米国の ACD 対応事例から考える ACD 対応措置

中曽根平和研究所
大澤　淳*

2022 年に米国元国家情報長官のデニス・ブレア提督が来日し、自民党の政務調査会でのヒアリングやメディアでの対談で、「日本のサイバー防衛はマイナー・リーグ」と評し[1]、「ブレア・ショック」が関係者を襲った。同年 12 月の国家安全保障戦略で、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」[2]と高らかに宣言してから２年半、2025 年 5 月に、「能動的サイバー防御（ACD）」関連法案が成立し、日本もこれから能動的サイバー防御を実行する時代に入る。

マイナー・リーグの選手が、いきなり大リーガーのような野球をするのが無理であるように、日本の能動的サイバー防御の実施も、欧米の事例を参考にしながら、これから一歩ずつ経験を積んでいく必要がある。また、欧米とは異なる日本独自のACDのやり方も模索することとなろう。そのためにも、日本より約 10 年先行している米国を始めとした先進国の ACD 対応事例は、日本版 ACD を考える上で参考になると考えられる。

１．米国の能動的サイバー防御のコンセプト

米国における ACD 対応のコンセプトは、2015 年頃から議論され、先のブレア提督が主導したジョージ・ワシントン大学のプロジェクトでは、「アクティブ（サイバー）ディフェンスとは、従来の受動的な防御と攻撃の間に位置するプロアクティブなサイバーセキュリティ対策の領域」と定義され、具体的には、①攻撃側と防御側の間のサイバー空間における技術的な相互作用の中での、②攻撃者に関するネット上での情報収集と政策ツールの発動によるサイバー攻撃の抑制、とされている[3]。

安全保障関係者の民間における議論を受けて、米国「国家安全保障戦略 2017」[4]では、サイバー分野の重点項目として「悪意のある行為主体を抑止して排除する」ことが記述され、これを受けた「国家サイバー戦略 2018」[5]では、「悪意のあるサイバー攻撃者を抑止し、コストを課す政策選択をする」ことが打ち出され、サイバー攻撃者の帰属性（アトリビューション）を明確にした上で、あらゆる政策手段を用いて「米国に対する悪意あるサイバー活動を特定し、抑止し、防止し、結果責任を問う」ことが定められた。これらの文書で、サイバー攻撃の帰属性の特定と政策ツールの発動によるACD対応が明確に戦略として位置付けられた。

これらが具体化された国防総省の「サイバー戦略

---

* 中曽根平和研究所上席研究員。電通総研経済安全保障センター研究主幹、笹川平和財団上席フェローを兼務。

[1] デニス・ブレア、兼原信克他「日本のサイバー能力は[マイナーリーグ]」『正論』2022 年 6 月号（2022 年 4 月 30 日）。

[2] 内閣官房「国家安全保障戦略」（2022 年 12 月）21 ページ。

[3] Blair, Dennis C., et al., eds. *Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats*. Washington, DC: George Washington University, Center for Cyber and Homeland Security, 2016.

[4] “National Security Strategy of the United States of America”, White House, December 2017.

[5] “National Cyber Strategy of the United States of America”, White House, September 2018.

2018」[6]では、新たに「前方防衛（Defend Forward）」という概念が提示された。「前方防衛」は、悪意のあるサイバー活動をその策源地で妨害し、停止させるために、武力紛争未満の活動を含む防衛行動を前方（敵の領域内）で行うというものである。

米国ではサイバー攻撃の検知およびアトリビューションは ACD の重要な要素であり、通信のモニタリング、メタ情報・メタデータの収集、シンクホール、攻撃者を追跡するようなビーコンやハックバックなどの技術的なオプションも実施されている。

実際に使われる ACD ツールとしては、サンドボックス、ハニーポット、ダークウェブ上での情報収集などの低強度なものに加えて、攻撃者が使うサーバーのシンクホールや攻撃インフラのテイクダウン、ハックバックなどの高強度なものも用意されている。

テイクダウンなどの高強度な ACD 対応の国内での発動は、裁判所命令に基づき司法省と米連邦捜査局（FBI）が実施している。また、安全保障上詳細は明らかになっていないが、外国でのハックバックやテイクダウンなどの高強度な ACD 対応については、大統領令を受けて米サイバー軍（USCYBERCOM）が実施しているとみられる。それ以外に、政策的なツールとして、制裁や訴追、外交交渉などが同時並行的に行われる。

2. ACD 対応事例

ここからは、実際に行われた米国の ACD 対応事例をいくつか見ていきたい。

先端技術へのサイバー攻撃に対する ACD 対応

一つ目は、APT1（中国人民解放軍61398部隊）の事例である。APT1 は、2006 年から 2013 年頃にかけて米国に対して情報窃取型のサイバー攻撃を行っていた。その主な目的は、米国の民間企業からの知的財産及び先端技術の窃取、政策関連情報の窃取である。この攻撃グループは、情報テクノロジーや航空宇宙関連などにとどまらず、鉄鋼、ソーラーパネル、金融、交通など幅広い米国の産業にサイバー攻撃を行い、技術情報を窃取していたことが明らかになっている。

この APT のサイバー攻撃キャンペーンに対して米国は、国防技術および自国の産業競争力が奪われる経済安全保障上の懸念から、ACD 対応を行っている。この時期の米国の ACD 対応は、技術的な ACD 対応戦略の位置付け前であり、政策的な ACD 対応が行われていたのが特徴的である。

具体的には、2013 年 2 月にセキュリティ企業マンディアント社が APT1 に関するレポート[7]を公表している。レポートの中で、サイバー攻撃のアトリビューション、APT1 と中国人民解放軍の関わり、攻撃の手口、攻撃対象などを明らかにした。この手法は、「名指し非難（Name and Shame）」と言われる ACD ツールである。これに続いて、2013 年 3 月には脆弱性対応として政府機関における中国製通信機器の調達・使用禁止の通達、2013 年 5 月には国防総省の「中国の軍事力に関する年次報告書」[8]による「名指し非難」が行われた。

さらに、2014 年 5 月に、米司法省は APT1 の実行犯である中国人民解放軍の 5 名を特定して訴追・指名手配している[9]。訴追状では、APT1 の攻撃者がウェスティングハウス（原子炉）、ソーラー・ワールド（太陽光パネル）、アレゲニー・テクノロジーズ（特殊金属）、US スチール（鉄鋼）などに対してサイバー攻撃を行い、産業スパイなどを行ったと指摘し、この 5 名を訴追している。

---

[6] “Summary, Cyber Strategy 2018”, Department of Defense, September 2018.
[7] “APT1: Exposing One of China’s Cyber Espionage Units,” Mandiant, February, 2013.
[8] “Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013,” Department of Defense, May 2013.
[9] “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” Department of Justice, May 19, 2024.

米国は、2015 年 9 月に行われたオバマ大統領と習近平主席の首脳会談において、中国の国家組織による米国民間企業へのサイバー攻撃を非難し、「米中両国は営業秘密を含む知的財産に対してサイバー攻撃を行わないこと」で合意に達した。この首脳合意を機に、中国を発信源とする米企業へのサイバー攻撃は劇的に減少したと分析されている[10]。

価値や選挙へのサイバー攻撃に対する ACD 対応

米国では、上記の APT1 のケースのような技術を標的とした情報窃取型サイバー攻撃への対応にとどまらず、米国の民主主義といった価値や選挙に対するサイバー攻撃に対しても ACD 対応を行った事例がある。

一つ目は、2014 年に発生したソニーピクチャーズ・エンターテイメントに対する北朝鮮による身代金要求（ランサム）型のサイバー攻撃である。この事例では、北朝鮮のサイバー攻撃者は、同社が制作した金正恩暗殺をテーマとした映画を公開しないように要求するとともに、要求が通らないと分かると、映画館に対するテロを示唆した。

映画の公開停止要求を表現の自由に対する脅迫と懸念した米国では、2014 年 12 月 19 日に FBI がサイバー攻撃を北朝鮮によるものと発表し、「名指し非難」を行うと共に、同日に英国と共同で北朝鮮のサイバー攻撃を非難する国際パブリックアトリビューションを外交措置として行った。さらに翌 2015 年 1 月には、攻撃主体として関与した北朝鮮の偵察総局などに対して経済制裁を行った。

二つ目は、選挙に対するサイバー攻撃や影響工作に対して、米国がかなり強い ACD 対応を行った例である。ロシアによる 2016 年の大統領選挙への介入に対する対応である。2016 年の大統領選挙では、民主党全国委員会にロシアの情報機関と関係があると指摘されている APT28/29 の攻撃主体が侵入して、秘密情報をリークすると同時に、ロシアの代理主体 IRA（Internet Research Agency）が Twitter や Facebook 上で偽情報の流布という影響工作を行った[11]。

このような選挙制度に対するサイバー攻撃に対して米国は、2018 年の中間選挙を前に、IRA（法人）および同社従業員 12 名と資金提供者のプリゴジン氏への司法訴追を行った。さらに強度な技術的 ACD 対応として、ハックバックやテイクダウンが IRA の攻撃アセットである米国外の IT 機器に対して行われた。報道[12]によれば、中間選挙直前の 11 月 6 日から数日間にわたって、トランプ大統領の命令に基づき、IRA の攻撃アセットのアクセス遮断を行うと共に、工作を行っている要員の PC 画面に警告を表示したとされる。

基幹インフラへのサイバー攻撃に対する ACD 対応

安全保障上重大なサイバー攻撃に対して、ACD 対応がなされた例として、2 つの例を紹介したい。一つは 2021 年に発生した、米国のコロニアル・パイプライン社に対するランサム攻撃である。もう一つは 2021 年頃から発生している、米国基幹インフラへの Volt Typhoon と呼ばれる中国の攻撃主体のサイバー攻撃である。

コロニアル・パイプラインの事例では、米国東部にガソリンと航空燃料を供給するパイプラインが停止し、社会経済活動に大きな影響が出た。2021 年 5 月 6 日に発生した攻撃に対して、翌日に米国政府は省庁横断会議を開催し、強度な ACD 対応を行った。FBI を中心に米国内のランサムウェアのデータ送信先サーバーをテイクダウン(5 月 7-8 日)、身代金

[10] “Red Line Drawn: China Recalculates Its Use of Cyber Espionage,” FireEye, June 20, 2016

[11] “Open Hearing: Social Media Influence in the 2016 U.S. Elections,” U.S. Senate Select Committee on Intelligence, November 1, 2017.
“Exposing Russia’s Effort to Sow Discord Online: The Internet Research Agency and Advertisements.” U.S. House of Representatives Permanent Select Committee on Intelligence

[12] Ellen Nakashima, “U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms,” The Washington Post, February 27, 2019.

が送金されたデジタルウォレットが保管されたサーバーから身代金を回収（5 月 7-9 日）、攻撃を行った犯罪グループが利用している攻撃インフラ（リークサイト、データ格納サイト、身代金交渉用のサイト）をテイクダウン（5 月 7-13 日）した。攻撃発生から 1 週間で、国内外での強度な ACD 対応によって、事件を収束させた。

米国が素早いACD対応が行えた背景には、FBIが半年以上前から攻撃グループの行動を通信のモニタリングによって監視していた、という事前の ACD 対応がある。このような事例は、日本が通信情報の利用をどのように行うかを考える上でも参考になる。

2021 年頃から発生している Volt Typhoon のサイバー攻撃では、中国政府と関係する攻撃主体が、将来の有事における機能破壊を目的として、サイバー侵入・偵察行為を、米国の基幹インフラに対して繰り返していると指摘されている。

これに対して、2023 年 5 月 24 日、マイクロソフトから Volt Typhoon の脅威インテリジェンスを発表し、「名指し非難」を行うと共に、国際連携によるパブリックアトリビューションとして、米英加豪 NZ などによる共同注意喚起の発出を行った。さらに、強度なACD対応として、2023 年 12 月、米司法省および FBI は、裁判所の許可に基づき、サイバー攻撃主体に乗っ取られているSOHOルーターなど数百のIT機器からなるボット群に対するテイクダウンを実施した。具体的な被害が出ていない中での強度な ACD 対応の背景には、将来の軍事衝突時の重要インフラへの破壊活動の阻止、という安全保障上の目的があったと考えられる。

3. 結語

ACD 発動の対象は、特定の目的を持って長期間活動しているサイバー攻撃主体となる。防衛技術の窃取や日本の安全保障情報、半導体や航空宇宙など特定産業の技術を窃取するなどの目的で情報窃取型のサイバー攻撃を行っている主体も含まれると考えられる。

このような攻撃主体は長い期間にわたって同じ目的を持ってサイバー攻撃を繰り返し行ってくるので、10年ほど遡って、過去の攻撃キャンペーンも見ないと、攻撃者の特定や意図、将来の標的は分からない。また、サイバー攻撃主体のアトリビューションは、攻撃主体と目的の特定に時間を要するため、ACD ツール発動の見極めが難しいのが、現実の課題としてある。

ACD 対応は、政治的意思決定の側面が大きく、一律に被害状況から対応措置をきめられるものでもない。攻撃者が国家主体の場合は意図と結果の両方、犯罪集団の場合は社会経済活動への影響からACD の対応の可否が判断されよう。米国では経済的な被害だけでなく、国家の基本的価値（表現の自由、民主主義）を破壊するような攻撃に対しても、強い ACD 対応を発動している。

これから本格化する日本の能動的サイバー防御の実施にあたっては、これらの欧米の事例を参考にしながら、試行錯誤をしていく必要がある。欧米とは異なる日本独自の ACD のやり方の追求も必要となろう。

以上

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/