第5節 サイバー空間をめぐる動向

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いる。一方、重要インフラの情報通信ネットワークに対するサイバー攻撃[1]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やメール送信などを通じたウィルスの送り込みによる機能妨害や情報の改ざん・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阻害などがあげられるが、インターネット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、複雑化している。サイバー攻撃の特徴としては、次のようなものがあげられる[2]。

① 多様性：実行者、手法、目的、状況などが多様
② 匿名性：実行者の隠蔽（いんぺい）・偽装が容易
③ 隠密性：攻撃の存在を察知し難いものや、被害発生の認識すら困難なもの
④ 攻撃側の優位性：手法によっては攻撃手段の入手が容易であることや、ソフトウェアのぜい弱性を完全に排除することが困難であることなど
⑤ 抑止の困難性：報復攻撃や防御側の対策による抑止効果が小さいことなど

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社会インフラに依存しており、当該社会インフラに対するサイバー攻撃が、任務の大きな阻害要因になり得る。そのため、サイバー攻撃は敵の軍隊の弱点につけこんで、敵の強みを低減できる非対称的な戦略として位置づけられつつあり、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されている。また、情報収集目的のために他国の情報通信ネットワークへの侵入が行われているとの指摘がある。

こうしたことから、今やサイバーセキュリティは、各国にとっての安全保障上の重要な課題の一つとなっている。

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いる[3]。

これらの一部については、中国の人民解放軍、情報機関、治安機関、民間ハッカー集団や企業など様々な組織の関与が指摘されている[4]。中国はサイバー空間に強い関心を有しているとみられ[5]、軍がサイバー部隊を編成し、訓練を行っていると

1 サイバー攻撃の標的には、大きくは国家間などの地球規模、国や政府機関などの国家規模、地域社会などの社会規模、経済界やインフラなどの地区規模、企業やグループなどの企業規模から、最小の個人規模まで様々なものがある。そのためサイバー攻撃への対策は、それぞれの規模に対して最適な対策が必要であると言われている。
2 12（平成24）年9月、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」
3 米議会下院国土安全保障委員会議長の発表（14（平成26）年11月）によると、米国コンピューター緊急対処チーム（US-CERT：The United States Computer Emergency Readiness Team）は、13（同25）年の米国政府に対するサイバー攻撃件数は46,605件発生したとしており、さらにUS-CERTがサイバー攻撃に対応した件数は、政府機関・企業などを含めて、合計228,700件に上るとし、サイバー攻撃に対応した件数は09（同21）年の倍になったとしている。また、15（同27）年2月の米国家情報長官「世界脅威評価」は、サイバースパイは日常的に、米国政府、米軍および企業を標的としており、その「攻撃者」には、①高度に洗練されたサイバー計画を有する国家（例えばロシアや中国）、②技術能力は低いが妨害の意図が大きい可能性のある国家（例えばイランや北朝鮮）、③利益を狙う犯罪者、④イデオロギーに動機づけられたハッカーや過激主義者がいるとの見解を示している。
4 14（平成26）年11月の米中経済安全保障再検討委員会の年次報告書は、中国政府は少なくとも2000年代中盤以降、米国に対する大規模なサイバー諜報を実施してきており、国防省、国防契約企業、民間企業を含めてさまざまな米国のネットワークに侵入した、としている。また、同年6月の米国防省「中華人民共和国の軍事および安全保障の進展に関する年次報告」では、中国軍は、攻撃的サイバー能力への投資を続けているとしている。
5 中国共産党第18回党大会において、胡錦濤（こきんとう）党総書記（当時）が実施した活動報告では、「海洋、宇宙、サイバー空間のセキュリティに重大な関心を払う」と発言している。

の指摘や、軍および治安機関が、IT企業などの人材やハッカーを採用しているとの指摘がある[6]。たとえば13（平成25）年2月、米国情報セキュリティ企業が発表した報告書では、06（同18）年以降、中国人民解放軍所属部隊が米国をはじめとする企業などへサイバー攻撃を行っていたと結論づけている[7]。また14（同26）年5月、米国司法省は、米国企業にサイバー攻撃を行ったとして、中国人民解放軍のサイバー攻撃部隊「61398部隊」の将校らを起訴したと発表した[8]。さらに同年7月、カナダ政府は中国からサイバー攻撃を受けたとして、中国を初めて名指ししている[9]。

14（同26）年10月、ホワイトハウスの非秘密情報システムが、ハッカーに侵入された。この事案については、ロシアの関与が指摘されている[10]。ロシアについては、軍や情報機関、治安機関などがサイバー攻撃に関与しているとの指摘があり[11]、また、軍によるサイバーコマンド創設の検討やハッカーの募集を行っているとみられる[12]。

13（同25）年3月には、韓国の放送局、金融機関などに対するサイバー攻撃が、また、同年6月から7月にかけて、韓国大統領府、政府機関、放送局、新聞社などに対するサイバー攻撃が発生した。これらの事案について韓国政府は、過去の北朝鮮によるサイバー攻撃の手口と一致したとしている[13]。さらに、14（同26）年11月から12月にかけて、米国の映画会社に対するサイバー攻撃が発生した。米連邦捜査局（FBI）は同年12月、このサイバー攻撃は北朝鮮政府に責任があると判断するのに十分な証拠があると発表した[14]。北朝鮮については、このようなサイバー攻撃への政府機関などの関与[15]のほか、国家規模で人材育成を行っているとの指摘もある[16]。

Federal Bureau of Investigation

10（同22）年6月、「スタックスネット」と呼ばれる高度に複雑な構造を有するマルウェア（破壊工作プログラム）が発見され、その後もたびたび高度なマルウェアが発見されている[17]。

政府や軍隊の情報通信ネットワークおよび重要インフラに対するサイバー攻撃[18]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、政府機関の関与も指摘されていることから、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。

なお、わが国においても、11（同23）年9月に

6 09（平成21）年の同報告書は、中国人民解放軍が民間企業や学界からコンピュータに関する専門技能を有する人材を採用し情報戦民兵部隊を編成したことや、サイバー空間を利用した訓練を行っていることを指摘するとともに、ハッカー・コミュニティからも人材を採用している可能性がある、としている。

7 13（平成25）年2月の米国情報セキュリティ企業「マンディアント」の「APT1：中国のサイバー諜報部隊の1つを暴露する」は、米国などに対する最も活動的なサイバー攻撃集団は、中国人民解放軍総参謀部第3部隷下の「61398部隊」であると結論づけている。

8 14（平成26）年5月19日、コメイFBI長官は、「中国政府が長い間、中国国営企業の経済的優位を得るために、サイバー攻撃を利用してきた」旨発言している。また同日、中国外交部報道官は「米国が事実をねつ造した」と発表し、米中戦略・経済対話の枠組みのもとに設置されている、サイバー作業部会の活動を停止させるとした。

9 14（平成26）年7月、カナダ政府発表による。

10 14（平成26）年10月の米ワシントンポスト紙は、ロシア政府の関与が疑われるハッカー集団からのサイバー攻撃だったと報じた。

11 04（平成16）年11月、米ダートマス大学セキュリティ技術研究所（現セキュリティ技術社会研究所）の報告書「サイバー戦：各国における方法と動機についての分析」では、ロシアによるサイバー攻撃への軍、情報機関、治安機関などの関与を指摘している。

12 13（平成25）年、ロシア紙「イズベスチヤ」電子版は、ロシア軍高官が、「国防相はサイバーコマンドを創設する準備を指示した」と述べたと報じた。また、12（同24）年10月の「The Voice of Russia」は、ロシア国防省がハッカーの募集を開始したと報じた。

13 韓国未来想像科学部（科学技術政策と情報通信技術（ICT）に関する事務を所掌する中央行政機関。13（平成25）年3月、教育科学技術部の科学技術関連業務と放送通信委員会および知識経済部の一部業務を移管して設置）報道資料（13（同25）年4月および7月）において、官・民・軍合同対応チーム（未来想像科学部、国防部、国家情報院、国内セキュリティ企業など18機関で構成）の調査結果として公表されている。

14 FBIはその証拠として次の3点を指摘。①サイバー攻撃に使われたマルウェア（破壊工作プログラム）は、北朝鮮関係者が以前利用していたものと酷似していた。②データを消去したマルウェアには、北朝鮮のIPアドレス（インターネット上の住所）が組み込まれていた。③今回攻撃に利用されたツールは、13（平成25）年3月に北朝鮮が、韓国の放送局や金融機関にサイバー攻撃したものと類似性があった。

15 13（平成25）年11月、韓国報道各社が、韓国国家情報院が国会情報委員会の国政監査で北朝鮮のサイバー戦能力などについて明らかにしたと報じるとともに、北朝鮮の金正恩国防委員会第1委員長が、「サイバー戦は、核、ミサイルと並ぶ万能の宝剣である」と述べたと伝えた。また、14（同26）年3月に米国防省が公表した「2013年北朝鮮に関する軍事および安全保障の進展に関する年次報告書」では、北朝鮮は軍事的な攻撃的サイバー作戦能力をおそらく保有しているとしている。さらに、15（同27）年1月、韓国の「2014国防白書」は、北朝鮮はサイバー部隊を集中的に増強し、規模は約6,000人と指摘している。

16 たとえば、11（平成23）年6月の韓国の脱北者団体「NK知識人連帯」主催「2011北朝鮮のサイバーテロ関連緊急セミナー」における「北朝鮮のサイバーテロ能力」と題した発表資料は、北朝鮮のサイバー関連組織について、政府機関などの関与を指摘し、サイバー戦力養成のため、全国から優秀な人材を発掘し、専門教育を行っている、としている。

17 特定のソフトウェアとハードウェアが組み込まれた制御システムを標的にするという点では確認されたものとして初のウィルス・プログラムであり、検知されることなく標的のシステムにアクセスし、情報の窃取やシステムの改変を実行する能力を有すると指摘されている。また、11（平成23）年10月に、「デューク」、12（同24）年5月「フレイム」、同年6月「ガウス」、同年8月「シャムーン」と呼称されるマルウェアの発見が伝えられている。

18 ウクライナの親ロシア派集団「サイバー・ベルクート」は14（平成26）年3月、NATOの複数のウェブサイトへのサイバー攻撃を行い、15（同27）年1月、ドイツ政府やドイツ連邦議会のウェブサイトへもサイバー攻撃を行った。また、国際ハッカー集団「アノニマス」は、14（同26）年10月、香港での民主派による大規模デモの最中に、中国政府や香港政府にサイバー攻撃を行うと宣言し、両政府の複数のウェブサイトがサイバー攻撃を受けた。さらに、15（同27）年1月、イスラム過激派の支持者とみられるハッカー「サイバー・カリフ」は、米中央軍の「ツイッター」の公式アカウントへの不正書き込みや、フランス国内の軍や民間企業等、2万件近いウェブサイトへの攻撃を行ったとされている。このように、ハッカー集団によるサイバー攻撃も多発している。

は、防衛装備品などを製造する民間企業のコンピュータが不正なプログラムに感染するという事態が発覚したほか、警察庁によると、12（同24）年9月のわが国政府による尖閣三島取得の閣議決定を行った日以降、数日の間に裁判所や行政機関、大学病院など少なくとも19のウェブサイトに対して攻撃が行われ、被害が発生した。

これらの他にも、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も指摘されている[19]。

3 サイバー攻撃に対する取組

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、政府全体レベルおよび国防省を含む関係省庁レベルなどで、各種の取組が進められている[20]。

近年新たな安全保障上の問題となっているサイバー攻撃に関しては、効果的な対応を可能とするうえで整理すべき論点が指摘されている。たとえば、サイバー空間における国家の行動にかかわる規範や国際協力に関して、幅広いコンセンサスはみられない。こうした問題意識を踏まえて、国際社会の合意によりサイバー空間における一定の行動規範の策定を目指す動き[21]があるが、米国や欧州、わが国などは、自由なサイバー空間の維持を訴え、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など、各国の主張は対立しているとの指摘もある。

参照 Ⅲ部1章1節6（サイバー空間における対応）

1 米国

11（平成23）年5月に発表された「サイバー空間のための国際戦略」は、サイバー空間の将来に関する米国のビジョンを提示し、その実現に向けて各国政府および国民と協力するためのアジェンダを設定した。また、優先的に取り組むべき七つの政策分野として、経済、ネットワーク防護、法執行、軍事、インターネット・ガバナンス、国際的な能力構築およびインターネットの自由をあげている。

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、同省のサイバー・セキュリティ・通信室（CS&C）が政府機関のネットワーク防御に取り組んでいる。

Office of Cybersecurity and Communications

米国は15年（同27）年2月に公表した「国家安全保障戦略」（NSS）において、今日の主要な脅威の一つとしてサイバー攻撃の脅威をあげている。国防省の取組としては、14（同26）年3月に公表された「4年ごとの国防計画の見直し」（QDR）において、米国の国益に対するリスクであるサイバーの脅威は、個人、組織、国家といった様々な主体により構成されており、国防省や産業ネットワーク・インフラへの不正アクセスによって、米国と同盟国・友好国の重要インフラが脅威にさら

National Security Strategy

Quadrennial Defense Review

19 12（平成24）年10月、米下院情報特別委員会による「中国通信機器企業華為技術および中興通訊が米国国家安全保障に及ぼす問題」と題する調査報告書では、米国重要インフラに対するサイバー攻撃能力や企図に対する懸念や、中国主要IT企業と中央政府、共産党、人民解放軍との不透明な関係がサプライチェーンリスクを増大させることへの強い懸念といった、国家安全保障上の脅威を理由に、中国大手通信機器メーカー「華為技術」および「中興通訊」の製品を利用しないように勧告された。フランス、オーストラリア、カナダ、インドおよび台湾などでも同様の動きがみられ、英国および韓国などでは注意を促す動きがみられる。

20 一般的に政府全体レベルでは、①サイバーセキュリティ関連部門の統合や運用部門の一元化、②専任のポストの設置や研究部門の新設および拡充などによる政策部門および研究部門の強化、③サイバー攻撃対処における情報機関の役割の拡大、④国際協力の重視、などの傾向があると考えられる。国防省レベルにおいても、サイバー空間における軍の作戦を統括する機関を新設するなど、サイバー攻撃への取組を国防戦略の中の重要な戦略目標と位置づけるなどの対応が進められている。

21 国連のサイバー問題に関する政府専門家会合は、日本、米国、ロシア、中国など計15か国（14（平成26）年7月の会合より計20か国）の専門家が参加し、04（同16）年から協議を続けている。13（同25）年6月に発表した国連総会向けの報告書は、国際法、特に国連憲章は、平和及び安定を維持し、開かれた、安全で、平和的で、アクセス可能なICT環境を促進するために適用可能であり、また，これらにとって不可欠であると提言した。

されているとの認識を示したうえで、米軍のサイバー戦能力を本土防衛上保持すべき重要な分野と位置づけ、引き続き、人材確保・育成およびサイバー任務部隊の拡充を行うとしている。

15（同27）年4月に公表された「米国防省サイバー戦略」は、サイバー脅威について、国家主体[22]および非国家主体が米国のネットワークに対する破壊的なサイバー攻撃や米国の軍事技術情報の窃取などを企図しており、米国は深刻なサイバー脅威にさらされているとの認識を示している。そこで、国防省は、①国防省のネットワーク、システムおよび情報の防護、②サイバー攻撃による深刻な結果からの米国およびその権益の防護、③軍事作戦の支援のための統合的なサイバー能力の提供、の三つをサイバー空間における主要な任務とし、当該サイバー能力には、敵国軍事システムの破壊を目的としたサイバー作戦が含まれるとしている。こうしたサイバー空間における任務を遂行するために、①サイバー作戦実施のための即応的な部隊および能力の構築・維持、②国防省の情報ネットワークおよびデータの防護並びに任務上のリスクの軽減、③関係省庁・企業等との連携を通じた重大なサイバー攻撃からの米国およびその権益の防護体制の構築、④紛争管理におけるサイバー空間における各種手段の活用、⑤同盟国およびパートナー国との緊密な協力関係の構築、という五つの戦略構想を示している。

組織面では、戦略軍隷下のサイバーコマンドが、陸海空海兵隊の各サイバー部隊を統括し、サイバー空間における作戦を統括する。また、任務の拡充にともなってその組織を拡充し、国防省の情報環境を運用・防衛する「サイバー防衛部隊」を既に保有していることに加え、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」、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」を創設し、これら三部隊を「サイバー任務部隊」と総称している。また、これら三部隊には複数のチームが所属しているとされ、現在数十チームが活動中としている。また、州兵や予備役を活用し、18（同30）年9月までに133チーム6,200人規模にするとしている[23]。

2 NATO

11（同23）年6月に採択したサイバー防衛に関する北大西洋条約機構（NATO）の新政策および行動計画は、①サイバー攻撃に対するNATOの政治的およ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（同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見なすことで合意している。

組織面では、北大西洋理事会（NAC）がNATOのサイバー防衛に関する政策と作戦の政治的監督を行っている。また、新規安全保障課題局（ESCD）がサイバー防衛に関して政策および行動計画を策定している。さらに、NATOサイバー防衛センター（CCDCOE）がNATOのサイバー防衛に関する研究や訓練などを行う機関として認可され、「サイバー紛争に関する国際会議」を毎年主催している他、「タリンマニュアル」の編さんを専門家に委託するなどの活動を実施している[24]。

NATOは08（同20）年以降、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。

3 英国

英国では、11（同23）年11月に新たな「サイバーセキュリティ戦略」を公表し、15（同27）年

22 米国防省サイバー戦略では、ロシアや中国は先進的なサイバー能力および戦略を獲得しているとした上で、ロシアの活動は秘密裏に行われており、その意図を読み取ることが難しいとしている。また中国は、知的財産を窃取し、中国企業に利益を与えているとしている。さらに、イランおよび北朝鮮のサイバー能力は高くないものの、米国および米国の権益に対する敵対的な意図を公然と示しているとしている。

23 15（平成27）年4月、上院軍事委員会における米サイバーコマンド司令官の発言。

24 13（平成25）年6月、NATO国防相会合では、初めてサイバー防衛を主要議題とし、緊急対応チームを創設するとともに、同年10月までにサイバー防衛体制を完全に稼働させることで合意した。

までの目標を設定するとともに、能力強化、規範策定、諸外国との協力、人材育成など具体的な行動計画を規定した。

組織面では、政府全体のサイバーセキュリティ戦略の立案・調整などを行うサイバーセキュリティ・情報保証部（OCSIA：Office of Cyber Security and Information Assurance）を内閣府のもとに、サイバー空間の監視などを行うサイバーセキュリティ運用センター（CSOC：Cyber Security Operations Centre）を政府通信本部（GCHQ：Government Communications Headquarters）のもとに設置している。また、国防省においては、省内のサイバー活動を一元化する国防サイバー作戦グループ（DCOG：Defence Cyber Operations Group）を12（同24）年4月までに暫定的に設置し、15（同27）年3月までに完全な運用能力を保有することとしている[25]。

また英国は、15（同27）年1月、キャメロン英首相とオバマ米大統領がサイバー防衛分野における協力強化[26]で一致するなど、各国との連携強化に努めている。

4 オーストラリア

オーストラリアは、13（同25）年1月、初の「国家安全保障戦略」を公表し、サイバー政策およ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。

組織面では、政府全体のサイバーセキュリティ政策を調整・統括する、サイバー政策グループ（CPG：Cyber Policy Group）をサイバー政策調整官（CPC：Cyber Policy Coordinator）のもとに設置し、オーストラリア通信電子局（ASD：Australian Signals Directorate）の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 Center）が、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への対処を行っている[27]。

5 韓国

韓国では、11（同23）年8月に「国家サイバーセキュリティ・マスタープラン」が制定され、サイバー攻撃対処における国家情報院[28]の統括機能が明確化されたほか、予防、検知、対応[29]、制度および基盤の五つの分野を重点的に推進することとされた。国防部門では、10（同22）年1月に、サイバー空間における作戦の計画、実施、訓練および研究開発を行うサイバー司令部が設置され、現在では国防部直轄部隊として運用されている[30]。

第6節　軍事科学技術と防衛生産・技術基盤をめぐる動向

1 軍事科学技術の動向

近年の情報通信技術（ICT：Information and Communications Technology）の大幅な進歩に代表される科学技術の発展は、様々な分野に波及し、経済、社会、ライフスタイルなど、多くの分野において革命とも呼ぶべき大きな変化が引き起こされている。

このことは軍事分野においても例外ではなく、米国をはじめとする先進諸国では、ICTの発展に端を発する変革が戦闘力などの飛躍的向上を実現できると考え、各種研究と施策が継続して行われている。

たとえば、ネットワークを活用することにより、偵察用の衛星や無人機などの情報収集システムを駆使して収集された敵部隊などに関する情報が共有されれば、遠隔地の司令部からであっても

25 このほか、13（平成25）年9月、英国防省は、コンピュータの専門家数百人を同国のサイバー防衛の最前線で勤務する予備役として採用することを発表し、統合サイバー予備役の創設を認めた。
26 ホワイトハウスの発表によると、英国のGCHQと保安庁（SS：Security Service）、米国の国家安全保障局（NSA：National Security Agency）と連邦捜査局（FBI）がサイバーセキュリティとサイバー防衛に関して密接に協力するとした。また英国政府と米国政府は、重要インフラへのサイバー攻撃に対する防護能力を確認する目的で、15（平成27）年後半に初の共同演習を行うと発表した。
27 ACSCは、豪州犯罪委員会、豪州連邦警察、豪州治安情報機関、豪州国防省及び司法省の職員から構成され、サイバー空間における脅威分析や官民双方のインシデント対応を行っている。
28 国家情報院長のもとには、国家のサイバーセキュリティ体制の確立および改善、関連政策および機関間の役割調整、大統領の指示事項に関する措置や施策などの重要事項を審議する国家サイバーセキュリティ戦略会議が設置されている。
29 14（平成26）年2月、韓国国防部は、他国を攻撃するサイバー兵器の開発計画を国会で報告したと伝えられている。
30 12（平成24）年8月に国防部が大統領に提出した「国防改革基本計画」（2012～2030）においては、将来に向けた軍改革の一つとして、サイバー戦対応能力を大幅に拡充することがあげられている。