安全保障委員会 講演会

1月23日開催

今日のサイバーセキュリティ環境下における サイバー攻撃への対応

サイバー空間が、陸海空、宇宙に次ぐ「第5の戦場」と呼ばれる中、イスラエルでは政府が主導して、多くのサイバーセキュリティ企業を輩出している。わが国においてもサイバー攻撃への対策は喫緊の課題である。元イスラエル首相府次官ハレル・ロッカー氏が、対応策を語った。

講演：ハレル・ロッカー 氏 元 イスラエル首相府次官、Pitkrai Investments Ltd.代表

ITの利用が広がるとともに サイバー攻撃が増えている

現代はITが生活の隅々にまで浸透している。それゆえ、発展したネットワークや技術をサイバー犯罪者が利用しやすくなっていて、サイバー攻撃の件数は指数関数的に増えている。技術への依存度が高まれば高まるほど、脆弱性もそれだけ高まってしまうのだ。もはやサイバーセキュリティは必須なものになっているといえる。

私はイスラエルの首相府次官を務めていたときに、国を挙げてサイバーセキュリティの強化に携わった。最も大切なのは科学技術能力の向上で、そのためには産学官の連携が欠かせなかった。産学連携の強固なベースを元に、政府が人材育成に巨額の投資をした。その結果、イスラエルには約300のサイバーセキュリティ関連の企業が生まれ、25の多国籍企業の研究拠点が集まった。産業全体が急成長しており、世界有数のサイバーセキュリティ専門企業の20%がイスラエルにある。

サイバー攻撃は、政府機関だけでなく企業もターゲットになっている。7割から9割は、特定の組織や企業を狙ったマルウエア（悪意のあるソフトウエア）である。そのため、汎用ソリューションでは通用せず、オーダーメイドの対応が必要である。対応するツールも日々進化しているが、それでもマルウエアの特定には平均で200日ほどかかり、封じ込めるのには70日ほどかかっている。このような現状に、多くの組織や企業が追い付いていないのが現状だ。状況は時々刻々変化しており、今後もさらに変わっていく。攻撃を完全に防ぐのは非現実的とさえいえる。

ハッカーを雇うのは 敵に弱みを見せることに

特に、日本を含む自由世界は、現在ハッカーの攻撃に対応できる備えが十分であるとはいえない。サイバーセキュリティが進んでいるアメリカの昨年の大統領選挙でさえも、裏でハッカーが暗躍したとの報道があった。大規模な組織ぐるみ、国ぐるみによる高度なサイバー攻撃が増えている。

ハッキングに対抗するためにハッカーを雇うという話を聞くことがあるが、これは警察が犯罪者を雇うようなものである。ハッカーの多くは産業スパイや、ある国の諜報員であったりする。そのためイスラエルでは、元ハッカーを雇うことはない。下手に雇うと、こちらの弱みを見せることになり、敵に手の内をさらす可能性もある。もしテロリストにその情報が渡れば、大変な窮状を招くことになるだろう。パートナーは、絶対に信頼できる相手でなくてはならない。

最も重要な対応策は サイバーセキュリティ人材の育成

日本は世界有数の技術立国だが、だからこそサイバー攻撃に対して脆弱になっていると思う。金融や重要インフラのシステムが破壊されれば、国の経済は壊滅的打撃を受けるだろう。

国や企業がサイバー攻撃に効果的な対応をするために最も重要なことは、サイバーセキュリティ人材への投資である。人材不足の中で、人員を急に増やすのは難しいので、現有人材の育成が現実的な選択となろう。また、場合によってはスキルレベルの要件を引き下げて採用し、研修や訓練に投資して、いい人材を定着させる努力が重要である。脅威は常に急展開するので、継続的な育成が欠かせない。

そして、長く信頼関係が築けるような良好なパートナーを探すことも必要だ。日本の場合、民主主義など重要な価値観を共有している自由世界の国がいいだろう。

その点、イスラエルは日本の友好国であり、産学官の連携も進んでいるので協力しやすいはずだ。イスラエル企業のツールやノウハウは、わが国のみならず、同盟国の政府機関や軍でも採用されている。イスラエルが、これまでにサイバー攻撃を受けた経験や、それに対応するノウハウを、日本と共有することは十分可能である。