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

成果報告書

2020年4月14日

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

目次構成

1. 調査の背景と目的

あらゆる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のサイバーセキュリティ対策を進めることは喫緊の課題である。独立行政法人情報処理推進機構（以下「IPA」という。）が実施した「2016 年度中小企業における情報セキュリティ対策に関する実態調査報告書 」によると、60%以上の中小企業は情報セキュリティ対策が十分ではないと認識しており、具体的な対策を実践する場合には、「どこからどう実施してよいかわからない」を挙げる企業が多く、中小企業がセキュリティ対策に取り組む上での障壁の一つとなっている。

中小企業のセキュリティ対策水準を向上するため、自社に適したサイバーセキュリティ対策製品・サービスの導入により具体的対策の実践を促すことの有効性は疑う余地がない。

一方で、多くの中小企業は IT やサイバーセキュリティに関する知識が乏しいため、どのようなセキュリティ対策が必要であるか、その対策上どのような製品・サービスを導入することが効果的であるか等を自ら判断できるとは言い難い。

このような状況の下、中小企業のサイバーセキュリティ対策を促すためには、中小企業でも扱いやすい製品・サービスについて、導入や運用することで得られる効果、費用、利用のし易さ、課題等についてわかりやすく提示する必要がある。

本事業では、中小企業における製品・サービス選びの一助となる情報を提示するために有効なプラットフォーム（以下、「中小企業向け情報提供プラットフォーム」とする。）の構築に向けた実現可能性調査を実施した。

なお、本調査は請負契約に基づき、株式会社野村総合研究所（以下「NRI」という。）が実施した。

2. 調査の概要

2.1. 調査の全体像と各調査の概要

本調査では、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証、評価項目の有効性検証、中小企業向け情報提供プラットフォームのコンテンツ作成、有識者委員会の設置及び運営、成果報告会の開催の 5 部構成で実施した。

各調査の流れを 2.1.1.に示す。また、実施概要については 2.1.2.～2.1.6.に記載する。

2.1.1.調査の全体像

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証の流れとしては、初めに評価項目の検証を行う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を公募する方法について、審査方法や通知方法を含めて検討し、その内容を公募要領として定めた。更に当該公募を行う際に、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から提供してもらう情報について検討し、それらの情報を収集するための応募用紙を作成した。次に、NRI が運営する同社のホームページ上に、評価項目の検証を行う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のお知らせを掲載し、応募事業者を広く募集した。また公募の募集期間満了後に、後述する有識者委員会を開催し、その場で採択事業者について厳正に審査し、3 社の採択を決定するとともに、応募事業者に対して、電子メールによる採否の通知を行った。採択後は、評価項目の検証に係る規約を定め、採択事業者に対しては、当該規約を遵守することに同意する同意書の提出を求めるとともに、併せて中小企業ユーザーの候補企業リストの提出を求めた。更に採択事業者から提出された中小企業ユーザーの候補企業リストについては、事務局側で評価項目の検証の協力依頼を行う中小企業ユーザーの優先順位を付けるとともに、当該優先順位に従って NRI と採択事業者が中小企業ユーザーを個別訪問し、協力依頼を行った。その後は採択事業者との間でサイバーセキュリティ製品・サービスの利用に係る契約を締結し、評価項目の検証の協力への承諾が得られた中小企業ユーザーから順次、サイバーセキュリティ製品・サービスの導入を行い、実証を開始した。

評価項目の有効性検証の流れとしては、初めに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について調査仮説を構築した。次に構築した調査仮説を検証するためにヒアリングシートを作成し、当該ヒアリングシートに基づき、中小企業ユーザーに対して、サイバーセキュリティ製品・サービスの評価に関するヒアリング調査を実施した。更に採択事業者に対してヒアリング調査を実施し、中小企業ユーザーへのヒアリング調査結果の内容や評価項目についての調査仮説の有効性を検証するとともに、前述した評価項目についての調査仮説に必要となる追加や修正についてのディスカッションを行った。中小企業ユーザーへのヒアリング調査及び採択事業者へのヒアリング調査については、評価項目の検証

期間内において、各社それぞれ２回ずつ実施した。次に後述する有識者委員会において、これらの調査結果をもとに議論を行い、その結果を踏まえて、中小企業向けサイバーセキュリティ製品・サービスに関する評価項目を再構成した。

中小企業向け情報提供プラットフォームのコンテンツ作成の流れとしては、初めに中小企業向け情報提供プラットフォームのイメージを構築したうえで、類似分野における国内の既存の情報提供プラットフォームの実態を調査し比較分析を行うことにより、中小企業向け情報提供プラットフォームのあるべき姿等についての検討すべき論点を抽出し整理した。次に後述する有識者委員会において、これらの検討すべき論点をもとに議論を行い、その結果を踏まえて、意義・目的や提供情報、情報の信頼性を担保するための検証手法を含め、中小企業向け情報提供プラットフォームのあるべき姿等の取りまとめを行った。更に前述した中小企業ユーザー及び採択事業者へのヒアリング調査結果を踏まえて、中小企業向け情報提供プラットフォームに掲載するコンテンツを作成した。

有識者委員会の設置及び運営については、中小企業がサイバーセキュリティ製品・サービスを選ぶ際に参考となる評価項目を策定し、その有効性を検証するとともに、中小企業における製品・サービス選びの一助となる情報を提供するためのプラットフォームについて検討を行い、あるべき姿や必要となる機能を整理することを目的として、サイバーセキュリティ分野の有識者、中小企業支援団体の有識者により構成される、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」を設置し、本調査期間内に３回の会合を開催し、その運営を行うとともに、専門的な見地からの助言を得た。

成果報告会の開催については、本調査全体について、プレゼンテーション形式による成果報告会を１回開催し、本調査結果についての説明を行った。

2.1.2. 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証の概要

(1)公募要領及び応募用紙の作成

①中小企業ユーザーの選定に対する支援、②自社製品・サービスの中小企業ユーザーへの導入・提供、③評価項目の策定や有効性検証への協力といった３つの取組に参加・対応してく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を公募した。

公募するにあたっては、公募期間、応募資格、実施内容、事業実施期間、応募手続き、審査方法、通知方法、留意事項、契約の要件、質問事項、応募先及び問合せ先を定めた公募要領を作成した。

公募要領を別紙１に示す。

また、公募を行う際の応募用紙については、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応募者の情報を収集するための項目や、採択事業者の審査を行うために必要となる項目として、製品・サービス名称、技術概要、ビジネス概要、中小企業ユーザ

ーへの訴求ポイントを設定した。中小企業ユーザーへの訴求ポイントについては、①導入のし易さ、②運用のし易さ、③導入・運用することで得られる効果、④導入時や運用時に要する費用、⑤導入や運用における課題の解決、⑥経営へのインパクト、⑦セキュリティ性能といった７つの観点からみた大企業向け製品・サービスには見当たらない特徴について記載を求めた。更に公募要領の応募資格を有し応募要件を満たす事業者であるかを確認するための項目も設定した。応募用紙を別紙２に示す。

(2)公募のお知らせを掲載するためのホームページの作成

評価項目の検証を行う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、事業実施期間内において、当該ホームページから前述した公募要領や応募用紙、質問状のファイルをダウンロードできるようにした。

公募のお知らせを掲載するためのホームページを別紙３に示す。

(3)応募状況と採択事業者の決定

公募期間内に５事業者の応募があった。そのうち１事業者は、代理店としての位置づけでの応募であったため、審査の対象外とした。

残り４事業者とその提案製品・サービスについては、後述する有識者委員会（第１回会合）において厳正に審査し、そのうち特徴的な製品・サービスを提供している３事業者を選定し採択を決定した。採択事業者とその提案製品・サービスは、以下のとおりである。

図表 2-1 採択事業者とその提案製品・サービスの概要

採択事業者		提案製品・サービス
①	eGIS 株式会社	EDR＋EDR 運用サービス 「セキュリティドクター」
②	NTT コミュニケーションズ株式会社	中小企業向けお勧めパッケージ （以下の３つのサービスを一体的に運用） １．簡易 SOC サービス「セキュリティサポートデスク」 ２．エンドポイントセキュリティ「マイセキュアビジネス」 ３．クラウドアプリセキュリティ「Cloud App Security」
③	株式会社 Blue Planet-works	エンドポイントセキュリティ 「AppGuard enterprise」、または「AppGuard solo」

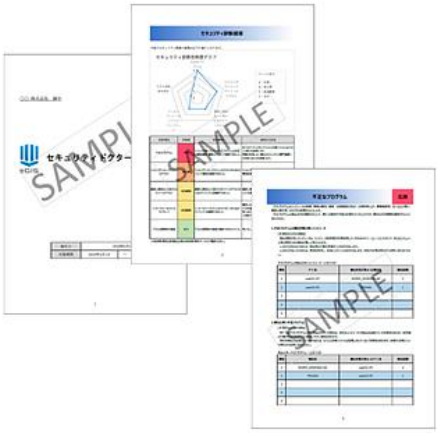
① eGIS 株式会社／EDR＋EDR 運用サービス「セキュリティドクター」

セキュリティドクターの特徴

脅威の早期発見と早期除去を行う次世代型のサイバーセキュリティサービス

- パソコン上の様々な動きを分析することで、既存のセキュリティ環境をすり抜け侵入してきた脅威を発見し除去
- 組織におけるサイバー脅威・情報漏えい等の予兆を24時間分析
- サイバー攻撃に伴う損害を補償するサービスを標準で搭載

診断書により会社の健康状態をチェック



機能１：脅威／サイバーリスク／情報漏えいリスク等の見える化
機能２：挙動ログの監視による脅威発見時のアラート通知

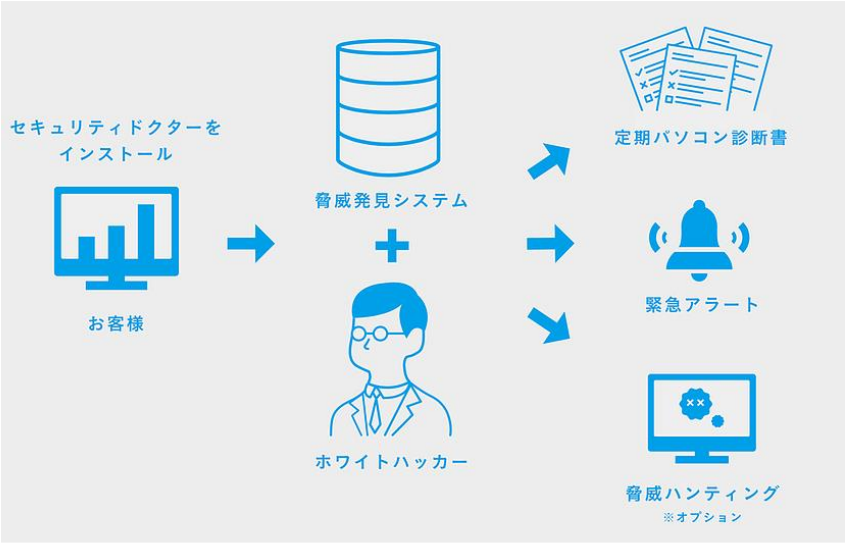
サイバー攻撃に伴う補償サービスが標準搭載

保険概要

損害	対象となる事故	対象損害
賠償損害	・情報漏えいまたはそのおそれ ・情報システムの所有、使用または管理に起因する他人の業務阻害等 ・サイバー攻撃に起因する他人の身体障害・財物損壊	法律上の損害賠償金 争訟費用 権利保全行使費用 訴訟対応費用
費用損害	・情報漏えいまたはそのおそれ ・情報システムの所有、使用または管理に起因する他人の業務阻害等 ・上記を引き起こす可能性のあるサイバー攻撃	事故対応費用 事故原因・被害範囲調査費用 広告宣伝活動費用 法律相談費用 コンサルティング費用 見舞金・見舞品購入費用 クレジット情報モニタリング費用 公的調査対応費用 情報システム等復旧費用 被害拡大防止費用 再発防止費用
	・上記を除き、サイバー攻撃またはそのおそれ	サイバー攻撃調査費用

サイバー攻撃による情報漏えい等の損害金を一部補償
※補償の対象範囲はセキュリティドクターがインストールされているパソコンのみ

セキュリティドクターの仕組み



独自開発された、高い探査能力

セキュリティドクター無料お試し版を使った企業様の９９％がウイルスを探知

リスク管理費用を抑える

自社で対策するよりも圧倒的にコストダウンが実現

出典： eGIS 株式会社カタログ等資料

②-１　NTT コミュニケーションズ株式会社／簡易 SOC サービス「セキュリティサポートデスク」

セキュリティサポートデスクの特徴

- ログの収集から原因究明までNTT Comにおまかせ

NTT Comのセキュリティサービスとあわせてご利用いただけるので、ログの収集からインシデント発生時の原因究明まで1社で完結。お客さまの負担を最小限にとどめ、迅速な対応が可能

- コミュニティや専門家に相談できる相談窓口

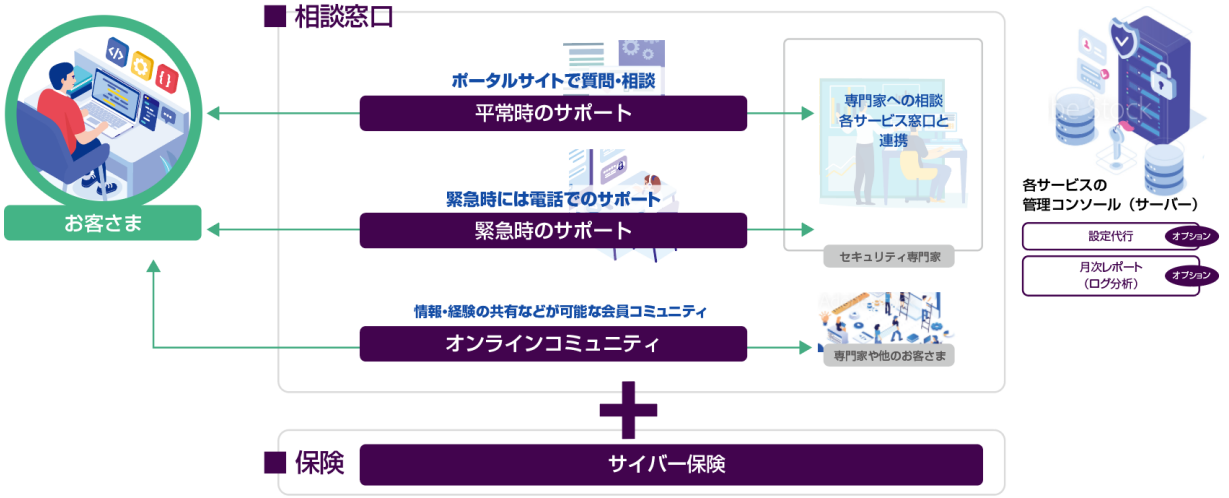
会員コミュニティとの情報共有が可能な掲示板を提供。脆弱性情報などのセキュリティ関連の情報交換を気軽に行うことが可能。またインシデント発生時には専門家による電話サポートも可能。セキュリティ担当者の業務を支援

- サイバー保険込み月額8万円から利用可能

セキュリティの専門家がサポートするヘルプデスク機能と、サイバー攻撃に対応する保険などをパッケージにしたサービスが月額8万円から利用可能。最大3,000万円の補償を受けることが可能。

セキュリティサポートデスクの仕組み

平常時から、インシデント発生時、事後対応までトータルで「安心」をお届け



平常時	インシデント発生時	事後対応
ログの分析や会員コミュニティでの情報交換の場の提供、そしてセキュリティエキスパートへ質問できる窓口の設置により、お客さまのセキュリティ対策をトータルで支援	お客さま環境においてインシデントが発生した場合、セキュリティエキスパートから不正の封じ込め対応などの専門的アドバイスが受けられるほか、お客さまのご要望により、弁護士やコールセンター事業者、フォレンジック調査会社を紹介	サイバー保険が組み込まれているため、事後対応を費用面からサポート。損害賠償責任に関する補償（最大2,000万円）と、原因／被害範囲調査費用や復旧費用、再発防止費用など各種費用に関する補償（最大1,000万円）

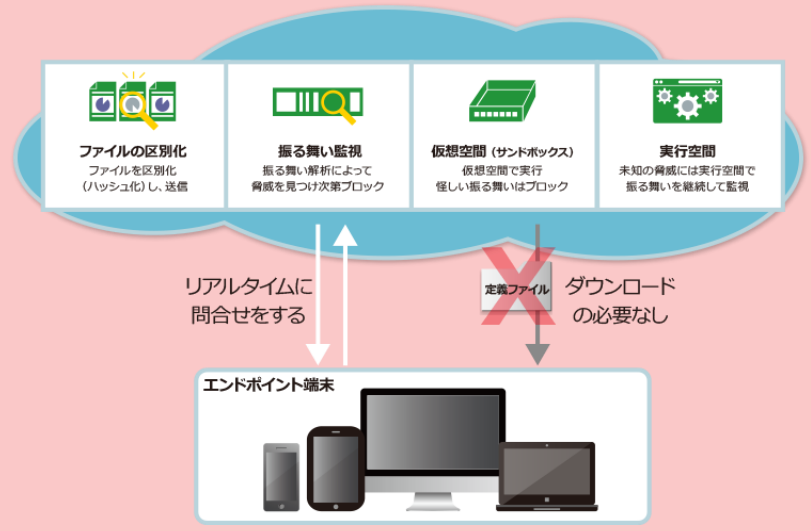
出典：NTT コミュニケーションズ株式会社カタログ等資料

②-２　NTT コミュニケーションズ株式会社／エンドポイントセキュリティ「マイセキュアビジネス」

マイセキュアビジネスの特徴

クラウドにすることでこれまでのセキュリティーソフトの難点を克服した法人向けセキュリティーサービス

- エンドポイント端末(PC、スマホなど)上の新しいファイルは、リアルタイムでクラウドに問い合わせを実施し脅威かどうかを判断
- クラウド上にある最新のセキュリティ情報を参照するため従来のような大容量の定義ファイルが不要
- スキャンは、定義ファイルの更新管理が不要なリアルタイムテクノロジーを採用しているため、エンドユーザーのパフォーマンスを劣化させることなく、利用者のセキュリティ環境を常時最新状態に保ち、あらゆる最新の脅威や攻撃から保護



次世代型エンドポイント保護ソリューション

超高速でエンドポイント端末への配備

- わずか1MB未満の業界最小クラスの端末アプリにより、インストール所要時間は通常数秒以内と高速。他のセキュリティ製品とも競合が発生しないので、セキュリティホールをつくることなく迅速な移行が可能

負荷のない軽快なパフォーマンス

- 初回のスキャンは数分以内、その後のスキャンはさらに短縮。スキャン中のCPU使用率も最小限

最新セキュリティインテリジェンスを活用したエンドポイント保護

- クラウド上にある最新のセキュリティ情報を参照するため従来のような大容量の定義ファイルが不要。社内ネットワークに未接続のユーザーも新しい脅威に対し瞬時に保護

グレー判定（未知の脅威）に対する最大限の防御

- 安全か危険か判定できない未知のファイルの振る舞いを監視。怪しい振る舞いを瞬時に検出すると同時に、その改変を修復

運用管理コストを大幅に削減

- 定義ファイルのバージョン管理や配布、製品アップデートに伴う作業が不要。管理のためのハードウェア設置やソフトウェアの導入も必要ないので、管理コストを大幅に削減

オンライン&オフライン時の防御

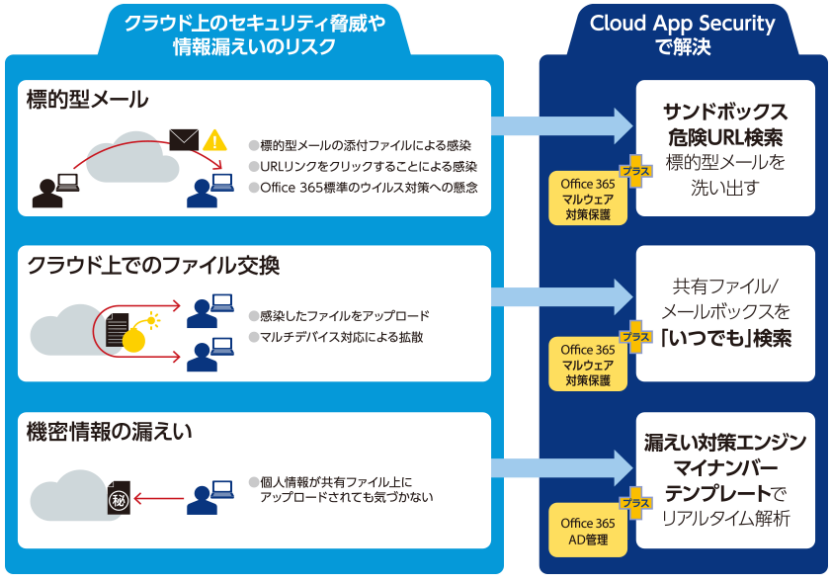
- エンドポイント端末（ＰＣ）に対するオンライン時とオフライン時のセキュリティ設定を別途設定可能。オフライン時もファイルの怪しい振る舞いを監視し、USBやCD、DVDドライブなどを通じた攻撃も防御

出典：NTT コミュニケーションズ株式会社カタログ等資料

Cloud App Securityの特徴

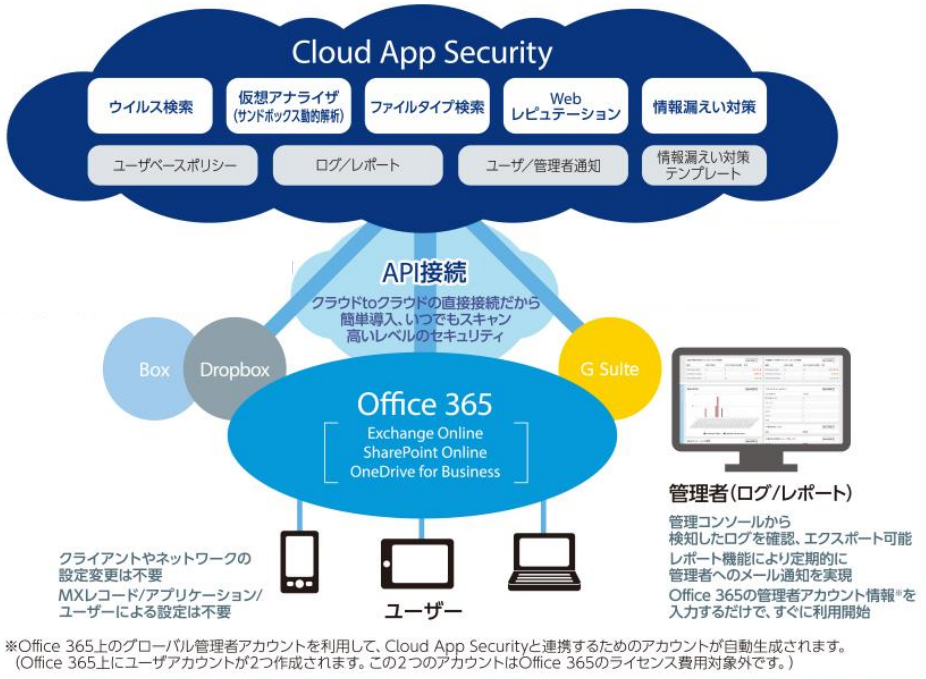
Office365標準セキュリティを強力にカバーするクラウド型セキュリティサービス

- Exchange Online向けに、サンドボックスによる標的型攻撃メール対策や不正プログラム対策(不審な添付ファイルのブロック)、スパムメール対策(文書内に記載されたURLの解析)を強化
- メール本文やファイル内の情報を検索(キーワード/正規表現を利用)することで個人情報、マイナンバー、マル秘ファイルなどの利用状況の可視化が可能



Cloud App Securityの仕組み

APIでクラウドtoクラウド直接接続であるため、簡単導入・いつでもスキャンが可能



- サンドボックス機能での標的型攻撃メールへの対策、ドキュメントの情報漏えい対策が可能
- API連携するため、DNSの切り替えやメールフローの変更不要で導入が容易
- Office365だけでなく、Box、Drop Boxなどにも対応

出典：NTT コミュニケーションズ株式会社カタログ等資料

③株式会社 Blue Planet-works／エンドポイントセキュリティ「AppGuard enterprise」、または「AppGuard solo」

AppGuardの特徴

定義ファイルに依存した検知・検出型ではなく、AIにも頼らない全く異なる免疫系を持ったエンドポイントセキュリティ製品

- 信頼するアプリケーションのみ起動
  アプリの起動場所(システムスペース、ユーザースペース)による制御。マルウェアが侵入しやすいユーザースペースからのアプリ起動を阻止
- 信頼できてもOSの動作を防御
  OSのレジストリ変更、設定変更を阻止
- システムスペースを防御
  システムスペースの改ざんや書き込みを阻止
- メモリを防御
  アプリケーションメモリの読み書きを阻止
- 重要なデータを保護
  重要データへのアクセス・読み込みを阻止
- AppGuardそのものを防御
  AppGuardの停止、アンインストールを阻止

AppGuardの防御の仕組み

AppGuard enterprise

日々の端末利用で発生するリスクから企業を保護する、一元管理されたマルウェア対策ソリューション。予め設定されている強固なポリシーで、エンドポイントを常時守り、例外設定や監視の際には、グループごとにポリシー設定やログの収集などの集中管理が可能。管理はAppGuard管理システムを利用

AppGuard solo

PC単体でユーザ自身が管理を行うことが可能な製品。PCにインストールするだけで、最新のランサムウェアや未知のマルウェアによる脅威からシステムを守り続ける。20名以下の規模の企業や、ユーザ自身で頻繁なチューニングを行う必要がある開発環境などにお薦め

出典：株式会社 Blue Planet-works カタログ等資料

(4)評価項目の検証に係る規約及び同意書の作成

評価項目の検証が適切に行われることを担保するため、評価項目の検証に係る規約を作成するとともに、検証に参画する採択事業者及び中小企業ユーザーそれぞれが、当該規約に同意する形を採り、同意書の提出を求めた。

評価項目の検証に係る規約と当該規約を遵守することに同意する同意書をそれぞれ別紙４、別紙５に示す。

(5)中小企業ユーザーへの協力依頼と承諾が得られた中小企業ユーザー

採択事業者から提出された中小企業ユーザーの候補企業リストについて、事務局側で評価項目の検証の協力依頼を行う中小企業ユーザーの業種・業態等を考慮したうえで優先順位を設定し、優先順位に従って事務局と採択事業者が中小企業ユーザーを個別訪問し、協力依頼を行った。

その結果、評価項目の検証への協力について、採択事業者１事業者につき、２社の中小企業ユーザーから承諾を得られ、順次、サイバーセキュリティ製品・サービスの導入を行った。

承諾が得られた中小企業ユーザーのプロファイルを以下に示す。

図表 2-2 承諾が得られた中小企業ユーザーのプロファイル

採択事業者	承諾が得られた中小企業ユーザー			
	業種	事業内容	資本金	従業員数
eGIS 株式会社	A 社（製造業）	バイオ燃料、化学品製造など	4 億 9,800 万円	45 名
	B 社（製造業）	工作機械、専用機械等の精密金型設計、部品、治具等の製作、特殊鋼材、一般鋼材のプレス加工など	1,000 万円	15 名
NTT コミュニケーションズ株式会社	C 社（SI 業）	システムコンサルティング、システム開発、システム運用支援、ソフトウェア販売など	約 5,000 万円	約 120 名
	D 社(ガス供給業)	LP ガスの個別・集中供給、ガス機器・住宅設備機器の販売・施工、ガス配管設備の設計・施工、冷暖房設備の販売・施工など	4 億 8,000 万円	約 160 名
株式会社 Blue Planet-works	E 社 （NI 業）	電話交換設備販売、設計施工、保守、光ファイバー設備、ＬＡＮ関連機器の販売、設計施工、携帯電話基地局の設置、保守など	1,000 万円	約 20 名
	F 社（卸売業）	陸用(建設・住宅、プラント)、舶用(造船)の配管機材全般(バルブ、継ぎ手、圧力計等)の卸業など	2,100 万円	約 10 名

注）SI は System Integration の略称、NI は Network Integration の略称

2.1.3. 評価項目の有効性検証の概要

（1）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の仮説構築

①導入のし易さ、②運用のし易さ、③導入・運用することで得られる効果、④導入時や運用時に要する費用、⑤導入や運用における課題の解決、⑥経営へのインパクト、⑦セキュリティ性能といった７つの観点について、詳細な評価項目レベルにまで具体化し、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の調査仮説を構築した。

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の調査仮説を以下に示す。

図表 2-3 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の調査仮説

評価項目の観点		詳細な評価項目	
1	導入のし易さ	1.1	大規模なシステム改修を伴わず実装が容易である
		1.2	現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である
		1.3	いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である
2	運用のし易さ	2.1	社内に専門的な人材がいなくてもメンテナンスが可能である
		2.2	万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である
		2.3	問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である
3	導入や運用を行うことで得られる効果	3.1	導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である
		3.2	サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である
4	導入時や運用時に要する費用	4.1	導入コストが安価である
		4.2	運用コストが安価である
5	導入や運用における課題の解決	5.1	製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠(利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等)に基づき、適切な説明がなされている
6	製品・サービスの経営へのインパクト	6.1	パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である
		6.2	オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である
		6.3	製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先(顧客)等の外部にアピールしやすい
7	製品・サービスのセキュリティ性能	7.1	対応可能な既存の脅威・インシデントのパターン・範囲が広範である
		7.2	未知の脅威・インシデントへの対応が可能である
		7.3	人為的ミスなどにより、製品そのものが他人(攻撃者)の手に渡るといった、万が一の場合でも悪用が難しい

(2)中小企業ユーザーに対するヒアリング調査

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の調査仮説を検証するためにヒアリングシートを作成し、各中小企業ユーザーに対して、当該ヒアリングシートに基づくヒアリング調査を実施した。ヒアリング調査は評価項目の検証期間内に時間的な間隔を空けて２回実施した。中小企業ユーザーに対するヒアリング調査の実施状況は以下のとおりである。

図表 2-4 中小企業ユーザーに対するヒアリング調査の実施状況

採択事業者	中小企業ユーザー			
	事業者	ヒアリング対象者	ヒアリング調査（１回目）	ヒアリング調査（２回目）
eGIS 株式会社	A 社	経営層、担当者	2019 年 12 月 13 日（金）	2020 年 1 月 10 日（金）
	B 社	経営層	2019 年 12 月 16 日（月）	2020 年 1 月 13 日（月）
NTT コミュニケーションズ株式会社	C 社	担当者	2019 年 12 月 20 日（金）	2020 年 1 月 8 日（水）
	D 社	担当者	2019 年 12 月 20 日（金）	2020 年 1 月 7 日（火）
株式会社 Blue Planet-works	E 社	経営層、担当者	2019 年 12 月 17 日（火）	2020 年 1 月 9 日（木）
	F 社	経営層、担当者	2019 年 12 月 17 日（火）	2020 年 1 月 9 日（木）

また、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の調査仮説を検証するために作成したヒアリングシートを別紙６に示す。

(3)採択事業者等に対するヒアリング調査

採択事業者及び中小企業ユーザーに対面し採択事業者が提供する中小企業向けサイバーセキュリティ製品・サービスを直接販売している販売代理店（そのような販売代理店が存在する場合のみ）に対して、ヒアリング調査を実施した。ヒアリング調査は評価項目の検証期間内に時間的な間隔を空けて２回実施した。採択事業者等に対するヒアリング調査の実施状況は以下のとおりである。

図表 2-5 採択事業者等に対するヒアリング調査の実施状況

採択事業者	販売代理店	ヒアリング調査（１回目）	ヒアリング調査（２回目）
eGIS 株式会社	東京システムリサーチ株式会社 株式会社ラック	2019 年 12 月 26 日（木）	2020 年 1 月 15 日（水）

採択事業者	販売代理店	ヒアリング調査（１回目）	ヒアリング調査（２回目）
NTT コミュニケーションズ株式会社	販売代理店なし	2019 年 12 月 26 日（木）	2020 年 1 月 10 日（金）
株式会社 Blue Planet-works	大興電子通信株式会社	2019 年 12 月 17 日（火）	2020 年 1 月 15 日（水）

ヒアリング調査では、中小企業ユーザーに対するヒアリング調査結果をもとに、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内容や、評価項目の調査仮説についての有効性を検証するとともに、評価項目の調査仮説に必要となる追加や修正についてのディスカッションを行った。

(4)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の策定

中小企業ユーザーに対するヒアリング調査結果や、採択事業者等に対するヒアリング調査結果をもとに、後述する有識者委員会において議論を行い、その結果を踏まえて、中小企業向けサイバーセキュリティ製品・サービスに関する評価項目の調査仮説を再構成し、評価項目を策定した。

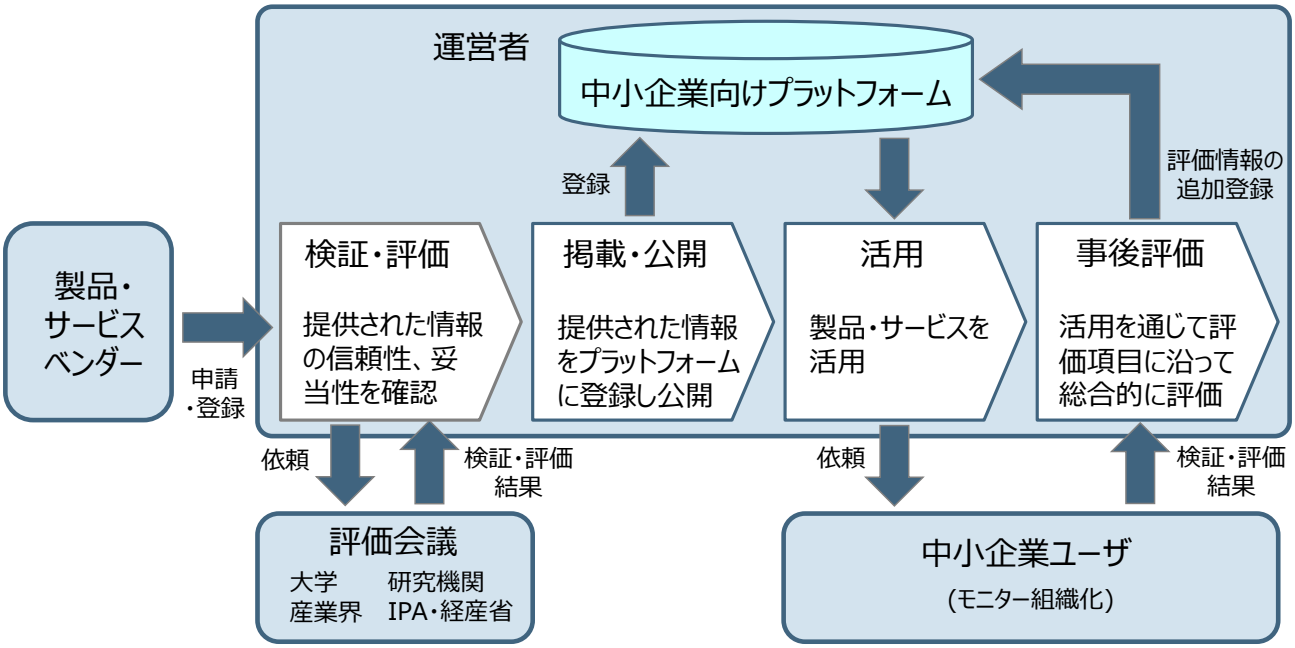
2.1.4. 中小企業向け情報提供プラットフォームのコンテンツ作成の概要

(1)中小企業向け情報提供プラットフォームのイメージの構築

中小企業におけるサイバーセキュリティ製品・サービス選びの一助となる情報を提供するための有効なプラットフォームについては、申請時にサイバーセキュリティ製品・サービスの提供事業者から提供される情報について、情報提供プラットフォームの運営者が評価項目に沿った評価や情報の信頼性の検証を実施しようとすると、コスト面、労力面の過重な負荷を強いられることから、事前評価のみならず、事後評価を上手く活用することが重要になると考えられる。

このような点を踏まえ、中小企業向け情報提供プラットフォームのイメージを構築した。当該イメージを以下に示す。

図表 2-6 中小企業向け情報提供プラットフォームのイメージ



(2)類似分野における国内の既存の情報提供プラットフォームの実態調査

類似分野における国内の既存の情報提供プラットフォームの実態について公開情報ベースの調査を行い、意義・目的、運営者、利用者、提供情報、適用条件、利用者にとってのメリット、提供機能、運営形態、収支構造といった観点から情報を整理したうえで、比較分析を行った。調査対象とした類似分野における国内の既存の情報提供プラットフォーム一覧を以下に示す。

図表 2-7 調査対象とした類似分野における国内の既存の情報提供プラットフォーム一覧

運用者		名称・URL	想定利用者	概要
公的機関（外郭団体含む）	国土交通省	新技術情報提供システム（NETIS）	関係府省、地方自治体、公共工事等に係る事業者	• 新技術の活用のため、新技術に関わる情報の共有及び提供 • NETIS 登録技術の検索、事前審査、活用効果調査による技術比較
	地方公共団体情報システム機構(J-LIS)	J-LIS LGWAN-ASPサービスリスト	地方公共団体	• LGWAN-ASPの目的、規定類、様式の情報提供 • LGWAN-ASPサービスとして登録/接続されているサービスの一覧
	中小企業基盤整備機構(中小機構)	中小企業ワールドビジネスサポート（SWBS） ※2019年12月リニューアルに向けてサイト閉鎖予定	中小企業	• 海外展開に意欲的な中小企業と海外展開をサポートする企業・団体との出会いの場 • 海外展開支援企業を検索、現地情報や海外展開イベントの情報を収集
		ここからアプリ	中小企業	• 生産性向上を目指す中小企業・小規模事業者が、使いやすい・導入しやすいと思われる業務用アプリの情報提供
	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)	JNSAソリューションガイド	中小企業	• JNSAの会員企業が取り扱う、ネットワーク・セキュリティ等に関する製品やサービス、イベント、セミナーの情報提供
業界団体（コンソーシアムを含む）	テレワーク導入推進コンソーシアム(TWIC)（テレワーク推進フォーラム会員である民間企業及び団体を構成員とした組織）	「テレワーク」を始めてみませんか？	中小企業	• 地域の中小企業を主な対象として、テレワークに関する中小企業経営者向けセミナーや、コンサルティング、テレワークツールの情報提供 • テレワークに係るガイドラインの情報提供 • 補助制度に係る情報提供、テレワークPCのパッケージ販売

(3)検討すべき論点の抽出・整理

中小企業向け情報提供プラットフォームのあるべき姿等について、検討すべき論点を抽出し整理した。検討すべき論点を以下に示す。

論点①　意義・目的について、どのように位置づけるか

情報提供プラットフォーム構築の意義・目的については、大きな視点で捉えた場合は、中小企業におけるサイバーセキュリティ対策の課題を解決するための支援や、小さな視点で捉えた場合には、中小企業におけるサイバーセキュリティ製品・サービスを導入するための支援のために必要である。

また、前者の場合については、こういう課題(発注元からの要求等)があるから、こういう解決(製品・サービス導入)をした方がよいというシナリオ・戦略とのセットが必要である。

論点②　運営者について、どのように考えるか

情報提供プラットフォームの運営者については、本事業で策定する評価項目に則った形での客観的な評価が必要であり、更に評価における中立性・公平性が求められるという点を考慮すると、公的機関とすることに優位性があると考えられる。

論点③　申請情報について、情報の信頼性をどのような手法・運用体制で担保するか

情報提供プラットフォーム上で提供される情報としては、評価項目に則った形で客観的な評価が行われ、その評価情報が、中小企業に対して提供されることが想定される。

論点④　登録の可否を判断するうえで、ベンダーから提供してもらうべき必要な情報は何か

登録の可否を判断するにあたっては、申請情報の信頼性を確認する以外に、ベンダーに関する情報(経営状況、反社会的勢力ではない表明等)、製品・サービスに関する情報(導入実績等)等についても確認することが想定される。

また、製品・サービスの導入促進のために、導入事例や無料使用期間の有無等の情報を掲載している情報提供プラットフォームも見受けられる。

論点⑤　提供機能としては、評価情報の提供までとするか、更にその先の事業者マッチングや製品・サービス販売等にまで踏み込むか

製品・サービスの導入促進のために、事業者マッチングや製品・サービス販売にまで踏み込んで機能を提供しているプラットフォームも見受けられる。

論点⑥　登録可否の判断や掲載可否の判断のルール化について、どのようなケースにおいて登録不可・掲載不可とするべきか

登録不可・掲載不可を認める場合、説明責任を果たすために、不可の理由を明確にする必要がある。また、評価の低い製品・サービスや掲載の取り消しを判断するにあたっては、評価の基準が必要である。

論点⑦　登録・掲載後、製品・サービスの内容に変更が生じたときに、どのような対応が必要になるか

掲載される情報は、あくまで時点評価に基づくものであり、その後に製品・サービスの内容に変更が生じることが想定される。

掲載される情報の陳腐化を回避するため、製品・サービスの内容に大幅な変更が生じたときに、情報のアップデートができる仕組みが必要である。

論点⑧　情報提供プラットフォーム上で情報を探す際のインデックスの付け方について、どのように考えるべきか

中小企業は、売上高や従業員の規模を始めとして、業種、IT 利用環境、商慣習などが多種多様であり、中小企業を一括りにして扱うことが難しく、企業によって情報提供プラットフォームに求められる情報の内容も異なる。

情報提供プラットフォーム上で必要となる情報を探しやすくするために、インデックスの設定が必要である。

(4)中小企業向け情報提供プラットフォームのあるべき姿等の取りまとめ

2.1.5.で後述する有識者委員会において、上記(3)で整理した検討すべき論点について議論を行い、その結果を踏まえて、中小企業向け情報提供プラットフォームのあるべき姿等の取りまとめを行った。

(5)中小企業向け情報提供プラットフォームに掲載するコンテンツの作成

中小企業向け情報提供プラットフォームのあるべき姿等や、中小企業ユーザー及び採択事業者等に対するヒアリング調査結果を踏まえて、中小企業向け情報提供プラットフォームに掲載するコンテンツを作成した。コンテンツについては、「５．中小企業に広く訴求するためのコンテンツ」に記載する。

2.1.5. 有識者委員会の設置及び運営の概要

中小企業がサイバーセキュリティ製品・サービスを選ぶ際に参考となる評価項目を策定し、その有効性を検証するとともに、中小企業における製品・サービス選びの一助となる情報を提供するためのプラットフォームについて検討を行い、あるべき姿や必要となる機能を整理することを目的として、サイバーセキュリティ分野の有識者、中小企業支援団体の有識者により構成される、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」を設置し、本調査期間内に３回の会合を開催し、その運営を行うとともに、専門的な見地からの助言を得た。

中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会の開催経緯と委員について以下に示す。

図表 2-8 中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会の開催経緯

会合	開催日	開催場所	審議事項
第１回会合	2019 年 10 月 8 日（火）	NRI 東京本社　会議室	・検討・検証の進め方について ・製品・サービスベンダーの公募の状況と事務局による一次評価結果について
第２回会合	2019 年 12 月 6 日（金）	IPA　会議室	・評価項目の検証に関する現状報告について ・発注元が、契約先及び再契約先に求めるサイバーセキュリティ対策について ・情報提供プラットフォームのあるべき姿等の検討について
第３回会合	2020 年 1 月 17 日（金）	NRI 東京本社　会議室	・評価項目の検証ヒアリング結果の報告について ・評価項目のあり方に関する検討について ・情報提供プラットフォームのあるべき姿等の検討について

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）
小松　靖直　　日本商工会議所　情報化推進部長
下村　正洋　　NPO 日本ネットワークセキュリティ協会　理事/事務局長
手塚　悟　　慶應義塾大学　環境情報学部　教授
中島　康明　　独立行政法人中小企業基盤整備機構　経営支援部長

【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

【事務局】
野村総合研究所　ICT メディア・サービス産業コンサルティング部

2.1.6. 成果報告会の開催の概要

本調査全体について、プレゼンテーション形式による成果報告会を１回開催し、本調査結果についての説明を行った。

2.2. 調査仮説の構築とその考え方

2.2.1. 評価項目に関する仮説の構築とその考え方

①導入のし易さ、②運用のし易さ、③導入・運用することで得られる効果、④導入時や運用時に要する費用、⑤導入や運用における課題の解決、⑥経営へのインパクト、⑦セキュリティ性能といった７つの観点について、詳細な評価項目レベルにまで具体化し、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の調査仮説を構築した。

図表 2-9 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の調査仮説（再掲）

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を伴わず実装が容易である
		②	現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である
		③	いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である
(2)	運用のし易さ	①	社内に専門的な人材がいなくてもメンテナンスが可能である
		②	万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である
		③	問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である
(3)	導入や運用を行うことで得られる効果	①	導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である
		②	サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である
(4)	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
(5)	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、誰もが納得のできる客観的な根拠(利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等)に基づき、適切な説明がなされている
(6)	製品・サービスの経営へのインパクト	①	パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である
		②	オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である
		③	製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先(顧客)等の外部にアピールしやすい
(7)	製品・サービスのセキュリティ性能	①	対応可能な既存の脅威・インシデントのパターン・範囲が広範である
		②	未知の脅威・インシデントへの対応が可能である
		③	人為的ミスなどにより、製品そのものが他人(攻撃者)の手に渡るといった、万が一の場合でも悪用が難しい

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の調査仮説とその考え方を以下に示す。

(1)導入のし易さの観点からみた評価項目に関する仮説の構築とその考え方

① 大規模なシステム改修を伴わず、実装が容易である

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、中小企業ユーザーの経営層は、導入決断を見送りがちである。また、中小企業ユーザー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繋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。

このような観点を踏まえ、「①大規模なシステム改修を伴わず、実装が容易である」を評価項目に関する調査仮説として取りまとめた。

② 現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である

中小企業ユーザーにおいては、コスト面の制約が大きいことから、機能がオーバースペックで利用料金が高くなるのであれば、必要最小限の機能のみが用意されていて、プラスアルファの機能はオプションで選択できるようになっている方がよいと考えがちである。特にセキュリティ担当者の確保が難しい中小企業ユーザーにおいては、自社でセキュリティ設計や必要となる機能の選定を行うことが困難であることから、必要最小限の機能が製品・サービスに用意されていることが重要である。

このような観点を踏まえ、「②現場の事情に合わせて使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である」を評価項目に関する調査仮説として取りまとめた。

③ いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である

中小企業ユーザーにおいては、セキュリティ担当者が確保されている場合が少ないだけでなく、システム担当者が確保されていて、セキュリティまで管理するような場合でも専業の担当者ではなく、他の業務との兼業の担当者が多いことから、導入時のインストール・設定作業に係る時間的な制約が大きい。また、担当者においては、製品・サービスやサイバーセキュリティに関する専門的な知識が必ずしも十分とは言えず、インストール・設定作業の途中段階でつまずけば、作業が完了しない状態を招いたり、その状態を放置したままになったりする可能性があることから、インストール・設定作業が負荷なく簡単かつ短時間に実施で

きることが重要である。
　このような観点を踏まえ、「③いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である」を評価項目に関する調査仮説として取りまとめた。

(2)運用のし易さの観点からみた評価項目に関する仮説の構築とその考え方

① 社内に専門的な人材がいなくても、メンテナンスが可能である
　中小企業ユーザーにおいては、製品・サービスのメンテナンス作業を自社の担当者のみで充足させるには、人材・スキル面や教育・研修に掛けられるコスト面の制約があり、自ずと限界が生じることから、専門的な知識を有する外部のセキュリティベンダーに委ねたいという思いが強い。また、製品・サービスの運用作業を内製化して対応している中小企業ユーザーにおいても、サイバー攻撃の手口が高度化・巧妙化する中で、製品・サービスのメンテナンスに係る管理が負担になりがちである。
　このような観点を踏まえ、「①社内に専門的な人材がいなくても、メンテナンスが可能である」を評価項目に関する調査仮説として取りまとめた。

② 万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である
　中小企業ユーザーにおいては、インシデント発生時の対応に係る知識や経験が必ずしも十分とは言えず、自社で対応しようとすれば、初動対応を見誤りがちである。また、勤務時間内にインシデントが発生すれば、外部のセキュリティベンダーの手を借りながら、ある程度までは自社でも対応が可能であるが、勤務時間外にインシデントが発生すれば、対応人員の確保が難しく、自社で実施できる対応が限られてくるため、対応が後手に回る可能性がある。
　このような観点を踏まえ、「②万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である」を評価項目に関する調査仮説として取りまとめた。

③ 問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である
　中小企業ユーザーにとって、何かトラブルやインシデントが発生した場合に、外部のセキュリティベンダーに対応方法を問合せ・相談できることは安心に繋がる。特に中小企業ユーザーの場合においては、トラブルやインシデントの発生によって業務停止に陥れば、経営にもたらされる影響が甚大になることから、早期の問題解決や復旧のために、問合せ・相談窓口の素早いレスポンスによる的確な対応が求められる。
　このような観点を踏まえ、「③問合せ・相談窓口へのアクセスが容易であり、速くて質の高

い応答を踏まえた対応が可能である」を評価項目に関する調査仮説として取りまとめた。

(3)導入や運用を行うことで得られる効果の観点からみた評価項目に関する仮説の構築とその考え方

① 導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である

中小企業ユーザーにおいては、サイバーセキュリティ対策に掛けられるコストが限られる中で、導入後に機能追加に伴う追加費用負担が求められれば、導入した製品・サービスの解約に繋がりやすくなる。更に、機能追加が頻繁に発生すれば、製品・サービスそのものに対する信頼が揺るぎかねない事態に発展する可能性がある。

このような観点を踏まえ、「①導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である」を評価項目に関する調査仮説として取りまとめた。

② サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である

中小企業ユーザーにおいては、担当者のサイバーセキュリティや製品・サービスに関する知識が必ずしも十分とは言えず、コストを掛けて学習しないと導入・運用ができないような製品・サービスは敬遠されがちであることから、必要最小限の知識で適切に製品・サービスを使用できるようになることが重要である。

このような観点を踏まえ、「②サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である」を評価項目に関する調査仮説として取りまとめた。

(4)導入時や運用時に要する費用の観点からみた評価項目に関する仮説の構築とその考え方

① 導入コストが安価である

導入コストが安価であることは、中小企業ユーザーの製品・サービス選びにおいて重要な要素の一つであり、導入コストが高額であれば、そもそも導入自体を検討の俎上に載せることは難しくなる。特に導入時には脅威・インシデントの発生を経験できることは稀であり、当該製品・サービスの費用対効果を実感しにくいため、価格設定の低さと、ボリュームディスカウントや償却期間の伸長などの観点からみたお買得感・割安感が先に立ちがちである。

このような観点を踏まえ、「①導入コストが安価である」を評価項目に関する調査仮説として取りまとめた。

② 運用コストが安価である

運用コストが安価であることも、導入コストと同様、中小企業ユーザーの製品・サービス選びにおいて重要な要素の一つである。特に中小企業ユーザーの経営層においては、必要となるサイバーセキュリティ対策は講ずるものの、セキュリティ運用のトータルコストは低く抑えたいという思いか強いことから、必要となる製品・サービスがパッケージ化されてディスカウントされていたり、万が一インシデントが発生した場合の対応費用や損害額をサイバー保険等の補償サービスで賄ったりすることができれば、更に評価は高くなりがちである。

このような観点を踏まえ、「②運用コストが安価である」を評価項目に関する調査仮説として取りまとめた。

(5)導入や運用における課題の解決の観点からみた評価項目に関する仮説の構築とその考え方

① 製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠（利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等）に基づく、適切な説明がなされている

中小企業ユーザーの担当者は、製品・サービスに関する知識が必ずしも十分とは言えないことから、導入時に製品・サービスの性能・スペックの信憑性について疑念が生じることは少ないと考えられるが、その一方で、世の中で騒がれているような脅威・インシデントに対して、適切に対応できるかどうかを気にしており、経営層からもそのような状況について確認を受ける場合もあることから、説明に使える客観的な根拠を把握することが重要である。

このような観点を踏まえ、「①製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠（利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等）に基づく、適切な説明がなされている」を評価項目に関する調査仮説として取りまとめた。

(6)製品・サービスの経営へのインパクトの観点からみた評価項目に関する仮説の構築とその考え方

① パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である

中小企業ユーザーの経営層の中には、何もインシデントが起きていないのであれば、現在の対策のままで十分であると考える経営層が多いと考えられる。そのような状況のもと、中小企業ユーザーの担当者においては、経営層に対してサイバーセキュリティ製品・サービス

の導入の必要性を如何に的確に説明することができるかが求められる。中小企業ユーザーの経営層は、コスト削減への意識が強いため、説明の際には、導入するサイバーセキュリティ製品・サービスによって、当該企業において必要となる対策がカバーされるとともに、費用についてもコスト削減に繋がるようなメリットを享受できていて、十分折り合っているなど、当該製品・サービスが必要となる対策面、費用面の双方からみて合理的な選択肢になっていることが重要になる。

このような観点を踏まえ、「①パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である」を評価項目に関する調査仮説として取りまとめた。

② オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である

中小企業ユーザーにおいては、人材の確保が難しい中で、サイバーセキュリティ製品・サービスの導入・運用は、担当者の作業負荷を高め、場合によっては人員の増員を余儀なくされる可能性がある。中小企業ユーザーの経営層においては、担当者の作業負荷が過重になることや人員の増員を伴うことを敬遠しがちである。このため、新たにサイバーセキュリティ製品・サービスを導入した場合でも、これまでどおり、システムの運用とセキュリティの運用の双方について、担当者への過重な作業負荷や人員の増員がない形で運用できることが重要となる。

このような観点を踏まえ、「②オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である」を評価項目に関する調査仮説として取りまとめた。

③ 製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先（顧客）等の外部にアピールしやすい

中小企業ユーザーの経営層においては、サイバーセキュリティや製品・サービスに関する知識が必ずしも十分とは言えないことから、製品・サービスの仕様や機能等について理解してもらうことは困難である。そのため、経営層に製品・サービスの導入の必要性を理解してもらうためには、製品・サービス自体の概念・コンセプトが明快で理解しやすいものになっている必要があり、そのような理解しやすい製品・サービスであれば、導入にあたってのハードルを一段と引き下げられる可能性がある。また、経営層においては、取引先（顧客）と

の取引において求められる対策は導入せざるを得ないという考えがあり、製品・サービスの導入・運用によって対策の取組状況を取引先（顧客）に対してアピールできるようになることはメリットであると考えられる。

このような観点を踏まえ、「③製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先（顧客）等の外部にアピールしやすい」を評価項目に関する調査仮説として取りまとめた。

(7)製品・サービスのセキュリティ性能の観点からみた評価項目に関する仮説の構築とその考え方

① 対応可能な既存の脅威・インシデントのパターン・範囲が広範である

中小企業ユーザーにおいては、サイバー攻撃の手口が高度化・巧妙化する中で、サイバーセキュリティ製品・サービスの導入・運用によって対応可能な脅威・インシデントのパターン・範囲については、広範である方がよいと考える企業が多いと考えられる。

このような観点を踏まえ、「①対応可能な既存の脅威・インシデントのパターン・範囲が広範である」を評価項目に関する調査仮説として取りまとめた。

② 未知の脅威・インシデントへの対応が可能である

中小企業ユーザーにおいては、ウイルス対策ソフトやファイアウォールの導入が比較的進んでいるが、大企業と比較するとまだまだ対策が手薄であると判断される場合が少なからず見受けられることから、攻撃者に狙われる機会が増えてきている。このため、既知の脅威・インシデントだけでなく、ウイルス対策ソフトでは十分検知できない未知の脅威・インシデントに対しても適切に対応できるようになることが必要になってきている。

このような観点を踏まえ、「②未知の脅威・インシデントへの対応が可能である」を評価項目に関する調査仮説として取りまとめた。

③ 人為的ミスなどにより、製品そのものが他人（攻撃者）の手に渡るといった、万が一の場合でも悪用が難しい

中小企業ユーザーにおいては、導入・運用するサイバーセキュリティ製品・サービスが引き金となって、情報漏えい事故等の脅威・インシデントを招くという事態を避けたいと考えており、セキュリティベンダー側が攻撃者や人為的ミス等による悪用防止を最優先に考えた製品・サービス設計を適切に行っているような製品・サービスを選択しがちである。

このような観点を踏まえ、「③人為的ミスなどにより、製品そのものが他人（攻撃者）の手

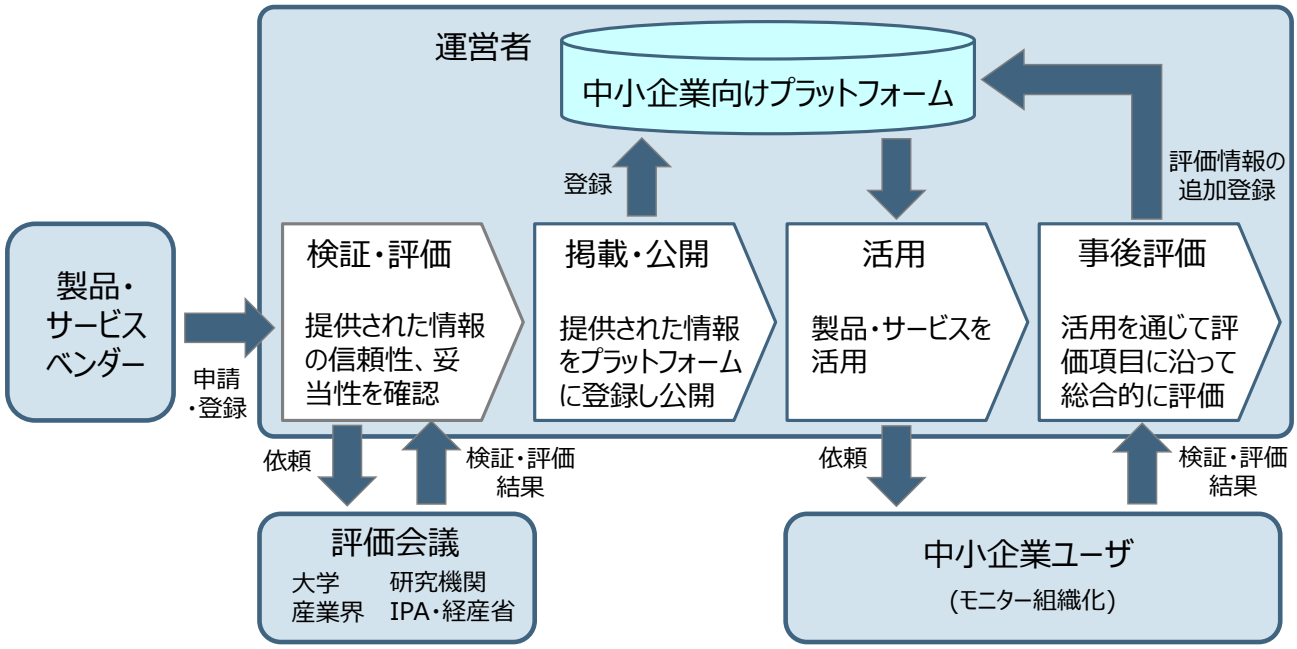
に渡るといった、万が一の場合でも悪用が難しい」を評価項目に関する調査仮説として取りまとめた。

2.2.2. 情報の信頼性を担保するための検証手法に関する仮説の構築とその考え方

中小企業におけるサイバーセキュリティ製品・サービス選びの一助となる情報を提供するための有効なプラットフォームについては、申請時にサイバーセキュリティ製品・サービスの提供事業者から提供される情報について、情報提供プラットフォームの運営者が評価項目に沿った評価や情報の信頼性の検証を実施しようとすると、コスト面、労力面の過重な負荷を強いられることから、事前評価のみならず、事後評価を上手く活用することが重要になると考えられる。

情報の信頼性を担保するための検証手法に関する調査仮説とその考え方を以下に示す。

図表 2-7 中小企業向け情報提供プラットフォームのイメージ（再掲）



（1）検証・評価に関する仮説の構築とその考え方

製品・サービスベンダーから申請・登録されるサイバーセキュリティ製品・サービスに関する情報については、大学、産業界、研究機関、情報処理推進機構（IPA）、経済産業省の有識者メンバーで構成される、中小企業向け情報提供プラットフォームの運営者が設置する評価会議にて、提供された情報の信頼性、妥当性の検証・評価を行ったうえで、その検証・評価結果に基づき登録の可否を判断することを、調査仮説として取りまとめた。但し、検証・評価においては、中小企業向けサイバーセキュリティ製品・サービスを提供するセキュリティベンダーに対して、検証・評価に係る過重なコスト負担を強いることは難しいと判断され

るため、サイバーセキュリティ製品・サービスの性能・スペックについては、技術的な検証を行わないものとした。また、申請・登録時には、製品・サービスベンダーから、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に沿った形で製品・サービスに関する情報を提供してもらうこととした。

(2)掲載・公開・活用に関する仮説の構築とその考え方

中小企業向け情報提供プラットフォームの運営者は、評価会議から報告を受けた検証・評価結果を踏まえて、製品・サービスベンダーが申請・登録されるサイバーセキュリティ製品・サービスに関する情報を情報提供プラットフォームに登録し公開すること判断することを、調査仮説として取りまとめた。また、中小企業は、公開されたサイバーセキュリティ製品・サービスに関する情報を、製品・サービス選びの一助として活用するものとした。

(3)事後評価に関する仮説の構築とその考え方

中小企業向け情報提供プラットフォームの運営者は、情報提供プラットフォームに登録したサイバーセキュリティ製品・サービスを活用している中小企業ユーザーの中から、事後評価のモニターとして協力してもらえる企業を募り、事後評価のモニターを組織化することを、調査仮説として取りまとめた。また、事後評価のモニターとなった中小企業ユーザーは、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に沿った形で、自社で活用している製品・サービスを検証し、総合的な評価を行うことにより、実施を見送ったサイバーセキュリティ製品・サービスの性能・スペックに関する技術的な検証についてカバーするものとした。更に、中小企業向け情報提供プラットフォームの運営者は、事後評価のモニターとなった中小企業ユーザーから報告を受けた検証・評価結果を踏まえて、既に情報提供プラットフォームに登録されるサイバーセキュリティ製品・サービスに関する情報を見直し、必要となる修正登録や追加登録を行うこととした。

2.2.3. 中小企業向け情報提供プラットフォームのあるべき姿等に関する仮説の構築とその考え方

類似分野における国内の既存の情報提供プラットフォームの調査結果を踏まえて、中小企業向け情報提供プラットフォームのあるべき姿等について、検討すべき論点を抽出し整理したうえで、論点ごとに調査仮説を構築した。

類似分野における国内の既存の情報提供プラットフォームの調査結果と、そこから導出された中小企業向け情報提供プラットフォームのあるべき姿等に関する調査仮説とその考え方を以下に示す。

（1）類似分野における国内の既存の情報提供プラットフォームの調査

中小企業向けプラットフォームの検討に向けた論点の洗い出しを実施するために、類似分野における国内の既存の情報提供プラットフォームの文献調査を実施した。文献調査の対象とした国内の既存の情報提供プラットフォームは、①新技術情報提供システム（NETIS）、②J-LIS LGWAN-ASP サービスリスト、③中小企業ワールドビジネスサポート（SWBS）、④ここからアプリ、⑤JNSA ソリューションガイド、⑥「テレワーク」を始めてみませんか？、の６つを選定した。上記の国内の既存の情報提供プラットフォームを調査するにあたり、（ア）意義・目的、（イ）運営者、利用者、提供情報、適用条件などの方向性、（ウ）利用者にとってのメリット、（エ）情報共有や情報比較などの提供機能、（オ）運営形態、（カ）収支構造に焦点を当てた。

① 新技術情報提供システム（NETIS）

(ア)意義・目的

公共工事等における、民間企業等で開発された有用な新技術の積極的な活用を支援するため、新技術に関わる情報の共有及び提供を目的とした、国土交通省のイントラネット及びインターネットで運用されるデータベースシステム。

(イ)運営者、利用者、提供情報、適用条件などの方向性

国土交通省が運営し、関係府省、地方自治体、公共工事等に係る事業者を利用者とする。新技術情報提供システム（NETIS）で提供されている情報は、従来技術との比較による、「経済性」「工程」「品質・でき形」「安全性」「施工性」「環境」の６項目の観点からの５段階評価（大幅に優れる、優れる、同等、劣る、大幅に劣る）と、概要、新規性及び期待される効果、適用条件、適応範囲、留意事項の項目により形成される。これらの情報は当該調査の対象となる工事等の完了までの適切な時期に実施される産・学・官からの事前審査と、利用者からの事後評価により担保されている。

(ウ)利用者にとってのメリット

新技術の情報の比較が可能。加えて、比較情報は産・学・官からの事前審査から担保されていることや、実際に利用者が活用した声の事後評価により、具体的な比較・検討を実施することが可能。

(エ)情報共有や情報比較などの提供機能

「公共工事等における新技術活用システム」という、民間事業者等により開発された有用な新技術を公共工事等において積極的に活用していくためのシステムがある。具体的には、新技術に関する情報収集と共有化、直轄工事等での試行及び活用導入の手続き、効果の検証・評価、さらなる改良と技術開発という一連の流れを体系化したもの。この一連の流れのうち、情報の収集と共有化の部分を担う。一方、事業

者マッチングや販売の機能は保有しない。

(オ)運営形態

運営の主軸は国土交通省だが、産・学・官で構成される新技術活用評価会議を所有する。また国土交通省により、プラットフォームの問合せ窓口を全国に構え、申請・相談に関する窓口は全国 19 か所、新技術全般に関する相談窓口は全国 21 か所に設置されている。

(カ)収支構造

サービス利用料（情報閲覧料)、登録料（新技術掲載料）無料で提供。

② J-LIS LGWAN-ASP サービスリスト

(ア)意義・目的

LGWAN－ASP(※)を活用することで、地方公共団体間の IT 化格差、IT 活用格差等を軽減し、品質及びサービスレベルの高いアプリケーションを地方公共団体間で共同利用することにより、地方公共団体の IT 化を促進し、かつ、地方公共団体が独自にシステムを構築するより、標準的で経済的なシステムを導入・運用すること。

※LGWAN：総合行政ネットワーク（Local Government Wide Area Network）は、地方公共団体の組織内ネットワークを相互に接続し、地方公共団体間のコミュニケーションの円滑化、情報の共有による情報の高度利用を図ることを目的とする、高度なセキュリティを維持した行政専用のネットワーク。

(イ)運営者、利用者、提供情報、適用条件などの方向性

地方公共団体情報システム機構が運営し、地方自治体(LGWAN 接続団体)、IT・通信サービス事業者を利用者とする。J-LIS LGWAN-ASP サービスリストで提供されている情報は、サービス分類、概要、URL、提供者名、問合せ先、LGWAN との接続時期といったサービス情報。これらの情報は「総合行政ネットワーク ASP 登録及び接続資格審査要領」にて情報提供者が審査を受けることにより担保されている。この審査は評価項目等を設けて点数をつける形ではなく、条件を満たす事業者を適切な情報提供者として判断するための審査。

(ウ)利用者にとってのメリット

標準的で経済的なシステム導入・運用が可能。加えて、地方公共団体に必要と考えられるネットワーク、サービス全般をパッケージでも、部分的にも、地方公共団体が選択して採用することが可能。

(エ)情報共有や情報比較などの提供機能

審査条件を満たしているサービスのサービス分類、概要、URL、提供者名、問合せ先、LGWAN との接続時期の項目で情報を提供。一方、事業者マッチングや販売の機能は

保有しない。

(オ)運営形態

地方公共団体情報システム機構にて運営。

(カ)収支構造

サービス利用料は無料。一方、情報掲載のための登録料は別途個別契約との記載があるため有償と思料する。

③ 中小企業ワールドビジネスサポート（SWBS）

(ア)意義・目的

海外展開に意欲的な中小企業と海外展開をサポートする企業・団体（SWBS 登録企業）とのマッチング、支援可能な地域や内容に応じた企業・団体の検索が可能で、海外展開に向けたネットワーク形成、掲載企業及び団体とのサイトを通じて具体的な相談海外進出を視野に入れる企業の海外進出計画の立案等、海外展開に意欲的な中小企業へファーストステップの支援。

(イ)運営者、利用者、提供情報、適用条件などの方向性

中小企業基盤整備機構が運営し、海外進出、もしくは海外進出支援を希望する企業及び団体を利用者とする。中小企業ワールドビジネスサポート（SWBS）が提供する情報は、支援内容、対象国、支援分野、関連キーワード、支援可能エリア、対応可能業態業種、URL、SWBS での支援実績、会社概要、問合せ窓口、支援フローといったサービス情報。これらの情報は中小企業基盤整備機構の事務局にて審査を受けることで担保されている。この審査は評価項目等を設けて点数をつける形ではなく、条件を満たす事業者を適切な情報提供者として判断するための審査。

(ウ)利用者にとってのメリット

海外進出の悩み解決や一次情報収集が可能。加えて、Yahoo!知恵袋や質問箱などの役割を担う掲示板があり、ユーザーの気軽かつ直接的なやり取りをプラットフォーム上で実現できる。

(エ)情報共有や情報比較などの提供機能

審査条件を満たしているサービスの情報を支援内容、対象国（カバーしている国と強みを持つ国）、支援分野（カバーしている分野と強みを持つ国）、関連キーワード、支援可能エリア、対応可能業態業種、URL、SWBS 上の支援実績、会社概要、問合せ窓口、支援フローの項目で比較可能な情報を提供。加えて、掲示板を設置し、サイト訪問者からの質問に答える、事例紹介、イベント紹介という形で事業者間のマッチングを提供。

(オ)運営形態

中小企業基盤整備機構にて運営。

(カ)収支構造

サービス利用料（情報閲覧料)、登録料（掲載料）無料で提供。

④ ここからアプリ

(ア)意義・目的

中小企業・小規模事業者の生産性向上を使いやすい、導入しやすいような業務用アプリ導入で実現するための支援。

(イ)運営者、利用者、提供情報、適用条件などの方向性

中小企業基盤整備機構が運営し、生産性向上の実現に向けて、困りごとを抱える中小企業を利用者とする。ここからアプリが提供する情報は、中小企業・小規模事業者向けの生産性向上アプリの概要、初期導入コスト、ランニングコスト、導入実績。これらの情報は中小企業基盤整備機構の事務局にて審査を受けることで担保されている。この審査は評価項目等を設けて点数をつける形ではなく、条件を満たす事業者を適切な情報提供者として判断するための審査。

(ウ)利用者にとってのメリット

中小企業・小規模事業者向けの生産性向上アプリの概要、初期導入コスト、ランニングコスト、導入実績等を参考にアプリを導入することにより、生産性向上の実現が可能。

(エ)情報共有や情報比較などの提供機能

審査条件を満たしている生産性向上アプリの概要、初期導入コスト、ランニングコスト、導入実績等。加えて、導入事例紹介、セミナー紹介という形で事業者間のマッチングを提供。

(オ)運営形態

中小企業基盤整備機構にて運営。

(カ)収支構造

サービス利用料（情報閲覧料)、登録料（掲載料）無料で提供。

⑤ JNSA ソリューションガイド

(ア)意義・目的

JNSA の会員企業が取り扱う、ネットワークやセキュリティ等に関する製品やサービス、イベント、セミナーの情報を提供し、セキュリティ対策の課題を解決するための支援。

(イ)運営者、利用者、提供情報、適用条件などの方向性

日本ネットワークセキュリティ協会が運営者し、中小企業をユーザーとする。JNSA ソリューションガイドが提供する情報は、統合型アプライアンス等に関する製品やサービス（概要、関連リンク、事業者名)、イベント、セミナーといったセキュリティ製品・サービス情報。これらの情報が掲載されている製品は、日本ネットワークセキュリティ協会の会員企業、当該企業が取り扱う製品・サービスが対象であり、掲載情報に関する審査・評価は実施しない。

(ウ)利用者にとってのメリット

JNSA の会員企業が取り扱う、ネットワーク、セキュリティ等に関する製品やサービス、イベント、セミナーの概要などを閲覧、導入することでセキュリティ対策の課題解決が可能。

(エ)情報共有や情報比較などの提供機能

会員企業が取り扱う製品・サービスの概要、関連リンク、事業者名の情報、イベント、セミナーの情報の共有。事業者マッチングや製品・サービス販売等、その他の機能は提供しない。

(オ)運営形態

日本ネットワークセキュリティ協会にて運営。

(カ)収支構造

サービス利用料（情報閲覧料)、登録料（掲載料）無料で提供。なお JNSA 会員企業の会費にて運営していると思料。

⑥ 「テレワーク」を始めてみませんか？

(ア)意義・目的

テレワーク導入の際に必要なガイドラインの確認､PC 等備品の比較･検討･購入等、テレワークの導入促進のための支援、テレワーク導入の包括的な支援。

(イ)運営者、利用者、提供情報、適用条件などの方向性

テレワーク導入推進コンソーシアムが運営し､テレワーク導入を検討している企業･団体を利用者とする。「テレワーク」を始めてみませんか？が提供する情報は、テレワークに関連するガイドライン情報、PC・ツールの情報（概要、参考価格、製品画像)、テレワークモデル、先行事例といったテレワーク関連製品情報、テレワークの普及促進のための情報。これらの情報が掲載されている製品は、テレワーク導入推進コンソーシアムの会員が取り扱うテレワーク関連製品が対象であり、審査・評価は実施しない。

(ウ)利用者にとってのメリット

テレワーク導入の際に必要なガイドラインの確認、PC 等備品の購入をユーザーが当該サイト上のみで一括で実施できることにより、テレワークの迅速・効率的な導入が可能。

(エ)情報共有や情報比較などの提供機能

会員企業が取り扱う製品の情報の共有。加えて、製品販売（サイト上の申し込みフォームから注文が可能)、テレワーク導入に必要なガイドラインの紹介を提供。

(オ)運営形態

テレワーク導入推進コンソーシアムにて運営。

(カ)収支構造

サービス利用料（情報閲覧料)、登録料（掲載料）無料で提供。なお会員企業の会費又は販売手数料にて運営と思料。

(2)中小企業向け情報提供プラットフォームのあるべき姿等に関する調査仮説とその考え方

中小企業向け情報提供プラットフォームのあるべき姿等についての検討すべき論点は、以下のとおりである。

論点①　意義・目的について、どのように位置づけるか
論点②　運営者について、どのように考えるか
論点③　申請情報について、情報の信頼性をどのような手法・運用体制で担保するか
論点④　登録の可否を判断するうえで、ベンダーから提供してもらうべき必要な情報は何か
論点⑤　提供機能としては、評価情報の提供までとするか、更にその先の事業者マッチングや製品・サービス販売等にまで踏み込むか
論点⑥　登録可否の判断や掲載可否の判断のルール化について、どのようなケースにおいて登録不可・掲載不可とするべきか
論点⑦　登録・掲載後、製品・サービスの内容に変更が生じたときに、どのような対応が必要になるか
論点⑧　情報提供プラットフォーム上で情報を探す際のインデックスの付け方について、どのように考えるべきか

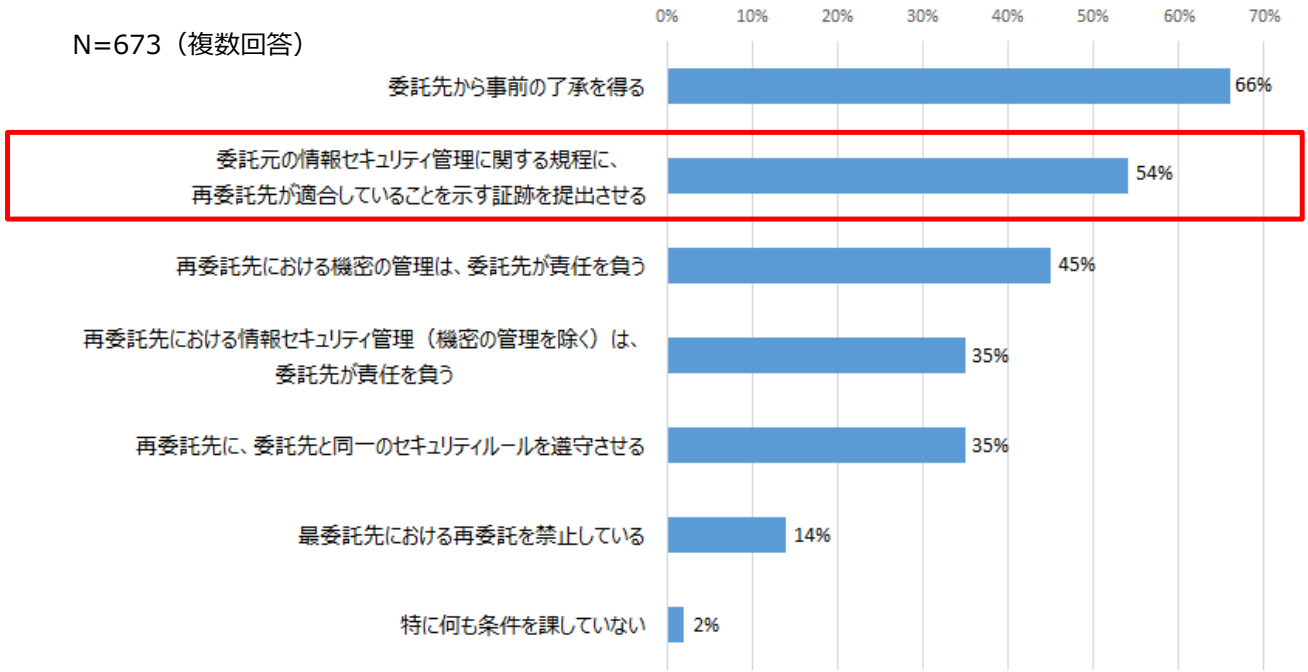
それぞれの論点ごとの調査仮説とその考え方を以下に示す。

(1)論点①に関する仮説の構築とその考え方

中小企業向け情報提供プラットフォーム構築の意義・目的については、中小企業におけるサイバーセキュリティ製品・サービスの導入のための支援や、中小企業におけるサイバーセ

キュリティ対策の課題を解決するための支援に資することを、調査仮説として取りまとめた。また、中小企業におけるサイバーセキュリティ対策の課題を解決するための支援においては、情報処理推進機構（IPA）が 2017 年 3 月に公表した「情報セキュリティに関するサプライチェーンリスクマネジメント調査報告書」の中で、「委託元が、委託先に対して再委託の許可を与える場合に、委託先の 54%に委託元の情報セキュリティ管理に関する規程に、再委託先が適合していることを示す証跡を提出させている」という結果が示されていることから、発注元が、契約先及び再契約先に求めるサイバーセキュリティ対策の領域をターゲットとすることとした。

図表 2-10 委託元が、委託先に対して再委託の許可を与える場合に遵守を求める情報セキュリティ管理の条件



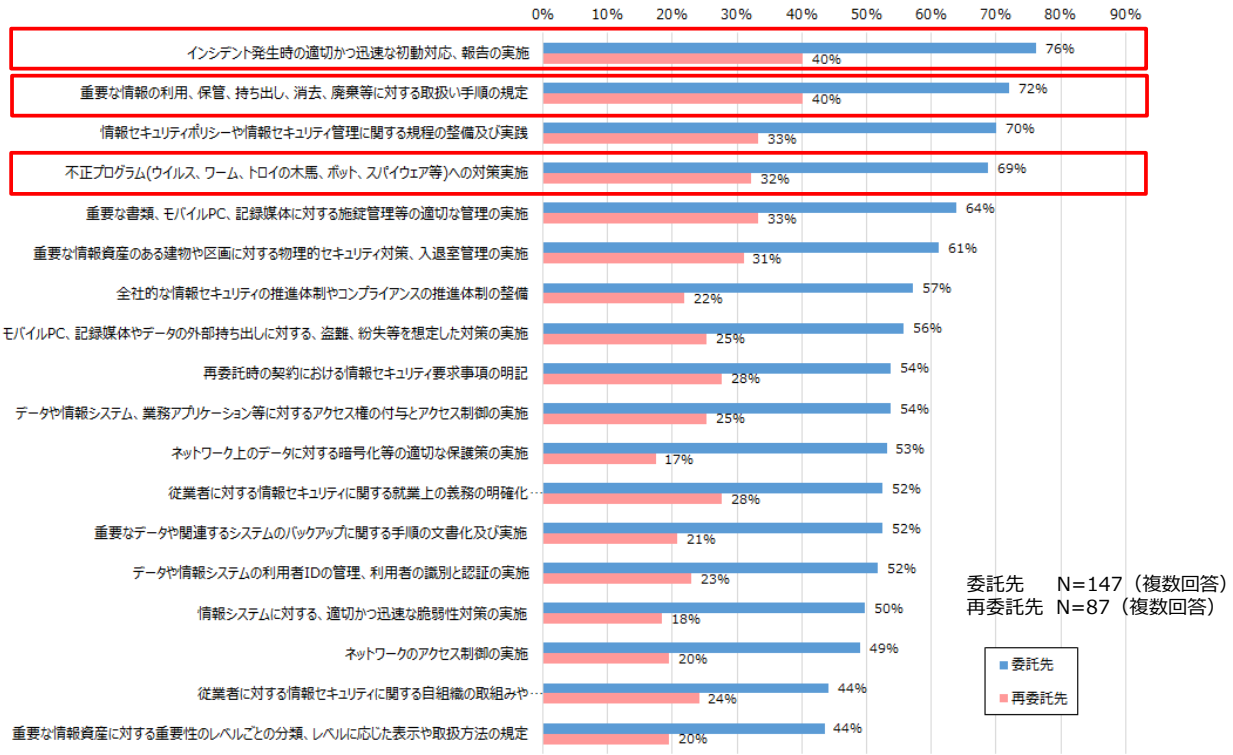
注）証跡の例としては、自己点検の結果や監査記録など

出所）「情報セキュリティに関するサプライチェーンリスクマネジメント調査報告書」（2017 年 3 月、IPA）

更に、発注元が、契約先及び再契約先に求めるサイバーセキュリティ対策の領域については、情報処理推進機構（IPA）が 2018 年 3 月に公表した「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」の中で、委託元が、委託先及び再委託先が最低限実施すべき情報セキュリティ対策として仕様書等に明記するもののうち、サイバーセキュリティ製品とは関係がない「情報セキュリティポリシーや情報セキュリティ管理に関する規程の整備及び実践」を除いて、「インシデント発生時の適切かつ迅速な初動対応、報告の実施」、「重要な情報の利用、保管、持ち出し、消去、廃棄等に対する取扱い手順の規程」、「不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、

スパイウェア等）への対策実施」の３つが上位であるという結果が示されていることから、①インシデント発生時の迅速な初動対応、②重要な情報の安全な取扱い、③不正プログラム対策の３つの対策に資するサイバーセキュリティ製品・サービスを、中小企業向け情報提供プラットフォームの登録対象とすることとした。

図表 2-11 委託先及び再委託先が最低限実施すべき情報セキュリティ対策として仕様書等に明記するもの



出所）「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」（2018年３月、IPA）

（2）論点②に関する仮説の構築とその考え方

情報提供プラットフォームの運営者については、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に則った形での客観的な評価が必要であり、更に評価における中立性・公平性が求められるという点を考慮すると、公的機関とすることに優位性があると判断し、情報提供プラットフォームの運営者は公的機関とすることを調査仮説として取りまとめた。

（3）論点③に関する仮説の構築とその考え方

申請・登録時にセキュリティベンダーから提供される情報の信頼性を担保する手法・運用体制については、「2.2.2. 情報の信頼性を担保するための検証手法に関する仮説の構築と

その考え方」で前述したとおり、モニターとして組織化された中小企業ユーザーによる事後評価を活用し、事後評価の結果を踏まえて、既に情報提供プラットフォームに登録されるサイバーセキュリティ製品・サービスに関する情報を見直し、必要となる修正登録や追加登録を行うことを、調査仮説として取りまとめた。

(4)論点④に関する仮説の構築とその考え方

登録の可否を判断するうえで、セキュリティベンダーから提供してもらうべき必要となる情報については、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に沿った提供製品・サービスの情報に加えて、ベンダーの信頼性・事業継続性についても確認できるようにするために、ベンダーに関する経営状況や反社会的勢力ではない表明等の情報や、提供製品・サービスに関する導入実績や導入事例、無料使用期間の有無等の情報も含めることを、調査仮説として取りまとめた。また、登録の可否の判断は、「2.2.2. 情報の信頼性を担保するための検証手法に関する仮説の構築とその考え方」で前述した評価会議で行うこととした。

(5)論点⑤に関する仮説の構築とその考え方

中小企業向け情報提供プラットフォーム上で提供する機能については、製品・サービスの導入促進のために、事業者マッチングや製品・サービス販売にまで踏み込んで機能を提供している類似分野のプラットフォームが見受けられるものの、先ずは中小企業におけるサイバーセキュリティ製品・サービス選びの一助となる情報提供を目指していることから、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に沿った提供製品・サービスの評価情報を提供することを、調査仮説として取りまとめた。

(6)論点⑥に関する仮説の構築とその考え方

登録可否の評価方法については、申請時にセキュリティベンダーから提供される情報の信頼性、妥当性の担保を、「2.2.2. 情報の信頼性を担保するための検証手法に関する仮説の構築とその考え方」で前述した評価会議による検証・評価だけで全て充足することには自ずと限界があることから、申請書に不備がなく、内容面もしっかりと記載されているか、カタログ等と照らし合わせてみた場合に虚偽の記載がないか、反社会的勢力に加担していないかなどの形式的なチェックにおいて判断し、必要に応じてセキュリティベンダーから提供される情報を中心に申請書の内容を確認するためのヒアリングを実施することを、調査仮説として取りまとめた。

また、情報提供プラットフォーム上で公開された情報の掲載取り消しの評価方法については、登録申請者であるセキュリティベンダーが重大なインシデントを起こした場合や廃業した場合に加えて、虚偽の記載が発覚した場合や、M&A 等により運営主体・体制や運営ポリシ

ーに変更が生じた場合に掲載を取り消すことを、調査仮説として取りまとめた。

(7)論点⑦に関する仮説の構築とその考え方

登録後に提供製品・サービスの内容に変更が生じたときに必要となる対応については、情報提供プラットフォーム上に掲載される情報は、あくまで申請・登録時の時点評価に基づく参考情報であることから、登録申請者であるセキュリティベンダーから申請された情報に基づくものであるというエクスキューズを入れて掲載すること、更にその情報を使うかどうかの判断は中小企業に委ねることを、調査仮説として取りまとめた。一方で、掲載された情報の陳腐化を回避するため、提供製品・サービスの内容に大幅な変更が生じたときには、登録申請者であるセキュリティベンダーに対し、報告の義務を課すこととした。また、運営主体・体制や運営ポリシーの変更、採用技術・システムの変更等を大幅な変更と考えることとした。

(8)論点⑧に関する仮説の構築とその考え方

中小企業は、売上高や従業員の規模を始めとして、業種、IT 利用環境、商慣習などが多種多様であり、中小企業を一律に一括りにすることが難しく、情報提供プラットフォーム上で求められる情報も異なることから、中小企業向け情報提供プラットフォーム上で必要となる情報を探す際のインデックスを付けることを、調査仮説として取りまとめた。

3. 検証結果とそこから得られた示唆

3.1. 導入実証による評価項目の有効性検証結果

3.1.1. 中小企業ユーザーに対するヒアリング調査結果

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の有効性を検証するため、中小企業ユーザーに対するヒアリング調査を行い、各評価項目に沿って、製品・サービスの導入・運用時における状況や対応内容、求めるレベルや範囲、重視度合い（「かなり重視される」「ある程度重視される」「あまり重視されない」「全く重視されない」の４段階での評価）を把握した。

中小企業ユーザーに対するヒアリング調査結果を以下に示す。

（1）導入のし易さの観点からみたヒアリング調査結果

① 大規模なシステム改修を伴わず、実装が容易である

【ヒアリング調査結果】

	重視度合い	本検証における状況・対応内容	求めるレベル・範囲
A 社	かなり重視	・システム改修は不要	・経営者の目線で見ると、システム改修は発生しない方がよい。システム関連の設備投資はなるべく平準化したい。 ・ネットワークの口（通信ポート）をできる限り増やしたくない。 ・ホストのサーバが１台あって、そこですべての PC を一元管理できるようになるなど楽なものがあればよい。 ・導入するにあたって、システムを停止する必要がなかったので、導入がスムーズであった。
B 社	ある程度重視	・システム改修は不要	・具体的コメントなし。
C 社	ある程度重視	・システム改修は不要	・端末の外部持ち出しを制限するようなケースなどシステム改修を伴う場合には別途費用がかかり、会社としての判断や関係部署との調整が必要になるが、今回はシステム担当だけでインストールなどの対応が可能であったため、楽であった。
D 社	ある程度重視	・システム改修は不要	・既存の基幹系システムの設計思想にはセキュリティの概念が入っておらず、いずれ全面改修が必要となる。改修が必要になるのであれば、タイミングを合わせて、一気に全面改修を実施したい。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
E 社	かなり重視	・システム改修は不要	・導入時にシステム改修が必要になることは導入の決断をしづらくさせる。 ・システム改修の規模にもよるがなるべく発生しないほうが良い。
F 社	ある程度重視	・システム改修は不要	・メインで利用している基幹システムが取引先用にカスタマイズされているため、基幹システム以外のサービス・製品を選ぶ際に、基幹システムに影響を与えないことが最も重要である。 ・基幹システムに影響を与えない程度のシステム改修なら程度により実施可能だが、すべての PC でシステム改修の実施が必要になるのは手間になるため難しい。

② 現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・ 不要な機能が全くない ・ ログ管理の機能が必要	・ 管理コンソールがあるとよい。何かあったときに確認できるように状態が見えるとよい。 ・ Mac の PC にインストールできるとよい。 ・ PC のシステムパフォーマンスへの影響を考慮すると、データを収集するタイミングをユーザー側で選べるようになるとよい。業務時間外にできるとよい。 ・ PC 内の作業内容・時間を見ているのであれば、管理コンソールでそのログも見えるとよい。
B 社	ある程度重視	・ 不要な機能が全くない ・ 必要となるオプション機能はない	・ アイコンがない。ウイルス対策ソフトは、稼動しているか、最新の状態になっているかを確認したり、手動でスキャンしたりすることができる。ウイルス対策ソフトと比較すると、静か過ぎて、慣れるまでは違和感がある。 ・ 最初、満足感が得られるまでは必要最小限の機能を安く使い続けることができるとよい。5 年ぐらい使い続けて、その後、オプションを選んで機能を充実させることができるとよい。次々に新しい製品や新しい機能が提供されるのは避けたい。
C 社	ある程度重視	・ 不要な機能が全くない ・ 必要となるオプション機能はない	・ お試し利用をできるようにしてほしい。インシデントが発生した時に、どのようなやりとりが必要になるかが分からないので、お試し利用の中で擬似的なインシ

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			デント対応訓練を経験でき、必要となるやりとりを見える化できるとよい。経営層に対して、製品を導入した意味を説明しやすくなり、無駄なコストをかけなくて済む。 ・ ISMS 審査でクラウド運用のセキュリティについて指摘を受けている。社内のネットワーク上のファイルサーバについては、いつ、誰が、どんなファイルを見ているかがアクセスログの監視を通じて分かるようになっているが、クラウドを使っている場合にも同様のことが分からないといけない。
D 社	かなり重視	・ 不要な機能は全くない ・ 数は少ないが、必要となるオプション機能はあった	・ エンドユーザーコンピューティングのインフラとしてみた場合には、最低限必要な機能が用意されている。(アプリケーションの機能としてみた場合には、機能が足りていない可能性がある) ・ OEM の良い面が出ている。世の中で普及している大手セキュリティベンダーの製品が用意されていて、相乗りで安価に提供されているのが非常に良い。 ・ クラウドアップセキュリティは IT・セキュリティのリテラシーが必要になるので、導入の際に伴走してくれる機能がほしい。 ・ オプションになっているログの月次レポートやログの相関分析も、一体的に提供してもらえる方がよい。 ・ セキュリティ設計は難しい。自社で必要な製品を選ぶのが難しい。このような製品・機能が必要であると決めてくれているのは助かるし、安心できる。表側に製品・機能があって、表頭に利用システム・利用環境があるマトリクス形式で必要な製品・機能が示されていると分かりやすくてよい。
E 社	ある程度重視	・ 不要な機能は全くない	・ オーバースペックであることで料金が高くなるのであればオプション制にしてもらい、元の機能はシンプルで安価な方が良い。
F 社	ある程度重視	・ 不要な機能は全くない ・ 機能全体を把握できているか不明なため、気にもしない	・ PC のメモリを過剰に取らない、PC の動きが重くならない範囲であれば機能が多くても構わない。 ・ 一方で機能が多数搭載されていても使いこなせるかどうかは不明。

ヒアリング調査を実施する中で、中小企業ユーザーにおいては、PC に必要となる機能を

インストールした後にPCの動作が重くなることを敬遠することが分かったため、PCのシステムパフォーマンス等への影響が小さいという評価項目を追加し、参考扱いでヒアリング調査を実施した。以下にヒアリング調査結果を示す。

○追加した評価項目（参考）：PCのシステムパフォーマンス等への影響が小さい

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A社	かなり重視	・ディスクアクセスへの負荷が大きい、メモリの使用率が高い	・PCのシステムパフォーマンスが低下すると社員からのクレームに直結しかねない。 ・推奨されるシステム要件の情報が提供されているが、PCの使い方は各社で異なるため、メモリの使用量などの実際の運用実績を知りたい。 ・この種の製品･サービスは、お試し利用で性能を確認・検証してから導入した方がよいと感じた。
B社	ある程度重視	・PCの動作が重くなった実感はない	・部からPCのシステムパフォーマンスが低下したという報告を受け、そのPCを調べたところ、古いPCで積んでいるメモリも小さいことが判明したので、PCのスペックが原因と判断した。
C社	ある程度重視	・PCの動作が重くなった実感はない	・予備のPCにインストールし、システムパフォーマンスへの影響を確認した後、本格的に導入を実施した。インストールした後にPCが使えないようなことになり、業務が滞留してしまうことは避けたい。 ・PCのスペックが良くなっているので、一昔前にウイルス対策ソフトをインストールしたときに、システムパフォーマンスが下がったようなことは起きない。 ・機能自体が成熟化していて、いずれも使い勝手がよくなっている。必要な機能が十分入っていて余計な機能はない。余計な機能が入っていて、PCのシステムパフォーマンスが下がったり、費用追加されるのは避けたい。
D社	かなり重視	・PCの動作が重くなった実感はない	・従来のエンドポイントセキュリティ製品は、１日１回のフルスキャンで、PCのシステムパフォーマンスが下がるものであると思っていたが、本製品はそのような感じが全くなく、システムパフォーマンスを犠牲にしなくて済んだのはよかった。もはや元に戻すつもりはない。
E社	ある程度重視	・PCの動作が重くなった実感はない	・セキュリティ製品全般としてインストールすれば多少なりとも動作が遅くなるも

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			のだと思っていたが、本製品はごく稀に少し重くなったなかと思う程度であるためとても良い。
F 社	かなり重視	・ PC の動作が重くなった実感はない	・ PC を操作する際に業務に支障が出るほど動作が重くならないのであれば気にならない。 ・ 本製品は導入前と後でPC操作に何の変化もないので問題ない。

③ いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・ 設定が全く必要ない ・ 管理者はシステム担当の専業者ではなく、研究開発担当も兼務しており、時間的な制約が大きい	・ インストールのみで、設定は不要であるため、導入は楽である。PC１台あたり、インストールに５分もかからない。 ・ マニュアルがあれば誰でも導入可能である。事前のベンダーとの打合せが不要であることもよい。 ・ 設定不要(設定はベンダー側のみ)で、管理コンソールを通じて、すべての PC を一元管理できるようにしてほしい。
B 社	ある程度重視	・ 設定が全く必要ない	・ 市販のソフトよりもインストールが難しいという印象であったが、マニュアルを見ながら、“次へ”、“次へ”と進むだけで普通にインストールができ、楽である。 ・ お手軽が一番なので、設定はない方がよい。
C 社	ある程度重視	・ 細かくはないが、ある程度の設定が必要になった	・ Office 製品の管理者のアカウントを登録するのみの設定で監視できるようになるのは楽であった。
D 社	あまり重視されない	・ クラウドアップセキュリティについては、細かくはないが、ある程度の設定が必要になった ・ エンドポイントセキュリティについては、メールでセキュリティプロファイルが配布され、ソフトウェアをダウンロードしてインストールするだけである ・ セキュリティサポートデスクについては設定が全く必要ない	・ クラウドアップセキュリティについては、一部の設定に苦労した。導入の際に伴走してくれる機能がほしい。お薦めの設定もあるとよい。 ・ エンドポイントセキュリティについては、ソフトウェアをインストールするとき、お薦めの設定が提示され、そのまま設定することなく使えるようになっているのはよい。 ・ セキュリティサポートデスクについては、導入時に何かつまずいた場合に、よろず相談において、どのように対応すればよいかを教えてくれるのは安心できる。
E 社	ある程度重視	・ 設定が全く必要ない ・ 設定に当てはまるかはわからないが、社内で利用してい	・ 専門的な知識がない者でもガイドライン等を見ながら実施できる範囲であれば負担にならない。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
		る外部システムの証明書発行が必要であったため実施した	
F 社	かなり重視	・ 設定が全く必要ない	・ 今回の製品は 1 台あたりの設定がインストール 5 分程度で済んだため負担が軽く良かった。 ・ 設定不要で、すべての PC を一元管理できるようにしてほしい。

(2)運用のし易さの観点からみた評価項目に関する仮説の構築とその考え方

① 社内に専門的な人材がいなくても、メンテナンスが可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・ 専門的な人材によるメンテナンス対応は全く必要ない	・ 中小企業においては、セキュリティ分野の人材リソースを確保するのが困難である。外部のセキュリティベンダーの人材リソースを活用して、運用体制を構築できる点がよい。 ・ 各PCにおけるソフトウェアのアップデート等の更新が、管理者の手を離れるのはよい。自動更新できるに越したことはない。 ・ 但し、何に対応するためのものであるか、どのような影響が起こり得るかといった情報は入手しておきたい。
B 社	ある程度重視	・ 専門的な人材によるメンテナンス対応は全く必要ない	・ ウイルス対策ソフトは使い始めてから５年間設定を変更したことがないが、本当にそれでよいのかどうか不安になる。セキュリティベンダー側がバックエンドで適切なメンテナンスをしてくれる方がよいが、今回の製品・サービスにおいても、ウイルス対策ソフトと同様に、何もアクションを起こす必要がなければ不安になるので、せめて、どのようなメンテナンスを実行したかといった情報は教えてもらいたい。
C 社	かなり重視	・ 専門的な人材によるメンテナンス対応は全く必要ない ・ 日々メンテナンスを行うような形態の製品・サービスではない	・ システム担当者を２名置いているが、兼務であり、インシデントが発生した場合でもすぐに動くことができない。余裕を持てるほど専門的な人材を確保することはできない。 ・ Web ベースであるため、客先で管理コンソールにアクセスして、状態を把握できるようになっているのはよい。
D 社	かなり重視	・ 専門的な人材によるメンテナンス対応は全く必要ない	・ 専門的な人材を用意することや、運用コストをかけることはできないので、セキ

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
		・仮想 UTM の場合、最初にセキュリティベンダーから質問を受けて、自社のセキュリティレベルを設定する。 ・現在は標準レベルで設定している ・対応レベルが決まっているので、インシデント発生時に何が(どこが)問題であったかを把握しやすい	ュリティベンダー側でメンテナンスしてくれるのは非常によい。
E 社	ある程度重視	・専門的な人材によるメンテナンス対応は全く必要ない ・日々メンテナンスを行うような形態の製品・サービスではない	・頻度、かかる時間による。 ・インストール同様､5 分程度の時間でクリックして進めるだけで可能なメンテナンスであれば、専門的な知識がなくても実施可能なので問題ない。
F 社	ある程度重視	・専門的な人材によるメンテナンス対応は全く必要ない ・日々メンテナンスを行うような形態の製品・サービスではない	・メンテナンスを実施するとすれば頻度、内容による。 ・内容が難しく専門的な知識が必要なのであれば自動更新や、専門担当者に実施してもらいたい。 ・頻度は年に 1 回、四半期に 1 回程度なら許容範囲だが、月に 1 回等は負担が大きいので避けたい。

② 万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である

万が一インシデントが起きた場合の対応の省力化に関するヒアリング調査結果と､勤務時間外の対応の省力化に関するヒアリング調査結果を２つに分けて以下に示す。

②－１　万が一インシデントが起きた場合の対応の省力化が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・実際にインシデントは起きていない ・アラート通知も届いていない	・アラートが出た後、自社側で積極的なアクションを起こす必要がなく、ベンダー側ですぐに対応してくれれば、省力化になり､役に立つと思う。但し､いざという時に困らなくて済むように、どのようなアクションが必要になるかを明確にしておいてほしい。
B 社	ある程度重視	・実際にインシデントは起きていない ・アラート通知も届いていない	・インシデントが発生すれば、先ずはディストリビュータに問合せを行い、対応や指示をしてもらうことになる。最初は電話で問合せできることが必要である。問合せへの自動音声対応は実施してもらい

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			たくない。
C 社	ある程度重視	・実際にインシデントは起きていない ・アラート通知も届いていない	・勤務時間内であれば、ある程度までは、自社でも対応可能である。インシデントが発生した場合、どの範囲にまで被害が及んでいるか、すぐに把握しないといけないので、それができるようになっていた方がよい。 ・何か人為的ミスや内部不正があれば、後からログを見て、誰が、どういう操作・悪さをしたかを確認できることが重要である。それを社員に周知すれば抑止力になる。
D 社	ある程度重視	・実際にインシデントは起きていない	・インシデント発生時には、フォレンジックサービスなど、必要となるサービスの窓口を紹介してもらえる。またアドバイスで、このような対応を行った方がよいという道筋を示してもらえるのはよい。なお、このようなインシデント対応に係る費用は保険の支払いで賄われ、1,000 万円分のインシデント対応に係る作業をしてもらえるという考え方に立つと、設定された価格は受容できる。
E 社	ある程度重視	・実際にインシデントは起きていない	・インシデント時に連絡するよう問合せ窓口が記載されているが、加えて自社で対応できるものがあれば実施できるようにマニュアル等の記載があれば良い。 ・インシデントが発生した際に、その PC だけで被害は済むのか、リカバリーにどの程度の時間を要するのかも事前に想定インシデントとして把握できると尚良い。
F 社	ある程度重視	・実際にインシデントは起きていない	・インシデントが起きたとしても自社側で実施できる対応は限られており、自信がないため担当者にすぐ連絡がつく等の人員的な対応を期待する。

②－２　勤務時間外の対応の省力化が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	あまり重視されない	・勤務時間外の対応は不要	・夜間などの勤務時間外に何かインシデントが発生して、メールで連絡をもらったとしても、対応のしようがないため、勤務時間外の対応については考える必要がない。
B 社	あまり重視されない	・勤務時間外の対応は不要	・勤務時間外には会社に社員がいないため、対応は不要であると考えている。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
C 社	全く重視されない	・勤務時間外の対応は不要	・勤務時間外に顧客側のシステムにインシデントや障害が発生した場合、緊急対応が求められるが、対応は顧客側が担当している。勤務時間外の対応は不要である。
D 社	あまり重視されない	・勤務時間外にシステム障害が発生した場合には、セキュリティベンダーの対応窓口が閉鎖しているので何も対応できず、いざとなれば緊急遮断するしかない ・どうしようもないため、あまり気にしていない	・夜間などの勤務時間外に呼び出されるのは避けたい。インシデントが発生したとしても、結局、自分たちは何もできない。専門的な人材に対応を依頼するしかない。
E 社	あまり重視されない	・勤務時間外の対応は不要	・担当者の外出も多いため、なるべく業務のスケジュールに影響が出ないように勤務時間外の対応が必要になることは避けたい。
F 社	あまり重視されない	・勤務時間外の対応は不要	・原則事務職が PC を操作するため、勤務時間外の対応は避けたい。 ・内容･目的･頻度によっては対応せざるをえないと理解している。

③ 問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・問合せ･相談窓口を利用しなかった	・トラブルやインシデントの場合、問合せへのレスポンスは早いに越したことがない。遅くとも 2 時間以内での解決が必要。 ・管理コンソールが用意されていないのであれば、エラーやトラブルが発生したときのために、ベンダーのホームページ上にトラブルシューティングや Q&A が用意されていて、ユーザー企業はそれを見て対応できると良い。
B 社	ある程度重視	・問合せ･相談窓口を利用しなかった	・問合せ･相談窓口の説明は、カタログやパンフレットに分かりやすく明示してもらいたい。問合せ先のメールアドレスはまだ見つけやすいが、問合せ先の電話番号は見つけにくくなっている。電話で問合せ･相談したい人にとっては、問合せ先の電話番号が見つけやすいほうが良い。 ・最近は、チャットで問合せ･相談できる製品・サービスもあり、レスポンスも速い。セキュリティ製品・サービスにおいても、そのような機能があると便利である。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
C 社	ある程度重視	・アカウントの登録でエラーが発生したため、問合せ・相談窓口を利用した	・問合せをした当日に設定ミスの連絡が入り、設定を修正したら、解決した。 ・双方のやりとりについては、特段ストレスはなかった。レスポンスがないとなると不安になる。
D 社	ある程度重視	・設定が上手くできなかったため、問合せ・相談窓口を利用した	・電話もメールも繋がり、双方のキャッチボールができた。窓口対応のサポートメンバーの感じもよかった。 ・調査の時間が必要になり、回答は翌日以降になった。導入時の問合せ･相談については、それぐらいのスピード感でもよいが、インシデント発生時の問合せ･相談においては、もう少し対応レスポンスが早い方がよい。 ・実際に稼働できるまではもっとサポートして伴走してもらえると助かる。 ・今回はたらい回しやマニュアルどおりの回答を読み上げて押し切ることはなかったが、もしそのような対応の悪いセキュリティベンダーの場合には、時間も取られるし、気持ちも削られる。
E 社	かなり重視	・問合せ･相談窓口を利用しなかった	・問合せ窓口の対応力も必要だが、トラブル対応集がホームページ上などで掲載されていると良い。 ・今回の製品ではホームページ上の Q&A が高い頻度で起きやすいものから順に掲載されており、理解しやすかった。
F 社	かなり重視	・問合せ･相談窓口を利用しなかった	・問合せ窓口の電話番号がわかりづらい、電話がつながらない等は不満に思う。 ・よくあるお問合せや Q&A が丁寧に作成されていると良い。

(3)導入や運用を行うことで得られる効果の観点からみた評価項目に関する仮説の構築とその考え方

① 導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・新たな機能追加は全く必要ない	・PC の安定的な稼動を最優先に考えているため、余計な機能の追加は避けたい。 ・オプションサービスを利用しなければいけない状況がどの程度発生するか、その

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			ときの追加費用がいくらぐらいになるかが気になる。セキュリティ対策の年間予算(10～20 万円)に収まるぐらいがよい。 ・ 自らがマルウェアを駆除するのは難しいため、オプションの駆除サービスが信頼できるのであれば、対応してもらった方が楽である。
B 社	あまり重視されない	・ 新たな機能追加は全く必要ない	・ 機能の追加を求めるのであれば、導入の際に説明してもらいたい。総合的な安心・安全を確保するために、自信をもって中小企業ユーザーに使ってほしい製品・サービスであれば、セキュリティベンダー側は最初からそのような機能は組み込んでほしい。
C 社	かなり重視	・ 新たな機能追加は全く必要ない	・ 追加費用が掛かるのは避けたい。機能追加はバックエンド側で実施されていて、機能追加も含めて定額でサービスが提供されていた方がよい。
D 社	かなり重視	・ 新たな機能追加は全く必要ない	・ 機能追加が求められるカスタマイズ製品は使いたくない。
E 社	かなり重視	・ 新たな機能追加は全く必要ない ・ そもそもオプションになっている機能がない	・ オプションであるなしに関わらず追加費用が掛かるのは避けたい。
F 社	かなり重視	・ 新たな機能追加は全く必要ない ・ そもそもオプションになっている機能がない	・ 導入する際に十分な効果を得るため、スムーズな運用をするためにかかる総コストはオプション等で後回しにせず教えてほしい。 ・ 費用対効果によるが、必要であればオプションを追加することも可能。

② サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・ 必要最小限だが、新しい知識の習得が必要	・ 技術情報は不要であるが、インストールするソフトウェアが何に関わるソフトウェアであるのかは最低限知っておきたい。例えば、動作の安定に必要なソフトウェアである、パフォーマンスへの影響があるソフトウェアであるなど。
B 社	ある程度重視	・ 必要最小限だが、新しい知識の習得が必要	・ どのような脅威に対応できる製品であるかを知っておきたい。全く何も知らないでインストールするのは好ましくない。
C 社	ある程度重視	・ 新しい知識の習得が全く必	・ 製品の説明には、専門用語が多く出てく

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
		要ない ・すべて既に知っている範囲の知識で対応できた	る。 ・権限のアカウントを登録するという作業は、ある程度知識がないと対応できない。 ・今回の製品・サービスはシステム担当者で対応できたが、学習コストを掛けないといけないような製品・サービスは敬遠する。そのようなコストを掛ける余裕がない。
D 社	あまり重視されない	・必要最小限だが、新しい知識の習得が必要	・セキュリティ側の知識はそれほど必要ではないが、使用されているアプリケーションの管理側の一部でシステム側の知識が必要であった。 ・新しい知識を蓄えていくこと自体は会社にとってプラスである。もちろん専門的な人材の確保が限られる中で限界はあるが、適切に使えるようになることや、何かあったときに対応できるようになることは必要である。
E 社	ある程度重視	・新しい知識の取得が全く必要ない	・良い製品に対応するために若干知識を身につける程度は実施可能。 ・マニュアル等を読んで理解し操作する程度であれば負担に感じない。
F 社	かなり重視	・新しい知識の取得が全く必要ない	・手間がかからないことが大切。 ・新しい知識であっても丁寧なマニュアルなどがあり、PC スキルの低い人でも実施可能な範囲であれば良い。

(4)導入時や運用時に要する費用の観点からみた評価項目に関する仮説の構築とその考え方

① 導入コストが安価である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった)	・イニシャルコストは気にする。何年もかけて償却できるのであれば、イニシャルコストとして支払う方がよい場合もある。
B 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった)	・自社の導入規模や導入環境、求めるセキュリティ性能に照らして、他製品との比較表で、コスト面で優れているところを示してもらいたい。それが分かると真剣にセキュリティベンダーの話を聞こうという気になる。 ・イニシャルコストとして支払う場合でも、ボリュームディスカウントが効き、ト

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			ータルコストが安いものであれば魅力的である。
C 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった)	・クラウドのメリットは初期投資が少なくて済むことである。
D 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった)	・製品を個社から調達するとイニシャルコストが高くなる。新しい脅威が次々に発生し、その都度すぐに新しい機種の製品が提供されるので、サービスとして調達できる方がよい。UTM だけでなく、エンドポイントセキュリティについても、現在導入済みの製品よりも安くなっているのでよい。
E 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった) ・本製品はイニシャル兼導入コストとなっている	・本製品は使用してみて費用対効果に満足している。 ・導入コストが安い製品はとりあえず使ってみようという気持ちになり、採用されやすいと思われる。 ・お試し版やお試し価格等があれば尚良い。
F 社	かなり重視	・イニシャルコストは掛からない(高額には全く感じなかった) ・本製品はイニシャル兼導入コストとなっている	・本製品は使用してみて費用対効果に満足している。 ・導入コストが高いと検討の俎上にあがらない。 ・費用感がわからないが、安かろう悪かろうは避けたい。 ・セキュリティ製品全般に対する知識が少ないため、安いのか高いのか判断ができない。

② 運用コストが安価である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・高額には感じない	・平常時はマルウェアを監視し、これによりインシデント発生時の対応もスムーズになるため、必要であるが、導入時点では、まだ効果や信頼度が分からない。このような効果や信頼度を実感できるまで、お試し期間として利用できるようになるとよい。 ・セキュリティ運用のトータル費用としてみた場合に、インシデント対応費用はいずれ必要になる費用であるため、それがサービスに含まれる保険でカバーできるのは魅力的である。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
B 社	ある程度重視	・許容範囲であり、あまり高額には感じなかった	・現在使用のウイルス対策ソフトは年間 13,000 円で、インストールの台数に制限がなかった。それよりは少し高額であるが、許容範囲である。 ・必ずしも安くなければいけないという訳ではない。セキュリティベンダー側で限界を超えて安値対応すれば、付加価値がなくなり、サービスが疎かになる。それは避けたい。 ・世の中で騒がれているような脅威やマルウェアが本当に食い止められるのかどうか、できれば半年など一定期間、実際に使ってみて、効果を確認したい。
C 社	かなり重視	・必要最小限の費用だが、高額に感じた	・リースと同じ感覚で使い続けられるのはよい。 ・保険がつくのは安心材料であり、トータルでみた場合は、必要最小限の費用になっていると感じる。 ・どの製品・サービスも性能や使い勝手が似たり寄ったりになってきているので、製品・サービス価格が上がれば、別の製品・サービスに乗り換えることで済んでしまう。そのため結局、製品・サービス選びでは、価格重視になってきている。
D 社	かなり重視	・高額には全く感じなかった ・個人情報の保有件数をもとにリスク評価を行い、万が一個人情報が漏洩した場合の損失額を算出している。 ・リスク評価の外注コストは高すぎてそこまでコストをかけられないので、簡単にアセスメントができるツールがあるとよい	・万が一、個人情報が漏洩した場合の損失額と比べれば、ランニングコストは見合う額である。 ・何か問題が発生したときに、問合せ･相談できるという部分は安心料である。
E 社	かなり重視	・許容範囲であり、あまり高額には感じなかった	・２カ月弱使用してみて費用対効果に満足しているため、来年以降も継続利用を検討中。 ・セキュリティインシデントを起こしたことがある企業であれば高額に感じないであろう。 ・規模が大きいほど PC の台数も増えるため、1 台あたり年間 1 万円弱かかるのは負担に感じるであろう。 ・可能であれば 1 台あたり年間 5 千円程度になると魅力的に感じる。
F 社	かなり重視	・許容範囲であり、あまり高額には感じなかった	・セキュリティ製品全般に対する知識が少ないため、安いのか高いのか判断ができ

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			ない。 ・ しかしながら、２カ月弱使用してみて費用対効果に満足しているため、来年以降も継続利用を検討中。 ・ 運用コストが高くて効果の実感を得られないと解約に繋がりやすい。 ・ 費用感がわからないが、安かろう悪かろうは避けたい。

(5)導入や運用における課題の解決の観点からみた評価項目に関する仮説の構築とその考え方

① 製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠（利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等）に基づく、適切な説明がなされている

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・ ある程度客観的な根拠が示されていたが、疑問点もあった	・ PC 内のデータや、PC での作業内容・時間が、ベンダー側にどの程度見られているのか不安である。ホワイトハッカーにどの程度の信頼を置いてよいのかユーザーには分からない。 ・ ホワイトハッカーチームが何人編成であるのか、どのようなバックグラウンドやプロファイルを持つ専門家が担当するのか、実績(こういうマルウェアについて何件のトラブルが発生し、その駆除に何時間で対応し解決できた等)がどれぐらいあるのかといった情報を提供してほしい。 ・ ホワイトハッカーにも認定制度があるのなら、そのような認定を受けたホワイトハッカーであれば信用できる。 ・ 導入実績や、未知の脅威の検知実績などの情報を提供してほしい。
B 社	ある程度重視	・ 疑問が全く生じなかった	・ ホワイトハッカーが脅威を監視・発見してくれるということで安心できる。 ・ 使用中のウイルス対策ソフトのベンダーは、数々の賞を受賞していたが、やはりそういうものに目が行く。 ・ 何かインシデントが発生したときに、差が出る。そのインシデントを防げないということになれば、この製品･サービスは駄目ということになる。様子を見ていくしかない。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
C 社	かなり重視	・ 疑問が全く生じなかった	・ 運用している限り、経営層から効果があるのかどうかを問われる。鍵となるのは、何かインシデントが話題に上がったときに、対応できることである。それができないと何も意味がない。インシデント検知を経験できるように、お試し利用の期間が設定されているとよい。 ・ 安心を買う製品･サービスの場合には、継続性が重要である。
D 社	かなり重視	・ 疑問が全く生じなかった	・ 知名度の高いセキュリティベンダーは信頼しやすいので、金額さえ折り合えば、疑念は生じない。他方、知名度の低いセキュリティベンダーは、信頼できるかどうかを調べるために時間が必要になる。 ・ 導入実績やシェアが気になる。何台の PC に導入･運用されているか、サポートデスクの場合には、何社に対してサービスを提供しているのか、定量的なデータが必要である。多くの会社や PC に導入されているものであれば、ノウハウが蓄積され、コストも下がっていく可能性があり、良いものだと思う。
E 社	かなり重視	・ 疑問が全く生じなかった	・ 従来のセキュリティ製品にはない観点で、トラブルの根源から防ぐという機能に納得して導入した。 ・ パンフレットやカタログにはなるべく実績や認定などの評価を載せてほしい。 ・ 掲載内容と価格を比較して導入可否を決めるため、十分な説明が求められる。 ・ パンフレットに性能・スペックを記載する際には、ユーザー目線に立って「こんなメールが来た時の不安」や「こんなポップアップがでてきたときの不安」をこのように解決しますという、馴染みやすい言葉で専門用語を使わずに説明してほしい。専門用語が使用されていると社員によっては理解が及ばず、社内全体への浸透が難しくなる。
F 社	かなり重視	・ 疑問が全く生じなかった	・ 経営者としてもセキュリティは気になるところだが専門知識がないため、信用しており自社の状態をよく理解しているディストリビュータの担当者が奨める製品は信頼する。 ・ セキュリティ製品に関する知識がないため、導入実績や具体的に解決してくれる悩み等を記載してもらえると理解しやすい。

(6)製品・サービスの経営へのインパクトの観点からみた評価項目に関する仮説の構築とその考え方

① パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況・対応内容	求めるレベル・範囲
A 社	かなり重視	・セキュリティとコスト削減の折り合いはある程度実現されていたが、要求を満たすことが必要 ・EDR 製品と EDR 運用サービスがパッケージ化されている	・EDR 製品と EDR 運用サービスがパッケージ化されているのは評価できる。パッケージとみた場合の費用は妥当である。 ・同じ事業者でウイルス対策ソフト(既知のマルウェア)と EDR(未知のマルウェア)がパッケージ化され、管理が集約化されれば、更なるコスト削減が期待される。
B 社	ある程度重視	・セキュリティとコスト削減の合理的な折り合いは求められる	・必要となるセキュリティ機能が一体的に提供されて、その分利用料金が上がるということと区別して考えたい。利用料金が上がって、それを許容できないのであれば、必要となるセキュリティ機能が７～８割程度カバーされるように、セキュリティ機能を選べるようになっている方がよい。
C 社	かなり重視	・セキュリティとコストはトレードオフの関係である ・セキュリティとコスト削減の合理的な折り合いは求められる	・必要となるセキュリティ対策製品とサポートサービスがパッケージ化されて、提供されるのはよいが、トータルで年間費用が高額になるのは厳しい。セキュリティエキスパートを確保するサービスでは、これぐらいの費用が掛かるのはよく分かる。AI の活用などを通じて、もう少し費用が安くなるとよい。
D 社	かなり重視	・経営層に、セキュリティの知識や、セキュリティ製品・サービスの知識がないため、基本的には判断を一任されているが、セキュリティとコスト削減の合理的な折り合いは求められる	・今後何をすべきかというコンサルテーションを行ってほしい。自社のリスク評価の結果をもとにセキュリティ対策の中で足りない対策が何か、そのような説明をもう少し行ってほしい。そのようなものがあれば更なる対策検討に弾みがつく。 ・経営者は製品の中身について興味がないので、リスクがどれぐらい存在して、この製品・サービスを導入すれば、どれぐらいリスクを低減できるのか、またセキュリティ対策として、コストが掛かるのをどれぐらい減らせるのか、そこが見えるようになるとよい。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
E 社	かなり重視	・他のセキュリティ製品と違う観点からアプローチしていることを理解しているため、パッケージ化されていなくても仕方ないように思えた	・お試し価格や、他のセキュリティ製品とのパッケージ販売があれば尚良い。 ・本来であればすべての PC、機器端末に本製品のようなセキュリティ対策を実施したいのでボリュームディスカウント等があれば尚良い。
F 社	かなり重視	・費用対効果は求められる	・可能であれば、セキュリティに関してはなにか 1 つインストールすればすべての問題、懸念が解決される形が理想的。 ・上記の形が達成されるのであれば少々高額でも検討の余地がある。

② オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	ある程度重視	・労務管理の一環で PC の利用時間を把握している	・PC 内の作業内容･時間を見ているのであれば、管理コンソールでそのログも見えるようにしてほしい。労務管理面からもログを取得したいので、一体的に運用できるとよい。 ・USB メモリの接続のログを含め使い道があるログについては、もっと開示してほしい。
B 社	あまり重視されない	・システム担当者は置いていない	・社長自らが、システムの全体管理を実施している。現場に対して対応の指示は出すが、基本的には社員各自の個々のスキルで対応してもらっている。 ・システムについては、運用の負荷がかからないものを導入しているが、同じ形で、セキュリティ製品・サービスについても、できる限りセキュリティ性能が高くて、運用の負荷がかからないものを導入せざるを得ない。
C 社	ある程度重視	・セキュリティ運用とシステム運用の両立が求められる	・ISMS の取得にあたり、セキュリティ事故が発生した場合のオペレーションについては、セキュリティ製品・サービスに頼らない運用の手順を規定している。経営層は、ISMS の規定遵守を気にしており、誰が、どのように監視するかを重視している。システム運用と同じ担当者がセキュリティも監視できるようになるのはよい。 ・インシデントが発生した場合には保険に頼ることが必要である。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			・担当者の数自体は減らないが、担当者１名でシステムとセキュリティの両方の運用を見ることができる程度の負荷で済んでいるのはよい。
D 社	あまり重視されない	・セキュリティ運用とシステム運用の両立は求められない ・システム専任者を置いている	・セキュリティ運用とシステム運用はむしろ分けたい。システム専任者には、セキュリティ監査の目を養ってもらいたい。システム運用者は監査を受ける側であり、オペレーションにおいて面倒なことが日々発生するので、ついつい対応を簡略化しがちである。そのため、監査を行う側のセキュリティ運用者は、監査を受ける側のシステム運用者と独立していた方がよい。両立している場合は、どうしてもセキュリティをないがしろにしてしまう。
E 社	ある程度重視	・本製品は該当しない	・セキュリティ製品にシステム運用への関与は期待していない。
F 社	あまり重視されない	・本製品は該当しない	・セキュリティとシステムの全体の運用負荷を軽減するような製品のイメージがわかないため、お答えできない。

③ 製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先（顧客）等の外部にアピールしやすい

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・概念･コンセプトが明快で理解されやすいことがかなり必要 ・将来的に株式の上場を考えている ・外部からの委託研究も実施している	・平常時は外部の専門家にマルウェアを検知してもらえる。また何かインシデントが発生した場合には外部の専門家に駆除してもらえるということを委託元や株主・機関投資家にアピールできるようになることは大きなメリットである。 ・未知のマルウェアの検知実績があれば、そのままアピールできるのでよい。
B 社	かなり重視	・概念･コンセプトが明快で理解されやすいことがかなり必要	・ウイルス対策ソフトでカバーできない残り数%の脅威をカバーする製品であるため、セキュリティ対策を強化する際には、当該製品を選ぶ必要がある。良いものであれば、他の企業と差を付けられ、発注元も見てくれる人は見てくれる。 ・発注元は、パスワードを設定して、機密性の高いデータを暗号化して管理するように言ってくるが、管理自体は甘いので対

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			応していない。ウイルス対策ソフトは他の企業でも導入しており、他の企業と同じレベルであれば、何かインシデントが起きても済まされると考えていた。
C 社	かなり重視	・概念・コンセプトが明快で理解されやすいことがかなり必要 ・IT 業界の中小企業においては、セキュリティ対策が導入されているのが当たり前であり、導入されていないと取引中止になる。 ・常に契約時に誓約書を書かされ、客先に持ち込む端末もチェックされる。	・経営層から目の前に見える部分のセキュリティ対策について説明を求められる。新しく導入する製品・サービスの仕様や機能について気にするが、カタログの中には、技術的な専門用語が多すぎて、なかなか理解されにくい。 ・発注元から ISMS の取得を求められる。ISMS の監査を継続してパスするためには、クラウドサービスセキュリティの導入が必要となっている。 ・クラウドのセキュリティについては、今はまだ発注元はうるさくないが、今後、段々要求が厳しくなることが予想される。あまりコストを掛けたくないが、いずれ対応せざるを得なくなる。但し対応したとしてもアピールには繋がらない。 ・経営者は製品・サービスの中身まで見ない。担当者に一任している。見るのはせいぜい年間予算の範囲内に収まるかどうかであり、収まったとしても、本当に必要であるのかどうかを問われる。 ・クラウドサービスのセキュリティについては、顧客との取引において必要なものは導入せざるを得ないため、今後、プログラムをクラウド経由で納品するような取引がこれまで以上に増えてくるのでリスクが高まるという説明をして、納得してもらった。
D 社	あまり重視されない	・概念・コンセプトが明快で理解されやすいことがかなり必要	・業界全体としてセキュリティ対策の取組みはまだまだこれからである。発注元はセキュリティ対応をほとんど求めてこない。契約先に対しても、セキュリティ対応を求めていない。セキュアメールを使うだけでも契約先から嫌がられる。但し今後は少しずつ変わっていき、セキュリティ対応が求められるようになる可能性がある。 ・このような企業規模で、このような IT を使っている場合に、このような製品･サービスを導入した方がよいと分かりやすく提示してもらえるとよい。チェックシートのような形式で、Yes、No だけで IT の利用状況等を把握できるようになっていると回答する側の負担がなくてよい。

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
E 社	かなり重視	・概念・コンセプトが明快で理解されやすいことがかなり必要	・民間、官公庁の顧客問わず、個人情報の取扱い等は問合せや監査が入るため、セキュリティ製品を導入していることは大きなアピールポイントになる。 ・第三者評価や認定を受けている製品であれば尚良い。
F 社	かなり重視	・概念・コンセプトが明快で理解されやすいことがかなり必要	・顧客から聞かれることはないため、具体的に求める内容やレベルはないが、なにか事故が起きた際にこのような製品を導入していて対策を実施していたと言えることは重要。

(7)製品･サービスのセキュリティ性能の観点からみた評価項目に関する仮説の構築とその考え方

① 対応可能な既存の脅威・インシデントのパターン・範囲が広範である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・広範な脅威に対応してくれるのはよい	・直近のサイバー攻撃など、世の中で騒がれている脅威には、最低限確実に対応してもらいたい。
B 社	ある程度重視	・広範な脅威に対応してくれるのはよい	・市販のウイルス対策ソフトと比べて、これだけの脅威(乗っ取りや踏み台攻撃、ランサムウェア、不正通信、情報漏えい、標的型攻撃)をブロックできるということで十分である。そのうえでオプションには、脅威ハンティングサービスが付いている。満足感が得られれば、オプションも使ってみようかなという気になる。
C 社	あまり重視されない(技術面の対策)、ある程度重視(人為的なミスの対策)	・広範ではないが、脅威のカバー範囲が必要	・技術面の対策はマンネリ化が進んでおり、ある程度の製品・サービスであれば、ある程度広範な脅威に対して、機械的にセキュリティを守る機能が備わっている。これからは人為的ミスをカバーできることが重視され、対応が必要である。人為的ミスにより、個人情報が共有ファイル上にアップロードされるような情報漏えいリスクはカバーされているが、外部サービスを使っている SNS やメール経由の情報漏えいリスクはカバーされていな

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			いので、監視やログ分析を通じてカバーできるようにしたい。 ・自社内におけるクラウドアプリの導入については、必要以上に対象を広げていくことは考えていない。使う人の教育が重要になるため、誰でも使えるようにしていない。教育とセットで考える必要がある。
D 社	製品やサービスによって異なる		・クラウドアプリのカバー範囲は広範なほどよい。 ・ログの分析で脅威やインシデントを検知することになる。保存期間が短いと後から脅威やインシデントを追跡できるようにするためには、専用のログ収集･管理ツールを導入することが必要になる。 ・多様な脅威・インシデントをカバーできるようになると、ポリシー設定が複雑になる。複雑になるのは面倒くさいので避けたい。
E 社	かなり重視	・広範な脅威に対応してくれるのはよい	・ウイルスやトラブルの根幹を抑えて防ぐ製品であるため範囲は広範であると理解している。 ・対応可能な対象は多いほど良い。
F 社	かなり重視	・広範な脅威に対応してくれるのはよい	・1 つの製品で広く全体的にカバーしてもらえるのであればそれに越したことはない。 ・今回の製品が具体的に何から守ってくれているのかは理解していないが、結果として問題が起きないことが重要のためあまり気にしない。

② 未知の脅威・インシデントへの対応が可能である

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・経営層に対しては、ウイルス対策ソフトでは検知されない未知の脅威を検出するためのソフトウェアであるという説明を行っている	・未知であるかどうかを問わず、脅威を検知したときには、その都度連絡が入るようにしてもらいたい。どこから来たかなど状況を知ることができれば、社員への注意喚起ができる。確認のタイミングは、四半期に 1 回のレポートよりも、その都度の方がよい。
B 社	かなり重視	・未知の脅威に対応できることがかなり必要	・ウイルス対策ソフトでは十分カバーできない未知の脅威に対応できるように、当該製品･サービスを導入した。セキュリティの知識は不足しているが、これを機に、脅威･インシデントやセキュリティ製品･

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			サービスについて勉強してみたいと考えている。今後はそういうことを知っておかないといけないと考えるようになってきた。
C 社	かなり重視	・未知の脅威に対応できることがかなり必要	・人為的ミスや内部不正に対応できることが気になる。中小企業で情報漏えいを起こせば、一発アウトである。それが一番怖いところである。 ・クラウドアプリの利用を通じて、ユーザーは気づかずに個人情報や機密情報を漏えいしがちである。人為的ミスが心配である。それをどのように検知するかが求められる。 ・インターネットに繋がっていれば、どこかのクラウドに情報を保存できてしまう。社員が顧客先で情報を不正に窃取し、情報を売るようなことがあってはならない。クラウドアップセキュリティは、このような内部不正に対する１つの抑止力となるのでよい。 ・外部からのサイバー攻撃や、マルウェアの感染による情報漏えいは、技術面の対策で守るしかない。技術面の対策でほぼ情報漏えいを防ぐことができるものと信用している。
D 社	かなり重視	・フィッシングメールのアラートが出たため、社内に周知メールを送ることができた	・PC の挙動を見るものであるため、人為的ミスによって起こる脅威はカバーしたい。
E 社	かなり重視	・未知・既知関係なく動きを感知して、根源から防ぐ製品のため満足している	・対応可能な対象は多いほど良い。
F 社	かなり重視	・今回の製品が具体的に何から守ってくれているのかは理解していないが、結果として問題が起きないことが重要のためあまり気にしない ・未知に関してはあったらいいなとは思うが、難しいことは理解している	・1 つの製品で広く全体的にカバーしてもらえるのであればそれに越したことはない。 ・自社の顧客の名前を使った巧みなウィルスメールもあり現場の人が判断できないため、万が一メールを開いてしまっても守ってくれる機能は非常に安心する。

③ 人為的ミスなどにより、製品そのものが他人（攻撃者）の手に渡るといった、万が一の場合でも悪用が難しい

【ヒアリング調査結果】

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
A 社	かなり重視	・システムを監視する専門家自体の信頼性に懸念を持ってしまう	・システムを監視する専門家が悪意を持てば、PC 内の研究成果等を盗み見ることができてしまうのでは、との懸念を持つ。信頼性はどのように担保されるのか。 ・監視のシステム自体が直接サイバー攻撃を受けて、そこから顧客の情報の漏えいが起きることがないか懸念される。
B 社	ある程度重視	・有用な情報もなく、お金もないので、情報を不正に窃取されても、大きな問題とはならない	・実際に悪用されて、何か被害が発生するとは考えていないが、悪用されてセキュリティベンダーを信用できなくなるのであれば、最初から悪用されない製品･サービスを導入しておきたい。 ・製品・サービスが悪用されて、PC 内に保存している情報やバックアップしている情報を消されるのは絶対に避けたい。
C 社	ある程度重視	・アカウントの乗っ取りを防げるように、必ず２段階認証を掛けるようにしている	・アカウントの乗っ取りなどを想定しにくいため、悪用の余地は少ない。アクセスログが残っているので、後から悪用を把握することもできる。 ・アカウントの乗っ取りがあれば、メールの添付ファイルをごっそりと抜かれるため、サーバ側で添付ファイルが残らないように運用している。データを共有できる機能が付いているクラウドアプリは、アカウントの乗っ取りがあれば、そこからデータが漏えいしてしまう可能性があり、非常に怖い。 ・プログラム資産の漏えいについては、漏れたとしても、どこまで漏えいしたかを見れば、プログラム変更で対応できるので、悪用を防げる。
D 社	ある程度重視	・直接、メール等のデータを引っ張ってくることができない	・フィッシングメールのアラートが出たとき、どのようなメールであるか確認しようとしたら、あて先や件名しか分からず、メール本文を見ることはできなかった。直接、メール等のデータを引っ張ってくることができないという作りは、最初は違和感があったが、悪用について改めて考えると、納得感がある。
E 社	かなり重視	・人為的なミス・故意に対するセキュリティ対策も実施しなくてはいけないという意識があるが、具体的に対策は実施できていない	・顧客とのメールのやり取りで添付をする際には特定のファイル転送サービス等を用いることが顧客からの指示で必須になっている。 ・PC のうち持ち運び可能なノート PC も顧客からワイヤーロックされている。 ・全体的に顧客からのセキュリティ監査に従っているが、個々のメールなどの対応

	重視度合い	本検証における状況･対応内容	求めるレベル・範囲
			が自動で暗号化されることが可能になれば手間が省けて良いと思う。
F 社	ある程度重視	・人為的ミスによる問題はセキュリティ製品でカバーできるものは限られていると認識している	・故意・事故に関わらず人員的な要因によるインシデントもカバーしてもらえたらありがたいと思う。 ・現状、すべての PC はインターネット接続されており、USB メモリも利用可能なため悪意がある人が操作したら情報を外に出すことは可能であろう。 ・一方で担当者が情報にアクセスしづらくなる等の手間が発生すると、業務に支障が出るため懸念。 ・具体的にどのような機能があればいいかはわからないが、人為的にもネットワーク的にも外部への流出リスクを最小限に抑えることができれば理想的である。

3.1.2. 採択事業者等に対するヒアリング調査結果

採択事業者及び中小企業ユーザーに対面し採択事業者が提供する中小企業向けサイバーセキュリティ製品・サービスを直接販売している販売代理店（そのような販売代理店が存在する場合のみ）に対するヒアリング調査を行い、評価項目の調査仮説についての有効性を検証するとともに、評価項目の調査仮説に必要となる追加や修正について把握した。

採択事業者等に対するヒアリング調査結果を以下に示す。

（1）導入のし易さの観点からみたヒアリング調査結果

① 大規模なシステム改修を伴わず、実装が容易である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・システム改修は不要。	・システム改修という概念が存在しない。大手企業向けに提供しているマネージドセキュリティサービスでは、設定変更などのシステム改修が必要になる。一方、中小企業向けのセキュリティサポートデスクについては、中小企業の担当者によるシステム改修によって接続できなくなることを避けたいという思いから、自社でバックエンドにおいて設定代行を行うというサービス形態を採用している。	・既存のアプリケーションを使い続けるために、証明書を発行する程度で、システム改修は不要。 ・システム改修を必要しないセキュリティ製品を元々目指していた。”Set & forget”（入れたら入れっぱなしで忘れてしまうほど簡単で負担がない）というコンセプトを掲げている。 ・*中小企業を主要顧客層として抱えていることから、システム改修等の人員的な手間がかかる製品は受け入れてもらいにくく、あまり扱わないようにしている。*

② 現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ある程度の従業員規模の中小企業の場合、ログを管理・閲覧したいという声が聞こえるが、管理コンソールを構築したとしても、結局、忙しくて時間がなく、知識も十分ではないため、ログの管理・閲覧は最初だけになってしまうのではないかと判断している。ログを閲覧するよりも、知らない間に分析や対処が終わっている方がユーザーにとって有益と考えている。 ・将来的には管理コンソールを構築し、四半期に１回に発行しているレポートもそこで閲覧できるようにしたいと考えているが、そのような状況から現在は対応の優先順位が低い。 ・お試し利用は１ヶ月間である。その間の脅威や対応の状況についてレポーティングを行っている。また、レポートのレビューの仕方について説明するガイドも作っている。 ・*レポートで脅威を煽るだけでなく、具体的な脅威に対して、きちんと守られているということを、中小企業ユーザーにもっときちんと説明すべきと考えている。*	・お試し利用については、今年１月から、管理ポータルでの情報収集や、相談のトライアルが無料でできるようになる。 ・インシデント対応については、中小企業ユーザー側で訓練ができるように動画を作成している。 ・これらの取組みの方向性が、中小企業ユーザー側から出た意見と一致するので安心した。	・そもそもの製品コンセプト策定の段階からシンプルなものを目指していた。 ・レジストリ改ざん、system space 書き込み、他アプリメモリ読み書きの、不正行為を発症させる原因の根源となり得るすべてを止めているので、それ以上の機能は利便性を下げると考え、あえて取り入れていない。 ・シンプルな機能だが、インシデントの原因となりうる①マルウェア、②人為的、③DDoS のうち、マルウェアに関してはアップガードのみで対応可能な機能を備えている。 ・*中小企業には機能や目的が単一など、複雑でない製品の方が受け入れてもらいやすいと考え、アップガードは中小企業のそういった要望に沿っている製品だと考える。*

ヒアリング調査を実施する中で、中小企業ユーザーにおいては、PC に必要となる機能をインストールした後に PC の動作が重くなることを敬遠することが分かったため、PC のシステムパフォーマンス等への影響が小さいという評価項目を追加し、参考扱いでヒアリング調査を実施した。以下にヒアリング調査結果を示す。

○追加した評価項目（参考）：PC のシステムパフォーマンス等への影響が小さい

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・導入の最初の段階は、PC の状況や環境を把握するために必要となる情報を収集するため、取得する情報が多くなり、PC のシステムパフォーマンスが低下するが、その後は徐々に負荷が減っていくので、最初だけの事象である。	・サービス導入後に顧客から寄せられる問合せの中で一番多いのが、PC のシステムパフォーマンスへの影響であるため、重要視し、対応にも力を入れている。 ・マイセキュアビジネスについては、第三者機関からシステムパフォーマンスへの負荷が非常に小さいソフトウェアとして認証を受けており、他社の製品と比較して、圧倒的な性能である。 ・クラウドアップセキュリティについては、メールについてもファイル共有についても、API を利用して、バックエンドで処理するというサービス形態になっており、システムパフォーマンスへの負荷が小さくなるよう設計されている。	・PC の動作を重くさせる要因となる動きをほとんどしない製品であるため、PC のシステムパフォーマンスへの影響はほとんどないはずである。 ・重くなる原因は①スキャン、②動的に動いている挙動の確認の２つであるが、アップガードはスキャンを実施していない。不正な動きは見ているが、動いた瞬間しか監視していないので、重くはならない。 ・*アップガードは PC システムパフォーマンスの影響はほとんどないと認識している。*

③ いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・設定が全く必要ないことはよい。更にサイレントインストールについても検討しているところである。中小企業ユーザーにおいては、設定途中で逆に問題が発生すれば、対応できなくなる。	・今後は顧客の要望を満たせるように、サンプル設定の選択肢の数を増やし、充実を図っていく予定である。アプリケーションの改修とは異なり、設定の改修は比較的容易であるため、バージョンアップを図っていきたい。クラウドアップセキュリティは毎月１回バージョンアップしているので、その中に、サンプル設定の充実に関する要望についても入れていく。	・中小企業向けのアップガードソロは導入時の場合の設定が不要なように構築している。 ・アップガードソロの場合は、少人数・小規模を対象としている製品であるため、事前に想定した機能の、想定設定をされたものを提供しているため、ユーザー側の設定は求められない。 ・*設定が必要だとすれば、他アプリなどの証明書を発行し、アップガードに添付するだけである。この操作についてはマニュアルでわかりやすい説明を提供しており、中小企業ユーザーからもわかりやすいとの評価をもらった。*

(2)運用のし易さの観点からみた評価項目に関する仮説の構築とその考え方

① 社内に専門的な人材がいなくても、メンテナンスが可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・最新のソフトウェアを１時間ごとに探して、最新のソフトウェアがあれば、自動更新を行っている。 ・何かトラブルが発生すれば、状況を確認して、すぐにソフトウェアを改修するという対応を採っている。ソフトウェアの改修情報については、現在公開していないが、今後どういう形で公開すべきであるかについて検討している。 ・EDR の運用代行を、サービスとして実施しているところが、中小企業ユーザーに対して一番響いている。運用を任せるが、レポートで状況確認ができるようになっていることが高く評価されている。	・中小企業においても、従業員の人数が増えると、中継サーバを社内に立てて、中継サーバ経由で、修正プログラムを配布するという形態を選択しがちであるが、その管理が負担になって、中継サーバ自体が十分にメンテナンスされておらず、修正プログラムのダウンロードができなくなってしまい、その結果、感染するというケースが散見される。そのような事態を避けるために、フルクラウドでサービスを提供している。	・メンテナンスという概念がないが、ユーザー側での操作が必要だとすれば、新しく他アプリインストールするときに、アップガード上でそのインストールを許可するかどうかのみである。 ・アップガード自体のアップデートは１年に２回くらいあるが、自動更新で実施されており、ユーザー側の操作は必要ない。 ・*アップガードについては、手動でのアップデートはない、実施する必要がないとの説明を受けている。*

② 万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である

万が一インシデントが起きた場合の対応の省力化に関するヒアリング調査結果と、勤務時間外の対応の省力化に関するヒアリング調査結果を２つに分けて以下に示す。

②－１　万が一インシデントが起きた場合の対応の省力化が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・*お試し利用において、地震時の避難訓練のように、インシデントの発生を体感できる場があるとよい。インシデントのアラート通知については、どのよう*	・インシデントが発生した場合、中小企業ユーザー側から電話による問合せがあれば、オペレーターが PC の影響範囲を調査することになる。	・インシデントが起きるというのは、アップガードの対象であるマルウェアの範囲では、マルウェアが入ってきたとしても不正行為を発症させない製品である

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
な情報が届くか、また対応については、どこの窓口に何を相談すればよいか、さらに報告については、どの機関にどのように報告すればよいかといったテンプレートが用意されていれば、インシデントの発生を体感することができるようになるとよい。 ・問合せ先の電話番号は、カタログやパンフレットには記載していないが、脅威を検知したときのアラート通知メールの本文中に記載している。問合せは基本的にメールで行う形になっている。 ・中小企業ユーザーからの問合せ・相談の一次受けは、ディストリビュータに対応してもらっており、その内容をエスカレーションしてもらっている。	・初動対応を間違うのが一番問題であるため、さまざまな状況に応じて、手はずを整えることができるように適切なアドバイスを行い、早期の信頼回復に繋げられるようにしている。問合せが殺到すれば、コールセンターを立ち上げなければならない。また、原因が分からないのであれば、フォレンジック調査により原因究明しなければならない。インシデント発生時の多岐にわたる状況に対してケースバイケースで対応できるようにしなければならない。	ため考えられない。 ・人為的なインシデントと、DDoS によるインシデントは製品の範囲外なのでカバーできない。

②－２　勤務時間外の対応の省力化が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・脅威のモニタリング時間は、平日の 9～17 時であり、勤務時間外の対応は行っていない。17 時以降に蓄積されているログは、翌日の朝一番に解析する運用になっており、そこで何か脅威が検出されればアラート通知を行っている。	・問合せ・相談対応の受付時間は、平日の 9～18 時である。中小企業向けのサービスとして、利用料金を低く抑えることができている大きな理由として、24 時間 365 日で問合せ・相談対応を受け付けていないことが挙げられる。もし 24 時間 365 日で問合せ・相談対応が必要になるのであれば、そのような対応を受け付けている大手企業向けのサービスの窓口を別料金で提供せざるを得ない。	・アップガードソロの製品については、中小企業が電話の対応等丁寧な対応を求めていることが多いため、委託先だが問合せ窓口を設けており、平日の 9～18 時に受け付けている。 ・アップガードエンタープライズにおけるお問合せは直販を実施していないため、原則ディストリビュータに問合せ窓口の役割を任せている。 ・*アップデートに関するお問合せは、Blue Planet Works ではなく、ディストリビュータで受けることとなっている。*

③ 問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ *中小企業ユーザーの場合、電話による問合せ・相談のニーズが高い。* ・ 中小企業ユーザーの場合、１社１社電話で対応するのは難しい。今後、FAQ やマニュアルづくりを進めていき、納品の際にそれらを渡して説明できるような形にもっていきたい。	・ 中小企業ユーザーからの問合せのオーダー処理を行う窓口と、問合せ・相談へのアドバイスを行う窓口が異なっている。このように窓口が２つに分かれていることは、開通案内書に記載されているが、中小企業ユーザー側では、認識されていないことが多い。 ・ 後者の窓口に対し、直接電話で問合せ・相談のあった中小企業ユーザーに対しては、セキュリティエキスパートが迅速に状況を確認して、電話でフォローする仕組みになっており、速やかなインシデントレスポンスが可能である。 ・ 他方、ポータルへの問合せ・相談については、SLA 上、１営業日以内にフォローする仕組みになっている。	・ 問合せ窓口はホームページ上で公開している。 ・ ただし、窓口への問合せの数自体が少なく、問合せがあったとしても、証明書の発行に関するものがほとんどで、委託先に提示している想定 Q&A で対応できない問合せはまだ受けていない。

(3)導入や運用を行うことで得られる効果の観点からみた評価項目に関する仮説の構築とその考え方

① 導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ *中小企業ユーザーの場合には、ウイルス対策ソフトと UTM のこの２つさえあれば、ある程度セキュリティを守ることができる。あれこれとセキュリティ機能・製品を追加することは必要*	・ 中小企業の場合は、導入後に機能追加やそれに伴う費用負担を求めると、解約に繋がりやすい。継続して使ってもらいたいため、導入後の機能追加を必要としないオールインワンによる提供形態	・ 追加機能は、アップガードソロもアップガードエンタープライズも提供していない。 ・ 追加機能なしで、マルウェア原因の不正行為を発症させないという目的を実現している。

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
がない。 ・ *脅威ハンティングの費用が保険の支払い対象になっており、保険で賄うことができる。脅威が発生した際には、保険会社との取り決めで、脅威が発生したという事実確認を行うことが必要であるため、IPA 等にその旨の報告を行ってもらわないといけない。* ・ 但し、現在、保険会社との連携を広げており、保険会社によってはIPA等への報告が不要になるところもある。受給条件は保険会社によって異なっている。	が必要となる。	

② サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ *中小企業の経営者は、セキュリティに関して敏感になってきているが、まだまだ何かインシデントが発生したら大変なことになるという認識のレベルであり啓発が必要である。* ・ *中小企業の経営者は、世の中で騒がれている脅威に対して、対策ができていれば安心する。その時になって始めて、この製品・サービスでこのようなことができるということに気づく。分からないけれど、守られているということが大切である。* ・ *最近は、EMOTET に対し、対応できているか聞かれる機会が多い。* ・ IT の知識が十分ではない担当者にも分かってもらえるように、レポートについては、使う用語の専門的なレベルを下げ	・ リテラシーが低い担当者にも、リテラシーを高めたいと考える担当者にも対応できるようになってもらうことが重要である。インシデント対応の訓練用の動画など、意識啓発や人材育成のための資料の提供や、オフ会の開催に今後、力を入れていきたい。	・ 証明書の貼り付け以外はユーザーが操作する必要はないため新しい知識は必要ない。 ・ ユーザー側で実施すべき設定や、定期的なアップデートがないので、知識は不要だが、製品のアプローチが今までにないものであるため、製品の概念を理解してもらえれば問題ないと考える。 ・ *中小企業は人員的な余裕もないため、機能や仕組みを完ぺきに理解していなくとも、結果としてセキュリティが守られていれば問題ないはずである。*

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
ることを意識して改善を行っている。		

(4)導入時や運用時に要する費用の観点からみた評価項目に関する仮説の構築とその考え方

① 導入コストが安価である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・イニシャルコストとしては、クラウド環境の確保や管理者登録などの事務について、初期事務手数料が発生する。 ・ログを活用したいという声が出ているが、ログを送信するために社内にサーバを立てることになれば、高額な費用が必要になる。イニシャルコストが掛からないサービス提供形態の方が、中小企業ユーザーには受け入れられやすい。	・大手企業向けに提供しているSOC・マネージドセキュリティサービスの場合は、接続設定に係る費用をイニシャルコストとして請求している。 ・クラウドの進展により、セキュリティサービスは ASP サービスとしての提供形態に移行してきている。SOC・マネージドセキュリティサービスについても、そのような流れの中で、業界全体が ASP サービスに向かっている。 ・セキュリティサポートデスクの接続設定は、中小企業において対応が難しいと考えられるため、自社で代行し、その費用についてもイニシャルコストとして請求しておらず、チャレンジ領域であると考えている。	・1 台あたり 1 年で 9,800 円だが、導入前に挙動などを確認してもらう無料のお試し期間を必要に応じて提供している。 ・ディストリビュータが導入台数によっては、導入支援コストをとっているかもしれない。 ・アップガードソロは台数に応じて価格が安くなることはなく、何台でも一律価格。エンタープライズは台数に応じて価格割引がある。 ・*アップガード製品は導入前に金額を提示すると、中小企業からは高いと思われがち。しかしながら導入後は効果に満足して、継続利用しもらいやすい。* ・*導入に関して支援を実施したとしても現在お金は取っていない。*

② 運用コストが安価である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ *中小企業の場合、セキュリティ対策に対しては、二の足を踏むことが多いため、費用が低廉なことが重要である。* ・ 極論にはなるが、ソフトウェアは無料で、インシデントの駆除やレポートの発行・提供などのエージェントの部分について課金するといった方向のビジネスモデルについても将来的に検討していきたい。脅威モニタリング等を自動化し、その費用をエージェントに反映できるようにしたい。	・ 設定価格にご意見をいただく機会もあるが、この利用料金で、サイバー保険の保険料も含まれていて、このサービス内容であることについて、理解をいただきたい。	・ アップガードソロに関しては、1 台あたり 1 年で 9,800 円が導入コスト兼運用コストとなっている。 ・ １製品当たりの金額で考えると少々高額かもしれないが、トータルでセキュリティを守るお金として、経営目線で考えると安いはずである。 ・ マルウェアについてアップガードで完ぺきに守る金額と、いくつかの製品を組み合わせて完ぺきに守ろうとしたときの金額感の差はパンフレットに掲載している。加えて、製品複数入れた際の人件費を考えるさらに安く感じてもらえるであろう。

(5)導入や運用における課題の解決の観点からみた評価項目に関する仮説の構築とその考え方

① 製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠（利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等）に基づく、適切な説明がなされている

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・ 中小企業ユーザーからどれだけ検知能力があるか製品性能について聞かれることはある。また、中小企業ユーザーの方からウイルス対策ソフトとの比較を質問されることがある。	・ 民間調査会社のネットワークセキュリティの市場調査レポートで、ここ３年間、SOC・マネージドセキュリティサービスのシェアが No.1 であるが、特にアピールを行っていない。 ・ 製品・サービスの性能・スペックを、顧客に信用・信頼してもらうためには、導入実績や、インシデ	・ 大手企業への導入の際には、PoC でマルウェア（既知とその場でホワイトハッカーが作成した未知の双方）をあてて全てはじき、問題が起きないことを証明している。

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
	ント対応事例の紹介が最低限必要になってくる。	

(6)製品・サービスの経営へのインパクトの観点からみた評価項目に関する仮説の構築とその考え方

① パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・基本的には、ログを見て、解析をかけるという製品・サービスになるため、解析によって見ているものが異なる製品・サービスであれば、そのような製品・サービスとの連携も将来的に実現可能である。	・中小企業においても、サイバーセキュリティ経営ガイドライン Ver 2.0 の最低限実施すべき事項となっている、ウイルス対策ソフト、SOC・マネージドセキュリティサービス、UTM、クラウドのセキュリティといった取組みが必要になると判断し、一体的にサービスを提供できるようにしている。 ・顧客から預かっているログの適切な保全サービスと、意識啓発や人材育成のための教育サービスに取り組むことを、全社共通の方針として定め、具体化に向けた検討を行っている。	・製品の機能が過不足なく、マルウェアを原因とする不正行為を発症させないものとなっているため、パッケージ化は実施していない。 ・大企業・多数向けのアップガードエンタープライズは台数に応じて、1 台あたりの金額を下げることはある。

② オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社

・*管理コンソールを作れば、対応できるようになる可能性がある。但し、システム運用側の情報を集約して送信するためのサーバを社内に立てる必要がある。* ・資産管理など、ログの使い方次第で、セキュリティとシステムの共同運用に繋がるサービス領域があるかもしれないが、今のところはそこまでサービスを広げていくことは考えていない。	・大手企業向けに、情報システム部門の機能を代行するサービスを提供しているが、中小企業においては、費用的な制約があり、そのような要望が寄せられていない。	・セキュリティ以外のシステムやオペレーションは、製品の範囲に含めていない。 ・資産管理システム等とは併用して利用することは可能であるため、マルウェア対策以外の製品とは併用しての利用を推奨する。 ・*中小企業は、セキュリティ製品はセキュリティのみを対象とし、システム製品はシステムのみを対象としているため、別々で考えていることが多く、また包含した製品は高額になりがちなので、第一印象のハードルが高く、受け入れられないのではないかと考えている。*

③ 製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先（顧客）等の外部にアピールしやすい

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・*未知の脅威への対応実績があるのであれば、それを謳うべきである。* ・サプライチェーン上の Tier1 や Tier2 であれば、対策の取組状況のアピールが求められるが、Tier3 以下に対して、取引先にアピールできるため、投資を行ってセキュリティ製品・サービスを導入した方がよいと言ってもなかなか響かない。	・マイセキュアビジネスやセキュリティサポートデスク、クラウドアップセキュリティについては、サイバーセキュリティ経営ガイドライン Ver 2.0 の最低限実施すべき事項に位置づけられている取組みであるため、実施しなければならないという説明を行っている。	・NISC のガイドラインの中に、マルウェアをはじくのではなく、マルウェアが不正行為を発症させないようなアプローチを推奨するというような文言が記載されているため、その文言を引用して説明を行っている。 ・中小企業に対しては、中小企業のみに閉じた話だけではなく、サプライチェーンマネジメントの一環としてセキュリティ対策は重要になると考えるため、サプライチェーン全体にフォーカスを当てた安全を説明する資料を今後作成する予定である。

(7)製品・サービスのセキュリティ性能の観点からみた評価項目に関する仮説の構築とその考え方

① 対応可能な既存の脅威・インシデントのパターン・範囲が広範である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・安全性の低い公共 WiFi に接続している、USB メモリの抜き差しが多い、ハードディスクのエラーログが多いなど、脅威予兆や故障予兆につながるリスクレベルの情報についても、レポートの中で提供しており、広範な範囲をカバーしている。 ・*対応可能な脅威のカバーが広範囲であることよりも、中小企業ユーザーに誤解を与えないように、この脅威に対しては、このようなレベルで対応できるということを明確化しておくことが重要である。そうした方が中小企業ユーザーにおいても製品・サービスを選びやすくなる。またそれが分からないまま契約を行い後々トラブルになることも避けられ、セキュリティベンダー側やディストリビュータ側にとってもそのようなトラブル対応が不要になるのでよい。*	・多層防御でセキュリティを守るという基本的な考え方に立っている。 ・サイバーセキュリティ経営ガイドライン Ver 2.0 においても、未知の脅威に対応できることが求められており、複数の種類の異なる脅威検知アルゴリズムを安価に、かつ安心して安全に導入できるようにしている。 ・NTT の研究所や他社が保有するさまざまな種類の脅威情報を、アンテナを広げて入手し、広範な脅威にカバーできるようにしている。 ・人為的なミスにより発生したインシデントについても、サイバー保険の支払いで各種費用を賄うことができるようにしている。	・マルウェアに関しては、マルウェアの種類、既知・未知に関わらず、不正利用を発症させないので範囲が広範であるといえる。 ・*製品の仕組み上、マルウェアが侵入しても問題が起きないという製品であるため、範囲は広範であると認識している。*

② 未知の脅威・インシデントへの対応が可能である

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・現在の技術・仕組みで十分未知の脅威の検出ができている。	・未知の脅威に対応できるようにするため、既に振る舞い検知やサンドボックスといった技術を取り入れている。	・未知のマルウェアにも対応可能である。

③ 人為的ミスなどにより、製品そのものが他人（攻撃者）の手に渡るといった、万が一の場合でも悪用が難しい

【ヒアリング調査結果】注）斜字体は販売代理店の意見、それ以外は採択事業者の意見

eGIS 株式会社 【販売代理店】 東京システムリサーチ株式会社 株式会社ラック	NTT コミュニケーションズ株式会社 【販売代理店】 なし	株式会社 Blue Planet-works 【販売代理店】 大興電子通信株式会社
・収集しているログは、PC の動作だけであり、ファイル名ぐらいは見ることはできるが、ファイル自体をアップしておらず、ファイルの中身まで見ることもできない。また、HTTP 通信において収集されたデータは、運用規約に基づいてログを扱っている。 ・従事するホワイトハッカーに対しては定期的に教育を実施している。また、ログを見る際にも、1 人で見ているのではなく、複数人で同じログを見るという形の運用を行っている。	・不正に窃取した ID･パスワードの活用による他人へのなりすましが大きな問題になっているため、セキュリティ業界全体が、2 段階認証などの必要となる対策に本格的に注力している。	・アップガードで活用されている技術は 20 年前にできた技術であり、常にリバースエンジニアリングを受け、悪用されようとしているが、悪用が実現したことはない。 ・アップガードは不正検知をすり抜けて、かつ実際に不正を発症させなくてはいけないため、悪用は困難と考えている。

3.1.3. 評価項目の有効性検証結果

前述した「3.1.1.　中小企業ユーザーに対するヒアリング調査結果」や「3.1.2.　採択事業者等に対するヒアリング調査結果」を踏まえると、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の調査仮説については、概ね有効であり、大枠を変える必要がなく、適用可能であるという結果が得られた。

中小企業ユーザーにおける各評価項目の重視度合いや、各評価項目の有効性に対する考察、新たに評価項目に盛り込むべき内容について、以下に整理する。

(1)導入のし易さの観点からみた評価項目の有効性検証結果

① 大規模なシステム改修を伴わず、実装が容易である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、２事業者が「かなり重視される」、４事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ) 評価項目の有効性に対する考察

新たな脅威の呼び込みや、基幹システムへの影響、追加投資や決裁・社内調整に係る負担増、改修自体の手間を敬遠し、システム改修は避けたいと考えている。また、システム改修だけでなく、システム停止やそれに伴う業務停止を伴うことも避けたいと考えている。

② 現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、１事業者が「かなり重視される」、５事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ) 評価項目の有効性に対する考察

導入時点において、機能が足りているか、足りていないかを判断することは困難であるため、お試し利用の期間を長く取れるなど、お試し利用をより一層充実してほしいと考えている。

また、自社においてセキュリティ設計を行ったり、必要となる機能・製品を選んだ

りすることは困難であるため、自社における利用状況・利用環境に照らし合わせて、自社にとって必要となる製品・機能を決めてもらいたいと考えている。

更に、必要となる機能を実装した場合でも、PC のシステムパフォーマンスが低下することは避けたいと考えている。

③ いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、1 事業者が「かなり重視される」、4 事業者が「ある程度重視される」、１事業者が「あまり重視されない」という評価結果となり、概ね有効であった。「あまり重視されない」と回答した事業者は、システム担当者の専任者を確保している事業者であり、自社での対応が可能であった。

(イ) 評価項目の有効性に対する考察

マニュアルどおりに進めるだけで、時間をかけずに簡単にインストール・設定ができるようにしてほしいと考えている。また、設定でつまずくという事態が発生する可能性があるため、設定が完了するまで、伴走してサポートしてもらいたいと考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「お試し利用の充実」や「PC のシステムパフォーマンス低下の回避」、「伴走型による手厚いサポート対応」といった内容が考えられる。

(2)運用のし易さの観点からみた評価項目の有効性検証結果

① 社内に専門的な人材がいなくても、メンテナンスが可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、2 事業者が「かなり重視される」、4 事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ) 評価項目の有効性に対する考察

セキュリティ製品・サービスの運用・メンテナンスのために、社内にセキュリティ分野の専門的な人材を確保することは困難であるため、セキュリティベンダー側の人材リソースを活用して、運用・メンテナンスをできるようにしてもらいたいと考えて

いる。また、担当者は兼務でセキュリティも管理しているため、運用・メンテナンスに係る管理負担が担当者の手を離れることはよいと考えている。

② 万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である

万が一インシデントが起きた場合の対応の省力化に関する有効性検証結果と、勤務時間外の対応の省力化に関する有効性検証結果を２つに分けて以下に示す。

②－１　万が一インシデントが起きた場合の対応の省力化が可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、６事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ) 評価項目の有効性に対する考察

インシデントが起きた場合に、セキュリティベンダー側がさまざまな状況に応じて適切なアドバイスを行うことにより、自社側で積極的なアクションを起こす必要がないことや、必要となる対応・アクションの道筋を示してもらえることはよいと考えている。

②－２　勤務時間外の対応の省力化が可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、５事業者が「あまり重視されない」、１事業者が「全く重視されない」という評価結果となった。評価項目の有効性については、必ずしも十分とは言えないが、セキュリティベンダー側の問合せ・相談窓口が 24 時間 365 日で対応しておらず、自社で対応のしようがないため、そのような評価結果になったと考えられる。

(イ) 評価項目の有効性に対する考察

インシデントや障害の発生により業務やシステムを絶対に停止できないような状況下に置かれている事業者においては、勤務時間外の対応が必要になることから、勤務時間外の対応の省力化が必要であると考えている。但し、そのような状況下に置かれていない事業者においては、そもそも勤務時間外の対応は避けたいと考えている。

③ 問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である

(ア)重視度合い

中小企業ユーザー６事業者のうち、２事業者が「かなり重視される」、４事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ)評価項目の有効性に対する考察

トラブルやインシデントが発生した場合の問合せ・相談への対応レスポンスは確実で、速いに越したことはないと考えている。また、セキュリティベンダーのホームページ上にトラブルシューティングや FAQ が掲載されていて、自社でもある程度それを見て対応できるようになっていてほしいと考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「さまざまな状況に応じた適切なアドバイス」や「トラブルシューティングや FAQ などのサポートの充実」といった内容が考えられる。

(3)導入や運用を行うことで得られる効果の観点からみた評価項目の有効性検証結果

① 導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることが可能である

(ア)重視度合い

中小企業ユーザー６事業者のうち、５事業者が「かなり重視される」、１事業者が「あまり重視されない」という評価結果となり、かなり有効であった。「あまり重視されない」と回答した事業者は、自信を持って中小企業ユーザーに使ってもらいたい製品・サービスであれば、セキュリティベンダー側は最初から必要となる機能を組み込んでいるとの考え方によるものであった。

(イ)評価項目の有効性に対する考察

PC の安定的な稼動を損なう可能性や追加費用の発生可能性を敬遠し、導入後に求められる機能追加は避けたいと考えている。また、導入後の機能追加を必要としないオ

ールインワンによる提供形態(定額で必要となる機能を提供する形態)にしてほしいと考えている。

② サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である

(ア)重視度合い

中小企業ユーザー６事業者のうち、1事業者が「かなり重視される」、4事業者が「ある程度重視される」、1事業者が「あまり重視されない」という評価結果となり、概ね有効であった。「あまり重視されない」と回答した事業者は、システム担当者の専任者を確保している事業者であり、サイバーセキュリティに関する知識を蓄積していくことは自社にとってプラスであると考える事業者であった。

(イ)評価項目の有効性に対する考察

サイバーセキュリティに関する専門技術的な知識よりも、製品・サービスを適切に使えるように、また何かトラブルが発生したときにある程度自社で対応できるように、製品・サービスに関する知識を身につけたいと考えている。また、コストを掛けてまで、サイバーセキュリティに関する専門技術的な知識や製品・サービスに関する知識を学習しないといけないような製品・サービスは敬遠したいと考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「PC の安定的な稼働への影響回避」や「製品・サービスに関する知識の習得」といった内容が考えられる。

(4)導入時や運用時に要する費用の観点からみた評価項目の有効性検証結果

① 導入コストが安価である

(ア)重視度合い

中小企業ユーザー６事業者のうち、６事業者が「かなり重視される」という評価結果となり、かなり有効であった。

(イ)評価項目の有効性に対する考察

導入コストが高いと、そもそも検討の俎上に載らないと考えている。また、イニシャルコストとして支払う場合には、PC のインストール台数に制限がない、製品のライフサイクルが長く償却期間を長く取れるなど、何らかの費用面のメリットの享受が必要であると考えている。

② 運用コストが安価である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、５事業者が「かなり重視される」、１事業者が「ある程度重視される」という評価結果となり、かなり有効であった。

(イ) 評価項目の有効性に対する考察

ランニングコストとして支払う場合には、万が一個人情報が漏えいした場合の損失額や、セキュリティ運用のトータル費用との見合いで支払額に納得感があるのがよいと考えている。また、インシデント対応に係る費用を、サービスに含まれているサイバー保険でカバーできるのは安心感があると考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「インストール台数の無制限や製品ライフサイクルの長期化に伴う償却期間の伸長等の費用面のメリットの享受」や「想定される損失額やセキュリティ運用のトータル費用等の必要費用との見合い」、「サイバー保険によるインシデント対応に係る費用の補完」といった内容が考えられる。

(5)導入や運用における課題の解決の観点からみた評価項目の有効性検証結果

① 製品・サービスの性能・スペックについて、誰もが納得のできる客観的な根拠（利用実績、ガイドライン・技術標準への準拠、技術特許、第三者評価等）に基づく、適切な説明がなされている

(ア) 重視度合い

中小企業ユーザー６事業者のうち、５事業者が「かなり重視される」、１事業者が「ある程度重視される」という評価結果となり、かなり有効であった。

(イ) 評価項目の有効性に対する考察

製品・サービスの性能・スペックに関する客観的な根拠として、企業への導入実績や、脅威の検知・駆除実績、市場シェア、運用チーム編成、運用担当者のスキル・経験などの参考情報をパンフレットやカタログ等に掲載してほしいと考えている。また、多くの企業やPCに導入されている製品・サービスであれば、運用ノウハウが蓄積されていくので、セキュリティ性能の面で安心である、またコストも下がっていく可能性があるので費用の面でも安心であると考えている。

製品・サービスの性能・スペックに関する客観的な根拠が提示されることも必要であるが、経営者は、製品・サービスの中身について興味がないので、自社内にリスクがどれぐらい存在して、製品・サービスを導入すれば、どの程度リスクを低減できるのかが見えるようなリスク評価やコンサルティングが、セットになっているとよいと考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「企業への導入実績や、脅威の検知・駆除実績、市場シェア、運用チーム編成、運用担当者のスキル・経験などの参考情報の提供」や「リスク評価やコンサルティングによるサポート」といった内容が考えられる。

(6)製品・サービスの経営へのインパクトの観点からみた評価項目の有効性検証結果

① パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である

(ア) 重視度合い

中小企業ユーザー6事業者のうち、5事業者が「かなり重視される」、1事業者が「ある程度重視される」という評価結果となり、かなり有効であった。

(イ) 評価項目の有効性に対する考察

セキュリティ製品とその運用サービスのパッケージ化や、必要となるセキュリティ製品・サービスのパッケージ化、世の中で普及している大手セキュリティベンダーの製品・サービスの相乗りでのパッケージ化は、費用が折り合えば魅力的であると考えている。

② オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、３事業者が「ある程度重視される」、３事業者が「あまり重視されない」という評価結果となり、概ね有効であった。「あまり重視されない」と回答した事業者の中には、システム担当者の専任者を確保している事業者や、そもそもシステム担当者もセキュリティ担当者も置いておらず、経営者自らがシステム全体・セキュリティ全体の管理を行っているため、運用の負荷がかからない製品・サービスを導入せざるを得ない状況であり、運用負荷の問題が前提にならない事業者が含まれていた。

(イ) 評価項目の有効性に対する考察

担当者１名でシステムとセキュリティの両方の運用を見ることができる程度の負荷で済むような製品・サービスがよいと考えている。

③ 製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先（顧客）等の外部にアピールしやすい

(ア) 重視度合い

中小企業ユーザー６事業者のうち、５事業者が「かなり重視される」、１事業者が「あまり重視されない」という評価結果となり、かなり有効であった。「あまり重視されない」と回答した事業者は、製品・サービスの概念・コンセプトが明快で理解しやすいよりも、自社の企業規模や IT の利用状況・利用環境を見て、必要となる製品・機能を分かりやすく提示してもらった方がよいとの考え方によるものであった。

(イ) 評価項目の有効性に対する考察

経営層への製品・サービスの説明にあたって、製品・サービスの概念・コンセプトが明快で理解されやすいことが必要であると考えている。また、経営層は顧客との取引において必要なものは導入せざるを得ないと考えている。

更に、個人情報保護対策を求める取引先等に対して製品・サービス導入をアピール

できるようになることはメリットであると考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、既存の評価項目である程度カバーされており、新たに評価項目に盛り込むべき内容は特にないと考えられる。

(7)製品・サービスのセキュリティ性能の観点からみた評価項目の有効性検証結果

① 対応可能な既存の脅威・インシデントのパターン・範囲が広範である

(ア)重視度合い

中小企業ユーザー６事業者のうち、３事業者が「かなり重視される」、１事業者が「ある程度重視される」という評価結果となり、かなり有効であった。

他方、残りの２事業者のうち、１事業者においては、サイバーセキュリティ製品・サービスの技術面の機能は成熟化しており、既にある程度対応可能な脅威・インシデントの範囲が広範にカバーされているため、「あまり重視されない」という評価結果となった。但し、脅威・インシデントのうち、人為的なミスによる脅威・インシデントについては、必ずしも十分対応がカバーされているとは言えないことから、人為的なミスを防ぐための機能として捉えた場合には、「ある程度重視される」という評価結果となった。

更に残りの１事業者においては、セキュリティ機能ごとに評価結果が分かれ、クラウドセキュリティの機能では、「かなり重視される」、SOC やマネージドセキュリティの機能では、「ある程度重視される」、エンドポイントセキュリティの機能では、「あまり重視されない」という評価結果となった。クラウドセキュリティの機能については、クラウドアプリケーションの利用範囲が広がれば、カバーが必要となる脅威・インシデントの対応範囲もより広範になるため、「かなり重視される」という考えによるものであった。

(イ)評価項目の有効性に対する考察

直近のサイバー攻撃など、世の中で騒がれているような脅威・インシデントに、最低限かつ確実に対応してもらいたいと考えている。

使用するアプリケーションの利用範囲が広がれば、カバーすべき脅威・インシデントの対応範囲も広がるため、アプリケーションを使うユーザー側の意識啓発や人材育成のための教育とセットでサイバーセキュリティ製品・サービスの導入について考え

ないといけないと考えている。

② 未知の脅威・インシデントへの対応が可能である

(ア) 重視度合い

中小企業ユーザー６事業者のうち、６事業者が「かなり重視される」という評価結果となり、かなり有効であった。

(イ) 評価項目の有効性に対する考察

未知の脅威・インシデントとしては、新たな手口によるサイバー攻撃や、新種のマルウェアによる感染等に加えて、想定していない人為的なミスや内部不正による脅威・インシデントに対しても、適切に対応できることが必要であると考えている。

③ 人為的ミスなどにより、製品そのものが他人（攻撃者）の手に渡るといった、万が一の場合でも悪用が難しい

(ア) 重視度合い

中小企業ユーザー６事業者のうち、２事業者が「かなり重視される」、４事業者が「ある程度重視される」という評価結果となり、概ね有効であった。

(イ) 評価項目の有効性に対する考察

セキュリティベンダーの担当者が悪意を持てば、PC 内の情報を盗み見できたり、PC 内の情報を消したりすることができるという状況は避けたいと考えている。

また、セキュリティベンダー側が、ユーザー側における製品・サービスの使い勝手をある程度犠牲にしてでも、悪用防止を最優先に考えた製品・サービス設計を行っていることについては、悪用を防ぐうえで仕方がないと考えている。

以上の重視度合いや、評価項目の有効性に対する考察を踏まえると、新たに評価項目に盛り込むべき内容としては、「人為的なミスや内部不正への対応」や「悪用防止を考えた製品・サービス設計」、「製品・サービスを使う側のユーザーに対する教育との一体化」といった内容が考えられる。

3.1.4. 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の見直し

「3.1.3. 評価項目の有効性検証結果」の中で導出された新たに評価項目に盛り込むべき内容をもとに、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について、見直しを行った。以下に見直し後の中小企業向けサイバーセキュリティ製品・サービスに関する評価項目を示す。

図表 3-1 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（評価項目の有効性検証結果に基づく見直し後）

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を伴わず実装が容易である
		②	現場の事情に合わせて、使う機能を自由に選べたり、必要機能が用意されていて、オーバースペックによる無駄を省くことが容易である
		③	いろいろと細かい設定を求められることがなく、作業負荷の軽減が可能である
		④	PCのシステムパフォーマンスやインストール済みのソフトウェアへの影響を最小限に抑えることが可能である
		⑤	本格的に導入する前に、お試し利用が可能であり、問題なく使えることの確認・検証が可能である
		⑥	確実に使えるようになるまで伴走型で手厚いサポート対応が可能である
(2)	運用のし易さ	①	社内に専門的な人材がいなくてもメンテナンスが可能である
		②	さまざまな状況に応じた適切なアドバイスや対応マニュアル、トラブルシューティング、FAQなどのサポートが充実していて、万が一インシデントが起きた場合の対応や勤務時間外の対応の省力化が可能である
		③	問合せ・相談窓口へのアクセスが容易であり、速くて質の高い応答を踏まえた対応が可能である
(3)	導入や運用を行うことで得られる効果	①	導入した後からあれこれと機能の追加を求めないなど、追加コストの発生を低く抑えることや、PCの安定的な稼動への影響を回避することが可能である
		②	サイバーセキュリティに関して身につける新しい知識が必要最小限でよくなり、対策の導入や運用に係る工数や負荷を低く抑えることが可能である
		③	製品・サービスを適切に使えるようになるため、必要最小限の製品・サービスに関する知識を身につけることが可能である
(4)	導入時や運用時に要する費用	①	インストール台数の無制限や製品ライフサイクルの長期化等の費用面のメリットを享受できるため、導入コストが安価である
		②	インシデント発生時に自社で想定される損失額やセキュリティ運用のトータル費用等の必要費用との見合いで、運用コストが安価である
		③	サイバー保険の活用等により、インシデント対応に係るコストを賄うことが可能である
(5)	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、誰もが納得のできる客観的な根拠(企業等の導入実績・市場シェア、脅威の検知・駆除実績、運用チーム編成・運用担当者のスキル・経験、ガイドライン・技術標準への準拠、技術特許、第三者評価等)に基づき、パンフレットやカタログ等において適切な説明がなされている
		②	自社にとって必要となる製品・サービスや機能・性能を、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一貫したサポートに基づき、提示することが可能である
(6)	製品・サービスの経営へのインパクト	①	パッケージ化によるディスカウントやリース・レンタル利用等を通じたコスト削減により、費用面と必要となる対策面の合理的な折り合いを実現するなど、インセンティブの付与が可能である
		②	オペレーション全体をグリップすることにより、セキュリティ運用とシステム運用の双方の運用負荷の問題を同時に解決できるようになるなど、インセンティブの付与が可能である
		③	製品・サービスの概念・コンセプトが明快で理解しやすく、運用負荷も必要最小限で、製品・サービスの確実な導入・運用が可能であり、対策の取組状況を取引先(顧客)等の外部にアピールしやすい
(7)	製品・サービスのセキュリティ性能	①	対応可能な既存の脅威・インシデントのパターン・範囲が広範である
		②	新たな手口によるサイバー攻撃や新種のマルウェアによる感染のみならず、想定していない人為的なミスや内部不正も含め、未知の脅威・インシデントへの対応が可能である
		③	人為的ミスやアカウントの乗っ取りなど万が一の場合でも悪用が難しく、そのような悪用防止を考えた製品・サービス設計になっている
		④	製品・サービスを使う側のユーザに対する教育サービスが組み込まれた製品・サービスになっている

注）赤字は、新規に評価項目を追加した箇所や、既存の評価項目の記載内容を一部修正した箇所を表している。

3.2. 仮説検証と考察

3.2.1. 情報の信頼性を担保するための検証手法に関する仮説検証と考察

「2.2.2. 情報の信頼性を担保するための検証手法に関する仮説の構築とその考え方」で前述した調査仮説について、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」において議論を行い、情報の信頼性を担保するための検証手法に関して、一定の方向性を導出し、取りまとめた。

情報の信頼性を担保するための検証手法に関する方向性とその考察、今後の検討課題について、以下に整理する。

(ア) 情報の信頼性を担保するための検証手法に関する方向性

中小企業向け情報提供プラットフォームに掲載される情報については、登録申請者から申請時に提供される評価項目に沿った形での情報が掲載されることになるが、登録申請者に対して、当該情報の裏付けとなる定量的な情報の提出を追加的に求めることにより、信頼性、妥当性を担保するものとする。

申請時に提供される情報の信頼性、妥当性に関する裏付け確認は、情報提供プラットフォームの運営者が追加的に提出される定量的な情報をもとに行い、その確認結果を踏まえて評価会議が登録可否や掲載可否の評価・判断を行うものとする。

なお、登録申請者から提供されるサイバーセキュリティ製品・サービスの性能・スペック等に関する情報を評価項目に沿った形で検証・評価しようとすると、運営者側や評価会議側で適切な評価を行うことが難しく、また、申請から掲載までのサイクルが長くなるなど、課題が多いことから、現実的ではないと判断した。

また、中小企業ユーザーのモニターの組織化による事後評価についても、中小企業ユーザー側の知識や利用状況によって評価にばらつきが生じたり、評価のサンプル数を多く確保できないと評価の精度が下がったりするなど、誤った情報の提供になる懸念があり、課題が多いことから、現実的ではないと判断した。

(イ) 考察及び今後の検討課題

サイバーセキュリティ製品・サービスの性能・スペック等については、申請書やカタログ、仕様書において定性的な表現での説明が多いため、評価会議により登録可否や掲載可否の評価・判断を行うことが難しくなることが懸念される。

このため、登録申請者に対して、評価項目に沿った形で各項目に対応する定量的な情報の提出を追加的に求める必要がある。例えば、定量的な情報としては、インストールに要する時間、設定項目数、Linux 等の外部対応必要数などが考えられる。

その一方で、定量的な情報については、当該情報を準備することがセキュリティベンダーにとって過重な負担にならないよう、また当該情報の準備に係る負担が情報提供プラットフォームへの掲載の制約要因とならないよう十分に配慮する必要がある。

このような定量的な情報を含め、評価・判断を行う際の具体的な基準については、今後検討していくことが必要である。

3.2.2. 中小企業向け情報提供プラットフォームに関する仮説検証と考察

「2.2.3. 中小企業向け情報提供プラットフォームのあるべき姿等に関する仮説の構築とその考え方」で前述した調査仮説について、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」において議論を行い、中小企業向け情報提供プラットフォームのあるべき姿等に関して、一定の方向性を導出し、取りまとめた。

中小企業向け情報提供プラットフォームのあるべき姿等に関する検討すべき論点を以下に再掲する。

論点① 意義・目的について、どのように位置づけるか
論点② 運営者について、どのように考えるか
論点③ 申請情報について、情報の信頼性をどのような手法・運用体制で担保するか
論点④ 登録の可否を判断するうえで、ベンダーから提供してもらうべき必要な情報は何か
論点⑤ 提供機能としては、評価情報の提供までとするか、更にその先の事業者マッチングや製品・サービス販売等にまで踏み込むか
論点⑥ 登録可否の判断や掲載可否の判断のルール化について、どのようなケースにおいて登録不可・掲載不可とするべきか
論点⑦ 登録・掲載後、製品・サービスの内容に変更が生じたときに、どのような対応が必要になるか
論点⑧ 情報提供プラットフォーム上で情報を探す際のインデックスの付け方について、どのように考えるべきか

また、それぞれの論点ごとの中小企業向け情報提供プラットフォームのあるべき姿等に関する方向性とその考察、今後の検討課題について、以下に整理する。

(1)論点①に関する方向性とその考察、今後の検討課題

(ア) 論点①に関する方向性

中小企業におけるサイバーセキュリティ製品・サービスの導入を支援し、ひいては中小企業におけるサイバーセキュリティ対策の課題解決に繋げることを、情報提供プラットフォーム構築・運用の意義・目的とする。

また、初期(立ち上げ時)においては、①インシデント発生時の迅速な初動対応、②重要な情報の安全な取扱い、③不正プログラム対策の３つに資する中小企業向けサイバーセキュリティ製品・サービスを対象範囲とし、中小企業におけるサイバーセキュリティ製品・サービスの導入を支援するものとする。

(イ) 考察及び今後の検討課題

情報提供プラットフォームに掲載される情報については、中小企業にとって何が有益であるか、中小企業の目線で考え方を整理することが重要である。

中小企業の担当者は、サイバーセキュリティ製品・サービスのカタログや仕様書として提供されている情報を読み解くのに困難を抱えている。そのような状況を考慮すると、サイバーセキュリティ製品・サービスのカタログや仕様書として提供されている情報を精査し、評価項目の区分に沿って、情報をかみ砕いて比較しやすい形で掲載することにより、中小企業の担当者の理解を増進するだけでも、情報提供プラットフォーム構築・運用の意義があると考えられる。

他方、サイバーセキュリティ製品・サービスのカタログや仕様書として提供されている情報のみを情報提供プラットフォームに掲載する場合については、中小企業にとって必ずしも有益であるとは言えない。また、テストベッド等において技術的な評価・検証を行った際の評価・検証結果の情報を情報提供プラットフォームに掲載する場合については、評価・検証に係るコストについて、登録申請者である中小企業に過重な負担を強いることになる。従って、そのような形での情報提供プラットフォーム構築・運用については、意義・目的が意にそぐわないと判断した。

情報提供プラットフォーム上で扱う中小企業向けサイバーセキュリティ製品・サービスの対象範囲については、発注元が、契約先及び再契約先に求めるサイバーセキュリティ対策として、相対的にみてニーズの高い、①インシデント発生時の迅速な初動対応、②重要な情報の安全な取扱い、③不正プログラム対策の３つの対策に資する製品・サービスを、初期(立ち上げ時)の対象範囲とすることが有益であると考えられる。

他方、セキュリティクリアランスに関わる製品・サービスについては、国内において提供されている例が少ないことから、中小企業向けサイバーセキュリティ製品・サービスの対象範囲には含めないこととした。また、サイバーセキュリティサービスについては、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しているため、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、サイバー

セキュリティ製品と紐づかないサービスについても対象範囲には含めないこととした。

(2)論点②に関する方向性とその考察、今後の検討課題

(ア)論点②に関する方向性

初期(立ち上げ時)の情報提供プラットフォームの運営者については、公的機関とすることが望ましい。

(イ)考察及び今後の検討課題

情報提供プラットフォームに掲載される情報については、中立性・公平性が求められることから、初期(立ち上げ時)においては、公的機関を前提として考えるのが自然である。

他方、情報提供プラットフォームが普及・浸透し、収益性が見込めるようになった段階においては、民間やコンソーシアムへの委託も視野に入れて検討していくことが必要である。

(3)論点③に関する方向性とその考察、今後の検討課題(再掲)

(ア)論点③に関する方向性(再掲)

中小企業向け情報提供プラットフォームに掲載される情報については、登録申請者に対して、申請時に提供される情報の裏付けとなる定量的な情報の提出を追加的に求めることにより、信頼性、妥当性を担保するものとする。

申請時に提供される情報の信頼性、妥当性に関する裏付け確認は、情報提供プラットフォームの運営者が追加的に提出される定量的な情報をもとに行い、その確認結果を踏まえて評価会議が登録可否や掲載可否の評価・判断を行うものとする。

(イ)考察及び今後の検討課題(再掲)

サイバーセキュリティ製品・サービスの性能・スペック等については、申請書やカタログ、仕様書において定性的な表現での説明が多いため、評価会議による登録可否や掲載可否の評価・判断が難しくなることが懸念される。

このため、登録申請者に対して、評価項目に沿った形で各項目に対応する定量的な情報の提出を追加的に求める必要がある。例えば、定量的な情報としては、インストールに要する時間、設定項目数、Linux 等の外部対応必要数などが考えられる。

その一方で、定量的な情報については、当該情報を準備することがセキュリティベンダーにとって過重な負担にならないよう、また当該情報の準備に係る負担が情報提供プラットフォームへの掲載の制約要因とならないよう十分に配慮する必要がある。

このような定量的な情報を含め、評価・判断を行う際の具体的な基準については、今後検討していくことが必要である。

(4)論点④に関する方向性とその考察、今後の検討課題

(ア)論点④に関する方向性

登録不可や掲載取り消しについて、情報提供プラットフォームの運営者または評価会議が明確に判断できるようにし、そのための対応ルールを策定するものとする。

また、情報提供プラットフォームに掲載される情報の情報源たる、登録申請者については、要件を明確にし、初期(立ち上げ時)においては、販売代理店・ディストリビュータを登録申請者の要件に含めないものとする。

さらに、登録の可否を判断するうえで、中小企業が重要視している、登録申請者の経営状態や事業継続性に関する情報についても、登録申請者に提供を求めるものとする。

(イ)考察及び今後の検討課題

あまりにも評価の低いサイバーセキュリティ製品・サービスについては、評価会議による評価で足切りし、登録不可とするという対応を実務上行うことが考えられる。また、登録申請者が重大なインシデントを起こした場合や登録申請者が廃業した場合においては、掲載の取り消しという対応を実務上行うことが考えられる。

登録不可や掲載取り消しとする際には、説明責任を果たすために、登録不可や掲載取り消しの理由を明確にする必要がある。特に登録不可の理由については、明確にできない場合が起こり得る。そのような懸念が生じるため、今後、登録不可や掲載取り消しとする際の具体的な対応ルールについて検討していくことが必要である。

販売代理店・ディストリビュータのビジネスモデルを考慮すると、販売代理店・ディストリビュータが登録申請者となる場合には、幾つかの製品をまとめてパッケージ化して、１つの製品とし、登録申請を行うケースや、複数の販売代理店・ディストリビュータから同じ製品・サービスが登録申請されるケースが出てくる可能性があるため、販売代理店・ディストリビュータを登録申請者の要件に含めないこととした。但し、製品・サービスの導入を検討する中小企業にとって販売代理店・ディストリビュータの存在は大きく、欠かせない役割を担っていることから、登録申請者の要件に含

めないという運用は、初期(立ち上げ時)においてのみ必要であるとした。

中小企業においては、製品・サービス選びの際に登録申請者の経営状態や事業継続性(サポート継続等)といった情報が重要視されるため、情報提供プラットフォームに掲載される情報の１つとして取扱う必要がある。但し、あくまで時点評価の情報になるため、参考情報であり、その情報を使うかどうかの判断は中小企業に委ねることとした。

(5)論点⑤に関する方向性とその考察、今後の検討課題

(ア)論点⑤に関する方向性

あくまで中小企業向けサイバーセキュリティ製品・サービスに対する中小企業の担当者の理解を増進するために資する情報の掲載を主軸とし、事業者間のマッチングや製品・サービス販売については実施しない方向とする。

(イ)考察及び今後の検討課題

事業者間のマッチングや製品・サービス販売は実施しない方向とするが、中小企業の製品・サービス選びの利便性を鑑みると、製品・サービスの販売元・販売代理店・ディストリビュータに関するリンク情報については、登録申請者に作成・提出してもらい、情報提供プラットフォーム上で一括して参照できるようにする必要がある。但し、リンク情報の更新については、登録申請者側に責任を持たせることが重要となる。

(6)論点⑥に関する方向性とその考察、今後の検討課題

(ア)論点⑥に関する方向性

登録可否の判断・評価の基準については、申請書に不備がなく、内容面もしっかりと記載されているか、カタログ等と照らし合わせてみた場合に虚偽の記載がないか、反社会的勢力に加担していないかなどの形式的なチェックにおいて判断し、必要に応じて申請書の内容を確認するためのヒアリングを実施するものとする。

掲載取り消しの判断・評価の基準については、登録申請者が重大なインシデントを起こした場合や廃業した場合に加えて、虚偽の記載が発覚した場合や、M&A 等により運営主体・体制や運営ポリシーに変更が生じた場合も含めるものとする。

(イ)考察及び今後の検討課題

起業して間もない企業が提供する製品・サービスについては、掲載していない中小

企業向け情報提供プラットフォームが存在したり、また、２期～３期連続で赤字が続く企業を対象外とするような政府の事業も存在したりするが、政府として、国産のサイバーセキュリティ製品・サービスやそれらの製品・サービスを開発・販売するベンチャー企業等を育てていくという方針を掲げていることから、登録可否の判断・評価の基準や掲載取り消しの判断・評価の基準については、あまりハードルを上げ過ぎないよう十分な配慮が必要である。

（7）論点⑦に関する方向性とその考察、今後の検討課題

(ア) 論点⑦に関する方向性

情報提供プラットフォームに掲載される情報は、あくまで時点評価に基づく参考情報であることから、登録申請者から申請された情報に基づくものであり、サイバーセキュリティ製品・サービスの性能・スペックを保証するものではないというエクスキューズを入れて掲載し、その情報を使うかどうかの判断は中小企業に委ねるものとする。

一方で、登録申請者に対して、サイバーセキュリティ製品・サービスの内容について、利用者側に影響のある変更が生じた場合には、情報提供プラットフォームの運営者に報告する義務を課すものとする。

(イ) 考察及び今後の検討課題

情報提供プラットフォームに掲載される情報の陳腐化を回避するため、サイバーセキュリティ製品・サービスの内容について変更が生じた場合には、情報のアップデートができる仕組みが必要である。

一方で、製品・サービスの内容の変更については、バージョン毎に管理されるサイバーセキュリティ製品とは異なり、サイバーセキュリティサービスは、頻繁にアップデートが発生するものであるため、報告を求める変更の程度を利用者側に影響のある変更とした。

（8）論点⑧に関する方向性とその考察、今後の検討課題

(ア) 論点⑧に関する方向性

情報提供プラットフォーム上で情報を探す際のインデックスの付け方については、従業員の規模やPCの台数、個人情報の取扱いの有無、年間のセキュリティ投資額等を参考としつつ、中小企業の意向を重視して設定し、必要となるサイバーセキュリティ

製品・サービスを検索できるようにする。

(イ) 考察及び今後の検討課題

中小企業は、売上高や従業員の規模を始めとして、業種、IT 利用環境、商慣習などが多種多様であり、中小企業を一律に一括りにすることが難しく、情報提供プラットフォームにおいて必要とする情報も異なる。情報提供プラットフォーム上で必要となる情報を探しやすくするために、インデックスの設定が必要である。どのような中小企業の意向を重視して、インデックスを設定するかについては、今後、検討していくことが必要である。

4. 評価項目

「3.1.4. 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の見直し」で前述した見直し後の中小企業向けサイバーセキュリティ製品・サービスに関する評価項目について、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」において議論を行い、その内容を踏まえて当該評価項目の最終版を取りまとめた。

「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」における議論においては、各評価項目で満たすべき要件について、セキュリティベンダーが申請しやすいように、また情報提供プラットフォームの運営者または評価会議が評価しやすいように、定性的なものにせず、できる限り「できる」、「できない」の２択や、「必要である」、「必要ではない」の２択から選べるような形にし、評価項目について説明する文章の表現方法についても、できる限りシンプルにした方がよいという意見が大勢を占めた。このため、見直し後の中小企業向けサイバーセキュリティ製品・サービスに関する評価項目について、構成や表現方法を大幅に変更することとなった。

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の最終版を、以下に示す。

図表 4-1 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（最終版）

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

5. 中小企業に広く訴求するためのコンテンツ

中小企業に広く訴求するために、セキュリティベンダー側、中小企業側に提供するコンテンツとして、「評価項目の定義・解説書」、「評価項目に沿った申請時の記載方法の手引書」、「中小企業におけるプラットフォームの活用方法」の３つのコンテンツを取りまとめた。それぞれのコンテンツについて、以下に示す。

5.1. 評価項目の定義・解説書

前述した導入実証による評価項目の有効性検証結果や、「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」における議論の内容を踏まえて、登録申請者がサイバーセキュリティ製品・サービスに関する情報を申請する際に用いる参考とすべき評価の観点や、詳細な評価項目について、それぞれの定義や解説を、評価項目の定義・解析書として取りまとめた。

5.1.1. 評価項目の観点に関する定義・解説

評価項目の観点としては、（１）導入のし易さ、（２）運用のし易さ、（３）導入時や運用時に要する費用、（４）導入や運用における課題の解決、（５）製品・サービスの効果、（６）製品・サービスに付帯するオプションサービスその他の６つの観点を設定した。

それぞれの観点を以下に定義・解説する。

（1）導入のし易さの観点に関する定義・解説

中小企業においては、セキュリティ担当者が確保されている場合が少ないだけでなく、システム担当者が確保されていて、セキュリティまで管理するような場合でも専業の担当者ではなく、他の業務との兼業の担当者が多いため、担当者に負担をかけずに、作業時間も費やすことなく、サイバーセキュリティ製品・サービスを容易に導入できることが求められる。

（2）運用のし易さの観点に関する定義・解説

中小企業において、サイバーセキュリティ製品・サービスの運用・メンテナンスに係る作業を、自社の担当者のみで充足させるには、専門的な知識・スキルの確保や、担当者の教育や研修に掛けられるコストが必ずしも十分ではないという制約があり、自ずと限界が生じるため、そのような状況下に置かれた場合でも、外部のセキュリティベンダーの手を借りて作業の省力化を図りながら、サイバーセキュリティ製品・サービスの運用・メンテナンスに対応できることが求められる。

（3）導入時や運用時に要する費用の観点に関する定義・解説

中小企業においては、導入時に要する費用が高額になれば、そもそもサイバーセキュリティ製品・サービスの導入自体を検討の俎上に載せることが難しくなる。他方、運用時に要する費用が高額になれば、経営層から導入するサイバーセキュリティ製品・サービスの費用対効果を問われることになり、導入時に脅威・インシデントの発生を経験できることが稀で、費用対効果を実感しにくい状況の中で、担当者はその対応や説明に苦慮することになる。このため、中小企業におけるサイバーセキュリティ製品・サービス選びにおいては、導入時や運用時に要する費用が安価であることが求められる。

(4)導入や運用における課題の解決の観点に関する定義・解説

中小企業においては、担当者が保有するサイバーセキュリティやサイバーセキュリティ製品・サービスに関する専門的な知識・スキルが必ずしも十分とは言えないことから、サイバーセキュリティ製品・サービスの導入や運用において、担当者が直面するさまざまな課題を解決できることが求められる。

(5)製品・サービスの効果の観点に関する定義・解説

中小企業においては、ウイルス対策ソフトやファイアウォールの導入が比較的進んでいるが、大企業と比較するとまだまだ対策が手薄であると判断される場合が少なからず見受けられることから、攻撃者に狙われる機会が増えてきている。サイバー攻撃の手口が高度化・巧妙化する中で、導入・運用するサイバーセキュリティ製品・サービスの効果によって、脅威・インシデントに対する防御をより一層充実・強化できることが求められる。

(6)製品・サービスに付帯するオプションサービスその他の観点に関する定義・解説

中小企業においては、サイバーセキュリティ対策に掛けられる費用が限られる中で、自社にとって必要となるサイバーセキュリティ対策を、サイバーセキュリティ製品・サービスやそれに付帯するオプションサービスのレベルで十分賄うことができ、それが費用面からみても十分合理性をもって折り合っていることが求められる。

5.1.2. 詳細な評価項目に関する定義・解説

評価項目の観点を更に具体化した詳細な評価項目を設定した。それぞれの詳細な評価項目を以下に定義・解説する。

(1)導入のし易さの観点

① 「大規模なシステム改修の必要性がない」に関する定義・解説

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繋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。

② 「必要となる機能を自由に選択することができる」に関する定義・解説

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な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。

③ 「インストールや設定の手間を省くことができる」に関する定義・解説

インストール・設定作業の負荷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、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。

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」に関する定義・解説

中小企業の担当者がインストール・設定作業の途中段階でつまずけば、作業が完了しない状態を招いたり、その状態を放置したままになったりする可能性がある。このため、担当者がインストール・設定作業を行う際に求められる知識については、できる限り必要最小限にし、マニュアル通りに簡単に作業を進められるようにすることにより、作業の停滞や未完了

を極力回避できるようにすることが必要である。このように、中小企業においては、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ことが求められる。

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」に関する定義・解説

中小企業にとって、サイバーセキュリティ製品・サービスを導入した後、その影響により PC のシステムパフォーマンスが低下し、PC が使いづらくなることで業務が停滞し支障が生じることは、経営を継続していくうえで命取りになる可能性がある。また、セキュリティベンダーによっては、推奨されるシステム要件に関する情報を提供しているところもあるが、PC の使い方は各社で異なるため、推奨されるシステム要件が見込みどおりに必ずしも十分に機能しているとは言えず、中小企業からはメモリの使用率の数値など、実際の影響について確認・把握したいという声も聞かれる。このように、中小企業においては、PC のシステムパフォーマンスへの影響が最小限であることが求められる。

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」に関する定義・解説

PC のシステムパフォーマンス低下以外に、業務の停滞や支障を招きかねないのが、サイバーセキュリティ製品・サービスが、既に PC にインストール済みのソフトウェアに影響を与えるような場合である。具体的には、基幹システムを始めとして、業務で頻繁に使用する電子メールやウェブサイトの閲覧、文書の作成・保存、プリンター等に関連するソフトウェアに影響を与え、使用できなくなるような事態が想定される。このように、中小企業においては、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ことが求められる。

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」に関する定義・解説

セキュリティベンダーによっては、提供するサイバーセキュリティ製品・サービスに関して、本格的に導入する前に、お試し利用をできるようにしているところもあるが、お試し利用を活用できる期間はあまり長く設定されていないため、お試し利用の期間中にトラブルや脅威・インシデントについて経験できることは稀であり、導入する側の中小企業では、当該製品・サービスが問題なく使えるということの確認・検証について、必ずしも十分できているとは言えない状況である。このようなお試し利用の更なる充実を含めて、中小企業においては、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ことが求められる。

⑧「導入に関してのサポート対応がある」に関する定義・解説

中小企業の担当者が保有するサイバーセキュリティやサイバーセキュリティ製品・サービスに関する知識が限られる中で、担当者のみでインストール・設定作業を行い、製品・サー

ビスを確実に使えるようにすることは現実には難しくなっており、多かれ少なかれセキュリティベンダーのサポート対応に依存せざるを得ない状況となっている。特に導入時には、インストール・設定作業中につまずくことが多いことが考えられ、また製品・サービスに対する習熟度も低いことが想定されることから、伴走型でより手厚いサポート対応が必要になっている。このような伴走型での手厚いサポート対応を含め、中小企業においては、導入に関してのサポート対応があることが求められる。

(2)運用のし易さの観点

① 「運用に関しての専門的な知識が必要ない」に関する定義・解説

中小企業においては、社内にサイバーセキュリティに関する専門的な人材を抱えることが難しいため、サイバーセキュリティ製品・サービスの運用・メンテナンス作業については、作業に係る負担の軽減を図る観点から、セキュリティベンダーに委ねる傾向にある。また、コスト面の制約からセキュリティベンダーに委ねることが難しく、専門的な知識が乏しい担当者が運用・メンテナンス作業に携わるような場合でも、適切に対応できることが必要である。このように、中小企業においては、運用に関しての専門的な知識が必要ないことが求められる。

② 「さまざまな状況に応じたサポートツールがある」に関する定義・解説

大企業向けサイバーセキュリティ製品・サービスと比較して、中小企業向けサイバーセキュリティ製品・サービスの利用料金を低く抑えることができている大きな理由は、セキュリティベンダーが 24 時間 365 日での、セキュリティエキスパートによる問合せ・相談対応を受け付けておらず、サポートの品質を一定のレベルまで引き下げていることである。このため、中小企業においては、何かトラブルやエラーが発生したときに、セキュリティベンダーが用意している対応マニュアルやFAQ、トラブルシューティング等を見ながら自社で対応できるようになっていることが必要である。このように、中小企業においては、さまざまな状況に応じたサポートツールがあることが求められる。

③ 「問合せ・相談窓口を設置している」に関する定義・解説

社内にサイバーセキュリティに関する専門的な人材を抱えることが難しい中小企業にとって、何かトラブルやインシデントが発生したときに、セキュリティベンダーに対応方法を問合せ・相談できることは安心に繋がる。特に中小企業の場合においては、トラブルやインシデントの発生によって業務停止に陥れば、経営にもたらされる影響が甚大になることから、早期の問題解決や復旧のために、問合せ・相談窓口へのアクセスが容易で、かつ問合せ・相

談窓口からの速くて質の高い応答をもとに適切に対応できることが必要である。このような確実なアクセスや応答時間の短縮等を含めて、中小企業においては、問合せ・相談窓口を設置していることが求められる。

(3)導入時や運用時に要する費用の観点

① 「導入コストが安価である」に関する定義・解説

サイバーセキュリティ製品・サービスの導入にあたり、中小企業にとっては、価格設定の低さはもちろんのこと、何らかの形で費用面のメリットを享受でき、お買得感・割安感があることも重要である。費用面のメリットとしては、複数台分のライセンスをまとめ買いした際のボリュームディスカウントや、製品とその運用サービスや、必要となる製品・サービスがパッケージ化されて提供された際のディスカウント、インストールする PC の台数の無制限、製品・サービスのライフサイクル期間に見合った償却期間の伸長、リース・レンタルでの利用等が想定される。このように、中小企業においては、導入コストが安価であることが求められる。

② 「運用コストが安価である」に関する定義・解説

中小企業においては、個人情報の漏えい事故など、脅威・インシデントの発生時に自社で想定される損失額との見合いや、セキュリティ運用のトータル費用との見合いで、サイバーセキュリティ製品・サービスに関する運用コストの経済性を見るのが適切であるとの考え方が強い。後者の場合には、セキュリティ運用のトータル費用を試算するうえで、導入後に求められる機能追加に伴う追加コストの発生や、運用に係る工数や負荷がもたらすコストへの影響、セキュリティ運用とシステム運用の双方の運用の一体化・集約化によるコスト削減効果等の観点も重要な要素となる。このような多様な経済性の観点を含めて、中小企業においては、運用コストが安価であることが求められる。

(4)導入や運用における課題の解決の観点

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」に関する定義・解説

中小企業の担当者は、導入検討しているサイバーセキュリティ製品・サービスの性能・スペックについて、経営層に説明する機会が生じるが、経営層が気にするのは、世の中で騒がれているような脅威・インシデントに対して、適切に対応できるかどうかという点である。このような説明において求められるのは、誰もが納得のできる客観的な根拠を提示できるこ

とである。客観的な根拠としては、企業等の導入実績、市場シェア、脅威の検知・駆除実績、運用チーム編成・運用担当者のスキル・経験、ガイドライン・技術標準への準拠、技術特許の取得、第三者評価機関による認証取得等が想定される。このような多様な観点を含めて、中小企業においては、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ことが求められる。

(5)製品・サービスの効果の観点

① 「既知の脅威・インシデントに対応することができる」に関する定義・解説

中小企業においては、サイバー攻撃の手口が高度化・巧妙化する中で、サイバーセキュリティ製品・サービスの導入・運用によって対応可能な脅威・インシデントの範囲が広範になればなるほど、安心できると考えている。そのような観点から、中小企業においては、既知の脅威・インシデントに対応することができることが求められる。

② 「未知の脅威・インシデントに対応することができる」に関する定義・解説

中小企業においては、ウイルス対策ソフトやファイアウォールの導入が比較的進んでいるが、大企業と比較するとまだまだ対策が手薄であると判断される場合が少なからず見受けられることから、攻撃者に狙われる機会が増えてきている。このため、既知の脅威・インシデントだけでなく、ウイルス対策ソフトでは十分検知できない未知の脅威・インシデントに対しても適切に対応できるようになることが必要になってきている。このように、中小企業においては、未知の脅威・インシデントに対応することができることが求められる。

③ 「ユーザー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」に関する定義・解説

一部の中小企業においては、現在のサイバーセキュリティ製品・サービスは、ある程度広範な脅威・インシデントに対して、セキュリティを守る機能が備わっていると捉え、既知の脅威・インシデントや未知の脅威・インシデントの対応がカバーされているだけでは、新たな投資へのインセンティブが働き難いと考えているところもある。クラウドサービスや IoT など新たな IT の利活用とそのセキュリティリスクが表裏一体となる中で、ユーザー側の人為的なミスや内部不正による脅威・インシデントが新たなセキュリティリスクとして浮上しつつあり、中小企業においても関心が高まっている。このような新たなセキュリティリスクの観点を含めて、中小企業においては、ユーザー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ことが求められる。

(6)製品・サービスに付帯するオプションサービスその他の観点

① 「サイバー保険等の補償サービスの利用ができる」に関する定義・解説

万が一、インシデントが発生した場合に必要となる原因・被害調査や復旧、再発防止等に係る費用や、損害賠償責任に関する補償費用を、サイバーセキュリティ製品・サービスに付帯するサイバー保険等の補償サービスにより賄うことができれば、中小企業にとって安心感があり、魅力的な製品・サービスとなる。このように、中小企業においては、サイバー保険等の補償サービスの利用ができることが求められる。

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」に関する定義・解説

中小企業においては、サイバーセキュリティに関する専門的な人材を抱えることが難しいため、自社でセキュリティ設計を行ったり、自社にとって必要となる対策や機能を選んだりすることが困難である。このため、サイバーセキュリティ製品・サービスに付帯するリスク評価(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により、自社内にどれぐらいのリスクが存在して、製品・サービスを導入すれば、リスクをどの程度低減できる可能性があるかといった内容を見える化したり、自社の従業員規模や IT の利用状況・利用環境を見て、必要となる対策や機能を分かりやすく提示してもらったりすることができれば、中小企業においてセキュリティベンダーとの信頼関係の醸成に繋がる。このようなリスクの見える化や必要となる対策や機能の提示を含め、中小企業においては、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ことが求められる。

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」に関する定義・解説

中小企業においては、インシデント発生時の対応に係る知識や経験が必ずしも十分とは言えず、自社で対応しようとすれば、初動対応を見誤りがちである。このため、サイバーセキュリティ製品・サービスに付帯するインシデント対応等の緊急対応サービスにより、セキュリティベンダーからインシデント発生時のさまざまな状況に応じて適切なアドバイスをもらいながら、必要となる対応・アクションの道筋を提示してもらったり、自社での積極的な対応・アクションを不要にできたりすることができれば、中小企業にとって安心感があり、魅力的な製品・サービスとなる。このように、中小企業においては、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ことが求められる。

④ 「勤務時間外対応のサポートサービスの利用ができる」に関する定義・解説

インシデントや障害の発生により業務やシステムを絶対に停止できないような状況下に置かれている中小企業においては、勤務時間内にインシデントが発生すれば、外部のセキュ

リティベンダーの手を借りながら、ある程度までは自社でも対応が可能であるが、勤務時間外にインシデントが発生すれば、対応人員の確保が難しく、自社で実施できる対応が限られてくるため、対応が後手に回る可能性がある。このため、サイバーセキュリティ製品・サービスに付帯する勤務時間外対応のサポートサービスにより、自社における勤務時間外の対応の省力化ができれば、中小企業にとって安心感があり、魅力的な製品・サービスとなる。このように、中小企業においては、勤務時間外対応のサポートサービスの利用ができることが求められる。

⑤ 「ユーザー側に対する教育サービスの利用ができる」に関する定義・解説

中小企業においては、使用するアプリケーションの利用範囲が広がれば、カバーすべき脅威・インシデントの対応範囲も広がるため、アプリケーションを使うユーザー側の意識啓発や人材育成のための教育とセットでサイバーセキュリティ製品・サービスの導入について考えないといけないと考えている。このため、サイバーセキュリティ製品・サービスに付帯するユーザー側に対する教育サービスにより、それが抑止力となって人為的なミスや内部不正による脅威・インシデントを防ぐことができれば、中小企業にとって有用である。このような意識啓発や人材育成を含めて、中小企業においては、ユーザー側に対する教育サービスの利用ができることが求められる。

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」に関する定義・解説

中小企業においては、導入・運用するサイバーセキュリティ製品・サービスが引き金となって、情報漏えい事故等の脅威・インシデントを招くという事態を避けたいと考えており、セキュリティベンダー側が製品・サービスの使い勝手よりも、攻撃者や人為的ミス等による悪用防止を最優先に考えた製品・サービス設計を適切に行っているような製品・サービスを選択しがちである。このように、中小企業においては、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ことが求められる。

5.2. 評価項目に沿った申請時の記載方法の手引書

セキュリティベンダーが評価項目に沿ってサイバーセキュリティ製品・サービスに関する情報の申請を行う際に、記載上の留意すべき点について、手引書として取りまとめた。

(1)導入のし易さの観点

① 「大規模なシステム改修の必要性がない」に関する記載上の留意すべき点

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。

〇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
〇機能追加や画面・帳票変更に関わるシステム改修
〇他組織のシステムとの連携に関わるシステム改修
〇その他のシステム改修

② 「必要となる機能を自由に選択することができる」に関する記載上の留意すべき点

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。

〇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
〇データや設定、操作の管理に関わる機能
〇アラートやログ情報等の情報提供に関わる機能
〇その他の機能

③ 「インストールや設定の手間を省くことができる」に関する記載上の留意すべき点

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。

〇利用者・管理者の登録や管理権限に関わる設定
〇システム・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
〇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
〇その他の設定

また、PC１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。

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」に関する記載上の留意すべき点

必要となる知識の習得内容・範囲から、どの程度必要最小限になっているかを判断できるように申請時に記載する必要がある。

必要となる知識の習得内容・範囲の例を以下に示す。

〇当該製品・サービスで使われている製品技術や、提供機能に関わる知識

〇システム・ネットワーク環境やセキュリティインシデント等の当該製品・サービスの導入や運用を行う上で必要となる知識

〇セキュリティインシデント対応に関わる知識

〇その他の知識

また、マニュアルの整備状況や記載内容等に関する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。

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」に関する記載上の留意すべき点

推奨されるシステム要件はもちろんのこと、メモリの使用率の数値など、実際の PC のシステムパフォーマンスへの影響に関する情報についても申請時に記載する必要がある。

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」に関する記載上の留意すべき点

PC にインストール済みのソフトウェアのうち、中小企業から報告があった影響が懸念されるソフトウェアについて申請時に記載する必要がある。

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」に関する記載上の留意すべき点

サイバーセキュリティ製品・サービスが提供する機能のうち、お試し利用が可能な機能について、有償、無償、利用期間などの利用条件や、実際に脅威・インシデントが発生した場合に必要となるやりとり、利用した結果のフィードバック等を含め、申請時に記載する必要がある。

⑧ 「導入に関してのサポート対応がある」に関する記載上の留意すべき点

導入に関するサポート対応について、通常の問合せ・相談窓口において実施するのか、代

理店・ディストリビュータが対応するのか、現場を訪問した担当者が伴走して対応するのか等、サポート対応のレベルについて申請時に記載する必要がある。

(2)運用のし易さの観点

① 「運用に関しての専門的な知識が必要ない」に関する記載上の留意すべき点

必要となる運用・メンテナンス対応の内容・範囲から、どの程度求められる専門的な知識が必要最小限になっているかを判断できるように申請時に記載する必要がある。

必要となる運用・メンテナンス対応の内容・範囲の例を以下に示す。

〇ソフトウェアや機器等のコンポーネントの更新や、セキュリティパッチの適応に関わる運用・メンテナンス対応

〇セキュリティポリシーの修正や設定の修正に関わる運用・メンテナンス対応

〇性能改善や性能向上に関わる運用・メンテナンス対応

〇その他の運用・メンテナンス対応知

② 「さまざまな状況に応じたサポートツールがある」に関する記載上の留意すべき点

対応マニュアルやFAQ、トラブルシューティング、管理コンソール等の利用可能なサポートツールについて、記載内容や利用方法等に関する情報を含め、申請時に記載する必要がある。

③ 「問合せ・相談窓口を設置している」に関する記載上の留意すべき点

利用可能な問合せ・相談窓口について、窓口の設置状況や連絡先（電話番号、メールアドレス等）や受付日・時間、応答に要する時間等の情報を含め、申請時に記載する必要がある。

(3)導入時や運用時に要する費用の観点

① 「導入コストが安価である」に関する記載上の留意すべき点

費用面のメリットの内容から、どの程度導入コストの削減を考えているかを判断できるように申請時に記載する必要がある。

費用面のメリットの内容の例を以下に示す。

〇ユーザー数や端末数に応じて増加するライセンスコストに関する費用面のメリット

〇調査費や工事費等の導入コストに関する費用面のメリット

〇製品・サービスそのものの価格に関する費用面のメリット

〇その他の費用面のメリット

また、必要となる製品・サービスがパッケージ化されて提供された際のディスカウントにに関する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。

必要となる製品・サービスのパッケージ化の例を以下に示す。

〇製品とその運用サービスのパッケージ化

〇世の中で普及している大手セキュリティベンダーの製品・サービスの相乗りでのパッケージ化

〇その他のパッケージ化

② 「運用コストが安価である」に関する記載上の留意すべき点

サイバーセキュリティ製品・サービスの運用に関わるトータル費用の多寡を判断できるように申請時に記載する必要がある。

運用に関わるトータル費用として考慮すべき観点の例を以下に示す。

〇導入後に求められる機能追加に伴う追加コスト

〇運用に係る工数や負荷がもたらす潜在コスト

〇セキュリティ運用とシステム運用の双方の運用の一体化・集約化による削減コスト

〇その他のコスト

(4)導入や運用における課題の解決の観点

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」に関する記載上の留意すべき点

製品・サービスの性能・スペックを裏付ける客観的な根拠として、企業等の導入実績、市場シェア、脅威の検知・駆除実績、運用チーム編成・運用担当者のスキル・経験、ガイドライン・技術標準への準拠、技術特許の取得、第三者評価機関による認証取得等を含め、申請時に記載する必要がある。

(5)製品・サービスの効果の観点

① 「既知の脅威・インシデントに対応することができる」に関する記載上の留意すべき点

対応可能な既知の脅威・インシデントについて、大分類に沿って、かつ検知・防御等に関する技術的な手法を含めて、申請時に記載する必要がある。

対応可能な既知の脅威・インシデントの内容・範囲の大分類の例を以下に示す。

〇外部からのサイバー攻撃等の脅威・インシデント

〇サプライチェーンを狙ったサイバー攻撃等の脅威・インシデント

○中小企業を狙ったサイバー攻撃等の脅威・インシデント
○その他の脅威・インシデント

② 「未知の脅威・インシデントに対応することができる」に関する記載上の留意すべき点
対応可能な未知の脅威・インシデントについて、検知・防御等に関する技術的な手法を含めて、申請時に記載する必要がある。

③ 「ユーザー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」に関する記載上の留意すべき点
対応可能なユーザー側の人為的なミスや内部不正による脅威・インシデントについて、検知・防御等に関する技術的な手法を含めて、申請時に記載する必要がある。

(6)製品・サービスに付帯するオプションサービスその他の観点

① 「サイバー保険等の補償サービスの利用ができる」に関する記載上の留意すべき点
利用可能なサイバー保険等の補償サービスについて、利用するメリットや効果はもちろんのこと、保険料の有無や、対象となる事故や損害、補償内容・範囲、補償給付限度額、補償給付が認められる条件、事故・損害証明等の必要となる手続きを含め、申請時に記載する必要がある。

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」に関する記載上の留意すべき点
利用可能なリスク評価(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について、利用するメリットや効果はもちろんのこと、利用料の有無や対象となるサービスの内容・範囲、中小企業に対して求められる対応や情報提供等を含め、申請時に記載する必要がある。

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」に関する記載上の留意すべき点
利用可能なインシデント対応等の緊急対応サービスについて、利用するメリットや効果はもちろんのこと、利用料の有無や対象となるサービスの内容・範囲、中小企業に対して求められる対応や情報提供等を含め、申請時に記載する必要がある。

④ 「勤務時間外対応のサポートサービスの利用ができる」に関する記載上の留意すべき点

利用可能な勤務時間外対応のサポートサービスについて、利用するメリットや効果はもちろんのこと、利用料の有無や対象となるサービスの内容・範囲、中小企業に対して求められる対応や情報提供等を含め、申請時に記載する必要がある。

⑤ 「ユーザー側に対する教育サービスの利用ができる」に関する記載上の留意すべき点

利用可能なユーザー側に対する教育サービスについて、利用するメリットや効果はもちろんのこと、利用料の有無や対象となるサービスの内容・範囲、中小企業に対して求められる対応や情報提供等を含め、申請時に記載する必要がある。

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」に関する記載上の留意すべき点

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について、悪用等の大分類に沿って、対応の考え方や技術的な手法を含めて、申請時に記載する必要がある。

悪用等の大分類の例を以下に示す。

〇個人情報や営業秘密情報の不正窃取に関わる悪用
〇プログラムの不正な追加や更新、削除に関わる悪用
〇なりすましやアクセス権限・管理権限の奪取に関わる悪用
〇その他の悪用

5.3. 中小企業における情報提供プラットフォームの活用方法の解説書

「3.2.2. 中小企業向け情報提供プラットフォームに関する仮説検証と考察」で前述した中小企業向け情報提供プラットフォームのあるべき姿等に関する方向性については、中小企業が当該プラットフォームを活用するうえで、当該プラットフォームに対する理解を得るために、また活用方法を決めるために必要となる基礎的な情報である。これらの基礎的な情報をユーザーにおけるプラットフォームの活用方法の解説書として提示する。

図表 5-1 中小企業向け情報提供プラットフォームのあるべき姿等に関する方向性

項目	あるべき姿として目指すべき方向性
意義・目的	○中小企業におけるサイバーセキュリティ製品・サービスの導入を支援し、ひいては中小企業におけるサイバーセキュリティ対策の課題解決に繋げることを、情報提供プラットフォーム構築・運用の意義・目的とする ○初期(立ち上げ時)においては、①インシデント発生時の迅速な初動対応、②重要な情報の安全な取扱い、③不正プログラム対策の３つに資する中小企業向けサイバーセキュリティ製品・サービスを対象範囲とし、中小企業におけるサイバーセキュリティ製品･サービスの導入を支援するものとする
運営者	○初期(立ち上げ時)の情報提供プラットフォームの運営者については、公的機関とすることが望ましい
情報の信頼性を担保するための手法・運用体制	○中小企業向け情報提供プラットフォームに掲載される情報については、登録申請者に対して、申請時に提供される情報の裏付けとなる定量的な情報の提出を追加的に求めることにより、信頼性、妥当性を担保するものとする ○申請時に提供される情報の信頼性、妥当性に関する裏付け確認は、情報提供プラットフォームの運営者が追加的に提出される定量的な情報をもとに行い、その確認結果を踏まえて評価会議が登録可否や掲載可否の評価・判断を行うものとする
登録の可否を判断するうえで提供を求める情報	○登録不可や掲載取り消しについて、情報提供プラットフォームの運営者または評価会議が明確に判断できるようにし、そのための対応ルールを策定するものとする ○情報提供プラットフォームに掲載される情報の情報源たる、登録申請者については、要件を明確にし、初期(立ち上げ時)においては、販売代理店・ディストリビュータを登録申請者の要件に含めないものとする

項目	あるべき姿として目指すべき方向性
	○登録の可否を判断するうえで、中小企業が重要視している、登録申請者の経営状態や事業継続性に関する情報についても、登録申請者に提供を求めるものとする
提供機能	○あくまで中小企業向けサイバーセキュリティ製品・サービスに対する中小企業の担当者の理解を増進するために資する情報の掲載を主軸とし、事業者間のマッチングや製品・サービス販売については実施しない方向とする
登録可否の判断や掲載可否の判断のルール	○登録可否の判断・評価の基準については、申請書に不備がなく、内容面もしっかりと記載されているか、カタログ等と照らし合わせてみた場合に虚偽の記載がないか、反社会的勢力に加担していないかなどの形式的なチェックにおいて判断し、必要に応じて申請書の内容を確認するためのヒアリングを実施するものとする ○掲載取り消しの判断・評価の基準については、登録申請者が重大なインシデントを起こした場合や廃業した場合に加えて、虚偽の記載が発覚した場合や、M&A 等により運営主体・体制や運営ポリシーに変更が生じた場合も含めるものとする
登録・掲載後、製品・サービスの内容に変更が生じた際に求める対応	○情報提供プラットフォームに掲載される情報は、あくまで時点評価に基づく参考情報であることから、登録申請者から申請された情報に基づくものであり、サイバーセキュリティ製品・サービスの性能・スペックを保証するものではないというエクスキューズを入れて掲載し、その情報を使うかどうかの判断は中小企業に委ねるものとする ○登録申請者に対して、サイバーセキュリティ製品・サービスの内容について、利用者側に影響のある変更が生じた場合には、情報提供プラットフォームの運営者に報告する義務を課すものとする
情報を探す際のインデックスの付け方	○情報提供プラットフォーム上で情報を探す際のインデックスの付け方については、従業員の規模や PC の台数、個人情報の取扱いの有無、年間のセキュリティ投資額等を参考としつつ、中小企業の意向を重視して設定し、必要となるサイバーセキュリティ製品・サービスを検索できるようにする

6. 本調査の総括

6.1. 中小企業向け情報提供プラットフォームを推進していくうえで必要となる取組

前述した導入実証による評価項目の有効性検証や、中小企業向け情報提供プラットフォームのあるべき姿等に関する「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」における議論の結果から見えてきた中小企業向け情報提供プラットフォームを推進していくうえで必要となる取組みとしては、以下の２点が挙げられる。

①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を用いた、情報提供プラットフォームの運営者または評価会議による検証・評価シミュレーションの実施
②中小企業向け情報提供プラットフォームの運営方法の更なる具体化に向けた検討

上記①については、登録申請者がサイバーセキュリティ製品・サービスに関する情報を申請する際に用いる、参考とすべき観点や記載項目・内容を評価項目として取りまとめ、その結果、実際に提供される情報の信頼性、妥当性を検証し、登録の可否や掲載の可否を評価・判断するにあたっては、評価項目を更に詳細にブレークダウンした評価基準を定めることが必要となることが分かった。

このため、各評価項目に沿った形で登録申請者に提出を求める情報については、当該検証・評価に係る作業を効率的に進められるように、提供情報の客観的な根拠になり得る定量的な情報を含め提供情報のあり方についての検討を深めるとともに、実際にそのような情報に基づき当該検証・評価に係る作業に関するシミュレーションを行い、その結果を踏まえて、判断の要素や検証・評価を行ううえでのポイント等を評価基準として取りまとめていく取組みが必要になると考えられる。

上記②については、本事業の実施期間上の制約から、本事業においては、中小企業向け情報提供プラットフォームのあるべき姿を中心として議論することとなり、意義・目的や運営者、情報の信頼性を担保するための手法・運用体制、提供機能、登録可否や掲載可否の判断のルールなどの方向性について取りまとめた。

次のステップとしては、中小企業は、売上高や従業員の規模や、業種、IT の利用状況・利用環境、商習慣、個人情報の取扱い状況、セキュリティ投資額などが多種多様であり、中小企業を一律に一括りにして扱うことが難しく、企業によって求められる情報の内容や提供方法も異なることから、中小企業向け情報提供プラットフォームにおいて、どのような中小企業にターゲットを絞り、どのような形で必要となる情報を提供していくかについて具体化していく取組みが必要である。

また、ターゲットとすべき中小企業が決まれば、次に中小企業向け情報提供プラットフォ

ームを持続可能な形で運営するための方法について具体化していく取組みが必要である。具体化に向けては、組織・体制や、対価や対価を払いたくなるような提供価値を含めた運営形態のあり方について検討し、そのうえで収支構造を検証するなど、中小企業向け情報提供プラットフォームの事業性・経済性に関するフィージビリティについて検証していく取組みが必要である。

6.2. 今後に向けた解決すべき課題

前述した「中小企業向けセキュリティ製品等の情報提供プラットフォーム検討委員会」における議論をもとにした中小企業向け情報提供プラットフォームのあるべき姿等の方向性の取りまとめだけでなく、中小企業からみた情報提供プラットフォームの提供価値に対するニーズやサイバーセキュリティ製品・サービス選びに必要となる情報、またセキュリティベンダーや販売代理店・ディストリビュータからみた情報提供プラットフォームの提供価値に対するニーズや期待されるサイバーセキュリティ製品・サービスに関する情報の掲載方法、情報提供にあたっての制約・課題等について、現場のより詳細な意見・ニーズの把握に努めるとともに、これらの結果を踏まえて、中小企業向けサイバーセキュリティ製品・サービスに関する評価項目や、中小企業向け情報提供プラットフォームの具体化に向けた検討を行うことが重要である。

また、中小企業向け情報提供プラットフォームの運営方法については、運営者の候補として想定される事業者・団体や、サイバーセキュリティや中小企業支援に関係する政府機関などのさまざまな意見を聴取しつつ、経済産業省が実施する「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」等の本事業と関連性のある事業との連携の可能性を含めて、視野を広げて具体化に向けた検討を行うことが重要である。