

中小企業向けサイバーセキュリティ製品・サービスに関する  
情報提供プラットフォーム構築に向けた試行環境調査  
成果報告書

2022年4月28日



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

*This page is intentionally left blank*

## 目次構成

1. 調査の背景と目的	1
2. 調査の概要	2
2.1. 調査の全体像	2
2.2. 試行環境調査の概要	2
2.2.1. 登録申請様式及び申請受付マニュアルの作成の概要	2
2.2.2. 中小企業向け製品・サービス公募の試行実施の概要	3
2.2.3. 中小基盤の構築と製品・サービス情報の掲載の概要	4
2.2.4. 中小基盤の公開とアクセスの概要	5
2.2.5. 中小企業による中小基盤に対する評価アンケートの実施の概要	6
2.3. セキュリティ製品・サービスの市場調査の概要	10
2.4. 中小基盤の有用性検証及び構築上の課題洗い出しの概要	13
2.5. 有識者検討委員会の設置及び運営の概要	13
3. 試行環境調査の結果	15
3.1. 登録申請様式及び申請受付マニュアルの作成	15
3.1.1. 登録申請様式の作成	15
3.1.2. 申請受付マニュアルの作成	22
3.2. 中小企業向け製品・サービス公募の試行実施	26
3.2.1. 試行対象製品・サービスの公募	26
3.2.2. 試行対象製品・サービスの選定	26
3.2.3. 中小基盤への登録申請	29
3.3. 中小基盤の構築と製品・サービス情報の掲載	29
3.3.1. 仮設サイトの構築	29
3.3.2. 製品・サービス情報の掲載	39
3.3.3. 中小企業ユーザーの事後評価情報の登録	44
3.4. 中小基盤の公開とアクセス	44
3.4.1. 中小基盤へのアクセス状況の集計・分析	45
3.4.2. 情報提供機能や検索機能の利用状況の集計・分析	47
3.5. 中小企業による中小基盤に対する評価アンケートの実施	49
3.5.1. アンケート項目の作成	49

3.5.2. アンケート結果の集計・分析 .....	50
4. セキュリティ製品・サービスの市場調査の結果 .....	62
4.1. セキュリティ製品・サービスの市場調査に関するアンケートの実施 .....	62
4.1.1. アンケート項目の作成 .....	62
4.1.2. アンケート結果の集計・分析 .....	62
4.2. セキュリティ製品・サービスの市場調査に関するヒアリングの実施 .....	71
4.2.1. ヒアリング項目の作成 .....	72
4.2.2. ヒアリング結果の分析 .....	72
5. 中小基盤の有用性検証及び構築上の課題洗い出し .....	78
5.1. 中小基盤の有用性に関する全体評価 .....	78
5.2. 中小基盤に求められる要件の整理 .....	78
5.2.1. 中小基盤のターゲットユーザー.....	78
5.2.2. 中小基盤のサイト構成.....	79
5.2.3. 中小基盤に掲載する製品情報の内容.....	79
5.2.4. 中小基盤に掲載する製品情報の質.....	79
5.2.5. 中小基盤に掲載する製品情報以外の情報.....	79
5.2.6. 中小基盤上で提供する検索機能.....	80
5.3. 中小基盤の構築に向けた検討課題 .....	80
5.3.1. 中小基盤環境の構築(設置場所及び運営主体).....	80
5.3.2. 中小企業のアクセス促進に繋がる仕組み.....	81
5.3.3. 製品・サービスの応募促進に繋がる仕組み.....	82
5.3.4. 事業告知及びプロモーション手段.....	82
6. 本調査の総括 .....	84

## 1. 調査の背景と目的

産業活動においてサプライチェーンリスクの問題が顕在化しつつある昨今、サプライチェーンを構成する中小企業におけるサイバーセキュリティ対策促進が喫緊の課題である。そのような中、市場に流通しているセキュリティ製品・サービスは、中小企業から見て過度に高機能、運用コストが高い等、中小企業のニーズにマッチしていないとの声がある。また、中小企業にも導入できる製品・サービスであっても、導入効果等に関する理解を得にくいため、中小企業に使われにくいという声もあることから、中小企業でも扱いやすい製品・サービス選びの一助となる情報を提供するプラットフォーム（以下、「中小基盤」という。）が求められている。

このような状況を踏まえ、独立行政法人情報処理推進機構（以下「IPA」という。）では、令和元年度において「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査（以下「実現可能性調査」という。）」を、令和2年度において「中小企業向け情報提供プラットフォームの在り方に関するニーズ調査（以下「ニーズ調査」という。）」を実施した。

令和元年度の実現可能性調査では、サイバーセキュリティの有識者による検討委員会を開催し、中小企業が製品・サービスを選ぶ際に参考となる評価項目（以下「評価項目」という。）を作成し、中小企業のユーザー実証（3製品6ユーザー）により、評価項目の有効性を検証した。令和2年度のニーズ調査では、実現可能性調査の結果を元に、中小企業へのアンケート調査（有効回答数：1,961件）、並びに製品・サービスベンダーへのヒアリング調査（5者）を実施し、中小基盤の在り方に関して、それぞれのニーズの整理を行った。

本事業は、上記の実現可能性調査とニーズ調査で得られた内容を踏まえて、中小基盤の構築を試行的に実施（以下「試行環境調査」という。）を実施し、併せてセキュリティ製品・サービスの市場調査を実施することで、中小基盤の有用性を検証した上で、将来的な中小基盤の構築上の課題の洗い出しを行った。

## 2. 調査の概要

### 2.1. 調査の全体像

本事業においては、中小基盤の構築を試行的に実施する「試行環境調査」と、「セキュリティ製品・サービスの市場調査」の2つの調査を実施した。これらの結果から、中小基盤の有用性を検証するとともに、中小基盤の構築上の課題を抽出し整理した。

これらの調査結果は課題として取りまとめ、サイバーセキュリティの有識者、専門家等より構成した「有識者検討委員会」に諮って、専門的な視点から助言を得た。

### 2.2. 試行環境調査の概要

試行環境調査は、大別すると「中小企業向け製品・サービス公募の試行実施」、「中小基盤の構築」、「中小基盤の運用」の3つのプロセスにより実施した。

「中小企業向け製品・サービス公募の試行実施」については、中小企業向け製品・サービス公募の準備作業として、登録申請様式及び申請受付マニュアルを作成し、中小企業向け製品・サービスの公募を行った上で、応募のあった製品・サービスの中から中小基盤に掲載する製品・サービスを選定した。これらのプロセスの実施内容を「2.2.1. 登録申請様式及び申請受付マニュアルの作成の概要」、「2.2.2. 中小企業向け製品・サービス公募の試行実施の概要」に詳述する。

「中小基盤の構築」については、中小基盤の仮設サイト（以下「仮設サイト」という。）を構築し、構築した仮設サイトに選定した製品・サービスに関する情報等の情報を掲載した。これらのプロセスの実施内容を「2.2.3. 中小基盤（仮設サイト）の構築と製品・サービス情報の掲載の概要」に詳述する。

「中小基盤の運用」については、仮設サイトを期間限定で特定対象者に公開し、中小基盤に対する中小企業の評価を得るため、仮設サイト上でWebアンケートを実施した。これらのプロセスの実施内容を「2.2.4. 中小基盤（仮設サイト）の公開とアクセスの概要」、「2.2.5. 中小企業による評価アンケートの実施の概要」に詳述する。

#### 2.2.1. 登録申請様式及び申請受付マニュアルの作成の概要

登録申請様式については、必要な情報を製品・サービスベンダーから収集できるよう、製品・サービスベンダーが製品・サービスに関する情報の中小基盤への掲載を申請するための様式（以下「登録申請書」という。）と、製品・サービスを導入済みの中小企業ユーザーから収集した評価情報について中小基盤への掲載を申請するための様式（以下「中小企業ユーザーによる製品等の評価情報提出用紙」という。）の2つの様式を作成した。

登録申請書の作成においては、令和元年度の実現可能性調査で作成した中小企業が製品・サービスを選ぶ際に参考となる「評価項目」や、各種コンテンツ（評価項目の定義・解説書、申請時の記載方法の手引書、中小基盤の活用方法の解説書）の内容を踏まえ、申請者にとって分かりやすいものとし、かつ申請者間で申請される情報の記載の粒度や書きぶり、情報量

の同質性を担保できるよう、登録申請書の記載例を作成するとともに、評価項目についても各評価項目で想定する内容の例示を作成した。

また、申請受付マニュアルについては、試行環境調査に係る中小企業向け製品・サービスの公募を行う際に、製品・サービスの申請の受付から、提出された登録申請書の内容確認、中小基盤への登録可否の判断等、製品・サービスベンダーからの提供情報を中小基盤へ登録するまでに必要となる手続きについて記載したマニュアルを作成した。

## 2.2.2. 中小企業向け製品・サービス公募の試行実施の概要

中小基盤に掲載する中小企業向け製品・サービスに関する情報を収集するため、中小基盤への情報掲載を申請する製品・サービスベンダーを募集する公募（以下「中小企業向け製品・サービス公募」という。）を試行的に実施した。

具体的には、告知方法、公募期間、応募資格、実施内容、選定方法、通知方法等を含む中小企業向け製品・サービス公募の実施方針について検討し、有識者検討委員会に諮問した上で、当該実施方針を取りまとめて、中小企業向け製品・サービス公募を実施した。

中小企業向け製品・サービス公募の実施方針を以下に示す。

### 【中小企業向け製品・サービス公募の実施方針】

#### (1) 告知方法

中小企業向け製品・サービス公募のお知らせを掲載するためのホームページを作成する。当該ホームページの告知については、特定非営利活動法人日本ネットワークセキュリティ協会（以下「JNSA」という。）の協力のもと、会員企業への電子メールによる告知や、メールマガジンによる告知を行う。

#### (2) 公募期間

令和3年10月21日（木）から、令和3年11月4日（木）17:00まで（必着）

#### (3) 応募資格

「中小企業向けサイバーセキュリティ製品・サービスの提供事業者」として応募可能な事業者は、以下に該当する事業者とする。

##### ① 中小企業向けサイバーセキュリティ製品・サービスを提供している事業者

（ただし、サイバーセキュリティサービスに関しては、サイバーセキュリティ製品と紐づく付帯的なサービスを想定する。セキュリティコンサルティングサービスやセキュリティ監査サービスなど製品と紐づかないサービスは対象外とする。）

##### ② 本事業が対象とする試行対象製品・サービス分野のサイバーセキュリティ製品・サービスを提供している事業者

（試行対象製品・サービス分野としては、A. インシデント発生時の迅速な初動対応（セキュリティ監視製品（UTM、IDS等））、B. 重要な情報の安全な取扱い（重要情報の保護に関する製品（認証、暗号等））、C. 不正プログラム対策（エンドポイントセキュリティ製品（EDR等））の3分野を想定する。ただし、一般に幅広く普及している製品・サービス（ウイルス対策ソフトなど）は対象外とする。加えて、部品・モジュール的に運用さ

れている製品・サービスについても、対象外とする。)

- ③本事業の実施に係る規約を遵守し、規約で定める同意書の提出が可能な事業者  
(本事業の実施への協力にあたり、採択された事業者においては同意書の提出を依頼する。)

(4) 実施内容

採択された事業者は主に以下のことに取り組む。

- ①中小企業ユーザーによる申請されたサイバーセキュリティ製品・サービスの評価情報の提出

(申請されたサイバーセキュリティ製品・サービスを既に導入している中小企業ユーザー(2ユーザー以上)の協力のもと、申請されたサイバーセキュリティ製品・サービスの評価や、当該評価情報の提出を行う。なお、提出期間は、採択通知後1週間程度を想定する。)

- ②本事業における各種情報提供等への協力

(採択されたサイバーセキュリティ製品・サービスに関する申請された情報や、中小企業ユーザーによる評価情報の提供とそれらの情報の中小基盤の仮設サイトへの掲載と公開について承諾し、必要に応じて、採択されたサイバーセキュリティ製品・サービスに関する追加的な情報の提出への協力を行う。)

(5) 選定方法

別途設置する第三者による委員会にて、採択の可否を判断しつつ候補を選定する。

(6) 通知方法

採択の可否が決定次第、応募者に対して電子メールにて結果を通知する。

中小企業向け製品・サービス公募にあたって、公募期間、応募資格、実施内容、応募手続き、選定方法、通知方法の他、留意事項、質問事項、応募先及び問合せ先を含め、それらを定めた公募要領を作成した。

加えて、実施内容が適切に行われることを担保するため、本事業の実施に係る規約を作成するとともに、申請者が当該規約に同意していることを確認するための同意書を作成した。

応募のあった中小基盤に掲載する製品・サービスの選定においては、有識者検討委員会の委員からも意見を聴取し、その内容を十分踏まえた上で評価を行った。

### 2.2.3. 中小基盤(仮設サイト)の構築と製品・サービス情報の掲載の概要

以下に示す中小基盤の仮設サイト構築の要件を満たした上で、選定・採択した製品・サービスに関する情報や、中小企業ユーザーによる製品・サービスの評価情報をHTML形式でコンテンツ化し掲載した仮設サイトを構築した。

#### 【中小基盤の仮設サイト構築の要件】

- (1) 中小企業が見て分かりやすいページ構成とし、中小企業が必要な情報が検索できる機能を備える



- (2) アクセス状況や情報への閲覧状況を記録分析できるようにする
- (3) 仮設サイトへのアクセスが安全に行えるよう、必要なセキュリティ対策を講じる

上記の仮設サイト構築の要件のうち、(1)については、中小企業が見て分かりやすいように、「サイトの説明」、「検索」、「製品・サービス紹介」、「アンケート」をホームページのタブメニューとして設定するとともに、各製品・サービスに関する情報への効率のよいアプローチ方法として、以下に示す3つの方法を仮設サイトに実装した。

- ①「サイトの説明」ページ及び「検索」ページの中で提供される注目ワードによる検索機能を利用して、各製品・サービスに関する情報にアプローチする方法
- ②「検索」ページの中で提供される「製品・サービスの種類から探す」、「目的から探す」、「自社の特徴から探す」といった各種検索機能を利用して、各製品・サービスに関する情報にアプローチする方法
- ③「製品・サービス紹介」ページの中で提供される製品・サービス一覧機能から対象製品・サービスを選択して各製品・サービスに関する情報にアプローチする方法

上記①に関しては、ランサムウェア対策、テレワークのセキュリティ対策、GDPR(EU一般データ保護規則)への対応といった注目ワードによる検索機能を実装した。また、上記②に関しては、製品・サービスの種類、予算、対応可能な脅威、ユーザーサポート体制、お試し利用の有無、従業員規模、業種による検索機能を実装した。

(2)については、ページビュー数や各製品・サービスに関する情報へのアクセス数、各検索条件による検索回数等の記録分析ができるように必要となるログを収集する機能を実装するとともに、(3)については、ファイアウォール、ウェブアプリケーションファイアウォール(WAF)、ウイルス対策ソフトの導入・運用や、ドメイン認証、自動バックアップ等の必要なセキュリティ対策機能を実装した。

なお、(1)の仮設サイトのページ構成ならびに検索機能については、有識者検討委員会にて意見を聴取し、その内容を踏まえた上で検討を行った。

#### 2.2.4. 中小基盤(仮設サイト)の公開とアクセスの概要

完成した中小基盤の仮設サイトを Web 環境上に公開し、前述したページビュー数や各製品・サービスに関する情報へのアクセス数、各検索条件による検索回数等を含め、仮設サイトへのアクセスに関する調査・分析を行った。

また、中小基盤の仮設サイトを中小企業に閲覧してもらうため、セキュリティ対策自己宣言「SECURITY ACTION」制度の宣言事業者のうち、情報提供・調査への協力について承諾を得ている事業者 71,123 社に対して、中小基盤の仮設サイトの評価アンケート依頼メールを送り、仮設サイトの閲覧を促すとともに、仮設サイトでの Web アンケートに協力いただいた。なお、中小基盤の仮設サイトの公開期間は、2021年12月7日(火)から2022年1月31日(月)までの56日間とし、仮設サイト上で提供する「アンケート」ページのみ、アンケート結果の集計・分析が必要となるため、2022年1月14日(金)までの公開とした。

### 2.2.5. 中小企業による評価アンケートの実施の概要

中小基盤の仮設サイトに掲載された情報や検索機能が、中小企業にとって活用しやすいものであるかを確認するため、前述した仮設サイト上で提供する「アンケート」ページにて、中小基盤の仮設サイトの有用性評価に関するアンケート調査（以下「有用性評価アンケート調査」という。）を実施した。

有用性評価アンケート調査の設問については、有識者検討委員会で意見を聴取し、その内容を踏まえた上で作成を行った。有用性評価アンケート調査の調査票を以下に示す。



図表 2-1 有用性評価アンケート調査の調査票(続き)

**中小基盤の仮設サイトで提供している、製品・サービスの検索機能についてお伺いいたします。**

**問 8** 貴社において、サイバーセキュリティ製品・サービスの導入を検討する際に、中小基盤の仮設サイトで提供している、製品・サービスの検索機能は、どの程度役に立つと思えますか。当てはまるものにチェックを入れてください。

- かなり役に立つ
- 多少役に立つ
- あまり役に立たない
- まったく役に立たない
- 分からない

問 8 で、「かなり役に立つ」、「多少役に立つ」とお答えになられた方にお伺いします。  
「あまり役に立たない」、「まったく役に立たない」、「分からない」とお答えになられた方は、問 11 へお進みください。

**問 9** 問 8 で、役に立つとお答えになられた製品・サービスの検索機能について、以下の中から当てはまるものにチェックを入れてください。(複数回答可)

- 注目ワードによる製品・サービス検索
- 製品・サービスの種類から探す (製品・サービスの種類による製品・サービス検索)
- 目的から探す / 予算に合うものを選びたい (予算による製品・サービス検索)
- 目的から探す / 事故が起きないように対策したい (対応可能な脅威による製品・サービス検索)
- 目的から探す / 手厚いサポートを受けたい (ユーザーサポート体制による製品・サービス検索)
- 目的から探す / お試し利用をしたい (お試し利用による製品・サービス検索)
- 自社の特徴から探す / 従業員規模から探す (従業員規模による製品・サービス検索)
- 自社の特徴から探す / 業種から探す (業種による製品・サービス検索)
- その他 ( )

**問 10** 問 9 でお答えになられた製品・サービスの検索機能について、貴社においてサイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容を、下の自由記述欄にご記入ください。

問 10 にお答えになられた方は問 12 にお進みください。

**問 11** 問 8 で、「あまり役に立たない」、「まったく役に立たない」、「分からない」とお答えになられた、具体的な理由や内容を、下の自由記述欄にご記入ください。

**中小基盤の仮設サイトで提供している、製品・サービスの各種情報についてお伺いいたします。**

**問 12** 貴社において、サイバーセキュリティ製品・サービスの導入を検討する際に、中小基盤の仮設サイトで提供している、製品・サービスの各種情報について、どの程度役に立つと思えますか。当てはまるものにチェックを入れてください。

- かなり役に立つ
- 多少役に立つ
- あまり役に立たない
- まったく役に立たない
- 分からない

問 12 で、「かなり役に立つ」、「多少役に立つ」とお答えになられた方にお伺いします。  
「あまり役に立たない」、「まったく役に立たない」、「分からない」とお答えになられた方は、問 15 へお進みください。

**問 13** 問 12 で、役に立つとお答えになられた製品・サービスの各種情報について、以下の中から当てはまるものにチェックを入れてください。(複数回答可)

- 製品・サービス一覧
- 各製品・サービスの提供事業者や製品・サービス名称
- 各製品・サービスのテクノロジー (技術概要)
- 各製品・サービス情報
- 各製品・サービスに関するお問い合わせ
- 各製品・サービスのユーザーの評価情報
- 各製品・サービスの詳しい情報 (詳細情報)
- 資料ダウンロードで提供されるダウンロードファイル情報 (ダウンロード可能な事業者提供情報)
- その他 ( )

図表 2-1 有用性評価アンケート調査の調査票(続き)

問14 問13でお答えになられた製品・サービスの情報について、貴社においてサイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容を、下の自由記述欄にご記入ください。

問14にお答えになられた方は問16にお進みください。

問15 問12で、「あまり役に立たない」、「まったく役に立たない」、「分からない」とお答えになられた、具体的な理由や内容を、下の自由記述欄にご記入ください。

問16 サイバーセキュリティ製品・サービスの導入に際し、中小基盤の本番サイトが提供されれば、利用してみたいですか。当てはまるものにチェックを入れてください。

- ぜひ利用したい
- 条件によっては利用したい
- 利用したいとは思わない
- 分からない

問16で、「条件によっては利用したい」とお答えになられた方は問17へお進みください。

「利用したいとは思わない」とお答えになられた方は問18へお進みください。

また上記以外の方は問19へお進みください。

問17 問16で、「条件によっては利用したい」とお答えになられた方にお伺いします。中小基盤の本番サイトにおいて、どのような条件が緩和・改善されれば、利用したいと思えますか。条件に関する具体的なお考えについて、下の自由記述欄にご記入ください。

問17にお答えになられた方は問19にお進みください。

問18 問16で、「利用したいとは思わない」とお答えになられた方にお伺いします。「利用したいとは思わない」とお答えになられた、具体的な理由や内容を、下の自由記述欄にご記入ください。

問19 中小基盤の本番サイトが提供された場合に、以下の機能が備わっていて、使えた方がよいと思えますか。当てはまるものにチェックを入れてください。

- ①製品・サービスの評価情報を自らが書き込むことができる機能  使えた方がよい  どちらでもよい  使えなくてもよい
- ②同じ種類の製品・サービスが複数掲載されている場合に、それぞれの  使えた方がよい  どちらでもよい  使えなくてもよい  
特徴や機能を比較して表示できる機能

問20 その他、今後、中小基盤の仮設サイトから本番サイトへ更新していくにあたって、もっと充実してほしい情報や追加してほしい機能、改善してほしいサイトのデザインはありますか。情報や機能、デザインに関するご要望の具体的な内容を、下の自由記述欄にご記入ください。

問21 差支えなければ、貴社の企業名について、お答えください。

アンケートは以上です。ご協力ありがとうございました。

### 2.3. セキュリティ製品・サービスの市場調査の概要

将来的な中小基盤の構築に向けた具体化検討のための前提情報として、市場に流通しているセキュリティ製品・サービスのうち、中小企業にも導入できる製品・サービスがどれくらいあるのか、また、製品・サービスベンダーが中小企業向けセキュリティ製品・サービスを提供する上で、どのような制約事項があるのか等を把握するため、中小企業向けセキュリティ製品等の市場調査に関するアンケート（以下「市場アンケート調査」という。）を実施した。市場アンケート調査は、以下の2つを調査対象として実施した。

#### 【市場アンケート調査の調査対象】

- (1) JNSA が提供する「JNSA ソリューションガイド」に掲載されている 385 点の製品(2021年6月時点)を提供するベンダーを含む JNSA の会員企業
- (2) 中小基盤の仮設サイトに中小企業向けセキュリティ製品・サービスを掲載したベンダー

市場アンケート調査の設問については、有識者検討委員会にて意見を聴取し、その内容を踏まえた上で作成を行った。市場アンケート調査の調査票を以下に示す。

図表 2-2 市場アンケート調査の調査票

「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」 中小企業向けサイバーセキュリティ製品・サービスの市場調査に関する質問票		事務局																											
<p>本日はご多忙のところ、中小企業向けサイバーセキュリティ製品・サービスの市場調査を御協力いただきありがとうございました。今後の中小基盤の本番サイト構築に向けた検討の参考とさせていただきます。以下の質問票にご回答いただきますよう、お願い申し上げます。</p>																													
<p><b>問1 貴社が提供しているサイバーセキュリティ製品・サービスの中に、中小企業向けを謳っている製品・サービスがありますか。当てはまるものにチェックを入れてください。またそのような製品・サービスを提供している場合は、( ) 内に製品・サービスの商品点数を併せてお答えください。</b></p> <p><input type="checkbox"/> 中小企業向けを謳っている製品・サービスがある (商品点数: )</p> <p><input type="checkbox"/> 中小企業向けを謳っていない製品・サービスはない</p>																													
<p><b>問2 貴社が提供しているサイバーセキュリティ製品・サービスの中に、中小企業向けを謳っていないが、中小企業に対しても十分適用でき、中小企業への豊富な導入実績のある製品・サービスがありますか。当てはまるものにチェックを入れてください。また提供している場合は、( ) 内に製品・サービスの商品点数を併せてお答えください。</b></p> <p><input type="checkbox"/> 中小企業に対しても十分適用でき、中小企業への豊富な導入実績のある製品・サービスがある (商品点数: )</p> <p><input type="checkbox"/> 中小企業に対しても十分適用でき、中小企業への豊富な導入実績のある製品・サービスはない</p>																													
<p><b>問3 中小企業向けに、セキュリティ製品・サービスの提供ビジネスを展開していく上で、何が障壁になるとお考えですか。当てはまるものにチェックを入れてください。(複数回答可)</b></p> <p><input type="checkbox"/> 企業数が多く、要望が多様であるため、対応負荷が大きがちである</p> <p><input type="checkbox"/> 予算が小規模であり、提供可能な機能やサービスが限定されがちである</p> <p><input type="checkbox"/> 業績が不安定で景気の影響を受けやすく、製品・サービスの解約率が高くなりがちである</p> <p><input type="checkbox"/> 購買ニーズの把握が難しく、営業が非効率になりがちである</p> <p><input type="checkbox"/> 経営層や従業員が多忙で時間の制約が大きく、成約に至るまでの時間が長くなりがちである</p> <p><input type="checkbox"/> その他 ( )</p>																													
<p>問1で「中小企業向けを謳っている製品・サービスがある」、問2で「中小企業に対しても十分適用でき、中小企業への豊富な導入実績のある製品・サービスがある」のいずれかにお答えになられた方は問4へお進みください。それ以外の方は問10へお進みください。</p>																													
<p><b>問4 貴社では、どのような製品・サービス分野のサイバーセキュリティ製品・サービスを提供していますか。当てはまるものにチェックを入れてください。またそのうち、中小企業への導入実績が最も高い製品・サービス分野はどれですか。</b></p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;"></th> <th style="width: 20%; text-align: center;">製品・サービス分野</th> <th style="width: 20%; text-align: center;">中小企業への導入実績が最も高い製品・サービス分野</th> </tr> </thead> <tbody> <tr> <td>インシデント発生時の迅速な初動対応 (セキュリティ監視製品 (UTM、IDS等)、ログ管理・SIEM製品等)</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>重要な情報の安全な取扱い (重要情報の保護に関する製品 (認証、暗号、DLP、アクセスコントロール等))</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>不正プログラム対策 (エンドポイントセキュリティ製品 (EDR、マルウェア対策ソフト等))</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>クラウドサービスやネットワークの安全な利活用 (クラウドセキュリティ製品 (CASB等)、VPN機器・サービス等)</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>サイバー攻撃の早期の封じ込めや復旧 (データバックアップ対策、インシデント対応支援サービス等)</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>脆弱性やリスクの可視化・管理 (脆弱性診断、ペネトレーションテスト、リスクアセスメント等)</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>従業員等へのセキュリティ教育・訓練 (標的型メール訓練、インシデント対応模擬訓練等)</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>その他 ( )</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>				製品・サービス分野	中小企業への導入実績が最も高い製品・サービス分野	インシデント発生時の迅速な初動対応 (セキュリティ監視製品 (UTM、IDS等)、ログ管理・SIEM製品等)	<input type="checkbox"/>	<input type="checkbox"/>	重要な情報の安全な取扱い (重要情報の保護に関する製品 (認証、暗号、DLP、アクセスコントロール等))	<input type="checkbox"/>	<input type="checkbox"/>	不正プログラム対策 (エンドポイントセキュリティ製品 (EDR、マルウェア対策ソフト等))	<input type="checkbox"/>	<input type="checkbox"/>	クラウドサービスやネットワークの安全な利活用 (クラウドセキュリティ製品 (CASB等)、VPN機器・サービス等)	<input type="checkbox"/>	<input type="checkbox"/>	サイバー攻撃の早期の封じ込めや復旧 (データバックアップ対策、インシデント対応支援サービス等)	<input type="checkbox"/>	<input type="checkbox"/>	脆弱性やリスクの可視化・管理 (脆弱性診断、ペネトレーションテスト、リスクアセスメント等)	<input type="checkbox"/>	<input type="checkbox"/>	従業員等へのセキュリティ教育・訓練 (標的型メール訓練、インシデント対応模擬訓練等)	<input type="checkbox"/>	<input type="checkbox"/>	その他 ( )	<input type="checkbox"/>	<input type="checkbox"/>
	製品・サービス分野	中小企業への導入実績が最も高い製品・サービス分野																											
インシデント発生時の迅速な初動対応 (セキュリティ監視製品 (UTM、IDS等)、ログ管理・SIEM製品等)	<input type="checkbox"/>	<input type="checkbox"/>																											
重要な情報の安全な取扱い (重要情報の保護に関する製品 (認証、暗号、DLP、アクセスコントロール等))	<input type="checkbox"/>	<input type="checkbox"/>																											
不正プログラム対策 (エンドポイントセキュリティ製品 (EDR、マルウェア対策ソフト等))	<input type="checkbox"/>	<input type="checkbox"/>																											
クラウドサービスやネットワークの安全な利活用 (クラウドセキュリティ製品 (CASB等)、VPN機器・サービス等)	<input type="checkbox"/>	<input type="checkbox"/>																											
サイバー攻撃の早期の封じ込めや復旧 (データバックアップ対策、インシデント対応支援サービス等)	<input type="checkbox"/>	<input type="checkbox"/>																											
脆弱性やリスクの可視化・管理 (脆弱性診断、ペネトレーションテスト、リスクアセスメント等)	<input type="checkbox"/>	<input type="checkbox"/>																											
従業員等へのセキュリティ教育・訓練 (標的型メール訓練、インシデント対応模擬訓練等)	<input type="checkbox"/>	<input type="checkbox"/>																											
その他 ( )	<input type="checkbox"/>	<input type="checkbox"/>																											
<p><b>問5 問4でお答えになられたサイバーセキュリティ製品・サービスについて、製品・サービス名称や技術面・機能面の特徴、実現できること (解決可能な課題、対応可能な脅威) を、下の自由記述欄にご記入ください。</b></p> <div style="border: 1px solid black; height: 40px; margin-top: 10px;"></div>																													
<p>ここから先の質問は、提供している製品・サービスが複数点存在する場合は、中小企業への導入実績が最も高い製品・サービスを念頭に置いて、質問にお答えください。</p>																													
<p><b>問6 サイバーセキュリティ製品・サービスの中小企業ユーザーへの導入実績について、当てはまるものにチェックを入れてください。</b></p> <table style="width: 100%;"> <tr> <td><input type="checkbox"/> 100社未満に導入</td> <td><input type="checkbox"/> 5,000社～1万社未満に導入</td> </tr> <tr> <td><input type="checkbox"/> 100社～300社未満に導入</td> <td><input type="checkbox"/> 1万社～3万社未満に導入</td> </tr> <tr> <td><input type="checkbox"/> 300社～500社未満に導入</td> <td><input type="checkbox"/> 3万社～5万社未満に導入</td> </tr> <tr> <td><input type="checkbox"/> 500社～1,000社未満に導入</td> <td><input type="checkbox"/> 5万社～10万社未満に導入</td> </tr> <tr> <td><input type="checkbox"/> 1,000社～3,000社未満に導入</td> <td><input type="checkbox"/> 10万社以上に導入</td> </tr> <tr> <td><input type="checkbox"/> 3,000社～5,000社未満に導入</td> <td></td> </tr> </table>			<input type="checkbox"/> 100社未満に導入	<input type="checkbox"/> 5,000社～1万社未満に導入	<input type="checkbox"/> 100社～300社未満に導入	<input type="checkbox"/> 1万社～3万社未満に導入	<input type="checkbox"/> 300社～500社未満に導入	<input type="checkbox"/> 3万社～5万社未満に導入	<input type="checkbox"/> 500社～1,000社未満に導入	<input type="checkbox"/> 5万社～10万社未満に導入	<input type="checkbox"/> 1,000社～3,000社未満に導入	<input type="checkbox"/> 10万社以上に導入	<input type="checkbox"/> 3,000社～5,000社未満に導入																
<input type="checkbox"/> 100社未満に導入	<input type="checkbox"/> 5,000社～1万社未満に導入																												
<input type="checkbox"/> 100社～300社未満に導入	<input type="checkbox"/> 1万社～3万社未満に導入																												
<input type="checkbox"/> 300社～500社未満に導入	<input type="checkbox"/> 3万社～5万社未満に導入																												
<input type="checkbox"/> 500社～1,000社未満に導入	<input type="checkbox"/> 5万社～10万社未満に導入																												
<input type="checkbox"/> 1,000社～3,000社未満に導入	<input type="checkbox"/> 10万社以上に導入																												
<input type="checkbox"/> 3,000社～5,000社未満に導入																													

図表 2-2 市場アンケート調査の調査票(続き)

**問7 サイバーセキュリティ製品・サービスの中小企業ユーザーの中で、ボリュームゾーンの業種（上位3業種）について、当てはまるものにチェックを入れてください。**

- |                                       |  |  |  |
|---------------------------------------|--|--|--|
| <input type="checkbox"/> 農業、林業        | <input type="checkbox"/> 電気・ガス・熱供給・水道業   | <input type="checkbox"/> 不動産業・物品賃貸業      | <input type="checkbox"/> 医療、福祉             |
| <input type="checkbox"/> 漁業           | <input type="checkbox"/> 情報通信業           | <input type="checkbox"/> 学術研究、専門・技術サービス業 | <input type="checkbox"/> 複合サービス事業          |
| <input type="checkbox"/> 鉱業、採石業、砂利採取業 | <input type="checkbox"/> 運輸業・郵便業（倉庫業を含む） | <input type="checkbox"/> 宿泊業、飲食サービス業     | <input type="checkbox"/> サービス業（他に分類されないもの） |
| <input type="checkbox"/> 建設業          | <input type="checkbox"/> 卸売業・小売業         | <input type="checkbox"/> 生活関連サービス業、娯楽業   | <input type="checkbox"/> 公務（他に分類されるものを除く）  |
| <input type="checkbox"/> 製造業（印刷業を含む）  | <input type="checkbox"/> 金融業・保険業         | <input type="checkbox"/> 教育、学習支援業        | <input type="checkbox"/> その他               |

**問8 サイバーセキュリティ製品・サービスの中小企業ユーザーの中で、ボリュームゾーンの従業員規模（上位1区分）について、当てはまるものにチェックを入れてください。**

- |                                  |                                    |                                    |
|----------------------------------|------------------------------------|------------------------------------|
| <input type="checkbox"/> 5名以下    | <input type="checkbox"/> 21名～50名   | <input type="checkbox"/> 201名～300名 |
| <input type="checkbox"/> 6名～10名  | <input type="checkbox"/> 51名～100名  | <input type="checkbox"/> 301名以上    |
| <input type="checkbox"/> 11名～20名 | <input type="checkbox"/> 101名～200名 | <input type="checkbox"/> 把握していない   |

**問9 以下に示す、中小企業ユーザーが製品・サービス選びにおいて重視している、中小企業向けサイバーセキュリティ製品・サービスに関する評価項目（評価項目の観点、詳細な評価項目）のうち、サイバーセキュリティ製品・サービスの中小企業ユーザーへの訴求ポイントとして、当てはまるものにチェックを入れてください。（複数回答可）**

- 選択肢割愛 ※令和元年度調査で取りまとめた23の評価項目を選択肢とする。

問12へお進みください。

**問10 今後、中小企業向け製品・サービスを提供する予定はありますか。当てはまるものにチェックを入れてください。**

- 近々、中小企業向け製品・サービスを提供する予定がある（開発中）  
 将来的に、中小企業向け製品・サービスを提供する予定がある（計画中）  
 今後も中小企業向け製品・サービスの提供は行わない

問10で、「近々、中小企業向け製品・サービスを提供する予定がある（開発中）」、「将来的に、中小企業向け製品・サービスを提供する予定がある（計画中）」とお答えになられた方は、問11へお進みください。  
「今後も中小企業向け製品・サービスの提供は行わない」とお答えになられた方は、問12へお進みください。

**問11 貴社では、どのような製品・サービス分野のサイバーセキュリティ製品・サービスを提供する予定ですか。当てはまるものにチェックを入れてください。**

- インシデント発生時の迅速な初動対応（セキュリティ監視製品（UTM、IDS等）、ログ管理・SIEM製品等）  
 重要な情報の安全な取扱い（重要情報の保護に関する製品（認証、暗号、DLP、アクセスコントロール等））  
 不正プログラム対策（エンドポイントセキュリティ製品（EDR、マルウェア対策ソフト等））  
 クラウドサービスやネットワークの安全な利活用（クラウドセキュリティ製品（CASB等）、VPN機器・サービス等）  
 サイバー攻撃の早期の封じ込めや復旧（データバックアップ対策、インシデント対応支援サービス等）  
 脆弱性やリスクの可視化・管理（脆弱性診断、ペネトレーションテスト、リスクアセスメント等）  
 従業員等へのセキュリティ教育・訓練（標的型メール訓練、インシデント対応模擬訓練等）  
 その他（ ）

**問12 中小企業向けサイバーセキュリティ製品・サービスの市場構造や市場環境を深堀して把握するためのヒアリングをお願いした場合に、御協力いただくことは可能ですか。当てはまるものにチェックを入れてください。**

- 協力してもよい  
 条件によっては協力してもよい（条件： ）  
 協力は難しい

問12で、「協力してもよい」、「条件によっては協力してもよい」とお答えになられた方は、問13へお進みください。  
それ以外の方は問14へお進みください。

**問13 ヒアリングをお願いさせていただく際に必要となる連絡先（御担当者名、メールアドレス）について、お答えください。**

御担当者名

メールアドレス

**問14 貴社の企業名について、お答えください。**

アンケートは以上です。ご協力ありがとうございました。



また、市場アンケート調査の回答先から5社に対して、Web会議によるヒアリング調査(以下「ベンダーヒアリング調査」という。)を実施した。

#### 2.4. 中小基盤の有用性検証及び構築上の課題洗い出しの概要

2.2.4. で前述した「仮設サイトへのアクセスに関する調査・分析結果」、2.2.5. で前述した「有用性評価アンケート調査の結果」、2.3. で前述した「市場アンケート調査の結果」、「ベンダーヒアリング調査の結果」の4つの調査結果をもとに、中小基盤の有用性に関する全体評価と、中小基盤に求められる要件の整理を行い、今後、中小基盤を構築するとした場合に留意すべき観点として、以下の4つの観点を設定し、それぞれの観点からみた中小基盤の構築に向けた検討課題の洗い出しを行った。

##### 【中小基盤の構築における課題検討の観点】

- (1) 中小基盤環境の構築(設置場所及び運営主体)
- (2) 中小企業のアクセス促進に繋がる仕組み
- (3) 製品・サービスの応募促進に繋がる仕組み
- (4) 事業告知及びプロモーション手段

上記で抽出した検討課題は、有識者検討委員会に諮り、専門的な視点から助言を得た。

#### 2.5. 有識者検討委員会の設置及び運営の概要

中小基盤の課題等について検討を行うため、サイバーセキュリティの有識者、専門家等より構成した有識者検討委員会を設置し、専門的な視点から助言を得た。有識者検討委員会は本調査期間内に3回の会合を開催し、事務局にてその運営を行った。

有識者検討委員会の開催概要と委員名簿について以下に示す。

図表 2-3 有識者検討委員会の開催概要

会合	開催日時	開催方法	審議事項
第1回 会合	2021年10月14日(木) 10:00～12:00	Web会議に よる開催	<ul style="list-style-type: none"> <li>・中小基盤への掲載製品等の公募の進め方について</li> <li>・登録申請書及び申請受付マニュアルについて</li> </ul>
第2回 会合	2021年11月15日(月) 10:00～12:00	Web会議に よる開催	<ul style="list-style-type: none"> <li>・中小基盤への掲載製品・サービス公募の応募状況と掲載方針に関して</li> <li>・中小基盤の仮設サイトの画面イメージについて</li> <li>・中小基盤の有用性評価アンケートの実施について</li> </ul>
第3回 会合	2022年2月7日(月) 13:00～15:00	Web会議に よる開催	<ul style="list-style-type: none"> <li>・試行環境調査並びに市場調査結果報告について</li> <li>・中小基盤の有用性評価と構築上の課題の洗い出し結果について</li> </ul>

＜有識者検討委員会 委員名簿＞ (敬称略)

【座長】

森井 昌克 神戸大学大学院工学研究科 教授

【委員】 (五十音順)

岩本 真人 特定非営利活動法人日本ネットワークセキュリティ協会  
中小企業支援施策 WG リーダー

押田 誠一郎 独立行政法人中小企業基盤整備機構 経営支援部長

佐藤 健志 日本商工会議所 情報化推進部長

手塚 悟 慶應義塾大学 環境情報学部 教授

宮下 清 一般社団法人日本情報システム・ユーザー協会 主席研究員

【オブザーバー】

経済産業省 商務情報政策局 サイバーセキュリティ課

独立行政法人情報処理推進機構 セキュリティセンター 企画部 中小企業支援グループ

### 3. 試行環境調査の結果

#### 3.1. 登録申請様式及び申請受付マニュアルの作成

中小企業向け製品・サービス公募の準備作業として、登録申請様式及び申請受付マニュアルを作成した。

##### 3.1.1. 登録申請様式の作成

登録申請様式については、「登録申請書」と「中小企業ユーザーによる製品等の評価情報提出用紙」の2つの様式を作成した。

###### (1) 登録申請書

登録申請書のファイル(Excel ファイル)は、「応募用紙①」、「応募用紙②」、「応募用紙①を回答する前にお読みください」、「応募用紙②を回答する前にお読みください」の4つのシートにより構成した。

応募用紙①は、応募者情報、中小企業向けセキュリティ製品・サービスに関する情報といった基本情報を収集するとともに、応募資格の確認を行うための様式として位置付けて作成した。このうち、製品・サービスに関する情報については、製品・サービスの特徴やメリットを中小企業に分かりやすく伝え、中小企業にとって活用しやすいものとするため、製品・サービス名称、技術概要(①実現できること(解決すべき課題、対応する脅威等)、②適用環境・適用シーン、③一般的な製品等との違い、④ユーザーの関わり方、⑤自社サイトの関連ページのURL)、ビジネス概要(①ターゲット顧客の特徴、②導入時・運用時に要する費用、③導入実績、④ユーザーサポート体制、⑤自社サイトの関連ページのURL)といった情報を収集した。

応募用紙②は、令和元年度の実現可能性調査で作成した、中小企業が製品・サービスを選ぶ際に参考となる「評価項目」に沿って、申請者が応募する中小企業向けセキュリティ製品・サービスについて評価した情報を収集するための様式として位置付けて作成した。「評価項目」は、「導入のし易さ」「運用のし易さ」「導入時や運用時に要する費用」「導入や運用における課題の解決」「製品・サービスの効果」「製品・サービスに付帯するオプションサービスその他」という6つの観点とそれらに紐づく23の詳細な評価項目により構成されている。

中小企業が製品・サービスを選ぶ際に参考となる「評価項目」を以下に示す。

図表 3-1 中小企業が製品・サービスを選ぶ際に参考となる評価項目

評価項目の観点	詳細な評価項目
(1) 導入のし易さ	① 大規模なシステム改修の必要性がない
	② 必要となる機能を自由に選択することができる
	③ インストールや設定の手間を省くことができる
	④ 必要最小限の知識でインストールや設定を行うことができる
	⑤ PCのシステムパフォーマンスへの影響が最小限である
	⑥ PCにインストール済みのソフトウェアへの影響が最小限である
	⑦ 本格的に導入する前に、有償、無償を問わず、お試し利用ができる
	⑧ 導入に関してのサポート対応がある
(2) 運用のし易さ	① 運用に関しての専門的な知識が必要ない
	② さまざまな状況に応じたサポートツールがある
	③ 問合せ・相談窓口を設置している
(3) 導入時や運用時に要する費用	① 導入コストが安価である
	② 運用コストが安価である
(4) 導入や運用における課題の解決	① 製品・サービスの性能・スペックについて、客観的な根拠が明示されている
(5) 製品・サービスの効果	① 既知の脅威・インシデントに対応することができる
	② 未知の脅威・インシデントに対応することができる
	③ ユーザ側の人為的なミスや内部不正による脅威・インシデントに対応することができる
(6) 製品・サービスに付帯するオプションサービスその他	① サイバー保険等の補償サービスの利用ができる
	② リスク評価(リスクアセスメント)やコンサルティング等のサポートサービスの利用ができる
	③ インシデント対応等の緊急対応サービスの利用ができる
	④ 勤務時間外対応のサポートサービスの利用ができる
	⑤ ユーザ側に対する教育サービスの利用ができる
	⑥ サービス提供者側で悪用等の悪意がある行動を防止する仕組みがある

「応募用紙①」を回答する前にお読みください」シートは、申請される情報の記載内容の粒度や書きぶり、情報量の同質性を、申請者間で担保できるようにすることを目的として、応募用紙①のうち、技術概要、ビジネス概要について記載例を作成した。

「応募用紙②」を回答する前にお読みください」シートは、令和元年度の実現可能性調査で作成した「評価項目の定義・解説書」「申請時の記載方法の手引書」「中小基盤の活用方法の解説書」の3つのコンテンツの内容と紐づけつつ、各評価項目が申請者に正しく理解され、申請者にとって評価しやすいものとするを目的として、各評価項目で想定される内容例を作成した。

「応募用紙①」、「応募用紙②(一部抜粋)」、「応募用紙①を回答する前にお読みください」、「応募用紙②を回答する前にお読みください(一部抜粋)」の各シートについて、それぞれ以下に示す。

図表 3-2 「応募用紙①」のシート

独立行政法人情報処理推進機構委託事業 「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」 中小企業向けサイバーセキュリティ製品・サービスの提供事業者の公募 応募用紙①															
<p>【応募方法】                  以下の項目にご記入頂き、最下段記載の応募先までにメール添付にてご提出下さい。                  回答欄の大きさは適宜調整頂いて結構です。</p>															
<p><b>1. 応募者情報</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">(1) 事業者名</td><td></td></tr> <tr><td>(2) 担当者(代表者)の氏名</td><td></td></tr> <tr><td>(3) 所属</td><td></td></tr> <tr><td>(4) 役職</td><td></td></tr> <tr><td>(5) 勤務先住所</td><td></td></tr> <tr><td>(6) 電話番号</td><td></td></tr> <tr><td>(7) 電子メール</td><td></td></tr> </table>		(1) 事業者名		(2) 担当者(代表者)の氏名		(3) 所属		(4) 役職		(5) 勤務先住所		(6) 電話番号		(7) 電子メール	
(1) 事業者名															
(2) 担当者(代表者)の氏名															
(3) 所属															
(4) 役職															
(5) 勤務先住所															
(6) 電話番号															
(7) 電子メール															
<p><b>2. 応募される中小企業向けサイバーセキュリティ製品・サービスに関する情報</b></p> <p>(1) 名称 製品・サービスの名称をご記載下さい。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="height: 20px;"></td></tr> </table>															
<p>(2) 技術概要</p> <p>製品・サービスの技術面の特徴が明確に分かるように、概要（①何を実現するための製品・サービスであるか、②どのような利用環境やシーンに適用できるか、③一般的な製品・サービスとの違いが何か、④ベンダーやディストリビューターの手を借りずにユーザー自身で導入・運用ができるか等）を簡潔にまとめて下さい。別途補足資料がある場合は、応募時にメール添付を、また自社サイトに関連ページがある場合は、URLの記載をお願い致します。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">①実現できること（解決すべき課題、対応する脅威等）</td><td></td></tr> <tr><td>②適用環境・適用シーン</td><td></td></tr> <tr><td>③一般的な製品等との違い</td><td></td></tr> <tr><td>④ユーザーの関わり方</td><td></td></tr> <tr><td>⑤自社サイトの関連ページのURL</td><td></td></tr> </table>		①実現できること（解決すべき課題、対応する脅威等）		②適用環境・適用シーン		③一般的な製品等との違い		④ユーザーの関わり方		⑤自社サイトの関連ページのURL					
①実現できること（解決すべき課題、対応する脅威等）															
②適用環境・適用シーン															
③一般的な製品等との違い															
④ユーザーの関わり方															
⑤自社サイトの関連ページのURL															
<p>(3) ビジネス概要</p> <p>製品・サービスのビジネス面の特徴が明確に分かるように、概要（①ターゲット顧客の特徴（業種、従業員規模等）、②導入時や運用時に要する費用（初期費用、ランニング費用）、③導入実績、④ユーザーサポート体制等）を簡潔にまとめて下さい。別途補足資料がある場合は、応募時にメール添付を、また自社サイトに紹介ページがある場合は、URLの記載をお願い致します。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">①ターゲット顧客の特徴</td><td></td></tr> <tr><td>②導入時・運用時に要する費用</td><td></td></tr> <tr><td>③導入実績</td><td></td></tr> <tr><td>④ユーザーサポート体制</td><td></td></tr> <tr><td>⑤自社サイトの関連ページのURL</td><td></td></tr> </table>		①ターゲット顧客の特徴		②導入時・運用時に要する費用		③導入実績		④ユーザーサポート体制		⑤自社サイトの関連ページのURL					
①ターゲット顧客の特徴															
②導入時・運用時に要する費用															
③導入実績															
④ユーザーサポート体制															
⑤自社サイトの関連ページのURL															
<p><b>3. 応募資格の確認</b></p> <p>(1) 公募要領の2. 応募資格①～③について該当していますか。該当するものに○印をご記入ください。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 70%;">①中小企業向けサイバーセキュリティ製品・サービスを提供している事業者であるか</td><td></td></tr> <tr><td>②本事業が対象とする試行対象製品・サービス分野のサイバーセキュリティ製品・サービスを提供している事業者であるか</td><td></td></tr> <tr><td>③本事業の実施に係る規約に遵守し、規約で定める同意書の提出が可能な事業者である</td><td></td></tr> </table> <p>(2) 公募要領の3. 実施内容の(1)～(2)について実施することは可能ですか。実施可能なものに○印をご記入ください。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 70%;">①中小企業ユーザーによる申請されたサイバーセキュリティ製品・サービスの評価情報の提出</td><td></td></tr> <tr><td>②本事業における各種情報提供等への協力</td><td></td></tr> </table>		①中小企業向けサイバーセキュリティ製品・サービスを提供している事業者であるか		②本事業が対象とする試行対象製品・サービス分野のサイバーセキュリティ製品・サービスを提供している事業者であるか		③本事業の実施に係る規約に遵守し、規約で定める同意書の提出が可能な事業者である		①中小企業ユーザーによる申請されたサイバーセキュリティ製品・サービスの評価情報の提出		②本事業における各種情報提供等への協力					
①中小企業向けサイバーセキュリティ製品・サービスを提供している事業者であるか															
②本事業が対象とする試行対象製品・サービス分野のサイバーセキュリティ製品・サービスを提供している事業者であるか															
③本事業の実施に係る規約に遵守し、規約で定める同意書の提出が可能な事業者である															
①中小企業ユーザーによる申請されたサイバーセキュリティ製品・サービスの評価情報の提出															
②本事業における各種情報提供等への協力															

図表 3-3 「応募用紙②」のシート(一部抜粋)

独立行政法人情報処理推進機構委託事業 「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」 中小企業向けサイバーセキュリティ製品・サービスの提供事業者の公募 応募用紙②	
【応募方法】 以下の項目にご記入頂き、最下段記載の応募先までにメール添付にてご提出下さい。 回答欄の大きさは適宜調整頂いて結構です。	
<h3>1. 導入のし易さ</h3>	
<b>① 導入にあたってのシステム改修の必要性</b>	
製品・サービスの導入時に、既に運用しているシステム改修の必要がある場合は、システム改修の対応内容及び範囲を選択すること	
(1) 導入時のシステム改修の有無について、該当するものを選んでお答えください (プルダウンより選択)	
(2) システム改修がある場合の内容・範囲について、該当するものを選んでお答えください (該当に☑)	
a. システムを構成するプログラムやデータベース、端末、ネットワークに関わる改修	<input type="checkbox"/>
b. 機能追加や画面・帳票変更に関わる改修	<input type="checkbox"/>
c. 他組織のシステムとの連携に関わる改修	<input type="checkbox"/>
d. その他の改修 その他の改修があるとお答えになられた場合、具体的な内容を下の自由記載欄にご記入ください	<input type="checkbox"/>
<b>② 製品・サービスに含まれる機能</b>	
以下に示す機能について、製品・サービスの提供上の位置づけを記載すること	
(1) 以下に示す機能のうち、製品・サービスとしての提供内容に含まれている機能を選んでお答えください (該当に☑)	
a. 設定代行	<input type="checkbox"/>
b. 顧客要件に基づくカスタマイズ(サービス構成変更・設定変更等)	<input type="checkbox"/>
c. セキュリティに関する問い合わせ・相談窓口対応	<input type="checkbox"/>
d. 検出された脅威の駆除や回復作業	<input type="checkbox"/>
e. 管理コンソール・管理ツールの提供	<input type="checkbox"/>
f. 定期的なレポート発行(アラート数・検出数等)	<input type="checkbox"/>
g. その他の機能 その他の機能があるとお答えになられた場合、具体的な内容を下の自由記載欄にご記入ください	<input type="checkbox"/>
h. 上記の機能のうち、製品・サービスとしての提供内容に含まれている機能はない	<input type="checkbox"/>
(2) 以下に示す機能のうち、製品・サービスとしての提供内容に含まれていないが、オプション選択で利用可能である機能を選んで、お答えください (該当に☑)	
a. 設定代行	<input type="checkbox"/>
b. 顧客要件に基づくカスタマイズ(サービス構成変更・設定変更等)	<input type="checkbox"/>
c. セキュリティに関する問い合わせ・相談窓口対応	<input type="checkbox"/>
d. 検出された脅威の駆除や回復作業	<input type="checkbox"/>
e. 管理コンソール・管理ツールの提供	<input type="checkbox"/>
f. 定期的なレポート発行(アラート数・検出数等)	<input type="checkbox"/>
g. その他の機能 その他の機能があるとお答えになられた場合、具体的な内容を下の自由記載欄にご記入ください	<input type="checkbox"/>
h. 上記の機能のうち、製品・サービスとしての提供内容に含まれていないが、オプション選択で利用可能である機能はない	<input type="checkbox"/>

図表 3-4 「応募用紙①を回答する前にお読みください」のシート

**応募用紙①を回答する前にお読みください**

応募用紙にご記入いただく回答については、**出来る限り具体的、かつ分かりやすい書きぶり、記入をお願いいたします。**記入例を以下に示しますので、ご参考ください。

<p>(2) 技術概要</p> <p>製品・サービスの技術面の特徴が明確に分かるように、概要（①何を実現するための製品・サービスであるか、②どのような利用環境やシーンに適用できるか、③一般的な製品・サービスとの違いが何か等）を簡潔にまとめて下さい。別途補足資料がある場合は、応募時にメール添付を、また自社サイトに関連ページがある場合は、URLの記載をお願いします。</p>	
①実現できること（解決すべき課題、対応する脅威等）	<p><b>【記入例】</b></p> <p>進化するランサムウェア攻撃の脅威から組織の貴重な情報資産を守るため、各階層を連携させた多層防御のアプローチと、AI・機械学習を用いた脅威検出、検出時のネットワーク分離・遮断、バックアップデータのクラウドストレージへの保管による保護により、高度なランサムウェア攻撃を防御する対策ソリューションである。</p>
②適用環境・適用シーン	<p><b>【記入例】</b></p> <p>JavaScriptとCookieが動作するWebブラウザ（対応ブラウザはMicrosoft Internet Explorer, Google Chrome, Mozilla Firefoxの3種類）から閲覧・編集可能なオープンソースのCMSに適用できる。CMSの脆弱性を狙った攻撃に対して不安があり、セキュリティを強化したいユーザーにお勧めのセキュリティ対策製品である。</p>
③一般的な製品等との違い	<p><b>【記入例】</b></p> <p>これまでのウイルス対策ソフトやUTMでは検知できず、システム内部への侵入を許してしまった脅威に対して、複数の異なるエンドポイントで取得した各種ログデータをサーバ上に集約し、相互のアクティビティを関連付けて分析することで、脅威の存在をいち早く検知し、除去する対策を提供できるEDRソリューションである。</p>
④ユーザーの関わり方	<p><b>【記入例】</b></p> <p>製品の導入にあたっては、ベンダーの支援のもと、ユーザーにPoC（Proof of Concept）開発を通じてトライアル導入を行っていただいた上で、ベンダーと一緒に適切な検知ポリシーを決めたり、適切なチューニング作業を行っていただく必要がある。他方、運用時には、製品に実装された機械学習機能が、通知ポリシーの見直しや再設定に関わるチューニング作業を行うため、ユーザーに何も作業を行っていただく必要はない。</p>
<p>(3) ビジネス概要</p> <p>製品・サービスのビジネス面の特徴が明確に分かるように、概要（①ターゲット顧客の特徴（業種、従業員規模等）、②導入時や運用時に要する費用（初期費用、ランニング費用）、③導入実績、④ユーザーサポート体制等）を簡潔にまとめて下さい。別途補足資料がある場合は、応募時にメール添付を、また自社サイトに紹介ページがある場合は、URLの記載をお願いします。</p>	
①ターゲット顧客の特徴	<p><b>【記入例】</b></p> <p>幅広い業種に適用可能である。特に全業種の中で比較的多く導入が進んでいるのが、機密性の高い情報や個人情報を扱っている医療分野の常勤スタッフ5名以下の診療所や薬局である。</p>
②導入時・運用時に要する費用	<p><b>【記入例】</b></p> <p>初期費用は無料で、月額3,000円/台のランニング費用で利用可能である。契約はライセンス契約となり、ランニング費用には、インシデント発生時の調査・分析（フォレンジック調査、マルウェア解析等）費用以外のログ収集・監視費用や脅威アラート通知費用、初期対応費用などが含まれる。</p>
③導入実績	<p><b>【記入例】</b></p> <p>国内を中心に、3,000社を超える企業に導入されている。約80%のお客は、セキュリティ予算の限られている中小企業であり、コロナ禍においてテレワーク環境を利用し始めたことをきっかけに導入し、リスクの軽減や攻撃の抑え込みに役立っている。</p>
④ユーザーサポート体制	<p><b>【記入例】</b></p> <p>複数のチャネル（Webフォーム入力、電話、電子メール、チャット）による問い合わせを受け付ける窓口を設置しており、24時間受付可能で、年中無休（午前9時～午後5時に回答）のユーザーサポート対応を実施している。</p>

図表 3-5 「応募用紙②を回答する前にお読みください」のシート(一部抜粋)

応募用紙②を回答する前にお読みください				
応募用紙②でご記入いただく各項目は、独立行政法人情報処理推進機構（IPA）が令和元年度の「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査」において取りまとめた、 <b>中小企業向けサイバーセキュリティ製品・サービスに関する評価項目が元になっています。</b> 回答にあたっては、以下に示す、「 <b>評価項目の定義・解説</b> 」、「 <b>申請時の記載上の留意すべき点</b> 」、「 <b>想定する内容の一例</b> 」を参考にしつつ、 <b>出来る限り具体的、かつ分かりやすい書きぶり</b> で、記入をお願いいたします。				
中小企業向けサイバーセキュリティ製品・サービスに関する評価項目				
評価項目の観点	詳細な評価項目	評価項目の定義・解説	申請時の記載上の留意すべき点	想定する内容の一例
(1) 導入のし易さ	① 大規模なシステム改修の必要性がない	サイバーセキュリティ製品・サービスを導入する際に、既に運用している自社のシステムの改修が生じる場合には、追加のシステム投資が必要となり、コストの負担増が避けられない状況となるため、中小企業の経営層は、導入決断を見送りがちである。また、中小企業の担当者においても、自社のシステム改修は、新たな脅威の呼び込みにつながる恐れがあることに加えて、社内の承認プロセスにおいて、関係部署との調整等の煩雑な手続きが必要となり、時間や労力を費やすことが求められるため、敬遠されがちである。このように、中小企業においては、サイバーセキュリティ製品・サービスを導入する際に、大規模なシステム改修の必要性がないことが求められる。	必要となるシステム改修の対応内容・範囲から、システム改修の規模がどの程度であるかを判断できるように申請時に記載する必要がある。 必要となるシステム改修の対応内容・範囲の例を以下に示す。 ○システムを構成するプログラムやデータベース、端末、ネットワークに関わるシステム改修 ○機能追加や画面・帳票変更に関わるシステム改修 ○他組織のシステムとの連携に関わるシステム改修 ○その他のシステム改修	<b>導入にあたってのシステム改修の必要性</b> 【例①】 専用機器を設置することなく、インターネット経由によるクラウドサービスの形態で、専用機器が提供する同じ機能をサービスとして提供しているため、企業のネットワーク構成の変更が不要である。  【例②】 ソフトウェアベースで動作し、環境を選ばず、既存のデバイスやプラットフォームにソフトウェアをアドオンするだけで、ネットワーク接続を自動的に確立し利用できるようになるため、アプリケーションの改修が不要である。
	② 必要となる機能を自由に選択することができる。	機能のオーバースペックによる費用負担の増大は、中小企業がサイバーセキュリティ製品・サービスの導入を推進するうえで、制約要因となることが懸念される。従って、必要となる機能については、使う機能を必要最小限に絞り込んだり、オーバースペックによる無駄な機能を省いたりすることが避けられない状況となる。また、必要となる機能が必要ときにオプションで選択できるようになっているなど、費用の削減効果によって、投資を判断する傾向にあるため、中小企業においては、サイバーセキュリティ製品・サービスを導入する際に、現場の事情に合わせて、必要となる機能を自由に選択することができることが求められる。	必要となる機能については、中小企業によって目的や考え方が異なることから、大分類に沿って申請時に記載する必要がある。 必要となる機能の大分類の例を以下に示す。 ○セキュリティをより一層高めるための対策に関わる機能 ○データや設定、操作の管理に関わる機能 ○アラートやログ情報等の情報提供に関わる機能 ○その他の機能	<b>製品・サービスに含まれる機能</b> 【例①】 デバイスの状態を確認したいIT担当者向けに、デバイスに関する詳細情報や設定情報、操作情報等を一元的に管理し、監視もできる管理コンソールを、オプションで提供している。  【例②】 ファイルサーバーへのアクセスでは、ログの監視を通じて、いつ、誰が、何のファイルを開覧したかを把握できるとともに、経営層への報告が必要なIT担当者向けに、アクセス記録に関する月次レポートをオプションで提供している。
	③ インストールや設定の手間を省くことができる	インストール・設定作業の負担を重視する中小企業の担当者にとって、サイバーセキュリティ製品・サービスの導入を決定する大きな要因は、必要となるソフトウェア等のインストールに要する時間をどれだけ短縮できるかや、必要となる設定項目数をどれだけ削減できるかに掛かっているため、インストールに要する時間が長かったり、いろいろと細かい設定を求められたりするサイバーセキュリティ製品・サービスは、敬遠されがちである。このようなインストールに要する時間の短縮や必要となる設定項目数の削減を含めて、中小企業においては、サイバーセキュリティ製品・サービスを導入する際に、インストールや設定の手間を省くことができることが求められる。	必要となる設定の対応内容・範囲から、設定の手間がどの程度であるかを判断できるように申請時に記載する必要がある。 必要となる設定の対応内容・範囲の例を以下に示す。 ○利用者・管理者の登録や管理権限に関わる設定 ○システム・ネットワーク環境、データ管理等のセキュリティポリシーに関わる設定 ○性能や安定性を向上するためのチューニングに関わる設定 ○その他の設定 また、PC 1 台当たりのインストールに要する時間や必要となる設定項目数といった定量的な情報についてもできる限り申請時に記載する必要がある。	<b>ユーザーが行うインストール・設定作業の対応内容・範囲</b> 【例①】 使用環境により状況が異なるため、インストールが完了するまでに5分～10分程度の時間がかかる場合がある。  【例②】 インストール後の初期設定では、提供する2つの機能に対応した計5つの項目を設定するだけで、すぐに使用できるようになる。



(2) 中小企業ユーザーによる製品等の評価情報提出用紙

中小企業ユーザーによる製品等の評価情報提出用紙のファイル (Excel ファイル) は、製品・サービス選びを行う中小企業にとって、製品・サービスを導入済みの企業による評価情報が有益な情報となるため、「製品・サービスを選定する際に重視した評価項目とその具体的な内容」、「製品・サービスを利用する上でメリットを感じた評価項目とその具体的な内容」の2点に関して、製品・サービスを実際に導入している中小企業ユーザーから評価情報を収集するための様式として位置付けて作成した。

今回の試行環境調査においては、中小基盤の仮設サイトへの掲載申請者が、応募する中小企業向けセキュリティ製品・サービスについて、既に導入済みの中小企業ユーザーから2社を選択して評価情報の提出を行った。

図表 3-6 中小企業ユーザーによる製品等の評価情報提出用紙(一部抜粋)

独立行政法人情報処理推進機構委託事業 「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」 中小企業向けサイバーセキュリティ製品・サービスの提供事業者の公募 中小企業ユーザーによる製品等の評価情報提出用紙				
【提出方法】 以下の項目にご記入頂き、最下段記載の応募先までにメール添付にてご提出下さい。 回答欄の大きさは適宜調整頂いて結構です。				
<b>1. 中小企業ユーザーに関する情報</b>				
(1) 事業者名				
(2) 担当者(代表者)の氏名				
(3) 所属				
(4) 役職				
(5) 勤務先住所				
(6) 電話番号				
(7) 電子メール				
<b>2. 導入している中小企業向けサイバーセキュリティ製品・サービスに関する評価情報</b>				
※回答する前に、別シートの「(参考)評価項目の観点、詳細な評価項目に関する解説」を必ずお読みください。また、必要に応じて、解説に記載されている、「想定する内容の一例」等をご確認ください。				
<b>(1) 当該製品・サービスを選定する際に重視したポイント</b>				
貴社においては、導入製品・サービスの選定時において、何を重視しましたか。以下に示す評価項目の中から、あてはまるものを選んで、○を付けてください。(複数回答可) また、○を付けた評価項目について、貴社が重視した具体的な内容をお知らせください。(自由記述) ※重視した内容については、理由・背景や、評価のポイント(他社製品・サービスと比較したときの優位性等)を含めて、具体的に記述してください。				
評価項目の観点	詳細な評価項目	重視した項目 回答欄 (複数回答可)		重視した具体的な内容 回答欄 (自由記述)
A. 導入のし易さ	1. 大規模なシステム改修の必要性がない		⇒	
	2. 必要となる機能を自由に選択することができる		⇒	
	3. インストールや設定の手間を省くことができる		⇒	
	4. 必要最小限の知識でインストールや設定を行うことができる		⇒	
	5. PCのシステムパフォーマンスへの影響が最小限である		⇒	
	6. PCにインストール済みのソフトウェアへの影響が最小限である		⇒	
	7. 本格的に導入する前に、有償、無償を問わず、お試し利用ができる		⇒	
	8. 導入に関するサポート対応がある		⇒	
B. 運用のし易さ	9. 運用に関する専門的な知識が必要ない		⇒	
	10. さまざまな状況に応じたサポートツールがある		⇒	
	11. 問合せ・相談窓口を設置している		⇒	
C. 導入時や運用時に要する費用	12. 導入コストが安価である		⇒	
	13. 運用コストが安価である		⇒	



ファイルの再提出を求める内容の電子メールを送信する。

### ③応募資格等の確認

- 登録申請書の申請内容をもとに、公募要領に定める、応募資格への該当性や、実施内容への協力の可否について確認を行う。
- 該当性を確認する応募資格を、以下に示す。
  - 中小企業向けサイバーセキュリティ製品・サービスを提供している事業者であるか
    - ✓ サイバーセキュリティサービスに関しては、サイバーセキュリティ製品と紐づく付帯的なサービスを想定する。よって、セキュリティコンサルティングサービスやセキュリティ監査サービスなど製品と紐づかないサービスは対象外とする。
  - 本事業が対象とする試行対象製品・サービス分野のサイバーセキュリティ製品・サービスを提供している事業者であるか
    - ✓ 試行対象製品・サービス分野としては、A. インシデント発生時の迅速な初動対応（セキュリティ監視製品（UTM、IDS等））、B. 重要な情報の安全な取扱い（重要情報の保護に関する製品（認証、暗号等））、C. 不正プログラム対策（エンドポイントセキュリティ製品（EDR等））の3分野を想定する。
    - ✓ 一般に幅広く普及している製品・サービス（ウイルス対策ソフトなど）は対象外とする。加えて、部品・モジュール的に運用されている製品・サービスについても、対象外とする。
  - 本事業の実施に係る規約を遵守し、規約で定める同意書の提出が可能な事業者であるか
- 協力の可否を確認する実施内容を、以下に示す。
  - 申請されたサイバーセキュリティ製品・サービスを既に導入している中小企業ユーザー（2ユーザー以上）において、申請されたサイバーセキュリティ製品・サービスの評価や、当該評価情報の提出（採択通知後1週間以内の提出）への協力が得られるか
  - 申請されたサイバーセキュリティ製品・サービスの情報の提出や、中小企業ユーザーによる評価情報の中小基盤への掲載、必要に応じて、申請されたサイバーセキュリティ製品・サービスに関する追加的な情報の提出を含め、本事業における各種情報提供等への協力が得られるか
- 応募資格（試行対象製品・サービス分野の製品・サービスであるかを含む）への該当性が認められない申請者（製品・サービスベンダー）や、実施内容への協力が得られない申請者（製品・サービスベンダー）については、後述す

る評価項目に沿った提供情報の確認を行わない。

#### ④評価項目に沿った提供情報の確認

- 申請された登録申請書の記載内容をもとに、中小企業に対する提供情報としての有用性を評価する。
- 有用性を評価する際の視点を、以下に示す。
  - 各評価項目に沿って申請された内容が、評価項目の定義・解説や、申請時の記載上の留意すべき点で示した内容や考え方に沿ったものであるか
  - 各評価項目に沿って申請された内容の記載のレベルや書きぶりが、適正かつ具体的であるか
  - 各評価項目に沿って申請された内容が、中小企業に対する提供情報として十分有用であるか
  - 各評価項目で想定する機能や特徴以上に、中小企業におけるセキュリティ対策の普及促進やセキュリティレベルの向上に繋がるものとしてPRするものがあるか
- 各評価項目に沿って申請された内容を、上記の4つの視点から評価し、該当する場合は1点を付与する。総合点の高いものから順に、掲載製品等の選定に向けた意見収集の対象とする候補製品・サービスを、3分野9製品以上という条件に合うように選定する。

#### ⑤掲載製品等の選定に向けた意見収集

- 有識者検討委員会に対し、試行対象製品・サービス分野の偏りがないように、中小基盤に登録・掲載する製品・サービスを3分野9製品・サービス以上選定することを目的として、掲載製品等の選定に向けた意見収集を依頼する。
- 有識者検討委員会による意見収集においては、事務局から評価項目に沿った提供情報の確認結果を提示するとともに、申請者（製品・サービスベンダー）との質疑応答を行う機会を設けることにより、評価項目に沿った提供情報の確認結果に関する補足情報や、各製品・サービスに関する参考情報を提供する。

#### ⑥採択（最終判断）と確認結果の通知

- 有識者検討委員会において収集された掲載製品・サービスの選定に向けた意見をもとに、中小基盤への登録・掲載の可否を最終判断し、採択を行う。
- 採択された各製品・サービスを提供する申請者（製品・サービスベンダー）

(以下、「採択者」という。)を含め、すべての申請者に対して、電子メールにより確認結果を通知する。

- 採択者に対して、確認結果の通知メールの中で、同意書の提出を求める。

#### ⑦同意書の提出・受領

- 採択者から電子メールを使って送信・提出された同意書の電子ファイルを受領する。
- 同意書の電子ファイルの受領後は、採択者に対し、同意書を受領した旨を通知する電子メールを送信する。
- 提出された同意書について、同意書の記載に間違いがないことや、組織全体の代表者または試行環境調査に係る規約への同意を承認し決裁する責任者による押印があることを確認する。
- 不備が見つかった場合は、採択者に対して、その旨を説明し、同意書の電子ファイルの再提出を求める内容の電子メールを送信する。

#### ⑧登録内容（掲載情報）の調整

- 登録申請書を通じて提出された提供情報について、中小企業ユーザーにとって更に有用な情報とするために改善すべき内容(内容の具体化、内容の補充、適切な表現への修正等)がないかを確認する。
- 必要に応じて、採択者と調整しつつ、中小基盤への登録・掲載内容の改善のために必要な追加情報の提出を求める。

#### ⑨追加情報の提出

- 事務局からの求めに応じた採択者から、電子メールを使って送信・提出された追加情報の電子ファイルを受領する。
- 追加情報の電子ファイルの受領後は、事務局からの求めに応じた採択者に対し、追加情報を受領した旨を通知する電子メールを送信する。

#### ⑩中小基盤への提供情報の登録

- 上記の⑧の調整や⑨の追加情報の提出を経て、中小基盤への登録・掲載内容を確定させる。
- 中小基盤への登録・掲載内容の確定後、中小基盤への登録・掲載内容について、採択者の承諾を得る。
- 採択者と事務局の双方で合意した中小基盤への登録・掲載内容をもとに、中小基盤への登録(仮設サイトへの掲載)を行う。

## 3.2. 中小企業向け製品・サービスの公募の試行実施

中小基盤に掲載する中小企業向け製品・サービスに関する情報を収集するため、中小企業向け製品・サービス公募を試行的に実施した。

### 3.2.1. 試行対象製品・サービスの公募

最初に、中小企業向け製品・サービス公募のお知らせを掲載するためのホームページを作成した。また、当該ホームページから、申請者が以下に示す必要書類のファイルをダウンロードできるようにした。

- (1) 登録申請書
- (2) 中小企業ユーザーによる製品等の評価情報提出用紙
- (3) 公募要領
- (4) 本事業の実施に係る規約
- (5) 質問状

中小企業向け製品・サービス公募にあたって、公募期間、応募資格、実施内容、応募手続き、選定方法、通知方法の他、留意事項、質問事項、応募先及び問合せ先を含め、それらを定めた公募要領を作成した。

加えて、実施内容が適切に行われることを担保するため、本事業の実施に係る規約を作成するとともに、申請者が当該規約に同意していることを確認するための同意書を作成した。

公募期間内に13社より13製品・サービスの応募があった。この数には、中小企業向け製品・サービスを提供するベンダーに対する個別の応募協力依頼による応募も含まれる。

個別の応募協力依頼を実施する中で聞かれた中小企業向け製品・サービス公募に協力できない製品・サービスベンダーの主な理由としては、以下の3つの理由が挙げられている。

- (1) 申請者の業務が忙しく時間が取れない。
- (2) 営業担当者との調整が時間的に間に合わない。
- (3) 公募要領が規定する採択後1週間での中小企業ユーザーによる製品等の評価情報の提出が困難である。

上記を踏まえると、製品・サービスベンダー側の時間的な制約が想定以上に大きいことが分かる。このため、公募期間、申請情報の提出期間については、十分な余裕を持って期間を設定することが必要になると考えられる。

また、応募があった製品・サービスベンダーからの登録申請書の申請を受け付けた後、申請受付マニュアルにおいて規定した、「申請の不備等の形式的な確認」、「応募資格等の確認」、「評価項目に沿った提供情報の確認」の3つのプロセスを実行した。

申請の不備等の形式的な確認では、導入時・運用時に要する費用について具体的な記載がないという1件の不備が確認された。費用の多寡によっては中小企業向け製品・サービスであるかどうかの疑義が生じる可能性があるため、ベンダーに確認を行い、当該費用はリーズナブルであり、情報提供についても問題がないことを確認した。

応募資格等の確認では、中小企業ユーザーによる製品等の評価情報の提出について、提供元が販売パートナーであるため該当しないとの記載があり、1件の不備が確認された。当該ベンダーに確認を行い、ベンダー側において販売パートナーと連携することにより、中小企業ユーザーによる製品等の評価情報の提出が可能であり、応募資格への該当性に関して問題がないことを確認した。

評価項目に沿った提供情報の確認では、申請される情報の記載の粒度や書きぶり、情報量の高質性をベンダー間で担保できるよう、登録申請書の記載例や各評価項目で想定する内容の例を作成したが、高質性の差についてはベンダー間で大きな開きがあった。

### 3.2.2. 試行対象製品・サービスの選定

応募があった13社13製品・サービスの中から、中小基盤に掲載する製品・サービスを選定した。

公募要領において、試行対象製品・サービス分野3分野から9製品・サービス以上を採択することについて規定しているところ、当初想定していたような、応募多数による採択製品・サービスの絞り込みが特に必要な状況が発生していない点を踏まえ、応募があった13社13製品・サービスすべてを、中小基盤に掲載する製品・サービスとして選定した。

なお、応募があった13社13製品・サービスを、中小基盤に掲載する製品・サービスとして選定するにあたり、その内容を有識者検討委員会に諮問し、意見を収集した上で、特段の問題点の指摘がないことを確認した。

上記を踏まえて、中小基盤に掲載する製品・サービスのベンダー13社に対して電子メールにて通知するとともに、公募要領が規定する採択後1週間での中小企業ユーザーによる製品等の評価情報の提出と、同意書の提出を求めた。

その結果、13社のうち1社が、中小企業ユーザーによる製品等の評価情報提出用紙に基づく評価情報の提出が難しい状況となったため、採択の取消しを行った。また、12社より同意書の提出を受け、不備がないことを確認した。

最終的に中小基盤に掲載する製品・サービスとして採択した 12 社 12 製品・サービスを以下に示す。

図表 3-8 中小基盤に掲載する製品・サービスとして採択した 12 社 12 製品・サービス

採択ベンダー		製品・サービス名称	製品・サービス概要
①	株式会社網屋	ALog シリーズ製品	IT システムのログを包括的に管理・活用することで、サイバー攻撃や内部不正から情報資産を守る統合ログ管理ソリューション
②	株式会社フーバーブレイン	Eye “247” AntiMalware USAVIV	ランサムウェアや他の外部からの脅威から企業の情報資産を守るための多層防御型のセキュリティ対策ソリューション
③	株式会社ハンモック	AssetView	セキュリティの入口対策・内部対策・出口対策（多層防御）を実現し、IT 資産の統合管理を行うトータルクライアントソリューション
④	バラクーダネットワークスジャパン株式会社	Barracuda Web Application Firewall/Barracuda WAF-as-a-Service	「Web アプリケーションの脆弱性を悪用した攻撃」から Web サイトを保護するセキュリティ対策ソリューション
⑤	トレンドマイクロ株式会社	Cloud Edge	企業ネットワークの入り口に設置することで、多様な脅威からユーザーの環境を保護する UTM 製品
⑥	デジタルアーツ株式会社	i-FILTER@Cloud	Web フィルタリング、標的型攻撃対策、内部情報漏えい対策に対応した製品
⑦	株式会社テクノル	MRB-cloud	インターネットに向けた通信をすべて監視して、危険なサイトに近づかないように防御する UTM 製品
⑧	株式会社クイリー	Llave（ジャーベ）	PC 端末、外部デバイス内の機密データのほか、ファイルサーバやクラウドストレージサービスなどに保管された共有データファイルを、簡単操作で暗号化できる製品
⑨	ウォッチガード・テクノロジー・ジャパン株式会社	WatchGuard Firebox アプライアンス	企業ネットワークのインターネット境界で、入口対策及び出口対策機能を実装した、多層防御を実現し、サイバー攻撃に備えるためのセキュリティアプライアンス製品
⑩	MS&AD インターリスク総研株式会社	防検サイバー	高度なサイバー攻撃への対策運用を実現するための管理セキュリティサービス付きの EDR 製品



⑪	eGIS 株式会社	セキュリティドクター	PC に侵入した脅威を「検知」し、「アラート」を提供し、脅威を「ハンティング」する、「EDR」 + 「EDR 運用サービス」
⑫	株式会社 Blue Planet-works	AppGuard	エンドポイントに対する不正ソフトウェア又は不正アクセスを用いたすべての攻撃に対応した製品

### 3.2.3. 中小基盤への登録申請

中小基盤に掲載する製品・サービスを選定するプロセスの中で、申請受付マニュアルに従い、登録申請書の申請を受け付け、申請内容の確認を行うとともに、申請内容に不備があるベンダーに対して、内容の確認や、採択の取消しによる必要な対応を行った。

前述したとおり、最終的に採択した製品・サービスベンダー12社から、中小企業ユーザーによる製品等の評価情報提出用紙に基づき、1製品・サービスあたり2ユーザーから評価情報の提出を受けた。

## 3.3. 中小基盤の構築と製品・サービス情報の掲載

選定・採択した製品・サービスに関する情報や、中小企業ユーザーによる製品・サービスの評価情報を HTML 形式でコンテンツ化し掲載した中小基盤の仮設サイトを構築した。

また、中小基盤の仮設サイトには、ページビュー数や各製品・サービスに関する情報へのアクセス数、各検索条件による検索回数等の記録分析ができるように必要となるログを収集する機能や、ファイアウォール、ウェブアプリケーションファイアウォール(WAF)、ウイルス対策ソフトの導入・運用や、ドメイン認証、自動バックアップ等の必要なセキュリティ対策機能を実装した。

### 3.3.1. 仮設サイトの構築

中小基盤の仮設サイトのホームページ構成を以下に示す。

#### (1) フロントページ（「サイトの説明」のトップページ）

フロントページにおいては、「本事業紹介・サイト紹介」に関する情報を掲載し、中小企業が、試行環境調査や、中小基盤の仮設サイトに関する取組について内容を理解できるよう、イラストや文章を用いて分かりやすく解説した。

また、フロントページを表す「サイトの説明」というタブの他、中小企業の利用目的に合わせて効率的なサイト閲覧を可能とするため、「検索」、「製品・サービス紹介」、「アンケート」をタブメニューとして設定し、タブごとに表示内容を変更でき

るようにした。

その他にも、フロントページ上で「注目ワード」による検索機能を提供した。「注目ワード」を用いた検索では、近年、サプライチェーンの業務・開発・製造現場において、「ランサムウェア攻撃」の被害が拡大している点や、新型コロナウイルス感染症対策やDX（デジタルトランスフォーメーション）の推進をきっかけに、中小企業においても、テレワークの利用が拡大し、攻撃を受けるリスクが高まってきている点、さらに中小企業においても個人情報扱う機会が増えており、漏えいに対する不安が高まってきている点について考慮した上で、あらかじめ、「ランサムウェア対策」、「テレワークのセキュリティ対策」、「GDPR（EU一般データ保護規則）への対応」という3つの注目ワードを設定した。

さらに、中小基盤に掲載する各製品・サービスに紐づく注目ワードを設定することにより、中小企業が当該機能を利用して、検索したい注目ワードを選択するだけで、該当する製品・サービスに関する情報に効率よくアプローチできるようにした。

フロントページ（「サイトの説明」のトップページ）の画面を以下に示す。

図表 3-9 フロントページ(「サイトの説明」のトップページ)の画面



本事業紹介・サイト紹介

産業活動においてサプライチェーンリスクの問題が顕在化しつつある昨今、サプライチェーンを構成する中小企業におけるサイバーセキュリティ対策促進が喫緊の課題です。そのような中、市場に流通しているセキュリティ製品・サービスは、中小企業から見て過度に高機能、運用コストが高い等、中小企業のニーズにマッチしていないとの声があります。また、セキュリティ製品・サービスの提供事業者においても、中小企業にも導入できる製品・サービスであるが、導入効果等に関する理解を得にくいため、中小企業に使われていないケースがあります。

そこで、本事業においては、中小企業でも扱いやすい製品・サービス選びの一助となる情報を提供するプラットフォーム（以下、「中小基盤」とする。）の仮設サイトを構築することになりました。中小基盤の仮設サイト運営の試行的な取組みを通じ、中小基盤の有用性検証や構築上の課題等の洗い出しを行うとともに、中小企業におけるセキュリティ対策の普及促進やセキュリティレベルの向上、中小企業向け製品・サービスのビジネス機会拡大の促進に寄与していきたいと考えています。

なお、本サイトは仮設サイトではあるものの、掲載製品・サービスは実際に提供されているものですので、もしもご興味がありましたら掲載事業者にお問合せいただくことができますので、ご活用いただければ幸いです。

※本事業は、独立行政法人情報処理推進機構委託事業「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」のことを指します。

※中小基盤の仮設サイトは、本事業の委託・再委託を受けた株式会社野村総合研究所と株式会社イーサーが運営するサイトになります。

※中小基盤への掲載製品・サービスは、株式会社野村総合研究所が実施した「本事業への協力が得られる中小企業向けサイバーセキュリティ製品・サービスの提供事業者の公募」において、採択されたサイバーセキュリティ製品・サービスになります。

※本サイトでは、各ブラウザ（Google Chrome、Microsoft Edge、Internet Explorer、Safari）それぞれ最新バージョンにて動作確認しております。

■お問い合わせ先

株式会社野村総合研究所 ICTメディアコンサルティング部  
「中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた試行環境調査」事務局係  
電子メール：a-hiraiwa@nri.co.jp（担当：平岩、山本）



HOME

サイトの説明 検索 製品・サービス紹介

## (2) 「検索」ページ

「検索」ページ上においても、フロントページと同様、注目ワードによる検索機能を提供した。加えて、「製品・サービスの種類から探す」、「目的から探す」、「自社の特徴から探す」という検索機能を提供した。

「製品・サービスの種類から探す」を用いた検索では、あらかじめ、中小基盤に掲載する各製品・サービスの種類を分類・整理し、それをもとに、「UTM」、「エンドポイントセキュリティ」、「EDR」、「ファイル暗号ツール」、「Web フィルタリングツール」、「端末管理ツール」、「ログ管理ツール」、「WAF」という8つの製品・サービスカテゴリを設定した。

中小基盤に掲載する各製品・サービスに紐づく製品・サービスカテゴリを設定することにより、中小企業が当該機能を利用して、検索したい製品・サービスカテゴリを選択し、クリックするだけで、該当する製品・サービスに関する情報に効率よくアプローチできるようにした。

また、「目的から探す」を用いた検索では、中小企業が目的に合わせて検索できるよう、「予算に合うものを選びたい」、「事故が起きないように対策したい」、「手厚いサポートを受けたい」、「お試し利用をしたい」という4つの目的を設定した。

さらに、「自社の特徴から探す」を用いた検索では、中小企業が自社の特徴に合わせて検索できるよう、「従業員規模から探す」、「業種から探す」という2つの特徴を設定した。

「検索」ページのトップページの画面を以下に示す。

図表 3-10 「検索」ページのトップページの画面



「目的から探す」から「予算に合うものを選びたい」を選択した際の検索については、中小企業における支払い可能な費用を考慮した上で、初期導入コストについては、10万円を上限として、また、ランニングコスト(年額)については、100万円

を上限として、それぞれ以下に示す4つのカテゴリを設定した。

図表 3-11 「予算に合うものを選びたい」を用いた検索ページの画面



The screenshot shows a search interface for '製品・サービス紹介' (Product/Service Introduction). It features a search bar with the text '予算（セキュリティ関連の年間予算額）に合うものを選びたい' (I want to choose something that fits my budget (annual budget related to security)). Below the search bar are two filter sections: '初期導入コスト' (Initial introduction cost) and 'ランニングコスト（年額）' (Running cost (annual amount)). Each filter section has a list of radio button options. At the bottom, there are two buttons: '前のページへ戻る' (Return to previous page) and '探す' (Search). A breadcrumb trail at the bottom reads 'HOME / 製品・サービス紹介 / 目的から探す - 予算に合うものを選びたい'.

製品・サービス紹介

### 目的から探す

予算（セキュリティ関連の年間予算額）に合うものを選びたい

初期導入コスト

- 1万円未満
- 3万円未満
- 5万円未満
- 10万円未満

ランニングコスト（年額）

- 10万円未満
- 30万円未満
- 50万円未満
- 100万円未満

[前のページへ戻る](#) [探す](#)

HOME / 製品・サービス紹介 / 目的から探す - 予算に合うものを選びたい

「事故が起きないように対策したい」を用いた検索については、IPA「情報セキュリティ10大脅威」の脅威カテゴリをもとに、以下に示す13のカテゴリを設定した。

また、「手厚いサポートを受けたい」を用いた検索では、あらかじめ、中小基盤に掲載する各製品・サービスのユーザーサポート体制を分類・整理し、それをもとに、以下に示す7つのカテゴリを設定した。

さらに、「お試し利用をしたい」を用いた検索では、お試し利用のサービスの提供があるかどうかのみで検索できるようにした。

図表 3-12 「事故が起きないように対策したい」を用いた検索ページの画面



製品・サービス紹介

### 目的から探す

事故が起きないように対策したい

対応可能な脅威

- 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
- ビジネスメール詐欺による金銭被害
- ランサムウェアによる被害
- 予期せぬIT基盤の障害に伴う業務停止
- 不注意による情報漏えい
- Web上の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
- 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
- IoT機器のボット化などの不正利用、情報漏えい
- 制御系システムへの攻撃による製造ラインの停止
- シャドーITによる不正アクセス、情報漏えい
- 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

[< 前のページへ戻る](#) [Q 探す](#)

複数の項目にチェックを入れた場合には製品・サービスの絞り込みが可能です。

[HOME](#) / [製品・サービス紹介](#) / [目的から探す - 事故が起きないように対策したい](#)

図表 3-13 「手厚いサポートを受けたい」を用いた検索ページの画面



製品・サービス紹介

### 目的から探す

手厚いサポートを受けたい

ユーザーサポート体制

- かんたん操作マニュアル（取扱説明書を含む）
- ユーザー補助設定ツール・アプリ
- 専門スタッフの現場訪問によるサポート
- サポートデスク（問合せ・相談窓口）によるサポート
- トラブル対応マニュアル及びFAQ
- トラブルシューティングツール
- 管理コンソールによる対応

[< 前のページへ戻る](#) [Q 探す](#)

複数の項目にチェックを入れた場合には製品・サービスの絞り込みが可能です。

[HOME](#) / [製品・サービス紹介](#) / [目的から探す - 手厚いサポートを受けたい](#)

「自社の特徴から探す」から「従業員規模から探す」を選択した際や「業種から探す」を選択した際の検索については、中小企業向け製品・サービスの多くが、従業員規模や業種を問わない製品・サービスとなっている点を考慮した上で、あくまで中小企業ユーザーのうち、従業員規模、業種の双方の観点からみた当該製品・サービスにおけるボリュームゾーンの顧客層を当該検索結果として示すこととした。また、中小企業において、上記の内容が理解され、当該検索結果があくまで目安として適切に活用されるよう、検索ページに解説文を付記した。

あらかじめ、従業員規模を区分する6つのカテゴリ、業種を区分する14のカテゴリの中から、中小基盤に掲載する各製品・サービスに紐づくボリュームゾーンの顧客層のカテゴリを設定することにより、中小企業が当該機能を利用して、検索したいカテゴリを選択し、「探す」ボタンをクリックするだけで、該当する製品・サービスに関する情報に効率よくアプローチできるようにした。

図表 3-14 「従業員規模から探す」を用いた検索ページの画面

製品・サービス紹介

### 自社の特徴から探す

中小企業向けセキュリティ製品・サービスの多くが、従業員規模や業種を問わない製品・サービスとなっているため、ここでの検索結果は、あくまで中小企業ユーザーのうち、当該製品・サービスにおけるボリュームゾーンの顧客層を示すものとなっています。

従業員規模から探す

従業員規模

- 10名以下
- 11~20名
- 21~50名
- 51~100名
- 101~300名
- 301名以上

< 前のページへ戻る

Q 探す

HOME / 製品・サービス紹介 / 自社の特徴から探す - 従業員規模から探す



図表 3-15 「業種から探す」を用いた検索ページの画面



### （3）「製品・サービス紹介」ページ

「製品・サービス紹介」ページでは、中小基盤に掲載する各製品・サービスについて、「ベンダー名」、「製品・サービス名称」、「製品・サービス概要」、「製品・サービスの種類」といった4つの情報を一覧できる機能（以下「製品・サービス一覧機能」という。）を提供した。

製品・サービス一覧機能から検索したい製品・サービスを選択し、クリックするだけで、該当する製品・サービスに関する詳細な情報に効率よくアプローチできるようにした。各製品・サービスに関する詳細な情報については、「3.3.2. 製品・サービス情報の掲載」に後述する。

なお、中小基盤に掲載する製品・サービスは12製品・サービスであり、1ページ内にすべての製品・サービスを掲載することが困難であったため、2ページにわたって9製品・サービスと3製品・サービスに分けて掲載した。

図表 3-16 「製品・サービス紹介」ページのトップページの画面



図表 3-17 「製品・サービス紹介」ページの2ページ目の画面



#### (4) 「アンケート」ページ

「アンケート」ページでは、前述した有用性評価アンケート調査の調査票に従って、選択式または自由回答形式で各設問に回答できる機能を提供した。

#### 3.3.2. 製品・サービス情報の掲載

前述したとおり、中小基盤の仮設サイトでは、中小企業は、以下に示す3つのアプローチ方法を通じて、該当する製品・サービスに関する詳細な情報にアクセスすることができるように構築した。

- ① 「サイトの説明」ページ及び「検索」ページの中で提供される注目ワードによる検索機能を利用して、各製品・サービスに関する情報にアプローチする方法
- ② 「検索」ページの中で提供される「製品・サービスの種類から探す」、「目的から探す」、「自社の特徴から探す」といった各種検索機能を利用して、各製品・サービスに関する情報にアプローチする方法

- ③「製品・サービス紹介」ページの中で提供される製品・サービス一覧機能から対象製品・サービスを選択して各製品・サービスに関する情報にアプローチする方法

各製品・サービスに関する詳細な情報について紹介するページのページ構成を以下に示す。

(1) 各製品・サービス情報のトップページ

各製品・サービス情報のトップページには、「ベンダー名」、「製品・サービス名称」、「製品・サービスの種類」を、ページの先頭に掲載するとともに、各製品・サービスの特徴やメリットを、中小企業に分かりやすく伝え、中小企業にとって活用しやすいものとするため、「各製品・サービスのテクノロジー」、「各製品・サービス情報」という見出しを付けて、関連する有用な情報を掲載した。

「各製品・サービスのテクノロジー」については、製品・サービスの概要を掲載するとともに、各製品・サービスの技術面の特徴を際立たせるため、「適用環境・適用シーン」、「一般的な製品等との違い」、「悪用等の悪意がある行動を防止する仕組み」といった3つの点から技術面の特徴に関する解説を掲載した。

「各製品・サービス情報」については、当該製品・サービスを利用する際のメリットを、中小企業に分かりやすく伝えるため、中小企業が製品・サービス選びで特に重視する「初期導入コスト」、「ランニングコスト」、「お試し利用」、「導入実績」、「導入時サポート」、「問合せ・相談窓口」、「その他サポートツール」、「ユーザー教育」、「対応可能な脅威」といった9つのポイントからビジネス面の特徴に関する情報を掲載した。

また、上記の情報を閲覧した後、当該製品・サービスに関心を持った中小企業が、ベンダーに問合せできるよう、各ベンダーの連絡先（電話番号、メールアドレス）、担当者、関連するウェブページ等の情報を、ページの末尾に掲載した。

さらに、より詳しい情報について知りたい中小企業のために、「ユーザーの評価情報」、「製品・サービスの詳しい情報」、「資料ダウンロード」から情報収集ができるページに遷移できるようリンクのボタンを実装した。

図表 3-18 各製品・サービス情報のトップページの画面(eGIS 株式会社のセキュリティドクターの例)

製品・サービス紹介

## セキュリティドクター

eGIS株式会社  
セキュリティドクター

EDR

Tech eGIS株式会社のテクノロジー

WindowsOSを使用しているエンドポイントのPCに対し、セキュリティ対策として広く普及している既存のセキュリティ製品等では検知できず、PCに侵入してきてしまった脅威を「検知」し、「アラート」を提供し、脅威を「ハンディング」するサービスを提供する、侵入検知型セキュリティである「EDR」+「EDR運用サービス」となります。

また、当該製品のデフォルトサービスとして、既にPCに侵入してしまっているウイルスや、PCの不正通信等を脅威レポートとして可視化し、企業毎の脅威/リスクを炙りだします。

さらに、サイバー保険も搭載しており、本製品で見つかった脅威の駆除費用にお使い頂けます。(プレミアムプランのみ/保険支払い条件あり)

**【適用環境・適用シーン】**

Windows OSが稼働する端末に運用可能です。特に、外部とのメール等でのやり取りが多いPCや、インターネットアクセスが多いPC、社外やテレワークで使用するPC、不特定多数の方が使用するPCへの導入をお勧めしています。

**【一般的な製品等との違い】**

一般的なウイルス対策ソフトウェアは、世界中のウイルス情報のパターンファイルと照らし合わせて駆除を行っていますが、当該製品は、既存のセキュリティ対策製品をすり抜けてくる脅威を、PCのハッシュ情報のログや、Windowsイベントログ等をモニタリング/分析していくことで、PCに侵入してきた脅威を検知します。セキュリティエンジニアが居ない企業であっても容易に高水準のセキュリティサービスを導入することが可能です。ログはPCから収集し、暗号化を行ってクラウドへ蓄積されます。

**【運用等の懸念がある行動を防止する仕組み】**

収集したPCの挙動ログを6か月後に自動消去する機能を実装しているほか、PCの挙動ログを暗号化してログ収集サーバにアップロードしています。

Info 製品・サービス情報

<b>初期導入コスト</b>	<b>お問い合わせ・相談窓口</b>
50,000円/1社 (初期登録手数料)	電子メール、ウェブページ
<b>ランニングコスト</b>	<b>その他のサポートツール</b>
6,000円/台・年 (スタンダードプランの場合の希望小売価格)、18,000円/台・年 (プレミアムプランの場合の希望小売価格)	トラブル対応マニュアル及びFAQサイト
<b>お試し利用</b>	<b>ユーザー教育</b>
あり	社員に対するセキュリティ教育サービス (有料)
<b>導入実績</b>	<b>対応可能な脅威</b>
約150社、約2,000ライセンス	ランサムウェアによる被害
<b>導入時サポート</b>	<b>緊急対応 (インシデント対応) 支援</b>
インストールマニュアルの提供	駆けつけ対応 (有料)、リモート駆除対応

**ユーザーの評価情報**

👤 ユーザーの評価情報を知りたい方はこちらへ

**製品・サービスの詳しい情報**

📄 もっと詳しく情報を知りたい方はこちらへ

**資料ダウンロード**

📄 ベンダー提供情報ダウンロード

**製品・サービスに関するお問い合わせ**

**eGIS株式会社 営業部**

住所：東京都港区芝4-3-11 VORT三田駅前6F  
 電話番号：03-6435-2820  
 メール：sd\_sales@egis.co.jp  
 担当：セールス担当 亀崎 晋平  
 製品・サービス関連ウェブサイト：<https://www.egis.co.jp/product>

なお、上記のサイトは組織のセキュリティポリシーの設定如何等によっては、閲覧できない可能性があります。

HOME / 製品・サービス紹介 / セキュリティドクター

(2) 「ユーザーの評価情報」ページ

「ユーザーの評価情報」ページには、製品・サービスベンダーから提出のあった「中小企業ユーザーによる製品等の評価情報提出用紙」の情報のうち、中小企業にとって参考となる評価情報を分かりやすく掲載した。詳細は 3.3.3. で後述する。

(3) 「製品・サービスの詳しい情報」ページ

「製品・サービスの詳しい情報」ページには、製品・サービスベンダーから提出のあった「応募用紙②」の情報のうち、中小企業にとって参考となる情報を、「導入のし易さ」、「運用のし易さ」、「導入時や運用時に要する費用」、「導入や運用における課題の解決」、「製品の効果」、「製品・サービスに付帯するオプションサービス、その他」といった実現可能性調査で取りまとめた評価項目の観点ごとに分かりやすく掲載した。

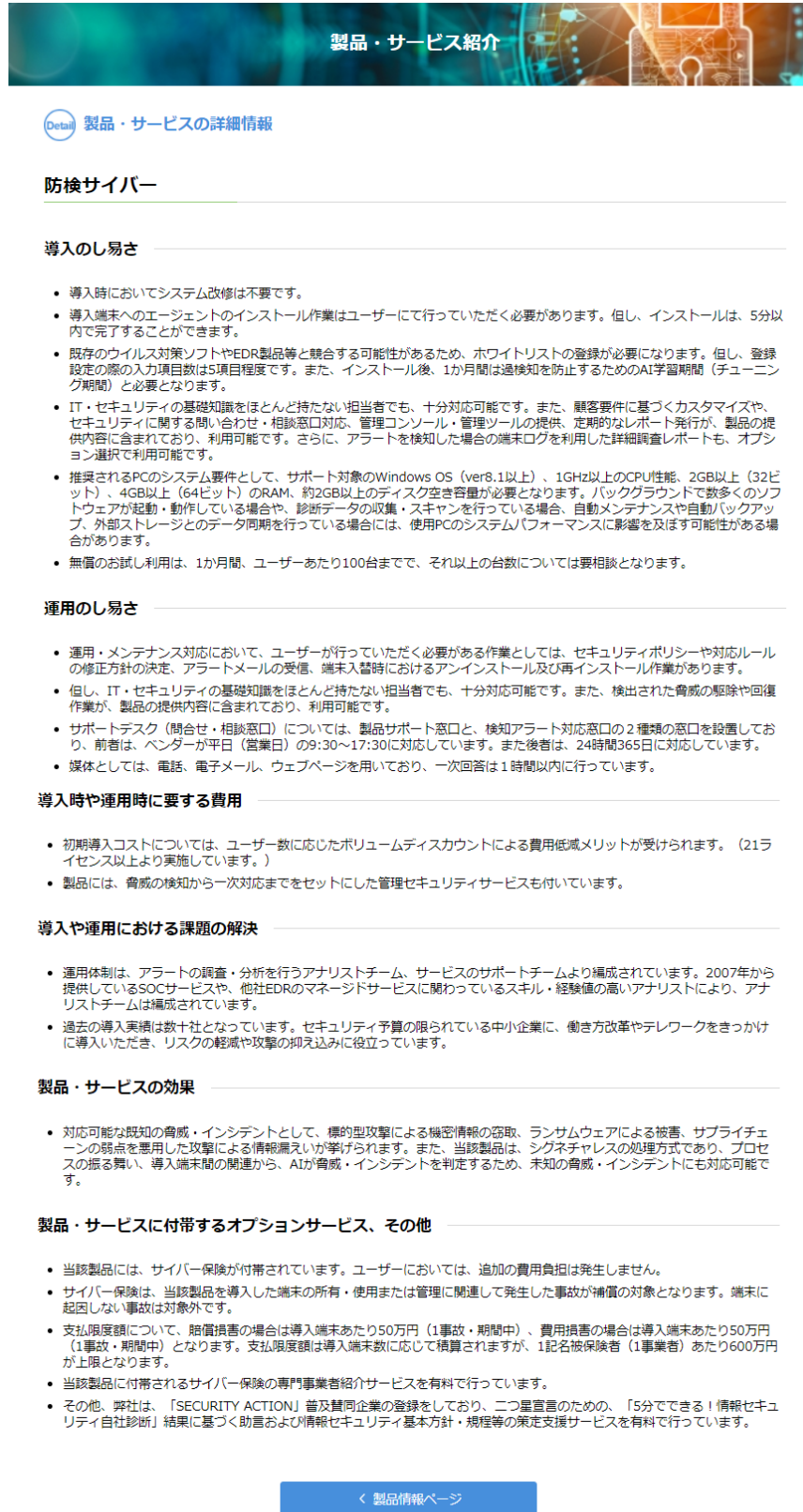
「製品・サービスの詳しい情報」ページの画面を次ページに示す。

(4) 「資料ダウンロード」ページ

製品・サービスベンダーから提出のあった「応募用紙②」に記載されている、実現可能性調査で取りまとめた評価項目の観点や詳細な評価項目に対応した各製品・サービスの情報を整理し、ダウンロード用のファイルとして作成した。

その上で、中小企業が当該ファイルを「資料ダウンロード」ページ上でダウンロードし、入手できるようにする機能を提供した。

図表 3-19 「製品・サービスの詳しい情報」ページの画面  
(MS&AD インターリスク総研株式会社の防検サイバーの例)



製品・サービスの詳細情報

防検サイバー

導入のし易さ

- 導入時においてシステム改修は不要です。
- 導入端末へのエージェントのインストール作業はユーザーにて行っていただく必要があります。但し、インストールは、5分以内で完了することができます。
- 既存のウイルス対策ソフトやEDR製品等と競合する可能性があるため、ホワイトリストの登録が必要になります。但し、登録設定の際の入力項目数は5項目程度です。また、インストール後、1か月間は過検知を防止するためのAI学習期間（チューニング期間）と必要となります。
- IT・セキュリティの基礎知識をほとんど持たない担当者でも、十分対応可能です。また、顧客要件に基づくカスタマイズや、セキュリティに関する問い合わせ・相談窓口対応、管理コンソール・管理ツールの提供、定期的なレポート発行が、製品の提供内容に含まれており、利用可能です。さらに、アラートを検知した場合の端末ログを利用した詳細調査レポートも、オプション選択で利用可能です。
- 推奨されるPCのシステム要件として、サポート対象のWindows OS（ver8.1以上）、1GHz以上のCPU性能、2GB以上（32ビット）、4GB以上（64ビット）のRAM、約2GB以上のディスク空き容量が必要となります。バックグラウンドで数多くのソフトウェアが起動・動作している場合や、診断データの収集・スキャンを行っている場合、自動メンテナンスや自動バックアップ、外部ストレージとのデータ同期を行っている場合には、使用PCのシステムパフォーマンスに影響を及ぼす可能性がある場合があります。
- 無償のお試し利用は、1か月間、ユーザーあたり100台までで、それ以上の台数については要相談となります。

運用のし易さ

- 運用・メンテナンス対応において、ユーザーが行っていただく必要がある作業としては、セキュリティポリシーや対応ルールの修正方針の決定、アラートメールの受信、端末入替時におけるアンインストール及び再インストール作業があります。
- 但し、IT・セキュリティの基礎知識をほとんど持たない担当者でも、十分対応可能です。また、検出された脅威の駆除や回復作業が、製品の提供内容に含まれており、利用可能です。
- サポートデスク（問合せ・相談窓口）については、製品サポート窓口と、検知アラート対応窓口の2種類の窓口を設置しており、前者は、ベンダーが平日（営業日）の9:30～17:30に対応しています。また後者は、24時間365日に対応しています。
- 媒体としては、電話、電子メール、ウェブページを用いており、一次回答は1時間以内に行っています。

導入時や運用時に要する費用

- 初期導入コストについては、ユーザー数に応じたボリュームディスカウントによる費用低減メリットが受けられます。（21ライセンス以上より実施しています。）
- 製品には、脅威の検知から一次対応までをセットにした管理セキュリティサービスも付いています。

導入や運用における課題の解決

- 運用体制は、アラートの調査・分析を行うアナリストチーム、サービスのサポートチームより構成されています。2007年から提供しているSOCサービスや、他社EDRのマネージドサービスに関わっているスキル・経験値の高いアナリストにより、アナリストチームは構成されています。
- 過去の導入実績は数十社となっています。セキュリティ予算の限られている中小企業に、働き方改革やテレワークをきっかけに導入いただき、リスクの軽減や攻撃の抑え込みに役立っています。

製品・サービスの効果

- 対応可能な既知の脅威・インシデントとして、標的型攻撃による機密情報の窃取、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が増えられます。また、当該製品は、シグネチャレスの処理方式であり、プロセスの振る舞い、導入端末間の関連から、AIが脅威・インシデントを判定するため、未知の脅威・インシデントにも対応可能です。

製品・サービスに付帯するオプションサービス、その他

- 当該製品には、サイバー保険が付帯されています。ユーザーにおいては、追加の費用負担は発生しません。
- サイバー保険は、当該製品を導入した端末の所有・使用または管理に関連して発生した事故が補償の対象となります。端末に起因しない事故は対象外です。
- 支払限度額について、賠償損害の場合は導入端末あたり50万円（1事故・期間中）、費用損害の場合は導入端末あたり50万円（1事故・期間中）となります。支払限度額は導入端末数に応じて積算されますが、1記名被保険者（1事業者）あたり600万円が上限となります。
- 当該製品に付帯されるサイバー保険の専門事業者紹介サービスを有料で行っています。
- その他、弊社は、「SECURITY ACTION」普及賛同企業の登録をしており、二つ星宣言のための、「5分でできる！情報セキュリティ自社診断」結果に基づく助言および情報セキュリティ基本方針・規程等の策定支援サービスを有料で行っています。

< 製品情報ページ

### 3.3.3. 中小企業ユーザーの事後評価情報の登録

中小企業ユーザーによる製品等の評価情報については、製品・サービスベンダーから提出のあった中小企業ユーザー各2社の業種を明らかにした上で、実際に製品・サービスを導入したお客様からの声として、「ユーザーの評価情報」ページに評価したポイントや具体的な内容を分かりやすく示した。

図表 3-20 「ユーザーの評価情報」ページの画面(株式会社 Blue Planet-works の AppGuard の例)

製品・サービス紹介

Voice ユーザーの評価情報

## AppGuard

実際に製品・サービスを導入したお客様からの声

🚚 運輸業 (A社)

🏭 製造業 (B社)

**コストメリットが高かった！**  
運用コストについて、EDRと比較した際にコストメリットが高かった。また、ライセンス費用にサイバー保険が付いていて、いざという時にも安心できる。

**ユーザーサポートがきめ細かった！**  
事前に無償にて3ヶ月程度の動作検証を行い、またインストールから基本的な設定作業までを無償で支援してもらえなど、きめの細かいサポートが得られた。

**PCへの影響が最小限でした！**  
定義ファイルの更新などがなくて、PCの動作は軽かった。また、影響が出た場合でも、例外設定で回避ができるため、PCへの影響は最小限である。

**既知/未知を問わず防御が可能で安心できました！**  
サポート切れの古いiOSを使わざるを得ない状況だが、古いiOSやアプリケーションにとっては既知の脅威への対応も困難なケースが多いところ、既知/未知を問わず防御が可能なのは極めて有益であった。

← 製品情報ページ

HOME / 製品・サービス紹介 / ユーザーの評価情報 - AppGuard

### 3.4. 中小基盤の公開とアクセス

中小基盤の仮設サイトを2021年12月10日(金)から2022年1月31日(月)の期間限定で特定対象者に公開した。公開期間中、中小基盤の仮設サイトへのアクセス状況や情報提供機能や検索機能の利用状況について、集計・分析を実施した。

中小基盤の仮設サイトについては、セキュリティ対策自己宣言「SECURITY ACTION」制度の宣言事業者のうち、情報提供・調査への協力について承諾を得ている事業者71,123社に

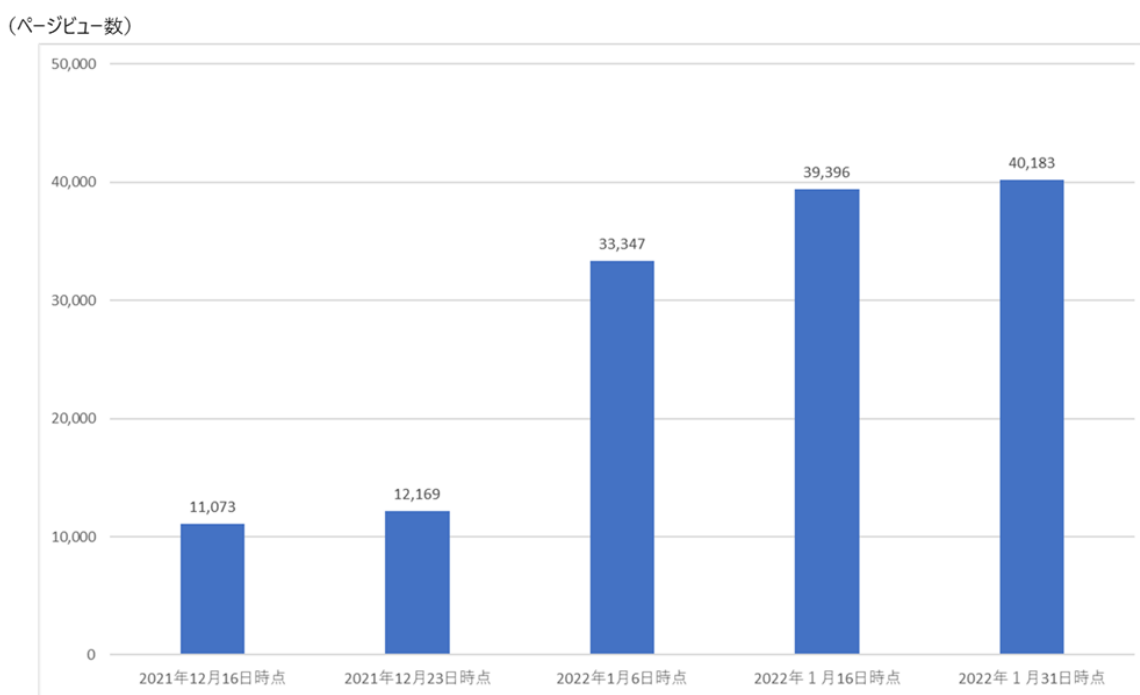


対し、事務局からメールで仮設サイトの閲覧と有用性評価アンケートへの協力依頼を実施した。

### 3.4.1. 中小基盤へのアクセス状況の集計・分析

中小基盤のページビュー数(累積数)は、サイト開設から約1週間で10,000ページビューを超え、約1か月で約40,000ページビューに到達した。最終的に、中小基盤のページビュー数(累積数)は40,183件となった。

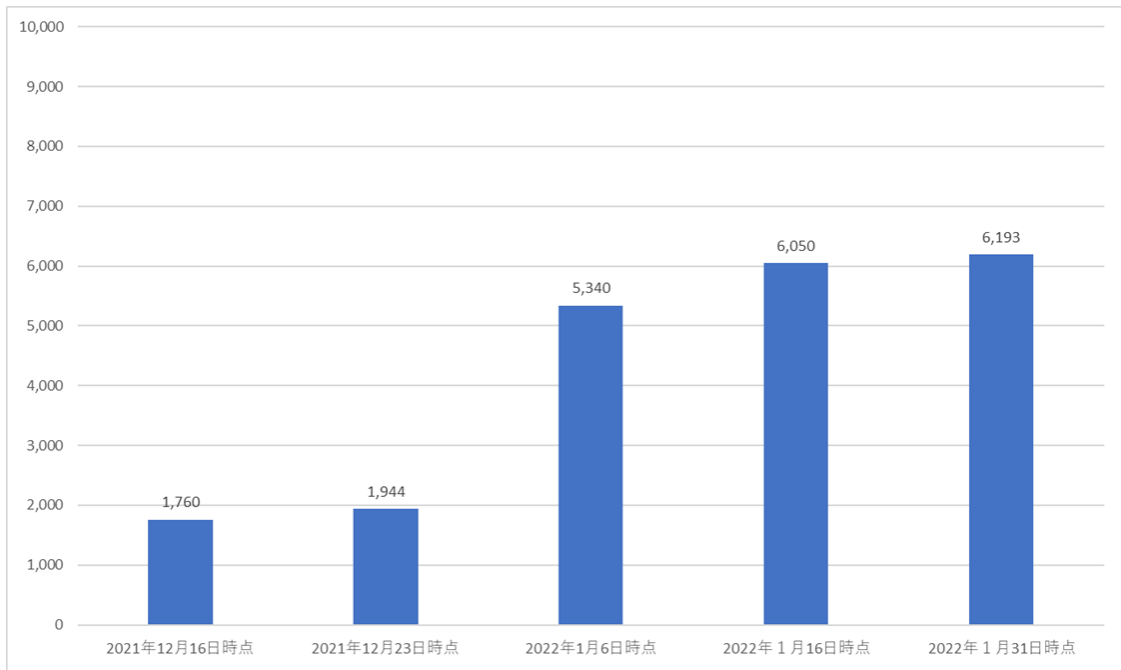
図表 3-21 中小基盤の仮設サイトのページビュー数(累積数)



サイト開設期間中に中小基盤にアクセスしたユーザー数(重複を除くユニークユーザー数:以下同じ)は、サイト開設から約1週間で1,500ユーザーを超え、約1か月で約6,000ユーザーに到達した。最終的に、中小基盤の仮設サイトにアクセスしたユーザー数は6,193人となった。

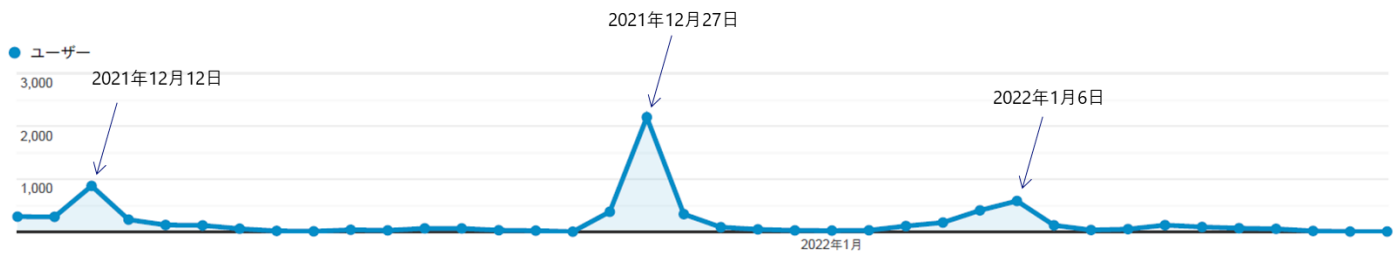
図表 3-22 中小基盤の仮設サイトにアクセスしたユーザー数(ユニークユーザー数)

(ユーザー数)



中小基盤のアンケートページへのアクセスユーザー数は、事務局からのアンケート協力依頼メール発出直後の2021年12月12日(日)、2021年12月27日(月)、2022年1月6日(木)に3つの山(アクセス集中の波)が出来ている。

図表 3-23 中小基盤の仮設サイトのアンケートページへのアクセス状況



### 3.4.2. 情報提供機能や検索機能の利用状況の集計・分析

製品・サービス掲載ページのページビュー数(累積数)の上位1位は、トレンドマイクロ(株)／Cloud Edge(UTM)、上位2位は、(株)フーバーブレイン／Eye” 247” AntiMalware USAVIV(エンドポイントセキュリティ・UTM)、上位3位は、(株)ハンモック／AssetView(端末管理ツール)となった。

図表 3-24 各製品・サービス掲載ページのページビュー数(累積数)

掲載製品 ・サービス	2021年 12月16日時点		2021年 12月23日時点		2022年 1月6日時点		2022年 1月16日時点		2022年 1月31日時点	
	ページ ビュー 数	順位	ページ ビュー 数	順位	ページ ビュー 数	順位	ページ ビュー 数	順位	ページ ビュー 数	順位
Cloud Edge (トレンドマイクロ(株))	202	1位	216	1位	490	1位	604	1位	618	1位
Eye” 247” AntiMalware USAVIV (株)フーバーブレイン)	191	2位	209	2位	455	2位	523	2位	543	2位
AssetView (株)ハンモック)	165	3位	176	3位	385	3位	446	3位	445	3位
ALog シリーズ製品 (株)網屋)	111	6位	123	6位	327	4位	387	4位	402	4位
Llave (ジャーベ) (株)クイリー)	119	5位	145	4位	295	5位	352	5位	375	5位
MRB-cloud (株)テクノ)	126	4位	138	5位	270	6位	301	6位	312	6位
i-FILTER@Cloud (デジタルアーツ(株))	109	7位	116	7位	220	7位	270	7位	281	7位
セキュリティドク ター (eGIS 株式会社)	69	10位	79	9位	197	8位	227	8位	231	8位
WatchGuard Firebox アプライア ンス (ウォッチガード・テク ノロジー・ジャパン(株))	101	8位	107	8位	179	9位	224	9位	231	8位
防検サイバー (MS&AD インターリスク 総研(株))	72	9位	75	10位	168	10位	198	10位	203	10位
AppGuard (株)Blue Planet- works)	63	11位	70	11位	152	11位	185	11位	192	11位
Barracuda Web Application Firewall/Barracuda WAF-as-a-Service (バラクーダネットワー クスジャパン(株))	62	12位	64	12位	113	12位	132	12位	137	12位

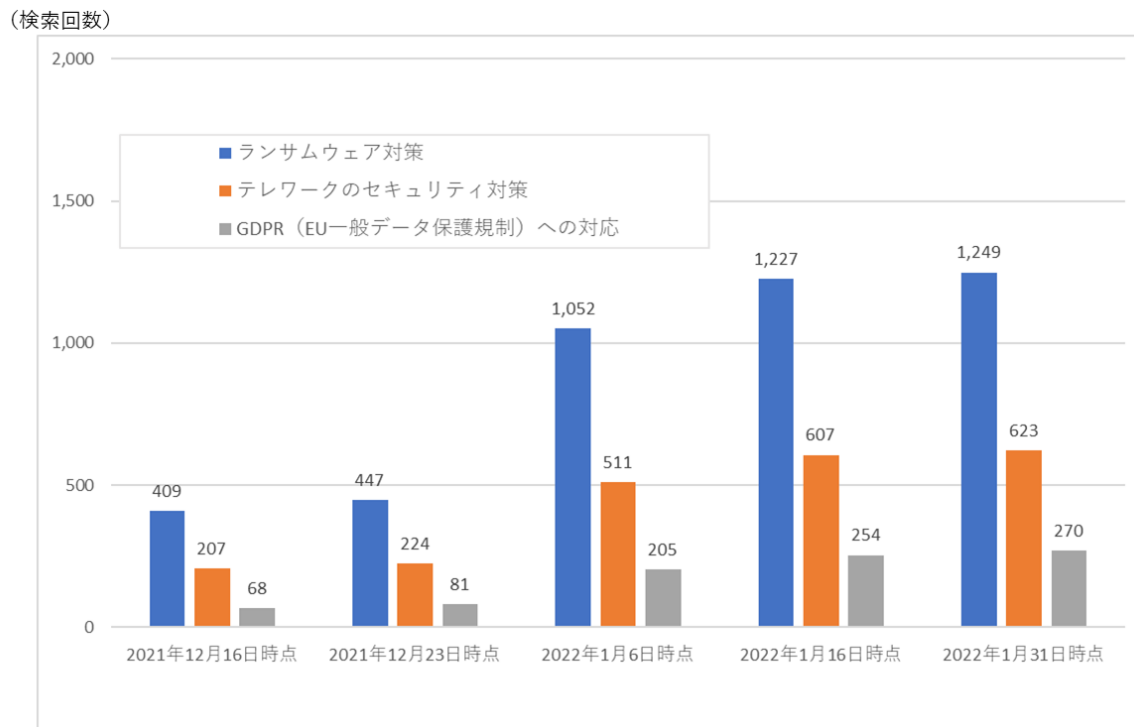
検索機能のうち、検索回数が多いのは、「製品・サービスの種類」による検索では「UTM」、  
「エンドポイントセキュリティ」を検索条件にした検索であり、「従業員規模」による検索  
では「10名以下」、「21～50名」を検索条件にした検索であった。「予算」による検索で  
は初期導入コスト「1万円未満」、ランニングコスト「10万円未満」をアンドの検索条件に  
した検索が多く利用された。

図表 3-25 各検索条件による検索回数(累積数)(上位5位)

検索回数 順位	2021年 12月16日時点		2021年 12月23日時点		2022年 1月6日時点		2022年 1月16日時点		2022年 1月31日時点	
	検索条件	検索回数	検索条件	検索回数	検索条件	検索回数	検索条件	検索回数	検索条件	検索回数
1位	「製品・サービスの種類から探す」/UTM	72	「製品・サービスの種類から探す」/UTM	78	「製品・サービスの種類から探す」/UTM	174	「製品・サービスの種類から探す」/UTM	209	「製品・サービスの種類から探す」/UTM	211
2位	「製品・サービスの種類から探す」/エンドポイントセキュリティ	47	「製品・サービスの種類から探す」/エンドポイントセキュリティ	48	「製品・サービスの種類から探す」/エンドポイントセキュリティ	117	「製品・サービスの種類から探す」/エンドポイントセキュリティ	134	「製品・サービスの種類から探す」/エンドポイントセキュリティ	135
3位	「目的から探す」－「予算に合うものを選びたい」/初期導入コスト：1万円未満&ランニングコスト：10万円未満	41	「目的から探す」－「予算に合うものを選びたい」/初期導入コスト：1万円未満&ランニングコスト：10万円未満	44	「自社の特徴から探す」－「従業員規模から探す」/10名以下	105	「自社の特徴から探す」－「従業員規模から探す」/10名以下	121	「自社の特徴から探す」－「従業員規模から探す」/10名以下	124
4位	「自社の特徴から探す」－「従業員規模から探す」/10名以下	36	「自社の特徴から探す」－「従業員規模から探す」/10名以下	36	「目的から探す」－「予算に合うものを選びたい」/初期導入コスト：1万円未満&ランニングコスト：10万円未満	91	「目的から探す」－「予算に合うものを選びたい」/初期導入コスト：1万円未満&ランニングコスト：10万円未満	107	「目的から探す」－「予算に合うものを選びたい」/初期導入コスト：1万円未満&ランニングコスト：10万円未満	108
5位	「製品・サービスの種類から探す」/EDR	28	「自社の特徴から探す」－「従業員規模から探す」/21～50名	30	「製品・サービスの種類から探す」/ファイル暗号化ツール	72	「自社の特徴から探す」－「従業員規模から探す」/21～50名	93	「製品・サービスの種類から探す」/ファイル暗号化ツール	95

また、「注目ワード」による検索は、「ランサムウェア対策」をキーワードにした検索回数が多かった。

図表 3-26 注目ワードによる検索回数(累積数)



### 3.5. 中小企業による中小基盤に対する評価アンケートの実施

中小基盤上で提供されている情報提供機能や検索機能が、中小企業にとって活用しやすいものであるか等を確認することを目的に、中小基盤の仮設サイト訪問の目的や、中小基盤の仮設サイトにおける情報検索の達成度等について、有用性評価アンケートを実施した。

有用性評価アンケートの実施概要を以下に示す。

- (1) 調査対象 : セキュリティ対策自己宣言「SECURITY ACTION」制度の宣言事業者のうち、情報提供・調査への協力承諾を得ている事業者 71, 123 社
- (2) 実施時期 : 2021年12月10日(金)から2022年1月14日(金)までの36日間
- (3) 調査手法 : Web アンケート調査 (仮設サイト上) 設問数 21 問
- (4) 有効回答数 : 2, 286 サンプル

#### 3.5.1. アンケート項目の作成

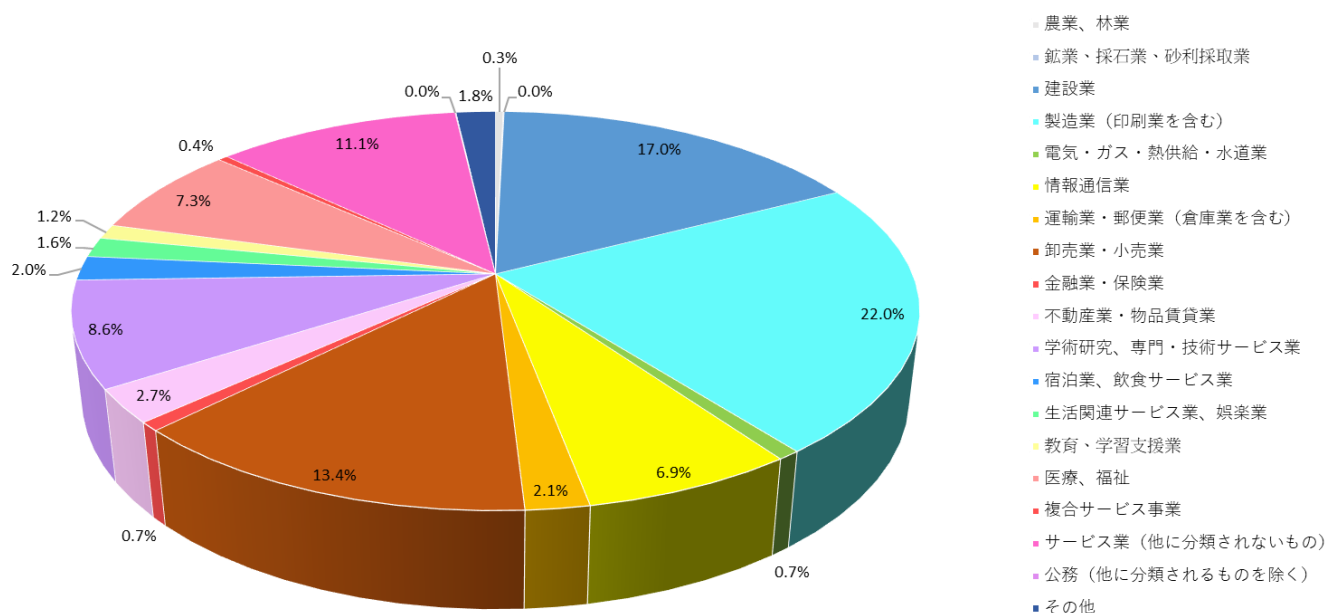
有用性評価アンケートのアンケート項目は、有識者検討委員会において、調査仮説や設問文、各選択肢等について検討を行い、それらの検討内容を反映しながら、アンケート項目の取りまとめを行った。(有用性評価アンケートの調査票は図表 2-1 を参照)

### 3.5.2. アンケート結果の集計・分析

中小企業による中小基盤に対する有用性評価アンケートの結果（有効回答数：2,286 サンプル）を以下に示す。

問1の「回答者の企業・団体の主たる事業の業種」について、多い業種から製造業（印刷業を含む）の503社(22.0%)、建設業の389社(17.0%)、卸売業・小売業の307社(13.4%)、サービス業（他に分類されないもの）の254社(11.1%)、学術研究、専門・技術サービス業の196社(8.6%)、医療、福祉の168社(7.3%)、情報通信業の157社(6.9%)であった。

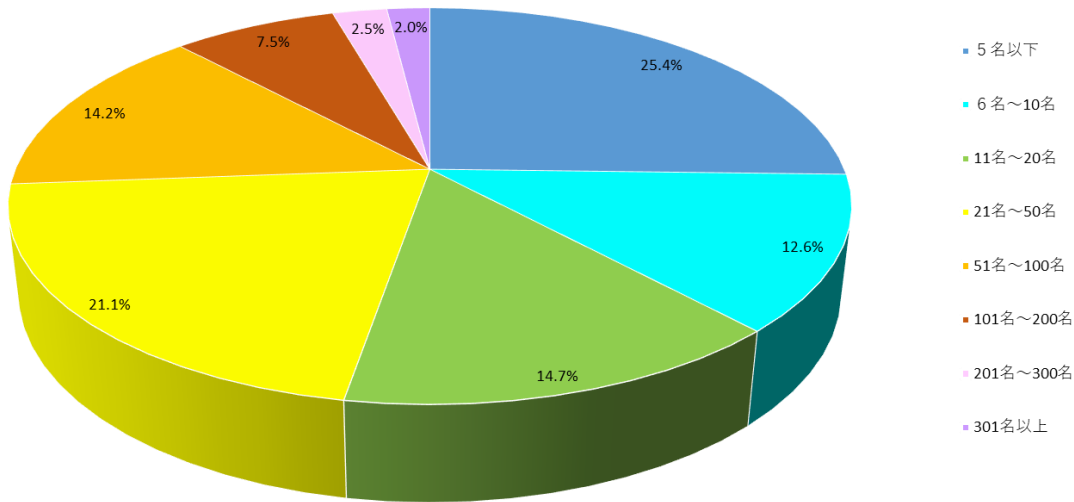
図表 3-27 回答者の企業・団体の主たる事業の業種(N=2,286)



問2の「回答者の企業・団体の総従業員数（正社員以外の雇用形態の社員も含む。派遣社員や、常駐する他社の社員は除く）」について、多い順から5名以下の581社(25.4%)、21名～50名の482社(21.1%)、11名～20名の335社(14.7%)、51名～100名の325社(14.2%)、6名～10名の289社(12.6%)、101名～200名の172社(7.5%)、201名～300名の57社(2.5%)、301名以上の45社(2.0%)であった。

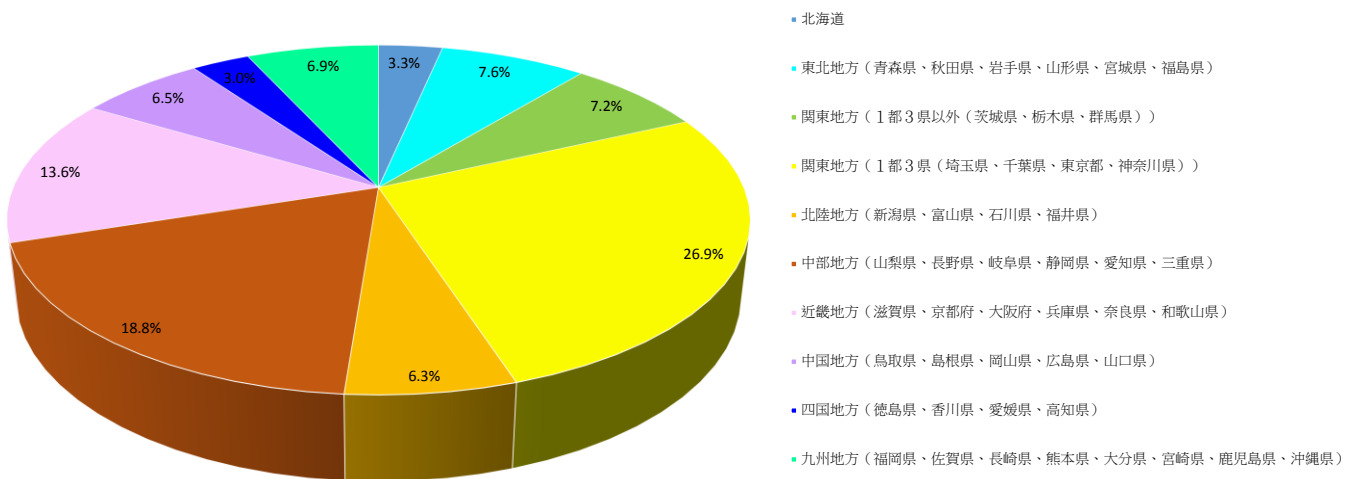
図表 3-28 回答者の企業・団体の総従業員数

(正社員以外の雇用形態の社員も含む。派遣社員や、常駐する他社の社員は除く)(N=2,286)



問3の「回答者の企業・団体の所在地」について、多い順から関東地方(1都3県)の614社(26.9%)、中部地方の429社(18.8%)、近畿地方の311社(13.6%)、東北地方の174社(7.6%)、関東地方(1都3県以外)の164社(7.2%)、九州地方の157社(6.9%)、中国地方の149社(6.5%)、北陸地方の143社(6.3%)、北海道の76社(3.3%)、四国地方の69社(3.0%)であった。

図表 3-29 回答者の企業・団体の所在地(N=2,286)

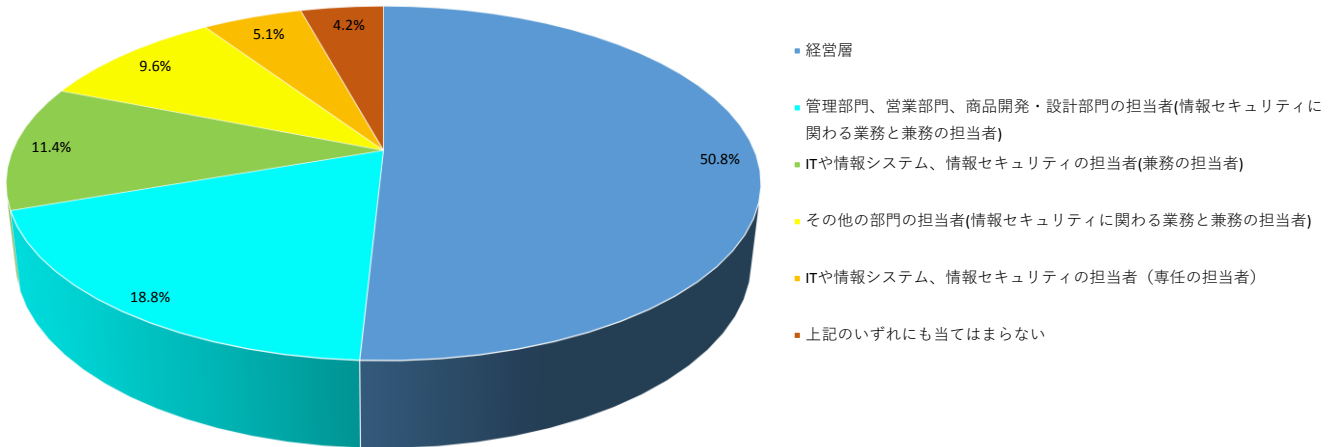


問4の「回答者の立場」について、多い順から経営層の1,162名(50.8%)、管理部門、営業部門、商品開発・設計部門の担当者(情報セキュリティに関わる業務と兼務の担当者)の430名(18.8%)、ITや情報システム、情報セキュリティの担当者(兼務の担当者)の261名(11.4%)、その他の部門の担当者(情報セキュリティに関わる業務と兼務の担当者)の219名(9.6%)、ITや情報システム、情報セキュリティの担当者(専任の担当者)の117名(5.1%)で

あった。

上記のいずれにも当てはまらないと回答した回答者は、総務系、事務系、経理系、企画系、個人事業主等が含まれた。

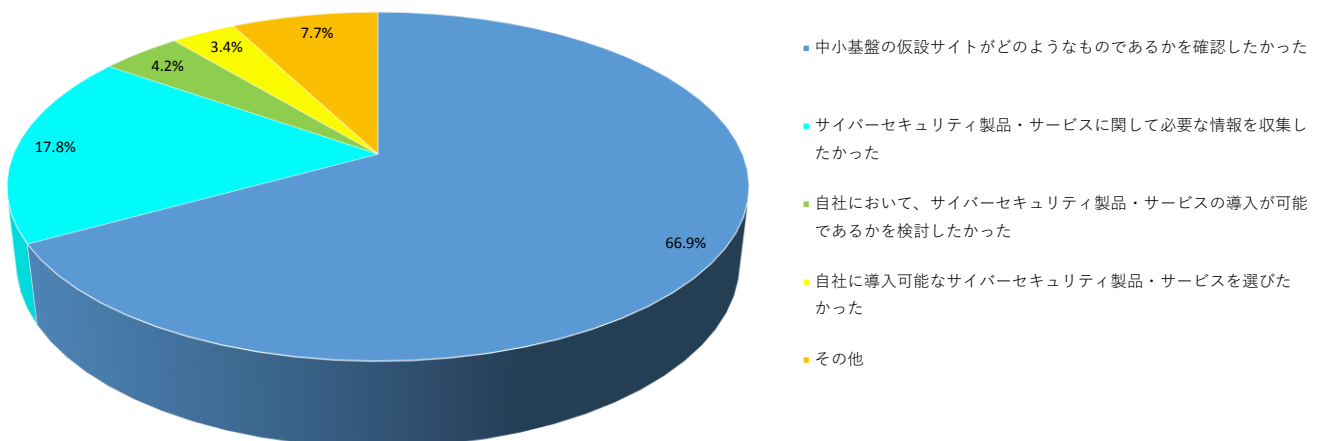
図表 3-30 回答者の立場(N=2,286)



問5の「中小基盤の仮設サイト訪問の目的」について、最も多かったのが、「中小基盤の仮設サイトがどのようなものであるかを確認したかった」(66.9%)であった。次いで、「サイバーセキュリティ製品・サービスに関して必要な情報を収集したかった」(17.8%)が多かった。以下「自社において、サイバーセキュリティ製品・サービスの導入が可能であるかを検討したかった」(4.2%)、「自社に導入可能なサイバーセキュリティ製品・サービスを選びたかった」(3.4%)であった。

その他と回答した回答者の意見は、事務局から「アンケート依頼があったため」(133名)との回答が多かった。

図表 3-31 中小基盤の仮設サイト訪問の目的(N=2,286)

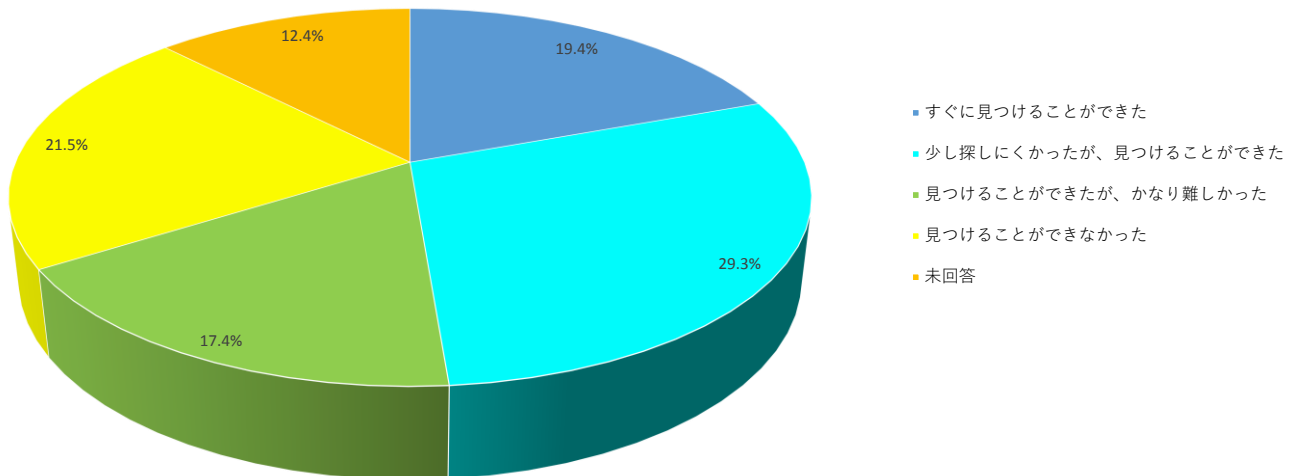




問6の「中小基盤の仮設サイト上で提供している製品・サービスの検索機能によるお探しの情報への到達状況」について、多い順から「少し探しにくかったが、見つけることができた」(29.3%)、「見つけることができなかった」(21.5%)、「すぐに見つけることができた」(19.4%)、「見つけることができたが、かなり難しかった」(17.4%)であった。

本設問は、問5の中小基盤の仮設サイト訪問の目的について、「サイバーセキュリティ製品・サービスに関して必要な情報を収集したかった」、「自社において、サイバーセキュリティ製品・サービスの導入が可能であるかを検討したかった」、「自社に導入可能なサイバーセキュリティ製品・サービスを選びたかった」と回答した回答者を対象にした(回答数:581)。

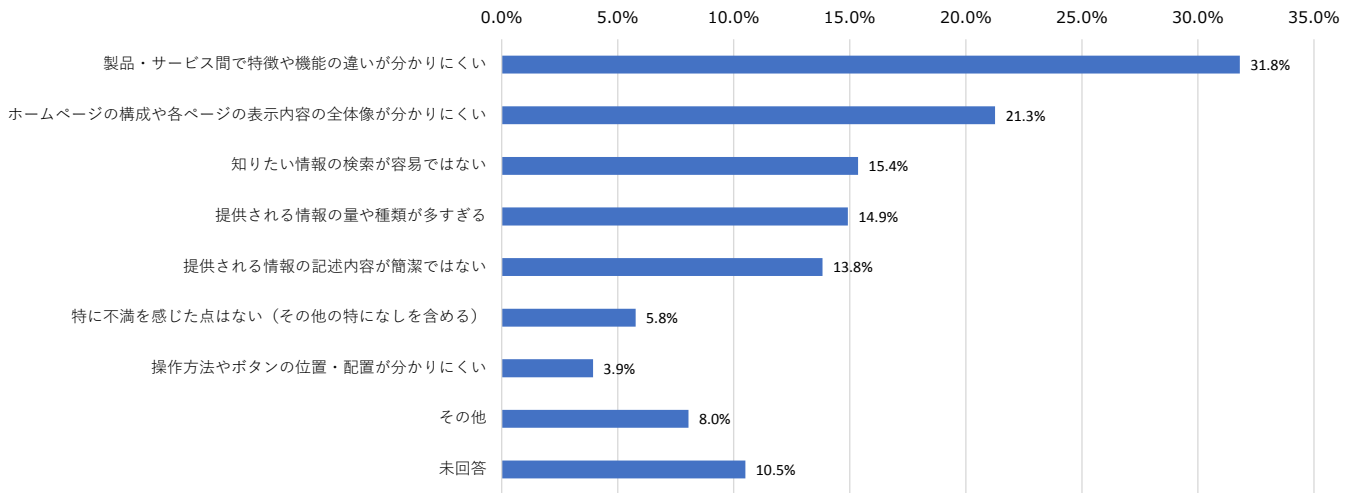
図表 3-32 中小基盤の仮設サイト上で提供している製品・サービスの検索機能によるお探しの情報への到達状況(N=581)



問7の「中小基盤の仮設サイトに対する不満点(複数回答可)」について、最も多い回答が「製品・サービス間で特徴や機能の違いが分かりにくい」(31.8%)であった。次いで、「ホームページの構成や各ページの表示内容の全体像が分かりにくい」(21.3%)が多かった。以下「知りたい情報の検索が容易ではない」(15.4%)、「提供される情報の量や種類が多すぎる」(14.9%)、「提供される情報の記述内容が簡潔ではない」(13.8%)であった。「特に不満を感じた点はない」と回答したのは5.8%であった。

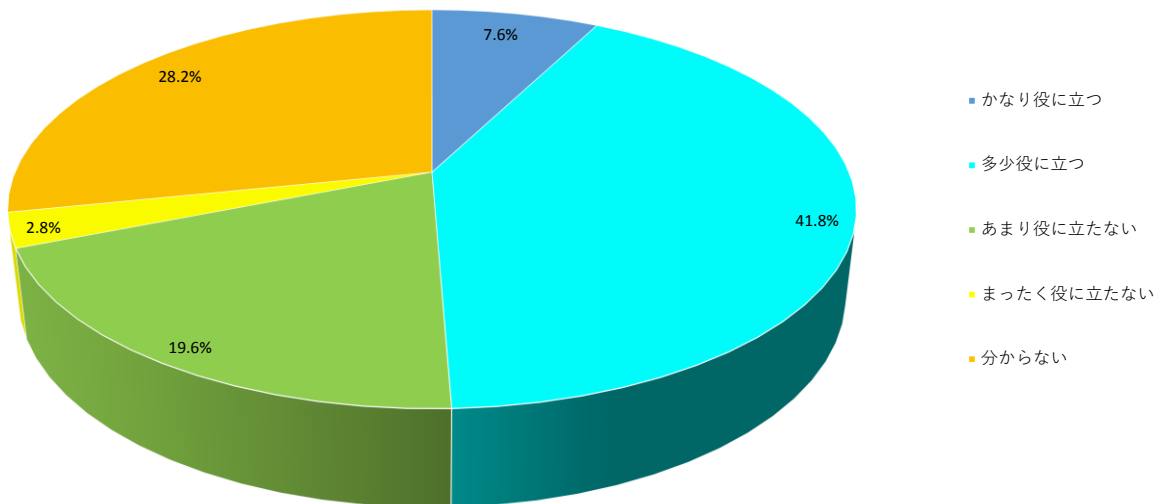
その他と回答した回答者の意見は、「専門用語が多いことから理解が難しい」、「セキュリティの知識がないため、何から検索し手を付ければ良いかわからない」、「モデルケース等を提示してもらいたい」等の専門性に関する課題や、「インシデント事例や、中小企業が抱える困りごとから検索を行いたい」等の検索に対する要望や、「製品同士の比較機能がない」、「サイトの全体像が把握できない」等の仮設サイトの機能、構成に関する課題が挙げられた。

図表 3-33 中小基盤の仮設サイトに対する不満点 (N=2,286)



問8の「中小基盤の仮設サイトの検索機能の有用度合い」について、最も多い回答が「多少役に立つ」(41.8%)であった。次いで、「分からない」(28.2%)が多かった。以下「あまり役に立たない」(19.6%)、「かなり役に立つ」(7.6%)、「まったく役に立たない」(2.8%)であった。

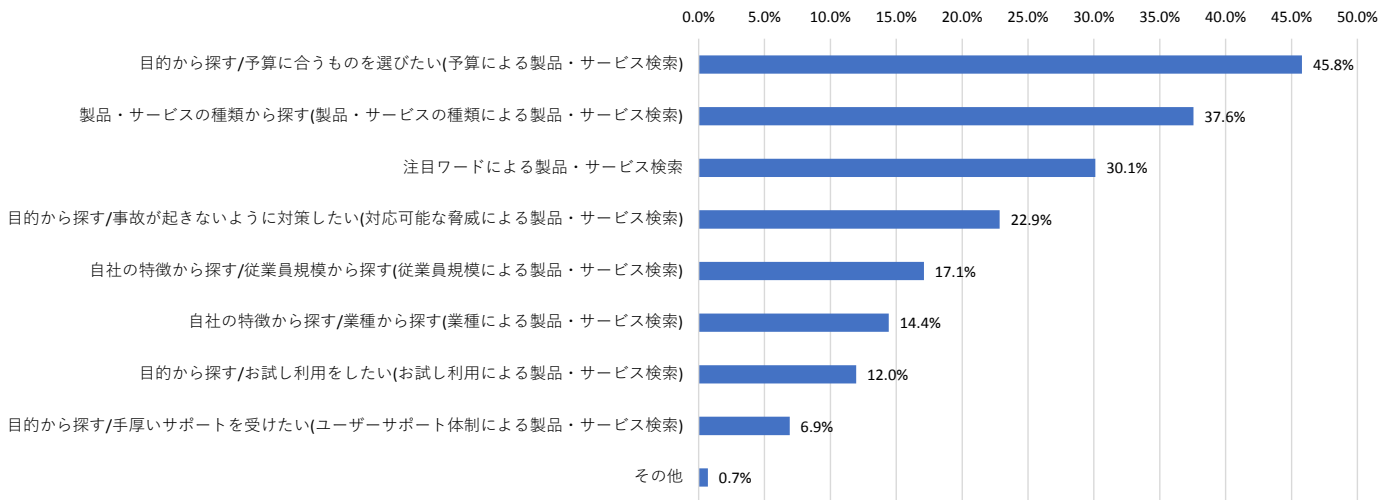
図表 3-34 中小基盤の仮設サイトの検索機能の有用度合い (N=2,286)



問9の「役に立つ検索機能 (複数回答可)」について、最も多い回答が「予算に合うものを選びたい(予算による製品・サービス検索)」(45.8%)であった。次いで、「製品の種類から探す(製品の種類による製品・サービス検索)」(37.6%)が多かった。以下「注目ワードによる製品・サービス検索」(30.1%)、「事故が起きないように対策したい(対応可能な脅威による製品・サービス検索)」(22.9%)であった。

本設問は、問8の中小基盤の仮設サイトの検索機能の有用度合いについて、「かなり役に立つ」、「多少役に立つ」と回答した回答者を対象にした（回答数：1,129）。

図表 3-35 役に立つ検索機能(N=1,129)



問10の「製品・サービスの検索機能について、サイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容（自由回答）」について、回答内容のうち、「イニシャル/ランニングコストから予算(概算)にあった製品が検索できるメリットは大きい」、「予算内での検討が可能である」等の予算による製品・サービス検索についての意見や、「従業員規模から探す」の検索機能は、自社の規模に見合う情報を判断する上で有用である」「規模による経費対効果を推測しやすい」等の従業員規模による製品・サービス検索についての意見、「ニュースや新聞で出てくるキーワードでの検索から、製品やサービスを絞り込めるのはわかりやすい」等の注目ワードによる製品・サービス検索についての意見等が得られた。

本設問は、問8の中小基盤の仮設サイトの検索機能の有用度合いについて、「かなり役に立つ」、「多少役に立つ」と回答した回答者を対象にした。

問11の「製品・サービスの検索機能について、サイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容（自由回答）」について、回答内容のうち、「従業員数や予算などを組み合わせた検索が出来るか、もしくはフローチャートのように条件分岐しながら製品を探せると良い」、「取り組みたい課題から検索できると良い」、「フリーワード検索を搭載してほしい」等の検索機能の改善に関する意見が挙げられた。

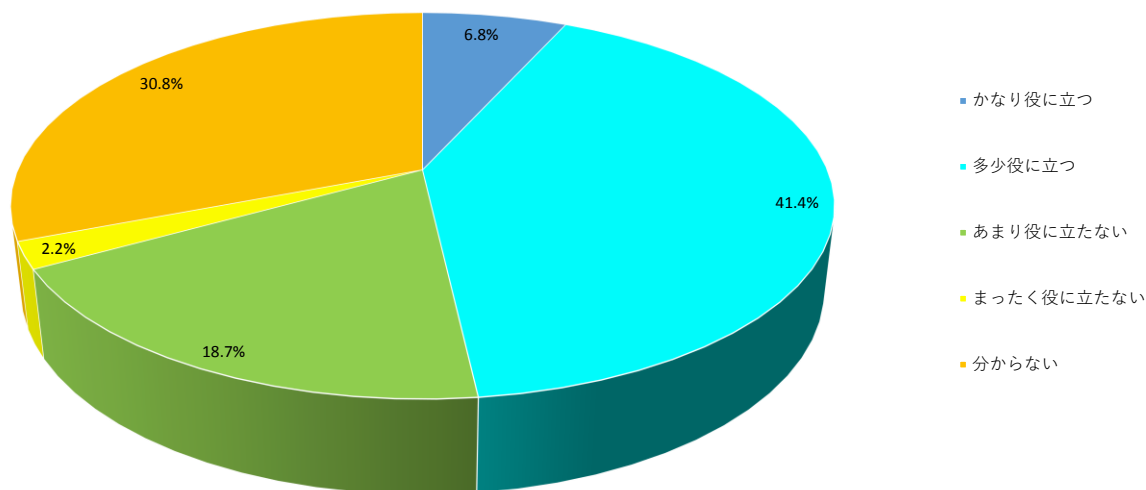
しかしながら、寄せられた意見の多くは「そもそもの記載内容が専門的すぎるため何を検索して良いか分からない」、「どこから手を付けてよいのか、そもそもどういった対策がある

のかが分からない」、「どんな脅威があって、どこまで対応すれば良いのか分からないため、検索に至らない」、「サイトを訪問しても何をしてよいか分からない」等、ユーザーのサイバーセキュリティに関する知識が十分でないことに起因すると考えられる意見も寄せられた。

本設問は、問8の中小基盤の仮設サイトの検索機能の有用度合いについて、「あまり役に立たない」、「まったく役に立たない」、「分からない」と回答した回答者を対象にした。

問12の「中小基盤の仮設サイト上で提供される製品・サービスの各種情報の有用度合い」について、最も多い回答が「多少役に立つ」(41.4%)であった。次いで、「分からない」(30.8%)が多かった。以下「あまり役に立たない」(18.7%)、「かなり役に立つ」(6.8%)、「まったく役に立たない」(2.2%)であった。

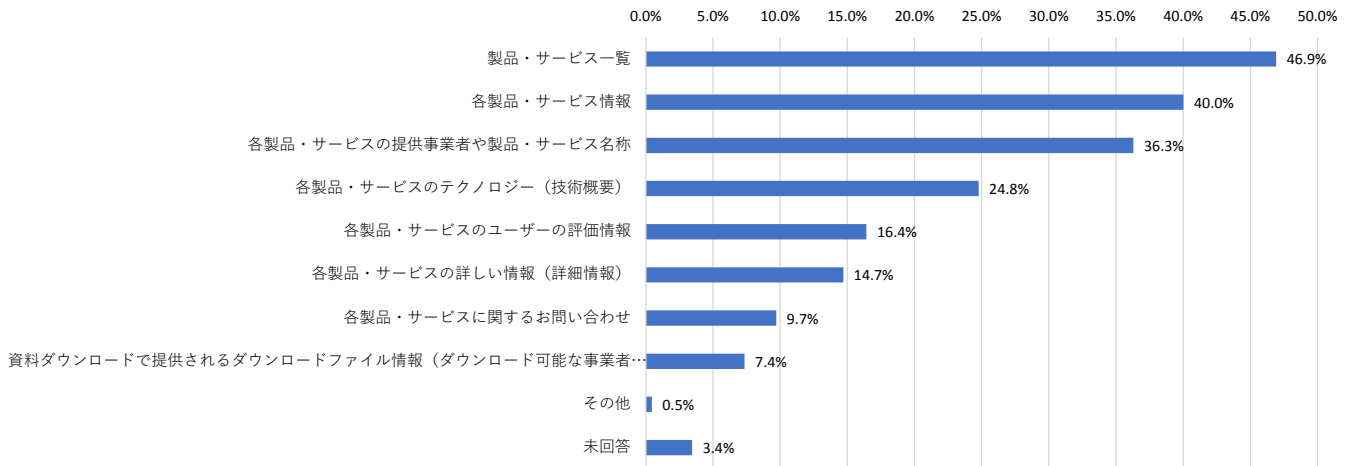
図表 3-36 中小基盤の仮設サイト上で提供される製品・サービスの各種情報の有用度合い(N=2,286)



問13の「役に立つ製品・サービスの各種情報(複数回答可)」について、最も多い回答が「製品・サービス一覧」(46.9%)であった。次いで、「各製品・サービス情報」(40.0%)が多かった。以下「各製品・サービスの提供事業者や製品・サービス名称」(36.3%)、「各製品・サービスのテクノロジー(技術概要)」(24.8%)、「各製品・サービスのユーザーの評価情報」(16.4%)、「各製品・サービスの詳しい情報(詳細情報)」(14.7%)であった。

本設問は、問12の中小基盤の仮設サイトの製品・サービスの各種情報の有用度合いについて、「かなり役に立つ」、「多少役に立つ」と回答した回答者を対象にした(回答数:1,102)。

図表 3-37 役に立つ製品・サービスの各種情報(N=1,102)



問 14 の「製品・サービスの各種情報について、サイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容 (自由回答)」について、回答内容のうち、「導入コスト、運用コスト、サポート内容等が一覧で見ることが出来るのは視認性が良い」、「個々のベンダーのサイトには金額が書かれていないことが多いが、初期導入コストと運用コストが簡潔に記載されているので、初期の情報収集に有用」、「具体的な費用例を見ながら比較検討できるポータルサイトを求めている。専門スタッフによる訪問ユーザーサポートがあるかについても、検索では得づらい情報であるため、項目に含まれているのは有用である」等の各製品・サービス情報に関する意見、「ユーザーの評価情報は非常に重要であり、評価数が多いほど情報の信頼性が高まる」等の各製品・サービスのユーザーの評価情報に関する意見、「資料ダウンロードが会員登録等なしに気軽に入手できる点が便利」等の各製品・サービスの詳しい情報 (詳細情報) に関する意見等が得られた。

また、「IPA が推奨する商品があるというのは心強い」、「ある程度信頼のおける機関が推奨する製品は効果が期待できる」、「第三者目線で客観的に比較しているので参考になる」、「政府関係機関が運用しているサイトは、経営者に受け入れてもらいやすい」等の運営主体側の信頼性に期待する意見等も見受けられた。

本設問は、問 13 の中小基盤の仮設サイトの検索機能の有用度合いについて、「かなり役に立つ」、「多少役に立つ」と回答した回答者を対象にした。

問 15 の「製品・サービスの各種情報について、サイバーセキュリティ製品・サービスの導入を検討する際に、役に立つと思われた具体的な理由や内容 (自由回答)」について、回答内容のうち、「図解がなく文字の羅列のため、読む気にならない。商品カタログを添付してほしい」、「想定される脅威と製品のカバー範囲等の視覚的な図が欲しい」、「IT 関連の用語には意味や概念が難解なものが多いため、用語解説やインシデント事例の解説等から必要

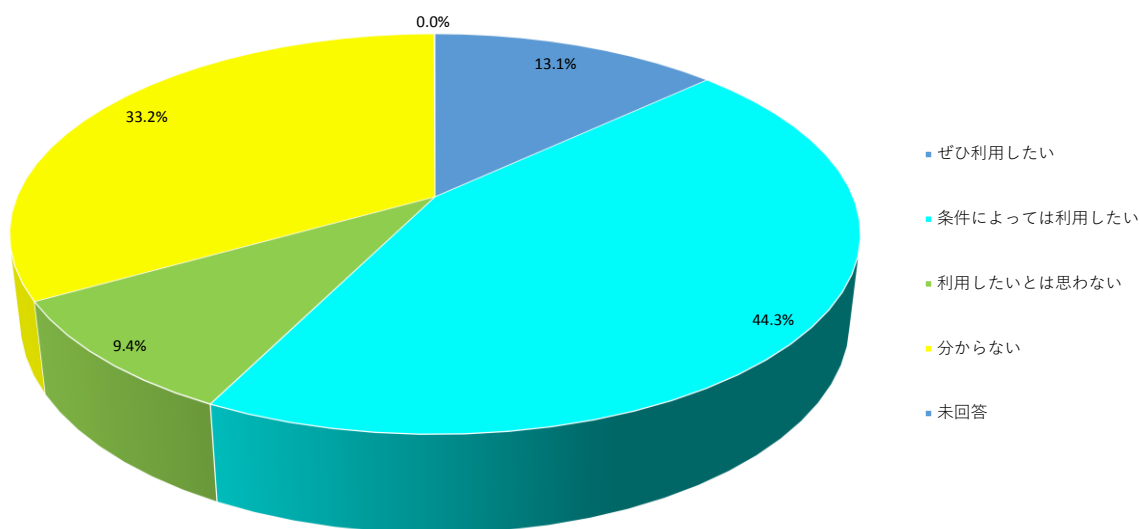
商材の提案をしてほしい」、「企業規模や予算に応じて、優先順位や社員の教育・訓練に関わる説明が欲しい」等の機能追加を希望する意見や、「なぜその対策が必要かの説明がないと、検討事項としての優先順位が下がる」、「このような特徴を持つ企業には、このような観点から製品・サービスを選ぶ必要があるというようなガイドラインを示してほしい」等のサイバーセキュリティ全般に係るリテラシー向上に資する情報提供を希望する意見等が挙げられた。

また、問 14 と同様に、「製品やサービスがどのように選定され、掲載されているか分からないため不安である」という運営主体側に信頼性や透明性を求める意見も見受けられた。

本設問は、問 13 の中小基盤の仮設サイトの検索機能の有用度合いについて、「あまり役に立たない」、「まったく役に立たない」、「分からない」と回答した回答者を対象にした。

問 16 の「中小基盤の本番サイトの利用意向」について、最も多い回答が「条件によっては利用したい」(44.3%)であった。次いで、「分からない」(33.2%)が多かった。以下「ぜひ利用したい」(13.1%)、「利用したいとは思わない」(9.4%)であった。

図表 3-38 中小基盤の本番サイトの利用意向(N=2,286)



問 17 の「サイバーセキュリティ製品・サービスの導入に際し、中小基盤の本番サイトを「条件によっては利用したい」と回答した回答者の条件内容（自由回答）」について、回答内容のうち、「紹介される製品のアイテム数の増加」、「具体事例の掲載と費用対効果案の掲載」、「周辺サービスの手厚さに関する情報の掲載」等の製品・サービスの掲載情報に関する意見や、「単一条件だけでなく複合条件検索の実現」、「中小基盤の困りごとからの検索」、「検索ワードの増加」等の製品・サービスの検索機能に関する意見や、「簡単な比較機能の搭載」、「画像やイラスト等によるわかりやすさの向上」等の視認性の向上に関する意見や、「フローチャートで自社に必要な製品・サービスを絞り込んでいく機能」の操作性の向上に関する

意見、「自社の課題が解決できる最適な製品・サービスかを判断できるガイダンスの提供」、「用語集の提供」、「解説、Q&A、コンサルティングサービス等のコンテンツ追加」、「中小企業が要求されるセキュリティを要素、種類、規模で分類または類型化し、それらの区分毎に推奨できる製品・サービスの公表」等の補助機能の充実に関する意見が得られた。

また、「IPA お墨付きの信頼できる製品・サービスの掲載」、「情報の確かさ、新しさ、公平性の担保」、「サービスの登録基準、掲載されている製品の掲載根拠等の明確化」、「公的な機関が選定したセキュリティ製品という安心感」、「中立的で技術力の有る機関が責任を持って対象製品・サービス等を評価し、その結果を公表すること」等の運営主体側や掲載情報の信頼性に期待する意見等も見受けられた。

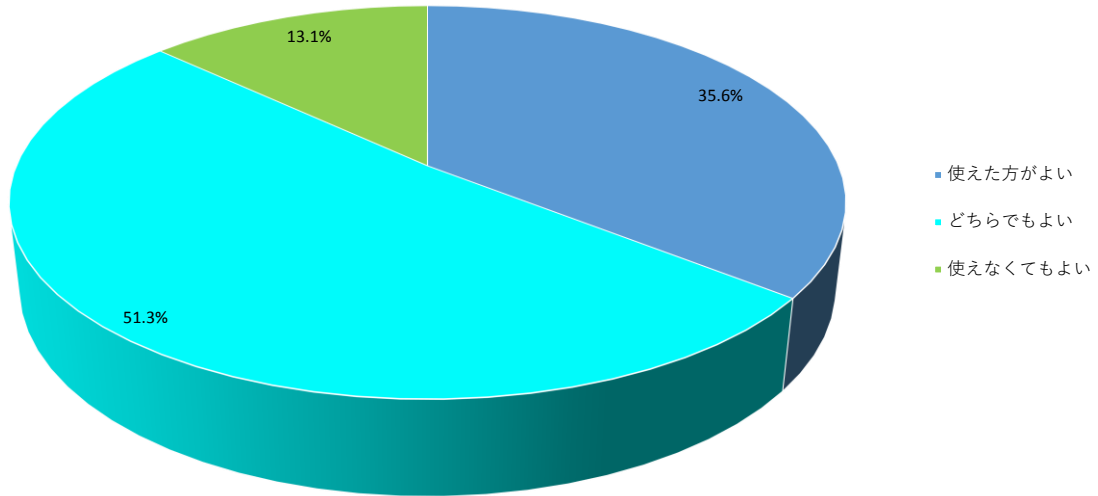
本設問は、問 16 の中小基盤の本番サイトの利用意向について、「条件によっては利用したい」と回答した回答者を対象にした。

問 18 の「サイバーセキュリティ製品・サービスの導入に際し、中小基盤の本番サイトを「利用したいと思わない」と回答した回答者の理由（自由回答）」について、回答内容のうち、「セキュリティ対策については業者、ベンダーに外注か委託している」、「掲載情報が初心者向けではなく理解が出来ないため」、「製品を選定、判断することが出来ない」等の意見が得られた。

本設問は、問 16 の中小基盤の本番サイトの利用意向について、「利用したいと思わない」と回答した回答者を対象にした。

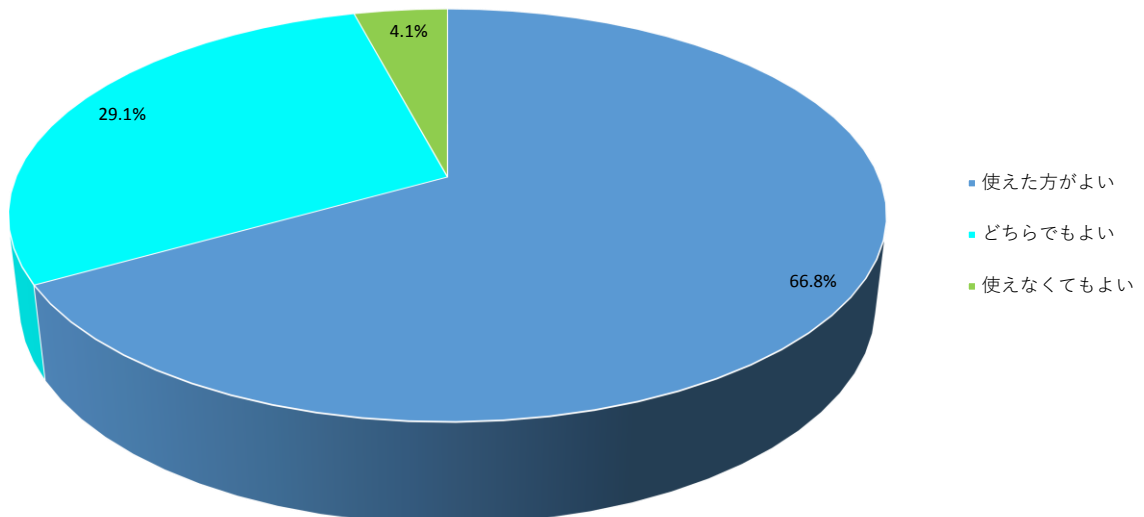
中小基盤の本番サイト上で提供してほしい機能のうち、問 19-①の「製品・サービスの評価情報を自らが書き込むことが出来る機能の需要度」について、最も多い回答が「どちらでもよい」(51.3%)であった。次いで、「使えた方がよい」(35.6%)、「使えなくてもよい」(13.1%)であった。

図表 3-39 中小基盤の本番サイト上で提供してほしい機能  
 (製品・サービスの評価情報を自らが書き込むことができる機能) (N=2,286)



問 19-②の「同じ種類の製品・サービスが複数掲載されている場合に、それぞれの特徴や機能を比較して表示できる機能の需要度」について、最も多い回答が「使えた方がよい」(66.8%)であった。次いで、「どちらでもよい」(29.1%)、「使えなくてもよい」(4.1%)であった。

図表 3-40 中小基盤の本番サイト上で提供してほしい機能  
 (同じ種類の製品・サービスが複数掲載されている場合に、それぞれの特徴や機能を比較して表示できる機能) (N=2,286)



問 20 の「中小基盤の仮設サイトから本番サイトへ更新していくにあたって、充実してほ



しい情報や追加してほしい機能、改善してほしい内容等（自由回答）」について、回答内容のうち、「機能比較の一覧表」、「IT、セキュリティ関連用語の説明」、「インシデント事例、被害事例、脅威等のわかりやすい事例からの製品紹介」、「業種、業界、規模ごとのおすすめポイントの掲載」、「販売店、ディストリビューターの情報」等の充実してほしい情報に関する意見や、「検索ワードの充実化」、「Q&A の設置」等の追加してほしい機能に関する意見が得られた。

また、「掲載情報の正確性」、「悪質な製品・サービスの排除」等の運営主体側や掲載情報の信頼性に期待する意見等も見受けられた。

## 4. セキュリティ製品・サービスの市場調査の結果

### 4.1. セキュリティ製品・サービスの市場調査に関するアンケートの実施

中小基盤の構築に関連して、市場に流通しているセキュリティ製品・サービスのうち、中小企業にも導入できる製品・サービスがどれくらいあるのか、また、製品・サービスベンダーが中小企業向けセキュリティ製品・サービスを提供する上で、どのような制約事項があるのか等を把握することを目的として、市場アンケート調査を実施した。

市場アンケート調査の実施概要を以下に示す。

- (1) 調査対象 : 特定非営利活動法人日本ネットワークセキュリティ協会 (JNSA) の会員企業 261 社 (2021 年 11 月 11 日時点) と、中小基盤にセキュリティ製品・サービスを掲載している製品・サービスベンダー 8 社 (双方の重複分 (4 社) を除いた社数) を合わせた 269 社
- (2) 実施時期 : 2021 年 12 月 7 日 (火) から 2022 年 1 月 6 日 (木) までの 31 日間
- (3) 調査手法 : Web アンケート調査 設問数 14 問
- (4) 有効回答数 : 27 サンプル

#### 4.1.1. アンケート項目の作成

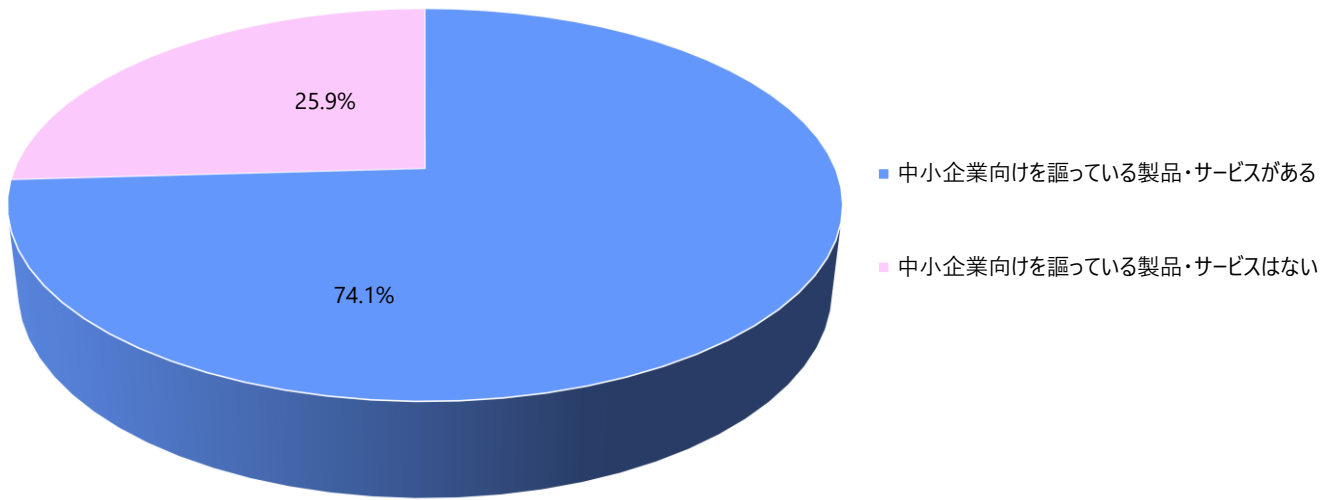
市場アンケート調査のアンケート項目については、有識者検討委員会の岩本委員 (JNSA) のご意見を参考に、調査仮説や設問文、各選択肢等について検討を行い、有識者検討委員会森井座長の確認のもと、取りまとめを行った。(市場アンケート調査の調査票は図表 2-2 を参照)

#### 4.1.2. アンケート結果の集計・分析

市場アンケート調査の結果 (有効回答数 : 27 サンプル) を以下に示す。

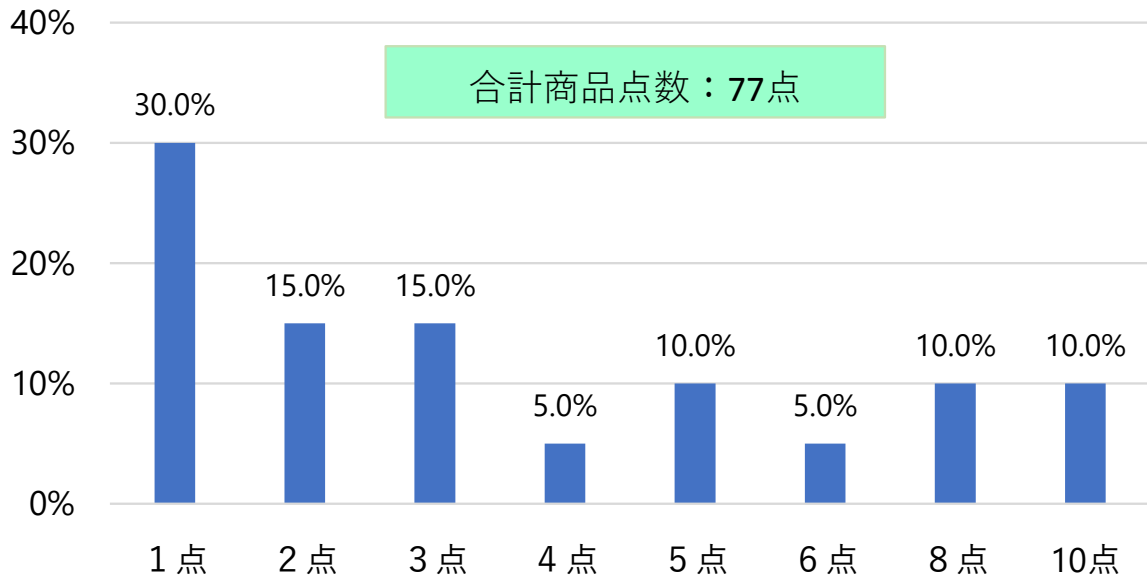
問 1 の「中小企業向けを謳っているセキュリティ製品・サービスの有無」について、20 社 (74.1%) が中小企業向けを謳っている製品・サービスがある、7 社 (25.9%) が中小企業向けを謳っている製品・サービスはないと回答した。

図表 4-1 中小企業向けを謳っているセキュリティ製品・サービスの有無 (N=27)



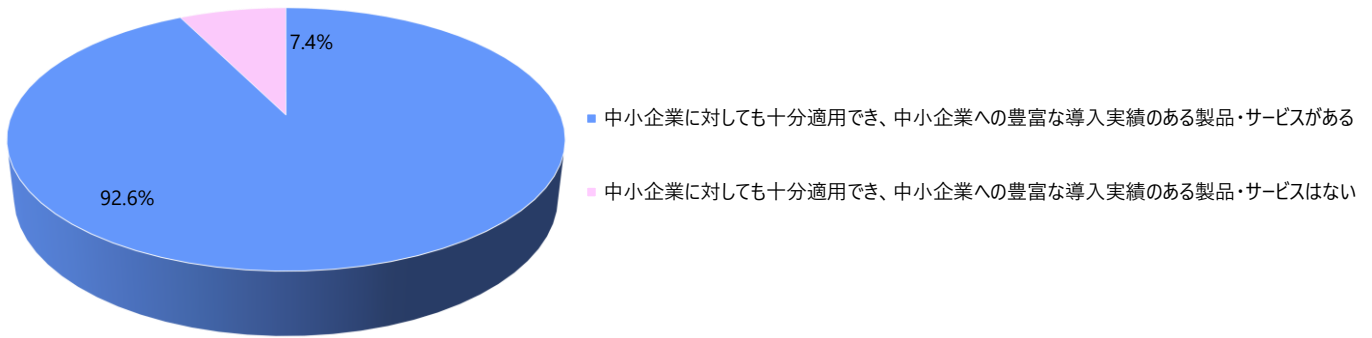
問1の「中小企業向けを謳っているセキュリティ製品・サービスの商品点数」について、6社(30.0%)が1点、3社(15.0%)が2点、3社(15.0%)が3点、1社(5.0%)が4点、2社(10.0%)が5点、1社(5.0%)が6点、2社(10.0%)が8点、2社(10.0%)が9点と回答し、ベンダー20社で合計77点であった。

図表 4-2 中小企業向けを謳っているセキュリティ製品・サービスの商品点数 (N=20)



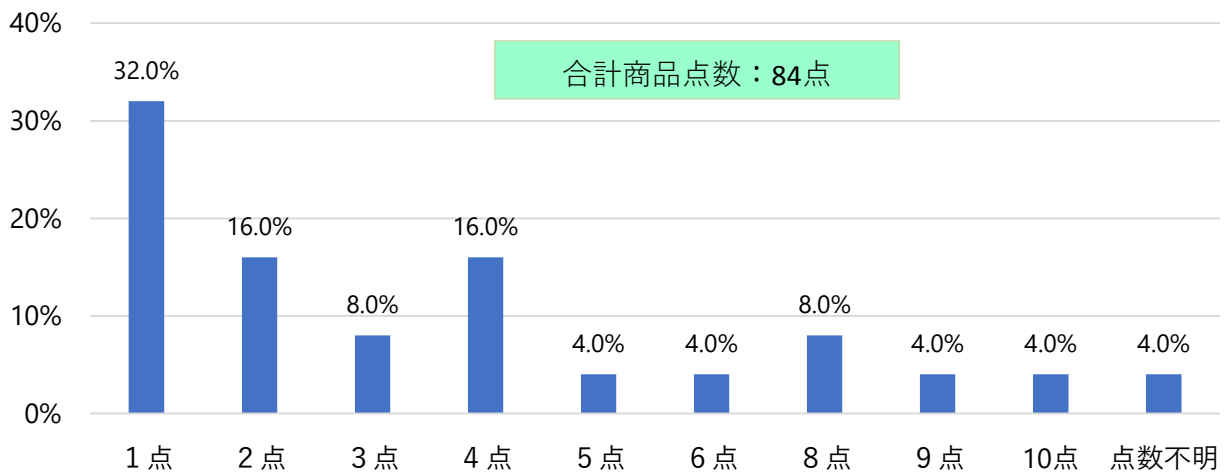
問2の「中小企業への豊富な導入実績のあるセキュリティ製品・サービスの有無」について、26社（92.6%）が中小企業に対しても十分運用でき、中小企業への豊富な導入実績のあるセキュリティ製品・サービスがある、1社（7.4%）が中小企業に対しても十分運用でき、中小企業への豊富な導入実績のあるセキュリティ製品・サービスはないと回答した。

図表 4-3 中小企業への豊富な導入実績のあるセキュリティ製品・サービスの有無(N=27)



問2の「中小企業への豊富な導入実績のあるセキュリティ製品・サービスの商品点数」について、8社（32.0%）が1点、4社（16.0%）が2点、2社（8.0%）が3点、4社（16.0%）が4点、1社（4.0%）が5点、1社（4.0%）が6点、2社（8.0%）が8点、1社（4.0%）が9点、1社（4.0%）が10点、1社（4.0%）が点数不明と回答し、ベンダー26社で合計84点であった。

図表 4-4 中小企業への豊富な導入実績のあるセキュリティ製品・サービスの商品点数(N=25)

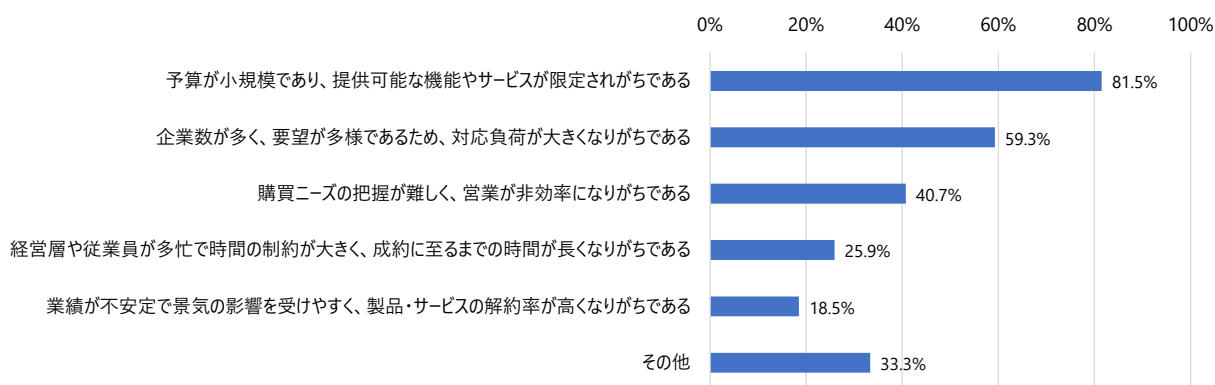


問3の「中小企業向けにセキュリティ製品・サービスの提供ビジネスを展開する上での障壁（複数回答可）」について、最も多い回答が「予算が小規模であり、提供可能な機能やサービスが限定されがちである」（81.5%）であった。次いで、「企業数が多く、要望が多様で

あるため、対応負荷が大きくなりがちである」(59.3%)が多かった。以下「購買ニーズの把握が難しく、営業が非効率になりがちである」(40.7%)、「経営層や従業員が多忙で時間の制約が大きく、成約に至るまでの時間が長くなりがちである」(25.9%)、「業績が不安定で景気の影響を受けやすく、製品サービスの解約率が高くなりがちである」(18.5%)と回答した。

「その他」の自由回答では、「セキュリティ対策に興味になさすぎる。情報リテラシーが低い」、「導入のための技術的理解度の低さ」、「利益が取れない(持ち出しになる可能性もあり、他サービスとのセット販売が必要になる)」、「親会社や大手取引先の利用している製品に左右されるために、顧客自身の要望にマッチしていても導入が難しい場合がある」、「例えば安くても、業務にプラスのものがなくなかなか導入に至らない」等の回答が得られた。

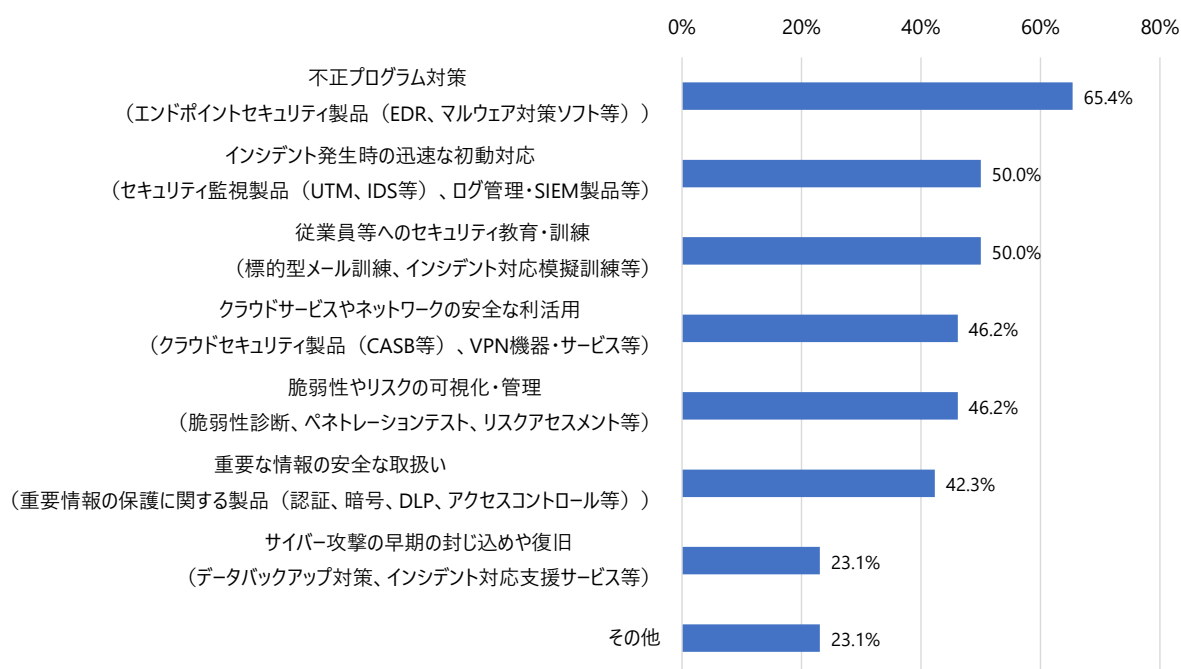
図表 4-5 中小企業向けにセキュリティ製品・サービスのビジネスを展開する上での障壁(N=27)



問4の「中小企業向けセキュリティ製品・サービスの分野(複数回答可)」について、最も多い回答が不正プログラム対策(エンドポイントセキュリティ製品(EDR、マルウェア対策ソフト等))(65.4%)であった。次いで、インシデント発生時の迅速な初動対応(セキュリティ監視製品(UTM、IDS等)、ログ管理・SIEM製品等)(50.0%)と、従業員等へのセキュリティ教育・訓練(標的型メール訓練、インシデント対応模擬訓練等)(50.0%)が多かった。以下、クラウドサービスやネットワークの安全な利活用(クラウドセキュリティ製品(CASB等)、VPN機器・サービス等)(46.2%)、脆弱性やリスクの可視化・管理(脆弱性診断、ペネトレーションテスト、リスクアセスメント等)(46.2%)、重要な情報の安全な取扱い(重要情報の保護に関する製品(認証、暗号、DLP、アクセスコントロール等))(42.3%)、サイバー攻撃の早期の封じ込めや復旧(データバックアップ対策、インシデント対応支援サービス等)(23.1%)と回答した。

「その他」の自由回答では、「IT資産管理ソフト」、「セキュアDNSサービス」、「メールの誤送信対策」、「脆弱性対策、サーバ対策製品」、「内部ネットワークにおける対策、内部拡散防止」、「認証基盤」との回答が得られた。

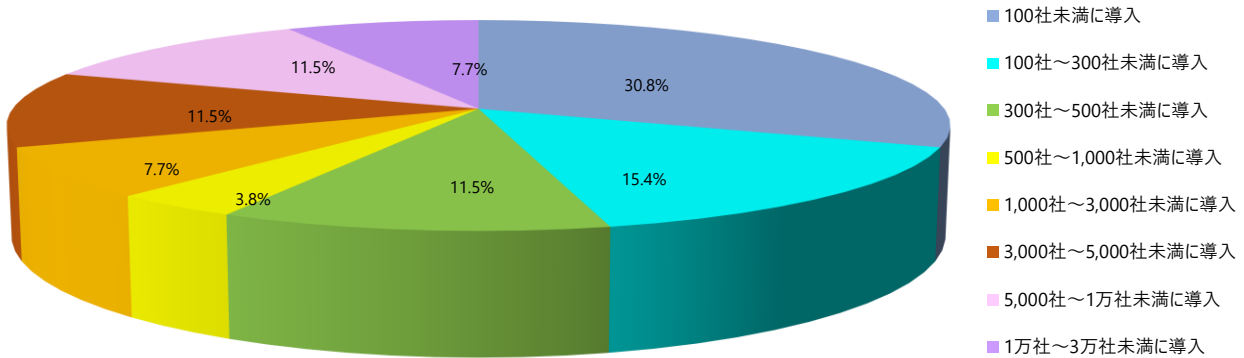
図表 4-6 中小企業向けセキュリティ製品・サービスの分野(N=26)



問5の「セキュリティ製品・サービスの名称、技術面・機能面の特徴等」について、アンケート回答ベンダーの取扱い製品・サービスの名称、技術面・機能面の特徴等を記載いただいた。(中小基盤の仮設サイトの掲載製品・サービスベンダー10社がアンケート回答)

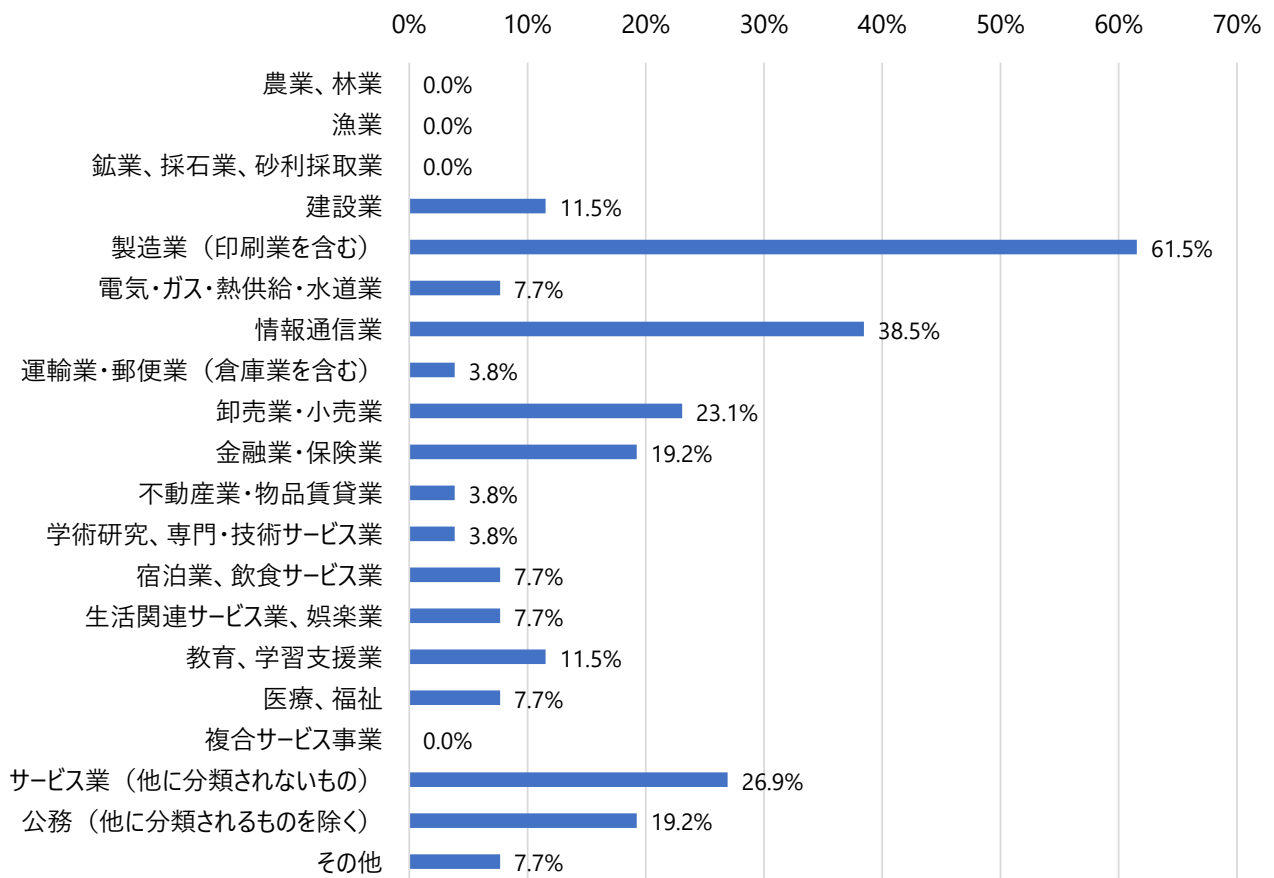
問6の「セキュリティ製品・サービスの中小企業ユーザーへの導入実績」について、最も多い回答が100社未満に導入(30.8%)であった。次いで、100社~300社未満に導入(15.4%)が多かった。以下、300社~500社未満に導入(11.5%)、3,000社~5,000社未満に導入(11.5%)、5,000社~1万社未満に導入(11.5%)が並び、1,000社~3,000社未満に導入(7.7%)、1万社~3万社未満に導入(7.7%)、500社~1,000社未満に導入(3.8%)と回答した。セキュリティ製品・サービスの中小企業ユーザーへの導入実績については、約半数が、導入社数300社未満、約6割が導入社数500社未満にとどまっていた。

図表 4-7 中小企業向けにセキュリティ製品・サービスのビジネスを展開する上での障壁(N=26)



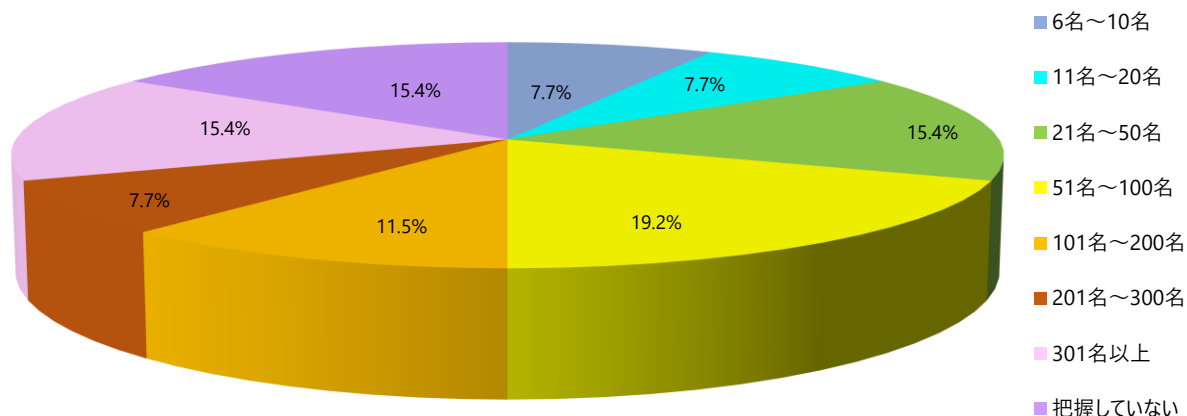
問7の「中小企業ユーザーにおけるボリュームゾーンの業種（上位3業種）」について、最も多い回答が製造業（印刷業を含む）（61.5%）であった。次いで、情報通信業（38.5%）が多かった。以下、サービス業（他に分類されないもの）（26.9%）、卸売業・小売業（23.1%）となった。

図表 4-8 中小企業ユーザーにおけるボリュームゾーンの業種(上位3業種)(N=26)



問8の「中小企業ユーザーにおけるボリュームゾーンの従業員規模（上位1区分）」について、最も多い回答が51名～100名（19.2%）であった。次いで、21名～50名（15.4%）、301名以上（15.4%）、把握していない（15.4%）が並んで多かった。以下、101名～200名（11.5%）と回答した。中小企業ユーザーにおけるボリュームゾーンの従業員規模については、約半数が、従業員規模100名以下であった。

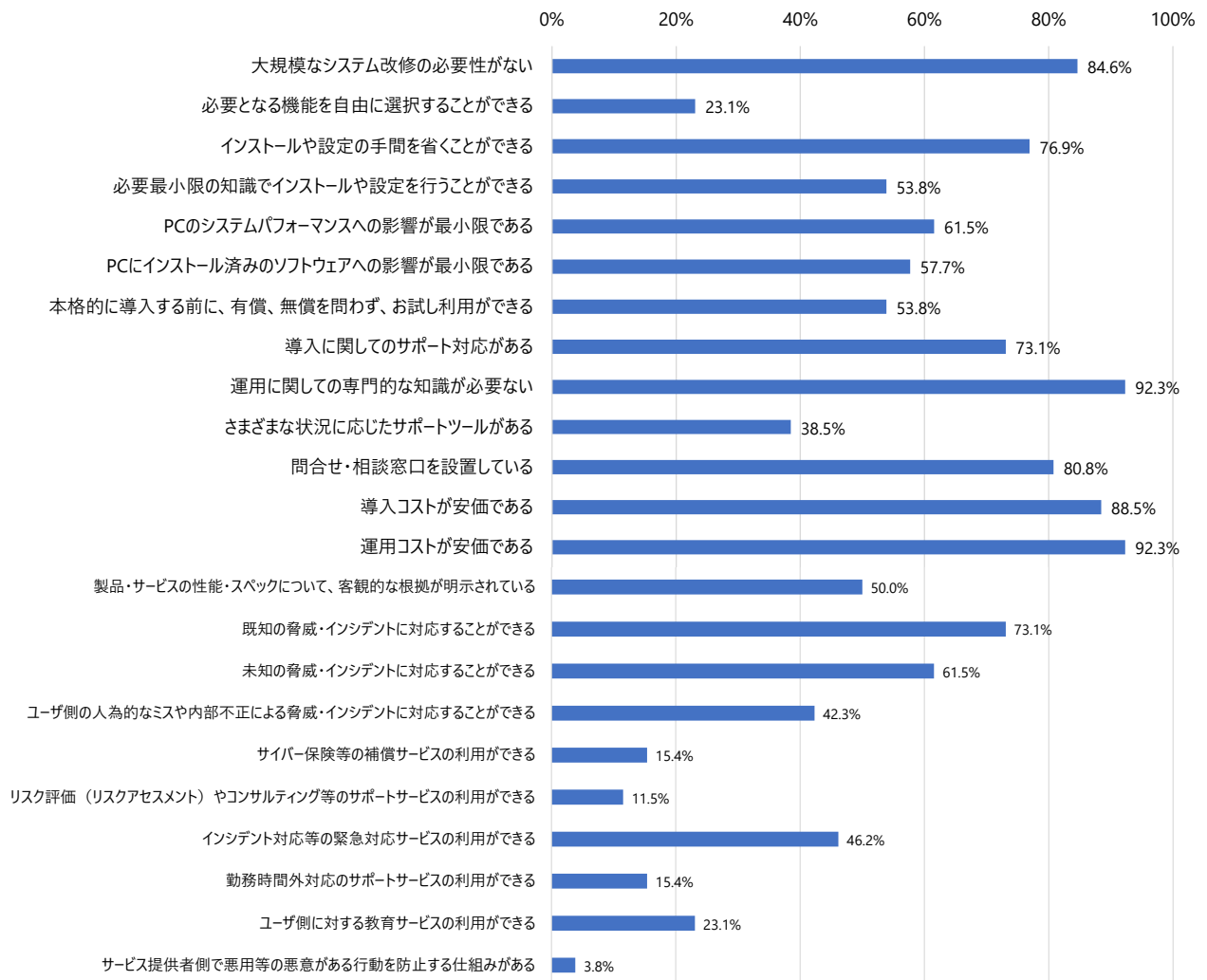
図表 4-9 中小企業ユーザーにおけるボリュームゾーンの従業員規模(上位1区分)(N=26)



問9の「中小企業ユーザーが製品・サービス選びで重視している評価項目のうち、中小企業ユーザーに訴求している項目（複数回答可）」について、最も多い回答が「運用に関しての専門的知識が必要ない」（92.3%）と、「運用コストが安価である」（92.3%）であった。次いで、「導入コストが安価である」（88.5%）が多かった。以下「大規模なシステム改修の必要性がない」（84.6%）、「問合せ・相談窓口を設置している」（80.8%）と回答した。導入・運用のし易さ、運用時や導入時に要する費用に関わる評価項目については、中小企業ユーザーへの訴求度が相対的に高かった。一方で、導入や運用における課題の解決や、製品・サービスに付帯するオプションサービスその他に関わる評価項目については、中小企業ユーザーへの訴求度が相対的に低かった。

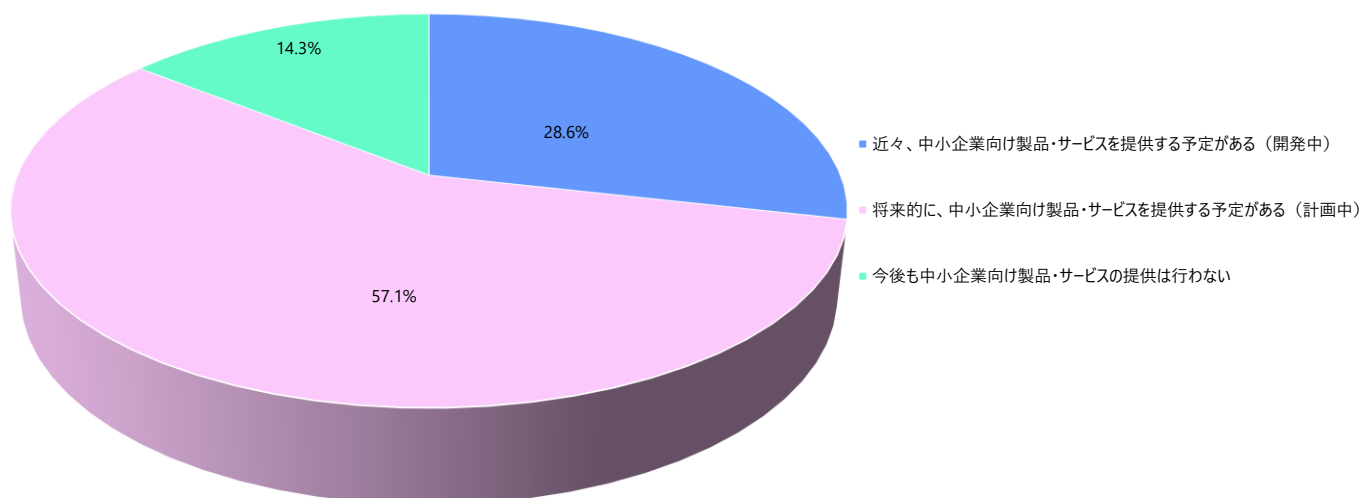


図表 4-10 中小企業ユーザーが製品・サービス選んで重視している評価項目のうち、  
中小企業ユーザーに訴求している項目 (N=26)



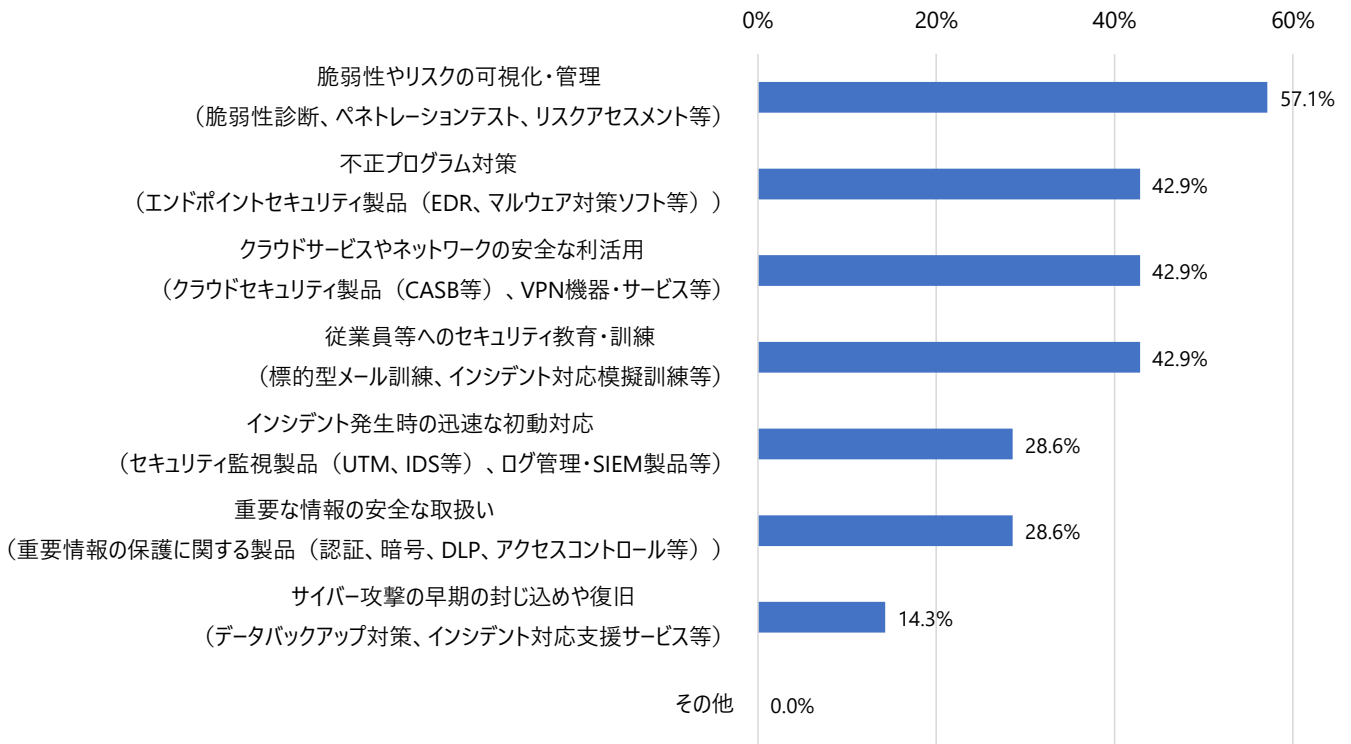
問 10 の「中小企業向けセキュリティ製品・サービスを提供する予定」について、最も多い回答が、「将来的に、中小企業向け製品・サービスを提供する予定がある (計画中)」(57.1%) であった。次いで、「近々、中小企業向け製品・サービスを提供する予定がある (開発中)」(28.6%) が多かった。「今後も中小企業向け製品・サービスの提供は行わない」(14.3%) は 1 社であり、中小企業向けを謳っているセキュリティ製品・サービスを提供していないベンダー 7 社のうち、6 社が中小企業向けセキュリティ製品・サービスの提供について開発中または計画中であった。

図表 4-11 中小企業向けセキュリティ製品・サービスを提供する予定(N=7)



問 11 の「提供予定のセキュリティ製品・サービス分野（複数回答可）」について、最も多い回答が、脆弱性やリスクの可視化・管理（脆弱性診断、ペネトレーションテスト、リスクアセスメント等）（57.1%）であった。次いで、不正プログラム対策（エンドポイントセキュリティ製品（EDR、マルウェア対策ソフト等））（42.9%）、クラウドサービスやネットワークの安全な利活用（クラウドセキュリティ製品（CASB 等）、VPN 機器・サービス等）（42.9%）、従業員等へのセキュリティ教育・訓練（標的型メール訓練、インシデント対応模擬訓練等）（42.9%）が並んで多かった。以下、インシデント発生時の迅速な初動対応（セキュリティ監視製品（UTM、IDS 等）、ログ管理・SIEM 製品等）（28.6%）、重要な情報の安全な取扱い（重要情報の保護に関する製品（認証、暗号、DLP、アクセスコントロール等））（28.6%）と回答した。

図表 4-12 提供予定のセキュリティ製品・サービス分野(N=7)



問 12 の「ヒアリング協力の可否」について、16 社が「協力してもよい」、5 社が「条件によっては協力してもよい」、6 社「協力は難しい」と回答した。

#### 4.2. セキュリティ製品・サービスの市場調査に関するヒアリングの実施

市場アンケート調査の結果を踏まえ、さらに深掘した情報を把握するため、市場アンケート調査において、ヒアリングへの協力について承諾をいただいたベンダー16 社のうち、企業規模等を考慮した上で5 社を選定し、2022 年1 月14 日(金) から2022 年1 月18 日(火) の期間で、Web 会議によるベンダーヒアリング調査を実施した。

ヒアリング対象の5 社は、ベンチャー企業・中小企業区分から2 社、中堅企業区分から1 社、大企業区分から2 社を選定した。

ヒアリング対象のベンダーが取り扱う中小企業向けセキュリティ製品・サービス及び中小企業への導入実績がある製品等の概要を以下に示す。

図表 4-13 ヒアリング対象のベンダーが扱う中小企業向けセキュリティ製品・サービス及び

中小企業への導入実績がある製品等の概要

	A社	B社	C社	D社	E社
セキュリティ製品・サービスの種類	主な製品はクラウド型 WAF	主な製品はスイッチ	主な製品はエンドポイントセキュリティ	主な製品は IT 資産管理	主な製品は暗号化
導入実績	1,000～3,000社未満	3,000～5,000社未満	100社未満	100～300社未満	100～300社未満
ボリュームゾーンの顧客（中小企業ユーザー）	[業種] 業種問わず [従業員規模] 把握していない	[業種] 卸売業・小売業、学術研究、専門・技術サービス、医療・福祉 [従業員規模] 11～20名	[業種] 製造業、金融・保険業、公務 [従業員規模] 51～100名	[業種] 製造業、情報通信業、サービス業 [従業員規模] 把握していない	[業種] 製造業、卸売業・小売業 [従業員規模] 201～300名

#### 4.2.1. ヒアリング項目の作成

セキュリティ製品・サービスの市場調査に関するヒアリング項目の作成においては、事務局で調査仮説や設問文について検討を行い、取りまとめを行った。

セキュリティ製品・サービスの市場調査に関するヒアリング項目を以下に示す。

- (1) 中小企業向けセキュリティ製品・サービスの市場構造
- (2) 中小企業向けセキュリティ製品・サービスのビジネス拡大に向けた課題
- (3) 中小基盤上で中小企業向けに提供が必要となる機能等

#### 4.2.2. ヒアリング結果の分析

ベンダーヒアリング調査のヒアリング結果と分析を以下に示す。

##### 4.2.2.1. 中小企業向けセキュリティ製品・サービスの市場構造

ベンダーヒアリング調査で得られた情報では、中小企業向けセキュリティ製品・サービスについて、ビジネスとして成立しているベンダーの例や、積極的に営業を行っているベンダーの例はあまり多く聞かれなかった。ランサムウェア対策等により、中小企業のセキュリティ意識は年々高まっているとの意見があるものの、市場拡大のスピードは緩やかであり、中小企業におけるセキュリティ製品・サービスの普及には、まだ時間がかかるとの見解を持つベンダーが多かった。

しかしながら、技術革新やビジネスモデル革新（クラウド型、サブスクリプション型）が促進することによる製品価格の低価格化の実現については、今後中小企業の製品導入に繋がる一定の効果が見込めるという意見が得られた。

以下、中小企業向けセキュリティ製品・サービスの市場構造についてのヒアリング内容を示す。

[A 社]

- ・ セキュリティ業界において、①クラウド型/SaaS型サービスの展開、②サブスクリプション型ビジネスの展開という2つの動きが進んでおり、導入・運用面、費用面の双方からみて中小企業がセキュリティ製品・サービスを導入しやすい環境が整ってきている。

[B 社]

- ・ 中小企業におけるセキュリティ製品・サービスの普及には、まだ時間がかかる。ビジネスになっていない。(ただし、直近のビジネスは右肩上がり)
- ・ 取扱い製品のユーザーの80%が中小企業ユーザーである。

[C 社]

- ・ 大手企業と取引する上で導入が求められるセキュリティ対策についても、仕方なく導入しているという意識が強い。
- ・ 中小企業は、セキュリティ投資に前向きではなく、コストをかけて営業をかけたとしても、導入社数の規模が大きくなることもあり、中小企業への積極的なアプローチは考えていない。

[D 社]

- ・ 中小企業のセキュリティ意識が年々高まっており、提案の価格帯が中小企業のニーズに合致し、手厚いサポートが付いているセキュリティ製品・サービスであれば、中小企業においても活用されやすいと考えている。

[E 社]

- ・ 市場の伸びは微増である。中小企業におけるランサムウェア対策が市場の拡大を牽引している。
- ・ リテラシーの違いから中小企業とベンダーとの間で会話が成立せず、営業活動が非効率となるため、中小企業向けのセキュリティビジネスは、ボランティアな企業活動と

いう側面が強い。

#### 4.2.2.2. 中小企業向けセキュリティ製品・サービスのビジネス拡大に向けた課題

ベンダーヒアリング調査で得られた情報では、中小企業向けセキュリティ製品・サービスのビジネス拡大の課題について、製品・サービスは、中小企業の支払い可能費用を強く意識しつつ、中小企業でも構築・運用しやすいもの（エンドポイントセキュリティや EDR、「防御」を中心の製品、ポリシー設定決め打ちのワンタッチ製品等）とすることが重要だという意見が多く見受けられた。販売方法は、販売店や代理店との協業が不可欠だが、代理店からはサポートに手がかからない製品・サービスが求められるという傾向が把握された。また、サポートに関する中小企業からの問合せはほとんどないが、これは製品導入後、放置された状態が多いこと示唆しており、障害が起きた時のみ連絡が入るケースが多いとの意見があった。

以下、中小企業向けセキュリティ製品・サービスのビジネス拡大の課題についてのヒアリング内容を示す。

[A 社]

○製品・サービス

- ・ コスト重視の中小企業と安全重視のベンダーとで親和性がない点を考慮すると、80点程度のレベルで双方の満足が得られる製品の提供が重要である。

○販売方法

- ・ 中小企業側のリテラシーが低く、またベンダー側の製品紹介は分かりにくいいため、中小企業は製品選びにおいて適切な判断ができてないとの懸念がある。

○サポート

- ・ 設定や更新の作業を中小企業に任せると、製品導入後に放置された状態になるため、気づかないうちに攻撃され、導入自体の意味がなくなってしまうことがある。

[B 社]

○製品・サービス

- ・ UTM や SIEM による脅威検出は、導入・運用費用が、中小企業側の予算感に合わない。エンドポイントセキュリティや EDR のような導入しやすい価格帯の製品の提供が重要である。

○販売方法

- ・ 中小企業側は、セキュリティ製品の内容についての理解度も低いため、販売店経由でサポートに手がかからない製品・サービスの提供が必要である。

#### ○サポート

- ・ 販売店経由で製品等を提供すると、中小企業が製品等の導入・運用において何を困っているのかといった情報が入ってこない。
- ・ 中小企業からの問合せは、何か障害が起きた時のみ連絡が入る。

#### [C社]

##### ○製品・サービス

- ・ 中小企業の支払い可能な費用を考慮すると、多層防御は困難であり、NIST の CSF の「防御」を中心として、インシデントを発生させない製品の提供が重要である。

##### ○販売方法

- ・ 営業コストをかけられないため、代理店との協業が不可欠である。ただし、代理店は中小企業に対して売れる製品しか売らないというのが現状である。

##### ○サポート

- ・ 製品サポートに関する中小企業からの問合せはほとんどないが、何か起きると、名刺の連絡先などの属人的な繋がり、営業時間内・外を問わず、担当者に連絡が入る。

#### [D社]

##### ○製品・サービス

- ・ 中小企業にとって必要な製品は多岐にわたるが、提案の価格帯が合わないと導入してもらえないため、基本サービスとオプションサービスに分けて提供できるようにすることが重要である。

##### ○販売方法

- ・ 全国に分散する2千名の営業員が販売しているが、提案しても、中小企業からの質問に答えられない営業員や、質問に答えられないから提案しない営業員もいるため、教育が課題になっている。

##### ○サポート

- ・ 中小企業にとっては製品導入がすべてであり、取引先に導入完了という報告さえできればよい。中小企業では、更新作業等を行っていないため、過去に製品を導入したことを忘れてしまっている場合がある。

#### [E社]

##### ○製品・サービス

- ・ 構築ポリシー設定等が必要となる製品は、提案の価格帯が合わないので、中小企業には簡単に導入・運用できるワンタッチ製品（ポリシー設定の決め打ち等）しか導入さ

れない。

#### ○販売方法

- ・ 100 件営業して、成約は 1~2 件程度にとどまるため、営業効率が極端に悪い。また、全国に拠点がないため、製品の販売・導入は地域の代理店との協業が不可欠である。

#### ○サポート

- ・ サポートに関する中小企業からの問合せはほとんどない。運用実績のレポートを取引先への報告資料として活用できれば安心する。
- ・ 業界ごとにインフラサービスとして提供できるようにすることが重要である。

### 4.2.2.3. 中小基盤上で中小企業向けに提供が必要となる機能等

ベンダーヒアリング調査で得られた情報では、中小基盤上で中小企業向けに必要な機能等について、中小基盤上で提供する製品・サービス情報が中小企業に理解できるようにするための標準フォーマットの作成や、中小企業が取っ付きやすくする工夫が必要という意見があった。また、中小企業向けセキュリティ製品・サービスを扱う代理店の紹介情報や販売地域の検索など、中小基盤を活用してもらうための仕掛けも求められている。加えて、業界ガイドラインと製品の紐づけ等の工夫が必要との意見があった。

以下、中小基盤上で中小企業向けに必要な機能等についてのヒアリング内容を示す。

#### [A 社]

- ・ ベンダーが提供する製品説明用の資料は、ベンダーごとに記載の内容や粒度、書きぶり等が大きく異なる。まずは、製品説明用の資料について、簡潔にポイントをまとめるような標準フォーマットを提供することが重要である。
- ・ 中小企業が取っ付きやすいようにマンガを入れたり、ツイッターや動画を活用したりするような工夫も必要である。

#### [B 社]

- ・ 製品を導入・運用するにあたって、ユーザー側で準備しなければならないものが何であるかを、中小企業にきちんと伝えることが重要である。
- ・ パスワードの強度を高めることや、ソフトウェアのアップデートによる脆弱性対策を行う等、新たな製品を導入しなくても、中小企業において出来る対策は幾つもある。そのような情報を提供することも重要である。

#### [C 社]

- ・ 中小基盤について、中小企業にどのように告知していくのが重要となる。



- ・ 代理店がビジネスを展開する上で、中小基盤を活用できるようにすることが重要である。

[D 社]

- ・ 業界のガイドラインで求められる対策と、当該対策を実現する上で導入すべき製品を相互に紐づく形で、製品情報が提供されることが重要である。

[E 社]

- ・ 製品の提供が可能であるかを明らかにするため、協業している代理店（SIer 含む）の情報や、当該代理店の販売地域に関する情報を提供することが重要である。
- ・ サイバーセキュリティ経営ガイドラインの実践のためのプラクティス集のような記載のレベルで、業種ごとに、同業他社の対策事例を紹介する情報を提供することも重要である。

## 5. 中小基盤の有用性検証及び構築上の課題洗い出し

「3. 試行環境調査の結果」、「4. セキュリティ製品・サービスの市場調査の結果」を踏まえ、中小基盤の有用性検証及び構築上の課題の洗い出しを行った。将来的な中小基盤の構築に向けた検討課題については、有識者検討委員会において議論を行い、専門的な視点から助言を得た。

### 5.1. 中小基盤の有用性に関する全体評価

中小基盤の仮設サイトに対する有用性評価アンケートの回答者（2,286件）のうち、セキュリティ製品・サービスの導入検討において、中小基盤の仮設サイト上に掲載されている情報が役に立つかの質問に対し、「かなり役に立つ(6.8%)」、「多少役に立つ(41.4%)」との回答があったものの、「分からない」とする回答も3割を超えるなど、有用性の観点では一定の潜在的なニーズがあることが確認されたにとどまった。

また、中小基盤の本番サイトの利用意向については、有用性評価アンケートの回答者の約6割が利用する可能性があると回答（「ぜひ利用したい(13.1%)」と、「条件によっては利用したい(44.3%)」を合計した割合）しているものの、利用する条件として「信頼できる製品、サービスの掲載」、「情報の確かさ、新しさ、公平性の担保」等、中小基盤に掲載する製品・サービスの品質等に係る検証・評価を前提としたコメントも多く含まれており、本番サイトの利用意向は構築仕様に依るところと思われる。

一方、中小企業向けセキュリティ製品・サービスのベンダー側からみた状況について、今回実施した市場アンケート調査（JNSA 会員企業を中心にアンケート依頼社数 269 社のうち 27 社から回答）では、ベンダーが中小企業向けにセキュリティビジネスを展開していく上での障壁として、「予算が小規模で提供可能な機能やサービスが限定されがち」、「企業数が多く、要望が多様であるため対応負荷が大きくなりがち」といった事項を挙げる回答が多く、アンケート回答ベンダーへの個別ヒアリング調査（5社）の結果からも、中小企業向け市場を拡大させるためには少なからず課題があるとベンダー側が捉えているという傾向が見られた。

### 5.2. 中小基盤に求められる要件の整理

「3. 試行環境調査の結果」から、中小基盤のターゲットユーザー、サイト構成、掲載する情報、検索機能等について考察を行い、中小基盤に求められる要件の整理を行った。

#### 5.2.1. 中小基盤のターゲットユーザー

当初「製品導入の目利きが自力でできる企業」としての IT や情報システム、情報セキュ

リティの担当者を主なターゲットユーザーと想定していたが、有用性評価アンケートに回答した約7割が「経営層」、「管理部門、営業部門、商品開発・設計部門の担当者」であったことから、これらの層もターゲットユーザーから排除しない方が望ましいと考えられる。

### 5.2.2. 中小基盤のサイト構成

有用性評価アンケートに回答した者の約2割が、サイトの分かりやすさや使い勝手に関する不満点として、「ホームページの構成や各ページの表示内容の全体像が分かりにくい」を挙げている。このため、情報セキュリティに関するリテラシーが十分ではないユーザー向けに、サイトの構成や、各ページの表示内容の全体像、情報提供機能や検索機能等の使い方について説明するページを作成すると効果的であると考えられる。

### 5.2.3. 中小基盤に掲載する製品情報の内容

中小基盤に掲載する情報としては、掲載製品・サービスの一覧情報や、製品・サービスの初期導入コスト、年間ランニングコストに関する費用面の記載、導入に関する実績面の記載について中小企業の関心が高い。

掲載製品・サービスの一覧情報については、表示の順番が情報閲覧に影響を与えないよう、製品・サービス一覧における適切な表示方法について考慮する必要がある。また、実績面の記載については、提供情報の陳腐化が情報閲覧に影響を与えないよう、実現可能性にも配慮しつつ情報の適切な更新方法について考慮することが望ましい。

### 5.2.4. 中小基盤に掲載する製品情報の質

ベンダーより提供される製品・サービス情報については、記載の粒度や書きぶり、情報量の同質性担保を図るため、登録申請書の記載方法に関する標準フォーマットを作成したが、この点、有用性評価アンケートにおいては専門用語が多くて分かりにくい等のコメントが寄せられ、中小企業への理解しやすさへの配慮が必ずしも十分でないケースがあった。このため、ベンダーから登録申請書を受け付ける段階での、文章の構成や表現等の質的管理を図ることが重要と考えられる。

### 5.2.5. 中小基盤に掲載する製品情報以外の情報

中小企業向けビジネスにおいては、製品・サービスの営業や導入サポートを、協業する代理店経由で行うケースが多いことから、中小基盤に掲載の製品・サービスにおいても、営業対象エリアを含めた代理店情報も併せて掲載すると、中小企業ユーザーにとって使いやすいものになると考えられる。

なお、一次代理店や二次代理店等を含む代理店の定義や代理店情報に含める情報と中小基

盤への掲載方法については別途検討する必要があると考えられる。

#### 5.2.6. 中小基盤上で提供する検索機能

中小企業ユーザーによる検索は、「製品・サービスの種類」、「予算規模（初期導入コスト、ランニングコスト）」、「従業員規模」、「注目ワード」を検索条件として設定することが多く、複数の条件設定による高度な検索の要望もあるため、このような基礎的なニーズを満たすことで、中小企業ユーザーにとって使いやすいものになると考えられる。なお、「注目ワード」による検索を可能とするにあたっては、新たなキーワードを設定する際のルールや方法について留意する必要がある。

### 5.3. 中小基盤の構築に向けた検討課題

今後、中小基盤を構築するとした場合に留意すべき観点として、以下に示す4つの観点を設定し、「3. 試行環境調査の結果」、「4. セキュリティ製品・サービスの市場調査の結果」を踏まえ、それぞれの観点からみた中小基盤の構築に向けた検討課題の洗い出しを行った。抽出した検討課題は有識者検討委員会に諮り、専門的な視点から示唆や意見を得た。

<課題検討の観点>

- ・ 中小基盤環境の構築（設置場所及び運営主体）
- ・ 中小企業のアクセス促進に繋がる仕組み
- ・ 製品・サービスの応募促進に繋がる仕組み
- ・ 事業告知及びプロモーション手段

#### 5.3.1. 中小基盤環境の構築（設置場所及び運営主体）

有用性評価アンケート回答の一部において、IPAが中小基盤の中小企業向けセキュリティ製品・サービスの情報に対してお墨付きを付与していることを前提としたコメント、あるいはそれを求める趣旨のコメントが寄せられており、中小基盤の運営主体の信頼性に対する期待があるといえる。

また、市場調査におけるベンダーヒアリングでは、中小企業の実態にそぐわない製品・サービスを提供しているベンダーがあるのではないかと考えている中小企業が少なからずある、とのコメントも寄せられた。

以上の点について、調査結果をもとに有識者検討委員会にて議論が行われ、以下の意見が示された。

##### 【有識者検討委員会で示された意見】

- 運営主体の信頼性に対する期待については、信頼性の担保の仕方によっては、情報に誤りがあった際に運営主体側において責任を負わなければならない、場合によっては市場を歪めてしまうおそれもあることから、お墨付きを与えるにしても、どのレベルのお墨付

きを与えるのかまで慎重に検討する必要がある。

- 正確性を担保することと、信頼性を担保することは別である。正確性の担保にあたっては情報の真偽を確認すれば足りるが、信頼性の担保にあたっては、情報セキュリティの製品・サービス等のソリューションや脅威は進化が著しいこともあり、中立・公正の評価を実施するのは非常に難しい。
- 中小基盤の目的は、中小企業において容易にセキュリティ製品・サービスを検索できるようにすることであると認識しているため、有用性や信頼性のハードルが高くなりすぎてしまうことにも懸念がある。
- 粗悪もしくは悪意のある事業者の製品・サービスを掲載しないことは重要だと思うが、それ以上の確からしさを保証するのは難しいのではないかと。最低限、粗悪もしくは悪意のある事業者を外し、誓約書を収集する等の対応で十分ではないかと考える。

### 5.3.2. 中小企業のアクセス促進に繋がる仕組み

中小基盤へのアクセス促進については、セキュリティ製品・サービスの導入検討や選定を行う中小企業を中小基盤に誘導する仕組みを検討する必要がある。多数の中小企業による中小基盤へのアクセスがあることは、製品・サービスベンダーにとっても中小基盤への掲載情報の提供にあたってのインセンティブにもなり得る。

以上の点について、調査結果をもとに有識者検討委員会にて議論が行われ、以下の意見が示された。

#### 【有識者検討委員会で示された意見】

- 中小企業において、どのようなセキュリティ対策が必要かを判断、もしくは製品・サービスを選定する上で自社にとって効果的かを判断するのが難しい、という出発点に立ち返ると、「SECURITY ACTION」制度や「サイバーセキュリティお助け隊サービス」事業とも連携して検討を進めるのが適当ではないか。それぞれの事業ごとに性質は異なるものの、中小企業に対してセキュリティ対策を普及するのであれば、中小基盤だけではなく、一体的に周知するポータルサイトの仕組みも選択肢として考えられる。
- サプライチェーンを構成する大企業や業界団体も、中小企業のセキュリティ対策について同じ問題意識を有しているはずなので、大企業や業界団体とも連携して、中小企業のセキュリティ対策の底上げを実施することを検討しても良いと考えられる。例えば、中小企業とも取引のある大企業・業界団体とも連携の上、中小基盤に掲載する製品・サービスを選定することで、中小企業向けの製品・サービスの情報源としての魅力が上がるのではないかと。

### 5.3.3. 製品・サービスの応募促進に繋がる仕組み

今回の試行環境調査では、「製品・サービスの評価情報の提出」はベンダー公募条件とされており、当該製品・サービスに係る中小企業ユーザー2社分の評価情報を提出することが実施内容に含まれていたところ、情報提供が難しいベンダーからの応募辞退があり、中小基盤への製品・サービス掲載のハードルの一つとなっていた。この点、「製品・サービスの評価情報」を含め、情報提供量の多さが中小基盤に掲載する製品・サービスの応募促進の妨げになる可能性があると考えられる。

他方で、中小基盤の仮設サイトに対する有用性評価アンケートでは、中小基盤に掲載された情報の量や種類、記述内容に関する不満は多くなく、初期導入コスト、年間ランニングコストに関する費用面の記載、導入に関する実績面の記載が製品・サービスの検討に役立つとのコメントが多かったことを考慮すると、中小基盤の構築にあたっては製品・サービスベンダーに対して一定量の情報提供を求めるニーズがあると考えられる。

中小企業向けセキュリティ製品・サービスの市場調査においては、中小企業向けセキュリティビジネスを拡大させるためには少なからず課題があるとベンダー側が考えているという傾向が見られた。また、ランサムウェア対策等により、中小企業のセキュリティ意識は年々高まっているとの見方があるものの、市場拡大のスピードは緩やかであり、中小企業におけるセキュリティ製品・サービスの普及にはまだ時間がかかるとの見解があった。

以上の点について、調査結果をもとに有識者検討委員会にて議論が行われ、以下の意見が示された。

#### 【有識者検討委員会で示された意見】

- 中小基盤への製品・サービス掲載のハードルについて、ベンダーにとって申請や登録に係る工数、ある程度詳細な機能情報や運用に係る情報提供の負担があっても、それが中小企業へのビジネス促進に繋がるのであれば、問題とはならないのではないかと。
- 中小基盤を活用することで、ベンダー側が中小企業向けにビジネスを展開することに伴う課題をどれだけ解決できるかが重要となる。市場アンケート調査で、中小企業向けセキュリティ製品・サービスのビジネス展開の障壁として挙げられた「購買ニーズの把握が難しく、営業が非効率になりがちである」等の課題は、中小基盤により解決することが出来る余地があるのではないかと。

### 5.3.4. 事業告知及びプロモーション手段

市場調査のベンダーヒアリングでは、中小企業へのセキュリティ製品・サービスの提供には、中小企業との接点が多い代理店や地域の販売店のサポートが不可欠であるとのコメントが寄せられた。中小基盤においても、認知度を高めるための方策や利用促進策として、これらの代理店・販売店との連携が有効であると考えられる。

一方、自動車業界など業界ガイドラインがある場合、業界ガイドラインにおいて取引先等に対して要求されるセキュリティ対策と、その対策を実現するために必要なセキュリティ製品・サービスの関係性が具体的に示されていると、中小企業がセキュリティ製品・サービスの導入検討や選定を進めやすいのではないかと、どのベンダーの指摘がある。中小基盤においても、業界ガイドラインの作成者（業界の大手企業）やベンダーとの連携のもと、業界ガイドラインと中小基盤に掲載する製品・サービスとの紐づけを図ることが、当該業界における中小基盤の利用促進の観点からも有効であると考えられる。

以上の点について、調査結果をもとに有識者検討委員会にて議論が行われ、以下の意見が示された。

**【有識者検討委員会で示された意見】**

- 代理店・販売店について検索するにあたっては、製品・サービスを先に検索して、当該製品・サービスを提供している代理店・販売店を検索する場合と、代理店・販売店を検索した後に、代理店・販売店が取り扱っている製品・サービスを検索する場合が考えられる。前者のように製品・サービスから取り扱っている代理店・販売店を検索するのであれば、ベンダー側に問合せれば情報を得られるかもしれないが、後者のように代理店・販売店から検索する場合、地域ごとに洗い出して、取り扱っている製品・サービスを紐づけるのは難しいのではないかと。
- 業界ガイドラインが存在する業種では、該当するガイドラインが中小企業においてどのようなセキュリティ対策を実施すべきかの目安となるといえる。中小基盤と業界ガイドラインとの紐づけが明確になれば、中小企業の中小基盤へのアクセスの増加、掲載製品・サービスの認知度向上に繋がり、ひいてはこれが情報を提供するベンダー側のメリットにもなるため、好循環になるのではないかと。

## 6. 本調査の総括

本調査は、令和元年度に実施した、中小企業がセキュリティ製品・サービスを選ぶ際に参考となる評価項目の作成等を含む実現可能性調査、並びに、令和2年度に実施した、中小企業及び製品・サービスベンダーそれぞれにおける中小基盤のニーズ調査の内容を踏まえ、実施したものである。

本調査では、中小基盤の仮設サイトの構築による試行環境調査、及びセキュリティ製品・サービスの市場調査の結果に基づき、有識者検討委員会による専門的な視点から助言を得ることで、中小基盤の有用性の検証と構築上の課題等を洗い出すことができた。

将来的な中小基盤の構築に向けた具体化の検討にあたっては、その有用性の観点では一定の潜在的なニーズがあることは前提とすることができるものの、有識者検討委員会の助言・指摘も踏まえ、掲載情報の信頼性に対するユーザーの期待・要望への対応、業界ガイドラインと掲載するセキュリティ製品・サービスの紐づけ、情報の受け手である中小企業と情報の出し手である製品・サービスベンダー双方のメリット等について留意することが望ましく、その在り方については慎重かつ十分な検討を要すると考えられる。

以上