ZDNet Japan

サイバーセキュリティ人材を育てる

- 「五輪にはボランティアで働けるエンジニアが必要」発言の真意を聞く
- セキュリティ人材の確保、日本と米国やシンガポールでどう違う？
- セキュリティの要の「橋渡し人材」
  -- 経営と現場をつなぐ 2 つのタイプとは？

ZDNet Japan

サイバーセキュリティ人材を育てる

「五輪にはボランティアで働けるエンジニアが必要」発言の真意を聞く

「5 年間で 4 万人のエンジニアが必要 --IT 分野の新業界団体『日本 IT 団体連盟』発足」で新団体の呼びかけ役となった一般社団法人コンピュータソフトウェア協会（CSAJ）会長の荻原紀男氏（豆蔵ホールディングス代表取締役社長）の発言が注目を集めている。

荻原氏は、10 月 9 日に開催された「CEATEC JAPAN 2015」のパネルディスカッション「明日の IT 政策とソフトウェア産業を考える」で「五輪そのものに対して、ボランティアで対応できるエンジニアが必要で、今後 5 年間で 4 万人のエンジニアを育てなくてはいけない」と発言。この発言を巡って、ソーシャルメディアなどで、ボランティアでソフトウェアエンジニアを働かせることに対する批判が上がる一方、ソフトウェア業界の“ブラック”ぶりを浮き彫りにする発言ではないか、といった声すら上がった。荻原氏にこの発言の意図を改めて聞いた。

コンピュータソフトウェア協会（CSAJ）会長 荻原紀男氏

五輪後を見据えた人材育成を議論

――2020 年の東京五輪でサイバー攻撃からの防衛組織として“サイバーディフェンスリーグ”で対応するなどの構想の中でソフトウェアエンジニアをボランティアで働かせるといった発言に多くの批判が集まっている。

その発言に対しては、まったくブレるものはない。前提として考えてもらいたいのは、これからのサイバー攻撃は、まさに戦争を仕掛けられているのと同じだという点だ。

五輪委員会やオフィシャルスポンサーだけでなく、日本の電気やガス、交通といった社会インフラが狙われる可能性がある。国の重要インフラを破壊されるのは、戦争と言わずに何というのか。これは最悪のシナリオであることには違いないが、日本の政府や業界、企業は、それに対する危機意識が低すぎる。

そして、これを守るためのエンジニアが不足しているのは明らかだ。そのためには人材を育成しなければならない。それが 4 万人。今から教育をしなくては間に合わない。だが、国はそれに対して費用を出す計画がない。

新たに設立する日本 IT 団体連盟では、業界がひとつになり、大きな力で国に提言するという狙いがある。まずは、サイバーディフェンスを担うエンジニアを育成するための予算を獲得する。そこで育成されたエンジニアが 2020 年に開催される東京五輪の開催期間中

こちらは、2015/10/16 に公開された記事（https://japan.zdnet.com/article/35071996/）を再録したものです。仕様等は公開時点のものです。

ZDNet Japan

サイバーセキュリティ人材を育てる

の 1 カ月間でもいいから、ボランティアで働くという仕組みを提案した。

――なぜ、ボランティアで働かなくてはならないのか。

メリットがないものに国は予算をつけない。高齢化が進展する日本では、介護士の育成は急務であるのは周知の通り。だが、ここにも予算がついていない。介護士育成に予算がつかないのに、なぜ IT 産業のエンジニア育成に予算をつけなくてはならないのか。

それならば、1 カ月間、国のサイバーディフェンスのために、ボランティアで働いてもらうことで恩返しをするというのがひとつの提案だ。2020 年の東京五輪に役立つエンジニアたちは当然、五輪後もあらゆる企業で戦力として活用される人材になる。2020 年をゴールに考えたものではなく、その先の時代に向けた人材育成という観点で議論していく必要がある。

――ボランティア以外の選択肢はないのか。

国から IT 人材育成のための予算を取るひとつの手段がボランティアであるが、当然、ほかにも考え得ることはあるだろう。ただ、ボランティアといっても、いくつかの手法がある。

先に触れたように、国の予算で育ててもらったことに対して、1 カ月間のボランティア活動で恩返しをするというのもひとつの方法。あるいは、企業が給与を支払いながら、一定期間ボランティアを働くということも考えられる。

ネットワーク関連のイベントとして最大規模を誇る「Interop Tokyo」では、業界関係者や学生がボランティアでイベントの設営に当たってきたという経緯がある。このイベントでは、かつての日本パーソナルコンピュータソフトウェア協会（JPSA、現在の CSAJ の前身）に加盟するソフトウェア企業のエンジニアたち、WIDE プロジェクトに関連する学生たちが手弁当で NOC（ネットワークオペレーションセンター）を設置、運営するといったことも行ってきた。

その中で光ケーブルの敷設作業や融着作業を学んだり、米国人エンジニアから最新技術を学んだりといったこともできた。なかには、こうしたボランティア活動を通じて資格を取得したり、技術認定を受けたりといったこともあった。当時は大学生だったボランティアで勉強していた人が今では教える側に立っているケースもある。ボランティア活動をしながら、学んだり実践したりといったことができる場でもあった。

東京五輪に向けて、エンジニアがボランティアで参加するという取り組みについても、同様の成果を期待できるのではないだろうか。ボランティアそのものが問題ではなくて、人材が不足しているということが問題であることに気が付いてほしい。われわれがやらなくてはならないのは、エンジニアの底上げであり、企業で戦力となるエンジニアの育成。そのための手法を考えていく必要がある。

――ソフトウェア産業そのものが“ブラック化”しているという指摘もある。短期間とはいえ、ボランティアとして働かせることは、それを助長することにつながるのではないか。

そうは思わない。ブラック化といわれる背景にはいくつかの理由がある。そのひとつは、ブラック業界であるという印象を持たせる動きがあることだ。エンジニアは、大手メーカーとソフトウェア企業の取り合いの中にいる。

サイバーセキュリティ人材を育てる

中小規模の SIer（システムインテグレーター）では、新卒が取れない、中途も採用できないという問題に直面している。地方都市にある 10 人規模の SIer ならばなおさらだ。ソフトウェア産業と対峙してエンジニアを獲得したいと思っている企業たちがソフトウェア産業のブラックぶりを吹聴している実態がある。

2 つめには、元請け、下請けによる多重構造がある点。調査をすると「元請けとの打ち合わせは午後 11 時からと言われた」という声が出ていた時期もあった。そうしたことがいまだに一部にあることは理解している。また、こうしたことが極端にクローズアップされているのも事実だ。

だが、このような多重構造は、今後は成り立たなくなっていくだろう。そのなかでは、SIer 同士の合従連衡のような動きも出てくる可能性もある。また、これまで力がなかった 3 次請け、4 次請けといった企業が新団体に加盟することで元請けと対等に話ができるようになるということにもつながるはずだ。

――独立行政法人情報処理推進機構（IPA）が発行した「IT 人材白書 2014」では、給与・報酬に対して「満足していない」「どちらかと言えば満足していない」という回答が 45.3%と半分近くに達している。この点でも正当な給与がもらえていないという業界の課題が浮き彫りになるのではないか。

今は過渡期だと考えている。これから多重構造が崩れていくと話したが、クラウド時代や IoT（Internet of Things、モノのインターネット）時代を迎えて、多重構造はフラット化していくのが自然の流れだと思っている。一部の企業では、これまでのように顧客の要望を聞いて、それを期日通りに仕上げるという体質から脱皮しようとする動きもある。次に何が求められるのかということを知り、先にこちらから提案するといった動きである。これも多重構造からの脱却に向けた動きだ。

また、IoT によってハードウェアとソフトウェアが別々であった時代が終わるとともに、さまざまな業種、業界で IT エンジニアが求められる時代がやってくる。エンジニアはますます不足するのは明らか。そうすれば、自然と給与は上昇する。

今はその入り口にいると判断している。これから日本のエンジニアの給与は上がっていくはずだ。そして、それを加速するためには、エンジニア自らが次に求められるものを提案する仕事へとシフトしていかなくてはならない。日本 IT 団体連盟も、そうした動きを支援していくことになる。

――エンジニアの労働条件を高めるためには、労働組合という手法もあるのではないか。

エンジニアは力を持った人材のことを指す。どんな企業に行っても活躍できる技量を持っているはずだ。そうした業界で労働組合の存在はあわない。

30 年を経て初めて業界がひとつになるチャンス

――日本 IT 団体連盟には、CSAJ と並ぶ代表的なソフトウェア関連団体である情報サービス産業協会（JISA）が加盟を表明していない。

すでに話をしている。私自身は JISA の参加には手応えを感じている。また、ヤフーなどが参加しているセーファーインターネット協会（SIA）が、新たに日本 IT 団体連盟に加盟することになった。今後、総務省

こちらは、2015/10/16 に公開された記事（https://japan.zdnet.com/article/35071996/）を再録したものです。仕様等は公開時点のものです。

サイバーセキュリティ人材を育てる

が管轄する社団法人テレコムサービス協会にも積極的に参加を呼びかけていく。

私は新団体の会長になろうとは考えていない。いや、絶対にならない。設立準備に関わった一般社団法人全国地域情報産業団体連合会（ANIA）会長の長谷川亘氏、全国ソフトウェア協同組合連合会（JASPA）会長の中島洋氏、特定非営利活動法人日本情報技術取引所（JIET）理事長の酒井雅美氏も新団体の会長にはならないと宣言している。

荻原氏は豆蔵ホールディングスの代表取締役社長が本業

色の付かない人を会長に据えたいと考えている。会長になりたいとか、理事にしがみつきたいという気持ちはまったくない。今大切なのは、業界をどう発展させるかということ。そのためには、人材育成も必要であり、海外の企業に打ち勝つための体力や仕掛けも必要。そして、国に対して提言できる力をわれわれの業界として持つことが必要だ。

私は、政策推進のために官学を回りたい。その活動を通じてエンジニアの教育予算を獲得したい。だが、「これをやれ」と言われたら、「はい、わかりました」といって、業界のために役に立つことをしたい。

私は豆蔵ホールディングスの社長を務めているが、新団体の活動が会社の利益に役立つことはひとつもない。サイバーディフェンスを強化しても、豆蔵ホールディングスの業績にはなんら影響しない。

だが、今、30 年の時を経て初めて業界がひとつになるチャンスを得た。このチャンスを生かしていきたいと考えている。海外から要人が来て、日本の IT 産業のトップに会いたい思ったときにどの団体のトップに会えばいいのか、経済産業省や総務省が悩むようではいけない。

今後、30 年かかるのか 50 年かかるのかわからないが、将来的にはハードウェアの業界団体まで含めて、IT 業界団体をひとつにしたい。これは、業界の発展のためにも必要な取り組みだと考えている。

サイバーセキュリティ人材を育てる

セキュリティ人材の確保、日本と米国やシンガポールでどう違う？

NRI セキュアテクノロジーズは 3 月 28 日、企業の情報セキュリティ実態を調べた 2017 年版のレポートを発表した。セキュリティ人材の不足感が強まる中、日本と海外では人材確保に向けた取り組みに違いがみられた。

まず人材の充足状況は、「不足している」「どちらかといえば不足している」の合計が前年比 7.4 ポイント増の 89.5%だった。直近の 4 年間では最も高く、「長らく微増減を繰り返す傾向にあったが、今回は顕著な上昇。経済産業省の『サイバーセキュリティ経営ガイドライン』が企業に浸透しつつあるようだ」（ストラテジーコンサルティング部長の足立道拡氏）としている。

人材の獲得や不足に伴う改善については、30.8%が何もしていないと回答した。一方で獲得や改善に取り組む企業では「社内人材の能力向上」（35.5%）や「中途採用の強化」（20.4%）のほか、「アウトソーシング強化推進」（25.8%）や「属人化の解消」（21.9%）、「業務の機械化・自動化」（19.1%）が挙げられ、採用と業務改善の両面で対応している状況が明るみとなった。

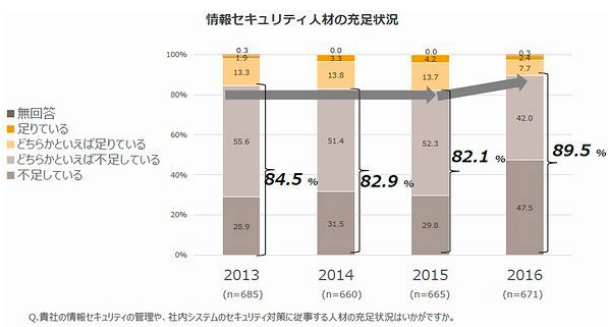
なお、最高情報セキュリティ責任者（CISO）を設置していない企業は 52.5%で、前回調査の 53.4%からはわずかな改善がみられた。

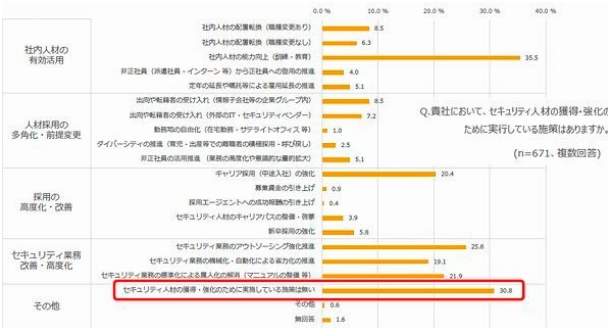
調査は上場と未上場の大企業の計 3000 社の IT、セキュリティ担当者を対象に、2016 年 9 月 5 日から 10 月 14 日までアンケートを行い、671 社から回答を得たもの。今回で 15 回目となる。

海外は給料とキャリアパスの魅力を訴求

従来の調査対象は国内企業だったが、今回は国際比較を実施する目的から従業員 500 人以上の米国とシンガポールの企業にも初めて調査した。回答数は米国が 500 社、シンガポールが 134 社、日本が 474 社（671 社のうち従業員 500 人以上の社数）。

セキュリティ担当者が最も困っていることに、米国では「情報収集や関係者共有」（23.8%）や「経営層への報告」（22.4%）、シンガポールでは「トレンド・他社動向の把握」（32.1%）や「インシデント発生時の緊急対応」（19.4%）が挙げられた。





サイバーセキュリティ人材を育てる

一方、日本（本質問のみ有効回答 456 社）ではこれらの回答割合が 2 カ国に比べて低く、高いのは「専門人材の不足」（43.2%）や「自社対策の遅れ」（19.3%）だった。2 カ国で人材不足や対策の遅れを課題に挙げる回答は、日本よりも少なかった。

海外調査を担当したセキュリティコンサルタントの山本直美氏によると、情報セキュリティを実施するきっかけは、3 カ国とも経営層の指示を挙げる企業が 3 割台だった。日本と 2 カ国との違いでは、2 カ国とも関連法規の改定を挙げる企業が多い一方、日本では少ない。日本が高く、2 カ国が低いものは「外部監査・第三者評価の結果」「内部監査・内部有識者の指摘」だった。また、CSIRT（類似機能の体制を含む）の設置状況は 2 カ国とも 9 割近くに上るが、日本は約 7 割だった。

人材の獲得・強化に向けた実行施策では 3 カ国とも社内人材の能力向上を挙げる回答が目立つ。しかし、2 カ国では「非正社員から正社員への登用」「募集賃金の引き上げ」「キャリパスの整備・啓発」にも積極的なのに対し、日本はいずれも実施率が低い状況だった。

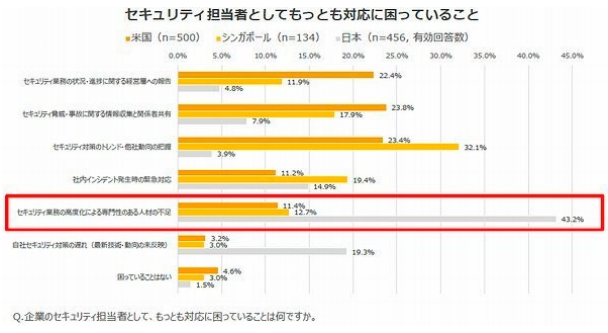
これらの結果について山本氏は、海外では法令対応を契機に、IT 部門や情報セキュリティ部門だけでなく、法務や広報など他部署との連携も含めた情報セキュリティの管理体制が進んでいると解説する。さらに、専門人材の獲得では社内外からの獲得や維持のために、人事部との連携も必要だと述べている。

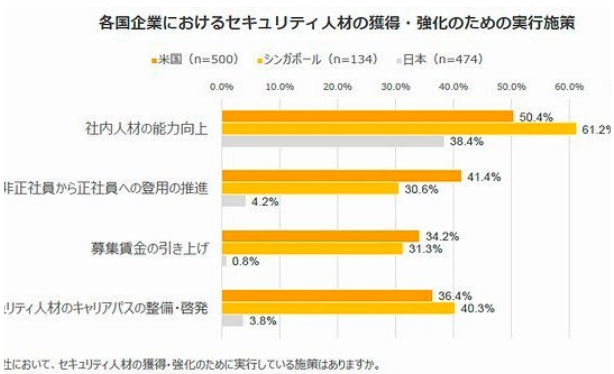
日本がセキュリティ体制を強化するには？

調査結果を踏まえて足立氏は、日本では 2015 年 12 月に公表されたサイバーセキュリティ経営ガイドラインを契機に、経営レベルの情報セキュリティへの取り組みが本格化し始めたが、米国やシンガポールでは日本より先にそうした動きが始まったことから、取り組みが進んでいると指摘する。

特に多くの日本企業は、IT 部門あるいは情報セキュリティ部門が存在していても他の管理部門や事業部門との連携が薄く、セキュリティ事案に関する調整や権限も実施しづらい状況にあるという。サイバーセキュリティ経営ガイドラインで要請されているような管理体制を実現するには、最高経営責任者（CEO）の直下に CISO を設置し、CISO のもとで全社横断の情報セキュリティを推進する統括部門を整備することが望ましいとしている。

「CISO を中心にセキュリティ統括部門が活躍する企業は、セキュリティ人材にとっても魅力的であり、人





こちらは、2017/03/29 に公開された記事（https://japan.zdnet.com/article/35098866/）を再録したものです。仕様等は公開時点のものです。

サイバーセキュリティ人材を育てる

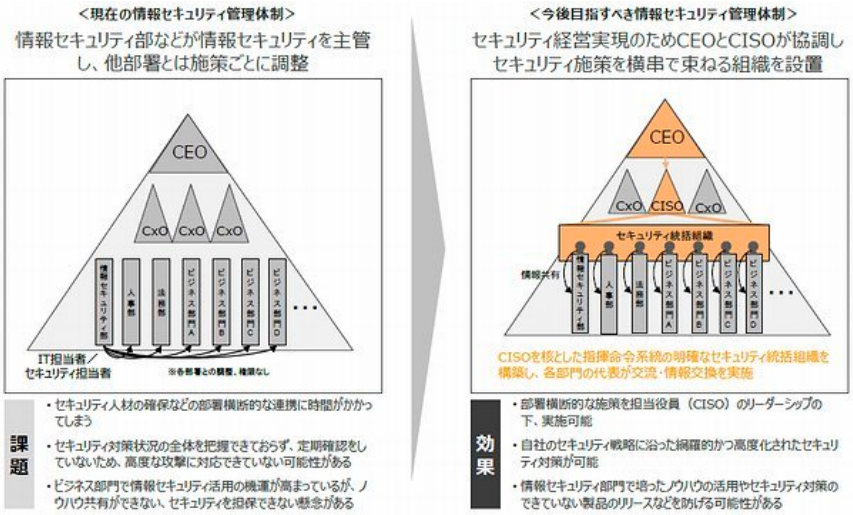
材を確保しやすくなる。一部の企業では人材を確保する狙いから戦略的にも CISO を設置しているようだ」（足立氏）

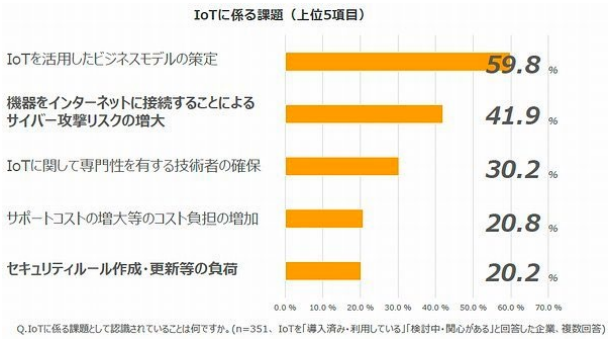
またセキュリティコンサルタントの金子洋平氏は、IoT や人工知能（AI）など企業が新規ビジネスなどで注目するテクノロジへの取り組みが、情報セキュリティの強化に貢献するとアドバイスする。

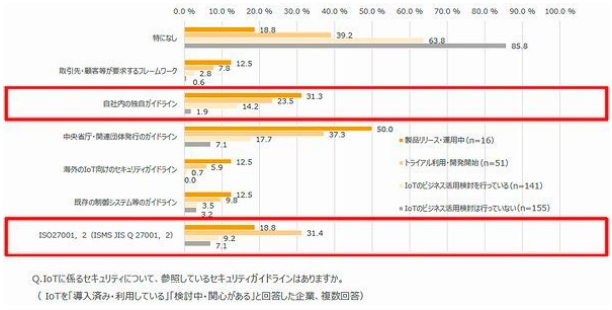
調査では日本企業の約半数が、IoT や AI を「導入済み・利用している」か「検討中・関心あり」と答えた。特に IoT の課題では、「ビジネスモデルの策定」（59.8%）に次いで「サイバー攻撃リスクの増大」（41.9%）が挙げられた。IoT の利用が進んでいる企業ほど、情報セキュリティについては自社独自のガイドラインを設けているという回答が目立つ。

「当初は ISO 27001 を参考にしつつ、利用するほどに国や業界のガイドラインを生かして自社の観点で整備していく傾向にある。IoT のような新規分野は、安全な収益確保に不可欠なセキュリティの知見が少なく、IT 部門やセキュリティ部門が持つノウハウや経験が強く期待される」（金子氏）

足立氏は、「横断型のセキュリティ統括部門を現在の組織構造にうまく当てはめながら整備すると同時に、新規分野では（システムの開発や運用、セキュリティを同時並行的に実施する取り組みである）『DevSecOps』のようなのような新たなアプローチを取り入れていくべき」と話している。







ZDNet Japan

サイバーセキュリティ人材を育てる

セキュリティの要の「橋渡し人材」-- 経営と現場をつなぐ２つのタイプとは？

経済産業省が 2016 年 6 月に公表した「IT 人材の最新動向と将来推計に関する調査結果」によると、セキュリティ人材は 2016 年時点で約 13 万 2000 人が不足し、2020 年には 19 万 3000 人に拡大すると予想されている。中でもユーザー企業の半数近くが、「部署横断、全体的な情報セキュリティ対策の統括者」や「部署内の情報セキュリティ管理者」の不足を挙げている状況だ。

情報セキュリティの統括者や管理者は、対策現場の責任者であると同時に、対策について経営層とコミュニケーションをする「橋渡し役」といえる立場だ。現在では情報セキュリティが企業の経営課題の 1 つに位置付けられているが、経営層が必ずしもセキュリティに詳しいわけでない。一方で対策の現場は、サイバー攻撃など日々の脅威に対応していることから、経営層への報告や提案のためにリソースを確保しづらく、経営層と接する機会が少なければ、コミュニケーション自体も難しい。そこで橋渡し役となる人材が求められている。

政府のサイバーセキュリティ戦略本部が 2016 年 3 月に取りまとめた「サイバーセキュリティ人材育成総合強化方針」の中では、この橋渡し人材層の育成が重点項目の 1 つに挙げられた。内閣サイバーセキュリティセンターが 3 月 13 日にパブリックコメントの募集を開始した「サイバーセキュリティ人材育成プログラム」（案）でも、企業が IT 活用を進めるにあたって情報セキュリティの観点から橋渡し役となる人材の必要性に触れている。

企業は、セキュリティを推進するために欠かせない橋渡し役の人材をどう確保、育成すればよいか――そのポイントについて BPO や IT サービスを手掛ける大宣システムサービス（以下、dss）執行役員 リサーチ＆コンサルティング アナリストの石橋正彦氏に聞いた。

石橋氏は、日本ユニバック（現日本ユニシス）やベリタスソフトウェア（現ベリタステクノロジーズ）、ベリングポイント（現 PwC）でシステム開発や技術サポート、セキュリティ監査などを担当。ガートナー ジャパンでは IT セキュリティとリスクマネジメント分野のリサーチディレクターを歴任し、現在は IT システムおよび IT 人材全体の観点からコンサルティングやリサーチを行う。

石橋氏は、まず IT 人材全般について人数が不足している以上に、IT システムに関する知識と実務経験を併せ持つ人材が足りないと指摘する。加えてセキュリティの橋渡し人材には、経営層と会話ができるコミュニケーション力も要求されるため、これらを踏まえて内部あるいは外部から候補者を選ぶことになると話す。

サイバーセキュリティ人材を育てる

石橋氏によれば、橋渡し役人材の候補には２つのケースがある。１つは、社内の情報システム部門もしくはグループ内の情報システム子会社の出身者であり、もう１つは外部のセキュリティベンダーやSIerの出身者だ。それぞれに強みと弱みがあるという。

まず内部出身者の弱みは、ITシステムの実務経験に乏しいケースがある点だ。効果的なセキュリティを推進するには、ITシステムや業務の知識だけでなく、利用実態に即した対策を講じる必要があり、「特にシステムの企画や製品選定などの経験だけでは、実務を回し切れない。橋渡し役には、サイバー攻撃のパターンや攻撃の手口、被害の内容や対策手法などについて理解と実務経験が求められる」（石橋氏）という。

逆に強みは、社内あるいは企業グループの組織文化を理解し、人脈を生かしやすい点にある。というのも、現在の情報システム部門や情報システム子会社では40代以上のシニア層が最も厚く、経営に近い立場にいる同年代や先輩世代が多いためだ。

「セキュリティではヒト・モノ・カネの経営リソースが不可欠になるので、経営層への提案や交渉、内部調整などの局面において、身近な同僚や年長者とのつながりを生かしやすい」（石橋氏）

一方、外部候補者の弱みや強みは、内部候補者とは逆になる。

強みは製品・サービスなどに直接携わる立場から、ITシステムやセキュリティの知識、経験があり、顧客企業側の実情にも詳しい点ということがある。しかし、内部出身者の立場で経営層とコミュニケーションをしたり、交渉などをスムーズに進めたりするための人脈に乏しいことが弱みになってしまう。

理想的なセキュリティの橋渡し人材の条件は、豊富な知識と実務経験、交渉力やコミュニケーション能力の高さ、幅広い人脈を兼ね備えていることになる。だがビジネス全般において、それら全てを兼ね備える人材はなかなかいない。

石橋氏は、「いずれのケースでも弱みを補完しなければ結果的に孤立し、セキュリティ対策を進めづらくなる」と話す。

まず、内部出身の橋渡し役人材が弱点を補うには、セキュリティ対策の現場の実務を支える人材を確保できるかがポイントになる。

「内部のIT部門に比べて、外部のベンダーやSIerには30代の若い人材が多い。システムの企画経験があれば、外部とつながりを生かして若手に来てもらう。彼らにとっても、セキュリティだけなく、ユーザーの立場でITシステム全体について経験できるメリットがある」（石橋氏）

先述のように、内部出身者は上層部とのコミュニケーションや人脈といった強みを生かすことに注力し、若い世代が実務面を経験できる環境であれば、後継者の育成にもつながりやすい。また、内部出身者が情報セ

サイバーセキュリティ人材を育てる

キュリティを統括することで、企業がセキュリティレベルを維持しやすいという。

一方で外部出身の橋渡し役人材が弱点を補うには、「最高情報セキュリティ責任者」（CISO）や「最高セキュリティ責任者」（CSO）など肩書や、執行役員クラスの権限を持てるかがポイントになる。さらには、内部出身者と同じく実務を支える人材も不可欠になる。

石橋氏によれば、セキュリティ対策が経営レベルで求められるようになったことで、経営層の中には、社内にセキュリティ監視センター（プライベート SOC）を作ればいいと安易に考える企業が少なくない。そのためベンダーや SIer などの出身者を採用するが、SOC の構築には大きな予算が必要になり、そもそも実務担当者がいなければ運用はできない。

「経営層とやり取りできる肩書や権限、実務を支えるメンバーがいなければ、孤立してストレスを抱えてしまい、数年後に退職してしまいかねない。内部出身者の場合もそうだが、セキュリティ対策は『チーム』で取り組むべきもの。経営層がそのことを理解しないといけない」（石橋氏）

セキュリティ強化を喫緊の課題とする経営層にとって、橋渡し役人材の確保を急ぐ場合は、内部出身者の登用が近道になる。ただ、その場合でも対策の実務面を拡充しないといけない。石橋氏は、「近年に CSIRT を立ち上げた企業では、担当者から『1 人 CSIRT になってしまい、だれにも相談できない』という悩みが聞かれる」と話す。

CSIRT の「T」は Team を指す。つまり、チームとしてセキュリティ対策を運用する体制でなければ、橋

渡し役人材をどこから登用しようにも、実効性のある対策はうまく行かないといえるだろう。

また石橋氏は、外資系ベンダーや国内ベンダーに所属してきた経験を踏まえて、IT 人材にとってセキュリティがキャリアの幅を広げるチャンスになるとも語る。「多くのユーザー企業で IT 部門の高齢化が大きな課題となっている。セキュリティの橋渡し役人材のようなキャリアは、昇進先としても転職先としても可能性を広げられる機会になる」

今後は企業ビジネスで IT の役割がますます高まるだけに、内部出身者にとっても外部出身者にとっても、組織全体のコミュニケーションから実務までを経験すればセキュリティの仕事が自身のキャリアアップにつながる。企業としてもセキュリティの向上と IT 人材の活用を図ることが重要になるようだ。

大宣システムサービス 執行役員 リサーチ＆コンサルティング アナリストの石橋正彦氏。同社は BPO や IT サービスで多数の個人情報を取り扱うことから、情報セキュリティをより強化するために外部出身の石橋氏を招いたという