特集／経済安保を巡る諸情勢

〈6〉サイバー安全保障分野の対応能力向上に向けて
―能動的サイバー防御法及び国連サイバー犯罪条約を活用して―

国際安全保障研究家　福井　康人

はじめに

近年になってから様々なサイバー攻撃に晒され、対象も中央官庁から一般の医療機関や企業まで様々な組織のコンピューターが攻撃され、機能不全に陥り、金銭の詐取が行われ、いわゆるランサム・ウエア等の実例を挙げると頻繁に起きている。その手法も益々高度化しており、特定のURLを掲載したメールを不用意にクリックすると、ウイルスに感染し、内蔵データが暗号化されて解除のために金銭を要求されたりする。この手法も既に進化して、QRコードから特定のサイトに誘導する手法も現れている。更にはAI機能により、ウイルス対策ソフトを無力化するウイルスも出回り始めており、サイバー安全保障分野も追いつくのが大変なくらい、ウイルス技術も日進月歩の状況にある。

そのような中で、多くのサイバー攻撃が国外から発信されており、専門家チームが攻撃者を特定するのも、通常は複数のサーバーを踏み台にして攻撃が行われたりすることが多いので、即座に犯人を特定することは容易でなく、正に軍隊のような集団が背後に居るのではないかと思われるような事例もある。このため日本でも、国レベルの対応が必要とされ、2025年5月に内閣官房のサイバー安全保障体制準備室が中心となって、いわゆる「能動的サイバー防御(ADC)法」[1]の整備が検討された結果として、既に法改正が実施され[2]、これまでNISCと呼ばれていた内閣官房の一部門が国家サイバー統括室（NCO）に改組されて、既に活動を開始している。

本稿では、この制度について解説するとともに、長年の条約交渉の結果、昨年末の国連総会で採択され、2025年10月25日及び26日に署名開放された国際サイバー犯罪条約は40か国が締結後90日で発効し、サイバー安全保障の観点から有益なようなものである。同条約についてもこれまでも取り上げたことが有るものの、まだ条約交渉が難航していた時のものなので、本稿の後半に取り上げて、この両者の目的が異なるものの、協働しうるものであること

[1] 正式には、「重要電子計算機に対する不正な行為による被害の防止に関する法律（サイバー対処能力強化法）（令和７年法律第４２号）」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う 関係法律の整備等に関する法律（令和７年法律第43号）」の二法を指すが、本稿では便宜上以下「対処能力強化法」及び「同整備法」とする。

[2] 内閣官房、サイバー安全保障整備準備室『サイバー対処能力強化法及び同整備法について』令和７年５月。同資料には内閣官房サイバー安全保障体制整備準備室から法案提出した際の説明資料の一つを法案成立後に加筆訂正されたもので、日本政府の公式見解をまとめたものとも言える。なお、筆者が特に参考になったものは検討会議資料の中で酒井啓一教授の説明資料『サイバー安全保障分野での対応能力の向上に向けた有識者会議第１回アクセス・無害化措置に関するテーマ別会合』は国際法の観点から書かれた有益な資料である。
URL ＜ https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/siryou6-5.pdf ＞ accessed 24 September 2025.

を示したい。

特に前者は既にNCOが稼働し始めているものの、求人広告やニュースを見ていると実務を担う警察なども、今もサイバー人材が不足している模様である。また、民間企業でも採用が追い付かず苦労しているように見える。本稿を執筆するにあたり参考にしたものは、先ず前者の関係では国会事務局関係者が執筆したものとして柿沼重志による『能動的サイバー防護の導入―サイバー対処強化法案及び整備法案の概要と主な論点』[3]や持永大による『能動的サイバー防御』[4]が挙げられる。前者は各種レクに同席することが有る関係者が執筆しているので内容が比較的正確であり、二冊目の文献は日本の国家安全保障戦略の進化の観点から書かれており、諸外国の類似例も取り上げられている。

また、国連サイバー犯罪条約については、国連薬物犯罪事務所（UNODC）が条約について作成過程等を公開している他、後述するが同条約が国際組織犯罪防止条約（UNTOC）及び国連腐敗防止条約（UNCAC）等を前例としている条文も多いことから[5]、これらの条約のコメンタリーも同条約の内容を理解する上で参考になる[6]。いずれにしても、この条約には市民社会との協力が謳われていて、アカデミアからの参加者も居るので、将来には同条約のコメンタリーも刊行される可能性が高いと思われる。

なお本稿は通説的な理解を基にまとめたものであるが、筆者自身の調査研究の結果であり、著者が過去に所属した機関等の意見を代表したものではなく、筆者の理解を纏めたものであることを予め付言させて頂く。

１．能動的サイバー防御法

（１）基本的考え方

このような取組が始まったのは、過去の経緯をたどると令和４年12月１６日に国家安全保障会議が決定し、閣議決定された「国家安全保障戦略」に由来する[7]。その中でも、サイバー安全保障の能力向上について、「武力攻撃に至らないものの、国、重要インフラ等に対する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。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備する」ことを言及している[8]。

ではこの国際法の観点から見た位置付けについては上掲注2に引用した『アクセス・無害化措置と国際法の関係係－能動的サイバー防御（ACD）の国際法上の評価―』のまとめにあるように、「ACDが国際違法行為であると相手国から主張される場合に備える必要」があるとして、「違法性阻却事由の援用」が必要であり、「先行国際違法行為の存在を条件とする対抗措置より重大な危険の存在でも援用可能な緊急避難の方が有用」であるとしている。

他方、差し迫った重大な危険があり、困難であるというように瞬時に攻撃が実施され、攻撃を受けてからの反撃が極めて困難であることは、タリン・マニュアル2.0の規則26にも合致するものである[9]。事実、万が一サイバー攻撃を受けたら、事前に防御ソフトが作動しておらず、ファイアー・ウォールの

[3] 柿沼重志による『能動的サイバー防護の導入―サイバー対処強化法案及び整備法案の概要と主な論点』「立法と調査」平成7年4月、参議院事務局企画調整室。
[4] 持永大『能動的サイバー防御』平成7年2月、日本経済出版社。
[5] UNODC, 'Draft text of the convention (version as of *2 September 2023*).'URL<https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf> accessed 24 September 2025. 以前は途中過程迄公開されていたが、条約文が確定したことも踏まえ、現在は最終版の条約案しか公開されていないが、これを見ても、最終段階でもかなり、纏めるのに苦労したことが伺われる。
[6] Andreas Schloenhardt (ed.) et ali., 'UN Convention against Transnational Organized Crime: A Commentary,' OUP, June 2023: Cecily Rose et ali.' The United Nations Convention Against Corruption: A Commentary (Oxford Commentaries on International Law), OUP, March,2019.
[7] 国家安全保障会議『国家安全保障戦略』平成４年１２月２６日閣議決定
[8]『前掲書』21頁。
[9]『タリン・マニュアル2.0』規則26は、「国は、根本的な利益に対する重大かつ急迫した危険を示す行為に対応して、そ の性質上サイバーであるか否かを問わず、緊急避難を理由として行動することが できる。ただし、そうすることが当該利益を守る唯一の手段である場合に限られる」と規定している。なお、同マニュアルはソフト・ローであるが、同分野での事実上権威ある文書として参照されることが多い。

ような事前にどこかの段階で侵入を止められなければ、マルウエア等のサイバー攻撃が成功すれば、直ちにその効果が表れて、コンピューター・システムはダウンする。なので、システムの回復はおろか、反撃さえも出来ずに、場合によっては攻撃者が突き止められないまま、多大な損害や身代金を要求される事態になり、攻撃を受けてからの反撃等では間に合わないので、兆候が察知された段階で、対処するのは理にかなっている。

（2）対処能力強化法の概要

この法律は幾つかの部分に分けられるが、①法目的の説明、②官民連携の強化、③通信情報の利用、④分析情報・脆弱性情報の提供を内容にしている。以下それぞれの主要項目の概要について説明していくが、これらも強化法本体のみならず、サイバーセキュリティ基本法についての改正が主要部分を占めるもので、強化法による新たな制度とこれまでの基本法からの踏襲と組み合わされていることが特徴的である。

先ず、①法目的の説明については、同法第１条に「（前略）サイバーセキュリティが害された場合に国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機のサイバーセキュリティを確保する重要性が増大していることに鑑み、重要電子計算機に対する特定不正行為による被害の防止のため」に目的規定を置いて、「重要電子計算機に対する不正な行為による被害の防止を図ることを目的とする」ことを明らかにしている。更に衆議院での修正のあった「通信の秘密の自由」についても同法第２条２項に規定した上で、基本方針についても同法第３条に規定している[10]。

第２点目の官民連携の強化については、基幹インフラ事業者によるインシデント報告等（同法第２章）、情報共有のための協議会設置（同法第９章）、電子計算機の使用者に対する情報共有（同法第８章第 41 条）、脆弱性対応の強化等（同法第 8 章第 42 条、サイバーセキュリティ基本法第 7 条）、罰則法の整備（強化法第 12 章）が主要な内容になっている。

第 3 点目の通信情報の利用については、（同意によらない）通信情報の利用（同法第 4 章、第 6 章）[11]、調査すべき情報の選別[12]（同法第 1 章第 2 条第 8 項、第 5 章第 22 条、第 7 章第 35 条）、当事者協定（同意）に基づく通信情報の取得[13]（同法第 3 章）、関係行政機関の分析への協力[14]（同法第 5 章第 27 条）、取得した通信情報の制限（同法第 5 章）、独立機関の設置（同法第 10 章）、罰則の整備（同法第 12 章）がかなり詳細に規定されている。

第 4 点目の分析情報・脆弱性情報の提供について

---

[10] 同法第３条第２項は、同第１項は総理大臣が発議し、閣議決定を求める条件が付されており、概ね以下の内容を想定して、必要に応じて項目の追加も可能である。
①重要電子計算機に対する特定不正行為による被害の防止に関する基本的な事項
②当事者協定の締結に関する基本的な事項
③情報保有機関における通信情報の取扱いに関する基本的な事項
④情報の整理及び分析に関する基本的な事項
⑤総合整理分析情報の提供に関する基本的な事項
⑥協議会の組織に関する基本的な事項

[11] 具体的には、内外通信の分析及び内外通信又は内外通信の分析であり、それぞれ強化法第 4 章及び強化法第 6 章に詳細に規定されており、中立性を保つために設置される独立機関の事前承認を得て実施される。

[12] 人による知識を伴わない自動的な方法により、対象とすべき通信のうち、機械的情報（同法第 2 条 8 項によれば IP アドレス、指令情報等の本質でない情報）であってサイバー攻撃に関係があると認めるに足りる状況があるものを、承認を受ける際に定めた基準に基づき、選別することを指す。

[13] 内閣総理大臣が基幹インフラ事業者その他の電気通信薬務との協定に基づき、当該利用者が送受信する通信情報を受けることを指す（同法第 11 条から 13 条）。

[14] 同法第 27 条第 1 項は「内閣総理大臣は、自動選別又は選別後通信情報の分析（以下この項において「自動選別等という」）を行うために必要があると認める時には、防衛大臣その他の関係行政機関の長（当該行政機関が合議制の機関である場合にあっては、当該行政機関。以下この条において同じ。）に対し、自動選別等に関する専門的知識を有する職員による 自動選別等の実施に用いる電子計算機の貸与その他の必要な協力を要請出来ることが出来る。」と規定している