2021 年度

サイバーセキュリティ検証基盤の運用

2022 年 3 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（付録 D 及び付録 E を除く）

表　目次（付録 D 及び付録 E を除く）

用語集・略語集（付録 D 及び付録 E を除く）

本報告書では、以下のとおり用語を定義する。

用語	概要
AI	Artificial Intelligence の略。人工知能のこと。
IEC	International Electrotechnical Commission の略。国際電気標準会議のこと。
IP アドレス	インターネットなどのネットワークに接続されたコンピュータや通信機器の一台ごとに割り当てられた識別番号のこと。
ISO	International Organization for Standardization の略。国際標準化機構のこと。
IoT	Internet of Things の略。直訳すると、モノのインターネットという意味であり、コンピュータだけでなくあらゆるモノをインターネットに接続して相互通信すること。
JNSA	日本ネットワークセキュリティ協会のこと。
MITRE ATT&CK	サイバー攻撃の戦術やテクニックなどを、攻撃のライフサイクル別に整理・体系化し、フレームワークとして定義したもの。
NISC	内閣サイバーセキュリティセンターのこと。
OS	Operating System の略で、ソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアのこと。
OSINT	Open Source INTelligence の略。特定の情報要件に対処する目的で、一般に入手可能な情報を収集し、利用し、適切な対象者に適時に普及させた情報のこと。
OWASP	Open Web Application Security Project の略。Web をはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティのこと。 https://owasp.org/
OWASP Benchmark	OWASP が公開している実行可能なオープンソースの Web アプリケーションのこと。意図的に脆弱性が含まれており、あらゆる種類の Web アプリケーション脆弱性検出ツールの公正なテストを目的としている。 https://owasp.org/www-project-benchmark/
OWASP Juice Shop	OWASP が公開している実行可能なオープンソースの Web アプリケーションのこと。意図的に脆弱性が含まれており、SPA で構成されている点が特徴である。 https://owasp.org/www-project-juice-shop/

用語	概要
PCI-DSS	加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱うことを目的として策定された、クレジットカード業界のセキュリティ基準のこと。
R&D	Research and Development の略。企業などで科学研究や技術開発などを行う業務のこと。
RPA	Robotic Process Automation の略。人間がコンピュータを操作して行う作業を、ソフトウェアによる自動的な操作によって代替すること。
SOC	Security Operation Center の略。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のこと。
SaaS	Software as a Service の略。ソフトウェアをサービスとして利用できるようにしたもの。
VC	Venture Capital の略。
Web ブラウザ	Web ページを閲覧するためのアプリケーションソフトのこと。
Whois 情報	ドメインや IP アドレスの所有者の情報のこと。
エンドポイント	通信ネットワークの末端に接続された機器や端末のこと。
シグネチャ	株式会社ゼロゼロワンが独自開発した、IoT 機器の判別パターンのこと。
自動クローリング	自動的に Web サイト等の Web ページを巡回する処理のこと。
セキュリティタグ	株式会社ゼロゼロワンがそれぞれの IoT 機器について公開されている情報を収集し、セキュリティ情報としてシグネチャと関連付けた情報のこと。セキュリティリスクレベルの判定の根拠ともなる。
セキュリティパッチ	ソフトウェアに脆弱性が発見された際に利用者に配布される修正プログラムのこと。
バナー情報	サービスが出力するメッセージの中で、ソフトウェア名称やバージョン情報などに関する情報のこと。
ファームウェア	コンピュータや電子機器などに内蔵されるソフトウェアの一種で、本体内部の回路や装置などの基本的な制御を司る機能を持ったもの。
フォールスネガティブ	検知漏れのこと。
フォールスポジティブ	誤った検知のこと。
ブラックリスト	通信やアクセスを許可しないアドレスなどのリストのこと。
ホワイトリスト	通信やアクセスを許可するアドレスなどのリストのこと。
ポート	同じコンピュータ内で動作する複数のソフトウェアのどれが通信するかを識別するもの。
マルウェア	ユーザの望まない悪さをするプログラムのこと。具体的には、ウイルスやスパイウエアなどの不正プログラムを指す。

1. 概要

1.1 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。この会議の審議の下で、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、本検証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。

ついで 2020 年度はここまでに得られた知見に基づいて、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。またこの基盤を試行的に運用して、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った。加えて、本基盤で検証するセキュリティ製品の市場参入促進に有効な仕組みの検討を行い、また 2019 年度に作成した「試行導入・導入実績公表の手引き」を改良した[3]。

2020 年度の活動を通じて、以下の知見や課題を得ることができた。

(1) 得られた知見

- 三つの役割から成る検証体制の有効性：

  製品の市場参入促進に寄与する検証を現実的な期間・コストで実施することと、検証の公平性・精密さを追及することとは、高いバランスを取って進める必要がある。この実現には、(A)検証実務、(B)検証項目・方法・結果等の妥当性のチェック、(C)これら二つの役割の調整、

[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
[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
[3] IPA「2020 年度 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/shikoukekka2021.html

の三つを独立させる体制が有効であることを確認した。IPA は、中立な公的機関である特性を活かし、調整の役割（C）を担うことができる。

- 市場参入促進の仕組みへの期待：

  市場参入を促進する仕組みとしては、検証結果を市場に発信する機能への期待が高いことが確認された。セキュリティ製品・サービスベンダへのインタビューにて、第三者による検証を受けその結果を市場に発信する場が提供されれば、市場参入前の製品にとって効果的な機会となる、との声が寄せられた。またユーザ企業へのインタビューでは、第三者による客観的な検証結果の情報は製品検討に役立ち、通常は自社で行う PoC[4]の一部を代替しうるとの意見が得られた。

(2) 明らかになった課題

- 本基盤の適用条件の整理：

  検証対象が、競合の激しい分野の製品・サービスの場合は、その強みが、競合他社の製品・サービスとの比較になるケースがある。この場合、強みの公平な検証には比較対象の検証試験も必要となるが、動作環境を統一できない／公平な検証条件が設定しにくい／検証実務の期間・コストが複数製品分増大する等、困難が発生する。本基盤による検証が困難な製品・サービスについては、その特性を整理して検証対象分野や製品・サービスの選定の選定基準に反映する必要がある。

本事業はサイバーセキュリティ検証基盤（以下、検証基盤）に関する三か年目の事業であり、今年度の事業を通じ、上述の知見・課題を踏まえたうえで検証基盤の改良を行い、本基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を行った。さらに、市場参入促進の仕組みの更なる具体化などに取り組んだ。

1.2 実施概要

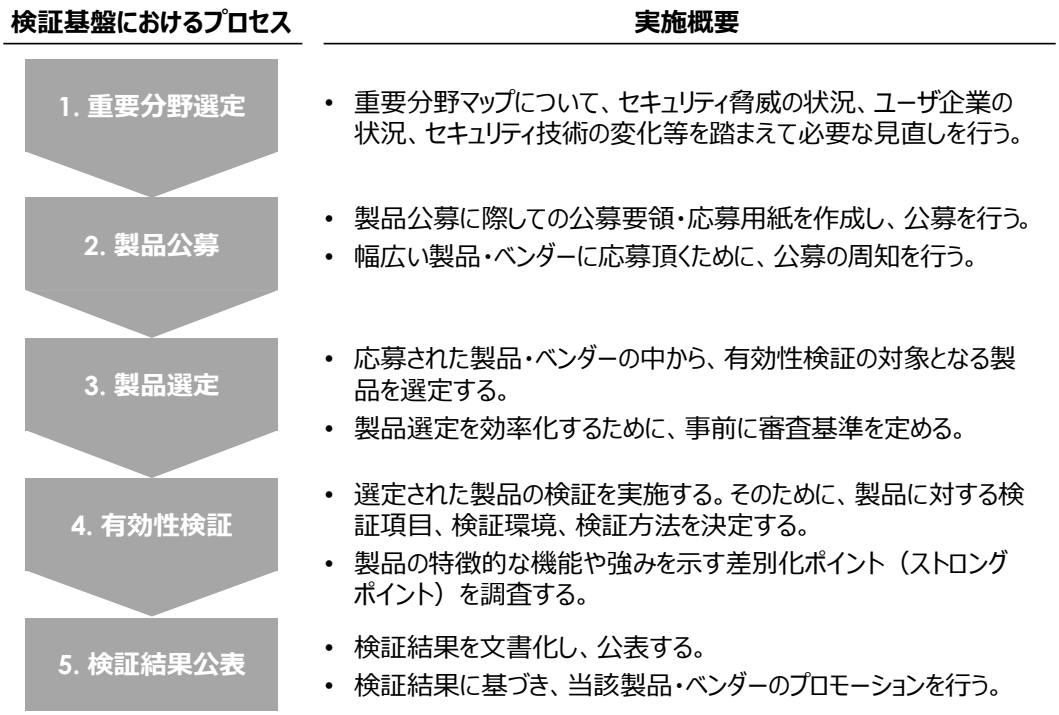
目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

- 有効性検証の実施（本報告書 第 2 章～第 4 章）：

  昨年度構築したサイバーセキュリティ検証基盤の仕組みを基本に必要な改良を施して、有効性検証を実施した。具体的な有効性検証のプロセスを図 1 に示す。このプロセスに示すとおり、まず今年度の検証対象となる重要分野を選定した後、当該分野に該当する製品の公募を実施した。応募のあった製品に対する審査を実施した後、選定された 2 製品に対

[4] Proof of Concept、概念検証。ここでは、製品の正式な導入の前に行う試行導入のこと。

する有効性検証を実施した。選定された 2 製品の有効性検証の結果については、本報告書の付録 D 及び付録 E に示しているとおり、それぞれ報告書として取りまとめた。



出所）IPA「2020 年度サイバーセキュリティ検証基盤の構築に関する報告書」[5]

図 1　有効性検証における検証基盤のプロセス

- 市場参入促進の仕組みの検討（本報告書 第 5 章）：

  検証基盤を含む市場参入促進の仕組みを検討した。昨年度事業において、日本発のサイバーセキュリティ製品の市場参入促進する上で効果的な役割（機能）について検討し、検証基盤とこれらの役割から成る市場参入促進の仕組みについて検討した。今年度事業においては、特に昨年度調査でスタートアップ企業等の要望の多かった、SI 事業者や販社など市場へのチャネル上に居る役割（企業等）とのマッチング機会の創出に焦点を絞り、市場参入促進の仕組みのゴール像を作成した。加えて、ゴール実現までのロードマップ案を作成した。

- 有識者会議の実施支援：

  本事業の実施項目全般について有識者会議に諮り、その意見を反映して実施した。また、第三回以降の有識者会議の運営全般を IPA と連携して行った。各回の開催日時及び議題は

[5] https://www.ipa.go.jp/security/economics/shikoukekka2021.html

以下のとおりである。

表 1　有識者会議の開催概要

回・実施日	議題
第三回 （2022 年 2 月 1 日）	• 製品公募の結果及び製品選定案に関する御報告 • 製品選定に関する討議 • 検証項目・検証方法の策定方針に関する御報告 • 検証項目・検証方法の策定方針に関する討議
第四回 （2022 年 2 月 7 日）	• 個別検証項目・個別検証方法の案に関する御報告 • 個別検証項目・個別検証方法の案に関する討議 • セキュリティ製品ベンチャー等の市場参入促進の仕組み検討に関する御報告 • セキュリティ製品ベンチャー等の市場参入促進の仕組みに関する討議
第五回 （2022 年 2 月 16 日）	• 個別検証項目・検証方針に関する御報告 • 個別検証項目・検証方針に関する討議 • セキュリティ製品ベンチャー等の市場参入促進の仕組み検討に関する御報告 • セキュリティ製品ベンチャー等の市場参入促進の仕組みに関する討議
第六回 （2022 年 3 月 3 日）	• 有効性検証結果に関する御報告 • 有効性検証結果に関する討議 • セキュリティ製品ベンチャー等の市場参入促進の仕組み検討に関する御報告 • セキュリティ製品ベンチャー等の市場参入促進の仕組みに関する討議

2. 重要分野マップの見直し

2.1 重要分野マップ見直し結果

今年度見直された重要分野マップを図 22（付録 A）に示す。セキュリティ脅威の状況やユーザ企業の状況を加味した上で、IPA により重要分野マップの見直しが行われた。有識者の意見を踏まえ、昨年度の重要分野マップに対して、国内外でゼロトラストへの対応が注目を集めていることを踏まえ、「データ保護」及び「ID/アクセス管理」の 2 つの重要分野が追加されることとされた。また、「脆弱性の可視化」という重要分野について、「リスクの可視化・緩和」と修正されることとされた。なお、図 22 の縦軸の組織に対するサイバーセキュリティ脅威について、「情報セキュリティ 10 大脅威 2021」[6]の「組織」の区分で新たに挙げられた脅威に基づき、「テレワーク等のニューノーマルな働き方を狙った攻撃」及び「インターネット上のサービスへの不正ログイン」が追加された。

[6] https://www.ipa.go.jp/security/vuln/10threats2021.html

3. 製品公募・対象製品選定

3.1 製品公募・対象製品選定のプロセス

見直しを行った重要分野マップを踏まえ、今年度の公募の対象分野を決定した。対象分野として、IPA より以下の 4 分野が提案され、有識者の承認を経て決定された。

(1) 脅威の可視化

エンドユーザやシステム管理者などが晒されているセキュリティ上の脅威を可視化することに資する製品。下記の機能等を想定する。

① マルウェアの感染などによる不審な内部通信の発生を捉え、通知する

② 通信フローを監視し、定常時とは異なる状況を検知した場合に通知する

(2) リスクの可視化・緩和

OS、ファームウェア、ソフトウェア等に含まれるリスクを検出し、検出したリスクに対する緩和策の提案や対策の優先度付けを実施することで、リスクの可視化・緩和に資する製品。下記の機能等を想定する。

① 製品を構成しているオープンソースソフトウェア(以下、OSS)に内在する脆弱性の検出とリスク評価を自動で行い、リスクに対する緩和策や対策の優先度を表示する

② 検出されたリスクが内在する OSS を含んだシステム、アプリケーションなどの対策状況を組織単位、ソフトウェア単位などで表示・管理する

(3) データ保護

IT 資産上の様々なデータを、漏えい、改ざん、盗聴等のセキュリティ脅威から保護する製品。下記の機能等を想定している。

① IT 資産上のデータを自動的に暗号化し、保護する

② IT 資産上のデータを自動的にバックアップし、必要な時にバックアップデータを即座に復元する

(4) ID/アクセス管理

IT 資産に対するアクセスに対して、利用者の ID や関連する情報（端末情報、OS、アプリ、バー

ジョン、セキュリティパッチ等）に基づいてその信頼性を判断し、認証する製品。下記の機能等を想定している。

① アクセスした端末の真正性（正当性）を判断し、不正な端末の接続を拒否・通知する

② IT 資産におけるアクセスログや操作ログ等を自動で収集し、動作の正当性を検証する

③ 利用者 ID を登録・修正・削除する

④ 利用者のアクセス権を設定・修正する

⑤ 利用者を認証（認証の支援も含む）する

これらの重要分野に該当する製品を公募・選定するために、表 2 に示すスケジュールで製品の公募・選定を実施した。

表 2　公募・選定の実施スケジュール

プロセス	実施時期	実施概要	実施主体
製品公募	1/11（月）～1/21（金）	製品公募実施、応募受付	IPA・MRI
	1/21（金）17:00 まで	応募締め切り	―
製品審査・選定	1/24（月）～1/25（火）	製品一次審査の実施	IPA・MRI
	1/26（水）～1/31（月）	製品二次審査の実施	有識者
	1/27（水）9:00 まで	ヒアリング対象ベンダに対する質問の事前受付	有識者
	1/27（木）10:00～12:00、13:00～15:00	製品一次審査を通過したベンダに対するヒアリング	一部有識者
	（ヒアリング実施後随時）	ヒアリング録画の共有、ヒアリング議事録の策定・共有	IPA・MRI
	1/31（月）正午まで	製品二次審査の締め切り	有識者
	2/1（火）16:00～18:00 【第三回有識者会議】	製品二次審査結果の御報告、検証対象製品に関する審議・決定	有識者・IPA・MRI

以降では、各プロセスの実施概要について実施内容を説明する。

3.2　製品公募

製品公募では、上記の重要分野に該当するセキュリティ製品について、以下の 2 種類の製品種別（種別 A / 種別 B）を募集した。

[種別 A]

日本の市場において新規性の高いセキュリティに関する機能を有する製品であり、種別 A に応募する応募者は応募書類の中で、上記に該当する機能があることを説明することを求めた。なお、種別 A の製品は、上記に該当する機能が応募書類等の説明内容通りであることを検証する対象である。

[種別 B]

セキュリティ機能に関する優れたユーザビリティを備えた製品であり、種別 B に応募する応募者は応募書類の中で、該当するユーザビリティを明記することを求めた。種別 B の製品は、該当するユーザビリティが応募書類の説明内容通りであることを検証する対象であり、この検証のための導入環境(IT 環境)は、民間事業者等のオフィス等を想定した実環境とする。なお、種別 B の製品が想定するユーザであって、ユーザビリティの検証に協力する者（以降、「検証協力ユーザ」）は、種別 B に応募するセキュリティ製品ベンダが用意することとした。

種別 B の検証では、検証項目・検証方法・検証実務・検証結果等の検討に検証協力ユーザの意見を反映することとし、応募する製品ベンダは、検証協力ユーザから下記の協力について事前に同意を得たうえで応募することとした。

- 種別 B の製品を利用する具体的な業務タスクを想定し、そのタスクで検証したいユーザビリティに関する項目（機能充足性／機能正確性／効率性・運用操作性／習得性／ユーザエラー耐性／その他のユーザビリティの項目）について、意見を出すこと。
- 策定途中の検証項目を確認し、意見を出すこと
- 検証途中の結果等を確認し、意見を出すこと
- 検証結果の公表に際し、公表内容の選択・表現等の調整に協力すること

具体的なユーザビリティ項目に関する概要は以下のとおりであり、応募の際に、応募ベンダが選択（複数選択可）するものとした。

① 機能充足性

設定した業務タスクを実施するために必要なセキュリティ機能が、その製品によってすべて提供されており不足がないこと。それによって、対象製品を用いることで対象ユーザが業務タスクを完了できること。

② 機能正確性

設定した業務タスクを実施する上で、対象製品の提供するセキュリティ機能が正しく（必要な精密さで）動作すること（例：脅威の見逃しや誤検知がないこと）。また、機能の選択、設定、運用が正しくできること。それによって、対象ユーザが正確に業務タスクを実施できること。

③ 効率性・運用操作性

設定した業務タスクを実施するために対象製品の提供するセキュリティ機能を利用することで、ユーザに過度な負担が掛からないこと。例えば十分な自動化、機能の統合、状態の可視化、操作ガイドの呈示、ヘルプデスクへのリンク等が提供されており、対象ユーザが操作に時間を掛けずとも、効率的に業務タスクが実施できること。

④ 習得性

設定した業務タスクを実施するためのセキュリティ機能の操作方法は、理解・習得が容易であること。それによって、対象ユーザがすぐに操作できるようになること。

⑤ ユーザエラー耐性

ユーザのエラー操作（誤操作）に対し耐性があり、例えば、誤操作の可能性を警告する／状態の復旧が容易である／影響を最小限に抑える、などの機能を備えていること。それによって、対象ユーザが誤操作を起こしても、被るロス（時間、業務中断等）が最小限に抑えられること。

⑥ その他のユーザビリティの項目

対象製品は、対象ユーザに上記①～⑤以外の便益を提供すること。

加えて、種別 B の検証について、検証協力ユーザの具体的な業務タスクを設定したうえで、特定のセキュリティ機能について検証することを求めた。また検証は、下記に示すような、「製品の使用環境」と「対象ユーザ」を想定したうえで行うことを求めた。

・製品の使用環境

（例）一般事務部門のオフィス環境／サーバールーム／SOC、など

・対象ユーザ

（例）一般事務部門の社員／IT システム運用部門のオペレータ／SOC 等セキュリティ部門の技術者、など

種別 A 及び種別 B の両方の製品種別の募集について、有識者会議にて選定したキーワードである「ゼロトラスト対応」もしくは「IoT」に関連するものが望ましいと位置づけた。また、本事業の主旨から、商用利用可能な OSS や無償ツール等は応募の対象外とし、既に市販しているものに限定した。また、種別 A と種別 B のいずれも当該製品を他の製品と比較する検証は行わないこととした。

以上の内容について製品公募の際の公募要領及び仕様書に明記し、応募ベンダに求めるとともに、要求内容に関して応募ベンダが記載する応募用紙を作成し、応募ベンダによる記載を求めた。表 2 に示すとおり、製品公募は 2022 年 1 月 11 日（月）から 2022 年 1 月 21 日（金）にかけて実施した。なお、検証の対象とする製品数は種別 A を 1 製品、種別 B を 1 製品とした。

3.3 対象製品の審査・選定

製品公募の結果、計 11 件（種別 A：7 製品、種別 B：4 製品）の応募が寄せられた。応募された製品に対して製品選定のための一次審査・二次審査を実施した。審査のプロセスを図 2 に示す。

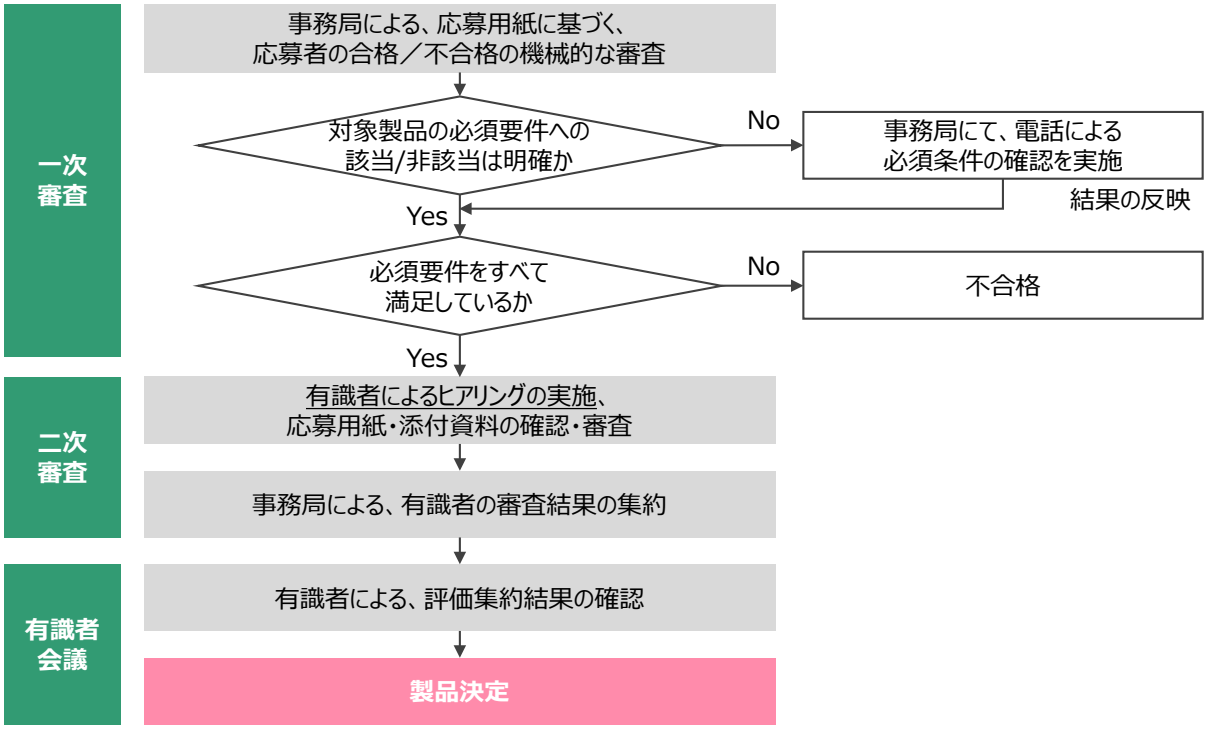


図 2　対象製品の審査・決定プロセス

一次審査及び二次審査における審査項目の概要を図 3 に示す。具体的には、昨年度の事業で構

築した検証基盤の仕組みに従い、募集要件の必須要件及び追加要件に基づき製品の審査項目・審査基準を策定した。必須要件はすべての応募者に必ず求められる要件として位置づけられ、一つでも必須要件を満たしていない場合、不合格とした。必須要件への準拠の確認は一次審査にて実施し、事務局（IPA 及び MRI）にて、機械的に合格・不合格を判断した。一次審査の審査項目及び審査方法を表 3 に示す。一次審査は 2022 年 1 月 24 日（月）から 2022 年 1 月 25 日（火）にかけて実施し、一次審査の結果、応募された 11 製品すべてが一次審査に通過した。

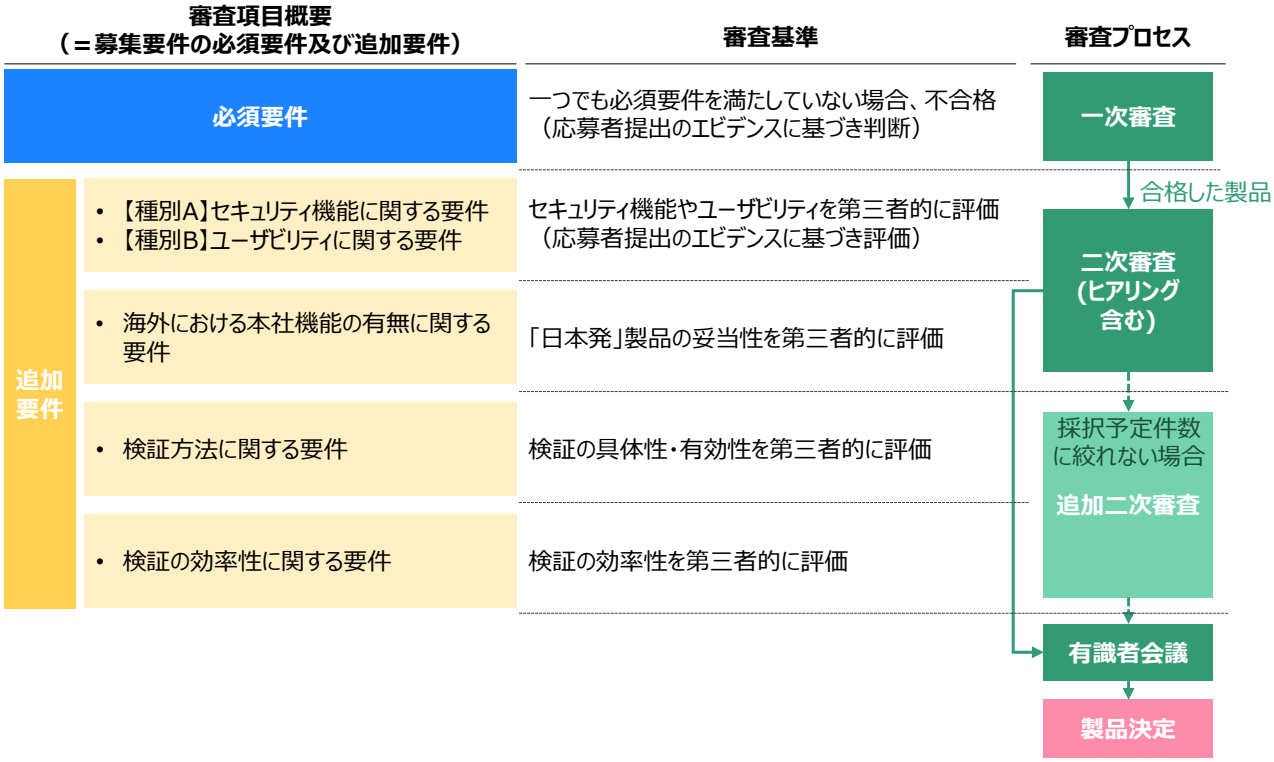


図 3　審査項目・審査基準及び対応する審査プロセスの概要

表 3　一次審査の審査項目・審査方法

区分	審査項目	審査者	審査方法
必須要件	• 応募ベンダは、法人格を有しているか。 • 応募ベンダは、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（あるいは技術開発、製品企画等）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。	IPA・MRI	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。
	• 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(1)～(4)のいずれかに該当するか。 • 応募製品を検証するために考えられる検証項目が記載されているか。 • 【種別Bの製品のみ】応募製品がいずれかの優れたユーザビリティ項目を有するか。		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。
	• 【種別Bの製品のみ】検証協力ユーザを用意し、検証協力ユーザから協力の合意を得ること。また、検証項目・検証方法・検証実務・検証結果等の検討に、検証協力ユーザの意見を反映すること。【種別Bの製品のみ】検証協力ユーザの意見も確認し、検証協力ユーザの利用を想定した業務タスクで検証すること。 • 【種別Bの製品のみ】検証結果のまとめにおいては「手引き」を参照して行うものとし、併せて検証項目の設定等の作業において「手引き」がどの程度有用であったか、意見を出すこと。		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。

一次審査を通過した 11 製品について、応募者が記載した追加要件に基づき二次審査を行った。二次審査では、製品のセキュリティ機能やユーザビリティに関する審査、「日本発」製品であることの判断等を行った。製品のセキュリティ機能やユーザビリティに関して専門的な観点から審査するために、有識者による審査を実施した。二次審査の審査項目及び審査方法を表 4 に示す。二次審査は 2022 年 1 月 26 日（水）から 2022 年 1 月 31 日（月）にかけて実施し、各有識者において、種別 A・種別 B それぞれにおいて検証対象とする 1 製品を選定いただき、有識者の選定結

果を集約し、選定件数が多い製品を検証対象製品候補とした。

表 4　二次審査の審査項目・審査方法

区分	審査項目	審査者	審査方法	
追加要件	【種別Aの製品に関する審査項目】 • 応募者により記載されたセキュリティ機能は、新規性の高いセキュリティ機能であるか。 • 新規性の高いセキュリティ機能を示すエビデンスの内容は十分か。 • 新規性の高いセキュリティ機能を本事業の検証期間（3週間程度）で検証可能か。 • 新規性の高いセキュリティ機能はユーザ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。	有識者がそれぞれ審査・選定、結果集約
	【種別Bの製品に関する審査項目】 • 記載された内容は、想定ユーザ・想定使用環境・想定業務タスクにおいて優れたユーザビリティであるか • 優れたユーザビリティを有していることを示すエビデンスの内容は十分か • 優れたユーザビリティは本事業の検証期間（3週間程度）で検証可能か • 優れたユーザビリティはユーザニーズに応えるものか			
	• 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ではないか。	IPA・MRI・一部有識者	応募者による応募用紙の記載に基づき確認。	IPA・MRI・一部有識者により判断
	• 記載された製品の検証方法は具体的か • 検証方法は製品のセキュリティ機能やユーザメリットを検証するに相応しいものか	検証者	応募者による応募用紙の記載に基づき確認。	**追加二次審査** 検証者にて審査 ↓ 検証対象製品決定
	• 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。	

二次審査の一環として、一次審査を通過した 11 の製品ベンダに対するヒアリングを実施した。ヒアリングは各社 15 分とし、冒頭 5 分で応募用紙記載のポイントを説明いただいた後、残りの 10 分で応募内容に関する質疑応答を実施した。なお、ヒアリングに参加できない有識者もいたところ、事前に質問を受け付けた。また、有識者の二次審査においてヒアリングの結果を活用いただけるよう、ヒアリングの様子は録画するとともに、質疑応答の議事録を作成し、ヒアリング実施後すぐに有識者全員に対して録画データ及び議事録を共有することで、二次審査にヒアリング

の情報を反映できるようにした。

有識者による二次審査の審査結果を集約した結果、種別 A において得票数が高い製品は、株式会社ゼロゼロワンの Karma であった。また、種別 B においては、2 つの製品が同率で最多票であった。有識者会議において決選投票した結果も同率であったため、図 3 の審査プロセスに従い、追加二次審査を実施した。追加二次審査では、検証者である FFRI セキュリティによって検証方法の具体性や検証の効率性に関する確認を行い、その結果、株式会社エーアイセキュリティラボの AeyeScan を検証対象候補として選定した。これら種別 A・種別 B のそれぞれ 1 製品・計 2 製品を今年度の有効性検証の対象とすることを 2022 年 2 月 1 日（火）の有識者会議に諮り、決定した。

3.4 選定された製品の概要

3.4.1 株式会社ゼロゼロワン：Karma（種別 A）

株式会社ゼロゼロワンの Karma は IoT 機器を検索するための検索エンジンであり、ポートや IP アドレス、バナー情報、Whois 情報等を組み合わせることで、日本国内の IoT 機器を検索することが可能である。検索においては日本語を用いることができる点が特徴であるほか、収集した OSINT 情報だけでなく、ゼロゼロワン社が開発するシグネチャを検索内容に含めることで、より詳細な結果を得ることができる。

3.4.2 株式会社エーアイセキュリティラボ：AeyeScan（種別 B）

株式会社エーアイセキュリティラボの AeyeScan は SaaS 型の Web アプリケーション診断プラットフォームである。Web アプリケーションの診断においては「IPA の安全な Web サイトの作り方」のガイドライン等の診断項目を充足しているほか、AI や RPA 技術を活用した自動クローリングによる簡易かつ高精度な脆弱性診断が可能である点が特徴である。

4. 有効性検証

4.1 有効性検証のプロセス

選定された 2 製品に対して有効性検証を実施した。有効性検証のプロセス及び実施スケジュールを表 5 に示す。

表 5 有効性検証の実施スケジュール

プロセス	実施概要	実施時期	実施主体
検証項目マスターリスト・検証方法マスターリストの策定	重要分野に共通して適用される検証項目・検証方法の大分類（マスターリスト）を策定する。	1/12(水)～1/28(金)	MRI・FFRI セキュリティ
製品決定（2/1）			
検証準備	応募者と連携して検証環境に導入し稼働させる準備を行う。種別 B の場合、オフィス等の IT 環境を想定した実環境を準備する。	2/1(火)～2/7(月)	FFRI セキュリティ・応募ベンダ・検証協力ユーザ
個別検証項目案・個別検証方法案の策定	選定された製品のベンダや検証協力ユーザと協議し、製品を効果的に検証できるよう、個別検証項目・個別検証方法をマスターリストから選定する。	2/1(火)～2/4(金)	MRI・FFRI セキュリティ・応募ベンダ・検証協力ユーザ
個別検証項目案・個別検証方法（暫定版）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・個別検証方法の暫定版について審議する。	2/7(月)【第四回有識者会議】	有識者
検証項目・検証方法の確定	有識者会議の結果を踏まえて、検証項目・検証方法を確定する。	2/8(火)～2/10(木)	MRI・FFRI セキュリティ・応募ベンダ・検証協力ユーザ
検証項目・検証方法に基づく検証の実施	確定した検証項目・検証方法に基づき、製品の検証を実施する。	2/8(火)～3/3(木)	MRI・FFRI セキュリティ・応募ベンダ・検証協力ユーザ

検証結果の中間報告	有識者に対して検証結果の中間報告を行い、有識者により検証方針を確認・修正する。	2/16(水)【第五回有識者会議】	有識者・MRI・FFRI セキュリティ
検証結果の最終報告	有識者により検証結果の確認を行う。	3/3(木)【第六回有識者会議】	有識者・MRI・FFRI セキュリティ

4.2 検証項目・検証方法の策定

選定された製品に対する検証は、昨年度構築した検証基盤に基づき、各製品に対する「検証項目」と「検証方法」に基づき実施した。「検証項目」は各製品が有する優れたセキュリティ機能（種別 A）や優れたユーザビリティ項目（種別 B）を確認するための項目であり、それらを確認する具体的な手順・方法として「検証方法」が位置づけられる。具体的な検証項目・検証方法の策定プロセスを図 4 に示す。

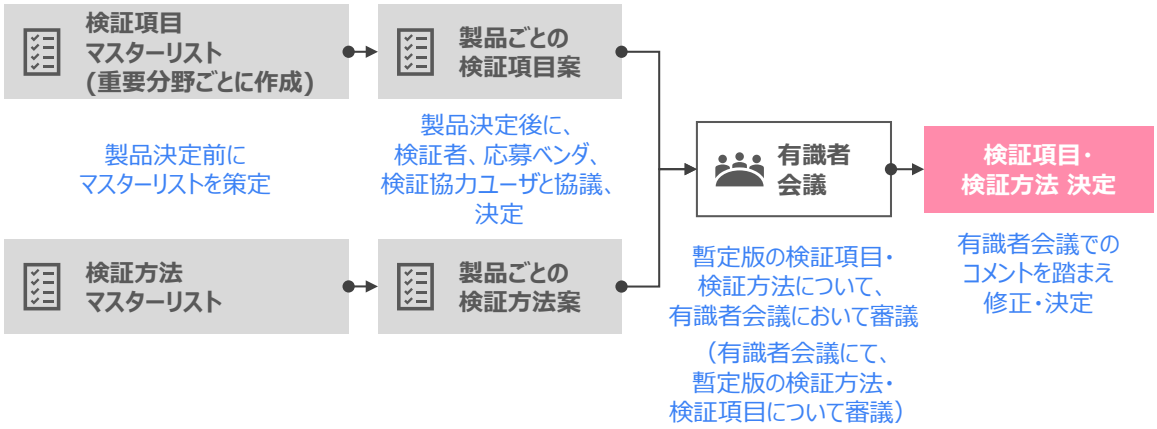


図 4　検証項目・検証方法の策定プロセス

検証項目・検証方法は対象製品ごとに異なるため、実際の策定は製品決定後に実施するものの、検証項目・検証方法の策定期間を可能な限り短縮するために、図 4 に示すとおり、事前に検証項目と検証方法のマスターリストを策定した。検証項目のマスターリストについて、2 つの種別（種別 A・種別 B）と 4 つの重要分野ごとに、計 8 つのマスターリストを策定した。

種別 A の検証項目マスターリストでは、重要分野ごとに、日本の市場において新規性が高いセキュリティに関する機能に係る検証に適用されうる検証項目を含めた。種別 A における重要分野ごとの検証項目マスターリストを表 6 から表 9 に示す。例えば表 6 に示す重要分野「(1) 脅威の可視化」については、様々な脅威を検知・遮断する機能が求められるとともに、検知した脅威

の情報を適切にユーザに通知し、ユーザが適切な対応を取れるよう優先度も含めて脅威を可視化することが求められる。

表 6　【種別 A】「重要分野(1): 脅威の可視化」に関する検証項目マスターリスト

項番	分類	検証項目
1	脅威の検知・対応	検知できる脅威や不正通信の種類に関する検証項目
2		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
3		脅威や不正通信の検知タイミングに関する検証項目
4		検知した脅威や不正通信の遮断に関する検証項目
5	セキュリティルールの管理	ブラックリスト・ホワイトリスト等の設定に関する検証項目
6	検知した脅威の管理・通知	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
7		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
8		検知した脅威情報や不正通信の表示に関する検証項目
9		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
10		脅威や不正通信への対応管理機能に関する検証項目
11	検知仕様	検知仕様に関する検証項目
12	誤検出・検出漏れ	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
13	ガイドライン等への準拠	ガイドラインやフレームワーク（MITRE ATT&CK 等）への準拠に関する検証項目

表 7　【種別 A】「重要分野(2): リスクの可視化・緩和」に関する検証項目マスターリスト

項番	分類	検証項目
1	リスクの検出	検出できるリスクの種類に関する検証項目
2		検出したリスクに関する情報の質・量に関する検証項目
3		古い OSS における脆弱性の検出に関する検証項目
4		依存関係のある OSS の脆弱性の検出に関する検証項目
5		新たな脆弱性が検出できるまでの期間に関する検証項目
6	セキュリティルールの管理	ブラックリスト・ホワイトリスト等の設定に関する検証項目
7	リスクの緩和	検出されたリスクに対する対応に関する検証項目
8		検出したリスクに対する対策の優先度付けに関する検証項目
9	検出したリスクの可視化・管理	検出したリスクの情報の管理に関する検証項目
10		検出したリスクに関する情報の通知に関する検証項目
11		検出したリスクの可視化に関する検証項目
12		検出したリスクへの対応管理機能に関する検証項目
13		ソフトウェア構成情報の取得・管理に関する検証項目
14	検出仕様	検出仕様に関する検証項目

項番	分類	検証項目
15	誤検出・検出漏れ	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

表 8　【種別 A】「重要分野(3): データ保護」に関する検証項目マスターリスト

項番	分類	検証項目
1	データの保護	保護できるデータの種類に関する検証項目
2		保護できるデータの単位に関する検証項目
3		データ保護・復号のタイミングに関する検証項目
4		データ保護の所要時間に関する検証項目
5	保護しているデータの管理	保護されたデータの管理方法に関する検証項目
6		保護されたデータに係る通知に関する検証項目
7		保護されたデータの表示・可視化に関する検証項目
8		保護されたデータの管理機能に関する検証項目
9	データ保護仕様	データ保護仕様に関する検証項目
10	ガイドライン等への準拠	法規制やガイドライン（PCI-DSS 等）への準拠状況に関する検証項目

表 9　【種別 A】「重要分野(4): ID/アクセス管理」に関する検証項目マスターリスト

項番	分類	検証項目
1	アクセス管理	アクセスした端末の正当性の確認に関する検証項目
2		不正アクセスの接続拒否・通知に関する検証項目
3	ID 管理	利用者 ID の登録・修正・削除等の管理に関する検証項目
4		利用者のアクセス権の設定・修正に関する検証項目
5		IT 資産における情報の自動収集に関する検証項目
6	認証	ユーザ認証手段の質・量に関する検証項目
7		認証及び動作正当性検証のタイミングに関する検証項目
8	セキュリティルールの管理	ブラックリスト・ホワイトリスト等の設定に関する検証項目
9	情報管理機能	検出したアクセスの情報の質・量に関する検証項目
10		組織内で使用されている ID・IT 資産の管理・表示に関する検証項目
11		組織内で検出された不正な ID・アクセスの管理・表示に関する検証項目
12		情報の管理方法に関する検証項目
13	仕様	不正なアクセスの検出仕様、動作の正当性判断の仕様に関する検証項目

項番	分類	検証項目
14	誤検出・検出漏れ	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
15	ガイドライン等への準拠	法規制やガイドラインへの準拠状況に関する検証項目

種別 B の検証項目マスターリストは、公募要領で応募ベンダに対して求めた 6 つのユーザビリティ項目に基づき、重要分野ごとに策定した。種別 B における重要分野ごとの検証項目マスターリストを表 10 から表 13 に示す。この検証項目マスターリストは、ユーザビリティに関する国際標準である ISO/IEC 25010:2011[7]や IPA のガイドライン「つながる世界のソフトウェア品質ガイド」[8]に基づき策定した。

表 10　【種別 B】「重要分野(1): 脅威の可視化」に関する検証項目マスターリスト

項番	分類	検証項目
1	① 機能充足性	不審な内部通信の監視・通知に関する検証項目
2		通信フローの監視・検知に関する検証項目
3	② 機能正確性	脅威の見逃しや誤検知に関する検証項目
4		検知した脅威や不正通信の分析漏れ・分析ミスに関する検証項目
5	③ 効率性・運用操作性	脅威や通信フローの監視・検知の自動化に関する検証項目
6		検知した脅威や不正通信の自動分析に関する検証項目
7		脅威の分析結果を踏まえた自動優先度付けに関する検証項目
8		脅威の検知結果、分析結果、優先度付け結果の出力に関する検証項目
9	④ 習得性	製品の操作方法に関する検証項目
10		製品の操作マニュアルやベンダサポートに関する検証項目
11	⑤ ユーザエラー耐性	製品の誤操作への警告に関する検証項目
12		製品利用時の誤操作訂正に関する検証項目
13		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
14	⑥ その他	製品の自動アップデートに関する検証項目
15		導入できる環境や製品リプレースに関する検証項目
16		初期設定の容易性や導入コストに関する検証項目
17		導入の際に生じるシステム停止時間に関する検証項目

[7] Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models

[8] https://www.ipa.go.jp/sec/publish/20150529.html

項番	分類	検証項目
18		他ツールとの相互運用性に関する検証項目
19		耐障害性に関する検証項目
20		導入により生じるシステムへの影響に関する検証項目

表 11　【種別 B】「重要分野(2): リスクの可視化・緩和」に関する検証項目マスターリスト

項番	分類	検証項目
1	① 機能充足性	リスクの検出に関する検証項目
2		検出したリスクの分析・評価に関する検証項目
3		検出したリスクの可視化に関する検証項目
4	② 機能正確性	リスクの見逃しや誤検知に関する検証項目
5		検知したリスクの分析漏れ・分析ミスに関する検証項目
6	③ 効率性・運用操作性	リスクの検知の自動化に関する検証項目
7		リスクの分析・評価の自動化に関する検証項目
8		リスクの可視化の自動化に関する検証項目
9		リスクの分析・評価結果を踏まえた自動優先度付けに関する検証項目
10		リスクの検知結果、分析結果、優先度付け結果の出力に関する検証項目
11	④ 習得性	製品の操作方法に関する検証項目
12		製品の操作マニュアルやベンダサポートに関する検証項目
13	⑤ ユーザエラー耐性	製品の誤操作への警告に関する検証項目
14		製品利用時の誤操作訂正に関する検証項目
15		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
16	⑥ その他	製品の自動アップデートに関する検証項目
17		導入できる環境や製品リプレースに関する検証項目
18		初期設定の容易性や導入コストに関する検証項目
19		導入の際に生じるシステム停止時間に関する検証項目
20		他ツールとの相互運用性に関する検証項目
21		耐障害性に関する検証項目
22		導入により生じるシステムへの影響に関する検証項目

表 12　【種別 B】「重要分野(3): データ保護」に関する検証項目マスターリスト

項番	分類	検証項目
1	① 機能充足性	データの保護・暗号化に関する検証項目
2		保護したデータに対する必要時の復元に関する検証項目

項番	分類	検証項目
3	② 機能正確性	IT 資産が動作している際のデータ保護に関する検証項目
4		保護されたデータの管理に関する検証項目
5	③ 効率性・運用操作性	データの保護・暗号化の自動化に関する検証項目
6		保護したデータの復元の自動化に関する検証項目
7		保護されたデータに関する自動通知に関する検証項目
8	④ 習得性	製品の操作方法に関する検証項目
9		製品の操作マニュアルやベンダサポートに関する検証項目
10	⑤ ユーザエラー耐性	製品の誤操作への警告に関する検証項目
11		製品利用時の誤操作訂正に関する検証項目
12		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
13	⑥ その他	製品の自動アップデートに関する検証項目
14		導入できる環境や製品リプレースに関する検証項目
15		初期設定の容易性や導入コストに関する検証項目
16		導入の際に生じるシステム停止時間に関する検証項目
17		他ツールとの相互運用性に関する検証項目
18		耐障害性に関する検証項目
19		導入により生じるシステムへの影響に関する検証項目

表 13　【種別 B】「重要分野(4): ID/アクセス管理」に関する検証項目マスターリスト

項番	分類	検証項目
1	① 機能充足性	アクセスした端末や IT 資産の動作の正当性検証に関する検証項目
2		不正な端末の接続拒否・通知に関する検証項目
3		IT 資産におけるアクセスログや操作ログ等の収集に関する検証項目
4		利用者 ID の登録・修正・削除等の管理に関する検証項目
5		利用者のアクセス権の設定・修正に関する検証項目
6	② 機能正確性	不正端末やアクセスの見逃しや誤検知に関する検証項目
7	③ 効率性・運用操作性	端末や IT 資産の正当性検証の自動化に関する検証項目
8		不正端末の接続拒否・通知の自動化に関する検証項目
9		ログの自動収集・自動分析に関する検証項目
10		利用者 ID やアクセス権の自動管理に関する検証項目
11		端末の検知結果、ログの収集・分析結果の出力に関する検証項目
12	④ 習得性	製品の操作方法に関する検証項目
13		製品の操作マニュアルやベンダサポートに関する検証項目

項番	分類	検証項目
14	⑤ ユーザエラー耐性	製品の誤操作への警告に関する検証項目
15		製品利用時の誤操作訂正に関する検証項目
16		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
17	⑥ その他	製品の自動アップデートに関する検証項目
18		導入できる環境や製品リプレースに関する検証項目
19		初期設定の容易性や導入コストに関する検証項目
20		導入の際に生じるシステム停止時間に関する検証項目
21		他ツールとの相互運用性に関する検証項目
22		耐障害性に関する検証項目
23		導入により生じるシステムへの影響に関する検証項目

検証方法のマスターリストについては、すべての種別・重要分野共通のリストとして策定した。策定した検証方法マスターリストを表 14 に示す。種別 A の検証実施にあたって、可能な限り検証環境での実検証を優先とし、客観性が損なわれる可能性があるヒアリングに基づく評価は、実検証やデータや記録に基づく評価が困難な場合の例外的措置として位置づけた。他方、種別 B の検証においても可能な限り検証環境での実検証を重視するが、種別 B では優れたユーザビリティ項目に対する検証が求められるところ、検証協力ユーザに対するヒアリングを実施することとした。また、種別 B では、検証結果のまとめは 2019 年度事業で策定し 2020 年度事業で改良した「手引き」を参照して行うものとし、検証方法マスターリストにも当該検証に係る内容を含めた。

表 **14**　検証方法マスターリスト

分類	**検証方法**	
	種別 A	**種別 B**
検証準備	検証実施に向けた役割分担の整理（種別 A・B 共通）	
	検証に用いる検証環境の設定（種別 A・B 共通）	
	検証環境に対する製品のインストール・設定（種別 A・B 共通）	
	検証に必要なデータの設定（種別 A・B 共通）	
	検証実施スケジュールの策定（種別 A・B 共通）	
	検証項目・検証方法の策定（種別 A・B 共通）	
検証実施	検証環境での実検証　《**優先度：高**》	検証環境での実検証　《**優先度：高**》

分類	検証方法	
	種別 A	**種別 B**
	データや記録に基づく評価　**《優先度：低》**	検証協力ユーザに対するヒアリングに基づく評価　**《優先度：中》**
	ベンダに対するヒアリングに基づく評価　**《優先度：例外》**	データや記録に基づく評価　**《優先度：低》**
	―	ベンダに対するヒアリングに基づく評価　**《優先度：例外》**
検証結果のまとめ	検証結果報告書の作成（種別 A・B 共通）	
	―	「手引き」の評価

4.2.1　Karma（種別 A）の検証項目・検証方法の概要

検証対象製品が決定次第、検証者及び応募ベンダと協議し当該製品の機能や特性を踏まえたうえで、マスターリストの項目を具体化し、個別製品ごとの検証項目及び検証方法を策定した。今回選定された Karma 及び AeyeScan はいずれも「重要分野(2): リスクの可視化・緩和」であるため、表 7 及び表 11 に基づきそれぞれ検証項目を策定した。

種別 A である Karma について、特に重要な検証項目を一部抜粋したものを表 15 に示す。全体版は付録 B を参照のこと。

表 15　Karma において新規性の高いセキュリティに関する機能・検証項目（抜粋版）

検証項目（抜粋）				**新規性の高いセキュリティに関する機能**		
分類	**No.**	**区分**	**検証項目**	**IoT 機器の正しい情報を検出できること**	**セキュリティリスクのある IoT 機器を検出できること**	**日本語検索が可能であること**
リスクの検出	1-1	リスクの検出	IoT 機器の正しい情報を検出できること	✓		
	1-2		セキュリティリスクのある IoT 機器を検出できること		✓	

	1-3		日本語の文字列を含んだ検索ができること			✓
	1-4		インターネット経由で IoT 機器の検出ができること	✓	✓	✓
	1-5		条件を絞り込んだ検索ができること	✓	✓	✓

各検証項目に対して、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダヒアリングに基づく評価」の 3 つの方法のうち、どの方法で検証を行うか決定した。決定した検証方法のうち、表 15 で示した検証項目に対する検証方法について一部抜粋したものを表 16 に示す。全体版は付録 B を参照のこと。

表 16　Karma の検証項目に対する検証方法（抜粋版）

検証項目（抜粋）				**検証方法**		
分類	**No.**	**区分**	**検証項目**	**検証環境での実検証**	**データや記録に基づく評価**	**ベンダヒアリングに基づく評価**
リスクの検出	1-1	リスクの検出	IoT 機器の正しい情報を検出できること	✓	✓	
	1-2		セキュリティリスクのある IoT 機器を検出できること	✓	✓	
	1-3		日本語の文字列を含んだ検索ができること	✓		
	1-4		インターネット経由で IoT 機器の検出ができること	✓		
	1-5		条件を絞り込んだ検索ができること	✓		

4.2.2　AeyeScan（種別 B）の検証項目・検証方法の概要

種別 B である AeyeScan について、特に重要な検証項目を一部抜粋したものを表 17 に示す。全体版は付録 C を参照のこと。

表 17　AeyeScan におけるセキュリティ機能に関するユーザビリティ項目・検証項目（抜粋版）

検証項目（抜粋）				セキュリティ機能に関するユーザビリティ項目			
分類	No.	区分	検証項目	① 機能充足性：AI,RPA 技術を活用した自動クローリング能力	② 機能正確性：画面クローリング性能（範囲、深度）	③ 効率性・運用操作性：脆弱性の検出箇所を視覚的に分かりやすくレポート	④ 習得性：設定項目が少なく、操作が容易
機能充足性	1-1	監視、検知、通知	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性項目が対象に含まれていること	✓			
	1-3	自動分析	AI によるフォーム自動入力値が正しいこと	✓			
機能正確性	2-1	検知の正確性	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性が検出されること		✓		
	2-2		自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していること		✓		
効率性・運用操作性	3-1	レポーティング	脆弱性の検出箇所を視覚的に分かりやすくレポートできること			✓	

検証項目（抜粋）				セキュリティ機能に関するユーザビリティ項目			
分類	No.	区分	検証項目	① 機能充足性：AI,RPA 技術を活用した自動クローリング能力	② 機能正確性：画面クローリング性能（範囲、深度）	③ 効率性・運用操作性：脆弱性の検出箇所を視覚的に分かりやすくレポート	④ 習得性：設定項目が少なく、操作が容易
習得性	4-1	習得性	初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していること				✓

各検証項目に対して、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダヒアリングに基づく評価」の 3 つの方法のうち、どの方法で検証を行うか決定した。決定した検証方法のうち、表 17 で示した検証項目に対する検証方法について一部抜粋したものを表 18 に示す。全体版は付録 C を参照のこと。

表 18　AeyeScan の検証項目に対する検証方法（抜粋版）

検証項目（抜粋）				検証方法			
分類	No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
機能充足性	1-1	監視、検知、通知	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性項目が対象に含まれていること	✓		✓	

検証項目（抜粋）				検証方法			
分類	No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
	1-3	自動分析	AI によるフォーム自動入力値が正しいこと	✓			
機能正確性	2-1	検知の正確性	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性が検出されること	✓		✓	
	2-2		自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していること	✓			
効率性・運用操作性	3-1	レポーティング	脆弱性の検出箇所を視覚的に分かりやすくレポートできること	✓	✓		
習得性	4-1	習得性	初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していること	✓	✓		

4.3 検証に向けた準備

4.3.1 Karma（種別 A）の検証に向けた準備

Karma の検証環境は(1) インターネット上に公開されている IoT 機器を検索するための検証環境及び(2)検証実施者が調達した IoT 機器を検索するための検証環境の 2 環境を構築した。環境(1)では、Karma を利用して検索機能や結果表示に関する検証を実施した。環境(2)では、上述の環境(1)では実施困難な正確性の検証(検索結果と実際の IoT 機器との照合)を補完的に実施した。

(1)　インターネット上に公開されている IoT 機器を検索するための検証環境

図 5 で示すとおり、社内ネットワークに検証用 PC を用意し、Web ブラウザからインターネット経由で Karma を利用する環境を構築した。

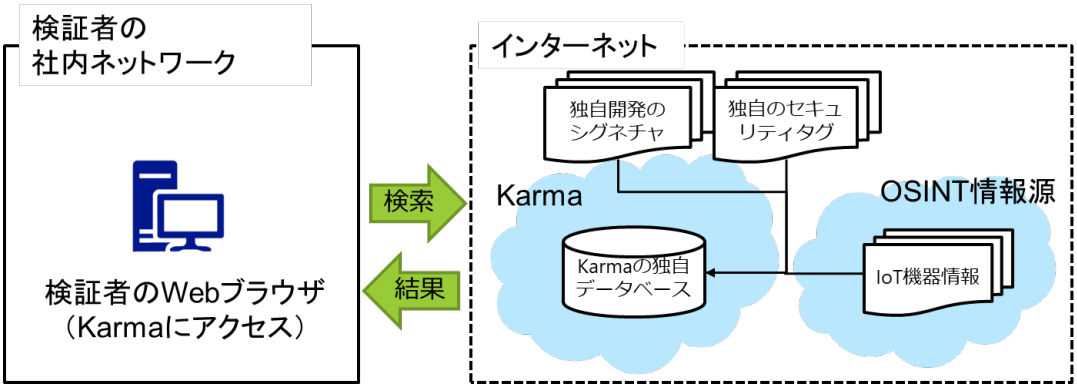


図 5　インターネット上に公開されている IoT 機器を検索するための Karma 検証環境

Karma の利用にあたって、製品ベンダからアカウント情報の提供を受け、Web ブラウザ上の検索画面から IoT 機器の検索を実行した。

これにより、インターネット上の IoT 機器情報が検索できることを、検索ヒット件数等から確認した。

(2)　検証実施者が調達した IoT 機器を検索するための検証環境

図 6 のイメージで示すとおり、社内ネットワークに検証実施者が調達した IoT 機器を設置し、直接収集したバナー情報から Karma のシグネチャ・セキュリティタグで検索する環境を構築した。

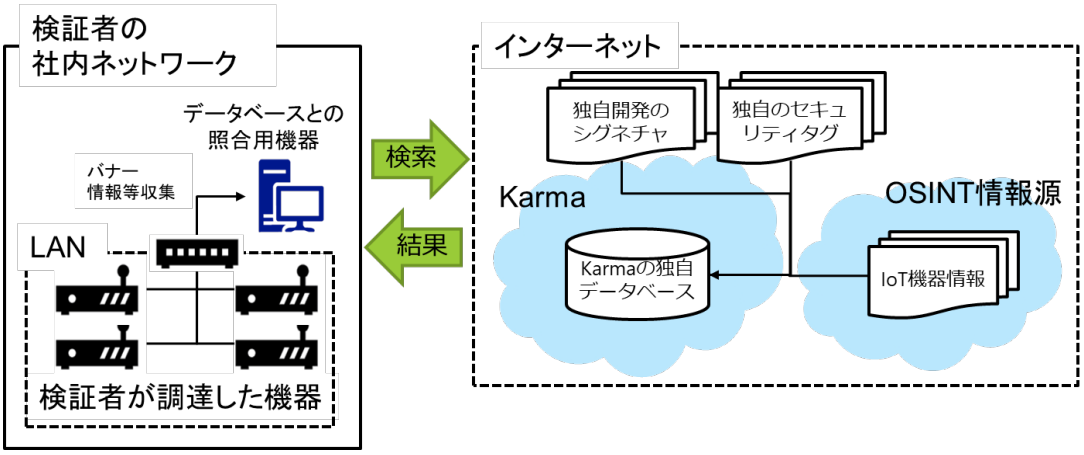


図 6　検証実施者が調達した IoT 機器を検索するための Karma 検証環境のイメージ

これにより、Karma 独自のシグネチャ及びセキュリティタグの正当性を IoT 機器個別に確認した。

4.3.2　AeyeScan（種別 B）の検証に向けた準備

以下の 3 つの検証用 Web サイトを AWS 上に構築した。

- 検証用 Web サイト①：OWASP Benchmark を稼働させた Web サイト
- 検証用 Web サイト②：日本語入力フォーム画面を含む自作の Web サイト
- 検証用 Web サイト③：OWASP Juice Shop を稼働させた Web サイト

図 7　AeyeScan 検証用 Web サイト①画面イメージ

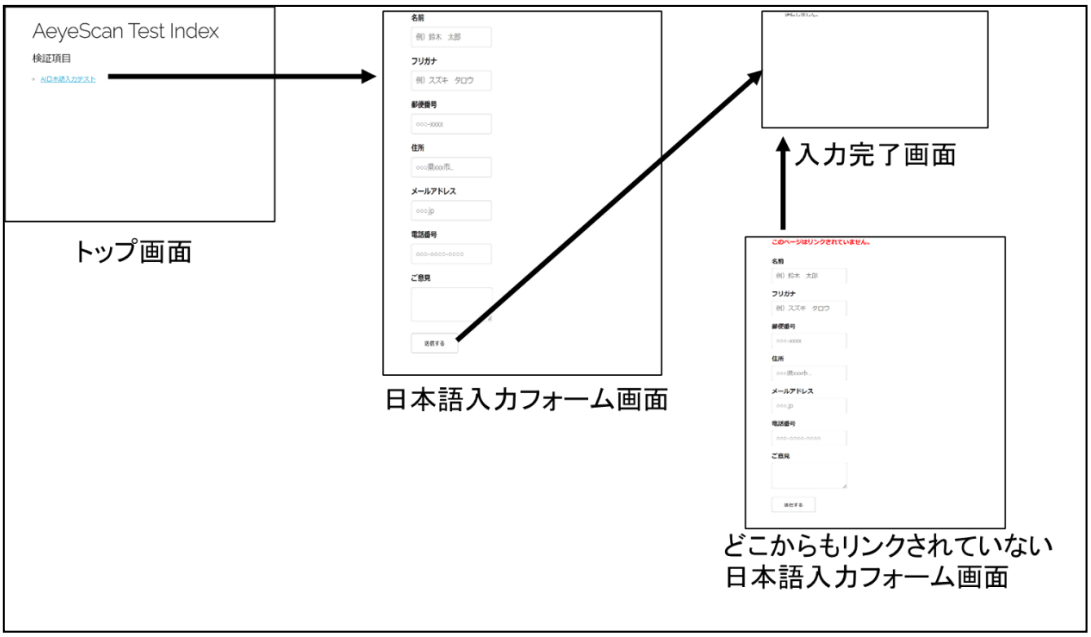


図 8　AeyeScan 検証用 Web サイト②画面イメージ

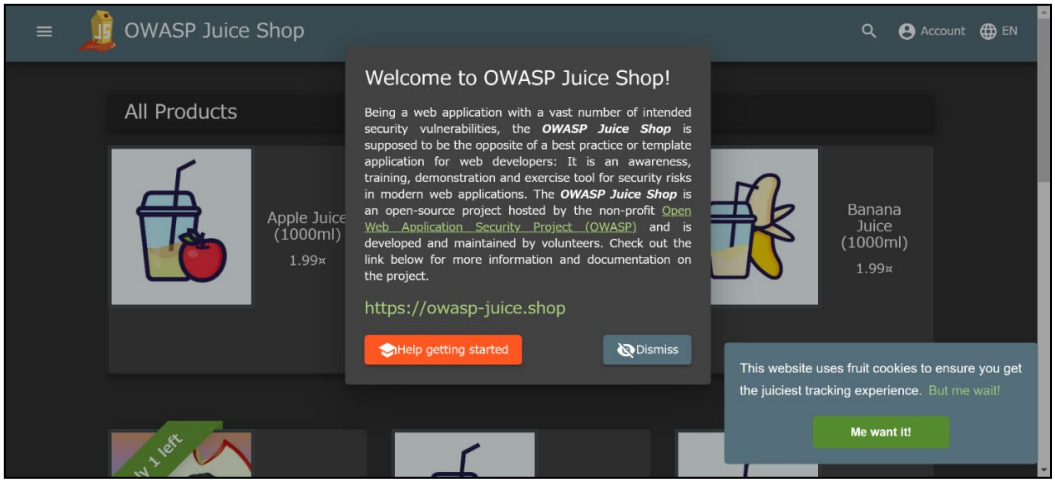


図 9　AeyeScan 検証用 Web サイト③画面イメージ

AeyeScan の利用にあたって、まずアカウント情報が提供された後、スキャン一覧画面にて検証用 Web サイト①、②、③を新規登録した。その後、その登録情報に対して脆弱性診断を実施するための設定をした後、診断を実行することで各検証項目を検証した。

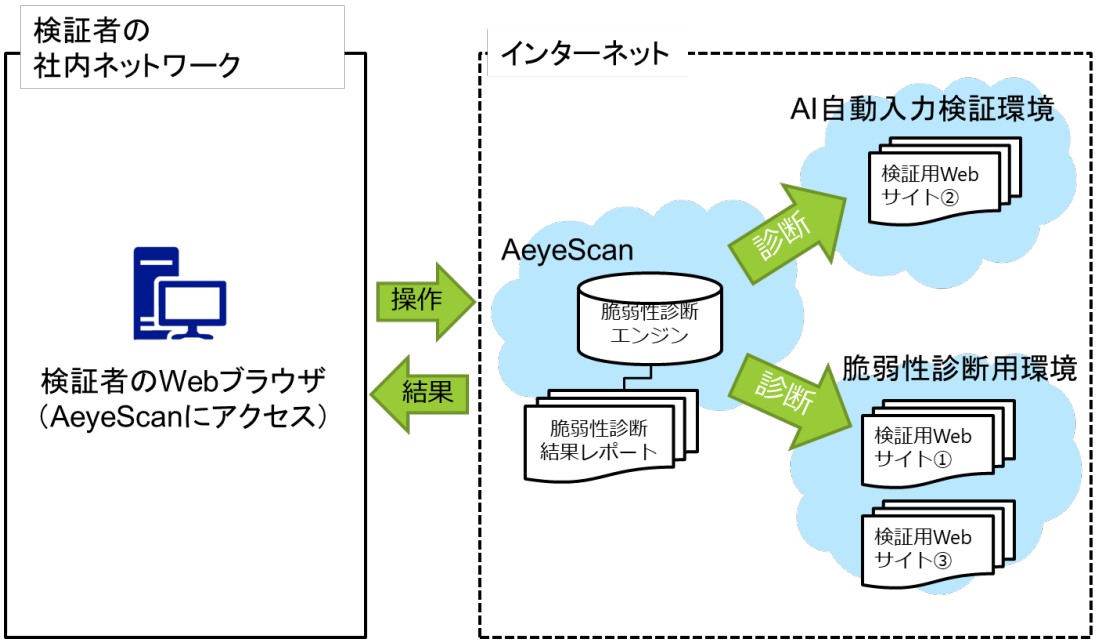


図 10　AeyeScan による脆弱性診断イメージ

4.4　検証結果

4.4.1　Karma（種別 A）の検証結果概要

本検証では、応募ベンダが対象製品において新規性の高いセキュリティに関する機能としている 3 つの事項である「IoT 機器の正しい情報を検出できること」、「セキュリティリスクのある IoT 機器を検出できること」、「日本語検索が可能であること」に関連する検証項目について、4.3.1 項に示す検証条件の下で検証を行い、当該機能が応募ベンダの主張する内容どおりであることを確認した。詳細な検証報告書は付録 D を参照のこと。

4.4.2　AeyeScan（種別 B）の検証結果概要

本検証では、応募ベンダが対象製品においてセキュリティ機能に関するユーザビリティ項目であるとしている 4 つの事項である「① 機能充足性：AI,RPA 技術を活用した自動クローリング能力」、「② 機能正確性：画面クローリング性能（範囲、深度）」、「③ 効率性・運用操作性：脆弱性の検出箇所を視覚的に分かりやすくレポート」、「④ 習得性：設定項目が少なく、操作が容易」に関連する検証項目について、4.3.2 項に示す検証条件の下で検証を行い、当該項目が応募ベンダの主張する内容どおりであることを確認した。詳細な検証報告書は付録 E を参照のこと。

4.5 「試行導入・導入実績公表の手引き」の評価

種別 B の製品について、2019 年度事業で策定し 2020 年度事業で改良した「手引き」[9]に基づき検証を実施した。本項では、手引きに基づく検証実施を踏まえ、手引きに対する評価結果を示す。

手引きでは、製品試行導入のフェーズを「準備」「実施」「評価」の 3 つのフェーズに分類し、それぞれのフェーズで確認すべき内容について記載されている。本事業での検証準備にあたって、手引きの「準備」フェーズの記載を参考にしたため、特に「準備」フェーズの記載に関する手引きの評価を行う。手引き表 2-5 では試行導入における「スケジュール」の検討が重要である旨が言及されている。具体的には、「試行導入に割ける期間が限られている場合は検証項目の取捨選択を行い、限られた時間の中で評価を行う必要がある」との記載がなされている。本事業における検証ではこの記載を参照し、スケジュール内で実施が困難な検証項目はあらかじめ外すことができた。一方で、手引きでは、検証項目の取捨選択の考え方が明記されていない。そのため、検証項目の取捨選択の考え方に関して、例えば、検証対象製品が主張する新規性の高いセキュリティに関する機能に直接的に影響する検証項目は優先度を高めて検証を実施するなど、検証項目の優先度に基づく取捨選択の方向性についても言及することが望まれる。また、手引きでは「検証項目の決定」に関して、「検証項目は個別の機能の検証（＝「単体テスト」のような観点）と、実際に自組織で製品を運用する際のシナリオに沿った検証（＝「システムテスト」のような観点）の両方の観点で用意することが求められる」と言及されている。本事業における検証は主に前者の単体テストであったが、製品の評価を行ううえでは、製品ユースケースを考慮したシステムテストも重要となる。現状の手引きでは、単体テストとシステムテストの両方の重要性は言及されつつも、どちらのテストをどの程度実施すべきという指標に関しては言及がなされていない。この指標は製品のユースケースやそれぞれのテストに要するコストによっても変動するところであるが、製品を試行導入する方が検証項目を決定するうえで参考となる情報であるため、追記することが望まれる。

手引きの第 3 章では、試行導入結果についての情報を公開するポイントについても言及されている。本事業の検証においても検証結果報告書を作成し、その公開がなされるところ、公開に向けた調整にあたって手引きの記載を参照した。手引きにおいて情報公開に伴うメリット・デメリットの例が示されているため、検証結果報告書の作成に関する製品ベンダとの議論にあたって、公

[9] IPA「試行導入・導入実績公表の手引き」 https://www.ipa.go.jp/files/000090566.pdf

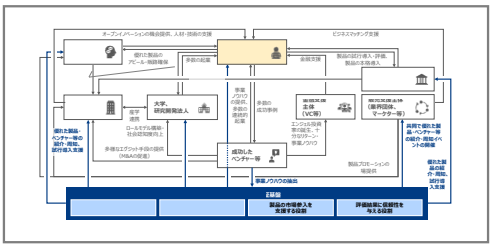
開のメリット・デメリットを意識した議論を行うことができた。試行導入結果について情報を公開する際、手引きの第 3 章の記載が参考になるといえる。

5. 市場参入促進の仕組みの検討

5.1 市場参入促進の仕組みの検討プロセス

2020 年度事業において、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役割（機能）について検討し、検証基盤とこれらの役割から成る市場参入促進の仕組みを検討して、本基盤とこれらの役割間の関係性を表す図（図 12 参照。）を作成した。本年度はこの図を出発点として、特に昨年度調査でスタートアップ企業等の要望の多かった、SI 事業者や販社など市場へのチャネル上に居る役割（企業等）とのマッチング機会の創出に焦点を絞り、調査検討を行った。具体的には、セキュリティ製品ベンチャー等と SI 事業者や販社とのマッチング機会の創出に関する諸外国の取組の調査や SI 事業者や販社に対するヒアリング調査を通じて、マッチング機会の創出に係るゴール像及びゴール実現までのロードマップ案を作成した。今年度の検討プロセスイメージを図 11 に示す。以降では、このプロセスに従い調査・検討した結果を示す。

（参考）昨年度調査結果：
検証基盤と役割間の
関係性を表す図



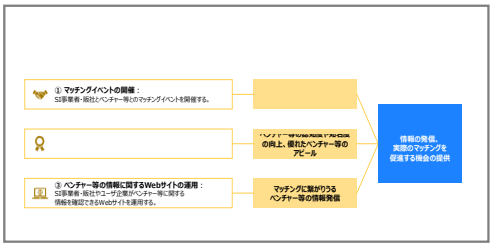
**マッチング機会に関する
既存の取組の調査**

既存の取組における実施内容や効果、
目指すべき姿を調査する

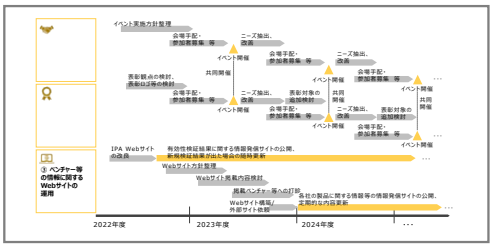
**SI事業者や販社に対する
ヒアリング調査**

市場へのチャネル上に居る役割として、
求めるマッチング機会のニーズを聴取する

**マッチング機会の創出に係る
ゴール像の作成**

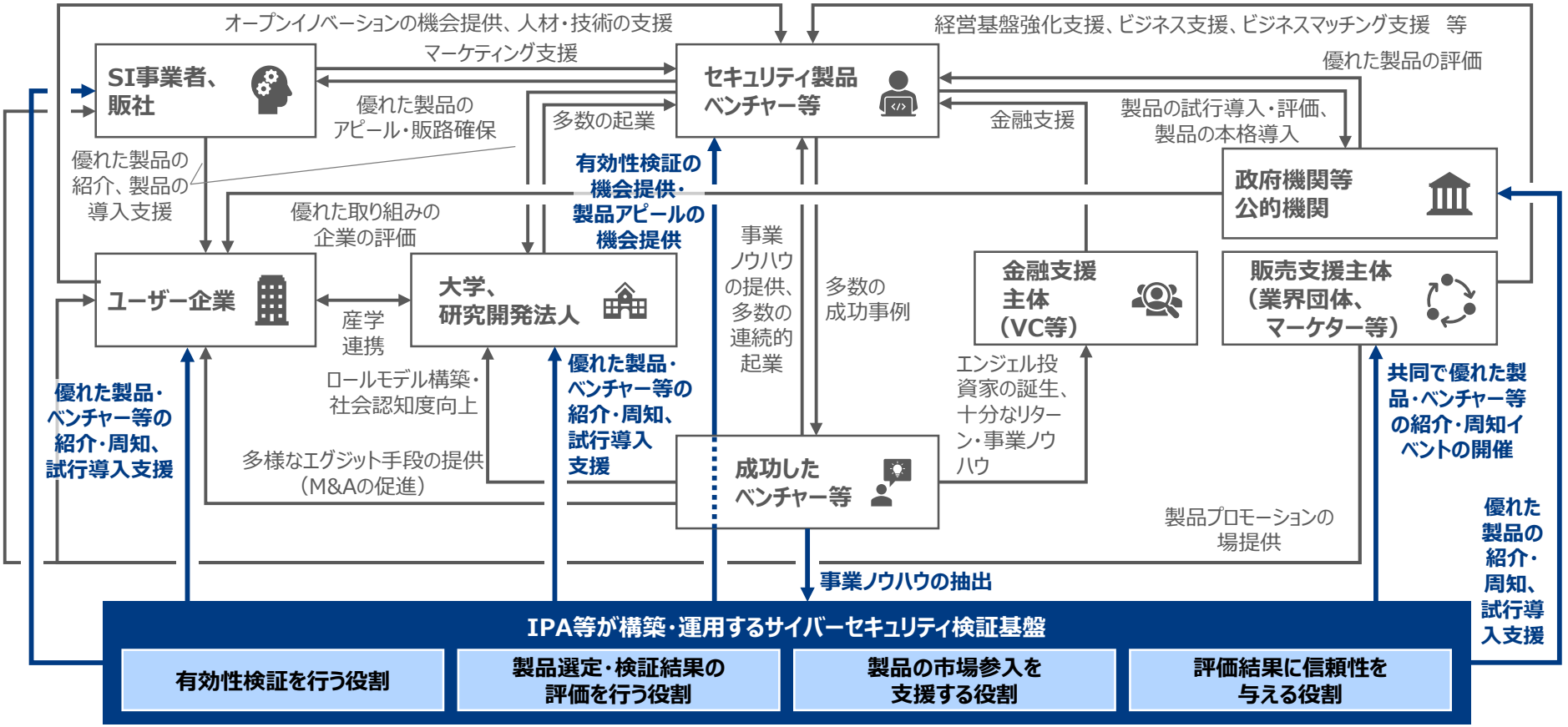


**ゴール実現までの
ロードマップ案の作成**



7

図 11　マッチング機会創出に係る今年度の検討プロセス



出所）IPA「2020 年度サイバーセキュリティ検証基盤の構築に関する報告書」[10]に対して三菱総合研究所加筆

図 12　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）と今年度調査の主な検討対象

[10] https://www.ipa.go.jp/security/economics/shikoukekka2021.html

5.2 マッチング機会に関する諸外国における取組

セキュリティ製品ベンチャー等と SI 事業者や販社とのマッチング機会の創出に関する諸外国の取組について、文献調査を行った。諸外国調査の対象は、シンガポールの CSA（サイバーセキュリティ庁）が支援している ICE71（Innovation Cybersecurity Ecosystem at Block71）[11]と、欧州委員会のパートナー組織に位置づけられているベルギーの非営利団体 ECSO（European Cyber Security Organisation）[12]とした。これらの機関で実施されている関連施策の概要を表 19 に示す。

表 19　マッチング機会の創出に関する諸外国の取組の概要

取組名	ICE71 Scale	ICE71 Community	European Cybersecurity STARtup Award	Cybersecurity made in Europe	Cyber Investor Days
概要	ベンチャー等がネットワーク構築や製品テストできる施設の提供	ベンチャー等と、企業等が登録するメーリングリスト等のプラットフォームの提供	最先端のベンチャー等に対する表彰イベント	ベンチャー等に対する適格性ラベルの付与	ベンチャー等と、販社・投資家とのマッチングイベント
関連機関	ICE71(Innovation Cybersecurity Ecosystem at Block71)、シンガポール CSA（サイバーセキュリティ庁）		ECSO（European Cyber Security Organisation）		
目的	ベンチャー等と企業等とのネットワーク構築、製品テスト機会の提供	ベンチャー等と企業、投資家、メディア関係者、求職者等とのネットワーク構築	最先端のベンチャー等の知名度向上	サイバーセキュリティ関連企業の知名度向上	ベンチャー等に対する資金調達や市場参入機会の提供
実績	39 のベンチャー	400 のベン	第 1 回のイベント	73 のサイバー	第 9 回のイベン

[11] ICE71 https://ice71.sg/

[12] ECSO https://ecs-org.eu/

	等が登録（2021 年 12 月時点）	チャー等と VC が ICE71 のネットワークに参加	では、地域コンテストで勝利したベンチャー等 8 社の中から、ドイツのベンチャー等が選出	セキュリティ関連企業がラベルを取得（2022 年 2 月時点）	トでは、選抜された 15 のベンチャー等と、100 人以上の投資家が参加
開始時期	2018 年 3 月	不明	2021 年 2 月	2020 年 7 月	2018 年 2 月

（表内「ベンチャー等」は、サイバーセキュリティ製品・サービスに関連するベンチャー企業等を指す。）

出所）各取組の公開情報に基づき三菱総合研究所作成

以降では、それぞれの取組の概要について記載する。

5.2.1 シンガポール ICE71 における取組

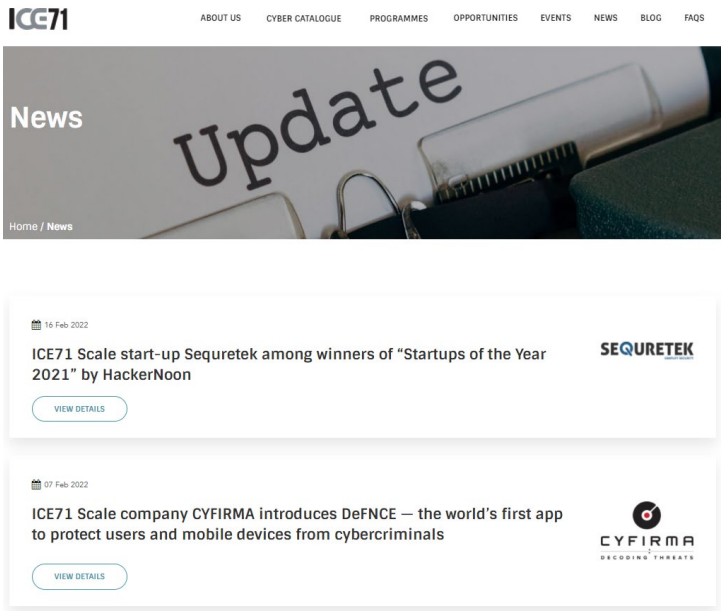
2018 年に設立された、シンガポールのサイバーセキュリティ・エコシステムの強化を目的とした組織である ICE71 は、Singtel グループのベンチャーキャピタル部門 Singtel Innov8 とシンガポール国立大学の起業部門 NUS Enterprise によるパートナーシップで構成され、CSA より支援を受けている。このプログラムでは、サイバーセキュリティ製品・サービスに関連するベンチャー企業等を様々な側面から支援している。ICE71 のネットワークには、現時点で 400 を超えるベンチャー企業等が参加し、具体的な取組として、セキュリティ製品ベンチャー等と企業とのマッチングを促進するメーリングリスト等を提供する ICE71 Community やセキュリティ製品をテストできる施設を無償で提供する ICE71 Scale などが挙げられる。

ICE71 Community は、サイバーセキュリティに関心のある人や企業が集うコミュニティであり、個人であれば無料で参加することができる。メーリングリストが設けられているほか、ナレッジシェアイベントやネットワーキング・イベント、サイバーセキュリティスキルを紹介する機会など、様々な機会が提供される。

ICE Scale は、シンガポール及びアジア太平洋地域でのベンチャー等のビジネスの成長をサポートすることを目的としたプログラムである。アジア太平洋地域に進出している、もしくは進出する準備ができている世界中のベンチャー企業の応募を受け付けており、2021 年 12 月時点で 39 のベンチャー企業が参加している。参加が認められた企業には、オフィススペース、仮想環境での検証、概念実証、製品展示のためのプラットフォーム等のサイバーセキュリティ関連のリソース

が無償で提供される。また、Singtel Innov8 を通じて、投資家、企業、メンター等のネットワークを活用する機会が与えられるほか、ICE71 Community、NUS Enterprise、その他の政府及び企業パートナーを通じて地域の市場にアクセスすることが可能となる。

ICE71 のウェブサイトでは、ICE71 Scale の参加企業の動向が紹介されている（図 13 参照）。加えて、ICE71 は、Singapore Cybersecurity Startup Map を作成しており、2020 年のバージョンでは 136 のベンチャー企業が掲載されている（図 14 参照）。このシンガポールの例のように、セキュリティ製品ベンチャー等が集うプラットフォームを構築し、マッチング支援や広報支援を行っていくことが国内でも望まれる。また、施設等の提供を通じた検証支援も行うことができれば、シードステージやアーリーステージの段階にある企業の発展にも寄与できると思われる。



出所）ICE71[13]

図 13　ICE 71 Scale の参加企業の動向が掲載されている Web ページ

[13] ICE71 News　https://ice71.sg/news/

出所）ICE71[14]

図 14　ICE71 Singapore Cybersecurity Startup Map 2020

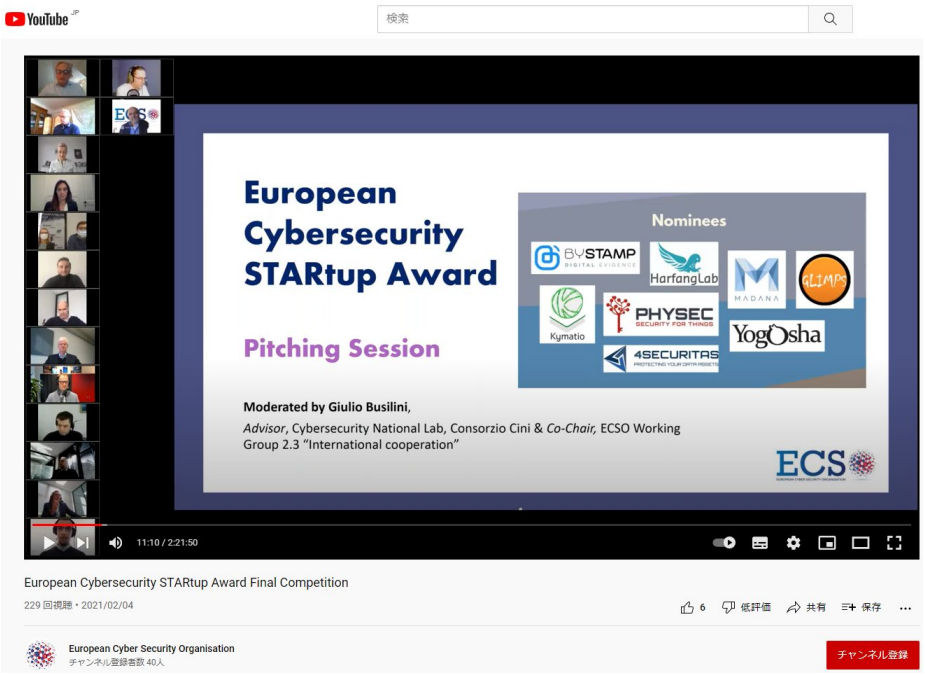
5.2.2　欧州 ECSO における取組

2016 年に設立された ECSO は、ベルギーの法律に基づく完全自己資金による非営利団体である。欧州委員会のパートナー組織として、欧州のサイバーセキュリティ・エコシステムを構成する様々なステークホルダーとの協力関係を構築・強化することを目指して、多様な取組を行っている。具体的には、優れたセキュリティ製品ベンチャー等に対して表彰を与える European Cybersecurity STARtup Award、セキュリティ製品ベンチャー等に対して適格性ラベルを付与する Cybersecurity made in Europe、セキュリティ製品ベンチャー等と投資家とのマッチングイベントである Cyber Investor Days といった取組が挙げられる。

European Cybersecurity STARtup Award は、欧州における最先端サイバーセキュリティ企業の認知度向上を目的として創設された表彰イベントである。オンラインで行われた 2021 年の第 1 回最終コンペティションでは、地域コンテストで勝利したベンチャー企業 8 社が、国際的な投資家、企業の CISO、大手サイバーセキュリティ製品企業の代表者、ECSO の代表者、サイバーセキュリティ専門家により構成された審査員に対してピッチを行った（図 15 参照）。その結果、革新的なソリューション、成長志向のビジネスプラン、市場参入戦略、ビジネスモデル、資金使途、チームプロフィール、ピッチパフォーマンス等が総合的に評価されたドイツの PHYSEC 社が最優秀賞

[14] ICE71 ICE71 Singapore Cybersecurity Startup Map 2020 https://ice71.sg/the-singapore-cybersecurity-startup-community-map-2020/

を受賞した。



出所）ECSO European Cybersecurity STARtup Award YouTube[15]

図 15　European Cybersecurity STARtup Award の最終コンペティションの様子

Cybersecurity made in Europe は、信頼できるセキュリティ製品を販売する欧州企業であることを示すためのラベルであり、欧州のサイバーセキュリティ企業を宣伝し、欧州市場及びグローバル市場での認知度を高めるためのマーケティングツールとしての活用が期待されている。ラベルを取得する際には技術監査を必要とせず、自己宣言に依っている。ラベルの取得を希望する企業は、研究開発の大部分が欧州で行われていることの証明書等を含む企業に関するファクトシートや、ENISA"Indispensable baseline security requirements for the procurement of secure ICT products and services"[16]への適合に関する宣言書などをラベル発行団体に提出する必要がある。2022 年 2 月時点で、73 の企業がラベルを取得している。本ラベルのその他の概要は表 20 に示す。

表 20　Cybersecurity made in Europe の概要

スキーム所有者・監督者	ECSO

[15] European Cybersecurity STARtup Award Final Competition https://www.youtube.com/watch?v=9YpY2txO3vw

[16] ENISA, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

ラベル発行者	ECSO が認定したパートナー （2022 年 2 月時点で 16 団体）
有効期間	12 か月間 （継続使用を希望する場合は、前回の適格性チェックや承認の後に行われた関連するすべての変更を示す必要がある。）
対象	欧州を拠点とするサイバーセキュリティ企業
ラベル取得企業数	2022 年 2 月時点で 73 企業
ラベル取得費用	€500～€1,000 程度 （ラベル発行団体によって異なる）

出所）公開情報に基づき三菱総合研究所作成

Cyber Investor Days は、欧州のセキュリティ製品ベンチャー企業等に対して資金調達や市場参入の機会を提供するとともに、投資家や販社に対してベンチャー企業等を認知する機会を与えるマッチングイベントである。参加企業は、ECSO 選定委員会に提出された申請書やプレゼンテーションに基づき、ECSO とパートナー企業が共同で 15～20 社ほど選定する。イベントは 2 日間にわたって行われ、投資家やインテグレータ、CIO 向けのワークショップやベンチャー企業等向けの個別のトレーニングセッションのほか、ピッチやビジネス商談会といった催しが行われる。2018 年に開始されてから、これまでに 10 回のイベントが開催されており、第 9 回のオンラインイベントには、15 のセキュリティ製品ベンチャー企業等と 100 人以上の投資家が参加した。ECSO の事例のように、萌芽的な企業がアピールできる機会を用意することは有用であり、国内でも同様の施策が求められると考えられる。

5.3 SI 事業者・販社に対するヒアリング調査

SI 事業者や販社など市場へのチャネル上に居る役割（企業等）とのマッチング機会の創出に向け、SI 事業者・販社 3 社に対してヒアリングを行った。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. 国内のベンチャー等が販売するセキュリティ製品の取扱い状況について
2. 国内のベンチャー等が販売するセキュリティ製品と海外の製品との違いについて
3. 国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、現状抱えている課題や想定される懸念事項について
4. セキュリティ製品を販売する国内・海外のベンチャー等と繋がるために、現状活用してい

る機会について

5. セキュリティ製品を販売する国内のベンチャー等とのマッチング機会として望まれる形式について
6. 国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、望まれるインセンティブや政府に期待することについて

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。

5.3.1 国内のベンチャー等が販売するセキュリティ製品の取扱い状況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 21 に示す。今回ヒアリングを行った SI 事業者・販社は、国内のベンチャー等が販売するセキュリティ製品をほとんど取り扱っていなかった。取り扱っていない理由として、国内製品に対する情報チャネルを有していない等の理由が挙げられた。

表 21　国内のベンチャー等が販売するセキュリティ製品の取扱い状況に関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• 国内のベンチャー等が販売するセキュリティ製品はごく少数しか取り扱っていない。
SI 事業者・販社 B 社	• 国内のセキュリティ製品は取り扱っていない。その理由は大きく 2 つある。1 つ目は、グローバルで通用するレベルのサイバーセキュリティ製品を取り扱うことをモットーとしているからである。2 つ目は、海外製品に関する人脈を広く有している一方、国内製品に関しては情報チャネルを有していないからである。
SI 事業者・販社 C 社	• 国内のベンチャー等が販売するセキュリティ製品は取り扱っていない。

5.3.2 国内のベンチャー等が販売するセキュリティ製品と海外の製品との違いに関するヒアリング結果

ヒアリングでの主な回答結果を表 22 に示す。販売状況や性能面・技術面に関して、国内のベ

ンチャー等が販売するセキュリティ製品と海外の製品との間で大きな差異は感じられないという意見が得られた。また、国内企業の利点として、トラブルが生じた際の対応が優れていることや日本の商習慣を理解していること、日本語話者によって製品が作られていることなどが挙げられた。他方、技術力をアピールする力や先端性については海外企業の方が優れているという意見も挙げられた。国内ベンチャー等のセキュリティ製品のさらなる市場参入を促進するためには、その製品の特長・性能や国内製であることの利点を適切にアピールすることが求められる。

表 22　国内のベンチャー等が販売するセキュリティ製品と海外の製品との違いに関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• 販売状況に関しては、国内のベンチャー等が販売するセキュリティ製品と海外の製品とで特に差異は感じていない。
SI 事業者・販社 B 社	• 性能面や技術面に関して、海外製品と国内製品との間に大きな差はない。一方、最先端製品はシリコンバレーやイスラエル発のものが多いと感じている。 • 新しい製品は実際に運用を始めるとトラブルが生じることがある。その点をカバーする技術力に関しては、日本のメーカーの方が優れている側面もある。
SI 事業者・販社 C 社	• 国内企業の利点として、日本の商習慣（決裁に時間がかかりリードタイムが長くなってしまうこと等）を理解していることやトラブルが生じた際に開発者に直接会えることといった点が挙げられる。 • 日本語話者によって作られた製品であるということは、日本人ユーザにとってアドバンテージである。 • 技術力をアピールする力は、海外企業の方が優れている。

5.3.3　国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、現状抱えている課題や想定される懸念事項に関するヒアリング結果

ヒアリングでの主な回答結果を表 23 に示す。まず挙げられたのは顧客ニーズに関する意見である。国内のベンチャーはその製品の利用価値についてうまくアピールできていないとの指摘があった。そのため、マッチングの場では、技術的な面だけでなく顧客目線でのアピールを行うことが求められる。次に、収益性や営業効率が海外製品と比べて見劣りするという意見が挙げられ

た。排他的な契約を結ぶことで独占的に販売するといったビジネスモデルは国内製品では採用しづらいため、国内製品を選ぶメリットを感じにくいという指摘である。さらに、ベンチャー企業は狭く深く付き合えるディストリビューターを見つけ、二人三脚で販売を行っていく方が良いという意見が得られた。これらの意見を踏まえると、マッチングの機会を設けるだけでなく、セキュリティ製品ベンチャー等が抱えるビジネス構造上の課題についても対応していく必要がある。

ヒアリングでは企業自体の信頼性に関する意見も挙げられた。大企業と比較した際、ベンチャー企業においては倒産のリスクも懸念されるが、ベンチャー企業の信頼性を判断するための情報が海外企業と比べて取得しづらいという指摘がなされた。そのほか、最先端の国内製品を見つけられない、国内製品がグローバル展開に対応できるかについて懸念がある等の意見も挙げられた。

表 23　国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、現状抱えている課題や想定される懸念事項に関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• SI 事業者が国内製品に求めることは、優先度が高い順に「顧客ニーズ」「収益性」「営業効率（競合が多すぎないこと）」であるが、これらの要素が海外製品に比べて見劣りすることが問題だと考えている。 • 企業の信頼性の判断は、海外企業に比べて難しいと感じている。
SI 事業者・販社 B 社	• 国内製品は独占的に販売することが難しいと思われる。そのため、国内製品を販売する際には何らかのインセンティブが必要である。 • 国内調査は行っているが、調査が足りていないのか選定基準を満たすような最先端の国内製品が見つからない。 • 国内製品がグローバル展開に対応できるのかについて懸念がある。

ヒアリング先	主な回答
SI 事業者・販社 C 社	• 国内のベンチャー企業は技術の特徴だけをアピールすることが多いが、マーケティングの観点で利用価値等をアピールすることも重要である。 • ベンチャー企業は、狭く深く付き合いできるディストリビューターを見つけ、二人三脚で販売を行っていく方が良い。そうでなければ、薄利となってしまう。 • ベンチャーの場合、会社が倒産するリスクも懸念点として考えられる。日本の経営者は、国内企業と比べて海外企業に対する倒産リスクを想定しない傾向にある。 • 国内のベンチャーは実績のアピールがうまくできていない。海外企業は実績のアピールがうまく、国防総省で採用されていること等を示して売り込んでいる。

5.3.4 セキュリティ製品を販売する国内・海外のベンチャー等と繋がるために、現状活用している機会に関するヒアリング結果

ヒアリングでの主な回答結果を表 24 に示す。全社に共通していた意見として、人づてで多くの情報を得ているという意見が挙げられる。いち早く情報を仕入れるには、人づてが一番だという意見も得られた。ほかには、業界団体のコミュニティや Web サイト、メーカーによる売り込み、展示会といった機会を活用しているとの意見が挙げられた。ただし、展示会では様々な企業が一斉に来訪するため、まだ世に出ていない情報は得られないという指摘もなされた。また、海外製品の情報は海外支社の担当者から得ているとの回答が得られた。

表 24　セキュリティ製品を販売する国内・海外のベンチャー等と繋がるために、現状活用している機会に関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• JNSA をはじめとした業界団体のコミュニティや Web 等から情報収集を行っているほか、他社等から人づてにご紹介いただくことが多い。 • 海外支社から情報を得ている。
SI 事業者・販社 B 社	• 新規のセキュリティ製品を探すため、イスラエルやアメリカ、ヨーロッパの展示会に参加している。情報セキュリティ EXPO といった国内のセキュリティ関連の展示会にも訪問やブース出展を行っている。展示会では様々な企業が一斉に来訪するため、まだ世に出ていない情報は得られない。 • 新規製品を探す際に最も重要なのは、人脈である。いち早く情報を仕入れるには、人づてが一番である。
SI 事業者・販社 C 社	• 海外支社の担当者がカンファレンスやシンポジウムに参加するなどして集めた海外製品の情報をレポートにまとめている。このレポートをもとに、製品を取り扱うか否かについて、自社内で議論をしている。 • 国内のイベントに参加する機会は少ない。 • セキュリティ業界内で転職を重ねている人づてで、情報が入ってくることが多い。 • ディストリビューターの役割を積極的に担っているため、メーカーからご紹介に来ていただける機会が多い。

5.3.5　セキュリティ製品を販売する国内のベンチャー等とのマッチング機会として望まれる形式に関するヒアリング結果

ヒアリングでの主な回答結果を表 25 に示す。国内のベンチャー等のセキュリティ製品を紹介する場があれば積極的に参加したいという声が複数社より寄せられた。具体的なマッチング機会の形式については、メーリングリストやポータルサイト、オンラインイベント等どのような形態でも良いという意見が挙がった一方、各企業のアピールポイントをきちんと把握するためには、イベントの方が良いという意見も挙がった。また、マッチング機会の場では、製品の特徴やビジネスモデル等について知りたいという意見も得られた。

表 25　セキュリティ製品を販売する国内のベンチャー等とのマッチング機会として望まれる形式に関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• IPA が得た情報を発信いただければありがたいが、それで状況が大きく変わるとは考えていない。
SI 事業者・販社 B 社	• 国内ベンチャーのセキュリティ製品を紹介する場があれば、是非参加したい。 • メーリングリスト、ポータルサイト、オンラインイベント等どのような形態でも良い。
SI 事業者・販社 C 社	• 知らない企業も多いため、様々な企業の取り組みについて知ることができる機会があれば、R&D の担当者等に参加させたい。 • メールは読めないことが多いため、各企業のアピールポイントをきちんと把握できるイベントの方が良い。 • マッチング機会の場では、製品の特徴やビジネスモデル等について知りたい。

5.3.6　国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、望まれるインセンティブや政府に期待することに関するヒアリング結果

ヒアリングでの主な回答結果を表 26 に示す。政府機関や国内の代表企業が積極的に国内のベンチャー等が販売するセキュリティ製品を採用し、お墨付きを与えるべきだという声がヒアリングを実施した 3 社すべてから寄せられた。他国ではこういった取り組みが進められているため、我が国でも実施の検討を行うことが望まれる。ほかには、企業自体の信頼性を確認してほしい、国内製品の導入による税制優遇といったインセンティブが求められる、国内企業に不足しているマーケティングの観点を補う仕組みを設けるべき、国内ベンチャーに対する財務面での支援を行うことが重要、SI 業界の不適切な慣行に対する規制を行ってほしい等の意見も挙げられた。本事業では、セキュリティ製品ベンチャー等と SI 事業者や販社とのマッチング機会について調査・検討を行ったが、今後、より大局的な施策に関しても議論することが望まれる。

表 26　国内のベンチャー等が販売するセキュリティ製品を取り扱うことに関して、望まれるインセンティブや政府に期待することに関する主な回答

ヒアリング先	主な回答
SI 事業者・販社 A 社	• 国家機関や国内の代表企業で、国内のベンチャー等が販売するセキュリティ製品を積極的に採用するべきである。韓国では、こういった取り組みを積極的に行っている。 • 国によるお墨付きは一つでも多くあった方が良い。 • 企業の信頼性を国に確認していただけると参考になる。製品の紹介に来たベンチャー企業が信頼できるか判断に迷う時がある。
SI 事業者・販社 B 社	• まずは国が、国内製品を利用したり投資を行ったりすることが重要だと思われる。
SI 事業者・販社 C 社	• 経産省や IPA、NISC といった政府機関や他の機関等が、国内のベンチャー等が販売するセキュリティ製品を評価し、お墨付きを与えるような仕組みを作ることが必要だろう。 • 新しい製品を積極的に導入するアーリーアダプター的な企業を募集しておくのも一案かもしれない。企業体力があり、国のために貢献してくれる企業に、製品を先んじて導入していただき、その企業には優遇措置を与えるといった仕組みが考えられる。 • 国内製品を導入すると税制が優遇されるといったインセンティブがあれば良い。 • 国内ベンチャーに不足しているマーケティングの観点を補うような仕組みがあれば良い。 • 国内ベンチャーに対して、投資をはじめとした財務面での支援を行うことも必要だと思われる。 • SI 事業者は、顧客からの無茶な注文に応じざるを得ない状況にある。こうした事態に対して規制を加えなければ、業界自体が廃れてしまう可能性がある。

5.4　マッチング機会に関する仕組みのゴール像

マッチング機会の創出に関する諸外国の取組の調査結果及び SI 事業者や販社に対するヒアリング調査結果を踏まえ、我が国で創出すべきマッチング機会に関するゴール像の作成を行った。過年度調査におけるベンチャー等の意見や今年度調査における SI 事業者・販社の意見を踏まえると、我が国で創出すべきマッチング機会に関するゴール像として、「ベンチャー等やそのセキュリ

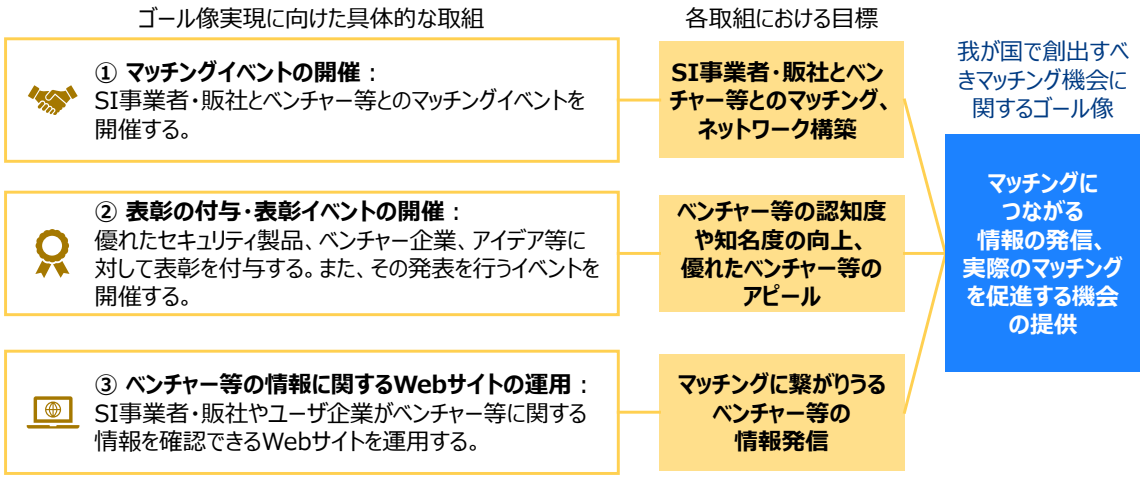
ティ製品に関する情報を定常的に発信しつつ、ベンチャー等のアピールポイントを訴求し実際のマッチングを促進するイベント等の機会も提供すること」が求められると考えられる。そして、このゴール像の実現のためには、諸外国の取組を参考に、「集中的なマッチング機会」と「継続的なマッチング機会」の両方を提供することが必要である。

- 集中的なマッチング機会：表彰イベントやマッチングイベントの開催等、ある一定期間内で開催するセキュリティ製品ベンチャー等と SI 事業者や販社とのマッチングを支援・促進する機会。
- 継続的なマッチング機会：検証用施設の提供、HP やメーリングリストの運営等、継続的にセキュリティ製品ベンチャー等と SI 事業者や販社とのマッチングを支援・促進する機会。

ゴール像実現に向けた具体的な「集中的なマッチング機会」と「継続的なマッチング機会」の取組として、以下の 3 つの取組の推進が望まれる。

① マッチングイベントの開催
② 表彰の付与・表彰イベントの開催
③ ベンチャー等の情報に関する Web サイトの運用

図 16 にこれら 3 つの取組の概要及び各取組における目標を示す。以降では、それぞれの取組の具体的な実施イメージについて説明する。



出所）諸外国における取組及び SI 事業者・販社へのヒアリング結果を踏まえ三菱総合研究所作成

図 16 マッチング機会の創出に係るゴール像とゴール像実現に向けた具体的な取組

(1)　マッチングイベントの開催について

ゴール像実現に向けた具体的な取組の一つとして、SI 事業者・販社とベンチャー等とのマッチングイベントを開催し、SI 事業者・販社とベンチャー等とのマッチング及びネットワーク構築に寄与することが望まれる。具体的なマッチングイベントの実施イメージを図 17 に示す。欧州 ECSO の Cyber Investor Days や他分野でのマッチングイベントの取組を参考に、参加するベンチャー等ごとにブースを設け、各ブースにてベンチャー等が自社製品をアピールするとともに、協業可能性に関する相談等を実施する個別商談ブースを設置することが効果的である。

参加するベンチャー等について、有効性検証に応募いただいた企業に対しては参加を推奨しつつ、我が国全体の市場参入促進に寄与するために、応募のないベンチャー等（アーリーステージのベンチャー等も含む）の参加も可能とすることが望ましい。また、本取組の主な対象者は SI 事業者・販社であるが、欧州 ECSO の取組や販社へのヒアリング結果を踏まえると、ユーザ企業や VC 等の金融支援主体も参加可能とすることで、ベンチャー等の市場参入促進に繋がると考えられる。

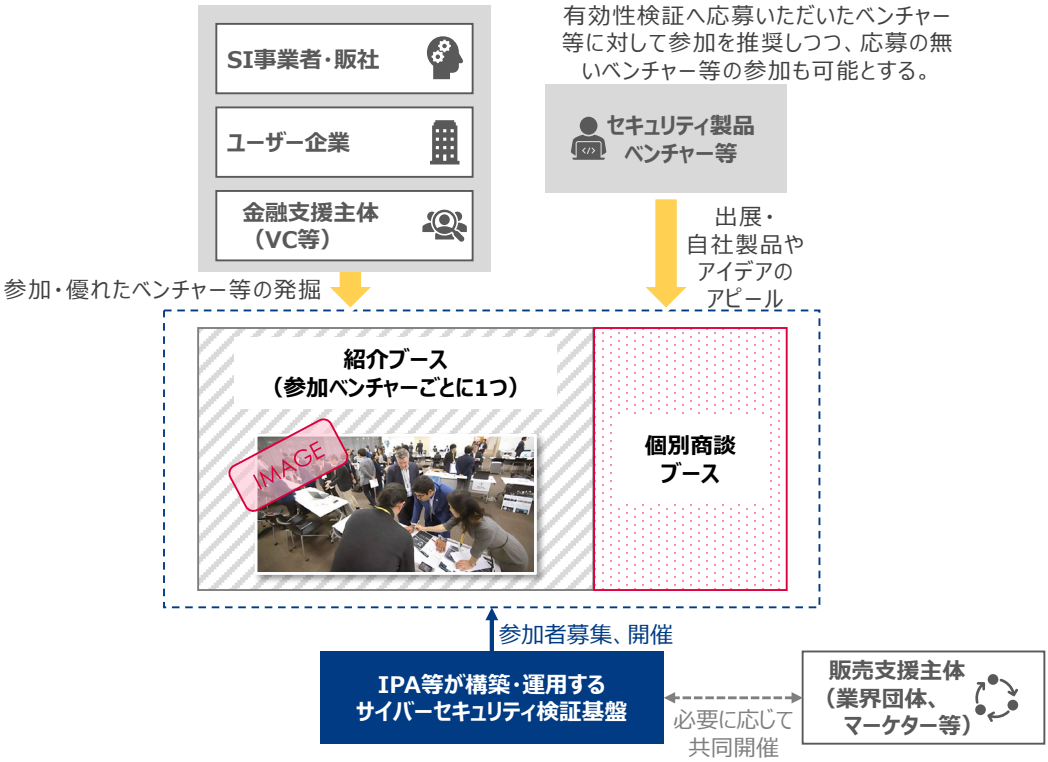


図 17　取組① マッチングイベントの実施イメージ

国内における他分野でのマッチングイベントとして、医療・ヘルスケア分野でのマッチングイ

ベントである「ジャパン・ヘルスケアベンチャー・サミット（JHVS)」が挙げられる。JHVS は、医療系ベンチャーを育てるエコシステムを確立するため、医療系ベンチャーと大手企業、金融機関、研究機関等とのマッチングやネットワーキングを促進することを目的としたイベントであり、厚生労働省主催により 2017 年から開催されている。パシフィコ横浜において、2020 年 10 月に開催された JHVS 2020 では、112 の医療ベンチャー等が出展し、13,787 人の来場があった。また、このイベントを通じて 1,188 件のマッチングが成立[17]したと報告[18]されている。JHVS 2020 後のアンケート結果によれば、参加者の満足度は非常に高く、90%以上の出展者が次回も出展することを希望しているほか、新たなコネクション構築につながったとする意見が多数挙げられた。JHVS では、各出展ベンチャーに対して個別ブースが用意されるほか、個別に商談を行うための商談ブースも別途用意される。前述のとおり、本稿で考える取組①においても、このイベントを参考に、紹介ブース及び個別商談ブースを設けることが効果的であると考えられる。

（2） 表彰の付与・表彰イベントの開催について

ゴール像実現に向けた具体的な取組の一つとして、優れたセキュリティ製品に対して表彰を付与するとともに、表彰結果を公表するイベントを開催することで、認知度・知名度の向上やアピール機会の創出を行うことが必要であると考えられる。表彰イベントの実施方針について、欧州 ECSO の European Cybersecurity STARtup Award の取組を参考に、有効性検証の対象となった製品の表彰だけではなく、ベンチャー等によるプレゼンテーションや当該プレゼンテーションに対する有識者による講評の時間を設けることで、参加者に対する製品のアピールに繋がり、幅広いベンチャー等の市場参入促進において効果的であると考えられる。プレゼンテーションや表彰の対象となるベンチャー等については、有効性検証の対象となったベンチャー等に限らず、幅広いベンチャー等を対象とすることが望まれる。

表彰の観点について、欧州 ECSO の European Cybersecurity STARtup Award の取組では、製品に関する観点のほか、ベンチャー等が有するビジネスモデルや戦略、資金の使途等も評価の観点に含まれる。各表彰においては、表彰を受けたベンチャー等がアピールできるよう、ロゴやマークを用意することが、製品の市場参入促進においては重要となる。将来的には、このような幅広い観点に基づき、幅広いベンチャー等に対して表彰の間口を広げることが望まれるが、初期段階

[17] マッチングシステムによって面談が成立した件数。

[18] 厚生労働省、ジャパン・ヘルスケアベンチャー・サミット 2020 の概要
https://www.mhlw.go.jp/content/10807000/000741764.pdf

では幅広の表彰を用意することは現実的ではないため、有効性検証結果を踏まえ、新規性の高いセキュリティ機能に関する表彰や優れたユーザビリティ項目に関する表彰を与えることが望ましい。したがって、図 18 に示すように、徐々に観点を増やし、将来的には幅広い製品に対して表彰が付与できる仕組みが構築されると良い。ただし、表彰の位置づけ、表彰付与の主体のあり方、詳細な表彰の観点等については今後詳細な検討・設計が必要となる。

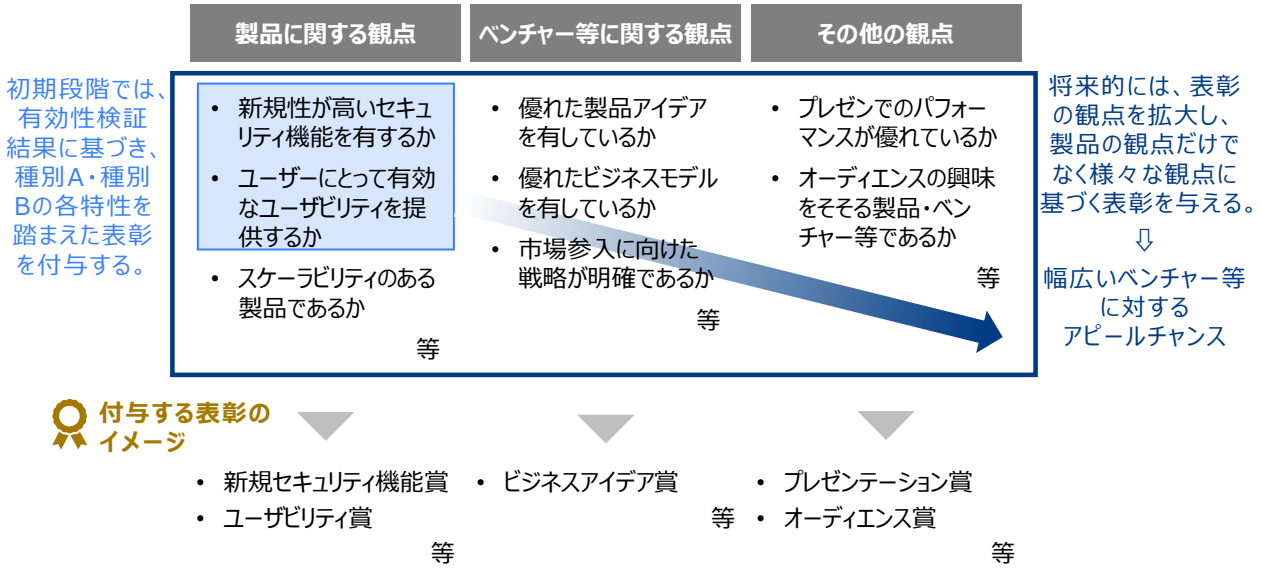


図 18　取組② 製品に対する表彰の観点

（3） ベンチャー等の情報に関する Web サイトの運用について

ゴール像実現に向けた具体的な取組の一つとして、マッチングに繋がりうる情報を定常的に発信することが望まれる。これに際し、シンガポール ICE71 の取組を参考に、ベンチャー等に関する情報が確認できる Web サイトを運用することが望まれる。Web サイトでは、最低限、有効性検証結果に関する情報を掲載することが必要である。具体的には、図 19 に示すとおり、過去の有効性検証結果を一覧で確認できる公開方法に変更し、SI 事業者・販社やユーザ企業が効率的に情報を入手できる仕組みとすることが望まれる。将来的には、各社の製品に関する情報、各社の情報（他コンペでの受賞歴など）、関連するイベントの情報（取組①・②に関する情報など）等を発信することが望まれる。これらの情報を発信するサイトについては、既存の外部サイトを活用することも想定される。なお、Web サイトを介して直接的にマッチングを促進する目的では、一方向の情報発信だけでなく、ベンチャー等と SI 事業者・販社とが相互に直接コンタクトできる機能も備えることが望まれる。

出所）IPA ウェブサイト [19]及び NEDO ウェブサイト [20]に基づき三菱総合研究所作成

図 19　取組③ Web サイトの構築及び Web サイトにおける情報発信イメージ

5.5　ゴール実現までのロードマップ案

マッチング機会に関する仕組みのゴール像に向けた 3 つの取組について、各取組の実施に係るロードマップ案を作成した。このロードマップ案を図 20 に示す。本図に示すとおり、「集中的なマッチング機会」と「継続的なマッチング機会」の両方を並行して実施するとともに、実施可能な範囲からスモールスタート的に取組を推進することで、マッチング機会創出に関するゴール像に徐々に近付けることが必要である。

取組①のマッチングイベントの開催に係るロードマップ案に関して、将来的には、医療分野の JHVS のような大規模なイベントを開催することが望まれる。しかしながら、これまでセキュリティ製品ベンチャー等に特化したマッチングイベントは国内で開催されていないところ、初回は

19 https://www.ipa.go.jp/security/economics/shikoukekka2019.html

20 https://startips.nedo.go.jp/

スモールスタート的に開催しつつ、イベント後に出展者や参加者のニーズを抽出し、より良いイベント内容に徐々に改善することが必要である。そのため、初回のイベントは IPA「コラボレーション・プラットフォーム」等の既存のイベントの枠組みを活用して開催することが望まれる。また、参加いただくベンチャー等について、アーリーステージのベンチャー等も含め幅広いベンチャー等の参加を認める。なお、検証基盤や有効性検証の知名度向上の目的も兼ね、過去に有効性検証に応募いただいたベンチャー等に対して積極的な参加を依頼することが望まれる。

取組②の表彰の付与・表彰イベントの開催に係るロードマップ案に関して、本取組によるプレゼンテーション・表彰の直後に取組①のマッチング機会を設けることがベンチャー等の市場参入促進に対して効果的と考えられる。そのため、取組①のマッチングイベントと合同で本取組の表彰イベントを開催することを提案する。したがって、初回のイベントでは IPA「コラボレーション・プラットフォーム」等の既存のイベントの枠組みを活用するとともに、表彰対象は有効性検証対象製品（種別 A・種別 B）に限った形で開催することが現実的である。なお、取組①と同様に、プレゼンテーションに参加いただくベンチャー等について、アーリーステージのベンチャー等も含め幅広いベンチャー等の参加を認めるが、過去に有効性検証に応募いただいたベンチャー等に対しても積極的な参加を依頼することが望まれる。そして、表彰の観点について、前述のとおり初期段階では有効性検証の結果に基づく表彰が望まれるが、徐々に表彰の観点を拡大することが望まれる。

取組③のベンチャー等の情報に関する Web サイトの運用に係るロードマップ案に関して、将来的には、各社の製品に関する情報、各社の情報（他コンペでの受賞歴など）、関連するイベントの情報（取組①・②に関する情報など）等を発信することが望まれるが、まずはこれまでの有効性検証結果に関して適切に発信することが必要である。このために、今後、IPA の Web サイトを改良し、有効性検証結果を一覧で確認できる公開方法に変更するとともに、トップページ等にリンクを貼ることで情報を適切に周知することが必要である。なお、このような公開方法とすることで、SI 事業者・販社やユーザ企業が効率的に情報を入手できるだけではなく、有効性検証に応募することのインセンティブ向上にも寄与すると想定される。

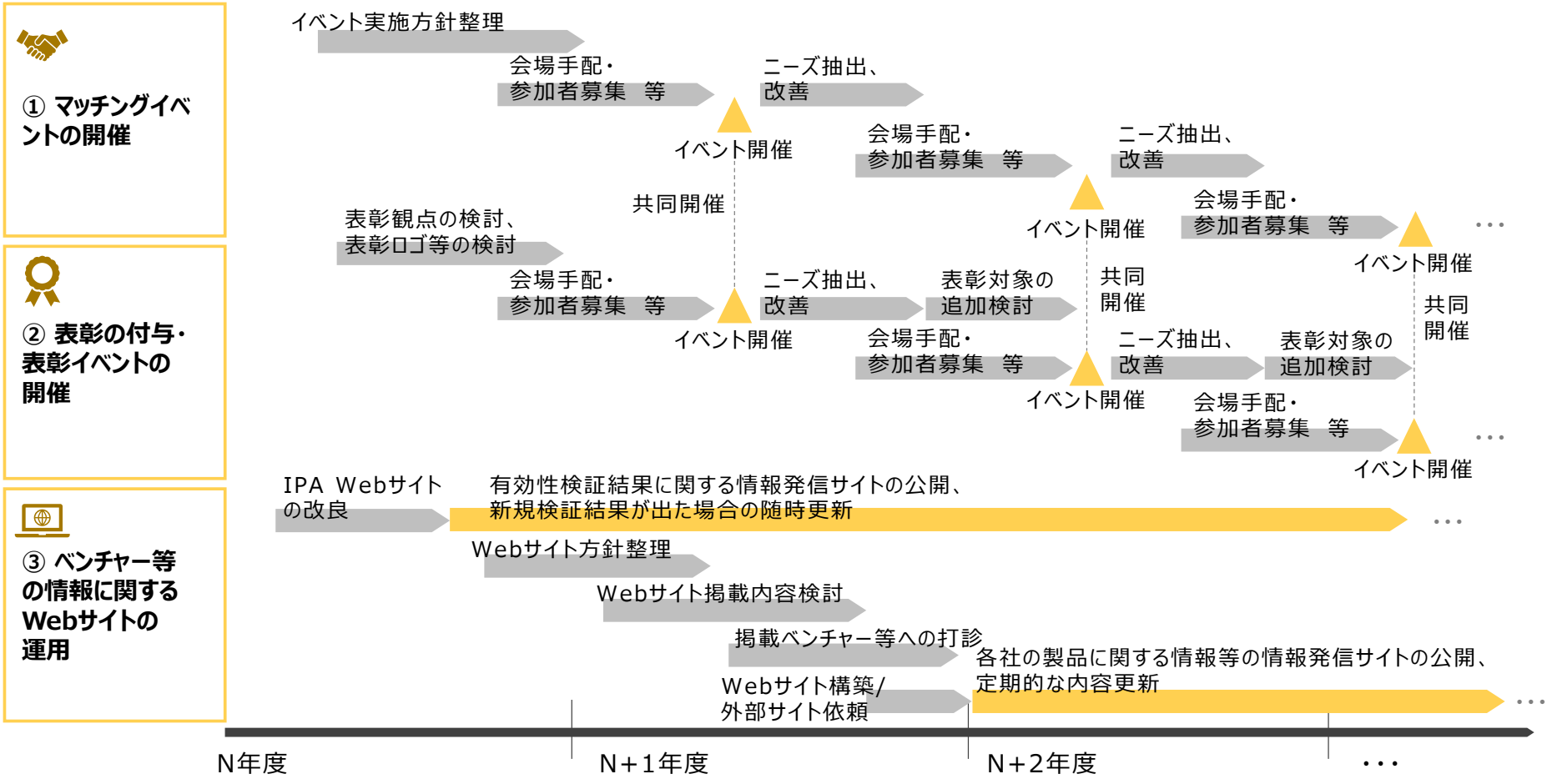


図 20　ゴール像実現までのロードマップ全体像（案）

6. まとめ・考察

本事業では、過年度までの知見・課題を踏まえたうえで検証基盤の改良を行い、検証基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を行った。さらに、市場参入促進の仕組みの更なる具体化などに取り組んだ。

6.1 有効性検証について

昨年度構築したサイバーセキュリティ検証基盤の仕組みを基本に必要な改良を施して、有効性検証を実施した。まず今年度の検証対象となる重要分野を選定した後、当該分野に該当する製品の公募を実施した。応募のあった製品に対する審査を実施した後、選定された 2 製品に対する有効性検証を実施した。選定された 2 製品の有効性検証の結果については、本報告書の付録 D 及び付録 E に示しているとおり、それぞれ報告書として取りまとめた。

以降では、今年度の有効性検証を通じて得られた結果を踏まえ、今後望まれる方向性について考察する。昨年度構築した検証基盤に改良する形で、今年度は製品審査において応募ベンダに対する有識者のヒアリングを実施した。ヒアリングに参加した有識者は一部に限られたが、当日参加した有識者からは、審査にあたっての貴重な機会であったとの意見を頂いた。また、ヒアリング時の様子を録画するとともに、議事録を有識者に展開することで、ヒアリングに参加できなかった有識者においても参考となったとの意見が挙げられた。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ところ、応募ベンダの主張を効果的かつ効率的に聴取できるヒアリングの機会は今後も実施することが望まれる。

有効性検証の対象となった製品ベンダの市場参入を促進する観点で、有効性検証対象製品のユースケースを明確にし、それに則した有効性検証を行うべきとの意見が有識者より複数挙げられた。より具体的には、製品の有効性検証にあたって製品の強みやアピールポイントを意識した検証が必要であり、想定するユーザやユースケースを明確にした上で検証することが望ましいとの意見が挙げられた。今年度、種別 B の募集にあたって対象製品の使用環境と対象ユーザを明記することを求めたが、種別 A においても、製品応募時に製品ベンダが特に訴求したい製品ユースケースを明確化し、それに則した形で検証を行うことが望まれる。

種別 B の製品の有効性検証について、今年度は有効性検証期間の制約により、検証者による検証を行いつつ、適宜検証協力ユーザから意見を頂く形式で実施した。他方、種別 B は民間事業者

等のオフィス等を想定した実環境において製品が有するユーザビリティ項目を検証する種別であるところ、本来は検証協力ユーザの環境に導入し、そのユーザビリティを検証者が客観的に判断する体制が理想的である。ただし、このような体制を構築する場合、有効性検証の応募段階で検証協力ユーザが帯同することのインセンティブが不明確であるところ、本質的には、種別 B の製品が決定した上で、実環境での検証に協力いただける検証協力ユーザを公募することが望まれる。種別 B の検証の進め方、そして検証協力ユーザの関与の仕方については、今後も議論が必要である。

6.2 市場参入促進の仕組みの検討について

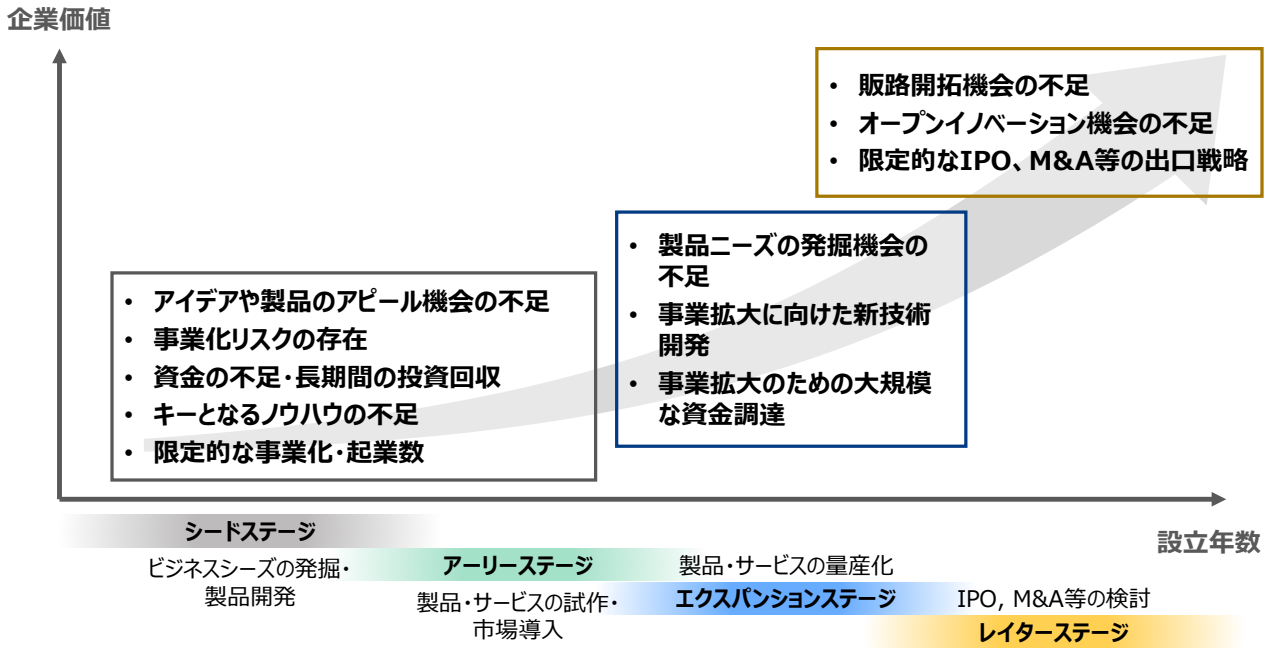
検証基盤を含む市場参入促進の仕組みを検討した。今年度事業においては、特に昨年度調査でスタートアップ企業等の要望の多かった、SI 事業者や販社など市場へのチャネル上に居る役割（企業等）とのマッチング機会の創出に焦点を絞り、市場参入促進の仕組みのゴール像を作成した。加えて、ゴール実現までのロードマップ案を作成した。本事業で作成したロードマップ案に基づき、「集中的なマッチング機会」と「継続的なマッチング機会」の両方を並行して実施することが望まれる。なお、各取組はスモールスタート的に始めつつ、段階的に取組を拡大することで、マッチング機会創出に関するゴール像に徐々に近付けることが必要である。各取組の推進にあたっては、本検証基盤だけでなく、関連する業界団体等のステークホルダーとの連携が必要不可欠である。今後、各取組の具体的な推進に向け、関係するステークホルダーとの調整を行うことが望まれる。

以降では、市場参入促進の仕組み検討を通じて得られた結果を踏まえ、今後望まれる方向性について考察する。取組②として、市場参入促進に向けた表彰の付与について言及したが、具体的な表彰のあり方についてはより詳細な検討が必要である。より具体的には、表彰の位置づけ、表彰付与の主体、詳細な表彰の観点等について詳細な検討を継続する必要がある。今年度の調査では、表彰の観点について、欧州 ECSO の European Cybersecurity STARtup Award を参考に検討したが、今後、諸外国の取組だけでなく、日本の商習慣や国民性も考慮した検討が望まれる。

また、国内セキュリティ製品ベンチャー等の市場参入を促進する観点では、国内の SI 事業者や販社とのマッチング機会を創出するだけでなく、海外展開の支援も検討することが望まれる。具体的な支援策として、海外ユーザ企業とのマッチング支援、海外アクセラレータとのマッチング支援、海外セキュリティカンファレンスへの参加支援等が考えられる。これらの支援についても、前述と同様に本検証基盤だけでの支援は困難であるため、RSA Conference に日本パビリオンの

出展を支援している JNSA やスタートアップ企業の海外進出を支援している JETRO 等、海外ビジネスに知見を有したステークホルダーと連携することが望まれる。

今年度の調査においては、セキュリティ製品ベンチャー等と SI 事業者や販社など市場へのチャネル上に居る役割とのマッチング機会の創出に焦点を絞り、ゴール像及びロードマップ案の作成を行ったが、幅広いステージのセキュリティ製品ベンチャー等の市場参入促進のためには、マッチング機会の創出に限らず、製品のテスト支援やビジネス的側面での支援等、様々な取組を実施することが必要である。図 21 に示すとおり、セキュリティ製品ベンチャー等が抱える主な課題はベンチャー等のステージによって異なり、例えばシードステージからアーリーステージのベンチャー等であれば、アイデアや製品のアピール機会が不足する一方で、エクスパンションステージ以降では、製品ニーズの発掘機会の不足や販路拡大機会の不足が課題となる。



出所）ヒアリング結果及び内閣官房「「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」[21]等に基づき三菱総合研究所作成

図 21　セキュリティ製品ベンチャー等が抱える代表的な課題（ステージ別）

本事業で実施した有効性検証の主な対象は、製品が完成しているエクスパンションステージ以降のベンチャー等となるが、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等に対しても市場参入促進の仕組みが必要である。ここで、幅広いステージのセキュリティ製品ベンチャー等の市場参入促進のためには、製品に対する技術的な有効性検証だけではなく、ビジ

[21] https://www.kantei.go.jp/jp/singi/keizaisaisei/venture_challenge2020/venture_challenge/dai1/siryou1.pdf

ネス的支援を講じることが望まれる。すなわち、技術的な支援だけでなく、セールスやマーケティングの観点も含めたビジネス面での支援が望まれる。他方、本検証基盤のみでビジネス面での支援は困難であるため、成功したベンチャー等と連携して事業ノウハウ等を抽出するとともに、中小機構や業界団体等と連携し、具体的なビジネス的支援策についても検討することが望まれる。今後、シードステージやアーリーステージも含めたベンチャー等に対してヒアリングを行い、具体的にどのようなビジネス的支援が必要かを抽出するとともに、支援にあたって協力可能なステークホルダーとの連携を検討することが望まれる。

付録A.重要分野マップの見直し結果

＜重要分野＞①脅威の可視化、 **②リスクの可視化・緩和**、 ③IT資産管理、 ④脅威インテリジェンスの整理・管理、 ⑤マルウェア感染/発症の重篤度判定、 ⑥教育・トレーニング、 ⑦ハイレベルセキュリティ検証、⑧IT資産の認証/検証、**⑨データ保護、⑩ID/アクセス管理**

組織に対するサイバーセキュリティ脅威(*) ＼ 対策が必要なプロセス	資産管理			リスク管理・緩和				防御		監視・検知				対応・復旧				教育・訓練
	IT資産管理	**ID/アクセス管理**	**IT資産の認証/検証**	脆弱性管理	**リスクアセスメント**	**リスク緩和**	テスト(ペネトレーションテスト等)	境界防御	**データ保護(暗号化)**	クラウド/サーバ	ネットワーク	エンドポイント	リアルタイム検知	インシデントレスポンス	分析(フォレンジック)	復旧	サイバー保険	
標的型攻撃による機密情報の窃取			○	○					○			○		○				○
内部不正による情報漏えい		○							○	○		○		④	○			⑥
ランサムウェアによる被害			○									○	○	○			○	○
サプライチェーンの弱点を悪用した攻撃による情報漏えい	○		○	○	○					○			⑤				○	
テレワーク等のニューノーマルな働き方を狙った攻撃	○		○		○				○			○						○
ビジネスメール詐欺による金銭被害					○							○		○			○	○
予期せぬIT基盤(クラウド、データセンター)の障害に伴う業務停止	③								⑨							○	○	○
不注意による情報漏えい	○	⑩	⑧		②				○		①	○						○
Web上サービスからの個人情報窃取				○	○				○	○				○				
DDoS攻撃によるサービス停止					○			○		○	○					○		
利用しているオープンソースソフトウェアの脆弱性による不正アクセス、情報漏えい	○			○	○								○	○				
IoT機器のBot化などの不正利用、情報漏えい	○		○	○	○		○ ⑦						○					
制御系システムへの攻撃による製造ライン停止				○	○		○					○	○					
シャドーITによる不正アクセス、情報漏えい	○	○	○		○					○			○					
インターネット上のサービスへの不正ログイン		○		○	○						○						○	

(*)：IPA が 2021 年 1 月 27 日に公開した「情報セキュリティ 10 大脅威 2021(https://www.ipa.go.jp/security/vuln/10threats2021.html)」の組織編に上げられた脅威に、制御システムへのサイバー攻撃など組織として対策すべき事項を付け加えた。

図 22　重要分野マップの見直し結果

付録B.Karma（種別 A）の検証項目・検証方法

表 27　Karma（種別 A）の検証項目・検証方法

検証項目				検証対象の有する新規性の高いセキュリティに関する機能			検証方法		
分類	No.	区分	検証項目	IoT機器の正しい情報を検出できること	セキュリティリスクのあるIoT機器を検出できること	日本語検索が可能であること	実検証 検証環境での実検証	データ データや記録に基づく評価	ヒアリング ベンダヒアリングに基づく評価
リスクの検出	1-1	リスクの検出	IoT機器の正しい情報を検出できること	✓			✓	✓	
	1-2		セキュリティリスクのあるIoT機器を検出できること		✓		✓	✓	
	1-3		日本語の文字列を含んだ検索ができること			✓	✓		
	1-4		インターネット経由でIoT機器の検出ができること	✓	✓	✓	✓		
	1-5		条件を絞り込んだ検索ができること	✓	✓	✓	✓		
	1-6		検出にかかる時間が一般的な許容範囲内であること	✓	✓	✓	✓		
	1-7		古いIoT機器におけるリスクの検出ができること	✓	✓		✓	✓	
	1-8		新たに製品化されたIoT機器が検出できること	✓			✓	✓	✓
	1-9		新たに発見された脆弱性が検出できること		✓		✓	✓	✓
検出したリスクの可視化・管理	2-1	検出したリスクの管理	検出したリスクの統計情報表示ができること		✓		✓		
	2-2	検出したリスクの表示	検出したリスクの絞り込み表示ができること	✓	✓	✓	✓		
	2-3		結果のエクスポートができること	✓	✓	✓	✓		
検出仕様	3-1	検出仕様	検出の手法として不正アクセス禁止法に抵触しない方法で情報を取得していること	✓	✓			✓	✓
	3-2		検出の手法として倫理的に問題ない方法で情報を取得していること	✓	✓			✓	✓
誤検出・検出漏れ	4-1	誤検出・検出漏れ	誤検出率が一般的な許容範囲内であること	✓	✓		✓	✓	✓
	4-2		検出不能率が一般的な許容範囲内であること	✓	✓		✓	✓	✓
その他	5-1	認証	不正ログイン対策がされていること				✓		✓
	5-2	データ保持	取得データの所在地（リージョン）が日本国内であること					✓	✓
	5-3		プライバシーポリシー（個人情報保護方針）を明記していること				✓	✓	✓

付録C.AeyeScan（種別 B）の検証項目・検証方法

表 28　AeyeScan（種別 B）の検証項目・検証方法

検証項目				検証対象の有するセキュリティに関する優れたユーザビリティ項目				検証方法			
分類	No.	区分	検証項目	① 機能充足性：AI,RPA技術を活用した自動クローリング能力	② 機能正確性：画面クローリング性能（範囲、深度）	③ 効率性・運用操作性：脆弱性の検出箇所を視覚的に分かりやすくレポート	④ 習得性：設定項目が少なく、操作が容易	実検証 検証環境での実検証	ヒアリング(検証協力ユーザ) 検証協力ユーザに対するヒアリングに基づく評価	データ データや記録に基づく評価	ヒアリング(ベンダ) ベンダヒアリングに基づく評価
機能充足性	1-1	監視、検知、通知	「IPAの安全なWebサイトの作り方」等のガイドラインに列挙される脆弱性項目が対象に含まれていること	✓						✓	
	1-2		リンクから辿れないページは手動で分析可能であること	✓				✓			
	1-3	自動分析	AIやRPAによるフォーム自動入力値が正しいこと	✓				✓			✓
	1-4		分析時の画面遷移は自動的に実行されること	✓				✓		✓	
機能正確性	2-1	検知の正確性	「IPAの安全なWebサイトの作り方」等のガイドラインに列挙される脆弱性が検出されること		✓			✓	✓	✓	
	2-2		自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していること		✓			✓			
効率性・運用操作性	3-1	レポーティング	脆弱性の検出箇所を視覚的に分かりやすくレポートできること			✓		✓	✓		
	3-2	操作性	人間による操作時間を計測し、妥当な時間内に完了していること			✓		✓	✓	✓	
	3-3		CIツール等と連携し、診断の自動化可能であること。			✓		✓		✓	
	3-4		運用操作性について検証協力ユーザーの観点から良好であること			✓		✓	✓		
習得性	4-1	習得性	初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していること				✓	✓	✓		
	4-2		マニュアル、サポートデスクの提供により理解・習得が容易であること				✓	✓	✓		
	4-3		習得性について検証協力ユーザーの観点から良好であること				✓	✓	✓		
その他	5-1	認証	多要素認証によりユーザー認証ができること	✓				✓			✓
	5-2	データ保持	取得データの所在地（リージョン）が日本国内であること	✓							✓
	5-3		プライバシーポリシー（個人情報保護方針）を明記していること	✓						✓	

セキュリティ製品の有効性検証の検証結果について

株式会社ゼロゼロワン　「Karma」

独立行政法人情報処理推進機構

令和 4 年 3 月

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
AP	Access Point の略で、通信ネットワークの末端でコンピュータなどからの接続要求を受け付け、ネットワークへの通信を仲介する施設や機器のこと。
ASN	AS を識別するために割り当てられる番号のこと。AS とは、ひとつのルーティングポリシー配下にある IP ネットワークの集合のことをいう。
CIDR 表記	CIDR とは、Classless Inter-Domain Routing の略で、IP アドレスのクラスを使用せず、IP アドレスのネットワーク部・ホスト部の桁数を自由に決めることができるようにした仕組みのこと。CIDR 表記とは、IP アドレスの範囲を表記する方法のひとつで、「先頭アドレス/ネットワーク部のビット数」という表記のこと。
CSIRT	Computer Security Incident Response Team の略。セキュリティ上の問題が発生した場合に原因解析などの対応を行う組織のこと。
ICS	Industrial Control System の略で、電力、ガス、水道、鉄道等の社会インフラや、石油、化学、鉄鋼・自動車・輸送機器、精密機械、食品、製薬、ビル管理等の工場・プラントにおける監視・制御や生産・加工ラインにおいて用いられている制御システムのこと。
IoT	Internet of Things の略。直訳すると、モノのインターネットという意味であり、コンピュータだけでなくあらゆるモノをインターネットに接続して相互通信すること。
ISP	Internet Service Provider の略。一般的にはプロバイダーとも呼ばれる。
JSON	JavaScript Object Notation の略で、軽量なテキストベースのデータ交換用フォーマットでありプログラミング言語を問わず利用できるデータ記述言語であり、名称と構文は JavaScript におけるオブジェクトの表記法に由来するもの。
JVN	Japan Vulnerability Notes で、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報のポータルサイトのこと。
Mirai 亜種	Mirai とは、2016 年に発見された IoT 機器を主な標的としたマルウェアのこと。Mirai 亜種とは、Mirai と似た動作や構造を有し、Mirai と同様に IoT 機器を主な標的としたマルウェアの総称のこと。
NICT	国立研究開発法人情報通信研究機構のこと。
OSINT	Open Source INTelligence の略。特定の情報要件に対処する目的で、一般に入手可能な情報を収集し、利用し、適切な対象者に適時に普及させた情報のこと。

用語	概要
SaaS	Software as a Service の略。ソフトウェアをサービスとして利用できるようにしたもの。
S/N	Serial Number の略で、ある決まった個々の識別をするために割り当てられる、一意の整数のこと。
UTM	Unified Threat Management の略で、マルウェアやハッキングなどの脅威からコンピュータネットワークを効率的かつ包括的に保護する管理手法のこと。
Whois 情報	ドメインや IP アドレスの所有者の情報のこと。
エクスポート	コンピュータでソフトウェアなどからデータを出力すること。
グローバル IP アドレス	インターネットに直に接続された機器に割り当てられる IP アドレスのこと。
クローリング	プログラムを使って Web サイトの情報を自動収集すること。
シグネチャ	本報告書では、株式会社ゼロゼロワンが独自開発した IoT 機器の判別パターンのこと。
スキャン	攻撃・侵入の前段階に行われる、標的サイトの各ポートにおけるサービスの状態の調査のこと。
セキュリティタグ	株式会社ゼロゼロワンがそれぞれの IoT 機器について公開されている情報を収集し、セキュリティ情報としてシグネチャと関連付けた情報のこと。セキュリティリスクレベルの判定の根拠ともなる。
ゼロデイ	セキュリティの脆弱性を解消する手段がなく脅威にさらされる状態のこと
バナー情報	サービスが出力するメッセージの中で、ソフトウェア名称やバージョン情報などに関する情報のこと。
ファームウェア	コンピュータや電子機器などに内蔵されるソフトウェアの一種で、本体内部の回路や装置などの基本的な制御を司る機能を持ったもの。
踏み台	踏み台とは、攻撃者がサーバを攻撃する際に、攻撃拠点として利用するサーバ(既に攻撃者によって侵入されているサーバ)のこと。
プロトコル	通信に関する規格のこと。
ポート	TCP/IP において、トランスポート層のプロトコル（TCP 及び UDP）で用いられる、0 から 65535 までの番号が付与された論理的な情報の送受信口のこと。
ボットネット	マルウェアによって乗っ取られた複数のコンピュータで構成されるネットワークのこと。
ホスト	コンピュータネットワークに接続されたコンピュータ、デバイスのこと。
マルウェア	コンピュータの正常な利用を妨げ、利用者やコンピュータに害をなす不正な動作を行うソフトウェアのこと。
ルーター	コンピュータネットワークの中継・転送機器の一つで、データの転送経路を選択・制御する機能を持ち、複数の異なるネットワーク間の接続・中継に用いられるもののこと。

1. はじめに

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）では、信頼できるセキュリティ製品・サービスとセキュリティに関する隠れたニーズとを掘り起こし、それらの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。新型コロナウィルス感染拡大を契機に急速にデジタル化・IT 化への期待が進む一方で、サイバー攻撃は衰えることなく、その対策としてセキュリティ製品の活用が求められている。国内では現在、セキュリティ製品の多くが海外製品で占められているが、日本で開発された新たなセキュリティ製品の市場参入を促進するためには、サイバー攻撃の脅威や対策動向等を踏まえ、今後重要度が増すと考えられる製品分野を明らかにする必要がある。加えて、その分野に該当する国産のセキュリティ製品に対し、有効性検証・実環境における試行導入検証を実施しその内容を発信することが、ユーザの国産製品選定を容易にすると考えられる。

これを受けて独立行政法人情報処理推進機構（以下、IPA）は、実際にセキュリティ製品を検証し、結果を公表する「セキュリティ製品の有効性検証」の仕組みの構築を行った。これにさきがけて、2019 年 9 月に立ち上げた「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（以下、有識者会議）」において、検証の具体的な試行を行うこととし、検証対象となる製品分野、検証方法などにおける課題やあるべき姿を抽出することを目的に試行的な検証を行ってきた。

今年度は、昨年度構築した基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を実施した。有識者会議の検討において、今年度は「脅威の可視化」、「リスクの可視化・緩和」、「データ保護」、「ID/アクセス管理」に係る製品分野を検証対象とすることを方針とするとともに、以下の 2 種類の製品種別（種別 A/種別 B）を対象に検証を実施することとした。

[種別 A]

日本の市場において新規性の高いセキュリティに関する機能を有する製品とする。種別 A に応募する応募者は応募書類の中で、上記に該当する機能があることを説明するものとし、上記に該当する機能が応募書類等の説明内容通りであることを検証する対象とする。

[種別 B]

セキュリティ機能に関する優れたユーザビリティを備えた製品とする。種別 B に応募する応募者は応募書類の中で、該当するユーザビリティを明記するものとし、種別 B の製品は、上記に該

当するユーザビリティが応募書類の説明内容通りであることを、検証する対象とする。

本報告書は、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有効性検証を行った結果を報告するものである。今年度は種別 A・種別 B について、それぞれ 1 製品を選定し、検証を実施した。以下では、種別 A にて選定した株式会社ゼロゼロワン(以下、製品ベンダ)の「Karma」を対象に実施した有効性検証の検証結果について示す。

2. 検証対象製品について

2.1 検証対象製品を取り巻く環境

近年、IoT 機器を狙ったサイバー攻撃は増加傾向にあり、NICT サイバーセキュリティ研究所がまとめた「NICTER 観測レポート 2019(※１)」によると、2019 年に観測されたサイバー攻撃関連の通信は 2018 年と比較して約 1.5 倍に増加したと報告された。その内およそ半数がウェブカメラやホームルーターなど IoT 機器で動作するサービスや脆弱性を狙った攻撃であった（調査目的のスキャンパケットを除く)。さらに、IoT マルウェアの一種である「Mirai 亜種」が機能を拡張し、攻撃活動を進化させていく様子がダークネット観測で確認されたと報告があった。

（※１） NICTER 観測レポート 2019
（https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf）

引用元: IoT 機器の情報を可視化する SaaS 型の検索エンジン「Karma」の正式版を提供開始｜株式会社ゼロゼロワンのプレスリリース
(https://prtimes.jp/main/html/rd/p/000000002.000054541.html)

2.2 製品概要

製品ベンダは設立当初より、総務省と NICT が取り組む「NOTICE(※1)」との連携、ファームウェア解析を通じた IoT 機器のセキュリティ検証に取り組んできた。IoT 機器の脆弱性や IoT 機器を狙うマルウェアなどによって、利用者が知らないうちに被害者や加害者になることのないよう、安心して IoT 機器を使える世の中にしたいという思いから Karma の開発に至った。

Karma は IoT 機器を検索するためのエンジンである。ポート、IP アドレス、バナー情報、WHOIS 情報を個別または組み合わせることによって、日本国内のあらゆる IoT 機器を検索することができる。また、製品ベンダが独自開発したシグネチャ・セキュリティタグを用いた検索を行うことで、より詳細な結果を得ることができる。加えて、日本語を含む文字列を検索することも可能である。

次のような活用例を想定している。

- 特定の IoT 機器について、どの程度使用されているか確認したい。
- 特定の IoT 機器についてファームウェアバージョンの傾向を知りたい。(※2)
- ニュースで報じられた IoT 機器のボットネットに使用されているポートについて、どのように分布しているのか確認したい。
- 自社が管理しているグローバル IP アドレスにおいて、意図せず IoT 機器が外部公開されていないか確認したい。
- 自社で導入を予定している IoT 機器が、他社で使われている実績があるか確認したい。
- 踏み台になり得る IoT 機器が自社に存在しないか、またどのように分布しているかを確認したい。

(※1)NOTICE（National Operation Towards IoT Clean Environment）は、総務省、NICT 及びインターネットプロバイダが連携し、IoT 機器へのアクセスによる、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組である。（平成 31 年 2 月 20 日（水）より実施）

（※2）原則としてシグネチャが開発されている IoT 機器のみでの対応となる。シグネチャは随時開発している。

2.3 製品の導入事例

2.3.1 大手 IoT 機器メーカーでの導入事例

大手 IoT 機器メーカーが自社製品を市場投入した後、ファームウェアのアップデートがどのように実施されているか状況を把握したいという要望があり、Karma が採用された。Karma を活用することによって、ファームウェアアップデートを含めた製品の様々な使用状況を可視化することができた。こうして得られたデータは、安全な製品の開発のための参考情報として活用された。

2.3.2 大手 ISP 事業者での導入事例

大手 ISP 事業者の CSIRT において、インターネット上で利用されている IoT 機器及びその利用状況を調査したいという要望があった。独自開発のシグネチャ・セキュリティタグを用いて効率的に調査・対処が可能なことから、Karma が採用された。

3. 検証する新規性の高いセキュリティに関する機能・検証項目

3.1 検証する新規性の高いセキュリティに関する機能

Karma の新規性の高いセキュリティに関する機能とされる事項のうち、本検証では以下の 3 つの事項に対して検証を実施した。

（1） IoT 機器の正しい情報を検出できること

今までの IoT 機器検索エンジンではバナー情報から機器を推測することしかできなかったが、本サービスでは、製品ベンダがそれぞれの IoT 機器の特徴となるものを独自のシグネチャ及びセキュリティタグ（サポート期間が終了している、初期の認証情報が公知である等）として開発し、バナー情報と組み合わせることで、不正な通信を行うことなく特定の IoT 機器を検索することができる。

（2） セキュリティリスクのある IoT 機器を検出できること

それぞれの IoT 機器に付与されるセキュリティタグを検索することで、セキュリティリスクのある IoT 機器や、特定の IoT 機器においてセキュリティリスクのあるものだけを抽出することができる。

（3） 日本語検索が可能であること

海外の IoT 機器検索エンジンでは実現されなかった日本語検索を可能とし、検索結果に含まれる日本語も文字化けせずに表示することができる。

3.2 検証項目・検証方法

3.2.1 検証項目・検証方法の策定方針

検証項目・検証方法の策定方針は以下のとおりとした。

- 検証項目・検証方法の策定期間を可能な限り短縮するために、製品決定前に検証項目マスターリスト及び検証方法マスターリストを策定する。
- 検証対象製品が決定次第、検証実施者、製品ベンダと協議し、検証項目マスターリストの

項目を具体化して検証項目を策定する。

- 検証実施にあたって、可能な限り「検証環境での実検証」を重視するが、定量的な評価を裏付けるために「データや記録に基づく評価」も併用する。
- 客観性が損なわれる可能性がある「ベンダヒアリングに基づく評価」は、実検証やデータや記録に基づく評価が困難な場合の例外的措置として位置付ける。
- 策定した検証項目・検証方法は有識者による確認・審議をもって確定とする。

3.2.2 検証項目・検証方法の策定結果

Karma の新規性の高いセキュリティに関する機能を検証するための検証項目を策定した。検証項目は、検証のための 5 つの分類（「リスクの検出」、「検出したリスクの可視化・管理機能」、「検出仕様」、「誤検出・検出漏れ」、「その他」）から具体化したものである。各検証項目に対して、3 つの検証方法（「検証環境での実検証」、「データや記録に基づく評価」、「ベンダヒアリングに基づく評価」）のうち、どの方法で検証を行うか決定した。

(1) 「リスクの検出」に関する検証項目・検証方法

Karma の新規性の高いセキュリティに関する機能とされる事項を踏まえ、「リスクの検出」に関して、表 3-1 に示す検証項目を決定した検証方法で検証した。

表 3-1 「リスクの検出」に関する検証項目・検証方法

検証項目			検証方法		
No.	区分	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
1-1	リスクの検出	IoT 機器の正しい情報を検出できること	✓	✓	
1-2		セキュリティリスクのある IoT 機器を検出できること	✓	✓	
1-3		日本語の文字列を含んだ検索ができること	✓		

1-4		インターネット経由で IoT 機器の検出ができること	✓		
1-5		条件を絞り込んだ検索ができること	✓		
1-6		検出にかかる時間が一般的な許容範囲内であること	✓		
1-7		古い IoT 機器におけるリスクの検出ができること	✓	✓	
1-8		新たに製品化された IoT 機器が検出できること	✓	✓	✓
1-9		新たに発見された脆弱性が検出できること	✓	✓	✓

(2) 「検出したリスクの可視化・管理」に関する検証項目・検証方法

Karma の新規性の高いセキュリティに関する機能とされる事項を踏まえ、「検出したリスクの可視化・管理」に関して、表 3-2 に示す検証項目を決定した検証方法で検証した。

表 3-2 「検出したリスクの可視化・管理」に関する検証項目・検証方法

検証項目			検証方法		
No.	区分	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
2-1	検出したリスクの管理	検出したリスクの統計情報表示ができること	✓		
2-2	検出した	検出したリスクの絞り	✓		

	リスクの表示	込み表示ができること			
2-3		結果のエクスポートができること	✓		

(3) 「検出仕様」に関する検証項目・検証方法

Karma の新規性の高いセキュリティに関する機能とされる事項を踏まえ、「検出仕様」に関して、表 3-3 に示す検証項目を決定した検証方法で検証した。

表 3-3 「検出仕様」に関する検証項目・検証方法

検証項目			検証方法		
No.	区分	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
3-1	検出仕様	検出の手法として不正アクセス禁止法に抵触しない方法で情報を取得していること		✓	✓
3-2		検出の手法として倫理的に問題ない方法で情報を取得していること		✓	✓

(4) 「誤検出・検出漏れ」に関する検証項目・検証方法

Karma の新規性の高いセキュリティに関する機能とされる事項を踏まえ、「誤検出・検出漏れ」に関して、表 3-4 に示す検証項目を決定した検証方法で検証した。

表 3-4 「誤検出・検出漏れ」に関する検証項目・検証方法

検証項目			検証方法		
No.	区分	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
4-1	誤検出・検出漏れ	誤検出率が一般的な許容範囲内であること	✓	✓	✓
4-2		検出不能率が一般的な許容範囲内であること	✓	✓	✓

(5) 「その他」に関する検証項目・検証方法

Karma の新規性の高いセキュリティに関する機能とされる事項を踏まえ、「その他」に関して、表 3-5 に示す検証項目を決定した検証方法で検証した。

表 3-5 「その他」に関する検証項目・検証方法

検証項目			検証方法		
No.	区分	検証項目	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
5-1	認証	不正ログイン対策がされていること	✓		✓
5-2	データ保持	取得データの所在地（リージョン）が日本国内であること		✓	✓
5-3		プライバシーポリシー（個人情報保護方針）を明記していること		✓	✓

4. 検証環境・検証条件

4.1 検証環境

検証環境は(1)インターネット上に公開されている IoT 機器を検索するための検証環境及び(2)検証実施者が調達した IoT 機器を検索するための検証環境の 2 環境を構築した。環境(1)では、Karma を利用して検索機能や結果表示に関する検証を実施した。環境(2)では、上述の環境(1)では実施困難な正確性の検証(検索結果と実際の IoT 機器との照合)を補完的に実施した。

このように 2 段階で検証を実施した理由は次の通りである。

環境(1)での検索結果は OSINT 情報源が過去にインターネット上をクローリングして収集した情報が基になっているため、検索結果と実際の IoT 機器を照合して正確性を評価することが困難である。また、検証実施者が検証用の IoT 機器をインターネットに公開しても、OSINT 情報源のクローリング(タイミングは OSINT 情報源に依存)の結果が Karma 独自のデータベースに反映されるまでタイムラグが生じるため、効率的な検証実施が困難である。加えて、脆弱性のある IoT 機器をインターネットに公開するリスクも生じる。

このような問題を補完するため、社内ネットワーク上に構築した環境(2)を使ってシグネチャ・セキュリティタグの正確性検証を効率的に実施した。

(1) インターネット上に公開されている IoT 機器を検索するための検証環境

図 4-1 で示すとおり、社内ネットワークに検証用 PC を用意し、Web ブラウザからインターネット経由で Karma を利用する環境を構築した。

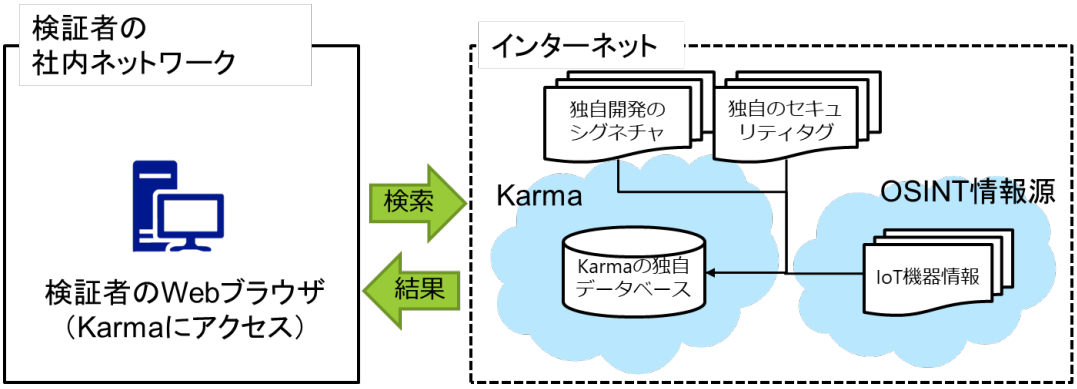


図 4-1 インターネット上に公開されている IoT 機器を検索するための検証環境

Karma の利用にあたって、製品ベンダからアカウント情報の提供を受け、Web ブラウザ上の検索画面から IoT 機器の検索を実行した。

これにより、インターネット上の IoT 機器情報が検索できることを、検索ヒット件数等から確認した。

(2) 検証実施者が調達した IoT 機器を検索するための検証環境

図 4-2 のイメージで示すとおり、社内ネットワークに検証実施者が調達した IoT 機器を設置し、直接収集したバナー情報等から Karma のシグネチャ・セキュリティタグで検索する環境を構築した。

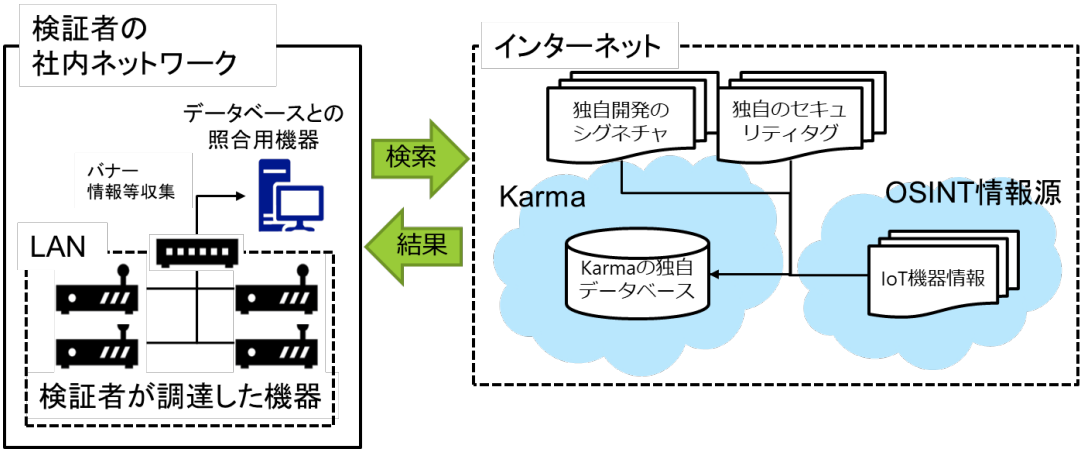


図 4-2 検証実施者が調達した IoT 機器を検索するための検証環境のイメージ

これにより、Karma 独自のシグネチャ及びセキュリティタグの正当性を IoT 機器個別に確認した。

このような環境を構築したのは、本章の冒頭で述べた通り、調達した IoT 機器をインターネット上に公開してから、OSINT 情報源からのクローリングを受けて Karma のデータベースに登録されるまでにリードタイムがあり、ファームウェアアップデート前後での結果比較等が困難な点が大きい。そこで、データベースとのシグネチャ照合用機器において IoT 機器のバナー情報等を直接収集し、即時に Karma データベースでの検索を実施できるようにした。なお、シグネチャ照合用機器が収集する情報は OSINT 情報源が収集するものと同様のものとし、検索結果に差が生じないように留意した。

4.2 検証条件

4.1 でも述べた通り、検証は(1) インターネット上に公開されている IoT 機器を検索するための実検証及び(2)検証実施者が調達した IoT 機器を検索するための実検証の 2 段階で実施した。

各検証個別の条件を次に示す。

(1) インターネット上に公開されている IoT 機器を検索するための実検証

図 4-1 の検証環境で実際に Karma を利用してインターネット上の IoT 機器を検索し、検索結果を確認した。

(2) 検証実施者が調達した IoT 機器を検索するための実検証

図 4-2 の検証環境で、Karma の正確性について以下の条件で検証した。

- 現行の IoT 機器製品を検証実施者が調達し、Karma のデータベースで特定可能であることを証明する。
- 機器の絶対数の多い家庭用ルーターに対して、日本市場でシェア上位メーカーの現行製品を調査する。
- 製品ベンダに対し、調達した製品名の事前告知はしない。
- 現行製品の中で脆弱なもの、比較的セキュアなもの等、複数のパターンを検討する。
- ファームウェアがアップデートされないまま残されている可能性のある 2,3 年前の製品を検討する。
- 検証実施者で現行製品を複数機種購入し、社内ネットワークに設置する。
- シグネチャとセキュリティタグの正確性を検証するために社内ネットワーク環境で検証をする。
- Karma のデータベースで調達した IoT 機器を検索し、情報がどこまで取得可能かを検証する。
- 脆弱性については JVN を情報比較先とし、Karma の検索結果の情報が正当かを検証する。
- 社内ネットワーク内でファームウェアをアップデートすることで検索結果の前後比較を実施する。

この条件のもと、検証実施者で調達した IoT 機器については、その選定理由とともに表 4-1 に示す。

表 4-1 調達した IoT 機器と選定理由

説明	調達機器 1	調達機器 2	調達機器 3	調達機器 4
タイプ	ルーター	ルーター	ルーター	ルーター
メーカー	「メーカーA」	「メーカーB」	「メーカーC」	「メーカーD」
シリーズ	「シリーズ A」	「シリーズ B」	「シリーズ C」	「シリーズ D」
モデル	「モデル A」	「モデル B」	「モデル C」	「モデル D」
発売年	2019 年	2021 年	2018 年	2018 年
選定理由	国内上位のシェアを持つメーカーから、比較的売上シェアの高いモデルを選定した。	国内上位のシェアを持つメーカーから、比較的発売時期の新しいモデルを選定した。	国内上位のシェアを持つメーカーから、比較的売上シェアの高いモデルを選定した。	国内上位のシェアを持つメーカーから、比較的売上シェアの高いモデルを選定した。

検証条件でも述べている通り、すべて家庭用ルーターを調達して比較検証を行ったが、Karma はカメラ、プリンター等、他の様々な IoT 機器についても対応している(詳細は表 5-4 を参照)。

5. 検証結果

5.1 「リスクの検出」に関する検証結果

5.1.1 検証項目 1-1 の検証結果

(1) 検証項目の内容

IoT 機器の正しい情報を検出できること。

(2) 検証結果

Karma で特定の IoT 機器を検索し、その検索結果の内容が正しいことを確認した。

(3) 検証内容の詳細

本検証項目は実検証及びデータや記録に基づく評価により実施した。

実検証では①インターネット上に公開されている IoT 機器の検索と、②検証実施者が調達した IoT 機器による正確性検証の 2 段階で確認した。①では、メーカー名及び IoT 機器製品名を指定して検索が可能なこと、結果の一覧及び詳細が表示されることを確認した。②では、実際の IoT 機器と Karma の検索結果を照合することで、①で確認困難な検索結果の正確性について確認した。

1) 実検証①(インターネット上に公開されている IoT 機器の検索)

Karma で特定メーカーの特定 IoT 機器製品名による検索を行った。

メーカーが「メーカーA」かつ、モデルが「モデル A」の IoT 機器を指定した検索式で検索を行った。これにより、指定したメーカーかつモデルの IoT 機器が検索され、結果が表示されることを確認した。

検索式: vendor:メーカーA model:モデル A

図 5-1 のとおり、検索結果が表示された。

図 5-1 特定メーカーの特定 IoT 機器製品名による検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

また、一覧の中から特定の機器を選択して詳細結果を表示した。(図 5-2)

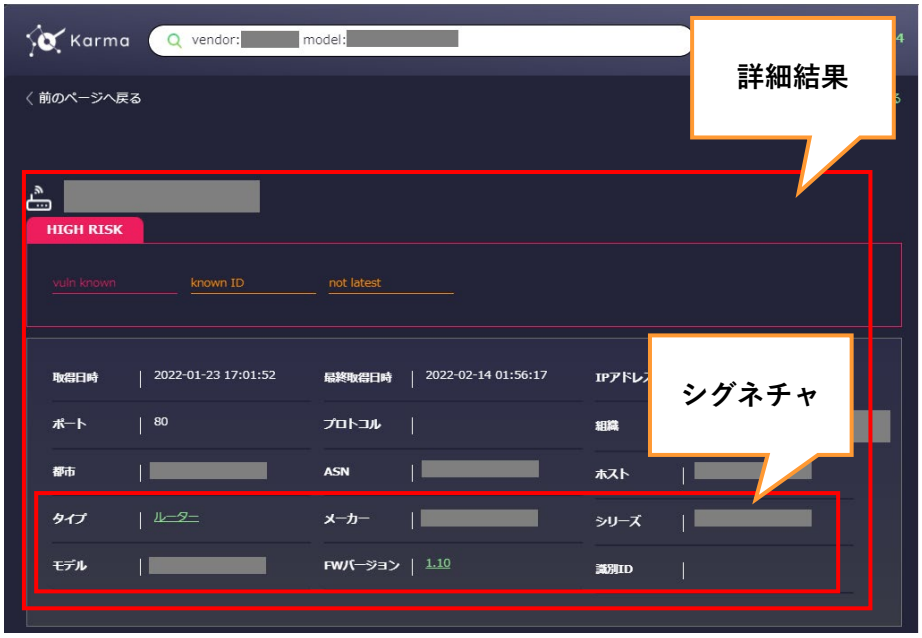


図 5-2 特定メーカーの特定 IoT 機器製品名による検索の詳細結果画面

IoT 機器のタイプ、メーカー、シリーズ、モデル、ファームウェアバージョンが表示されることを確認した。1 点、図 5-2 では「識別 ID」が空欄となっているが、バナー情報及びその他の情報から S/N 等の固有 ID を判別できないモデルの IoT 機器であるためである。これは Karma の仕様によるもので、一部の IoT 機器ではバナー情報及びその他の情報から識別 ID を判別できない場合がある。

図 5-2 のそれぞれの項目の内容については表 5-1 に示す。

表 5-1 詳細情報の項目の説明

詳細情報の項目	説明
取得日時	データを取得した最初の日時
最終取得日時	データを取得した最新の日時
IP アドレス	グローバル IP アドレス
ポート	ポート番号
プロトコル	推測されるプロトコル
組織	グローバル IP アドレスを管理する組織名
都市	都市名
ASN	AS 番号
ホスト	ホスト名
タイプ	IoT 機器の種別

メーカー	IoT 機器のメーカー
シリーズ	IoT 機器の製品シリーズ
モデル	IoT 機器の製品モデル
FW バージョン	IoT 機器のファームウェアバージョン
識別 ID	IoT 機器が持つ固有の ID
バナー情報	IoT 機器が応答したバナー情報の内容

2） 実検証②(検証実施者が調達した IoT 機器による正確性検証)

検証実施者が調達した IoT 機器に対し、Karma のデータベースによる検索を行った。

該当の IoT 機器について正しく判定され、検索が正確なものであることを確認した。(詳細については 5.6 章参照)

表 5-2 に、IoT 機器と検索結果の照合結果を抜粋する。

表の中で 1 点、調達機器 4 についてのみファームウェアバージョンが「unknown」と表示されているが、シグネチャにバージョン情報を持たない IoT 機器であり、想定通りの動作であることを製品ベンダから確認した。これは、一部の IoT 機器ではファームウェアバージョンによってバナー情報等に差異がみられないなどの理由で、バージョン情報を規定できないためである。

表 5-2 シグネチャについての正確性（調達 IoT 機器の説明）

説明	調達機器 1	調達機器 2	調達機器 3	調達機器 4
メーカー	「メーカーA」	「メーカーB」	「メーカーC」	「メーカーD」
シリーズ	「シリーズ A」	「シリーズ B」	「シリーズ C」	「シリーズ D」
モデル	「モデル A」	「モデル B」	「モデル C」	「モデル D」
ファームウェアバージョン	最新の 2 世代前	最新の 1 世代前	最新版	最新版

表 5-3 シグネチャについての正確性（シグネチャによる判定）

シグネチャ	調達機器 1	調達機器 2	調達機器 3	調達機器 4
VENDOR	「メーカーA」	「メーカーB」	「メーカーC」	「メーカーD」
SERIES	「シリーズ A」	「シリーズ B」	「シリーズ C」	「シリーズ D」
MODEL	「モデル A」	「モデル B」	「モデル C」	「モデル D」
VERSION	最新の 2 世代前	最新の 1 世代前	最新版	unknown(※1)

シグネチャの正確性判定	OK	OK	OK	OK（※1）

(※1)シグネチャにバージョン情報を持たない IoT 機器であり、想定通りであることを確認した。

3） データや記録に基づく評価

製品ベンダが独自で開発したシグネチャ及びセキュリティタグは、2022 年 1 月時点で、7 のタイプ（IoT 機器種別）を対象に 3,000 個超であり、継続して追加・メンテナンスしていることを確認した。対応しているタイプ（IoT 機器種別）については表 5-4 に示した通り、カメラ、プリンター等、他の様々な IoT 機器についても検索可能なことを確認した。

表 5-4 Karma が対応している IoT 機器種別と説明

タイプ（IoT 機器種別）	説明
AP	アクセスポイント
Camera	カメラ
ICS	産業用制御システム用装置
NAS	ネットワーク接続型ストレージ
Printer	プリンター・複合機
Router	ルーター
UTM	統合脅威管理用装置

5.1.2 検証項目 1-2 の検証結果

（1） 検証項目の内容

セキュリティリスクのある IoT 機器を検出できること。

（2） 検証結果

Karma でセキュリティタグを持つ IoT 機器を検索し、その検索結果の内容が正しいことを確認した。

セキュリティタグとはセキュリティリスクがあることを示すものであり、これが付与された IoT 機器はセキュリティリスクのある IoT 機器といえる。

（3） 検証内容の詳細

本検証項目は実検証及びデータや記録に基づく評価により実施した。

実検証では①インターネット上に公開されている IoT 機器の検索と、②検証実施者が調達した IoT 機器による正確性検証の 2 段階で確認した。①では、セキュリティタグを持つ IoT 機器を指定して検索が可能なこと、結果の一覧及び詳細が表示されることを確認した。②では、実際の IoT 機器と Karma の検索結果を照合することで、①で確認困難な検索結果の正確性について確認した。

1） 実検証①(インターネット上に公開されている IoT 機器の検索)

Karma でセキュリティタグを持つ IoT 機器の検索を行った。

メーカーが「メーカーA」、モデルが「モデル A」、セキュリティタグを付与されている IoT 機器を指定した検索式で検索を行った。これにより、セキュリティリスクのある IoT 機器が検索され、結果が表示されることを確認した。

検索式: vendor:メーカーA model:モデル A has:tag

図 5-3 のとおり、検索結果が表示された。

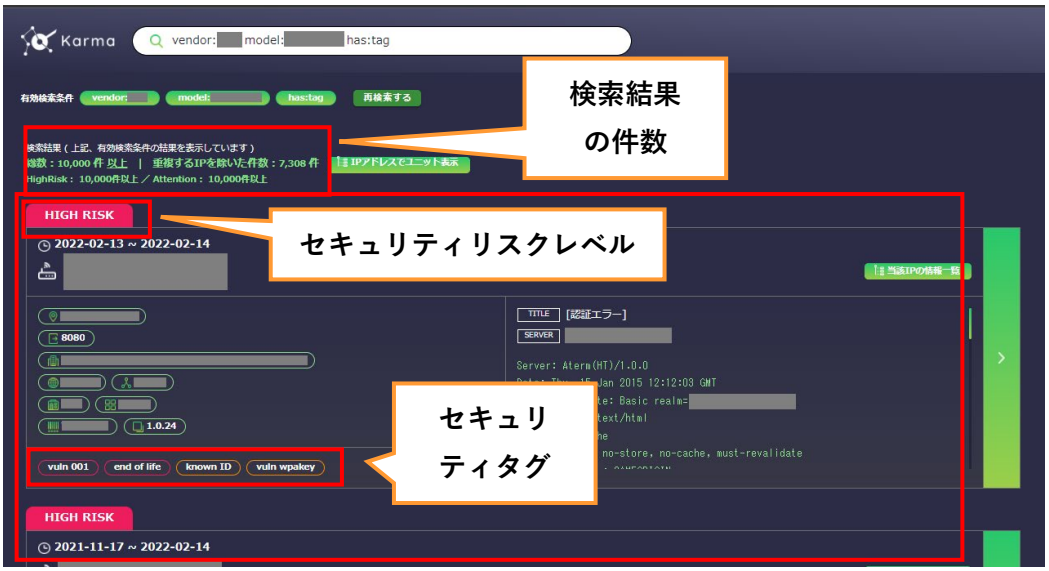


図 5-3 セキュリティタグを持つ IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

また、一覧の中から特定の機器を選択して詳細結果を表示した。(図 5-4)

図 5-4 セキュリティタグを持つ IoT 機器検索の詳細結果画面

該当の IoT 機器に付与されたセキュリティタグが表示されることを確認した。

2） 実検証②(検証実施者が調達した IoT 機器による正確性検証)

検証実施者が調達した IoT 機器に対し、Karma による検索を行った。

該当の IoT 機器のセキュリティリスクについて正しく判定され、検索が正確なものであることを確認した。(詳細については 5.6 章参照)

表 5-5 に、調達機器 1 のファームウェアアップデートによるセキュリティタグ付与の変化を抜粋する。

表 5-5 セキュリティリスクについての正確性

シグネチャ/セキュリティタグ	調達機器 1		
検出回	1 回目	2 回目	3 回目
VERSION	最新の 2 世代前	最新の 1 世代前	最新版
TAGS	known_id	known_id	known_id
	not_latest	not_latest	
	vuln_known		

ここで、調達機器 1 は、ファームウェアバージョンが最新の 2 世代前以前で過去に報告された脆弱性が報告されているモデルである。

① 検出回 1 回目で、ファームウェアバージョンが最新の 2 世代前の状態では過去に報告

された脆弱性があることを示すセキュリティタグ「vuln_known」が付与されている。

② 検出回 2 回目で、ファームウェアバージョンを最新の 1 世代前にアップデートすると、「vuln_known」は付与されなくなった。しかし依然として最新のファームウェアではないことを示すセキュリティタグ「not_latest」は付与されている。

③ 検出回 3 回目で、ファームウェアバージョンを最新版にアップデートすると、「not_latest」は付与されなくなった。管理者アカウント名が既知であることを示すセキュリティタグ「known_id」のみが付与されている状態になることを確認した。

各セキュリティタグの意味については、表 5-6 に説明を補足する。なお、これらのセキュリティタグは、製品ベンダが用意するタグの抜粋である。

表 5-6 セキュリティタグ（抜粋）の説明

セキュリティタグ	セキュリティリスクレベル	説明
end_of_life （サポート終了）	高リスク	サポートが終了している機器に付与されるセキュリティタグある。 脆弱性が新しく発見されたとしても修正されることはないため、直ちに対処が必要である。
initial_state （初期状態）	高リスク	初期設定がされていない機器に付与されるセキュリティタグである。 アクセスされた時点で任意の設定に変更させられる可能性が高いため、直ちに対処が必要である。
leaked_credential （認証情報が漏洩）	高リスク	管理者権限で利用できる ID 及びパスワードが流出している機器に付与されるセキュリティタグである。 アクセスされた時点で設定情報の窃取・改ざんが可能なため、直ちに対処が必要である。
vuln_known （既知の脆弱性）	高リスク	バナー情報から、脆弱なプロトコルやチップセットを使用していると判断された機器に付与されるセキュリティタグである。 利用におけるセキュリティの緩和策がないため、直ちに対処が必要である。

セキュリティタグ	セキュリティリスクレベル	説明
vuln_001 （ゼロデイ）	高リスク	製品ベンダが解析した結果、リモートからのShell の乗っ取りや、管理画面への侵入が可能等、重大な重要性があると判明した機器に付与されるセキュリティタグである。 脆弱性情報を得れば容易に攻撃できるため、直ちに対処が必要である。
no_updates （1 年以上更新なし）	注意	ファームウェアが最後に更新されてから 1 年以上経過している機器に付与されるセキュリティタグである。 機器メーカーが明言していないものの、サポート期間が終了している可能性があり、注意が必要になる。
not_latest （最新状態にしていない）	注意	使用しているファームウェアが最新ではない機器に付与されるセキュリティタグである。 更新されたファームウェアにおいて脆弱性が修正されている場合、注意が必要になる。
known_credential （認証情報が既出）	注意	デフォルト ID 及びパスワードが既知である機器に付与されるセキュリティタグである。 設定を変更していない場合、容易に不正にアクセスされるため注意が必要になる。
no_auth （認証機構無し）	注意	使用にあたり認証を必要としない機器に付与されるセキュリティタグである。 機密性が求められる業務に使用するには注意が必要になる。
known_id （ID が既出）	注意	デフォルト ID が既知である機器に付与されるセキュリティタグである。 デフォルト ID が変更できない場合もあるが、安易なパスワードを使用している場合、不正にアクセスされるリスクが高まるため注意が必要になる。

3） データや記録に基づく評価

製品ベンダで開発したシグネチャ・セキュリティタグは、2022 年 1 月時点で 7 種別、3,000 個超であり、継続して追加・メンテナンスしていることを確認した。対応している種別につ

いては前掲の表 5-4 に示した通り、カメラ、プリンター等、他の様々な IoT 機器についても検索可能なことを確認した。

5.1.3 検証項目 1-3 の検証結果

（1） 検証項目の内容

日本語の文字列を含んだ検索ができること。

（2） 検証結果

Karma で日本語の文字列を含んだ検索式で検索ができ、その検索結果の内容が正しいことを確認した。

（3） 検証内容の詳細

本検証項目は実検証により実施した。

Karma で日本語の文字列を含んだ検索式で検索を行い、検索が可能なこと、検索結果で日本語の文字化け等が発生せず正しく表示されることを確認した。

検索に用いる検索式は、2.3 章に紹介した導入事例に示した事業者及び、製品ベンダが主なターゲットとしている組織を想定して、2 つのユースケース、1)IoT 機器メーカー、2)ISP 事業者・一般組織を想定した。

1） IoT 機器メーカーを想定した検索式

IoT 機器メーカーが、自社製品の中で管理画面をインターネット公開しているものを検索するユースケースを想定し、メーカーが「メーカーA」かつ、バナー情報に「管理画面」という文字列を含む IoT 機器を指定する検索式で検索を行った。これにより、日本語文字列によって IoT 機器が検索され、結果が表示されることを確認した。

検索式: vendor:メーカーA inbanner:管理画面

図 5-5 のとおり、検索結果が表示された。

図 5-5 バナー情報に日本語を含む IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

ここから、一覧の中から特定の機器を選択して詳細結果を表示した。（図 5-6）

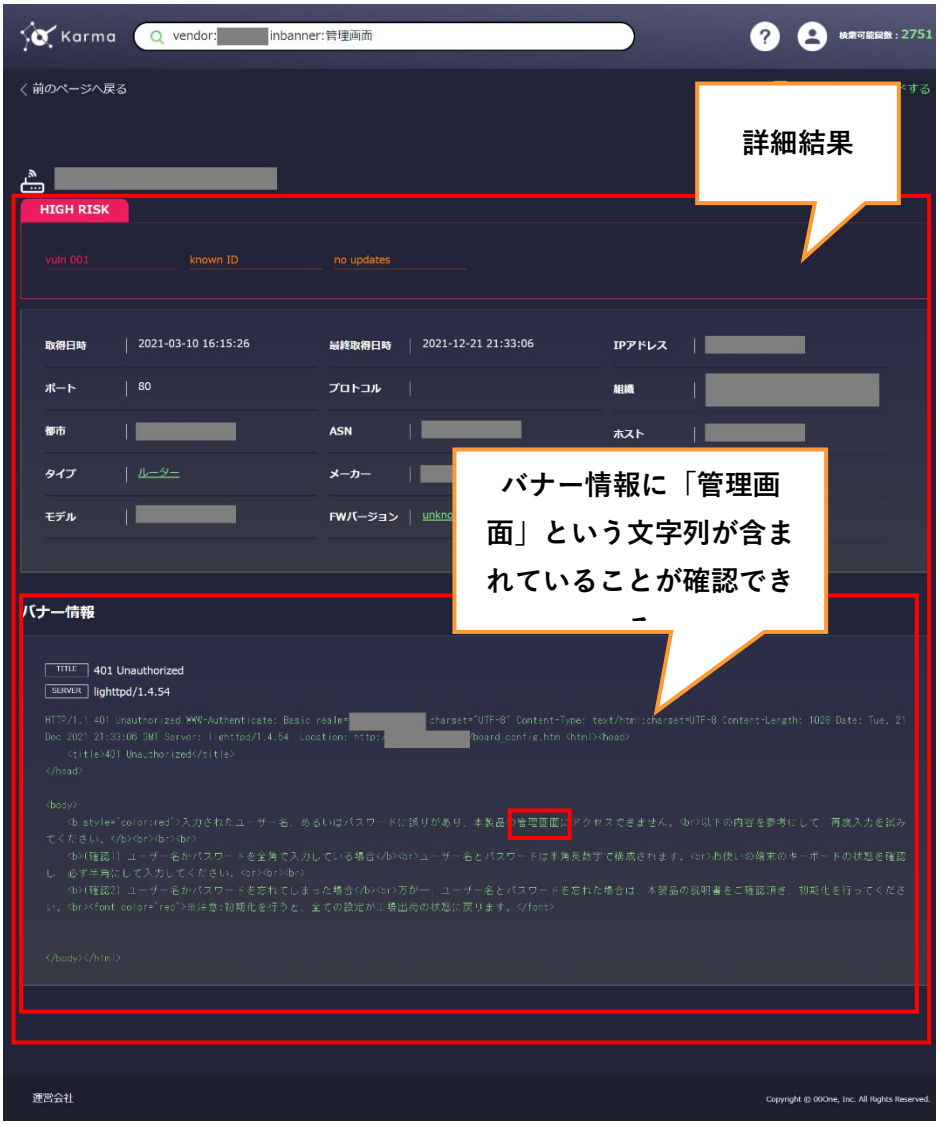


図 5-6 バナー情報に日本語を含む IoT 機器検索の詳細結果画面

該当の IoT 機器のバナー情報に「管理画面」という文字列が含まれていることを確認した。また、バナー情報やその他の情報が全体的に文字化けせずに表示されることを確認した。

2） ISP 事業者や一般組織を想定した検索式

ISP 事業者が、自身で管理するグローバル IP アドレスで管理画面又は管理者パスワード設定・変更画面をインターネット公開している IoT 機器を検索するようなユースケースを想定し、組織名が「組織 X」かつ、Web ページタイトルに「管理者パスワード」という文字列を含むものを指定する検索式で検索を行った。これにより、日本語文字列によって検索され、結果が表示されることを確認した。

検索式: org:組織 X intitle:管理者パスワード

図 5-7 のとおり、検索結果が表示された。

図 5-7 ISP 事業者や一般組織を想定した日本語検索の検索結果画面

Web ページのタイトルに「管理者パスワード」という文字列が含まれることを確認した。また、バナー情報やその他の情報が全体的に文字化けせずに表示されることを確認した。

5.1.4 検証項目 1-4 の検証結果

(1) 検証項目の内容

インターネット経由で IoT 機器の検出ができること。

(2) 検証結果

インターネット接続環境と Web ブラウザのみで利用可能なことを確認した。

ユーザ側での特別な設定なしにインターネット経由で IoT 機器の検出ができることを確認した。

(3) 検証内容の詳細

本検証項目は実検証により実施した。

検証項目 1-1 の検証結果により、インターネット接続が可能な端末と Web ブラウザのみで利用

可能であることを確認した。

5.1.5　検証項目 1-5 の検証結果

（1）　検証項目の内容

条件を絞り込んだ検索ができること。

（2）　検証結果

Karma で複数の条件を含んだ検索式により検索ができることを確認した。

（3）　検証内容の詳細

本検証項目は実検証により実施した。

Karma で複数の条件を含んだ検索式で検索を行い、検索可能なこと、結果が表示されることを確認した。

検索に用いる検索式は、2.3 章に紹介した導入事例に示した事業者及び、製品ベンダが主なターゲットとしている組織を意識して、2 つのユースケース、1)IoT 機器メーカー、2)ISP 事業者・一般組織を想定した。

1） IoT 機器メーカーを想定した検索式

IoT 機器メーカーが、特定の期間における自社製品の利用状況を検索するようなユースケースを想定し、メーカーが「メーカーA」かつ、シリーズが「シリーズ A」、OSINT の情報取得時期が 2022/1/1～2022/1/15 のシグネチャを含む IoT 機器を指定する検索式で検索を行った。これにより、指定期間の IoT 機器情報が検索され、結果が表示されることを確認した。

検索式: type:router vendor:メーカーA series:シリーズ A date:2022-1-1~2022-1-15

図 5-8 のとおり、検索結果が表示された。

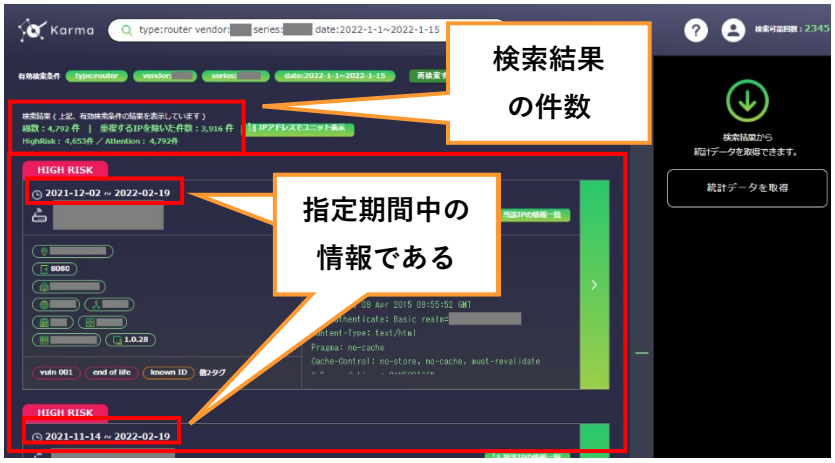


図 5-8 IoT 機器メーカーを想定した複数条件による IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

2） ISP 事業者や一般組織を想定した検索式

ISP 事業者や一般組織が特定の期間における管理グローバル IP の利用状況を検索するようなユースケースを想定し、組織名が「組織 X」、グローバル IP アドレスが***.***.***.***/18、OSINT の情報取得時期が 2022/1/1～現在を含むものを指定する検索式で検索を行った。なお、「*」は任意の数字を示す正規表現である。これにより、指定期間のグローバル IP アドレスの情報が検索され、結果が表示されることを確認した。

検索式: org:組織 X ip:***.***.***.***/18 date:2022-01~

図 5-9 のとおり、検索結果が表示された。

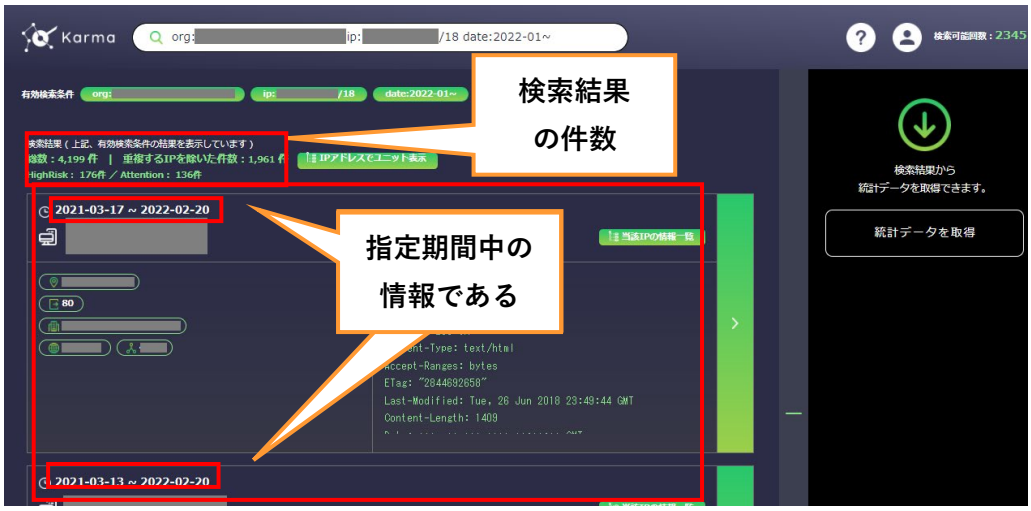


図 5-9 ISP 事業者や一般組織を想定した複数条件による IoT 機器の検索結果画面

該当する検索結果が件数とともに一覧表示されることを確認した。

5.1.6　検証項目 1-6 の検証結果

（1）　検証項目の内容

検出にかかる時間が一般的な許容範囲内であること。

（2）　検証結果

Karma で様々な検索式による検索を行い、時間計測を行い確認した。

これにより、検出にかかる時間が一般的な許容範囲内であることを確認した。

（3）　検証内容の詳細

本検証項目は実検証により実施した。

Karma で様々な検索式で検索を行い、リクエストから結果画面表示までの時間計測を行った。

前提条件として、検索を行った環境のインターネット通信速度は上り・下り 80Mbps の一般的なものであった。検索式と所要時間の一覧を表 5-7 に示す。なお、表中の「*」は任意の文字、あるいは数字を示す正規表現である。

表 5-7 検索式と所要時間(ms)

検索式	1 回目	2 回目	3 回目	平均
org:"*****" port:5555|60001	408	361	324	364.3
series:***** port:5555|60001	464	520	385	456.3
vendor:***** port:60001	355	413	352	373.3
vendor:*** tag:vuln_001&end_of_life	575	452	388	471.7
model:*****	242	358	339	313.0
tag:vuln_wpakey	420	382	482	428.0
org:"****** " intitle:管理者パスワード	608	513	466	529.0
vendor:*** inbanner:管理画面	410	403	356	389.7
vendor:*** inbanner:パスワード&ログイン	369	310	338	339.0
org:"*****" ip:***.***.***.***/18 date:2022-01~	516	494	507	505.7
type:router vendor:*** series:***** date:2021-1-1~	463	404	504	457.0
org:"***** " model:*****	431	379	310	373.3
org:"*****" tag:end_of_life	416	418	472	435.3
vendor:***** model:"*****"	431	419	345	398.3
vendor:***** tag:end_of_life	328	427	573	442.7
model:*****	502	425	655	527.3
tag:vuln_001 model:*****|*****	466	424	457	449.0
!tag:vuln_001 model:*****|*****	525	478	515	506.0

いずれも平均 500ms 程度であり、一般的な許容範囲内であることを確認した。

使用した検索式のオプションについての説明を表 5-8 に示す。

表 5-8 検索式のオプションと説明

検索式のオプション	説明
org	該当する組織に関する検索式のオプションで、組織名が指定文字列と完全一致するものを検索できる。
series	IoT 機器のシリーズに関する検索式のオプションで、該当するシリーズの IoT 機器を検索できる。
vendor	IoT 機器のベンダに関する検索式のオプションで、該当するベンダの IoT 機器を検索できる。
tag	セキュリティタグに関する検索式のオプションで、指定されたセキュリティタグが付加されている機器を取得できる。
model	IoT 機器のモデル名に関する検索式のオプションで、該当するモデルの IoT 機器を検索できる。
intitle	タイトルに含まれる文字列に関する検索式のオプションで、Web ページタイトルに指定文字列を含むものを検索できる。
inbanner	バナーに含まれる文字列に関する検索式のオプションで、バナーに指定文字列を含むものを検索できる。
date	期間に関する検索式のオプションで、該当する期間のデータを検索できる。
ip	IP アドレスに関する検索式のオプションで、該当する IP アドレスのデータを検索できる。CIDR 表記による指定も可能である。
type	タイプ（IoT 機器種別）に関する検索式のオプションで、該当するタイプの IoT 機器を検索できる。検索可能なタイプは表 5-4 を参照。

5.1.7 検証項目 1-7 の検証結果

(1) 検証項目の内容

古い IoT 機器におけるリスクの検出ができること。

(2) 検証結果

Karma で古いモデルの IoT 機器の検索ができることを確認した。

これにより、古い IoT 機器におけるリスクの検出ができることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及びデータや記録に基づく評価により実施した。

1) 実検証（インターネット上に公開されている IoT 機器の検索）

Karma で古いモデルの IoT 機器の検索を行い、end_of_life（サポート終了）のセキュリティタグが付与されることを確認した。2002 年 10 月発売の IoT 機器「モデル E」を指定する検索式により検索を行い、セキュリティタグを含む検索結果が表示されることを確認した。

検索式: model:モデル E

図 5-10 のとおり、検索結果が表示された。

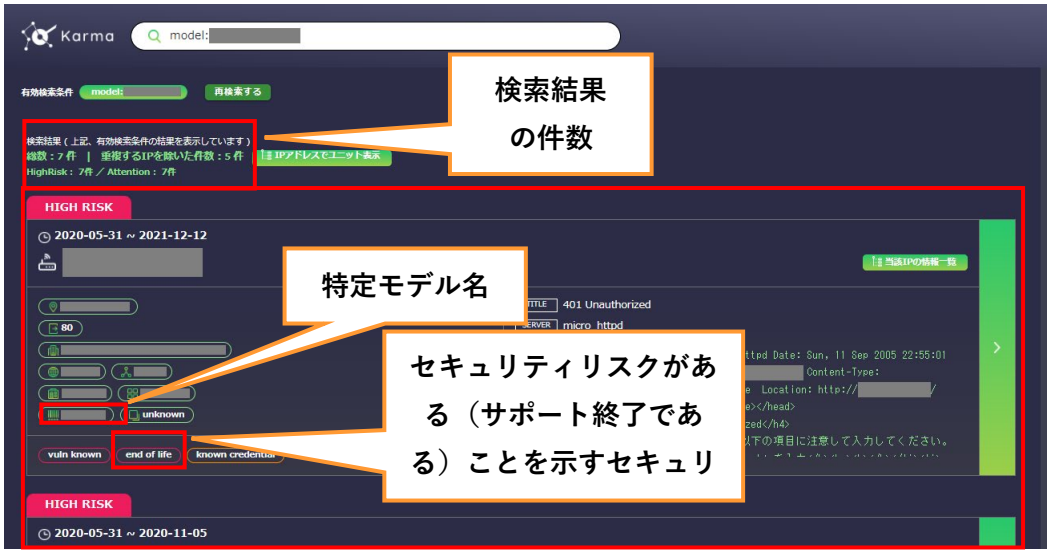


図 5-10 古い IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示され、セキュリティタグも付与されていることを確認した。

2) データや記録に基づく評価

製品ベンダで開発したシグネチャ・セキュリティタグは、2022 年 1 月時点で 7 種別、3,000 個超であり、過去に作成したものは削除せずメンテナンスする運用であることを確認した。対応している種別については前掲の表 5-4 に示した通り、カメラ、プリンター等、他の様々な IoT 機器についても検索可能なことを確認した。

5.1.8　検証項目 1-8 の検証結果

（1）　検証項目の内容

新たに製品化された IoT 機器が検出できること。

（2）　検証結果

Karma で新しいモデルの IoT 機器を検索でき、その検索結果の内容が正しいことを確認した。

これにより、新たに製品化された IoT 機器が検出できることを確認した。

（3）　検証内容の詳細

本検証項目は実検証、データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

実検証では①インターネット上に公開されている IoT 機器の検索と、②検証実施者が調達した IoT 機器による正確性検証の 2 段階で確認した。①では、指定モデルの IoT 機器を指定して検索が可能なこと、結果の一覧及び詳細が表示されることを確認した。②では、実際の IoT 機器と Karma の検索結果を照合することで、①で確認困難な検索結果の正確性について確認した。

1） 実検証①（インターネット上に公開されている IoT 機器の検索）

Karma で比較的新しく製品化された IoT 機器製品名による検索を行った。

2021 年 9 月発売の IoT 機器「モデル F」を指定した検索式で検索を行い、指定モデルの検索結果が表示されることを確認した。

検索式: model:モデル F

図 5-11 のとおり、検索結果が表示された。

図 5-11 新しく製品化された IoT 機器の製品名による検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

2） 実検証②(検証実施者が調達した IoT 機器による正確性検証)

検証実施者が調達した IoT 機器に対し、Karma データベースによる検索を行った。

比較的新しい発売時期の調達機器 2 について正しく判定され、検索が正確なものであることを確認した。(詳細については 5.6 章参照)

表 5-9 に、情報を抜粋する。

表 5-9 検証実施者が調達した IoT 機器の抜粋

説明	調達機器 2
タイプ（IoT 機器種別）	ルーター
メーカー	「メーカーB」
シリーズ	「シリーズ B」
モデル	「モデル B」
発売時期	2021 年 9 月

3） データや記録及びベンダヒアリングに基づく評価

製品ベンダで開発したシグネチャ・セキュリティタグは、2022 年 1 月時点で 7 種別、3,000 個超であり、継続して追加・メンテナンスしていることを確認した。対応している種別については前掲の表 5-4 に示した通り、カメラ、プリンター等、他の様々な IoT 機器についても検索可能なことを確認した。

またヒアリングにより、週次で新しい IoT 機器のシグネチャを追加していることを確認した。

5.1.9 検証項目 1-9 の検証結果

（1） 検証項目の内容

新たに発見された脆弱性が検出できること。

（2） 検証結果

Karma で新たに発見された脆弱性に基づいてセキュリティタグが付与された IoT 機器を検索でき、その検索結果の内容が正しいことを確認した。

これにより、新たに発見された脆弱性が検出できることを確認した。

（3） 検証内容の詳細

本検証項目は実検証、データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

実検証では①インターネット上に公開されている IoT 機器の検索と、②検証実施者が調達した IoT 機器による正確性検証の 2 段階で確認した。①では、指定セキュリティタグの IoT 機器を指定して検索が可能なこと、結果の一覧及び詳細が表示されることを確認した。②では、実際の IoT 機器と Karma の検索結果を照合することで、①で確認困難な検索結果の正確性について確認した。

1） 実検証①(インターネット上に公開されている IoT 機器の検索)

Karma において、既知の脆弱性を持つ IoT 機器の検索を行った。

対象の IoT 機器において過去に報告された脆弱性をターゲットとし、これを基に付与されるセキュリティタグ「vuln_known」（既知の脆弱性に関するセキュリティタグ）の有無を、

指定した検索式によって検索を行い、結果が表示されることを確認した。

検索式:

a. tag:vuln_known model:モデル A|モデル B

b. !tag:vuln_known model:モデル A|モデル B

検索式 a.について、図 5-12 のとおり、検索結果及び統計情報が表示された。

図 5-12 脆弱性に基づくセキュリティタグを持つ IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

統計情報のファームウェアバージョンからも、脆弱性に当てはまるものが表示されることを確認した。

また検索式 b.について、同一の機器で既知の脆弱性に基づくセキュリティタグを持たないものについても検索した。(図 5-13)

図 5-13 脆弱性に基づくセキュリティタグを持たない IoT 機器の検索結果画面

該当する IoT 機器の検索結果が件数とともに一覧表示されることを確認した。

統計情報のファームウェアバージョンからも、脆弱性に当てはまらないものだけが表示され、

脆弱性の有無を正しく判定していることを確認した。

2） 実検証②(検証実施者が調達した IoT 機器による正確性検証)

5.1.2（3）2）に記載した通り、調達機器 1 について、対象の IoT 機器において過去に報告された脆弱性に基づいたセキュリティタグが正しく付与されていることを確認した。

3） データや記録及びベンダヒアリングに基づく評価

製品ベンダで開発したシグネチャ・セキュリティタグは、2022 年 1 月時点で 7 種別、3,000 個超であり、継続して追加・メンテナンスしていることを確認した。対応している種別については前掲の表 5-4 に示した通り、カメラ、プリンター等、他の様々な IoT 機器についても検索可能なことを確認した。

またヒアリングによって、週次で新しい IoT 機器のセキュリティタグを作成していることを確認した。

5.2 「検出したリスクの可視化・管理」に関する検証結果

5.2.1　検証項目 2-1 の検証結果

（1）　検証項目の内容

検出したリスクの統計情報表示ができること。

（2）　検証結果

Karma で検索後、その検索結果から統計情報を表示できることを確認した。

（3）　検証内容の詳細

本検証項目は実検証により実施した。

5.1.9（3）1）a の検索式を用いた検索結果で統計情報を表示させた。

図 5-14 に、統計情報画面をすべてスクロールしたものを並べて示す。

図 5-14 統計情報表示画面(検証項目 2-1)

ファームウェアバージョンやセキュリティタグを含めて統計情報を表示できることを確認した。

それぞれの項目の意味については表 5-10 に示す。

表 5-10 統計情報の項目の説明

統計情報の項目	説明
TOP PORTS	検索された IoT 機器におけるポート番号のトップ 10
TOP PROTOCOLS	検索された IoT 機器におけるプロトコルのトップ 10

TOP CITIES	検索された IoT 機器における都市のトップ 10
TOP ORGANIZATIONS	検索された IoT 機器における組織のトップ 10
VENDORS	検索された IoT 機器のメーカー
SERIES	検索された IoT 機器の製品シリーズ
MODELS	検索された IoT 機器の製品モデル
FW VERSIONS	検索された IoT 機器のファームウェアバージョン
SECURITY TAGS	検索された IoT 機器に付与されたセキュリティタグ

5.2.2 検証項目 2-2 の検証結果

(1) 検証項目の内容

検出したリスクの絞り込み表示ができること。

(2) 検証結果

Karma の検索結果からさらに絞込んで検索・表示できることを確認した。

(3) 検証内容の詳細

本検証項目は実検証により実施した。

5.1.5（3）で用いた検索式で検索を行い、その結果から絞込みを行った。

1) IoT 機器メーカーを想定した検索式

検索結果画面で「統計データを取得」ボタンから統計情報を取得した。(図 5-15)

図 5-15 統計情報表示画面(検証項目 2-2-1)

統計情報中の「SECURITY TAGS」から「initial state」をクリックした。(図 5-16)

図 5-16 絞込み検索結果画面(検証項目 2-2-1)

検索式に「tag:initial_state」が付与され、絞込みがなされた検索結果が表示されることを確認した。

2） ISP 事業者や一般組織を想定した検索式

検索結果同画面で「統計データを取得」ボタンから統計情報を取得した。(図 5-17)

図 5-17 統計情報表示画面(検証項目 2-2-2)

この画面で統計情報の「TOP PORTS」中から「80」をクリックした。(図 5-18)

図 5-18 絞込み検索結果画面(検証項目 2-2-2)

検索式に「ports:80」が付与され、絞込み検索結果が表示されることを確認した。

5.2.3 検証項目 2-3 の検証結果

(1) 検証項目の内容

結果のエクスポートができること。

(2) 検証結果

Karma で検索後、その検索結果をファイルとしてエクスポートできることを確認した。

（3） 検証内容の詳細

本検証項目は実検証により実施した。

5.1.1（3）1）の検索式を用いた検索結果で詳細情報を表示させた。（図 5-19）

図 5-19 詳細結果画面からの JSON ファイルエクスポート

「JSON をダウンロードする」をクリックすると、JSON 形式のファイルをエクスポートすることができた。ファイルを開いて Web 画面と照合し、内容が正しいことを確認した。（図 5-20）


```
{
  "ID":"b180d287e453fe2c4bbeed7ac26713b7c246c50b",
  "IP":"[redacted]",
  "PORT":80,
  "CREATION_DATE":"2022-01-23 17:01:52",
  "DATE":"2022-02-14 01:56:17",
  "HOST":"[redacted]",
  "CITY":"[redacted]",
  "ASN":[redacted],
  "ORG":"[redacted]",
  "BANNER":"Location: http://[redacted]/html/login.html <html><hea
  "SERVER":"uhttpd/1.0.0",
  "VENDOR":"[redacted]",
  "SERIES":"[redacted]",
  "TYPE":"router",
  "MODEL":"[redacted]",
  "VERSION":"1.10",
  "TAGS":["known_id",
          "not_latest",
          "vuln_known"]
}
```


図 5-20 エクスポートした JSON ファイル

表 5-1 に示した詳細情報の項目と、JSON キーの対応については表 5-11 に示す。

表 5-11 詳細情報の項目と JSON キーとの対応

詳細情報の項目	JSON キー
取得日時	CREATION_DATE
最終取得日時	DATE
IP アドレス	IP
ポート	PORT
プロトコル	PROTOCOL
組織	ORG
都市	CITY
ASN	ASN
ホスト	HOST
タイプ（IoT 機器種別）	TYPE
メーカー	VENDOR
シリーズ	SERIES
モデル	MODEL
FW バージョン	VERSION
識別 ID	ID
バナー情報	BANNER

5.3 「検出仕様」に関する検証結果

5.3.1 検証項目 3-1 の検証結果

(1) 検証項目の内容

検出の手法として不正アクセス禁止法に抵触しない方法で情報を取得していること。

(2) 検証結果

検出の手法として不正アクセス禁止法に抵触しない方法で情報を取得していることを確認した。

(3) 検証内容の詳細

本検証項目はデータや記録に基づく評価及びベンダに対するヒアリングにより実施した。

Karma は独自のデータベース(OSINT 情報とシグネチャ・セキュリティタグを統合したもの)から検索を行う仕様である。また、Karma は複数の OSINT 情報源を利用しており、その中で違法の疑いが発生したものは切離すなどの対応が可能であることを確認した。

以上のベンダヒアリングの結果から、不正アクセス禁止法に抵触しない仕様であることを確認した。

5.3.2 検証項目 3-2 の検証結果

(1) 検証項目の内容

検出の手法として倫理的に問題ない方法で情報を取得していること。

(2) 検証結果

検出の手法として倫理的に問題ない方法で情報を取得していることを確認した。

(3) 検証内容の詳細

本検証項目はデータや記録に基づく評価及びベンダに対するヒアリングにより実施した。

図 4-1 に示した通り、Karma 自身はインターネット上の IoT 機器に対する直接的なスキャンは実施せず、OSINT の情報源と独自開発のシグネチャ・セキュリティタグとを統合したデータベースから検索を行うものである。IoT 機器に対する直接的なスキャンを行わないことから、倫理的な問題が発生しないことを確認した。

5.4 「誤検出・検出漏れ」に関する検証結果

5.4.1 検証項目 4-1 の検証結果

(1) 検証項目の内容

誤検出率が一般的な許容範囲内であること。

(2) 検証結果

検証実施者の調達した機器の検出率及び製品ベンダの示すデータにより、誤検出率が一般的な許容範囲内であることを確認した。

（3） 検証内容の詳細

本検証項目は実検証、データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

1） 実検証(検証実施者が調達した IoT 機器による正確性検証)

検証実施者が調達した IoT 機器に対し、シグネチャ・セキュリティタグによる検索を行った。

検証実施者が調達した IoT 機器について正しく判定され、4 機種中に誤検出がないことを確認した。(詳細については 5.6 章参照)

2） データや記録に基づく評価及びベンダに対するヒアリング

データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

横浜国立大学との共同研究(※1)において、学内ネットワークの IoT 機器を 223 件検出し、その後機器のユーザすべてにアンケートを実施したが、誤検出率は 0%であった。

(※1)SCIS2022 ドアを開け放したのは誰か？IoT 機器のセキュリティ問題の改善に向けた根本原因調査

(https://www.iwsec.org/scis/2022/program.html#3F1)

5.4.2 検証項目 4-2 の検証結果

（1） 検証項目の内容

検出不能率が一般的な許容範囲内であること。

（2） 検証結果

検証実施者の調達した機器の検出率及び製品ベンダの示すデータにより、検出不能率が一般的な許容範囲内であることを確認した。

（3） 検証内容の詳細

本検証項目は実検証、データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

1） 実検証(検証実施者が調達した IoT 機器による正確性検証)

検証実施者が調達した IoT 機器に対し、シグネチャ・セキュリティタグによる検索を行った。

該当の IoT 機器のセキュリティリスクについて正しく判定され、4 機種中に検出不能なものがないことを確認した。(詳細については 5.6 章参照)

2） データや記録に基づく評価及びベンダに対するヒアリング

データや記録に基づく評価及びベンダに対するヒアリングにより実施した。

横浜国立大学との共同研究(※1)において、学内ネットワークの IoT 機器を 223 件検出し、シグネチャ機能によってモデルが特定できたのは 216 件(96.9%)であり、検出不能率は 3.1%であった。

(※1)SCIS2022 ドアを開け放したのは誰か？IoT 機器のセキュリティ問題の改善に向けた根本原因調査

(https://www.iwsec.org/scis/2022/program.html#3F1)

5.5 「その他」に関する検証結果

5.5.1 検証項目 5-1 の検証結果

（1） 検証項目の内容

不正ログイン対策がされていること。

（2） 検証結果

顧客アカウントに対する各種不正ログイン対策がされていることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及びベンダに対するヒアリングにより実施した。

Web アプリケーションの開発には既成のフレームワークを使って作り込みを極力なくし、脆弱性対策を行っているとの回答を得た。また、一般的な Web アプリケーションの脆弱性は評価済みであると回答を得た。他に、ログインアラートメールによる対策を実施していることを確認した。図 5-21 に示す通り、複数の IP アドレスで同一アカウントによるログインをしたあと、ログインアラートメールが送信されることを実検証で確認した。

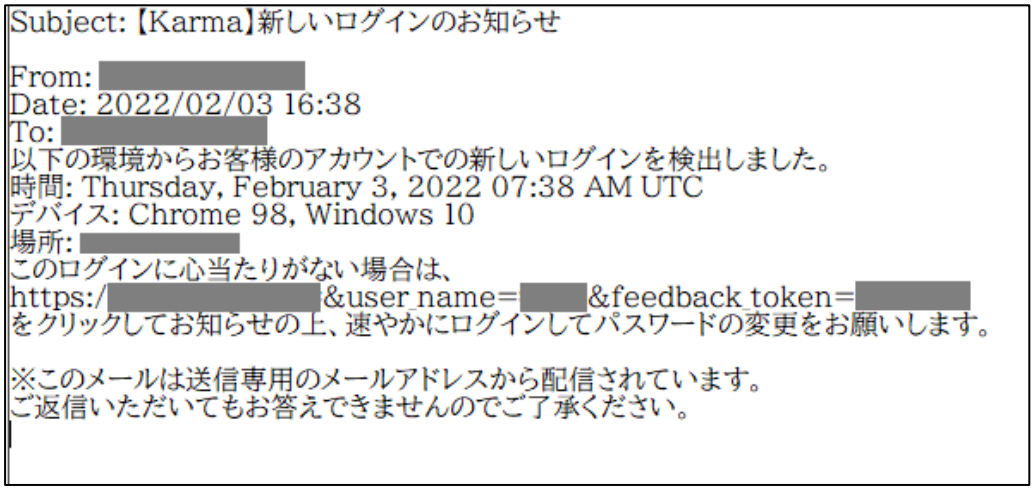


図 5-21 ログインアラートメールの内容

5.5.2 検証項目 5-2 の検証結果

(1) 検証項目の内容

取得データの所在地（リージョン）が日本国内であること。

(2) 検証結果

取得データの所在地（リージョン）が日本国内であることを確認した。

(3) 検証内容の詳細

本検証項目はデータや記録に基づく評価及びベンダに対するヒアリングにより実施した。

製品ベンダからの回答及び証拠画像を受け、データの所在地（リージョン）が日本国内であることを確認した。

5.5.3　検証項目 5-3 の検証結果

（1）　検証項目の内容

プライバシーポリシー（個人情報保護方針）を明記していること。

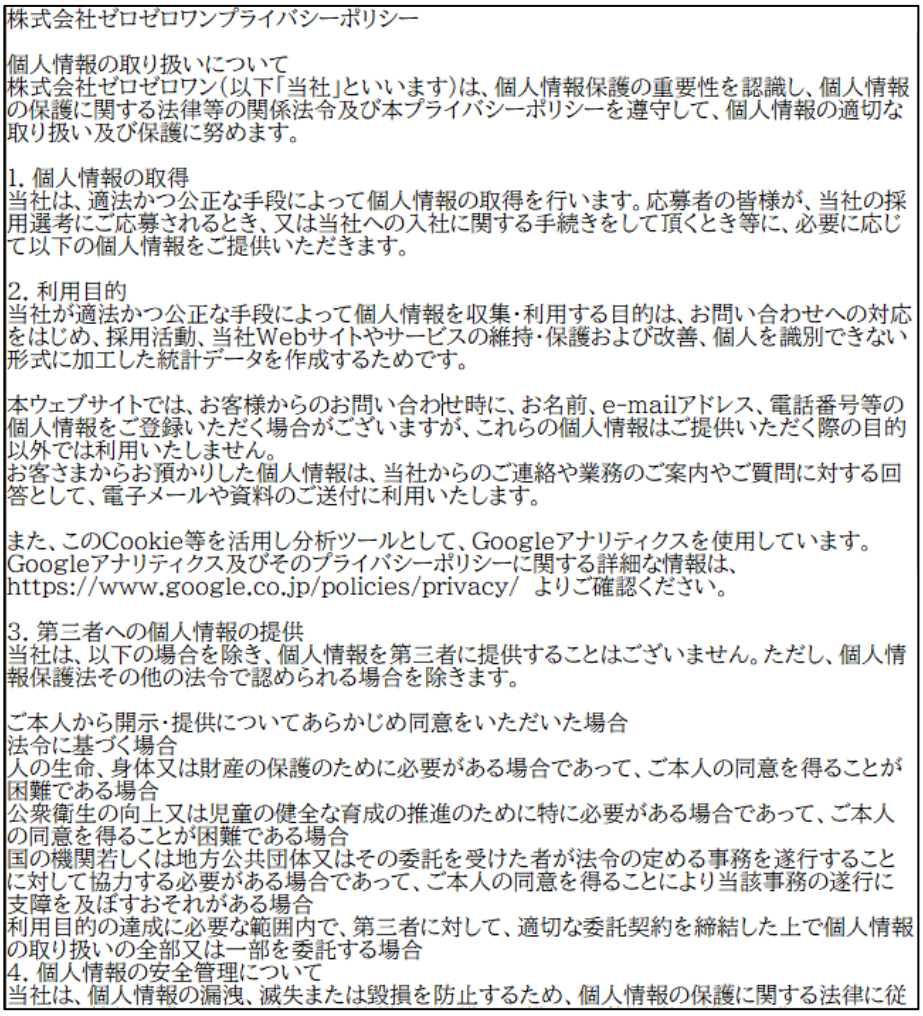
（2）　検証結果

プライバシーポリシー（個人情報保護方針）を明記していることを確認した。

（3）　検証内容の詳細

本検証項目はデータや記録に基づく評価及びベンダに対するヒアリングにより実施した。

製品ベンダのホームページにプライバシーポリシー（個人情報保護方針）が明記されていることを確認した(図 5-22)。また、Karma の利用規約には、当プライバシーポリシーに準ずることが明記されることを確認した。



株式会社ゼロゼロワンプライバシーポリシー

個人情報の取り扱いについて
株式会社ゼロゼロワン(以下「当社」といいます)は、個人情報保護の重要性を認識し、個人情報の保護に関する法律等の関係法令及び本プライバシーポリシーを遵守して、個人情報の適切な取り扱い及び保護に努めます。

1. 個人情報の取得
当社は、適法かつ公正な手段によって個人情報の取得を行います。応募者の皆様が、当社の採用選考にご応募されるとき、又は当社への入社に関する手続きをして頂くとき等に、必要に応じて以下の個人情報をご提供いただきます。

2. 利用目的
当社が適法かつ公正な手段によって個人情報を収集・利用する目的は、お問い合わせへの対応をはじめ、採用活動、当社Webサイトやサービスの維持・保護および改善、個人を識別できない形式に加工した統計データを作成するためです。

本ウェブサイトでは、お客様からのお問い合わせ時に、お名前、e-mailアドレス、電話番号等の個人情報をご登録いただく場合がございますが、これらの個人情報はご提供いただく際の目的以外では利用いたしません。
お客さまからお預かりした個人情報は、当社からのご連絡や業務のご案内やご質問に対する回答として、電子メールや資料のご送付に利用いたします。

また、このCookie等を活用し分析ツールとして、Googleアナリティクスを使用しています。
Googleアナリティクス及びそのプライバシーポリシーに関する詳細な情報は、
https://www.google.co.jp/policies/privacy/ よりご確認ください。

3. 第三者への個人情報の提供
当社は、以下の場合を除き、個人情報を第三者に提供することはございません。ただし、個人情報保護法その他の法令で認められる場合を除きます。

ご本人から開示・提供についてあらかじめ同意をいただいた場合
法令に基づく場合
人の生命、身体又は財産の保護のために必要がある場合であって、ご本人の同意を得ることが困難である場合
公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、ご本人の同意を得ることが困難である場合
国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、ご本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがある場合
利用目的の達成に必要な範囲内で、第三者に対して、適切な委託契約を締結した上で個人情報の取り扱いの全部又は一部を委託する場合
4. 個人情報の安全管理について
当社は、個人情報の漏洩、滅失または毀損を防止するため、個人情報の保護に関する法律に従

図 5-22 プライバシーポリシー(抜粋)

5.6 検証実施者が調達した IoT 機器による正確性検証結果のまとめ

本章では、検証実施者が調達した IoT 機器による正確性検証の結果をまとめる。

社内ネットワークに設置した当該の IoT 機器について、Karma のデータベースによる検索を行った。その結果を表 5-12、表 5-13、表 5-14、表 5-15 に示す。なお、表 5-12 及び表 5-13 に示す調達機器 1 では、同一機器にてファームウェアバージョンアップを実施し、検証を行った。

表の中で 1 点、調達機器 4 についてのみファームウェアバージョンが「unknown」と表示されているが、シグネチャにバージョン情報を持たない IoT 機器であり、想定通りの動作であることを製品ベンダから確認した。これは、一部の IoT 機器ではファームウェアバージョンによってバナー情報等に差異がみられないなどの理由で、バージョン情報を規定できないためである。

表 5-12 調達した IoT 機器 (調達機器 1 に関する抜粋)

説明	調達機器 1		
メーカー	「メーカーA」	「メーカーA」	「メーカーA」
シリーズ	「シリーズ A」	「シリーズ A」	「シリーズ A」
モデル	「モデル A」	「モデル A」	「モデル A」
ファームウェアバージョン	最新の 2 世代前 ※初回検索	最新の 1 世代前 ※アップデート 1 回目	最新版 ※アップデート 2 回目

表 5-13 検証実施者が調達した IoT 機器による正確性検証結果(調達機器 1)

シグネチャ/セキュリティタグ	調達機器 1		
VENDOR	「メーカーA」	「メーカーA」	「メーカーA」
SERIES	「シリーズ A」	「シリーズ A」	「シリーズ A」
MODEL	「モデル A」	「モデル A」	「モデル A」
VERSION	最新の 2 世代前	最新の 1 世代前 ※1	最新版 ※1
TAGS	known_id	known_id	known_id
	not_latest	not_latest	
	vuln_known		

(※1) 同一機器でファームウェアバージョンアップを実施した。

表 5-14 調達した IoT 機器 (調達機器 2～4 に関する抜粋)

説明	調達機器 2		調達機器 3	調達機器 4
メーカー	「メーカーB」	「メーカーB」	「メーカーC」	「メーカーD」
シリーズ	「シリーズ B」	「シリーズ B」	「シリーズC」	「シリーズD」
モデル	「モデル B」	「モデル B」	「モデルC」	「モデル D」
ファームウェアバージョン	最新の 1 世代前 ※初回検索	最新版 ※アップデート後	最新版	最新版

表 5-15 検証実施者が調達した IoT 機器による正確性検証結果(調達機器 2)

シグネチャ/セキュリティタグ	調達機器 2		調達機器 3	調達機器 4
VENDOR	「メーカーB」	「メーカーB」	「メーカーC」	「メーカーD」
SERIES	「シリーズ B」	「シリーズB」	「シリーズC」	「シリーズ D」
MODEL	「モデル B」	「モデルB」	「モデル C」	「モデル D」
VERSION	最新の 1 世代前	最新版(※1)	最新版	unknown (※2)
TAGS	known_id	known_id	known_id	known_id
	not_latest			

(※1) 同一機器でファームウェアバージョンアップを実施した。

(※2) シグネチャにバージョン情報を持たない IoT 機器であり、想定通りであることを確認した。

6. まとめ

Karma は、独自開発のシグネチャ・セキュリティタグを活用した IoT 機器検索エンジンである。製品ベンダは、それまでの IoT 機器検索エンジンでは困難であった IoT 機器の特定（メーカー、シリーズ、機種、及びファームウェアバージョン）ができることや、特定した IoT 機器について、重大なセキュリティリスクがもたらされるおそれがあるか、又は注意を要する IoT 機器なのかを容易に識別可能とした点が特徴であるとしている。加えて、日本語文字列による検索や、検索結果の日本語文字列を文字化けせずに表示できる点も特徴として挙げられる。

今回の検証は、前述の検証環境、検証条件、方法の範囲で、Karma の 3 つの新規性の高いセキュリティ機能とされている事項に対して、「リスクの検出」、「検出したリスクの可視化・管理」、「検出仕様」「誤検出・検出漏れ」「その他」の観点から検証を実施し確認した。

セキュリティ製品の有効性検証の検証結果について

株式会社エーアイセキュリティラボ　「AeyeScan」

独立行政法人情報処理推進機構

令和 4 年 3 月

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
AI	Artificial Intelligence の略。人工知能のこと。
API	Application Programming Interface の略。本報告書では Web API のことを示す。プログラム等から API を呼び出すことで、GUI で操作するのと同様の処理を行うことができるもの。
ASVS 4.0	Application Security Verification Standard 4.0 の略で、OWASP が公開しているアプリケーションセキュリティ検証標準バージョン 4.0 のこと。 https://owasp.org/www-project-application-security-verification-standard/
AWS	Amazon Web Services の略。
Basic 認証	特定のページに簡易的な認証設定をかけること。
CAPTCHA	画面操作を行っているのがコンピュータではなく人間であることを確認するための認証手段の一つ。
Chrome	Google が提供する Web ブラウザのこと。
CI	Continuous Integration の略。単体テストされたモジュール同士を早めに結合させて、品質を向上させる考え方のこと。
CSIRT	Computer Security Incident Response Team の略。企業や行政機関などに設置される組織の一種で、コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織のこと。
CSRF	Cross-Site Request Forgeries の略。ログインした利用者からのリクエストについて、その利用者が意図したリクエストであるかどうかを識別する仕組みを持たない Web サイトは、外部サイトを経由した悪意のあるリクエストを受け入れてしまう場合があり、利用者が予期しない処理を実行させられてしまうこと。
GUI	Graphical User Interface の略。システムから利用者へのグラフィカルな情報の提示・表示の仕方と、利用者がマウスなどのポインティングデバイスでシステムを操作したり情報を入力したりする手段や方式、機器、使い勝手のこと。
HTTP ヘッダ・インジェクション	Web アプリケーションで HTTP レスポンスヘッダの出力処理に問題がある場合、攻撃者は、レスポンス内容に任意のヘッダフィールドを追加したり、任意のボディを作成したり、複数のレスポンスを作り出すような攻撃を仕掛けられること。
Linux	オープンソースとして開発されている OS の一つ。

用語	概要
OS	Operating System の略。ソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェアのこと。
OS コマンド	コンピュータの利用者が OS に与える文字列による命令のこと。
OS コマンド・インジェクション	攻撃により、Web サーバの OS コマンドを不正に実行されてしまうこと。
OWASP	Open Web Application Security Project の略。Web をはじめとするソフトウェアのセキュリティ環境の現状、またセキュアなソフトウェア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的としたプロフェッショナルの集まる、オープンソース・ソフトウェアコミュニティのこと。 https://owasp.org/
OWASP Benchmark	OWASP が公開している実行可能なオープンソースの Web アプリケーションで、あらゆる種類の Web アプリケーション脆弱性検出ツールの公正なテストが目的となっており、意図的に脆弱性が含まれているもの。 https://owasp.org/www-project-benchmark/
OWASP Juice Shop	OWASP が公開している実行可能なオープンソースの Web アプリケーションで、SPA で構成されているのが特徴となっており、意図的に脆弱性が含まれているもの。 https://owasp.org/www-project-juice-shop/
OWASP TOP10	OWASP が公開している Web セキュリティのレポートのこと。 https://owasp.org/Top10/ja/
RPA	Robotic Process Automation の略。コンピュータを使って人間の代わりに業務を自動化する技術のこと。
SaaS	Software as a Service の略。インターネットを通じてソフトウェアを利用者に提供する方式のこと。
SPA	Single Page Application の略。単一の Web ページのみから構成され、ページの移動は行わずに JavaScript 等の処理によりコンテンツの切り替えを行うもの。
SQL	リレーショナルデータベース（RDB：Relational Database）の管理や操作を行うための問い合わせ言語のこと。
SQL インジェクション	Web アプリケーションで SQL 文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用をまねくこと。
Web アプリケーション	Web ページと共通の技術を応用して構築・運用されるアプリケーションソフトのこと。
安全な Web サイトの作り方	ウェブサイト開発者や運営者が適切なセキュリティを考慮したウェブサイトを作成するための IPA が公開している資料のこと。 https://www.ipa.go.jp/security/vuln/websecurity.html

用語	概要
インジェクション	ソフトウェアへの攻撃手法の一つで、外部から文字列の入力を受け付けるプログラムに対して開発者の想定外の不正な文字列を与え、システムを乗っ取ったり、データの改ざんや詐取を行ったりする手法のこと。
クリックジャッキング	Web アプリケーションでログインしている利用者のみが使用可能な機能を提供しているものがあり、該当する機能がマウス操作のみで使用可能な場合、細工された外部サイトを閲覧し操作することにより、利用者が誤操作し、意図しない機能を実行させられること。
クロスサイト・スクリプティング	利用者が入力した内容を表示するような構成の Web サイトに存在する欠陥を悪用して、攻撃者が用意した悪意のあるスクリプトを利用者の元に送り込んで実行させる攻撃のこと。
クロール	プログラムにより Web ページを収集して保存すること。
システムインテグレーター	企業や行政の情報システムの構築、運用などの業務を一括して請け負う事業者のこと。
巡回	AeyeScan が診断対象ページを特定するための事前処理で、巡回結果は画面遷移図として出力されるものをいう。
スキャン	AeyeScan による脆弱性診断のこと。
スクリーンショット	画面を画像ファイルとして保存したもの。
多要素認証	知っていること（例：パスワード）、持っているもの（例：IC カード）、身体的特徴（例：指紋）の認証要素のうち複数を組み合わせて認証することをいう。
ディレクトリ	ディレクトリの中にサブディレクトリを作成し、その中にさらにファイルやディレクトリを作ることができ、全体を階層構造で表すことができるもの。
ディレクトリ・トラバーサル	Web アプリケーションでファイル名指定の実装に問題がある場合、攻撃者に任意のファイルを指定され、Web アプリケーションが意図しない処理を行ってしまう脆弱性のこと。
二要素認証	多要素認証に記載した認証要素のうち 2 つを組み合わせて認証することをいう。
バッファオーバーフロー	Web アプリケーションを含むあらゆるプログラムは、指示された処理を行うためにメモリ上に自身が使用する領域を確保する。プログラムが入力されたデータを適切に扱わない場合、プログラムが確保したメモリの領域を超えて領域外のメモリを上書きされ、意図しないコードを実行してしまうこと。
ファイアウォール	ネットワークの境界に配置して特定の通信を遮断する装置のこと。
プラグイン	Web ブラウザの拡張機能のこと。
マルチテナント	複数の利用者で同一サービスを共有して利用すること。
メールヘッダ・インジェクション	Web アプリケーションで利用者が入力した商品申し込みやアンケート等の内容を、特定のメールアドレスに送信する機能を持つものがあり、外部の利用者がこのメールアドレスを自由に指定できてしまう脆弱性のこと。

1. はじめに

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）では、信頼できるセキュリティ製品・サービスとセキュリティに関する隠れたニーズとを掘り起こし、それらの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。新型コロナウィルス感染拡大を契機に急速にデジタル化・IT 化への期待が進む一方で、サイバー攻撃は衰えることなく、その対策としてセキュリティ製品の活用が求められている。国内では現在、セキュリティ製品の多くが海外製品で占められているが、日本で開発された新たなセキュリティ製品の市場参入を促進するためには、サイバー攻撃の脅威や対策動向等を踏まえ、今後重要度が増すと考えられる製品分野を明らかにする必要がある。加えて、その分野に該当する国産のセキュリティ製品に対し、有効性検証・実環境における試行導入検証を実施しその内容を発信することが、ユーザの国産製品選定を容易にすると考えられる。

これを受けて独立行政法人情報処理推進機構（以下、IPA）は、実際にセキュリティ製品を検証し、結果を公表する「セキュリティ製品の有効性検証」の仕組みの構築を行った。これにさきがけて、2019 年 9 月に立ち上げた「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（以下、有識者会議）」において、検証の具体的な試行を行うこととし、検証対象となる製品分野、検証方法などにおける課題やあるべき姿を抽出することを目的に試行的な検証を行ってきた。

今年度は、昨年度構築した基盤を運用して検証対象候補製品を公募し、その中から対象製品を選定して検証を実施した。有識者会議の検討において、今年度は「脅威の可視化」、「リスクの可視化・緩和」、「データ保護」、「ID/アクセス管理」に係る製品分野を検証対象とすることを方針とするとともに、以下の 2 種類の製品種別（種別 A/種別 B）を対象に検証を実施することとした。

[種別 A]

日本の市場において新規性の高いセキュリティに関する機能を有する製品とする。種別 A に応募する応募者は応募書類の中で、上記に該当する機能があることを説明するものとし、上記に該当する機能が応募書類等の説明内容通りであることを検証する対象とする。

[種別 B]

セキュリティ機能に関する優れたユーザビリティを備えた製品とする。種別 B に応募する応募者は応募書類の中で、該当するユーザビリティを明記するものとし、種別 B の製品は、上記に該

当するユーザビリティが応募書類の説明内容通りであることを、検証する対象とする。

本報告書は、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有効性検証を行った結果を報告するものである。今年度は種別 A・種別 B について、それぞれ 1 製品を選定し、検証を実施した。以下では、種別 B にて選定した株式会社エーアイセキュリティラボ(以下、製品ベンダ)の「AeyeScan」を対象に実施した有効性検証の検証結果について示す。

2. 検証対象製品について

2.1 検証対象製品を取り巻く環境

近年の開発・CSIRT・リスクマネジメントの現場において、以下のような課題・要望がある。

- セキュリティコードレビュー、テストに時間がかかり生産性が低下している。
- サイトの公開、リリースの事業状況にあわせて柔軟に脆弱性診断したい。
- コストが理由で脆弱性診断の実施を断念しているサイトがある。
- 脆弱性診断費用を抑えたい。

これらの課題・要望への解決策として脆弱性診断の内製化があるものの、脆弱性診断の内製化には以下のような課題がある。

- 自社で出来るか不安。
- 専任者が必要。
- 診断項目が不足、レポートがわからない。

2.2 製品概要

AeyeScan は、AI や RPA を活用した SaaS 型 Web アプリケーション脆弱性診断ツールである。

診断結果は画面キャプチャ付きの画面遷移図で可視化するだけでなく、わかりやすい日本語レポートを提供する。また共有アカウントの発行・管理、巡回診断スケジュールの設定等、脆弱性診断の内製化に必要な機能を提供する。

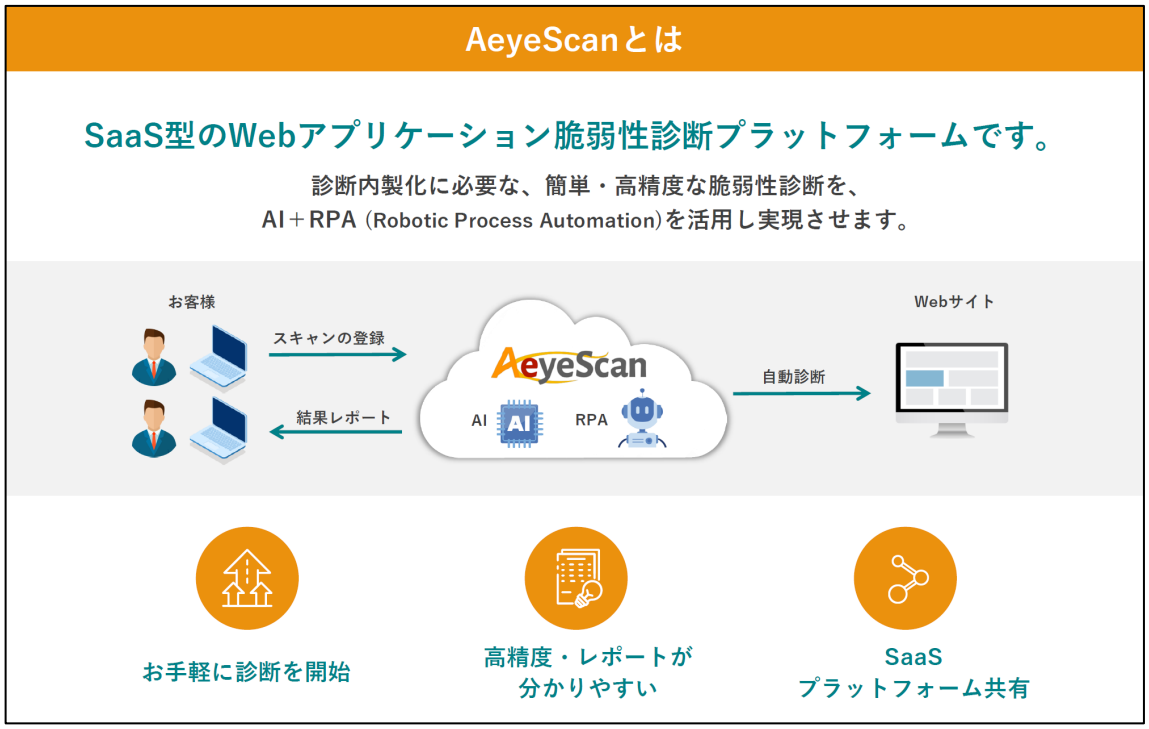


図 2-1 AeyeScan 製品概要

製品ベンダは、脆弱性診断の内製化に対する課題を解決するため、本製品の特徴として以下の 3 点を挙げている。

- 簡単操作
  - Web セキュリティの知識や Web アプリケーションの開発経験がなくても始められる。
- 業務の片手間で診断可能
  - SaaS 環境なので 24 時間放置。
  - AI と RPA による自動操作によって最短 10 分で診断を開始することができる。
- 業界標準の項目、わかりやすいレポート
  - 業界標準の脆弱性診断項目と評価基準レポート。
  - 画面遷移図の見やすいレポート。

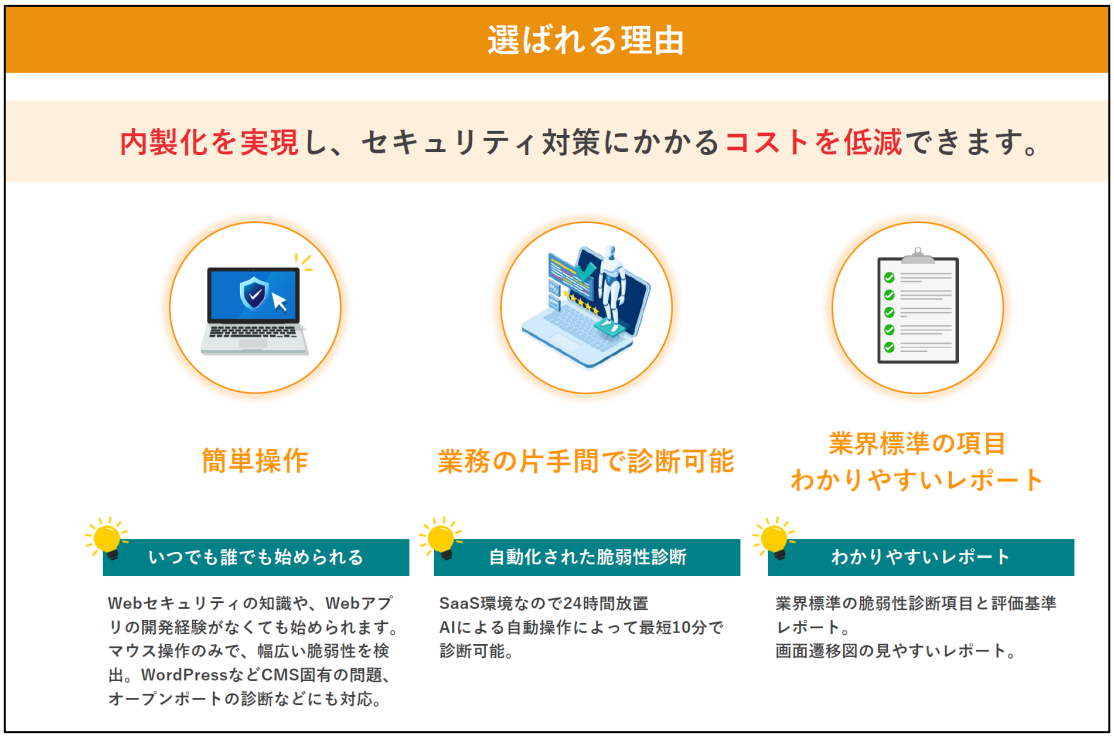


図 2-2 AeyeScan の特徴

2.3 製品の導入事例

2.3.1 大手情報通信会社での導入事例

大手情報通信会社が提供しているセキュリティ診断サービスにおいて、従来のセキュリティ診断サービスではコストや時間、リソースの問題でやむを得ず検査対象外としてきたより多くのページについても、AI と RPA を組み合わせて診断を実施できる新しいサービスを提供するため、本製品が採用された。

2.3.2 大手独立系システムインテグレーターでの導入事例

大手独立系システムインテグレーターにおいて、プロジェクトごと、担当者ごとにばらつきのあったセキュア開発のルール化を進める中で、もっと簡易かつ低コストで診断できる何らかの方法を提供したいという要望があり、本製品が採用された。

2.3.3 スタートアップ企業での導入事例

SaaS サービスを提供しているスタートアップ企業において、しっかりとした脆弱性対応を行いつつ、リリース速度を下げたくないという要望があり、脆弱性の発見から修正、再確認というプロセスを開発フローの中に組み込むため、本製品が採用された。

3. 検証するセキュリティに関する優れたユーザビリティ・検証項目

3.1 検証するセキュリティに関する優れたユーザビリティ

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項のうち、本検証では以下の 4 つの事項に対して検証を実施した。

（1） 機能充足性

「IPA の安全な Web サイトの作り方」[22]のガイドライン等の診断項目の充足性が優れている。また、AI や RPA 技術を活用した自動クローリング能力が優れている。

（2） 機能正確性

ブラウザやクラウド環境を活用した脆弱性の検出能力が優れている。また、画面クローリング性能（範囲、深度）が優れている。

（3） 効率性・運用操作性

特別な設定が不要で、脆弱性診断が完了する点が優れている。また、画面遷移図で脆弱性の検出箇所を視覚的に分かりやすくレポートできる点が優れている。

（4） 習得性

設定項目が少なく、操作が容易である点が優れている。

3.2 検証項目・検証方法

3.2.1 検証項目・検証方法の策定方針

検証項目・検証方法の策定方針は以下のとおりとする。

- 検証項目・検証方法の策定期間を可能な限り短縮するために、製品決定前に検証項目マスターリスト及び検証方法マスターリストを策定する。

[22] https://www.ipa.go.jp/security/vuln/websecurity.html

- 検証対象製品が決定次第、検証実施者、製品ベンダ及び検証協力ユーザと協議し、検証項目マスターリストの項目を具体化して検証項目を策定する。
- 検証項目の策定にあたり、IPA が公開している「試行導入・導入実績公表の手引き」も参照する。
- 検証対象製品が決定次第、検証実施者、製品ベンダ及び検証協力ユーザと協議し、検証方法マスターリストの項目を具体化して検証方法を策定する。
- 検証実施にあたって、可能な限り検証環境での実検証を重視するが、セキュリティに関する優れたユーザビリティ項目に対する検証が求められるところは検証協力ユーザに対するヒアリングを実施する。
- 策定した検証項目・検証方法は有識者による確認・審議をもって確定とする。

3.2.2 検証項目・検証方法の策定結果

AeyeScan のセキュリティに関する優れたユーザビリティとされている事項を検証するための検証項目を策定した。検証項目は、検証のための 5 つの分類（「機能充足性」、「機能正確性」、「効率性・運用操作性」、「習得性」、「その他」）から具体化したものである。各検証項目に対して、「検証環境での実検証」、「検証協力ユーザに対するヒアリングに基づく評価」、「データや記録に基づく評価」、「ベンダヒアリングに基づく評価」の 4 つの方法のうち、どの方法で検証を行うか決定した。

（1） 「機能充足性」に関する検証項目・検証方法

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項を踏まえ、「機能充足性」に関して、表 3-1 に示す検証項目を決定した検証方法で検証した。

表 3-1 「機能充足性」に関する検証項目・検証方法

検証項目			検証方法			
No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
1-1	監視、検知、通知	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙			✓	

		される脆弱性項目が対象に含まれていること				
1-2		リンクから辿れないページは手動で分析可能であること	✓			
1-3	自動分析	AI や RPA によるフォーム自動入力値が正しいこと	✓			✓
1-4		分析時の画面遷移は自動的に実行されること	✓		✓	

(2) 「機能正確性」に関する検証項目・検証方法

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項を踏まえ、「機能正確性」に関して、表 3-2 に示す検証項目を決定した検証方法で検証した。

表 3-2 「機能正確性」に関する検証項目・検証方法

検証項目			検証方法			
No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
2-1	検知の正確性	「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性が検出されること	✓	✓	✓	
2-2		自動クロールによる	✓			

		巡回結果（画面遷移図）が実際の画面と一致していること				

（3） 「効率性・運用操作性」に関する検証項目・検証方法

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項を踏まえ、「効率性・運用操作性」に関して、表 3-3 に示す検証項目を決定した検証方法で検証した。

表 3-3 「効率性・運用操作性」に関する検証項目・検証方法

検証項目			検証方法			
No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
3-1	レポーティング	脆弱性の検出箇所を視覚的に分かりやすくレポートできること	✓	✓		
3-2	操作性	人間による操作時間を計測し、妥当な時間内に完了していること	✓	✓	✓	
3-3		CI ツール等と連携し、診断の自動化が可能であること。	✓		✓	
3-4		運用操作性について検証協力ユーザの観点から良好であること	✓	✓		

（4） 「習得性」に関する検証項目・検証方法

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項を踏まえ、「習得性」に関して、表 3-4 に示す検証項目を決定した検証方法で検証した。

表 3-4 「習得性」に関する検証項目・検証方法

検証項目			検証方法			
No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
4-1	習得性	初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していること	✓	✓		
4-2		マニュアル、サポートデスクの提供により理解・習得が容易であること	✓	✓		
4-3		習得性について検証協力ユーザの観点から良好であること	✓	✓		

（5） 「その他」に関する検証項目・検証方法

AeyeScan のセキュリティに関する優れたユーザビリティとされる事項を踏まえ、「その他」に関して、表 3-5 に示す検証項目を決定した検証方法で検証した。

表 3-5 「その他」に関する検証項目・検証方法

検証項目			検証方法			
No.	区分	検証項目	検証環境での実検証	検証協力ユーザに対するヒアリングに基づく評価	データや記録に基づく評価	ベンダヒアリングに基づく評価
5-1	認証	多要素認証によりユーザ認証ができること	✓			✓
5-2	データ保持	取得データの所在地（リージョン）が日本国内であること				✓
5-3		プライバシーポリシー（個人情報保護方針）を明記していること			✓	

4. 検証環境・検証条件

4.1 検証環境

以下の 3 つの検証用 Web サイトを AWS 上に構築した。

- 検証用 Web サイト①：OWASP Benchmark を稼働させた Web サイト(図 4-1)
- 検証用 Web サイト②：日本語入力フォーム画面を含む自作の Web サイト(図 4-2)
- 検証用 Web サイト③：OWASP Juice Shop を稼働させた Web サイト(図 4-3)

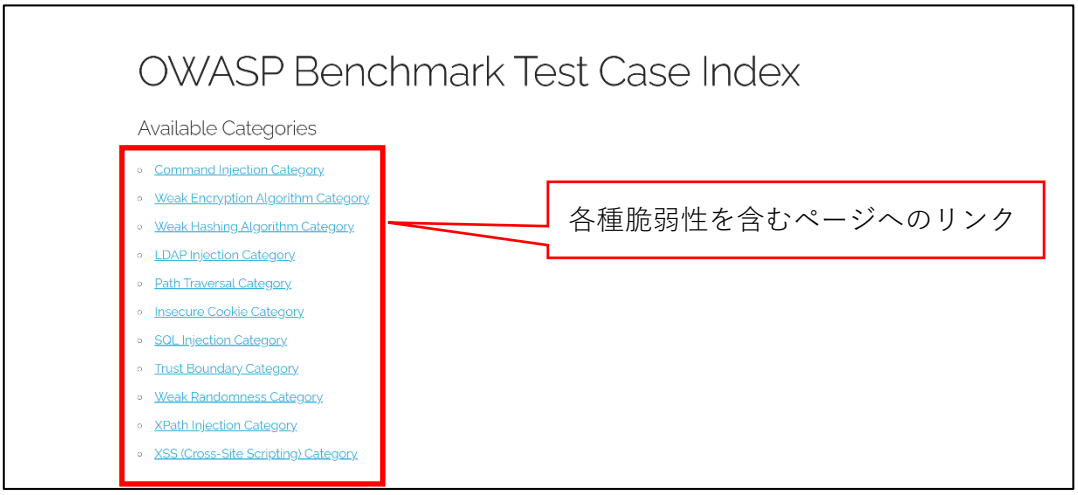


図 4-1 検証用 Web サイト①画面イメージ

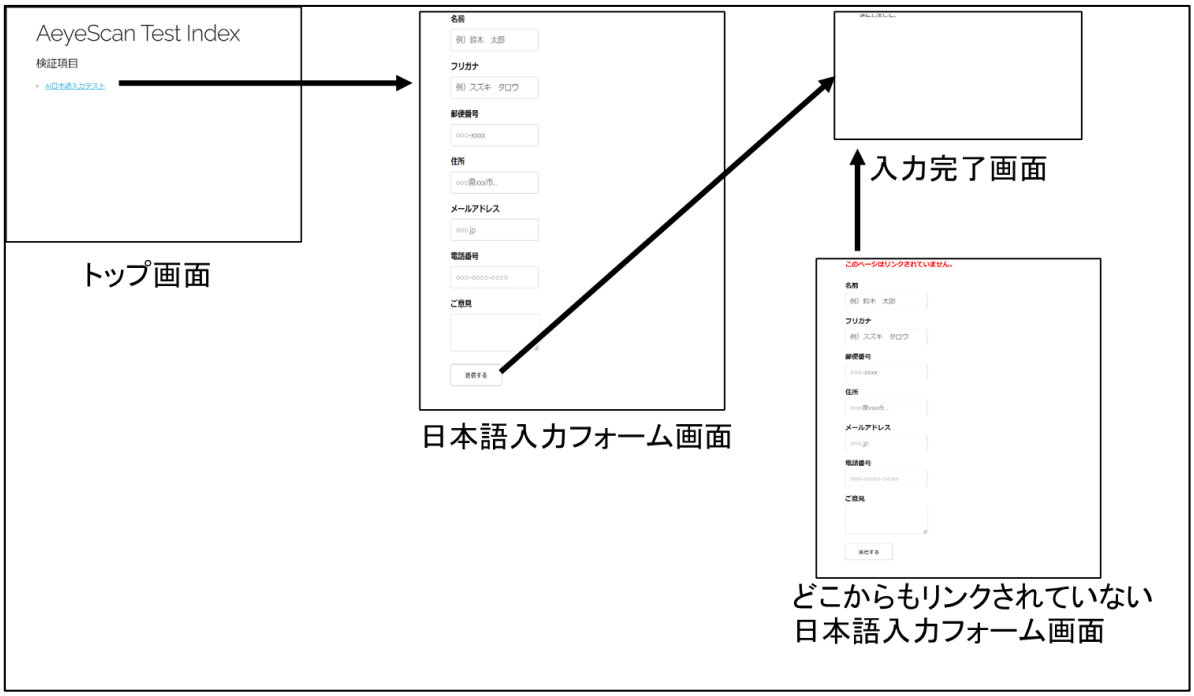


図 4-2 検証用 Web サイト②画面イメージ

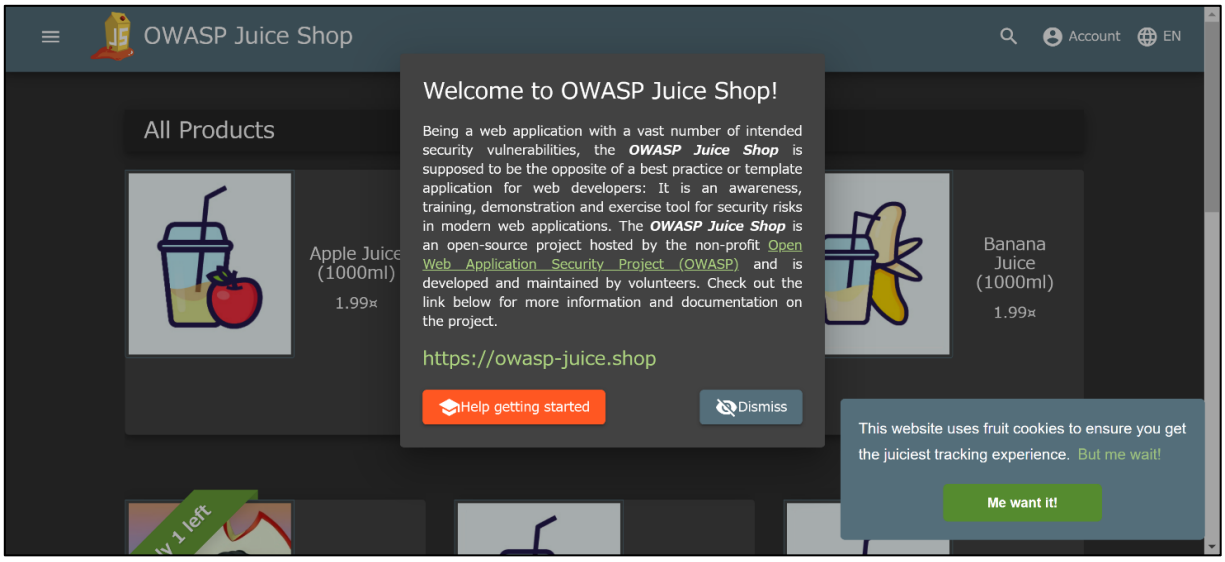


図 4-3 検証用 Web サイト③画面イメージ

AeyeScan の利用にあたって、まずアカウント情報が提供された後、スキャン一覧画面にて検証用 Web サイト①、②、③を新規登録した。その後、その登録情報に対して脆弱性診断を実施するための設定をした後、診断を実行することで各検証項目を検証した。(図 4-4)

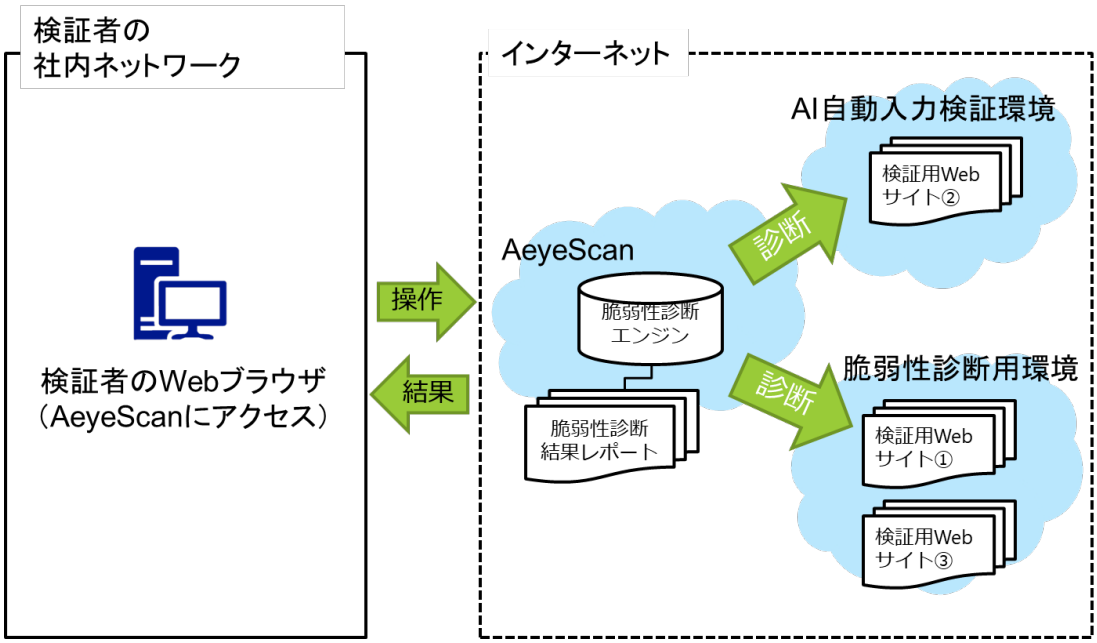


図 4-4 AeyeScan からの脆弱性診断イメージ

4.2 検証条件

検証用 Web サイトは AeyeScan からのアクセスのみを IP アドレス制限により許可した。

また、診断項目を確認するために、IPA の安全なウェブサイトの作り方に掲載されている以下の脆弱性を検出させ、診断結果を検証した。

- SQL インジェクション
- OS コマンド・インジェクション
- パス名パラメータの未チェック／ディレクトリ・トラバーサル
- セッション管理の不備
- クロスサイト・スクリプティング
- CSRF（クロスサイト・リクエスト・フォージェリ）
- HTTP ヘッダ・インジェクション
- メールヘッダ・インジェクション
- クリックジャッキング
- バッファオーバーフロー
- アクセス制御や認可制御の欠落

検証するセキュリティに関する優れたユーザビリティとされる事項のうち「IPA の安全な Web サイトの作り方」のガイドライン等の診断項目の充足性については、上記の診断結果と、製品ベンダが機能仕様として公開している診断可能項目に基づき評価を行った。

4.3 検証協力ユーザ

検証協力ユーザの担当者のプロフィールは以下のとおりである、

- 社内ＩＴを技術統括する部門に所属しており、セキュリティ施策の策定や強化、製品の技術検証などに携わっている。
- ユーザ企業として AeyeScan を利用する立場で本検証に参加している。
- AeyeScan の利用は今回が初めてである。
- 自社で携わっている EC サイトのテスト環境に対して AeyeScan で脆弱性診断を試行しており、セキュリティがわからない人でもどれくらい使えるか等の観点でチェックしている。

本検証において、検証協力ユーザとしての立場で以下の意見をいただいた。

- 検証項目
  - 項目数や内容についてレビューしていただいた。
- 検証結果
  - 主に定性的な検証項目に対する検証結果について意見をいただいた。内容については、当該検証結果にて記載する。
- 報告書
  - 報告書の内容全般について意見をいただいた。内容については、まとめにて記載する。

5. 検証結果

5.1 「機能充足性」に関する検証結果

5.1.1 検証項目 1-1 の検証結果

（1） 検証項目の内容

「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性項目が対象に含まれていること。

（2） 検証結果

データや記録に基づく評価により、「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性項目が診断項目に含まれていることを確認した。

（3） 検証内容の詳細

本検証項目はデータや記録に基づく評価により実施した。

AeyeScan の製品仕様として「IPA の安全な Web サイトの作り方」で提示された 11 種類の Web アプリケーションの脆弱性がすべて診断項目に含まれていることを確認した。それ以外のガイドライン等の観点として、OWASP TOP10 と ASVS 4.0 も診断項目に含まれていることを確認した。

AeyeScan の診断項目に含まれている脆弱性を以下に示す。

表 5-1 IPA の安全な Web サイトの作り方で示された脆弱性

名称	AeyeScan の診断項目
1) SQL インジェクション	○
2) OS コマンド・インジェクション	○
3) パス名パラメータの未チェック／ディレクトリ・トラバーサル	○

名称	AeyeScan の診断項目
4) セッション管理の不備	○
5) クロスサイト・スクリプティング	○
6) CSRF（クロスサイト・リクエスト・フォージェリ）	○
7) HTTP ヘッダ・インジェクション	○
8) メールヘッダ・インジェクション	○
9) クリックジャッキング	○
10) バッファオーバーフロー	○
11) アクセス制御や認可制御の欠落	○

表 5-2 OWASP TOP10 で示された脆弱性

名称	AeyeScan の診断項目
A1:2017-インジェクション	○
A2:2017-認証の不備	○
A3:2017-機微な情報の露出	○
A4:2017-XML 外部エンティティ参照(XXE)	○
A5:2017-アクセス制御の不備	○
A6:2017-不適切なセキュリティ設定	○
A7:2017-クロスサイト・スクリプティング(XSS)	○
A8:2017-安全でないデシリアライゼーション	○
A9:2017-既知の脆弱性のあるコンポーネントの使用	○
A10:2017-不十分なロギングとモニタリング	-(※1)
Other:その他	○

(※1) Web アプリケーションに対する診断では検出不可能なため対象外

表 5-3 ASVS 4.0 で示された脆弱性（抜粋）

名称	AeyeScan の診断項目
2.1.4 パスワードに Unicode 文字が使用できる。単一の Unicode 符号点は文字と見なされるため、12 文字の絵文字や 64 文字の漢字が有効に使用できる必要があります。	○
2.1.6 パスワード変更機能には、ユーザの現在のパスワードと新しいパスワードが必要とされる。	○
2.1.11 パスワード入力に対して、ペースト、ブラウザのパスワードヘルパー、および外部パスワードマネージャが使用できる。	○
2.5.2 パスワードのヒントや知識ベースの認証（いわゆる「秘密の質問」）が存在しない。	○
2.5.4 共有アカウントまたはデフォルトアカウントが存在しない（例えば"root", "admin", "sa"）。	○
3.1.1 アプリケーションが URL パラメータやエラーメッセージ内にセッショントークンを漏洩しない。	○
3.7.1 機密性の高いトランザクションやアカウントの変更を許可する前に、アプリケーションが完全で有効なログインセッションを確保していること、または再認証や二次検証を必要としている。	○
4.1.1 特に、クライアント側のアクセス制御が存在し、それが迂回される可能性がある場合には、アプリケーションは信頼できるサービスレイヤに対してアクセス制御ルールを適用する。	○
4.1.2 アクセス制御で使用されるすべてのユーザ属性とデータ属性およびポリシー情報は、特に認可されていない限りエンドユーザによって操作されない。	○

5.1.2 検証項目 1-2 の検証結果

（1） 検証項目の内容

リンクから辿れないページは手動で分析可能であること。

（2） 検証結果

実検証により、リンクから辿れないページは手動で分析可能であることを確認した。

（3） 検証内容の詳細

本検証項目は実検証により実施した。

AeyeScan では指定した URL を起点にリンクやフォームを辿って自動巡回して診断を実施する製品であるが、リンクから辿れないページや、特定の狭い範囲のページだけ診断を実施したい場合に手動巡回を行う機能を持っている。製品ベンダが公開している手動巡回プラグインをインストールしたブラウザでアクセスし、手動巡回を行う対象ページを記録し、記録したファイルを AeyeScan にインポートすることで記録したページに対する巡回・診断が可能となる。

まず以下の画面遷移を行う検証用 Web サイト②を作成した。矢印はリンクまたはフォームのボタンクリックによる画面遷移を示す。（図 5-1）

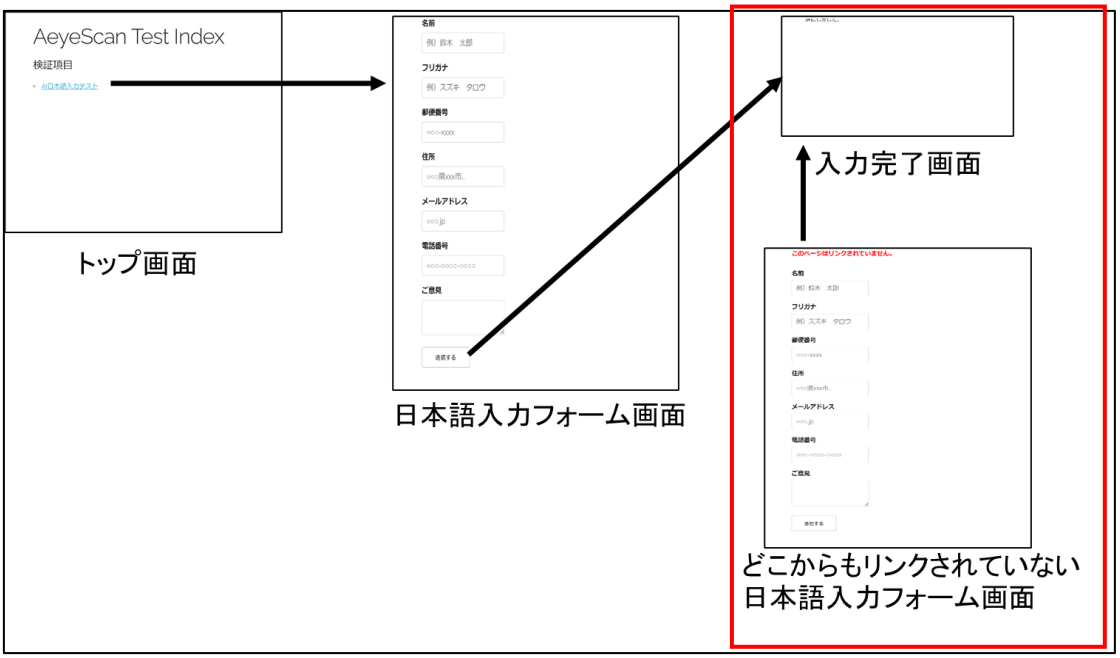


図 5-1 検証用 Web サイト②

上記の赤枠の画面については自動巡回できないため、以下の手順で手動巡回した。（図 5-2）

- 手動巡回プラグインを Chrome ウェブストアよりダウンロード、インストール。
- 手動巡回プラグインで各画面を巡回。
- 巡回データをダウンロード。
- 巡回データを AeyeScan にインポート。

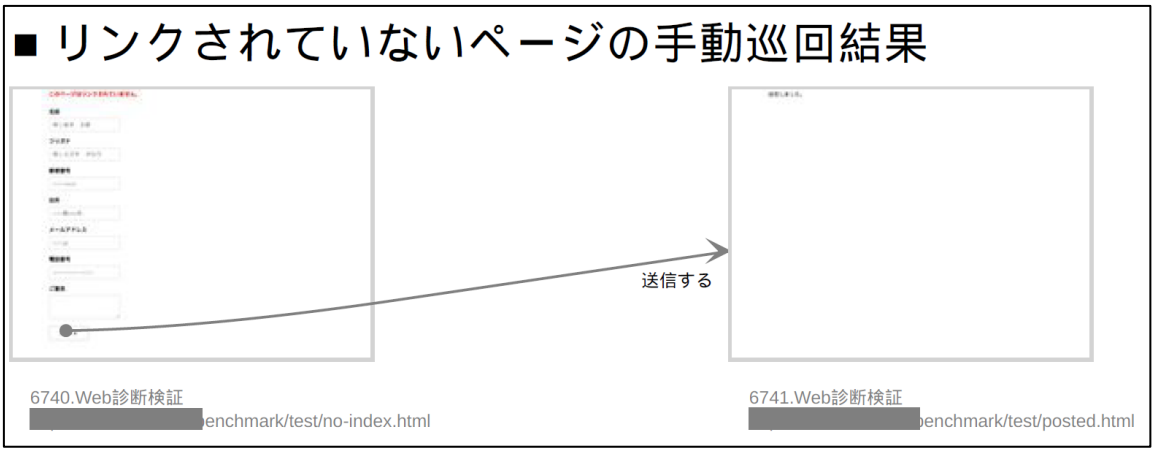


図 5-2 インポートした手動巡回結果

上記の手動巡回した画面遷移図に対して診断が実施されたことを確認した。

5.1.3 検証項目 1-3 の検証結果

(1) 検証項目の内容

AI や RPA によるフォーム自動入力値が正しいこと。

(2) 検証結果

実検証及びベンダヒアリングに基づく評価により、AI や RPA によるフォーム自動入力値が正しいことを確認した。

(3) 検証内容の詳細

本検証項目は実検証及びベンダヒアリングに基づく評価により実施した。

まず以下の入力フォームを持つ検証用 Web サイト②を作成し、日本語ラベルの内容に基づいた入力値が AI や RPA により自動入力されることを検証した。(図 5-3)

図 5-3 日本語入力フォーム画面

診断時に自動入力された値については、日本語ラベルの内容に基づいた入力値が AI や RPA により自動入力されることを確認した。（図 5-4）

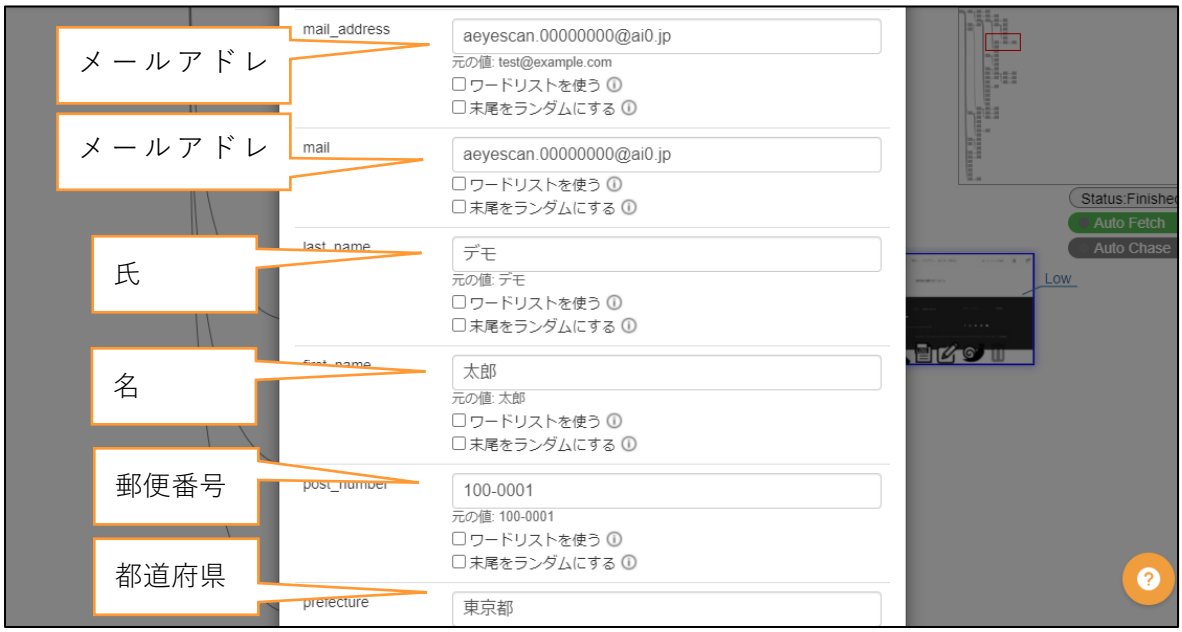


図 5-4 AI や RPA による自動入力値

また、AeyeScan において AI や RPA がどの機能に活用されているのかベンダヒアリングを行い、以下の点を確認した。

- ブラウザに表示された情報（「ボタン名」「アイコン種別」「CAPTCHA 画像」など）を AI で解析し、フォーム入力値と機能種別の自動判別に利用している。
  - フォーム入力値の自動判別は「当該ページに検索機能がある場合、検索用のワードを入力する」などの用途で使用している。
  - 機能種別の自動判別は「削除機能などの危険な操作は出来るだけ実行しない」などの用途で使用している。

5.1.4　検証項目 1-4 の検証結果

（1）　検証項目の内容

分析時の画面遷移は自動的に実行されること。

（2）　検証結果

実検証及びデータや記録に基づく評価により、分析時の画面遷移は自動的に実行されることを確認した。

（3）　検証内容の詳細

本検証項目は実検証及びデータや記録に基づく評価により実施した。

まず以下の画面遷移を行う検証用 Web サイト②を作成した。矢印はリンクまたはフォームのボタンクリックによる画面遷移を示す。（図 5-5）

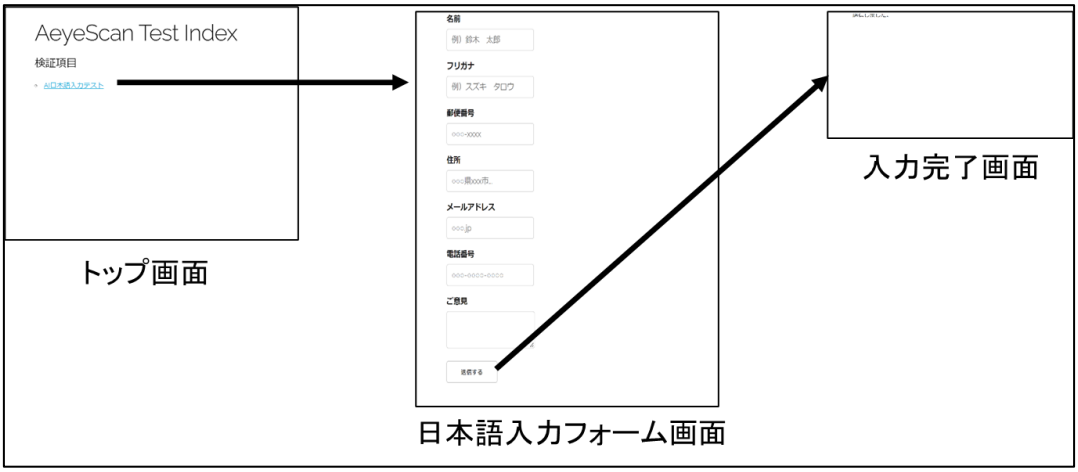


図 5-5 検証用 Web サイト②

上記の検証環境に対して AeyeScan で診断を実施し、診断完了後に自動的に出力された画面遷

移図は以下のとおりであった。（図 5-6）

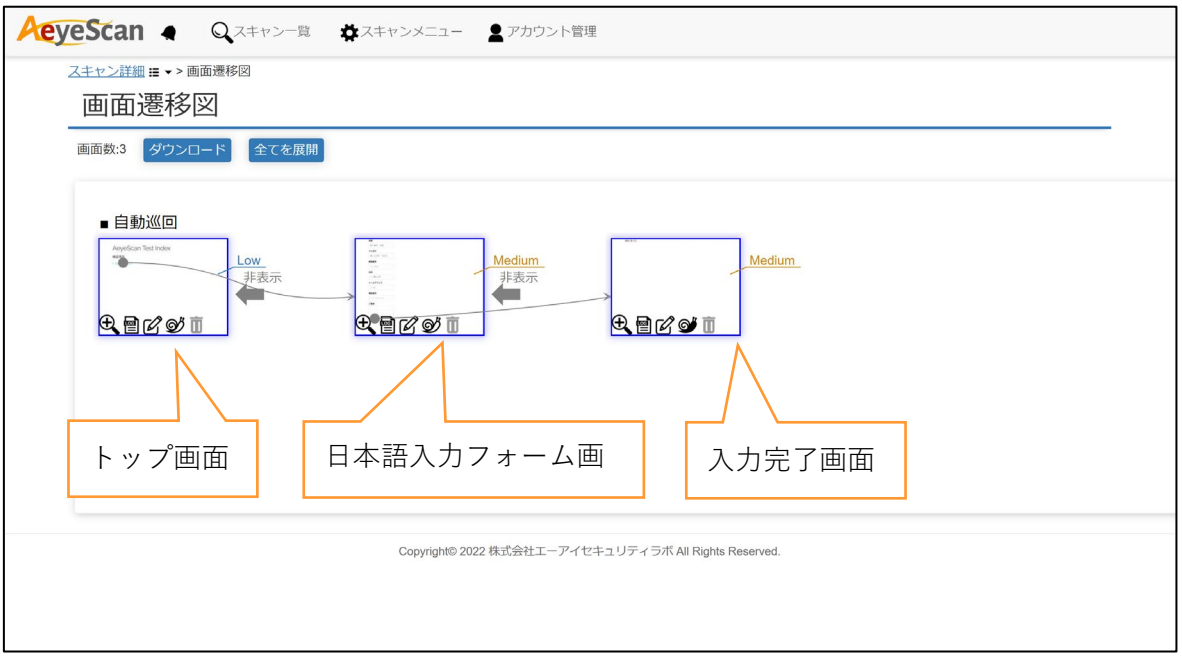


図 5-6 AeyeScan が自動出力した画面遷移図

トップ画面から入力完了画面までの計 3 画面が画面遷移図に出力されていることから、分析時の画面遷移は自動的に実行されることを確認した。

また、製品ベンダから提供されたデータに基づいて、AeyeScan にログイン ID とパスワードを事前に設定しておくことで、ログインが必要なページ（図 5-7）や Basic 認証が必要なページ（図 5-8）に対しても分析時の画面遷移は自動的に実行されることを確認した。

図 5-7 通常ログイン設定

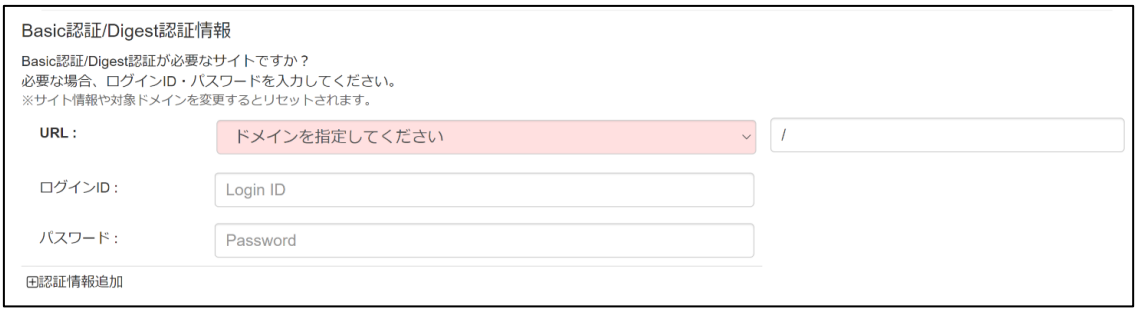


図 5-8 Basic 認証設定

5.2 「機能正確性」に関する検証結果

5.2.1 検証項目 2-1 の検証結果

(1) 検証項目の内容

「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性が検出されること。

(2) 検証結果

実検証、検証協力ユーザに対するヒアリング及びデータや記録に基づく評価により、「IPA の安全な Web サイトの作り方」等のガイドラインに列挙される脆弱性が検出されることを確認した。

(3) 検証内容の詳細

本検証項目は実検証、検証協力ユーザに対するヒアリング及びデータや記録に基づく評価により実施した。

AeyeScan の製品仕様としては「IPA の安全な Web サイトの作り方」で提示された 11 種類の Web アプリケーションの脆弱性をすべて診断項目として含まれており、そのうち 4 種類を対象として実検証を実施した。

表 5-4 IPA の安全な Web サイトの作り方で示された脆弱性

名称	実検証に基づく評価	データや記録に基づく評価
1) SQL インジェクション	○	○
2) OS コマンド・インジェクション	○	○
3) パス名パラメータの未チェック	○	○

名称	実検証に基づく評価	データや記録に基づく評価
／ディレクトリ・トラバーサル		
4）セッション管理の不備	-	○
5）クロスサイト・スクリプティング	○	○
6) CSRF（クロスサイト・リクエスト・フォージェリ）	-	○
7) HTTP ヘッダ・インジェクション	-	○
8）メールヘッダ・インジェクション	-	○
9）クリックジャッキング	-	○
10）バッファオーバーフロー	-	○
11）アクセス制御や認可制御の欠落	-	○

まず検証用 Web サイト①に OWASP Benchmark を稼働させた状態で、以下の 4 つの脆弱性カテゴリについて診断を実施した。（図 5-9、図 5-10）

- SQL インジェクション
- OS コマンド・インジェクション
- クロスサイト・スクリプティング
- ディレクトリ・トラバーサル

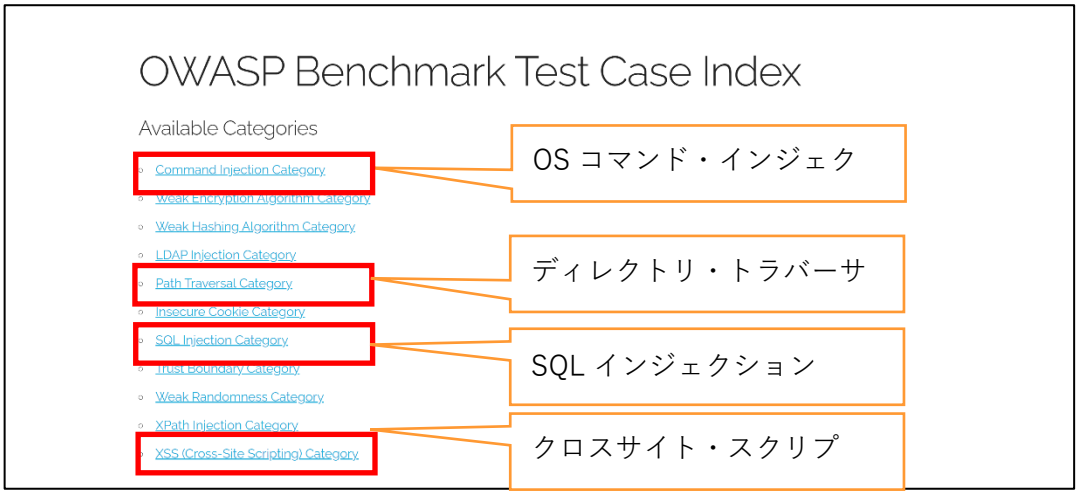


図 5-9 OWASP Benchmark 画面イメージ

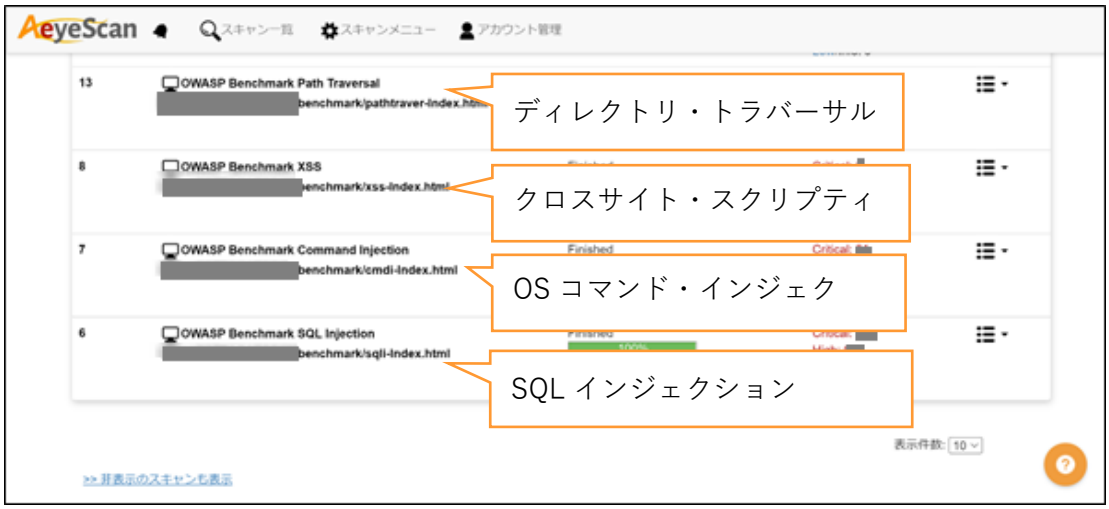


図 5-10 AeyeScan 診断イメージ

診断を実施後、出力された診断レポートから当該脆弱性が検出されたことを確認した。(図 5-11、図 5-12、図 5-13、図 5-14)

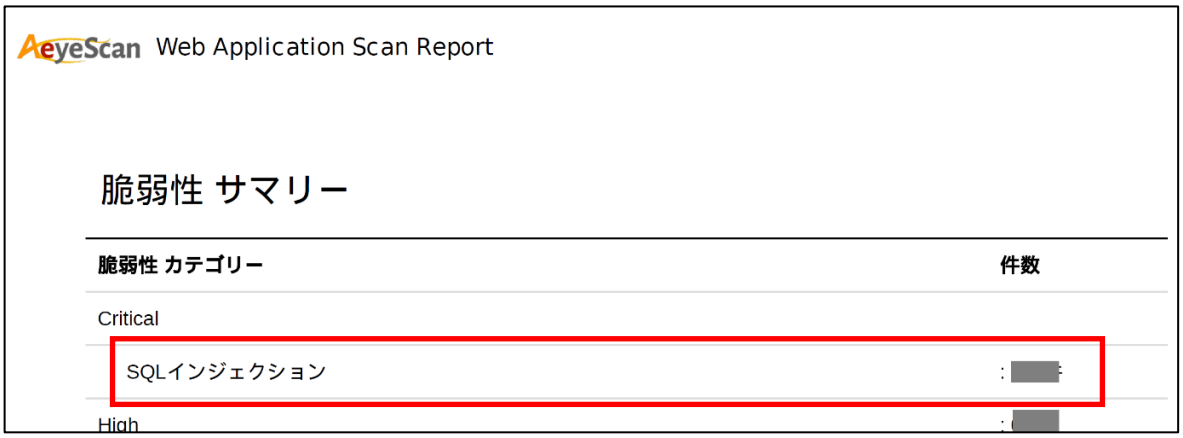
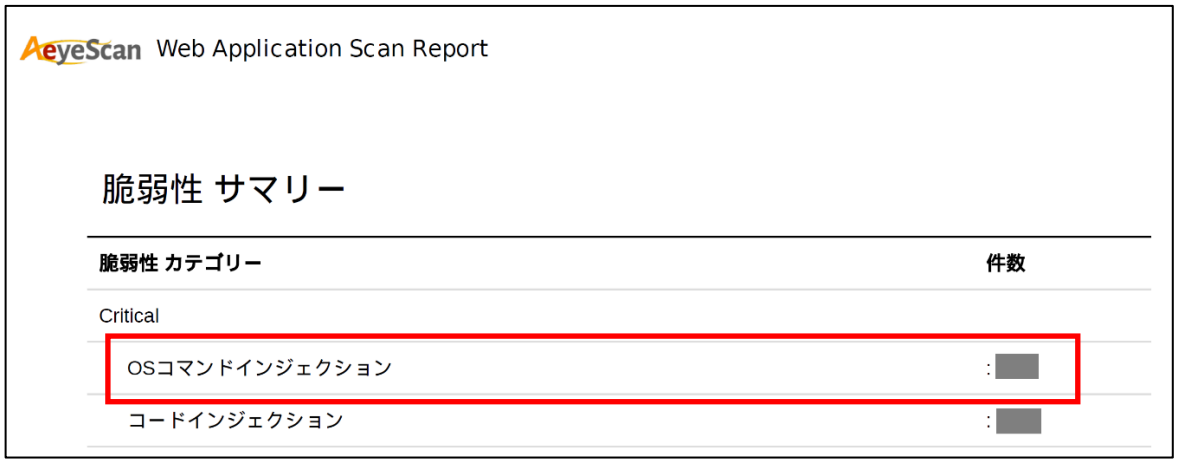


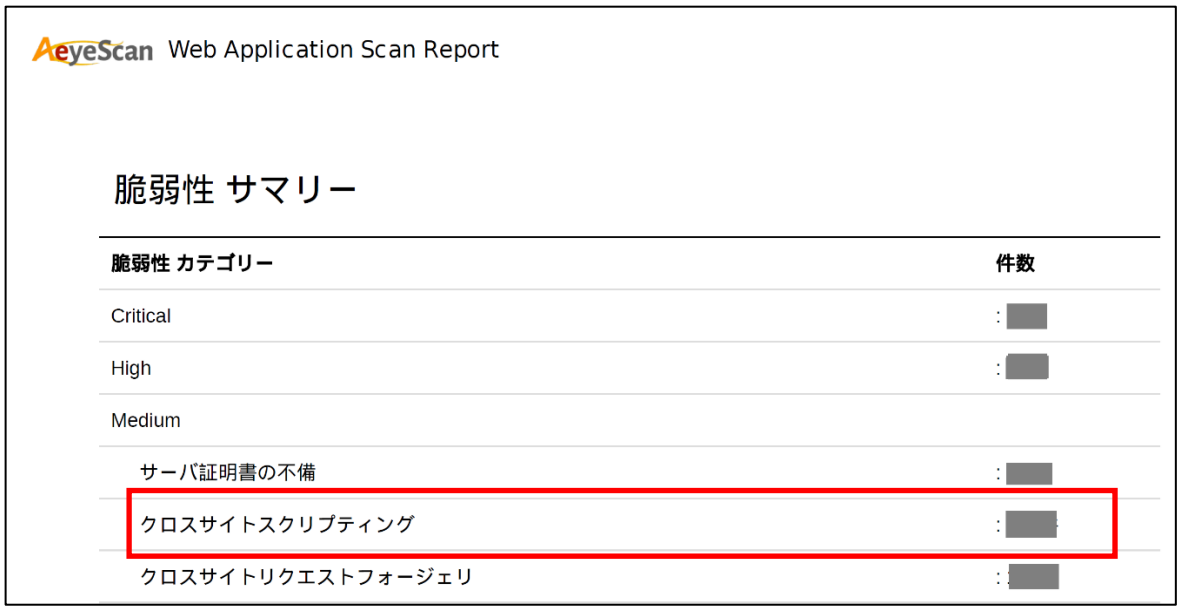
図 5-11 SQL インジェクション診断レポートサマリー(抜粋)


AeyeScan Web Application Scan Report

脆弱性 サマリー

脆弱性 カテゴリー	件数
Critical	
OSコマンドインジェクション	: [redacted]
コードインジェクション	: [redacted]

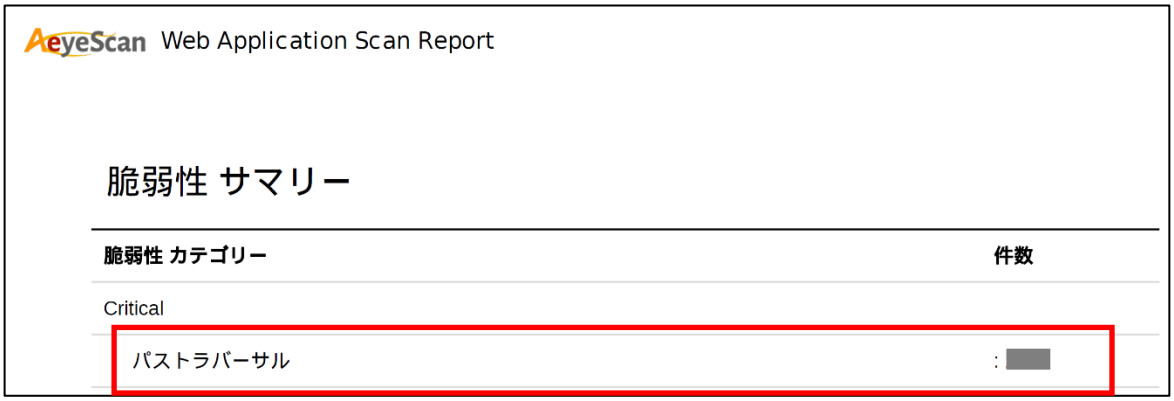
図 5-12 OS コマンド・インジェクション診断レポートサマリー(抜粋)


AeyeScan Web Application Scan Report

脆弱性 サマリー

脆弱性 カテゴリー	件数
Critical	: [redacted]
High	: [redacted]
Medium	
サーバ証明書の不備	: [redacted]
クロスサイトスクリプティング	: [redacted]
クロスサイトリクエストフォージェリ	: [redacted]

図 5-13 クロスサイト・スクリプティング診断レポートサマリー(抜粋)


AeyeScan Web Application Scan Report

脆弱性 サマリー

脆弱性 カテゴリー	件数
Critical	
パストラバーサル	: [redacted]

図 5-14 ディレクトリ・トラバーサル診断レポートサマリー(抜粋)

また、近年の Web アプリケーションで使用されることも多い SPA についても AeyeScan は診

断可能である。参考までに、検証用 Web サイト③(図 5-15)に OWASP Juice Shop を稼働させた状態で診断を実施した。診断は正常に完了し、出力された診断レポートから複数の脆弱性が検出されたことを確認した。

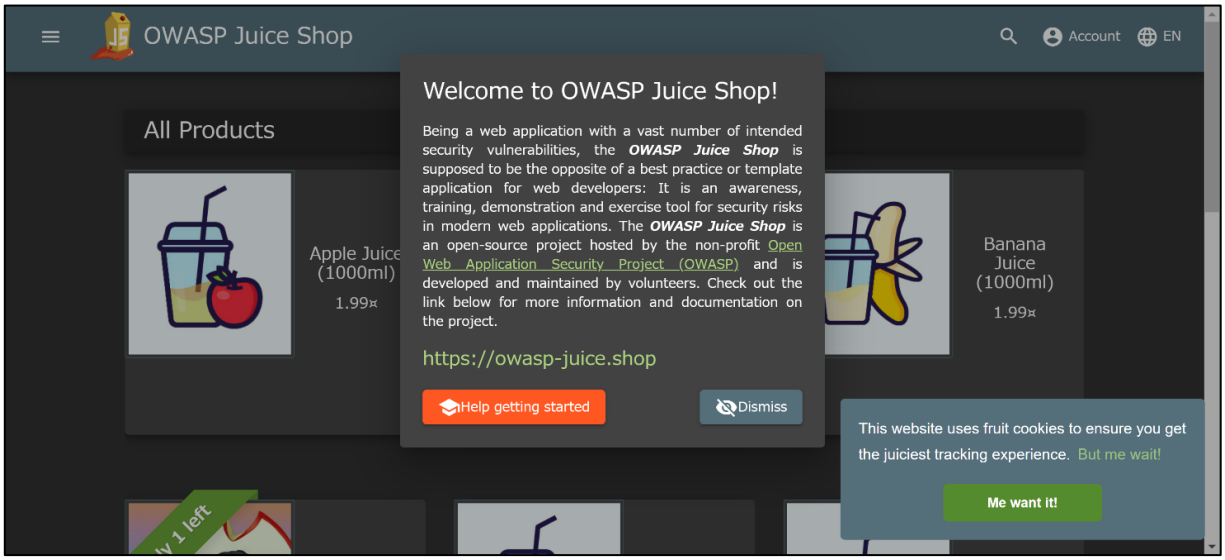


図 5-15 検証用 Web サイト③画面イメージ

1） 検証協力ユーザからの意見

検証協力ユーザから、検出されるはずの脆弱性が検出できていない箇所があるとの指摘があったため製品ベンダに確認したところ、当該画面が自動巡回できていないことが原因とのことで、製品ベンダ側の再検証により、手動巡回機能では正常な検出が可能であることを確認した。

自動巡回の精度については改善を継続的に取り組むとの回答を製品ベンダよりいただいた。

5.2.2 検証項目 2-2 の検証結果

（1） 検証項目の内容

自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していること。

（2） 検証結果

実検証により、自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していることを確認した。

（3） 検証内容の詳細

本検証項目は実検証により実施した。

検証項目 1-4 の検証結果により、自動クロールによる巡回結果（画面遷移図）が実際の画面と一致していることを確認した。

5.3 「効率性・運用操作性」に関する検証結果

5.3.1 検証項目 3-1 の検証結果

（1） 検証項目の内容

脆弱性の検出箇所を視覚的に分かりやすくレポートできること。

（2） 検証結果

実検証及び検証協力ユーザに対するヒアリングに基づく評価により、脆弱性の検出箇所を視覚的に分かりやすくレポートできることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及び検証協力ユーザに対するヒアリングに基づく評価により実施した。

検証実施者が検証項目 2-1 で検証した SQL インジェクションの診断レポートには、まず検出画面のスクリーンショットが掲載されており、視覚的にわかりやすく配慮されていることを確認した。（図 5-16）

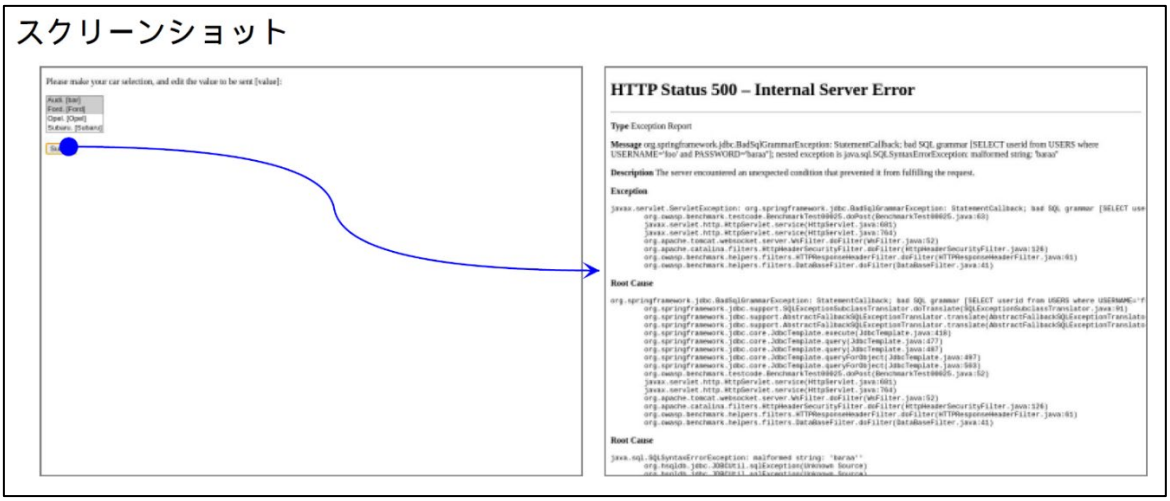


図 5-16 検出画面のスクリーンショット

次に、同レポートには脆弱性が見つかった箇所として以下の情報が明示されていることで、脆弱性の検出箇所が視覚的にわかりやすくレポートされていることを確認した。（図 5-17）

- 脆弱性検出画面
- 詳細ログ URL
- パラメータタイプ
- パラメータ名
- パラメータ正常値
- パラメータ操作値
- 検知理由

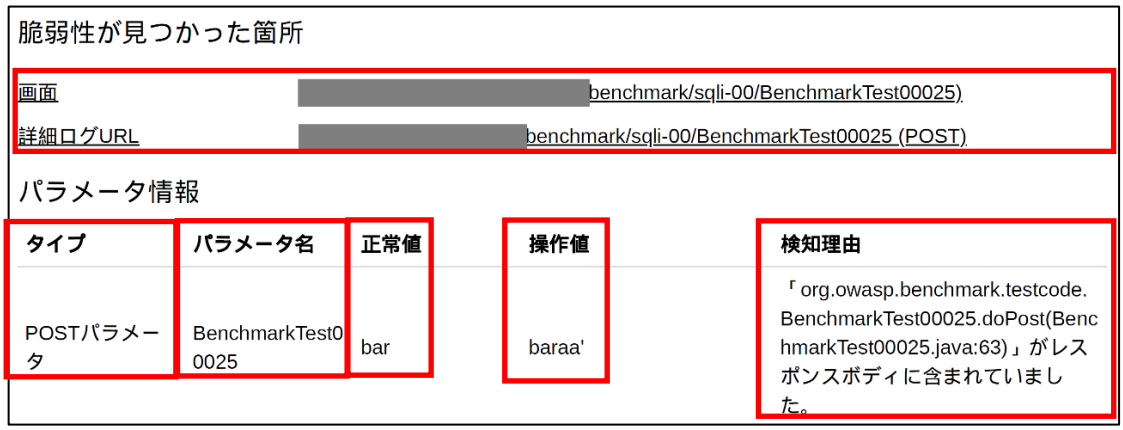


図 5-17 脆弱性が見つかった箇所

上記の内容は主に技術者向けであるが、同レポートには主に経営層向けとして以下の各種ガイドライン対応状況サマリー（図 5-18、図 5-19、図 5-20）やスキャンサマリー（図 5-21）が掲載されており、各種ガイドラインへの対応状況がわかりやすいこと、そして技術者と経営層にとっ

てそれぞれ知りたい情報がわかりやすく記載されていることを確認した。

- OWASP TOP10
- IPA「安全なウェブサイトの作り方」
- ASVS4.0

図 5-18 OWASP TOP10 対応状況サマリー（抜粋）

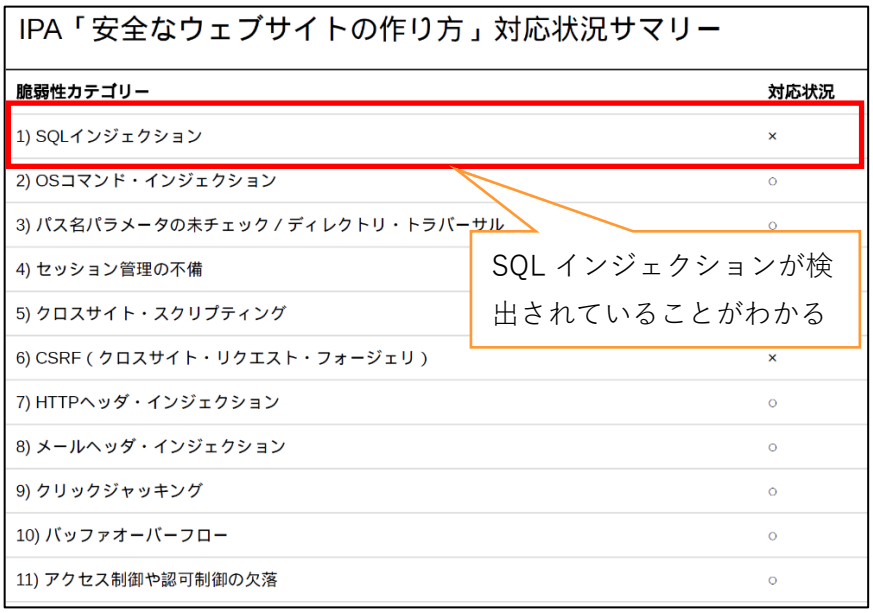


図 5-19 IPA「安全なウェブサイトの作り方」対応状況サマリー

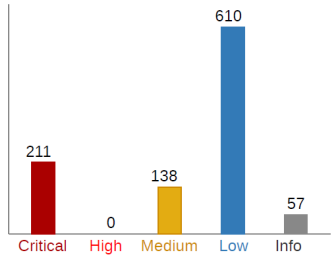
OWASP ASVS4.0 レベル1 対応状況サマリー

項番	内容	対応状況
2.1.1	ユーザが設定するパスワードは、最低12文字となっている。(C6)	×
2.1.2	64文字以上のパスワードが使用できる。(C6)	×
2.1.3	パスワードにスペースを含めることができ、切り捨てが行われない。任意で、連続した複数のスペースは1つにまとめてもよい。(C6)	×
2.1.4	パスワードにUnicode文字が使用できる。単一のUnicode符号点は文字と見なされるため、12文字の絵文字や64文字の漢字が有効に使用できる必要があります。	×
2.1.5	ユーザは自身のパスワードを変更できる。	-
2.1.6	パスワード変更機能には、ユーザの現在のパスワードと新しいパスワードが必要とされる。	○

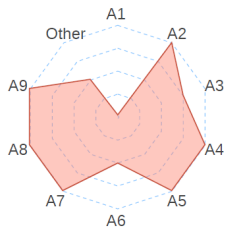
図 5-20 ASVS4.0 対応状況サマリー（抜粋）

スキャンサマリー

全体評価　Critical



深刻度ごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深刻度はCVSSv3 (https://www.ipa.go.jp/security/vuln/CVSSv3.html) に基づき以下の基準で設定しています。

深刻度	CVSSv3基本値	脆弱性に対して想定される脅威
Critical	9.0 ~ 10.0	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威
High	7.0 ~ 8.9	
Medium	4.0 ~ 6.9	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・その他、Critical/Highに該当するが再現性が低いもの
Low	0.1 ~ 3.9	・攻撃するために複雑な条件を必要とする脅威 ・その他、Mediumに該当するが再現性が低いもの
Info	0	

基本情報

サイトタイプ	PC向けサイト
トップURL	[redacted]
画面数	[redacted]
スキャン開始時刻	2022/02/14 16:59
スキャン終了時刻	2022/02/15 03:29
巡回ドメイン	なし

図 5-21 スキャンサマリー

1） 検証協力ユーザからの意見

レポートでは多くの診断結果が記載されているとの意見をいただいた。また、脆弱性が見つかった箇所の URL が記載されていることや、対策方法の参考情報への URL が記載されていること等でわかりやすいと感じているとの意見をいただいた。

検証実施者と同様の意見だったため、レポートは視覚的にわかりやすく配慮されていると考えられる。

また、より分かりやすいレポートの作成に向けた継続的改善に取り組むとの回答を製品ベンダよりいただいた。

5.3.2 検証項目 3-2 の検証結果

（1） 検証項目の内容

人間による操作時間を計測し、妥当な時間内に完了していること。

（2） 検証結果

実検証、検証協力ユーザに対するヒアリング及びデータや記録に基づく評価により、人間による操作時間を計測し、妥当な時間内に完了していることを確認した。

（3） 検証内容の詳細

本検証項目は実検証、検証協力ユーザに対するヒアリング及びデータや記録に基づく評価により実施した。

検証実施者が検証項目 2-1 で検証した 1 種類の診断開始から診断完了後のレポートダウンロードまでの人間による操作時間は約 10 分程度だったため、妥当な時間であると感じた。

製品ベンダからの参考情報として、診断開始から診断完了までの AeyeScan の処理時間については Web サイトの作りや画面数にも依存するため一律ではないものの、スキャン速度は 1 時間あたり 10 画面程度の処理時間であるとの情報を得た。

1） 検証協力ユーザからの意見

診断開始から診断完了後のレポートダウンロードまでの操作を実施していただき、操作時間は同様に約 10 分程度だったため、妥当な時間であるとの意見をいただいた。

検証実施者と同様の意見だったため、人間による操作は妥当な時間内に完了していると考えられる。

5.3.3 検証項目 3-3 の検証結果

(1) 検証項目の内容

CI ツール等と連携し、診断の自動化が可能であること。

(2) 検証結果

実検証及びデータや記録に基づく評価により、CI ツール等と連携し、診断の自動化が可能であることを確認した。

(3) 検証内容の詳細

本検証項目は実検証及びデータや記録に基づく評価により実施した。

AeyeScan は GUI から操作可能な機能を API として公開しているため、CI ツール等から API を実行することにより脆弱性診断の自動化が可能となっている。(図 5-22)

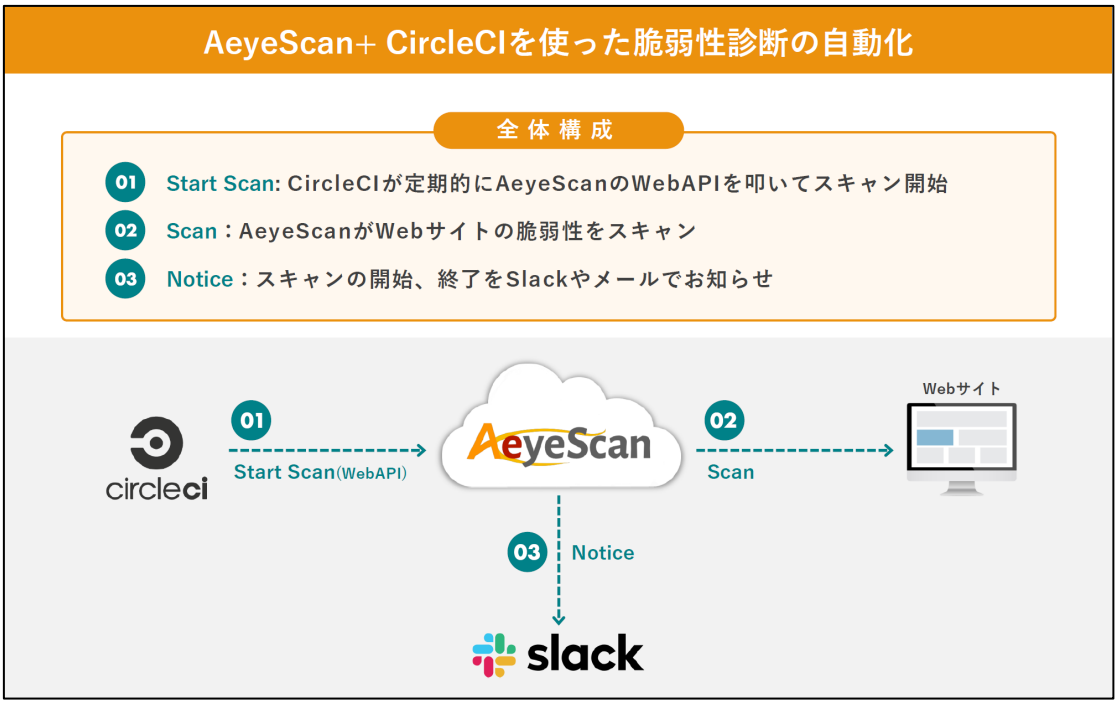


図 5-22 CI ツール連携イメージ

検証用 Web サイト②（日本語入力フォーム画面を含む自作の Web サイト）を用いた実検証では、CI ツールの代わりに AWS 上の OS コマンドから AeyeScan の診断用 API を実行することで、診断が開始されてレポートが作成されることを確認した。（図 5-23）

この結果、当該 API を CI ツール等から実行することで脆弱性診断を自動化できることを確認した。

図 5-23 API 実行結果イメージ

5.3.4 検証項目 3-4 の検証結果

（1） 検証項目の内容

運用操作性について検証協力ユーザの観点から良好であること。

（2） 検証結果

実検証及び検証協力ユーザに対するヒアリングに基づく評価により、運用操作性について検証協力ユーザの観点から良好であることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及び検証協力ユーザに対するヒアリングに基づく評価により実施した。

検証実施者が実検証として検証項目 1-3 や 2-1 等の操作を通じて運用操作性は良好だと感じた。

1） 検証協力ユーザからの意見

主に以下の点で運用操作性は良好だとの意見をいただいた。

- AeyeScan を利用する各部署の担当者ごとに権限管理ができること。
- 日中帯だけ診断を実施するような診断時間設定が可能であること。
- AeyeScan の IP アドレスが公開されていて固定なので、ファイアウォールでアクセス制限している Web サイトでも診断できること。

検証実施者と同様の意見だったため、運用操作性については良好であると考えられる。

5.4 「習得性」に関する検証結果

5.4.1 検証項目 4-1 の検証結果

（1） 検証項目の内容

初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していること。

（2） 検証結果

実検証及び検証協力ユーザに対するヒアリングに基づく評価により、初心者が操作を繰り返して習得する時間（回数）を計測し、妥当な時間（回数）内に完了していることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及び検証協力ユーザに対するヒアリングに基づく評価により実施した。

検証実施者が、まず脆弱性診断を実施する前に製品ベンダから提供されている公式マニュアルページを読むことである程度の基本操作を学習した。その後、検証項目 3-2 に対する操作について 2～3 回程度の繰り返し操作を行うことで脆弱性診断の基本操作は習得できたと感じた。

1） 検証協力ユーザからの意見

2～3 回程度の繰り返し操作を行うことで脆弱性診断の基本的な操作は習得できたとの意見だった。

検証実施者と同様の意見だったため、習得する時間（回数）については妥当であると考えられる。

5.4.2　検証項目 4-2 の検証結果

（1）　検証項目の内容

マニュアル、サポートデスクの提供により理解・習得が容易であること。

（2）　検証結果

実検証及び検証協力ユーザに対するヒアリングに基づく評価により、マニュアル、サポートデスクの提供により理解・習得が容易であることを確認した。

（3）　検証内容の詳細

本検証項目は実検証及び検証協力ユーザに対するヒアリングに基づく評価により実施した。

検証項目 4-1 のとおり、検証実施者が、まず脆弱性診断を実施する前に製品ベンダから提供されている公式マニュアルページを読むことで基本操作の理解は容易だと感じた。また、不明点についてはサポートデスクが提供されており、実際に問い合わせを行うことで回答を得ることができ、不明点の解消にもつながった。サポートデスクからの回答までの時間も良好であった。

1）検証協力ユーザからの意見

公式マニュアルページを確認することでおおむね自己解決できているので理解・習得は容易であるとの意見だった。

検証実施者と同様の意見だったため、マニュアル、サポートデスクの提供により理解・習得が容易であると考えられる。

5.4.3　検証項目 4-3 の検証結果

（1）　検証項目の内容

習得性について検証協力ユーザの観点から良好であること。

（2）　検証結果

実検証及び検証協力ユーザに対するヒアリングに基づく評価により、習得性について検証協力ユーザの観点から良好であることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及び検証協力ユーザに対するヒアリングに基づく評価により実施した。

検証項目 4-1 や 4-2 のとおり、検証実施者が習得性については良好であると感じた。

1） 検証協力ユーザからの意見

習得性については十分わかりやすいと感じているとの意見だった。

検証実施者と同様の意見だったため、習得性については良好であると考えられる。

5.5 「その他」に関する検証結果

5.5.1 検証項目 5-1 の検証結果

（1） 検証項目の内容

多要素認証によりユーザ認証ができること。

（2） 検証結果

実検証及びベンダヒアリングに基づく評価により、多要素認証によりユーザ認証ができることを確認した。

（3） 検証内容の詳細

本検証項目は実検証及びベンダヒアリングに基づく評価により実施した。

実検証にてアカウント管理画面で二要素認証が設定できることを確認した。

また参考情報として、ベンダヒアリングにて以下の回答を得た。

- 二要素認証で利用できる認証アプリケーションは「Google Authenticator」と「Microsoft Authenticator」。
- 二要素認証に加えて、アクセス元の IP アドレスを制限する機能がある。

これにより、アカウント管理画面に対するアクセス制御について適切であると考える。

5.5.2 検証項目 5-2 の検証結果

（1） 検証項目の内容

取得データの所在地（リージョン）が日本国内であること。

（2） 検証結果

ベンダヒアリングに基づく評価により、取得データの所在地（リージョン）が日本国内であることを確認した。

（3） 検証内容の詳細

本検証項目はベンダヒアリングに基づく評価により実施した。

ベンダヒアリングにて、AeyeScan が稼働しているサーバや取得データを保存しているサーバの所在地（リージョン）が日本国内であることを確認した

また参考情報として、AeyeScan のセキュリティに関する機能・設定として、以下の回答を得た。

- マルチテナント構成になっており、ユーザごとにデータベースを分けている。
- データの暗号化や適切なアクセス制御も実施している。

これにより、取得データの機密性について適切であると考える。

5.5.3 検証項目 5-3 の検証結果

（1） 検証項目の内容

プライバシーポリシー（個人情報保護方針）を明記していること。

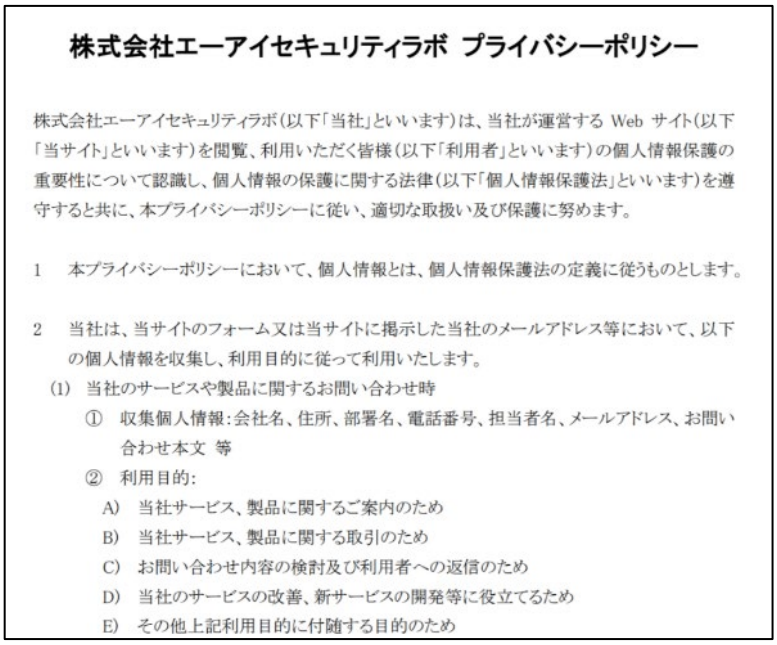
（2） 検証結果

データや記録に基づく評価により、プライバシーポリシー（個人情報保護方針）を明記していることを確認した。

（3） 検証内容の詳細

本検証項目はデータや記録に基づく評価により実施した。

製品ベンダから提供されたデータに基づいて、プライバシーポリシー（個人情報保護方針）を明記していることを確認した。（図 5-24）



株式会社エーアイセキュリティラボ プライバシーポリシー

株式会社エーアイセキュリティラボ(以下「当社」といいます)は、当社が運営する Web サイト(以下「当サイト」といいます)を閲覧、利用いただく皆様(以下「利用者」といいます)の個人情報保護の重要性について認識し、個人情報の保護に関する法律(以下「個人情報保護法」といいます)を遵守すると共に、本プライバシーポリシーに従い、適切な取扱い及び保護に努めます。

1　本プライバシーポリシーにおいて、個人情報とは、個人情報保護法の定義に従うものとします。

2　当社は、当サイトのフォーム又は当サイトに掲示した当社のメールアドレス等において、以下の個人情報を収集し、利用目的に従って利用いたします。

(1)　当社のサービスや製品に関するお問い合わせ時

①　収集個人情報:会社名、住所、部署名、電話番号、担当者名、メールアドレス、お問い合わせ本文 等

②　利用目的:

A)　当社サービス、製品に関するご案内のため

B)　当社サービス、製品に関する取引のため

C)　お問い合わせ内容の検討及び利用者への返信のため

D)　当社のサービスの改善、新サービスの開発等に役立てるため

E)　その他上記利用目的に付随する目的のため

図 5-24 プライバシーポリシー(抜粋)

6. まとめ

AeyeScan は、AI や RPA を活用した SaaS 型 Web アプリケーション脆弱性診断ツールである。製品ベンダは、脆弱性診断の内製化の課題であった「自社で出来るか不安」という点に対して、診断の操作が簡単であることや、業界標準の脆弱性診断項目と評価基準によるわかりやすいレポート出力により、Web セキュリティの知識や Web アプリケーションの開発経験がなくても脆弱性診断が内製化できる点が特徴であるとしている。加えて、AI や RPA による自動操作によって最短 10 分で診断を開始することができる点も特徴として挙げられる。

今回の検証は、前述の検証環境、検証条件、方法の範囲で、AeyeScan の 4 つのセキュリティに関する優れたユーザビリティとされている事項に対して、「機能充足性」、「機能正確性」、「効率性・運用操作性」、「習得性」、「その他」の観点から検証を実施し確認した。その結果、これまで脆弱性診断の内製化に対する課題が解決できずに導入に踏み切れなかったユーザ企業への導入が促進されるものと考えられる。