サイバー安全保障における先端技術保護
――アクティブ・サイバー・ディフェンスの現在

中曽根平和研究所主任研究員
大澤 淳
おおさわ じゅん　一九七一年生まれ。慶應義塾大学卒、同大学大学院法学研究科修士課程修了。世界平和研究所研究員、外務省国際情報統括官組織専門分析員、総合外交政策局外交政策調査員、ブルキングス研究所客員研究員、内閣官房国家安全保障局参事官補佐を経て、二〇一七年から現職。鹿島平和研究所理事、笹川平和財団特別研究員を兼ねる。

安全保障の大きな脅威であるサイバー攻撃対策は、受け身一方から能動的行動へ進化している。相手を逆探知し、技術・経済・訴追コストを賦課することで抑止を狙うACDとは何か。日本における本格導入の課題を探る。

「国家安全保障戦略」をはじめとする「安保三文書」では、サイバー安全保障分野で「能動的サイバー防御（アクティブ・サイバー・ディフェンス：ACD）」が採用された。ACDは、圧倒的に攻撃側が有利と言われるサイバー空間において、サイバー攻撃側にコストを賦課することで、その抑止を試みる、という考え方である。政府内では一四年頃から議論されており、一八年のサイバーセキュリティ戦略では、「積極的サイバー防御の推進」「サイバー攻撃に対する抑止力の向上」という形での記述がなされた。

安保三文書はACDに踏み込む

二〇一八年時点のACDは、サイバー攻撃の脅威情報の迅速な共有により、事前に防護手段を講じるという情報共有の側面が強い施策であった。これに対して、二二年の安保三文書での記述では、より踏み込んだ形でのACDの実施が謳われている。「国家安全保障戦略」では、「安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」との表現が盛り込まれた。また、自衛隊の役割についても、「今後、おおむね一〇年後までに、（中略）自衛隊以外へのサイバーセキュリティを支援できる態勢を強化する」との文言が「国家防衛戦略」に入り、自衛隊自身のネットワーク防衛のみならず、わが国全

体のサイバー空間の防衛にも一定の役割を果たすことが示された。

これらを受けて、具体的な「防衛力整備計画」では、二〇二七年度を目処に、自衛隊サイバー防衛隊等のサイバー関連部隊を約四〇〇〇人に拡充し、サイバー要員を約二万人体制に強化するとともに、サイバー・スレット・ハンティング（脅威追跡）機能を強化し、重要インフラ事業者および防衛産業などの民間との連携強化を行うことが記された。

米英仏などのサイバー先進国では、サイバー安全保障におけるＡＣＤの採用について、おおむね一八年頃までに戦略文書上に明記がなされ、体制整備とＡＣＤオペレーションの実施が行われてきている。今回の安保三文書改定により、わが国のサイバー安全保障も、文言上は欧米先進国と同様の戦略を持ち、体制整備が行われることになる。

ただし、サイバー安全保障は、陸海空などなじみの深い他の防衛分野と趣を異にしている。大阪の急性期医療センターがランサムウェアに襲われたように、サイバー空間では日々実際の攻撃が行われており、三六五日二四時間で対処する必要がある。では、具体的にどのようなオペレーションを行うのか、ＡＣＤは読者にも馴染みのない概念と思われるので、少し解説していきたい。

能動的サイバー防御（ＡＣＤ）の実際

従来のサイバーセキュリティが、エンドポイント防御やデータ・バックアップなどの抗たん性の確保といった、自己のＩＴネットワーク内の受動的な防御方法であるのに対して、ＡＣＤは、直接攻撃者に対してオペレーションの対応を行うところにその特徴がある。二〇一六年、デニス・ブレア元国家情報長官やマイケル・チェルトフ元ＤＨＳ（米国国土安全保障省）長官が参加した米・ジョージ・ワシントン大学のプロジェクト報告書では、「ＡＣＤ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対策の領域である」と定義している。

具体的なＡＣＤオペレーションは、次のような手順を経る。まず、国家安全保障に脅威を与えうるサイバー攻撃に対して、平素から通信のモニタリングなどを通じて警戒監視を行い、重大なサイバー攻撃を検知した場合には、サイバー攻撃者をハックバック（逆侵入）などの技術的な手段を用いて特定（アトリビューション）する。その上で攻撃者に対して、コストを賦課するため、テイクダウン（攻撃者が用いるＩＴ機器の停止）などの技術的な対抗手段を用

いて攻撃の無効化を試み、金融制裁や司法訴追などの政策的な対抗手段も用いて、さらに追い込んでいく。これにより、一方的に攻撃を受ける形ではなく、こちらから相手に働きかけることができる。

米国では、二一年五月六日に発生したコロニアル・パイプライン社に対するランサムウェア型サイバー攻撃に対して、ACDオペレーションを発動している。この攻撃は、ロシア系の「ダーク・サイド」というグループが犯人であり、FBIはこのグループを前年秋から監視していたが、サイバー攻撃による石油パイプラインの停止という国家安全保障上の重大事案を受けて、ホワイトハウスの国家安全保障会議が省庁横断チームを編成してACDを実施した。攻撃の二日後には攻撃者が用いる中継サーバーをテイクダウンし、三日後までに攻撃者が手に入れたビットコインの身代金を差し押さえた。攻撃者ダーク・サイドは五月一三日に、「攻撃から一切の手を引く」と表明し、米国政府に対して完全に白旗を揚げた。

ACDによる先端技術保護の課題と展望

米国では、重要インフラへのサイバー攻撃といった安全保障上の脅威への対抗措置だけでなく、サイバー攻撃を用いた知的財産や営業秘密の窃取（情報窃取型サイバー攻撃）にもACDを実施している。国家が関与して行われる情報窃取型サイバー攻撃によって、安全保障上重要な先進技術や企業競争力に直結する重要技術が盗まれ、国家の産業競争力が失われる懸念が生じているからである。実際に、サイバー攻撃によって窃取した軍事技術を戦闘機などの自国の兵器開発に利用する事例や、窃取した西側民間企業の技術を自国の企業に渡して産業競争力を高めた事例が発生している。

米国は二〇一四年頃から、このような先端技術を狙ったサイバー攻撃に対して、アトリビューションを実施して攻撃者を特定し、司法訴追を含むあらゆる政策を動員して攻撃側にコストを賦課するという、ACDによる対抗措置を取っている。一四年五月に米国司法当局は、米国のウェスティングハウス社（原子炉）、ソーラーワールド社（太陽光発電）、USスティール（鉄鋼）などのネットワークに情報を窃取する目的で侵入し、情報を窃取した疑いで、攻撃実行グループ「APT1」に属する中国人民解放軍61398部隊（上海）の将校五名を訴追した。

このような先端技術保護のためのACDの実施は、米英の国際協力で行われた事例もある。一七年四月に、英国の

大手防衛産業ＢＡＥとＰＷＣは、英国政府サイバーセキュリティ・センターの協力を得て、サイバー攻撃グループ「ＡＰＴ10」が行っている情報窃取型サイバー攻撃に関して報告書を公表した。報告書では、ＡＰＴ10の攻撃者のうち二名が、中国国家安全部と関係があることが指摘されていた。

一八年一二月米司法省は、クラウドサービスなどを提供する会社への不正アクセスを通じて、四五以上の企業の技術情報を窃取したとして、中国国家安全部の関係者である中国人ハッカー二名を訴追したと発表した。米国はこれらを含め、一四年から二〇年までの六年間で、人民解放軍の将兵五名、国家安全部の高官二名を含む、中国の軍や情報機関の協力者二〇名以上を特定して司法訴追している。

日本のＡＣＤは国内法整備が課題

こうしたＡＣＤによる先端技術保護の試みは、日本でも取り組みが始まっている。二一年四月二〇日に警察庁は、住所・氏名を偽って日本のレンタルサーバー会社と契約を行ったとして、中国共産党員の男を私電磁的記録不正作出・同供用の疑いで書類送検した。この男がサーバーのＩＤを転売した相手は、ＪＡＸＡをはじめ三菱電機やＩＨＩ、大学など、防衛・航空宇宙関連の約二〇〇の企業や研究機関へのサイバー攻撃を実行していた中国のサイバー攻撃グループ「Ｔｉｃｋ」であった。Ｔｉｃｋの背後には、中国人民解放軍６１４１９部隊（青島）が関わっていることが、警察庁長官の記者会見で指摘されている。

警察庁の取り組みは、地道なリアル捜査をベースとしてサイバー攻撃者の関係者を特定したものであり、サイバー技術を用いて攻撃者を特定する純粋なＡＣＤではなかった。しかし、今後ＡＣＤを実施する体制が整えば、日本でも欧米並みに、サイバー攻撃者にコストを賦課することで攻撃を難しくし、先端技術をサイバー攻撃から防護することが可能になる。

しかしながら、ＡＣＤを実施するためには、これからさまざまな国内法的な制約を改めていく必要がある。攻撃モニタリングには通信事業法の改正が、ハックバックには不正アクセス禁止法の改正が必要となる。これらの法的環境の整備には、険しい道を果敢に進まなければならないが、知的財産や営業秘密を狙った情報窃取型サイバー攻撃が、結果的に中国の技術力を強化し、中国の産業競争力を押し上げ、中長期的には国家間の力関係に重大な影響を及ぼすことを鑑みれば、安全保障上喫緊の課題として、優先的に取り組んでいく必要がある。●