ＩＣＴ教育に欠かせないサイバー攻撃対策
産官学一体での専門人材育成が急務!!

今号では、政府が推進する学校教育のＩＣＴ活用の動きを大々的に取り上げた。全国の小中学校で全生徒に１人１台学習用パソコンが配備され、さまざまな先端技術を取り入れた効率的・効果的な教育が実践されることに期待が集まっているが、気になるのはサイバーセキュリティリスクだ。来る「ＩＣＴ教育」時代において、日本の情報セキュリティは生徒たちの学習や生活のデータを守ることができるのだろうか。

「サイバー攻撃は10年くらい前から本格化し、５年くらい前からはセキュリティソフトをはじめとした個人レベルの対策では間に合わなくなってきている」と話すのは東京工業大学情報理工学院サイバーセキュリティ研究センター長の田中圭介教授。「事実、古くから使用されてきたタイプのセキュリティソフトで防ぐことができるサイバー攻撃は全体の5％と考えられている」という。それもそのはず、昨今のサイバー攻撃の種類は多様化の一途をたどっており、サイバー攻撃による金融犯罪も急増、その被害額はすでに強盗などの物理的な犯罪よりも大きくなっているそうだ。

では、日本のサイバー攻撃対策はどうなっているのか。２０１９年４月、内閣サイバーセキュリティセンター（ＮＩＳＣ）がサイバーセキュリティ分野において官民一体で情報共有・連携体制を構築する「サイバーセキュリティ協議会」の立ち上げを発表したが、遅きに失しているといわざるを得ない。しかもそのリリースには「サイバーセキュリティの確保は本来、各組織が自主的に取り組むべきもの」との文言もあり、いわば対策は各自治体や企業任せ。小規模な自治体や企業の多くはセキュリティに投じられる予算が少なく、手をこまねくしかないのが現状である。

そして、何より深刻なのがサイバーセキュリティについて統合的なリスクマネジメントができる人材が不足していることだ。政府ＣＩＯ（内閣情報通信政策監）補佐官制度やプロジェクトマネジメントの導入にかかわるなど、多くの海外・民間・政府のＩＴプロジェクトに携わってきた西野弘氏によれば「たとえばアメリカではサイバーセキュリティに関して高度な能力を持つ人材が国全体で７０００人ほど必要だといわれており、現状では４０００人いる。日本でも最低１０００人は必要といわれているが、まだ２００人程度」だという。

このような状況で、全国の小・中学校・高校でＩＣＴ教育を実践して本当に大丈夫なのだろうか。学校に高速通信網と１人１台のパソコンが整備されれば、生徒たち１人ひとりの学習や生活のデータが見える化され、グローバルな学習が可能となる。だがそれは裏を返せば、生徒たちが世界からのサイバー攻撃の脅威にさらされることも意味している。であれば、ＩＣＴ教育の推進とサイバー攻撃対策とは一体ですすめねばならないのではないか。文部科学省では16年９月から「教育情報セキュリティ対策推進チーム」を設置し、今後の学校におけるサイバーセキュリティの考え方について検討を行い、各自治体に「教育情報セキュリティーポリシー」を策定するよう促してきた。が、当の自治体にサイバーセキュリティの知識やノウハウがなく、人材も不足している現状では心もとない。

事態打開のためには、やはり地道な人材育成しかないだろう。たとえば東京工業大学は16年４月、野村総合研究所、楽天、ＮＴＴ、産業技術総合研究所、内閣サイバーセキュリティセンターと協力して「サイバーセキュリティ特別専門学修プログラム」を立ち上げた。前出の田中教授によると、これは「大学院生を対象とした副専攻相当のもので、サイバーセキュリティに関する理論と実践の両面を学ぶことができる」そうだ。現状では本格的にサイバーセキュリティを学べる大学は日本に数えるほどしかないというが、このような教育を受けた専門人材が、将来のＩＣＴ教育現場をサポートしていくことを期待したい。