

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: 岐阜県を中心とする中部エリア)

成果報告書

請負事業者: MS&AD インターリスク総研株式会社



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

目次

1. サマリー	2
2. 背景・目的	3
2.1. 実証事業請負の背景	3
2.2. 本実証事業の目的	4
3. 実証事業の概要	5
3.1. 実証対象エリアの選定	5
3.2. 実証運営体制と全体概要	5
3.2.1. 実施体制と役割分担	5
3.2.2. 本実証事業の全体概要	8
3.3. 実証メニューとスケジュール	10
3.4. 実証参加企業	11
4. 実証事業の詳細	14
4.1. 事業説明会	14
4.2. 実証参加企業の募集	15
4.2.1. 中部電力グループによる募集	16
4.2.2. 申込受付・実証メニュー管理システムの構築	17
4.2.3. 協力先のネットワーク	18
4.3. 中小企業の実態把握	19
4.3.1. 本実証事業（岐阜県を中心とする中部エリア）における検証モデル	19
4.3.2. 簡易セキュリティ診断	21
4.3.3. 標的型メール訓練	26
4.3.4. ワンストップセキュリティサービスの提供	30
4.3.5. EDR の提供	39
4.3.6. 事後アンケートの実施	44
4.3.7. 事後ヒアリングの実施	57
4.3.8. 地域コミュニティとの連携	69
4.4. 成果報告会	70
4.4.1. 開催概要	70
4.4.2. 開催結果	71
4.4.3. 成果報告会でのアンケート結果	71
5. 実証結果から得られた考察	73
5.1. 実証参加企業におけるサイバーセキュリティの実態	73
5.2. 中小企業におけるサイバーセキュリティの課題	78
5.3. 実証を踏まえ今後中小企業に必要と考えるサイバーセキュリティ対策	79
6. 実証を踏まえたビジネス化に向けた検討	84
6.1. 中小企業向けセキュリティサービスのビジネス化に向けた課題・検討	84

6.1.1.	実証事業終了後の継続的なサービス提供	84
6.1.2.	サイバー保険の活用	86
6.2.	まとめ	90

1. サマリー

本報告書は、MS&AD インターリスク総研株式会社（以下「MS&AD インターリスク総研」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。

岐阜県を中心とする中部エリア内の中小企業 76 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。

- 簡易セキュリティ診断
- 標的型メール訓練
- ワンストップセキュリティサービス
- EDR（エンドポイント監視サービス）

2. 背景・目的

2.1. 実証事業請負の背景

本実証事業の仕様書および提案書の内容から、「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:岐阜県を中心とする中部エリア)」(以下「本実証事業」)の背景を振り返る。

経済産業省の「産業サイバーセキュリティ研究会」ワーキンググループ2(経営・人材・国際)において、中小企業向けサイバーセキュリティ支援体制の整備の必要性が2018年ごろから議論され始め、当初はサイバー保険とIT人材の確保を連携させる取り組みが検討されていた。

その後、IPAが2019年1月に公表した「情報セキュリティ10大脅威2019」において、前年圏外から「サプライチェーンの弱点を悪用した攻撃の高まり」が初めて4位にランクインしたことから、サプライチェーンを構成する中小企業においてもサイバーセキュリティ対策の必要性に焦点が当てられ、2019年度に全国8地域でサイバーセキュリティお助け隊実証事業が行われた。

MS&AD インターリスク総研は愛知県において事業請負し、約200社を対象に実証を行った。その詳細は別途提出済みの令和元年度サイバーセキュリティお助け隊事業(愛知県)成果報告書にて報告済みである。

特に、セキュリティ機器・サービス設置の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、中小企業が確保できない「検知」や「初動対応」をカバーするサービスが必要であること、中小企業にとって許容可能な価格帯のサービスが必要であること、等が、MS&AD インターリスク総研が請け負った事業においても確認された。

また、MS&AD インターリスク総研が2019年に実施した「企業のサイバーセキュリティ対策に関する調査」において、過去のサイバーセキュリティ事故発生の有無について確認したところ、「把握していない・わからない」と回答した企業の割合は、サイバーセキュリティ社内組織体制を持つ企業の回答(6.5%)に比べ、持たない企業の回答(13.1%)は倍以上の開きが見られた。中小企業はリソースが不足しており、実施できていても「防御」までのケースが多く、「検知」や「対応」に必要な体制整備・人材育成等へ経営資源を投入できていない実態が見られた。

一方で、実施したアンケートやヒアリングの結果からは、「信頼できるサービスやベンダーを活用したセキュリティ体制構築が重要であり、価格はどちらかと言えば安い方が良いが、“ただ安ければ良い”というものではない」という事業者の意識があることがうかがえた。

中小企業の実態を踏まえた、意識向上と利用しやすいセキュリティサービスの提供を両輪で実施する必要があるという認識のもと、2020年度事業は、2019年度事業結果も踏まえて、中小企業の実態やニーズをより細かく把握し、持続可能なセキュリティ対策支援体制を構築することを目指して実施されたものである。

2.2. 本実証事業の目的

MS&AD インターリスク総研は本実証事業において、二つのコンセプトの実証を目的とした。

- ① 地域の中核企業・重要インフラ企業(電力、ガス等)を核とした中小企業向けサイバーセキュリティ普及モデルの構築
- ② 地域サイバーセキュリティコミュニティとの連携による全国展開可能な地域サイバーセキュリティ支援体制モデルの構築

中小企業と幅広く関わりがあり、持続的で不可欠なサービスを提供している地域の中核企業・重要インフラ企業(電力会社グループ)とともに中小企業のサイバーセキュリティ対策を行うことを目指した。

その理由として、地域の中核企業・重要インフラ企業は、幅広い支援を行うリソースがあり、中小企業との密接な結びつきを可能とする基盤を備えている。ここにサイバーセキュリティの観点も加え、中小企業に幅広いセーフティネットを提供するモデルを構築することが可能と考えた。

また、大企業を中心とした取引先等を含めたサプライチェーンのサイバーセキュリティ対策の重要性を訴えることで、サプライチェーンの対策促進も行うことを目指した。

更に地域サイバーセキュリティコミュニティは、地域によって成熟度は異なるものの、全国で支援体制を活性化させる動きが始まっている。この連携は全国その他地域でも展開可能なモデルとなり得る実現可能性の高いモデルとして実証することを目指したものである。

これらの検討にあたっては、令和元年度のサイバーセキュリティお助け隊で明らかとなった中小企業の実態・ニーズや課題を踏まえ、中小企業の実態やニーズを更に深掘りし、中小企業の意識向上を図るとともに、中小企業がより利用しやすいサイバーセキュリティ支援体制を構築し、普及可能で持続可能なビジネスモデルを構築することが必要であると認識して取り組んだ。

特に重要なのは「普及可能で持続可能なビジネスモデルの構築」と考える。中小企業側がサイバーセキュリティに関心を持ち、安心して利用し続けることができるモデルを作り、これを普及していくことが中小企業のサイバーセキュリティ対策を強化する最大のポイントである。

3. 実証事業の概要

3.1. 実証対象エリアの選定

岐阜県を中心とする中部エリアで実証を行った。

MS&AD インシュアランスグループおよび中部電力グループは、岐阜県を中心とするエリアにて新たにサイバーセキュリティサービスの試験的な提供を計画し、警察など行政機関との連携も進めていた。

岐阜県警、愛知県警のサイバー犯罪対策課とも連携が進み、中部経済産業局や名古屋工業大学、中部サイバーセキュリティコミュニティ(CCSC)などとは令和元年度事業から情報交換を行い、検討の土壌ができている点に加え、中小企業と幅広く関わりがあり、持続的で不可欠なサービスを提供している地域の中核企業・重要インフラ企業である中部電力グループとの協業という観点から、岐阜県を中心としつつも、中部エリア(中部電力営業エリア全域)を対象として、実証対象エリアを選定したものである。

3.2. 実証運営体制と全体概要

3.2.1. 実施体制と役割分担

MS&AD インシュアランスグループのリスク関連コンサルティング会社である、MS&AD インターリスク総研を主体とし、中部電力グループと協業したサイバーセキュリティ支援サービスの実証を行った。

サイバー保険に関連する部分は同じく MS&AD インシュアランスグループの保険事業会社 2 社(三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社)が検討を行った。

① 実施体制

中部地域のサイバーセキュリティ団体等との強力な結びつきを持つ中部電力株式会社は、関係団体やグループ会社との調整を担った。

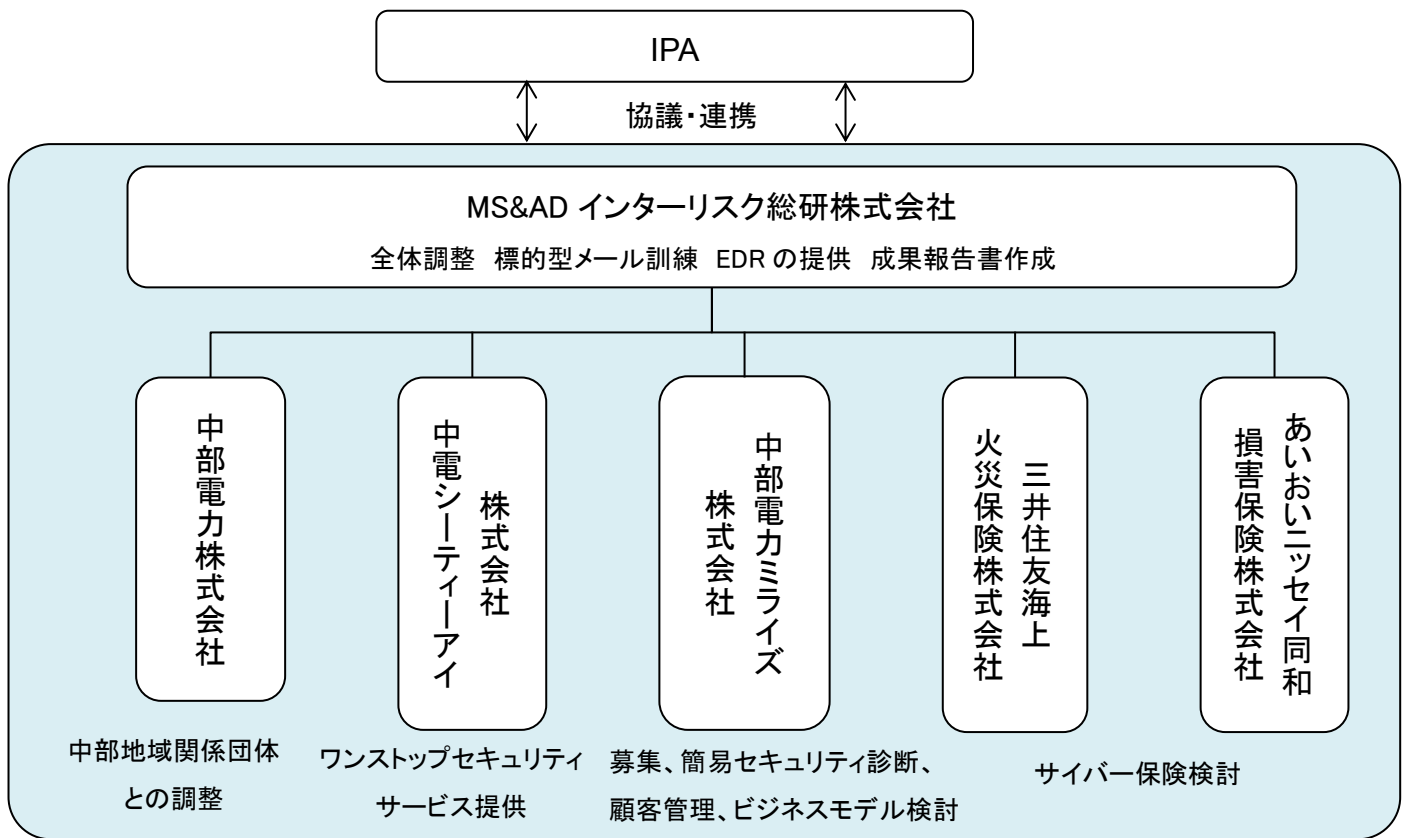
電力販売事業を行う中部電力ミライズ株式会社は接点のある大手企業のサプライチェーンや経営層との関係が深い中小企業に対して、実証参加企業募集、簡易セキュリティ診断、セキュリティ対策の必要性の訴求など実証参加企業の接点となる対応部分を中心に担った。

セキュリティ商材は、西日本電信電話株式会社(NTT西日本)より OEM 提供を受けた株式会社中電シーティーアイが提供を行った。

MS&AD インシュアランスグループの保険事業会社 2 社は、中小企業に最適なサイバー保険および付随サービスの検討を行った。

MS&AD インターリスク総研は説明会開催や募集管理など運営全般含めた全体調整に加え、標的型メール訓練や EDR 提供といった個別セキュリティサービスの提供を担った。

図 1 実施体制



② 実施内容・役割分担

表 1 実施内容と役割分担

実施項目	実施内容	目的	主な実施者
実証地域の選定	実証地域の選定	中部地域でのセキュリティ強化	全社
説明会の開催	説明会の開催	実証事業内容の説明	インタ総研
実証参加企業の募集	実証参加企業の募集	・サイバーセキュリティに課題を持つ企業の選定 ・具体的な募集活動	中電 ミライズ インタ総研
中小企業の実態把握	中小企業向けサイバーセキュリティサービスの構築	ニーズや実態を踏まえた中小企業 サイバーセキュリティ対策支援体制構築	インタ総研
	簡易セキュリティ診断	実証参加企業の簡易セキュリティ診断による 実態把握	ミライズ インタ総研
	標的型メール訓練	標的型メール訓練による従業員意識実態把握と セキュリティ意識向上	インタ総研
	ワンストップセキュリティサービスの提供	中小企業から見たシンプルなサービスの提供	CTI
	EDR の提供	UTM で特定の難しい端末単位での監視	インタ総研
	事後アンケートの実施	実証参加企業の課題の実態調査	ミライズ インタ総研
	事後ヒアリングの実施	ヒアリングによる一段踏み込んだ調査	インタ総研
地域実証の実施	実証事業終了後の継続的なサービス提供	重要インフラ企業を核とした中小企業向け サイバーセキュリティ普及モデル構築	全社
	地域コミュニティとの相乗効果	地域コミュニティとの連携による サイバーセキュリティ支援体制モデル構築	中電 インタ総研
実証結果を踏まえた検討の実施	中小企業向けセキュリティ簡易保険サービスの検討	セキュリティ簡易保険サービスのあり方 普及策について検討	MS AD
	実証結果を踏まえたビジネスモデルの構築、継続サービスの提供	サイバーセキュリティサービスの開発と継続可能なモデル構築	全社
成果報告会の開催	成果報告会の開催	成果報告を通じた中小企業の意識向上、 普及啓発	インタ総研
成果報告書の作成	成果報告書作成	事業の成果と課題・反省点を整理し、 今後の横展開への活用	ミライズ インタ総研

※表の略称は次のとおり。インタ総研…MS&AD インターリスク総研、中電…中部電力、ミライズ…中部電力ミライズ、CTI…中電シーティーアイ、MS…三井住友海上火災保険、AD…あいおいニッセイ同和損害保険

3.2.2. 本実証事業の全体概要

新型コロナウイルスの感染が完全には収束しない状況下での実証となることを鑑み、感染リスクを減らすため、可能な限り非対面での実施を志向した。また、実証事業に関する情報管理を徹底すると同時に、効率性・利便性にも配慮し、参加企業から入手する情報は、クラウド上に作成する本実証事業専用のシステムで管理を行った。

本実証事業の全体概要・総括は以下のとおりである。

① 募集活動

説明会や協業各社のネットワーク、地域コミュニティ等との連携により募集を行った。

当初ターゲットにしていた企業群が UTM 等のセキュリティ機器を既に導入しているケースが多く、募集に苦戦した。説明会の追加開催やターゲットを変更した募集活動などを行うことで、最終的には予定数を超過する実証事業参加を得ることができた。ターゲットとして見込んでいた企業規模がやや大きかった点が問題であった。対象を規模の小さい企業まで広げることで、中電グループへの安心・信用というブランドを活かした募集活動を進めることができた。

募集にあたっては、Web システムを活用した申込システムに集約することで、効率的な申込受付・データ収集等を行った。

詳細は「4.2 [実証参加企業の募集](#)」

② 簡易セキュリティ診断・実態把握

令和元年度事業で得られたデータを活用し、IPA の情報セキュリティ自社診断シートなどの項目を反映させ、ベライゾンジャパン合同会社と共同開発した簡易セキュリティ診断ツールを活用した。本簡易セキュリティ診断を実施し、中小企業の実態把握をするとともに自社の強み弱みを明らかにし、意識向上につなげることができた。

※なお、本簡易セキュリティ診断ツールでは SECURITY ACTION の一つ星、二つ星宣言項目をチェックすることで回答項目が自動的に減る仕組みを導入している。

今後は診断後の対策の記載を充実することと、保険引受への活用も見据える。

詳細は、「4.3.2 [簡易セキュリティ診断](#)」

③ 支援体制構築(ワンストップセキュリティサービス、標的型メール訓練、EDR)

中部電力グループ内の連携により、ワンストップセキュリティサービス(コールセンター、UTM 機器設置、駆けつけ対応までワンストップで提供できる体制を構築)を導入・運用する実証を行った。導入までに時間がかかり、実態の調査としての攻撃件数などの把握には課題が残ったが、サービスとして展開する検討の土台としての情報収集は一定実施できた。

詳細は、「4.3.4 [ワンストップセキュリティサービスの提供](#)」

MS&AD インターリスク総研は、標的型メール訓練サービスを提供し、従業員のセキュリティ意識向上を図ると同時に、開封率や教育状況などの実態把握を行った。標的型メール訓練については、中小企業での関心も高く、また結果に対する対策への意欲もあるため、実証事業外にはなるが、行動経済学を活用したフルバージョンの訓練を希望企業向けに実施する予定。

詳細は、「4.3.3 [標的型メール訓練](#)」

MS&AD インターリスク総研の EDR 導入によるエンドポイント監視と初動対応・駆けつけサービスも用意し、セーフティネットを更に強化した。EDR については導入がシンプルで、実施決定企業へのスピーディーな展開が可能であった。また実証を通じて得られた経験をもとに、12 月に本サービスを一般向けにリリースすることができた。

詳細は、「4.3.5 [EDR の提供](#)」

このような多重の支援体制を作ることで、防御・検知だけでなく、アセスメント、教育、初動対応までカバーすることができる体制を構築し、有事の際の報告や被害最小化に活用することができ、発注元や取引先にとっても安心できるサービスとなることを目指した。

④ ビジネスモデルの実証

上記③において実証するサービス提供スキームがビジネスとして成立することの検証、実証を進めながら改善を行い、ビジネスモデルの検討を行った。

なお、本実証事業は単に個社のビジネスとして育てるものではなく、同種の「中小企業と幅広く関わりがあり、持続的で不可欠なサービスを提供している地域の中核企業・重要インフラ企業」が保険も組み合わせたサイバーセキュリティサービスを開始する際のモデルケースとして活用し得るものを目指した。

本実証事業を通じて、中部電力グループ内での連携、MS&AD グループとの連携の課題や可能性を確認でき、新たなサイバーセキュリティサービスの提供に向けた準備を進めている。

詳細は、「4.3.1 [本実証事業\(岐阜県を中心とする中部エリア\)における検証モデル](#)」および「6 [実証を踏まえたビジネス化に向けた検討](#)」

⑤ 地域コミュニティとの相乗効果

上記①～④の実証・検討と並行して地域コミュニティとの連携も図った。

今回我々が実証を行った中部エリアには「中部サイバーセキュリティコミュニティ」や、令和 2 年度に新たに設立された「東海サイバーセキュリティ連絡会」といった会議体が存在する。いずれも MS&AD インシユアランスグループおよび中部電力グループが密接に関与する会議体で、「東海サイバーセキュリティ連絡会」に関しては、MS&AD インターリスク総研および中部電力が構成員として参加。

詳細は、「4.3.8 [地域コミュニティとの連携](#)」

⑥ 事後アンケート・ヒアリング

実証終了時に、実証参加企業へアンケート・ヒアリングによりニーズや実態把握を行い、本実証事業における実証内容や検討内容を整理し、本実証事業の成果として活用した。

セキュリティ対策要員の不足などの情報に加えて、中部電力グループがセキュリティサービスを提供することへの信頼度や安心感などが明確となり、地域の中核企業・重要インフラ企業（電力、ガス等）がセキュリティサービスを提供する価値を確認できた。

詳細は、「4.3.6 [事後アンケートの実施](#)」および「4.3.7 [事後ヒアリングの実施](#)」

3.3. 実証メニューとスケジュール

実証メニューおよび本実証事業を通じた検討は下記のスケジュールで行った。

実証参加企業向けメニューである「簡易セキュリティ診断」「標的型メール訓練」「ワンストップセキュリティサービス」「EDR(エンドポイント監視サービス)」は実証事業への参加申込次第、順次提供した。

表 2 実証メニューとスケジュール

実施内容	9 月	10 月	11 月	12 月	1 月	補足説明
説明会の開催	←→					9/7、9/9、9/10、9/17、9/25、9/30、10/5、10/8、10/13、10/16 の計 10 回開催
実証参加企業の募集	←→	←→	←→	←→		
中小企業向けサイバーセキュリティサービスの構築	←→	←→	←→	←→		
簡易セキュリティ診断	←→	←→	←→			参加申込次第、順次提供
標的型メール訓練	←→	←→	←→			参加申込次第、順次提供
ワンストップセキュリティサービスの提供	←→	←→	←→	←→		参加申込次第、順次提供
EDR の提供	←→	←→	←→	←→		参加申込次第、順次提供
事後アンケートの実施				←→		12/10～12/22 にかけて実施
事後ヒアリングの実施				←→		12/16～12/22 にかけて実施
実証事業終了後の継続的なサービス提供			←→	←→		
地域コミュニティとの相乗効果		←→	←→	←→		
中小企業向けセキュリティ簡易保険サービスの検討			←→	←→		
ビジネスモデルの構築、継続サービスの提供			←→	←→		
成果報告会の開催					←→	2021/1/15 開催

3.4. 実証参加企業

本実証事業参加企業数は 76 社となった。

従業員規模別では下記の区分においては、101 名～200 名の企業が最も多いが、半数以上が 100 名以下の企業となった。

業種は「製造業・建設業・運輸業」が最も多く、半数以上を占めた。

図 2 実証参加企業の内訳(従業員規模別) (N=76)

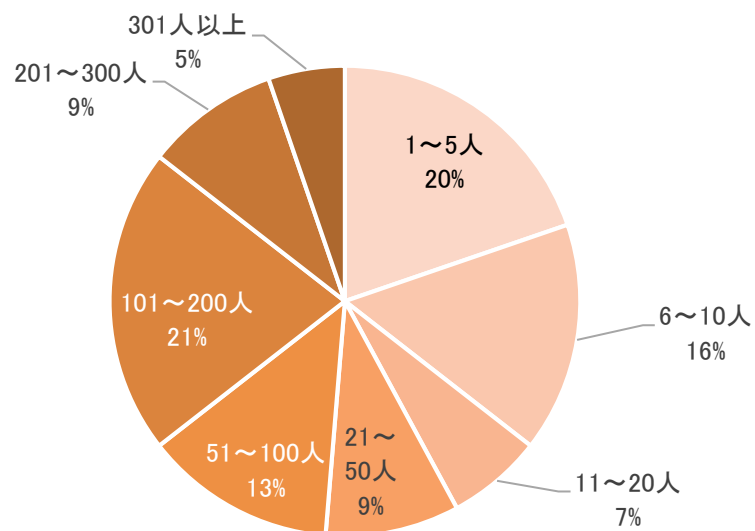
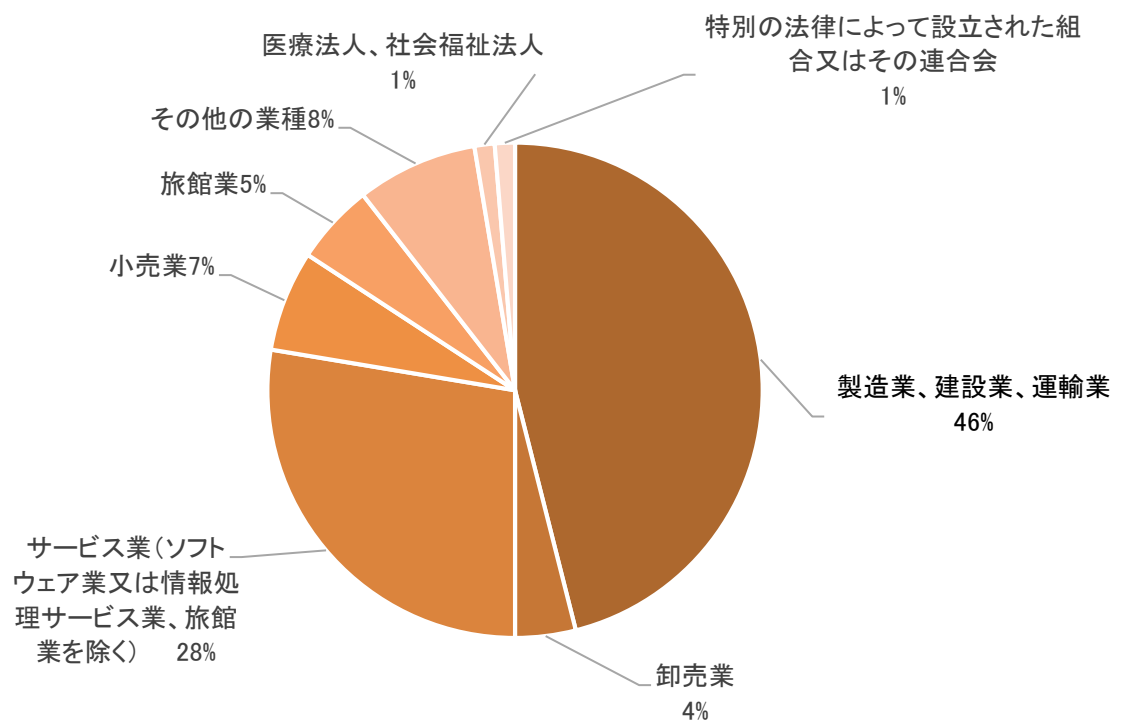


図 3 実証参加企業の内訳(業種分類) (N=76)



企業規模では「資本金 5,000 万円以下」が 7 割を占め、企業の所在地では「岐阜県」が約半数を占めた。

図 4 資本金別 (N=76)

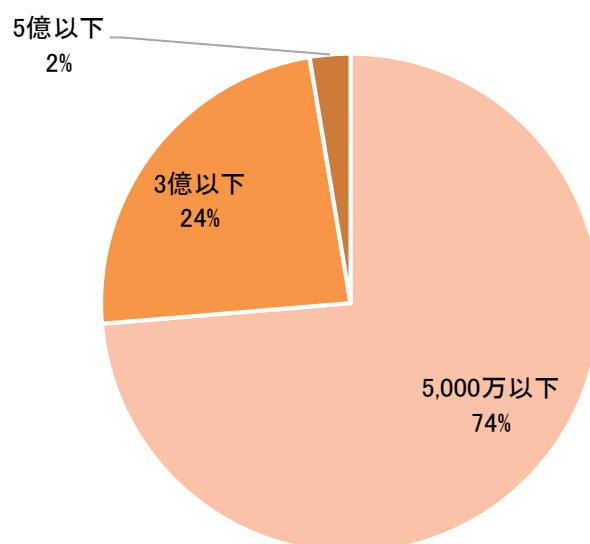
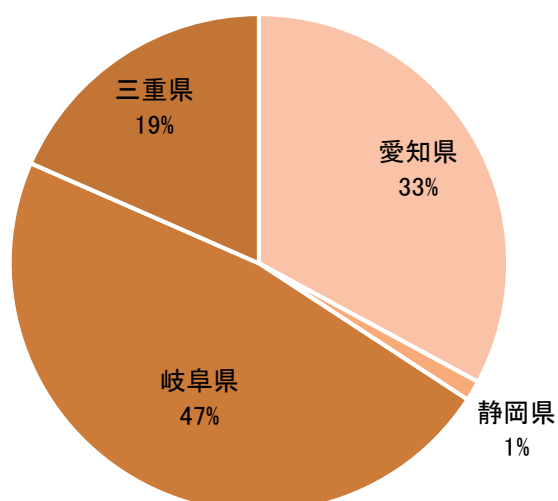


図 5 所在地別 (N=76)



4. 実証事業の詳細

4.1. 事業説明会

本実証事業に関心のある中小企業を説明会に呼び込み、事業の目的を説明した。

当初、対面とリモートの双方を開催予定であったが、新型コロナウイルスの感染状況等を踏まえ、全てリモートによる Web 会議方式とした。Web としたこと、実証参加企業が伸び悩んでいたこともあり、当初の予定から追加して計 10 回開催した。

説明会では、本実証事業への参加を呼びかけるとともに、SECURITY ACTION および中小企業の情報セキュリティ対策ガイドライン等の普及に向けた周知啓発活動を行った。なお、事業申込時アンケートや事後アンケートで対応したため、事業説明会参加者にアンケートは実施していない。

最終的には予定数を超過する企業が事業に参加することとなったが、説明会参加数が少なかった要因は、実証事業期間が短いため説明会開催案内～開催までの期間が短かった点が挙げられる。

一方で最大の要因は、募集の中心ターゲットとした中部電力ミライズの取引先に対しては直接訪問やメール、電話、DM による説明を軸としたためと考えられる。

後述する「本実証事業を知ったきっかけ」という事後アンケートの結果で約 7 割が「中部電力ミライズの紹介」を挙げていることがそれを裏付けている。

実際に説明会に一般参加した企業よりも、個別訪問等により説明を行った方が実証事業への参加率は良く、中小企業にとっても信頼のおける事業者から直接説明を受けた安心感が参加の決め手となったと考えられる。

表 3 事業説明会

説明会	日程	時間帯	参加数計
事業説明会 (Cisco WebEx によるリモート開催)	9 月 7 日(月)	13:30～15:00	19 社 (27 名)
	9 月 9 日(水)	13:30～15:00	
	9 月 10 日(木)	13:30～15:00	
	9 月 17 日(木)	13:30～15:00	
	9 月 25 日(金)	13:30～15:00	
	9 月 30 日(水)	13:30～15:00	
	10 月 5 日(月)	16:00～17:00	
	10 月 8 日(木)	10:00～11:00	
	10 月 13 日(火)	14:00～15:00	
	10 月 16 日(金)	15:00～16:00	
説明会アジェンダ	(1)お助け隊事業(岐阜県を中心とする中部エリア)事業説明 (MS&AD インターリスク総研)		

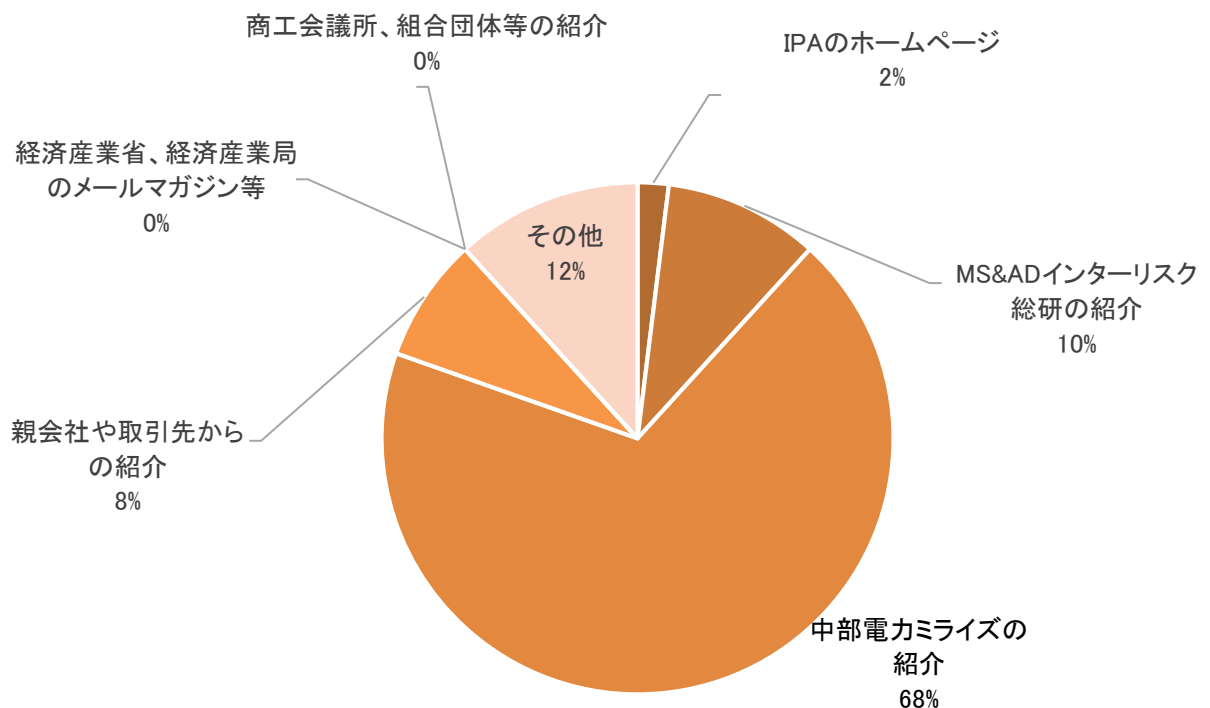
4.2. 実証参加企業の募集

本実証事業では、対象エリアにおいて、中小企業 50 社以上の実証参加企業数を確保することを予定していた。最終的に 76 社の参加を得て実証事業を行った。

募集にあたって当初苦戦をしたものの、追加募集策を実施したことで予定数の企業の参加を得た。

募集の中心ターゲットとした中部電力ミライズの取引先に対しては直接訪問やメール、電話、DM による説明を軸に募集活動を行った。下図は事後アンケートにより実証参加企業に聴取した本実証事業を知ったきっかけである。

図 6 本実証事業を知ったきっかけ (N=51)



4.2.1. 中部電力グループによる募集

本実証事業の実証参加募集は中部電力グループのネットワークを活用し、電力供給・販売サプライチェーンも含めた中部地域の中小企業の募集を行うことを目指した。

中部電力ミライズの取引先企業を中心にメールおよび訪問による PR を中心に実施したが、中部電力ミライズの個別担当企業の大半が既に UTM を設置している企業が多く、申込登録状況に応じて下記の追加募集策を実施した。

- ・個別担当企業以外への一部訪問 PR
- ・県警のサイバー犯罪対策課や一部の業界団体への PR
- ・中部電力ミライズ子会社の取引企業への訪問 PR
- ・ダイレクトメールによる PR 等

これにより、前述のとおり、実証参加企業の約 7 割が中部電力ミライズを通じて実証事業に参加したものである。アンケートやヒアリング結果にもあるとおり、信頼のおける企業から直接説明を受けたことが大きな要因であると考えられる。

表 4 中部電力ミライズによる募集活動実施数

PR 手法	実施件数	実施企業数
訪問	282	252
電子メール(訪問との重複を含む)	142	127
ダイレクトメール	96	96

4.2.2. 申込受付・実証メニュー管理システムの構築

本実証事業への参加申込、簡易セキュリティ診断、ワンストップセキュリティサービスやEDR、標的型メール訓練など各種サービスの実施に必要な情報を一元管理して受け付けることができるシステムを本実証事業専用として準備、活用した。

各メニューの進捗を協業各社とスムーズに情報共有することができた。

本システムに持たせた主な機能は下記のとおり。

- ・実証事業への仮申込、本申込
- ・実証事業の概要説明、参加資格、実証メニューの紹介
- ・説明会や問合せ一覧資料の掲載
- ・事業説明会、成果報告会へのアクセス
- ・顧客別ステータスのリアルタイム管理、顧客との対応記録 等

図 7 申込受付システム ホーム画面イメージ



4.2.3. 協力先のネットワーク

中部電力グループによる募集を主軸としつつも、その他関係先にも広く声かけを行った。

中部エリアには「中部サイバーセキュリティコミュニティ(CCSC)」や、中部経済産業局および総務省東海通信局の主催により、これから立ち上げ予定の「東海サイバーセキュリティ連絡会」といった会議体が存在し、これら会議体の構成員や、地域のステークホルダーとして欠かせない岐阜県警、愛知県警、名古屋工業大学、中部経済産業局などと連携調整は昨年度実証時より進めていたこともあり、これら協力先のネットワークに依頼しての募集も行った。

MS&AD グループのネットワークを活用し、三井住友海上火災保険およびあいおいニッセイ同和損害保険の代理店およびその取引先のうち、特にサイバーセキュリティ対策に関心が高く、積極的な実証事業参加が期待できる企業については参加呼びかけを行った。

中部電力ミライズによる声かけ以外の募集手段の主なものは以下のとおりである。

- ・中部経済産業局を通じた周知
- ・中部サイバーセキュリティコミュニティ(CCSC)構成員へのメール案内
- ・東海サイバーセキュリティ連絡会への周知
- ・令和元年度お助け隊事業関係先への周知
- ・MS&AD インターリスク総研の医療機関向けサイバーリスク外部評価サービス利用者へ周知
- ・ITC 中部への周知
- ・岐阜県情報産業協会への周知
- ・愛知県中小企業団体中央会への周知
- ・三井住友海上、あいおいニッセイ同和損保の取引先への周知 等

4.3. 中小企業の実態把握

4.3.1. 本実証事業(岐阜県を中心とする中部エリア)における検証モデル

地域中核企業・インフラ企業が新たにサイバーセキュリティサービスを立ち上げ、持続可能な支援体制を構築することを目指した。

中小企業の経営層と対話機会が多く、密接な関わりがある中部電力ミライズが実証参加企業との接点を担い、募集活動やサイバーセキュリティ意識調査、セキュリティ事前診断を行った。

中電シーティーアイが提供する「ワンストップセキュリティサービス」の申込受付～設置完了まで、中部電力ミライズおよび中電シーティーアイがサポートする支援体制を構築した。

更に中部電力ミライズは、MS&AD インターリスク総研が提供する EDR と標的型メール訓練サービスを紹介することで、中小企業にとって豊富なセキュリティサービスの展開を目指した。

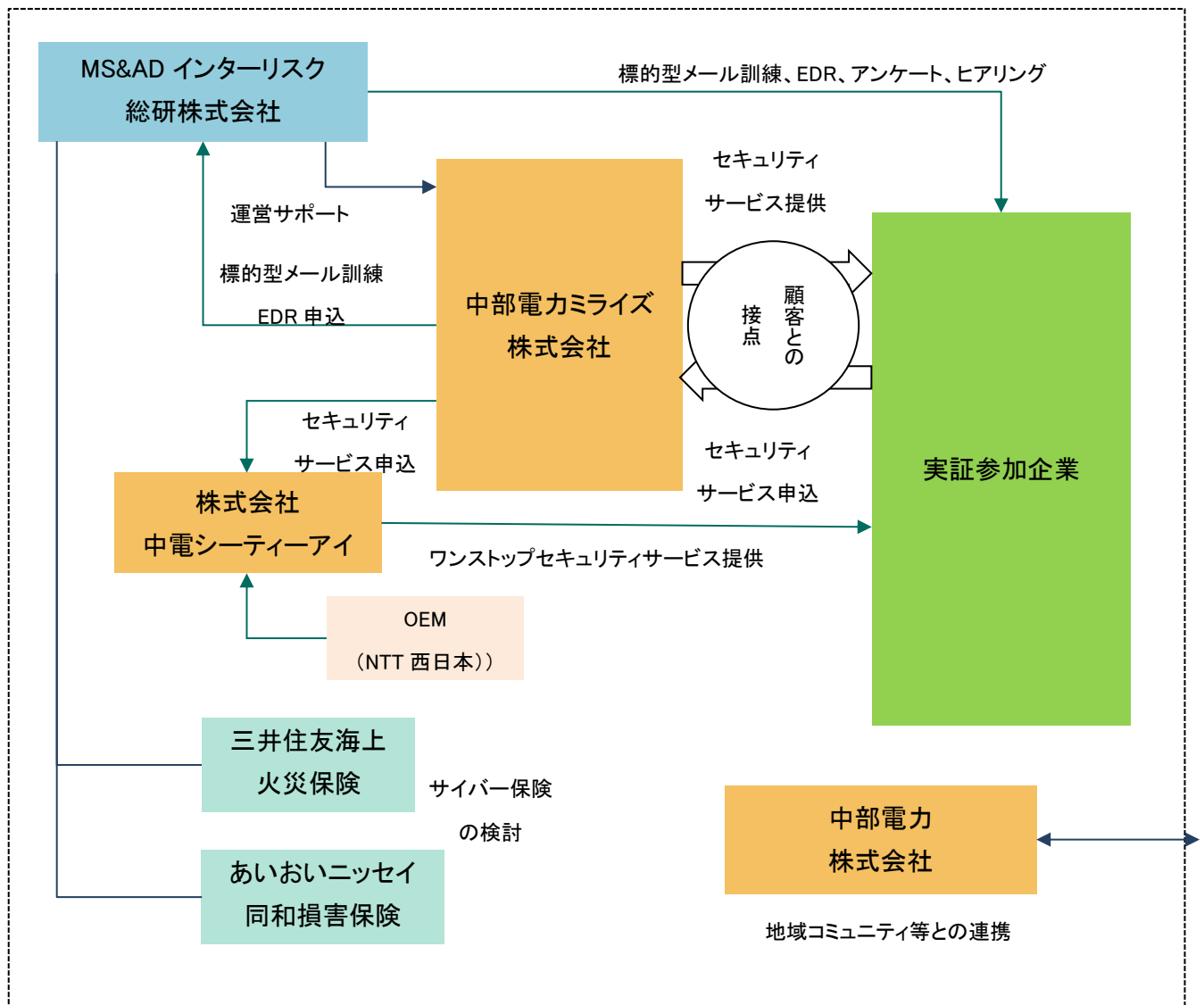
三井住友海上とあいおいニッセイ同和は実証のニーズを踏まえたサイバー保険の検討を行い、価格面、補償内容面、加入方法(加入スキーム)面等、多角的な視点で中小企業が加入しやすいサイバー保険のあり方について検討した。

本実証事業を通じて、各種提供サービスの有用性、中小企業のニーズや価値観を検証することができた。また、中部電力グループ内での連携、MS&AD グループとの連携の課題や可能性を確認でき、新たなサイバーセキュリティサービスの提供に向けた準備を進めている。

並行して地域サイバーセキュリティコミュニティとの結びつきを更に強化し、ビジネスモデル・サイバーセキュリティ支援体制モデル構築に活かす。

詳細は、「[6 実証を踏まえたビジネス化に向けた検討](#)」にて後述する。

図 8 全体スキーム図



4.3.2. 簡易セキュリティ診断

(1) 簡易セキュリティ診断について

令和元年度事業で得られたデータも活用し、MS&AD インターリスク総研および保険事業会社二社がベライゾンジャパン合同会社と共同開発した簡易セキュリティ診断ツールを用いたセキュリティ診断を実施した。

この診断ツールはIPAの「5分でできるセキュリティ自社診断 25問」の要素を参考に、SECURITY ACTION 自己宣言をしている企業は一部自動回答できる仕様を備え、大項目 24 問、小項目 98 問に渡る詳細なセキュリティ診断が可能となっている。

本ツールは 1000 点満点でセキュリティ対策状況を判定し、フィードバックレポートを生成することができるものを開発した。保険事業会社二社は今後、本ツールをサイバー保険の引受判断に活かすことを検討しており、そのための実証も兼ねたセキュリティ診断を提供した。

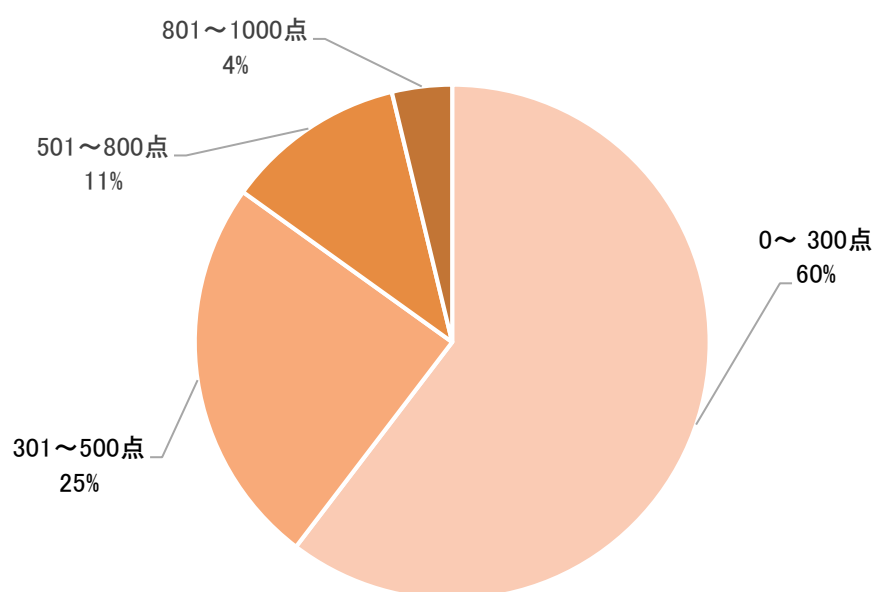
中小企業にとっては自社の実態把握をするとともに、自社の強み弱みを明らかにし、意識向上につなげる。同時に、集計したデータを分析し中小企業の実態調査を行った。

(2) 簡易セキュリティ診断の実施結果

① 全体の傾向

実証参加企業のうち 53 社から回答を得た。53 社の得点分布は下図のとおりとなっており、0 点～300 点が全体の 6 割を占めた。中小企業においては、セキュリティ体制が十分に整っていない現状が見て取れる。しかし自社の取り組み状況を網羅的に振り返ることのきっかけとして有益なツールとの声も多くあった。

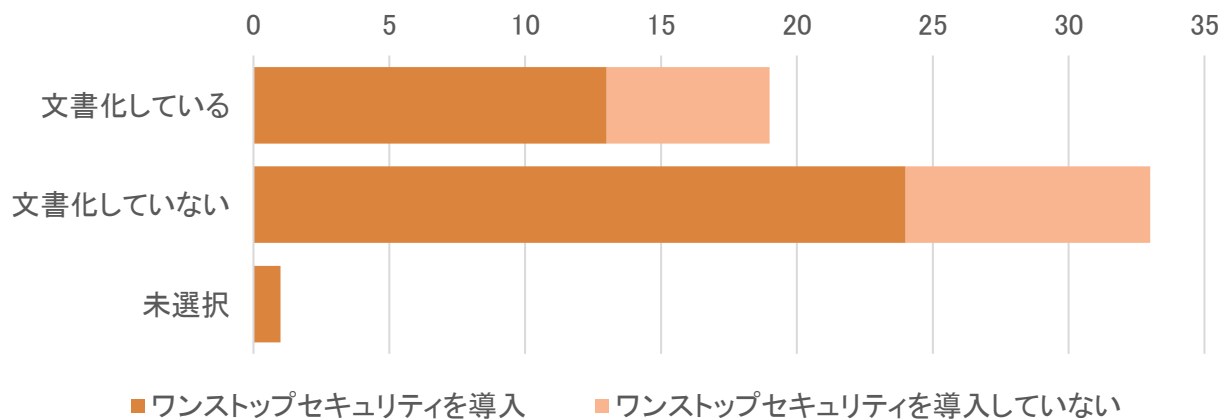
図 9 簡易セキュリティ診断 得点分布 (N=53)



②ネットワークセキュリティに関する設問

また、今回実証事業で提供したワンストップセキュリティサービス導入手続きの一環で会社のネットワーク構成図を提出する必要があった。簡易セキュリティ診断の設問の一つに「会社のネットワーク構成を文書化していますか」があり、本実証事業前から会社のネットワーク構成を文書化している企業は20社弱であった。

図 10 会社のネットワーク構成の文書化 (N=53)

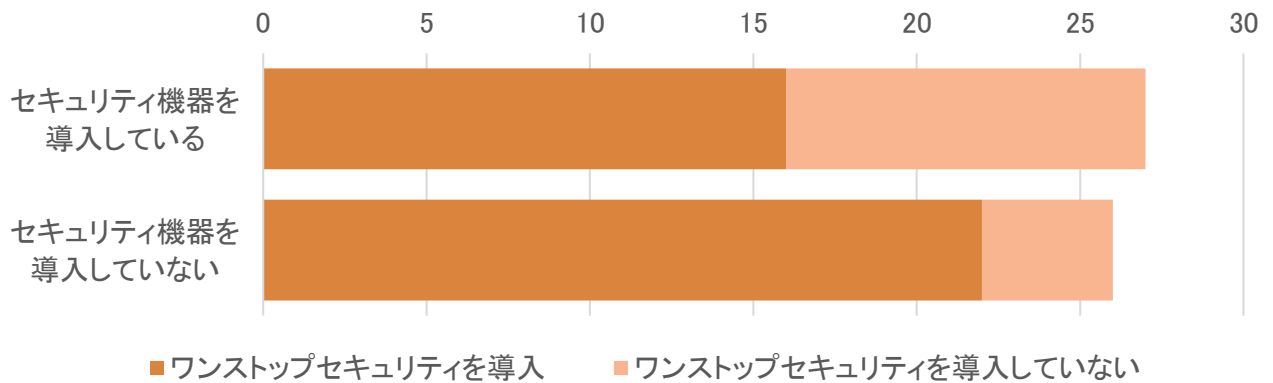


更に、「インターネットの脅威(攻撃)から会社のネットワークを守るためのセキュリティ機器を導入していますか」という設問において、今回の実証事業でワンストップセキュリティサービスを導入した企業との相関を図に示す。

何かしらセキュリティ機器(UTM 機器に限らない)を導入していると回答した中小企業は半数以上であったが、実証事業を通じて確認した際やヒアリング等で聴取した内容から、無償版の対策ソフト等のみを導入しているケースがあった。

特にワンストップセキュリティサービス(UTM)は、「セキュリティ機器を導入していない」と回答した企業のうち新規導入した企業が約85%、「セキュリティ機器を導入している」と回答した企業のうち新規導入した企業が約59%となっており、今回参加した中小企業の大半がこのようなサービスを導入していなかった実態が見て取れる。

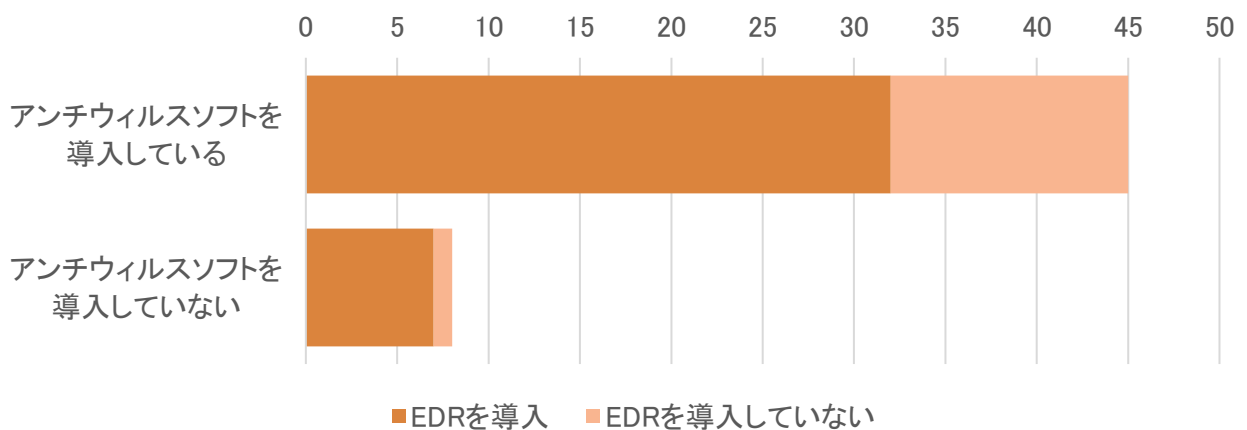
図 11 セキュリティ機器を導入状況(ワンストップセキュリティサービスとの関連) (N=53)



③エンドポイントセキュリティに関する設問

また、「会社で使用するパソコン等の機器のうち、ウィルス対策を必要とする機器にアンチウィルスソフトを導入していますか。」という設問については、中小企業においてアンチウィルスソフトを既に導入している企業は約 85%(45 社/53 社)であることがわかったが、MS&AD インターリスク総研のこれまでの調査と比較すると若干低い結果であった(2019 年度調査: 約 97%)。アンチウィルスソフトを補完する EDR は中小企業にとって受け入れやすく、導入手続きも簡便であることから、既にアンチウィルスソフトを導入している企業でも導入が進んだ。

図 12 業務で使用する PC へのアンチウィルスソフト導入状況 (N=53)



(3) 今後の課題と展望

大項目 24 問、小項目 98 問に渡る詳細なセキュリティ診断であったが、大半の企業が自立して回答できた。エクセルシートへの入力形式であったため、操作性に対して改善を望む声はあったものの、「自社の現状の対策状況について見直すことができた」という声が多く見られた、

今後、中小企業のセキュリティアセスメントツールとして、中小企業が自社の取り組みを振り返り、セキュリティ意識を高めるツールとして活用できることが期待できる。

本実証事業を通じて、中小企業向けのセキュリティサービス提供のドアノックツールや、サイバー保険引受におけるアンダーライティングへの活用も見越して検討を継続する。

なお、大企業向けには更に詳細な設問表があり、今後の活用に向けて併せてブラッシュアップしていく。

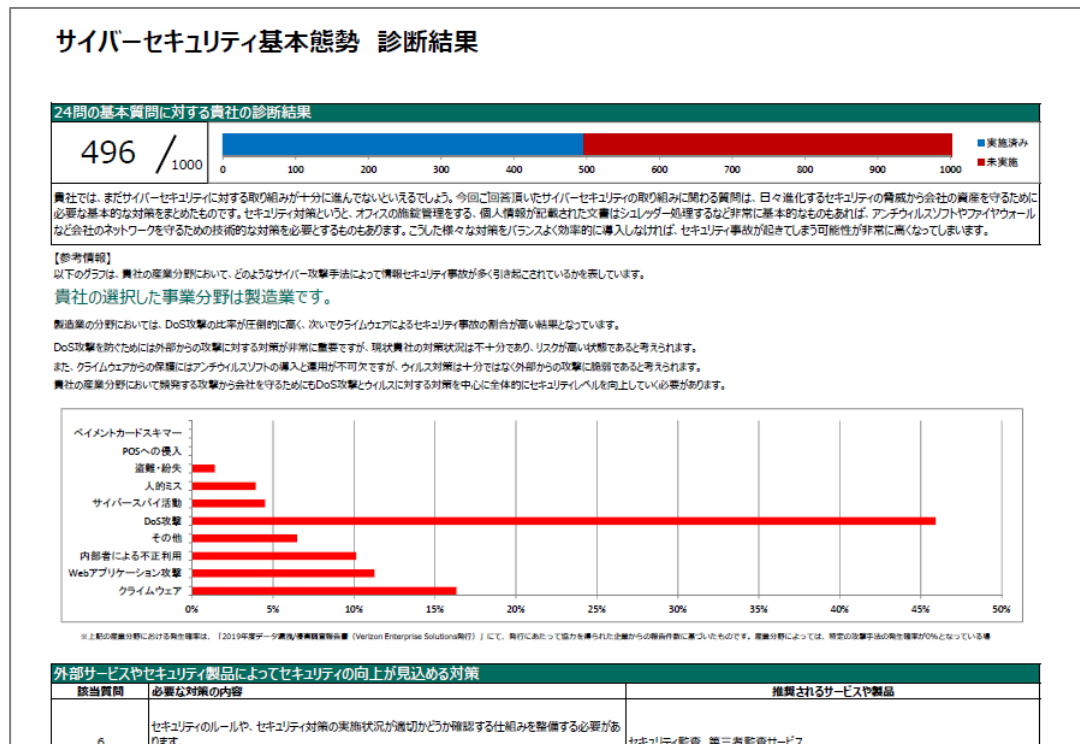
実際の質問票のサンプルは下記のとおり。下図には大項目 1 問目のみを記載しているが、実際は大項目 24 問までである。

図 13 簡易セキュリティ診断 質問票イメージ

サイバーセキュリティ基本態勢診断 質問票	
以下24の質問項目は、日々進化するサイバーセキュリティの脅威から会社の資産を守るために最低限必要なセキュリティ対策の取り組み状況に関するものです。 まずはそれぞれの基本質問回答欄で、「はい」か「いいえ」のいずれかを選択してください。 「はい」を選択した質問では、その下にある複数の選択肢のうち、あてはまるものを全てを“実施済み”を選択してください。	
御社の状況をより詳細に把握するために次の業種から該当する業種を選択してください	未回答
MS&ADグループでは、企業の皆様にIPA（独立行政法人 情報処理推進機構）が提唱する「セキュリティアクション セキュリティ対策自己宣言」の活用を推奨しております。 すでにセキュリティアクションに取り組みされており、一つ星もしくは二つ星の宣言をなさっている場合は、以下の該当するチェックボックスにチェックを入れてください。チェックを入れて頂くと、宣言しているセキュリティアクションの内容に応じて、一部の質問の回答と詳細な選択肢へのチェックが自動で入ります。ただし、回答の自動入力、一つ星、二つ星いずれの場合も、該当するセキュリティアクションのすべての項目に対して実施できている、と宣言している前提としております。したがって、宣言はしているものの一部の項目の実施ができていない場合などを考慮し、自動で入力された回答についてもその内容を確認し、該当しない項目についてはチェックを外す、など回答内容の精査をお願いいたします。 また、一つ星、二つ星の両方を宣言されている場合、以下の選択肢より、二つ星の選択をお願いいたします。	
☐ IPAの「セキュリティアクション セキュリティ対策自己宣言」一つ星を宣言している場合 ☐ IPAの「セキュリティアクション セキュリティ対策自己宣言」二つ星を宣言している場合	未回答 未回答
すべての選択をクリア	
質問	回答
1 情報セキュリティに関わるルールや対策を定めていますか。	☐ はい ☐ いいえ
日々変化する情報セキュリティの脅威から会社や従業員を守るためには、会社として明確なルールを定め、従業員がそのルールを守ることができるように、文書化し通知することが必要です。	
以下の選択肢のうち、あてはまるものを全てにチェックを入れてください（複数回答可）。	
☐	正式に文書化されていないが、従業員の間で認識しているセキュリティルールはある。
☐	情報セキュリティポリシーやセキュリティに配慮したパソコンの利用マニュアルなど必要なセキュリティルールを定め文書化している。
☐	文書化されたセキュリティルールや対策は、年度末など定期的に見直し、必要に応じて改定している。

実際のフィードバックレポートのサンプルは下記のとおり。各項目への回答状況に応じた点数と必要な対策をフィードバックする内容となっている。

図 14 簡易セキュリティ診断 フィードバックレポートイメージ



4.3.3. 標的型メール訓練

(1) 標的型メール訓練について

IPA の情報セキュリティ 10 大脅威 2020 において、2019 年から 2 年連続で 1 位にランクインしている「標的型攻撃による機密情報の窃取」に対する対策メニューとして、標的型メール訓練を実施した。

標的型攻撃を巧妙に模した「訓練メール」を実証参加企業の従業員に送信し、その対応を個々に評価し、適切な対応が行えるように教育の機会を提供した。訓練メールにより、不適切な行動(訓練メール記載の URL をクリック)した従業員に対して、今後適切な対応を行えるように、不審なメール受信時の対応のポイントを学習する画面が表示されるものである。

今回は実証期間が短く、MS&AD インターリスク総研が開発した行動経済学を活用した、学習効果が非常に高い訓練はできず、シンプルな訓練メール開封率を測定するステップのみの訓練となった。

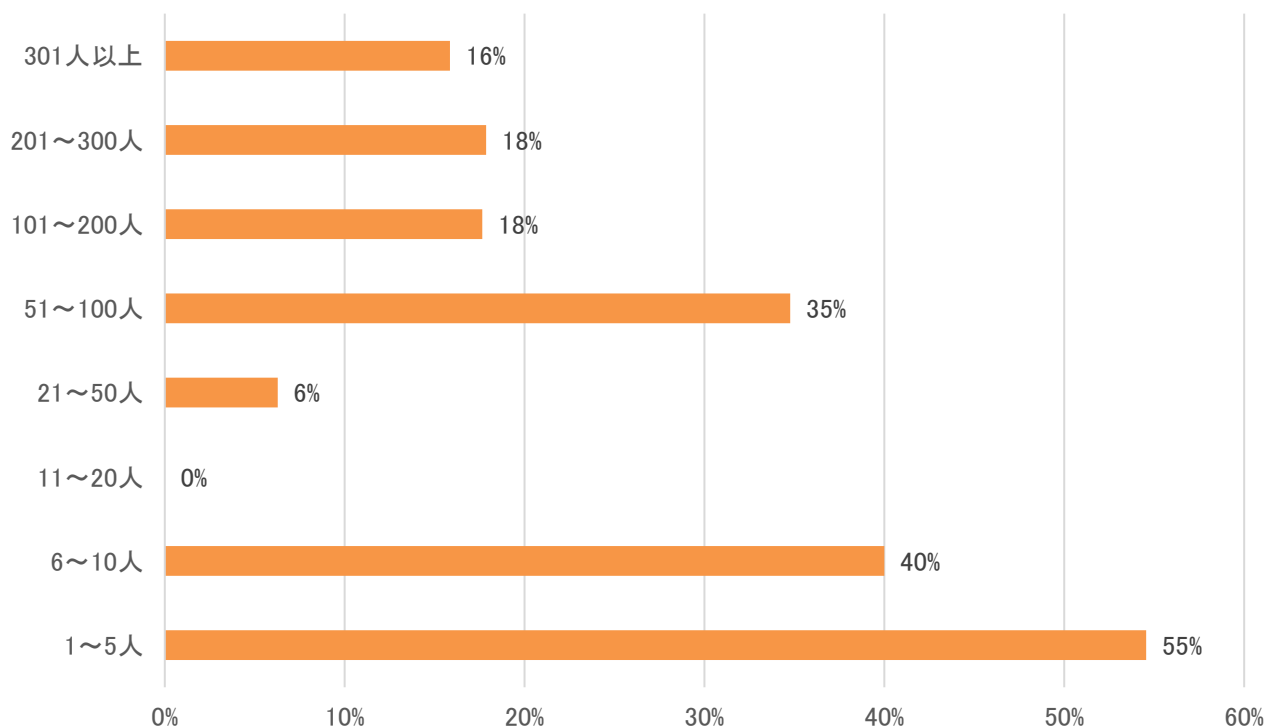
実証参加企業においても、標的型メール訓練を実施したいという希望は多く、本実証事業への募集活動において、その他のメニューが実施できないために参加見送りとなった企業であっても、標的型メール訓練はやってみたいという企業が多く見られた。

中小企業においても、標的型メール攻撃はかなり関心の高いテーマであることがわかる。

(2) 標的型メール訓練の実施結果

実証参加企業のうち、51 社にて標的型メール訓練を実施。開封率等の詳細は以下のとおり。下図は企業規模別の開封率平均値をグラフにしたもの。

図 15 従業員数別標的型メール訓練 開封率平均値 (N=51)



※上図は単に従業員規模別の開封率を平均したものであり、必ずしも従業員数=送信先数ではない

下表の補足説明、およびこのデータから読み取れるポイントとして以下が挙げられる。

- ・本実証事業参加企業のうち、1 社における送信先最大数の企業は「761 件」
- ・このうちメール開封者(URL クリック者)は 13 名で、メール開封率は 2%
- ・一方で、送信先数「126 件」という比較的大きな会社において、メール開封率 12%
- ・従業員(送信先数)10 名以上の企業で開封者 0 人の企業は 2 社のみ
- ・従業員(送信先数)50 名以上の企業になると開封者 0 人の企業は 0 社

どの企業でも本物の標的型メールを開封するリスクはあり、開封率を 0 にするのは難しいことがわかる。標的型メールを開封しないことも大切だが、開封してしまったあとの対処が重要であり、その気付きを与えてくれるのが本標的型メール訓練である。

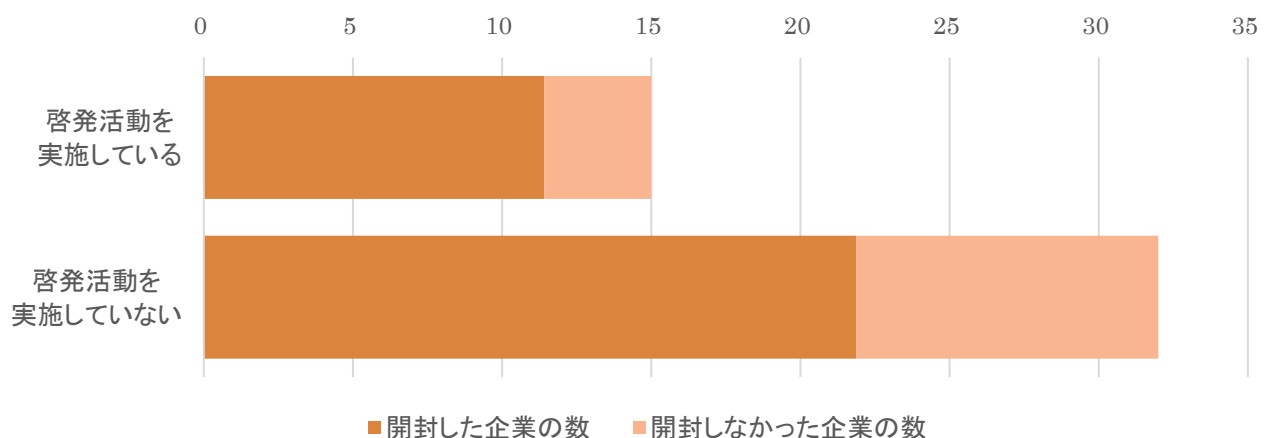
表 5 訓練メール送信数別 開封率平均 (51 社)

項目	開封率 (企業数ベース)	開封率 (送信数ベース)	備考
メール開封率(URL クリック率)	29%	7%	全社
メール開封率(URL クリック率)	15%	7%	送信先 10 名以上
メール開封率(URL クリック率)	5%	3%	送信先 100 名以上

次の図は、簡易セキュリティ診断の設問「従業員に対してセキュリティ教育などの啓発活動を実施していますか」に対して回答があった企業のうち、標的型メール訓練の開封状況との相関を示したものである。

「開封した企業の割合」で言えば、啓発活動を実施しているはずの中小企業の方が高い。一方で啓発活動を実施している企業は従業員 100 名以上の比較的大きな企業が多く含まれている。前述のとおりに、企業規模が大きくなれば開封率を 0 にすることは難しく、真に注意すべきは、予備知識もなく、対処方法もわからないまま、開封してしまう従業員がいることである。

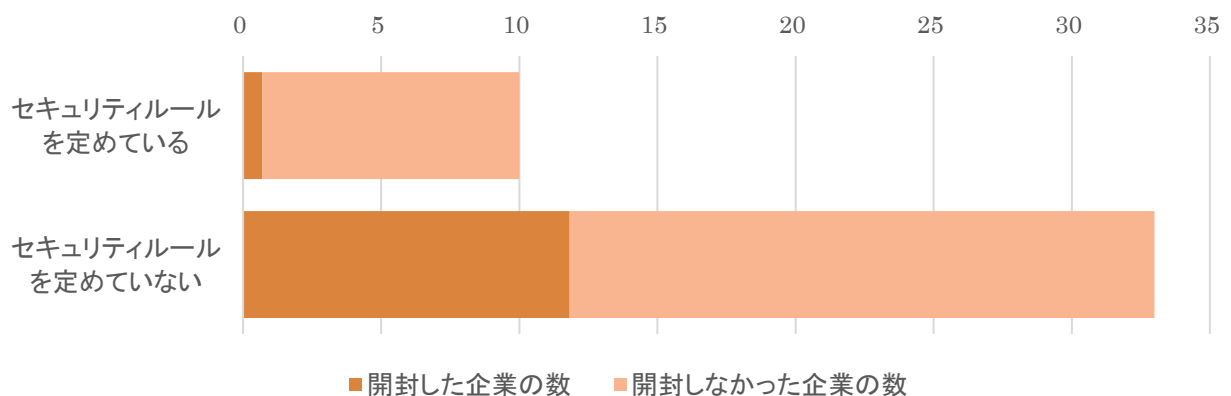
図 16 「従業員に対するセキュリティ教育などの啓発活動実施有無」との関係 (N=53)



次の図は、簡易セキュリティ診断の設問「電子メールの取り扱いに関わるセキュリティルールを定めていますか」に対して回答があった企業のうち、標的型メール訓練の開封状況との相関を示したものである。

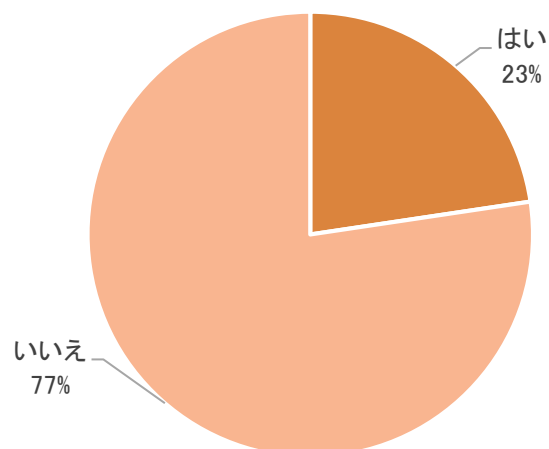
こちらはセキュリティルールを定めている企業が、明らかに開封した割合が少ない。こちらも真に注意すべきはセキュリティルールが定められていない企業であり、開封してしまった場合の対処を教育することが重要である。

図 17 「電子メールの取り扱いに関わるセキュリティルールの有無」との関係 (N=53)



簡易セキュリティ診断の設問「情報漏えいや不正アクセスなどの情報セキュリティ事故の発生に備えて体制や手順を整備していますか。」への回答状況は以下のとおり。8割近くがセキュリティ事故に備えた体制や手順を整備できておらず、標的型メールを開封してしまった際のような「いざという時」の対応が後手を踏み、結果的に被害が拡大してしまうことが懸念される。

図 18 情報セキュリティ事故の発生に備えて体制や手順を整備していますか。 (N=53)



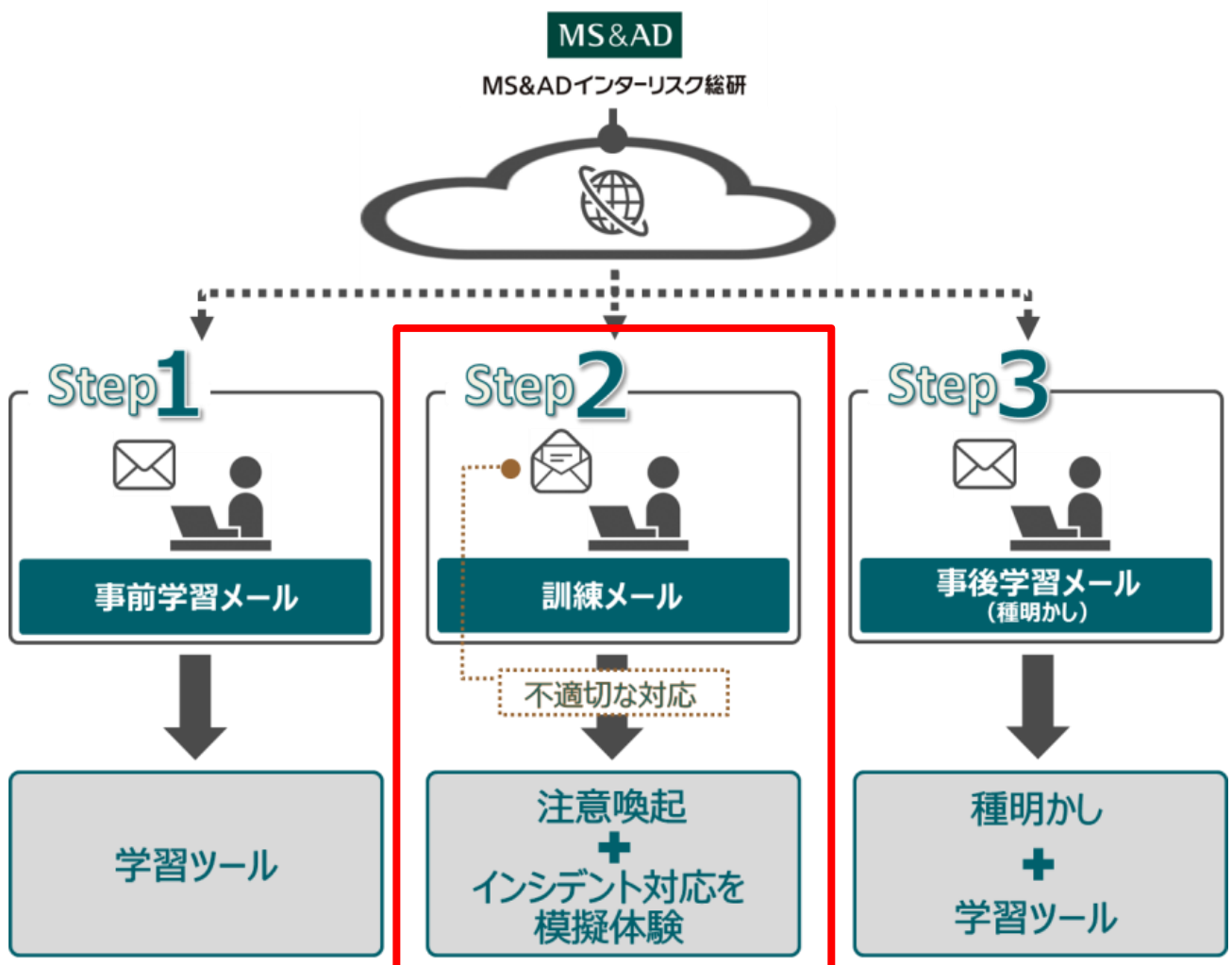
(3) 今後の課題と展望

MS&AD インターリスク総研の提供した標的型メール訓練は、下図のとおり、本来は STEP1(事前学習)～STEP3(事後学習)までのパッケージで提供するものである。しかし、本実証事業においては、実証期間が短いため、STEP2(訓練メール)のみを実施するスリムプランで実施した。

標的型メール訓練については、中小企業での関心も高く、また結果に対する対策への意欲もあるため、実証事業外にはなるが、行動経済学を活用したフルバージョンの訓練を希望企業向けに実施する予定。

本サービスは既に MS&AD インターリスク総研のサービスとして提供しているものである。今回、実証事業に参加した中小企業においても、一定自立してシステム操作を行い、訓練実施までできることがわかった。本実証事業を通じて得られた経験を、今後のサービス提供において活用していく。

図 19 標的型メール訓練 提供フロー



4.3.4. ワンストップセキュリティサービスの提供

(1) ワンストップセキュリティサービスについて

「コールセンター・UTM 設置・駆けつけ対応・監視サービス等の各機能が複数にわかれてしまった」という令和元年度の反省を踏まえ、各機能一体となったセキュリティサービスを活用した。

「インターネットとの境界が一つに集約されている」、「アンチウィルスソフトのみを導入している」、「かつて UTM を導入したものの運用がなされていない」等の企業に最適なサービスである。

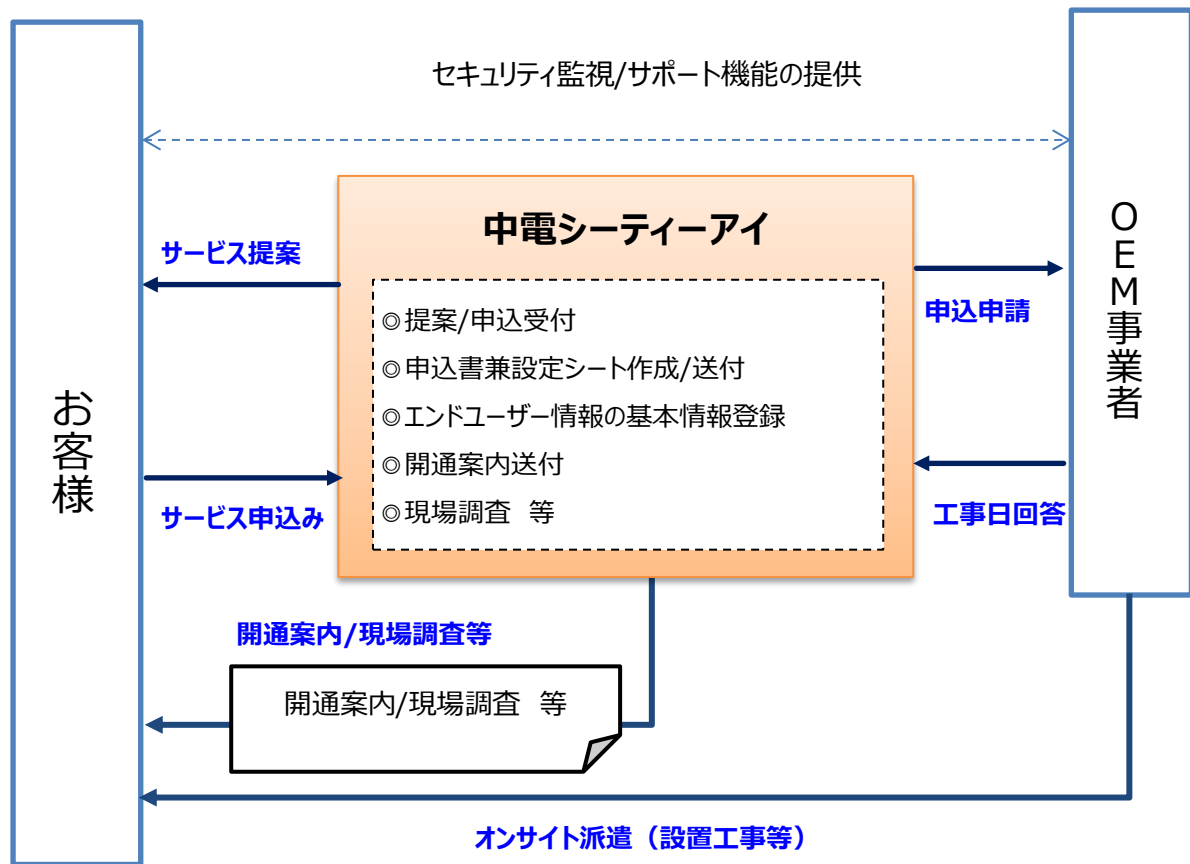
UTM の提供、監視サービス、各種照会が可能なコールセンター、有事の駆けつけをワンストップで提供する。このような支援体制を作ることで、防御・検知だけでなく、初動対応までカバーすることができる。有事の際の報告や被害最小化に活用することができ、発注元や取引先にとっても安心できるサービスとなることを目指した。

本サービス自体は既に市場で提供されているサービスを OEM 提供により、中電シーティーアイが新たなセキュリティサービスとして提供できるかについて実証した。

なお、下図には出てこないが、実際には MS&AD インターリスク総研や中部電力ミライズが本サービスを実証参加企業へ案内し、申込受付や申込必要情報の聴取等の役割を担った。

導入までに時間がかかり、実態の調査としての攻撃件数などの把握には課題が残ったが、サービスとして展開する検討の土台としての情報収集は一定実施できた。

図 20 ワンストップセキュリティサービスの提供フロー



ワンストップセキュリティサービスは本実証事業における大きな目的の一つである「中小企業のネットワーク監視機器」として、本実証事業のメニューの中でも特に中小企業にとってPRしたメニューである。下図は実際に本実証事業の募集時に活用したチラシにおいても、ワンストップセキュリティサービスの概要説明を重点的にPRした。

図 21 実証事業 案内チラシ

中部電力グループ

MS&AD

IPA

MS&ADインシチュアランスグループ

情報処理推進機構

本事業は、経済産業省の補助による独立行政法人情報処理推進機構（IPA）からの請負事業（請負者：MS&ADインターリスク総研）です。

～サイバーセキュリティお助け隊事業のご案内～

サイバー攻撃実態調査等を無償で実施します!!

このようなお客さまにぜひ...

取引先にセキュリティ強化を求められている

どこまで対策されているのか明確でない

何から手を付けていいかわからない

大量の個人情報を扱っている

サイバーセキュリティお助け隊実証事業

MS&ADグループと中部電力グループが連携し、岐阜県を中心とする中部エリア（中部電力営業エリア）において、新たなサイバーセキュリティサービスの試験的な提供を実施します。
 中小企業を対象に、①簡易セキュリティ診断によるセキュリティ対策状況把握、②標的型メール訓練によるセキュリティ意識向上、③ワンストップセキュリティサービス（コールセンター、UTM機器、駆けつけ）による相談受付・初期対応実施、④EDR（エンドポイント監視サービス）配備による攻撃実態把握、およびサイバー保険の検討等を実施します。

▼ ▼ ▼ 実証参加企業には以下のサービスが、実証期間中“無償”で提供されます ▼ ▼ ▼

- #### ① 簡易セキュリティ診断の実施

 - 各設問にご回答いただき、1000点満点でセキュリティ対策状況を判定します。
- #### ② 標的型攻撃メール訓練の実施

 - 標的型攻撃メールを模した「訓練メール」を訓練参加者に送信、対応評価や教育を実施
- #### ③ ワンストップセキュリティサービスによるサイバー攻撃実態の把握

 - 異常通信や振る舞いを検知・駆除
 - 脅威検知内容をレポート化しお客さまへ報告（月1回）

③-1 UTM設置とオフィスサポートセンターによる攻撃の常時監視

 - 不正通信/ウイルス感染の有無をオフィスサポートセンターから常時監視
 - インシデント発生時サポートセンターから能動的にお客様へ連絡
 - 遠隔支援による復旧支援ツール類の提供、回復手順の指示等を実施

UTM機器

③-2 24時間対応のコールセンター利用

 - セキュリティ全般の質問を受け付け

リモート対応

訪問サポート

③-3 訪問サポート

 - 遠隔での復旧が困難な場合に、必要に応じ現地駆けつけで復旧対応（OSリカバリ/機器交換等）
- #### ④ EDR（エンドポイント監視サービス）による監視

 - 次世代エンドポイントセキュリティ「EDR」+運用サービスを提供します。
 - 『振る舞い検知ソフト+アナリストによる監視』で、24時間お客様のパソコンをインシデントから守ります！

対象企業

参加企業数

実証期間

申込方法

： 中部電力エリアに所在する中小企業（中小企業の定義は募集要項・参加規約をご参照ください）

： 約50社

： 2020年9月～2021年1月

： 下記、実証事業専用ページからお申し込みください

<https://info.it-builder.jp/app/otasuke/otasukeannai>

右記QRコードからもアクセスいただけます。

【実証事業専用ページ】

防検サイバー

サイバーセキュリティお助け隊事業 成果報告書-MS&AD インターリスク総研株式会社

32

(2) ワンストップセキュリティサービスの提供

ワンストップセキュリティサービス導入にあたり、導入～運用にあたって提供した機能は主に以下のとおり。①～⑤は OEM 事業者がメイン、⑥～⑨は中電シーティーアイがメインで対応した。

- ① インターネットと企業ネットワーク間への UTM の設置
- ② UTM による不正通信の防護
- ③ UTM の常時監視と、危険度の高い通信を検知した場合の実証参加企業への通報
- ④ コールセンターでの実証参加企業からの問合せ対応
- ⑤ 有事の際の駆けつけサービス
- ⑥ 実証事業参加申込のあった企業に対する UTM 設置のための現地調査
- ⑦ 「ワンストップセキュリティサービス」の申込書作成
- ⑧ 設置工事業者との工事日程調整・調整状況管理
- ⑨ 工事に関する問合せ対応

申込を受け付けたものの、実際に現地調査や設置工事まで行った段階で既に UTM を導入していることが判明する、設置する場所がないことが判明するなどのケースも見られた。

昨年度事業と同様に、過去のシステム担当者が UTM 機器を購入したものの、運用がなされていないという実態があることがわかった。

表 6 ワンストップセキュリティサービス導入状況

分類	件数	特記事項
ワンストップ本申込件数	69 社	
岐阜県	35 社	
愛知県	22 社	
三重県	12 社	
UTM 設置件数	50 件(48 社)	
CloudEdge100	6 件	
CloudEdge50	13 件	
CloudEdge10	31 件	
現地調査等件数	12 件	うち、2 件スイッチングハブを用意
UTM 設置に至らなかった件数	19 社	主な理由 ・UTM を既に導入している ・UTM 設置に関する時間や場所を確保できない ・UTM 設置に関して社内の理解を得られない

本実証事業で導入した企業の従業員規模別割合、業種分類との関係を下図に示すが、実証参加企業の分布とほぼ同じであり、目立った相関関係は見られなかった。

しいて挙げれば従業員 100 名以下の企業が 7 割超であり、比較的小規模の企業で導入が進んだ。業種についても、本実証事業への参加業種として「製造業・建設業・運輸業」が最も多く、目立った相関は見られなかった。

図 22 ワンストップセキュリティサービス導入企業の従業員規模別割合 (N=50)

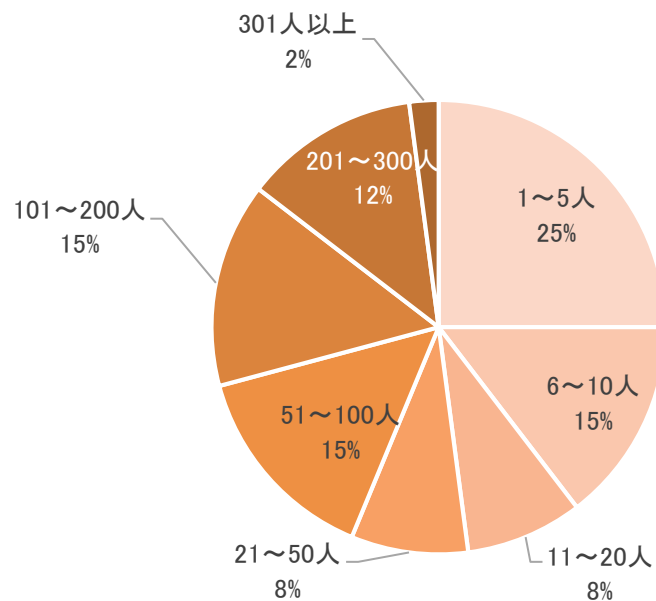
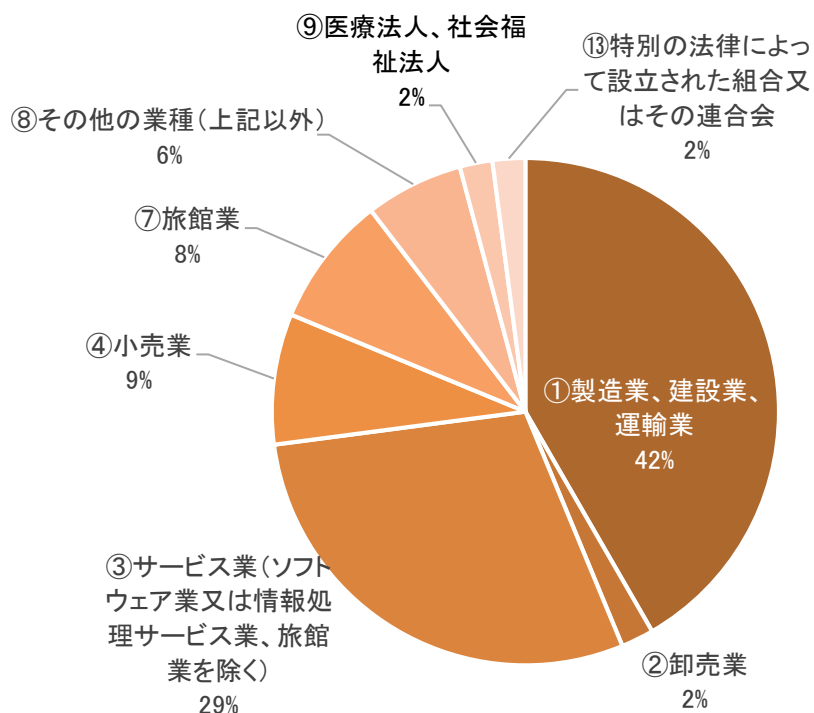


図 23 ワンストップセキュリティサービス導入企業の業種分類 (N=50)



(3) UTM 検知状況とコールセンター等の活用

導入した企業の検知データは下表のとおり。データから読み取れる主なポイントは、

- ・ C&C コールバックを UTM 設置によりブロックした。11 月～12 月の本通信は 1 企業において発生したもので、WindowsXP 端末により発生。当該端末を買い替えたことにより、以後検知せず。1 月は別企業でも発生。
- ・ IPS（侵入防御システム）にて検知、防御が必要な通信を多数検知。中小企業においても、攻撃通信の標的となることが再確認できた。
- ・ スпамメール対策は最も数が多く検知されたもの。無数に飛び交うメールは危険なものが多く、中小企業でもサイバー被害のきっかけとなり得ることを示している。
- ・ ランサムウェアのブロックは 1 企業において発生したものの。UTM によりブロックされており感染被害を防いだ。
- ・ コールセンター対応は、C&C コールバックと UTM 機器の通信障害に関するものが主たる対応となった。
- ・ 現地駆けつけ対応は発生せず。実証期間が短いこともあり、駆けつけが必要なインシデントは発生しなかった。

表 7 UTM 検知状況とコールセンター等の活用状況

分類	件数				特記事項
	10 月	11 月	12 月	1 月	
導入数	11	28	44	50	累計
脅威イベント	243	10,342	135,186	174,356	2021 年 1 月末日時点
C&C コールバック	0	3,500	626	42	
IPS（侵入防御システム）	13	2,594	24,260	51,792	
Web レピュテーション	2	30	149	180	
ウィルス/不正プログラム	2	12	19	30	
スパムメール対策	226	4,172	110,132	122,312	
ボットネット	0	0	0	0	
ランサムウェア	0	34	0	0	
不審オブジェクト	0	0	0	0	
仮想アナライザ	0	0	0	0	
機械学習型検索	0	0	0	0	
お客様通報	3	26	5	7	コールセンター利用は C&C コールバックと CloudEdge 障害に関する能動的な連絡詳細は後述する
現地駆けつけ	0	0	0	0	

(4) 主なコールセンター利用歴

ワンストップセキュリティサービスのコールセンター対応の主なものは下表のとおり。コールセンターに相談したものの、結果として UTM 起因でないケースも見られたが、UTM を設置したことで相談窓口ができたことは中小企業にとっては心強い存在になっていると見受けられる。

表 8 ワンストップセキュリティサービスのコールセンター対応

相談者	相談内容	対応概要
A 社	UTM でブロックされたメールの確認方法を知りたい	メールの確認のための管理コンソール画面を案内。 不正メール(感染メール)は添付ファイルをブロックするが受信はすると案内し対応完了。
B 社	特定 IP の通信をスキャン除外してほしい	業務に必要な、特定 IP をホワイトリストに追加する設定を実施し、対応完了。
C 社	C&C コールバック発生	フルスキャンの提案を実施。 端末の特定完了し、WindowsXP 端末であることが判明。端末入れ替えを検討する。 →後日端末を入れ替えし、対応完了
D 社	UTM 設置後、特定システムの DB にアクセス不可となった	UTM の電源オンオフの切り替えや設定情報の見直しを行い、アクセス可能となり対応完了。
E 社	メールに記載されている URL にアクセスできない	UTM 起因の問題ではなく、URL の記載が間違っていることがわかり、対応完了。

また、ワンストップセキュリティサービス導入までの手続きや機能の確認のため、中電シーティーアイが受け付けた問合せもあり、上記とは別に下記に記載する。

中小企業においては、社内ネットワーク環境がわからないため申込書類の作成を支援してほしい等のフォローが必要なケースがまだまだ多くあることがわかる。

中小企業向けに、「あるべきネットワーク構成」と言えるようなスタンダードなネットワーク構成パターンが定義されていると中小企業にとって目指すべき姿が明確になると考えられる。

【ワンストップセキュリティサービス手続きや機能等の主な照会受付内容】

- ・ 社内のネットワーク環境がわからずフロア図や構成図の作成を支援してほしい
- ・ UTM 設置の工事時間を時間指定したい
- ・ 休日や夜間に UTM 装置の設置工事を行いたい
- ・ 既存環境で利用しているシステムへの影響を確認したい
- ・ スイッチングハブや LAN ケーブルを用意してほしい

(5) 主な検知事例

本実証事業における主な検知事例(インシデント対応事例)として、前述の C&C コールバックの事例を紹介する。

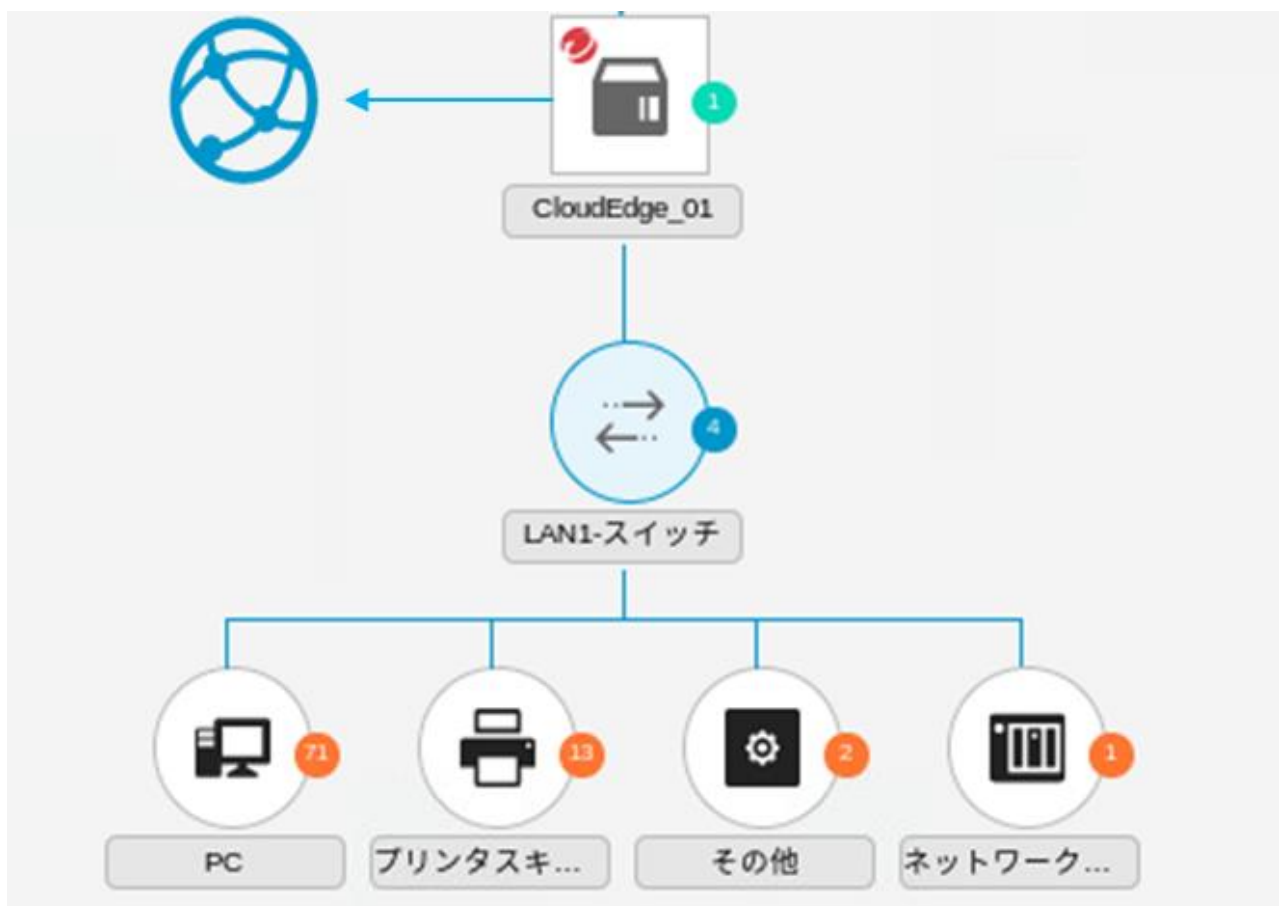
【当該実証参加企業の概要】

- ・ C 社(製造業)
- ・ インターネットに接続している PC 台数は約 100 台
- ・ 本実証事業にて 11 月に UTM を導入
- ・ 当該企業のネットワーク構成イメージは下図のとおり

【インシデント発生の経緯】

- ・ 設置からすぐに UTM が「C&C コールバック」と見られる通信を検知。UTM にてブロック。
- ・ コールセンターより能動的に連絡し、実証参加企業対応開始。
- ・ 実証参加企業の検知端末は特定済み(WindowsXP 端末)
- ・ 当該端末は買い替えにより入れ替える予定のため、検知から C&C コールバックのアラームは出続けていたが、端末特定済みで同一端末のみのアラートであり UTM がブロックしていることから、買い替え様子見とすることとした。
- ・ 後日、当該端末を買い替えし対応完了

図 24 ネットワーク構成イメージ図



(6) 今後の課題と展望

前述のとおり、ワンストップセキュリティサービス自体は既に市場にあるサービスのため、コールセンターやリモート対応、駆けつけ対応などサービス提供のベンダー側としてのインフラは整っているものである。一方で、このサービスを OEM 事業者として中電シーティーアイが運用していく上では、一部サービス内容にカスタマイズ(工事日程調整フロー、申込書のわかりやすさ改善、工事進捗情報共有体制など)が必要と見られる点の実証を通じて見えてきた。

今回の実証事業におけるワンストップセキュリティサービスの検証ポイントは、このサービスを新たに提供する中電シーティーアイがスムーズに提供できるか、今後ビジネスモデルとして活用できるかという点であった。

この点についてはいくつか課題、改善を要す点があることがわかった。

【主な課題と改善点】

- ・ 利用者環境への事前調査について、当初は電話対応のみであることを想定していたが、実際は、ほとんどの実証参加企業について現地調査が必要であり、現在のリソースでは対応が難しい。(特に、遠方地が困難)
- ・ 現地調査や顧客・工事会社との電話での対応など要員がほぼ張り付かないと対応が困難
- ・ 駆けつけサービスの内容が、UTM 故障と被害 PC のクリアインストール(バックアップがある時のみ実施)のみでありセキュリティサービスとして提供するには改善が必要。
- ・ LAN ケーブルやスイッチングハブの手配など、現地の工事担当で臨機応変に対応できない手続きがあった。

これらを踏まえ、今後のビジネスとして進めていくために必要なポイントが 2 点挙げられる。

- ① 中部電力グループ内にて、現地対応可能な導入体制を検討
- ② OEM 提供元へサービスの改善を要求する。

本実証事業を通じて、中部電力グループがサイバーセキュリティサービスを提供したモデルを検証・改善し、今後サービス提供を進めていく準備を調整している。

4.3.5. EDR の提供

(1) エンドポイント監視サービス(EDR)について

ネットワーク一括監視型の UTM だけでなく、端末監視型のエンドポイント監視サービス(EDR)も導入することで多層防御によるセキュリティ強化を実証参加企業に提供した。

本実証事業では MS&AD インターリスク総研が提供する脅威の検知・対応に重点をおいたエンドポイント監視サービス(防検サイバー)を実証事業にて活用した。本サービスの導入に適している企業は、既に UTM など一定のセキュリティを導入している、あるいは本実証で導入するものの、在宅勤務の増加や持ち出しなど境界防御の限界を感じている企業である。

本サービスは、実証事業開始時点ではサービスとして提供していなかったが、エンドポイント監視と初動対応・駆けつけサービスも含むサービスとして整備し、本実証事業を通じてビジネス化を検討してきた。EDR は導入がシンプルで、実施決定企業へのスピーディーな展開が可能であったことから検証にも早期に着手することができ、実証を通じて得られた経験をもとに、2020 年 12 月に本サービスをビジネス化し、一般向けにリリースすることができた。

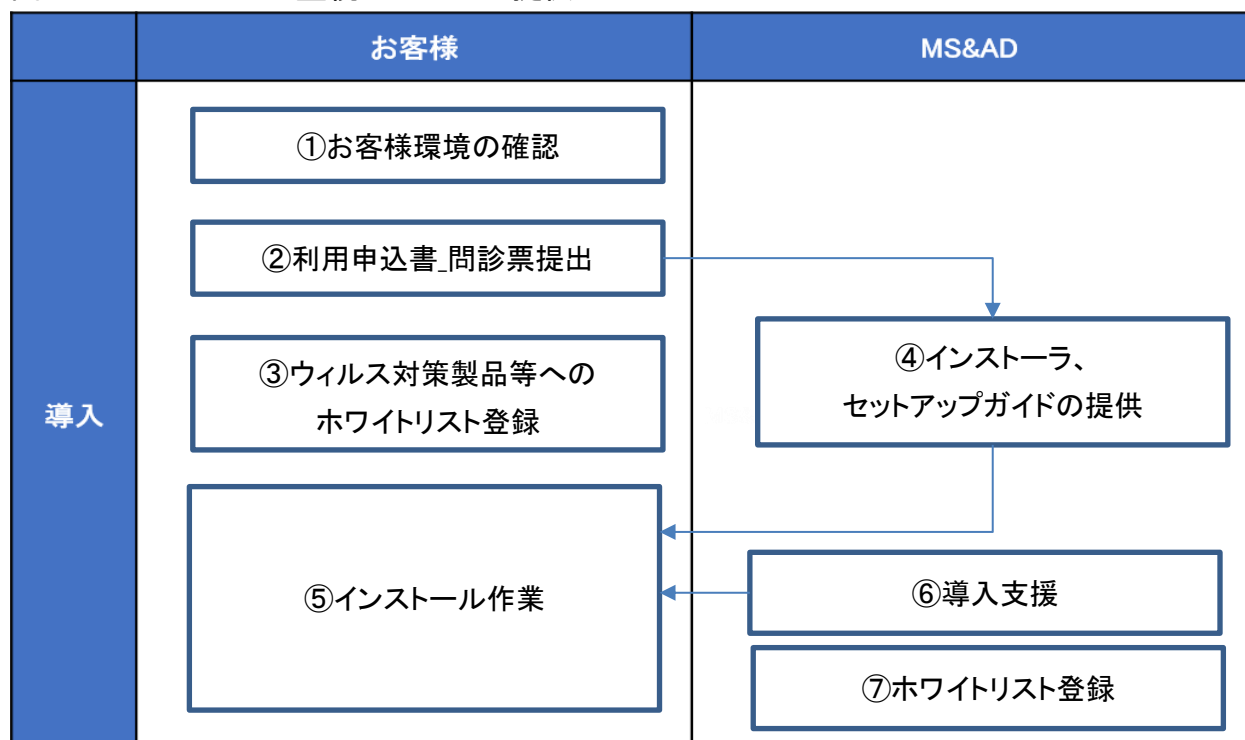
MS&AD インターリスク総研：【次世代エンドポイントセキュリティ(EDR)＋管理セキュリティサービス防検サイバーの提供を開始】<https://www.irric.co.jp/topics/press/2020/1224.php> (2020 年 12 月 24 日)

日本経済新聞：【月 1000 円で「暴露型」ウィルス対策】

<https://www.nikkei.com/article/DGXZQODZ142FW0U0A211C2000000/> (2020 年 12 月 24 日)

なお、下図には出てこないが、中部電力ミライズが本サービスを実証参加企業へ案内し、申込受付や申込必要情報の聴取、インストール支援等の役割を担った。

図 25 エンドポイント監視サービスの提供フロー



(2)エンドポイント監視サービス(EDR)の提供

エンドポイント監視サービス(EDR)導入にあたり、導入～運用にあたって提供した機能は主に以下のとおり。①～④は提供ベンダーがメイン、⑤～⑨は MS&AD インターリスク総研がメインで対応した。

- ① EDR 導入による端末の遠隔監視、ログ保存
- ② AI とアナリストによる防御・検知機能の提供
- ③ 脅威を検知した際の迅速なアラート発出
- ④ 機能や検知データに関する問合せ対応窓口(コールセンター)の設置
- ⑤ インシデント発生時の駆けつけ支援体制
- ⑥ 防検サイバー仕様書と問診票の案内、提出依頼
- ⑦ 防検サイバーインストーラの提供、端末へのインストール支援
- ⑧ 顧客別インストール数の管理
- ⑨ 申込やインストールに関する問合せ対応

防検サイバーの導入手順は簡便であり、インストーラ提供からインストール完了まで早ければ 1 分程度で完了する簡易な方式を採用したため、中小企業独力で対応を見込んでいた。実際に自力で導入完了まで実施できた企業が多数を占めたが、一部、電話や訪問による支援によって導入完了となった企業もあった。

一方で、申込を受け付け、実際にインストーラの提供を行ったものの、端末が EDR サポート対象外であることが判明するケースが見られた。それがインストール支援のための現地訪問支援によって判明するなど、IT リテラシーの低さを示すケースも見られた。

表 9 エンドポイント監視サービス導入状況

分類	件数	特記事項
EDR 本申込件数	60 社	
岐阜県	30 社	
愛知県	25 社	
三重県	4 社	
静岡県	1 社	
EDR 導入件数	50 件	
EDR 設置に至らなかった件数	10 社	主な理由 ・導入予定端末の OS が EDR サポート対象外であった。 ・EDR 導入に関して社内の理解を得られない

本実証事業で導入した企業の従業員規模別割合、業種分類との関係を下図に示す。前述のワンストップセキュリティサービス導入企業の割合に比べ、従業員 51 名以上の比較的大規模な企業での導入が進んだ。ネットワーク全体に関わる UTM 機器よりも端末単位でインストールできるため、比較的大規模な企業においても導入の障壁が低かったと考えられる。

しいて挙げれば従業員 100 名以下の企業が 7 割超であり、比較的小規模の企業で導入が進んだ。業種については、本実証事業への参加業種として「製造業・建設業・運輸業」が最も多く、目立った相関は見られなかった。

図 26 EDR 導入企業の従業員規模別割合 (N=50)

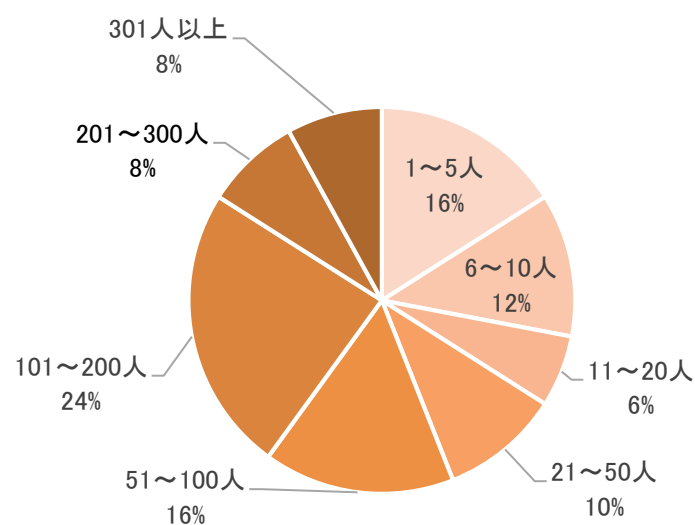
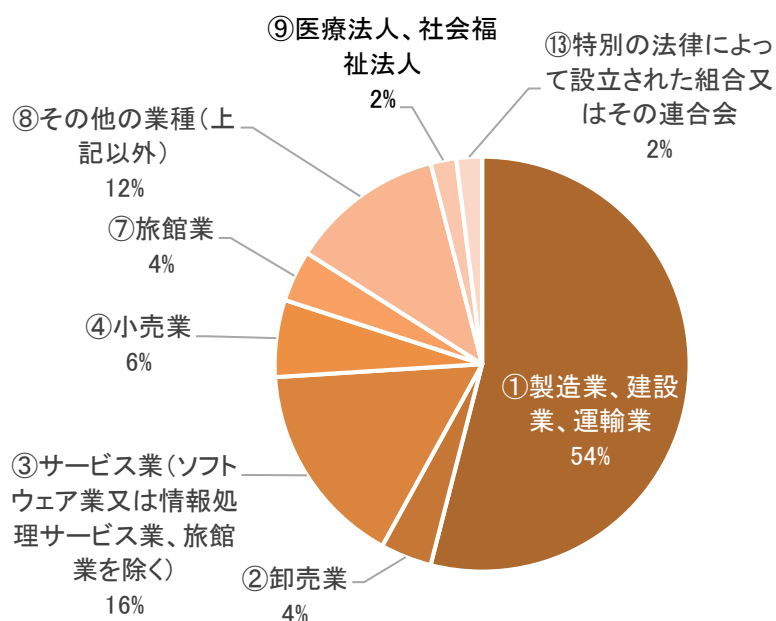


図 27 EDR 導入企業の業種分類 (N=50)



(3) EDR 検知状況とコールセンター等の活用

導入した企業の検知データは下表のとおり。

なお、防検サイバーは導入から1ヵ月間はAIの学習期間として、検知はするものの過検知が多くなる傾向があるため、アラートを送信しない仕様となっている。

データから読み取れる主なポイントは、

- ・ 導入から1ヵ月間に検知した「不審なコマンド実行」や「不審なプロセス起動」は大半が過検知によるもの。そういった中にも、サポートが終了したメンテナンスされないソフトウェア(プラグイン)の振る舞いを検知しているケースもあり、ユーザーに対する注意喚起になった。
- ・ 実証期間が短いこともあり、AI学習期間後の本格稼働データは十分に取得できていない。
- ・ コールセンター利用は個別アラートの内容や脅威レベルに関する問い合わせ。
- ・ 実証期間が短いこともあり、駆けつけが必要なインシデントは発生しなかった。

表 10 EDR 検知状況とコールセンター活用状況

分類	件数				特記事項
	10月	11月	12月	1月	
導入数	8	29	50	50	累計
脅威イベント	235	3,613	4,173	2,702	2021年1月 末日時点
不審なプロセス起動	15	42	40	25	
不審な通信	4	0	36	0	
不審なファイル生成	0	0	4	2	
不審なコマンド実行	201	3,571	3,995	2,640	
不審なAPI実行	15	0	97	34	
不審なツール実行	0	0	0	0	
不審なファイル操作	0	0	0	0	
不審なレジストリ登録	0	0	0	0	
不審なファイル読み込み	0	0	0	0	
不審な常駐プログラム登録	0	0	1	4	
お客様通報	0	0	48	73	コールセンター 利用は運用に 関する問合せと 個別アラートの 問合せ 詳細は後述す る

(4) 主なコールセンター活用歴

エンドポイント監視サービス(EDR)のコールセンター対応の主なものは下表のとおり。

個別アラートの内容や月次報告書の読み方についてなど、運用面の確認が主な内容となった。

表 11 EDR のコールセンター対応状況

相談者	相談内容	対応概要
F 社	EDR 導入台数の報告を受けたが、認識と齟齬がある。	監視状況確認と報告のタイミングの時差により、監視台数が最新状況と異なるケースがある旨を説明。改めて最新状況を確認し、ユーザーの認識と合致したことを確認し対応完了。
G 社	監視状況月次報告書の読み方。	月次報告書にて、該当項目を説明し対応完了。
H 社	個別アラートの解説と対処方法の相談	個別アラートについて、なぜ検知したか、推奨される対応方法を説明し、対応完了。

(5) 今後の課題と展望

導入した企業からもヒアリングやアンケートにおいて、サービスに関する提供物の見にくさ・わかりにくさを指摘する声があり、導入フローやグラフィカルなアラートや報告書の整備など、一部サービス内容にカスタマイズが必要と見られる点は課題として残るが、これらを検証できたことは大きな収穫であった。

前述のとおり、本サービスは、実証事業開始時点ではサービスとして提供していない段階であったが、エンドポイント監視と初動対応・駆けつけサービスも含むサービスとして整備し、本実証事業を通じてビジネス化を検討してきた。EDR は導入がシンプルで、実施決定企業へのスピーディーな展開が可能であったことから検証にも早期に着手することができ、実証を通じて得られた経験をもとに、2020 年 12 月に本サービスをビジネス化し、一般向けに[リリース](#)することができた。

4.3.6. 事後アンケートの実施

実証事業参加企業に対し、実証事業の効果を検証するため、事後アンケートを行った。

実施時期は 12 月 10 日(木)～12 月 22 日(火)にかけ Web 回答方式で実施し、51 社から回答を得た。

回答率が高かった要因は、Web 回答方式でアクセスが簡便であったことに加え、前述のとおり、中部電力ミライズと顔が見えている実証参加企業が多かったため、本実証事業の主旨を理解し、中小企業目線の課題やニーズの回答を得たものである。

アンケートの回答結果について、主なものを記載するが、本実証事業において複数回異なるタイミングでアンケートを取っており、事後アンケートをメインにその他アンケート結果も記載する。

(1) 実証事業参加申込時に確認した意識調査結果

次の 3 つの設問は、実証事業参加申込時に確認した意識調査結果である。サイバーセキュリティ対策を課題と認識している企業が大半であるも、取引先やサプライチェーンから具体的なサイバーセキュリティ対策までは求められていないケースが多い。

図 28 自社のサイバーリスクに対して、どの程度の課題として位置付けていますか。

(N=76)

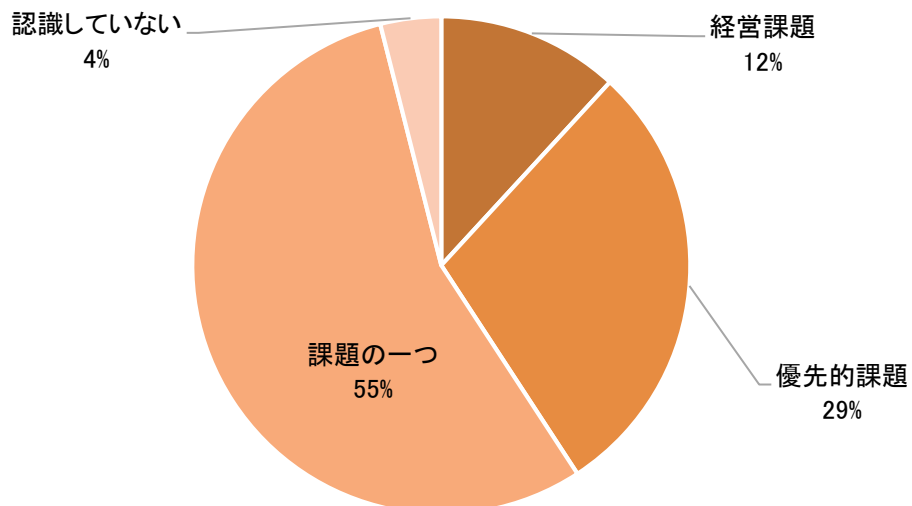


図 29 取引先やサプライチェーンからサイバー対策の実施を要求されていますか。
(N=76)

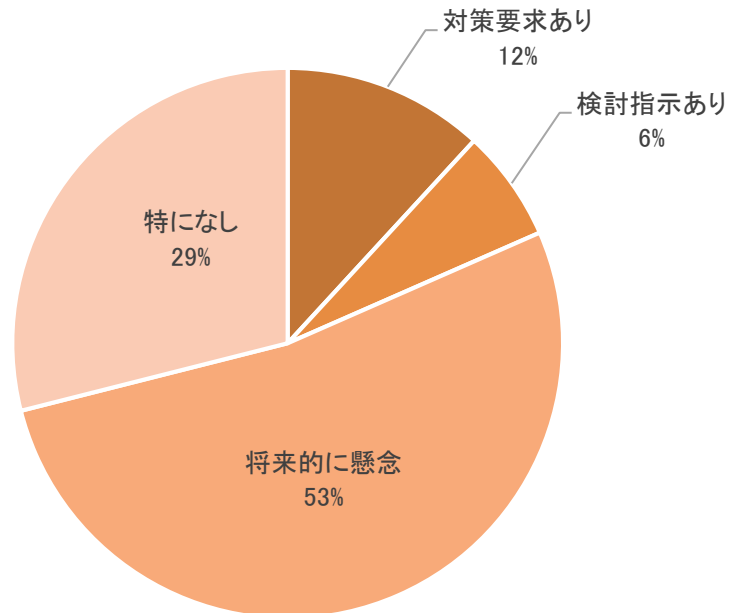
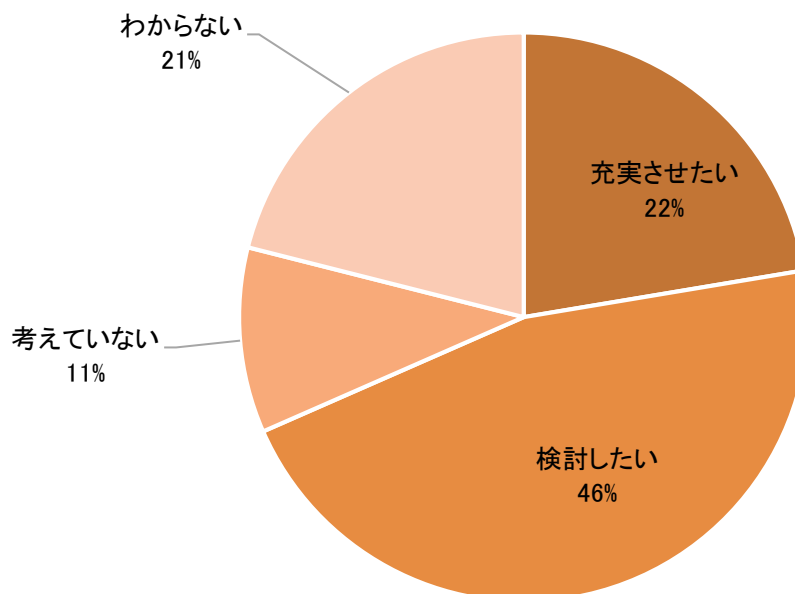


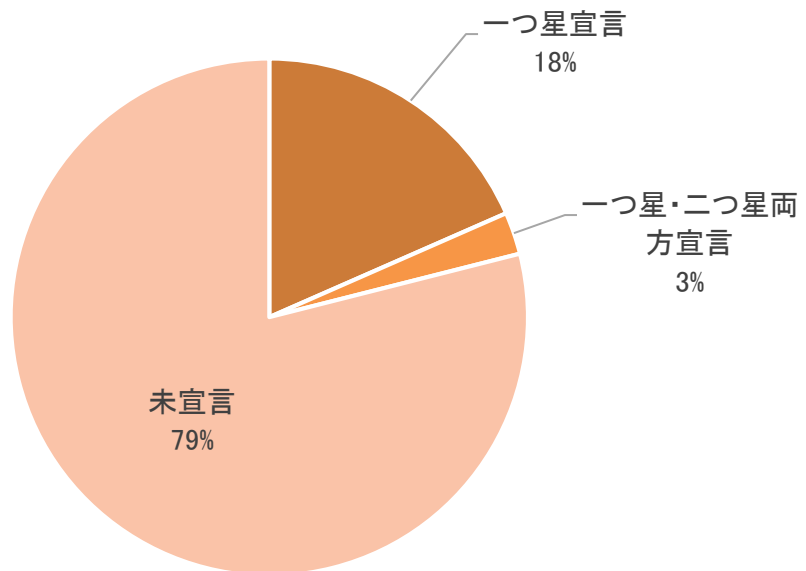
図 30 1年以内にサイバー対策を今より充実させたいと考えていますか。(N=76)



(2) SECURITY ACTION 宣言状況

SECURITY ACTION は大半の企業が未宣言である実態がわかった。事業説明会や成果報告会、実証事業を通じて SECURITY ACTION 宣言を呼びかけてきたが、引き続き各企業へ宣言を依頼・支援していきたい。

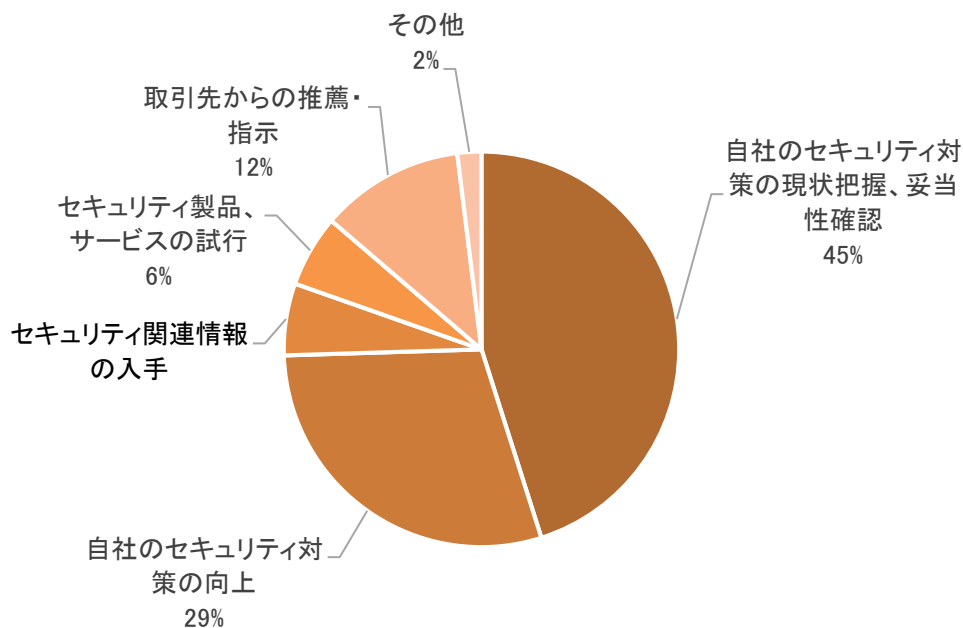
図 31 SECURITY ACTION 宣言状況 (N=76)



(3) お助け隊事業への参加目的、国に望む政策

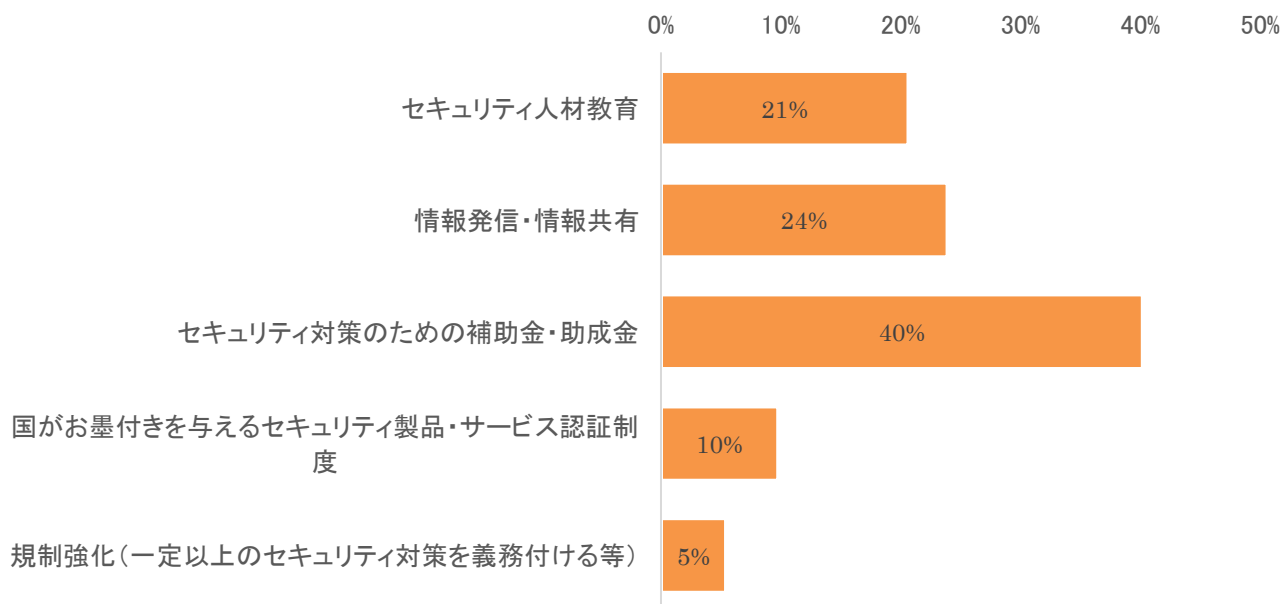
自社のセキュリティ対策の現状把握、妥当性確認、向上が7割超を占めた。今回実施した簡易セキュリティ診断による現状の可視化がニーズにもマッチしており、その機能を更に強化し、セキュリティ対策の向上を寄与していきたい。

図 32 お助け隊事業に参加した主な目的、期待についてご回答ください (N=51)



国に望む政策としては補助金・助成金が最も多く、次いで情報発信や人材教育を望む声が多い。

図 33 今後のサイバーセキュリティ対策を進めるために国に望む政策 (N=92、複数選択)



(4) サプライチェーンにおける要求レベル

昨年度実証のヒアリングではほぼ要求はなかったものの、1年間で40%強の企業が取引要件～実態調査レベルの要求があり、全体として前進していることが見受けられる。

図 34 「取引先(発注元)→貴社」に対してどの程度の要求を求められていますか。
(N=51)

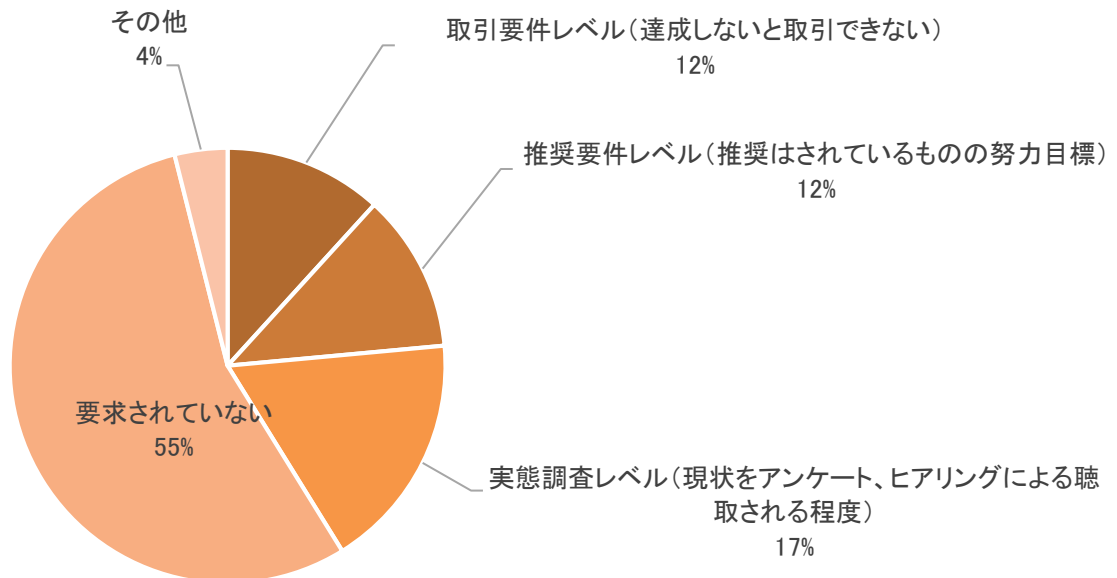


図 35 取引先(発注元)から要求されているセキュリティ対策を全てご回答ください。(N=66、複数選択)

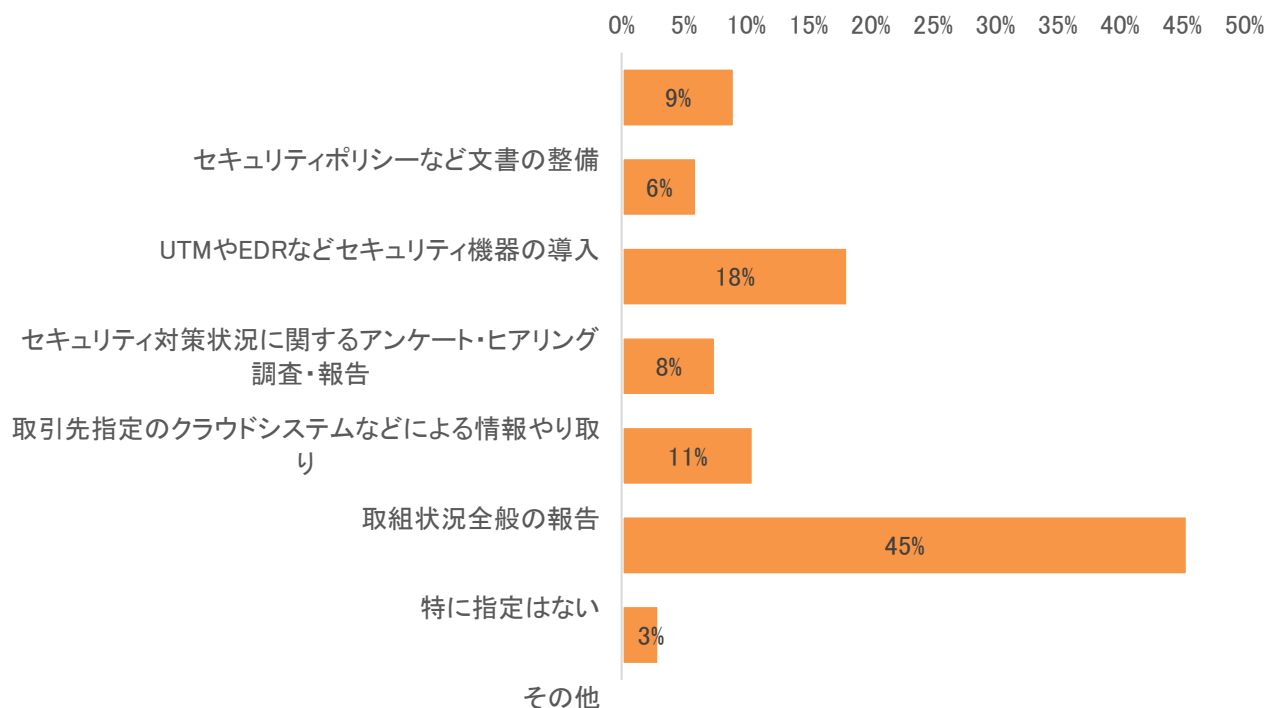


図 36 「貴社→取引先(発注先)」に対してどの程度の要求を求めていますか。 (N=51)

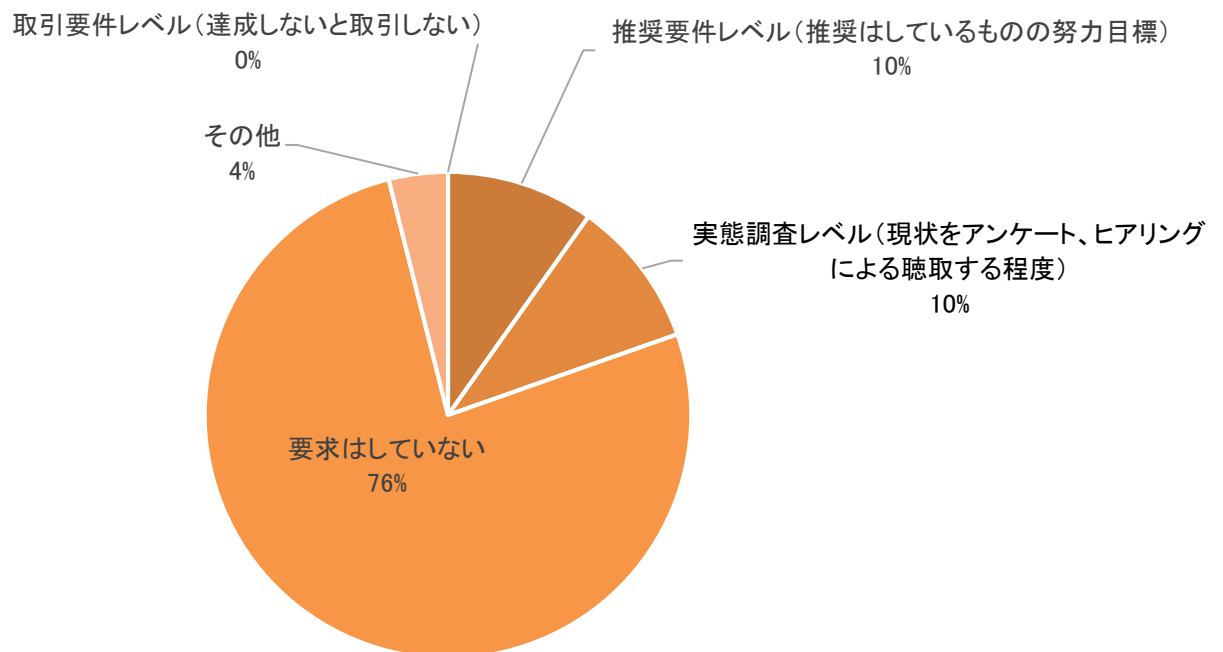
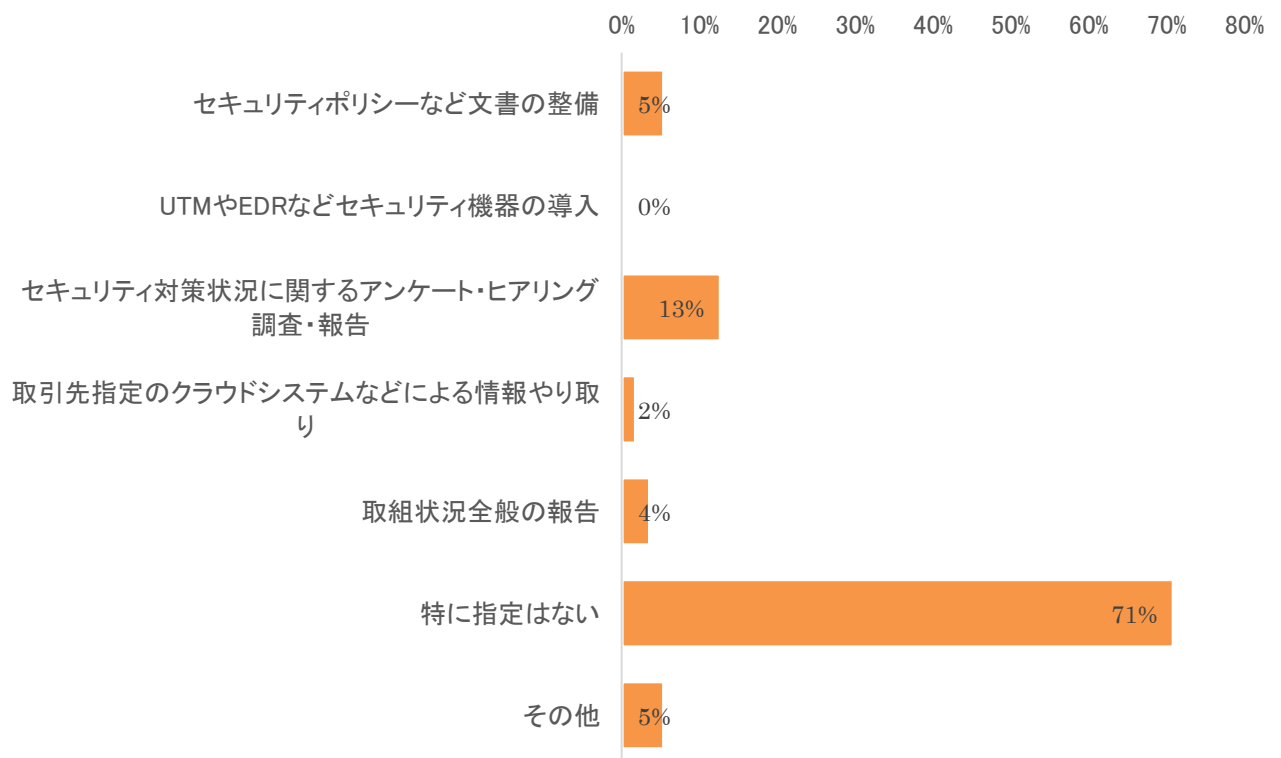


図 37 取引先(発注先)に対して求めているセキュリティ対策についてご回答ください。
(N=55、複数選択)



(5) お助け隊メニューについて

図 38 「ワンストップセキュリティサービス」で特に活用できたものについて教えてください
(N=51)

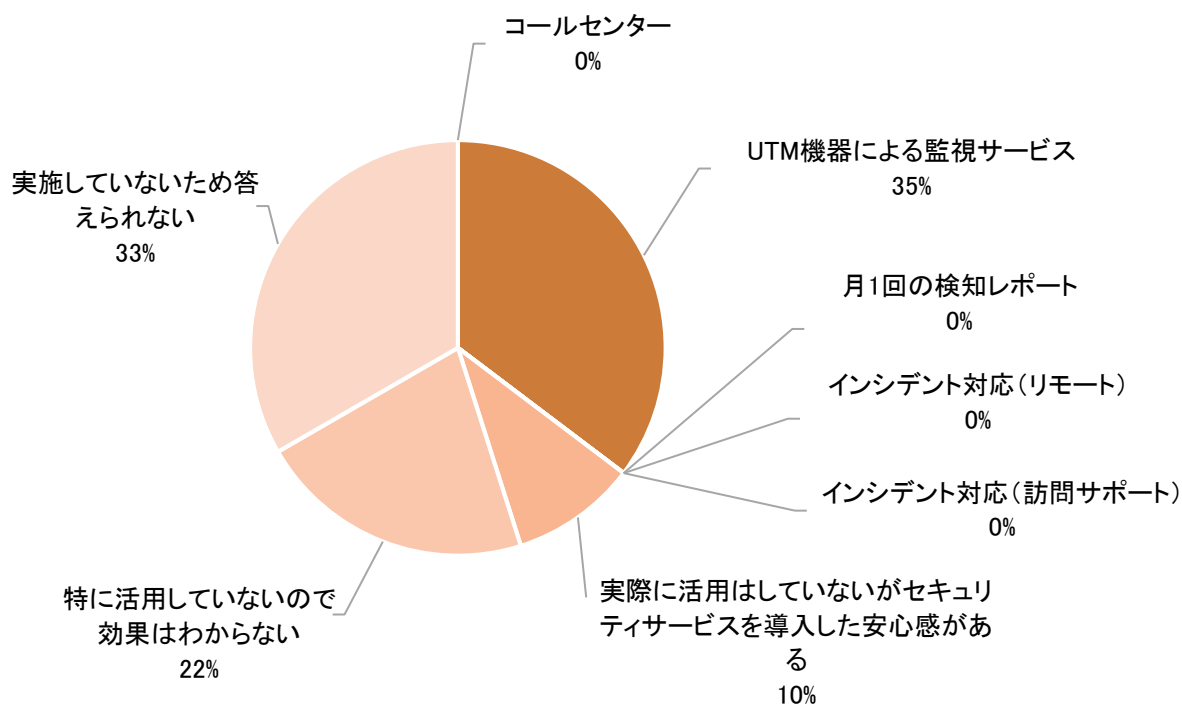


図 39 今後も継続して(あるいは新規で)「ワンストップセキュリティサービス」の導入をしたい
と思いますか。(N=51)

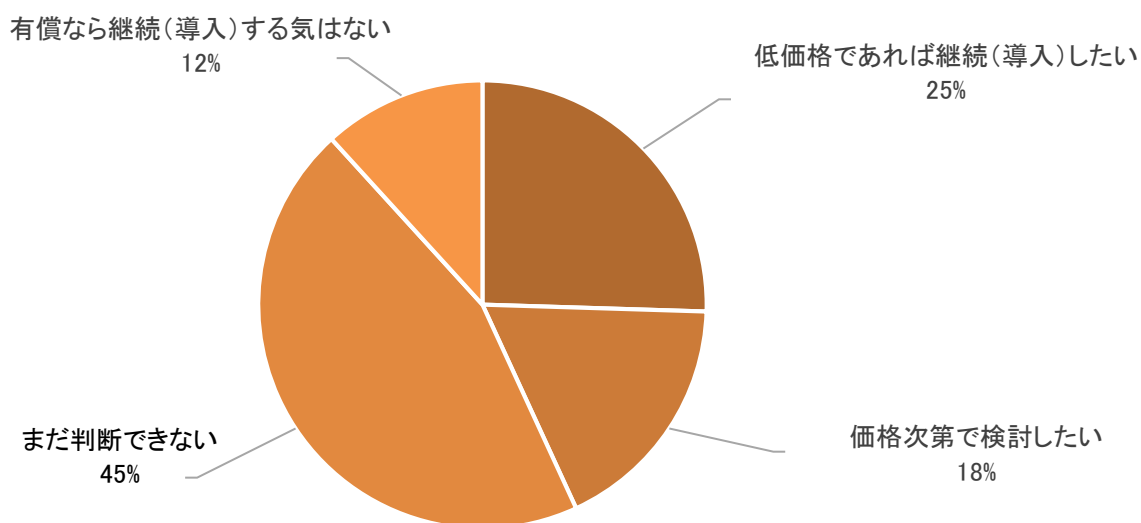


図 40 UTM の設置、コールセンターの利用、駆けつけ対応を含む今回のワンストップセキュリティサービスにかけられる費用についてご回答ください。 (N=51)

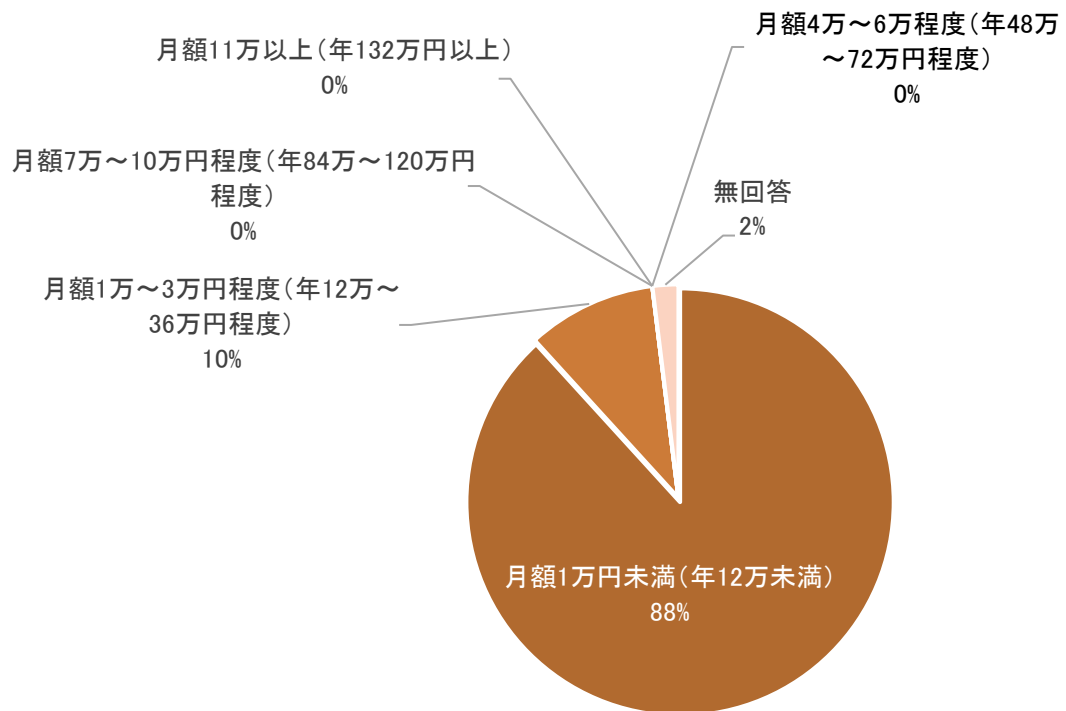


図 41 「EDR(エンドポイント監視サービス)」で特に活用できたものについて教えてください。
(N=51)

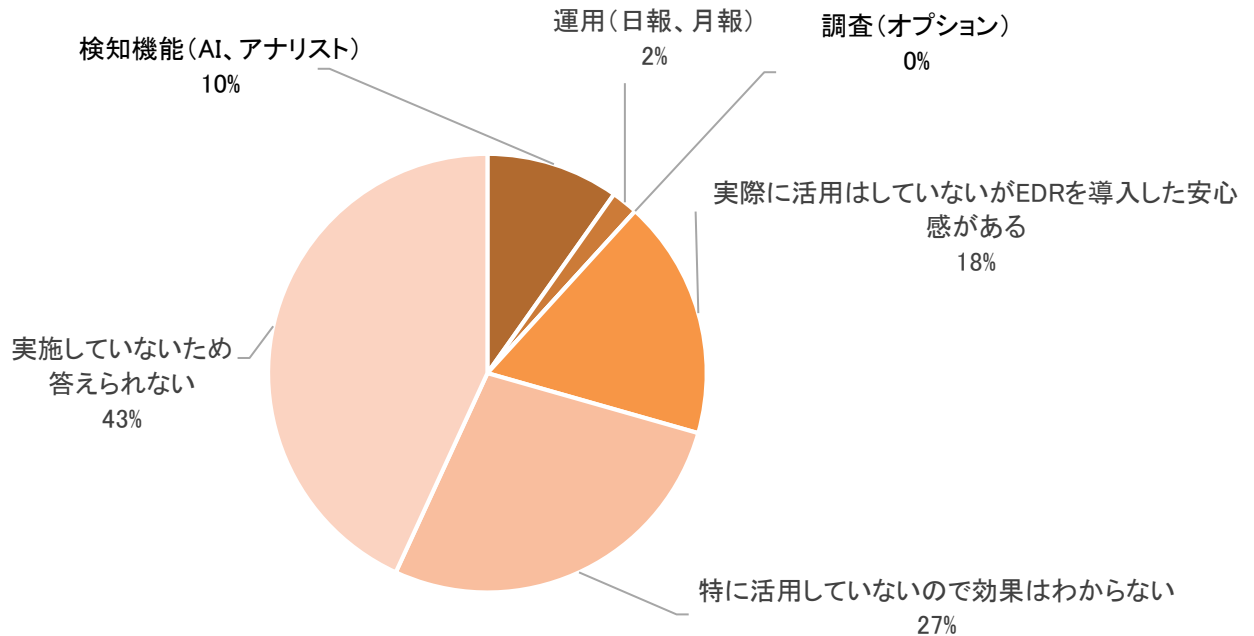


図 42 今後も継続して(あるいは新規で)「EDR(エンドポイント監視サービス)」の導入をしたいと思いますか。(N=51)

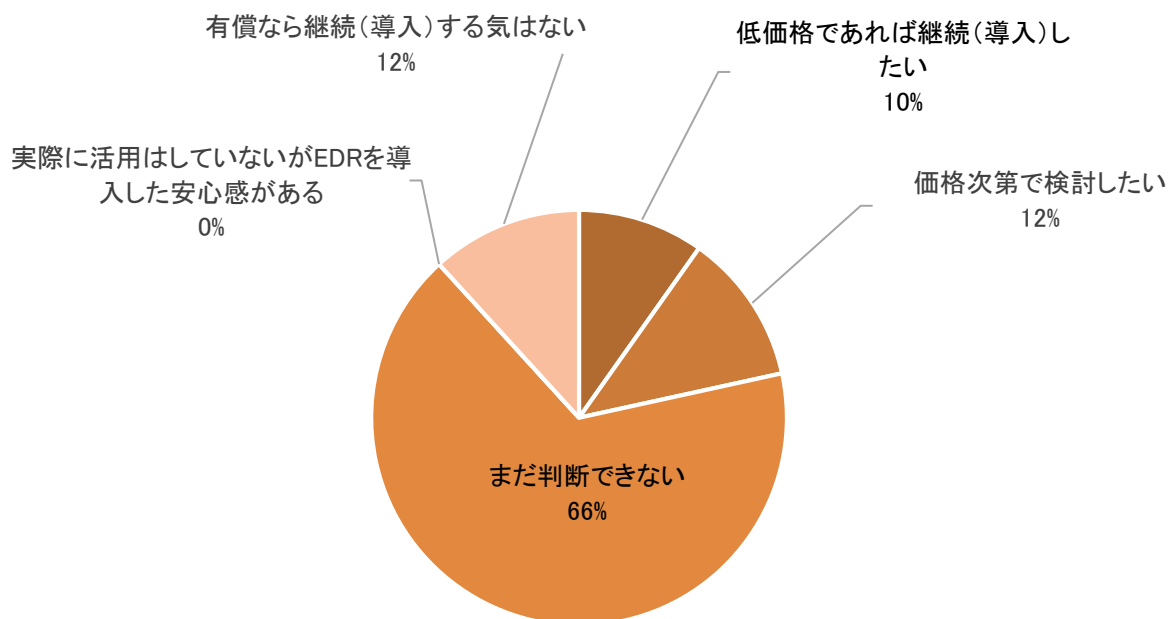
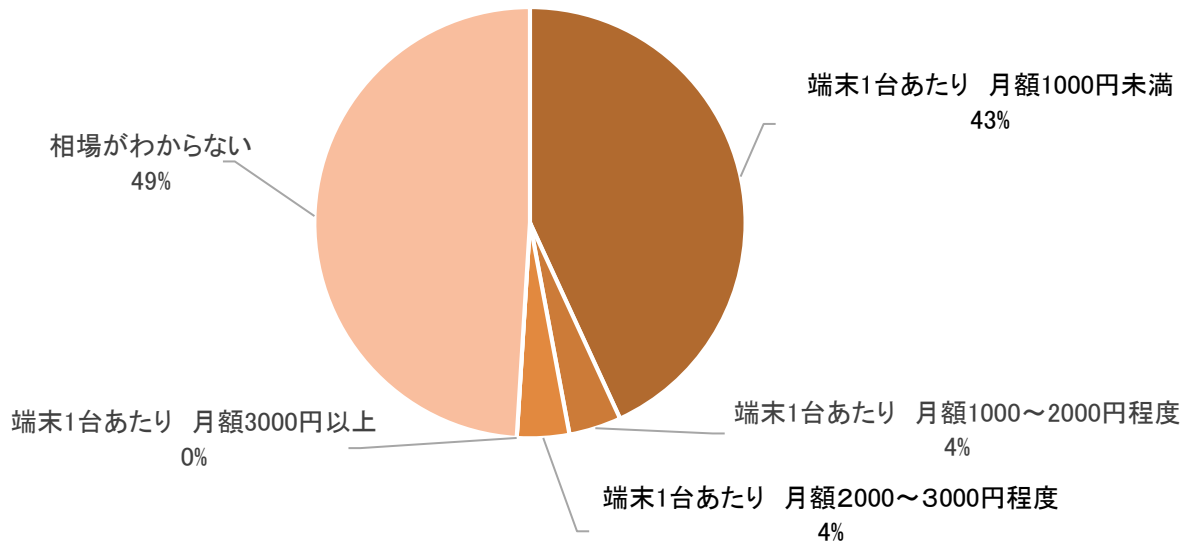
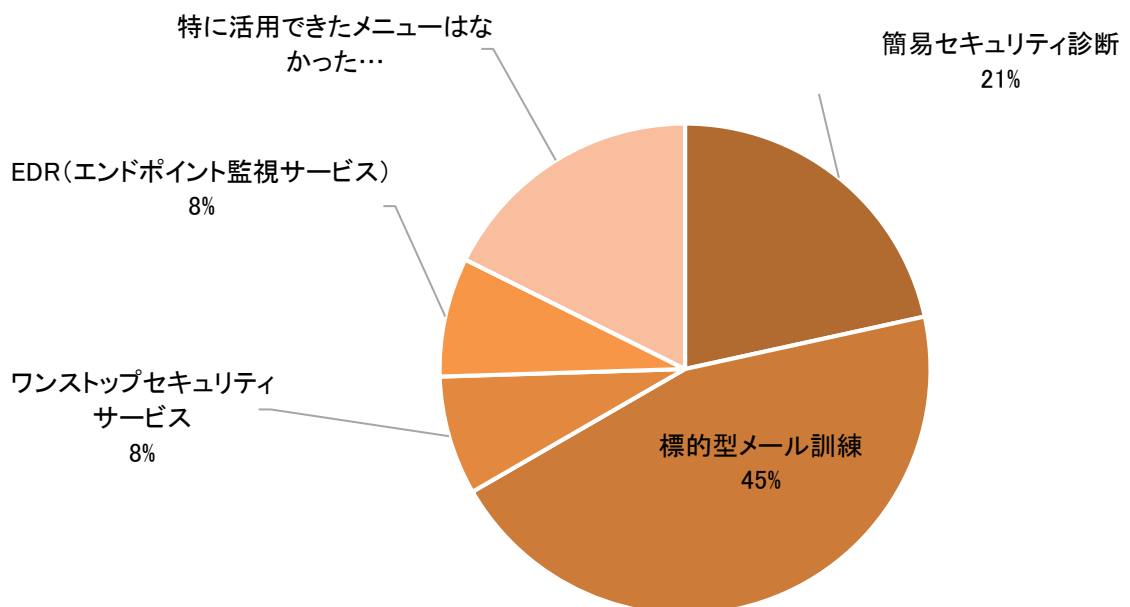


図 43 EDR(エンドポイント監視サービス)にかけられる費用についてご回答ください。
(N=51)



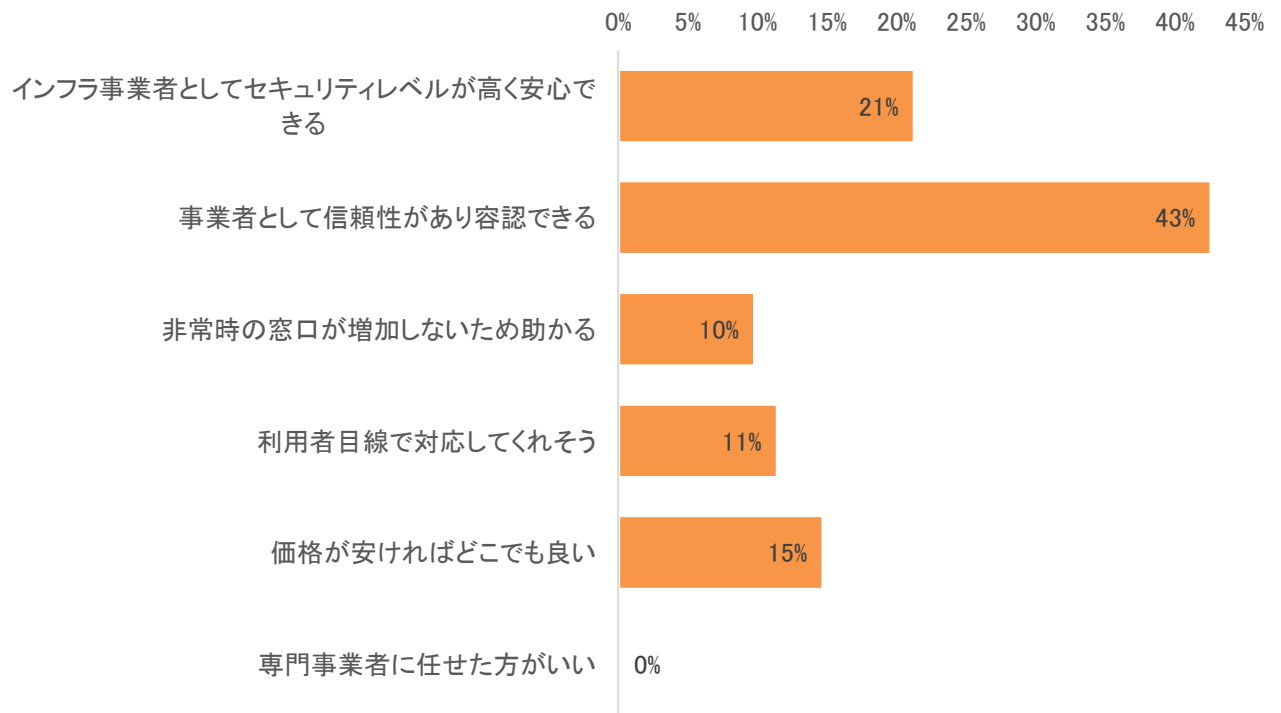
標的型メール訓練の評価が高く、メール攻撃への危機意識や対策の必要性については一定理解されていることがわかる。一方、検知や初動対応に関する認識はまだ低い。

図 44 お助け隊メニューの中で特に活用できたメニューについてご回答ください。 (N=51)



(6) 電力会社グループがサイバーセキュリティサービスを提供することについて

図 45 電力会社がこれらのサービスを提供するとしたら、どのように感じますか。(N=61、複数選択)



(7)サイバー保険について

既契約者の割合は他調査と大差なし。一方、検討に向けては7割近い参加者が検討しており、サイバー保険へのニーズの高まりを感じる。

図 46 既にサイバー保険(情報漏えい保険を含む)に加入していますか。 (N=51)

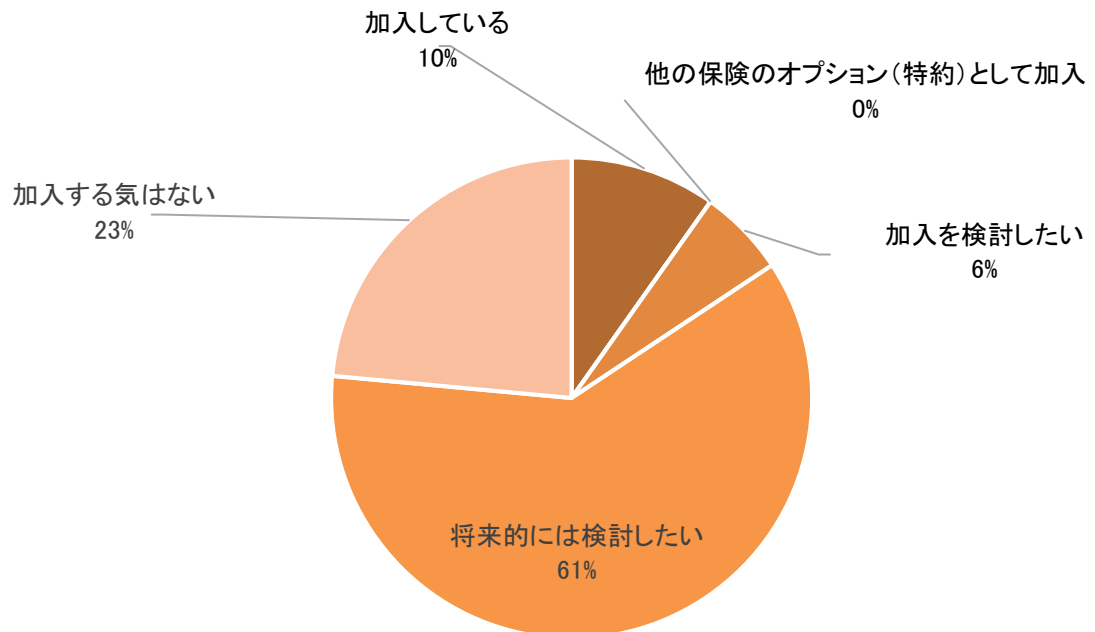


図 47 サイバー保険の補償範囲について、最も期待する補償範囲を教えてください。(N=51)

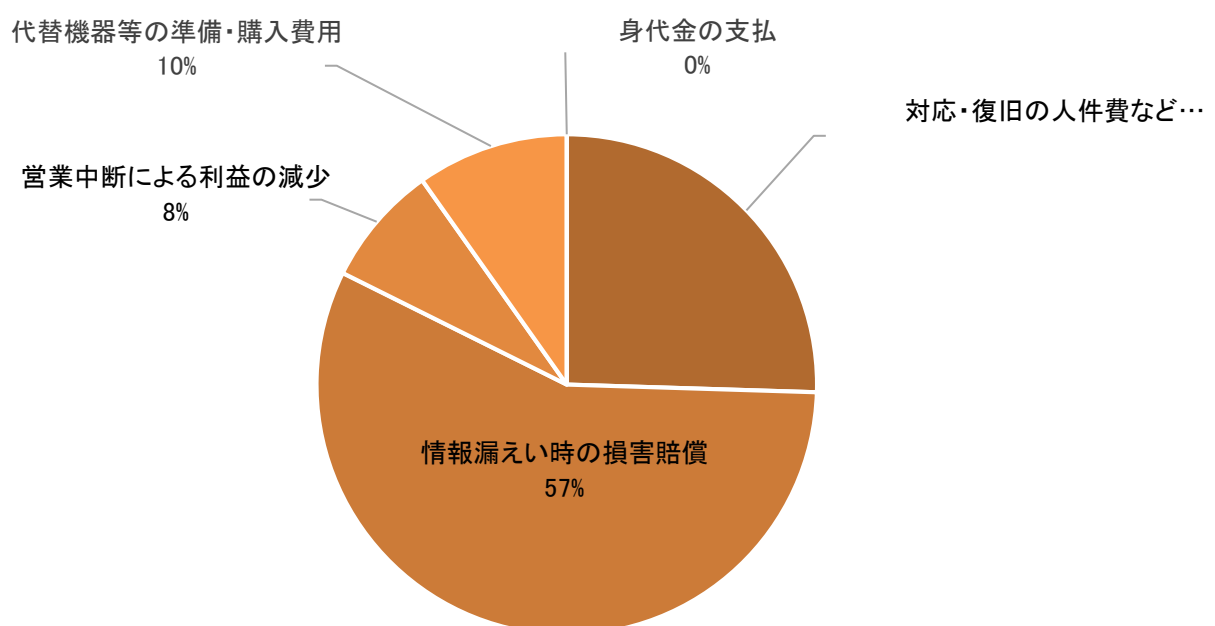
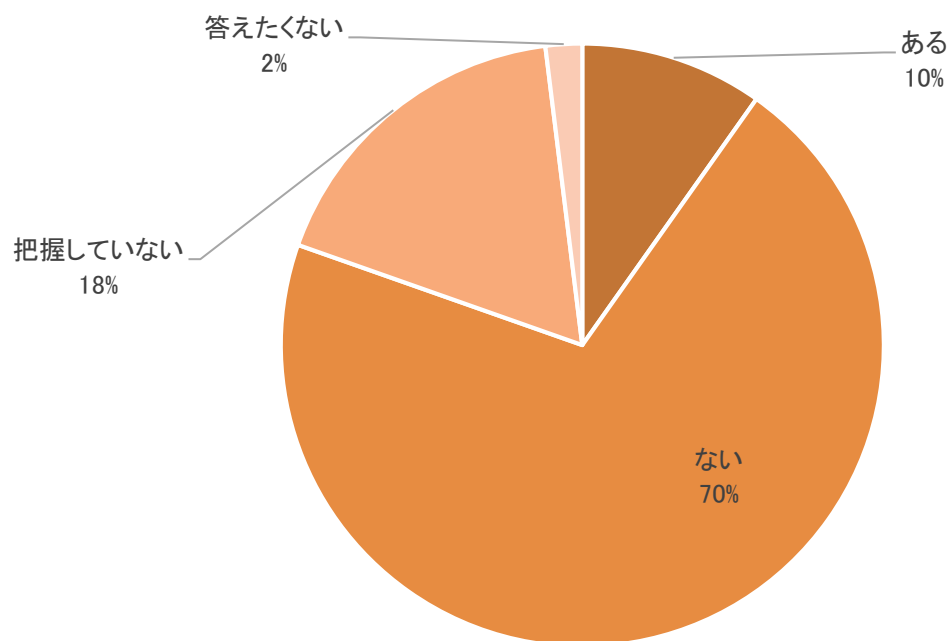


図 48 サイバーセキュリティに関する事故(会社、顧客への何らかの被害)が発生したことはありますか。 (N=21)



4.3.7. 事後ヒアリングの実施

本実証事業に参加した企業のうち 5 社に対してヒアリングを実施した。

新型コロナウイルスの状況も踏まえて、全て Web もしくは電話によるリモートでヒアリングを行った。
ヒアリング対象企業は、実証メニューを積極的に利用した企業を中心に選定した。

(1) A社のヒアリング結果

表 12 A社のヒアリング結果

企業属性			
属性		内容	
1	業種	⑦旅館業	
2	従業員数	約 80 名	
3	参加事業所の所在地	岐阜県	
4	PC 台数	9	
5	ヒアリング担当者	社長	
ヒアリング内容			
ヒアリング項目		回答内容	
1.お助け隊実証事業の参加動機、期待するものについて			
	1	お助け隊実証事業の参加動機、期待するものの	顧客管理、従業員の情報管理が足りていないと自覚していた。実証事業を通して勉強しようとしていた。総務部や予約センターが IT を担当しているが、まずは自分で体験したかった。
2.自社のサイバーセキュリティに関する課題、実態、対策状況について			
	1	現在の社内セキュリティ状況	社内では詳しいものがおらず、委託で業者に頼んでいる。過去に外部委託先の IT ベンダーより、シマンテックのセキュリティソフトを入れてもらったことはある。
	2	宿泊施設だが、お客様の個人情報管理は誰が管理しているか。	外部システムで顧客情報や予約情報を管理している。当社では社内のネット担当者が宿泊プランを考案している。しかし、インターネット回線の敷設などは業者に委託している。業者からアンチウィルスソフトの提案はあったが、 <u>通信回線のセキュリティの提案はない</u> 。
	3	サイバーセキュリティ上の懸念	<u>メールが一番心配</u> している。標的型メールなど。実証メニューの標的型メール訓練はためになった。今後も活用してみたい。
	4	サプライチェーンからの要求事項	取引先から指示はない。
3.実証事業の各メニューについてご意見・ご感想・ご要望等			

1	簡易セキュリティ診断	インターネットの技術の進化を感じた。読んでいてわからない単語が多くあった。 <u>診断票の使い勝手は悪くないが、レポートだけでなく、わからないこと、できていないことにアフターフォローがあると嬉しい。弱点を補う具体的な話をいただけると対応しやすい。</u>
2	標的型メール訓練	日頃、メール攻撃に関する教育は実施していたが、今回の訓練で1名開いてしまったことで、全社員に情報共有を実施した。
3	ワンストップセキュリティサービス	ポップアップが出てくるのはわかりやすかった。安心感はあるが、 <u>二方で利用している実感はない。</u> 現実としてセキュリティ事故もなく、どのくらいが妥当か判断が難しいが、サービス内容から UTM の費用は妥当だと思う。
4	EDR	<u>インストールは簡単だったが、どのような対策になっているのかわからなかった。</u> 市販で販売しているウィルス対策ソフトは導入済みである。導入を主要なパソコンに絞るのであれば、費用は妥当だと思う。
5	お助け隊事業全般について	今回 <u>サイバーセキュリティについて自身が何も把握できていないこと</u> を感じた。一つ一つのメニューを勉強していきたい。 <u>中部電力ミライズから何度が訪問支援いただき、助かっている。</u> 自社のセキュリティがどういう状況であるか、把握できるとより良い。
4.電力会社グループと保険会社グループが協業した今回の事業の運営体制について		
1	電力会社と保険会社グループによるサイバーセキュリティサービスの提供について	おまかせすることができた。宿泊に関することなど、 <u>多方面で中電にお世話になっており、中電グループがサイバーセキュリティサービスを行うことについて違和感なかった。</u>
5.中小企業が利用しやすい・選択しやすいサイバーセキュリティサービスについて		
1	中小企業が利用しやすいサイバーセキュリティサービスについて	インターネットと聞くだけで拒否反応が出るため、機能としてわかりやすく、状況を報告いただけるものが良い。
6.「サイバー保険」に対する率直なイメージ		
1	サイバー保険に対する理解度、イメージについて	<u>サイバー保険があることすら知らなかった。</u> 情報漏えいの賠償や調査費用を補償するものとは知らなかった。 <u>セキュリティ機器にサイバー保険が付帯されていることは安心感があり、ありがたい。</u>

7.今後の取り組みについて		
1	実証事業に参加して気付いたこと、今後の取り組みについて教えてください。	個人情報の漏えいが怖い。 従業員の雇用契約は紙ベースであり、データで管理できていない。 宿泊されるお客様のデータはシステム会社のサーバーで管理している。 営業社員には在宅勤務時にパソコンを持ち帰らせていない。 <u>紙で資料を持ち帰らせて仕事をさせている。</u> 今回実証に参加して、いかに自身がサイバーセキュリティに関して無知であるかわかった。今後一つ一つ勉強していきたい。

(2) B社のヒアリング結果

表 13 B社のヒアリング結果

企業属性		
属性		内容
1	業種	①製造業、建設業、運輸業
2	従業員数	約 30 名
3	参加事業所の所在地	岐阜県
4	PC 台数	15
5	ヒアリング担当者	社長
ヒアリング内容		
ヒアリング項目		回答内容
1.お助け隊実証事業の参加動機、期待するものについて		
1	お助け隊実証事業の参加動機、期待するもの	自社のセキュリティ対策の現状把握、妥当性確認のため。中部電力ミライズから紹介があり、チラシによる簡単な説明を受け、<u>無料であれば試してみよう</u>と考え、参加した。
2.自社のサイバーセキュリティに関する課題、実態、対策状況について		
1	現在の社内セキュリティ状況	スタンドアロン端末、セキュリティソフト、<u>1～2 年前に UTM を導入</u>した。 これまでサイバー事故がなかったため、この対策を継続してきた。 <u>全て社長本人がセキュリティを進めている。</u>昔からこの分野が好きで対応している。
2	機密情報のやりとりはあるか	当社は機密情報を手渡しでやりとりしており、社内では厳重に管理している。
3	サイバーセキュリティ上の懸念	自社の規模からどこまでが必要なセキュリティ対策かわからない。 <u>社長以外にセキュリティに対応できる人がいない</u>ことも課題。

	4	サプライチェーンからの要求事項	取引先の大企業から求められているのは、維持管理、災害対策はあったが、セキュリティは触れられる程度。
3.実証事業の各メニューについてご意見・ご感想・ご要望等			
	1	簡易セキュリティ診断	この粒度で確認が必要と実感したが、我々の業界ではここまでの対策は不要だと思った。ただし、情報流失はリスクと感じており、ルールの簡単な文書化が必要と感じた。 <u>既存ではルールやポリシーはない。</u>
	2	標的型メール訓練	社員がどういったメールに反応してしまうか、興味があった。明らかに怪しいメールはクリックしないが、代表名で送ってみた。普段朝礼でコミュニケーションしている。滅多にないことで、逆に怪しまれたかもしれない。 開いてしまった2名へ簡単な個別の指導をした。普段、重要情報をメールで送ることはないが、今後は注意するよう伝えた。
	3	ワンストップセキュリティサービス	これまでソニックスウォールを入れており、ここの一年は更新していなかった。機器とソフトのバージョンアップだけで、コールセンターは付いていない。新しいものを確認したく、導入してみた。 <u>ソニックスウォールと対比して、端末を特定でき、細かく分析することができるようになった。使いやすい印象である。</u> 価値はこれから検討になると思う。月額数万円という感覚。 <u>無料の機器を渡り歩いても良い</u> と思っている。
	4	EDR	インストールは簡単に完了した。 まだ活用はできてないので、評価はできない。 <u>アラートが1件あり、Criticalとあったが、良くわからなかった。</u> 月額については、台数が増えると価格が増えるので、UTMも込みで考える必要がある。 <u>現在大半がWindows10でWindows Defenderを使っているが、それで他に入れる必要がないという結論に至った。</u>
	5	お助け隊事業全般について	<u>同時多発的にメールがきて混乱した。</u> その後、メニューの流れのまとめがきて、理解できた。 最初の入り口の時点で、説明をもっと明確に、シンプルにさせていただくとわかりやすい。文字数が多いとわかりづらい。
4.電力会社グループと保険会社グループが協業した今回の事業の運営体制について			
	1	電力会社と保険会社グループによるサイバーセキュリティサービスの提供について	<u>地元の信頼のおける会社だったので、信頼感があった。一つの窓口で全てが完結するとありがたい。</u> 提携している保守ベンダーは特におらず、セキュリティ商材の案内もない。

5.中小企業が利用しやすい・選択しやすいサイバーセキュリティサービスについて			
	1	中小企業が利用しやすいサイバーセキュリティサービスについて	セキュリティは無料のものを選ぶようなレベルである。 とりあえず入れてみる、という感覚である。 一度、業務フローをヒアリングしてもらい、強み、弱みを分析、適切なサービスを提案していただく。
6.「サイバー保険」に対する率直なイメージ			
	1	サイバー保険に対する理解度、イメージについて	とある取引先 2 社より、サイバー攻撃を受けて情報漏えいした場合、サイバー保険で対応する、という説明が来た。そこでサイバー保険を認知した。業務フローをコンサルいただく中で保険についても提案いただけると、加入したくなる。
7.今後の取り組みについて			
	1	実証事業に参加して気付いたこと、今後の取り組みについて教えてください。	サイバー対策は PR 材料にもなると考えている。 いいきっかけをいただき、大変感謝している。

(3) C 社のヒアリング結果

表 14 C 社のヒアリング結果

企業属性		
属性		内容
1	業種	①製造業、建設業、運輸業
2	従業員数	約 300 名
3	参加事業所の所在地	愛知県
4	PC 台数	100
5	ヒアリング担当者	システム担当者(総務部門)
ヒアリング内容		
ヒアリング項目		回答内容
1.お助け隊実証事業の参加動機、期待するものについて		
	1	お助け隊実証事業の参加動機、期待するもの 中部電力ミライズから話があり、自社のセキュリティ対策の向上と、UTM の試用のために参加した。社員が関係ないサイトを閲覧することや、どのようなサイバー攻撃が来ているのか知りたかった。
2.自社のサイバーセキュリティに関する課題、実態、対策状況について		
	1	現在の社内セキュリティ状況 総務部で、人事、安全、労務、IT 等の業務を行っており、 <u>セキュリティ業務は人手不足。費用面・経営層の理解の面でも課題がある。</u>
	2	機密情報のやりとりはあるか 専用のパソコン、専用のシステムで限られた社員しか触れないように、各部門でパスワード管理がなされているはずである。

3	サイバーセキュリティ上の懸念	対策費用の捻出。メイン事業である製造にかかる予算と比べて、サイバーセキュリティに費用をまわせない。費用が足りない、というよりは、必要性やどの程度の費用をかければ良いか、理解されていない。
4	サプライチェーンからの要求事項	<u>大きな取引を行う得意先から、サイバーセキュリティのポリシー、組織体制(サイバーセキュリティ担当者)、今回の簡易セキュリティ診断のような確認はあるが、監査はない。</u> それ以外に製造の安全面などで確認がある。「できなければ取引停止」のような要求があれば即対応となると思う。当社から、委託先へは要求したことがない。
3.実証事業の各メニューについてご意見・ご感想・ご要望等		
1	簡易セキュリティ診断	<u>実施できている/できていない分野が明確になり、その点で役に立った。</u> 端末の管理はできているが、その他はできていないことも多かった。社内ではセキュリティポリシーの整備をしようとしていたが、業務多忙で手が付けられなかった。 <u>IPA のホームページでひな形を見してみる。</u>
2	標的型メール訓練	全社員同じ時間に訓練をしたので、従業員も怪しんでクリックを回避したかと思う。ばらばらの時間帯に送っても良かった。 社員の中では、 <u>着信を総務部に知らせてきて、確認をしていた動きは良かった。</u> 社内ではメールは TEXT 形式に設定を統一し、標的型攻撃メールのリスクを減らしていたが、URL アクセスした 3 人について、HTML 形式で設定されていた。そこは直した。
3	ワンストップセキュリティサービス	C&C コールバックを検知したあと、無料に対応するようと言う指示が通達され、端末を特定し、無料のウィルス対策ソフトでスキャンした。その後パソコンの入れ替えを行い、以後検知していない。 <u>UTM 導入してシステム停止などを懸念したが、当社の業務には影響がなく、その点は良かった。</u>
4	EDR	<u>導入は簡単だった。</u> 他の社員も作業したが問題なかった。 まだアラートが来ていないので、評価自体はできていない。
5	お助け隊事業全般について	UTM 導入で手間がかかったくらいで、それ以外では電話で疑問を解消できたので、不満はない。

4.電力会社グループと保険会社グループが協業した今回の事業の運営体制について		
1	電力会社と保険会社グループによるサイバーセキュリティサービスの提供について	中部電力が、電力以外の分野も行うことで広がりを期待した。中部電力との付き合いは長く、<u>中部電力からの紹介があれば、検討する</u>と思う。 UTM においては、工事調整などの面で一部手間取ったが解消済み。 なお、保守 IT ベンダーはいるが、普段関わりはない。当社のネットワークの仕組みもわからない。かなり前の世代で対応し知らないことも多い。
5.中小企業が利用しやすい・選択しやすいサイバーセキュリティサービスについて		
1	中小企業が利用しやすいサイバーセキュリティサービスについて	UTM が実証期間中は無償であるが、コスト面が気になる。<u>ワンストップセキュリティサービスの月額費用は、個人的には安く感じる。有償継続は引き続き検討する。</u>
6.「サイバー保険」に対する率直なイメージ		
1	サイバー保険に対する理解度、イメージについて	現在サイバー保険には加入していない。 <u>UTM 導入やセキュリティルールを作ることが優先であり、サイバー保険は優先順位が高いものではない。</u> 会社のトップがどのように思っているかわからないということもある。ないよりはある方が嬉しい。上乘せ保険までは考えていない。 別々の保険会社よりは一つの保険会社の方が安心感はある。
7.今後の取り組みについて		
1	実証事業に参加して気付いたこと、今後の取り組みについて教えてください。	<u>無償で UTM 機器導入ができる事業があれば教えてほしい。</u> ワンストップセキュリティサービスの有償継続については検討したい。

(4)D社へのヒアリング結果

表 15 D社へのヒアリング結果

企業属性		
属性		内容
1	業種	②卸売業
2	従業員数	約 150 名
3	参加事業所の所在地	愛知県
4	PC 台数	100
5	ヒアリング担当者	システム担当者(総務部門)

ヒアリング内容		
ヒアリング項目		回答内容
1.お助け隊実証事業の参加動機、期待するものについて		
	1 お助け隊実証事業の参加動機、期待するもの	サプライチェーン上流企業から推奨され参加した。 情報収集と社員のレベルアップが一番の目的である。
2.自社のサイバーセキュリティに関する課題、実態、対策状況について		
	1 現在の社内セキュリティ状況	工場のインターネットは本社を経由して受け渡している。 工場は独立した回線であったが、本社と同レベルのセキュリティにする必要があり、本社から専用線を引き、インターネットと接続している。 <u>セキュリティに関する規程を作成はしたが、周知、教育指導が行き届いていない。</u>
	2 機密情報のやりとりはあるか	重要な設計図も取り扱っている。関係者のみ扱う厳重な管理をしている。
	3 サイバーセキュリティ上の懸念	メールのフィルタリング等、対策などがばらばらになっている。それをひとまとめにする UTM を検討していた。 そのためには <u>いろいろなネットワークをひとまとめにする必要が出てきており、課題</u> である。
	4 サプライチェーンからの要求事項	大企業からサイバーセキュリティに対する指導を含めたアンケートがくるため、対策をする必要がある。 <u>1社は取引要件レベル</u> 。他の企業は調査となっているが、いつまでに対応するか回答をする必要がある。
3.実証事業の各メニューについてご意見・ご感想・ご要望等		
	1 簡易セキュリティ診断	試しに実際運用している社員が記載した内容では大きく開きがあった。 対策について、社内周知できていないことがわかった。
	2 標的型メール訓練	非常に良かった。 <u>社員の警戒度がわかった</u> 。新人や若手は引っかけやすい。部長職でも一名引っかけ残念。 最初に予告メールを送り、間をあけて訓練を行った。 ある程度予告により、開封率が下がった。もしくは開いた人が周りにネタを開示したのかもしれない。 <u>総務に相談もあった。あとからネタばらしを行った。総務に連絡をすることは良いことだと考える。</u> 報告書をもう少し充実してほしい。

	3	ワンストップセキュリティサービス	今回実証期間が短く、ネットワークを止めることができないため、導入は断念した。今後導入するとしたら、大手で信頼できるところ。また通信のボトルネックにならないところ、できるだけ低価格、リモートメンテナンスのサービスがあることは必要。(K社の規模であれば月額3万円程度となることについて)リーズナブルであると感じる。
	4	EDR	不明なソフトをインストールしてください、ということで最初は不安だった。導入の際に説明がもう少しほしかった。導入の運用スケジュールもほしい。運用ベンダーから詳細説明をされるべきだとも感じる。(AIの学習期間などもわからなかった。)最初はアラートも不審メールかと思った。プラグインのレポートは一部しっかりしていたが、 <u>月報はログの塊でわかりづらい</u> 。 EDRは必要なので続けたいと思う。ないよりはましである。
	5	お助け隊事業全般について	短い時間で一度に多くのことをやりすぎである。受け入れる方は一社なので、一つに集中した方がよい。
4.電力会社グループと保険会社グループが協業した今回の事業の運営体制について			
	1	電力会社と保険会社グループによるサイバーセキュリティサービスの提供について	インターネットプロバイダのような、IT、サイバーセキュリティに精通した会社に対応すべきと考えている。 セキュリティ関連は同じベンダーに対応してほしい。導入、トラブルに関して連絡が取りやすい。
5.中小企業が利用しやすい・選択しやすいサイバーセキュリティサービスについて			
	1	中小企業が利用しやすいサイバーセキュリティサービスについて	中小企業向けのもので、低コスト、費用対効果が高い、専門性がない人間でも対応できる操作性がほしい。
6.「サイバー保険」に対する率直なイメージ			
	1	サイバー保険に対する理解度、イメージについて	<u>ベターであり、マストではない。あれば良い程度</u> 。社内的にも同じ認識 <u>IPAのセキュリティ支援員からセキュリティ事故を起こすと4億5000万かかると聞いて、若干意識は変わったと思う。</u> 目に見えないから余計こういった考えになる。
7.今後の取り組みについて			
	1	実証事業に参加して気付いたこと、今後の取り組みについて教えてください。	現在、IPAのセキュリティマネジメント指導業務を受けている。 社員教育とネットワークの統合が大きな課題である。

(5) E社へのヒアリング結果

表 16 E社へのヒアリング結果

企業属性		
属性		内容
1	業種	③サービス業(ソフトウェア業または情報処理サービス業、旅館業を除く)
2	従業員数	約 20 名
3	参加事業所の所在地	岐阜県
4	PC 台数	12
5	ヒアリング担当者	社長
ヒアリング内容		
ヒアリング項目		回答内容
1.お助け隊実証事業の参加動機、期待するものについて		
1	お助け隊実証事業の参加動機、期待するもの	中部電力グループからの紹介である。経済産業省の取り組みであり、参加者を集めているため、「協力してくれないか」という依頼で参加した。 話をもらった時に、<u>ゲームメーカーのサイバー攻撃被害のニュースを聞いていた。</u> <u>大企業でも被害を受けるとは思いながらも、中小企業で同等の対策を行うことはできない認識である</u>
2.自社のサイバーセキュリティに関する課題、実態、対策状況について		
1	現在の社内セキュリティ状況	パソコンに触る社員は限られており、厳密には教育していない。セキュリティ対策は、パソコンに触る社員と相談しながら決めている。
2	機密情報のやりとりはあるか	顧客台帳や損害保険関連資料はあるが、一部の社員によって厳重に管理されている。
3	サイバーセキュリティ上の懸念	我々のような零細企業では優先順位として、どうしてもセキュリティ対策の順位が下がってしまう。
4	サプライチェーンからの要求事項	サプライチェーンから要求はない。損害保険を扱っているので、保険会社から情報管理の指示はある。
3.実証事業の各メニューについてご意見・ご感想・ご要望等		
1	簡易セキュリティ診断	やってみたが良くわからないという印象。自社の対策を見直すツールとして活用してみる。
2	標的型メール訓練	パソコンに触る従業員に教育をすることが大切と認識。 一方で<u>こういった攻撃メールは、全く他所の話として、自社とは関係ないという認識を持った。</u>

	3	ワンストップセキュリティサービス	今回初めて UTM を導入した。言葉も知らなかった。 インターネット回線については業者に引いてもらっており、今まで対策を行ったことはなかった。各種情報の確認はシステムを委託している保守ベンダーに対応いただいた。
	4	EDR	導入作業は中電ミライズの支援を受けて実施した。 導入している実感はない。
	5	お助け隊事業全般について	特になし。
4.電力会社グループと保険会社グループが協業した今回の事業の運営体制について			
	1	電力会社と保険会社グループによるサイバーセキュリティサービスの提供について	中電はいろいろやっているの、そのうちのひとつといった印象。特に不信感はない。 信頼感はあるが、購入するかはわからない。
5.中小企業が利用しやすい・選択しやすいサイバーセキュリティサービスについて			
	1	中小企業が利用しやすいサイバーセキュリティサービスについて	<u>システム保守会社に勧められれば対応を受け入れると思う。</u> システム保守会社には経理、整備関連のシステムを導入いただいている。システム保守会社からセキュリティの話を聞いたことはない。
6.「サイバー保険」に対する率直なイメージ			
	1	サイバー保険に対する理解度、イメージについて	<u>全く知らなかった。</u> 今後、ニュースなどで取り扱われればイメージが付くが、事故をイメージできず、現時点では必要性はわからない。
7.今後の取り組みについて			
	1	実証事業に参加して気付いたこと、今後の取り組みについて教えてください。	<u>(サイバーセキュリティに限らず)事業継続の上では本業の売り上げの減少が一番大きなリスクである。</u> しかし本実証事業を通じて、サイバー分野について少し知れたので、有益な情報や機会があれば教えてほしい。

(6)ヒアリング総括

各社約1時間程度のヒアリングによって多くの貴重な情報を得ることができた。

ヒアリング結果から読み取れるポイントは、以下6点。

① お助け隊に期待するもの

中小企業がどこまでセキュリティ対策をすべきか不安や課題を抱えながらも従業員教育や自社のセキュリティ対策向上などを期待して参加している。無償という点は魅力的だが、一方で有償の場合にどこまで対応できるかは、本業利益や経営層の理解なども絡んでくるため、意思決定は簡単ではない。

② 中小企業の実態

従業員規模がおおよそ100名規模を超えると、(総務部門等の兼務で)社内セキュリティ担当を担っているケースが多い。それ以下の場合には代表者が直接セキュリティの対応を行っている。

セキュリティ対策を進める課題としては、人材不足、コスト、経営層の理解、自社にとってどのようなセキュリティサービスが適切か判断できないという声が多かった。

サプライチェーンの要求は一部取引要件レベルで要求されているケースもあるが、多くは注意喚起やチェックシート等による確認程度であるものの、昨年度よりは増加しているという現状がわかった。

③ 実証事業の各メニュー

簡易セキュリティ診断はIPAの自社診断25問ツールをベースにしているため、中小企業が網羅的に自社のセキュリティ体制を振り返るのに有益なツールであることがうかがえた。

標的型メール訓練は非常に人気が高く、従業員の警戒レベルや教育に活用できるとの声があった。自社従業員のセキュリティ意識の確認、ルールの周知程度の確認にも利用できた。

ワンストップセキュリティサービスは実証期間が短いこともあり、有用なサービスか十分に判断できない面もあるが、導入フローや電力会社グループがサービス提供することに抵抗感はなかった。また、費用面についても、機能や運用面も踏まえるとリーズナブルな価格であると受け止めがあった。

EDRはインストールは極めて簡単であるとの印象があるも、AIの学習期間があることや、実証期間が短いことからセキュリティ対策として十分な検証期間が足りていないという印象が強い。サービスの有用性を理解してもらうためにも検証期間がもう少し必要ということがわかった。

全体としては、実証期間が短かったため、「サービスの価値」を実感してもらえるところまで至れなかった面があり大変残念であった。できるだけその価値を説明することで、継続してサービスを利用してもらえるように誘導している。

④ 電力会社グループと保険会社グループの協業

中部電力グループは地域の重要インフラとして、大きな信頼感を得ており、サイバーセキュリティサービスを始めることについても抵抗感はないことがわかった。我々の仮説である「地域の重要インフラ企業によるサイバーセキュリティサービスモデル」は安定的なマーケットの拡大や将来性、中小企業へ広く普及させることのできるモデルであることがわかり、今後横展開をする際に、他地域の中核企業への説明にも活用できる基礎資料を収集することができた。

⑤ 中小企業が利用しやすいサイバーセキュリティサービスについて

中小企業にとって信頼できる事業者、かつ運用・管理サービスが付いており、コスト面で許容できる範囲のサービスを望む声が多い。無償のソフトやこうした実証事業において無償で活用できる機会を得ることはとても重要との声があった。

それだけコスト面およびそのコストを捻出するための経営層の理解、などに制約があることがわかり、引き続き経営層への啓発活動の重要性が明確となった。このような観点からも、中小企業の経営層へアプローチがしやすい中部電力グループのような地域中核企業が中心となる今回のモデルの優位性を改めて認識した。

また、自社のやり方が正しいのか、全体を俯瞰してコンサルティングするサービスを望む声もあった。

⑥ 「サイバー保険」に対する理解度、イメージ

サイバー保険の存在や補償内容はほとんど知られていない実態については、昨年度から大きな変化はなく、保険よりも、まずは対策を行うことが優先という実態がわかった。商品付帯サイバー保険については、セキュリティ機器に付帯されていることは安心感があるとの声が多かった。損害保険協会が実施するサイバー保険の普及活動を活用し、サイバー保険の認知度を上げるとともに、⑤の意見を踏まえたサイバー保険付きのセキュリティ機器の提供を増やしていく必要性を認識した。

4.3.8. 地域コミュニティとの連携

今回我々が実証を行った中部エリアには「中部サイバーセキュリティコミュニティ」や、令和2年度に新たに設立された「東海サイバーセキュリティ連絡会」といった会議体が存在し、本実証事業と並行してこれら地域コミュニティとの連携強化を図ってきた。

「中部サイバーセキュリティコミュニティ」とは令和元年度事業から情報共有を行い、コミュニティメンバーを対象に、お助け隊実証事業の成果や課題の報告を含めた、報告会を企画中である。

「東海サイバーセキュリティ連絡会」においては、本実証事業の情報共有を行い、募集についても協力を得てきた。今後開催される連絡会議において、本実証事業の成果を共有する機会も予定されている。

こうした地域コミュニティとの連携強化により、中小企業を含め、中小企業と取引のある大企業やその他関係機関においてもサイバーセキュリティに関する意識が高まり、結果として中小企業のサイバーセキュリティ強化の大きなムーブメントにつながると考えられる。

本実証事業を通じて得られた知見を活用し、更なる連携強化を図る。

4.4. 成果報告会

4.4.1. 開催概要

本実証事業での成果を取り纏め、報告会通じて実証参加企業へフィードバックを行った。

報告会では、SECURITY ACTION および中小企業の情報セキュリティ対策ガイドライン等の普及に向けた周知啓発活動を行った。

実証事業により得られた中小企業の実態詳細とニーズの把握、明確化された必要なセキュリティ対策サービス、人材、スキルを踏まえた「中小企業サイバーセキュリティ対策支援」について、中小企業向け簡易セキュリティ保険サービスを織り込みつつ、取り纏め、報告を行った。

当日プログラムは下記のとおり。

表 17 成果報告会プログラム

参加対象	全企業 (お助け隊事業(中部エリア)に参加した中小企業以外の参加も可能)
プログラム	13:30～13:35 開会挨拶(中部経済産業局) 13:35～14:00 「中小企業向け 情報セキュリティ対策支援事業の紹介」(IPA) 14:00～15:20 「サイバーセキュリティお助け隊事業(中部エリア)成果報告」(MS&AD インターリスク総研) 15:20～15:30 質疑応答(10分)および Web アンケート

4.4.2. 開催結果

新型コロナウイルス等の社会情勢を考慮して、当初予定を変更して、全てリモートによる開催とした。

2021 年 1 月 15 日(金)13:30～15:00 に開催した。

開催結果は下記のとおり。

表 18 成果報告会 開催結果

成果報告会	日程	時間帯	参加数計
事業説明会 (Cisco WebEx によるリモート開催)	2021 年 1 月 15 日(金)	13:30～15:30	38 社 (63 名)

4.4.3. 成果報告会でのアンケート結果

成果報告会にてアンケートを実施した。

詳細な事後アンケートがあるため、それとは別に簡易なアンケートを行った。

その内容は次のとおり。

図 49 本日の成果報告会は貴社のサイバーセキュリティ対策を検討する上で、参考になりましたか (N=42)

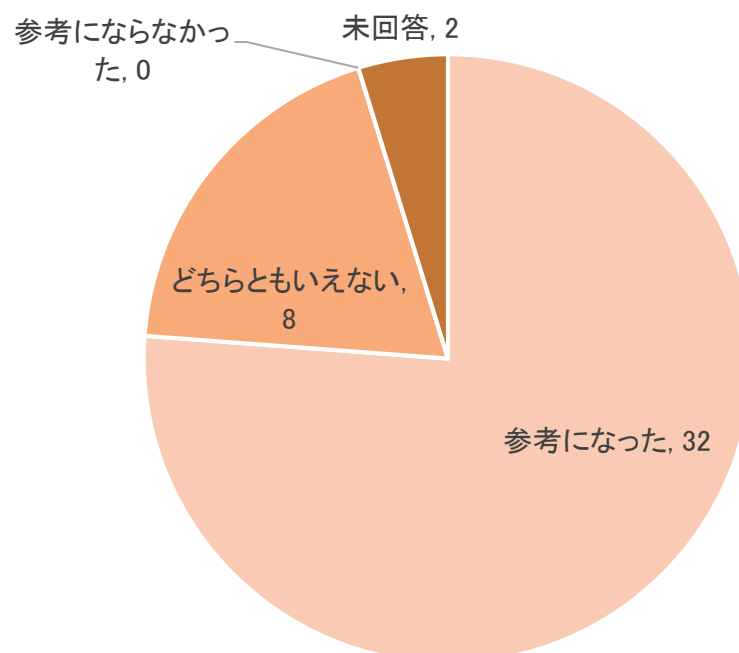


図 50 本日の成果報告会の中で、最も興味・関心があるテーマをご回答ください。 (N=42)

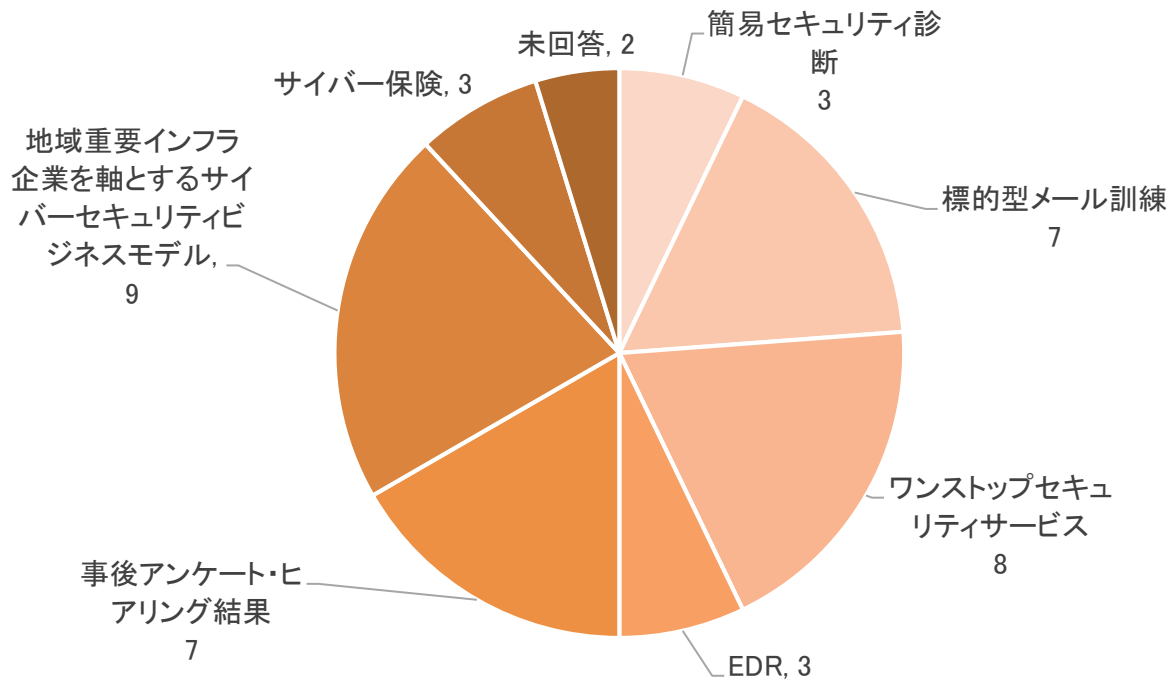


表 19 今後、サイバーセキュリティに関するどのような情報がほしいですか

分類	主な意見	備考
コスト関連	IT 補助金の情報があればいただきたいです。	
	国の補助金・助成金	
	EDR、運用開始ソフトなどの補助金	
	サイバーセキュリティ対策に関する補助金情報	
製品・サービス関連	小規模な事業所としての運用対策・情報	
	新しい技術などの情報を配信していただきたい。	
人材関連	セキュリティ担当に対する人材育成ツールまたはサービス	
	サイバーセキュリティ対策について、人材を考えるとするとどのような知識を必要とするのか	
その他	インシデント発生情報	事故事例
	新たな脅威やそれに対する対策が得れるとありがたいです。	
	実際の事故事例と対策内容	
	保険の情報はほしい。	サイバー保険
	各地域のお助け隊事業について	他地域情報
	国としての対策方針など最新情報	国の方針

5. 実証結果から得られた考察

5.1. 実証参加企業におけるサイバーセキュリティの実態

岐阜県を中心とする中部エリア(中部電力エリア)の中小企業 76 社に対して実証を行った。

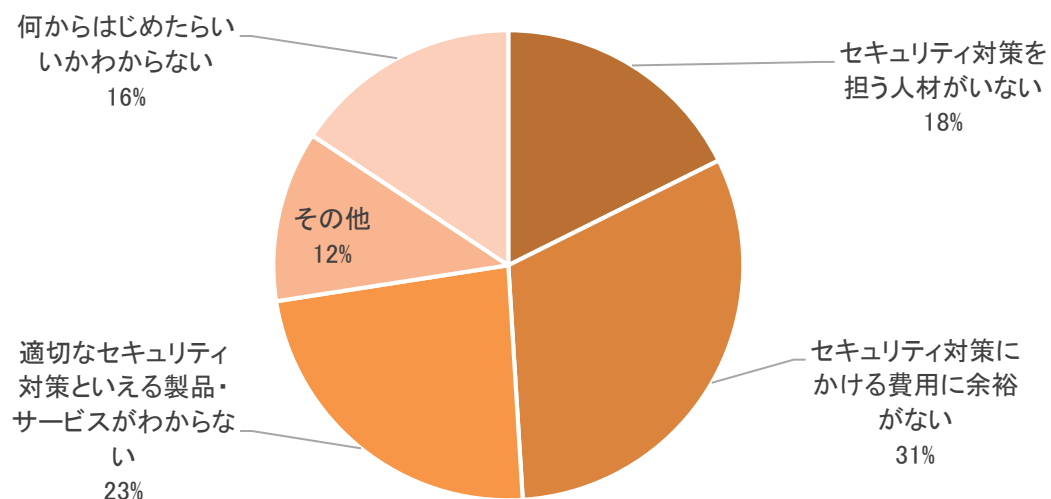
実証参加企業の業種や従業員規模、所在地等のデータは前述のとおり。

下図は、事後アンケートの項目一つである「サイバーセキュリティ対策を進める上での課題について、特に当てはまるものをご回答ください。」に対する回答結果(図 51)である。

最も多いのは「セキュリティ対策にかかる費用に余裕がない」が 31%

次いで「適切なセキュリティ対策と言える製品・サービスがわからない」が 23%、「セキュリティ対策を担う人材がいらない」が 18%となっている。この 3 つで 7 割超を占めている。

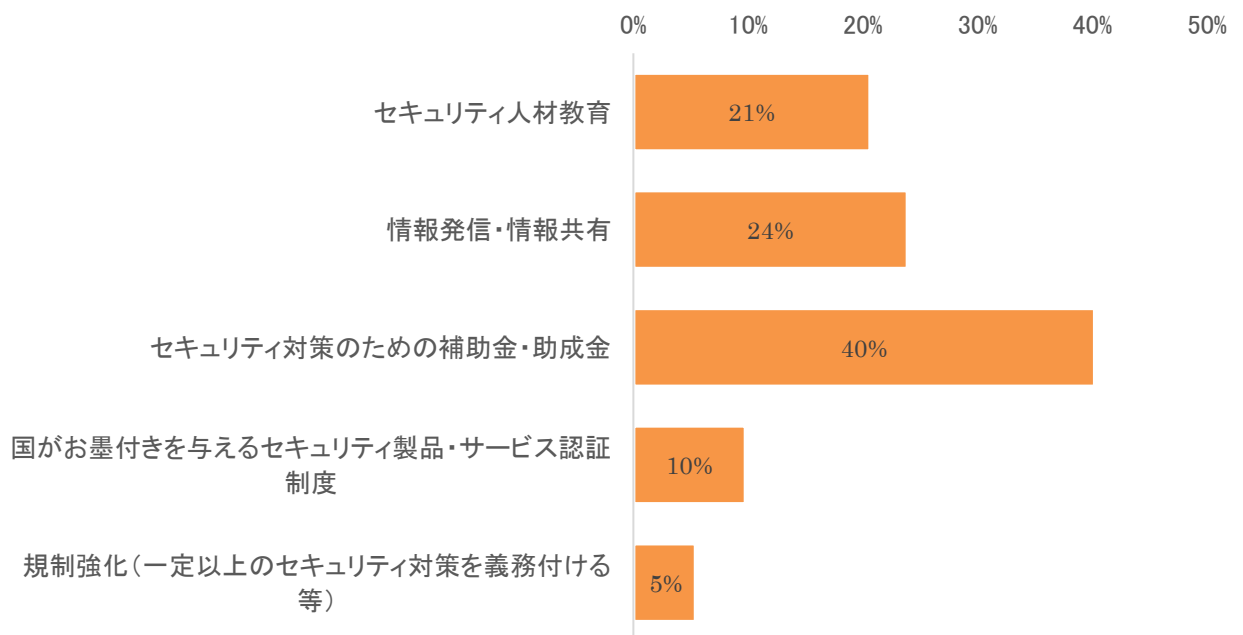
図 51 サイバーセキュリティ対策を進める上での課題について、特に当てはまるものをご回答ください。(N=51)



そして、再掲であるが事後アンケートの別項目である「今後のサイバーセキュリティ対策を進めるために国に望む政策について教えてください。」に対する回答結果(図 52)は次のようになっている。

最も多いのは「セキュリティ対策のための補助金・助成金」が 40%。次いで「情報発信・情報共有」が 24%、「セキュリティ人材教育」が 21%。「国がお墨付きを与えるセキュリティ製品・サービス認証」が 10%となっている。前述の「コスト」「人材」「適切なサービス」の 3 要素だけで 7 割超を占めている。

図 52 (再掲) 今後のサイバーセキュリティ対策を進めるために国に望む政策 (N=92、複数選択)



ただし「情報発信・情報共有」はセキュリティ製品やサービスに関する有益な情報提供も含むと考えられること、また、「適切なセキュリティ対策と言える製品・サービスがわからない」の答えを必ずしも国に求めているわけではないという点から単純比較はできないものの、「コスト」「人材」「適切なサービス」の 3 要素が、実証参加企業が抱える問題意識の主なポイントであると言える。

ヒアリングを行った企業からもこの 3 点が自社の課題であるとの声が多かった。

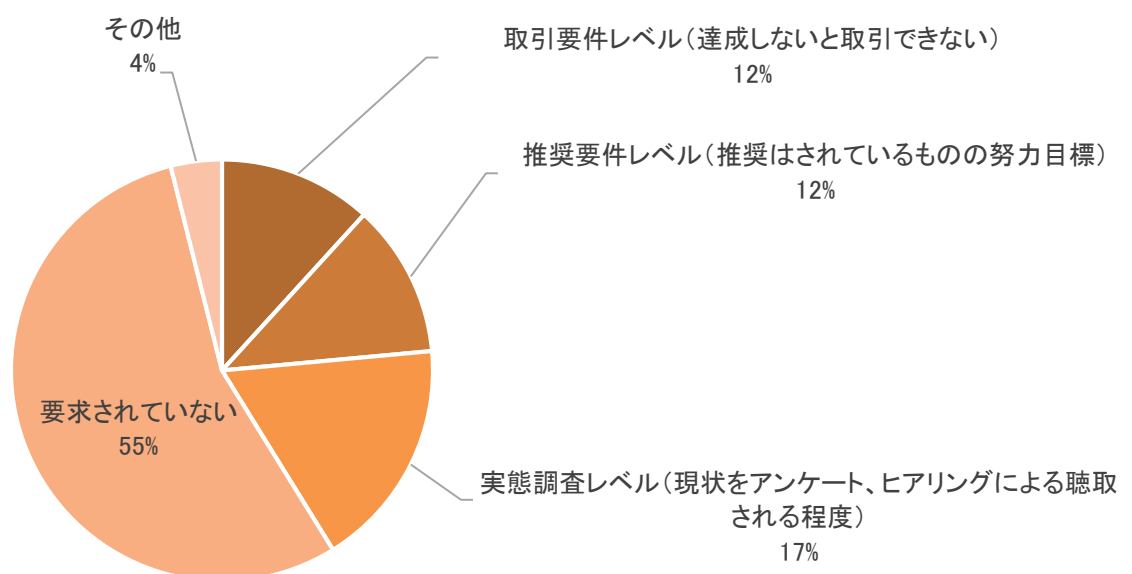
ヒアリングを通じて確認できたセキュリティ対策を進める課題としては、「コスト・経営層の理解(コスト支出の決定権を持つという意味でコストに分類)」、「人材不足」、「自社にとってどのようなセキュリティサービスが適切か判断できない」という声が多かった。

また、ヒアリングを通じて特に顕著に表れていたのが、従業員規模がおおよそ 100 名規模を超えると、社内セキュリティ担当者をおいているケースが多く、それ以下の場合は代表者が直接セキュリティの対応を行っているケースが多かった。

中小企業におけるサプライチェーン上流企業の要求は、一部取引要件レベルで要求されているケースもあるが、多くは注意喚起やチェックシート等による確認程度、あるいはそもそも要求されていないという現状がわかった。

下図は再掲になるが、事後アンケートの設問「セキュリティ対策について、「取引先(発注元)→貴社」に対してどの程度の要求を求められていますか。」に対する回答内容(図 53)である。

図 53 「取引先(発注元)→貴社」に対してどの程度の要求を求められていますか。
(N=51)



次に、本実証事業において提供した各種サイバーセキュリティ対策に対する受け止めについて考察する。

全体を通して「中小企業にとって不要な対策」という受け止めはなく、「自社の取り組みを見直すきっかけになった」等の前向きな意見が多かった。

一方で実証期間が短い中で多くのメニューを詰め込んだこと、問合せ窓口や運営事業者を一本化できなかったことがわかりづらさを招いた点があり、お助け隊事業者側として反省すべきがあった。

各メニューについて振り返る。

まず、簡易セキュリティ診断は、大半の企業が自立して回答できたことは実証参加企業の意欲の高さを示しているものと考え、「自社の現状の対策状況について見直すことができた」という声もあり、網羅的に自社の取り組みをチェックできたことは良いきっかけになった。300点以下が6割を占めている実態からすると、サイバーセキュリティに関する取り組みはごく一部ないし全く取り組めていない実態

が浮き彫りとなった。簡易診断については、よりわかりやすく、対策が見えやすい形が求められていることが明確になったため、今後改善を図っていきたい。

次に、標的型メール訓練は非常に人気が高く、中部電力ミライズの募集活動において、他メニューが実施できないことから、参加を見合わせるようになった企業においても、「標的型メール訓練だけでもやりたい」という企業が多数いた。標的型メール攻撃に対する認知度は高く、実証参加企業においても極めて関心の高いメニューであったと言える。開封率の結果から、どの企業でも本物の標的型メールを開封するリスクはあり、開封率を 0 にするのは難しいことがわかった。標的型メールを開封しないことも大切だが、開封してしまったあとの対処に関する取り組みはまだ不十分であり、「事後対応」を含めた訓練が求められることが、改めて明確となった。

実証事業に参加した企業のうち、実証事業を契機に本メール訓練実施も含めたセキュリティ対策基本計画の 3 カ年計画を策定し、自社のセキュリティ対策強化に活かす積極的な企業の事例も見られた。

ワンストップセキュリティサービスは実証期間が短いこともあり、有用なサービスか十分に判断できない面もあるが、導入フローや電力会社グループがサービス提供することに抵抗感はなかった。しかしながら、申込を受け付けたものの、実際に現地調査や設置工事まで行った段階で既に UTM を導入していることが判明する、設置する場所がないことが判明するなどのケースも見られた。昨年度事業と同様に、過去のシステム担当者が UTM 機器を購入したものの、運用がなされていないという実態があることがわかった。どの企業においてもインターネットに接続している以上、不審な通信や攻撃にさらされることは改めて確認できているが、問題はその実態を踏まえた管理・運用を行い活用できるかどうかである。人材、コストの問題を踏まえると管理サービス付きで中小企業でも手が出せる価格帯のサービスが現時点では最適であると考えられる。

アラートやインシデントについて特筆すべき事項として次のものが挙げられる。

- ・ C&C コールバックを UTM 設置によりブロックした。11 月～12 月に検知した本通信は 1 企業において発生したもので、WindowsXP 端末により発生。当該端末を買い替えたことにより、以後検知せず。1 月は別企業でも発生している。
- ・ IPS(侵入防御システム)にて検知、防御が必要な通信を多数検知。中小企業においても、攻撃通信の標的となることが再確認できた。
- ・ スпамメール対策は最も数が多く検知されたもの。無数に飛び交うメールは危険なものが多く、中小企業でもサイバー被害のきっかけとなり得ることを示している。
- ・ ランサムウェアのブロックが 34 件発生しているが、これは 1 企業において発生したもので、UTM によりブロックされており感染被害を防いだ。
- ・ コールセンター対応は、C&C コールバックと UTM 機器の通信障害に関するものが主たる対応となった。
- ・ 昨年度事業では現地駆けつけ対応が 3 件発生したが、今年度は現地駆けつけ対応は発生せず。実証期間が短いこともあり、駆けつけが必要なインシデントは発生しなかった。

UTMを導入した企業で、特に検知・対応が発生した企業は本サービスを導入した有用性を強く実感している様子が見られた。これをきっかけとして、自社の攻撃実態の把握や自社にて持つべき知識や体制の見直しにつながっていくと考えられる。

EDRはインストールは極めて簡単であるとの評価を得たものの、AIの学習期間があることや、実証期間が短いことからセキュリティ対策として十分な効果を実感する検証期間が足りていないという印象が強かった。サービスの有用性を理解してもらうためにも検証期間がもう少し必要ということがわかった。

アラートやインシデントについて特筆すべき事項として次のものが挙げられる。

- ・ 導入から1ヵ月間に検知した「不審なコマンド実行」や「不審なプロセス起動」は大半が過検知によるもの。そういった中にも、サポートが終了したメンテナンスされないソフトウェア（プラグイン）の振る舞いを検知しているケースもあり、ユーザーに対する注意喚起になった。
- ・ 実証期間が短いこともあり、AI学習期間後の本格稼働データは十分に取得できていない。
- ・ コールセンター利用は個別アラートの内容や脅威レベルに関する問合せ。
- ・ 実証期間が短いこともあり、駆けつけが必要なインシデントは発生しなかった。

EDRを導入した企業で、特にアラート通知を受け取った企業は、EDRの有用性を実感する機会になったと考えられる。一方で、本サービスの月報やアラート通知の内容や見やすさについては、不十分であるとの声も多く、今後のサービス改善に重要なポイントの検証とすることができた。

また、導入面では、申込を受け付け、実際にインストーラの提供を行ったものの、端末がEDRサポート対象外であることが判明するケースが見られた。それがインストール支援のための現地訪問支援によって判明するなど、ITリテラシーの低さを示すケースも見られた。こちらもUTMと同様に、検知する前提で、管理・運用を行い活用できるかどうかが重要であり、管理サービス付きで、中小企業でも手が出せる価格帯のサービスが最適であると考えられる。

今後のサービス改善という課題はあるものの、導入の容易さや、使い始めての問題がなかったことから、EDRについては12月下旬に、新サービスとしてローンチを実現できた点は、お助け隊実証事業による大きな成果であった。

今回の実証事業では、中部電力ミライズによる各種サービスの申込支援として、実証参加企業の3割(22社)に対して訪問サポートを複数回実施した。対応内容のほとんどは、UTMの設置に伴う現状確認で、次いでEDR、標的型攻撃メール訓練、簡易セキュリティ診断となった。

訪問支援を通じて見えてきた点は、各メニューが同時進行で複数のメールが配信されているため、順を追って対処できておらず、何をすべきかわからなくなるケースやエクセルやワードに不慣れで対処できていないケースも見られた。

サイバー保険に関しては、サイバー保険の存在や補償内容はほとんど知られていない実態である点は昨年度実証から大きな変化はなかった。加入している企業は1割程度で、日本損害保険協会の調査結果とほぼ同水準であった。

保険よりも、まずは対策を行うことが優先という実態がわかった。商品付帯サイバー保険については、セキュリティ機器に付帯されていることは安心感があるとの声が多かった。

5.2. 中小企業におけるサイバーセキュリティの課題

「セキュリティ対策にかかる費用に余裕がない」

「適切なセキュリティ対策と言える製品・サービスがわからない」

「セキュリティ対策を担う人材がいない」

この3点が実証事業を通じて、中小企業にとっての大きな課題として見えてきた。

これは本実証事業に参加した企業のみならず、多くの中小企業に言えることと考える。

中小企業におけるサイバーセキュリティの課題を集約すればこの3点のいずれかに該当することが大半であると考えられる一方で、中小企業のサイバーセキュリティ対策への関心度、理解度、社内体制、中小企業を取り巻く環境、などを踏まえれば、実際の対策状況は千差万別である。

だからこそ、中小企業にとって信頼できる事業者、かつ運用・管理サービスが付いており、コスト面で許容できる範囲のサービスを望む声が多い。無償のソフトやこうした実証事業において無償で活用できる機会を得ることはとても重要との声があった。

それだけコスト面およびそのコストを捻出するための経営層の理解、などに制約があることがわかる。この点についても、中小企業の経営層に直接コンタクトできる企業からの推薦や提案があることが効果的であることも見て取れた。また、自社のやり方が正しいのか、全体を俯瞰してコンサルティングするサービスを望む声もあった。

更に潜在的な課題として、令和元年度事業でも報告した「無関心層の存在」が挙げられる。実証事業に参加していない企業は多く存在しており、中には「サイバーセキュリティ対策には一切関心がない」という企業が今回の中部電力ミライズによる募集活動においても多数見られた。こうした無関心層には、国等からの情報発信やサプライチェーン上流からの取り組み強化によって、まずは関心を持ってもらうことから始めるアプローチが必要と考える。

5.3. 実証を踏まえ今後中小企業に必要と考えるサイバーセキュリティ対策

(1)コスト面のアプローチ

中小企業にとって最も重要なのはコスト面であることがわかるが、まずは次のデータを示す。

次の二つの図は、再掲であるが、本実証事業の事後アンケートで「ワンストップセキュリティサービス(UTM)にかけられるコストはいくらか(図 54)」「EDR にかけられるコストはいくらか(図 55)」という設問に対する回答である。

UTM に関しては、「月額 1 万円未満」が約 9 割、EDR に関しては相場がわからないという回答が最も多いが、次いで多いのが「端末 1 台あたり月額 1000 円未満」である。

安いサービスを望む声は多いものの、ヒアリングや実証企業とのやりとりの中で、その機能や管理サービスの充実を求める声もあり、昨年度に引き続き単に安ければいいというものではないことがわかる。

中小企業の人材面や IT リテラシー面も踏まえると、全ての中小企業で運用管理を行う人材を設置することは至難であり、UTM も EDR も管理サービス付きであることが必須と考える。

サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)と経済産業省、IPA が連携して検討が進められている「サイバーセキュリティお助け隊サービス制度」の審査基準にこの点が含まれていることを踏まえ、民間事業者は適合する製品・サービスを展開していくことが必要と考える。

一方で民間事業者にとっては、価格とサービス品質は比例するものであり、中小企業の求める価格帯が、ニーズに合致する品質を提供できる水準であるかは疑問が残る。管理サービス付きサイバーセキュリティ商材のサービス品質を上げつつも、価格を抑える企業努力は必要だが、ビジネスとして検討する以上、その採算性を踏まえることは必須である。

そこで、コスト面の対策として、一定期間の国等による補助金・助成金を組み込んでいくことを提案する。

例えば特許庁における「海外知財訴訟費用保険制度」はその保険料を国が一部負担するスキームとなっている。

また、経済産業省の「IT 導入補助金」は有益な IT ツールを導入する際の費用を一部負担するスキームとなっている。

サイバーセキュリティ管理サービス付きサービスを中小企業が導入する際の費用の一部を負担するスキームを組み合わせることで、中小企業にとって導入ハードルが下がり、結果として民間事業者にとっても採算が取れる水準でのサービス開発につながると考えられ、これによってコスト面の課題解消につながると考える。

図 54 (再掲)UTM の設置、コールセンターの利用、駆けつけ対応を含む今回のワンストップセキュリティサービスにかけられる費用についてご回答ください。 (N=51)

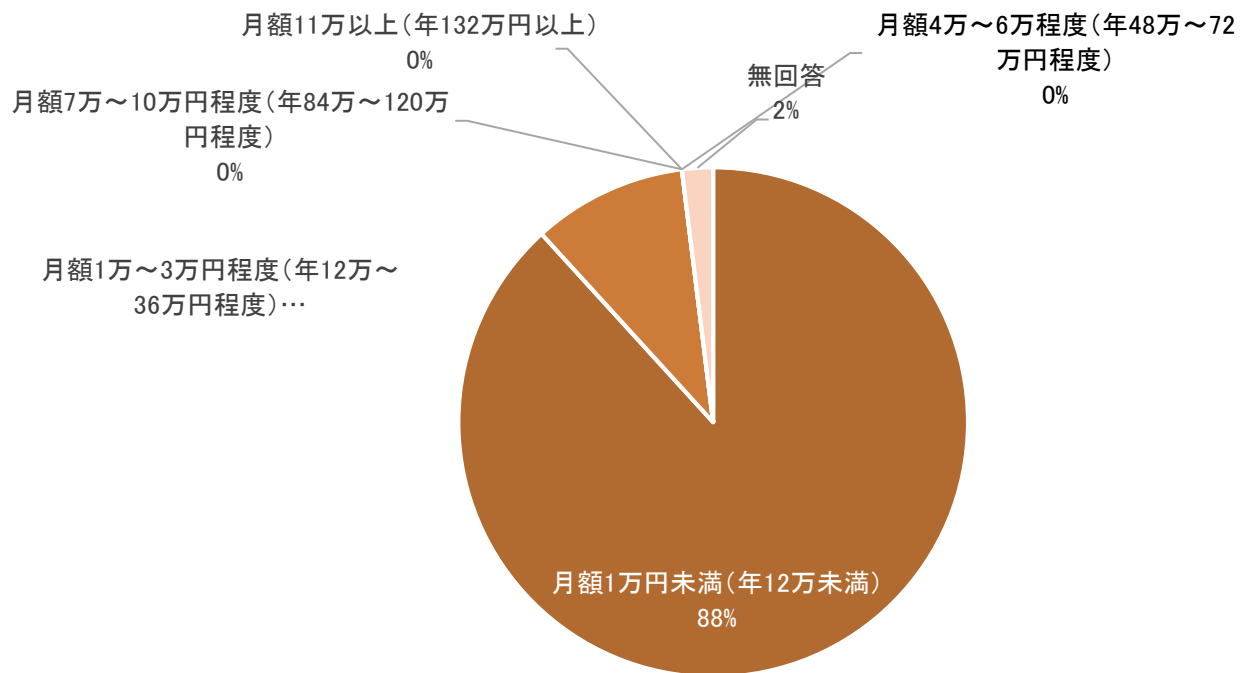
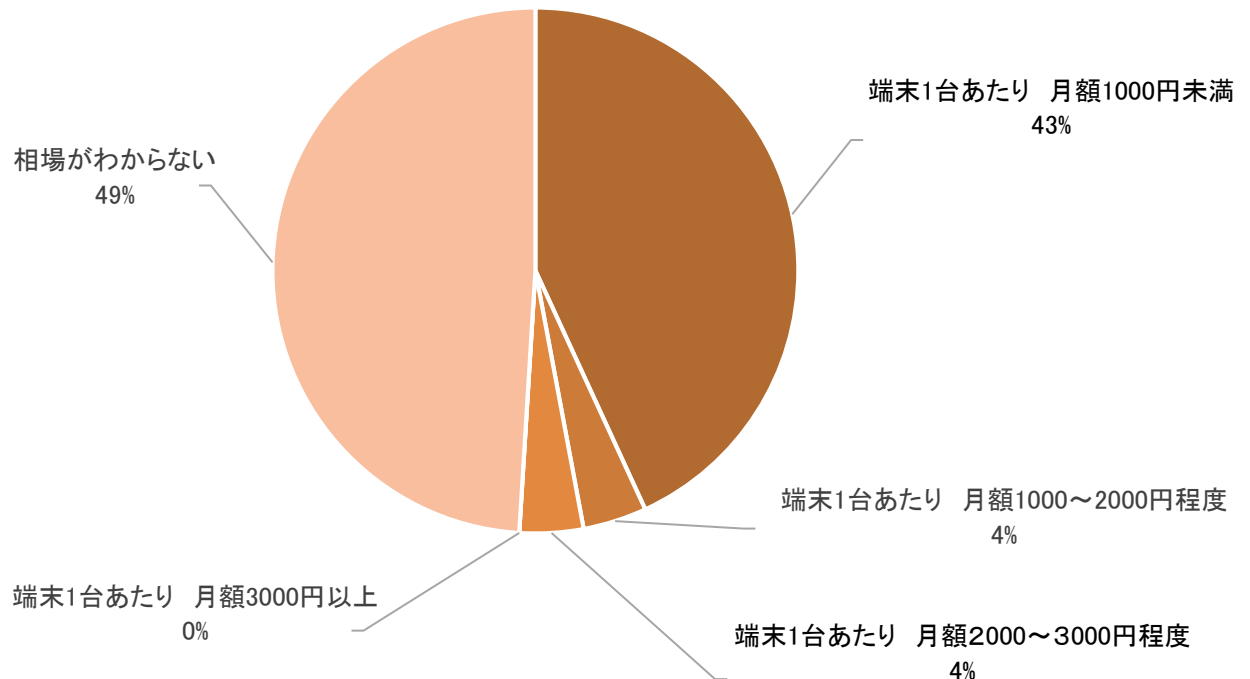


図 55 (再掲)EDR(エンドポイント監視サービス)にかけられる費用についてご回答ください。 (N=51)



(2) 適切な製品・サービス面のアプローチ

次に、中小企業にとって適切な製品・サービスがわからないというポイントについて、以下のデータを示す。本実証事業の事後アンケートで「お助け隊事業で活用できたメニューは何か」という設問に対する回答内容(図 56)である。

本実証事業において我々が用意したサービスメニューは 4 つ。限られた実証期間に同時進行で進めたこともあり、中小企業にとってはやや過剰で人的リソース的にもオーバーワーク気味な側面も見られたが、改めて各メニューの目的・意図を振り返る。

「簡易セキュリティ診断」で網羅的に自社の取り組み状況を振り返り、対策のポイントを見つける。

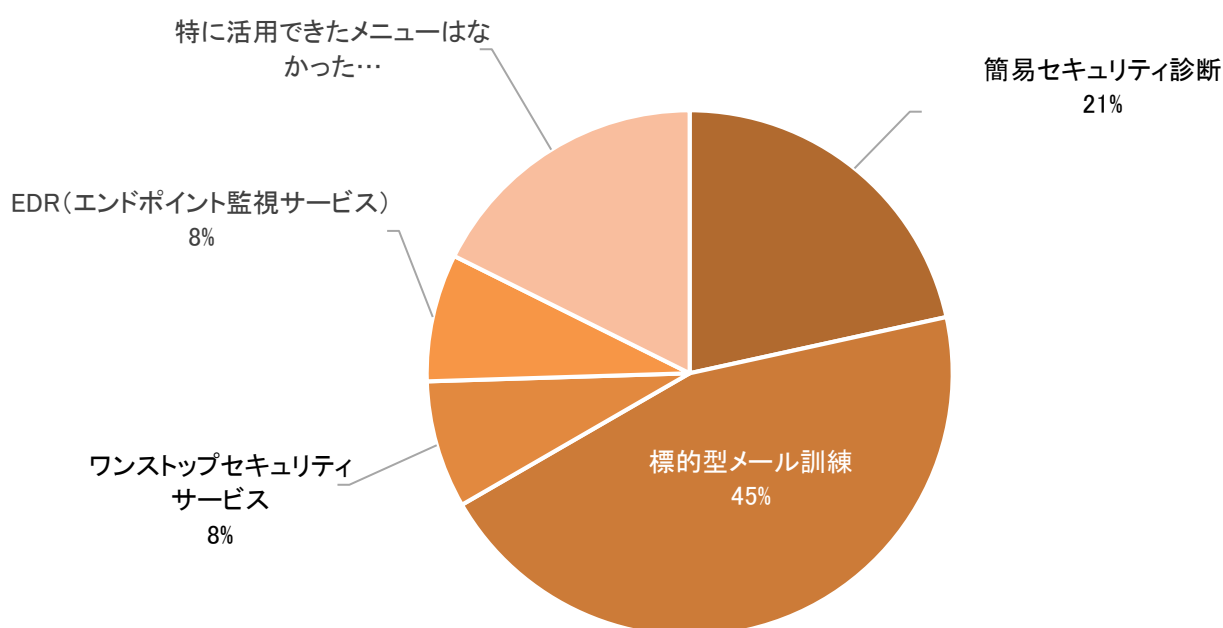
「標的型メール訓練」で、標的型メール攻撃の認知度および警戒心を高め、訓練メールへの対応を個々人に評価し、適切な対応が行えるよう教育を行う。繰り返し実施することで、部署ごと・従業員ごとの傾向をつかみ、実効性ある対策を検討する。

「ワンストップセキュリティサービス」でネットワーク監視型の UTM を設置し、コールセンター、駆けつけ機能、監視サービス機能がワンパッケージになった管理サービス付き UTM サービスの使い勝手、社内での運用を検証する。

「EDR(エンドポイント監視サービス)」でエンドポイント監視型の EDR を設置し、こちらもコールセンター、駆けつけ機能、監視サービス機能がワンパッケージになった管理サービス付き EDR サービスの使い勝手、社内での運用を検証する。

これらがサイバーセキュリティ対策の全てではなく一部ではあるものの、ここから言えることは中小企業が「まず関心を持ち→知識を付け→使い勝手を確認しながら→自社の規模や取り巻く環境から最適なサービスを見つけていく行動」につなげることが重要と考える。

図 56 (再掲)お助け隊メニューの中で特に活用できたメニューについてご回答ください。
(N=51)



前述のとおり、「適切な製品・サービスがわからない」という点について単にその機能と価格が判断基準ではないと考える。

次に示すのは、再掲になるが本実証事業の事後アンケートで「電力会社がこれらのサービスを提供するとしたら、どのように感じますか。」という設問に対する回答である。(図 57)、

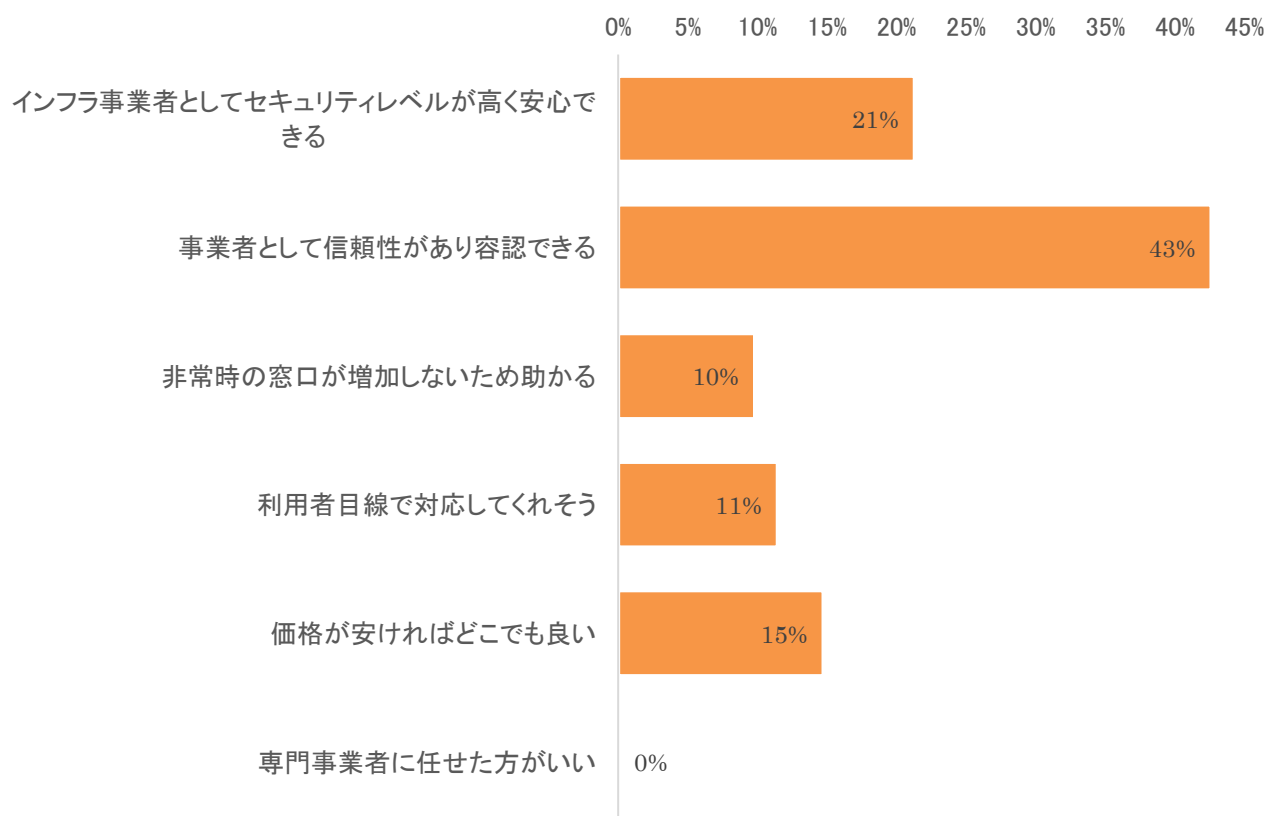
今回我々が実証した電力会社等の中小企業と密接な結びつきのある重要インフラ企業によるサービス提供は中小企業にとって信頼度が高く安心できるとの声が多く見られた。

我々が実証した「電力会社グループと保険会社グループによるサイバーセキュリティ対策サービスの提供」は、こうしたアプローチの理にかなったマーケティングスタイルと考える。

ヒアリングにおいても、中部電力グループは地域の重要インフラとして、大きな信頼感を得ており、サイバーセキュリティサービスを始めることについても抵抗感はないことがわかった。我々の仮説である「地域の重要インフラ企業によるサイバーセキュリティサービスモデル」は安定的なマーケットの拡大や将来性、中小企業へ広く普及させることのできるモデルであることがわかった。

このように中小企業との接点を増やし継続的にサイバーセキュリティ対策を案内・提供していくことが、結果として「適切な製品・サービスがわからない」という点の解消につながると考える。

図 57 (再掲)電力会社がこれらのサービスを提供するとしたら、どのように感じますか。
(N=61、複数選択)



(3) 人材面のアプローチ

前述のとおり、中小企業においてセキュリティ人材の確保は大きな課題となっている。

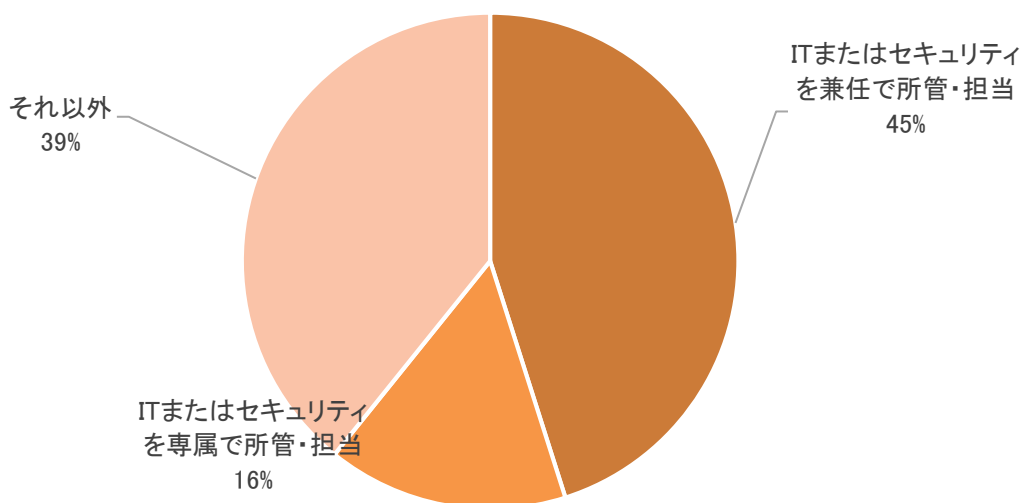
下図は、本実証事業の事後アンケートで「IT またはセキュリティ業務に関してあなたの業務内容を教えてください。」という設問に対する回答である。(図 58)

IT またはセキュリティ業務を専属で所管・担当しているのはわずか 16%であった。この実態を踏まえると、恒常的に多忙で限られた経営資源でやりくりしている中小企業においてセキュリティ専門人材を育成していくことは至難である。

そこで管理サービス付きサイバーセキュリティサービスによってアウトソースすることでその不足を補うことが最適と考えられる。しかしアウトソースすれば万事 OK というものではない、管理サービスにも限界があり、例えば月次レポートやインシデントの可能性のあるアラームの通知を受けた際に、アウトソース先との窓口となり、対応できるレベルに育成する必要性は残る。

また、アウトソースするにしても目利き力のない中小企業にとって、現在検討されている「お助け隊認証マーク」のような、公的に第三者が評価したサービスが明確になることは、非常に価値が高いと考える。

図 58 IT またはセキュリティ業務に関してあなたの業務内容を教えてください。 (N=51)



また、サイバーセキュリティ対策はセキュリティ担当者だけいけば良いというものではなく、従業員教育や社内ルールの周知徹底など、社員全員の IT リテラシーの向上がつきものとなる。

これらは情報発信やセミナー、コンサルティングサービス、あるいは今回実施した標的型メール訓練などの意識向上取り組みを活用して、従業員全体の底上げを図る必要がある。

前述の(1)や(2)の取り組みを推し進めることで、必然的にそれに対応する中小企業の人材は知識を付け、経験を積み、自社がやるべきことが見えてくる環境を整備していく必要がある。

お助け隊事業はその一環であるが、国には是非継続して中小企業のサイバーセキュリティ対策支援の枠組みの用意を期待する。

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サービスのビジネス化に向けた課題・検討

6.1.1. 実証事業終了後の継続的なサービス提供

(1) 全体論

我々の事業で目指したポイントは下記 2 点である。

- ① 地域の中核企業・重要インフラ企業(電力、ガス等)を核とした中小企業向けサイバーセキュリティ普及モデルの構築
- ② 地域サイバーセキュリティコミュニティとの連携による全国展開可能な地域サイバーセキュリティ支援体制モデルの構築

①については、企業の経営層と対話機会が多く、エネルギー事業を切り口に省エネや BCP 等多様な課題解決コンサルティングを既に実施している中部電力グループが、多様なサイバーセキュリティ対策サービスを提供するスキームについて実証を行った。

実証を通じて、中部電力グループと MS&AD グループでそれぞれのリソースや目指す方向性のすり合わせを行い、継続的なサービス提供について議論を重ねてきた。

議論の中で、中部電力グループの認識としても、新型コロナの影響もあり、リモートワークやネット通販などが増加し、官公庁関連の申請においても電子化が進む傾向にある。インターネットの利用拡大していくことでサイバーリスクは増大するため、電力供給先企業のサイバー対策は、安定収入を確保する上でも重要と認識していることがわかった。また、事後アンケートでも中部電力グループがサイバー対策のサービスを行うことについて、9 割近くが良い印象を持たれており、これまでお客様の目線に立った営業活動からの信頼関係が評価されていることを確認するとともに、お客様のニーズに対して答えられるようなサイバー対策に関連する以下のサービス化に向けて、次年度中を目途に検討を進めていくステージに移行した。

- ・中部電力ミライズの Web サイトから簡易セキュリティ診断などの無償サービスの提供
- ・認定基準に合致したネットワークと端末機との両面に対する監視サービスの提供
- ・標的型攻撃メール訓練などを中心としたサイバー教育の支援サービスの提供

本成果報告書提出時点では検討を続けている段階であり、詳細については記載できないが、事業目的である「地域の中核企業・重要インフラ企業(電力、ガス等)を核とした中小企業向けサイバーセキュリティ普及モデルの構築」の目的は達成できたものと考えている。

②については、前述のとおり、中部エリアのコミュニティとの連携強化を本実証期間中も行ってきた。

「中部サイバーセキュリティコミュニティ」とは令和元年度事業から情報共有を行い、コミュニティメンバーを対象に、お助け隊実証事業の成果や課題の報告を含めた報告会を企画中である。

「東海サイバーセキュリティ連絡会」においては、本実証事業の情報共有を行い、募集についても協力を得てきた。今後開催される連絡会議において、本実証事業の成果を共有する機会も予定されている。

こうした地域コミュニティとの連携強化により、中小企業を含め、中小企業と取引のある大企業やその他関係機関においてもサイバーセキュリティに関する意識が高まり、結果として中小企業のサイバーセキュリティ強化の大きなムーブメントにつながると考えられる。

こちらも発展途上であるが、事業目的である「地域サイバーセキュリティコミュニティとの連携による全国展開可能な地域サイバーセキュリティ支援体制モデルの構築」の目的および構築に向けて必要となる基礎データの収集は達成することができた。

(2) 個別サービス

次に個別サービスの継続提供の方向性について記載する。

① 簡易セキュリティ診断

中小企業向けのセキュリティサービス提供のドアノックツールや、サイバー保険引受におけるアンダライティングへの活用も見越して検討を継続する。

なお、大企業向けには更に詳細な設問表があり、今後の活用に向けて併せてブラッシュアップしていく。

中部電力グループとのコラボレーションも含め、簡易セキュリティ診断ツールとして継続的なサービス提供を行う予定。

② 標的型メール訓練

既に MS&AD インターリスク総研の有償サービスとして提供しているものではあるが、本実証事業を通じて得られた知見や寄せられた意見を反映し、報告書の充実化やパッケージプランの多様化なども含め、今後のサービス提供において活用していく。

③ ワンストップセキュリティサービス

本実証事業を通じて、検証できた課題を整理し、中部電力グループがサイバーセキュリティサービスを提供したモデルを検証・改善し、今後サービス提供を進めていく準備を調整している。具体的な価格帯は、最も廉価な UTM で月額 1 万円を下回るサービスとして提供可能な見込みであり、サイバーセキュリティお助け隊サービス制度にも適合する商材として対応可能な予定である。

④ EDR

本サービスは、実証事業開始時点ではサービスとして提供していない段階であったが、エンドポイント監視と初動対応・駆けつけサービスも含むサービスとして整備し、本実証事業を通じてビジネス化を検討してきた。EDR は導入がシンプルで、実施決定企業へのスピーディーな展開が可能であったことから検証にも早期に着手することができ、実証を通じて得られた経験をもとに、2020 年 12 月に本サービスをビジネス化し、一般向けにリリースすることができた。

こちらも経済産業省のお助け隊サービス認証にも適合する商材として対応可能である。

6.1.2. サイバー保険の活用

本実証事業を通じて、MS&AD グループの保険会社 2 社（三井住友海上火災保険、あいおいニッセイ同和損害保険）と中小企業のサイバーセキュリティ対策とサイバー保険について議論を重ねてきた。その検討結果を実証事業の総括とともに記載する。

(1) サイバー保険の実態

① サイバー保険の必要性

昨今、政府機関や企業に対する、標的型メール等による不正アクセスなど、いわゆるサイバー攻撃の急激な増加により、個人情報情報の漏えい、データの損壊・改ざん等の深刻な被害が生じており、その手法もより巧妙化しつつある。このような社会的な情勢を受け、事業者は、高額な損害賠償請求を受ける、あるいは事故対応に多額の費用が発生するといったリスクにさらされている。

サイバーセキュリティ関連サービスを導入、従業員教育を行うなど対策を講じた上でも残存するリスクをヘッジする方法の一つがサイバー保険による備えである。

② サイバー保険の認知度や加入率

日本損害保険協会が 2020 年 12 月 9 日に公表した「国内企業のサイバーリスク意識・対策実態調査 2020」において、国内企業のサイバーリスクへの意識や対策状況が報告されている。

「サイバー保険の内容について良く知っている」と回答したのは大企業において 11.5%、中小企業においては 10.6%であった。

また、「サイバー保険に加入している」と回答したのは、大企業において 9.8%、中小企業においては 6.8%という実態である。

③ サイバー事故の実態

同様に日本損害保険協会の最新の調査によれば、過去にサイバー被害を受けたことがあると回答した企業は、全体で 13.4%、大企業で 17.1%、中小企業で 11.4%であった。

また、被害総額については、大企業と中小企業であまり差はなく、「100 万円未満」が全体で 85.9%を占めるものの、「100 万円以上」も 14.1%おり、中小企業に限っても「100 万円以上」が 12.7%という結果が出ている。

また、本実証事業参加企業において実際にサイバー事故は発生していないが、参考データとして、MS&AD インシュアランスグループで取り扱っているサイバー保険における事故の実例の一部(表 20)を記載する。

表 20 サイバー保険における事故の実例(一部)

	業種	売上高	事故概要	支払保険金※
費用損害	小売業	1 億～5 億円	顧客向けに公開していた自社通販サイトが不正サーバーからの DoS 攻撃により、同サイトの管理サーバーがダウン。復旧および被害調査を行った。	約 1,100 万円
	卸売業	10 億～20 億円	従業員の PC がウィルスに感染し、メールシステムが乗っ取られた。不正操作により取引先およびお客様のもとに迷惑メールが複数送信された。	約 300 万円
	サービス業	1 億円未満	従業員が詐欺の電話に誘導され PC 操作を行い、遠隔操作ウィルスを含む不正ファイルをダウンロード。情報漏えいの恐れが発生。	約 200 万円
賠償損害	小売業	1 億～10 億円	顧客情報を漏えいさせたことにより、取引先の業務を阻害したとして、取引先に生じた営業損失について損害賠償請求された。	約 1,600 万円

※支払保険金は、当該事例において実際に支払いされた保険金であって、保険対象外の損害も発生している

これらの結果から、中小企業であってもサイバー被害を受ける可能性は十分にあり、費用損害のみならず賠償損害も発生している実態がわかる。費用損害よりも、賠償損害は発生頻度は少ないものの、一旦発生すると被害額は大きくなる傾向にある。

費用の中でも争訟費用(訴訟に限らず、裁判の申し立て手数料、証人、鑑定人、通訳人の日当・旅費等)については、賠償損害の一部として補償を提供することが一般的であることから、賠償損害への補償も不可欠であると言える。

(2) 実証事業におけるサイバー保険の検討

本実証事業においては、中小企業にとって望ましいサイバー保険の加入方式、価格設定、補償内容など実証事業全体を通じて検討を行うことを目的とした。また、検討にあたっては実証事業後の新たなビジネスモデル(継続したサービス化)を見据えて、具体的な保険およびサービスのあり方・提供スキームについて検討を行った。

本実証事業において、主に実施した検討のポイントは下記のとおり。

① 簡易セキュリティ診断ツール

IPA が出しているものをベースに、保険引受に活用していくことは国の施策と連動し普及につながる。このツールを保険引受上のリスクアセスメントツールとして活用していくことを検討した。

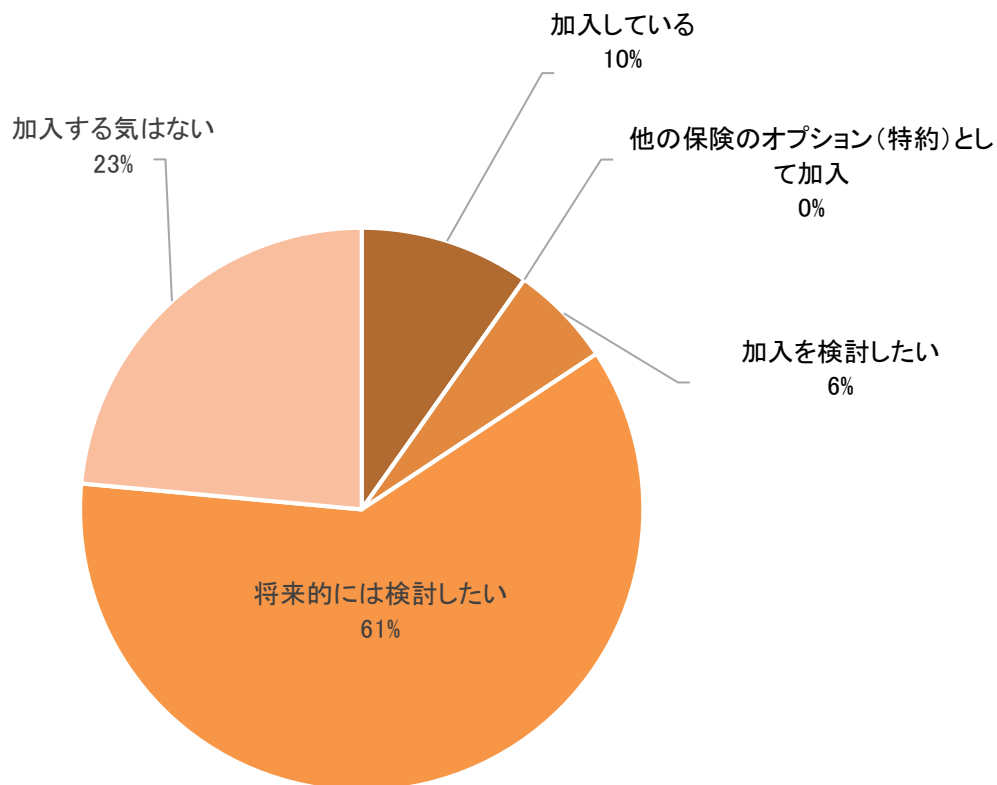
② 中小企業が取引先等から求められているセキュリティ対策レベル

事後アンケートによる中小企業の実態(取引等から求められるレベル)では大半が求められていない、あるいはアンケートレベルの照会であることがわかった。

再掲になるが事後アンケートによるサイバー保険関連の設問「サイバー保険に加入していますか」に対する回答結果(図 59)では、わずか 10%が加入しているとされ、損害保険協会の調査結果よりもやや高いとは言え、極めて低い水準であることがわかる。

ヒアリングにおいても、その存在や必要性を認識している企業はほとんどおらず、サイバー保険の認知度の低さを実感した。

図 59 既にサイバー保険(情報漏えい保険を含む)に加入していますか。 (N=51)



③ 加入方式

実証事業で提供した UTM および EDR には MS&AD グループのサイバー保険を商品付帯方式でセットし、提供した。商品付帯方式は最低限の補償内容にとどまっていることから、上乗せ加入は既に可能であり、今後シームレスな加入方式を検討していく必要がある。

④ その他昨年度の検討結果も踏まえた更なる検討

(3) 実証事業を通じて得られたサイバー保険のあるべき姿

MS&AD グループでは下記のようなポイントでサイバー保険およびその周辺環境の整備を進めていく予定である。

① 保険会社のサイバー保険関連サービスの整備

- ・ 簡便なセキュリティ診断による告知(簡易セキュリティ診断の活用)
簡易診断(告知書)は今後、中小企業向けリスク診断(アンダーライティング)としてブラッシュアップして活用する。中電グループとの連携も含め、Web 回答方式の充実化も検討する。
- ・ 補償内容について、現在の汎用商品における設計の柔軟性向上を検討する。
- ・ 損害サポート体制(保険事故発生時の対応)の強化・拡充
- ・ コールセンターの構築(MS&AD グループで構築中)

② マーケティング

- ・ セキュリティ商材とサイバー保険のパッケージ(商品付帯方式)
- ・ ワンストップセキュリティサービス(UTM)への商品付帯サイバーの構築
- ・ EDR(防検サイバー)への商品付帯サイバーの提供(既にリリース済み)
- ・ お助け隊サービス認証の活用

③ 中電グループとの協業による保険加入方式の検討

- ・ 中電グループとの協業を進めていく中で、セキュリティ商材との一体化、そのスキームと連動した加入方式の検討は継続して行う
- ・ こうしたスキームは他の重要インフラ事業者等にも転用し得るスキームであり、全国に横展開できる方式の検討を継続して行う

④ 情報共有の場の整備

- ・ 我々は昨年度事業でも結論付けたように「広く薄い」1 階建て部分(商品付帯)と「上乗せ」2 階建て部分(任意加入)を一体で提供していくような形式が適切と考えている。こうしたセキュリティ商材と一体となったサイバー保険の加入方式を普及させるための環境整備(認知度の向上、情報共有体制整備、保険設計の柔軟性、加入方式の簡便性)を進めていく。
- ・ 経済産業省との連携の下に経済 3 団体の主導により、サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)が立ち上げられたことに伴い、そちらでの情報共有体制に期待したい。

(4) 今後の課題

我々「MS&AD グループ」としては 1 階建て、2 階建て方式を基軸としつつも、その加入方式や付帯サービスの充実化を図っていくことを目指す。

中小企業向けには保険単体によるリスクソリューションの提供よりも、リスク低減や被害の縮小を実現するサービスと保険を一体型で展開していくことが重要であることを、昨年度および今年度の実証を通じて確認できた。保険代理店という販売網の構造だけ(サイバー保険のみの拡販だけ)ではなかなか普及が進まない実態も損保協会の調査等からも明らかになっている。

サイバー保険の認知度はまだまだ低く、損害保険協会での活動は活発化しているものの、損害保険業界だけでは難しい。

セキュリティ業界(セキュリティベンダー、IT ベンダー等)との協業が必要であるものの、保険会社+セキュリティ業界だけでは、中小企業の経営者へのリーチや安心感・信頼感において、もう一段の力が必要になっている。そこで経産省などの国の枠組み、商工団体などの組織的な力、あるいは今回の実証で中部電力グループが担ったように、地域の中核企業の関与が重要なラストピースになる。

6.2. まとめ

MS&AD インターリスク総研は 2019 年度に愛知県において事業請負し、約 200 社を対象に実証を行った。この実証を通じて、以下の気付きを得ることができた。

- サイバーセキュリティに関心はあるものの、対策に積極的に取り組む企業ばかりではない。
- 持続的な取り組みには、地場企業やコミュニティとの連携やサービス提供者への信頼や安心感が重要である。
- 「実証」終了後対策を継続するためには、サービスの価格設定がカギになる。

これらを踏まえて、2020 年度は次のとおりコンセプトを明確にして実証を行った。

- ① 積極的に取り組む意欲のある企業 50 社に限定して、参加を募り、
- ② 中小企業の経営層と対話可能な地場の重要インフラ企業(中部電力グループ)との協業により、
- ③ また、地域コミュニティとの連携強化により
- ④ 「実証終了後もサービスが継続利用されること」、「持続可能で全国に横展開可能なモデルが構築すること」が可能との仮説を持ち、実証を計画・実行した。

実証後に実施したアンケートやヒアリングの結果から、「サービス提供者への信頼や安心感」が得られたという声も多く、電力会社グループとの協業モデルが受け入れられ、今回の仮説が成り立つことを確認することができた。

一方、個々のサービスに関しては、「現地支援を行うリソースが必要」や「(UTM や EDR 等のセキュリティサービスにおける)レポートのわかりやすさ向上が必要」等の指摘があり、今後サービスレベルを向上させる余地を認識するとともに、具体的な改善策の検討を既に関係者で進めている。

また、実証を通して、中小企業の抱える課題が、下記 3 点に概ね集約されることが改めて確認された。

- ① コスト負担(セキュリティ対策にかかる費用に余裕がない)
- ② 製品・サービスの選定(自社の実態に即した適切な製品・サービスがわからない)
- ③ 人材確保(セキュリティ対策を担う人材がいらない)

我々が今回の実証事業で構築した「保険会社グループと地場の重要インフラ企業との協業によるサイバーセキュリティサービス提供」モデルは、中小企業でも納得感のある価格帯で(コスト面)、経産省お助け隊サービス認証(適切な製品・サービス面)も見越した管理サービス付きサイバーセキュリティサービス(人材面)を、中小企業に信頼され接点の多い重要インフラ企業が提供していくことにより、上

記の中小企業が抱える3つの課題を解消し、中小企業のサイバーセキュリティレベルを引き上げる持続可能なモデルになり得ることが確認できた。

現状では、中小企業のサイバーセキュリティ対策(サイバー保険への加入を含む)はまだ道半ばである。だからこそ「安心と安全を提供する」損害保険会社グループとして、今回の実証で大きな役割を担った中電グループのような地域インフラ企業(中核企業)や、地域コミュニティと組み、サイバー保険の提供にとどまらない役割を果たしていくことの重要性を再認識した。

今後も、中小企業へのサイバーセキュリティ対策の普及を図るため、引き続き国や関係機関等の支援を受けつつ、取り組みを強化していく。

以上