概観　日本の防衛力　5

サイバー攻撃対応力

安全保障研究委員会
井上　廣司　陸自72

政府は、サイバーセキュリティ基本法に基づき、今後3年間の「サイバーセキュリティ戦略」を7月27日に閣議で決定した。

同戦略は、現状について実空間で収集された大量のデータを分析、活用するなど、サイバー空間と実空間の一体化が進み、サイバー空間の脅威が実空間に影響をもたらす可能性が増加していると指摘している。

脅威に対して事前に防御策を取る「積極的サイバー防御」の推進を掲げ、サイバー関連事業者と連携しながら、脅威情報の共有や活用の促進、攻撃者の情報の収集などを推進する方針を掲げた。さらに国家の強靭性の確保として、サイバー攻撃に対する抑止力の向上なども盛り込み、防衛省、自衛隊におけるサイバー攻撃対処を行う部隊の能力向上を図ることとした。

また、2019年度予算の概算要求で、内閣のサイバーセキュリティセンター（NISC）の予算を2018年度の1・7倍の約42億円を計上する方針を固めた。2020年の東京オリンピック・パラリンピックに向けた防衛態勢を強化することが狙いである。

評価の難しい分野であるが、日本のサイバー攻撃対応力を概観する。

サイバー空間とは、リチャード・クラーク『世界サイバー戦争』によれば、「地球上に存在するコンピューター・ネットワークすべてと、これらのネットワークに接続・制御されるものすべての総称である」と定義され、安全保障の分野では、陸、海、空、宇宙に続く、「第五の戦場」と位置づけられている。

すでに、世界20カ国でサイバー部隊が創設され、その内、他国の情報を破壊できるサイバー能力を持つのは7カ国（米国、ロシア、フランス、イギリス、中国、北朝鮮、イラン）と言われている。防衛省によれば、北朝鮮のサイバー部隊は約7千人、ロシアは約1千人、中国は宇宙・サイバー・電子戦を含めて約13万人といわれている。特にロシアは、参謀本部情報総局（GRU）にテロ対策やサイバー攻撃の任務が加わり、作戦領域を拡大しているとの見方が出ている。

日本政府にとって、サイバー攻撃対処は深刻な課題である。4月に、内閣サイバーセキュリティセンター（NISC）は、中央省庁職員の公用メールアドレス2千件余が流出したとして注意喚起を行った。防衛省・自衛隊は、迷惑メールを含めると年間100万件以上の攻撃を受けている。

サイバー攻撃の種類には、概ね次の4種類がある。

① スパイウェア
個人情報や入力したID、パスワードなどを特定の場所に送信するプログラムの総称

② スパムメール
不特定多数のメールアドレスに大量送信される迷惑メール

③ パソコン乗っ取り
他人のコンピューターを乗っ取り、遠隔操作するためのマルウェア（ウイルス、ワームなどの不正プログラム）

④ 脆弱性分析（標的型メール）
返信すると、ウイルスに感染し、情報が盗み出される。防衛省が受けている攻撃はこの標的型メールが多く、最近では統合幕僚長の名前でメールが送りつけられるケースが起きている。

サイバー攻撃では、あらゆるものが対象となる。2008年には、埋め込み型心臓ペースメーカーを遠隔地から乗っ取られることが証明された。

物理的な設備も攻撃にさらされている。有名なのが、2010年、イラン核施設が乗っ取られ、遠心分離機の回転数を操作し、ウランの精製率を下げた事件である。後にこの原因がコンピューターウイルス「スタックスネット」（Stuxnet）であることが判明した。コンピューターの指令によってアナログの物理的設備を混乱・破壊できることが証明された。

2014年、ロシアがクリミアを併合したウクライナ紛争の際、サイバー攻撃と電子戦でウクライナ側が混乱に陥ったと言われている。

このようなサイバー攻撃に対処するため、2014年防衛省にサイバー防衛隊が創設された。現在、約110人態勢でシステムを監視しており、今年度末には約150人態勢に増員されるが、北朝鮮、ロシア、中国などに較べれば、あまりにも少ない。防衛省は、新たに民間からハッカーなどの人材を受け入れたい考えだが、希望者が殺到する状況にはない。

米国の情報セキュリティ会社「ファイア・アイ」は、北朝鮮、ロシア、中国のサイバー能力は高く、日本にとって大きな脅威だと分析している。

サイバーの分野では、攻撃側が圧倒的に有利である。新種のマルウェアを開発して送りつければ、防御側は対処やマルウェアの解析に追われることになる。対応は、自らのシステムを守り、関係機関に警戒情報を提供することしかできない。反撃するためには、相手（発信元）の特定が必要であるが、サ

イバー空間の広がりとともに非常に難しくなってきている。

現在、防衛省のサイバー防衛隊が行っている訓練の多くは、標的型メールなどへの対処能力向上であり、サイバー攻撃に関する基礎的な知識や技能は保持しているものの、専守防衛への配慮から攻撃を前提とした本格的な能力の保有には踏み出していない。

日本の場合、戦争放棄の憲法9条、国防の基本方針から専守防衛を基本としていることから、敵地攻撃能力と同様に政治的に大きな壁がある分野である。今年中に策定されると見られる防衛計画の大綱と新中期防衛力整備計画の中で、サイバー攻撃能力保有に踏み込むかどうかが焦点になる。

自衛隊は日本に対するサイバー攻撃対処の任務を与えられていない。自衛隊法第6章「自衛隊の行動」第76条「防衛出動」は対象が「武力攻撃」であり、物理攻撃でないサイバー攻撃は対象外である。現状では、自衛隊が守るのは、自衛隊の指揮系統などのシステムであり、国の重要インフラではない。一方で諸外国では、サイバー攻撃に対する防衛は軍隊の管轄である。

現代社会はコンピューターやネットワークに依存していると言っても過言ではない。それが脅かされれば国民生活への打撃は大きい。

これは日本だけの問題ではなく、世界の問題でもある。そのために、サイバー攻撃に関する国際法などで規制すべきであるとの議論もある。

実は、2001年に欧州議会が発案した「サイバー犯罪条約」がある。2004年に発効し、日本も同年に批准している。

この「サイバー犯罪条約」は、①違法アクセス・傍受の禁止、②コンピュータシステムの妨害と③マルウェアの製造を取り締まり、締約国は犯罪摘発、犯罪人の引き渡し、証拠データの保存が求められる。

ただこの条約は、欧米主導の規制であり、当然のように中国、ロシアは無視している。

サイバーセキュリティの専門家であるK・エラザリ氏は、「米国をはじめ各国政府はサイバースペースに軍備を施して、中央の役所や秘密機関によってデジタル世界を警備しようとしているが、これは決してうまくいかない。かえって事態を悪化させる」と述べている。

その理由の一つが、サイバースペースの広大さである。そもそも単一のサイバースペースというものが存在しない。サイバースペースは多数のシステムが相互接続された巨大なシステムであり、常に変化しながら拡大している。

そんなものを制御できるわけがない。

2020年には、産業用・軍事用・航空宇宙用などのシステムを含め、約500億個の機器がインターネットに接続される。新たに接続される機器は全てサイバー攻撃の対象となりうるし、攻撃者はその最も弱いリンクを見つけ出すことにたけている。

もう一つが、サイバースペースは、公共のパブリック・コモンズではないということである。領土や国際水域などとは異なり、政府や軍隊が実効支配できるスペースではない。サイバースペースを構成する技術やネットワークの大部分は、営利目的の多国籍複合企業が所有・運営している。この空間が包含する技術の数と種類は急激に増え続けており、政府が管理できる範囲を超えている。

その他に、各国政府がサイバースペースの安全確保に関して重大な葛藤を抱えている。それがサイバースペースの脆弱性である。誰かのサイバーセキュリティ上の重大な脆弱性は、別の誰かの秘密兵器となる。

例えば、前述したK・エラザリ氏によれば、米国防総省はサイバースペースの防御法よりも攻撃の研究開発に多くの人材を雇っており、国家安全保障局（NSA）はサイバースペース攻撃の為に防御の2・5倍の費用をかけている。また、今回「国家サイバー戦略」の発表にあたり、ボルトン大統領補佐官は「オバマ大統領時代の制限を取り払い、攻撃的なサイバー作戦を可能にするものだ」と述べている。

残念ながら、日本のサイバー攻撃への対応力は、基本的な技術は保有しているものの人材や資金を見ても明らかなように主要国に較べれば甚だ弱小と言わざるを得ない。能力的には、防衛省のシステムを守ることと攻撃メールに関する情報収集や脅威情報の提供に限定される。対応能力の強化のためには、攻撃機能の保持が必要かもしれない。

では、サイバー攻撃にどう対応すべきなのだろうか。K・エラザリ氏は、「サイバーセキュリティは公衆衛生の問題に似ている。公衆衛生の問題において、疾病対策センターのような役所は重要な役割を担っているが、自分では病気の拡大を阻止できない。一般市民がやるべきことをやって、役所はその仕事を達成できる」と言う。

サイバーセキュリティを公衆衛生と考えて、官民を問わず、それぞれが手を洗い、予防接種をすることで対応するしかない日本としては、各組織が基本的な対応力を身に付け、縦割りの壁をこえてサイバー攻撃に関する情報を共有することが重要である。