セキュリティベンダーの重要性と影響力の増大

著者：樋崎 充、大塚 悠也

AI、IoTなどのテクノロジーの進展に伴いセキュリティは、社内システムを守るものだけではなく、顧客への製品・サービス提供においてもキーファクターとなる。本稿では、サイバーセキュリティが経営にどのような影響を与えるのか、少し先の未来を想像した上で論じてみたい。

欧米に遅れる日本の経営

近年、サイバー攻撃が増加している。パソコン、インターネットが普及し始めた当初は各種システムへの侵入目的は腕試し、興味本位が主だったが、徐々に金銭や企業の機密情報奪取へと目的が移りかわっている。一説には、セキュリティ産業のグローバルの市場規模が8〜9兆円弱に対し、サイバー攻撃のブラックマーケットは12兆円を超えるともいわれる。さらには水面下では国家間のサイバー攻撃も激しさを増しているといわれている。そのため政府は、サイバー防衛隊を2023年度までに約500人と現状の3倍超に増やすことを計画している[1]。しかし、米国のサイバー攻撃に対応する部隊は約6,000人、予算は約2.2兆円（2017年、日本の予算は632億円）、北朝鮮のサイバー部隊は約7,000人、中国は数万人規模ともいわれ文字通り桁が違う状況である。

以前はパソコンのセキュリティを担保することが中心であったが、スマートフォンやIoT機器の普及に伴いさまざまなデバイスでセキュリティ侵害のリスクが増加している。総務省も家庭用のIoT機器の調査および利用者への注意喚起の取り組みを2019年2月から開始した。

企業においてもさまざまなサイバー攻撃による被害が起きている。世界150カ国・地域でデータを暗号化し身代金を要求するランサムウェア（WannaCryなど）や航空会社の経理担当者に向けた詐欺メールによる金銭奪取などが記憶に新しい。

サイバーセキュリティはもはや経営の問題として捉えなおすべきだという論調もある中、日本はいまだ意識が低い状況にある。経営との橋渡しが期待されるCISO（情報セキュリティ最高責任者）の任命率も欧米と比較すると20ポイント以上の差があり、専任のCISOも少ない（図表1参照）。また、日本のCISOに求められるものは技術・スキル面に片寄っており、経営との橋渡しや事業目標との整合を期待する向きも少ない（図表2参照）。

サイバーセキュリティは自社の防衛とともに顧客へセキュアな製品を届けるという守りと攻めの両側面があり、テクノロジーの進展に伴い両側面ともますます強化する必要性が高まる。

守りを重ねる日本、重要な資産を守り抜く米国

これまで日本の企業は、被害を発生させないためにも「防御」することに注力してきた。その結果、さまざまな製品を組み合わせた多層防御が築かれている。ファイアウォールを設置し、アンチウイルスソフトを入れ、ソフトウェアにパッチを当てるといった対策を行い、さらにIPS（不正侵入防止）やWAF（WEBアプリケーションに特化したファイアウォール）などのセキュリティ製品を重ねて、複数の防御策を組み合わせている企業が多数存在する。

これに対し米国では多層防御にとどまらず、侵入されることを前提とした上で、対処するという考えが浸透している。具体

1：2019年2月20日付 日本経済新聞 「防衛省、サイバー反撃で専門人材」，https://www.nikkei.com/article/DGKKZO41466640Z10C19A2MM8000 ［2019年3月25日閲覧］

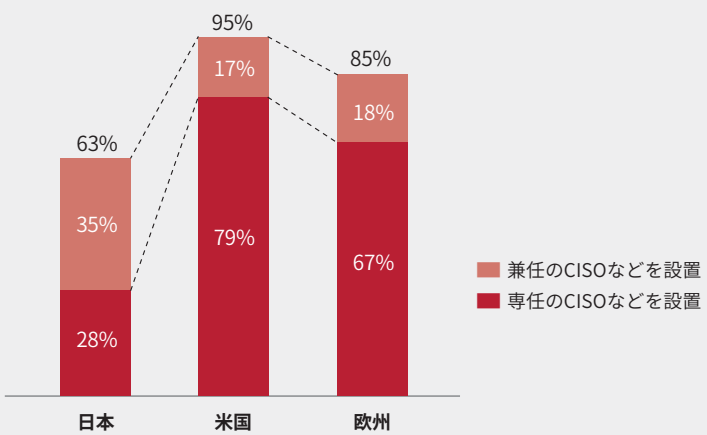
樋崎 充（といざき・みつる）
mitsuru.toizaki@pwc.com

PwCコンサルティング、Strategy&のパートナー。約15年にわたり、IT関連企業、総合電機メーカー、電子部品メーカー、製薬会社に対し、事業戦略、組織戦略、M&A戦略、SCM戦略の立案および実行支援などのプロジェクトを手がけてきた。

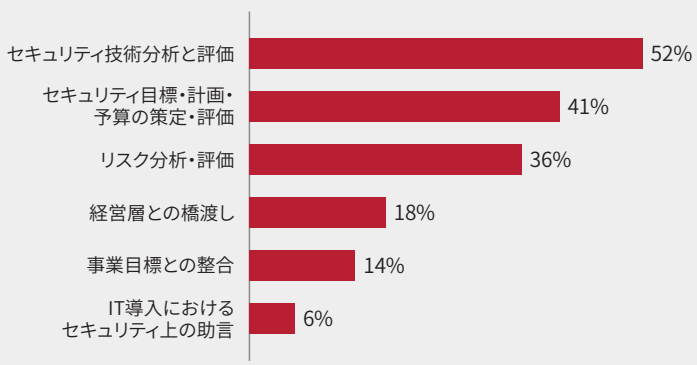
大塚 悠也（おおつか・ゆうや）
yuya.otsuka@pwc.com

PwCコンサルティング、Strategy&のシニアアソシエイト。事業会社を経て戦略コンサルティングに約7年従事。ハイテク業界を中心に製造、サービス、金融など幅広いクライアントに対する、全社、事業戦略の立案および実行支援などのプロジェクトに取り組む。

図表1
CISO任命率



図表2
日本において重要視されているCISOの役割



出所：IPA「企業のCISOやCSIRTに関する実態調査2017」（小数点以下は四捨五入）

的には、組織において守るべき資産（システム・データなど）を「特定」し、そのための「防御」策を施し、防御策が突破された場合に「検知」し、隔離などの「対応」を行い、「復旧」させるという考え方である。これは2014年に重要インフラ向けのベストプラクティスのセキュリティ対策フレームワークとして米国国立標準技術研究所（NIST）が提示をしたものであるが、重要インフラだけではなく、どの企業においても取り入れられる考え方である。

「攻められないためにも多重の守りを重ねに重ねる日本」と「攻められても重要な資産だけは守り抜くことを考える米国」。恒常的にリアルな戦争に直面し、まことしやかに国家間でのサイバー戦争を繰り広げているといわれる米国に比べると、言語のバリアーなどもあり、まだサイバー被害が比較的少ない平和な日本との間で思想の違いがあらわれているように思われる。

現実的には、完璧に防御しきることは困難であるため、攻められる/侵入されることを前提に対策を考える必要があるだろう。日本企業も重要な資産を守り抜く発想に切り替えていく必要がある。しかし、重要な資産を守り抜くためには、そもそも自社の資産を把握しきることが必要であるが、自社の守るべき資産を把握しきれていない企業が大半ではないだろうか。特に日本企業は外部のシステムベンダーにさまざまなシステム構築を依頼しているため、ベンダー各社は構築部分を把握しているが、発注企業側が全体を把握しきれていないなどということは往々にしてある。Strategy&で重要インフラを運営する企業を含む複数社に独自にヒアリングしたところ、資産を把握し、どのシステムが攻撃されるとどこにどれだけ影響があるかをサイバーセキュリティの観点から検討しきれている企業は、皆無に等しかった。

2019年は20カ国・地域（G20）首脳会合、ラグビーワールドカップ、2020年には東京オリンピック・パラリンピックなどと国際イベントが目白押しであり、ハッカーにとっては自身の攻撃能力をアピールする絶好の機会である。2012年のロンドンオリンピックでは、電力システムへのDDoS攻撃（分散型サービス妨害攻撃）などがあり、2016年リオデジャネイロオリンピックでは、情報漏洩が発生し、2018年平昌オリンピックでは、不正プログラムなどによりITシステムが停止している。また、近隣の複数のスキーリゾート施設でもゲートとリフトの操作を行えなくなったなど、オリンピック会場だけではなく、その周辺や関与した関係者など、さまざまな場所・人が狙われた。

無差別な攻撃の中に、政府機関、公共施設、研究・教育機関、交通機関、ライフライン、化学・石油などの重要産業やその取引先を狙った一点突破の攻撃が今後1〜2年で行われる可能性が高まっている。さらには、最悪のシナリオとして想定されるのは2020年を境に日本語を活用した標的型攻撃の精度が高まることである。今までは同じ攻撃を行うなら、経済大国とはいえ日本語という言語バリアーを有する日本に対してサイバー攻撃を行うよりは、英語を使用して欧米中心に標的型攻撃を行う方が確率論的には攻撃者にとって効率的であったが、東京オリンピックなどを契機に経験を積んだ攻撃者が日本語のバリアーも突破することも想定されるのではないか。今後、日本においても深刻化するであろうサイバー攻撃には、侵入を前提とした上で、本当に守るべきものは何かを検討すること、そして、まず資産の把握から始める必要があるだろう。

セキュアな製品を届けるという視点

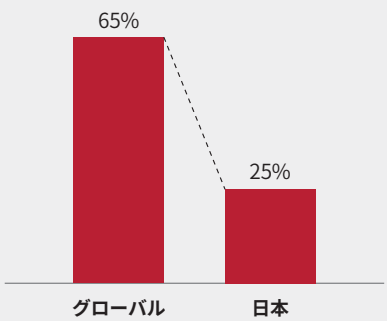
一方、セキュリティは自社防衛だけでは足りず、顧客への製品提供でも必須になっていく。

近年消費者の嗜好が多様になる中、モノを売って終わりではなく、顧客を継続的にサポートしながらその満足を追求するいわゆるas a Serviceモデルへとビジネスを転換しようとする動きが各社に見られる。そのための効果的な手段としてコネクテッド、主にインターネットを介して繋がり続けるサービスが模索されている。

しかし、インターネット空間と繋がるということは、一方でサイバー攻撃の脅威にもさらされ続けていることになる。近年では、さまざまなデバイスがコネクテッド/繋がる製品として発売される中、同時にハッキングの事例も増え続けている。

例えば、2015年には米国のセキュリティ研究者が遠隔からカーナビシステムを経由して自動車へ侵入。エンジン制御などに関わるシステムを不正に作動させる実験に成功した。この結果、開発自動車メーカーは140万台のリコールを行う必要

図表3
開発におけるセキュリティアセスメント実施企業の割合



出所：PwC「グローバル情報セキュリティ調査2017 Vol.3：IoTの可能性を探る」

が生じた。

また、同じく米国での医療機器ハッキング事例として、体内に埋め込んだペースメーカーで取得したデータをサーバーに送信し、ペースメーカーのファームウェアのアップデートを行う機器がハッキング可能であったケースが存在する。

製品・サービスをコネクテッドにすることは、上記のようなリスクがあることも理解しなければならない。この点、PwCのグローバルセキュリティ調査によると、研究開発フェーズからサイバー攻撃の脅威を多角的に分析し、当該コネクテッドな機器に求められるサイバーセキュリティ要件を明確にした上で、次工程の製造フェーズに受け渡すといった綿密な設計（セキュリティアセスメント）をできている日本企業は海外に比べて著しく低いことがわかる（図表3参照）。

一部の大企業では、このようなリスクに対処するため、製品の開発から販売後のアフターフォローまでをセキュリティの観点から一貫して責任を持つ社内組織（PSIRT）の設置を行う企業も出てきているものの、実運用に至っている企業は殆どなく、緒に就いたところである。

拡大するセキュリティベンダーの影響力

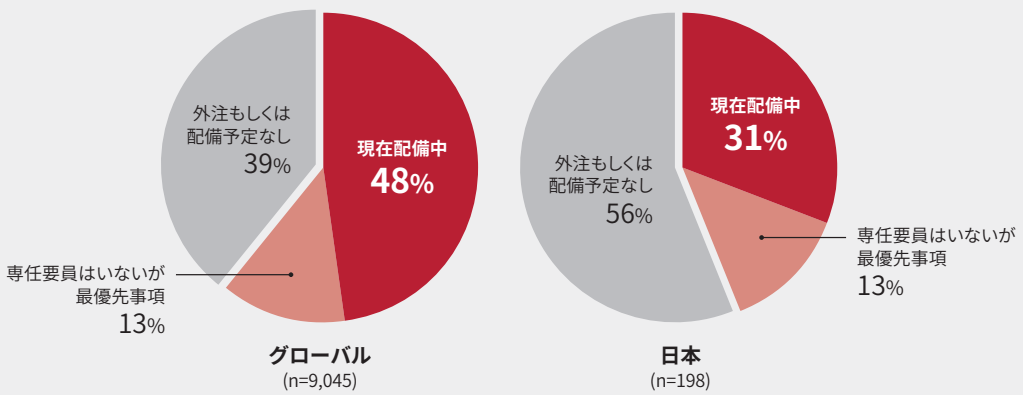
さらに未来に目を向けると、IoTやAIなどが今後進展していくことに疑いの余地はないだろう。コネクテッドカーとして自動車が制御され、スマートホームとして住宅が繋がり、政府や地方自治体も巻き込み街灯、信号、交通監視や各種建物、インテリジェントビルディングなどが繋がるスマートシティーが作り出され、消費者の利便性と生活の質の向上、また行政のコスト削減が果たされていくだろう。

そして、一部の大手企業がセキュアな製品を提供すれば良いのではなく、全ての会社に今以上にセキュアな製品が求められる日がくる。たとえ大手自動車メーカーが、コネクテッドカーに万全のセキュリティ対策を行って発売したとしても、それと繋がる自社製品に万が一にも脆弱性があり、そこからコネクテッドカーがハッキングされたとしたら、社会にも自社にも甚大な被害を及ぼすかもしれない。

大企業・中小企業問わず、自社の製品がさまざまなモノと繋がる世界では、自社の根幹となる業務システムや工場/プラントだけではなく、顧客への提供製品・サービスにもサイバーセキュリティ対策が必須となる。

図表4

社内ビジネス部門をサポートする専任セキュリティ要員を雇っているか



出所：PwC「グローバル情報セキュリティ調査2017 先進的サイバーセキュリティおよびプライバシーの実現」

このような未来に対応していくためにセキュリティベンダーは、各製品にマルウェア[2]が侵入してきた際に悪さの前兆を検知する仕組みを提供していくだろう（当然、侵入されないことが最良ではあるが、100%侵入を防ぐことは不可能に等しい）。彼らは、膨大な数のマルウェアの挙動、振る舞いをデータベース化しており、既知/未知のマルウェア問わず、被害を起こす直接的なアクションよりも前にその予兆を検知し、対処をするための技術を日々ビッグデータ解析により磨いている。自社製品の挙動とこの仕組みを突き合わして異常を検知するためには、セキュリティベンダーが製品の挙動を理解する必要があり、そのためにもログやプログラムや開発過程を公開する必要が出てくる恐れがある。セキュリティベンダーに対し自社の製品を丸裸にせざるを得ない日が来るかもしれない。

これだけでも、十分リスクではあるが、仮にセキュリティベンダーが使用許諾を突然停止したら発売済みの製品が安全に使えなくなってしまう恐れもある。また政府の意向で特定メーカーの通信機器を排除したように諸外国のセキュリティ製品が急に使えなくなることもあるかもしれない。米国系大手ITベンダーがさまざまなデータをおさえたことが各国で問題となっているが、セキュリティレイヤーもまた米国系が強固になると、設計・開発から発売、その後のフォローまで一連の仕組みや製品のログ、プログラムなども実質的におさえられてしまうことになるのではないか。せめてもの対策として国内のセキュリティベンダーを活用することも考えられるが、残念なことに日本のセキュリティベンダーでグローバルスタンダードになれているものはほとんどないのが実情である。セキュリティ製品を思い浮かべていただいた際に、純国産企業が浮かぶ方は多くはいないのではないか。

上記リスクに対処する一つの方法としては、自社でセキュリティ対策を内製化していくことが考えられる。自社製品に最も詳しいのは自社であるため、自社製品の平常状態からの外れ値を異常と規定してマルウェアの異常な挙動を捉えにいくことにより対処ができるかもしれない。

しかし、セキュアな開発を行うための人材確保が今後大き

2：マルウェアとは悪意のあるソフトウェアや悪質なコードの総称。コンピューターウイルスはマルウェアの一種

な問題となるだろう。もともと日本はIT構築を外に発注する傾向にあり、セキュリティにおいても同様である。日本は諸外国と比べても自社専任のセキュリティ要員を確保できていない状態にある（図表4参照）。さらには、数十万人の単位でセキュリティ人材が不足するという試算もある。

平成の時代30年はインターネットとともに急激なスピードで変化した。このスピードは、今後ますます加速していく中、企業の5年、10年先を見据えて、セキュリティを自社のビジネスの中にどのように取り込むべきなのか。今まさに経営者が真剣に考える時期に来ているのではないだろうか。