セキュリティ業務を担う人材のスキル可視化施策の考察

～プラス・セキュリティ人材の可視化に向けて～

＜1.0 版＞

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）
JTAG 認定ワーキンググループ

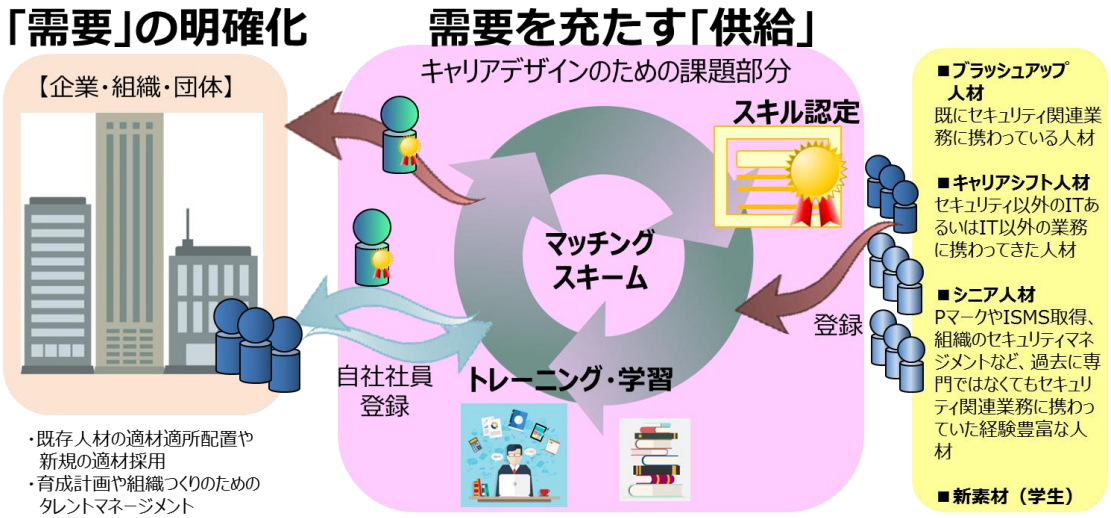
2019 年 10 月 30 日

目次

本書の目的

NPO日本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）」の活動を2017年より開始した。

「JTAG（ジェイタッグ）」とは、社会的な課題となっているセキュリティ人材の不足解消と、多様な働き方の推進のために、 国内「J」apanのセキュリティ事業者や人材サービス事業者、ユーザー企業が「TAG」を組み、「需要」の明確化とその需要を充たす「供給」を担うスキームをつくり、企業内/外の人材流動化を促進させていくことを目的としている。また、その良循環が成されることでIT産業の構造変革の下支えとなることを目指している。



本書は、JTAG構想におけるセキュリティ人材のスキル認定制度構築を念頭にセキュリティ人材の尺度を統一させ、信頼度や真の実力値が判定できる基準について策定し、活用の可能性について考察したものである。必要とされるセキュリティ業務への適材適所の配置・調達、育成のための効果的な教育プラン立案を可能とすることはもちろん、求められる職務への適正な認定がなされる制度によって、セキュリティ業務に携わる人材の地位向上に寄与することを目的としている。

なお、昨年度公開した「セキュリティ業務を担う人材のスキル可視化ガイドライン」の内容にもとづいて各種指標の実効性を検証する目的で概念実証（以下トライアル）を実施した。その結果やトライアル実施者の意見等を反映し新たに「セキュリティ業務を担う人材のスキル可視化施策の考察」第1版として公開したものである。内容としては各種スキル指標・評価範囲・判断基準の修正や、セキュリティに関連したサンプルプロファイルの策定追加、コンピテンシー(※1)についてのトライアル実施での分析結果・考察追加など、多岐に渡ってアップデートされている。また、セキュリティ業務を担う人材のスキル可視化によって個人や企業/組織にとってどのような利活用が期待されるのか、実運営で提供できるのか、将来に向けての提言も盛り込んだ。

このガイドライン策定における大きな特徴、考え方は2つに集約される。

1. セキュリティ人材の広範囲な定義（図1）
   セキュリティ業務を主として行う専門人材だけでなく、一般企業において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（以降、「プラス・セキュリティ人材」と呼ぶ）にも焦点をあてる

（※1）コンピテンシー：業務遂行能力の高い人物（ハイパフォーマー）に共通する行動特性

2.　多視点からのセキュリティ人材スキル判断基準（図2）

業務経験やコンピテンシーなどの暗黙知を基準として取り入れることで、その人材の精度の高い総合実力を導けることを念頭におく

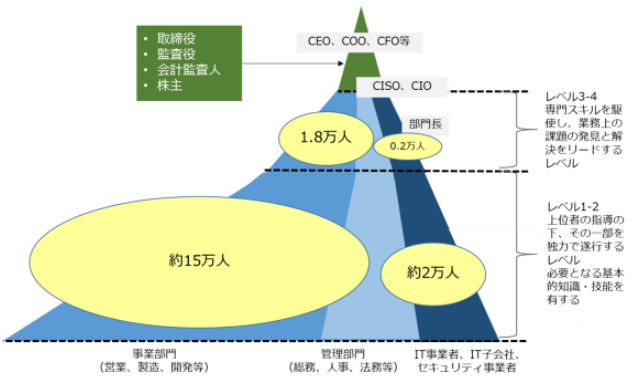


図1

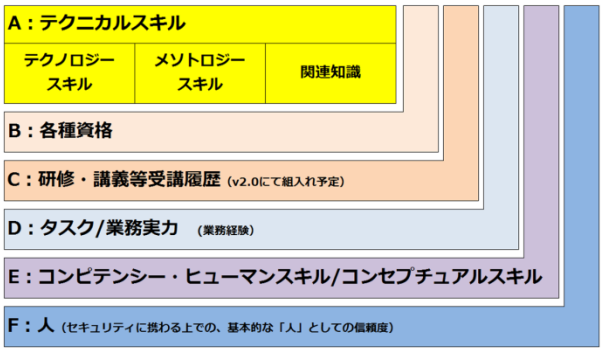


図2

出典：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」

その他の特長としては、

・育成教育プランとの連携における利用価値提供できるように指標を整理する
・ユーザー企業の IT を利活用している人や部門に焦点をあてたセキュリティ視点の業務や職務、役割の定義（通常業務との兼務者が多い）も導けるようにする
・シニア人材の活用（特にマネージメント系）に資することができるものとして整理する
・認定制度運営にあたっては、持続し運営ができることを念頭におく

なお、現在の可視化の仕組みは主に社会人を対象に組み立てられている。これから社会に飛び立つ学生については、指標設定やスキル基準などが適切かどうかさらに検討が必要なため、新たに検討していく。

人生100年時代と言われる今、長い仕事人生において自分のキャリアパスを描きながら生き抜いていく知恵と、適切な情報を選び使いこなしていく力が若い方々には特に必要になる。その道しるべを具体的に描く道具として役に立つものに仕上げたい。また、学校機関においては、セキュリティ分野の業務や役割ごとのスキルが整理され明確になることで、カリキュラムの組み立てに役立たせていただけること、また、学生の就職に対してきめ細かなアドバイスのツールとなることも期待できる。

1. 策定のポイント

1.1. JTAG における「セキュリティ人材」の定義について

1.1.1. 「セキュリティ人材」不足の正確な現状について

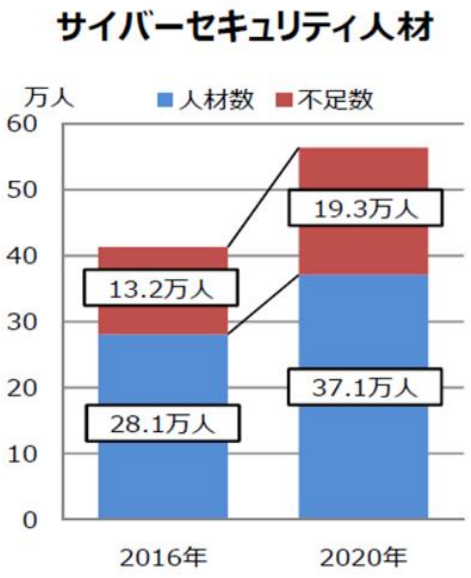


図3 サイバーセキュリティ人材数推移

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」

2016 年の経済産業省での調査では、セキュリティ人材が 13.2 万人と大幅に不足しており、その数は 2020 年に向けて不足人数が大きく増えると報告されている(図 3)。この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おり、市場拡大が見込まれるセキュリティ分野においての人材不足が深刻化すると指摘されている。

しかし、2016 年に大きく報道された際には、セキュリティ専門人材が不足とされていたために、多くの一般の人々にはホワイトハッカー(※2)のようなセキュリティに特化した人材が大幅に不足しているとの誤解を生んでしまった。経済産業省の調査報告をさらに良く見ると、現在不足しているセキュリティ人材の多くは、

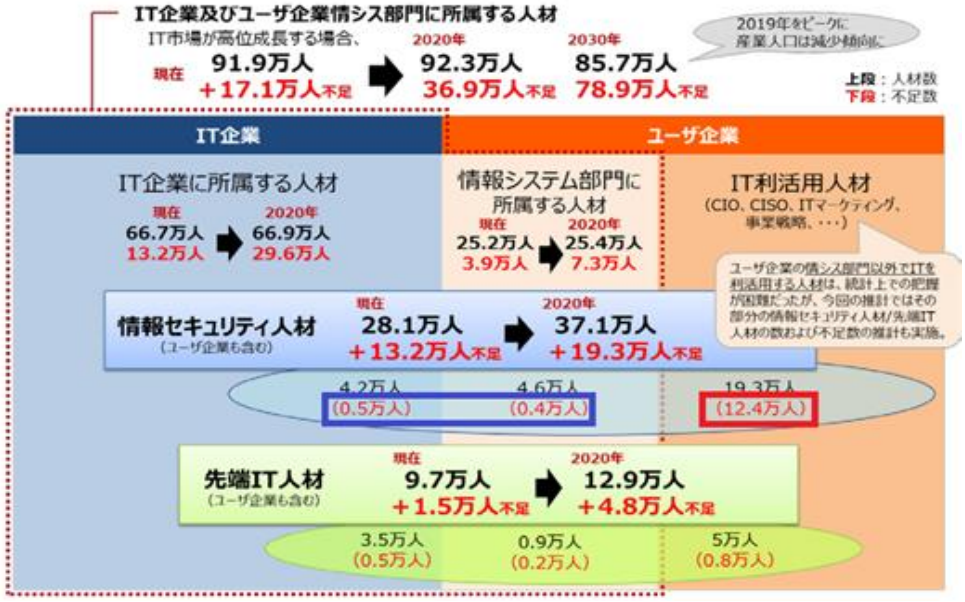


図4 「IT 人材不足が深刻化 2030 年には 78.9 万人不足に」

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

(※2)ホワイトハッカー:IT 関連の高度な知識や技術を使ってセキュリティ対策を施す活動や、コンピューターやネットワークへの悪意を持った攻撃を防ぐ活動を行う

IT 企業やユーザー企業の情報システム部門に所属する人材ではなく、ユーザー企業において IT を利活用する中で、セキュリティ確保もできる人材が 2016 年調査時点に 12.4 万人と大幅に不足していることがわかる。(図 4 赤枠内)このような人材はセキュリティ専門家とは限らない。図 4 青枠内のいわゆるセキュリティ専門人材については、IT 利活用人材に比べれば不足人数は少ないが、スキル不足への対応は特に必要であるなど、問題は依然解決されていない状況である。

1.1.2. 人数面で大幅に不足している利活用実施部門におけるセキュリティ人材対応への必要性

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、国においても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。(図 5)

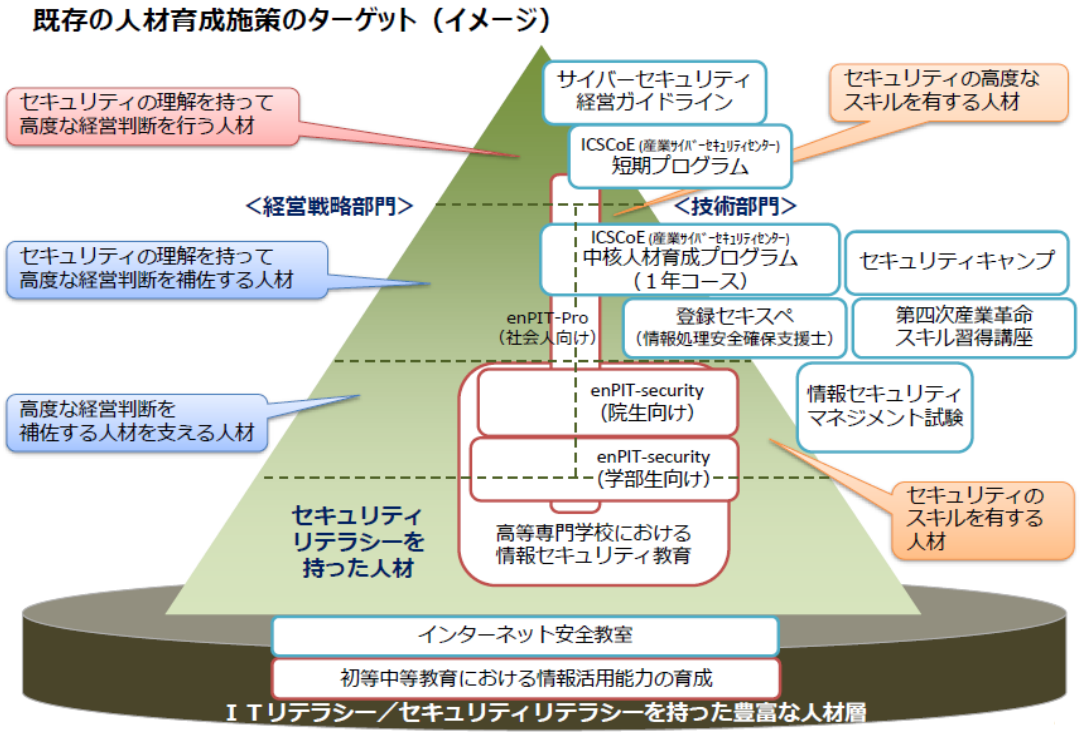


図5 経済産業省 「現存のセキュリティ人材育成施策とターゲットイメージ」

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

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が、スキル習得を中心とした施策であったため、図 5 を見ても明らかなように、右側のセキュリティ技術育成に偏重した施策であり、左側の経営や事業部門でのセキュリティ人材の育成施策はほとんどない現状である。

また図 6 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ー企業での「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。セキュリティ専門人材だけの数値化(見える化)であれば、従来のセキュリティ資格やセキュリティ教育受講歴などからある程度の対応が可能である。しかし、今まで特に国策や資格などもなく

人材育成に対して未対応であったエリアのプラス・セキュリティ人材については、従来は客観的な指標がなかったため、人材の数値化（見える化）を実現することは不可能であった。

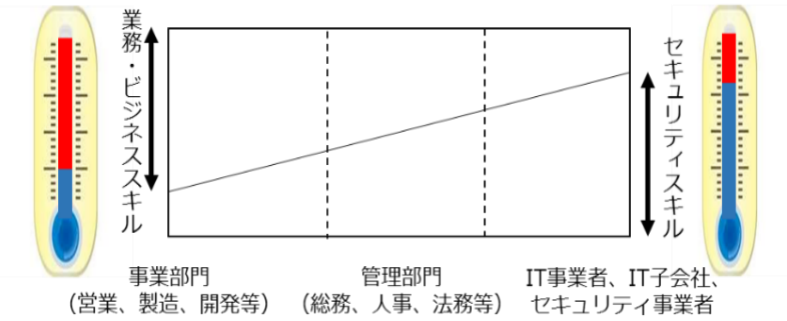


図 6　所属企業・部門におけるセキュリティスキルと業務ビジネススキルとの関係イメージ

出典：JCIC 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」

1.1.3.　従来の「安心・安全を守る」役割から、新たな「攻め（積極的な）」役割を担う「攻めのプラス・セキュリティ人材」が登場

昨今の DX（デジタルトランスフォーメーション）化(※3)の流れにおいて、セキュリティ人材に期待される役割にも変化が出てきている。新たな役割とは、「攻めの IT 投資」を実現するために必須となる「攻めのセキュリティ」である。

図 7 は、JEITA(※4)より公開されている日本と米国における IT 投資の目的を調査したものになる。2013 年当時では、日本では IT 投資の目的は、業務効率化やコスト削減中心であったが、米国では素手のビジネスモデル変革やサービス開発強化などのいわゆる「攻めの IT 投資」が既にな

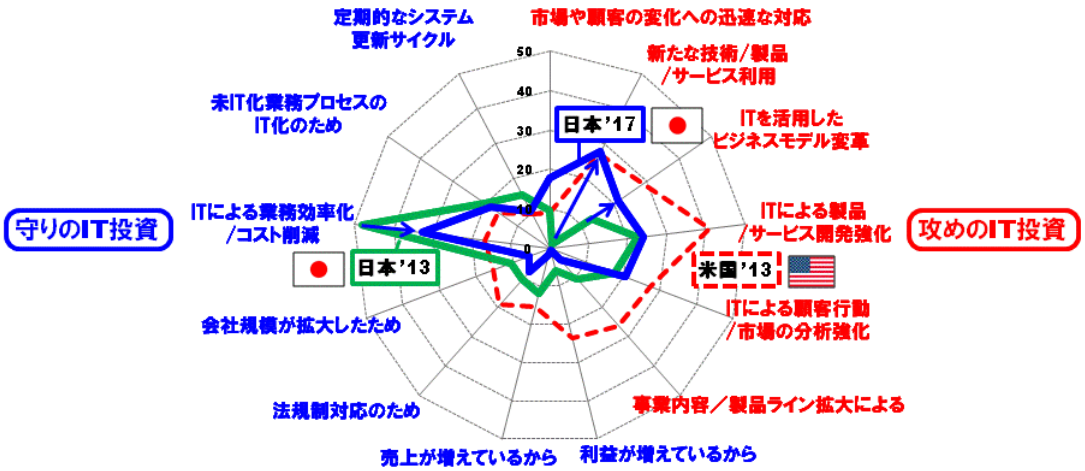


図 7　IT 投資　日米比較

出典：JEITA『2017 年 国内企業の「IT 経営」に関する調査結果

https://www.jeita.or.jp/japanese/exhibit/2018/0116.pdf

(※3) DX：デジタル技術を浸透させることで人々の生活をより良いものへと変革すること
https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/20180907_report.html

(※4) JEITA：Japan Electronics and Information Technology Industries Association 一般社団法人電子情報技術産業協会
https://www.jeita.or.jp/japanese/

されていたことがうかがえる。日本における 2017 年追加調査では、13 年の米国には及ばないものの、攻めの IT 投資にシフトされ始めていることが明確になり、国内においても DX 化の波が確実に浸透しつつある状況である。

セキュリティ面においても IT 部門ではセキュリティに対する取り組みを強化する予定であることがうかがえる。図 8 は、IPA において、今後の IT 業務の増減を調査したものである。ユーザー企業およびネットサービス企業ともに、“情報セキュリティリスク管理業務”が増加する見通しはトップとなっている。ネットサービス企業では実に約 6 割の企業が“情報セキュリティリスク管理”業務を増加予定であると回答している。ユーザー企業においても、増加予定業務ではセキュリティ関連業務が 1 位であるが、増加予定企業が約 3 割とまだまだ少ないと考えられる。ネットサービス企業は、経営の IT 依存度が高いため、情報セキュリティに対する危機感が、ユーザー企業と比較して高いと思われる。しかし、DX 化の流れは確実にユーザー企業を巻き込むことになるため、ユーザー企業においても経営の IT 依存度が高まると、セキュリティに対する取り組みもネットサービス企業同様に高まると推測できる。

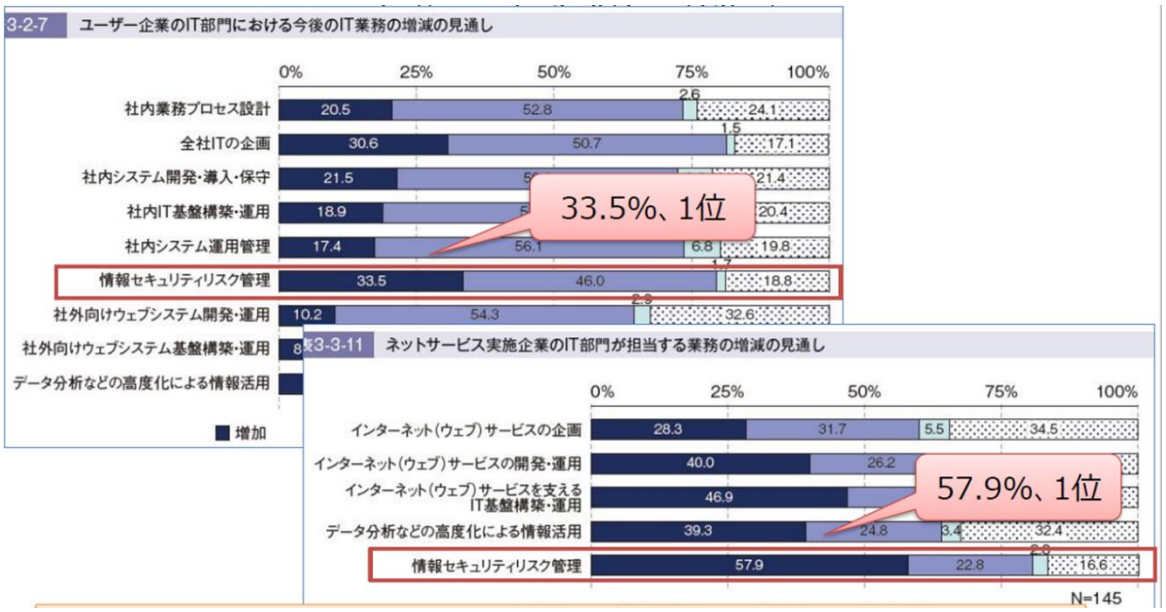


図 8　今後の IT 業務の増減調査

出典：IPA「いま求められるセキュリティ人材確保のために」より

https://www.ipa.go.jp/files/000069702.pdf

1.1.4.　セキュリティ専門人材に加えて、プラス・セキュリティ人材の見える化を実現

DX 化や Society5.0(※5) 時代においては、セキュリティは社会を支えるシステム基盤の役割へと変化している。そのような状況においては、セキュリティに携わる人材もセキュリティ専門家だけでなく、本来の業務を担いながら（IT 利活用人材）セキュリティも知っておいてほしい、いわゆるプラス・セキュリティ人材の必要性が急増している。プラス・セキュリティ人材は、ユーザー部門の方からのジョブチェンジやセキュリティスキルの追加習得が望まれる。図 9 ではジョブのミスマッチを表したものであるが、今後の人手不足と過剰人材増問題を解決する一施策としては、現場業務の知識が豊富な

（※5）Society5.0：内閣府により、目指すべき未来社会の姿として提唱された「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）」
https://www8.cao.go.jp/cstp/society5_0/index.html

人材にセキュリティを学ばせ、プラス・セキュリティ人材として、再度現場で活躍していただくことも積極的に検討していくことが重要である。JTAG では、このような社会状況も踏まえ、セキュリティ人材を「セキュリティ専門人材」と「プラス・セキュリティ人材」と定義した上で下記の点を実現したことが大きな特長となっている。

1） セキュリティ専門人材を一括りでなく、自社に必要な役割やスキルで見える化

従来であれば、セキュリティスキルのレベルを IPA の情報処理安全確保支援士や民間資格の CISSP(※6)や CISM(※7)などの資格保有だけで判断する例が多かったが、セキュリティ専門人材と言ってもその役割は多種多様である。JTAG では情報セキュリティスキル分野（SecBoK）を利用し、複数のスキル分野ごとによるスキルレベルの診断や、自社で必要な人材のスキル項目をピックアップして検索するなどが可能となっている。

また、厚労省が推進している職業情報提供サイト（日本版 O-NET(※8)）の目的ともなっている、『職業を「ジョブ」「タスク」「スキル」などの観点から分析し、労働市場の共通言語・共通基準としてデータベース化することで職業情報を「見える化」し』といった点については、SecBoK2019 の基本的な考え方である「スキル」「ロール（役割）」「タスク」の視点での可視化とも共通する部分が多くあるため、将来的にはセキュリティ分野に留まらず、他分野での適用も期待されるものである。その結

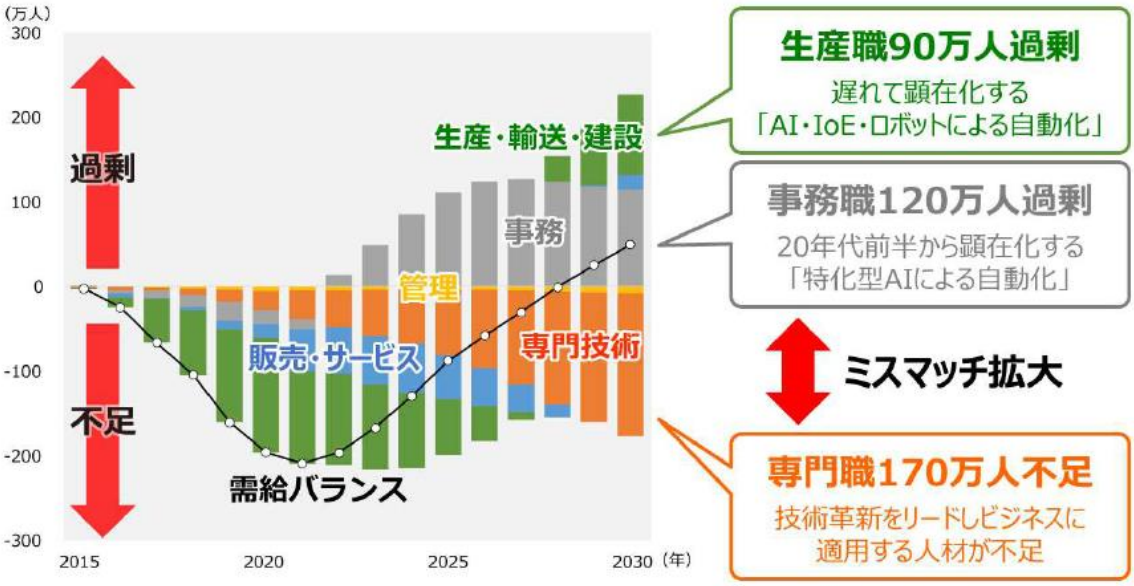


図 9 デジタル技術進展に伴う職のミスマッチ

出典：三菱総合研究所 「日本版 O-NET 概要と民間ビジネス活用の可能性」より
https://www.mri.co.jp/opinion/column/trend/trend_20180806.html

---

(※6) CISSP: Certified Information Systems Security Professional
(ISC)² (International Information Systems Security Certification Consortium) が認定を行う国際的に認められた情報セキュリティ・プロフェッショナル認証資格 https://japan.isc2.org/cissp_about.html

(※7) CISM: Certified Information Systems Manager
ISACA (Information System Audit and Control Association) が認定を行う国際的に認められた公認情報セキュリティ・マネージャー資格 http://www.isaca.gr.jp/cism/index.html

(※8) O*NET：Occupational Information Network 米国労働省が運営する職業に関する総合的なデータベース
https://www.onetonline.org/
日本版 O-NET：日本政府が進めている米国の O-NET にならった職業情報の見える化。2020 年から日本版 O-NET を稼働させるとしている
https://www.mhlw.go.jp/stf/shingi/other-syokuan_196434_00002.html
https://www.jil.go.jp/institute/siryo/2018/203.html
https://www.mri.co.jp/knowledge/insight/20181002.html

果、産業全体の人材の流動化促進によって職のミスマッチを減らし、将来の需給バランスを適性に保つアプローチに繋がれば社会的貢献ともなる。

図 9 は、日本におけるデジタル技術進展に伴う職のミスマッチを表したものである。プラス・セキュリティ人材は、セキュリティのテクニカルスキルに加えて業務知識も求められるため、セキュリティ専門家からの移行だけでなく、業務経験豊富なユーザー部門の方からのジョブチェンジやセキュリティスキルの追加習得が望まれる。ここにフォーカスしたアプローチが、今後の日本社会で想定されるミスマッチから生まれる専門職不足と AI やロボット化による過剰人材増問題の解決のサンプルとしての一施策となるかもしれない。

2) 可視化が困難だったプラス・セキュリティ人材の見える化を実現

事業部門で IT 利活用しながらセキュリティ確保も担当するプラス・セキュリティ人材は、セキュリティのテクニカルスキルのみでは判断ができないため、人材の見える化が困難であった。特に「攻めのプラス・セキュリティ人材」は、事業部門に配属されるケースが多いため、従来はその可視化が困難であった。そこで JTAG では ISACA（情報システムコントロール協会）等関連団体との密接な連携により、マネージメントスキルを判断できる項目を取り入れると共に、業務経験も重要であると判断し、どの分野で何年の業務経験を積んだのかも人物の総合ポイントに加味するロジックを開発した。業務経験やマネージメント経験も人物評価項目に加味することで、経験豊富なシニア IT 人材の利活用に向けても大きく貢献することが期待できる。

＜JTAG の評価項目で参照している既存のフレームワーク＞

参照対象	指標／知識体系
IT スキル項目	iCD(※9)
情報セキュリティ知識項目	SecBok(※10)
IT／コーポレートガバナンス	COBIT(※11)
スキルレベル	ITSS(※12)
資格レベル	ISV Map(※13)
能力成熟度モデル	CMMI(※14)

このように JTAG は、セキュリティ人材不足問題を正確に理解した上で、その対策に向けて有効な手段となるように検討されている。セキュリティ専門人材はもちろん、プラス・セキュリティ人材への対応という新たな取り組みにも対応しているものである。またシニア IT 人材利活用への対応についても、今後日本が直面する労働人口不足への取り組みとして大変有用なツールであると考えている。

(※9) iCD：ｉコンピテンシディクショナリ / IPA(独立行政法人情報処理推進機構)
https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/
(※10) SecBok：Security Body of Knowledge 2017 版 / JNSA（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）
https://www.jnsa.org/result/2017/skillmap/
(※11) COBIT：Control objectives for Information and related Technology v1.3 / ISACA が提供する IT 及び企業ガバナンスのフレームワーク
http://www.isaca.org/cobit/pages/default.aspx
(※12) ITSS：IT スキル標準(IT Skill Standard) / IPA(独立行政法人情報処理推進機構)
https://www.ipa.go.jp/jinzai/itss/index.html
(※13) ISV Map：ITSS キャリアフレームワークと認定試験・資格の関係 Ver11r1 / SSUG（特定非営利活動法人 スキル標準ユーザー協会）
https://www.ssug.jp/docs/
(※14) CMMI：Capability Maturity Model Integration / カーネギーメロン大学 および ISACA
https://cmmiinstitute.com/cmmi

1.2. スキル評価基準全体の考え方

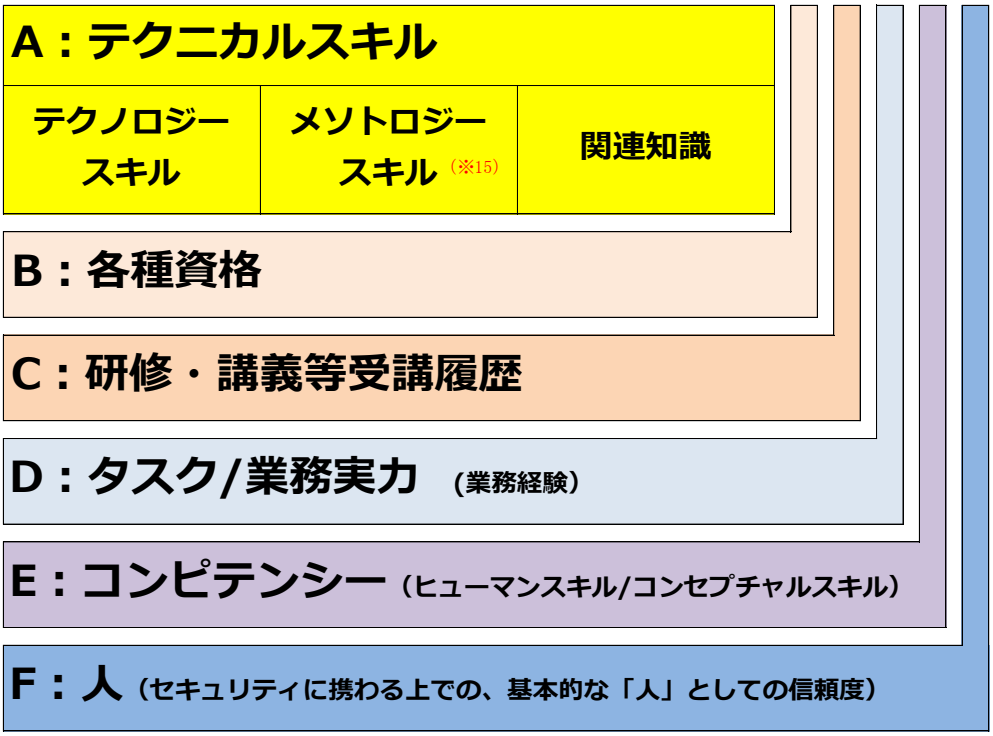


図 10 評価基準構成図

1.2.1. 評価基準項目策定の考え方

1）情報セキュリティ人材に限らず、企業における人材の能力や業務遂行力、それを実現するためのヒューマンスキルやコンセプチュアルスキル(※16)などのコンピテンシーを評価する絶対的に正しい方法というのは無い。とはいえ、企業側は常に試行錯誤しながら評価方法をより良いものにしていく努力が求心力として求められる。JTAG のスキル可視化は社員の評価目的ではないが、常にブラッシュアップやメンテナンスが迅速に継続して行えることを念頭に、図 10 のようにモジュール化をベースにした。

2）また、モジュール化は企業内のタレントマネージメント(※17)において、必要なモジュールだけを使って活用することも想定している。

3）セキュリティ専門業務以外でも、その業務内において或る程度想定されるセキュリティに関連業務や役割について考慮し、その人材の実力値の一部として算入した。また、その経験が深く長いほど力が蓄積されているはず、との前提から経験年数も算入している。JTAG キャリアデザインワーキンググループ（以下キャリアデザイン WG）での調査で、セキュリティ専門業務従事でなくても関連する業務において長年の経験を積み重ねて、CISO(※18)をサポートするレベルのシニア層が多く存在していることも明らかになっており、専門業務以外でも真のセキュリティ実力値として顕在化できる工夫をした。

（※15）メソトロジースキル：方法論や整理の技法を理解して応用できる能力
（※16）コンセプチュアルスキル：知識や情報を体系的に組み合わせ、複雑な事象を概念化し、物事の本質を把握する能力
（※17）タレントマネージメント：従業員のスキルや能力を最大限に活かすために、戦略的な人材配置や育成、評価を行うマネージメント
（※18）CISO：Chief Information Security Officer 情報セキュリティ担当の役員

1.2.2. 各評価基準項目におけるレベル設定の考え方

ITSS のスキルレベルを参考に独自の評価基準を織り交ぜてレベル基準を策定した。

業界をリードし市場への影響力があるレベルにある	レベル 7
業界に貢献し認知されるレベルにある	レベル 6
所属団体・組織内で貢献し認知されるレベルにある	レベル 5
●技術領域スキルについては非機能要件を考慮して最適化できる、最適解が出せる、定石外しができる ●手法/方法については最適に使いこなせる、最適な手法を選択できる、状況に応じて自在に駆使できる ●関連するスキルについては上級管理者と議論ができる	レベル 4
●技術領域スキルについては機能要件を把握し、自立してある限定条件下で仕事ができる ●手法/方法については最低限の使い分けができる、又は活用して結論を導いたことがある ●関連知識領域については課題点について提案したことがある	レベル 3
●指導や指示があればそのスキルを使って業務がこなせる、そのスキルを活用できる。又は、スキルを必要とする業務について難易度は別にしてなんらかの経験がある	レベル 2
●技術、手法、方法など内容について講義などの受講や自己学習を通してどのようなものなのかを知っている、基本的な知識はある、概要は言える	レベル 1
●内容についてほとんど知らない、知識がない	レベル0

図 11　JTAG 評価レベル定義

2. スキル評価基準

2.1. 数値化の基本的考え方

「A:テクニカルスキル」、「B:各種資格」、「C:研修・講義等受講履歴」、「D:タスク／業務実力(業務経験)」については、実力値としての見える化を数値で実現した。

・資格基礎点と業務経験基礎点を総合判断して、個人の基礎点を算出する。
・資格基礎点は、各資格の特徴・専門分野を評価し各スキルに対する基礎点を定義した。総合評価は、資格のみを取得し業務経験に乏しい場合や、豊富な業務経験はあるが資格が無い場合なども考慮して算出する。
・業務経験は業務の内容と経験年数を評価し基礎点を計算する。特にセキュリティ関連の業務の割合を入力することで、セキュリティ分野での点数を加算する仕組みとした。
・資格と業務で自動算出される基礎点は図8のスキルレベルの定義により、最大レベル4になるように調整した。

なお、基礎点の配点設定等に関しては 300 人を超えるトライアル調査(1,2 次)の結果を踏まえ精度をあげるための調整を重ねた。2 次トライアルについては 11 月中旬公開予定の「セキュリティ業務を担う人材のスキル可視化施策　概念実証報告(仮称)」を参照いただきたい。

2.2. A:テクニカルスキル

評価対象項目の洗出しについては SecBoK を中心に、不足する部分は iCD などを参考に JTAG としての指標の考え方に合わせて整理し表現等を一般的にわかりやすいものに変更した。この項目に対して各種資格や業務経験ごとに点数が設定されている。

		大項目	中項目
テクノロジ	ICT技術全般	計算機の構成	電子工学
			並列、分散コンピューティング
			コンピュータおよび電子デバイスの物理的構成要素とアーキテクチャ
			エンコード
			コンパイラ
		システムインテグレーション	上流設計工程
			設計工程
			プログラミング手法
			プログラミング言語
			デバッグ
			テスト工程
			テストシナリオの作成と実行
		ネットワーク	コンピュータネットワークの構成
			通信方式
			ネットワークプロトコル
			ネットワーク管理、分析、運用
		サーバ	オペレーティングシステムの構造
			スクリプト作成、コマンドライン操作
			サーバ管理、分析、運用
			サーバの仮想化技術
		データベース	データ構造
			データマイニング
			データベース操作
			データベース設計・構築・運用

		情報工学	ソフトウェア工学
			システム工学
			プロセス工学
			CMMI（能力成熟度モデル統合）
			構造解析
			数学
		DRP（災害復旧計画、技術系）	Server 設計、開発（対サイバー攻撃含む）
			Storage設計、開発（対サイバー攻撃含む）
			Network設計、開発（対サイバー攻撃含む）
			Dataのバックアップ、計画、運営
			構成情報管理、バックアップ
テクノロジー	情報セキュリティ技術	ネットワークセキュリティ	ネットワークセキュリティ基礎
			ネットワークセキュリティ　解析
			ネットワークセキュリティ　侵入検知
			ネットワークセキュリティ　アクセス制御
			ネットワークセキュリティ　深層防御
		脆弱性診断（プラットフォーム、アプリ等共通）	ペネトレーションテストの基礎知識
			ツール利用技術
		システムセキュリティ	システム、アプリケーションの脅威と脆弱性に関する知識
			保護コンポーネント、ツールに関する知識（FW、ルータ、アンチウイルスソフト等）
			リバースエンジニアリング技術に関する知識
			セキュアなシステム設計に関する知識
			セキュアプログラミングに関する知識
		セキュリティ運用	運用手法
			製品知識
			セキュリティシステムリスクマネジメント
			インシデントハンドリングに関する知識
		暗号・アクセス制御（認証、電子署名等）	暗号
			アクセス制御
		サイバー攻撃手法	サイバー攻撃基礎知識
		マルウェア解析	マルウェア解析基礎知識
			マルウェア解析手法
		デジタルフォレンジック	フォレンジック基礎知識
			フォレンジック手法
メソロジ	事業・管理・マネジメント・経営	情報セキュリティマネジメント	情報セキュリティマネジメント総論
			情報セキュリティマネジメント手法
			情報セキュリティプログラムの開発と管理
			情報セキュリティインシデントの管理
			情報資産の管理
		BCM（事業継続マネジメント）	BCM立案、設立、決定
			BCM運営（PDCA,テスト）
			BCP（事業継続プラン）計画、設計
			施設（Data Center、Office等）設計、開発,運用
		リスクマネジメント	リスク特定
			リスク評価
			BIA(Business Impact Analysis) 事業影響度分析
			リスク対応計画
		事業・戦略	IT ガバナンス
			予算（計画、管理）
			エンタープライズアーキテクチャ
			ビジネスアナリシス
			ビジネスプロセスマネジメント
		経営・組織・マネジメント	経営・組織論
			ナレッジマネジメント
			組織・リソースマネジメント
		ビジネス基礎	技術トレンド
			ビジネススキル
			英語

		教育
		国際ビジネス
	法/制度・標準・監査	標準
		法/制度
		監査手法、手順
		監査、評価、管理
	マネージメント/リーダーシップ　スキル	リーダーシップスキル
		分析能力
		クリティカルシンキング（見かけに惑わされず、多面的にとらえて本質を見抜くこと）
		対人能力・コミュニケーション
		水平思考（既存の枠にとらわれない思考）
		コーチングスキル

図 12　JTAG の評価指標

2.3.　B:各種資格

試験・資格の選出は、『ITSS のキャリアフレームワークと認定試験・資格とのマップ　Ver11r2』を参考に、公的資格や民間資格の中から、認知度が高く、受験者数が多い試験・資格で、テクノロジーカテゴリやメソトロジーカテゴリの各指標を測定するに適しているものを選出している。なお、選出の際には、トライアル実施者の保有資格も参考情報として活用した。カテゴリ内の配点は、各試験のシラバスに含まれている項目のみから行なっている。

各種英語能力英語試験に関しても、評価が行えるように追加した。

今後も関連資格は追加、修正を継続して行う予定である。

2.4.　C:研修・講義等受講履歴（次期バージョンにて組み入れ予定）

業務遂行のための知識やスキルの習得は IT では重要な課題である。自己学習や OJT も有効であるが、専門の教育機関による体系だった学習は効率面でも大変重要な手段である。JTAG のスキル診断評価により、想定する職種とのギャップが明確になるので、それを埋めるための教育プログラムを例示する事ができる。そもそも ISEPA はセキュリティ人材育成のための教育提供事業者の集まりでもあることから、各種教育プログラムを豊富に例示できる。

また、これから社会人として活躍する大学や高等専門学校などで提供されている専門課程を経た人材は相応の即戦力としても JTAG の対象となっていくことや、社会人で CySec や情報セキュリティ大学院大学などのプログラムを経た人材は高いスキルを保持していると評価できる。そのような視点から、次期バージョンでは指標として組入れていく予定である。

2.5.　D:タスク/業務実力（業務経験）

業務経験基礎点は、担当業務とその経験年数を考慮し点数化した。基本的な考え方は専門的分野を概ね 10 年経験するとその分野では熟練者（レベル4）である事を前提とした。もちろん個人により同じ年数を経過しても習得できるレベルには差があるため、あくまでも平均的な尺度としての業務経験値としている。また、特に専門性が高く短期間で一人前になれる業務に関してはその点も考慮して基礎点を設定している。

図 13　A、B、C、D にて数値化されたレーダーチャート

各種資格およびタスク／業務実力（業務経験）は、「2.1.数値化の基本的な考え方」において定義したように、各資格の特徴を鑑みた共通の基礎点および業務の内容と経験年数を評価した基礎点であり、その範囲にとどまっている。

その資格や業務経験がどのような実績につながったか、また、経験をもとにどのような成果を創出できるのかを考慮した「見える化」について、今後本ガイドラインでは追加検討していきたい。

2.6.　E:コンピテンシー・ヒューマンスキル・コンセプチュアルスキル

セキュリティ人材に必要なテクニカルスキルについての評価指標は整ったなかで、各種業務遂行にはその他にも必要なスキルがあり「セキュリティ専門人材」および「プラス・セキュリティ人材」として組織における業績や評価の高い人材のコンピテンシーを測定することも重要であることはβ版[※19]のレポートの通りである。

今回のトライアルでは、コンピテンシー・ヒューマンスキル・コンセプチュアルスキルの可視化および組織における業績や評価の高い人材の分析に取り組んだ。A. テクニカルスキルにマネージメント/リーダーシップスキル、ビジネス基礎、経営・組織・マネージメント、事業・戦略という項目を診断しているが、よりこれらの詳細を明らかにしていく取組みである。

可視化の方法として、人財アセスメント・組織分析・人財コンサルティング事業を通じた豊富なアセスメントツールとその実績および蓄積データを保有している株式会社ネクストエデュケーションシンクに協力いただいた。同社が保有するアセスメントツール（200 種類）の中には、ITSS に対応したアセスメントツールもある。IT 分野における知見および実績を期待できることから、複数のアセスメントツールによる診断手法を採用した。

本診断はA. テクニカルスキルに該当するセキュリティ技術は対象外となる。JTAG スキル診断入力フォームで適合度を診断している業務モデルをベースに、A. テクニカルスキルに該当するセキ

（※19）β版：セキュリティ業務を担う人材のスキル可視化ガイドライン～プラス・セキュリティ人材の可視化に向けて～＜β版＞
https://www.jnsa.org/isepa/images/outputs/JTAG_guideline-%CE%B2_190118.pdf

ュリティ技術を除外した際の人物像として共通のコンピテンシー・ヒューマンスキル／コンセプチュアルスキルが必要とみられる業務モデルをグループ化して分析を行った。
「A:テクニカルスキル」、「B:各種資格」、「C:研修・講義等受講履歴」、「D:タスク／業務実力（業務経験）」のレーダーチャート化と連動させた可視化方法については、今回のトライアル2の各種分析を実施しながら具体策を導き出していく。詳細については 11 月中旬公開予定の 2 次トライアル結果をまとめた「セキュリティ業務を担う人材のスキル可視化施策　概念実証報告（仮称）」を参照いただきたい。

2.7.　F:人（セキュリティに携わる上での、基本的な「人」としての信頼度）

セキュリティに携わる人材において、その人物の信頼度は大変重要である。海外では秘密にすべき情報を扱う職員に対して、その適格性を確認するセキュリティ・クリアランス制度などが成立している。米国の公務員、特に FBI のような機密情報に関係する職員に対しては、より厳密に適用されており、下記の様な審査項目がある。
・母国への忠誠度合
・外国からの影響や傾斜
・財政状況
・酒類消費
・麻薬関与
・犯罪歴
・IT 不正利用　など
しかし日本においては、プライバシーに関する内容に触れることになり、法律が制定されていないこともあるため、民間企業において運用することは困難な状況であり、JTAG においても同様の状況である。そこで JTAG においては、セキュリティ・クリアランス制度には及ばないが、その人物の信頼度を確認する手段として下記の対応が効果的と考える。

1）情報処理安全確保支援士資格制度との連携

情報処理安全確保支援士制度では、情報処理の促進に関する法律により、禁錮以上の刑に処せられている者や不正アクセス行為の禁止等の刑に処せられている者などは、登録できないと欠格事項が設定されている。JTAG では情報処理安全確保支援士資格保有の確認をとることで人物の信頼度の確証の1つとして判断材料に組み入れる。
また、監査系やセキュリティ関連の資格などで倫理規定の順守など明確に規定しているものがある。これらについても内容を検討しながら順次組み入れていく。

2）履歴書および業務経歴書などでの確認

自己申請にはなるが、JTAG 登録時に履歴書や業務経歴書内の信賞必罰事項により確認する。

3）正式認定のためのインタビューの実施

比較的高いレベルの認定については、認定審査官によるインタビューを実施することにより、人物の信頼度に関して確認することを実施する。
また、登録者本人が想定する自動計算との差異、登録時の情報だけでは判断できない評価ポイントなどの判断についてはインタビューでカバーされ、より精度の高い実力値の見える化が可能となる。（詳細については「第 6 章認定の仕組みつくり」を参照）
将来的には、自由民主党 IT 戦略特命委員会で公表された「デジタル・ニッポン 2017」内で創設を目指すとされている「セキュリティ・クリアランス(SC)制度」などとの連携なども視野に入れる。

2.8.　スキル評価の表現について

前述した6つのスキル評価基準(「A」～「F」)について、どのようなアウトプットを想定しているかを説明する。

2.8.1.　スキル評価の表現方法、考え方

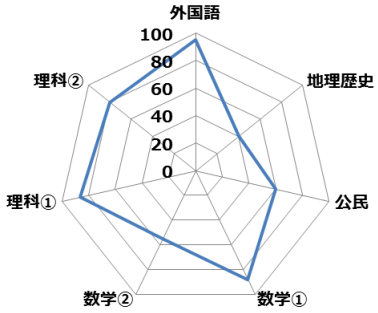
●「A:テクニカルスキル」
●「B:各種資格」
●「C:研修・講義等受講履歴」
●「D:タスク／業務実力(業務経験)」

この4つの指標については数値化しているが、優劣を定義する資格や試験のように「合否」や「適／不適」を判定するものではない。また、初級/中級/上級やAランク/Bランクなどの絶対的な表現ではない。指標項目に対して“どのような状態にあるのか”を表すものである。

例えば、大学入試センター試験のようなイメージとなる。

X 子さん

外国語	95 点
地理歴史	40 点
公民	60 点
数学①	88 点
数学②	55 点
理科①	86 点
理科②	80 点

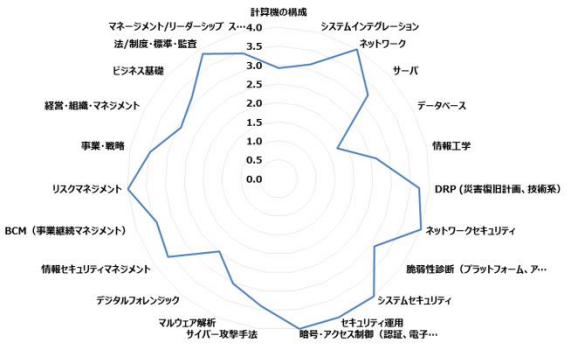


＊X 子さんは*“外国語が 95 点、地理歴史が 40 点・・・・・・・です”*ということ。

上記と同様に、スキル評価は *“A さんは・・・・・・・・・・・・・という人”* となる。

A さん

計算機の構成	2.9
システムインテグレーション	3.1
ネットワーク	4.0
サーバ	3.2
データベース	1.8
情報工学	2.6
DRP (災害復旧計画、技術系)	3.7
ネットワークセキュリティ	4.0
脆弱性診断 (プラットフォーム、アプリ等共通)	3.1
システムセキュリティ	4.0
セキュリティ運用	4.0
暗号・アクセス制御 (認証、電子署名等)	4.0
サイバー攻撃手法	3.4
マルウェア解析	3.0
デジタルフォレンジック	2.5
情報セキュリティマネジメント	3.6
BCM (事業継続マネジメント)	3.4
リスクマネジメント	4.0
事業・戦略	3.5
経営・組織・マネジメント	2.9
ビジネス基礎	3.1
法/制度・標準・監査	3.9
マネージメント/リーダーシップ スキル	3.4



セキュリティ業務遂行能力がJTAGの基準でどの位置にあるかということであり、その判定基準が技術偏重ではなくあらゆる組織のセキュリティ業務を考慮していることに重要な意味を持つ。

また、JTAG のアウトプットとしては評価対象者の“セキュリティ業務遂行能力を数値化したスコア”、“業務カテゴリに分解されたスコアから算出される各業務への適合度”、さらにより精度の高い適合性を見つけ出すための“コンピテンシー情報”となる。

●「E:コンピテンシー・ヒューマンスキル・コンセプチュアルスキル」
●「F:人」

性格や行動の特性が業務内容への向き不向きを左右するのではないかという漠然とした体感は

ないだろうか。具体例を挙げていうと、営業担当とプログラマーを比較した場合、業務内容の違いからそれぞれに求められる素養もまた異なるだろうと想像ができ、その「素養」にはスキルだけでなく、性格や行動特性も含まれるのではないかということである。

粘り強く継続作業ができる人、アイデアに富んですぐに行動に移せる人、コミュニケーションが得意な人など、人それぞれの得意分野があり、それぞれの個性と業務上必要とされる行動の方向性が近ければ、より高いパフォーマンスを発揮できるのではないかと考え、JTAG ではそれを裏付けるための分析を進めている。最終的には、セキュリティ人材に必要なコンピテンシー可視化し、指標として定義することを目標としている。

先天的に備わっている「性格」は変えにくいものである一方で、「行動特性」は思考の仕方をトレーニングすることで後天的に得られるものである。「性格」の受容、かつ「行動特性」の訓練によってスキルアップ、キャリアアップを図ることができることが可能になる。指標化されたコンピテンシー情報により、より高い適性の方向性が見えることが期待される。

また、利用者側の立場ではスキルとコンピテンシーを有機的に連携させたビジュアル的にも分かりやすい表現方法が必要である。そのためには、サービスとして享受できるような仕組みを前提に検討することが重要であり、WG 内で継続検討している。

2.8.2. 評価基準「A」「B」「C」「D」項目の表現方法：セキュリティ業務遂行能力総合スコア

スキル評価指標項目の大項目23種類（図 12）において、JTAG 評価レベル定義（図 11）のレベル設定に由来する7レベルを上限とし、7レベル×23分類の161ポイントとする。また、そのスコアをレーダーチャートとして視覚的にも3表現する。レーダーチャートは上から時計回りに、「IT テクニカルスキル」「セキュリティテクニカルスキル」「マネージメントスキル」で領域が分かれており、強み弱みがどの領域に分布しているかについて把握できる。

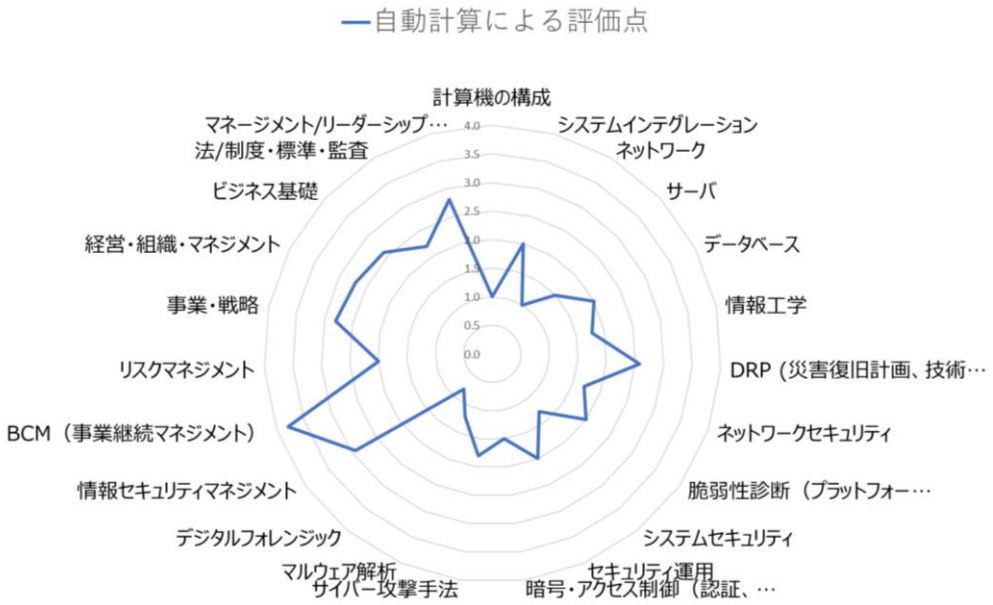


図 14　セキュリティ業務遂行能力のレーダーチャート（サンプル）

なお、JTAG としては登録者本人の評価だけでなく、主だった業務/職務/役割の理想モデルについても同様の評価軸で定義して比較ができるようにしている。次の「第3章サンプルプロファイル」で解説をしていく。

2.8.3. 「E:コンピテンシー」「F:人」項目の表現方法

評価基準「A」「B」「C」「D」項目とは違い、数値で表現するのは難しい。「E:コンピテンシー」については業務/職務/役割ごとの適性や傾向などを関連付けた表現ができるように検討中である。また、「F:人」については前述の 2.7 項で説明しているように、「A」～「E」についての確認という意味合いとなる。ただし、○×などという判断ではなく、あくまで“その時点での人物像や実力値に対して本人とのコミュニケーションによって確認をした”、という表現方法となることが想定される。

3. サンプルプロファイルの策定について

3.1. サンプルプロファイルのねらい

セキュリティ人材の育成にあたり、各種スキルの評価基準を設定し、それらの評価を行うことは重要であるが、それと同じくらいに重要なことが「どのようなスキルをどのレベルまで高めることにより、どのような業務に従事することができるのか」、という指標を示すことである。

セキュリティ人材と一言で括っても、セキュリティ専門部門の第一線で活躍する者、経営者の補佐役となる者、あるいは、法務やコンプライアンスなどセキュリティに関連した部門での業務に従事する者など様々である。また、業務を行う立場についても、セキュリティや IT 企業でサービスやソリューション提供する側と、それらを自社の業務として活用する側とで分かれてくる。

これらを全て一元的に網羅するのは困難であるが、代表的なものを選び出し前章で取り上げたスキル評価基準の組み合わせによって表した。その結果、それぞれのサンプルプロファイルと自身の現状とのギャップを測ることができ、向上させるべきスキルと向上の程度を把握することができる。具体的に把握できれば個人レベルでのスキル向上の目標がさらに明確になる。同時に、組織レベルでも必要な人材像が明確になり、効果的な人材育成策の策定と実行が可能になる。また、複数のサンプルプロファイルを組み合わせることにより、組織やチームの機能として必要なスキル種類とレベルを見える化することもできる。

サンプルとなる業務の選び出しに際しては、JTAG で参照している既存のフレームワークに加えて、下記の文書で定義されている職種なども参照した。なお、JTAG キャリアデザイン WG で策定している「キャリアパスグランドデザイン」(※20)とも連動している。いずれの業務モデルも専門職ではなくてもセキュリティに関連した業務に従事するケースを念頭において設定されている。

＜サンプルプロファイル策定にあたって追加で参照した文書＞

参照対象	文書名
CSIRT(※21)の役割	日本 CSIRT 協議会 「CSIRT 人材の定義と確保 Ver.1.5」
セキュリティ対応組織の役割	ISOG-J 「セキュリティ対応組織（SOC/CSIRT）の教科書」

なお、これらはあくまでサンプルとしての位置づけであり、職種や職責は企業・団体によって異なるものであるので、その点は使用に際して適宜読み替えていただきたい。

また、セキュリティ人材の業務は、セキュリティや IT の技術の進化、あるいは、社会の動きに伴って変化していくので、サンプルプロファイルも今後、定期的にアップデートしていく予定である。

（※20）キャリアパスグランドデザインの考察 V1.0
https://www.jnsa.org/isepa/images/outputs/JTAGreport2019_CD.pdf

（※21）CSIRT: Computer Security Incident Response Team
組織の情報セキュリティ問題を扱うインシデント対応チーム

3.2. サンプルプロファイルの体系について

サンプルプロファイルの作成にあたり、セレクトしたサンプルプロファイルをどのように体系づけるかを検討した。その結果、業務毎の分類では不十分であるとの結論に至り、「業務・役割」の上位に「領域・分野」の概念を設けることにした。これにより、例えば同じ「マネージャ」でも、「CSIRT」領域の「マネージャ」なのか、「セキュリティ診断サービス」領域の「マネージャ」なのか区別を行うことができ、より正確なサンプルの定義が可能になる。

結果として、次の3つのカテゴリ毎にそれぞれ領域・分野を定義した。

＜分野・領域のカテゴリと属性＞

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

IT 利活用部門におけるセキュリティ人材対応の必要性を鑑み、セキュリティ以外の IT の部分を手厚くした。そして、同様の理由で、IT 以外の分野でセキュリティ業務に従事する「プラス・セキュリティ」の分野もやや幅広く設けた。

3.3. IT 専門職（セキュリティ）

セキュリティを専門とする IT 業務の領域・分野として、SOC(※22)・CSIRT・IR（インシデントレスポンス）・セキュリティ診断サービスを選び出し、それぞれ次の業務・役割を現時点で設定した。（追加や細分化、再整理は継続して検討していく）

これらの分野・領域は、セキュリティソリューションを専門に提供している IT 企業やその部門、あるいは、ユーザー企業のセキュリティに関係する部門での就業を想定している。この理由により、ユーザー企業のリスク管理部門、情報システム部門、IT 利活用部門などにおけるセキュリティ関連業務に関しては、後述の「3.4. IT 専門職（非セキュリティ）」に含めた。

第一階層：領域・分野	第二階層：業務・役割					
SOC	マネージャ	オペレーター	分析業務	情報収集業務		
CSIRT	マネージャ	現場責任業務	POC	分析業務	情報収集業務	評価業務
IR（インシデントレスポンス）	マネージャ	現場責任業務	分析業務			
セキュリティ診断サービス	マネージャ	診断責任者	コーディネーター	診断担当者		

図 15　IT 専門職（セキュリティ）職種一覧

3.4. IT 専門職（非セキュリティ）

セキュリティ以外の IT 分野として、次の 25 の領域・分野を選び出し、業務・役割を設定した。これらの分野・領域は、セキュリティ以外の IT ソリューションを提供する IT 企業、あるいは IT に関連

(※22) SOC: Security Operation Center
企業などにおいて、情報システムを監視し、サイバー攻撃の検出や分析、対応策のアドバイスなどを行う組織

するユーザー企業の部門での就業を想定している。そのため、「セキュリティ」とは、前述の通り、ユーザー企業のリスク管理部門、情報システム部門、IT 利活用部門などにおける就業を想定している。

各領域・分野については、IT 全般をカバーするとともに、企業内でセキュリティに関連することが多いと思われるものを選び出し、業務・役割を割り振った。なお、クラウドと EA(※23)/アーキテクトに関しては、他領域・分野と幅広く関連することを考慮して、同領域・分野からのアプローチとなる「逆引き」と、他の関連分野・領域からのアプローチとなる「順引き」がそれぞれ可能な形にした。

また、IT 部門の業務ではないが、リスク管理部門の主要業務でセキュリティとも関連が深く、現在では IT 抜きでの業務遂行が想定できないことから、「リスクマネジメント」「内部統制」も領域・分野に含めた。そして、特に IT に特化した分野については、「IT リスクマネジメント」、「IT 内部統制」として独立して分類した。

第一階層：領域・分野	第二階層：業務・役割					
経営	CIO	CTO	CSO / CISO	CRO		
情報システム	マネージャ	ITインフラ運用	システム開発			
セキュリティ	CSO / CISO	マネージャ	エンジニア	リサーチャ		
サイバー攻撃/調査	マネージャ	POCノティフィケーション担当	オペレーター・分析業務補助	分析業務		
ITリスクマネジメント	CRO	マネージャ	エンジニア	アナリスト	法的対応	
リスクマネジメント	CRO	マネージャ	オペレーショナルリスク担当	法的対応	財務リスク担当	不正検知担当
IT内部統制	マネージャ	IT全般統制	IT業務統制			
内部統制	マネージャ	全社統制	IT全般統制	IT業務統制	業務統制	
IT企画・戦略・予算	マネージャ	業務担当者	戦略企画			
ネットワーク（含 クラウド）	マネージャ	エンジニア	アーキテクト	オペレーター	運用エンジニア	研究開発
業務系アプリケーション（含 クラウド）	マネージャ	開発エンジニア	アーキテクト	オペレーター	運用エンジニア	研究開発
Webアプリケーション（含 SaaS）	マネージャ	開発エンジニア	アーキテクト	オペレーター	運用エンジニア	研究開発
組み込みソフトウェア開発	マネージャ	エンジニア	研究開発			
サーバ/ストレージ（含 クラウド）	マネージャ	エンジニア	オペレーター	アーキテクト	研究開発	
データベース（含 クラウド）	マネージャ	エンジニア	オペレーター	アーキテクト	研究開発	
OA機器（PC・スマホ・タブレットなど）	マネージャ	エンジニア				
サービス（ヘルプ）デスク	マネージャ	アナリスト	オペレーター	エンジニア		
IT社内（外）教育・インストラクター	マネージャ	インストラクター	戦略企画	啓発担当		
ITプロジェクト	マネージャ	システム開発	戦略企画			
システム監査	マネージャ	システム監査（全般）	ネットワーク・セキュリティ監査	クラウド監査	リスク監査	
ITコンサルタント	マネージャ	ソリューション	マネジメント	セキュリティ	リスク	戦略
BCM/BCP 事業継続	マネージャ	一般事業継続担当	IT事業計画担当	IT－DRP担当	BIA(事業影響度分析）担当	
プリセールス	マネージャ	ソリューションコンサルタント	エンジニア			
クラウド	ネットワーク	サーバ/ストレージ	アプリケーション	アーキテクト	戦略企画	
EA／アーキテクト	マネージャ	ネットワーク	アプリケーション	サーバ/ストレージ	データベース	クラウド

図 16 IT 専門職（非セキュリティ）職種一覧

（※23）EA：Enterprise Architecture エンタープライズアーキテクチャ

3.5. プラス・セキュリティ

第一階層：領域・分野	第二階層：業務・役割		
プラス・セキュリティ：購買	マネージャ	業務担当者	
プラス・セキュリティ：営業	マネージャ	業務担当者	
プラス・セキュリティ：販売	マネージャ	業務担当者	
プラス・セキュリティ：一般事務	マネージャ	業務担当者	
プラス・セキュリティ：庶務（秘書を含む）	マネージャ	業務担当者	
プラス・セキュリティ：総務	マネージャ	業務担当者	
プラス・セキュリティ：財務	マネージャ	業務担当者	
プラス・セキュリティ：経理	マネージャ	業務担当者	
プラス・セキュリティ：人事	マネージャ	業務担当者	
プラス・セキュリティ：法務	マネージャ	業務担当者	アシスタント
プラス・セキュリティ：内部監査	マネージャ	業務担当者	アシスタント

図 17　プラス・セキュリティ職種一覧

セキュリティに関連すると思われる非 IT の分野として、次の 11 の領域・分野を選び出し、業務・役割を設定した。これらの分野・領域は、IT 企業・ユーザー企業を問わず、IT に関連しないが、セキュリティとの関連がある、あるいは、セキュリティのスキルが要求されると思われる部門での就業を想定している。例えば、「一般事務」などは、一見するとセキュリティとは無関係なようだが、企業・組織の機密情報や従業員・顧客の個人情報を扱う上ではセキュリティの知識とスキルが必要になるし、それは、「総務」・「庶務(秘書を含む)」などにも当てはまる。

3.6. サンプルファイルの活用

サンプルプロファイルについては登録者評価と同様にスキル評価基準の組み合わせによって表現される。

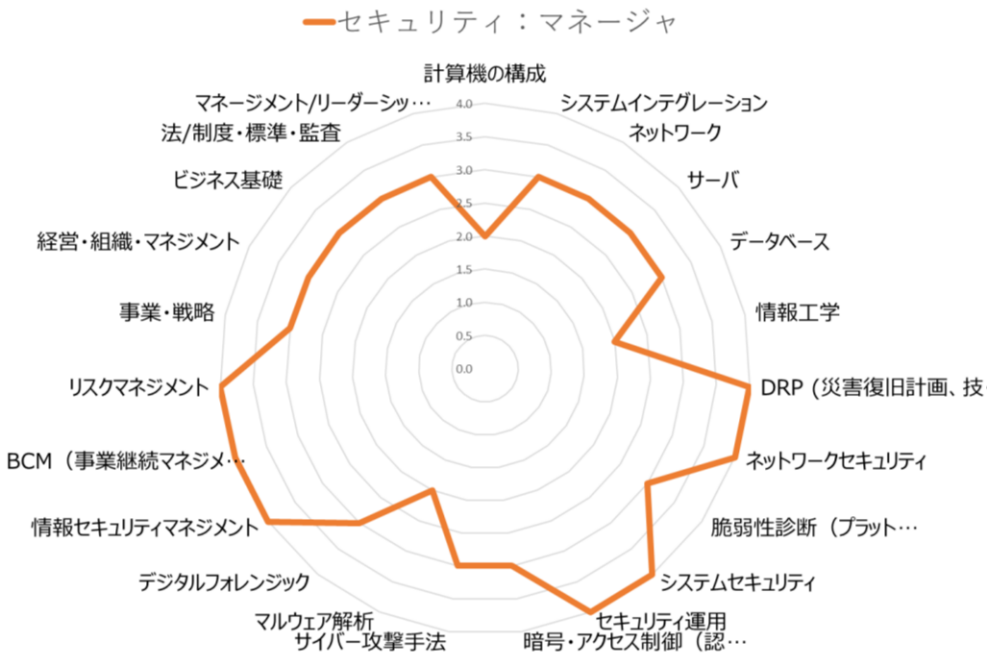


図 18　サンプルプロファイル　レーダーチャート例

そして、スキル診断の結果を同様にレーダーチャートで表現し、上記のサンプルプロファイルのレーダーチャートに重ねることによって現状のスキルレベルとの比較を視覚的に行うことができる。また、比較に際しては、適合度を百分率（パーセント）で表現することで、数値による客観性も担保されている。なお、適合度は 100%以上の数値も許容し、100%以上の適合度の場合は、その業務に対して「オーバースペックである」と表現できるようにしている。

図 19　サンプルプロファイルとスキルチャート例

このような比較により、個人および組織・企業において次のような活用を想定している。

個人：

- 自己のスキルレベル・特定の業務における遂行能力の把握
- 目指す業務とのギャップ把握
- 目指す業務に向けた方策把握
- 求人や特定のセキュリティ業務とのマッチ度把握

企業・組織

- 所属メンバーのスキルレベル・特定の業務における遂行能力の把握
- 組織の能力レベル把握・人材ポートフォリオ作成
- 求人と応募者のマッチ度把握

3.6.1.　個人レベルにおける活用

第一に挙げられるのが、自己のスキルレベルおよび特定の業務における遂行能力の把握である。セキュリティ業務の遂行能力とは専門的なものだけでなく、JTAG の“それぞれの業務における基礎的な能力が必要である”という考えに基づくと、一般的な“仕事をこなす実力”とも捉えることもできる。スコアのポイントでは業務遂行能力の「量」、レーダーチャートでは得意/不得意の「分野」が明らかになるので、自身の現在値を的確に把握することができる。また、セキュリティ関連業務に対して本人もこれまで意識していなかった適性への気づきも期待できる。

次に挙げられるのが、目指す業務とのギャップ把握である（図 19　サンプルプロファイルとスキルチャート例　参照）。

23種類のスキル評価基準項目によって、自らの現在のスキルレベル、および、業務遂行能力と、特定業務に要求されるスキルレベル・業務遂行能力とのギャップが数値化されるので、自らが目指す業務に不足している力はどの分野でどの程度まで伸ばす必要があるかを把握することができる。

そして、ギャップを把握した後には、目指すポジションに向けたアクションプランニングにも活用できる。具体的には、ギャップを埋めるための教育の受講や、特定の分野における一定期間の業務経験である。JTAG においては、ISEPA 会員各社をはじめとする教育事業者との連携を進めており、将来的には、各スキル評価基準とリンクする形で具体的な教育プランを提示する予定である（詳細は「第 4 章：各種教育研修との連携について」参照）。

また、業務経験を区別する場合において、JTAG で策定したサンプルプロファイルの名称が業務や職務、役割の共通言語として使われることが期待できる。

なお、当人の目指す業務がまだ明確に定まっていなかったり、どの業務を目指すべきかについて暗中模索していたりする場合には、求人や特定のセキュリティ業務とのマッチ度把握に活用することにより、現在のスキルと親和性の高い業務を探し出し、具体的なキャリアパスとして視野に入れることが可能になる。また、学生のキャリアデザインにもこの機能としては現時点で活用可能性はある。

3.6.2.　組織レベルにおける活用

活用するにあたり、所属メンバーのスキルレベル・業務遂行能力についてセキュリティを軸に一元的な評価指標で測れるメリットがある。

1）タレントマネージメントツールとしての活用が挙げられるが、それに加えて、定期的に測定を行うことで育成計画とのマッチングの度合・達成度を把握し必要に応じて計画を軌道修正することに役立つ。また、評価指標は数値で出されるので、仮に人事評価への利用をする場合には定量的に行うことができる。各種資格もスキルレベル・業務遂行能力に反映されるので、資格取得を目標とした場合に自己学習計画の策定にも活用できる。また、新卒入社者の業務適性判断や社内における人材発掘への活用も可能である。

2）軸が固定されているため、所属メンバーのスキルレベル・業務遂行能力を足し合わせることで、組織やチームとしてのスキルレベル・業務遂行能力を把握すること、および、組織内の人材ポートフォリオ作成にも活用できる。

たとえば、CISO の設置・任命を計画する際、このツールで可視化された人材を組織が求める CISO モデルに照らし合わせてスクリーニングしたり、そのモデルの機能を特定の一人で満たせない場合は複数人でチームを組成し各人の強みを組み合わせてチームとして CISO 機能を実現したりすることも可能となる。セキュリティ人材の適材適所の配置のみならず、人材配置の充足度をはかる指針となり、事業戦略に応じた組織構築を支えるツールとしても期待される。

なお、セキュリティ業務の遂行にあたっては、各社の業種・規模・組織体系などによって差異が生じてくるので、活用にあたっては、それを加味して多少の読み替えを行う事が必要である。例を挙げると、同じ「セキュリティエンジニア」の業務でも、IT サービスを提供する事業者と、IT サービスを使用する事業者とでは、前者が自ら手を動かして業務を遂行することが多いのに対し、後者はベ

ンダーに指示して自らはマネージメントを行うケースが多い。このような場合、後者に区分される企業においては、マネージャの要素が強くなるので、テクニカル面のスキルレベルは低めで許容される代わりに、マネージメント面のスキルレベルについては高めで要求することになる。具体的には下図のようになる。

図 20　スキルチャート(テクニカル)例

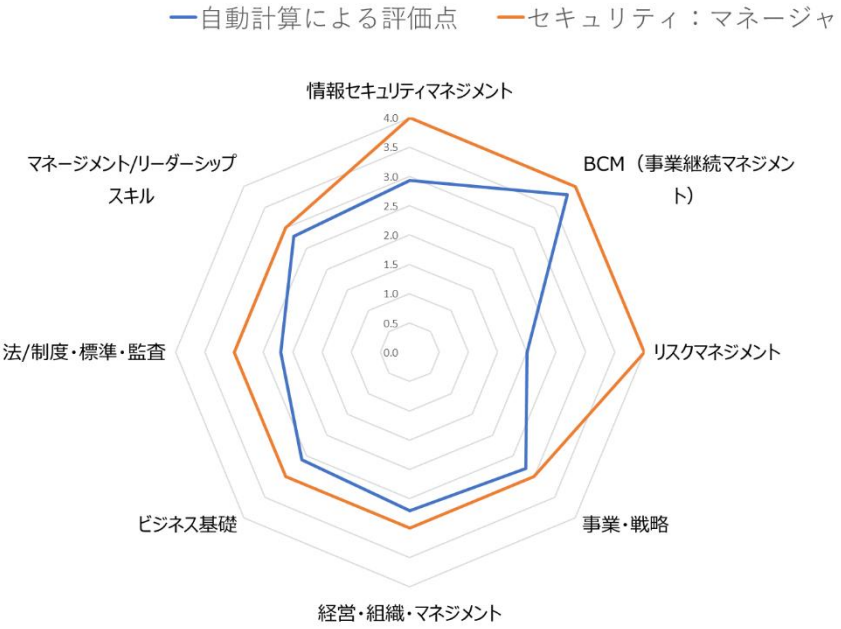


図 21　スキルチャート(マネージメント)例

さらに、外部から人材を獲得する場合には、求人をスキル評価指標及びレーダーチャートで提示し、また、応募者のスキルレベル・業務遂行能力を同様に提示してもらうことで、求人と応募者のマッチ度を比較的正確に把握することができる。こうすることで、自社の要求に対して適性かどうか

把握でき、ミスマッチの発生を最小に抑えながら人材の確保ができる。

また、組織やチームの人材ポートフォリオに沿って組み合わせを基にした「組織サンプルプロファイル」の作成も準備している（例えば CSIRT、SOC、リスク管理部門のサイバーセキュリティチームなど）。

これが実現すれば、現状の組織について「組織サンプルプロファイル」とのスキルレベル・業務遂行能力のギャップを測ることができ、組織育成やチームづくり、また、働きやすい環境づくりなど働き方改革の取り組みにも活用できることが見込まれる。

（詳細は「5.1.2.2. 組織やチームのタレントマネージメントとしての利用」参照）

3.6.3. ユーザー独自のスキル定義も可能

今回策定したモデルはあくまでサンプルである。仮に、自社の形態に合わせて読みかえたとしても業種業態や組織規模、外部への委託度合などによって求められる内容や重要度が各企業・組織で大きく異なってくる場合がある。つまりサンプルプロファイルとは隔たりが出てくる。よって、読み替えでも適合しない場合は、ユーザー側で自社や自組織に適したスキルモデルを設定して、より精度の高いマッチングが可能となる機能も備えていく（図 22）。

図 22 ユーザー定義のモデルと対象者評価点のレーダーチャート比較（サンプル）

4. 各種教育研修との連携について

本プログラムが提供するスキル診断で、本人の現在の実力値と目標とする職種（サンプルプロファイルからのセレクトやユーザー独自のスキルセットなどで設定）とのスキルギャップを特定することができる。そのギャップを埋めるための教育プログラムを、ISEPA 会員各社が提供しているトレーニングを一覧で表示していくことで、効率的な人材育成のための教育研修プランニングガイドとして使用することができる。

ＪＴＡＧスキル指標　教育研修マッピング

大項目	中項目	本人評価点数		サンプルプロファイルでの理想点数	本人にとっての研修有用性	研修のスキル設定 A社 ネットワークセキュ…イ研 a. 受講に際しての前提スキル	研修のスキル設定 b. 受講後期待される到達スキル	本人評価点数と研修のスキル設定との誤差 マイナス値は受講前提レベルを満たしていない ↓ 受講に際しての前提スキルとの誤差	本人評価点数と研修のスキル設定との誤差 マイナス値は有効ではない（本人のスキルを下回っている） ↓ 受講後期待される到達スキルとの誤差
計算機の構成	電子工学	1.4	0.9	2.0	必要	0.5	0.5	0.4	-0.4
	並列、分散コンピューティング		1.7			0.5	0.5	1.2	-1.2
	コンピュータおよび電子デバイスの物理的構成要素とアーキテクチャ		1.2			0.5	0.5	0.7	-0.7
	エンコード		1.3			0.0	2.0	1.3	0.7
	コンパイラ		1.2			0.5	1.5	0.7	0.3
システムインテグレーション	上流設計工程	4.0	4.0	3.0	不要	0.0	0.0	4.0	-4.0
	設計工程		4.0			0.0	0.0	4.0	-4.0
	プログラミング手法		4.0			0.0	0.0	4.0	-4.0
	プログラミング言語		3.1			0.0	0.0	3.1	-3.1
	デバッグ		3.1			0.0	0.0	3.1	-3.1
	テスト工程		3.6			0.0	0.0	3.6	-3.6
	テストシナリオの作成と実行		3.5			0.0	0.0	3.5	-3.5
	コンピュータネットワークの構成		3.4			1.0	2.0	2.4	-1.4
	セキュアなシステム設計に関する知識		2.8			0.0	0.0	2.8	-2.8
	セキュアプログラミングに関する知識		2.9			0.0	0.0	2.9	-2.9
セキュリティ運用	運用手法	3.5	3.2	4.0	必要	0.0	1.0	3.2	-2.2
	製品知識		2.8			0.0	1.0	2.8	-1.8
	セキュリティシステムリスクマネジメント		3.3			0.0	1.0	3.3	-2.3
	インシデントハンドリングに関する知識		3.9			0.0	1.0	3.9	-2.9
暗号・アクセス制御（認証、電子署名等）	暗号	3.1	2.6	3.0	不要	0.0	0.5	2.6	-2.1
	アクセス制御		3.6			0.0	1.0	3.6	-2.6
サイバー攻撃手法	サイバー攻撃基礎知識	2.8	2.8	3.0	必要	0.0	1.0	2.8	-1.8
マルウェア解析	マルウェア解析基礎知識	2.5	3.1	2.0	不要	0.0	0.5	3.1	-2.6

図 23　教育研修のスキルとのマッピング表（例）

マッピングについての基本的な考え方、設定方法は下記となる。

a. 受講するための前提として必要なスキルを JTAG レベル指標に基づいて数値化
b. 受講完了で到達が期待されるスキルについて数値化
c. 本人のスキルとのギャップに基づいて推奨される方策の提示
　例）到達期待より本人のスキルが下回っている場合に、ある閾値設定に基づいて、有用性ある研修が推奨として提示される。また、受講するための前提スキルについては本人のスキルが研修設定のスコアより相応に下回っている場合は提示しない、などの方法で目指すサンプルプロファイルとのギャップに対して自動的に推奨研修が提示されるような仕組み化を継続検討中。

5. 各種サービスとしての提供可能性について

人材像、スキルの可視化について可能な限り精度を上げていく方策とロジックの基盤はできてきた。同時に、そのデータをどのように活用していけるのか、どのように利用できたら嬉しいのか、ユーザー視点からの利用シーンをもとにサービスとしてのイメージを検討してきた。

また、可視化利用のステップ以前に、大きな枠組みとしてキャリアグランドデザインを描くことがとても有効である。この点については先般公開したキャリアデザイン WG のレポートで提唱している「キャリアキューブ」との連携も利用価値が高まる。

なお、「キャリアキューブ」はセキュリティに限らず、他領域においても基本となるエッセンス、考え方は活用できる可能性を秘めている。

5.1. 人材関連サービスとしてのイメージ

活用の幅を広げるためには需要側のニーズやデータを同時に収集することが鍵となる。そのデータを登録者のデータと連携することで、JTAG の目的である組織内外における人材の流動化に役立ついろいろなサービスが可能となってくる。また、登録数やニーズ数が増加するほど、より精度が上がることでマッチングに対してもさらに的確なものになっていく。

なお、登録された実力値や人材像の情報について JTAG で「○○さんは、JTAG 評価での○○○○○のとおりの人材です」と認定することで、企業や組織などの需要側に対して大きな安心感を与えることができる。(認定の仕組みについては次の第 6 章で解説)

注1) 活用例示はビジュアル的に説明するためのアイデアベースであり、JTAG として提供を約束しているものではない。

注2) 「3.6.サンプルプロファイルの活用イメージ」も併用参照いただきたい。

5.1.1. セキュリティ人材採用活動への活用

登録データから要望する人材をセレクトできれば、より的確な人材採用アクションの助けとなる。さらに、ユーザーの独自定義で重要スキルにメリハリをつけたサーチができれば、さらに適材適所への近道になる。JTAG メンバー企業、トライアル協力企業、キャリアデザイン WG のインタビュー協力者など多数の方々からの意見としては当然ながら一番多く、また、早期実現の要望であった。

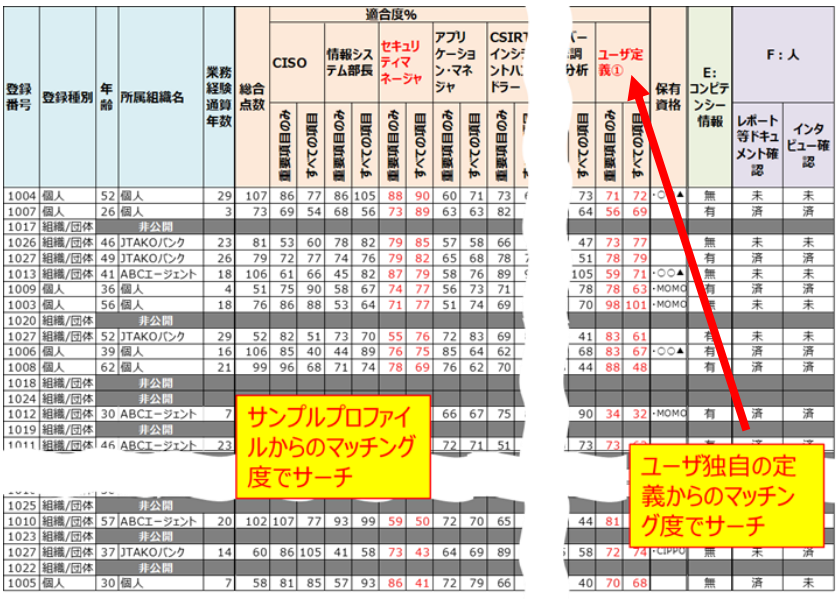


図 24

5.1.2.　自社のタレントマネージメントとしての利用

自社の人材についてセキュリティスキルをアップさせたい、ある人材をセキュリティ関連の仕事にシフトさせたい、セキュリティに関連する新しい組織やチームをつくるときに的確な人材をアサインしたい等々、人に起因する課題は多い。対象者のスキルが見える化されることでこのようなケースでのタレントマネージメント目的での利用価値があがる。

5.1.2.1.　個々人の育成視点

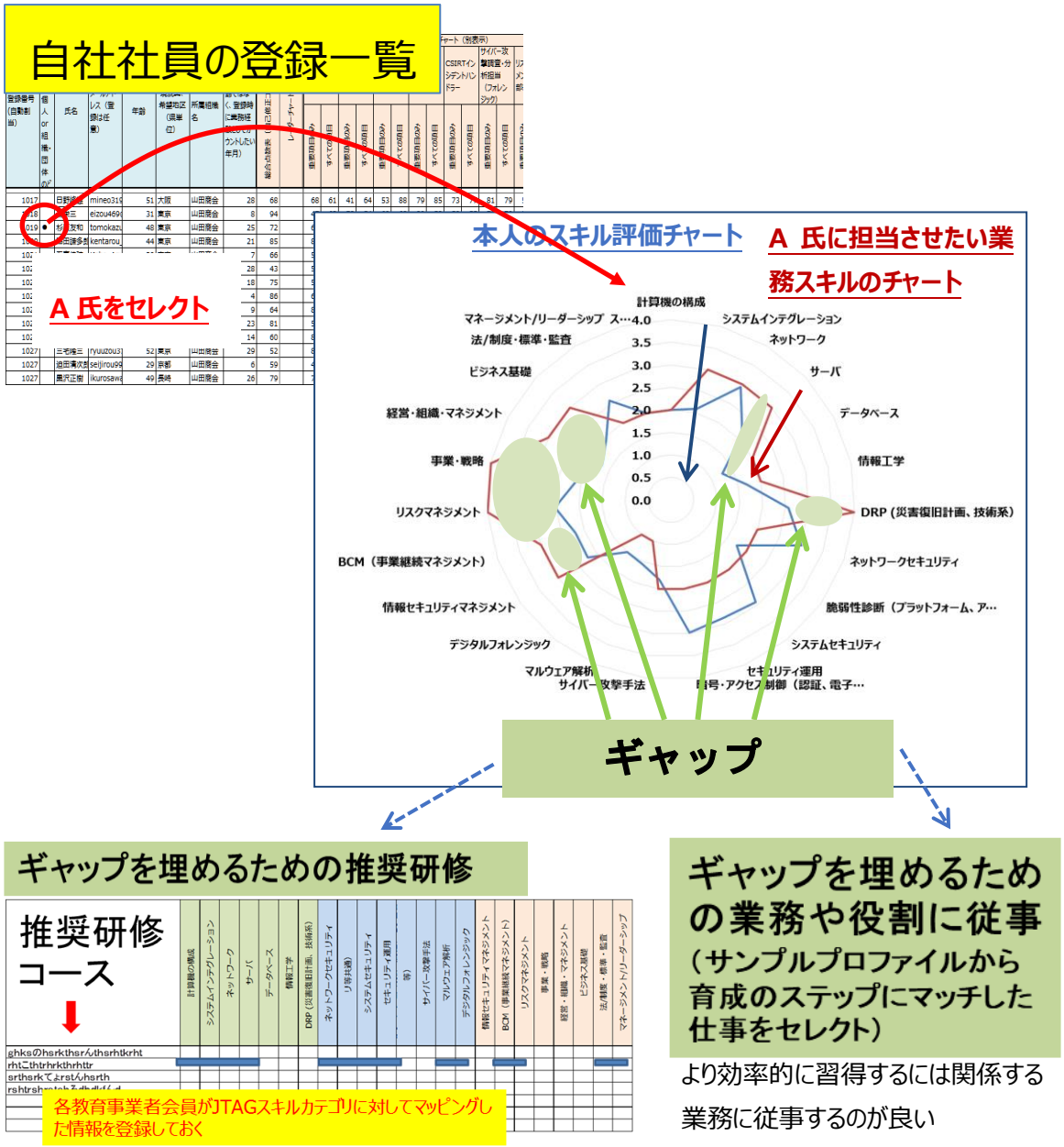


図 25

ギャップをおぎなうための研修や、ステップとなる業務について計画が立てやすくなる。

5.1.2.2. 組織やチームのタレントマネージメントとしての利用

組織やチームの人材ポートフォリオに沿った組み合わせを基に「組織サンプルプロファイル」を作成し、メンバーのレーダーチャートを重ねることで、スキルレベル・業務遂行能力のギャップを測ることができる。

(例):新たに CSIRT をつくるためにメンバーを 4 人アサイン予定していたとする。まずは、自社の CSIRT としての必要なスキルやそのレベル感を設定して、予定メンバーの状態と比較する。

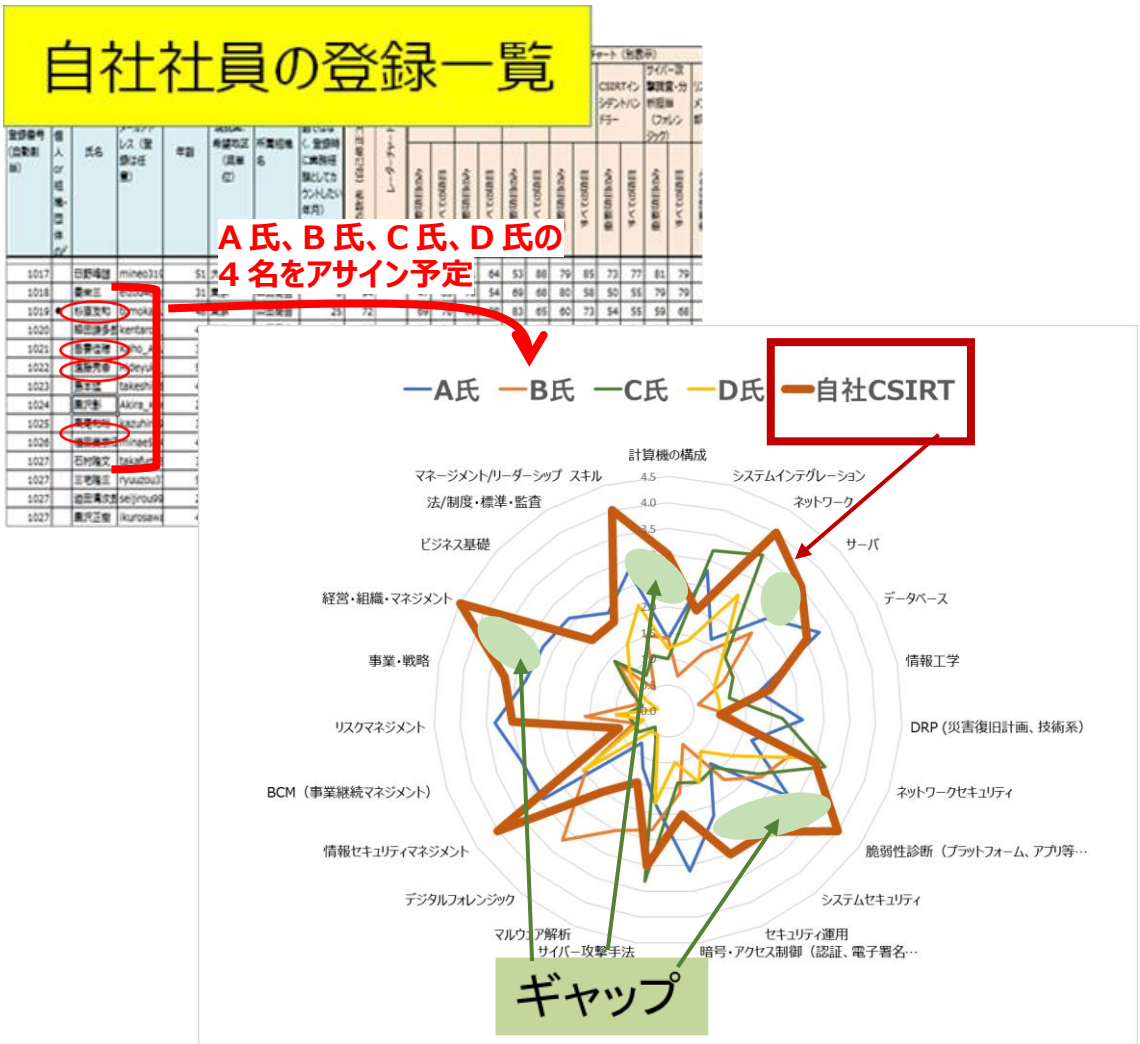


図 26

この比較において組織やチームの満たしたい機能に対してのギャップが掴める。このギャップをおぎなうための、いろいろな方策が具体的に検討できる。
例えば、ギャップ部分についてユーザーが独自に定義をして他の社員に対して適用して探したり、もしくは、その 4 人を早期教育して鍛え上げたりする計画をたてるという対策もありえる。また、社外からの力でギャップを埋めるという策も検討できる。その際には、ギャップ部分(要望するスキル)について具体的に提示することで派遣や業務委託での対応や、パートナー先に外注するときのミスマッチを減らすことが可能となる。

5.1.2.3. 派遣や業務委託など人材サービス利用時への応用（提供側、需要側双方）

需要側としては、委託内容の必要スキルを具体的に提示できる。また、提供側としては要望に対してより的を絞った無駄の少ない提案が可能となる。派遣採用に限らず、昨今利用が拡大している業務委託について、スキルのミスマッチや力量の見誤りが発生することで需要・供給双方にとってロスが起きるリスクがある。それを防ぎ生産性をあげる事業活動にとって大きな役割を担える可能性がある。

人材ニーズ情報

セキュリティマネージャー ▼ | 10年以上 ▼ | 40歳以上 ▼ | 東京近郊 ▼

企業名	会員区分	ニーズ登録日	要望業務		その他要望内容				
			業務名	あなたのマッチング度（重要項目のみ）	業務経験年数	年齢帯	地域		緊急度
[redacted]	C会員	20181112	セキュリティマネージャー	84%	15年以上	40～60	東京近郊	1200～	高い
	C会員	20181124	セキュリティマネージャー	84%	10年以上	40～50	東京近郊	～1000	普通
	C会員	20171221	セキュリティマネージャー	84%	10年以上	40～50	東京近郊	～1000	高い
	C会員	20181221	セキュリティマネージャー	84%	15年以上	40～50	東京近郊	1200～	普通
	C会員	20181129	セキュリティマネージャー	84%	20年以上	60～	東京近郊	1300～	比較的高い
	A会員	20181114	セキュリティマネージャー	84%	10年以上	40～50	東京近郊	～1000	普通
	A会員	20181010	セキュリティマネージャー	84%	20年以上	40～60	東京近郊	1000～	比較的高い
	A会員	20181214	セキュリティマネージャー	84%	20年以上	60～	東京近郊	1000～	高い
	B会員	20181126	セキュリティマネージャー	84%	15年以上	40～60	東京近郊	～1000	高い

図 27

＊ニーズに対しての情報がたくさん集まるほど、より精度の高いマッチングが可能となっていく。

需要側：
要望業務についてのスキルレーダーチャート

供給側：
要望に対してセレクトした人材のレーダーチャートを比較して提案

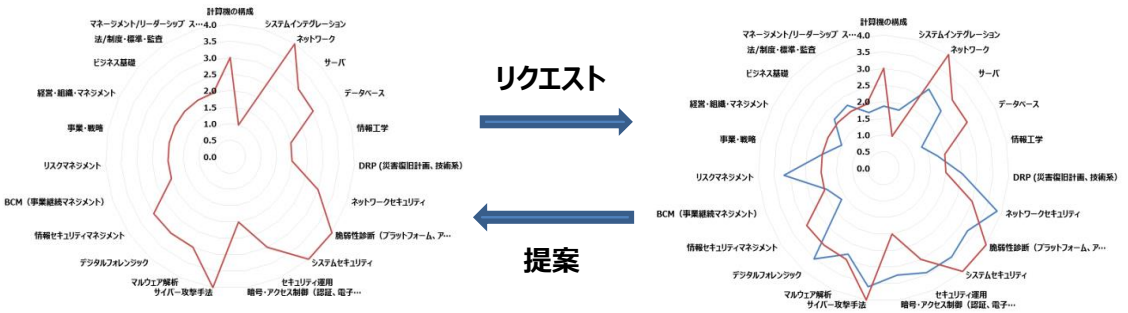
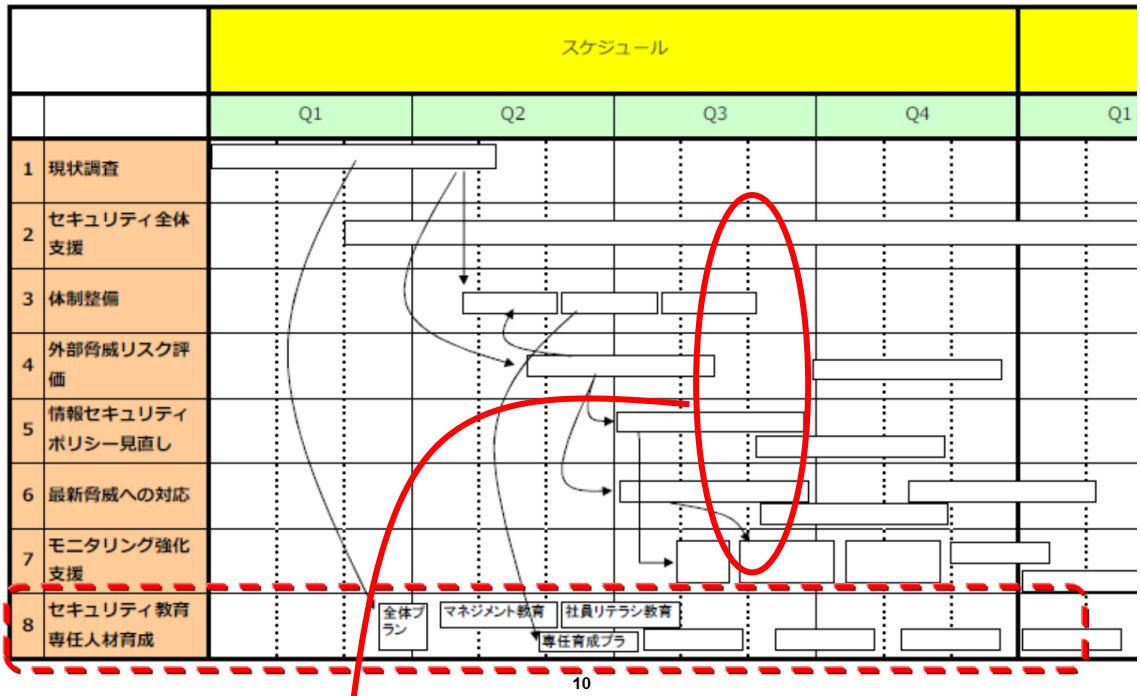


図 28

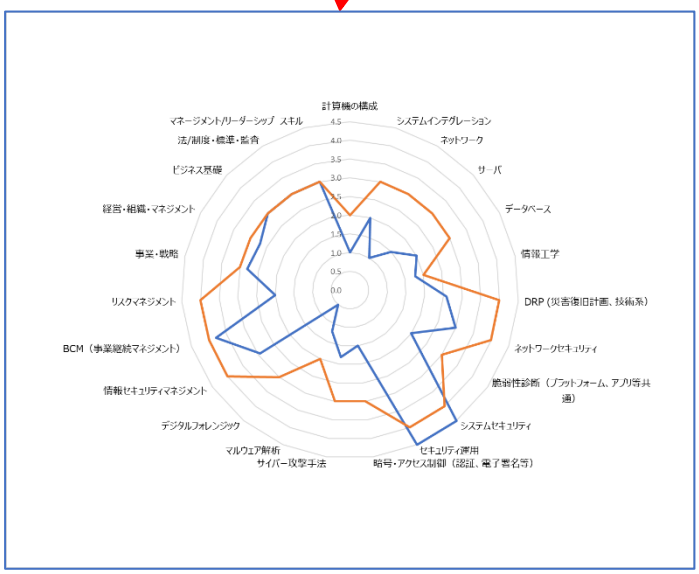
5.1.2.4. セキュリティ施策実行時の活用

企業においてセキュリティ施策を立案し実行するためには、それぞれのステップやフェーズにおいて、その施策を遂行する「人」の課題は無視できない。推進できるリーダーはいるのか、その内容を高いレベルで遂行できる人材はいるのか、いないとしたら他から調達できるのか、できない場合は施策の変更が必要となるかなど、施策の根本的な部分を揺るがす場合もある。つまり、人材リソースが解決されないと、施策も「画に描いた餅」となってしまうことから、人材リソースの育成や確保の計画は施策を立てる上の要素としては必ず組み込むことが重要である。

このような場合に、きめ細かな計画立案と柔軟な人材の異動や変更に対してスキル可視化が手助けになる。



例）このフェーズで必要となる●▲■の人材は、、、



時間軸を含め、施策フェーズごとに対して人員配置、調達（社内外）など、きめ細かいプランニングに活用

図 29

5.2. キャリアグランドデザインとの連携

JTAG のキャリアデザイン WG は、キャリアパスグランドデザインと題して、キャリアの在り方を描く活動をしている。2019 年上期の成果物では、「キャリアキューブ」の提唱を行った。

セキュリティ人材のキャリアモデルを明確化する事は、キャリアをスムーズに進めるとともに、キャリア形成を支援するためにも必要であり、重要な要素となっている。スキル可視化は或る一時点の能力評価を詳細に表すものに対し、「キャリアキューブ」は長期視点での経歴や経験を表すことに優れている。それぞれを使い分け連携して利用することでさらに明確な道筋をたてることに役立つ。（詳細は、「キャリアパスグランドデザインの考察_ver1.0」(※24)参照）

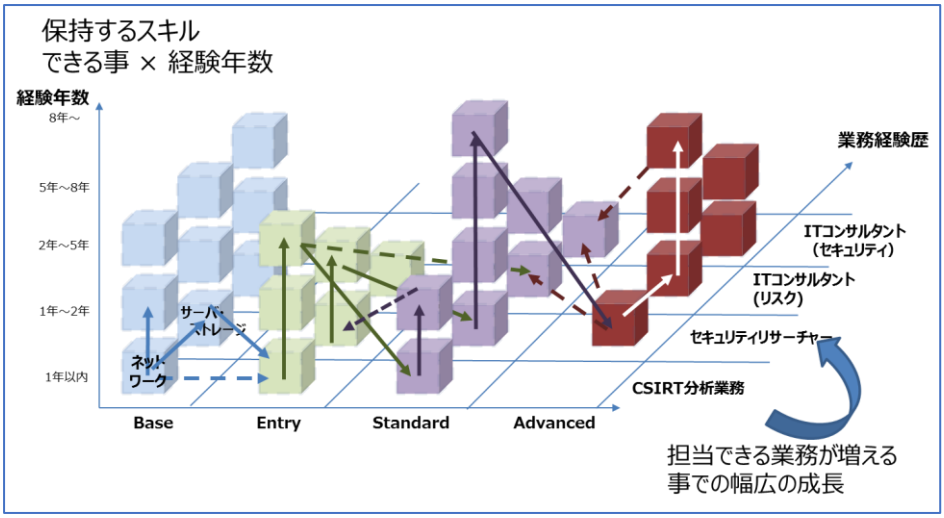


図 30

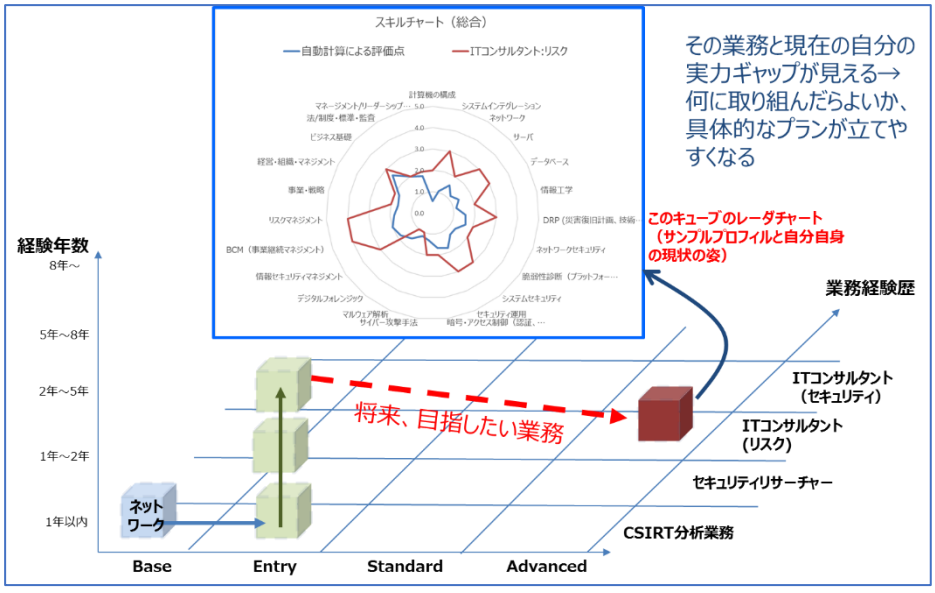


図 31

(※24)キャリアパスグランドデザインの考察_ver1.0
https://www.jnsa.org/isepa/images/outputs/JTAGreport2019_CD.pdf

5.3.　各種情報提供

需要側と供給側双方のデータが蓄積されることで、キャリアデザインに対していろいろな情報提供や分析が可能となっていく。需要と供給双方の情報をもとにしたニーズや市場分析などのマーケット情報、コンピテンシーとの相関分析情報、職/スキル/市場などの将来予測など、多数のデータの蓄積されるほど良質のアウトプットができてくる。

また、需要側が一元的な JTAG 指標に基づいたより具体的なニーズ情報を提供することで、獲得競争は厳しくなる可能性もあるが、マーケット全体が増大することで個々の企業にとっては職のミスマッチが防げる可能性が高くなる。これは、登録ニーズのボリュームの効果だけではない。例えば、需要側に対して JTAG としての認定がされることで、供給側としてはより安心して流動化のモチベーションを高めることができる。(「企業認定」については今後検討予定)

5.4.　サービス化への課題

ここまでアイデアベースでの利用シーンを提示してきたが、実際に効果的かつ効率的に利用してもらい人材の適材適所、社内外における人材の流動化が促進されなければ意味がない。

これまで可視化の仕組みは windows のエクセルベースでブラッシュアップを重ねてきたが、自動的に数値化するためにレーダーチャートやマッチング度算出の裏側では多種多様、さらに多量のインプット情報が複雑な計算ロジックで動いている。また、対象者が登録する際の簡便さ、分かりやすさについては意識して作成してきたが、エクセルでは UX(User Experience)(※25)に優れているとは言い難い。

今後、データを役に立つ姿でアウトプットし縦横無尽な方法で利用できるようにするためには、やはり UX に優れたシステム化が必須である。

(※25)UX(ユーザーエクスペリエンス):ユーザーが製品やサービスを通じて得ることのできる体験やユーザーが感じたこと。またサービスの質に関わることも指す。

6. 認定の仕組み作りについて

JTAG 構想においてセキュリティ人材のスキル認定制度構築はとても重要な基盤である。認定をするからにはできるだけ公正・公平な情報と方法に基づくことが必須である。それが大前提のスキル可視化、人物像の見える化である。

ここで開発したスキルを測るツールでは、自己の業務経験や取得資格により各専門分野における評価を測定できる。しかしツールでの入力項目では判定しきれない活動や実績、その評価が第三者的に認定されることは、本人のキャリアパスや採用企業にとって非常に有意義であり、JTAG の主旨からすると重要な要素だと考える。

そこで JTAG では中立公正な認定者（アプレイザー）の設定準備を検討している。アプレイザーは基本的に被認定者 1 人に対して2人以上の対応が良い。複数人でインタビューや追加の資料を検討することにより、個人のスキルを認定する事を想定している。なお、“認定”という意味は、アプレイザーがその権限で登録者に対してレベル付けして評価をするものではない。JTAG 登録に際してはあくまで自己申告となり、結果は自動的に算出される。それに対しての誤差や自動計算では表現されない部分についてなどを、本人との面談などで確認するというものである。その意味合いとしては、例えば不動産の場合、その物件は登記簿通りのものかなどと確認する“鑑定士”のイメージに近い。

アプレイザーに任命されるには、その妥当性や中立性を担保するために、JTAG とは別組織の高度業務経験者や学識経験者で構成されるアプレイザー認定委員会（仮称）により承認されるのが良い。また、登録者は技術者だけに限らないため、アプレイザーも事業系やマネージメント系など比較的幅広い人選が必要と思われる。

なお、スキル可視化の利活用は IT 業界に閉じたものではなく、あらゆる業種で利用されることで社会全体の情報セキュリティ力の向上に寄与していく。それは「プラス・セキュリティ人材」にも十分にフォーカスしている主旨としても重要なポイントである。よって、運営する側は先端を行く大企業や特定の組織や団体の考えにとらわれることなく常に広い視野を持ち、様々な規模の企業や組織を念頭において、利用のしやすさや馴染みやすさの制度運営が求められる。

7. 今後の活動について

セキュリティ人材の尺度を統一させ、信頼度や真の実力値が判定できる基準策定、ベースとなるロジックの確立はほぼ固まってきた。しかし、JTAG 構想におけるセキュリティ人材のスキル認定制度をつくり普及させ、キャリアパスグランドデザインや各種の需要供給情報の提供などにより、セキュリティ人材の流動化、処遇やポジションの向上を達成するためにはまだ課題は多い。

今後の活動は、優先順位を決めてその課題を解決していくことである。下記に、主だったものについて抽出していく。

7.1. スキル可視化の仕組み

1） 評価基準のブラッシュアップ

先般実施した 300 名を超えるトライアルの結果からも改善点がいくつか見えていることから継続して実施していく。

・資格項目についてはまだ網羅できていないことから、対象者が多いものから順次追加していく。
・登録時の業務経験入力項目については、一旦この状態で仮置きとする。エクセルで作成しているため登録者にとって UX が悪くなってしまう理由も大きい。ただし、微修正については随時行なっていく。
・コンピテンシーについては、トライアル結果の分析を踏まえて、どのように連携させれば効果的なのか検討を継続していく。このパートは採用やタレントマネージメントでの利用時に重要な要素となるので、組み立てれば完了というものではなく、JTAG が存在する限り継続して丁寧に検討していくべきと考える。
・サンプルプロファイルは、キャリアアップグランドデザインとの連動、ユーザー企業のさらなる実体調査（キャリアデザイン WG との連携）にて、次のトライアル実施時までにアップデートをする。
・スキル評価指標精度向上とコンピテンシー関連の連携検討のために3次トライアルを計画する。

2） システム化

エクセルでの可視化は限界にきており、利用価値を高めるためにはシステム化の検討が不可欠となっている。WG メンバーでの検討はもちろんだが、この分野に長けている協力者を得て検討をしていきたい。なお、業務経験など登録者本人の機微な情報を扱うためセキュリティには細心の手当てが必要である。また、単純に点数が出せるだけでなく、UX に優れたシステム化という点も重要となる。次年度初めまでには基本的な機能部分についてサンプルシステムを準備し、3 次トライアルが実施できると良い。

3） 企業認定のための指標検討

企業の認定についても検討を始めていく。特に、供給側が流動先の希望をセレクトする場合には、判断指標として重要な情報となる可能性が高い。

JNSA には様々な部会が活動しており、企業・組織や経営者、CISO における情報セキュリティのあるべき姿や対応策等に対して、豊富な知見とノウハウを有している。これらの部会の協力を得ながら、「人材」についての要素をクローズアップした評価指標としていく。

また、企業認定ということでは他団体でも企業のセキュリティ成熟度やセキュリティ施策の取組等の視点から検討していることから、連携を念頭に進めていきたい。

7.2. プロモーション、外部との連携活動

本格的に活動を開始して約 2 年が経過した。その過程において、ユーザー企業やいろいろな団体との会話を積み重ねてきて貴重な意見を頂戴した。今後はさらに強化をしていき、広く利用してもらうための活動を強化していく。

構想としては、省庁や IPA(※26)、NISC(※27)、FISC(※28)、金融 ISAC(※29)、CRIC(※30)、CSSC(※31)などはもちろんだが、経団連などの一般ユーザーが加盟している団体や、IT 団体連盟や JCIC などとの連携は深めていきたい。また、JTAG からの協力という点では、考え方として親和性がある厚労省の日本版 O-NET についても意義があると考える。

7.3. 認定制度の運営

スキルの可視化を使った認定制度の運用と第 5 章で解説した各種サービスを仮に実現する場合、まずは相応の資金とリソースが必要になる。また、登録者やアプレイザーの募集や、アプレイザーを認定する第三者機関の立ち上げ、利用ユーザーとなる団体や企業・組織などとの調整に労力がかなり掛かることが予測される。

円滑に立ち上げていち早く役に立つ仕組みとして利用者に届けるためには、現在の WG レベルの活動では限界がある。これをひとつの事業として、何かしらの法人（利益追求ではない組織）形式で進めていくことが最適だと思われる。

これは運営上の問題だけでなく、JTAG の仕組みを普及させて、人材の社内外での流動化を図りセキュリティ人材を増やしていく観点から、セキュリティベンダー中心ではなく多種多様な業種/業態のユーザー企業や団体との協力体制が鍵になる。そのためにも、ISEPA 内の活動の一部ではなく、独立した組織としての体を成すことが効果的と考える。早期に JTAG メンバーや現在協力をいただいている有志によって立ち上げていく活動も並行していきたい。特に、システム化についてはある程度の投資が必要になるため、重要なステップとなる可能性が高い。

(※26) IPA: Information-technology Promotion Agency, Japan 独立行政法人情報処理推進機構 https://www.ipa.go.jp/
(※27) NISC：National center of Incident readiness and Strategy for Cybersecurity 内閣サイバーセキュリティセンター https://www.nisc.go.jp/
(※28) FISC：The Center for Financial Industry Information Systems 金融情報システムセンター https://www.fisc.or.jp/
(※29) 金融 ISAC http://www.f-isac.jp/
(※30) CRIC: Copyright Research and Information Center 著作権情報センター http://www.cric.or.jp/about/index.html
(※31) CSSC: Control System Security Center 技術研究組合制御システムセキュリティセンター http://www.css-center.or.jp/

おわりに

セキュリティ業務を担う人材のスキル可視化施策の検討と本書の発行にあたり、これまで相当な時間を提供していただいた JTAG メンバーはもちろん、たくさんの方にご協力いただきました。この場を借りまして厚く御礼申し上げます。特に、2次トライアルに参加いただいた 300 名近い方々と、各企業にてそれを取り纏めていた方々には多大な尽力をいただき感謝いたします。トライアル結果についてはスキル可視化や認定の仕組み策定に対して想定以上に重要な位置づけとなりました。また、ブラッシュアップする過程で、セキュリティ以外にも応用できる仕組みとなる可能性も確認できました。よって、詳細解説をすることで JTAG 活動以外にも役に立つのではないかと判断し、単独のレポートとして纏めることにしました。11 月中旬に公開できるよう現在準備中です。

「セキュリティ業務を担う人材のスキル可視化施策　概念実証報告（仮称）」

昨年度公開した「セキュリティ業務を担う人材のスキル可視化ガイドライン　＜β 版＞」までの期間も含めて約 2 年にわたり議論、検証、策定作業を重ねてきました。中心になって検討してきたメンバーが20代から60代までの幅広い年齢層、これまで経験してきた業種や業務、いわゆる人生経験という点も比較的バラバラで、多様な価値観の集まりであることから広い視点から検討を進めることができました。時には、セキュリティという枠を超えた「人生100年」という観点からもかなり議論が交わされてきました。若い方々にはこれから先のキャリアグランドデザインのために、シニアもしくはこれからシニアとなっていく方々にも長い仕事人生の再設計に役立たせてもらうことを意識して、スキル可視化やそれを活用した施策の検討を重ねてきました。

今回のレポートでは可視化の精度向上ブラッシュアップだけでなく、利用展開アイデア、利用ターゲット、利用シーン、さらに快適に利用してもらうための方策、マーケットへの展開施策まで検討した結果についてまとめています。つまり、JTAG はスキル可視化ツールのような複雑で小難しいものを作って公開して終わる活動ではなく、それを使った仕組み自体をつくり広く企業や組織に利用してもらい普及することによって人材の流動化を実現することが目的です。

まだ道のりは長いですが、早期に実現できるように活動は継続していきますので、多くの企業様に JTAG の活動への賛同、参加いただければ幸いです。

なお、JTAG 並びにワーキンググループ活動につきまして、ご質問がありましたらお問い合わせ先までご連絡をお願いいたします。

＜お問合せ先＞

JTAG 事務局（JNSA 内）jtag-sec@jnsa.org

執筆者

大槻 晃助　（株式会社ラック） 認定ワーキンググループリーダー
新井 是昭　（ヤマト運輸株式会社）
伊井 あすみ（株式会社ラック）
板倉 恭子　（ネットワンシステムズ株式会社）
伊藤 良孝　（株式会社インターネットイニシアティブ）
大隈 啓史　（パーソルプロセス&テクノロジー株式会社）
尾方 佑三子（株式会社ラック）
柏谷 知美　（ネットワンシステムズ株式会社）
川口 倫弘　（大同生命保険株式会社）
砂田 浩行　（株式会社日本総合研究所）
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
平山 敏弘　（株式会社アイ・ラーニング）　JNSA 教育部会長
三浦 順子　（トレノケート株式会社）
三舩 果菜子（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）
持田 啓司　（株式会社ラック）　　ISEPA 代表
米澤 一樹　（パーソルプロセス&テクノロジー株式会社）
渡邉 真裕子（トレノケート株式会社）
※認定 WG リーダー以外は五十音順

＜ISEPA 情報会員＞
五島 浩徳 （ISACA 東京支部 2015-2017 年度会長、ITGI Japan 理事）

オブザーバー
舘岡 均 （特定非営利活動法人 日本システム監査人協会）

協力
株式会社ネクストエデュケーションシンク