現場レポート

サイバーディフェンス研究所

本誌編集委員

二〇一二年一二月、イランのエネルギー関連施設が米国とイスラエルからサイバー攻撃を受けた。この攻撃は、その数か月前に起きたサウジアラビア石油会社と米国の金融機関に対するイランによるサイバー攻撃への報復であると言われている。世界では、上記のようなサイバー空間における国家間や国家と私人間での争いが頻発している。このような世界情勢の中で、我が国のサイバーセキュリティの現状はどうなっているのだろうか。企業や公的部門にサイバー攻撃対策の指導業務を行っているサイバーディフェンス研究所の上級分析官、名和利男氏にお話を伺った。（文責　武智昭憲）

■サイバーディフェンス研究所について

サイバーディフェンス研究所の起源は、米国法人アイディフェンス社の日本法人であるアイディフェンスジャパンである。アイディフェンスは、設立当初、中国やロシアによる米国へのサイバー攻撃に備えて、企業や国家機関に情報提供を行っていた。アイディフェンスジャパンは、中国からのサイバー攻撃に関する情報を収集するための前線基地として日本に設立された組織である。このアイディフェンスジャパンが土台となり、様々な変遷を辿って四年ほど前に現在のサイバーディフェンス研究所が誕生した。

前身であるアイディフェンスジャパンはもともと、「模擬攻撃監査（ベネスレーションテスト）」という事業を中心に行っていた。これは、依頼を受けた企業のネットワーク等に同社が模擬攻撃を仕掛ける事で、事前に対処方法やシステムの弱点を確認することを目的とする事業である。

現在は、サイバーディフェンス研究所となって、事業内容はかなり多様化しており、中でも「研修サービス」は同社の主力商品となっている。「研修サービス」では、サイバーテロ対策を担う警察官、重要なインフラを担う民間企業や官庁の担当者、時にはサイバーセキュリティ会社の技術者を対象として、サイバー攻撃への対応策を指導する。攻撃者の視点に立って自己のセキュリティシステムを見ることで、受講生がシステムの欠陥・弱点を分析する力を養うことを目標としているそうだ。しかし、研修内容を完全にマスターできる受講生は二割程度だという。このような受講結果を名和氏は嘆いていた。真にサイバー攻撃に対応できる人材の育成において、日本は遅れている。

■サイバー攻撃の現状

現在のサイバー攻撃の技術水準は、悪用すればインターネット上のＳＮＳなどに記載されている個人情報を元に、企業や国家の機密情報を探り出すことができるほど高まっている。それを基に綿密に作戦を立て、サイバー攻撃を仕掛けることも可能だ。実際、冒頭で述べたイランのエネルギー関連施設で発生した事件は、こうした過程を辿って引き起こされたと言われている。

通常、エネルギー関連施設のようなインフラを制御しているシステムは外部から遮断されているため、マルウェア（悪意を持ったソフトウエアの総称）に感染することはないが、マルウエアに感染したＵＳＢメモリデバイスを媒介して、マルウェアを制御システム内に送り込むことは可能である。マルウェアは、電力を発生させるためのタービンを制御しているコンピュータ内に入り込んだ場合、そのタービンの正常な機能を狂わせる。その結果、タービンが停止して、電力が供給できなくなり、社会に混乱をもたらすのである。

■サイバー攻撃への対応策―日本と米国の違い

上記のような脅威への対応において、残念ながら日本は欧米に比べて遅れている。その原因を名和氏は、「欧米のシステムエンジニアの所掌する業務範囲は限られている。それ故、システムトラブルが発生した場合、現場のみの判断で対応することはなく、経営者を始めとした組織の上層部まで問題を報告することが多い。結果として、問題認識が組織全体に共有されやすい。一方、日本では現場の人間の所掌業務の範囲が広いため、システムトラブルが発生しても現場で処理してしまう。律儀に上層部にシステムトラブルを報告すると、責任を追及される可能性があるので報告をすることが少ない。その結果、上層部の問題認識は甘くなる。だから、日本では、米国と比べてサイバー攻撃に対処するための適切な取り組みや措置がとられないまま現在にまで至ってしまった。」と分析する。

サイバーディフェンス研究所のホームページ。

日本が米国に後れをとっている一例として、人材確保の方法が挙げられる。米国では、一からの人材育成だけでなく、軍関係者が世界中の優秀なハッカーを競わせる大会を開き、その参加者の一部を雇用するというスカウト方式によるサイバーセキュリティ人材の確保も行っている。対照的に、日本は、一から育成することに重点を置いており、米国のような、既にある程度の技術を備えたハッカーを利用するという発想に欠けている。育成することももちろん大切だが、優秀な人材を確保するという目的に照らせば、米国の方法は非常に合理的だ。

また、意思決定過程にも違いがある。多様なサイバー攻撃に対応するためには、多様な知識・経験を持つ人材の協働が不可欠となる。米国では、様々な分野の人材が活発に意思疎通を行い、政策決定過程に参画し、政策に影響を与えている。しかし、日本における政府の意思決定は、IT知識の十分ではない官僚や現場を離れて久しい学者が、現場との意思疎通を重要視せず、自身の知見や見識の範囲内で前例踏襲という制約下の中で行なってしまうことが多い。極めて短い期間のうちに瞬く間に変化するサイバーセキュリティ情勢を議論する際に、彼らの知識や過去の経験が活かせる場面は限られており、会議の大半の時間は現状に即さない議論に費やされているのが現状である。だから、日本のサイバーセキュリティは後手に回るのだ。

■所感

名和氏は、現在の日本の状況を非常に危惧していた。世界規模でサイバー攻撃が増加する中で、現在の日本は、情報は盗まれ、攻撃され続けている。情報のグローバル化が進む現代において、サイバー攻撃に対する脆弱さは、日本のみならず、他国の機密情報の流出をも招きかねない。そうなれば、日本の信頼は失墜するだろう。日本も国際社会の一員として、サイバーセキュリティにおける責任を果たすことが求められている。そのためにも、日々変化するサイバー攻撃の脅威に迅速かつ柔軟な対応策を打ち出していかねばならない。