掲載日時: 2019-06-12 06:00:00

東京五輪後の日本のIT世界--セキュリティ対策の導入は「免罪符」

2020年以降の日本の経済情勢やITの動向を占ってきたが、今回はサイバーセキュリティの観点から過去の経緯も含めて分析してしてみたい。

著者：武田一城 (ラック)

URL：https://japan.zdnet.com/article/35138128/

本連載「企業セキュリティの歩き方」では、セキュリティ業界を取り巻く現状や課題、問題点をひもときながら、サイバーセキュリティを向上させていくための視点やヒントを提示する。

前回と前々回の記事では、東京五輪のような国際的なビッグイベントの後に、その前までの好景気に対する一定の反動が生じるも、その確率は減ってきていることを取り上げた。その一方、現代のインターネット社会ではビッグイベント開催期間に合わせたサイバー攻撃のリスクの高まりに対して企業の危機意識は高まっておらず、それが非常に大きな問題となる恐れがあることについて述べた。今回は、日本のセキュリティ市場の成り立ちやその傾向をひも解きながら、この問題をもう少し深掘りしていきたい。

事件や事故で拡大したセキュリティ業界

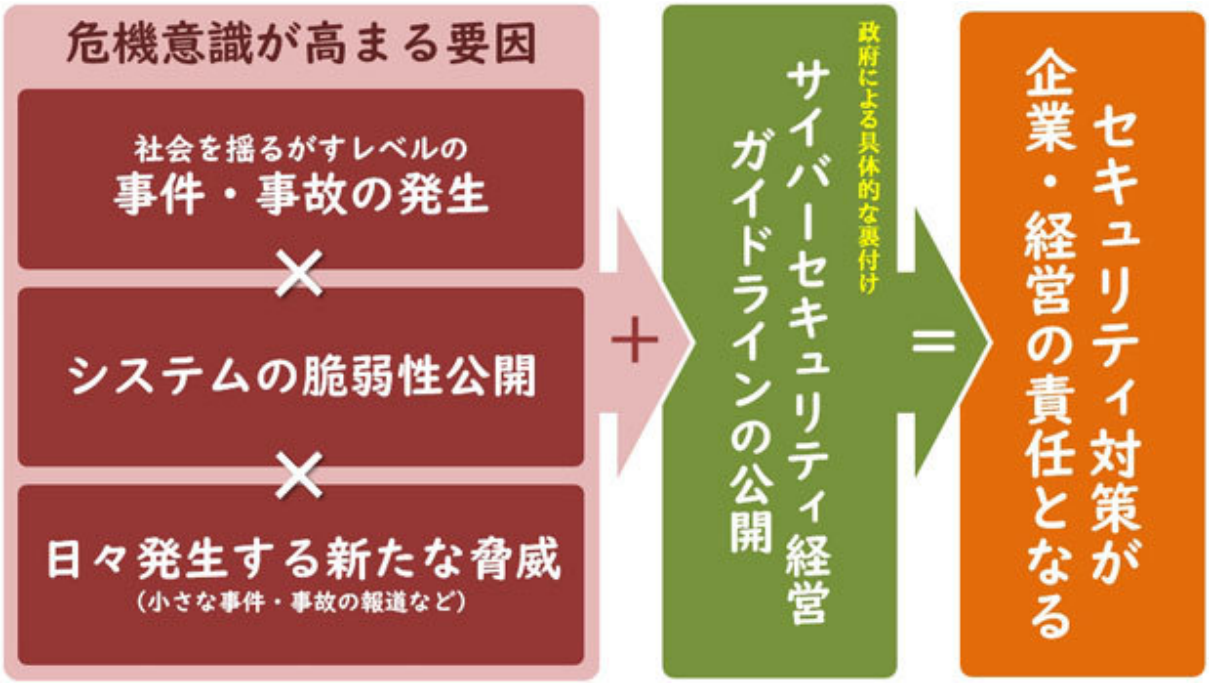
戦後、日本は奇跡と呼ばれるレベルの高度経済成長を遂げ、世界第2位の経済大国になった。しかし、それは過去の話となり、この20～30年はほとんど成長していない。成長著しい新興国には、大航海時代のスペインやポルトガル、産業革命期の英国もかつてそうだったように全盛期を過ぎた国家に映るだろう。その低成長の日本においてサイバーセキュリティ業界は、数少ない成長分野であり、日本において、直近10年ほどで最も拡大した分野の一つだろう。

なぜ、セキュリティ分野がこのような拡大を遂げられたのだろうか。まず、セキュリティだけでなくIT分野全体が好調だった。そのほかにも幾つか要因はあるが、セキュリティ市場が拡大する最大の要因は「大きな事件や事故」の発生だ。この10年間に多くのサイバー攻撃などによる事件や事故が発生した。特に大きかったのは、2011年の国内防衛産業を狙った標的型攻撃事件、そして2015年の日本年金機構への不正アクセスによる情報流出だ。これらの事件や事故により、一般の人にもサイバー攻撃の脅威がごく当たり前のこととして認識されるようになった。

脅威の認識が一般化すると、拡大スピードはどんどん加速する。一定レベルの危機意識を持った企業や組織では、直接的な事件や事故の報道はもちろん、OSやミドルウェアの脆弱性が発見されただけでも、その都度「ウチは大丈夫か？」という質問が経営者や管理者からシステムの現場に多く寄せられるようになる。もちろん、それらの全てが大きなリスクに直結するものではないが、質問や確認が繰り返されることで、サイバー攻撃の脅威とその対策検討が組織の中の日常風景となる。

さらに、経済産業省とその外郭団体である情報処理推進機構（IPA）から2015年に公開された「サイバーセキュリティ経営ガイドライン」が決定打となった。ここでいう“決定打”とは、このガ

イドラインに「サイバーセキュリティは企業経営者がリーダーシップを持って対処する」という記述だ。つまり、万一サイバー攻撃を受けた場合、その責任は経営にあるという事実を政府が公式に表明したことになる。これによって、経営者ののど元にセキュリティ対策の責任が突き付けられた格好となった。正直、このガイドラインに書かれた内容はごく当たり前なものばかりだが、公開のタイミングを含めて非常に意義のあるものになった。



今日の“セキュリティブーム”が生じた背景

このように、企業や組織がサイバー攻撃による事件や事故、脆弱性の報道などによって危機意識を持ちはじめたところで、政府から被害時の責任が経営者に属するということが明言された。この様な経緯で、システム部門の危機意識から10年ほど遅れて企業の組織全体と経営が動いたということになる。そして、経営者の具体的な次の一手は、サイバー攻撃の脅威が自社に及んだ場合に備えたセキュリティインシデントのための対応機能である「Computer Security Incident Response Team（CSIRT）」の設置だった。さらに、それを束ねる役割を持った「最高情報セキュリティ責任者（CISO）」を任命することも併せて一般的となった。その動きは、ここ数年の日本シーサート協議会（NCA）の会員数の推移を見ると一目瞭然だ。

リスクベースのセキュリティ対策ができない日本

そして、現在まで2011年の標的型攻撃事件に端を発したセキュリティ分野の拡大が10年近く続いている。実は、このような事件・事故による拡大は今回が初めてではなく、その前から何度も繰り返されてきたことだ。例えば、2005年に個人情報保護法（2017年に改正）が施行された際も、情報漏えいすると企業の代表者が逮捕されるという触れ込みで、2000年代前半に一時的なセキュリティブームが起きた。それ以前にも規模の大小はあるもの、事件や事故が起こるたびに何度か同じような状況が繰り返された。

だが、それらを経ても日本企業はリスクベースのセキュリティ対策を定着させることができなかった。本来なら企業全体のリスクを定量的に把握し、守るべき情報が何かということや、その重要性を規定した上で具体的なセキュリティ対策を施すべきだ。そして、その重要度や対策は企業や組織によって、その対策はそれぞれ異なるはずである。

ところが、現在の企業や組織のセキュリティ対策では、単純にCSIRTの設置とCISO任命のブームが起きているに過ぎないとも言える。付随的に、それらを機能させるためのセキュリティ人材育成ブームが起きたのは良い傾向だが、名ばかりのCSIRTを組織し、その担当者と責任者のCISOを決めるという手段が目的となってしまった「CISRT/CISOブーム」でしかないのだ。2020年の東京五輪を控えた今日に及んでも、自分たちにどのようなリスクがあり、そのために必要なセキュリティ対策について議論ができているところは、一流と言われる企業でもそれほど多くはないだろう。

このことは、2020年以降の日本のITやサイバーセキュリティを考える上で、非常に重要なポイントとなる。もし、政府関係者などの努力が実を結び、東京五輪に大規模なサイバー攻撃などが発生しなければ、今回の「CISRT/CISOブーム」は一過性のものとして終息してしまうからだ。そうなれば、次のビッグイベントやサイバー攻撃事件が発生し、顕在化するまで、日本のセキュリティ対策は停滞することになる。

サイバー攻撃による事件や事故は、一般の人々が想像するよりもかなり多く発生している。しかし、その多くは公表されない。個人情報の漏えいは、個人情報保護法で公表が義務付けられているために公表されているが、企業にとってもっと大事な機密情報などが漏えいしても公表する義務はない。そもそもサイバー攻撃を受けていることに気づかないことの方が多い。そのため、その間ずっと重要な機密情報が垂れ流される最悪の状況が続いてしまうのだ。

セキュリティ対策の導入は「免罪符」

なぜ、毎回このようになってしまうのだろう。その理由は非常に厳しい現実にある。日本におけるセキュリティ対策の本質とは、ほとんどの場合「免罪符」なのである。免罪符とは、「贖宥状（しょくゆうじょう）」とも呼ばれる。中世の欧州にカトリック教会が発行した罪の償いを軽減するとした証明書だ。元々は、十字軍の遠征に従軍できない代わりの寄進が起源というから、実に900年以上の歴史がある由緒正しいものだ。

しかし、それは「寄進」という名目の金銭で教会に罪を許してもらうことだ。その免罪したことの証明として、免罪符が発行されたのだ。つまりは、「お金で買える天国（または来世の幸福）へのチケット」である。宗教論などで異なる見方もあるだろうが、普通に考えれば、その金銭で保障された幸福というのは、非常に怪しいものと言って良いだろう。

このように、残念ながら現在の日本のセキュリティ対策は、「高価なセキュリティ対策のためのツール」を免罪符として購入しているようなものだ。その理由は既に述べたが、端的に言うとその企業や組織にとって、何が発生したら困るかということがベースになっていない対策だからだ。企業や組織の置かれた環境はそれぞれ異なり、同様にリスクも異なる。だからこそ、「リスクとは何か」を定義し、具体的な対処方法を考え、対策を吟味する。このようなリスクベースのセキュリティ対策を実施することこそ、最も重要であり、基本中の基本でもある。

ブームに乗ることが目的化している日本のセキュリティ対策では、具体的なリスク因子や懸念される影響、対応策をどうするのかなどがあまり考慮されず、当然検証や精査もされない。また、このリスクというのは定常的ではなく日々変化する。顕在化していないリスクが新たに見つかった場合にどうするのかといったリスク全体のマネジメントの整備も非常に重要だ。このような本質的に“やらなければならないこと”と免罪符の購入でしかない現実の間には大きなギャップがある。

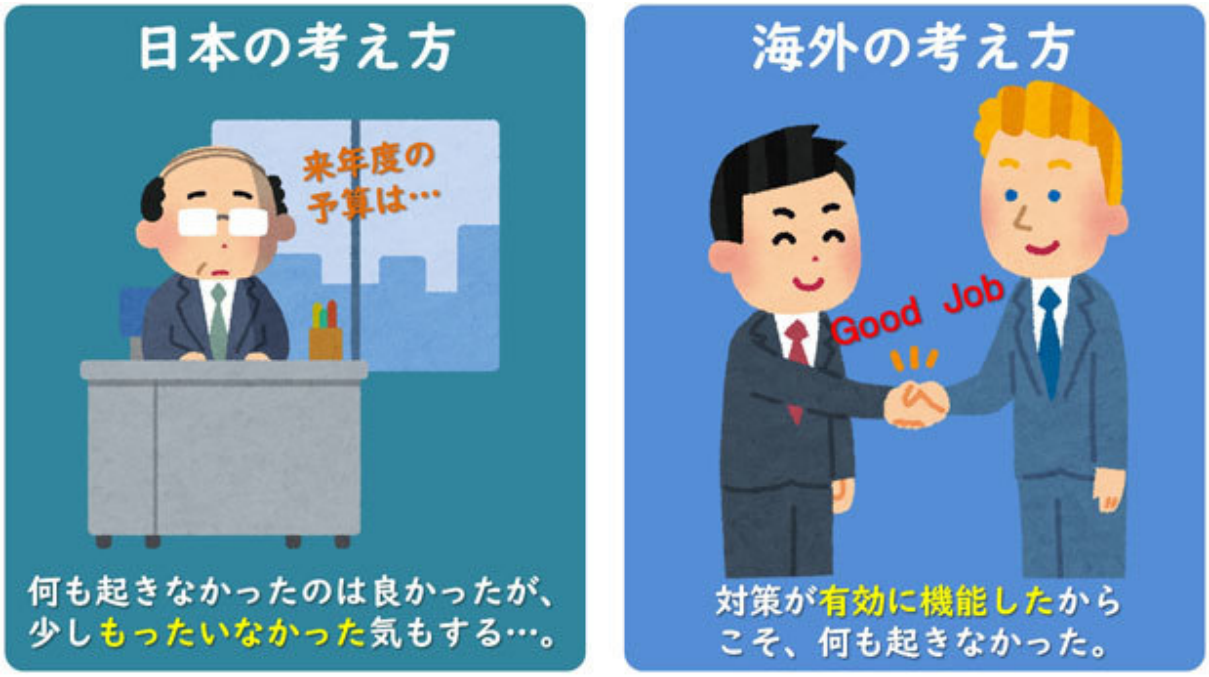
リスクに対する海外と日本の考え方の違い

改めて東京五輪後の日本のセキュリティがどうなるのか仮説を述べたい。もし東京五輪期間やその前後に大きな問題が発生せず、大会が成功裏に終わった場合、日本のセキュリティ対策の熱は一気に冷めるだろう。そして、何らかの被害が必ず発生すると対応策を尽くした人は、「嘘つき」呼ばわりされてしまうかもしれない。脅威を可視化し、周囲を説得し、セキュリティ対策予算を確保して陣頭指揮を執り、何の被害も出さなかった功労者であってもそうだろう。

仮に何も起こらなかったのが、エンジニアの現場での努力によってギリギリの所で脅威を防御によって実現したとしても、状況はあまり変わらないだろう。残念ながら、経営者を含む一般の人の中には、「そもそも対策なんていらなかった」「せっかく対策をしたのに損をした」と考える人々が一定数存在する。サイバーの脅威は、人間の目には見えないからだ。

このようなことは、日本以外ではあまり見られない特徴的なものだと言われる。諸外国では、「対策が有効に機能した」と単純に喜ぶからだ。対策を考え、指揮した責任者や担当者には、昇格や特別ボーナスなどの報奨もあるだろう。しかし日本の場合は、なかなかそうはならない。せいぜい労いの言葉が関の山だろう。その後は、良くて現状維持であり、大きなイベントが終わったということで体制の縮小や事実上のお役御免ということもあり得るのだ。

このリスクと対策おける考え方の違いの背景には、日本が本格的な外国勢力の侵略などを受けたことがないという歴史が大きく影響しているだろう。また日本は、世界的にも多くの自然災害を受ける可能性が高いエリアであるものの、日本の自然環境のもたらす恵みは、災害のリスクを上回る。人間にとって生活する上で欠かせない温暖な気候や豊富な水資源といった絶対的なメリットを提供してくれる。もちろん災害時には何らかの被害を受けてしまうが、ある程度辛抱すれば被害が回復してしまうことも少なくない。これはあくまで私見だが、日本は人間に都合の良い環境に恵まれ過ぎていることで、日本人自体がリスクに対して鈍感な平和ボケが常態化し、日本人の特徴の一つになってしまったのだと思われる。



リスクとその対応における日本と海外の考え方の違い

もちろん、東京五輪で大規模なセキュリティ事件や事故が起きた方がいいと言うつもりはないが、何も起きなければ、人々のセキュリティへの関心は薄まり、結局は別の大きな事件や事故が発生してしまうかもしれない。どうにも「痛しかゆし」という状況から日本はなかなか抜け出せそうにない。それでも、東京五輪を契機にリスクベースのセキュリティ対策やマネジメントの必要性を理解し、そのための投資意欲が根付く時代になることを切に願うしかない。

次回は東京五輪後のIT世界において、予想される状況や、今後期待できそうな分野などについて述べていきたい。

武田 一城（たけだ かずしろ）
株式会社ラック
1974年生まれ。システムプラットフォーム、セキュリティー分野の業界構造や仕組みに詳しいマーケティングのスペシャリスト。次世代型ファイアウォールほか、数多くの新事業の立ち上げを経験している。web/雑誌ほかの種媒体への執筆実績も多数あり。 NPO法人日本PostgreSQLユーザ会理事。日本ネットワークセキュリティ協会（JNSA）のワーキンググループや情報処理推進機構（IPA）の委員会活動、各種シンポジウムや研究会、勉強会での講演なども精力的に活動している。