第２４８回国際政経懇話会

「サイバー戦争に巻き込まれている日本」（メモ）

第２４８回国際政経懇話会は、伊東寛サイバーセキュリティ研究所長を講師に迎え、「サイバー戦争に巻き込まれている日本」と題して、下記１．～５．の要領で開催されたところ、その冒頭講話の概要は下記６．のとおりであった。

１．日　時：２０１２年9月6日（木）正午より午後２時まで
２．場　所：日本国際フォーラム会議室
３．テーマ：「サイバー戦争に巻き込まれている日本」
４．講　師：伊東　寛　サイバーセキュリティ研究所長
５．出席者：２７名

６．講師講話概要

伊東寛サイバーセキュリティ研究所長の講話概要は次の通り。その後、出席者との間で活発な質疑応答が行われたが、議論についてはオフレコを前提としている当懇話会の性格上、これ以上の詳細は割愛する。

サイバーと国家安全保障の関係

近年、コンピューターやネットワークの普及に伴い、サイバーという概念やそこから派生する問題が意識されるようになってきたが、サイバーと国家安全保障の関係についてはいまだほとんど注目されていないのが現状である。そもそも「サイバー戦争」自体を定義することが困難である一方、その実態は見えない水面下で進行している。したがって、これは「見えない戦争」とも呼ばれるが、国際法や戦争法自体もサイバー技術が生まれる以前に制定されたものであるため、これらの法によっても「サイバー戦争」を充分に規定することはできない。アルビン・トフラーはかつて、世界史の大きな流れを「武力」「経済力」「情報力」の３つのパワーの推移の観点から捉えたが、「武力」は第二次世界大戦にて、「経済力」は冷戦時代にてそれぞれのピークを迎えており、２１世紀は「情報力」によって特徴付けられる世界であることを予測した。「情報力」の優越を問われる主戦場はサイバー空間であり、これが「見えない」空間であるならば、国家間の「サイバー戦争」はすでに水面下で行われているといっても過言ではない。

サイバー攻撃の手法

サイバー攻撃の手法は、これまで「情報窃取型」が主たるもので、それは不特定多数を対象としたものであったが、近年はその重点を特定の個人、団体、組織を対象とするものへとシフトさせつつあり、従来のいわゆるバラマキ型の「ウィルス」に代わり狙った相手だけにマルウエア（ウイルス、ワーム等、悪意を持って利用されるいろいろなソフトウエアの総称）を送り込んでくる「標的型攻撃」というものが増えてきている。その手法は、非常に巧妙で、個人情報を調査した上で実在の人物からのなりすましメールを送り、それに添付したマルウェアを相手のネットワーク内に展開させたり、遠隔操作ツールを送って、相手のコンピューターを完全に乗っ取るなどの手口がある。また、不特定多数を対象としたウィルスとは異なり、このような標的型攻撃で用いられるマルウェアは通常のアンチウィルス・ソフトでは検出不可能なものが多い。ここで、昨今のＳＮＳ（ソーシャル・ネットワーキング・サービス）は、個人情報を露出するという側面があるため、標的型攻撃のための情報収集目的として利用される可能性が高く、その利用には注意が必要である。

「サイバー戦争」の実像

「サイバー戦争」は、国家組織による攻撃を含むものであり、個人のハッカーが技術力の誇示や金銭の入手を目的で行うものとは明確に異なる。ゆえに、強固なセキュリティで防備を施しても、攻撃側は組織的な調査を実行し、目的を達成するまでその攻撃を繰り返し仕掛けてくるだろう。問題は、そうした攻撃を防ぐことが非常に難しい点である。昨今、日本において金融、鉄道、航空等のシステムが原因不明の大規模障害を起こしているが、これは情報収集も兼ねた他国からの攻撃によるものであるとも推測できる。現に、２００３年には米国の主要な軍需産業から１０テラバイトという膨大な情報が盗まれるという事件が発生している。また、一見してサイバー攻撃とは分からない程度の障害を起こし、数パーセントの生産性の低下を狙って、国の基幹産業に影響を与えながら、相手の国力を低下させるという意図も考えられる。サイバー攻撃への防護策については、現在、各省庁がそれぞれに組織を作って対応しようとしているが、まだまだ不十分な面がある。今後、組織的にも予算的にも政府全体で一元化し、十分な調査研究を進めながら、その対策を図ることが求められる。

（文責、在事務局）