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

近年の情報通信技術（ICT）の発展により、インターネットなどの情報通信ネットワーク（Information and Communications Technology）は人々の生活のあらゆる側面において必要不可欠なものになっており、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。

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、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、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。また、軍隊は任務遂行上、電力をはじめとする様々な重要インフラを必要とする場合があり、これらの重要インフラに対するサイバー攻撃が、任務の大きな妨害要因になり得る。そのため、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。特に、中国及びロシアは、ネットワーク化された部隊の妨害やインフラの破壊などのために、軍のサイバー攻撃能力を強化していると指摘されている[1]。

2 サイバー空間における脅威の動向

このような状況のもと、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）（Advanced Persistent Threat）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、中国、ロシア、イラン、北朝鮮が、より多様な手段で、より積極的にサイバー攻撃を実施するようになっていると評価[2]しており、各国は、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。

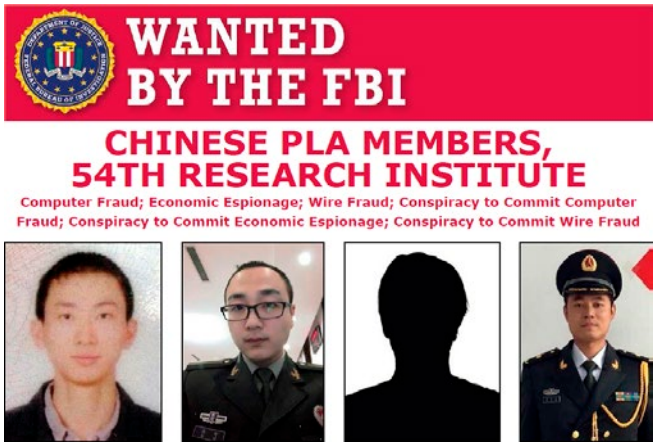
1 中国

中国では、15（平成27）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。また、中国は、16（平成28）年に公表された「国家サイバー空間安全戦略」において、サイバー空間を国家主権の重要部分であるとの認識を示している。さらに、19（令和元）年7月に発表された国防白書「新時代における中国の国防」では、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。

参照　I部2章2節5項（軍事態勢）

中国は、平素から機密情報の窃取を目的とした

1　米国家情報長官「世界脅威評価書」（18（平成30）年3月）による。
2　米国防情報長官「世界脅威評価書」（19（平成31）年1月）による。



米消費者信用情報会社に対する17（平成29）年のサイバー攻撃に関与した疑いで起訴された4名【FBI】

サイバー攻撃などを行っているとされており[3]、例えば、以下の事案への関与が指摘されている。

- 15（平成27）年6月、米国連邦人事管理局がサイバー攻撃を受け、同国の連邦職員や軍人などおよそ2,200万人分の個人情報が窃取されていたことが判明[4]
- 18（平成30）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
- 18（平成30）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
- 17（平成29）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。20（令和2）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

2 ロシア

ロシアについては、軍参謀本部情報総局（GRU）や連邦保安庁（FSB）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[5]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[6]、その要員は、約1,000人と指摘されている。16（平成28）年12月に公表された「情報安全保障ドクトリン」では、軍事・政治目的での情報技術の使用に関連した脅威が増大しているとの認識を示しており、19（令和元）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。

ロシアは、サイバーを用いた情報作戦により、情報窃取や破壊工作に加えて、民主主義プロセスに挑戦していると指摘されており[7]、例えば、以下の事案への関与が指摘されている。

- 14（平成26）年、米大手インターネット企業から5億件以上の個人情報が流出。17（平成29）年3月、米国政府は、サイバー攻撃を実施したとして、ロシア連邦保安庁（FSB）の要員2名を含む4名のハッカーを起訴[8]
- 15（平成27）年12月、ウクライナで大規模

Federal Security Service

解説 マルウェアとは

Malicious Software（悪意のあるソフトウェア）の略称であり、さまざまな脆弱性などを利用して攻撃を行うソフトウェアの総称

3 「米国防省サイバー戦略」（18（平成30）年9月）による。
4 米中経済安全保障再検討委員会の年次報告書（15（平成27）年11月）による。
5 17(平成29)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。
6 15（平成27）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。
7 18（平成30）年9月公表の「米国防省サイバー戦略」による。
8 17（平成29）年3月、米司法省発表による。

な停電を発生させたサイバー攻撃が発生。クリミア併合などで対立するロシア軍関与の疑いがあると報じられた

- 16（平成28）年の米大統領選挙の影響工作のためのサイバー攻撃[9]
- 17（平成29）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。18（平成30）年2月、米英両政府は、ロシア軍によるものと発表
- 18（平成30）年10月、米英両政府は、世界アンチ・ドーピング機関、化学兵器禁止機関、米国民主党全国大会などに対する一連のサイバー攻撃事案についてロシア軍参謀本部情報総局によるものと発表
- 20（令和2）年2月、米、英、ジョージア政府などは、19（令和元）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、ロシア軍参謀本部情報総局（GRU）によるものと発表[10]

3 北朝鮮

北朝鮮については、当局で人材育成を行っており[11]、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[12]。19（令和元）年9月には、米国財務省が重要インフラを対象とした悪意あるサイバー活動に関与したとして、北朝鮮当局が支援するサイバー集団3団体[13]を制裁対象に指定する旨を発表した。

北朝鮮は、サイバー攻撃を用いた金銭窃取のほか、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を行っているとみられている。例えば、以下のサイバー攻撃への関与が指摘されている。

- 16（平成28）年9月、韓国軍内部ネットワークへのサイバー攻撃が発生。17（平成29）年5月、韓国国防部は、北朝鮮ハッカー組織と推定される勢力によるものとの結論を下したと報じられた[12]。また、このサイバー攻撃により、韓国の軍事機密文書が流出したと指摘されている
- 17（平成29）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、豪州、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がある
- 17（平成29）年9月、複数の米国電力会社にスピアフィッシング・メールによるサイバー攻撃が発生。同年10月に、米国情報セキュリティ企業「ファイアアイ」は、北朝鮮との関連が濃厚とされるサイバー脅威グループによって行われたと公表
- 20（令和2）年4月、国連安保理北朝鮮制裁委員会の専門家パネルが公表した最終報告書によると、パネルは、加盟国による情報及び公開情報を踏まえ、北朝鮮が金融機関や暗号通貨取引所へのサイバー攻撃を継続していると結論付け、また、攻撃は巧妙さを増していると評価している。

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18（平成30）年8月、政府機関がファーウェイ（華為）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権限法を成立させた。また、中国の通信機器のリスクに関する情報を同盟

9 16（平成28）年10月の米国土安全保障省と米国家情報長官による共同声明、同年12月のロシアによる米国へのサイバー攻撃に関する米国土安全保障省及びFBIの共同報告書及び17（平成29）年1月の米大統領選に対するロシアのサイバー攻撃に関する米情報コミュニティの報告書による。
10 20（令和2）年2月、米司法省発表による。
11 17（平成29）年1月発刊の韓国の「2016国防白書」による。
12 19（平成31）年1月発刊の韓国の「2018国防白書」による。
13 「ラザルスグループ（Lazarus Group）」、「ブルーノロフ（Bluenoroff）」、「アンダリエル（Andariel）」として民間サイバーセキュリティ業界で知られる北朝鮮のAPT攻撃実施主体

国に伝え、不使用を呼びかけており、オーストラリアは、次世代通信規格「5G」の整備事業へのファーウェイとZTEの参入を禁止した。

政府や軍隊の情報通信ネットワーク及び重要インフラに対するサイバー攻撃は、国家の安全保障に重大な影響を及ぼし得るものであり、また、近年、国家が関与するサイバー攻撃が増加しているとみられることから、サイバー空間における脅威の動向を引き続き注視していく必要がある。

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）

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（Cybersecurity Infrastructure Security Agency/CISA）が政府機関のネットワーク防御に取り組んでいる。

米国は、国家安全保障戦略（17（平成29）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。また、米国防省は、国家防衛戦略（18（平成30）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（18（平成30）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たうえで、①サイバー軍の能力構築の加速、②悪意あるサイバー活動への対抗・抑止のための防衛、③同盟国及びパートナー国との協力促進といったアプローチが示されている。

19（平成31）年4月には、日米安全協議委員会（日米「2＋2」）が開催され、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、18（平成30）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。

2 NATO

11（平成23）年6月に採択されたサイバー防衛に関する北大西洋条約機構（NATO）の新政策及び行動計画は、①サイバー攻撃に対するNATOの政治上及び運用上の対応メカニズムを明確化し、②NATOが、加盟国によるサイバー防衛構築の支援や、加盟国がサイバー攻撃を受けた場合

North Atlantic Treaty Organization

の支援を実施することを明確にし、③パートナー国などと協力していくとの原則を定めている。また、14（平成26）年9月、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、17（平成29）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、23（令和5）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、NATOは08（平成20）年以降、NATOサイバー防衛能力を高めるためのサイバー防衛演習を毎年行っているほか、EUとの間でもサイバー安保・防衛分野での連携を進展させている。

研究や訓練などを行う機関としては、08（平成20）年、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、「タリンマニュアル」を作成するなどの活動を行っている。17（平成29）年2月、同マニュアルの続編となる「タリンマニュアル2.0」が公表され、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いる。また、19（令和元）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。

Cooperative Cyber Defence Centre of Excellence

3 英国

英国は、15（平成27）年11月の「NSS・SDSR2015」において、今後5年間で約19億ポンドをサイバー防衛能力向上のために投資し、サイバー空間における脅威を特定・分析する機能を強化していくことを明らかにした。16（平成28）年11月には、新たな「サイバーセキュリティ戦略」を公表し、英国がサイバーの脅威に対し安全かつデジタルの世界において繁栄するためのビジョンを提示した。このビジョンを達成するため、サイバー脅威に対し効果的に「防護」する手段及び攻撃的手段の保持による「抑止」、最先端技術の「開発」が必要としている。

National Security Strategy and Strategic Defence and Security Review 2015

組織面では、16（平成28）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。

National Cyber Security Centre　Government Communications Headquarters

4 オーストラリア

オーストラリアは、13（平成25）年1月の「国家安全保障戦略」において、サイバー政策及び作戦の統合が国家安全保障上の最優先課題の一つであるとした。16（平成28）年4月には、20（令和2）年までの新たな「サイバーセキュリティ戦略」を発表し、国民の安全の確保、民間企業によるサイバーセキュリティへの参画、脅威情報に関する情報共有などについて規定した。

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15（平成27）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、17（平成29）年7月に統合能力群内に情報戦能力部を、18（平成30）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、19（令和元）年10月、新設した特技の募集を開始した。

Australian Cyber Security Center

5 韓国

韓国は、18（平成30）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、19（平成31）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、国防部にサイバー対策技術チームを創設し、サイバー・ハッキング脅威に対応するとしているほか、「国防サイバー安保戦略書」や「国防サイバー危機対応実務マニュアル」に基づき、サイバー危機への迅速な対応手順を定めている。合同参謀本部においては、15（平成27）年にサイバー作戦総括部署を新設し、合同参謀本部議長にサイバー作戦に関する統制権限を付与して、「合同サイバー作戦」教範を発刊するなど、合同参謀本部を中心にサイバー作戦遂行体系を一元化している。