2021 年 7 月

攻めのプラス・セキュリティ人材で DX with Security の実現を

【要旨】

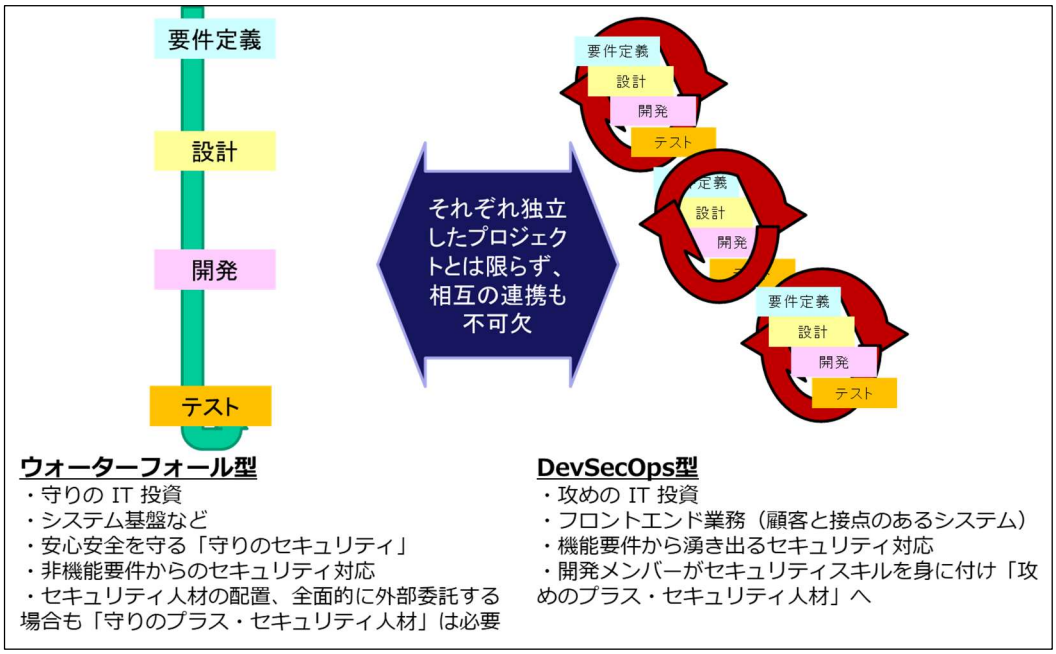
JCIC では、過去のセキュリティ人材に関するレポートで「プラス・セキュリティ人材」という概念を新たに提示した。以降、その必要性が認知され、「プラス・セキュリティ」に向けた施策や政策が多くの場で議論され始めている。本レポートは、プラス・セキュリティ人材育成の必要性に加えて、前回のレポートでも触れたセキュリティ人材可視化の推進を掘り下げ、その必要性を訴えるものである。特に企業経営者・経営層（特にユーザ企業経営者・経営層）、事業部門などにおいて事業戦略や新規サービス開発などを担当する管理者／マネージャ、および DX を推進する企業における人事／採用担当責任者に対して、「プラス・セキュリティ」の必要性と自組織におけるプラス・セキュリティ人材育成方法への理解を深めていただきたい内容となっている。また、本レポート内において多く使用されている、「プラス・セキュリティ人材」というワードは、JCIC が 2019 年 2 月に公開したレポート内で、「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スキルも必要となる人材を『プラス（＋）・セキュリティ人材』と呼ぶ」と定義したことにはじまり、その後の 2 年間ほどで急速にその考え方が広まった（「プラス・セキュリティ人材」の例は図表 1 参照）。経済産業省から公開されている、「サイバーセキュリティ体制構築・人材確保の手引き」内では、「『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のこと。『プラス・セキュリティ』は企業におけるあらゆる業務において必要となる」と説明され、人材像ではなく身に付けるべきものと定義されている。なお本レポート内で使用している「攻めのセキュリティ」とは、「攻撃」の意味ではなく、「攻めの IT 投資」から「攻め」というワードを使用しており、「DX を実現するための推進役としてのセキュリティ」を「攻めのセキュリティ」としている。

事業部門 （営業、製造、開発等）	管理部門 （総務、広報、法務等）
・顧客の個人情報を取り扱う営業担当者	・会社貸与PCやスマホの資産管理を行う総務部担当者
・工場のOTシステムの保安対策の一環としてサイバー攻撃対策を検討する設備担当者	・インシデント発生時に社内外連絡や調整を行うCSIRT のPoC（Point of Contact）機能を兼務する広報担当者
・自社のDX 展開におけるサイバーセキュリティ上の脅威を検討する、DX 推進担当者	・自社の契約書雛形に盛り込むセキュリティ対策について検討する法務担当者

図表 1 各部門におけるプラス・セキュリティ人材の例
経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」より JCIC 作成

1）攻めの IT 投資と DevSecOps、そして攻めのプラス・セキュリティ人材

「守りの IT 投資」と「攻めの IT 投資」という言葉が近年よく使用されているが、「攻めの IT 投資」における開発手法のキーワードに、「DevOps（デブオプス）」がある。開発のチーム（Development）と運用のチーム（Operations）が継続的に互いのミッションを補完することにより、迅速かつ確実な実装と運用を実現し、ビジネスにおけるシステムの有用性を高める概念が DevOps であり、このサイクルにセキュリティ要素を加えたものが DevSecOps である。DevOps、DevSecOps の下では、要件を迅速に開発へ反映させることが必要である。多くの組織では、DevOps、DevSecOps 環境においても、セキュリティ専門家をチームメンバーに置くことは困難と思われる。ビジネスの速度が速く、セキュリティリスクが高い時代においては、DevSecOps を採用することによって、企業は大きな価値を得ること（つまり



図表 2　開発手法とプラス・セキュリティとの関係
JCIC 作成

攻めの IT 投資の実現）が可能となるのである。 しかし、重要なのは、基幹システムなどのウォーターフォール型開発とフロントエンドサービスを実現する DevSecOps 型開発がともに連携し、機能することであり、すなわち「攻めのセキュリティ」と「攻めのセキュリティ」双方が必要である点である（図表 2）。

2）IT 部門やセキュリティ部門以外でも、自部門に必要なセキュリティスキルを把握して育成を

ユーザ企業や事業部門においてプラス・セキュリティ人材が普及していない原因は、「セキュリティは業務外」などの誤った認識から、必要なセキュリティスキルを理解していないことである。そのため、職務内容の定義が不明確となり、セキュリティ関連部門以外ではセキュリティミッションは対象外との認識で看過されるケースが多い。また、ユーザ企業・事業部門においてプラス・セキュリティ人材の必要性を理解した場合にも、次のステップとして人材の補強や育成を実施しようとした際に、自部門に必要なセキュリティスキルがわからないのが次の大きな問題となる。その際には、まず自部門の現状を理解することが必要であり、求めるセキュリティレベルと現在の保有レベルとのギャップを把握しなければならない。企業において重要なのは、個人毎のギャップと共に、自部門におけるギャップの把握である。現在の水準を評価するツールが先

進的な取り組み組織から公開されているので、そうしたツールの利用も選択肢となる。人材育成においても同様で、セキュリティ知識分野の人材スキルマップなど、効率よく有用な情報を利用することが必要である。

３）セキュリティ人材の可視化により職務が明確化、人材不足解消へ

日本の名だたる大企業が、職務を明確にして、年齢や年次を問わずに適切な人材を配置する「ジョブ型」への移行を加速させている。グローバルでの人材獲得競争が し烈さを増す現在、グローバル基準のジョブ型に移行する企業が、今後さらに増えることが予想される。セキュリティ業界は、中途採用においては比較的ジョブ型採用が進んでいる業界であると思われる。しかし、不足数が多いユーザ企業で必要なプラス・セキュリティ人材に関してはまだ進んでいない状況である。その原因はプラス・セキュリティ人材に求められるスキルを判断できない点にある。テクニカルなセキュリティスキルと業務スキルを兼ね備えた人材を募集する際に、求める人材のスキルを明確にして、採用時に見極めることは大変困難である。その際に、ジョブディスクリプション（職務記述書）に則った求人募集が可能となれば、人材採用活動時のマッチ度を高めて、効率的な組織強化が可能となる。また採用時だけでなく、業務委託時などでも、求めるスキルとの適合度を参考にして、ミスマッチを防ぐ情報として活用することが可能となる。

４）国策として、プラス・セキュリティ知識の拡充

JCIC では、「プラス・セキュリティ人材」という新しいワードを生み出し、その必要性を説き、広める活動を実施してきた。その必要性が認められ、NISC（内閣サイバーセキュリティセンター）では、2021 年度から始まる、「次期サイバーセキュリティ戦略」において、横断的な施策の 1 つである「人材確保、育成、活躍促進」で、「プラス・セキュリティ知識を補充できる環境整備」として取り上げられている。国策においてもプラス・セキュリティへの取り組みが喫緊の重要テーマと掲げられている点は、JCIC 活動の大きな成果である。セキュリティの可視化は、人材の可視化にとどまるものではない。その先には企業におけるセキュリティ力（実力）の見える化と続き、セキュリティに対する実力が企業の実力や競争力につながる。安全・安心な社会の実現および、安全を考慮した攻めの IT 投資となる DX with Security を実現し、競争力の高い企業になるためには、従来の「規制や禁止」による守りの実現だけでなく、「加速の推進役」となる「攻めのセキュリティ」が必須となる。本レポートでの提案をご理解いただき、プラス・セキュリティ知識（特に新たな考えである「攻めのプラス・セキュリティ」）の拡充を実行に移すことを強く望むものである。

1．はじめに

JCIC では、過去 2 度のセキュリティ人材レポートにおいて、「プラス・セキュリティ人材」という概念を提唱した。以降、その必要性が認知され、「プラス・セキュリティ」に向けた施策や政策が多くの場で議論されるに至った。今回のレポートでは、「攻めのプラス・セキュリティ人材育成」の必要性を再確認しつつ、人材育成体制の確立や遂行の促進剤となるセキュリティ人材可視化の推進と、ユーザ企業・事業部門で取り組むべきセキュリティ関連業務について、特に下記の方々の理解を促すことを目的としている。

・企業経営者・経営層（特にユーザ企業経営者・経営層）
・事業部門などにおいて事業戦略や新規サービス開発などを担当する管理者／マネージャ
・デジタルトランスフォーメーション（以下「DX」）を推進する企業の人事／採用責任者

本レポートにおいて「攻めのプラス・セキュリティ人材」の必要性を認識いただき、喫緊の課題である「守り」および「攻め」双方のプラス・セキュリティ人材育成を、一部の大企業だけでなく多くの企業において広く実践いただきたい。そのうえで、攻めの IT 投資により真の DX 化を実現するために、DX with Security を強く意識していただくと共に、今後取るべき対策について提言する。

2．攻めの IT 投資と DevSecOps、そして攻めのプラス・セキュリティ人材

2.1 新たな IT 投資により変化するプラス・セキュリティ人材

「守りの IT 投資」と「攻めの IT 投資」という言葉が近年よく使用されている。図表 3 は、「守りの IT 投資」と「攻めの IT 投資」を分類したものだ。「守りの IT 投資」においては、主な対象領域はバックエンド業務における SoR（System

	伝統的なIT投資	新たなIT投資
目的	守りのIT投資 (コスト削減) (ビジネスを支援)	攻めのIT投資 (売上・付加価値向上)(ビジネスを実行)
傾向	安定性重視	スピード重視
対象領域	バックエンド SoR（Systems of Record）	フロントエンド SoE（Systems of Engagement）
IT投資の形態	プロジェクト	プロダクト・サービス（価値提供）
オーナー	情報システム部門	LOB（事業部門：Line of Business）
プラットフォームへの要求	ウォーターフォール	アジャイル、DevOps 等
開発形態	信頼性・堅牢性	拡張性・柔軟性
人材の役割	ITベンダーへの外注が基本	ユーザー企業での内製や パートナリングによる開発が主体
開発運用体制	分業・専門分化	フルスタック・マルチロール
対象業務	予測可能	探索型
データ	構造	構造＋日構造＋外部
強み	統率力・実行力	機動力・柔軟性

出所）独立行政法人情報処理推進機構（IPA）「ITSS+（プラス）」より三菱総合研究所作成

図表 3 新たな IT 投資の位置づけ

出典：三菱総合研究所「デジタル経済の将来像に関する調査研究の請負　報告書」（赤枠囲みは引用者による）

of Record:記録のシステム）、つまり社内で扱う情報を安全に管理し、適切にアウトプットできる点を重視した基幹系システムである。他方、「攻めの IT 投資」においては、主な対象領域はフロントエンド業務における SoE（System of Engagement：顧客とのつながりのシステム）、つまりユーザと企業をどのように繋いでいくかという点を重視したシステムである。一方、「攻めの IT 投資」では、ICT の進化、およびサービスや顧客ニーズの多様化のスピードが速く、次々に新しいサービス・製品が求められる市場においては、要件定義からリリースまでの短い開発期間の反復（イテレーション）を重ねながら、よりよいシステムの開発を目指す「アジャイル型」の開発が近年増加している。

また、「攻めの IT 投資」における開発手法のキーワードに、「DevOps（デブオプス）」がある。開発のチーム（Development）と運用のチーム（Operations）が互いのミッションを補完することにより迅速かつ確実な実装と運用を実現し、システムの有用性を高める概念が DevOps である。DevOps モデルの上で実行される開発と運用が統合されたライフサイクルでは、あらゆる段階にセキュリティの要素を組み込むことが必要となる。それにより、ビジネス目標達成のためのライフサイクルを迅速かつ安全に実行することが可能となる。この DevOps から派生して、開発と運用にセキュリティ（Sec）を加えた概念である、「DevSecOps（デブセックオプス）」という考え方が注目されるようになってきている（図表 4）。

図表 4 DevSecOps ライフサイクルのセキュリティ
出典：トレンドマイクロ「DevSecOps 時代の Cloud Security」

ウォーターフォール型の開発と違い、システムライフサイクルが短く、開発スピードが速い DevSecOps 環境においては、要件を迅速に開発へ反映させる必要がある。しかし、多くの組織では、 DevSecOps 環境においてもセキュリティ専門家をチームメンバーに置くことは困難だ。本レポートでは、開発と運用を融合させた DevOps にセキュリティ対策を組み入れたものを DevSecOps と位置付けている。そこで DevSecOps 実現の際には、外注依存も厳しいケースが多いため、開発メンバーにプラス・セキュリティのスキル・意識が求められる。

従来、DevOps がもたらす主要な効果は、システムのビジネス稼働までの時間短縮、品質の向上、コスト削減であった。もちろん DevSecOps においても同様の効果が求められるが、それ以上に経営面からの価値が加わることが重要な点である。DevOps によって短期間で品質の高いアプリケーションを開発したとしても、サイバー攻撃によってサーバー

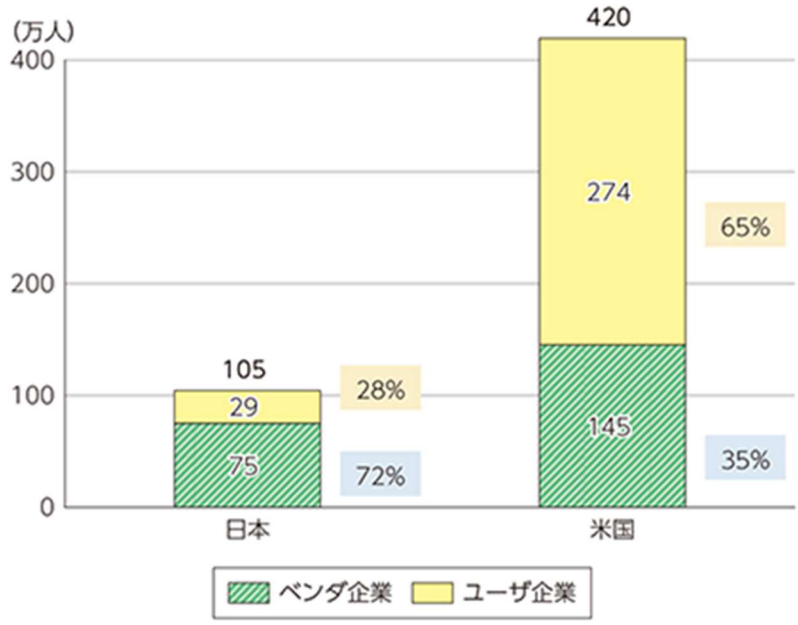
がダウンしたり、情報が漏えいしたり、セキュリティ上の脆弱性の問題があった場合はビジネスに大きな損害が生じる。深刻な問題であれば、サービスの中止はもとより、経営に大きな影響を与えることさえあり得るのである。セキュリティは、安全・安心を守るために、サイバー攻撃や不正などの問題が生じたときの保険（守り）としてとらえられてきた。しかし、ビジネスの速度が速く、セキュリティリスクが高い時代においては、DevSecOps を採用することによって、企業は大きな価値を得ること（つまり攻めの IT 投資の実現）が可能となるのである。

しかし、DevSecOps 型の攻めのプラス・セキュリティ人材がいれば足りるわけではない点に注意が必要だ。非機能要件からのセキュリティ対応を実現するために、「セキュリティ専門人材」と共に「守りのプラス・セキュリティ人材」も必要となる。重要なのは、基幹システムなどのウォーターフォール型開発とフロントエンドサービスを実現する DevSecOps 型開発が双方に連携すること、すなわち「攻めのセキュリティ」と「攻めのセキュリティ」双方が必要である点だ。

2.2 現在の日本の構造や体制では、なぜ DevSecOps は困難なのか

前項において、DevSecOps 開発を実施するユーザ企業に攻めのプラス・セキュリティ人材が必要なことを説いた。しかし、現状ではユーザ企業に攻めのプラス・セキュリティ人材がほとんどいないのが現状である。その理由はセキュリティだけの問題ではなく、我が国で ICT 利活用によるイノベーション促進及び付加価値増加を目指すにもかかわらず、現状では、ユーザ企業に ICT 人材が少ないという構造的問題と関係があると考えられる。

我が国は米国と比較して、ICT 人材の数が少なく、さらに人材がユーザ企業側に少なくベンダ側に偏在している傾向がある。総務省の「平成 30 年度版情報通信白書」では、2015 年の日米の情報処理・通信に携わる人材数を推計している（図表 5）。



図表 5　日本と米国の情報処理・通信に携わる ICT 人材
出典：総務省「平成 30 年版情報通信白書」

ICT 人材の分布について、従来から 7:3（ベンダー7 割：ユーザ企業 3 割）の内訳が日米では逆となっているとは指摘されてきたが、日本においては、ユーザ企業に ICT 人材が少ないという構造的特徴があり、当然セキュリティ人材

も同様であると考えられる。この特徴が、DevOps（DevSecOps）開発を困難にしている。DevSecOps は、短期間サイクルでスピードも速いため、開発を委託する場合であってもユーザ企業側にもセキュリティスキルのある人材の配置が不可欠である。

以前より、日本では図表 6 にある業種でセキュリティ人材が不足していると言われていたが、果たしてユーザ企業で採用・育成できているのだろうか。2014 年に情報処理推進機構（以下「IPA」）が行った調査から、ユーザ企業や事業部門でセキュリティ人材が不足している（不足する）と指摘されてきた。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。しかし、ユーザ企業側での ICT 人材の割合が少ない状況においては、プラス・セキュリティ人材が充足されることは困難である。世の中はデジタル化や DX 化などが叫ばれ、多くの企業でサービスや顧客ニーズの多様化の要求に応えるために、スピードが速く、次々に新しいサービス・製品の開発や提供を目指しているが、DevSecOps に対応できる攻めのプラス・セキュリティ人材がいないため、十分なセキュリティ対応が取られていないサービスや製品が供給される危険性が高まっている。

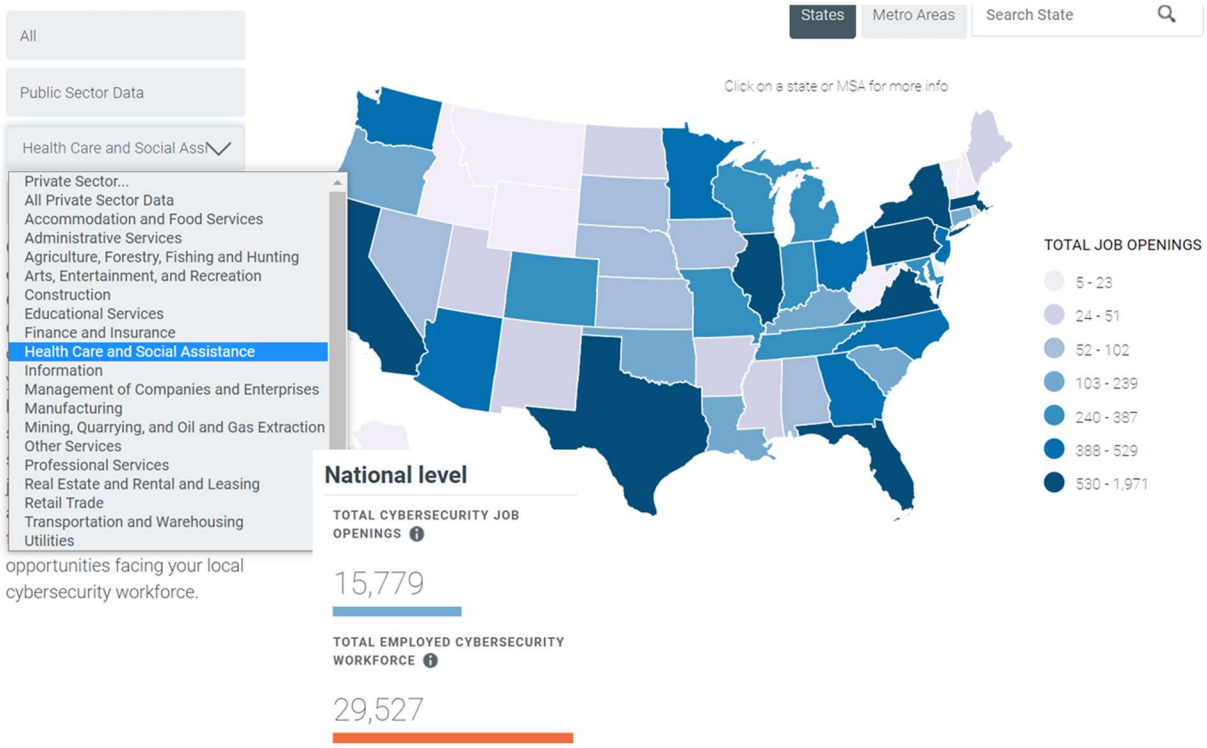
	業種	（人）
1	農林業・水産業・鉱業	256
2	建設・土木・工業	2,764
3	電子部品・デバイス・電子回路製造業	1,403
4	情報通信機械器具製造業	605
5	電気機械器具製造業	1,150
6	その他製造業	15,853
7	電気・ガス・熱供給・水道業	81
8	通信業	683
9	情報サービス業	1,885
10	その他の情報通信業	1,717
11	運輸・郵便業	6,716
12	卸売・小売業	14,480
13	金融・保険業	4,957
14	不動産業・物品賃貸業	1,547
15	学術研究・専門技術者	1,014
16	宿泊業・飲食サービス業	3,535
17	生活関連サービス業・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 6 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不足数等に関する追加分析について」内データより JCIC 作成

2.3 ユーザ企業のセキュリティ人材募集が当然の世界

米国では、Cyberseek という米国全土においてセキュリティ人材の雇用募集数（Job Openings）を概観できるウェブサイトがある。このサイトには、米国全土だけでなく、州や業種ごとでの募集数など、セキュリティ人材の募集に関するさまざまな情報が集約されている。そのサイトを見ると、多くの業種のユーザ企業側が既にプロパー社員としてのサイバーセキュリティ人材の必要性を認識し、募集していることがわかる。例えば日本でも不足していると言われている医療業界では、米国では既に約 3 万人がセキュリティ業務に従事しており、さらに約 1.6 万件の求人募集がある状況である(図表 7）。ここでは医療業界の例を挙げたが、他の業種においても、ユーザ企業側が、新規サービスへの対応や自社の価値拡大のためにセキュリティ人材を積極的に登用していることがうかがえる。



図表 7　米国での医療業界におけるセキュリティ人材求人例
出典：Cyberseek 「CYBERSECURITY SUPPLY/DEMAND HEAT MAP」

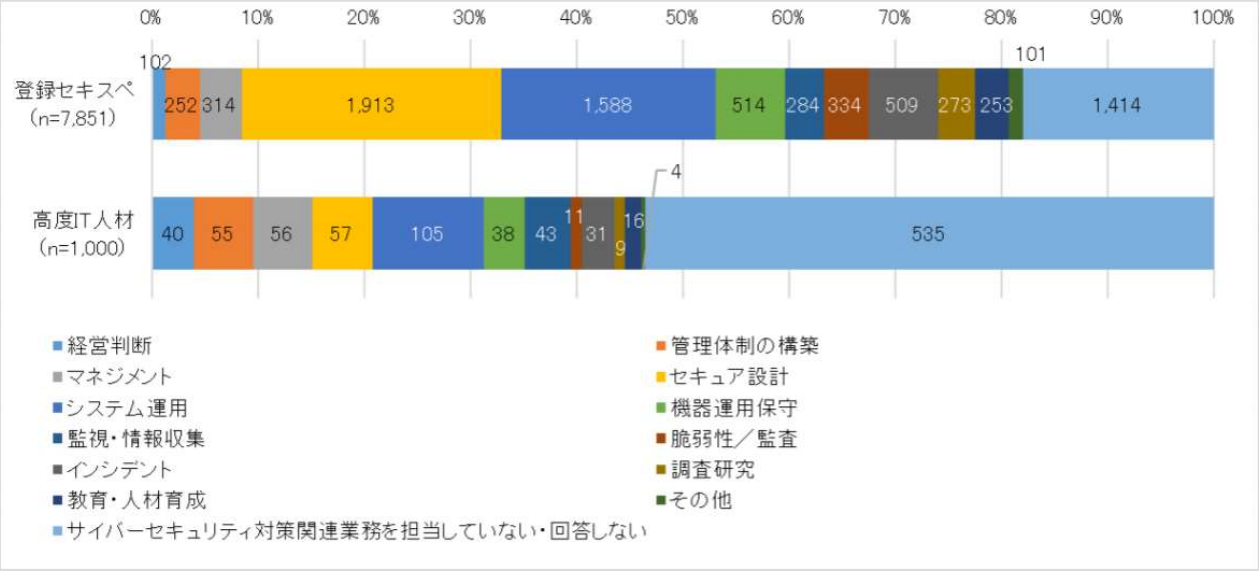
日本では未だセキュリティ人材求人募集をする企業がサイバーセキュリティ関連企業に偏っており、各ユーザ企業が自社社員としてセキュリティ人材を積極的に採用する米国と比べると、サイバーセキュリティに対する企業対処の差異があることがうかがえる。

3．IT 部門やセキュリティ部門以外でも、自部門に必要なセキュリティスキルを把握して育成を

3.1 埋もれた人材を掘り起こし、プラス・セキュリティ人材へ転換を

ユーザ企業や事業部門においてプラス・セキュリティ人材が普及出来ていない原因は、ユーザ企業や事業部門において、「セキュリティは業務外」の誤解などから、必要なセキュリティスキルを理解していない点にある。職務内容の定義が不明確で、セキュリティ関連部門以外ではセキュリティミッションは一切無しとなる。

上記を裏付けるデータを、IPA が情報処理安全確保支援士の登録者に実施した調査から見て取れる。サイバーセキュリティに関連する業務を明示的には担当していないと答えた人が情報処理安全確保支援士の約 2 割に及んだ（図表 8）。IPA では、「セキュアな業務遂行は当たり前で非明示的に行われている可能性や、サイバーセキュリティ対策が必要ではない業務担当の人でもセキュリティ知識が必要と考えて資格を取得している可能性などが考えられます。」と分析している。現在ほとんどの組織が ICT を利用していると考えられるので、ICT を利活用している企業や部門でセキュリティに関連した作業が「 0 」であることは通常考えられない。ましてや情報処理安全確保支援士資格を保有している人材を有効に活用できていない点は問題である。情報処理安全確保支援士資格者は約 2 万人なので、その 2 割である約 4,000 人が、高度なセキュリティスキルを有しながら、それを活用していない状況である。2019 年 2 月公開の JCIC レポート「セキュリティ人材不足の真実と今なすべき対策とは」内で「攻めのプラス・セキュリティ人材」は、約 1.2 万人不足としているが、埋もれた 4000 人をそれに充てれば、不足人数の約 1/3 がすぐに解消することも可能となる。



図表 8 情報処理安全確保支援士の職務分類
出典：IPA「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」

3.2 人材や部門の可視化で、自社・自部門に足りないセキュリティスキルの把握と必要スキルの習得を

ユーザ企業や事業部門において、「なぜセキュリティは自部門の問題である」との認識が薄いのか。またどうすればプラス・セキュリティ人材の普及が可能となるのか。普及を阻害する原因は、主に下記の問題点が考えられる。この問題点を解決しなければ、ユーザ企業や事業部門にプラス・セキュリティ人材が充足することは難しい。

・問題点 1 ：必要なセキュリティスキルの過不足が把握できておらず、セキュリティスキル不足の実感がない
・問題点 2 ：自社・自部門にプラス・セキュリティ人材が必要と理解しても、学ぶべきスキル項目がわからない

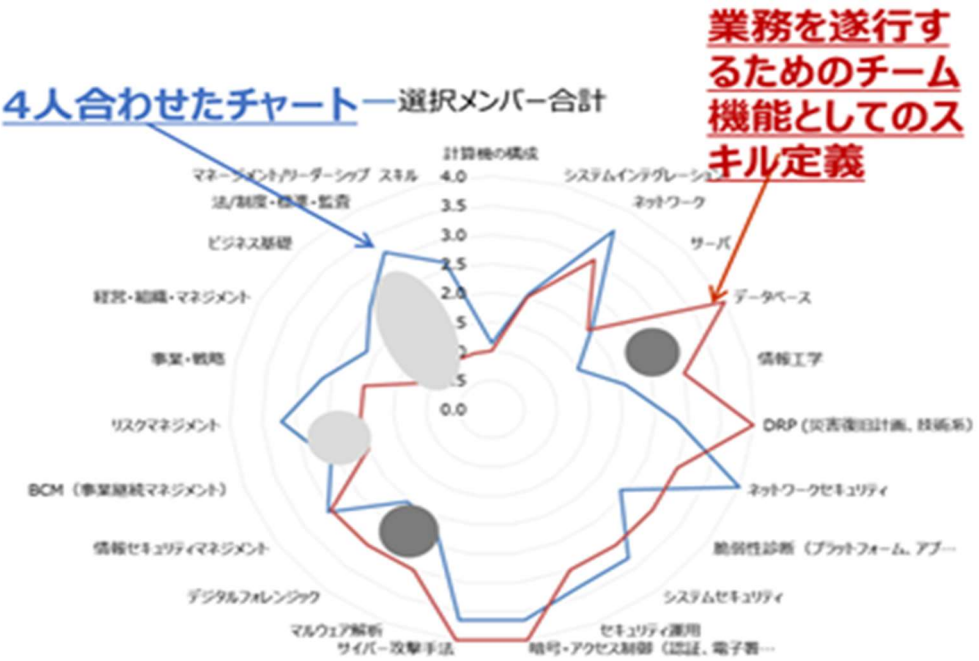
以降において、上記問題点の解決に何が必要なのかを述べる。

１）自社・自部門に必要なセキュリティスキルの過不足を可視化で把握し、セキュリティ不足危機を我が事と認識を

ユーザ企業・事業部門でプラス・セキュリティ人材の必要性を訴えられても「我が社（自部門）にセキュリティ人材を配置すべき」との認識はまだ低いのが現状である。それは、IPA から 2015 年に公開されている「IT 利用部門における情報セキュリティマネジメント人材の重要性」内にある、「ユーザ企業の約 7 割が、セキュリティ人材の育成を実施しておらず、その理由は第１位の『投資が出来ない』に次いで、『セキュリティ人材の必要性を認識していない』が続いている。」点などからもうかがえる。

また、プラス・セキュリティ人材の必要性を理解した場合にも、次に補強や育成を実施しようとした際に、自社・自部門に必要なセキュリティスキルがわからないことも大きな障壁となる。また、何から手を付けて、どのように取り組んだらよいのかもわからないなどの声も多く聞く。その際には、まず自社・自部門の現状を理解する必要がある。そのためには、必要なセキュリティレベルと現在保有しているレベルとのギャップを把握しなければならない。客観的にギャップを理解することで、セキュリティ不足危機を我が事と認識し、次に取るべき対策も明確になるのである。特に、企業において重要なのは、個人毎のギャップと共に、自社・自部門におけるギャップの把握である。

社員や部門のセキュリティスキル可視化は、組織やチームの現状での実力を評価したり、体制作りを行ったりする際に大変有用であり、足りないスキル項目や強化項目を把握して組織やチーム育成につなげられる。図表 9 では、4 人からなるチームのメンバー合計の実力（青線）と、組織がこのチームに要求するスキル（赤線）を重ね合わせて、そのギャップを評価している。これは 4 人チームの例であるが、さらに大きな組織や企業全体に広げて求めるスキルレベルとのギャップを把握して強化策を立てることも可能である。従来、社員個々のスキル診断などを実施しているケースは多いが、チームや組織の単位で現状と目標とのギャップを可視化し、補強と育成のポイントを明確にしているケースはまだわずかだ。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（以下、JTAG）では、先進的な取り組みとしてセキュリティ人材可視化ツールを作成し、その普及を図っている。



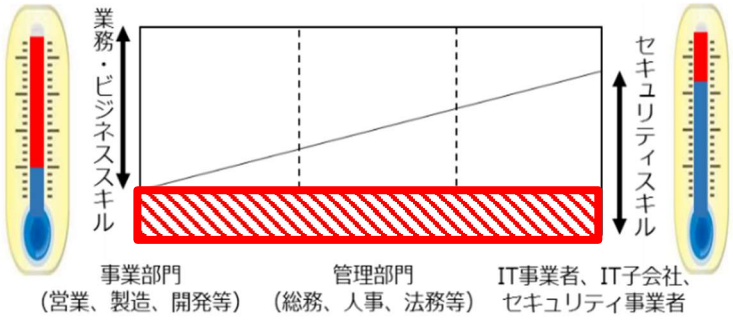
図表９　組織やチームのタレントマネージメントとしての利用

出典：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

部門で必要なセキュリティスキルが明確になれば、ユーザ企業や事業部門に所属していてもセキュリティ対応のミッションが明確になり、取り組みを正当に評価される環境が整う。さらには、情報処理安全確保支援士資格者を活用できていない状況から脱却できるのではないだろうか。また、それこそが JCIC の唱える「プラス・セキュリティ人材」が正当に評価され、それにより人材も増加するという好循環につながると考える。

2）自社・自部門に必要なプラス・セキュリティ人材が学ぶべきスキル項目の把握

「プラス・セキュリティ人材」と言っても、図表 10 に示すように、所属部門や担当の職務（横軸）により、同じスキルレベルの人材であっても必要とされる業務・ビジネススキルとセキュリティスキルの構成比が大きく異なると考えられる。また、職位によっても求められるセキュリティスキルレベルが異なる。それにより「プラス・セキュリティ人材は、何を学べばいいのかわからない」と言った問題が発生する。そこで、すべてのプラス・セキュリティ人材に共通するスキルエリア（図表 10 の赤枠斜線部分）だけでもスキル項目を明確にすることが重要となる。この取り組みに際して、NPO 日本ネットワークセキュリティ協会（以下「JNSA」）が公開している「セキュリティ知識分野人材スキルマップ（以下「SecBoK」）」の 2021 年版が多くの組織にとって非常に有用と思われる。



図表 10　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

SecBoK とは、情報セキュリティに関する業務に携わる人材が身につけるべき知識とスキルを体系的に整理したものであり、16 の役割と 1,000 以上のスキル項目で構成されている。SecBoK2021 版では、業務の種類や立場などによって求められるスキルが異なるプラス・セキュリティ人材に共通する、土台となるスキルを 3 つの分野（00 基礎、01IT・セキュリティ基礎、02IT ヒューマンスキル）に集約（図表 11）し、図表 10 の赤枠エリアに相当するスキルについて学ぶべき項目を明確にしている。SecBoK2021 では、技術的なスキルだけではなく、IT ヒューマンスキル項目を含み、プラス・セキュリティ人材のスキル習得や育成に対応できる内容となっている。

まずは、ベースとなるスキルをチェックし易くするため分野カテゴリーを改定

2021ID	旧2019ID	KSA-ID	新旧別	分野	大項目	中項目	レベル	小項目
1	1	K0052	旧NICEに類似項あり	00基礎	1数物情報学		L	数学に関する知識（例：対数、三角法、線形代数、微積分、統計、操作解析）
2	2	K0030	旧NICEに類似項あり	00基礎	2計算機・通信工学		L	コンピュータアーキテクチャ（例：回路基板、プロセッサ、チップ及びコンピュータハードウェア）に適用される電気工学に関する知識
：								
38	991	K0380	新規	01IT・セキュリティ基礎	1ICT	1ICT利活用	L	コラボレーションツールと環境に関する知識
39	992	K0576	新規	01IT・セキュリティ基礎	1ICT	1ICT利活用	L	情報環境に関する知識
：								
62	1086	K0239	新規	02ITヒューマンスキル	1コミュニケーション力		L	書面、口頭及び視覚メディアを介して通知する代替方法を含む、メディア制作、コミュニケーション及び普及の手法および方法に関する知識
63	1087	S0070	旧NICEと同一	02ITヒューマンスキル	1コミュニケーション力		L	情報を効率的に伝達するための他者とのコミュニケーションに関するスキル

図表 11　セキュリティ知識分野人材スキルマップ（SecBoK）2021

出典：NPO 日本ネットワークセキュリティ協会（JNSA）

４．　セキュリティ人材の可視化により職務が明確化、効率的な人材マッチングやジョブローテーションで人材不足解消へ

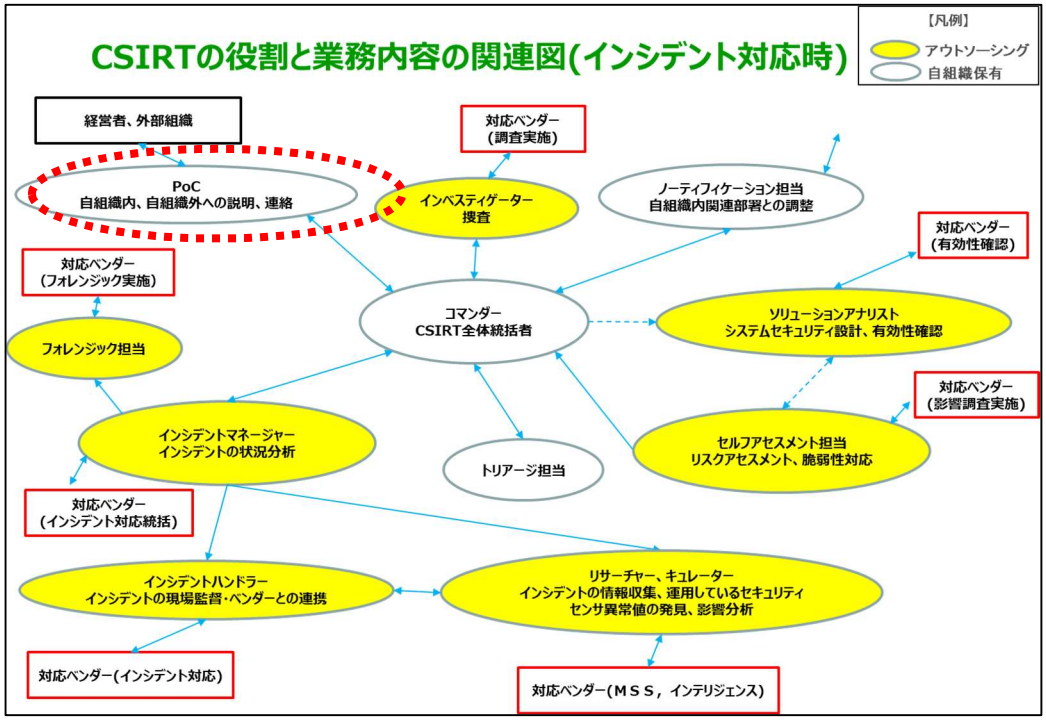
4.1　日本におけるジョブ型採用の現状と、セキュリティ人材不足解決策とは

日本の名だたる大企業が、職務を明確にして、年齢や年次を問わずに適切な人材を配置する「ジョブ型」への移行を加速させている。グローバルでの人材獲得競争がし烈さを増す現在、グローバル基準のジョブ型に移行する企業が、今後さらに増えることが予想される。ジョブ型の大きな特徴は、ジョブディスクリプション（職務記述書）が全てのポジションに示され、その能力や経験に見合った人材が採用・配置される点である。社員は社内にジョブがなくなれば会社を移り、会社側も新しいポジションには社外から人材を調達するなど、人材の流動化が進む傾向がある。そもそも「ジョブ型採用」に対応する英語はない。グローバルではジョブディスクリプションに基づいたジョブ型採用が当然であり、それ以外の採用方法がないためである。

日本特有である「新卒一括採用」におけるメンバーシップ型の採用では、採用時点で職務上必要なスキルを獲得している人材はまれであり、多くの場合は企業内で人材育成を図る。その後も各人の専門性とは無関係な人事ローテーションや転勤が行われる。高度経済成長期においては、売上が右肩上がりに拡大し、一定数の均質な人員を確保する目的でメンバーシップ型雇用が広く用いられてきたが、従来の日本型雇用は、今大きな転換点を迎えている。

4.2　セキュリティ人材可視化で、プラス・セキュリティ人材採用時に求めるスキルの明確化を

セキュリティの事件・事故発生時の対応組織として CSIRT（Computer Security Incident Response Team：シーサート）があるが、その中の役割の 1 つに PoC（Point of Contact）がある。PoC は、自組織外・自組織内の連絡および IT 部門での調整担当を実施する、セキュリティインシデント発生時には非常に重要な役割であ



図表 12　CSIRT の役割と業務内容の関連図(インシデント対応時)

出典：日本シーサート協議会　人材定義と確保

る。そのため、日本シーサート協議会では、アウトソーシングでは対応できず、自組織で実施すべき役割であると定義している（図表 12）。

CSIRT の一員と言うと高度なセキュリティスキルを持った専門家と思われるかもしれないが、PoC は、社外窓口として監督省庁や外部機関との連絡窓口となり、情報連携を行い、一方社内窓口としても IT 部門やセキュリティ部門、法務、渉外、広報等の各部門と情報連携を行う。このように、PoC には一定レベルのセキュリティスキルのほか社内外調整のコミュニケーションスキルが求められる。自社の業務知識も求められるため、IT 部門やセキュリティ部門ではなく、総務や広報等の部門の社員が担当するケースも多い。

この PoC のような、テクニカルなセキュリティスキルと業務スキルを兼ね備えた人材は、1 から自社で育成することは非常に難しいため、外部から人材を採用することも積極的に検討する必要がある。しかし、人材募集を行う際に、求めるスキルを明確にすることが難しく、また何を評価すればいいのかわからないというのが現状である。その際、SecBoK などのセキュリティスキルマップを利用し、ジョブディスクリプション（職務記述書）に則った求人募集により、求める人材に要求するスキルを明確化することで、人材採用活動時のマッチ度を高めて、効率的な組織強化が可能となる（図表 13、PoC 人材求人募集例）。

項目	記載例	SecBoKのID ()内は旧ID	NICE（旧版）ID
ロール名	**POC**		
職務内容 （NCA資料より）	自組織外・自組織内連絡担当、IT部門調整担当 社外窓口として、JPCERT/CC、NISC、警察、監督官庁、NCA、他CSIRT等との連絡窓口となり、情報連携を行う。 社内窓口として、IT部門、法務、渉外、IT部門、広報、各事業部等との連絡窓口となり、情報連携を行う。		
任用前提知識・スキル （SecBoKの対象）	コミュニケーションスキル（相手の意図や感情を理解する）	要追加	ー
	情報を効率的に伝達するための他者とのコミュニケーションに関するスキル	63(1087)	S0070
	レポーティングスキル（難しい内容を、読み手に合わせて書き砕く能力）	65(1089)	なし
	ITSSレベル2程度の基礎的なITリテラシー	41(994)	なし
追加教育知識・スキル （SecBoKの対象）	コミュニケーションスキル（組織として発信する文書の作成スキル）	要追加	ー
	メディアリテラシーに相当するスキル（すべての情報をうのみにしてはいけないという批判的視点など）	80(1104)	なし
	セキュリティマネジメントに関する知識	112(81)	K0276
	自社のセキュリティポリシー、規則、実施方法等に関する知識	120(89)	なし
	企業のインシデントレスポンスプログラム、役割及び責任に関する知識	346(315)	K0150
	ボードメンバーを含むすべてのレベルの管理者とのコミュニケーションを行うスキル（例：対人関係スキル、アプローチ力、効果的なリスニングスキル、視聴者のためのスタイルと言語の適切な使用など）	75(1099)	S0356
	脆弱性情報の発信源（例：アラート、アドバイザリ、正誤表、報告書）に関する知識	209(178)	K0040
	情報収集ならびに情報を生成、報告及び共有するための主要な方法、手順及び技術に関する知識	879(1055)	K0315
必要な経験・資格 （参考）	経験：業務を通じた顧客・取引先・関係機関等との対話・交渉経験 資格：なし		
あると望ましい経験・資格（参考）	経験：広報・渉外等部署での業務経験 資格：情報セキュリティマネジメント試験		

図表 13　セキュリティ知識分野人材スキルマップ（SecBoK）2021

出典：NPO 日本ネットワークセキュリティ協会（JNSA）

この手法は業務委託などでにもミスマッチを防ぐ材料として活用できる。日本には自社で育成し、経験を積んだ人材の流出を危惧する企業が多いが、ジョブ型雇用は企業の組織力アップにも有効である。弱点を含む組織の持つ力を可視化することにより、効率よく育成と採用の両面を実施しながら組織力を高めることが、今後ますます必要となる。企業や組織では、人材の可視化が実現できることで、今後各部署で増強すべきスキルが明確になり、適材適所配置を行う際に各人員のスキル情報を参考情報として活かすことで効果的な人事ローテーションができる。それと共に、社員のタレントマネージメントや育成プラン、キャリアチェンジを具体的にイメージする手助けにもなるため、今後さらに積極的な取り組みが求められると考えられる。

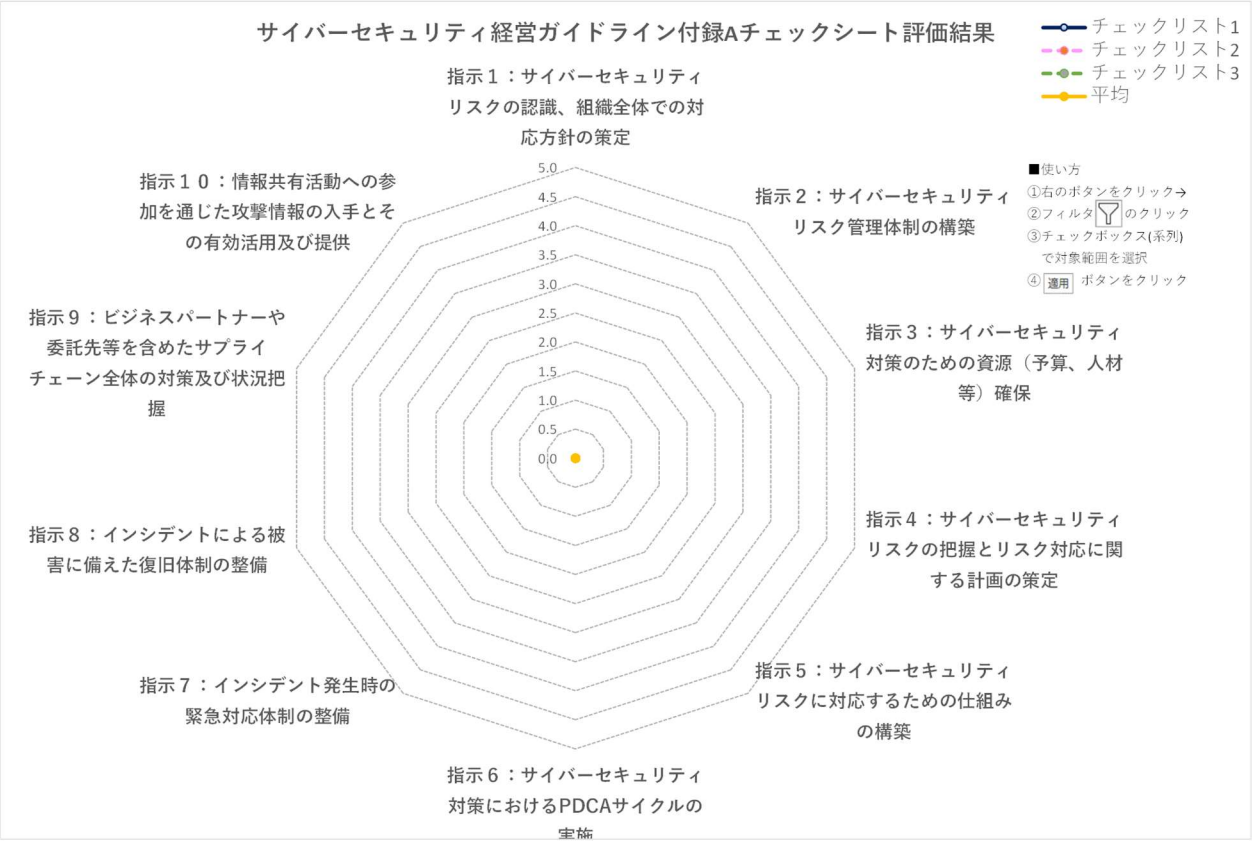
５.まとめ

本レポートでは、はじめに続き 2 章において、攻めの IT 投資時代においては、DevSecOps の取り組みが重要であり、そのためにはユーザ企業や事業部門に攻めのプラス・セキュリティ人材が必要となるが、その取り組みは米国と比較して大きく遅れている問題点を指摘した。3 章では、ユーザ企業や事業部門で必要なセキュリティスキルを理解することが難しい点に触れ、人材や部門のスキル可視化を実施することで現状での過不足部分を明らかにする方法について述べた。続く 4 章では、人材を可視化することで実現するジョブ型雇用について、セキュリティ人材募集例により、特にプラス・セキュリティ人材の募集には効果的であることを説いた。JCIC では、過去 2 回の人材育成レポートで、「プラス・セキュリティ人材」という新しいワードを生み出し、その必要性を説き、広める活動を実施してきた。その必要性が認められ、NISC（内閣サイバーセキュリティセンター）が掲げた 2021 年度から始まる「サイバーセキュリティ戦略」において、横断的な施策の 1 つである「人材確保、育成、活躍促進」「プラス・セキュリティ知識を補充できる環境整備」として取り上げられている（図表 14）

図表 14　横断的施策

出典：NISC 「次期「サイバーセキュリティ戦略」骨子について（普及啓発・人材育成関係）」

経済産業省においても、「サイバーセキュリティ経営ガイドライン」に基づいてサイバーセキュリティの体制を構築し、人材を確保するための要点をまとめて公開した「サイバーセキュリティ体制構築・人材確保の手引き」内に、「プラス・セキュリティの取り組み推進」として取り上げられている。国策においてもプラス・セキュリティへの取り組みが喫緊の重要テーマと掲げられている点は、JCIC の活動が社会や業界に認められた大きな成果である。 セキュリティの可視化は、人材の可視化にとどまるものではない。その先には企業におけるセキュリティ力（実力）の見える化へと続き、セキュリティに対する実力が企業の実力や競争力につながる。その企業のセキュリティ力を可視化する 1 つの方法としては、既に経済産業省が、「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール」を公開している（図表 15）。サイバーセキュリティの実践状況を企業自身がセルフチェックで可視化するためのサイバーセキュリティ経営ガイドラインベースの可視化ツールである。企業は自社の状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能となるツールである。



図表 15　サイバーセキュリティ経営ガイドライン付録　チェックシート評価結果チャート

出典：経済産業省が、「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール」

本レポートにおいて「攻めのプラス・セキュリティ人材」の必要性を認識いただき、日本において特に多くの人数が不足し、喫緊の課題である「守り」および「攻め」双方のプラス・セキュリティ人材育成を、一部の大企業だけでなく多くの企業において広く実践していただきたい。そして安全・安心な社会の実現および安全を考慮した攻めの IT 投資となる DX with Security を実現し、競争力の高い企業になるため、本レポートでの提案をご理解いただき、実行に移すことを強く望むものである。

以上

参考文献

１）株式会社三菱総合研究所，「デジタル経済の将来像に関する調査研究の請負　報告書」，2019 年 3 月
https://www.soumu.go.jp/johotsusintokei/linkdata/r01_04_houkoku.pdf

２）トレンドマイクロ，「DevSecOps 時代の Cloud Security」，2018 年 7 月
https://www.trendmicro.com/ja_jp/business/campaigns/aws/resources/devsecops_whitepaper.html

３）総務省，「平成 30 年版情報通信白書」
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/pdf/index.html

４）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/

５）Cyberseek，「CYBERSECURITY SUPPLY/DEMAND HEAT MAP」
https://www.cyberseek.org/heatmap.html

６）情報処理推進機構，「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」，2019 年 7 月
https://www.ipa.go.jp/files/000076776.pdf

７）情報処理推進機構，「IT 利用部門における情報セキュリティマネジメント人材の重要性 ～機密情報を脅威から守るために～」，2015 年，https://www.ipa.go.jp/files/000048311.pdf

８）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(JTAG)「IT 総合能力診断サービス」，
https://www.j-tag.or.jp/

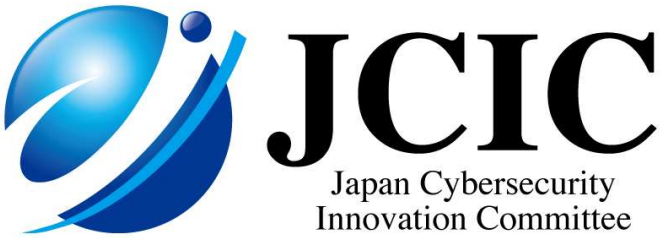
９）NPO 日本ネットワークセキュリティ協会（JNSA），「セキュリティ知識分野人材スキルマップ（SecBoK）2021」，2021 年 5 月，https://www.jnsa.org/result/skillmap/

１０）日本シーサート協議会（NCA），「CSIRT 人材の定義と確保」，2017 年 3 月
https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

１１）内閣サイバーセキュリティセンター（NISC），「次期「サイバーセキュリティ戦略」骨子について（普及啓発・人材育成関係）」，2021 年 6 月
https://www.nisc.go.jp/conference/cs/jinzai/dai15/pdf/15shiryou0301.pdf

１２）経済産業省，「サイバーセキュリティ体制構築・人材確保の手引き」，2020 年 9 月
https://www.meti.go.jp/press/2020/09/20200930004/20200930004.html

１３）経済産業省，サイバーセキュリティ経営ガイドライン実践状況の可視化ツール，2020 年 3 月
https://www.ipa.go.jp/security/economics/checktool/index.html



[本調査に関する照会先]

客員研究員　平山敏弘　hirayama@j-cic.com

JCIC 事務局　info@j-cic.com