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

インターネットは、様々なサービスやコミュニティが形成され、新たな社会領域（サイバー空間）として重要性を増している。このため、サイバー空間上の情報資産やネットワークを侵害するサイバー攻撃は、社会に深刻な影響を及ぼすことができるため、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、不正アクセス、マルウェア（不正プログラム）による情報流出や機能妨害、情報の改ざん・窃取、大量のデータの同時送信による機能妨害のほか、電力システムや医療システムなど重要インフラのシステムダウンや乗っ取りなどがあげられる。また、サイバー攻撃にAIが利用される可能性も指摘されるなど、攻撃手法は高度化、巧妙化している。

軍隊にとっても情報通信は、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、情報通信ネットワークへの軍隊の依存度が一層増大している。サイバー攻撃は、攻撃主体の特定や被害の把握が容易ではないことから、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攻撃能力を開発しているとみられる。

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。また、高度サイバー攻撃（APT）は、特定の組織を執拗に攻撃するとされ、長期的な活動を行うための潤沢なリソース、体制及び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。

Advanced Persistent Threat

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。こうした中、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が増加傾向にあり、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。

1　中国

中国では、2015年12月末、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。戦略支援部隊は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、中国が平時において、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、軍のサイバー戦能力を強化していると考えられる。

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[3]、近年では、次の事案への関与が指摘されている。

- 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。
- 米セキュリティ企業によれば、中国政府が支援しているとされる「APT41」が2021年～2022年にかけ

1　米国防情報長官「世界脅威評価書」（2022年2月）による。
2　台湾国防部「国防報告書」（2021年11月）による。
3　「米国防省サイバー戦略」（2018年9月）による。

米国州政府のネットワークに侵入したと指摘。

- 2022年6月、米国の国家安全保障局、サイバーセキュリティ・インフラストラクチャセキュリティ庁、連邦捜査局は共同で、2020年以降、中国政府が支援するサイバーアクターがネットワークデバイスの脆弱性を悪用し、様々な官民の組織を標的にしているとして、注意喚起と対応策を発表。
- 2022年7月、ベルギー政府は、内務省、国防省へのサイバー活動について中国政府が支援しているとされる「APT27」、「APT30」、「APT31」などが関与したとし、中国政府を非難。
- 2022年8月、台湾外交部は、米下院議長の訪台にあわせて発生した台湾の政府機関などを標的としたサイバー攻撃について、使用されたIPアドレスが中国やロシアなどのものであったと公表。

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及び文化交流局の4つの主要な情報機関並びに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、人材育成はこれらの機関が行っており[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。2023年4月に発表された「国連安保理北朝鮮制裁委員会専門家パネル2022最終報告書」においては、北朝鮮はサイバー攻撃手法を洗練させており、2022年だけで6億3,000万から10億ドル相当以上の暗号資産を窃取したと指摘されている。近年では、次の事案への関与が指摘されている。

- 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。
- 2022年4月、米財務省は、人気オンラインゲームにおいて発生した6億ドル相当の暗号資産窃盗について、北朝鮮軍偵察総局の関与が指摘されるサイバーアクター「ラザルス」による犯行であった旨を発表。
- 2022年7月、米司法省は、前年5月に北朝鮮のサイバーアクターがランサムウェア「マウイ」を使用し、米カンザス州の医療センターから得ていた身代金を含む約50万ドルを押収した旨を発表。
- 2023年1月、米連邦捜査局は、2022年6月に発生した1億ドル相当の暗号資産窃盗について、「ラザルス」の犯行であり、流出した暗号資産6,000万ドル相当を別の暗号資産に資金洗浄していた旨を発表。

3　ロシア

ロシアについては、軍参謀本部情報総局、連邦保安庁、対外情報庁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、ロシアがスパイ活動、影響力行使及び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いる[10]。近年では、次の事案へ

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「2022国防白書」(2023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。
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」(2022年2月) による。

の関与が指摘されている。

- 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、そのほか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、ロシア連邦保安庁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、ロシア軍参謀本部情報総局によるものと指摘。
- 2022年3月、米連邦捜査局は、米国の重要インフラへのサイバー攻撃について、ロシア連邦保安庁職員3名と国防省傘下の研究所職員1名を起訴した旨を発表。
- 2022年4月、米司法省は、ロシア軍参謀本部情報総局がマルウェアを使用し、指令や遠隔操作を受け入れるようにさせたコンピュータネットワークについて、裁判所が認可した方法でネットワークを無効化した旨を発表。

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。

米国議会は2018年8月、政府機関がファーウェイ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いる。これに対して、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とZTE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、2022年7月、米IT企業は、ランサムウェアの配布などサイバー攻撃に必要なツールの課金形態によるサービスについて、犯罪を助長する様々なオンラインサービスが増加し、その経済圏が継続的に成長していると指摘している。また、同年12月、米保健学術団体は、米国の公衆衛生セクターへのランサムウェアによるサイバー攻撃によって、2016年から2021年までに約4,200万人分の個人情報が流出し、医療提供の妨害などの年間発生件数が2倍以上に増加したと指摘している。

3 サイバー空間における脅威に対する動向

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、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4節5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」[11]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

11 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。防御対象の中心はネットワーク。

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・インフラストラクチャセキュリティ庁（CISA）が政府機関のネットワーク防御に取り組んでいる。2022年4月、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」を新設した。

Cybersecurity and Infrastructure Security Agency

米国は、国防省サイバー戦略（2018年9月）において、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、国家安全保障戦略（2022年10月）において、サイバー攻撃の抑止を目指しサイバー空間における敵対的行動に断固として対応するとし、国家防衛戦略（2022年10月）では、サイバー領域における抗たん性の構築を優先し、直接的な抑止力の手段として攻勢的サイバーをあげている。

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、2022年1月、行政管理予算局は「ゼロトラスト戦略」を発表し、各省庁がゼロトラスト[12]モデルのセキュリティ対策を実施するものとしている。また、2023年3月、国家サイバーセキュリティ戦略を発表し、中国、ロシア、イラン、北朝鮮などがサイバー攻撃を積極的に使用して安全保障と繁栄を脅かしているとし、重要インフラの防衛や脅威アクターの阻止と解体などに注力するとしている。

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）などから構成されている。これら3部隊は「サイバー任務部隊」と総称され、25の支援チームを含め全体として133チーム、6,200人規模である。

また、2022年10月には、サイバー軍主催の多国間サイバー演習「サイバー・フラッグ23-1」が開催され、わが国を含む8か国から250人以上のサイバー要員が参加している。

2　韓国

韓国は、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[13]。

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、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か国の首脳は、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、AI、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。また、2022年11月、サイバー攻撃を未然に阻止するための「常設共同タスクフォース」の新設を発表した。同タスクフォースは通信局及び連邦警察から選抜された

Australian Cyber Security Centre

12 「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、端末などの機器を疑い、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。

13 韓国国防部「2022国防白書」（2023年2月）による。

100名のサイバー要員で構成されるとし、サイバーセキュリティ大臣は攻勢的なサイバー防衛を明言した。

また、軍は、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（DSCC）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。
Defence Signals Intelligence and Cyber Command

4 欧州

NATOは、2014年9月のNATO首脳会議において、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）が認可された。同センターは、2017年2月、サイバー活動に適用される国際法をとりまとめた「タリンマニュアル2.0」を公表し、2020年12月には、同マニュアルを3.0へ更新する取組を開始している。また、2022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2022」、同年11月にはNATO主催のサイバー防衛演習「サイバー・コアリション2022」が開催され、NATO加盟国のほか、わが国も参加している。
Cooperative Cyber Defence Centre of Excellence

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」の設立などを提唱し、2021年6月には同ユニットの具体的構想を発表した。また、2022年11月、EUの市民とインフラの保護能力強化などのための「EUサイバー防衛政策」を発表している。

NATO主催のサイバー防衛演習「サイバー・コアリション2022」の様子【NATO HP】

英国は、2021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。
National Cyber Security Centre
Government Communications Headquarters
National Cyber Force

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（当時）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。