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）

成果報告書

請負事業者：ＳＯＭＰＯリスクマネジメント株式会社

目次

0. はじめに

0.1. 本報告書の位置付け

本報告書は、『「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）」提案書』（以下「提案書」という。）の「1.6 成果報告書の作成」に基づく成果報告書として、２０１９年度（令和元年度）の「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）」（以下「本実証事業」という。）の実施内容及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。

0.2. 本報告書の目的

本実証事業は、特定地域の中小企業を対象として、サイバーセキュリティに関する悩みや、対策のニーズ、サイバー攻撃被害の実態等を把握するとともに、セキュリティインシデントが発生した際の支援体制の構築等に向けた実証を通じて、中小企業におけるサイバーセキュリティの意識向上を図り、中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを目的とする施策である。

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。）では、本実証事業の実施に当たり、我が国の中小企業の多くが「図 1　中小企業における課題」に記載されるような課題を抱えているものと認識し、このような課題を解決するためのサービスの在り方として、サービス受給側の中小企業にとって受け入れやすく、かつ、サービス提供側の事業者にとっても事業としての採算が取れる（ビジネスベースに乗る）仕組みが必要であるとの考え方に基づき、地域実証を通じて、こうした課題の実態を明らかにした上、サービスの受給側及び提供側の両側面から望まれる中小企業向けサービスの在り方を検討してきた。

本報告書は、本実証事業に係る取組の内容及び結果等を報告することを目的とし、我が国の中小企業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向けサービスの在り方などに関する検討に資することを期待するものである。

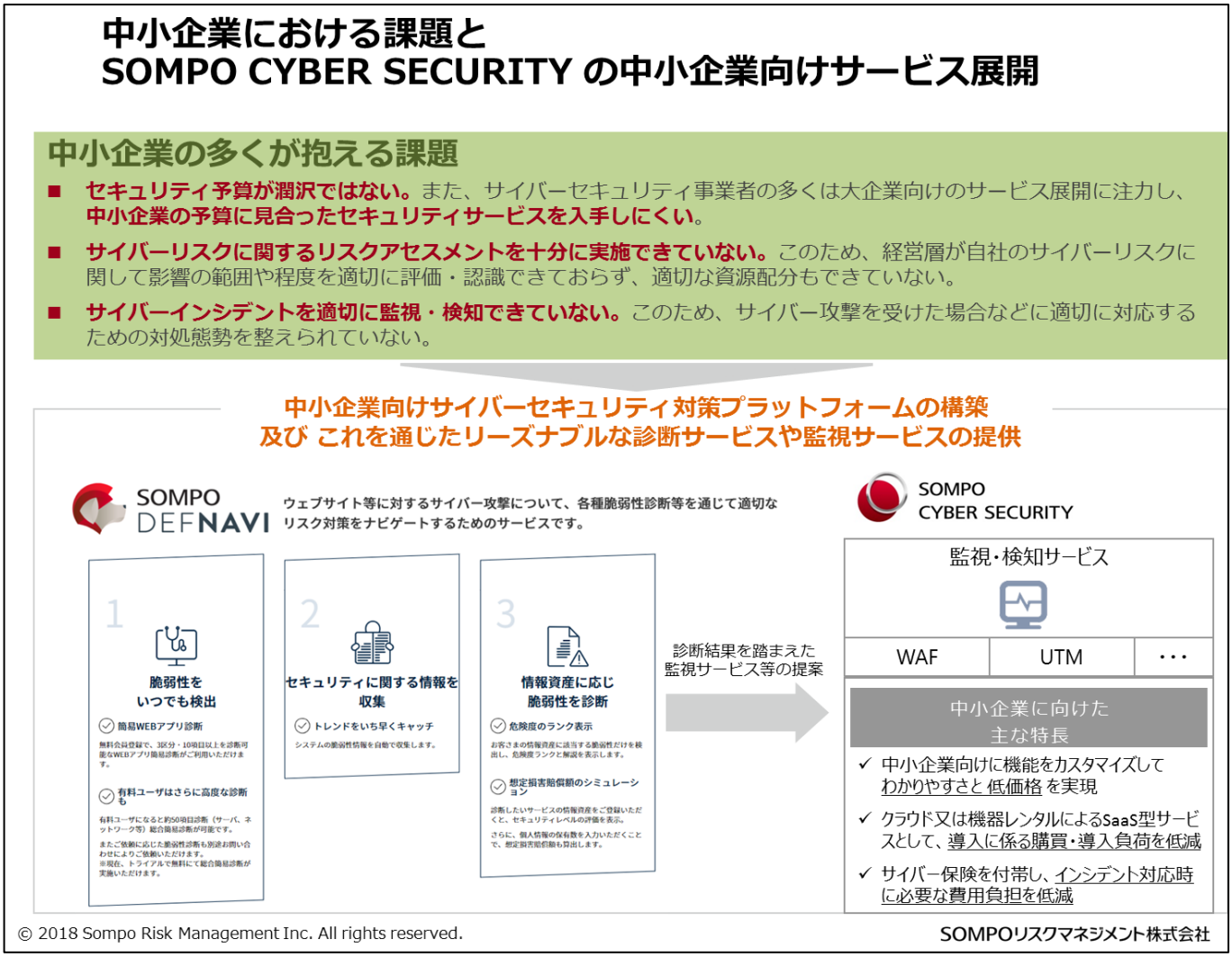

図 1　中小企業における課題

（経済産業省産業サイバーセキュリティ研究会ＷＧ２第３回会合ＳＯＭＰＯリスクマネジメント提出資料から抜粋）

0.3. 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、「1. 実施概要」、「2. 地域実証の結果」、「3. 考察（実施結果を踏まえた検討)」及び「4. 総括」の 4 部構成で編纂した。

「1. 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及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。

「2. 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の実態及び中小企業向け事後対応支援を実施する中で得た中小企業向け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。

「3. 考察（実施結果を踏まえた検討)」では、本実証事業を通じて得られた中小企業の実態等を踏まえ、中小企業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を整理し、中小企業向けセキュリティ対策サービス、サイバー保険及び普及啓発の在り方について考察する。

「4. 総括」では、本実証事業の成果及び考察した在り方をより強力に推進していくための提言について記載する。

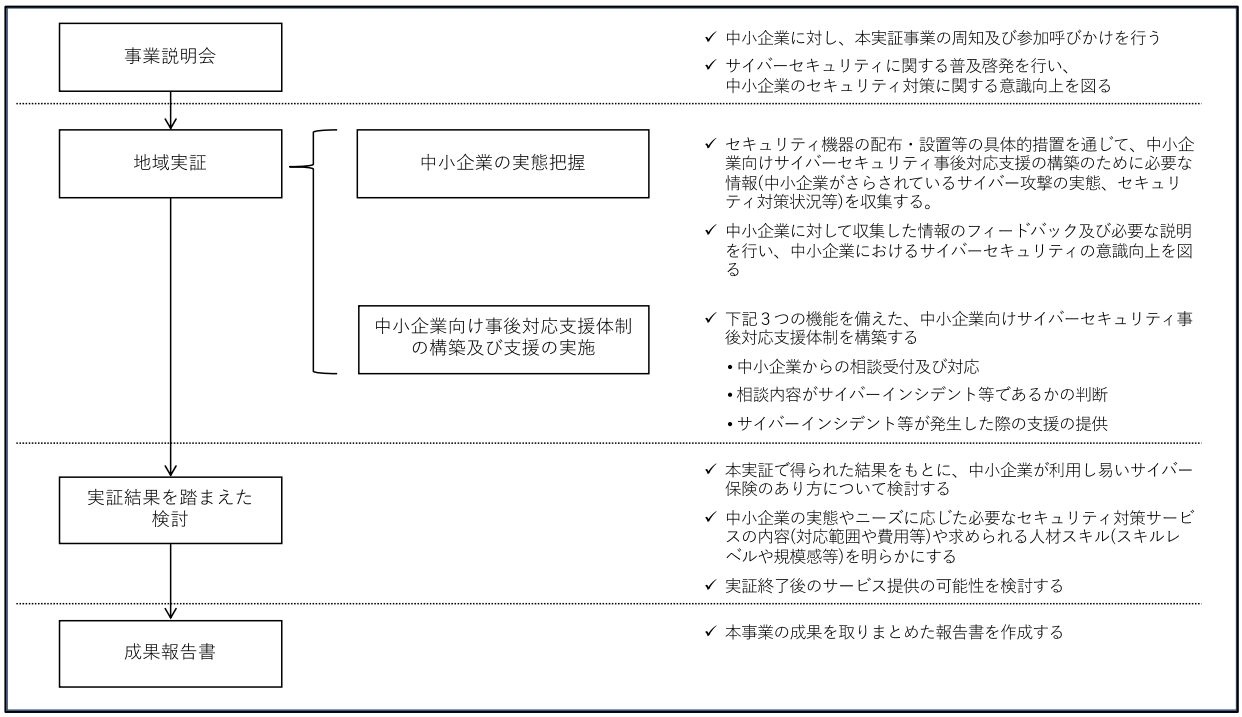

図 2　本実証事業の枠組み

1. 実施概要

1.0. 全体概要

1.0.1. 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、「神奈川県」において実施した。

① 地域の選定理由及び妥当性評価

神奈川県には、自動車を始めとする重要製造業のサプライチェーンを構成する中小企業が集積しているだけでなく、超高齢社会到来といった我が国の重要課題の解決や、新技術に基づく産業競争力強化のための新たな価値を創造する拠点として、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も多く所在していることから、神奈川県は、我が国において極めて重要性の高い産業拠点であり、また中小企業防護の必要性の高い地域であるといえる。このような地域の重要性及び中小企業防護の必要性を踏まえ、地域実証の対象地域として神奈川県を選定した。

なお、神奈川県は、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い。また、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

神奈川県は、関東平野の南西部に位置し、東部は東京湾、南部は相模湾に面し、北部から北西部を丹沢・箱根山系に囲まれた丘陵地及び平坦な低地を中心とする地域である。豊かな自然に恵まれながら首都圏の一角に位置する神奈川県は、横浜港、川崎港、横須賀港といった国際貿易港を擁し、２０１０年（平成２２年）に再拡張・国際化された東京国際空港（羽田空港）に隣接するなど、アジア、そして世界に開かれた国際交流拠点としての役割を果たしている。また、首都圏の中に位置する神奈川県は、商業、居住などさまざまな機能を担っている。

イ．経済的特徴

神奈川県の総生産は、２０１４年（平成２６年）度で約３０．３兆円と、フィリピンやフィンランドの一国の経済に匹敵する高い経済力を有している[1]。

また、神奈川県の産業構造は、付加価値額[2]で見ると、「製造業」（２１．２％）、「卸売業、小売業」（１７．０％）、「医療、福祉」（９．４％）、「学術研究、専門・技術サービス業」（７．８％）の順、従業者数で見ると、「卸売業、小売業」（１９．６％）、「製造業」（１４．５％）、「医療、福祉」（１２．０％）、「宿泊業、飲食サービス業」（１０．４％）の順となっている。これらの産業を付加価値額で全国と比較すると、「製造業」全国４位、「卸売業、小売業」同４位、「医療、福祉」同３位、「学術研究、専門・技術サービス業」同２位、「宿泊業、飲食サービス業」同３位と、製造業を中心に、多様で活発な産業活動が行われている[3]。

---

[1] 平成２６年度神奈川県県民経済計算

[2] 企業等の生産活動によって新たに生み出された価値のことで、生産額から原材料等の中間投入額を差し引くことによって算出できる。付加価値額＝売上高－費用総額＋給与総額＋租税公課。

[3] 経済センサス-活動調査（平成２４年）

（2） 実施期間

① 本実証事業の実施期間

２０１９年（令和元年）６月１３日から２０２０年（令和２年）２月１７日まで

② 地域実証の実施期間

２０１９年（令和元年）８月１日から２０２０年（令和２年）１月３１日まで

（3） 参加企業数

本実証事業への申込企業数：１５０社
（うち、２０２０年（令和２年）１月３１日時点で地域実証を開始できた企業数[4]：１１０社）

表 1 参加企業数の内訳

参加申込企業数		150社
（内訳）実証開始企業数		110社
	UTM監視・検知サービス	38社
	クラウド型WAFサービス	0社
	パソコン監視分析サービス	72社
導入不可・中止企業数		40社

1.0.2. 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。

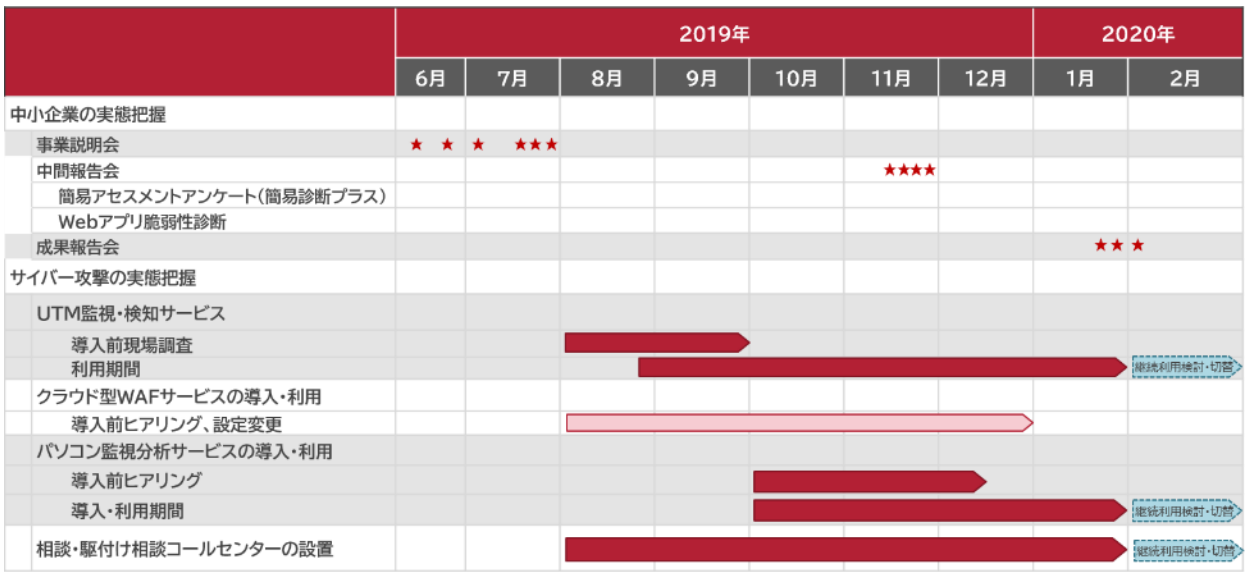

図 3 実施スケジュール（概要）

[4] 対象とする中小企業において、次のいずれかの状態になったことをもって、地域実証を開始したものとみなす。
①ＵＴＭを設置し、ログの取得が可能になった状態
②ＤＮＳの設定を変更し、クラウド型ＷＡＦによる検知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

1.0.3. 本実証事業の実施体制

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） ＵＴＭ監視・検知サービス

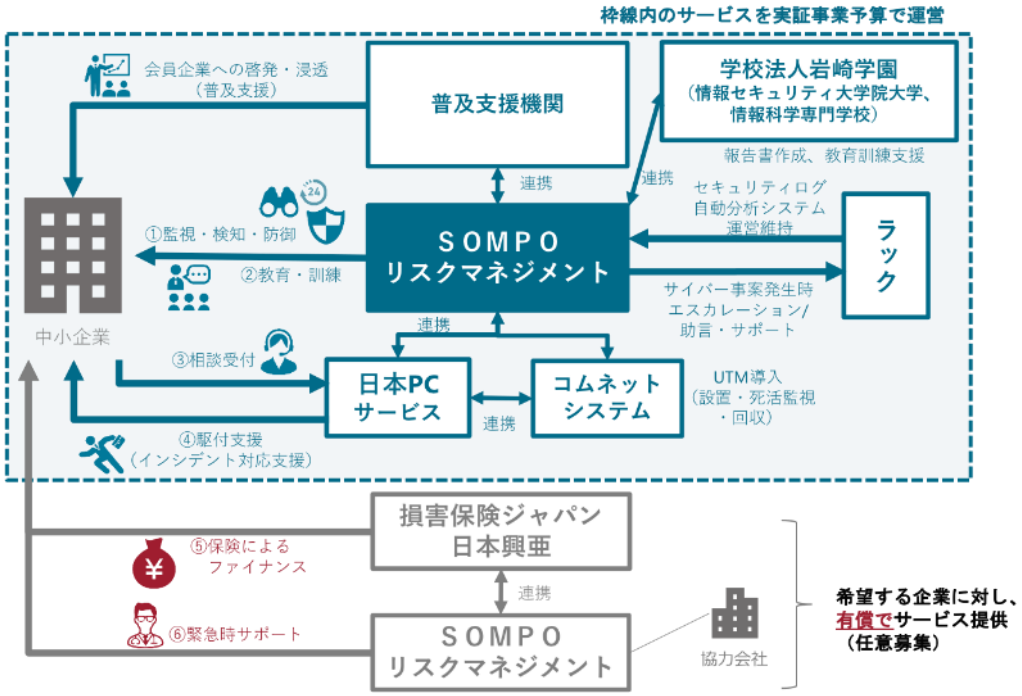

図 4 ＵＴＭ監視・検知サービスの実施体制

（2） クラウド型ＷＡＦサービス

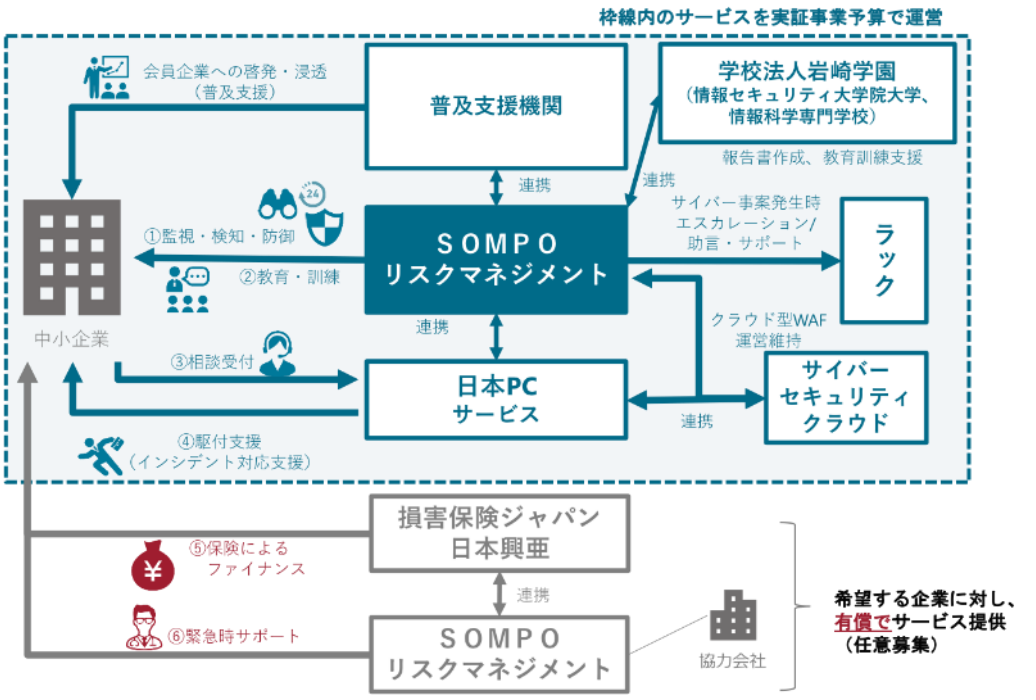

図 5 クラウド型ＷＡＦサービスの実施体制

（3） パソコン監視分析サービス

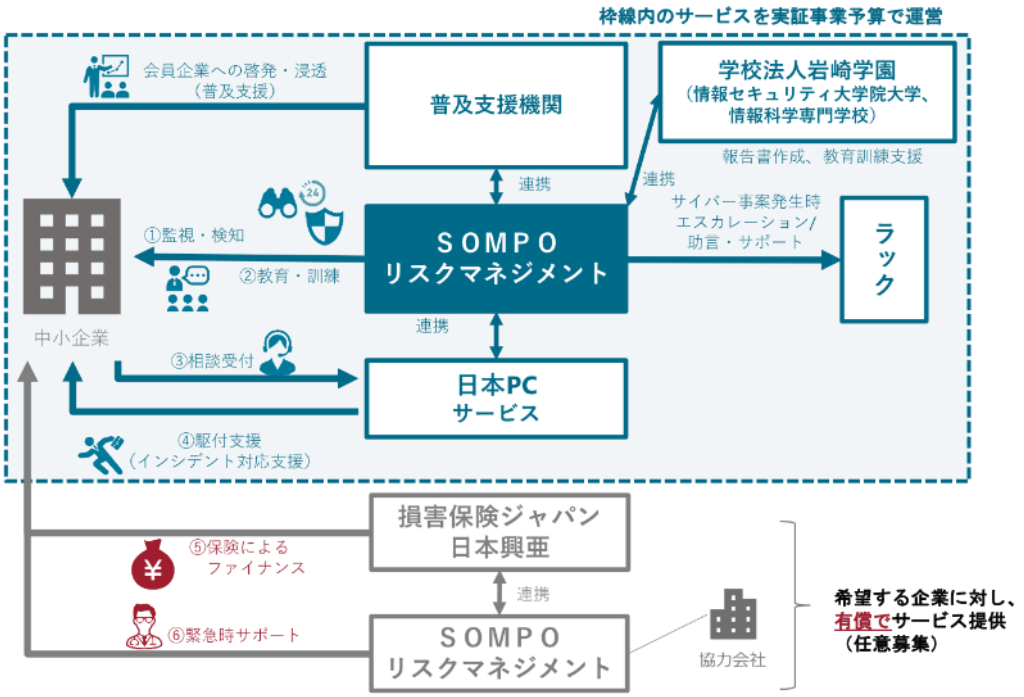

図 6　パソコン監視分析サービスの実施体制

1.1. 事業説明会の実施概要

本実証事業では、神奈川県に所在する中小企業を対象に、事業説明会として、「募集説明会」（２０１９年（令和元年）6月開催)、「中間報告会」（同年１１月開催）及び「成果報告会」（２０２０年（令和２年）１月～２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。

1.1.1. 募集説明会

（1） 開催内容

募集説明会は、神奈川県に所在する中小企業に対し、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

２０１９年（令和元年）６月１４日（金） １５時３０分～１８時００分

② 開催場所

損害保険ジャパン日本興亜株式会社（以下「損害保険ジャパン日本興亜」という。）
横浜ビル会議室

③ 参加者数（定員数）

１７名（１２０名）

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」
独立行政法人情報処理推進機構（以下「IPA」という。）
ⅲ. 「Society5.0 とサイバーリスク　今必要な戦略マネジメントという発想」
情報セキュリティ大学院大学
ⅳ. 「中小企業にも迫るサイバーリスク　サイバー119 と JSOC のデータから」
株式会社ラック（以下「ラック」という。）
ⅴ. 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について
ＳＯＭＰＯリスクマネジメント
ⅵ. 閉会のご挨拶
損害保険ジャパン日本興亜

（2） 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、損害保険ジャパン日本興亜神奈川本部と連携し、同社の代理店網を活用して中小企業の参加を呼び掛けた。呼掛け先の中小企業のスケジュールの都合等により、募集説明会の参加状況が芳しくなかったことから、下記のとおり募集説明会を複数回追加開催した。

表 2　募集説明会の追加開催状況

開催日時	参加者数（定員数）
２０１９年6月２８日（金）　１５時３０分～１７時００分	２（３０）
２０１９年7月　９日（火）　１０時００分～１１時３０分 １６時００分～１７時３０分 ※同日で午前・午後の２回開催	９（３０）
２０１９年7月１９日（金）　１６時００分～１７時３０分	11（６０）
２０１９年7月２５日（木）　１０時００分～１１時３０分 １６時００分～１７時３０分 ※同日で午前・午後の２回開催	８（６０）
２０１９年7月３０日（火）　１０時００分～１１時３０分 １６時００分～１７時３０分 ※同日で午前・午後の２回開催	５（６０）

また、地域における中小企業のサイバーセキュリティ対策強化に対する目的意識を共有するサプライチェーンの上流企業、地域金融機関、地方公共団体、中小企業関連団体等との連携についても画策した。サプライチェーンの上流企業（自動車製造メーカー及び Tier１企業）については、下請代金支払遅延等防止法（昭和３１年法律第１２０号）第４条１項６号に規定する「役務の利用強制」に抵触することへの危惧などの理由から、当初想定していた形での協力を得ることができなかった。地域金融機関、地方公共団体、中小企業関連団体については、店頭にチラシを置くなどの募集活動に係る一定の支援協力を得ることができたが、参加企業の獲得にはつながらなかった。

（3） 募集説明会に関する追加的な取組

参加企業に対して、サイバーセキュリティに関する普及啓発及び中小企業のセキュリティ対策に関する意識向上についても付随的な目的とし、これを狙った講演を募集説明会のプログラムに盛り込んだ。

普及啓発の観点からは、情報セキュリティ大学院大学から、 Society5.0 で実現する「つながる社会」におけるサプライチェーンリスク等の解説を行うとともに、価値創造と危機管理の両面からサイバーセキュリティの重要性を説いた。

意識向上の観点からは、ラックから、同社の「サイバー１１９」の出動状況や「ＪＳＯＣ」で検知した重要インシデントの発生状況を紹介し、中小企業においても現実にサイバー攻撃の影響が及んでいることなどを解説した。

1.1.2. 中間報告会

（1） 開催内容

中間報告会は、地域実証を約３か月間実施して得られた中小企業におけるセキュリティインシデントや被害の発生状況、中小企業からの問合せ内容などをフィードバックすることで、中小企業におけるサイバーセキュリティの意識向上を図ることを目的として開催した。

① 開催日時

（第１回）２０１９年（令和元年）１１月１９日（火） １０時００分～１２時００分
（第２回）２０１９年（令和元年）１１月２５日（月） １５時００分～１７時００分
（第３回）２０１９年（令和元年）１１月２７日（火） １０時００分～１２時００分
（第４回）２０１９年（令和元年）１１月２７日（火） １５時００分～１７時００分
（第５回）２０１９年（令和元年）１１月２９日（金） １５時００分～１７時００分

② 開催場所

（第１回）損害保険ジャパン日本興亜　馬車道ビル会議室
（第２回）損害保険ジャパン日本興亜　馬車道ビル会議室
（第３回）損害保険ジャパン日本興亜　第１伊藤ビル会議室
（第４回）損害保険ジャパン日本興亜　第１伊藤ビル会議室
（第５回）損害保険ジャパン日本興亜　馬車道ビル会議室

③ 参加者数（定員数）

（第１回）１２名（６０名）
（第２回）　７名（６０名）
（第３回）　３名（２５名）
（第４回）　１名（２５名）
（第５回）　４名（６０名）

④ 来場した参加申込企業の数

１９社

⑤ 議事次第

ⅰ. 事業概要説明

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅱ. 「中小企業におけるサイバーセキュリティの状況と課題」
（実証事業を通じて見えてきた状況についてケーススタディを通じて考察）

- 不正な通信の発生状況
- 導入過程で見えてきた課題
- 状況を踏まえた中小企業がサービス導入する際の留意事項
- 導入できないケースに学ぶ事前確認注意点、既存ベンダーの利用の仕方

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

iii. 「中小企業における情報セキュリティ対策支援のご紹介」

ＩＰＡ[5]

iv. 「セキュリティに関する簡易アンケート」

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

（2） 参加企業確保のための取組

募集説明会の開催に当たり、中小企業のスケジュール調整が困難であり追加開催を行わざるを得なかった経緯を鑑みて、中間報告会募集用の専用ウェブサイトを構築して呼び込みやすくするとともに、あらかじめ開催日時と場所を複数設定することにより中小企業がスケジュール調整しやすくなるように配慮した。

（3） 中間報告会に関する追加的な取組

中小企業のサイバーセキュリティ対策状況を把握することを目的として、「サイバーリスク簡易診断アンケート」によりサイバー攻撃対策として考慮すべき「組織的」、「人的」、「物理的」及び「技術的」な対策を中心にサイバーリスクへの対応状況を把握するとともに、「情報漏えい」、「ＤｏＳ攻撃」、「ＩＴ（クラウド）サービス停止」、「金融取引」及び「恐喝」の五つのシナリオに基づく想定損害額を簡易算出して把握することにしていたが、中小企業が当初の想定以上に自らの対策状況などを認識していないことが地域実証を通じて明らかになったことから、独力でアンケートを適切に回答できない可能性が高いと判断し、中間説明会において各設問の解説を交えつつアンケートを実施した。

1.1.3. 成果報告会

（1） 開催内容

成果報告会は、地域実証を約６か月間実施して得られた中小企業におけるセキュリティインシデントや被害の発生状況、中小企業からの問合せ内容などをフィードバックすることで、中小企業におけるサイバーセキュリティの意識向上を図ることを目的として開催した。

① 開催日時

（第１回）２０２０年（令和２年）１月２４日（金）　１５時００分～１７時００分
（第２回）２０２０年（令和２年）１月２７日（月）　１０時００分～１２時００分
（第３回）２０２０年（令和２年）２月　４日（火）　１５時００分～１７時００分

② 開催場所

（第１回）損害保険ジャパン日本興亜　第１伊藤ビル会議室
（第２回）損害保険ジャパン日本興亜　馬車道ビル会議室
（第３回）損害保険ジャパン日本興亜　馬車道ビル会議室

[5] 第１回開催のみ登壇

③ 参加者数（定員数）

（第１回）　５名（２５名）
（第２回）１６名（６０名）
（第３回）１５名（６０名）

④ 来場した参加申込企業の数

２７社

⑤ 議事次第

ⅰ．本実証事業の概要（実施した内容、スキーム）

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅱ．神奈川県における中小企業の状況

（本実証事業を通じて見えてきた状況）

・参加者数や属性等
・簡易診断プラスの状況
・想定損害額の中央値　　など

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅲ．神奈川県の中小企業へのサイバー攻撃の実態

・ＵＴＭ監視・検知サービスで検知されたサイバーインシデントの状況
・パソコン監視分析サービスで検知されたサイバーインシデントの状況
・中小企業からの問合せ内容　　など

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅳ．地域実証で確認された脅威

ⅰ）インシデント事例（Ｘ社の事例）
ⅱ）ＩＰＳ機能が遮断した通信の代表的なもの
ⅲ）Web Blocker で遮断した通信の代表的なサイト

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅴ．中小企業向けのセキュリティ対策ツールと保険
（商品付帯と上乗せの使い分けを説明　導入時のネックと一緒に）

ＳＯＭＰＯリスクマネジメント　サイバーセキュリティ事業本部

ⅵ．「中小企業における情報セキュリティ対策支援のご紹介」

ＩＰＡ[6]

[6] 第２回開催のみ登壇

図 7　成果報告会（１月２７日開催）の様子

（2） 参加企業確保のための取組

中間報告会と同様に、成果報告会募集用の専用ウェブサイトを構築して呼び込みやすくするとともに、あらかじめ開催日時と場所を複数設定することにより中小企業がスケジュール調整しやすくなるように配慮した。

（3） 成果報告会に関する追加的な取組

なるべく多くの実証開始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発生したセキュリティインシデントの事例を想定損害額と共に紹介し、中小企業がサイバー攻撃の脅威を自分事として受け止めやすいよう工夫した講演を行い、セキュリティ対策の必要性について具体的に訴求した。

1.2. 地域実証の実施概要

1.2.1. 参加事業者の概況

（1） 参加事業者の選定条件

本実証事業では、中小企業基本法（昭和３８年法律第１５４号）第２条第１項に規定する中小企業者のうち、神奈川県内に主たる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） 参加事業者の構成

本実証事業への参加意思を確認できた中小企業（以下「参加申込企業」という。）は、全体で１５０社であった。また、２０１９年（令和元年）１２月３１日時点で地域実証を開始できた中小企業（以下「実証開始企業」という。）は１１０社であった。

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開始企業の内訳は、下記のとおりであった。

（実証開始企業の業種別構成：全体）

業種分類	社数
J 金融業、保険業	34
I 卸売業、小売業	15
R サービス業(他に分類されないもの)	9
G 情報通信業	9
E 製造業	8
D 建設業	8
P 医療、福祉	6
N 生活関連サービス業、娯楽業	5
L 学術研究、専門･技術サービス業	5
M 宿泊業、飲食サービス業	4
K 不動産業、物品賃貸業	3
H 運輸業、郵便業	2
B 漁業	1
O 教育、学習支援業	1
総計	110

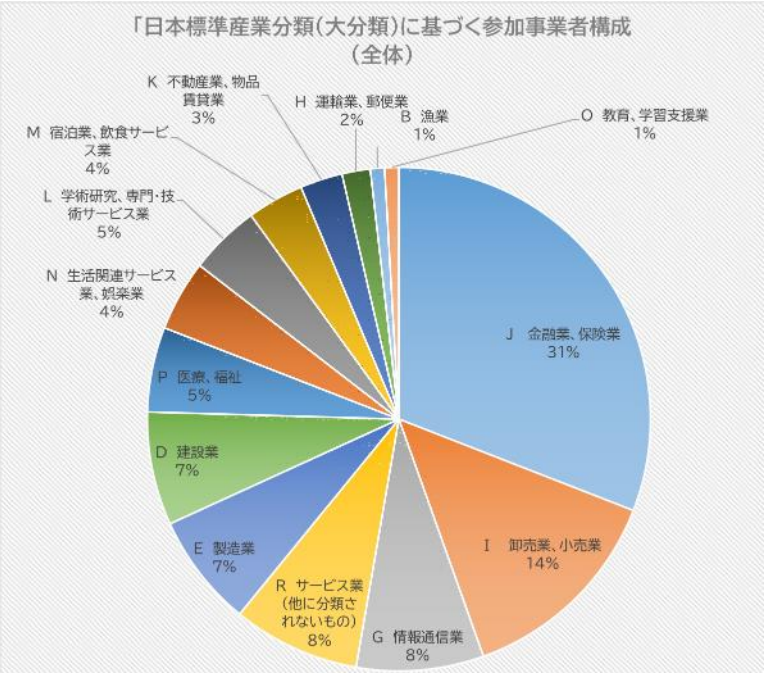

図 8 「日本標準産業分類（大分類）に基づく実証開始企業構成（全体）

（実証開始企業の業種別構成：ＵＴＭ監視検知サービス）

業種分類	社数
E 製造業	7
J 金融業、保険業	6
D 建設業	5
N 生活関連サービス業、娯楽業	4
P 医療、福祉	3
M 宿泊業、飲食サービス業	3
I 卸売業、小売業	3
R サービス業(他に分類されないもの)	2
G 情報通信業	2
H 運輸業、郵便業	2
B 漁業	1
総計	38

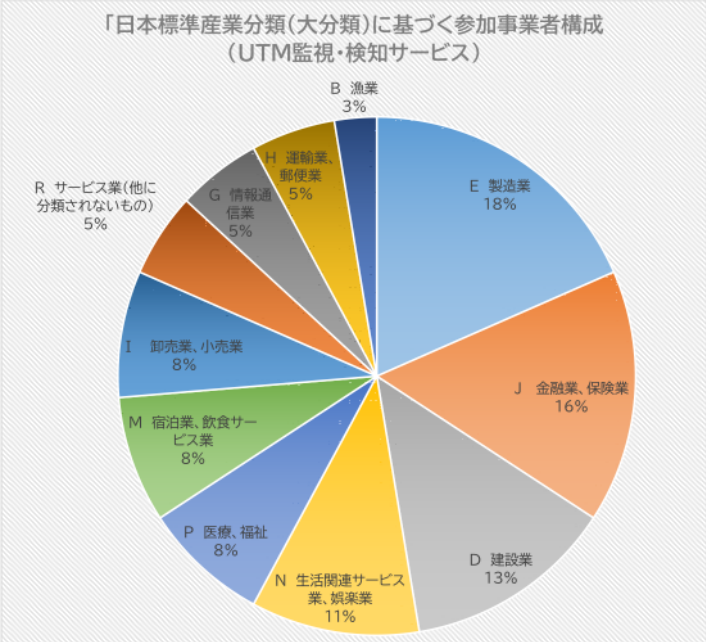

図 9　「日本標準産業分類（大分類）に基づく実証開始企業構成（ＵＴＭ監視・検知サービス）

（実証開始企業の業種別構成：パソコン監視分析サービス）

業種分類	社数
J 金融業、保険業	28
I 卸売業、小売業	12
R サービス業(他に分類されないもの)	7
G 情報通信業	7
L 学術研究、専門・技術サービス業	5
P 医療、福祉	3
D 建設業	3
K 不動産業、物品賃貸業	3
M 宿泊業、飲食サービス業	1
E 製造業	1
N 生活関連サービス業、娯楽業	1
O 教育、学習支援業	1
総計	72

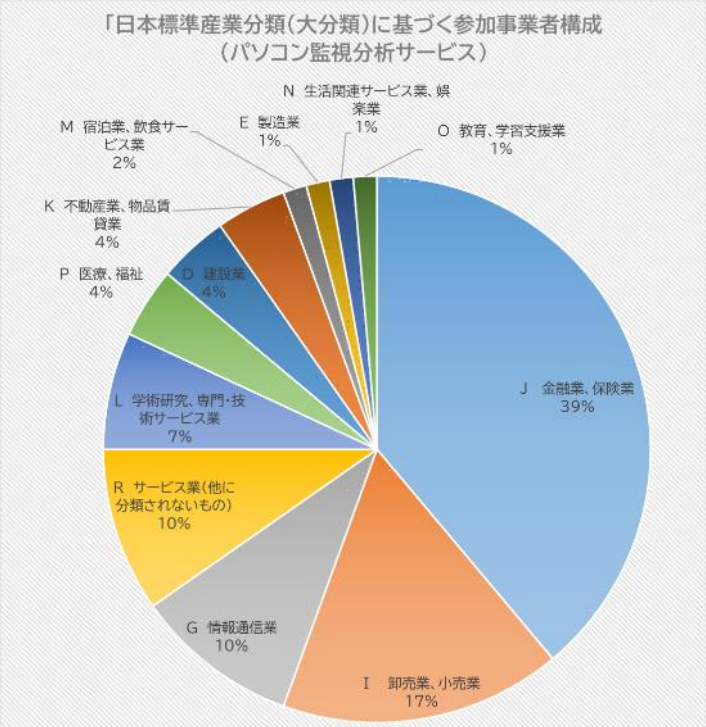

図 10　「日本標準産業分類（大分類）に基づく実証開始企業構成（パソコン監視分析サービス）

② 従業員規模別構成

参加事業者の従業員数別の内訳は、下記のとおりであった。

（実証開始企業の従業員規模別構成：全体）

行ラベル	個数 / 従業員数②
①1~5名	36
②6~10名	24
③11~20名	22
④21名~30名	5
⑤31名~40名	2
⑥41名~50名	6
⑦51名~60名	1
⑧61名~70名	3
⑨71名~80名	1
⑩81名~90名	1
⑪91名~100名	5
⑫100名超	4
総計	110

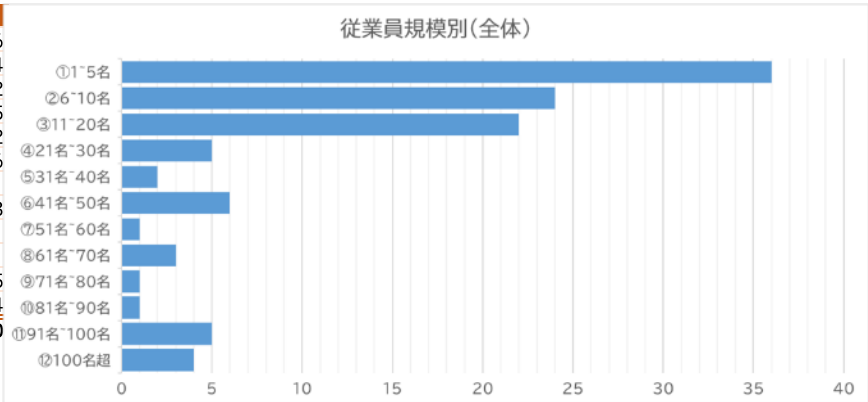

図 11　従業員規模別の実証開始企業構成（全体）

（実証開始企業の従業員規模別構成：ＵＴＭ監視・検知サービス）

行ラベル	個数 / 従業員数②
①1~5名	10
②6~10名	4
③11~20名	7
④21名~30名	3
⑤31名~40名	1
⑥41名~50名	4
⑦51名~60名	1
⑧61名~70名	2
⑩81名~90名	1
⑪91名~100名	3
⑫100名超	2
総計	38

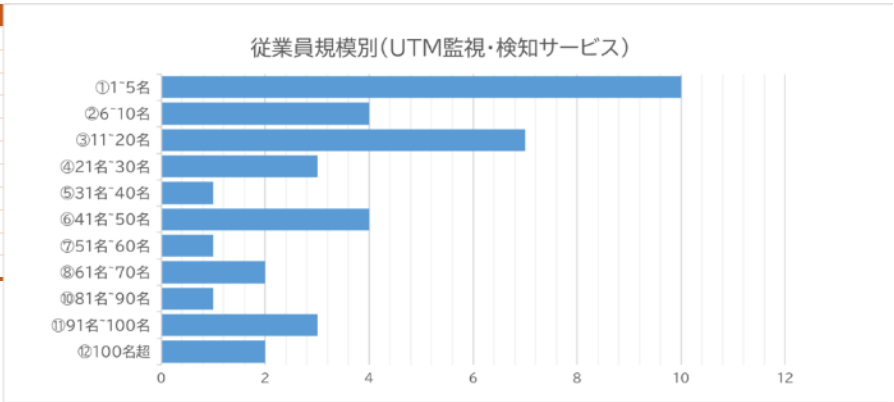

図 12　従業員規模別の実証参加企業構成（ＵＴＭ監視・検知サービス）

（実証開始企業の従業員規模別構成：パソコン監視分析サービス）

行ラベル	個数 / 従業員数②
①1~5名	26
②6~10名	20
③11~20名	15
④21名~30名	2
⑤31名~40名	1
⑥41名~50名	2
⑧61名~70名	1
⑨71名~80名	1
⑪91名~100名	2
⑫100名超	2
総計	72

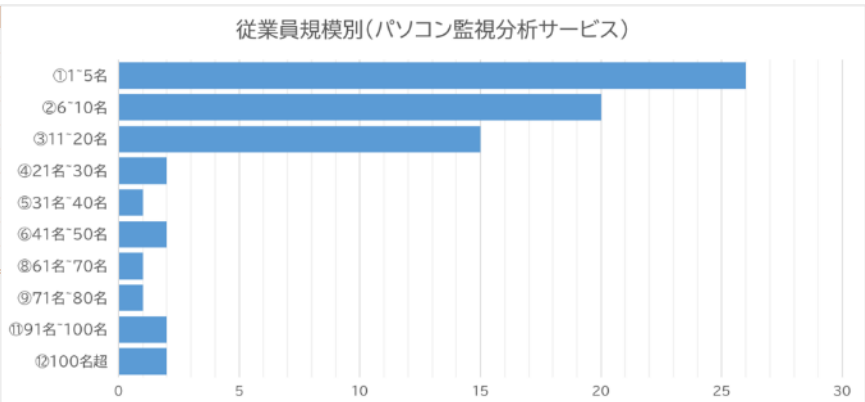

図 13　従業員規模別の実証参加企業構成（パソコン監視分析サービス）

1.2.2. 中小企業の実態を把握するための取組

中小企業向けサイバーセキュリティ事後対応支援の構築のために必要な情報（中小企業がさらされているサイバー攻撃の実態、セキュリティ対策状況、中小企業における困り事（問合せ内容）の実態等）を収集するため、参加申込企業に対し、「ＵＴＭ監視・検知サービス」、「クラウド型ＷＡＦサービス」又は「パソコン監視分析サービス」のいずれかの導入を行った。また、「サイバーリスク簡易診断アンケート」及び「ＷＥＢアプリ簡易診断」を実施した。

各サービスについて実施した内容は、次のとおりである。

（1） ＵＴＭ監視・検知サービス

①ＵＴＭ監視・検知サービス － サービス概要

実証開始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・ジャパン株式会社のＵＴＭ[7] 「Firebox M370 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については、当該機器を活用した。以下「ＵＴＭ」という。）及び Syslog サーバーを設置し、ＵＴＭのセンサー（ＩＰＳ[8] 機能及びＵＲＬフィルタリング（Web Blocker）機能）からのアラート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」に送信し分析することで、導入企業におけるセキュリティインシデントを検出するものである。

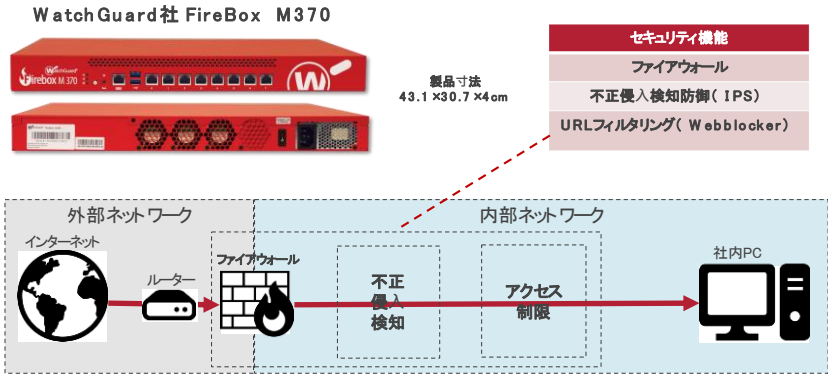

図 14 ＵＴＭの機能概要

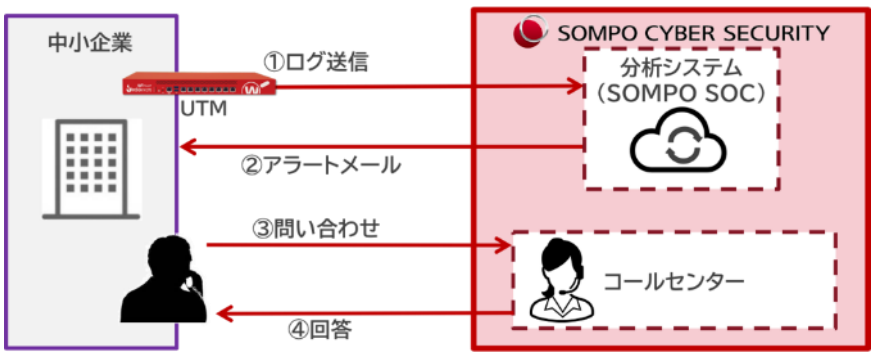

図 15 ＵＴＭ監視・検知サービスのサービス概念図

[7] 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

[8] ＩＰＳ（Intrusion Prevention System）：不正侵入検知防御システム

②ＵＴＭ監視・検知サービス　－　導入方法

ＵＴＭ及び Syslog サーバーの導入については、株式会社コムネットシステム[9] 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、設置及び動作確認を実施することにより、中小企業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。

発注から納品までの全体フロー

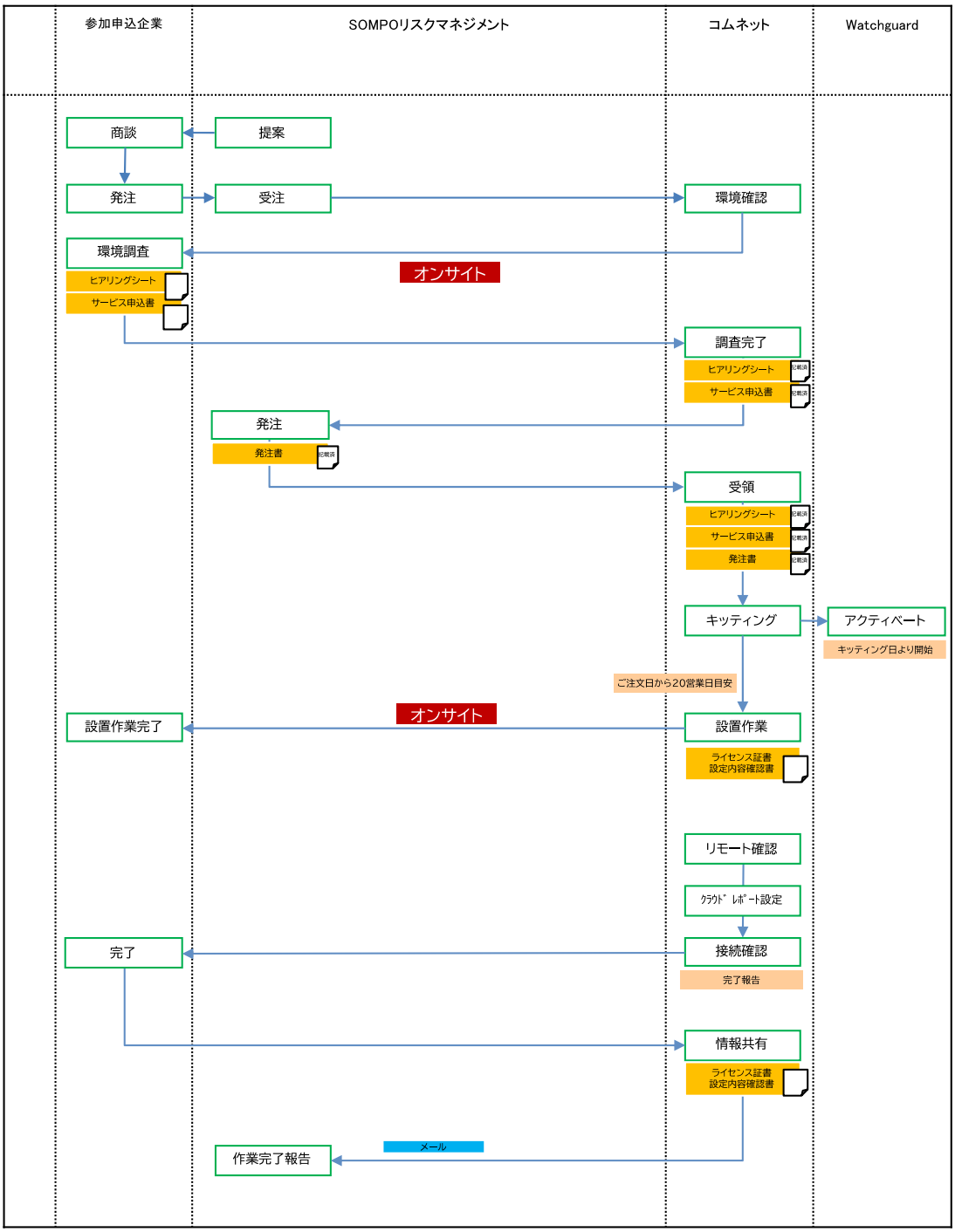

図 16　ＵＴＭ監視・検知サービスの導入フロー

[9] https://www.comnetsystem.co.jp/

③ＵＴＭ監視・検知サービス　－　導入状況

ＵＴＭ監視・検知サービスについては、５０社への導入を上限として、参加申込企業に対するサービス提案を実施した。最終的に６１社への提案を行い、３８社への導入を行った。

表 3　ＵＴＭ監視・検知サービスの導入状況

ＵＴＭ監視・検知サービス	
提案企業数	61 社
うち、導入不可・中止	23 社
導入完了企業数 （導入割合）	38 社 (62%)

(2)　クラウド型ＷＡＦサービス

① クラウド型ＷＡＦサービス　－　サービス概要

中小企業に対して、ＳＯＭＰＯリスクマネジメントが提供するクラウド型ＷＡＦ[10] サービス（以下「ＷＡＦ」という。）を用いて、中小企業におけるセキュリティインシデントを検出するものである。

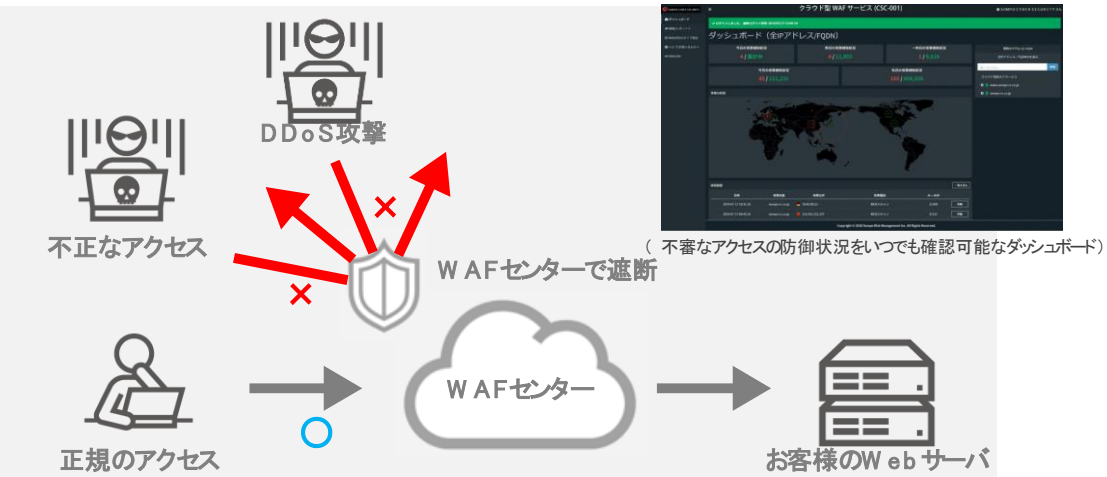

図 17　クラウド型ＷＡＦサービスのサービス概念図

② クラウド型ＷＡＦサービス　－　導入方法

本実証事業では、中小企業側でＤＮＳ[11] サーバーの設定変更を行うだけで導入することができるクラウド型のサービスを適用することにより、中小企業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。

---

[10] ＷＡＦ（Web Application Firewall）：ウェブアプリケーションの脆弱性を悪用した攻撃から当該ウェブアプリケーションを保護するセキュリティ対策の一つ

[11] ＤＮＳ（Domain Name System）：ドメインとＩＰアドレスを対応付けて管理するシステム

③ クラウド型ＷＡＦサービス － 導入状況

クラウド型ＷＡＦサービスについては、７５社への導入を上限として、参加申込企業に対するサービス提案を実施した。

しかしながら、ＷＡＦに対するニーズが想定よりも低かったことや、導入に当たり参加申込企業が自らＤＮＳサーバーの設定変更を行う必要がある中で、システム専任担当者がいないなどの理由によって業務で利用しているネットワーク設定の変更を行うための意思決定ができない、システムベンダーに丸投げしているため設定変更ができないなど、導入に向けた調整が不能又は時間が掛かるケースが発生した。この結果、サービス提案を行った１２社の全てが導入不可となった。

表 4　クラウド型ＷＡＦサービスの導入状況

クラウド型ＷＡＦサービス	
提案企業数	12 社
うち、導入不可・中止	12 社
導入完了企業数 （導入割合）	0 社 (0%)

（3） パソコン監視分析サービス

① パソコン監視分析サービス － サービス概要

実証開始企業に対して、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。

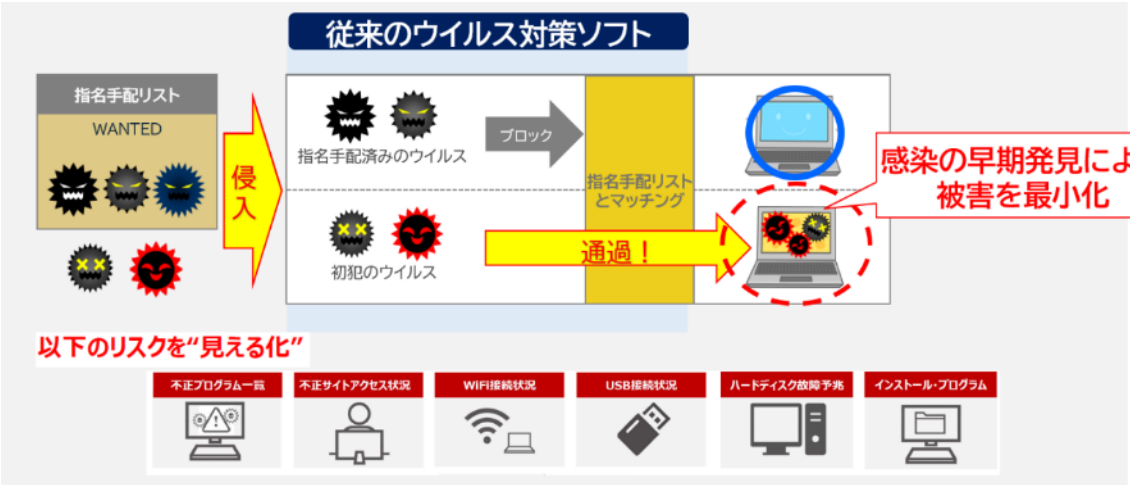

図 18　パソコン監視分析サービスのサービス概念図

なお、パソコン監視分析サービスについては、本実証事業の開始時点では予定していないサービスであったが、ＵＴＭ監視・検知サービス又はクラウド型ＷＡＦサービスの導入に向けた参加申込企業との調整を行う中で、特にＷＡＦについては前述のとおり当初の想定以上に導入が困難であることが明らかになってきたことから、本実証事業への参加意思があるにもかかわらず地域実証に参加することができないという機会損失を低減することを目的として、ＥＤＲによる実態把握を推進することとした。

② パソコン監視分析サービス － 導入方法

参加申込企業に対し、ＥＤＲのインストーラーを作成・提供することにより、システムネットワークの設定変更などの専任のシステム担当者がいない中小企業でも簡単に導入することができる仕組みを構築し、参加申込企業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。

③ パソコン監視分析サービス － 導入状況

パソコン監視分析サービスについては、予算上の制約から８０社への導入を上限として、参加申込企業に対するサービス提案を実施した。最終的に８７社への提案を行い、７２社への導入を行った。

なお、導入台数は全体で１２３台であり、１社当たりでは１．７台であった。

表 5　パソコン監視分析サービスの導入状況

パソコン監視分析サービス	
提案企業数	87 社
うち、導入不可・中止	15 社
導入完了企業数 （導入割合）	72 社 (83%)

(4)　サイバーリスク簡易診断アンケート

① サイバーリスク簡易診断アンケート － サービス概要

サイバーリスクへの対応や個人情報保護法への適合等の状況をアンケート方式で簡易診断し、また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含む分析レポートを作成・提供するものである。

図 19　サイバーリスク簡易診断　分析レポートのイメージ

② サイバーリスク簡易診断アンケート － 実施方法

中間報告会において、各設問に対する解説を交えながら実証開始企業が適切にアンケートに回答できるように工夫した。

③ サイバーリスク簡易診断アンケート － 実施状況

中間報告会において、実証開始企業１８社からアンケートを回収し、分析レポートを作成した。

（5） ＷＥＢアプリ簡易診断

①ＷＥＢアプリ簡易診断 － サービス概要

ＳＯＭＰＯリスクマネジメントが提供する「SOMPO DEFNAVI ＷＥＢアプリ簡易診断サービス」[12]を利用し、ウェブサイトに対するサイバー攻撃について、基礎的な対策をナビゲートするレポートを作成・提供するものである。

図 20 ＷＥＢアプリ簡易診断 分析レポートイメージ

なお、当初は、グルーバルＩＰアドレスを所持している中小企業に対しては、ＳＯＭＰＯリスクマネジメントが提供する「SOMPO DEFNAVI 総合簡易診断サービス」[13]を用いて、リスク状態を診断する予定であったが、グルーバルＩＰアドレスを所持している実証開始企業が少数であったことなどを踏まえ、「SOMPO DEFNAVI ＷＥＢアプリ簡易診断サービス」によるウェブアプリケーション（ウェブサイト）の脆弱性に係る診断を実施した。

---

[12] ウェブアプリケーションにおける脆弱性の有無を診断するサービス

[13] ウェブアプリケーション及びプラットフォーム（ＯＳ、サーバー、ミドルウェア）における脆弱性の有無を診断するサービス

②ＷＥＢアプリ簡易診断 － 導入方法

通常の「SOMPO DEFNAVI ＷＥＢアプリ簡易診断サービス」では、ユーザー企業がＳＯＭＰＯリスクマネジメントウェブサイト（SOMPO DEFNAVI）上で自己診断できるようになっているが、本実証事業では回収率を高めるため、中間報告会において実証開始企業に同意を得た上で、ＳＯＭＰＯリスクマネジメント職員が診断を実施した。

③ＷＥＢアプリ簡易診断 － 導入状況

実証開始企業１６社の簡易診断を実施し、分析レポートを作成した。

1.2.3. 事後対応支援体制の構築及び支援の実施

（1） 相談受付・駆け付け支援サービスの実施

実証開始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、一般的な中小企業の営業時間帯や中小企業向けサービスとしての実現可能性を考慮して、土日祝日を除く、平日午前９時から午後５時までとした。

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を用意した。

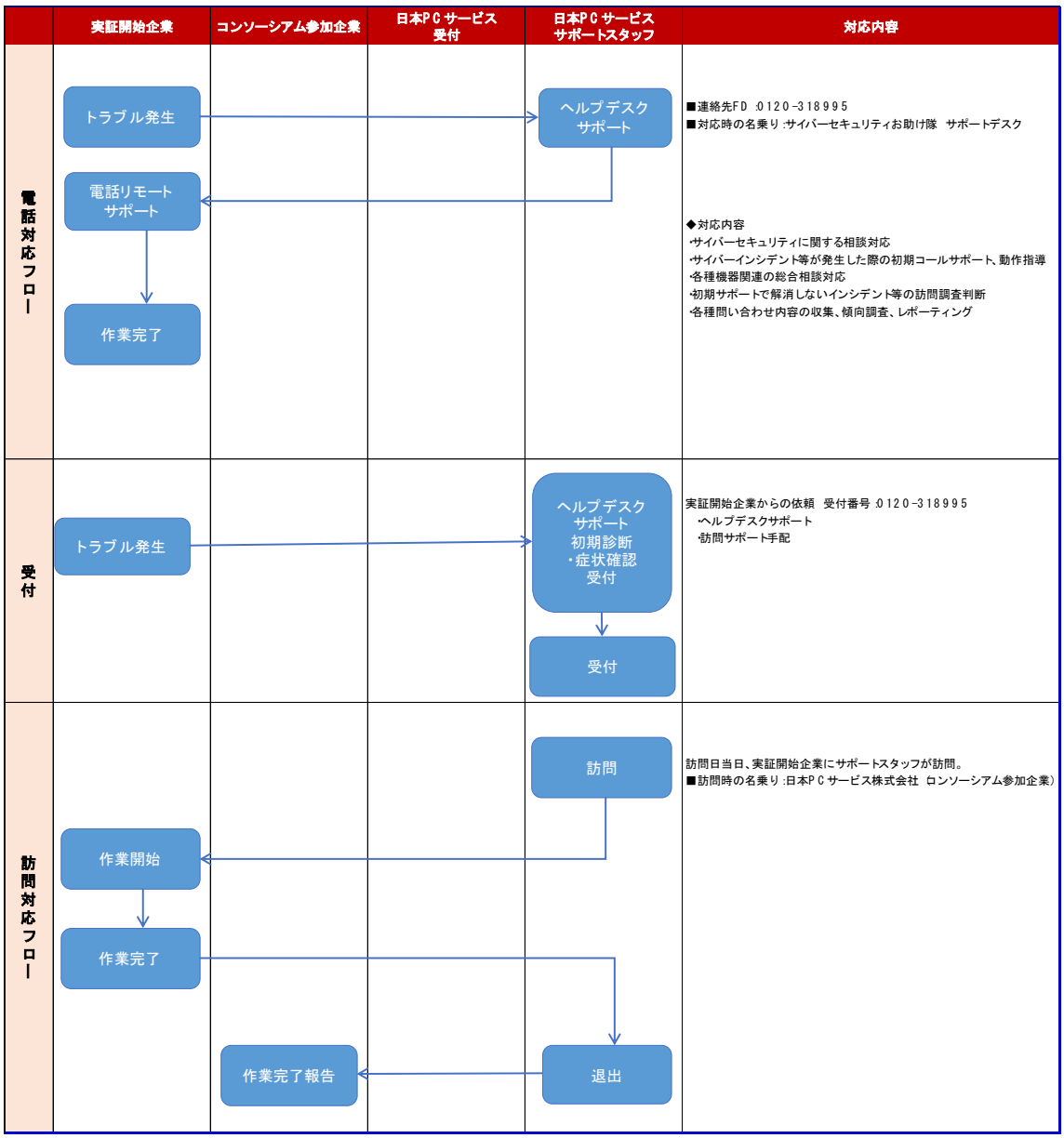

図 21　相談受付・駆け付け支援サービスの運用フロー

（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、中小企業のセキュリティインシデントに関する監視及び検出を行い、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。

「(1)　ＵＴＭ監視・検知サービス」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開始企業の管理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)　クラウド型ＷＡＦサービス」では、実証参加企業のウェブサイトにアクセスするユーザーと当該企業のサーバーとの間にクラウド型のＷＡＦセンターを設置し、http/https 通信を通る不正なアクセスを遮断し、そのログデータについて土日祝日を含む２４時間対応で収集する仕組みを用意した[14]。

「(3)　パソコン監視分析サービス」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）及び被疑ファイル（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開始企業の管理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・駆け付け支援サービスの実施」又は「(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、実証開始企業からセキュリティインシデント若しくはそのおそれ（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又は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又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、一般的な中小企業の営業時間帯や中小企業向けサービスとしての実現可能性を考慮して、土日祝日を除く、平日午前９時から午後５時までとした。

なお、本機能は、中小企業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（中小企業向けサイバー保険の在り方を含む。）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）することは行わないこととした。ただし、中小企業が利用しやすいサービスの在り方やサイバー保険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）を得ること及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ＳＯＭＰＯリスクマネジメントが無償で提供した。

[14] クラウド型ＷＡＦサービスについては、実証開始に至る企業が現れなかったため、未適用で終了した。

1.3. 地域実証終了後のサービス提供

実証開始企業のうち、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本実証事業を通じて得た知見などに基づき開発した次に掲げるサービスを有償提供する。実証開始企業に対しては、２０１９年（令和元年）１２月から翌年１月に掛けて個別に地域実証の終了及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参加企業に対して後続サービスの案内を行った。

２０２０年（令和２年）２月１２日現在、ＵＴＭ監視・検知サービスについては０社（検討中３社)、パソコン監視分析サービスについては５社（検討中１０社）から後続サービスの利用意思を確認している。

なお、上記サービスの概要については、「3. 考察（実施結果を踏まえた検討）3.2. 中小企業向けセキュリティサービスの在り方」の中で記載する。

2. 地域実証の結果

2.1. 中小企業の実態

本実証事業では、地域実証後に自立的なサービス展開につなげるための情報を収集することを目的として、取引関係を前提とする圧力募集等を行わず、サービス内容についての提案に対して興味を抱いた、又は本実証事業の趣旨に賛同した中小企業に対する通常の営業手法に近い形での募集を行った。普及支援機関である損害保険ジャパン日本興亜のチャネルを通じて募集したことから、損害保険代理業の割合が約３０％と高くなってはいるものの、「1. 実施概要 1.2. 地域実証の実施概要 1.2.1. 参加事業者の概況（2） 参加事業者の構成」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、神奈川県内の中小企業の数は、１８７，４２８社（２０１６年（平成２８年）６月現在）[15]であり、実証開始企業からの回答率（ログの収集率）が９５％である場合、許容誤差５％・信頼度９５％に必要なサンプル数は７３社[16]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開始企業の実態については、神奈川県内の中小企業の実態を表したものとして評価できるもの考える。

2.1.1. 中小企業のセキュリティに対する意識の実態

本実証事業においては、参加申込企業に対し、各事業説明会や各種連絡の際に「SECURITY ACTION」制度の紹介を実施しており、２０２０年（令和２年）１月２４日時点で１３社において自己宣言されていることを把握している。参加申込企業の「SECURITY ACTION」の宣言状況について、地域実証の開始時からの件数推移を調査したところ、下表のとおりであった。

表 6 参加申込企業の SECURITY ACUTION 宣言状況

宣言内容	8 月末	10 月末	12 月末	8 月からの増加数
★（一つ星）	2 社	5 社	9 社	＋7 社
★★（二つ星）	1社	3 社	4 社	＋3 社
計	3 社	8 社	13 社	＋10 社
参加申込企業数	74 社	125 社	150 社	＋76 社
宣言企業割合	4.05％	6.40％	8.67％	

損害保険代理店の割合が多く、業務委託元である損害保険会社のグループ企業であるＳＯＭＰＯリスクマネジメントがアンケート方式による意識調査を行うと、回答内容に一定のバイアスが生じることが懸念されたことから、実際の行動結果としての宣言状況を定点的に観測してきた。自己宣言事業者は、少数ではあるものの、参加申込企業数に対する割合を含めて着実に増加しており、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。

---

[15] 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）」

[16] 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。

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

また、こうした状況に加え、募集説明会の参加企業数５２社に対して、これを上回る１５０社からの参加申込を受け付けたことなどを鑑みると、中小企業の多くがセキュリティに対して関心を持っているが、具体的な行動を起こす上での何らかの障壁があることが推測できる。

2.1.2. 中小企業のセキュリティ対策状況の実態

（1） サイバーリスク簡易診断アンケート結果から見える対策状況

実証開始企業１８社からのアンケート結果に基づき、平均的なサイバーリスクに関する状況を評価した。

① サイバーリスクへの対応状況

アンケート回答企業ごとに、サイバー攻撃対策として考慮すべき「組織的」、「人的」、「物理的」及び「技術的」な対策を中心としたサイバーリスクへの対応状況について、八つの項目別の達成度で評価した。１８社の平均評価結果は、下図のとおりであった。

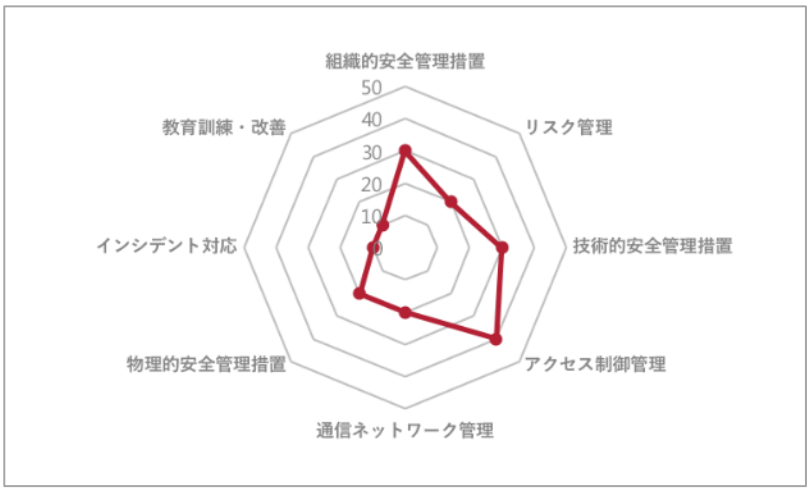

図 22　サイバーリスクへの対応状況（達成度）

パスワード設定やＩＤ管理などの「アクセス制御管理」についての達成度は高く、一定の対応を講じられていることが明らかになった。また、「組織的安全管理措置」及び「技術的安全管理措置」についても、一定の対応ができている状況が窺える。

一方、「リスク管理」、「通信ネットワーク管理」、「インシデント対応」及び「教育訓練・改善」については、達成度が低い状況であった。

この結果は、経営層のセキュリティ意識が一定程度は醸成されており、ウイルス対策ソフトの導入といった基礎的な対策については講じられているが、組織全体を俯瞰したセキュリティポリシーの策定やネットワーク対策までは講じられていないレベルの成熟度合い（手の届く範囲での対応に止まっている）であることを示唆しているものと推測する。中小企業においては、サイバーセキュリティ対策に対して投下できる資源が限られていることから最低限の対応に止まっている（資金がないから対策できない）とも推測できるが、「インシデント対応」及び「教育訓練・改善」の達成度の低さを鑑みると、そもそも自社がサイバー攻撃の被害を受けることについての想像ができておらず、サイバー攻撃による影響を重大なリスクとして十分に認識できていない（自社への影響がよく分からないから対策しない）という仮説について、そのとおりの実態であることが検証できたものと考える。

② 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」及び「恐喝」の五つのシナリオに基づく想定損害額[17]を算定した。１８社の平均値及び中央値は、下表のとおりであった。

表 7　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	**4,387 万円**	**2,994 万円**
損害賠償費用	1,137 万円	188 万円
事故対応費用	1,527 万円	1,284 万円
お詫び対応費用	617 万円	432 万円
売上機会損失額	1,106 万円	605 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４，３８７万円、中央値は２，９９４万円となっており、一たびサイバー攻撃の被害を受けた場合には、中小企業の経営を揺るがすだけのインパクトが生じ得ることが窺える。ただし、「損害賠償費用」については、平均値は１，１３７万円と中小企業にとっては大きな金額であるものの、中央値は１１８万円と小さく、当該数値がサイバー攻撃を受けた場合の影響についての中小企業の感覚に近いものであると推察される。

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「① サイバーリスクへの対応状況」の結果及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弱く、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、中小企業に対し、リスクに関する啓発及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。

なお、想定損害額は、国内外の損害保険会社における過去の保険金支払額などを基にして算定された数値である。このため、今後、これまであまり保険金支払の対象になっていなかったサイバー攻撃に起因する事業中断等による取引先への影響（いわゆるサプライチェーンリスク）といった新しい傾向が金銭的な形で中小企業に対して転嫁（損害賠償や調査費用の請求など）されるようになると、現時点の想定損害額から大きく増加することが予想されるため、「最低でもこの程度の損害が生じ得る」という前提に基づくリスクマネジメントが求められる。

[17] ＳＯＭＰＯリスクマネジメントが海外の損害保険会社や損害保険ジャパン日本興亜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うる損害額の想定値

（2） ＷＥＢアプリ簡易診断結果から見える脆弱性状況

中間報告会において同意を得た１６社を対象として、ＷＥＢアプリ簡易診断によるウェブサイトの脆弱性を診断した。診断対象とする脆弱性は、「暗号通信に関する脆弱性」、「ウェブサーバーの設定不備」及び「ソフトウェアの古いバージョン利用」の３区分・１５項目であり、結果は下図のとおりであった。

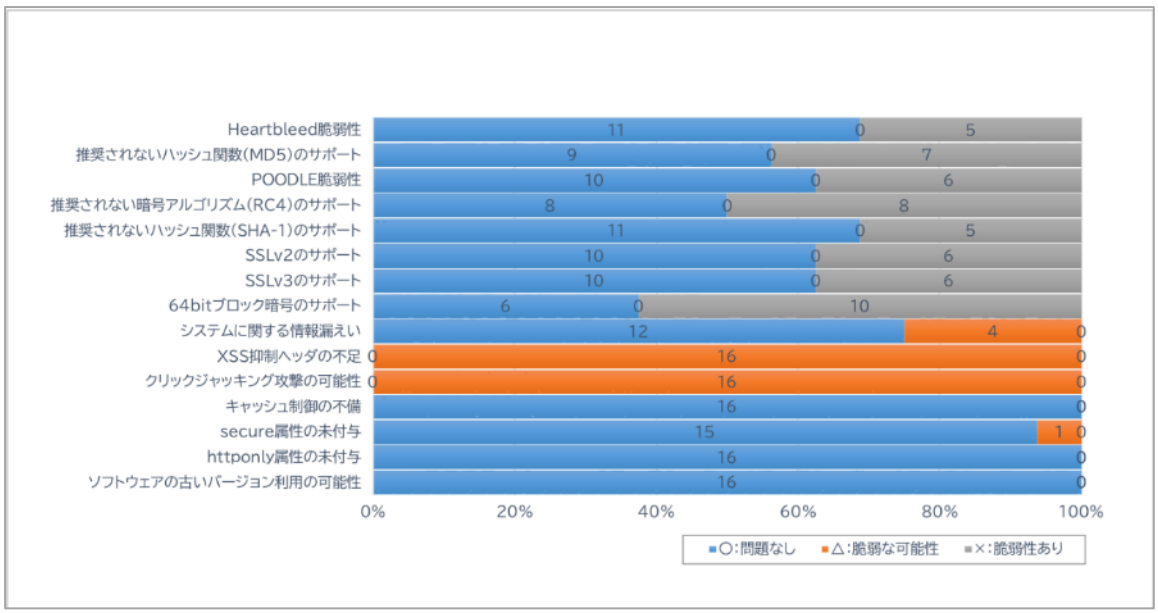

図 23 ＷＥＢアプリ簡易診断結果

該当企業においては、ウェブサイトを積極的に業務に活用しておらず、多くのウェブページがサービス紹介ページといった静的コンテンツで構成されている傾向が見られたが、問合せフォームを設置しているウェブサイトもある中で、「暗号通信に関する脆弱性」に対する対応が不十分であるケースが多かった。

また、ウェブサイトの開設後のセキュリティ対応が十分でなく、診断対象であるウェブサイトの全てにおいて、「ウェブサーバーの設定不備」に関する項目のうち、クロスサイトスクリプティングやクリックジャッキングを防ぐための対策が講じられていないことが判明した。

2.1.3. 中小企業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

実証開始企業（１１０社）からの相談窓口となるコールセンター及び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３０件であり、その内訳は下記のとおりであった。１１０社に対して３０件の問合せを受け付けていることから、中小企業に対する相談受付サービスについての一定のニーズが見込まれるが、問合せの多くは「サービス導入に関する疑問・相談（8 件)」、「導入サービスの操作等（９件)」及び「サービス導入後のトラブル（7 件)」といったサービス導入に関する問合せであり、これが全体の７割超を占める結果となった。

本実証事業の開始に当たり、中小企業向けサービスとして、一定のニーズがあることを想定していた「よろず相談」（例えば、「原因は分からないが、パソコンの調子が悪い。」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）については、わずか３件であった。

これらの結果については、実証開始企業への個別ヒアリングによると、「何かあれば取引先システムベンダーに問い合わせる。」といった回答もあり、こうした中小企業におけるシステム利用状況に照らして勘案すると、「よろず相談」については、有事の際のセキュリティ関連サービスとしてのニーズは乏しく、平時の業務システム関連サービスに組み込まれる形で提供されることが望まれるものと推測する。

（単位：件）

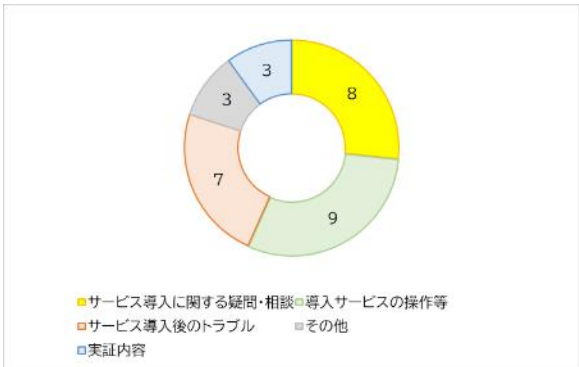

図 24　相談受付サービスの問合せ状況

（単位：件）

表 8　相談受付サービスの問合せ状況（内訳）

対応種別	アラート種別		発生件数	
コールセンター対応	実証参加に関する問合せ	事業趣旨、内容、スケジュールについて	2	2
	セキュリティ機器設置等の問合せ	パソコン監視分析サービスのインストール方法について	5	14
		ＵＴＭ の設定について	5	
		ＵＴＭ 監視 分析サービスのレポートの見方について	2	
		ログインパスワードについて	1	
		サービスからの案内メールについて	1	
	セキュリティ対応の相談	システム障害について	5	10
		パソコンの動作が重い	2	
		インターネットにうまく繋がらない	2	
		迷惑メールが来ているが無視しておけばよいか	1	
	その他	サービス内容について	2	4
		別サービスを希望	1	
		実証終了後のサービスの価格について	1	
		計		３０

分類	件数
サービス導入に関する疑問 相談	8
導入サービスの操作等	9
サービス導入後のトラブル	7
実証内容	3
その他	3
計	３０

（2） 導入時等における個別ヒアリングの状況

各サービスの導入に当たり、往訪による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 ＵＴＭ監視・検知サービスの導入に係る問題点

ア．ネットワークに関する知識が不足しており、サービス導入が困難であった

ＵＴＭ監視・検知サービスでは、ＵＴＭの設定に必要なＩＰアドレスを把握するために実証開始企業から当該企業のネットワークを管理するベンダーに聴取してもらう必要があるが、こうした対応についても、基本的な知識がないことからうまくいかず、導入に時間を要したり、導入を断念したりするケースがあった。

イ．導入手続が煩雑であり、スケジュール調整が困難であった

ＵＴＭ監視・検知サービスでは、導入前に訪問し、オンサイトでネットワーク環境を調査する必要があるが、システム担当が会社代表者や他業務との兼務者であることが殆どであることから、多忙で訪問の日程調整が困難であった。この結果、導入に時間を要したり、導入を断念したりするケースが生じた。

ウ．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などに関する協力を得ることが困難であった。この結果、導入に時間を要したり、導入を断念したりするケースが生じた。

② パソコン監視分析サービスの導入時に頂戴した主な意見

ア．導入負荷が小さい

・ＵＴＭは導入に当たりネットワークを止めることに抵抗があったが、ＥＤＲは端末ごとに都合の良いタイミングで導入できた。

・インストールが１５分程度で終わった。簡単で良かった。

イ．働き方改革、在宅勤務に良い

・在宅勤務を推奨しており、Wi-Fi やＵＳＢ接続状況を把握できるのは魅力的である。

ウ．セキュリティを考える良いきっかけとなった

・不正プログラムの有無だけでなく、感染しやすさを可視化してくれるのは、自社のセキュリティを把握し、対応を検討するための導入ツールとして良いと感じた。

2.1.4. 中小企業に対するセキュリティインシデントの実態

実証開始企業の５９％[18]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、中小企業を５社集めると、そのうちの３社がサイバー攻撃を受けて危険にさらされている可能性があるという状況である。

また、ＩＰＳと WebBlocker 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監視・検知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監視・検知サービス

ＵＴＭ監視・検知サービスについては、参加申込企業６１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３８社であった。

表 9　ＵＴＭ監視・検知サービスにおける取得データの概要

データ内容	
取得日数	平均１０３日間
主な取得データの種類	ＩＰＳ機能のログ情報 ＵＲＬフィルタリング機能のログ情報 ファイアウォール機能のログ情報
件数	
期間中総件数（３６社分）	約３億６，０００万件
期間中１社あたりの件数	約１，０００万件
１日あたり総件数（３６社分）	約３４０万件
１社１日あたりの件数	約９万件

＊データ取得１週間未満でサービス導入中止となった２社を除く

実証開始企業３８社において、計４件の緊急度「高」のアラートを発信し、このうち１件は「不正なＩＰアドレスへの通信」が成立していた。また、残りの３件においても、不正なアクセスがあったが、ＵＴＭによって防御できていた状況であった。

なお、当該４社は、いずれも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。

---

[18] ＵＴＭ監視・検知サービスにおいてＩＰＳ又は WebBlocker のいずれかが稼働した企業（ＵＴＭ監視・検知サービス導入企業３８社から①データ取得が１週間未満でサービス導入中止となった２社及び②地域実証実施前から既設のＵＴＭを利用しておりＩＰＳの稼働が確認できない企業８社を除いた２８社中２３社）及びパソコン監視分析サービスにおいて不正プログラムが検出された企業（１週間以上の監視を行うことができた６７社中３３社）を集計

② 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、５１１件の稼働を確認した。

なお、２８社（導入企業３８社から①データ取得が１週間未満でサービス導入中止となった２社及び②地域実証実施前から既設のＵＴＭを利用しておりＩＰＳの稼働が確認できない企業８社を除いた数）のうち、９社において稼働を確認した。

（稼働割合：約３２％）

表 10　ＩＰＳの稼働状況（上位３位）

ア.Microsoft Office の初期化されていないメモリ使用の脆弱性(164件)
・Microsoft Office ソフトウェアでメモリ内のオブジェクトが適切に処理されない場合に、リモートでコードが実行される脆弱性。 ・攻撃者がこの脆弱性を悪用した場合、特別に細工したアプリを使用して、現在のユーザーのセキュリティコンテキストで任意のスクリプトを実行する可能性がある。
イ.LNK のリモートでコードが実行される脆弱性(109件)
・.LNK ファイルが処理される場合に、リモートでコードが実行される可能性がある脆弱性。 ・攻撃者がこの脆弱性を悪用した場合、攻撃者がローカルユーザーと同じユーザー権限を取得する可能性がある。
ウ.複数の Microsoft Windows 製品における任意のコードを実行される脆弱性(67件)
・Windows PDF のリモートでコードが実行される脆弱性。 ・攻撃者がこの脆弱性を悪用した場合、任意のコードを実行される可能性がある。

③ ＵＲＬフィルタリングの稼働状況

ＵＲＬ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、７，５９８件の稼働を確認した。

なお、２８社（導入企業３８社から①データ取得が１週間未満でサービス導入中止となった２社及び②地域実証実施前から既設のＵＴＭを利用しておりＵＲＬフィルタリングの稼働が確認できない企業８社を除いた数）のうち、２４社において稼働を確認した。

（稼働割合：約８６％）

表 11　ＵＲＬフィルタリングの稼働状況（上位３位）

ア. 迷惑ソフトがインストールされていることによる不正なサイトへのアクセス(3,885件)
・インストールすると不要な広告を出す仕組みになっているソフトウェアによる広告へのアクセス。 ・無料でダウンロードできるツールと一緒にインストールされるケースが多く、不要な広告を大量に表示する。
イ. 改ざんされた可能性のあるサイトへのアクセス(1,705件)
・アクセスすると不正なプログラムが実行されるように改ざんされたと思われるサイトへのアクセス。 ・ブロックしていなければ、例えば第三者からコンピュータを乗っ取られ遠隔で操作されてしまう可能性がある。
ウ. ボットネットへのアクセス(843件)
・ボットへ攻撃の指令を出すサーバへのアクセス。ボット化した端末から指令を受けに行こうとしている可能性がある。 ・ブロックしていなければ、ボットとして勝手にインターネットへの攻撃に加担してしまうことになる。 ・また、コンピューターの能力を攻撃に割かれてしまうので、動きが遅くなるといった被害も発生する。

（2） パソコン監視分析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 － パソコン監視分析サービス

パソコン監視分析サービスについては、参加申込企業８７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７２社であった。

表 12 パソコン監視分析サービスにおける取得データの概要

取得データの内容		
取得日数	平均53日間分	
導入台数	123台(1社平均1.7台)	
取得データの種類	①不正なプログラムの有無	②不正なプログラムサイトへのアクセス状況
	③フィッシングサイトへのアクセス状況	④悪意のあるサイトへのアクセス状況
	⑤安全とは言えないサイトへのアクセス状況	⑥セキュリティの低いWi-Fiへの接続回状況
	⑦USB接続状況	⑧機器の故障予見有無

② パソコン監視分析サービスにおける検知結果

実証開始企業７２社のうち、１週間以上の監視を行うことができた６７社を対象に分析したところ、約５０％の企業において不正プログラムが検出された。このうち１件については緊急度「高」のアラートを発信し、リモートアクセスでの駆除対応を実施した。また、不正なプログラムを配布するサイトなどへのアクセスについても多く確認された。

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、８社（約１２％）のみであった。

表 13 パソコン監視分析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

分析対象:1月31日までに1週間以上の監視を行った67社
分析対象日数:平均53日間

① 不正プログラム	
確認数	1142件
検出割合	49%(67社中33社)
不正プログラムの主な種類	
アドウェア･リスクウェア※	397件
トロイの木馬	145件
② 不正サイトへのアクセス	
確認数	452回(67社中15社、22%)
③ フィッシングサイトへのアクセス	
確認数	146回(67社中7社、10%)
④ 悪意のあるサイトへのアクセス	
確認数	4,095回(67社中46社、69%)
⑤ 安全とは言えないサイトへのアクセス	
確認数	294回(67社中2社、3%)
⑥ セキュリティの低いWi-Fiへの接続回数	454回
⑦ USB接続回数	486回

※アドウェア・・・広告表示によって収入を得ることを目的としたソフトウェア
※リスクウェア・・悪意のあるソフトウェアではないが、使い方によっては悪用可能なソフトウェア

（3） 駆け付け支援サービスの実施内容

前述のとおり、ＵＴＭ監視・検知サービスを導入した企業において４件、パソコン監視分析サービスを導入した企業において１件の計５件の緊急度「高」のアラートを発信し、このうちの１件については「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、駆け付け支援を実施した。

① 該当企業（Ｘ社）の概要

・業種　　：サービス業
・従業員数　　：約１００名
・情報システム要員　　：専任者は置いていない
・セキュリティ対策状況：各端末にウイルス対策ソフトは導入済
・サイバー保険　　：未加入

② 事案の概要及び対処内容

ア．２０１９年（令和元年）１１月下旬に「ＵＴＭ監視・検知サービス」において、ＵＴＭを通り抜けたと思われる社内から外部への不正な通信を検知し、アラートを発信した。

イ．Ｘ社担当者と共に状況を確認したところ、Windows XP でしか動作しないソフトウェア利用のために使用している Windows XP 端末から通信が行われていることが判明した。

ウ．当該端末はインターネットに接続していないとの認識であったが、社内プリンタ使用のために社内ＬＡＮに接続されており、意図せずインターネットに接続されていたことが判明した。また、当該端末はインターネットに接続していない認識であったことから、ウイルス対策ソフトが導入されていないことも判明した。

エ．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（中小企業向けサイバー保険の在り方を含む。）について検討するための情報を得ることを目的として、駆け付け支援対応の窓口となる日本ＰＣサービス株式会社による駆け付け支援（ウイルス探索及び駆除対応）を実施することを決定した。

オ．当該端末を調査した結果、ワーム、トロイの木馬、迷惑ソフトその他計２５ファイルの不正プログラムが発見されたため、当該不正プログラムの駆除を実施した。

③ 駆け付け支援対応後の状況

Ｘ社では、ＵＴＭのＵＲＬフィルタリングによる不審な通信のブロックが月１，０００件以上発生していたが、不正プログラムの駆除を行った後はブロック件数が激減した。また、迷惑ソフト等により挙動が不安定であった Windows XP 端末が安定して業務効率が向上した。

なお、Ｘ社からは、当該経験を経て、改めてサイバーセキュリティの重要性を認識できたとの声を頂戴した。

また、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 14　インシデント等対応の内訳

対応種別		発生件数
インシデント等対応	電話およびリモートによるインシデント対応（訪問によるインシデント対応の一次対応を含む）	5
	訪問によるインシデント対応	1
	機器設置等のトラブル対応（UTM撤去2 社、EDRアンインストール5 社）	7
	その他（導入支援での訪問）	8
	計	21

④ 検知・駆除できていなかった場合の想定損害額

前記「2.1.2. 中小企業のセキュリティ対策状況の実態 (1) サイバーリスク簡易診断アンケート結果から見える対策状況 ② サイバー攻撃を受けた場合の想定損害額」の手法を用いて、X社の想定損害額を算定したところ、下記のとおりであった。

表 15 X社想定損害額

内訳	金額
損害賠償費用	1,600,000円
事故対応費用	10,000,000円
お詫び対応費用	16,000,000円
売上機会損失額	27,400,000円
合計	**55,000,000円**

2.2. 中小企業向けサイバーセキュリティ事後対応支援体制の構築

本実証事業では、前記「1. 実施概要 1.0. 全体概要 1.0.3. 本実証事業の実施体制」に記載した支援体制により、「中小企業からの相談受付及び対応」、「相談内容がセキュリティインシデントであるかの判断」及び「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」に関する取組を行った。これらのサービス・機能に関し、地域実証及び関連する各種取組を通じて、中小企業向けサービスの在り方を検討する上で参考になる知見を得ることができた。

本章では、本実証事業を通じて得た知見について、主にサービス提供側における事項を紹介する。

2.2.1. 中小企業からの相談受付及び対応

前記「2.1.3. 中小企業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」において記載したとおり、中小企業においては、「相談受付サービス」に対する一定のニーズが認められたが、当初想定していた「よろず相談」のニーズについては乏しいことが窺えた。

また、コールセンターの開設時間については、中小企業の営業時間帯や中小企業向けサービスとしての実現可能性を考慮して、土日祝日を除く平日午前９時から午後５時までの条件で地域実証を運用したが、個別ヒアリング等からも休日夜間における相談ニーズは発現せず、中小企業向けサービスにおいては２４時間３６５日対応のサービス供給は必要な条件ではないといえる。このことは、サービス受給側のセキュリティへの資源配分が不十分であり、セキュリティ対策に携わる要員体制も十分に整っていないといった状況にあることが要因であると推測されるが、こうした推測を裏付けるように、サービス導入時の個別ヒアリングその他地域実証を通じた中小企業との対話の中で、「セキュリティ担当者は総じて複数業務との兼務であり、かつ、セキュリティが主たる業務で、複数人体制でもない」、「情報システム担当を設置しておらず、ネットワーク全般を委託先ベンダーに全面的に依存している」といった実態が明らかになっている。

地域実証の中で見えてきた中小企業の実態

- ✓情報システム部門や専任担当者を設置している事業者は少なく、多くの事業者が情報システムの導入、保守、運用等をシステムベンダー（地場ベンダーであるケースが多い）に依存（丸投げ）していた。
- ✓セキュリティ担当者がいたとしても、総じて複数業務との兼務であり、かつ、セキュリティが主たる業務でなく、複数人体制でもない状況であった。このため、日々の実施業務のうち、定常的・突発的に発生する業務を常に優先せざるを得ず、セキュリティ事故が発生していない状況下では事前予防としてのサービス導入の打合せは後回しにされる傾向が強かった。
- ✓よろず相談についてのニーズは殆どない。これについては、丸投げしているシステムベンダーの存在や、製造業や自動車修理業のように業務上でＰＣを使う場面が限定されていることによるものと推測される。

2.2.2. 相談内容がセキュリティインシデントであるかの判断

前記「1.2.3. 事後対応支援体制の構築及び支援の実施　(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」に記載したとおり、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、「ＵＴM監視・検知サービス」及び「パソコン監視分析サービス」により、中小企業のセキュリティインシデントに関する監視及び検出を行った結果、前記「2.1.4. 中小企業に対するセキュリティインシデントの実態」において示したとおり、過半数の中小企業からセキュリティインシデントに関する痕跡が確認された。セキュリティインシデントが確認された実証開始企業においては、その多くがウイルス対策ソフトを導入しているにもかかわらず、地域実証によって、初めてその事実に気付かされたという状況であった。さらには、既設のＵＴMの監視をすり抜けた高度な攻撃が「ＵＴM監視・検知サービス」によって検知された事案も発生している。

こうした状況が明らかになったことにより、これまでセキュリティ対策を講じていない、又は講じていたとしても基礎的な「防御」機能に主眼を置いていた中小企業においても、「検知」や「対応」といった機能にまで目を向けることが必要であることが浮き彫りとなった。

一方、多くの中小企業において、情報システムの導入、保守、運用等をシステムベンダー（地場ベンダーであることが多かった。）に依存（丸投げ）していることが多く、このような中小企業では自社のネットワーク構成がどのような状態なのかさえも十分に把握できていないという実態があった。また、既存ネットワーク構成自体に不備があり、セキュリティ対策の導入以前にシステム環境の整備が必要なケースも確認されている。インターネット回線が遅かったり、端末のスペックが低かったりすることで、セキュリティ対策導入に苦労したケースもあった。加えて、地域実証に参加する前からＵＴMを設置している企業の中には、ネットワーク構築の際にベンダーに勧められるまま導入したものの、セキュリティ機器との認識が乏しく、ＵＴMからのアラートメールの発生頻度が高く煩わしいことを理由にアラート機能を切っていたというケースもあった。

なお、このようなケースでは、地域実証におけるＵＴM等のネットワーク機器、ＤＮＳその他の設定変更を伴うＷＡＦの導入などについて、システムベンダーから既存設定の変更を拒否されるなどの非協力的な反応が返ってくることも多かった。

地域実証の中で見えてきた中小企業の実態

- ✓実証事業への申込事業者については、セキュリティに関する一定の関心は持っている。ただし、実際にセキュリティ対策を導入し、効果的に利用できている事業者は少ない。
- ✓機能等を認識して管理・運用している中小企業は少ない。ネットワーク構築の際に勧められて導入したままの状態で、ＵＴMがセキュリティ機器であるという認識が乏しい。（折角導入しているのに、その機能を十分に使いこなせていない。）
- ✓既存ネットワーク構成に不備があり、セキュリティ対策の導入以前にシステム環境の整備が必要なケースも確認されている。また、インターネット回線が遅かったり、端末のスペックが低かったりすることで、セキュリティ対策導入に苦労したケースもあった。
- ✓中小企業においても、一定のサイバーインシデントの発生（マルウェア感染を含む。）を確認できた。いずれも、本実証事業による監視・検知サービスが導入されたことにより、認識することができたもの。

2.2.3. 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「2.2.2. 相談内容がセキュリティインシデントであるかの判断」において記載したとおり、地域実証を通じて「検知」機能を有するセキュリティ対策を導入したことによって初めて自らにセキュリティインシデントが発生していることを認識したというケースが殆どであった。地域実証開始企業においては、ＳＯＭＰＯリスクマネジメントからのアラートメールを受信した後に自律的・能動的に対応できたケースは殆ど見られず、またアラートメール自体を閲覧できていなかったり、読んでいても理解できていなかったりするケースも多かった。また、ＵＴＭ監視・検知サービスでは、専用のＷｅｂポータルを用意し、実証開始企業が自らのログの分析状況やアラートの詳細を閲覧できる機能を提供していたが、これらの機能を積極的に活用していた企業はいなかった。

こうした中小企業の実態を踏まえると、インシデント発生時の対処支援については、インバウンドで支援要請を受けた場合に発動するという提供の形態ではなく、セキュリティインシデントを検知したサービス提供側からのアウトバウンドによる積極的な働き掛けを行うような提供形態が望ましいものと考えられる。即ち、中小企業向けサービスについては、「検知」と「対応」が一体となったサービスとして提供されることが望ましく、サービス提供事業者においては一元的にこれらのサービスを中小企業に提供できるだけのケイパビリティが求められる。本実証事業においては、複数のサービス提供事業者がコンソーシアムを組むことによってケイパビリティを確保してきたが、実証終了後においても、こうしたサービス提供企業間の連携によるサービス提供を実現するための枠組みを整えていくことが重要になると考えられる。

また、地域における支援体制を構築する上で、駆け付け支援サービス等における労働集約性の高さを解決するための低コストの人材確保が課題として掲げられており、ＩＴシルバー人材の活用が一つの方策として検討されている。本実証事業の枠組みの中ではＩＴシルバー人材の活用は実現しなかったが、神奈川県在住のＩＴシルバー人材にヒアリングしたところ、次のような意見を聴取することができた。ヒアリング数が１名のみであり、ＩＴシルバー人材の活用に係る意見を代表するものではないが、参考意見として掲載する。

ITシルバー人材の活用についてのヒアリング内容（参考）

- ✓中小企業は低コストを期待しているので、現役の方が現地駆付けをしても、それに見合う費用をいただけないため、ＩＴシルバー人材の活用という構想になっているのだと理解している。
- ✓私の様なＳＥの技術や経験が活かせる受け皿が現在無いので、この構想が実現するのであれば、是非参加させて頂きたい。
- ✓ＩＴシルバー人材の大半はソフト開発人材と思われるので、再教育が必要という所がこの構想のハードルだと考えている。
- ✓ＩＴシルバー人材に駆付け支援だけを期待するのであれば、発生頻度も低いことから、一人でかなりの地域をカバーでき、ビジネスとして成り立つのではないか。

3. 考察（実施結果を踏まえた検討）

3.1. 実証結果を踏まえた課題の抽出及び整理

本実証事業を通じて得られた中小企業の実態等を踏まえ、中小企業にサイバーセキュリティ対策を定着させていくために、サービスの受給側及び提供側の両側面から望まれる中小企業向けサービスを検討する上で解決すべき課題について、「意識」、「資源」及び「能力」の観点から整理した。

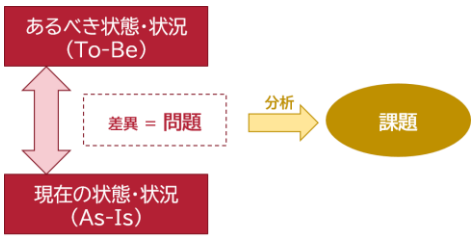

図 25　課題策定のイメージ

図 26　中小企業の実態を踏まえた課題抽出

3.1.1. 「意識」に関する課題

本実証事業を通じて把握した中小企業の実態から、セキュリティ対策を実際に講ずる上での起点となる「意識」面での問題が抽出された。参加申込み企業の経営層においては一定のセキュリティ意識が醸成されているが、セキュリティに関するリテラシーが不足していることから、これを向上させることが課題となる。

中小企業側（サービス受給側）の観点からは、セキュリティに関する知識の習得、自社がサイバー攻撃を受けた場合における事業影響度分析、リスクアセスメントによる自社のセキュリティ状態の把握などの取組を通じて、まずは自らのセキュリティ状態を把握し、リスクを理解することが必要である。

サービス提供側の観点からは、中小企業への意識啓発や、中小企業が理解しやすい方法でセキュリティ対策の導入を促進するとともに、中小企業のセキュリティに関するリテラシーを向上させるための取組が必要になる。また、こうした取組の推進により、中小企業向けセキュリティサービスの市場を活性化することを通じて、上記中小企業の取組を促進することも求められる。

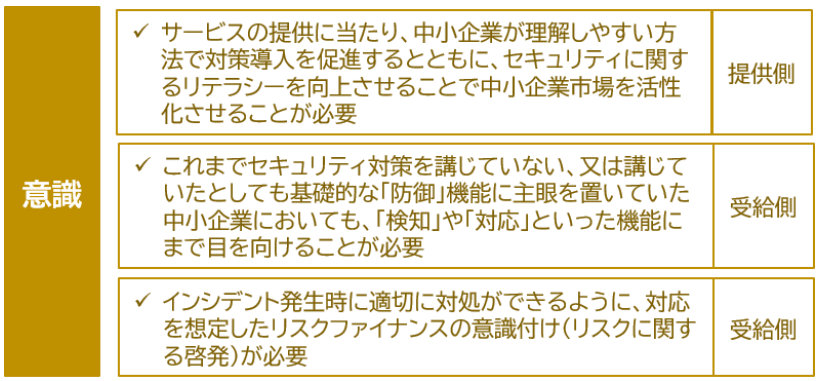

図 27 「意識」に関する課題

3.1.2. 「資源」に関する課題

企業経営においては、セキュリティ対策を経営上の「投資」に位置付けることが重要であるとの考え方[19]がある。しかしながら、本実証事業を通じて把握した中小企業の実態としては、セキュリティについて、利益を生み出すための投資として捉えるというところまでは、まだ到達できていないといえる。

中小企業は、「ヒト」「モノ」「カネ」に加えて「トキ」（時間）の制約が大きく、これらが相俟ってセキュリテュ対策の導入を阻害しているという実態があることから、この制約を打破すること、又はこの制約の中で実行性を伴うセキュリティ対策を行うことが課題となる。

中小企業側（サービス受給側）の観点からは、サイバーセキュリティに関する機能と責任を明確にした上で、セキュリティ対策を担当する組織内での役割を定義し、要員を配置することが必要である。要員については、専任であることが望ましいが、従業員数が少ない中小企業において専任担当者を置くことは現実的には困難であるケースが多いことから、まずは組織におけるサイバーセキュリティについての責任の所在を明確にした上、セキュリティベンダーや各種相談窓口などの外部の能力や知見を活用することを前提として、他の業務との兼務であったとしても、セキュリティに関する検討を行うことができるだけの態勢を整えておくことが必要である。

19 内閣官房内閣サイバーセキュリティセンター「企業経営のためのサイバーセキュリティの考え方」
https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

サービス提供側の観点からは、中小企業における資源の制約があることを踏まえて、中小企業が受容可能な低価格のセキュリティ対策サービスやサイバー保険の提供を行うことにより、中小企業における入手可能性（アベイラビリティ）を確保することが必要である。また、リテラシーが低く、要員態勢が整えられていない中小企業にあっては、導入に当たっての作業負荷や煩雑さが大きな障壁となることから、導入時のサポートを手厚くするなど、中小企業に負荷を掛けないためのサービス内容及び提供プロセスを構築することが求められる。

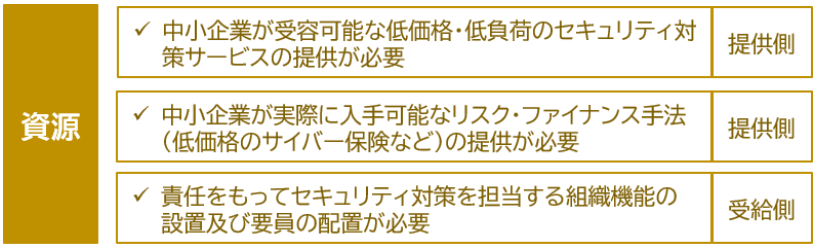

図 28　「資源」に関する課題

3.1.3. 「能力」に関する課題

中小企業は、情報システムやセキュリティ対策に関する組織機能、知識（ナレッジ）、技能（スキル）等を含む広い意味での能力を十分に保持しておらず、経営層が一定のセキュリティ意識を持っていたとしても、部分的な対策のみで完結して不十分なセキュリティ状態になっているなど、組織として効果的なセキュリティ対策を講じられていないという実態がある。このため、セキュリティ意識を実効性のあるセキュリティ対策につなげるためには、中小企業の組織的な対応能力（ケイパビリティ）を向上させることが課題となる。

中小企業側（サービス受給側）の観点からは、意識の醸成及び資源の投下を前提として、これを効率的かつ効果的にセキュリティ対策に生かすことができるように、自社のネットワークやセキュリティ対策製品・サービスに関するリテラシーを醸成することが必要である。中小企業の多くは、取引先ベンダーにネットワークの管理・運用を丸投げしていることで、自社内にネットワークに関する知見やノウハウが蓄積されていない（されにくい）という状況にあったが、中小企業が限られた資源の中でこれを内製化することは困難であることから、外部の知見や能力として活用していくことが有効であり、特にセキュリティベンダーの営業地域から外れる地方の中小企業においては、取引先ベンダーとの連携によってセキュリティ対策の導入・運用を推進していくことが望ましい。

サービス提供側の観点からは、中小企業の多くがセキュリティインシデントの発生を認識できておらず、また認識できたとしてもインシデント対応を実行することが難しいという現状を踏まえ、中小企業が運用可能な範囲で「検知」機能及び「対応」機能を備えたセキュリティ対策サービスを提供することが必要である。また、技術的な知識や導入・運用負荷を極力求めない内容の簡便なセキュリティ対策サービスとして提供され、かつ、インシデントの発生を前提として事後対応を含めたサービスとして提供されることが望ましい。

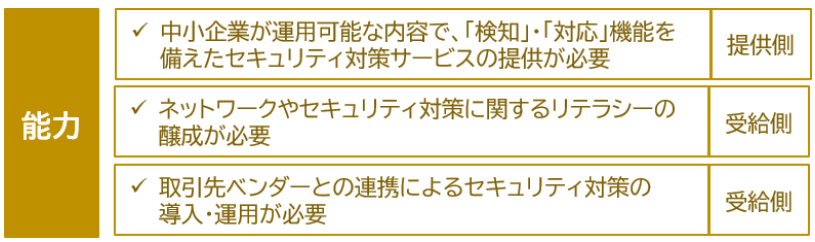

図 29　「能力」に関する課題

3.2. 中小企業向けセキュリティサービスの在り方

前記「3.1. 実証結果を踏まえた課題の抽出及び整理」において整理された課題を解消するための中小企業向けセキュリティサービスの在り方について、次のとおり考察する。

3.2.1. 中小企業向けサービスの在り方

（1） 推奨される要件

本実証事業を通じて策定された課題を踏まえ、中小企業向けサービスの在り方として推奨される要件を下記のとおり定義した。

中小企業が理解できること

- ✓セキュリティ及びその周辺事項に関するリテラシーが不足していることを踏まえて、中小企業が対策の目的や効果などを理解した上で導入できるようにコンセプトや機能をシンプルにするなど、理解を促すための工夫がなされていること。
- ✓サイバー攻撃を受けている状況をレポートや管理画面上で可視化するなど、リスクを認識させるための機能が備わっていることが望ましい。

中小企業が導入・運用できること

- ✓導入や対策に関する実行支援・相談受付等のサポートサービスが標準的に付帯されていること。
- ✓要員やリテラシーが不足していることなどを考慮し、中小企業の業務上の必要性を超えた過剰なアラート発信や通信遮断などを起こさないことが望ましい。

中小企業の価格受容性があること

- ✓中小企業が購買可能な価格設定であること。特に多額の一時金負担等を極力抑え、費用負担を期間平準化できること。
- ✓インシデント対応費用のように予算化しにくい費用については、サイバー保険を付帯するなど、リスクファイナンス機能と一体化したサービスであることが望ましい。

中小企業が実際に入手可能であること

- ✓中小企業向けサービスとしてカテゴライズされ、サービス提供者が利益を出せる形（事業として成り立つ形）で安定的に提供されること。
- ✓インターネット販売や地域のベンダーとの連携により、地方所在の中小企業であっても入手可能であること。

中小企業がセキュリティインシデントを認識し、対処につなげられるサービス（役務）であること

- ✓全てのサイバー攻撃を入口で防ぎきることができないことを前提として、「防御」だけでなく、「検知」及び「対応」に係る機能（出口対策）が実装されており、インシデント対応を支援するサービスと合わせて提供されること。
- ✓インシデント対応については、検知結果を踏まえて、サービス提供者側から中小企業にアプローチし、適切な対処を促すような支援が伴うことが望ましい。

図 30　中小企業向けサービスの在り方（推奨される要件）

(2) 地域実証で検証しきれなかった論点

地域実証で検証しきれなかった論点として、次の事項が挙げられる。

- ✓ ＷＥＢアプリ簡易診断によるウェブサイトの脆弱性診断結果を踏まえると、クラウド型ＷＡＦサービスの有効性については期待されるところであるが、導入実績がなかったため、対策としての有効性が検証できなかった。
- ✓ ＩＴシルバー人材の活用について、地域実証の中に組み込むことができなかったため、実効性についての検証ができなかった。

3.2.2. ＳＯＭＰＯリスクマネジメントが本実証事業を通じて得た知見などに基づき開発したサービス

ＳＯＭＰＯリスクマネジメントは、本実証事業を通じて得た知見などを踏まえて、次の中小企業向けサービスを開発した。

（1） SOMPO SOC（「UTM 監視・検知サービス」の後続サービス）

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。

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。

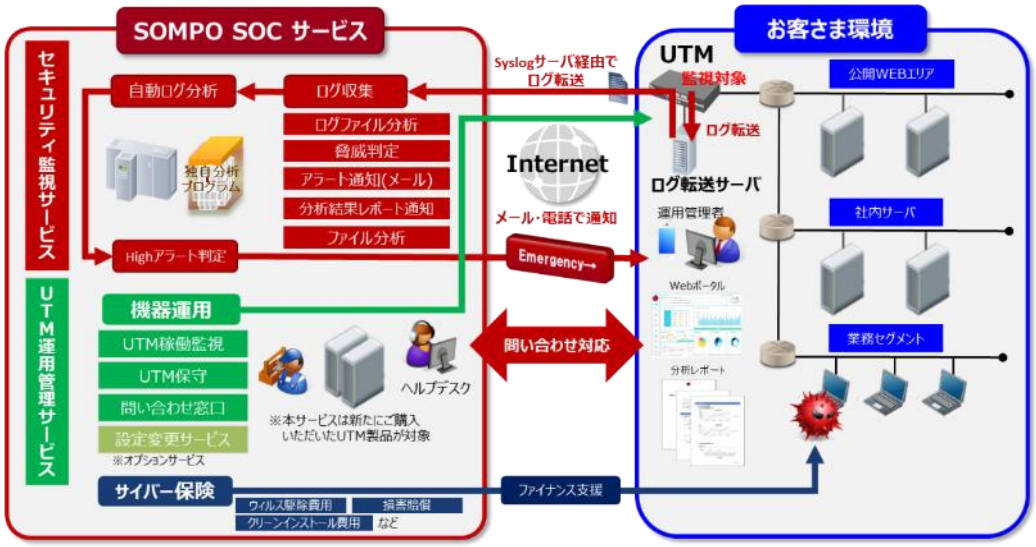

図 31 「SOMPO SOC」サービス全体像

② サービスの特長・機能

ア．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。

イ．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。

中小企業では、既にＵＴＭを導入済でも、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 16　「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・対応していただく事象。 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

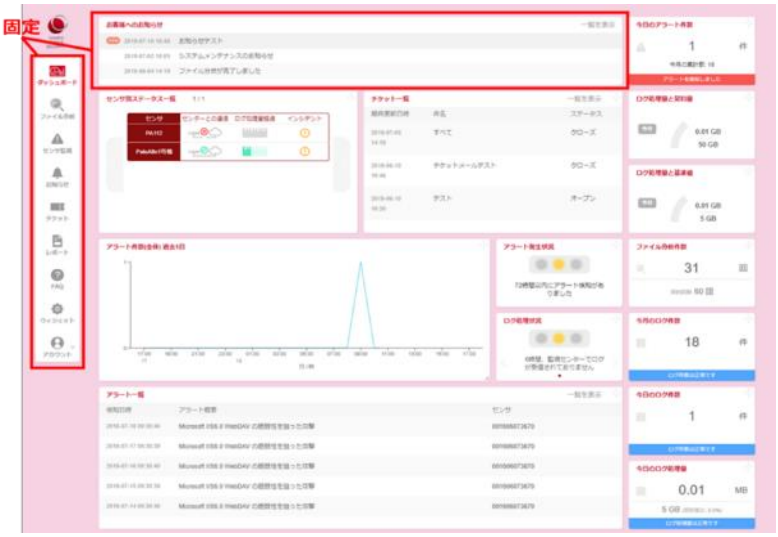

図 32　「SOMPO SOC」専用ＷＥＢポータルイメージ（ダッシュボード）

図 33　「SOMPO SOC」専用ＷＥＢポータルイメージ（アラート詳細内容）

ウ．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。

(参考)

「セキュリティ監視サービス」(販売予定価格)

初期費用：１５２，０００円（税抜)、月額利用料金：１６，０００円（税抜）

年間合計：３４４，０００円（税抜）

※分析ログ容量５Ｇの場合の初年度費用

次年度以降月額利用料金１７，０００円（税抜)、年間合計２０４，０００円（税抜）

※ＵＴＭを新たに購入する場合の「ＵＴＭ運用管理サービス」は別途要

エ．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：損害保険ジャパン日本興亜）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。

（2） SOMPO SHERIFF（「パソコン監視分析サービス」の後続サービス）

① サービスの概要

「SOMPO SHERIFF」[20]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、早期に駆除する。

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受託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。

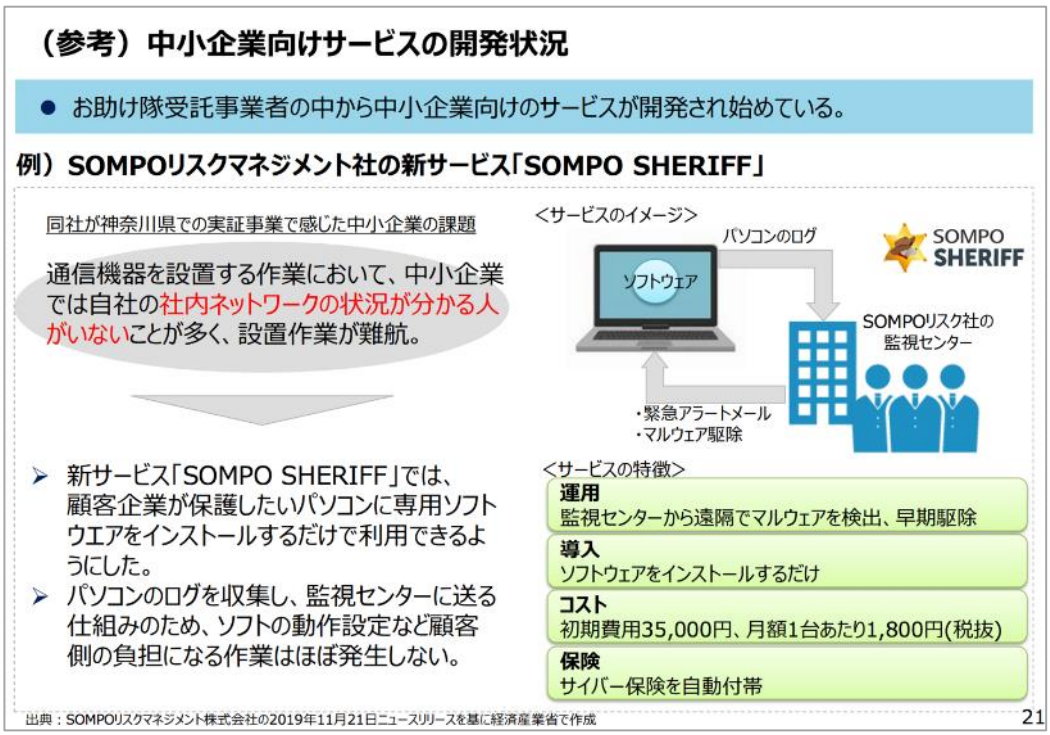

図 34 「第５回産業サイバーセキュリティ研究会ワーキンググループ２（経営・人材・国際）」資料３ 事務局説明資料（抜粋）

② サービスの特長・機能

ア．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。

イ．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及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。

[20] https://www.sompo-defnavi.com/resource/sheriff01

ウ．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きたさない。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。

エ．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。

オ．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。

（参考）

初期費用：35,000 円（税抜）、月額利用料金：1 台当たり 1,800 円（税抜）

カ．サイバー保険を自動付帯

「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）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。

キ．パソコン無料セキュリティ診断

「SOMPO SHERIFF」では、中小企業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。

3.3. 中小企業向けサイバー保険の在り方

3.3.1 推奨される要件

前記「2.1.2. 中小企業のセキュリティ対策状況の実態　(1)　サイバーリスク簡易診断アンケート結果から見える対策状況 ② サイバー攻撃を受けた場合の想定損害額」及び「2.1.4. 中小企業に対するセキュリティインシデントの実態　(3)　駆け付け支援サービスの実施内容」から、サイバー保険として備えるべき要件を次のとおり定義した。

インシデント対応費用が補償されること

- ✓中小企業がインシデント対応を行う上で必要な調査費用、不正プログラム駆除費用等が補償されること。
- ✓中小企業においては、費用対効果の観点から被害に遭った場合に調査等を行うことなく、ＯＳ再インストールやＰＣ自体の買換えを行うケースもあるため、こうした費用についてもカバーされることが望ましい。

保険金の支払だけでなく、インシデント対応サービスの提供や斡旋を合わせて提供されること

- ✓インシデントが発生した後にセキュリティベンダーを手配しようとしても、平時に取引関係がない場合には契約手続等に手間取り迅速な対応ができない可能性があることから、インシデント対応サービスの提供や斡旋がサービスとして付帯していることが望ましい。

中小企業の価格受容性があること

- ✓中小企業が加入可能な保険料設定であること。

中小企業が実際に入手可能であること

- ✓サイバー保険は、保険の目的の理解や取り付ける書類が専門的で難しく、一般的に保険代理店にとって募集が難しい保険商品として位置付けられているため、一般の加入者が気軽に加入し難いことから、保険の単独加入でなく、セキュリティ対策と併せて加入できることが望ましい。

図 35　中小企業向けサイバー保険の在り方（推奨される要件）

中小企業向け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、中小企業向けサービスにあっては、セキュリティ対策サービスへの商品付帯契約として、サイバーリスクに関してプレ・インシデントからポスト・インシデントまでを一元的にカバーできるような提供形態が望ましいといえる。

3.3.2. 地域実証で検証しきれなかった論点

本実証事業においては、実証事業の仕様に基づく制約により、実際にサイバー保険を付帯し、インシデント対応に適用していないことから、保険契約の引受け、保険金請求等の実務的な観点での在り方については検証していない。

3.4. 中小企業に向けた普及啓発の在り方

最終報告会において、地域実証において実際に発生した事故事例を紹介し、サイバーセキュリティ対策の必要性を説いた。身近な事故事例を紹介することで、最終報告会の参加者からは、「脅威を感じた。早急に対策を検討したい。」との声を多く得ることとなった。前記「3.1. 実証結果を踏まえた課題の抽出及び整理」の中で触れているとおり、自社がサイバー攻撃の被害を受けることについての想像ができていない中小企業に対してサイバーセキュリティ対策の啓発を行う上では、こうした身近な実例を示すことが有効であり、また想定損害額等のデータを提示することでリスク認識しやすくなることから、損害保険会社やＳＯＭＰＯリスクマネジメントのようなリスクマネジメント事業者と協調した普及啓発が有効であると考えられる。

4. 総括

4.1. 本実証事業の総括

ＳＯＭＰＯリスクマネジメントでは、我が国の中小企業の多くが「0.2. 本報告書の目的　図 1　中小企業における課題」に記載されるような課題を抱えているものと認識（仮説立案）し、このような課題を解決するためのサービスの在り方として、サービス受給側の中小企業にとって受け入れやすく、かつ、サービス提供側の事業者にとっても事業としての採算が取れる（ビジネスベースに乗る）仕組みが必要になると考えてきた。

本実証事業を通じて、当該仮説が中小企業の実態と合致していることが立証されたことから、中小企業に向けた関連施策の採るべき方向性として、前記「3. 考察（実施結果を踏まえた検討）」において考察した中小企業向けセキュリティサービスの在り方、中小企業向けサイバー保険の在り方及び中小企業に向けた普及啓発の在り方に沿うべきことを示すことができた。また、前記「3.2. 中小企業向けセキュリティサービスの在り方」及び「3.3. 中小企業向けサイバー保険の在り方」において推奨要件を定義し、今後具体的なサービス設計を行う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。

4.2. 考察した在り方の実現に向けて、政府への提言

中小企業向けセキュリティサービス、サイバー保険及び普及啓発をより強力に推進していくためには、次のような公的な支援があることが望ましいと考える。

地場のITベンダーに対する中小企業及びセキュリティベンダーとの協力要請

✓地方の中小企業に対してセキュリティ対策サービスを導入する上では、外部の知見や能力として中小企業の取引先ベンダーと連携した推進が望ましい。
このため、地方版コラボレーションプラットフォーム等の地域連携の場を通じて、地場のＩＴベンダーとのセキュリティ対策推進に係る協力体制を構築するなどの取組が有効であると考える。

セキュリティインシデントに関する積極的な情報開示の推進

✓リスクを認識させるには、実際の事故事例を紹介することで自社にも起こり得ることを想像させることが有効であることから、例えばサイバーセキュリティ協議会で収集した情報のうち、有益な情報については、積極的に情報開示されることが望ましい。

サイバー保険とセキュリティ対策とを一体化したサービスの普及に向けた推進

✓損害保険の商品付帯契約を引き受ける場合、各損害保険会社が自律的に適正性を判断し、個別案件ごとに保険設計を行っている。

✓インシデント対応支援を円滑にするためにサイバー保険とセキュリティ対策とを一体化したサービスとして広く展開しようとする場合には、サービスの在り方についてのガイドラインを制定して標準的なサービスとして設計できるようにするなど、サービスの普及に向けた推進がなされることが望ましい。

図 36　考察した在り方の実現に向けた提言

以上