ますます深刻化する セキュリティー人材不足 今、企業に求められる対応とは

制度やプログラムの活用で 計画的な人材確保の推進を

企業をサイバー攻撃の脅威等から守るためのセキュリティー人材。情報資産を狙ったサイバー攻撃が増加の一途を辿るなか、その重要性が増す一方で人材不足が顕著となっています。自社の課題を掘り起こし、必要な人材像を明確にした上で、計画的に人材を確保することが求められています。

2020年には19万人ものセキュリティー人材不足

企業におけるITへの依存度は日々増加しています。IoT（Internet of Things）やクラウド、ビッグデータ、人工知能（AI）、VR技術など技術革新が加速する中、企業経営とITはさらに緊密度を増しています。しかし、技術革新という光の裏には、脅威という影が付きまといます。その重要性が高まるにつれ、企業や組織を狙った標的型攻撃、DDoS攻撃、フィッシング、ランサムウェアなどの脅威も年々深刻度を増しています。

さらに日本では、2020年に東京オリンピック・パラリンピック競技大会という世界的イベントを控えています。ロンドン、リオに続いて開催される日本も、サイバー攻撃の標的となることは容易に想像でき、国を挙げたITインフラの強化が大きな課題です。

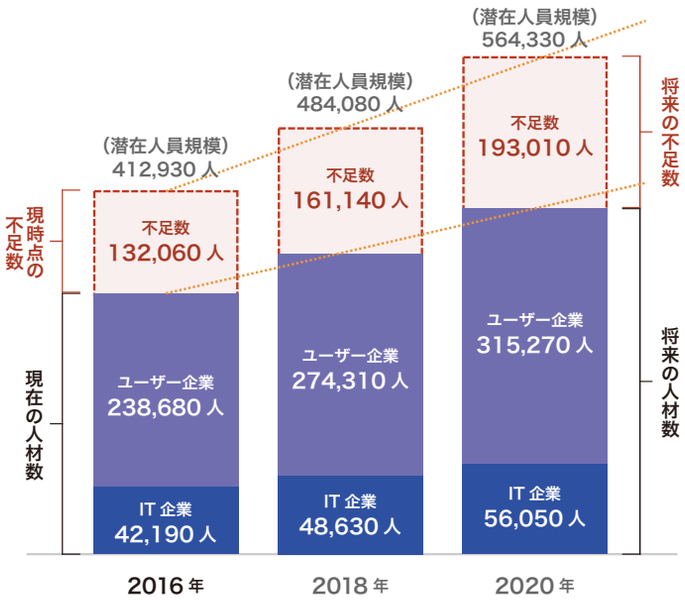
こうした脅威に対し、予防的な措置はもちろん、脅威の検知、駆除、事後対応などの検討、実行を担う、いわゆる「セキュリティー人材」が必要不可欠です。しかし、十分な人材が確保できていないのが実情で、政府でもセキュリティー人材不足を喫緊の課題と捉えています。

経済産業省が2016年6月に公開した「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、2016年の時点でIT企業とユーザー企業で働くセキュリティー人材は推定28万870人です。それに対し試算では、潜在的に必要とされているセキュリティー人材を41万2930人としています。そこには13万2060人が不足しているという大きなギャップが見られます。この人材不足はさらなる増加が予想され、2020年には19万3010人に達すると見られています。

ますます深刻化するセキュリティー人材不足 今、企業に求められる対応とは

セキュリティー人材の不足は、どのような事態を招くのでしょうか。巧妙化の進むサイバー攻撃への対応力が低下し、十分なセキュリティー対策を講じることができなければ、企業も大きなダメージを負いかねません。

顧客から預かった個人情報や、取引先から預かった機密情報の流出などが発生すれば、損害賠償による金銭的な負担はもちろん、信頼やブランドイメージを大きく損なう可能性もあります。またサービスが停止すれば売上機会を損失し、企業経営へ大きな影響を及ぼします。サイバー脅威は経営リスクにつながるという認識は、今やあらゆる業界における共通課題といえます。



セキュリティー人材発掘、育成に向けた取り組み、産官学で展開

深刻化が進むと予測されるセキュリティー人材不足。この危機的状況を打開すべく、政府では人材育成を強化する方針を打ち出しています。

政府が2016年8月に策定した年次計画「サイバーセキュリティ2016」では、横断的施策として人材の育成と確保を提言。大学や高等専門学校におけるセキュリティー教育や、在職者、離職者を対象とした職業訓練のみならず、初等教育や中等教育の段階においても、セキュリティー教育を推進する必要性を訴えています。

国だけでなく、産業界からもセキュリティー人材の育成強化を求める声が上がっています。日本経済団体連合会（経団連）では、2016年1月に発表した「サイバーセキュリティ対策の強化に向けた第二次提言」において、「サイバーセキュリティを支える根幹は人材」であるとして、各業界における人材の採用と育成、求められる人材のレベルに応じた教育、人材を評価する仕組みや基準の策定などに取り組むべきとの方針を示しました。

それでは、具体的にはどのような取り組みが行われているでしょうか。現在、人材育成を目的として数々のイベントが全国的に展開されており、日本ネットワークセキュリティ協会（JNSA）およびSECCON実行委員会が開催するセキュリティー技術の競技会「SECCON」や、情報処理推進機構（IPA）が若年層を対象に実施している勉強会「セキュリティ・キャンプ」などはその代表例です。

「SECCON」は、学生や国内外の技術者を対象にセキュリティーの知識や技術を競う競技「CTF（Capture The Flag）」です。2015年は65カ国から3343人が参加しました。海外からも参加者を募ることで国際的な競争力を持つ技術者の育成を目指しています。一方「セキュリティ・キャンプ」では、2004年以降、合宿形式で集中的に専門知識を学ぶ「全国大会」を毎年開催しています。高度な技術を持った人材を毎年50名ほど輩出しており、すでにITやセキュリティー業界で活躍している卒業生もいます。

また、大学などの教育機関とIT企業が共同で情報セキュリティー人材を育成する講座を開設するなど、産学連携の試みも広がりを見せているほか、学生に情報セキュリティーに従事することの魅力を実感してもらうために就労機会を提供するインターンシップや、セキュリティー企業と学生の交流会なども行われており、優秀な人材の獲得合戦がすでに始まっています。

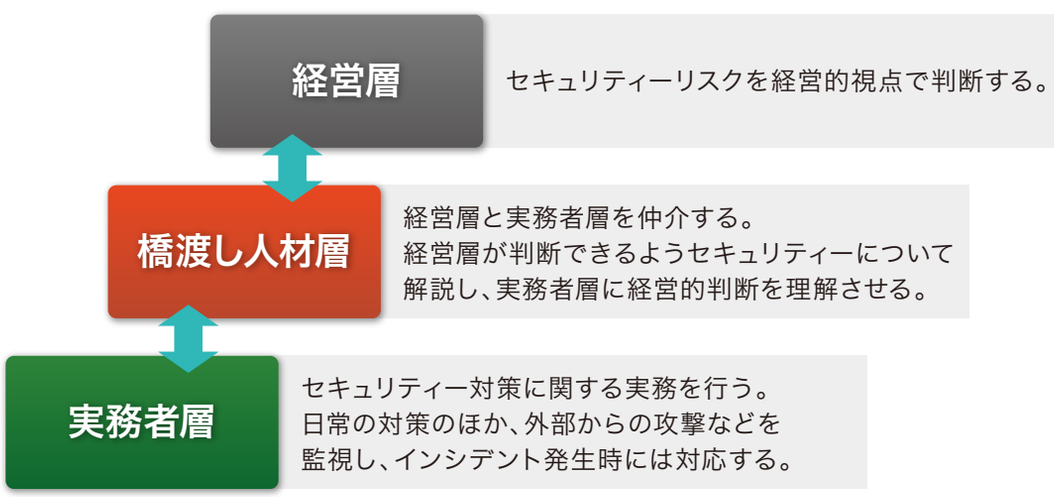
NTTにおいても、2015年4月から早稲田大学ともにサイバーセキュリティー人材育成を目的とした寄付講座「NTT寄附講座：サイバー攻撃対策講座」を開設し、今年度も継続しています。学部学生を対象とした「サイバー攻撃対策技術の基礎」では、マルウェア感染を中心に、ネットワーク上で発生する攻撃手法や対策を講義しました。また大学院生を対象とした「高度サイバー攻撃対策技術」では、上記に加え、対策手法を創出するための研究立案について、実践的な演習を交えて講義しました。

「橋渡し人材」など、求められる人材が多様化する傾向も

優秀な人材、即戦力になる人材が欲しいのはどの企業、組織でも同じでしょう。しかし、ひと口に「セキュリティー人材」と言いますが、その言葉が意味するのはどのような人材でしょうか。

「セキュリティー人材」と聞くと、高い技術を持ち、システムの脆弱性を見つける「ハッカー」のような存在を想起する人が多いかもしれませんが、それはあくまで限られた一面に過ぎません。内閣サイバーセキュリティセンター（NISC）がとりまとめた「サイバーセキュリティ人材育成総合強化方針」では、求められる人材は「実務者層」と「橋渡し人材層」など、立場ごとに異なるとし、特に「橋渡し人材」の育成を推進すべきと提言しています。

＜求められる2タイプのセキュリティー人材像＞



「橋渡し人材」とは文字通り、経営層と実務者層の間の橋渡しを行う人材です。政府は企業における「サイバーセキュリティー経営」を推し進めていますが、経営層の示す経営方針に基づくサイバーセキュリティー対策を実践するほか、組織内の関係部署間の総合調整や、実務者層との間のコミュニケーションを支援することで、実務者層をまとめてリードすることが求められます。

このような人材には、サイバーセキュリティーの「技術」に関する知識だけでなく、「経営」や「業務」、「法律」など幅広い分野の知識も有する「ハイブリッド型人材」が求められるなど、要件も異なります。

こうした課題を踏まえ、重要インフラ分野を中心とした主要企業で構成される「産業横断サイバーセキュリティ人材育成検討会」では、業界や企業の特質に即した必要な人材の定義を進め、2016年9月に第一期最終報告書とリファレンスを公開しました。

またJNSAは、セキュリティー人材が身につけるべき知識と技術を体系的に整理した「情報セキュリティスキルマップ」を作成し、最新の脅威や技術の変化に対応した「セキュリティ知識分野（SecBoK）人材スキルマップ2016年版」を提供しています。「情報セキュリティマネジメント」や「アプリケーションセキュリティ」「OSセキュリティ」など、16の分野ごとに必要な知識を参照することができます。

民間だけでなく、国も制度整備を進めています。経済産業省は、国家資格となる「情報処理安全確保支援士」制度を2016年度内に新設し、「情報処理安全確保支援士試験」を2017年度から実施することを決定しました。2016年春期からは、管理部門から一般ユーザーまで広く対象とし、情報セキュリティーに関する基本的な知識や技能を問う「情報セキュリティマネジメント試験」も開始しています。このような制度や資格試験が、企業における人材育成や人材確保に貢献しているといえるでしょう。

人材確保に不可欠な経営者のリーダーシップ

しかし、制度などの周辺環境がいくら整備されていても、自組織を守るために必要なセキュリティー対策やそれを実現していくための人材像が明確になっていなければ意味がありません。

セキュリティー対策を「経営課題である」とした「サイバーセキュリティ経営ガイドライン」が示すように、自社におけるセキュリティー上の課題を経営者が認識し、CISO（最高情報セキュリティー責任者）が中心となってどのような人材が必要なのか検討した上で、人材確保に向けた取り組みを進めていくことが、安定した企業運営を継続するための近道となります。

セキュリティーの根幹を支えるのは人材です。今後人材不足の深刻化へ対応していくには、自社が必要とする人材をいかに発掘し育成していくかを喫緊の課題と捉え、計画的に人材を確保していくことが求められているといえるでしょう。

NTTコムウェア株式会社
URL：http://www.nttcom.co.jp/
WEB掲載：2016.10