



セキュリティ業務職種のキャリア展望について  
(キャリアデザイン WG 2020 年度成果物)

V1.0

## 目次

はじめに .....	3
1. 『セキュリティ業務職種のキャリア展望について』の作成にあたって.....	4
2. JTAG における WG と 法人(JTAG 財団)の関係性について.....	5
3. JTAG 財団で定める職種について.....	7
4. キャリア相関マップの全体的な考察 .....	11
5. キャリア相関マップの特徴的な点の考察 .....	14
異動や転職の事例 .....	16
6. 技術職から非技術職へのキャリアチェンジの可能性考察 .....	17
ヒアリング結果詳細 .....	19
7. プラス・セキュリティ人材のキャリアチェンジの可能性の考察.....	25
8. 計画的偶発性理論に基づくキャリアの展望 .....	29
1. 分析の目的と背景.....	29
2. 計画的偶発性理論.....	30
3. 調査概要 .....	30
4. 基本属性 .....	31
5. 分析結果 .....	32
6. 業務内容・役割（ラベル）別の傾向.....	33
7. 業務特性（タグ）別の傾向 .....	36
8. 考察と今後の課題.....	38
おわりに .....	39

## はじめに

NPO ネットワークセキュリティ協会（以下 JNSA）の下部組織にあたる、情報セキュリティ教育事業者連絡会（以下 ISEPA）では、「JTAG（ジェイタッグ）」の活動（以下、「JTAG 活動」）を 2017 年より行ってきた。「JTAG 活動」では、社会的課題となっているセキュリティ人材不足の解消、今後も求められるセキュリティ人材の働き方の多様化といった、働きやすさを追求するための様々な活動を行っている。そして昨年、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（「JTAG 財団」）を立ち上げ、今後ますますセキュリティ人材市場への働きかけを行う体制を整えている。「キャリアデザインワーキンググループ」は、これまでの ISEPA「JTAG 活動」の WG としての活動を継続しつつ、「JTAG 財団」との連携により、よりいっそうのセキュリティ人材に貢献する活動を行っていく。

昨年より、COVID-19 の影響で世界には大きな混乱がもたらされ、テレワークやオンライン会議、サテライトオフィスなどを伴う「働き方改革」が多くの企業・組織で導入されている。そして、安全にそれらのツールを導入・運用するためのスキルや、全体の意識改革も必要とされている。AI や IoT などの技術革新と合わせて、『セキュリティ』はテクノロジーと業務運用、リテラシの分野でますますその必要性が高まっている。

その反面、全体的な人材不足は年々進んでおり、経済産業省が 2020 年 1 月 16 日に開催した「第 15 回 産業構造審議会 産業技術環境分科会 研究開発・イノベーション小委員会」では、2025 年には約 45 万人の、2030 年には約 57 万人の AI/IT 人材需給ギャップが生じるとの予測も発表されている。

様々な分野で必要とされるセキュリティ人材をどのように確保するかは、長年の企業・組織における課題といえる。しかし、採用要件やスキルアップフローを具体化できない企業、組織も多いのではないかと。採用側と求職者側で、経験とスキルのギャップや理解不足を解消し、相互に納得した未来を期待できるキャリアパスを共有できることが求められる。

キャリアデザインワーキンググループでは、2019 年の成果物として「キャリアパスグランドデザインの考察」をレポートし、キャリアパス、モデルを「キャリアキューブ」という目に見える形で表すことを提案した。

「JTAG 活動」ではセキュリティが多くの業種・職種におけるキャリアパスに影響を与えるものであることを想定している。キャリアデザインワーキンググループでは、積み上げるキャリアと職種間の相関、次のキャリアにつなげるために必要なスキルには、様々なモデルがあると考えている。これらを丁寧に考察し、ひとつひとつ形にして提示することで、様々なセキュリティ人材の長期的な指標となり、キャリア形成の一助となれば幸いである。

## 1. 『セキュリティ業務職種のキャリア展望について』の作成にあたって

キャリアデザインワーキンググループでは、活動当初からセキュリティ業務に携わる方々の調査<sup>1</sup>を行ってきた。2018年の調査を振り返ると、「セキュリティ業務についたきっかけは時代背景と共にセキュリティの必要性が高まったから」・「人事異動によりセキュリティをするようになった」という意見が見られた。また、そこからのキャリア展望としては、「自分でどうにかするしかなかった」、「自分で勉強などをしてスキルを高めていった」という話をよく聞いた。

セキュリティの必要性が高まる今日において、セキュリティ担当者の不足という状況では、人事異動によりセキュリティ業務につく方も一定数いると想定される。半面、キャリア希望やキャリアアップなど、本人のモチベーションやキャリア形成の多様化を考えると、過去の事例だけではとらわれないキャリアの在り方を考える必要性があるとも言える。さらに、セキュリティ業務からキャリアの開始を希望する方も増えていることだろう。その方々は過去に前例が少ないキャリアの築き方をしていくことになる。

今回のレポートは、2つのテーマでまとめている。

1つ目のテーマは、セキュリティ業務のキャリアアップ・キャリアチェンジの可能性を、実績だけで考えるのではなく、JTAG 財団が定めたサンプルプロファイル<sup>2</sup>を用いて行った。ITSS など指標がいくつかある中サンプルプロファイルを使う理由は、セキュリティ職種以外の IT 専門職が含まれているためである。2019 年に発表した『キャリアパスグランドデザインの考察』<sup>3</sup>で調査したところ、セキュリティ職種だけでキャリアを形成する人は少なく、関連する IT 職種にも従事するケースが多い。そのため、キャリアをより具体的に考察するために、セキュリティ職種とセキュリティ以外の IT 職種が含まれているサンプルプロファイルを活用した。

2つ目のテーマは、「個人のキャリアの8割は、偶然の出来事によって決定される」という計画的偶発性理論を用いて、特性を見ていく。キャリアアップ・キャリアチェンジのタイミングは、外的要因による点も過去のインタビューを見るとポイントだと言える。より良いキャリアを築き活躍していくためには、ある程度の偶然を味方につける必要もあるのではないだろうか。

なお、今回のレポートでは、担当制を用いて執筆している。ワーキンググループメンバーがそれぞれの担当を持ち、活動を行った。調査では、追加インタビューやアンケート、データ分析を行っている。それらをまとめたものが本レポートである。

---

<sup>1</sup> 2018 年上期調査 [https://www.jnsa.org/isepa/images/outputs/JTAGreport2018\\_1H\\_1.2.pdf](https://www.jnsa.org/isepa/images/outputs/JTAGreport2018_1H_1.2.pdf)

2018 年下期調査 [https://www.jnsa.org/isepa/images/outputs/JTAGreport2018\\_2H.pdf](https://www.jnsa.org/isepa/images/outputs/JTAGreport2018_2H.pdf)

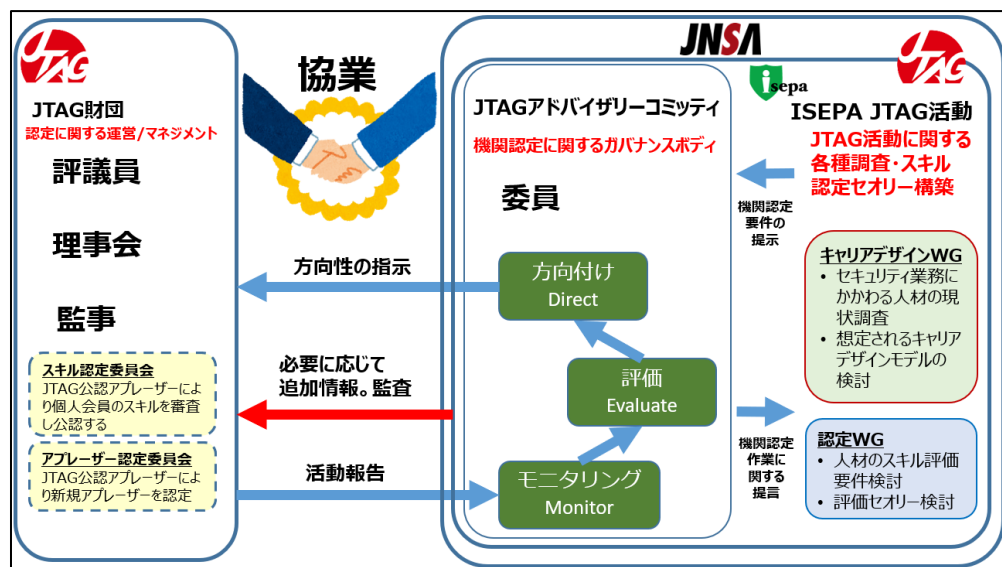
<sup>2</sup> <https://www.j-tag.or.jp/sample-profile>

<sup>3</sup> [https://www.jnsa.org/isepa/images/outputs/JTAGreport2019\\_CD.pdf](https://www.jnsa.org/isepa/images/outputs/JTAGreport2019_CD.pdf)

## 2. JTAG における WG と 法人(JTAG 財団)の関係性について

ISEPA では社会的課題となっている、「セキュリティ人材不足の解消」だけでなく、「今後も求められるセキュリティ人材の働き方の多様化」、「働きやすさの追求」をするための様々な活動を JTAG 活動として行っている。「キャリアデザインワーキンググループ」、「認定ワーキンググループ」のワーキンググループ活動では、調査や分析など研究職の部分を行っており、レポート発表などを行ってきた<sup>4</sup>。

約 2 年の活動により、ワーキンググループで進めていたセキュリティ人材のスキル可視化の考え方がほぼ完成形となった。今後スキル認定などを具体的に推進していくため、2020 年 2 月に JTAG 財団の立ち上げを行った。同年 12 月 25 日には、セキュリティ人材のスキルアセスメントサービス『IT 総合能力診断サービス VisuMe』<sup>5</sup>のリリースとともに、JNSA との協業を発表した。JTAG 財団として新しく立ち上げた理由として、事業色が強い「個人のスキル認定」や「人材流動化サービス」は NPO である JNSA から切り離れた別団体に活動するとしたためである。



参考：NPO 日本ネットワークセキュリティ協会（JNSA）と協業のお知らせ より  
ワーキンググループにて作成

<sup>4</sup> <https://www.jnsa.org/isepa/outputs/>

<sup>5</sup> <https://www.j-tag.or.jp/service>

財団設立に伴い、JNSA 内では JTAG 財団の適正な運用を監督するため、理事会直下の組織として「JTAG アドバイザリーコミッティ」を設置してガバナンス機能を持たせることとしている。

JTAG 財団では、VisuMe のサービス展開やサービスに関係する施策を進めている。

=====

#### JTAG 財団で定める事業概要

当法人は、セキュリティ人材のエコシステムを構築することで持続性の高いセキュリティキャリア形成モデルを支え、適切な人材流動化によるセキュリティ人材の充足を実現することで、社会全体の様々な分野で活躍する専門家のキャリア構造改革において先駆的役割を担うことを目的とします。その目的に資するため、次の事業を行います。

1. セキュリティ人材のスキル認定制度運用
2. セキュリティ人材スキル可視化プラットフォームの各種サービス提供
3. セキュリティ人材育成のための各種教育研修の紹介・斡旋
4. セキュリティ人材のキャリアデザイン調査、需要供給調査・分析
5. 上記に付随した各種コンサルティング
6. その他人材のキャリア基盤拡充、キャリアアップのための活動全般
7. その他前各号に関連する事業

=====

引用：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 事業概要  
(<https://www.j-tag.or.jp/business-summary>)

JTAG 活動の役割分担としては、JNSA ではこれまでどおりスキル可視化のセオリー検討・見直しといった研究色の強い活動を行い、JTAG 財団がスキル診断サービスを事業展開する。ワーキンググループ活動では、調査・分析で終わっていたことが、実際に実行できる環境が整ってきた。スキル可視化およびキャリアデザインの継続研究と、実際の人材流動化を促進する事業活動を車の両輪のように一体運用することができ、社会貢献度が最大化される。そして、双方で連携することで JTAG としての本来の目的である、人材不足の解消・多様な働き方といった流動化を目指していく。

### 3. JTAG 財団で定める職種について

JTAG 財団では、IT 総合能力診断サービス『VisuMe』の提供にあたり、自身の診断結果と比較ができる『サンプルプロファイル』を定義している。サンプルプロファイルは IT 専門職(セキュリティ)が 4 種、IT 専門職 (非セキュリティ) が 25 種、プラス・セキュリティが 11 職種となっている。職種を見ると、数が多いという第一印象を持つはずである。

カテゴリ：領域	分野数	属性
IT専門職 (セキュリティ)	4	セキュリティを専門とするIT業務に従事する人材
IT専門職 (非セキュリティ)	25	セキュリティ以外の分野でIT業務に従事するIT人材
プラス・セキュリティ	11	IT以外の分野でセキュリティに関連する業務に従事する人材

参考：<https://www.jnsa.org/isepa/images/outputs/JTAGreport2019.pdf>

よりキャリアデザインワーキンググループで作成

実際、ITSS+ (セキュリティ領域) では、企業のセキュリティ対策に必要なとなるセキュリティ関連業務のまとまりを 17 分野に整理している。

ITSS+ (セキュリティ)			JTAG 大分類
経営層	デジタル	IT経営 (CIO/CDO)	経営
	セキュリティ	セキュリティ経営 (CISO)	経営 情報システム セキュリティ
	その他	企業経営 (取締役)	経営
戦略マネジメント層	デジタル	システム監査	システム監査
		デジタルシステムストラテジー	IT内部統制 内部統制 IT企画・戦略・予算 BCM・BCP クラウド
	セキュリティ	セキュリティ監査	システム監査
		セキュリティ統括	セキュリティ ITコンサルタント
	その他	経営リスクマネジメント	経営 ITリスクマネジメント リスクマネジメント
		法務	ITリスクマネジメント リスクマネジメント プラス・セキュリティ・法務
		事業ドメイン (戦略・企画・調達)	IT企画・戦略・予算 IT社内「外」教育・インストラクター ITプロジェクト ITコンサルタント
ITSS+ (セキュリティ)			JTAG 大分類
実務者・技術者層	デジタル	デジタルシステムアーキテクチャ	セキュリティ ネットワーク「クラウド含む」 業務系アプリケーション「クラウド含む」 サーバ・ストレージ「クラウド含む」 データベース「クラウド含む」 ITプロジェクト クラウド EA・アーキテクト
		デジタルプロダクト開発	情報システム ネットワーク「クラウド含む」 業務系アプリケーション「クラウド含む」 組み込みソフトウェア開発 サーバ・ストレージ「クラウド含む」 データベース「クラウド含む」 ITプロジェクト
		デジタルプロダクト運用	OA機器「PC・スマホ・タブレットなど」 サービス「ヘルプ」デスク
	セキュリティ	脆弱性診断・ペネトレーションテスト	サイバー攻撃・調査 セキュリティ診断サービス
		セキュリティ監視・運用	サイバー攻撃・調査 SOC CSIRT
	その他	セキュリティ調査分析・研究開発	セキュリティ サイバー攻撃・調査 SOC CSIRT
		事業ドメイン (生産現場・事業所管理)	情報システム ネットワーク「クラウド含む」 業務系アプリケーション「クラウド含む」 組み込みソフトウェア開発 サーバ・ストレージ「クラウド含む」 データベース「クラウド含む」 IT社内「外」教育・インストラクター プリセールス クラウド

ITSS+ (セキュリティ領域) と JTAG 大項目を比較

キャリアデザインワーキンググループで作成

ITSS+と比較をすると JTAG の大分類が複数含まれる項目が存在する。大項目と合わせて小項目が存在する為である。また、実務者・技術者層がより詳細に細分化されているという特徴が見えてきた。JTAG 財団では、『JTAG が対象とするセキュリティ人材は、セキュリティの専門家だけに限りません。企業や組織におけるセキュリティ専門以外の技術担当者や、総務、法務、人事、営業やマーケティングなど IT を利活用し本来の業務を担う際に、セキュリティについて理解を深め自らの業務に活かしていくことを求められる方々もセキュリティを維持するための重要な人材として見える化を実現していきます。また、自組織内のセキュリティ委員や ISMS 担当、責任者など、本務以外の仕事としてセキュリティ系マネジメントの役割を担う方々についてもその範囲としています。』<sup>6</sup>というように、専門職種以外にも目を向けている点がある。

現在、JTAG 財団の Web ページでは、『サンプルプロファイル 大分類：領域・分野について』の説明として、大分類について説明がなされている。各職種がどのように定義されているかは、JTAG 財団ウェブページで確認ができる。

【サンプルプロファイル 大分類：領域・分野についての説明】

検索	
大分類：領域・分野	説明
経営	一人又は複数で構成された、組織に対し経営責任と環境マネジメントシステムの実施に必要な人・物・金の経営資源を配分する権限を持っている人達
情報システム	自組織及び顧客向け情報システムのプロジェクトマネジメント、要件調整、設計、開発、テスト、もしくは保守運用に関する担当
セキュリティ	自組織及び顧客向け情報セキュリティ及び物理セキュリティ業務における企画・製品導入・関係組織との連携・脅威動向調査・インシデント対応・社員の啓発・教育等の担当
サイバー攻撃/調査	自組織及び顧客向け各種セキュリティ機器やサービス、エンドポイント等の監視・分析業務の担当
ITリスクマネジメント	自組織及び顧客向けに対して組織が管理するリスクの中で特に情報化運営に関連するリスクを正確に把握し、包括的且つ適切にコントロールすることで、情報システムの機密性・完全性・可用性を維持し、情報システムを安全に運用する担当
リスクマネジメント	自組織及び顧客向けに組織がビジネスを進めていく中で、事業承継やセキュリティ、内部統制など、経営に影響を及ぼすさまざまな様々な「リスク」を認識、評価し、計画性を持って対応する担当
IT内部統制	自組織及び顧客向け組織などの業務を適正に保つ内部統制の仕組みのうち、情報システムに関連するシステムの維持・運用担当者で、一般的にはIT全社統制、IT全般統制、IT業務処理統制の三段階で構成される
内部統制	自組織及び顧客向け組織がその目的を有効・効率的かつ適正に達成するために、その組織の内部において適用されるルールや業務プロセスを整備し運用すること、ないしその結果確立されたシステムを維持・運用する担当

抜粋：【サンプルプロファイル 大分類：領域・分野についての説明】

(<https://www.j-tag.or.jp/sample-profile>)

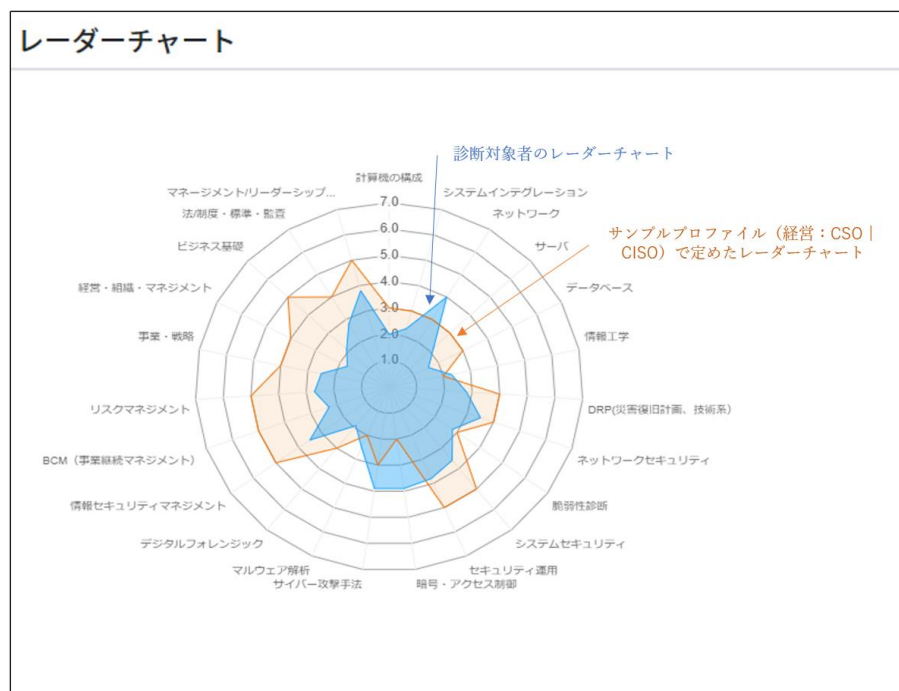
<sup>6</sup> <https://www.j-tag.or.jp/visualization>



セキュリティの仕事というのは多岐にわたる。どのような職種についていくことが良いのかを考えた場合、一つ一つの職種を知ることは非常に有益になるのではないだろうか。

これらの情報を見ると、セキュリティ関係業務と一言と言っても、求められる能力や担う業務内容などの違いが見えてくる。キャリアを築いていくという事を考えた場合でも、セキュリティというひとくくりで話を進めるのではなく、もう少し細かい業種で考えていく事が良いと言える。また、同じセキュリティだからと言って広い範囲の中でキャリアパスを考えると思わぬ落とし穴にはまり、思うようにステップアップできないといったケースも考えられるのではないだろうか。

JTAG 財団ではこれらの職種のスキルバランスをレーダーチャートで表示しており、IT 総合能力診断サービス『VisuMe』において、自身のレーダーチャートと比較ができるようになっている。これにより、現在の自身のスキルと対象職種のスキルのギャップを把握することが出来る。自分が現在対象職種についている場合には、不足するスキルが何かを把握することにつながる。また、今後自分が対象職種につきたい場合には、足りないスキルは何かを考えるきっかけとすることができる。どちらも自身の不足スキルを補う、強みのスキルを磨くといった行動につなげることによって、出来る対象職種を増やしていくことでキャリアアップにつなげることが可能となる。



引用 ; VisuMe で表示されるレーダーチャート

VisuMe を活用し、サンプルプロファイルの対象職種と自身のスキルのギャップを把握することで、職種に対してキャリアを考えることはできてくる。しかし、長期的な視点で、サンプルプロファイルで定めた職種間をどのようにキャリアアップしていくことが望ましいのかは現在定まっていない。今回 JTAG キャリアデザインワーキンググループでは、JTAG 財団で定めたサンプルプロファイルを分析・考察し、対象職種間のキャリアチェンジ・キャリアアップについて考察を行った。JTAG 財団と ISEPA JTAG 活動は今後も連携をとりながら活動をしていくことで、それぞれを補い、よりよい活動につなげていくことが出来る。今後も各調査を行いながら、財団との連携を図っていく。

#### 4. キャリア関連マップの全体的な考察

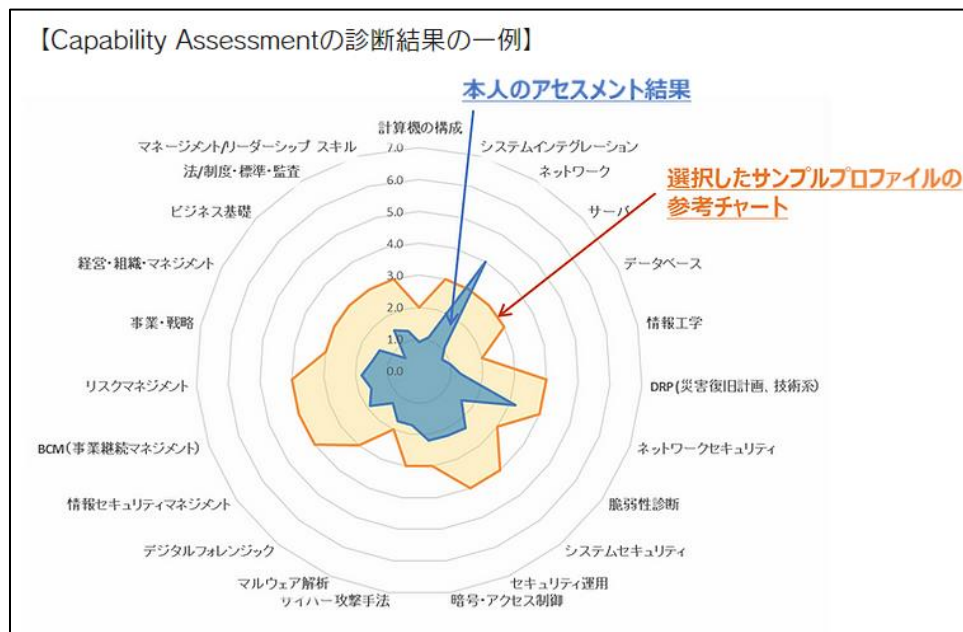
2020 年の活動として、JTAG 財団で定めたサンプルプロファイルで定められている各職種の関係性の調査を行った。

JTAG 財団で定める Capability Assessment（スキル診断）には、23 の評価項目がある。技術基礎から IT 技術、マネジメントと幅広い項目が定められている。

計算機の構成	ネットワークセキュリティ	情報セキュリティマネジメント
システムインテグレーション	脆弱性診断（プラットフォーム、アプリ等共通）	BCM（事業継続マネジメント）
ネットワーク	システムセキュリティ	リスクマネジメント
サーバ	セキュリティ運用	事業・戦略
データベース	暗号・アクセス制御（認証、電子署名等）	経営・組織・マネジメント
情報工学	サイバー攻撃手法	ビジネス基礎
DRP（災害復旧計画、技術系）	マルウェア解析	法/制度・標準・監査
-	デジタルフォレンジック	マネジメント/リーダーシップ スキル

参考：VisuMe よりキャリアワーキンググループで作成

これら項目は、VisuMe 上で評価点を用いてレーダーチャート化されており、自身の診断結果と比較ができるようになっている。これにより自身の不足スキルを把握し、今後のトレーニングなどを検討することが出来る。



引用：<https://www.j-tag.or.jp/use>

今回キャリアデザインワーキンググループでは、サンプルプロファイルの職種間でのキャリアアップ、キャリアチェンジをしていくことを想定した考察を進めた。

#### サンプルプロファイルのキャリアアップ、キャリアチェンジの関係性の考察方法

##### ◆分析手法

JTAG 財団で定めた各職種のサンプルプロファイルに定められたスキル診断評価点を元に職種間の相関を分析

##### ◆分析対象職種

129 職種（プラスセキュリティを除外）

##### ◆まとめ方法

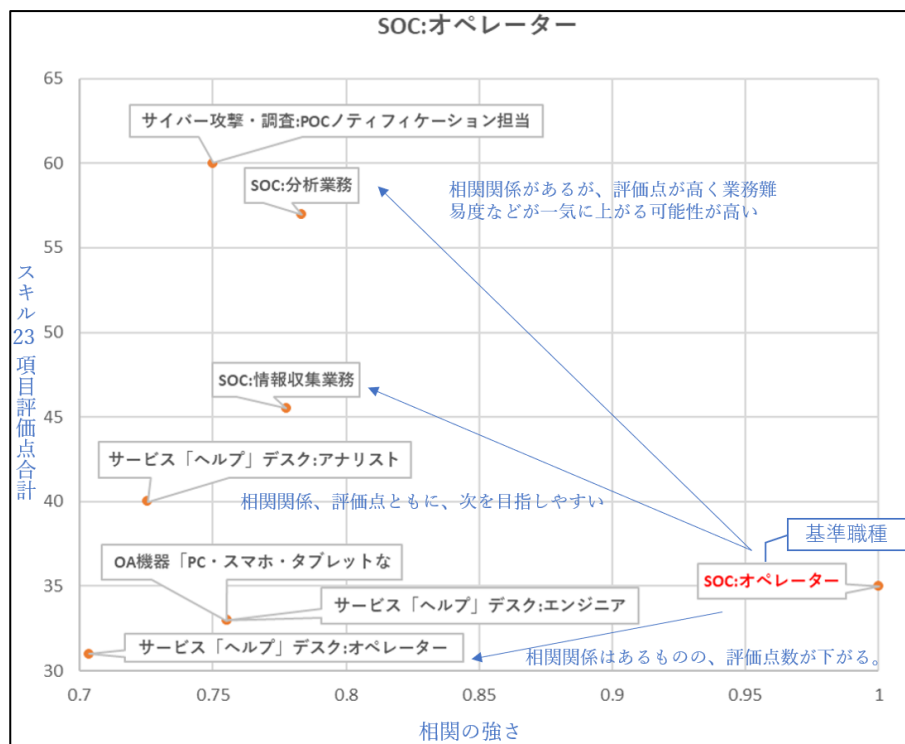
縦軸：JTAG 財団設定のスキル 23 項目の評価点の合計、横軸：相関の強さ

※ 相関の強さの閾値として、0.7 以上と定義

##### ◆考察方法

キャリアデザインワーキンググループにて議論検討

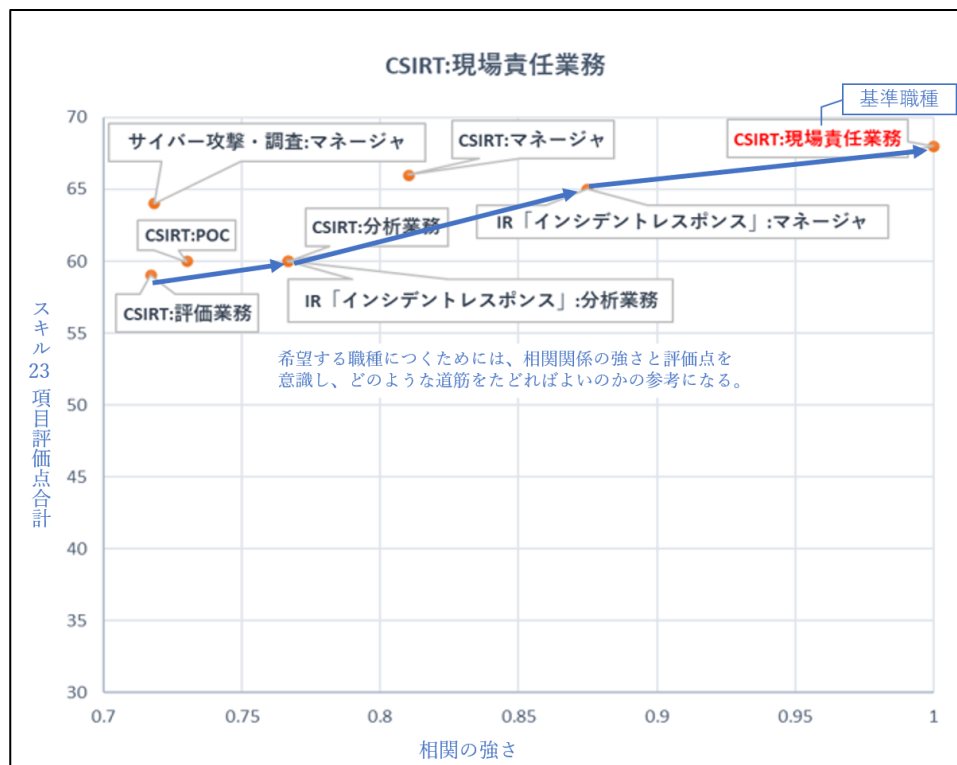
分析の結果、以下のような相関マップを作成した。



SOC オペレーターから見た相関がある職種

サンプルプロファイルよりキャリアワーキンググループで作成

現在従事している職種から次のキャリアパスを描いた際にどのような職種についていくのが良いのかを検討する際に役に立つ相関マップとなる。また、目標とする職種を目指すために、どのような職種を経験していく道筋があるのかを検討する際にも活用できる。



CSIRT 現場責任者から見た相関がある職種

サンプルプロファイルよりキャリアワーキンググループで作成

「セキュリティでキャリアを考えたい」という場合でも、技術系・非技術系、構築開発・分析運用、予防・検知・復旧など業務内容もそれぞれに違いがある。それに伴い、求められるスキルも変わる。これらを把握し、戦略的にキャリアを考察する指標にできる可能性がある。

今回の検討はあくまで評価点上の検討であり、キャリアの具体性等までの調査は各職種においては調査していない。また、サンプルプロファイルで定められている評価点は時代の変化とともに変わる可能性がある。ただし、各職種で見えていくと特徴的な点も見えてきた。「①相関が無い職種・多い職種の考察」「②技術職から非技術職へのキャリアチェンジの可能性の考察」は次節以降でまとめている。また、職種の特異性から、相関分析対象からは除いたプラス・セキュリティ人材について、「③プラス・セキュリティ人材のキャリアチェンジの可能性の考察」として、考察を行った。

## 5. キャリア関連マップの特徴的な点の考察

ここでは関連マップの特徴的な点について考察を進めてみる。

関連マップでは、129 の職種について、現在の職種からどういった職種へのキャリア展開が可能か、もしくは、目指す職種に対してどういったキャリアパスがあるのか可視化されており、組織・個人ともに非常に参考になる内容になっている。

一方で、数値上全く関連関係が算出されないものや、関連が非常に多いものとのばらつきもあるため、個々の職種ごとに検証を試みた。

検証にあたり、これまでに社内異動や転職などで職種を実際に転換してきた事例の有無や、企業が採用にあたり求める要件を参考にしている。

### ◆関連関係が数値上算出されない職種◆

#### 【プリセールス】

プリセールスという職種の性格上、特定の製品やサービスを担ぐことになるが、セキュリティの多層防御が求められている中で、複数製品の最適化提案を求められることは多い。その点を考慮すると、実際にはセキュリティコンサルティングに近い業務を行っているケースが多いと思われる。

ゆえに、エンジニア、ソリューションコンサルタントともに相関性を定義できると推察。ただ、特定の製品・サービス 1 種類のみの経験だと厳しい点もあることから、プリセールスとして複数の製品・サービスを経験することでキャリアの幅が広がるものと捉えたい。

#### 【組み込みソフトウェア開発：エンジニア】

今までにないビジネスやサービス開発にあたり「IoT」を推進するケースが増大してきている。IT 側が OT 側を理解できていないこと、また、逆もあることから、セキュリティエンジニア・コンサルタント双方で組み込み経験者を求めている。実際の異動・転職事例は少ないと思われるが、今後のキャリアパスがあるものとして関連関係があると定義したい。

#### 【オペレーター:ネットワーク、業務アプリケーション、Web アプリケーション】

若年層であれば、このポジションから運用エンジニアへの転身は可能で、その先あらゆるエンジニア職への更なる転身が実現可能と考える。オペレーター → 運用エンジニア → SOC → セキュリティ他職種、といったようにセキュリティ領域への転身も十分あり得る。

## ◆相関関係が多い職種の考察◆

### 【内部統制：全社統制】

上位の職制では様々な職種への相関が高く出ている。

IT 内部統制→IT 職種は十分あり得る。内部統制→プロジェクト：マネージャー（0.87）、業務アプリケーション：マネージャ（0.85）のような内部統制では、IT の知見を多く持たない人もいる。このような場合は、IT 系職種へのキャリア展開は実情難しいと感じる。

### 【WEB アプリケーション「SaaS 含む」：開発エンジニア】

クラウド：アプリケーション（0.93）に対して、IT プロジェクト：システム開発（0.74）は低めの相関値と感じる。システム監査：クラウド監査（0.70）との相関も SaaS 系クラウドであれば数値以上の相関があるものと推察できる。

また、脆弱性診断などセキュリティ職への転身が可能なので相関対象として算出を進めたい。

## ◆相関マップにない職種について◆

AI エンジニアやデータサイエンティストなど、セキュリティ職種として求められるケースが増えている。今後の調査では、こちらも相関対象としていきたい。

## ◆最後に◆

相関マップは、現在の職種からどういったキャリアが展開できるのか非常に参考になるが、上記のように検証を行いながら都度改修を行うことで利用価値がさらに高まると感じた。セキュリティ→セキュリティだけではなく、セキュリティ外→セキュリティの相関も提示しているので、セキュリティに関心を持っている方にぜひ利用を薦めたい。一方で、もともとセキュリティに関心を持っていない方が異動以外でセキュリティ職務につくことがほぼないことも判明した。

セキュリティを取り巻く環境も日々変化しているので、セキュリティ以外の職種からどういったキャリア展開ができるのか、その職務や役割の魅力も含めて発信していくことが肝要であると感じた。

また、相関関係が数値上ない職種なども判明した。これらの結果は JTAG 財団とも連携をして行く。併せて、AI エンジニアやデータサイエンティストなど、これから主流になるものを早期にとらえ、JTAG 財団へ提起していく。

## 異動や転職の事例

以下にヒアリングで確認できた異動や転職の事例を記載する。

ヒアリングは、3名（約30分）・メール回答1名に実施した。なお、今回お話を伺った人たちは、転職支援を行っている10年以上のアドバイザー経験を有している。

### 「異動事例」

- ・情報システム→事業企画、経営企画
- ・情報システム→バックオフィス
- ・事業企画→IT企画
- ・SE→企画

### 「転職事例」

- ・業務コンサルティング→ガバナンス、リスク
- ・知財（技術）→コンプライアンス
- ・PMO→事業企画、内部統制



## 6. 技術職から非技術職へのキャリアチェンジの可能性考察

技術職から非技術職へキャリアチェンジした方へインタビューを中心として話を聞き、実態をまとめた。調査内容は以下の通り。

### ■ヒアリング項目

- 1 技術職→非技術職へシフトした経緯、きっかけ
- 2 技術職・非技術職でのやりがい
- 3 技術職で得られた知見を今どのように活かしているか
- 4 今後のキャリアパス
- 5 同領域における高パフォーマンス者の特徴

### ■調査機関

2020 年 10 月～2021 年 1 月

### ■調査実施方法

該当者への対面 or リモートインタビュー

### ■調査対象人数

12 名(平均年齢 43 歳)

### ■インタビュー時間

各 30 分程度

### 考察のまとめ

ここ 3, 4 年の技術の変化などの時代背景がある中で、技術レベルが追い付かずキャリアチェンジする方はいなかった。会社指示でチェンジする方はいたが、現業務での評価が上がりマネジメントへチェンジを打診される方が多かった。又、本人が希望してチェンジする方もいた。

技術職のやりがいについては、今までできなかったことができるようになったこと、作りたいものを作れたことにやりがいを感じるといった回答が多かった。一方で、非技術職のやりがいは、自分視点ではなく周囲からの感謝がやりがいに繋がっているといった特長が多かった。

技術職の経験は、非技術職でも活かされているという回答も多く見られた。技術職の経験は、「現場のことが分かる」・「気持ちが分かる」といったような、寄り添った会話やアドバイスができるといった回答から、技術的な面よりも気持ちの面で活かされているという事が分かった。

今回のヒアリングでは 30 代後半から 40 代前半メンバーが中心で、今まで 3～5 回職場・業務内容を変えている方が多いことも影響があったのか、再び技術職に戻りたいという方はいなかった。現業務の継続や、技術を“活かせる”マネジメント業務、コンサル業務、経営戦略とい

う回答があり、技術職に戻りたいという気持ちは無いが、技術職で培ったスキルや経験を活かせる業務を行いたいという方がほとんどだった。また、技術を全く活かさない業務に就いている方は今回の対象者にはいなかった。今後も技術職に戻ってもついていけない、大変そうという発言は一部あったが、技術を活かした非技術職業務にやりがいを感じている方が殆どだった。最後に、同領域における高パフォーマンス者の特徴は、「コミュニケーション力」、「推進力」、「柔軟性」がある方が多かった。また、自分自身の能力やスキルを把握しており、キャリアビジョンや今後やりたい事が、見えている方が多いという特徴があった。特に主体的に動いている方が成功しており、今後キャリアチェンジをしようと思っている方や人事の参考になれば幸いである。

## ヒアリング結果のまとめ

主な質問内容	サマリー	回答例抜粋
キャリアステップ	<ol style="list-style-type: none"> <li>1. 技術職→マネージャー/プリセールス・コンサル</li> <li>2. 技術職→面談・カウンセリング・人事</li> </ol>	インフラエンジニア→PM (Project Manager) →SM (Service Manager) →営業→人事
技術職→非技術職へシフトした経緯、きっかけ	<ol style="list-style-type: none"> <li>1. 会社からの指示や案件状況によりシフト</li> <li>2. 希望。スキルの幅を広げたい</li> </ol>	テクニカルサポートを行っている際にクレーム対応や顧客対応が評価されチームリーダーへ。その後インフラ系チームを任せられマネージャーとなった。(現業での活躍が評価されマネジメント業務)特に忌避感はなく、給料が上がるならやろうかなという感じだった。自分の特性も考えコミュニケーションやマネジメント力を活かした業務に就きたかった。技術を突き詰めることに限界を感じた。マネジメントやコンサルができることもお客様の為になると感じたから。
技術職・非技術職でのやりがい	<ol style="list-style-type: none"> <li>1. プロジェクトの成功、周囲からの称賛。感謝</li> </ol>	技術職：何かができるようになった喜びがある、作りたいものが作れた時。 非技術職：一時は退職も考えていたが、今まで一番良い PM と周囲の方々に称賛された。もう少し一緒に頑張りましょう」などとメンバーに励まされて嬉しかった。

主な質問内容	サマリー	回答例抜粋
技術職で得られた知見を今どのように活かしているか	1. 技術者の立場に立てる	現場経験があると、現場のことが分かる、気持ちが分かる。寄り添った会話やアドバイスができる
今後のキャリアパス	1. 技術に継続して携わりたい 2. 技術適正が無いので、非技術職の部分で考えたい	今後も引き続き技術には携わっていきたい。しかしながら年齢・経験も含め会社に期待されていることも理解はしているので、そちらもこなしていく。ただし、マネジメントだけをやっていくのはつまらないと感じている。SEとしての技術を生かしながら会社に貢献できることを考え、実行していく。
同領域における高パフォーマンス者の特徴	1. コミュニケーション能力 2. 大きな失敗経験がある 3. 経験に基づく戦略が立てられる	コミュニケーション力がある。推進力がある。コミュニケーション力がなくても進んでいける方、周りを巻き込む力がある方は、成功している方が多い。

## ヒアリング結果詳細

### ■ケース1：

技術→マネージャー/プリセールス

#### 【1 技術職→非技術職へシフトした経緯、きっかけ】

会社の業務命令

#### 【2 技術職・非技術職でのやりがい】

仕事自体が面白いと思っているから、技術職・非技術職関係なくやりがいを感じている。

#### 【3 技術職で得られた知見を今どのように活かしているか】

仕事の整理をする時、人の管理をする時、マネジメントをする際に活かされている

#### 【4 今後のキャリアパス】

業務命令に従って会社の事業体に合わせてやらなければならないことを実施する

#### 【5 同領域における高パフォーマンス者の特徴】

会社との関係が良好な方。会社に対するロイヤリティが高い方。技術的経験を活かしたマネジメントが強みだが、モチベーターは少ない。マネジメントする際はそこが課題と上げている方は多い。

## ■ケース 2：

技術→マネージャー/プリセールス

### 【1 技術職→非技術職へシフトした経緯、きっかけ】

企業起点 & 自己起点の両方。上長からエンジニア+実施責任者や SM として幅広く経験できるからと言われた（企業起点）。エンジニアはある程度経験を積んだので、違うことをしてみたいと思い自分もやりたいと思った（自己起点）。技術のみスキルアップしていくよりも、人の育成やキャリアマネジメントに向いていると思った。スキル＝単価という印象で、技術力もそれほどないし単価はあがるが今後を見据えた時それ以上のものがあまり考えられず、それだけだとエンジニアとしてのキャリアが狭まる。それよりも技術経験を活かして、さらに視野・幅を広げていくことのほうがキャリアとしての方向性が広がると思った。

### 【2 技術職・非技術職でのやりがい】

自分だけが対象ではなく、他のメンバーにやってもらうことでプロジェクトは回っていくが、それがうまく動いているときにやりがいを感じる。プレイヤーだと他メンバーのやっている内容、状況、意味などが理解できていないケースが多く、うまく合わない人への拒絶反応がありもどかしさを感じることもある。しかしながら、マネージャーの立場であれば、全体を客観視し、動きをみてコントロールすることができ、自分にそれが向いていると実感できる。

### 【3 技術職で得られた知見を今どのように活かしているか】

実務経験としての技術知識や経験などから、さらに人事的な部分への派生ができています。顧客やエンジニアなど同じ目線で物事をとらえて考えることができる。例として、案件拡大、メンバーアサイン、メンバーからの相談事項（エンジニア目線で考えられる）などに活かされている。同じ目線で顧客やメンバーの理解や気持ちがわかるので、例えば営業に対してエンジニア事情を共有することで、何が大変なのかを伝えた上で提案しやすくなる。また、クレームや提案時の顧客への共感ができることで、いろいろと対応しやすい。

### 【4 今後のキャリアパス】

通信キャリア系のプロジェクトが多かったので、別の業界・分野での業務も行い、マネジメント力をさらに強化し伸ばしていきたい。

### 【5 同領域における高パフォーマンス者の特徴】

コミュニケーション力が高い。

- ヒアリング力（顧客やメンバーからのニーズヒアリング力）

- トーク力（提案など相手にきちんと伝える、伝わる）

数字に強い（事業計画など）。

例）予算をもとに提案や事業計画であればいくらの案件を受注しないといけないなど、数字にきちんと繋げて考察できる

### ■ケース 3：

インフラエンジニア→PM (Project Manager) →SM (Service Manager) →営業→人事

#### 【1 技術職→非技術職へシフトした経緯、きっかけ】

会社異動、業務命令。常駐していた案件が炎上していて PM をやらざるを得なかった。SM になったのは自分の意志、PM をやっていて技術者よりもマネジメントの方が向いていると思ったから。営業になったのは、契約管理や営業行為を学びたかった。スキルアップしたかったため。人事を希望したのは、育成に興味があったから。

#### 【2 技術職・非技術職でのやりがい】

技術職は、何かができるようになった喜びがある、作りたいものが作れた時。非技術職は PM 時に周りのメンバーの方々に称賛された時。「一時は退職も考えていたが、今まで一番良い PM。もう少し一緒に頑張りましょう」などとメンバーに励まされて嬉しかった。

#### 【3 技術職で得られた知見を今どのように活かしているか】

現場経験があると、現場のことが分かる、気持ちが分かる。寄り添った会話やアドバイスができる。

#### 【4 今後のキャリアパス】

2つある。

一つは人事をやるにも知識やスキルが足りない。もう1回現場に戻って、現場のスキルをつけたい。特にコンサル系業務。もう一つは人事の知識を上げて、ラインマネージャーを目指す。

#### 【5 同領域における高パフォーマンス者の特徴】

コミュニケーション力がある。推進力がある。コミュニケーション力がなくても進んでいける方、周りを巻き込む力がある方は、成功している方が多い。

### ■ケース 4：

技術職 → リーダー → マネージャー

#### 【1 技術職→非技術職へシフトした経緯、きっかけ】

20代は開発系 SE、その後テクニカルサポートなどを行っている際にクレーム対応や顧客対応が評価されチームリーダーへ。その後インフラ系チームを任せられ、マネージャーとなった。マネジメント業務に関しては特に忌避感はなく、給料が上がるならやろうかなという感じだった。

#### 【2 技術職・非技術職でのやりがい】

現状は少人数のため、メンバーと一緒に頑張ってプロジェクトを回しており、プロジェクトが成功することに対し手喜びを感じる。また、メンバーの成長を見ることにも喜びを感じている。マネジメントも面白いが、それだけをやりたくないわけではなく、一部でもいいから手を動かして

いたいという思いはある。技術面でもメンバーを引っ張っていきたい。

【3 技術職で得られた知見を今どのように活かしているか】

バリバリの SE をやろうとしても、必ず顧客との対応等コミュニケーションを要求される場に引っ張られるケースが多かった。これにより、社内、ベンダー、顧客などとのコミュニケーション力が磨かれ、現場やシステムのことを理解しながら案件獲得やプロジェクトマネジメント、チームマネジメントができていく。

【4 今後のキャリアパス】

今後も引き続き技術には携わっていきたい。しかしながら年齢・経験も含め会社に期待されていることも理解はしているので、そちらもこなしていく。ただし、マネジメントだけをやっていくのはつまらないと感じている。SE としての技術を生かしながら会社に貢献できることを考え、実行していく。

【5 同領域における高パフォーマンス者の特徴】

1 回は何か大きな苦勞をしてきている。何かを行うときに、きちんとリスクも含めて考えられる。いろいろな経験をしてきているので、こういったことが考えられる。

■ケース 5：

技術職(ヘルプデスク) →リーダー→マネージャー (プリセ) →コンサル

【1 技術職→非技術職へシフトした経緯、きっかけ】

20 代はヘルプデスク、資産管理系プロジェクトの責任者を経験。その後は会社指示、会社都合で非技術職領域へシフト。

※HD (メンバー) 半年案件終了→同企業 資産管理 PJ (責任者) IT 離れ→社内アシスタント SM1 年半→HD (LD) →在宅支援センター (センター長) →SM→コンサルタント

【2 技術職・非技術でのやりがい】

技術職 (OA 関連 HD) は、PC 周りであってもできることが多いこと分かった時 (Excel、PC 設定) 非技術職は、PJ 目標 (金額・ゴール目的) が定められている期間より前に達成したとき、チームとしてアウトプット出さなければならない状態は特に。

【3 技術職で得られた知見を今どのように活かしているか】

技術職領域での職務経験はあまりなく活かしていないが、現場経験がマネージャーとしてマネジメントをする上で活かしている SE 経験がない人がマネージャーになることも可能ではあるが、表面的なところしか管理できない可能性がある。また、メンバーからしても経験者がいると安心感がある。

【4 今後のキャリアパス】

技術職領域は適性が無いと感じる。役職には興味無い。人財開発には興味あり。ある程度給

与をもらえて、チームマネジメントに携われるポジションでキャリアを積みたい。

【5 同領域における高パフォーマンス者の特徴】

技術・非技術共通：能動的、与えられたタスクの目的が分かっていて、コミュニケーション能力がある方

■ケース 6：

開発 → 小規模チームリーダー → SM → マネージャー

【1 技術職→非技術職へシフトした経緯、きっかけ】

開発者として活動していたが、3 年目くらいから新卒の育成の役割で小規模なチームリーダーを任されるようになった。その後 7 年目くらいまではチームの規模が拡大。転職し、ある注力プロジェクトのプロジェクトリーダーを経て、PM、SM、マネージャーへと至る。

【2 技術職・非技術職でのやりがい】

マネージャーとしてのモチベーションは、チームメンバーが楽しく仕事ができている様子を見ること。メンバーが自分の能力を発揮しやすい環境を作ってあげることが重要だと感じている。技術に対してのこだわりはそれほど強くはないが、自分ができることがどれだけ広がるか、それにより自分の視野がどれだけ広がるかには興味がある。

【3 技術職で得られた知見を今どのように活かしているか】

技術職を経験してきた管理者は、技術を身に着ける苦労をわかっており、現場の言い分が理解できる。それに引きずられすぎることには注意が必要だが、技術をわかっていない管理者は話が通じないことがある（経験談）。技術職メンバーの管理職は技術職上がりの人がいいと思う。

【4 今後のキャリアパス】

ラインマネージャーにはそれほど興味がない。どちらかというと現場に近いマネジメントをしていきたい。その後は出来れば IT コンサルが行えるようになりたい。

【5 同領域における高パフォーマンス者の特徴】

居心地がよかったプロジェクトのマネージャーは、物事を判断する価値観をチームに合わせている。

自分ができるからできるはずという考え方で進められると、メンバーとしてはつらく、モチベーションが上がらないことがある。

■ケース7:

IT コールセンター(メンバー→SV→責任者)5年→クラウドサービスインフラ運用(メンバー)  
⇒サービスマネージャー→コンサルタント

【1 技術職→非技術職へシフトした経緯、きっかけ】

IT マネジメント側に移りたい希望が元々あった。やっていくことが上流工程へ。 自然の流れで非技術職へシフト。エンジニアとして技術追求するよりも、人活かすほうが上向いていると思っていた。

【2 技術職・非技術職でのやりがい】

技術職：IT スキル向上。資格勉強。お客さん（やエンド）やメンバーからの感謝。直折衝により。非技術職：成果、数値。安定運用。メンバモチベーション

【3 技術職で得られた知見を今どのように活かしているか】

インフラ技術が分かることがプロジェクトに貢献する上で役に立っている

【4 今後のキャリアパス】

コンサルタントを極める。または、研修内製化、ローテーションの仕組み作り等、当社エンジニア活かせる土台作り、支援担当。

【5 同領域における高パフォーマンス者の特徴】

共通：1 言ったら10を理解する。物事を俯瞰して考えられる。先を見据えた回答をくれる

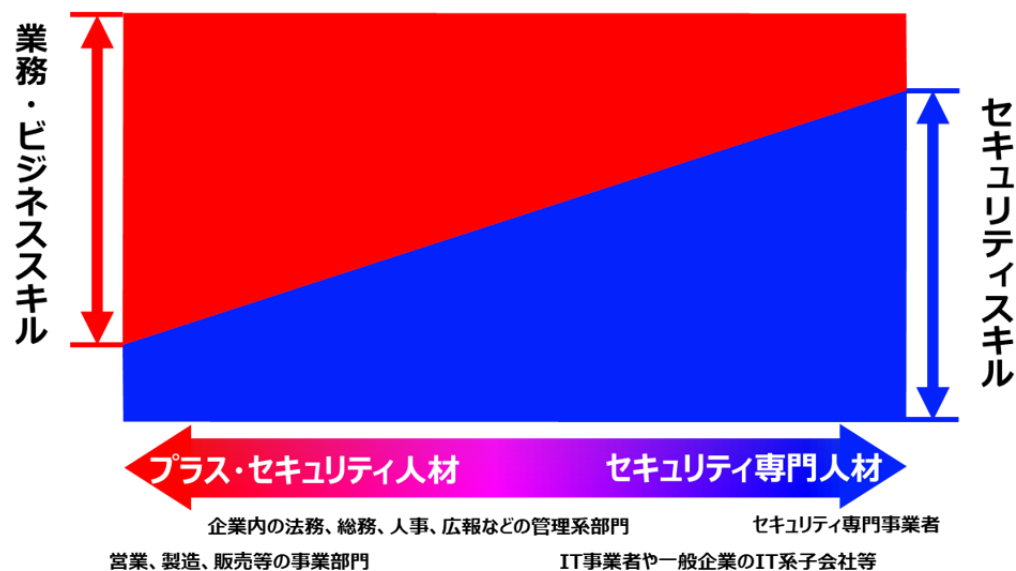


## 7. プラス・セキュリティ人材のキャリアチェンジの可能性の考察

プラス・セキュリティ職からセキュリティ職へのキャリアチェンジの可能性を調査するために、アンケートおよびインタビューを実施し、その結果や考察をまとめた。

### 1. プラス・セキュリティ人材の定義

JTAG では、セキュリティ人材をセキュリティの専門家だけに限らないと考えている。企業や組織におけるセキュリティ専門以外の技術担当者や、総務・法務・人事・営業など IT を利活用し本来の業務を担っていく必要がある。セキュリティについて理解を深め、自らの業務に活かしていくことを求められる人材も、セキュリティを維持するための重要な人材として考えられる。また、自組織内のセキュリティ委員や ISMS 担当・責任者など、本務以外の仕事としてセキュリティ系マネジメントの役割を担う人材についてもその範囲としている。このような事業運営におけるあらゆる業務に対してセキュリティも知っている人材を「プラス・セキュリティ人材」と定義している。



引用：JTAG 財団の定義するセキュリティ人材とは？

(<https://www.j-tag.or.jp/visualization>)

## 2. アンケートおよびインタビュー結果のまとめ

今回、プラス・セキュリティ職からセキュリティ職へキャリアチェンジの経験がある7名にアンケート、4名にインタビュー（各30分程度）を実施した。アンケート、インタビューの質問項目は下記の通りである。

No.	質問内容
1	現在の業務
2	過去に経験したプラス・セキュリティ職
3	プラス・セキュリティ職から異動直後に就いたセキュリティ職
4	3の職種（プラス・セキュリティ職から異動直後に就いたセキュリティ職）に就いたとき、どのように知識や技術を学んだか
5	3の職種（プラス・セキュリティ職から異動直後に就いたセキュリティ職）に就いたきっかけ
6	2での経験（プラス・セキュリティ職）でセキュリティ職に役立ったこと
7	「セキュリティ職」に初めて就いて大変だと感じたこと
8	「セキュリティ職」をしていて良かったと感じたこと
9	「セキュリティ職」をしていて悩むこと
10	「セキュリティ職」に就いて、報酬や評価に変化はあったか
11	「セキュリティ職」に就いたことにより今後のキャリア(観)に影響を与えているか
12	今後のキャリアパス

ここからは回答の中で、特徴的であったものを4点記載する。

### 1. セキュリティ職に就いたきっかけ

回答者のほとんどは「会社からの異動命令」がきっかけでセキュリティ職に就いている。

### 2. セキュリティ職に就いた後の待遇（報酬や評価）の変化

全員が共通して「セキュリティ職に就いたことでの変化は、特になかった」と回答があった。

### 3. セキュリティ職に就いて“大変だ”と感じたこと

新しい知識やスキルを身に付けること、情報収集が大変だという回答が多く見られた。さらに、これからセキュリティ職を目指す人に向けて、「セキュリティ職では、幅広い技術の習得が必要であるため、教育体制が整っている会社に就職することを勧める。」「日々勉強の仕事。飽きっぽい人には向いているかもしれない。」「様々なことを経験でき、キャリアパスも沢山ある。」といった内容のメッセージを複数いただいた。

#### 4. 今後のキャリアパス

全員が「引き続きセキュリティ職に従事したい」という回答であり、セキュリティ以外の業務に就きたいという回答はなかった。具体的には、セキュリティの知識を活かして経営陣への橋渡しとなれるような業務をしていきたい、新規企画立上げや教育に携わりたい、より専門性の高い業務に就きたいといったものがあった。

#### ※その他の特徴

インタビューを行なったうちの2名は、セキュリティ職にすぐに就くのではなく、データセンター運用の経験があった。そこでの経験を経て、セキュリティ意識や知識（物理セキュリティ等）がついたと回答している。このように、セキュリティ職にすぐに就くのではなく、運用業務などでセキュリティを学び、その後にセキュリティ職に就くというキャリアパスもあるということが分かった。

さらに、プラス・セキュリティ職の経験で役立ったことについて、インタビューを行なったうちの2名は、それぞれITスクール、塾での講師経験があり、その経験が業務に役立ったと回答している。インシデント発生時に分かりやすく説明する際に役立った、塾で英語を教えたので海外ベンダーとやり取りする際に役立ったと回答があった。このように、プラス・セキュリティ職で培ったスキルはセキュリティ職に様々な形で活かしているということが分かった。

### 3. 考察

今回の調査のために JNSA 会員・キャリアデザイン WG 参加企業の皆さまに協力いただき、アンケート/インタビューを実施したが、本アンケートの対象者に該当する人が少なく、なかなか回答を集めることができなかった。

例としては、協力いただいた企業の中の1社では、社員約4500名のうち対象者は10名程との確認であった。

少ない理由として、「IT＝専門職」といったイメージや新しい知識・スキルを身に着けることのハードルの高さが考えられる。また、自組織内のセキュリティ委員やISMS担当など、本務以外の仕事としてセキュリティ系マネジメントの役割を担うプラス・セキュリティ人材には、本務の仕事があるため、自らの意思で、セキュリティ職へキャリアチェンジすることが難しいのではないだろうか。実際、今回の調査でもセキュリティ職に就いたきっかけの多くが「会社からの異動命令」であった。

#### 4. まとめ

プラス・セキュリティ職からセキュリティ職へのキャリアチェンジの可能性を調査し、数は少なかったが、実際にキャリアチェンジをして、現在セキュリティ職で活躍されている方のお

話を聞くことができた。また、プラス・セキュリティ職で培ったスキルが現在の業務にどのように活かしているかという話は、これからセキュリティ職を目指す人にとって参考になれば幸いである。

今後、プラス・セキュリティ職からセキュリティ職へキャリアチェンジする人の増加のためには、会社の異動命令といった受動的なきっかけではなく、自身の意思でセキュリティ職に就くことを希望するといった能動的なきっかけが増えることが必要なのではないだろうか。そのために、「IT に関する業務の経験があるから、セキュリティ職に就く」というルートだけでなく、「性格的に向いている（資質がある）かもしれないから、セキュリティ職に挑戦してみる」というルートがあってもよいと考える。

JTAG 財団のサービス「IT 総合能力診断サービス VisuMe（ビジュミー）」では、2 種類の診断を実施し、人材の能力・コンピテンシーの見える化を実現している。また、キャリアデザイン WG では、キャリアの指標作成や計画的偶発性理論に基づくキャリアの調査を行っている。このような VisuMe の診断結果と WG の調査結果から、自身に向いている職種・向いていない職種を知ることができたら、キャリアの選択肢や可能性が広がるのではないだろうか。今後、より人材の流動化を促進できるように、VisuMe のサービス開発および、WG の調査、それらの連携を進めていきたいと考えている。

## 8. 計画的偶発性理論に基づくキャリアの展望

### 1. 分析の目的と背景

セキュリティ人材へのキャリアチェンジについては、「セキュリティ業務を担う人材の現状調査」(ISEPA,2019)<sup>7</sup>のインタビュー(表1)より、「職場の配属」、「上司からの指示」、「現業業務でセキュリティの業務が必要になった」など、最初から自らが意志をもってキャリア選択した人だけでなく、偶発的な出来事からセキュリティ人材としてのキャリアをスタートした方が一定数いることが示された。

- |   |   |
|---|---|
| A | 自分の意志というよりも、配属されたからという要素が強い。データセンターでのセキュリティ担当になったことからセキュリティのキャリアがスタートした。」   |
| B | 情報システムの運用に携わる中で必然的にセキュリティ業務も担当していくようになった。したがって、何かをきっかけでセキュリティ業務を担当するといったわけではない。                                     |
| C | 積極的にセキュリティ業務を指向したわけではない。人事異動の結果、システムリスク管理部門での勤務を経て、現在のセキュリティ統括部門に移ってきた。ただし、嫌々やっているわけではなく、これまでの社会人経験の中では現在が最も充実している。 |
| D | 上司の指示でセキュリティ業務についた。当時は全く興味がなかったが今となってはやりがいを感じている。   |

表1 セキュリティ業務を担う人材のキャリア選択 (インタビュー内容)

そこで、本調査では、キャリア理論の「計画的偶発性理論」で定義されている5つの行動特性に着目し、変化の激しいセキュリティ人材の行動特性及びセキュリティ人材のラベル別(職種別)の特性をアセスメントデータから明らかにすることを試みた。

<sup>7</sup>特定非営利活動法人 日本ネットワークセキュリティ協会 情報セキュリティ教育事業者連絡会 (ISEPA) (2019) セキュリティ業務を担う人材の現状調査報告書 <https://www.jnsa.org/isepa/images/outputs/JTAGreport2018.pdf>

## 2. 計画的偶発性理論

計画的偶発性理論 (Planned Happenstance Theory) は、心理学者のジョン・D・克蘭ボルツによって 1999 年に提唱されたキャリア理論である。克蘭ボルツがビジネスパーソンとして成功した人のキャリアを調査したところ、そのターニングポイントの 8 割が、本人の予想しない偶然の出来事によるものであった。克蘭ボルツは、「不確実な出来事を学習の機会へと創造し変換する重要性」を述べ、キャリア開発においてチャンスとなる出来事を自ら起こし、認識し、受け入れ、創造し、活用することを支援する行動特性として下記の 5 つを挙げた<sup>8</sup>(表 2)。

1	新たな学習機会を模索する「好奇心 (Curiosity)」	新しいことに興味を持つ
2	めげない努力を示す「持続性 (Persistence)」	失敗してもあきらめない
3	態度や状況の変化を示す「柔軟性 (Flexibility)」	柔軟な姿勢をとる
4	新たな機会を実現可能と捉える「楽観性 (Optimism)」	何事もポジティブに
5	不確実な結果に対する行動を示す「冒険心 (Risk Taking)」	挑戦する

表 2 計画的偶発性理論における行動特性

## 3. 調査概要

本調査は、2019 年 11 月 25 日 日本ネットワークセキュリティ協会 情報セキュリティ教育事業者連絡会 (ISEPA) JTAG 認定 WG グループ「セキュリティ業務を担う人材のスキル可視化における概念検証報告書 ～トライアル結果の考察～」<sup>9</sup>のデータを元に分析を実施したものである。

- ・実施期間：2019 年 7 月～9 月
- ・方法：ネクストエデュケーションシンク社 (以下、NET 社) が提供する JTAG コンピテンシー診断 (WEB 診断 2 種類)
- ・対象：JTAG 会員企業 12 社 N=244 名

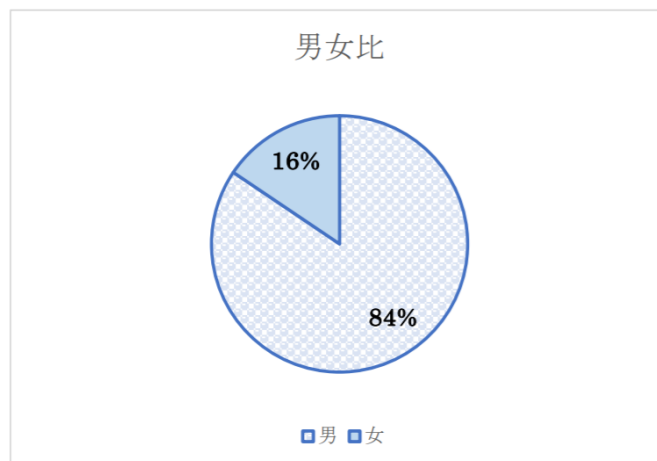
また、計画的偶発性理論の 5 つの行動特性については、JTAG コンピテンシー診断 (①行動特性②適性資質) から、類似概念の項目群を選定し、これらと計画的偶発性理論の 5 つの行動特性との対応関係を検討した上でスコア化を試みた。

<sup>8</sup> 岡田昌毅 (2013) .働くひとの心理学 ― 働くこと、キャリアを発達させること、そして生涯発達すること ― ナカニシヤ出版

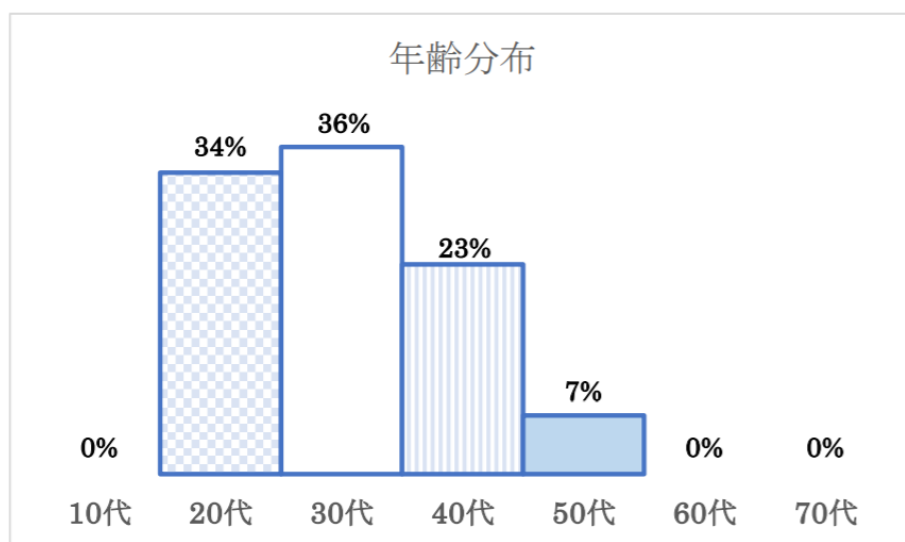
<sup>9</sup>日本ネットワークセキュリティ協会 情報セキュリティ教育事業者連絡会 (ISEPA) JTAG 認定 WG グループ (2019) .セキュリティ業務を担う人材のスキル可視化における概念検証報告書 ― トライアル結果の考察 ―  
[https://www.jnsa.org/isepa/images/outputs/JTAGreport2019\\_trial.pdf](https://www.jnsa.org/isepa/images/outputs/JTAGreport2019_trial.pdf)

#### 4. 基本属性

調査対象者の基本属性については、性別では男性が大半を示し（約 84%）、年齢構成としては 20 代～30 代で約 70%を占める結果となった。



男性 84%（204 名） 女性 16%（40 名）



20 代 34%（82 名）、30 代 36%（89 名）  
40 代 23%（57 名）、50 代 7%（16 名） 計 244 名

## 5. 分析結果

5つの行動特性について、企業内で成果をあげている高業績者を「ハイパフォーマー」と定義し、①ハイパフォーマー、②非ハイパフォーマー、③全国平均で比較をおこなった（図1）。全国平均は、セキュリティ人材に限定せず、様々な職種を含むNET社が保有するデータから算出したものを示す。

業務内容・役割を特定せず、セキュリティ人材を一括りに纏めた場合では、属性別で、行動特性のスコア平均について大きな傾向の違いは示されなかった。また、ハイパフォーマーと非ハイパフォーマーで比較を行った場合、物事をポジティブに捉える「楽観性」については、ハイパフォーマーが、非ハイパフォーマーよりも有意に高い結果が示された。このことは、ラベル（職種）に関わらず、セキュリティ人材のハイパフォーマーに共通する特性と想定できる。

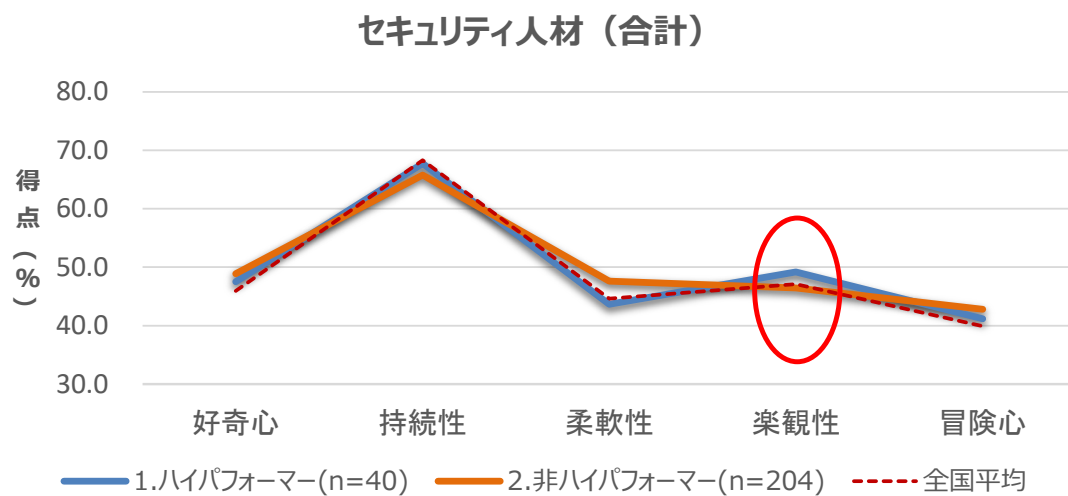


図1 セキュリティ人材（合計）：ハイパフォーマーと非ハイパフォーマーの比較



## 6. 業務内容・役割（ラベル）別の傾向

次に、2019 年 11 月発表の報告書の中で分類したセキュリティ人材の業務内容・役割別ラベルの傾向について分析を実施した。その中で特徴的な結果が得られた「マネージャー」「エンジニア」「アナリスト・分析」、「コーディネーター」に着目し、先述と同様にハイパフォーマーと非ハイパフォーマーで特性の違いを分析した。（表 3 太字のラベル）

各ラベルの説明については、2019 年 11 月発表のセキュリティ業務を担う人材のスキル可視化における概念検証報告書 ～トライアル結果の考察～ P11 の「1.2.4 ラベルについて」を参照のこと。

業務内容・役割（ラベル）	
1. マネージャー	6. コーディネーター
2. エンジニア	7. 現場責任者・PM
3. コンサルタント・監査	8. オペレーター
4. 業務担当	9. 評価・診断
5. アナリスト・分析	

表 3 2019 年 11 月発表の報告書の中で分類した業務内容・役割（ラベル）

### 6-1. 「マネージャー」

「マネージャー」については、失敗しても諦めない「持続性」の項目は、ハイパフォーマーが、非ハイパフォーマーよりも高いことが示された。一方で、不確実な状況でも行動をおこす「冒険心」は、ハイパフォーマーよりも非ハイパフォーマーの方が高い結果となった。

ハイパフォーマーのマネージャーは、柔軟性も低いため、リスクマネジメントをしながら、確実に実行可能な計画を立てた上で、粘り強くマネジメント業務を遂行する実務実行力が高いことが推察される。

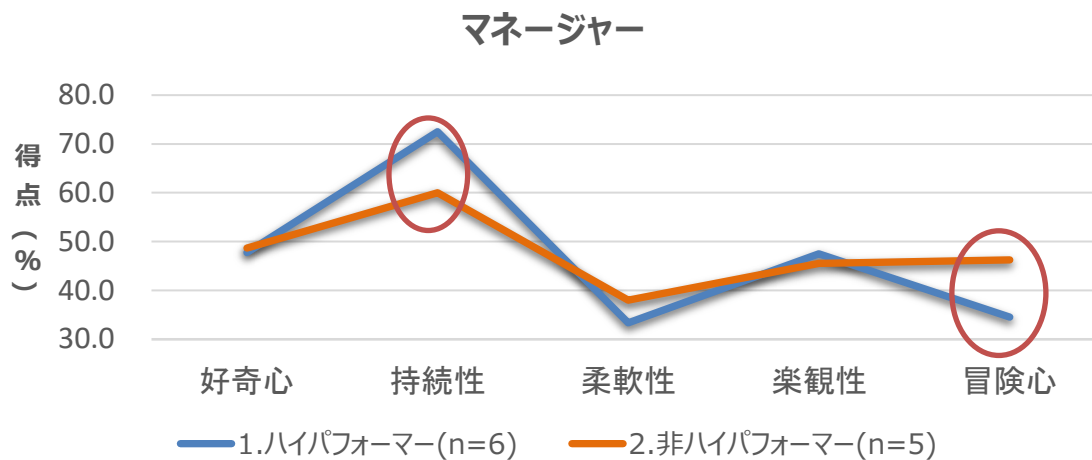


図 2 マネージャー：ハイパフォーマーと非ハイパフォーマーの比較

#### 6-2. 「エンジニア」

「エンジニア」については、物事をポジティブに捉える「楽観性」の項目は、ハイパフォーマーが、非ハイパフォーマーよりも高いことが示された。このことは、物事をポジティブに捉え、仕様変更や不確実な状況の開発プロジェクトや、運用業務においても柔軟な業務対応をし、パフォーマンスを発揮していることが推察される。

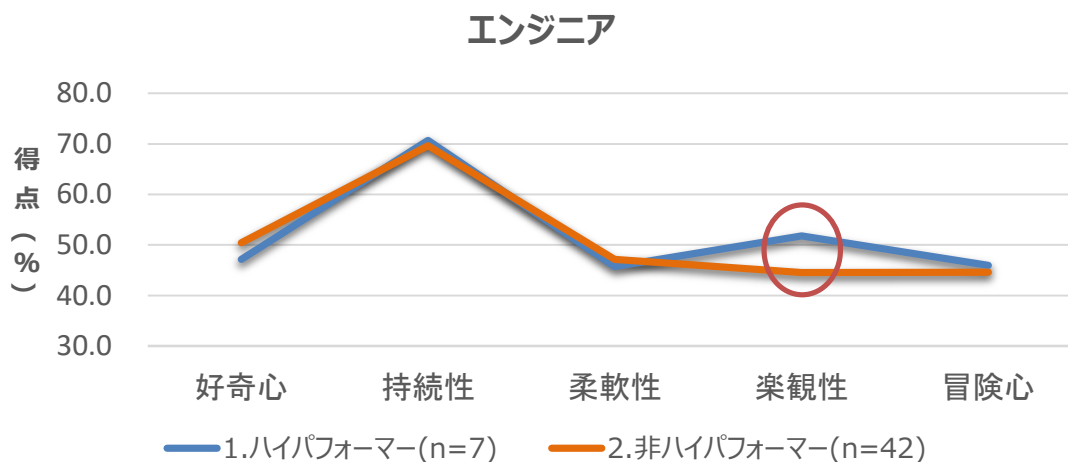


図 3 エンジニア：ハイパフォーマーと非ハイパフォーマーの比較

### 6-3. 「アナリスト・分析」

「アナリスト・分析」については、柔軟な姿勢をとる「柔軟性」の項目は、ハイパフォーマーが、非ハイパフォーマーよりも高いことが示された。分析のアプローチや評価・解釈などについて、自分の考えに固執せず、柔軟性をもった思考や行動が出来ると考えられる。

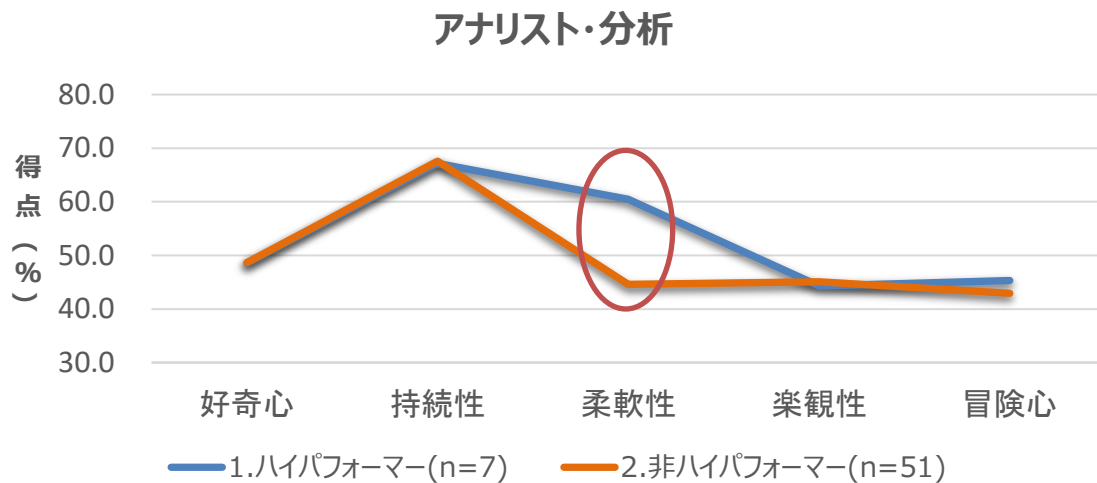


図 4 アナリスト・分析：ハイパフォーマーと非ハイパフォーマーの比較

### 6-4. 「コーディネーター」

「コーディネーター」については、柔軟な姿勢をとる「柔軟性」の項目は、ハイパフォーマーが、非ハイパフォーマーよりも低いことが示された。

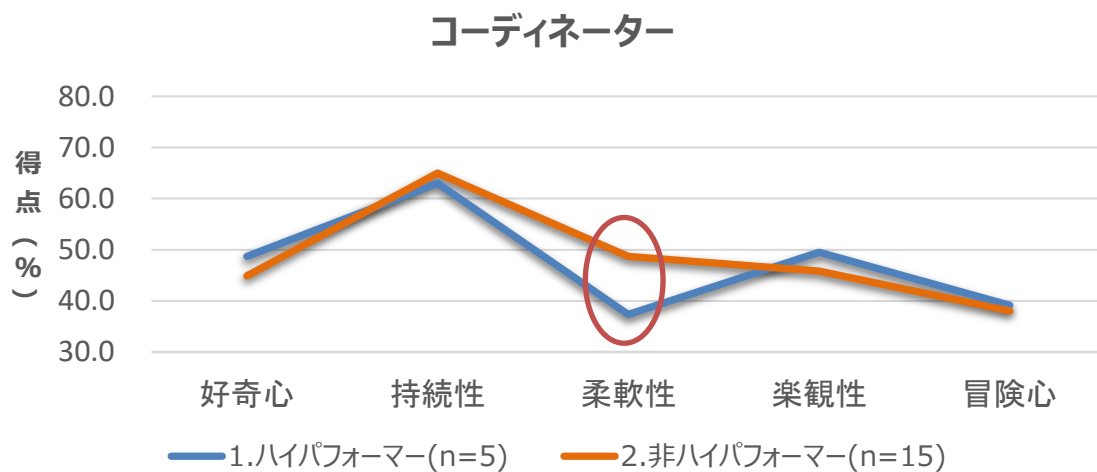


図 5 コーディネーター：ハイパフォーマーと非ハイパフォーマーの比較

## 7. 業務特性（タグ）別の傾向

次にセキュリティ人材の「業務特性」に着目し、先述と同様にハイパフォーマーと非ハイパフォーマーで傾向の違いを確認した。先述の業務内容・職種を分類した「ラベル」と区別するため、業務特性別の分類については「タグ」と呼称の上、考察する。本レポートでは、分析結果に特徴が表れた「開発」と「運用」に着目して結果を述べる。（表4太字のラベル）

業務特性（タグ）	
1. アーキテクト	5. 開発
2. マネージャー	6. 企画
3. 運用	7. 講師
4. 営業	8. 事務

表 4 業務特性（タグ）

### 7-1. 開発

「開発」の性質を持つ業務については、柔軟な対応を行う「柔軟性」と、物事をポジティブに捉える「楽観性」の2項目で、ハイパフォーマーが、非ハイパフォーマーよりも高いことが示された。

このことは、物事をポジティブに捉え、開発業務においても仕様変更や不確実な状況の開発プロジェクトにおいても柔軟な業務対応をし、パフォーマンスを発揮していることが推察される。

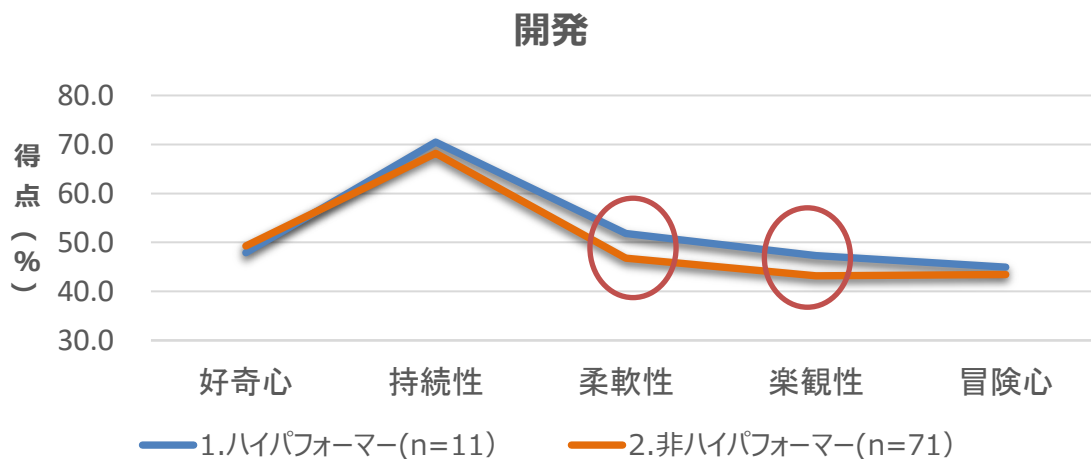


図 6 開発：ハイパフォーマーと非ハイパフォーマーの比較

## 7-2.運用

「運用」の性質を持つ業務については、物事をポジティブに捉える「楽観性」や失敗しても諦めない「持続性」が、ハイパフォーマーが、非ハイパフォーマーよりも高いことが示された。一方で、「柔軟性」や「好奇心」は、ハイパフォーマーよりも非ハイパフォーマーの方が高い結果となった。

これは、ハイパフォーマーに「柔軟性」や「好奇心」がないということではなく、「運用」のハイパフォーマーは、自身の好奇心を発揮し行動や業務を遂行するよりも、規律を守り的確に、そして安定的な業務遂行をしていると考えられる。

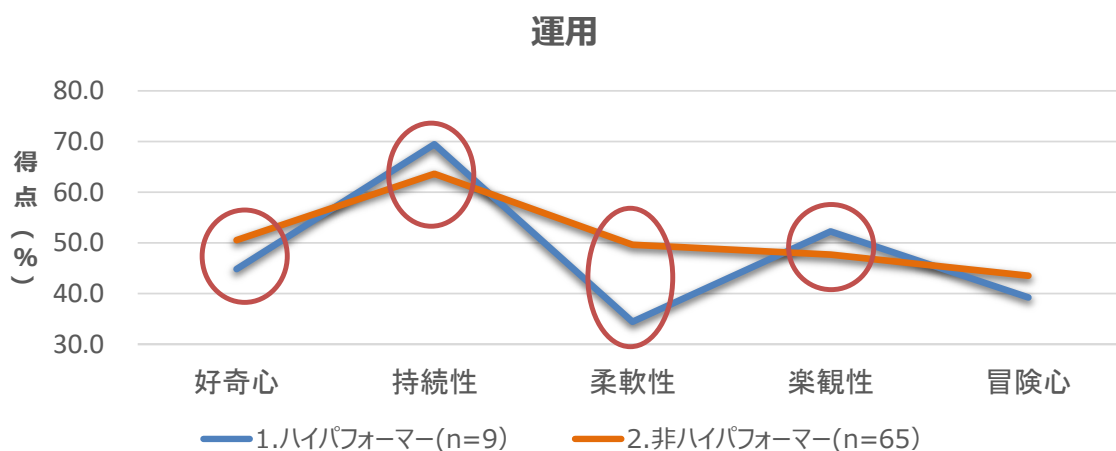


図 7 運用：ハイパフォーマーと非ハイパフォーマーの比較

## 8. 考察と今後の課題

今回、セキュリティ人材のキャリア選択の特徴を探索的に明らかにするために、「計画的偶発性理論」の5つの行動特性に着目し分析を試みた。

今回の調査では統計処理には十分といえるサンプル数ではないため、今後サンプル数を増やし、詳細な分析を行う必要があるものの、本サンプル上のハイパフォーマーは環境変化や新たな機会をポジティブに捉える（楽観性）傾向が高いことが示された。また、一見似たような性質を持ちそうなラベルとタグ、例えば「エンジニア（ラベル）」と「開発（タグ）」で行動特性の違いが見られるように、業務内容・役割（ラベル）、業務特性（タグ）、によってハイパフォーマーに現れる行動特性に特徴の違いがあることが推察される。

クランボルツは、キャリアの意思決定において、予期せぬことが個人のキャリアを左右し、また、予期せぬ出来事を避けるのではなく、起きたことを最大限に活用すること、偶然を積極的に作り出しキャリア形成の力にすることの重要性を述べている。

予期しなかった出来事を学習・成長の機会と認識し、活かすためには、個人は、これらのコンピテンシーに関する自己理解と発揮、また組織には、本人の成長を支援する仕組みが不可欠である。業務におけるパフォーマンスの発揮という側面に加え、セキュリティ人材のよりよいキャリア選択を支援するためにも、当ワーキングでは、コンピテンシーの発揮と業務内容・性質との関係性を明らかにするためにデータを蓄積し、調査分析を継続することが必要であると考えられる。

## おわりに

日本国内においては2021年5月にデジタル改革関連法案が成立するなど、ITおよびセキュリティ業務に携わる人材の需要は高まる一方であり、セキュリティ業界団体として人材需給ギャップの解消に向けて取り組みをさらに強化していくべき状況となってきた。

さらには、COVID-19による就業環境への長期的な影響もあり、図らずも働き方を大きく変えて行かざるを得ない状況となっているが、それはセキュリティ業務においても例外ではない。

このような状況の中で、今回キャリアデザインワーキンググループではセキュリティ業務に携わる人材のキャリアデザインにおける可能性を探る考察を行った。

まずは、職種間でのキャリアアップ、キャリアチェンジを検討する際に活用できる関連マップにより考察を行った。結果として職種間での相関関係が強いものとそうではないものに分かれてはいるが、目指すべき職種をイメージしやすいことから、組織内での個人に対する成長促進に活用できるのではないだろうか。

また考察を進めるなかで、セキュリティ業務に携わっている人材の多くが、自らが意志をもってキャリア選択したわけではないことも明らかとなってきた。「個人のキャリアの8割は、偶然の出来事によって決定される」という計画的偶発性理論を前提とすれば、ある程度の偶然を味方につける能力も必要となるのではないだろうか。

今回の考察では、科学的な立証というところまでは行きつかなかったものの、職種間の関連マップによるキャリアデザイン手法の検討や、計画的偶発性理論による組織と個人の成長の仕組み構築に関して、具体的な取り組み検討のきっかけになったと思う。これらについて、キャリアデザインワーキンググループの中で、さらなる考察を進めていくこととしたい。

## セキュリティ業務職種のキャリア展望について検討委員会

玉川 博之（株式会社 VSN、キャリアデザインワーキンググループリーダー）

大槻 晃助（株式会社ラック、認定 WG ワーキンググループリーダー）

尾方 佑三子（株式会社ラック）

金田 克彦（株式会社パソナテック）

佐々木 啓行（株式会社パソナテック）

高橋 真樹（ネットワンシステムズ株式会社）

平野 恭祐（株式会社パソナテック）

松木 努（株式会社リクルート）

水野 太真巳（パーソルプロセス&テクノロジー株式会社）

三船 果菜子（パーソルプロセス&テクノロジー株式会社）

持田 啓司（株式会社ラック、情報セキュリティ教育事業者連絡会代表）

渡邊 洋治（株式会社ネクストエデュケーションシンク）

※リーダー以外は五十音順

## ご協力いただいた JTAG 財団企画運営統括委員会の皆さま

砂田 浩行（株式会社横浜銀行）

米澤 一樹（パーソルプロセス&テクノロジー株式会社）

宮坂 孝（NTT データ先端技術株式会社）

館岡 均（特定非営利活動法人 日本システム監査人協会）

<お問合せ先>

JTAG 事務局（JNSA 内） [jtag-sec@jnsa.org](mailto:jtag-sec@jnsa.org)