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：千葉県）

成果報告書

請負事業者：SOMPOリスクマネジメント株式会社

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

目次

1. はじめに

1.1.サマリー

本報告書は、ＳＯＭＰＯリスクマネジメント株式会社（以下「ＳＯＭＰＯリスクマネジメント」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（サイバーセキュリティお助け隊事業）（以下「本実証事業」という。）」において実施した実証内容および本実証事業の結果（アウトプット）並びに本実証事業から得られた成果（アウトカム）をとりまとめたものである。

千葉県内の中小企業 66 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。

- サイバーリスクの診断・評価
- UTM（UTM＋SOC）
- EDR
- セキュリティに関するアンケート

1.2.本報告書の目的

本実証事業は、特定地域の中小企業等を対象として、サイバーセキュリティに対する意識や対策導入状況、サイバー攻撃被害の実態等をきめ細かく把握することで、その実態に即したサービス内容や、これに必要な人材・体制などを明らかにし、中小企業等の実態に合ったサイバーセキュリティ対策を定着させていくことを目的として、持続可能なサイバーセキュリティ対策支援体制を構築するための実証を行うとともに、中小企業等におけるサイバーセキュリティの意識向上を図る施策である。

ＳＯＭＰＯリスクマネジメントでは、本実証事業の実施に当たり、我が国の中小企業等の多くが「図 1　中小企業等の実態と課題」に記載されるような課題を抱えているものと認識し、サイバーセキュリティ対策の中小企業等への定着に向けては、意識啓発のための継続的な取組を行うことが必要であり、そのための課題抽出を行う必要があるとの考え方に基づき、地域実証を通じてこうした中小企業等の意識啓発に向けた課題の実態を明らかにした上、中小企業等向けのサイバーセキュリティ対策支援サービスの在り方（保険の在り方を含む。）およびその持続可能な提供のために必要な態勢について検討してきた。

本報告書は、本実証事業に係る取組の内容および結果等を報告することを目的とし、我が国の中小企業等に向けたサイバーセキュリティ関連政策の方向性、サイバー保険を含むサイバーセキュリティ関連サービスの提供事業者が志向すべき中小企業等向けサービスの在り方・支援体制などに関する検討に資することを期待するものである。

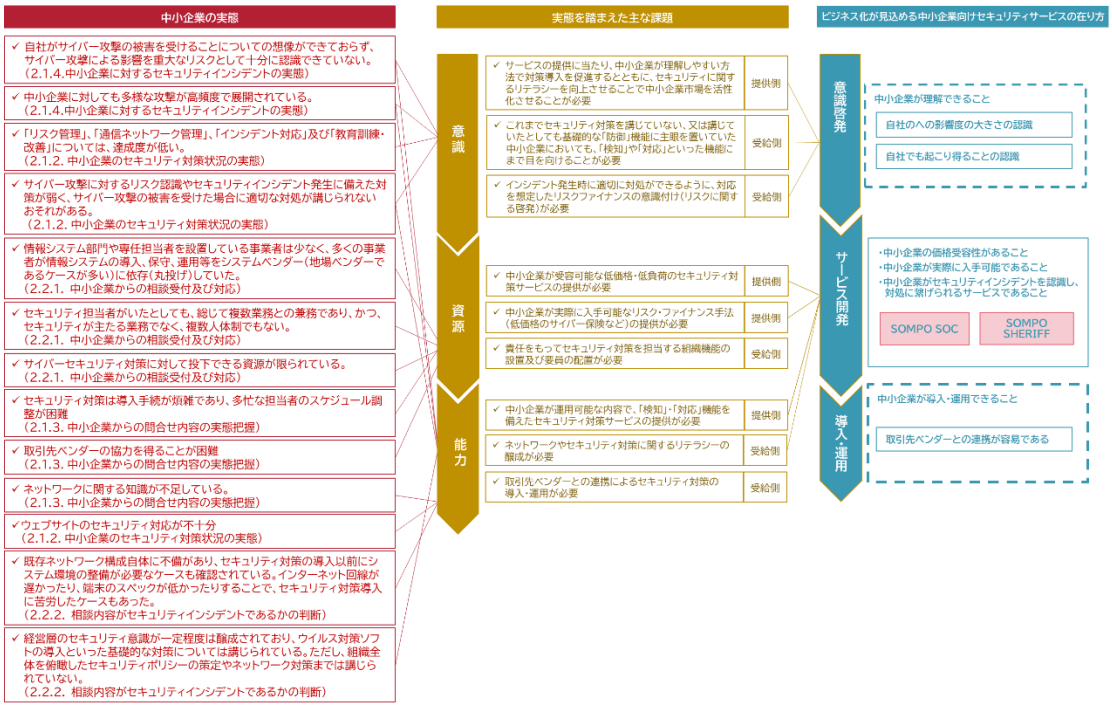

図 1　中小企業等の実態と課題

1.3.本報告書の構成

本実証事業では、「図 2　本実証事業の枠組み」に記載された枠組みに従い取組を実施してきた。本報告書は、当該枠組みに沿って、「2.実施概要」、「3.地域実証の結果」、「考察」、「5.実証結果を踏まえたビジネス化に向けた検討」および「総括」の 5 部構成とした。

「2.実施概要」では、本実証事業における取組の全体像を説明した上、事業説明会の開催概要および地域実証の概要について記載する。また、地域実証終了後のサービス提供について記載する。

「3.地域実証の結果」では、地域実証の結果として把握できた中小企業等の実態および中小企業等向け事後対応支援を実施する中で得た中小企業等向けのサイバーセキュリティ対策支援サービスの在り方を検討する上での知見などについて記載する。

「考察」では、本実証事業を通じて得られた中小企業等の実態等を踏まえ、中小企業等にサイバーセキュリティ対策を定着させていくために解決すべき課題について考察する。

「5.実証結果を踏まえたビジネス化に向けた検討」では、中小企業等向けサイバーセキュリティ対策支援サービスやサイバー保険および普及啓発の在り方について記載する。

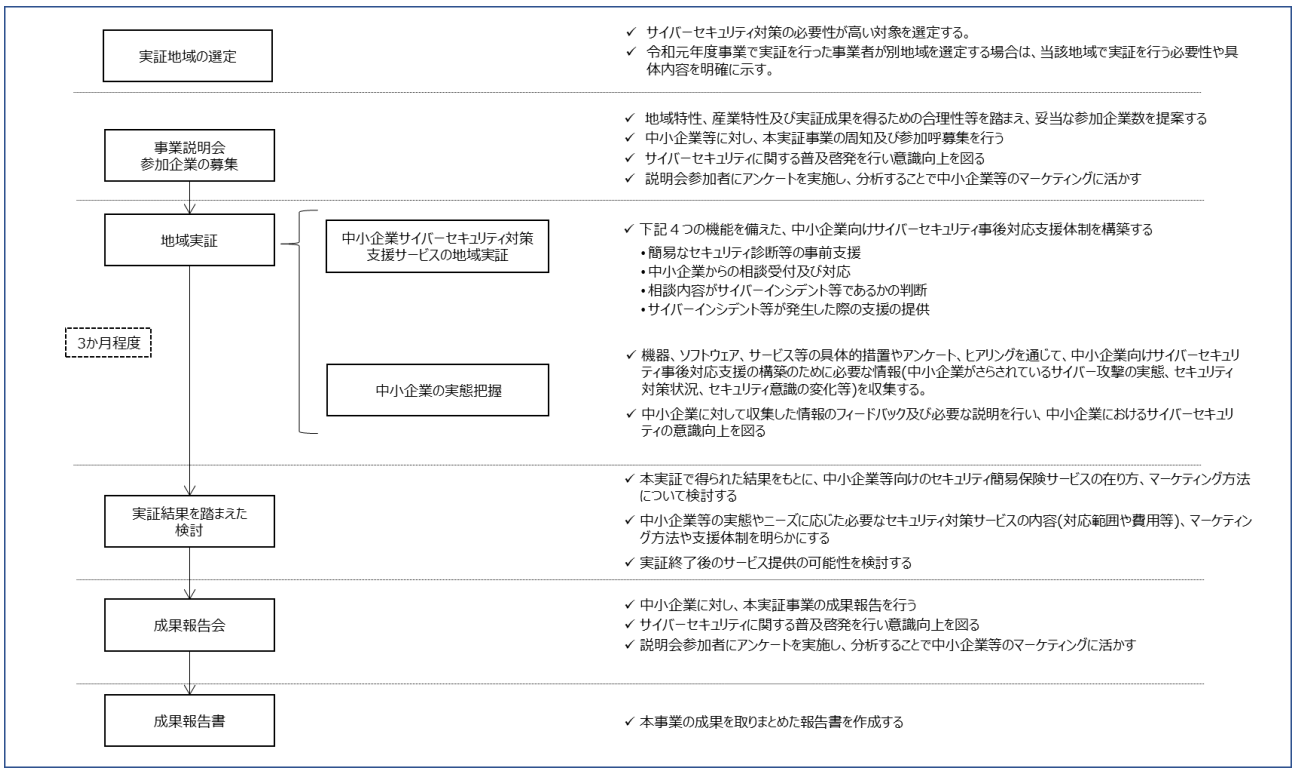

図 2　本実証事業の枠組み

2. 実施概要

2.1.全体概要

2.1.1. 本実証事業の全体像

(1) 実施地域

本実証事業の地域実証は、「千葉県」において実施した。

① 地域の選定理由および妥当性評価

千葉県には、エネルギー産業や物流業を始めとしたサプライチェーンを構成する中小企業等が集積しているだけでなく、中小製造業の生産性の向上や事業の高付加価値化を推進するための IoT 推進など、我が国全体を俯瞰した場合のバリューチェーンを構成する中小企業等も多く所在していることから、千葉県は、我が国において極めて重要性の高い産業拠点であり、また中小企業等防護の必要性の高い地域であるといえる。

ＳＯＭＰＯリスクマネジメントは、このような地域の重要性および中小企業等防護の必要性を踏まえ、地域実証の対象地域として千葉県を選定した。

なお、千葉県は、ＳＯＭＰＯリスクマネジメントを始めとする支援体制各社の通常の営業エリアであり、実行性の面からも問題はなく、本実証事業の目的にも適合していることから、地域の選定について妥当であると判断した。

② 地域の概要

ア．地理的特徴

千葉県は、首都圏の東側に位置し、東西に狭く、南北に長く外海に突出した半島になっており、南東は太平洋に面し、西は東京湾に臨んでいる。また、北西は江戸川を隔てて東京都および埼玉県に、北は利根川を隔てて茨城県に接している。地形は 200～300 メートル級の山々が続く房総丘陵と比較的平坦な下総台地、利根川流域と九十九里沿岸に広がる平野となっている。また、東、南、西の三方を海に囲まれ、その海岸線の長さは 533.5 キロメートル（平成 28 年 3 月 31 日現在）におよび、房総の海浜は、屈曲が多く天然の景勝に富んでいる。このように三方を海に囲まれた千葉県は、冬は暖かく夏は涼しい海洋性の温暖な気候で、特に、南房総沿岸は、沖合を流れる暖流（黒潮）の影響を受け、冬でもほとんど霜が降りない。降水量は夏季に多く、冬季は少なくなっている。このような比較的平坦な地形や太平洋沿岸の風速 7.5m／秒の風況の良いエリアなど再生可能エネルギーの導入に適した自然環境、京葉臨海コンビナートへの立地企業の生産活動を通じて発生する副生水素等を活用し、産業界において、環境・エネルギー分野に関する個々の取組が進んでいる。

イ．経済的特徴

千葉県の県内総生産（平成 27 年度：名目）は、約 20 兆 2,186 億円で全国第 6 位である。県内総生産額の経済活動別の構成比では、製造業が 19.0%と割合が高い。産業構造を特化係数（産業ごとの構成比を全国の構成比で除した値。特化係数が 1 を超えればその産業のウェイトが全国水準を上回っている。）で見ると、石油・石炭 製品（3.19）、鉄鋼（3.02）、電力・ガス・熱供給（2.58）、化学製品（2.37）で 2.00 を超えている。

（2） 実施期間

① 本実証事業の実施期間

2020 年（令和 2 年）9 月 7 日から 2021 年（令和 3 年）1 月 25 日まで

② 地域実証の実施期間

2020 年（令和 2 年）9 月 25 日から 2021 年（令和 3 年）12 月 25 日まで

（3） 実証参加企業数

本実証事業への参加申込企業 68 社のうち最終的に参加となった企業数：66 社

（注）参加申込後、次のいずれかの状態になったことをもって、実証へ参加したものとみなす。

①セキュリティに関するアンケートに回答し、ＳＯＭＰＯリスクマネジメントが回答を確認できた状態

②UTM を設置し、ログの取得が可能になった状態

③EDR をインストールし、ログの取得が可能になった状態

表 1 実証参加企業数の内訳

実証参加企業	66 社
セキュリティに関するアンケート	65 社
UTM サービス	59 社
EDR サービス	51 社

2.1.2. 本実証事業の実施スケジュール

下記のスケジュールで本実証事業を実施した。

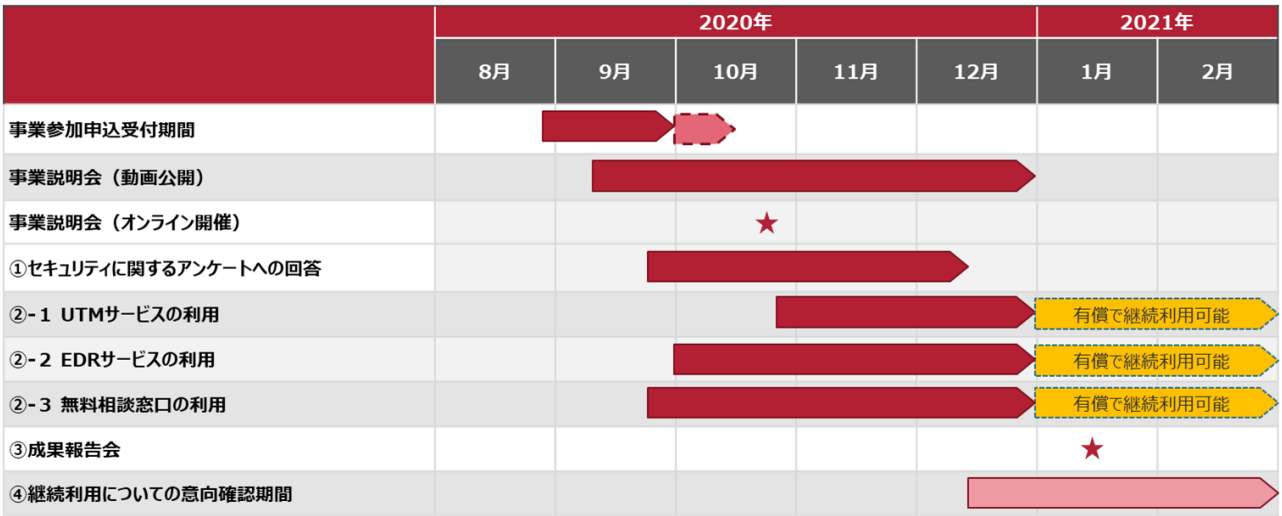

図 3 実施スケジュール（概要）

2.1.3. 本実証事業の実施体制（コンソーシアム体制）

本地域実証事業に当たり、下図に示す支援体制を構築した。

（1）コンソーシアム体制

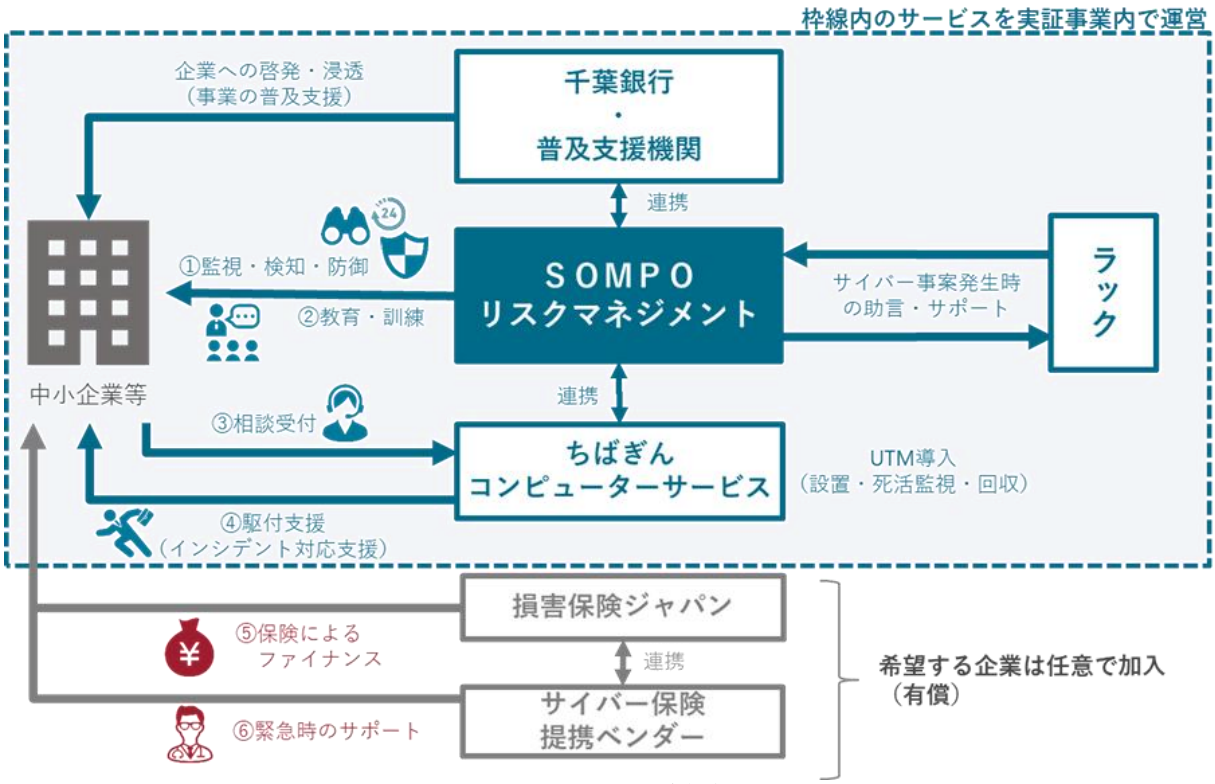

図 4　中小企業等に対する支援体制

2.2.事業説明会の実施概要

本実証事業では、千葉県に所在する中小企業等を対象に、事業説明会として、募集説明会（2020 年（令和 2 年）10 月動画公開）および「成果報告会」（2021 年（令和 3 年）1 月開催）を実施した。事業説明会のそれぞれの実施概要については、次のとおりである。

2.2.1. 募集説明会

(1) 開催内容

募集説明会は、千葉県に所在する中小企業等に対し、本実証事業の周知を図るとともに、本実証事業への参加を呼び掛けることを第一義的な目的として開催した。

① 開催日時

2020 年（令和 2 年）10 月 26 日（月） 13 時 30 分～14 時 30 分

② 開催方法

Web 会議ツール（Zoom）のウェビナー機能によるオンライン開催

③ 参加者数

4 名（4 社）

④ 議事次第

ⅰ. 開会のご挨拶（ＳＯＭＰＯリスクマネジメント）

ⅱ. 「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）

ⅲ. 「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ついて」（ＳＯＭＰＯリスクマネジメント）

ⅳ. 閉会のご挨拶（ＳＯＭＰＯリスクマネジメント）

(2) 実証参加企業確保のための取組

本実証事業の普及支援機関として、株式会社千葉銀行、ちばぎんコンピューターサービス株式会社、損害保険ジャパン株式会社千葉本部および関東経済産業局と連携し、以下の取組により中小企業等の参加を呼び掛けた。

①個社訪問による呼び掛け

169 社に対して対面で参加を呼び掛けた。

②会誌における情報発信

7,000 社を対象に会誌において本実証事業に関する情報発信を行った。

③メルマガにおける情報発信

3000 社を対象にメールマガジンにおいて本実証事業に関する情報発信を行った。

また、事業に関する情報の一元的な発信と集約による効率的な普及啓発の実現を目的として、本実証事業専用ウェブサイトを開設した。本実証事業の紹介や説明会の開催案内等の情報を掲載するとともに、説明会への申込みやアンケート調査などを、当該ウェブサイトを通じて行えるようにすることで、実証参加企業の本実証事業参加に係る負荷を軽減するよう配慮した。

(3) 募集説明会に関する追加的な取組

募集説明会に都合がつかず参加できないことにより中小企業等が実証事業への参加を断念することを防止するため、事業説明の動画を作成し、専用ウェブサイト上で公開した。

① 動画公開日

2020（令和 2 年）年 9 月 14 日（月）

② 動画収録時間

20 分 37 秒

③ 動画視聴数

195 回（2020 年（令和 2 年）12 月 25 日（金）時点）

④ 動画内容

ⅰ．事業の背景と目的
ⅱ．全体像とスケジュール
ⅲ．実施内容
ⅳ．千葉県お助け隊事業参加企業向けサイバー保険のご案内
ⅴ．参加手続きについて
ⅵ．FAQ

2.2.2. 成果報告会

(1) 開催内容

成果報告会は、地域実証を約 3 か月間実施して得られた中小企業等に向けられたサイバー攻撃の発生状況やそこから想定される損害、セキュリティに関するアンケートを通じて得られた中小企業等のセキュリティの実態などをフィードバックすることで、中小企業等におけるサイバーセキュリティの意識向上およびセキュリティ対策の定着を図ることを目的として開催した。

① 開催日時

2021 年（令和 3 年）1 月 15 日（金） 14 時 00 分～15 時 30 分

② 開催方法

Web 会議ツール（Zoom）のウェビナー機能によるオンライン開催

③ 参加者数

10 名（9 社）

④ 議事次第

ⅰ. 千葉県サイバーセキュリティお助け隊　成果報告（ＳＯＭＰＯリスクマネジメント）

- 実証事業概要（目的と背景、実施した内容、実施体制、参加者数や属性等）
- 中小企業等のサイバーセキュリティの実態（アンケート結果等）
- 中小企業等に向けられているサイバー攻撃の実態（確認されたサイバー攻撃等）
  UTM（UTM＋SOC）サービスによる観測結果
  EDR サービスサービスによる観測結果
- 中小企業等における実態についてのまとめ
- 実証結果から得られた中小企業等の実態に即したサービス、保険の活用方法
- 事後アンケート（ウェブアンケート）実施のお願い

ⅱ. 「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）

(2) 実証参加企業確保のための取組

本実証事業の普及支援機関として、株式会社千葉銀行、ちばぎんコンピューターサービス株式会社および損害保険ジャパン株式会社千葉本部と連携し、中小企業等の参加を呼び掛けた。

(3) 成果報告会に関する追加的な取組

当日の都合がつかず成果報告会に参加できない企業向けに、募集説明会と同様、成果報告動画を作成し、専用ウェブサイト上で公開した。

また、なるべく多くの実証参加企業に後続サービスの加入（サービスの継続利用）をしてもらえるように、地域実証において実際に観測されたサイバー攻撃の内容（アラート件数およびアラートが示す内容）を可能な限り平易な言葉で紹介するとともに、成果報告会に先立って、各実証参加企業に対し、個別に観測されたアラート件数などのデータをフィードバックしておくことで、中小企業等がサイバー攻撃の脅威を自分事として受け止めやすくなるように工夫した。

2.3.地域実証の実施概要

2.3.1.　実証参加企業の概況

（1）　実証参加企業の選定条件

本実証事業では、「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）事業内容（仕様書）　3. 事業概要」に記載された「中小企業等」の定義を満たす中小企業等のうち、千葉県内に事業所を設置しているものを対象として参加者を募集した。

（2）実証参加企業の構成

本実証事業に参加した中小企業等（以下「実証参加企業」という。）は、2020 年（令和 2 年）12 月 25 日時点で 66 社であった。

なお、提案書において、募集する中小企業等の数を「50 社以上とし、最終的な実証参加企業の数が 50 社から 100 社までの範囲に収まるように参加を呼び掛ける。」と定めており、実証参加企業 66 社については所期の要件を満たしている。

①　業種別構成

「日本標準産業分類」（平成 25 年（2013 年）10 月改定）の大分類による実証参加企業の内訳は、下記のとおりであった。

（実証参加企業の業種別構成：全体）

業種分類	社数
D　建設業	11
E　製造業	11
R　サービス業（他に分類されないもの）	11
H　運輸業、郵便業	8
P　医療、福祉	6
J　金融業、保険業	5
I　卸売業、小売業	4
K　不動産業、物品賃貸業	4
L　学術研究、専門・技術サービス業	2
G　情報通信業	1
N　生活関連サービス業、娯楽業	1
Q　複合サービス事業	1
T　分類不能の産業	1
総計	66

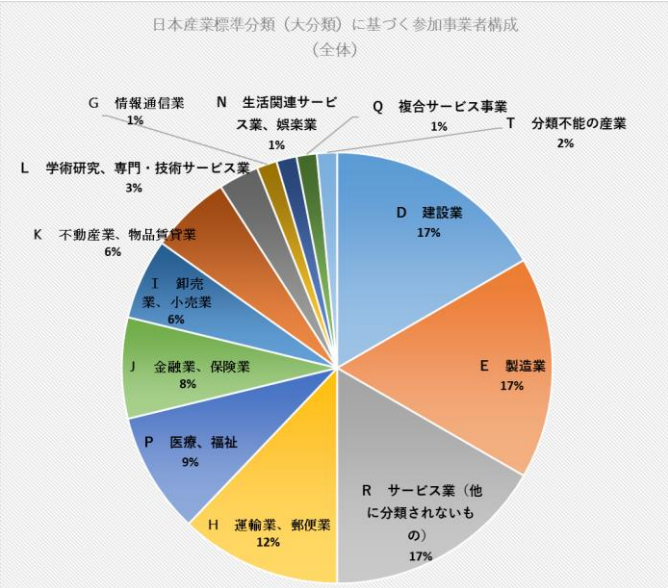

図 5　「日本標準産業分類（大分類）に基づく実証参加企業構成（全体）

（実証参加企業の業種別構成：セキュリティに関するアンケート）

業種分類	社数
E　製造業	11
R　サービス業（他に分類されないもの）	11
D　建設業	10
H　運輸業、郵便業	8
P　医療、福祉	6
J　金融業、保険業	5
I　卸売業、小売業	4
K　不動産業、物品賃貸業	4
L　学術研究、専門・技術サービス業	2
G　情報通信業	1
N　生活関連サービス業、娯楽業	1
Q　複合サービス事業	1
T　分類不能の産業	1
総計	65

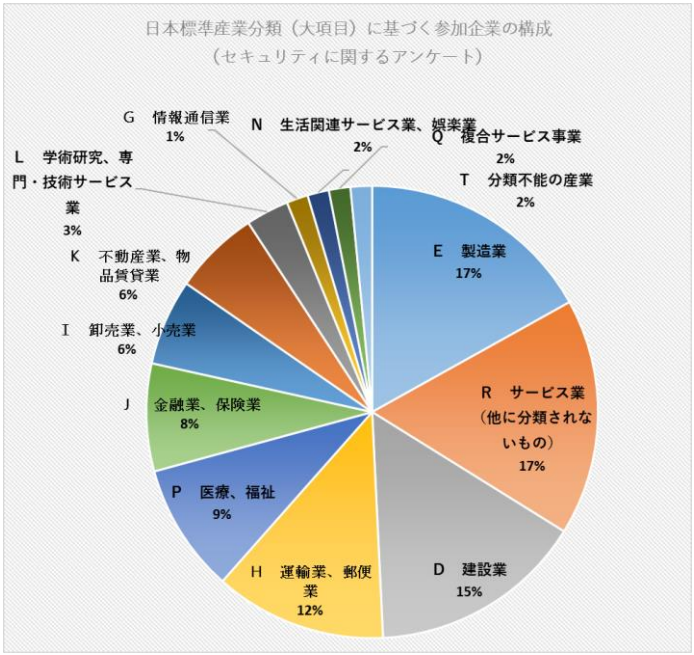

図 6　「日本標準産業分類（大分類）に基づく実証参加企業構成（セキュリティに関するアンケート）

（実証参加企業の業種別構成：UTM サービス）

業種分類	社数
D　建設業	11
E　製造業	10
H　運輸業、郵便業	8
R　サービス業（他に分類されないもの）	7
P　医療、福祉	5
I　卸売業、小売業	4
J　金融業、保険業	4
K　不動産業、物品賃貸業	4
L　学術研究、専門・技術サービス業	2
G　情報通信業	1
N　生活関連サービス業、娯楽業	1
Q　複合サービス事業	1
T　分類不能の産業	1
総計	59

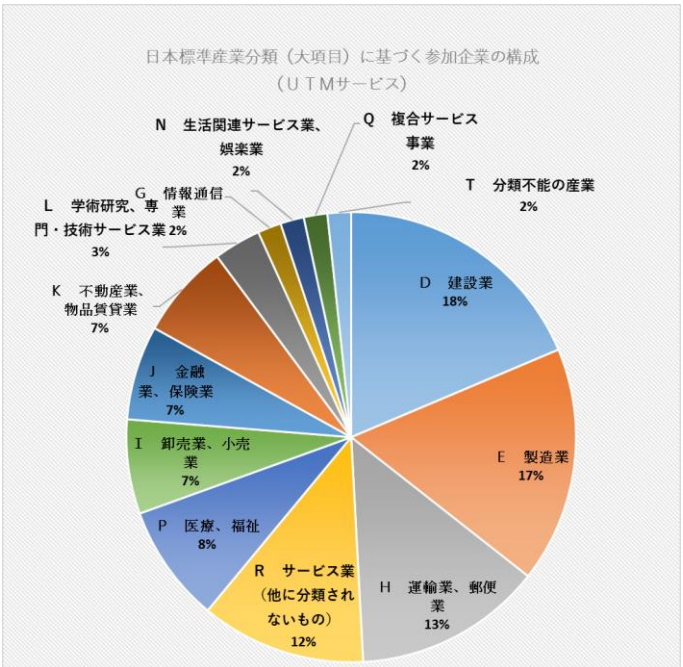

図 7　「日本標準産業分類（大分類）に基づく実証参加企業構成（UTM サービス）

（実証参加企業の業種別構成：EDR サービス）

業種分類	社数
D　建設業	10
E　製造業	10
R　サービス業（他に分類されないもの）	8
H　運輸業、郵便業	6
P　医療、福祉	5
I　卸売業、小売業	4
J　金融業、保険業	4
G　情報通信業	1
K　不動産業、物品賃貸業	1
L　学術研究、専門・技術サービス業	1
T　分類不能の産業	1
総計	51

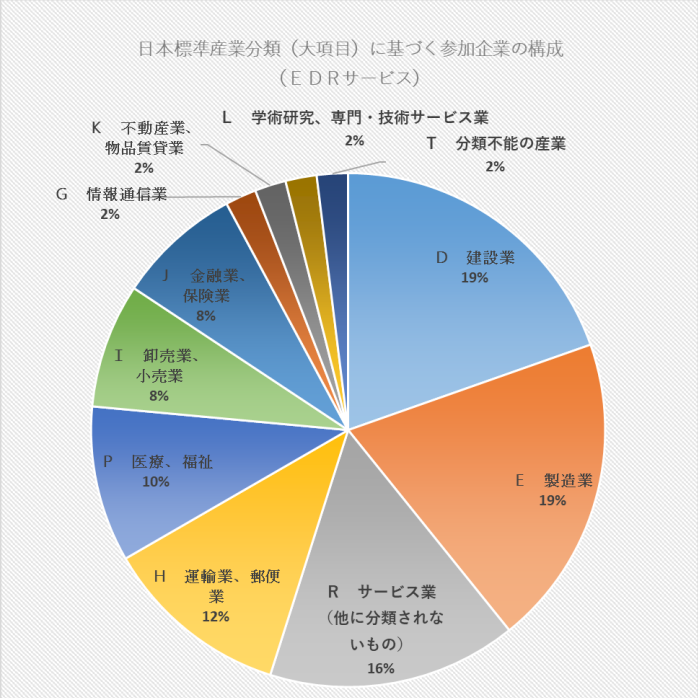

図 8　「日本標準産業分類（大分類）に基づく実証参加企業構成（EDR サービス）

② 従業員規模別構成

実証参加企業の従業員数別の内訳は、下記のとおりであった。

（実証参加企業の従業員規模別構成：全体）

従業員数　区分	社数
1～5人	7
6～10人	8
11～20人	5
21～50人	16
51～100人	11
101～200人	13
201～300人	3
301人以上	3
総計	66

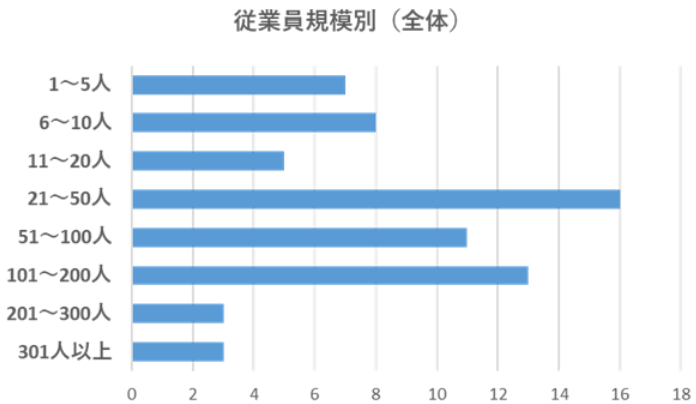

図 9　従業員規模別の実証参加企業構成（全体）

（実証参加企業の従業員規模別構成：セキュリティに関するアンケート）

従業員数区分	社数
1~5人	7
6~10人	8
11~20人	5
21~50人	16
51~100人	10
101~200人	13
201~300人	3
301人以上	3
総計	65

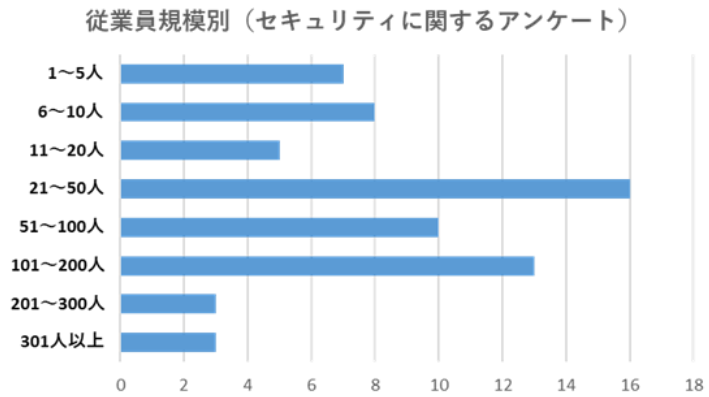

図 10　従業員規模別の実証参加企業構成（セキュリティに関するアンケート）

（実証参加企業の従業員規模別構成：UTM サービス）

従業員数区分	社数
1~5人	6
6~10人	7
11~20人	4
21~50人	16
51~100人	10
101~200人	11
201~300人	2
301人以上	3
総計	59

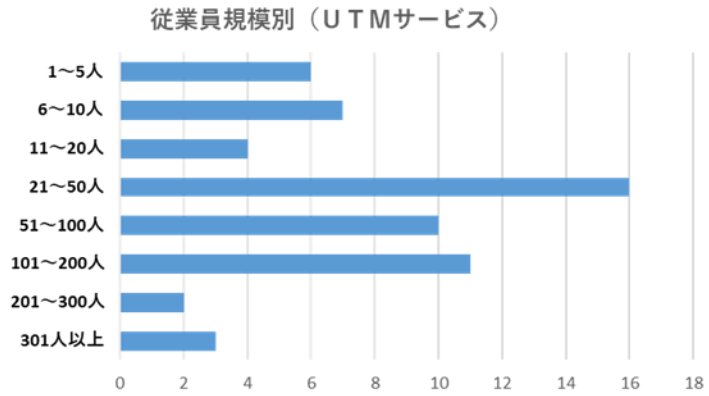

図 11　従業員規模別の実証参加企業成（UTM サービス）

（実証参加企業の従業員規模別構成：EDR サービス）

従業員数区分	社数
1~5人	5
6~10人	5
11~20人	3
21~50人	13
51~100人	8
101~200人	11
201~300人	3
301人以上	3
総計	51

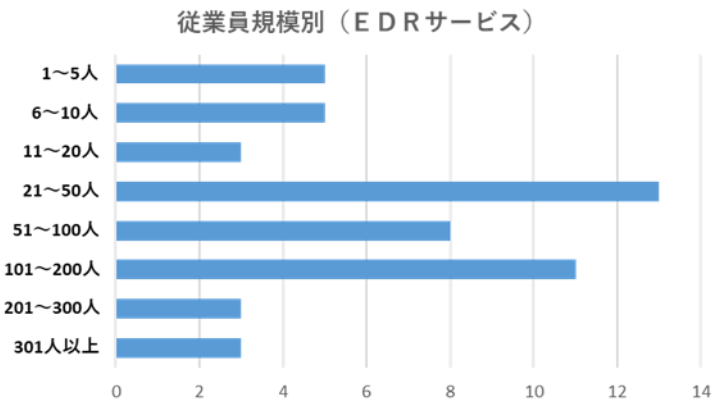

図 12　従業員規模別の実証参加企業構成（EDR サービス）

2.3.2. 中小企業等の実態把握

中小企業等向けのサイバーセキュリティ対策支援体制構築のために必要な情報（中小企業等が晒されているサイバー攻撃の実態、セキュリティ対策状況、セキュリティ意識の変化など）を収集するため、実証参加企業に対し、「サプライチェーンリスク評価サービス」、「UTM サービス」、「EDR サービス」の全ての実施・導入を行った。また、「セキュリティに関するアンケート」を実施した。

各サービスにおいて実施した内容は、次のとおりである。

(1) サプライチェーンリスク評価サービス

① サービス概要

中小企業等のウェブサイトの URL から検出できる、公開されている IP アドレスやドメインのサイバーリスクを診断・評価するものである。評価に当たっては、攻撃者が組織に侵入するための活動を独自にシミュレートした結果などを踏まえた評価基準に基づき、利用しているアプリケーションの脆弱性の有無、ソーシャルエンジニアリングへの脆弱性の有無、設定の管理不行き届きの有無などの観点から定量的に評価（スコアリング）するものである。

② 導入状況

実証参加企業 66 社のうち、自社ドメインを保有する 57 社に対し、評価を実施した。

表 2 サプライチェーンリスク評価サービスの導入状況

サプライチェーンリスク評価サービス	
実証参加企業	66 社
うち自社ドメインなし	9 社
導入企業数 （導入割合）	57 社 （86%）

③ 導入方法

対象とする中小企業等のウェブサイトの URL 情報から非侵入的に実施した。

（2）UTM（UTM＋SOC）サービス

① サービス概要

実証参加企業に対してネットワークセキュリティ機器（ＳＯＭＰＯリスクマネジメントから提供する機器はウォッチガード・テクノロジー・ジャパン株式会社[1] の UTM[2] 「Firebox シリーズ Basic Security ライセンス」を使用した。既設の機器を使用していた中小企業等については、当該機器を活用した。以下「UTM」という。）を設置し、UTM のセンサー（ファイアウォール機能、IPS 機能、ウェブフィルタリング機能、スパムフィルタ機能およびアンチウイルス機能）により各セキュリティインシデントを検出する。あわせて、Syslog サーバーを設置し UTM センサーからのアラートに係るログのうちファイアウォール機能および IPS 機能に係るログデータをＳＯＭＰＯリスクマネジメントの「セキュリティログ自動分析システム」に送信し分析し、中小企業等におけるセキュリティインシデントを影響度合いや再現性を考慮した 3 段階（「High」、「Medium」、「Low」）のランク付けを行い可視化するものである。

なお、既設の UTM を使用した中小企業等においては、いずれもスパムフィルタ機能とアンチウイルス機能を有効として設定されていなかったため、当該機能についてはデータを取得していない。

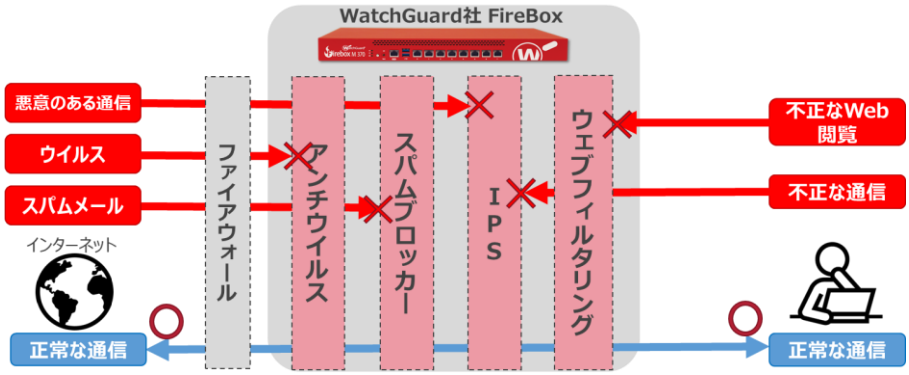

図 13　UTM の機能概要

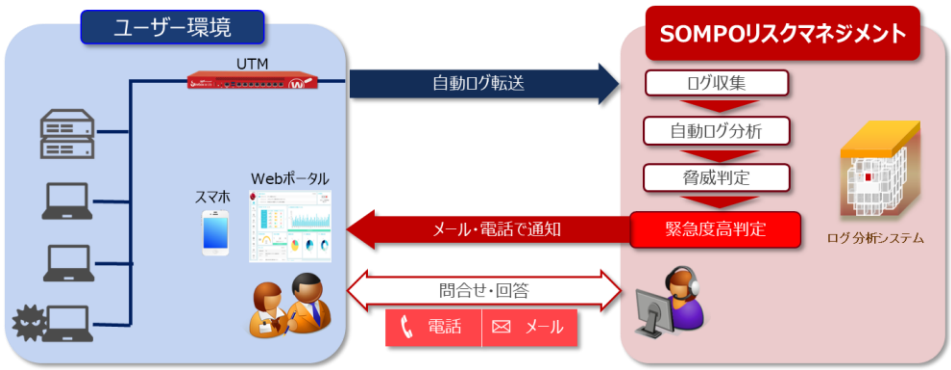

図 14　SOC サービスのサービス概念図

[1] ウォッチガード・テクノロジー・ジャパン株式会社：https://www.watchguard.co.jp/（2021 年 1 月 19 日参照）.

[2] UTM（Unified Threat Management）：様々なネットワークセキュリティ機能を統合した統合脅威管理機器

② 導入方法

UTM および Syslog サーバーの導入については、ちばぎんコンピューターサービス株式会社が事前のキッティング並びにオンサイトでのネットワーク環境確認、設置および動作確認を実施することにより、中小企業等における受入れが円滑に進められるように取り計らった。

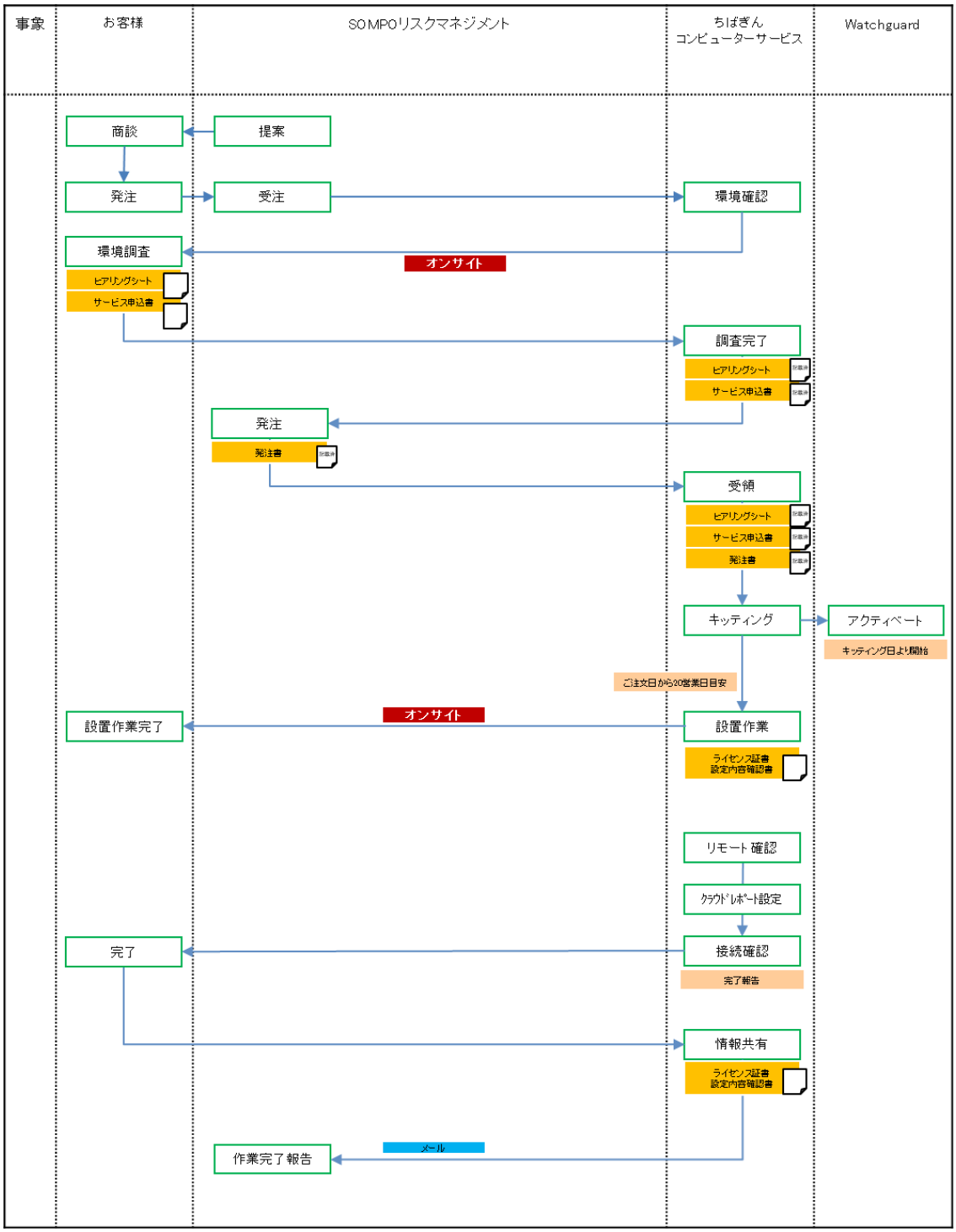

図 15　UTM（UTM＋SOC）サービスの導入フロー

③ 導入状況

UTM サービスは参加申込企業 68 社に導入を提案し、最終的に 59 社への導入を行った。

表 3　UTM サービスの導入状況

UTM サービス	
提案企業数	68 社
うち、導入不可・中止	9 社
導入完了企業数 （導入割合）	59 社 （87%）

(3)　EDR サービス

① サービス概要

ＳＯＭＰＯリスクマネジメントが提供するエンドポイントセキュリティ対策ソフトウェア（以下「EDR」という。）を用いてパソコンの挙動ログを収集し、ＳＯＭＰＯリスクマネジメントのセキュリティエンジニアが分析することで、不正プログラムの感染などのセキュリティインシデントを検出するものである。

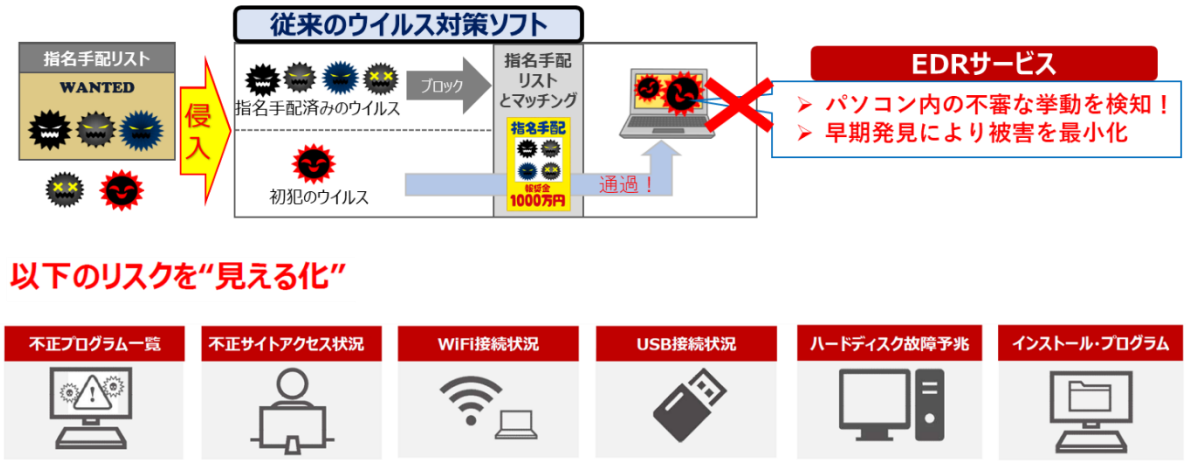

図 16　EDR サービスのサービス概念図

② 導入方法

実証参加企業に対し、EDR のインストーラーを作成・提供し、実証参加企業自身で導入した。

③ 導入状況

EDR サービスは参加申込企業 68 社に導入を提案し、最終的に 51 社への導入を行った。なお、導入台数は全体で 492 台であり、1 社当たりでは 9.6 台であった。

表 4　パソコン監視分析サービスの導入状況

EDR サービス	
提案企業数	68 社
うち、導入不可・中止	17 社
導入完了企業数 （導入割合）	51 社 （75%）

(4)　セキュリティに関するアンケート

① 概要

実証参加企業のセキュリティ対策の導入状況やセキュリティに対する意識等について把握するため、セキュリティに関するアンケートを行った。アンケート項目には、SECURITY ACTION の一つ星の宣言条件である「情報セキュリティ 5 か条」について確認する項目や、サイバーリスクに関するシナリオに基づく想定損害額を算出するための項目を含めるなど、中小企業等に分かりやすくフィードバックするための項目を含む内容で実施した。

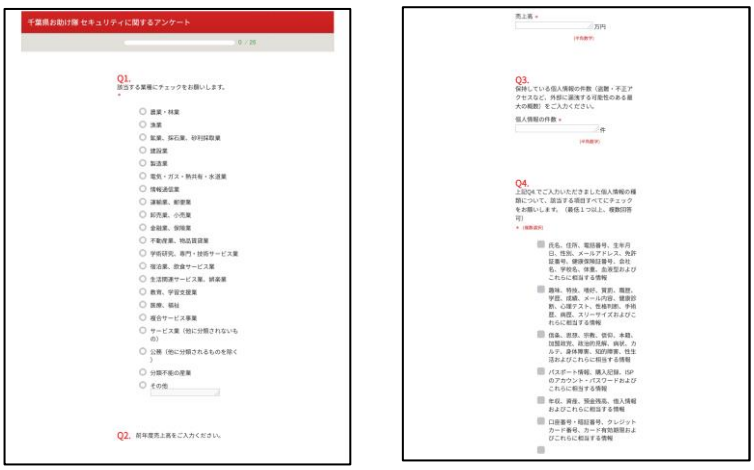

図 17　セキュリティに関するアンケート（ウェブサイトの回答ページ）のイメージ

② 実施方法

専用ウェブサイト上に回答ページを開設し、募集説明会参加後または募集説明会動画視聴後（以下「事前アンケート」という）および成果報告会参加後または成果報告会動画視聴後（以下「事後アンケート」という）に回答するよう誘導した。

③ 実施状況

ア．事前アンケート

実証参加申込企業 68 社に対して実施を提案し、最終的に 65 社から回答を得た。

表 5　セキュリティに関する事前アンケートの実施状況

セキュリティに関する事前アンケート	
提案企業数	68 社
うち、回答不可、中止	3 社
実施完了企業数 （実施割合）	65 社 （96%）

イ．事後アンケート

実証参加企業 66 社に対して実施を提案し、1 月 25 日時点で 12 社から回答を得た。

表 6　セキュリティに関する事後アンケートの実施状況

セキュリティに関する事後アンケート	
提案企業数	66 社
うち、未回答	54 社
実施完了企業数 （導入割合）	12 社 （18%）

④ 実施結果

実施結果は後述の「中小企業等の実態把握　アンケート・ヒアリングによる支援体制構築に必要な情報の収集」に記載している。

2.3.3. 事後対応支援体制の構築および支援の実施

(1) 相談受付・駆付け支援サービスの実施

実証参加企業からの相談を受け付けて適切な対処に誘導するために、相談窓口となるコールセンターを設置した。コールセンターの開設時間は、一般的な中小企業等の営業時間帯や中小企業等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 時までとした。

相談受付内容については、IT やサイバーセキュリティに関する中小企業等の知識が乏しいと想定していることから、セキュリティインシデントであることが特定された事象に限定せず、そのおそれのある事象についても幅広く対象とした（例えば、「原因は分からないが、PC の調子が悪い。」といったサイバー攻撃を受けている可能性が窺えるような相談を含む）。

なお、電話番号については、実証開始企業が電話料金を気にせずに相談できるように、専用フリーダイヤル（0120-3 1 8（サイバークイックゴー） 995 ）を用意した。

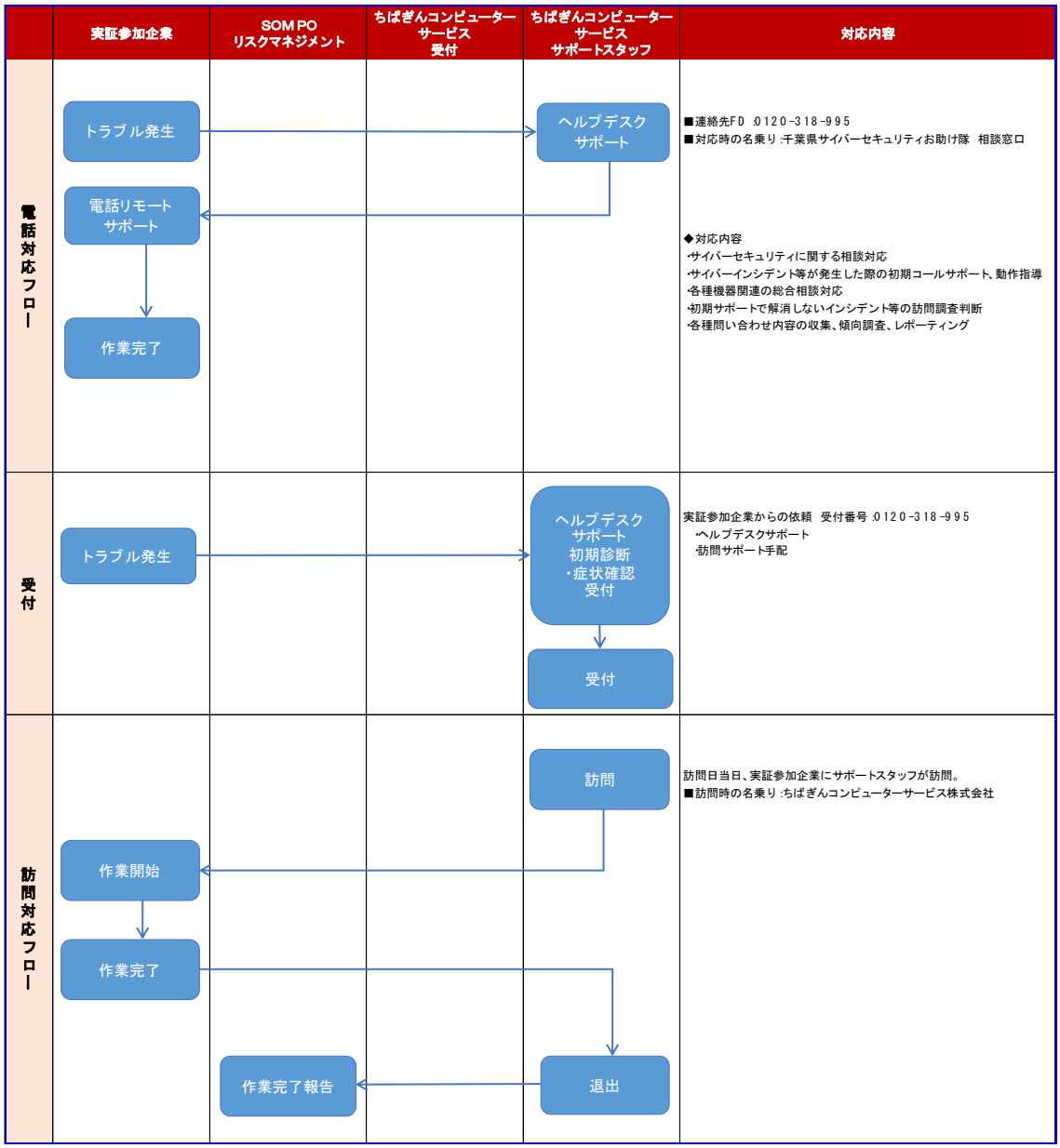

図 18 相談受付・駆付け支援サービスの運用フロー

(2) インシデント対応の実施

① 相談内容がセキュリティインシデントであるかの判断

相談内容がセキュリティインシデントであるかを判別するために、中小企業等のセキュリティインシデントに関する監視および検出を行い、これらの情報を収集した上、相談内容と突き合わせて情報処理安全確保支援士を含むＳＯＭＰＯリスクマネジメントスタッフが総合的に分析する体制を構築した。

「(2) UTM（UTM＋SOC）サービス」では、土日祝日を含む 24 時間対応の管理により検出されたセキュリティインシデントに対し、「セキュリティログ自動分析システム」によって、影響度合いや再現性を考慮した 3 段階（「High」、「Medium」、「Low」）のランク付けを行った上で、アラートメールを実証参加企業の担当者に対して発出し、セキュリティインシデントの詳細情報と推奨する対応を助言する仕組みを構築した。

「(3) EDR サービス」では、実証参加企業の使用するパソコン（エンドポイント端末）にインストールした EDR が収集した挙動ログを分析し、脅威ファイル（不正プログラム）および被疑ファイル（不正プログラムである疑いのあるプログラム）の特定を行った上で、アラートメールを実証参加企業の担当者に対して発出し、セキュリティインシデントの詳細情報と推奨する対応を助言する仕組みを構築した。

② セキュリティインシデント等が発生した際の支援の提供

前記「(1) 相談受付・駆付け支援サービスの実施」または「(2) インシデント対応の実施 ① 相談内容がセキュリティインシデントであるかの判断」に記載された取組を通じて、実証参加企業からセキュリティインシデントもしくはそのおそれ（以下「セキュリティインシデント等」という。）に関する支援要請を受けた場合またはＳＯＭＰＯリスクマネジメントが支援の必要があると判断した場合には、情報処理安全確保支援士を含むＳＯＭＰＯリスクマネジメントスタッフが電話または駆け付けによるセキュリティインシデント等への対処支援を行った。当該対処支援の提供時間帯は、一般的な中小企業等の営業時間帯や中小企業等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 時までとした。

なお、本機能は、中小企業等において求められる、セキュリティインシデント等の発生時の適切な対処支援の在り方（中小企業等向け簡易保険サービスの在り方を含む。）について検討するための実態把握を目的とし、フォレンジック調査費用、障害復旧費用、パソコン買換費用、第三者への損害賠償金などのインシデント等への対処費用自体を本実証事業の予算から支出（肩代わり）することは原則として行わないこととした。ただし、中小企業等が利用しやすいセキュリティサービスや簡易保険サービスの在り方を検討するための補完的な情報（サービス利用料金、保険料の値ごろ感、支払保険金の傾向など）を得ることおよびセキュリティインシデント等の発生後に円滑な対処支援を行うことにより実証開始企業が安心して地域実証に参加できる仕組みを構築することを目的として、検知した不正プログラムの駆除対応等のサービスを状況に応じて提供することとした。

2.4.地域実証終了後のサービス提供

実証参加企業のうち、地域実証終了後に同様のサービスの継続利用を希望する者に対しては、ＳＯＭＰＯリスクマネジメントが昨年度の実証事業を通じて得た知見などに基づき開発した SOMPO SOC および SOMPO SHERIFF を有償提供する。実証参加企業に対しては、2020 年（令和 2 年）12 月から翌年 1 月に掛けて個別に地域実証結果のフィードバックおよび後続サービスの案内を行うとともに、成果報告会においても実証参加企業に対して後続サービスの案内を行った。

2021 年（令和 3 年）1 月 25 日現在、SOMPO SOC（UTM＋SOC サービス）については 10 社（検討中 8 社）から後続サービスの利用意思を確認し SOMPO SHERIFF（EDR サービス）については 5 社から利用検討の意向を確認している。

なお、上記サービスの概要については、「実証結果を踏まえたビジネス化に向けた検討 実証終了後に後続サービスとして提供するサービス」に記載する。

3. 地域実証の結果

3.1.中小企業等の実態把握

本実証事業では、地域実証後に自立的なサービス展開に繋げるための情報を収集することを目的として、普及支援機関である株式会社千葉銀行、ちばぎんコンピューターサービス株式会社および損害保険ジャパン株式会社のチャネルを通じ、提案したサービス内容に対して興味を抱いた、または本実証事業の趣旨に賛同した中小企業等に対する通常の営業手法に近い形での募集を行った。実証参加企業の属性については「実施概要地域実証の実施概要 2.3.1. 実証参加企業の概況（2）実証参加企業の構成」に示すとおり、特定業種への偏りは少なく、対象業種は広範にわたっている。

なお、千葉県内の中小企業の数は、120,789 社（2016 年（平成 28 年）6 月現在）[3]であり、実証開始企業からの回答率（データ取得率）が 95%である場合、許容誤差 10%・信頼度 95%に必要なサンプル数は 19 社[4]であるため、実態把握を行う上での企業数は確保できており、本実証事業において把握した実証参加企業の実態については、千葉県内の中小企業等の実態を表したものとして評価できるものと考える。

3.1.1. アンケート・ヒアリングによる支援体制構築に必要な情報の収集

サイバー攻撃を受けた際の状況、自覚の有無、サイバーセキュリティに係る体制整備や導入しているセキュリティ対策の状況、セキュリティへの意識とその変化などを把握するため、中小企業等に対しセキュリティに関するアンケートを実施した。なお、アンケートおよびヒアリングで確認する内容は千葉県の有力企業である千葉銀行グループとの意見交換を実施したうえで策定した。アンケートはウェブアンケート方式にて事前アンケートと事後アンケートを実施した。

また、UTM サービス導入のための現地調査の際に簡単なヒアリングを行い、ネットワーク構成図を作成した。

（1）中小企業等のセキュリティに対する意識の実態

中小企業等のセキュリティに対する意識の実態を把握するために、次の質問項目についてアンケートで確認した。

[3] 中小企業庁ホームページ「都道府県・大都市別企業数、常用雇用者数、従業者数（民営、非一次産業、2016 年）」

[4] N＝母集団の個数、p＝回答率、 k＝を正規分布による信頼度（95%）における定数（1．96）、L＝許容誤差（5%）とする場合に必要となる標本数 n を下記数式によって求めた。なお、許容誤差 10%の場合は、n＝19 社。

$$n = \frac{N}{\frac{N-1}{p(1-p)}\left(\frac{L}{2k}\right)^2 + 1}$$

① 「SECURITY ACTION」の宣言状況

実証参加企業のセキュリティに対する意識の現状を把握するため、セキュリティへの取組の自己宣制度である「SECURITY ACTION」の宣言状況を事前アンケートにおいて確認した。また、本実証事業においては、実証参加企業に対し説明会や各種案内の際に「SECURITY ACTION」制度の紹介および宣言の推奨を行い、実証参加を通じたセキュリティ意識の変化を把握するため実証終了時点（2020 年（令和 2 年）12 月 25 日）での宣言状況を確認した。宣言社数推移は下表のとおりであり、本実証事業を通じてのセキュリティ意識の啓発について一定の効果が認められたものと考える。

表 7　実証参加企業の SECURITY ACUTION 宣言状況（実証参加時）

SECURITY ACTION を宣言していますか（n＝65）	
一つ星を宣言している	2 社
二つ星を宣言している	0 社
宣言していないがこれを機に宣言してみたい	29 社
宣言しておらず今後も宣言してみたいと思わない	30 社
よく分からない・不明	4 社

表 8　SECURITY ACUTION 宣言企業数の推移

	実証開始時	実証終了時	増分
一つ星	2 社	7 社	＋5 社
二つ星	0 社	1 社	＋1 社
合計	2 社	8 社	＋6 社

② IPA「情報セキュリティ 5 か条」の実施状況について

セキュリティ意識の把握および「SECURITY ACTION」の普及促進に繋げることを目的として、IPA の「情報セキュリティ 5 か条」の実施状況も事前アンケートにおいて確認した。結果は以下のとおりで、社内での情報共有の仕組みの構築ができていないことが推察される。

パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態 にしていますか？(n=65)		パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義 ファイルは最新の状態にしていますか？(n=65)		パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？(n=65)		重要情報に対する適切なアクセス制限を行っていますか？(n=65)		新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？(n=65)	
実施している	32	実施している	42	実施している	14	実施している	18	できている	9
一部実施している	27	一部実施している	17	一部実施している	31	一部実施している	31	一部できている	23
実施していない	3	実施していない	2	実施していない	14	実施していない	14	できていない	30
わからない	3	わからない	4	わからない	6	わからない	2	わからない	3

図 19　情報セキュリティ 5 か条の実施状況

② セキュリティ対策を強化するきっかけとなる事由について

中小企業等の意識啓発に効果的な要素を把握するため、自社がセキュリティ対策を強化するきっかけとなる事由について事前アンケートにおいて確認した。回答結果および結果から推測される内容は、以下のとおり。

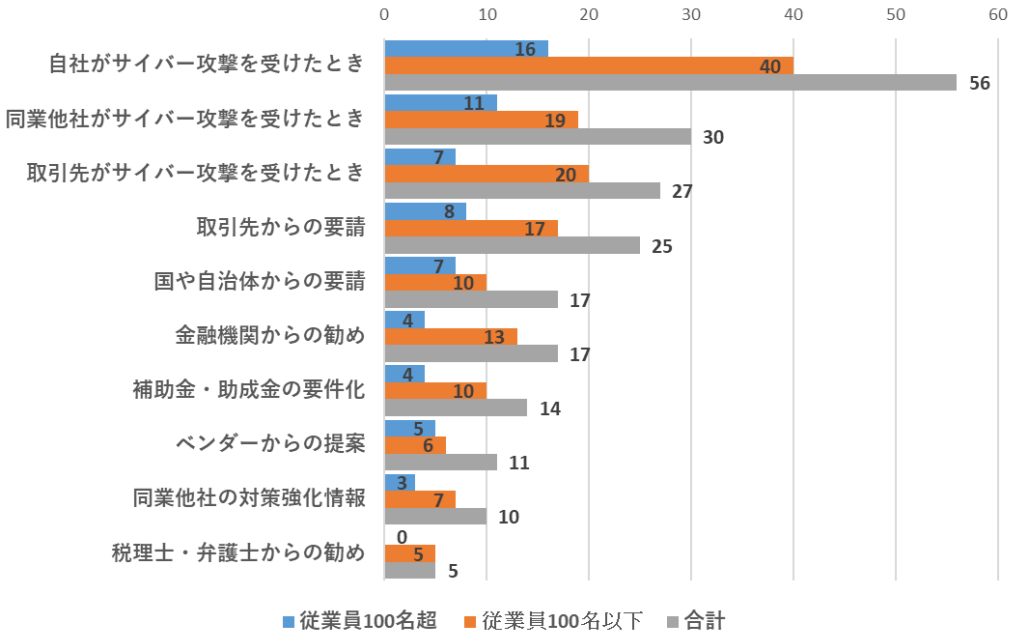

図 20　自社でセキュリティ対策を強化するきっかけになるとしたら何が考えられますか？（複数回答可）

ア．自社や自社と関係のある主体がサイバー攻撃を受けることが最もセキュリティ意識に影響する

トップ 3 がいずれも「サイバー攻撃が発現したとき」であったことから、千葉県の中小企業等においては、自社や自社と関係性のある主体が実際にサイバー攻撃を受けた場合にセキュリティが最も意識されることが推測できる。

イ．第三者からの要請については幅広い主体からの要請が受け入れられている

第三者からの要請に関する項目では、最も多く回答があったのは「取引先からの要請」であった。一方、「国や自治体からの要請」、「金融機関からの勧め」および「ベンダーからの提案」についても 2 割前後の回答があったことから、千葉県の中小企業等においては、要請に直接的な圧力が生じる取引先だけでなく、国・地方自治体、金融機関、ベンダー等からの働き掛けについても一定の効果が期待できるものと考えられる。

③ 自社へのサイバー攻撃を認識したことがあるか

「サイバー攻撃を受けた経験」の有無についても事前アンケートにおいて確認した。回答結果は下表のとおりであった。セキュリティを意識する重要な事由であるとの回答が多い一方で、自社がサイバー攻撃を受けたことがあると認識している企業は約 10%と少数であることから、実証参加時点においてセキュリティ対策の強化のきっかけを実際に得ている企業が多くないことが窺える。

表 9　自社へのサイバー攻撃を認識したことがあるかの回答状況

自社へのサイバー攻撃を認識したことはありますか？（n＝65）	
ある	7 社
Emotet、なりすましをされた	4 件
スパムメールを受信した	2 件
ランサムウェアに感染した	1 件
ない	58 社

④ セキュリティ対策実施の要請を受けたことがあるか

中小企業等がセキュリティを意識する事由として考えられる「第三者からの要請」について、「実際に経験したことがあるか」および「（経験がある場合は）どのような主体からの要請等であったか」を事前アンケートにおいて確認した。

要請を受けたことがある企業は全体の約 14%の 9 社と少数であり、要請主体は金融機関・保険会社、ベンダー・出入り業者であった。第三者からの要請は中小企業等がセキュリティ対策を意識する有力な事由であると考えられるが実際にはあまり行われておらず、こうした主体への働きかけることにより要請を促すことが中小企業等の意識啓発に向けては効果的と考えられる。

表 10　セキュリティ対策実施要請を受けたことがあるかの回答状況

これまでに取引先などからセキュリティ対策実施の要求を受けたことがありますか？（n＝65）	
ある	9 社
金融機関・保険会社からの要請	4 社
ベンダー・出入り業者からの要請	3 社
取引先からの要請	1 社
回答不可	1 社
ない	41 社
把握していない	15 社

⑤ サイバー攻撃による被害で事業中断と情報漏えいのどちらにリスクを感じているか

中小企業等の意識啓発に盛り込むべきコンテンツを把握するため、サイバー攻撃により引き起こされる被害のうち、情報漏えいと事業中断のどちらの方がよりリスクを感じているのかを事前アンケートにおいて確認した。回答結果は、下表のとおりであった。

「事業中断と情報漏えいの両方」との回答が約 70%と最も多くなったものの、「事業中断」と回答した企業よりも「情報漏えい」と回答した企業の方が多く、「サイバー攻撃による被害＝情報漏えい」と認識している企業も少なからず存在していることが確認できた。

表 11　サイバー攻撃による被害で事業中断と情報漏えいのどちらをおそれているかの回答状況

自社にとってサイバー攻撃を受けたことにより引き起こされるどんな事態が怖いですか？（n＝65）	
事業中断	4 社
情報漏えい	14 社
情報漏えい・事業中断の両方	46 社
無回答	1 社

⑥ 自社がサイバー攻撃の被害を受けると思うか

実証参加を通じてのセキュリティ意識の変化を確認するための指標とするため、「自社がサイバー攻撃による被害を受けると思うか」について、事前アンケートおよび事後アンケートの両方で確認した。回答結果は下表のとおりであった。

攻撃を受ける可能性があると回答した企業の割合が増えていることおよびよく分からないと回答した企業の割合が減っていることから、実証を通じた意識啓発は一定の効果があったといえる。

表 12　自社がサイバー攻撃の被害を受ける可能性があると思うかの回答状況

自社がサイバー攻撃の被害を受ける可能性があると思いますか（n＝65、12）			
	実証開始時	実証後	増減
可能性は十分にあると思う	21 社（32%）	4 社（33%）	+1%
可能性は低いがあり得るとは思う	31 社（48%）	7 社（58%）	+10%
受けないと思う	4 社（6%）	1 社（8%）	+2%
よく分からない	9 社（14%）	0 社	-14%

⑦ 自社がセキュリティ対策を進める上で課題と感じていることはあるか

セキュリティ対策を進める上で課題についての認識状況についても事後アンケートにおいて確認した。

課題を認識しているという回答のうち、「会社全体の危機意識」について課題があるとの回答が最も多く全体の 3 割を占める結果となった。

表 13　自社がセキュリティ対策を進める上での課題認識についての回答状況

自社がセキュリティ対策を進める上での課題があれば教えてください（n＝12）	
会社全体での危機意識	4 社
社内教育ができていない	1 社
対策に掛ける予算の確保	1 社
拠点が全国に点在していることによる管理・対応の負荷	1 社
課題はない	5 社

(2) 中小企業等のセキュリティ対策状況の実態

中小企業等のセキュリティ対策の導入状況を把握するため、次の質問項目について事前アンケートで確認した。

① セキュリティ対策の導入状況

代表的なセキュリティ対策についての導入状況を確認した。

最も導入が進んでいたのはウイルス対策ソフトであり、全体の約 92%が「導入している」と回答した。また、データのバックアップ（40%）や UTM（約 34%）、ファイアウォール（約 31%）についても一定の導入が進んでいることが分かった。データのバックアップについては、近年ランサムウェアによる被害がクローズアップされたこともあり、中小企業等においても導入が進んでいると考えられる。

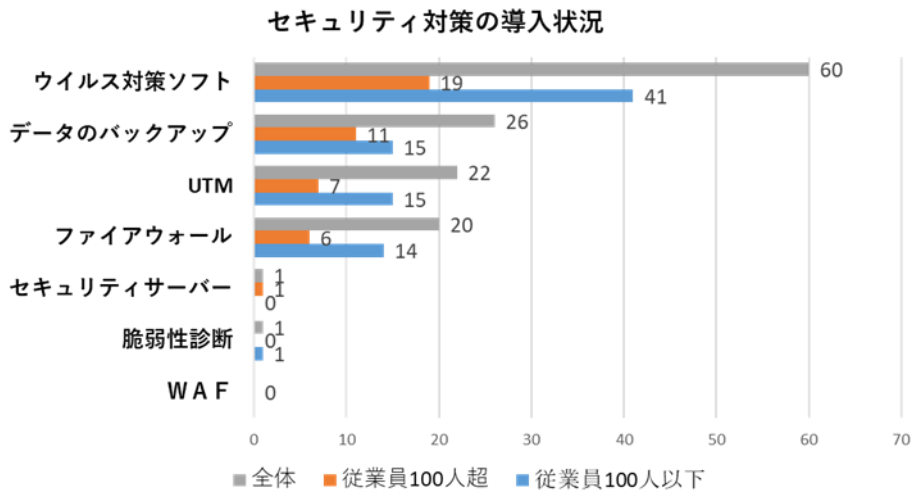

図 21　現在自社で導入済のセキュリティ対策に関する回答状況（複数回答可、n＝65）

② 現在セキュリティ対策に掛けている年間費用

中小企業等が利用しやすいサービス価格の検討の参考にするため、現在セキュリティ対策に掛けている年間費用についても確認した。

セキュリティに関するアンケートに回答した 65 社のうち、費用について回答があったのは 41 社（約 63%）で、残りの 24 社は「把握していない」との回答であった。このことは、中小企業等において自社の情報資産の把握・管理ができていないという実態を示唆している。

年間費用は 41 社の平均値は 895,249 円、中央値は 200,000 円であった。企業規模の幅が広く、回答された費用についてもばらつきが見られた。平均値については一部の高額な回答により実態よりも高めになっていることから、中央値の 200,000 円の方がより中小企業等の実態を表していると推測される。

従業員数による規模別で見ると、従業員 100 人以下では年間 12 万円以下が、従業員 100 人超では年間 50 万円以下が最も多い結果となった。

表 14　セキュリティ対策に掛けている年間費用（回答があった 41 社に関する統計）

セキュリティ対策に掛けている年間費用	
平均値	895,249 円
中間値	200,000 円

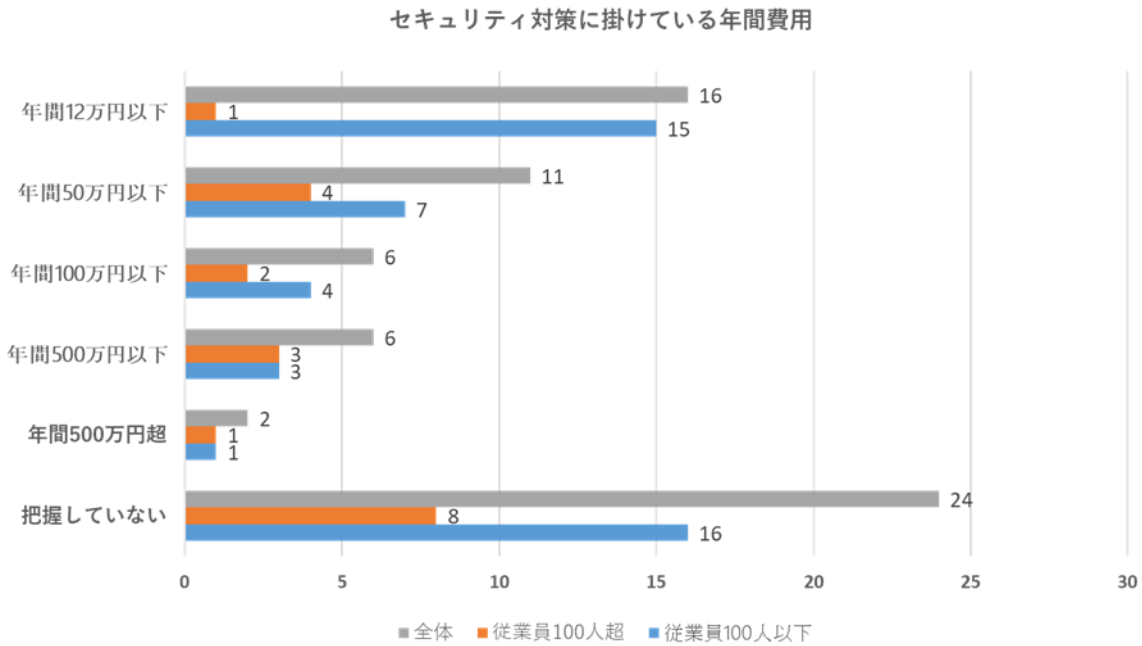

図 22　現在自社でセキュリティ対策に掛けている年間費用に関する回答状況（n＝65）

(3) 中小企業等のセキュリティに関する体制整備状況の実態

中小企業等におけるセキュリティに関する体制整備状況を確認するため、次の質問項目について事前アンケートで確認した。

① セキュリティの専任者がいるか

セキュリティに関する体制整備の状況として、「セキュリティ担当者の有無」について確認した。

「専任者がいる」と回答したのは全体で 5 社（約 8%）と少数だが、兼務担当者も含めると 49 社（約 75%）であり、セキュリティに関する体制については一定程度整備されていることが分かった。一方、「担当者がいない」との回答が 16 社（約 25%）と高いことは、「アンケート・ヒアリングによる支援体制構築に必要な情報の収集　(2) 中小企業等のセキュリティ対策状況の実態 ② 現在セキュリティ対策に掛けている年間費用」において示唆された、「自社の情報資産についての把握・管理ができていない」という実態に関連していると考えられる。

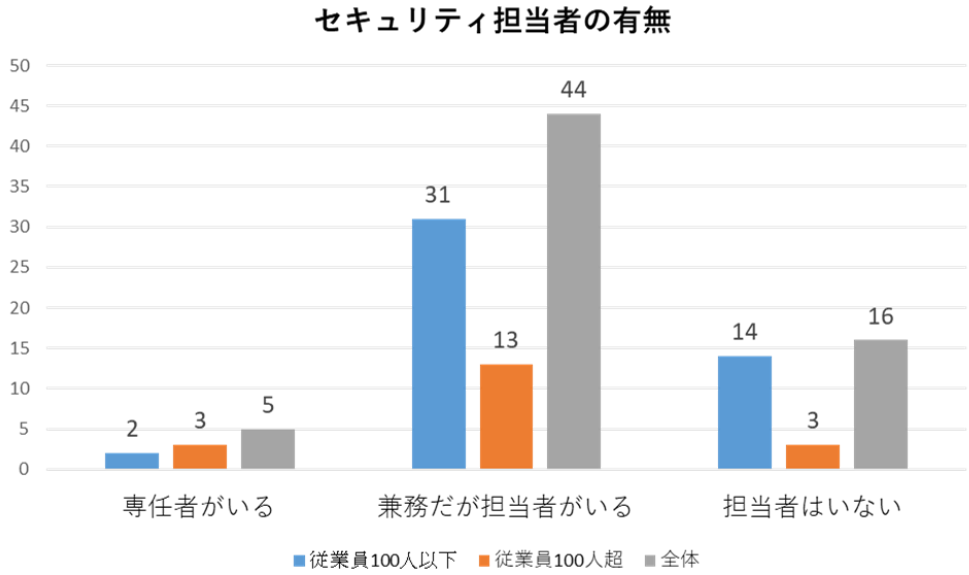

図 23　セキュリティ担当者の有無に関する回答状況（n＝65）

(4) テレワーク・在宅勤務に関する状況

中小企業等の実態に即したサービス内容の検討に活用するため、今後、中小企業等においても導入・利用が不可欠になると考えられるリモートワーク・在宅勤務の導入状況等を事前アンケートにおいて確認した。

① テレワーク・在宅勤務の実施状況

テレワーク・在宅勤務を実施しているかについては、65 社のうち 19 社（約 29%）が実施していると回答した。従業員人数による規模で実施率を比較すると、従業員 100 人以下では 46 社のうち 12 社で実施率 26%、従業員 100 人超では 19 社中 7 社で実施率 37%と 11%の差があるものの大きな差があるとは言えない結果となった。

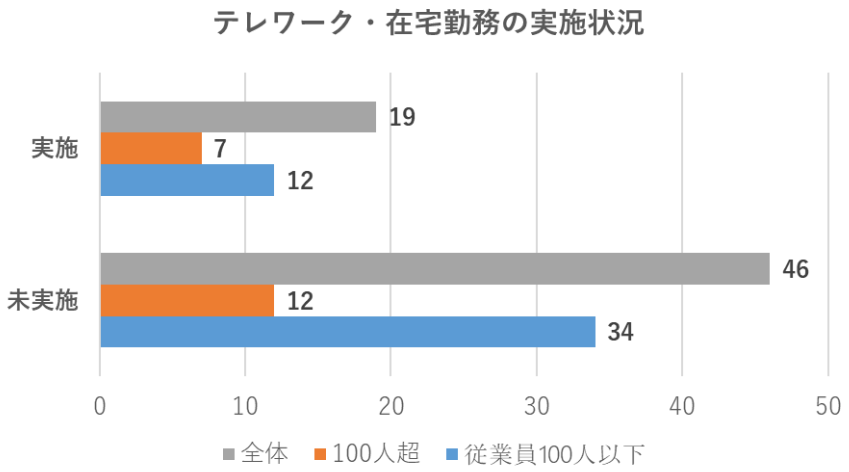

図 24　テレワーク・在宅勤務の実施状況に関する回答状況（n＝65）

② テレワークのために導入した対策

テレワーク等の社外業務のために導入・実施した対策についても確認した。

リモートツール、VPN その他の技術的対策の実施以外にも、社外業務時の個人情報の持ち出し等に関するルールの整備と徹底についても回答があった。

表 15　テレワーク等の社外業務のために導入・実施した対策

テレワークなどの社外での業務のために 導入・実施した対策があれば教えてください（複数回答可、n＝65）	
リモート・遠隔操作ツールの導入	5 社
VPN の導入	5 社
シンクライアントの導入	4 社
ウェブ会議ツール導入・実施	2 社
社外業務時のルール整備と徹底	2 社

③ テレワーク等の社外業務に関して感じているリスク

中小企業等がテレワーク等の社外業務を実施する上での課題を把握するため、当該業務に

関して中小企業等が感じているリスクについて確認した。

最も回答が多かったのは「社外で業務用パソコンを利用するための技術的な対策がとれていない」ことであり、65 社のうち、26 社（40%）がリスクを感じていると回答した。2 番目に多かったのは 20 社（約 31%）が回答した「私用パソコンの業務利用」で、3 番目に多かったのは 19 社（約 29%）が回答した「USB メモリの利用」であった。

これら上位 3 つの回答から中小企業等が VPN の構築やシンクライアント端末の導入などを実施することができないまま、やむを得ず従業員の私用パソコンを業務利用させており、そのことに不安を感じていることが分かる。

表 16　テレワーク等の社外業務に関して感じているリスクや不安

テレワークなどの社外での業務に関して 感じているリスク・不安はありますか？（複数回答可、n＝65）	
社外で業務用パソコンを利用するための技術的な対策がとれていない	26 社
私用パソコンの業務利用	20 社
USB メモリの利用	19 社
フリーWi-Fi への接続	14 社
私用スマートフォンの業務用パソコンへの接続	10 社
オンラインストレージなどファイルツールの利用	10 社
フリーメールの利用	8 社
Web 会議サービスのセキュリティが不安	7 社
セキュリティ強化によるパフォーマンスの低下	1 社
パソコンの紛失・破損	1 社

(5) 中小企業等のネットワーク構成の状況

UTM サービス導入のために現地訪問とヒアリングによる環境調査を実施し、ネットワーク構成図を作成した。64 社[5]分の構成図から傾向および想定されるリスク等を分析した。

① 構成の傾向と想定されるリスク

まず、通信キャリアの光ファイバー回線（ONU）からルーターを経由し、社内のサーバーやパソコン、プリンタ等の社内ネットワークが直接インターネットへ接続されている環境が多く確認された。

また、使用されているルーターの多くは家庭等でも使われる有線・無線 LAN ルーターなどの IoT 機器で、これらの IoT 機器は ID・パスワードのメーカー出荷時の初期設定からの変更管理等の適切な実施が求められる。適切な実施がされていない場合、インターネットからアクセス可能な IoT 機器のポートに対して当該 IoT 機器の初期設定の ID とパスワードを使ったログインをされるリスクがある。

また、旧式の IoT 機器も散見されたことから、IoT 機器の制御プログラム（ファームウェア）の公表された脆弱性に対しても、修正プログラムの速やかな適用などの適切な管理の実施がもとめられる。

これらの環境を悪用された場合、当該中小企業等の IP アドレスを踏み台とした他の企業への攻撃等が実施される等により、踏み台にされた中小企業等が攻撃通信の発信元となってしまうことも想定され、当該中小企業等がサイバー攻撃の加害者として特定されるなどのリスクがある。

更に、不正な通信内容や悪用されている通信先 IP アドレスに対する通信等への防御ツール

[5] 現地調査の結果最終的に UTM サービス導入不可となった 5 社を含む 64 社

が設置されていない状況も確認されたことから、悪意のある通信に対して脆弱な社内ネットワーク環境であることが確認された。

これらの環境が犯罪者に悪用された際には、「社内の重要な情報が窃取されるリスク」、「社内のシステムが使用不能になるリスク」、「関係先に悪意のあるプログラムを配信してしまうリスク」等が現実となり中小企業の事業継続に大きな影響を与える可能性がある。

② ネットワーク構成図の活用方法等

サイバーリスクの適切な認識と管理のためには、インターネットとの接続点の接続形態と接続箇所の数などの現状のネットワーク構成を特定し、それぞれに実装されている対策も含め今回作成したようなネットワーク構成図などで見える化したうえで、対策の必要性を検討することが重要である。

最新のネットワーク構成が継続的に更新・維持されネットワーク図として見える化されていることで、インターネットと社内ネットワークの接続点に係るリスクや通信内容および通信先への送受信に係るリスクなどに応じた UTM やエンドポントツールの導入および更新の必要性の検討といった具体的なリスク管理の実施が可能になるとともに、サイバー攻撃を受けた際にはサイバーセキュリティ事故に対処する専門ベンダーとの連携や関係先との連携においても基礎情報としてネットワーク構成図を共有することで速やかな状況把握並びに対処方針の確立に資するものと期待される。

人的リソースに限りのある中小企業等においてはセキュリティの専任担当者を配備できない企業も多いことが確認されており、取引ベンダーに管理を任せきりにすることで、自社の情報資産の一部であるネットワーク構成がブラックボックスとなってしまうリスクがある。このため中小企業から取引ベンダーに対して、最新のネットワーク図の納品ならびに説明を要請するなどのリスク管理も重要と考えられる。

(6) サイバー攻撃を受けた場合の想定損害額

アンケート回答企業ごとに、規模や業種特性を踏まえた「情報漏えい」、「DoS 攻撃」、「IT（クラウド）サービス停止」、「金融取引」および「恐喝」の五つのシナリオに基づく想定損害額[6]を算定した。65 社の平均値および中央値は、下表のとおりであった。

表 17　サイバー攻撃を受けた場合の想定損害額

	平均値	中央値
想定損害額	**6,290 万円**	**1,988 万円**
損害賠償費用	613 万円	53 万円
事故対応費用	932 万円	571 万円
お詫び対応費用	1,006 万円	80 万円
売上機会損失額	3,739 万円	1,284 万円

被害を受けた相手に対する「損害賠償費用」やインシデント対応のために必要なさまざまな「事故対応費用」を合計した「想定損害額」の平均値は 6,290 万円、中央値は 1,988 万円となっており、ひとたびサイバー攻撃の被害を受けた場合には、中小企業等の経営を揺るがすだけのイ

[6] ＳＯＭＰＯリスクマネジメント株式会社が海外の損害保険会社や損害保険ジャパン株式会社等のサイバーセキュリティに関連した保険金支払事例等を基に開発した試算モデルにより算定した当該企業に発生し得る損害額の想定値

ンパクトが生じ得ることが窺える。

また、「損害賠償費用」のほかにも、各費用項目において、平均値と中央値の間には、保有する個人情報の数などの違いによる一定のばらつきが認められたが、「事故対応費用」については平均値と中央値との乖離が小さく、保有個人情報の規模や業種にかかわらず、一定の費用負担が必要になることが読み取れる。

この結果は、前記「セキュリティに関するアンケート」の結果および上記結果を踏まえると、サイバー攻撃に対するリスク認識やセキュリティインシデント発生に備えた対策が進んでおらず、サイバー攻撃の被害を受けた場合に適切な対処が講じられないおそれがある一方で、経営に一定以上のインパクトを生じる損害が発生する可能性があることから、中小企業等に対し、リスクに関する啓発およびファイナンス面での支援の両面から施策を講じていくことの必要性を示唆するものといえる。

3.1.2. 中小企業等の公開情報におけるサイバーリスクの実態

中小企業等が実際にサプライチェーン攻撃の対象となった場合のリスクを把握するため、「サプライチェーンリスク評価サービス」の公開情報に対する外部評価機能を用いて調査した。

(1) サプライチェーン攻撃の起点となり得る弱点の状況

ドメイン情報等のインターネット上の公開情報を基に、攻撃者が標的型攻撃の対象を偵察するのと同じ視点で、中小企業等の公開情報に攻撃の起点となり得る脆弱性等の弱点が存在しないかを確認し、リスクを各項目 100 点満点で評価した。評価結果および確認された主な指摘事項は下表のとおりである。

「メールサーバーの設定」および「公開サーバーの脆弱性」の平均点が低く、対策の必要性を訴求していく必要性があると思われる。

また、重大なインシデントに繋がる可能性のある指摘事項も確認されており、千葉県の中小企業等がサプライチェーン攻撃の起点として攻撃者から狙われる可能性があると推察される。

表 18 公開情報の外部評価結果

評価分類	カテゴリー	検出課題例	評価平均
サーバーやアプリケーションの設定情報	アセットに対する評価	フィッシングサイトのホスティング、悪意のあるコンテンツのホスティング、C&C サーバーとしてフラグ付け、不審な URL　など	99.7
	DNS	DNS ゾーン転送、オープン DNS リゾルバ、DNSSEC の設定　など	87.9
	公開されているサービス	公開されているデータベースサービス、公開されている脆弱な OS サービス、公開されているクリアテキスト管理サービス、公開されているコンソールサービス　など	84.7
	メールサーバー	SPF の存在、DKIM の有無、DMARK の有無　など	57.9
	TLS	TLS の脆弱性、HTTPS の非サポート、信頼されていない TLS 証明書、推奨されない TLS プロトコル、HTTPS リダイレクト、TLS の弱い鍵　など	71.1
	Web サーバー	WAF の存在、Content-Security-Policy レスポンスヘッダ、Web サーバーヘッダーで公開されているバージョン情報、XSS レスポンスヘッダ　など	80.8
公開サーバー・アプリケーション・ドメイン	アプリケーションのセキュリティ	SSH バージョン 1 のプロトコル、Web アプリケーションのオープンリダイレクト・XSS・CSRF、公開されている WordPress ユーザーデータ　など	94.8
	ドメインに対する攻撃	ドメインハイジャック、ドメインタイポスクワッティング　など	83.3
	テクノロジー	CMS テクノロジー 、Web アプリケーションテクノロジー、Web サーバーテクノロジー、一般的なテクノロジー　など	36.6

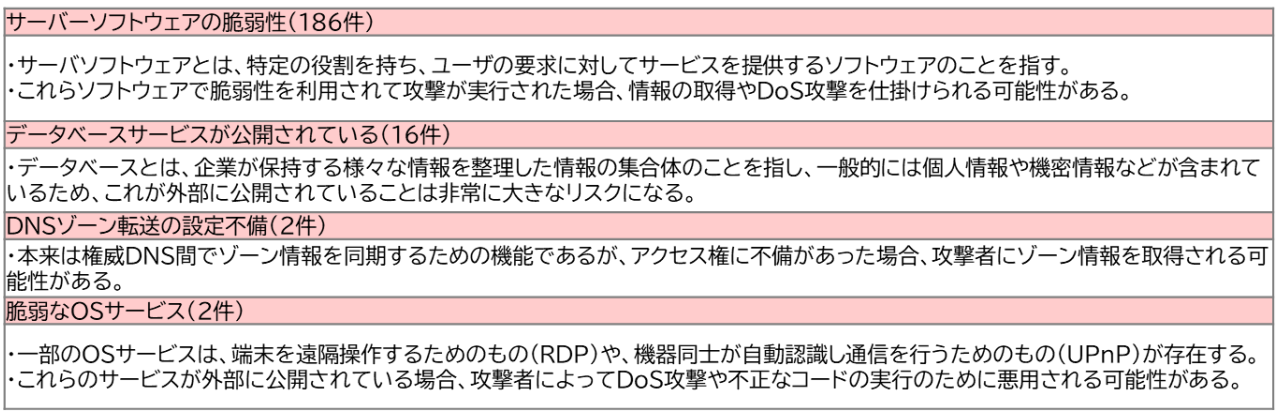

図 25 公開情報における主な指摘事項

3.1.3. 中小企業等からの問合せ内容の実態把握

(1) 相談受付サービスのコールセンター等に寄せられた問合せ状況

実証参加企業（66 社）からの相談窓口となるコールセンターおよびＳＯＭＰＯリスクマネジメントに直接入電した問合せ件数は全体で 19 件であり、その内訳は下表のとおりであった。

問合せの内容は、「実証参加に関する問合せ（10 件）」、「EDR の導入に関する問合せ（6 件）」、「ウェブアンケートへの回答に関する問合せ（2 件）」、「実証終了後のサービスの取扱いについて（1 件）」といった実証参加に伴う平時の問合せであり、セキュリティインシデントの相談や IT に関する困りごとなどの有事における相談はなかった。

この結果から、中小企業等向けのセキュリティサービスにおいては、サービス導入・利用に伴う操作方法等の取扱いに関する問合せ対応の機能が求められると考えられる。

表 19 コールセンターなどに寄せられた問合せ内容

コールセンターなどに寄せられた問合せ内容	
実証参加に関する問合せ	10 件
セキュリティ機器設置等の問合せ	6 件
アンケート回答に関する問合せ	2 件
実証終了後のサービスについて	1 件
総計	19 件

(2) サービス導入時における個別ヒアリングの状況

各サービスの導入に伴う現地調査での往訪時や電話での導入勧奨の際に個別ヒアリングを実施した。個別ヒアリングの結果、中小企業等がセキュリティサービスを導入する上での問題点や、中小企業等向けサービスの在り方を検討する上で参考にすべき意見などが抽出できた。

① 自社の情報資産について把握・管理されておらず状況把握が困難であった

UTM サービスの導入可否確認のための現地調査を実施したところ、事前ヒアリングシートで UTM 未導入と回答されているにもかかわらず、UTM が導入済で急遽調査内容を変更しなければならないケースが散見された。また、ネットワーク構成について担当者にヒアリングをしたが把握しておらず、ネットワークを構築しているベンダーに直接聴取したり、現地端末等を見ながら確認したりする必要があり、想定以上に調査時間を要するケースも散見された。

また、セキュリティに関するアンケートにおいては、対策の導入状況に関する項目への回答が独力で答えられないとの申し出を受けたこともあり、実際に導入状況に係る項目が未回答の企業も多かった。

② 取引先ベンダーの協力を得ることが困難であった

ネットワークの管理を委託しているベンダーから、既存のネットワークに機器を導入しないでほしいとの要請を受けるなど、機器の導入や既存設備の設定変更等に関する協力を得られないケースが散見された。この結果、導入を断念するケースが生じた。

③ 担当者以外のリテラシー不足により対策導入に当たり担当者に掛かる負荷が大きい

EDR サービスの導入は実証参加企業自身で各パソコンにインストール作業を行う必要があるが、他の従業員では実施が難しいという理由から担当者が 1 人で導入するケースが多く、作業時間の制約もあり希望している台数への導入を断念せざるを得ない企業が多かった。

3.1.4. 中小企業等に対するセキュリティインシデントの実態

実証参加企業の約 95%[7]において、セキュリティインシデントに関する痕跡が確認された。これは、中小企業等を 100 社集めると、そのうちの 95 社がサイバー攻撃を受けて危険に晒されている可能性があるという状況である。

また、ウイルス検知機能、スパムメールフィルター、IPS、ウェブフィルタリングが頻繁に稼働しており、更には UTM をすり抜けた高度な攻撃も確認されていることから、中小企業等に対しても多様な攻撃が高頻度で展開されている状況にあることが窺える。

（1） UTM サービスにおけるセキュリティインシデントの検知状況

① 地域実証における監視実績（全体概要）

UTM サービスについては、参加申込企業 68 社に対して導入提案を行い、最終的に機器の設置が完了してログを取得できたのは 59 社であった。

表 20 UTM サービスにおける取得データの概要

データ内容	
取得対象	59 社
取得日数	平均 34.5 日間
取得データの種類	ゲートウェイアンチウイルス機能のログ スパムメールフィルター機能のログ IPS 機能のログ ウェブフィルタリング機能のログ

導入企業 59 社において、1 件の緊急度「高」のアラートを発信し、「不正な IP アドレスへの通信」が成立していることが確認された。

なお、当該 1 社は、セキュリティ対策としてパソコンのウイルス対策ソフトについては導入済であり、中小企業等におけるセキュリティ対策の強化の必要性を裏付ける結果となった。

② ゲートウェイアンチウイルスの稼働状況

ゲートウェイアンチウイルスの稼働件数：

ウイルスの受信について、52 件の稼働を確認した。

59 社のうち、8 社において稼働を確認した。（稼働割合：約 14%）

なお、実証では UTM のパフォーマンス低下により導入企業の業務に支障が出ることを避けるため、1MB 未満のファイルのみゲートウェイアンチウイルス機能による分析対象とした。

表 21 UTM のゲートウェイアンチウイルス機能で検知したウイルスの種類

種類	件数
トロイの木馬	46
アドウェア	6

[7] UTM サービスと EDR サービスの両サービスを導入し UTM サービスのいずれかの機能が稼働もしくは EDR サービスでの不正プログラムの検知があった企業（48 社中 46 社）、UTM サービスのみ導入しいずれかの機能が稼働した企業（11 社中 11 社）、EDR サービスのみ導入し不正プログラムの検知があった企業（3 社中 2 社）を集計

③ スパムメールフィルターの稼働状況

スパムメールフィルターの稼働件数：

スパムメールの受信について、67，080 件の稼働を確認した。

59 社のうち、43 社において稼働を確認した。（稼働割合：約 73%）

なお、実証においては、検知したスパムメールをブロックするのではなく、メールの件名に下表記載の分類でタグ付けし、通知した。

表 22　UTM のスパムメールフィルター機能で検知したスパムメールの分類

分類・タグ名	説明	件数
confirmed SPAM	既知のスパム送信者から送られてきており迷惑メールと確定しているメール	26,279
suspect SPAM	新たなスパム攻撃に関連があると思われるメール	351
bulk SPAM	発信者は既知のスパム送信者ではないが、全体送信のメールなど迷惑メールである可能性があるメール	40,450
合計		67,080

④ IPS の稼働状況

IPS の稼働件数：

不審な通信の検知・防御について、490 件の稼働を確認した。

なお、59 社のうち、19 社において稼働を確認した。（稼働割合：約 32%）

ア.ＷＥＢ シェルスクリプトによるリモートコマンド実行（１３１件）
・シェルスクリプトを経由して任意のコマンドを実行できる脆弱性。 ・攻撃者に任意のコマンドをリモートで実行される可能性がある。
イ.ＴＣＰ ＰＡＷＳ機能の消去（８２件）
・ＰＡＷＳ機能を有効にしたＴＣＰには、受信ホストの内部タイマを更新できる脆弱性が存在する。 ・この脆弱性を利用されると、正常な通信が妨害、拒否される可能性がある。
ウ.ＷＥＢ Ｍａｓｓｃａｎ/Ｓｙｓｓｃａｎ Ｓｃａｎｎｅｒによるスキャニング（６７件）
・Ｍａｓｓｃａｎ/Ｓｙｓｓｃａｎ Ｓｃａｎｎｅｒは脆弱性をスキャンするツール。 ・攻撃者にスキャンされた場合、脆弱性を露呈、利用される可能性がある。
エ.ＷＥＢクロスサイトスクリプティング（６４件）
・クロスサイトスクリプティング（ＸＳＳ）は、攻撃者が他のユーザーが閲覧するＷｅｂページにクライアント側のスクリプトを注入することを可能にする脆弱性。 ・脆弱性のある標的サイト（例：ＳＮＳや掲示板など）では無く、そのサイトを利用したエンドユーザに、なりすましやＩＤ/パスワード盗用などの被害を与える可能性がある。
オ.ＷＥＢクロスサイトスクリプティング（ｃｏｏｋｉｅの盗難）の試み（３３件）
・クロスサイトスクリプティング（ＸＳＳ）は、攻撃者が他のユーザーが閲覧するＷｅｂページにクライアント側のスクリプトを注入することを可能にする脆弱性。 ・脆弱性のあるサイト（例：ＳＮＳや掲示板など）では無く、そのサイトを利用したエンドユーザに、ｃｏｏｋｉｅに保存された情報の盗用などの被害を与える可能性がある。
カ.Ｐｈｏｔｏｄｅｘ ＰｒｏＳｈｏｗ Ｐｒｏｄｕｃｅｒ５.０.３２５６ バッファオーバーフロー（２１件）
・Ａｄｏｂｅ Ｓｈｏｃｋｗａｖｅ Ｐｌａｙｅｒのリモートコード実行の脆弱性。 ・この脆弱性を利用されると、標的パソコンの乗っ取り、誤作動、他のパソコンを攻撃するなどの被害が発生する可能性がある。
キ.ＷＥＢ ＰＨＰ ＣＧＩ引数インジェクション（１８件）
・ＣＧＩとして実行されたバージョン５.３.１２ および ５.４.２ までの ＰＨＰ には、引数注入の脆弱性がある。 ・この脆弱性を利用されると、攻撃者に悪意のあるコードをリモートで実行される可能性がある。
ク.ＷＥＢディレクトリトラバーサルの脆弱性（１６件）
・ディレクトリトラバーサルとは、「親ディレクトリへの横断（ｔｒａｖｅｒｓｅ）」を示すような文字が渡されてしまう脆弱性。 ・この脆弱性を利用されると、情報漏洩が発生する可能性がある。

図 26　主な IPS の稼働状況（内訳）

⑤ ウェブフィルタリングの稼働状況

ウェブフィルタリングの稼働件数：

不審な URL への接続の検知・防御について、118,141 件の稼働を確認した。

なお、59 社のうち、52 社において稼働を確認した。（稼働割合：約 88%）

ア.ゲームサイトへのアクセス(42,723 件)
・ユーザーがゲームをプレイまたはダウンロードできるようにするサイトへのアクセス。 ・セキュリティ上、望ましくない可能性のあるソフトウェアをインストールされる可能性がある。
イ.Facebookへのアクセス(16,068 件)
・Facebookへのアクセス。 ・業務上必要性が低いサイトへのアクセスをブロックした。
ウ.成人/アダルトコンテンツサイトへのアクセス(13,603 件)
・露出症を含む性行為または性行為を描写またはグラフィカルに説明するサイトへのアクセス。 ・不正ウィルスに侵入されたり、詐欺サイトや脅迫サイトに誘導される恐れがある。
エ.不正の可能性の高いサイトへのアクセス(7,699 件)
・過度に露出（ソフトウェアの仕様上セキュリティを考慮していないもの）に対するアクセス。 ・脆弱性に応じた影響が発生する。
オ.望ましくない可能性のあるソフトウェアをインストールされるサイトへのアクセス(6,129 件)
・ユーザのセキュリティやプライバシーに対して予期しない影響を及ぼす可能性のあるアプリケーションをインストールできるサイトへのアクセス。 ・コンピュータのリソースが消耗する可能性がある。
カ.セキュリティが破られたWebサイトへのアクセス(2,836 件)
・マルウェア、不正なコード等を埋め込まれてしまったサイト。 ・ブロックしなければ侵害の内容に応じた影響が発生する。
キ.Twitterへのアクセス(2,574 件)
・Twitterへのアクセス。 ・業務上必要性が低いサイトへのアクセスをブロックした。
ク.ギャンブル系サイトへのアクセス(2,517 件)
・ギャンブルの情報の提供や促進をするサイトへのアクセス。 ・業務上必要性が低いサイトへのアクセスをブロックした。 ・不正ウィルスに侵入されたり、詐欺サイトや脅迫サイトに誘導される恐れがある。
ケ.帯域を消費しやすいサイトへのアクセス(2,285 件)
・個人向けのオンラインストレージ、バックアップ、ホスティングサービスを提供するWebサイトへのアクセス。 ・コンピュータの負荷を高める可能性があるためブロックした。
コ.悪意のあるWebサイトへのアクセス(2,271件)
・ユーザの同意なしに、システム変更やユーザへ害を及ぼそうとするサイトへのアクセス。 ・ブロックしなければ、ユーザの意図しない操作が発生する可能性がある。

図 27　主なウェブフィルタリングの稼働状況（内訳）

(2) EDR サービスにおけるセキュリティインシデントの検知状況

① 地域実証における監視実績

EDR サービスについては、参加申込企業 68 社に対して導入提案を行い、最終的に導入が完了してログを取得できたのは 51 社であった。

表 23 EDR サービスにおける取得データの概要

データ内容	
取得対象	51 社
導入台数	492 台（1 社平均 9.6 台）
取得日数	平均 57.8 日間
データの種類	①不正なプログラムの有無 ②不正なサイトへのアクセス履歴 ③Wi-Fi への接続履歴 ④USB 機器の接続履歴

② EDR サービスにおける検知結果

実証参加企業 51 社を対象に分析したところ、75%の企業において不正プログラムが検出された。また、不正なプログラムを配布しているサイトといった不正なサイトへのアクセスについても多数確認された。

なお、地域実証期間において、不正プログラムや不正なサイトへのアクセスといったセキュリティインシデントが検知されなかった企業は、3 社（約 6%）のみであった。

表 24 EDR サービスにおけるセキュリティインシデントの検知状況

不正プログラム	
確認数	4,122 件
検出割合	75%（51 社中 38 社）
うちウイルス対策ソフトにより隔離済	3,724 件（90%）
隔離されていない不正プログラム	398 件（10%）
不正サイトへのアクセス	
確認数	891 回（51 社中 24 社、47%）
Wi-Fi 接続履歴	
確認数	9,277 回
うちセキュリティレベルの低い Wi-Fi への接続	46 回（51 社中 7 社、14%）
USB 機器の接続履歴	
確認数	7,339 回（51 社中 42 社、82%）

(3) 駆付け支援サービスの実施内容

前述のとおり、UTM サービスを導入した企業において 1 件の「不正な IP アドレスへの通信」が成立していることが確認されたため、緊急度「高」のアラートを発報し、支援を実施した。

① 該当企業（X 社）の概要

- 業種　　：製造業
- 従業員数区分　　：100 名～200 名
- 情報システム要員　　：専任者は置いていない（兼務による担当者あり）
- セキュリティ対策状況：ウイルス対策ソフト、UTM、データのバックアップを導入している
- サイバー保険　　：未加入

② 事案の概要および対処内容

ア．2020 年（令和 2 年）12 月下旬、UTM サービスの SOC 機能において、直近 1 か月の間にマルウェアの通信先となっていたことが確認されている IP アドレスへの通信が UTM を通り抜けて成立していることを検知し、アラートを発報した。

イ．X 社担当者に確認したが、当該通信が検知された時点の作業内容は覚えておらず、意図した通信であったかは不明であった。

ウ．X 社担当者に対し、接続元端末を LAN から分離した上、ウイルス対策ソフトでのフルスキャンを実行してもらうよう指示した。スキャンの結果、何も検知されなかったため、SOC 機能により再びアラートが発報されるまで様子を見ることについて X 社担当者から了解を得て、案件クローズとした。

エ．当該 IP アドレスはホスティング業者のもので複数のドメインに紐付いており、マルウェアが通信をする際に当該 IP アドレスを経由したと考えられる。

オ．SOC 機能は日本国内に特化した独自のブラックリストを持っているが、今回検知した不正な IP アドレスについては UTM のブラックリストには載っていなかった。

なお、導入時対応を含むインシデント等による対応の内訳は、下表のとおりであった。

表 25　インシデント対応などの状況

インシデント対応などの内訳		件数
電話・リモートによるインシデント対応		2 件
	UTM サービスのアラート対応（電話による誘導）	1 件
	EDR サービスでの不正プログラム（ブラウザ・ハイジャッカー）検知に伴う駆除対応（リモート駆除）	1 件
機器設置等のトラブル対応		3 件
	UTM サービス導入後のネットワーク不良（症状改善）	2 件
	UTM サービス導入後のネットワーク不良（症状改善せず、撤去）	1 件

③ 検知・駆除できていなかった場合の想定損害額

前記「(4)　セキュリティに関するアンケート」で取得したデータを用いて X 社の想定損害額を算定したところ、下表のとおりであった。

表 26　X 社想定損害額

内訳	金額
損害賠償費用	3,640,000 円
事故対応費用	12,090,000 円
お詫び対応費用	2,400,000 円
売上機会損失額	36,630,000 円
合計	**54,760,000 円**

4. 考察

4.1.実証参加企業におけるサイバー攻撃の実態

千葉県の中小企業等に向けられているサイバー攻撃の実態について、各サービスで確認されたセキュリティインシデントの内容等から考察した。

4.1.1. サイバー攻撃の対象

サイバー攻撃を受けている対象の傾向を把握するため、UTM サービスのうち、外部からの攻撃の検知機能である「アンチウイルス機能の稼働件数」、「スパムメールフィルター機能の稼働件数」および「IPS 機能による検知のうち外から内に向けられた通信の検知件数」を、業種別と従業員人数による規模別で 1 社当たりに換算して比較した。当該比較分析は、UTM サービスを導入した 59 社を対象とした。EDR サービスについては 1 社当たりの導入台数および導入範囲のばらつきの幅が大きく傾向を分析するには不適当であったため、EDR サービスによる不正プログラムの検知件数は分析対象に含めなかった。

業種別の比較では IPS が「H 運輸業、郵便業」でのみ確認されていること以外の傾向は見られず、特定の業種に偏ることなく幅広い業種が攻撃の対象となっていることが分かる。

従業員人数による規模での比較では、規模が大きい方が検知件数が多い傾向はあるものの、規模に正比例してはおらず、規模を問わず攻撃の対象となっていることが推測できる。

表 27 UTM サービスによる外部からの攻撃の検知状況（業種別）[8]

業種	社数	アンチウイルス		スパムメール		IPS（外→内）		3 機能計	
		業種計	1 社あたり	業種計	1 社あたり	業種計	1 社あたり	業種計	1 社あたり
D 建設業	11	0	0	1,625	148	0	0	1,625	148
E 製造業	10	44	① 4.4	8,895	④ 890	0	0	8,939	② 813
R サービス業（他に分類されないもの）	8	0	0	8,109	③ 1,014	0	0	8,109	③ 737
H 運輸業、郵便業	7	0	0	5,850	⑤ 835	250	① 36	6,100	⑤ 555
P 医療、福祉	5	6	② 1.2	455	91	0	0	461	42
I 卸売業、小売業	4	0	0	6,591	② 1,648	0	0	6,591	④ 599
J 金融業、保険業	4	0	0	93	23	0	0	93	8
K 不動産業、物品賃貸業	4	1	④ 0.25	35,095	① 8,774	0	0	35,096	① 3,191
L 学術研究、専門・技術サービス業	2	1	③ 0.5	147	74	0	0	148	13
G 情報通信業	1	0	0	50	50	0	0	50	5
N 生活関連サービス業、娯楽業	1	0	0	165	165	0	0	165	15
Q 複合サービス事業	1	0	0	5	5	0	0	5	0
T 分類不能の産業	1	0	0	0	0	0	0	0	0
総計	59	52	0.9	67,080	1,137	250	4	67,382	6,126

[8] ①～⑤の数字は各機能における件数上位 5 業種

表 28　UTM サービスによる外部からの攻撃の検知状況（業種別）[9]

従業員数区分	社数	アンチウイルス		スパムメール		IPS（外→中）		3 機能計	
		計	1 社あたり	計	1 社あたり	計	1 社あたり	計	1 社あたり
1～5 人	6	2	③ 0.33	1,909	318	0	0	1,911	319
6～10 人	7	2	④ 0.29	289	41	0	0	291	42
11～20 人	5	0	0.0	1,594	319	0	0	1,594	319
21～50 人	15	0	0.0	39,268	① 2,618	94	② 0.5	39,362	② 2,624
51～100 人	10	0	0.0	4,738	⑤ 474	0	0	4,738	⑤ 474
101～200 人	11	40	① 3.6	10,294	③ 936	156	① 14	10,490	③ 954
201～300 人	2	6	② 3	6,938	② 3,469	0	0	6,944	① 3,472
301 人以上	3	0	0.0	1,924	④ 641	0	0	1,924	④ 641
総計	59	50	0.8	66,954	1135	250	4	185,317	3,141

4.1.2.　サイバー攻撃の種類・内容

「中小企業等に対するセキュリティインシデントの実態」に記載したとおり、導入した UTM サービスおよび EDR サービスの各機能が頻繁に稼働していることから、千葉県の中小企業等に対しては、サイバー攻撃が高頻度で向けられていると推測される。また、「中小企業等に対するセキュリティインシデントの実態　(1)　UTM サービスにおけるセキュリティインシデントの検知状況　④　IPS の稼働状況」に記載した実証参加企業自身ではなく、実証参加企業のウェブサイト訪問者を狙った攻撃や、「中小企業等に対するセキュリティインシデントの実態　(3)　駆付け支援サービスの実施内容」に記載した UTM 機器による検知をすり抜けた通信、「中小企業等に対するセキュリティインシデントの実態　(2)　EDR サービスにおけるセキュリティインシデントの検知状況」に記載したウイルス対策ソフトで隔離等がなされていない不正なプログラム等が確認されていることから、向けられている攻撃の内容は多様かつ高度なものであると考えられる。

- ✓ ＵＴＭサービスおよびＥＤＲサービスにおいて多数のサイバー攻撃の痕跡が確認された
- ✓ クロスサイトスクリプティングにより実証参加企業自身ではなく実証参加企業のサイト訪問者を狙った攻撃も多数確認された
- ✓ ＵＴＭによる監視だけでは検知できずＳＯＣ機能による分析がなければ捕捉できなかった高度な攻撃も確認された
- ✓ ＥＤＲサービスで検知した不正プログラムのうち、ウイルス対策ソフトによって隔離などの処理がされていないものが確認された

[9] ①～⑤の数字は各機能における件数上位 5 区分

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

「中小企業等の実態把握」において把握した実証参加企業におけるセキュリティに関する実態から、中小企業等がセキュリティ対策を進める上での課題について考察した。

4.2.1. セキュリティ意識に関する課題

セキュリティ対策実施の起点となる意識に課題があることは、昨年度ＳＯＭＰＯリスクマネジメントが実施した「中小企業向けサイバーセキュリティ事後対応支援実証事業（地域名：神奈川県）」において確認されているが、「中小企業等の実態把握 (1) 中小企業等のセキュリティに対する意識の実態」に記載のとおり、千葉県の中小企業等においてもセキュリティ意識における同様の課題が確認されている。

まず、86%の中小企業等が「自社がサイバー攻撃を受けること」がセキュリティ対策を講じるきっかけになると考えているが、実際に自社への攻撃を認識したことがある企業は全体の約 10%にとどまっている。また、36%がきっかけになると考えている「取引先からの要請」について実際に要請を受けたことがある企業は 1 社だけであったことから、実証参加企業においてはセキュリティ意識が醸成されるのに効果的と考えられる事由が発生しておらず、セキュリティ対策を実施するための動機付けが乏しく、セキュリティ意識が十分に醸成されていないことが推察される。

加えて、「中小企業等からの問合せ内容の実態把握 (2) サービス導入時における個別ヒアリングの状況」に記載のとおり、情報資産の管理までを一任できる取引ベンダーの存在が、セキュリティ意識が不十分なままでの一定のセキュリティ水準の維持を可能にしている一方で、中小企業等のセキュリティ意識が醸成されにくい環境を作り出していると考えられる。

- ✓ セキュリティ対策を講じるきっかけになる「自社へのサイバー攻撃の認識」や「取引先からの対策実施の要請」については、ほとんどの実証参加企業が実際に経験したことがなく、セキュリティ対策を実施する意識の醸成は十分とは言えない
- ✓ 情報資産の管理まで任せられてしまう取引ベンダーの存在が、一定のセキュリティ水準の維持を可能にしている一方で、意識が醸成されにくい環境を作り出している可能性がある

4.2.2. セキュリティに関する体制整備・教育に関する課題

「アンケート・ヒアリングによる支援体制構築に必要な情報の収集 (1) 中小企業等のセキュリティに対する意識の実態」に記載したとおり、専任のセキュリティ担当者を設置している企業は実証参加企業の僅か 8%にとどまっており、多くの企業はセキュリティ担当者を他の業務と兼務させている（兼務のセキュリティ担当を設置している企業の割合が約 68%と最も多くなっている）。

また、「中小企業等からの問合せ内容の実態把握 (2) サービス導入時における個別ヒアリングの状況」に記載のとおり、実証参加企業の多くがセキュリティ担当者を 1 人しか置いていないことに加え、セキュリティ担当者以外の従業員の IT やセキュリティに関するリテラシーが低いため、対策の導入時や導入後の運用において、セキュリティ担当者に掛かる負荷が大きく、このことが新たなセキュリティ対策の導入を検討する際のネックになっていると推察される。

- ✓ セキュリティの担当者は専任者は少なく、兼務による担当者がほとんどで且つ１人の場合が多い
- ✓ 担当者以外の従業員のリテラシーが低いことが、セキュリティ対策導入時や導入後の担当者の負荷を大きいものにしており、新たな対策導入を検討する際のネックになっている可能性がある

4.3.中小企業等において必要なセキュリティ対策

4.3.1. UTM サービスによるネットワークの境界防御

「実証参加企業におけるサイバー攻撃の実態 サイバー攻撃の種類・内容」に記載したとおり、千葉県の中小企業等に対して多様な攻撃が高頻度で行われていることから、中小企業等においても、従来のウイルス対策ソフトによるエンドポイント対策に加えて、ネットワークの境界に設置して配下のネットワークを複数の機能で監視・検知する UTM サービスなどの境界防御を目的とする対策の導入が必要であるといえる。

4.3.2. EDR によるエンドポイントの防御

テレワーク等により社外でパソコン等をネットワークに接続する機会が増えれば、社内ネットワークの外側で攻撃を受ける可能性が高くなる。「中小企業等に対するセキュリティインシデントの実態 (2) EDR サービスにおけるセキュリティインシデントの検知状況」に記載したとおり、ウイルス対策ソフトでは安全に隔離等の処理ができないものも存在することが確認されているため、ウイルス対策ソフトの機能を補完する対策として、パソコン等への EDR サービスの導入も必要であるといえる。

4.4.中小企業等におけるセキュリティ対策の効果

「成果報告会 (3) 成果報告会に関する追加的な取組」に記載したとおり、本実証では、実証参加企業に対し、」UTM サービスにより実際に検知された攻撃の件数および EDR サービスによる監視結果をレポートにして実証結果のフィードバックを行った。フィードバックに対して実証参加企業から得られた意見のうち、主なものを整理した。

4.4.1. UTM サービスの検知件数が想像以上に多く、危機意識が強まった

「中小企業等の実態把握 アンケート・ヒアリングによる支援体制構築に必要な情報の収集 (1) 中小企業等のセキュリティに対する意識の実態」に記載したとおり、実証参加時点ではサイバー攻撃を受けた経験があると認識している企業は約 10%であったが、中小企業等が UTM サービスの検知結果のフィードバックを受けることにより自社にもサイバー攻撃が向けられていることを認識し、危機意識を高める効果があることが検証された。

4.4.2. EDR の検知結果がレポート形式で提供されることは、社内のパソコン利用実態の把握や社内共有に有用であった

「中小企業等の実態把握 (3) EDR サービス ① サービス概要」に記載のとおり、EDR サービスには不正サイトへのアクセス履歴や Wi-Fi への接続履歴を見える化する機能があり、本実証では各項目について期間中に確認された全履歴をセキュリティレポートにして実証参加企業に提供した。

当該セキュリティレポートは、接続日時や暗号化方式の情報に基づく Wi-Fi のセキュリティ強度などを評価して一覧化して提供されるもので、中小企業等が自社におけるパソコンの利用状況を詳細に把握することにより、セキュリティ意識の醸成に繋がることを期待するものであったが、その効果が検証できた。また、レポート形式で提供したことについて、「社内共有しやすい」との評価もあり、セキュリティ担当者が少ない中小企業等において、分かりやすいアウトプットを提供することを通じて社内共有のきっかけを作ることも意識啓発に有用である可能性が示唆された。

5. 実証結果を踏まえたビジネス化に向けた検討

5.1.中小企業等向けのセキュリティ簡易保険サービスの在り方およびマーケティング方法の検討

中小企業等向けのセキュリティ対策支援サービスの一部として提供する場合の簡易保険の補償内容および提供方法（マーケティング方法）並びに任意保険の普及促進方法について、実証結果を踏まえて、次のとおり整理した。

5.1.1. 簡易保険で補償されるべき内容

「中小企業等に対するセキュリティインシデントの実態」に記載したとおり、実証を通じて多数のサイバー攻撃の検知が確認されたが、同時にほとんどの攻撃が導入した UTM サービスや EDR サービスによって検知・防御が可能であることが分かった。

中小企業等に向けたサイバー保険については、事故が生じた際のリスク移転（リスク・ファイナンスの機能だけでなく、インシデントが発生した後にスムーズな調査等の手配を行うための与信（クレジット）の機能が重要な位置付けとなっている。こうした観点から、セキュリティ対策支援サービスの一部として簡易保険を提供する場合、情報漏えいが発生したことによる損害賠償費用や取引先や顧客へのお詫びに係る費用の補償といった、支払われる機会が少ない補償内容よりも、一緒に提供されるセキュリティ対策により攻撃を検知したことに伴って必要となるウイルス駆除やパソコンの初期化といった初動対応のための費用や、攻撃を受けた範囲などの調査をするための費用に対する補償に重点を置いた設計とすることが望ましいと考える。

5.1.2. 簡易保険の提供方法（マーケティング方法）

セキュリティ対策による検知に伴って発生する費用に対する保険金が確実に支払われるためには、セキュリティ対策の導入に係る契約締結時に保険加入も完了することが望ましい。セキュリティベンダーが損害保険会社や保険代理店と連携し、セキュリティ対策と同時にサイバー保険を提案する方法も可能ではあるが、利用者である中小企業等の担当者の負荷を考慮すると、セキュリティベンダー等のサービス提供者を保険契約者とし、サービス利用者を補償対象（被保険者）とする「付帯方式保険」が望ましいと考える。

5.1.3. 任意サイバー保険との連動による普及促進方法

セキュリティ対策支援サービスの一部として提供する場合の簡易保険の普及促進方法として、セキュリティ対策支援サービスが導入されていることを条件として、利用者が任意で加入するサイバー保険に割引を適用する方法が考えられる。サイバー保険を任意で加入する場合、保険料が高額になりがちなため、保険料の割引は中小企業等にとって一定の訴求効果が期待できる。

なお、本実証では、損害保険ジャパン株式会社の協力の下、実証参加企業限定ではあるが、割引を適用できる特別なサイバー保険を提供した。参考として、当該サイバー保険の内容を簡単に記載する。実証参加企業の当該保険の提案状況は、1 社が加入済、9 社が見積もり希望・検討中である。

（1） 必要な部分に絞った分かりやすい補償内容

中小企業等の加入を想定し、記者会見費用やコールセンター設置費用など、必要性が乏しいと思われる部分を削った分かりやすい補償内容にした。

（2） 保険料はプラン選択方式、算出のための難しい告知は不要

通常のサイバー保険は、保険料算出のためにセキュリティに関する告知を行う必要があるが、内容が専門的な項目もあり保険加入のネックになるため、告知を不要とし、プランを選ぶだけで保険料が決まる簡便な方式を採用した。

（3） UTM、EDR の導入による割引を適用

両サービスの導入によるサイバーリスクの低減を評価し、保険料の割引を適用できるようにした。

5.2.中小企業等の実態やニーズに応じた必要なセキュリティ対策の内容

5.2.1. 推奨される要件

「実証参加企業におけるサイバー攻撃の実態」、「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」、「中小企業等において必要なセキュリティ対策」において考察した内容および前記「中小企業等向けのセキュリティ簡易保険サービスの在り方およびマーケティング方法の検討」を踏まえ、中小企業等の実態に即したセキュリティ対策サービスの要件について、次のとおり整理した。

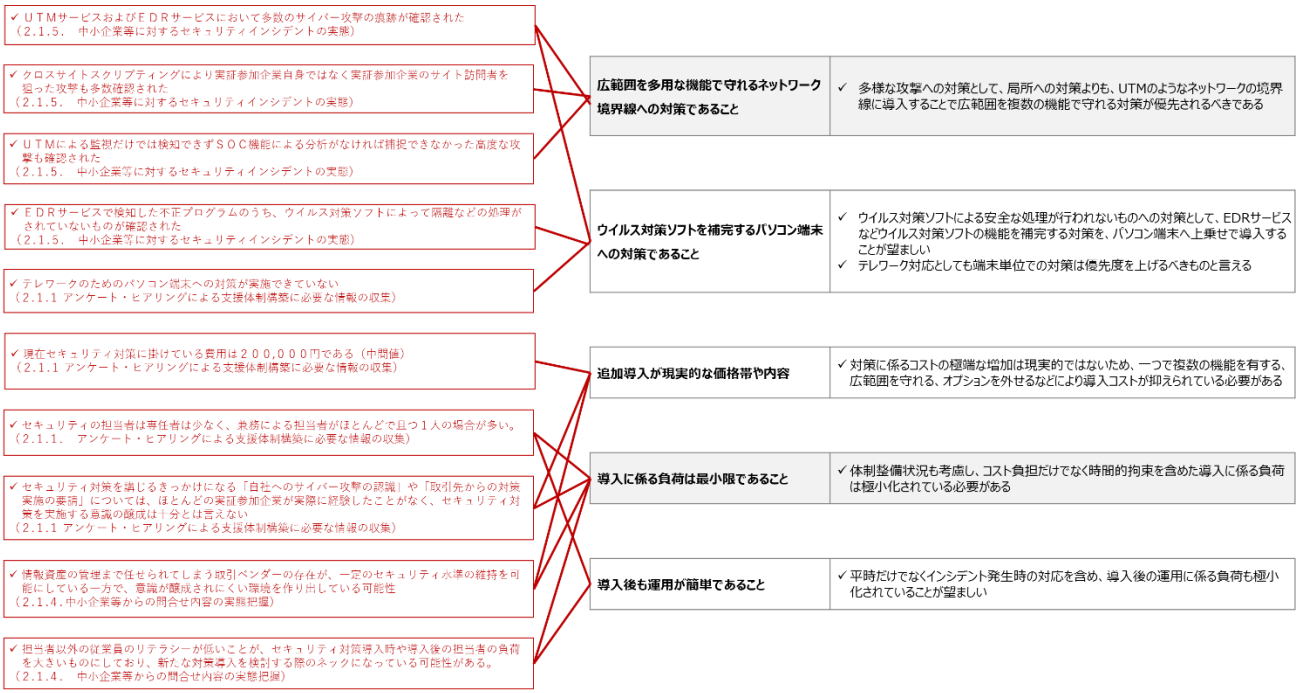

図 28 中小企業等の実態に即したセキュリティ対策サービスの要件

5.3.実証終了後に後続サービスとして提供するサービス

本事業で提供した UTM サービスと EDR サービスには、ＳＯＭＰＯリスクマネジメントが「令和元年中小企業向けサイバーセキュリティ事後対応支援実証事業（地域：神奈川県）」の実施を通じて得た知見などを踏まえて開発した SOMPO SOC と SOMPO SHERIFF を使用した。両サービスは本実証を通じて得られた中小企業等の実態に即したサービス像に合致しているため、実証終了後も当該両サービスを提供することとしている。以下に両サービスの内容を記載する。

5.3.1. SOMPO SOC サービス

(1) サービスの概要

「SOMPO SOC」は、ネットワーク内の監視対象機器のセキュリティログをクラウド上に自動で収集･分析し､不正アクセス等の重要なセキュリティインシデントを検知するサービスである。（2020 年 2 月販売開始）

企業側のネットワーク環境に設置された UTM のログをログ転送サーバー（Syslog サーバー）経由でＳＯＭＰＯリスクマネジメントの分析システムに送信し、分析結果をアラート通知する「セキュリティ監視サービス」と、「UTM（Syslog サーバーを含む。）運用管理サービス」で構成される。

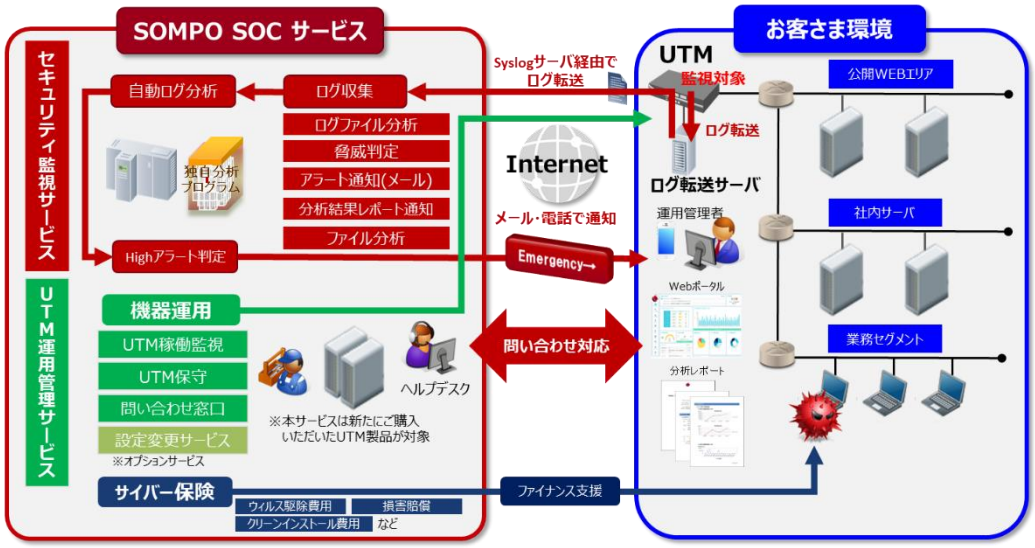

図 29 「SOMPO SOC」サービス全体像

(2) サービスの特長・機能

① 豊富な分析知見と高度ログ自動分析エンジン

24 時間 365 日セキュリティログを収集し、大企業向け SOC サービスで得られる脅威情報から新たに生成される分析ルールを適用させた高度自動分析エンジンにより、高品質なセキュリティ監視サービスを提供する。

② マネージド運用による業務負荷の軽減

UTM によるセキュリティの運用管理を総合的にサポートすることで、業務負荷の軽減を図る。UTM のログを分析した結果は「High」「Medium」「Low」の 3 段階に分類し、重要度に応じてメールや専用の Web ポータルを通じて通知されるため、専任のアナリスト等の要員手配が困難である中小企業等においても大きな運用負荷は掛からない。

Web ポータルでは、セキュリティインシデントの発生状況やログ分析状況を 24 時間 365 日

閲覧することが可能であり、アラート状況等のサマリー情報のほか、重要度の高いアラートの内容・解説についてのレポートを作成する。

中小企業等では、既に UTM を導入済みでも、実際には十分に運用できていないケースも多く、そのような場合でも「SOMPO SOC」のセキュリティ監視サービスは極めて有効である。

表 29 「SOMPO SOC」ログ分析結果における重要度

重要度	説明
High（重大）	お客様に緊急に確認・対応してもらう事象。 特定のシステムを狙っている可能性がある攻撃、または不正侵入やウイルス感染による致命的な被害にさらされている通信を検知したもの。 例） ・SQL インジェクションなどの公開サービスに対する危険な攻撃、または攻撃が成功した通信 ・内部からのボット・ワームの通信
Medium（注意）	攻撃による影響はない場合が多いものの、確認が必要な事象。 外部からの機械的な攻撃や、内部からの好ましくない通信を検知したもの。 例） ・外部からのボット・ワームによる感染活動 ・P2P ソフトの利用など内部からの情報漏えい等につながる可能性のある通信
Low（情報）	実害はないが情報として認識した方が良い事象。 危険度の低い通信を検知したもの。 例） ・外部からのボット・ワームのポートスキャン活動

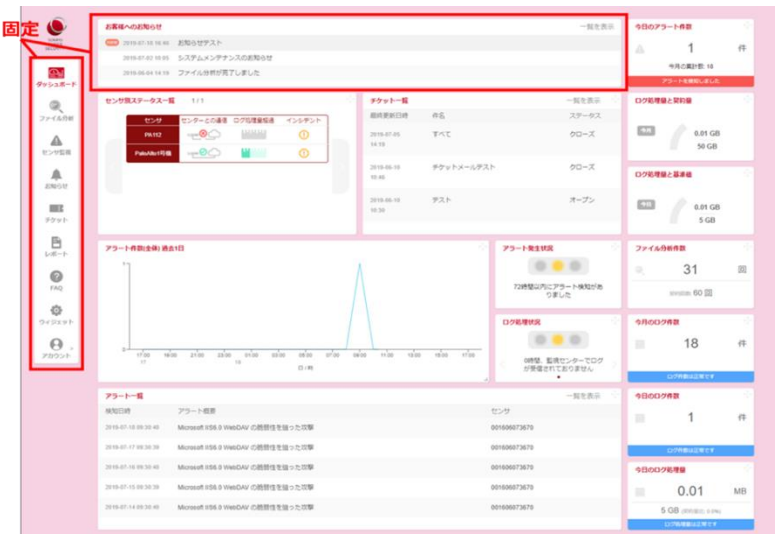

図 30 「SOMPO SOC」専用 Web ポータルイメージ（ダッシュボード）

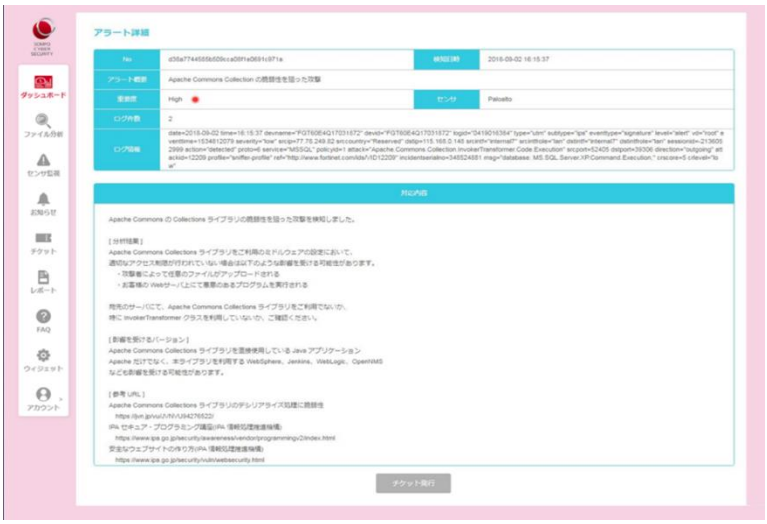

図 31　「SOMPO SOC」専用 Web ポータルイメージ（アラート詳細内容）

③ リーズナブルな費用

大企業向けサービスをベースに新たに開発した監視分析システムをクラウド上で稼働させることで、専門のアナリストがいなくても高度で高品質なセキュリティ常時監視サービスをリーズナブルな価格で提供することが可能となる。

④ サイバー保険を自動付帯

「SOMPO SOC」で検知したマルウェア感染やスキャン通信の対応に特化した専用のサイバー保険（引受保険会社：損害保険ジャパン株式会社）を自動付帯している。損害賠償責任だけでなく、ウイルス検索費用やウイルス駆除費用、オンサイト対応費用、データ保護費用、OS クリーンインストール費用等の各種費用損害についても当該サイバー保険の保険金が充当される。

（参考）

保険金額：300 万円

※ただし、1 事故当たり 30 万円を限度とする。

5.3.2. SOMPO SHERIFF

(1) サービスの概要

「SOMPO SHERIFF」[10]は、地域実証でも利用した EDR によって従来のウイルス対策ソフトでは防ぐことができずに侵入してきたウイルス感染による脅威を早期に検知し、検知した脅威については、ＳＯＭＰＯリスクマネジメントのデータ解析システムと専門のセキュリティエンジニアが調査・分析の上、緊急アラートメールでサービス利用者に通知し、早期駆除を可能にするサービスである。

なお、当該サービスについては、2020 年（令和 2 年）1 月 15 日開催の「第 5 回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事後対応支援実証事業の請負事業者による中小企業向けサービスの一例として紹介されている。

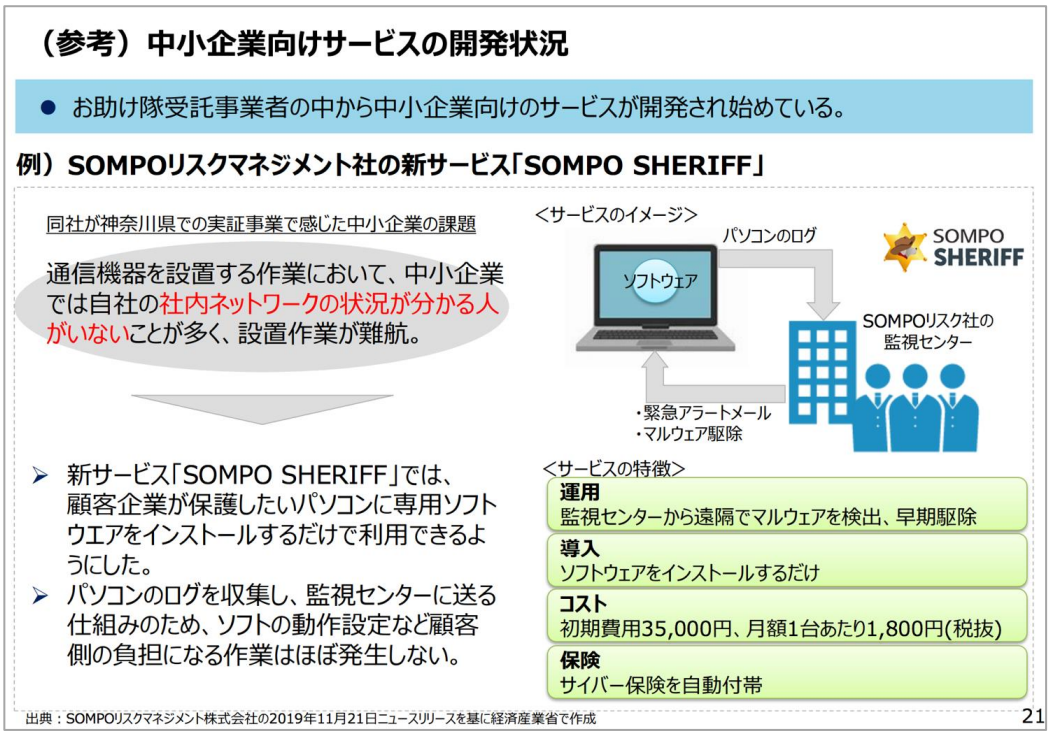

図 32 「第 5 回産業サイバーセキュリティ研究会ワーキンググループ 2（経営・人材・国際）」資料 3 事務局説明資料（抜粋）

(2) サービスの特長・機能

① ウイルス感染による脅威を早期検知（緊急アラート）

パソコン上のさまざまな挙動ログをＳＯＭＰＯリスクマネジメントのデータ解析システムと専門のセキュリティエンジニアが調査・分析することで、従来のウイルス対策ソフトで検知されない未知のウイルスも含めて、緊急性の高いウイルス感染の脅威を検知し、緊急アラートメールで通知する。

[10] ＳＯＭＰＯリスクマネジメント株式会社「SOMPO SHERIFF」：
https://www.sompocybersecurity.com/lp/sheriff/index.php（2021 年 1 月 19 日参照）

② 検知したウイルスを早期分析・駆除（脅威ハンティング機能）

緊急アラートで通知した脅威ファイルおよび被疑ファイルについては、専門のセキュリティエンジニアがリモートアクセスにより早期に分析・駆除する。

③ 面倒な設定や調整（チューニング）は不要

パソコンの挙動ログを収集するための EDR をインストールするだけで、サービス利用者の通常業務に支障を来たさない。また、サービス利用者側でのルール設定や機器の調整（チューニング）等の作業を生じさせない仕組みにしたことにより、中小企業では困難である専任のエンジニア等の要員手配が不要である。

④ 定期的なレポートでパソコンのリスクを“見える化”

定期的にセキュリティレポートを提供する。当該レポートは、ウイルス感染状況のほか、不正なプログラムサイト、フィッシングサイト等へのアクセス状況、セキュリティレベルの低い Wi-Fi への接続状況、USB の接続状況などのリスクを“見える化”するとともに、ソフトウェアのインストール状況やハードディスクの故障予兆などの従業員によるパソコンの利用状況を明らかにすることで、サービス利用者のセキュリティ対策の検討に資するものとなっている。

⑤ リーズナブルな費用

パソコンを常時監視・分析し、ウイルス感染時の事後対応までを中小企業等が自力で行うのは、人件費その他のコスト負担が大きく、現実的に困難である。「SOMPO SHERIFF」の導入により、監視・分析から駆除までのリスクマネジメントに係る費用を大幅に抑えることが可能である。

⑥ サイバー保険を自動付帯（標準プランのみ）

「SOMPO SHERIFF」で検知した緊急性の高いウイルス感染の対応に特化した専用のサイバー保険（引受保険会社：損害保険ジャパン日本興亜株式会社）を自動付帯している。上記②の分析・駆除費用については当該サイバー保険の保険金が充当されるため、分析・駆除に必要な追加費用負担が不要となり、円滑に対処することが可能となるため、サービス利用者にとっては更なる安心を得ることができる。

（参考）

保険金額：300 万円

※ただし、被疑ファイル分析・脅威ファイル駆除に係る費用については、1 アラート当たり 16,000 円を限度とする。

⑦ パソコン無料セキュリティ診断

「SOMPO SHERIFF」では、中小企業等が本サービスの導入検討に当たり、「パソコン無料セキュリティ診断」（1 か月間、無料で EDR を用いてパソコンの挙動ログを収集し、結果をセキュリティレポートとして発行するサービス）を利用できるようにしている。これは、費用対効果が分かりにくいセキュリティ対策について、現状ではセキュリティ対策費用を「投資」として捉えられていない中小企業等が無償で自社のリスクを認識し、セキュリティ対策が必要な投資であることを経営層に明示的に理解させる機会を設けることで、中小企業マーケットでの普及を図る試みである。

なお、「SOMPO SHERIFF」の申込みがあった場合、「無料セキュリティ診断」で発見された脅威ファイルについては、無料で駆除を行う。

6. 総括

6.1.本実証事業の総括

ＳＯＭＰＯリスクマネジメントでは、昨年度に神奈川県において実施したサイバーセキュリティお助け隊事業において、中小企業等に向けたサービスを普及させるためには、中小企業等の多くが「本報告書の目的 図 1　中小企業等の実態と課題」に記載されるような意識啓発に関する課題を抱えており、この課題の解決に向けて意識啓発の継続的な取組を行うことの重要性や、地域実証の結果として把握できた中小企業等の実態および中小企業等向け事後対応支援を実施する中で得た中小企業等向けのサイバーセキュリティ対策支援サービスの在り方についての考察を行った。また、こうした取組の中で得た知見を生かし、「SOMPO SOC」および「SOMPO SHERIFF」を開発した。

今年度の取組においては、中小企業等に向けたセキュリティ対策として UTM や EDR といった検知・防御サービスが有効であるとの仮説に基づき、中小企業等に向けられた攻撃の実態を踏まえ、このようなサービスを普及させるために効果的なアプローチ方法や課題、中小企業等に必要なセキュリティ対策や簡易保険の在り方などを見出すために地域実証を実施した。

本実証事業を通じて、UTM や EDR の有効性、意識啓発に関する課題、中小企業等に向けたアプローチ方法などが確認・検証され、中小企業等の実態に即したサービスについて「中小企業等の実態やニーズに応じた必要なセキュリティ対策の内容」に推奨要件を定義するとともに、当該推奨要件に適合したサービスを普及させるフェーズに取組を前進させることができた。これらの検証結果を本実証事業の成果としたい。

以上