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＞

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 年 1 月 18 日

目次

本ガイドライン策定の目的

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。国内の情報セキュリティ事業者やユーザー企業、人材サービス事業者、教育提供事業者が広く協力して、セキュリティ人材ニーズの明確化、情報セキュリティ人材の基盤拡充策について検討を行っている。

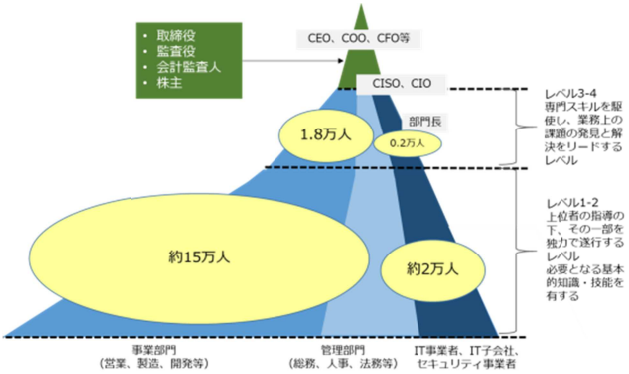
本書は、JTAG構想におけるセキュリティ人材のスキル認定制度構築を念頭にセキュリティ人材の尺度を統一させ、信頼度や真の実力値が判定できる基準について策定したものである。このガイドラインによって、必要とされるセキュリティ業務への適材適所の配置・調達、育成のための効果的な教育プラン立案を可能とすることはもちろん、求められる職務への適正な認定がなされる制度によって、セキュリティ業務に携わる人材の地位向上に寄与することを目的としている。

なお、本書はβ版であるが、すべての根底となる基本的な考え方、人材の定義や指標項目、判断基準、評価の範囲などの具体的表現方法など初版に向けて固まったことからトライアルの実施を目的に公開するものである。

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メインで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）にも焦点をあてる

2．多視点からの判断基準（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、その人材の精度高い総合実力を導けることを念頭におく



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」

図１

図２

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その利用価値までを念頭において指標を整理する
・ユーザー企業の IT 利活用部門に焦点をあてたセキュリティ視点の業務ロールの定義（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、持続した安定運営ができることを念頭におく

次ページ以降に、それぞれについて解説をしていく。

1. 本ガイドライン策定のポイント

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

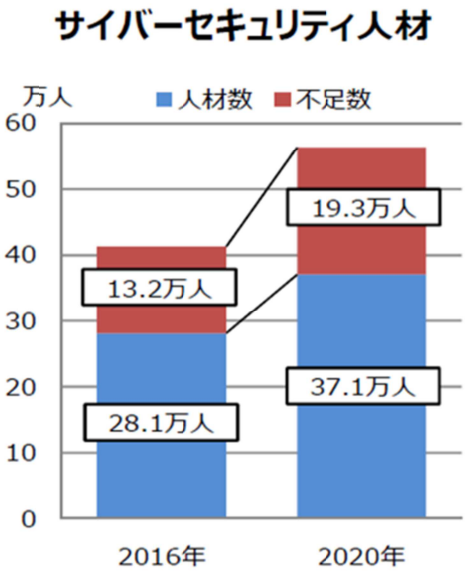


図３　サイバーセキュリティ人材数推移
出典：経済産業省
「今後の情報政策・商務サービス政策の重点について」

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 年に向けてその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ける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の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、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

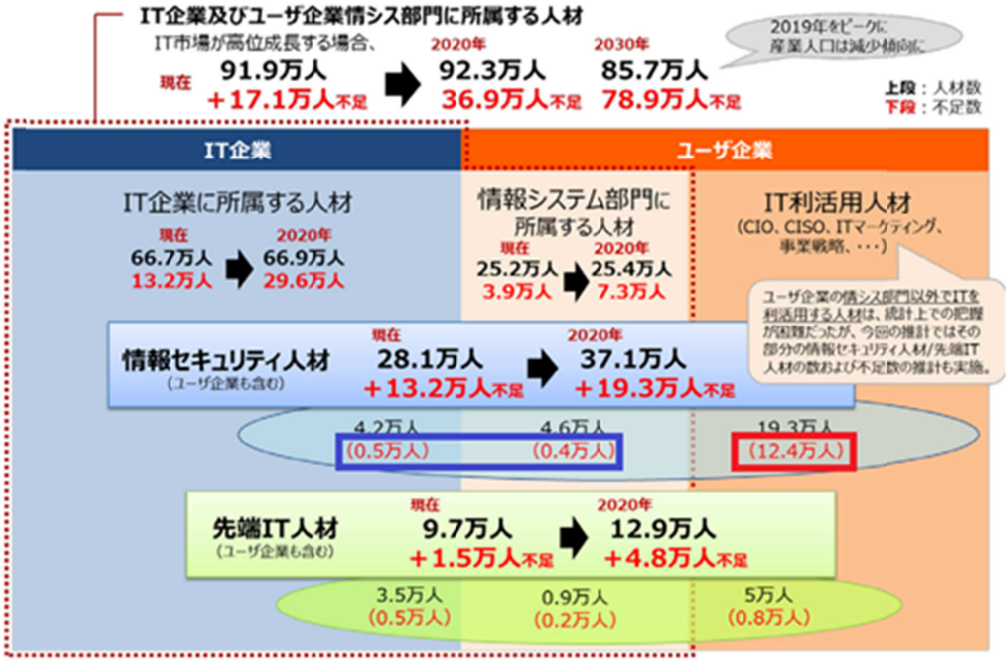


図４　「IT 人材不足が深刻化 2030 年には 78.9 万人不足に」

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

用する中で、セキュリティ確保もできる人材が 2016 年調査時点において 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のスキル不足への対応は依然必要であるが、不足人数の点では大きな問題とはなっていない。

1.1.2　人数面で大幅に不足している IT 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)

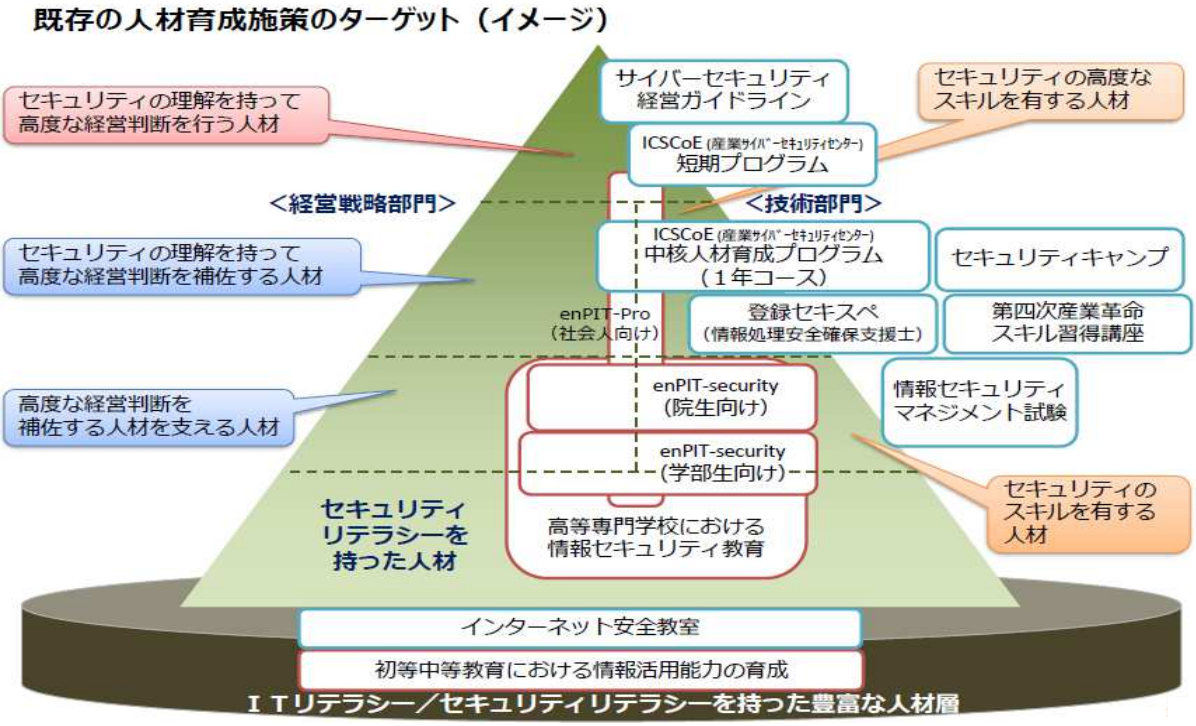


図５　経済産業省「現存のセキュリティ人材育成施策とターゲットイメージ」

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 で表しているように、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が、今まで施策や資格などもなく未対応であったことが現状である、人数的に多くの不足が叫ばれているプラス・セキュリティ人材の数値化（見える化）を実現することは不可能であった。

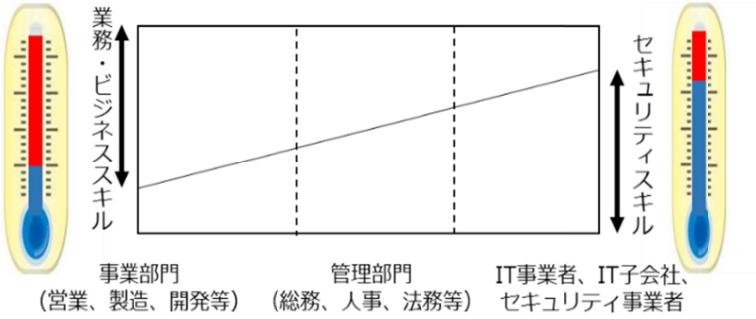


図 6 所属企業･部門におけるセキュリティスキルと業務ビジネススキルとの関係イメージ
出典：JCIC レポート「セキュリティ人材不足の真実と今なすべき対策とは」

1.1.3 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

JTAG では、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情報処理安全確保支援士や CISSP 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の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ことなどが可能となっている。

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。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※1
情報セキュリティ知識項目	Secbok※2
IT／コーポレートガバナンス	COBIT※3
スキルレベル	ITSS※4
資格レベル	ISV Map※5
能力成熟度モデル	CMMI※6

1：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)
2：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）
3：Control objectives for Information and related Technology v1.3 / ISACA および ITGI
4：IT スキル標準(IT Skill Standard) / IPA(独立行政法人情報処理推進機構)
5：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）
6：Capability Maturity Model Integration / カーネギーメロン大学 および ISACA

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。

1.2. スキル評価基準全体の考え方

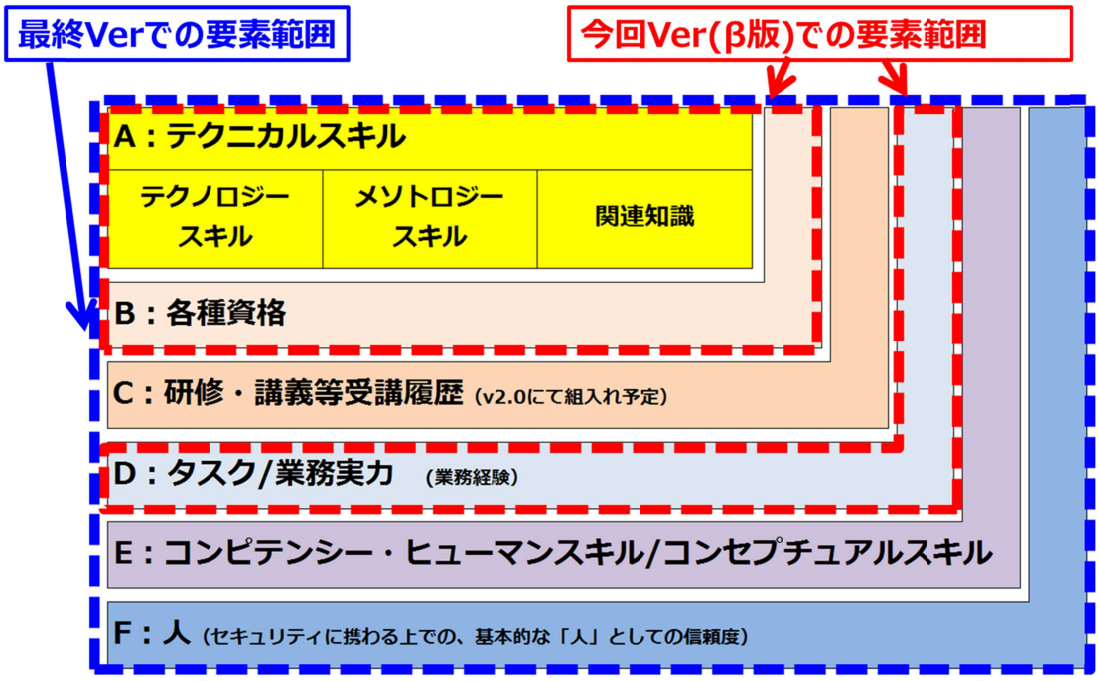


図７　評価基準の概念図

1.2.1　評価基準項目策定の考え方について

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などのコンピテンシーなど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。社員の評価目的ではないが、認定ガイドラインについても、常にブラッシュアップ、メンテナンスが継続して行えることを念頭に、図７のようにモジュール化をした。

２）また、企業内のタレントマネジメントにおいて、それぞれの企業で必要なモジュールだけを使って自社利用に役立つことも想定している。

３）セキュリティ専門業務以外でも、その業務内である程度想定されるセキュリティに関連するであろう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。また、その経験が深い、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。これらのことは、JTAG キャリアデザイン WG での調査でも明らかになってきている、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積み重ねで CISO 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からも、真の実力値として顕在化できる工夫をした。

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スキル評価基準を策定した。

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８　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

スキルは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、各資格の特徴を鑑み共通な基礎点を定義した。資格のみの取得で業務経験がない場合や、長い業務経験はあるが資格が無い場合なども考慮してスキル基礎点を算出する。
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とこで、セキュリティ分野での点数を加算する仕組みとした。
資格と業務で算出された基礎点は 1.2.1 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。

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、不足する部分については 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。

		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
メソトロジ	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 9　JTAG の評価指標

2.3. B：各種資格

各種資格は、IT セキュリティ関連を中心に選び出してあるが、関連性のある資格は随時追加する予定である。各資格は「A.テクニカルスキル」の中項目にレベルを紐づけしてある。テクニカルスキルだけではなくその資格を取得する前提となる項目に関してもマッピングした。（例えば、「英語のみの受験の資格は英語のスキルがあるとみなす」など。）

2.4. C：研修・講義等受講履歴（v2.0 にて組入れ予定）

業務遂行のためのスキルアップとしていろいろな手段による個人学習はもちろん重要だが、基本から体系的に習得しておくことは効率面、実務に対する効果性という点から非常に重要である。また、実践力を付けるためにも、実務への応用方法や周辺技術、手法などについて専門教育を受けておくことは実力を上げるために役立つ。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、資格取得までには至らなくても専門の教育事業者が提供する学習機会を活かしていることは本人の実力評価に加味するべきものと考える。

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、社会人が 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、v2.0 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第一人者（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た。

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な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までを鑑み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

これまでの内容で、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が、各種業務遂行にはその他にも必要なスキルがある。
ロバート・L・カッツ氏によると、人材に必要なスキルとしてテクニカルスキル／ヒューマンスキル／コンセプチュアルスキルの 3 つが提唱されている。
発表された当時は管理者に必要なスキルとして定義されたが、今日では管理者のみにとどまらず職務ごとにバランスは異なるもののすべての人材に 3 つのスキルが求められる。
ある職務や役割で結果を出せる人材には、テクニカルスキルに加え、ヒューマンスキル（＝他者との良好な協働関係を作ることができるスキル）およびコンセプチュアルスキル（＝物事の大枠をとらえ、創造力を働かせ、明確なビジョンを打ち出せる力）が欠かせない。

よって本認定では、テクニカルスキルに加え、ヒューマンスキルやコンセプチュアルスキルを評価指標に加え、総合的に評価し、個人の不足したスキルを強化することや、チームメンバーに不足したスキルを採用によって補うなど、組織の最適化に貢献していく方針である。

加えて、個人や組織の成長には、「コンピテンシー」についての考慮も必要と考えている。コンピテンシーとは、Evarts(1987)の定義も加味すると、「職務や役割における効果的ないし

は優れた行動に結果的に結びつく個人特性」と考えられている。
このことから、「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だと考える。
その行動特性をもとに、採用条件や人材配置の検討ならびにスキル強化を行うことでコンピテンシーの不一致から特定の業務で成果が出ないといった、個人・企業ともに不幸な結果を防ぐことにつながると考える。

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を実施する。

１）情報処理安全確保支援士資格制度との連動

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者や不正アクセス行為の禁止等の刑に処せられていない者などは、登録できないとされている。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認を実施する。

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）上位レベル者に対するインタビューの実施

また IPA　IT スキル標準レベル 5 以上の認定については、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。

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。

3. 評価のアウトプットについて

3.1. 登録者の人材像、実力値の可視化

この可視化ツールで表現されるのは、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と、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である。将来的に実現される認定制度において JTAG が認定するのは、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。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ことに留意されたい。

1）セキュリティ業務遂行能力総合スコア

２３種類の各指標において、ITSS 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。

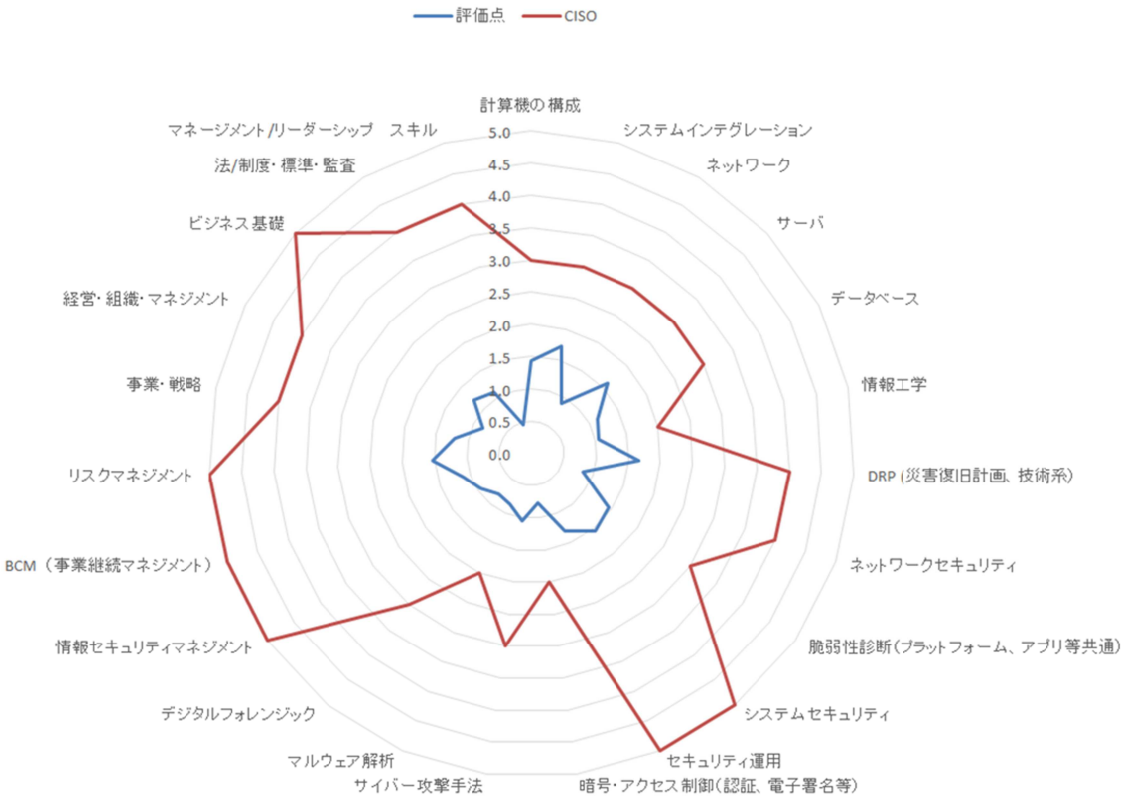


図 10　セキュリティ業務遂行能力のレーダーチャート（サンプル）

2）各業務モデルへの適合度

JTAG が用意する業務モデル（いわゆるお手本）に対して、どの程度適合しているかを算出し、適合度を百分率（パーセント）で表現する。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」を表現できるようにしている。また、適合度を測る対象である業務モデルは、組織に求められる

標準的なセキュリティ業務のスキル項目とその業務に求められるスキルレベルを JTAG が収集・分析するデータを元にプリセットしたものである。業務モデルの種類については、今後キャリアデザイン WG で検討されるものと連動することを想定している。いずれの業務モデルもセキュリティ業務に従事することを念頭において設定されている。

一方で、各業務モデルは業種業態や組織の規模によって求められる内容が異なることも課題として認識しており、固定のものでは適合しない組織も想定されることから、ユーザー側で業務モデルを設定できる機能も備える。

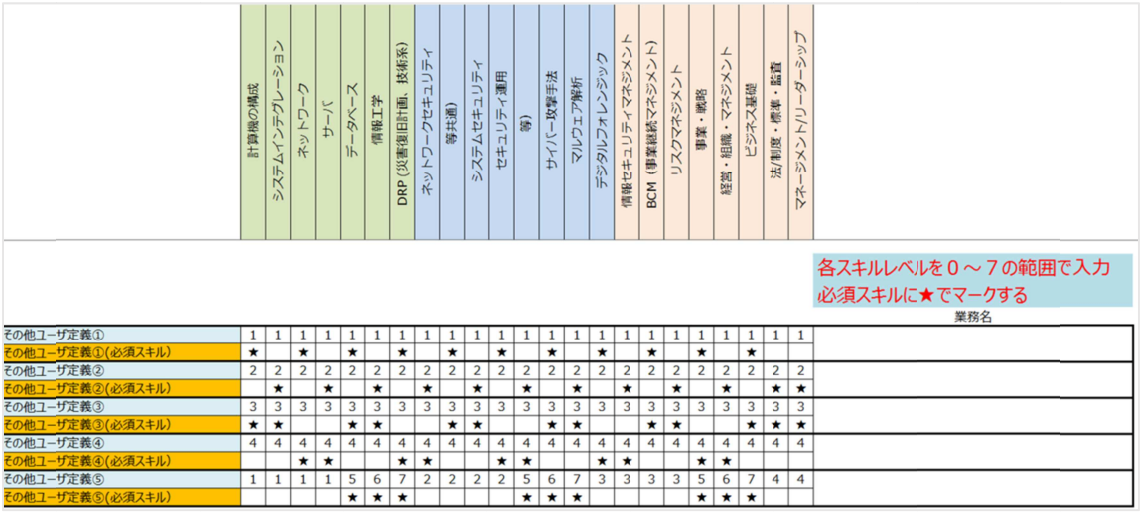


図 11　ユーザーによる業務モデル設定機能イメージ

3.2.　利用イメージ（個人）

この可視化ツールを「個人」として利用する第一の有効性は、フォームへの入力が資格と業務経験という「事実」に基づく自己申告でという点で、主観に依存せず客観的に現時点の業務遂行能力を認識できることである。セキュリティ業務の遂行能力は専門的なものだけを指すのではなく、それぞれの業種における基礎的な能力が必要であるという JTAG の考えに照らし合わせると、セキュリティに限らず一般的な「仕事をこなす実力」ととらえることもできる。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し、自身の理想や目指す役割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に対する判断材料に資するものとなるだろう。また、目指す役割がまだ明確に定まっていなかったり、どの役割を目指すべきかについて模索していたりする段階の場合、業務モデルへの適合度を参考に現在のスキルと親和性の高い業務を探し出し、キャリアパスとして視野に入れることが可能になる。

3.3.　利用イメージ（組織/企業）

組織や企業においてこの可視化ツールを利用するメリットとしては、所属メンバーの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ることができる点にある。得意分野に着目してタレントマネジメントツールとして活用できる他、軸が固定されているため組織内の人材ポートフォリオの構築にも寄与する。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ものになるだろう。

これらの評価方法の流れとして、

1．役割（ロール）ごとに人材像をあらかじめモデル化
2．認定対象者の認定時点におけるコンピテンシーおよび各スキルを測定
3．人材像モデルと認定対象者の測定値の比較
4．比較結果から適性のある職務の提唱やスキルの強化

により、認定時点において適性のある職務、遂行できる職務、スキル強化により目指せる職務が明確になり、適応しやすい職務の推奨、組織における人材育成のプラン指標になるものの策定を予定している。

結果として、セキュリティもできる人材を必要とする企業には、人材の発掘、望ましい社内配置転換のベースとなる個人スキル評価資料の提供を、そして様々なキャリアを模索する個人には、セキュリティ関連業務に対して本人も認識のなかった適性への気づき、および就職機会の拡大が期待できることから、セキュリティもできる、ミスマッチの無い人材の確保に寄与できることを目標としている。

4. 教育研修サービスとの連携について

ISEPA 会員各社の提供している各種教育サービスについて、テクニカルスキル部分への対応が一目でわかることで、登録人材がスキルアップを必要とする領域について効果的、効率よい教育を享受できることを狙いとする。また、各業務モデルについての必要スキルとのマッチングによって、企業のセキュリティ組織の人材配置のための育成プランを立て易くする。

図 12　連携イメージ図

5. 認定の仕組みの運営ついて

本ガイドラインは 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策定しているものである。人材の真の実力値を高い精度で表現するために精緻な情報を元とし、複雑なロジックで組み立てられている。よって、その情報が有効活用されるためには、登録者本人を含め登録情報を利用する組織／団体にとってわかりやすい、具体的なメリットが見え易くする工夫が必要である。また、認定そのものが社会全般に対して信頼度の高い、限りなくフェアーなポジションとして受け入れられることが大前提である。

なお、本ガイドラインの利活用は 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。そのためには、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囚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、利用のし易さや馴染み易さの制度運営が求められる。

6. 今後の活動について

直近の活動としては 4 月末頃までにバージョン 1.0 の完成を目指す。そのためには各指標数値についてさらに精度をあげる必要があるので、セキュリティ含めコアな技術スキル部分については JNSA の各部会の協力、マネジメント系のスキルについては他の業界団体への協力要請も視野に入れていく。また、業務モデルの再整理と理想モデル例を導き出ために、なるべく多くの登録サンプル収集も計画していく。

なお、このプロセスを進めながら実際に制度を円滑に運営する場合のリソース、費用、協力体制などを検討し仮説としての運営イメージを描きだしていき、来年度の具体的アクションのプランニングを進め、当初の構想を実現するために活動を継続していく。

おわりに

本書の発行にあたり、多くの方にご協力いただきました。この場を借りまして御礼申し上げます。

『情報セキュリティ人材』の不足については長年にわたり指摘されてきているところですが、2016 年 6 月の『IT 人材の最新動向と将来推計に関する調査結果』でも、2020 年には 19.3 万人のセキュリティ人材が不足すると発表されています。その後の 2018 年に発表された『IT 人材白書 2018』や『情報セキュリティ白書 2018』でも、情報セキュリティ人材については「人材の不足・確保ができていない」という結果が出ており、不足の解消どころか、さらに不足感が強くなってきている状況です。

注目すべきは、2020 年に不足すると言われている 19.3 万人を単純に逆算してみると、IT 系企業で約 3 万人、ユーザー企業で約 16 万人と圧倒的にユーザー企業でセキュリティ人材が不足すると考えられる点です。これは、情報セキュリティ事業者によるサービス提供拡大に伴う不足だけでなく、IT を利用するユーザー系企業のセキュリティ意識や必要性の高まりも起因していると考えられます。

情報セキュリティに関して言えば、人材投資をすることで収益を上げることはできない反面、人材がいないことにより発生するセキュリティインシデントに対するコストは、事前の投資に比べると圧倒的に高額となってしまいます。

このため、自組織に必要なセキュリティ業務に対して、必要十分なスキルを持った人材の育成と適材配置が重要となってきます。

JTAG の活動では、自組織を守るための人材が不足しているのでは？と仮説を立てることで、実際の現場でどのように必要な人材を育成し、さらには必要業務に配置を行っているかをインタビュー調査し 2018 年 11 月 2 日に公開しました。この調査から見えてきたことは、仮説のとおり、現実問題として人材不足を痛切に感じながらも、なかなか潤沢な人材配置はできていないということでした。

そのため、調査を反映した活動として、自組織を守るための人材に焦点を当てて、本来必要と思われる自組織を守る情報セキュリティ人材のスキルや業務経験を可視化し、事業運営におけるすべての業務に対して適材配置に活用できる、スキル評価ガイドラインを検討し、自己成長や組織内での育成のために使うことができるタレントマネジメントツールを構築し、認定制度の実現を目指して推進しています。

初回バージョン（β版）として、知識面は SecBoK を活用し、あわせて業務経験を診断要素として取り込んだスキル評価ガイドラインを作成しました。多くの方にお使いいただいて、自己成長や組織の適材配置の参考にしていただきたいと考えています。また、今後はスキル評価の精度を高めるためにトライアル診断も募集を計画していますのでぜひお試しください。

なお、今後は過去の研修受講履歴や、業務経験の中から見えてくるヒューマンスキルについても要素として取り入れることで、より業務適性を図れるものにしていく予定です。

本ガイドラインを通じて、自組織を守るセキュリティ人材が具体化され、適切な育成や採用によりセキュリティ人材の増加を図るとともに、適材適所での配置がされることで、多くの組織におけるセキュリティ人材の価値向上に寄与できれば幸いです。

＜お問合せ先＞

JTAG 事務局（JNSA 内）jtag-sec@jnsa.org

執筆者

＜JNSA 正会員＞
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（リコージャパン株式会社）
尾方 佑三子（株式会社ラック）
砂田 浩行（株式会社日本総合研究所）
平山 敏弘（アクセンチュア株式会社）JNSA 教育部会長
三浦 順子（トレノケート株式会社）
持田 啓司（株式会社ラック）ISEPA 代表
渡邉　真裕子（トレノケート株式会社）

※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）