産業界が求める
プラス・セキュリティに関する調査
（概要説明資料）

2022年8月

独立行政法人情報処理推進機構

目次

1.調査の背景・目的 …… 2

2.調査概要 …… 3

3.調査結果 …… 7

4.まとめ …… 10

1.調査の背景・目的

- 近年、情報セキュリティ対策が強固とは言えない中小企業を対象としたサイバー攻撃やそれに起因する大企業等への被害が顕著化してきており、大企業のみならずサプライチェーンを構成する中小企業であっても、サイバー攻撃の脅威にさらされている実情が明らかになっている。
- また、このような背景のもとで独立行政法人情報処理推進機構が事務局を務める「サプライチェーン・サイバーセキュリティ・コンソーシアム（以下「SC3」という。）」内の「SC3産学官連携WG」においても、セキュリティ人材の育成・活躍促進についての議論が行われ、セキュリティ対策を本務とするセキュリティ専門人材に加え、セキュリティ対策を本務としないが、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「プラス・セキュリティ※1」の取組についても議論が開始されているところである。
- そこで「SC3産学官連携WG」におけるこれら議論に供するとともに、特にプラス・セキュリティに着目し、産業界が求めるプラス・セキュリティの素養を調査し整理することを目的として、中小企業を含むサプライチェーンを構成する各業界において、プラス・セキュリティに関する取組状況等についてのヒアリング調査を行い、その結果を通じて産業界が求めるプラス・セキュリティのスキル項目と要件等について情報収集・分析する「産業界が求めるプラス・セキュリティに関する調査」を実施した。

※1：経済産業省　サイバーセキュリティ経営ガイドライン Ver2.0 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 第1.1版（2021年4月）
https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf

2.調査概要

2.1 概要

調査概要は以下のとおり。

調査手法	ヒアリング調査　（リモート形式）
調査対象	大企業・中堅企業のIT/セキュリティ統括部門等
調査件数	8件
調査時期	2022年1月～2月
調査実施会社	パーソルテクノロジースタッフ株式会社 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(JTAG財団)
調査項目	プラス・セキュリティに関して、企業のセキュリティ担当者が求める素養や担ってほしいタスクと、現在の教育プログラムや人事配置等の取組状況

2.調査概要

2.2 調査対象

業界、業種、ビジネススタイルが異なる大企業及び中堅企業を選定し、IT／セキュリティ統括部門等へ調査を実施した。

企業名	業種・主たる事業	ヒアリング先の主たる担当業務
A社	金融業（保険）	自社のDX推進と、導入システムのサイバーセキュリティ強化の統括業務を担当
B社	教育、学習支援業	自社の顧客情報を中心とした個人情報の取り扱いに関わるポリシー策定と、運用に向けた関連部門の指導・管理を担当
C社	サービス業（人材）	自社のセキュリティ対策に関わる技術部門の責任者
D社	金融業（銀行）	自行のサイバーセキュリティ対策に関わる中期計画の立案とインフラシステム整備を担当
E社	サービス業（人材）、情報通信業（ソフトウェア開発）	自社の人材育成を中心としたセキュリティに関連する事業の企画立案を担当
F社	運輸業（鉄道業）	自社およびグループ全体のセキュリティルールの策定、社内教育、セキュリティ対策に関わるシステムの導入等の統括を担当
G社	印刷業	自社のサイバーセキュリティ/個人情報保護対策、社内教育を担当する部門の責任者
H社	運輸業	自社のインシデントに関わる全てを統括する部門の責任者

2.調査概要

2.3 調査仮説と調査項目（1/2）

調査は「プラス・セキュリティ」に関する概念について説明を行った上で、以下の項目について実施した。

	調査内容／[仮説]	調査項目
理想の把握	企業が理想とする「プラス・セキュリティ」とは。 [仮説①]セキュリティ担当は、幅広い部門に「プラス・セキュリティ」が必要と考えているのではないか。	① どの部門に「プラス・セキュリティ」が備わっているとよいか。 ② 「プラス・セキュリティ」にどのようなタスクを担ってほしいか。 ③ それらの人材に求めるセキュリティの知識・スキルはあるか。 ④ それらの人材に求められるコンピテンシーは何か ⑤ 「プラス・セキュリティ」の人材に資格・試験は必要か。また、現在の資格・試験で該当するものがない場合、どのような資格・試験制度があれば良いか。
現状の把握	各社はどの程度「プラス・セキュリティ」を実現できているか。 取組を進める上での障壁は何か。 [仮説②]セキュリティ担当の問題意識に対し、他部門では認識がまだ広まっていないのではないか。 [仮説③]必要なスキル等について体系だった整理とそれに紐付く教育プログラムが必要なのではないか。 [仮説④]専門人材やセキュリティ・リテラシーが備わった人材が不足しているのではないか。	⑥ プラス・セキュリティが求められる部門において、どの程度「プラス・セキュリティ」の認識が普及しているか。 ⑦ 事業部門等「プラス・セキュリティ」が求められる部門で、セキュリティタスクを担っていることやその責任が明確化され、本人たちに認識は浸透しているか ⑧ セキュリティが専門ではない社員に対して、セキュリティに関する教育プログラムを実施しているか ⑨ 社員のリスキル、リカレント教育に取り組んでいるか。 ⑩ 「プラス・セキュリティ」を実現するために、人材の流動措置、計画をとっているか。 ⑪ 人材育成にあたり、「プラス・セキュリティ」が求められる部門は、セキュリティ部門と連携した教育・人事配置などが行われているか

2.調査概要

2.3 調査仮説と調査項目（2/2）

調査は「プラス・セキュリティ」に関する概念について説明を行った上で、以下の項目について実施した。

	調査内容／[仮説]	調査項目
解決策	理想と現実のギャップを埋めるために、どのような取組が必要か。 [仮説⑤]これを明らかにすることで、具体的な出口につなげられるのではないか。	⑫「プラス・セキュリティ」の意識や理解を促すために、どのような普及策が効果的と考えるか。 ⑬「プラス・セキュリティ」対象者にはどのような教育プログラムが必要と考えるか。DXやリスクマネジメントとの連動などのニーズはあるか。 ⑭ 教育機関に求める教育プログラム・取組はあるか。 ⑮ 人材の流動化のために必要な施策はあるか。 ⑯ どのような形でスキル・アビリティ・コンピテンシーが整理されていると人材育成という観点から使いやすいか。 ⑰ その他、ギャップを埋めていくために必要な取組はあるか。

3.調査結果(1/3)

調査結果のサマリーは以下のとおりである

	調査結果
理想の把握	**①どの部門に「プラス・セキュリティ」が備わっているとよいか。** 社内のシステム部門、事業部門におけるシステム部門、DX推進部門、事業企画部門、営業部門、法務部門、広報部門、監査部門、部門に限らずマネージャー層、経営層など企業によって異なる回答を得た。また、全ての部門に備わるべきと回答した企業が2社あった。
	②「プラス・セキュリティ」にどのようなタスクを担ってほしいか。 システム部門ではセキュリティを考慮したシステム導入や運用、インシデント対応を担うことが期待されている。また、事業部門ではセキュリティを意識した業務設計や個人情報保護等への対応、セキュリティ管理体制の推進を担うことなどが期待されている。
	③それらの人材に求めるセキュリティの知識・スキルはあるか。 部門や担うべきタスクによって異なるとの回答であった。例えば、法務部門においてはクラウド事業者のチェックやランサムの支払いに関する議論ができたり、データ分析部門においては個人情報保護法に基づく匿名化を行ったり、経営者においてはサイバーセキュリティ経営ガイドラインを理解し実践する能力などが求められる。
	④それらの人材に求められるコンピテンシーは何か。 コミュニケーション力を挙げる企業が多く、その他にマネジメント、ロジカルシンキング、先見性、決断力等が身に付けられていることが求められる。
	⑤「プラス・セキュリティ」の人材に資格・試験は必要か。また、現在の資格・試験で該当するものがない場合、どのような資格・試験制度があれば良いか。 「プラス・セキュリティ」に関する資格・試験が「あったら良い」という回答が多数を占めた。一方で、半数が現在は該当する資格・試験制度が無いと回答した。既存の資格・試験制度であればITパスポート試験や情報セキュリティマネジメント試験が、必要な資格に近いものとして想定されている。

3.調査結果（2/3）

	調査結果
現状の把握	**⑥プラス・セキュリティが求められる部門において、どの程度「プラス・セキュリティ」の認識が普及しているか。** 経営層を含め「プラス・セキュリティ」という言葉自体の認識度合は低い。セキュリティ担当者の中には名称は知っているが、プラス・セキュリティの内容まではあまり理解されておらず、普及しているとは言えない状況である。
	⑦事業部門等「プラス・セキュリティ」が求められる部門で、セキュリティタスクを担っていることやその責任が明確化され、本人たちに認識は浸透しているか。 「プラス・セキュリティ」という言葉の浸透は不充分であるが、果たすべき役割は理解されている。それぞれの業務において必要な「プラス・セキュリティ」は何か、などは整理されていない。
	⑧セキュリティが専門ではない社員に対して、セキュリティに関する教育プログラムを実施しているか。 大企業においては、全従業員を対象に年1回以上実施しており、体制もできている。近年は、標的型メール訓練を含め、インシデント対応訓練を実施しているところも増えている。
	⑨社員のリスキル、リカレント教育に取り組んでいるか。 デジタル人材育成やDX推進を目的としたリスキル、リカレント教育に取り組んでいる企業は多いが、セキュリティが含まれている企業は少ない。
	⑩「プラス・セキュリティ」を実現するために、人材の流動措置、計画をとっているか。 「プラス・セキュリティ」の対象となる人材や組織に対して、プラス・セキュリティを意識した人材の流動化（採用や異動等）はほとんど行われていない。現状はDXの推進が優先されており、「プラス・セキュリティ」人材対象の登用は難しいため、社内人材を育成しているケースもある。
	⑪人材育成にあたり、「プラス・セキュリティ」が求められる部門は、セキュリティ部門と連携した教育・人事配置などが行われているか。 システム部門とセキュリティ部門が情報共有や連携したセキュリティ教育を実施しているが、「プラス・セキュリティ」に関して体系的な教育プログラムはない。

3.調査結果（3/3）

	調査結果
解決策	**⑫「プラス・セキュリティ」の意識や理解を促すために、どのような普及策が効果的と考えるか。** セキュリティの知識およびスキルがあることの証拠的な称号（例：セキュリティマスター）が与えられると良い。そのような人たちが現場の相談事を聞き、アドバイスできると全体的なレベルがあがる。
	⑬「プラス・セキュリティ」対象者にはどのような教育プログラムが必要と考えるか。DXやリスクマネジメントとの連動などのニーズはあるか。 具体的な被害や損害について自分事として理解できるようなリスクマネジメント教育を追加していくことが重要。
	⑭教育機関に求める教育プログラム・取組はあるか。 学校でセキュリティリテラシーやリスクマネジメントの教育があると良い。大学・専門学校での「プラス・セキュリティ」用研修コースの提供やカリキュラム化、共通テストへのセキュリティ項目追加
	⑮人材の流動化のために必要な施策はあるか。 幹部層も含めた中途採用の実施、副業としてセキュリティ専門人材をシェアできる枠組みやIT知識のあるシニア人材の活用ができると良い。
	⑯どのような形でスキル・アビリティ・コンピテンシーが整理されていると人材育成という観点から使いやすいか。 スキルやコンピテンシーなどの整理は自社では難しい。「プラス・セキュリティ」の体系が整理され、業務や役割ごとに必要なスキル・コンピテンシーが整理されていると使いやすい。シンプルなものが良い。
	⑰その他、ギャップを埋めていくために必要な取組はあるか。 社内の人事評価に連動させることができれば職員のモチベーション向上にもつながる。 「プラス・セキュリティ」への取組メリットについて経営者の理解を得ることが重要。

4.考察(1/3)

4.1　プラス・セキュリティの体系化の必要性

- 全ての調査対象においてプラス・セキュリティに関する概念的なイメージを持っているものの、その内容やレベル感については様々であり、プラス・セキュリティに関して体系化を望む声も少なからずあった。
- 調査対象によって内容やレベル感が異なる原因は、どの部門にどのような知識・スキル・コンピテンシーを身に付けてほしいかが異なるためである。この点、企業毎に異なる人材像の設定自体は否定されるものではなく、これら企業において活用可能な形で整理・体系化することは、我が国全体のセキュリティレベル向上に資するものと考えられる。
- なお、ITやセキュリティに関するリテラシーについては、「プラス・セキュリティ」として求められるものなのか、「プラス・セキュリティ」以前に社会人として当然備えるべきものかは、上記体系化の中であわせて整理されることが望まれる。

4.2　プラス・セキュリティが備わっていてほしい部門・人材

- プラス・セキュリティが備わっていてほしい部門について、社内のシステム部門、事業部門におけるシステム部門、DX推進部門、事業企画部門、営業部門、法務部門、広報部門、監査部門などの「部門」のほか、部門に限らずマネージャー層や経営層などの「管理者層」が挙げられた。
- この点、プラス・セキュリティ人材に担ってほしいタスクを問う設問においても、部門毎に担ってほしいタスクと、部門共通で管理者層に担ってほしいタスクが挙げられている。
- これらのことから、「部門」と「管理者層」の双方において求められる知識・スキル・コンピテンシーを明らかにしていくことが求められる。

4.考察(2/3)

4.3　プラス・セキュリティに必要な知識、スキル、コンピテンシー

- プラス・セキュリティ人材に求められるサイバーセキュリティに関する知識やスキルについては、例えば、法務部門においてはクラウド事業者のチェックやランサムの支払いに関する議論ができること、データ分析部門においては個人情報保護法に基づく匿名化を行えること、経営者においてはサイバーセキュリティ経営ガイドラインを理解し実践する能力など、部門や担うべきタスクによって異なる回答があった。
- 一方で、プラス・セキュリティ人材に求められるコンピテンシーについては、コミュニケーション能力を挙げる企業が多く、部門や担うべきタスクに限らず共通して求められるものと考えられる。
- これらのことから、部門や担うべきタスクによって異なる知識・スキル・コンピテンシーと、共通して求められる知識・スキル・コンピテンシーが存在するといえるところ、「部門や担うべきタスク」と「知識・スキル・コンピテンシー」の2軸による整理がプラス・セキュリティの体系化にあたって有用ではないかと考えられる。
- なお、ITパスポートや情報セキュリティマネジメント試験がプラス・セキュリティに関する資格・試験制度として近いものと考えられているため、知識・スキルの整理にあたってはこれら既存試験制度も参考になり得るものと考えられる。

4.考察(3/3)

4.4　プラス・セキュリティに対する体系だった教育の必要性

- セキュリティに関する教育プログラムについて、調査対象となった大企業においては、概ね年間計画を立てて全従業員に対するリテラシーレベルの教育を実施している。加えて、管理者層に対するセキュリティ講習や、IT部門向けにインシデント対応訓練など、プラス・セキュリティという観点での教育を実施する調査対象もあったが、まだ少数である。この点、プラス・セキュリティに関して体系化が行われることは、人材育成の目安となり、プラス・セキュリティに関する教育を実施する企業の拡充につながることが期待できる。また、この教育を担おうとする教育企業や教育機関の充実化により、企業におけるプラス・セキュリティに関する教育の更なる実施増加が期待される。
- デジタル人材育成やDX推進を目的としたリスキル・リカレント教育に取り組んでいる企業は多いが、その中にセキュリティが含まれている企業は少ない。この点、本調査において明らかになったとおりデジタル人材やDX推進人材はプラス・セキュリティが備わっているべき人材と考えられており、現在のリスキル・リカレント教育の対象にセキュリティを含めることには異論がないものと考える。このような教育のためのモデルカリキュラムの作成・提供はプラス・セキュリティに関する教育の推進に資するものと考えられる。