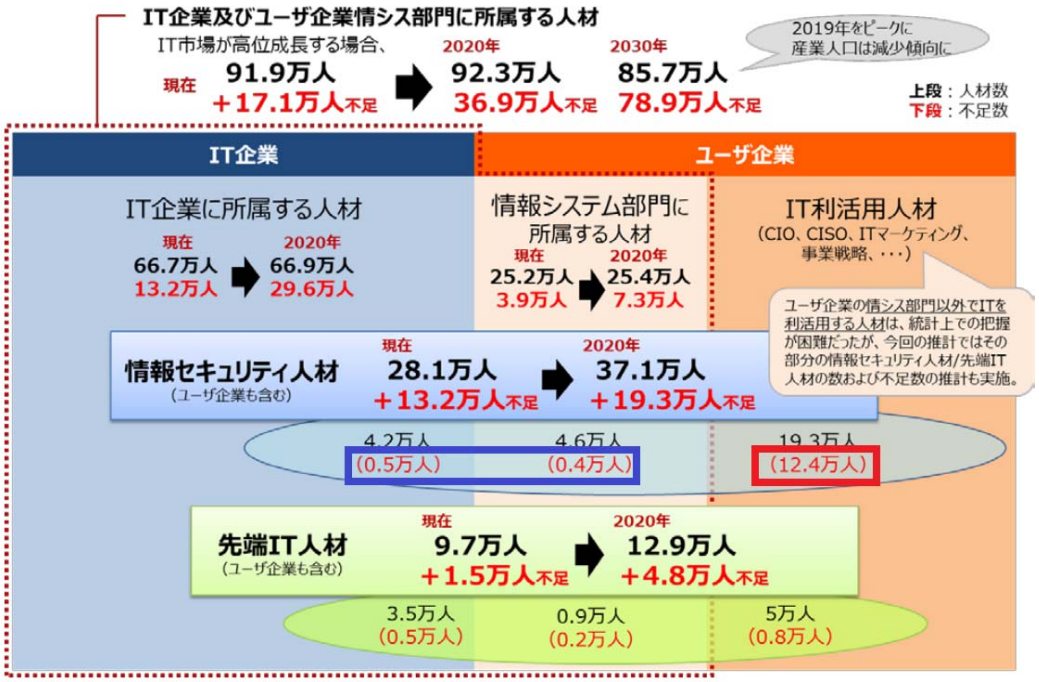
2019 年 2 月

セキュリティ人材不足の真実と今なすべき対策とは
~今必要なのは「プラス（＋）・セキュリティ人材」だ~

【要旨】

セキュリティ人材は、IT ベンダー/セキュリティ関連企業に所属し、セキュリティを主たる業務とする「セキュリティ専門人材」と、本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる「プラス（＋）・セキュリティ人材」に大別できる。当レポートは、人材が大きく不足しているのは、プラス・セキュリティ人材であることを示すと共に、今後取るべき対策について提言するものである。当レポートを通じて、IT ベンダー／セキュリティ関連企業や関連省庁、およびユーザ企業の経営/総務/人事部門のマネジメント層に対して「自社におけるプラス・セキュリティ人材の必要性」への理解を促すと共に、日本の企業文化を活かした人材育成などの新たな取り組みについての提言を行なっている。なお、様々な場面で「情報セキュリティ人材」と「サイバーセキュリティ人材」が混在して使用している例が散見されるが、当レポートにおいては広義の意味で「セキュリティ人材」と統一して使用することとする。

１）「セキュリティ人材」は、「セキュリティ専門人材」と「プラス・セキュリティ人材」に大別して考える必要がある



図表 1「IT 人材不足が深刻化 2030 年には 78.9 万人不足に」

出典：経済産業省「IT 人材の最新動向と将来推計に関する調査結果」IT 人材の需給に関する推計

現在不足しているセキュリティ人材の多くは、ユーザ企業において、自社システムのセキュリティ確保を管理できる人材であるが、このような人材はセキュリティ専門家とは限らない。2016 年の経済産業者からの報告でもユーザ企業での IT 利活用人材において、セキュリティがわかる人材が足りない（12.4 万人の不足）と報告されている（図表 1 の赤

枠参照）。一方、IT 企業とユーザ企業の情報システム部門に所属するセキュリティ人材（当レポートでは「セキュリティ専門人材」と定義）の不足数は、合計 0.9 万人（図表 1 の青枠参照）と相対的な不足感はそれほどでもない。

セキュリティ人材不足の解消にはセキュリティに特化した専門家育成が急務と考えられていたが、現状は、情報サービス業や情報通信業などの業種よりも、卸売業・小売業や医療・福祉業などの業種における不足感が高いことが報告されている（図表 4 参照）。これらの業種で必要なのは、ホワイトハッカーのようなセキュリティ専門人材とは限らない。それにもかかわらず、ホワイトハッカーのような人材が不足していると広く社会一般に解釈されているのが現状であり、国も技術寄りの対策を重視していた。しかし、現在大幅に不足しているのは、ユーザ企業において本来の業務を担いながら IT 利活用をする中でセキュリティスキルも必要となる「プラス・セキュリティ人材」であり、その育成が重要である。

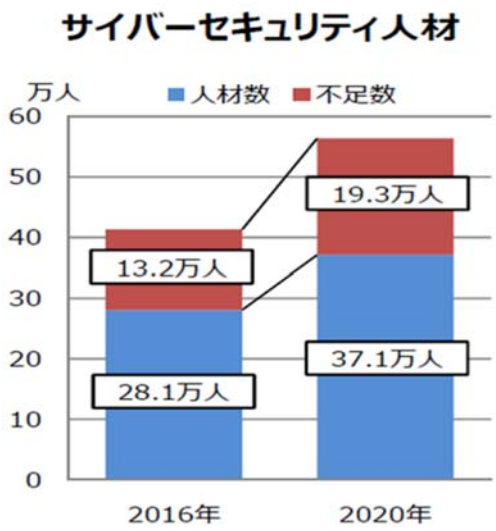
２）定期的な人事異動などを活用した「プラス・セキュリティ人材」育成が有効

よく「日本企業は、2-3 年で異動してしまうので、専門家を育成できない」との声を聞く。しかし、セキュリティ担当部門に配属になり一定のセキュリティスキルを身に付けた人がまた現場に戻り、また新たな社員がセキュリティ部門に配属されるといったローテーションのサイクルが、この十数万人不足といったプラス・セキュリティ人材の育成には、まさに好都合であり、現場での「セキュリティ版消防団」構築を推し進めることにつながる。人事異動により、セキュリティスキルや経験を身に付けた人材のユーザ企業におけるキャリアパスを明確化することも重要である（図表 8 および 9 参照）。

３）不足しているセキュリティ人材を把握する術は日本にはないのが現状、よって人材の見える化が重要

日経産業新聞 2018 年 8 月 28 日版に掲載された『セキュリティ人材、消えた「19 万人不足」』との記事では、『情報セキュリティ人材の不足を指摘する声が多いが、サイバー防衛の現場からは「不足感はない」との反論が多い。』と指摘されている。サイバー防衛の現場で必要なのは、セキュリティ専門人材であるため、このようなコメントが出ていると推測できる。一方、プラス・セキュリティ人材の不足感は高いままである。ではなぜ「日本では本当に人材が不足しているのか、いないのか。」といった議論がいつまでも続いているのか。その原因の 1 つが、日本においては人材の見える化ができていないためである。人材の見える化を推し進めることにより、セキュリティ専門人材の充足度やプラス・セキュリティ人材の不足度も明確になり、客観的に判断することが可能となるため、セキュリティ人材見える化の取り組みも必須である（図表 10 および 11 参照）。

1．はじめに



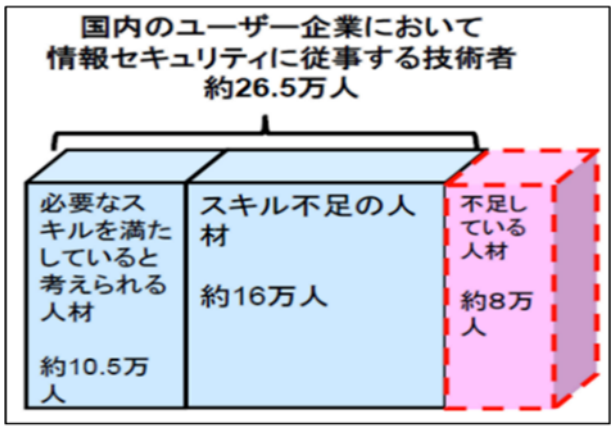
図表２　サイバーセキュリティ人材数推移
出典：経済産業省
「今後の情報政策・商務サービス政策の重点について」

セキュリティ人材が大幅に不足しており、2020 年に向けてその不足人数が大きく増えると報告されている（図表２）。経済産業省の調査ではセキュリティ人材不足は一過性の問題ではなく 2030 年に向けても不足が続くとの予測結果も出ている（図表 1）。それらの調査（図表 1 および図表 2）によると、IT 人材（IT 企業と、ユーザ企業の情報システム部門に所属する人材の合計）は現在 91.9 万人であり、人口減少と、退職者が就職者を上回ることで 2019 年から先は減少に転じるものの、IT 需要の拡大により人材ギャップは悪化すると予測されている。特に市場拡大が見込まれるセキュリティ分野については、人材不足が深刻化すると指摘されている。

セキュリティ分野の人材不足が深刻化していると言われる要因の 1 つとして、「セキュリティ人材の定義」が不明確な点があげられる。セキュリティに携わる人材は、最高情報セキュリティ責任者である担当役員の CISO（Chief Information Security Officer、以下 CISO）から、セキュリティに特化した高度なスキルを有するホワイトハッカーまで様々であるにもかかわらず、セキュリティ人材として一括りにされている。必要なセキュリティ人材の内訳を明確にし、その人材に必要なスキルを明確化することで、各人材の育成計画が可能になると共に、教育カリキュラムやシラバスに関しても身に付けるスキルを意識しながら作成することが可能になる。

また、現在不足している人材の多くは、ユーザ企業において、自社システムのセキュリティ確保を管理できる人材であるが、このような人材はセキュリティ専門家とは限らない。経済産業省もユーザ企業での IT 利活用人材において、セキュリティがわかる人材が足りないと報告しているにも関わらず、現状では、ホワイトハッカーのようなセキュリティ専門人材が不足していると一般的には解釈されている。セキュリティ人材は、IT ベンダー/セキュリティ関連企業に所属し、セキュリティを主たる業務とする「セキュリティ専門人材」と、本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる「プラス・セキュリティ人材」に大別できる。当レポートは、人材が大きく不足しているのは、プラス・セキュリティ人材であることを示すと共に、今後取るべき対策について提言するものである。

2．セキュリティ人材不足の現状の正しい理解と「プラス・セキュリティ人材」育成の必要性



図表 3　情報セキュリティ人材育成に関する基礎調査

出典：IPA「情報セキュリティ人材育成に関する基礎調査」

セキュリティ人材不足が問題視され始めたきっかけは、2014 年の独立行政法人情報処理推進機構（以下 IPA）調査「情報セキュリティ人材育成に関する基礎調査」の試算が公開されてからである。その後 2016 年の経済産業省からの調査（図表 1 および図表 2）で、さらにセキュリティ人材不足数が大幅に増加していることが報告され、現在に至っている。2014 年 IPA の報告（図表 3）では、国内企業においてセキュリティ人材は約 8 万人と大幅に不足しており、さらに情報セキュリティに従事している技術者のうち、およそ 6 割に当たる約 16 万人がスキル不足との調査結果が出る

	業種	（人）
1	農林業・水産業・鉱業	256
2	建設・土木・工業	2,764
3	電子部品・デバイス・電子回路製造業	1,403
4	情報通信機械器具製造業	605
5	電気機械器具製造業	1,150
6	その他製造業	15,853
7	電気・ガス・熱供給・水道業	81
8	通信業	683
9	情報サービス業	1,885
10	その他の情報通信業	1,717
11	運輸・郵便業	6,716
12	卸売・小売業	14,480
13	金融・保険業	4,957
14	不動産業・物品賃貸業	1,547
15	学術研究・専門技術者	1,014
16	宿泊業・飲食サービス業	3,535
17	生活関連サービス業・娯楽業	3,301
18	教育・学習支援業	2,094
19	医療・福祉	8,473
20	複合サービス業	614
21	その他サービス業	8,462
	計	81,590

図表 4　情報セキュリティ人材の不足数 8 万人の業種別内訳

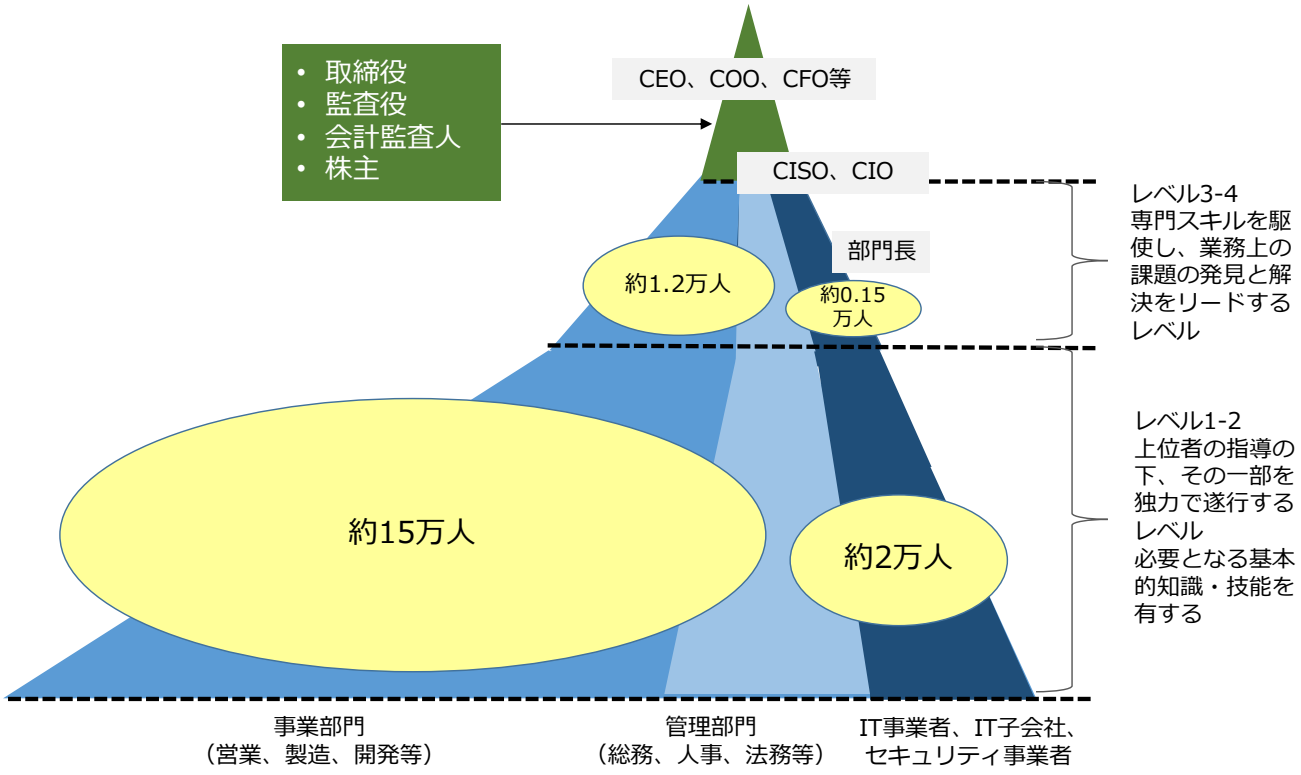
出典：IPA「情報セキュリティ人材育成に関する基礎調査」

など、セキュリティ人材の育成は急務であるとの内容であった。しかし、ここには誤解があった。この調査報告書をさらに見てみると、セキュリティ人材の不足数 8 万人の業種別内訳（図表 4）も公開されているが、一般にはこの内容までは正しく認識されていなかった。これによれば、情報サービス業や情報通信業などのセキュリティ専門家が多く所属する業種よりも、卸売業・小売業や医療・福祉業などの業種における不足感が高いことがわかる。従来のセキュリティ人材育

成は技術重視で進められてきたが、セキュリティ人材不足を解決するためには、ユーザ企業において活躍できるセキュリティ人材、すなわちプラス・セキュリティ人材の育成を検討する必要があると考えられる。そのためには、従来のセキュリティ専門家が業務を学ぶことに加えて、ユーザ企業での業務担当者がセキュリティを学ぶことが必要になる。

図表 5 は、2020 年に不足すると言われる 19.3 万人のセキュリティ人材数とスキルレベルおよび所属先の関係を表したものである。この内訳は、図表 4 の業種内訳より、約 9 割がユーザ企業側、残りの 1 割がセキュリティ企業側での不足人数と想定したものである。また縦軸は、IPA の IT スキル標準に対応した業務遂行レベルであり、円の大きさは不足人数を表している。よくある正三角形のピラミッドでないのは、不足者数が左側でより不足していることを表しており、図表 5 左下側にある事業部門に所属し、日常の業務をこなしながら必要なセキュリティ技術を身につけた人材である「プラス・セキュリティ人材」の大量な育成が必要となることがわかる。

右側の主にセキュリティ事業者に所属する、いわゆるセキュリティ専門人材も不足しているが、即戦力として争奪戦となっている中間層の人材数は約 1500 人と全体から見たボリューム的には少なく、その層の人材をセキュリティ業界内で取り合っている状況である。セキュリティ事業者間で必要な人材にあたる、セキュリティスキルレベルの高い 1500 人の不足も大きな問題ではあるが、十数万人不足と比較しては、数の点では大きな問題ではないため、セキュリティ専門事業者などにとっては人材不足数の確保を問題としていないケースもある。



図表 5　セキュリティ人材不足数の各部門とスキルレベルとのマッピング
出典：JCIC 作成

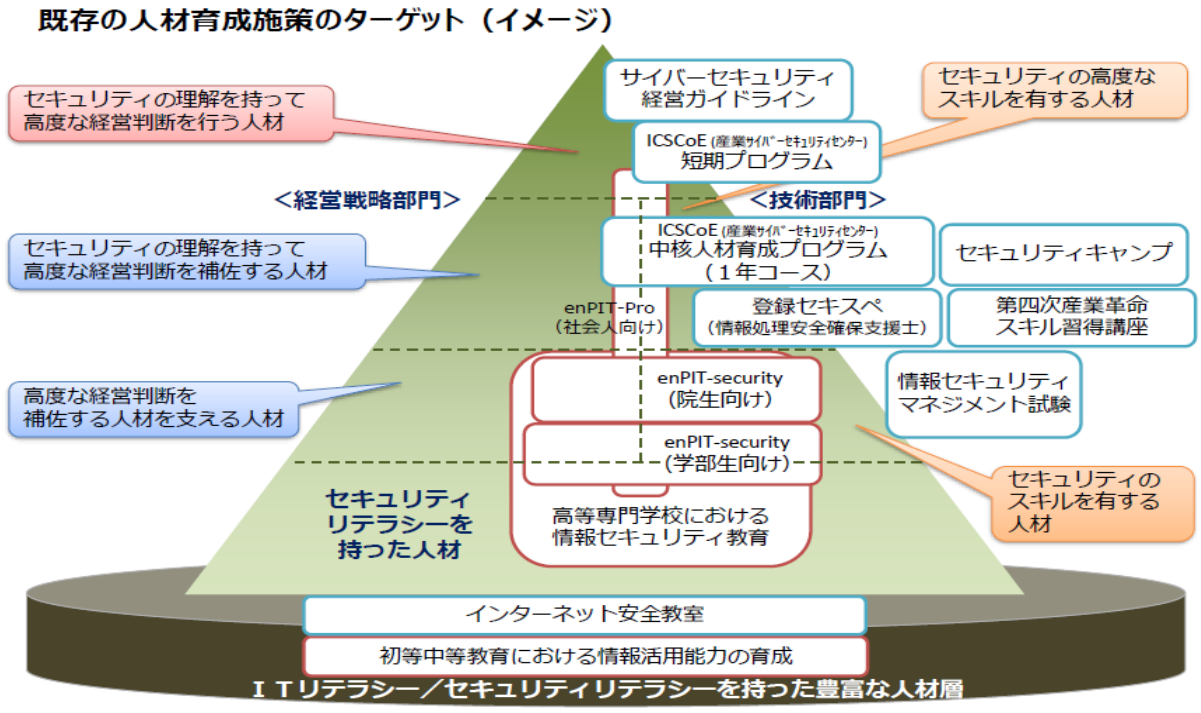
不足人数として一番問題視されているのが、左側の事業部門側で本来の業務を担いながら IT を利活用する中で、セキュリティについてのスキルも必要となるプラス・セキュリティ人材である。セキュリティ中堅レベルの 1 つの基準となる国家資格情報処理安全確保支援士について、2018 年 10 月登録に関する IPA 集計結果を見ると、登録者の所属業種は、1 位情報処理、2 位ソフトウェア、6 位コンピュータ関連の 3 業種だけで、登録者数の 70%強を占めている。12 位卸売・小売業では 1%、14 位医療・福祉業ではわずか 0.5%であり、ユーザ企業側のセキュリティ技術者は少

ない。現状、情報処理安全確保支援士登録者の多くが IT 企業の所属であり、ユーザ企業所属の有資格者数が少ない状況であり、図表 4 のユーザ企業側でのセキュリティ人材不足との関連性は明らかである。

3．セキュリティスキル向上政策からのセキュリティ専門人材育成への偏重と急務なプラス・セキュリティ人材育成対策

それではなぜセキュリティ人材＝セキュリティ専門人材との考え方になってしまったのだろうか。従来セキュリティは暗号化以外においては、比較的新しい分野であると共に技術の進歩が大変早い分野である。そのためセキュリティスキルの習得こそがセキュリティ人材の育成につながるとの方針より、セキュリティスキル向上の施策が次々と実施されてきた。当初はこのスキル向上施策により、一定レベルのセキュリティスキルの向上とセキュリティ人材の輩出が功を奏していた。しかし、スキル習得を中心とした施策であったため、結果的にセキュリティ専門人材中心の育成が進められていた。

ところが Society5.0 などの IT を利活用して社会を変えようとの時代の流れにおいては、セキュリティを守ることではなく、新たなビジネスを実現するためにセキュリティも必要との考え方に移行してきている。すなわち、セキュリティスキルに偏重することなく、何々をする人というロール（役割）の考え方もセキュリティ分野に必要となってきたのである。「内部監査を行う」、「経営の中長期計画を作成する」といった各ロールを担うには、業務遂行のためにビジネスを理解している必要がある。時代の変化やセキュリティの重要性の高まりにより、スキル・ロール双方を兼ね備えたプラス・セキュリティ人材の必要性が高まってきており、不足数も年々膨らんできているのがセキュリティ人材数の現状である。

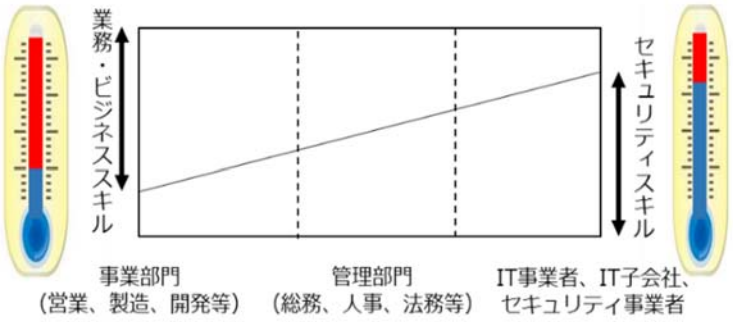


図表 6　経済産業省 「現存のセキュリティ人材育成施策とターゲットイメージ」

参照 http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_2/pdf/001_04_00.pdf

図表 6 は、経済産業省が公開している既存のセキュリティ人材育成のターゲットと現状施策とのマッピングである。これを見ると一目瞭然であるが、右側に多くの施策があることがわかる。右側は技術部門となっており、セキュリティを主業務とする IT 事業者やセキュリティ事業者などが当てはまる。一方、左側は経営戦略部門となっているが、いわゆる事業部門やユーザ企業が当てはまる。左側には既存の施策が全くないことが明白である。図表 5 で説明した、不足数が大

きい通常の業務を担いながらセキュリティのスキルも必要な人材のエリアとぴったり重なっていることがわかる。また図表 7 に表しているように、右側のセキュリティ事業者側のセキュリティ専門人材と左側の事業部門やユーザ企業での「プラス・セキュリティ人材」では、同じスキルレベルの人材であっても、必要とされるスキル（業務・ビジネススキルとセキュリティスキル）の割合が異なる点にも注意が必要である。

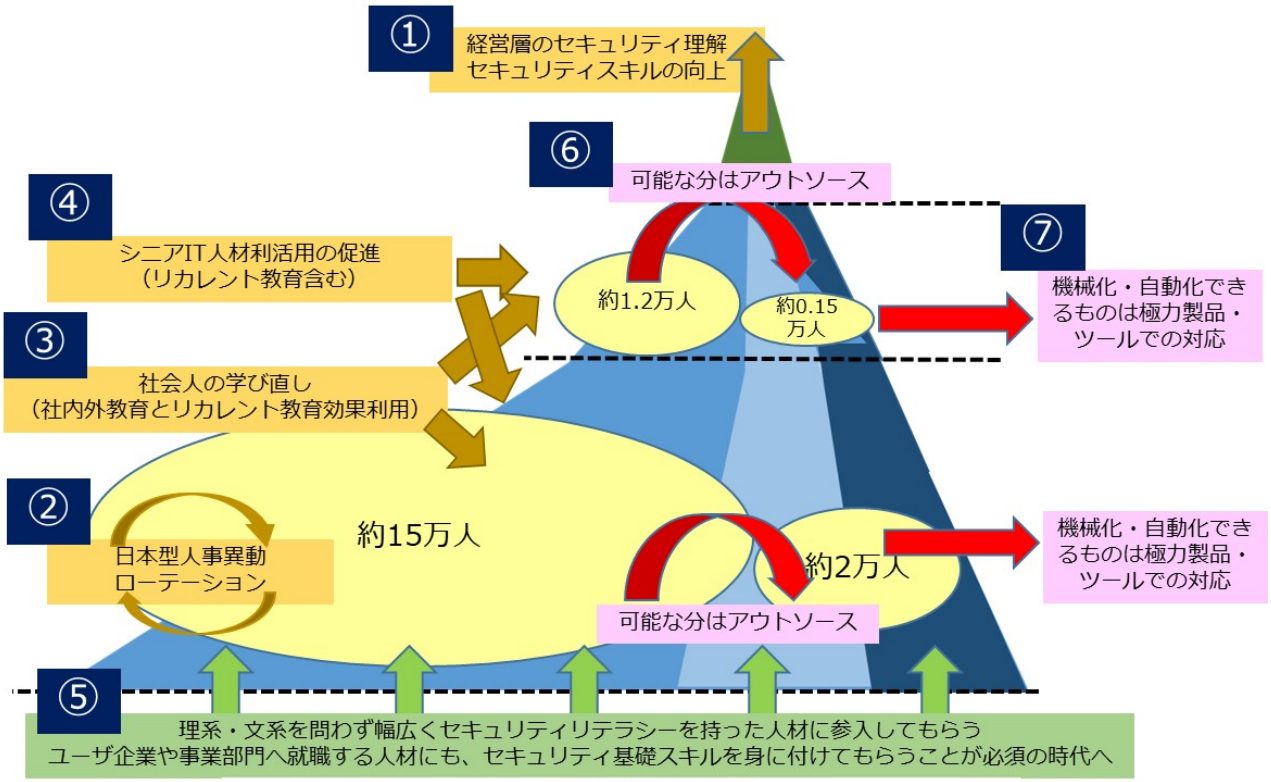


図表 7　所属企業・部門におけるセキュリティスキルと業務ビジネススキルとの関係イメージ

出典：JCIC 作成

４．今後取り組むべき対策の方向性

セキュリティ人材育成の方法は、セキュリティ専門人材とプラス・セキュリティ人材を区別して問題解決に臨む必要があることをここまで説明してきた。また育成すべきと声を上げても現在セキュリティに関連してる人材だけでは全く足りない状況であるため、図表 8 は、セキュリティ人材不足対策の方向性を示したものである。



図表 8　セキュリティ人材育成へ向けて今後取り組むべき対策の方向性

出典：JCIC 作成

施策分類	施策項目	概要
社会人のセキュリティスキル向上の施策	①経営マインド向上のための社会人向けセキュリティ教育	経営やビジネスのわかるセキュリティ責任者の育成も急務で必須であるが、現状日本での教育コースがないため、海外ビジネススクール利用なども視野に入れた検討が必要。
	②日本型人事異動を有効活用したプラス・セキュリティ人材育成	プラス・セキュリティ人材育成は、セキュリティ部門に配属され、一定のスキルを身に付けた社員が次の人事異動で現場に戻り、代わって他の社員がまたセキュリティ部門に配属されるといった異動のサイクルが好都合。
	③外部養育機関利用によるリカレント教育	自社だけでセキュリティ教育を実施することは大変困難であるため、情報セキュリティ教育分野における短期コースからプロ人材育成教育コースなど、幅広い教育コースの利用も検討。
	④シニアIT人材利活用によるセキュリティ分野への参入	業務を深く理解している人材に対してセキュリティの必要部分のみを学ばせる方が現実的である分野に関しては、シニアIT人材利活用も有効な手段。
大学教育などでの長期間をにらんだ学術機関における対策	⑤理系文系問わずの幅広い対象へのプラス・セキュリティ教育	理工系大学生だけでなく、大学卒業生約55万人の全員が対象となる「プラス・セキュリティ人材」の育成検討が必要。
アウトソーシングを考慮したセキュリティ対策	⑥セキュリティ専門家へのアウトソーシング	アウトソーシング可能な部分は外部専門機関のセキュリティ専門家に任せることを検討。
	⑦製品・ツールによる自動化や人手の軽減	人手の対応だけではどれだけ人材を育成しても追いつかない状況であるためツール利用による自動化などの検討が必要。

図表 9　セキュリティ人材育成へ向けて取り組む対策の概要
出典：JCIC 作成

社会人のセキュリティスキル向上の施策

①　経営マインド向上のための社会人向けセキュリティ教育の実施

実態の伴った CISO 数の不足が指摘されている日本においては、人材数の問題だけでなく経営やビジネスのわかるセキュリティ責任者の育成も急務で必須である。下記は海外での教育事例であるが、日本においてもビジネススクールや大学院専門課程での高度人材育成も忘れてはいけない重要な育成項目である。

・CISO 育成：カーネギーメロン大学エクゼクティブ向けサイバーリーダーシップ認定プログラムなど CISO 育成講座

・ビジネススクール：海外では、ビジネススクールでのサイバーセキュリティコース設置が当たり前にあるが、日本ではほとんどないことからも、経営層のセキュリティスキル向上の取り組みが今後必須である。（MIT スローンコース MBA 科目「サイバーセキュリティ」など）

・マスターコースのセキュリティ人材育成：バーモント州にある Norwich 大学では、1998 年から米国土安全保障省と共にサイバーセキュリティの研究を始め、2001 年からは米国防総省ともサイバーセキュリティの共同研究をしている。

②　日本型人事異動を有効活用したプラス・セキュリティ人材の育成と普及への施策

「日本企業は、2-3 年で異動してしまうので、特に技術の進歩と変化の激しいセキュリティ専門家を育成できない」との声を聞く。しかし、一定のセキュリティスキルをセキュリティ部門で身に付けた社員が次の人事異動で現場に戻り、代わって他の社員がまたセキュリティ部門に配属されるといった異動のサイクルが、「プラス・セキュリティ人材」の増加には逆に

好都合である。ここでは高度なスキルは求められず、業務で個人情報を取り扱う方や業務部門・管理部門で情報管理を担当する方に資格取得を推奨している、IPA の情報セキュリティマネジメント資格レベルで十分である。結果として、IT を利活用し業務を担うセキュリティも知っている「プラス・セキュリティ人材」がセキュリティ専門部署以外に広がり、現場でのセキュリティインシデントの火消し版とも言える「セキュリティ版消防団」構築を推し進めることにつながる。セキュリティ版消防団は、防火責任者と同様に一定の組織には必ず防火責任者のセキュリティ版であるデータ保護安全責任者（仮称）のような人材を配置するといった対策である。企業経営の安定には、定期的な人事異動などを活用した「プラス・セキュリティ人材」育成が有効となる。

③ 外部教育機関利用による体系だったセキュリティ分野のリカレント教育

自社だけでセキュリティ教育を実施することは大変困難である。それに対しては、例えば社会人を対象として働きながら学び続けることができる取り組みを推進することも検討すべきである。例としては、情報セキュリティ分野における人材育成教育コースとして、2018 年 4 月より「enPiT Pro Security（ProSec）」というコースが全国 7 大学で開講されている。その他にも国でもリカレント教育として様々な社会人の学び直しを推進している状況である。また IPA では、2017 年 4 月に 産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）を発足して、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析などを通じて、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応する人材育成を実施している。上記の教育コースは、数日の入門編短期コースから数か月から 1 年程度の本格的なプロ育成コースまで、幅広く体系的な教育コースを提供しているので、それぞれの目的にあった選択をすることが可能である。セキュリティ人材の育成は、技術進歩も早く自社での教育だけでは大変難しい分野であるため、上記の様な体系だった外部教育などを効果的に利用することも大変重要である。

④ シニア IT 人材利活用によるセキュリティ分野への参入

セキュリティと言えばスピードの変化に対応したスキルが必要なため技術一辺倒に思われるケースも多いが、実は管理や監査または調達などといった業務分野の経験やスキルを必要とする部門も数多く存在する。このような分野においてはセキュリティに特化したスキルを持つ人材に業務を学ばせるより、業務を深く理解している人材に対してセキュリティの必要部分を学ばせる方が現実的である。またこのような業務経験やスキルは短期間で育成することが難しい分野であるため、候補となる人材はシニア世代にも多く存在する。長期的には日本においての労働人口減少対策にもつながるシニア IT 人材利活用は、セキュリティ専門外からの社会人学び直し対策も含めて、今後より推進すべき施策の 1 つであると考える。

大学教育などでの長期間をにらんだ学術機関における対策

⑤ 理系・文系問わずに幅広い層からの参入による、プラス・セキュリティ人材の育成

セキュリティ関連の大学研究室に在籍している学生の年間輩出数は、わずか約 1200 人であり、そのうち約半数は暗号化関連の研究室である。情報処理業界への新卒就業者は約 2.5 万人、理工系卒業生は約 10 万人であり、これだけの学生の参入だけでは、とてもセキュリティ人材不足解消はできない。情報処理業界への就業者が全てセキュリティに従事することは考えにくいため、理工系大学生だけでなく、大学生約 55 万人の全員が対象となる「プラス・セキュリティ人材」の育成を検討する必要がある。特に経済・経営系や法学系については、「経営やビジネスのわかる、プラス・セキュリティ人材」候補に十分なりえるため、セキュリティは理系といった概念を取り払うことが重要である。

アウトソーシングを考慮したセキュリティ対策

セキュリティ人材不足の解決を促すため、さらに自動化・製品対応による効率化やアウトソーシングの検討など、複合的な対策で対応を進めることも必要である。ただし、すべてを丸投げすることでは解決されず、発注先のユーザ企業や事業部門においても的確なベンダー管理や作業品質評価ができるために、最低限のプラス・セキュリティ人材の育成を図ることが必要である。

⑥ セキュリティ専門家へのアウトソーシング

役割を明確にし、自組織で必要な役割を把握して自社での人材育成と、アウトソーシング可能な部分は外部専門機関の専門家に任せることを検討。ただし何を依頼すべきか／依頼しているのかなど、依頼している業務の評価をできることが必要である。

⑦ SIEM・AI などの製品利用による自動化や人手の軽減など、効率化を実現

監視・管理すべき情報量の日々増大するセキュリティ分野においては、人手の対応だけではどれだけ人材を育成しても追いつかない状況である。セキュリティ情報イベント管理（SIEM：Security Information and Event Management）や AI によるインシデント分析などを効率よく利用することが必要である。ただしツールやサービスの導入ありきではなく、役割や機能を明確化し、ツール化すべき部分と人手で対応しなければならない部分を明確に理解して設計・運用することが必要である。

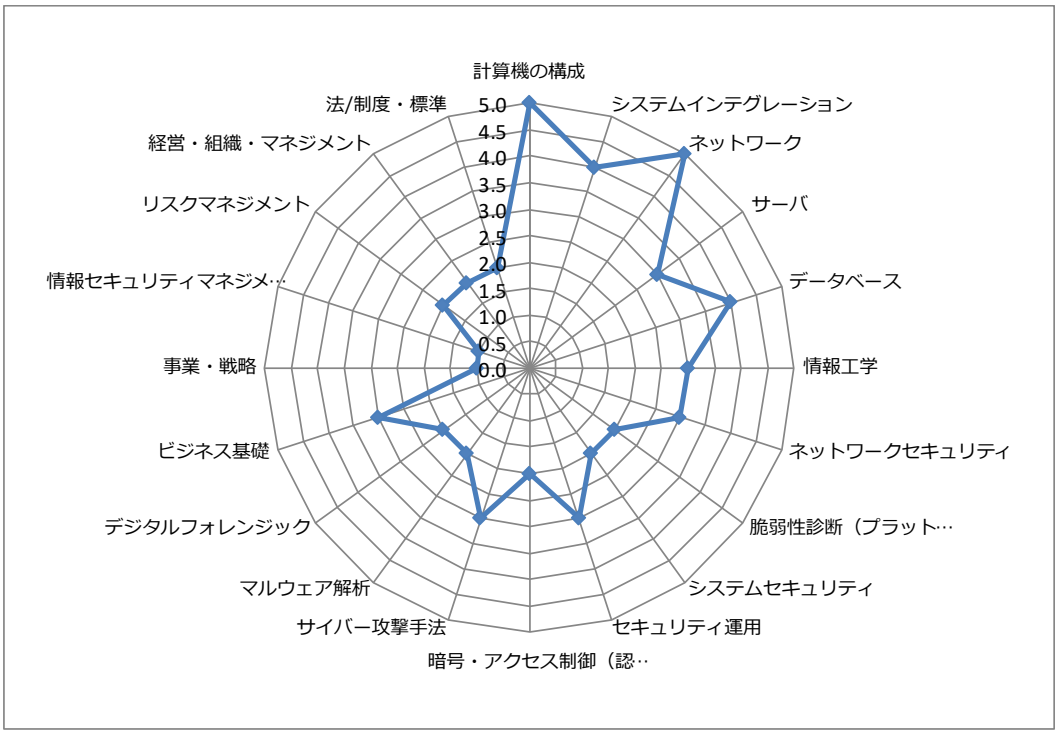
上記で述べたように、今後取り組むべき対策としては、セキュリティ人材といった一括りではなく、「セキュリティ専門人材」と「プラス・セキュリティ人材」を明確にすると共に、製品やツールを有効活用できる分野も明確にすることが必要である。育成すべき人材に関しては、セキュリティ専門人材の育成分野と業務を理解した上でセキュリティも知っているプラス・セキュリティ人材分野では育成方法も異なるため、どこをターゲットにするかを明確にしなければ効果的な対策に繋がらない。また労働力も無限ではなく限られた範囲の中での育成が必要となるので、「セキュリティは理系」「育成は若手」といった固定概念ではなく、様々な人材がセキュリティ関連の仕事に従事できる可能性があることを理解して、発想の転換を行う必要がある。

５．人材の見える化から、企業のセキュリティレベルの見える化、そして安心安全な社会の実現へ

多くの企業に IT が利活用される現代においては、セキュリティはすべての業務に関わるため、すべての企業での対策が必要である。組織内のセキュリティ問題を扱う、セキュリティインシデントに対応するチームである「CSIRT（Computer Security Incident Response Team）」に代表されるように、多くの場面でチームでの対応が求められ、それを実行するセキュリティ人材が重要になる。各人の保有スキルの見える化を実現することで、チームにおいてどの程度の実力があるのかも測定することが可能になる。人材の見える化については、NPO 日本ネットワークセキュリティ協会（JNSA）下の情報セキュリティ教育事業者連絡会において、「国内（J）のセキュリティ事業者やユーザー企業がタッグ（TAG）を組み、セキュリティ人材の適切な育成、適職認定を行うことで、セキュリティ業務への適任の人材配置を行う」目的の人材エコシステム（JTAG）の完成を目標として、人材の見える化や認定制度の実現を進めている。図表 10 および 11 の例では、セキュリティスキル見える化例を示す。この例では A さんの総合スコアは、「54 点」であり、これは 20 分野の総合スキルを点数化したものである。

個人総合スコアの積み上げは、企業におけるセキュリティ実力の見える化を実現することにつながる。その実現により、スコアが個人のスキルアップや育成だけの使用に留まらず、自社や自組織のスコアによりセキュリティの実力を判断するこ

とが可能となる。また自社や自組織に必要なスキル分野を抜き出し、本当に必要な分野に対する充足度を測ることも可能となる。セキュリティ人材不足が一向に解決されない現在、本当に必要な人材を明確にし、その育成に重点を置く施策が必要であり、効率よく、かつ確実に成果をあげるためにも人材の見える化が必要となる。



図表 10　人材見える化　総合スコア例
出典：NPO 日本ネットワークセキュリティ協会・JTAG 作成

計算機の構成	5.0
システムインテグレーション	4.0
ネットワーク	5.0
サーバ	3.0
データベース	4.0
情報工学	3.0
ネットワークセキュリティ	3.0
脆弱性診断（プラットフォーム、アプリ等共通）	2.0
システムセキュリティ	2.0
セキュリティ運用	3.0
暗号・アクセス制御（認証、電子署名等）	2.0
サイバー攻撃手法	3.0
マルウェア解析	2.0
デジタルフォレンジック	2.0
ビジネス基礎	3.0
事業・戦略	1.0
情報セキュリティマネジメント	1.0
リスクマネジメント	2.0
経営・組織・マネジメント	2.0
法/制度・標準	2.0
Aさん　セキュリティスキル総合スコア	54.0

図表 11　人材見える化　総合スコア
出典：NPO 日本ネットワークセキュリティ協会・JTAG 作成

６．まとめ

当レポートでは、不足していると言われているセキュリティ人材とは、セキュリティ専門人材ではなくプラス・セキュリティ人材（セキュリティも知っている人材）であることを明らかにした。この点については、セキュリティ専門家の間では認識されていたが、メディアなどで誤った認識に基づいて報道されることもあり、その結果ホワイトハッカーのようなセキュリティ専門人材が大幅に足りないのかと世間が誤解してしまう。また「消えた 19.3 万人」との記事が出れば、セキュリティ人材は充足していると誤解されるなど、一般の人々の認識もぶれてしまっているのが現状である。適切なセキュリティ人材育成のためには、今後「セキュリティ人材の見える化」も必須となるため、この点については JCIC でも引き続き調査研究を行い次稿で取り上げたい。

当レポートにおいてプラス・セキュリティ人材育成施策として人事ローテーションの有効活用など、従来のセキュリティ専門人材の育成方法とは異なる提案などを行っている。日本において特に多くの人数が不足しているプラス・セキュリティ人材育成は喫緊の課題であるため、安心安全な社会の実現に向け、各省庁でのセキュリティ担当やユーザ企業での総務や人事などのセキュリティ組織作り担当の方々が、今必要なプラス・セキュリティ人材の育成施策について意識変革を行い、当レポートでの提案を実行に移すことが急務である。

以上

参考文献

1）情報処理推進機構，「情報セキュリティ人材の育成に関する基礎調査」，2014 年 7 月
https://www.ipa.go.jp/security/fy23/reports/jinzai/
2）経済産業省，「IT 人材不足が深刻化 2030 年には 78.9 万人不足に」，
http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html
3）経済産業省，「情報セキュリティ分野の人材ニーズについて」
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/it_jinzai_wg/pdf/002_03_00.pdf
4）経済産業省，平成 24 年度情報セキュリティ対策推進事業、「情報セキュリティ人材の育成指標などの策定事業」事業報告書，2013 年 3 月、http://www.meti.go.jp/policy/it_policy/jinzai/24freport3.pdf
5）日本ネットワークセキュリティ協会，「セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版」
http://www.jnsa.org/result/2016/skillmap/
6）日本シーサート協議会，「CSIRT 人材の定義と確保 Ver.1.5」、
http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf
7）平山敏弘，「情報セキュリティ人材育成におけるセキュリティ知識項目（SecBoK）の有効活用」，情報処理学会第 78 回全国大会　年会論文集， p.3-515-516，2016 年 3 月
8）情報処理学会情報処理教育委員会，「情報専門学科におけるカリキュラム標準 J07」，2010 年 6 月
https://www.ipsj.or.jp/12kyoiku/J07/J0720090407.html
9）文部科学省，「 工学分野における理工系人材育成の在り方に関する調査研究（情報セキュリティ人材育成に関する調査研究）」2017 年 3 月
http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2017/06/19/1386824_001.pdf
10）平山敏弘，「産学共同による産業フィールド知識を活かした情報セキュリティ教育の実証と提言」教育情報研究：日本教育情報学会学会誌 27（1），2011-07-04， P3-10，2011 年 7 月
11）成長分野を支える情報技術人材の育成拠点の形成（enPiT）社会人を対象に情報セキュリティリーダ教育 enPiT-PRO Security，http://www.seccap.pro/

[本調査に関する照会先]

主任研究員　平山敏弘　hirayama@j-cic.com

主任研究員　上杉謙二　uesugi@j-cic.com