第2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。一方、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 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[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]。

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]。

08(平成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[2]。さらに、09(同21)年７月には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して、11(同23)年３月には韓国の国防部を含む政府

1-1 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。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(11(平成23)年11月)では、中国人民解放軍がコンピュータ・ネットワーク攻撃に関与しているとみられ、また、中国の軍事戦略は、米国を含む敵国に対する、コンピュータ・ネットワークを通じた情報収集活動および攻撃を想定しているとされている。

1-2 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。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」(12(同24)年５月)は、米国を含む世界中の多数のコンピュータ・ネットワークおよび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いると指摘している。

2-1 米中経済安全保障再検討委員会の議会への年次報告書(11(平成23)年11月)では、10(同22)年には米国防省に対する悪意あるサイバー活動が合計55,812件発生したとされる。

2-2 前掲リン米国防副長官(当時)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など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に転送することが可能となる事態が生起した。

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[3]。

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[4]。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も発見されている[5]。

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、同年中には、立法府や行政機関に対しても攻撃が行われた。

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、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。

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、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、各国においてサイバー攻撃への対応が進められている[1]。

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[2]など、新たな取組に向けた議論がみられる[3]。

2-3　マレン統合参謀本部議長(当時)の演説(09(平成21)年７月８日)およびリン国防副長官(当時)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。

4　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

5　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」(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。

3-1　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。

2　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。

3　このほかにも、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)を適用することは困難とみられている。
Rules of Engagement

11(平成23)年11月には、英国政府の主催でサイバー空間に関する国際会議が開催された。同会議では、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議論が進められる予定である[4]。

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、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)が全体的な総合調整を行っている[5]。
National Cyber Security Division

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)は、国際公共財(グローバル・コモンズ)として陸、海、空、宇宙空間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[6]。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[7]、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。
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[8]、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

4　11(平成23)年の会議には、60か国の政府機関、民間セクター、NGO代表など約700名が参加した。なお、12(同24)年にハンガリーで、13(同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。

5　同省の国家サイバーセキュリティ・通信統合センター(NCCIC)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。
National Cybersecurity and Communications Integration Center

6　11(平成23)年11月に国防省が議会に提出した「米国防省サイバー空間における政策に関する報告書」においても、同様の見解が示されている。同報告書はさらに、国防省が大統領の命令があった場合には攻撃的なサイバー作戦を実施すること、米国政府がサイバー空間を通じた情報収集活動を実施していること、国連憲章や武力紛争法などの既存の法規範がサイバー空間においても適用されることなどを示している。

7　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。

8　国防省は、新たな作戦概念の採用に向けて、サイバーセキュリティに関する職員の意識改革に取り組んでおり、今後、部内者(インサイダー)による脅威に対処するための内部監視などの強化や、アクティブ・ディフェンスという防衛手段を採用するとしている。なお、同防衛手段に関し、リン国防副長官(当時)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。

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、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部隊であ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。

2 NATO

11(同23)年６月の北大西洋条約機構(NATO)国防相会合において、サイバー防衛に関するNATOの新政策および行動計画が採択された。同政策は、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るものである。

組織面では、最高意思決定機関である北大西洋理事会(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、防衛問題に関しNACへの助言を行う機関である防衛政策計画委員会(DPPC)が専門家レベルで監督・助言を行うほか、サイバー防衛に関し責任を有する政治・軍・運用・技術スタッフの代表により構成されるサイバー防衛管理委員会(CDMB)[9]は、NATO本部および関連組織間の調整を行う。国際事務局内では、新規安全保障課題局(ESCD)が、サイバー防衛に関する政策および行動計画を策定している。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)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行っている。

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)(後に、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)へ改編)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)のもとに設置することとした[10]。10(同22)年10月に公表された「国家安全保障戦略」(NSS)および「戦略防衛・安全保障見直し」(SDSR)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)の新設を決定した。11(同23)年11月には、新たな「サイバーセキュリティ戦略」が公表され、DCOGは12(同24)年４月までに暫定的に設置され、14(同26)年４月までに完全な運用能力を保有することとされた。

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)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[11]。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)のもとにサイバーセキュリティ運用センター(CSOC)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・支援を行っている。

9　CDMBは、10(平成22)年８月に国際事務局内に新設された新規安全保障課題局(ESCD)から、委員会の運営に関して支援を受ける。
10　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。
11　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。

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」が制定された。同プランには、制度面の整備、関連部署の役割分担、分野別の重点課題などに関する事項が含まれており、サイバー攻撃対処における国家情報院[12]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。このほか、11(同23)年10月に開催された米韓安保協議会議において、米韓間におけるサイバー空間の分野での協力を強化することで合意している。

参照　Ⅱ部３章６節・Ⅲ部１章２節３

12　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。また、軍のネットワークの防護については国軍機務司令部(Defense Security Command)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。
National Cybersecurity Center