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：広島県、山口県)
成果報告書

請負事業者：株式会社日立製作所

目次

エグゼクティブサマリー 3
1. 実施概要 6
1.1. 事業の背景・目的 6
1.2. 事業の内容 9
1.3. 実施スケジュール 9
2. 事業説明会の開催 12
2.1. 事業説明会 12
2.1.1. 集客方法 13
2.1.2. 事業説明会(事業開始) 14
2.1.3. 事業説明会(中間報告) 18
2.1.4. 事業説明会(成果報告) 20
2.1.5. 個別集客活動 21
2.2. セキュリティよろず相談会 24
3. 中小企業の実態把握 27
3.1. 支援機能とサービス 27
3.1.1. 支援機能の利用方法 27
3.1.2. 4 つのサービスでの情報収集 28
3.1.3. 情報収集の計画 29
3.2. 情報収集の実績 30
3.3. セキュリティ情報収集システム設計 / 構築 31
3.3.1. インターネット出入り口の監視サービス概要 31
3.3.2. エンドポイント監視サービス概要 33
3.4. セキュリティ機器配布 / 設置(端末) 35
3.4.1. 対応支援に必要な情報収集 37
3.5. 実証参加企業の分析 38
3.5.1. 分析概況 46
3.5.2. セキュリティ対策別実施状況 48
3.5.3. セキュリティ対策別未実施理由 52
3.5.4. 業種別セキュリティ対策実施状況 55
3.5.5. 組織規模別セキュリティ対策実施状況 60
3.5.6. 標的型攻撃対策問診結果との比較 66

4. 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 69
4.1. (3 つの機能)を備えた支援体制の構築 69
4.2. 地元企業との連携 70
5. 地域実証の実施 72
5.1. 支援内容と実績 72
5.1.1. セキュリティ対策の簡易アセスメントによる支援 74
5.1.2. 現場セキュリティアセスメントによる支援 77
5.1.3. インターネット出入り口の監視サービス(UTM)による支援 81
5.1.4. エンドポイント監視サービスによる支援 85
5.2. セキュリティ監視の内容と実績 86
6. 実証結果を踏まえた検討の実施 89
6.1. 中小企業サイバーセキュリティ支援に必要な人材スキル 89
6.2. 実証終了後のサービス提供の検討 90
6.2.1. サイバーセキュリティ支援サービス関連 90
6.2.2. サイバー保険のあり方検討 93

エグゼクティブサマリー

◆ 目的

本章は「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」成果報告書を要約したものである。

本国の産業競争力全体において大きな影響力を持っている中小企業に対してサイバーセキュリティ対策支援を進めることは喫緊の課題であり、必要とされるサービスを提供し中小企業のセキュリティ対策強化を図る必要がある。本事業は中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らかにし、中小企業の支援機能を低コストで構築することで、中小企業のセキュリティ対策強化、サイバーセキュリティの意識向上を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを目的とする。

中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らかにするための中小企業の実態把握を行うために、以下の 3 つの機能を備えた体制の構築を行い、4 つのサービス提供にて中小企業の実態調査、セキュリティサービス提供におけるセキュリティ対策実装時の課題抽出及び、中小企業に向けたサイバーセキュリティの事後支援を実施した。

◆ 実施対象と地域

本事業の対応地域は当初、重要産業(防衛、自動車)及びそのサプライチェーンを構成する中小企業が多数集積する広島を中心に周南、徳山、防府を含めた地域で本事業を開始した。早期の目標達成、効果的な実証の実現に向けて対象地域を広島県と山口県とし実証参加の中小企業数を**110社**として事後支援サービスの展開を行った。

◆ 実施内容

中小企業の実態と必要なセキュリティサービス、サイバー保険について検討した結果を報告する。

● <3 つの支援機能>

①中小企業からの相談受付及び対応

②相談内容がサイバーインシデント等であるかの判断

③サイバーインシデント等が発生した際の支援の提供

● <４つのサービス>

(1) セキュリティ対策の簡易アセスメント

中小企業のセキュリティ対策状況の把握を目的として、個々の中小企業のセキュリティ対策状況を株式会社日立製作所（以下「日立製作所」という。）の分析ナレッジを利用した診断書を利用し、優先すべきセキュリティ対策の課題を可視化した。

(2) 現地セキュリティアセスメント

専任コンサルタントが現場に訪問し、インタビュー形式によるヒアリング、およびセキュリティ対策実機の確認によりセキュリティ対策の簡易アセスメント結果とのギャップ抽出を行い、具体的に必要なセキュリティ対策の意識付けを図った。

(3) インターネットの出入り口の監視サービス

インターネットの出入り口に統合脅威管理装置(UTM※1)を導入し通信内容の監視を行い、セキュリティインシデント等の実態把握とセキュリティ対策機器を現場に導入する際の問題点を抽出した。

(4) エンドポイント監視サービス

エンドポイント(PC)にセキュリティ監視エージェント(EDR※2)を導入しマルウェア等の不正な挙動について監視を行い、セキュリティインシデント等の実態把握とセキュリティ対策製品を現場に導入する際の問題点を抽出した。

◆ **求められる人材スキルとサービス**

事業説明会での施策である「セキュリティアセスメント、アンケート、セキュリティよろず相談会」ならびに実証事業の収集データより中小企業のセキュリティ対応サービスの内容、求められる人材スキル内容を整理した。

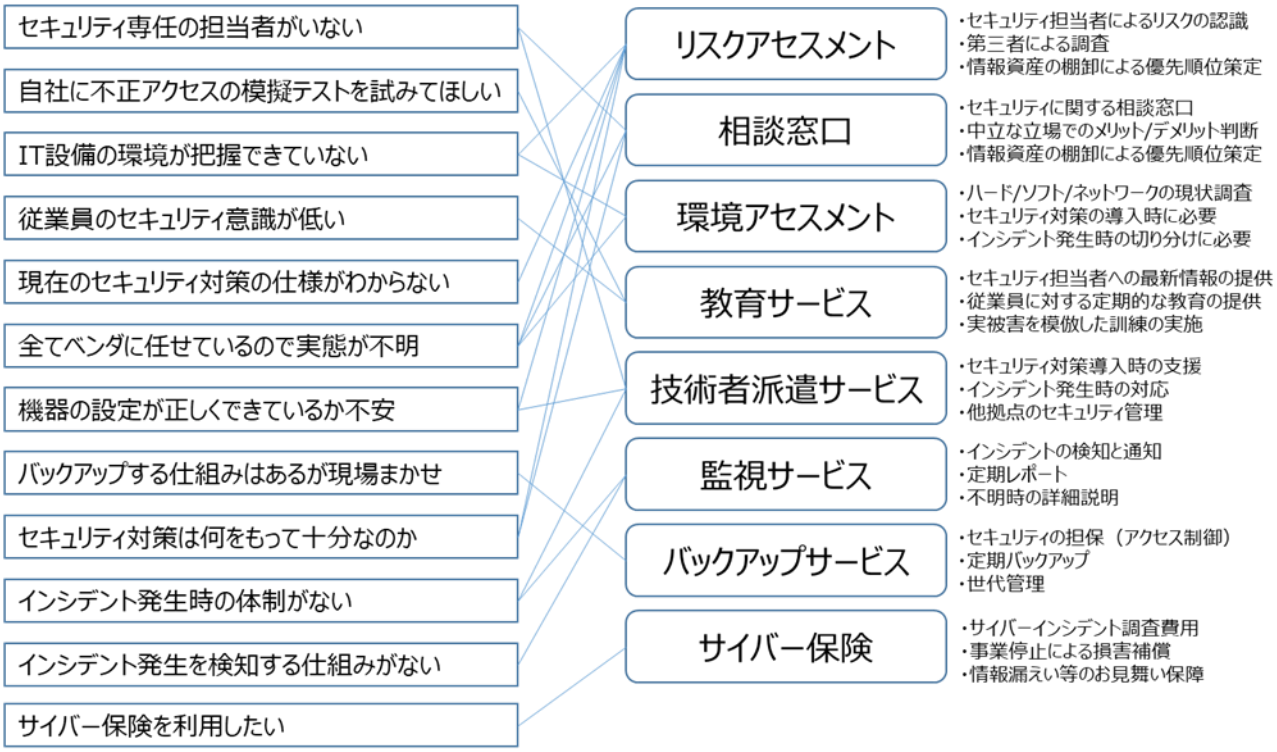


図 1 中小企業の声からの必要なサービス

また、中小企業に必要なサービスの検討は、以下の 5 つの観点より、セキュリティ対策実装の相談窓口や、セキュリティ対策製品の導入における事前調査を含めた環境コンサルティングが必要と考える。

(1) 中小企業でセキュリティ対策要員の有無の調査では、「社員での対応が可能」+「外注に依頼している」を合わせて 36%であった。また、セキュリティ対応要員が「いない」との回答は全体の 25%であり、セキュリティ対策に対応できる人材がさらに必要と考える。

※1 UTM：Unified Threat Management の略　※2 EDR: Endpoint Detection and Response の略

(2) よろず相談の内容、現地セキュリティアセスメントからも、セキュリティ製品が「どのようなインシデントに対応するのか」、「どのような対策を行えばよいのかわからない」の声も聴かれる。中小企業においてはセキュリティ対策、およびその必要性の認知度の低さも一要因となっている。

(3) セキュリティ対策の簡易アセスメントより、「パターンに依存しないアンチウィルス」などの新しいウイルスの検知防御に対応できていない。また、「情報の流出を防止する（出口対策）」の実装率が低いため、マルウェア感染後に情報が流出するリスクは高いと考える。

(4) セキュリティ対策の導入においては、中小企業に向けたサイバーセキュリティ対策製品を効率よく、また的確に導入させるため、セキュリティ対策の導入前に現状を調査するサービス等にて実証参加企業環境の可視化をする必要があると考える。

(5) 今回の提供サービスで統合脅威管理装置(UTM)導入時の環境確認では、製造機器、情報系機器が同一 LAN に混在している企業もあった。この場合、製造機器については、機密性よりも可用性を重視するケースが多いため影響を考慮したセキュリティ機器の実装を行わないと生産ライン等に影響を与える可能性があると考える。今後が Society5.0、Connected Industries が実現する社会が浸透していくと、情報系のプロトコルのみでは対応できない状況や、製造機器への影響なども考慮したセキュリティ対策機器の導入が必要と考える。

◆ **サイバーセキュリティ保険のあり方**

サイバーセキュリティ保険については、以下の２つの案をベースとして検討ができると考える。

(1) 中小企業向けセキュリティサービスへのサイバー保険自動付帯

（保険加入スキーム＋普及啓発の観点）

- 統合脅威管理装置(UTM)やエンドポイント(EDR)等の監視系サービスへサイバー保険を自動的にセットして販売する。
- 監視サービスの機能に連動させることで保険の有無責の判断を早期に行い、同時に付帯サービスの活用をより円滑に行う。（インシデント対応をサポートするベンダの手配も含めた迅速な保険対応）
- 企業の保険料負担はないが補償範囲は限定的なため、いわゆる“自賠責保険”のような位置づけであり、別途通常のサイバー保険加入を促すための導線が必要。

(2) サイバー保険 付帯サービスの拡充

（付帯サービス＋普及啓発の観点）

- インシデント発生時の対応サービスだけでなく、平時の対策の策定に向けた簡易なリスクアセスメントや診断・スコアリングサービス等を提供。
- 緊急時の原因調査やコールセンターの設置、除去・回復等に関わるサービスについては、円滑な初動対応に向けた活用しやすいスキームを構築。

1. 実施概要

1.1. 事業の背景・目的

IoT や AI といった技術により実現される「Society5.0」「Connected Industries」では、サイバー空間とフィジカル空間が密接に関わることにより、サイバー攻撃がフィジカル空間へ及ぼす影響が大きくなる。また、「Connected Industries」を始めとするネットワーク化の進展は、企業間のつながりなど様々な形のつながりを生むため、悪意のある者にとって新たな攻撃の機会となるおそれがある。さらに、攻撃の手法も進化しており、サイバー攻撃の脅威はあらゆる産業活動に潜むようになっている。例えば、スマートフォンのファームウェアに、ユーザの個人情報等を国外に送信する機能が埋め込まれる等、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつある。

サイバーセキュリティ対策を理由として、サプライチェーンへ参加できなくなる中小企業が多数生まれることは、多くの中小企業の経営を苦しめるだけでなく、我が国の産業競争力全体にとって大きな影響を与えることになるため、中小企業のサイバーセキュリティ対策支援を進めることは喫緊の課題である。

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

このような実態から、困ったときに気軽に相談できる窓口や、サイバー攻撃に遭った際に事後対応をするサービスに対するニーズはあるが、サービス提供側が、中小企業の被害実態や、中小企業支援に必要な人材スキル等の把握ができていないため、現状は中小企業のニーズに合った製品、サービスが提供されてない。

そのため、中小企業の被害実態等を把握することで、中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らかにし、中小企業の支援機能を低コストで構築することで、中小企業のセキュリティ対策強化を図る必要がある。

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

- Society5.0、Connected Industries が実現する社会

  ネットワーク化や IoT(Internet of Things)の利活用が進む中、世界では、ドイツの「インダストリー4.0」等、ものづくり分野で IT を最大限に活用し、第４次産業革命とも言うべき変化を先導していく取組みが、官民協力の下で打ち出され始めている。

  我が国においても、平成 28 年 1 月 22 日に閣議決定された「第 5 期科学技術基本計画」において、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱して

いる。また、経済産業省においては「Society5.0」の実現に向けて、様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取組を推進されている。

【出典】「Society 5.0 で実現する社会」(内閣府)
URL：https://www8.cao.go.jp/cstp/society5_0/index.html

図 1.1 Society 5.0 で実現する社会のイメージ

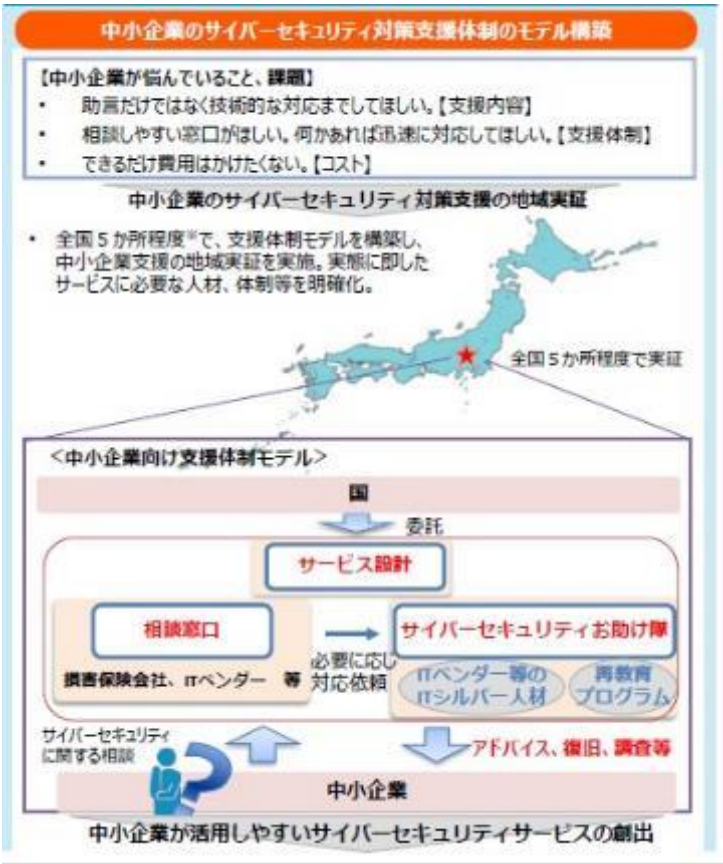
- サプライチェーンを構成する中小企業のサイバーセキュリティ対策の強化

「Society5.0」へ向け、様々なデータのつながりが価値を生む一方、サイバーセキュリティの面では、サプライチェーン全体での対策の必要性が高まっている。また、グローバルサプライチェーンの中で、我が国企業が競争力を確保するためにも、中小企業を含めて諸外国の規制動向も踏まえながら、サイバーセキュリティ対策を推進していく必要がある。

このため、サプライチェーンを構成する中小企業のサイバーセキュリティ対策の強化に向け、中小企業のニーズに合致した支援体制の構築が必要である。

本事業では、損害保険会社、IT ベンダの連携や、中小企業に対する専門的なアドバイス等を実施する支援体制のモデルを構築し、地域実証を行う。

実証を通じ、中小企業のサイバーセキュリティ対策の実態を把握し、実態に即したサービス内容やこれに求められる人材のスキル、支援体制等を明らかにすることにより中小企業が活用しやすいサイバーセキュリティサービスの創出をめざす。



【出典】第４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１

(制度・技術・標準化) 資料 5(経済産業省)

URL： https://www.meti.go.jp/main/yosangaisan/fy2019/pr/ip/shojo_09.pdf

図 1.2 中小企業サイバーセキュリティ対策支援のイメージ

日立製作所は、広島県情報産業協会及び中国経済局、損害保険会社等と連携し重要産業(防衛、自動車)及びそのサプライチェーンを構成する中小企業が多数集積する広島を中心に周南、徳山、防府を含めた地域で当初、本事業を行うこととした。

その後、早期の目標達成、効果的な実証実現に向けて対象地域を広島県と山口県として本事業を行った。

広島県と山口県の中小企業の中で、約１万社に本実証事業への参加を呼びかけた結果、**110 社**の中小企業に参加頂いた。

参加を呼び掛けた中小企業の全体数からすると、極一部の対象ではあるが、中小企業におけるサイバーセキュリティの意識向上は図れたものと考えている。

本実証事業にて中小企業の実態を把握出来たことから、今後、サイバーセキュリティ対策の定着に向けて、必要なサービスについて検討して行く。

1.2. 事業の内容

本事業では、損害保険会社、IT ベンダの連携や、中小企業に対する専門的なアドバイス等を実施する支援体制のモデルを構築し、地域実証を行う。

実証を通じ、中小企業のサイバーセキュリティ対策の実態を把握し、実態に即したサービス内容や求められる人材のスキル、支援体制等を明らかにすることにより中小企業が活用しやすいサイバーセキュリティサービスの創出を目指した検討を行う。

1.3. 実施スケジュール

本実証事業の実施に当たっては、各種プロジェクトマネジメントの資格保有、プロジェクト経験実績のあるメンバーによる作業計画の策定を行い、過去の類似プロジェクトの経験者や、現行のサイバーセキュリティ対策サービスの実務者を本事業の推進体制に含め推進する。

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

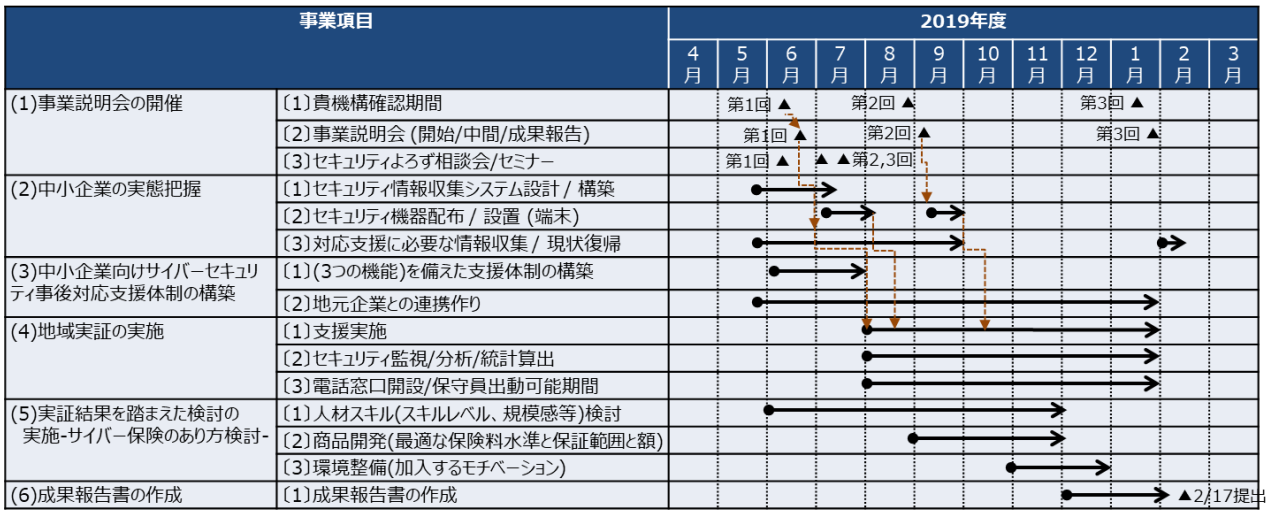


図 1.3 本事業の実施スケジュール（計画時）

（１） 事業説明会の開催

事業の対象である地域の中小企業へ向けて、本実証事業の周知及び参加呼びかけを行うことを目的とする。さらに、当該説明会の参加者に対しサイバーセキュリティに関する普及啓発を行い、中小企業のセキュリティ対策に関する意識向上を図る。

- 事業説明会(事業開始)

「中小企業の情報セキュリティ対策ガイドライン」やサイバー保険の利用の仕方、セキュリティ診断による可視化などを、参加者に説明する。

参加中小企業にセキュリティアセスメントシートに記載していただき、セキュリティアセスメントシートの分析結果を回答することにより、現状のセキュリティリスクや中小企業の実態を可視化させ、サイバーセキュリティ対策の意識向上を図る。

実施日：6 月に 1 回、7 月に 2 回の計 3 回の実施を計画。

また、参加申込企業数が目標数に届かない場合は、事業説明会(事業開始)の実施回数の増を日立製作所が検討する。

- 事業説明会(中間報告)

広島県情報産業協会及び中国経済局、損害保険会社等と連携し、広島を中心としたエリアで説明会を実施する。

「中小企業セキュリティガイドライン」への理解の促進、サイバー保険の利用の仕方、実証の中間報告を実施する。

実施日：9 月上旬の実施を計画。

- 事業説明会(成果報告)

広島県情報産業協会及び中国経済局損害保険会社等と連携し、広島を中心としたエリアで説明会を実施する。「中小企業セキュリティガイドライン」への理解の促進、サイバー保険の利用の仕方、実証の成果報告を実施する。

実施日：1 月下旬の実施を計画。

（2） 中小企業の実態把握

現地で「セキュリティよろず相談会」の実施により、中小企業の状況・スキル等の実態情報を収集する。セキュリティアセスメント(セミナー開催時のアンケート)の実施、現場セキュリティアセスメントの実施等により、詳細な現場のセキュリティ実態情報を効果的に収集する。

現場への機器導入等によるセキュリティインシデントの情報収集のためのセキュリティ監視サービスを実証参加企業先に導入することで、継続した情報(中小企業の生の声・セキュリティインシデントの実態)の収集を行う。

（3） 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

- 受付チームによる中小企業からの相談受付及び対応(機能①)
- 相談内容がサイバーインシデント等であるかの判断（機能②)
- サイバーインシデント等が発生した際の支援の提供(機能③)

上記 3 つの機能を備えた体制を既存の実績のあるサービスインフラで提供する。

広島県情報産業協会及び中国経済局、損保会社等と連携し、重要産業及びそのサプライチェーンを構成する中小企業が多数集積する広島を中心に周南、徳山、防府を含めた地域で本事業を行う。

（４） 地域実証の実施

2019 年 8 月~2020 年 1 月までの 6 か月間を実証期間として推進する。

約 120 社の会員を持つ地域の業界団体　広島県情報産業協会及び中国経済局、損保会社等を含めた地域コミュニティを活用し、中小企業を中心に 100～200 社程度を確保する。

（５） 実証結果を踏まえた検討の実施

実証を通じた実態把握のデータより中小企業の保険加入(活用)の促進策の方向性を整理し、保険サービスメニューのレベル分けなども含め、中小企業が利用しやすいサイバー保険の検討を実施する。

「セキュリティアセスメント、アンケート、セキュリティよろず相談」ならびに実証事業の収集データより中小企業のセキュリティ対応サービスの内容、求められる人材スキル内容を整理し、各種サービスメニューのレベル分けなどの検討を実施する。

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

（６） 成果報告の作成

上記の（１）～（５）についての結果を成果報告書として作成する。

本事業のスケジュールで計画からの大きな差異は、図 1.4 本事業の実施スケジュール（実績）の（２）中小企業の実態把握、〔２〕セキュリティ機器配布／設置(端末)であり、当初計画していた事業説明会のみでは、セキュリティ機器の導入参加企業の目標数を確保できなかったため、対象地域の拡大、および説明会の追加実施等を行いセキュリティ機器の導入参加企業確保を行った事により延長となった。

詳細な内容は 2.1.5 個別集客活動ならびに、3.4 セキュリティ機器配布 / 設置(端末)に記載する。

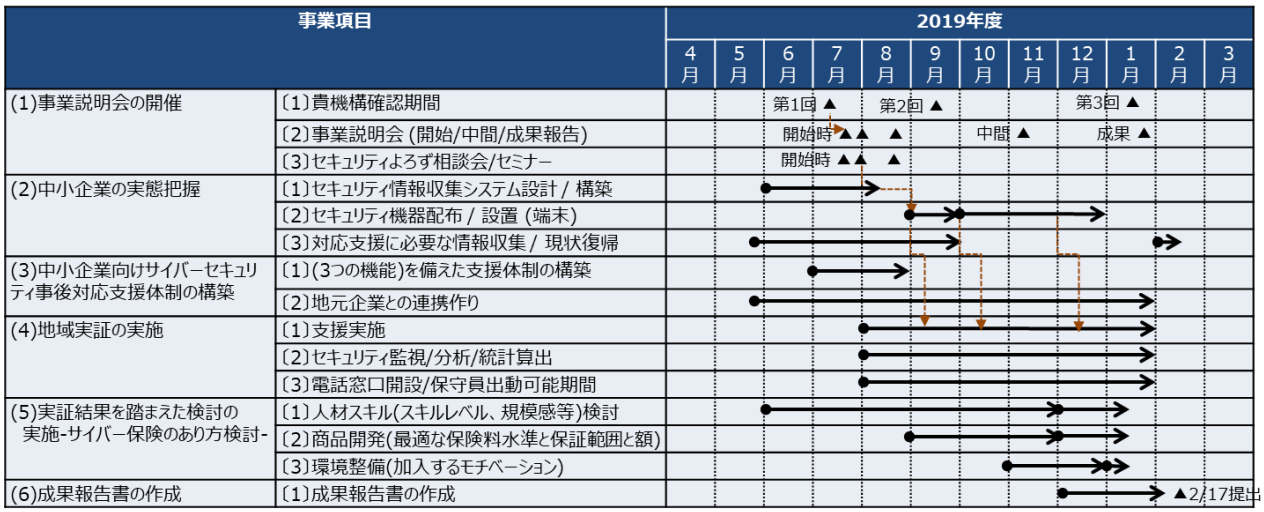


図 1.4 本事業の実施スケジュール（実績）

2. 事業説明会の開催

本事業の中小企業への周知及び、実証サービス参加企業集客のため、広島県情報産業協会及び中国経済局、損保会社等と連携し事業説明会を開催した。

本章では、事業説明会の回数、集客方法、実施内容及び成果について報告する。

2.1. 事業説明会

広島県情報産業協会及び中国経済局、損害保険会社等と連携し、広島を中心としたエリアで説明会を実施とし、説明会およびセミナー等は、事業開始(6 月 1 回、7 月 2 回の 3 回)、中間報告(9 月 1 回)、成果報告(1 月 1 回)の計 5 回を実施する予定であったが、事業参加企業の促進を行うため、事業説明会(事業開始)の追加開催を計画し、事業説明会(事業開始)5 回、事業説明会(中間報告)1 回、事業説明会(成果報告)1 回の計 7 回を実施した。

内容	計画	実績
事業説明会(事業開始)	3 回	5 回
事業説明会(中間報告)	1 回	1 回
事業説明会(成果報告)	1 回	1 回
合計	5 回	7 回

表 2.1 事業説明会の実施回数

2.1.1. 集客方法

中国経済産業局からのメールマガジン会員への広報、広島商工会議所、福山商工会議所、呉商工会議所より工業部会員へのダイレクトメール（郵送）、商工会議所で過去に開催したセキュリティセミナー参加者への FAX での案内及び、一般社団法人広島県情報産業協会(以下「広島県情報産業協会」という。)、日立製作所グループの顧客等へダイレクトメール、電話、訪問によるお声がけを通じ、延べ約 13,000 社に対して御案内を実施した。また、地元の中小企業向けメディアからの発信（ひろしまサンドボックス等地元誌への記載）、福山商工会議所会報へのセキュリティ関連記事の掲載による広報も併せて実施した。

事業説明会(事業開始)5回での参加社数は109社で、参加者数/案内数での割合は0.86%にとどまった。

また、分析内容からも面識のある方からのご案内（地元企業の勧誘、営業個別勧誘）が効率的であり集客を効率よく促すには「知己（信頼のおける）のあるベンダ」からの中小企業のご担当者に向けた「わかり易い主旨説明」が有効である。(表 2.2 事業説明会(事業開始)連絡手法別状況 参照)

開催会場（開催日）	案内数	連絡方法	手段	手段別案内数	手段別参加社数	手段別参加社数(%)	参加社数(%)	実証参加中小企業数(%)
広島商工会議所（7/24）（7/29）	4,545社	ダイレクトメール	郵送/FAX/手渡し	2,100社	18社	0.86%	65社（1.43%）	40社（0.88%）
		個別ダイレクトメール	メール	1,290社	2社	0.16%		
		地元企業の勧誘	メール	30社	6社	20.0%		
		HIAからのご案内	メール	1,000社	3社	0.30%		
		営業個別勧誘	対面勧誘・メール	125社	12社	9.60%		
福山商工会議所（7/31）	5,036社	ダイレクトメール	郵送/FAX	5,000社	2社	0.04%	11社（0.22%）	9社（0.18%）
		地元企業の勧誘	メール/電話	15社	3社	20.0%		
		営業個別勧誘	メール/電話	21社	3社	14.3%		
呉商工会議所（8/1）	3,025社	ダイレクトメール	郵送・FAX	3,000社	5社	0.17%	12社（0.40%）	9社（0.30%）
		地元企業の勧誘	メール/電話	15社	3社	20.0%		
		営業個別勧誘	メール/電話	10社	1社	10.0%		
日立笠戸協同組合(8/26)	31社	地元企業の勧誘	メール/FAX	31社	21社	67.7%	21社（67.7%）	20社（64.5%）
合計	12,606社						109社（0.86%）	78社（0.61%）

表 2.2 事業説明会(事業開始)連絡手法別状況

実証参加の中小企業については、重要産業及びそのサプライチェーンを構成する中小企業が多数集積する広島を中心に周南、徳山、防府を含めた地域で事業説明会(事業開始)を当初計画の 3 回から 4 回に増やし実施した。目標 100 社の実証参加企業を募集してきたが、4 回の説明会で実証参加の中小企業が目標 100 社の 6 割程度であった。

実証事業の対象地域について事業説明会後のよろず相談、ホームページ参照からのお問い合わせ等により個別説明を求める声もあった。事業開始当初計画していた、周南、徳山、防府地区の対象企業に加えてさらにこれら地域の企業と取引等がある関連企業にまで対象を広げ実証参加の中小企業数の増加を行った。

説明会の会場を山口県とし追加説明会の開催、集客方法としては、日立製作所ホームページでの案内の他 、日立笠戸協同組合経由にて傘下企業 31 社に直接、実証参加を働きかけ山口県周南市、防府市以外の他市町村の中小企業に対してアプローチした。

また、日立製作所グループの山口支店のパートナーを含めたコネクション (10 社程度)を活用しての勧誘活動を実施し、山口県では 20 社の実証参加企業を確保した。また、企業側のご都合で事業説明会のような集合説明会に参加いただけない場合については、継続的に小規模集合(5 名程度)で実施するミニセミナー、企業への個別訪問またはオンライン会議システムによる個別説明を実施し、110 社の実証参加企業を確保した。

詳細については 2.1.5 個別集客活動に記載する。

2.1.2. 事業説明会(事業開始)

事業説明会(事業開始)は、中国経済局、広島、福山、呉の商工会議所及び、地域の業界団体である、広島県情報産業協会、損害保険会社等と連携し広島県内 3 か所の計 4 回、追加開催として山口県エリアで 1 回実施した。以下に開催場所、開催日、参加企業数、事業参加の中小企業数を記載する。

項	事業説明会(事業開始)開催場所	開催日	参加企業数（人数）	実証参加中小企業数
1	広島商工会議所 会議室	2019 年 7 月 24 日	29 社（46 名）	18 社
2	広島商工会議所 会議室	2019 年 7 月 29 日	36 社（62 名）	22 社
3	福山商工会議所会議室	2019 年 7 月 31 日	11 社（21 名）	9 社
4	呉商工会議所会議室	2019 年 8 月 1 日	12 社（15 名）	9 社
小 計			88 社（144 名）	58 社
5	日立笠戸協同組合	2019 年 8 月 26 日	21 社（26 名）	20 社
合 計			109 社（170 名）	78 社

表 2.3 事業説明会(事業開始)実績

2.1.2.1. 実施内容

説明会では、事業内容の説明とサイバーセキュリティの普及啓発を行い、意識向上を図るため、セミナー形式での開催として以下の内容にて実施した。

- サプライチェーンの中での中小企業にかかるサイバーセキュリティの事故事例の紹介。
- 中小企業の支援施策内容の紹介。
  - 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介。
- 中小企業向けサイバーセキュリティ事後対応支援事業の説明。
  - 本実証事業の目的、実施内容とスケジュール、実施体制、実証での提供サービス概要。

- 中小企業向けサイバーセキュリティ事後対応支援事業内での提供サービスの説明。
  - サイバーセキュリティ事後対応支援事業内での 4 種類の提供サービス具体的な内容、仕組みおよび提供方法の説明。
  - 「セキュリティ対策の簡易診断」の実施。図 2.2 情報セキュリティ 10 大脅威 2019 （IPA ホームページより）より、組織での脅威 1 位である「標的型攻撃による被害」に関する「セキュリティ対策の簡易診断」を実施し、内容の診断後に、セキュリティ診断書として、現在のセキュリティ対応状況、および弱点の可視化、今後の優先対策案を記載しメールまたは郵送にて送付しサイバーセキュリティ対策の意識向上の支援を実施した。
  - 「セキュリティ対策の簡易診断」はセミナー形式で実施し、専門用語、サイバーセキュリティ対策の仕掛けについて設問ごとに解説を行いながら実施した。また、専門スタッフの会場内配置により質問・相談が行えるようにして、IT リテラシーが高くない方でも「セキュリティ対策の簡易診断」に回答頂けるようにして実施した。
- 中小企業向けサイバーセキュリティ事後対応支援事業終了後の提供サービスの説明。
  - 実証終了後の提供サービスの継続的に利用する場合の価格、条件についての説明を実施。
- 説明会の終了後、希望者について個別のサイバーセキュリティに関するよろず相談会を実施。

開催に際して、地元の中小企業の参加しやすい時間帯、開催時間について地域の商工会議所からアドバイスを頂き、午後開始で 1.5 時間程度での実施内容として設定した。

以下に事業説明会(事業開始)実施時の内容を記載する。

項	時間	報告項目	発表者
1	15:00～15:05	開会	日立製作所
2	15:05～15:10	挨拶	広島県情報産業協会
3	15:10～15:40	講演：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
4	15:40～16:00	お助け隊事業内容について	日立製作所
5	16:00～16:20	お助け隊ご提供サービスのご紹介	株式会社　日立システムズ （以下「日立システムズ」という。）
6	16:20～16:50	セキュリティ対策の簡易診断	日立システムズ
7	16:50～17:00	お助け隊 今後の計画のご説明	日立システムズ

表 2.4 広島商工会議所実施内容（2019 年 7 月 24 日、7 月 29 日）

図 2.1 事業説明会(事業開始)広島商工会議所実施風景

項	時間	報告項目	発表者
1	―	開会	日立製作所
2	15:00～15:05	挨拶	福山商工会議所
3	15:05～15:40	講演：サイバー攻撃の最新動向と対策に向けた取組や中小企業に求められる対策 ※中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介含む	日立製作所
4	15:40～15:50	お助け隊事業内容について	日立製作所
5	15:50～16:00	お助け隊ご提供サービスのご紹介	日立システムズ
6	16:00～16:25	セキュリティ対策の簡易診断	日立システムズ
7	16:25～16:30	お助け隊 今後の計画のご説明	日立システムズ

表 2.5 福山商工会議所実施内容（2019 年 7 月 31 日）

項	時間	報告項目	発表者
1	―	開会	日立製作所
2	13:30～13:35	挨拶	呉商工会議所
3	13:35～14:10	講演：サイバー攻撃の最新動向と対策に向けた取組や中小企業に求められる対策 ※中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介含む	日立製作所
4	14:10～14:20	お助け隊事業内容について	日立製作所
5	14:20～14:30	お助け隊ご提供サービスのご紹介	日立システムズ
6	14:30～14:55	セキュリティ対策の簡易診断	日立システムズ
7	14:55～15:00	お助け隊 今後の計画のご説明	日立システムズ

表 2.6 呉商工会議所実施内容（2019 年 8 月 1 日）

項	時間	報告項目	発表者
1	―	開会	日立製作所
2	13:30～13:35	挨拶	呉商工会議所
3	13:35～14:10	講演：サイバー攻撃の最新動向と対策に向けた取組や中小企業に求められる対策 ※中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介含む	日立製作所
4	14:10～14:20	お助け隊事業内容について	日立製作所
5	14:20～14:30	お助け隊ご提供サービスのご紹介	日立システムズ
6	14:30～14:55	セキュリティ対策の簡易診断	日立システムズ
7	14:55～15:00	お助け隊 今後の計画のご説明	日立システムズ

表 2.7 日立笠戸協同組合 実施内容（2019 年 8 月 26 日）

■「情報セキュリティ10大脅威 2019」　　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位 (*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

（*1）クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

URL https://www.ipa.go.jp/security/vuln/10threats2019.html

図 2.2 情報セキュリティ 10 大脅威 2019

2.1.3. 事業説明会(中間報告)

事業説明会(中間報告)は、実証参加企業が多い、広島にて開催した。

集客方法としては、日立製作所ホームページでの案内の他 、事業説明会(事業開始)の参加者、事業説明会(事業開始)とは個別に事業参加を募った企業に対して、メールによる案内およびテレマーケティングを利用した電話での説明会の参加を働きかけ 18 社の企業の参加予定を確保した。実績としては、説明会への欠席者もあり最終的には 15 社の参加であった。

以下に開催場所、開催日、参加企業数、事業参加の中小企業数を記載する。

項	事業説明会(中間報告)開催場所	開催日	参加企業数（人数）	中小企業数
1	日立システムズ　中国支社 会議室	2019 年 11 月 6 日	15 社（17 名）	11 社

表 2.8 事業説明会(中間報告)実績

2.1.3.1. 実施内容

説明会では、事業実施状況の中間報告、サイバーセキュリティの普及啓発を行い、意識向上を図るため、セミナー形式での開催として以下の内容にて実施した。

- サプライチェーンの中での中小企業かかるサイバーセキュリティ被害で事業存続にかかわる実状の紹介。
- 中小企業の支援施策内容の紹介。
  - 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介。
- 中小企業向けサイバーセキュリティ事後対応支援事業の説明。
  - 本実証事業の目的、実施内容とスケジュール、実施体制、中間報告の位置づけを説明。
- 中小企業向けサイバーセキュリティ事後対応支援事業の中間報告
  - 本事業の 10 月時点の参加企業の状況、「セキュリティ対策の簡易診断」の分析結果の報告、よろず相談会での相談対応から、資料ご紹介の実施。
- サイバー保険の概要と今後の方向性の説明。

項	時間	報告項目	発表者
1	―	開会挨拶	日立製作所
2	14:00～14:10	本事業と中間報告について	日立製作所
3	14:10～14:45	講演：「サイバーセキュリティ ～中小企業に迫る事業存続の危機～」	日立製作所
4	14:45～14:55	サイバーセキュリティお助け隊の中間報告について	日立システムズ
5	14:55～15:15	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	15:15～15:25	サイバー保険の概要と今後の方向性について	日立システムズ
7	15:25～15:30	サイバーセキュリティお助け隊提供サービスの説明	日立製作所

表 2.9 事業説明会(中間報告)実施内容

中間報告の主な内容を以下に記載する。

実証事業参加状況（2019/10/25 時点）		
1	アセスメント実施数(参加者数)	101 社(150 名)
2	辞退、無効社数(中小企業以外)	7 社(中小以外 6 社)
3	有効参加社数	94 社

表 2.10 事業説明会(中間報告)の報告内容 1

提供サービス実績報告		
1	セキュリティ対策の簡易診断	実施済 94 社
2	現場セキュリティアセスメント	実施済 6 社
3	インターネットの出入り口の監視サービス	導入済 1 社
4	エンドポイント監視サービス	導入済 4 社

表 2.11 事業説明会(中間報告)の報告内容 2

事業説明会(中間報告)の効果としては、中小企業のセキュリティ対策の簡易アセスメント集計分析より、被害を食い止める（出口対策）部分のセキュリティ対策の実施が弱いことが分かった。セキュリティリスクの危機感を覚えて、本事業で提供するサービスの導入検討を頂き、サービス利用頂ける成果につながった。

事業説明会(中間報告)参加での提供サービス導入数		
1	現場セキュリティアセスメント	追加実施 1 社
2	インターネットの出入り口の監視サービス	追加導入 2 社
3	エンドポイント監視サービス	追加導入 2 社

表 2.12 事業説明会(中間報告)参加での提供サービス導入数

2.1.4. 事業説明会(成果報告)

事業開説明会（成果報告）は、実証参加が多かった広島エリアにて開催を行った。

日立製作所のホームページへの掲載、事業開始説明会の参加者、事業開始説明会とは個別に事業参加を募った企業向けにメールによる案内及び、電話での参加依頼を行った。

以下に開催場所、開催日、参加企業数、事業参加の中小企業数を記載する。

項	事業説明会(成果報告)開催場所	開催日	参加企業数（人数）	中小企業数
1	日立システムズ 中国支社 会議室	2020 年 1 月 28 日	22 社 （29 名）	6 社

表 2.13 事業説明会(成果報告)実績

2.1.4.1. 実施内容

説明会では、事業実施状況の成果報告とサイバーセキュリティの普及啓発を行い、意識向上を図るため、セミナー形式での開催として以下の内容にて実施した。

- サプライチェーンを構成する中小企業のサイバーセキュリティ被害動向と事例の紹介。
- 中小企業の支援施策内容の紹介。
  - 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介。
- サイバーセキュリティお助け隊の成果報告。
  - 本実証事業の目的、実施内容とスケジュール、実施体制、成果報告の概要を説明。
  - 本事業の参加企業の状況、中小企業の実態データの分析結果、本事業の実証実績の報告を実施。
- サイバー保険の概要と今後の方向性の説明。

項	時間	報告項目	発表者
1	14:00～14:05	主催挨拶	日立製作所
2	14:05～14:35	「事例から学ぶ中小企業におけるサイバーセキュリティ対策解説」	日立システムズ
3	14:35～15:15	サイバーセキュリティお助け隊の成果報告 ・全体概要 ・実証参加企業 ・実証サービス結果 ・サイバー保険の概要と今後の方向性	日立製作所 日立システムズ 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。）
4	15:15～15:30	中小企業における情報セキュリティ対策支援のご紹介	IPA

表 2.14 事業説明会(成果報告)実施内容

2.1.5. 個別集客活動

重要産業及びそのサプライチェーンを構成する中小企業が多数集積する広島を中心に周南、徳山、防府を含めた地域で事業説明会(事業開始)を当初計画の 3 回から 4 回と増やして実施し、実証参加企業を募集してきたが、目標の参加中小企業数が目標 100 社の 6 割程度であった。

また、実証事業の対象地域について、事業説明会や、ホームページ参照からのお問い合わせ等もあり、事業開始当初計画していた、周南、徳山、防府地区の対象企業に加えて、さらに、これら地域の企業と取引等がある企業にまで対象を広げ、 8 月下旬～12 月末まで事業説明会でのセキュリティ事例、実績などを利用し、セキュリティ意識の向上のための活動とあわせて、個別集客活動を実施することで実証参加の中小企業数の増加を行った。

集客方法としては、日立製作所ホームページでの案内の他 、実証参加いただいている中小企業、および事業説明会で参加いただいた企業で中小企業の子会社をもつ企業に対してアプローチした。また、並行して勧誘中の広島県では、日立製作所グループの中国支社の個別勧誘活動、損害保険ジャパン日本興亜のご紹介による個別勧誘活動を通じてのアプローチを実施した。

日立製作所グループの個別勧誘活動、損害保険ジャパン日本興亜のご紹介による個別勧誘活動を通じ、個別に訪問を行い実証参加の勧誘を実施した。実施内容と実績を以下に記載する。

項	実証参加説明	実施日	参加企業数	実証参加 中小企業数
1	個別訪問(日立製作所内取引先から紹介)	2019 年 9 月 19 日	1 社	1 社
2	個別訪問(日立製作所内取引先から紹介)	2019 年 9 月 20 日	1 社	1 社
3	個別訪問(日立製作所取引先)	2019 年 10 月 8 日	1 社	1 社
4	個別訪問(日立製作所内取引先から紹介)	2019 年 10 月 10 日	2 社	2 社
5	個別訪問	2019 年 10 月 17 日	1 社	1 社
6	個別訪問	2019 年 10 月 23 日	2 社	2 社
7	個別訪問(日立製作所取引先)	2019 年 10 月 24 日	1 社	1 社
8	個別訪問(日立製作所取引先から紹介)	2019 年 11 月 1 日	1 社	1 社
9	個別訪問(日立製作所取引先から紹介)	2019 年 11 月 5 日	2 社	2 社
10	個別訪問(日立製作所取引先から紹介)	2019 年 11 月 11 日	1 社	1 社
11	個別訪問	2019 年 12 月 18 日	1 社	0 社

表 2.15 個別訪問による勧誘活動実績

- お客様事業所での小規模集合で実施するミニセミナーでの勧誘活動

  お客様先で「小規模の集合(5 名程度)で実施したい要望」にこたえ、ミニセミナーを開催した。

  内容と実績を以下に記載する。

項	実施報告項目	適用ミニセミナー
1	講演：サイバー攻撃の最新動向と対策に向けた取組や中小企業に求められる対策 ※中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業の紹介含む	表 2.17 ミニセミナーでの勧誘活動実績 項 1，2，4 にて実施
2	お助け隊事業内容について	全ミニセミナーで実施
3	お助け隊ご提供サービスのご紹介	全ミニセミナーで実施
4	セキュリティ対策の簡易診断	表 2.17 ミニセミナーでの勧誘活動実績 の項 1，2 にて実施
5	お助け隊 今後の計画のご説明	全ミニセミナーで実施

表 2.16 小規模集合で実施するミニセミナー内容

項	**ミニセミナー実証参加説明**	**実施日**	**参加企業数（参加人数）**	**実証参加中小企業数**
1	福山地区Ａ組合ミニセミナー	2019 年 9 月 19 日	5 社（5 名）	5 社
2	Ｂ損害保険尾道支社 ミニセミナー	2019 年 10 月 17 日	5 社（5 名）	1 社
3	広島総合 IT 展覧会セキュリティセミナー	2019 年 11 月 15 日	4 社（4 名）	0 社
4	Ｃ社岩国事業所 ミニセミナー	2019 年 12 月 9 日	7 社（8 名）	2 社

表 2.17 ミニセミナーでの勧誘活動実績

- オンライン会議システム利用による個別説明での個別勧誘活動

  中小企業側のご都合で、事業説明会のような集合説明会に参加いただけない企業のご要望に対応するため、オンラインセミナーと称して、法人向けオンライン商談システムの活用した Q&A 形式での「オンライセミナー」を追加計画し、事業内容概要、提供サービスの説明等を実施した。

  計画と実績を表 2.18 オンラインセミナー計画と実績に記載する。

項	オンラインセミナー実施期間 実証参加説明	実証参加説明実施日	参加企業数	実証参加 中小企業数
1	オンラインセミナー （9 月 11 日～9 月 18 日）	2019 年 9 月 12 日	1 社	1 社
2		2019 年 9 月 17 日	3 社	3 社
3	オンラインセミナー（顧客要望実施）	2019 年 9 月 26 日	1 社	1 社
4	オンラインセミナー （10 月 10 日～10 月 17 日）	該当顧客なし	0 社	0 社
5	オンラインセミナー （10 月 25 日～10 月 31 日）	2019 年 10 月 25 日	3 社	3 社
6	オンラインセミナー （11 月 1 日～11 月 7 日）	2019 年 11 月 5 日	1 社	1 社
7		2019 年 11 月 6 日	1 社	1 社
8		2019 年 11 月 7 日	1 社	1 社

表 2.18 オンラインセミナー計画と実績

2.2. セキュリティよろず相談会

セミナー実施後にセキュリティよろず相談会を設け、参加企業におけるサイバーセキュリティを主とした相談会を行った。

セキュリティよろず相談の実績について以下に記載する。

項	よろず相談会	実施日	参加企業数 （参加人数）	相談社数
1	広島商工会議所　会議室	2019 年 7 月 24 日	29 社	1 社
2	広島商工会議所　会議室	2019 年 7 月 29 日	36 社	3 社
3	福山商工会議所会議室	2019 年 7 月 31 日	11 社	2 社
4	呉商工会議所会議室	2019 年 8 月 1 日	12 社	1 社
5	日立笠戸協同組合	2019 年 8 月 26 日	21 社	2 社
6	福山地区 A 組合ミニセミナー	2019 年 9 月 19 日	5 社	0 社
7	広島総合 IT 展覧会セキュリティセミナー	2019 年 11 月 15 日	4 社	0 社
8	C 社岩国事業所　ミニセミナー	2019 年 12 月 9 日	7 社	2 社

表 2.19 セキュリティよろず相談会実施状況

また、よろず相談会での相談内容（11 件）と対応内容を以下に記載する。

項	相談内容	対応内容
1	「セキュリティの対応は外注業者にて実施している。今気にしている点として、外部との大量のデータ通信時の注意点やセキュリティ対策について相談したい」	・現場セキュリティアセスメントのご提供
2	「IT の構築についてベンダ任せでセキュリティの対応できているかが不安。訪問にてセキュリティ対策の現状を見てほしいので希望する」	・現場セキュリティアセスメントのご提供
3	「新しいウイルス対策ソフト導入検討している。今のセキュリティ対策状況がよいのかぜひ現場セキュリティアセスメントを受けてみたい」	・現場セキュリティアセスメントのご提供
4	「EDR(CYBERREASON)の導入を検討している。Cisco AMP も試してみたい。既存 PC はアンチウィルスソフトが入っているが Cisco AMP 導入において既存アンチウィルスソフトのアンインストールが必要か？」の問い合わせ。	・エンドポイント監視サービスの導入の提案。 エンドポイント監視サービス導入には至らず ・サービス提供利用ツールの機能説明 「既存アンチウィルスソフトとの共存で導入できるようにしてサービス提供している。製品の機能仕様はアンチウィルスも装備している。本実証で提供するサービスはアンチウィルスの機能については、既存のアンチウィルスを変更せずに導入できるように機能の有効化をしない形で提供している。」
5	「セキュリティを盤石にしても従業員の不注意で感染してしまう。迷惑メール訓練の導入を検討しているが効果はあるのか教えてほしい」	・日立製作所の標的型メール訓練の事例をご説明。 「標的型メール訓練の実施による擬似訓練を年 1 回程度で繰り返し実施しています。繰り返し実施することで社員の意識向上により訓練メールの添付ファイルの開封率は下がってきた。メールでのサイバー攻撃の注意が足りない人が特定されてきたので、特定者に個別の教育を行っています。」 ・ｅラーニング教育、教育後アンケートで理解度など情報採取が可能とのアドバイス実施。

6	「セキュリティ対策があまりできていないと感じている、評価もかねてネットワークの監視サービスを導入してみたい」	・インターネット出入り口の監視サービス導入のご提供。
7	「知識のある人が社内にいないのが課題だが、どこからセキュリティ対策を行うのがよいかがわからない」	「守りたいデータ（情報資産）が何なのかを整理し、守りたいデータの利用される環境に対してセキュリティ対策を順次行う。」アドバイスを実施。
8	「使用しているセキュリティソフトの仕様もよくわからない、現場セキュリティアセスメントを受けて問題点があるのかを確認してみたい」	・現場セキュリティアセスメントのご提供。
9	「現在、統合脅威管理装置(UTM)の導入を検討している。比較したいため今回提供サービスの UTM のスペックを教えてほしい」	・機器スペックの提示。 インターネット出入り口の監視サービスで利用している統合脅威管理装置(UTM)の機器スペックを後日メールで送付。
10	「本社はセキュリティ管理されているが、出張所では、PC1 台とモバイルＷｉｆｉルータを利用して直接プロバイダーに接続して利用している。この環境で何を実施すればよいか相談したい。サービス提供を希望するが利用できますか？利用環境を見てほしい」	・利用環境の調査実施 エンドポイント監視は適用可能、インターネット出入り口監視は、事務所内にLAN環境がないため、監視機器が接続不可。 ・エンドポイント監視サービスのご提供。
11	「PC をインターネットで接続しているが、どこまでのセキュリティが導入されているかわからない。現場を見て監視サービスの導入をしてほしい」	・利用環境の調査実施 アンチウィルスのみ実装済み、エンドポイント監視、インターネット出入り口監視の両サービスが可能にて提供。 ・エンドポイント監視サービスのご提供。 ・インターネット出入り口の監視サービス導入のご提供。

表 2.20 よろず相談内容一覧

よろず相談会での相談内容では、セキュリティ強化のため対策機器等の導入を検討している企業は、「他社製品との比較に使いたい」、「セキュリティの対策も併せて外注業者へ一任しているのが、対応範囲が不明」、「どこまでの対策を実施すればよいか」などの内容で、セキュリティ対策を実施するにおいての対策範囲や、優先度がわからないなどの傾向がみられた。

3. 中小企業の実態把握

事業説明会での施策である「セキュリティアセスメント、アンケート、セキュリティよろず相談会」ならびに実証事業の収集データより中小企業のセキュリティ対応サービスの内容、求められる人材スキル内容を整理する。

中小企業の相談窓口となる「セキュリティよろず相談会」を現地で実施し、中小企業の状況・スキル等の実態情報を効率的および効果的に収集する。

セミナー開催時のアンケートの活用、また、現場でのヒアリング等による現場セキュリティアセスメントの実施により、より詳細な現場のセキュリティ実態情報を効果的に収集することで中小企業の意識と現場の実態のギャップを把握する。

また、現場への機器導入等によりセキュリティインシデントの情報収集、およびセキュリティ対策の実装における課題抽出を行い、中小企業の必要とするサイバーセキュリティサービスの検討材料とする。

また、以下の 3 つの支援機能と 4 つのサービスを利用し情報の収集及び支援活動を行った。

3.1. 支援機能とサービス

3.1.1. 支援機能の利用方法

中小企業の実態把握のため以下の 3 つの機能を利用し情報の収集及び支援活動を実施した。

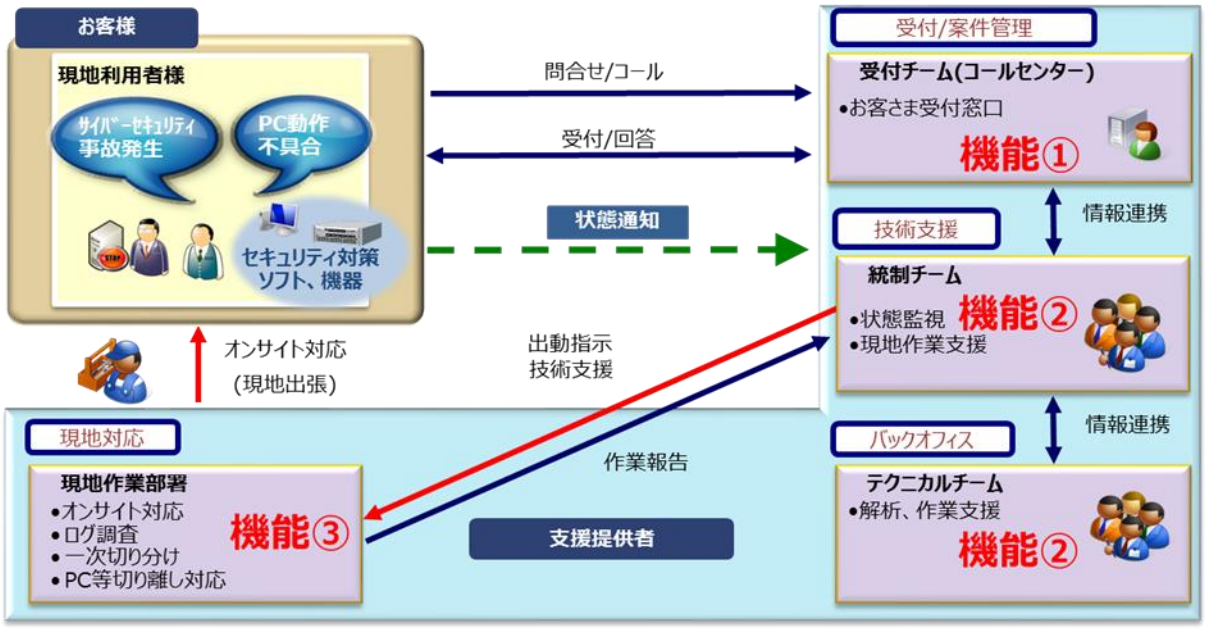


図 3.1 3 つの支援機能の概要

- 受付チームによる中小企業からの相談受付及び対応(機能①)
  - 機器導入時は、機器導入前のネットワーク構成等の相談、導入に必要な環境情報収集のヒアリングシート送付連絡・受付、およびヒアリングシート未提出の企業に対して電話でのフォローコールの実施。
  - サービス提供中は、安定稼働の支援として参加企業への稼働状況の確認。
  - サービス導入の勧誘、およびセミナー情報、サイバーセキュリティ情報の発信。

- 相談内容がサイバーインシデント等であるかの判断（機能②)
  - 受付内容がサイバーインシデントであるかの判断。
  - 機器導入時は入手したヒアリングシートの確認と、ヒアリングシート未提出企業のネットワーク構成図の作成による支援。
  - サービス提供中は、テクニカルチームにて個別チューニングの検討・適用の実施。
  - 監視サービスでのレポート作成、脆弱性情報等の改善提案策定。

- サイバーインシデント等が発生した際の支援の提供(機能③)
  - セミナー実施後のサービス導入の勧誘及び、実証参加企業からの要望による現地訪問での個別説明。
  - 機器導入前のネットワーク構成等を現地にて確認支援。

3.1.2. 4 つのサービスでの情報収集

中小企業の現場の状況、情報インフラ等の環境に応じて対応するため、2 種類のアセスメントサービス、および 2 種類のセキュリティ監視サービスを準備し、本実証サービスで活用した。

(1) セキュリティ対策の簡易アセスメント
  - サービス名称：セキュリティ簡易アセスメント

(2) 現場セキュリティアセスメント
  - サービス名称：現場セキュリティアセスメント

(3) ネットワークに関するセキュリティ監視(UTM 等を活用)
  - サービス名称：インターネット出入り口の監視サービス

(4) エンドポイントに関するセキュリティ監視(PC 等の端末の監視)
  - サービス名称：エンドポイント監視サービス

● 情報収集と実証サービスの考え方・選定理由

【情報収集目的：中小企業のセキュリティ意識と実装状態の把握】

- 中小企業のセキュリティ意識と実装状態の概要を把握
- セキュリティ対策の可視化による意識付けを図る

→ (1) セキュリティ対策の簡易アセスメント 診断結果フィードバック

- 具体的なセキュリティ対策の実装状態の把握
- セキュリティ対策の認識度向上への貢献
- 具体的なセキュリティ対策内容の意識付けを図る

→ (2) 現場セキュリティアセスメントの実施

【情報収集目的 1：セキュリティ対策の実装における課題の抽出】

【情報収集目的 2：中小企業で発生しているインシデントの把握】

- 脅威の侵入を防ぐ（入口対策）/被害を食い止める（出口対策）の状況

→ (3) ネットワークに関するセキュリティ監視（UTM 活用）サービスの提供

- 情報に拡散を防ぐ（内部対策）の状況

→ (4) エンドポイントに関するセキュリティ監視(EDR 活用)サービスの提供

3.1.3. 情報収集の計画

4 つのサービスを利用した実態把握の情報収集の計画を図 3.2 中小企業の実態把握データ収集計画内容に記載する。

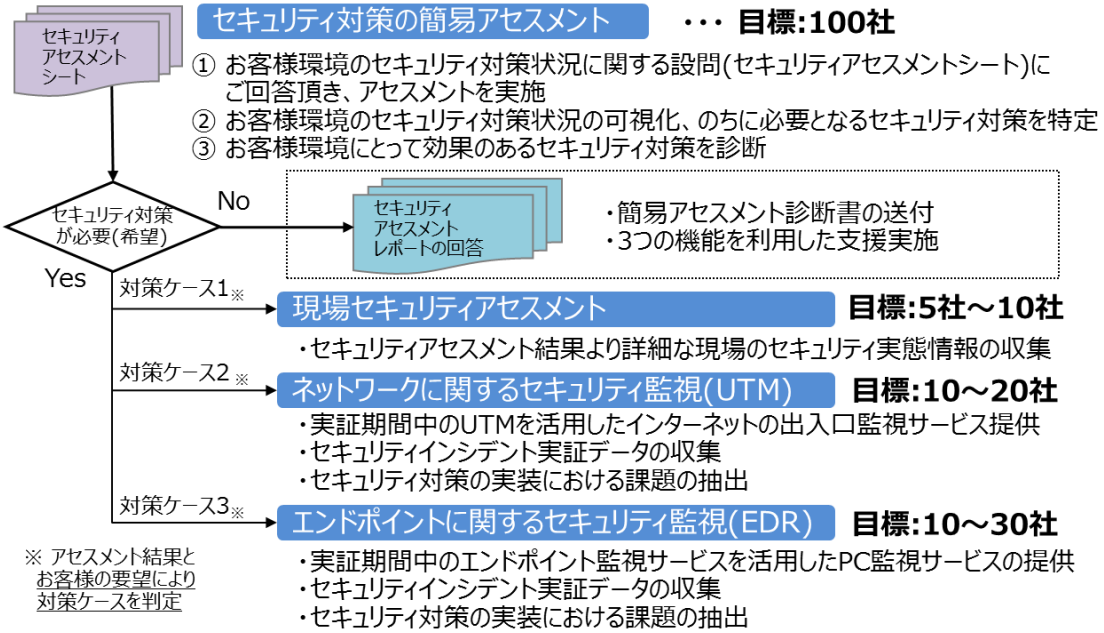


図 3.2 中小企業の実態把握データ収集計画内容

3.2. 情報収集の実績

中小企業に 4 つのサービスのいずれか、もしくは複数のサービスを合計 110 社に提供した。サービス毎導入数についても目標内の企業数を確保しさらに、全 110 社に対して、3 つの機能を活用した支援を実施した。また、主な支援内容についての実績を記載する。（実施内容の詳細は、5．地域実証の実施　にて記載する。）

以下に 4 つのサービスを提供した企業数と複数サービス提供の組み合わせの内訳を記載する。

項	サービス	サービス毎導入数	サービス略名	複数サービス提供内訳											
				4つ全部	簡易・現場・EDR	簡易・UTM・EDR	簡易・現場	簡易・UTM	簡易・EDR	現場・UTM・EDR	UTM・EDR	簡易のみ	現場のみ	UTMのみ	EDRのみ
1	セキュリティ対策の簡易アセスメント	107社	簡易	○	○	○	○	○	○			○			
2	現場セキュリティアセスメント	9社	現場	○	○		○			○			○		
3	ネットワークに関するセキュリティ監視	10社	UTM	○		○		○		○	○			○	
4	エンドポイントに関するセキュリティ監視	13社	EDR	○	○	○			○	○	○				○
合計			**110社**	1社	1社	4社	6社	3社	4社	1社	1社	88社	0社	0社	1社

図 3.3 サービス提供企業数と複数サービス提供内訳

項	内容	件数	サイバー駆けつけ支援	備考
1	セキュリティよろず相談会での相談	11 社	―	セミナー、ミニセミナー後実施
2	ネットワークに関するセキュリティ監視でのインシデント検知	48,061 件	なし	脆弱性通信検知多数企業で改善提案を実施
3	エンドポイントに関するセキュリティ監視でのインシデント検知	2 件	なし	アドウェアの検知
4	現地ネットワーク環境調査支援	3 社	―	UTM 導入 3 社実施
5	サイバーセキュリティセミナー、マルウェア情報等の情報提供支援	4 回	―	**110 社**へメール送付・電話による連絡

表 3.1 主な支援内容の実績

3.3. セキュリティ情報収集システム設計 / 構築

セキュリティ情報を収集するための 2 つの監視サービスで提供する機能概要を記載する。

3.3.1. インターネット出入り口の監視サービス概要

実証参加企業ネットワーク上に統合脅威管理装置(UTM)を設置し、インターネット経由でインシデントのリモート監視を行った。

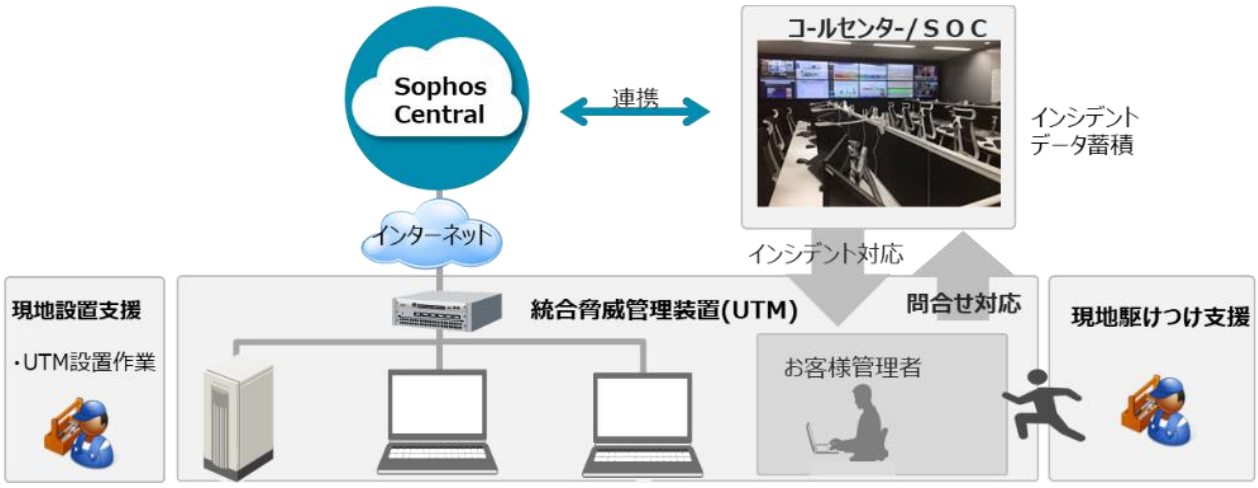


図 3.4 インターネット出入り口の監視サービス概要

3.3.1.1. 機能仕様

インターネット出入り口の監視サービスの機能仕様を記載する。

- 統合脅威管理装置(UTM)で提供する機能

No	機能	概要
1	IPS（侵入防止システム）	外部からの不正な攻撃を検知、トラフィックを遮断することで不正アクセスを防御する機能。
2	C&C／ボットネット防止	外部の攻撃サーバ（C&C サーバ）宛に内部から送信されるトラフィックをブロックする機能。
3	サンドボックス	外部からのダウンロードしたファイルを保護された領域で確認し、システムが不正に操作されないようにする機能。
4	Web スキャン	Web サーバに対するアップロード／ダウンロードファイルをスキャンする機能。 HTTPS 通信への適用時は CA 証明書が必要

表 3.2 統合脅威管理装置(UTM)で提供する機能

- 中小企業のネットワーク構成変更を極力発生させないように、統合脅威管理装置(UTM)を L2 モード(ブリッジモード)にて導入する。
- インシデント発生時の通信をブロックするモードとしないモードを準備することで中小企業の現場の状況、情報インフラ等の環境に応じて対応する。

- 設置準備について
  - 機器の設置時において中小企業の業務への影響を最小限にするために、設置する機器に事前に日立製作所にて必要なパラメータ等を設定して中小企業へ機器を配布する。
  - 現地への機器設置は日立製作所の作業員を派遣し、機器の設置を支援する。

- アラート監視
  - 実証参加企業ネットワーク上に統合脅威管理装置(UTM)を設置し、インターネット経由でインシデントのリモート監視を実施する。
  - 統合脅威管理装置(UTM)から送信される検知アラート監視について、日立製作所技術者が検知内容を確認し、検知内容の解説と実証参加企業での対応の必要性などをメールでご連絡する。

- イベント分析
  - 統合脅威管理装置(UTM)の脅威検知イベントについて日立製作所技術者が検知状況を分析し、感染端末の感染経路や、被害状況を確認し、対応方法について適切なアドバイスをメール・電話等で提供する。
  - 月次レポートを提供し、中小企業のサイバーインシデント状況を可視化する。

- サイバーインシデント対応
  - サイバーインシデント発生時は、必要に応じ現地へ駆けつけ支援し、一次切り分け／PC 機器等の切り離しを実施する。

3.3.2. エンドポイント監視サービス概要

監視対象 PC へエンドポイント監視用ソフトウェア（EDR エージェント）をインストールし、インターネット経由でインシデントのリモート監視を行った。

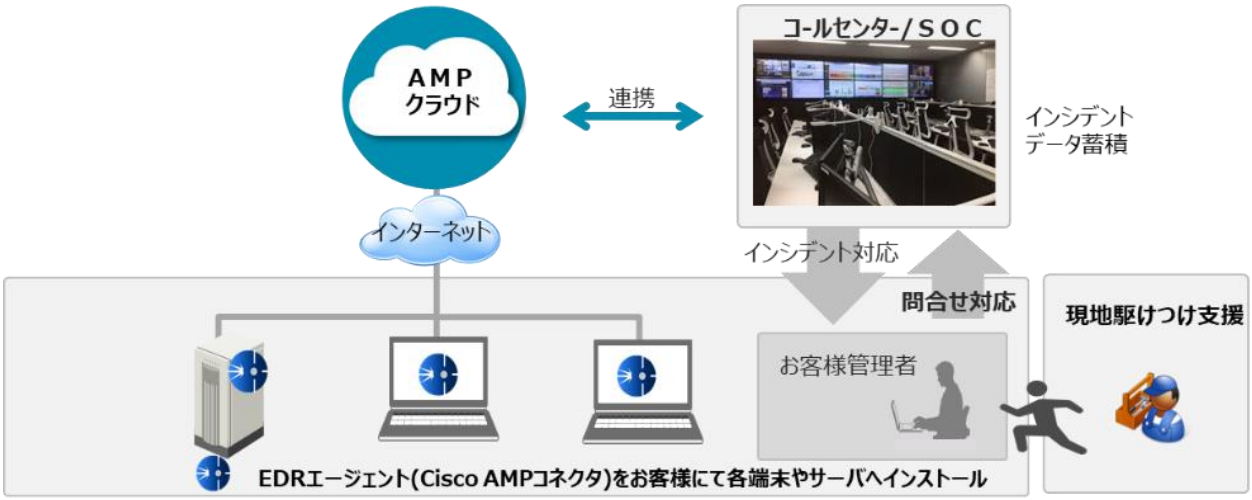


図 3.5 エンドポイント監視サービス概要

3.3.2.1. 機能仕様

エンドポイント監視サービスの機能仕様を記載する。

- エンドポイント監視サービスで利用するソフトウェアで提供する機能

No	機能	概要
1	事前対策機能	エンドポイント監視用ソフトウェア（製品名 Cisco AMP）がインストールされている端末の一元管理および脆弱なソフトウェアがある端末のチェックを行う機能。
2	マルウェア検知・防御機能	パターンファイルやハッシュ値照合による既知のマルウェアの検知・防御や、振る舞いや機械学習、マルウェアが発生させる不正通信、およびサンドボックス解析などを行うことによる未知のマルウェアの検知・防御を行う機能。
3	事後対応機能	モニタリングにより蓄積したログをクラウドにて分析を行い、マルウェアの侵入経路、感染原因および感染範囲を特定する機能。

表 3.3 エンドポイント監視サービスで利用するソフトウェアで提供する機能

- インシデント発生時の通信ブロックを実施しない検知のみモードを提供することで中小企業の PC 動作に影響を与えないようにする。
- 導入に際して対象 PC の既存ソフトウェアの変更無いようにエンドポイント監視用ソフトウェア（製品名 Cisco AMP）の持つアンチウィルス機能を利用しない設定にて導入する。

- 導入方法について
  - 各サービス提供企業の導入する PC 環境情報より、パラメータ設定済みのエージェントを作成後、ダウンロード専用サイトへ登録後、メールにて中小企業に通知する。
  - 中小企業にてダウンロード専用サイトよりパラメータ設定済みのエージェントソフトウェアをダウンロードし当該 PC へインストールする。

- アラート監視
  - 監視対象 PC へエンドポイント監視用ソフトウェアをインストールし、インターネット経由でインシデントのリモート監視を実施する。
  - エンドポイント監視用ソフトウェアから送信される検知アラートについて、日立製作所技術者が検知内容を確認し、検知内容の解説とお客様での対応の必要性などをメール等でご連絡する。

- イベント分析
  - エンドポイント監視用ソフトウェアの脅威検知イベントについて、日立製作所技術者が検知状況を分析し、感染端末の感染経路や、被害状況を確認し、対応方法について適切なアドバイスをご提供する。

- サイバーインシデント対応
  - サイバーインシデント発生時は、必要に応じ現地へ駆けつけ支援し、一次切り分け／PC 機器等の切り離しを実施する。

3.4. セキュリティ機器配布 / 設置(端末)

２つの監視サービスを提供するにあたって 8 月の展開を計画していたが下記理由によりスケジュールの変更を行い機器の配布／設置を 12 月まで延長して実施した。

また、事業説明会などのアンケートで機器導入を希望しなかった 28 社、および既にサービス提供を実施している中小企業に対して、改めて「インターネット出入り口の監視サービス」、および「エンドポイント監視サービス」の再勧誘を実施した。

メールでの連絡のみでは回答がないことが多く、実施においてはメールでのご連絡とあわせて電話でのフォローを複数回（3 回/週程度までのコール）実施し、ご担当者へ直接アプローチする方式で実施した。これにより、3 社に「インターネット出入り口の監視サービス」、および「エンドポイント監視サービス」を導入した。

あわせて、中小企業におけるネットワーク機器の導入は、ネットワーク環境を把握していないケースが多く、ネットワークエンジニア等の現地派遣による調査、ネットワーク情報のパケットキャプチャリング等によるネットワーク構成把握が必要となり、機器導入前の事前調査を実施した。

以下に遅延の要因を記載する。

- スケジュール遅延による要因
  - 事業説明会(事業開始)の開始が遅れたことにより実証参加企業の確保が遅れた。
    - 改善策：事業説明会の回数を増やし実証参加企業の確保を実施した。

- 世間の情勢による要因
  - 9 月末まで、消費税変更による駆け込み納期対応のため、中小企業の担当者が本業にて忙殺され、サービス導入の検討及び意思決定に時間が割けない状況となり計画通りの進捗とならなかった。また、多忙のため機器導入に関わる作業時間の捻出ができないため機器導入に伴うサービスは辞退するとの回答、および 10 月以降での対応希望の回答が多数発生した。
    - 改善策：10 月末までを目途に、サービス導入の検討状況の確認をメール、および電話で個別にフォローを実施した。10 月中旬より中小企業の担当者と連絡がつきやすくなり改善傾向となり、導入検討を再度案内し、実証参加企業の確保に向けてフォローを実施した。
  - Windows 7 のサポート切れに伴う PC 等の変更前のためエンドポイント監視サービスの導入も見合わせたいとの回答もあった。

- 導入環境による要因
  - 統合脅威管理装置(UTM)導入については、ネットワークの構成把握が必須となるが、中小企業の担当者ではネットワーク構成を把握されていないケースが多く、統合脅威管理装置(UTM)の導入までにネットワーク構成の確認のための連絡が長くかかり導入まで時間を要した。特に従業員数が 100 名未

満の企業ではネットワーク構成図がないまたは、外注者へ社内 IT 管理を一任している事があり確認までに時間を要した。

また、お客様の他拠点との VPN ネットワークを利用しているケースも多く、他拠点のネットワーク構成の把握が必要なケースもあった。（統合脅威管理装置(UTM)導入 10 社中 4 社実施）

・ 改善策：ネットワーク構成はヒアリング情報に基に、統合脅威管理装置(UTM)導入構成案を作成し提案型とした。これにより、情報のやり取り回数が減り、導入まで時間短縮を図った。

▸ お客様にてネットワーク構成がわからない、知識がなくわからないケースもあり、現地へ伺ってネットワーク環境調査を行わないと導入ができなかった。

・ 改善策：現地へ伺ってネットワーク環境調査を実施。
（統合脅威管理装置(UTM)導入 10 社中 3 社実施）

● お客様状況による要因

▸ ミニセミナー実施で従業員数 10 名以下の企業では、「PC でのメールを連絡手段として使用しないことが多く、電話および FAX が連絡方法の主体」とのご意見があった。

導入検討中のフォローについて、メールでの連絡後に、電話でのアプローチを実施するが、担当者の不在、取次も伝わっていないケースが多く連絡がスムーズにとれなかった。

また、短期間に何度もフォローすると、強制的な印象を与える場合もあり、反感を買い逆効果になることもあったため、不快にならない範囲でのフォローを実施した。

・ 改善策：3 回/週程度までの電話コールによる繰り返しのフォローを実施。

3.4.1. 対応支援に必要な情報収集

本事業で対応支援を行う上で必要な情報と入手方法を記載する。

- 監視体制で必要となる情報
  - サービス利用申込書にて入手する情報
    - サイバーインシデント発生時の連絡先（会社名、ご担当者名、電話番号、メールアドレス）
- 駆けつけ支援、機器据付時に必要な情報
  - サービス利用申込書にて入手する情報
    - お客様基本情報（会社名、機器設置先住所、ご担当者名、電話番号、メールアドレス）
- 現場セキュリティアセスメント利用時
  - サービス利用申込書にて入手する情報
    - お客様基本情報（会社名、機器設置先住所、ご担当者名、電話番号、メールアドレス）
  - アセスメント時に現地で確認する情報
    - システム構成や運用状況を確認するため、ネットワーク構成図、システム構成図、業務フロー図、運用体制図、運用フロー図、運用手順書のドキュメント
    - 組織のセキュリティポリシやルールを確認するため、セキュリティポリシ、セキュリティスタンダード、セキュリティガイドラインのドキュメント
- インターネット出入り口の監視サービス利用時
  - サービス利用申込書にて入手する情報
    - お客様基本情報（会社名、機器設置先住所、ご担当者名、電話番号、メールアドレス）
    - サイバーインシデント発生時の連絡先（会社名、ご担当者名、電話番号、メールアドレス）
  - ヒアリングシートにて入手する情報
    - 統合脅威管理装置(UTM)へ付与する IP アドレス
    - ネットワーク構成図
    - ＦＷの設定情報、Web アプリ情報、DNS 情報、Proxy 利用情報
- エンドポイント監視サービス
  - サービス利用申込書にて入手する情報
    - お客様基本情報（会社名、機器設置先住所、ご担当者名、電話番号、メールアドレス）
    - サービス利用申込者サイバーインシデント発生時の連絡先
      （会社名、ご担当者名、電話番号、メールアドレス）
  - ヒアリングシートにて入手する情報
    - エンドポイントデバイス(PC 等の)OS 情報、Proxy 利用情報
    - 特殊な業務プログラムのインストール情報（プログラム名、インストールパス情報）

3.5. 実証参加企業の分析

実証参加の中小企業の内訳は、業種では製造業が約 7 割、従業員数は 100 人以下が 7 割、資本金 3000 万円以下が約 7 割であった。

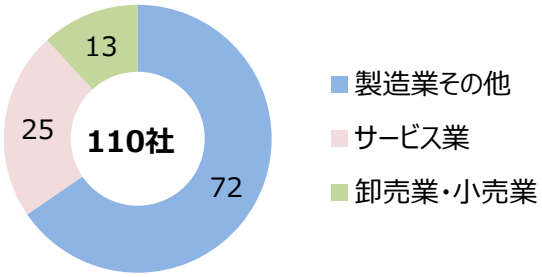


図 3.6 参加企業の業種内訳

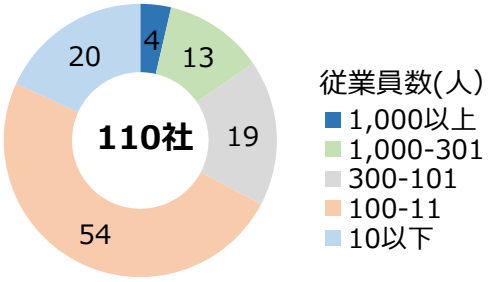


図 3.7 参加企業の従業員数内訳

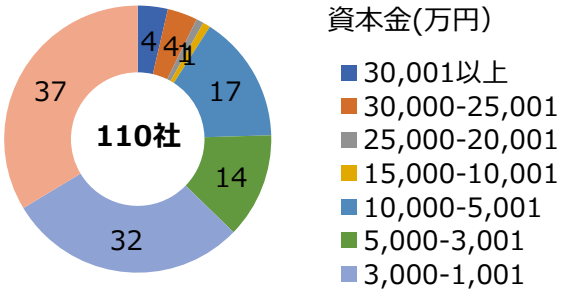


図 3.8 参加企業の資本金内訳

- 実証参加中小企業へのアンケート状況（回答数：106 社）

  セミナー実施時にアンケートを行い、中小企業の調査を行った。

  サイバーセキュリティ対策の実施状況についての意識調査では、対策が「不十分だができている」、「不十分」の合計で 56%(59 社)であり、サイバーセキュリティへの備えに不安が多数あることが伺える。

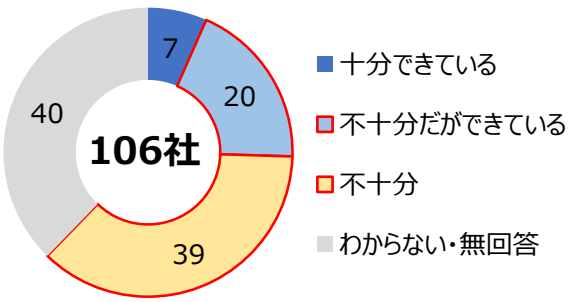


図 3.9 セキュリティ対策認識度

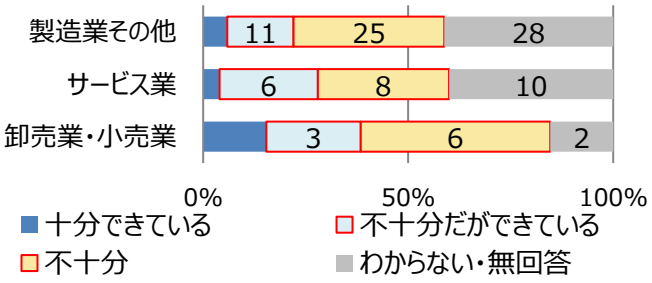


図 3.10 セキュリティ対策認識度（業種別）

また、よろず相談会での相談内容では、セキュリティ対策機器等の導入を検討している企業は、「他社製品との比較に使いたい」、「セキュリティ対策も併せて外注業者へ一任している」、「対応範囲が不明、どこまでの対策を実施すればよいかわからない」などの内容で、セキュリティ対策を実施する場合の対策範囲や、優先度がわからないなどの傾向がみられた。

項	相談内容	該当数	対応内容
1	「セキュリティはどこに、いくらかければいいのかわからない」	3 社	・中間報告にてサイバーリスクの金額換算を参考紹介。 ・守りたいデータの優先度を決め対応のアドバイスを実施。 ・利用環境調査
2	「他社製品との評価のために本サービスを利用したい」	1 社	・監視サービスの提供。
3	「セキュリティ対策をどこまで実施してよいかわからないのでセキュリティアセスメントを希望したい」	2 社	・現場セキュリティアセスメントの提供。
4	「セキュリティ対策は外注業者へ一任しており心配しているため、現地セキュリティアセスメントを希望したい」	2 社	・現場セキュリティアセスメントの提供。
5	「セキュリティ対策導入計画中で機能面の比較をしたいスペックを教えてほしい」	2 社	・機器スペックの提示。
6	「セキュリティを盤石にしても従業員の不注意で感染してしまう教育が難しい」	1 社	・標的型訓練サービス、ｅラーニング教育等のアドバイス実施。

表 3.4 よろず相談会での相談内容

アンケート調査よりサプライチェーンでのセキュリティ強化のため取引先からの調査、対策実施依頼があったかの問いに、「対応依頼があった」の回答は 15%（16 社/106 社）、また、対応依頼のあった企業でセキュリティ対策要員がいるかの問いには、56%（9社/16社）が「社員での対応が可能」と回答をしている。また、「外注に依頼している」回答は 19%（3 社/16 社）対応要員がいる合計は 75%（12 社/16 社）であった。

また、106 社全体でのセキュリティ対策要員の有無は、「社員での対応が可能」+「外注に依頼している」を合わせて 36%（22 社+16 社/106 社）、セキュリティ対応要員が「いない」との回答は全体の 25%（27 社/106 社）であった。これにより、取引先からの調査、対策依頼がある場合、セキュリティの対応要員を配置しているのが全体平均36%と比べて75%と高いといえる。また、サプライチェーンの弱点を悪用した攻撃への備えとして、企業は自社のみならず、ビジネスパートナーを含めたサプライチェーン全体での対策が求められていることから、取引先からの要請といった動きは今後さらに顕著になってくることが予想され、対応要員の確保が課題になると考える。

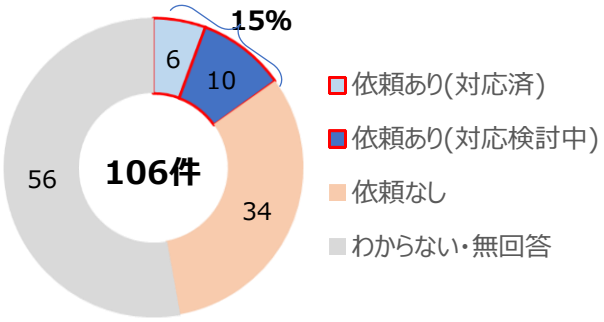


図 3.11 取引先からのセキュリティ対策の調査依頼・改善依頼

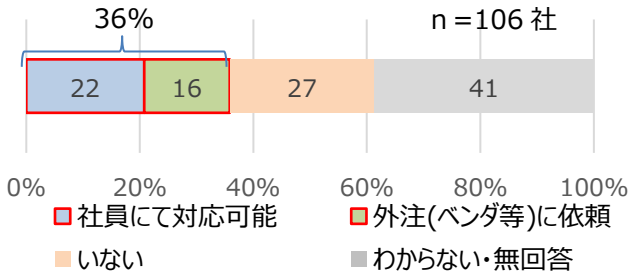


図 3.12 セキュリティ対応要員の要否（全体）

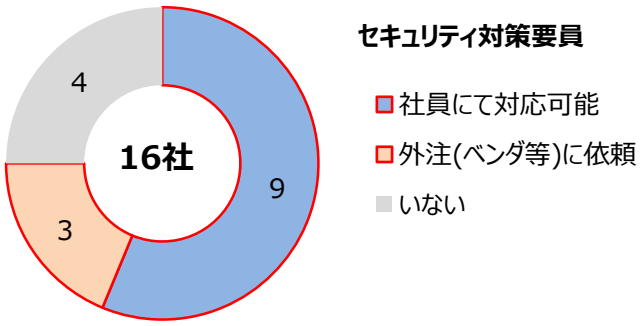


図 3.13 対策依頼あり時のセキュリティ対応要員の要否

参加中小企業のアンケートでの業務利用調査にて、従業員数が少数の企業においても業務でインターネットを利用した受発注、販売、宣伝等の Web 系サービスの利用（図 3.14 参加中小企業の業務内容 参照）、および業務サーバの設置場所の 25%（図 3.15 業務サーバの設置場所 参照）がクラウド利用でありインターネット越しの外部通信によるセキュリティ脅威が考えられる。また。タブレット・スマートフォンの業務利用（図 3.14 参加中小企業の業務内容 参照）もあり、無線 LAN の利用による盗聴などの脅威も考えられる。

現場でのセキュリティ機器導入時のネットワーク調査は、ルータ等のアカウントが初期設定のままになっているケースも多く、外部からの侵入ルートとして無線 LAN を利用したサイバー攻撃のリスクを含んでいると考えられる。

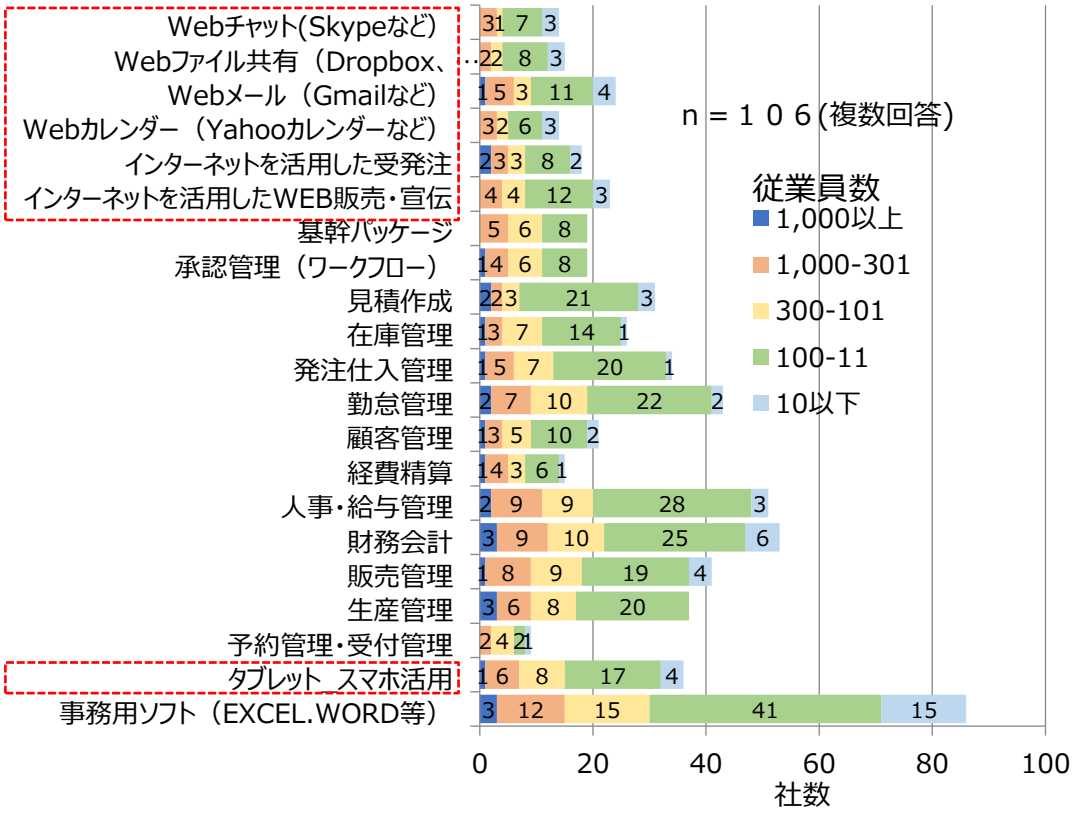


図 3.14 参加中小企業の業務内容

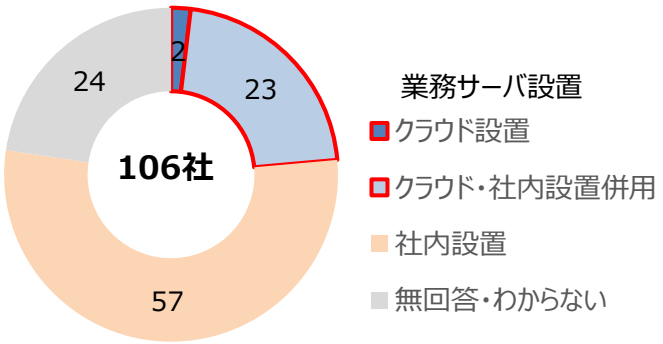


図 3.15 業務サーバの設置場所

参加中小企業のアンケートでのサイバーセキュリティ対応時に利用したいサービスの調査では、「インシデント発生時のマルウェア等の除去、装置の回復の支援」が 41 社と他のサービスより多く、意識醸成ならびに態勢整備が進んでおらず有事対応に不安が大きい中小企業においては、相談窓口等の平時対応に関するサービスよりも、緊急時の対応へのニーズが高いことがわかる。

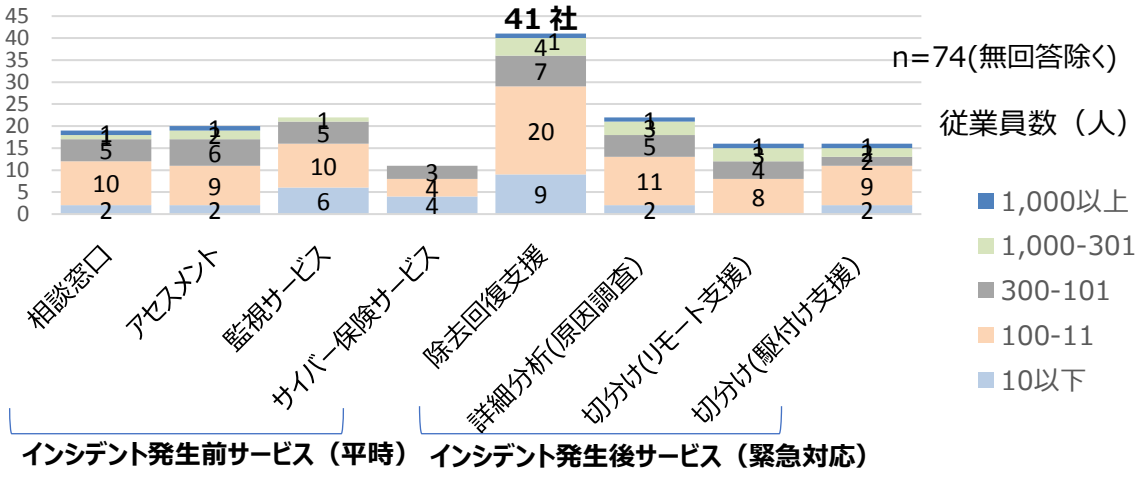


図 3.16 サイバーセキュリティ関連の利用したいサービス

- SECURITY ACTION セキュリティ対策自己宣言

事業説明会(事業開始)及び、ミニセミナーの「お助け隊事業内容について」の中で、SECURITY ACTION 及び中小企業の情報セキュリティ対策ガイドラインの普及に向けた周知啓発活動への協力を行った。具体的には、SECURITY ACTION セキュリティ対策自己宣言書の、「★一つ星」中小企業の情報セキュリティ対策ガイドライン付録の「情報セキュリティ 5 か条」に取組むことを宣言及び、「★★二つ星」中小企業の情報セキュリティ対策ガイドライン付録の「5 分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針（理念、指針、原則、目標等を表した「方針書」「宣言書」等）を定め、外部に公開したことを宣言、また、中小企業の IT 導入補助金の申請要件となった点を説明した。

事業説明会の実施アンケートでの情報収集にて 106 社中「★一つ星」及び、「★★二つ星」の自己宣言済は 9 社、これから「★一つ星」、および「★★二つ星」の自己宣言を実施予定との回答を得た企業が 44 社もあり、取引先からのセキュリティ対策要請増加の動きを受け、今後企業における取り組みが進んでいくものと思われる。

	宣言実施済 中小企業	宣言実施予定 （推進中）	合計
★　一つ星	5 社	37 社	42 社
★★　二つ星	4 社	7 社	11 社
計	9 社	44 社	53 社

（2020 年 1 月 31 日時点集計）

表 3.5 SECURITY ACTION セキュリティ対策自己宣言書の推進

- 「セキュリティ対策の簡易診断」の分析
  - 基本情報
    - 分析対象回答数：107 件

    分析対象は中小企業の定義に該当する企業の回答のみを対象とした。

    同一企業で複数名から回答が得られた場合は、以下のルールによって回答を選別した。

    回答者アンケートによる担当業務の回答が「情報管理システム」のものを選別した。

    回答者のセキュリティ対策へのかかわりに関する回答が「対策を導入」、「運用を実施」、「施策を承認」、「施策を企画」（記載は優先順）を選別した。

    上記の選別の結果、複数の回答が候補となった場合は対象となる回答のワーストケース（ただし、無回答・無効回答を除く）を採用した。
  - アセスメント実施内容
    - 調査方法
  - 調査対象者
    - 実証参加企業
  - 調査手法
    - 会場調査（セミナー形式）
    - データによる郵送調査
    - 訪問留置調査
  - 回答取得方法
    - セルフアセスメント方式

      ただし、会場調査では説明員による設問の説明を実施している。郵送調査および訪問留置調査では要求により設問の説明を実施している。
  - 回答方法
    - 多項選択回答形式

- 設問内容

以下の 18 問について回答者にアンケート形式で実施した。

No.	設問内容
No.01	インターネットとの接続箇所において、インターネットから自組織内への通信を、必要な通信に限定していますか。
No.02	インターネットとの接続箇所において、サイバー攻撃を検知または防御していますか。
No.03	組織外から受信する電子メールに対して、パターンマッチ型のウィルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウィルスチェックは含みません。
No.04	インターネット（ウェブ）からダウンロードするファイルに対して、パターンマッチ型のウィルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウィルスチェックは含みません。
No.05	組織外から受信する電子メールに対して、サンドボックスなどのパターンに依存しないウィルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウィルスチェックは含みません。
No.06	インターネット（ウェブ）からダウンロードするファイルに対して、サンドボックスなどのパターンに依存しないウィルス・マルウェア対策を実施していますか。なお、この対策にはパソコン上で実施するウィルスチェックは含みません。
No.07	パソコンにパターンファイルを常に最新に更新しているパターンマッチ型のアンチウィルス・マルウェアソフトウェアを導入し、ウィルス・マルウェア対策を実施していますか。
No.08	パソコンにふるまい検知型などのパターンに依存しないアンチウィルス・マルウェアソフトウェアを導入し、ウィルス・マルウェア対策を実施していますか。
No.09	パソコンのオペレーティングシステムに対するセキュリティパッチを適用していますか。
No.10	組織内部のネットワーク上で、不正な通信が行われていないか監視を行っていますか。
No.11	組織内のサーバ（ファイルサーバなど）のアクセスログや認証ログを保管し、分析していますか。
No.12	組織内からインターネット（ウェブ）へのアクセスにウェブプロキシサーバを経由する構成としていますか。
No.13	インターネット（ウェブ）へのアクセスにおいて、業務上不要なサイトや悪意のあるサイト（マルウェアを配布しているサイトなど）へのアクセスを制限していますか。
No.14	インターネット（ウェブ）へのアクセスにおいて、攻撃者が準備しているサーバ（C&C サーバなどマルウェアの接続先のサイトなど）へのアクセスを制限していますか。
No.15	重要な情報が保管されているサーバやパソコンのデータバックアップを取得していますか。
No.16	サーバやパソコン上のプログラムの実行記録や通信の実施記録を取得し、保管していますか。
No.17	サイバーセキュリティ事故（インシデント）が発生した場合の対応手順・対応体制を定めていますか。
No.18	標的型攻撃に関する教育や情報提供を実施していますか。

表 3.6 セキュリティ対策の簡易アセスメント設問内容

- 回答選択肢

回答	回答基準
導入済	実施・導入している
一部導入	一部実施・導入している
検討中	実施・導入を検討している
コスト面で不要	実施・導入を検討している（した）が、主にコスト面で導入していない
機能面で不要	実施・導入を検討している（した）が、主に機能面で不要と判断し導入していない
未検討	実施・導入の検討をしていない（したことがない）。設問に記載された対策を知らない

表 3.7 セキュリティ対策の簡易アセスメント 回答選択肢

無回答、選択肢以外の回答等については「無効回答」としている

各設問は下記のカテゴリに分類し分析を行う。ネットワークとカテゴリの関係を図 3.18 ネットワーク構成とカテゴリの関係に記載する。

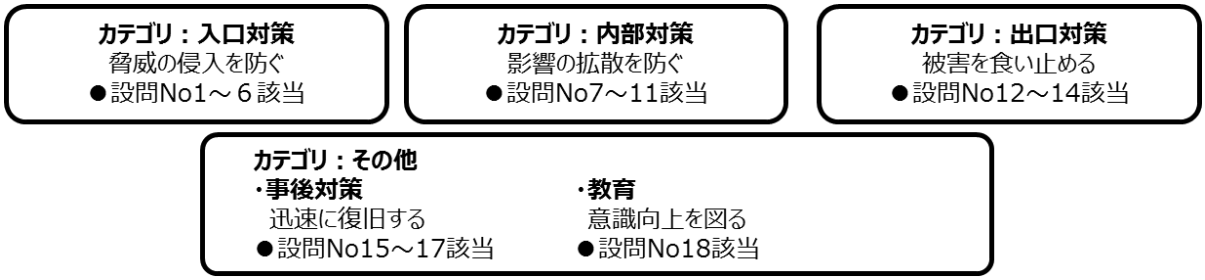


図 3.17 設問内容分類

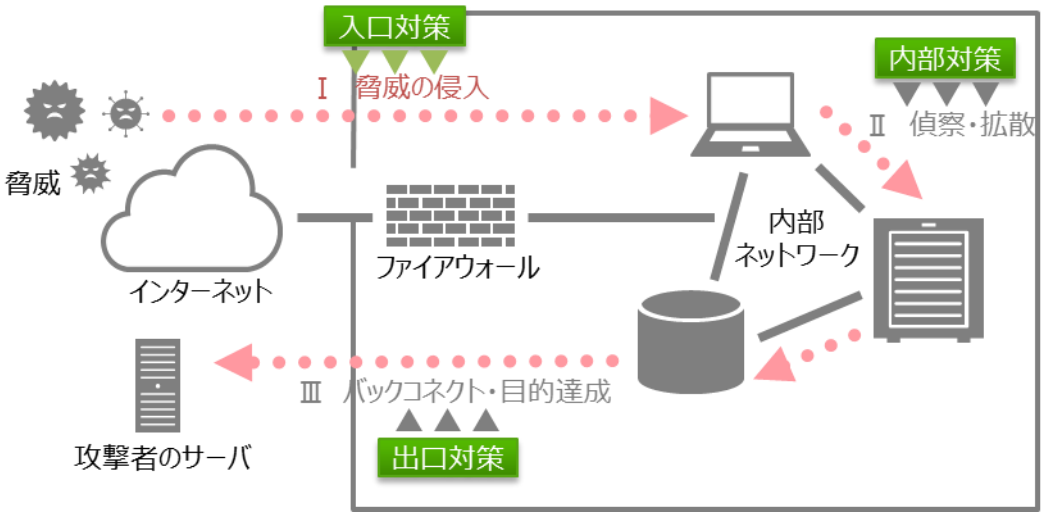


図 3.18 ネットワーク構成とカテゴリの関係

3.5.1. 分析概況

- 「セキュリティ対策の簡易アセスメント」の分析サマリ
  - データのバックアップ（No.15）は 88%にて実施済み。本アセスメント対象項目のうちもっと高い実施率[1]であった（3.5.2.4 その他（インシデント対策、教育）参照）。

    現地セキュリティアセスメントでの調査ではバックアップは行っているが、サーバ（ファイルサーバ含む）のバックアップ取得はできているが PC 内のデータまでバックアップされていない企業が複数で確認された。

    また、バックアップの世代管理が行われていない企業が多数であった。インシデント発生時の復旧が迅速に行えないリスクがあると考える。
  - エンドポイントセキュリティにおけるパターンマッチ型アンチウィルス（No.07）の導入状況とセキュリティパッチの適用（No.09）状況の実施率が 80%前後と他のサンプルより高い（3.5.2.2 内部対策 参照）。

    現地セキュリティアセスメントでの調査ではアンチウィルスの導入はされているが、インストールされているアンチウィルスの機能について知らない企業が多数であった。インシデント発生時の原因調査が迅速に行えないリスクがあると考える。
  - セキュリティ対策のうち、入口対策におけるパターンに依存しないメール向けのアンチウィルス（No.05）と入口対策におけるパターンに依存しないウェブ向けのアンチウィルス（No.06）、エンドポイントにおけるパターンに依存しないアンチウィルス（No.08）、不正な通信の監視（No.10）、ログの分析（No.11）、プロキシ（No.12）、攻撃者のサーバへのアクセス制御（No.14）については導入率が 30%を下回っている状況（図 3.19 セキュリティ対策実施状況 参照)。

    パターンに依存しないアンチウィルスなどの新しいウイルスの検知防御に対応できていない、また情報の流出を防止する（出口対策）の実装率が低いためマルウェアの感染後の情報流出のリスクは高いと考える。
  - セキュリティ対策を実施していない理由では、該当のセキュリティ対策について検討をしていないもしくは対策自体を知らないとの回答が最も多い。

    セキュリティ対策の内容やその対策の必要性に係る認知度が低いことが要因として考えられる。現場セキュリティアセスメントによる訪問先においても、「どのような対策を行えばよいのかわからない」との声が聞かれている。（3.5.3 セキュリティ対策別未実施理由 参照）業種別のセキュリティ対策状況では、情報通信業においてインシデント対応（No.17）の実施状況が高い（3.5.4 業種別セキュリティ対策実施状況 参照）。
  - 組織規模別のセキュリティ対策状況では、従業員数 10 名以下の組織において対策状況が低い（3.5.5 組織規模別セキュリティ対策実施状況 参照）。

[1] ここでの実施率は、「実施済」と「一部実施」との回答の割合を指す。

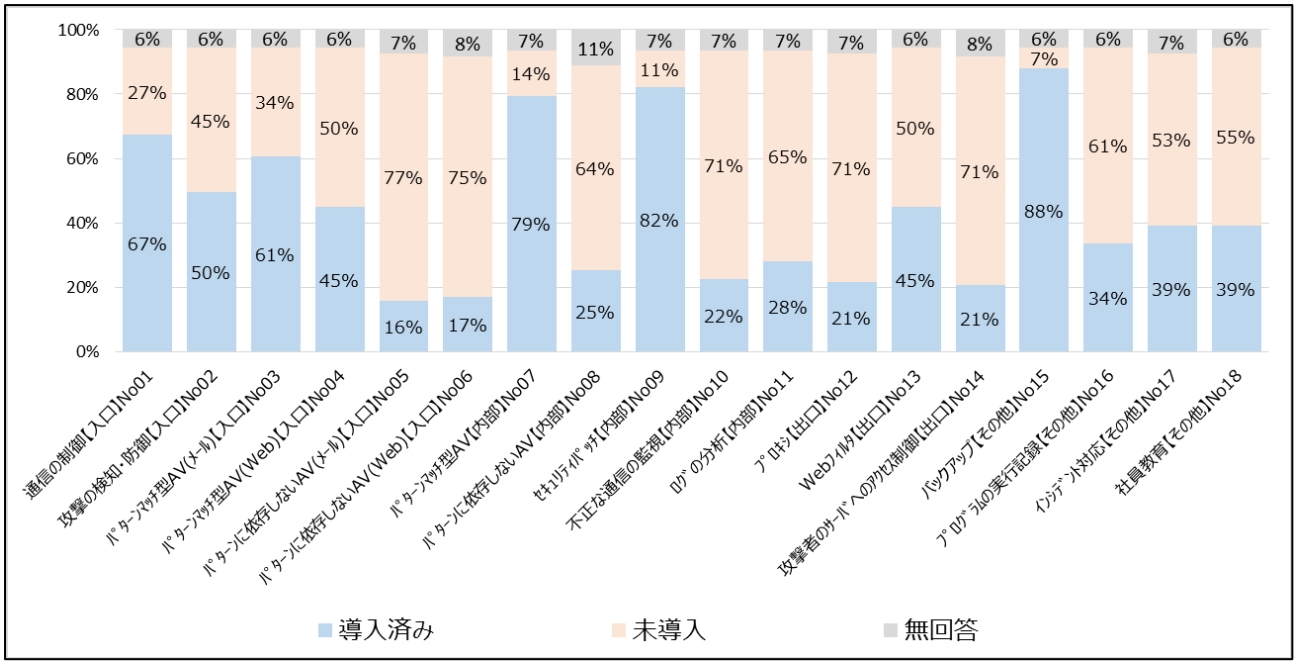


図 3.19 セキュリティ対策実施状況

（単位：社）

n=107	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
無効回答	6	6	6	6	8	9	7	12	7
未導入	29	48	36	53	82	80	15	68	12
導入済み	72	53	65	48	17	18	85	27	88

n=107	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
無効回答	7	7	8	6	9	6	6	8	6
未導入	76	70	76	53	76	7	65	57	59
導入済み	24	30	23	48	22	94	36	42	42

表 3.8 セキュリティ対策実施状況

3.5.2. セキュリティ対策別実施状況

3.5.2.1. 入口対策

- 「セキュリティ対策の簡易アセスメント」の分析(入口対策)
  - 入口対策ではファイアウォール等などによる通信の制御（No.01）と入口対策におけるパターンに依存するメール向けのアンチウィルス（No.03）の導入状況が比較的他のサンプルより高い。
  - 入口対策におけるパターンに依存するメール向けのアンチウィルス（No.03）、および入口対策におけるパターンに依存するウェブ向けのアンチウィルス（No.04）には対象による導入差異がみられ、メールに対する対策の導入が高い。
  - 現場セキュリティアセスメントにおいて、アンチウィルス機能が搭載された外部メールサービスを利用しているケースが複数みられたことから、外部サービスの活用が比較的しやすいメールにおいて導入が進んでいる可能性が考えられる。
  - パターンに依存しないアンチウィルスチェック（No.05）、および入口対策におけるパターンに依存しないウェブ向けのアンチウィルス（No.06）の導入状況は全アセスメント項目中で最も低い状況である。パターンに依存しないアンチウィルスについては、対象による導入差異がほぼ見られず、導入しているか、導入していないかの二極化の状況がみられる。

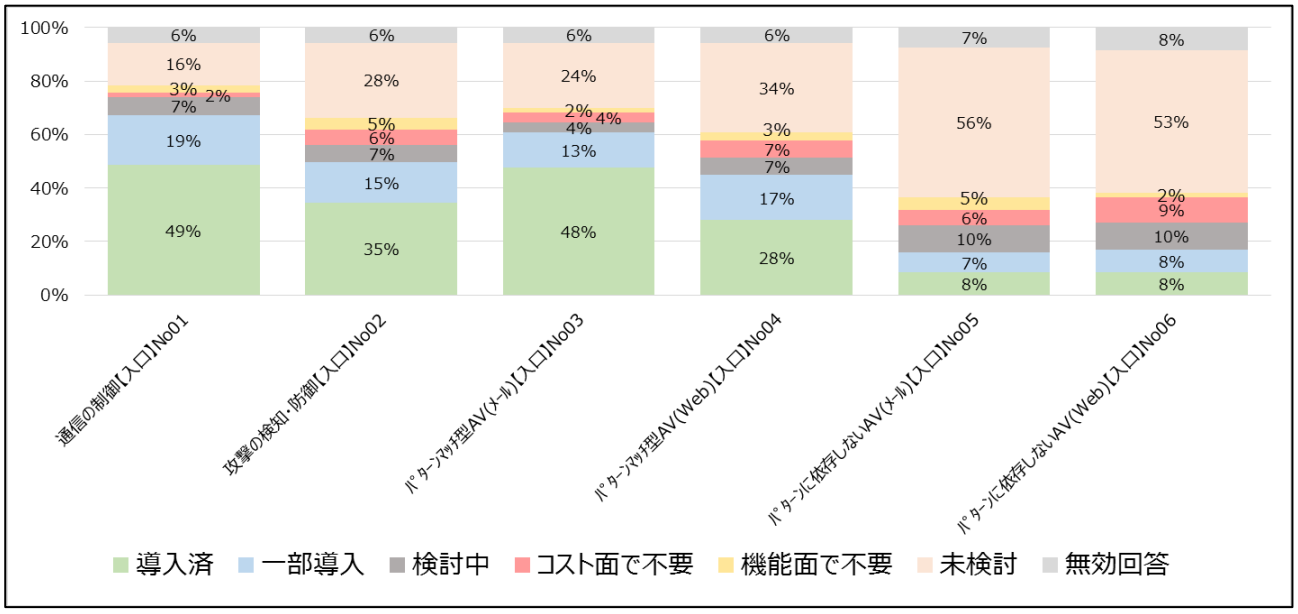


図 3.20 セキュリティ対策別実施状況(入口対策)

（単位：社）

n=107	No.01	No.02	No.03	No.04	No.05	No.06
未検討	17	30	26	36	60	57
機能面で不要	3	5	2	3	5	2
コスト面で不要	2	6	4	7	6	10
検討中	7	7	4	7	11	11
一部導入	20	16	14	18	8	9
導入済	52	37	51	30	9	9
無効回答	6	6	6	6	8	9

表 3.9 セキュリティ対策別実施状況(入口対策)

3.5.2.2. 内部対策

- 「セキュリティ対策の簡易アセスメント」の分析(内部対策)
  - 内部対策ではパターンマッチ型アンチウィルス（No.07）とセキュリティパッチの適用（No.09）の導入状況が他のサンプルより高い（80%前後の導入率）。
  - パターンに依存しないアンチウィルスチェック（No.08）の導入状況はサンプル全体のなかで低い。

    現場セキュリティアセスメントにおいて、エンドポイントセキュリティ対策として導入している製品に搭載された機能を把握していない状況が複数みられた。現在のエンドポイント向けアンチウィルスソフトウェアには複数のセキュリティ対策が統合されていることが多く、昨今ではパターンファイルに存しないアンチウィルス機能も搭載されていることが多い。このことから、パターンに依存しないアンチウィルスチェック（No.08）の対策については実態よりも低い導入状況を示している可能性が考えられる。
  - セキュリティ監視・分析（No.10 および No.11）の実施状況はサンプル全体のなかでも低い。

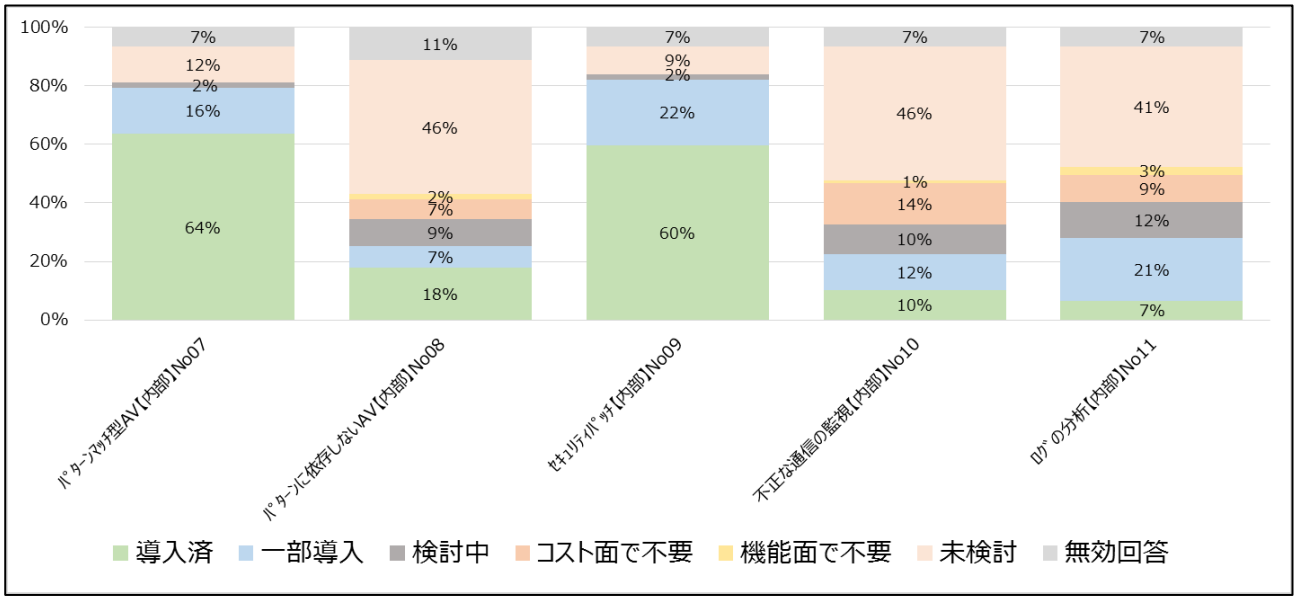


図 3.21 セキュリティ対策別実施状況(内部対策)

（単位：社）

n=107	No.07	No.08	No.09	No.10	No.11
未検討	13	49	10	49	44
機能面で不要	0	2	0	1	3
コスト面で不要	0	7	0	15	10
検討中	2	10	2	11	13
一部導入	17	8	24	13	23
導入済	68	19	64	11	7
無効回答	7	12	7	7	7

表 3.10 セキュリティ対策別実施状況(内部対策)

3.5.2.3. 出口対策

- 「セキュリティ対策の簡易アセスメント」の分析(出口対策)
  - 出口対策のなかでは Web フィルタ（No.13）の実施状況が比較的高いものの 45%の導入率にとどまる。

    Web フィルタ（No.13）の実施状況が高い理由としては、UTM に搭載された機能の使用やエンドポイントセキュリティ対策製品による実施が一因として挙げられる。
  - プロキシ（No.12）、および攻撃者のサーバへのアクセス制御（No.14）の実施状況は「導入済」と「一部導入」をあわせて 20%程度とサンプル全体のなかでも低い。

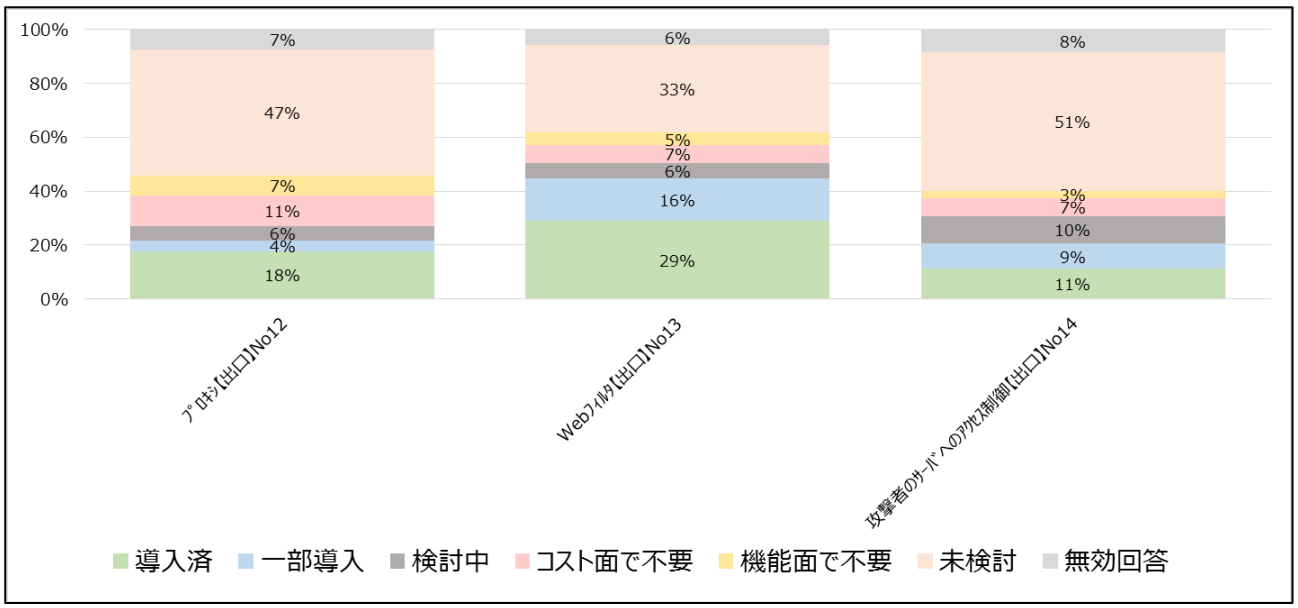


図 3.22 セキュリティ対策別実施状況(出口対策)

（単位：社）

n=107	No.12	No.13	No.14
未検討	50	35	55
機能面で不要	8	5	3
コスト面で不要	12	7	7
検討中	6	6	11
一部導入	4	17	10
導入済	19	31	12
無効回答	8	6	9

表 3.11 セキュリティ対策別実施状況(出口対策)

3.5.2.4. その他（インシデント対策、教育）

- 「セキュリティ対策の簡易アセスメント」の分析(その他)
  - データのバックアップ（No.15）は全アセスメント項目でもっと高い 88%の実施率であった。
    バックアップの取得状況は高いものの、実施状況の内訳では「一部導入」の比率が高い状況となっている。現場セキュリティアセスメントにおいても、サーバ（ファイルサーバ等）のバックアップは適切に取得されているものの、クライアント PC 上に保存されたデータの管理がされていない状況が複数確認された。このことが一部導入の比率が高い要因の一つとなっていることが考えられる。
  - インシデント対応（No.17）、および社員教育（No.18）の実施状況は、「導入済」と「一部導入」をあわせて 40%程度とサンプル全体のなかでもやや高めである。
  - プログラムの実行記録（No.16）の実施状況は、「導入済」と「一部導入」をあわせて 33%、「導入済」においては 9%でサンプル全体のなかでも低い。

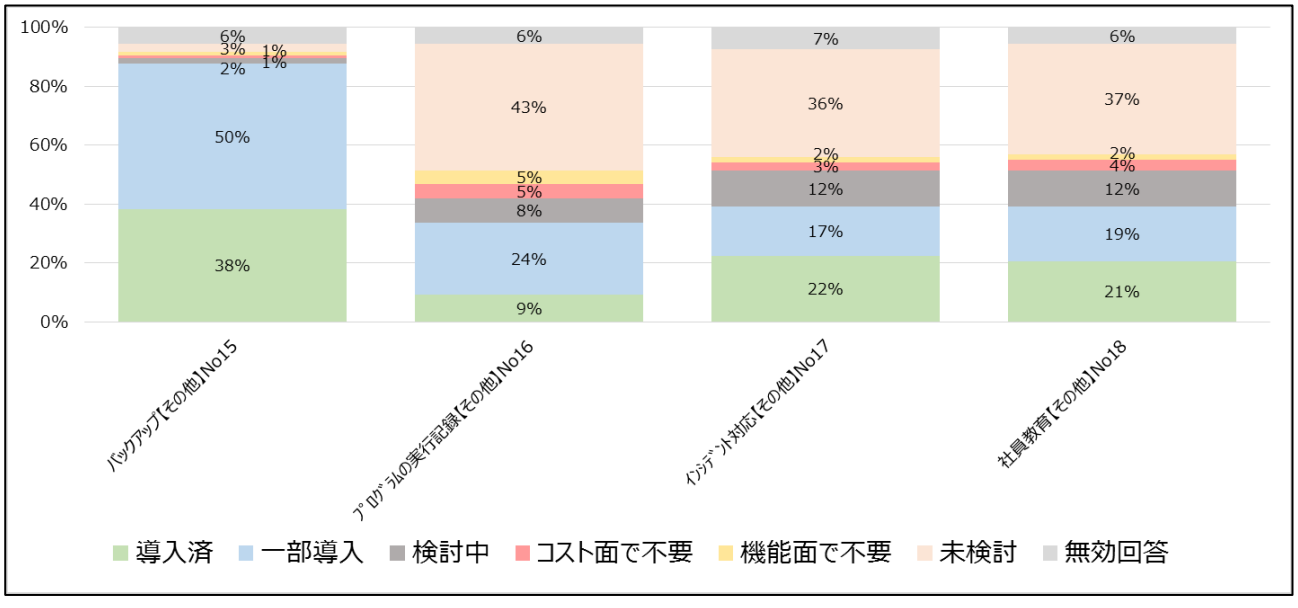


図 3.23 セキュリティ対策別実施状況(その他)

（単位：社）

n=107	No.15	No.16	No.17	No.18
未検討	3	46	39	40
機能面で不要	1	5	2	2
コスト面で不要	1	5	3	4
検討中	2	9	13	13
一部導入	53	26	18	20
導入済	41	10	24	22
無効回答	6	6	8	6

表 3.12 セキュリティ対策別実施状況(その他)

3.5.3. セキュリティ対策別未実施理由

3.5.3.1. 入口対策

- 「セキュリティ対策の簡易アセスメント」の未実施理由分析(入口対策)
  - 未実施理由の大半を「未検討」が占める。
  - ファイアウォール等などによる通信の制御（No.01）について導入を検討している回答比率が比較的多い。回答数では、入口対策におけるパターンに依存しないメール向けのアンチウィルス（No.05）、および入口対策におけるパターンに依存しないウェブ向けのアンチウィルス（No.06）を「検討中」との回答が 11 件と多い。

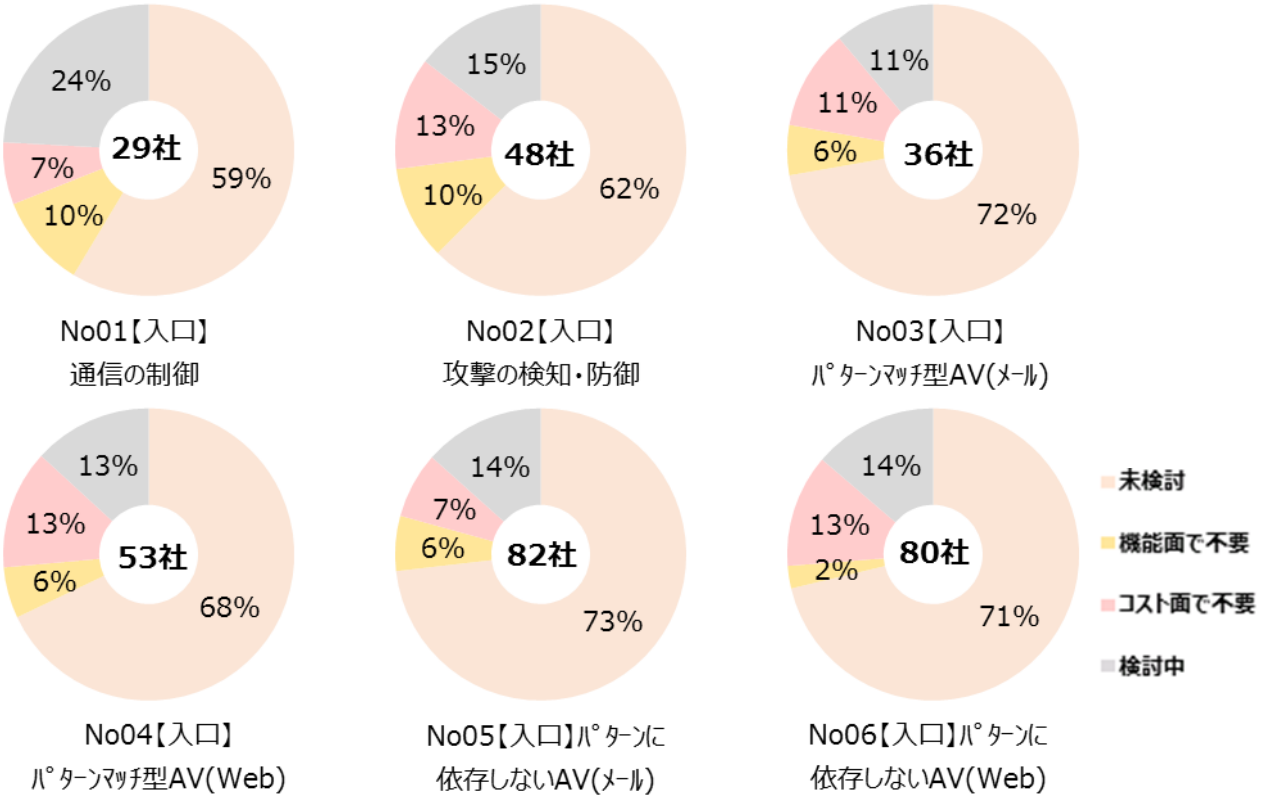


図 3.24 セキュリティ対策別未実施理由（入口対策）

3.5.3.2. 内部対策

- 「セキュリティ対策の簡易アセスメント」の未実施理由分析(内部対策)
  - 未実施理由の大半を「未検討」が占める。
  - パターンマッチ型アンチウィルス(No.07)、およびセキュリティパッチの適用（No.09）について、導入を検討し、「コスト面で不要」や「機能面で不要」と判断した回答がなく、導入の必要性が高いと判断される傾向があると考える。
  - ログの分析（No.11）は導入を「検討中」とした回答が多い。
  - エンドポイントにおけるパターンに依存しないアンチウィルス（No.08）、および不正な通信の監視（No.10）、ログの分析（No.11）はコスト面が未導入に至った理由の大半を占める。

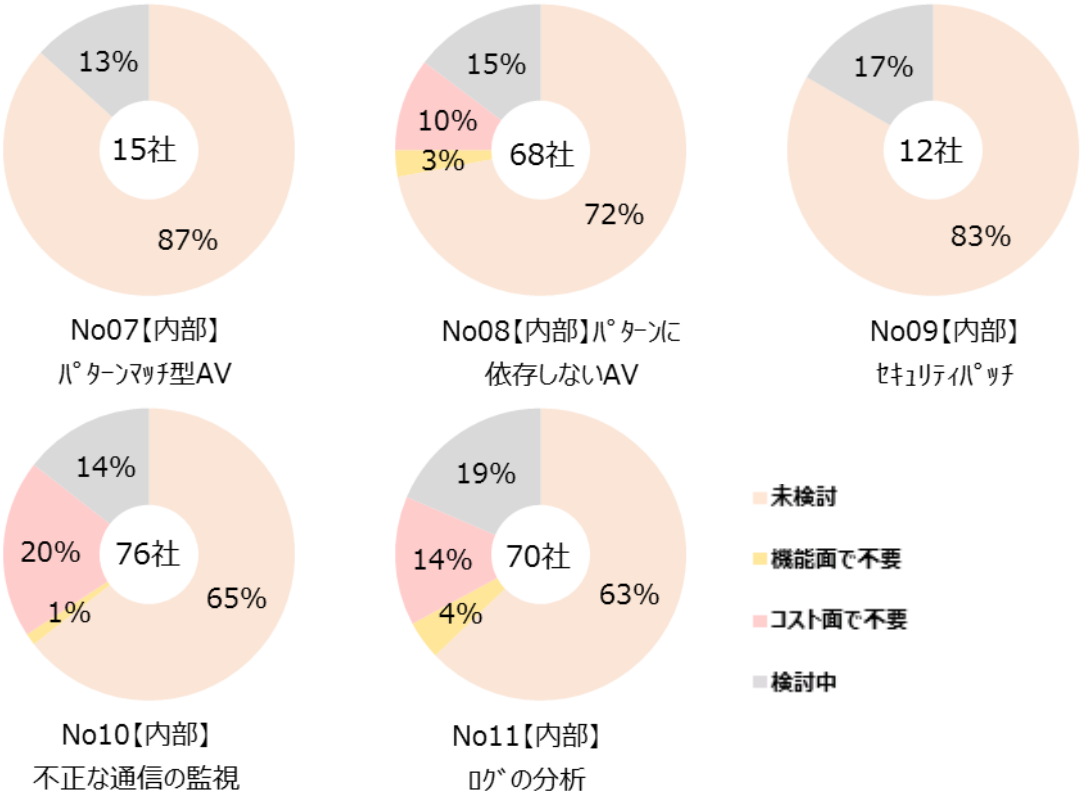
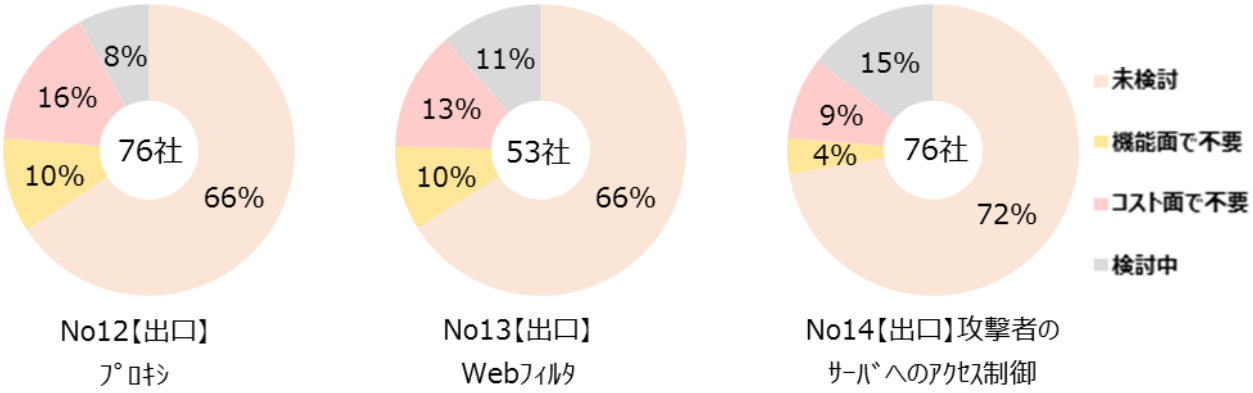


図 3.25 セキュリティ対策別未実施理由（内部対策）

3.5.3.3. 出口対策

- 「セキュリティ対策の簡易アセスメント」の未実施理由分析(出口対策)
  - 未実施理由の大半を「未検討」が占める。
  - 未導入に至った最大の理由はコスト面(9%～16%)であるが、機能面で未導入(4%～10%程度)と判断された比率も大きい。



No12【出口】
ﾌﾟﾛｷｼ

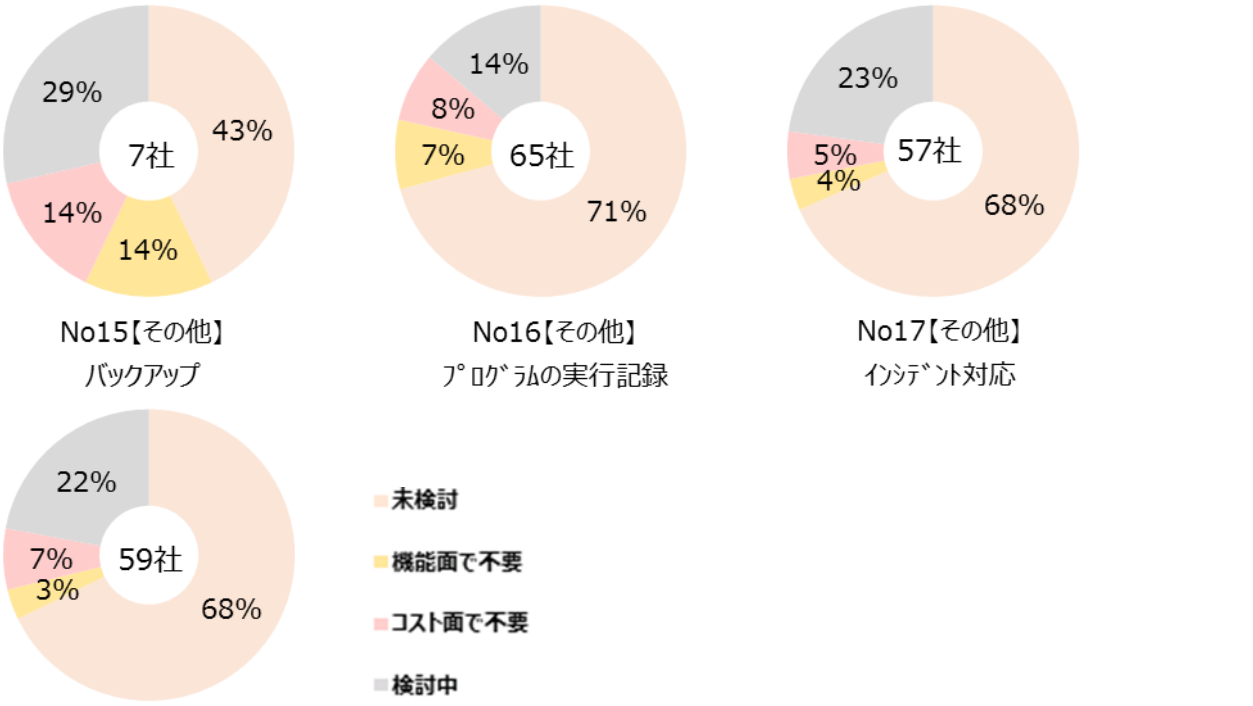
No13【出口】
Webﾌｨﾙﾀ

No14【出口】攻撃者のｻｰﾊﾞへのｱｸｾｽ制御

図 3.26 セキュリティ対策別未実施理由（出口対策）

3.5.3.4. その他（インシデント対応、社員教育）

- 「セキュリティ対策の簡易アセスメント」の未実施理由分析(その他)
  - 未実施理由の大半を「未検討」が占める。
  - インシデント対応（No.17）、および社員教育（No.18）は導入を「検討中」(22%)とした回答が多い。



No15【その他】
ﾊﾞｯｸｱｯﾌﾟ

No16【その他】
ﾌﾟﾛｸﾞﾗﾑの実行記録

No17【その他】
ｲﾝｼﾃﾞﾝﾄ対応

No18【その他】
社員教育

図 3.27 セキュリティ対策別未実施理由（その他）

3.5.4. 業種別セキュリティ対策実施状況

業種別セキュリティ対策実施状況では、回答のあった業種のうちサンプル数の多い業種を対象に分析を実施する。対象とする業種は以下の通りとする。

業種名	サンプル数
製造業	55
建設業	8
卸売業、小売業	13
情報通信業	10

表 3.13 業種別セキュリティ対策実施状況

3.5.4.1. 製造業

- 「セキュリティ対策の簡易アセスメント」の業種別分析(製造業)
  - サンプル全体の対策実施状況とほぼ同様の対策実施傾向を示しているものと考えられる。
  - 本アセスメントの分析対象サンプルの約半数を製造業の回答が占めるため、全体の回答に製造業の傾向が反映されていることに起因するものと考えられる。

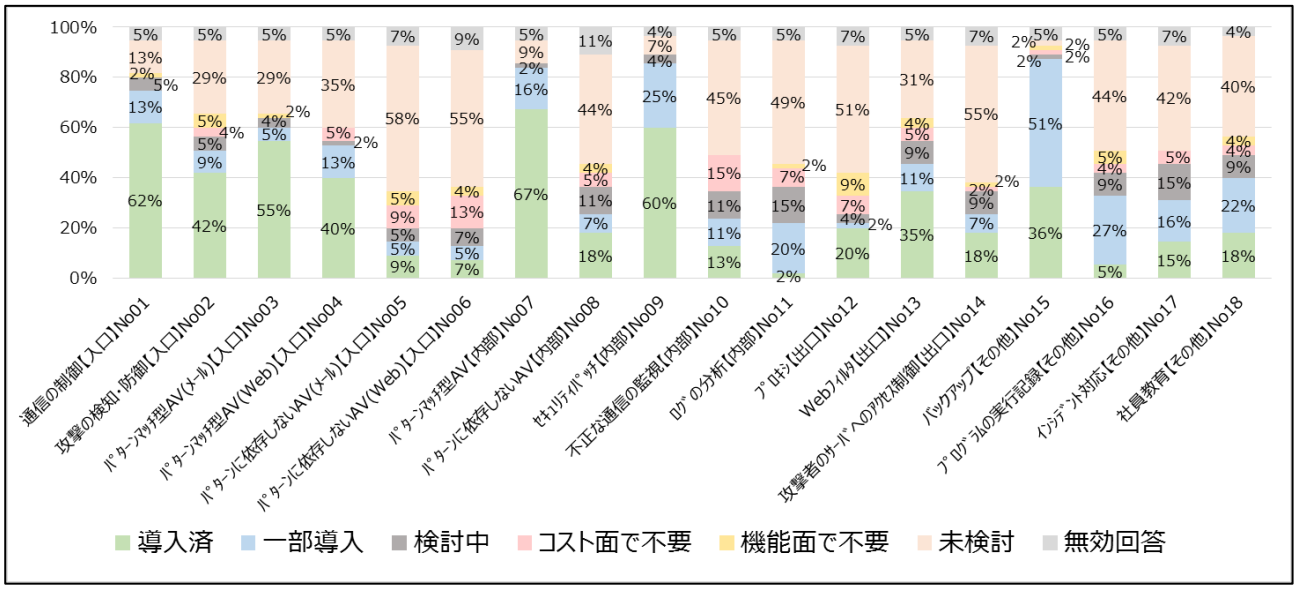


図 3.28 業種別セキュリティ対策実施状況（製造業）

（単位：社）

n=55	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	7	16	16	19	32	30	5	24	4
機能面で不要	1	3	1	0	3	2	0	2	0
コスト面で不要	0	2	0	3	5	7	0	3	0
検討中	3	3	2	1	3	4	1	6	2
一部導入	7	5	3	7	3	3	9	4	14
導入済	34	23	30	22	5	4	37	10	33
無効回答	3	3	3	3	4	5	3	6	2

n=55	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	25	27	28	17	30	1	24	23	22
機能面で不要	0	1	5	2	1	1	3	0	2
コスト面で不要	8	4	4	3	1	1	2	3	2
検討中	6	8	2	5	5	1	5	8	5
一部導入	6	11	1	6	4	28	15	9	12
導入済	7	1	11	19	10	20	3	8	10
無効回答	3	3	4	3	4	3	3	4	2

表 3.14 業種別セキュリティ対策実施状況（製造業）

3.5.4.2. 建設業

- 「セキュリティ対策の簡易アセスメント」の業種別分析(建設業)
  - サンプル全体の対策実施状況との間で傾向に大きな差異はない。
  - 対策未実施の理由として、「コスト面で不要」の回答がない点がサンプル全体の回答との大きな差異である。
  - ファイアウォール等などによる通信の制御（No.01）、および入口対策におけるパターンに依存するメール向けのアンチウィルス（No.03）について「未検討」との回答がない点も特徴である。

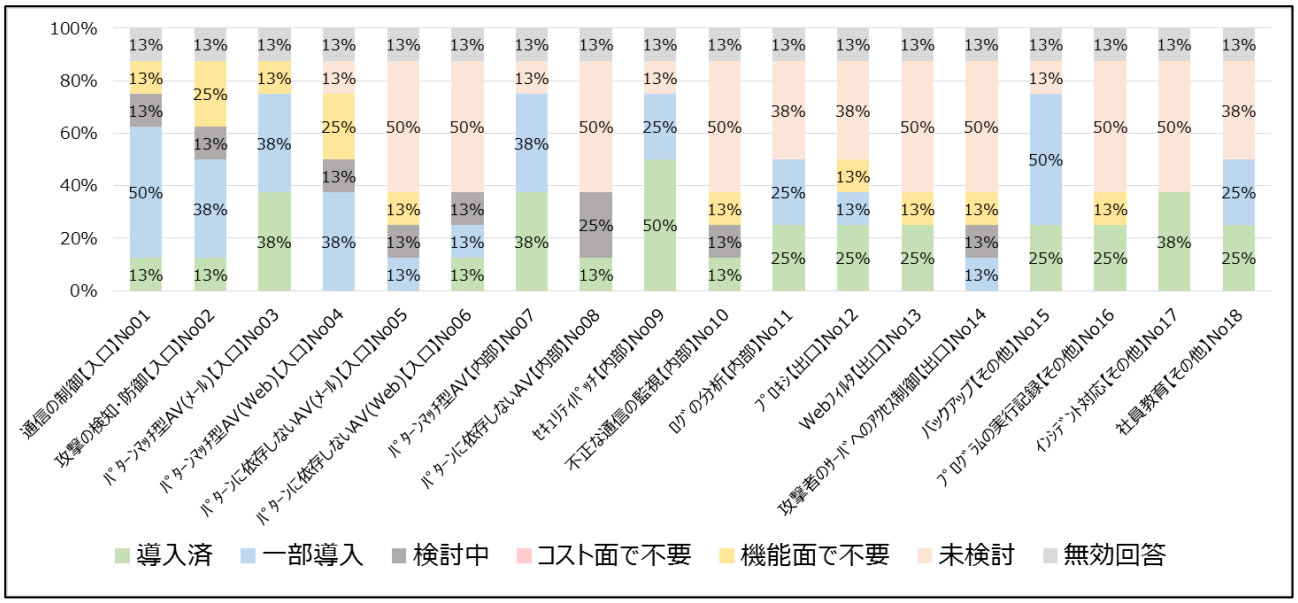


図 3.29 業種別セキュリティ対策実施状況（建設業）

（単位：社）

n=8	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	0	0	0	1	4	4	1	4	1
機能面で不要	1	2	1	2	1	0	0	0	0
コスト面で不要	0	0	0	0	0	0	0	0	0
検討中	1	1	0	1	1	1	0	2	0
一部導入	4	3	3	3	1	1	3	0	2
導入済	1	1	3	0	0	1	3	1	4
無効回答	1	1	1	1	1	1	1	1	1

n=8	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	4	3	3	4	4	1	4	4	3
機能面で不要	1	0	1	1	1	0	1	0	0
コスト面で不要	0	0	0	0	0	0	0	0	0
検討中	1	0	0	0	1	0	0	0	0
一部導入	0	2	1	0	1	4	0	0	2
導入済	1	2	2	2	0	2	2	3	2
無効回答	1	1	1	1	1	1	1	1	1

表 3.15 業種別セキュリティ対策実施状況（建設業）

3.5.4.3. 卸売業、小売業

- 「セキュリティ対策の簡易アセスメント」の業種別分析(卸売業、小売業)
  - サンプル全体の対策実施状況との間で傾向に大きな差異はない。
  - 「機能面で未導入」と判断した回答がログの分析(8%)、インシデント対応(8%)のみで少ない。

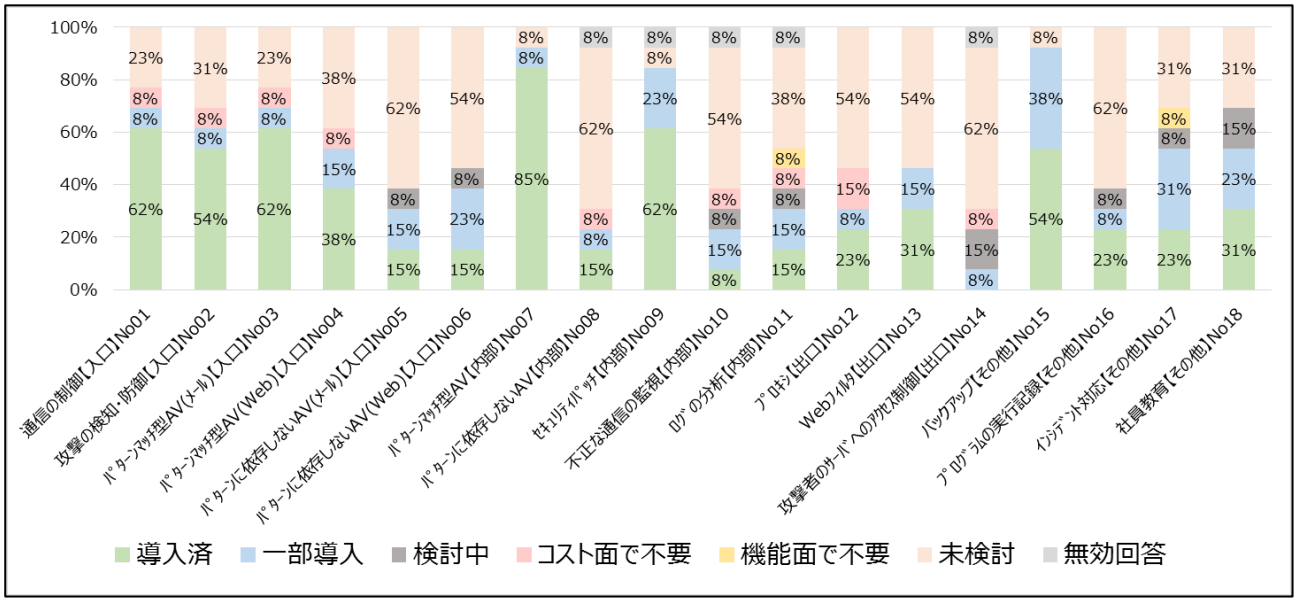


図 3.30 業種別セキュリティ対策実施状況（卸売業、小売業）

（単位：社）

n=13	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	3	4	3	5	8	7	1	8	1
機能面で不要	0	0	0	0	0	0	0	0	0
コスト面で不要	1	1	1	1	0	0	0	1	0
検討中	0	0	0	0	1	1	0	0	0
一部導入	1	1	1	2	2	3	1	1	3
導入済	8	7	8	5	2	2	11	2	8
無効回答	0	0	0	0	0	0	0	1	1

n=13	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	7	5	7	7	8	1	8	4	4
機能面で不要	0	1	0	0	0	0	0	1	0
コスト面で不要	1	1	2	0	1	0	0	0	0
検討中	1	1	0	0	2	0	1	1	2
一部導入	2	2	1	2	1	5	1	4	3
導入済	1	2	3	4	0	7	3	3	4
無効回答	1	1	0	0	1	0	0	0	0

表 3.16 業種別セキュリティ対策実施状況（卸売業、小売業）

3.5.4.4. 情報通信業

- 「セキュリティ対策の簡易アセスメント」の業種別分析(情報通信業)
  - 他業種と比較して、サイバーセキュリティに社員で対応できるとの回答割合が高く、パターンマッチ型アンチウィルス（No.07）、およびセキュリティパッチの適用（No.09）、データのバックアップ（No.15）については実施率が 100%であった。
  - インシデント対応（No.17）について、サンプル全体の対策実施状況と比較して実施率(70%)が高い、他業種と比較して、サイバーセキュリティに社員で対応できるとの回答割合が高い点が、対策実施状況に反映されている可能性が考えられる。

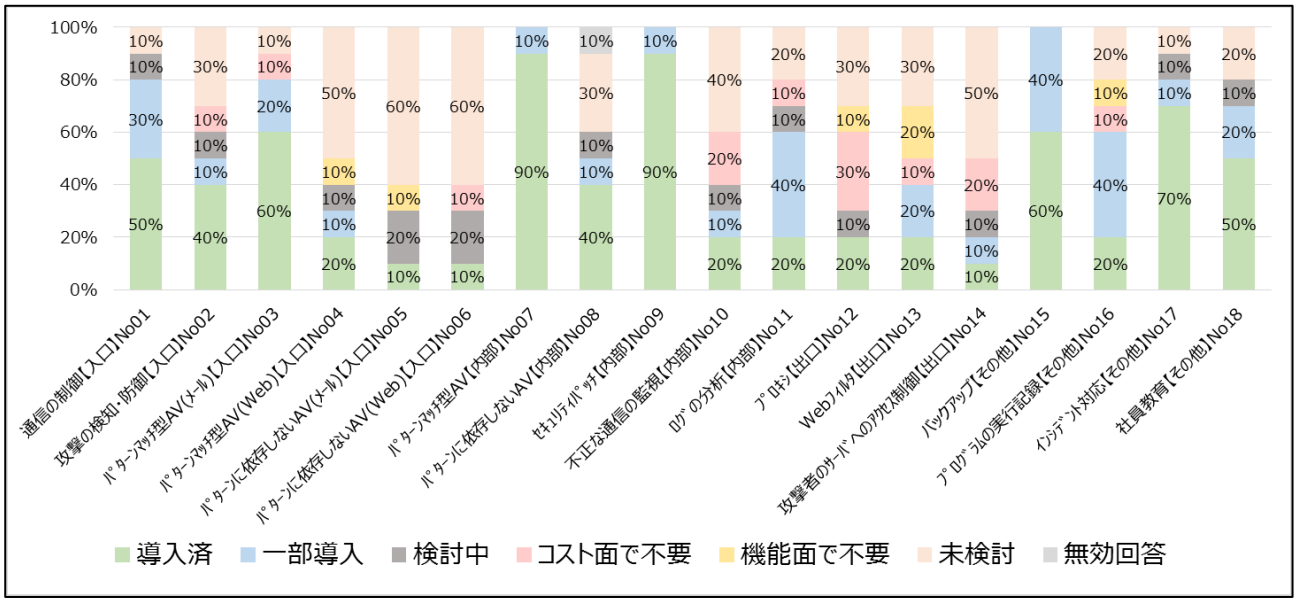


図 3.31 業種別セキュリティ対策実施状況（情報通信業）

（単位：社）

n=10	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	1	3	1	5	6	6	0	3	0
機能面で不要	0	0	0	1	1	0	0	0	0
コスト面で不要	0	1	1	0	0	1	0	0	0
検討中	1	1	0	1	2	2	0	1	0
一部導入	3	1	2	1	0	0	1	1	1
導入済	5	4	6	2	1	1	9	4	9
無効回答	0	0	0	0	0	0	0	1	0

表 3.17 業種別セキュリティ対策実施状況（情報通信業）（1/2）

（単位：社）

n=10	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	4	2	3	3	5	0	2	1	2
機能面で不要	0	0	1	2	0	0	1	0	0
コスト面で不要	2	1	3	1	2	0	1	0	0
検討中	1	1	1	0	1	0	0	1	1
一部導入	1	4	0	2	1	4	4	1	2
導入済	2	2	2	2	1	6	2	7	5
無効回答	0	0	0	0	0	0	0	0	0

表 3.18 業種別セキュリティ対策実施状況（情報通信業）（2/2）

3.5.5. 組織規模別セキュリティ対策実施状況

組織規模別セキュリティ対策実施状況では、回答者の所属する組織の従業員数（公表されている数値または日立製作所の推測による数値）を基に組織規模を４段階に分類し分析を実施する。組織規模の分類基準を以下に示す。

従業員数	組織規模	サンプル数
10 名以下	Home	23
11 名以上 100 名以下	Small	52
101 名以上 300 名以下	Medium	18
301 名以上	Large	14

表 3.19 組織規模別セキュリティ対策実施状況

3.5.5.1. Home（従業員数 10 名以下）

- 「セキュリティ対策の簡易アセスメント」の組織規模別分析(従業員数 10 名以下)
  - パターンマッチ型アンチウィルス（No.07）、およびセキュリティパッチの適用（No.09）をはじめ、サンプル全体の対策実施状況と比較して実施率が低い。
  - データのバックアップ（No.15）については、サンプル全体と同様に実施率が 78%と高い。
    現場セキュリティアセスメントにて訪問した同規模の組織においてもバックアップは取得しているとの回答が得られている。

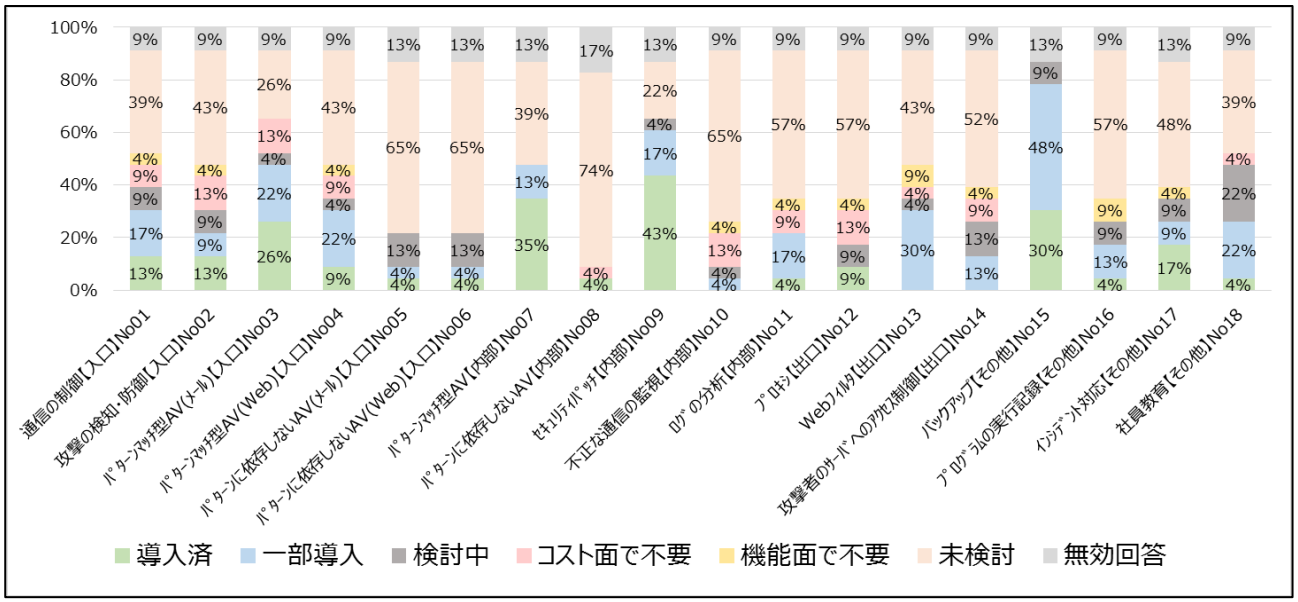


図 3.32 組織規模別セキュリティ対策実施状況（Home）

（単位：社）

n=23	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	9	10	6	10	15	15	9	17	5
機能面で不要	1	1	0	1	0	0	0	0	0
コスト面で不要	2	3	3	2	0	0	0	1	0
検討中	2	2	1	1	3	3	0	0	1
一部導入	4	2	5	5	1	1	3	0	4
導入済	3	3	6	2	1	1	8	1	10
無効回答	2	2	2	2	3	3	3	4	3

表 3.20 組織規模別セキュリティ対策実施状況（Home）(1/2)

n=23	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	15	13	13	10	12	0	13	11	9
機能面で不要	1	1	1	2	1	0	2	1	0
コスト面で不要	3	2	3	1	2	0	0	0	1
検討中	1	0	2	1	3	2	2	2	5
一部導入	1	4	0	7	3	11	3	2	5
導入済	0	1	2	0	0	7	1	4	1
無効回答	2	2	2	2	2	3	2	3	2

表 3.21 組織規模別セキュリティ対策実施状況（Home）(2/2)

3.5.5.2. Small（従業員数 11 名以上 100 名以下）

- 「セキュリティ対策の簡易アセスメント」の組織規模別分析(従業員数 11 名以上 100 名以下)
  - サンプル全体の対策実施状況とほぼ同様の対策実施傾向を示している。

    本アセスメントの分析対象サンプルの約半数を Small 規模の組織の回答が占めるため、全体の回答に本規模の組織の傾向が反映されているものと考えられる。

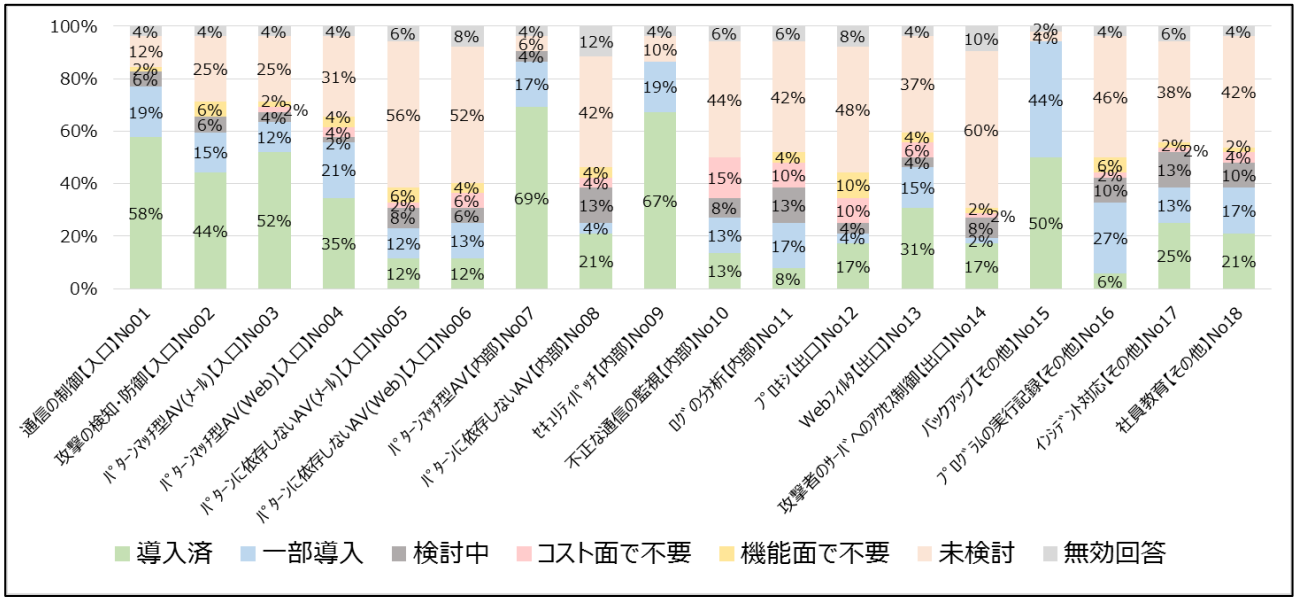


図 3.33 組織規模別セキュリティ対策実施状況（Small）

（単位：社）

n=52	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	6	13	13	16	29	27	3	22	5
機能面で不要	1	3	1	2	3	2	0	2	0
コスト面で不要	0	0	1	2	1	3	0	2	0
検討中	3	3	2	1	4	3	2	7	0
一部導入	10	8	6	11	6	7	9	2	10
導入済	30	23	27	18	6	6	36	11	35
無効回答	2	2	2	2	3	4	2	6	2

n=52	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	23	22	25	19	31	2	24	20	22
機能面で不要	0	2	5	2	1	0	3	1	1
コスト面で不要	8	5	5	3	1	0	1	1	2
検討中	4	7	2	2	4	0	5	7	5
一部導入	7	9	2	8	1	23	14	7	9
導入済	7	4	9	16	9	26	3	13	11
無効回答	3	3	4	2	5	1	2	3	2

表 3.22 組織規模別セキュリティ対策実施状況（Small）

3.5.5.3. Medium（従業員数 101 名以上 300 名以下）

- 「セキュリティ対策の簡易アセスメント」の組織規模別分析(従業員数 101 名以上 300 名以下)
  - サンプル全体の対策実施状況との間で傾向に大きな差異はない。
  - パターンマッチ型アンチウィルス（No.07）について実施率が 100%[2]である。
  - 対策未実施理由として、「コスト面で不要」と判断した回答が 13 項目/18 項目と比較的多い。
    Medium 規模の組織は製造業（サンプル数 12/18 件）が大半を占めている。

[2] 無効回答を除く

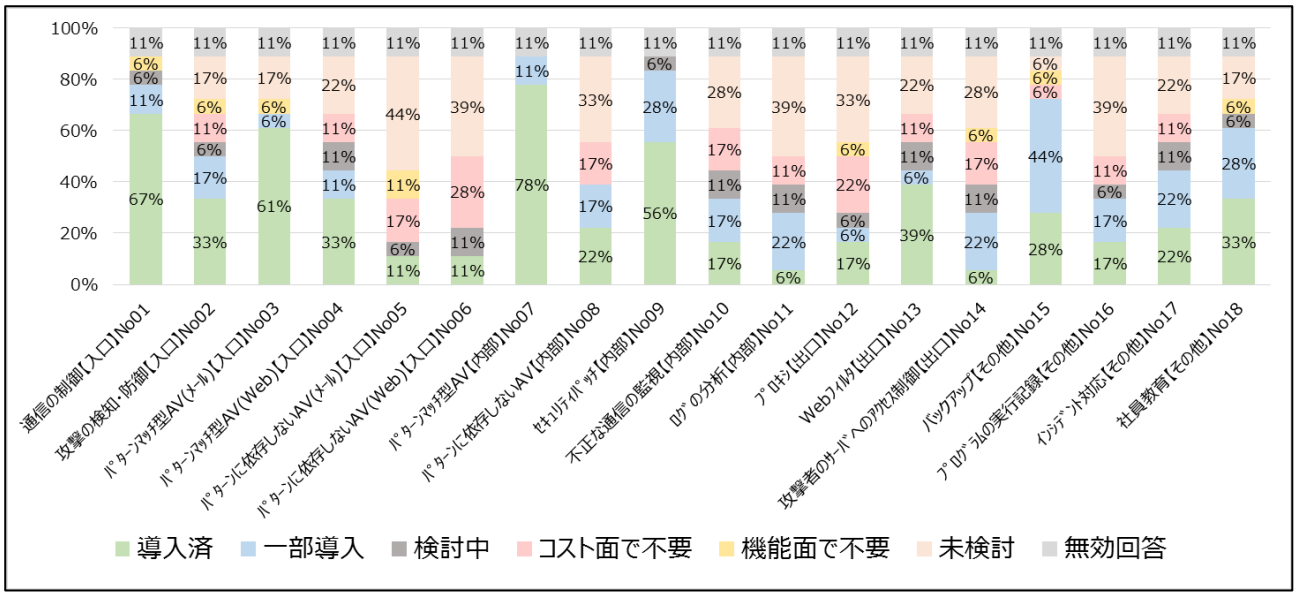


図 3.34 組織規模別セキュリティ対策実施状況（Medium）

（単位：社）

n=18	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	0	3	3	4	8	7	0	6	0
機能面で不要	1	1	1	0	2	0	0	0	0
コスト面で不要	0	2	0	2	3	5	0	3	0
検討中	1	1	0	2	1	2	0	0	1
一部導入	2	3	1	2	0	0	2	3	5
導入済	12	6	11	6	2	2	14	4	10
無効回答	2	2	2	2	2	2	2	2	2

n=18	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	5	7	6	4	5	1	7	4	3
機能面で不要	0	0	1	0	1	1	0	0	1
コスト面で不要	3	2	4	2	3	1	2	2	0
検討中	2	2	1	2	2	0	1	2	1
一部導入	3	4	1	1	4	8	3	4	5
導入済	3	1	3	7	1	5	3	4	6
無効回答	2	2	2	2	2	2	2	2	2

表 3.23 組織規模別セキュリティ対策実施状況（Medium）

3.5.5.4. Large（従業員数 301 名以上）

- 「セキュリティ対策の簡易アセスメント」の組織規模別分析(従業員数 301 名以上)
  - サンプル全体の対策実施状況と間で傾向に大きな差異はない。
  - セキュリティパッチの適用（No.09）、およびデータのバックアップ（No.15）について実施率が 100%である。
  - 検討の結果不要と判断した回答の比率が 7%～14%で少ない。
  - 検討中との回答の比率が多い。

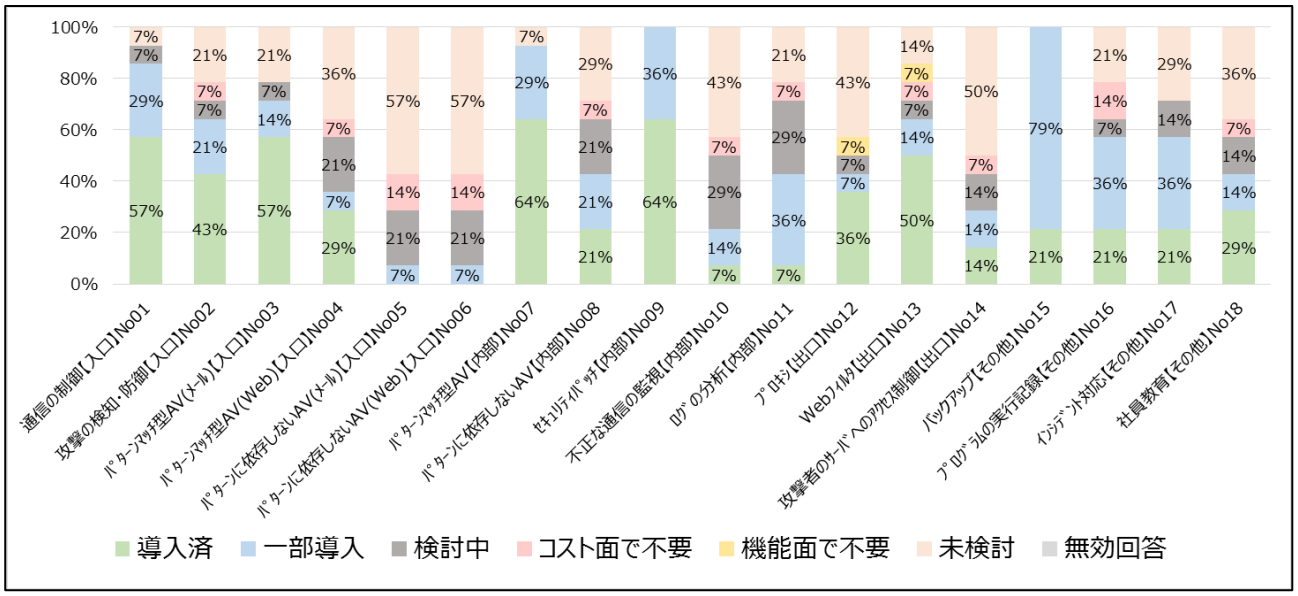


図 3.35 組織規模別セキュリティ対策実施状況（Large）

（単位：社）

n=14	No.01	No.02	No.03	No.04	No.05	No.06	No.07	No.08	No.09
未検討	1	3	3	5	8	8	1	4	0
機能面で不要	0	0	0	0	0	0	0	0	0
コスト面で不要	0	1	0	1	2	2	0	1	0
検討中	1	1	1	3	3	3	0	3	0
一部導入	4	3	2	1	1	1	4	3	5
導入済	8	6	8	4	0	0	9	3	9
無効回答	0	0	0	0	0	0	0	0	0

表 3.24 組織規模別セキュリティ対策実施状況（Large）(1/2)

n=14	No.10	No.11	No.12	No.13	No.14	No.15	No.16	No.17	No.18
未検討	6	3	6	2	7	0	3	4	5
機能面で不要	0	0	1	1	0	0	0	0	0
コスト面で不要	1	1	0	1	1	0	2	0	1
検討中	4	4	1	1	2	0	1	2	2
一部導入	2	5	1	2	2	11	5	5	2
導入済	1	1	5	7	2	3	3	3	4
無効回答	0	0	0	0	0	0	0	0	0

表 3.25 組織規模別セキュリティ対策実施状況（Large）（2/2）

3.5.6. 標的型攻撃対策問診結果との比較

標的型攻撃対策問診は、日立システムズが独自に実施している標的型攻撃メールへのセキュリティ対策実施状況を可視化するための調査である。本調査項目は、実証実験にて用いたセキュリティ対策の簡易アセスメントの設問項目とほぼ同等の内容である。ここでは、標的型攻撃対策問診における調査結果との差異について記載する。

標的型攻撃対策問診の調査概要は以下の通り：

- 標的型攻撃対策問診の設問項目は、セキュリティ対策の簡易アセスメントの設問項目と同等である。ただし、プログラムの実行記録（No.16）の設問については時期によって調査を行っていない。
- 標的型攻撃対策問診はセルフアセスメント形式で行っている。
- 回答は、設問ごとに「導入済み」、「検討中」、「未導入」から一つを選択する形式で実施している。

標的型攻撃対策問診の調査対象組織の概要は以下の通り：

従業員数	組織規模	サンプル数
10 名以下	Home	0
11 名以上 100 名以下	Small	1
101 名以上 300 名以下	Medium	17
301 名以上 [3]	Large	21
計		39

表 3.26 標的型攻撃対策問診（別調査比較１）

[3] 1,000 人以上の組織を 13 サンプル含む

プログラムの実行記録（No.16）の設問のみサンプル数は 16 である。プログラムの実行記録（No.16）の調査対象組織の概要は以下の通り：

従業員数	組織規模	サンプル数
10 名以下	Home	0
11 名以上 100 名以下	Small	0
101 名以上 300 名以下	Medium	8
301 名以上 [4]	Large	8
計		16

表 3.27 標的型攻撃対策問診（別調査比較 2）

3.5.6.1. 比較結果

- 「セキュリティ対策の簡易アセスメント」の分析結果と標的型攻撃対策問診結果との比較
  - セキュリティパッチの適用（No.09）についてセキュリティ対策の簡易アセスメントの結果は顕著に実施状況が良く、現場セキュリティアセスメントでは、セキュリティパッチの適用を自動設定としている（WSUS 等について未導入）との回答が複数みられた。これにより高い実施率になっているものと考えられる。標的型攻撃対策問診の調査対象の実施状況に対する追加のデータは有していないため評価できない。
  - プロキシ（No.12）、および Web フィルタ（No.13）、攻撃者のサーバへのアクセス制御（No.14）についてセキュリティ対策の簡易アセスメントの結果は導入・実施状況が悪い。 セキュリティ対策の簡易アセスメントの調査対象組織の規模が小さい（＝端末数が少ない）ことから、ウェブプロキシの導入が進んでいないものと思われる。
  - 標的型攻撃対策問診の調査では、会社規模が Large 規模の組織においてウェブプロキシの導入が進んでいる結果となっている。また、ウェブプロキシとあわせて URL フィルタリングの導入が進められているものと考えられる。商用 URL フィルタリングには、攻撃者の準備しているサーバへのアクセスを制限するためのデータを保有している製品が存在し、そのような製品が採用されていることが伺われる。
  - インシデント対応（No.17）、および社員教育（No.18）についてセキュリティ対策の簡易アセスメントの結果は顕著に実施状況が良い。 調査対象規模の違いから実施していると判断する状況に差が生じている可能性が考えられるが、明確に状況を説明するデータや情報を有していない。

[4] 1,000 人以上の組織を 5 サンプル含む

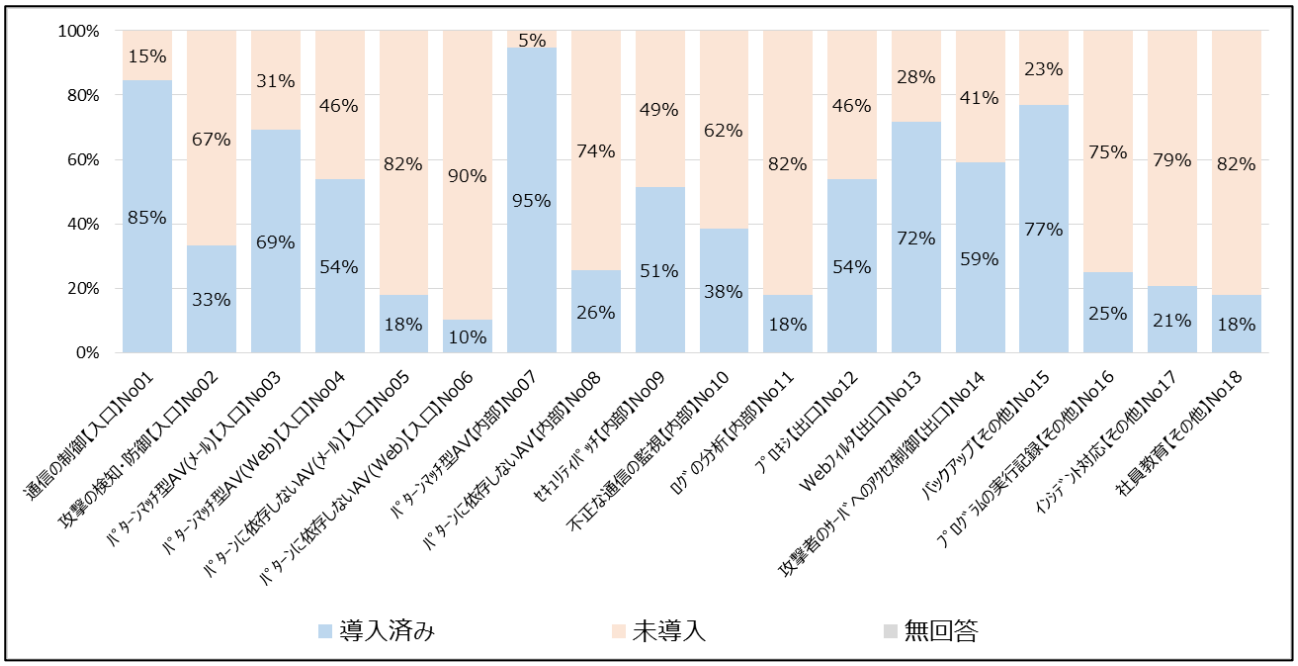


図 3.36 標的型攻撃対策問診（別調査比較）

4. 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

4.1. (3 つの機能)を備えた支援体制の構築

本事業では、プロジェクトマネージャー、プロジェクトリーダ、簡易アセスメントの担当者、および現場セキュリティアセスメントの担当者に情報処理安全確保支援士を配置し、以下の３つの機能を備えた体制の構築を行い、中小企業向けサイバーセキュリティの事後対応支援を実施した。

- 中小企業からの相談受付及び対応(機能①)
  - 本事業に参加いただいた中小企業からのサイバーセキュリティに関する内容を、既に日立製作所にてサービス提供している、お客様からの問合せ等を受付対応するコールセンターの体制を利用して本実証事業専用の受付窓内（電話、メール）を開設し構築した。
  - コールセンターは、平日の 9 時～17 時での受付体制で実施した。
  - コールセンターは、受付内容を統制チームへエスカレーションを行った。
- 相談内容がサイバーインシデント等であるかの判断（機能②)
  - 統制チームは、本事業での提供する監視サービス毎に、インターネット出入り口の監視(UTM)技術チーム、エンドポイント監視を行う EDR 技術チームの 2 チームの体制を構築した。
  - 統制チーム内のセキュリティオペレータセンタで監視を実施し、サイバーインシデント発生時のデータ収集を実施した。
  - インターネット出入り口の監視は、総合脅威管理装置(UTM)にて、情報漏えいが発生する様な危険度が高いサイバーインシデントの検出時は、24 時間お客様への緊急通報を行う体制を構築した。
  - エンドポイント監視は、マルウェア感染で情報漏えいが発生する様な危険度が高いサイバーインシデント検出時の平日 9～17 時において、中小企業へ通報の連絡を実施した。
  - サイバーインシデントの内容に応じて、サービス提供や運用実績のあるセキュリティテクニカルチームと連携しサイバーインシデントの解析を実施した。
- サイバーインシデント等が発生した際の支援の提供(機能③)
  - サイバーインシデント等が発生した際に、迅速な対応のためにメール／電話での初期対応のアドバイスによる支援を実施し、その上で必要に応じて現地への日立製作所作業員の派遣を行い、統制チームと連携して対象機器の切り分け、切り離し作業支援を平日 9～17 時で実施した。

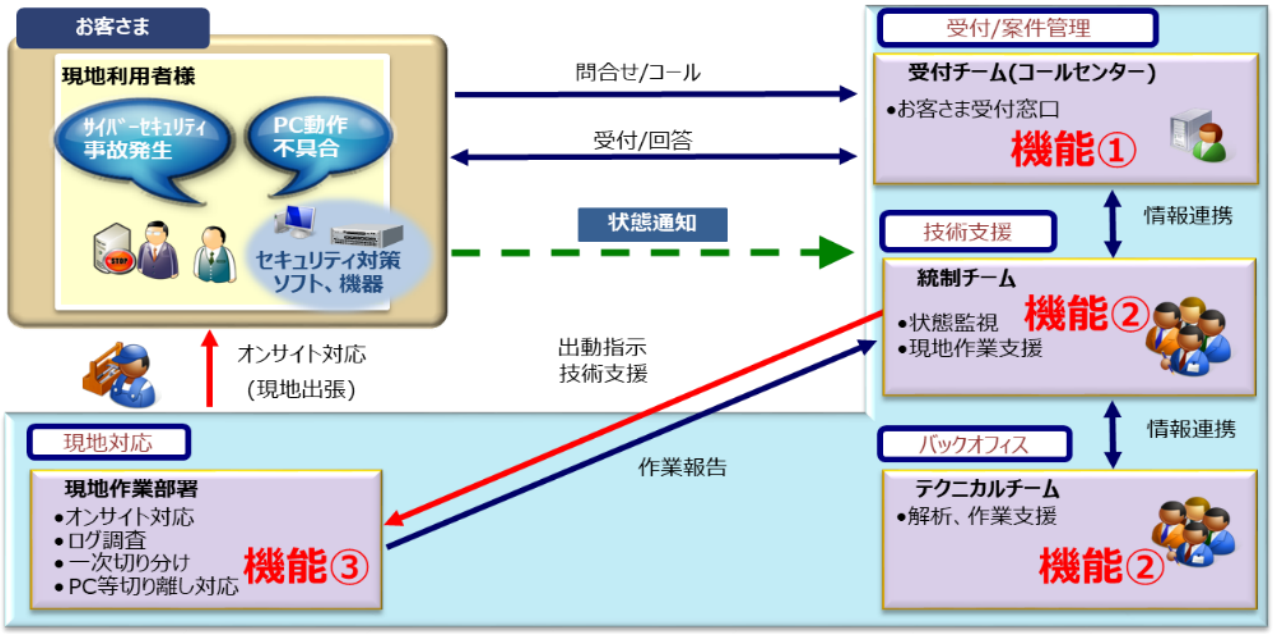


図 4.1 (3 つの機能)を備えた支援体制

4.2. 地元企業との連携

日立製作所グループのみでは、中小企業に対するアプローチルートが少ないため、中小企業へのアプローチのため地元企業等の連携し下記を実施した。

- 実証参加企業の集客の連携
  - 広島県情報産業協会の協力　(会員数：約 120 社)
    - 広島県情報産業協会の会員企業及び、会員企業のお客様への参加案内を実施。
  - 広島商工会議所
    - 広島商工会議所の工業部会員企業に、事業説明会への参加案内を実施。
  - 福山商工会議所
    - 福山商工会議所の会員企業に、事業説明会への参加案内を実施。
  - 呉商工会議所
    - 呉商工会議所の会員企業に、事業説明会への参加案内を実施。
  - 日立笠戸協同組合
    - 日立製作所　笠戸事業所と取引がある、サプライチェーンへの実証参加案内を実施。

日立製作所グループのみでは、中小企業に対するアプローチルートが少ないため、中小企業への販路、およびサービス提供できるベンダとの協業の検討が課題となった。

- 関係先からのアドバイス

  広島情報産業協会、広島・福山・呉 商工会議所、日立笠戸協同組合への協力依頼時に、ご意見、アドバイスをいただいた。

  - 実証参加呼びかけについては、地元ベンダの協力体制を円滑にするためにも、SI ベンダ色が強調されないほうがよい。
  - 商工会議所等を利用する場合は経済産業省、IPA が主催でのアナウンスであるほうが効果的である。

5. 地域実証の実施

5.1. 支援内容と実績

実証参加企業 110 社に対しての支援内容として 3 つの機能を設けた。

- 中小企業からの相談受付及び対応 (以下：機能①)
- 相談内容がサイバーインシデント等であるかの判断 (以下：機能②)
- サイバーインシデント等が発生した際の支援の提供(以下：機能③)

＜3つの機能＞
1 中小企業からの相談受付及び対応
2 相談内容がサイバーインシデント等であるかの判断
3 サイバーインシデント等が発生した際の支援の提供

項	サービス	社数	合計社数	電話 (非対面)	メール	会話 (対面)
1	**セキュリティ対策の簡易アセスメント**	107	**110社** 162名	・実証後のサービス内容の確認 1 ・サービス内容を教えて欲しい ・セミナの内容に関するお問合せ ・本実証参画のメリットについて ・個別に自社内で実証成果の説明希望 ・対策サービスのご案内	3 ・対策サービスご案内 ・簡易アセスメント結果回答 ・相談受付の問合せ先 (メールアドレス)連絡	・セミナ・よろず相談会 ・Web会議システムで アセスメント実施 ・個別に現地で実証成果の 説明を実施 1 2 3
2	**現場セキュリティアセスメント**	9		1 3 ・サービス説明+相談受付 ・セキュリティ対策の適切性を確認したい	・サービス説明 1 2 ・レポート報告 ・サービス内容に対する問合せ (機能、掛かる時間)	1 2 3 ・相談受付 ・判断および支援提供
–	**よろず相談会**	11		・IT外注ベンダに任せっきり 第三者による確認希望 1 2 3	・相談受付・支援等 1 2 3	・相談受付・支援等 1 2 3
3	**インターネット出入りの監視サービス**	10		1 2 3 ・安定稼働確認 ・設置後の機器調整 ・月次レポート (解説)	・NW/利用アプリの構成情報確認 ・設置後の機器設定の個別調整 ・月次レポート (解説) ・サービス内容に関する問合せ (機能、掛かる時間) 1 2 3	1 2 3 ・NWの構成確認 ・ルータPW初期設定からの改善 ・設置環境改善のアドバイス
4	**エンドポイント監視サービス**	13		1 2 3 ・安定稼働確認 ・相談への問合せ対応	・安定稼働確認 1 2 3 ・設置後の環境設定調整 ・サービス内容に関する問合せ (機能、掛かる時間)	・アンチウィルスソフトの ライセンス期限切れ ・アンチウィルスソフト 動作してなかった 1 2 3

図 5.1 支援体制を利用した支援内容 概要

本機能はサービス設計時の機能に、実証サービスを提供する過程で支援対応の改善のため下記の内容も実施した。

- 機能①：ミニセミナー実施にメールや郵便によるダイレクトメール送付では応答が遅れると参加企業から伺った。実態としても問い合わせの反応が悪かった。電話・メールの受付としてのインバウンド機能のみでなく、実証参加企業に対しての連絡や御用聞きといったアウトバウンドでのアプローチを実施する機能を追加した。
- 機能②：機能①の追加に伴いサイバーインシデントの判断のみの対応だけでなく、相談の内容調査・解析、解決案の策定を実施した。
- 機能③：機能②と同様にサイバーインシデント解決の調査・支援だけでなく、実証参加企業の不安や不明点の解決のため現地での支援活動を実施した。

上記 3 つの機能を使用した支援内容の具体的な内容について記載する。

(1)サービス提供前準備の支援

サービスのご案内と参加意思の確認を行った後にサービス導入に必要となる情報を送付いただくため参加企業よりヒアリングシートを記入し提出頂くが、提出までに長時間を要している事が多く、未提出の企業に対して電話でのフォローコールを行った。未提出の理由としては、実証参加企業が現地設備の情報を持っていない、資料が残っていないなどにてヒアリングシートへ記入ができなくなっている状況が多かった。実証参加企業先へ訪問してのヒアリング、および対象機器の PC、ネットワークの環境確認を行う支援を行った。

（機能①）：ヒアリングシート未提出の企業に対して電話でのフォローコールを実施した。

（機能②）：入手したヒアリングシートの確認と未提出企業にはネットワーク構成図作成による提案を実施した。

（機能③）：ヒアリングシートが提出できない企業に対して現地訪問による環境調査を実施した。

(2)サービス提供中の安定稼働支援

サービス導入後の企業に対して、安定稼働の支援として、通報やログに現れない現象がないか、使用感はどうか等の確認をメール、および電話で実施した。

対応事例として、エンドポイント監視サービス使用の実証参加企業において PDF の表示が遅くなったとのご申告があり個別チューニングを実施し解決を図った。

（機能①）：安定稼働の支援として参加企業へ状況ヒアリングを実施した。

（機能②）：テクニカルチームにて個別チューニングの検討・適用を実施した。

(3)セミナー後の個別説明支援

成果報告会（中間報告）に参加いただいた企業よりセキュリティの危機感を覚え、セキュリティ啓発として自社内で成果報告会（中間報告）の個別説明の依頼を頂き、現地訪問し実施した。

（機能①）：成果報告会（中間報告）後サービス導入の勧誘を実施し、実証参加企業からの要望をヒアリングした。

（機能②）：個別説明支援の調整・準備を実施した。

（機能③）：現地訪問し個別説明を実施した。

(4)監視サービスでの改善提案支援

ルータおよび NAS(Network Access Storage)の脆弱性のある通信を多数検知。

この状態を実証参加企業へ報告および改善案の提案を実施した（現地駆けつけに至るインシデントの検出はなし）。

（機能①）：脆弱性に関連する通信が検知されたことをご連絡、改善策の提案を実施した。

（機能②）：ログを調査、原因究明と改善案の検討を実施した。

5.1.1. セキュリティ対策の簡易アセスメントによる支援

3 つの機能を用いた支援状況を以下に記載する。

項	項目	内容
1	目的（ねらい）	中小企業のセキュリティ対策状況の把握、個々の中小企業のセキュリティ対策状況を踏まえて推奨対策プランを提示し、優先すべき課題の可視化した。 ・標的型攻撃の対策状況および弱点を可視化 ・可視化した結果から、優先すべき対策を明示
2	実施内容	・セミナー参加者等に標的型攻撃に対する 18 問のセキュリティ対策状況の質問を実施し回答を収集した。 ・日立製作所の分析ナレッジを利用したセキュリティ対策の簡易アセスメント結果（以下、診断書）を提示した。
3	実施結果	・実証参加企業 107 社（126 名）に対し診断書を送付。 ・実証参加企業反応：本内容を基に外注ベンダに対策検討依頼した。 現場セキュリティアセスメントの実施依頼があった。 ・集計結果：情報漏えい等被害と食い止める（出口対策）対策率が低い。 ・規模別の対策状況は従業員数 10 名以下の対策状況が低い。

表 5.1 セキュリティ対策の簡易アセスメント概要

アセスメント結果は、企業毎に効果の高いセキュリティ対策内容、実証参加企業の特徴や、対応方針のアドバイスの記載により、対策の優先度など決めていただく判断材料としている。また、セキュリティ対策においては、同業種の状況を鑑み、導入を決める企業も少なくない。現場セキュリティアセスメント時のヒアリングでも、「実際に知っている企業(同業種)が被害にあわなければ危機感を感じない」との意見もあった。

本診断書は、同業種のセキュリティ対策毎の実装率を記載しており、同業種と自社の比較検討を可能としている。また、サイバー攻撃の手法別にどのようなセキュリティ対策製品が有効であるかを図式化してあり、回答頂いた企業のセキュリティ対策実装状況と合わせて危険度が判るようにしている。

（図 5.2 セキュリティ対策の簡易アセスメント診断書、図 5.3 セキュリティ対策の簡易アセスメント診断書（サイバー攻撃の手法別の記載例）参照）

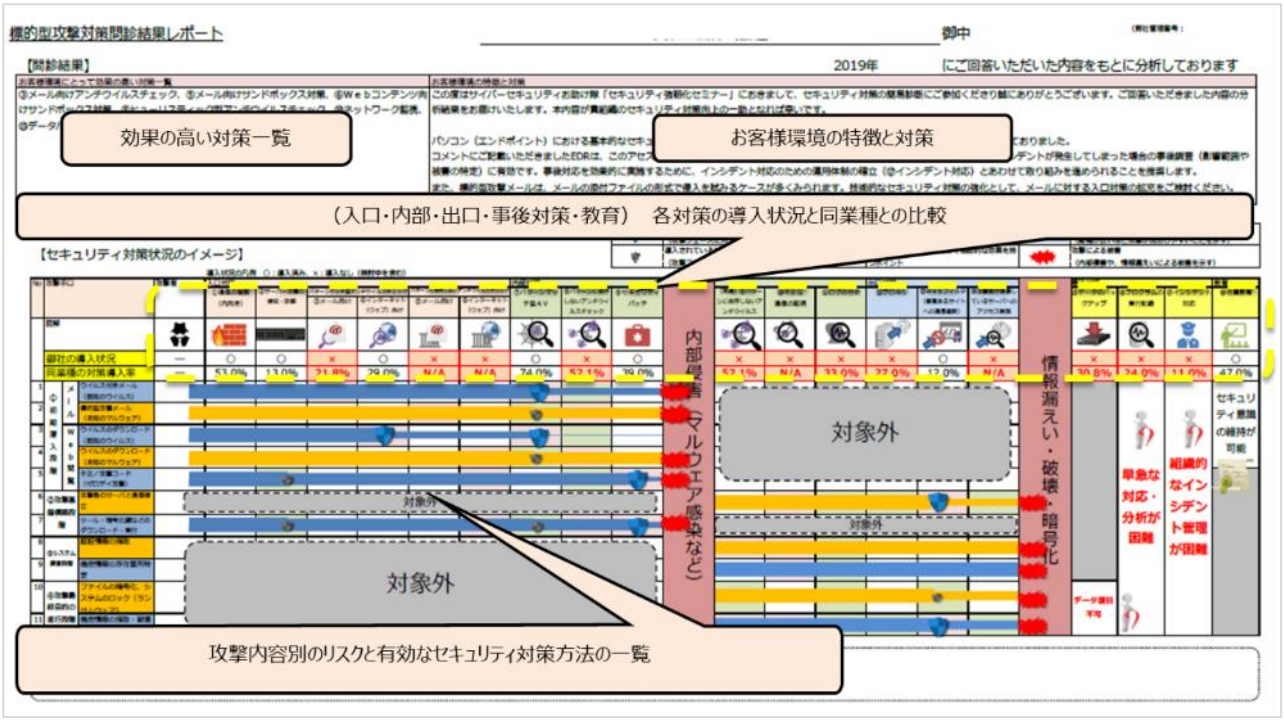


図 5.2 セキュリティ対策の簡易アセスメント診断書

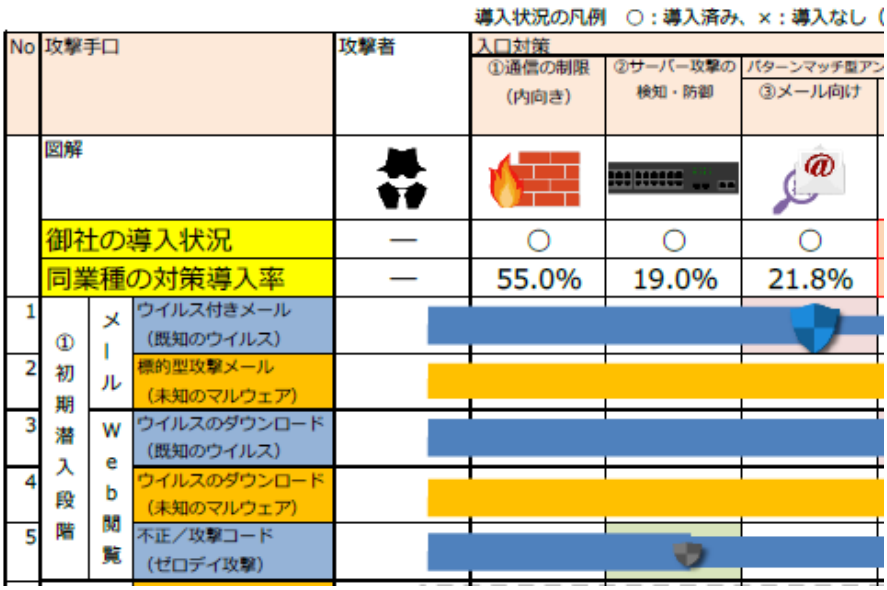


図 5.3 セキュリティ対策の簡易アセスメント診断書（サイバー攻撃の手法別の記載例）

セキュリティ対策の簡易アセスメントを実施した結果の活用と中小企業の反応を以下に記載する。

- セキュリティ対策の簡易アセスメントの診断結果を実証参加企業 107 社(126 名)へ回答を実施した。セキュリティ対策の簡易アセスメント診断書より対策状況の弱点、および優先すべき対策の可視化を行った。

一部の実証参加企業は、自社の IT 運用を任せている協力ベンダに本診断書の対策内容について実装検討依頼をした。また、更なる詳細な対策方針が知りたいので、現場セキュリティアセスメントを希望された企業もあった。

- セキュリティ対策の簡易アセスメントの結果より、本実証事業で提供するサービス内容の詳細について問い合わせがあり、説明の対応を行った。
- セキュリティ対策の簡易アセスメントを行った 107 社の集計より、情報漏えい等被害と食い止める（出口対策）対策率が低く、特に攻撃者のサーバへのアクセス制御については導入率が 30%を下回っている状況であった。中小企業においては、PC 等であれば攻撃者のサーバへのアクセス制御が可能なウイルス対策製品、および脅威の侵入を防ぐ(入口対策)の機能を合わせ持つ、統合脅威管理装置(UTM)の導入は、コストパフォーマンスがよいため、本事業の監視サービス利用を促進した。
- セキュリティ対策の簡易アセスメント集計結果を事業説明会(中間報告)の報告にて、セキュリティの危機感を覚えたとして、実証参加企業の情報連絡会で、個別に実績報告の説明依頼を受け、説明対応を実施した。その後、当該中小企業の支店においてセキュリティリスクを感じているため、本事業の提供サービスのインターネットの出入り口の監視サービス、エンドポイント監視サービスの導入にてリスクの可視化の支援を行った。

  監視結果は、即時情報漏えいにつながるような、インシデントは検知されなかったが、脆弱性を持つ通信を約３万件／月検知した。また、脆弱性を持つ通信の対応についての改善提案（該当機器のファームウェアの更新、および脆弱性のない通信プロトコルに対応した機器への入替検討依頼）を実施した。

  実証参加企業の反応としては、リスクの可視化、および改善依頼を受けたこともあり本実証参加に意義があったとの感想をいただいている。

5.1.2. 現場セキュリティアセスメントによる支援

現場セキュリティアセスメントは、専任コンサルタントの中小企業へ訪問し、標的型攻撃による情報流出に対するセキュリティ上のリスクについて①セキュリティ対策の実施状況、②セキュリティインシデント監視・運用の実施状況、③セキュリティポリシ・ルールの確立状況について約 90 問のアセスメント項目の対面インタビュー、および内容により現地の実機の確認を実施した。

項	項目	内容
1	目的（ねらい）	現場でヒアリングによりセキュリティ対策の簡易アセスメント結果とのギャップの抽出し、対策案をご説明することにより、必要なセキュリティ対策の意識付けを図る。
2	実施内容	・専任コンサルタントの訪問により対策実施状況のアセスメントを実施した。 ①セキュリティ対策の実施状況 ②セキュリティインシデント監視・運用の実施状況 ③セキュリティポリシ・ルールの確立状況
3	実施結果	・実証参加企業　9 社にて実施 指摘内容例:（セキュリティ対策の簡易アセスメント：内部対策 OK：インシデント対応 NG） ・（内部対策）全 PC アカウントが Administrator 権限で設定、ファイルサーバのアクセス権が不適切。 →部門責任者と部門ユーザの権限を分けるなど、アカウント権限を管理する。 ・（インシデント対応）インシデント発生時の対応内容が明確でない。 →エスカレーションフローの作成、関係者の連絡先と連絡方法の整備。

表 5.2 現場セキュリティアセスメント概要

セキュリティ対策の簡易アセスメントの診断結果ではよい結果であったが、現場セキュリティアセスメントを実施した結果、危険度の高い不具合が複数の企業で見つかった。

- 入口対策としてインターネット（Web サイト）へのアクセス時にユーザ認証などのアクセス制限が適用されていないため組織内部へ侵入したマルウェアが実施する攻撃者の準備したサーバへ接続するために実施する通信（コネクトバック通信）を食い止めることができず、マルウェア感染を起こすリスクがあった。
- 内部対策としては、全 PC アカウントが Administrator 権限で設定かつパスワードが同一の値で設定されているおり、マルウェアによって一旦 Administrator アカウントのパスワードが奪取された場合、マルウェアによる被害の拡大を食い止めることが困難な状況となるリスクがあった。
- 出口対策では、ファイルサーバのアクセス権が適切に設定されておらず、かつ、重要な情報に対するファイル単位の表示制限や暗号化などのセキュリティ制限についても実施されていなかった。マルウェアや攻撃者によって情報の窃取が試みられた際に、被害が広範囲となるリスクが大きい状況となっていた。

- 人的・組織的対応としては、セキュリティインシデント発生時の対応内容が明確になっていない、一部の運用を除き、セキュリティポリシ、セキュリティスタンダードなどに相当する組織内の規程が存在していない企業が複数あった。
- インシデント対応としては、エスカレーションフロー（インシデントが起こった時の対応方針）の作成ができていない、関係者の連絡先、連絡手段などが明文化されていなかった。

  対応内容の明確化、エスカレーションフロー等の整備できていないことにより、サイバーインシデント発生時の対応が遅れる事が懸念される。

これらの対応においては、SECURITY ACTION セキュリティ対策自己宣言の推進によりポリシーの整備を実施していくことが有効であると考える。

セキュリティ対策の簡易アセスメント結果からのギャップとしては、データのバックアップは実施済みだが、現場セキュリティアセスメント時の調査では、サーバ（ファイルサーバ等）のバックアップは適切に取得されているものの、バックアップの世代管理が行われていない、また、クライアント PC 上に保存されたデータの管理がされていない企業が多数で見られマルウェア感染時等の回復に時間を要すことが懸念される。また、セキュリティ対策の簡易アセスメント結果からインシデント対応ができているが、現場セキュリティアセスメント時の調査では、エスカレーションフローの作成ができていない、関係者の連絡先、連絡手段などが明文化されていないことも見られサイバーインシデント発生時の対応が遅れる事が懸念される。

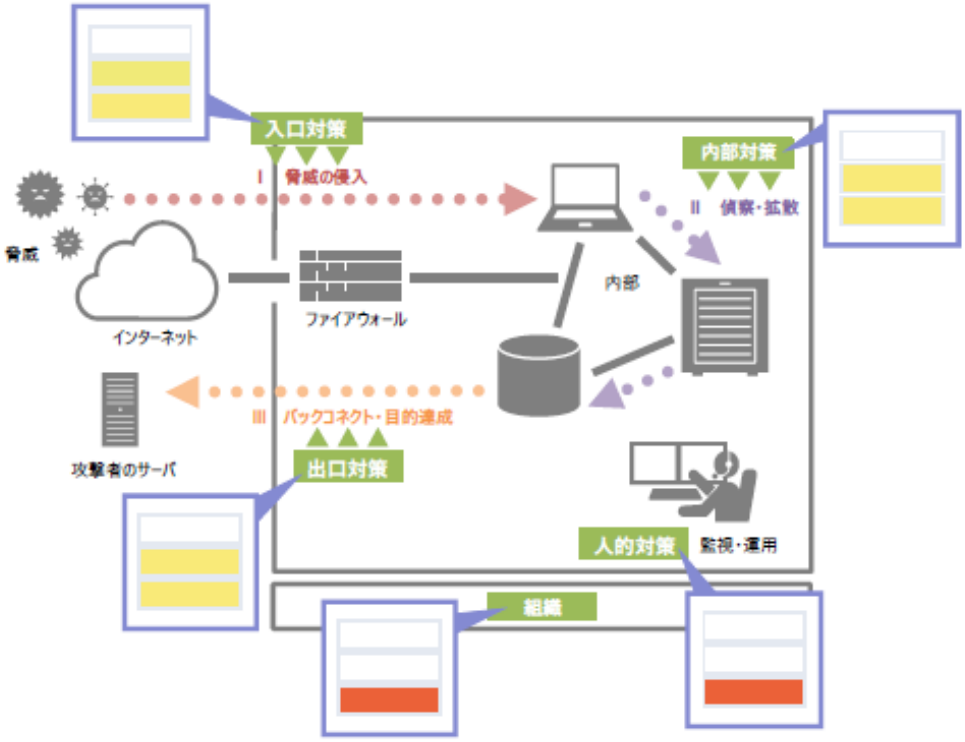
現場アセスメントでの確認事項（観点）と不具合内容の指摘について下記に記載する。

項	項目	確認観点	確認項目数	不具合件数	指摘不具合内容
1	メール環境	・スパムメールに対する対策の実施状況 ・マルウェアに対する対策の実施状況	7	5	・パターンマッチに依存しないアンチウィルスの対策が実施できていない。
2	インターネット閲覧環境	・インターネット閲覧時におけるアクセス制限の実施状況 ・マルウェアに対する対策の実施状況 ・ブラウザのセキュリティ設定の実施状況	6	6	・ウェブのアクセス先に関する制御は行われていない。 ・業務上の必要性の有無にかかわらずインターネットアクセスが可能な環境である。
3	エンドポイント	・外部記録メディアに対するセキュリティ設定の実施状況 ・マルウェアに対する対策の実施状況 ・セキュリティパッチの適用状況 ・アカウントと権限の割り当て状況 ・パスワード管理の実施状況	11	9	・ユーザが利用するアカウントとして管理者権限が割り当てられている。 ・クライアント PC の管理者アカウントのパスワードにすべて同一の値が設定されている。 ・ネットワークに接続していない PC のセキュリティ対策ができていない。（アンチウィルスソフト導入もなし） ・パターンマッチに依存しないアンチウィルス

					ソフトウェアの導入がされていない。 ・USBデバイスの利用を制御（管理）できていない。 ・タブレットのセキュリティ対策がされていない。 ・古いパソコンでないと動かないソフトウェアがあり、サポート切れOSや30年前のPC等が稼働している。
4	インフラ・ネットワーク	・インターネット等の外部接続ポイントの管理状況 ・ネットワークレベルでのアクセス制御の実施状況 ・セキュリティパッチの適用状況 ・アカウントと権限の割り当て状況 ・アクセスログ・操作ログの記録と保管の状況	34	5	・ファイルサーバのアクセス権の設定が不適切に設定されている。（ファイル・ディレクトリに対するアクセス権の設定） ・インターネット等の外部接続ポイントの管理ができていない。
5	運用	・アクセスログ・操作ログの分析状況 ・インシデント対応体制と手順の整備状況 ・脆弱性の発見と評価の方法	11	9	・セキュリティインシデント発生時の対応内容が明確化されていない。 ・クライアントPCのアンチウィルスソフトウェアの動作状況の管理がなされていない。 ・インシデント対応フロー等の整備が行われていない。 ・サーバやUTM等のログは取得しているが監視はできていない。 ・ログ情報の記録はしているが、確認ができていない。（解析不可含む）。 ・UTM導入しているが運用として実施が必要な内容がわからない。 ・サーバ（ファイルサーバ等）のバックアップは適切に取得されているものの、バックアップの世代管理が行われていない、また、クライアントPC上に保存されたデータの管理がされていない。
6	組織	・セキュリティポリシ等の整備・運用状況 ・標的型攻撃メールに対する教育の実施状況・	20	6	・セキュリティ教育を実施していない。 ・会社として利用して良いクラウドサービスの基準を作成ができていない。 ・セキュリティポリシが明文化されていない。
合計			89	40	—

表 5.3 現場アセスメントでの確認事項（観点）と不具合内容

現場アセスメントの結果報告した、現場セキュリティアセスメント診断書の例を以下に記載する。



〔凡例〕

：セキュリティ対策が実施されており、リスクが低い状態

：セキュリティ対策の実施内容、または範囲に問題が見られる状態

：セキュリティ対策が不十分であり、リスクが高い状態

セキュリティリスク：

組織内部にマルウェアが持ち込まれる（メール添付ファイルや USB などの外部接続デバイス、ユーザによるソフトウェアインストールなど）リスクが高い状況です。また、インターネット（Web サイト）へのアクセス時にユーザ認証などのアクセス制限が適用されていないため、組織内部へ侵入したマルウェアが実施するコネクトバック通信[1]を食い止めることができず、マルウェア感染による実害を防ぐことができない恐れがあります。

代替案：

クライアント PC やサーバなどに導入されているアンチウイルスソフトウェアの稼働状況/シグネチャの更新ステータス/感染駆除通知などについて、管理者が集中管理できる仕組みの導入を推奨します。また、Active Directory や資産管理

図 5.4 現場セキュリティアセスメント診断書（一部抜粋）

5.1.3. インターネット出入り口の監視サービス(UTM)による支援

項	項目	内容
1	目的（ねらい）	・セキュリティインシデントの実態の把握 ・セキュリティ対策を現場に導入する際の問題点の抽出
2	実施内容	・現地のネットワーク上に統合脅威管理装置(UTM)の導入にてインシデント の監視を実施。
3	実施結果	・実証参加企業　10 社に導入 ①　インシデント件数 ・平均　約 67 件/日・社 主な内容:メール通信に対する既知の脆弱性を不正利用する試み ・駆けつけ支援が必要なインシデントは発生 0 件 ②導入時の問題点 ・実証参加企業にてネットワーク構成、利用アプリケーションの把握が正しくできていない （構成情報なし）。ヒアリングのみでは導入計画の策定が困難、 現地での構成調査が必要となったケースがあった。

表 5.4 インターネット出入り口の監視サービス(UTM)概要

中小企業の 100 人以下の企業については自社のインターネット、社内ネットワークの構成情報を把握していないケースが多く、ネットワーク構成図や、外部サービスの利用、利用サービスの所在もわからないケースやネットワーク運用等を外注している中小企業については外注ベンダへの確認が必要になり構成把握までに時間を要した。

統合脅威管理装置(UTM)の導入時はネットワーク構成、利用アプリケーションをヒアリングシートに実証参加企業で記入していただき機器を準備していたが、ヒアリングの回答が十分に得られないケースが発生した。その中でもネットワーク構成図がないケースが多く、そのために個別にメール、および電話で情報を入手し、その内容を基にネットワーク構成案を図式化して情報共有化、可視化を行う支援を実施した。

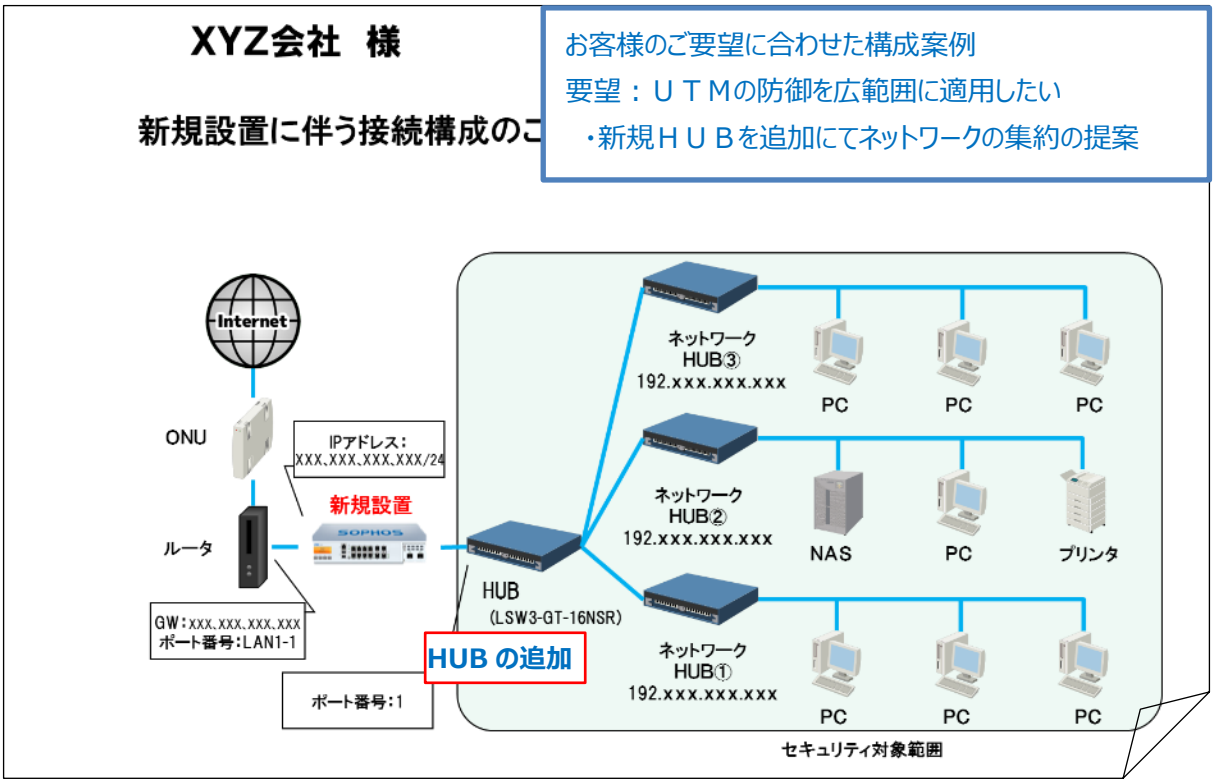
また、実証参加企業の個別要望事項（例、機械系ネットワークへ影響させないために実証の範囲より除外したい）、保護範囲が幅広くなるようなネットワーク構成案を数点提示した。

これにより、ネットワーク上の 統合脅威管理装置(UTM)の導入ポイントを決定までのスピードアップを図った。

統合脅威管理装置(UTM)の導入においては、ネットワーク技術者が、実証参加企業先に訪問しネットワーク構成を調査しないと、導入できない中小企業もあったため、個別にネットワークアセスメントを行った。

統合脅威管理装置(UTM)などの機器設置が必要な場合は、個別にネットワークアセスメント等の事前導入コンサルサービスの提供が必要と考える。

以下にネットワーク構成の図式化した提案書の例を以下に記載する。



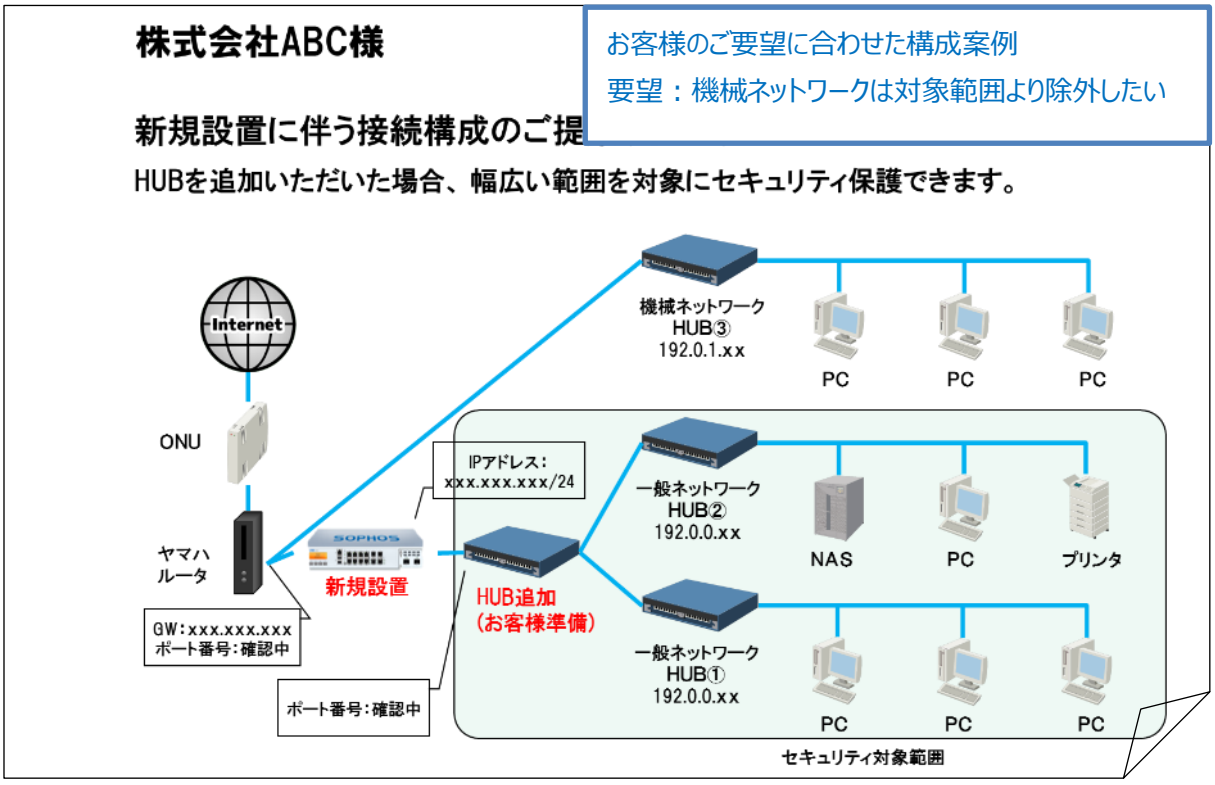


図　5.5 ネットワーク構成図提案書

インターネット出入り口の監視サービスでは以下の月次レポートを実証参加企業へメールにて送付した。記載内容は、あまりネットワークやセキュリティの知識がない方でもわかりやすいようにシンプルな形式とした。レポート内容は、高度な脅威検出数(ATP※3検知)、攻撃検出数(IPSでの検知)、マルウェア検知（サンドボックス実行での検知含む）、検出数グラフ、コメントに攻撃等の詳細情報を記載した。

※3 ATP：Advanced Persistent Threat、持続的標的型攻撃

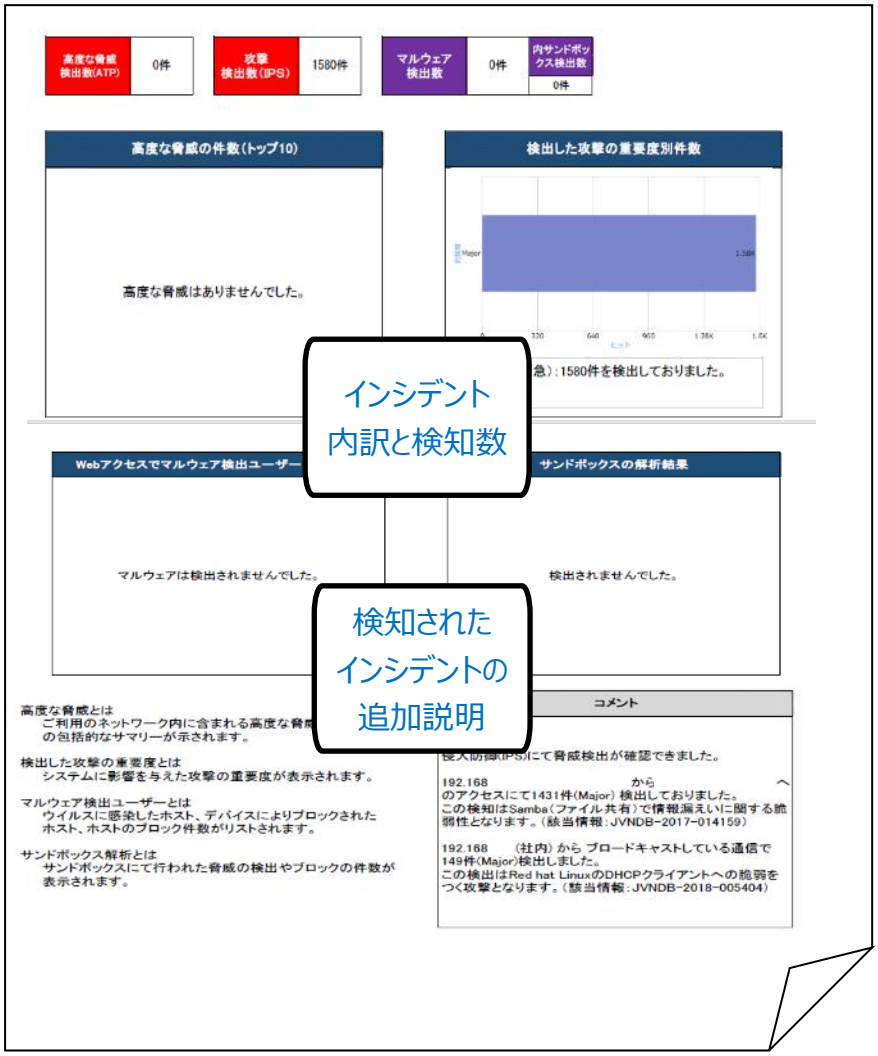


図 5.6 インターネット出入り口の監視サービス月次レポート例

統合脅威管理装置(UTM)では、高度な脅威検出数(ATP検知)を情報漏えい対象インシデントとして実証参加企業の緊急連絡、リモートでの調査、および必要に応じ現地駆けつけによる切り分け支援を行うこととしているが、現地駆けつけによる支援は発生しなかった。

ただし、月次レポート内容に脆弱性の検知数が異常に多いもの、検知にてパケットドロップが多いものについては実証参加企業へ業務への影響の有無、内容のご説明、および改善案の提示を以下のように実施した。

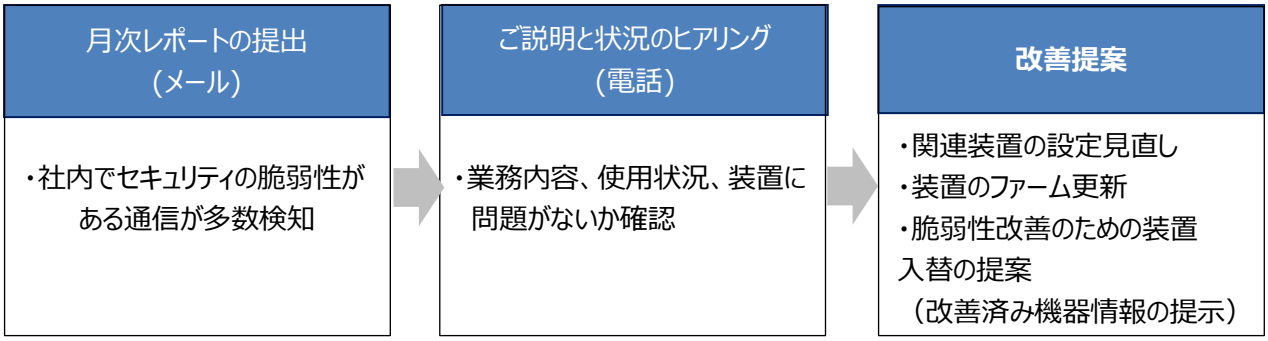


図 5.7 インターネット出入り口の監視サービスの支援内容と改善提案

- 対応事例

本レポート内容（図 5.8 月次レポート報告内容 参照）より、NAS と PC 間のファイル共有にて SMB1.0 での脆弱性がある旨をお伝えし、NAS 側での改善方針のご提案を実施した。

＜月次レポート内容より＞

侵入防御(IPS)にて脅威検出が確認できました。 PC(社内) から NAS(社内) へのアクセスにて 1431 件(Major) 検出しておりました。この検知は Samba（ファイル共有）で情報漏えいに関する脆弱性となります。（該当情報：JVNDB-2017-014159）ルータ(社内) から ブロードキャストしている通信で 149 件(Major)検出しました。この検出は Red hat Linux の DHCP クライアントへの脆弱をつく攻撃となります。（該当情報：JVNDB-2018-005404）

図 5.8 月次レポート報告内容

5.1.4. エンドポイント監視サービスによる支援

項	項目	内容
1	目的（ねらい）	・セキュリティインシデントの実態。 ・セキュリティ対策を現場に導入する際の問題点の抽出
2	実施内容	・現地の PC にエンドポイントでの検出と対応用ソフトウェア(EDR)導入によりセキュリティインシデントの監視を実施した。
3	実施結果	・実証参加企業　13 社に導入。 ①インシデント件数 ・アドウェア検知　2 件 駆けつけ支援が必要なインシデントは発生　0 件 ②導入時の問題点 ・実証参加企業にて、利用アプリケーションを正しく把握できていない。 導入後にチューニングが必要な場合があった。 （例）導入後の状況確認（電話問診）で「Firefox の動作が少し重くなった」、「PDF の表示が遅くなった」

表 5.5 エンドポイント監視サービス支援概要

サービス導入後の企業に対して、安定稼働の支援として、通報やログに現れない現象がないか、使用感はどうか等の確認をメール、および電話で実施した。

対応事例として、エンドポイント監視サービス使用の実証参加企業において、「Firefox の動作が少し重くなった」、「PDF の表示が遅くなった」とのご申告があり個別チューニングを実施し解決を図った。

5.2. セキュリティ監視の内容と実績

- インターネット出入り口の監視サービスの統合脅威管理装置(UTM)で検出したイベントを下記に記載する。(期間：2019/9/25~2020/1/31)

いずれも脆弱性の通信、情報漏えいにつながる検知でないと判断し、現地駆けつけにいたるインシデントではなかった。

ただし、1 社で多くの脆弱性の通信がある場合は個別の連絡を実施し、改善策の提案を行った。

項	検知メッセージ	件数	解説
1	FILE-IMAGE libpng chunk decompression integer overflow attempt	Detect 3	Google Chrome で使用されていた libpng の整数オーバーフローを起こす 脆弱性を検出。
2	FILE-IMAGE Microsoft Windows Media Player Malformed PNG detected Iccp overflow attempt	Drop 3	ファイルイメージ Microsoft Windows Media Player の不正な PNG が iTXt オーバーフローの試行を検出しパケットを廃棄。
3	FILE-IMAGE Microsoft Windows Media Player Malformed PNG detected zTXt overflow attempt	Detect 8	ファイルイメージ Microsoft Windows Media Player の不正な PNG が zTXt オーバーフローの試行を検出。
4	FILE-OFFICE Microsoft Windows Image File Handling Information Disclosure	Drop 15	Windows 画像ファイル処理情報漏えいの脆弱性を検出しパケットを廃棄。
5	FILE-PDF Adobe Acrobat file extension overflow attempt	Detect 3	FILE-PDF Adobe Acrobat、および Adobe Acrobat Reader U3D RHAdobeMeta バッファオーバーフローの試みを検出。
6	SERVER-MAIL Dovecot Submission-Login Service NULL Pointer Dereference	Detect 1,938	サーバに対するsubmission-login サービスの NULL ポインターの逆参照の脆弱性を不正利用する試みを検出。
7	SERVER-SAMBA Samba write andx command memory leak attempt	Drop 1	SERVER-SAMBA Samba 書き込み andx コマンドのメモリリークの試行を検出。
8	SERVER-SAMBA Samba Writeable Share Insecure Library Loading	Detect 13	Samba の既知の脆弱性を不正利用する試みを検出。

項	検知メッセージ	件数	解説
9	SERVER-WEBAPP TRUFFLEHUNTER TALOS-2018-0703 attack attempt	Drop 5	SERVER-WEBAPP TRUFFLEHUNTER TALOS-2017-0428 攻撃の試みを検出しパケットを廃棄。
10	OS-LINUX Red Hat NetworkManager CVE-2018-1111 DHCP Command Inject	Detect 823	DHCP client が NetworkManager に提供しているスクリプトに脆弱性を検出。
11	SERVER-SAMBA Samba write andx command memory leak attempt	Detect 45,007	Samba の既知の脆弱性を不正利用する試みを検出しパケット廃棄。
12	BROWSER-IE Microsoft Internet Explorer address bar spoofing without scripting	Detect 1	Microsoft Internet Explorer で、リモート攻撃者がアドレスバーをスプーフィングして、無効な URI を使用する脆弱性を検出。CVE-2004-2219
13	FILE-IMAGE Microsoft Windows Media Player Malformed PNG detected sPLT overflow attempt	Detect 1	ファイルイメージ Microsoft Windows Media Player の不正な PNG が sPLT オーバーフローの試行を検出。 CVE-2006-0025
14	FILE-OTHER ClamAV MEW PE file integer overflow attempt	Detect 1	ClamAV 0.92 より前の libclamav 整数オーバーフローにより、MEW 圧縮 PE ファイルを介してヒープベースのバッファオーバーフローの試行を検出。 CVE-2007-6335
15	OS-WINDOWS Microsoft Windows DHCP client Options parsing buffer overflow attempt	Detect 89	Microsoft Windows DHCP クライアントのバッファオーバーフローを悪用する試行を検出。
16	OS-WINDOWS name query overflow attempt UDP	Detect 150	WINDOWS 名前クエリオーバーフローを悪用する試行を検出。 CVE-2003-0825
合計		48,061	

表 5.6 統合脅威管理装置(UTM)の検出したイベント

- エンドポイント監視サービスで検出したイベントを下記に記載する。

(期間：2019/9/25~2020/1/31)

エンドポイント監視での検出は 2 件、いずれもアドウェアと判断され現地駆けつけにいたるインシデントはなかった。

項	検知メッセージ	件数	解説
1	検出名：W32.Gen:Adware.19hb.1201 重要度：中 外部への通信：なし 判定：悪性（低） 検体情報： ファイル名：PandoraRecovery-26575194[.]exe	Detect 1	VirusTotal では検出率：25/57 となっており、多くのベンダで不要なアプリケーションもしくはアドウェアとして判定。 本検体は Pandora Recovery というゴミ箱から削除されたファイルを復元するフリーソフトのツールと推測される。
2	検出名：PUA.Win.File.Generic::231444.in02 重要度：中 外部への通信：なし 判定：悪性（低） 検体情報： ファイル名：Thunderbird Setup 68.3.1.exe[.]part	Detect 1	今回検出されている対象は Thunderbird のインストーラーにバンドルされているファイル（内部ファイル）と推測される。 Thunderbird のインストーラーに脅威の情報は見受けられませんでしたが、バンドルされているファイル（内部ファイル）は VirusTotal では 16/70 のベンダが不要なアプリケーションもしくはアドウェア等の判定をしていることから、悪性が低いと評価。本検体が Firefox から Download フォルダに生成されていることから、ユーザにより手動で取得したものと考えられます。

表 5.7 エンドポイント監視サービスの検出したイベント

6. 実証結果を踏まえた検討の実施

6.1. 中小企業サイバーセキュリティ支援に必要な人材スキル

セキュリティ対策の簡易アセスメントからは、パソコン上の基礎となるセキュリティ対策（アンチウィルス、パッチ）の実施率が高い。ただし、未知のウイルス検知を行うパターンに依存しないアンチウィルスの導入は低いとの内容より考察されることとしては、セキュリティ対策、およびその必要性の認知度の低さが一因となっている。

また、よろず相談の内容、現場セキュリティアセスメントからも、セキュリティ製品が「どのようなインシデントに対応するのか」 「どのような対策を行えばよいのかわからない」との声も聴かれる。これについては、セキュリティ対策実装の相談窓口や、コンサルが有効と考える。

以下に、中小企業の声より必要なサービスを図 6.1 中小企業の声からの必要なサービスに記載する。

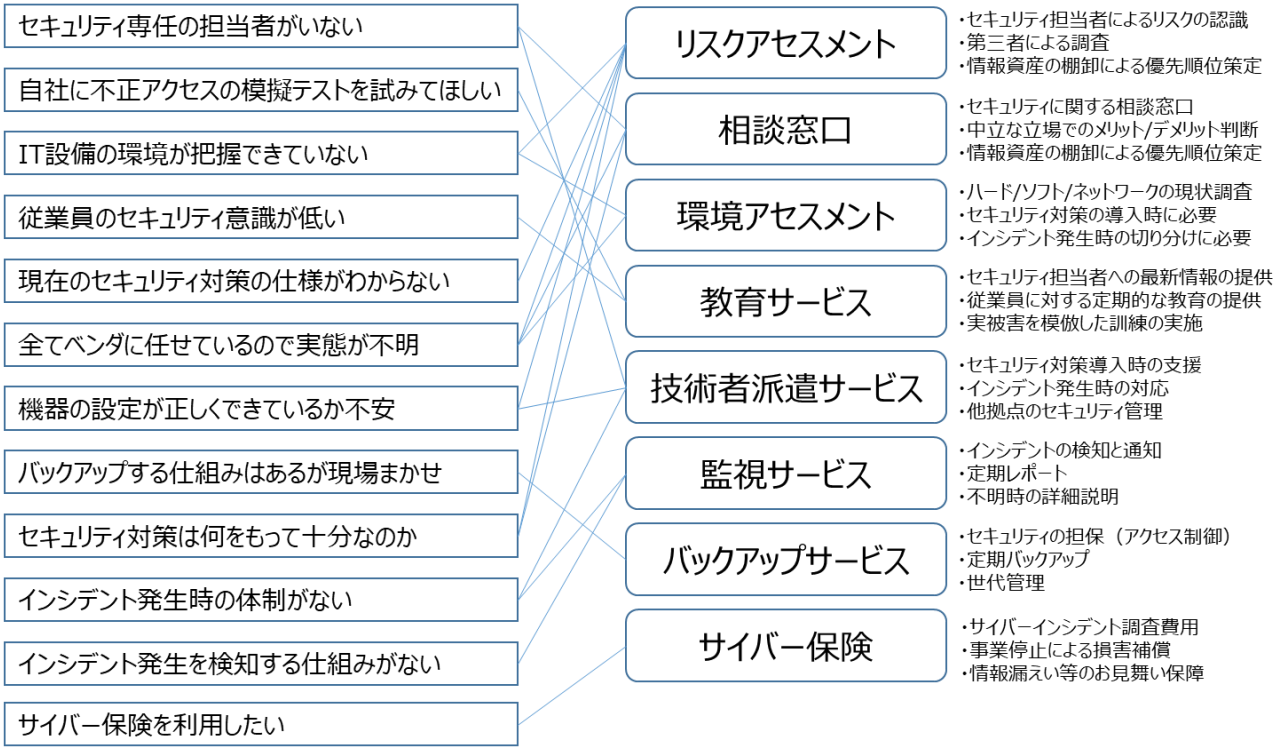


図 6.1 中小企業の声からの必要なサービス

6.2. 実証終了後のサービス提供の検討

6.2.1. サイバーセキュリティ支援サービス関連

本実証で得た情報では、総合脅威管理装置(ＵＴＭ)等のネットワーク機器をセキュリティ対策機器として導入する場合、ネットワークの環境、利用アプリケーション等の情報が必要となるが、実証参加企業でこれらの情報が管理されていない状況が伺えた。

また、セキュリティ対策の簡易アセスメントでは情報の流出を防ぐ(出口対策)の実装状況が芳しくない。特にPCのアンチウィルス送付の導入は進んでいるが、未知のウイルスに対応できる製品を利用している中小企業はまだ少なく、セキュリティ製品の機能を知らないことも一要因として考えられる。

（1） セキュリティに対応できる要員配置

アンケート分析より「わからない・無回答」を除いた有効回答65社のうち、対応できる要員を配置できている先は約半分の38社のみであった。従業員300名超の企業でも、要員配置ができていない先が多く（有効回答7社中5社）、企業規模に関わらず中小企業では態勢整備が十分に進んでいないことが分かる。セキュリティの対策要員を配置している中小企業は36%（「社員に対策要員がいる」+「外注（ベンダ）に依頼」の合計）であり、セキュリティ対策の普及にはセキュリティ対策の知識と実装できる技術の底上げが必要と考える。

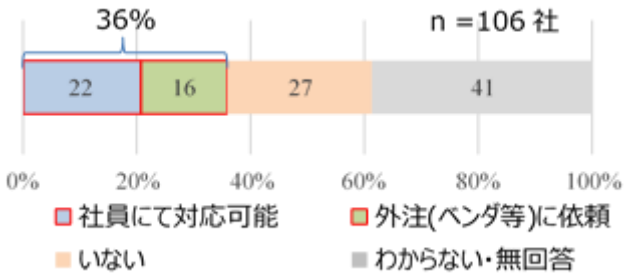


図 6.2 セキュリティ対応要員の要否（全体）

（2） 取引先からのサイバーセキュリティ対策の調査依頼または改善依頼

「わからない・無回答」を除いた有効回答（50 社）のうち、約 3 割（16 社）の企業が何かしらの依頼があったと回答している。

近年大きな脅威となっているサプライチェーンの弱点を悪用した攻撃への備えとして、企業の経営者は自社のみならず、ビジネスパートナーを含めたサプライチェーン全体での対策が求められていることから、取引先からの要請といった動きは今後さらに顕著になってくることが予想される。これにより、取引先からの調査、対策依頼がある場合対応要員の確保や社員の育成が課題になると考える。

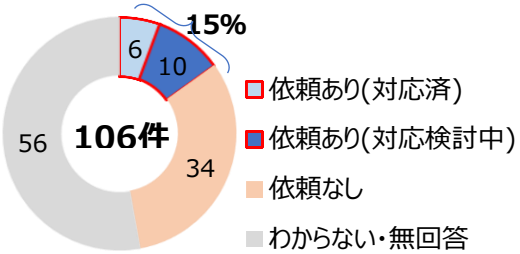


図 6.3 セキュリティ対策の調査依頼・改善依頼

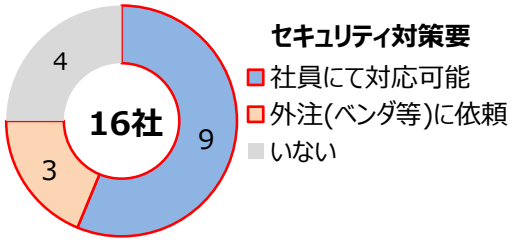


図 6.4 対策依頼あり時のセキュリティ対応要員の要否

（3） 今後利用したいセキュリティサービス

無回答を除いた有効回答 74 社のうち、半数以上（41 社）の企業がインシデント発生後の除去・回復支援サービスに関心を示している。

意識醸成ならびに態勢整備が進んでおらず有事対応に不安が大きい中小企業においては、相談窓口等の平時対応に関するサービスよりも、緊急時の対応へのニーズが高いことがわかる。

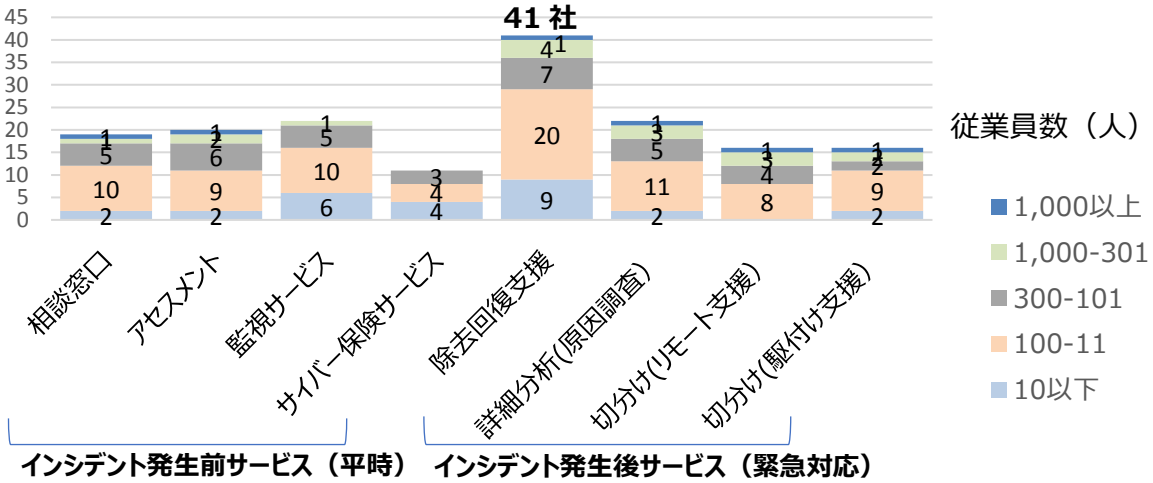


図 6.5 サイバーセキュリティ関連の利用したいサービス

また、よろず相談でも聞こえてきた声として「社員のセキュリティ意識の向上が難しい」との意見には、教育ツール、e ラーニング、疑似体験サービス（例：標的型攻撃メール訓練）なども有効と考える。

「どのようなインシデントに対応するのか」「どのような対策を行えばよいのかわからない」「ネットワーク等の環境管理が十分でない」という、中小企業の実態を踏まえ、IT ベンダの人材には、セキュリティ対策の製品知識と実装できる技術、および現場のネットワーク調査の支援ができる技術が、必要なスキルと考える。したがって、IT シルバー人材の活用を考えるときにも、同様なスキル(セキュリティ対策の製品知識と実装できる技術等)を有していることが望ましい。

（4）サイバーセキュリティ対策製品の導入時の課題

本実証を通して、中小企業に向けたサイバーセキュリティ対策製品を効率よく、また的確に導入普及させるためにはセキュリティ対策の導入前に、現状を調査するサービスにてお客様環境の可視化をする必要があると考える。

今回の UTM 導入時の確認では、製造機器、情報系機器が同一 LAN に混在している企業もあった。今後が Society5.0、Connected Industries が実現する社会が浸透していくと、情報系のプロトコルのみでは対応できない状況や、製造機器への影響なども考慮してセキュリティ対策機器の導入が必要と考える。

これらの情報の可視化ができると、セキュリティ対策機器等が安全かつスムーズに導入が可能となり、安価な形で提供できるサービスを検討する必要があると考える。

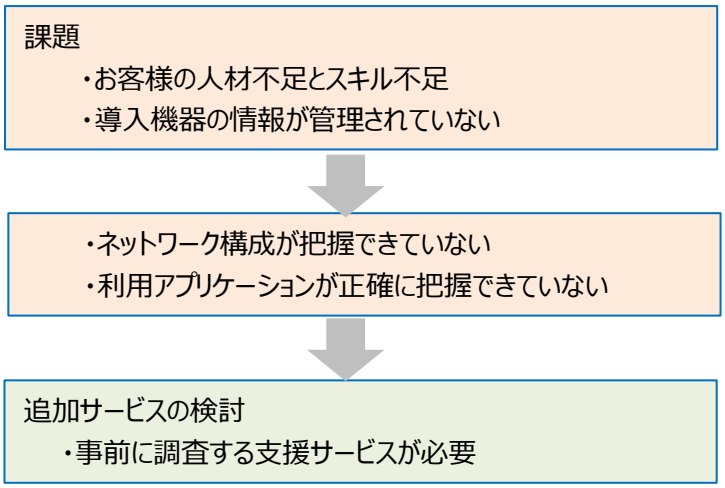


図 6.6 課題と追加サービス検討

6.2.2. サイバー保険のあり方検討

本実証事業の参加企業に対して実施した各種アンケートおよびセキュリティアセスメントの結果から、中小企業のサイバー攻撃への対策状況の実態に即したサイバー保険、およびセキュリティサービスについて検討を行った。

6.2.2.1. 中小企業の実態と保険検討の方向性

本実証事業の参加企業に対して実施した各種アンケート、およびセキュリティ対策の簡易アセスメントの結果から、中小企業のサイバー攻撃への対策状況の実態に即したサイバー保険、およびセキュリティサービスについて検討を行った。

アンケートを通して得られた中小企業のサイバーセキュリティ対策への関心・意識の実態から、サイバー保険の加入・普及におけるポイントや課題を整理し、今後の検討に向けた方向性について考察を行った。

（1） セキュリティに対応できる要員配置

「わからない・無回答」を除いた有効回答 65 社のうち、対応できる要員を配置できている先は約半分の 38 社のみであった（表 6.2 サイバーセキュリティに対応できる要員配置の状況）。

従業員 300 名超の企業でも、要員配置ができていない先が多く（有効回答 7 社中 5 社）、企業規模に関わらず中小企業では態勢整備が十分に進んでいないことが分かる。

《保険加入・普及におけるポイント》

サイバーセキュリティに関わる平時の対策、さらにはインシデント発生時の事後対応を行うには、担当者を配置した組織・体制だけでなく、様々な状況に対応できるように、予算手当を含む態勢整備が必須であり、中小企業におけるサイバー保険では、その観点からのサポート機能について潜在的なニーズがあると推察される。

従業員数	社数	割合
従業員1,000名以上	4社	4%
300名超　1,000名未満	10社	9%
100名超　300名未満	23社	22%
10名超　100名未満	53社	50%
10名以下	16社	15%
無効回答	0社	-
合計：	106社	100%

表 6.1 従業員数規模

要員配置状況	社数	割合
あり（社員にて対応可能）	22社	34%
あり（ベンダ等に外注）	16社	25%
なし（要員不在）	27社	41%
わからない・無回答	41社	-
合計：	106社	100%

表 6.2 サイバーセキュリティに対応できる要員配置の状況

（2） サイバーセキュリティ対策に対する社内での意識・認知

「わからない・無回答」を除いた有効回答（66 社）のうち、半数以上（39 社）が意識醸成できていないと回答している（表 6.3 サイバーセキュリティ対策に対する社内での意識・認知）。特に、サイバーセキュリティに対応できる要員配置ができていない企業（27 社）のうち約７割（18 社）が意識醸成できていないと回答している。中小企業においては、意識醸成が十分にできていないことが、要員配置を含めてサイバーセキュリティ対策への適切な投資を妨げており、サイバーセキュリティ対策を進める上での大きな障害になっていると考えられる。

《保険加入・普及におけるポイント》

意識醸成が不十分である企業は、サイバー保険を含めた事後対応の観点からのセキュリティ対策に対する投資意欲やコスト受容度についても低いと推測されることからも、サイバー保険の普及には、補償範囲や保険料水準並びに付帯サービスといった保険設計の観点だけでなく、如何に保険の必要性を訴求するか、そのアプローチやプロモーションにおける工夫も必要であると考えられる。

対策に対する意識・認知	社数	割合
十分できている	7社	11%
不十分だができている	20社	30%
できていない（不十分）	39社	59%
わからない・無回答	40社	-
合計：	106社	100%

表 6.3 サイバーセキュリティ対策に対する社内での意識・認知

（3） 取引先からのサイバーセキュリティ対策の調査依頼または改善依頼

「わからない・無回答」を除いた有効回答（50 社）のうち、約３割（16 社）の企業が何かしらの依頼があったと回答している（表 6.4 取引先からの調査依頼または改善依頼）。

近年大きな脅威となっているサプライチェーンの弱点を悪用した攻撃への備えとして、企業の経営者は自社のみならず、ビジネスパートナーを含めたサプライチェーン全体での対策が求められていることから、取引先からの要請といった動きは今後さらに顕著になってくることが予想される。

《保険加入・普及におけるポイント》

その動きを受け、保険スキームの観点でも、上位サプライヤーがグループ会社間や取引先間の経済損失連鎖の回避を目的として、サプライチェーン全体を包括的にカバーするような加入方式が今後普及していく可能性もある。このような包括加入方式を推進する場合、例えば、保険会社がサプライヤーに求めるセキュリティガイドラインと併せて、セキュリティサービス・機器等の導入推奨の一環として保険加入を促すというアプローチも効果的だが、一般的に中小企業の多くは複数のサプライチェーンで取引を行っているため、補償の重複や保険料コストの負担が過度に大きくならないような、より合理的な加入スキームを構築することが課題となる。

一方、多くの中小企業は多様な商流の中で様々なサプライチェーンを構成していることから、十分なセキュリティ対策を講ずることや、自社の業務領域の全てを網羅するようサイバー保険を手配することについて、特定のサプライチェーンに依存することなく、中小企業が自立的に対応することが本来望ましい形と言える。

また、調査・改善の依頼元である取引先からは、通常、その調査・改善の結果としてのセキュリティ対策状況などを明らかにすることが求められることから、保険加入の証左として取引先に提示できる証明書の発行や、セキュリティ対策状況の簡易診断サービスによる診断レポートの提供といった付帯サービスのニーズも高まってくる可能性がある。

実際に、今回のアンケートでは SECURITY ACTION 宣言済み企業は「一つ星」「二つ星」合わせて 9 社にとどまっているが、実施予定と回答した企業が 44 社もあり、今後の取引先からの要請増加の動きを受けて企業における取り組みが進んでいくものと思われる。

取引先からの調査・改善	社数	割合
依頼あり（対応済）	6社	12%
依頼あり（対応検討中）	10社	20%
依頼なし	34社	68%
わからない・無回答	56社	-
合計：	106社	100%

表 6.4 取引先からの調査依頼または改善依頼

6.2.2.2. 中小企業のセキュリティ対策状況と保険検討の方向性

アンケート、およびセキュリティ対策の簡易アセスメントを通して得られた現在のサイバーセキュリティ対策の状況から、サイバー保険に求められる加入・普及におけるポイントや課題を整理し、今後の検討に向けた方向性について考察を行った。

中小企業におけるセキュリティ対策の状況においては次のような課題や傾向がみられる。

（1） セキュリティ対策の導入状況

入口対策・内部対策と比較して、出口対策への対応が遅れている

（表 6.5 現在導入しているセキュリティ対策・複数回答可）。

日々高度化・巧妙化が進むサイバー攻撃に対して、入口対策や内部対策だけでは不十分であることは明らかである。しかし、セキュリティ予算が潤沢ではなく、専任の担当者が不在であるケースが多い中小企業においては、メール対策や Web 対策など多様なセキュリティを導入・運用し、多層防御の態勢を構築することは極めて困難であると考えられる。

そのため、中小企業においては、FW（ファイアウォール）や AV（アンチウィルス）といった複数の機能を統合したUTMが運用管理の負荷やコストの観点からも非常に有効なサービスであると考えられるが、未導入企業において UTM 等を検討している先は 2 割にも満たない状況である。

《保険加入・普及におけるポイント》

サイバー保険は、基本的にはインシデント発生後の事後対応をサポートするものであり、攻撃者から狙われにくくするための入口対策や脅威を早期に検知・防御するための内部対策および出口対策を企業が積極的に講ずることが前提となっている。

中小企業が平時、および緊急時双方の対策を総合的・包括的に検討することができるよう、UTM 等のセキュリティサービスを導入している場合にサイバー保険で大幅な割引を適用する、セキュリティサービスにサイバー保険を自動的にセットするなど、相乗効果を促進するような保険の設計や加入スキームの検討が期待される。

導入しているセキュリティ対策（導入率：高）	社数	割合
【入口】攻撃の検知・防御（FW等）	72社	67%
【入口】パターンマッチ型AV（メール）	65社	61%
【内部】パターンマッチ型AV	85社	79%
【内部】セキュリティパッチ適用	88社	82%
ヒアリング社数：	107社	

導入しているセキュリティ対策（導入率：低）	社数	割合
【出口】プロキシ	23社	21%
【出口】攻撃者のサーバへのアクセス制御	22社	21%
ヒアリング社数：	107社	

表 6.5 現在導入しているセキュリティ対策（複数回答可）

（2） 今後利用したいセキュリティサービス

無回答を除いた有効回答 74 社のうち、半数以上（41 社）の企業がインシデント発生後の除去・回復支援サービスに関心を示している（表 6.6 今後利用したいセキュリティサービス・複数回答可）。

意識醸成ならびに態勢整備が進んでおらず有事対応に不安が大きい中小企業においては、相談窓口等の平時対応に関するサービスよりも、緊急時の対応へのニーズが高いことがわかる。

《保険加入・普及におけるポイント》

一般的なサイバー保険では、損害賠償金に対するファイナンス機能だけでなく、インシデント発生時の被害拡大防止のための除去・回復支援や原因究明・影響範囲調査といった緊急対応を支援するサービスも付帯されており、その対応費用も保険でカバーすることができる。

インシデント発生時の対応サービスへのニーズが高いにも関わらず、サイバー保険への関心が低いことについては、付帯サービスの存在、および内容が企業に十分に認知されていないことが考えられるため、今後は、被保険者＝企業にとって分かりやすく、使いやすいサービスといった観点からの利用条件・手順等の見直しを含めた、サイバー保険の普及啓発全般についての施策が必要と考えられる。

利用したいセキュリティ対策（ニーズ：低）	社数	割合
【平時の支援】状況監視（みまもりサービス）	19社	18%
【平時の支援】セキュリティアセスメント（調査）	19社	18%
【平時の支援】サイバーセキュリティ相談窓口	19社	18%
【平時の支援】保険サービス	11社	10%
ヒアリング社数：	106社	

利用したいセキュリティ対策（ニーズ：高）	社数	割合
【緊急時対応】サイバー攻撃の除去・回復支援	41社	39%
ヒアリング社数：	106社	

表 6.6 今後利用したいセキュリティサービス（複数回答可）

（3） 未実施のセキュリティ対策の検討状況

導入率の低いサービスでの未実施理由をみると、ほとんどの企業が「未検討」となっている。これについては、多くのケースで企業が対策やサービスの存在自体を知らない、内容を理解していない状況と推測される

（表 6.7 未実施のセキュリティ対策および検討状況）。

要員不足により企業内の態勢が整備されておらず、自律的な判断が行えていない中小企業においては、機能やコストを理由としてセキュリティ対策の実施を見送ったというケースでも、実際には導入に向けた十分な検討が行われていない可能性も懸念される。

先のアンケートでの「今後利用したいセキュリティサービス」では、セキュリティアセスメントや相談窓口といった平時の支援サービスに対する関心は低かったものの、実際にはセキュリティ対策の策定に向けたコンサルティング実施による企業のリテラシー向上や態勢整備支援がまずは必要であるとも言える。

《保険加入・普及におけるポイント》

サイバー保険の提案にあたっては、保険設計に必要な情報を入手するための告知書の取り付けだけでなく、現在の対策状況を簡易にアセスメントし、推奨されるセキュリティ対策の提案・アドバイスを行えるような仕組みも、企業に対する普及啓発の観点では有効である。

未実施のセキュリティ対策	未導入	うち未検討	未検討割合
【入口】攻撃の検知・防御	29社	17社	59%
【入口】非パターンマッチ型AV（メール）	82社	60社	73%
【入口】非パターンマッチ型AV（ウェブ）	80社	57社	71%
【内部】非パターンマッチ型AV	68社	49社	72%
【内部】不正な通信の監視	76社	49社	64%
【内部】ログの分析	70社	44社	63%
【出口】プロキシ	76社	50社	66%
【出口】Webフィルタリング	53社	35社	66%
【出口】攻撃者のサーバへのアクセス制御	76社	55社	72%
【その他】プログラムの実行記録	65社	46社	71%
【その他】インシデント対応	57社	39社	68%
【その他】社員教育	59社	40社	68%
ヒアリング社数：	107社	107社	

表 6.7 未実施のセキュリティ対策および検討状況

6.2.2.3. 中小企業におけるサイバー保険のあり方

これまでの考察から、中小企業におけるサイバー保険としてのあり方について整理をすると、以下のような観点での検討が必要となる。

（1） 保険加入スキームの観点

サプライチェーン全体でのリスクマネジネントの観点から、上位サプライヤーが包括的にカバーするような加入方式により、合理的な補償内容や保険料が実現できる加入スキームが求められる。この際、多くの中小企業は複数のサプライチェーンを構成しており、サイバー保険に個別に加入する方が、重複加入等が発生せず効率的なケースがあることを踏まえて、最適な加入方式が選択できるようなスキームとすることが望ましい。

また、保険だけでなく、他のセキュリティ対策との相乗効果を図るべく、セキュリティサービス導入時の大幅な割引適用やセキュリティサービスにサイバー保険を自動的にセットして販売するスキームなど、さらに柔軟な保険設計が可能となることを期待したい。

（2） 付帯サービスの観点

中小企業が抱える要員不足による課題への対応策として、緊急時だけでなく平時の対策についても広範囲な提案・アドバイスを行えるようなサポート機能を充実させることが有効である。中小企業はセキュリティ対策に関するリテラシーが、まだ高くないため、ほとんどのサービスが未検討のままとなっていることからも、簡易なアセスメントを行うことで潜在的な保険ニーズの掘り起こしにつながることが期待できる。

また、ニーズの高い、緊急時の除去・回復サービスや原因調査等については、従来の付帯サービスでの対象範囲を拡大するとともに、インシデント発生時において円滑に活用できるような仕組みが求められる。

（3） 普及啓発の観点

セキュリティ対策への意識が低い中小企業に対しては、いかに保険の必要性を訴求するのか、アプローチやプロモーションにおける工夫が必要となる。

また、サイバー保険には既にニーズの高い緊急時の対応サービスが付帯されていることについての認知度が低いため、保険代理店だけでなく関連機関や様々なチャネルを活用した丁寧な普及活動も必要である。

6.2.2.4. 中小企業におけるサイバー保険（検討案）

（1） サイバー保険 サプライチェーン包括加入方式

（保険加入スキームの観点）

- グループ会社・取引先等を保険対象として包括的にカバーすることで、サイバー攻撃の経緯や感染経路等に関わりなく、被害拡散の防止・早期復旧を促すことができる。
- スケールメリットを活かした合理的な保険料を上位サプライヤーが支払うことで、各サプライヤーのコスト負担を軽減する。
- サプライチェーンを構成する中小企業に対しては、付帯サービスとして簡易なリスクアセスメントを実施し、保険だけでなく他のセキュリティ対策の推奨・導入促進を上位サプライヤーと連携して行い、長期的に安定した保険カバーの提供に努める。

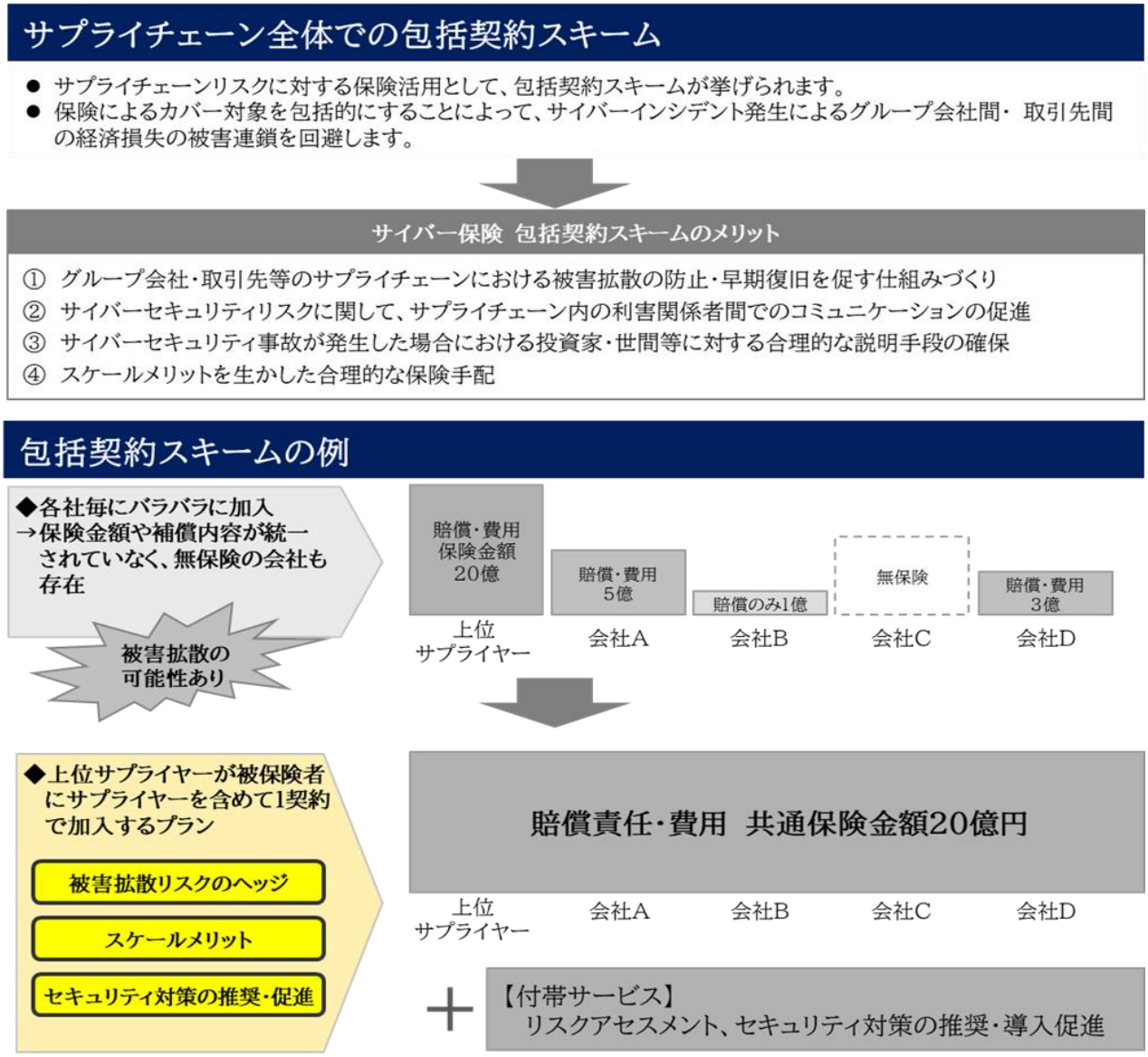


図 6.7 サイバー保険 サプライチェーン包括加入方式

※ 複数のサプライチェーンを構成する中小企業などで、個別加入するサーバ保険がある場合の保険料割引制度など、合理的な保険スキームを検討

（2） 中小企業向けセキュリティサービスへのサイバー保険自動付帯

（保険加入スキーム＋普及啓発の観点）

- 統合脅威管理装置(UTM)やエンドポイント(EDR)等の監視系サービスへサイバー保険を自動的にセットして販売する。
- 監視サービスの機能に連動させることで保険の有無責の判断を早期に行い、同時に付帯サービスの活用をより円滑に行う（インシデント対応をサポートするベンダの手配も含めた迅速な保険対応）。
- 企業の保険料負担はないが補償範囲は限定的なため、いわゆる“自賠責保険”のような位置づけであり、別途通常のサイバー保険加入を促すための導線が必要。

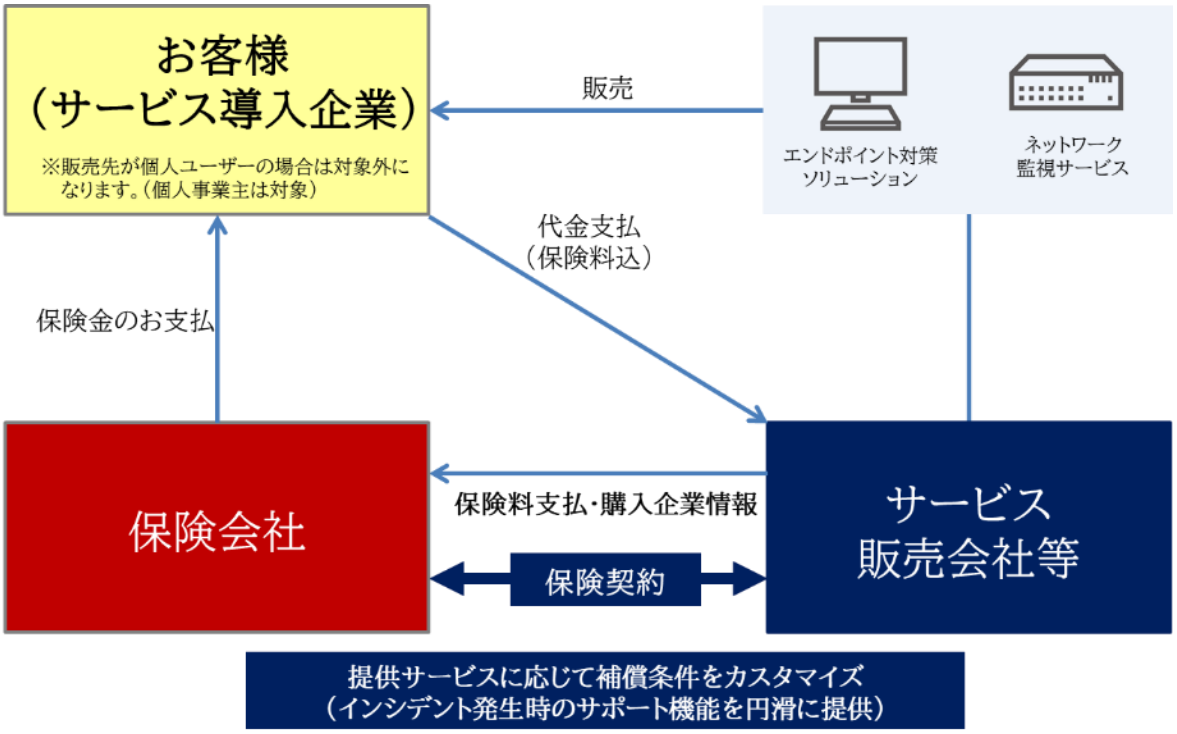


図 6.8 中小企業向けセキュリティサービスへのサイバー保険自動付帯

※ 別途、サイバー保険への個別加入を促すための普及啓発などのアプローチが必要

例）簡易なアセスメントサービスの提供（Web サービス等）

サービス導入企業に対する定期的な保険サービスの案内（メルマガ等）

（3） サイバー保険 付帯サービスの拡充

（付帯サービス＋普及啓発の観点）

- インシデント発生時の対応サービスだけでなく、平時の対策策定に向けた簡易なリスクアセスメントや診断・スコアリングサービス等を提供。
- 緊急時の原因調査やコールセンターの設置、除去・回復等に関わるサービスについては、円滑な初動対応に向けた活用しやすいスキームを構築。

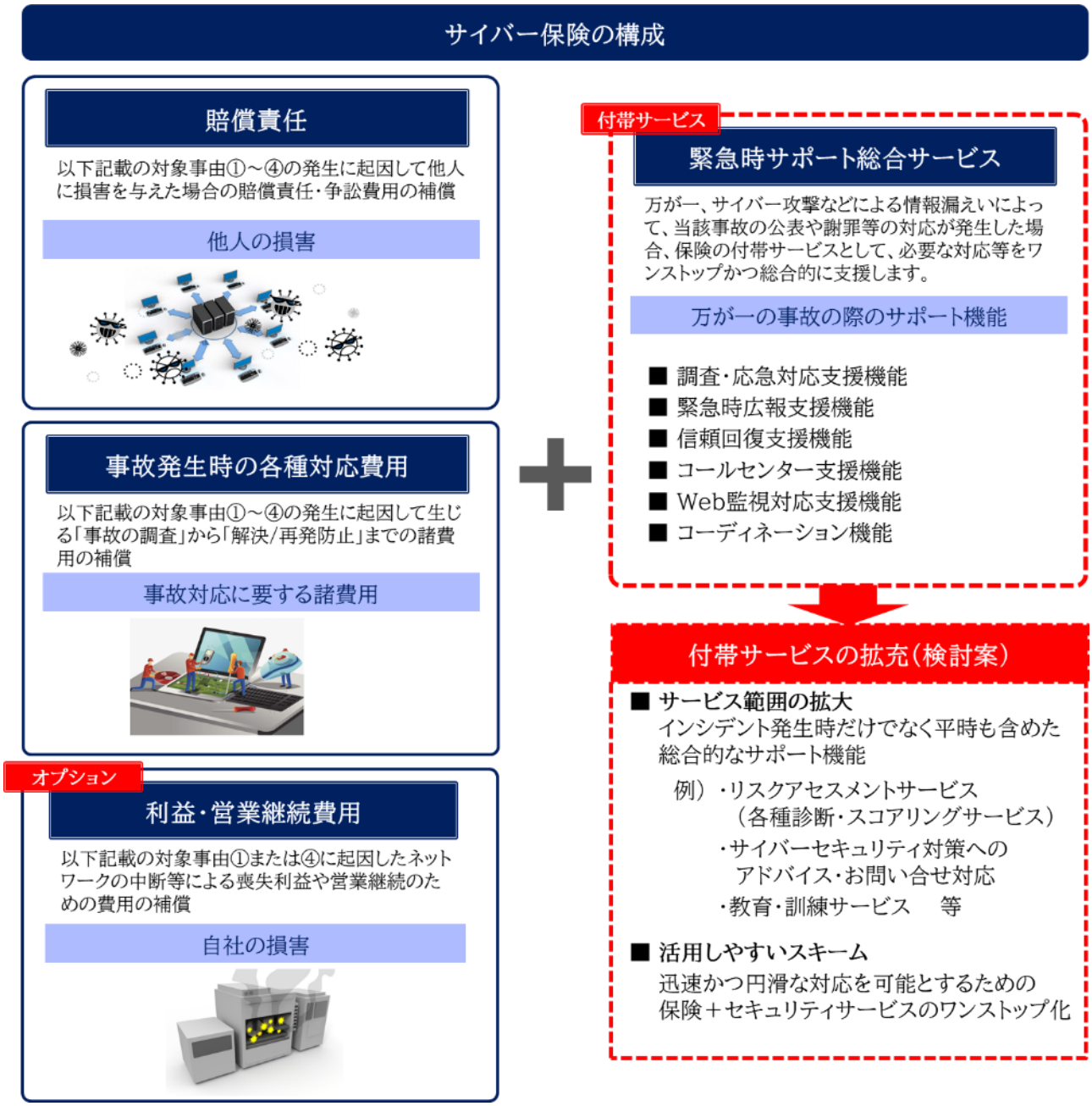


図 6.9 サイバー保険 付帯サービスの拡充

－以上－