の人権を守るのか

そもそも、犯罪捜査には被害防止目的が内在している。逮捕起訴を含む犯罪捜査によって加害行為を鎮圧するのは、正に被害拡大防止を目的としている。また、刑事法学においては、刑罰や犯罪検挙の機能として「一般予防」（一般の人々に対する犯罪抑止効果）と「特別予防」（犯人に対する再犯防止効果）が挙げられており、サイバー犯罪捜査がサイバーセキュリティ、サイバー犯罪の被害防止に役立つのは常識であろう。

なぜ「選別後通信情報」を犯罪捜査に利用してはいけないのであろうか。そもそも、「選別後通信情報」には、国外の加害関係コンピュータとの通信の中でも（通常の通信の内容を含まない）通信メタデータとハッカー関連の指令情報などの機械的情報しか含まれない。一般国民のインターネット通信の内容は全く含まれないのである。そのような「選別後通信情報」を捜査に利用することによって侵害される人権とは、誰の人権であろうか。

某国の在京大使館のサイバーセキュリティ担当官から、本法律について説明を求められたことがある。「選別後通信情報」は捜査に利用しないという国会答弁があると説明したところ、「それは一般犯罪捜査には利用しないという意味ですね」と質問されたので、サイバー犯罪捜査にも利用しないという意味であると答えたところ、同担当官は絶句していた。

例えば、米国では、外国諜報監視法 FISA 第 702 条により、サイバーセキュリティという行政目的での通信情報収集（通信内容を含む）が広汎に認められており、これはサイバーセキュリティ対策上大きな貢献をしている。そして、FISA という国家安全保障の行政目的で収集した通信は、通信内容を含めて捜査に使用できるのである[43]。また、英国でも 2016 年調査権限法（IPA）によって収集した通信情報は、（通信内容を裁判の証拠として提出することは禁止されているものの）、通信内容と通信メタデータともに捜査に使用することができる[44]。

本答弁に関して、参議院内閣委員会では同年 5 月 15 日に石川大我議員が「情報を広く見ておいて…、それを裁判の証拠としたい場合には令状を取るんだというふうにも読めるんですけれども、そうなると、結局は情報を見て必要なものは令状で正しく取るとなると、これ違法収集証拠になるんじゃないか」と質問したのに対しては、警察庁サイバー警察局長は、「選別後通信情報を犯罪捜査に活用する場面は通常想定されない」「今御指摘があったような、事前に通信情報の内容を全て閲覧して、何といいますか、当たりを付けるとかいうことの御指摘ございましたけれども、警察が新法に規定する利用、提供の制限に反する取扱いをすることはございません。」と答弁をしている。

[43] 茂田ブログ、「サイバー安全保障・政府有識者会議の事務局資料の重大な誤り （行政通信傍受資料の捜査利用等に関して）」（2024 年 9 月 2 日）、https://shigetatadayoshi.com/2024/09/02/errors-in-reference-materials-of-a-government-advisory-board/.

--茂田「米国における行政傍受の法体系と解釈運用」（警察政策学会資料第 94 号、2017 年 6 月）、40 頁。同「スパイ防止に必要な制度と法律」（警察政策学会資料第 147 号、2026 年 5 月）30 頁、4-2（1）行政通信傍受、参照。

但し、行政通信傍受情報を裁判で使用するには、一定の手続が必要であり、FBI もパラレル・コンストラクションという手法を用いて、裁判での証拠使用は極力回避している。

[44] 英国 Investigatory Powers Act 2016。Section 20 により、通信傍受目的には、重罪（serious crime）の防止と探知が明記されており、これによって収集された情報は当然のことながら犯罪捜査に利用で

サイバーセキュリティ目的で収集した通信情報を、サイバー犯罪捜査に利用させないなどという法制の国が、一体、我が国以外で存在するのであろうか[45]。

結局、「選別後通信情報」の捜査利用禁止によって保護されるのは、一般国民の「通信の秘密」や、国民がサイバー攻撃の被害に遭わない安全な生活を営む権利ではなく、憲法の「通信の秘密」の理念と、国外ハッカーの犯罪遂行のための通信ではないか。犯罪捜査には使用しないとの解釈には疑問を抱かざるを得ない。

（イ）国際協力が成り立つのか

最近、サイバー攻撃の激化に対抗して、国際的に協力して対処する事例が増加している。国際共同捜査を行い、共同でパブリック・アトリビューションをしたり、参加国の一部が指名手配をしたり訴追したりするのである。著名な事例では、2024 年 7 月に発出されたサイバーセキュリティの国際アドバイザリーがある。これは、中国海南省国家安全庁傘下のハッカー集団 APT40 の脅威に対して、豪州が中心となって注意を喚起したものであるが、共同署名国には米英加ニュージーランドの UKUSA 加盟国に加えて、日本、韓国、ドイツも加わっており注目を集めた。このアドバイザリーはパブリック・アトリビューションの一種である。これより先 2021 年には、米国司法省が APT40 メンバー4 人を起訴すると共に、米英と EU 諸国は中国による国家支援のハッキングを公に非難している。

このように、サイバーセキュリティの国際協力においては、パブリック・アトリビューションや、起訴という犯罪捜査も総合して行うものである。しかし、我が国が「選別後通信情報」を犯罪捜査には使用できないという立場であるならば、強化法第 28 条（外国の政府等に対する選別後通信情報の提供）の規定の解釈としては、他国によって捜査情報として利用の可能性がある限り他国には提供できないこととなる。

そうなると、外国政府や国際機関に提供する際には、捜査には使用しないという確約を求めることになろう。しかし、米英初め多くの外国はそのような制限の論理を理解できないであろう。我が国の解釈で国際協力が成り立つのであろうか。

（ウ）アクセス・無害化措置の過程で得た情報も犯罪捜査に使用しない

国会審議における政府答弁[46]によれば、アクセス無害化措置の過程で得た情報の犯罪捜査での使用は想定していないという。米国司法省による起訴状などの資料を見ると、米国は正にハッカー集団のサーバーにアクセスしてハッカー集団を解明して、これに基づいて起訴していると推定できる。

我が国では、アクセス・無害化措置によって、脅威ハッカー集団のシステムにアクセスし

きる。但し、Section 56 によって、通信内容を裁判に証拠として提出して開示するのは禁止されている。これは、被告人の保護のためというよりは、インテリジェンス能力の秘匿や外国インテリジェンス機関との協力関係の維持が理由とされている。

[45] なお、我が国では、通信メタデータ（metadata, traffic data）も通信内容（content）も、「通信の秘密」対象として同一の保護を与えようとするが、英米では、両者は区別され、両者の保護水準は異なっている。

[46] 衆議院内閣委員会。4 月 4 日塩川鉄也議員の質問に対する警察庁サイバー警察局長答弁。

たとしても、その集団構成員を解明して起訴する意図はないと表明していることとなる。これも不可解である。

（エ）防衛出動時にも使用できないのか

更に、万が一、我が国が他国と交戦状態となり防衛出動が下令された場合には、「選別後通信情報」を、自衛隊部隊は強化法の枠組（アクセス・無害化措置）の中では使用できるが、武力の行使、即ち破壊的結果をもたらすサイバー攻撃のためには使用できないという解釈にならざるを得ないであろう。国家が、その生存を賭けて持てる資源を総動員して戦うべき時に、そのような使用目的の制限を付して、良いのであろうか[47]。

６　官民連携の課題

官民連携では、不正アクセス行為などのインシデント情報を、所管大臣と内閣総理大臣に報告する対象事業者が、16 業種の基幹インフラ事業者に限定されている。報告義務を負う事業者の範囲が狭過ぎるのではないかと危惧する声も聞くが、当初は限定されていても仕方がないと考える。2026 年 6 月には医療分野も対象事業者に加えれている。

むしろ本法律で気になるのは、基幹インフラ事業者が提出するインシデント情報の報告先である。以前から、所管官庁や個人情報保護委員会など、政府の報告先が幾つもあり、これでは煩雑であるので報告窓口を一本化してほしいという要請があったが、この法律は依然として、事業の所管官庁など複数の報告先があり、報告窓口の一本化が実現していない[48]。

その背景には、今回の強化法によっても、サイバーセキュリティの所管官庁が依然として一元化されていないことが挙げられる。即ち、内閣官房の国家サイバー統括室は創設されたものの、依然として事業所管官庁との二元体制が温存されているのである。事業所官官庁のサイバーセキュリティ担当者の講演を聞いても、省庁によってその専門性と取組内容に格差を感じる。

もっとも、国家サイバー統括室が真に一元的な所管官庁となるには、その専門能力や事務量など十分な力量の確保が課題であろう。UKUSA 諸国のうち米国以外の英加豪ニュージーランドがシギント機関の附置機関にサイバーセキュリティを所管させているのも、限られた専門人材を有効に活用しようという意図であろう。

７　政府の組織・体制の整備の課題

強化法及び整備法によって、2025 年 7 月に組織・体制の整備がなされた。次に簡単に整理

---

47 実務上は、自衛隊法第 88 条（防衛出動時の武力行使）の解釈で、「選別後通信情報」を武力行使のために使えると解釈するのであろうか。これは自衛隊法の現在の解釈体系から判断して、相当に苦しい解釈であろう。

48 国会審議では、報告様式の統一化を行い、煩雑さを軽減するとしている。

する。

(1) サイバーセキュリティ戦略本部の強化（整備法）

サイバーセキュリティ戦略本部が強化された。従来、本部長は官房長官であったが、総理大臣に格上げされ、全閣僚が本部員となった（改正サイバーセキュリティ基本法第 28 条、第 30 条）。また、「サイバーセキュリティ推進専門家会議」が新設された（第 30 条の 2）。副本部長は、サイバー安全保障担当大臣が就いている。

国家サイバー統括室のウェブサイト[49]を見ると、戦略本部は、2025 年 7 月発足時の会合を除いて、その後サイバーセキュリティ戦略を決定した第 2 回会合を含めて、2026 年 6 月の第 5 回会合まで全て持ち回り開催となっている。

他方、推進専門家会議は、2025 年 7 月以来、2026 年 6 月までに会合を 7 回開催している。また、戦略本部の下部組織として、サイバーセキュリティ戦略推進会議が発足している。サイバー安全保障担当大臣を議長、内閣サイバー官を議長代理として、関係行政機関の職員で構成するもので、実施会合は公表されていない。実質的な政府全体の体制としては、戦略推進会議と推進専門家会議が中心となって機能していくのであろう。

(2) サイバー通信情報監理委員会の新設（強化法第 10 章、改正内閣府設置法第 4 条、第 64 条）

2026 年 4 月に内閣府内に発足した。委員は 5 人で、委員長は元裁判官、委員 2 人は学者と弁護士で委員 2 人が技術の知見を有する者からなっている[50]。

(3) 内閣サイバー官と国家サイバー統括室の設置（整備法）

内閣サイバー官が新設されると共に（改正内閣法第 19 条の 2）、従来の「内閣サイバーセキュリティセンター（NISC）」（2015 年発足）が改組され、「国家サイバー統括室」（National Cybersecurity Office）」が設置された（内閣官房組織令第 4 条の 2）[51]。

国家サイバー統括室の態勢は令和 8 年度の定員は 262 人で、同室のウェブサイト[52]によれば、室長が内閣サイバー官（国家安全保障局次長を兼務）で、その下に、統括官 3 人、審議官 5 人、6 つのユニットが置かれている。組織編成は次の通りである。

① 総括・戦略担当統括官（ユニット担当の審議官が 3 人）

- 総括・戦略ユニット ～ 総合調整、CS 戦略の立案・調整
- 制度・監督ユニット ～ 情報セキュリティ対策の統一的基準の策定・運用・監督
- 国際戦略ユニット ～ 海外サイバー当局との連携

---

[49] https://www.cyber.go.jp/council/index.html#council-cs。 2026 年 4 月 29 日最終閲覧。

[50] ttps://www.sangiin.go.jp/japanese/joho1/kousei/gian/221/meisai/m221400221004.htm

[51] https://www.cyber.go.jp/about/index.html。2026 年 4 月 29 日最終閲覧。

[52] https://www.cyber.go.jp/about/index.html。2026 年 4 月 29 日最終閲覧。

② 対外調整・官民連携担当統括官

・ 対外調整・官民連携等ユニット ～ 政府関係機関の CS の監視や事案発生時の対処、官民連携枠組等を通じた情報収集、情報提供、支援

③ 能動的サイバー防御・サイバー情報担当統括官（ユニット担当審議官 2 名）

・ 能動的サイバー防御運用総括ユニット ～ 能動的サイバー防御の運用に関する企画及び立案

・ サイバー情報ユニット ～ サイバー攻撃等に係る情報の収集・分析、サイバー情報の共有

（4）課題

体制的には整備されたようであるが、課題は、同室が真の専門家集団となる人事をどのように構築していくかであろう。改組前の NISC の職員は、生抜き職員がずっといるわけではなく、多くの官庁からの 2 年間程度の出向者や 1 年から数年の任期制職員が大多数を占めていたと見られる。そこで、真の専門家集団になるような人事をどのように構築して行くのかという課題がある。

米国を除く UKUSA 諸国ではサイバーセキュリティの主管官庁として国家サイバーセキュリティセンターをシギント機関に附置しているが、シギント機関の専門的知見やインフラの他、専門人材の支援が見込めるからであろう。しかし、我が国にはこの条件が存在しない。

日本の公務員の人事制度は、一つの役職の任期が短いため、どうしても専門性が高まらず、また、知識経験の蓄積が不十分な傾向にある。強化されたとはいっても、国家サイバー統括室の規模は未だに小さく、プロパー職員集団の構築もなかなか容易ではない。少なくとも、出向者については、勤務期間を最低 4 年間とし、内閣サイバー官や統括官は内部昇格人事を基本とする、最低限、国家サイバー統括室の勤務経験者とするなど、知識経験の蓄積ができる人事とする必要があろう。人事の課題に正面から取り組む必要があろう。

８ 最後に

以上論じたように、今回の「サイバー対処能力強化法及び同整備法」は、多くの課題を残す法律であり、これで欧米水準のサイバー対応能力が構築できるとは到底言えない。

しかしそれでも、本法律は、我が国のサイバーセキュリティ対策において大きな前進である。残された課題は、制定後の運用実績を見て改正を重ねていけば良いのであり、そうしてこそ本法律の意義が大きなものとなろう。

ところで、課題を残す法律制定の背景には、我が国における人権の理解の在り方が横たわっている。一部の学識者は憲法が保障する「通信の秘密」と国家権力を対置して、「通信の秘密」という人権を必死で守ろうとする。

しかし、サイバー空間に国境はない。国内も国外からの脅威に常時晒されているのである。そして、現代社会のサイバーセキュリティは、国民の豊かで安全で自由な生活を確保するた

め不可欠な社会基盤である。即ち、外国インテリジェンス機関がサイバー空間を通して、我が国の機密情報を容易に窃取し、情報工作によって世論を分断できるようでは、外交の場で不利益を被るのみならず、我が国の国家体制の弱体化や民主政治に混乱が生じ、引いては、国民の人権を守るべき国家の枠組自体が危うくなる。また、サイバー攻撃によって基幹インフラ企業が機能不全に陥れば、国民生活に直接的な被害が生じる。更に、企業に対するハッキングによって、優れた先端科学技術や企業秘密が流出し続ければ、民間企業の競争力が低下して、国民生活が貧困化してしまう。或いは、ランサムウェア攻撃やインターネット詐欺などのサイバー犯罪が横行し適切に取り締まれなければ、国民生活が犯罪の脅威に晒される。つまり、サイバーセキュリティとは、豊かで安全で自由な国民生活という人権を守るための重要な社会基盤なのである。

一方、「通信の秘密」も大切な人権であるが、この理念を教条的に掲げれば、それは、犯罪のための通信の秘密の擁護に陥ってしまうこととなる。本法律の「選別後通信情報」の扱いにそれが現れている。

「通信の秘密」という人権も、サイバーセキュリティによって守られるべき国民の豊かで安全で自由な生活も、共に重要な人権である。従って、この両者の人権を守るためには、サイバーセキュリティ確保のための各種の施策が、どのような状況でどのように「通信の秘密」を侵害する虞があるのか、それは豊かで安全で自由な国民生活を守るために許容できる範囲のものなのかを、具体的に検討する必要がある。

そうなれば、「通信の秘密」を教条的に掲げた不毛な議論も終りを告げるであろう。

（以上）

大川原化工機国賠事件・控訴審判決と
警視庁の検証報告書を読む

茂田　忠良

<目次>

はじめに

「大川原化工機株式会社」（横浜市）は、乾燥噴霧器（スプレードライヤー）を 2016 年と 2018 年にそれぞれ中国と韓国に輸出した。本件輸出について、警視庁公安部は、生物兵器製造に転用可能な装置を無許可で輸出した外為法違反事件（即ち、大量破壊兵器等に関する不正輸出事件）として、2020 年 3 月以降に社長ら 3 人を逮捕し、続いて東京地検が起訴した。しかし 2021 年 7 月に至って、東京地検は本件輸出品が規制対象に当たるか疑義が生じたとして、起訴を取り消した。

これに対して、大川原化工機や関係者が 2021 年 9 月に、警視庁公安部や東京地検による逮捕、取調、勾留請求、及び起訴に至る一連の行為は違法であったとして、国や都を相手に国家賠償を求めて提訴した。本国家賠償請求訴訟において、東京地裁は 2023 年 12 月に国や都による各種の違法行為を認定し、総額約 1 億 6200 万円の損害賠償を命じた。これに対しては原告被告両者が控訴し、東京高裁は 2025 年 5 月に控訴審判決を下した。本控訴審判決[1]は、事実認定において一審判決よりも都や国に対してより厳しいものとなり、総額 1 億 6600 万円の損害賠償を命じた。

国家賠償訴訟における敗訴を受けて、警視庁は、検証チームを設置して、警察捜査の問題点と再発防止策をとりまとめ、2025 年 8 月に検証報告書[2]を公表した。

本論考は、本件公安部捜査の問題点とその背景に潜む課題について論究するものである（東京地検の行為については論究の対象としていない）。先ず、本控訴審判決が認定した事実関係

---

1 東京高等裁判所令和 7 年 5 月 28 日判決（令和 6 年（ネ）第 453 号）。

2 警視庁、「国家賠償請求訴訟判決を受けた警察捜査の問題点と再発防止策について」2025 年 8 月 7 日。（以下、検証報告書）

を基に、警視庁公安部の捜査の問題点・違法性を明らかにする（第 1 章、第 2 章）。次に、警視庁の検証報告書を基に、いわば現場の暴走による違法捜査を許してしまった警視庁公安部の捜査管理の問題点を明らかにする（第 3 章）。次に、以上を前提として、より広い視点から、本事件捜査の本質的な問題点（第 4 章）、そして、本事案を通じて浮かび上がった我が国の現行法制度やその運用に潜む課題（第 5 章）について論ずる。

1　社長 O 氏、営業担当取締役 S 氏、技術顧問 A 氏逮捕の違法性

外為法 48 条 1 項に基づく輸出貿易管理令によって輸出規制対象とされた「噴霧乾燥機」は、更に経済産業省令が 3 つの要件を定めている。本事案の焦点は、大川原化工機が中国や韓国に輸出した噴霧乾燥機が経産省令が定めた要件に該当するか否かであった。

この点について本控訴審判決は、通常要求される追加捜査も行わずに、経産省令の定めた要件について合理性を欠く解釈に基づいて、O 氏、S 氏、A 氏 3 名を逮捕したと認定して、「犯罪の嫌疑の成立に係る判断に基本的な問題があった」[3]違法な逮捕である批判している。具体的には次の 2 つの問題点を指摘している。

(1) 最低温箇所の特定に係る捜査の問題[4]

外為法に基づく輸出貿易管理令によって輸出規制対象とされた「噴霧乾燥機」の要件について、経産省令による要件は「定置した状態で内部の滅菌又は殺菌をすることができるもの」と定めている。この解釈について、警視庁公安部は、「空焚き」による乾熱殺菌によって省令に規定された大腸菌やペスト菌などの細菌の 1 種類でも全て死滅できれば「殺菌」の要件に該当するとしていた（以下「公安部解釈」）。

仮にこの公安部解釈によるとした場合でも、「空焚き」によって「殺菌」要件に該当すると言うためには、噴霧乾燥器内部が全て一定の温度以上になることが必要であり、従って噴霧乾燥機内部の最低温箇所を特定して、当該場所の温度を測定する必要があった。警視庁公安部は独自に最低温箇所を特定して温度測定実験を行ったが、これに対して、大川原化工機の A 技術顧問や他の社員が最低温箇所は他にあると再三指摘しており、その情報は捜査指揮に当たる M 警部にまで報告され公安部内で情報共有されていた[5]。

従って、最低温箇所に関する追加捜査を実施していれば、噴霧乾燥器内に温度が上がらない場所があり、「殺菌」要件に該当しないことが明らかになったにもかかわらず、公安部は追加捜査をしなかったと、控訴審判決は厳しく批判している。

---

[3] 判決本文 94 頁。
[4] 判決本文 70～75 頁。
[5] 判決要旨 5～6 頁、判決本文 72 頁。

（2）合理性を欠く法令解釈（経産省令の要件）[6]

次に、控訴審判決は、輸出規制対象とされた「噴霧乾燥機」の「殺菌」要件についての公安部解釈自体の正当性を否定している。即ち、警視庁公安部は、「空焚き」によって省令に規定された細菌の 1 種類でも全て死滅できれば「殺菌」の要件に該当すると解釈していたのであるが、これを否定しているのである。

経産省令による要件「定置した状態で内部の滅菌又は殺菌をすることができるもの」について、「滅菌」については、日本薬局方に滅菌法の定義があるところ、本件乾燥噴霧器は到底その要件を満たせるものではなかった。他方「殺菌」については定義が曖昧であったため、警視庁公安部としては、経産省令に規定された細菌の 1 種類でも全て死滅できれば「殺菌」の要件に該当する、且つ、「空焚き」による乾熱殺菌も「殺菌」方法に含まれると、「殺菌」の要件を「滅菌」の要件と比べて緩く解釈したのである。

これに対して、本控訴審判決は、日本薬局方で規定する「滅菌法」の 1 つの乾熱法は要件が極めて厳しいことを指摘した上で、後述する国際的な AG 合意などの経緯から、「殺菌」とは、殺菌効果のある化学物質の使用を通じて微生物の感染能力を破壊することを意味し、空焚き等の物理的な方法による破壊は含まない。また「殺菌」は「滅菌」と併記され同様の概念であるから、「殺菌」も「滅菌」同様に、全ての微生物を死滅させ得ることが要件であって、1 種類の微生物の死滅で足りることにはならないと指摘[7]して、警視庁公安部による「殺菌」要件の解釈を否定した。

更に控訴審判決は、警視庁公安部による法令解釈に対しては、経産省の担当課からその問題点の指摘を受けながら、解釈の合理性について再考しなかったと批判している[8]。

２　営業担当取締役 S 氏に対する違法な取調と弁録作成

本事案では、外為法違反が成立するためには、当該乾燥噴霧器が輸出規制対象であることを知りながら無許可で輸出されたことを立証する必要があった。そのために、公安部の取調官であった A 警部補は、S 営業担当取締役から、その事情を認識し容認していた旨の供述を引き出そうとした。控訴審判決はその A 警部補の取調を「偽計的」として厳しく批判している。控訴審判決が指摘した事実は次の二つである。

（1）「偽計的」な任意取調の違法性

S 取締役は、2018 年 12 月から 2020 年 2 月の間に 39 回にもわたって任意取調べを受けている。この間 A 警部補は、犯意を繰り返し否定する S 取締役に対して、熱風で殺菌できることを知りながら、技術担当顧問 A 氏の判定に従って、会社として輸出規制対象「非該当」と判断したこと、本件乾燥噴霧器が輸出規制対象である「殺菌」性能を有していること、など

---

[6] 判決本文 75～93 頁。
[7] 判決本文 82～84 頁。
[8] 判決要旨 8 頁。判決本文 86～94 頁。

を認める供述調書に署名私印するように仕向けていた。その際A警部補は、外為法違反成立のポイントとなる「殺菌」要件の解釈について、警視庁公安部自体は「装置内の特定又は不特定多数の病原菌等有害な菌を全て死滅させること」と解釈していた[9]にもかかわらず、S取締役にはこれを伝えず、「熱風によって装置内部の細菌が一部でも死滅すれば『殺菌』に当たる」と誤解させて[10]、S取締役に対して、本件乾燥噴霧器の「殺菌」機能そして犯罪事実を認めるかのような供述内容を誘導したと、控訴審判決は厳しく批判している[11]。

このような任意取調は、真実を解明するというよりは、犯罪の構成要件に合致する供述を「偽計的」に引き出そうとするものであり、到底許容されるものではない。

(2)「偽計的」な弁解録取書作成の違法性

2020年3月に外為法違反でS取締役が逮捕された際に作成された弁解録取書において、S取締役が「(CISTEC作成の)ガイダンスに従って、許可の申請の要らないものと考え輸出した」と記載するように求めた(註:これは外為法違反の故意を否定する供述である)。これに対して、A警部補は同趣旨の記載に同意しながら、実際の弁解録取書には「社長らと共謀して無許可で輸出した」旨の記載をして一旦S取締役に署名私印させている。その後S取締役が、弁解録取書の勝手な修正に気が付いて抗議したため、当該部分を削除した弁解録取書を再度作成した[12]。

勝手な修正にS取締役が気付かなければ、本人の意思と異なる弁解録取書がそのまま証拠化されていたこととなる。控訴審判決は、この弁解録取書の作成を「偽計的」であると批判している[13]。

3　公安部の捜査指揮系統の機能不全[14]

以上、本件控訴審判決によれば、警視庁公安部は、外為法よって輸出規制対象とされた「噴霧乾燥機」の要件について合理性を欠く法令解釈(公安部解釈)に基づき捜査を行い、且つ、公安部解釈に則っても必要な「噴霧乾燥器」内の最低温箇所について捜査を尽くさずに、社長O氏、営業担当取締役S氏、技術顧問A氏を逮捕し、また、A警部補は取締役S氏に対する取調と弁解録取書作成に当たって違法な行為を行った。

それでは、このような違法捜査が行われた背景と原因はどこにあったのか、警視庁の検証報告書によって見ていこう。

---

9 判決本文101頁。
10 判決本文102頁。
11 判決要旨9頁、判決本文95～106頁。
12 判決要旨9頁、判決本文106～112頁。
13 判決要旨9頁、判決本文112頁。
14 検証報告書26頁

（1）公安部の捜査指揮系統の機能不全

警視庁検証報告書によれば、そもそも控訴審判決が指摘した違法な捜査が行われた原因は、「（外事 l 課）第 5 係長（M 警部）が検挙を第一に考えて自身の捜査方針にそぐわない捜査上の消極要素に対し十分な注意を払うことなく捜査を進めていた」。そして「（同人を監督すべき）担当管理官は第 5 係長の捜査方針に賛同し、同人に捜査指揮上の判断を任せていた状況」[15]があったという。現場の捜査員からは捜査方針に疑問を呈する意見もあったが、2 人は取り合わず消極要素に十分な注意を払わなかったという[16]。つまり、担当管理官と M 警部が検挙第一で暴走したということである。

現場の捜査担当者が暴走することは（好ましいことではないが）起こり得ることである。本事案の最大の問題は、これを指揮監督して是正すべき上司の指揮監督が機能していなかったことである。検証報告書によれば、本事件は、2018 年 8 月に公安部長指揮事件に指定されると共に、M 警部が捜査主任官に指名された。従って、公安部長や外事第 l 課長が指揮監督すべき事件であり、この指揮監督が適正に行われていれば、違法な捜査は行われなかった筈である。

先ず、直近上司の外事第 l 課長（逮捕起訴時の課長）については、（第 l 章で既述した）最低温箇所の特定に関する捜査の問題[17]や経産省令で定める要件についての合理性を欠く法令解釈など、捜査の消極要素について認識していなかったという[18]。また、「逮捕に至る本件捜査の重要な場面において、主体的に捜査方針の検討に参画した状況が認められなかった」[19]。更に、「公安部長等四役[20]に適時・適切な報告がなされるよう、部下職員を十分に指揮監督していなかった」[21]。端的に言えば、課長としての職責を果たしていなかったのである。

それでは、公安部長以下の公安部最高幹部による指揮監督の状況についてであるが、「公安部長等四役への報告・指揮伺いが形骸化して」いたという[22]。「消極要素となり得る情報が、外事第 l 課から公安部長等四役にほとんど報告されず、…報告は、単に捜査の大まかな概要や予定を伝えるだけの形骸化したものとなっていた」[23]。従って、公安部長等四役は、消極要素の報告を受けていず、認識もしていなかったという[24]。更に「四役も自ら積極的に捜査上の消極要素等を明らかにして慎重に検討し、必要に応じて捜査方針を再考させるべきであった

---

15 前掲。
16 検証報告書 23 頁。
17 検証報告書 16 頁。
18 検証報告書 18 頁。
19 検証報告書 24 頁。
20 公安部四役とは、公安部長、同部長を補佐する参事官 2 名と公安総務課長の 4 人をいう。検証報告書 7 頁。
21 検証報告書 26 頁。
22 前掲。
23 検証報告書 19 頁。
24 前掲。

が、これを怠り、実質的に捜査指揮をしていない状況であった」[25]。つまり、公安部の最高幹部については、報告・指揮伺いが形骸化し、実質的に捜査指揮をしていない状況であったとされる。

(2) 再発防止策

検証報告書は、このような捜査の問題点を明らかにした上で、再発防止策を記述している。本違法捜査の、主たる原因が公安部最高幹部による捜査指揮が形骸化していたことであるので、従って、最も重要な改善策・再発防止策は、捜査の管理監督機能の強化であり、その趣旨に添った改善策が提示されている。

主な取組としては、部長捜査会議制度（公安部長、参事官、公安総務課長、事件主管課長、捜査主任官等が参加）の導入。公安捜査監督指導室を新設して指導室長が部長捜査会議に同席するなどして、公安部長以下の公安部幹部による捜査指揮の実質化を図る。また、担当課長の実質的な捜査指揮を担保するために、捜査会議の運営に関するガイドラインを策定して、担当課長が捜査会議に定期的に参加して捜査員から意見を聞いたり、主要な捜査書類を確認したりする機会を設けることとしている。これらの改善策の方向性は適切と評価できよう。

(3) 残る疑問

本検証報告書は、公安部最高幹部への報告・指揮伺いが形骸化して最高幹部による事件指揮が実質的に不存在であったと述べているが、残る疑問が一つある。それは第 1 に、本事件は公安部長指揮事件であったということである。第 2 に、本事件のような大量破壊兵器等に関する不正輸出事件は、公安部でも数年に 1 件[26]という稀な事件であり、極めて重要な事件であった筈である。第 3 に、本事件は被疑者が犯罪を否認している否認事件であった。そして、検証報告書によれば、本事件では捜索差押（2018 年 10 月）から逮捕起訴（2020 年 3 月以降）までの間に、主要関係者の供述要旨が公安部長等四役に対して計 8 回報告されているのである[27]。8 回に亘る報告では、当然のことながら否認事件であることは報告されていた筈である。報告されていれば、なぜ被疑者が否認しているのかという否認事由とこれに対する捜査側の反証が議論される筈であり、そうなれば、第 1 章で既述したような公安部解釈の問題点や最低温箇所の特定の問題点が浮かび上がってきたのではないだろうか。実に不可思議である。

4　そもそも事件化する必要性のない事案であった

警視庁公安部の捜査の問題点についての控訴審判決及び警視庁の検証報告書の指摘事項は以上である。ところで、控訴審判決では指摘されず、検証報告書でも婉曲な言及にとどまっ

---

[25] 検証報告書 26 頁。
[26] 検証報告書 22 頁。
[27] 検証報告書 39-40 頁。

ているが、本件捜査の基本的且つ本質的問題は、そもそも事件化する必要のない事案を有罪判決の獲得を目指して事件化したことにあるのではないだろうか。

そもそも「乾燥噴霧器」の輸出規制の端緒となったのは AG 合意である。AG（オーストラリア・グループ）は生物化学兵器の拡散防止を目的とする国際輸出規制レジーム[28]で、2012 年に乾燥噴霧器を規制対象に追加した。そして、米英など主要国では、輸出規制対象となる「滅菌又は殺菌をすることができる」乾燥噴霧器とは、CIP（薬液による自動洗浄）機能付き、蒸気による滅菌機能付きのものと取り扱われていた。大川原化工機においても、規制対象はこのような滅菌・殺菌機能を付加した乾燥噴霧器を指すものと解釈しており、問題となった（滅菌殺菌機能を特に付加していない）噴霧乾燥機については輸出許可を申請せずに輸出していた。実際、同種の噴霧乾燥機の輸出に当たって、許可申請をした実例は、藤崎電機という会社が念のために申請した 1 件のみであり、その他の企業は許可申請をしていなかったという[29]。

また、要件「滅菌又は殺菌をすることができる」については、「滅菌」については、日本薬局方に滅菌法の定義があるところ、その要件は高度であり本件噴霧器は到底その要件を満たせるものではなかった。他方、「殺菌」については定義が曖昧であり、経産省から関係業者に対して「殺菌」には本事案で問題とされた「空焚き」による乾熱殺菌が含まれるという行政指導がされた事実も伺われないのである[30]。

このような事情であるから、大川原化工機において、輸出許可を要しないと判断したことには相当の理由があり、本来、輸出許可が必要なものを脱法的に無許可で輸出しようという意図がないことは明白であった。そして、この事情は、度重なる任意取調において警視庁公安部の担当者も十分覚知し得た筈のものである。

更に、大河原化工機が中国に輸出した乾燥噴霧器も、申請していれば許可が受けられたものであったという[31]。（註：判決文には、韓国向け輸出品については、申請すれば許可が受けられたものか否かについての言及はないが、中国向け同様許可が受けられたものであったと見られる）。

このような一連の経緯から判断すれば、仮に結果的に「空焚き」による乾熱殺菌が輸出規制の対象要件に含まれ得たとしても、大河原化工機の担当者に外為法違反の無許可輸出の犯意がないのは明白であり、行為に悪質性がないことも明白であった。従って、本事案においては、経産省において要件の解釈を明確化して関係業者に徹底し、今後の注意を促せば十分な事案であり、とても事件化すべきであった事案とは考えられない。つまり、大局を俯瞰することができる警視庁公安部の幹部が、捜査の実態を把握して、常識に則って判断していれ

---

28 安全保障に係る国際輸出規制レジームには、オーストラリア・グループ（AG）の他、原子力関連資機材・技術に関する「原子力供給国グループ（NSG）」、ミサイル関連資機材・技術に関する「ミサイル技術管理レジーム（MTCR）」、通常兵器関連の「ワッセナー・アレンジメント（WA）」がある。

29 判決本文 93 頁。

30 前掲。

31 判決本文 119 頁。

ば、事件化は避けられた筈の事案であった[32]。

そもそも事件化する必要のない事案を事件化しようとしたために、控訴審判決が指摘した逮捕の違法性、取調の違法性という問題が生じたと考えられる。

５　背景に潜む課題

以上、大川原化工機国賠事件の控訴審判決、警視庁の検証報告書を基に、公安部捜査の問題点を見てきたが、本件捜査に極めて問題があったのは明らかであり、警視庁は再発防止策を講じると共に、報道によれば関係者を処分している[33]。

そこで、視点を変えて、本件事案の背景に潜む、我が国の刑事司法制度と国家安全保障に係わる事案の抑止対策の課題と問題点を指摘しておきたい。

(1)「故意」（内心の意思）偏重、自白偏重の刑事司法

本事案で外為法違反の不正輸出が成立するためには、輸出規制対象の物品を無許可で輸出した事実の立証では不十分で、輸出規制対象物品であることを認識した上で無許可輸出をしたことを立証する必要があった。そこで、A 警部補は、S 営業担当取締役からその旨の供述を引き出そうとして、任意取調 39 回という取調偏重の捜査を行い、「詐術的」な取調や弁解録取書の作成にまで至ったのである。

しかし、そもそもこのように内心の意思を偏重する刑事司法は、好ましいものなのであろうか。我が国の「故意」偏重の刑事司法制度が、自白偏重、取調偏重の捜査を誘発しているのではないだろうか。外為法違反の立法論としては、重過失によって輸出規制対象物品であることを認識せずに輸出した場合も可罰的と規定するべきであろう[34]。そうなれば、所管省が輸出規制対象物品を明確に規定して、且つ関係業者がその情報を容易に知り得る状態に置いて

---

32 これらの論点に関連して、検証報告書 25 頁には、「犯罪構成要件該当性に関する国民の予測可能性との関係において、立件に向けて捜査を継続することが妥当かどうかについても慎重に検討すべきであった。」「当初から刑事事件として立件することを目指すのではなく、捜査の対象とした違法行為について高度の悪質性が存在するかが検討されるべきであった。」「悪質性が高いと言えない事案であれば、所管省庁に対し行政指導等の行政措置の発動を促すことも選択選択肢として検討する必要があると考えられる。」という記述があるが、これは本文に記載した筆者の見解と一致するものと考えられる。

33 報道に拠れば、処分対象（退職者に対する処分「相当」認定を含む）は 19 人。懲戒処分は、W 管理官（退職）と M 警部（退職）の 2 人で、減給 100 分の 10（1 ヵ月）。残りの 17 人は監督上の措置で、訓戒が 3 人、逮捕時の公安部長（退職）、逮捕時の外事第 1 課長（退職）、S 取締役の取締官 A 警部補。注意が 3 人、逮捕時の公安部参事官、捜査開始時と捜索差押時の外事第 1 課長 2 人（共に退職）。この他に捜査初期の公安部長、参事官ら 11 人（内、退職者 4 人）が口頭厳重注意や業務指導とされた。例えば、「捜査指揮、機能不全　大川原冤罪、警視総監謝罪　元公安部長ら 19 人『処分』　検証報告」『毎日新聞』2025 年 8 月 8 日付朝刊、1 面参照。この他、同日の主要各紙でも同様の報道がなされている。

34 米国の立法例を見ると、例えば、国防情報漏洩罪（合衆国法典 18 篇 793 条）では、重過失による漏洩も故意犯と同様に扱っている。漏洩する積りはなかったという「故意」の否定による抗弁を封じているのである。このように「故意」という内心の意思に関わりない犯罪構成要件の立て方を工夫すべきであろう。

いれば、仮に個別の担当者が輸出規制対象であることを認識していなかったと主張しても、認識しなかったことに重過失があると認定できるので、無理な取調を生む素地もなくなるであろう。（なお、本事件は、そもそも輸出規制対象物品であるか否かが明確に定められておらず、警視庁の公安部解釈を関係業者は事前に知り得る状態になかったのであるから、そもそも事件化することに無理があった事案である。）

本事件では、「故意」の立証にエネルギーを注ぎ過ぎて、許可申請が必要な輸出規制対象製品か否かという、最も重要且つ基本的な命題についての捜査立証が疎かにされてしまったようにみえる。

更に、「故意」偏重の刑事司法は他にも好ましくない副産物を生んでいる。警察が検察に送致した事件の起訴率が激減しているのである。検察統計によって 2000 年と 2023 年との罪名別の起訴率を比較すると、総起訴率は 53.9%から 32.0%へと減少しており、これ自体大きな問題であるが、特に殺人未遂を含む殺人罪の起訴率は、61.2%から 27.4%へと半分以下に激減しているのである[35]。この背景を考えると、殺人の故意の立証に自信が持てないために、殺人罪で送致を受けても傷害致死罪で、殺人未遂罪で送致を受けても傷害罪で起訴する事例が増加しているのではないだろうか。我が国では、殺人罪には殺人の「故意」が必要とされているために、外形的には全く同様な「殺人」行為でも、犯人の内心の意思の立証度合によって、殺人罪になったり傷害致死罪になったりしてしまう可能性がある。これに対して、米国では、殺人の故意の立証は、殺人罪（murder）成立の必須要件ではなく、犯人に極度の無謀性（extreme recklessness）や悪意（malice）が見られれば、殺人罪が成立する。つまり、普通の人が見て殺人だと考える行為は、殺人罪で処罰されるのである。普通の人の感覚に添った常識的な刑事司法である。我が国でも、外形的に普通の人が「殺人」と考える行為は、その外形的な状況から殺人の故意を「推認する」べきであろう。我が国も、「故意」偏重を反省する必要があるのではないだろうか。

漏れ聞くところでは、事件担当検事もつい「故意の供述」は取れていますかと、刑事に訊ねることが多いそうであるが、法曹関係者全体の意識改革が必要ではないだろうか。

（2）国家安全保障に係わる事案の取締りの課題

本外為法違反の不正輸出事件では強引で無理な事件化が見られたが、なぜ、強引で無理な事件化が行われたのであろうか。警視庁の検証報告書は、その主因として、担当警部と担当管理官の検挙第一による暴走と公安部最高幹部による捜査指揮の形骸化を挙げているが、筆者は、背景原因の一つに事件化への渇望と焦りがあったのではないかと考える。

そもそも、我が国では、国家安全保障に係わる事件の検挙は極めて少ない。国家安全保障に係わる事件とは、スパイ、テロ、国家転覆、大量破壊兵器拡散など国家の安全保障に係わ

[35] 検察統計「被疑事件の罪名別起訴人員、不起訴人員及び起訴率の累年比較」2023 年、https://www.e-stat.go.jp/dbview?sid=0003274052

る事件であり、本件で問題となった生物兵器製造に転用可能な物品の不正輸出や先端技術の窃取・流出なども含まれる。正に国家の安全を脅かす重大な事件であり、各国ともこの種の事件の防止摘発に力をいれている。

ところで、国家安全保障に係わる事件の検挙件数を見ると、例えば、米国においては FBI 国家安全保障部門による先端技術窃取などの検挙件数は、平均して年間約 30 件以上に及んでいる[36]。また、韓国においては産業技術の対外流出の摘発件数だけでも毎年約 20 件に及んでいる[37]。これに対して、警視庁公安部による大量破壊兵器等に関する不正輸出事件の検挙件数は、既述の通り数年に 1 件程度[38]であり、これにスパイ、テロその他を加えた、国家の安全保障に係わる事件の総検挙件数を見ても、警察庁の広報資料を見る限り、年間ゼロ件ないし 1、2 件というところではないであろうか。一方、我が国における検挙件数が少ないからと言って、機微な産業技術の流出や不正輸出が、我が国では米韓両国と比べて格段に少ないということはあり得ない。つまり、多くの事案が探知検挙できないままに放置されていると考えて間違いないのである。このような状況の下で、国家安全保障に係わる事件を検挙するために強引な捜査が生じてしまうのではないだろうか。

しかしながら、米国と我が国で検挙件数に大差が生じる原因は、我が国の公安捜査員の能力や努力に問題があるためではなく、取締りに関する法制度に大きな違いがあるためである。つまり、米国 FBI は、極めて広範な情報収集権限を付与されているほか、広汎な罰則規定があり、また、司法制度の運用も取締りがし易い運用となっている。例えば広義の通信傍受だけを見ても、通信回線の傍受の他、IT 企業のデータセンターにおける収集、容疑者のスマートフォンのハッキングなどの権限まで認められており、その権限行使の要件は緩やかである。容疑者によるグーグル検索やグーグルマップ検索など各種のウェブの検索履歴の把握やスマートフォンの位置情報の把握も容易である。更には、秘密捜索や秘密裡の会話傍受設備の設置も認められている。

米国の国家安全保障に係わる事件の起訴状や FBI 捜査官による宣誓供述書などは詳細であり、FBI による調査・捜査手法が概ね推定できるが、そこでは、広汎な調査・捜査権限によって客観的な証拠を収集して事件化している姿が見て取れる。強引な取調による故意の立証などは見られないし、そもそも強引な取調をする必要がないのである。

このような制度的違いについての議論を回避して、既存の限定された刑事司法制度の中で対処し続けようとすれば、国家安全保障に係わる事件の取締りは殆ど望めないこととなり、「スパイ天国」と言われる我が国の現状は何も変わらないであろう。そうなると、目に見え

---

36 宇生航「米司法省報道発表“Justice News”から見た先端技術窃取をはじめとする懸念国有害活動の摘発傾向と我が国の経済安全保障上の諸取組への含意」『警察政策』第 26 巻（2024 年）211-216 頁。本研究で集計対象とされたのは、先端技術窃取、不正輸出、カウンターインテリジェンスの 3 種の類型の摘発件数であり、国際テロなどは含まれてていない。

37 流出対策委員会「韓国における対中国技術流出事案の特徴」『治安フォーラム』2025 年 1 月号、21-32 頁。

38 検証報告書 22 頁。

ないところで、日々国益が侵害され続け、平穏で豊かな生活を享受するという国民の人権も侵害され続けるのである。

国家安全保障に係わる事件に関する FBI による調査や捜査の具体的手法については、既に、筆者の様々な論文や論考で明らかにしている[39]。我が国でも、国家安全保障に係わる事案の取締りについては、理念的な憲法解釈に留まることなく、米欧の法律制度の実態を真摯に研究した上で、国民の人権を守りつつ、実効性ある取締りが可能な法制の構築が望まれる。

終りに

以上、大川原化工機国賠事件の控訴審判決と警視庁の検証報告書を基に、警視庁公安部による捜査の問題点、そして、その背景に潜む課題を見てきた。

警視庁公安部の捜査について、控訴審判決が具体的に論究しているのは、①社長 O 氏、営業担当取締役 S 氏、技術顧問 A 氏逮捕の違法性と、②営業担当取締役 S 氏に対する違法な取調と弁録作成の 2 点であるが、本事件はそもそも事件化する必要のない事案であり、警視庁の検証報告書が指摘する通り、公安部最高幹部の指揮監督に問題があったと言える。

更に、本事案の背景として、我が国の法律制度の構築運用に内在する課題を 2 点提起した。先ず第 1 に、我が国の刑事司法の在り方の課題、即ち「故意」（内心の意思）の立証偏重が自白偏重の刑事司法を生み、普通の人の感覚から遊離した刑事司法の運用を生み出しているのではないか、という点である。第 2 に、国家安全保障に係わる取締りの法律制度の在り方である。例えば米国では、FBI が極めて広範な情報収集権限を付与されているほか、広汎な罰則規定があり、また、司法制度の運用も取締りがし易い運用となっていることを指摘した。今後、このような法律制度の構築運用の問題について、論議が活発化することが期待される。

なお最後に、本国家賠償請求訴訟の裁判に出廷して証言した公安部の警察官 3 人、T 警部補、H 警部補、F 警部補の勇気に敬意を表したい。彼らの証言によって、控訴審判決が認定した警視庁公安部による捜査の問題点が明らかになったのである。ところが、残念なことに、この内1人が既に警視庁を辞職している。報道によれば、2026 年 3 月に辞職した警部補は、警視庁による検証報告書（2025 年 8 月）について、「捜査幹部らの都合のいい話だけが記載され」「不誠実」であり「失望した」と批判し、それが辞職の動機である旨を述べている[40]。

39　著者の最近の著作を例示すると次の通りである。
○「スパイ防止に必要な制度と法律」（警察政策学会資料第 147 号、2026 年 5 月）
○「江蘇省国家安全庁第 6 局による経済スパイ」「韓国国情院による対米影響力工作」（警察政策学会資料第 137 号、2024 年 12 月）。
○「国外活動に対する FBI の情報収集力」（『治安フォーラム』2024 年 5 月号）
○「テロ対策に見る我が国の課題」（警察政策学会資料第 113 号、2020 年 11 月）。本論考は、テロの未然防止のための情報収集について論じたものであるが、その情報収集の手法は、スパイ対策や先端技術の流出対策にも同様に適用され得るものである。

40 遠藤浩二「大川原冤罪　元警部補、貫いた正義～不誠実な検証に落胆」『毎日新聞』2026 年 5 月 28 日付。

筆者は、同警部補の発言の適否を判断する情報を持ち合わせていない。しかし、関係警察官からこのような批判が発せられること自体が、警視庁による検証の信頼性に疑問を惹起するものである。従って、本件のように組織の体質が問われている重大な非違事案の場合は、仮にも調査検証の信頼性に疑義が生じないないように、国家公安委員会或いは関係都県公安委員会の下に、第三者委員を含む検証委員会を設置して、形式的にも公正且つ独立した組織体による調査検証を行うことが望ましいであろう。

（以上）

警察政策学会資料　第 150 号

国家諜報長官 DNI の権限
サイバー対処能力強化法及び同整備法の評価と課題
大川原化工機国賠事件・控訴審判決と
警視庁の検証報告書を読む

令和 8（2026）年 8 月

編集　警察政策学会
　　テロ・安保問題研究部会

発行　警察政策学会

〒 102－0093
東京都千代田区平河町 1－5－5　後藤ビル 2 階
電話（03）3230－2918・(03－3230－7520)
FAX（03）3230－7007