社会動向レポート

サイバーセキュリティ対策に携わる人材をめぐる需給ギャップの実態と今後の展望

デジタルコンサルティング部
上席主任コンサルタント　冨田　高樹

独立行政法人情報処理推進機構（IPA）が2012年に「国内で情報セキュリティ人材が8万人不足」という報告書を公表[(1)]して以来、「サイバーセキュリティに詳しい人材は常に不足しており引く手あまた」というイメージがある。しかし厚生労働省が求職者向けに職業の内容や必要となるスキルに関する情報提供を行っている職業情報提供サイト“jobtag”で「セキュリティエキスパート」を調べてみると、「年収」と「求人倍率」のいずれにしても、情報系の他の職業と比較してそれほど優遇されているわけでもなく、求人が突出して多いわけでもないことがわかる[(2)]。本稿では、このようなギャップが生じる背景について分析するとともに、社会におけるサイバーセキュリティ対策をさらに進めていく観点から、これらの対策に携わる人材についてどのように捉え、その育成ならびに能力発揮を促していくべきか、最新の状況をもとに論じる。

1. セキュリティに携わる人材への注目の始まり

本稿の議論を始めるにあたり、「情報セキュリティ」と「サイバーセキュリティ」という2つの用語について説明しておきたい。かつて、「セキュリティ」に関する業務といえば警備や防犯に関するものであったが、およそ1980年代以降、情報化社会における「情報」を守ることは物理的な侵入を防ぐ警備等の活動とは別の概念であるとして、「情報セキュリティ」という表現が用いられるようになった。それが現在「サイバーセキュリティ」と言われるようになったのは、そのほうが格好良いからではなく、それなりの理由がある。すなわち、社会のデジタル化が進んだ結果、情報のみならず「情報をやりとりするサイバー空間そのもの」を保護する必要が生じたことで、「情報（のみ）を守る」という印象が強い情報セキュリティよりも、サイバーセキュリティのほうが用語として適切な場合が出てきた。一方で、サイバーセキュリティでは紙媒体に記録された情報は保護の対象とならないので、紙か電子かを問わず「情報」を保護しなければならない場合等において、情報セキュリティの概念は依然として重要である。このように両者が混在する状況の中、警備などのセキュリティとの区別が容易な文脈においては、「情報」も「サイバー」もつけずに単にセキュリティと呼ぶことも多く、本稿でも同様とする。

日本でセキュリティに携わる人材に社会的な注目が高まったのは、概ね2000年前後からである。ただしそれまでセキュリティ対策を担う人材がいなかったわけではない。1980年代前半から暗号理論分野の研究者コミュニティが存在し、ウイルス対策ソフトウェア等の研究開発も、コンピュータウイルスによる被害が生じ始めた頃

から、国内の専門人材により継続的に行われている。そのような中で、2001年に情報処理技術者試験においてセキュリティ対策に携わる人材に求められる知識を問うものとして、初めて試験名に「セキュリティ」という言葉を含む「情報セキュリティアドミニストレータ試験」が追加された。これに象徴されるように、それまで情報システムやネットワークの構築や運用に関する業務の一部として捉えられていたセキュリティ対策が、ひとつの産業分野として注目され始めたのがこの時代である。2000年には日本ネットワークセキュリティ協会(JNSA)が設立されるなど、セキュリティの専門家によるコミュニティ活動を通じた社会への情報発信も積極的に行われるようになった。2003年には個人情報保護法が公布・施行され、一定規模の個人情報を扱う組織に対し保護すべき情報の漏えい防止対策実施が義務づけられた。これにより、多くの企業において個人情報保護責任者又はそれに相当する役割が規定されたことも、情報を保護するための対策を担う人材の確保・育成を促すきっかけとなった。

2. セキュリティに携わる人材に求められる要件の明確化と育成に関する取り組み

セキュリティ対策を担うことのできる人材をその他の人材から識別するには、まずそれがどのような人材なのかを明らかにする必要がある。

表　セキュリティに携わる人材に求められる知識・スキルを定義する取り組み事例

	雇用側	育成側
2000～2004年	『情報セキュリティアドミニストレータ試験』開始(2001年，経済産業省＋JIPDEC) IT スキル標準(ITSS)』公表(経済産業省，2002年) 『情報セキュリティスキルマップ』公表(2003年，IPA) 『CISSP 試験』日本語対応(2004年，(ISC)[(2)])	『セキュリティ・キャンプ』事業開始(2004年，IPA) 情報セキュリティ大学院大学創設(2004年)
2005～2009年	『テクニカルエンジニア(情報セキュリティ)試験』開始(2006年，経済産業省＋IPA) 『情報セキュリティスペシャリスト試験』開始(2009年，経済産業省＋IPA)	『カリキュラム標準 J07』公表(2008年，情報処理学会) 『情報セキュリティ人財アーキテクチャガイドブック』公表(2009年，情報セキュリティ教育事業者連絡会)
2010～2014年	『i コンピテンシディクショナリ(iCD)』公表(2014年，IPA)	『enPiT（成長分野を支える情報技術人材の育成拠点の形成』開始，2012年，文部科学省) 『CYDER（実践的サイバー防御演習)』実証実験開始(2013年，総務省＋NICT)
2015～2019年	『CSIRT 人材の定義と確保』公表(日本 CSIRT 協議会, 2015年) 『情報セキュリティマネジメント試験』開始(2016年，経済産業省＋IPA) 『セキュリティ知識分野(SecBoK)人材スキルマップ2016年版』公表(2016年，JNSA) 『産業横断人材定義リファレンス』公表(2016年，産業横断サイバーセキュリティ人材育成検討会) 『情報処理安全確保支援士試験』開始(2017年，経済産業省＋IPA)	長崎県立大学に情報システム学部情報セキュリティ学科を創設(2016年) 『SecHack365』事業開始(2017年，NICT) 『大学における情報セキュリティ教育のためのモデル・コア・カリキュラム』公表(2017年，文部科学省) 『カリキュラム標準 J17』公表(2018年，情報処理学会)
2020年以降	『ITSS＋(セキュリティ分野)』公表(2020年，経済産業省＋IPA) 『IT 総合能力診断サービス VisuMe』開始(2020年，一般財団法人日本サイバーセキュリティ人材キャリア支援協会) 『デジタルスキル標準』公表(2022年, 経済産業省＋IPA)	『プラス・セキュリティ知識補充講座カリキュラム例』公表(2022年，NISC)

（資料）各公表資料をもとにみずほリサーチ＆テクノロジーズにて作成

そこで人材の雇用側(おもに産業界)と育成側(おもに教育界)の双方から、セキュリティに携わる人材が備えるべき知識やスキルがどのようなものかを定義する取り組みが実施されてきた。その主な事例を表に示す。このうち、試験制度や教育プログラムは、そのシラバスやカリキュラム等を通じて身につけるべき知識やスキルを明らかにする効果ももたらしている。

これらの取り組みを通じて人材像がより明確になっていく中で、セキュリティに携わる人材の多様さ、すなわちそれぞれの属性に応じた境遇や、求められるものの違いが浮き彫りになっていった。例えば、表に示したITSS+（セキュリティ領域）[(3)]では全部で17種類の分野が定義されている。具体的にどのような属性があるのか理解してもらうため、ここでは次の3点の属性に関する区分を紹介する。

【属性区分1】所属企業の業態：ベンダー企業かユーザー企業か

人材がセキュリティ関連の製品やサービスを提供する事業を営むベンダー企業で活躍するのか、いわゆるユーザー企業で活躍するのかの相違である。ベンダー企業におけるセキュリティ関連業務は自社の営利活動の一部であって、優秀な人材が活躍するほど自社の事業に好影響を及ぼすので処遇との連動が生じやすい。実際、ベンダー企業では高度なセキュリティの専門能力を有する人材を年収3,000万円レベルで優遇する例[(4)]もみられ、冒頭で紹介したセキュリティに携わる人材の高給イメージを生じさせる要因となっている。

これに対して、ユーザー企業におけるセキュリティ関連業務はあくまで自社の本来業務を成立させるための手段であり、セキュリティ対策が一定水準まで整備されるとそれ以降の取り組みが経営上の収益に結び付きにくくなるため、人材が活躍することによる効果が必ずしも可視化されなくなってしまう。それならばベンダー企業で活躍する人材のほうが給与に恵まれているかといえば必ずしもそうではなく、給与水準の高い業種のユーザー企業でセキュリティ対策を担う人材のほうが待遇に恵まれている場合もある。ベンダーの売上がユーザー企業による調達に依存し、「利益を産まないセキュリティに過大な投資は避けたい」とどうしても考えがちなユーザー企業が多数を占める限り、いくら人材不足下での採用のために処遇改善が求められても無い袖は振れないという面がある。

【属性区分2】セキュリティ関連業務の専任か兼務か

セキュリティに関する業務のみを専任で担当するか、他業務との兼務でセキュリティに関する業務を行うかの相違である。実は、本稿の執筆に際して「セキュリティ人材」という表現を意図的に避けているが、これがこの論点に関係している。「セキュリティ人材」と言うと、どうしても「セキュリティに専念している人材」という印象を強く与えてしまうが、実際にはセキュリティ対策を他業務との兼務で担当している人材が圧倒的に多い。したがって、セキュリティに携わる人材すべてについて論じたいときに、「セキュリティ人材」という表現は使いにくいのである。

このように、人数的には多数を占めるセキュリティを兼務で担当する人材であるが、その育成は簡単ではない。他業務との兼務である以上、セキュリティに関する教育に費やすことのできる時間やリソースは専任者に比べると少なくなってしまうため、体系的に専門性を身につけるのに時間がかかる。これが人材不足にもつながっているが、その解決は容易ではない。サイバーセキュリティに関するインシデント対応を

例にとると、実際のところ一部の事業者等を除けば深刻なセキュリティインシデントがそれほど頻繁に発生するわけではないため、インシデント対応に備えた担当者を専任で確保すると一見暇に見えてしまうようなこともある。かといって、兼務であれば担当者は他業務を遂行する傍らでセキュリティインシデントにも対応せざるをえず、報われない状況に陥ることになりがちである。

【属性区分3】マネジメント系か技術系か

サイバーセキュリティに関するリスクは自然災害や部外者の侵入等、企業活動を取り巻く他のリスクと比較すると、暗号理論や通信方式等、いわゆる情報通信技術により密接に結びついている。そのため、セキュリティに携わるすべての人材は情報通信技術に関して一定の知見を備えることが望ましい。しかしながら、我が国の高等教育体系ではこれまで「文系」と「理系」が明確に区分されがちであったこともあって、米国等と比較するとマネジメント系の業務を担っている人材のうち、情報通信技術を理解するための背景的な知識を習得している人材が少ない傾向がみられる。セキュリティ対策においてマネジメント系の業務は対策方針(ポリシー)の策定や対策実施状況の管理、監査等多岐にわたることもあり、これらの役割を担うために必要な知識やスキルを備えた人材の不足が多くの業種で指摘されるようになった。このような状況を打開するため、現実には技術系の人材がマネジメント系の業務まで担当したり、マネジメント系の担当者と共同で対応したりといった対応がなされている。ただし、前者では担当者が「セキュリティ何でも係」のようになって疲弊する、後者ではそれぞれのバックグラウンドが異なることで言葉が通じず、うまくコミュニケーションできないといった問題も生じており、問題の解決は決して容易ではない。米国等と比較して我が国のセキュリティ分野で長年にわたって人材不足が示されているのは、このような背景も影響していると考えられている。

以上で示したような状況から、セキュリティに携わる人材をめぐる現在の状況は、言ってみれば「対策に必要な幅広い知識や能力を身につけていて、程々の処遇で活躍してくれる人材が足りない」に近く、限られた高度な専門性を備えた人材を除くとイメージほどは恵まれていないという状況が浮かび上がってくる。最近は人工知能(AI)やデータサイエンス関連分野に従事する人材の不足感も指摘されているが、今後セキュリティ分野と同様の経過をたどるかどうかは、当該業務に従事する人材への投資が企業活動に必須であることを経営層にどこまで認識してもらえるかに依ることになろう[(5)]。

これだけを読むとセキュリティ分野のキャリアは努力に見合わないようにも思えるが、その一方で専門性獲得のハードルが高いことは、いったん専門的な知識やスキルを習得し現場経験を積んでしまえば以後のキャリアは競争も少なく伸ばしやすいことを意味する。サイバー攻撃は全世界にあまねく繰り広げられている関係でその対策が企業によって異なるようなことはあまりなく、いったん習得したスキルを別の組織でも発揮しやすい。さらに、セキュリティ分野は国内においてスキル向上を目的とするコミュニティ活動が盛んな業種のひとつであり、コミュニティ活動で注目されることが転職のきっかけにもつながりやすい。かくして、よりよい仕事環境や処遇を求める人材の流動性が高いのもセキュリティ分野の特徴である。企業のセキュリティ責任者の方と話をしていると、「若手が育つのは喜ばしいが、育ちすぎると出て行ってしまう」という嘆きを聞くことがある。転職先は本

人のキャリア志向によって様々であるが、いずれにしても「育ちすぎる」とはすなわち、当人の能力に見合う報酬を出せていない状況であるから、残念ながら諦めざるを得ないところであろう。

3. セキュリティに携わる人材のスコープを拡げる「プラス・セキュリティ」

これまで説明してきた内容は、セキュリティ専任であっても兼務であっても、セキュリティの担当者または責任者として扱われる人材に関することであった。ところが、デジタル社会の成熟とともに、「セキュリティ対策はセキュリティの担当者が行っていればよい」ではうまくいかないことが明らかになった。本章ではその背景を示すとともに、セキュリティに携わる人材の育成に関してどのような見直しがなされたのかを示す。

デジタルトランスフォーメーション(DX)については、すでにバズワードとしての旬も過ぎ、多くの企業においてこれまでの取り組みの成果が問われる段階となっている。DX の特徴として、それが新事業創成や業態変革等、社外に向けたビジネスに関するものであれば、社内の情報システム部等の IT 系部門の主導でなく、事業部門主導で行われる傾向が強いことが挙げられよう。クラウドコンピューティングサービスや各種のデジタルプラットフォーム等の充実により、デジタルサービスを活用する場合であっても、IT 系部門が保有する技術的な知識やスキルよりも、事業部門が有する業務知識のほうが重要な位置を占め得ることがその背景にある。反面、サイバーリスクのマネジメントという観点から見ると、この事業部門主導の体制には不安がある。最近のデジタルサービスは容易に構築でき、適切なサービスを選択することでセキュリティ対策を初めから附随させることも可能であるが、サービスを組み合わせる中で思わぬセキュリティ上の盲点を生じさせることがある。近年クラウドサービスの設定ミスによる情報漏えい事故が多発し、総務省がこの事故に特化した対策ガイドライン[(6)]を公表しているほどであるが、これまで IT 系部門等の専門家を中心に運用されていたクラウドサービスが、事業部門を含めたより幅広い利用者によって運用されるようになったことも、その原因の一つと考えられている。

そこでこのようなデジタル環境を取り巻く変化に対応する新たなセキュリティの概念として、2019年に「プラス・セキュリティ」が提唱[(7)]された。経済産業省の資料[(8)]によれば、プラス・セキュリティとは『自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態』と定義されている。すなわち、事業部門の事業担当者が自ら取り組むことで生じうるセキュリティ上のリスクを認識して対策を講じることのできる能力を身につけることを求めるものである。もちろん、これは事業部門の担当者に2. で示したようなベンダー企業の人材並みのセキュリティ知識・スキルを求めるものではない。ベンダーへの委託を活用しつつ、すべてを丸投げするのではなく、当事者意識をもってサイバーリスクをマネジメントする能力(例：ベンダーとのコミュニケーション、サービスに応じたデジタルリスクの理解等)の獲得を目指すことが適切である。このようなニーズを踏まえ、セキュリティ教育・研修サービスを提供している事業者から複数のプラス・セキュリティ講座が提供されている。リテラシーとしてのセキュリティ教育との相違点は、リテラシーが全員が習得しておくべき内容、プラス・セキュリティが担当業務や役割に応じて習得すべき内容と整理できる。なお、プ

ラス・セキュリティの対象者として最も重要なのは経営者であり、まず経営者がセキュリティを外部に丸投げすれば済むものと考えず、自社のコーポレートガバナンスやエンタープライズリスクマネジメントにおけるサイバーリスクの影響について認識し、必要な対策が担保されるようにする必要がある。これらを促すための取り組みが政府機関において進められている[(9)]。

4. セキュリティに携わる人材のこれから

「プラス・セキュリティ」の取り組みが進むことで、2. までで論じた「プラス」でないセキュリティに携わる人材の将来はどのようになるのだろうか。ベンダー企業で活躍する人材においては、これまで主たる交渉相手であったユーザー企業の IT 部門の人材に加えて、事業部門の人材とのコミュニケーションの機会が増える。そのため、デジタルに詳しくない人材とのコミュニケーションや、顧客の業務への理解等、セキュリティの本質部分とはやや異なる領域の知識・スキルを発揮できる人材が重宝される可能性が高い。ユーザー企業においては、これまでのセキュリティ担当者が不要になることは考えられないが、仕事の内容が変わる可能性はある。有志企業によるコミュニティ活動である一般社団法人サイバーリスク情報センター 産業横断サイバーセキュリティ検討会[(10)]では、企業内に「セキュリティ統括」機能を設けて、社内のセキュリティに関する情報の共有や対策の統括を行うことを提唱しているが、このような機能はプラス・セキュリティの進展に伴ってより重要性が高まるものと考えられる。事業をデジタルビジネスに大きく依存している企業においては、このセキュリティ統括機能と全社のリスクマネジメント機能が実質的に共通化することも考えられ、デジタル化の進展とともにセキュリティに携わる人材がリスクマネジメント業務を担っていくようなキャリアも、今後は増えていく可能性がある。

もう1点、セキュリティに携わる人材の将来を展望する上で重要なのが、AI（人工知能）活用の影響である。2022年に生成 AI が注目される以前から、セキュリティ対策製品においてはサイバー攻撃の検出・識別に AI 技術を用いるものがあった。企業におけるデジタル活用が進む中、それに伴って発生するアクセスログ等のデータは増大の一途にあり、一定規模以上の企業において異常の検出を人手で行うのはすでに現実的ではない。AI 技術の発展とともに、それをセキュリティ対策に用いられていくのはほぼ必然といえる。そのような状況において、今後は程度の差はあっても、セキュリティに携わるすべての人材が AI に関する知識・スキルを保有することが求められることになろう。特に、「AI を使ったサイバー攻撃を受ける可能性」や「AI 利用時のセキュリティ上の留意点」といった知識はすべての人材に求められるのではないか。

本稿では企業でセキュリティに携わる人材の位置付けと求められる知識やスキルについて、これまでの経緯と展望について整理した。人材の需給バランスが給与に反映されやすい米国等ではサイバーセキュリティの求人は IT 系の中でも処遇に優れた業務と位置付けられているのに対し、我が国では残念ながらそれほど恵まれた業務とはみなされていないのが実態である。しかしながら、デジタル活用が続く限り、今後 AI 技術が発展する中でもセキュリティ関連業務への需要は高まることはあっても低下することは考えにくい。専門性を磨く価値のある職種として、若手人材が長期的なキャリアを考えて選ぶ有力な選択肢の一つと言える。今後プラス・セキュリティに関する啓発や実践が進んでいくことで、経営層を筆頭に企業全体でのセキュリティへの理解が深まり、現状よりも処遇が改善

される可能性も期待できる。現在セキュリティ分野で活躍している人材も、そうした期待を抱きつつ、さらなるスキル向上に積極的に取り組んでほしい。

注

(1) 『情報セキュリティ人材の育成に関する基礎調査』（独立行政法人情報処理推進機構（IPA），2012年4月）https://warp.da.ndl.go.jp/info:ndljp/pid/8198317/www.ipa.go.jp/security/fy23/reports/jinzai/index.html（国立国会図書館によるアーカイブ）

(2) 2023年10月時点でセキュリティエキスパート（オペレーション）の全国平均の年収は534.6万円、有効求人倍率は1.82倍である。（出典：厚生労働省職業情報提供サイト jobtag（日本版 O-NET）https://shigoto.mhlw.go.jp/User）

(3) https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/security.html

(4) 次の記事をはじめとする報道による。『NTT、サイバー人材に年3000万円も　実力主義で役員並み』（日経産業新聞，2023年7月20日）

(5) 経済産業省では「サイバーセキュリティ経営ガイドライン」（2023年3月（第3版））の公表を通じてサイバーセキュリティ対策への投資を将来の事業活動・成長に必要な費用であることを訴えている。https://www.meti.go.jp/policy/netsecurity/mng_guide.html

(6) 『クラウドサービス利用・提供における適切な設定のためのガイドライン』（総務省，2022年10月）https://www.soumu.go.jp/main_content/000843318.pdf

(7) 『セキュリティ人材不足の真実と今なすべき対策とは』（一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）平山敏弘・上杉謙二，2019年2月）https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf

(8) 『サイバーセキュリティ経営ガイドライン付録 F サイバーセキュリティ体制構築・人材確保の手引き』（経済産業省，2022年6月（第2版））（公表 URL は上記「サイバーセキュリティ経営ガイドライン」と同じ）

(9) （取り組みの例）『プラス・セキュリティ知識補充講座カリキュラム例』（内閣サイバーセキュリティセンター，2022年6月）https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

(10) https://cyber-risk.or.jp/