2021年度に実施した有効性検証の結果概要

2021年度 情報処理推進機構 委託事業
「サイバーセキュリティ検証基盤の運用」事業の結果より

三菱総合研究所

デジタル・イノベーション本部

サイバーセキュリティ戦略グループ　篠原巧

2022年12月20日

目次

本講演では、2021年度に実施した検証基盤の運用について、製品公募・製品選定・有効性検証の結果概要をご紹介する。

- 2021年度事業では、2020年度事業で構築した検証基盤の仕組みに基づき、製品の公募・選定・有効性検証を行った。

検証基盤の仕組み・プロセス	実施概要
1. 重要分野選定	• 重要分野マップについて、セキュリティ脅威の状況、ユーザ企業の状況、セキュリティ技術の変化等を踏まえて必要な見直しを行う。
2. 製品公募	• 製品公募に際しての公募要領・応募用紙を作成し、公募を行う。 • 幅広い製品・ベンダーに応募頂くために、公募の周知を行う。
3. 製品選定	• 応募された製品・ベンダーの中から、有効性検証の対象となる製品を選定する。 • 製品選定を効率化するために、事前に審査基準を定める。
4. 有効性検証	• 選定された製品の検証を実施する。そのために、製品に対する検証項目、検証環境、検証方法を決定する。 • 製品の特徴的な機能や強みを示す差別化ポイントとされる事項を調査する。
5. 検証結果公表	• 検証結果を文書化し、公表する。 • 検証結果に基づき、当該製品・ベンダーのプロモーションを行う。

2021年度の実施結果について、本日ご紹介

製品公募・対象製品選定の結果

- 対象製品公募・選定の全体プロセス
- 製品公募における募集要件
- 対象製品の審査・選定のプロセス
- 対象製品の審査の観点
- 選定された製品の概要

2021年度の有効性検証では、種別・種別Bの2つの製品種別を募集し、公募の結果、計11製品の応募が寄せられた。

- 2021年度の有効性検証では、種別A・種別Bの2つの製品種別を募集した。
- 種別Aとして、国内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を募集した。
- 種別Bとして、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を募集した。
- 各種別について、2週間程度の製品公募期間後、応募された製品に対する審査・選定を行った。
- 製品公募の結果、11製品の応募が寄せられた

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
- 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

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
- 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
- 応募にあたって、製品が想定するユーザであり、本事業の検証に協力するユーザを応募ベンダが用意することを求めた

プロセス	実施時期	実施概要	主な実施主体
製品公募	2022年1月11日（月）～1月21日（金）	• 有効性検証対象製品の公募、応募の受付を行った。	検証基盤運用主体
製品審査・選定	1月24日（月）～1月25日（火）	• 応募された製品に対する一次審査を行った。	検証基盤運用主体
	1月26日（水）～1月31日（月）	• 一次審査を通過した製品に対する二次審査を実施した。	有識者
	1月27日（木）	• 一次審査を通過した応募ベンダーに対するヒアリングを実施した。	有識者
	2月1日（火）	• 二次審査結果に対する有識者の審議を行い、検証対象製品を決定した。	有識者

応募要件では、客観的な審査と効率的な検証のトレードオフを考慮するために、必須要件と追加要件によって構成した。

- 応募要件は、必須要件と追加要件によって構成した。
- 必須要件では、本事業の目的に資する製品を客観的に判断することを目的に、応募ベンダーが法人格を有していることや有識者検討会において選定された重要分野に該当すること等を求めた。
- 追加要件では、効率的な検証を行うことを目的として、対象とする製品の新規性の高いセキュリティ機能や優れたユーザビリティ等について、記載を求めた。

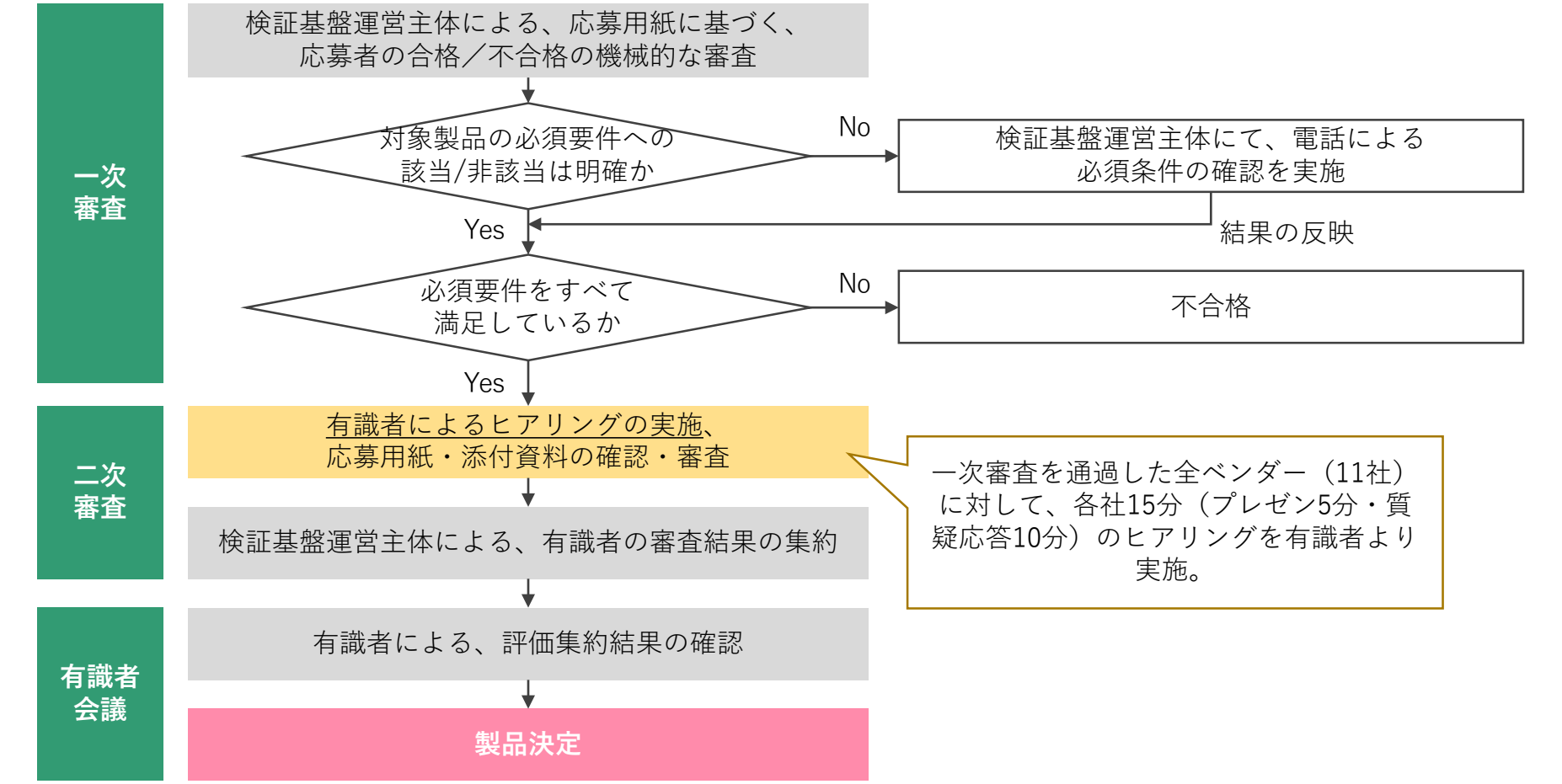
応募者に課した応募要件（必須要件＋追加要件）

区分	要件項目
必須要件	• 応募ベンダーは、法人格を有していること。 • 応募ベンダーは、日本国内に開発拠点を有していること。さらに、応募製品はこの拠点で製品開発されたものであること。 • 対象とする製品は、新規に市販を開始してから5年以内であること。 • 応募製品が、有識者検討会において選定した重要分野に該当すること。 • 検証の実施に当たって、検証項目、検証環境、公表内容等について検証者と協議・調整すること。 • 検証の実施に当たって、製品やその稼働に必要な付帯物、検証用データ、利用環境等を無償で貸与すること。 • 検証を効率的に実施するために、検証者及び検証基盤運用主体との連絡体制を構築すること。 • 【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。 等
追加要件	• 【種別Aの製品のみ】新規性の高いセキュリティ機能を有すること。 • 【種別Bの製品のみ】想定ユーザ・想定使用環境・想定業務タスクに対して、優れたユーザビリティを有すること。 • 海外に本社機能を有する親会社が存在するかを記入すること。存在する場合、親会社の国籍や社名を記入すること。 • 想定される検証方法を第三者が理解できるように記載すること。 • 限られた期間内で検証を完了するための工夫を記載すること。 等

応募が寄せられた製品について、一次審査・二次審査を通じて製品選定を実施した。
二次審査では、有識者によるベンダーヒアリングも実施した。

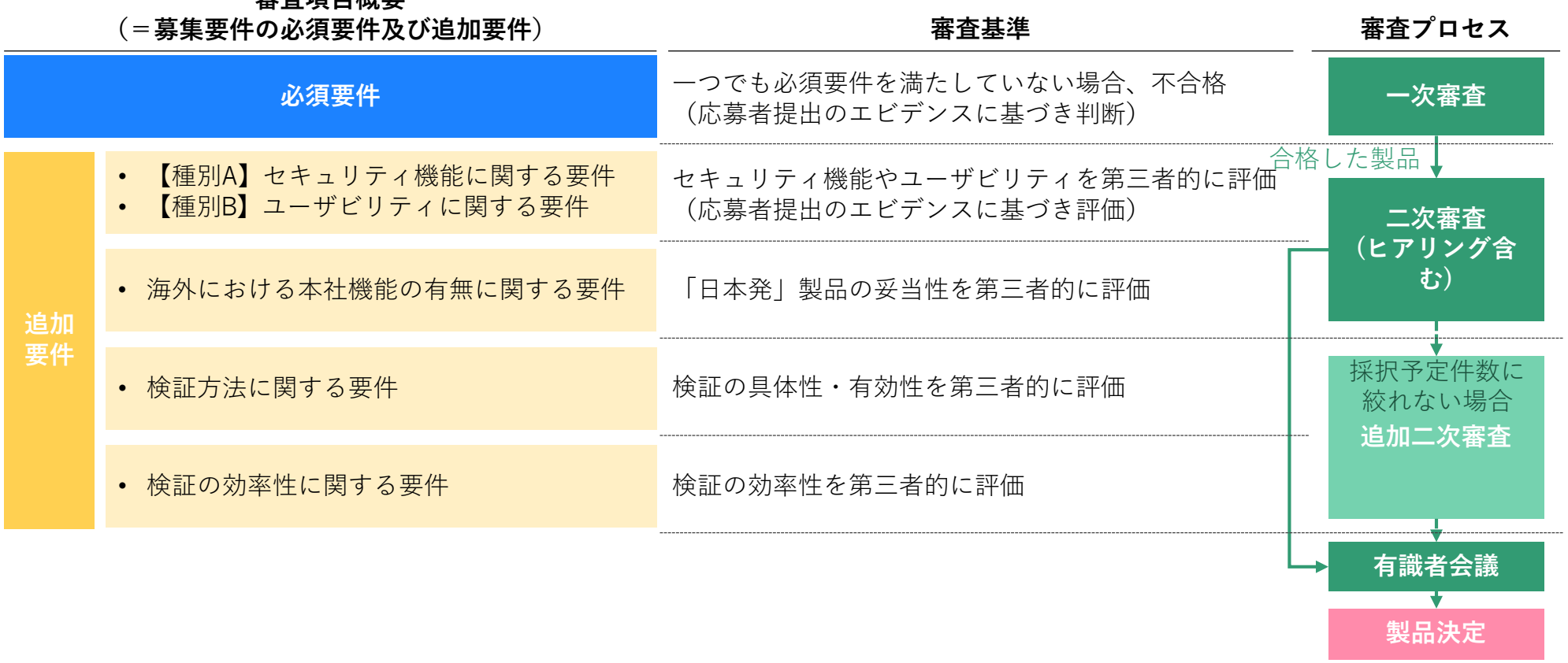
- 一次審査では、応募要件のうち必須要件を満足しているかを機械的に確認・審査した。
- 二次審査では、有識者による審査を行った。二次審査の一環として、一次審査を通過したベンダーに対するヒアリングも実施した。

対象製品の審査・選定のプロセス



一次審査では、応募要件のうち必須要件に基づき審査を行った。
二次審査では、応募要件のうち追加要件に関する審査を有識者より実施した。

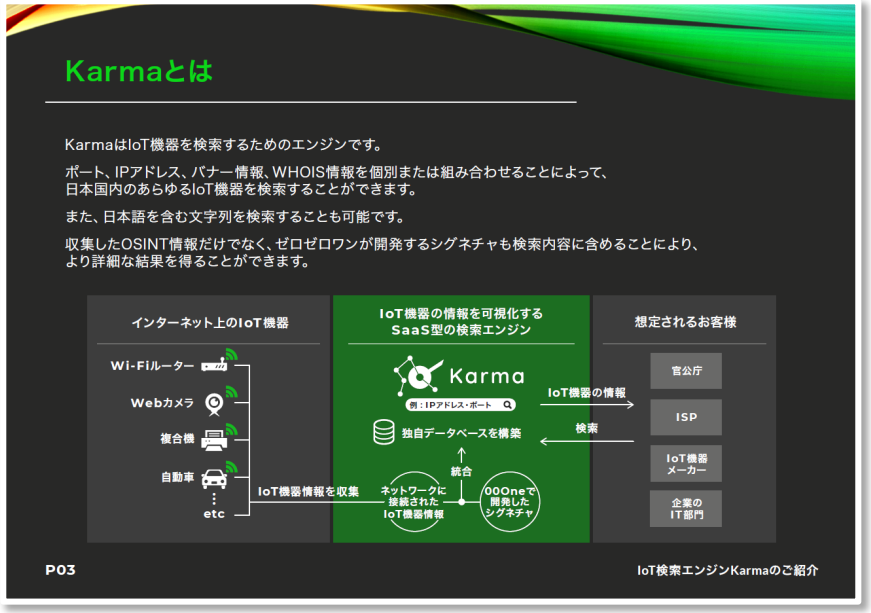
- 応募要件のうち、必須要件はすべての応募者が満たす必要のある審査基準として扱い、一つでも必須要件を満たしていないと評価される応募者は不合格とした。（一次審査）
- 二次審査では、応募者のエビデンスやヒアリング結果に基づき、追加要件に関する審査を有識者が実施した。審査後、各有識者において検証対象製品の投票をいただいた。（種別A・Bで各1製品）
- 最終的に有識者の選定結果を集約し、得票数が高い製品を選定した。



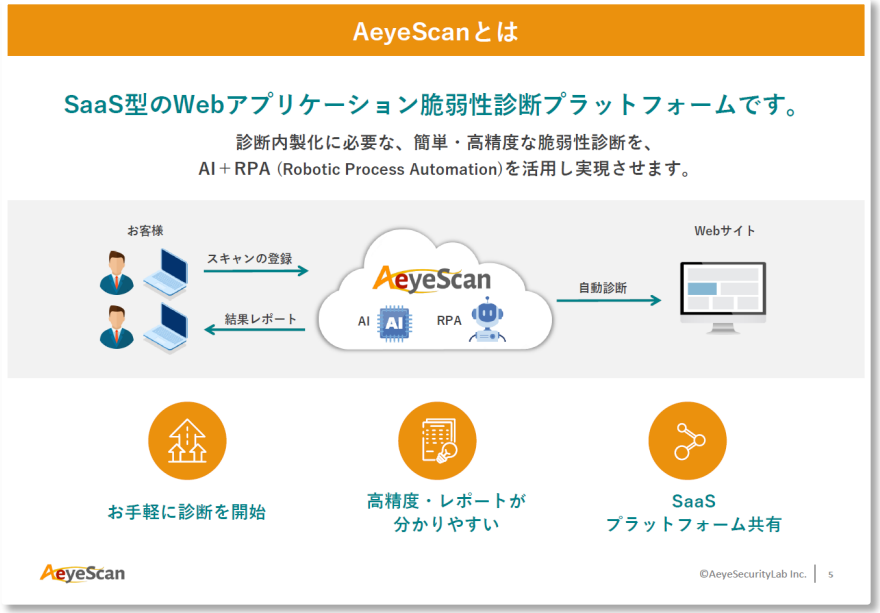
製品審査の結果、2021年度の有効性検証対象製品として、種別AはKarma、種別BはAeyeScanがそれぞれ選定された。

- 二次審査の結果、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、種別Bにおいて得票数が高い製品は株式会社エーアイセキュリティラボのAeyeScanであった。
- これらの製品を有効性検証の対象とすることを有識者会議に諮り、対象製品として決定した。
- 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、IPアドレス情報等の複数の情報を用いて、日本国内のIoT機器を検索することができる。
- 株式会社エーアイセキュリティラボのAeyeScanは、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り、AI・RPA技術を活用した簡易かつ高精度な脆弱性診断が可能である。

株式会社ゼロゼロワン：Karmaの概要【種別A】



株式会社エーアイセキュリティラボ：AeyeScan【種別B】



出所）株式会社ゼロゼロワン、株式会社エーアイセキュリティラボ

有効性検証の結果

- 有効性検証の全体プロセス
- 検証対象製品における主張ポイント
- 検証項目・検証方法
- 検証環境
- 検証結果

選定された2製品それぞれについて検証項目・検証方法を策定するとともに、検証環境を構築した上で有効性検証を行った。

- 選定された2製品に対して、以下のプロセスで検証を実施した。
- 検証環境構築等の検証準備と並行して各製品に適用する検証項目・検証方法の策定を行った。
- 有識者の確認を経て確定した検証項目・検証方法に基づき、各製品の検証を実施した。

プロセス	実施時期	実施項目概要	主な実施主体
検証準備	2022年2月1日（火） ～2月7日（月）	• 応募ベンダーと連携し、検証環境を構築した。	応募ベンダー・検証者・ 検証基盤運用主体
検証項目・検証方法案の策定・確定	2月1日（火）～ 2月10日（木）	• 応募ベンダーや検証協力ユーザと協議し、製品を効果的に検証できる検証項目・検証方法を策定した。 • 策定した検証項目・検証方法を有識者に確認いただき、有識者の意見を踏まえて確定した。	応募ベンダー・ 検証協力ユーザ・ 検証者・有識者
検証実施	2月8日（火）～ 3月3日（木）	• 確定した検証項目・検証方法に基づき、製品に対する有効性検証を実施した。	検証者
検証結果の中間報告	2月16日（火）	• 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・修正した。	有識者
検証結果の最終報告	3月3日（木）	• 有識者により検証結果の確認を行った。	有識者

有効性検証で確認すべきKarmaの新規性の高いセキュリティに関する機能、AeyeScanのセキュリティ機能に関するユーザビリティ項目をそれぞれ設定した。

- 種別Aの有効性検証の目的は、製品ベンダーが主張する新規性の高いセキュリティに関する機能が、ベンダーの主張通りであることを検証・確認することである。
- 同様に、種別Bの有効性検証の目的は、製品ベンダーが主張するセキュリティ機能に関するユーザビリティ項目が、ベンダーの主張通りであることを検証・確認することである。
- このために、検証で確認すべきKarmaにおける新規性の高いセキュリティに関する機能と、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を、応募ベンダーと協議して設定した。

【種別A】 Karmaにおいて新規性の高いセキュリティに関する機能	【種別B】 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
① IoT機器の正しい情報を検出できること	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 セキュリティリスクのあるIoT機器を検出できること	② 機能正確性：画面クローリング性能（範囲、深度）
③ 日本語検索が可能であること	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

ベンダーが主張する新規性の高いセキュリティに関する機能について、当該機能の検証に資する検証項目・検証方法を策定した。

- 検証者及び応募ベンダーと協議し、Karmaの機能や特性、応募ベンダーが主張する新規性の高いセキュリティに関する機能を踏まえ、検証項目を策定した。
- 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。

Karmaにおける主要な検証項目と、対応する新規性の高いセキュリティに関する機能・検証方法（抜粋版）

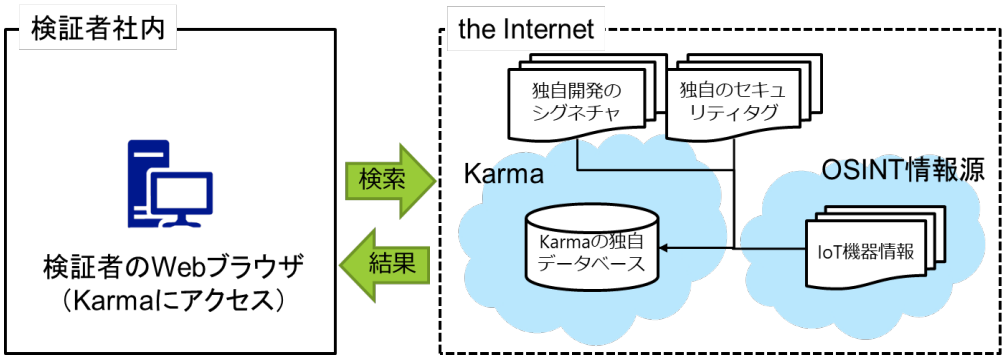
検証項目（抜粋）		新規性の高いセキュリティに関する機能			検証方法		
区分	検証項目	① IoT機器の正しい情報を検出できること	② セキュリティリスクのあるIoT機器を検出できること	③ 日本語検索が可能であること	検証環境での実検証	データや記録に基づく評価	ベンダヒアリングに基づく評価
リスクの検出	IoT機器の正しい情報を検出できること	✓			✓	✓	
	セキュリティリスクのあるIoT機器を検出できること		✓		✓	✓	
	日本語の文字列を含んだ検索ができること			✓	✓		
	インターネット経由でIoT機器の検出ができること	✓	✓	✓	✓		
	条件を絞り込んだ検索ができること	✓	✓	✓	✓		

※ 本資料では主要な検証項目のみ抜粋している。

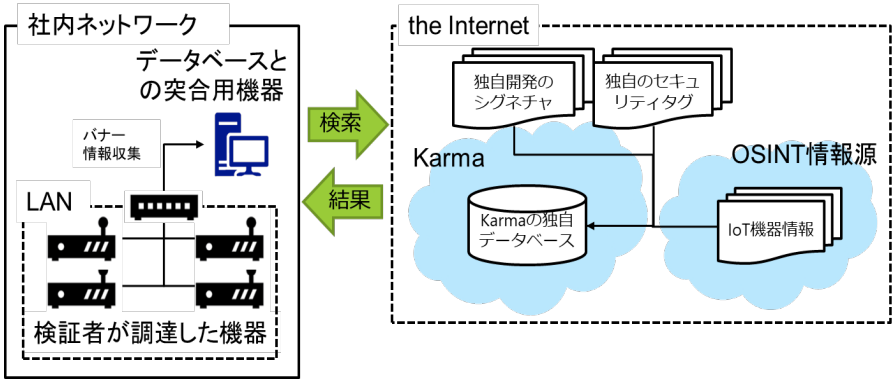
ベンダーが主張する新規性の高いセキュリティに関する機能を検証するために、Karmaの検証環境として、2つの検証環境を構築した。

- IoT機器の正しい情報がKarmaで検出できるかを確認するために、Karmaの検証環境として、2つの検証環境を構築した。
  - (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
  - (2)検証者が調達したIoT機器を検索するための検証環境
- また、セキュリティリスクのあるIoT機器を検出できるかを確認するために、本検証では、2～3年前に販売されたファームウェアアップデートが実施されていない可能性が高い家庭用ルータを複数調達した。
- なお、検証の公正性を担保するために、株式会社ゼロゼロワンに対しては、調達した製品名は事前に一切告知せず検証を実施した。

Karmaの検証環境(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の検証環境(2)
検証者が調達したIoT機器を検索するための検証環境



有効性検証によって、ベンダーがKarma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つの事項を確認できた。

- Karmaに対する有効性検証によって、応募ベンダー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つの事項を確認できた。
  - ① IoT機器の正しい情報を検出できること
  - ② セキュリティリスクのあるIoT機器を検出できること
  - ③ 日本語検索が可能であること

Karmaにおける主要な検証項目に対する検証結果

検証項目（抜粋）		検証結果
区分	検証項目	
リスクの検出	IoT機器の正しい情報を検出できること	• インターネット上に公開されているIoT機器を検索することで、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。 • 検証者が調達したIoT機器に対する確認では、実際のIoT機器とKarmaの検索結果を照合するとで、検索結果の正確性を確認した。
	セキュリティリスクのあるIoT機器を検出できること	• インターネット上に公開されているIoT機器を検索することで、セキュリティリスクが存在する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。 • 検証者が調達したIoT機器に対する確認では、実際のIoT機器とKarmaの検索結果を照合するとで、検索結果の正確性を確認した。
	日本語の文字列を含んだ検索ができること	• Karmaで日本語の文字列を含んだ検索式で検索が可能であり、その検索結果の内容が正しいことを確認した。
	インターネット経由でIoT機器の検出ができること	• 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。
	条件を絞り込んだ検索ができること	• IoT機器メーカーを想定したユースケースとして、特定の期間における自社製品の利用状況について、条件を絞り込んだ検索が可能であることを確認した。 • ISP事業者を想定したユースケースとして、特定の期間における管理グローバルIPの利用状況について、条件を絞り込んだ検索が可能であることを確認した。

※ 本資料では主要な検証項目・検証結果のみ抜粋している。

ベンダーが主張するセキュリティ機能に関するユーザビリティ項目について、当該機能の検証に資する検証項目・検証方法を策定した。

- 検証者及び応募ベンダーと協議し、AeyeScanの機能や特性、応募ベンダーが主張するセキュリティ機能に関するユーザビリティ項目を踏まえ、検証項目を策定した。
- 種別Bの有効性検証においては「検証協力ユーザに対するヒアリングに基づく評価」も実施した。

AeyeScanにおける主要な検証項目と、対応するセキュリティ機能に関するユーザビリティ項目・検証方法（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				検証方法			
区分	検証項目	① 機能充充足性	② 機能正正確性	③ 効率性・運用操作性	④ 習得性性	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
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	✓				✓		✓	
自動分析	AIによるフォーム自動入力値が正しいこと	✓				✓			
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		✓			✓		✓	
	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		✓			✓			
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	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				✓	✓	✓		

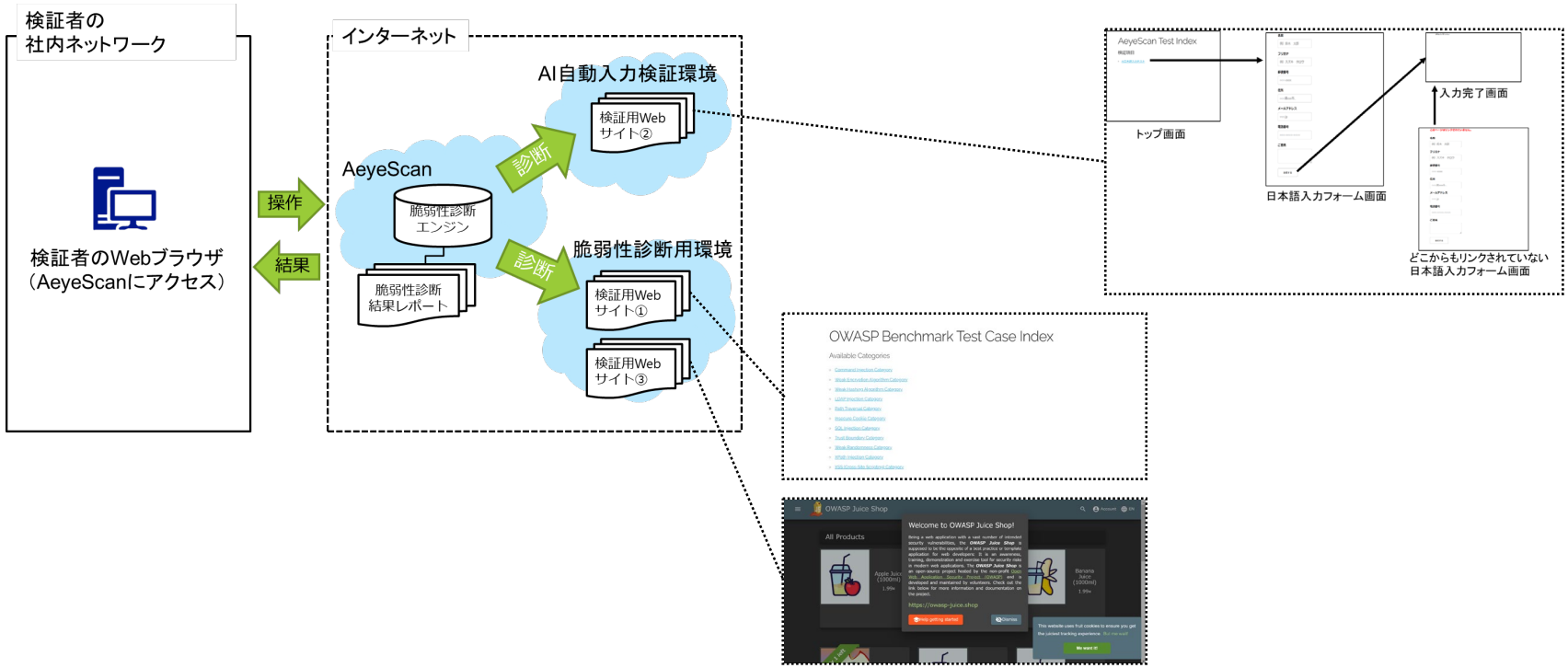
※ 本資料では主要な検証項目のみ抜粋している。

ベンダーが主張するセキュリティ機能に関するユーザビリティ項目を検証するために、3つの検証用WebサイトをAWS上に構築した。

- AeyeScanによる脆弱性検知の正確性やAIによる自動分析の確認のために、本検証では以下の3つの検証用WebサイトをAWS上に構築した。
  - (1) OWASP Benchmarkを稼働させたWebサイト【脆弱性検知検証用】
  - (2) 日本語入力フォーム画面を含む自作のWebサイト【AI自動入力検証用】
  - (3) OWASP Juice Shopを稼働させたWebサイト【脆弱性検知検証用】

※ OWASP BenchmarkやOWASP Juice Shopとは、多くの脆弱性を意図的に埋め込んだテスト用のWebアプリケーション。

AeyeScanの検証環境



有効性検証によって、ベンダーがAeyeScan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としている4つの事項を確認できた。

- AeyeScanに対する有効性検証によって、応募ベンダー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つの事項を確認できた。
  - 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

AeyeScanにおける主要な検証項目に対する検証結果

検証項目（抜粋）		検証結果
区分	検証項目	
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	• 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。
自動分析	AIによるフォーム自動入力値が正しいこと	• 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。
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	• 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。
	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	• 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。
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	• 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。
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	• 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、妥当な時間内に習得が完了していることを確認した。

※ 本資料では主要な検証項目・検証結果のみ抜粋している。

有効性検証の結果、ベンダーが主張するKarmaにおける新規性の高い機能、AeyeScanにおけるユーザビリティ項目をそれぞれ確認できた。

2021年度事業のまとめ

- 種別A・種別Bの2つの製品種別を対象に公募を行い、計11製品の応募が寄せられた。
- 応募のあった製品に対する審査・選定を行った。
- 審査・選定の結果、種別AとしてKarma、種別BとしてAeyeScanを選定し、有効性検証を実施した。
- 種別AのKarmaについて、応募ベンダーが新規性の高いセキュリティに関する機能とする「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」の3つの事項について、有効性検証を通じて確認した。
- 種別BのAeyeScanについて、応募ベンダーが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「機能充足性」、「機能正確性」、「効率性」、「習得性」の4つの事項、有効性検証を通じて確認した。

今後の方向性

- より多くの国内セキュリティ製品を対象とした市場参入支援
- より効果的な第三者評価の仕組み構築
- 市場環境を考慮した検証項目・検証方法のアップデート

未来を問い続け、変革を先駆ける

MRI 三菱総合研究所