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、AIを利用したサイバー攻撃の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、サイバー空間は、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、サイバー空間への依存度が増大している。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できる非対称な攻撃手段として認識されており、多くの国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っている。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、体制や能力が必要となることから、組織的活動であるとされる。

Advanced Persistent Threat

このよう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。こうしたなか、米国は、攻撃主体が悪意のあるサイバー活動によって非対称な優位性を獲得し、重要インフラを標的にすることで、米国の軍事的優位性を低下させていると評価しており、特に、中国、ロシア、北朝鮮、イランをあげている[1]。

1 中国

中国では、これまで、サイバー戦部隊は戦略支援部隊のもとに編成されていたとみられてきたが、この戦略支援部隊は、2024年に信息（情報）支援部隊などに再編された可能性が指摘されている。なお、2024年以前の戦略支援部隊は17万5,000人規模とされており、このうち、サイバー攻撃部隊は3万人との指摘もあった。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や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、サイバー空間において、日常的に技術窃取や国外の敵対者の監視活動を実施しているとされ[3]、2023年には、次の事案への関与が指摘されている。

- 2023年4月、米司法省は、米居住の中国反体制派のオンライン会議において、反体制派の発信をメッセージの大量送信により妨害したとして、中国政府職員を起訴。
- 2023年5月、米国と英国などは、中国政府が支援するサイバーアクター「Volt Typhoon」が米国の重要

1 米国防省「サイバー戦略2023」（2023年）による。
2 台湾国防部「国防報告書」（2021年）による。
3 米国防省「サイバー戦略2023」（2023年）による。

インフラに侵入していたと公表。痕跡が残らないように、侵入先の環境にあるネットワークツールを使用して検知を回避していたと指摘。

- 2023年7月、米IT企業は、中国を拠点とするサイバーアクター「Storm-0558」が米国務省、商務省などの電子メールアカウントをハッキングしていたと公表。
- 2023年8月、米IT企業は、中国を拠点とするサイバーアクター「Flux Typhoon」が台湾の政府機関などに侵入し、長期的なアクセスを確立・維持していたと公表。
- 2023年9月、警察庁・内閣サイバーセキュリティセンターなどは、中国を背景とするサイバーアクター「BlackTech」がわが国を含む東アジアと米国の政府、産業、技術分野などの情報窃取を目的としたサイバー攻撃をしたとして注意喚起。

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つの主要な情報機関と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、米国と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。2024年に発表された「国連安保理北朝鮮制裁委員会専門家パネル2023年最終報告書」においては、2017年から2023年までの北朝鮮の関与が疑われる暗号資産関連企業に対する58件のサイバー攻撃の被害が約30億ドルにのぼるほか、北朝鮮は外貨収入の約5割をサイバー攻撃により獲得し大量破壊兵器計画に使用していると報告されている。2023年には、次の事案への関与が指摘されている。

- 2023年4月、米司法省は、サイバー攻撃によって得た暗号資産を資金洗浄したなどとして北朝鮮の朝鮮貿易銀行の幹部を起訴。
- 2023年6月、韓国と米国は、北朝鮮のサイバーアクター「キムスキー」がソーシャルエンジニアリングを利用した不正アクセスによって外交情報を収集していたとして注意喚起。
- 2023年7月、米セキュリティ企業は、北朝鮮偵察総局傘下とみられるサイバーアクターが米ソフトウェア事業者のシステムに侵入し、この事業者の顧客に対して悪意のあるスクリプトを実行したと発表。
- 2023年8月、米連邦捜査局は、北朝鮮のサイバーアクターが6月に複数事業者から数億ドル相当の暗号資産を窃取していたとして注意喚起。
- 2023年10月、韓国国家情報院は、8月と9月に北朝鮮のハッカーが韓国国内の造船企業やその従業員に対して、技術情報窃取とみられるサイバー攻撃の試みを検知したとして注意喚起。

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年に公表した国家安全保障戦略において、宇宙・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。なお、2019年には、サイバー攻撃などの際にグローバルネットワークから自国のネットワークを遮断し、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

4　米国防情報局「北朝鮮の軍事力」(2021年) による。
5　韓国国防部「2016国防白書」(2017年) による。
6　韓国国防部「2022国防白書」(2023年) による。
7　米国防情報局「北朝鮮の軍事力」(2021年) 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。

ターネット主権法を施行している。

ロシアは、スパイ活動、影響力行使、攻撃に関する能力を向上させているとされ[10]、2023年には、次の事案への関与が指摘されている。

- 2023年4月、ポーランドは、ロシア連邦保安庁に関連するサイバーアクターがEU諸国の省庁などを標的とする広範な諜報活動を観測したとして注意喚起。大使館を装い、マルウェアを挿入させるリンク付き電子メールを送信していたと指摘。
- 2023年5月、米国と英国などは、ロシア連邦保安庁がマルウェア「Snake」を使用し、50か国以上で20年近く諜報活動をしていたと発表。マルウェアに感染したコンピュータは、暗号化したネットワークを構築し、偽装した通信を中継していたと指摘。
- 2023年6月、ウクライナは、ロシアのサイバーアクター「APT28」がウクライナの省庁などに対して、ウェブメールの脆弱性を悪用した諜報活動をしていたとして注意喚起。
- 2023年8月、ウクライナ、英国、米国は、ロシア軍参謀本部情報総局がウクライナ軍の使用する端末に対して新しいマルウェア「Infamous Chisel」を展開しようとしていたとして注意喚起。
- 2023年12月、英国と米国などは、ロシア連邦保安庁傘下のサイバーアクター「Star Blizzard」が英国やその他の地域の組織や個人を標的とするスピアフィッシング攻撃をしていたとしてロシアを非難。

4　その他の脅威の動向

近年では、日常的に使用する製品の脆弱性やセキュリティが緩い取引先などを介したサプライチェーン攻撃や、重要インフラなどの産業制御システムへのサイバー攻撃も注目されている。

サプライチェーン攻撃は、製品の部品調達から販売に至る供給過程において、信頼している組織やソフトウェアを侵害して標的となる組織に侵入するため、従来セキュリティの回避が懸念されている。2023年に、米国と英国などは、ランサムウェア攻撃を仕掛けるアクター「cl0p」が政府機関の使用するソフトウェアの脆弱性を利用して政府ネットワーク内に侵入していたとして注意喚起している。

産業制御システムへのサイバー攻撃は、これまでは独自仕様やクローズドなシステムであったものが、ITの利用によりオープンなシステムに移行することで、攻撃の標的になりやすくなっていることから、重要インフラなどへのサイバー攻撃が懸念されている。2022年に欧州のセキュリティ企業は、ウクライナ送変電施設へのロシアのサイバー攻撃において、ITネットワークよりも内側にある産業制御システムに侵入し、破壊的なマルウェアを展開しようとしていたと指摘している。

また、宇宙システムについても、2022年に衛星通信事業者に対するロシアのサイバー攻撃によって衛星通信サービスが中断している。このため、各国は衛星通信に関する新たなアドバイザリやガイドラインなどによりセキュリティ対策を強化するほか、欧米では、宇宙システムの脆弱性を明確にする侵入試験やハッキング競技会なども実施されている。

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、各国で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。国連では、2021年から2025年にかけ、サイバー空間における脅威認識、規範、国際法の適用など幅広い議論をするオープン・エンド作業部会が開催されている。

参照　Ⅲ部1章4節5項（サイバー領域での対応）

10　米国防省「サイバー戦略2023」（2023年）による。

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。
Cybersecurity and Infrastructure Security Agency

戦略面では、国家サイバーセキュリティ戦略を発表し、重要インフラの防御や脅威アクターの阻止・解体などに注力するとしている。また、連邦政府機関のサイバーセキュリティを強化するための「ゼロトラスト[11]戦略」を発表し、各省庁に対してゼロトラストモデルのセキュリティ対策を求めている。さらに、不足するサイバー人材を確保するため国家サイバー人材・教育戦略を発表し、国民の基本的サイバースキルの習得やサイバー教育の変革などに長期的に対処するとしている。

安全保障に関しては、国家安全保障戦略において、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防御をあげている。また、国防省のサイバー戦略2023では、攻撃者の組織・能力・意図を追跡し、悪意のあるサイバー活動を妨害・劣化させて防御するほか、統合軍のサイバー領域での作戦を支援し、同盟国や関係国と協力して防御するとしている。

なお、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うることを確認している。

米軍は、2018年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。米サイバー軍は、国防省の情報ネットワークの防護、敵のサイバー活動監視や攻撃防御、統合軍の作戦支援などのチームから構成されており、6,200人規模である。また、米軍は、ラトビアやリトアニアなどのパートナー国において、重要なネットワーク上の悪意のあるサイバー活動に対して、防御し妨害する作戦を実施している。

2　韓国

韓国は、2024年、北朝鮮などによるサイバー脅威や高度化するサイバー環境に対応するため、攻勢的サイバー防御や抗たん性確保などを目標とする新しい「国家サイバー安保戦略」を発表している。

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。2023年には、米韓サイバー安全保障協力を強化するため、米韓高官級協議体「高位運営グループ」が発足している。

3　オーストラリア

オーストラリアは、2022年に発表した国防サイバーセキュリティ戦略において、サイバー脅威環境に適応した任務重視かつ最新のサイバーセキュリティをベストプラクティスとパートナーシップによって実現するとし、運用モデル実装や能力取得など行動目標を定めている。また、2023年に公表した「2023年から2030年までのサイバーセキュリティ戦略」において、2030年までにサイバーセキュリティの世界的なリーダーになるためのロードマップを定めている。

2023年に公表した国防戦略見直しでは、ドメイン統合作戦を支援するサイバー能力を広範に強化すべきとしており、2024年に公表した国家防衛戦略および統合投資プログラムにおいて、2034年までの10年間にわたり、サイバー能力を含む防衛能力を向上させることとしている。

組織面では、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、サイバー攻撃を未然に阻止するため、通信局と連邦警察から選抜された100名のサイバー要員で構成される常設共同タスクフォースの新設を発表し、サイバーセキュリティ大臣は攻勢的なサイバー防御を明言した。
Australian Cyber Security Centre

11 「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。

豪軍は、2017年に統合能力群内に情報戦能力部を、2018年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年に新設した特技の募集を開始した。
Defence Signals Intelligence and Cyber Command

4　欧州

EUは、2020年に「デジタル10年のためのEUのサイバーセキュリティ戦略」を発表し、強靱なインフラと重要サービスのための規則改正や、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目標としている。加えて、EUの市民とインフラの保護能力強化などのため、2022年にEUサイバー防衛政策を発表している。

また、域内のサイバー協力のため、サイバー防御活動の共通フレームワークを加盟国軍のサイバー事案対処チームでの利用を進めるほか、加盟国相互のサイバーセキュリティ支援などに取り組んでいる。2023年には、サイバー関連の危機対応のため、加盟国間の情報共有と状況認識を強化する運用者レベルでの演習を実施している。

NATOは、2014年の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。また、2023年のNATO首脳会議では、サイバー防衛分野の政治、軍事、技術を統合して平時・危機・有事を通して軍民協力を確保し、重要インフラを含む国家サイバー防衛をさらに強化するとしている。

NATO主催のサイバー演習「サイバー・コアリション2023」の様子【NATO HP】

組織面では、NATOサイバーセキュリティセンターがNATO自身のネットワークを保護するほか、サイバー領域作戦センターがサイバー領域における作戦行動の調整、行動自由の確保、脅威への回復力を提供している。2023年には、悪意のある重大なサイバー活動に対する支援として仮想サイバー事案支援能力（VCISC）を立上げている。
Virtual Cyber Incident Support Capability

また、研究や訓練などを行う機関としてNATOサイバー防衛協力センター（CCDCOE）が2008年に認可された。CCDCOEは、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2017年に公表しており、このマニュアルを3.0へ更新する取組が進められている。また、2023年、CCDCOE主催「ロックド・シールズ」や、NATO主催「サイバー・コアリション」のサイバー防衛演習が開催され、NATO加盟国のほか、わが国も参加している。
Cooperative Cyber Defence Centre of Excellence

英国は、2021年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・抑止などの戦略的目標を掲げている。また、2023年に公表した「国家サイバー部隊：責任あるサイバー戦力の実践」では、テロ活動の妨害、APT脅威への対抗、選挙干渉の軽減などを実施し、今後、国家サイバー部隊の規模・能力・機能統合を追求するとしている。

組織面では、2016年に、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を政府通信本部に新設した。また、2020年に軍のネットワーク防護を担当する第13通信連隊を発足させたほか、国家サイバー部隊を設立している。

フランスは、2015年に発表した国家デジタルセキュリティ戦略において、サイバー空間の基本的利益を保護し、サイバー犯罪への対応を強化するなどとしている。また、2018年の「サイバー防御の戦略見直し」では、サイバー危機管理プロセスを明確化している。

組織面では、2017年に統合参謀本部隷下にサイバー防衛軍を発足させており、2025年までに約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。また、2023年に成立した「2024から2030年の軍事計画法」では、サイバー任務のための戦術・手法・手順を構築するセンター・オブ・エクセレンス（研究拠点）の創設を目指すとしている。