第2章 国際社会の課題

第1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IT革命により、インターネットなどの情報通信ネットワーク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、情報通信ネットワーク、特に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り、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。

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、以下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・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、ソフトウェアの脆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、IT革命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[2]。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[3]。

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[1]。

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

1-1　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」
1-2　リン米国防副長官（当時）論文「新たな領域の防衛：ペンタゴンのサイバー戦略」フォーリン・アフェアーズ誌2010年9／10月号。
1-3　11（平成23）年2月、リン米国防副長官（当時）はスピーチで、政府のネットワークから軍事計画や兵器システムの設計に関する情報が抜き出されるなどの外国情報機関による侵入事例を指摘した。
2-1　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。

が指摘されている[2]。中国はサイバー空間に強い関心を有しているとみられ[3]、軍がサイバー部隊を編成し、訓練をおこなっているとの指摘や、軍、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[4]。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初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[5]。

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[6]。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[7]、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[8]。

09（同21）年7月、米国および韓国の国防部を含む政府機関などのウェブサイトに対するサイバー攻撃や、11（同23）年3月の韓国国防部を含む政府機関などのウェブサイトに対するサイバー攻撃が発生した。これら事案について韓国警察庁は、攻撃元は中国所在の北朝鮮通信省（ていしん）のIPアドレスであったとしている[9]。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[10]。

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た[11]。また、11（同23）年10月には、スタックスネットと構造が類似した新たなウィルスのほか、12（同24）年5月、6月、8月にも高度なウィルスが発見されている[12]。

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が指摘されている[13]。

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

2 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。

3 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。

4 11（平成23）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、中国の政府または軍は、コンピュータ・ネットワークへの侵入活動を支援しているとみられ、軍自身もコンピュータ・ネットワーク・アタックに関与していると考えられる、としている。また、09年（同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の編成についてやサイバー空間を利用した訓練を行っていることについての事例と共に、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。

5 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。また、13（同25）年、ドニロン安全保障担当米大統領補佐官のアジア協会講演では、中国に対して、①サイバー問題のリスク認識共有、②サイバー不法活動の停止、③共通行動規範の作成を要請する、と発言している。

6 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。

7 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、ロシアのサイバー攻撃に軍、情報機関、治安機関などの関与を指摘している。

8 11（平成23）年11月、国家情報長官国家カウンターインテリジェンス局報告書「サイバー空間で米国の経済機密を盗むスパイ」は、ロシアの情報機関は、経済発展と安全保障を支援する経済情報と技術を収集するために、サイバーなどの作戦を使用している、と記述がある。13年（同25）年、露紙「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、露国防省がハッカーの募集を開始したと報じた。

9 また、11（平成23）年4月に発生した韓国農協のネットワーク障害や、12（同24）年6月の韓国報道機関へのサイバー攻撃についても、韓国政府は、北朝鮮が関与したとする捜査結果を発表している。

10 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、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。

11 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。

12 産業用制御システムのサイバーセキュリティを担当する米政府機関であるICS-CERTは､11（平成23）年10月に､コンピュータ･ウィルス「デューク一」（W32．DUQU）に関する警報を発出した。民間研究機関の分析によると、同ウィルスのプログラムはスタックスネットと多くの点で共通点を持つとされる。情報セキュリティ大手カスペルスキー社は、12（同24）年5月「フレイム」と呼称される大容量で複雑なコンピュータ・ウィルスを、同年6月に「ガウス」と呼称されるコンピュータ・ウィルスを発見したと発表。同年8月サウジ国営の原油精製企業「サウジアラムコ社」のシステムは「シャムーン」と呼称されるコンピュータ・ウィルスによる攻撃を受け、大規模な被害を受けたと伝えられている。

13 11（平成23）年7月、マイクロソフト社「サイバー・サプライ・チェーン・リスク管理」

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。

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[1]。

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[2]。

11（同23）年11月にロンドン、12（同24）年11月にブダペストで、サイバー空間に関する国際会議が開催された。会議では、サイバー空間における経済成長と発展、社会的便益、安全かつ信頼できるアクセス、国際安全保障、サイバー犯罪などについて議論され、今後開催予定のフォローアップ会議においてさらに議論が進められる予定である[3]。

サイバー空間の諸問題や活用案を議論する国際会議風景（ブダペスト）
（12（平成24）年11月）【ハンガリー首相公式HP】

1 米国

11（同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7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、インターネットの自由を挙げている。

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）（National Cyber Security Division）が全体的な総合調整を行っている。

国防省の取組としては、10（同22）年2月に公表された「4年ごとの国防計画の見直し」（QDR）（Quadrennial Defense Review）は、国際公共財（グローバル・コモンズ）として海、空、宇宙空間とともにサイバー空間をあげ、国際公共財へのアクセスを保証することが必要だとしている。さらに、サイバー空間を、米軍の戦力を強化すべき6つの任務領域のうちの一つとしている。

1 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したり、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。

2 サイバー攻撃をめぐっては、攻撃者を特定することが難しく、また、攻撃側に特に守るべきものがない場合が多いことなどから、攻撃を思い止まらせる抑止が困難とされている。また、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付けについては、現時点においては国際社会でコンセンサスが形成されておらず、サイバー攻撃に対し軍隊の既存の交戦規則（ROE：Rules of Engagement）を適用することは困難とみられている。

3 13（平成25）年には韓国でフォローアップ会議が開催される予定である。

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。その上で、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1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5つの戦略構想を示している。

組織面では、09（同21）年6月にサイバー空間における作戦を統括する部隊であるサイバーコマンドの創設を決定し、10（同22）年11月から本格運用を開始している。

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：North Atlantic Treaty Organization）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：North Atlantic Council）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、サイバー防衛に関して政策および行動計画を策定する新規安全保障課題局（ESCD：Emerging Security Challenges Division）、NATOのサイバー防衛に関する研究機関となることを目標としたNATOサイバー防衛センター（CCD COE：Cooperative Cyber Defence Centre of Excellence）などを設置している。

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[4]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：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、14（同26）年4月までに完全な運用能力を保有することとしている。

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1つであるとした[5]。

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 Coordinater）のもとに設置し、オーストラリア通信電子局（ASD：Australian Signals Directorate）のサイバーセキュリティ運用センター（CSOC：Cyber Security Operations Centre）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かか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[6]。

4 09（平成21）年6月に公表した「サイバーセキュリティ戦略」において、サイバー空間のリスク低減、機会活用、知識・能力・意思決定を向上することで英国の利益を確保するとの方針を示した。また、10（同22）年10月に公表された「国家安全保障戦略」（NSS：National Security Strategy）および「戦略防衛・安全保障見直し」（SDSR：Strategic Defence and Security Review）においては、サイバー攻撃を最も優先度が高いリスクの一つとして評価した。

5 09（平成21）年5月に発表した国防白書では、サイバー攻撃の脅威が予想よりもはるかに高まる可能性を指摘しつつ、豪軍が優先的に強化すべき能力の1つとしてサイバー戦能力を提示した。また、同年11月、国家安全保障を支え、デジタル空間での経済利益を最高のものとする、安全で強靱かつ信頼できる電子運用環境を維持することを目的とした「サイバーセキュリティ戦略」を策定。

6 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。

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[7]の統括機能が明確化されたほか、予防、検知、対応、制度、基盤の5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[8]。このほか、12（同24）年6月の米韓外交・国防長官会議（「2＋2」）において、両国間のサイバー分野における調整のため、サイバー安全保障協議体の設立が採択され、これに基づき、同年9月、両国の外交・国防当局をはじめとする関係機関が参加し、第1回米韓サイバー政策協議会を開催し、サイバー空間における両国の関係機関間の協力、サイバー犯罪対処などが協議された。

参照▶ Ⅱ部2章5節・Ⅲ部1章1節3

7 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。

8 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1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。