サイバー安全保障基本法が必要ではないか

佐藤　謙

１．サイバー攻撃による被害が多発かつ深刻化している。

我が国では、サイバーセキュリティ基本法の下、セキュリティ強化のための各種対策が講じられ、内閣官房のNISCも情報共有等の機能を果たしている。防衛省においても、サイバー領域における自衛隊の能力向上の施策が展開されてきているが、国の安全保障上の体制としては早急に整備すべき点が残されているように思う。

サイバー攻撃についての国の見解は、武力攻撃の一環として行われる場合、またそれのみで行われる場合であっても物理的攻撃と同様の深刻な被害をもたすものについては武力攻撃に該当するとしている。この見解に異論はなく、武力攻撃に該当する場合には自衛権の発動をもって自衛隊が対処することになるのは言うまでもないが、武力攻撃に至らないが安全保障上看過できないサイバー攻撃については、対処の体制は整っていないのが現状のように思う。仮に武器等防護の規定を想起するにしても、現行法上、自衛隊による防護対象は自らのシステムに限定されざるを得ない。

因みに、いわゆるハイブリッド戦では、第一フェーズとしての相手国の意思決定に影響を与える情報操作を行うサイバー攻撃、第二フェーズとしての民間重要インフラや軍事指揮通信系統などに対する機能破壊を行うサイバー攻撃、第三フェーズとしての通常戦闘―という諸相が想定されている。現象としては、例えば電力システムの停止という個別企業に対するサイバー攻撃であっても、国家に対する攻撃の手段として行われているものであれば、単なるセキュリティの問題としてではなく、国家の安全保障の観点から国が主体的に対応することが求められよう。

２．国の安全保障の現行体制は、当然のことながら、従来の実空間での経験と問題意識を基盤に形成されてきているが、新たな課題として現れてきたサイバー攻撃への対応を考えると、例えば以下に見る如く、サイバー空間の実空間と異なる特性が顕著であるとともに、サイバー空間では実空間にはない独特のオペレーションの必要性もある。

①サイバー攻撃は、そもそも民生分野の事案か安全保障分野の事案か、事案発生時点で即断することは難しい。

②安全保障に関わる事案であっても、どこまでが平時かグレーゾーンか、武力攻撃か判然としないし、その間の移行も瞬時に起こり得る。

③実空間では攻撃を受けたかどうかは明らかだが、サイバー空間ではシステム停止等の事象が発生・調査するまで、攻撃を受けたかどうか分からないことが多い。従って、サイバー空間では、不審な通信が行われていないかを常時監視（モニタリング）することが安全確保のために重要である。なお、我が国では、通信の秘密等の関係から、越境通信であっても国や通信事業者によるモニタリングは行われていない。

④実空間では攻撃が誰によるものかという帰属性（アトリビューション）は一偽装工作も勿論あり得るものの一通常明らかだが、サイバー空間では攻撃の帰属性を解決するためには、様々な関連情報の外、通信記録の解析のみならず通信経路を遡及して発信元を探知する必要が出てくる。その際には相手システムへの逆探知・逆侵入も必要となるが、我が国では、不正アクセス禁止法等に抵触する可能性がある。
⑤武力攻撃に至らないサイバー攻撃であっても、安全保障上看過できない事案に対しては、攻撃のコストを課し、攻撃を止めさせ、二度と攻撃させないようにするために対抗措置を実施することが必要である。その際には相手システムの停止等の措置も必要になってくるが、我が国では、不正アクセス禁止法等に抵触する可能性がある。

３．我が国においては、これまで、サイバー空間の安全はコンピュータシステムを管理するそれぞれの企業や組織に対応が委ねられてきたのが実態で、現行のサイバーセキュリティ基本法もこの大枠を前提にしている。しかしながら、国際社会においては既にサイバー空間がセキュリティ問題を超える国家間の、いわば戦場と化しており、各国ともその脅威への備えに余念がない。従って、我が国としても、国家の安全保障を確保するため、早急に体制整備を図る必要があるが、上述のようなサイバー空間の特殊性を踏まえると、サイバー空間の安全保障という新たな分野について、パッチワーク的でなく全体像を示していくことが、国民の理解と協力を得る道ではないかと考える。
そのため、国のサイバー安全保障の基本方針、国の役割と権限、関係者の協力、サイバー安全保障に責任と権限を有する組織など、サイバー安全保障に関する基本事項を一括して定める「サイバー安全保障基本法（仮称）」を整備することを検討すべきではないだろうか。

（後書き）諸賢の「市ヶ谷台論壇」に対する日頃のご協力に感謝しております。この度は、いわば席亭が高座に上るようなことで恐縮ですが、議論のきっかけとしてご理解頂ければと思います。