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：岩手県）

成果報告書

請負事業者：富士ソフト株式会社

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

目次

サマリー

本報告書は、富士ソフト株式会社（以下「富士ソフト」という。）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。

岩手県内の中小企業 71 社を対象に、以下の 4 つ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。

- 簡易セキュリティ診断
- 中小企業等からのサイバーセキュリティに関する相談の受付および対応
- セキュリティ対策機器（ネットワークセンサー）の設置
- サイバーインシデントが発生した際の支援の提供

1. 背景・目的

1.1 背景

近年、サプライチェーン全体の中で、セキュリティ対策が整備されていな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いる。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いことが多く、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が多く発生している。

また、新型コロナウイルスの大規模流行に伴う政府による緊急事態宣言の要請により、企業・組織が在宅勤務などのテレワークを実施している。 このコロナ禍における緊急のテレワーク推進は、今後の社会の在り方が変わる大きなきっかけであり、企業・組織でテレワークは常態化していくと考えられる。しかし、テレワーク普及のためには、土台となる「セキュリティ対策」が必要だが、中小企業においては、この状況下において、セキュリティ対策整備が不十分であるにも関わらず、急務でテレワーク環境を構築したため、多くのリスクを抱えている可能性がある。

この状況は、中小企業が支える日本のサプライチェーンに、大きなセキュリティリスクを抱える可能性がある。まずはその状況を見える化し、中小企業の経営者および社員の意識改革を促し、セキュリティ強化に繋げる必要があると考える。

1.2 目的

本実証事業の目的は、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浸透・定着させることである。

1.2.1 コンセプト

新型コロナウイルスの影響により、テレワークの増加という背景を踏まえ、オフィスのみではなく、新たな作業環境を狙ったサイバー攻撃に対するリスクも併せた、中小企業のセキュリティ対策の把握を主眼とした実証事業を実施。

I. 地域一帯を 1 つの大きな単位としてセキュリティ対策母体とする手法の検証

II. コロナ禍を配慮した新たな働き方に即したサイバーセキュリティの実態把握

1.2.2 実証プロセス

説明会開催による意見交換、アンケート集計等での実態把握およびネットワーク通信状況の分析から、中小企業が晒されているサイバー攻撃の実態を見える化。

見える化された脅威への対策として、中小企業での課題・ニーズを明確にし、セキュリティソリューション、サイバー保険の在り方および地域密着の支援体制について検討・考察し、提言を実施。

提言としてまとめられた内容を、実証対象地域における中小企業向けサイバーセキュリティ支援対策に有効活用することで、実証対象地域でのビジネス化を検討する。（＝地域密着の新たなビジネスを創出）

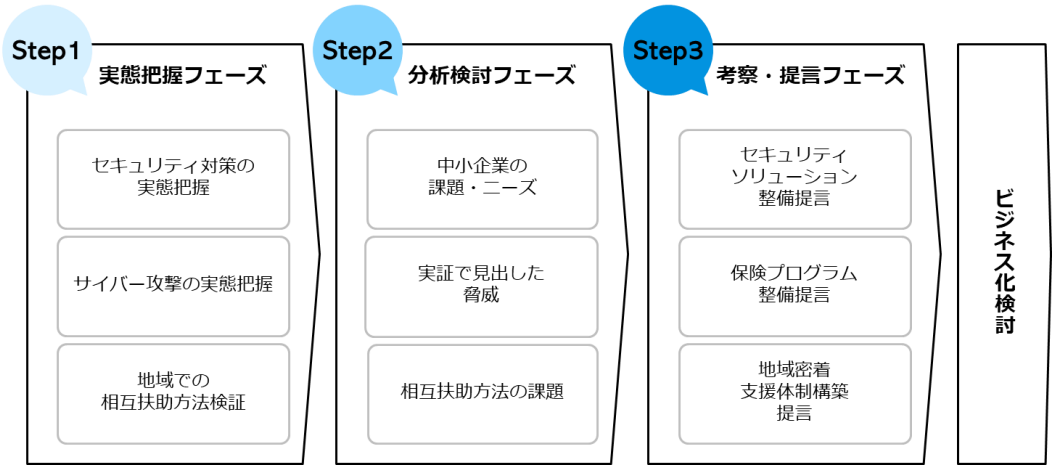

図 1.2.2-1 実証プロセスイメージ

2. 実証事業の概要

2.1 実証対象（地域／産業分野）の選定

実証事業コンセプトに基づき、地元密着度の高い検証を実現するため、富士ソフトの拠点がある岩手県大船渡市を中心とし、周辺自治体、地元経済団体および地元 IT 企業との連携による実証事業を実施。

2.1.1 産業構造的選定根拠

岩手県では、農業をはじめ林業、水産業、建設業の地域特性を活かした産業がメインであったが、近年は先端技術産業や自動車関連産業をはじめとする企業誘致の進展や、地場産業の振興などにより、平成 26 年には製造品出荷額が 2 兆 2,706 億円となった。中でも輸送用機械器具や食料品製造業の工業出荷額の割合が増加傾向で、自動車、半導体関連などの完成品メーカーと、それを支える基盤技術を有する中小企業群が集積した、国内有数のものづくり産業集積の実現を目指しており、これからサプライチェーンが多く確立され、サイバーセキュリティ対策の必要性が高まるものと判断して選定した。

※岩手県：岩手県の産業

https://www.pref.iwate.jp/kensei/profile/1000651.html （2020/7/13 参照）

2.2 スケジュール

本実証事業の全体スケジュールは以下のとおりに実施。

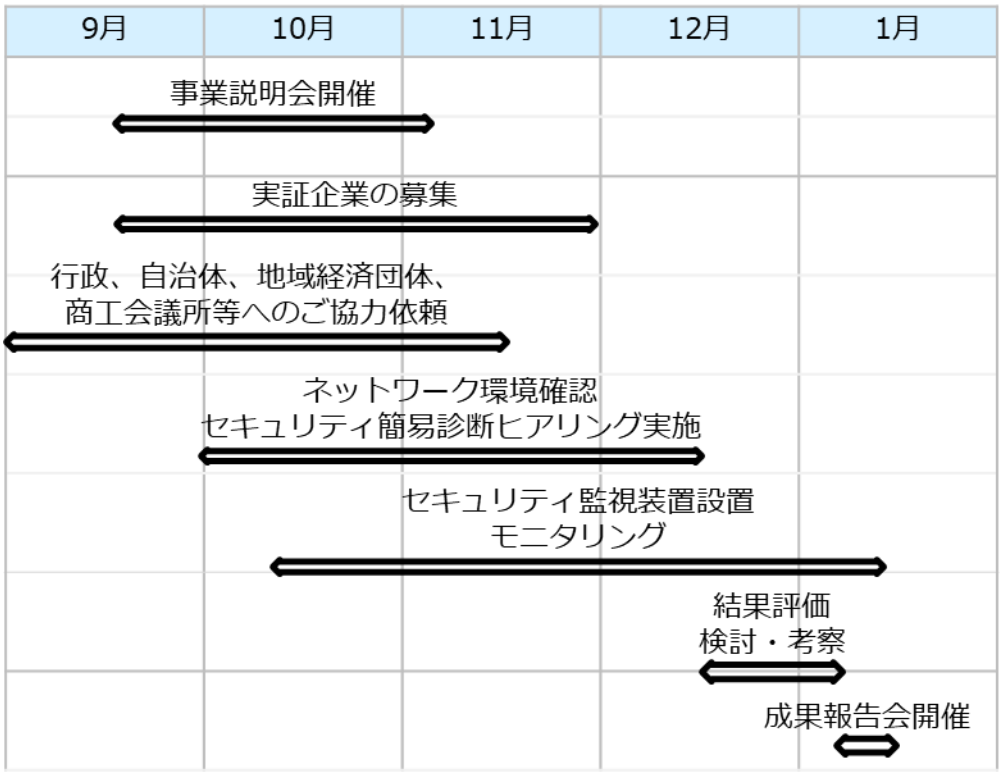

図 2.2-1 全体スケジュール

2.3 実証参加企業

本実証事業への参加申込企業数は 72 社、うち実際に実証を開始できた企業数は 71 社である。

2.3.1 業種傾向

「2.1.1 産業構造的選定根拠」に基づき、製造業が多く全体の 20%を占めたが、サービス業も同率となった。建設業、情報通信業が続いて 10%となった。一部偏りは、見受けられるものの、概ね多種多様な業種が参加した。

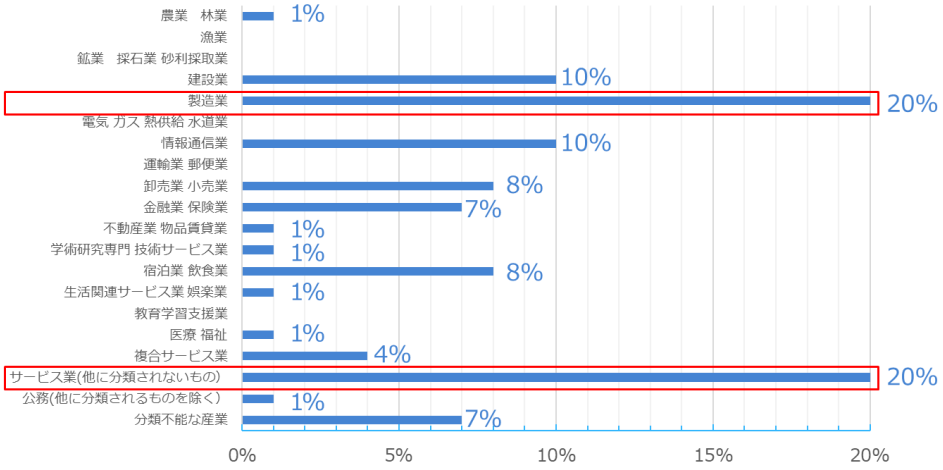

図 2.3.1-1 実証参加企業の業種一覧

2.3.2 従業員数

小規模な企業が大多数であり、50 名を超えるような企業は少数（18%）であった。富士ソフトの拠点がある大船渡エリアを中心に実証参加企業を募った影響もあり、個人事業主の割合が比較的多かった。

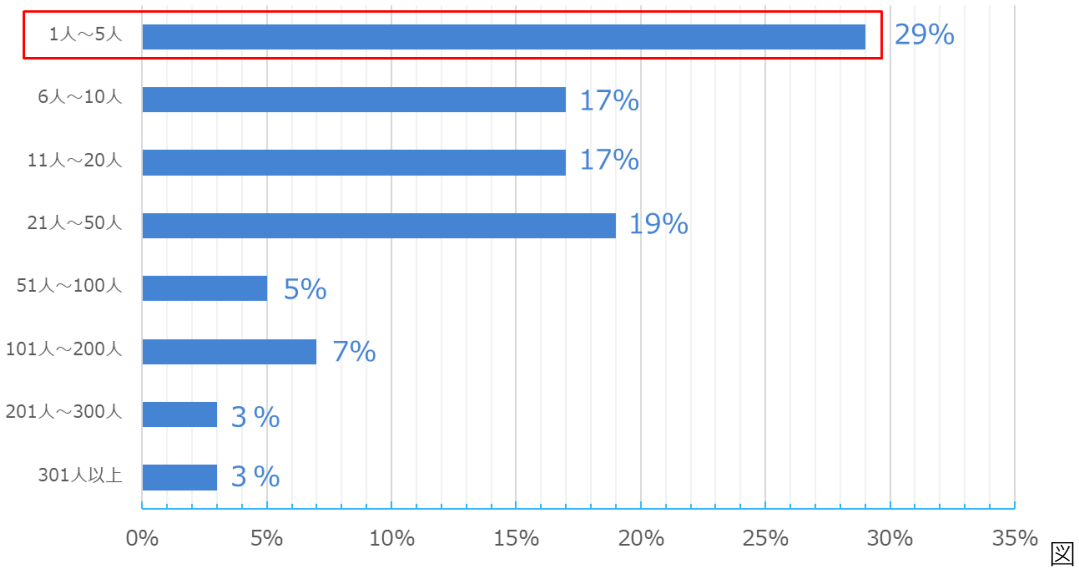

図 2.3.2-1 実証参加企業の従業員数分布

2.4 実施内容

現在、新型コロナウイルスの影響でテレワークが加速し、オフィス環境のセキュリティ対策もままならないまま、中小企業でもテレワークが実施されている。このため、本実証事業では、セキュリティ監視システムと、従来のオフィス環境に設置する“ネットワークセンサー”で実現する「オフィスＳＯＣ」と、新たな仕組みの“テレワーク用ネットワークセンサー”で実現する「おうちＳＯＣ」にて、オフィス環境およびテレワーク環境におけるサイバー攻撃状況の見える化を実施した。

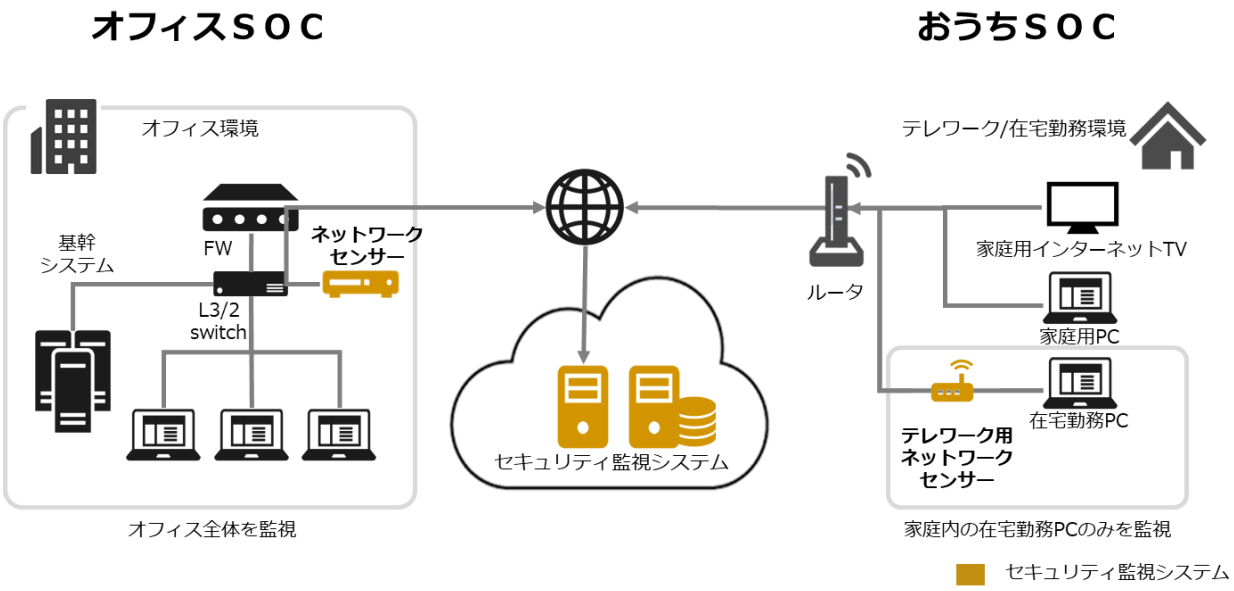

図 2.4-1 実施概要図

2.4.1 提供サービス

新たに構築した「ネットワークセキュリティ監視・定期分析サービス」を用いて、対象企業のネットワーク挙動を AI で監視し、定期的に専門技術者が分析することにより、水面下で侵攻するサイバー攻撃の真の可能性と対策を分かりやすく通知するサービスと、地域に密着したビジネスを展開している富士ソフト大船渡テレワーク室の人員による「駆け付けサービス」を組み合わせることで、地域の中小企業に利用しやすく、検証終了後も継続可能なサービスを提供した。

テレワーク環境もオフィス環境同様に狙われているが、テレワーク環境は、社員自身が IT 環境を整備・管理する必要があるが、大半は IT に対する知識、経験が不足していることが多いと想定される。大半は、あまり費用をかけず、機器の設定も甘くなりがちで、異常に気が付くのが困難な状態のため、両環境のサイバー攻撃を見える化する必要があると考えた。

【提供サービス一覧】

I. 簡易セキュリティ診断

II. 中小企業等からのサイバーセキュリティに関する相談の受付および対応

III. 監視システム、分析サービス等による中小企業等の実態把握のための措置

IV. サイバーインシデントが発生した際の支援の提供

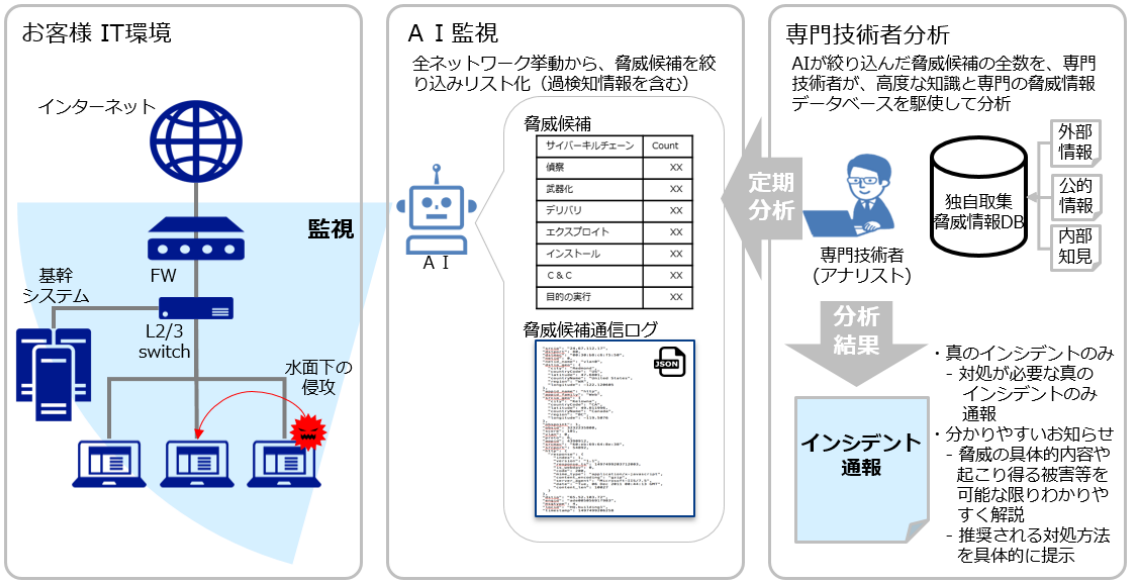

図 2.4.1-1 提供サービス概要図

3. 実施結果

3.1 説明会の開催

9 月 16 日から 30 日にかけて、大船渡市、釜石市、陸前高田市、盛岡市の実会場で 4 回、新型コロナウイルスの影響を踏まえウェブセミナー形式で 2 回、合計 6 回開催。更に、10 月半ばの時点で実証参加企業が計画数に満たない状況であったため、追加で 11 月 5 日、6 日にウェブセミナー形式にて開催。（合わせて計 8 回実施）

※上記とは別に、大船渡市の企業向けに個別の説明会を 2 回実施。

図 3.1-1 説明会風景（大船渡会場）

3.1.1 開催日程

表 3.1.1-1 説明会開催日程

	開催日	開催時間	会場	参加社数（人数）
第 1 回	2020 年 9 月 16 日	14:30~16:30	大船渡商工会議所	15（19）
第 2 回	2020 年 9 月 17 日	14:30~16:30	釜石・大槌地域 産業育成センター	7（8）
第 3 回	2020 年 9 月 18 日	14:30~16:30	陸前高田市 コミュニティホール	3（3）
第 4 回	2020 年 9 月 24 日	14:30~16:30	盛岡地域交流センター	7（7）
第 5 回	2020 年 9 月 25 日	14:30~16:30	ウェブセミナー形式	7（8）
第 6 回	2020 年 9 月 30 日	15:30~17:30	ウェブセミナー形式	4（4）
第 7 回	2020 年 11 月 5 日	14:00~14:40	ウェブセミナー形式	4（4）
第 8 回	2020 年 11 月 6 日	14:00~14:40	ウェブセミナー形式	3（3）

3.1.2 アジェンダ

表 3.1.2-1 説明会アジェンダ

時間	内容	講演者
10 分	岩手県お助け隊事業に関するご説明	富士ソフト
20 分	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について	IPA
15 分	サイバーセキュリティ最新動向	富士ソフト
15 分	本実証事業で使用する AI セキュリティ監視システムのご説明	富士ソフト
20 分	企業がサイバーリスク保険を活用する本当の理由	東京海上日動火災保険
5 分	中小機構 IT 経営簡易診断 のご案内 （9 月 24 日の盛岡会場のみ）	経済産業省 東北経済産業局

※第 7 回、8 回は富士ソフトセッションのみにて実施。

3.1.3 実証参加企業の募集

(1) 岩手県内の行政機関、各経済団体、各商工会議所などの協力

◆陸前高田商工会：会員宛に説明会の案内チラシ郵送（540 部）
◆いわて産業振興センター：メーリングリスト宛に説明会案内送付（約 1,100 件）
◆釜石・大槌地域産業育成センター：
メーリングリスト宛に説明会案内送付、HP 掲示板の説明会案内を掲載
◆大船渡商工会議所：会員宛に説明会の案内チラシ郵送　（1,600 部）
◆岩手県商工会連合会：岩手県の各商工会宛に、メールにて募集協力の呼びかけを実施
◆岩手県庁：製造業を中心としたメーリングリスト宛に説明会案内送付（約 1,000 件）
◆盛岡市：盛岡地域起業家セミナー参加者のメーリングリスト宛に説明会案内送付（約 200 件）
◆岩手県情報サービス産業協会：メーリングリスト宛に説明会案内送付（47 社）
◆岩手県中小企業診断士協会：会員宛に説明会案内送付
◆岩手県中小企業団体中央会：HP 掲示板に説明会案内を掲載

(2) 東京海上日動火災保険株式会社による募集活動

本実証事業の協力会社である東京海上日動火災保険株式会社の盛岡中央支社（盛岡市）、岩手南支社（北上市）から、保険代理店への募集依頼および自社の実証事業参加の呼びかけを実施。

(3) メディアの活用

◆岩手日報：実証参加募集の広告を掲載／ホームページにバナー広告を掲載
◆東海新報：2020 年 10 月 23 日付の紙面に本実証に関する記事を掲載

(4)　個社への直接アプローチ

大船渡市を中心に、テレアポや各所からの紹介により、地場企業に対して直接訪問し本実証事業の内容、メリットの説明を実施し参加の呼びかけを実施。

また、10 月に 2 回、11 月に 1 回の計 3 回、神奈川県から岩手県に向かい、盛岡市、久慈市の企業に直接訪問し、本実証事業への参加の呼びかけを実施。

結果、実証参加企業の半数以上が、この直接訪問をきっかけとした参加であった。

3.2 実態把握結果

本実態把握結果は、説明会・報告会参加者を対象にアンケートを実施し、岩手県下の中小企業におけるセキュリティ対策およびテレワークに関する、実施状況、意識、課題、要望を収集・把握するために実施した結果となる。

3.2.1 アンケート概要

(1) アンケート回答企業プロファイル

アンケートに回答した企業は、90 社で、業種では、製造業とサービス業が多く、従業員数では、1～5 名または 21～50 名が最も多くなる結果となっている。

また、その中で、情報システム担当者については、専任者がいる企業は、約 14%であり、約 86%の企業で、兼任または、不在な状況となっている。

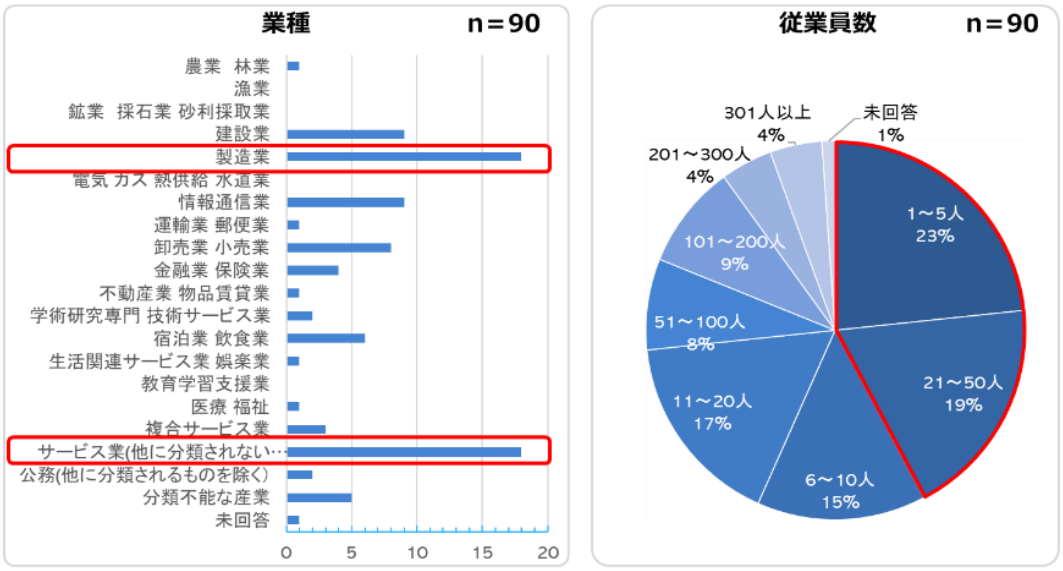

図 3.2.1-1 業種・従業員数

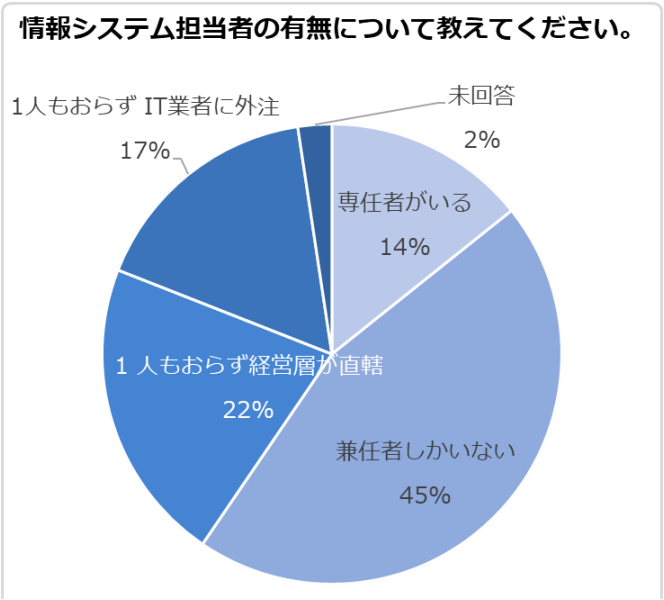

図 3.2.1-2 情報システム担当者の有無

(2) アンケート項目

表 3.2.1-1 アンケート項目

No.	項目
	企業状況確認
1	業種を教えてください。
2	従業員数を教えてください。
3	情報システム担当者の有無について教えてください。
	現状のサイバーセキュリティ対策意識調査
1	サイバーセキュリティ対策のセキュリティ実施状況について教えてください。
2	サイバー攻撃対策としてアンチウイルスソフトだけだと不十分だと知っていますか。
	セキュリティ課題意識調査
1	サイバーセキュリティ対策の課題は、ありますか。
2	具体的な課題について近しいものをお選びください。
	セキュリティニーズ意識調査
1	サイバーセキュリティ対策として最も重要視していることを 1 つ教えてください。
2	サイバーセキュリティ対策の年間経費について教えてください。
3	取引先からサイバー攻撃対策を求める傾向の有無についてお答えください。
	セキュリティリスク意識調査
1	サイバー攻撃に対するリスクについて教えてください。
2	サイバー攻撃で事故が発生した場合、想定される影響についてお答えください。

	サイバー攻撃意識調査
1	サイバー攻撃 被害の経験は、ありますか。
2	サイバー攻撃で事故が発生した場合、想定される影響についてお答えください。
	サイバー保険意識調査
1	サイバー保険の存在を知っているか教えてください。
2	既存のサイバー保険やサービスの価格帯は高いと思うか教えてください。
	在宅勤務/テレワーク意識調査
1	在宅勤務/テレワーク実施の有無について教えてください。
2	在宅勤務/テレワークを進める上でのセキュリティの課題について教えてください。
3	在宅勤務/テレワークでのセキュリティに対する心配事項を教えてください。

3.2.2 現状のセキュリティ対策意識調査結果

セキュリティ対策として、最も多いのは、約 80%の企業が導入しているウイルス対策ソフトとなり、次いで、ファイヤーウォールとなっているが、簡易セキュリティ診断時のヒアリングにて、このファイヤーウォールは、ほぼ全て OS 標準のものであったと判明しており、多くの企業が実施しているセキュリティ対策は、ウイルス対策のみということが明確になった。

しかしながら、「ウイルス対策ソフトだけではセキュリティ対策が不十分なのを知っているか」という質問に対し、約 65%の企業で「知っている」と回答しているが、セキュリティ対策状況は、圧倒的に、ウイルス対策ソフトしか導入していないことが分かる結果となった。

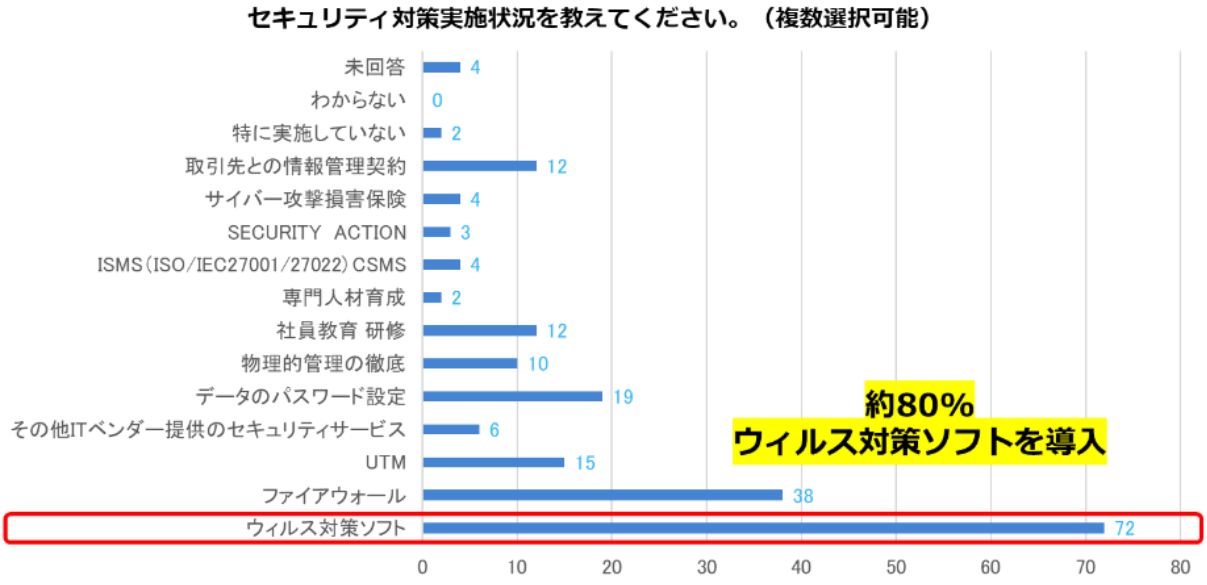

図 3.2.2-1 セキュリティ対策状況

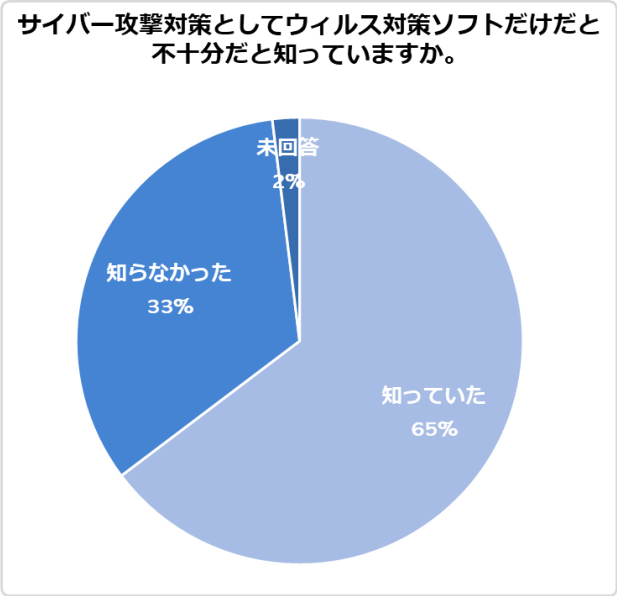

図 3.2.2-2　ウイルス対策ソフトに対する認識

3.2.3 セキュリティ課題意識調査結果

約 70%の企業で、セキュリティに課題を持ち、63 社もの企業が「なにを、どこまで？」「本当に大丈夫か？」などと不安を抱え、分からないため対策しきれていないことが浮き彫りとなる結果となった。

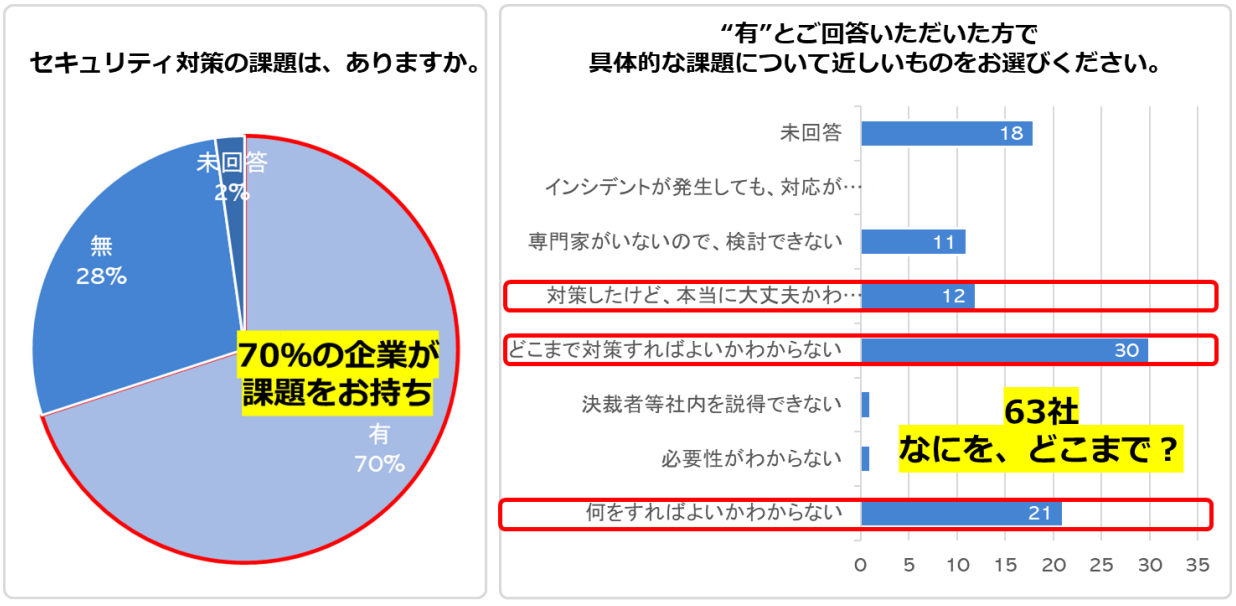

図 3.2.3-1 セキュリティ課題

3.2.4 セキュリティニーズ調査結果

「価格」が重要視されることは当たり前ながら、次いで「機能」が重要視される傾向となっている。また、当初の予想に反して「駆け付け」は、あまり重要視されていないことが分かる結果となった。

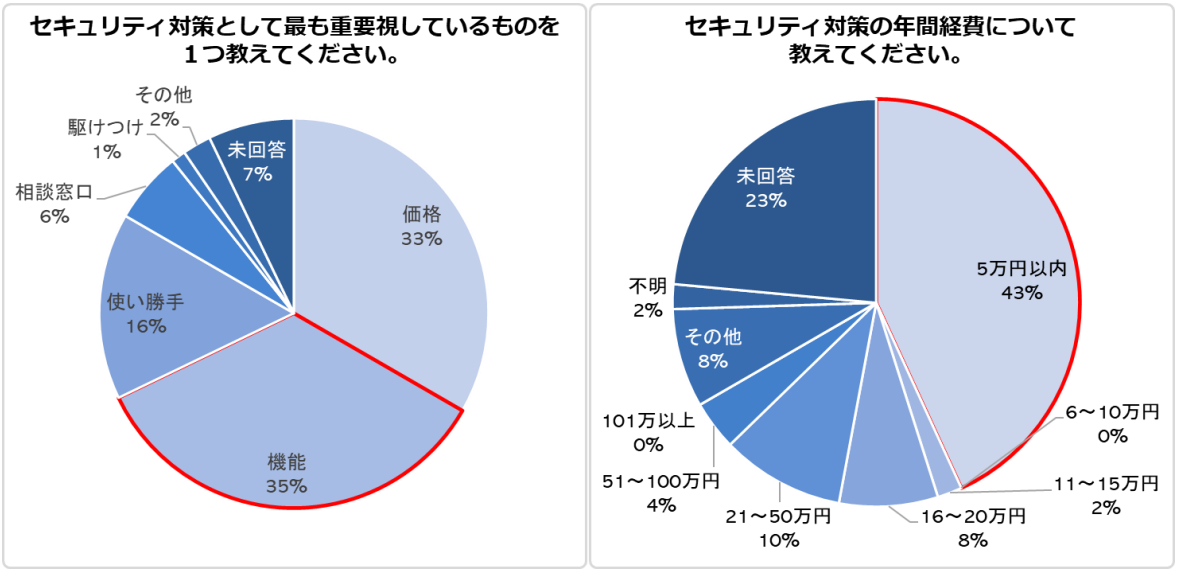

図 3.2.4-1 セキュリティニーズ 重要視/価格

取引先からの委託条件に、「サイバー攻撃対策が要求されつつあるか」の問いに、約 30%の企業が、「要求されつつある」と回答しており、本件が委託条件になりつつあることが伺われる。しかしながら、半数以上の約 66%の企業が、「その動向はない」と回答しており、急に、委託条件に、サイバー攻撃対策が要求される状態にはないことが明らかとなる結果となった。

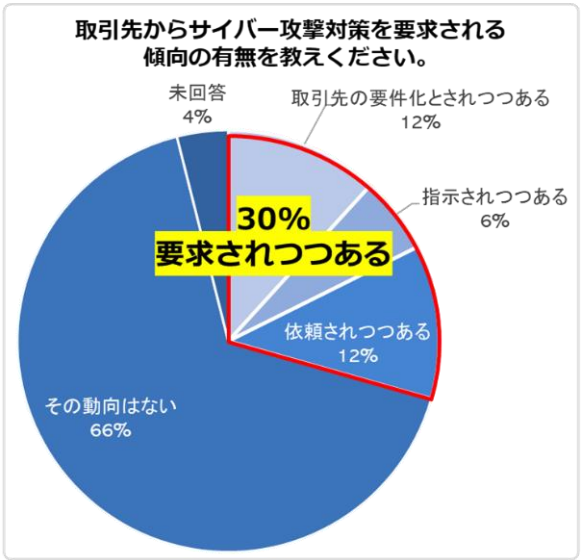

図 3.2.4-2 セキュリティニーズ 取引先要求

3.2.5 セキュリティリスク意識調査結果

約 81%もの企業が、「サイバー攻撃を受けるリスク」を懸念しており、また、サイバー攻撃を受けた場合に、約 79%もの企業が、「事業継続の影響」を懸念していることが分かる結果となった。

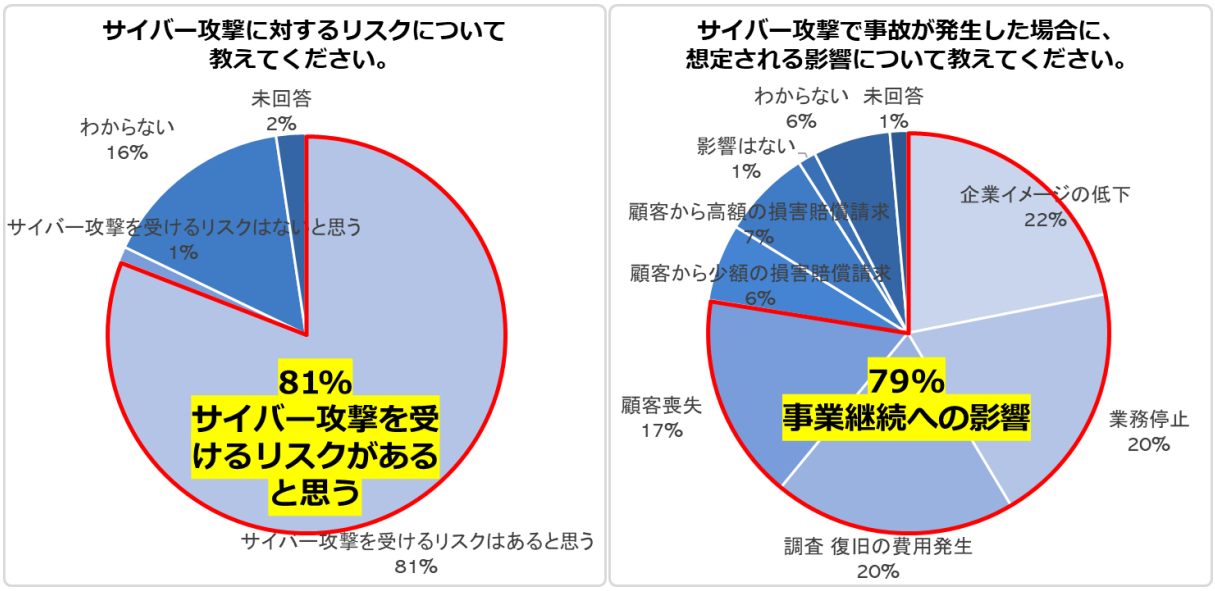

図 3.2.5-1 セキュリティリスク意識

3.2.6 サイバー攻撃意識調査

約 32%の企業は、「何らかのサイバー攻撃を受けた経験がある」ということが判明し、中小企業でも確実にサイバー攻撃を受けていることを証明する結果となった。

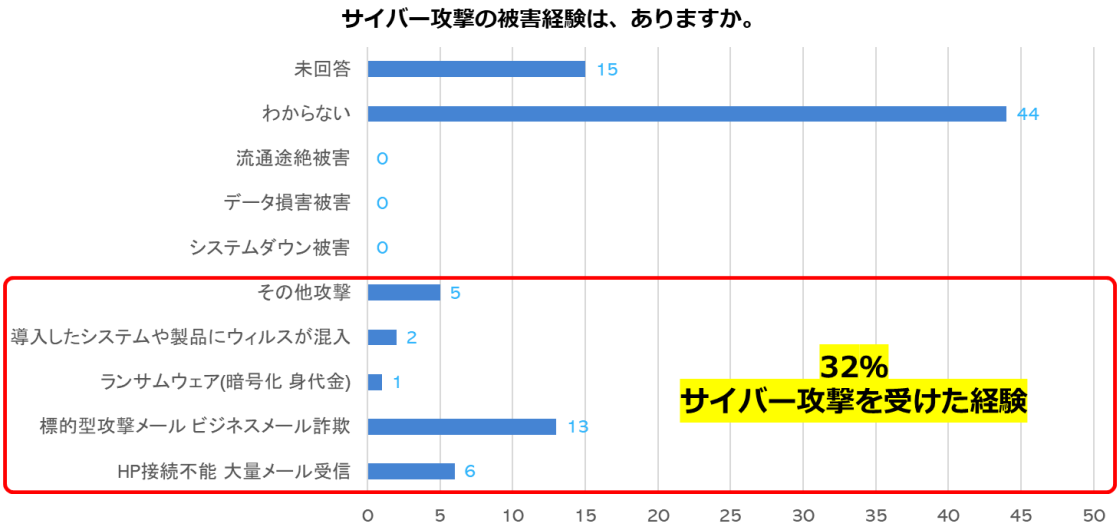

図 3.2.6-1 サイバー攻撃状況調査

3.2.7 サイバー保険意識調査結果

約 49%の企業が、「知っている」と回答しているが、その企業のうち約 66%の企業が、次のサービス価格に関する質問で、「分からない」と回答している。このため、実際に保険を検討した、あるいはその保険の価格を含め内容を正確に把握していると思われる企業は、は、「高いと思う」「高くない」と回答した企業のみとなり、最初に「知っている」と答えた企業のうち、約 16%のみである。この結果から、中小企業には、サイバー保険が浸透していないことが判明する結果となった。

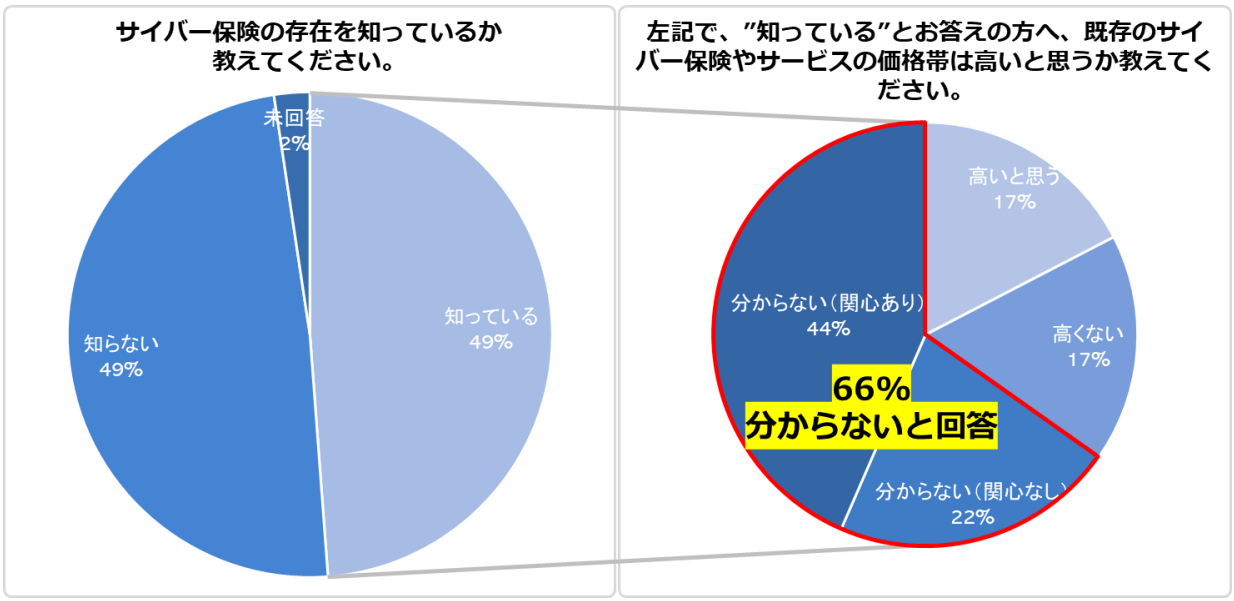

図 3.2.7-1 サイバー保険意識調査

3.2.8 在宅勤務/テレワーク意識調査

(1) 在宅勤務/テレワーク実施について

アンケート時点では、約 33%の企業が、在宅勤務/テレワーク実施の有無に対し「有」と回答し、多くの企業で在宅勤務/テレワークを導入したことが分かる結果となった。

しかしながら、およそ、1 か月後に実施した簡易セキュリティ診断時には、コロナ禍が、一旦、弱まったこともあり、約 10%の企業以外は、「無」に変更となり、セキュリティの監視対象としないとの回答が多い結果となった。ここから、在宅勤務/テレワークの実施は、緊急回避的な対応であったことが推測される。

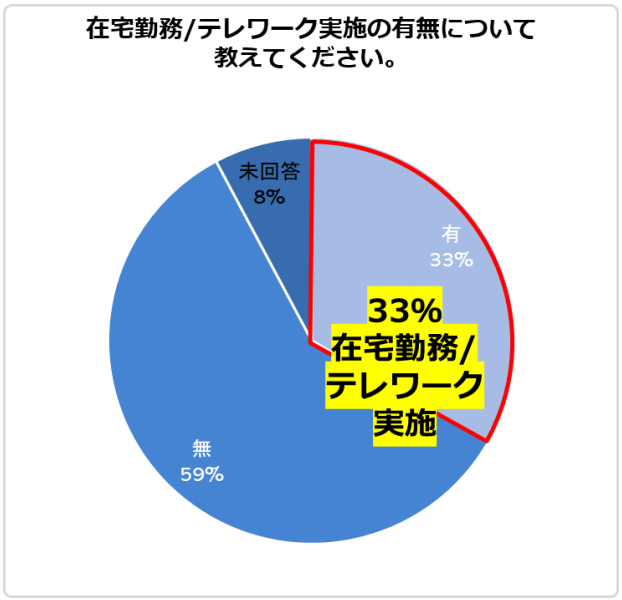

図 3.2.8-1 在宅勤務/テレワーク実施調査

(2) 在宅勤務/テレワークを進める上で、セキュリティの課題について

本課題の調査については、オフィス環境でのセキュリティ課題と差はなく、オフィス環境で課題であった「なにを、どこまで？」が課題という結果となった。

また、心配事項の調査については、ウイルス感染よりも、「機密情報の漏洩」が、多く、約34%もの企業での心配事項となってる。

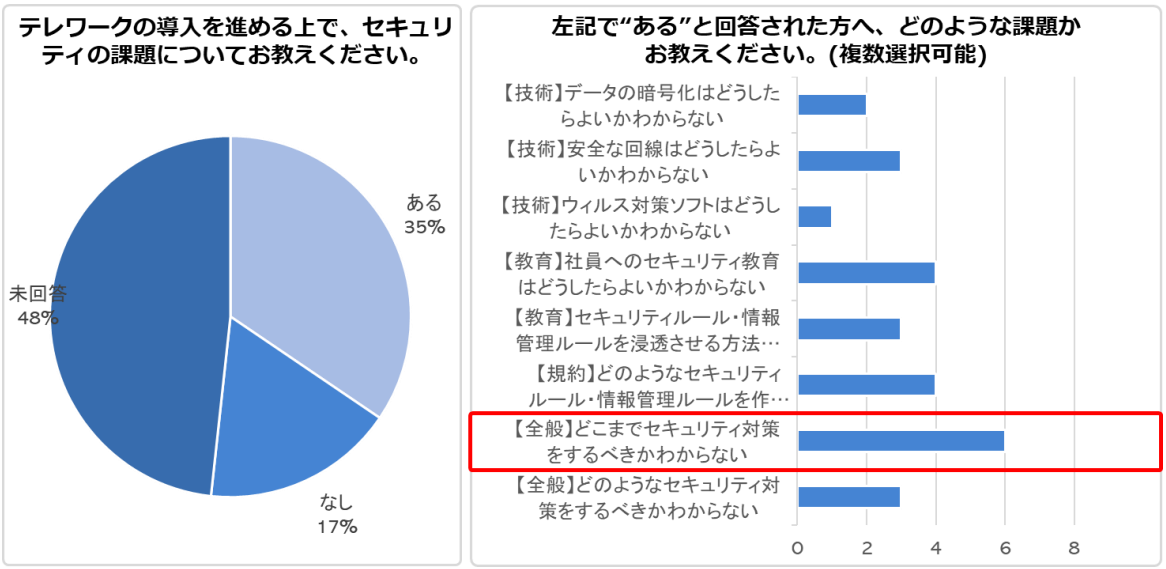

図 3.2.8-2 在宅勤務/テレワークを進める上でのセキュリティの課題の調査

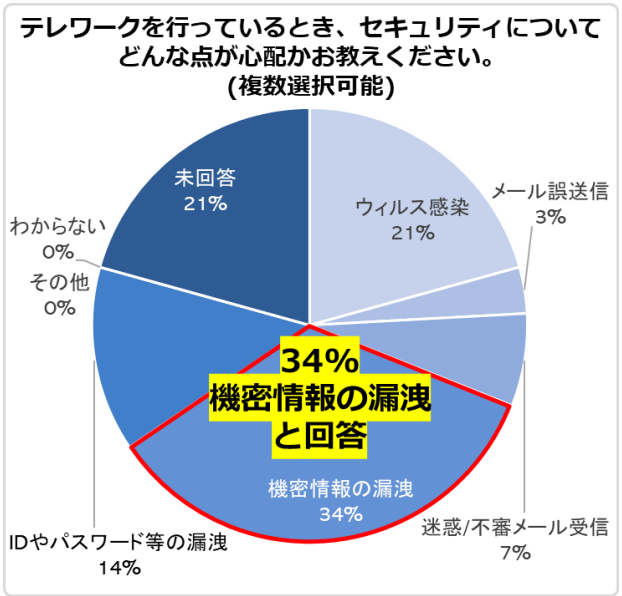

図 3.2.8-3 在宅勤務/テレワークでのセキュリティに対する心配事項の調査

3.3 実証の実施結果

本実証の実施結果は、実証参加企業 71 社の協力を得て、以下を実施した結果を纏めたものである。

〇セキュリティ対策実態調査結果：
事前に用意した簡易セキュリティ診断項目を、リモートヒアリングを実施し、各企業のセキュリティ対策状況を見える化した結果である。

〇サイバー攻撃実態調査結果：
各企業の IT 環境内に、ネットワークセンサーを設置し、各企業のネットワーク挙動をセキュリティ監視システムとアナリストにて、監視・分析し、サイバー攻撃の状況を見える化した結果である。

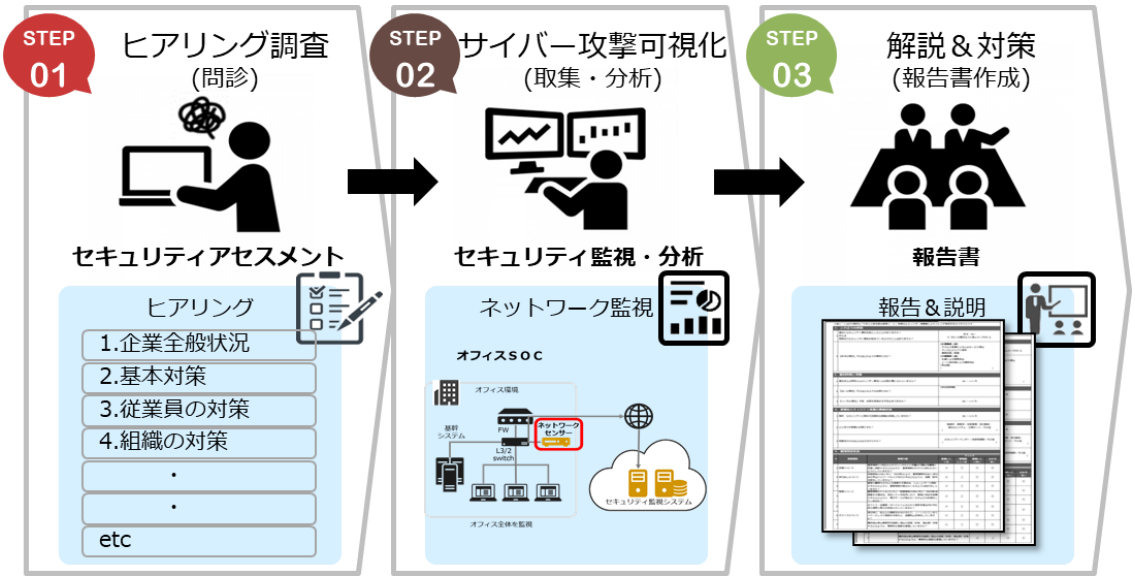

図 3.3-1 実施概要

3.3.1 セキュリティ対策実態調査

本調査では、富士ソフトの提供する簡易セキュリティ診断をベースに、実証事業終了後にSECURITY ACTION を宣言しやすくするための変更と、サイバー攻撃実態調査のため、各企業に設置し、ネットワークセンサーの設置確認項目を加えたものを、企業毎にリモートでヒアリングの上、企業毎に分析し、オフィス環境と在宅/テレワーク環境に分けて記載している。

図 3.3.1-1 簡易セキュリティ診断兼設置確認イメージ

(1) オフィス環境の調査結果

全国全業種平均と比べ「破棄、施設管理、社内規定周知」では、平均より高水準だが、「事故対応、対策の明確化、インターネット」は、平均より低い状況であり、もしも、ウイルス対策ソフトのみでは防げないサイバー攻撃を受けた場合には、被害に歯止めがかからず、被害が広がる恐れがあることが分かる結果となった。

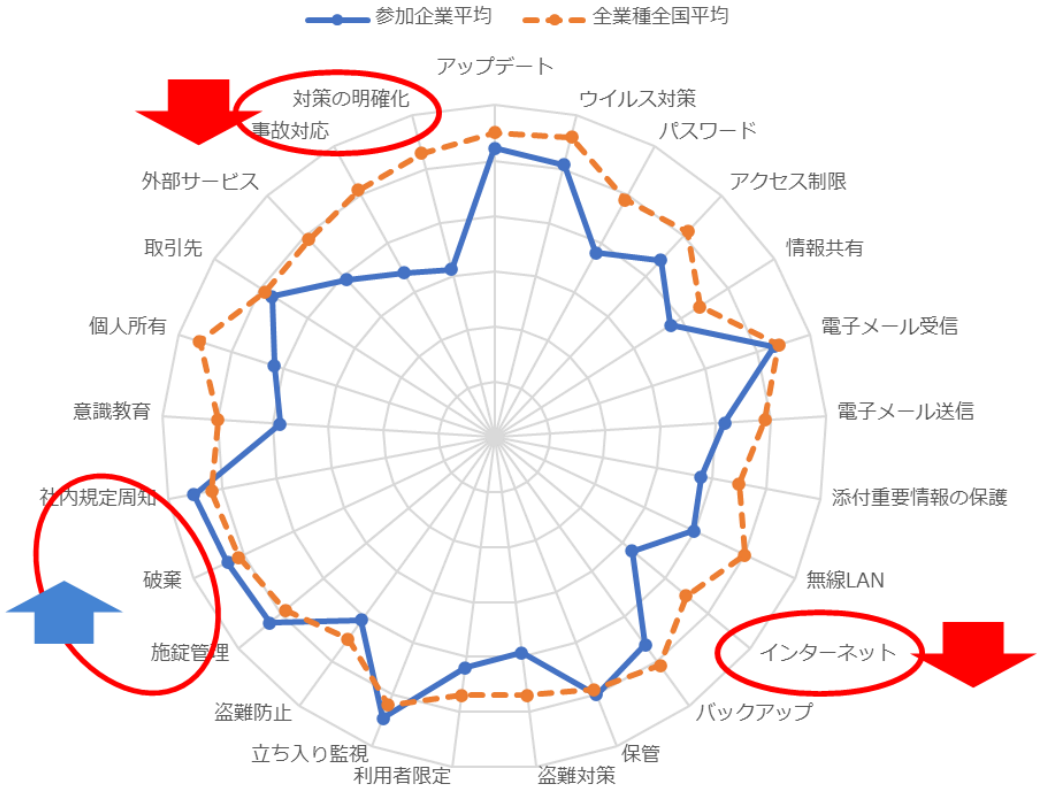

図 3.3.1-2 実証参加企業全体のオフィス環境での簡易セキュリティ診断結果

(2) 在宅/テレワーク環境の調査結果

本実証事業開始時点で、在宅/テレワーク環境における全国全業種平均データがないため、実証参加企業平均で分析を実施すると、「対策の明確化、無線 LAN、ルーター対策」面での対策が低い状況であり、特に、ルーター対策については、ルーターが乗っ取られると情報流出に、繋がりかねないが、多くの実証参加企業では、対策がなされていないことが分かる結果となった。

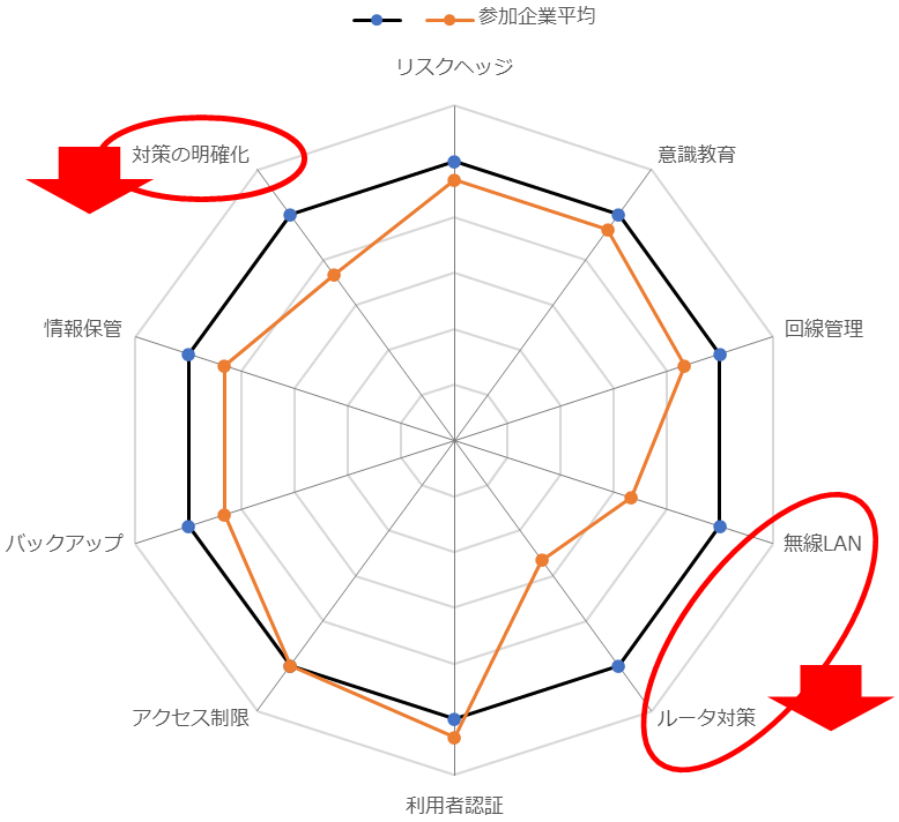

図 3.3.1-3 実証参加企業全体の在宅/テレワーク環境での簡易セキュリティ診断結果

3.3.2 サイバー攻撃実態調査結果

本調査では、富士ソフトの提供するセキュリティ監視・分析サービスをベースに、在宅/テレワーク環境などに対応したネットワークセンサーを新たに用意した。実証参加企業のオフィス環境や在宅/テレワーク環境に、ネットワークセンサーを設置することで、ネットワーク挙動を監視し、設置企業におけるセキュリティ的な脅威を検出するものである。

表 3.3.2-1 ネットワークセンサー/接続補助機器

No	機器名	説明
1	オフィス用 ネットワークセンサー	ファイヤーウォール、ルーター、L3/L2 スイッチなどのミラーポートに接続し使用するタイプ（有線接続のみ対応）
2	小型オフィス用 ネットワークセンサー	小型オフィスのルーター配下に接続し、スイッチハブとして使用するタイプ（有線/無線接続対応）
3	在宅/テレワーク用 ネットワークセンサー	在宅/テレワーク環境のルーター配下に接続し、セグメントを分離して使用するタイプ（有線/無線接続対応）
4	L2 スイッチ（接続補助機器）	実証参加企業環境において、ミラーポートが用意できない場合に、本機器を接続しミラーポートを使用することで、オフィス用ネットワークセンサーを接続する。 なお、企業規模に対応し、8 ポートと 16 ポートのものを用意した。

ネットワークセンサーの設置については、下記「図 3.3.2-1 セキュリティ監視システム ネットワークセンサー設置フロー」のとおり、参加申し込み企業毎に、事前の簡易セキュリティ診断兼設置確認と接続方法の案内を行い、得た情報を基に、現地対応チームにて事前設定を済ませた形でキッティングを行い、実証参加申込企業に宅配便で送付することで、中小企業におけるネットワークセンサーの設置が円滑に進められるように取り計らった。

なお、設置にサポートが必要な実証参加申込企業向けに、現地対応チームによる訪問での設置も提供した。

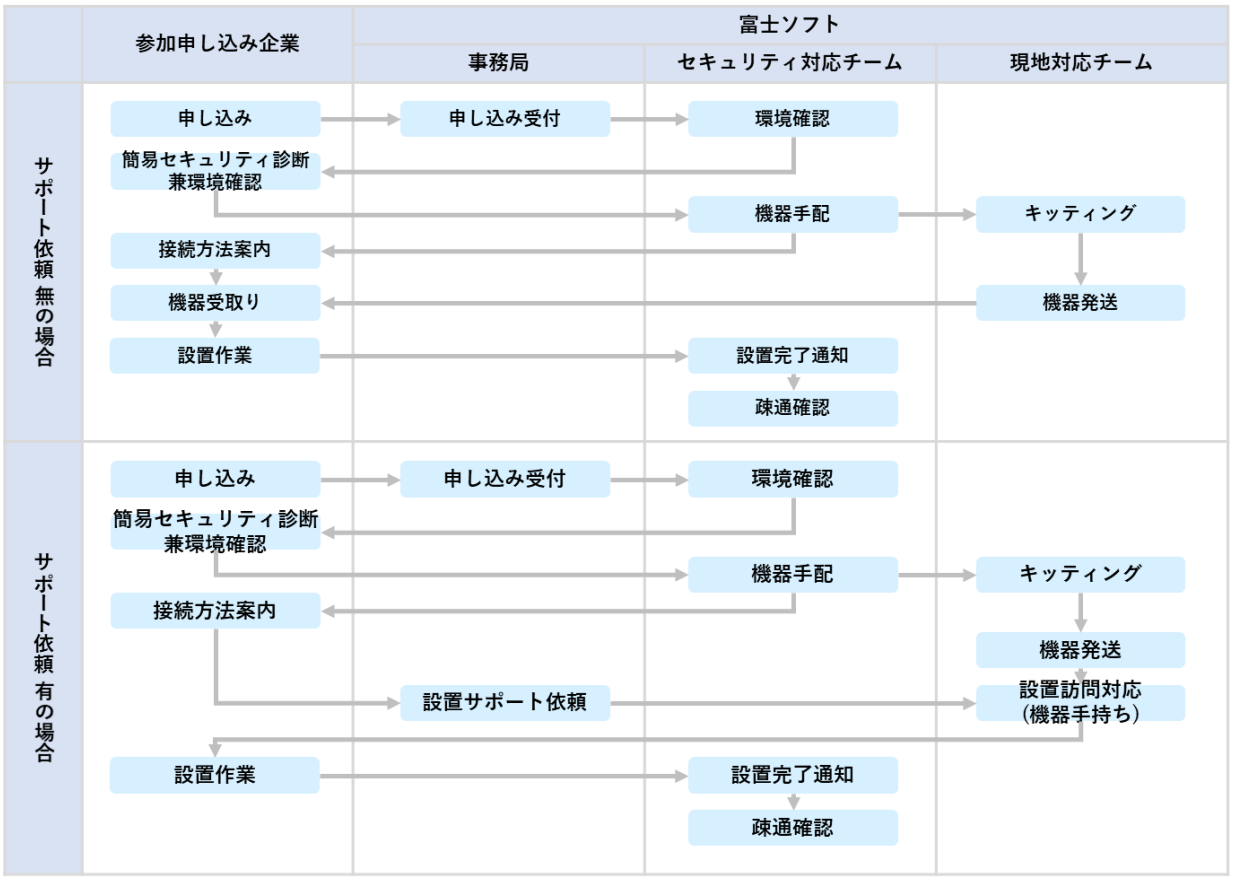

図 3.3.2-1 セキュリティ監視システム ネットワークセンサー設置フロー

実証参加企業からの各種問合せや問題発生時の対応は、下記「図 3.3.2-2 問合せ/問題発生時、通報時フロー」のとおり、一本化するため、事務局内に窓口を設置した。対応時間は、一般的な中小企業の営業時間帯や中小企業向けサービスとしての実現可能性を考慮して、土日祝日を除く、平日午前9時から午後5時30分までとした。

また、ネットワークセンサーの設置企業で、一定のリスクがあるセキュリティ的な脅威を発見した場合は、事務局内の窓口を通さず、直接実証参加企業へ通報を実施できるフローとした。

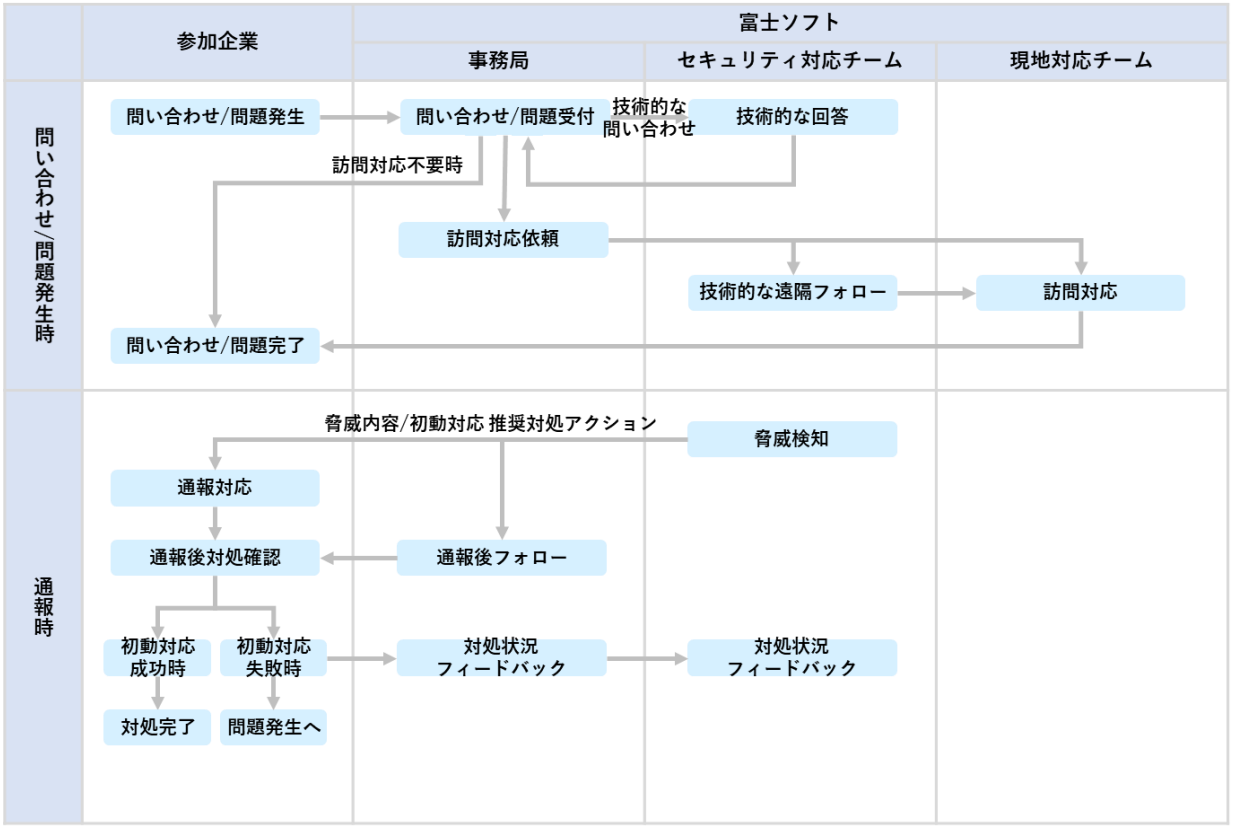

図 3.3.2-2 問合せ/問題発生時、通報時フロー

(1) 検出アラートについて

本結果は、水面下で侵攻するサイバー攻撃の状況を “セキュリティイベント”と“トラフィックイベント”を、セキュリティ監視システムにて観測・収集し、AI 基準で洗い出した結果である。本結果を基に、アナリストが分析を実施し、通報が必要と判断したものを対象企業に通報し、「3.3.2(2) 検出インシデントについて」として計上した。

また、インシデントではないが、セキュリティ上好ましくない運用として、「パスワードなど重要情報の非暗号化通信」や「特権アカウント常用」などを、検出した場合も注意喚起のためのお知らせを実施した。

表 3.3.2-2 アラート一覧

サイバーキルチェーン	セキュリティイベント	累計
目的の実行	DNS トンネリング攻撃	298 件
	ブルートフォース攻撃によるログイン成功	0 件
	SYN Flood 攻撃の検知	1 件
C & C	既知の C & C サーバーへの通信	1,049 件
	DGA による C & C サーバーへの通信	0 件
デリバリー	マルウェア配布サイトへのアクセス	1 件
エクスプロイト	異常なプロセスの実行	1 件
偵察	ブルートフォース攻撃によるログイン失敗	1,399 件
	リバースブルートフォース攻撃によるログイン失敗	0 件
	ポートスキャン	569 件
	URL スキャン	152 件
	フィッシングサイトへのアクセス	69 件
合計		**3,539 件**

(2) 検出インシデントについて

本結果は、アナリストが分析した結果、通報が必要と判断したものの数を表している。通報内容には、発生事象とアナリストが分析し検討した対処方法を併記することで、初動対応の分かりやすさの向上を図った。本検証事業では、危険度：高レベルの事象は発見できなかったが、危険度：中～低レベルの事象を発見し、対象企業と連携の上、対処を実施した。

表 3.3.2-3 インシデント対応一覧

対応種別	総計	相談・インシデントなど対応状況	発生件数
インシデント対応	7 件	電話およびリモートによるインシデント対応	7 件
		訪問によるインシデント対応（駆け付け）	0 件

なお、検出したインシデントの事例は、以下のとおりである。

表 3.3.2-4 検出インシデント事例

危険度	インシデント名	詳細
中	アドウェア感染	迷惑ソフトに分類されるソフトウェアの利用痕跡を検出。 当該ソフトウェアは、有償ソフトウェアのダウンロードを促す広告ポップアップを表示の上、トロイの木馬の関連であるサイトに通信を行っていることが確認されている。 このため、セキュリティ対策が不十分な端末では、マルウェア感染、データ漏洩・破壊されるなどの被害を受ける可能性があるため、通報し、迷惑ソフトの削除等の対策の実施を案内した。
中	フィッシングサイトへのアクセス	フィッシング関連サイトへアクセスした痕跡を検出。 当該通信先は、フィッシング、およびマルウェアに関連するサイトとして確認されている。 このため、アクセスにより該当端末がマルウェアへ感染や、サイト上で個人情報の入力を促され、それに従うことにより不正な情報窃取が行われる可能性があるため、通報し、使用者を特定し、フィッシングサイトに情報入力していないか等の確認と対策の実施を案内した。

低	不正な URL スキャンへの応答	不審な IP アドレスから、当該企業のインターネット上に公開している端末に、URL スキャンが実施され、成功レスポンスをしたことを検出。 当該通信内容には、PHP フレームワークで構築された Web サイトに対する OS コマンドインジェクションの攻撃コードが含まれていた。 このため、成功レスポンスにより、Web サイトに存在する脆弱性が晒された状態となり、後続の攻撃により不正アクセスや情報漏洩などの被害を受ける可能性があるため、通報し、公開している端末のログイン履歴確認と脆弱性対策の実施を案内した。

(3) 問合せ・訪問対応状況について

本結果は、問合せ窓口での電話およびメールでの問合せ受付件数と、現地大船渡実働メンバーの訪問対応件数を表している。

今回、セキュリティ機器の設置には、事前ヒアリングの上、メールでの個々の企業に合わせた結線方法の提示、およびマニュアルの準備と、実証参加企業の手間がかからないように準備しての対応であった。しかし実際は想定と異なり、セキュリティ機器の接続方法の確認や、既存ネットワーク機器の設定方法など、非常に多くの問合せを受けた。また、セキュリティ機器設置後に PC からプリンターに印刷指示が届かないなど一部トラブルも発生した。

電話およびメールの対応で問題が解決しない場合は、現地大船渡実働メンバーが直接実証参加企業に訪問し、セキュリティ機器自体の設置作業、上記トラブルの原因調査、および解決に向けた作業を実施したケースも合わせて 37 件発生した。

問合せ件数、およびその他訪問対応の件数から鑑みるに、もっと簡単に導入できるように改良を施す必要があることが分かった。

表 3.3.2-5 問合せ・訪問対応一覧

対応種別	総計	相談・インシデントなど対応状況	発生件数
問合せ窓口対応	143 件	実証参加に関する問合せ	13 件
		セキュリティ機器設置に関する問合せ	130 件
		セキュリティ対応の相談	0 件
		その他	0 件
その他訪問対応（※1）	37 件	機器設置などのトラブル対応	6 件
		セキュリティ機器の導入・設置支援	31 件

※1 「その他」の記載は、インシデント対応による訪問との区別を示す。

3.4 報告会等による実証事業成果の周知

実証事業の総括として、実証事業で得られたデータや検知事例、駆け付け事例、アンケートおよびヒアリング結果に基づいた結果や傾向、分析内容等を報告。また、実証事業を通じて東京海上日動火災保険と連携し、中小企業向けサイバーセキュリティサービスや保険に関する報告会を実施し、自治体、各団体、大学からの参加者も含む 25 社（26 名）が参加した。　※うち、実証参加企業は 14 社（15 名）

参加者からは、「大変参考になった」、「今後社内でも最低限のセキュリティ対策の普及に努めていかなければと、痛切に実感致しました」等の感想が挙がり、本実証事業を通じて、参加した企業のセキュリティ対策に関する意識が確実に高まったことを実感した。

3.4.1 日程

新型コロナ感染者増加の影響を踏まえ、ウェブセミナー形式のみにて開催。

表 3.4.1-1 成果報告会開催日程

	開催日	開催時間	会場	参加社数（人数）
第 1 回	2021 年 1 月 12 日（火）	14:00~15:10	ウェブセミナー形式	12（12）
第 2 回	2021 年 1 月 13 日（水）	14:00~15:10	ウェブセミナー形式	6（7）
第 3 回	2021 年 1 月 14 日（木）	14:00~15:10	ウェブセミナー形式	7（7）

3.4.2　アジェンダ

表 3.4.2-1 成果報告会アジェンダ表

時間	内容	講演者
10 分	中小企業向け情報セキュリティ対策支援事業のご紹介	IPA
30 分	サイバーセキュリティお助け隊 事業報告	富士ソフト
15 分	中小企業向けサイバー保険について	東京海上日動火災保険
10 分	SECURITYACTION 制度のご紹介	IPA セキュリティプレゼンター
5 分	各種施策のご案内のご案内	経済産業省 東北経済産業局

4. 考察

4.1 実証参加企業におけるサイバー攻撃の実態

前述の「3.2.6 サイバー攻撃意識調査」で示すとおり、中小企業でも約 32%が「何らかのサイバー攻撃を受けたことがある」との回答があり、また、「3.3.2 サイバー攻撃実態調査結果」で示すとおり、セキュリティ監視システムを使用したサイバー攻撃の実態把握においても、本実証事業中に、7 件の通報を実施するなど、大企業と同様に、サイバー攻撃のリスクに晒されていることが分かる結果となった。

(1) 業種別アラート分布

下図は、検出したアラートを業種別に集計したものである。また、保有 PC 数を併記することで、保有 PC 数とアラート検出数の関係性を分析した。

今回の検証結果では、基本的に、保有 PC 数とアラート検出数には、相関関係はなく、業種的には、情報通信業にアラートが集中した結果となった。

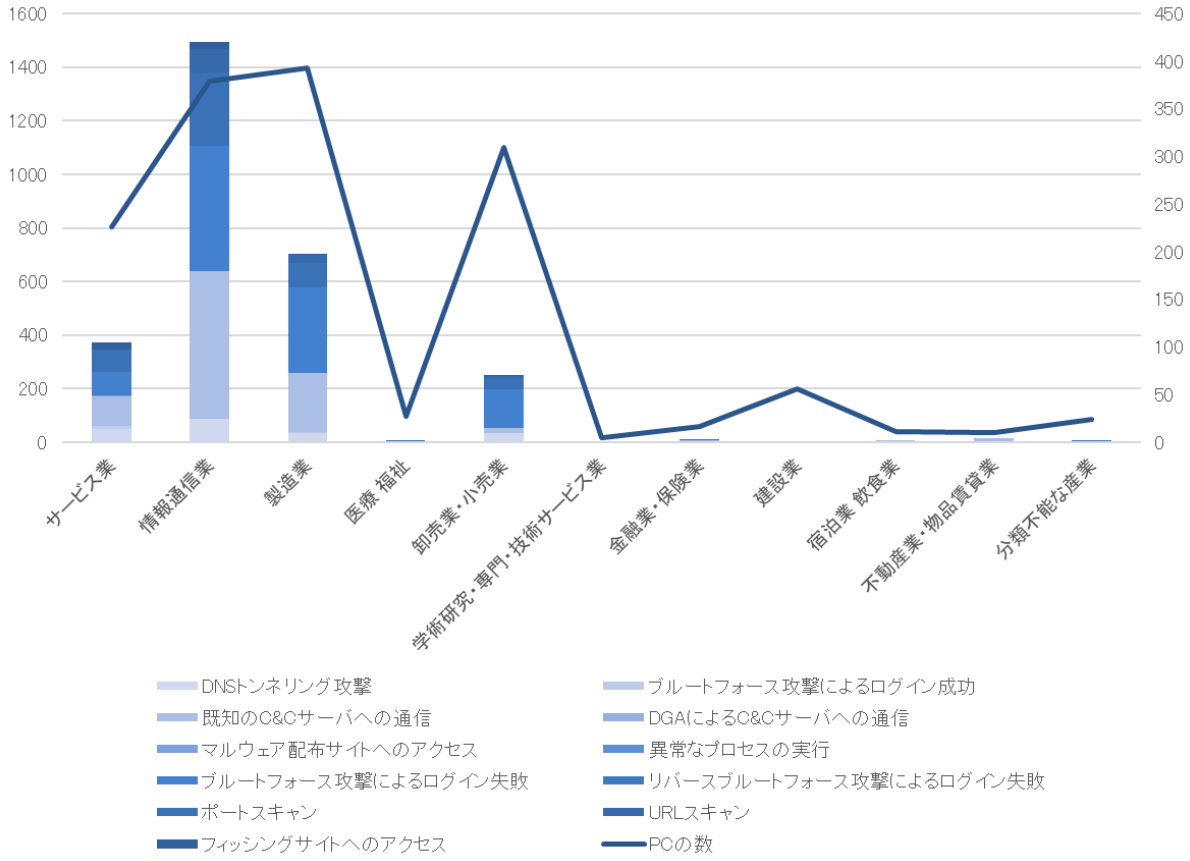

図 4.1-1 業種別アラート分布図

(2) 業種別 PC 1 台当たりの平均アラート検出数

下図は、業界別に、PC 1 台当たりの平均アラート検出数を算出したものである。前述のとおり、情報通信業が最多となるが、前述の「図 4.1-1 業種別アラート分布図」では、ほぼ目立つことがなかった、金融業・保険業、宿泊業・飲食業、および不動産業・物品賃貸業での平均アラート数が高いことが分かる結果となった。

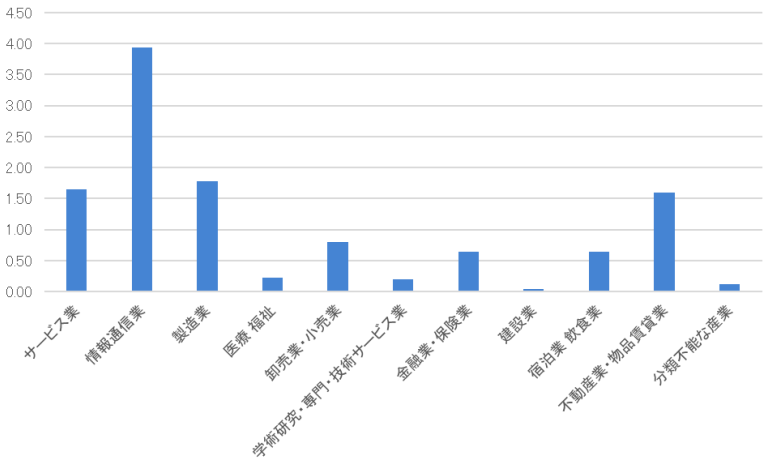

図 4.1-2 PC1 台当たりの平均アラート検出数

(3) 保有 PC 数から見る企業毎のアラート分布

下図は、企業毎のアラート検出数とその保有 PC 数を併記したものである。保有 PC 数とアラート数には相関関係はなく、前述の「4.1(1) 業種別アラート分布」を裏付ける結果となった。

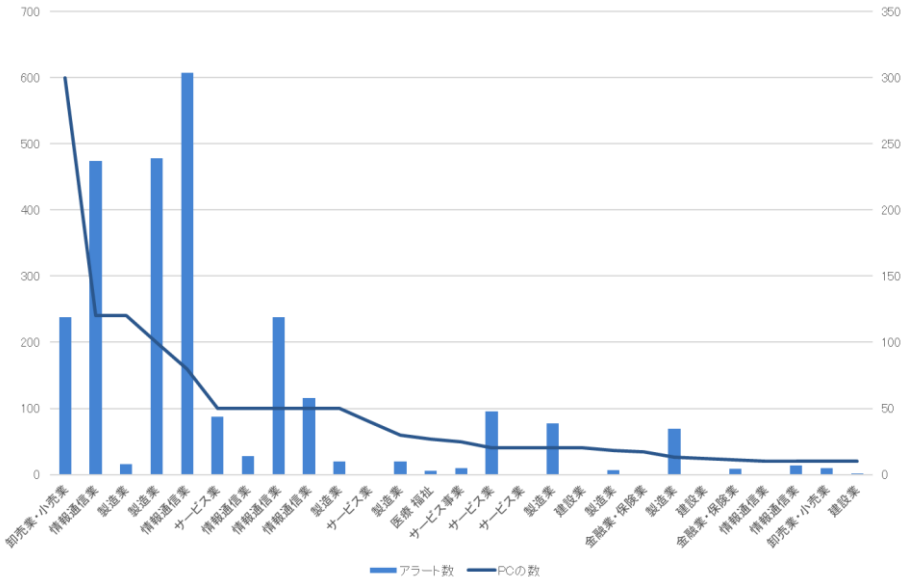

図 4.1-3 保有 PC 数から見る企業毎のアラート分布図（上位 30 社）

4.2 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

以下は、前述の「3.2 実態把握結果」「3.3 実証の実施結果」から、課題抽出および整理を実施した結果となった。

(1)「意識」に関する課題

前述の「3.2.6 サイバー攻撃意識調査」で示すとおり、約 68%の企業では、サイバー攻撃を受けたことがなく、セキュリティの課題や、サイバー攻撃のリスクを感じながらも、「3.2.2 現状のセキュリティ対策意識調査結果」で分かるとおり、セキュリティにかけられる費用も少ないことから、必要最低限の対策であるウイルス対策ソフトのみの導入で留まっており、最終的には「対岸の火事的な」状況となっていることが推測される。

また、簡易セキュリティ診断時のヒアリングで、セキュリティ対策の運用を確認した際には、半数の企業で、導入したままで運用がされないため、サイバー攻撃を受けているかどうか、また、被害があるかどうかも、分からないという実態であった。

実際、メディアから様々なサイバー攻撃の報道があるため、リスクがあることも、いざサイバー攻撃が発生した場合には、企業イメージが低下してしまう影響を筆頭に、自社への影響が大きいことも理解しているが、実際には、発生したことがないので、イメージができないとの意見が挙がった。

上記を踏まえると、セキュリティ対策の普及には、中小企業側に、「対岸の火事」ではなく、身近なところに迫ったリスクであることを、認識してもらう取り組みが必要である。
このため、中小企業でイメージできる身近な事例を収集し、積極的に中小企業に紹介し啓発を促すことと、簡易セキュリティ診断やセキュリティ健康診断のような「どこまで、なにを？」「セキュリティ対策したけど、大丈夫？」の声に応えるサービスの拡充を図り、中小企業が、自社のセキュリティ的弱点とリスクを知ってもらう機会を増やす必要がある。

(2)「資源」に関する課題

前述の「3.2.4 セキュリティニーズ調査結果」で示すとおり、約 43%の企業で、年間のセキュリティ予算は、5 万円以下であり、高額なセキュリティサービスは、受け入れられないため、低価格であることが重要である。

また、「3.2.1(1)　アンケート回答企業プロファイル」内「図 3.2.1-2 情報システム担当者の有無」で示すとおり、専任の情報システム担当者がいる企業は、約 14%であり、専任者のいない企業では、ネットワーク構成やセキュリティ対策方法が分からないという状況が散見した。

今回の簡易セキュリティ診断で浮き彫りとなった「事故対応」や「対策の明確化」などは、サイバー攻撃を受けた場合に、日ごろからの備えが重要となる対策であるため、まずは、企業内で、セキュリティの責任の所在を決め、本件に関する検討をすることが重要である。

(3)「能力」に関する課題

今回の簡易セキュリティ診断におけるヒアリング時に、サイバー攻撃発見時の通報において、該当 PC を特定する方法に関して確認を実施した。結果、セキュリティ監視システムで把握できる情報のみでは、企業側が、特定するための情報を保持していないため、通報しても、受け取った企業側が、該当 PC を特定できず対応ができない恐れがあることが分かった。詳細には、情報資産の管理台帳を持つ企業が、21 社あり、IP アドレスまで管理している企業は、10 社であった。

また、今回セキュリティ監視システムと接続するためのネットワークセンサーは、円滑に設置できるように、企業毎にネットワーク状況をリモートヒアリングし接続方法を伝える施策を行った。しかしながら、リモートヒアリングのため、実際のネットワーク状況が聞いていた内容と異なることがあり、結果、訪問設置が必要となったケースが 10 件以上あったり、また、対象企業のシステム委託業者との連携が必要となったりと、サービス提供側の認識を改める必要があることが分かった。

上記を踏まえると、サービスの普及には、検知・対応のみの提供ではなく、中小企業側で、通報や対策を受け入れやすくするためのサービスの提供や、ネットワークセンサーなどの機器設置において、もう 1 段分かりやすい仕組み（操作動画など）と、訪問でのサポートを用意することが望ましいことが分かった。

4.3 中小企業において必要なセキュリティ対策

本実証事業では、以下の 2 つのコンセプトをベースに、地域実証および関連する各種取り組みを通じて、中小企業向けサービスの在り方を検討する上で、参考になる知見を得ることができた。

I. 地域一帯を 1 つの大きな単位としてセキュリティ対策母体とする手法の検証
II. コロナ禍を配慮した新たな働き方に即したサイバーセキュリティの実態把握

4.3.1 中小企業向けサービスの在り方

本実証事業の目的である「地域一帯を 1 つの大きな単位としてセキュリティ対策母体とする」を、サービスの在り方として、前述の「4.2 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」に対し、下記 3 つを実現が可能な、「図 4.3.1-1 スキーム」にて、地域密着の商工会議所や業界団体などと連携し、「地域全体を、1 つの会社と見立てた SaaS 型セキュリティサービス」を提供する、共同セキュリティ対策の仕組みを定義した。

- 「意識」→会員に対するセキュリティの啓発活動が可能
- 「資源」→共同とすることで、個社の費用を抑えることや情報共有が可能
- 「能力」→駆け付け対応で、地域密着の IT 業者と連携し、地域への還元が可能

共同セキュリティ対策の仕組みについては、現在、3 つの商工会議所と、1 つの地方業界団体と相談のうえで、継続的に検討を進めている。ポイントとしては、集客面、コスト面、他者優勢性に関して、ビジネス提案できるかという点となり、今回の実証事業の結果をベースに協議中となる。

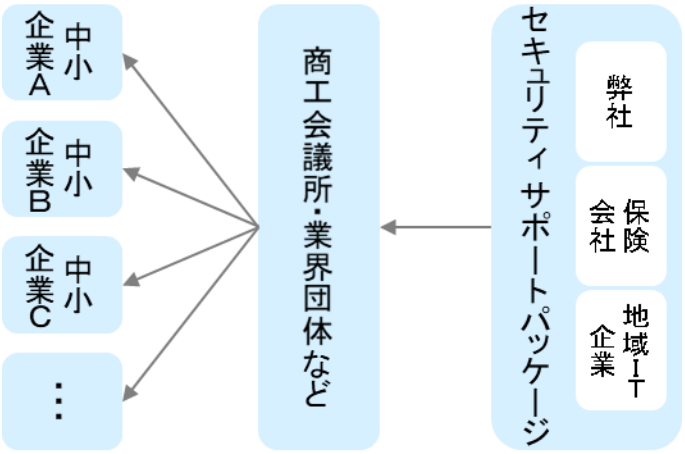

図 4.3.1-1 スキーム

また、提供課題である低価格化についても、下記 3 つの技術項目を基に、「図 4.3.1-2 技術イメージ」のように、リスク面と、技術面でバランスをとり提供することを定義した。

- 中小企業が導入しているエンドポイントセキュリティ対策
- 監視対象を絞り込んだ、富士ソフトセキュリティ監視システムの導入
- 簡易サイバー保険によるリスクヘッジ

本実証事業では、「監視対象を絞り込んだ、富士ソフトセキュリティ監視システムの導入」を検証したが、「3.3.2 サイバー攻撃実態調査結果」で示すとおり、計画どおりのアラートを検出することができた。

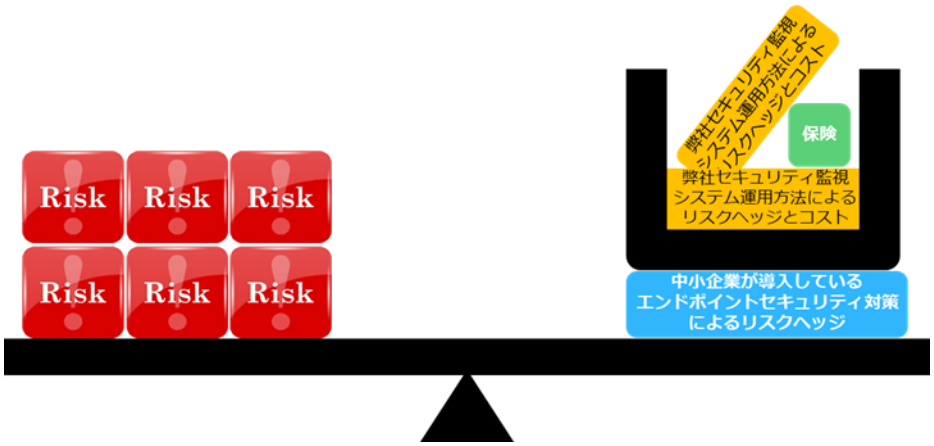

図 4.3.1-2 技術イメージ

4.3.2 コロナ禍を配慮した新たな働き方に即したサイバーセキュリティの実態把握

本実態把握は、「コロナ禍を配慮した新たな働き方に即したサイバーセキュリティの実態把握」について、前述の「3.2.8 在宅勤務/テレワーク意識調査」に加え、本実証事業に参加、かつ、実際に在宅勤務を導入し実施している 7 社の企業に、アンケートをした結果を加味して考察したものである。

なお、説明会アンケート時には、34%の企業で在宅勤務を実施しているとのアンケート結果だったが、簡易セキュリティ診断時には、10%の企業まで減じたことは、在宅勤務が、定着していない可能性がうかがえる。

(1) 在宅勤務/テレワーク時のセキュリティリスク把握状況

既に、在宅勤務/テレワークを実施されているため、リスクに関して、未回答を除くと 100%の企業で「知っている」との回答を得た。しかしながら、在宅勤務/テレワークのリスク軽減に有効な、対象者へのセキュリティ対策の指示が、実施されていないケースがあるなど、前述の「図 3.2.8-2 在宅勤務/テレワークを進める上でのセキュリティの課題の調査」の結果と合わせて考察すると、「どこまで、なにを？」や、「社員への教育が分からない」という声が散見されており、一般のオフィス環境と同様の問題が生じている結果となった。

在宅勤務/テレワーク環境のセキュリティ対策は、対象者が自ら IT 環境を整備・管理する必要があるが、大半は IT に対する知識、経験が不足していることが多いと想定される。そのため、サービス提供側としては、オフィス環境と在宅勤務/テレワーク環境の両方を守る仕組みを提供することが望ましいと考える。

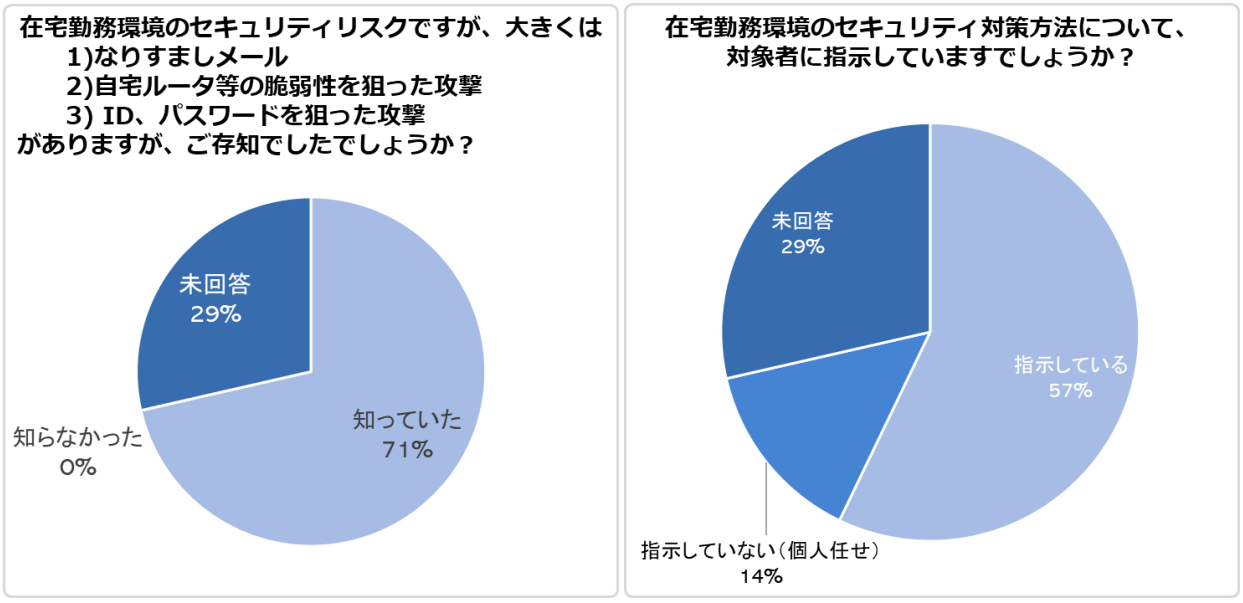

図 4.3.2-1 在宅勤務/テレワーク時のセキュリティリスク把握状況調査

(2) 在宅勤務/テレワーク時のセキュリティニーズ確認

一方、在宅勤務に関するセキュリティニーズとして、万が一、在宅勤務中にウイルス感染などの被害にあった場合、どのような対応を希望するか確認した。結果、在宅勤務場所まで、駆け付けを希望するケースがあり、働き方改革により、セキュリティのサービスの仕方も新たに検討する必要があることが分かった。

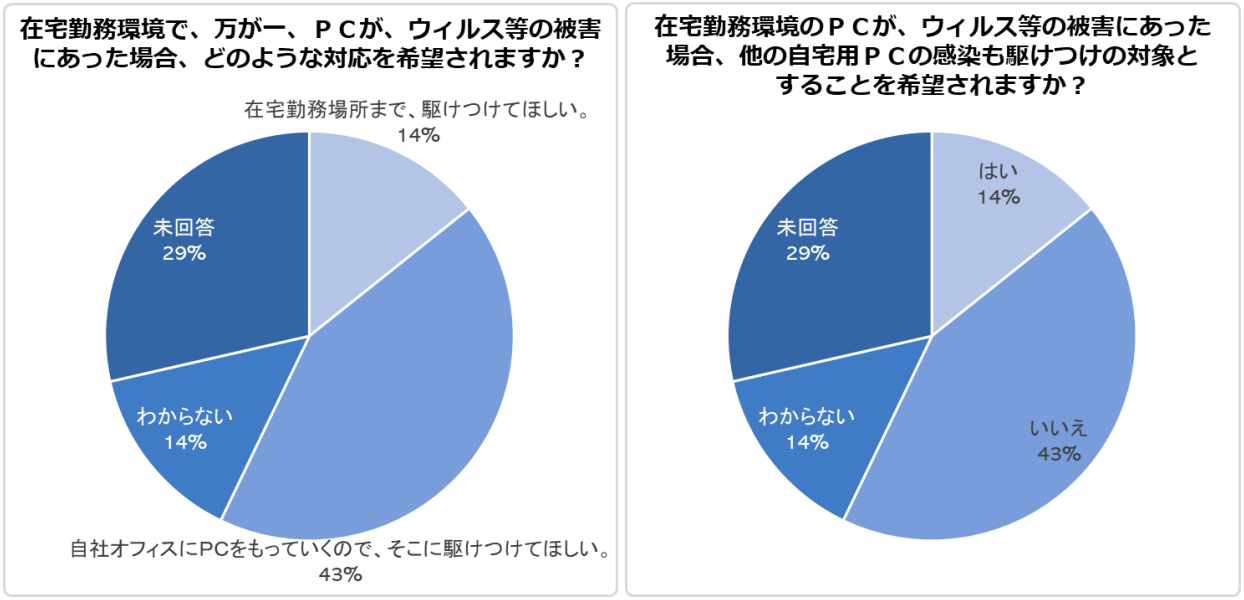

図 4.3.2-2 在宅勤務/テレワーク時のセキュリティニーズ確認

4.3.3 本実証事業を通じて得た知見などに基づき検討したサービス

(1) セキュリティ監視システム

今回、ネットワークセンサーを、想定した接続方法のみで設置できた実証参加企業は、10 社のみであり、それ以外は、L2 スイッチの追加購入や、テレワーク用ネットワークセンサーの改良による小型オフィス兼用モデルで実現した。

中小企業の多くでは、ファイヤーウォール ＋L3 スイッチなどの構成は少なく、ルーターのみのケースが多いことが判明したため、今後は、テレワーク用ネットワークセンサーを更に改良し、中小企業向けに相応しい、機器に仕上げることを検討する。

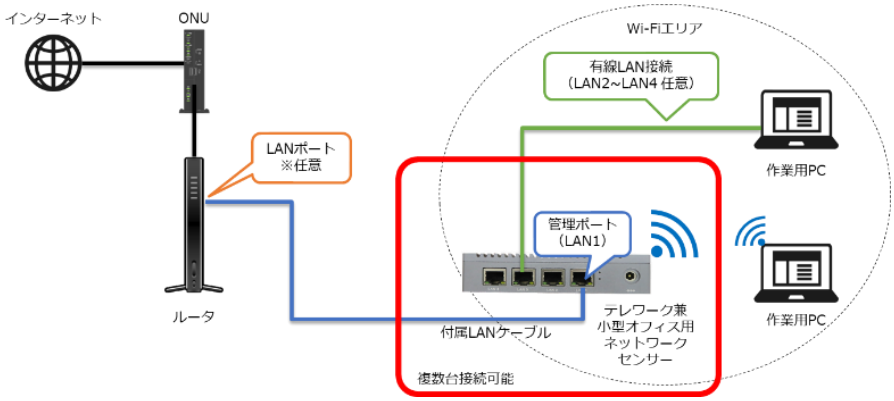

図 4.3.3-1 小型オフィス設置例

(2) セキュリティ健康診断

当初、セキュリティ監視システムによる収集・分析した結果を提示する予定だったが、簡易セキュリティ診断などで、専門用語が多く、分かりにくいと声が挙がったため、全面的に見直しを実施し、専門用語を減らし、一目で問題点を把握できるように変更を実施した。今後更に改良し、中小企業向けに相応しいサービス化を図ることを検討する。

図 4.3.3-2 セキュリティ健康診断書

4.4 中小企業におけるセキュリティ対策の効果

実証参加企業において、前述の「3.2.3 セキュリティ課題意識調査結果」で示すとおり、約 70%企業がセキュリティに課題を持ち、63 社もの企業が、セキュリティ対策について、「なにを、どこまで？」、「セキュリティ対策したけど本当に大丈夫？」という声が、多い状況であることが分かる結果となった。

セキュリティに関して、一定の興味があるが、どうしたら良いか分からない状態の企業が多いと判断し、本実証事業における簡易セキュリティ診断を、啓発活動の場として考え、全てリモートヒアリングにて、セキュリティ対策の説明を実施し、71 社中 25 社から、SECURITY ACTION の一つ星または二つ星を得たいとの希望があった。

このことから推測するに、リモートヒアリングは、中小企業におけるセキュリティ対策として有効と思われる。

また、今回、簡易セキュリティ診断の結果でも、「なにを、どこまで？」、「セキュリティ対策したけど本当に大丈夫？」という声に応える構成とした。

表 4.4-1 簡易セキュリティ診断構成説明

No.	お客様の声	内容説明
1	セキュリティ対策は、**なにを？**	簡易セキュリティ診断結果で、**弱点を抽出し**記載することで「なにを？」を把握できる結果としている。
2	セキュリティ対策は、**どこまで？**	簡易セキュリティ診断結果のグラフ内で、目標（対象企業が所属する**業界平均のセキュリティ対策状況**）を設定することで「どこまで？」を把握できる結果としている。 また、解説と（なるべく費用のかからない）対策を記載し、自社の守るべき**情報資産や業務都合**を基に、優先度を付けて自ら、対応できる結果としている。
3	セキュリティ対策したけど、**大丈夫？**	セキュリティ監視システムで、対象企業の社内システムやネットワークを監視・分析し、**セキュリティ状態上の問題がないか、見える化**し、「大丈夫？」を示す**セキュリティ健康診断と推奨対策**を記載することで、簡単に問題点と対策を把握できる結果としている。

本件、報告会のアンケートにて、「簡易セキュリティ診断」と「セキュリティ健康診断」について、確認した結果でも、報告会参加企業の約 80%から「良かった」との回答を得る結果となり、効果的であったことを認識した。

5. 実証を踏まえたビジネス化に向けた検討

5.1 サイバー保険の活用

前述の「4.1 実証参加企業におけるサイバー攻撃の実態」および「3.2.6 サイバー攻撃意識」で示すとおり、中小企業でも、サイバー攻撃に晒されている現実と、約 79%もの多くの中小企業で事業継続の不安を抱えていることが判明した。

このため、中小企業でも、事業継続に対するリスクヘッジ可能なサイバー保険は、今後重要になると考えられる。

しかしながら、前述の「3.2.7 サイバー保険意識調査結果」で示すとおり、約 80%の企業でサイバー保険を認識しておらず、知名度のなさが普及に繋がらない一因と考えられる。

また、費用に関しても、前述の「3.2.4 セキュリティニーズ調査結果」で示すとおり、セキュリティにかける年間費用が、約 43%もの企業で、5 万円以下であるため、低額である必要があると考えられる。

これら前提条件を基に、東京海上日動火災保険と検討している保険は、以下のとおりである。

基本的には、「図 5.1-1 サイバーリスク保険 補償内容一覧」と「図 5.1-2 サイバーリスク保険 今後の展開」のとおり、低価格な初期対応費用と、本格対応費用を分離し、2 階建てとし、

- 1 階建て部分は、セキュリティ監視サービスなどにバンドルする全員加入のもの
- 2 階建て部分は、希望する企業に対する任意加入のもの

を用意し、普及を図ることを検討している。

なお、ヒアリングの最中に、よく耳にした「自社が被害に遭う想像ができないため、保険の検討ができない。」、「保険屋さんの情報は大企業のものでしょ。中小企業だと想像できない。」という声に対しては、中小企業を中心とした事例紹介が必要となるため、今後予定されている「サイバーセキュリティお助け隊サービスブランド化」における「情報共有」で、これら事例紹介が増えることを期待している。

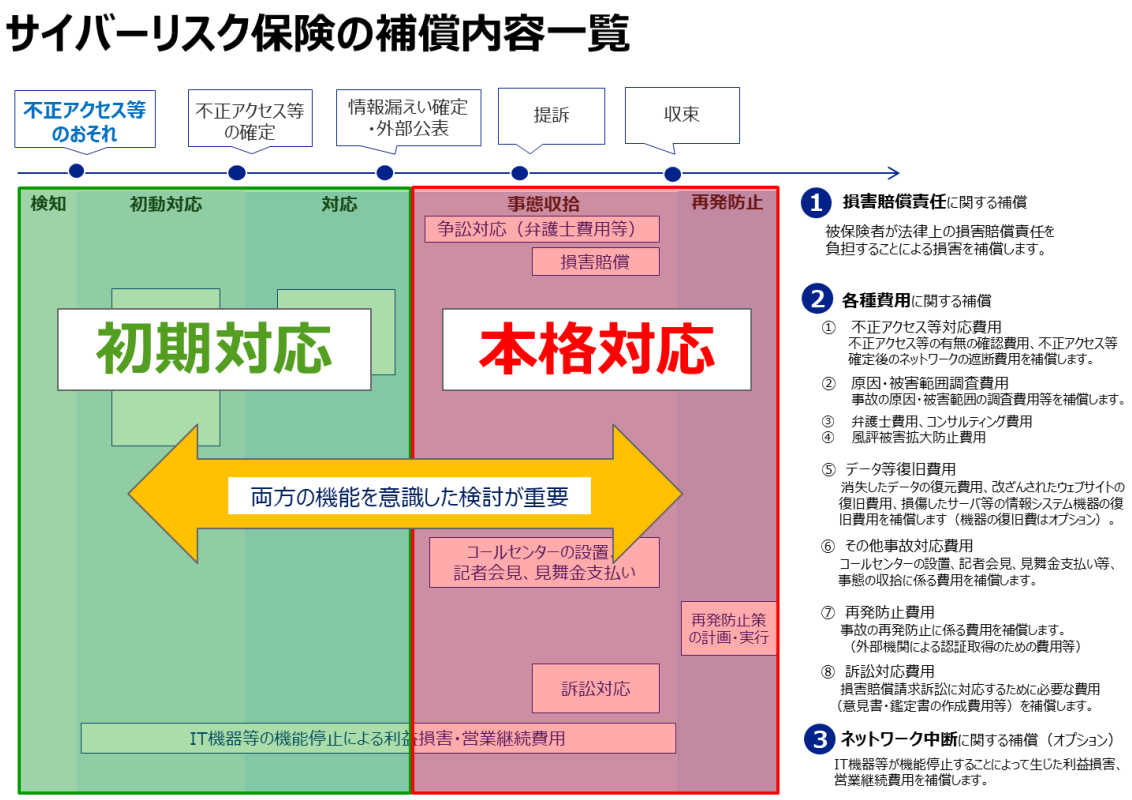

図 5.1-1 サイバーリスク保険 補償内容一覧

今後の展開

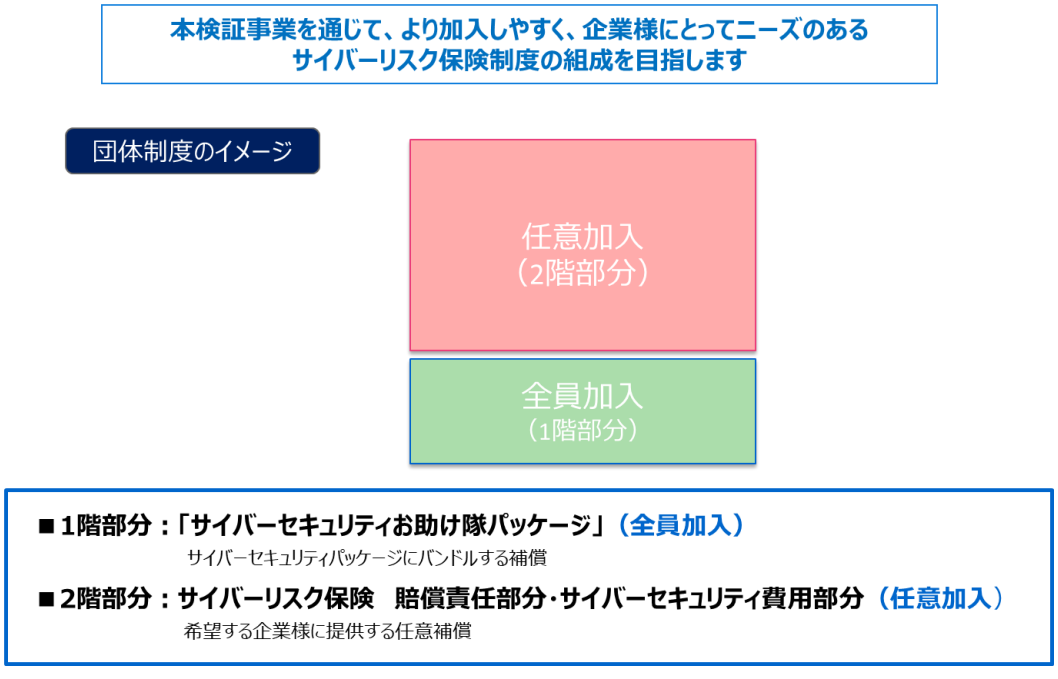

図 5.1-2 サイバーリスク保険 今後の展開

5.2 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

5.2.1 実証を踏まえた中小企業向けビジネス化の課題

(1) 必要性における課題

前述の「4.2 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」で示すとおり、中小企業にセキュリティを普及させるために、課題に対する対策について検討を進めている。

◆「なぜ、必要？」「対岸の火事」

身近な実例の欠如のため、イメージできないことによることが大きい。このため、中小企業での事例にて、啓発することを検討している。

◆「なにを、どこまで？」「セキュリティ対策したけど、大丈夫？」

セキュリティ対策という幅広く漠然とした用語が先行しているために、「なにを、どこまで？」ということや「セキュリティ対策したけど、大丈夫？」ということが不安視されている。　この状況を変えるため、以下を検討している。

- 簡易セキュリティ診断で「なにを、どこまで？」の声に応え、企業の啓発を支援する。
- セキュリティ健康診断で「セキュリティ対策したけど、大丈夫？」の声に応え、企業のセキュリティ対策の向上を図る。

◆「セキュリティ運用」

半数の企業で、導入したまま運用がされないため、サイバー攻撃を受けているかどうか、また、被害があるかどうかも、分からないという実態となっている。

このような状態でも、セキュリティ対策の向上が図れるサービスを検討している。

(2) コストにおける課題

現在、「4.3.1 中小企業向けサービスの在り方」内の「図 4.3.1-2 技術イメージ」で示すとおり、リスク面と技術面によるバランスで、低価格化を検討しているが、アンケートで判明しているセキュリティ対策の年間予算のボリュームゾーンに近づけるためコストの検討を進めている。

(3) セキュリティ監視サービスにおける課題

現在、本実証事業で発生した、課題に対する対策について検討を進めている。

◆セキュリティ監視サービス

- 分かりやすさの追求
  簡易セキュリティ診断時ヒアリングで受けた指摘の中に、「専門用語が多く難しい」との意見が多数あり、商用化時には、専門用語を少なくし、分かりやすさを追求する。
- 通報フォロー
  通報しても、「忙しくて対応しきれない」、「IP アドレスによるパソコンの特定が難しい」など、通報が有効に活かせないケースがあり課題となっている。通報方法を含め、再検討を実施する。
- 保守委託業者
  ユーザー企業によっては、社内システムやネットワークなどの管理を、保守委託業者に委託しているケースがあるため、保守委託業者がいる場合の連携方法を検討する。

◆ネットワークセンサー

- 実機
  主に、小型オフィス向けネットワークセンサーで発生した問題として、複合機(スキャナー)との相性が悪い、Wi-Fi 電波干渉の発生などがあったため改善を検討する。
- 設置
  本実証事業では、予め設置に問題が発生することが予想されていたため、設置マニュアル整備や、個別の接続案内による対策を実施していたが、10 社以上で設置するために訪問が必要となった。このため、設置マニュアルの改善を検討する。
  また、ネットワークセンサーに対する各種設定を、事前のヒアリングで得た情報で設定し提供していたが、ヒアリングと異なることが多く、再送などの手間が多く発生した。このため、ユーザーで変更できるように改善を検討する。

5.2.2 商用化段階での中小企業向けサービスについて

(1) セキュリティ監視サービス

下記「図 5.2.2-1 セキュリティ監視システム」を中心に、今回の実証事業で課題となった、前述の「5.2.1(3) セキュリティ監視サービスにおける課題」を改善し、セキュリティサポートパッケージとして提供することを検討する。

提供内容は、以下を想定している。

◆ユーザー企業向け

- 簡易セキュリティ診断＋セキュリティ健康診断
- セキュリティ監視（SaaS 型）
- 相談窓口
- リモート支援
- 駆け付け支援

◆事業実施主体者向け

事業実施主体者向けに、営業/運営ツール、紹介資料などの整備をする。

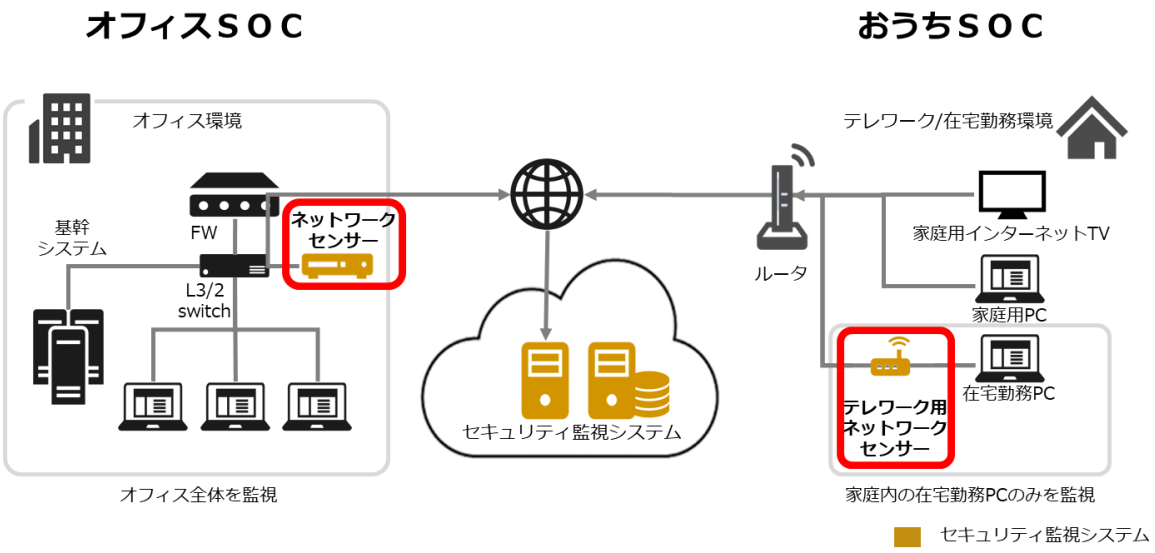

図 5.2.2-1 セキュリティ監視システム

(2) 座組・商流

下記「図 5.2.2-2 座組・商流」で示すとおり、座組・商流の検討を進めてる。
各ステークホルダーの役割は、以下を想定している。

◆商工会議所/業界団体

事業実施主体、ユーザー企業募集/管理/料金徴収、地域 IT 事業者募集/管理

◆地域 IT 事業者

駆け付け対応（現地支援）

◆東京海上日動火災保険

サイバーリスクに関する保険提供

◆富士ソフト

セキュリティサポートパッケージ提供
（セキュリティ監視機器/セキュリティ監視/技術支援/相談受付窓口/リモート支援/サイバー簡易保険など）

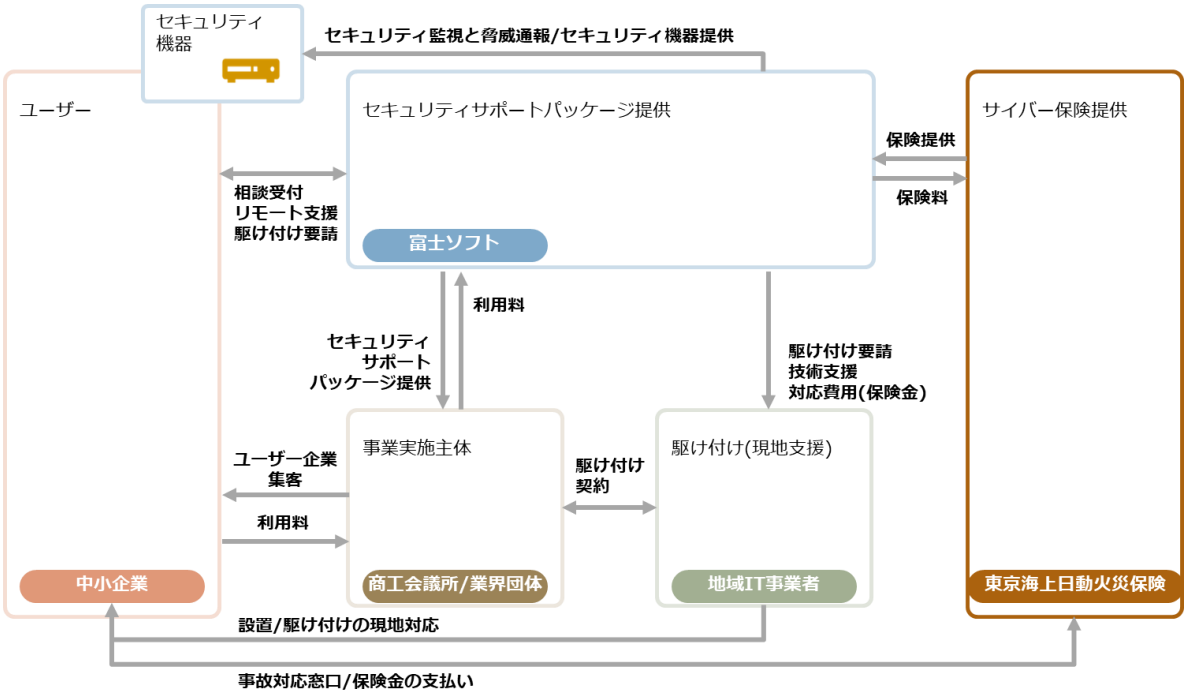

図 5.2.2-2 座組・商流

(3) サイバー保険

前述の「5.1サイバー保険の活用」で示すとおり、サイバー保険の検討を進めている。

◆セキュリティサポートパッケージ バンドルの簡易保険（1 階部分の全員加入）

全員加入の簡易保険については、以下の内容で検討を進めている。

- セキュリティ監視システムでサイバー攻撃を検知し、リモート対応が困難と判断し、駆け付け対応が必要と判断した時。
- 上記駆け付け対応にかかる費用を保険金で支払う。なお現在、保険金の限度額については、検討を進めている。

◆上乗せ保険 賠償責任部分／サイバーセキュリティ費用部分（2 階部分の任意加入）

個人情報を大量に扱うなど、企業の業務内容によっては、更に補償が必要となるため、業務都合に合わせて、上乗せの保険が契約できる準備をしている。この上乗せ保険は、東京海上日動火災保険が提供しているサイバー保険を適用することで検討を進めている。

(4) サービス提供の可能性について

本実証事業の目的である、「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浸透・定着させることである。」という点については、本実証事業終了時のアンケートに、約 84％の企業から「良かった」「意識変化があった」と回答を得た点から考えると、まずは達成できたものと考える。

しかしながら、今回の実証事業でも、前述の「4.2(1)「意識」に関する課題」が大きく影響していることは明確であり、「5.2.2(2)座組・商流」のステークホルダーと、サービス提供の実現に向けた協議でも、ステークホルダーが、この点を危惧していることが改めて明確となった。

多くの中小企業では、セキュリティに対する最大の課題である、「リスクが分からないことが、リスクである」ということに気が付かないまま、セキュリティの事件は「対岸の火事」と考えている。

このため、まずは監視サービスの継続を希望される実証参加企業に対し、「5.2.2(2)座組・商流」のステークホルダーと連携の上で体制を構築し、小規模のモデルケースとしてスタートを狙う。ステークホルダーとなる、対象エリアの商工会議所、および各業界団体とは継続して協議をし、その過程で会員企業へのセキュリティの啓発とマーケティング調査を図る予定である。

なお、本実証事業終了時点で、価格次第との前提付きで、23 社から継続の要望を受けている。

以上