IPA Better Life with IT

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（概要版）

2020年4月

独立行政法人情報処理推進機構

セキュリティセンター

調査の目的

IPA

中小企業のセキュリティ対策水準の向上には、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る**具体的対策の実践を促す**ことが有効

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か、どのような製品・サービスを導入することが効果的か等の**判断は困難**

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ことを目的に、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構築に向けた**実現可能性調査を実施**

調査の概要

IPA

● 調査の構成

有識者による委員会の設置、運営のもと下記を実施

- 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

● 中小企業ユーザーへの導入実証

- 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
- 製品・サービス提供事業者から中小企業ユーザー候補の提出を受け選定し導入実証実施

● 評価項目の有効性検証

- 中小企業向け製品・サービスに関する評価項目について調査仮説を構築
- 中小企業ユーザーに対し、調査仮説をもとに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実施
- 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。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実施
- 有識者委員会でこれらの調査結果をもとに議論し評価項目を再構成

● 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

- 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
- 類似分野の国内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。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検討すべき論点を抽出し整理
- 有識者委員会において、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
- 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

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

- 中小企業が製品・サービスを選ぶ際に参考となる評価項目を策定し、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、「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・開催

【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

【開催経緯】

会合	開催日	審議事項
第１回会合	2019年10月8日（火）	・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）	・評価項目の検証に関する現状報告について ・発注元が、契約先およ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）	・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

製品・サービス提供事業者

- 5社の応募があり、「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」での審査を経て、３社を採択。

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（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」

検証参加中小企業ユーザーの概要

	事業内容	資本金	従業員数
A社（製造業）	バイオ燃料、化学品の製造など	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、省力化機械部品加工、LED機器	1,000万円	15名
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
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

eGIS

NTTコミュニケーションズ

Blue Planet-works

情報提供プラットフォームの検討に関する具体的な作業方針・手順について

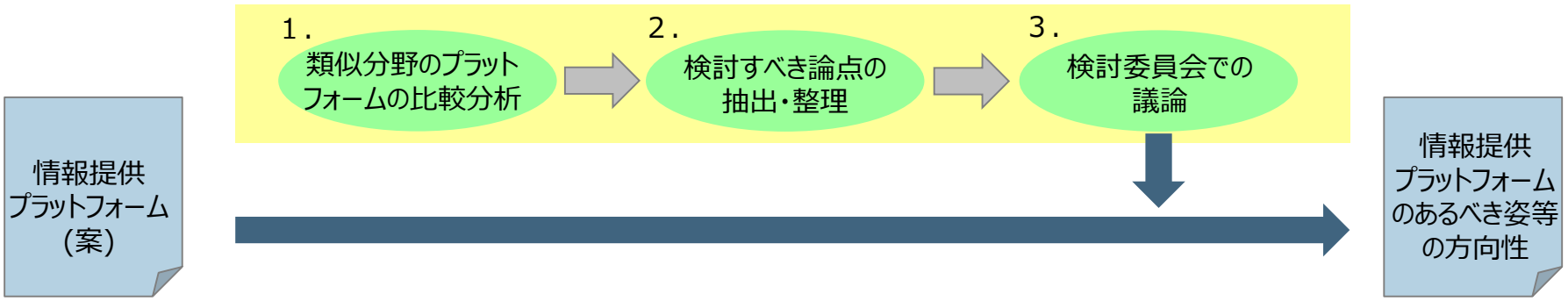
- 中小企業向けセキュリティ製品等に関する情報提供プラットフォームの検討にあたっては、類似分野における国内の既存の情報提供プラットフォームとの比較分析を行いながら、以下のような方針・手順で検討。

<情報提供プラットフォームの検討手順>

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との比較分析

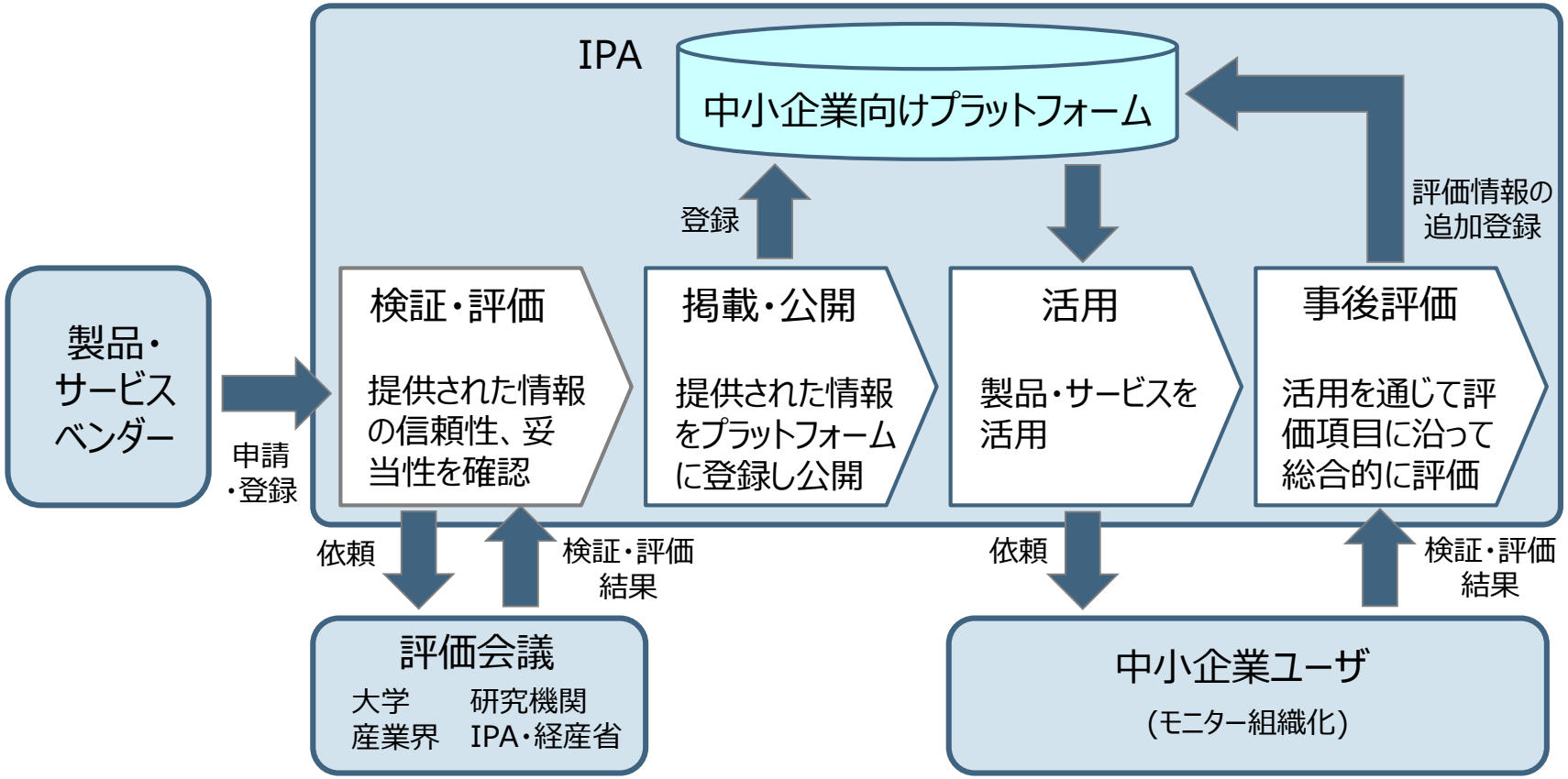
2．情報提供プラットフォームのあるべき姿および必要となる機能についての検討すべき論点の抽出・整理

3．検討委員会での議論にあわせて、あるべき姿および必要となる機能の取りまとめ



中小企業向けセキュリティ製品等に関する情報提供プラットフォーム（案）

- 評価項目に沿った評価や提供された情報の信頼性、妥当性の確認をすべて申請時・登録時に実施しようとすると、コスト面、労力面の負荷が大きくなるため、事後評価を上手く活用することが重要。



評価項目の策定に向けた具体的な作業方針・手順について

IPA

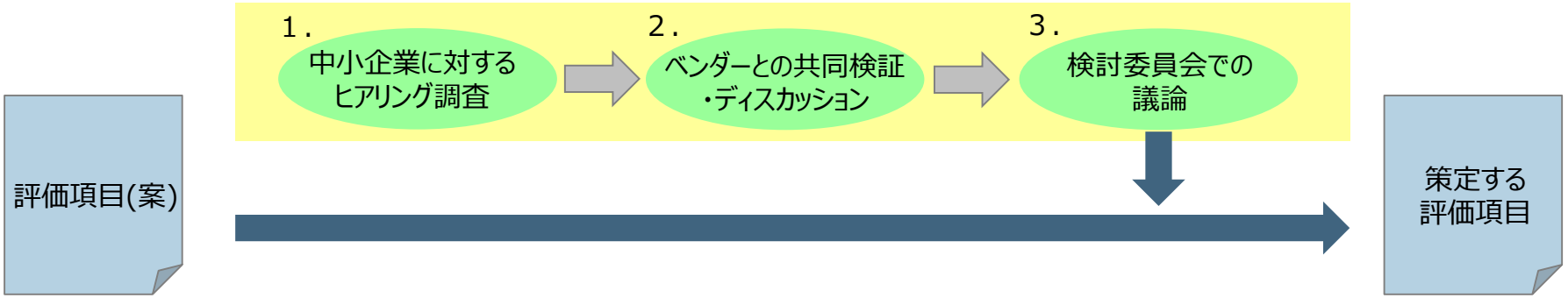
- 中小企業ユーザにおいて、セキュリティ製品・サービスの導入実証を行いながら、以下のような方針・手順で評価項目を策定。

＜評価項目の策定手順＞

1．中小企業ユーザにおけるセキュリティ製品・サービスの評価に関するヒアリング調査

2．ヒアリング結果を基にした、製品・サービスベンダーとの共同検証および必要な評価項目のピックアップのためのディスカッション

3．検討委員会での議論にあわせて、必要となる評価項目を再構成



中小企業向けセキュリティ製品・サービスに関する評価項目（案）

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

※本調査では、セキュリティ製品・サービスに対する技術面の検証を行わないため、「７　製品・サービスのセキュリティ性能」を評価項目に含めるかどうかは要検討

類似分野における国内の既存情報提供プラットフォーム調査

- 国内情報提供プラットフォームとの比較分析をもとに、本事業の情報提供プラットフォームのあるべき姿について議論

類似分野における国内の情報提供プラットフォーム一覧

運営者		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

情報提供プラットフォームの比較①

IPA

整理項目		新技術情報提供システム（NETIS）	J-LIS LGWAN-ASP サービスリスト	中小企業ワールドビジネスサポート（SWBS）	ここからアプリ	JNSAソリューションガイド	「テレワーク」を始めてみませんか？
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の支援	地方公共団体間のIT化格差、IT活用格差等の軽減、IT化の促進のための支援	海外進出を視野に入れる企業の海外進出計画の立案などのファーストステップの支援	中小企業・小規模事業者の生産性向上をアプリ導入で実現するための支援	セキュリティ対策の課題を解決するための支援	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
方向性	運営者	国土交通省	地方公共団体情報システム機構	中小企業基盤整備機構	中小企業基盤整備機構	日本ネットワークセキュリティ協会	テレワーク導入推進コンソーシアム
	利用者	関係府省、地方自治体、公共工事等に係る事業者	地方自治体（LGWAN接続団体）、IT・通信サービス事業者	海外進出、もしくは海外進出支援を希望する企業および団体	生産性向上の実現に向けて、困りごとを抱える中小企業	中小企業	テレワーク導入を検討している企業・団体
	提供情報	従来技術との比較による、「経済性」「工程」「品質・出来形」「安全性」「施工性」「環境」の６項目の観点からの５段階評価情報	サービス分類、概要、URL、提供者名、問い合わせ先、LGWANとの接続時期といったサービス情報	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、問い合わせ窓口、支援フローといったサービス情報	関連キーワード、概要、メーカーHP、製品画像、製品情報（アプリ名、事業者名、初期導入コスト、ランニングコスト、無料使用期間の有無、導入実績等）といったアプリ情報	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	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
	適用条件	新技術提供者において、産・学・官からの事前審査と、利用者からの事後評価を受けること	「総合行政ネットワークASP登録及び接続資格審査要領」にて審査を受けること	中小企業基盤整備機構の事務局にて審査を受けること	中小企業基盤整備機構の事務局にて審査を受けること	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、審査・評価はなし	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、審査・評価はなし

情報提供プラットフォームの比較②

IPA

整理項目		新技術情報提供システム（NETIS）	J-LIS LGWAN-ASP サービスリスト	中小企業ワールドビジネスサポート（SWBS）	ここからアプリ	JNSAソリューションガイド	「テレワーク」を始めてみませんか？
利用者にとってのメリット		新技術の活用が可能	標準的で経済的なシステム導入・運用が可能	海外進出の悩み解決や一次情報収集が可能	生産性向上の実現が可能	セキュリティ対策の課題解決が可能	テレワークの迅速・効率的な導入が可能
提供機能	情報共有・情報比較	情報収集と共有化、直轄工事等での試行およ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、その中でプラットフォームは情報の収集と共有化の部分を担う	審査条件を満たしているサービスの情報の共有	審査条件を満たしているサービスの情報の共有	審査条件を満たしているアプリの情報の共有	会員企業が取り扱う製品・サービス、イベント、セミナーの情報の共有	会員企業が取り扱う製品の情報の共有
	その他		事業者マッチングやサービス販売など、その他の機能は特になし	掲示板を提供し、サイト訪問者からの質問に答えたり、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	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	事業者マッチングや製品・サービス販売など、その他の機能は特になし	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
運営形態		産・学・官で構成される新技術活用評価会議にて審査	地方公共団体情報システム機構にて運営	中小企業基盤整備機構にて運営	中小企業基盤整備機構にて運営	日本ネットワークセキュリティ協会にて運営	テレワーク導入推進コンソーシアムにて運営
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）はなし	サービス利用料はなし、登録料は別途個別契約との記載があるため有償と思料	サービス利用料（情報閲覧料）、登録料（掲載料）はなし	サービス利用料（情報閲覧料）、登録料（掲載料）はなし	サービス利用料（情報閲覧料）、登録料（掲載料）はなし なお、会員企業の会費にて運営	サービス利用料（情報閲覧料）、登録料（掲載料）はなし なお、会員企業の会費又は販売手数料にて運営と思料

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

- 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、以下に示す８つの検討すべき論点を抽出。

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

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①

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

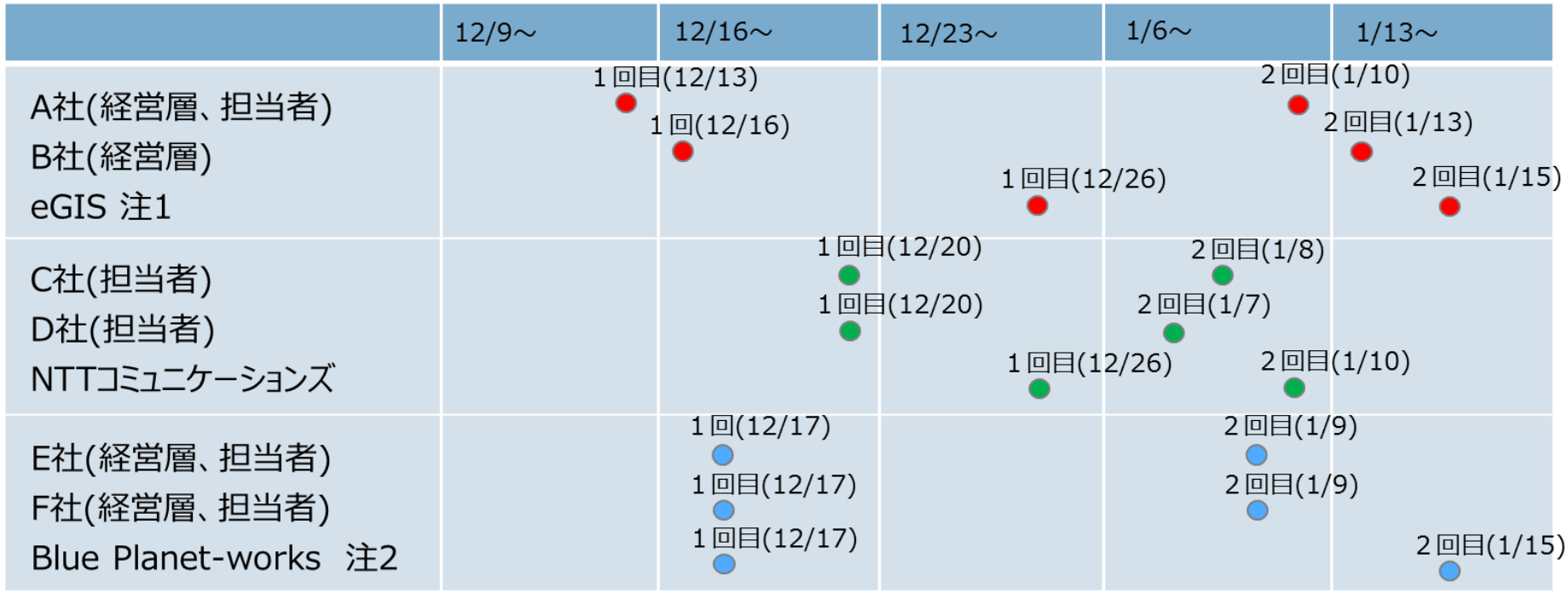
中小企業向け情報提供プラットフォームのあるべき姿等に関する方向性②

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 ○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の増進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

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③

項目	あるべき姿として目指すべき方向性
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

評価項目の検証ヒアリング



注1：eGISのディストリビュータとして、東京システムリサーチ、ラックも参加

注2：Blue Planet-worksのディストリビュータとして、大興電子通信も参加

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『１　導入のし易さ』に対するヒアリングを通して得られた意見・評価

IPA

- 「お試し利用の充実」、「PCのシステムパフォーマンスの低下回避」、「使えるようになるまでの伴走型サポート」などについて、評価項目に盛り込む必要がないか

詳細な評価項目		重視度合い	考察
1.1	大規模なシステム改修を伴わず実装が容易である	かなり重視　2 ある程度重視　4	● 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 ● 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が必要になることも避けたいと考えている
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	かなり重視　1 ある程度重視　5	● 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、お試し利用をより一層充実してほしいと考えている ● 自社でセキュリティ設計を行ったり、必要な機能・製品を選んだりすることは困難であるため、利用状況・利用環境に照らして、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 ● 機能のオーバースペックはもちろんのこと、正規の機能を実装していたとしても、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
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	かなり重視　1 ある程度重視　4 あまり重視されない　1	● 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 ● 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

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『２　運用のし易さ』に対するヒアリングを通して得られた意見・評価

IPA

- 「インシデント発生時における必要となる対応の道筋の提示」、「トラブルシューティングやQ＆Aの充実」などについて、評価項目に盛り込む必要がないか

詳細な評価項目		重視度合い	考察
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	かなり重視　2 ある程度重視　4	● 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 ● 担当者は兼務でセキュリティも管理しているため、運用・メンテナンスが担当者の手を離れることはよいと考えている
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	【インシデント対応】 かなり重視　0 ある程度重視　6 【勤務時間外の対応】 かなり重視　0 あまり重視されない　5 全く重視されない　1	【インシデント対応】 ● 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 【勤務時間外の対応】 ● 対応のしようがないため、勤務時間外の対応について考える必要がない、勤務時間外の対応は避けたいと考えている
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	かなり重視　2 ある程度重視　4	● 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速いに越したことはないと考えている ● 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Q&A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

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『3　導入や運用を行うことで得られる効果』に対するヒアリングを通して得られた意見・評価

IPA

- 「PCの安定的な稼動への影響回避」、「製品・サービス側の知識の習得」などについて、評価項目に盛り込む必要がないか

	詳細な評価項目	重視度合い	考察
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	かなり重視　5 あまり重視されない　1	● 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 ● 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(定額でサービス提供)にしてほしいと考えている
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	かなり重視　1 ある程度重視　4 あまり重視されない　1	● セキュリティ側の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・サービス側の知識やシステム側の知識を身につけたいと考えている ● コストを掛けて学習しないといけないような製品は敬遠したいと考えている

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『４　導入時や運用時に要する費用』に対するヒアリングを通して得られた意見・評価

IPA

- 「想定される損失額やセキュリティ運用のトータル費用との費用見合い」、「サイバー保険によるインシデント対応に係る費用のカバー」などについて、評価項目に盛り込む必要がないか

	詳細な評価項目	重視度合い	考察
4.1	導入コストが安価である	かなり重視　6	● 導入コストが高いと、検討の俎上に載らないと考えている ● 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、何らかの費用的なメリットが必要であると考えている
4.2	運用コストが安価である	かなり重視　5 ある程度重視　1	● 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 ● 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

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『5　導入や運用における課題の開設』に対するヒアリングを通して得られた意見・評価

IPA

- 「企業への導入実績や、脅威の検知・駆除実績、市場シェアなどの参考情報の提供」、「リスク評価やコンサルティングとのサービス一体化」などについて、評価項目に盛り込む必要がないか

	詳細な評価項目	重視度合い	考察
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	かなり重視　5 ある程度重視　1	● 企業への導入実績や、脅威の検知・駆除実績、市場シェアなどの参考情報をパンフレットやカタログに掲載してほしいと考えている ● 多くの企業やPCに導入されているものであれば、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も安心であると考えている ● 経営者は、製品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

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『6　製品・サービスの経営へのインパクト』に対するヒアリングを通して得られた意見・評価

IPA

- 「パッケージ化の形態」などについて、評価項目に盛り込む必要がないか

詳細な評価項目		重視度合い	考察
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	かなり重視　5 ある程度重視　1	● 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
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	かなり重視　0 ある程度重視　3 あまり重視されない　3	● 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
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	かなり重視　5 あまり重視されない　1	● 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 ● 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 ● 個人情報保護対策を求める取引先等に製品・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

中小企業向けセキュリティ製品・サービスに関する評価項目（案）
『7　製品・サービスのセキュリティ性能』に対するヒアリングを通して得られた意見・評価

IPA

- 「ユーザ教育とのサービス一体化」、「人為的なミスへの対応」、「悪用防止を考えた製品・サービス設計」などについて、評価項目に盛り込む必要がないか

	詳細な評価項目	重視度合い	考察
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	かなり重視　4 ある程度重視　3 あまり重視されない　2 ※ 本項目ではセキュリティ機能ごとに評価が分かれたため回答数の合計が6を超える	● 直近のサイバー攻撃など、世の中で騒がれている脅威に、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を増やせば、カバーすべき脅威も広がり、アプリケーションを使う人の教育とセットで考えないといけないと考えている
7.2	未知の脅威・インシデントへの対応が可能である	かなり重視　6	● 未知の脅威としては、新種のサイバー攻撃やゼロデイ攻撃のようなものだけでなく、想定していない人為的なミスや内部不正も含め、対応できることが必要であると考えている
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	かなり重視　2 ある程度重視　1 あまり重視されない　3	● 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る、PC内の情報を消すことができるということは避けたいと考えている ● セキュリティベンダー側が悪用防止を考えたサービスの作りにしていることや、そのために使い勝手を犠牲にしていることについて気付きにくいと考えている

中小企業向けセキュリティ製品・サービスに関する評価項目の見直し案

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
		1.4	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
		1.5	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
		1.6	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	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	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
		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
		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
		3.3	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	4.1	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
		4.2	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
		4.3	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	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(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
		5.2	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	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	新種のサイバー攻撃やゼロデイ攻撃のみならず、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
		7.3	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
		7.4	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

検討委員会における議論を通して得られた意見

- 「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、出来る限り「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、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案について、構成や表現方法を大幅に変更することとなった。

中小企業向けセキュリティ製品・サービスに関する評価項目の最終版

評価項目の観点		詳細な評価項目	
1	導入のし易さ	1.1	大規模なシステム改修の必要性がない
		1.2	必要となる機能を自由に選択することができる
		1.3	インストールや設定の手間を省くことができる
		1.4	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
		1.5	PCのシステムパフォーマンスへの影響が最小限である
		1.6	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
		1.7	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
		1.8	導入に関してのサポート対応がある
2	運用のし易さ	2.1	運用に関しての専門的な知識が必要ない
		2.2	さまざまな状況に応じたサポートツールがある
		2.3	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	3.1	導入コストが安価である
		3.2	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	4.1	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	5.1	既知の脅威・インシデントに対応することができる
		5.2	未知の脅威・インシデントに対応することができる
		5.3	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	6.1	サイバー保険等の補償サービスの利用ができる
		6.2	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
		6.3	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
		6.4	勤務時間外対応のサポートサービスの利用ができる
		6.5	ユーザ側に対する教育サービスの利用ができる
		6.6	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

中小企業に広く訴求するためのコンテンツ

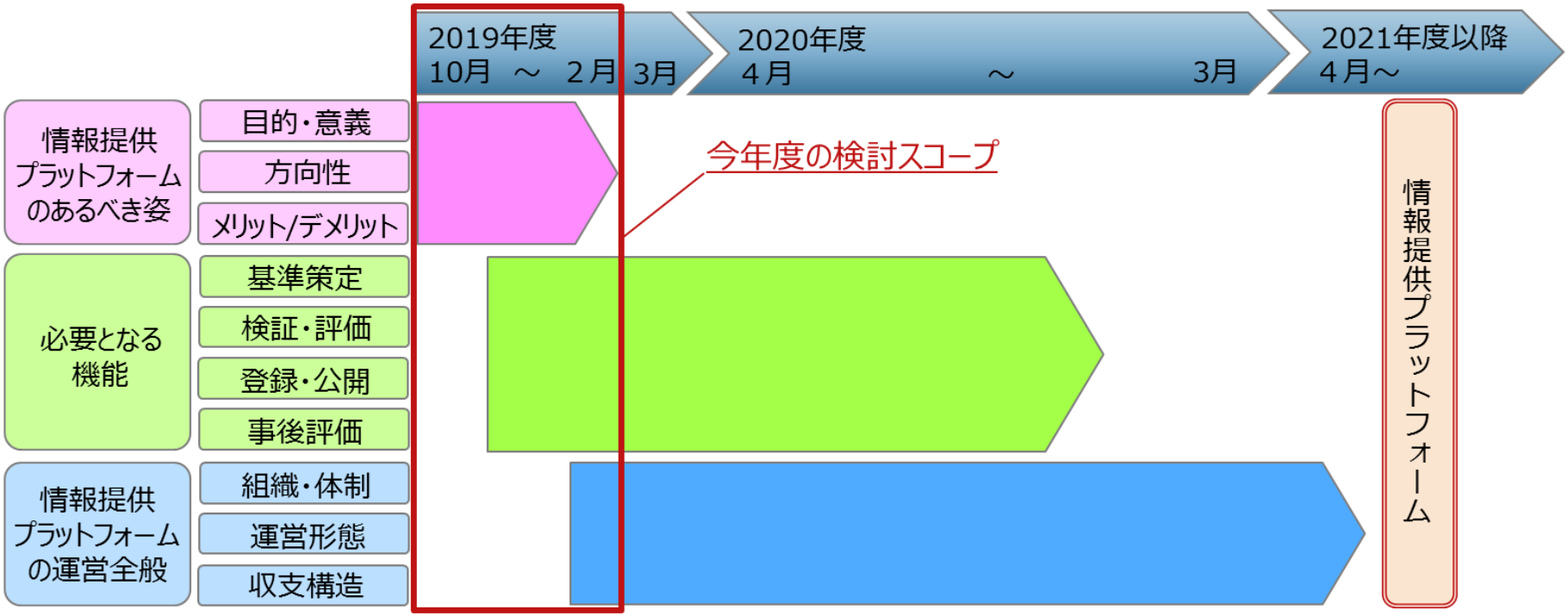
IPA

- 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」、「中小企業ユーザ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。

コンテンツの種類	コンテンツの概要
評価項目の定義・解説書	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。
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。
中小企業ユーザ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	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。

情報提供プラットフォーム構築に向けたスコープ（案）

- 中小企業向けセキュリティ製品等に関する情報提供プラットフォームについては、①目的・意義や、利用者、提供情報等の方向性、メリット/デメリットといったあるべき姿に関する議論と、②基準策定、検証・評価、登録・公開等の必要となる機能に関する議論、③組織・体制や、運営形態等の運営全般に関する議論。
- 必要となる機能と運営全般に関する検討すべき事項については、来年度の継続的な検討事項として整理。



情報提供プラットフォームを推進していくうえでの必要となる取組

【必要となる取組】

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

〇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、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ていく取組が必要

〇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が必要

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

〇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が必要

〇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が必要

〇組織・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が必要

今後に向けた解決すべき課題

IPA

【解決すべき課題】

①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

②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、「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