サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か：日米比較を軸に

林　紘一郎 *

田川　義博 †

概要

政府はサイバーセキュリティ事案の重大性に対処するため，新しい「サイバーセキュリティ戦略」を閣議決定し，サイバーセキュリティ基本法等の改正とともに「積極的サイバー防御」に乗り出す方針を打ち出した.しかしサイバー攻撃に対する対抗手段の分類や適法性の議論は進んでおらず，とりわけ重要インフラを民間企業が担っていることからも，被害者である企業による「積極的サイバー防御」の具体化が望まれる.

そこで共著者は，passive defense と offense 間のグレイ・ゾーンにある active cyber defense に関して，米国でも明確ではないさまざまなレベルの対抗手段の適法性を，実施主体の問題も含めて分析した.日米のサイバー対処能力の差等を考えるとき，米国での議論をそのままわが国に移植することはできないが，少なくとも attribution の探知と，公衆衛生に類似の cyber hygiene までは許容されるべきと考える.

その際，わが国に固有の課題として，電話時代からの伝統的な「通信の秘密」の解釈を，インターネットの技術的特性や ISP 等への期待や役割の変化に即して，見直すべきことを提案する.それにより「弱みを強みに転換」し，技術力向上や官民の情報共有の強化などと相俟って，わが国のサイバー防御能力の全体的向上を図るべきことを訴えたい.

1　サイバー攻防の非対称と，それを打破する議論と実践

1.1　サイバー攻撃に対する被害者の自力救済

サイバーセキュリティ事案の重大性に対処するため，政府は 2018 年 7 月 27 日に新しい「サ

* 情報セキュリティ大学院大学教授.なお筆者は現在，内閣サイバーセキュリティ戦略本部員（非常勤）を兼任しているが，本稿は研究者の視点から論じた個人的見解である.

† 情報セキュリティ大学院大学セキュア・システム研究所客員研究員.

イバーセキュリティ戦略」（以下「新戦略」）を閣議決定し，サイバーセキュリティ基本法の改正等と相俟って「積極的サイバー防御」（Active Cyber Defense = ACD[1] ）に乗り出す方針を決定した.しかし官民の情報共有等の体制作りは進展したものの [2]，サイバー攻撃への対抗手段 [3] がどこまで許されるかの議論が進んでおらず，中でも被害者である民間企業が採り得る対抗策については不確実性が高い.

特に注意を要するのは，その適法性（legitimacy または legality）である.近代民主主義国においては，刑事罰の執行はもとより民事の強制手段も国家に一元化されると解されているから，特段の規定がない限り自力救済 [4] はできないのが原則だからである [5] .また銃器の保持が禁止されていることも [6]，烈度（intensity あるいは severity）の高い自力救済の手段を制約することを通じて「禁止」の姿勢を明確にしていることになろう.

他方，米国においてはやや事情が異なり，憲法修正 2 条が‘A well regulated militia being necessary to the security of a free state， the right of the people to keep and bear arms， shall not be infringed.’と規定しており，これは州の権限ではなく国民の権利だと解されている [7] .そこで銃の保有率が世界一で [8]，正当防衛のために拳銃を使う可能性が高い [9] .加えて民事の自力救済の一部が，コモン・ローの伝統を引き継いだ形で許容される余地がある（詳細は第 4 章で論ずる）.

このような法環境を前提にして，米国では「コンピュータ犯罪であるハッキングに対して，被害者である民間企業が反撃することが可能ではないか」という解釈論や，「現行法で不可能なら，立法によって自力救済の道を開くべきだ」という立法論が展開されてきた.本稿は，こうした米国での議論を，わが国の法制の中に移し替えて議論しようとするものである.

---

[1] 「新戦略」における「積極的サイバー防御」は Proactive Cyber Defense と暫定的に訳されている（暫定英訳版）から，ACD と同じかどうかは議論の余地がある.しかし「サイバー攻撃に対して能動的に防御していく取組」という定義（p.20 注 42）からは，そのように推測される.また本稿は「仮に対応していないとすれば直ちに対応すべきである」という政策論を展開する.なお英国の「国家サイバーセキュリティ戦略 2016－2021」は，’apply active cyber defense measures to significantly enhance the levels of cybersecurity across UK networks’と明言している.

[2] 後述する 5.3 の諸法律の改正による.

[3] 国際法の分野では，被害者が採り得る手段の総称として「対抗手段（countermeasure）」の語が一般化している（Schmitt［2017］）.国内法での用語は一定していないが，本稿では国際法に準ずる.

[4] 英語では self-help で「自助努力」と同じ意味を持つが，法律用語しては以下の Black’s Law Dictionary の説明が的確である.An attempt to redress a perceived wrong by one’s own action rather than through the normal legal process.

[5] わが国の民法に自力救済を規定した条文はないが，通説・判例は原則禁止の姿勢をとっている.民法 202 条 2 項によれば，たとえ相手が盗んだものであっても一度占有すれば占有権が発生し，それを自力で奪い返すと占有権侵害となって，相手側に不法行為による損害賠償請求権などが発生するからである.

[6] 銃砲刀剣類所持等取締法（銃刀法）3 条.

[7] District of Columbia v. Heller， 554 U.S. 570 (2008).

[8] The Small Arms Survey 2015.
http://www.smallarmssurvey.org/publications/by-type/yearbook/small-arms-survey-2015.html

[9] いわゆる服部君事件が起きた 1992 年に，共著者は共に東海岸に在住していたが，NY 日本商工会議所の要職にあり滞米期間の長い某氏でさえ，現地生まれのお嬢さんに「何も心臓を狙わなくてもよいのに」と言ったところ「お父さんは何年アメリカにいるの？1 発で仕留めなければやられてしまうのよ」と切り返されて驚いた，という話を聞いた.なお発砲者は刑事では無罪，民事では有責とされた.

1.2 サイバー攻防における攻撃者優位（7 つの非対称）

なぜ自力救済が議論されるかというと，「サイバー上の違法行為は行為者の特定が難しい」という事情，すなわち attribution 問題 [10] と連動しているからである.行為者が特定できなければ対抗手段に訴えるのも難しいので [11]，攻撃者から見れば「ヤリ得」「割の良い商売」となり，「サイバー空間は新しい wild west だ」という悪名を払拭できない.「新戦略」にいう「積極的サイバー防御」は，文字通り読めば「防御に積極的に取り組もう」という姿勢を示した，新鮮味のないスローガンと映るかもしれないが，attribution 問題との関連で理解すれば画期的なものとも考えられる.

そこで改めて，サイバー攻防において攻撃者と防御者が「武器対等の原則 [12]」に沿っているかどうかを検証してみよう.図表1 は林［2016a］を，その後の知見を踏まえて全面的に改定したものであるが [13]，サイバー攻防においては攻撃者優位，すなわち「攻守の非対称」が 7 つの局面の全てで生じており，中でも Attribution 問題は「非対称」をもたらす第 1 の要因になり，攻撃者は低コストで大きな成果が得られる（④ 項）ことを示している.

図表1 サイバーセキュリティにおける攻撃者優位（7 つの非対称）[14]

評価基準	攻撃側	防御側
①実行者の特定	実行者を秘匿する手段がある	Attribution が難しい
②実行行為の隠密性（または時間稼ぎ）	侵入等を隠す手段があり，タイミングを計った hit-and-away も容易	気付かないか，原因を究明するのに時間がかかる
③攻撃手段・組織と攻撃の成否	入手が容易で安価な非合法ソフトを用いたゲリラ的攻撃.一点突破でも成功	合法の範囲で対応.全面防御できなければ失敗
④費用と便益，サンクションの有効性	低コストで大きな利益（社会的影響を含む）.検知されるような低レベルの実行者には賠償能力がない	(reputation risk も含めて)大きなコスト負担.刑事訴追も民事訴訟も困難
⑤人材と国際協力	多数のボランティアと予備軍.緩やかな国際連携(アノニマスが好例)	正規の採用後選抜.国内組織が中心で，一部国際連携
⑥国家の関与	(一部国家による)違法行為の黙認と暗黙の支援	民営のインフラは民間主導.政府が主体の場合も国際秩序を遵守
⑦コンピュータ資源	(方式によっては)膨大な分散計算資源を活用	(セキュアな環境の)有限資源

[10] アトリビューションとは本来「所属」や「帰属」といった意味だが，サイバーセキュリティの文脈では誰がサイバー攻撃を行なっているのかを特定するという意味で使われている.
[11] 特に，匿名訴訟を許さず，民事裁判においては被告の特定までを原告の責任（負担）としているわが国の法制（民事訴訟法 133 条）では，attribution 問題は「裁判を起こせるかどうか」に直結する.
[12] ここでは「正当防衛」における適用など，個別具体的な法理としてではなく，スポーツやゲームを含めた，あらゆる競技や紛争の解決における一般原則として使っている.
[13] 林［2014］［2015］以降一貫して指摘してきたものである.
[14] 「新戦略」も，「攻撃者の非対称な優位性」を認めている（p.6）.

1.3 Attribution 問題解決の糸口

20 世紀末までは，「attribution 問題は直ぐには解決できないだろう」とする一種のあきらめが支配していたが，2000 年代における熾烈なサイバー攻撃を受けて，米国を中心に連邦政府，情報サービス（OTT = Over-The-Top）企業[15]，セキュリティ・ベンダなどが人材と資金の投入を惜しまず努力した結果，少なくとも次の 2 つの認識が共有されるまでに至っている．

① Attribution は「白か黒か」といったデジタル的なものではなく，白と黒の間に連続的に続くグレイ・ゾーンにあるもので，spectrum，あるいは sliding scale（可変的）だと考えるべきである．

② それを一刀両断に解決する万能薬（silver bullet）はないが，インテリジェンス活動と同様に，地道な努力の積み重ねで「解決に逐次接近する」ことは可能である．

このような共通認識を導いた理論として Rid [2013] や Rid & Buchanan [2015] のリアリズム，後述の Lee [2015] の分析などが陰ながら寄与しているだろう．しかし何といってもオーロラ作戦への反撃（2010 年）や，多くのボットネット[16] の takedown（壊滅作戦）といった実践の成果が大きい．attribution 問題を完全に解決することはできないし，刑事訴追の要件である「合理的な疑いの余地がない」（beyond a reasonable doubt）程度に解明することも難しいが，国際政治の現実の中で「強力な手掛かり（strong clues）になる[17]」という自信が生まれたからである[18]．

オーロラ作戦（Operation Aurora）は，中華人民共和国の Elderwood グループ等によって遂行された一連の APT = Advanced Persistent Threat 攻撃に付されたニックネームで，被害にあった企業の中で Google が最初（2010 年 1 月 12 日）に公表した．当時，Internet Explorer について未公表であった脆弱性（2009 年の 9 月に把握されていた）が攻略（いわゆる Zero-day 攻撃）され，複数種のバック・ドアが設置された．これを利用した APT 攻撃により Gmail のアカウントにアクセスし，ソース・コードのバージョン管理に用いられていた Perforce も攻略された．

一般的な感染経路は，次のように分析されており，それぞれは単純な手順である（McAfee [2010]）．1）攻撃対象に，一般的に信頼されている発信元からリンクを示す e メールかインスタント・メッセージが届く，2）受信者がリンクをクリックすると，台湾のサイトに誘導され，同時にマルウェアに感染する，3）受信者の Internet Explorer が Zero-day 攻撃の JavaScript をダウンロードして実行する，4）台湾のサーバーからは画像に潜んだバイナリが送られる，5）それによってバック・ドアが仕込まれ，台湾の C&C サーバーに支配される，6）結果として，攻撃者が被害者の内部ネットワークに侵入し，SCM（Software Configuration Management）システムなどを狙ってくる．

Google に対する攻撃は，2009 年 12 月 15 日からとされるが，それ以前から開始されていた

[15] インフラやプラットフォームを利用して上位レイヤのサービスを提供するので，このように呼ばれる．
[16] bot は robot の略で，一定のタスクや処理を自動化するためのアプリケーションやプログラムを指すが，セキュリティ分野で botnet と言えば，マルウェアに感染させられて C&C（Command and Control）サーバーの意のままに操作される（ゾンビ）コンピュータ群のこと．
[17] 高名なセキュリティ専門家である Alperovitch の実感による（Alperovitch [2011]）．Clarke & Knake [2010] も同旨．
[18] 2012 年秋には国務省顧問の Koh が「国家間のサイバー攻撃には自衛権の行使が認められ，民間企業が政府の指示の下で，あるいは自己の意思と制御の下で行なう場合も同様である」と述べた（Koh [2012]）．

懸念もある.攻撃は同社のみならず，少なくとも 20 社の大企業を標的としたものであることが判明し，「米国内で活動している中国の情報機関の諜報員が，米国の法執行機関に監視されているかどうかを探るため」といった報道がある.

2010 年 1 月 4 日にバック・ドアの通信相手となる C&C サーバーがテイクダウンされて作戦は終了し，2010 年 3 月 22 日 Google は中国本土で展開するネット検索サービスから撤退し，以降，中国からのアクセスについては Google 香港のサイトに転送する方針を明らかにした.この間米国政府，特にクリントン国務長官は「中国政府は徹底的な調査を」と主張することで，Google を間接的に支援していた[19].この間の Google の行為は，わが国の不正アクセス禁止法に相当するアメリカの CFAA（Computer Fraud and Abuse Act of 1984）に違反する疑いが残るが，司法省は訴追の意向を示さず，また民事訴訟も起きていない[20].

一方，サイバー攻撃の「踏み台」となっている，ボットネットの壊滅作戦は各方面で試みられているが，中でも最大規模のものは 2014 年 11 月に発見されたボットネットである Dridex/Bugat（以下単に Dridex）に対する，大規模な国際共同作戦である.Dridex は金融機関向け「トロイの木馬」型マルウェアで，e メールの添付資料を通じて広がり，他人の認証を奪って送金を可能にする.中小の金融機関に重点的攻撃を加えたとされ，被害国は 27 か国，イギリスでは 30 億ドル超，アメリカでは 10 億ドルの被害が生じたという.

Dridex は，その直前に猛威を振るった Gameover Zeus を改良してアンチ・ウイルス・ソフトへの耐性を強め，peer-to-peer の C&C サーバー構造を取るなどしていたため，撃退には困難があった.しかし，英米を中心とする国際協力により，2015 年 10 月には C&C サーバーの指令をシンク・ホール化することに成功した[21].しかしマルウェアを除去するには至らず，汚染されたボットのサニタイズは個々のユーザに委ねられている[22].なお米国では，この壊滅作戦は裁判所の令状を得て行なわれたが，同時に司法省は首謀者とみられるモルドバ国籍の Andrey Ghinkul を不正アクセスなど複数の罪で訴追し，2016 年 2 月にキプロスで逮捕している.

1.4 その後の展開

引き続き米国は，膨大な資源（コンピュータ・パワー，人員，予算）を使った作戦を継続し，中国人民解放軍の 5 名の将校を起訴し，Sony Pictures Entertainment へのサイバー攻撃に北朝鮮が関与したと公表した.これらの行動の結果，オバマ・習近平会談（2015 年 9 月）において「（国家は民間組織へのサイバー攻撃を）実施せず支援せず」の原則を確認できたこと

[19] 米政府のこうした態度は，この問題を単なる民間企業間の紛争と見るのではなく，「情報の自由な流通」を旨とするインターネットの基本原理への挑戦，と見たものと推測される.
[20] 以上の Operation Aurora に関する記述は，Huang [2014] pp. 1247-1249，Center for Cyber & Homeland Security [2016] pp. 13-15， MacFee [2010] や新聞報道などによる.
[21] マルウェアによる C&C サーバーへの DNS リクエストを妨害し，有効なサーバーの IP アドレスではなく，偽造アドレスに誘導することで，マルウェアと C&C サーバーとの通信を途絶すること.
[22] 以上の Dridex に関する記述は，トレンドマイクロ・セキュリティ・ブログ [2014]，Center for Cyber & Homeland Security [2016] pp. 13-15 や，新聞報道などによる.

で，時代の変わり目になったとの評価もある[23].しかし，このような成功は，米国の膨大なサイバー予算と人員を動員して初めて可能になったものであり，他の諸国が追随可能とは思われない（田川・林 [2017a]，本稿 5.4 の図表 9. および第 8 章も参照）.

現に本年 9 月 20 日に発表された米国の Natinal Cyber Strategy[24] においては，インターネットは米国が生み出したという自負と自信に基づき，'an open, interoperable, reliable and secure Internet' を維持し，「個人の自律，言論の自由，市場原理，プライバシー」などのアメリカ的価値を守るために，先頭に立つとの強い意思表示をしている（p.2）.もっとも，この戦略は cybersecurity strategy ではなく cyber strategy なので範囲が広く，安全保障全体が含まれる.そこでは現政権の方針を反映して，アメリカ第一主義とロシア・中国・イラン・北朝鮮を名指ししたサイバー攻撃非難などが鮮明で，防御面では，サプライ・チェーン全体を通じたセキュリティの確保や，知的財産の保護・標準化の戦略的意義などを強調している.

1.5 Hack Back 論争

1.3 の諸行動のうち，官民合同作戦については，今後も機会を見て続けられると思われる[25].また Operation Aurora 対策のような単一企業による対抗手段に関しても，その後も継続していると見られる.Black Hat の調査によれば「情報セキュリティ専門職のうち 36％（正確には，frequently 13% と，once 23% の和）が，報復的なハッキング（Retaliatory Hacking）を行なっている」と報じられているからである[26].

ただし，「報復的なハッキング」の内容は明らかではなく，多くの文献が「Hack Back は法的に許されていない」と述べており，有名な Hack Back Debate でも明確な結論が出ていないことから見れば，どの程度の烈度の対抗策かは必ずしも明確ではない.また時間の経過とともに，かつては大がかりな作戦を要した手段が，ソフトウェア・パッケージで可能になるなどの変化が生ずることもある[27].

ここで Hack Back Debate について，若干付言しておこう.これは 2012 年に Baker（NSA 出身，Steptoe & Johnson のパートナー），Kerr（元司法省，現 George Washington 大教授），Volokh（UCLA 教授，Volokh Conspiracy の創設者）の間で交わされたスリリングなブログ（Steptoe Cyberblog [2012]）である.Baker 対 Kerr，Volokh 対 Kerr の 2 部構成となっており，Baker がインテリジェンスの経験者として，Volokh が Law & Technology の専門家として，ともに hack back を弁護する立場から Kerr に挑戦したが，Kerr が法律的な厳密な議論で「守り切った」ような印

[23] その評価に関しては，土屋 [2015] などを参照.この合意の後，中国がこれまで共同歩調を取ってきたロシアに同調しないと述べていることを評価する向きがある一方で，懐疑派はなお多数を占めている.
[24] https://www.whitehouse.gov/wp.../09/National-Cyber-Strategy.pdf
[25] 金融分野の事例につき，Harrington [2014] pp. 35-36 を参照.ただし Rowe et al. [2011] が指摘するように，作戦終了後に費用・便益分析を行ない公表する例は少ないようである.
[26] Boose [2012] の記事が元で，Harrington [2014] も Jasper [2017] もそれに依拠している.また大企業による ACD の事例は，多数報告されている（Glosson [2015] などを参照）.
[27] Center for Cyber & Homeland Security [2016] には，銀行向けソフトが開発され passive defense の範囲が広まった例が紹介されている（p.24）.

象を受ける.

そして彼の立場の背景には，司法省 CCIPS（Computer Crime & Intellectual Property Section）による，次のような有権解釈があると推測される[28]．

‘Although it may be tempting to do so (if the attack is ongoing), the company should not take any offensive measures on its own, such as “hacking back” into the attacker’s computer----even if such measures in theory be characterized as “defensive”. Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, “hacking back” can damage the system of another innocent party’.

1.6 サイバー防御の変質

2010 年代初頭から現実味を帯びてきた ACD は，近年に至って徐々に変質しつつあるかに見える.共著者は，その特質を以下の 3 点に要約できると考えている.

① 当初は「行為者を特定し早期に反撃を加える」ことを想定していたが，次第に「被害が生じても早期に無害化あるいは緩和し，潜在的被害者ともインシデント情報を共有して耐性を強める」ことに重点が移りつつある（counterattack から neutralization あるいは mitigation へ），

② attribution の概念も上記に応じて変化し，当初は「犯罪捜査における犯人特定モデル」を追求していたが，今では「仮に実行者を特定できなくても，ネットワークあるいはシステムに支障を及ぼし，同一あるいは同一グループによる攻撃の蓋然性が高い事象があれば，その弊害を除去する」ことを attribution と捉える程度に変化している（実行者の特定から潜在的同一攻撃要因の特定へ），

③ これはサイバー事案の対処策について，物理的世界で有効であった諸概念（武力の行使＝use of force や抑止＝deterrence など）から離れて，独自の概念や手法を生み出そうとする動きと捉えることができる.ただし，その際にも物理的アナロジーが有効である限りはそれを用い，それを越える部分に新しい概念を適用しようとしている.

上記 ① の推論は，「ACD には hack back を含まない」という点に関しては，ほぼどの論稿も一致していることによって，補強されるだろう.Hack Back はセキュリティ分野ではよく使われる用語で，2003 年が初出というが（Harrington [2014] p.3 [4]），後述の Center for Cyber & Homeland Security [2016] における定義で，offensive であるとして active defense から除外することとなり，最近の論稿である Hoffman & Levite [2017] もその立場を確認している.因みに米軍の用語で active defense とは，’the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy’[29] であるから，それとは違

[28] これは Kerr が引用したものだが，現行の Prosecuting Computer Crime Manual にも全く同一の表現がある.
htpps://.justice.gov/criminal-ccips/ccips-documents-and-reports
[29] US DOD Joint Publication 1-02, DOD Dictionary of Military and Associated Terms 2 (2012)

った定義を採用することになる.

また ② は，多くの論稿が attribution をかなり広義に解釈しているし，白か黒かの二値的なものではなくspectrumだとする見方と符合している.本稿でも，この用語を ② の意味で用いることにしたい.

1.7 本稿の検討対象と方法

本稿は，上記の議論の展開を踏まえて，わが国における「積極的サイバー防御」を具体化しようとするものである.しかし，共著者の能力と時間の制約もあって，検討の枠組みを以下の範囲に限定せざるを得ない.

① 日本の領土内で，日本法に基づいて行なう手段に限定し，国際法の分野は除く[30].これは一見，国境のないインターネットについて自ら境界線を引くことによって，全体像を捉え損なうと思われるかもしれない.しかし実は，国際法の分野での議論が必ずしも確立しているとは言えない（Tallinn Manual 2.0 = Schmitt [2017] においても，自衛権の発動条件については議論の余地がある[31]）ので，適用分野を絞ることによって論点の明確化を図るものと理解していただきたい[32].

② 日本政府が主体となって実施するのではなく，民間企業が主体となる手段に限定する.これは上記のように論点を絞ることに伴う流れである.ただし，官民協力までは視野に入れて論ずる[33].

③ モデルとしては米国における「サイバー攻撃の被害者である民間企業の自力救済」を中心に議論する.米国には多くの実例と議論の蓄積があるため，わが国への教訓を引き出すに適しているからである.本来なら英国なども参照すべきであるが，今回はあきらめざるを得ない[34].

④ 日本の現行法を前提にし，これに最低限の修正を加えることを提言する.サイバーに関する法的規律のあり方を from scratch で議論することにも利点はあるが，サイバー攻撃が複雑化・巧妙化しており，今後 IOT（Internet of Things）や AI（Artificial Intelligence）やロボットの登場によって，複雑性が何倍にもなる事態が予想されるので，本稿では incremental approach を採ることにした[35].

---

[30] これに連動して，国家安全保障に直結する分野も検討から除外される.

[31] 国際法では自衛権の議論は進んでいるものの，国家の自衛権を民間企業に発動することは認められていないし（Garrie & Reveves [2016] p.1831），私企業の countermeasures は議論すらされていない（Jasper [2017] p.178）ので，このような方法論はやむを得ないものとも考えられる.

[32] 国際法は通常条約として締結され，批准・国内法化という手続きを経て国内法になるので，その面からも国内法に絞ることに一定の合理性があると考えられる.

[33] 本来ならインテリジェンス機関との情報共有までを視野に入れるべきかもしれないが，本稿では除外する.ご関心のある向きは，林・田川 [2016] を参照されたい.

[34] この点に関心をお持ちの向きは，林 [2016b] および 林・田川 [2016] を参照願いたい.

[35] これは林の長年の主張である paradigm-shift approach とは正反対である（林 [2017] 参照）.

2 Active Cyber Defense = ACD と自力救済（Self-Help）

2.1 ACD 論争の前史：NRC [2009] と Kesan の貢献

20 世紀末からサイバー攻撃が深刻化したことから，ACD の可能性に関する議論と実践が始まった.1998 年に Electronic Disturbance Theater という集団がペンタゴンのサイトに DoS 攻撃を仕掛けた時には，ペンタゴンがこれを自動返送した.1999 年に WTO（World Trade Organization）のサーバーをホストしていた Conxion 社に対する DoS 攻撃に際しては，同社が Electrohippies を名乗るグループの仕業と突き止めて，メール爆弾を自動返送することで数時間攻撃サーバーを止めた（Kesan & Majuca [2009]）.

しかし，事象の発生と対策の検討には時差があるのが当然で，政府を含むレベルで ACD の可能性を検討したのは，National Research Council 内に設置された Committee on Offensive Information Warfare が出した報告書（以下，NRC [2009]）が，最初ではないかと思われる.だが，軍と産業が「複合体」を形成している米国の常で，この報告者は国家安全保障を主たる対象としたものであり，本稿の問題意識を超えるものである.

国家安全保障と無縁ではないが，民間にも適用可能なものとして分析した先駆的論文は，Kesan & Majuca [2009] であろう.これは「法と経済学」の方法論に拠り，1）刑事訴追に期待する，2）民事裁判に期待する，3）自力救済に訴える，の 3 つの選択肢が，どのような条件なら最適であるかを，経済モデルの分析から明らかにしたものである.

その結論は，自力救済が最適解となるのは，1）反撃コストと被害者の損害の和が第三者の損害可能額を上回り，2）無関係の第三者ではなく攻撃者を狙い打ちする蓋然性が相対的に高く，3）刑事訴追や民事訴訟による救済が非効率か実現困難な場合，の 3 要件が満たされた場合だとする.しかも，それには a）攻撃者のコンピュータ・システムに不当な損害を与えてはならず，b）合理的で比例的な手段しか用いず，c）対抗手段の実施者は無関係の第三者に与えた損害に対して民事責任を負う，という条件付きだという（pp. 10–11， pp. 40–41）.

この論文が「法と経済学」のものであったのに対して，Kesan & Hayes [2012] は，純粋の法学の論文として執筆されたもので，ACD を 1）侵入を検知する，2）侵入者を追跡する，3）ある種の対抗手段を講ずる，の 3 要素の組み合わせであるとしている.その上で，国際法の「抑止」（deterrence）を実現に近づけるためには，retributive（応報的）なものではなく，mitigative（鎮静的）な対抗手段が望ましいと主張している.

Kesan の両著作は示唆に富んでいるが，この間に反撃用ソフトが複数開発されたものの，サイバー攻撃が止むどころか更に複雑化・深刻化していったので，実用的価値の面では時代に先駆け過ぎ，その後の理論と実践の展開を待たねばならなかったように思われる [36] .

[36] なお，このほかに実務家の手になる Harrington [2014] があり，技術的な観点を広くカバーしているので，法律論と並行して読むと参考になる点が多い.

2.2 Huang [2014] における議論

「積極的サイバー防御」(ACD)を，本稿の問題意識に近い形で擁護した最初の試みは，おそらく Huang [2014] であろう[37].彼の分析は，以下の 4 点に特徴があると思われる.1) 法学者らしく「解釈論と立法論」を分け立法論として論じている，2) attack 対 counterattack という二元論を維持しており，その間のグレイ・ゾーンは無視している，3) それは技術的な細部には立ち入らず専ら法律論に終始していることと符合している，4) 結果として技術専門家以外にも分かり易いという利点はあるが，逆に「技術的にどこまでできるのか」が曖昧になっている[38].

彼の問題意識のうち最も強いのは，現在の法制に対する不満であろう.次のまとめが，その懸念を端的に示している(Huang [2014] p. 1247).‘The end result is that the overall structure of U.S. hacking law does little to deter criminals and foreign government, but leaves U.S. corporations overly cautious and unwilling to publicly respond in kind.’

2.3 Lee [2015] における議論

Lee [2015] のユニークさは，Defense と Offense は discrete に区分されるものではなく，その間に active defense という領域が存在することを明言し，同時にこれらが sliding scale として連続していることを示した点にあると思われる.また同時に intelligence を独立項目とし，すべての手段の前にアーキテクチャによるセキュリティの確保が必要なことに気づかせてくれたことも重要である[39].

彼は，これらの手段を左右に書き分けているが，ここでは烈度の高低により上下のレイヤ構造に変えて表示(上に行くほど烈度が高い)してみると，図表 2 のようになる.このように Lee [2015] は，ACD を攻撃と防御の中間にあり，連続的に変化するものと捉えた点では恐らく最初の論文であったが，残念ながら技術的側面を含めて ACD の内容を更に細かく分析し，それぞれの適法性を検討するものではなかった.

図表 2 The Sliding Scale

レイヤ	定義
Offense	Legal countermeasures and self-defense actions against an adversary
Intelligence	Collecting data, exploiting it into information, and producing intelligence

[37] 同じ George Washington University の先任教授である Kerr は，Huang より 10 年ほど先んじてこの問題を論じているが，どちらかと言えば懐疑的な態度であるのに対して，Huang は明らかに擁護的である(Kerr [2005] [2016] など参照).なおサイバーセキュリティ専門家の中で最大の懐疑派は，’a remarkably bad idea that would harm the national interest’だとする Lewis [2013] であろう.

[38] 次の記述が，これらの特徴を最も簡潔に述べている.This Note uses the term “counterattack” to encompass any unauthorized access by victims against their attackers, which other authors have described using the term“hackback”or“counterstrike”. This Note also uses“self-help”to describe the legal privilege to engage in counterattacks. In addition, this Note’s use of the term “counterattack”includes read-only access and other activities involving little or no harm.(Huang [2014] p. 1264 注 105)

[39] 後者は今日では，security-by-design と言い換えることができよう.

Active Defense	The process of analysts monitoring for, responding to, and learning from adversaries internal to the network
Passive Defense	Systems added to the architecture to provide reliable defense or insight against threats without consistent human interaction
Architecture	The planning, establishing, and upkeep of systems with security in mind

(Source)Lee [2015] p.2.原文は上記の手段を左右に書き分けているが，本稿では烈度の高低により上下のレイヤ構造に変えて表示（上に行くほど烈度が高い）

2.4 Center for Cyber & Homeland Security [2016] における議論

Lee［2015］における議論をさらに精緻化したのが，Center for Cyber & Homeland Security［2016］である[40] .このレポートは，サイバー攻撃が巧妙化・複雑化したためファイアウォールのような単純な防御では防ぎきれず，また政府と民間のいずれかだけでは民間主体のインフラを守りきれないので官民協調が不可欠であるところ，こうした目的に合致する枠組みが不十分であるとして，大統領府・議会・民間企業に対して「何をなすべきか」の具体策を提言している[41]

その提言は多岐にわたるので次章で詳しく分析するが，基本になっているのは以下の 2 つの図表である.まず図表 3 においては，OffenceとDefenseの間にActive Defenseという領域があることを確認し，報告書のメイン・タイトルの通り「グレイ・ゾーンに分け入って」分析を加える.その際，ACD をまず技術面から細分して，個々の技術が何を意味するか，どの程度の烈度にあるかによって，対抗手段としての有効性と適法性を検討しようとしている[42] .

図表 3 Active Defense（The Gray Zone）and Technological Definition

Impact and Risk	Measures	Technological Definition
Offensive Cyber		Hacking back/Operations intended to disrupt or destroy external networks or information without authorization, etc.
Active Defense with higher impact/ risk and requires	Rescue Missions to Recover Assets	The use of hacking tools to infiltrate the computer networks of an adversary who has stolen information in an attempt to isolate the degree to which that information is compromised and ultimately recover it. Rarely successful.
	White-hat Ransomware	The legally authorized use of malware to encrypt files on a third party's computer system that contain stolen information in transit to a

[40] 他に Craig, Shackelford & Hiller [2015] も，G8を含んだ各国のサイバー法制を比較するとともに，ACD 用製品の機能を相互に比較している点が興味深い.しかしベンダの発想に偏っているきらいがあるので，ここでは採用しなかった.
[41] Center for Cyber & Homeland Security [2016] Foreword and Acknowledgements, Executive Summary など参照.
[42] 読者の便宜のためには，図表を邦訳すべきかもしれないが，適法・不適法は技術の烈度や法概念と密接に関連しているので，敢えて英語のままとしていることをお許し願いたい.

close government cooperation		malicious actor's system. Public-private partners then inform affected third parties that they have been compromised and are in possession of stolen property, which must return in order to regain access to their files.
	Coordinated Sanctions, Indictment & Trade Remedies	Coordinated action between the private sector and the government to impose costs on known malicious cyber actors by freezing their assets, bringing legal charges against them, and enforcing punitive trade policies that target actors or their state sponsors.
	Botnet Takedowns	Technical actions that identify and disconnect a significant number of malware-infected computers from the command and control infrastructure of a network of compromised computers.
Active Defense with lower impact/ risk	Intelligence Gathering in Deep Web/ Dark Net	The use of human intelligence techniques such as covert observation, impersonation, and misrepresentation of assets in areas of the Internet that typically attract malicious cyber actors in order to gain intelligence on hacker motives, activities, and capabilities.
	Beacons: Provide information on external networks	Pieces of software or links that have been hidden in files and, when removed from a system without authorization, can establish a connection with and send information to a defender with details on the structure and location of the foreign computer systems in traverses.
	Beacons: Notify owner in case of theft	Pieces of software or links that have been hidden in files and send an alert to defenders if an unauthorized user attempt to remove the file from its home network.
	Hunting	Rapidly enacted procedures and technical measures that detect and surgically evict adversaries that are present in a defender's network after having already evaded passive defenses.
	Denial and Deception	Preventing adversaries from being able to reliably access legitimate information by mixing it with false information to sow doubt and create confusion among malicious actors.
	Tarpits, Sandboxes & Honeypots	Technical tools that respectively slow hackers to a halt at a network's perimeter, test the legitimacy of untrusted code in isolated operating systems, and attract hackers to decoy, segmented servers where they can be monitored to gather intelligence on hacker behavior.
	Information Sharing	The sharing of actionable cyber threat indicators, mitigation tools, and resilience strategies between defenders to improve widespread situational awareness and defensive capabilities.
Passive Defense		Basic security controls, firewalls, antivirus, patch management,

	scanning and monitoring, etc.

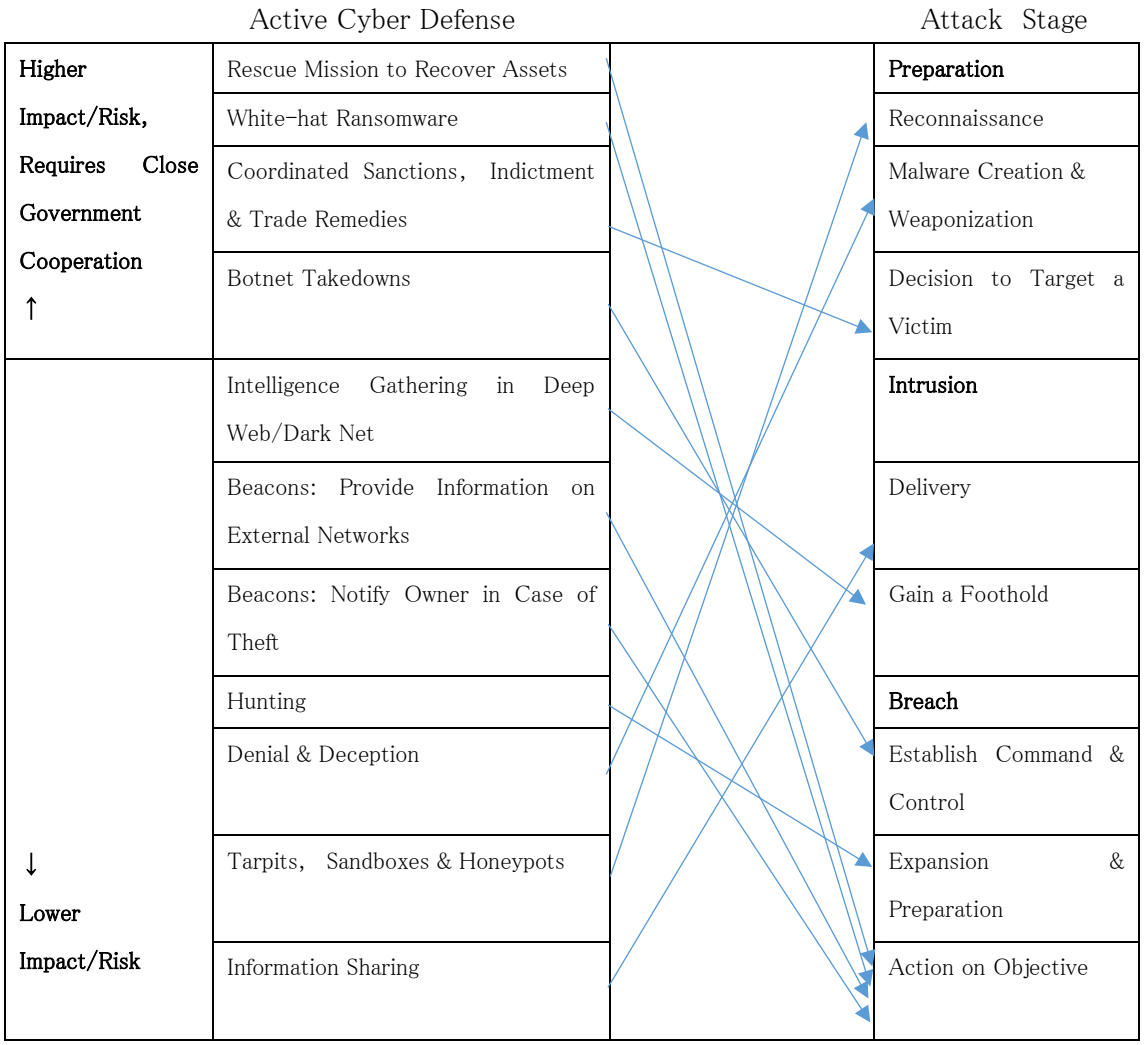
(Source) Center for Cyber & Homeland Security [2016] pp.10-11.原文は 2 図に分かれ，上記の手段を左右に書き分けているが，本稿では両図を統合した上，烈度の高低により上下のレイヤ構造に変えて表示（上に行くほど烈度が高い）

さらに図表 4 においては，ACD のどの手法が攻撃のどの段階で有効であるかを分析している．一般的には攻撃の前段階では烈度の低い対抗策が取られ，攻撃の激化とともに烈度の高い対抗手段が必要でもあり，有効であると想定される.その予想どおり，烈度の低い対抗手段が攻撃の前段階（攻撃者の preparation 段階）で有効なケースが示唆されている．

以上の分析に関して，Center for Cyber & Homeland Security [2016] は自らの立場を次のように要約している（p.9）．

‘Active defense is a term that captures a spectrum of proactive cybersecurity measures that fall between traditional passive defense and offense. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defense includes those operations that enable defenders to collect intelligence on threat actors and indicators on the Internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behavior of malicious actors. The term active defense is not synonymous with “hacking back” and the two should not be used interchangeably.’

図表 4　ACD と Attack の対応関係



(Source) Center for Cyber & Homeland Security [2016] における図 4 を，ACD の烈度の高低を上下に書き直したことに伴って修正.

2.5　Hoffman & Levite [2017] における議論

前節の報告書以降に公表された Hoffman & Levite [2017] は，以下の 5 点において先行研究を補強し，新たな視点を提供するものとして注目される[43]．

① Active Measures から hack back を除くとの見方を支持している，
② 初めて ACD の利害得失分析を実施し，個別企業への効果だけでなく，社会全体への効果（外部経済・不経済）も考慮している，
③ 初めて ACD の Code of Conduct（CoC）を提案している，
④ 保険会社の機能（リスク分析，情報アクセス，インセンティブ付与）に期待している，

[43] このまとめ方は共著者独自のものである.なお別の見方として，高橋郁夫弁護士のサイト（http://www.itresearchart.biz/?p=1144）に，簡潔な解説がある.

⑤　国内法の適合性以上に，国際法上の議論に重点がある.

このうち ② が最も注目されるので，以下にその図表を引用するとともに，彼ら自身の本文中の説明で補強しよう.

図表 5　民間による ACD の利害得失

Criteria		Advantages	Risks
個社レベル	予知能力の拡大と誤診	潜在的脅威を予知し，不意打ちを減殺し，資産を守る	人的エラーや，攻撃者の誘導に乗ってしまう逆効果
	選択肢の拡大と誤用	攻撃者に対抗する手段が多様になり，かつどこで，いつ，どのように実行するかの柔軟性がある	Attribution を間違えることなどで，善意の第三者のコンピュータやネットワークに偶発的損害を与える危険
	攻撃停止措置と紛争の拡大	第 1 次攻撃を受けた後，計画されたあるいは実行中の攻撃を妨害し，あるいは中止させる高度の能力	ACD に対して攻撃者が反撃してきた場合，紛争がエスカレートする危険
	抑止効果と不確実性	攻撃を難しくし，データの利用を妨害し，攻撃の直接・間接費用を高めることで，将来の攻撃を抑止する効果の増大（特に attribution ができた場合）	外部ネットワークに影響を及ぼす手段が招く，政治的・法律的効果を含めた戦略的含意の不確実性
社会全体のレベル	官民機能の相互補完と調整問題	官と民が，それぞれの任務を果たすことで，シームレスな相互補完になる.また，すべてを政府に依存する場合のモラル・ハザードを回避できる	それぞれの行為が，他者を補うことから，攻撃者の反撃がどちらにも向かう危険がある.また cloud や IoT の普及で，調整問題がより難しくなる
	外部効果の内部化・産業化と依存度	個々の安全の向上は正の外部性を有する.これを内部化することで，セキュリティ産業が成長する	旧来の政府の業務を民間に外注する傾向が進むと，軍産複合体に代わって，軍・インターネット複合体が生ずる
	社会全体の安全の向上と実効性	犯罪対策の SCP（Situational Crime Prevention）のように，Cyber Hygiene を推進できる	SCP も CH も，概念が先行し，実効性の検証はこれからである

（Source）Hoffman & Levite [2017] p.6 の Table 1 に，共著者が pp. 6-8 の記述を追加.

この表は客観的に良くまとまっているが，ソマリアの海賊対策における民間の自力救済をモデルにしているためか，「hack back は ACD に含まれない」との自身の定義 ① にかかわらず，前節の分析（図表 3. と 4.）と比較しうる Figure 1～3（p.9 および pp.20～21）において，対抗手段の中に hack back を含めてしまっている[44] .そのため折角の分析ではあるが，この部分は本

[44] 実は Figure 1 が先に考案され，Levite が Center for Cyber & Homeland Security のプロジェクトで紹介したことから，図表 3 の左半分ができたようである（Hoffman & Levite [2017] Figure 1 の Note）.

論文で生かすことができない.代わりに上記 ③～⑤の部分を,「ISP の役割」を論ずる際(後述の 6.3)に併せて議論しよう[45].

2.6 仮のまとめと付言

以上を要するに, この分野の研究として Center for Cyber & Homeland Security [2016] は, 以下の諸点において他の諸研究よりも優れていると思われる[46].

① これまでの議論の蓄積を集大成した感がある,
② 関係者へのヒアリングを中心にまとめられたので, 実効性が期待できる,
③ プライバシーなどの人権にも配慮している[47] ,
④ 技術的な対抗手段はもちろん, 非技術的なもの(情報共有, 技術的に attribution が確定した後の公表など)も含まれており包括的である,
⑤ 最もクリティカルな適法性に関して, 全面的に答えることはできないが, ある程度の判断基準を示している,
⑥ 基本的人権を保障するための監視機関や報告制度にも触れている.

そこで次章では, この報告書の内容を, かなり細部にわたって紹介することにしたいが, その前に「そもそも自力救済(や, それに代替する手段)がインターネットの世界で有効なのか」という問いに触れておきたい.この点について米国では, 1) 自力救済について相当量の議論があるほか[48], 2) アーキテクチャで解決すべしとする説や, 3) ISP(Internet Service Provider)に責任を負わせるのが妥当とする説など, およそ 3 種の議論がある.

このうち 1) は, 本稿の主題そのものであり, 2) は, Lessig [1999b] に端を発する「コードが法である」という流れの延長線上にあり, 前述の Lee [2015] が指摘したアーキテクチャの重視(私流には security-by-design の発想)もそれに連なるものと思われる[49] .3) は, 一見したところ自力救済の放棄に見えるが, その実個々のユーザの自力救済を ISP に一括して代行させようとするものである.

したがって本稿では, 1) に関してはACD に関する限り以後の議論の中の随所で紹介し, 3) に関しては独立の項目(6.3)として取り上げたい.2) にも触れたいところだが, このテーマに踏み込むと,「インターネットは自律分散型の意思決定に委ねるべきで, サイバー法という最低限の規律だけが必要だ」というサイバー自律派と,「サイバー空間にも実空間の法が適用されるべきで, 両者に差はない」という実空間との一元派の神学論争に巻き込まれかねないので[50],

---

[45] ②において「hack back は費用便益分析でも割に合わない」ことを示唆する分析が見られるが, 理念的なもので実データによる裏付けがないので, 仮説として今後の検証を待たねばならない.
[46] 他に有名な手法として, ロッキード・マーティンが開発した Cyber Kill Chain があるが, やや軍事的なので採用は避けた.この手法が日本年金機構への攻撃の分析に適用可能なことを示した, 森ほか [2016]を参照.
[47] もっとも, この Task Force の 4 人の共同議長の 1 人である Nuala O'connor が「Additional View」を添付資料として提出している点が気になるが, additional なものであり報告書自体には賛成しているので, 課題の部分を強調するのが真意かと思われる.
[48] 事象をより根源的に捉える傾向がある「法と経済学」においては, spam mail や DDoS 攻撃の差し止めのほか, Digital Rights Management や, その対極にある fair use も自力救済になる(Smith [2005])が, 本稿ではそこまで射程を広げることができない.
[49] わが国でも松尾(編)[2017] など, アーキテクチャを重視した書籍が出ている.
[50] その源流は, イースターブルックの「馬の法」(Easterbrook [1996])とレッシグの「サイバー法」(Lessig [1999a])論争である.

ここでは避けておきたい.

代わりに，これらの議論を整理した Kerr［2005］が，次のような注目すべき指摘をしているので，それによって当面の議論を集約しておこう.彼は「メタファーやアナロジーは有効な場合があるが，それらに過度に依存すると正しい姿が見えなくなることがある」と警告し，‘incorporating assumptions from the physical world breaks down when applied to the Internet’であると率直に認め，‘a physical description of the Internet differs dramatically from a virtual description of Internet applications’ではあるものの，なお自身は‘any effective model for deterring computer crime must be rooted in the former rather than the latter’と主張している.

これは現実論としては評価すべきで，特に刑事法の分野では賛同する論者が多いかと思われる.共著者は後述のとおり，所有権を重視した有体物の法体系から離れて，「占有できない」情報の特性に配慮した「情報法」を構想すべきである，との立場を採っている.しかし林が，この点を論ずるだけで 1 冊の本を書いた（林［2017］）ほどだから，本稿では ACD に焦点を合わせるため，とりあえずは彼の主張を認めて以下の論議を進めていこう[51].

3 米国での検討：グレイ・ゾーンに分け入る

3.1 Center for Cyber & Homeland Security [2016] の概要

この報告書は，分析の部分と提言の部分から成り立っている.本来なら，この順序に従って論ずるのが理解に資すると思われ，実際報告書の構成はそうなっている.しかし報告書のタイトルが示すように，この作業は「グレイ・ゾーンに分け入る」ことであるにもかかわらず，ACD がどこまで法的に許容されるかはなお不明確である.そこで本稿では，順序を逆にして，まず提言を概観し，その後に問題点を指摘することとする.

提言部分は，全体で15の行動指針から成り，行政府に対するものが9件と過半を占め，議会に対するものと民間企業に対するものが各 3 件となっている.以下，その順に節を改めて拙訳により紹介する（原文と同様，15 件全体を通番で表示する）.なお翻訳は分かり易さを重視するため，厳密な意味での「逐語訳」になっていない部分があることを，予めご了承いただきたい.

3.2 行政府に対する提言

(1) 司法省（DOJ）は民間企業向けのガイドラインを策定し，現行法においていかなる ACD が解釈上許されるのかを明確にし，併せて当該 ACD が企業自身のデータやシステムの

[51] 実は米国の議論は，「サイバー法」という virtual place を前提にした議論であり，客体である情報を中心に据えた「情報法」という視点は希薄である.共著者は，この点が議論の混乱を招いているのではないかという疑問を払拭できないが，差し向き林［2017］を参照いただくことにして別途の機会に論じたい.

セキュリティに関する限り，DOJ は刑事訴追も民事訴訟も提起しないことを明示すべきである．

(2) 司法省と連邦取引委員会（FTC）は，“Antitrust Policy Statement on Cybersecurity Information Sharing”（2014）を改定し，独禁法が ACD に関する業界内協調行動に対して障害となるものではないことを明言すべきである．

(3) 国土安全保障省（DHS）は，業界主導の ISACs[52] や ISAOs[53]，また同省所属の NCCIC[54] といった既存の組織間調整メカニズムを利用して，ACD に関する官民協調手順の開発を調整すべきである．

(4) 国立標準技術研究所（NIST[55]）は，民間企業による ACD のリスク評価と実行に関して，ガイドライン，ベスト・プラクティス，コアとなる能力の開発を進めるべきである．その際，被害企業が自ら ACD の手段を実行する場合には，それに対応する（第三者ベンダの場合には他の企業を保護する）能力証明と結びついた 3－5 段階の成熟度モデルを用いるべきであり，そうしたガイドラインは産業別に異なるかもしれないが，2013 年から 2014 年にかけて開発した Cybersecurity Framework との一貫性を維持すべきである．

(5) 国防省（DOD），国土安全保障省，インテリジェンス・コミュニティ，全米科学財団（NSF[56]）などサイバーセキュリティ関連の R&D 資金を提供する連邦機関は，新しい ACD 手段（attribution 問題の解決を促進する能力を含む）に関する研究に優先順位を与えるとともに，現状の ACD 手段の効率性を評価すべきである．

(6) 国務省（DOS）は，外国政府と協力して ACD 手段の標準化と手順の策定に携わるべきである．これはサイバー脅威の被害者である大企業の多くが，グローバルに事業展開しているため，1 ダース以上の国々で情報とシステムを守らなければならない点に鑑みて，特に重要である．

(7) プライバシーと市民的権利監視委員会（PCLOB[57]）は，現に行なわれているか，この報告書で提案されている，民間企業の ACD に関する行政府の活動に関して，レビューを実施し結果を報告書として公開すべきである．

(8) 大統領府（White House）は，民間企業の ACD 活動に対して連邦機関がいつ，いかなる方法で支援すべきかに関するガイドラインを，政策として準備すべきである．それには，民間企業の成熟度，脅威の主体（分かれば），インフラストラクチャーや情報の経済的・安全保障的重要性などが反映されなくてはならない．後者の要素は，DHS が Executive Order 13636「重要インフラのサイバーセキュリティに関する改善策」の 9 条で指定する“critical infrastructure at greatest risk”のリストに含まれる情報共有・調整活動・インテリジェンス面の支援・訓練と関連するであろう．

[52] Information Sharing and Analysis Centers
[53] Information Sharing and Analysis Organizations
[54] National Cybersecurity and Communications Integration Center
[55] National Institute for Standards and Technology
[56] National Science Foundation
[57] Privacy and Civil Liberties Oversight Board

(9) 大統領は大統領令により，上記 (1)～(6) 項の要求事項を定めるとともに，それらを実現するデッドラインを明確にすべきである.

3.3 議会に対する提言

(10) 議会は上記 (1)～(7) で提言した活動の，実施を監督する法律の制定を目指し，そのデッドラインを設定し厳守すべきである.議会はまた，連邦政府監査院 [58] に法律の実施状況をレビューする責任と権限を付与すべきである.

(11) 議会は CFAA と Cybersecurity Act of 2015 の文言が，民間企業の ACD を制約している点を再検証し，リスクが低いか中程度の対抗手段が，必ずしもこれらの法律で直接的に禁止されていないことを明確にすべきである.

(12) 議会は，法律に規定された他の手段（例えば，訴追，制裁，貿易対抗策など）が，民間企業が悪意あるサイバー行為者に対して自身を保護するのに役立つか否か，またどのように役立つかを検証すべきである.Executive Order 13694「重大な悪意によるサイバー利用行為に関与した者の資産の凍結」は，この原理を実践するのに適した例であるが，他の手段もサイバー抑止と ACD に利用可能であろう.

3.4 民間企業に対する提言

(13) 民間企業は他の企業と協調して，自産業内の ACD 手段に関して，業界標準やベスト・プラクティスの開発を主導すべきである.こうした活動は，世界中の主要企業を巻き込んで国際的規模で展開すべきである.

(14) 民間企業は，データ流出や他の形態のサイバー攻撃に対して，事故が起きてから事後的に対応するのではなく，将来起こるかもしれない仮定の攻撃に備えて，一定の ACD 手段に訴えるつもりか否かを，CEO・CIO などのトップ・レベルで政策決定すべきである.民間企業は産業標準とベスト・プラクティスを生かして運用手順を定め，全社のリスク評価と分析に基づき，インシデント対応手順としてより広い視野のサイバー戦略と統合すべきである.これらの政策は，企業固有の伝統的なサイバー防御計画への広義のコミットメントおよび投資戦略と，一体化されねばならない.

(15) 業界団体は ACD に関して，ISP，ウェブ・ホスティング会社，クラウド・サービス事業者あるいはそれら企業の顧客との間の協調関係のベスト・プラクティスを見直すべきである.これらのサービス提供者は日常業務として顧客のネットワークに対して契約上の事前のアクセス権を付与されていることが多く，その権限を生かせるからである.こうした事業者は，顧客のサイバー脅威に対して ACD 手段を取る上で適した立場にあるかもしれない.

[58] Government Accountability Office

3.5 提言の基礎となる現状認識

提言の基礎となる現状認識は，報告書の第 2 章「現行の政策，法，技術の文脈」の中で述べられている.その要点は，以下の 5 点にまとめることができよう.

① ACD がグレイ・ゾーンに属するという特性は，その手段の適法性の面に最も顕著に表れている，
② 明確なのは，現行の米国法において，民間企業に「自衛（あるいは自力救済）」を明文で認める法は存在しない，ということである，
③ しかし大企業の一部は，米国法の適用外において，米国法で認められない方法で，自社資産をサイバー攻撃から守る手段を追求している，
④ 他方で大部分の企業は，ACD により得られる強い抑止の姿勢を示すに必要な行動（単独であれ協調行動であれ）を，追求しようとしていない.これには次のような多くの要因がある：法的な曖昧さ，リスク回避の傾向，資源の制約，協調的指導力の欠如，ACD の理解不足，
⑤ よって行政府・議会・民間企業は，前節で述べた行動指針を速やかに実行に移すべきである.

3.6 現行法の曖昧さと社会的受容度の判断基準

現行法の曖昧さが残る中で，どのような ACD なら許されるかを判断するのは容易ではないが，Center for Cyber & Homeland Security [2016] が考慮すべき要素として指摘している 5 点（p.26）を，共著者流にまとめ直すと，以下のようになる.

① 時間的要素：対抗策が攻撃前になされるのか，攻撃中か，それとも攻撃後か.（攻撃前は許されないとして）攻撃中にそれを止めようとする手段の方が，攻撃後に報復的に，あるいは成果物を取り戻すためになされる対抗手段よりも [59]，適法的だと考えられる.
② 目的あるいは機能的要素：脅威情報の収集目的か，インシデントの発生阻止か，ネットワーク攻撃を止めるためか，損害を緩和するためか，盗まれた資産（情報）を取り戻すためか，あるいは攻撃者に追加費用を負担させるためか.このコロラリーとして，データの機密性・完全性・可用性の，どの要素に影響を与えるか.観察やアクセスの方が，データの完全性打破やデータ破壊よりも受け容れられやすい.
③ 効果と空間的要素：対抗手段の及ぶ範囲が被害者のネットワークに閉じたものか，それとも攻撃者や第三者のネットワークにも及ぶのか.マルウェアの自動除去や脆弱性にパッチを当てることは望ましいが，善意の第三者のデータやネットワークの被害は補償しなければならない.クラウドやインターネットの特性から，行為者を特定することは難しく，特に

[59] 注 53 で指摘したように「情報法」ではなく「サイバー法」を構想する論者が多い米国では，「知的財産を取り戻す」ことを主張する者も（必然的に）多いし，現に IP Commission Report [2013] は，明確にその立場を採っている.しかし共著者は「複製による移転」と「情報流通の不可逆性」を与件とする「情報法」では，有体物のように完全に取り戻すことは技術的にも法的にも不可能なことだと考える.

悪意ある行為者がプロキシ―を使う場合はそうである.

④ 権限的要素：監視機関や法執行機関あるいはネットワークの保有者の許諾を得た ACD か否か.ボットネットの壊滅は，官民が協力して行なうものとして一般化しつつあるが，当初は法執行機関との協力の下，裁判所の令状を得て行なわれた.法執行機関等の政府機関は，民間企業がこうした協調行動を取れば，ACD をより好意的に見るだろう.

⑤ 負の影響の最小化要素：ACD の行為者に，効率を最大化し負の影響（他のシステムやネットワークへの偶発的損害や被害の拡大）を最小化する能力があれば，より好意的に見られるだろう.

ここで掲げられた諸点は，良く考えらえたものと思われる.しかし，ACD として検討対象にされた対抗手段が網羅的か，烈度の評価が適切かなどの問題点に加え，前述のとおり法的な根拠が曖昧なままでは，モヤモヤ感が残ってしまう [60] .

3.7 立法化の試みと挫折

米国においても，新たな立法によってモヤモヤを解消する努力があったが，その試みは現在までのところ挫折している.

直近の試みは，115 会期の下院に提出された Active Cyber Defense Certainty Bill（H.R. 4036）で，CFAA 1030 条等に以下のような例外条項を盛り込むものであった [61] .

① 被害者が attribution を明確にするためのデータを取得する行為には，データの破壊，コンピュータの基本機能の毀損，バック・ドアの設置などに該当しない限り，CFAA を適用しない，

② 被害者が attribution 情報を法執行機関と共有するため，攻撃者の継続的な違法行為を阻止するため，または予防目的で攻撃者の行動をモニターするために行なう無権限アクセスは，刑事訴追に対する抗弁になり得るが，民事免責は与えられない，

③ ただし上記の行為は，甚大な物理的損害や財務的損失を与えるものであってはならず，公衆衛生や安全に危害を及ぼしてはならず，attribution 目的であっても第三者のコンピュータに故意に侵入したり，偵察の必要レベルを超えてはならない，

④ ②の行為を行なうには，事前に連邦捜査局（FBI）に通報して，受領の通知を受けなければならない，

⑤ 本法は 2 年限りの時限立法とする.

しかし，これらの手法には連邦政府関係者からも懸念が表明され，下院の委員会には付託されたものの，採決するまでに至らなかった [62] .

---

[60] 注 49 で紹介した O’Connor の意見は，以下のように述べている.If policy makers draw only one lesson from the report， it should be that the “gray zone” between lawful and unlawful defensive measures must shrink. The current level of ambiguity between lawful and unlawful defensive measures poorly serves corporate， privacy， data security， national security， and law enforcement interests.

[61] https://www.govtrack.us/congress/bills/115/hr4036/text

[62] https://www.congress.gov/bill/115th-congress/jouse-bill/4036/all-actions?overview=closed#tabs

一方州レベルでは，ジョージア州で逆に CFAA を強化する法案が可決された[63].これは前年に同州で 750 万人もの有権者登録情報が漏えいしたことが発覚し[64]，規制強化派が議会の多数を占めたためだが，ディール州知事が拒否権を発動したため発効しなかった.こうした動きからすると，米国内には規制強化派と緩和派の両派があり，なおせめぎ合っているかに見える.

3.8 最新のサイバー戦略における対応

ところで，ホワイトハウスが新しい「サイバー戦略」を公表したことは 1.4 で紹介したが，それによって Center for Cyber & Homeland Security [2016] の提言が，どの程度具体化したのかを検証しておこう.

この戦略は 4 部からなるが，一般的な安全保障とは違うサイバーセキュリティについては，Pillar I: Protect the American People， the Homeland， and the American Way of Life に記述されている.この部分は 6 ページと短く見えるが，Pillar Ⅱは 4 ページ，Pillar Ⅲは 2 ページ，Pillar Ⅳは 3 ページしかないので，相対的に重みがあると考えられる.

Pillar Ⅰは，Secure Federal Networks and Information，Secure Critical Infrastructure，Combat Cybercrime and Improve Incident Reporting，の 3 節から成っており，第 2 節の Priority Actions として注目される記述には，以下の 2 点がある.

① The Administration will clarify the roles and responsibilities of Federal agencies and the expectations on the private sector related to cybersecurity risk management and incident response. (p.8)

② Information and communications technology (ICT) underlies every sector in America. ICT providers are in a unique position to detect， prevent， and mitigate risk before it impacts their customers， and the Federal Government must work with these providers to improve ICT security and resilience in a targeted and efficient manner while protecting privacy and civil liberties. (p.9)

これらは，前記提言のうち大統領府に期待されていた (8) に応えるとともに，(9) に間接的に含まれていた (1)～(6) の前進も図ろうとするもののように見える.しかし，具体性に乏しいので，どのような方針が出てくるかは今後の各省の動きを待つしかないだろう.本稿との関係ではむしろ，② において他のインフラストラクチャーよりも，通信インフラにより多くの期待がかけられているのではないかと思われるが，これまた今後の FCC 等の動きの中で明確になるまで待つしかあるまい.

[63] 可決された法案(SB 315)では，Any person who intentionally accesses a computer or computer network with knowledge that such access is without authority shall be guilty of the crime of unauthorized computer access. となっていた.
[64] 米国では選挙人名簿に登録しなければ，選挙権が与えられない.選挙には 2 大政党ごとの大統領予備選挙も含まれるので，必然的に支持政党に関する情報も登録されている.この情報は選挙を妨害したい攻撃者にとっては価値が高い.

4 米国法における問題点

4.1 問題点の摘出

O'Connor の補足意見（注 62）が代弁するように，ACD の適法性が明確でない中で書かれたためか，Center for Cyber & Homeland Security [2016] の本文には，現行法分析の視点は希薄である.その代り同報告書には，有力な法律事務所の 1 つである Covington & Burling， LLP によるコメントが，付属資料 2. として付けられている.

この分析は「簡にして要を得た」もので，そこに掲載された判例や参考文献を加え，更に肉づけを施せば，本稿の目的に応えられるであろう.以下，関連性が強い法律の順に検討を加えるが，1.7 で述べた方針に従い，国際法は除外する.

4.2 CFAA（Computer Fraud and Abuse Act of 1984）

ACD を検討する際に，最初に取り上げねばならないのは，わが国の不正アクセス禁止法にほぼ相当する CFAA である[65].同法 1030 条以降の unauthorized access などの禁止行為のコアとなる制約条件は，次のようにまとめられる[66] [67].

It is illegal for anyone who:

a) Accesses a computer without authorization or exceeds authorized access， and thereby obtains information from any protected computer（1030 条(a) (2)項）

b) Knowingly and with intent to defraud， accesses a protected computer without authorization， or exceeds authorized access， and by means of such conduct furthers the intended fraud and obtains anything of value（1030 条(a) (4)項）

c) Knowingly causes the transmission of a program， information， code， or command, and as a result of such conduct， intentionally causes damage without authorization, to a protected computer（1030 条(a) (5)項）

この条文は，攻撃者に適用することを前提に作られたものである.しかし，同じ条文は ACD にも適用されるので，以下のような制約条件となって現れる.

① この法律は「インターネットに接続していれば，いかなるコンピュータも protected computer に当たる」と非常に広く解釈する判決がある，

[65] 18 U.S.C. Section 1030 et seq. なお制定当初の法律名は Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 であったが，前者の部分は独立して 18 U.S.C. 1029 となった.

[66] 次項以降も含めて制約条件のまとめは原則的に Covington & Burling， LLP によるもので，読者が理解しやすいように条文をまとめているので，法律の原文に忠実とは限らない点に注意していただきたい.

[67] ただし CFAA に関する限り Kerr [2016] の記述の方が正確なので，それにより補正する.なお同論文は，CFAA 違反に対する実際の科刑は Federal Sentencing Guideline によっているが，fraud 中心の経済犯をモデルにしているので，trespass 中心の property モデルに改定すべきだと主張している.

② しかし他方で，authorization，without authorization や excessive authorized access に関しては曖昧さを残す判決もある，
③ そこで，aggressive cyber defense 手段（ACD とは別の概念であることに注意）のほとんど（多分，より中間的なものの一部も含めて）は，この法律に違反することになるだろう，
④ 例えば，盗まれた情報資産の取戻し・消去・変更や攻撃を避けるためのマルウェアの送信のための手段はいかなるものでも，unauthorized access と，当該コンピュータからのデータの取得や損害の発生を伴う可能性が高い，
⑤ それより烈度の低い，被害企業外のネットワークの観察やモニタリング，ビーコニングなどは，コンピュータにアクセスするものの，情報の取得や損害の発生を伴うものではないので，違法か否かは不明確である，
⑥ 上記の ① と ②の関係については，ACD のうち攻撃者のコンピュータやネットワークにアクセスし，データを取得したり破壊したりするものであれば，without authorization や excessive authorized access になり易い．

なお，法執行機関等が正規の手続きを経て行なうアクセスを，禁止するものではないとの為念規定がある（1030 条(f) 項）．

4.3 ECPA：Wiretap Act

次に関係が深い法律が ECPA（Electronic Communications Privacy Act of 1986）であるが，ECPA は Wiretap Act，Stored Communications Act，Pen Register Act と呼ばれている 3 部構成となっている．第 1 と第 3 の部分は，それぞれ独立に ACD と関わりがあるので[68]，まずは第 1 のものから分析する．Wiretap Act の第 2510 条は，次のように規定する[69]．

It is illegal for anyone to:

a) Intentionally or purposefully intercept (or endeavor to intercept), disclose or use the contents of any wire, oral, or electronic communication;
b) Intentionally or purposefully use (or endeavor to use) a device to intercept oral communication.
c) A “device” is any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than a telephone or telegraphy equipment given to the user by a provider of wire or electronic communication and used in the ordinary course of business, or a hearing aid or similar device.

この規定に抵触しそうな ACD として，例えばシンク・ホール化による偽アドレスへの転送（redirect）がある．転送以前に，不正な通信の内容を監視すれば，通信の傍受に当たる恐れがあるからである．ただし，既に同法には法執行機関が攻撃者の行動を監視する場合に，一定

[68] 実は第 2 の部分も関係するのだが，米国では（あるいは日本以外の先進国では）通信内容とメタデータは別扱いとなっているので，メタデータを扱う第 2 の部分を無視したのであろう．わが国ではそうはいかないので，この論点は第 7 章で再説する．
[69] 18 U.S.C. Section 2510 et seq.

の条件を満たせば（ネットワークの所有者や管理者が認めた場合や合法的な捜査である場合など）適法とする例外規定があるので [70]，これを拡大するか条件を追加していく道がある．

4.4 ECPA：Pen Register/Trap and Trace

第 3 の法である Pen Register Act には，次のような規定がある [71]．

ECPA prohibits anyone from:

a) Installing a pen register or trap and trace device without obtaining a court order (3121 条)，

b) A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication…” (3127 条 3 項)，

c) A “trap and trace device” is a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication…” (3127 条 4 項)．

Trap and trace 機器の禁止は，ハニー・ポットやシンク・ホールなど，侵入源を特定するために使われる，中程度の烈度の ACD 手段に影響を及ぼすだろう．この場合でも裁判所の令状があれば適法になるので，その分政府の役割が重要になろう．

4.5 Cybersecurity Information Sharing Act of 2015[72]

以上の法律は，ACD を実施する場合に何らかの支障になりそうなものであったが，逆に予め免責を定めた法律として，サイバーセキュリティ情報共有法があるので，その適用可能性を検討しよう．これは 2015 年末に，2016 年統合予算法の一部として制定され，5 部からなる「2015 年サイバーセキュリティ法」の最初の部で，最重要部分と考えられている（永野 [2016]）．

米国では従来から，事故情報を共有しようにも，1) 民間が政府と共有したデータが情報公開法によって開示されるのではないか，2) 共有データに含まれる個人データのプライバシーが心配だ，3) 競合会社と情報を共有することが独禁法違反とされる可能性がある，4) 提供情

[70] 18 U.S.C. Section 2511 (e) (f)
[71] 18 U.S.C. Section 3121-27
[72] この法律は Covington & Burling, LLP のメモには含まれていないので，この節の記述は，ほぼ林 [2016b] による．なお図表 1 の ⑥ で示した「国家の（暗黙の）関与」をも念頭におけば，更に多くの法律が関係してくるが，ここでは省略する．詳しくは Garrier & Reeves [2016] を参照されたい．

報が元になって違法行為を指摘される危険がある，といった懸念があって，共有が期待通りに進まなかったといわれる.

この法律は，上記の 4 点の懸念を払拭するためのもので，独禁法上の免責に加えて，民間企業が情報ネットワーク・システムをモニタリングすることや，政府と CTI（Cyber Threat Indicator）や DM（Defensive Measures）に関する情報を共有したことで，裁判で訴追されることはないことを保証している.そして，これらの免責規定を民間から政府へ情報が提供されるインセンティブとするほか，政府側も機密指定の情報をセキュリティ・クリアランスを条件に民間に提供するなど，互恵的な仕組みを作っている.

ここで共有される情報には，上記のとおり 2 種類ある.まず CTI は，次の 8 つの態様を含むものとされる.1）脆弱性情報の収集などの偵察，2）脆弱性の利用の仕方，3）脆弱性を前提にした特異な行動，4）ユーザの合法的アクセスによってセキュリティ管理を破る方法，5）悪意の C&C（Command & Control），6）秘密裏に盗み出された情報など顕在・潜在の被害，7）法によって禁じられていない，その他の特性，8）これらの組み合わせ.

もう 1 つの情報は DM で，既知または疑わしい脅威または脆弱性を，探知・予防または軽減するために，情報システムまたは情報そのものに，保存・処理・送信された情報に適用される行為で，デバイス・手法・シグナチャー・技術・その他の方法をいう.ただし，他者の情報システムまたは情報そのものを破壊し，不正なアクセスを可能にしまたは重大な害悪を及ぼすものは含まれない.

また本稿との関連では，同法が「自身のネットワークはもとより，委託を受けた他者のネットワークも，サイバーセキュリティのためにはモニターでき，defensive measures を取ることも許される」と明記したことが注目される.該当の条文のうち，民間企業に関する部分のみを摘記すれば，以下の通りである.

SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

an information system of such private entity;

an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

an information system of such private entity in order to protect the rights or property of the private entity;

an information system of another non-Federal entity upon written consent of such

entity for operation of such defensive measure to protect the rights or property of such entity;

しかも，こうした情報共有やモニタリングによって，法的責任を追及されないとする免責規定もある.モニタリングに関する部分だけを摘記すれば，以下の通りである.

SEC. 106. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 104(a) that is conducted in accordance with this title.

これらの規定を見ると，わが国の場合に比べて，免責条件が広く明確であるかに見受けられる.しかし Center for Cyber & Homeland Security [2016] によれば「法的な不確実性が残っている」というのだから，判例法の国である米国が他方で due process of law の国でもあることを感じさせる[73].

4.6 Common Law Theories of Trespass

米国は英国と同様，多くの紛争が裁判所で処理され，それが蓄積して判例法となっている.そのうち，原則に基づく処理は common law と，例外処理は equity と呼ばれる.近年では社会の複雑化に対応して制定法が増えているので，判例をまとめた上でその共通点を restatement という文書にして，各州が立法化を図る際の参考にしている.しかし，立法ではカバーされない事態に対処するため，common law の原則に直接依拠した判決が出されることもある.

サイバー事案で最も頻繁に使われるのは，trespass to chattel（動産に対する侵害）である.これは不動産に対する trespass（不法侵入）の法理を動産にも拡大したもので，現行の restatement である Restatement (Second) of Tort では，‘intentionally----dispossessing another of the chattel, or using or intermeddling with a chattel in the possession of another’（217 条）とされている.したがって，侵害を主張する側は 1）故意，2）動産に対する介入，3）実際の損害，を証明しなければならない[74].

この法理は一旦 conversion の法理[75] の陰に隠れたように思われたが，長距離電話の料金を免れる不正アクセスに適用されて生き返った[76]（Guzman [2010]）.サイバー事案の具体例としては，スパム・メールがサーバーの許容度を超えたとして認めた例（CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997)），継続的・自動的で受信者が望まな

[73] Due process of law とは，一般的には刑罰を受ける手続きと実体がともに適正であることが要求されるという法理で，罪刑法定主義と並ぶ刑事法の大原則である.米国では憲法修正 5 条が，連邦政府に対し適正手続なしに個人の財産等を奪ってはならない旨定め，修正 14 条は州政府に対し同様の適正手続の保障を要求するので，両条文の効力は刑事事件のみならず，民事事件にも及ぶ.

[74] 初期の判決では，3）を不要とする eBay v. Bidders’ Edge 判決（100 F.Supp.2d 1058 (N.D. Cal. 2000)）もあったが，Intel v. Hamidi（30 Cal. 4th 1342 (2003)）以降は実害が必要との解釈が一般的であるが，なお異論もある.

[75] わが国の概念では「横領」が最も近いように思われる.

[76] Thrifty-Tel., Inc. v. Bezenek, 54 Cal. Rptr. 2d 468（Ct. App. 1996）

いアクセスについて認めた例（Register.com, Inc. v. Verio, Inc., 356 F. 3d 393 (2d Cir. 2004)）などがあるが，特定の個人を相手に裁判を起こすのは容易でない．

4.7 Common Law Theories of Negligence

コモン・ローの理論として，もう1つしばしば議論されるのが，過失としての注意義務違反で，これは ACD に関して抗弁となるよりも，それ以前に「被害が生じないように十分に配慮したか」という注意義務を問われることになる．注意義務としては，大別して特定の業務に従事する者の善管注意義務と，契約上の義務違反に分かれ，さらに（一般的な不法行為と同様）因果関係や，損害発生の有無などが問題になる．

近年，この分野で議論が高まっているのが，ボットネットからの攻撃に関して，誰が責任を負うべきかに関するものである．コンピュータの所有者，ISP，ソフトウェア・ベンダのいずれもが候補になり得るが，とりわけ「ISP に責任を負わせるべきだ」とする主張が注目されている．

しかし被害者が善管注意義務違反を主張し，因果関係を証明するのは挑戦的な作業であるのに加え，ISP は約款等に免責条項を定めて責任を逃れようとするだろう．また，攻撃者に盗まれたデータを取り戻すためや，ネットワークとコンピュータへの実害を回復するための論拠とはなり得ない．

4.8 Self-defense of Property と Necessity[77]

広義の自力救済の一種であるが，特に不動産や動産の自己防衛（self-defense of property）が認められるか，という議論がある．自身の動産を守るために，他人の行動に介入することが許される場合があることは，restatement も次のように述べて，これを認めている．

“one is privileged to commit an act which would otherwise be a trespass to a chattel or a conversion if the act is, or is reasonably believed to be, necessary to protect the actor’s land or chattels or his possession of them, and the harm inflicted is not unreasonable as compared with the harm threatened.”（260 条 1 項）．

サイバー攻撃の被害者である企業は，この条項を援用することができそうだが，Kesan & Hayes［2012］は，その時点ではこの法理を抗弁として用いたケースはないという．おそらく，他の不法行為要件に該当するか，CFAA 違反を問われる危惧もあるからであろう．なお米国では lease と license を明確に区分する伝統があり，前者については借主が厚く保護され，貸手が強制的に（例えば部屋の鍵を変えてしまうなどの方法で）借手を閉め出すと 3 倍賠償を命じられることさえある[78]．他方 license の場合には全く逆で，平和的手段であれば，貸手が借手の意に

[77] この法理は Covington & Burling, LLP のメモには含まれていないので，この節の記述は主として Huang［2014］による．なお，この法理の適用例として，後に 6.4 で紹介するソマリアの海賊対策がある（Hoffman & Levite［2017］）．
[78] ニューヨーク州法にある RPAL 853（New York’s Real Property Actions and Proceedings Law Section 853）が顕著な例である．

反して取り戻すことも可能とされている[79]．

また，わが国の「緊急避難」に類似の概念として，necessity の法理がある.これは 1）遅滞を許さないほどの急迫または強度の権利・利益の侵害があり，2）必要最低限の救済手段であり，3）平和を破らない範囲に限り，4）法的な救済に訴える時間を許さないほどの間に実行される，の 4 条件を満たすものとされる.

ACD に関して，これらの法理で身を守ることができるのは，被告が抗弁（legal defense）として利用するという受け身の場合に限られるだろうから，こうした規定があることが ACD を実行する上での安心材料にはなり得ないだろう[80]．

4.9 Cyber Nuisance を加えた仮のまとめ

上記のコモン・ロー上の諸概念のうち，Trespass の法理が有体物の所有権を模したものであるのに対して，Negligence は権利・義務関係にない当事者間においても損害賠償責任の発生を認めるものであり，Calabresi & Melamed [1970] の有名な分類によれば前者が property rule，後者が liability rule の代表格になる.そして米国の主流派は trespass を推しているが，negligence こそ，サイバー時代の解釈の中心になるべきだとの主張もある（Guzman [2010]）.

以上の諸概念のほかに，Nuisance の法理も考えられる.これは negligence の一類型ともいえるが，加害行為の過失証明の軽減や，さらには無過失責任の可能性なども含めて，公害など近代的な不法行為（原因行為の特定の困難さ，複合汚染の存在，被害者の広汎さなどの点で，従来のものとは異なる）に適用されて発展してきた.

そこで Guzman [2010] が行なった，Trespass，Nuisance，Negligence の 3 つの法理の比較（pp.552-557）を，共著者流に以下のようにまとめてボットネットや DDoS 攻撃などに当てはめると，次のような知見が得られ理解が深まるように思われる.

① trespass を所有権類似の強い排他権として認めると，アクセスを拒否できる範囲が広がりすぎて anti-commons 状態となると同時に[81]，被害者に攻撃者の意図を証明する責任を課すことになり，救済の道をも閉ざす.

② nuisance はネットワーク時代の不法行為に適した理論ではあるが，論者の多くがサーバーを不動産に見立てて議論している.これは上記の欠点を含むものになってしまう.

③ negligence は既に確立された法理であり，攻撃者の不法行為と防御者の防御義務を比較衡量して判断することができる.trespass 派には従来の「権利と義務が対になっ

[79] これは「property とは何か」という論点と関連するようで，lease では借手に property が移転するが，license では貸手に残ると考えられているようである（林 [2010] 参照）.
[80] 以上のほか，CATV がネットワークと並んで主要なインターネット・アクセス手段である米国では Cable Act も主要な法源となる（Harrington [2014]）が，ここでは省略する.
[81] 「コモンズの悲劇」（牧草地を共有にしておくと，家畜に牧草を食べさせる人が増えて，コモンズが維持できなくなる）は有名だが，ソ連邦崩壊後には「アンチ・コモンズの悲劇」として，所有権が不完全な排他性しか与えないと取引が成り立たないことも知られている.

ている」点で受け入れられやすく，nuisance 派にも「ボットネット被害などの社会的コストを内部化する」という点で相性が良い.

上記の指摘のうち，最後の ③ は，前段が被害企業の自力救済を部分的に容認する根拠として，後段が cyber hygiene を理由づけるとして使えるのではないかと考えるが，ここではとりあえず，上記の議論を図表 6. として仮にまとめるにとどめ，具体的提案は第 6 章までお待ちいただきたい.

図表 6　Cyber Nuisance を加えた自力救済適法化法理の仮のまとめ

適法化の法理		概要	長所	短所	主たる提唱者
立法	CFAA の適用除外	立法により CFAA の適用除外条項を定める	正当な範囲が明確になり安心して対抗手段が取れる	正当な範囲が狭められる，技術が先に進んでしまうといったことがある	Huang [2014]
	ECPA の適用除外	同上	同上	同上	
	CISA の拡張	立法により情報共有の違法性の懸念を払拭する	情報共有の合法性が保障され安心できる	保証されるのは情報共有だけで，他の対抗手段に及ばない	
コモン・ローの解釈	Trespass to Chattel	この法理を裁判で積極的に援用し勝訴を増やす	立法プロセスを経ずコモン・ローの伝統の中で解決できる	判例を増やすのは立法以上の時間がかかる.また有体物アナロジーを引きずる	Epstein [2005]，Kerr [2016] など
	Self-defense of property	同上	同上	同上.特に有体物アナロジーには抵抗感がある	
	Nuisance	同上	同上	前段は同上.後段は有体物アナロジーから離れるので裁判で認めてもらうのに努力を要す	Kam [2004]
	Negligence	同上	同上	同上.ただし nuisance よりは説得しやすい	Guzman [2010]
	Necessity	同上	同上	抗弁にはなり得ても積極的適法化理由にはならない	

4.10 上記の分析と提言との関係

これまでの記述から，適法性に関するモヤモヤ感（3.6）が払拭されたかとなると，はなはだ心もとない.Center for Cyber & Homeland Security [2016] もその辺りは心得ているようで，前述のとおり本文では ACD の社会的受容度の 5 基準を上げるにとどめ，法的な検討は Covington & Burling, LLP のメモに委ねている.共著者がさらに進んで，提言部分を先に紹介し分析部分を後回しにしたのも，同様の配慮からであった.

それでは提言と法的な検討は，どのように結びついているのだろうか？ 私たちの分析は以下のとおりである.

① 現行法の解釈だけでは解決できない問題が多いので，有権解釈あるいは行政指針による明確化が不可欠との認識を共有している（提言(1)(2)），
② ソフト・ローや，研究開発・標準化などの分野でも，行政のリーダーシップに期待している（提言 (3)(4) (5) (6) (8) (9)）
③ しかし，なお残る疑問点に関しては，立法化を促している（提言 (11)(12)）
④ 民間企業には ACD へのコミットメントを促し，業界全体の国際協調の展開を期待している（提言 (13)(14)(15)）
⑤ ACD を促進することによってプライバシー侵害などの懸念を払拭するような仕組みに配慮している（提言 (7)）
⑥ 全体像の把握と進捗管理を大統領と議会の双方に期待している（提言 (9)(10)）.

なお提言そのものではないが，2.3 で紹介した第 1 章の記述から間接的に，以下の取り扱いが暗示されていると考えられる.

⑦ ACD については，技術的条件が重層的に作用し，かつ変化が激しいので，法的な取扱いを細部まで規定することはできない.Self help として実施可能なものと，政府との協調行動の場合に限って適法と考えられるものに 2 分する程度の，大まかな分類が妥当と思われる.

上記の検証によって，サーバーセキュリティの分野ではソフト・ローの役割が重要であること，逆にハード・ローの役割は限定的であること，しかしなお，ハード・ローが最後の拠り所であることが明確になったのではないかと思われる.ただし ⑦ 項については，attribution 問題を改善にするためのビーコンなどを，優先すべきではないかと考える.

最後にここまでの検討結果を，国際法の枠組みも踏まえて，最大公約数的に大胆に要約すると，①「武力の行使」（use of force[82]）に至らない違法行為には，② 均衡性のある対抗措置が許される（比例原則[83]）が，③ 他人に危害を及ぼしてはならない（危害防止原則[84]）という

[82] 国際関係において武力に訴えること.国連憲章下においては戦争だけでなく，国連の目的と両立しない一切の武力の行使が禁止され，さらに武力による威嚇 threat of force すなわち武力の行使をほのめかして自己の要求を実現することなども一般に禁止される.
[83] 達成されるべき目的とそのために取られる手段としての権利・利益の制約との間に均衡を要求する原則.
[84] 個人の自由は最大限に尊重されなくてはならず，自力救済が認められる場合でも，他人に危害を及ぼしてはならないという原則.

 もので，米国のコモン・ローも，同じような含意を持っていると考えられる.

5 日米比較とわが国における検討

5.1 CFAA と不正アクセス禁止法との対比

コンピュータに不正に侵入する方法には種々のものがあり，年々複雑化・巧妙化しているのに対して，法的な整備は遅れがちであった.その傾向は各国とも同じであるが，総じていえばコモン・ローの国の方が，制定法の国よりもキャッチ・アップが早い印象は否定できない [85] .裁判所は現に起きているケースを，なるべく早く裁かなければならないが，立法府が法律を制定するには，時間がかかることが多いからである.

しかし，米国の CFAA が 1984 年の制定であるのに，わが国の不正アクセス禁止法が 1999 年に制定されたという 15 年の差は，上述の法の起源や，経済力・情報サービス産業の差だけでは説明できない.そして，両者を個々の項目ごとに比較（図表 7）してみると，以下の 3 点においてわが国の法制が，制定年度の遅れをなお取り戻していないように見える.

まず第 1 に，CFAA では，いかなるコンピュータへの不正侵入も対象となり得るのに対して，わが国の不正アクセスの範囲（アクセス制御機能付きのコンピュータに，不正取得した識別符号を入力することや，制御による制限を免れる情報を入力することによって，利用可能にする行為.同法 2 条 4 項，3 条）が狭すぎることである.いたずらや能力誇示（愉快犯）が主流であった時代ならともかく，経済的利益の搾取や政治的プロパガンダなどが主目的となっている現在のサイバー犯罪に対処するには，これでは狭すぎるだろう.

第 2 に，CFAA が侵入を与件として，侵入後の対策を主眼に策定されているのに対して，不正アクセス禁止法が（法律の名に反して）アクセス以前の ID 等の窃取に重点を置いていることが目につく（第 ① 項）.事前対策を重視するのは悪いことではないが [86] ，ID 等の窃取を事前に防止するのは不可能に近い.サイバーの世界では「時間」こそ最大の要素なので（図表1の ② 参照），インシデントの発生はやむを得ないこととして，その後「後手」に回るのを回避するために，attribution 問題の改善により多くの時間資源を投入すべきではないかと考える [87] .

加えて第 3 に，CFAA においては国家安全保障やインテリジェンスのための適用除外や正

[85] 法制度が経済効率にどのような影響を与えるかを分析する理論の 1 つが LOT（Legal Origins Theory）で，Porta et al. [2008] はコモン・ローの一般的優位を主張している.しかし第 4 章で見たように property rule に固執することが，情報に対する関心を薄めることにもつながるので，断定的なことはいえない.

[86] これは「専守防衛」を主眼とする，わが国の防衛政策とも符合するので，事前と事後を対比して選択した結果ではなく，平仄を合わせただけではないかと懸念される.

[87] わが国では個人情報保護法（共著者はこの法律の基本は「個人データ保護法」だと思っている.林 [2017] 参照）への過剰な反応もあって，個人データの漏えい・流出がメディアで頻繁に報じられ，その後の窃用を「なりすまし」として区分している.米国では漏えいと窃用を一体として ID theft と呼んでおり，それ自体が犯罪化されている（Identitiy Theft And Assumption Deterrence Act of 1998）.ただし「米国では情報窃盗という犯罪がある」というのは誤解で，ID 以外にも窃用はかなり広範囲に罰せられるが，知得が罰せられるのは知的財産だけである.

当化（違法性阻却）事由が考慮されているのに，不正アクセス禁止法では，そのような配慮が希薄であることが気になる.サイバー犯罪は，今や国家の関与が疑われる事案も多く，サイバー・テロにもつながる危険があるので，官民の協力がなければ attribution の解明もままならないことは，1.3 で触れたとおりである.

図表 7　CFAA と不正アクセス禁止法の対比

比較項目	CFAA	不正アクセス禁止法
①禁止行為	コンピューター一般に対する権限外アクセス，コンピュータ詐欺，コンピュータ損壊（識別符号の不正取得は ID Theft として詐欺に該当すれば，刑法を適用）	アクセス権の元となる識別符号の不正取得等，アクセス制御されたコンピュータへの権限外アクセス（コンピュータ詐欺とコンピュータ損壊は，刑法を適用）
②被害者の防御義務	義務規定なし（ただし due diligence など common law 上の一般的義務は課されるものと思われる）	アクセス管理者は識別符号等の適切な管理やアクセス制御機能の維持向上の努力義務がある（罰則はない）
③適用除外と正当業務	法執行やインテリジェンス活動には適用しないことが，CFAA の中で規定されている.また国家安全保障とインテリジェンスにかかわるもの（研究開発を含む）であれば，他の法律や大統領令などで違法性が阻却される	米国のような適用除外規定がなかったが，今回の NICT 法の改正によって適用除外の例ができた.またアンチ・ウイルス・ソフトの開発のためであっても，米国のように明確な違法性阻却とならない
④刑の長期	連邦量刑ガイドラインにより刑が加重・減刑されるため，最長 35 年になるとの計算もある[注]	3 年以下の懲役
⑤抑止効果	年平均 100 件程度の起訴では抑止にならないとの主張がある	近年では年 200 件程度の起訴があり，それなりに機能しているが，3 年以下の懲役では効果が薄い
⑥ID 窃盗	ID の取得と窃用は併せて ID theft として犯罪化され，FTC 等に届ければ支援が受けられる	情報は窃盗の対象とならないとされるので，専ら個人データや知的財産の範囲内で保護される

（注）ただし Kerr［2016］のように，経済犯（fraud）をモデルとした量刑指針では問題が多いので，財産権侵害犯（trespass）モデルに変更すべきだとする主張がある.

こうした両国の差を，自力救済という視点から再整理すると，日本法の方が，アクセス制御を基本とした入口防御に力点があるため，防御措置（8 条）そのものが自力救済に依存しており，さらに入口が破られて以降は法定救済手段が明記されていない結果，自力救済に頼らざるを得ないことになっている.つまり，他の法分野では「自力救済」を厳しく禁止しているわが国の方

が，ことサイバーの世界になると二重の意味での「自力救済依存」（その実は「打つ手なし」）体制なのである.

5.2 民事訴訟に関する日米の法文化の差

CFAA と不正アクセス禁止法の対比は比較的容易であるが，それ以外に第 4 章で検討した米国法を，わが国の法制と個々に比較することは容易ではないし，「労多くして益少なし」という結果に終わるだろう.そこで，本稿のテーマが民間企業の対抗手段であることから，図表 8 を使って，民事を中心にした「日米の法文化の差」について，ごく簡単に付言するにとどめよう.既に述べた匿名訴訟を含めて，大きな差は 4 点ある.

図表 8 民事を中心にした日米の法文化の差

比較項目	米国	日本
①匿名訴訟	認められる	認められない
②職権による証拠の収集	Discovery と subpoena の制度により，裁判所主導で証拠を集める仕組みがある（当事者に提出義務がある）	証拠の収集は原告と被告に任せられており，職権による収集や開示は限定的である
②’②に対応する証拠保全義務	個人はともかく法人は，証拠を保全して「自分の身は自分で守る」ことを期待される	公文書管理の杜撰さに見られるように，証拠として「メモを取る・記録を残す」という文化が定着していない
③IT を使った証拠固め・分析	デジタル・フォレンジックとして日常的に行なわれている	裁判手続き全体を通じて，IT の活用の最初期段階にある
④損害賠償額の上限	懲罰的損害賠償として，実損を超える賠償が認められることがある	実損額を超える賠償は認められない

上記のうち共著者が特に注目しているのは，② と ②’が対になった制度であり，その基本は discovery といって「原告と被告がお互いの証拠を出し合わなければならない」「第三者が証拠を持っている場合にも，裁判所は職権で証拠を集めることができるし，両当事者はそれを請求できる（違反には刑事罰を科す）」という仕組みである.

言い換えれば，米国の制度は「公正な裁判のために，できるだけ広く証拠を集めて判断する」必要があり，そのため「税金を投入することを厭わない」という建前で成り立っているのに対して，日本の制度は「訴訟当事者が自助努力で証拠を集めるべきで，税金を投入するなど考えられない」という対照的な差となって現れている.

この制度は「紙」が証拠の中心だった時代に発展したものだが，電磁的媒体が主流になった時代に対応するように改正され（e-discovery と呼ぶ），今日では弁護士事務所の作業における比率も高まっている.コンピュータを用いた分類や分析が主体になるので，その結果は

forensic 技術と結合して，新しい証拠論を形成しつつある.

もちろん，それには膨大な作業を伴うから，ただでさえ「訴訟社会」の弊害が目立つのに，更なるコストの増大を招くのではないかとの批判が絶えないし，クライアント側が悲鳴を上げているとの報道もある.しかし，インターネットというサイバー空間を使った活動が増えるにつれて，intangible な活動を「目に見える」形に整えなければ，公正な裁判にならないのだから，このトレンドは今後も続くものと思われる.

そして，こうした制度の背景には「メモを取る・記録を残す」という習慣が根付いている米国と，公文書管理法はできたものの，未だに何が公文書であるか決められないわが国の発想の差が横たわっている[88] .それが延いては attribution 問題の解決に影を落としているように思われてならないが，この点に深入りする余裕はないので，関連の文献を参照願いたい[89] .

5.3 サイバー防御を強化するための法改正と「積極的サイバー防御」

ところで自助努力の元になるのは，「情報の非対称性」の克服，すなわち「情報の共有」である.ACD というと何となく勇ましいが，その第一歩が「情報の共有」であることは，本稿の一貫した認識である.

そこで内閣情報セキュリティセンターの主導で，「サイバーセキュリティ基本法」を改正して，「サイバーセキュリティ協議会」という連絡調整機関を作ることが提案されていることに注目している[90] .これに先行する形で，総務省は「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部改正法」を提出し，こちらは既に成立している[91] .後者の法律は本項では NICT 法と呼ぶ.

改正電気通信事業法では「第 7 節 認定送信型対電気通信サイバー攻撃対処協会（第 126 条の 2～第 116 条の 8）」を新設した.（以下，協会と呼ぶ.）「送信型対電気通信設備サイバー攻撃」の定義は「情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する攻撃のうち，送信先の電気通信設備の機能に障害を与える電気通信の送信（当該電気通信の送信を行なう指令を与える電気通信の送信を含む.）により行なわれるものをいい，電気通信事業者がその業務上記録している通信履歴の電磁的記録により，送信元の電気通信設備を合理的に特定できる場合に限る.」となっている（電気通信事業法 116 条の 2）.

この規定は電気通信事業者による攻撃通信の発生の防止を図るために，協会が C&C サーバー等に関する情報を集約し，分析・検証した上で電気通信事業者との間で情報共有を図ろ

[88] 林は学者になった初期に，1950 年から 2 年 2 か月しか存在せず郵政省に吸収された「電波監理委員会」の歴史を調べたことがあったが，先行研究が充実していることに驚いた.その理由の大半は，GHQ が克明なメモを残していたからであることは，容易に推測できた.

[89] 林 [2017] pp. 274-282 およびそこで引用されている諸文献を参照.

[90] https://www.cas.go.jp/jp/houan/180308/siryou1.pdf 残念ながら前期の国会では成立しなかったが，継続審査とされているので，早期の成立が待たれるところである.

[91] http://www.soumu.go.jp/menu_hourei/k_houan.html

うとするものである.協会が「通信の秘密」に該当する情報を扱うことから，法改正を行なって協会の設立の手続き，業務及び役職員の「通信の秘密」に係る規定を置いている.なお，「通信の秘密」に関する規定については，7.2.4 において述べる.

また改正 NICT 法では，5 年間の時限措置として，パスワード設定に不備のある IoT 機器の調査（特定アクセス行為）を NICT が行なうことができる規定を新設している.この調査結果を協会経由で電気通信事業者に情報提供して，情報提供を受けた電気通信事業者は，パスワード設定に不備のある機器に係る利用者を特定して注意喚起を行なうとの仕組みになっている.NICT の行なう調査行為は，不正アクセス禁止法に該当する行為であるため，不正アクセス禁止法の特別法として NICT 法を改正したものである.

他方，経済産業省は， サイバー対策が一企業内にとどまらず，グループ企業や部品・材料の供給先なども含めた「サプライ・チェーン全体」として確保されていなければならない時代になったとの認識の下で，企業間で営業秘密をシェアする場合に準じて，こうした情報も「限定提供データ」として不正競争禁止法で守る改正案を国会に提出し，これも成立している [92] .グループ企業間で「脆弱性情報」を共有すれば，この規定で守られるのではないかという見方があるが，その細部は検討中のようである.

こうした法改正は，新戦略（2018 年のわが国の「サイバーセキュリティ戦略」）における ACD を先取りしたものともいえる.共著者は新戦略の評価すべき点は，次の 3 点と考えているからである.

①「積極的サイバー防御」の観点から，目的達成のための施策の 3 番目である「国際社会の平和・安定及び我が国の安全保障への寄与」の 4.3 項が，現行の戦略よりも具体的かつ詳細になり，その概念が第 2 の目標である「国民が安全で安心して暮らせる社会の実現」にも及ぶことが明示され，方向性が明確になった，

② インシデント情報の共有について進展が見られることにも，注目している.電気通信事業法等の一部改正法は既に成立し，前述のとおり情報通信研究機構で IoT 端末等の脆弱性を探知し，その情報を資格のある電気通信事業者等と共有する仕組みが導入された，

③ 別途創設される予定の「サイバーセキュリティ協議会」には，中央官庁・地方自治体・重要インフラ事業者・サイバー関係事業者，教育研究機関などが，横断的に参加することが想定されている.産業や分野の壁を超えるのみならず，同種の海外の機関との連携等を通じて，セキュリティ対策の第一歩である情報共有を抜本的に強化するものと思われる.

このコメントのうち ① は，まさに本稿執筆の動機となったものである.なぜなら片方で，この指摘こそ旧戦略に比べて著しい進歩であると感ずる反面，「積極的サイバー防御」の具体的内容は必ずしも明確ではなく，特にどのような手段なら適法かが分からないため，結果として本稿の主題である民間企業には適用されないのではないか（あるいは民間企業が萎縮して手

[92] http://www.meti.go.jp/press/2017/02/20180227001/20180227001.html

段を取らないのではないか)，との懸念を抱いたからである.

「新戦略」の「目的達成のための施策」は「経済社会の活力の向上及び持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安定及び我が国の安全保障への寄与」の 3 つに分類されている.ごく大雑把に集約すると，経済・社会・国家の視点であると言い換えても良かろう.この最後の「国家の視点」において「積極的サイバー防御」が最も強く要請されることは疑いがないが，経済と社会が不可分に結びついている現代においては，民間企業(特に重要インフラ事業者)の役割が重要であり，そこにも「積極的サイバー防御」が求められるはずである.

5.4 「サイバーセキュリティ庁の創設を」という提言

そのような懸念に応えてくれたのが，笹川平和財団(安全保障事業グループ) による「日本にサイバーセキュリティ庁の創設を！」という提言(2018 年 10 月 29 日)であった(笹川平和財団 [2018]).同提言は，まず現状認識として図表 9 のような国際比較により，わが国のサイバーセキュリティ政策を相対評価している.

図表 9 における個々の評価に深入りすると，個別の項目ごとに ○ が正しいか △ か，といったエンドレスな論争になりそうなので避けておきたい.個別項目の評価は別にして，総体としてわが国が比較劣位にあるという認識は，共著者自身の見方(林 [2016b])や，調査結果(田川・林 [2017b])とも符合するもので，現状認識という面ではほぼ異論がない.

図表 9 先進各国のサイバーセキュリティ政策の比較

各国のサイバーセキュリティ戦略		英	米	独	仏	日
体制整備	1. 国家戦略に政府の主体的な役割が明記されているか	○	○	○	△	△
	2. 様々なサイバー攻撃への対処が一元化されているか	○	○	○	○	×
	3. 機動的なサイバー攻撃対処体制が整備されているか	○	△	○	○	×
法制度	4. 政府によるサイバー脅威情報の収集を認める法律があるか	○	○	○	○	×
	5. 重要インフラ事業者にサイバーインシデント報告義務があるか	○	△	○	○	△
	6. 重要インフラ事業者にサイバーインシデント連絡担当者の必置規制があるか	○	△	○	○	×
	7. 政府によるプライバシー侵害を監視する独立機関があるか	○	○	○	○	×

人材育成・産業育成	8. サイバーセキュリティ機関が実施する産業育成プログラムがあるか	○	○	△	△	△
	9. サイバーセキュリティ機関が実施する人材育成プログラムがあるか	○	○	△	○	△

このような国際比較による自己点検を踏まえ，笹川平和財団［2018］は，以下のような結論を導いている（「報告書要旨」から.アンダーラインは原典）.

「欧米先進国においては，政府がサイバーセキュリティに主体的な役割を果たすとともに，①サイバー攻撃に一元的に対処する体制整備，②サイバー脅威情報の収集及び重要インフラ事業者のサイバーインシデントの報告に係わる法整備，③政府によるサイバーセキュリティ人材と産業の育成，が着々と進められている.

これは，国家を背景としたサイバー攻撃の激化や国家レベルで開発されたサイバー攻撃ツールの拡散といった，日々増大するサイバー脅威への対応は民間の努力だけでは限界 との認識が欧米各国で共有されていることによる.しかしながら，日本においては，サイバーセキュリティは基本的に民間企業の責任であるとし，各省庁は所管の範囲内で最大限の努力をしているものの，縦割りによる対応には限界があり，人材育成・産業育成も不十分である.これでは重要インフラへのサイバー攻撃に的確に対処することも，政府の機密情報を守ることも，国民の生命と財産を守ることも困難である.」

そして，次の 3 点の具体的提言をしている.

① サイバーセキュリティ庁の設置

サイバー攻撃に一元的に対応する実務機関として，現行の内閣サイバーセキュリティセンターを発展的に改編・強化して内閣府外局にサイバーセキュリティ庁を設置し，サイバー攻撃の検知・分析・判断・対処までを一元的かつ迅速に行なう.

② サイバー攻撃に対処するための法整備

サイバーセキュリティ基本法を改正して「サイバーセキュリティ」の定義をより広義なものに見直すとともに，政府の主導的役割を明らかにし，併せてサイバー攻撃に対処するための関連法の一括改正を行なう.また，政府によるプライバシー侵害を監視するための委員会を国会に設置する.

③ 人材育成・産業育成のためのエコシステムの整備

サイバーセキュリティ人材とサイバーセキュリティ産業を育成するため，サイバーセキュリティ特区を新設して技術開発と産業育成を行なうとともに，初等教育から専門教育，社会人教育までのサイバーセキュリティ教育体制を整備する.

そして，これらの提言を達成するためには，従来の PDCA（Plan-Do-Check-Act）に代わって，OODA（Observe-Orient-Decide-Act）サイクル [93] を重視すべきことを提案している.これは，

[93] OODA は，朝鮮戦争に従軍したボイド大佐が，航空戦の経験から生み出しとされるモデルで，軍関係者には広く知られているが，PDCA のように標準化の世界で広く使われているモデルとは異なる.

PDCA では 1) Plan 機関と Act 機関が離れすぎている，2) それでは想定外を含むインシデントに即断・即決ができない，の 2 点で本稿の主題である ACD への要諦が強まっていることともつながる要素があり，検討に値する.

しかし提言が「機能論」よりも「組織論」を重視している点が，気がかりである.もちろん国家の機能が効率的・効果的に果たされるためには，組織が明確になっていることが重要であることは否定できない.しかし，組織を一元化すればすべてが解決する訳ではなく，組織が立派でも内部が腐敗したり非効率に陥っている例は枚挙にいとまがない.

最も懸念される具体的ケースとして，緊急事態への対処や NISC と国家安全保障局との関係などを考えて見よう.なるほど現在の仕組みでは，NISC は内閣官房に属し，その長（内閣サイバーセキュリティセンター長）は，3 人いる内閣官房副長官補の 1 人である.これは恒久的な組織とは趣を異にし，政策を決定し実行する機関ではなく，調整機関と呼ぶのがふさわしいと思われるだろう.

しかし，仮にその提言が実現した場合に，現状が改善されるかというと，緊急事態への対処や NISC と国家安全保障局との関係では自信がない.なぜならセンター長は危機管理担当でもあり，国家安全保障局の次長も兼務している.つまり「組織」を「人」で補っている.提案では，これらの調整問題は「組織論」としては改善されそうに見えるが，組織は人で動いており，官邸全体の調整力は無視できないからである.

この点を言い換えれば，提言においては「組織論」に終始した感が否めないので，それと同程度に「機能論」を掘り下げて欲しかった，ということになろう.その際に，OODA モデルの妥当性が同時に議論されることになろうから，両者相まって次期サイバーセキュリティ戦略の有力な検討資料になることが期待される.ひょっとすると，欧米比較が重視されがちな政策論に対して，わが国の組織風土にふさわしい「日本型サイバーセキュリティ戦略」を見出すことができるかもしれない.

サイバーセキュリティは，ほぼ全官庁に係るテーマであり，官邸全体の調整力によって，全官庁のヨコ串を通す [94] 方が，統一官庁を作るよりも統一的，機動的なサイバーセキュリティ政策の展開ができるとも考えられる.

5.5 attribution 問題の改善が先決

注 16 で触れたように「攻撃と防御の非対称」を認めた「新戦略」は，同時に「防御側優位に向けた転換を目指す」（p.26）としているが，スローガンとしてならともかく，早期の実現は不可能であろう.図表1. で示したように，非対称の原因の第一は attribution 問題であり，米国の努力を以ってしても「先行きに若干の明るい光が見えた」程度に過ぎないからである.

また，わが国の裁判制度が匿名訴訟を排除し，「原告が被告を特定しなければならない」との義務を課している以上，原告に「attribution を特定するまでの時間と手段」を与えなければ，

[94] この点に関しては，林・田川・淺井［2011］で詳しく論じた.

憲法32条で保障されているはずの「公正な裁判を受ける権利」が，絵に描いた餅になってしまう.つまり制度の改変によって「武器対等の原則」に近い状態が達成される時点までは，自力救済を認めることが許されるのではないかと考える.

この意味では，Center for Cyber & Homeland Security [2016] が，2 種のビーコン（Notify owner in case of theft と Provide information on intelligence gathering）までは自力救済の許容範囲としているのは，妥当な線ではないかと思われる [95] [96].これは同書自身が挙げる 5 項目の社会的受容度基準に合致するからである（3.6）.また，廃案になった Active Cyber Defense Certainty Bill も，attribution 中心の構成になっていた（3.7）.

このような発想を，わが国で生かすことは可能だろうか.具体例として，いわゆるプロバイダ責任（制限）法 [97] の有効性を検証してみよう.この法律は，わずか 5 条と短いが，インターネット利用におけるコンテンツ保護を規律する重要なもので，損害賠償責任等を免除する規定（3 条，3 条の 2）と，発信者情報開示の規定（4 条）の 2 つの部分からなっている.前者は，インターネット上の情報流通によって権利侵害が発生した場合，情報の仲介者である ISP 等が当該情報を削除するか維持するかの判断に迷うことを避けるため，行為者への通知（米国では notice）から送信防止措置（同 takedown）に至る過程を明記して，その要件を満たす場合にはプロバイダの責任を制限（あるいは免責）している [98] .

後者の規定は，被害者が情報を発信した者を特定するために必要な発信者情報（IP アドレス等）の情報開示を請求する際に，ISP 等の「通信の秘密」侵害等の民事上の責任（損害賠償責任）を制限することにより，民事訴訟によらずに開示・不開示の判断が ISP 等によって速やかに行われることを目指したものである.

しかし実際は，後述する「通信の秘密」の厳格な解釈と運用もあって，ISP 等は発信者情報を開示したがらない.そこで被害者側は，まず開示を求める裁判（発信者情報開示の仮処分申請）を起こして，期待する情報を得た後に，いよいよ本来の訴訟に訴えるという「二度手間」になっているという.これでは法の期待する目的に沿わないので，何らかの改善策が不可欠であろう [99] .

いずれにしても attribution が「シロかクロか」ではなく，グレイ・ゾーンを段階的にクロに近づける作業でしかない以上（1.3 および 1.6 参照），「十分なレベルの努力がなされたか」否かが重要になり，そのレベルは通常定められた framework に則っているかどうかという，一種のコンプライアンス問題として判断されることになろう.この点で Mandiant 等のセキュリティ・ベンダにも

[95] 同書は，Intelligence Gathering in Deep Web/Dark Net までを，私企業がイニシアチブを取って実行できる対抗手段としているが，インテリジェンスの法制が十分整備されていないわが国では，この点の検討を保留せざるを得ない.関心をお持ちの向きは，田川・林 [2017a] を参照されたい.

[96] 因みにこの報告書を教材として，共著者が勤める大学院でケース・スタディを行なってみたところ，院生の多数が同じ見解だった.

[97] 正規の名称は「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（2001 年法律第 137 号）

[98] ただし林は，この法律が本当に責任を制限するものか，逆に責任を加重するのではないかという懸念をぬぐえないので，制限の部分をカッコで括っている（林 [2005]）.

[99] 日本弁護士連合会 [2011] は，上記のほか以下の改善を提案していた.1）開示する発信者情報の範囲に関する包括的な規定，2）請求者の住所も管轄裁判所に，3）裁判中における当該発信者の通信履歴の保全，4）プロバイダが判決に従わない場合の，主務大臣による措置命令.

在籍し，弁護士の資格を持つ著者らの共同執筆による McGee, Sabett & Shah［2013］が，adequate あるいは good enough なフレームワークの条件として，次の 7 点を挙げているのは，傾聴に値する（pp.31-32）.

① 技術的・政治的現実にマッチするよう，柔軟で実行可能かつ濫用困難なもので，
② Attribution を法概念としてよりも，政治概念と捉え，
③ 責任は単一ではなく a mosaic of responsibility であることを前提に，
④ Mosaic は政治的・経済的・社会的・技術的等の諸要素から，全体として攻撃源を合理的に指し示すもので，
⑤ 「なりすまし」は例外ではなく通常だと考え，
⑥ 上記の諸条件が満たされれば攻撃者特定の「一応の証拠」（prima facie evidence）になるが，なお攻撃者と名指しされた側にも反証の機会が残り，
⑦ 証明責任は被害者である原告が責任のモザイクをどう構成できるかにかかる一方，攻撃者とされる被告には反証権のほか，あらゆる防御権（抗弁）が認められる.

その際基本とすべき原理は，縷々述べてきたように「攻守の非対称」を解消し，当事者が「武器対等の原則」で正々堂々と論戦する場（level playing field）を維持することである.「積極的サイバー防御」といっても基本はその点にあり，それ以上でも，それ以下でもない[100].

6 わが国における法的根拠と担い手の検討

6.1 適法化理由1：自律システムにおける「攻守の非対称性」の改善

この章では，わが国において「積極的サイバー防御」を認める法的根拠と，その担い手を考察しよう.ここで原点である図表1に戻ってみると，ACD の必要性は「攻守の非対称性」，とりわけ attribution 問題から生じていたことが確認できる[101].これを「武器対等の原則」のレベルまで引き上げないと，攻撃者優位が続いて安定的なサイバー攻撃の抑止は不可能なので，その限りで「自力救済」が求められる余地があろう.

電話事業における新サービスでプライバシー保護とのバランス論で議論を呼んだ「発信者番号表示システム」が，最終的に世論に受け容れられたのも，「発信者には発信の自由がある

[100] なお，本稿では意図的に国際法を検討の対象外としてきた（1.4 節）が，自力救済の議論に関しては国際法に学ぶべき点も多い.なぜなら，国際法は主権国家間の取り決めを基に形成されるので，取り決めの合意に至らない場合などで，自力救済の余地が国内法の場合よりも広いからである.その意味では「新戦略」が「サイバー空間における責任ある国家の行動に関する G7（ルッカ）宣言」（2017 年 4 月）を引用しているのは，国内法における自力救済を考える上で，ある種のヒントを提供しているように思われる.

[101] 「攻守の非対称性」の多くが，実は「情報の非対称性」でもある（特に ① ② ③ と ⑦）.そして「情報の経済学」の貴重な教訓は，「情報の非対称性があると市場取引が歪んでしまう」ということであった.いわゆる「レモンの市場」「モラル・ハザード」「逆選択」などの現象は，いずれも「歪み」が直感的に理解できるケースであり，2007 年以降 10 年以上続いている，わが国の「品質表示の偽装」問題も同根である.このように，「情報の非対称性」が存在する場合には，「市場の自律性に任せる」ことですべてを解決しようとしても限界があり，何らかの制度や公的介入が要請される（林［2017］）.

のに，受信者には発信者を知る自由もない」という「片務性を是正するため」であったとの評価（斎藤［1979］）は正しいだろう.このような理解に立てば，サイバー攻撃においては攻守の非対称が顕著で，その最大の原因が attribution 問題にある以上，それを改善する範囲で「自力救済」を認めることは是認されるものと考えられよう.

しかし他方で，インターネットは「自律システム」（Autonomous System = AS）が相互接続を続けた結果，ある程度自然発生的に形成されたものである.従って，かつての電話会社のような中央集権的管理者は不在で，RFC（Request For Comment）などによるボランタリーな協調型の合意形成が基本になっている.それを極端に推進する「インターネット原理主義者」もいるが，大多数は緩やかな合意形成である「自律・分散・協調」を価値として認めている.

「新戦略」においても，自律性は重要な原則の 1 つであるとして，次のように述べている（p.9）.これは「サイバーセキュリティ基本法」3 条 1 項・2 項に対応するものでもある.「サイバー空間は多様な主体の自律的な取組により発展を遂げてきた.サイバー空間が秩序と創造性が共存する空間として持続的に発展していくためには，国家が秩序維持の役割を全て担うことは不適切であり，不可能である.サイバー空間の秩序維持に当たっては，様々な社会システムがそれぞれの任務・機能を自律的に実現することにより，悪意ある主体の行動を抑止し，対応する以外になく，これを推進していく.」

だが，自助努力と自力救済でもめごとが解決でき，制度や法律が不要の世界があれば望ましいが，そうはいかないのが現実である.近代国家は，ホッブスの「万人の万人に対する闘争」状態を回避するためにできたとする有名な仮説があるが，インターネットの世界にも蛮人が出現した以上，自力救済を制限して国家による法的救済により多くを期待することになるのは，歴史的に見ても必然だろうと思われる.

この点で，注 74 で引用した Intel v. Hamidi 判決を不服として，Epstein が展開している反論が興味深い.この事件では，動産に対する侵害（trespass to chattel）概念が適用されるか否かが論議の中心ではあるが，Epstein［2005］は判決が「インテルは自己のネットワークを Hamidi に使わせないようにする技術も資金もあるのだから，自己解決せよ」といっているのは許せないとして，以下のような議論を展開している（ただし，図表自体は共著者が作図したものである）.

図表 10 は，縦軸に国家による法的救済の有無を，横軸に自力救済が認められるか否かを取って，マトリクスにしたものである.(a) における両立は近代法においては回避され，(d) における救済の不在は，被害者に「泣き寝入り」を強いるので許されない.残るのは (b) か(c) だが，これこそ「法的救済と自力救済のバランス論」である.

ところが Epstein は Intel 判決のように「『自力救済があるので，法的手段は認めない』という判決は聞いたことがない」という.それは図表 10 において，本稿が検討している(c)の命題とは逆になるからである.そこで彼は「これではインターネットのもたらす問題として，『権利あるところに救済あり』の格言が通用しないかもしれないという不安・不信を醸成してしまう」と批判している.

図表 10　Epstein の議論

法的救済＼自力救済	認められる	認められない
認められる	(a) 近代法においては法的救済が優先され，自力救済と両立することはない	(b) 法的救済が原則で，ごく限られた例外的な場合にのみ，自力救済が認められる
認められない	(c) 法的救済の道がない場合に，例外的に自力救済が認められるかという，一般的な命題になる	(d) どちらも認められないとすれば，違法・不法な行為が放置される恐れがある

共著者は Intel v. Hamidi の判決自体は支持するので，結論部分において Epstein とは違う見解の持ち主であるが，上記の指摘には無視できない要素が入っていることを認めざるを得ない.それは，「国家が権利侵害を救済するのでなければ，インターネットは無法地帯になりかねない」という警告であり，少なくとも「攻守の非対称性の解消」までは国家の役割と考えるべきだろう.

これに応えるには，2 つの方法があると思う.1 つは既に触れた，「少なくとも attribution を突き止めるまでは，善意の第三者に危害を及ぼさない範囲での自力救済を認める」ということであり，第 2 はウィルスという単語を共有する限り，「インターネットにも公衆衛生と同様な公的介入を認める」ということである[102].第 1 の点は既に述べたので，ここでは主として第 2 の点を敷衍しよう.

6.2　適法化理由2：自律システムにおける自己管理と Cyber Hygiene

自律システムにおける，もう 1 つの特徴は，システムの運用と管理を自己責任で実施することである.これは当然のことのように思われるが，サイバー攻撃が日常化している現在では，特別な意味を持っている.

不正アクセス禁止法でも，「アクセス制御機能を特定電子計算機に付加したアクセス管理者は，当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに，常に当該アクセス制御機能の有効性を検証し，必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする.」（第 8 条）と規定している.

今日のコンピュータは，ネットワークに接続する場合は，何らかの「アクセス制御」を求められることが多いから，これはあらゆるシステム管理者の義務になったと考えられる（もっとも，努力

[102] 感染症の蔓延とコンピュータ・ウィルスの拡散は，以下の 4 点で類似性があるように思われる.1）1 つの感染が大被害を及ぼすことがなくても，閾値を超えると壊滅的な状況になり得る，2）感染者が気付かないうちに，次の感染を発生させることが多い，3）従って対策には疫学的な対応が必要になる，4）同時に，関係者全体の気づき（awareness）が不可欠である.

義務ではあるが).特に，重要インフラと分類されるサービスを提供する者は，その「機能」を安全に維持することが「任務」でもあると考えられる.この点に関して「新戦略」が「任務保証」という語を使って，次のように述べているのは示唆に富んでいる(pp.10-11)[103] .

「『任務保証』とは，企業，重要インフラ事業者や政府機関に代表されるあらゆる組織が，自らが遂行すべき業務やサービスを『任務』と捉え，係る『任務』を着実に遂行するために必要となる能力及び資産を確保することである.その際には，一部の専門家に依存するのではなく，各々の組織の『任務』に該当する業務・サービスを遂行する観点から，その責任を有する者が主体的にサイバーセキュリティの確保に取り組むことが肝要である.」

ここでは「自己責任」や「自己管理」といった用語は使われていないが，それが暗示されていることは明らかだろう.4.5 で紹介した米国の Cybersecurity Information Sharing Act of 2015 では，自己のシステムはもちろん，他社の委託に基づく場合や，連邦政府からの依頼がある場合には，サイバーセキュリティ目的でモニタリングすることが合法化されている(同法 104 条(a)).また，わが国でも先見の明のある実務家は，早くも 2005 年に，システム管理者にはこのような権利と義務があることを主張していた(高橋・吉田 [2005]).

このような責任は，ボットネットなどが一般化した現状では，自社保有のシステムの安全だけではなく，広く社会システム全体としての安全にも及ぶと考えるのが妥当であろう.いわば「公衆衛生」のインターネット版である.

世界保健機関(WHO)は公衆衛生を「組織された地域社会の努力を通して，疾病を予防し，生命を延長し，身体的，精神的機能の増進をはかる科学であり技術である」と定義しており [104]，それは疫学，生物統計学，医療制度などを含み，環境・社会・行動衛生，職業衛生，食品衛生も重要な分野を構成する広い概念である.しかし本稿との関連では，感染症対策が最も近いと思われる.

ボットネットはウィルスに感染しているので，その対策として無力化・壊滅化などが実施されることは既にみてきた.これらをサイバーセキュリティを所管する行政府が認定し，民間企業に権限を委譲するか，民間と共同で実施するのであれば，善意の第三者に害を加えるのでない限り是認すべきことは，感染症の対策として予防接種を受ける努力義務(予防接種法 9 条)や健康診断受診・就業制限・入院などの強制措置(感染症予防法 17 条～19 条)とのアナロジーで考えることができると思われる.

その意味では，Center for Cyber & Homeland Security [2016] が，ボットネットのテイクダウンなどの対抗手段は，High Impact/Risk であっても，政府との密接な協力の下でなら是認される(Requires Close Government Cooperation)としている(図表 3 と 4)のは，妥当な線だと思われる.

これをサーバー管理者の権限と責任として図式化すれば，以下のようになろう.

安定的なコンピュータ・ネットワークの維持―＞設備維持管理権と義務―＞(一定範囲の)

[103] 初期には「機能保証」といっていたが，その後「任務保証」に統一された.
[104] http://www.euro.who.int/en/health-topics/Health-systems/public-health-services

自力救済―＞cyber hygiene としての許容性

つまり，ウィルスに汚染されたコンピュータの存在が明らかなら，それを公的機関に確認してもらった上で，単独あるいは共同作業として無力化・壊滅させるのは，広くインターネット利用者の責任であると捉え，cyber hygiene として，その行為を自力救済として是認しても良いと考える．共著者は既に 2016 年に同様の主張をしているが（林・田川 [2016]），ここでその立場を再確認したい．

6.3 ISP への期待と制約，わが国における特殊事情

サイバーセキュリティの日米比較は，種々の観点から行なわれているが，わが国の絶対的人材の不足と偏在（ユーザ企業に人材が少なくIT ベンダに偏っている[105]）は，多くの調査で共通の特徴である.そこで，少なくとも attribution を突き止めるまでは自力救済が認められ，さらには cyber hygiene としてボットネットのテイクダウン等が認められるにしても，それを誰が実行するかが問題になる.

被害者が実行するのが常識的だが，実は第 4 章の末尾で述べた ③ の要件（他人に危害を与えないこと）が意外に難しい.技術的成熟度が低い企業にも自力救済を認めると，攻撃者ではない第三者に反撃を加えて，実害を生じさせるかもしれない.その反撃の被害者が自力救済という名で再反撃をすれば，反撃の連鎖になって法治国家の伝統をないがしろにする結果を招きかねない.

とすれば，誰が「有資格者」なのだろうか.この点を突き詰めていくと，必然的に「ISP への期待と責任」に触れざるを得ないが，米国では FCC（連邦通信委員会）内の助言機関である CSRIC = Communiations Security， Relaiability and Interoperability Counicil が（CSRIC [2010]），国際機関としては OECD（Organization for Economic Cooperation and Development）が（OECD [2010]），それぞれ ISP の役割について検討を進めてきた.また，著名なセキュリティ専門家であるシュナイヤーも，前述の「公衆衛生」の観点から「ISP は社会全体の情報システム部門になるべきだ」と主張している（Schneier [2007][106]）.

そこには日米（更には先進国全体）に共通の要素と，わが国に固有の事情とがあるが，まず両国に共通の事情としては，以下の 5 点がある（この点に触れた文献は多いが，以下は Rowe et al. [2011] を中心に共著者がまとめたものである）[107].

① 重要インフラ事業者には，そのサービス提供を断絶させない（事業を継続させる）「任務」が期待されており，中でも電力・水道などの Basic Human Needs を提供する事業者とともに，ISP の「任務」は重要視されている，

[105] ある調査では，IT 人材は米国ではユーザ企業に 7 割，IT ベンダに 3 割いるが，わが国ではその比率が逆転し，3 対 7 になっているという.経済産業省が，2015 年に産業構造審議会に提出した資料による.
[106] ただし彼は同時に，ネットワーク監視システムを導入すれば，その脆弱性を突かれるリスクも増大するので，「ISP への課題を最小化すべし」とも主張している（OECD [2010]）.
[107] なお，ここでISPとは「電気通信事業者」として登録しているか否かや，プロバイダ責任（制限）法の適用があるかなどに拘らず，電気通信設備を持たずネットワーク監視を専業にする事業者も含むなど，純粋に機能的な概念であると理解していただきたい.

⑧ attribution 問題を改善し対策を講ずるには，被害を受ける恐れのある民間企業からの要請ないし同意に基づき対応できるISPが最も好位置にいる[108]，

⑨ 個別ネットワーク（それ自体が前述のAutonomous Systemである）と，個別ネットワーク内の特定加入者への攻撃には，当該ネットを管理するISPが対応するのは当然である．

④ ネットワークを利用した攻撃，あるいはネットワーク全体への攻撃や悪影響を除去するには，ISPの協力が不可欠であるし[109]，今や有力なISPはMSSP（Managed Security Service Provider）として，セキュリティ・ベンダと並んでセキュリティをコア・ビジネスにしている，

⑤ オープン・ネットワーク政策を進めれば進めるほど，「公正なネットワーク管理」（legitimate network managemant）の必要性が高まり，それは必然的にISPの役割重視につながる[110]．

これら日米の共通要素に加えて，米国における「ISP責任論」の基本は「法と経済学」の影響を受けた理論を根拠にしたもので，資源配分の効率性の観点から「最も安い費用でリスクを回避できるのは誰か[111]」という分析をすれば，ISPに行き着くはずという主張である[112]．これに対して，わが国の「ISP 責任論」は，悲しいかな「ISP 以外に頼りにできる主体がいない」という消去法の結果である点で，著しく異なっている[113]．

なお米国の場合は，前述（4.5）のCyber Security Information Sharing Act of 2016における情報共有が，一部セキュリティ・クリアランスと一体となっていたことを想起して欲しい．その具体化であるECS（Enhanced Cybersecurity Services）プログラムにおいては，政府から提供されたCTIやDMといった情報を他の民間企業にも提供できるCSPs（Commercial Internet Service Providers）と，自社のネットワーク管理のためだけに利用できるOIs（Operational Implementers）の区分が設けられている．

規制が嫌いな米国でさえ，先に挫折した法案（3.7）の中で，成熟度モデルによるACD権限の付与と制約を設けていたことは，FBIへの事前届出制度と相俟って，ACDが未熟なユーザやISP等によって乱発されないよう，慎重に対処している証拠と考えられる．

---

[108] この点は米国の新しいCyber Strategyにおいても確認されている（3.8節）．なお，この任務の遂行にはインテリジェンス機関の協力が不可欠になりつつあるが，国際法と国際関係を除く本稿の主旨から割愛する（わが国の能力が疑問視されていることは，否定できないだろう）．

[109] データは古いが，Rowe et al.［2011］には，ISP 10社だけで世界中にスパムをばらまくIPアドレスの30%を管理し，Eeten et al.［2010］には，マルウェアに感染した端末の80%以上はISPのネットワーク内にあり，ISP 50社だけで，その約50%を管理している，という記述がある．

[110] 米国のFCC（Federal Communications Comission）が打ち出した「オープン・ネットワーク戦略」においては，legitimate network management の要素として‘ensuring network security and integrity’が含まれている．

[111]「最安価リスク回避者」（Least Cost Avoider）の概念は，Calabresi［1970］等によって展開されたもので，確かに資源配分効率だけを考えれば，最適解になる．

[112] もっともLichtman & Posner［2004］は更に議論を精緻化して，次のように主張している．経済理論の教えに従えば，次の2条件が同時に満たされる場合は，間接責任を問う必要はない．1）直接行為者が法の想定内（同定可能で支払い能力がある）で，2）取引コストが高くなく，直接行為者が責任を全面的（あるいは一部）移転する契約が可能．しかしサイバー攻撃のように上記の2条件が欠ける場合は，法の規定が重要になり，以下の追加的2要素がある場合には，間接責任が有効になる．a）責任を負う可能性のある主体が，違法行為を発見し回避できる立場にある（control 要素），b）当該主体に違法行為から生ずる外部不経済を内部化するインセンティブを付与することができる（activity level 要件）．

[113] ただし米国でも，ISPの役割が期待されていることは変わりがない（3.4節の提言（15）参照）．またHoffman& Levite［2017］が指摘するように，保険業にも期待したいところである．

6.4 ソマリア海賊事件の教訓？

この点に関して，Hoffman & Levite［2017］の指摘が示唆に富んでいる.彼らは，ソマリアが無政府状態になったことを奇貨として海賊が横行した際に，有力な海運会社が（物理的）セキュリティ会社や損害保険会社と組んで，「自力救済」に訴えざるを得なくなったケースを詳細に分析している.

そこで得た教訓は，1) 業界団体（Security Association of the Maritime Industry = SAMI）を作り，2) Code of Conduct（CoC）を定めて遵守する（できる）社だけを会員として認めて偶発事故を最小化するなどの努力の結果，3) Private Maritime Security Contractors = PMSCs が健全に発展した，というのである（pp. 13-15）.

この教訓を ACD にも生かすべきだという彼らの主張は説得力がある.因みに，この時定められた CoC は，その後 ISO 規格（ISO 28007-1:2015 Ships and marine technology -- Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships (and pro forma contract)と 100 Series Rules for the Use of Force[114]）として生かされているという.

一方サイバーセキュリティの分野で attribution 解明への光を見出したのは，米国の Google のような IT 企業と，McAfee などのセキュリティ・ベンダであった（1.3）が，同種の力量を持つ企業をわが国で見つけることは難しい.しかし，伝統的なコモン・キャリアは米国に匹敵する能力を持っているし[115]，関連会社として活躍している ISP も有能である.加えて，これらの企業群が共同で運営している ICT-ISAC は，わが国における ISAC の先駆者として知識と経験を蓄積している[116].

このような能力を蓄えることができたのは電気通信の自由化が世界的潮流となり，それまで POTS（Plain Old Telephone Service）の分野で各国市場をほぼ独占的に支配してきた安定的産業構造が激変したこと，コンピュータ通信が POTS を追い越すことが確実視され，新しいビジネス・チャンスが生まれたことなどが，契機となっている.伝統的なキャリアは市場の変化に対応すべく，顧客のネットワーク監視を請け負ったり，グローバルなワン・ストップ・サービスを提供するなどで対応し，それが今日では MSSP への飛躍につながっている.MSSP は ISP が高度化したもので，今後はクラウド事業者の一部もこの分野に参入してくるだろう.

6.5 ACD を具体化するための法制度整備

2018 年 9 月 20 日に公表された米国のサイバー戦略では，サイバー攻撃等を検知（detect），防止（prevent），緩和・無害化（mitigate）する防御策として，情報共有をベースに官民の緊密な連携体制の構築を始めとして，技術開発，人材育成，利用者への啓発など幅広い取組が必

[114] https://www.humanrightsatsea.org/rules-for-the-use-of-force-ruf/
[115] 特に NTT グループは Tier 1 キャリアであることに加え，国際的な事業展開の結果，セキュリティをコア・ビジネスの 1 つに据えて NTT セキュリティを設立するなど，この分野に注力している.
[116] その後にできた金融や電力の ISAC は，いずれも Telecom-ISAC（その後 ICT-ISAC に名称変更）をモデルにしている.

要であることを強調している.

われわれも，これに倣うと同時に，民間企業等が実行しようとするサイバー攻撃等への対処策に関して，その合法性・違法性の判断がしやすいような法制度整備を行なうことも，重要な課題だと思われる.違法なサイバー攻撃等への法的な対処策として，現在の法治国家においては，刑事責任，民事責任を問い得る法制度整備を行なうことが大原則である.しかし法が予想しないようなサイバー攻撃等があって，detect，prevent，mitigate し得るためには，まずもって自助努力による attribution 問題の改善が必要であり，被告の特定までを原告の負担としているわが国の法制度化では，不可欠ではないかとする問題提起を行なった.その上で外部不経済の解消のための cyber hygiene も許容されるのではないか，という方向で検討を進めてきた.

民間企業のサイバー攻撃に対する対抗手段である ACD は，侵入検知，侵入者の追跡，ある種の対抗手段を講ずる，の 3 要素の組合せであるとの指摘（p.9）があるように多様な内容が含まれている.第 2 章の図表 2，図表 3 に示されたように，ACD は伝統的な offense と passive defense の間のある spectrum ないし sliding scale（可変的尺度）の幅広いものであることまでは，大方の意見は一致している.しかし議論が進んでいる米国においても，ACD の個々の対抗手段の適法性に関しては未だ議論段階で，具体化は今後に待たなければならない状況である.

その意味で，自力救済という用語の意味内容は一義的に決まりにくく，幅があることについて，ご理解いただきたい.その上で，以下では日本での ACD の具体化に向けた法的な課題について，述べることにしたい.

第 4 章および第 5 章において分析してきたことのまとめとして，現在と近い将来において必要と考えられる法的課題例を挙げると，以下のようになる.

① CFAA と不正アクセス禁止法との対比（図表 7）に基づく不正アクセス禁止法改正，
② 民事訴訟における匿名訴訟やデジタル・フォレンジックの活用（図表 8），
③ 笹川平和財団の 4 つの法制度に関する指摘（図表 9），
　・政府によるサイバー脅威情報の収集
　・重要インフラ事業者にサイバーインシデントの報告義務
　・重要インフラ事業者にサイバーインシデント連絡担当者の必置義務
　・政府によるプライバシー侵害を監視する独立機関の設置
④ 笹川平和財団の提言，
　・サイバーセキュリティ基本法におけるサイバーセキュリティの定義の見直し
　・サイバー攻撃等への対処のための政府の主導的な役割を定める関連法の一括改正
⑤ プロバイダ責任（制限）法の改正.

このような法制度整備と共に，どのような自力救済であれば認められるのか，刑事免責とともに民事免責も認められるのか（緊急避難が根拠であるとしても，刑事の免責しか認められない場合もあろう）などについてのガイドライン作成することで，積極的サイバー防御の具体化が可能になると考えられる.

7 積極的サイバー防御と「通信の秘密」

7.1 「通信の秘密」の法解釈

「積極的サイバー防御」を推進するための法的課題の 1 つが，電気通信事業者が業務遂行上長年悩みつつ対処してきた「通信の秘密」の規定である.本章では，まず「通信の秘密」の伝統的な法解釈について述べ(7.1)，インターネット時代において電気通信事業者の役割が重くなってきたことに伴う解釈の変化に触れて(7.2)，サイバーセキュリティ強化に伴う「通信の秘密」に関する現在の法解釈動向を概観した後(7.3)，積極的サイバー防御を推進するための若干の提案を行なう(7.4).

「通信の秘密」に関しては，憲法 21 条 2 項に「検閲は，これをしてはならない.通信の秘密は，これを侵してはならない.」との規定があり，法律では電気通信事業法，有線電気通信法および電波法にそれぞれ条文がある.ここでは，「通信の秘密」の法解釈の中心となっている電気通信事業法に関して述べる.

まず「通信の秘密」に関する電気通信事業法の関連条文を掲載する.なお文中の下線は共著者が付加したものである.

（検閲の禁止）

第 3 条 電気通信事業者の取扱中に係る通信は，検閲してはならない.

（秘密の保護）

第 4 条 電気通信事業者の取扱中に係る通信の秘密は，侵してはならない.

2 電気通信事業に従事する者は，在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない.その職を退いた後においても，同様とする.

（適用除外等）

第 164 条 この法律の規定は，次に掲げる電気通信事業については，適用しない.

一 専ら一の者に電気通信役務（当該一の者が電気通信事業者であるときは，当該一の者の電気通信事業の用に供する電気通信役務を除く.）を提供する電気通信事業

二 その一の部分の設置の場所が他の部分の設置の場所と同一の構内（これに準ずる区域内を含む.）又は同一の建物内である電気通信設備その他総務省令で定める基準に満たない規模の電気通信設備により電気通信役務を提供する電気通信事業

三 電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務（ドメイン名電気通信役務を除く.）を電気通信回線設備を設置することなく提供する電気通信事業

2 この条において，次の各号に掲げる用語の意義は，当該各号に定めるところによる.

一 ドメイン名電気通信役務 入力されたドメイン名の一部又は全部に対応してアイ・ピー・アドレスを出力する機能を有する電気通信設備を電気通信事業者の通信の用に供する電気通信役務のうち，確実かつ安定的な

提供を確保する必要があるものとして総務省令で定めるものをいう.

二 ドメイン名 インターネットにおいて電気通信事業者が受信の場所にある電気通信設備を識別するために用いる電気通信番号のうち，アイ・ピー・アドレスに代って用いられるものとして総務省令で定めるものをいう.

三 アイ・ピー・アドレス インターネットにおいて電気通信事業者が受信の場所にある電気通信設備を識別するために用いる電気通信番号のうち，当該電気通信設備に固有のものとして総務省令で定めるものをいう.

3 第 1 項の規定にかかわらず，第 3 条及び第 4 条の規定は同項各号に掲げる電気通信事業を営む者の取扱中に係る通信について，第 157 条の 2 の規定は第三号事業を営む者について，それぞれ適用する.

第 179 条 電気通信事業者の取扱中に係る通信（第百六十四条第三項に規定する通信を含む.）の秘密を侵した者は，二年以下の懲役又は百万円以下の罰金に処する.

2 電気通信事業に従事する者が前項の行為をしたときは，三年以下の懲役又は二百万円以下の罰金に処する.

3 前 2 項の未遂罪は，罰する.

第 190 条 法人の代表者又は法人若しくは人の代理人，使用人その他の従業者が，その法人又は人の業務に関し，次の各号に掲げる規定の違反行為をしたときは，行為者を罰するほか，その法人に対して当該各号に定める罰金刑を，その人に対して各本条の罰金刑を科する.

一 第 181 条 1 億円以下の罰金刑

二 第 177 条から第 188 条（第 180 条，第 181 条，第 183 条及び第 184 条を除く.） 各本条の罰金刑

7.1.1 「通信の秘密」の保護対象データ，侵害者と保護義務者

「通信の秘密」は「電気通信事業者の取扱中に係る通信」を対象とするもので，通信内容と通信の構成要素[117] の両方のデータが含まれるとするのが通説である.米国や EU でも保護対象は通信内容と通信の構成要素の両方が含まれているが，両者の扱いが異なっており，保護の強弱には大きな差がある.なお通信の構成要素に該当する用語は，米国ではメタデータ，EU ではトラフィック・データ，英国法ではコミュニケーションズ・データと呼ばれているが，本稿では日米比較が主であるからメタデータと呼ぶ.

「通信の秘密」を侵すとは，知得，窃用，漏えいの三つの行為のいずれかまたは複数を行なうことであり，4 条 1 項の規定は国民が遵守すべき規定であって，これに違反した場合には 179 条 1 項で処罰され，電気通信事業の従事者が違反した場合には，同条 2 項が適用され刑罰が加重されている.また 164 条 1 項に該当する電気通信事業については，電気通信事業法の適用除外にはなるが，同条 3 項によって検閲の禁止（3 条）と秘密の保護（4 条）の規定は適用されることになっている.

伝統的な電話サービスでは，これらの規定の適用関係は比較的明快であるが，インターネット・サービスでは，電気通信事業者中心の電話事業とは異なり，多彩なアプリ・サービスが多様

117 「通信の構成要素には，通信当事者や通信回数・年月日など通信内容ではないが，通信そのものの構成要素であり，これらの事項を知られることによって通信の意味内容が推知されるような事項はすべて含まれる.」（電気通信関係法コンメンタール編集委員会［1973］p.39）.金光・吉田［1953］も同旨.

な事業者によって提供されており，多層レイヤ化が進展している.これを「通信の秘密」の観点からみると，1）法の適用事業者，2）法の適用除外になってはいるが「通信の秘密」の規定は適用される事業者（164 条 3 項），3）「通信の秘密」の適用対象外事業者の 3 種類に分かれている.

このように「通信の秘密」に関しては，事業者間で equal footing になっておらず，インターネット時代にうまく対応できていない状況で，いわば「過剰」（伝統的な解釈と運用が厳格過ぎる.後述の注 134 参照）と，「空白」（本来適用されるべき原則が適用されない）の 2 つの領域が共存している.

7.1.2 「電気通信事業者の取扱中に係る通信」の意義

「取扱中に係る通信」には，発信者から受信者までネットワークを流通している通信と，電気通信事業者が業務上の必要性から知得してサーバー等に蓄積・保存している情報の両方が含まれている[118].

他方で，1）電気通信事業者以外の者が蓄積・保存している情報は，これに該当しない.2）携帯電話の基地局に係る位置情報のうち，個々の通話に利用される基地局情報は「取扱中」に該当するが，通信を成立させるために登録する位置情報は，「取扱中」ではないので「通信の秘密」の対象外である.3）また GPS 情報は，基地局の位置情報よりも精度が高いものの，「取扱中」に該当しないので，「通信の秘密」ではなく，個人情報として保護される[119].このように，「取扱中」かどうかで「通信の秘密」該当性が判断されるために，類似の情報でも「通信の秘密」に該当する情報と，個人情報に該当する情報とに分かれている.

7.1.3 「通信の秘密」（4 条 1 項）と「他人の秘密」（4 条 2 項）の区分に関する 2 つの解釈

憲法・有線電気通信法・電波法の 3 法には，この 2 つの区分は設けられていない.制定過程の経緯については明らかではないが，1947 年に制定された郵便法では，8 条 1 項で「何人も信書の秘密を侵してはならない」ことを，同 2 項で「郵便の業務に従事する者は在職中郵便物に関して知り得た他人の秘密を守らなければならない」ことを定めている.電気通信事業分野でも，この規定を受けた公衆電気通信法（1953 年制定）を経て 1984 年に制定された現行の電気通信事業法においても，この区分が維持されているが，これに関しては 2 つの解釈がある.

1 つは，「他人の秘密」の方が「通信の秘密」よりも保護範囲が広いとする解釈である.「通信の秘密」を超えるが「他人の秘密」には該当する例として，人相（電報を窓口で受け付けた場

[118] また，別人が通話を傍受して録音したテープを入手して他人に聞かせた行為も，なお「取扱中に係る」 という条件を満たすとの最高裁判決がある（最二小決 2004 年 4 月 19 日 刑集 58 巻 4 号 281 頁）.
[119] 「緊急時等における位置情報の取扱いに関する検討会 報告書 位置情報プライバシーレポート」 総務省，2014 年 7 月，pp.6～8

合)，言葉の訛り(通話を交換手が媒介した場合)，プッシュホンに記憶された相手番号等[120]が挙げられているが，かなり限定的である.加えて，この例は電話利用の例であって，インターネット利用の例は挙げられておらず，両者の差分がほとんどないと考えられるのに，この解釈を根拠に 2 つの区分を維持するのは疑問である.

なお，このように両者の範囲がほぼ重なり合うにしても，「通信の秘密」の範囲を超える「他人の秘密」を守らなかった場合には，4 条 1 項違反ではないので，179 条 2 項の罰則の適用がないことについては異論がなく[121]，この点については「罪刑法定主義」を厳守した法解釈が行なわれている.

2 つ目の解釈は，4 条 1 項と 2 項は規律対象者と遵守義務が異なるとの解釈である.すなわち 1 項は電気通信事業の従事者以外の者に対する規定であり，知得・窃用・漏えいのすべてが禁止されているのに対して，電気通信事業の従事者は「通信の秘密」に該当する情報を業務遂行のため知得するが，これは正当業務行為であって違法性が阻却される.そこで 2 項では，電気通信事業の従事者は「通信の秘密」に該当する情報を知得することができるが，その知得した「他人の秘密」を守らなければならないと規定されているとするものである.

「他人の通信」の意義に関して，小向［2006］は，通信の秘密に該当するかどうかということと，その情報の知得が「通信の秘密」の侵害になるかは別の問題であるとして，「電気通信事業者がその設備を用いて通信役務を提供するために発信者及び受信者の情報等を利用することは，通信当事者が当然に予測することであり，通信の秘密の問題は生じないと考えられる」と述べている(p.120).

この 1 項の「侵してはならない」と 2 項の「守らなければならない」との規定の違いは，制定当時はそれほどの違いと意識されていなかったようである[122].その理由としては，電話利用においては，電気通信事業の従事者であっても，自分が預かった通信にノータッチ(hands-off)が大原則であり，実務上も「通信の秘密」に該当する情報を知得する必要性が，ほぼなかったためではないかと考えられる.

その後，「通信の秘密」に該当する情報を利用して，料金明細サービスや発信者表示サービスなどが提供されるようになってきたために，この違いが次第に意識されるようになり，インターネット利用において本格的に議論されるようになったものと考えられる.

しかしながら，長い間に培われた「通信にノータッチ」との規範意識は根強く，また「通信の秘密」に該当する情報を知得することの是非については，総務省の研究会等での検討を経て，個別にその正当性の線引きがなされてきた.すなわち通信当事者の個別・明確な同意の有無，または(正当行為，正当防衛，緊急避難という)違法性阻却事由の有無によって判断している.このため，正当性根拠の明確でない知得は，「通信の秘密」侵害になって刑罰が科される恐れがあるために，電気通信事業者は，「通信の秘密」に該当する情報の知得について，慎重なス

120 「郵便・信書便における通信の秘密」，郵便・信書便制度の見直しに関する研究会 2007 年 3 月 27 日資料 2，総務省，p.2
121 電気通信法制研究会［1987］p.268
122 高橋・林・舟橋・吉田［2009］pp.4～8

タンスを取らざるを得ない状況が続いている.

もちろん従事者に認められているのは，業務上の必要性がある場合の「通信の秘密」に該当する情報の知得だけであり，知得した情報を窃用，漏えいすれば，「通信の秘密」の侵害行為であって [123]，4 条 1 項違反となる.しかし，どのような情報なら知得できるかということに関して，事前の線引きが難しい状況では，より慎重な扱い（リスク回避的な行動）が誘引されるのは，避けられないと思われる.

7.1.4 電話利用において「通信の秘密」と「他人の秘密」が問題とされた事例

前 7.1.3 において，電話利用においては「通信にノータッチ」が大原則で，実務上も「通信の秘密」に該当する情報を知得する必要性が，ほぼなかったと述べた.

この数少ない例外の一つが，1963 年に発生した吉展ちゃん誘拐・脅迫電話事件である.誘拐犯（と思われる人物）から吉展ちゃん宅に脅迫電話がかかってきたときに，当時の電電公社はわが国で初めて脅迫電話の録音と逆探知 [124] を試みたが（前者は成功，後者は失敗），当時の公衆電気通信法 [125] 上の疑義を明らかにすべく，郵政省経由で内閣法制局に対して，次の照会を行なった.

① 電話を利用して刑法 222 条に規定する脅迫の罪を現に犯している者がある場合に，被害者の要請によって，電電公社の職員が当該電話の発信場所を探索し，これを司法警察職員等の捜査官憲に通報することは，公衆電気通信法第5条第2項の規定に違反することになるか.

② 司法警察職員等の捜査官憲が，電話による通話の一方当事者甲の同意を得て，甲の利用する電話の端末において他方の当事者乙の通話を録音することは，公衆電気通信法第 5 条第 1 項の規定に違反することになるか.

これに対する法制局の回答は「お尋ねの問題は，いずれも消極に解する.」，つまり両方とも「侵害にはならない」ということであった.

まず ① の逆探知を認める理由については，「電話の発信場所は，発信者がこれを秘匿したいと欲する場合がありうるから，第2項にいう『他人の秘密』に該当すべきものと解すべきである」としつつも，「電話を利用して脅迫の罪を現に犯している者がある場合において，被害者の要請があるときは，公社の職員が当該電話番号の発信場所を探索し，これを捜査官憲に通報することは，許されるものと解すべきである.」と回答している.

この回答に関する論評として，片桐 [1986] は「本法制意見は，逆探知が合法であるためには，発信者が現行犯人であることと被害者の要請があることとの双方を要するものとしていると解される」と述べている.

---

[123] 大阪高判 1967 年 12 月 25 日，昭 41（ネ）665 号事件.この判決は，通信の秘密を侵したことを理由とする交換手の懲戒免職処分を有効と認めた事例（いわゆる福知山電報電話局事件）である.

[124] 当時の電話は発信から着信まで多段階の電話局を経由し，通話中は当該回線を専有していたので，通話の継続中にその経路を逆にたどって発信者を突き止めること.

[125] 公衆電気通信法 5 条 1 項と 2 項は，現在の電気通信事業法 4 条 1 項と 2 項と同趣旨の規定である.

ついで ② の録音を認める理由については，「電話による通話の一方の当事者甲がその利用する電話の端末の設備において聴取しうる他方の当事者乙の通話の内容は，甲の支配下に置かれた事項であって，法5条1項にいう『公社----の取扱中に係る通信の秘密』の範囲外にある事項である.」と回答している.これは，前 7.1.2 において述べた「取扱中」の範囲外であるので，「通信の秘密」の対象外であるとするものである [126] .

この回答に関する論評として，前掲片桐は「本法制意見は，一方当事者甲の利用する電話の端末の設備において聴取し得る他方当事者乙の通話の内容は甲の支配下に置かれたものであるから，（法 5 条 1 項に）当たらないとしている.したがって，司法警察職員等が通話の内容を録音するためには，通話の内容を支配する甲の同意があれば足りることとなり，乙が現行犯人である等他の要件を要しない.学説は，多くは，一方当事者の同意があれば違法ではないとしている.（注略）」と述べている [127] .

ところが，この内閣法制局の回答を受けて，電電公社の社内ルールとして発出された「通信の秘密について」という通達（電文 1100 号）では，この両者を区分したような記述なり構成にはなっていなかった.当時は，「通信の秘密」と「他人の秘密」の規定の違いは，前 7.1.3 で述べたように，それほど意識されていなかったことを伺わせる出来事である.

7.2 インターネット利用における電気通信事業者の役割の変化と「通信の秘密」

7.2.1 インターネット利用における電気通信事業者の役割の変化と根拠規定

電話サービスが中心の時代において，電気通信事業者は，自らが預かって運ぶ「通信」にノータッチ（hands-off）であることが当然視されていたことは前述した.しかしインターネット利用では，以下の 2 つの理由によって，電気通信事業者は「通信の秘密」の保護を制限することを求められたり，認められたりする事例が多くなっている.

① インターネット利用においては，電話のように 1 対 1 の秘匿性を有する通信よりも，「公然性を有する通信」といわれる，多数の人に見られることを想定（期待）した情報が圧倒的に多くなってきた.インターネットは万人に開かれているが，その中に潜む蛮人がいるために，いわゆる「違法有害情報」が多く流通している.このため，プロバイダ責任制限法 4 条の発信者情報開示の規定や，事業者の自主的な取組みである児童ポルノのブロッキングのような「通信の秘密」の保障を制限する行為が認められていて，実施されている.この問題は本来，通信当事者や利用者間の問題であるが，電気通信事業者はそれらの通信を

[126] 照会事項 ① で，法 5 条 2 項（他人の秘密）の規定に違反するかと照会したのは，公社職員が逆探知を行なっているからで，また照会事項 ② で，法 5 条 1 項の規定に違反するかと照会したのは，公衆電気通信事業の従事者ではない者が行なった行為なので，1 項の規定違反になるかとの照会になったものと考えられる.

[127] 「特別の事情がない限り，受信者のみの承諾をもって通信の秘密が放棄されたとはいえないであろう」との反対意見（例えば，多賀谷・岡崎［1998］p.47 注（15））もあるが，少数意見と思われる.

運んでいる，いわば「媒介者としての責務[128]」を果たしているといえる.

② 自律・分散・協調を旨として運営されているインターネットは，悪意の攻撃に対して脆弱性を有している.サイバー攻撃が高度化・多様化していて，その被害が深刻化しているなかで，インターネット・サービスを安定的に提供するためには，管理面，技術面，政策・法制度及び倫理面のそれぞれの面からサイバーセキュリティ対策の強化が不可欠である.

ただし，電気通信事業者が「通信の秘密」の保護を制限する行為を行なうには，相応の根拠が必要である.それらに該当するものとして，図表 11 に掲げる法律や事業者が自主的に定めたガイドライン[129] がある.

図表 11 「通信の秘密」の保護を制限する根拠規定

	違法有害情報対策（媒介者の責務）	インターネット・サービスの安定的提供
法律	プロバイダ責任制限法 青少年インターネット利用環境法	迷惑メール防止法
ガイドライン[130]	インターネット上の自殺予告案件への対応に関するガイドライン プロバイダ責任制限法発信者情報開示関係ガイドライン	電気通信事業におけるサイバー攻撃への対処と通信の秘密に関するガイドライン 帯域制御の運用基準に関するガイドライン

注：「通信の秘密」の保護の制限は，左欄においては権利を侵害されたと主張する者の個人的法益と「通信の秘密」の保護法益との比較衡量，右欄においてはインターネット・サービスの安定的提供という社会的法益と「通信の秘密」の保護法益との比較衡量に基づいて行なわれる.

7.2.2 電気通信事業者が「通信の秘密」の保護を制限している事例

このような制限規定が，どのように定められているかを，もう少し細部に入って紹介しよう.総務省では，サイバー攻撃の拡大・深刻化に対処するために，2013 年に「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を設置して，「通信の秘密」の問題を検討してきた.その成果として，2014 年 4 月に「第一次とりまとめ」を，また 2015 年 9 月には「第二次とりまとめ」を公表している.

このとりまとめの内容を反映する形で，テレコム 5 団体が業界自主ルールとして「電気通信

128 「媒介者としての責務」の一つの例として，海賊版サイト問題のブロッキングが大きな問題として論議され注目を集めているが，本項の目的はサイバーセキュリティ強化の観点から「積極的サイバー防御」を論ずることであるので，「媒介者としての責務」の問題にはこれ以上深入りしない.

129 ガイドラインの法的な性格について，「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」において，「本ガイドラインはあくまで業界における解釈に過ぎず，法的な効果があるものではありませんが，通信の秘密に関わる解釈指針として，日々刻々と進化するサイバー攻撃等への対処の是非について，電気通信事業者及び関係者による法的判断の解釈の参考として参照されることを期待する」と述べられている.

130 これらのガイドラインは，事業者団体が自主的に定めたものであるが，内容は総務省の研究会等の議論を踏まえて定められているので，いわば「共同規制」的な手法が取られているといえる.

事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン[131]」を策定・公表しており，実務上はこのガイドラインに従った形でサイバー攻撃への対処が行なわれている.

図表 12 は，図表 3 と対比する意味で，総務省研究会の「第一次とりまとめ」で取上げられた課題と結論部分を共著者なりに要約したものである.米国のものが概念的・政策的であるのに対して，わが国のものが具体的・実務的なものである点に，両国の ACD と通信の秘密に関する世間一般の見方や反応が，凝縮されているように思われる.

なお，総務省の研究会メンバーである小山覚は，研究会の C&C サーバー対策に賛成しつつも，「事業者のコスト負担問題」と「感染したマルウェアの駆除が難しい」ことを今後の課題として指摘している[132] .

図表 12 サイバーセキュリティ上の課題と対処方針

課題	論点	結論
ACTIVE* の 普及・展開	利用者がマルウェア配布サイトにアクセスしようとする際，ISP がアクセスに係る IP アドレスまたは URL を検知し，注意喚起画面を表示することについて，どのような場合に「通信の秘密」を侵害しない有効な同意といえるか.	以下の 3 条件を満たせば，約款による包括的な同意であっても有効といえる.1）随時，同意内 容を変更できる，2）相応の周知が図られている，3）注意喚起画 面でも同趣旨が説明されている.
マルウェア感染駆除の拡大	C&C サーバーが takedown された場合，マルウェア感 染端末との間の通信履歴のうち IP アドレスとタイム・ スタンプにより，ISP が利用者を割り出して注意喚起す ることは，通信の秘密を侵すことになるか.	注意喚起の用途以外に使用しない場合は，緊急避難として違法性が阻却され，侵害とはならない.
DNSAmp 攻 撃**の防止	ISP ネットワークの入口か出口において，通過するすべての宛先IPアドレスとポート番号を調べ，動的 IP ア ドレス宛でかつ UDP53 番ポートに対して送信された通信をブロックすることは，通信の秘密を侵すことになるか.	DNSAmp 攻撃防止の用途以外に使用しない場合は，通信事業者の正当業務行為として違法性が阻却され，侵害とはならない
SMTP 認証 *** の情報を悪用したスパム・メールへの対処 (1)	サーバーの負荷増大の警告が出た場合，滞留したメールに係る SMTP 認証の発信元 IP アドレス，タイム・スタ ンプ，メール・アドレス，SMTP 認証の ID を分析して，不正使用の蓋然性が高いものについて，認証を一時停止す	左記の用途以外に使用しない場合は，通信事業者の正当業務行為として違法性が阻却され，侵害とはならない.

131 このガイドラインは，初版が 2007 年 5 月，第 2 版が 2011 年 3 月，第 3 版が 2014 年 7 月，現行の第 4 版は 2015 年の 11 月に策定されていて，第 2 版からは公表されるようになった.
132 https://digitalforensic.jp/2015/08/10/column374/

	るとともに，利用者にパスワード変更を依頼することは，通信の秘密を侵すことになるか.	
SMTP 認証 *** の情報を悪用したスパム・メールへの対処 (2)	他人の SMTP 認証の ID・パスワードを悪用したスパム・メールを防止するため，大量の認証失敗の警告が出た場合に，認証発信元アドレス，タイム・スタンプ，認証回数，認証間隔の分析から SMTP 認証の ID・パスワードのハッキング攻撃の蓋然性が高いものについて，攻撃期間中認証を止めることは，通信の秘密を侵すことになるか.	左記の用途以外に使用しない場合は，通信事業者の正当業務行為として違法性が阻却され，侵害とはならない.

＊ Advanced Cyber Threat response InitiatiVE という，総務省主導の官民連携プロジェクト

** DNS アンプ攻撃は，ドメイン名と IP アドレスの相互変換（名前解決）を行なう Domain Name Server に対して，交信するデータを増幅させることにより機能を妨害する DDoS 攻撃の一種

*** SMTP（Simple Mail Transfer Protocol）は e-mail の標準的手順.その認証とは，利用者がメールの送信依頼を行なう際に認証過程を導入し，正規の利用者であることを確認してから送信を受け付けること.

7.2.3 「第三次とりまとめ」

本稿執筆中の 2018 年 9 月 26 日に，総務省の上記研究会から「第三次とりまとめ」が公表された.このとりまとめでは，爆発的に増大する IoT 機器を悪用したサイバー攻撃が広がることを背景に，以下の事項について「通信の秘密」の観点から検討を行なっている.

① マルウェアに感染している可能性が高い端末の利用者に対する注意喚起，
② 注意喚起を目的とする，マルウェアに感染している可能性が高い端末の検知，
③ 有効な同意に基づく通信遮断を目的とする，C&C サーバーである可能性が高い機器の検知，
④ マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起.

このとりまとめで注目されるのは，次の 2 点である.

まず第 1 点は，これらの注意喚起なり検知を，利用者の被害や電気通信役務提供の支障発生の「未然防止」のために行なうとの観点が，採り入れられていることである.事後対応を原則としてきた解釈から，事前対策も取入れた ACD に近づいたものと評価できる.

また第 2 に，従来は通信の秘密侵害にはならない「利用者の有効な同意」といえるには「個別具体的かつ明確な同意」が必要とされていたところ，第三次とりまとめでは「例外」としつつも，一定の条件を付して契約約款等による包括的な同意でも良いとしている点である.その理由は，「利用者が，ISP において通信の秘密を侵すことについて通常承諾すると想定し得るため」であるとしている.

この理由づけを敷衍すると，サイバーセキュリティ被害が拡大・深刻化するにつれて，利用

者は「通信の秘密」に該当する情報であっても，それを活用することで安全な通信が確保されるなら，ISP が窃用・漏えいしない限り [133]，「より積極的な役割」を果たして欲しいという意向があると想定することと近い.その意味では，本稿で論じている「積極的サイバー防御」においてISP がより大きな役割を果たすことが望まれているとの想定と，軌を一にする面があると考えられる.

なお第三次とりまとめは，「円滑なインターネット利用環境の確保に関する検討会」が本年 2 月に公表した「対応の方向性」において，通信ネットワークの障害等に対する対処策の実施に向けて，通信の秘密やプライバシー保護等との関係で配慮すべき事項を検討するとし，その要請が研究会にあって，とりまとめられたものである.

同検討会の基本的な考え方としては，「現在は主として DDoS 攻撃等は発生した事後対処に主眼が置かれているが，（中略）今後は攻撃の予防に向けた対策を強化する必要がある.」というものである.また，同検討会の議論の中では，IoT 機器を含む脆弱な端末設備のセキュリティ対策を行なう場合には，国際競争力確保等及び IoT 機器の普及の阻害とならないようにすることも指摘されており，サイバーセキュリティ対策に産業的視点が加えられていることが注目される.

7.2.4 改正電気通信事業法・国立研究開発法人情報通信研究機構（NICT）法の成立

5.3 で述べたように，上記改正法が本年 5 月に成立・公布され，改正電気通信事業法の第 7 節 認定送信型対電気通信設備サイバー攻撃対処協会（以下，協会と呼ぶ）（第 116 条の 2 ～第 116 条の 8）の規定が新設された.また改正 NICT 法では時限立法ではあるが，NICT の業務として，「特定アクセス行為」を行なう規定が新設された.

「通信の秘密」の観点から注目されるのは，電気通信事業法 168 条の 4 において，「協会の役職員は業務に関して知り得た秘密を漏らしてはならない」と規定されており，168 条の 8 の 5 項で「協会が取り扱う（中略）通信履歴の電磁的記録は，電気通信事業者の取扱中に係る通信とみなして 3 条（注：検閲の禁止）及び 4 条の規定（注：秘密の保護）の規定を適用し，（中略）協会が行なう同号に掲げる業務に従事する者は，電気通信事業に従事する者とみなして同条第 2 項の規定を適用する.」と規定されていることである.

「通信の秘密」の観点からは，みなし規定によって 4 条 2 項の適用対象者の範囲を，初めて拡大したことが注目される.

133 「窃用・漏えいしない限り」というのは，図表 12 における「（特定の）用途以外に使用しない限り」と表裏一体であると考えられる.

7.3 インターネット利用を前提にした「通信の秘密」の再構築

7.3.1 通信当事者からみた「通信の秘密」の意義と電気通信事業者の対応

歴史的にみると，「通信の秘密」は公権力による検閲から信書を保護するための「信書の秘密」として近代憲法に登場した.離れた場所の間で通信を行なう場合には，通信を運ぶことを第三者に依頼せざるを得ないが，この第三者は電気通信においては電気通信事業者である.この電気通信事業者を信頼できなければ，通信当事者は安心して通信することができない.

従って通説では，「通信の秘密」の保護法益はプライバシーであるとされているが，それに加えて電気通信事業者を信頼して，通信当事者が安心して他からの干渉を受けずに，通信ができるという「通信の自由」を守るために「通信の秘密」の規定が設けられているとの意味合いもある（海野［2015］特に，pp.128-133）.

電気通信事業者は「通信の秘密」ないし「他人の秘密」を事業者の責務として，また企業倫理として長い間遵守してきた.この結果，「電気通信事業法において憲法と同じ通信の秘密が保護されており，しかもそれが非常に広くかつ強力な保護であると理解されている結果，一般的な個人情報・プライバシー保護を遥かに超える義務が，電気通信事業者に課されている[134]」との指摘がなされ，いわば「過剰」な状態が続いている.

しかしながら 7.2 で述べたように，インターネット利用において電気通信事業者は，「通信の秘密」を遵守することを引き続き求められると同時に，他の優越する法益を達成するため「通信の秘密」の保護を制限することも求められる，というディレンマ状況にある.

また 7.1.2 の位置情報に関して述べたように，当事者からみて同じような情報でも，あるものは「電気通信事業者の取扱中に係る通信」に該当するために「通信の秘密」となり，あるものは「取扱中の通信」に該当しないので，「通信の秘密」ではなく，個人情報・プライバシー情報として保護されていて，両者間の保護のバランスが取れていない.

7.3.2 メタデータの重要性

サイバーセキュリティ対策強化の観点からは，メタデータを知得，保存，分析，活用することがより重要になっている.

またインターネットはコンピュータ・ネットワークであり，業法によって規制されている電気通信事業者と当初から自由で規制されていないコンピュータ事業者によって，自律・分散・協調の仕組みの中で，サービスが提供されてきた.このため，メタデータは自分の情報[135]であって，自由に利用して良いと考えるコンピュータ事業者と，規制の下で利用するという電気通信事業

134 宍戸常寿「通信の秘密について」http:www.win-cls.sakura.ne.jp/pdf/35/02.pdf
135 この考え方にベースには，米国には個人が第三者に任意で提供した情報についてはプライバシーに対する合理的な期待（reasonable expectation of privacy）を有しないとの「Third-Party Doctrine」法理があるためであると考えられる.以下の文献を参照. “The Fourth Amendment Third-Party Doctrine” Congressional Research Service, 2014 年 6 月 5 日.https://fas.org/sgp/crs/misc/R43586.pdf

者間の見方には大きな違いがある.

米国の OTT 事業者は，ごく最近まで「情報サービス」を提供している者として，電気通信事業法の適用を受けずに自由に活動していて [136]，コンピュータ事業者の発想でメタデータや通信内容を活用して新しいサービス・市場を創造することを当然視していると考えられる.

もっとも，サイバーセキュリティ対策において，「積極的サイバー防御」を行なうために，メタデータを知得，保存，分析，活用するとしても，それはメタデータを保護しなくとも良いということではない.むしろ知得を今まで以上に認めるとすればするほど，知得後のメタデータの窃用・漏えいを防ぐための安全管理を強化しなければならない.「電気通信事業における個人情報保護に関するガイドライン」（平成 29 年 4 月 18 日総務省告示第 152 号）のような規定の意味合いが，より重要になってくる.

また「利用と保護」のバランスに関する法的な規範性を高める意味合いから，現在電気通信事業者団体が自主的に制定している「電気通信事業におけるサイバー攻撃への対処と通信の秘密に関するガイドライン」を，総務省告示とすることも，将来的な課題となるように考えられる [137].

本稿では，民間企業のサイバーセキュリティ対策において「通信の秘密」をどう考えたら良いかを論じているため，「通信の秘密」に関する国家権力の関与の問題は当面の検討対象外ではあるが，官民の情報共有が不可欠になった現状では，触れておかざるを得ない.

インターネットでは，テロの呼びかけやテロ要員のリクルートが行なわれ，また国家機密や企業の営業秘密を窃取し犯罪に利用する行為が多発しており，国家の関与が疑われるサイバー攻撃等も多く，欧米では国家安全保障，インテリジェンス活動および犯罪捜査のために，通信内容やメタデータの取得，保存，分析，活用などが幅広く行なわれていて，そのための法制度も整備されている.

2013 年にエドワード・スノーデンが暴露した米国のインテリジェンスに関する NSA（国家安全保障局）のプリズム，電話のメタデータ収集，アップストリームの三つのプログラムのすべてで，メタデータの収集・分析等が行なわれていた.

また，バルク・データの収集・分析については，米国では見直しが行なわれ，EU 市民の個人データの移転に関しては EU・米国間でセーフハーバー協定に代わり，新たにプライバシー・シールド協定が結ばれたが，英国で成立した IPA（Investigatory Powers Act）2016 では，プライバシー保護を強化する規定は盛り込まれたものの，バルク・データ収集については基本的な変更は行なわれていない [138].

---

136 1934 年通信法の適用を受けるのは「通信サービス」の提供者であり，「情報サービス」は長らく適用外とされてきた.近年この種の二分法を改め，通信法を広く適用しようとする動きがあるが，政権の交代もあり，なお最終決着していない.

137 ガイドラインの法的な性格については，注 129 と 130 を参照.

138 バルク・データ収集というのは，特定の情報を対象にした情報収集ではなく，ネットワーク上を流通する情報をある箇所ですべて収集する方式をいう.この問題については，以下の文献を参照.林・田川 [2016]，田川・林 [2017a].

7.3.3 メタデータに関する手続的保障の重要性

電気通信事業法 4 条の「通信の秘密」の保護対象は，通信内容とメタデータの両方である.EU でも e プライバシー指令（2002/58/EC）5 条において，通信（内容）とトラフィック・データの両方を対象として通信の秘密（confidentiality of communications）の遵守を規定している.また米国では「通信の秘密」に関する直接の規定はないが，「電子通信プライバシー法（ECPA）」において，「通信におけるプライバシー」として，通信内容とメタデータの両方が保護されている.

ただし，いずれの国にあっても，両者を全く同一に扱うのではなく，利用態様や人権侵害の蓋然性などを総合的に判断して保護レベルを決めている.そこで，両者を区分した上でそれぞれの保護水準を論ずる必要があるが，サイバーセキュリティ対策強化の観点からは，メタデータを知得，保存，分析，活用することがより重要になっている.また前節で述べたように，国家の「通信の秘密」への関与に関しては，欧米では通信内容やメタデータを取得，保存，分析，活用することが幅広く行なわれていて，そのための法制度も整備されている.

しかし，メタデータの重要性が高いにも関わらず，米国の法的な手続きにおいては，メタデータ利用の方が通信内容を利用する場合よりも手続き的に容易である [139].これに対して，米国では現行法がインターネット利用の現状に適合的ではないとの批判がなされてきた（「インターネットと通信の秘密 第 2 期研究会報告書」[2014]）.また，英国の IPA（Investigatory Powers Act 2016）においても，メタデータの方が利用しやすい手続きになっている.

7.1.1 で述べたように，メタデータを「通信の秘密」の保護対象とした理由は，「これらの事項を知られることによって通信の意味内容が推知される」ためというのが通説であった.しかし，今日のサイバーセキュリティ対策におけるメタデータやログの活用は，通信内容を推知するために利用されているわけではなく，サイバー攻撃に対して detect，prevent，mitigate するために用いられている.この過程で攻撃者の範囲を絞り込むことができるとすれば，通信内容よりもメタデータを利用した場合である.攻撃側はネットワーク化していると同時に，暗号通信など秘匿の手段を使うからである.

このため，「通信の秘密」の保護対象であるメタデータなりログを知得，活用している現状は，「通信の秘密」の保護対象にメタデータを加えた理由・趣旨とは異なっている.従って，通説の「通信の秘密」の保護対象とする理由とは異なる観点から，メタデータの取得や利用に関する手続的保障を，検討する時期に来たのではないかと考えられる.

7.3.4 サイバーセキュリティの観点からみた「通信の秘密」の再構築

音声アナログ電話とブロードバンドでは，その技術的基礎が異なっているので，現在の「通信の秘密」の概念を見直すべきとの主張を早くから行なってきたのが，多賀谷一照である（多

[139] 4.3 節で述べた ECPA に関して，米国人の感覚では stored communiation に関してメタデータを規律する第 2 部は，人間侵害の蓋然性が低いと考えるようである.注 68 を参照.

賀谷［1995］pp.109-133）.

彼の認識では，電話では電気通信事業者以外の第三者が「通信の秘密」を侵す可能性は低いが，データ通信（今日的にはインターネット[140]）においては，第三者が「通信の秘密」を侵す可能性が高まったので，形式秘としての「通信の秘密」の保護では，情報の保護システムとしては不十分になる可能性がある，というものである.

多賀谷はこのような認識に基づいて，「通信の秘密」の主観性・形式性が，人格権的な保護の法理に近い外形をもっているのは，音声通信の技術的特徴・制約に負うところが多いとして，「通信の秘密」の再構築に当たって考慮すべき，以下の基本原則を提言している.

① 基本的セキュリティの確保：電気通信事業者が保障すべきは，システムとしての通信の秘密総体，通信が安全かつ確実になされることである，
② 狭義の「通信の秘密」の概念：「通信の秘密」の概念は，通信のすべてではなく，人と人との間の私的な 1 対 1 の通話の実質をもつものに限定して維持されるべき，
③ 他の法益による通信内容の保障：②によって，「通信の秘密」として保護されない通信も，プライバシー保護，営業秘密の保護，消費者の保護など，他の法益の観点から保護の対象となる，
④ 「通信の秘密」のソフト的な捉え方・暗号処理：企業等がその営業目的などの重要な通信を行なう場合には，一般レベルでの「通信の秘密」では，セキュリティレベルとしては不十分.21 世紀においては，通信内容の保護，セキュリティ保護の重点は，回線のセキュリティから暗号鍵の保護に移っていることであろう.

このように，将来を見据えた提言を行なった洞察力に驚くとともに，本章で論じてきた「通信の秘密」の問題意識と底流で共通しており，共感する部分が多い.

7.4 再構築への一つの試論

7.4.1 議論の錯綜の要因

上記の分析を踏まえて，「通信の秘密」に関して一見混乱しているかに見える現状を整理し再構築して，サイバーセキュリティ対策に関してユーザ主導で電気通信事業者をエンパワーする方途を検討したい.

まず，議論の整理から始めよう.インターネットと通信の秘密に関して，現在の議論が錯綜しているかに見える要因として，1) コンピュータ屋と通信屋という発想の違うプレイヤーの存在，2) その間の法的な取扱の不整合，3) 「電気通信事業者の取扱中に係る」という限定規定の影響，の 3 点があると思われる.

まず第 1) について.インターネット・サービスは，異なる発想（マインドセット）を有する多様な

[140] データ通信という用語が使われているのは，インターネットが広く普及する以前の 1995 年になされたためである.

事業者によって提供されているが，彼らを大別すればコンピュータ屋と通信屋に分かれる.

前者は，主としてコンピュータ・ビジネスをリードした米国の事業者によって構成され，自分が提供するサービスによって取得した利用者のメタデータなどは，プライバシー保護の必要はあるものの，自由に利用して，サービスを改善したり新たなサービス・市場を生み出したいとの発想を持っている.

それはコンピュータ事業が初めから非規制であった（コンピュータ製造業も，コンピュータ・サービス業も AT&T や IBM に関する独禁法問題を除き，一度も事業法的規制を受けたことがない）ことに加えて，インターネットについても「非規制政策」を継続したこと（林 [2002]），更に第三者法理（Third-Party Doctrine[141]）が判例で認められていることに起因していると考えられる.この発想を共有する米国の OTT 事業者ないし GAFA（Google, Amazon, Facebook, Apple）に代表されるグローバル企業は，日本市場においても電気通信事業法の「通信の秘密」の非適用事業者として，自由に活動している.

一方，電気通信事業法の「通信の秘密」の適用事業者である電気通信事業者は，本稿で述べてきたように厳格な「通信の秘密」の解釈と運用を遵守しなければならない，との発想を維持してきた.しかし，インターネットがコンピュータ・ネットワークとしての特性を強めるにつれて，前者の発想が次第に前面に出るようになってきている.

そこで第 2）に，このようにインターネット・サービスにおいては，異なる出自と発想を有し，電気通信事業法の適用関係が異なる事業者が混在している結果，競争上 equal footing になっていない.ここで競争上問題になる非対称性とは，a）電気通信事業法 4 条の適用事業者，b）電気通信事業法 164 条 3 項の適用事業者，c）電気通信事業法の適用対象外の事業者，の 3 種類の事業者が，類似のサービスを提供しているにもかかわらず，異なった法的取り扱いを受けていることを意味している.

またこの非対称性は，電気通信事業法の効力が及ぶのが原則として日本国内に限られるのに対して，インターネット・サービスの広がりが電気通信事業法のカバーする範囲を超えている，との現象に関連する問題でもある.なぜなら，電気通信事業者の活動範囲は主として国内であり，国内法で対応可能であるのに対して，OTT 等の情報サービス会社の活動はグルーバルだからである.

第 3）は「通信の秘密」の規律対象が，「電気通信事業者の取扱中に係る通信」となっていることに起因する不整合である.携帯電話の基地局情報に係る位置情報のうち，個々の通話に利用される基地局情報は「取扱中」に該当するが，通信を成立させるために登録する位置情報は「取扱中」ではなく，「通信の秘密」の保護の対象外[142]である.また GPS 情報は，基地局の位置情報よりも精度が高いものの，「取扱中」には該当しないので，「通信の秘密」ではなく，個人情報として保護される.このように類似情報であって，あるものは「通信の秘密」に該当し，あるものは該当しないという，類似情報間において不整合がみられる.もう一つの不整合は，通

141 第三者法理については，注 135 を参照.
142 この問題については，注 119 参照.また石井 [2013] 参照.

信ログとEUのPNR（Passenger Name Record）指令のような非通信の間にみられるが，これについては第 8 章で述べる.

7.4.2 ユーザの同意あるいは要請に基づくサイバーセキュリティ対策の強化

7.3.4 で述べたように，インターネット利用においては「通信の秘密」の規定は情報の保護システムとしては不十分であり，電気通信事業者が保障すべきは，「システムとしての通信の秘密総体」，つまり「通信が安全かつ確実になされる」ようにすることである，との多賀谷説に賛同したい.この考え方は，セキュリティ・バイ・デザイン，サプライ・チェーン全体のセキュリティ確保など，多段階的なサイバーセキュリティ対策を強化することで実現すべきことを意味すると考えられる.

ところで 6.1 と 6.2 で述べたように，インターネットは自律システム（AS）の相互接続で成り立っている訳だから，全体を統制する主体が存在せず，ネットワーク機能の維持はそれぞれのシステム管理者に委ねられている.セキュリティが破られるのは，APT のようにエスタブリッシュメントを標的にした大規模攻撃の場合もあるが，the weakest point から入って徐々に大きな目標に近づいていく方法も，作戦的に展開されている.こうした多面的な攻撃に対応するためには，多層防御が必要になってくるが，それを自ら実行できる組織は，資金や人材の面から限られている.

そこで世間では，セキュリティ・ベンダーに頼ったり，業務システムの運用をクラウド事業者に委託する際に，ネットワーク監視も併せてアウトソースするなどの方法が取られている.このような中にあって ISP は，ネットワークの安定的運用が本来の業務であるから，他の事業者に対しても比較優位を持っている面がある[143]．

そこで「通信の秘密」の解釈・運用に関して再確認しておきたい点は，「ユーザの同意あるいは要請」を，明確にすることではないかと思われる.前 7.1.4 の法制局見解における「受信者の同意があればその内容を録音することも『通信の秘密』に触れるものではない」という法理が，インターネットにも準用可能だとすれば，ユーザが専ら自己のネットワークのセキュリティ確保のために，自らあるいは他者に委託してネットワーク監視を行なうことは，「通信の秘密」に触れるものではないと考えられる.

また仮に，より人権に配慮する観点から，法制局見解とは異なり「現行犯人であることを要する」と解釈しても，ウィルス作成罪や供用罪（刑法 168 条の 2 及び 168 条の 3）が法制化された今日では，これらに該当するデータを送信すること自体が違法なのだから，自己防衛する根拠は十分にあるだろう.

しかしなお，権利侵害を最小化するため法的根拠が必要であるとか，行為者の免責を明確にする必要があれば，契約約款に明記するか，4.5 で紹介した米国の 2015 年 CISA 法のよう

143 そして現に，グローバル・ネットワークに関する一元管理を中心に MSSP（Managed Security Service Provider）となることを，将来の事業ドメインにすると宣言している先駆的事業者も存在する.

な免責規定を，サイバーセキュリティ基本法か，他の適切な法律に明記することも考えられる.

7.4.3 インターネット・サービスの安定的提供のための特定の通信への役務提供拒否

上記の課題を実現するためには，新たな立法ないし既存法の改正による方法か，法解釈を変更して新たなガイドライン策定ないし既存ガイドラインの改正による方法が考えられる.それぞれの関係者が早急に検討されることを期待したい.

ここでは「通信の秘密」の厳格な解釈と運用の基礎にある，「利用の公平」に関して，若干の見直しを提案するため，インターネット・サービスの安定的提供のために特定の通信への役務提供拒否を可能にする電気通信事業法 6 条（利用の公平）の改正を提案したい.「利用の公平」は，電気通信事業者に，その役務の提供について「あまねく公平な取り扱い」を義務付けるもので，電気通信事業者が自ら運ぶ通信にノータッチ（hands-off）を求める基礎となっている規定である.

この規定は「あらゆる顧客を差別しない」ことを規定したもので，理念としては維持されるべきであるが，「対電気通信設備サイバー攻撃」を行なった者に対しても，「黙ってサービスを継続せよ」というのは，常識に反すると思われる.

既に迷惑メール防止法（特定電子メールの送信の適正化に関する法律 2002 年法律第 26 号）11 条では，いわゆる迷惑メールの送信者に対して，電子メールの送受信の支障を生じさせる恐れがある場合には，電気通信事業者は電子メール通信役務の提供を拒むことができると規定している.

また郵便法 12 条には，郵便禁制品に該当する物は郵便物として差し出すことができない，との規定がある.この規定は物に関する規定であって情報ではないが，迷惑メール 11 条の規定も併せ考えて，試案として巻末の参考資料に掲げる電気通信事業法の一部改正案を提案したい.この改正案は，不正な通信に対して電気通信事業者は役務提供を拒否できるとすることで，サイバーセキュリティ力を強化することによって，インターネット・サービスの安定的提供を確保しようとするものである.

なお，立法の経験もなく専門家でもない共著者が条文案まで提案したのは，ひとえに理解を深めていただきたいためだけである.実際の法制化に当たっては専門家の筆によって，より正確で整合性のある条文に仕上げていただけるものと期待している.

8 弱みを強みに転換する：まとめに代えて

8.1 小括

さて，そろそろ紙幅も尽きてきたし，実力もないのにあまりに大きなテーマに挑戦してしまったことを後悔してもいるので，この辺りでまとめの作業に入ろう.ここまでの議論を集約するとともに若干の補足を加えて，共著者が主張し，今後の早急な検討を促したいことの要点だけを記せば，以下の 7 点になる．①～④ は日米に共通の考え方で，⑤～⑦ は，わが国に特有のものである.

① 法治国家における救済は国家の手でなされるのが原則であり，自力救済は例外であるが，インターネットの世界には，attribution 問題に代表される「攻守の非対称」があるので，その歪みを是正する点までは自力救済が許されるべきである.

② 具体的には，attribution 問題を改善にするための情報の取得と，公衆衛生に類似するネットワーク全体の cyber hygiene あるいは清浄化（sanitization）を，サイバー攻撃の被害者側の対抗手段として適法化すべきである.

③ しかし第三者に危害を及ぼすことを避けるため，公的機関の関与の下で，サイバー攻撃に対する対抗手段を取ることが必要である [144].

④ プライバシーをはじめとした人権侵害の弊害を防止するため，国会の両院に「人権保障審査会」をおき，「通信の秘密」の順守状況とともに，行政の関連部門（消費者庁，公正取引委員会，個人情報保護委員会など）の活動のモニターを担わせるべきである [145].

⑤ わが国にはグローバルな競争力を持った IT 企業やセキュリティ・ベンダが少ないことも踏まえ，対電気通信設備サイバー攻撃を先駆的事例として，民間企業からの要請ないし同意に基づいて，電気通信事業者が上記 ② に記した範囲の行為を行なうことを容認すべきである [146].

⑥ また，電気通信事業者がユーザの委託を受けて，サイバーセキュリティの監視・マルウェアの除去，正常な機能の回復などを含む MSSP（Managed Security Service Provider）となることを支援すべきである [147] .

⑦「過剰と空白」を解消するなど，電話時代に生成された伝統的な「通信の秘密」を見直し

144 なお本来なら，この手続きを詳しく論ずべきかもしれないが，その時間と紙幅がない.要点は，インターネットの「自律・分散・協調」理念を生かしつつも，自力救済の実行者を認定するなどの最低限の安全措置を導入することであり，中国・ロシアなどに倣って国家主権を振りかざすことではない.

145 本文で深入りする余裕がなかったが，「通信の秘密」の弾力的解釈と「プライバシー侵害防止」とが両立すべきことは言うまでもない.ご関心があれば，林・田川 [2016] を参照願いたい.

146 電気通信事業者への期待が「過大」になるのではないか，との懸念が生ずるかもしれない.注 108 で紹介したシュナイヤーの懸念も同根であるが，それは制度設計の工夫で緩和するしかあるまい.もっとも，わが国における「媒介者としての責務」が，ISP に海賊版サイトのブロッキングまで求めるのは，弊害の方が大きいと思われる.この点に関しては，前掲注 130 も参照.

147 Rowe et al. [2011] が強く主張する点だが，同時に Lichtman and Posner [2004] が心配するモラル・ハザード（ユーザーは MSSP に頼り切りになって自助を怠る）にも配慮しなければならない.

て，インターネット時代にふさわしものに転換すべきである.

8.2 発想の原点：わが国のサイバー実力と経路依存性

ここで，小括で示した発想を持つに至った，背景情報を記しておこう.

まず，共著者にはサイバーセキュリティ能力に関する日米の実力の差は，読者の想像以上に大きい，という認識がある.それは，田川［2013］，田川・林［2017a］，田川・林［2017b］，林・田川［2012］，林・田川［2016］などの共同研究を通じて得られた感覚である.日米の軍事費以上に，日米のサイバーセキュリティ予算の開きが大きいことだけを取っても，納得していただけるだろう[148].笹川平和財団［2018］の指摘に同調した(5.4)のは，そのような経験に基づくものであった.

しかしに私たちは同時に，世の中の制度は多かれ少なかれ「経路依存性」を帯びており[149]，人為的に変更するのは容易ではないことも意識している.特に，社会的受容度が要件になるものは，そうなり易い.例えば，Nシステム[150]や，防犯カメラ(監視カメラ)はどうして受け容れられたのか？防犯カメラやドライブ・レコーダ映像の任意提出は非難されないで，むしろ奨励されるが，通信ログの保全や提供は厳しく指弾されるのは何故か[151].こういった疑問に，合理性だけを根拠に答えることは不可能だろう.

その極端な例は，PNR(Passenger Name Record[152])と通信ログの間の非対称的感覚ではないかと思われる.前者が航空交通のログで後者が通信のログだと考えれば，同じ扱いでも良いのではないかと考えられるが，誰もそのような主張はしていないようである[153].

それでは，このような「経路依存性」はどこまで達したら，人為的な「路線修正」を検討すべきであろうか.共著者は，2 つの条件(閾値)を考えている.1 つは，具体的な不具合の頻度であり，他の 1 つは「呪縛」(あるいは思考停止)という状況に陥っているか否かである.

前者は，少なくともサイバーセキュリティに関しては，見直しの必要があることまではコンセンサスが形成されつつある.7.1 で述べたことがその証拠になり得るが，その方法論は現状を維持しつつ，違法性阻却の範囲を逐次拡大するというものであった.しかし，それでは変化の激しいサイバー事案の「後追い」をするだけに終わってしまう，というのが共著者の懸念である.ところ

148 公開データによれば，2014 会計年度の米国のインテリジェンス予算は全体で 708 億ドルで，わが国の防衛予算全体よりも大きい（警察政策学会［2015］）.
149 「経路依存性」や「初期値過敏性」は，複雑系の経済学で脚光を浴びたが，およそあらゆる制度に付随する特質であろう（林［1998］）.
150 自動車ナンバー自動読取装置.日本の主要道路に警察が設置し，走行中の自動車のナンバープレートを自動的に読み取り，手配車両のナンバーと照合するシステム.
151 6.1 節で紹介した発信者番号表示システムのように，導入したいとする側が論点を明確にし，理詰めで社会を説得した例は，むしろ希である.
152 航空会社が保有する旅客の予約や搭乗手続きに関する情報.旅客予約記録.予約者の氏名・国籍・生年月日・性別・旅券番号・出発地・最終目的地，予約日・航空券番・旅行業者の名称・旅行日程・同行者の氏名・クレジットカード番号，携帯品の個数・重量・手荷物番号，搭乗手続きをした時刻・搭乗手続き番号など 35 項目が記録されており，テロ対策としても利用される.
153 それどころか，2013 年に JR 東日本が日立製作所に乗車履歴データを売ろうとした際，強い反発が起きたほどであった.

が，弊害を具体的に示すとなると，意外に難しい．

弊害は計量化できそうに思えるが，実は経路依存の弊害はそれに無意識で従っている人には意識されないので，むしろ「外圧」の方が核心を突いている場合がある．ガイアツを評価することは「非国民」との批判も聞こえてきそうだが，グローバル化した経済では関税のような目に見える部分は次第に平準化され，「非関税障壁」として見えない（あるいは見えにくい）部分が議論の中心になっている．つまり「制度の平準化」が求められる時代になっている．

サイバー分野の具体例として，国際的な情報共有を取り上げてみよう．ボットネット壊滅作戦のような国際共同作戦を実施する場合はもちろんのこと，4.5 で紹介した CTI（Cyber Threat Indicator）を共有する場合でも，秘密保全の法規と管理体制が同レベルに無い国と情報を共有すれば，「レベルの低い国が常に得をする」結果となる．そこで，レベルの高い国は「同じレベルの保護」を求めてくる[154]．わが国が遅まきながら「特定秘密保護法」を制定したのは，こうした背景があったと思われる．

8.3 呪縛からの脱却

このように目に見えない問題が重要なことは，後者の呪縛の方により当てはまる．実は「通信の秘密」は，このレベルに達しているのではないか，というのが共著者の共通認識である．私たちばかりか，前出（7.2.2）の小山（注 132）が「通信の秘密のトラウマ的な心理的障壁」と述べていたのは，電気通信事業に従事する者が全体としてマインド・コントロールされ呪縛に陥っていることを，簡潔な表現で示唆しているものと思われる．

これを純法律論として考察した藤田・高部・高嶋［2015］の次の件は，その間の事情を正確に伝えてくれる（pp.778-779）．

「一般に我が国における通信の秘密に対する姿勢は極めて慎重であり，知得する目的の正当性を厳格に吟味するとともに，これを第三者に開示する際には厳格な手続を要求する傾向にある．これは，旧公衆法時代から，通信の秘密が憲法の保障する基本的人権の 1 つして重要視され，（中略）罰則付きの通信の秘密保護規定が置かれ，通信の秘密の要素に該当する情報については特に必要がない限り極力知得すらすべきでないという認識が共有されていたことの影響である．」

そこで，いよいよ人為的な「路線修正」が必要な時期が来たと考えて，本稿をまとめるに至ったのである．しかし共著者は同時に，それに伴う困難と弊害にも気が付いている．困難とは，通説に慣れ親しんだ人々を説得することで，それにはなるべく平易な表現と比喩が有効であろう．その例として，先に注 96 で紹介した大学院でのケース・スタディの際，「インターネットNシステム」という比喩が院生から出されたことは，ヒントになるのではないかと考えている[155]．

---

[154] EU が個人データの保護に関して，adequate level of protection に無い国へは加盟国国民のデータを移転しないとしているのは，この原理を守っているだけともいえる．

[155] 外科手術の比喩も有効かもしれない．外科医が手術の前に「私の行為は違法性が阻却されるか」と自問するのは希であろう．それほどまでに外科手術の正当性は広く認識されており，不必要な施術や加害行為とみなされるケースは例

人為的な「路線修正」に伴う弊害に関しては，小括（8.1）の ④ でも触れたが，「通信内容」はもちろん「メタデータ」であっても，その秘密性は守るのが原則であって，それを利用するのは例外だから，例外措置を必要とする十分な理由が無ければならないし，手続きが守られるよう，監視機能を強化しなければならない.この点で，わが国の公文書管理の実態がはなはだ心もとないことは，多くの人が感じていることだろう.

8.4 弱みを強みに変える

最後に，「通信の秘密」の厳格な解釈と運用をインターネット時代に対応させるだけで，8.2 で共有したようなわが国のハンディキャップが改善されるのか，という疑問に答えよう.答えはもちろん「イエス」だが，そこには 3 つの側面がある.ます第 1 は，通信の秘密の厳格な解釈と運用によるログの未活用は，現状では「弱み」に違いないが，そこには大きな活用の余地が残っている訳だから，「強み」に転ずる要素でもあることである.

第 2 の側面として，私たちはデジタル社会が以下のような発想の転換を求めていると考えている.つまり，「デジタル社会では，匿名性確保と事後追跡可能性という 2 つの相反する要請のバランスを取ることが大切である」「現状では匿名性が担保される一方で，事後追跡可能性が狭められている」という仮説である.もしこの仮説が正しければ，ID とログは「サイバー空間の存在証明」のように考えることができるので [156]，その基本要素を改善することは，比較優位をもたらす可能性を秘めている [157] .

第 3 の側面として，その発想を延長すれば，技術変化で「Code が法になる」（Lessig の表現）より前に，「将来はどうあるべきか」を考えておくことが大切だと思う.GPS 捜査の合憲性が争われた米国の最高裁判決 [158] で「装着型 GPS 装置」の違法性を争っているうちに「すべての自動車に GPS 機能が事前搭載されるようになったら，妥当性の根拠が変わってしまう」という指摘 [159] があったことを思い出す.

以上のように私たちは，時代に遅れることなく，かつ人権の保障に配慮しつつ，「通信の秘密」の弾力的な解釈と運用で「弱みを強みに変える」ことは十分可能であると考えるが，読者の忌憚のないご批判を仰ぎたい.

[謝辞とお断り]

本稿を執筆するにあたっては，テーマの特殊性に鑑みて，（わが国では）異例の手順を踏んだ.本学の紀要は，運営母体である岩崎学園の創立記念日である 11 月 1 日発行と決められて

外中の例外である.
156 事実，ID をなくしたら「存在しないと同じ」ことになり，ログが消去されたら「過去に起きたことは（証明できないから）無かったこと」になる.
157 e-discovery について述べた，5.2 節を参照.
158 United States v. Jones, 565 U.S. 400 (2012)
159 上記判決におけるアリート判事ほか 3 名の補足意見.

いる.そこで，通常なら10月中旬の脱稿が期待されている(あるいは，それで十分である)ところ，共著者は第1稿を8月13日に，第2版を8月20日に，第3版を9月2日にと，立て続けに改版し発行した.そして多くの方々にコメントを求めたところ，実に有益なコメントを多数いただいたので，それらを生かしつつ推敲を重ね，10月15日に第4版，10月29日に第5版に達したところで，完成稿とすることができた.

この間，コメントをいただいた多くの方々に感謝している.既に公表された著作物によって，ご自身の立場を明確にされている方々には，「引用」によって共著者が謝意を表しているとご理解いただきたい.しかし，かなりの数の方は，法的にあるいは契約上「守秘義務」を負っているため，ここでお名前を上げることができない.それらの方々には，共著者の主張の陰にコメントの趣旨が生かされているので，「行間を読む」ことでお礼の気持ちを汲んでいただけるよう期待している[160].

このような事情があるため，読者にも「説得力が足りないな」という印象を持たれる方があるかもしれない.本文で展開した議論は，すべて公開情報で確認できるものに基づき，共著者自身が「証明力が足りない」と自覚した部分は，「仮説」という補足を付した上で注に回すなどの工夫をしたつもりであるが，なお説得力に欠けるとすれば，それは私たちの力量不足という批判を甘受するつもりである.

いずれにしても，情報セキュリティをテーマにする以上，私たちの悩みは今後も続くであろう.共著者は「これが最後の共同作品」との思いを込めて，この拙文を送り出す.次の世代が，私たちの意図と悩みをともに背負って，更なる展開をされることを期待する.

引用文献

[1] 石井徹哉 [2013]「通信の秘密侵害罪に関する管見」『千葉大学法学論集』27巻4号
[2] インターネットと通信の秘密研究会(第2期)[2014]『インターネット時代の「通信の秘密」各国比較』 http://lab.iisec.ac.jp/~hayashi/ の「プロジェクト」欄からアクセス可能
[3] 海野敦 [2015]『「通信の秘密不可侵」の法理』勁草書房
[4] 片桐裕 [1986]「電話の逆探知・通話の録音等」前田正道(編)『法制意見百選』ぎょうせい
[5] 金光昭・吉田修三 [1953]『公衆電気通信法解説』日信出版
[6] 警察政策学会テロ・安保問題研究部会 [2015]『米国国家安全保障庁の実態研究』同学会
[7] 小向太郎 [2006]『情報通信法と情報の自由：インターネットにおける情報流通を中心として』中央大学大学院法学研究科博士請求論文
[8] 斎藤文男 [1979]「電話システムと通信の秘密」『法政研究』45巻3－4号
[9] 笹川平和財団安全保障事業グループ [2018]『政策提言：日本にサイバーセキュリティ庁の創設

[160] 著作物については，原則として10月15日までに発行のものを，ウェブ・サイトについては同日現在のものを，報告書類については同日までに最終案が入手できたものを対象にしている.従って，谷脇康彦 [2018]『サイバーセキュリティ』(岩波新書)については，残念ながら触れることができなかった.

を！』
[10] 高橋郁夫・林紘一郎・舟橋信・吉田一雄 [2009]「通信の秘密の数奇な運命（事業法）」『情報ネットワーク・ローレビュー』第 8 巻
[11] 高橋郁夫・吉田一雄 [2006]「ネットワーク管理・調査等の活動と『通信の秘密』」JAIPA 行政法律部会報告 www.jaipa.or.jp/info/2005/iw2005.pdf
[12] 多賀谷一照 [1995]『行政とマルチメディアの法理論』弘文堂
[13] 多賀谷一照・岡崎俊一 [1998]『マルチメディアと情報通信法制―通信と放送の融合』第一法規出版
[14] 田川義博 [2013]「インターネット利用における『通信の秘密』」『情報セキュリティ総合科学』Vol. 5 http://www.iisec.ac.jp/proc/vol0005.html
[15] 田川義博・林紘一郎 [2017a]「英国 IPA(Investigatory Powers Act) 2016 に関する調査報告書」http://lab.iisec.ac.jp/~hayashi/170612%20IPA2016.pdf
[16] 田川義博・林紘一郎 [2017b]「サイバーセキュリティのための情報共有と中核機関のあり方 ―3 つのモデルの相互比較とわが国への教訓― 」『情報セキュリティ総合科学』Vol. 9 http://www.iisec.ac.jp/proc/vol0009/tagawa-hayashi17.pdf
[17] 土屋大洋 [2015]「意外だが，良く分かる米中のサイバー合意」連載「サイバーセキュリティと国際政治」『NEWSWEEK』オンライン版 https://www.newsweekjapan.jp/tsuchiya/2015/09/post-4.php
[18] 電気通信関係法コメンタール編集委員会 [1973]『電気通信関係法 詳解』一二三書房
[19] 電気通信法制研究会 [1987]『逐条解説 電気通信事業法』ぎょうせい
[20] トレンドマイクロ・セキュリティ・ブログ [2014]「オンライン銀行詐欺ツール DRIDEX，文書ファイルに埋め込まれた不正なマクロ経由で感染」 https://blog.trendmicro.co.jp/archives/10238
[21] 永野秀雄 [2016]「米国におけるサイバーセキュリティ法制の展開と現状―国家安全保障上の不可欠な制度基盤としてー」桜川ほか『国家安全保障と国際関係』内外出版
[22] 日本弁護士連合会 [2011]「『プロバイダ責任制限法検証に関する提言（案）』に対する意見書」
[23] 林紘一郎 [1998]『ネットワーキング：情報社会の経済学』NTT 出版
[24] 林紘一郎 [2002]「インターネットと非規制政策」林紘一郎・池田信夫（編著）『ブロードバンド時代の制度設計』東洋経済新報社
[25] 林紘一郎 [2005]『情報メディア法』東京大学出版会
[26] 林紘一郎 [2010]「著作権（著作物）と Property， Property Rule， そして Property Theory」『アメリカ法』2010-1
[27] 林紘一郎 [2014]「サイバーセキュリティと通信の秘密」土屋大洋（監修）『仮想戦争の終わり』角川学芸出版
[28] 林紘一郎 [2015]「サイバー攻撃と防御における非対称と解決の可能性」『第 48 回安全工学研究発表会予稿集』安全工学会
[29] 林紘一郎 [2016a]「サイバーセキュリティ担当の憂鬱」『予防時報』日本損害保険協会
[30] 林紘一郎 [2016b]「サイバーセキュリティ事故情報共有のあり方」『情報通信学会誌』Vol. 34，

No.3
[31] 林紘一郎 [2017]『情報法のリーガル・マインド』勁草書房
[32] 林紘一郎・田川義博 [1994]『ユニバーサル・サービス』中央公論社
[33] 林紘一郎・田川義博 [2012]「心地よい DPI（Deep Packet Inspection）と『程よい通信の秘密』」『情報セキュリティ総合科学』Vol. 4
[34] 林紘一郎・田川義博 [2016]「サイバーセキュリティにおけるバルクデータの意義」『情報セキュリティ総合科学』Vol. 8 http://www.iisec.ac.jp/proc/vol0008/hayashi-tagawa16.pdf
[35] 林紘一郎・田川義博・淺井達雄 [2011]『セキュリティ経営：ポスト 3.11 の復元力』勁草書房
[36] 藤田潔・高部豊彦（監修）高嶋幹夫（著）[2015]『実務 電気通信事業法』NTT 出版
[37] 松尾陽 (編) [2017]『アーキテクチャと法』弘文堂
[38] 森滋男・天野純一郎・岡田周平・桑田雅彦・大坪雄平・水越一郎・後藤厚宏 [2016]「日本年金機構サイバー攻撃事案におけるサイバーキルチェーン分析」『情報処理学会 コンピュータセキュリティシンポジウム 2016』pp863-869
[39] Alperovitch, Dmitri [2011] 'Towards Establishment of Cyberspace Deterrence Strategy,' in Czosseck, Christian et al. (eds.) "Proceedings of the Third International Conference on Cyber Conflict," CCD COE Publication
[40] Boose, Shelly [2012] 'Black Hat Survey: 36% of Information Security Professionals Have Engaged in Retaliatory Hacking,' "Business Wire," July 26
[41] Calabresi, Guido [1970] "The Costs of Accidents: A Legal and Economic Analysis," Yale University Press
[42] Calabresi, Guido & A. Douglas Melamed [1972] 'Property Rules, Liability Rules and Inalienability: One View of the Cathedral' "Harvard Law Review," Vol.85, No. 6
[43] Center for Cyber & Homeland Security, George Washington University [2016] 'Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats' https://cchs.gwu.edu/gray-zone-active-defense-private-sector-against-cyber-threats
[44] Clarke, Richard A., & Robert K. Knake [2010] "The Next Threat To National Security And What To Do About It" HarperCollins 北川智子・峯村利哉（訳）[2011]『世界サイバー戦争：核を超える脅威』徳間書店
[45] Craig, Amanda M., Scott J. Shackelford & Jannie S. Hiller [2015] 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis,' "American Business Law Journal" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573787
[46] CSRIC（Communications Security, Reliability and Interoperability Council）[2010] "Final Report: Internet Service Provider (ISP) Network Protection Practices," https://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf#search='csric+isp'
[47] Easterbrook, Frank H. [1996] "Cyberspace and the Law of the Horse," University of Chicago

Legal Forum.

[48] Eeten, Michel van, et al. [2010] 'The Role of Internet Service Providers in Botnet Mitigation: An Emperical Analysis on Spam Data' http://dx.doi.org/10.1787/5km4k7m9n3vj-en

[49] Epstein, Richard A. [2005] 'Intel v. Hamidi: The Role of Self-Help in Cyberspace,' "Journal of Law, Economics and Policy," Vol.1, Issue 1

[50] Garrie, Daniel & Shane R. Reeves [2016] 'An Unsatisfactory State of the Law; The Limited Options for a Corporation Dealing with Cyber Hostilities by State Actors', "Cardozo Law Review", Vol. 37, No.5

[51] Glosson, Anthony D. [2015] 'Active Defense: An Overview of the Debate and a Way Forward,' "Mercatus Working Paper," Mercatus Center at George Mason University https://www.mercatus.org/system/files/Glosson-Active-Defense.pdf#search=%27glosson+mercatus+working+paper%27

[52] Guzman, T. Luis de [2010] 'Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges,' "Catholic University Law Review," Vol. 59, Issue 2

[53] Harrington, Sean L. [2014] 'Cyber Security Active Defense: Playing with Fire or Sound Risk Management,' "Richmond Journal of Law and Technology," Vol. 20, Issue 4

[54] Hoffman, Wyatt & Ariel (Eli) Levite [2017] 'Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace?' Carnegie Endowment for International Peace https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236

[55] Huang, Shane [2014] 'Proposing a Self-Help Privilege for Victims of Cyber Attacks,' "The George Washington Law Review," Vol .82, No. 4

[56] IP Commission [2013] "The IP Commission Report," Commission on the Theft of American Intellectual Property http://ipcommission.org/report/index.html

[57] Jasper, Scott [2017] "Strategic Cyber Deterrence: The Active Defense Option," Bowman & Littlefield

[58] Kam, Steven [2004] 'Intel Corp. v. Hamidi: Trespass to Chattels and a Doctrine of Cyber-Nuisance,' Berkeley Technology Law Journal, Vol. 19, Issue 1

[59] Kerr, Orin S. [2005] 'Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability,' "Journal of Law, Economics, and Policy", Vol. 1, No. 1

[60] Kerr, Orin S. [2016] 'Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases,' "The George Washington Law Review," Vol. 84, No. 6

[61] Kesan, Jay P. and Ruperto P. Majuca [2009] 'Hacking Back: Optimal Use of Self-Defense in Cyberspace' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1363932.

[62] Kesan, Jay P. and Carol M. Hayes [2012] 'Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace,' "Harvard Journal of Law and Technology," Vol. 25, No. 2

[63] Koh, Harold [2012] ‘Remarks at CYBERCOM Interagency Legal Conference’ www.harvardilj.org/wp-content/.../12/Koh-Speech-to-Publish1.pdf

[64] Lee, Robert M. [2015] ‘The Sliding Scale of Cyber Security,’ “SANS Institute InfoSec Reading Room” https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

[65] Lessig, Lawrence [1999a] ‘The Law of the Horse: What Cyberlaw Might Teach,’ “Harvard Law Review,” Vol. 113, Issue 2.

[66] Lessig, Lawrence [1999b] “CODE and Other Laws of Cyberspace,” Basic Books 山形浩生・柏木亮二(訳)[2001]『CODE―インターネットの合法・違法・プライバシー』翔泳社

[67] Lewis, James Andrew [2013] ‘Private Retaliation in Cyberspace’, Center for Strategic and International Studies https://www.csis.org/analysis/private-retaliation-cyberspace

[68] Lichtman, Douglas Gary, & Eric A. Posner [2004] ‘Holding Internet Service Providers Accountable,’ John M. Olin Program in Law and Economics Working Paper No. 217

[69] McAfee [2010]‘Protecting Your Critical Assets, Lessons Learned from ″Operation Aurora″’ https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf

[70] McGee, Shane, Rady V. Sabetto, and Anand Shah [2013] ‘Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense,’ “Journal of Business & Technology Law,” Vol. 8, Issue 1

[71] National Research Council [2009] “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” The National Academies Press

[72] OECD(Organization for Economic Cooperation and Development)[2010] “Internet Intermediaries in Advancing Public Policy Objectives” https://www.oecd.org/internet/ieconomy/45997042.pdf#search='oecd+isp+public+objectives'

[73] Porta, Rafael La; Florencio Lopez-De-Silanes & Andrei Shleifer [2008] ‘The Economic Consequences of Legal Origins.’ “Journal of Economic Literature,” Vol. 46, No. 2

[74] Rid, Thomas [2013] “Cyber War Will Not Take Place”, Oxford University Press

[75] Rid, Thomas, and Ben Buchanan [2015] ‘Attributing Cyber Attacks,’ “Journal of Strategic Studies,” Vol. 39, No. 1

[76] Rowe, Brent, et al. [2011] ‘The Role of Internet Service providers in Cyber Security,’ https://sites.duke.edu/.../ISP-Provided_Security-Research-Brief_Row...

[77] Schmitt, Michael N., (General Editor) [2017] “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations”, Cambridge University Press 主要原則の抄訳と解説は，中谷和弘・河野桂子・黒崎将広 [2018]『サイバー攻撃の国際法：タリン・マニュアル 2.0 の解説』信山社

[78] Schneier, Bruce [2010] ‘Home Users: A Public Health Problem,’ in “Schneier on Security” https://www.schneier.com/essays/archives/2007/09/home_users_a_public.html

[79] Smith, Henry E [2005] ‘Self-Help and the Nature of Property,’ “Journal of Law, Economics

and Policy, ” Vol. 1, Issue 1
[80] Steptoe Cyberblog [2012] ‘The Hackback Debate’
https://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/

参考資料

「自己の設備に向けられた送信型対電気通信設備サイバー攻撃に対処するとともにウィルス作成罪等の実効性を高めるための電気通信事業法等の一部を改正する法律（案）」
新旧対照

.

同法案により，第 1 から第 3 を同時に改正する.

第 1：電気通信事業法（昭和 59 年法律第 86 号）第 6 条第 1 項の次に以下の第 2～第 7 項を追加し，同法 41 条および 52 条の改正も併せて行う.アンダーラインが追加部分.

（利用の公平とその例外）
第 6 条
1 電気通信事業者は，電気通信役務の提供について，不当な差別的取扱いをしてはならない.
2 電気通信事業者は前項の規定にかかわらず，その提供する電気通信役務のために使用する電気通信設備に対して，送信型対電気通信設備サイバー攻撃を反復継続して行った者に対して，電気通信役務の提供を拒否することができる.
3 電気通信事業者は第 1 項の規定にかかわらず，その提供する電気通信役務のために使用する電気通信設備を介して，刑法（明治 40 年法律第 45 号）第 168 条の 2 及び第 168 条の 3 に定める罪又はこれらの罪の未遂罪（以下，本条において「ウィルス作成罪等」という.）の元となる不正指令電磁的記録を送信することを，拒否することができる.
4 電気通信事業者は第 1 項の規定にかかわらず，その提供する電気通信役務のために使用する電気通信設備を介して，ウィルス作成罪等の元となる不正指令電磁的記録を送信する送信型対電気通信設備サイバー攻撃を反復継続して行った者，並びに同行為を行ったことにより有罪判決を受けてから 3 年を経ていない者に対して，電気通信役務の提供を拒否することができる.
5 前 3 項の規定は，行為者が代表権を有する法人に対しても適用する.
6 電気通信事業者は，前4項の事実を確認するために必要最低限の措置を採ることができる.この場合において当該措置に関して本法第 44 条に定めに基づいて総務大臣に届け出る管理規定に記載し，同一の内容を約款で公告したときには，本法第 4 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して，当該措置は正当業務行為として違法性が阻却されるものと推定する.
7 前項の規定は，電気通信事業者の顧客が被害を受け，当該顧客の委任を受けて電気通信事業者が

実施する場合にも適用する.
8 前 2 項の規定に基づき，個人情報保護法（平成 15 年法律第 57 号）に沿って匿名加工した情報を共有する仕組みに関しては，第 116 条の 2 ないし第 116 条の 8 の手続きに従う.

（電気通信設備の維持）
第 41 条 電気通信回線設備を設置する電気通信事業者は，その電気通信事業の用に供する電気通信設備（専らドメイン名電気通信役務を提供する電気通信事業の用に供するもの及びその損壊又は故障等による利用者の利益に及ぼす影響が軽微なものとして総務省令で定めるものを除く.）を総務省令で定める技術基準に適合するように維持しなければならない.
2 基礎的電気通信役務を提供する電気通信事業者は，その基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備（前項に規定する電気通信設備及び専らドメイン名電気通信役務を提供する電気通信事業の用に供する電気通信設備を除く.）を総務省令で定める技術基準に適合するように維持しなければならない.
3 総務大臣は，総務省令で定めるところにより，電気通信役務（基礎的電気通信役務及びドメイン名電気通信役務を除く.）のうち，内容，利用者の範囲等からみて利用者の利益に及ぼす影響が大きいものとして総務省令で定める電気通信役務を提供する電気通信事業者を，その電気通信事業の用に供する電気通信設備を適正に管理すべき電気通信事業者として指定することができる.
4 前項の規定により指定された電気通信事業者は，同項の総務省令で定める電気通信役務を提供する電気通信事業の用に供する電気通信設備（第 1 項に規定する電気通信設備を除く.）を総務省令で定める技術基準に適合するように維持しなければならない.
5 第 1 項，第 2 項及び前項の技術基準は，これにより次の事項が確保されるものとして定められなければならない.
一 電気通信設備の損壊又は故障により，電気通信役務の提供に著しい支障を及ぼさないようにすること.
二 電気通信役務の品質が適正であるようにすること.
三 通信の秘密が侵されないようにすること.
四 利用者又は他の電気通信事業者の接続する電気通信設備を損傷し，又はその機能に障害を与えないようにすること（不正指令電磁的記録の送信及び送信型対電気通信設備サイバー攻撃に対する耐性を含む）.
五 他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること.
第 41 条の 2 ドメイン名電気通信役務を提供する電気通信事業者は，そのドメイン名電気通信役務を提供する電気通信事業の用に供する電気通信設備を当該電気通信設備の管理に関する国際的な標準に適合するように維持しなければならない.

第 2:有線電気通信法（昭和 28 年法律第 96 号）第 5 条の第 3 項・第 4 項を加え，電波法（昭和 25 年

法律第 131 号）第 30 条に第 2 項・第 3 項を加える.

（技術基準）
有線電気通信法第 5 条
1 有線電気通信設備（政令で定めるものを除く.）は，政令で定める技術基準に適合するものでなければならない.
2 前項の技術基準は，これにより次の事項が確保されるものとして定められなければならない.
一 有線電気通信設備は，他人の設置する有線電気通信設備に妨害を与えないようにすること.
二 有線電気通信設備は，人体に危害を及ぼし，又は物件に損傷を与えないようにすること.
3 有線電気通信設備を設置した者は，前項の基準を達成するよう有線電気通信設備を維持・管理しなければならない.
4 有線電気通信設備を設置した者は，前項の事実を確認するために必要最低限の措置を採ることができる.この場合において当該措置を約款で公告したときには，当該措置は本法第 59 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して，違法性が阻却されるものと推定する.

（安全施設）
電波法 30 条
1 無線設備には，人体に危害を及ぼし，又は物件に損傷を与えることがないように，総務省令で定める施設をしなければならない.
2 無線設備を設置した者は，前項の基準を達成するよう無線設備を維持・管理しなければならない.
3 無線設備を設置した者は，前項の事実を確認するために必要最低限の措置を採ることができる.この場合において当該措置を約款で公告した場合には，当該措置は本法第 59 条に定める「秘密の保護」及び不正アクセス禁止法第2条第四号の「不正アクセス」の適用に関して，違法性が阻却されるものと推定する.

第 3：犯罪捜査のための通信の傍受に関する法律（平成 10 年法律第 137 号）別表第 2 に，次の事項を追加する

別表第 2「二 イ」の次に以下を挿入し，現在の「二 イ」以下を逐次繰り下げる
（新「二 イ」）刑法第 168 条の 2 若しくは第 168 条の 3 に定める罪又はこれらの罪の未遂罪