第3節 サイバー領域をめぐる動向

1 サイバー空間と安全保障

IoTやAI、5G、クラウドサービスなどの利用拡大、テレワークの定着など、情報通信ネットワークは経済社会において、必要不可欠なものになっている。そのため情報通信ネットワークに対するサイバー攻撃は、人々の生活に深刻な影響をもたらしうるものであるとともに、サイバー空間における諜報活動の一環であるサイバー攻撃は国の安全保障にとって現実の脅威となっている。

サイバー攻撃の種類としては、情報通信ネットワークへの不正アクセス、メール送信などを通じたウイルスの送り込みによる機能妨害、情報の改ざん・窃取、大量のデータの同時送信による情報通信ネットワークの機能妨害のほか、電力システムなどの重要インフラのシステムダウンや乗っ取りを目的とした攻撃などがあげられる。また、ネットワーク関連技術は日進月歩であり、AIを利用した攻撃が行われる可能性も指摘されるなどサイバー攻撃も日に日に高度化、巧妙化している。

軍隊にとって情報通信は、指揮中枢から末端部隊に至る指揮統制のための基盤であり、情報通信技術（ICT）の発展によって情報通信ネットワークへの軍隊の依存度が一層増大している。攻撃の実施主体や被害の把握が困難なサイバー攻撃は、敵の軍事活動を低コストで妨害可能な非対称的な攻撃手段として認識されており、多くの外国軍隊がサイバー空間における攻撃能力を開発しているとみられる。

Information and Communications Technology

2 サイバー空間における脅威の動向

諸外国の政府機関や軍隊のみならず民間企業や学術機関などの情報通信ネットワークに対するサイバー攻撃が多発しており、重要技術、機密情報、個人情報などが標的となる事例も確認されている。例えば、高度サイバー攻撃（APT）のような、特定の標的組織を執拗に攻撃するサイバー攻撃は、長期的な活動を行うための潤沢なリソース、体制、能力が必要となることから、組織的活動であるとされている。このような高度なサイバー攻撃に対処するために、脅威認識の共有などを通じて諸外国との技術面・運用面の協力が求められている。また米国は、情報窃取、国民への影響工作、重要インフラを含む産業に損害を与える能力を有する国家やサイバー攻撃主体は増加傾向にあり、特にロシア、中国、イラン及び北朝鮮を最も懸念していると評価[1]しているように、各国が、軍としてもサイバー攻撃能力を強化しているとみられる。

Advanced Persistent Threat

1 中国

中国では、2015年12月末、中国における軍改革の一環として創設された「戦略支援部隊」のもとにサイバー戦部隊が編成されたとみられる。同部隊は17万5,000人規模とされ、このうち、サイバー攻撃部隊は3万人との指摘もある。台湾国防部は、サイバー領域における安全保障上の脅威として、中国は平時では、情報収集・情報窃取によりサイバー攻撃ポイントを把握し、有事では、国家の基幹インフラ及び情報システムの破壊、社会の動揺、秩序の混乱をもたらし、軍や政府の治安能力を破壊すると指摘している[2]。また、中国が2019年7月に発表した国防白書「新時代における中国の国防」において、軍によるサイバー空間における能力構築を加速させるとしているなど、中国は、軍のサイバー戦力を強化していると考えられる。

1 米国防情報長官「世界脅威評価書」（2021年4月）による。
2 台湾国防部「国防報告書」（2021年11月）による。

参照　3章2節2項5（軍事態勢）

中国は、平素から機密情報の窃取を目的としたサイバー攻撃などを行っているとされており[3]、例えば、次の事案への関与が指摘されている。

- 2018年1月及び2月、米海軍の契約業者が中国政府のハッカーによるハッキングを受け、潜水艦搭載の超音速対艦ミサイルに関する極秘情報が流出。
- 2018年12月、米国などは、中国国家安全部と関連するサイバーグループ「APT10」が少なくとも12か国に対して知的財産などを標的とするサイバー攻撃を実施したと発表。
- わが国において、「APT10」による民間企業、学術機関などを対象とした広範な攻撃が確認。
- 2017年、米国の消費者信用情報会社から、名前、生年月日、社会保障番号、運転免許証番号、クレジットカード番号などの個人情報が窃取されるサイバー攻撃が発生。2020年2月、米司法省は、当該サイバー攻撃に関与した疑いで中国軍関係者4名を起訴。
- 2020年7月、新型コロナウイルス感染症のワクチン開発にかかわる企業を含む民間企業などを標的とした知的財産や企業秘密の窃取を目的とするサイバー攻撃を実施したとして、米司法省は中国国家安全部関係者とみられる2名を起訴。
- 2021年7月、米国は、同年3月に発覚したマイクロソフト社メールサーバーソフトの脆弱性を狙ったサイバー攻撃が、中国国家安全部に関連する実施主体によるものであると公表。わが国を含む米国の同盟国なども同日、一斉に中国を非難した。

2　北朝鮮

北朝鮮には、偵察総局、国家保衛省、朝鮮労働党統一戦線部、文化交流局の4つの主要な情報及び対外情報機関が存在しており、情報収集の主たる標的は韓国、米国及びわが国であるとの指摘がある[4]。また、人材育成は当局が行っており[5]、軍の偵察総局を中心に、サイバー部隊を集中的に増強し、約6,800人を運用中と指摘されている[6]。

各種制裁措置が課せられている北朝鮮は、国際的な統制をかいくぐり通貨を獲得するための手段としてサイバー攻撃を利用しているとみられる[7]ほか、軍事機密情報の窃取や他国の重要インフラへの攻撃能力の開発などを行っているとされる。例えば、次のサイバー攻撃への関与が指摘されている。

- 2017年5月、マルウェア「ワナクライ」により、世界150か国以上の病院、学校、企業などが保有する電子情報を暗号化し、使用不能にするサイバー攻撃が発生。わが国や米国、英国、オーストラリア、カナダ、ニュージーランドは、その背後に北朝鮮の関与があったことなどを非難する声明を発表。また、このサイバー攻撃によって14万ドル分のビットコインが集められたとの指摘。
- 2021年2月、米司法省は、北朝鮮軍偵察総局所属の北朝鮮人3名をサイバー攻撃に関与した疑いで起訴。
- 2021年4月に公表された「国連安全保障理事会北朝鮮制裁委員会専門家パネル最終報告書」において、大量破壊兵器や弾道ミサイル計画を支える利益を生み出すために金融機関や仮想通貨取引所に対する攻撃が継続していると評価し、2019から2020年11月までに計3億1,640万ドル相当を窃取したとする分析を公表。
- 2021年5月、韓国原子力研究所は、北朝鮮のサイバーグループがVPNサーバの脆弱性を悪用して内部ネットワークに侵入したと発表。

3　ロシア

ロシアについては、軍参謀本部情報総局（GRU）

3　「米国防省サイバー戦略」（2018年9月）による。
4　米国防情報局「北朝鮮の軍事力」（2021年10月）による
5　韓国国防部「2016国防白書」（2017年1月）による。
6　韓国国防部「2020国防白書」（2020年2月）による。
7　米国防情報局「北朝鮮の軍事力」（2021年10月）による

や連邦保安庁（FSB）、対外情報庁（SVR）がサイバー攻撃に関与しているとの指摘があるほか、軍のサイバー部隊[8]の存在が明らかとなっている。サイバー部隊は、敵の指揮・統制システムへのマルウェア（不正プログラム）の挿入を含む攻撃的なサイバー活動を担うとされ[9]、その要員は、約1,000人と指摘されている。また、2021年7月に公表した「国家安全保障戦略」において、宇宙及び情報空間は、軍事活動の新たな領域として活発に開発されているとの認識を示し、情報空間におけるロシアの主権の強化を国家の優先課題として掲げている。また、2019年11月、サイバー攻撃などの際にグローバルネットワークから遮断し、ロシアのネットワークの継続性を確保することを想定したいわゆるインターネット主権法を施行させた。

米国は、ロシアはスパイ活動、影響力行使、攻撃能力に磨きをかけており、今後もサイバー上の最大の脅威であり続けると認識しており[10]、例えば、次の事案への関与が指摘されている。

- 2017年6月、ウクライナを中心に各国でランサムウェア「NotPetya」によるサイバー攻撃が発生。2018年2月、米英両政府は、ロシア軍によるものと発表。
- 2020年2月、米、英、ジョージア政府などは、2019年10月に発生したジョージア政府機関、報道機関などに対する大規模なサイバー攻撃について、GRUによるものと発表[11]。
- 2020年10月、米司法省は、2015年及び2016年のウクライナ電力網に対するサイバー攻撃や2017年及び2018年の平昌オリンピックに対するサイバー活動などに関与したとしてロシア軍参謀本部情報総局の将校ら6名を起訴したと発表し、英国も米国の発表を支持した。また、英国は2020年に東京オリンピック・パラリンピック関連組織に対してもロシアがサイバー偵察を行ったと発表。
- 2020年12月、米政府機関などが長期にわたるサイバー諜報を受けていたことが判明。本事案に関し、2021年1月、米国政府は、本攻撃の目標を、情報収集を目的とした攻撃と断定、同年4月には、米英政府などが、SVRによるものと発表。
- 2021年4月、米政府は、2020年の大統領選挙に影響を与えるロシア政府主導の試み、その他の偽情報や干渉行為を実行する32の組織・個人を制裁。
- 2021年11月、ウクライナ保安庁は、2014年以降、FSBが関連するサイバーグループが、重要インフラの制御奪取、諜報、影響工作及び情報システムの妨害を企図し、ウクライナの公的機関及び重要インフラに対しサイバー攻撃を実施したと公表。
- 2022年2月、米、英、豪政府は、ウクライナ金融機関に対するサイバー攻撃が、GRUによるものと指摘。

4 その他の脅威の動向

意図的に不正改造されたプログラムが埋め込まれた製品が企業から納入されるなどのサプライチェーンリスクや、産業制御システムへの攻撃を企図した高度なマルウェアの存在も指摘されている。

この点、米国議会は2018年8月、政府機関がファーウェイ社などの中国の大手通信機器メーカーの製品を使用することを禁止する条項を盛り込んだ国防授権法を成立させた。また、中国の通信機器のリスクに関する情報を同盟国に伝え、不使用を呼びかけており、オーストラリアは、第5世代移動通信システムの整備事業へのファーウェイ社とZTE社の参入を禁止しており、英国は2027年末までにすべてのファーウェイ社製品を第5世代移動通信システム網から撤去する方針を表明している。

また、新型コロナウイルスの混乱に乗じ、製薬会

8 2017年2月、ロシアのショイグ国防相の下院の説明会での発言による。ロシア軍に「情報作戦部隊」が存在するとし、欧米との情報戦が起きており「政治宣伝活動に対抗する」としている。ただし、ショイグ国防相は部隊名の言及はしていない。
9 2015年9月、クラッパー米国家情報長官（当時）が下院情報委員会で「世界のサイバー脅威」について行った書面証言による。
10 米国家情報長官「世界脅威評価書」（2021年4月）による。
11 2020年2月、米司法省発表による。

社や研究機関などへのワクチン・治療法研究データの情報窃取、テレワーク基盤への脆弱性を悪用したサイバー攻撃などが頻発している。このような状況に対して、2020年6月にNATOは、医療機関や研究機関などパンデミックの対応に携わる人々に対する悪意あるサイバー活動を非難する声明を発出している。

3 サイバー空間における脅威に対する取組

こうしたサイバー空間における脅威の増大を受け、各国において、各種の取組が進められている。

サイバー空間に関しては、国際法の適用のあり方など、基本的な点についても国際社会の意見の隔たりがあるとされ、例えば、米国や欧州、わが国などが自由なサイバー空間の維持を訴える一方、ロシアや中国、新興国などの多くは、サイバー空間の国家管理の強化を訴えている。また、国際社会においては、サイバー空間における法の支配の促進を目指す動きがあり、例えば、サイバー空間に関する国際会議などの枠組みにおいて、国際的なルール作りなどに関する議論が行われている。

参照　Ⅲ部1章3節2項（サイバー領域での対応）

さらに、2020年からの新型コロナウイルス感染症への対応の結果として、テレワークやICTを活用した教育、Web会議サービスなど世界的に新たな生活様式が確立された。一方で、これらのデジタルサービスの進展に伴い、従来型のサイバーセキュリティ対策の主要な前提となっていた「境界型セキュリティ」[12]の考え方の限界が指摘されており、各国で新たなセキュリティ対策の検討が進められている。

1 米国

米国では、連邦政府のネットワークや重要インフラのサイバー防護に関しては、国土安全保障省が責任を有しており、国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（CISA）が政府機関のネットワーク防御に取り組んでいる。2021年10月には、ブリンケン国務長官が国務省内に国際サイバー安全保障や国際デジタル政策などに取り組む「サイバー空間・デジタル政策局」を新設する考えを表明している。

Cybersecurity Infrastructure Security Agency

米国は、国家安全保障戦略（2017年12月）において、多くの国がサイバー能力を、影響力を行使する手段と捉えており、サイバー攻撃は現代戦の重要な特徴となっているとしたうえで、米国に対してサイバー攻撃を加えてくる相手を抑止、防御し、必要であれば打ち負かすとしている。これを受けて、米国防省は、国家防衛戦略（2018年1月）において、サイバー防衛、抗たん性、運用全体へのサイバー能力の統合に投資していく方針を示している。さらに、米国防省サイバー戦略（2018年9月）においては、米国が中露との長期的な戦略的競争関係にあり、中露はサイバー空間における活動を通じて競争を拡大させ、米国や同盟国、パートナーへの戦略上のリスクになっていると指摘している。

また、連邦政府機関におけるサイバーセキュリティを強化するため、2021年9月に行政管理予算

ブリンケン国務長官の発表【米国務省】

12 境界線で内側と外側を遮断して、外側からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防衛対象の中心はネットワーク。

局及びCISAは、ゼロトラスト[13]に関する文書をパブリックコメントにかけるなど、次世代のセキュリティ環境の検討を進めている。

2019年日米「2＋2」では、サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約にいう武力攻撃に当たり得ることを確認している。

米軍においては、2018年5月に統合軍に格上げされたサイバー軍が、サイバー空間における作戦を統括している。同軍は、国防省の情報環境を運用・防衛する「サイバー防護部隊」(68チーム)、国家レベルの脅威から米国の防衛を支援する「サイバー国家任務部隊」(13チーム) 及び統合軍が行う作戦をサイバー面から支援する「サイバー戦闘任務部隊」(27チーム) (これら三部隊を「サイバー任務部隊」と総称。25の支援チームを含め計133チーム、6,200人規模) などから構成されている。また、サイバー軍は米国と同盟国が悪意のあるサイバー空間の活動に対し、特定、連携、対応する能力の向上を目的として、2021年11月、23か国200人以上のサイバー要員による多国間サイバー演習「サイバー・フラッグ21-1」を実施した。

2 韓国

韓国は、2018年12月、「文在寅政府の国家安保戦略」を発表し、その中で、サイバー空間における脅威に対応する民・官・軍の協力を基盤としてサイバー脅威に対する予防及び対応能力を強化し、国際協力を活性化するとしている。また、国民の安全を守り、国家安全保障を堅固にするため、2019年4月に「国家サイバー安保戦略」を韓国として初めて策定するとともに、同戦略を具体化するため、同年9月には「国家サイバー安保基本計画」を発表した。

国防部門では、韓国軍は、サイバー作戦態勢を強化し、サイバー空間における脅威に効果的に対応するため、2019年に合同参謀本部を中心としたサイバー作戦の遂行体系を構築するとともに、合同参謀本部、サイバー作戦司令部、各軍の連携体制を整備した。同年2月、「国軍サイバー司令部」は「サイバー作戦司令部」に改編された。また、各軍の「サイバー防護センター」は「サイバー作戦センター」に改編され、人員が補強された[14]。

3 オーストラリア

オーストラリアは、2020年8月に発表した「サイバーセキュリティ戦略」では、自国のネットワークの安全性を確保するため、サイバー空間における防御的な能力だけでなく、攻撃的な能力の権限と技術力を確保することを明言している。また、豪英米3国の首脳は、2021年9月に新たな安全保障協力の枠組みとなる「AUKUS」の設立を発表し、原子力潜水艦の共同開発に加え、サイバー能力、人工知能、量子技術などで協力するとしている。

組織面では、政府内のサイバーセキュリティ能力を1カ所に集約した、オーストラリアサイバーセキュリティセンター (ACSC) を設置し、政府機関と重要インフラに関する重大なサイバーセキュリティ事案に対処している。ACSCは2015年7月、初のサイバーセキュリティに関する報告書を公表し、オーストラリアに対するサイバー脅威の数、種類、強度のいずれも増加しているとしている。また、豪軍では、2017年7月に統合能力群内に情報戦能力部を、2018年1月にその隷下に国防通信情報・サイバー・コマンドを設立した。空軍では、職種区分としてネットワーク、データ、情報システムなどを防護するサイバー関連特技を新設し、2019年10月、新設した特技の募集を開始した。

Australian Cyber Security Center

4 欧州

NATOは、2014年9月のNATO首脳会議にお

13 「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方。利用者を疑い、端末等の機器を疑い、許されたアクセス権でも、なりすましなどの可能性が高い場合は動的にアクセス権を停止する。防御対象の中心はデータや機器などの資源。

14 韓国国防部「2020国防白書」(2021年2月) による。

いて、加盟国に対するサイバー攻撃をNATOの集団防衛の対象とみなすことで合意している。

組織面では、2017年11月に、サイバー作戦センターの新設及び加盟国が有するサイバー防衛能力のNATO任務・作戦への統合に関する方針に合意した。ベルギーに置かれた同センターは、2023年には全面稼働し、サイバー攻撃の能力を持つとの見通しが示されている。

また、研究や訓練などを行う機関としては、2008年にNATOサイバー防衛協力センター（CCDCOE）が認可され、エストニアの首都タリンに設置された。同センターは、サイバー活動と国際法の関係に関する研究などを行っており、2017年2月には、「タリンマニュアル2.0」が公表された。本マニュアルは、国家責任法、人権法、航空法、宇宙法、海洋法といった平時に関する法規範から、武力紛争法といった有事に関する法規範に至るまで、幅広い論点について検討が行われており、2020年12月には、同マニュアルを3.0へ更新する取組が開始されている。また、2019年12月、NATOサイバー防衛演習「サイバー・コアリション2019」が開催され、NATO加盟国27か国やEUなどのほか、わが国も初めて正式に参加した。2021年4月には、CCDCOE主催のサイバー防衛演習「ロックド・シールズ2021」にも初めて正式に参加した。

EUは、2020年7月に欧州域内におけるサイバー攻撃を実施した中国籍・ロシア国籍計6名及び中国・北朝鮮・ロシアの3組織に対し制裁を課すことを決定したと発表した。また、同年10月に英国と共同で独連邦議会へのサイバー攻撃を理由にロシアへの制裁発動を発表している。同年12月には、「デジタル10年のためのEUのサイバーセキュリティ戦略」において、EU内のサイバー脅威への集団的な状況認識の欠如を指摘し、民間・外交・警察・防衛各分野横断型の「共同サイバーユニット」の設立など提唱し、2021年6月には同ユニットの具体的構想を発表した。

英国は、同年12月に公表した国家サイバー戦略において、敵対勢力の探知・阻止・抑止など5つの戦略的目標を掲げたほか、今後3年間でサイバー分野に26億ポンドを投資することを表明している。

組織面では、2016年10月に、国のサイバーインシデントに対応し、官民のパートナーシップを推進するため、国家サイバーセキュリティセンター（NCSC）を政府通信本部（GCHQ）に新設した。また、2020年6月に軍のネットワーク防護を担当する「第13通信連隊」を発足した。同年11月には、国家サイバー部隊（NCF）の設立を公表しており、重大犯罪の予防、敵武器システムの妨害などの活動を行うため、GCHQ、国防省などの人員を集約している。

フランスは、2017年5月に統合参謀本部隷下にサイバー防衛軍を発足させている。2021年9月にはパルリ軍事相が、同国に対するサイバー攻撃の増加と深刻さを指摘し、2025年までに同軍の人員を約5,000名規模の人員に増強し、サイバー防衛能力を強化するとしている。