機器のサイバーセキュリティ確保のための
セキュリティ検証の手引き

別冊 3　検証人材の育成に向けた手引き

経済産業省　商務情報政策局

サイバーセキュリティ課

目次

1 背景と目的

1.1 背景：検証サービス事業者における検証人材の重要性

本手引きの本編では、検証サービス事業者のサービス高度化を目的として、機器のセキュリティを検証するセキュリティ検証（以降、省略し「検証」という）において検証サービス事業者が実施すべき事項を示した。これらにより、質の高い検証サービスを行うことができるというビジネスの信頼性、及び適切な情報管理等に基づきサービスを提供するという情報管理の観点での信頼性という二つの信頼性向上が期待される。併せて、適切な検証体制を構築するために、検証依頼者が実施すべき事項や持つべき知識についても示したほか、二者が適切なコミュニケーションを行うための情報を記載した。

手引き本編第 3.2.2 項では、検証サービス事業者の信頼性には、質の高い検証サービスを行うことができるというビジネスの信頼性、及び適切な情報管理等に基づきサービスを提供するという情報管理の観点での信頼性の二つが存在すると述べた。検証サービス事業の多くは機密情報を扱うため、情報管理に係る取り組みはビジネスの基盤として不可欠であり、十分に構築されていない場合、事業継続に影響を及ぼす可能性もある。ビジネスの信頼性は、事業者に属する人材が有する知識やスキル、それらによって確立される経験や実績、及び検証サービス事業者が有する設備や検証環境によって醸成されるものであり、これらは質の高い検証サービスの提供に寄与する。また、検証人材の知識やスキルは、事業を通じて事業者全体のノウハウとして蓄積され、事業者としてのノウハウも質の高いサービス提供に不可欠な要素である。質の高いサービスの提供は、検証依頼者からの信頼性向上だけでなく事業の収益にも寄与し、得られた収益は人材のスキル育成や高価な検証設備の購入に充てることができる。以上の要素は、一般的に 4 つの経営資源と呼ばれる「ヒト・モノ・カネ・情報」と同等であり、これらの 4 要素は検証サービス事業者の信頼性向上と質の高いサービス提供のために図 1-1 のように相互に作用するものである。

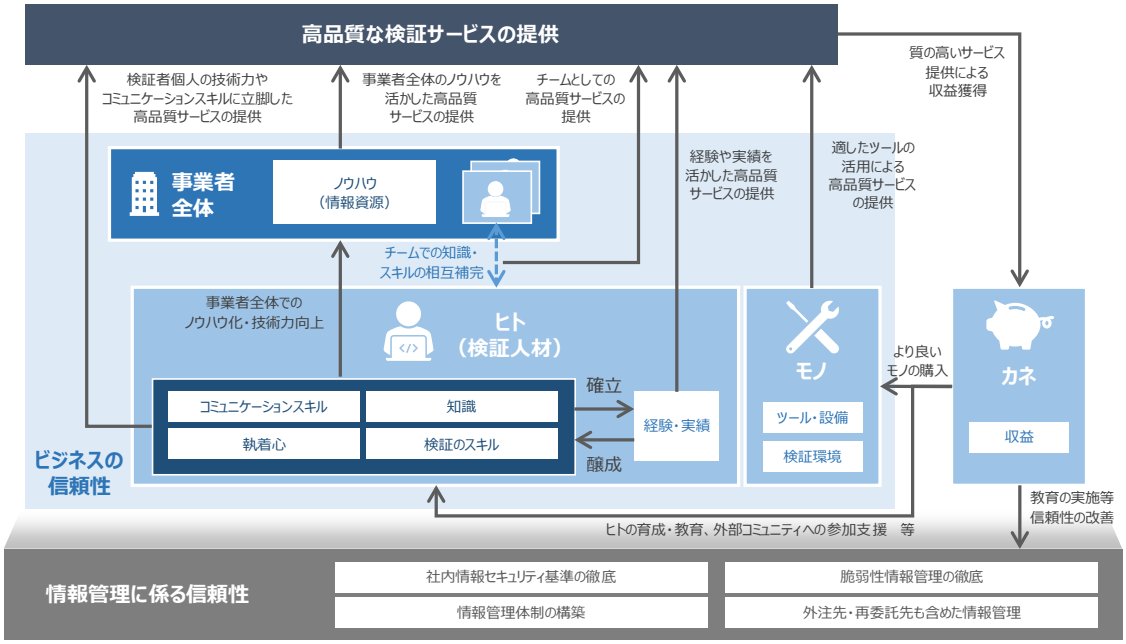

図　1-1　検証サービス事業者における「ヒト・モノ・カネ・情報」の位置付け

一般の企業経営と大きく異なる部分として、検証サービス事業においては４つの経営資源のうち「ヒト」、すなわち検証人材の要素が極めて大きな役割をなす点が挙げられる。検証人材のスキルや知識は経験や実績と大きく関係し、これらの要素は事業者の信頼性向上に直接的に寄与するものである。また、検証人材のスキルや知識がノウハウとして事業者に蓄積されることで、事業者全体として再現性のある高品質な検証サービスを提供できることとなる。

1.2　本別冊の目的

本別冊では、高品質な検証サービスの提供及びビジネスの信頼性向上に大きく寄与する「検証人材」にフォーカスを当て、検証人材に求められるスキル・知識や、検証人材のキャリアの可能性を示す。検証人材のキャリアは一意に定まるものではなく、常に先進的な検証を実施する人材、ツールを活用して標準的な検証を実施する人材、マネジメントの立場から検証を支援する人材等、様々なキャリアが存在する。本別冊では、様々なキャリアに求められるスキル・知識を確認するために、技術的なスキル・知識だけでなくコミュニケーションスキル等の非技術的なスキル・知識も記載している。また、様々なキャリアの可能性を理解するために、検証人材におけるキャリアの考え方や、キャリアを設計する上で必要な観点を示している。加えて、検証サービス事業者内の検証人材を育成するために求められる取り組みについても記載している。

1.3　本別冊の対象者・活用方法

本別冊の内容は、検証サービス事業者に属する検証人材だけではなく、検証人材をマネジメントする立場の人材においても、自社が求める人材像を確認することに役立つ。また、検証人材を志す学生・社

会人においても、必要なスキル・知識やキャリアを理解し、自己研鑽を行うこともできる。

併せて、メーカの開発者、検証担当者、セキュリティ担当者等の検証依頼者の立場においても、自社の人材レベル向上のために活用することが期待される。

1.4 本別冊の構成

第 1 章においては、本手引き別冊の背景として、検証サービス事業者における検証人材の位置付けを示した。また、本別冊の目的、対象者及び活用方法を示した。

第 2 章においては、検証人材に求められるスキル・知識を、多くの検証手法に共通して求められる基礎的なスキル・知識、各検証手法に求められるスキル・知識、そして効率的な検証を行うために必要な非技術的スキル・知識に分類し、その具体例を示す。併せて、スキル・知識を獲得するために望まれる取り組みについて記載する。

第 3 章においては、検証人材のキャリアを構想・設計する上で考慮すべき観点を示す。そのために、検証人材を 3 軸に基づき整理し、検証人材のキャリアの可能性を整理する。

第 4 章においては、検証サービス事業者において検証人材を育成するにあたって実施が望まれる取り組みを示す。

第 5 章においては、付録として本別冊で使用する用語の定義と参考とした文書を示す。

2 検証人材に求められるスキル・知識

当然ながら、検証人材には検証に係る技術的なスキル・知識が求められる。これには、個々の検証手法に関する知識だけでなく、コンピュータ、ソフトウェア、ネットワーク、ハードウェア、OS、セキュリティ、暗号・認証に関する基礎知識も含まれる。また、効果的かつ効率的な検証実施のために、最新の脆弱性や脅威の動向を把握しておくことが望まれるほか、検証対象機器や関連サービスに関しても把握しておくことが望まれる。併せて、検証依頼者との適切な検証体制を構築し、検証結果を適切に伝えるために、非技術的なスキルや知識も持ち合わせていることが望ましい。求められるスキルや知識の例として、コミュニケーション、論理思考力、文書化に関するスキルや知識が挙げられる。検証は、複数の人材がチームを組んで実施することが多く、チームとして協調して検証を進めることが必要となるため、社内関係者との円滑なやり取りにおいてコミュニケーションは特に重要な要素となる。上記以外にも、チームを率いるプロジェクトマネージャーの立場の人材においては、一般的なプロジェクトマネジメントに関するスキル・知識が求められる。

加えて、検証人材は検証の倫理性を常に意識する必要がある。仮に検証技術を悪用した場合、機器の破壊だけではなく、他システム、組織、情報等に対して悪影響や損害・損失を及ぼす可能性がある。検証人材は、検証技術がサイバー攻撃と表裏一体であることを理解し、正義感と高い倫理観を持ち合わせた上で、セキュリティ向上を目的として検証技術を活用することを常に心がけなければならない。また、検証による法令違反を防ぐためには検証に関連する法令を理解し遵守する必要がある。

多くの検証手法に共通して求められる基礎的なスキル・知識、各検証手法（本編における表 2-1 参照）に求められるスキル・知識、そして効率的な検証を行うために必要な非技術的スキル・知識の具体例を表 2-1 に示す。

表 2-1 検証人材に求められるスキル・知識

項目	具体例
技術的なスキル・知識 - 基礎スキル・知識	
コンピュータの基礎	• 計算機のアルゴリズムに関する知識 • コンピュータの構成に関する知識（基本的なコンピュータのコンポーネント、ネットワークの種類 等）
ソフトウェアの基礎	• プログラミングスキル（C、C++、Python、Java 等） • ソフトウェア設計ツール、手法に関する知識 • プログラミング言語の構造やロジックに関する知識 • ソフトウェアデバッグに関する知識 • ネットワークアプリケーションの仕組みに関する知識
ネットワークの基礎	• 通信プロトコルに関する知識（TCP/IP、OSI 参照モデル 等） • ネットワークインフラやデバイス構成に関する知識 • ネットワークセキュリティに関する知識（暗号化、ファイアウォール、境界防御 等）

項目	具体例
ハードウェアの基礎	• CPU アーキテクチャに関する知識（ARM、MIPS、x86 等） • コンピュータアーキテクチャ（回路基板、プロセッサ 等）に適用される電気工学に関する知識
OS の基礎	• Windows, Linux のポートやサービスに関する知識 • Windows, Linux のシステム管理に関する知識（プロセス管理、ディレクトリ構造、アクセス管理 等） • Windows, Linux 上のセキュリティ対策に関する知識 • 代表的な OS コマンドラインに関する知識（cat, cp, mv, ls 等）
セキュリティの基礎	• 基本的なサイバーセキュリティの概念、原則、制限及び効果に関する知識 • 情報セキュリティ 3 要素/6 要素/7 要素に関する知識 • 組織におけるセキュリティ対策フェーズに関する知識 • プライバシーに関する知識
暗号・認証の基礎	• 暗号化アルゴリズムに関する知識 • 暗号鍵管理に関する知識 • 認証及びアクセス制御の手法に関する知識 • 機器やアプリケーションアクセス時の認証手法に関する知識
技術的なスキル・知識 – 各検証手法に関するスキル・知識	
設計文書レビュー	• 設計文書に基づき、機器が実現すべき機能を整理するスキル • フローチャートやシーケンス図に基づき処理を理解するスキル • 設計文書に基づき機能要件・非機能要件の問題を特定するスキル • 設計文書に基づきセキュリティ対策上の問題を特定するスキル（エラー処理、入出力処理 等）
ソースコード解析	• ソースコードを解読し、重要プログラムを特定するスキル • コード解析ツールを利用するためのスキル・知識 • セキュアコーディング技術に関する知識 • 代表的な非推奨関数の知識 • ソフトウェア構成のセキュリティ影響に関する知識 • 論理に基づきソフトウェア構造を確認するスキル（形式手法 等）
ファームウェア解析	• 情報取り出しのためのメモリダンプ分析に関するスキル • 機器のデバッグインタフェースに関する知識（UART, JTAG 等） • フラッシュメモリからファームウェア抽出を行うスキル • 基盤からモジュールやメモリ等の製品情報を調査するスキル

項目	具体例
バイナリ解析	• CPU 命令や OS のメモリ管理に関する知識 • リバースエンジニアリングツールを活用するスキル • バイナリ解析ツールを活用するスキル • ビットマップ表示からファームウェアの構成を想定するスキル • 逆アセンブル結果や逆コンパイル結果を解読し、重要プログラムを特定するスキル • 逆アセンブル結果や逆コンパイル結果から脆弱性を検出するスキル
ネットワークスキャン	• ネットワークスキャンツールを使用し、脆弱性を特定するスキル • ネットワーク管理コマンドに関する知識（ping, traceroute, nslookup 等） • 代表的なポートやサービスに関する知識 • 攻撃への悪用事例があるポートやサービスに関する知識 • 検証対象機器・関連サービスの機能や仕様を踏まえ、不要サービスやポートを特定するスキル
既知脆弱性の診断	• 脆弱性スキャンを実行し、機器や関連サービスの脆弱性を認識するスキル • 脆弱性スキャンツールの結果に基づき、影響や根本原因を分析するスキル • 脆弱性に基づきエクスプロイトを行うスキル • 通信上の脆弱性を識別するためのネットワーク脆弱性解析ツールに関するスキル
ファジング	• オーバーフローにつながりうるテストデータに関する知識 • 検証対象機器・関連サービスの異常動作に関する知識 • 検証対象機器・関連サービスの特性を踏まえてテストデータを作成するスキル • 異常動作やログに基づき、根本原因を探索するスキル
ネットワークキャプチャ	• ネットワークトラフィックの収集・フィルタリングに関するツールやコマンドを活用するスキル • 収集したパケットを分析し、怪しい兆候を検出するスキル • 代表的なプロトコルのパケット構造に関する知識
ハードウェア解析	• 回路解析に関する知識 • 回路解析に関する設備を活用するスキル（デジタルオシロスコープ 等） • デバイスや基盤を破壊せずに抽出するスキル • 揮発性データの解析に関するスキル
技術的なスキル・知識 - その他の関連スキル・知識	

項目	具体例
検証対象機器	• 検証対象機器・関連サービスのプロトコルやサービスに関する知識 • 検証対象機器・関連サービスが扱うデータに関する知識 • 検証対象機器に接続されうるシステムやサービスに関する知識 • 機器・関連サービスに関して報告されている既知脆弱性に関する知識 • 検証対象機器・関連サービスに対して想定される脅威に関する知識
セキュリティ機能	• 代表的な脆弱性に対する対策に関する知識 • 機器やアプリケーションのハードニング技術に関する知識 • ホワイトリスト・ブラックリストに関する知識
セキュリティ脅威・脆弱性	• 機器やアプリケーションの脅威や脆弱性に関する知識 • 最新の脅威動向や重大な脆弱性を把握・調査するスキル
サイバー攻撃手法	• ハッキング手法に関する知識 • サイバー攻撃の戦略・戦術・手順に関する知識 • ネットワークに対する一般的な攻撃手法に関する知識 • 代表的な攻撃や技術に関する知識（DDoS 攻撃、なりすまし 等） • 一般的なマルウェアやマルウェア感染経路に関する知識
脅威分析・リスク評価	• 代表的な脅威抽出・脅威分析・脅威評価手法に関する知識（DFD, STRIDE, DREAD, Attack Tree 等） • 代表的な脆弱性評価基準に関する知識（CVSS 等） • 検出された脆弱性の影響を分析し、検証結果の総合評価を行うスキル • 検証対象機器・関連サービスに対する攻撃者の目標を理解するスキル
検証プロセスの設計	• 検証目的を達成するための検証プロセスを策定するスキル • 検証目的を踏まえて検証項目を選定・考案するスキル • 検証目的を踏まえて検証項目の優先順位を付けるスキル • 既存の検証手法をカスタマイズするスキル
セキュリティ標準・ガイドライン	• ISO/IEC 27000 シリーズ（ISMS）、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）、NIST Cybersecurity Framework 等、代表的なセキュリティ標準・ガイドラインの内容に関する知識 • 代表的な脆弱性評価基準に関する知識（CVSS 等） • IoT セキュリティガイドライン、IoT 開発におけるセキュリティ設計の手引き、NISTIR 8259 等、代表的な IoT セキュリティ標準・ガイドラインの内容に関する知識
非技術的なスキル・知識	

項目	具体例
コミュニケーション	• 難しい内容を相手の理解度に合わせて説明するスキル • 自身の要求を相手に適切に伝えるスキル • 社内関係者と協調して検証を行うスキル • 検証依頼者の要求を抽出し理解するスキル • 検証依頼者の要求を具体化しサービスとして提案するスキル
論理思考力	• 検証の目的と効果を理解するスキル • 複数の視点から物事を捉えるスキル（攻撃者の視点、機器利用者の視点 等） • 帰納的・演繹的・弁証的に物事を思考するスキル
文書化	• 事実に基づき正確な検証レポートを執筆するスキル • 文書品質を担保するスキル（誤字脱字、体裁、表記統一 等） • 難しい内容を読み手に合わせて文書化するスキル
マネジメント	• 検証プロジェクトの進捗を管理するスキル（WBS の作成、スケジュール管理等） • 検証プロジェクトの予算、課題、品質を管理するスキル • プロジェクトメンバーへの支援・教育を行うスキル
語学	• セキュリティに関する動向を把握するための語学スキル（主に英語）
法令・倫理	• 関連する法令に関する知識 • 社内のコンプライアンスやセキュリティポリシー等の規定に関する知識 • 倫理的なハッキングに関する意識・知識・正義感

※ 一部のスキル・知識の具体例は日本ネットワークセキュリティ協会（JNSA）のセキュリティ知識分野（SecBoK）2019[1]に基づき作成。スキル・知識については、米国 NIST の NICE（National Initiative for Cybersecurity Education）フレームワーク[2]も参考となる。

各検証人材においては、この表に基づき、不足しているスキル・知識や得意な検証手法を把握することが期待される。それぞれのスキル・知識の関係性を整理すると図 2-1 のようなイメージとなる。根底には法令・倫理に関する知識が存在し、その上に技術的な基礎スキル・知識、関連する技術的スキル・知識及び非技術的スキル・知識が並行して位置付けられる。技術的な基礎スキル・知識は検証手法に関するスキル・知識のベースとなるため、多くの検証人材が幅広くスキル・知識を持ち合わせていることが望まれる。関連する技術的スキル・知識や非技術的なスキル・知識についても幅広く持ち合わせていることが望まれるが、必ずしも網羅的に必要なわけではない。一部のスキル・知識であっても、その上に成り立つ検証手法に関するスキル・知識を支えることができる。

[1] JNSA, セキュリティ知識分野（SecBoK）2019 https://www.jnsa.org/result/2018/skillmap/

[2] NIST, NICE Framework Resource Center https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

これらのスキル・知識の上に、各検証手法に関するスキル・知識が成り立つ。それぞれの検証手法に係るスキル・知識の獲得にあたっては、スキル・知識の幅とレベルの双方を意識することが望ましい。幅広いスキル・知識を有していることは対応できる検証の幅が広いことを意味し、高いレベルのスキル・知識を有していることは深さを重視した検証を行えることを意味するが、前述のとおり、検証はチームで実施することが多いため、一人がすべての検証手法について卓越したスキル・知識を持ち合わせている必要はない。チームで検証を実施する場合には、メンバーの持ち合わせたスキル・知識が相互に補完されることで、効率的に検証を行うことができる。スキル・知識のレベルを突き詰めていくか、広範な検証に対応できるよう幅広いスキル・知識を獲得するかは、個々人の得意分野や趣味嗜好にも依存するため一概に方針を示すことは避けるが、目指すべき検証人材像を踏まえ、求められるスキル・知識を自身で検討・抽出することが必要である。

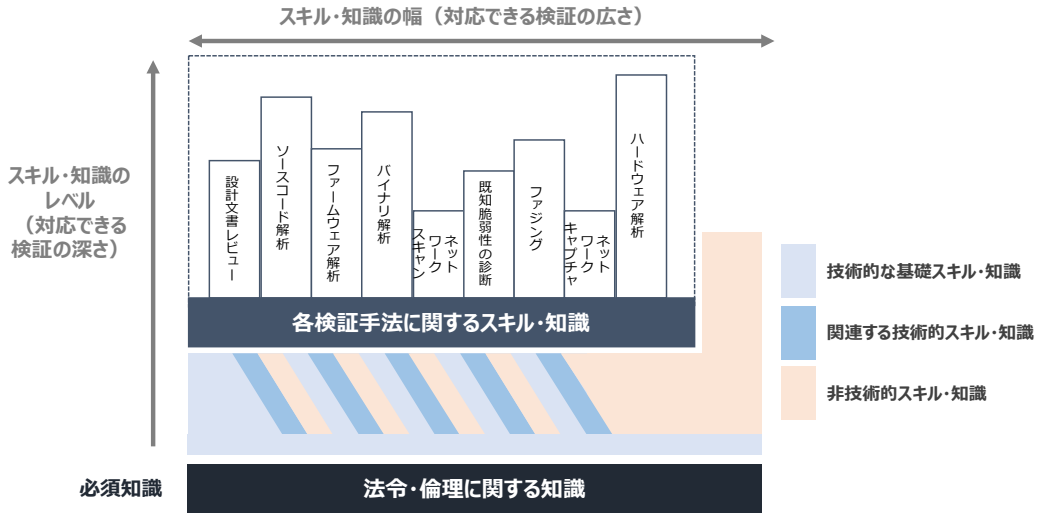

図 2-1 検証人材に求められるスキル・知識の幅とレベルのイメージ

図 2-1 で示しているとおり、各検証手法に関するスキル・知識のレベルはそれぞれの検証手法によって異なる。これは、それぞれの検証手法を実施する際に要するスキル・知識だけでなく、検証結果の分析に要するスキル・知識のレベルも異なる点に留意が必要である。例えば、ネットワークキャプチャは多くの場合に自動化ツールを用いて実行することができるため、通信パケットの取得自体のレベルは高くない。他方で、不審なパケットが無いか等は人の目で分析・確認する必要があるため、収集したパケットを分析し、不審な兆候を検出するスキルが必要となる。参考として、表 2-1 で示した各検証手法に求められるスキル・知識について、そのスキル・知識のレベルと検証に要するコストのレベルを三段階で整理したものを表 2-2 に示す。それぞれのスキル・知識やコストは、利用する検証環境や対象機器によっても変わるため、表 2-2 はあくまでイメージの位置付けであるが、求められるスキル・知識のレベルや要するコストは、獲得すべきスキル・知識を検討する際の一つの判断基準となりうる。

表 2-2 各検証手法におけるスキル・知識及びコストのレベルイメージ

検証手法		スキル・知識のレベル		検証に要するコストのレベル	
		検証に要するスキル・知識	検証結果の分析に要するスキル・知識	検証ツールの金銭的コスト	検証と結果分析に要する時間的コスト
静的手法	設計文書レビュー	★★☆	★★☆	★★☆	★★★
	ソースコード解析	★★★	★★☆	★★★	★★★
	ファームウェア解析	★★☆	★★☆	★★☆	★★☆
	バイナリ解析	★★★	★★★	★★☆	★★★
動的手法	ネットワークスキャン	★☆☆	★☆☆	★☆☆	★☆☆
	既知脆弱性の診断	★☆☆	★★☆	★★☆	★★☆
	ファジング	★☆☆	★★☆	★☆☆	★★☆
	ネットワークキャプチャ	★☆☆	★★☆	★☆☆	★★☆
	ハードウェア解析	★★★	★★★	★★★	★★★

スキル・知識の獲得のためには、実際の事業を経験するだけはなく、自己研鑽が不可欠である。特に、検証人材を志す初級的な人材であれば、本手引きの別冊 1 や書籍、インターネットを用いて検証手法に関する知識を獲得するほか、脅威情報や脆弱性に関する情報を日頃から収集することが望まれる。直接的に検証手法に関する知識ではないものの、機器やソフトウェアの開発に係る自己研鑽も効果的である。併せて、学んだ知識を実際の IoT 機器等に適用することでスキルとして蓄積されることとなるため、関連法令を遵守しつつ、実際の機器等に対して技術を適用する機会を設けることが望まれる。高いレベルのスキル・知識を獲得するためには、幅広い分野の機器に関する経験を積み、様々な検証を経験することが望まれる。また、既存の検証ツールをカスタマイズすることや独自の検証ツールを開発することは、検証手法の本質的理解につながるだけではなく、自身のスキル・知識を一部形式知化することにつながる。

自身のスキル・知識を確認する機会として、CTF（Capture the Flag）等のセキュリティコンテストに出場することが考えられるほか、CEH（Certified Ethical Hacker）、GIAC（Global Information Assurance Certification）、OSCP（Offensive Security Certified Professional）等の試験を受講することが挙げられる。直接的に検証に関する知識を測る資格ではないものの、技術的な基礎スキル・知識について総合的に評価するにあたっては、IPA が実施する情報処理技術者試験の受講も一つの機会として挙げられる。

3 検証人材のキャリアの考え方

検証サービス事業者に所属する検証人材においては、スキル・知識の獲得や検証の経験を蓄積することによって、検証業務で担う役割を拡大することが望まれる。図 1-1 のとおり、検証人材のスキル・知識の獲得と、経験の蓄積は相互に作用するものである。これらを検証人材としてのキャリアの中で養うことで、役割の拡大、ひいては質の高い検証サービスの提供に寄与するものとなる。本節では、検証人材がその役割を拡大させるために、自らの手で主体的にキャリアを構想・設計し、実現していくための考え方を示す。

キャリアを構想・設計をする上では、現在のスキル・知識やライフスタイルなどを考慮した上で、検証事業を通じて実現したい将来像やそれに近づくためのプロセスを明確にすることが重要である。当然ながら、キャリアは一意に決まるものではない。そのため、本別冊では、検証人材におけるキャリアの可能性を示し、キャリアを構想・設計する上で考慮すべき観点を示す。まず、事業者における検証人材を以下の 3 つの軸に基づき、図 3-1 のように整理する。

- **検証の「深さ」の重視度合い** [3]
- **検証の「広さ」の重視度合い** [4]
- **実務として検証を実施するか、マネジメントの立場から検証を主導するか**

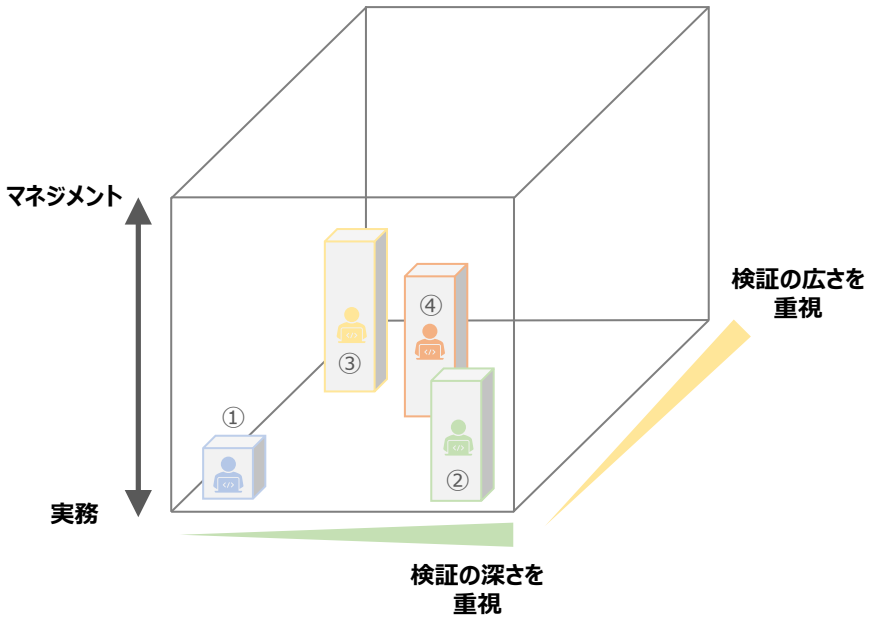

図 3-1 3 軸による検証人材のマッピングイメージ

[3] 本手引きでは、「特定の検証技術に関する高いレベルのスキル・知識に基づき、検証対象機器に対して詳細な検証を実施すること」を「深さ」を重視した検証とする。

[4] 本手引きでは、「広範な検証技術に関するスキル・知識に基づき、検証対象機器に対して網羅性を意識した検証を実施すること」を「広さ」を重視した検証とする。

検証サービス事業者におけるスキル・知識が限定的な新入社員は、図 3-1 内①の人材としてマッピングされる。②の人材は、深さを重視した検証を実施できる人材である。このような人材は、高いスキル・知識に裏付けされた技術力により、ゼロデイ脆弱性など高度な脆弱性の検出を行うことができる。③の人材は、広さを重視した検証を実施・マネジメントできる人材である。このような人材は、様々な機器の検証プロジェクトを主導することができる。最後に、④の人材は、深さを重視した検証と広さの重視した検証の両方に対応できる人材である。このような人材は、検証依頼者との相談の中で依頼者のニーズを引き出し、どのような検証を実施する必要があるかを検討することができる。

検証人材と聞いたとき、深さを探求する人材をイメージされることが多い。挑戦的な検証を行い、高度な脆弱性を検出できる人材は業界でも重宝される。一方で、セキュリティ技術が自動化しつつあり、ある程度自動化ツールで脆弱性の検出が可能となった昨今では、標準化されたプロセスを用いて網羅的な検証を行う人材の需要も存在する。また、チームとして検証を行うために、実際に手を動かす実務者だけではなく、それを総括するマネージャーも必要となる。

キャリアアップするにつれマネジメント能力は必要とされるが、すべての検証人材がマネージャーを目指す必要があるわけではない。また、どの領域にマッピングされる検証人材が望ましいというわけではなく、いずれの人材もセキュリティ検証業界に必要な人材であることに留意する必要がある。そのため、検証人材のキャリアの可能性は、図 3-2 に示すとおり多数存在する。検証サービス事業者における新入社員を考えたとき、①のキャリアに描かれるように検証プロジェクトの経験を通じて検証手法に関するスキル・知識のレベルや幅を向上させつつ、マネジメントスキルも向上させるキャリアが想定される。②の人材のように、対応できる検証の深さや広さを伸ばさず、マネジメントに注力するようなキャリアも想定される。例えば、持ち合わせた高いレベルのスキル・知識を形式知化することで、標準化された検証サービスを展開する事業者のマネージャー（経営者）として事業を牽引するキャリアが考えられる。③の人材のように、幅広い検証に対応できる強みを伸ばしつつ、更にマネジメントスキルを高めてマネージャーの立場から事業を推進するキャリアも考えられる。他にも、④の人材のように、マネジメントスキルは伸ばさず、検証手法のスキル・知識を更に向上させることで、第一線で挑戦的な検証を実施するキャリアも考えられる。

図 3-1 及び図 3-2 は、検証の領域に限定した人材のマッピングを行っている。しかしながら、検証領域外の業務に関する知見・経験も検証人材としてのキャリアに大きく寄与することに留意が必要である。例えば、組込み機器の開発経験を有していれば、ファームウェア解析やリバースエンジニアリングを効果的に行うことができるほか、モバイルアプリの開発経験を有していれば、アプリをデコンパイルした際のコードを効率的に解析することができる。このような開発の経験のほか、マルウェア解析、インシデントレスポンス対応、ツール開発、調査研究等の業務に関する経験は、効果的な検証実施に大きく寄与する。検証以外の業務を担うことで、結果的に検証人材としてのキャリア向上につながるほか、検証人材に留まらない総合的なセキュリティエンジニアとしてのキャリアも存在することを踏まえ、自身のキャリアを設計することが望まれる。

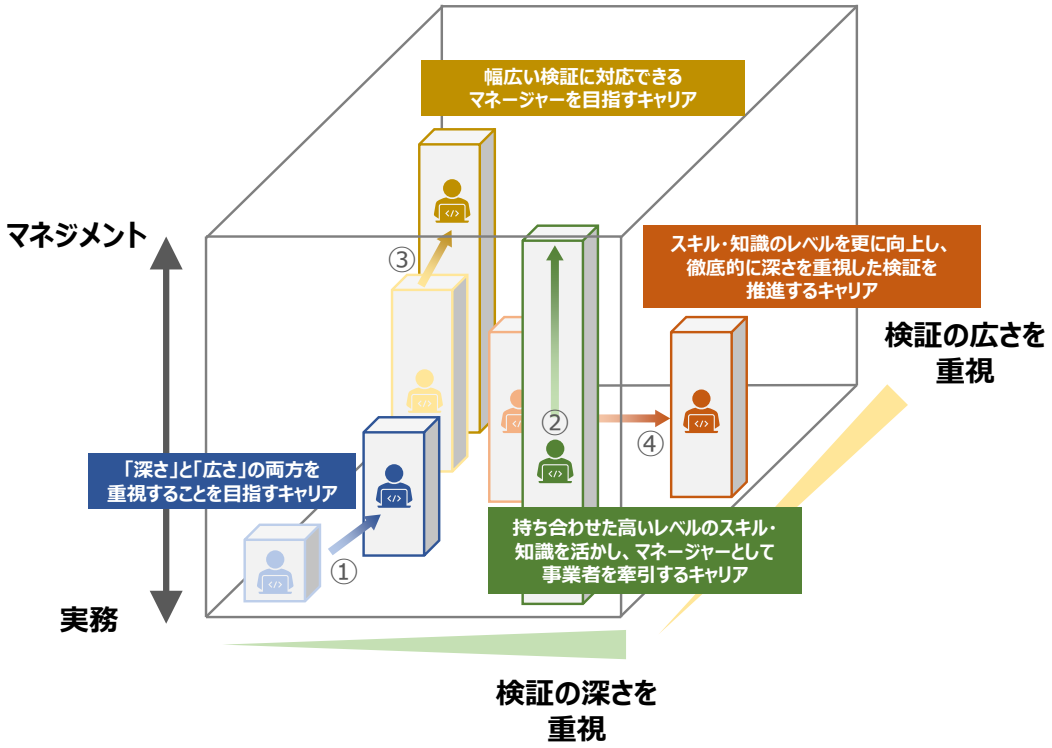

図 3-2 検証人材のキャリアイメージ

自身のキャリアを設計するためには、何年後の将来に、どのような検証人材になりたいかを検討することが必要である。この際、「Will（何をしたいか）」、「Can（何ができるか）」、「Must（何をする必要があるか）」の３つの観点が重要となる。Will の観点では、自身のこれまでの検証の実績や経験を踏まえ、どのようなプロジェクトにやりがいを感じたか、どのようなプロジェクトで成功体験を感じたかを振り返った上で、今後どのような経験をしたいか、どのような検証対象や技術に挑戦していきたいか等を検討することが望ましい。Can の観点では、これまでの検証の実績や経験に加えて、持ち合わせているスキル・知識は何かを確認する。スキル・知識の確認にあたっては、表 2-1 等の体系表から確認することが望ましい。Can の観点では、単純にできる項目を認識するだけではなく、不足していると思われる項目も認識する必要がある。最後に、Must の観点では、検証サービス事業者の一員として実施しなければならない役割や自身の価値観及び行動特性を踏まえ、現状の「Can」を活用して「Will」を実施するためにやるべきことを確認することが望まれる。

4 検証人材の育成に向けて

本節では、検証サービス事業者に所属する検証人材のキャリア実現を支援するために、事業者として実施することが望まれる人材育成の取り組みに関して記載する。

人材育成の取り組みを検討する前段階として、事業者が必要とする人材像を明確にすることが必要である。どの領域の検証人材を求めるかは、事業規模や事業ポートフォリオによって大きく異なる。図 3-1 の 3 軸に基づいた場合、図 4-1 に示すとおり、顧客の幅広い要望に応えるために、検証の深さ・広さ共に対応できる検証サービス事業者（A.）もいれば、挑戦的な検証を事業の主軸とした事業者（B.）であれば、検証の深さを重視する人材が必要となろう。標準化されたプロセスを活用し、網羅性を重視した検証を実施する事業者（C.）であれば、深さより広さを重視した検証人材が重要となる。検証サービス事業者においては、検証人材に求められる役割やスキル・知識を整理し、事業者が必要とする検証人材像を定義することが必要である。この人材像は、職務の内容や職責に応じて複数の段階を設定することが望ましく、検証人材のキャリアに広く対応できる形が望ましい。

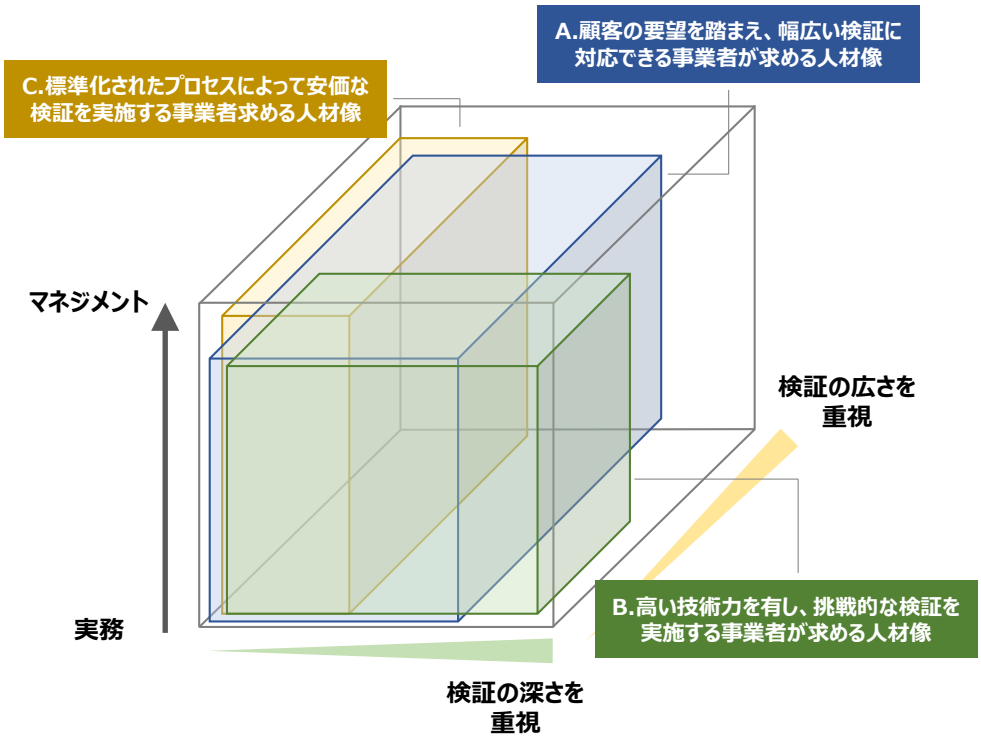

図 4-1 検証サービス事業者が求める人材領域イメージ

検証サービス事業者として、検証人材のキャリアの構想・設計やキャリア実現を支援し、検証人材としてのキャリアを拡大することは、直接的に検証サービス事業者としての質の高い検証サービスの提供に寄与する。特定のスキルや資格を有した人材が要件に含まれる検証依頼も存在するため、検証人材のキャリア支援による検証人材のスキル・知識の向上は、直接的に事業者としての利益拡大につながる。検

証人材のキャリアの構想・設計やキャリア実現を支援するためには、検証人材における実際の検証業務と自己研鑽を有機的に連携させることが不可欠である。実際の検証業務を通じて幅広い検証に関するプロジェクトを経験することで、検証の経験知を蓄積することができ、広さと深さの両方の観点で、検証人材が持つスキル・知識を向上させることができる。幅広い検証に対応できる比較的大規模な事業者であれば、ジョブローテーションを受け入れ、様々な検証の経験を積ませることはキャリアの支援につながる。事業展開が限定的な比較的小規模な事業者においては、後述する自己研鑽を支援する仕組みを充実化させるほか、副業や兼業を許可することも考えられる。検証人材の成長意欲を高めることが重要であり、個人の成長につながるプロジェクトへのアサインや配属を行うことが望ましい。このためにも、上司との間でキャリアや異動希望などをすり合わせる機会を設けることが望ましい。

成長意欲を高めるためには、検証人材による自己研鑽を支援・推奨する仕組みも必要である。スキル・知識を確認するための資格取得に係る受験費用の負担、CTF 等のセキュリティコンテストやセキュリティカンファレンスへの受講費用の負担等、主に金銭面で個人の成長を支援することが望まれる。また、社内外のコミュニティへの参加も支援することも望まれる。多くの検証サービス事業者は社内での勉強会を有しているほか、社外コミュニティに属している検証人材は多い。このような社内外のコミュニティへの参加を業務として認め、参加を奨励することが望ましい。更には、セミナーでの講演、ブログ記事や調査レポートの執筆等、対外発信についても促進することが望ましい。このような機会は検証人材のスキル・知識や実績の対外的なアピールにつながるだけではなく、顧客（検証依頼者）に対して自社の取り組みを伝える機会にもなり、検証依頼につながる可能性もある。検証人材の育成のためには、自己研鑽を支援する仕組みを整えるだけではなく、人材評価の枠組みに組み込むことが望ましい。すなわち、資格の取得、コミュニティへの参加、対外発信等を人材評価の項目に含めることが望まれる。

5 付録

5.1 用語集

- **Attack Tree**
  脅威をルートノードとした木を作成することで、脅威を実現するための攻撃手段を洗い出す手法。

- **CTF（Capture the Flag）**
  情報セキュリティの技術を競い合う競技であり、自らのスキル・知識を駆使して埋め込まれた答え（Flag）を探索するゲーム・競技。個人で Flag を探索する形式もあれば、チームに分かれて Flag を奪い合う形式も存在する。

- **CVSS（Common Vulnerability Scoring System）**
  脆弱性の深刻度を同一の基準の下で定量的に比較できる評価方法であり、0～10.0 の間でスコアが定まる。FIRST (Forum of Incident Response and Security Teams) が管理。

- **CWE（Common Weakness Enumeration）**
  Common Weakness Enumeration の略。ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準。米国非営利団体 MITRE を中心として仕様策定。

- **DFD（Data Flow Diagram）**
  システムにおけるデータとその流れを示した図。

- **DREAD**
  Damage、Reproducibility、Exploitability、Affected users、Discoverability の五つの観点の頭文字から構成される用語で、これら五つの観点に基づきリスクのスコアリングを行う手法。

- **IoT（Internet of Things）**
  既存又は開発中の相互運用可能な情報通信技術により、物理的又は仮想的なモノをネットワーク接続した、高度なサービスを実現するグローバルインフラ。[IoT セキュリティガイドライン ver 1.0]

- **IoT 機器**
  IoT を構成する、ネットワークに接続される機器。

- **ISMS（Information Security Management System）**
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組み。国際規格 ISO/IEC 27001 に要求事項が定められている。

- **JTAG (Joint Test Action Group)**
  IEEE1149.1 で標準化されているポートの通称。IC チップとその周辺の集積回路を含むチップセットとの相互通信や IC チップ自体の検査、回路動作に対する監視および書き換えを行うこと等が可

能。

- **OWASP（Open Web Application Security Project）**
  Web をはじめとするソフトウェアのセキュリティ関する情報共有と普及啓発を目的とした、オープンソース・ソフトウェアコミュニティ。

- **SSL/TLS（Secure Socket Layer/Transport Layer Security）**
  通信相手の認証や通信内容の暗号化等を目的として使用されるプロトコル。TLS は SSL の後継のバージョンにあたるが、本別冊では断りがある場合を除き、これらを総称し、SSL/TLS と表記する。

- **STRIDE**
  Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の六つの脅威の性質の頭文字から構成され、これら六点の性質から脅威を洗い出していく手法。

- **UART (Universal Asynchronous Receiver/Transmitter)**
  デバッグ等を目的として、外部端末から回路基板にアクセスするために使用されるシリアル信号とパラレル信号の変換を行う集積回路。

- **脅威（Threat）**
  システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。[JIS Q 27000:2014]

- **脅威情報（Threat Intelligence）**
  脅威からの保護、攻撃者の活動検知、脅威への対応等に役立つ可能性のある情報。[NIST SP 800-150]

- **脅威分析（Threat Analysis）**
  機器やソフトウェア、システム等に対する脅威を抽出し、その影響を評価すること。主に、製品の要件定義、設計フェーズにて行われる。

- **サイバー攻撃（Cyber Attack）**
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000:2014]

- **サイバーセキュリティ（Cybersecurity）**
  電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

- **サプライチェーン（Supply Chain）**

複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れ。[ISO 28001:2007, NIST SP 800-53 Rev.4]

- **脆弱性（Vulnerability）**
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q 27000:2014]

- **脆弱性検証（Vulnerability Validation）**
  脆弱性の存在を確認するアクティブなセキュリティ検証手法。[NIST SP 800-115]
  脆弱性を洗い出すことを目的とする。

- **セキュリティ検証（Security Validation）**
  機器、システム、組織における脅威に対するセキュリティ対策の妥当性や脆弱性の有無を確認する手法。本手引きでは、特に機器に対するセキュリティ検証について記載している。

- **認証（Authentication）**
  エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000:2014]

- **バックドア（Backdoor）**
  機器に設けられた、正規のログイン方法ではない非公表のアクセス方法。潜在的なセキュリティリスクとなりうる。[NIST SP 800-82 Rev.2]

- **ファジング（Fuzzing）**
  検証対象の機器やソフトウェアに脆弱性を引き起こしうるデータ（ファズデータ）を送り込み、その挙動を確認することで脆弱性を検出する手法。

- **プロトコル（Protocol）**
  複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

- **ペネトレーションテスト（Penetration Test）**
  組織が有するすべてのシステムや、指定されたシステム全体を対象とし、明確な意図を持った攻撃者によって、その目的が達成されうるかを確認するセキュリティ検証手法。

- **マルウェア（Malware）**
  許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェア。[NIST SP 800-53 Rev.4]
  セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

- **リスク（Risk）**

目的に対する不確かさの影響。[JIS Q 27000:2014]

5.2 参考文書

- **サイバーセキュリティ経営ガイドライン Ver2.0 付録 F**
  サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）
  https://www.meti.go.jp/policy/netsecurity/mng_guide.html
- **脆弱性診断士スキルマッププロジェクト（ISOG-J 及び OWASP Japan）**
  https://wiki.owasp.org/index.php/Pentester_Skillmap_Project_JP
- **セキュリティ知識分野（SecBoK）2019（JNSA）**
  https://www.jnsa.org/result/2018/skillmap/
- **NIST SP 800-181: Workforce Framework for Cybersecurity (NICE Framework)**
  https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center