

サイバーセキュリティと社会情報基盤 ～ 九州をサイバーセキュリティの安全都市に！！ ～

1. サイバーセキュリティの現状と課題

2014年の世界におけるサイバー犯罪による経済的損失は、年間約59兆円¹といわれており、日本の税収を上回る規模の損失が世界で発生している。また、日本政府に対するサイバー攻撃の件数も2013年度では、前年度の5倍の約500万件²超となるなど、サイバー犯罪は国家の安全保障や危機管理上の重要な問題となっている。

さらに、サイバー攻撃の技術についても日々進化しており、例えば、改ざんされたホームページを閲覧したパソコンにウイルスを侵入させ、企業や個人の重要な情報を入手したり、国家の存立基盤である社会インフラの基幹システムを攻撃するなど、経済的なメリットを狙った詐欺や社会システムの破壊を目的としたサイバー攻撃が増加している。

こうした中、我が国では、企業や大学、国民が行うべきセキュリティ対策の基本方針を定めた「サイバーセキュリティ基本法」が2014年11月に制定され、専門人材の育成などに取り組んでいるが、サイバー攻撃の技術が日に日に進歩している中で、防御策の構築が後手に回っているのが実状である。

2. 九州大学における取組み

九州大学では、情報の格付けやセキュリティ保護の方針を詳細に定めたセキュリティポリシーの下、学生全員に対し、あらかじめスペックを指定したパソコンに、基本ソフトやウイルス対策ソフトを大学側が提供するほか、外部からの攻撃防止及び内部から外部への攻撃防止等を目的としたファイアーウォールシステムを構築するなど、大学内のネットワーク環境の安全性を高め、学生が必要な時に必要な情報を入手できる学習環境を整備している。

加えて、サイバーセキュリティセンターを設立し、サイバーセキュリティに関する研究、教育に取り組んでいる。

その教育のコアは、「サイバーセキュリティ・フォー・オール」という考えであり、学生全員に対する学習教育を進めている。また、カリキュラムづくりや教材開発の面でアメリカの大学とも連携を図っている。

今後は、全職業人が最新の知識を持てるような一般利用者のリテラシー向上や高度な人材育成、研究機関の高度化・グローバル化に取り組んでいくこととしている。

¹ 米政策研究所：戦略国際問題研究所発表

² NISC(内閣官房情報セキュリティセンター)「サイバーセキュリティ政策に係る年次報告(2013年度)」

3. 安全なサイバー空間の構築によって新たなビジネスチャンスを掴む

(1) サイバー空間を制するものが世界を制する

サイバー空間は、国を超え、誰もが容易に参加できることから多くの人々によって利用され、いまや欠くことのできない経済社会の活動基盤となっている。

そして、これからは、IOT (Internet of Things) といわれるように、家電、自動車、スマートメーター等の様々なモノやサービスがインターネット等に接続され、そこから得られるビッグデータの利活用等により新たなビジネスへの展開も大いに期待できるため、ものづくり大国である日本が自由、公正かつ安全なサイバー空間の創出に官民を挙げて取り組んでいけば世界を制するといっても過言ではない。

また、サイバー空間の特徴である「いつでも、どこでも、誰とでも」という機能をフルに活用することにより、大企業が優位であった海外企業や消費者との取引が、中小企業やベンチャー企業でも容易にできるようになり、企業の活動拠点が必ずしも大都市に集中する必要もなくなることから、地方創生の後押しにもなりうるのではないか。

(2) サイバーセキュリティなくしてオープンなサイバー空間の発展なし

サイバー空間は、オープンであってこそいろんな応用が働き日々進化するものであるが、一方でどこからでも攻撃することが可能になるという裏腹な面を持っている。

また、各国で情報漏えい事件等が頻繁に報道されていることなどをみれば、リスクをゼロにすることは困難と思われ、いかにリスクを減らすかということが重要である。一方、あまりに厳格な対策はプライバシー等の問題を惹起することにも繋がりがかねないことに留意する必要がある。

サイバーセキュリティの強化による安全なサイバー空間の構築は、既に経済活動の基盤となっている背景を鑑みれば、サイバー空間を活用するシステムの構築以上に早急に高度化を図る必要がある。また、利用者の意識の向上も喫緊の課題である。

このため、安全で安心なサイバー空間の構築には、サイバー攻撃に対抗するための日進月歩の技術革新が必要であるほか、リテラシー教育の徹底により、システム的な検知が困難な問題点をも見つけ出し、不正行為を排除できる環境整備も必要である。また、そうした環境整備に向けて行政や民間企業、さらには国家などが組織的に対応することが望まれる。

他方、このサイバーセキュリティ確保のためのインフラ整備は、新たなビジネスを生み出す可能性を秘めていることも指摘しておきたい。

(3) 九州を世界的なビジネスセンターへ

安全で安心なサイバー空間を構築すれば、その地域は、世界のデータの集積拠点として、またイノベーションの中心地として、世界のビジネスセンターになり得る可能性がある。

そのためにも、九州大学の取組みによってサイバーセキュリティに対する

意識が一般利用者へも浸透し、さらに専門人材の育成や先端技術の進化によって安全性を向上させることにより、ここ九州が世界的なビジネスセンターとして発展していくことを期待したい。

平成27年8月31日

九州の未来力2030

座長 森 本 廣