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[1]。

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。このような情報通信ネットワークへの軍隊の依存を受け、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[2]。

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[3]。中国はサイバー空間に強い関心を有しているとみられ[4]、軍がサイバー部隊を編成し、訓練を行っているとの指摘や、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[5]。たとえば13（平成25）年2月、米国情報セキュリティ企業

1 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」
2 米中経済安全保障再検討委員会（中国との通商・経済関係が米国の安全保障に及ぼす影響について監視・調査および報告書の提出を行うことを目的として米議会に設置された超党派諮問機関）の議会への年次報告書（12（平成24）年11月）では、11（同23）年には米国防省に対する悪意あるサイバー活動が合計50,097件発生したとされる。
3 12（平成24）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、中国発のサイバー攻撃には、人民解放軍、情報機関、治安機関などがサイバー攻撃に関連している、としている。また、13（同25）年5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」は、12（同24）年の米国政府に対するサイバー攻撃の一部が、中国の政府および軍に直接帰属されると思われるものであったとして、13（同25）年6月のアジア安全保障会議（シャングリラ会合）においてヘーゲル米国防長官が、一部のサイバー攻撃が中国政府や軍に関連していると発言している。
4 中国共産党第18回党大会において、胡錦濤（こきんとう）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。
5 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。

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[6]。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[7]。

08（同20）年、米中央軍の秘密情報などを取り扱うネットワークに、可搬記憶媒体を介してコンピュータ・ウィルスが侵入し、外部に情報が転送される可能性がある深刻な事態に陥った。この事案については、ロシアの関与が指摘されている[8]。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[9]、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[10]。

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[11]。北朝鮮については、サイバー攻撃への政府機関などの関与や国家規模で人材育成を行っているとの指摘もある[12]。

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コンピュータ・ウィルスが発見され、その後もたびたび高度なウィルスが発見されている[13]。

また、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[14]。

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。

6 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。

7 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。

8 08（平成20）年11月のロサンゼルス・タイムズ（電子版）は、米軍高官はロシアが発信源と思われる国防省へのサイバー攻撃について大統領に対し異例の報告を行ったと報じた。また、11（同23）年6月のロイター通信は、米国防省は本事案に対する発信源に対し一切のコメントを拒否しているものの、米政府内外の専門家は、ロシア情報機関の関与を疑っていると報じた。

9 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。

10 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。

11 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。

12 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。また、13（同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。

13 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、「デューク一」、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」と呼称されるコンピュータ・ウィルスの発見が伝えられている。

14 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。

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[15]。

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があるなど、新たな取組に向けた議論がみられる[16]。

参照 Ⅲ部1章1節5（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、同省の国家サイバーセキュリティ部（NCSD）が全体的な総合調整を行っている。

National Cyber Security Division

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。

Quadrennial Defense Review

11（同23）年7月に公表された「米国防省サイバー空間における作戦のための戦略」は、サイバー脅威に関する認識として、外国からのサイバー攻撃などの外的脅威とともに、部内者（インサイダー）による内的脅威も存在すること、敵対者が、国防省のネットワークやシステムの妨害などを追求している可能性があることを示した。そのうえで、サイバー脅威に対処するため、①サイバー空間を陸、海、空、宇宙空間と同様に一つの作戦領域と位置付け、サイバー空間の潜在力を最大限に活用、②国防省のネットワークおよびシステムを防護するため、防衛のための新たな作戦概念を採用、③政府全体のサイバーセキュリティ戦略を可能にするため、他省庁および民間部門と協力、④サイバーセキュリティを強化するため、同盟国およびパートナー国との強固な関係を構築、⑤サイバー分野における優れた人材および急速な技術革新を通じて国家の創意を強化、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」、統合軍による積極的なサイバー攻撃能力の立案プロセスを支援する「サイバー戦闘任務部隊」を15（同27）年9月までに創設する予定としている[17]。さらに、14（同26）年2月には米陸軍本部が「サイバー電磁活動（Cyber Electromagnetic Activity）」というドクトリンを発表するなど、指針の整備を進めている。

15 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。

16 国連、NATO、サイバー空間における国際会議などにおいて、サイバー攻撃が武力攻撃に該当するかどうかを含めた国際法上の位置づけなど、国際的なルール作りに関する議論が進められている。

17 13（平成25）年3月、上下院各軍事委員会における米サイバーコマンド司令官の発言および提出資料

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。

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（CCD COE）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た[18]。

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）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）を政府通信本部（GCHQ）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）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[19]。

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）をサイバー政策調整官（CPC）のもとに設置し、オーストラリア通信電子局（ASD）のサイバーセキュリティ運用センター（CSOC）が、サイバー空間における高度な脅威についての分析を政府に提供し、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への対処に関する調整・支援を行っている[20]。

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[21]の統括機能が明確化されたほか、予防、検知、対応、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[22]。

18 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。

19 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。

20 オーストラリアは、13（平成25）年1月、サイバー攻撃への国家的な対処能力を高めるため、各省庁のサイバー安全保障担当者を1か所に集めた、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）の設立を発表した。

21 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。

22 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。