2020年度に実施した検証基盤構築及び運用の結果概要

2020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構築・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

2021/06/29

目次

検証基盤の仕組みのうち、製品公募・製品選定・有効性検証の仕組み構築結果、及び構築した仕組みに基づく運用結果について、本日ご紹介する。

- 2020年度事業では、セキュリティ製品の有効性を検証する検証基盤の構築を実施した。
- また、構築した検証基盤に基づき、公募・選定・有効性検証を行い、検証基盤の実効性や今後の方向性を整理した。

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。

各仕組みの構築結果、及び構築した仕組みに基づく運用結果について本日ご紹介

製品公募の仕組み

- 対象製品公募の仕組み・プロセス
- 製品及びそのベンダーに課した応募要件

5つの要素で構成される製品公募の仕組みを構築した。構築した仕組みに基づき、応募要件の整理や関連資料の作成等を行い、対象製品の公募を行った。

- 製品公募の仕組みは5つの要素によって構成され、各ステップに従って製品公募を実施した。（製品公募期間：2020年12月2日～2020年12月10日）
- 応募用紙では、応募要件に満足していることを示す記載を求めるとともに、要件を満たしていることを支持するエビデンスの提示を求めた。

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

応募要件は、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。

- 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、「日本発」製品であることや、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、対象とする製品の差別化ポイントと考えられる事項等について、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。 等
追加要件	• 対象とする製品の差別化ポイント（機能、性能、定量的データ、評価・レビュー結果、受賞実績 等）を第三者が理解できるように記載すること。 • 応募製品が、有識者会議にて選定したキーワードに関連する製品であること。 • 海外に本社機能を有する親会社が存在するかを記入すること。存在する場合、親会社の国籍や社名を記入すること。 • 検証の実施に当たって、製品性能、運用容易性、導入容易性等を検証する方法を第三者が理解できるように記載すること。 等

製品選定の仕組み

- 製品選定の仕組み・プロセス
- 製品審査概要
- 製品選定結果・検証対象製品概要

3つの要素で構成される製品選定の仕組みを構築した。構築した仕組みに基づき、審査項目の策定や製品の審査等を行い、検証対象となる製品の選定を行った。

- 製品選定の仕組みは3つの要素によって構成され、各ステップに従って製品選定を実施した。（製品選定期間：2020年12月11日～2020年12月18日）
- 製品選定時に用いる審査項目は、応募要件に基づき策定した。
- 製品の一次審査では、応募要件のうち必須要件を満足しているかを確認・審査した。
- 製品の二次審査では、一次審査を通過した製品・ベンダーが優れた差別化ポイントを有しているか有識者に審査いただき、その審査結果を踏まえて検証対象となる2製品を選定した。

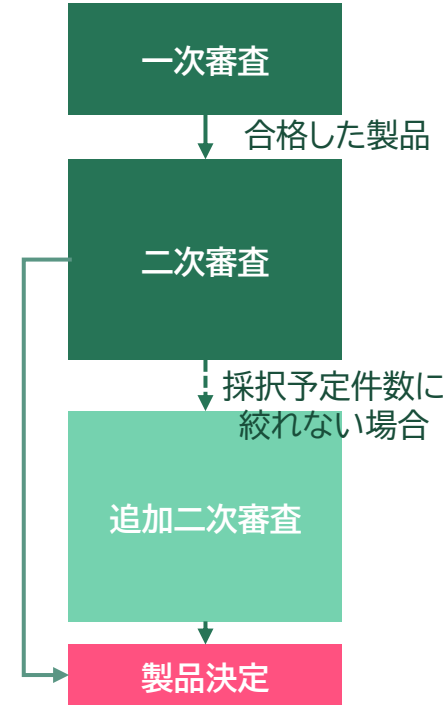
構成要素	具体的な実施事項	主な実施主体
① 製品審査項目・基準の策定	• 製品選定時に用いる**審査の項目及び基準を、応募要件に基づき策定**する。	検証基盤運用主体
② 製品の一次審査	• 製品審査基準に基づき、応募された製品・ベンダーが**必須要件に満足しているかを、エビデンスに基づき確認**する。 • 必須要件を満足しない応募製品・ベンダーについては、一次審査にて不合格とする。 • ある応募ベンダーの必須要件への該当に疑念が生じた際に、当該ベンダーに対して電話による必須条件の確認（ヒアリング）を実施する。	
③ 製品の二次審査	• 製品審査基準に基づき、応募された製品・ベンダーが**優れた差別化ポイントを有しているかを、エビデンスに基づき確認**する。 • 優れた差別化ポイントを有している製品・ベンダーのうち、採択予定の製品件数（2件）までの上位製品を検証対象として選定する。	有識者

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確認・審査した。
二次審査では、一次審査を通過した製品の差別化ポイント等を確認・審査した。

- 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、一次審査に合格した製品の差別化ポイントを、応募者エビデンスに基づき判断した。
- 二次審査では、有識者により審査項目の合否をそれぞれ審査(点数付け)し、評価合計点に基づき、各有識者にて最大2製品を選定いただいた。
- 最終的に有識者の選定結果を集約し、得票数が高い2製品を選定した。

審査項目概要 (＝応募要件の必須要件及び追加要件)		審査基準
必須要件		一つでも必須要件を満たしていない場合、不合格 (応募者提出のエビデンスに基づき判断)
追加要件	• 差別化ポイントに関する要件 • キーワードに関連する要件	差別化ポイントを第三者的に評価 (応募者提出のエビデンスに基づき評価)
追加要件	• 海外における本社機能の有無に関する要件	「日本発」製品の妥当性を第三者的に評価
追加要件	• 検証方法に関する要件	検証の具体性・有効性を第三者的に評価
追加要件	• 検証の効率性に関する要件	検証の効率性を第三者的に評価

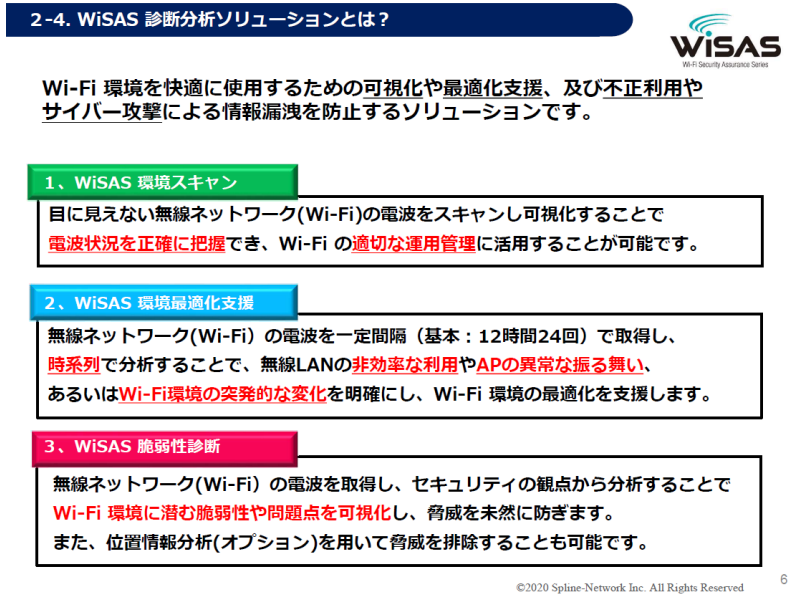
審査プロセス



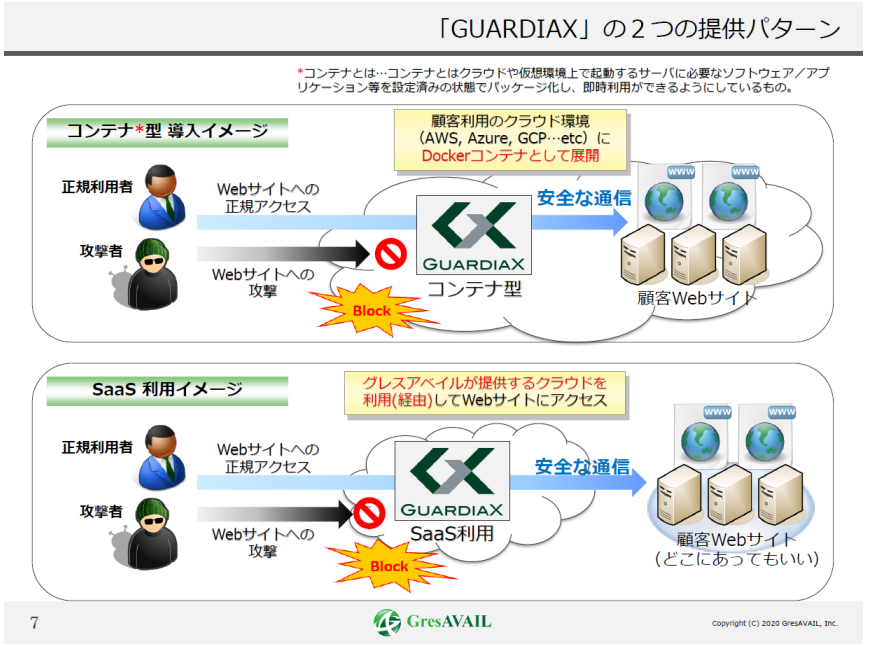
有識者による二次審査の結果を集約し、得票数が高い2製品であったWiSAS及びGUARDIAXを、今年度の有効性検証の対象として決定した。

- 有識者の選定結果を集約し、得票数が高い2製品はWiSAS及びGUARDIAX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。
- 株式会社スプライン・ネットワークの製品WiSAS（Wi-Fi Security Assurance Series）は、Wi-Fiセキュリティに特化したソリューションであり、Wi-Fiに関する様々な脅威を検知・監視することができる。
- 株式会社グレスアベイルの製品GUARDIAXはSaaS型／コンテナ型のWAFである。（今回の検証では、SaaS型を対象とした。）

WiSASソリューションの概要



GUARDIAXソリューションの概要



出所）株式会社スプライン・ネットワーク、株式会社グレスアベイル

有効性検証の仕組み

- 有効性検証の仕組み・プロセス
- 検証対象製品の差別化ポイントとされる事項
- 検証項目と検証方法の概要
- 検証対象製品における検証項目と検証方法
- 検証環境
- 検証結果

4つの要素で構成される有効性検証の仕組みを構築した。構築した仕組みに基づき、検証項目・検証方法の策定等を行い、実際の有効性検証を行った。

- 有効性検証の仕組みは4つの要素によって構成され、各ステップに従って有効性検証を実施した。（有効性検証期間：2021年1月5日～2021年2月26日）
- 有効性検証の目的は、選定された製品の差別化ポイントとされる事項を検証することであり、この事項を効果的に検証できる検証項目及び検証方法を策定した。
- 有効性検証は、策定した検証項目・検証方法に基づき、検証環境での実検証を中心とした検証を実施した。

構成要素	具体的な実施事項	主な実施主体
① 検証項目の策定	• 対象製品の差別化ポイントとされる事項を踏まえて、**有効性検証の検証項目を策定**する。	検証基盤運用主体
② 検証方法の策定	• 検証項目を**検証するための具体的な方法を策定**する。	検証基盤運用主体／検証者
③ 有効性検証の実施	• 検証計画を策定する。 • 検証に当たって必要となる検証環境を準備・構築する。 • 選定した検証製品に対して、**策定した検証項目・検証方法に基づき検証を実施**する。	検証者
④ 検証結果レポートの作成	• 検証結果を踏まえて、**検証結果レポートを作成**する。	検証基盤運用主体／検証者

（検証項目・検証方法及び検証途中結果に関しては、有識者に内容を確認いただいた。）

各製品ベンダーに対するヒアリングを通じて、それぞれの製品における差別化ポイントとされる事項を4点抽出した。

WiSASの差別化ポイントとされる事項

不正なWi-Fi APを検知、遮断できること

なりすましWi-Fi AP（SSIDを偽装）、非認可で持ち込まれているWi-Fi AP、非認可でテザリングに使用されているスマートフォンを検知、通知、遮断し、その位置を二次元平面で特定できること。

不正な端末の接続を検知、遮断できること

設置されている正規Wi-Fi APに非認可で接続しようとする端末を検知、通知、遮断し、その位置を二次元平面で特定できること。

Wi-Fi Directへの不正な端末の接続を検知、遮断できること

複合機やプリンター、プロジェクター、スキャナー等に装備されている Wi-Fi Direct機能に接続しようとする不正な端末を、検知、通知、遮断、そして、そのWi-Fi Direct機能が搭載されている機器の位置を二次元平面で特定できること。

Wi-Fi環境へのDoS攻撃の有無を確認できること

Wi-Fi環境を調査し、DoS攻撃の有無を確認できること。

GUARDIAXの差別化ポイントとされる事項

強固な防御ルールであること

Webアプリケーションの脆弱性を利用した攻撃に対する防御ルールが強固であること。

偽陽性が少ないこと

偽陽性（正常なアクセスを誤って防御してしまう）が少ないため、短期間（最短1日）での導入や利便性の高い運用が可能であること。

攻撃状況が判るダッシュボードであること

WAFのダッシュボードにより攻撃（不正アクセス）の状況が判ること。

防御ルールをWebサイト単位でチューニングできること

Webサイト毎にチューニングした防御ルールを設定できること。

選定された製品の差別化ポイントとされる事項を効果的に検証できる検証項目及び検証方法を、製品ごとに策定した。

- 検証基盤で扱う重要分野に共通して適用される、3つの検証項目の大分類「製品機能・性能」、「運用性」、「導入容易性」を設定し、それぞれの大分類の下に各製品の個別の検証項目を策定した。
- それぞれの検証項目について、「検証環境での実検証」、「データや記録に基づく評価」、「ベンダーヒアリングに基づく評価」のいずれかの検証方法で検証を実施することとした。
- 可能な限り「検証環境での実検証」による検証とし、一部の客観的・定量的な評価が可能な項目については、「データや記録に基づく評価」を実施した。

検証項目		検証方法	
大分類	検証項目例	検証方法	優先度
製品機能・性能	• 検知できる脅威や不正通信の種類に関する検証項目 • 脅威や不正通信への対応管理機能に関する検証項目　等	検証環境での実検証	高
運用性	• 自動監視・自動検知に関する検証項目 • ダッシュボード等における脅威の検知結果・分析結果の整理に関する検証項目 等	データや記録に基づく評価	低
導入容易性	• 導入できる環境に関する検証項目 • 設置の際に生じるシステム停止時間に関する検証項目　等	ベンダーヒアリングに基づく評価	例外的に実施

スプライン・ネットワーク社と協議の上、WiSASの差別化ポイントとされる事項を検証する検証項目及び検証方法を策定した。

- WiSASに関して23の検証項目を策定し、策定した検証項目に基づき検証を実施した。

WiSASにおける主要な検証項目と、対応する差別化ポイントとされる事項・検証方法（抜粋版）

検証項目		差別化ポイントとされる事項				検証方法		
大分類	検証項目	不正なWi-Fi APを検知、遮断できること	不正な端末の接続を検知、遮断できること	Wi-Fi Directへの不正な端末の接続を検知、遮断できること	Wi-Fi環境へのDoS攻撃の有無を確認できること	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価
製品機能・性能	認可されていないWi-Fi APをフロア内に持ち込んだ時、それを検知・遮断し、そのAPが設置されている場所を特定できるか	✔				✔	✔	
	認可されていない端末が、フロア内に設置されているWi-Fi APに接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか		✔			✔	✔	
	フロア内のプリンターに装備されているWi-Fi Direct機能が有効にされている時に、認可されていない端末がWi-Fi Directに接続された場合、それを検知・遮断できるか			✔		✔	✔	
	フロア内に設置されているWi-Fi APがDoS攻撃を受けた場合、それを検知できるか、また、レポートされるか				✔		✔	✔
	不正Wi-Fi APの持ち込み、端末の不正接続の対策に有用な情報が記載されているか	✔	✔	✔	✔	✔	✔	

※ 本資料では主要な検証項目のみ抜粋している。

グレスアベイル社と協議の上、GUARDIAXの差別化ポイントとされる事項を検証する検証項目及び検証方法を策定した。

- GUARDIAXに関して22の検証項目を策定し、策定した検証項目に基づき検証を実施した。

GUARDIAXにおける検証項目と、対応する差別化ポイントとされる事項・検証方法（抜粋版）

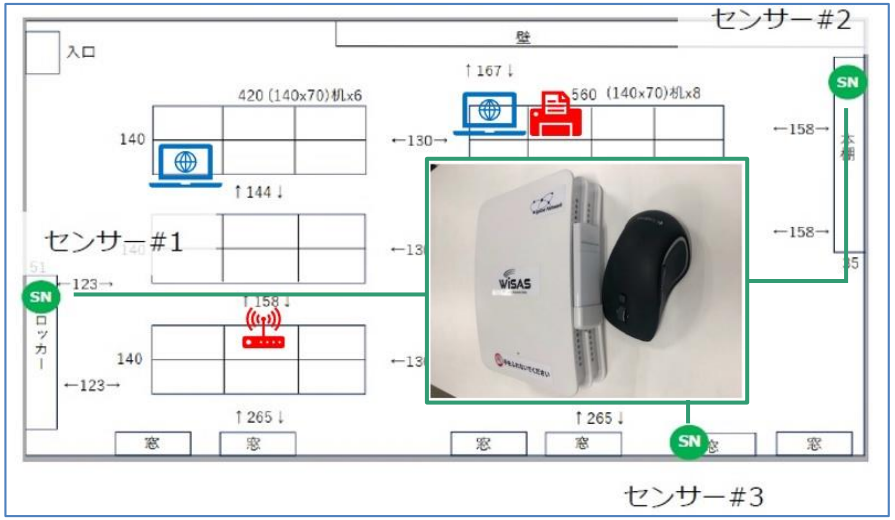
検証項目		差別化ポイントとされる事項				検証方法		
大分類	検証項目	強固な防御ルールであること	偽陽性が少ないこと	攻撃状況が判るダッシュボードであること	防御ルールをWebサイト単位でチューニングできること	検証環境での実検証	データや記録に基づく評価	ベンダーヒアリングに基づく評価
製品機能・性能	他社製WAFと比較して強固な防御ルールを実現できているか	✔			✔	✔	✔	
	他社製WAFと比較して偽陽性が少ないか		✔			✔	✔	
	ダッシュボードにおいて攻撃の有無を確認できるか			✔		✔		
	ダッシュボードにおいて検知した攻撃の詳細を確認できるか			✔		✔		
	ダッシュボードにおいて検知した攻撃のレベル分けができるか			✔		✔		

※ 本資料では主要な検証項目のみ抜粋している。

WiSASの検証は、オフィスビルの1フロアを活用して実施した。
また、GUARDIAXの検証は、検証用のWebサイトを構築して実施した。

- WiSASの検証は、縦：約15m、横：約10m、高さ：約2.7mのオフィスビルフロアにて実施した。
  - フロア内に3台のWiSASセンサーを設置し、また、ホワイトリスト（WL）に登録したWi-Fi APや端末、Wi-Fi Direct搭載プリンターを設置した。
  - この環境に対して、WLに登録されていないWi-Fi APや端末を持ち込みや接続した場合の結果を検証した。
- GUARDIAXの検証は、AWS上に検証用のWebサイトを構築し、GUARDIAXのSaaS版を経由して検証する環境を構築した。
  - Burp Suiteを用いてWebサイトへの攻撃を実施し、防御性能や偽陽性が少ないことを検証した。

WiSASの検証環境

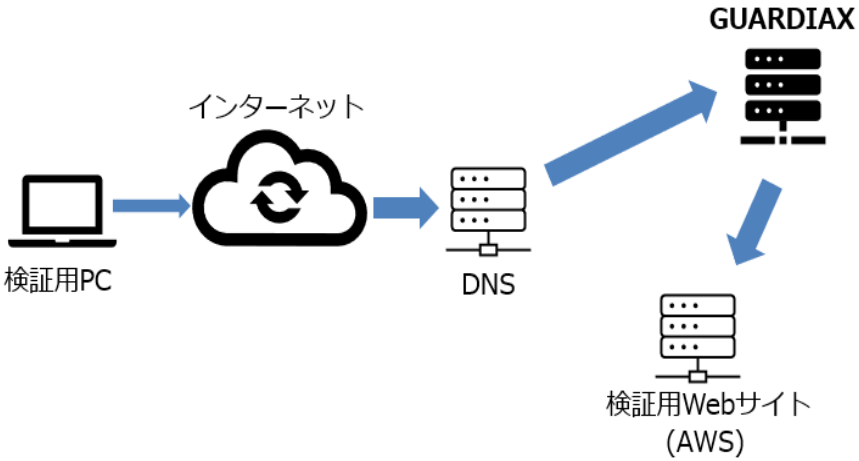


ホワイトリストに登録したWi-Fi AP

ホワイトリストに登録した端末

Wi-Fi Direct搭載プリンター

GUARDIAXの検証環境



「製品機能・性能」、「運用性」、「導入容易性」の観点から検証を実施し、WiSASの差別化ポイントとされる4点を確認することができた。

- 今回の検証の範囲で、WiSASの差別化ポイントとされる以下の4点を確認することができた。
  - 不正なWi-Fi APを検知、遮断できること
  - 不正な端末の接続を検知、遮断できること
  - Wi-Fi Directへの不正な端末の接続を検知、遮断できること
  - Wi-Fi環境へのDoS攻撃の有無を確認できること

WiSASにおける主要な検証項目に対する検証結果

検証項目		検証結果
大分類	検証項目	
製品機能・性能	認可されていないWi-Fi APをフロア内に持ち込んだ時、それを検知・遮断し、そのAPが設置されている場所を特定できるか	• 認可されているWi-Fi APと同じSSIDになりすましたWi-Fi AP（認可されていない Wi-Fi AP）が検知・遮断できた。 • また、そのWi-Fi APが設置されている場所を特定できた。
	認可されていない端末が、フロア内に設置されているWi-Fi APに接続した時、それを検知・遮断し、その端末が設置されている場所を特定できるか	• 認可されているWi-Fi APに対して、認可されていない端末が接続した場合に、その端末を検知・遮断できた。 • また、その端末が設置されている場所を特定できた。
	フロア内のプリンターに装備されているWi-Fi Direct機能が有効にされている時に、認可されていない端末がWi-Fi Directに接続された場合、それを検知・遮断できるか	• Wi-Fi Direct機能が有効にされてプリンターに対して、認可されていない端末がWi-Fi Directに接続された場合、それを検知・遮断することができた。
	フロア内に設置されているWi-Fi APがDoS攻撃を受けた場合、それを検知できるか、また、レポートされるか	• 過去の事例より、Wi-Fi APがDoS攻撃を受けた場合に検知し、レポートされることを確認した。
	不正Wi-Fi APの持ち込み、端末の不正接続の対策に有用な情報が記載されているか	• 不正Wi-Fi APの持ち込み、端末の不正接続の対策として有用な情報が報告書に記載されていることを確認した。 • 具体的には、報告書の各項目において、対策として有用な情報が記載されているほか、認可されていないWi-Fi APが検出された場合の危険性も記載されていた。

※ 本資料では主要な検証項目・検証結果のみ抜粋している。

「製品機能・性能」、「運用性」、「導入容易性」の観点から検証を実施し、GUARDIAXの差別化ポイントとされる4点を確認することができた。

- 今回の検証の範囲で、GUARDIAXの差別化ポイントとされる以下の4点を確認することができた。
  - 強固な防御ルールであること
  - 偽陽性が少ないこと
  - 攻撃状況が判るダッシュボードであること
  - 防御ルールをWebサイト単位でチューニングできること

GUARDIAXにおける主要な検証項目に対する検証結果

検証項目		検証結果
大分類	検証項目	
製品機能・性能	他社製WAFと比較して強固な防御ルールを実現できているか	• 今回の検証の範囲において、OWASP Top 10をはじめとする**主要な攻撃を防御**できることを確認した。 • また、製品ベンダーから提供されたデータに基づいて、強固な防御ルールを実現していることを確認した。
	他社製WAFと比較して偽陽性が少ないか	• 今回の検証の範囲において、攻撃文字列に似せた文字列(正常なリクエスト)に基づいたリクエストをしても、その**リクエストを誤って遮断することが無い**ことを確認した。 • また、製品ベンダーから提供されたデータに基づいて、偽陽性が少ないことを確認した。
	ダッシュボードにおいて攻撃の有無を確認できるか	• **ダッシュボードにおいて攻撃の有無を確認**できた。 • 具体的には、検知した攻撃件数と脅威度の割合、タイムライン、攻撃元国別Top5、攻撃元IPアドレスのTop5、攻撃元マップを視覚的に確認できた。
	ダッシュボードにおいて検知した攻撃の詳細を確認できるか	• **ダッシュボードにおいて検知した攻撃の詳細を確認**できた。 • 具体的には、攻撃を検出した時間、脅威度、攻撃元国名、攻撃元IP、攻撃元ホスト、攻撃のコード(パス)、攻撃の種類、WAFが行ったアクション(検知のみ／通信のブロック)、WAFが攻撃と判断したコード(検知コード)を確認することができた。
	ダッシュボードにおいて検知した攻撃のレベル分けができるか	• 検知した攻撃の脅威レベルは3段階でレベル分けがされていた。

※ 本資料では主要な検証項目・検証結果のみ抜粋している。

2020年度事業では、セキュリティ製品の有効性を検証する検証基盤を構築し、構築した検証基盤に基づき、製品の公募・選定・有効性検証を行った。

2020年度事業のまとめ

- 公平性を確保しながら製品公募・対象製品選定を実施する仕組み、効率的な有効性検証の仕組み、及び検証結果公表等の仕組みから成るサイバーセキュリティ検証基盤について、構築を行った。
- 構築した検証基盤を実際に運用して、検証対象候補の製品を公募し、計6製品の応募が寄せられた。
- WiSAS及びGUARDIAXを対象製品として選定し、有効性検証を実施した。
- 「製品機能・性能」、「運用性」、「導入容易性」の観点から有効性検証を実施し、それぞれの製品において差別化ポイントとされる事項を確認することができた。

今後の方向性

- 検証作業のさらなる効率化　⇒　より多くの製品に対する有効性検証の実施
- 市場環境を考慮した検証項目・検証方法の策定
- 検証基盤の効果測定

未来を問い続け、変革を先駆ける

MRI 三菱総合研究所