令和２年度中小企業サイバーセキュリティ対策支援体制構築事業

（サイバーセキュリティお助け隊事業）

（実証対象：愛知県、岐阜県、三重県）

成果報告書

請負事業者：名古屋商工会議所

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

目次

1. サマリー

本報告書は、名古屋商工会議所が「令和２年度中小企業サイバーセキュリティ対策支援体制構築事業」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

愛知県、岐阜県、三重県内の中小企業 140 社を対象に、以下のサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- 簡易セキュリティアセスメント
- エンドポイントに関するセキュリティ対策（Defender 監視）
- エンドポイントに関するセキュリティ対策（Web 対策ツール）
- エンドポイントに関するセキュリティ対策（Web 対策ツール）
- ネットワークに関するセキュリティ対策（UTM 導入）

2. 背景・目的

2.1 背景

近年、サプライチェーン全体の中で対策が弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化してきている。具体的には、令和元年 7 月に大阪商工会議所より公表された調査結果によると、30 社の中小企業を調査したところ、30 社全てでサイバー攻撃を受けていたことを示す不審な通信が記録されていた。また、同会議所が同年 5 月に公表した調査では、大企業・中堅企業 118 社に「取引先がサイバー攻撃被害を受け、影響が自社に及んだ経験があるか」を調査したところ、25%の企業が経験ありと回答した。

多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも多く発生している。また、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く、IT に関するトラブルが発生した際にシステムの不具合が原因なのか、サイバー攻撃が原因であるか自社で判断することは困難である。

このような実態から、トラブル時に相談できる窓口や、サイバー攻撃に遭った際に事後対応を支援するサービス（事後対策支援）を提供する体制構築を目指し、令和元年度に全国 8 地域で「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」（以下「サイバーセキュリティお助け隊事業」という。）を実施したところ、1,064 社の中小企業が参加し実証に取り組んだ結果、延べ 128 件のインシデント対応支援が発生し、そのうち 18 件の駆け付け支援を実施した。しかしながら、令和元年度のサイバーセキュリティお助け隊事業では、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難であり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、事後対策だけでなく事前対策も必要とする中小企業も多いこと、サービス購入費用が中小企業にとって許容可能な価格である必要があること等が明らかになり、現状は、中小企業への意識喚起が不十分であるとともに、中小企業のニーズに合った製品、サービスが提供されてない状況であることが確認された。

そのため、上述のような中小企業の実態・ニーズを踏まえ、損害保険会社、IT ベンダー、地元の

団体等が連携して中小企業セキュリティ対策支援体制を構築し、中小企業の実態やニーズをよりきめ細かく把握することで、その実態に即したサービス内容やこれに必要な人材、体制等を明らかにし、中小企業の実態やニーズに合致した持続可能なセキュリティ対策支援体制を構築することで、中小企業のセキュリティ対策強化を図る必要がある。

2.2 目的

本実証事業の実施を通じて、中小企業におけるサイバーセキュリティの意識向上を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を定着させて行くことを目的とする。

3. 実証事業の概要

3.1 実証対象の選定

本実証事業では中小・小規模事業者が継続利用しやすい価格帯のサービスとするため、駆け付けサポート等の現地サービスは、名古屋中小企業 IT 化推進コンソーシアムである Pit-Nagoya 会員の地域 IT ベンダーによるサービス提供とする。そのため地域 IT ベンダーが駆け付け等対応可能なエリアである東海 3 県（愛知、岐阜、三重）を実証対象地域として選定した。

図 3.1 名古屋からの駆け付け範囲

【名古屋中小企業 IT 化推進コンソーシアム（Pit-Nagoya）について】

名古屋商工会議所では令和元年 10 月に、地域の中小企業の IT 化推進を支援することで地域経済の持続的な成長へと繋げることを目的に、地域 IT ベンダーを会員とし日立システムズおよび NTT 西日本を運営事務局とした、『名古屋中小企業 IT 化推進コンソーシアム（Pit-Nagoya）』を立ち上げた。Pit-Nagoya では中小企業の IT 化を推進する上で、サイバーセキュリティ対策は最重要課題であると捉えており、重点取り組みテーマとして活動している。

本実証事業では名古屋商工会議所を中心に、Pit-Nagoya 事務局を担う日立システムズおよび NTT 西日本、会員である地域 IT ベンダーの協力により、コンソーシアム全体で実証事業を実施した。

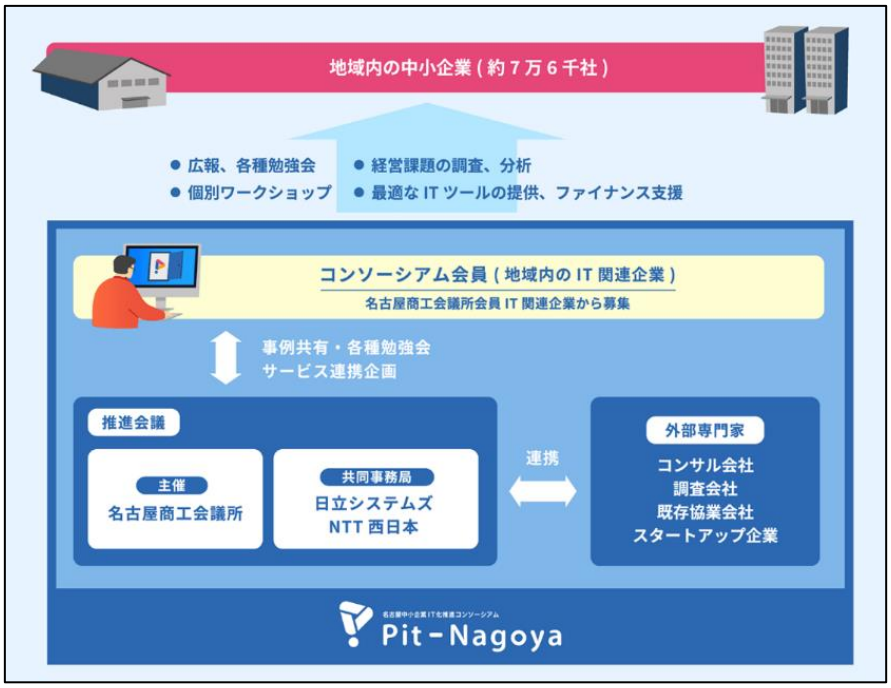

図 3.2 Pit-Nagoya 概要

東海３県には各種製造業の集積が存在しており、名古屋地域の企業は製造業等の基盤を活かし、域内外を結ぶサプライチェーンを形成している。更に東海 3 県は産業集積や整備されたインフラがあるポテンシャルのある地域であり、これを支える中小企業の発展を支援する必要がある。

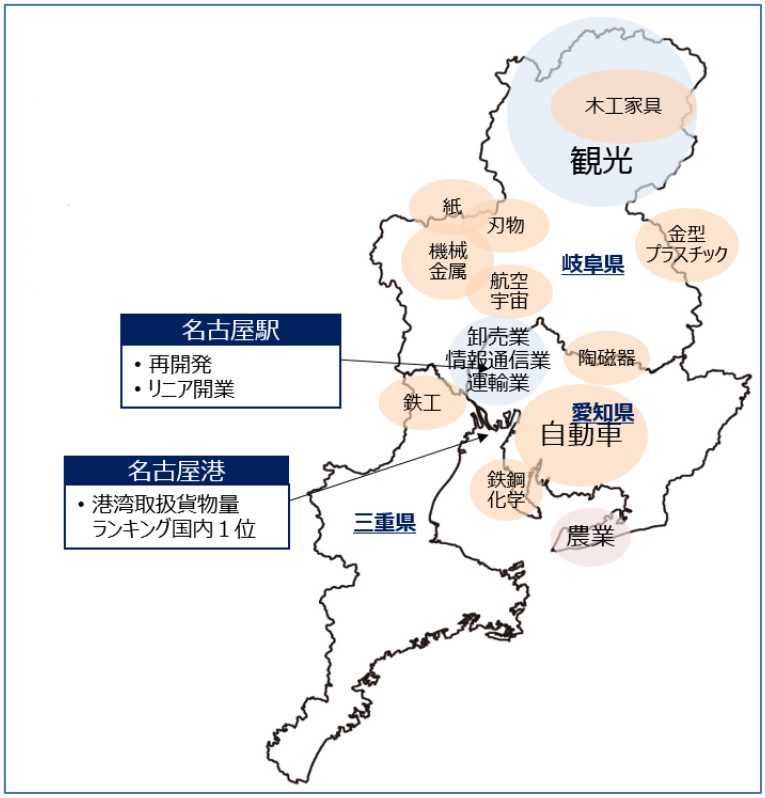

図 3.3 地域選定における東海３県

名古屋商工会議所が会員企業に対して行ったアンケートによると、情報セキュリティ対策（予防対策）は、「ウイルス対策ソフトを導入している」が最も多く 895 社（89%）の一方で、「ウイルス対策ソフトを含め OS やソフトウェアは常に最新の状態にしている」は 498 社（50%）にとどまる。情報セキュリティ対策（事故対策）は、「情報管理責任者を配置している」が最も多く 525 社（52%）、次いで「情報漏えい等発生時の対策支援先や相談先を把握している」が 324 社（32%）、未回答が 224 社（22%）であり「何もしていない」が多かったものと推察される。

※調査対象：名古屋商工会議所会員企業 7,000 社　回答数 1,006 社（回収率 14.3%）

【セキュリティまで十分に手が届かない理由（仮説）】

東海３県における基幹産業（産業機械、素材等のもの作り）を構成する中小企業では、取引先の経営変化に伴い IT 投資を十分に確保できるほど利益率が確保できていないケースが多いと想定している。その結果、IT 投資は業務効率化がわかりやすい生産系システムなどの基幹系、事務系へ投資が

多くなりやすく、セキュリティ面への投資が後回しになりやすい。こうした背景の中で、社長、従業員のセキュリティに対する意識が高まらず、セキュリティ面への対策がおざなりになりがちである。

更に、昨今導入が進む IoT ツールに関しては、ほぼ無防備な状況になりがちになっている。今後はコロナ禍で進展したテレワークへの IT 投資も増加しておりセキュリティ対策の幅が広がる一方でセキュリティ対策への投資は据え置きとなり、結果的に薄いセキュリティ対策となってしまうことが懸念される。

本実証事業ではこれらの仮説を踏まえて、詳細な実態を把握し課題解決策を明確化した。そのために、ヒアリング・地域実証は東海 3 県の商工会議所が連携して実施することにより多くの会社と連携し、説明会などを通して危機意識を醸成することで、円滑で効果の高い活動を推進した。

3.2 スケジュール

作業スケジュール（計画時）について、実証事業項目毎の工程と実施事項を以下に記載する。

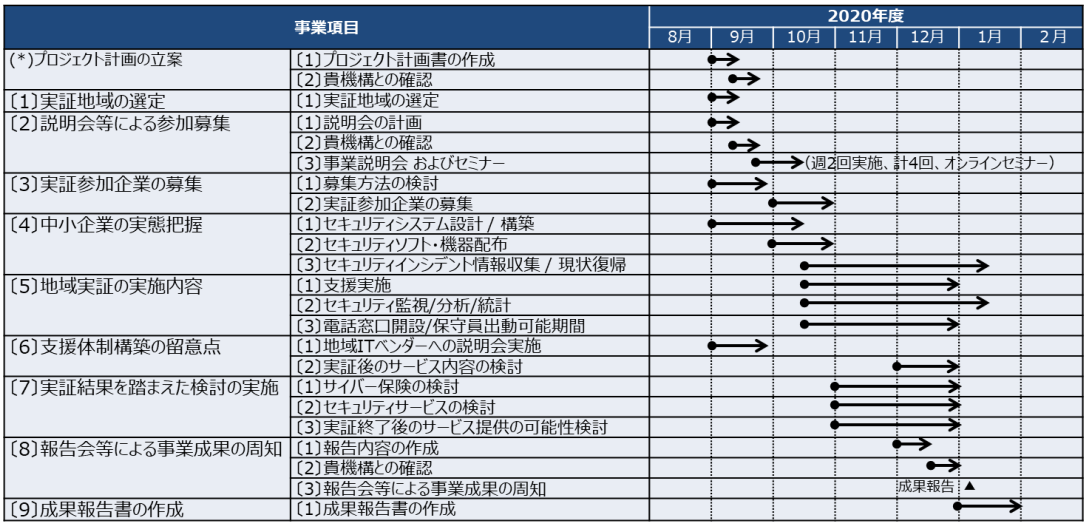

図 3.4 作業スケジュール

本実証事業の実施スケジュールの各項目について以下に示す。

3.2.1 実証地域の選定

本実証事業では中小・小規模事業者が継続利用しやすい価格帯のサービスとするため、駆け付けサポート等の現地サービスは、Pit-Nagoya 会員の地域 IT ベンダーによるサービス提供とする。そのた

め地域 IT ベンダーが駆け付け等対応可能なエリアについて実証対象地域として選定した。

3.2.2 説明会等による参加募集

昨今の事情を鑑み、事業説明会の形式としてはインターネットを利用したオンライン形式にて実施した。なお、オンライン形式とすることで参加者の移動時間や移動費用を抑えられるとともに、都市部以外の中小企業の参加も見込んだ。実証事業の対象である地域の中小企業へ向けて、本実証事業の周知および参加呼びかけを行うことを目的とし、更に、当該説明会の参加者に対しサイバーセキュリティに関する普及啓発を行い、中小企業のセキュリティ対策に関する意識向上を図った。

聴講した中小企業にはオンラインにて簡易セキュリティアセスメントに回答してもらい、個別にセキュリティアセスメントシートの分析結果を提供することにより、現状のセキュリティリスクや中小企業の実態を可視化させ、サイバーセキュリティ対策の意識向上を図った。

実施日：9 月に 1 回、10 月に 3 回の計 4 回の実施を計画。また、参加申込企業数が目標数に届かない場合は、事業説明会の実施回数の増を検討することとした。

3.2.3 実証参加企業の募集

実証期間が 3 か月と短いことを考慮し、100 社（そのうち、実証ツール導入による検証：50 社）の実証参加企業を募った。名古屋商工会議所会員企業の小規模事業者を含む中小企業を中心に、地域の有力企業のサプライチェーンや重要インフラを保有する企業層をターゲットとし、下記の施策を中心に実証参加を訴求した。

- 名古屋商工会議所ホームページでの事業説明会開催を広報、実証参加をアピール
- Pit－Nagoya 参画企業の取引がある、サプライチェーンへの参加の案内
- 地域コミュニティ団体経由で実証地域の企業へ参加案内を実施
- 損保会社による地場のお客様を経由した実証参加案内を実施

3.2.4 中小企業の実態把握

事業説明会申込時の事前アンケートおよび事業説明会でのオンラインによる簡易セキュリティア

セスメント実施により、詳細なセキュリティ実態情報を効果的に収集した。また現場への機器導入等によるセキュリティインシデントの情報収集のためのセキュリティ監視サービスを客先に導入することで、継続した情報（セキュリティインシデントの実態）の収集を行った。

3.2.5 地域実証の実施内容

2020 年 9 月中旬（説明会実施）~2021 年 1 月中旬（報告会実施）までの期間を実証期間とした。

- 名古屋商工会議所および中部経済産業局、損保会社等を含めた地域コミュニティを活用し、中小企業を中心に 100 社（そのうち、実証ツール導入よる検証は 50 社）を目標として募集した。
- IT リテラシーが低い中小企業でもできるセキュリティ対策（下記）を導入した。

① エンドポイントに関するセキュリティ対策製品（Defender 監視ツール）の導入

② Web アクセスに関するセキュリティ対策製品（i-FILTER　Agent 版）の導入

③ メール受信に関するセキュリティ対策製品（i-FILTER　Agent 版）の導入

④ ネットワークに関するセキュリティ対策製品（UTM）の導入

3.2.6 支援体制構築の留意点

本実証では地域 IT ベンダーの協力が不可欠だが、その際の情報共有の手段について考慮する必要があった。そのため顧客情報やインシデント対応情報は、クラウド上の情報連携ツールを利用することで、支援体制間の迅速な情報共有を図った。

3.2.7 実証結果を踏まえた検討の実施

実証を通じた実態把握のデータより中小企業の保険加入（活用）の促進策の方向性を「商品開発（最適な保険料水準と補償範囲､金額)」と「環境整備（加入するモチベーション)」の 2 軸で整理し、保険サービスメニューのレベル分けなども含め、中小企業が利用しやすいサイバー保険の検討を実施した。主な検討項目は下記の 2 つ。

- 「簡易セキュリティアセスメント、アンケート」ならびに、実証事業の収集データより中小企業のセキュリティ対応サービスの内容、各種サービスメニューのレベル分け

・ 実証終了後の実サービスを見据えて、本実証事業で使用する機器・サービス等の選定・利用を行うことで、中小企業へのサイバーセキュリティ対策のサービス内容理解促進および安価なサービス提供の実現

また、東京海上日動では既存でサイバー保険に加入している顧客（愛知県下：100 社）や代理店ネットワーク（愛知県下：250 店の代理店）が存在しており、そのチャネルを活用して保険を案内する。

3.2.8 報告会等による実証事業成果の周知

報告会は 1 月中旬に 1 回実施した。新型コロナウイルス感染予防の観点から、オンライン形式とした。報告会内容は以下のとおり。

- 事業説明会の開催結果
- 地域実証の実施結果報告
  - 実証参加企業数
  - 継続的なサービス展開に繋げるための具体的な取り組み
  - 中小企業の実態やニーズに応じた必要なセキュリティ対策サービスの内容
- 実証結果を踏まえた検討結果
  - 今後中小企業に有効と思われるセキュリティ対策サービス
  - 中小企業が利用しやすいサイバー保険のあり方

3.2.9 成果報告書の作成

上記 1-8 の実施結果を踏まえ、下記について報告する。

- 事業説明会の開催結果記載（実施計画における結果）
  - 実施回数、参加企業数、アンケート内容・結果等
- 事業説明会での施策である「簡易セキュリティアセスメント、アンケート」ならびに実証事業の収集データより中小企業のセキュリティ対応サービスの内容を整理
- サイバーセキュリティ事後対応支援体制の構築結果報告
- 地域実証の実施結果報告
  - 実証参加企業数、継続的なサービス展開に繋げるための具体的な取り組み、中小企業の実

態やニーズに応じた必要なセキュリティ対策サービスの内容等

- 検討結果記載
  - 中小企業が利用しやすいサイバー保険のあり方、実証終了後のサービス提供の可能性等

3.3 実証参加企業

3.3.1 募集方法

名古屋商工会議所からのメールマガジン会員への広報、チラシ配布、Fax 送信、Pit-Nagoya 協賛企業の顧客への電話、訪問による声がけも併せて実施した。以下に事業説明会および実証参加における募集手段を記載する。

表 3.1 実証参加企業募集方法一覧

案内方法	案内数	参加社数
チラシ配布	2,000	140 社
メールマガジン配信	11,000	
Fax 送信	3,500	
個別訪問	135	
その他	200	
合計	16,835	

3.3.2 実証参加企業

本実証では合計 140 社の中小企業が実証事業に参加した。多くの中小企業はセキュリティ対策の意識が低いという状況の中、また、コロナ禍という世界的に未曾有な状況下において、多くの企業から実証参加協力を得られたことは幸甚である。本実証事業では「金融・保険業」「卸売・小売業」「製造業」の 3 業種が実証参加企業の中でも多くを占めていることがわかった。また従業員数が 10 人以下の企業が 6 割以上を占めていることがわかった。業種別および従業員数別の実証参加企業数内訳について以下に示す。

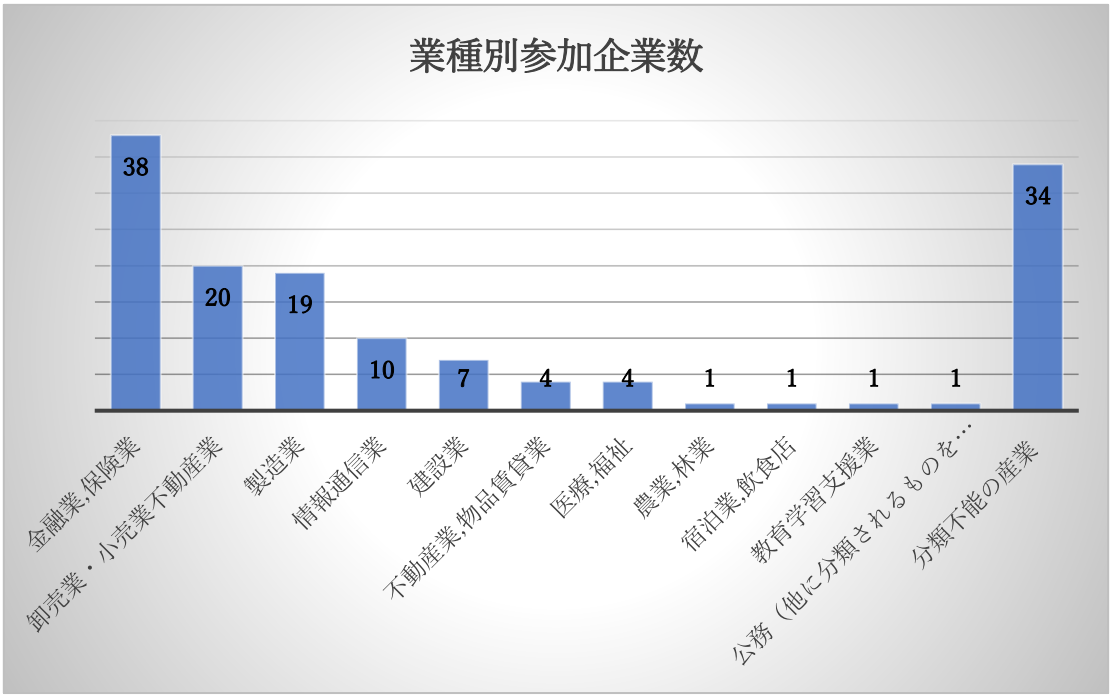

図 3.5 業種別参加企業数

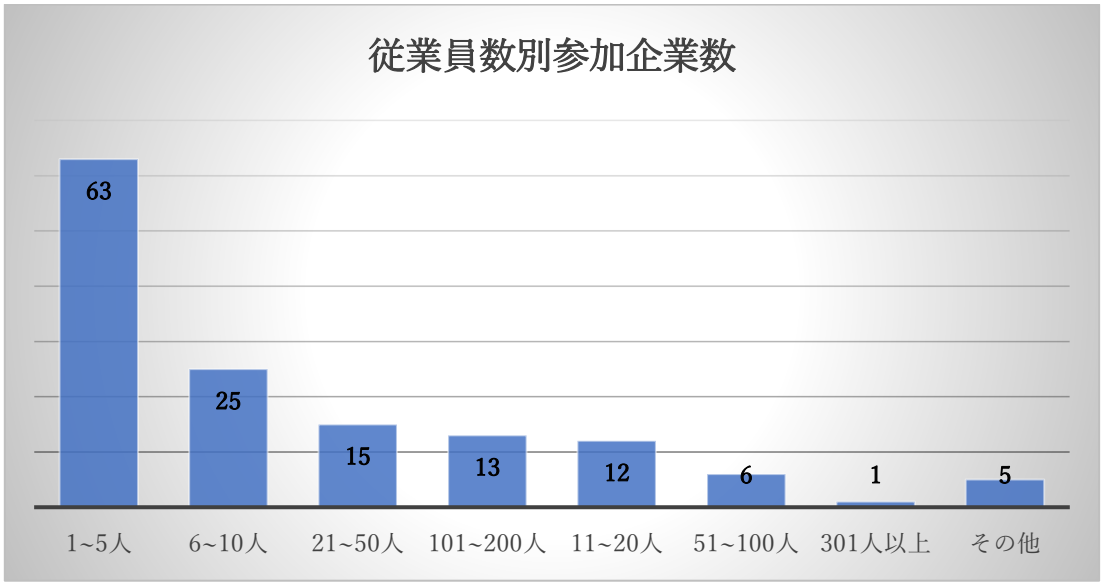

図 3.6 従業員数別参加企業数

3.4 実施内容

事業説明会での施策である「簡易セキュリティアセスメント」の結果レポート提示により各企業におけるセキュリティリスクへの意識向上を図る。事業説明会開催時のアンケートおよび現場への機

器導入等から得られたログの活用により、中小企業の意識と現場の実態のギャップを把握する。

また、上記ログによるセキュリティインシデントの情報収集およびセキュリティ対策の実装における課題抽出を行い、中小企業の必要とするサイバーセキュリティサービスの検討材料とする。

3.4.1 簡易セキュリティアセスメントの実施

簡易セキュリティアセスメント（事業説明会開催時の Web 回答）の実施により、現場のセキュリティ対策状況を収集することで中小企業の実態把握に利用した。

簡易セキュリティアセスメント結果は企業毎に効果の高いセキュリティ対策内容、顧客の特徴や対応方針のアドバイスの記載により、対策の優先度などを決めてもらう判断材料としている。また、セキュリティ対策においては、同業種の状況を鑑み導入を決める企業も少なくない。本診断書は、同業種のセキュリティ対策毎の実装率を記載しており、同業種と自社の比較検討を可能としている。また、サイバー攻撃の手法別にどのようなセキュリティ対策製品が有効であるかを図式化してあり、回答した企業のセキュリティ対策実装状況と合わせて危険度がわかるようにしている。

表 3.2 簡易セキュリティアセスメント概要

項	項目	内容
1	目的 （ねらい）	中小企業のセキュリティ対策状況の把握、個々の中小企業のセキュリティ対策状況を踏まえて推奨対策プランを提示し、優先すべき課題を可視化する。 ・標的型攻撃の対策状況および弱点を可視化 ・可視化した結果から、優先すべき対策を明示
2	実施内容	・説明会参加者等に標的型攻撃に対する 18 問のセキュリティ対策状況の質問を実施し回答を収集した。 ・日立システムズの分析ナレッジを利用したセキュリティ対策の簡易セキュリティアセスメント結果（以下、診断書）を提示した。
3	実施結果	・参加中小企業 140 社に対し診断書をメール送付。 ・顧客反応：セキュリティリスクについて再認識するきっかけになった。 ・集計結果：情報漏えい等の被害を食い止める「出口対策」の実施率が低い。

【設問内容】

以下の 18 問について回答者にアンケート形式で実施した。

表 3.3 セキュリティ対策の簡易セキュリティアセスメント設問内容

No.	設問内容
No.01	インターネットとの接続箇所において、インターネットから自組織内への通信を、必要な通信に限定していますか。
No.02	インターネットとの接続箇所において、サイバー攻撃を検知または防御していますか。
No.03	組織外から受信する電子メールに対して、パターンマッチ型のウイルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウイルスチェックは含みません。
No.04	インターネット（ウェブ）からダウンロードするファイルに対して、パターンマッチ型のウイルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウイルスチェックは含みません。
No.05	組織外から受信する電子メールに対して、サンドボックスなどのパターンに依存しないウイルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウイルスチェックは含みません。
No.06	インターネット（ウェブ）からダウンロードするファイルに対して、サンドボックスなどのパターンに依存しないウイルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウイルスチェックは含みません。
No.07	パソコンにパターンファイルを常に最新に更新しているパターンマッチ型のアンチウイルス・マルウェアソフトウェアを導入し、ウイルス・マルウェア対策を実施していますか。
No.08	パソコンにふるまい検知型などのパターンに依存しないアンチウイルス・マルウェアソフトウェアを導入し、ウイルス・マルウェア対策を実施していますか。
No.09	パソコンのオペレーティングシステムに対するセキュリティパッチを適用していますか。
No.10	組織内部のネットワーク上で、不正な通信が行われていないか監視を行っていますか。
No.11	組織内のサーバー（ファイルサーバーなど）のアクセスログや認証ログを保管し、分析していますか。
No.12	組織内からインターネット（ウェブ）へのアクセスにウェブプロキシサーバーを経由する構成としていますか。
No.13	インターネット（ウェブ）へのアクセスにおいて、業務上不要なサイトや悪意のあるサイト（マルウェアを配布しているサイトなど）へのアクセスを制限していますか。
No.14	インターネット（ウェブ）へのアクセスにおいて、攻撃者が準備しているサーバー（C&C サーバーなどマルウェアの接続先のサイトなど）へのアクセスを制限していますか。

No.	設問内容
No.15	重要な情報が保管されているサーバーやパソコンのデータバックアップを取得していますか。
No.16	サーバーやパソコン上のプログラムの実行記録や通信の実施記録を取得し、保管していますか。
No.17	サイバーセキュリティ事故（インシデント）が発生した場合の対応手順・対応体制を定めていますか。
No.18	標的型攻撃に関する教育や情報提供を実施していますか。

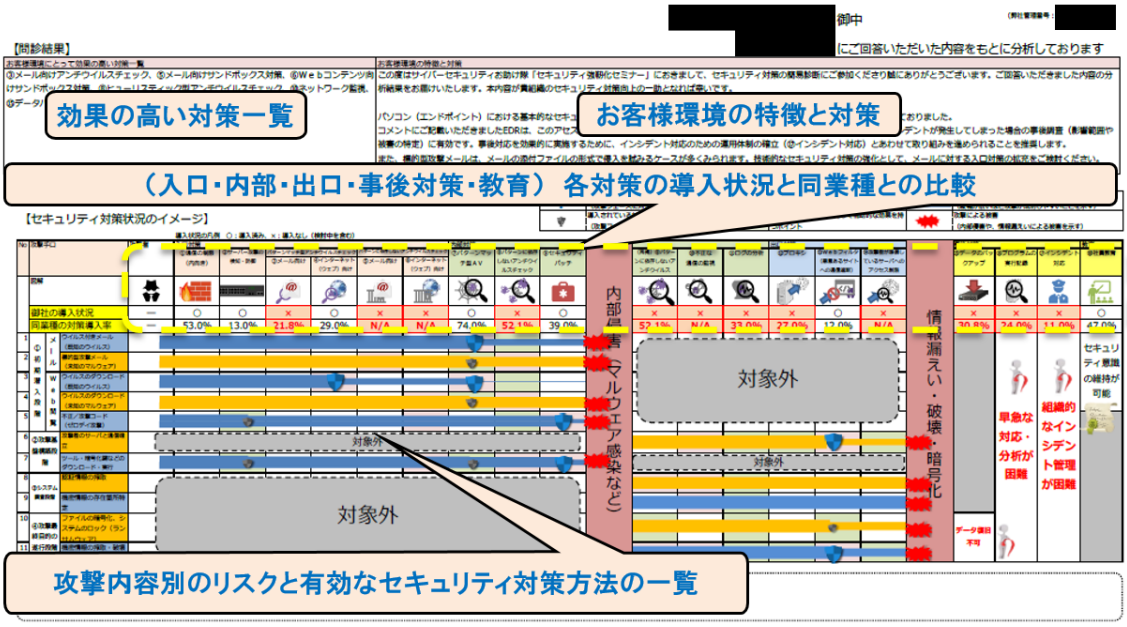

図 3.7 セキュリティ対策の簡易セキュリティアセスメント診断書

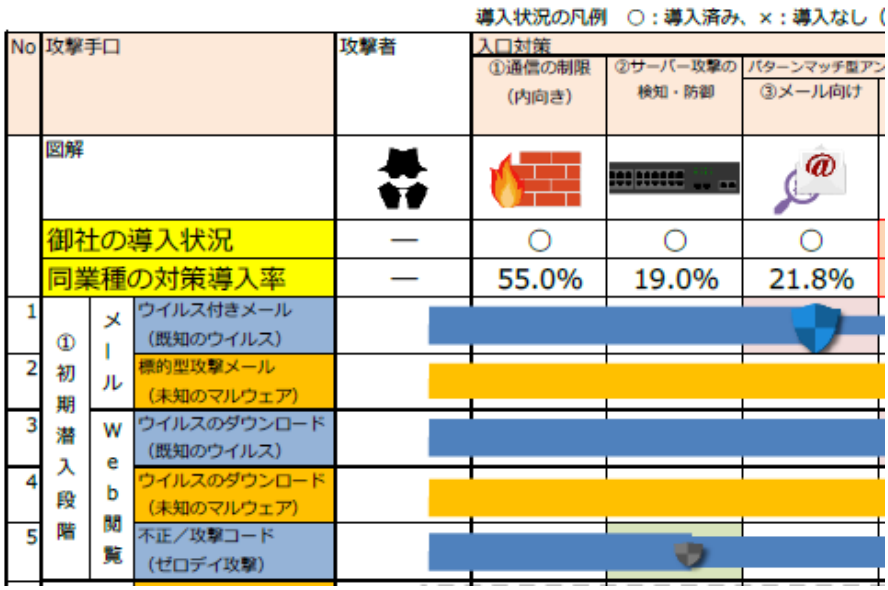

図 3.8 セキュリティ対策の簡易セキュリティアセスメント診断書

（サイバー攻撃の手法別の記載例）

3.4.2 セキュリティ対策製品によるサービス提供

1) エンドポイントに関するセキュリティ対策（Defender 監視）

中小企業のセキュリティ対策を低コストで実現するにあたり、OS に付随する無償版アンチウイルスソフト（Windows Defender）の利用を推奨する。ただし、万が一 Windows Defender が動作しない状況になった場合、ユーザーが気付かぬうちにセキュリティリスクを抱えることになってしまう。そこで安価にセキュリティ対策を実施し、かつ不具合によるセキュリティリスクを回避することを目的として、日立システムズの提供する Defender 監視ツール「MMR20」を提供した。本ツールは Windows Defender が停止した際にポップアップにてユーザーへ通知する機能を持ち、通知内容として連絡先を表示する機能を持つ。本実証では通知時の連絡先として「問合せ窓口（コンタクトセンター）」を登録することにより、万が一 Windows Defender が停止し、ポップアップ通知が表示されたとしてもユーザーが相談先に困らないようにした。

また、今回本ツールの前提条件として OS が Windows10 以降であることとした。MMR20 の動作要件としては Windows8 以降となるが、セキュリティ対策の一環として PC の OS を Windows10 とすることを Pit-Nagoya としては推奨しているため、その方針を鑑み Windows10 以上を前提条件としている。

表 3.4 エンドポイントに関するセキュリティ対策概要

項	項目	内容
1	目的 （ねらい）	・低コストにてアンチウイルス対策(Defender)を実装した際の Defender サービス停止リスクを軽減。 ・通知内容に問合せ窓口を併記し対応不可のリスクを軽減。
2	前提条件	OS が Windows10 であること。 他社製のアンチウイルス製品が未導入であること。
3	実施内容	現地の PC に専用ツールを導入。

表 3.5 MMR20 の概要

項	項目	内容
1	機能	Defender が停止中の場合、警告をダイアログで表示する。ダイアログとして下記情報を含める。 ・企業名、電話番号、Email アドレス
2	動作要件	Defender を AV 製品として利用している OS が Windows8 以降
3	備考	他社製の AV 製品を使用している場合は、Defender が無効化されるため使用不可。

【Defender 監視サービスの提供イメージ】

① 監視対象 PC へ Defender 監視ツールをインストールし、インシデントを監視する。

② インシデント発生時はコンタクトセンターへ連絡してもらい、駆け付け要否判断等の対応をするとともに、事象について分析用に収集・蓄積する。

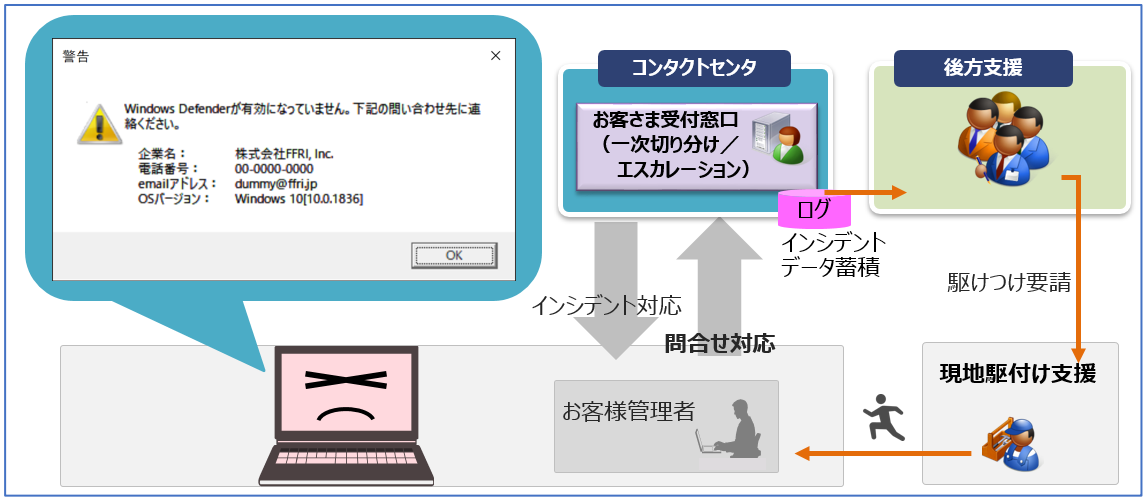

図 3.9 Defender 監視サービスの概要

2) エンドポイントに関するセキュリティ対策（Web 対策ツール）

昨今のマルウェア等を含むセキュリティリスクの入口は、Web（HTTP,HTTPS）経由がほとんどである。そのため手始めのセキュリティ対策としては Web 閲覧時の対策をするのが最も効果的と言える。本実証事業では Web 対策ツールとしてデジタルアーツ社の i-FILTER を採用した。また専用サーバーを設置するオンプレミス版では中小企業に対する導入時の敷居が高いため、導入が簡単なクラウド型の製品（i-FILTER ブラウザー＆クラウド）を選定した。

i-FILTER は Web フィルタリングソフトの位置づけであるが、マルウェア等の通信先である不正サイトへの通信において、ブラウザーを使用しない場合でも遮断することができる。そのため仮にマルウェア等に感染してしまった場合でも、C&C サーバー（攻撃者が準備しているサーバー）への通信を遮断することでその後の感染拡大を防ぐ手段としても有効と考える。なお、昨今脅威となっている標的型攻撃メールにおいても、URL リンクをクリックして感染させるタイプであれば本ツールにて対策が有効である。

導入時には各 PC にエージェントをインストールするのみであり、各種設定や状況確認についてはクラウド側の管理サイトより一括管理が可能となる。今回は一般企業が業務に必要としないサイト（アダルト・ギャンブル等）についてフィルタする設定とした。万が一業務に必要なサイトがブロックされてしまう場合には、本実証事業用に用意した問合せ窓口（コンタクトセンター）に連絡をして頂き、必要に応じてリモートで対応をする体制とした。

表 3.6 Web 対策ツール概要

項	項目	内容
1	目的（ねらい）	意図しないサイトへアクセスしてしまうことによるセキュリティリスクの軽減。
2	前提条件	対象 PC が Windows8.1 以降であること
3	実施内容	現地の PC に「i-FILTER ブラウザー＆クラウド」のエージェントを導入。定期的にリモートにてブロックログを確認。

表 3.7 i-FILTER ブラウザー＆クラウドの概要

項	項目	内容
1	機能	アプリによらず Web アクセスを制御
2	動作要件	Windows8.1 以降
3	備考	クライアント証明書が必要なサイトにアクセスする場合は、個別設定が必要。

【Web 対策ツールの提供イメージ】

① 監視対象 PC へ i-FILTER（Agent）をインストールし、危険サイト閲覧を防止する。

② ログデータは分析用に後方部隊にて収集・蓄積する。

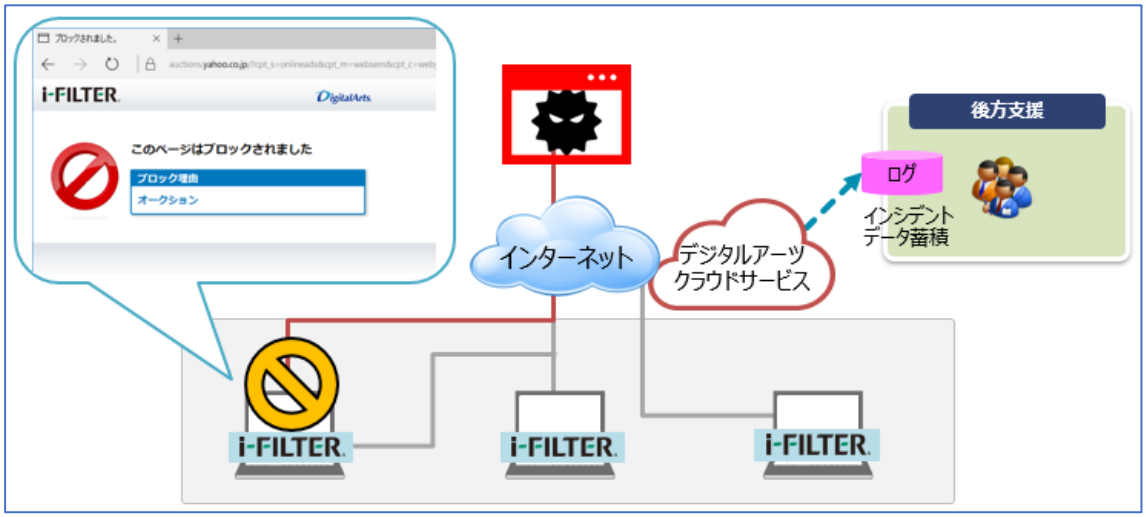

図 3.10 Web 対策ツールの提供イメージ

3) メール受信に関するセキュリティ対策（メール対策ツール）

「情報セキュリティ 10 大脅威 2020」（IPA ホームページ）より、組織での脅威 1 位では昨年に引き続き「標的型攻撃による被害」となっている。その手段はメールを装う場合が多く、中小企業においてもメールに対するセキュリティ対策は急務である。そこで本実証事業ではメールに対するセキュリティ対策としてデジタルアーツ社の m-FILTER を採用した。専用サーバーを設置するオンプレミス版では中小企業に対する導入時の敷居が高いため、導入が簡単なクラウド型の製品（m-FILTER@Cloud）を選定した。

導入時の各種設定や状況確認についてはクラウド側の管理サイトより一括管理が可能となる。なお m-FILTER については現在企業が使用しているメール環境にも一部設定が必要となるため、デジタルアーツ社において実績がありなおかつ設定手順書も準備されている環境（下記）を使用している企業であることを前提条件とした。

・G-Suite（Google）

・Exchange Online（Microsoft）

また、メールについては特に従業員が多い企業において必要なメールが届かない場合の業務影響も大きいと考えられるため、万が一フィルタ条件に該当した場合でも無条件に削除をするのではなく、メールのヘッダーにその旨を記載しユーザーに注意を喚起する方式とし、本実証事業における業務影響を考慮した。また万が一動作不具合等があった場合には、本実証事業用に用意した問合せ窓口（コンタクトセンター）に連絡をして頂き、必要に応じてリモートで対応をする体制とした。

表 3.8 メール対策ツール概要

項	項目	内容
1	目的 （ねらい）	標的型攻撃メールを受信した際のセキュリティリスクの軽減。
2	前提条件	メールサービスとして下記を使用していること ・G-Suite（Google） ・Exchange Online（Microsoft）
3	実施内容	お客様メールサーバーと m-FILTER@Cloud を連携

表 3.9 m-FILTER@Cloud の概要

項	項目	内容
1	機能	「送信元」「添付ファイル」「本文・URL」の偽装判定を行い、安全なメールだけを受信。危険なメールは隔離およびメール無害化を実施。
2	動作要件	設定用サイトへアクセスする際に 80,443 以外のポートでアクセスできる必要あり。
3	備考	連携設定をする際に下記の管理アカウントが必要。 ・既存メールサービスの管理ページ ・既存ドメインネームの管理ページ

【Defender 監視サービスの提供イメージ】

① お客様メールサーバーと m-FILTER@Cloud を連携し、不正メール対策を実施する。

② ログデータは分析用に後方部隊にて収集・蓄積する。

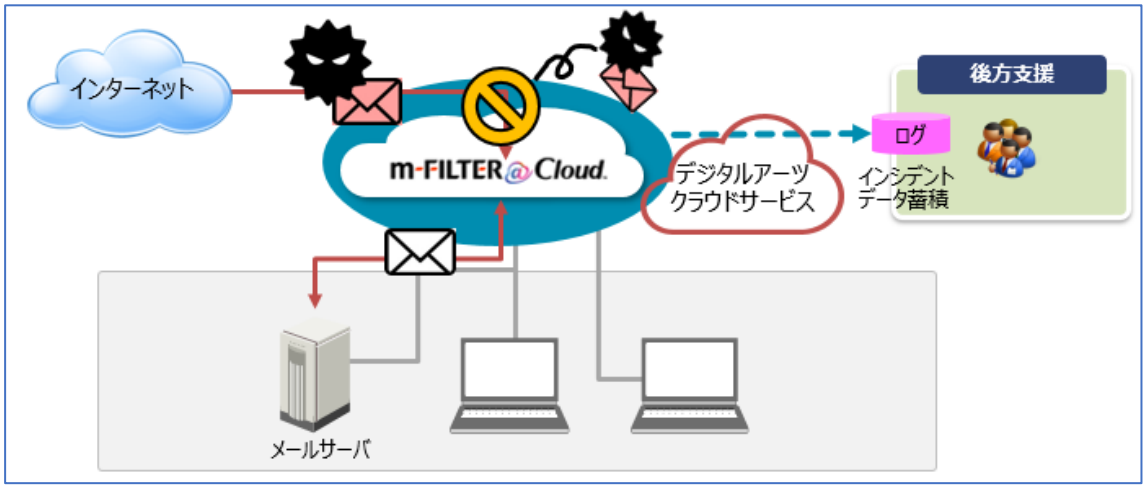

図 3.11 Defender 監視サービスの提供イメージ

4) ネットワークに関するセキュリティ対策（UTM 導入）

お客様のネットワーク上に統合脅威管理装置（UTM）を設置し、インターネット経由でインシデントのリモート監視を行った。本実証事業では NTT 西日本の「セキュリティおまかせプラン」のサービスを採用した。本サービスでは統合脅威管理装置（UTM）を企業へ設置し、インシデント発生時にはコンタクトセンターからの遠隔サポートを提供する。

また、UTM による防御状態について毎月レポートを送付する。なお設置する UTM はトレンドマイクロ社の Cloud Edge という機器であり、メールセキュリティ、Web フィルタリングや不正プログラム対策など総合的にセキュリティ対策が可能な製品となっている。

本実証事業ではまず導入先に伺い、ネットワークの状況等現場の状況を確認した後に、別途工事日を調整して導入するという流れとした。

表 3.10 UTM 導入の概要

項	項目	内容
1	目的 （ねらい）	セキュリティインシデントの実態把握
2	前提条件	なし
3	実施内容	現地のネットワーク上に統合脅威管理装置（UTM）を導入し、インシデントのリモート監視を実施。

表 3.11 Edge Cloud の概要

項	項目	内容
1	機能	ファイアーウォール、 マルウェア対策、メール・Web セキュリティ機能、HTTPS スキャニング他
2	備考	クラウド上の管理コンソールにてリモート管理が可能。

【UTM 導入の提供イメージ】

① お客様のネットワーク上に統合脅威管理装置（UTM）を設置し、不正な通信を抑止する。

② インシデントデータは分析用にコンタクトセンターにて収集・蓄積する。

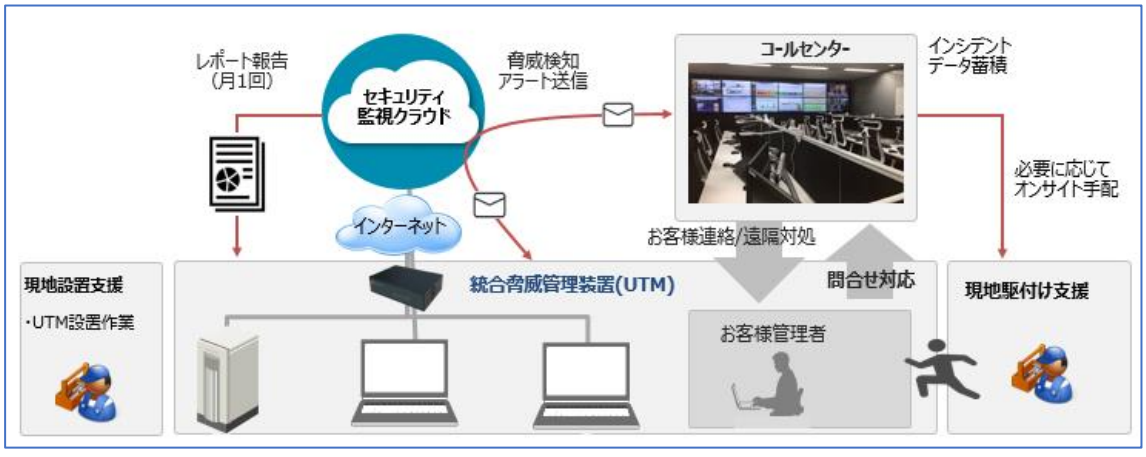

図 3.12 ネットワークに関するセキュリティ対策の提供イメージ

3.4.3 駆け付け支援を実施した中小企業へのヒアリング

本実証事業に参加した企業には問合せ窓口（コンタクトセンター）の連絡先を知らせ、何かしら困ったことが発生した場合には連絡できるようにした。なお、コンタクトセンターでは解決できない場合、地域 IT ベンダーの作業員が現地へ赴き、実証参加企業に対してクラウド上の情報連携ツールを用いた問診票に基づきヒアリングを実施する。問診結果を元に必要に応じて現地対応を実施後、問診結果、作業結果を分析用に後方部隊にて収集・蓄積することとした。

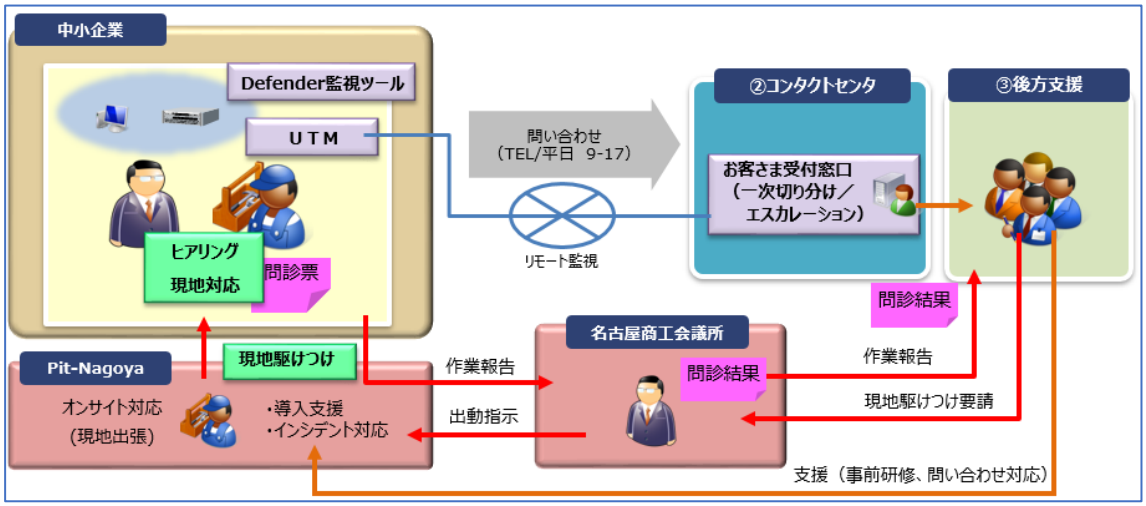

図 3.13 駆け付け支援の提供イメージ

3.4.4 問合せ窓口の提供

今回、問合せ窓口として日立システムズおよび NTT 西日本のコンタクトセンターを用意した。なお、万が一問合せ先を間違えた場合は、実証参加企業へ連絡先を相互に案内できるように手配した。

表 3.12 問合せ窓口の概要

窓口	日立システムズ	NTT 西日本
対応サービス名	Defender 監視ツール Web 対策ツール メール対策ツール その他困りごと	UTM
アクセス方法	電話、メール	電話、メール
対応時間	日立システムズ営業時間内	NTT 西日本営業時間内

3.5 地域 IT ベンダーとの連携

3.5.1 連携方法の概要

本実証事業におけるサービス提供期間においてはコンタクトセンター、後方支援、現地対応および事務局が相互に情報連携をする必要がある。ただしそれぞれが異なる企業であるため一般的な情報共有手段としてはメールを介した情報共有となるが、それでは緊急の駆け付け要請があった場合などにおいて迅速な連携が難しい。そこで本実証事業では関係者間の情報連携ツールを採用した。

3.5.2 アプリの内容

今回関係各所と情報連携するために使用したアプリについては以下の 4 つとなる。

(1)「参加企業管理」アプリ

表 3.13 参加企業管理アプリの概要

項	項目	内容
1	目的	実証に参加した企業の情報を管理する
2	主な項目	会社名、連絡先、担当者名、導入サービス名、導入日など
3	備考	関連する問合せおよび現地作業へのリンクあり

(2)「問合せ管理」アプリ

表 3.14 問合せ管理アプリの概要

項	項目	内容
1	目的	実証参加企業より問合せのあった内容を管理する
2	主な項目	問合せ企業名、問合せサービス、問合せ内容、進捗状況、対応期限など
3	備考	関連する現地作業へのリンクあり 導入、撤去時には「現地対応」レコード起票のため、最初に「問合せ管理」アプリに仮レコードを起票する必要がある。

(3) 「現地対応管理」アプリ

表 3.15 現地対応管理アプリの概要

項	項目	内容
1	目的	現地作業者への指示および現地作業結果を管理する
2	主な項目	問合せ内容、現地作業者の連絡先、現地作業の内容、現地作業結果など
3	備考	実証参加企業への駆け付けだけでなく、導入・撤去時の地域 IT ベンダーへの作業指示にも使用する。

(4) 「FAQ 管理」アプリ

表 3.16 FAQ 管理アプリの概要

項	項目	内容
1	目的	FAQ の管理や作業者への手順書の配布等に使用する。
2	主な項目	分類、製品、質問、回答、添付ファイルなど
3	備考	

3.5.3 運用フロー

本実証サービスにおける問合せ発生時の運用フローについて下記に示す。

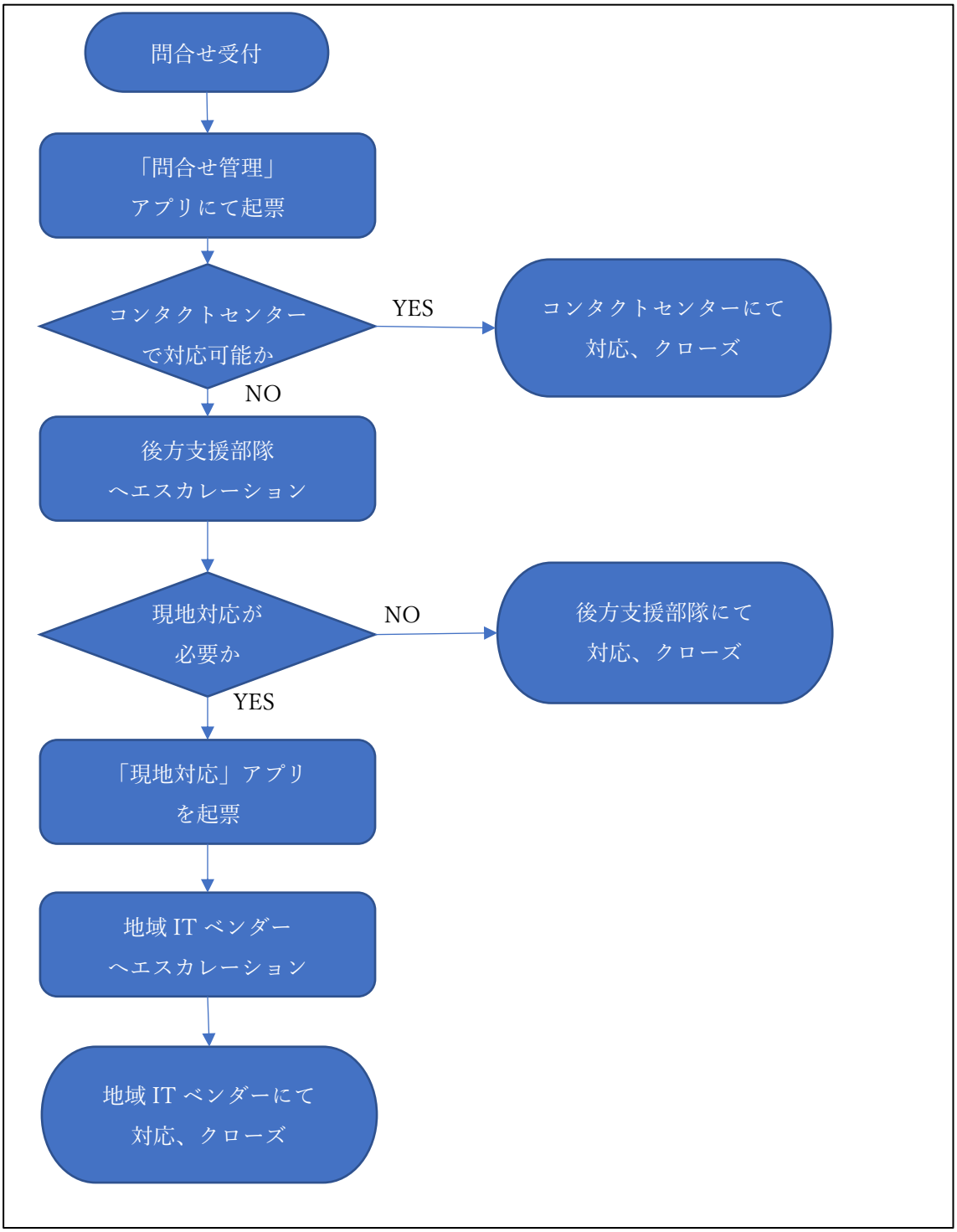

図 3.14 問合せ時の運用フロー

4. 実施結果

本実証事業の中小企業への周知および実証参加企業募集のため、日立システムズ、NTT 西日本、損害保険会社等と連携し事業説明会を開催した。本章では事業説明会の回数、実施内容および成果について報告する。

4.1 事業説明会

実証事業開始の周知および実証参加企業募集のため、愛知を中心としたエリアで説明会を実施し、実証事業開始時の 9 月 1 回、10 月 3 回の計 4 回を実施する予定であったが、実証参加企業の促進を行うため、事業説明会（事業開始）の追加開催を計画し、計 5 回を実施した。

表 4.1 事業説明会日程

項	事業説明会開催場所	開催日	参加企業数
1	Zoom による オンライン開催	2020 年 9 月 29 日（火）	23 社
2		2020 年 10 月 2 日（金）	17 社
3		2020 年 10 月 8 日（木）	22 社
4		2020 年 10 月 12 日（月）	15 社
5		2020 年 11 月 6 日（金）	59 社
合　　計			136 社

説明会では実証事業内容の説明とサイバーセキュリティの普及啓発を行い、以下の内容にて実施した。

【実施内容】

◆ 安全な IT 活用について

- PC においては Windows Defender によるセキュリティ対策に一定の効果がある。低コストでのセキュリティ対策として PC の OS を Windows10 に無償アップグレードした後、Windows Defender を有効にすることを推奨。
- IPA 推奨のパスワードの使い方として、パスワードを流用しないことおよび推奨するパスワードの設定方法について教示。

◆ 大事な資産を守るために

・ 近年法人での不正送金事犯では 4 年前に比べ全体被害額は下がっているものの、件数は増加しており中小企業が被害に遭うリスクも増加傾向。

・ 不正送金被害を受けた際の金融機関の補償について解説。使用している OS が最新状態であること、セキュリティ対策ソフトを導入し更新されていることが補償の要件となっている。

・ 対策すべきは PC のみではなく、スマート・フォンやフィーチャー・フォンについても 3-4 年程度で機種変更が必要。

◆ お助け隊事業内容について

・ 本実証事業の目的、実施内容とスケジュール、実施体制、実証での提供サービス概要。

◆ お助け隊ご提供サービスの紹介

・ 5 種類の提供サービスの具体的な内容、仕組みや導入時のメリットおよび前提条件の説明。

◆ セキュリティ対策の簡易セキュリティアセスメント

・ ブラウザーによるオンライン形式で実施し、専門用語、サイバーセキュリティ対策の仕掛けについて設問毎に解説を行いながら実施した。また Zoom の挙手機能を利用し設問毎に入力状況を確認しながら実施した。また Zoom のチャット機能を利用し質問・相談が個別に行えるようにして、IT リテラシーが高くなくても「セキュリティ対策の簡易診断」に回答できるようにして実施した。

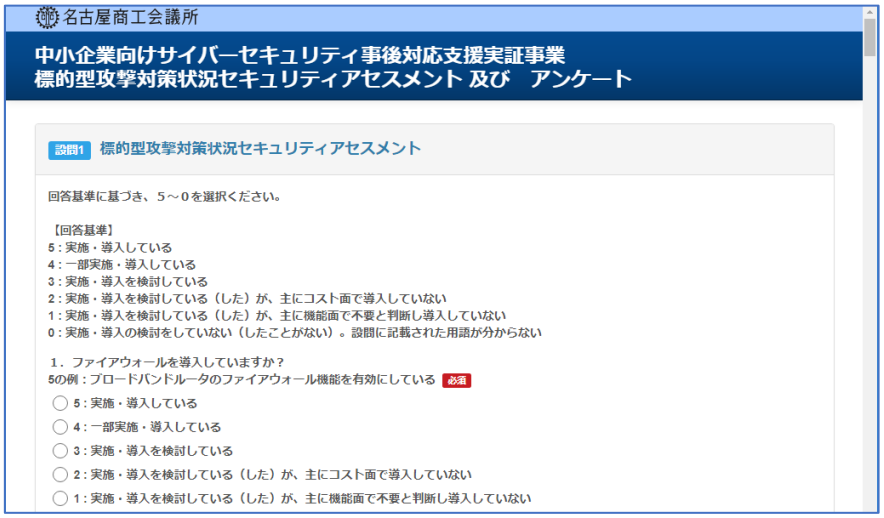

図 4.1 オンラインでの簡易セキュリティアセスメントのイメージ

開催に際して地元の中小企業の参加しやすい時間帯、開催時間について協議し、午後開始でオンラインでの開催を踏まえ 1.5 時間程度での実施内容として設定した。以下に事業説明会実施時のアジェンダを記載する。

表 4.2 事業説明会アジェンダ

項	時間	報告項目	発表者
1	15:00～15:05	はじめに	名古屋商工会議所
2	15:05～15:15	安全な IT 活用について	日立システムズ
3	15:15～15:25	大事な資産を守るために	日立システムズ
4	15:25～15:35	お助け隊事業内容について	名古屋商工会議所
5	15:35～15:45	お助け隊ご提供サービスの紹介	日立システムズ NTT 西日本
6	15:45～16:30	セキュリティ対策の簡易診断	日立システムズ

図 4.2 事業説明会実施風景（Zoom 配信会場）

【動画配信】

なお、説明会に参加できなかった企業への参加促進策として、説明会と同様の内容を動画としてオンデマンド配信する試みも実施した。

表 4.3 事業説明会オンデマンド配信概要

事業説明会オンデマンド配信概要	
配信場所	YouTube
URL	https://www.youtube.com/watch?v=Tageq4bNXOs
タイトル	サイバーセキュリティお助け隊事業 実証参加募集
配信者	名古屋商工会議所【Pit-Nagoya】名古屋中小企業 IT 化推進コンソーシアム
動画時間	1 時間 2 分 3 秒
配信期間	2020 年 10 月 23 日から 2021 年 1 月 31 日まで
視聴数	43（2021 年 1 月 6 日時点）

図 4.3 オンデマンド配信のイメージ

4.2 実態把握結果

4.2.1 事業説明会申込みアンケートの結果

事業説明会への申込時のアンケート結果の結果を以下に示す。

まず業種としては金融／保険業、製造業、卸売／小売業の 3 種で全体の 6 割以上を占めていることがわかった。

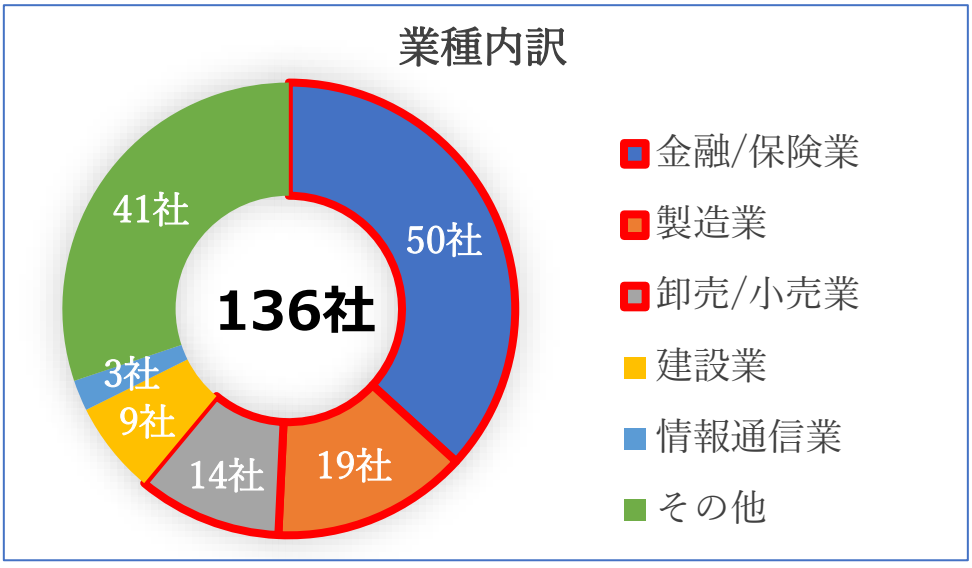

図 4.4 事業説明会申込みアンケートでの業種内訳

次に資本金では 7 割近くの企業が資本金 1,000 万円以下の企業であることがわかった。

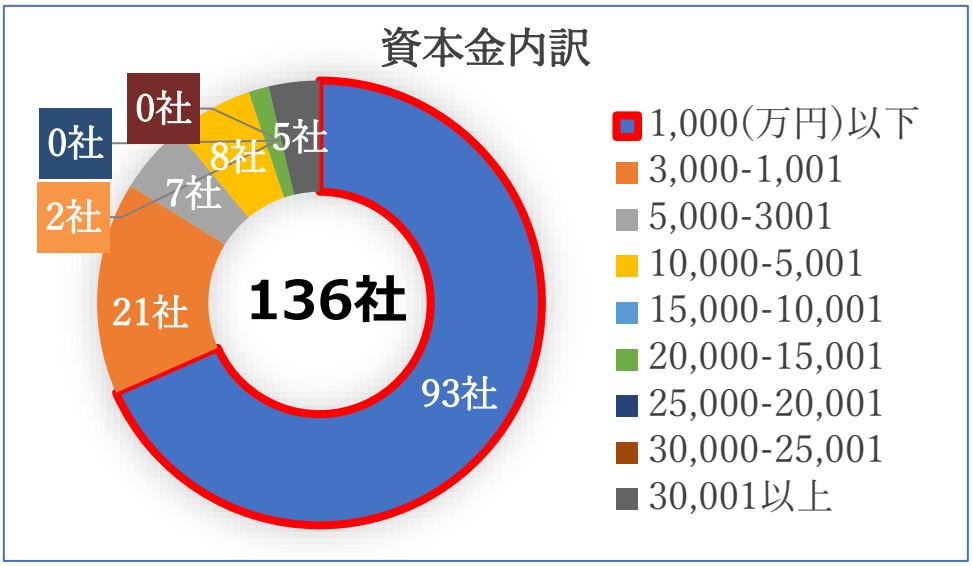

図 4.5 事業説明会申込みアンケートでの資本金内訳

次に従業員数としては 10 名以下の企業が 6 割近くを占めていることがわかった。

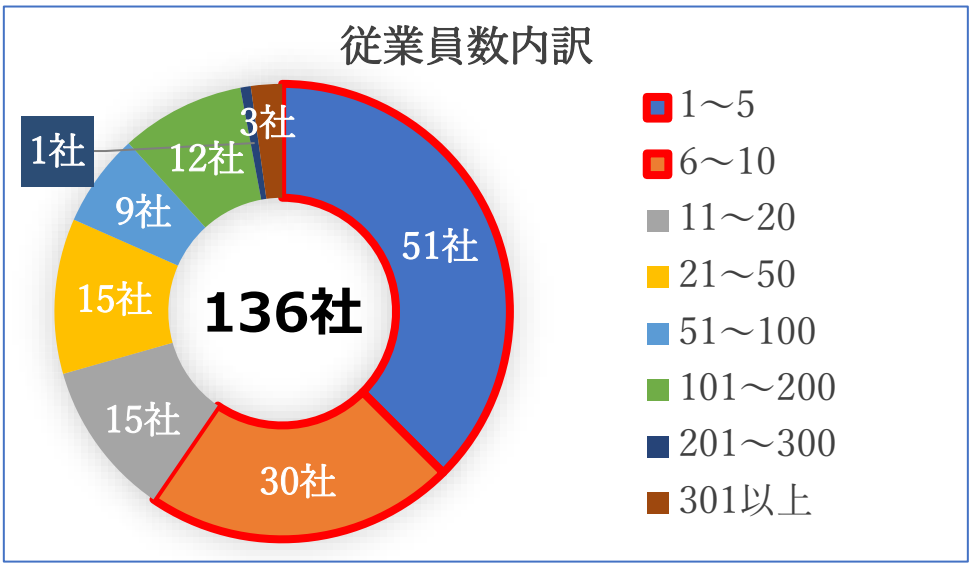

図 4.6 事業説明会申込みアンケートでの従業員数内訳

次にセキュリティ対策の認識度については、十分にできていると回答した企業は 1 割未満であり、9 割強の企業が「不十分」または「わからない」と回答している。そのため、中小企業においてはセキュリティ全般に対する知識の習得が必要と言える。

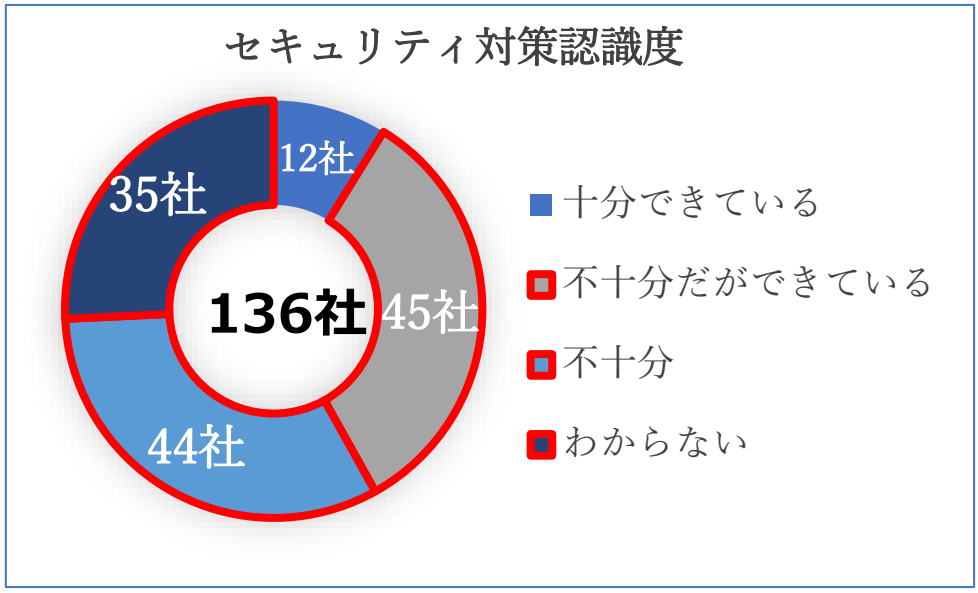

図 4.7 事業説明会申込みアンケートでのセキュリティ対策認識度

取引先からのセキュリティ対策・調査・改善依頼については、依頼があったと回答した企業は 1 割程度であることがわかった。

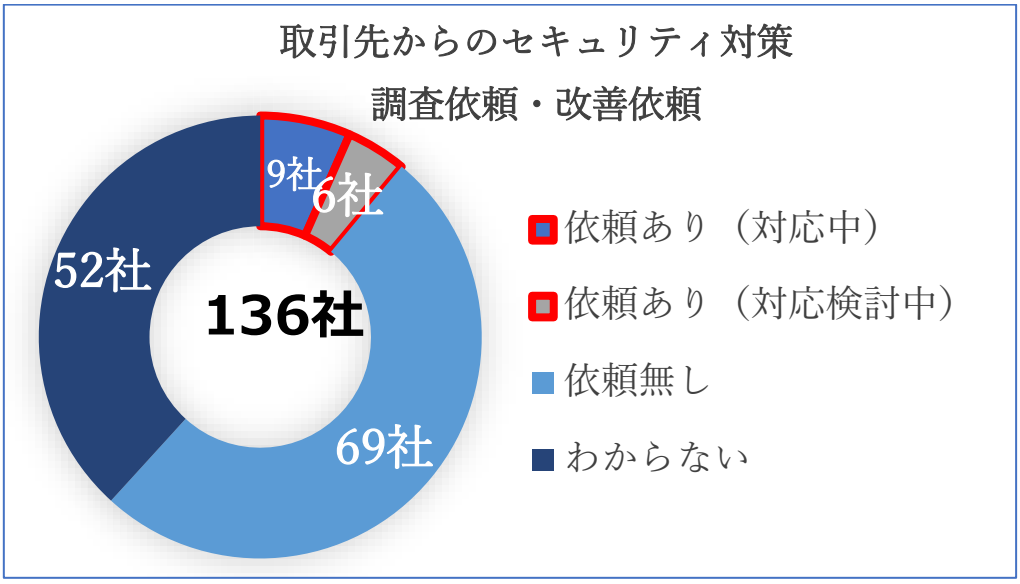

図 4.8 事業説明会申込みアンケートでの取引先からの対策依頼等

また、今後セキュリティインシデントが発生した場合に対応する要員について尋ねたところ、約半数の企業では「社員または外部ベンダーに依頼する」という回答だったが、残りの半数の企業については「いない」もしくは「わからない」という回答であった。このことから約半数の中小企業においてはセキュリティインシデント発生時に対応すべき要員がいないという状況が判明した。

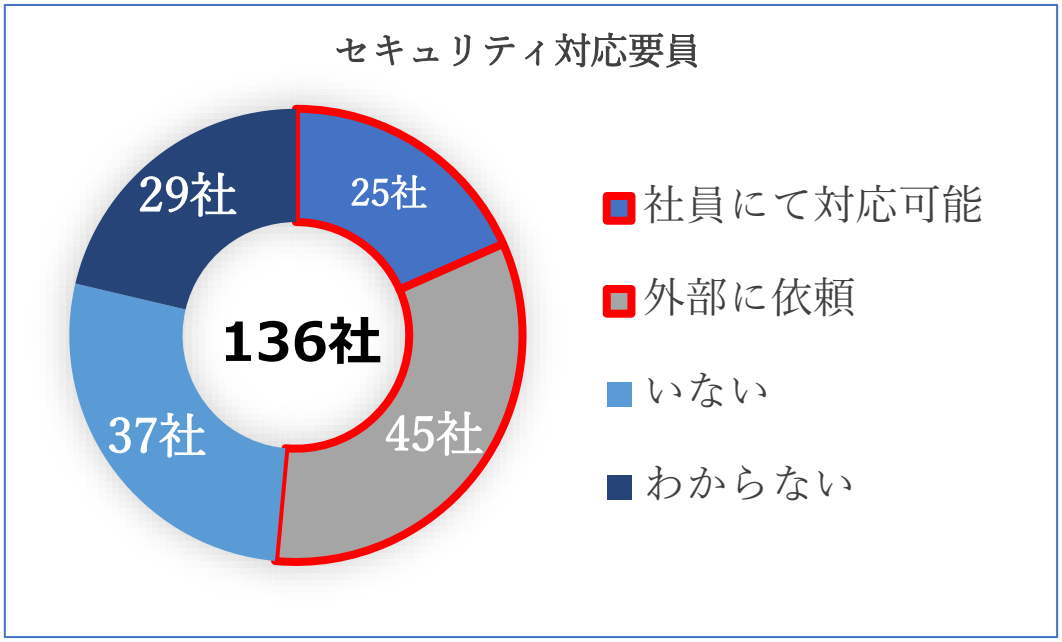

図 4.9 事業説明会申込みアンケートでのセキュリティ対応要員

4.2.2 簡易セキュリティアセスメントの結果

簡易セキュリティアセスメントでは 18 項目の設問に対して下記の選択肢について集計し、実施率・導入率としている。

表 4.4 簡易セキュリティアセスメント選択肢

ポイント	選択肢
5	実施・導入している
4	一部実施・導入している
3	実施・導入を検討している
2	実施・導入を検討している（した）が、主にコスト面で導入していない
1	実施・導入を検討している（した）が、主に機能面で不要と判断し導入していない
0	実施・導入の検討をしていない（したことが無い）。設問に記載された用語がわからない

※実施率が低いことと、設問の理解度が低いことは同義となる。

1) 入口対策

入口対策としてはファイアーウォールおよびメールサーバーへの対策が半数以上の企業で実施されていた。ただしファイアーウォールについては侵入検知・防御機能を持った IDS/IPS システムの導入率が低く 3 割弱の導入率となっており、許可済みのプロトコル等に対する動的に検知・防御する次世代型システムの普及度が低いという状況となっている。

ウイルス対策においても従来のパターンマッチ型対策にとどまっており、次世代型とも言えるふるまい検知型の対策については 1 割程度の導入率にとどまっている。

パターンマッチ型の対策についてもメールと比較し Web については導入率が低い結果となった。これは Web のプロキシサーバーよりもメールサーバーの導入率が高いことも起因していると思われる。中小企業において従業員数との兼ね合いからメールサーバーをオンプレミスで自社に設置するのではなく、クラウドのメールサービスの利用が増加してきており、ウイルス対策についてもメールサービスのオプションを利用する機会が増えているものと推測される。一方で Web プロキシサーバーは入口対策としては有効ではあるが業務として必須ではないため導入率が低く、その結果ウイルス対策の導入率も低くなっていると思われる。

以下にアセスメント結果における入口対策の状況を示す。

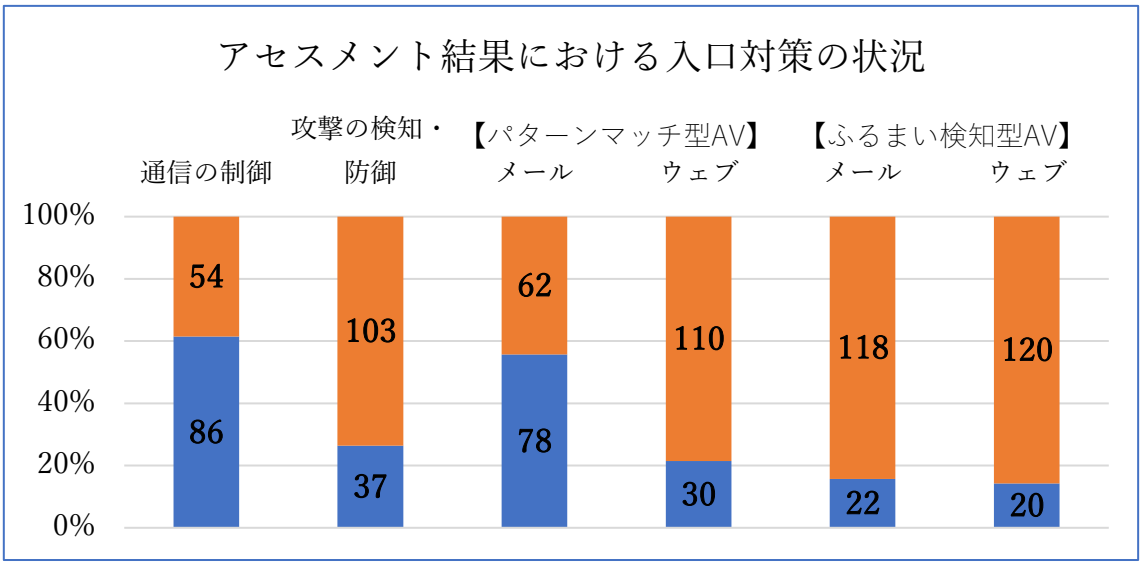

図 4.10 アセスメント結果における入口対策の状況

表 4.5 アセスメント結果における入口対策の概要

できている点	・ 従来型のファイアーウォール導入 ・ メールサーバーへの従来型のアンチウイルス導入
できていない点	・ 次世代型の攻撃検知・防御の導入 ・ Web アクセスのアンチウイルス導入

2) 内部対策

内部対策においても入口対策と同様にパターンマッチ型ウイルス対策が先行して導入されており、導入率は 9 割を超えている。一方でふるまい検知型のウイルス対策は 3 割を下回っており中小企業において導入率の低いことが判明した。また OS のセキュリティパッチについても高い実施率であったが、一方で不正通信ログの監視や操作ログの分析など、効果の見えづらい対策については実施率が低かった。以上より中小企業の内部対策においてはそれぞれのセキュリティ対策の実施率に極端に差があることがわかった。これはセキュリティの脅威に対する認知度の違いによるものと思われる。

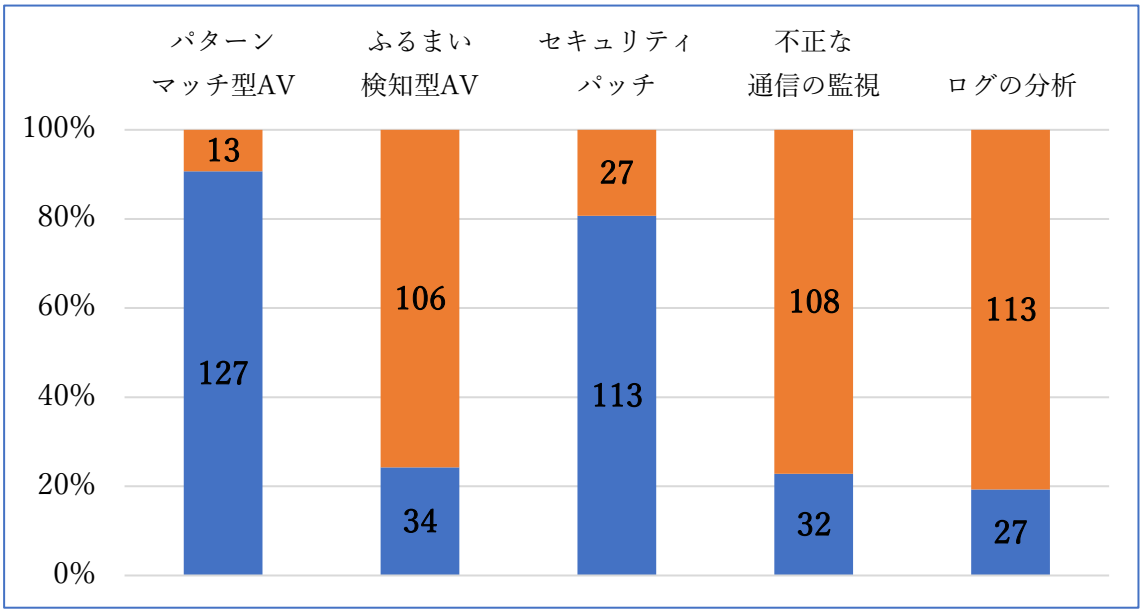

図 4.11 アセスメント結果における内部対策の状況

表 4.6 アセスメント結果における内部対策の概要

できている点	・ 従来型のアンチウイルス導入 ・ OS の最新パッチ適用
できていない点	・ 次世代型のアンチウイルス導入 ・ 不正通信の監視、定期的なログ分析

3) 出口対策

出口対策（インターネット閲覧時のプロキシサーバーと Web フィルタリングおよび C&C サーバー等へのアクセス制御）においては全般的に実施率が低い結果となった。出口対策は万が一内部でマルウェア等に感染した場合でも社外サーバーとの通信を防御する最後の要となる部分ではあるが、中小企業における実施率は 2 割程度であった。このため中小企業においてマルウェア等に感染してしまった場合、その後攻撃者サーバーからの攻撃命令の受信・実行が容易になされてしまうことによる情報流出のリスクが高いという実態が把握できた。

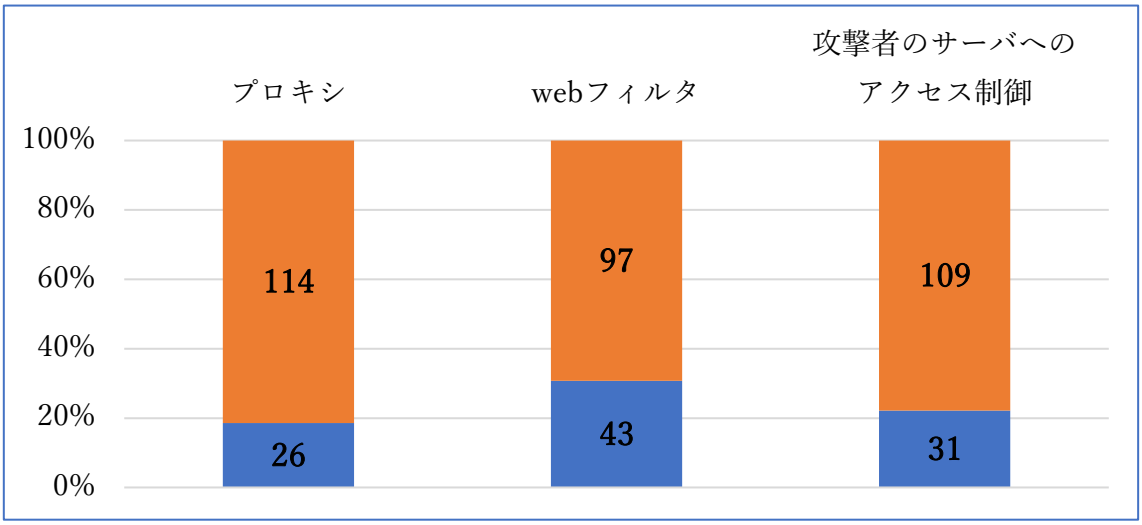

図 4.12 アセスメント結果における出口対策の状況

表 4.7 アセスメント結果における出口対策の概要

できている点	・　（なし）
できていない点	・　出口対策導入（全般）

4) その他のセキュリティ対策

その他のセキュリティ対策としては下記についての設問となっている。

- 重要データのバックアップ
- PC やサーバーにおけるプログラムの実行記録
- インシデント発生時の対応手順および体制
- 社員に対するセキュリティ脅威についての教育

バックアップについては 7 割を超える実施率となっており認識の高さが伺えるが、それ以外の項目においては 3 割程度の実施率の低さであった。やはりここでも効果の見えづらい対策については実施率が低いことがわかった。

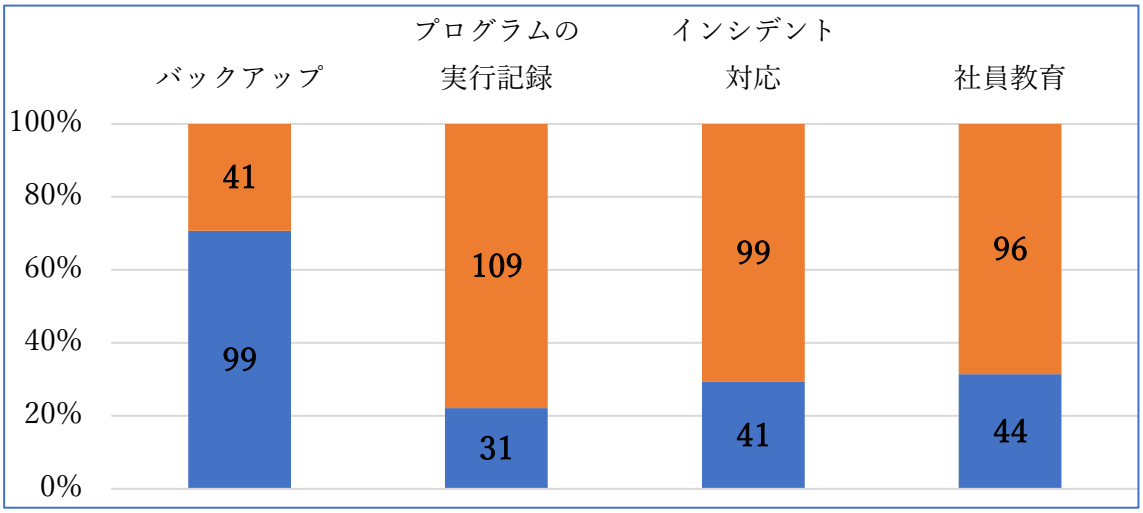

図 4.13 アセスメント結果における対策状況（その他）

表 4.8 アセスメント結果における対策状況（その他）の概要

できている点	・ 重要データのバックアップ運用
できていない点	・ 不正プログラム実行の監視 ・ インシデント対応時の体制、手順の準備 ・ セキュリティ脅威に対する社員教育

4.3 実証の実施結果

中小企業に 4 つのサービスのいずれか、もしくは複数のサービスを合計 73 社に提供した。サービス毎導入数についても目標内の企業数を確保した。以下に 4 つのサービスを提供した企業数と複数サービス提供の組み合わせの内訳を記載する。

表 4.9 提供サービス提供内訳

項	サービス名	サービス毎	サービス略名	複数サービス提供内訳					
				DF のみ	DF＋Web	Web のみ	Web+メール	メールのみ	UTM のみ
1	Defender 監視ツール	6	DF	●	●				
2	Web 対策ツール	41	Web		●	●	●		
3	メール対策ツール	7	メール				●	●	
4	UTM 導入	29	UTM						●
提供数				1	5	31	5	2	29
合計（サービス数）				73					

4.3.1 エンドポイントに関するセキュリティ対策（Defender 監視）

Defender 監視ツールの提供における実施結果では、最終的に本ツールに関するインシデントは 0 件となっている。なお、本ツールは安価にセキュリティ対策を実施するという方針の下、リモートでのログ収集機能等は実装されていない。そのためインシデント（Defender サービス停止時のポップアップ通知）に関する問合せ窓口（コンタクトセンター）への問合せ有無を以てインシデント数としている。

本ツールにおいては導入企業数が 6 社にとどまっている。その理由として、そもそも Windows Defender を利用する場合には他社製のアンチウイルスソフトがインストールされていないことが前提となる。ところが現在中小企業が使用している PC においては基本的にアンチウイルスソフトが導入済みであり、前提条件に合わなかったという状況がある。実際、本実証において Defender 監視ツールを希望していたにも関わらず、導入前に状況　確認をしたところ既に他社製のアンチウイルスソフトがインストール済みであったため、今回のサービス提供を見合わせたというパターンが多く見受けられた。

導入サービスの計画時には「安価なセキュリティ対策として OS 付属の無償ツール（Windows Defender）が推奨であり、Defender 使用時の万が一の不具合を監視することが中小企業にとって有用」との方針にて本ツールを採用したが、本実証結果より多くの中小企業では既に使用する PC に他社製のアンチウイルスソフトが導入済みであるということが判明した。

ここで中小企業におけるサイバーセキュリティ対策が進んでいないと言われる状況において、他社製のアンチウイルスソフトについては既に導入が進んでいるという推定要因についてもいくつか挙げられる。企業自体の PC におけるウイルス対策への認識度が上がり、また近年アンチウイルスソフトの価格が下がったことで費用対効果が見込まれたことで積極的に購入するパターンが推測される。一方で購入した PC 内に既に有償版アンチウイルスソフトが同梱されており、そのまま購入するパターンなども推測される。

なお、説明会開催前の事前アンケートでは本ツールを希望する企業（複数選択あり）の数が 4 割を超える状況であったが、実際にサービス導入に至った企業は 1 割に満たなかった。このことから Windows Defender はアンチウイルス機能であり、他社製のアンチウイルスソフトと競合するという点についてまだ認識が及ばない参加者も多かったと予想され、セキュリティや IoT 全般に関する認識不足が否めない。実際、本ツールを希望した企業への導入前の状況確認時に、上記について中小企業の担当者に説明したところ、「無償でアンチウイルス機能（Windows Defender）が使用できるのであればそもそも有償版なんて購入していなかった」との声も聞かれた。

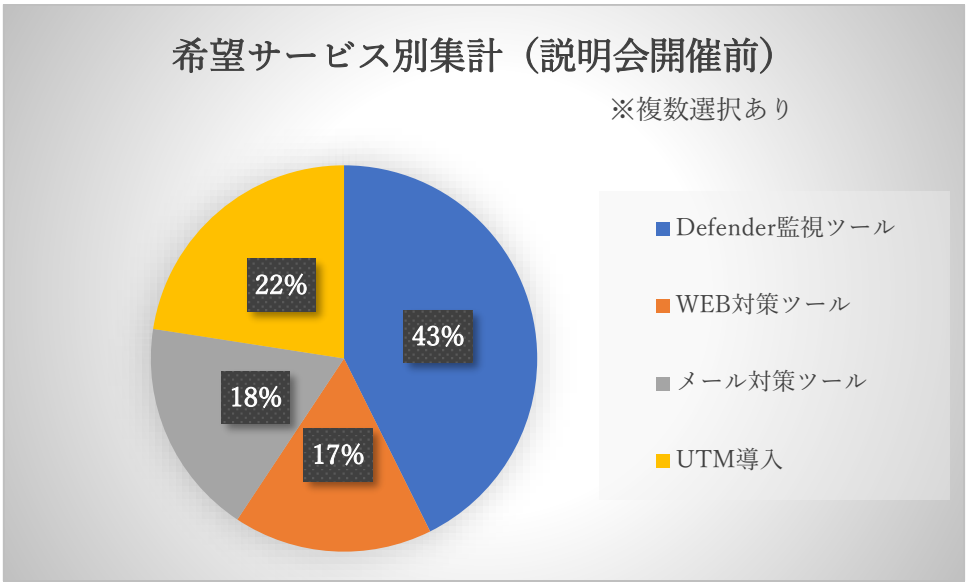

図 4.14 希望サービス別集計

表 4.10 Defender 監視ツールにおける結果概要

項	項目	内容
1	実施内容	現地の各 PC に専用ツール（MMR20）を導入。
2	実施結果	・参加中小企業　6 社に導入。 ①インシデント件数 ・Defender サービス停止の検知 0 件（本ツールに関する問合せなし） ②本実証にてわかったこと ・基本的にアンチウイルスソフトは導入済みのため Defender を使用しておらず、前提条件に合う企業が少ない。 ・アンチウイルスソフトが導入済みである理由としては、いくつか要因が考えられる。 - ウイルスのリスクについては認知度が高く対策済み - アンチウイルスソフトの低価格化 - Defender ツールが有用との認識が無かった
3	今後の課題	・Widnows Defender がアンチウイルスとして無償で利用可能であることの周知

4.3.2 エンドポイントに関するセキュリティ対策（Web 対策ツール）

Web 対策ツールは 41 社への導入であり、不正サイトとしてブロックされた件数は合計で 624 件だった。なお、そのほとんどが「違法ソフト・反社会的サイト」となっている。ブロック数が多い企業は一部であり、75%の企業ではブロック数が 10 回以下であった。反対に一部の企業では 200 回近くブロックされていることがわかる。今回採用した Web 対策ツールではブロックされる際にブラウザー上で明確なブロック通知が表示される。そのため意図的にブロック対象のサイトを閲覧しようとしたユーザーに対しては 2 回目以降の閲覧に対する抑止力となり、同一ユーザーにおいてブロックが頻発することは少ない。

ただし、上述した企業では同一ユーザーによるブロックが頻発していることから、ユーザーが意図的に閲覧しようとしているのではなく、Web ページ内に隠されて接続されているか、もしくはブラウザー以外の通信によってユーザーが意図せずに不正サイトにアクセスされている可能性も考えられる。

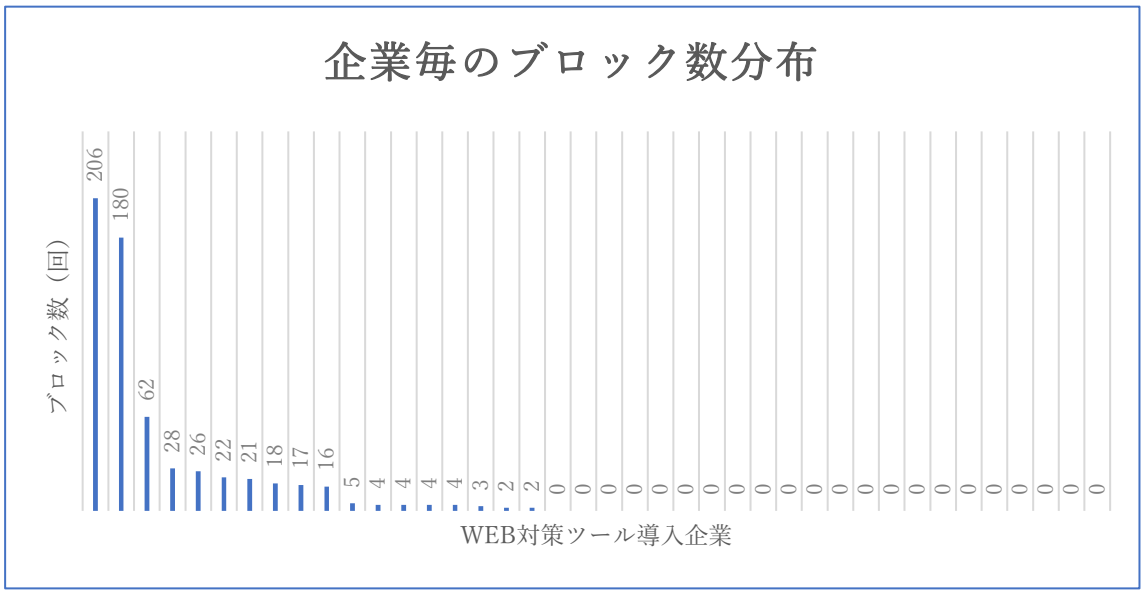

図 4.15 企業別 URL ブロック数

なお、今回 Web 対策ツールを導入した企業において、一部から「インターネットの接続が遅くなった」との声が聞かれた。Web 対策ツールではサイトにアクセスする際に、最初にベンダーのデータベースサーバーへ問合せをし、アクセス先がブロック対象か否かを常時照会している。そのため導

入した企業のネットワーク環境（特にインターネット接続が早くない場合）によっては導入前よりもアクセス速度が遅いと体感する可能性もある。こちらについてはセキュリティ対策における安全性と利便性のトレードオフとも思われるが、中小企業においてはインターネットへの接続環境が不十分である状況も十分に考えられるため、今後お助け隊として提供するサービス選定時の課題とすべきポイントである。

実証開始当初は、Web 対策ツールの導入企業数が全く目標に届かない状況であった。そのため導入企業（実証参加企業）を再度募るための訴求を行い、ようやく目標数に達した経緯がある。なお、説明会時点では Web 対策ツールの機能として「Web フィルタリング」と紹介し、「PC の私的利用防止」をアピールしていた。再募集においては「標的型攻撃メールの URL リンク対策」について訴求したところ導入企業が増加している。このことからセキュリティ対策ツールの機能を説明する際に、ユーザーが気にしているキーワード（今回では「標的型攻撃」）を使用することで訴求力を向上させることができると身をもって体験した。

表 4.11 Web 対策ツール結果概要

項	項目	内容
1	実施内容	現地の PC に「i-FILTER ブラウザー＆クラウド」のエージェントを導入。定期的にリモートにてブロックログを確認。
2	実施結果	・参加中小企業 41 社に導入。 ①インシデント件数 ・不正サイトのブロック数：624 件 →不正サイト等の傾向が強い。また平均的ではなく一部企業におけるブロック実績が多い。 ②導入時の問題点 ・導入前よりも Web アクセスが遅くなったとの申告あり。経路が増えるためやむを得ない部分あり。 ・当初は導入希望が少なかったが、「URL リンク型の標的型攻撃メールにも効果的」を訴求したところ、導入希望が増えた。
3	今後の課題	・　セキュリティと利便性のトレードオフを認識してもらう。 ・　導入判断のための知識を付ける教育機会が必要。 ・　セキュリティ対策の機能についてはユーザーが気にしているキーワードで訴求すべきである。

4.3.3 メール受信に関するセキュリティ対策（メール対策ツール）

メール対策ツールは 7 社への導入となった。デジタルアーツ社の m-FILTER@Cloud を採用したが、前提条件がやや厳しいため導入目標数を 5 社としていた。セキュリティインシデントとしては標的型攻撃メールについての検知は無く、スパムメール受信が 60 件となっている。本実証においては、メール対策の導入における敷居の高さを実感した。今回のメール対策ツールでは、クラウド上にあるデジタルアーツ社のメールサーバーを経由させることで、各種メールセキュリティ機能を実装することが可能となる。ただしその場合はデジタルアーツ社のメールサーバーから導入企業のメールサーバーを経由してメール送信をすることになるため、メールの踏み台対策として企業のドメイン名設定に対して TXT レコードを追加する必要がある。このような条件を付けることで企業のドメインに対して管理権限のある、正しい管理者であることを判定している。更に企業が使用しているメールサービスのスパム判定機能を回避するための詳細なルール設定等が必要となり、これらを中小企業が単独で実装することの難しさを理解した。

メール対策ツールについてはゲートウェイ型の入口対策であるため、比較的従業員数の多い企業において費用対効果のあるセキュリティ対策と言えるが、従業員数が多ければメール関連の設定変更における業務影響やリスクも大きくなるため、簡単には実装に踏み込めない状況であることも理解できた。

なお、今回導入した企業の中には、導入後にメールの配送遅延が発生した。これは今回提供した Web 対策ツールの環境が試用版環境であり、お客様のメール送受信量が想定よりも多かったことが原因であった。当日のうちに遅延については解消されたものの、メール対策におけるリスクを露呈した形となった。今後お助け隊として提供するサービスは安価であることが大前提になると思われるが、導入時のリスクが高いことはそのまま導入費用にも反映せざるを得ないため、導入時のリスク考慮についてもサービス選定時の課題とすべきポイントと思われる。

表 4.12 メール対策ツール結果概要

項	項目	内容
1	実施内容	実証参加企業メールサーバーと m-FILTER@Cloud を連携
2	実施結果	・実証参加中小企業　7 社に導入。 ①インシデント件数 ・標的型攻撃メール（疑い）の受信：0 件 ・スパムメール（疑い）の受信：60 件 ②導入時の問題点 ・中小企業においては取引先がフリーメールを使用していることも多い。 →初期設定では一旦保留される（承認処理が必要） ・今回の前提条件が厳しい→導入作業時の業務影響リスクもある。
3	今後の課題	・　運用ポリシーの策定 ・　安価なサービスの提供

4.3.4 ネットワークに関するセキュリティ対策（UTM 導入）

UTM 導入については 29 社への導入となった。導入サービス計画時には 10 社を目標としていたが、本サービスを希望する企業が多かったため、可能な範囲で導入企業数を増加することとした。

現地駆け付けを必要とするような重大インシデントについての発生は無かったが、事前に脅威をブロックするインシデントについては合計で 400 万件を超える数を検知した。これは導入企業 1 社 1 日平均で 500 件を超える数の検知数となっており、中小企業においても日々のサイバーセキュリティの脅威にさらされている実態を認識することができた。本サービスで検知した主な内容を以下に示す。

表 4.13 UTM 導入にて検知された主なインシデント

項	分類	項目	内容
1	外部→内部 （入口）	マルウェアの 事前検知・駆除	19 件
2		外部からの 不正アクセス検知および防御	576 件
3	内部→外部 （出口）	マルウェアの事後検知	0 件
4		不正 URL へのアクセス （ブロック）※1	4,286,363 件（Web 広告、詐欺サイト、フィッシングサイト）
5		不正サイトの検知 （ブロック）※2	26 件

※1　予め指定された URL へのアクセス制御機能によってブロックされた件数

※2　Web サイトにアクセスした際に不正なサイトであることを動的に検知し、ブロックした件数

特筆すべきは入口対策としてマルウェアの事前検知・駆除で 19 件、不正アクセス検知・防御で 576 件の防御実績があったことである。今回の UTM による防御が無かった場合、実際に感染していた可能性も大いにあり、改めて中小企業におけるサイバーセキュリティに関する脅威およびその対策の重要性を把握することができた。

その他の脅威としてはブロックした不正 URL において 99.99%が広告サイトとなっており、重大なインシデントを危惧するデータではないが、ごく一部ではあるものの詐欺サイトやフィッシングサイトについてもブロックしており、ここからも Web 経由でのサイバーセキュリティに関する脅威を把握することができた。

表 4.14 ブロックされた不正 URL 種別の割合

項	不正 URL 種別	割合
1	Web 広告	99.99%
2	詐欺サイト フィッシングサイト スパム	0.01%

なお、UTM 導入においては導入時に事前に導入先の環境確認を行うが、一部の企業では条件が合わない状況であることが判明した。導入時には NW 機器としてルーターが必要となるが、調査の結果ルーターが存在しない場合は NTT 西日本より無償提供を行った。

しかし、NW 環境が変更されることになるため、残念ながら UTM 導入を辞退する企業も存在した。

表 4.15 UTM 導入結果概要

項	項目	内容
1	実施内容	現地のネットワーク上に統合脅威管理装置（UTM）を導入し、インシデントの監視を実施。
2	実施結果	・実証参加中小企業　29 社に導入 ①インシデント件数 ・平均 約 512 件/日・社 主な内容:悪意のある URL へのアクセス（事前にブロック） ・駆け付け支援が必要なインシデントは発生 0 件 ②導入時の問題点 ・実証参加企業はネットワーク構成を正確に把握できていない場合が多いため、サービス提供事業者による実証参加企業環境の現地調査が必要となる。 ・実証参加企業のネットワーク構成によっては、ルーターを増設しないと UTM を導入できないケースがあった。ルーター貸出の無償提供も案内したが、ネットワーク構成は変更できないとのことで実証事業参加を辞退した。 ・実証期間終了後の継続については全ての企業で辞退しており、継続時のコストを懸念したと推察。
3	今後の課題	・安価なサービス提供

4.4 問合せ窓口への問合せ結果

本実証事業にて設置した問合せ窓口への問合せ結果を以下に示す。結果として UTM 導入に関連する訪問対応以外では 2 件のみの問合せとなった。

表 4.16 問合せ・駆け付け状況

対応種別	総計	相談・インシデント等対応状況	発生件数
問合せ窓口対応	2 件	実証参加に関する問合せ	0 件
		セキュリティ機器設置等の問合せ	2 件
		セキュリティ対応の相談	0 件
		その他	0 件
インシデント対応	0 件	電話およびリモートによるインシデント対応	0 件
		訪問によるインシデント対応（駆け付け）	0 件
その他訪問対応	51 件	機器設置等のトラブル対応	2 件
		その他（セキュリティ機器の導入・設置支援等）	49 件

【1 件目】

実証参加企業にて Web 対策ツールのインストールを実施したが、インストーラの場所がわからないとの問合せであった。後方支援部隊にエスカレーション後に確認したところ、提供した手順書のバージョンが古かったことが判明。手順書をメールにて再送後インストーラの場所を提示し、最終的にインストールを完了することができた。

表 4.17　1 件目の問合せ概要

項	項目	内容
1	問合せ内容	インストール手順について不明な点がある。
2	関連するサービス	Web 対策ツール
3	駆け付け対応	不要
4	最終対応者	後方支援（第二ライン）
5	根本原因	送付した手順書の不備。
6	対応結果	最新版を個別に送付し、インストーラのダウンロード方法を指南。その後無事インストールを完了できた。

【2 件目】

メール対策ツールを週末に導入し、翌営業日午後での問合せであった。当初は「メール対策ツールから送信されたと思われる承認確認メールが届いたが、対応方法がわからない」（事象 1）という内容であった。これは宛先がフリーメールの場合は承認処理が必要となるが、事前説明が漏れていたために問合せる結果となった。本来であれば実証参加企業の代理で承認処理を実施することで対応可能のはずだったが、ここで管理ページにログインできないという事象が発生した（事象 2)。また対応中にメール送受信が遅延しているという状況も判明した（事象 3)。メーカーの担当者にも支援をもらい、事象 2 と 3 の原因はクラウドサーバー側のパフォーマンス不足であることが判明し、クラウドサーバー側で調整した結果その後自然復旧となった。今回は無償評価用環境の想定以上の負荷が発生したことが原因であったが、この結果一部の業務に影響が出たことで迷惑をかけることとなった。

また、後程判明したことだが、当初はお実証参加企業が問合せ窓口のフリーダイヤルに電話をかけたものの、IP 電話を使用していたためフリーダイヤルにかからなかったことがわかった（事象 0)。この結果より、今回の問合せに関して想定外の事象が 4 件発生しており、該当企業には心配と迷惑をかけることとなった。

本問合せ結果より、問合せ窓口の連絡先としてはフリーダイヤルのみではなく通常の外線番号も伝えることと、メール対策ツールについて処理が必要な場合の対応手順の事前説明および導入企業のメール使用状況（負荷量）について事前に確認すべきであることがわかった。

表 4.18　2 件目の問合せ概要

項	項目	内容
1	問合せ内容	事象 0：フリーダイヤルにかからない 事象 1：承認確認のメールが届いたが、内容がわからない 事象 2：管理ページに接続できない 事象 3：メール送受信が遅延
2	関連するサービス	メール対策ツール
3	駆け付け対応	不要
4	最終対応者	後方支援（第二ライン）
5	根本原因	事象 0、1：事前説明の不備 事象 2、3：環境確認の不足
6	対応結果	事象 0　：営業経由での連絡 事象 1　：管理ページより代理で承認作業を実施 事象 2、3：クラウドサーバー側でパフォーマンスを調整後、自然復旧
7	その他	・対応中にクラウドサーバーのパフォーマンス不足が発生し、個別に対応した。 ・企業からは当初問合せ窓口のフリーダイヤルに電話したが繋がらず、担当営業経由での連絡となった。

4.5 駆け付け支援およびヒアリングの実施結果

本実証事業では駆け付け支援については事案が発生しなかった。そのため駆け付け支援実施時に想定していたヒアリングについても、回答数は 0 件となっている。駆け付け支援が発生しなかった件について想定される理由としては、セキュリティインシデント相当の問合せが無かった事が直接の理由であるが、そもそも問合せ窓口への問合せ件数自体が少なかったたことが挙げられる。当初より駆け付け支援については問合せ件数全体のごく一部と想定していたが、その母数自体が少なかったために駆け付け支援を必要とする問合せも発生しなかったと想定される。

もう一つの理由として、今回提供したサービスが基本的にリモート管理可能であったことも上げられる。前述した問合せ内容の 2 件目では「メール送受信の遅延」という一部業務への影響が発生するような問合せであり、セキュリティインシデントではないものの、従来であれば現地対応も必要となるケースであった。ところがメール対策ツールはクラウドサービスであるため、後方支援部隊およ

びメーカーも含めてリモートで対応できた事が、駆け付け支援の実施件数が 0 件となった事を象徴していると思われる。

以上より、今後はクラウドを利用した製品提供も増えてくることが予想され、それに伴い緊急時の顧客への対応についてもリモートで対応できる機会が多くなると思われる。現地への駆け付け対応のために人員等を常時確保しておくことは当然コストがかかり、最終的に中小企業へのサービス提供費用に反映される。今後はリモート対応を前提とすることで安価でかつ、いざというときにも安心できる、中小企業のニーズに対応したサービスが提供できると思われる。

4.6 報告会等による実証事業成果の周知

成果報告会も事業説明会と同様に Zoom によるオンライン開催とした。名古屋商工会議所のホームページへの掲載、事業開始説明会の参加者、事業開始説明会とは個別に実証事業参加を募った企業向けにメールによる案内を行った。なお参加申込時には実証参加企業には実証内容についてのアンケート、また今後のサイバーセキュリティお助け隊に求めるサービス内容等のアンケートに回答してもらった。

以下に開催場所、開催日、参加企業数、実証事業参加の中小企業数を記載する。

表 4.19 成果報告会実績

項	事業説明会開催場所	開催日	参加企業数
1	Zoom によるオンライン開催	2021 年 1 月 14 日	29 社

4.6.1 実施内容

成果報告会では、実証事業実施状況の成果報告とサイバーセキュリティの普及啓発を行い、事業説明会と同様にオンライン形式での開催として以下の内容にて実施した。

・ サイバーセキュリティお助け隊の成果報告。

  ・ 本実証事業の目的、実施内容とスケジュール、実施体制、成果報告の概要を説明

  ・ 実証参加企業の状況、中小企業の実態データの分析結果、本実証事業の実証実績の報告を実施

・ 実証結果を踏まえた中小企業に推奨するサイバーセキュリティ対策案

・ サイバー保険の概要と今後の方向性の説明。

・ 中小企業の支援施策内容の紹介。

・ 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介。

以下に成果報告会実施時のアジェンダを記載する。

表 4.20 成果報告会アジェンダ

項	時間	報告項目	発表者
1	13:30～13:35	主催挨拶	名古屋商工会議所
2	13:35～14:15	サイバーセキュリティお助け隊の成果報告	日立システムズ 東京海上日動
3	14:15～14:30	中小企業における情報セキュリティ対策支援のご紹介	IPA

図 4.16 成果報告会実施風景（Zoom 配信会場）

4.6.2 アンケート結果

なお、成果報告会の実施にあたり参加者には事前にアンケートに回答してもらった。一部は実証事業の参加者向けの内容となるが、参加していない企業からも回答を得た。

1) セキュリティ対策に関するサービスに求める内容

今後提供して欲しいセキュリティ対策関連サービスについての設問では、「相談窓口」との回答が多かった。ただし今回の実証にて用意した問合せ窓口（コンタクトセンター）に対し、相談に関する問合せは 0 件であったことを考慮すると、必要とされているのは単に窓口を用意するのみではないと思われる。

次に多いのは安価なセキュリティ対策製品となっている。中小企業が許容するセキュリティ対策における月額費用については後述するが、高額な統合製品よりも安価な部分対策製品が求められるのが実態である。ただしどの部分の対策をするかについてはセキュリティに関する全般的な知識も必要であることから、本来必要とされるサービスとしては上述した相談窓口も絡めた必要最小限のセキュリティ対策と言えるかもしれない。

3 番目に多い要素としてはサイバー保険となった。ただ、こちらも後述するサイバー保険加入率から推察するに実際のサイバー保険における理想と現実の差があると思われる。

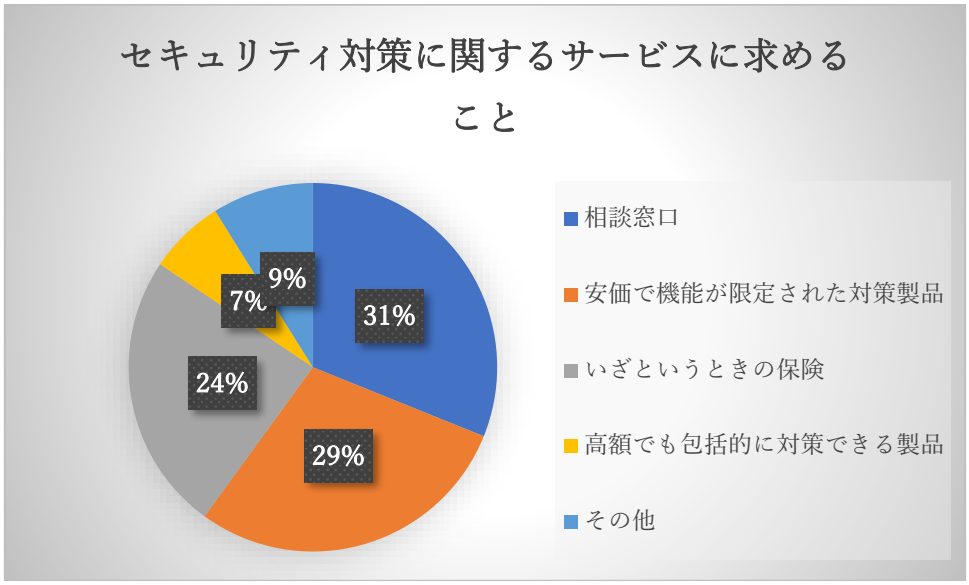

図 4.17 セキュリティ対策に関するサービスに求めることに対するアンケート結果

2) セキュリティ対策への月額予算

セキュリティ対策への月額予算については大きな差異は無かったものの、比較的 1 万円以内が主流と思われる。そのため今後お助け隊として提供するサービス選定時にはこれらの価格帯を意識する必要がある。また未回答となった企業も多かった。予算はあるものの企業情報として回答できないという状況もあるかと思うが、まだ検討段階である企業も多いことが予想される。

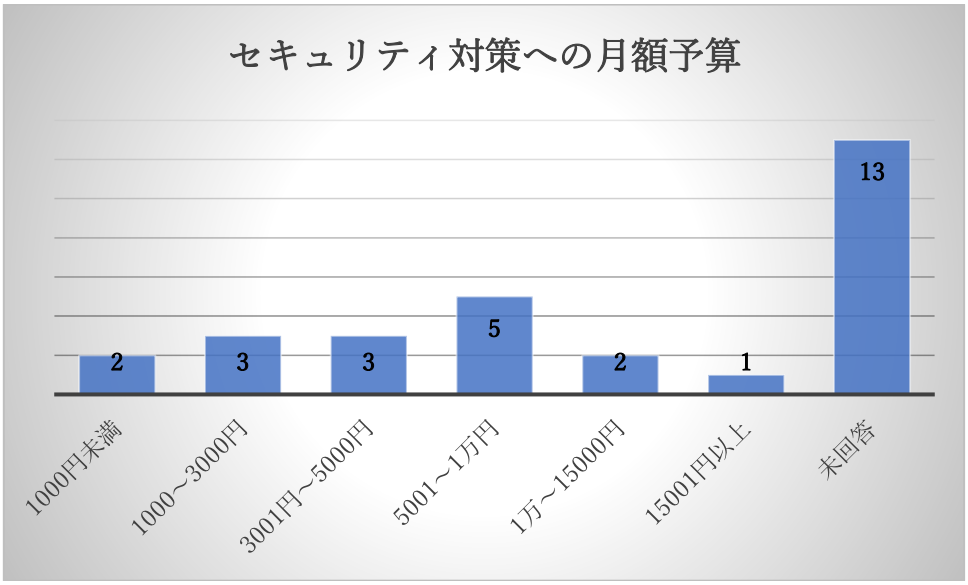

図 4.18 セキュリティ対策への月額予算に対するアンケート結果

3) サイバー保険への加入状況

最後にサイバー保険への加入状況についての設問では、加入済みの企業は 3%にとどまった。未加入の理由では「内容をよく知らない」が多く、上述した「サービスとして求める内容」のアンケート回答において「サイバー保険」が上位であるにも関わらず未加入企業が多い実態の理由としては、やはり企業へのサイバー保険内容の周知が不十分であることがうかがえる。

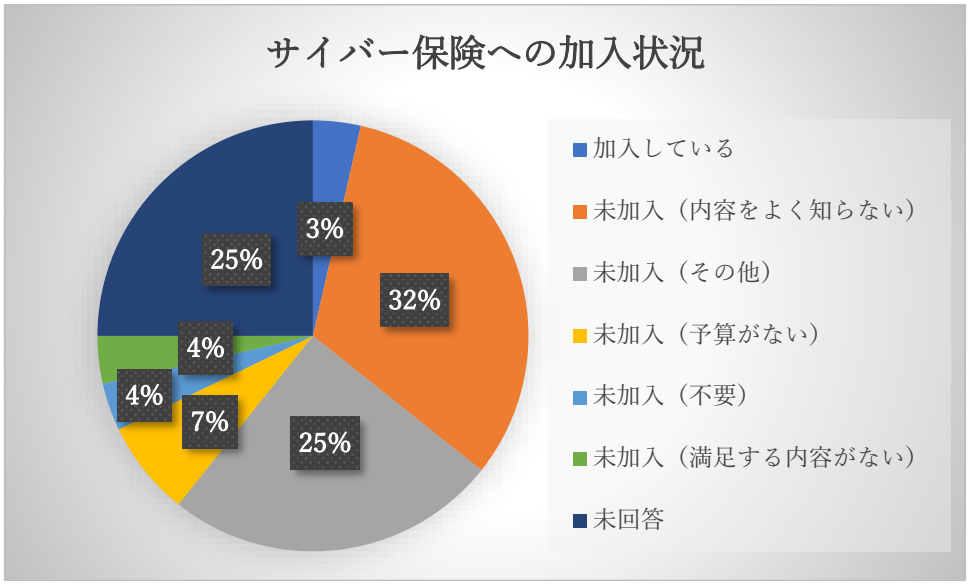

図 4.19 サイバー保険への加入状況に対するアンケート結果

5. 考察

5.1 実証参加企業におけるサイバー攻撃の実態

本実証結果では重大インシデントは発生しなかったものの、中小企業が日々サイバーセキュリティの脅威に脅かされている実態が判明している。本実証事業にてインシデントが発生しなかった理由として、まず一つ目にはアンチウイルスソフトの導入率が高いことが挙げられる。前述のとおり、アセスメント結果では実証参加企業の 9 割以上でアンチウイルスソフトが導入済みであり、このことから最低限のセキュリティ対策が実施されているためにインシデントが発生しなかったと推察される。

二つ目の理由としては、今回提供したサービスによって事前にインシデント要因を検知・防御できていたことが挙げられる。特に Web アクセスにおいては Web 対策ツールおよび UTM 導入を合わせて四百万件以上の Web アクセスを事前にブロックしており、このように悪意のあるサイト等から利用者を事前に防御できたことで、インシデント発生を抑える効果に繋がったものと推察される。

5.2 実証不参加理由分析

今回の実証期間にてサービス導入に至らなかった企業の中で、未導入の理由について確認したところ多かった理由は「対策済み」であった。ただし本実証の提供サービスとしてはエンドポイント・Web・メールと複数の対策ツールを用意しており、現在の中小企業の実態から全ての要素において対策済みの企業が多いとは言えない状況において未導入の理由として「対策済み」が多かった件に対しては、説明会等における提供サービスの説明・周知をもっと十分にすべきだったと思われる。

少数意見とはなるが「その他」の内容として「情シス部門が判断するため」「説明会の内容が理解できなかった」といった意見も見られた。本実証ではあまりスケジュールの余裕が無かったため周知・説明の機会があまり取れなかったが、本来はもっと時間をかけて、また説明会に参加する担当者についても導入要否・可否について判断できる担当者を予め選定して参集することにより、サービスの導入企業をもっと増やすことができた可能性がある。

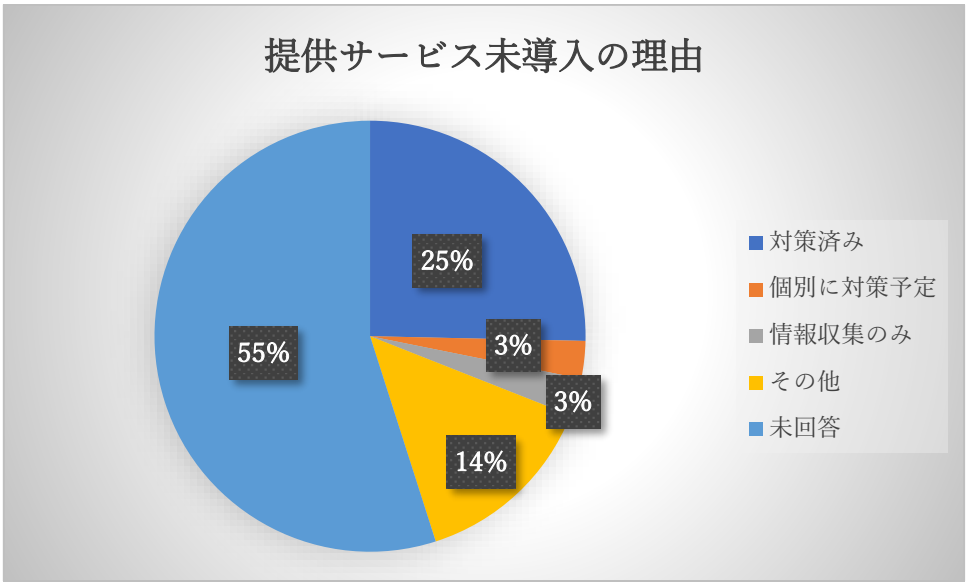

図 5.1 提供サービス未導入の理由

5.3 中小企業におけるセキュリティ対策を進める上での課題

本実証を通して、中小企業におけるセキュリティ対策を進める上での課題がいくつか判明した。課題とその内容について以下に示す。

① リスクを把握できていない、知識不足

企業においてそもそもセキュリティの脅威に対する知識が少ないため、リスクが把握できず、本来必要となるリスク対策の必要性を理解してもらえないという実態がある。

② 安全性と利便性のトレードオフへの理解

セキュリティ対策製品と導入環境の相性によっては、導入後に一部のパフォーマンスが低下することも考えられる。これはサイバーセキュリティ分野に限られたことではないが、安全性・利便性・費用において全てを満足することは難しいという点を理解してもらう必要がある。

③ セキュリティ対策の予算

本実証事業で把握できた中小企業のセキュリティ対策の予算としては、月額 1 万円未満という状況であった。セキュリティ対策の実施率を上げることを優先するのであれば、この金額を踏まえた上で今後の提供サービスを選定する必要がある。ただし、予算については中小企業の規模によるため本

来は一概に語ることは難しい。必要なことはリスクを把握した上で、企業毎に費用対効果が見込まれる範囲に収まるセキュリティ対策を導入すべきである。

④　導入作業時におけるリスク

セキュリティ対策製品の一部、特に入口・出口対策となるゲートウェイ型の製品については、導入時に業務影響が発生するリスクがある。SI ベンダーにおいてこのようなリスク作業は通常だが、その場合はスケジュールや手順・体制等を考慮した上で費用に反映されるのが一般的である。しかし安価なサービス提供を目指すには、導入時のリスクをどのようにリスクヘッジするかが課題となる。

⑤　セキュリティ要員の人材不足

事業説明会の事前アンケート結果より、セキュリティインシデント発生時の対応要員については約半数の企業で「不在もしくは不明」という状況であった。また成果報告会の事前アンケートにて今後希望するサービスとして「相談窓口」を希望される企業が最も多かったことについても、各企業にセキュリティに詳しい人材がいないという実態に起因していると推測される。

⑥　マルウェアに対する対策

簡易セキュリティアセスメントの結果より、従来型のアンチウイルス対策の実施率は 9 割であったのに対し、ふるまい検知型のアンチウイルス製品については 3 割を下回っていた。この点についても従来型対策のみにおけるリスクが把握できていない、従来型とふるまい検知型の違いについての知識が不十分という課題と関連していると思われる。

⑦　出口対策

簡易セキュリティアセスメントの結果より、出口対策が不十分という結果であった。出口対策は、万が一企業内部でマルウェア等に感染した場合でも社外サーバーとの通信を防御する最後の要となる部分ではあるが、このような二次被害へのリスク対策は費用対効果が見えにくく、対策が後手に回っていると推測される。

5.4 中小企業において必要なセキュリティ対策

中小企業において必要なセキュリティ対策について以下に述べる。「セキュリティ対策を進める上での課題」を考慮した上で、セキュリティ対策を考えるにあたり以下の３つの方針が必要との認識である。

◆　出口対策・マルウェア対策

本実証事業での簡易セキュリティアセスメント結果より、出口対策全般の実施率が低いことが判明している。そのために中小企業全般としてまずは出口対策を実施することで、情報漏えい等の被害拡大を防ぐことが最優先と考える。そのための対策ツールとしては常に不正サイト情報を更新し、不正サイトへの通信を検知・ブロックできる製品が必要となる。

◆　セキュリティ知識が無くとも導入判断できる

多くの中小企業において専門的なセキュリティ知識を持つことは難しいため、セキュリティ対策の導入については「導入判断を相談できる窓口がある」もしくは「専門知識が無くとも導入判断ができるサービスを提供する」のいずれかになる。本実証事業での問合せ結果がほぼ皆無であったことからもわかるように、単純に窓口を用意すれば良いというものではなく、企業から信頼される雰囲気が必要と思われる。一方で難しい導入判断をする必要の無い、包括的なセキュリティ対策を提供できるサービスとすることで、導入判断のハードルを下げるのも一つの手段と思われる。UTM のような総合対策製品が考えられるが、ただしこの場合は比較的費用が高額となる可能性があり、次項の費用対効果との兼ね合いになるものと思われる。

◆　費用対効果が見込める

企業が導入するセキュリティ対策について、費用対効果があると認識してもらう必要がある。費用については認識しやすい一方でセキュリティの効果というものはなかなか把握しづらい特性を持っている。セキュリティ対策とは「脅威が発生していない」ことこそが効果と言えるが、その点を企業のステークホルダーに認識してもらう必要がある。もしくは、導入した対策ツールによって回避できた脅威（不正通信のブロック、駆除したマルウェアの名前）について、例えば月次レポートのような形で定期的に報告するサービスを組み込むことで、対策ツールの効果について認識してもらうこと

はできると思われる。

以上を踏まえた上で、Pit-Nagoya としては下記のセキュリティ対策を推奨する。

1. UTM の導入

セキュリティ対策を導入するにあたり、最初のハードルは担当者による導入製品の選定である。ただし必要十分な製品を選定するには現在のセキュリティ対策状況をはじめ、Web やメールといった各 IT インフラの状況を把握していることが必要となる。更にそれら IT インフラへの対策製品の有効有無等を判断する必要もあり、IT・セキュリティ知識が十分でない担当者にとっては判断が難しいと言わざるを得ない。

そのため出口対策・マルウェア対策も含め包括的にセキュリティ対策を講じることができる UTM（総合脅威管理装置）であれば、既存 NW への機器の接続であるため視覚的にも認識しやすく、導入可否についての判断も比較的容易と思われる。ただし UTM は機器にもよるが比較的価格が高価となるため、導入する企業の人員規模によっては費用対効果が見込めないという判断もありえる。その場合は以下に述べるエージェント型 Web 対策ツールを推奨する。

2. エージェント型 Web 対策ツールの導入

従業員数および対策すべき PC が少ない企業においては、PC 単位に導入可能なエージェント型の対策ツールの導入を推奨する。導入方法は基本的にエージェントを各 PC にインストールのみとなり、また費用については製品により異なるものの、1 ユーザー1 月あたり数百円で導入可能であるため費用対効果も見込める。また検知対象をブラウザー通信に限定しない Web フィルタ系の製品とすることで、マルウェア感染後の外部攻撃命令サーバーとの通信をブロックし被害を最小限にとどめることが期待できる。

5.5 中小企業におけるセキュリティ対策の効果

本実証を通した中小企業におけるセキュリティ対策の効果について以下に述べる。

5.5.1 事業説明会

安価なセキュリティ対策ツールとして Windows Defender を紹介したところ、「無償のアンチウイルス機能として Defender が利用できることを知らなかった」、との意見があった。この実証参加企業は既に有償のアンチウイルスソフトを使用していたが、このように Defender 機能を知らずに有償アンチウイルスソフトを利用していた企業においては、今後ウイルス対策を Windows Defender に移行することにより、今まで使用していた有償のアンチウイルスソフトへの投資を別のセキュリティ対策に割り当てることができ、今後のサイバーセキュリティリスクの低減に期待できる。

5.5.2 簡易セキュリティアセスメント

結果レポートの内容を確認した実証参加企業より、「改めてセキュリティの確認をして行く必要があると感じた」との意見があった。結果レポートを見た他の実証参加企業においても今後のセキュリティ対策を考えるためのきっかけとなることが期待できる。

5.5.3 Web 対策ツール

不正なサイトについて Web 接続を実際にブロックできた。ブロック対象となったカテゴリはほぼ「違法ソフト・反社会的サイト」であることが判明しており、ユーザーに対して不正なサイトであることを認識させることができた。これにより不正なサイトにアクセスすることに対する危機感と、フィルタされたことにおける安心感を与えることができ、今後のセキュリティへの意識向上に繋がることが期待できる。

5.5.4 メール対策ツール

スパムメール（疑い含む）について検知することができた。なお、今回導入された実証参加企業の中に継続利用を望まれる企業があり、本実証への参加をきっかけとして今後のセキュリティへの意識向上に繋がったと思われる。継続希望された企業については、引き続き Pit-Nagoya にて対応して行く。

5.5.5 UTM 導入

UTM 導入により多数のマルウェアの事前駆除および外部からの不正アクセスについても防御した実績を確認できた。これらの概要については月次レポートとして実証参加企業に送付されている。これにより今回 UTM が導入されていなければマルウェア等に感染していたかもしれないというセキュリティリスクについて認識できたものと思われる。

なお、今回 UTM 導入した企業においては継続希望する企業はいなかったものの、UTM の駆除実績等について認識してもらうことにより、UTM の撤去後はネットワークが保護されないことへの不安を感じ、今後のセキュリティ対策を考えるためのきっかけとなることが期待できる。

上述したセキュリティ対策の効果概要について以下に示す。なお本実証に参加した企業より、提供サービス全体を通して継続利用時の費用等について問合せがいくつかあった。本実証への参加をきっかけとして今後のセキュリティへの意識向上に繋がったと思われる。これらの企業についても、引き続き Pit-Nagoya にて対応して行く。

表 5.1　セキュリティ対策の効果概要

項	項目	内容
1	技術面での効果	・スパムメールの検知 ・マルウェアの事前駆除 ・外部からの不正アクセス防御 ・不正 URL へのアクセスをブロック ・不正サイトへの接続をブロック
2	心理面での効果	・導入サービスの継続希望、あるいは継続時の概算費用の問合せあり。 ・改めてセキュリティ対策について再認識した。 ・無償のアンチウイルスについて理解 ・実績を認識頂くことで、今後のセキュリティ対策を検討するきっかけとなることが期待される。
3	備考	実証参加企業からはその他に下記のような意見が挙がった。 ・メール内の URL からフィッシング被害を受けることが　多いので、それが防げるのであれば導入メリットがある。(Web 対策ツール) ・メールサーバーの機能も一緒に含めて、設定済みで販売してくれると色々と手間が省けて良い。(メール対策ツール)

6. 実証を踏まえたビジネス化に向けた検討

6.1 中小企業向けセキュリティビジネス化に向けた課題・検討

本実証事業の実証結果を元に、中小企業等の実態やニーズに応じた必要なセキュリティ対策サービスの検討内容について以下に示す。

6.1.1 提供サービス

提供するサービスとしては「UTM」「エージェント型 Web 対策ツール」（以下 Web 対策ツール）の二種とする。基本的な考え方としては、保護対象となる PC が 10 台程度までであれば Web 対策ツール、それ以上は UTM を推奨とする。当然、UTM と Web 対策ツールでは保護する範囲が異なるため、利用用途が機微な情報を扱うもしくは社会的重要性などがある企業の場合は、台数のみでの判断基準とすべきではないことを併記しておく。上記の判断基準はあくまでも目安であり、サービス種類を絞り込み、かつ判断基準を明確化することで「どの対策製品を選択すれば良いのかわからない」といった悩みに対応するものである。なお、中小企業の実態として「パターンマッチ型アンチウイルスおよび OS パッチ最新化については対策済み」であることを基本としているため、これを実施していない企業についてはまずは Windows10 へのアップデートおよび Windows Defender の有効化を前提条件とする。

6.1.2 費用

成果報告会参加申込時のアンケートの結果より、セキュリティ対策への予算として月額 1 万円以内が主流という内容を考慮し、UTM については月額 1 万円以内、Web 対策ツールについては PC1 台あたり月額数百円程度として検討する。

6.1.3 体制

基本的には本実証の体制と同様に、Pit-Nagoya というコンソーシアムを中心にしてサービス提供することを想定している。UTM については本実証では NTT 西日本が直接提供する形であったが、今後は UTM および Web 対策ツールのいずれのサービスも Pit-Nagoya に所属する地域 IT ベンダー

によって提供することを想定している。

6.1.4 駆け付け支援

上述したサービスの費用については駆け付け支援等については考慮していない。今後の検討課題にはなるが、後述するサイバー保険における 1 階部分での対応（初回の駆け付けのみ無料）等をサービスおよび費用を組み合わせることで、中小企業にとって安心感のあるサービスを提供できることを目指す。

6.1.5 サイバー保険

成果報告会参加申込時のアンケート結果より「今後求めるサービス」として「保険」が 24%を占めていたことから、サイバー保険についてもサービスに加える必要があるとの認識である。上述したが、他サービスと組み合わせる・オプションとする等については今後の検討課題となるが、駆け付け支援を希望する企業については後述するサイバー保険の補償内容として提供できるようにすることも検討する。

6.2 サイバー保険の活用

6.2.1 実証のアンケート結果

中小企業におけるサイバーセキュリティ対策への意識について確認したアンケート項目について報告する。

① サイバーセキュリティ対策の意識について　図 4.7 参照

→「不十分」or「わからない」の回答が、92.6%（126/136）

②サイバーセキュリティに対応できる要員がいますか　図 4.9 参照

→「いない」or「わからない」の回答が、50.7%（66/136）

③貴社でサイバーリスクが顕在化した場合の想定被害額は把握されていますか

→「把握していない」の回答が、97.1%（132/136）

④サイバーセキュリティ対策について今後、利用したいサービス内容について

→（Top1）サイバーセキュリティ相談窓口の提供、46.3%（63/136）

→（Top2）サイバーセキュリティ関連保険サービス、17.6%（24/136）

アンケートを通じ、企業のサイバーセキュリティ対策の意識・優先順位が低いと推察される。一方で、企業のニーズとしては、相談窓口や関連保険サービスの提供が必要と考えられる。

6.2.2 実証期間中のサイバーインシデント状況①

サイバー攻撃に関するアラート種別と検知状況については、 4.3.4（表 4.13 参照）のとおり、「外部からの不正アクセス検知および防御」576 件、「マルウェアの事前検知・駆除」19 件以外にも、「不正サイトの検知 （ブロック）」26 件があった。

6.2.3 実証期間中のサイバーインシデント状況②

上記（1）記載のとおり、企業のニーズとしては、相談窓口や関連保険サービスのニーズが高いと考えられるものの、4.4（表 4.16）および 4.5 に記載したとおり実証期間中のインシデント（駆け付け支援）発生件数は「機器設置のトラブル対応」「セキュリティ機器の導入・設置支援等」を除いて 0 件であった。

6.2.4 実証期間を通じて、わかったこと

各企業へのリスク周知と、対応するセキュリティ対策が課題であると推察される。

① 各企業のサイバーセキュリティ対策への優先順位が低い

アンケート結果からもわかるとおり、企業のサイバーリスク対策への認識・優先順位が低い実態があった。（6.2.1①参照） セキュリティ対応要員については半数近くの企業が「いない」、「わからない」という回答であり、実証参加企業の募集にも苦労した。また企業向けにニーズ喚起する実証事業者側のノウハウも不十分であり、「なぜサイバーセキュリティ対策が必要なのか」を周知できる体制整備と、企業のサイバーセキュリティ対策の優先順位を向上する広宣が必要。

② サイバーインシデントの発生リスクは依然高い

A,外部からの不正アクセス検知および無害化が 576 件発生（導入企業 10 社中）。

B,セキュリティ上のリスクがある不正サイトへの接続が 26 件発生（導入企業 10 社中)。

「外部からの不正アクセス（外→内)」のみならず、「不正サイトへのアクセスブロック検知」をはじめとした内から外へのアラートも発生。

こうしたヒューマンエラー（内部原因）による情報セキュリティ事故が台頭している実態も踏まえ、十分なサイバーセキュリティ対策をしていないと重大なインシデントが常に発生するリスクを企業が抱えていることがわかった。

③ 相談窓口の必要性および当該費用感

今回の実証にて設けたコンタクトセンターへの問合せは 0 件であったが（6.2.3 参照)、今後提供してほしいセキュリティ対策サービスとしては、「相談窓口」との声が多かった。(図 4.17)

一方で、3・5 記載のとおり、駆け付け対応には一定の費用がかかる。

中小企業の予算が限定的であることを鑑みると（図 4.18)、中小企業が許容するセキュリティ対策月額予算（1 万円程度）以内のサービス提供は必要と考えられる。(例：駆け付けサービス)

6.2.5 実証実験を通じて得られる保険の方向性

① 万が一の場合のサイバー被害額が巨額になると想定される一方で、サイバーセキュリティ対策への関心が低いもしくは優先順位が低い中小企業が多い実情を鑑みると、まずは事前の補償「各種セキュリティ商材（ハード面のセキュリティ対策)」を提供の上で、「最低限の費用（フォレンジック費用) 補償 (ソフト面のセキュリティ対策)」を付帯することがファーストステップ。

② その上で、サイバーセキュリティ対策に対する予算を確保できる中小企業に対しては、「上乗せ補償」として、名古屋商工会議所が提供するサイバーリスク補償を提供することで、充実した見舞金カバーを提供することが可能となる。

③ また、中小企業が IT 人材の不足に悩まされる一方で、実証実験結果より、緊急時のトラブル解消はもちろんのこと、通常（平常）時の対策についてもアドバイスを必要としていることがわかった。その観点では、サイバーリスク保険は事後の補償をカバーするだけでなく、事前の

補償「サイバークイックアシスタンス・サイバーエキスパートアシスタンス（相談サービス）」が付帯されており、有用であると言える。加えて、代理店が介在することでベンダーとは別の観点からアドバイスを受けられる。

6.2.6 商用化後の保険プログラムのイメージ

ユーザーのニーズに応じて、以下の 2 階立て補償を提供することを想定している。

1 階部分：「サイバーセキュリティお助け隊サービス」（全員加入）※「簡易型保険」

商用化されるサイバーセキュリティパッケージにバンドルする補償を組成する。

2 階部分：サイバーリスク保険　賠償責任部分・サイバーセキュリティ費用部分（任意加入）

希望するユーザーに提供する任意補償を組成する。

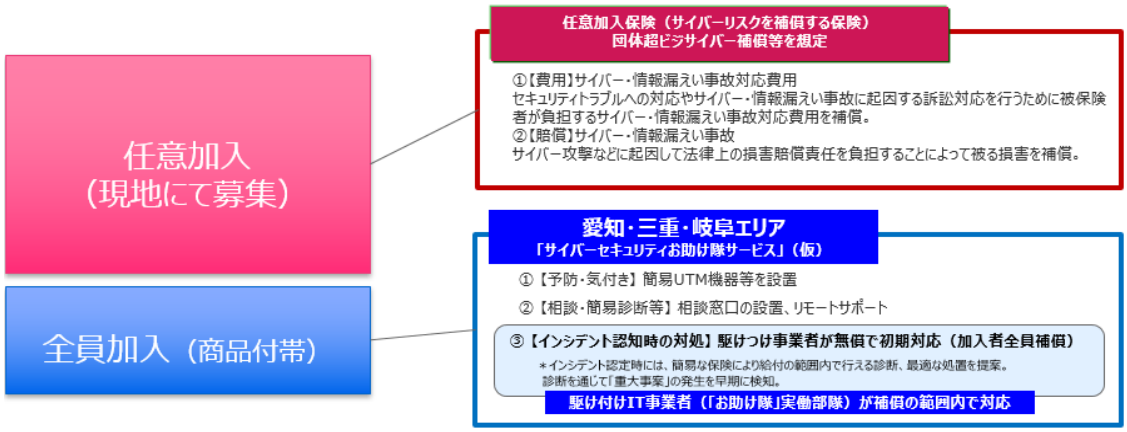

図 6.1 保険プログラムのイメージ

6.2.7 サイバーリスク保険の補償内容

サイバーリスク保険は、次の 3 つの補償により、事業活動を取り巻くサイバーリスクを包括的に補償する。

① 損害賠償責任に関する補償

自社ネットワークの所有・使用・管理等に起因して発生した他人の事業の休止または阻害や情報漏えい等について、被保険者が法律上の損害賠償責任を負担することによって被る損害を補償する。

② サイバーセキュリティ事故対応費用に関する補償

情報漏えい、不正アクセス等に起因して一定期間内に生じた不正アクセス等対応費用・再発防止費

用等や訴訟対応費用を被保険者が負担することによって被る損害を補償する。

③ ネットワーク中断に関する補償（オプション）

不測かつ突発的なネットワークの操作・データ処理上の過誤などまたは不正アクセス等に起因して、ネットワークを構成する IT 機器等が機能停止することによって生じた被保険者の①利益損害、②営業継続費用を補償する。事故発生から収束までの対応フローにおいて、各種費用が発生するが、サイバーリスク保険は以下のとおりトータルで補償することで、中小企業を守る。

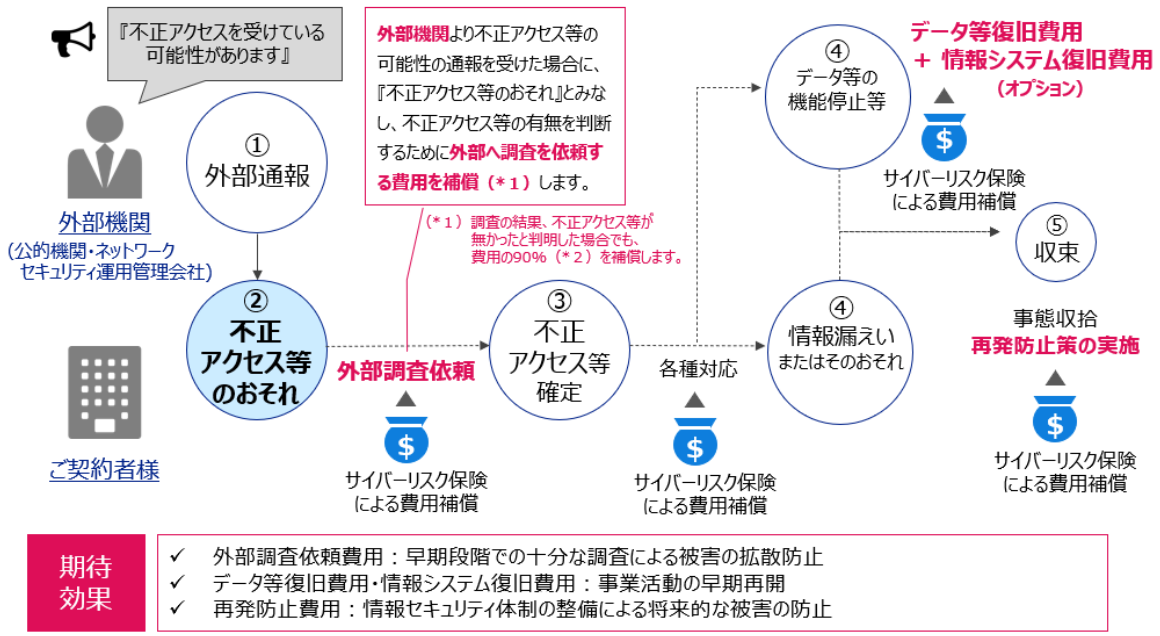

図 6.2 ネットワーク中断に関する補償のイメージ

(1) サイバーリスク保険のサービス（緊急時ホットラインサービス）

サイバーリスク保険では、保険による補償とは別に、「緊急時ホットラインサービス」が利用可能。事故発生時に、迅速な事態収拾のための支援サービスを提供する。

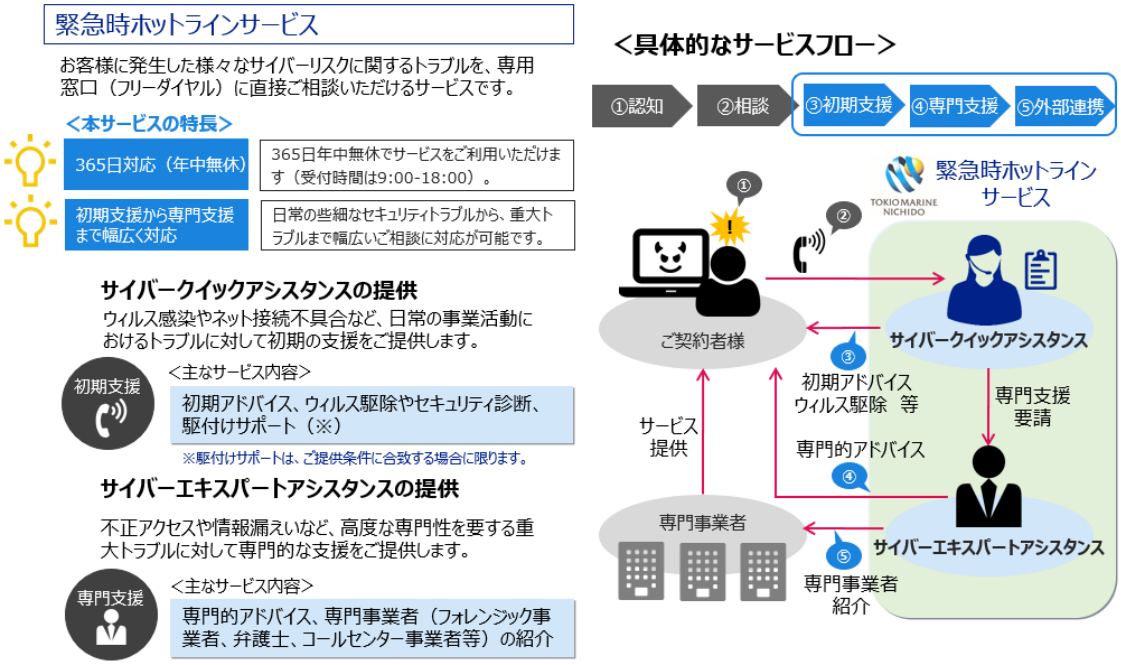

図 6.3 緊急時ホットラインサービスのイメージ

(2) サイバーリスク保険の提供を通じて

サイバーリスク保険をサイバーセキュリティ対策の 1 パーツとして組み込むことで、多くの中小企業の皆様へ安心と安全を提供すべく、手に取りやすい商品・サービスの創出を行う。保険の機能を活用してもらうことで、中小企業の事業基盤が強固になり、伸展する一助になれば幸甚である。

以上