サイバーセキュリティ検証基盤
の構築に関する
報告書

2021 年 4 月

IPA
独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目 次

図 目 次

表 目 次

用語集・略語集

本報告書では、以下のとおり用語を定義する。

用語	概要
Common Criteria（CC）	情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格をいう。
CSAJ	Computer Software Association of Japan の略。
EDR	Endpoint Detection and Response の略で、パソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューションのことをいう。
JNSA	Japan Network Security Association の略。
OSS	Open Source Software の略。
PoC	Proof of Concept の略で、新しい概念や理論、原理、ソリューションなどが実現可能であることを示すための簡易な試行をいう。
SOC	Security Operation Center の略で、ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織をいう。
WBS	Work Breakdown Structure の略で、プロジェクト全体を細かい作業に分割した構成図のことをいう。
サンドボックス	ソフトウェアの特殊な実行環境として用意された、外部へのアクセスが厳しく制限された領域のことをいう。
システムアーキテクチャ	システムの設計方法、設計思想、及びその設計思想に基づいて構築されたシステムの構造をいう。
ゼロトラスト	信頼できないことを前提としてセキュリティ対策を講じる考え方をいう。
フィッシングサイト	暗証番号やクレジットカード番号などを詐取するために、正規の Web サイトを装ったサイトをいう。
フォールスネガティブ	検知漏れのことをいう。
フォールスポジティブ	誤った検知のことをいう。
ランサムウェア	悪意のあるソフトウェア（マルウェア）の一種で、感染したコンピュータを正常に利用できないような状態に置き、復元のために犯人への金品の支払いを要求するものをいう。

1. 調査概要

1.1 調査背景・目的

経済産業省の産業サイバーセキュリティ研究会 WG3（サイバーセキュリティビジネス化）は、信頼できるセキュリティ製品と隠れたニーズを掘り起こし、ビジネスマッチングの場を提供することにより、セキュリティ産業の発展を目指すとしている[1]。これは具体的には、日本で開発されたセキュリティ製品について有効性検証・実環境における試行導入を実施しその結果を発信することで、ユーザーが、日本で開発された製品を選定しやすい環境を構築するものである。

独立行政法人情報処理推進機構（以下「IPA」という。）は、経済産業省の委託を請け、2019 年 9 月にこの事業のあり方を検討する「サイバーセキュリティ検証基盤構築に向けた有識者会議」を設置した。この会議は検証体制や検証方法等の実施案を検討し、その実効性や課題を明らかにするため、少数の製品を題材とした実験的な検証を行った[2]。また、本基盤構築の参考とすべく、セキュリティ製品を生み出す社会の仕組みの例について、海外調査を行った。

この活動を通じて得られた知見や明らかになった課題を以下に示す。

(1) 得られた知見

- 日本発のセキュリティ製品には、国内のユーザー企業が直面しているセキュリティ課題の解決に特長・強みを備えた製品が存在する。こうした特長・強みを活かすことで、日本発のセキュリティ製品が海外製品との差別化を図れる可能性がある
- 日本発のセキュリティ製品の特長を専門家が中立・公平に検証し、その結果をユーザー企業に分かりやすく公表することによって、当該製品の市場参入を促進する効果が期待できる

(2) 明らかになった課題

- 検証対象製品は、公平性の観点から広く公募することが望ましい一方、様々な候補製品に対応する一律な審査基準を作ることには困難がある
- 昨年度、実験的に検証作業を実施したところ、製品機能の調査、検証環境構築、製品の挙動分析等にかなりの時間とコストを要した。本基盤の実運用に向けて、一製品あたりの検証に掛かる時間・コストを低減する必要がある
- 本基盤で検証するセキュリティ製品に対し、十分な市場参入の機会を提供するには、それを促進する社会の仕組み（エコシステム）が重要であることが海外調査で再確認された

本事業は 2019 年度に続く二か年目の事業である。2020 年度は、上述の知見・課題を踏ま

[1] 経済産業省「産業サイバーセキュリティ研究会WG３　第４回　事務局説明資料」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/pdf/004_03_00.pdf （2020 年 12 月 18 日閲覧）

[2] IPA「セキュリティ製品の有効性検証の試行について」 https://www.ipa.go.jp/security/economics/shikoukekka2019.html （2020 年 12 月 18 日閲覧）

えた上で、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤について、構築を行う。さらに、本基盤を実際に運用して、検証対象候補の製品を公募しその中から対象製品を選定して検証を行う。

さらに、本基盤で検証するセキュリティ製品の市場参入を支援する上で有効な、我が国の状況にあったエコシステムの検討を行う。また加えて、昨年度の成果である「試行導入・導入実績公表の手引き」[3]の改良を行う。

1.2 調査実施概要

業務概要は下記のとおりである。

- サイバーセキュリティ検証基盤の構築
- サイバーセキュリティ検証基盤の運用
- エコシステムの検討
- 19 年度成果「試行導入・導入実績公表の手引き」の改良

本報告書では、このうち、「サイバーセキュリティ検証基盤の構築」、「エコシステムの検討」、「19 年度成果「試行導入・導入実績公表の手引き」の改良」に関する調査結果について記載する。

[3] IPA「試行導入・導入実績公表の手引き」https://www.ipa.go.jp/files/000081564.pdf （2020 年 12 月 18 日閲覧）

2. サイバーセキュリティ検証基盤の全体像

公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤を構築した。図 2-1 に示すとおり、検証基盤におけるプロセスを「1. 重要分野選定」、「2. 製品公募」、「3. 製品選定」、「4. 有効性検証」、「5. 検証結果公表」の 5 つと捉え、各プロセスに必要な仕組み（構成要素、手順、実施事項等）の検討を行った。

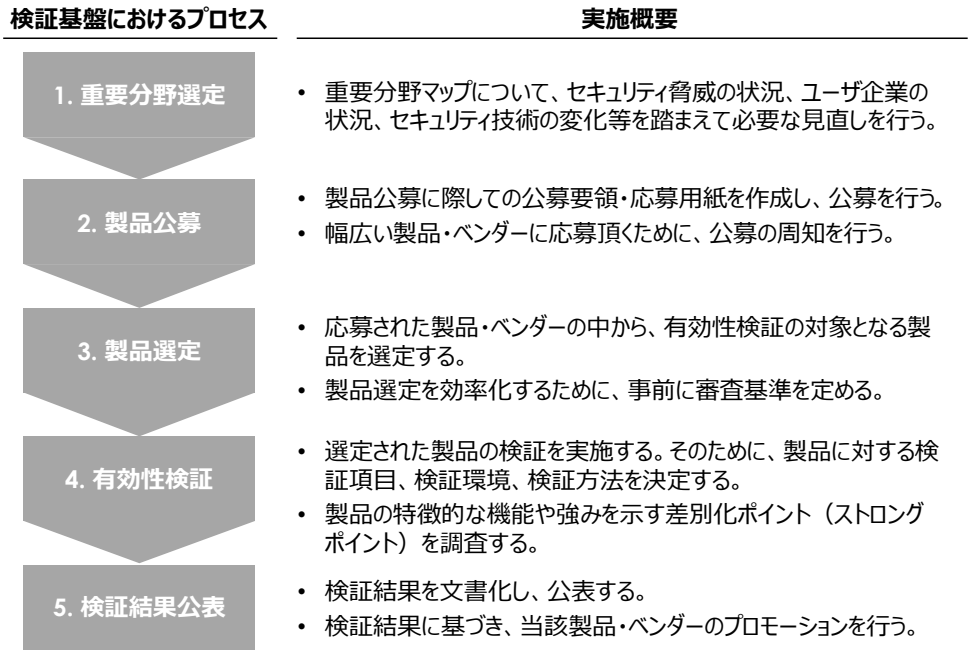


図 2-1　サイバーセキュリティ検証基盤の全体像

3. 重要分野マップの見直し検討

まず、サイバーセキュリティ検証基盤で対象とする重要分野の検討を行った。検討に当たっては、昨年度事業の成果である「2019 年度版セキュリティ製品・サービス重要分野マップ」[4]（以降、「重要分野マップ」と呼ぶ。）をベースとして、セキュリティ脅威の状況、ユーザー企業の状況、セキュリティ技術の変化等を踏まえて必要な見直しを行い、重要分野の背景に関する説明加筆等を行った。なお、重要分野マップとは、日本発の製品・サービスが強みを持っているか、日本固有のニーズがあるか等の観点から選定した重要分野をセキュリティ対策全体の中にマッピングしたものである。

3.1 見直し検討のための調査方法

見直し検討に当たっての前提条件として、重要分野マップにおける重要分野は以下の条件の下で絞り込みがなされた。

条件 1：その分野に日本発製品が存在する
条件 2：日本のユーザーの重要・喫緊課題に対応する
条件 3：検証作業の負担が許容範囲内

条件 2 の検討に当たっては、セキュリティ脅威の状況やユーザー企業の状況を加味する必要がある。そのため、社会的に影響が大きかったと考えられる情報セキュリティにおける事案をまとめたような「情報セキュリティ 10 大脅威」で示された脅威に加え、CTI（Cyber Threat Intelligence：サイバー脅威インテリジェンス）事業者のレポート等を参照し、直近のセキュリティ脅威トレンドを加味することが望まれる。加えて、見直し検討に当たっては、セキュリティ製品や脅威動向に関して専門的な知見を有した有識者からの意見を踏まえることが有効である。これらを踏まえると、見直し検討に考慮すべきセキュリティ脅威の状況やユーザー企業の状況として、以下の項目が挙げられる。

- **新型コロナウイルス感染症拡大に乗じたセキュリティ脅威の増加：**
  新型コロナウイルス感染症に関連する情報共有を謳ったフィッシングサイトやランサムウェアが増加している。また、新型コロナウイルス感染症拡大防止に向けてユーザー企業がテレワークを推進しているが、テレワーク下におけるセキュリティリスクも懸念されている。
- **ゼロトラスト・アーキテクチャに関するガイドラインの発表：**
  これまでの境界防御によるセキュリティの限界や、クラウドサービス活用の推進、テレワークの増加等の現況を踏まえ、新たなセキュリティモデルとしての「ゼロトラスト」が注目を集めている。2020 年 8 月には、米国国立標準技術研究所（NIST）により“Special Publication（SP）800-207: Zero Trust Architecture”の正式版が公開[5]され、ゼロトラスト・アーキテクチャが満たすべき 7 つの基本原則が定義された。今後、国内外のゼロトラストに関する標準的な考え方になると推測される。
- **モバイル端末を対象としたセキュリティ脅威の増加：**

[4] IPA「2019 年度版セキュリティ製品・サービス重要分野マップ」https://www.ipa.go.jp/files/000081561.pdf（2021 年 1 月 14 日閲覧）
[5] NIST「SP 800-207: Zero Trust Architecture」https://csrc.nist.gov/publications/detail/sp/800-207/final （2021 年 1 月 18 日閲覧）

2020 年 3 月に英国メディアによって、10 億台以上の Android デバイスがセキュリティアップデート等のサポート対象から外れており、サイバー攻撃に対して脆弱な状態にあると指摘された[6]。また、Android 端末向けのスパイウェアも登場[7]するなど、モバイル端末がサイバー攻撃の対象として注目を集めつつある。このような脅威に対して、モバイル端末に対するセキュリティソリューションである MTD（Mobile Threat Defense）のようなソリューションが登場している。

なお、重要分野の背景に関する説明加筆や、重要分野のうち検証すべき領域をさらに絞り込む観点では、直近でのセキュリティ脅威やユーザー企業の状況を加味した「キーワード」を設定することが有効である。キーワードは特定のセキュリティ脅威に対応付けられるものではなく、複数のセキュリティ脅威に跨るものである。キーワードを設定することで、重要分野のうち特に注目すべき領域に焦点を絞り込むことができるほか、製品公募に当たって応募多数となった場合に、スクリーニングに活用することができる。

[6] Which? Press Office「Void Android: More than one billion Android devices at risk of hacking attacks」 https://press.which.co.uk/whichpressreleases/void-android-more-than-one-billion-android-devices-at-risk-of-hacking-attacks/ （2021 年 1 月 18 日閲覧）

[7] TrendMicro「「Earth Empusa」の標的型攻撃で使用された Android 向け不正アプリ「ActionSpy」」 https://blog.trendmicro.co.jp/archives/25790 （2021 年 1 月 18 日閲覧）

4. 製品公募の仕組み定式化

選定した重要分野に関する日本発のセキュリティ製品を検証するために、まず製品を公募する仕組みの定式化を行った。

4.1 製品公募の仕組みにおける構成要素

製品公募の仕組みにおける構成要素を表 4-1 に示す 5 つと捉え、各要素に必要な実施事項の検討を行った。

表 4-1 製品公募の仕組みにおける構成要素・実施事項

構成要素	具体的な実施事項
① 有効性検証のスケジュール策定	• 最低限確保すべき期間と検証全体の期間を加味し、公募期間、製品審査期間、検証期間等を含む検証全体のスケジュールを策定する。
② 製品及びそのベンダーに課す応募要件の整理	• 公募に際して製品及びベンダーに課す応募要件を整理する。 • 応募要件は、客観的な審査と効率的な審査・検証のトレードオフを考慮するために、必須要件と追加要件によって構成する。
③ 公募要領・仕様書・応募用紙の作成	• 策定したスケジュール及び応募要件を反映した公募要領・仕様書を作成する。 • また応募用紙を作成する。
④ 製品公募の事前周知	• 多くの応募を得るために、公募の対象となる重要分野の製品を開発しているベンダーに対して、事前に公募を周知する。
⑤ 製品公募の実施・周知	• 製品の公募を行い、応募があった場合には応募用紙を受理する。 • 公募に関して質問があった場合には、質問への回答を行う。 • 多くの応募を得るために、公募を開始した旨を HP やその他の媒体を活用して周知する。

以降、それぞれの構成要素における具体的な実施事項について記載する。

4.2 有効性検証のスケジュール策定

製品公募を開始するに当たって、はじめに有効性検証全体に係るスケジュールを策定す

る。これは、検証全体のスケジュールによって、以降で作成する公募要領や仕様書に含める要件が変わる可能性があるためである。有効性検証全体のスケジュール作成に当たっては、最低限確保すべき期間と検証全体の期間を加味し、公募期間、製品審査期間、検証期間等を含む検証全体のスケジュールを策定する。なお、可能な範囲で、構成要素は並行して実施する。また、多くの製品応募を得るために、製品公募の実施期間は一週間以上設けるべきである。また、客観的かつ適正な製品選定を行うために、製品審査期間も一週間以上設けるべきである。併せて、効果的な検証を実施するために、検証期間は一ヶ月以上設けるべきである。ただし、この期間は選定した重要分野及び採択予定件数に依存するものであり、大規模環境や大量のテストデータを必要とする分野の場合、更に長い期間を設ける必要がある。なお、日付の換算は営業日換算で行うことが望まれる。

以上の留意事項を踏まえると、図 4-1 に示すような有効性検証スケジュールが一例として考えられる。

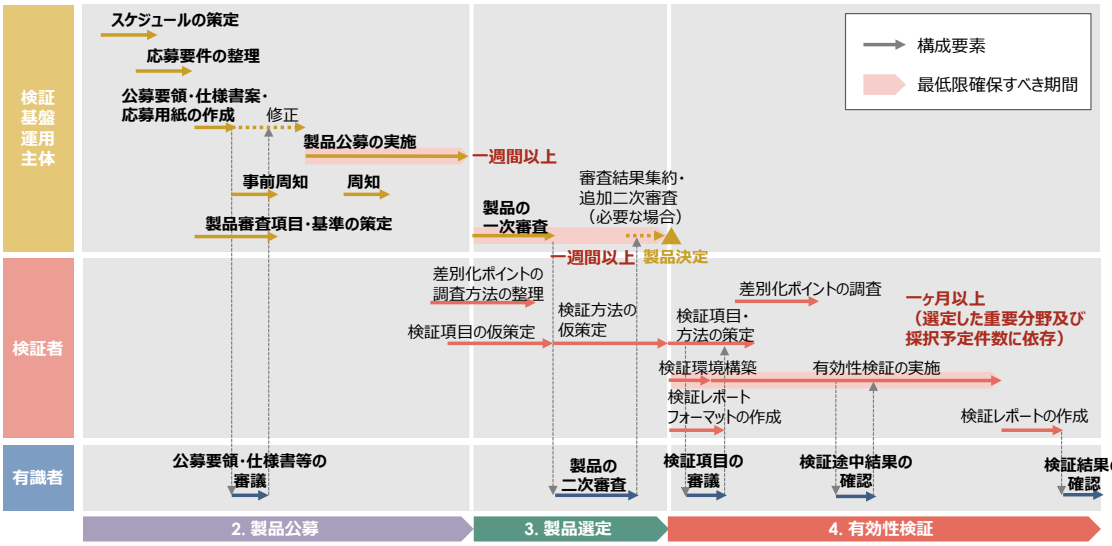


図 4-1　有効性検証のスケジュール整理イメージ

なお、「検証基盤運用主体」とは、サイバーセキュリティ検証基盤の運用を担当するとともに、公募・選定・検証に係る一連のプロセスの公平性を担保する役割を担う（以下、単に「運用主体」と記すことがある）。「検証者」は、選定された製品・ベンダーに対して有効性検証を行う役割を担う。そして、「有識者」は専門的な観点から製品選定・検証結果の評価を行う役割を担う。

4.3　製品及びそのベンダーに課す応募要件の整理

製品の選定に当たっては、優れた日本発のセキュリティ製品を中立・公平に選定することが望まれる。一方で、審査に必要な期間が限られている場合、効率的な審査を行う必要がある。本基盤では、このトレードオフを考慮するために、製品及びそのベンダーに課す応募要件は、必須要件と追加要件によって構成するものとして整理した。

製品及びそのベンダーに課す応募要件の項目を表 4-2 に示す。必須要件では、本事業の目的である「日本発」製品であることを確認することに加え、製品審査及び検証作業の効率化のために、製品や検証環境の提供、検証者及び検証基盤運用主体との連絡体制の構築等を

求める。また、製品の有効性検証では、製品ベンダーが主張する製品の差別化ポイント（ストロングポイント）の確からしさを確認することとなる。差別化ポイントに関する検証を効率化するために、対象製品の差別化ポイントを第三者が理解できるように記載することを追加要件として求めた。なお、「日本発」製品であることの定義については、継続して議論することが望まれる。

表 4-2　製品及びそのベンダーに課す応募要件

区分	要件項目
必須要件	• 応募ベンダーは、法人格を有していること。 • 応募ベンダーは、日本国内に開発拠点を有していること。さらに、応募製品はこの拠点で製品開発されたものであること。 • 対象とする製品は、新規に市販を開始してから 5 年以内であること。 • 暴力団排除に関する誓約事項について、誓約する者であること。 • 応募製品が、有識者検討会において選定した重要分野に該当すること。 • 検証の実施に当たって、検証項目、検証環境、公表内容等について検証者と協議・調整すること。 • 検証の実施に当たって、製品やその稼働に必要な付帯物、検証用データ、利用環境等を無償で貸与すること。 • 検証を効率的に実施するために、検証者及び検証基盤運用主体との連絡体制を構築すること。 • 応募製品の技術・機能等を正しく理解した上で検証方式を策定することを目的として、検証者及び検証基盤運用主体に対して、応募製品の技術責任者、開発責任者等を知らせ、必要に応じて相談できるようにすること。 • 本試行検証の実施に当たって、応募者と検証者、検証基盤運用主体との間で秘密保持契約の締結を求めないこと。 • 要件を満たしていることを支持するエビデンスの提示に当たっては、その箇所（ページ番号、章番号 等）を明確にすること。
追加要件	• 対象とする製品の差別化ポイント（機能、性能、定量的データ、評価・レビュー結果、受賞実績 等）を第三者が理解できるように記載すること。 • 応募製品が、有識者会議にて選定したキーワードに関連する製品であること。 • 海外に本社機能を有する親会社が存在するかを記入すること。存在する場合、親会社の国籍や社名を記入すること。

区分	要件項目
	• 検証の実施に当たって、製品性能、運用容易性、導入容易性等を検証する方法を第三者が理解できるように記載すること。 • 期間内で対象製品の検証を完了するための工夫（検証環境設定の容易性、連絡体制の整備、検証に必要な事前の整備 等）を第三者が理解できるように記載すること。

4.4　公募要領・仕様書・応募用紙の作成

製品及びそのベンダーに課す応募要件を踏まえ、公募要領・仕様書・応募用紙を作成する。公募要領では、本事業の概要を示すとともに、応募に係る要件や応募方法を記載する。仕様書においては、有効性検証の概要を示し、有効性検証実施のために応募者に求める協力事項を記載する。応募用紙では、必須要件・追加要件に満たしていることを求めるとともに、要件を満たしていることを支持するエビデンスの提示を求める。エビデンスは機能、性能、処理能力を表す数値・検証データや受賞した外部の賞の公表ページ等、客観的に差別化ポイントを判断できるものと位置付ける。なお、エビデンスの提示に当たっては添付ファイルを認めることとする。

以下にそれぞれの構成案を示す。具体的な内容については、都度検討することが望まれる。

表 4-3　公募要領 構成案

1. 概要
   1.1 背景・目的
   1.2 公募の内容
   1.3 スケジュール外観
2. 応募資格
3. 応募書類作成要領
4. 応募要領
   4.1 提出書類
   4.2 提出期限
   4.3 提出先
   4.4 提出方法
   4.5 応募に関する質問の受付等
5. 審査方法等
   5.1 審査方法
   5.2 採択件数
6. その他

(別添 1) 個人情報の取扱いに関する特則
(別添 2) 特定個人情報の取扱いに関する特則

表 4-4　仕様書 構成案

1. 件名
2. 背景・目的
3. 実施内容
4. 応募者に求める協力事項

5. 募集する製品について 6. 検証実施期間

表 4-5　応募用紙 構成案

1. 応募者情報 2. 応募資格のエビデンス 3. 応募するセキュリティ製品・事業者に関する情報 4. 応募資格の確認

4.5　製品公募の事前周知

多くの応募を得るために、公募の対象となる重要分野の製品を開発しているベンダーに対して、事前に公募を周知することが望ましい。事前周知に当たっては、事業の背景・概要を示すとともに、採択された場合のメリットを提示することが望まれる。ただし、「応募すれば採択される」という誤解を避けるための記載を行う必要がある。

事前周知の対象とする製品ベンダーとしては、有識者より提案された製品ベンダーのほか、重要分野を踏まえて調査した結果明らかになった製品ベンダーを含む。

4.6　製品公募の実施・周知

作成した公募要領・仕様書・応募用紙に基づき、製品の公募を開始する。前述のとおり、公募の期間は 1 週間以上を設けるべきである。また、公募に関して質問があった場合には、質問への回答を行う。質問の受付期間を公募期間内に設定する必要がある。

また、多くの応募を得るために、公募を開始した旨を HP やその他の媒体を活用して周知することが望まれる。事前周知と同様に、公募を開始した旨を周知するに当たっては、事業の背景・概要を示すとともに、採択された場合のメリットを提示するとともに、「応募すれば採択される」という誤解を避けるための記載を行う。周知する媒体としては、検証基盤運用主体が有するメーリングリストや公式 Twitter アカウント等を活用することが望まれる。併せて、セキュリティ製品ベンダーが所属する日本ネットワークセキュリティ協会（JNSA）やコンピュータソフトウェア協会（CSAJ）等の業界団体に対して、製品公募に関する周知を行うことで、セキュリティ製品ベンダーに直接的に周知することが可能となる。

5. 製品選定の仕組み定式化

製品の公募に対して応募があった製品・ベンダーから、検証対象とする製品・ベンダーを選定する仕組みの定式化を行った。

5.1 製品選定の仕組みにおける構成要素

製品選定の仕組みにおける構成要素を表 5-1 に示す 3 つと捉え、各要素に必要な実施事項の検討を行った。

表 5-1 製品選定の仕組みにおける構成要素・実施事項

構成要素	具体的な実施事項
① 製品審査項目・基準の策定	• 製品選定時に用いる審査の項目及び基準を、応募要件に基づき策定する。
② 製品の一次審査	• 製品審査基準に基づき、応募された製品・ベンダーが必須要件に満足しているかを、エビデンスに基づき確認する。 • 必須要件を満足しない応募製品・ベンダーについては、一次審査にて不合格とする。
③ 製品の二次審査	• 製品審査基準に基づき、応募された製品・ベンダーが優れた差別化ポイントを有しているかを、エビデンスに基づき確認する。 • 優れた差別化ポイントを有している製品・ベンダーのうち、採択予定の製品件数までの上位を検証対象として選定する。

以降、それぞれの構成要素における具体的な実施事項について記載する。

5.2 製品審査項目・基準の策定

まず、製品選定時に用いる審査の項目及び基準を決定する。効率的かつ客観的に審査を行うために、審査項目は公募時に課した応募要件（必須要件・追加要件）とする。必須要件は、すべての応募者が満たす必要のある審査基準として扱い、一つでも必須要件を満たしていないと評価される応募者は不合格とする。追加要件は、一次審査合格後の追加審査基準要素として扱う。特に、一次審査に合格した製品の差別化ポイントを応募者提出のエビデンスに基づき判断し、検証する製品・ベンダーを評価・決定する。二次審査によって対象製品が採択予定件数に絞れない場合には、追加二次審査として検証を効率的かつ効果的に実施できるかを第三者的に判断し、製品・ベンダーを評価・決定する。

審査項目と審査基準、そして審査のプロセスは図 5-1 に示すとおりである。なお、一次審査及び二次審査項目詳細は、第 5.3 節（製品の一次審査）及び第 5.4 節（製品の二次審査）

にてそれぞれ記載する。

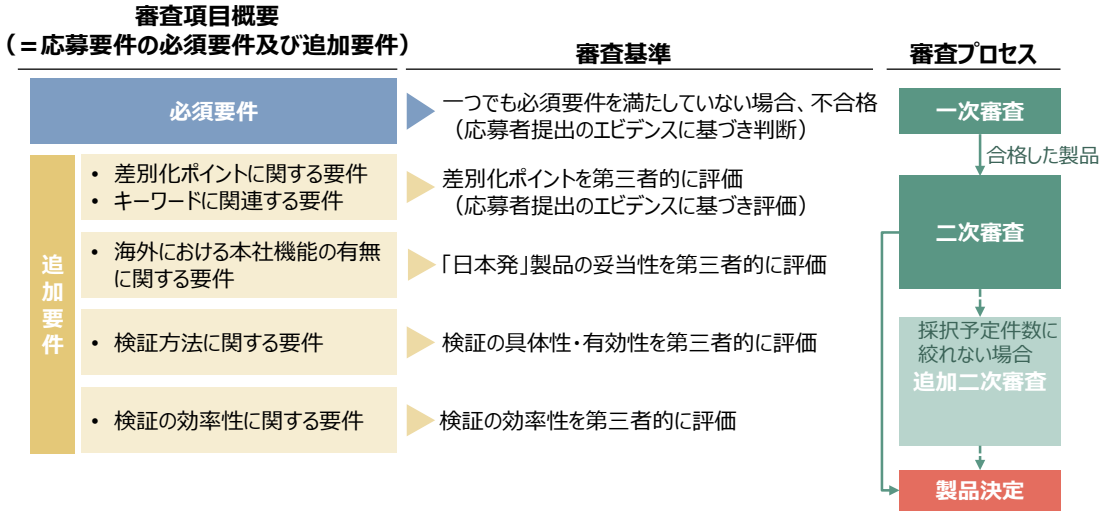


図 5-1　審査項目概要・基準及びプロセス

5.3　製品の一次審査

製品の一次審査においては、応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づいて、応募者の合格／不合格を審査する。前述のとおり、審査項目は応募要件の必須項目に基づき設定し、表 5-2 に示すとおり、それぞれの項目を応募用紙やエビデンスに基づいて審査する。いずれの審査項目についても、応募用紙やエビデンスに基づいて機械的に審査できるため、審査効率化のために運用主体が審査することが望まれる。審査の結果、一つでも必須要件を満たしていないと評価される応募者は不合格とする。

表 5-2　製品の一次審査における審査項目と審査方法

区分	審査項目	審査方法
必須要件	• 応募ベンダーは、法人格を有しているか。 • 応募ベンダーは、日本国内に開発拠点を有しているか。さらに、応募製品はこの拠点で製品開発されたものであるか。 • 対象とする製品は、新規に市販を開始してから 5 年以内であるか。	応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づき確認。

区分	審査項目	審査方法
	• 暴力団排除に関する誓約事項について、誓約する者であるか。 • 検証の実施に当たって、検証項目、検証環境、公表内容等について検証者と協議・調整するか。 • 検証の実施に当たって、製品やその稼働に必要な付帯物、検証用データ、利用環境等を無償で貸与するか。 • 検証を効率的に実施するために、検証者及び検証基盤運用主体との連絡体制を構築するか。 • 応募製品の技術・機能等を正しく理解した上で検証方式を策定することを目的として、検証者及び IPA に対して、応募製品の技術責任者、開発責任者等を知らせているか。 • 本試行検証の実施に当たって、応募者と検証者、検証基盤運用主体との間で秘密保持契約の締結を求めないか。	応募者による応募用紙の記載に基づき確認。
	• 応募製品が、有識者検討会において選定した重要分野に該当するか。 • 近年注目されるサイバーセキュリティ脅威に対して有効な製品であるか。	応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づき確認。
	• 要件を満たしていることを支持するエビデンスの提示に当たっては、支持している箇所（ページ番号、章番号 等）を明確にしているか。	応募者による応募用紙の記載に基づき確認。

5.4　製品の二次審査

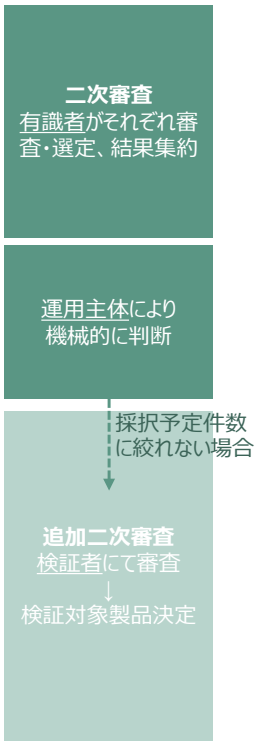
一次審査に合格した製品に対して、応募者による追加要件に対する記載に基づき二次審査を行う。二次審査に係るプロセスを表 5-3 に示す。二次審査では、製品の差別化に関する審査や「日本発」製品であることの判断を行う。製品の差別化ポイントの審査に当たっては、専門的な観点から審査するために、有識者による審査を行う。有識者が各審査項目の合否をそれぞれ審査し、各有識者が採択予定件数の製品を選定する。各審査項目の審査に当たっては、「強い差別化ポイントである」、「差別化ポイントである」、「差別化ポイントではない、差別化ポイントであると判断できない」等、3 段階以上の審査項目を設けると良い。有識者の選定結果を集約し、選定件数が多い製品上位から検証対象製品として決定する。なお、「日本発製品」でない可能性を把握するために、判断材料として、本社機能を有した海外親会社

の有無、その国籍・社名について、運用主体が確認する。

二次審査の結果、選定件数が多い製品が同率であった場合等、対象製品が採択予定件数に絞れない場合には追加二次審査を行う。追加二次審査では、検証者によって、検証の効率性・有効性を考慮した審査項目をもとに合否を審査する。

表 5-3　製品の二次審査における審査項目と審査方法

区分	審査項目	審査者	審査方法
追加要件	• 記載された製品の差別化ポイント（機能、性能、定量的データ、評価・レビュー結果、受賞実績 等）は、差別化ポイントとして相応しいものか • 差別化ポイントのエビデンスの内容は十分か • 差別化ポイントは検証することが可能か • 差別化ポイントはユーザーニーズに応えるものか	有識者	応募者による応募用紙の記載、及び応募者によって提出されたエビデンスに基づき確認。
	• 海外に本社機能を有する親会社が存在しているか。 • 存在する場合、親会社の国籍や社名を記入されているか。 • 親会社は懸念等が存在するベンダーではないか。	運用主体	応募者による応募用紙の記載に基づき確認。
	• 記載された製品性能、運用容易性、導入容易性等を検証する方法は具体的か • 検証方法は製品性能、運用容易性、導入容易性等を検証するために相応しいものか • 検証方法は、事業の期間内で実施可能な内容か	検証者	応募者による応募用紙の記載に基づき確認。
	• 記載された検証を完了するための工夫（検証環境設定の容易性、連絡体制の整備、検証に必要な事前の整備 等）は具体的か • 工夫は、検証作業を効率化する工夫として相応しいものか		応募者による応募用紙の記載に基づき確認。

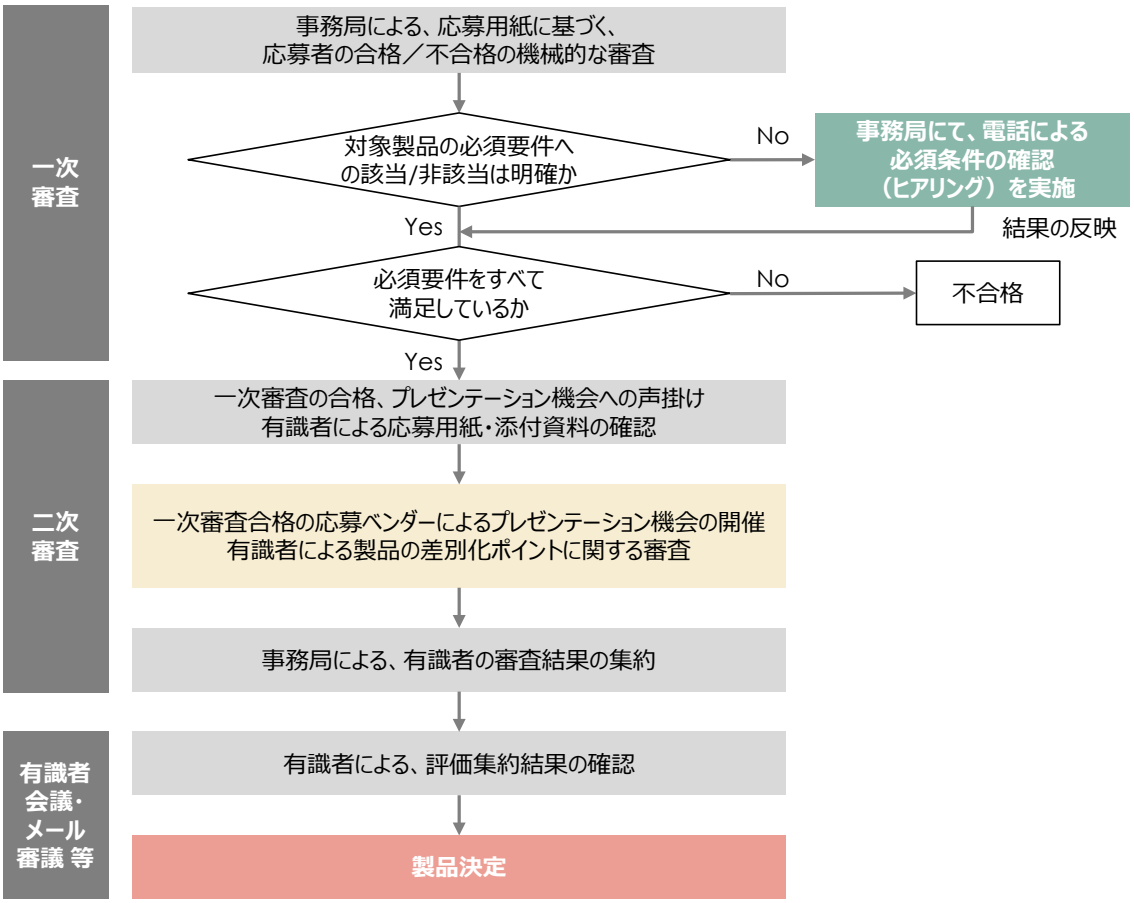


5.5　ベンダーへのヒアリング及びベンダーによるプレゼンテーションの実施

製品審査に当たって、応募ベンダーに対してプレゼンテーションの機会を提供することが望まれる。プレゼンテーションの実施有無は、有効性検証全体のスケジュールを踏まえて決定すべきであるものの、応募ベンダーに対して双方向で差別化ポイントを確認できるという利点がある。プレゼンテーションは、必須要件をすべて満足している一次審査に合格した応募ベンダーのみを対象に、製品の二次審査にて実施することが望まれる。プレゼンテーションの時間は 5 分～10 分程度の短時間とし、応募ベンダーが主張したい製品の差別化ポイントを重点的に説明いただくこと望ましい。プレゼンテーションや応募用紙・添付資料の内容を踏まえ、有識者による質疑応答を行い、その結果を踏まえ、各審査項目の合否を有識者がそれぞれ審査し、個々人にて採択予定件数の製品を選定する方針が考えられる。なお、プレゼンテーションを実施する場合には、公募要領にて実施概要やプレゼンテーションの位置付けを提示する必要がある。

プレゼンテーションと比較して簡易的に実施できるヒアリングについては、応募ベンダーを救済する目的で実施することが望まれる。ヒアリング及びプレゼンテーション機会の実施に係るフローを図 5-2 に示す。フローに示すとおり、一次審査の段階で、応募ベンダー

記載の応募用紙における必須要件への該当に疑念が生じた場合にヒアリングを実施することが望まれる。必須条件の確認のみであるため、簡易的に電話等でのヒアリングとする。



※ 二次審査において選定件数が多い製品が同率であった場合等、対象製品が採択予定件数に絞れない場合には追加二次審査を行うが、本フローでは省略している。

図 5-2　応募ベンダーに対するヒアリング・プレゼンテーション機会の実施フロー

6. 検証の仕組み定式化

検証対象として選定した製品に対する検証の仕組み定式化を行った。

6.1 検証の仕組みにおける構成要素

検証の仕組みにおける構成要素を表 6-1 に示す 4 つと捉え、各要素に必要な実施事項の検討を行った。

表 6-1 有効性検証の仕組みにおける構成要素・実施事項

構成要素	具体的な実施事項
① 検証項目の策定	• 有効性検証の検証項目を策定する。
② 検証方法の策定	• 検証項目を検証するための具体的な方法を策定する。
③ 有効性検証の実施	• 検証計画を策定する。 • 検証に当たって必要となる検証環境を準備・構築する。 • 選定した検証製品に対して、策定した検証項目・検証方法に基づき検証を実施する。
④ 検証結果レポートの作成	• 検証結果を踏まえて、検証結果レポートを作成する。

以降、それぞれの構成要素における具体的な実施事項について記載する。

6.2 検証項目の策定

6.2.1 検証項目の策定ステップ

まず、製品に対して適用する検証項目を策定する。検証項目の策定に当たっては表 6-2 に示すステップを辿る。

本ステップにおいては、検証対象製品が決定する前段階で、選定した重要分野に適用される検証項目の大分類を策定する。また、策定した大分類に基づき、各重要分野で検証すべき個別検証項目を仮策定する。個々で仮策定された個別検証項目は一種のカタログであり、製品選定後に、選定された製品ベンダーと協議し、製品の差別化ポイントを効果的に検証できるよう個別検証項目案を選択することとなる。選択された検証項目案に対して有識者による確認・審議を行い、項目の妥当性を判断する。

表 6-2　検証項目の策定ステップ

検証項目の策定ステップ	実施概要	実施主体
重要分野の選定	• 有識者会議において検証の対象となる重要分野の選定を行う。	有識者
検証項目 大分類の策定・個別検証項目の仮策定	• 重要分野に共通して適用される検証項目の大分類を策定する。 • 策定した大分類に基づき、各重要分野で検証して確認すべき個別検証項目を仮策定する。	検証基盤運用主体・検証者
製品決定		
個別検証項目案の策定	• 選定された製品のベンダーと協議し、製品の差別化ポイントを効果的に検証できるよう、仮策定された個別検証項目に加筆修正を行い、個別検証項目の案とする。	検証基盤運用主体・検証者・応募ベンダー
個別検証項目案の審議	• 有識者会議やメール審議等において個別検証項目案の妥当性を審議する。	有識者
検証項目の確定	• 有識者会議の結果を踏まえて、検証項目を確定する。	検証基盤運用主体・検証者・応募ベンダー

6.2.2　検証項目の大分類・個別検証項目の策定

サイバーセキュリティ検証基盤では、Common Criteria（CC）認証のように情報セキュリティの観点で適切な設計や正しい実装がされていることを厳密に評価検証するのではなく、差別化ポイントを評価し対象製品にアワードを与えるような検証を実施することを目的としている。そのため、厳密な検証項目を策定するのではなく、それぞれの製品の情報や差別化ポイントを踏まえて、製品毎に検証項目を策定する必要がある。

一方で、検証作業全体の効率化のために、ある程度事前に想定される検証項目を策定することが望まれる。本基盤では、重要分野に共通して適用される差別化ポイントを評価する検証項目の大分類を予め設定し、それぞれの大分類の下に各製品の個別検証項目を策定する

形とする。本基盤では、重要分野に共通して適用される大分類を「製品機能・性能」、「運用性」、「導入容易性」の 3 つとする。

製品の選定前に、この大分類に基づき、各重要分野における個別の検証項目を仮策定する。仮策定する検証項目は一種のカタログであり、例えば表 6-3 に示すように、各重要分野の製品が満たしていると想定される差別化ポイントを検証する仮の項目となる。検証対象となる製品及びそのベンダーが選定された後、運用主体及び検証者と製品ベンダーにて協議し、製品の差別化ポイントを効果的に検証できるよう、適切な個別検証項目を製品毎に抽出し、個別検証項目の案とする。その後、対象製品における個別検証項目及び検証方法について、製品の差別化ポイントを評価するうえで妥当であるかを有識者により審議し、決定する。有識者による検証項目の確認においては、専門的な視点から製品の差別化ポイントを抽出するために、製品ベンダーに確認すべき項目も提示いただくことが望ましい。

表 6-3　検証項目の大分類及び個別検証項目仮策定の例

大分類	重要分野「脅威の可視化」における個別検証項目（仮）	重要分野「脆弱性の可視化」における個別検証項目（仮）	重要分野「IT 資産の認証/検証」 における個別検証項目（仮）
製品機能・性能	• 検知できる脅威や不正通信の種類に関する検証項目 • 検知した脅威や不正通信に関する情報の質・量に関する検証項目 • ブラックリスト・ホワイトリストの作成仕様に関する検証項目 • ブラックリスト・ホワイトリストの作成期間に関する検証項目 • 検知した脅威や不正通信の情報の管理に関する検証項目 • 検知した脅威や不正通信の対応優先	• 検出できる脆弱性の量に関する検証項目 • 検出した検出に関する情報の質・量に関する検証項目 • 新規脆弱性が検出できるまでの期間に関する検証項目 • 検出された脆弱性に対する対応に関する検証項目 • ソフトウェア構成情報の取得に関する検証項目 • 古い OSS における脆弱性の検出に関する検証項目 • 検出した脆弱性への対応管理機能に関する検証項目	• 認証/検証の判断ロジックに関する検証項目 • 不正な IT 資産の接続防止に関する検証項目 • 検出した不正な IT 資産に関する情報の質・量に関する検証項目 • IT 資産情報の取得に関する検証項目 • ブラックリスト・ホワイトリストの作成仕様に関する検証項目 • ブラックリスト・ホワイトリストの作成期間に関する検証項目

大分類	重要分野「脅威の可視化」における個別検証項目（仮）	重要分野「脆弱性の可視化」における個別検証項目（仮）	重要分野「IT 資産の認証/検証」 における個別検証項目（仮）
	度に関する検証項目 • 脅威や不正通信への対応管理機能に関する検証項目 • 検知した脅威情報や不正通信の一覧表示に関する検証項目 • 検知仕様に関する検証項目 • 検知した脅威や不正通信の情報の通知に関する検証項目 • フォールスポジティブやフォールスネガティブの発生度合いに関する検証項目	• 検出した脆弱性の一覧表示に関する検証項目 • 検出した脆弱性の情報の通知に関する検証項目 • フォールスポジティブやフォールスネガティブの発生度合いに関する検証項目	• IT 資産情報や認証情報への対応管理機能に関する検証項目 • 動作ログの適切な管理に関する検証項目 • 組織内で使用されている IT 資産の一覧表示に関する検証項目 • 組織内で検出されている不正な IT 資産の一覧表示に関する検証項目 • 検知仕様に関する検証項目 • 検知した不正な IT 資産の情報の通知に関する検証項目 • フォールスポジティブやフォールスネガティブの発生度合いに関する検証項目

大分類	重要分野「脅威の可視化」における個別検証項目（仮）	重要分野「脆弱性の可視化」における個別検証項目（仮）	重要分野「IT 資産の認証/検証」 における個別検証項目（仮）
運用性	• 通信フローの自動監視・自動検知に関する検証項目 • 検知した脅威や不正通信の自動分析に関する検証項目 • 脅威分析の結果の優先度付けに関する検証項目 • 脅威のレベル分けに関する検証項目 • ダッシュボード等における脅威の検知結果・分析結果の整理に関する検証項目 • 検知に用いるデータの自動更新に関する検証項目 • 製品自体の不具合や脆弱性が見つかった場合の対応に関する検証項目 • 製品のロードマップや事業計画に関する検証項目	• 脆弱性の自動検査に関する検証項目 • 検出した脆弱性の自動分析に関する検証項目 • 検出された脆弱性の優先度付けに関する検証項目 • 脆弱性のレベル分けに関する検証項目 • ダッシュボード等における脆弱性の検出結果の整理に関する検証項目 • 検出に用いるデータの自動更新に関する検証項目 • 製品自体の不具合や脆弱性が見つかった場合の対応に関する検証項目 • 製品のロードマップや事業計画に関する検証項目	• IT 資産情報の自動収集に関する検証項目 • 検出された不正な IT 資産の自動分析に関する検証項目 • 検出された資産の優先度付けに関する検証項目 • ダッシュボード等における IT 資産の検出結果の整理に関する検証項目 • 不正な IT 資産のレベル分けに関する検証項目 • ログの収集・分析に関する検証項目 • IT 資産の追加・削除の容易性に関する検証項目 • 検出した結果の通知に関する検証項目 • 認証/検証に用いるデータの自動更新に関する検証項目 • 製品自体の不具合や脆弱性が見つかった場合の対応に関する検証項目 • 製品のロードマップや事業計画に関する検証項目

大分類	重要分野「脅威の可視化」における個別検証項目（仮）	重要分野「脆弱性の可視化」における個別検証項目（仮）	重要分野「IT 資産の認証/検証」 における個別検証項目（仮）
導入容易性	• 導入できる環境に関する検証項目 • エージェントのインストールに関する検証項目 • 初期設定の容易性に関する検証項目 • 設置の際に生じるシステム停止時間に関する検証項目 • 製品費用に関する検証項目	• 導入できる環境に関する検証項目 • エージェントのインストールに関する検証項目 • 初期設定の容易性に関する検証項目 • 設置の際に生じるシステム停止時間に関する検証項目 • 製品費用に関する検証項目	• 導入できる環境に関する検証項目 • 既存システムの変更要否に関する検証項目 • エージェントのインストールに関する検証項目 • 初期設定の容易性に関する検証項目 • 設置の際に生じるシステム停止時間に関する検証項目 • 製品費用に関する検証項目

※ この個別検証項目はあくまで仮であり、実際には製品ベンダーと協議して、適切な個別検証項目を抽出することに留意。

6.3 検証方法の策定

それぞれの検証項目を検証する方法を、運用主体及び検証者にて策定する。有効性検証における検証方法として、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つの方法が考えられる。可能な限り多くの検証項目について検証環境での実検証を実施することが望ましいものの、複数の客観的な評価が求められる項目や長時間・高コストを要する項目は実検証が困難である。よって、このような項目のうち、定量的な評価が行える項目や客観的な評価が求められる項目については、データや記録に基づく評価を行う。加えて、ベンダーヒアリングに基づく評価では、ベンダーの恣意的な回答により評価の客観性に影響を及ぼす可能性がある。そのため、検証環境での実検証及びデータや記録に基づく評価が困難な項目に対して例外的に適用することとし、ヒアリングに基づく評価に至った項目について、その理由も含めて有識者に状況説明を行うことが望まれる。

例として、表 6-3 で示した重要分野「脅威の可視化」の検証項目に対して、想定される検証方法を示した対応関係を表 6-4 に示す。すべての検証項目についてベンダーヒアリングに基づく評価の対象になりうるものの、前述のとおり評価の客観性の観点から例外的な検証方法として位置付け、ベンダーのノウハウや仕様等、ヒアリングに基づいた評価でのみ確認できる項目に関して用いることとする。

表 6-4　検証項目に対する検証方法の策定方針イメージ

大分類	重要分野「脅威の可視化」における個別検証項目（仮）	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価
製品機能・性能	• 検知できる脅威や不正通信の種類に関する検証項目	✓	✓	✓
	• 検知した脅威や不正通信に関する情報の質・量に関する検証項目	✓	✓	✓
	• ブラックリスト・ホワイトリストの作成仕様に関する検証項目			✓
	• ブラックリスト・ホワイトリストの作成期間に関する検証項目		✓	✓
	• 検知した脅威や不正通信の情報の管理に関する検証項目	✓		✓
	• 検知した脅威や不正通信の対応優先度に関する検証項目	✓		✓
	• 脅威や不正通信への対応管理機能に関する検証項目	✓	✓	✓
	• 検知した脅威情報や不正通信の一覧表示に関する検証項目	✓	✓	✓
	• 検知仕様に関する検証項目			✓
	• 検知した脅威や不正通信の情報の通知に関する検証項目	✓		✓
	• フォールスポジティブやフォールスネガティブの発生度合いに関する検証項目		✓	✓
運用性	• 通信フローの自動監視・自動検知に関する検証項目	✓	✓	✓
	• 検知した脅威や不正通信の自動分析に関する検証項目	✓	✓	✓
	• 脅威分析の結果の優先度付けに関する検証項目	✓	✓	✓
	• 脅威のレベル分けに関する検証項目	✓	✓	✓
	• ダッシュボード等における脅威の検知結果・分析結果の整理に関する検証項目	✓	✓	✓
	• 検知に用いるデータの自動更新に関する検証項目		✓	✓
	• 製品自体の不具合や脆弱性が見つかった場合の対応に関する検証項目		✓	✓
導入容易性	• 導入できる環境に関する検証項目	✓		✓
	• エージェントのインストールに関する検証項目	✓		✓
	• 初期設定の容易性に関する検証項目	✓	✓	✓
	• 設置の際に生じるシステム停止時間に関する検証項目		✓	✓
	• 製品費用に関する検証項目		✓	✓
	優先度	高	低	例外

「データや記録に基づく評価」に関して、表 6-5 に示すようなデータや記録が考えられる。製品機能・性能をデータや記録に基づいて評価する際、製品ベンダーにより提供される機能や処理能力等を示す数値・検証データを活用する。また、運用性や導入容易性について、客観的に差別化ポイントを評価するために、受賞履歴、特許取得状況、信頼できる第三者による評価を示すインタビュー記事等を参考に、第三者の意見を踏まえた評価を行う。なお、第三者によるインタビュー記事等をデータや記録として用いる場合、当該情報が信頼に足る情報であるかを有識者に確認することが望ましい。

表 6-5　差別化ポイントを示すデータや記録と検証項目大分類との対応

差別化ポイントを示すデータや記録	主に確認可能な検証項目 大分類			客観的 or 主観的	定量的 or 定性的
	製品機能・性能	運用性	導入容易性		
機能・性能・処理能力を示す数値・検証データ	✓			主観的	定量的
特許取得履歴を示す公表ページ	✓			客観的	定量的
受賞した外部の賞の公表ページ	✓			客観的	定量的

差別化ポイントを示すデータや記録	主に確認可能な検証項目 大分類			客観的 or 主観的	定量的 or 定性的
	製品機能・性能	運用性	導入容易性		
信頼できる第三者による評価を示すインタビュー記事		✓	✓	客観的	定性的
信頼できる第三者による評価を示すブログ記事		✓	✓	客観的	定性的

製品ベンダーと協議の上、各検証項目に対する検証方法を決定する。本事業における検証では、応募者と検証者、検証基盤運用主体との間で秘密保持契約の締結を求めないことを必須要件としているため、製品ベンダーが提示可能な範囲でのデータや記録の提示に基づく評価となることに留意が必要である。また、新型コロナウイルス感染症拡大等の影響により、実環境での検証が困難になることも想定される。社会情勢を踏まえ、必要に応じて検証方法の代替案を事前に取り決めておくことが望まれる。

6.4 有効性検証の実施

検証項目・検証方法が決定した後、実際の有効性検証に移る。それに先立ち、運用主体及び検証者にて WBS 等に基づいた検証計画を策定する。検証計画のイメージを図 6-1 に示すが、実際の検証計画ではより詳細にタスクを構造化することに留意が必要である。また、検証に当たって必要となる検証環境を、運用主体及び検証者と製品ベンダーにて協力して準備・構築する。検証環境の準備に関しては、応募者に対して応募要件の必須要件として求めている[8]。そのため、製品選定後に、選定された製品ベンダーと協力して検証環境を構築する。検証項目を構築した後、製品ベンダーによる協力のもと検証者によって実検証を行う。なお、検証の公平性を担保し、専門的な観点から検証を深掘りする目的で、最終的な検証結果だけでなく検証の途中結果に対しても有識者による確認・審議を行う。

[8] 具体的には、「対象製品、付属物、検証用データ、利用環境等、検証に関して検証者が必要とする物品等を無償で提供すること」を求めている。

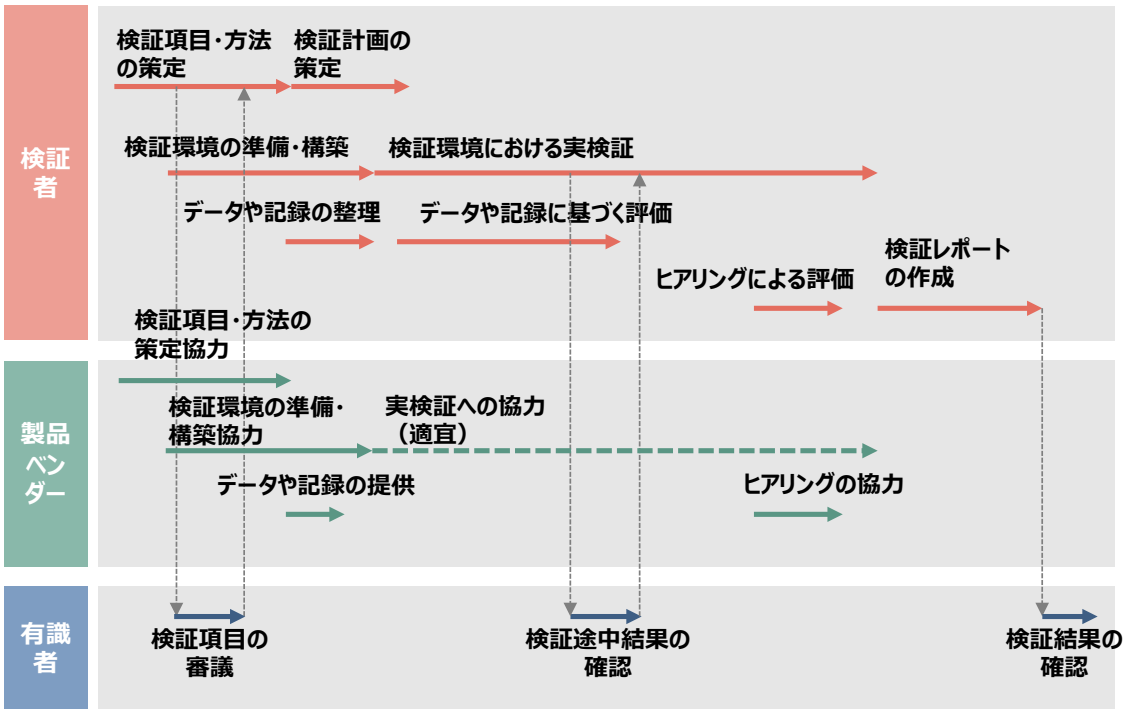


図 6-1　検証計画のイメージ

6.5　検証結果レポートの作成

検証後、検証者において検証結果を取りまとめたレポートを作成する。複数製品における検証で記載項目に差異が生じないよう、検証実施前に検証結果レポートフォーマットを運用主体及び検証者にて策定することが望まれる。レポートフォーマットの構成例を表 6-6 に示す。

表 6-6　検証結果レポートフォーマット例

目次
1. はじめに
2. 対象製品
   2.1 対象製品の概要
   2.2 対象製品の特徴・強み
   2.3 対象製品の適用範囲
3. 検証項目
   3.1 製品機能・性能に関する検証項目
   3.2 運用容易性に関する検証項目
   3.3 導入容易性に関する検証項目
4. 検証環境・検証実施期間
5. 検証結果
   5.1 製品機能・性能に関する検証結果
      5.1.1 検証項目 1-1 に対する検証結果
         ・・・
   5.2 運用性に関する検証結果
      5.2.1 検証項目 2-1 に対する検証結果
         ・・・
   5.3 導入容易性に関する検証結果

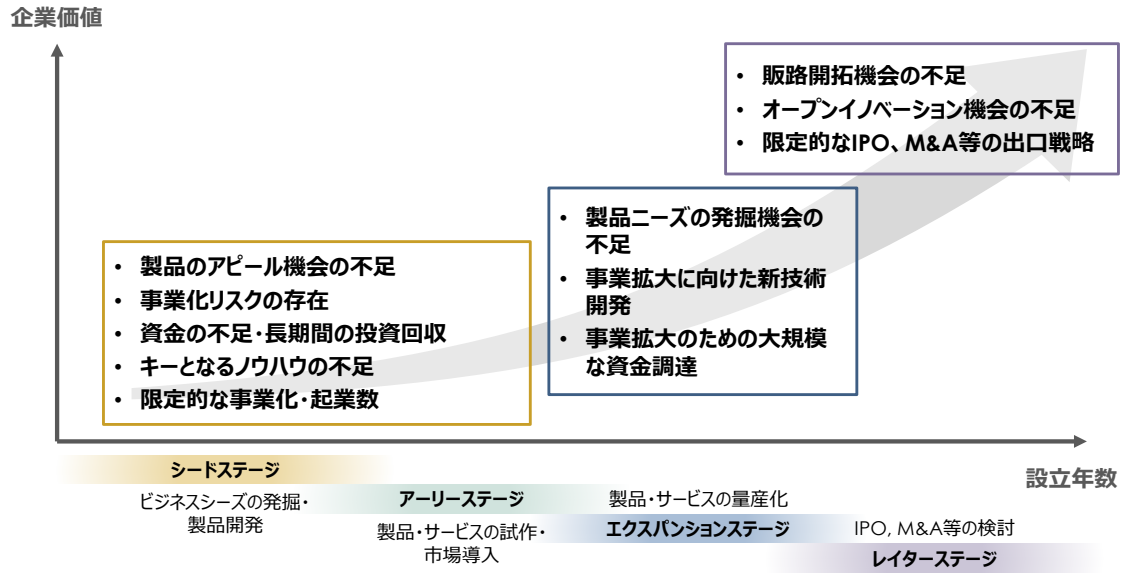
7. エコシステムの検討

昨年度の事業において、サイバーセキュリティ検証基盤で検証したセキュリティ製品に対して十分な市場参入の機会を提供するためには、それを促進する社会の仕組み（エコシステム）が重要であることが確認された。これを踏まえ、今年度の事業においては、日本発のサイバーセキュリティ製品の市場参入を促進する上で効果的なプレイヤーを整理し、本基盤とそれらのプレイヤーからなるエコシステムを検討した。

調査に当たっては、まずセキュリティ製品ベンチャー等における現状の課題と、その課題の解決の方向性（エコシステムが実現すべき機能）を整理した。その上で、実現すべきエコシステムの機能を提供するプレイヤー・役割を整理し、各プレイヤーの関係性を図として整理した。その関係性に基づき、本基盤が提供すべき機能と関係するプレイヤーを整理し、それぞれの機能の提供に向けて解決すべき本基盤の課題を抽出し、抽出した本基盤の課題について、解決の方向性や発展の方向性を検討した。併せて、継続的にエコシステムが自律的に機能するために、本基盤の将来的な民間移管の可能性について検討した。検討・調査に当たっては、エコシステムを構成する役割の担い手になりうる団体・企業等のプレイヤーにヒアリング調査を行った。

7.1 セキュリティベンチャー等における現状の課題と解決の方向性

本事業で検討するエコシステムにおいては、特に日本国内に開発拠点を有するセキュリティベンチャー（スタートアップ、大学発ベンチャー）や中堅のセキュリティベンダー（以降、「セキュリティ製品ベンチャー等」と呼ぶ）を対象にする。セキュリティ製品ベンチャー等が目指す最終的なゴールは様々であるが、本事業では市場参入を行い、国内のユーザー企業へ製品を浸透させることをゴールと想定した検討を行う。一般的にベンチャー企業はシードステージ、アーリーステージ、エクスパンションステージ、レイターステージという4つのステージに分類され、それぞれのステージのベンチャー企業が抱えている課題は異なる。図 7-1 にステージ別のセキュリティ製品ベンチャー等における代表的な課題を示す。ステージを経て企業価値が向上するにつれ、解決すべき課題も変化していく。国内のユーザー企業へ製品を浸透させるためには、まず導入に向けた検討の俎上に乗ることが重要である。そのためには製品の差別化ポイントをユーザー企業へ訴求することが必要であるが、これに際して、シードステージやアーリーステージのセキュリティ製品ベンチャー企業等においては製品のアピール機会が不足していることが課題として考えられる。エクスパンションステージの企業においては、製品・サービスの量産化が進み、ある程度市場認知は進んできたことが想定されるが、製品ニーズを発掘する機会が限定的であることが課題として考えられる。レイターステージにおいては、製品を継続的に販売するための販路開拓の機会が不足していることが挙げられる。



出所）内閣官房「「ベンチャー・チャレンジ 2020」にかかる政府関係機関コンソーシアム及びアドバイザリーボード（第 1 回）事務局説明資料」[9]等に基づき三菱総合研究所作成

図 7-1　セキュリティ製品ベンチャー等におけるステージ別の代表的な課題

ヒアリング調査結果より、成功したセキュリティ製品ベンチャーにおいても同様の課題を抱えたとの意見が得られた。また、一般的なイノベーター理論と同様に、いかにアーリーアダプターを獲得するかが事業展開において重要との意見が得られた。他方で、セキュリティ製品の特性上、アーリーアダプター獲得の障壁が高いとの意見が得られた。特にブルーオーシャンの製品の場合、その製品領域や解決しうる課題（セキュリティ脅威）が認知されていないため、セキュリティをコストとして捉えている企業には認知されず、市場参入に時間を要するとの意見が得られた。

加えて、日本の IT 産業の特性も課題となっていることが挙げられた。前述のとおり、国内のユーザー企業へ製品を浸透させることがセキュリティ製品ベンチャー等における一つのゴールであるが、そのためにはユーザー企業に対して製品を販売する SIer や IT ベンダー、販売会社に製品を取り扱ってもらう必要がある。セキュリティ製品の有効性をユーザー企業だけでなく、SIer や IT ベンダーといった販売企業にも訴求することの重要性が意見された。

セキュリティ製品ベンチャー等が抱える代表的な課題に対して解決の方向性を検討した。この結果を表 7-1 に示す。セキュリティ製品ベンチャー等に対して十分な市場参入の機会を提供するためには、エコシステムの機能としてこれらの課題解決に導く必要がある。

[9] 内閣官房「「ベンチャー・チャレンジ 2020」にかかる政府関係機関コンソーシアム及びアドバイザリーボード（第 1 回）事務局説明資料」
https://www.kantei.go.jp/jp/singi/keizaisaisei/venture_challenge2020/venture_challenge/dai1/siryou1.pdf （2021 年 2 月 5 日閲覧）

表 7-1　セキュリティ製品ベンチャー等の課題に対する解決の方向性

ステージ	ベンチャー等における代表的な課題	課題解決の方向性（＝実現すべきエコシステムの機能）
シードステージ ビジネスシーズの発掘・製品開発 **アーリーステージ** 製品・サービスの試作・市場導入	製品のアピール機会の不足	• 製品の有効性検証の機会創出 • 優れた製品の紹介・周知
	事業化リスクの存在	• 成功したベンチャー等による事業ノウハウの提供 • 企業からの人材・技術の支援
	資金の不足・長期間の投資回収	• 金融支援主体（ベンチャーキャピタル等）による金融支援
	キーとなるノウハウの不足	• 成功したベンチャー等による事業ノウハウの提供
	限定的な事業化・起業数	• 大学、研究開発法人等からの多数の起業
エクスパンションステージ 製品・サービスの量産化	製品ニーズの発掘機会の不足	• 優れた製品の紹介・周知 • マーケティング支援 • 製品の試行導入・評価の機会提供
	事業拡大に向けた新技術開発	• 金融支援主体（ベンチャーキャピタル等）による金融支援 • 企業からの人材・技術の支援 • 製品の有効性検証の機会創出
	事業拡大のための大規模な資金調達	• 金融支援主体（ベンチャーキャピタル等）による金融支援
レイターステージ IPO, M&A 等の検討	販路開拓機会の不足	• ビジネスマッチングの支援 • マーケティング支援 • 優れた製品の紹介・周知
	オープンイノベーション機会の不足	• ユーザー企業とのオープンイノベーション機会の創出
	限定的な IPO、M&A 等の出口戦略	• 多様なエグジット手段の提供

7.2　エコシステムを構成するプレイヤー

前節で示したとおり、セキュリティ製品ベンチャー等が抱える課題に対して、課題解決を導くことがエコシステムに求められる。サイバーセキュリティ検証基盤がすべての課題解決を導くことは現実的に困難であり、民間企業を含むその他のプレイヤーを巻き込んで課題解決を行うことが必要となる。本調査では、表 7-1 で示した実現すべきエコシステムの機能を提供するプレイヤーとして、サイバーセキュリティ検証基盤を含めて 9 つのプレイヤーとして整理し、それぞれの役割を整理した。この結果を表 7-2 に示す

表 7-2　エコシステムの機能を提供するプレイヤー・役割

プレイヤー	役割	実現すべきエコシステムの機能
サイバーセキュリティ検証基盤	• 日本発のセキュリティ製品の公募、選定、有効性検証等を行い、当該製品に対して十分な市場参入の機会を提供する。	• **製品の有効性検証の機会創出** • **優れた製品の紹介・周知** • **製品の試行導入・評価の機会提供** • **製品の有効性を示す技術情報の提供** • **事業ノウハウの抽出・提供**
セキュリティ製品ベンチャー等	• 日本発の優れたセキュリティ製品を開発・販売する。	• ユーザー企業等への製品の販売
金融支援主体（ベンチャーキャピタル、金融機関、エンジェル投資家等）	• セキュリティ製品のベンチャー等に対して金融支援を行う。	• 金融支援
ユーザー企業	• ベンチャー等のセキュリティ製品を試行的に導入し、有効性を評価する。 • ベンチャー等のセキュリティ製品を本格的に導入する。 • オープンイノベーションの機会を提供するとともに、人材や技術の支援を行う。	• 製品の試行導入・評価 • 製品の本格導入 • 製品に対する技術支援・人材支援 • オープンイノベーション機会の創出

プレイヤー	役割	実現すべきエコシステムの機能
SIer、IT ベンダー	• ユーザー企業等とベンチャー等の中間に位置し、優れた製品の販路となる。 • セキュリティ製品をユーザー企業等に導入する。 • セキュリティ製品ベンチャー等に対してマーケティングの支援を行う。	• 優れた製品の紹介 • 取扱い製品の評価 • 製品の試行導入／本格導入支援 • マーケティング支援
政府機関等公的機関	• ベンチャー等のセキュリティ製品を試行的に導入し、有効性を評価する。 • ベンチャー等のセキュリティ製品を本格的に導入する。	• 製品の試行導入・評価 • 製品の本格導入
販売支援主体（業界団体、マーケター等）	• ベンチャー等に対して、ビジネスマッチングの支援を行う。 • ベンチャー等に対して、販売やプロモーションの支援を行う。	• ビジネスマッチングの支援 • 優れた製品の紹介・周知
大学、研究開発法人	• ベンチャー等のセキュリティ製品を試行的に導入し、有効性を評価する。 • ベンチャーが生まれる場にもなりうる。（大学発ベンチャー等）	• 製品の試行導入・評価 • 製品の本格導入 • 起業（産学連携等）
成功したベンチャー等	• 金融支援主体や本基盤に対して事業ノウハウの提供を行う。 • エンジェル投資家や連続的起業により、他のプレイヤーになりうる。	• 事業ノウハウの提供

実現すべきエコシステムの機能を提供するためには、それぞれのプレイヤーが独立して

機能を提供するのではなく、プレイヤー間で相互に連携し、セキュリティ製品ベンチャー等の課題を解決しうる好循環を作り出すことが必要である。各プレイヤーの役割及び実現すべきエコシステムの機能を踏まえたエコシステムの将来像を図 7-2 に示す。なお、この関係性図は第 7.3 節で示すヒアリング調査結果を踏まえて策定したものであり、今後も継続して改訂していくことが望まれる。

セキュリティ製品ベンチャー等が市場参入し、ユーザー企業に対して製品を販売することが一つのゴールとなるが、そのためには IT ベンダーや SIer のような販売会社を販路として確保する必要がある。そこでサイバーセキュリティ検証基盤の役割としては、セキュリティ製品ベンチャー等に対して有効性検証の機会を提供するとともに、検証した結果に基づき製品アピールの機会を提供することが望まれる。製品アピールの機会を提供するに当たっては、業界団体等の販売支援主体とサイバーセキュリティ検証基盤とが共同で製品プロモーションの場を提供することも考えられる。

ユーザー企業や販売会社への製品の有効性の訴求においては、導入実績が重要となる。前述のとおり、ユーザー企業がベンチャー等のセキュリティ製品のアーリーアダプターとなることは障壁が高い。そこでは、政府機関等の公的機関に望まれる役割として、当該セキュリティ企業の製品を試行的に導入することや、ベンチャー等のセキュリティ製品を導入する等の先駆的な取り組みをしているユーザー企業を評価しアーリーアダプターとなるユーザー企業を増やしていく仕組みを作るなどがある。

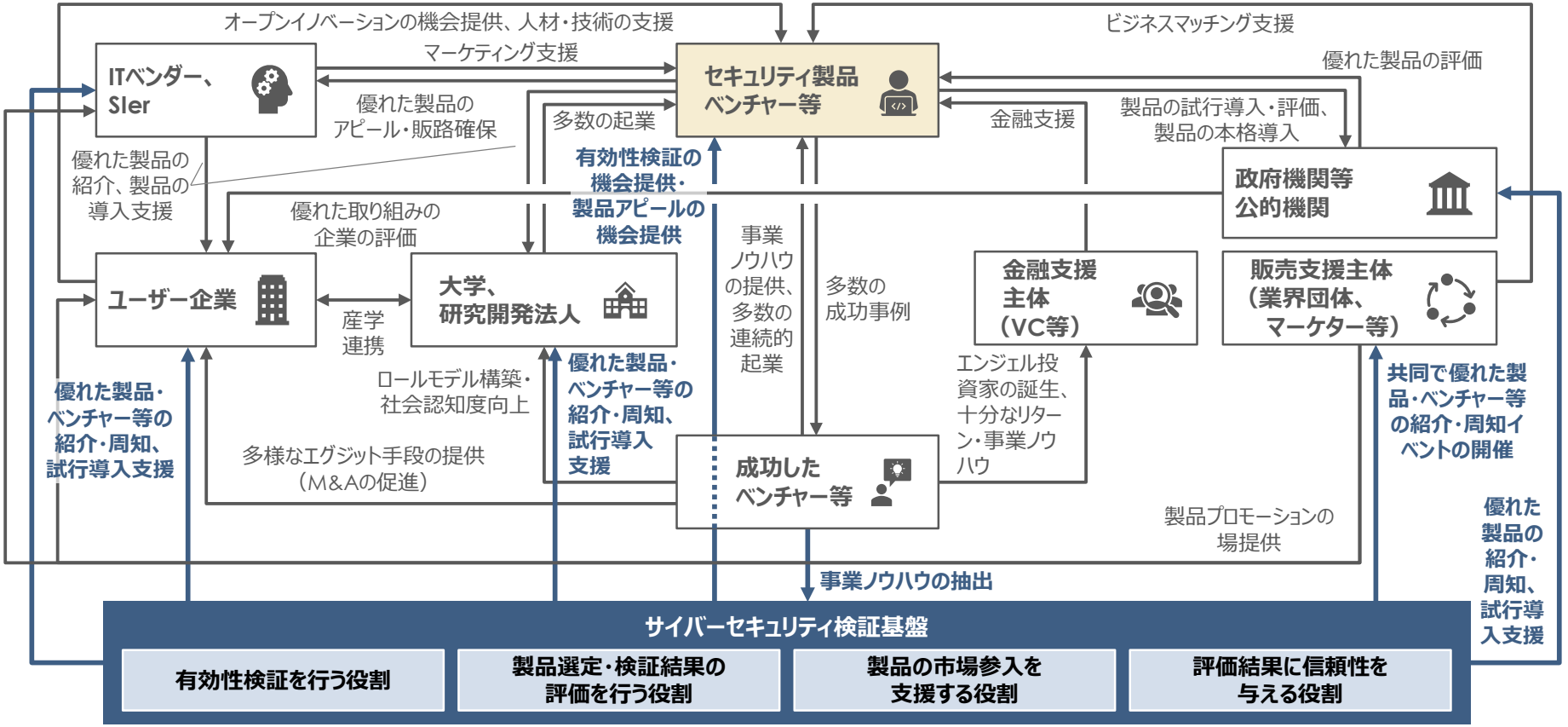
サイバーセキュリティ検証基盤の役割として、「有効性検証を行う役割」、「製品選定・検証結果の評価を行う役割」、「製品の市場参入を支援する役割」、「評価結果に信頼性を与える役割」の 4 つの役割が存在する。

「有効性検証を行う役割」は、セキュリティ製品を検証する環境を構築し、実際の検証を行う役割である。定式化された検証の仕組みに則り、効果的かつ効率的に検証を実施することが望まれる。

「製品選定・検証結果の評価を行う役割」は、有効性検証公募時の製品選定や検証結果を専門的・技術的知見から評価する役割である。製品選定段階では優れたセキュリティ製品を発掘し、検証結果の評価においては、当該製品の差別化ポイントを示す検証結果となっているか、専門的な観点から評価する役割を担う。また、検証対象製品の中から、特に優れた製品をアワードの対象として選定することが望まれる。

「製品の市場参入を支援する役割」は、優れた製品・ベンチャー等を紹介・周知するイベントの開催や、ユーザー企業に対する試行導入支援を行う役割である。製品に関する専門的・技術的観点だけでなく、セキュリティ製品ベンチャー等のビジネス的観点も踏まえた支援を行うことが望まれる。そのためには、成功したベンチャー等と連携し、ベンチャー等の事業ノウハウを抽出・蓄積することが必要となる。

最後の「評価結果に信頼性を与える役割」は、「製品選定・検証結果の評価を行う役割」によって与えられた評価結果やアワードの選定結果の信頼性を担保し、それを公表する役割を担う。



出所）経済産業省「イノベーション・ベンチャー政策について」[10]等に基づき三菱総合研究所作成

図 7-2　参入支援の仕組みを構成するプレイヤー・役割の関係図（将来像）

[10] 経済産業省「イノベーション・ベンチャー政策について」http://www.kantei.go.jp/jp/singi/keizaisaisei/miraitoshikaigi/innovation_dai3/siryou4.pdf （2021 年 2 月 5 日閲覧）

7.3　ヒアリング調査結果概要

エコシステムの構築に向け、エコシステムを構成する役割の担い手になりうる団体・企業等のプレイヤーに対してヒアリングを行った。ヒアリングは、セキュリティ製品ベンチャー等 3 社、IT ベンダー2 社、ユーザー企業 2 社、販売支援主体（業界団体）1 組織、金融支援主体 1 社、成功したベンチャー等 2 社の計 11 社に対して実施した。ヒアリングでは主に以下の観点に対する意見を聴取した。

1. セキュリティ製品ベンチャー等が抱えている課題について
2. ベンチャー製品の市場参入に当たって望まれる政策的支援について
3. セキュリティ製品の有効性周知に当たって望まれる場について
4. ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際の課題について
5. ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際に望まれる支援策について
6. セキュリティ製品ベンチャー等への投資活動における課題や障壁について

以降ではそれぞれの観点に対するヒアリング調査結果の概要を示す。

7.3.1　セキュリティ製品ベンチャー等が抱えている課題に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-3 に示す。セキュリティ製品ベンチャー等が抱えている課題について、特に、IT ベンダーや SIer 等の販売会社に製品を扱って貰うことと、販売会社を介して販路を拡大することに課題を感じているとの意見が得られた。また、製品を担いでいただくためには製品の導入実績が必要となるほか、販売会社に対してのインセンティブが必要となるとの意見が得られた。

表 7-3　セキュリティ製品ベンチャー等が抱えている課題に関する主な回答

ヒアリング先	主な回答
セキュリティ製品ベンチャー　A 社	• IT ベンダーや SIer といった中間業者において、いかに製品を扱って貰うかが課題である。 • このような業者に担いていただくためには、製品導入の実績が必要となる。
セキュリティ製品ベンチャー　B 社	• 開発までは少数精鋭で良いが、売るためには組織力が求められる。販売店に担いでいただくことが重要。 • 製品導入の決定権を持つ人に当社製品によるセキュリティ対策の必要性を納得させることが障壁となっている。

ヒアリング先	主な回答
セキュリティ製品ベンチャー　C 社	• 製品を開発、販売していく中での資金力が課題である。マーケティングに必要なランディングページ作成や広告のための資金が不足している。また、実績不足も課題である。大手のユーザー企業へ営業しても実績が少ないため断られる。 • セキュリティ製品の導入は多くの場合トップダウンで決定する。そのため、直接的にユーザー企業にアプローチするという施策は厳しく、Tier 1 の企業や団体においてセキュリティ施策の重要性を掲げていただく方が効果的ではないか。 • 製品の主な対象である中小企業はそもそもセキュリティ製品に興味が無い。また、中小企業の場合は、セキュリティのリテラシーが低いように感じる。
販売支援主体　H 協会	• ベンチャー企業は、販路機会が無い場合、販路機会をどのように創出するかが課題になる。SIer の大手や独立系などが販路機会創出に協力的・積極的かどうかが論点。 • アーリーアダプターを見つけるには、ベンダーとのマッチングが重要。キャズムを超えるには、SIer や販売店を動かす必要がある。
金融支援主体　I 社	• 海外の企業と比べると、国内のセキュリティ製品ベンチャー企業はターゲット市場を国内に限定している点が異なる。ターゲット市場を英語圏にすると、市場は大きく広がり、入ってくる情報量で大きな差が出てくる。 • 他方で、海外製品と国内製品で技術力の差は小さいと考えている。

ヒアリング先	主な回答
成功したベンチャー等 J社	• コストメリットを武器に市場参入するベンチャーにとっては、圧倒的なコスト優位性をどのように確保するか、どのように人脈を作るかが課題となる。 • 今までに無いコンセプトに基づいて市場参入するベンチャーにとっては、マーケットインが最大の課題であり、マーケット認知が上手くいかないことが、ベンチャーの失敗要因になる。 • SIerとの信頼関係を作って販売チャネルを作ることが障壁になる。販売チャネルを作るためには導入実績が必要となる。イスラエルの有名な製品をSIerが担ぐのは、グローバルでの実績があるためである。 • 製品ベンチャーに対してではなく、製品を担ぐSIer等に対してインセンティブを与えると良いと考える。販売に係る部分を支援することが重要と考える。

7.3.2 ベンチャー製品の市場参入に当たって望まれる政策的支援に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-4 に示す。ベンチャー製品の市場参入に当たって望まれる政策的支援について、製品に対して IPA 等の公的機関からお墨付きを与える仕組みを求める意見が挙げられた。お墨付きの方法として、製品に対するアワードのほか、「IPA 有効性検証基盤の対象機器」等のメッセージでも効果的であるとの意見が得られた。また、セキュリティ製品ベンチャー等が登録できるポータルサイト等を求める意見が挙げられた。加えて、政府機関での製品導入機会は、市場参入や投資活動に良い影響を与えるとの意見が得られた。

表 7-4 ベンチャー製品の市場参入に当たって望まれる政策的支援に関する主な回答

ヒアリング先	主な回答
セキュリティ製品ベンチャー A社	• 国からのお墨付きを頂けた場合、今後の営業活動が進めやすくなる。特に、導入ハードルが高い企業に対しては、国からのお墨付きがあることで営業活動を進めやすくなる。ITリテラシーが高くない人に対しては、IPAという名前があれば話を聞いていただける機会が増えると感じる。 • 有効性検証の対象となった製品について、“IPA推奨”という表現は現実的には難しいが、“IPAの有効性検証対象機器”のような表現でも何らかのメッセージがあると良い。

ヒアリング先	主な回答
セキュリティ製品ベンチャー　B 社	• 当社の製品のような導入実績が少ない場合は、検討の俎上に載ることも難しい。そのため、政府機関等で導入する機会があれば良いと考える。 • 有効性検証の結果は、営業時の大きな武器になる。IPA のような公的機関でないと訴求効果は薄くなると考えられる。
セキュリティ製品ベンチャー　C 社	• セキュリティ製品を導入し、セキュリティ対策を行った場合の税制優遇措置があれば、中小企業も興味を持つようになると考える。 • IPA の有効性検証を受け、公表されることは営業トークとして有効。ユーザー企業への影響でいうと、国によるお墨付きが最も大きいが、世の中に影響力のある大企業が導入した実績も重要である。 • 国の機関として、こういった製品があるというお墨付きをしていただけるとありがたい。 • セキュリティ製品を開発、販売しようとしているベンチャー企業が登録するポータルサイトのような場があると良い。
販売支援主体 H 協会	• アワードを出すとするならば、公的な機関が発行したアワードであることが求められる。公平性の担保にも公的な役割が求められるため、このような役割の民間移管は考えにくい。 • アワードを与える場合、例えば経済産業大臣賞のような賞としての箔を付けることが必要だと考える。 • キャズムをどのように超えるかが課題であり、超えるには、そこを飛び越えやすい政府機関などの公的機関という立場が鍵になるのではと考えている。
成功したベンチャー等 J 社	• 製品の導入事例を生み出したいと考えている。日本の企業は、もっとセキュリティ製品の導入事例を公表して良いのではないかと考えている。 • 製品に付随するシールのようなもので、日本製品であるという担保があると望ましい。そのシールも経済産業省/IPA と記載されているものであって、よく分からない団体のお墨付きでは意味が無い。
成功したベンチャー等 K 社	• ユーザー企業のセキュリティリテラシーを向上させる啓蒙活動のような政策的支援があると良い。

ヒアリング先	主な回答
	• ユーザー企業が製品を試行するための資金の支援があれば、ユーザー企業のリテラシーは向上すると考える。 • 政府が製品を導入しているという事例があれば、投資活動に与えるインパクトは大きい。

7.3.3 セキュリティ製品の有効性周知機会に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-5 に示す。セキュリティ製品の有効性の周知に当たって望まれる機会について、ユーザー企業と製品ベンダーとをマッチングする活動を望む意見が挙げられた。また、ベンチャー等が販路について理解するためのワークショップ等のイベントや、有識者が製品に関する発信を行えるイベント等が有効であるとの意見が挙げられた。イベント等での周知のほか、インターネットメディアへの掲載が効果的であるとの意見が得られた。

表 7-5 セキュリティ製品の有効性周知機会に関する主な回答

ヒアリング先	主な回答
セキュリティ製品ベンチャー A 社	• ユーザー企業と製品ベンダーとをマッチングする活動も重要である。特定のセキュリティ製品（WAF、EDR 等）を必要としている企業が参加する個別の会議やイベントがあると良い。
セキュリティ製品ベンチャー B 社	• 製品を周知するセミナーや、セキュリティ対策の必要性を訴える場を作っていただきたい。
セキュリティ製品ベンチャー C 社	• 当社のターゲットである中小企業は、セキュリティは二の次で展示会にも参加しない。そのような中小企業にどのように周知していくかは課題としており、未だ答えを導けていない。
販売支援主体 H 協会	• 他イベントとタイアップすることは賛成である。例えば、当協会とタイアップして、製品の有効性検証の評価を発表していく等の協力を仰ぐのは良いかもしれない。

ヒアリング先	主な回答
ユーザー企業 I 社 （ベンチャー支援プログラム実施企業）	• 海外へ進出したい国内のセキュリティ製品ベンチャーへの支援として、セールスピッチを行う場を提供すること が考えられる。 • セキュリティ製品ベンチャーに対して、業界へのパイプを支援するのは一つの手段 である。 日本における販路の概要や特徴などを説明する勉強会等のワークショップのようなイベントを開催する のも良い。 • 経営層が目にしやすい、理解しやすい情報を公表する必要がある。経営層が製品の細かな性能や機能を理解するのは困難であり、自社と同じような業界の企業の導入実績が特に重要 ではないか。
成功したベンチャー等 J 社	• 製品の有効性の周知に当たっては、インターネットメディアが圧倒的に有効 だと考える。当社でも様々なマーケット施策は実施したが、Web のメディアが圧倒的である。
成功したベンチャー等　K 社	• 有識者や製品導入企業が参加する座談会のようなイベント があると良いかもしれない。政府がフェアな場を設けると、金融支援主体にとっては出資の判断材料になるかもしれない。有識者が強く発信できるフェアな場 を設けてもらえると良い。

7.3.4　ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際の課題に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-6 に示す。ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際の課題に関して、企業によってベンチャー等の製品を導入することへの課題意識は異なった。共通の意見として、導入時には、ベンチャー企業の製品を選定する根拠や妥当性を示すことが求められるとのことであった。ベンチャー企業の製品であっても、製品自体の価値があれば、コストを要したとしても採用するとの意見が挙げられた。

表 7-6　ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際の課題に関する主な回答

ヒアリング先	主な回答
IT ベンダー　D 社	• セキュリティ製品を担ぐに当たっての判断要素となるのは、「サポート体制」、「技術力」、「市場訴求力」、「当社が付加価値を与えられるか」の 4 点を考慮する。サポート体制を特に重視している。4 点がクリアになればベンチャー等であっても採用することとなる。 • 製品の技術力について、社内で検証環境を用意し検証している。ただ、検証環境では検証できない部分もあるため、実環境で検証することもある。 • 技術力という観点では、国内ベンチャーと海外ベンチャーで大きな差は無いと考えている。
IT ベンダー/ユーザー企業　E 社（アクセラレーションプログラム実施）	• ユーザー企業にとってベンチャー企業の製品は不安であり、特にセキュリティ製品はその考えが顕著だと考える。どのユーザー企業も実績の無い製品を導入することに抵抗がある。 • セキュリティ製品に対する PoC を実施する場合、普通のサービスを導入するくらいのプロセスや工数を掛けて、当社システムに導入して検証する。そのため、多くの製品は PoC を実施する段階で挫折している。 • セキュリティ製品は、特に信頼できる筋からの紹介でないと俎上に上がらない。著名なベンチャーキャピタルが出資している、海外では導入実績があるといった状況でないとアクセラレーションプログラムに採択できないのが現状である。
ユーザー企業　F 社	• 何故ベンチャー企業の製品なのかの説明や製品の技術を証明することが障壁である。この障壁を解決できれば、多少、コストが掛かっても導入することは可能である。 • ベンチャーの製品であっても、他社製品と比べて優位性や新規性が認められれば、コストが掛かったとしても導入している。製品に価値があるかどうかが大事である。 • 当社でのやり方の一つとしては、セキュリティリスクに対して先手の対策を行う会社であると、投資家含めたステークホルダーから評価を得られるというメリットを監査役や経営層へ説明している。

ヒアリング先	主な回答
ユーザー企業 G 社	• ベンチャー企業自体は導入を妨げる障壁とはならない。解決したい課題に対して、その製品が適合するかどうかが重要である。 • ベンチャー企業は、特定の課題に対するソリューションや製品を持っていることがあるほか、対応が丁寧な面もこれまで感じている。 • 社内で購買に係るルールが定められており、ベンチャー企業の製品の採用においても、採用の根拠を社内ガイドラインと照らして確認をすれば、社内の承認は障壁にはならない。

7.3.5　ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際に望まれる支援策に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-7 に示す。ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際に望まれる支援策について、ベンチャー等の製品の導入によるインセンティブが必要との意見が挙げられた。具体的なインセンティブとして、製品を導入した企業を表彰するような取り組みが望ましいとの意見が得られた。また、ユーザー企業が製品を試行導入する際の支援を求める意見が挙げられた。サイバーセキュリティ検証基盤での有効性検証結果は製品導入の判断材料になりえるとの意見が得られた。

表 7-7　ユーザー企業・IT ベンダーがベンチャー等の製品を導入する際に望まれる支援策に関する主な回答

ヒアリング先	主な回答
IT ベンダー D 社	• サイバーセキュリティ検証基盤での有効性検証がビジネス環境での検証結果であれば、当社の取り組みの中での判断材料になりうると考える。 • 仮に有効性検証の機能を自社が担うとしたときに、何の目的で、何をどこまで検証するかというガイドラインを策定することが最大の課題と考える。 • また、検証作業に掛かる費用の出処が気になる。製品ベンダーが支払い、政策としての資金援助があると良いかもしれない。

ヒアリング先	主な回答
IT ベンダー/ユーザー企業 E 社 （アクセラレーションプログラム実施）	• IPA 等の公的機関が製品についてある程度証明してくれるならば、社内プロセスも多少は軽くなる と考える。 • 公的機関がお墨付きを与えてくれるのであれば、導入障壁を下げる要因になるのではないか。 • サイバーセキュリティ検証基盤での検証結果を踏まえ、企業が本来 PoC で検証する範囲の一部を省略 したりすることができれば、当社として楽になると考える。
ユーザー企業 F 社	• 導入することでインセンティブを得られるといったメリットが無いと導入には至らない。市場で成熟していない ベンチャー企業の製品を導入した企業を表彰して、投資への一助とする役割があると良い と考えている。 • 本事業の対象となっているベンチャー企業の製品を導入することで、自社のセキュリティに対する取り組みの評価に直接的に影響することは無い。 • 役員もセキュリティ製品導入を納得するように、本事業がセキュリティ製品導入の後押しになること を望む。具体的な施策として一番分かりやすいのは 税制の優遇 ではないか。
ユーザー企業 G 社	• 当社のブランドイメージ向上に繋がる仕組み があれば良い。例えば、経済産業省が発表している DX 銘柄 は企業間の競争を促進する一つの良い例である。同様の取り組みがセキュリティにおいて存在しないことが疑問である。 • 本事業の検証結果は導入の判断材料になりうる と考えている。検証結果を提示するときに、具体的なユースケースを示すことが有効である。
成功したベンチャー等　K 社	• ユーザー企業が製品を試行するための資金の支援 があれば、ユーザー企業のリテラシーは向上すると考える。

7.3.6　セキュリティ製品ベンチャー等への投資活動における課題や障壁に関するヒアリング調査結果

ヒアリングでの主な回答結果を表 7-8 に示す。セキュリティ製品ベンチャー等への投資活動における課題や障壁について、ベンチャーキャピタル等の金融支援主体はベンチャーの技術力を根本まで理解しておらず、ビジネスの観点に重きを置いた投資活動を行っているとの意見が得られた。すなわち、製品の技術的な有効性検証結果を金融支援主体に提示し

ても、技術力への関心が薄いためその効果は限定的であるとの意見が得られた。また、出資先の製品を導入するユーザー企業を見つけることに課題を感じているとの意見が挙げられた。

表 7-8　セキュリティ製品ベンチャー等への投資活動における課題や障壁に関する主な回答

ヒアリング先	主な回答
ユーザー企業 I 社（ベンチャー支援プログラム実施企業）	• カタログスペックの確認に留まらず、当社で製品を導入して使用することを最低ラインとして投資の判断を行っている。製品の有効性検証結果の情報を公表いただいて出資の判断材料にするという仕組みは良いが、当社としてはいち早く製品を見つけたいという想いがある。 • 出資先の製品を導入するユーザー企業をどのように見つけるかが課題である。多くの企業はセキュリティ製品を導入済みであり、既存製品からの切り替えを促進する営業は困難である。また、セキュリティ製品を導入していない企業の場合は、セキュリティ製品の必要性を疑うことも多く、製品導入に消極的である。
成功したベンチャー等 K 社	• 前提として、金融支援主体は技術力、製品を根本まで理解していないと考えている。そのため、金融支援主体が理解できる内容や表現を確立し、交渉している。 • ビジネスモデルを分解して金融支援主体に説明できれば資金調達が実現できると考える。 • 製品を金融支援主体へアピールするという点では、世の中に無かった製品であるとアピールする方針か、導入事例をアピールする方針が挙げられる。 • 製品有効性の評価は、金融支援主体が出資決定判断の一番の材料にはならないと考える。結局は、その企業が成長するかどうかに基づき投資判断を行っている。

7.4　サイバーセキュリティ検証基盤が提供すべき機能・具体的な施策案

ヒアリング結果に基づき、サイバーセキュリティ検証基盤が実現すべき機能を整理し、各機能を提供するための具体的な施策案を検討した。この結果を表 7-9 に示す。

表 7-9　エコシステム構築に向け検証基盤が提供すべき機能・具体的な施策案

本基盤が実現すべき機能	関係する参入支援の仕組みのプレイヤー	機能の概要	機能提供のための具体的な施策
製品の有効性検証の機会提供	セキュリティ製品ベンチャー等	• 優れた日本発製品を発掘し、その有効性を確認するための機会を提供する。	• 最低限の公平性を担保しつつ、優れたベンチャー企業等の製品を選定し、有効性検証を行う。 • 有効性検証の対象となった製品・製品ベンダーは HP 等で公開する。 • 将来的には、年間を通じて有効性検証の活動を実施する。
製品の有効性の紹介・周知	ユーザー企業、IT ベンダー、SIer、大学、研究発法人、公的機関、販売支援主体（業界団体、マーケター等）	• 検証した製品の有効性や差別化ポイントを紹介・周知する。	• 有効性検証の対象となった製品のうち、特に優れた製品に対してアワードを与える。 • ベンチャー等と販売会社・ユーザー企業を結びつけるためのイベントを開催する。 • 本基盤の取り組みや優れた製品に関する情報を、メディアを介して発信することを検討する。

本基盤が実現すべき機能	関係する参入支援の仕組みのプレイヤー	機能の概要	機能提供のための具体的な施策
製品の試行導入・評価の機会提供	ユーザー企業、IT ベンダー、SIer、大学、研究開発法人、公的機関	• 優れた日本発製品を、実際に企業等において試行導入していただく機会を提供する。	• 「製品の有効性の紹介・周知」の機能と連携し、ユーザー企業・販売会社に対して、製品の有効性を示す情報を提供する。 • また、「試行導入・導入実績公表の手引き」の認知度を向上させる取り組みを行うとともに、手引きに基づき試行導入を行った結果をプラクティスとして共有する。 • 将来的には、優れたユーザー企業の取り組みを評価する仕組みの検討を行う。
事業ノウハウの抽出	成功したベンチャー等	• 成功したベンチャー等から、事業ノウハウや事業の経験を抽出し、その他の機能において活用する。	• 成功したセキュリティベンチャー等と定期的に意見交換を行い、市場参入を促進するに当たって必要となるノウハウを抽出・蓄積する。

（下線の項目はヒアリング調査の結果より優先度が高いと考えられる施策を示す。）

具体的な施策の実施に当たっては、参入支援の仕組みの将来像を念頭に置きつつ、優先度の高い施策からスモールスタートにて順次実施することが望まれる。

7.5 短期的に実施すべき施策案

表 7-9 で示した「機能提供のための具体的な施策」のうち、優先度が高い施策については順次実施することが望まれる。短期的に実施すべき施策として、図 7-3 に示すとおり、大きく分けて 2 つの施策が挙げられる。以降では、それぞれの施策に関する実施概要案を記載する。

① セキュリティ製品ベンチャー等に対する有効性検証の機会提供・結果公表
② セキュリティ製品ベンチャー等に対するアピール機会、販売会社・ユーザー企業とのマッチング機会提供

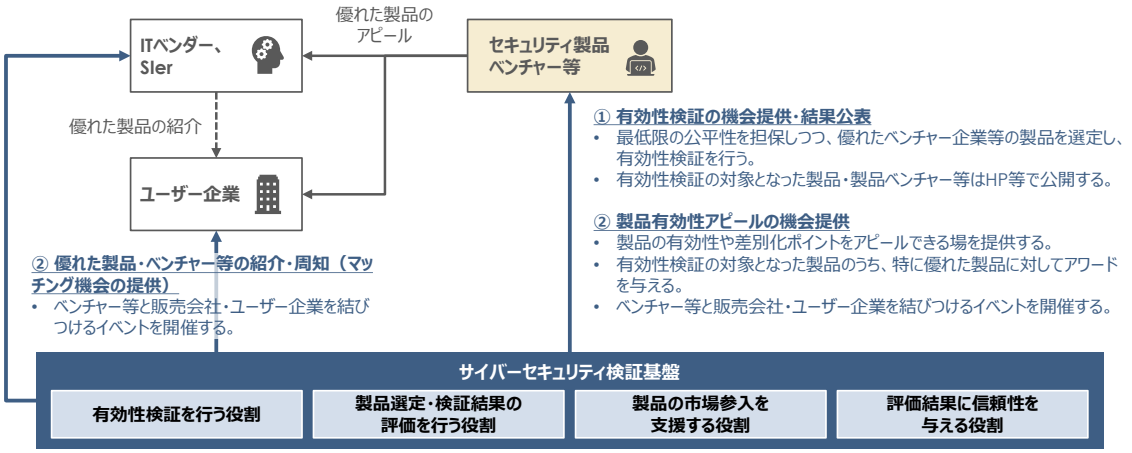


図 7-3　短期的に実施すべき施策の概要

7.5.1　施策案①：有効性検証の機会提供・結果公表

ヒアリング調査により、本基盤による有効性検証の結果がベンチャー企業等の営業時の大きな武器になるとの意見が得られた。また、ユーザー企業へのヒアリングでは、本基盤での有効性検証結果が、製品導入時の検討材料になりえるとの意見が得られた。日本発のサイバーセキュリティ製品の市場参入を促進するために、有効性検証を継続して実施するとともに、ベンチャー等の営業活動や販売会社・ユーザー企業による製品選定活動に活用できるよう、有効性検証結果を効果的に公表することが望まれる。

今後も有効性検証を継続する場合、年度毎の有効性検証結果を HP で公開するのではなく、図 7-4 のように有効性検証の対象となった製品・製品ベンチャー等を一覧として公開し、過去の有効性検証対象製品も確認できるような公開方法とすることが望まれる。

図 7-4　有効性対象製品・ベンダーの HP での公表方法イメージ

また、有効性検証結果を HP で公表するだけでなく、本基盤の活動について広報活動媒体等を用いて周知することも有効である。想定される広報活動媒体について、IPA の IPA News のほか、外部の媒体と連携することも効果的である。このような広報活動媒体に掲載する目的として、その記事を確認した販売会社やユーザー企業が製品ベンチャー等に対して注目するということだけではなく、有効性検証の対象となったベンチャー等が当該記事を営業の素材として使うことも想定される。

7.5.2　施策案②：アピール機会・マッチング機会提供

ヒアリングでは、製品の有効性を周知するイベントや、製品ベンチャー等と販売会社・ユーザー企業とをマッチングするイベントの重要性が意見された。このようなイベントのイメージを図 7-5 に示す。

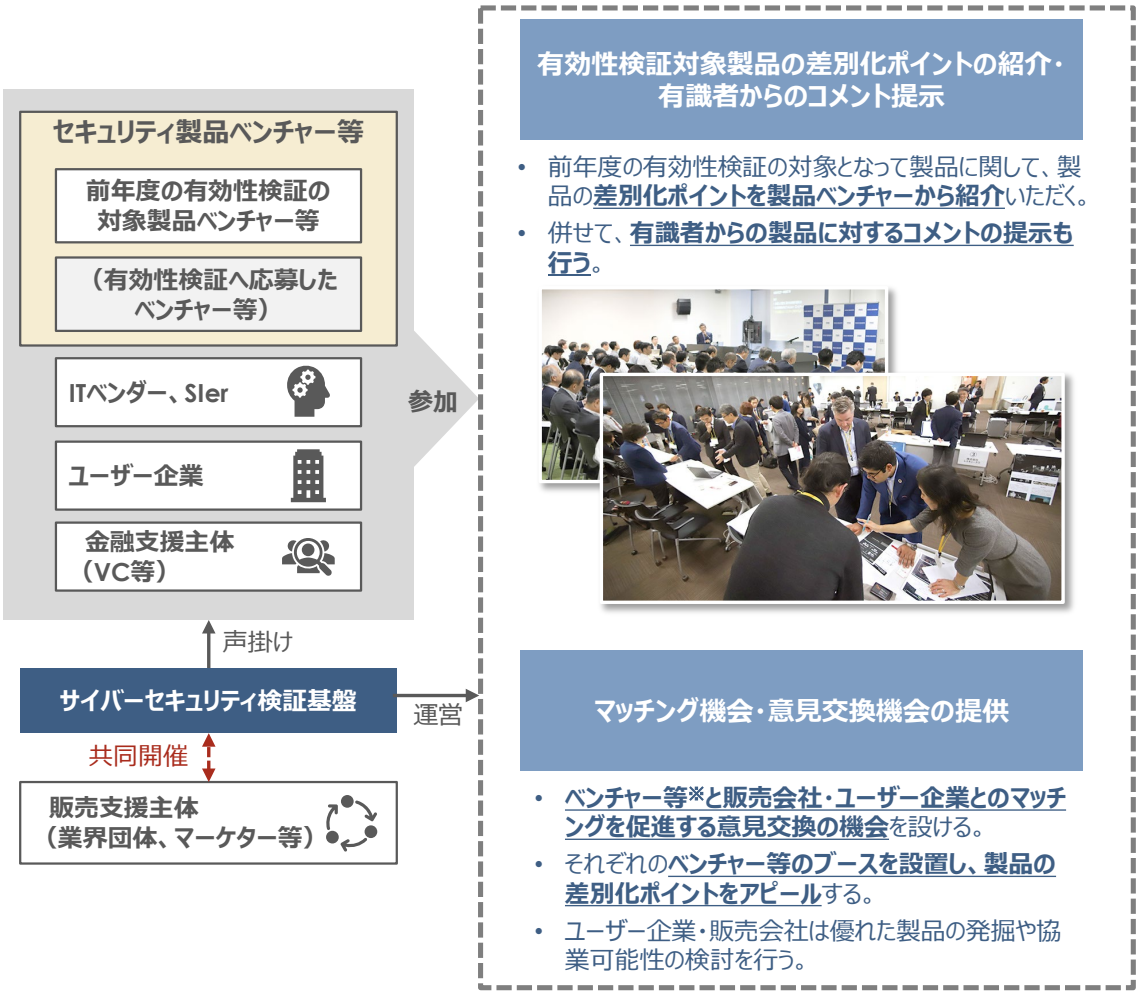
このようなイベントにおいて、2 つのプログラムが想定される。まず前年度の有効性検証の対象となった製品の差別化ポイントを紹介するほか、製品ベンチャーに対する有識者からのコメントの提示を行うことが、製品の市場参入を促進する上で重要となる。次に、イベント内に意見交換・ネットワークの機会を設けることで、ベンチャー等と販売会社・ユーザー企業のマッチングを促進が期待できる。

前者のプログラムにおいて、有効性検証の対象となった製品の差別化ポイントを第三者が紹介する場合、有効性検証の結果を適切に説明することが必要である。「有効性」の意味については更に検討する必要があるが、例えば、検証の結果当該製品の機能や優位点に関する製品ベンダーの主張が間違っていなかったことを説明すること、などが考えられる。後者のプログラムにおいては、前年度の有効性検証の対象となった製品ベンチャー等だけでなく、有効性検証に応募したが落選となったベンチャー等も参加できる方針とすることが考

えられる。

セキュリティ製品ベンチャー等が抱えている課題を踏まえると、イベントの主なスコープは販売会社としつつ、ユーザー企業においても参加いただける形式とすることが望ましい。また、投資先を探しているベンチャーキャピタルや投資会社にも参加いただけるよう間口を広げることが望ましい。本イベントの主目的は対象製品の差別化ポイントをアピールすることであるため、参加者への声かけに当たっては、対象製品の導入先となりうる分野、業種、規模、担当者等に限定して実施することが効果的である。

イベントの開催時期について、有効性検証終了後、間をあけずに実施することが望ましい。また、開催方法について、業界団体との共同開催や業界団体のイベントの一部として実施する等の方向性も考えられる。想定される業界団体として、JNSA や JUAS が挙げられる。有効性検証対象製品の導入先となりうる特定の分野や業種に限定した場合、当該分野の業界団体や ISAC 等と連携することも考えられる。



※ マッチング機会・意見交換機会では、前年度の有効性検証の対象となった製品ベンチャー等だけでなく、有効性検証に応募したが落選となったベンチャー等も参加できる方針とすることが考えられる。

画像出所）未来共創イノベーションネットワーク

図 7-5　アピール機会・マッチング機会イベントのイメージ

7.6　サイバーセキュリティ検証基盤の民間移管に向けた課題

図 7-2 では、参入支援の仕組みを構成するプレイヤー・役割の関係図について、その将来像を示した。このような将来像が自律的かつ継続的に機能し、セキュリティ製品への市場参入機会を提供するためには、本基盤の民間移管も想定する必要がある。図 7-2 及び図 7-6 で示すとおり、サイバーセキュリティ検証基盤には大きく分けて 4 つの役割が存在する。

「有効性検証を行う役割」は、セキュリティ製品を検証する環境を構築して、実際の検証を行う役割である。セキュリティ製品や有効性検証に関する知識を有した IT ベンダー等の民間企業に移管することで、効果的な検証を行うことができると考えられる。「製品選定・検証結果の評価を行う役割」は、製品選定段階では優れたセキュリティ製品を発掘すること、検証結果の評価では製品の差別化ポイントを示す検証結果となっているかを専門的な観点から評価することが必要である。そのため、専門家による有識者会議等によって選定・評価を行うことが望まれる。「製品の市場参入を支援する役割」は、優れた製品・ベンチャー等を紹介・周知するイベントの開催や、ユーザー企業に対する試行導入支援を行う役割である。セキュリティ製品の市場環境を理解するとともに、多くのユーザー企業にアプローチでき

る組織であることが望ましく、セキュリティ製品やユーザー企業に関する業界団体が候補として考えられる。最後に「評価結果に信頼性を与える役割」は、「製品選定・検証結果の評価を行う役割」によって与えられた評価結果の信頼性を担保し、それを公表する役割を担う。この役割について、ヒアリングでは、ベンチャー企業等の製品をユーザー企業や販売会社に訴求するためには、IPA 等の公的機関が検証結果に信頼性を与えることが有効であるとの意見があった。

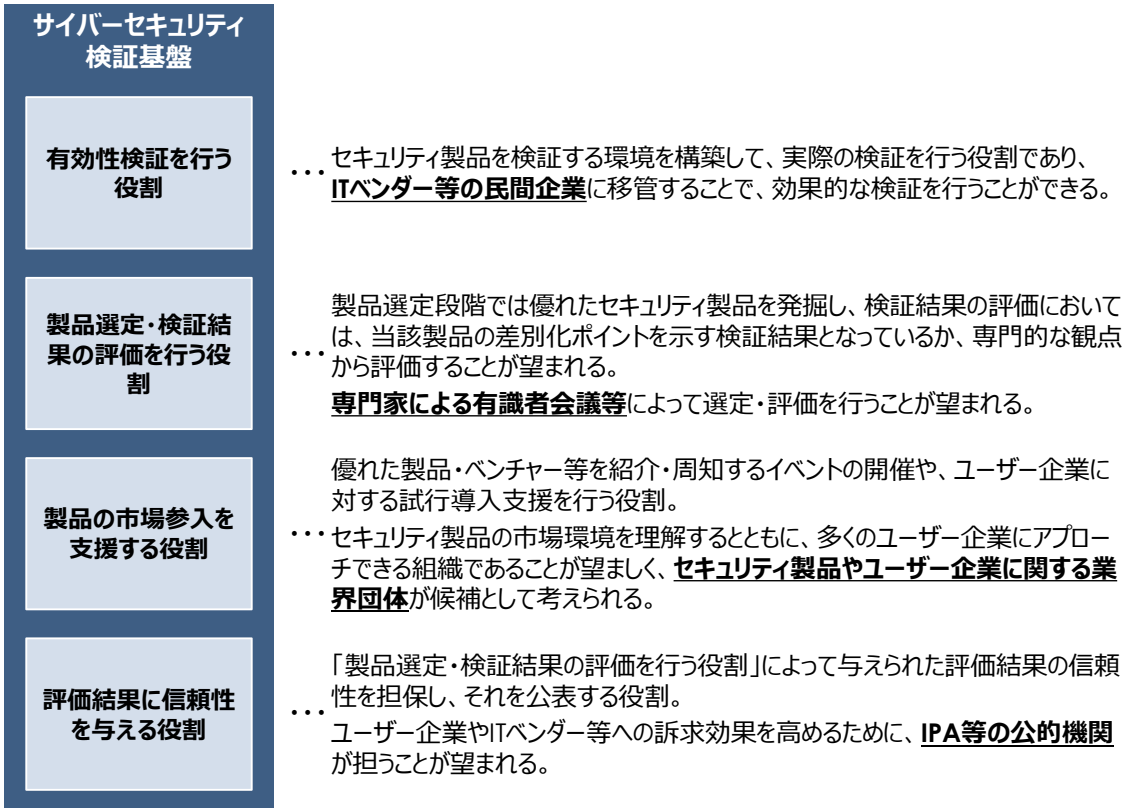


図 7-6　サイバーセキュリティ検証基盤の民間移管の可能性

民間移管における課題として、民間移管先に対するインセンティブの課題が第一に考えられる。「有効性検証を行う役割」の民間移管先として想定される IT ベンダー等に対してヒアリングを行ったところ、特に金銭的なインセンティブの不足に関して懸念が示された。有効性検証のための費用の出処が重要な論点であるが、将来的には、有効性検証を受ける製品ベンダーが支払いつつ、政策としての資金援助が有効であるとの意見がなされた。また、有効性検証のパターン化についても課題があるとの意見が得られた。検証の仕組みがある程度定式化されたとしても、解決するセキュリティ課題や詳細な検証シナリオは製品によって異なるため、複数の製品を同一条件で検証することが困難であるとの意見が得られた。関連して、本基盤における有効性検証の目的や検証の範囲に関するガイドラインを策定することが課題であるとの意見がなされた。

民間移管の可能性や具体的な移管先については、参入支援の仕組みの構築を通じて継続して検討する必要がある。その検討において、民間移管した将来的な参入支援の仕組みにおける資金スキームも検討する必要がある。

8. 19 年度成果「試行導入・導入実績公表の手引き」の改良

昨年度作成した「試行導入・導入実績公表の手引き」を改良した。改良に当たっては、現状の内容で考えられる改良に向けた論点を整理し、有識者へのヒアリングを踏まえ、改良方針を整理し、改良を行った。

8.1 手引き改良の論点

昨年度作成した手引きの内容を確認し、表 8-1 に示すとおり改良に向けた論点を整理した。なお、本事業に当たっては内容に関する論点のみを対象とした。一方、ユーザー企業による試行導入を促進するためには、本手引きの周知方法も検討課題であるため、継続した検討が望まれる。

表 8-1 手引き改良の論点

No.	論点	具体的な内容
1	手引きの対象製品	対象製品が、「ネットワーク上のセキュリティ脅威の可視化に関する製品」に限定されているが、その他の分野や内容を深掘るべきではないか。
2	手引きの想定読者	想定とする読者を、試行導入を検討しているユーザー企業としているが、製品を展開するベンダーも含められるのではないか。
3	製品を展開するベンダー（ベンチャー等）で準備すべき項目等	製品を展開するベンダーが試行導入や導入実績公表を行う際に準備すべき項目等も追記すべきではないか。
4	手引きの活用目的	サイバーセキュリティ検証基盤全体の目的は、優れた日本のセキュリティ製品の市場参入を促進・支援する環境を構築することである。 このことに鑑み、試行導入だけでなく製品の実導入に当たって活用できる手引きであることが望ましいのではないか。
5	導入実績の公表による懸念	導入実績の公表自体がセキュリティリスクに繋がる可能性があるが、この懸念について本文中で記載されていない。
6	導入実績の公表の目的	ユーザー企業が導入実績を公表することの目的が記載されていない。

8.2 ヒアリングの結果概要

手引きの改良に向け、整理した論点に関してユーザー企業に属する有識者にヒアリング

を実施した。ヒアリングでは、上記の論点を踏まえ以下の観点について意見を聴取した。

- セキュリティ製品を選定・導入する際に、製品ベンダーが提示すべき情報や実施すべき事項は何か。（論点 No.3）
- 試行導入を経て実導入するメリットは何か。（論点 No.4）
- 導入実績を公表しても直接的なセキュリティリスクに繋がりにくい製品として、どのような製品が考えられるか。（論点 No.5）

ヒアリングにおける主な回答を表 8-2 に示す。セキュリティ製品を選定・導入するに当たって、製品ベンダーが提示すべき情報や実施すべき事項として、概算見積もりを精緻に算出するために必要な情報の提示や、製品ベンダーの将来展望や戦略に関する説明を求める意見が挙げられた。試行導入を経て実導入を行うメリットとして、既に運用方法を知っていることや社内決裁が容易という点が考えられる。その他考えられるメリットとして、コストや手間の手戻りが生じないという意見がきかれた。また、試行導入時に PoC を入念に実施することで、機能要件、非機能要件、ユーザー利便性等様々な観点を詳細に検証することができ、製品の導入について納得した上で実導入を行えるとの意見が得られた。

論点 No.5 に関して、導入実績の公表自体がセキュリティリスクに繋がりうるセキュリティ製品も想定される。このような製品区分として、サンドボックス、アンチウイルスソフト、Web Application Firewall（WAF）等が挙げられるとの意見があった。このような製品は、サイバー攻撃を直接的に防御する製品であるため、公表する場合でも実名を公表するのではなく「一部上場企業 A 社」のように抽象度を高めた形での公表が望ましい。また、システムアーキテクチャに関する製品や SOC の導入実績など、対策の多くが明らかになるような製品・サービスについては、公表することで対策のレベルが明らかとなるために、基本的には実績公表は望ましくないとの意見が得られた。他方で、攻撃者への牽制になりうる製品は導入実績を積極的に公表すべきとの意見もあった。このような製品の区分として、ネットワーク上のセキュリティ脅威を可視化する製品等、間接的に攻撃を防御する製品が挙げられた。

表 8-2　手引き改良に係る主なヒアリング結果

ヒアリング先	主な回答
ユーザー企業 F 社	・ 製品ベンダーが概算見積もりを精緻に算出するために、ユーザー企業がどのような情報を提示すべきかの情報が欲しい。 ・ 試行導入を経たうえで実導入することのメリットは、コスト、手間の手戻りが無いことである。 ・ 攻撃者への牽制になりうる製品は導入実績を積極的に公表すべきと考える。他方で、公表することがセキュリティリスクに繋がる可能性のあるサンドボックス等の製品は公表しない方が良いと考える。 ・ 導入実績の公表やイベントでの周知に対するベネフィットとして、割引や新しいモジュールの先行利用などを交渉の材料として活用している。

ヒアリング先	主な回答
ユーザー企業 G 社	・ RSA カンファレンスや BlackHat 等のイベントでベンチャー企業がプレゼンテーションするときは、導入部分は製品開発者の想いからはじまる。その意味で、ベンチャー企業からは、「あなたの企業はどのように成長していくか」「製品をどのような想いで開発したか」「どのように市場開拓していきたいか」「市場の成長予測やトレンドをどのように捉えているか」を聞いてみたい。これらの情報は、ベンチャー企業や製品への期待感に繋がる。 ・ 当社では、試行導入としての PoC を入念に実施している。PoC の観点は、機能要件、非機能要件、ユーザー利便性の 3 点である。入念に PoC を実施していることもあり、様々な面で納得した上で実導入している。 ・ 誰に公開するか、及び内容のレベルをどの程度にするかで、リスクに繋がる程度が変わるため、公開の判断基準は異なる。公表については、当社にどのようなメリットがあるか、株主の評価に繋がりうるかについても考える必要がある。 ・ 公表したくない情報は、システムアーキテクチャや機能モデルなどのセキュリティ製品の使い方や仕組みである。公表することで、その会社がセキュリティ対策をどのように実施しているかが判明し、脆弱性に繋がる恐れがある。 ・ 公表することになった場合でも、自社名を明らかにしたうえで「こういうセキュリティ対策を実施している」とする表現は、避けたい場合がある。

8.3 ヒアリング結果を踏まえた手引きの改良

各論点に対して、ヒアリング結果を踏まえ、手引きの改良を行った。主な改良内容を表 8-3 に示す。なお、改良版の手引きは別紙に示す。

表 8-3 手引きの改良内容

No.	論点	改良内容	該当箇所
1	手引きの対象製品	本事業で実施する検証基盤の運用で選定された 2 製品を踏まえ、「ネットワーク上のセキュリティ脅威の可視化に関する製品」の観点を拡充した。	「2.1.2.導入すべき製品・サービスの決定」「2.2.製品試行導入におけるポイント」
2	手引きの想定読者	対象読者として、製品を展開するベンダーも含めた記載とした。	「1.3.手引きの対象読者」

No.	論点	改良内容	該当箇所
3	製品を展開するベンダー（ベンチャー等）が準備すべき項目等	試行導入や導入実績公表に当たって、製品を展開するベンダーが準備すべき情報や実施すべき項目を追加した。	「1.4.手引きの対象製品」 「5.製品ベンダーが準備すべき情報・実施すべき項目」
4	手引きの活用目的	製品の実導入に活用できるような内容を追記した。具体的には、試行導入を経て実導入を行うことのメリットを追記した。	「1.4.手引きの対象製品」 「4.試行導入後の実導入」
5	導入実績の公表による懸念	公表自体がセキュリティリスクに繋がりうる可能性を明示し、その上で、実績を公表することはオプションである旨を追記した。また、公表によるセキュリティリスクは製品の特徴によって異なるため、セキュリティリスクに繋がりにくいセキュリティ製品の例を追記した。	「3.1.1.公開可否判断のポイント」
6	導入実績の公表の目的	導入実績の公表の目的を整理し、追記した。	「1.2 目的」

9. まとめ・考察

本事業では、昨年度の事業の知見・課題を踏まえた上で、公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤について、構築を行った。さらに、本基盤で検証するセキュリティ製品の市場参入を支援する上で有効な、我が国の状況にあったエコシステムの検討を行った。また加えて、昨年度の成果である「試行導入・導入実績公表の手引き」の改良を行った。

9.1 サイバーセキュリティ検証基盤の構築について

検証基盤におけるプロセスを「1. 重要分野選定」、「2. 製品公募」、「3. 製品選定」、「4. 有効性検証」、「5. 検証結果公表」の 5 つと捉え、各プロセスに必要な仕組み（構成要素、手順、実施事項等）の検討を行った。重要分野の選定に当たっては、重要分野マップをベースにセキュリティ脅威の状況、ユーザー企業の状況、セキュリティ技術の変化等を踏まえて必要な見直しを行うこととした。見直し検討に当たっては、セキュリティ製品や脅威動向に関して専門的な知見を有した有識者からの意見を踏まえることが有効であるとした。

製品公募・選定のプロセスにおいては、優れた日本発のセキュリティ製品を中立・公平かつ限られた期間で効率的に公募・選定を行う必要がある。本基盤では、このトレードオフを考慮するために製品及びそのベンダーに課す応募要件を必須要件と追加要件によって構成するものとした。また、製品の選定における審査項目をこの必須要件と追加要件に基づき設定し、効率的かつ客観的に審査を行うこととした。審査は一次審査・二次審査の 2 つに分け、一次審査では応募用紙の記載事項に基づく機械的な審査、二次審査では製品の差別化ポイントに対する専門的な観点からの審査を行うこととした。加えて、応募用紙で表現しきれない差別化ポイントをプレゼンテーション等の機会で抽出することとした。

有効性検証のプロセスに関して、製品個別の検証項目・検証方法の策定の後、実際の検証を行うプロセスとした。それぞれの製品の差別化ポイントによって製品個別の検証項目が異なるものの、効率的に有効性検証を行うために、重要分野に共通して適用される検証項目の大分類を予め設定し、製品選定後に製品個別の検証項目を設定することとした。検証方法について、それぞれの検証項目に対して「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」の 3 つの検証方法にて検証することとした。検証に当たっては、検証の公平性を担保し、専門的な観点から検証を深掘りする目的で、最終的な検証結果だけでなく検証の途中結果に対しても有識者による確認・審議を行うこととした。

検証結果の公表について、有効性検証の対象となった製品・製品ベンダー等を一覧として公開し、過去の有効性検証対象製品も確認できるような公表方法が望ましいとした。また、有効性検証対象ベンダーのアピール機会を提供する施策についても検討を行った。

公平性を確保した効率的な有効性検証の仕組みとするために、現状の検証基盤では有識者の視点から検証項目や検証の途中結果、最終的な検証項目等を確認いただくこととしているが、公平性に係るより精緻な基準に関しては引き続き検討することが必要である。

9.2　エコシステムの検討について

日本発のサイバーセキュリティ製品の市場参入を促進する上で効果的なプレイヤーを整理し、本基盤とそれらのプレイヤーからなるエコシステムを検討した。まずセキュリティ製品ベンチャー等における現状の課題と、その課題の解決の方向性（エコシステムが実現すべき機能）を整理した。その上で、実現すべきエコシステムの機能を提供するプレイヤー・役割を整理し、各プレイヤーの関係性を図として整理した。検討・調査に当たっては、エコシステムを構成する役割の担い手になりうる団体・企業等のプレイヤーにヒアリング調査を行った。

ヒアリング調査の結果、セキュリティ製品ベンチャー等が抱えている課題や市場参入のために望まれる支援が明らかとなった。また、ベンチャー等の製品を担いで販売する IT ベンダーや、製品を導入するユーザー企業が抱えている課題や、導入のために望まれる支援も明らかとなった。このような課題を踏まえ、サイバーセキュリティ検証基盤が提供すべき機能と関係するプレイヤーを整理し、それぞれの機能の提供に向けた施策を整理した。この施策のうち、優先度が高い 2 つの施策をスモールスタート的にはじめるべき施策に位置付け、実施のイメージを整理した。施策②のアピール機会・マッチング機会提供については、実際の開催に向けた要件を今後さらに議論していくことが望まれる。

優先度が高い施策の 2 つは、主にセキュリティ製品ベンチャー等を対象とした施策である。上述のとおり、ベンチャー等の製品を担いで販売する IT ベンダーや、製品を導入するユーザー企業が抱えている課題や望まれる支援も明らかとなったため、今後は、販売会社やユーザー企業に対する施策を具体化することが望まれる。ヒアリング調査では、試行導入を支援する取り組みや、ベンチャー等の製品を採用することのインセンティブを求める意見があった。試行導入の促進に当たっては、「試行導入・導入実績公表の手引き」を活用した取り組みを推進するとともに、政府機関への試行導入を支援する機会等を設けることが期待されている。また、ベンチャー等の製品を採用することのインセンティブについては、優れたユーザー企業の取り組みを評価する仕組みの検討を行うことが望まれる。検討に当たっては、販売会社やユーザー企業の抱える課題をより広範かつ詳細に確認することが必要である。

ヒアリング調査や有識者会議において、セキュリティ製品ベンチャー等の市場参入を支援するための官の役割に関して様々な意見が挙げられた。上述した政府機関における試行導入機会のほか、ベンチャー企業の製品を大企業に紹介する役割を官が担うことについての意見も挙げられた。セキュリティ製品ベンチャー等の市場参入を支援するために望まれる官の役割の検討に当たって、イスラエルのような外国の取り組みを調査することは有効であるとの声があった。また、セキュリティ製品ベンチャー等の参入支援の検討の域を超えるものであるが、ヒアリング調査においては、サイバーセキュリティに関する先進的な取り組みを実施しているユーザー企業を評価する仕組みがあると良いとの意見が得られた。このような仕組みとして、経済産業省が公表している「DX 銘柄」「DX 注目企業 2020」[11]のように、サイバーセキュリティに関する取り組みを積極的に推進している企業を評価し、公表する仕組みについて意見が挙げられた。このような仕組みにおいて、ベンチャー等の製品を積極的に導入している企業を評価することができれば、セキュリティ製品ベンチャー等の

[11] 経済産業省「「DX 銘柄 2020」「DX 注目企業 2020」を選定しました」
https://www.meti.go.jp/press/2020/08/20200825001/20200825001.html （2021 年 2 月 24 日閲覧）

市場参入を促進することができると考えられる。

また、本事業では、継続的にエコシステムが自律的に機能するための、検証基盤の将来的な民間移管の可能性についても検討した。検証基盤の民間移管に当たっては数多くの課題が残存している。特に、民間移管先に対する金銭的なインセンティブに関する課題が存在する。民間移管した将来においては参入支援の仕組みにおける資金スキームも検討する必要がある。

9.3 「試行導入・導入実績公表の手引き」の改良について

昨年度作成した「試行導入・導入実績公表の手引き」を改良した。改良に当たっては、現状の内容で考えられる改良に向けた論点を整理し、有識者へのヒアリングを踏まえ、改良方針を整理し、改良を行った。「試行導入・導入実績公表の手引き」を活用した取り組みとしては、手引きに基づき試行導入を行った結果をプラクティスとして共有する取り組み等が想定される。また、ユーザー企業による試行導入を促進するためには、手引きの周知方法も重要な検討課題である。