第1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りつつある。他方、情報通信ネットワーク、特に生活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による情報の改ざんや窃取、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のテクノロジーは日進月歩であり、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）　物理的に人や物を損傷することなく、また実際に接触することなく攻撃を行うことができる。

2）　重要な情報通信ネットワークに障害を発生させることができれば、甚大な被害を与えることができる。

3）　地理的・時間的な制約がないことから、いつでもどこからでも攻撃を行うことができる。

4）　攻撃主体自らの関与が特定されないように、コンピュータ・ウィルスによって乗っ取った無数のコンピュータを経由するなどの各種の手段をとることから、直接的な根拠をもとに攻撃主体を特定することが困難である。

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、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、サイバー攻撃が敵の軍隊の弱点につけこみつつ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[1]。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[2]。

1　リン米国防副長官論文「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。また、米国議会の超党派諮問機関である米中経済安全保障再検討委員会の年次報告書（09（平成21）年11月）では、中国人民解放軍は紛争の初期段階において、敵対する政府および軍の情報システムに対して、コンピュータ・ネットワーク作戦を実施する可能性があるとされている。

2　11（平成23）年2月、リン米国防副長官はスピーチで、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。さらに、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」（10（同22）年8月）は、米国を含む世界中の多数のコンピュータ・システムが中国国内を発信源とした侵入および情報窃取の標的となっており、戦略的施設または軍事施設に関する情報もその対象となっている可能性があると指摘している。

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]。

近年では、政治的あるいは軍事的な紛争が勃発した際に、その主体は必ずしも明らかではないが、サイバー攻撃が発生する事象も見られる。たとえば、06（平成18）年のイスラエルとヒズボラの軍事紛争および08（同20）年のイスラエルとハマスの軍事紛争においては、サイバー攻撃の応酬が発生したとされている。また、08（同20）年8月にグルジア紛争が勃発した際、グルジアの大統領府、国防省、メディア、銀行などのウェブサイトが大規模なサイバー攻撃を受け、ウェブサイトの閲覧が困難になったり、改ざんが行われたりした。これらのサイバー攻撃はグルジア軍の軍事行動には大きな影響を及ぼさなかったが、紛争についてのグルジア政府の公式見解を示したウェブサイトを閲覧できなくなったほか、政府の機能の一部が阻害されたと考えられている[4]。08（同20）年には、イラクやアフガニスタンにおける米軍の作戦を指揮する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[5]。さらに、09（同21）年7月には米国および韓国の国防省を含む政府機関などのウェブサイトに対して、11（同23）年3月には韓国の国防部を含む政府機関などのウェブサイトに対してサイバー攻撃が発生し、ウェブサイトの閲覧が困難になるなどの被害が発生した[6]。また、インターネット上の情報の流れが、接続業者の操作により短時間特定の国を経由するように変更され、各種情報が読解、削除または改変できる状況下に置かれた可能性があるとの事例も指摘されている[7]。

10（平成22）年5月、米国で米戦略軍が主催したサイバー空間に関する国際シンポジウムの一場面〔米戦略軍〕

10（同22）年7月に発見された「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・ウィルスは、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[8]。

3 米中経済安全保障再検討委員会の議会への年次報告書（10（平成22）年11月）では、09（同21）年には米国防省に対する悪意あるサイバー活動が合計71,661件発生（前年比約31.2パーセント増）したとされる。また、豪州国防通信電子局（DSD）は10（同22）年10月、軍のネットワークに対する同年の攻撃件数は、1か月あたり700件に達し、前年比で3.5倍に及んだと発表した。

4 米国国家情報長官（DNI：Director of National Intelligence）「年次脅威評価」（09（平成21）年2月）。同報告書はまた、ロシアと中国を含む多くの国々が米国の情報インフラをサイバー攻撃によって混乱させる能力を有していると評価している。

5 前掲リン米国防副長官論文。中東地域の米軍基地において、外国の情報機関によってコンピュータ・ウィルスを埋め込まれた可搬記憶媒体が米軍のコンピュータに挿入され、中央軍のネットワークに当該ウィルスがアップロードされた。ウィルスは検知されずに秘密情報等を取り扱うシステムなどに拡散し、データを外国が管理するサーバーに転送することが可能となる事態が生起した。

6 マレン統合参謀本部議長の演説（09（平成21）年7月8日）およびリン国防副長官の演説（09（同21）年10月1日）。
11（同23）年4月、韓国警察庁は、同年3月に発生した韓国政府機関などに対するサイバー攻撃は、09（同21）年7月のサイバー攻撃と手口が同一であったと発表した。

7 米国国家情報長官（DNI）「世界脅威評価」（11（平成23）年2月）は、10（同22）年4月、中国のインターネット接続業者が不正確な情報を入力したことにより、インターネット上の大量の情報の流れが17分間にわたって中国国内を経由するように変更され、米国の政府や軍のウェブサイトを出入りする情報の流れが影響を受けたと指摘している。

8 11（平成23）年3月、米下院国土安全保障委員会サイバーセキュリティ、インフラ防護、セキュリティ技術小委員会で開催された公聴会における、レイティンガー国土安全保障副次官（当時）の証言。

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、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。

政府全体レベルで各国が現在進めているサイバーセキュリティ政策においては、新たな安全保障上の問題に対する国際的および政府横断的な効果的対処の必要性といった観点から、①複数の機関に分散している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。

また、国防省レベルにおいても、サイバー攻撃への対処やサイバー空間における活動の安全性の確保は各国の軍隊にとって死活的な問題になっており、国防政策においてサイバー攻撃への取組が重視されつつある。たとえば、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、各国における取組が進められている[9]。

さらに、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国際社会で合意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）を適用することは困難とみられている。また現状では、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、幅広い合意はみられない。こうした問題意識を踏まえて、サイバー攻撃に対する抑止やサイバー空間における交戦規則（ROE）の策定、さらには、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[10]など、新たな取組に向けた議論がみられる。

1 米国

米国は、09（平成21）年5月に発表された「サイバー空間政策見直し」に基づいて、サイバーセキュリティ調整官をホワイトハウスに新設し、サイバーセキュリティ政策について関係省庁間の調整を行うこととした。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。将来のサイバー空間を、新技術に対して開放的（open）で、相互に利用可能（interoperable）で、安全性（secure）や信頼性（reliable）が保たれたものにするため、サイバー空間に

9　本文で記述した各国の国防組織における取組のほかにも、たとえば、中国国防部報道官が11（平成23）年5月25日の定例記者会見で述べたところによれば、部隊のネットワークの防護と安全の水準を向上させる目的で、人民解放軍に「ネットワーク藍軍」を創設したとされている。

10　たとえば英国は、11（平成23）年2月のミュンヘン安全保障会議においてヘーグ外相が、①サイバー空間においては、政府が均衡性のある対応をとり、国内法および国際法に基づいて行動する必要、②全ての利用者がサイバー空間へアクセスする能力を有する必要、③言語、文化および思想の多様性に対する寛容さ、尊重を示す必要、④サイバー空間がイノベーションと、思想、情報および表現の自由なやり取りに対して開放的であり続けることを確保、⑤個人のプライバシー権および知的所有権を尊重する必要、⑥サイバー空間における犯罪活動に共同で対処する必要、⑦ネットワーク、サービスおよびコンテンツへの投資に対する公平な対価を確保する、競争的な環境の促進、の7原則を提示した。
米国は、11（同23）年5月に公表した「サイバー空間のための国際戦略」の中で、①基本的自由の擁護、②財産権の尊重、③プライバシーの尊重、④犯罪への適切な対処、⑤自衛権の留保、⑥インターネットの国際的な相互利用可能性の確保、⑦ネットワークの安定性の確保、⑧ネットワークへの信頼性あるアクセスの確保、⑨全ての利害当事者のためのインターネット・ガバナンス、⑩サイバーセキュリティにおける国家の「相当な注意（義務）」（due diligence）、といった原則を提示した。

おける適切な行動規範への国際的な合意を目指すとともに、その実現に向けて外交、防衛および能力構築における取組を統合するとしている。また、同戦略は、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が戦略目標の設定や全体的な総合調整を行う。また、09（同21）年に国土安全保障省に新設された国家サイバーセキュリティ・通信統合センター（NCCIC）National Cybersecurity and Communications Integration Centerは、政府のサイバーセキュリティ関連機関の業務を統合し、24時間態勢の警戒監視センターとしての役割を有している。

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）として陸、海、空、宇宙とともにサイバー空間を挙げ、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、サイバー空間における効果的な作戦を、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。「サイバー空間のための国際戦略」は、サイバー空間における敵対行動に対しては、その他の脅威に対するのと同様に対応し、米国は軍事を含むあらゆる手段を国際法に合致した形で適切に行使する権利を留保する、としている。その上で、①軍にとって信頼性があり安全なネットワークの必要性が高まっている状況を認識し、適応させる、②サイバー空間における潜在的脅威へ対抗するため、軍事同盟を構築および強化する[11]、③集団的安全保障の強化に向け、同盟国および友好国とのサイバー空間における協力を強化するなどとしている。また、リン国防副長官は、10（同22）年８月に公表した論文[12]で、現在国防省において策定中とされる新たなサイバー戦略の骨格を提示し、その中で、アクティブ・ディフェンス[13]という防衛手段の導入、ネットワーク防衛を規定する交戦規則（ROE）[14]の策定、政府および民間のネットワークの防衛、同盟国との協力、技術的優越性の維持などの重要性を強調した。

組織面では、ゲイツ国防長官（当時）が09（同21）年６月にサイバー空間における作戦を統括するサイバーコマンドの創設を決定した。サイバーコマンドは10（同22）年５月に初期運用を開始、同年11月から本格運用を開始している。

10（同22）年10月、国土安全保障省と国防省は覚書を締結し、国家全体のサイバーセキュリティのための戦略の策定、能力開発のための相互支援および現行の活動での協調において、両省の協力体制を拡大するための人員、装備および施設の提供についての枠組を取り決めた。

2 NATO

北大西洋条約機構（NATO）North Atlantic Treaty Organizationにおいては、最高意思決定機関である北大西洋理事会（NAC）North Atlantic Councilがサイバー防衛に関する政策と作戦を統括しており、NATOとしてのサイバー防衛政策を有している。10（同22）年11月に公表された「新戦略概念」は、サイバー攻撃を予防・検知する能力、サイバー防衛能力およびサイバー攻撃による被害から回復する能力を強化し、全てのNATO機関を一元化されたサイバー防護の下に置くとした。NATO国際事務局内の体制整備も進められており、10（同22）年８月に新設された新規安全保障課題局（ESCD）Emerging Security Challenges Divisionが、サイバー防衛を含む新たな安全保障上の課

11 具体的には、同盟国や友好国との間で、状況認識能力や共同警戒システムの強化、平時および有事における協働能力の強化、サイバー空間における集団的自衛手段の発展などに向けた取組を継続するとしている。

12 前掲リン米国防副長官論文。

13 リン国防副長官は11（平成23）年２月15日の講演において、「事後的な検知および通知のみを行う受動的な防御に依存するのは適切ではない。アクティブ・ディフェンスはネットワークの速さで作動し、センサー、ソフトウェアおよびインテリジェンスから得られる攻撃パターンに関するデータを用いて、コンピュータ・ウィルスがネットワーク侵入に成功する前に検知および阻止するものである。」と説明している。国土安全保障省は、コンピュータ・ウィルスが侵入する前に検知および阻止する侵入防止システムであるEINSTEIN3を、国家安全保障局（NSA）の技術的な協力を得て開発中である。

14 この論文では、ROEについて、単なるハッキング、犯罪活動、スパイ活動または米国に対する攻撃の識別に有益なものであるとともに、戦時および平時の行動を規定する法に基づき、各個別の事態において、必要性、適切性、均衡性および正当性を満たす行動を決定するものである必要があるとしている。

題にかかる企画・立案を担当している。また、サイバー防衛管理局（CDMA：Cyber Defence Management Authority）は、NATO内でサイバー防衛に関する調整の役割を担っている。また、08（同20）年に新設されたNATOサイバー防衛センター（CCD COE：Cooperative Cyber Defence Centre of Excellence）は、サイバー防衛における研究開発などを行っている。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実施している。

3 英国

英国では、09（同21）年6月に公表された「サイバーセキュリティ戦略」において、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部（OCS：Office of Cyber Security）を内閣府の下に、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）の下に設置することとした[15]。サイバーセキュリティ部（OCS）はその後、情報保証部門と統合しサイバーセキュリティ・情報保証部（OCSIA）となっている。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するとともに、国防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）の新設を決定した。

4 オーストラリア

オーストラリアは、09（同21）年11月に「サイバーセキュリティ戦略」を策定し、司法長官が議長を務める省庁間委員会であるサイバーセキュリティ政策調整（CSPC：Cyber Security Policy and Coordination）委員会が、危機管理や国際的な連携を含む政府全体のサイバーセキュリティ政策を調整・統括している[16]。09（同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。同白書の構想に基づき、国防省は、10（同22）年1月に国防通信電子局（DSD：Defence Signals Directorate）の下にサイバーセキュリティ運用センター（CSOC：Cyber Security Operations Centre）を発足させ、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・支援を実施している。

5 韓国

韓国では、「韓国情報保護白書」などにおいて、サイバーセキュリティに関する国家レベルの一元的管理体制の必要性が指摘されており、国家サイバーセキュリティに関する政策や管理については、国家情報院長が統括・調整を行っている[17]。国防部門では、軍のネットワークの防護について、国防情報戦対応センターが設置されているとともに、10（同22）年1月に国防情報本部の下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創設された[18]。同年12月に公表された「2010韓国国防白書」においては、サイバー司令部の創設にともない情報保護にかかわる任務を再確立した旨言及がなされている。

15 OCSおよびCSOCは、関係省庁からの出向職員によって構成されており、政府横断的な組織になっている。

16 このほか、「サイバーセキュリティ戦略」に基づき新設された司法省のCERT Australiaは、民間事業者に対する脅威情報の提供や、事案対処の支援を行っている。

17 国家情報院長の下には、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。また、軍のネットワークの防護については機務司令部の国防情報戦対応センターが、政府および公的機関のネットワークについては国家情報院の国家サイバーセキュリティ・センター（NCSC）が、民間のネットワークについては放送通信委員会の韓国インターネット・セキュリティ・センター（KISC/KrCERT）がそれぞれ担当している。

18 11（平成23）年4月、韓国国防部は、現在国防情報本部隷下にあるサイバー司令部を、国防部直轄部隊に変更する方針を発表した。