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

サイバー空間はインターネットをはじめとし、様々なサービスやコミュニティが形成された、新たな社会領域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、安全保障上の現実の脅威となっている。

またサイバー攻撃とは、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（DDoS攻撃）のほか、ランサムウェアによる電力システムや医療システムなど重要インフラに対するシステム障害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構築・強化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、洗練された手法で特定の組織を執拗に攻撃するサイバー攻撃とされ、こうした攻撃には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。こうしたなか、英国は、「現実的かつ継続的な脅威」として、中国、ロシア、北朝鮮、イランによるサイバー攻撃をあげている[1]。

1 中国

中国では、これまで、サイバー戦の任務を担う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年に廃止され、その隷下であったサイバー空間部隊が兵種に格上げされたとの指摘がある。台湾は中国のサイバー攻撃の手法について、サイバー部隊が段階的、継続的な基幹インフラのネットワークへの侵入を試みていること[2]、また、有事において、中国軍は台湾に対する作戦を支援するためサイバー攻撃を行い、台湾の基幹インフラを破壊し軍事装備システムの運用に影響を与える能力を有していることを指摘している[3]。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[4]、近年では、次の事案への関与が指摘されている。

- 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既存のツールを使用して検知を回避していたと指摘。
- 2024年2月、米国と英国などは、「Volt Typhoon」が、米国との重大な危機や紛争が発生した際に米国の重要インフラに対する破壊的なサイバー攻撃を行うためにITネットワーク上で準備活動を行っていたとし

1 英国国家サイバーセキュリティセンター「年次レビュー2024」（2024年）による。
2 台湾国家安全局「2024年中国共産党ハッキング手法分析」による。
3 台湾国防部「国防報告書」（2023年）による。
4 米国防情報局「北朝鮮の軍事力」（2021年）による。

て注意喚起。

- 2024年3月、米司法省は、中国国家安全部が運営しているとされるハッキンググループ「APT31」の一員が中国体制の批判を行う政治家や評論家などに対して不正なコンピュータ侵入や通信詐欺を繰り返していたとして、7人を起訴。
- 2024年11月、米連邦捜査局（FBI）と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）は共同声明で、中国関連の攻撃者が米国の複数の通信インフラに対する攻撃を行い、米国政府や政治活動に関与している個人の通話データを窃取したと発表。
- 2025年1月、米財務省は、中国を背景とするサイバーグループ「Salt Typhoon」が、米国の複数の主要な通信会社やインターネットサービスプロバイダのネットワークインフラに不正侵入したと指摘。
- 2025年1月わが国警察庁および内閣サイバーセキュリティセンターは、中国のAPTグループ「MirrorFace」が国内の組織、個人などに対するサイバー攻撃を行ったことを公表。

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、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[5]。また、人材育成はこれらの機関が行っており、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。2024年には、主に、次の事案への関与が指摘されている。

- 2024年3月、韓国国家情報院は、韓国国内の半導体関連企業が北朝鮮のハッカーによるサイバー攻撃を受け、設計図などを窃取されたことを公表。
- 2024年4月、韓国警察庁は、北朝鮮のサイバーアクター「ラザルス」、「アンダリエル」および「キムスキー」が韓国の防衛産業企業約10社に対し、技術データを窃取するため、少なくとも1年半以上にわたってサイバー攻撃を行っていたことを公表。
- 2024年12月、米FBI、米国防省サイバー犯罪センターおよびわが国警察庁は、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が、わが国の暗号資産関連事業者「株式会社DMM Bitcoin」から約482億円相当の暗号資産を窃取したことを特定し、合同で公表。
- 2025年1月わが国警察庁および内閣サイバーセキュリティセンターは、中国のAPTグループ「MirrorFace」が国内の組織、個人などに対するサイバー攻撃を行ったことを公表。

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]とされ、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。

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（当時）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（当時）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。

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]、2024年には、次の事案への関与が指摘されている。

- 2024年3月、米IT企業は、ロシアを背景とするサイバーアクター「Midnight Blizzard」が、同社のソースコードを窃取し、内部システムへの不正なアクセスを行っていたことを公表[11]。
- 2024年5月、ポーランドは、ロシア軍参謀本部情報局との関連が指摘されているサイバーアクター「APT28」が、複数のポーランド政府機関に対してマルウェアをダウンロードするように仕向けたフィッシングメールを送信していたと指摘。
- 2024年9月、米FBI、CISA、国家安全保障局（NSA）（National Security Agency）は、ロシア軍参謀本部情報総局29155部隊とのつながりがあるサイバーアクターが、スパイ活動、破壊工作、風評被害を与えることを目的として、世界の標的に対してコンピュータ・ネットワーク上で活動を行っているとして注意喚起。
- 2024年10月、ウクライナコンピュータ緊急対応チーム（CERT-UA）は、悪意のある電子メールが政府機関、企業および軍事機関の間で大量に配布されており、また、この攻撃はロシア政府が支援するサイバーアクター「APT29」によって行われているものである可能性があると発表。

4　その他の脅威の動向

近年では、供給過程で意図的に不正改造された部品やソフトウェアが組み込まれる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、生成AIを利用したサイバー脅威の増大が注目されている。

サプライチェーン攻撃については、2024年3月、米CISAなどは、データ圧縮ソフトウェア「XZ Utils」のバージョン5.6.0と5.6.1に不正アクセスを可能にする悪意のあるコードが埋め込まれていたとして注意喚起を行っている。産業制御システムへのサイバー攻撃については、2024年3月、米環境保護局とNSAは、イラン革命ガードとの関連が指摘されるハッカー集団や「Volt Typhoon」が米国の飲料水システムを含む重要インフラに対して悪意のある攻撃を行ったとして注意喚起している。

生成AIツールは、技術力の低い脅威アクターでも迅速に悪意のあるプログラムを作成することを可能にするため、サイバー攻撃への応用が懸念されている。検出されたビジネスメール詐欺メッセージの40％がAIによって生成されたものであるとの指摘もある[12]。

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1節1項5（サイバー領域における対応）、Ⅲ部1章2節4項2（サイバー領域）

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、CISAが政府機関のネットワーク防御に取り組んでいる。また、重要インフラなどに関する機微な情報の流出への対策として、2023年9月には、中国やロシアとのつながりが認められる企業によって設計、開発、

10　米国防省「サイバー戦略2023」（2023年）による。
11　2024年3月8日のマイクロソフト社の発表による。
12　2024年7月31日のVIPRE社の発表による。

製造および販売されたコネクテッドカー[13]の輸入を禁止する新たな規則案が示されている。

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[14]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2月、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。2024年9月には、下位文書として「国家サイバー安全保障基本計画」が策定され、目標の達成に向けた具体的な方針が示された。

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。また、2024年8月の乙支（ウルチ）演習の際には、サイバーレジリエンス[15]の確保を目的として、官・軍・民による初の実動型統合訓練が実施された。

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を重視し、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。

2024年11月には国内初となるサイバーセキュリティ法案、ランサムウェア報告やスマートデバイスのセキュリティ基準の成文化、重大なサイバーインシデント管理のための枠組みの導入を目指している。

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）（Australian Cyber Security Centre）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、2023年には、豪内務省傘下に、サイバー政策

13　ICT端末としての機能を有する自動車のことをさす。車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することができる。米国政府によれば、コネクテッドカーは、車両の安全性の促進や運転手のナビゲーション支援といった利点を持つ一方で、収集された地理情報や重要インフラに関する機微な情報の悪用や自動車の運用の妨害といったリスクも有している。

14　「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。

15　サイバー攻撃時によって指揮統制システムや情報通信ネットワークの一部が損なわれた場合においても、柔軟に対応して運用可能な状態に回復する能力。

の総合調整などを担う国家サイバー局（NOCS）を設置している。
National Office for Cyber Security

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。2024年には、消費者や企業の保護を目的としてサイバーレジリエンス法が施行され、他のデバイスやネットワークに直接または間接的に接続されるすべての製品に、サイバーセキュリティ要件が課されるようになった。

NATOは、2014年のNATO首脳会合において、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、2024年のNATO首脳会合では、統合サイバー防衛センターを新たに設置することが合意された。これは、既存の各種サイバー関連機能の統合を試みるものであり、これによってサイバー空間における状況把握、抗たん性、集団防衛を強化するとしている。

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、2024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

NATO主催のサイバー演習「サイバー・コアリション2024」の様子
【NATO HP】

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。

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。