特集の視点

IoT時代のサイバー・セキュリティー
―今そこにあるリスク

PROVISION 88号 コンテンツ・リーダー
日本アイ・ビー・エム株式会社
理事
セキュリティー事業本部
セキュリティー・サービス・デリバリー担当
我妻 三佳 Mika Agatsuma

ITの歴史を振り返ると、コンピューター・システムがこの世に出現したのが1960年代、さらに1990年代にはPCとインターネットという画期的なツールが、ビジネスから学術、行政、政治、ひいては一般個人の生活にも多大な影響を及ぼす変革をもたらしました。その当時から“ハッカー”と呼ばれる特殊スキル保有者が存在し、ハッキングという英語に私たちもコンピューター技術の負の意味合いを感じとったものです。今日誰もが被害に遭遇しかねないセキュリティー・リスクの存在と実態を、当時予想できた人がどれほど世の中に存在したでしょうか？

人類は、技術の進歩によってもたらされる利便性を享受することに貪欲になる余り、インターネットに接続された人々のモラルを疑うことを忘れ、予測できない危険の存在を無視しているかのようです。リスクが顕在化したときに改めてその存在を認めざるを得ず、己の危機回避能力のなさを悟り、今度は国の制度や法律が追いついていないと大騒ぎになるのです。現在日本のサイバー・セキュリティー問題はまさにこの段階にあります。社会基盤の主要な部分がインターネットと密接かつ不可欠なつながりがある以上、20世紀に後戻りもできず、大きな代償を払わざるを得ないケースが日々発生していることは否定できない事実です。今後もこの問題はテクノロジーだけでは解決できず、いわば私たちは、“終わりなき戦いの道”に足を踏み入れたと言えるでしょう。

サイバー・セキュリティー問題は、実は2000年代の前半からすでに顕在化していました。米国政府機関のシステムに中国から大量のサイバー攻撃が仕掛けられ、大量の政治や外交、軍事関連の機密情報が流出し、外交問題にまで発展しました。当時日本の政府関係者や政治家、民間企業は、将来こうした問題に直面することになるとは思いが至らず、国外の特定国家間の騒動に過ぎないと考え、国内では警鐘すら鳴らされませんでした。

当時からこの問題の重要性を察知し、さまざまなセキュリティー対策や人材育成など、今日大きな課題とされているセキュリティー上の各種問題に先取りして取り組んでいれば、日本の情報セキュリティー事情はもっと違ったものになっていたかもしれません。日本は第二次世界大戦後、他国との紛争に直接関わることなく70年以上の平和を謳歌してきました。セキュリティーなどの物騒な話には巻き込まれたくない、自分たちの身に起きる

はずがないという“逃げ”と“願望”が社会的な風潮として蔓延し、この深刻かつ重要な問題から目を背けてきました。

それに反して技術の進歩は、日本社会にも急速にサイバー・セキュリティー問題を顕在化させています。インターネットには国境がなく、通信回線に接続されていれば対象とする相手に容易につながることができ、追跡を逃れるためのさまざまな方策が存在しネット上で共有されています。さほど深い知識・経験や、技術的なスキルがなくても、容易にサイバー攻撃を仕掛けられる世の中になっているのです。昨今は金銭的な利益を享受するための攻撃が後を絶ちません。また、国家間紛争やテロの手段として、ネット上の攻撃が行われる時代になっています。技術があっても満足いく正業には就けない経済的に発展途上段階にある国の人間が金銭的なメリットを享受するために攻撃に加担しているのかと思いきや、2015年4月にオランダで開かれた「サイバー空間に関するハーグ国際会議」に参加した際に、世界はもはやこのような単純な構図では語れないことを悟らされました。

実は先進国以上に深刻なのは、経済発展の途上にあるアフリカや中南米などの発展途上国なのです。彼らの社会基盤の発展は、私たちとは考え方も展開もまったく異なります。彼らにとっては、整備された道路網や近代的な建物、鉄道などよりも、まずは全国津々浦々でインターネットにつながるための通信インフラを整備することが、社会インフラ整備の最重要課題です。インターネットは、先進国並みの経済的なメリットをいち早く享受するためのいわば経済発展のための必須基盤であり、そこでサイバー・セキュリティー上の問題に巻き込まれ経済的な損失や影響を被ることは、先進国以上に深刻な打撃となります。「インターネットは、自由、オープン、かつ安定したインフラですが、同時に参加する側にはモラルと責任が伴うことを、全世界で共有すべきである」と会議で主張したあるアフリカ代表の言葉が大変印象に残っています。人権保護とプライバシーの問題に加えて、インターネットが犯罪やテロの温床とならないための法的な枠組みや国際的な協力関係の整備は、ハーグ国際会議においてもさまざまな事例が発表されるなど、着実に進展し、成果も上がっています。この世界的な取り組みにおいて、今後は日本がリーダーとしての役割を果たせるようになることが期待されています。

2012年のロンドン・オリンピックは、サイバー・セキュリティー時代の幕開けと重なり、インテリジェンスとテクノロジーを駆使した可能な限りのセキュリティー対策強化で対抗し、期間中テロを含めた事故をゼロに抑えた大会でした。2020年の東京オリンピックはIoT時代のオリンピックとも言われ、さらに多様で複雑なセキュリティーの脅威に挑むこととなり、日本の底力が試される大会となります。4年前のPROVISION73号のセキュリティー特集の際には、積極的にセキュリティー対策を追求する企業や組織の存在はまだ小数派でした。しかしながら、ここ数年に国内で発生したさまざまなセキュリティーの問題は、日本でもセキュリティー・リスクが避けて通れない課題であることを実証したと言えます。また、東京オリンピックという世界的に注目度の高いイベントを控えていることも、意識を変化させてきている大きな要因となっています。

今号の特集が、いわゆる“終わりなき戦いの道”に踏み込んだセキュリティーの現状と、より身近に迫っているセキュリティー問題の理解を深めるための一助となれば幸いです。