令和２年度中小企業サイバーセキュリティ対策支援体制構築事業

（サイバーセキュリティお助け隊事業）

（実証対象：千葉県、埼玉県）

成果報告書

請負事業者：富士ゼロックス株式会社

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

目次

サマリー

本報告書は、富士ゼロックス株式会社（以下「富士ゼロックス」という。）が「令和 2 年度中小企業サイバーセキュリティ対策支援体制構築事業」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

千葉県、埼玉県内の中小企業 60 社を対象に、以下の 4 つのサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- セキュリティ対策機器（UTM）
- 専門家のヒアリング
- セキュリティ診断
- 標的型攻撃メール訓練

1. 背景・目的

本実証事業は、経済産業省と独立行政法人情報処理推進機構（以下「IPA」という。）が主導する、令和 2 年度中小企業サイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）である。中小企業を対象とし、サイバーセキュリティ対策のニーズ、サイバー攻撃による被害の実態等を把握するとともに、中小企業が必要とするサイバーセキュリティ対策支援サービスを検討するための実証事業である。

富士ゼロックスは本実証事業請負事業者として活動したので、以下に実証事業成果を報告する。

1.1 背景

令和 2 年 7 月閣議決定の成長戦略でもフォローアップされているとおり、サイバーセキュリティに対するニーズはさらに高まっている。サイバー犯罪・サイバー攻撃の複雑化・巧妙化や、新型コロナウイルス感染症の影響によるテレワーク、遠隔教育等の増加に伴うリスクの拡大に対応するため、サイバーセキュリティの確保、サイバーセキュリティ協議会の運用の充実・強化、サプライチェーンのリスクに関する技術検証体制の整備、デジタルトランスフォーメーションとサイバーセキュリティの一体的な推進といった必要な取り組みを着実に進める必要がある。さらには、「Society5.0」「Connected Industries」の実現に向け、産業構造、社会環境が大きく変化していく中で、中小企業においても、National Institute of Standards and Technology（以下、NIST）のサイバーセキュリティフレームワーク（以下、CSF）に基づくアプローチが重要になってくると考えられる。

上記の背景を踏まえて、中小企業においても、セキュリティリスクの洗い出し、企業等におけるセキュリティポリシーの策定および対策の実装、企業・業界等における信頼できるサプライチェーンの構築等について検討し、中小企業が自分事として実践・継続改善できるレベルを目指していくことが求められている。

1.2 目的

本年度事業では、昨年度に実施した、中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊事業）の成果を引き継ぎ、中小企業におけるサイバーセキュリティのさらなる意識向上を図るとともに、中小企業が必要とするサイバーセキュリティ対策を浸透・定着させることである。

具体的には「特定・防御・検出・対応・復旧」からなる NIST の CSF をベースに、昨年度事業で重点領域とした「防御・検知」をカバーしつつ、侵入前提のセキュリティ対策として、事前調査にあたる「特定」、およびサイバーレジリエンス「検知・対応・復旧」へ重点をシフトさせること、中小企業の実態やニーズに合致したトータルマネージドセキュリティとしての対策支援サービスへ着地させることを活動目標とした。

2. 実証事業の概要

2.1 実証対象地域の選定

本実証事業の対象地域は、千葉県、埼玉県の 2 県とした。選定理由については下記に示すとおりである。

選定理由

本実証事業では、CSF の全体プロセス「特定・防御・検出・対応・復旧」を対象として、昨年度事業で対象とした部分プロセス「防御・検出」と比べて、幅広い領域に渡る中小企業のセキュリティ対策状況等についての実態把握を目指している。そのため、サイバーセキュリティに対する関心が低い層から高い層の中小企業で実証実験を行うことが望ましく、本事業では千葉県、埼玉県を選定した。個別の選定理由は以下のとおり。

- 千葉県

  - 商業・工業ともに全国トップクラスであり、サイバーセキュリティに対する意識レベル、取り組み状況について、無関心の企業から対策実施中の関心の高い企業まで幅広い層が想定されるため、本実証事業での効果的な地域である。
  - 県下エリアごとに多様な特色がある。例えば、東葛エリアは高い技術力を持つものづくり中小企業・ベンチャー企業や大学等が集まり、東葛テクノプラザ等の産業支援機関を拠点に産学官連携の枠組みを生かした研究開発が盛んである。
  - 昨年度事業で未実施の地域であり、中小企業のサイバーセキュリティに対する意識啓発の観点からも重要な地域である。

- 埼玉県

  - 富士ゼロックスが昨年度事業の担当した地域であり、積極的にサイバーセキュリティへ取り組む企業が一定数存在することが確認されており、千葉県同様に、県下エリアごとに多様な特色がある等、本実証事業で効果的な地域である。
    ※昨年度事業の実証参加企業は本実証事業では対象外とする
  - 昨年度事業を起点にして、地域商工会議所でのセミナー開催等の継続支援が始まっており、実証終了後の自立的な支援サービスの普及展開、および地域連携のあり方を検討する観点からも重要な地域である。

2.2 スケジュール

2.2.1 実証プロセスの流れ

本実証事業は、以下のプロセスで実施した。
Process1. 事業説明会の実施と実証参加企業の募集
Process2. 中小企業のセキュリティ対策等の実態把握
Process3. 中小企業向けセキュリティ対策支援サービスのビジネス化に向けた検討

Process1. 事業説明会の実施と実証参加企業の募集

- 実証参加企業を募集する目的で、各県下で事業説明会を実施。地域の商工会議所等への協力要請、富士ゼロックス販売会社や IT 専門家である地域の IT コーディネーターによる訪問説明等を実施することで、対象地域の中小企業へ広く声掛けを行い、実証参加企業を募集した。

Process2. 中小企業のセキュリティ対策等の実態把握

- セキュリティ機器である Unified Threat Management（以下、UTM）を実証参加企業に設置し、リモートでセキュリティ監視・管理を実施。通信ログデータを収集し、実証参加企業が晒されているサイバー被害等の実態について調査した。また、実証参加企業からの支援要請に応じてコールセンターによるサポート、インシデント時の駆け付け対応等を実施した。
- IT コーディネーターによるヒアリングを実施。実証参加企業のセキュリティ対策状況等の実態について調査した。

Process3. 中小企業向けセキュリティ対策支援サービスのビジネス化に向けた検討

- Process2 における中小企業のセキュリティ対策等の実態把握からセキュリティリスクを洗い出し、中小企業向けのセキュリティ診断、UTM モニタリング等の支援すべき内容について検討した。
- 中小企業のセキュリティリスクの実態や低コストへの期待に合う補償内容を検討するために、インシデント発生時に必要と考えられる初動対応等を基本補償とする保険と、発生の可能性が低く、発生した場合の影響が大きいリスクに対する任意保険の観点から検討した。

2.2.2 活動スケジュール

図 2.2-1 に本実証事業の活動スケジュールを示す。地域実証事業は、2020 年 9 月上旬に開始した事業説明会の募集活動から始まり、UTM モニタリングやヒアリング活動等、2020 年 12 月 31 日まで、約 4 ヶ月実施した（成果報告会は 2021 年 1 月中旬に実施）。実際の活動では、実証参加企業の募集活動を 2020 年 11 月中旬まで実施し、UTM モニタリングは 2020 年 10 月中旬開始と遅延したが、概ね計画通りに活動を進めた。

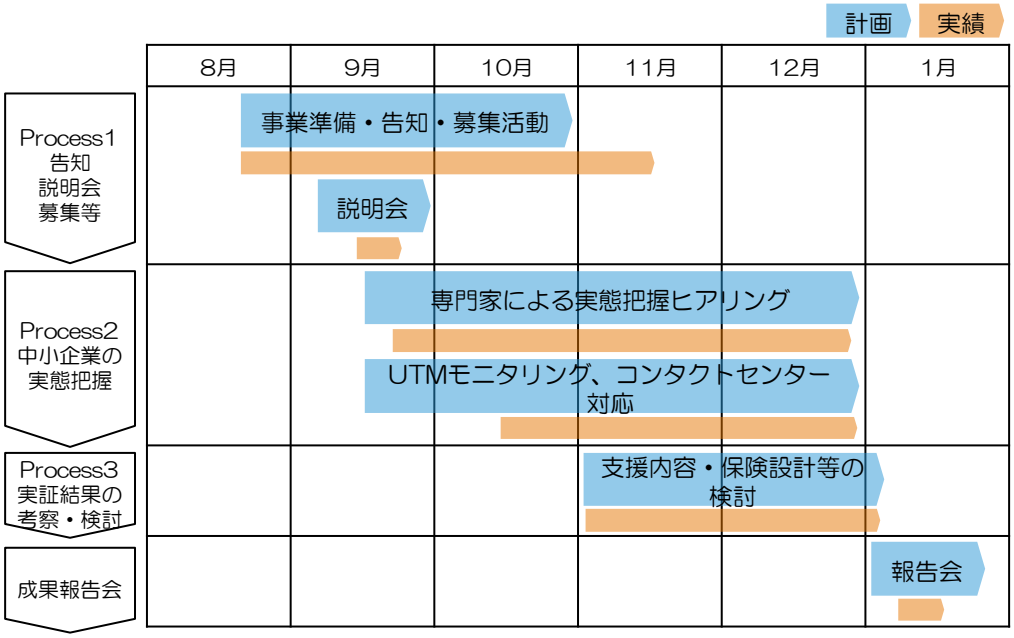

図 2.2- 1　活動スケジュール（計画、実績）

2.2.3 支援体制

図 2.2-2 に支援体制図を示す。本実証事業では、中小企業支援で必要となる 3 つの機能、1）中小企業からの相談受付および対応、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要員を多段階に配置して、発生リスクの内容に応じて対応できる体制とした。

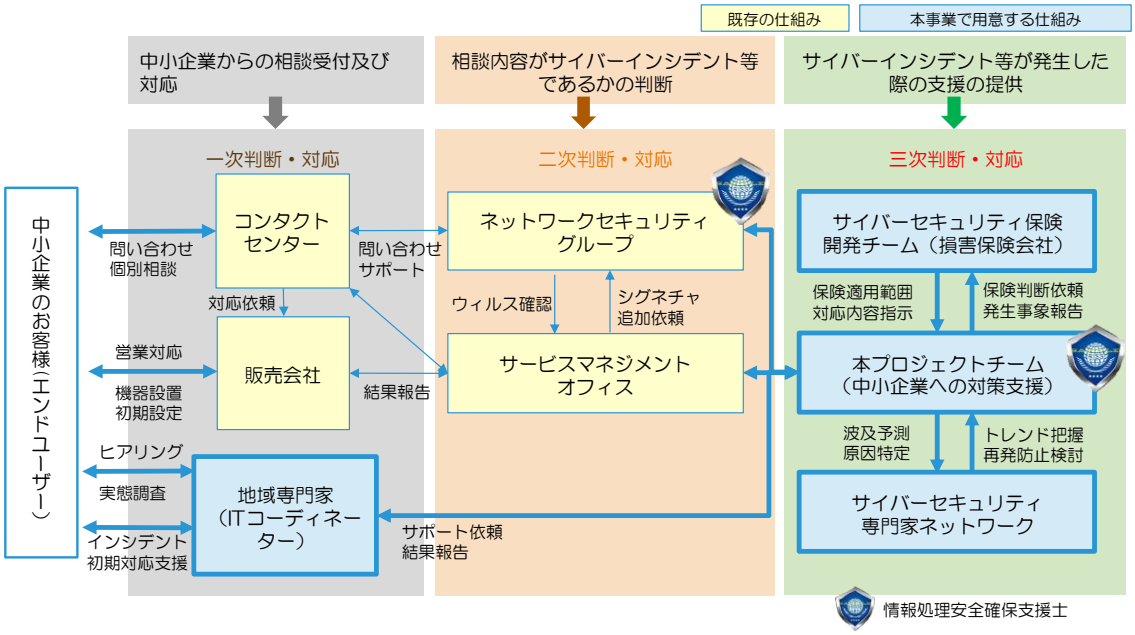

図 2.2- 2　支援体制図

(1) 既存の仕組みを適用

コンタクトセンター、富士ゼロックス各販売会社、ネットワークセキュリティグループ、サービスマネジメントオフィスは、富士ゼロックスが提供している既存サービスの仕組みを適用した。ネットワークセキュリティグループには、情報処理安全確保支援士を配置して、コンタクトセンターと連携して、実証参加企業からの問合せに対応する役割を担わせた。

(2) 本実証事業での独自体制

本プロジェクトチーム、地域専門家（IT コーディネーター）、サイバーセキュリティ保険開発チーム（東京海上日動火災保険）、サイバーセキュリティ専門家ネットワークは、本実証事業のために、新たな体制を組んだ。本プロジェクトチームには情報処理安全確保支援士を配置して、実証参加企業でのサイバー被害等について判定する役割を担った。

2.3 実証参加企業

2.3.1 募集活動

本実証事業では、以下の募集活動を実施した。

・オンライン事業説明会による募集
　※地域の商工会議所からの勧誘を含む（FAX、メルマガ、ホームページによる告知等）
・富士ゼロックス販売会社の営業・カスタマーエンジニア（以下、CE）による個別訪問による勧誘
・富士ゼロックスホームページによる告知
・IPA ホームページによる告知
・地域の IT コーディネーターを通じた勧誘
・本実証事業で協力関係にある損害保険会社（東京海上日動火災保険）を通じた勧誘
・サプライチェーンのコア企業からの紹介によるサプライヤーへの勧誘

オンライン事業説明会への参加企業は少なく、中小企業のサイバーセキュリティに対する意識はまだ低いといえる。昨年度事業の経験を踏まえて、富士ゼロックス販売会社の担当者や地域の IT コーディネーターを通じて追加アプローチを実施、丁寧な説明により、中小企業ごとの心配事や不明点等の不安を解消し、実証事業参加数を増やすことができた。実証参加企業の目標数 50 社に対し、最終的に、実証参加申込企業は 82 社、実証参加企業は 60 社に達した。

実証参加企業数（目標）	実証参加企業数（実績）
50 社	60 社 達成率：120%

表 2.3- 1　実証参加企業数

9～12 月の実証参加企業数の推移を図 2.3-1 に示す。申込後に UTM が設置できないことが分かり、参加に至らなかった企業については 3.2.1 で記述する。

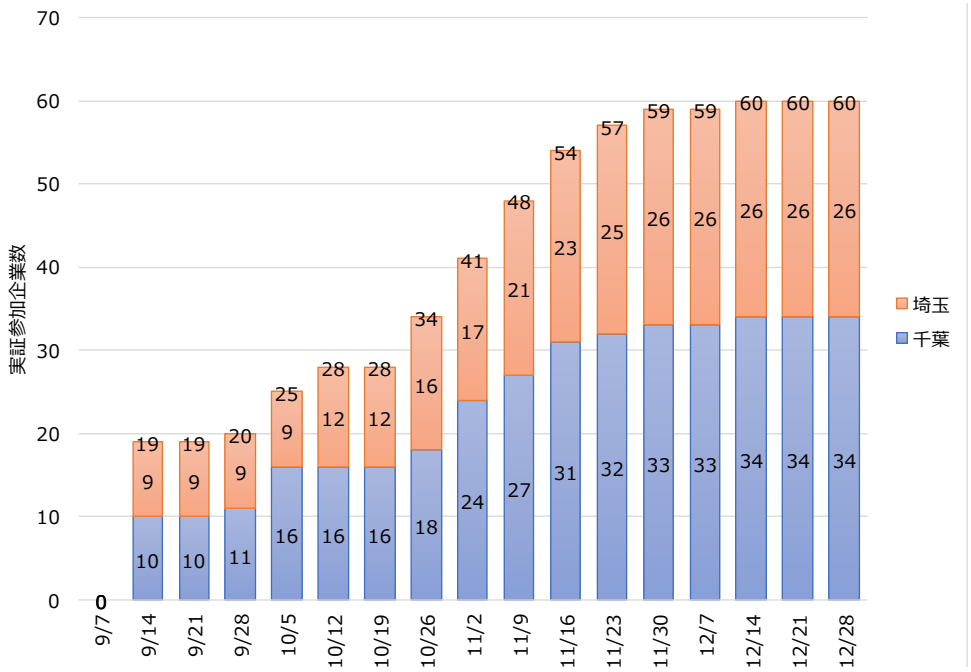

図 2.3- 1　実証参加企業数の推移

2.3.2 実証参加企業の属性情報

実証参加企業の属性情報について以下に示す。実証企業を地域別に見ると、千葉県 34 社、埼玉県 26 件である。従業員数別では約 3 割の 21 社が従業員数 10 名以下の小規模事業者である。また業種別では、製造業と建設業合わせて半数の 30 社となっている。その他の属性については以下のとおりである。

地域	（社）
千葉県	34
埼玉県	26
計	60

表 2.3- 2　地域

従業員数	（社）
1～5 人	16
6～10 人	5
11～20 人	10
21～50 人	22
51～100 人	6
101～200 人	1
計	60

表 2.3- 3　従業員数

正社員の割合	（社）
10%以下	1
30%以下	7
50%以下	7
70%以下	8
70%を超える	30
無回答	7
計	60

表 2.3- 4　正社員の割合

業種	（社）
製造業	16
建設業	14
サービス業	10
卸売業，小売業	3
医療，福祉	3
分類不能の産業	3
情報通信業	2
金融業，保険業	2
不動産業，物品賃貸業	2
教育，学習支援業	2
学術研究，専門・技術サービス業	1
複合サービス事業	1
生活関連サービス業，娯楽業	1
計	60

表 2.3- 5　業種

資本金	（社）
1000 万円以下	28
5000 万円以下	19
1 億円以下	4
3 億円以下	1
なし	2
不明	6
計	60

表 2.3- 6　資本金

売上高	（社）
1000 万円以下	6
1 億円以下	15
10 億円以下	25
100 億円以下	7
無回答	7
計	60

表 2.3- 7　売上高

拠点数（国内）	（社）
1 箇所	35
10 箇所以下	18
無回答	7
計	60

表 2.3- 8　拠点数（国内）

拠点数（海外）	（社）
0 箇所	51
10 箇所以下	2
無回答	7
計	60

表 2.3- 9　拠点数（海外）

2.4 実施内容

2.4.1 UTM モニタリングによる実態把握

UTM モニタリングの概要について表 2.4-1 に示す。

調査目的	中小企業におけるサイバー攻撃被害等の実態把握
調査手法	実証参加企業に UTM 端末を設置し、調査期間中に収集したログ情報を分析する
調査対象	36 台
調査期間	2020/10/16 ～ 2020/12/31　※UTM 端末ごとに調査開始日は異なる
調査項目	外部からの不正アクセス検知および防御 内部不正プログラム検知および防御 不正サイトへのアクセスブロック マルウェアの検知および無害化 スパムメールの検知

表 2.4- 1　UTM モニタリングの概要

(1) 使用する UTM 端末

本実証事業で使用した富士ゼロックスの商品・サービスである“beat”について記載する。強固なセキュリティ機能とアウトソーシングによる運用管理でワンストップサービスを提供できる、同商品・サービスは、中小企業向けに国内で開発製造されたものであり、既に国内の中小企業に多数採用されている。

1) UTM の監視機能

ハードウェア機能：
ファイアウォール、ゲートウェイ型アンチウイルス、クライアント用アンチウイルス、IPS（不正な通信対策）、迷惑メール判定機能、Web フィルタリング等
サービス機能：
ウイルスチェック用定義ファイル、不正アクセス対策用パッチ、新バージョンのプログラム等のセキュリティ自動アップデート等

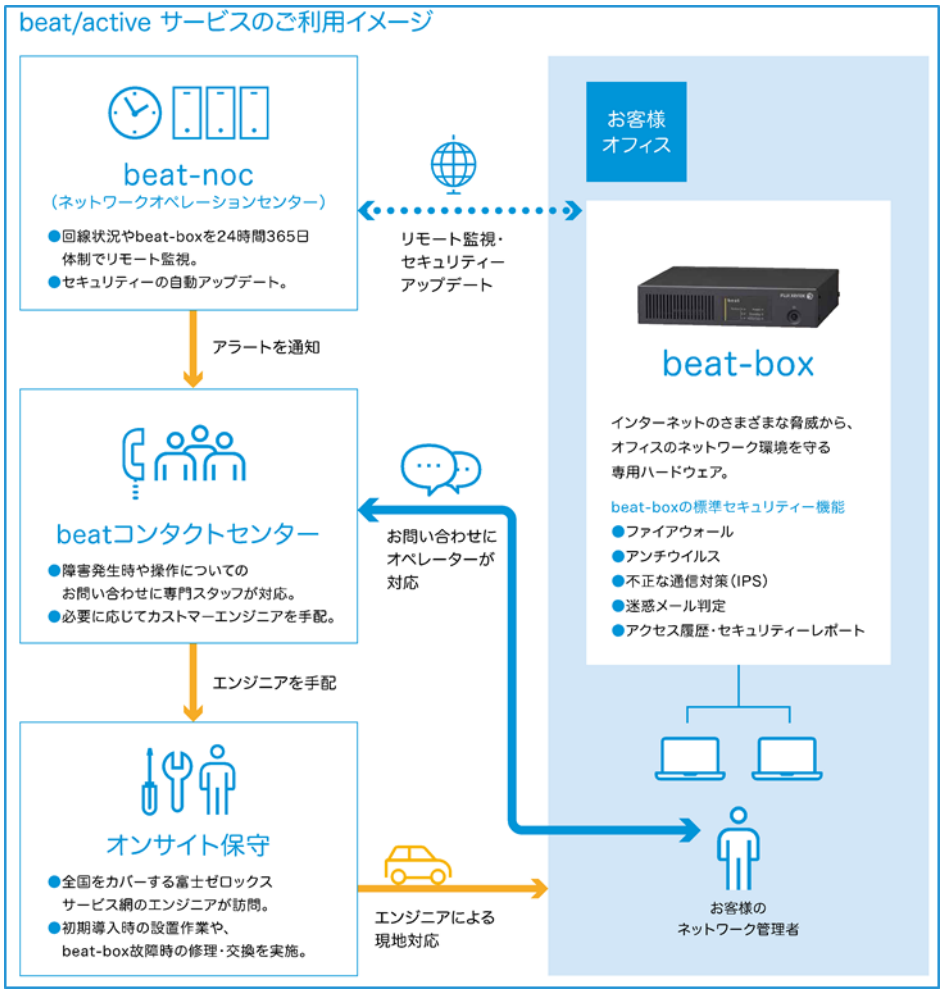

図 2.4- 1　UTM が提供するセキュリティ機能（利用イメージ）

2) 監視レポートの配信

UTM 端末の監視機能により収集したデータ結果を集計・分析し、グラフ等で可視化したレポートを実証参加企業に提供した。

3) エンドポイント管理機能

beat のオプション機能であるエンドポイント管理機能を提供した。ネットワーク上にあるパソコン等の情報資産の管理実態について調査した。

(2) インシデント処理

下表 2.4-2 に、インシデント発生時の一次措置を示した。富士ゼロックス UTM 端末は、ポート完全遮蔽により不正通信がブロックされるため、被害拡散を防ぐことができる。

リスク項目	監視対象	対応	判断基準
外部からの不正アクセス	外→内の ping/port-scan	遮断	外側起点（インターネット上のサーバーから通信が開始されるもの）はすべて遮断する
			LAN 側からインターネット上のサーバーにアクセスし、その応答として戻ってくる通信は遮断しない
不正な通信（IPS:不正侵入防止システム）	不正な通信の有無、禁止アプリケーションのパケットの有無	遮断 記録	不正な通信は、シグネチャごとにログに残しておき、（シグネチャが検出する）パケットの種類、誤検知の可能性等を総合的に判断することで危険性を判断、以後の不正な通信に関しては遮断する措置をとる
			禁止アプリケーションについても遮断する。管理画面から個別設定も可能
ウイルス・スパイウェア	HTTP・FTP、受信メール、送信メールに含まれるウイルスの有無	遮断	ウイルスとして検知された HTTP・FTP、受信メール、送信メールをすべて遮断する。ウイルスのパターンファイルは、インターネット上の管理サーバーから入手し、端末側で自動更新している
スパムメール	スパムメールの有無	遮断 通知	スパムメールであることを示すタグを付けて通過（振り分けはメーラーで実施する前提）させる設定。スパムメール判定には、信頼ある他社製エンジンを使用し、メールのヘッダ情報から総合的に判断している
			スパムメールと判定されかつ添付ファイルが付いているメールは遮断する
禁止指定サイトへのアクセス	コンテンツフィルタの履歴ログ	遮断	禁止指定のカテゴリのサイトを遮断する。どのカテゴリを遮断するかの設定については、お客様側の管理画面で指定する

表 2.4- 2　インシデント対応の一次措置

二次措置は（下図 2.4-2）、Network Operation Center（以下、NOC）とコンタクトセンターが連携対処する。NOC は、ウイルス検知アラート、更新変更エラー等、通常稼働とは異なる状態を判断した場合、コンタクトセンターへ通知する。コンタクトセンターは、実証企業へ電話連絡等で状況報告し、被害状況の把握、障害の切り分け、復旧に向けた支援を実施する。

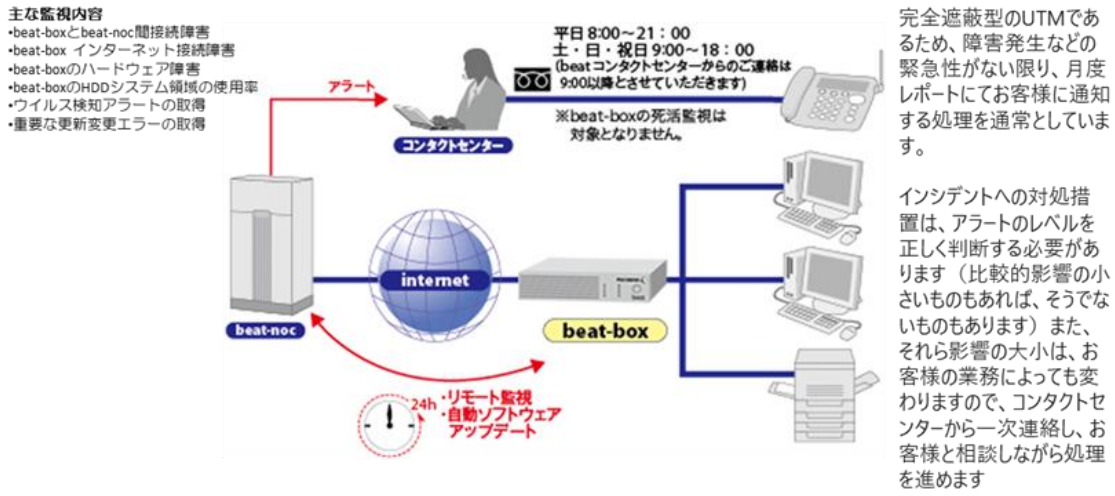

図 2.4- 2　インシデント対応の流れ

(3) モニタリング項目

本実証事業で実施したモニタリング項目は以下のとおり。

- 外部からの不正アクセス検知および防御

  外部からの不正アクセス通信を検知・遮断し、バッファーオーバーフローや SQL インジェクション等のソフトウェアやネットワークの脆弱性を突いた攻撃を防御

- 内部不正プログラム検知および防御

  ボットネットとの通信等、マルウェア感染等による内部から外部への不正通信や不正プログラムが含まれる通信を検知、感染を早期発見し防御

- 不正サイトへのアクセスブロック

  内部端末から、予め登録したセキュリティ上のリスクがある不正サイトへの接続をブロック（URL フィルタリング）

- マルウェアの検知および無害化

  メール添付ファイルや Web からのダウンロードファイルに含まれるウイルス、ランサムウェア、アドウェア等の検知と無害化

- スパムメールの検知

  受信したメールに含まれるスパムメールの検知

2.4.2 専門家のヒアリングによる実態把握

専門家によるヒアリング概要を表 2.4-3 に示す。

調査目的	中小企業におけるサイバーセキュリティ対策状況等の実態把握
調査手法	実証参加企業に専門家によるヒアリングを実施し、集計結果を分析する
調査対象	54 社
調査期間	2020/9/29 ～ 2020/12/31　※ヒアリング回数は企業により 1～2 回
調査項目	企業情報 情報セキュリティ対策レベルの数値化 セキュリティ対策状況 情報資産保有状況 Web 簡易診断 標的型攻撃メール訓練

表 2.4- 3　専門家ヒアリングの概要

(1) 専門家（IT コーディネーター）

IT コーディネーターは、経済産業省推進資格であり、経営系、IT 系の専門知見、専門資格等を持つ、IT 経営を実現するプロフェッショナルであり、各地域のコミュニティやネットワークを通じて、地域の中小企業の IT 化に寄り添った支援活動を日頃から実施している。本実証事業では、IT コーディネーター協会（※NPO 法人ちば経営応援隊等が実査を担当）と連携し、地域の IT コーディネーターによるヒアリングを進めた。

(2) ヒアリング項目

本実証事業で実施したヒアリング項目は以下のとおり。

- 企業情報（質問数：17 問）

  IPA が提供する「情報セキュリティ対策ベンチマーク（第 2 部）」
  https://security-shien.ipa.go.jp/diagnosis/（2020/12/22 参照）
  組織の情報セキュリティへの取り組み状況を自己診断し、スコアによる評価、他社との比較等ができる。本実証事業では、実証参加企業の基本的な企業情報を調査するために第 2 部（問 8,9 除く）を実施した。

- 情報セキュリティ対策レベルの数値化（質問数：25 問）

  IPA が提供する「5 分でできる！情報セキュリティ自社診断」
  https://security-shien.ipa.go.jp/diagnosis/（2020/12/22 参照）
  企業の情報セキュリティ対策のレベルを数値化し、情報セキュリティ対策の現状を把握することができる。本実証事業では、実証参加企業のセキュリティ対策状況の指標として実施した。
  Part1：基本的対策（5 問）
  Part2：従業員としての対策（13 問）
  Part3：組織としての対策（7 問）

- セキュリティ対策状況（質問数：21 問）

  実証参加企業のより詳細なセキュリティリスクを診断するツールとして実施。サイバー保険プログラム設計を考慮した項目で構成している。
  - セキュリティ全般（8 問）
    セキュリティ方針/手順の策定、体制の構築、監査の実施等、人的・組織的な観点からセキュリティ対策の実施度合いを確認する。
  - ネットワークセキュリティ（3 問）
    通信の制御や監視等、ネットワークに関する技術的なセキュリティ対策の実施度合いを確認する。
  - クライアントセキュリティ（5 問）
    ウイルス・マルウェア対策ソフトや外部媒体によるデータの持ち出し制限等クライアント機器に関する技術的なセキュリティ対策の実施度合いを確認する。
  - セキュアな環境、施設、オフィス（5 問）
    入退室制限やサーバー機器のラックへの格納・施錠等の施設・オフィスにおける物理的なセキュリティ対策の実施度合いを確認する。

- 情報資産保有状況（情報資産管理台帳）

  IPA が提供する「リスク分析シート」にある「情報資産管理台帳」シート
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/（2020/12/22 参照）
  業務で利用する電子データや書類を洗い出し、媒体や保存先等の管理方法や重要度を記載し、中小企業が保有する情報資産について整理する。

(3) Web 簡易診断

本実証事業で実施した Web 簡易診断では、予想損失額シミュレーションツールと外部診断ツール（SecurityScorecard）を紹介し、実証参加企業の希望に応じて実施内容を選択した。

- 予想損失額シミュレーションツール

  「サイバー攻撃のおそれ」「個人情報の漏えい」「Web 改ざん」「DoS 攻撃」の 4 つのシナリオごとに、経済的損失を定量的に評価する。企業ごとにヒアリングした結果を踏まえて算出するため、企業の実態に即した損失額を予想できる。

- 外部診断ツール（SecurityScorecard）

  SecurityScorecard が常時収集している膨大なデータを解析し、外部視点から企業・組織のサイバーセキュリティリスクを 10 のリスクファクターごとに 5 段階で評価・スコアリングを実施する。

外部診断ツール（SecurityScorecard）に関しては、前提条件として独自ドメインを所有している必要があること、また診断結果が直観的に分かり難い等の理由から希望する企業がでなかったため、本実証事業で使用した UTM のオプションである、エンドポイント管理機能による外部診断の結果を追加提供した。外部診断ツール（エンドポイント管理）は、社内ネットワーク上にある PC 等の情報資産に関する管理実態についての評価であり、管理を見直す判断材料となる。

(4) 標的型攻撃メール訓練

本実証事業で実施した標的型攻撃メール訓練は、インターネット接続環境で「標的型攻撃メール」を疑似体験する訓練サービスである。ウイルス対策だけでは完全に防ぐことは難しいといわれている「標的型攻撃メール」への対策として、訓練を通じて“不審なメールを開かない”ように意識付けをする。Web 簡易診断同様、実証参加企業の希望に応じて実施した。

なお、（3）Web 簡易診断での予想損失額シミュレーションと外部診断（Security Scorecard）、（4）標的型メール訓練で利用した標的型攻撃メール訓練は、東京海上日動火災が提供する Web ツールである。

https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/（2021/1/7 参照）

2.4.1 の UTM モニタリング、および 2.4.2 の専門家のヒアリングによる中小企業のサイバーセキュリティに関する実態把握の結果を踏まえて、中小企業向けセキュリティ対策支援サービスのビジネス化に向けて検討した。

- 実態に即したセキュリティ対策支援

  中小企業のセキュリティリスクを洗い出し、セキュリティ診断、UTM モニタリング等の支援すべき内容を明確化させる。

- サイバー保険プログラムの設計

  中小企業のセキュリティリスクの実態や低コストへの期待に合う補償内容を検討するために、インシデント発生時に必要と考えられる初動対応等を基本補償とする保険と、発生の可能性が低く、発生した場合の影響が大きいリスクに対する保険(リスク移転)等の観点で検討する。

3. 実施結果

3.1 事業説明会の開催

3.1.1 開催概要・結果

事業説明会の概要と結果を表 3.1-1 に示す。

開催日時	2020/9/24　14:00～15:30	2020/9/25　14:00～15:30	
場所 形態	千葉県 オンライン（Zoom）	埼玉県 オンライン（Zoom）	
協力	柏商工会議所	春日部商工会議所 所沢商工会議所	
参加企業（人数）	12 社（14 人）	11 社（11 人）	
アジェンダ	・　はじめに（開催挨拶） ・　基調講演「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） ・　実証事業説明「サイバーセキュリティお助け隊実証事業事業内容について」（富士ゼロックス） ・　その他（連絡事項、アンケート）		5 分 15 分 45 分 25 分

表 3.1- 1　事業説明会の概要と結果

事業説明会では、以下の募集活動を実施した。
- 地域の商工会議所による募集（FAX、メルマガ、HP 掲載　等）
- 富士ゼロックス各販売会社の営業・カスタマーエンジニア（以下、CE）による個別訪問による募集
- 富士ゼロックスホームページによる告知
- IPA ホームページによる告知
- 地域の IT コーディネーターを通じた勧誘
- 本実証事業で協力関係にある損害保険会社（東京海上日動火災保険）を通じた勧誘

2020 年 9 月 24 日に千葉県、2020 年 9 月 25 日に埼玉県の企業を対象とし、新型コロナウイルス感染症対策を考慮し、オンラインによる事業説明会（Zoom）を実施した。2 回の説明会参加企業は合計 23 社（25 名）、そのうち実証事業への参加申込は 5 社であった。

千葉県、埼玉県とも商工会議所の協力を得て、HP 掲載、FAX、メルマガ、チラシ配布等で各県下の中小企業へ幅広く開催を告知したが、説明会参加企業数は、目標（20 社/回）の 6 割程度であった。総じて、中小企業のサイバーセキュリティに対する意識・関心がかなり低いことおよび実証参加に対する重要性・意義について、十分に訴求しきれなかったことが要因と考えている。

3.1.2 参加者の反応

説明会への参加者アンケート結果（n=8）を以下に示す。

Q1. 本実証事業を知ったきっかけをお選びください。（複数選択可）

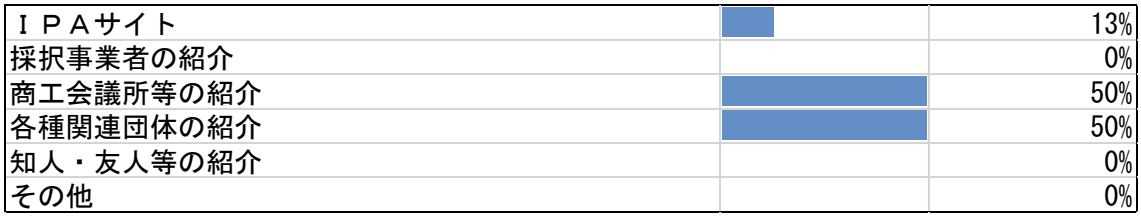

図 3.1- 1　Q1 の結果（n=8）

本実証事業を知ったきっかけは、「商工会議所の紹介」と「各種業界団体からの紹介」が大半を占めた。

Q2. お助け隊事業に期待する事項をお選びください。（複数選択可）

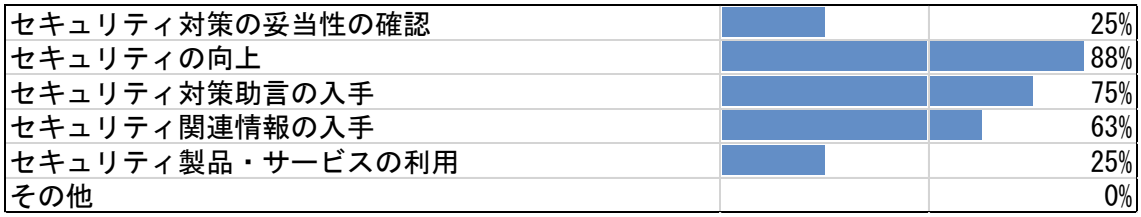

図 3.1- 2　Q2 の結果（n=8）

本実証事業に期待する事項は「セキュリティの向上」が約 9 割で最も高く、次いで「セキュリティ対策助言の入手」「セキュリティ関連情報の入手」である。

Q3. 貴社で導入しているセキュリティ対策をお選びください。（複数選択可）

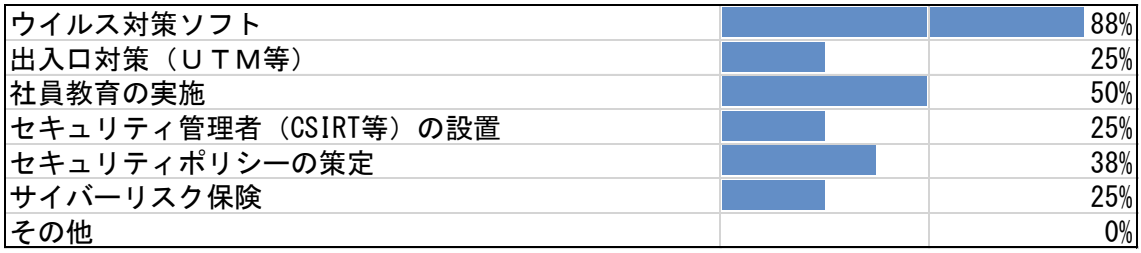

図 3.1- 3　Q3 の結果（n=8）

導入済みのセキュリティ対策は、「ウイルス対策ソフト」が約 9 割となっている一方で、「出入口対策」や「セキュリティ管理者の設置」は半数以下である。中小企業においては、セキュリティ対策＝ウイルス対策ソフト、の認識が強い傾向にあると考えられる。

Q4. 貴社でこれまで被害を受けたセキュリティ脅威がありましたらお選びください。（複数選択可）

標的型攻撃による被害	13%
ビジネスメール詐欺による被害	25%
ランサムウェアによる被害	0%
サプライチェーンの弱点を悪用した攻撃	13%
内部不正による情報漏えい	0%
サービス妨害攻撃によるサービスの停止	0%
インターネットサービスからの個人情報の窃取	13%
ＩｏＴ機器の脆弱性の顕在化	0%
脆弱性対策情報の公開に伴う悪用増加	13%
不注意による情報漏えい	13%
その他	0%
特になし	50%

図 3.1- 4　Q4 の結果（n=8）

アンケートに回答した半数の企業で、実際に「ビジネスメール詐欺による被害」等の脅威を受けている。

Q5. 今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

～5,000円	38%
5,000～10,000円	63%
10,000～50,000円	0%
50,000円～	0%
費用はかけない	0%

図 3.1- 5　Q5 の結果（n=8）

対策にかけられる月額費用の上限は、すべての企業で 1 万円以下となっており、低コストへの要望が高い。

Q6. サイバーリスクに関して、貴社の課題を教えてください。

リスクの洗い出し・評価・対策の検討	63%
対策にかける予算の確保	13%
専門人材の確保	38%
インシデント発生時の体制構築	25%
グループ会社、取引先も含めた対策の実施	13%
情報収集（最新技術動向や事故事例等）	63%
その他	0%

図 3.1- 6　Q6 の結果（n=8）

サイバーリスクに対する課題としては、「リスクの洗い出し・評価・対策の検討」「情報収集（最新技術動向や事故事例等）」の 2 項目が約 6 割と多い。

Q7. 取引先（業務委託元）から、貴社のセキュリティ対策状況に関して確認を受けたことはありますか。

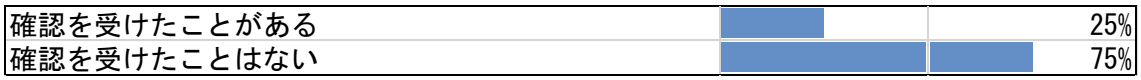

図 3.1- 7　Q7 の結果（n=8）

取引先から自社のセキュリティ対策状況について確認を受けた企業は 25%、4 社に 1 社は取引先から要請を受けている状況が分かる。

Q8. テレワークでのサイバーリスクに関して、貴社の課題を教えてください。

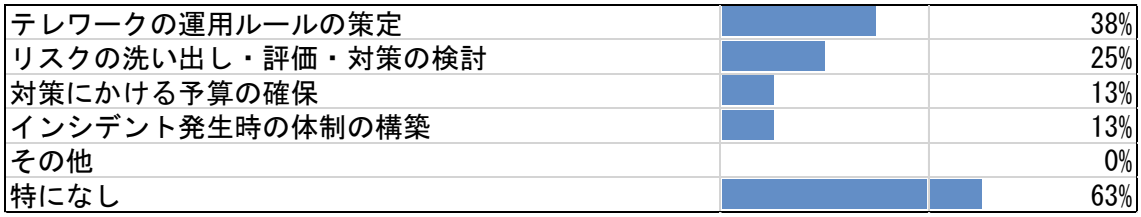

図 3.1- 8　Q8 の結果（n=8）

テレワークにおける課題は「特になし」を除けば、約 4 割の企業が「運用ルールの策定」を挙げている。

自由記述：

- リスクの把握や事故の想定額等が知りたい。（埼玉県製造業）
- サイバー攻撃を受けているのか感染しているのか等の現状が分からない。（埼玉県製造業）
- セキュリティの不備による信用失墜を防ぎたい。是非参加してサイバーセキュリティへの理解を深めたい。（千葉県サービス業）
- 本実証事業はとても良い。実証事業終了後に財力の弱い小規模事業者等には取り組みやすい価格帯が望ましい。（千葉県複合サービス事業）
- サイバーリスクに対して適切な認識、対策をできるようにしたい。（千葉県金融業・保険業）

3.1.3 事業説明会での気づき

説明会参加企業数は想定を下回り、中小企業のサイバーセキュリティに対する意識・関心はまだ低く、さらなる啓発が必要と考える。また、ウイルス対策ソフトと UTM の違いが分からない等のコメントもあり、サイバーセキュリティ対策に関する知識が不足していることの課題も明確になった。

3.2 実態把握結果

本実証事業で実施した UTM モニタリングおよび専門家によるヒアリングの実態把握について報告する。実施した企業数は以下のとおり。

実施内容	企業数（目標）	企業数（実績）
UTM モニタリング	30 社	36 社 達成率：120%
専門家のヒアリング	50 社	54 社 達成率：108%
Web 簡易診断	30 社	52 社 達成率：173%
標的型攻撃メール訓練	10 社	15 社 達成率：150%

表 3.2- 1　実態把握を実施した企業数

3.2.1 UTM モニタリングによる実態把握

(1) UTM の設置

UTM 設置数の推移を図 3.2-1 に示す。最終的に、UTM 設置企業は 36 社に達した。一方で、現地調査で設置 NG となり、UTM が設置できないことが原因で、実証参加できなかった企業を一定数発生させてしまった。

なお、設置不可となった主な理由は、以下に示すネットワーク構成上の問題であった。

・現行のネットワーク機器の設定等が不明でネットワーク環境を移行できない
・業務アプリケーション（会計ソフト等）の動作上の問題
・IPTV 回線を使用している

中小企業の実態として、ネットワーク環境を外部のシステムインテグレーターに任せている企業も多く、自社のセキュリティ環境について把握できていない、という状況が多くあった。VPN 等の複雑なネットワーク構成を構築している場合についても、設定変更が難しいため（検討に時間を要するため）に設置不可となる例も見られた。

また、UTM 設置段階では、実証参加企業と設置日の調整がつかず、想定以上に設置待ちの状態が長く続くことがあった。その原因は、UTM 設置作業に伴うネットワーク中断を回避したいという中小企業側の意向であり、業務に影響がでない時間帯（定時後等）で作業を指定され、調整に多くの時間を要した。

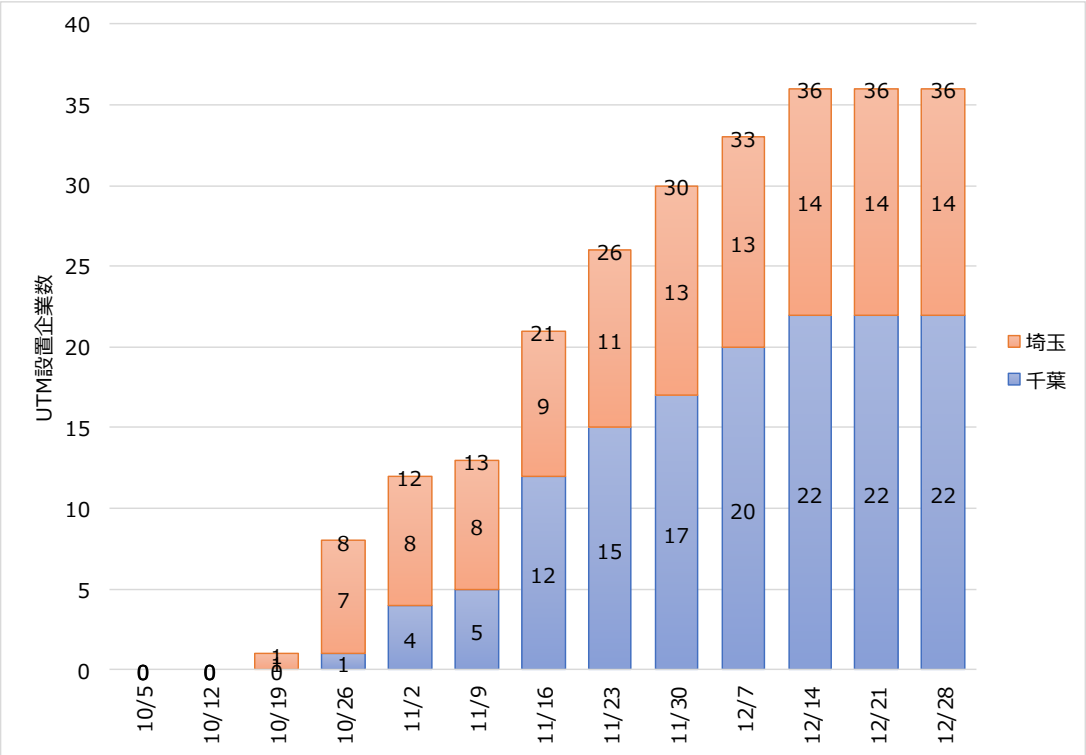

図 3.2- 1　UTM 設置企業数の推移

(2) 監視とログ収集

UTM 端末の開通・稼働状況

期間中、実証参加企業に設置した UTM の故障・不具合レポートは、UTM 起因ではない通信不具合が 1 件発生したが、NOC によるリモート監視にて検知、対応した。その他の動作不具合、ネットワーク障害等の発生はなかったことが確認されたため、実証参加企業 36 社の通信ログは正常に収集できたと判断した。
UTM のログ分析の結果については、3.3.3 中小企業のサイバー被害の実態把握で報告する。

実証参加企業へのレポート発行

UTM の通信ログは、実証参加企業ごとに集計・分析、サイバー攻撃の実態を可視化し、図 3.2-2 に示すレポートにて個別にフィードバックした。このレポートは、セキュリティの専門家でなくても全体把握できるように簡易な言葉で説明されており、中小企業側で不足しているサイバーセキュリティ対策の特定に役立てることができる。

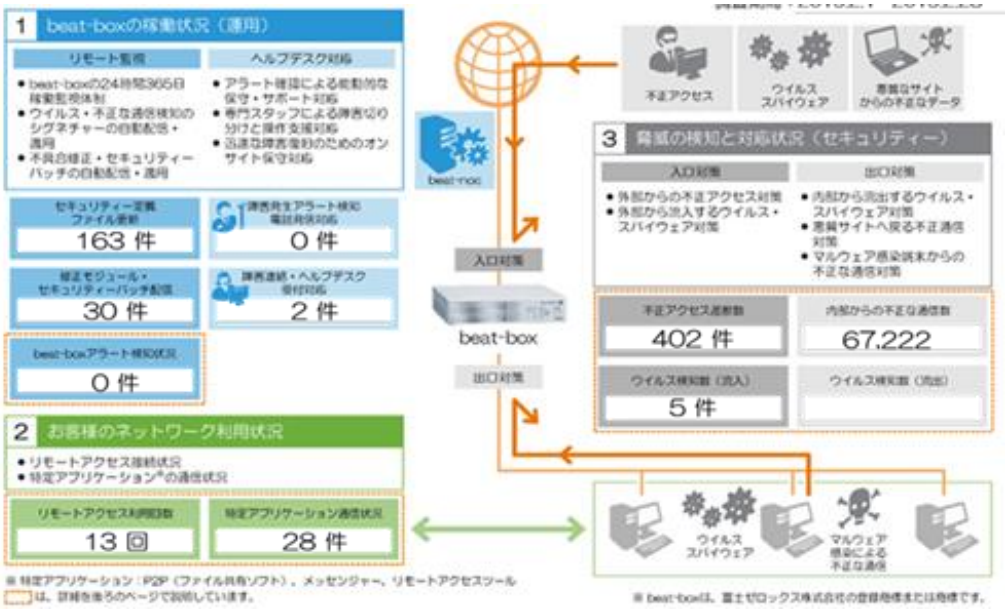

図 3.2- 2　UTM のレポート内容（例）

3.2.2 専門家のヒアリングによる実態把握

2.4.2 専門家のヒアリングによる実態把握で示したヒアリングの実施結果を表 3.2-2 に示す。

No	項目	実施件数
①	**企業の基本情報（全 17 問）**	53 社
②	**情報セキュリティレベルの数値化（全 25 問）**	53 社
③	**セキュリティ対策状況（全 21 問）**	53 社
④	**情報資産保有状況**	45 社
⑤	**Web 簡易診断 ※希望に応じて実施**	52 社
⑥	**標的型攻撃メール訓練 ※希望に応じて実施**	15 社

表 3.2- 2　ヒアリングの実施結果

① 企業の基本情報

一部の項目は 2.3.2 実証参加企業の属性情報で既に示しているので、ここでは残りの 10 項目について示す。

1. 主要な業務に関わるプロセスのうち、情報システム（外部のシステムを含む）に依存している割合。

図 3.2- 3　①-1 の結果（n=53）

2. 主要な業務に関わるプロセスのうち、インターネットに依存している割合。

図 3.2- 4　①-2 の結果（n=53）

3. 主要な情報システムについて、（月間）売上高に影響を及ぼさないで済む、許容停止時間。

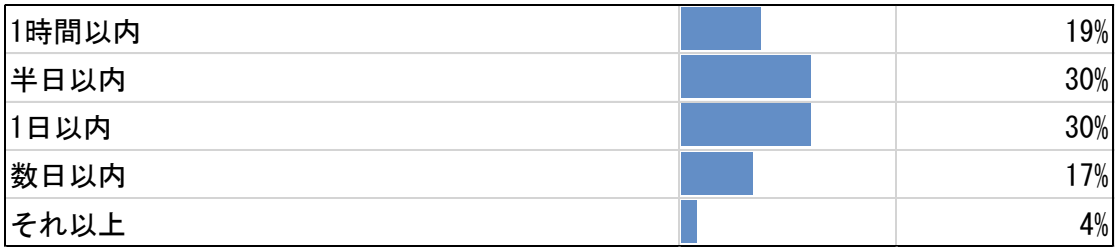

図 3.2- 5　①-3 の結果（n=53）

4. 主要な情報システムが営業日に「24 時間」停止した場合、その日の売上高に及ぼす影響。

図 3.2- 6　①-4 の結果（n=53）

1-4 の結果から、業務プロセスの 50%以上を情報システムに依存している企業は約半数、また 50%以上をインターネットに依存している企業は約 4 割を占めている。情報システムの停止が売上に影響しないで済む許容時間は 1 時間以内とする企業が約 2 割で、仮に 24 時間停止した場合、売上に大きな影響（50%減以上）を受ける企業は 8%となっている。

5. 個人情報漏えい等、情報セキュリティ関連の事故が発生した場合に発生する、ブランド（企業イメージ）への影響。

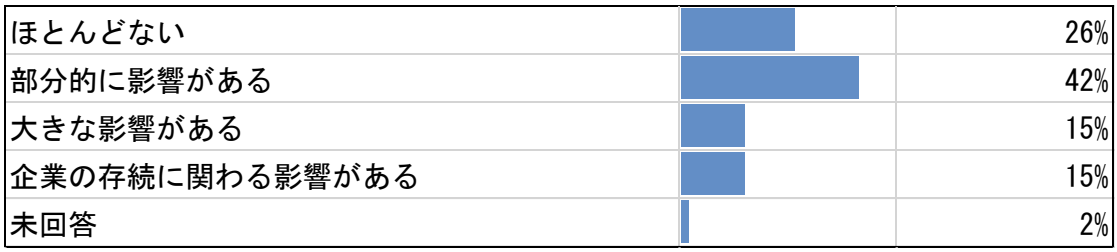

図 3.2- 7　①-5 の結果（n=53）

セキュリティ事故が発生した場合、企業ブランドに大きな影響がある、または企業の存続に関わる影響があると回答した企業は 3 割である。

6. 業務は、元請けや代理店、フランチャイジー等のビジネスパートナーにどの程度依存しているか。

図 3.2- 8　①-6 の結果（n=53）

元請けや代理店等のビジネスパートナーに依存度は、大きく依存している、またはビジネスパートナーなしでは事業が成り立たないと回答した企業は約 2 割である。

7. 外部に漏えいすると事業に極めて深刻な影響が生じる重要情報（国家機密、営業機密、プライバシー情報等）をどの程度保有、管理または使用しているか。

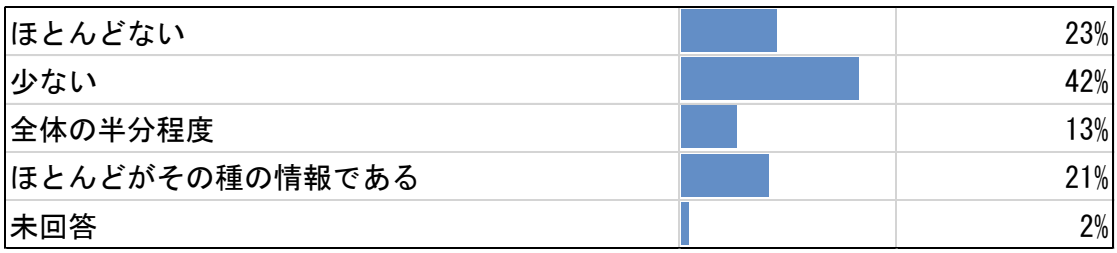

図 3.2- 9　①-7 の結果（n=53）

8. 事業を実施する上で何名分程度のお客様個人情報（取引先を含む）を取り扱っているか。

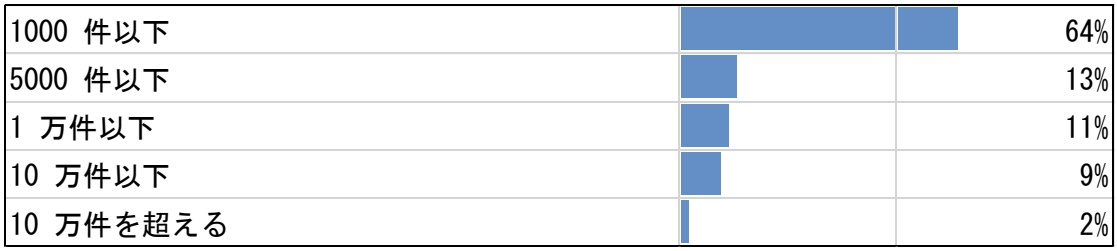

図 3.2- 10 ①-8 の結果（n=53）

1 万件を超えるお客様個人情報を保有している企業は約 1 割となっている。

9. 離職率（直近の 1 年間に退職・転職された従業員の割合）。

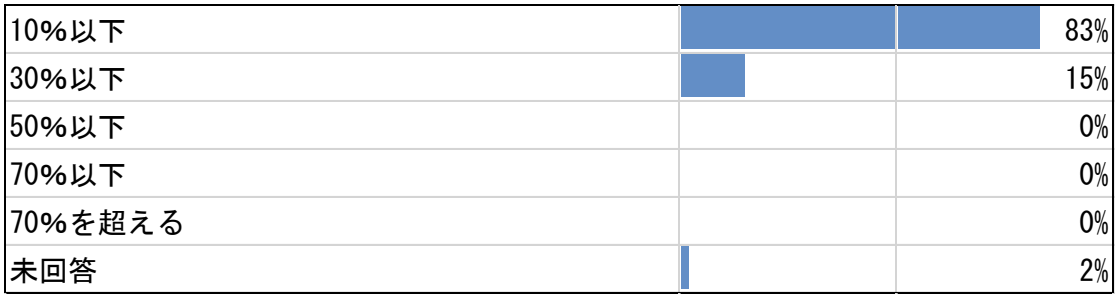

図 3.2- 11 ①-9 の結果（n=53）

10. 過去に事業活動に影響を与えるような IT 事故が発生したことがあるか。

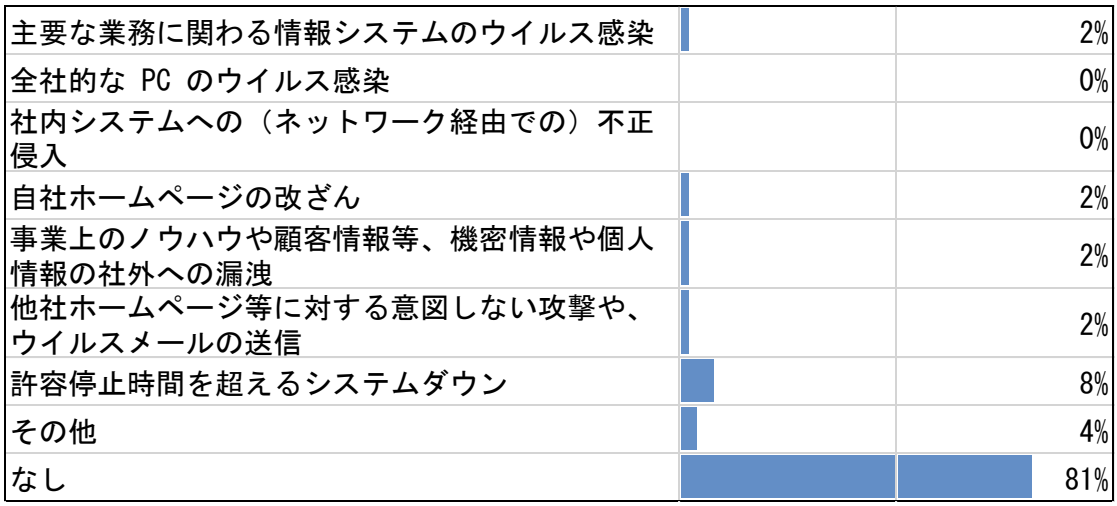

図 3.2- 12 ①-10 の結果（n=53）

過去に IT 事故が発生した企業は約 2 割で、内容としては許容停止時間を超えるシステムダウン、情報システムのウイルス感染、自社ホームページの改ざん等となっている。

② 情報セキュリティ対策レベルの数値化

「5 分でできる！情報セキュリティ自社診断」の診断結果（合計点）に関して、実証参加企業を 4 つのセキュリティレベルに分類した結果を示す。基本対策ができていない（49 点以下）企業は約 2 割であった。

合計点	セキュリティレベル	実証参加企業の割合
100 点	入門レベルのセキュリティ対策は達成済み	2%（1 社）
70-99 点	ほぼ達成できているが、部分的に対策不十分な点がある	37%（19 社）
50-69 点	対策が行き届いていないところが多い	38%（21 社）
49 点以下	いつ情報流出等の事故が起きても不思議ではない	23%（12 社）

表 3.2- 3　情報セキュリティ対策レベルの数値化（n=53）

③ セキュリティ対策状況

次に、実証参加企業のより詳細なセキュリティリスクについてヒアリングした結果を示す。

セキュリティ全般（8 問）

1. サイバー攻撃等のサイバーセキュリティリスクを経営リスクの 1 つとして認識し、サイバーセキュリティリスクに対する対応方針を組織外に宣言しているか。

図 3.2- 13　③-1 の結果（n=53）

サイバーセキュリティリスクに対する対応方針を組織外に宣言している企業は約 3 割に留まり、7 割は外部に対して明示できていないことが分かる。

2. 情報セキュリティに関するルールはあるか。また、そのルールには、個人情報保護および業務上の機密情報の取り扱いが含まれているか。
   ＊「ルールはあるが、個人情報保護または業務上の機密情報の取り扱いが含まれてない」場合は△を選択

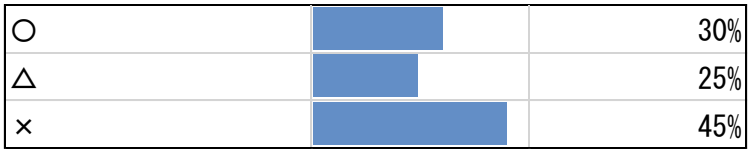

図 3.2- 14　③-2 の結果（n=53）

情報セキュリティ対策を正しく把握できている企業は約 30%、残り 70%のうち、25%は「個人情報保護または業務上の機密情報の取り扱い」が足りておらず、45%の企業では、情報セキュリティリスクに関するルールもない状態であった。

3. 従業員（社員・派遣社員・協力会社社員等）に情報セキュリティに関するルールを周知徹底しているか。
＊理解している従業員が 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は〇を選択

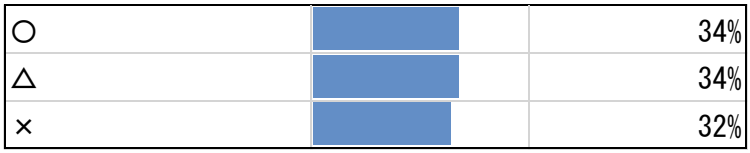

図 3.2- 15　③-3 の結果（n=53）

従業員に情報セキュリティ対策を徹底できている企業は約 3 割、残りの 7 割近くは不十分もしくはできていないと回答した。

4. 社外から最新のサイバー攻撃情報を入手することで、情報セキュリティに関するルールを定期的に確認し、必要に応じて見直しているか。
＊質問 2 が×の場合は×、「定期的に内容を確認しているが、サイバー攻撃のトレンドに対応するための見直しは行っていない」場合は△

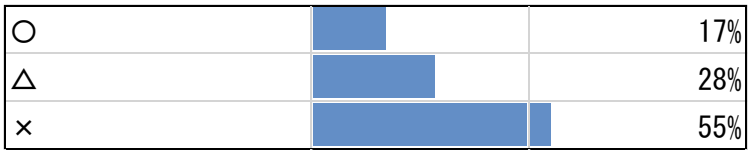

図 3.2- 16　③-4 の結果（n=53）

外部から最新のサイバー攻撃情報を入手し、そのトレンドを把握しながら対策を実施できている企業は 2 割以下と低い。残り 8 割以上は不十分もしくはできていないと回答した。

5. 組織内に SOC、CSIRT を設置する等、情報セキュリティインシデントの発生時に迅速に対応できる体制が構築されているか。

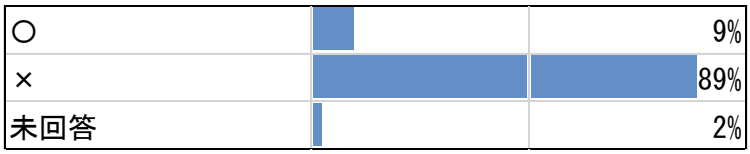

図 3.2- 17　③-5 の結果（n=53）

セキュリティインシデントが発生した場合に迅速に対応できる体制を構築している企業は 1 割程度に留まる。

6. 情報セキュリティについて、従業員（社員・派遣社員・協力会社社員等）の教育（e-learning、集合研修、標的型メール等に対する訓練等）を行っているか。
＊「教育を行ってはいるものの不十分と感じている」場合は△を選択

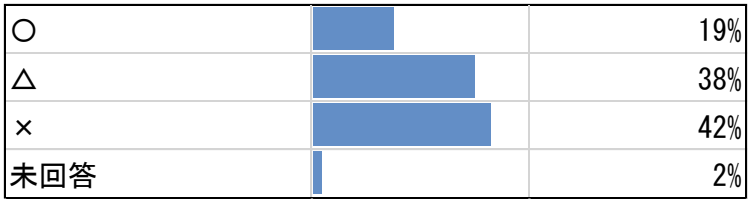

図 3.2- 18　③-6 の結果（n=53）

セキュリティ訓練に対しての実施レベルは 2 割以下と低く、残り 8 割は不十分もしくはできていないと回答した。

7. 社内に CISO（Chief Information Security Officer：最高情報セキュリティ責任者）等の情報セキュリティ関連業務を統括する役職を置き、定期的にセキュリティ対策状況が報告される等、組織としてセキュリティ状況を把握できる管理体制が構築されているか。

図 3.2- 19　③-7 の結果（n=53）

セキュリティ管理体制を構築できている企業は 1 割程度と極めて低い結果となった。

8. 系列企業、ビジネスパートナー、IT システム管理の委託先（外部委託している場合）のセキュリティ対策状況を把握しているか。

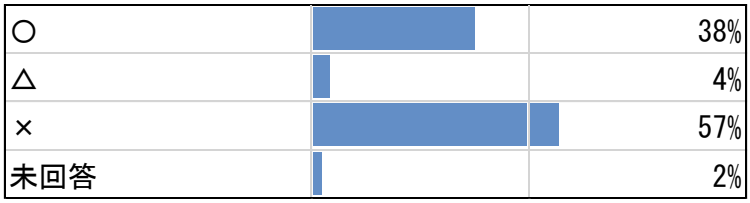

図 3.2- 20　③-8 の結果（n=53）

委託先のセキュリティ対策状況は、約 6 割の企業は把握できていない状態であった。

ネットワークセキュリティ（3 問）

9. IDS/IPS や WAF 等を導入する等、社外から社内へ、社内から社外への通信を定期的に確認しているか。

図 3.2- 21　③-9 の結果（n=53）

外部への通信内容を、IDS/IPS や WAF 等を通じて確認できている企業は 2 割以下で、大半の企業は確認できていない状況であった。

10. インターネットまたは無線ネットワーク上の通信を暗号化しているか。

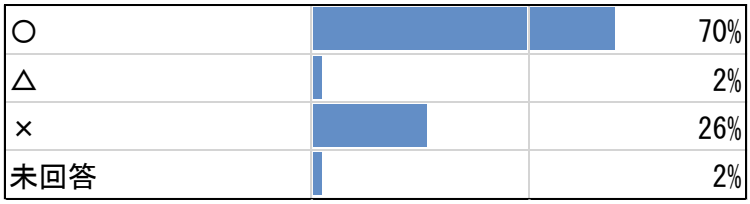

図 3.2- 22　③-10 の結果（n=53）

インターネットまたは無線ネットワーク上の通信の暗号化については、7 割の企業が実施しており、不十分もしくは実施できない企業は 3 割程度であった。

11. 社外から社内のサーバーにリモートアクセス（外部接続）する際に認証処理を行っているか。

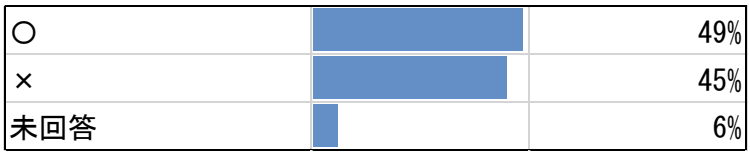

図 3.2- 23　③-11 の結果（n=53）

リモートアクセスでの認証処理は約半数の企業で実施できていない。

クライアントセキュリティ（5 問）

12. PC 等の社員用端末にアンチウイルスソフトやマルウェア対策ソフトをインストールしているか。
＊アンチウイルスソフトやマルウェア対策ソフトをインストールしている社員用端末が 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は○を選択

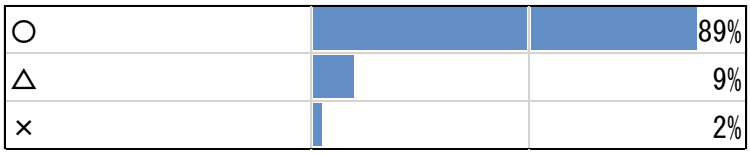

図 3.2- 24　③-12 の結果（n=53）

アンチウイルスソフトやマルウェア対策ソフト等は、約 9 割の企業で導入済みであることが分かった。

13. 社員用端末にインストールされたアンチウイルスソフトやマルウェア対策ソフトのパターンファイルや更新プログラムを定期的に更新しているか。
＊質問 12 が×の場合または定期的に更新している社員用端末が 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は○を選択

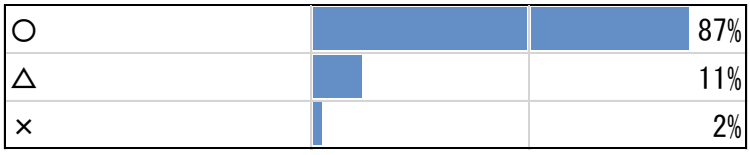

図 3.2- 25　③-13 の結果（n=53）

アンチウイルスソフトやマルウェア対策ソフトの定期更新についても、約 9 割の企業で概ね実施できており、最新の状態に更新している。

14. 社員用端末にインストールされた OS やミドルウェアの更新プログラムを定期的にインストールしているか。
＊質問 12 が×の場合または定期的にインストールしている社員用端末が 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は〇を選択

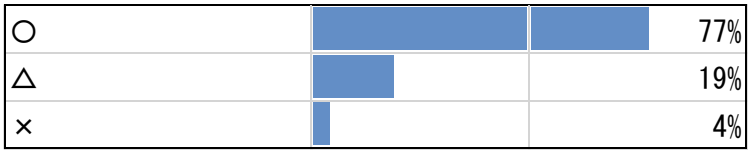

図 3.2- 26　③-14 の結果（n=53）

社員用端末の OS やミドルウェアの定期更新については、約 8 割の企業ができており、約 2 割の企業は不十分もしくはできていないと回答した。

15. 社員用端末に接続する外部媒体（USB メモリ、DVD ディスク等）は会社指定のものを使用しているか。
＊会社指定の外部媒体を使用しているケースが 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は〇を選択

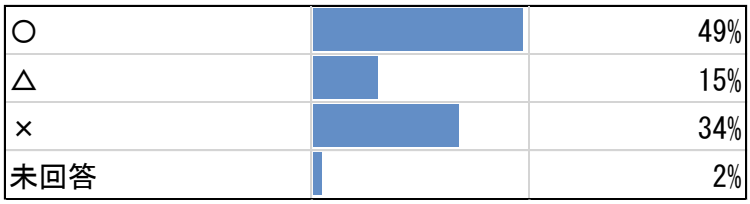

図 3.2- 27　③-15 の結果（n=53）

外部媒体（USB メモリ、DVD ディスク等）の利用で、会社の管理下にあるデバイス・媒体で情報管理できている企業は約半数、残りは会社の管理下にないデバイス・媒体が使われていることが分かった。

16. 機密性の高い情報を印刷またはコピーする際に出力制限をするまたは実行者を特定するソフトを導入しているか。
＊導入している端末が 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は〇を選択

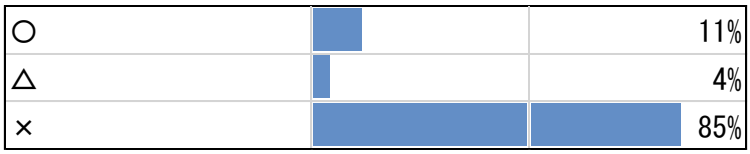

図 3.2- 28　③-16 の結果（n=53）

機密性の高い情報へのアクセス制限（印刷やコピー等の実行者特定）のソフト導入ができている企業は 1 割程度と低く、9 割近くの企業は管理できていないことが分かる。

セキュアな環境、施設、オフィス（5 問）

17. 従業員（社員、派遣社員、協力社員等）の入社時・退職時のルールには、入社・退職に伴う ID の発行・削除処理に関する内容が含まれているか。

図 3.2- 29　③-17 の結果（n=53）

従業員の入社・退職に伴う ID の発行・削除処理に関するルールが含まれている企業は 45%で、残り 55%はできていないことが分かった。

18. 入社時・退職時のルールに基づいて手続きが行われているか。
＊ルールに基づいた手続きが 50%未満と見込まれる場合は×、50%以上 80%未満の場合は△、80%以上の場合は○を選択

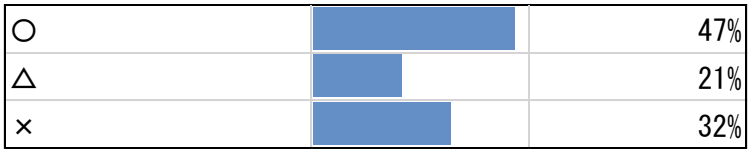

図 3.2- 30　③-18 の結果（n=53）

約半数の企業では、従業員の入社時、退社時のルールに基づいた手続きが不十分もしくはできていないと回答した。

19. 入室時に施錠、カード（ID カードや入館証等）認証等を行い、許可された者のみが入室できる仕組みを導入している等、外部の業者等がオフィス内の重要なエリアに立ち入れないように入室制限を行っているか。また、入退室の記録をとっているか。
＊入室制限または入退室の記録のいずれか一方のみを行っている場合は、△を選択

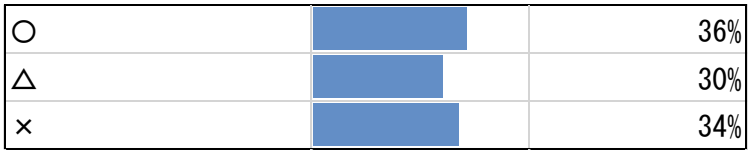

図 3.2- 31　③-19 の結果（n=53）

従業員の入退出を管理できている企業は約 4 割、残り 6 割以上は不十分もしくはできておらず、物理的なセキュリティにも課題があることが分かった。

20. 重要システム（個人情報や機密情報を保持・使用するシステム等）のログを収集しているか。

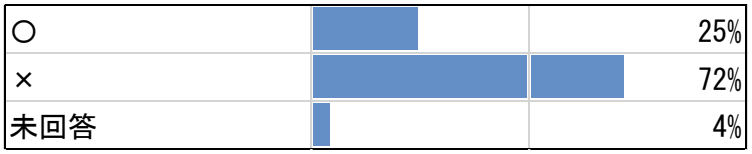

図 3.2- 32　③-20 の結果（n=53）

重要システムのログを収集している企業は 25%と低い。

21. 収集したログを分析する等セキュリティインシデントを特定するためのプロセス・仕組みが存在しているか。

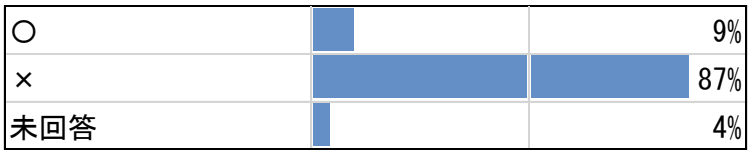

図 3.2- 33　③-21 の結果（n=53）

さらにシステムのログを分析する仕組みがある企業は 1 割以下に留まる。

③のヒアリング結果について、実証参加企業を 4 つのセキュリティレベルに分類した結果を表 3.2-4 に示す。②と比較して、より詳細なセキュリティ対策レベルでは、約 7 割の企業でセキュリティリスクが高い状況にあると判定された。中小企業においては、特にセキュリティインシデント等が発生した場合に、すぐに自社で対応できない（どうすれば良いか分からない）企業が多く、対策支援が必要な状況にある。

セキュリティレベル（合計点）	セキュリティレベル	実証参加企業の割合
Level.4（90-100 点）	全般に渡ってセキュリティ対策は高いレベルにある	6%（3 社）
Level.3（70-89 点）	一定レベルのセキュリティ対策を実施しているが、部分的に対策が不十分な点がある	9%（5 社）
Level.2（50-69 点）	セキュリティ対策が不十分な点が多い	17%（9 社）
Level.1（0-49 点）	セキュリティリスクが高い状況にある	68%（36 社）

表 3.2- 4　詳細なセキュリティ対策レベルの診断結果（n=53）

④ 情報資産保有状況

実証参加企業の情報資産の保有状況について調査した結果を示す。

業務分類	資産数（個数）	全資産に対する割合
営業（顧客リスト、契約書等）	203	42%
人事（社員名簿、マイナンバー等）	105	22%
技術（設計図、報告書等）	71	15%
経理（請求書、契約書等）	49	10%
その他	55	11%
合計	483	100%

表 3.2- 5　情報資産の業務分類（n=45 社）

重要度	資産数（個数）	全資産に対する割合
2	337	70%
1	140	29%
0	6	1%

表 3.2- 6　情報資産の重要度（n=45 社）

本実証事業で調査した 45 社の情報資産は合計 483 個で、顧客リストや契約書等の営業に関する資産が約 4 割、社員名簿やマイナンバー等の人事に関する資産が約 2 割を占めている。また、7 割が重要度 2※である。

※重要度の定義は以下のとおり。機密性、完全性、可用性の評価値の詳細については、IPA が提供する「リスク分析シート」にある「重要度定義」シートを参照のこと。

https://www.ipa.go.jp/security/keihatsu/sme/guideline/（2020/12/22 参照）

判断基準	重要度
機密性・完全性・可用性評価値のいずれかまたはすべてが「2」の情報資産	2
機密性・完全性・可用性評価値のうち最大値が「1」の情報資産	1
機密性・完全性・可用性評価値すべてが「0」の情報資産	0

表 3.2- 7　情報資産の重要度の定義

次に、重要度 2 の情報資産に関する保存媒体について示す。

資産の保存媒体	資産数（個数）	重要度 2 の資産に対する割合
書類	127	38%
社内サーバー	84	25%
社外サーバー	27	8%
事務所 PC	68	20%
可搬電子媒体	15	4%
モバイル機器	15	4%
未回答	1	0%
合計	337	100%

表 3.2- 8　重要度 2 の情報資産の管理媒体

実証参加企業の重要度 2 の情報資産に関しては、約 4 割が紙文書で保存、次いで社内外サーバーが約 3 割、PC が約 2 割となった。

⑤ Web 簡易診断ツール

Web 簡易診断ツールは、セキュリティ対策支援サービスの事業化に必要な情報（最低限の支援内容・費用、サイバー保険のニーズ等）の収集、実証参加企業におけるサイバーセキュリティの意識向上に効果がある。

予想損失額シミュレーション

シミュレーションによる“自社の損失額”は、具体的な数字で直観的に理解しやすく、サイバーインシデントを自分事として捉えるきっかけになる。実証参加企業の中にも比較的関心を持つ会社が多くあり、IT コーディネーターのフォローのもとで実施した。

※シミュレーション結果（予想損失額）は、仮定条件に基づいて算出されたものであり、サイバー攻撃時の損失額を保証するものではない。

以下には、「サイバー攻撃のおそれ」「個人情報の漏えい」「Web 改ざん」「DoS 攻撃」の 4 つのシナリオごとに、経済的損失を定量的に評価した結果を示す。

- シナリオ 1：「サイバー攻撃のおそれ」

想定シーン

1. 公的機関※1 から「貴社と外部に不審な通信が確認された」旨の連絡があった。
2. 社内のシステム部門が調査したところ、一週間前に不審なメールが従業員宛に届き、一部の従業員が誤って添付ファイルを開封したことが判明した。実際にサイバー攻撃の被害にあったかどうか、被害にあったとすればその範囲や規模は不明である（どのような社内データ・システムがアクセスされ、窃取・改ざん・破壊を受けたか分からない状態）
3. 被害状態を明らかにするため、外部の専門事業者に「フォレンジック調査」等※2 を依頼する。

※1：JPCERT/CC や IPA 等

※2：サイバー攻撃を受けたかどうか、受けた場合の被害の程度を明らかにするために、外部の専門事業者に委託する調査

予想損失額結果（n=52）

調査対象は感染したコンピューター端末、サーバー、通信記録・ログ等であり、損失額の内訳は以下のとおり。

・フォレンジック費用等

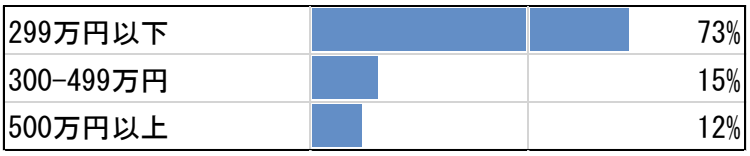

図 3.2- 34　シナリオ 1 による予想損失額の結果

サイバー攻撃を受けた可能性がある場合のフォレンジック調査費用の中央値は 275 万円（＝最低必要金額）。約 7 割は 299 万円以下である。調査費用は調査範囲や規模によってばらつき、最大で 825 万円となっている。

➢ シナリオ 2：「個人情報の漏えい」

想定シーン

1. お客様より「貴社にしか記載していない個人情報が漏れているようである。ダイレクトメッセージや勧誘の電話がかかってきており、原因調査と早急な対処をお願いする」旨の電話があった。その後、他のお客様からも同様の電話が入った。
2. 個人情報漏えいの痕跡について自社内で把握できなかったため、外部の専門事業者に依頼した。結果、自社従業員が標的型メール攻撃を受け、誤ってメールの添付ファイルを開封したことが判明した。 社内に侵入したウイルスにより、外部から社内のお客様情報のデータベースにアクセスされ、すべてのお客様の個人情報が窃取された。
3. お客様への通知とお詫び対応見舞金送付を含む 、広報対応、損害賠償請求等の対応が必要となった。

予想損失額結果（n=52）

損失額の内訳は以下のとおり。

・フォレンジック費用等
・お詫び対応費用（お見舞金）
・お詫び対応費用（広告費用）
・損害賠償金、訴訟対応費用

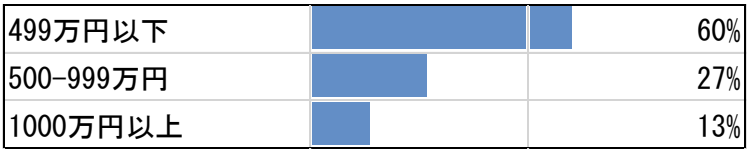

図 3.2- 35　シナリオ 2 による予想損失額の結果

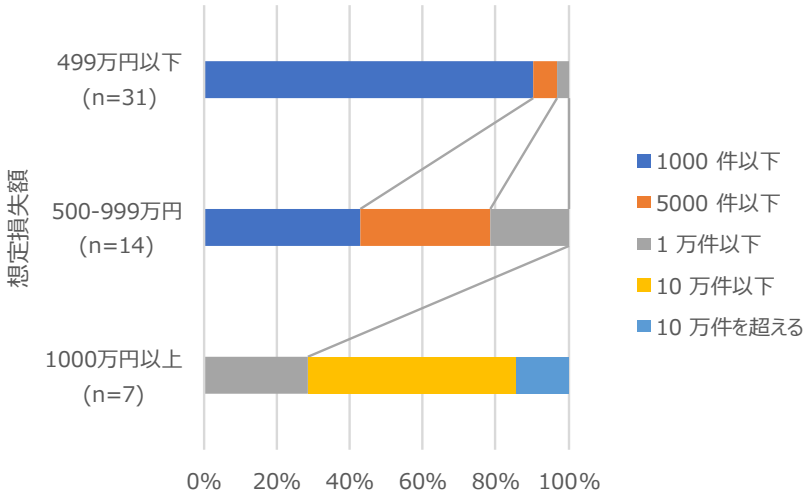

図 3.2- 36　保有する個人情報数との関係

個人情報を漏えいさせた場合にかかる費用の中央値は 420 万円。6 割は 499 万円以下である。図 3.2-36 で示すように、保有する個人情報数が多いほど高額になる傾向があり、最大で 37,267 万円となっている。

➢ シナリオ 3：「Web 改ざん」

想定シーン

1. お客様より「最近ウイルスに感染し、外部の専門事業者に調査を依頼したところ、貴社の Web サイトにアクセスしたことが原因のようである。事実確認と調査費用の負担をお願いする」旨の電話があった。
2. 自社で外部の専門事業者に依頼し調査したところ、自社の Web サーバーが改ざんされ、アクセスしたユーザーがウイルスに感染することが判明した。 あわせて、改ざんの原因が、自社の Web サーバーの重大な脆弱性の放置にあることも判明した。
3. ただちに Web サイトおよびサーバーを停止。Web サイトの復旧までに約 10 日を要し、この期間の Web サイト経由の売上・利益が失われた。この期間中、オフラインでのお客様対応に追われ、臨時の人件費等が発生した。 さらに、ウイルスに感染したことにより、コンピューター端末のソフトウェアの再購入を余儀なくされたお客様の一部から損害賠償を請求された。

予想損失額結果（n=52）

損失額の内訳は以下のとおり。

・フォレンジック費用等
・お詫び対応費用（広告費用）
・損害賠償金、訴訟対応費用
・休業損失
・営業継続費用等

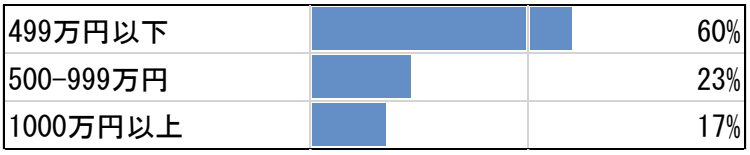

図 3.2- 37　シナリオ 3 による予想損失額の結果

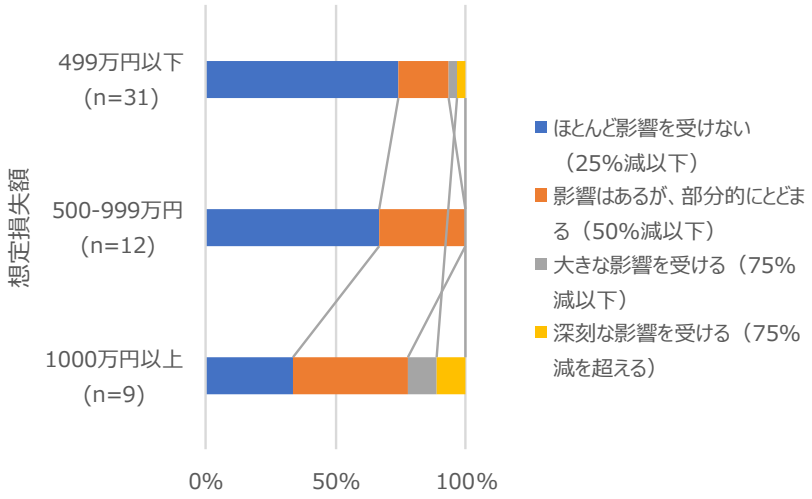

図 3.2- 38　情報システム停止による売上高への影響との関係

Web 改ざんされた場合にかかる費用の中央値は 473 万円。6 割は 499 万円以下である。図 3.2-38 で示すように、情報システム等の停止による売上への影響が大きいほど高額になる傾向があり、最大で 24,097 万円となっている。

➢ シナリオ 4：「DoS 攻撃」

想定シーン

1. 会社の端末が突然使用不能となった。
2. 原因を調査したところ、外部からの DDoS 攻撃（Distributed Denial of Service attack）により、会社の基幹システムを運用するサーバー等が停止した。DDoS 攻撃は丸一日近くに及び、攻撃が終わった後も引き続きサーバーに支障が生じ、会社業務に影響が及んだ。
3. 期間中、会社の重要システム（メールシステム、経理・計上システム等）が使えず、個別のお客様と商談等についての電子ファイルにアクセスできなかったため、オフラインでの対応に追われた。 最初の攻撃が終息した後も、短時間の DDoS 攻撃が繰り返し発生した。

予想損失額結果（n=52）

損失額の内訳は以下のとおり。

・休業損失

・営業継続費用等

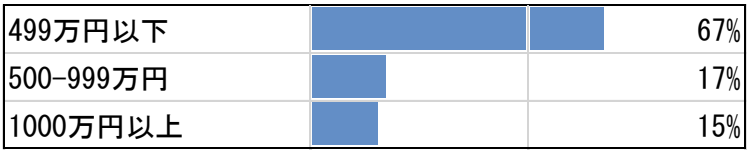

図 3.2- 39　シナリオ 4 による予想損失額の結果

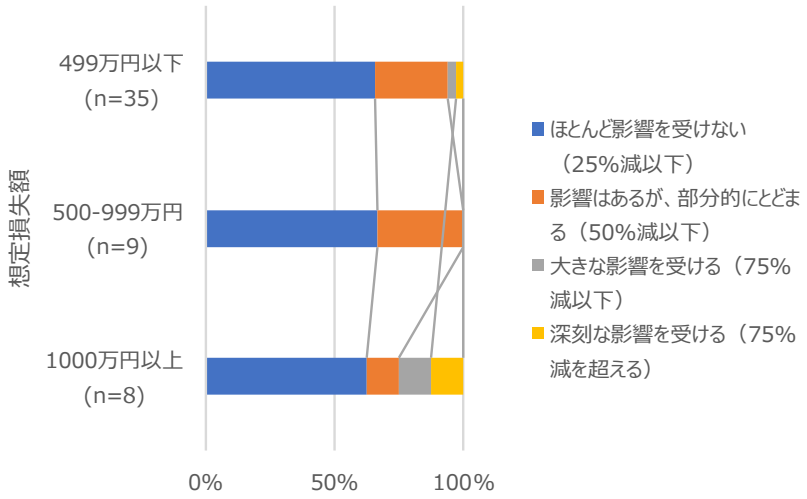

図 3.2- 40　情報システム停止による売上高への影響との関係

DDoS 攻撃を受けた場合にかかる費用の中央値は 229 万円。約 7 割は 499 万円以下である。図 3.2-40 で示すように、シナリオ 3 同様、情報システム等の停止による売上への影響が大きいほど高額になる傾向があり、最大で 9,761 万円となっている。

以上、4 つのシナリオから、インシデントが発生した場合の影響について、中小企業の実態に即した予想損失額を調査した。結果、いずれのシナリオにおいても、6～7 割の企業では損失額は 499 万円以下に収まることから、今後も追加で検証が必要であるが、サイバー保険による最低補償金額の目

安として 500 万円程度を考えている。また保有する個人情報数、事業の情報システムへの依存度、売上等によって高額となり得ることが分かった。中小企業ごとに影響は大きく異なるため、もしもの場合の損失額等について、自社のケースで事前に把握しておくことが重要であると考える。

外部診断ツール（SecurityScorecard）

外部診断ツール（SecurityScorecard）は、上記の予想損失額シミュレーションとセットで紹介したが、実施を希望する企業がでなかった。要因としては以下のように考えている。

- 前提条件として独自ドメインを所有している必要がある
- 診断結果が直観的に分かり難い（次のアクションに繋がらない）
- 実証参加企業の担当者がアカウント登録、診断手続きを進める必要がある（アカウント登録に数日を要する）

上記の理由から、中小企業に主体的に使用してもらうには、関心を持ちやすい内容であることはもちろん、ユーザーが目的を達成するために、少ないクリック数、短時間で結果が分かる等、効率良く実施できるようにする工夫も必要と考える。

外部診断ツール（エンドポイント管理）

外部診断ツールとして、UTM のオプションであるエンドポイント管理機能を利用した評価結果に関するレポートを追加提供した（対象 35 社）。エンドポイント管理機能は、社内ネットワーク上にある PC 等の情報資産の管理実態について評価することができる。表 3.2-9 に結果を示す。

スコアカテゴリ	内容	実証参加企業平均
ハードウェア	PC の経年、PC の HDD 利用率等からスコアリング	Ave：3.5 Max：5.0 Min：2.0
ソフトウェア	OS バージョン・統一性、office バージョン・統一性等からスコアリング	Ave：4.1 Max：5.0 Min：2.0
セキュリティ	セキュリティ対策の実施状況（アンチウイルス、Firewall、スクリーンセーバー等）、アンチウイルス等の統一性・最新化率等からスコアリング	Ave：4.5 Max：5.0 Min：2.9
総合診断	ハードウェア、ソフトウェア、セキュリティに加えて、サーバー等の周辺機器の情報を加味して総合的にスコアリング	Ave：4.0 Max：4.7 Min：3.3

表 3.2- 9　外部診断ツール（エンドポイント管理）の結果（n=26）

セキュリティ上重要な OS バージョンやウイルス対策等が不十分で、見直し・対策が必要と判定される企業も確認されている。診断結果は、今後のセキュリティ対策に役立つように、対象企業ごとに個別レポートとして提供した。エンドポイント側の IT 環境の調査、対応についても、定期的に実施する必要があると考えられる。

⑥ 標的型攻撃メール訓練

標的型攻撃メール訓練は、Web 簡易診断ツールと同じく、実証参加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にしている。実証参加企業の経営者やシステム管理者から、訓練の効果や手順等について、具体的なイメージできず分かり難いとの声があり、実施を希望する企業が少なかったが、IT コーディネーターのフォローのもと、以下の手順で事前通知、防災訓練型で一斉に実施した。

1. 標的型攻撃メール訓練を実施することを通達、承諾を得る
2. 1 で承諾を得た企業を対象として、標的型攻撃の訓練メールを送信
3. 訓練終了後、アンケート回答を依頼

訓練に使用したメールは下記のとおり。

――――――

From: 総務 <kyoyu-groupmail@infomaton.com>
Date: 2020 年 12 月 21 日（月） 9:00
Subject: 端末セキュリティパッチの適用手順
To: ★対象者メールアドレス★
★会社名★
★所属名★　★役職名★　★お名前★様
お疲れ様です。
総務より連絡です。
ニュースでも報道されておりますが、弊社も利用しているメーカの PC に脆弱性が発見されております。
以下の URL から手順書とセキュリティパッチをダウンロードし、各自対応願います。
※本メールは対象者のみに送付しております。
Version 1903 for x64-based Systems の適用について
本件は国内でもセキュリティ事故の発生が報告されているため、早急な対応をお願いします。
何卒、宜しくお願い致します。

――――――

訓練の実施結果および訓練後のアンケート結果を以下に示す。

項目	企業数	人数
訓練実施	15 社	25 名
アンケート回収	14 社（93%）	17 名（68%）

表 3.2- 10　標的型攻撃メール訓練の実施結果

1. 今回の訓練について難易度はどうか

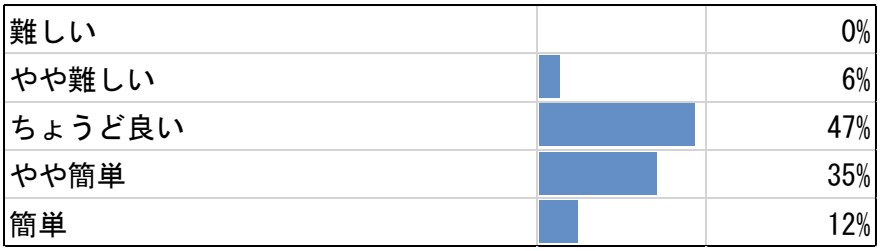

図 3.2- 41　Q1 の結果（n=17）

2. 送付された訓練メールについて、不審に感じた点はどこか（複数選択可）

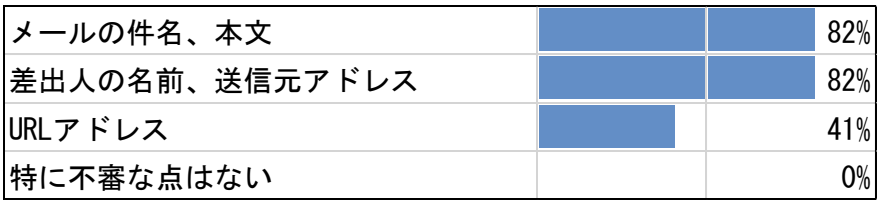

図 3.2- 42　Q2 の結果（n=17）

3. 訓練と知らなかった場合、URL をクリックしてしまうと思うか

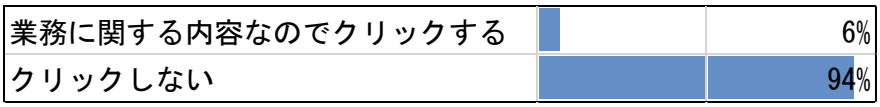

図 3.2- 43　Q3 の結果（n=17）

4. 標的型攻撃メール等の不審なメールを受信した際の自組織のルールや対応方法を知っているか

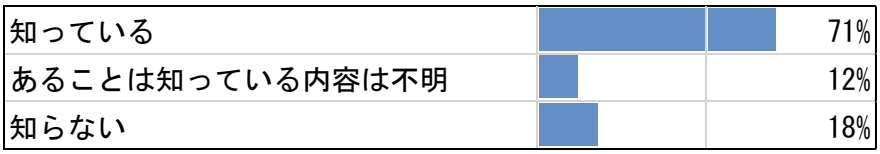

図 3.2- 44　Q4 の結果（n=17）

5. 不審なメールの添付ファイルを開いたり、URL をクリックしてしまった際に、対応窓口に連絡できるか

図 3.2- 45　Q5 の結果（n=17）

6. 不審なメールの添付ファイルを開いたり、URL をクリックしてしまった際に、PC をネットワークから遮断することはできるか

図 3.2- 46　Q6 の結果（n=17）

7. 標的型攻撃メールについて知っているか

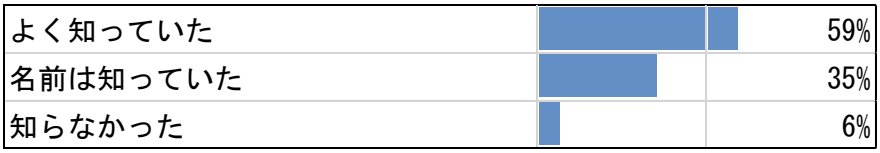

図 3.2- 47　Q7 の結果（n=17）

8. 今回の訓練で標的型攻撃メールに関する理解は深まったか

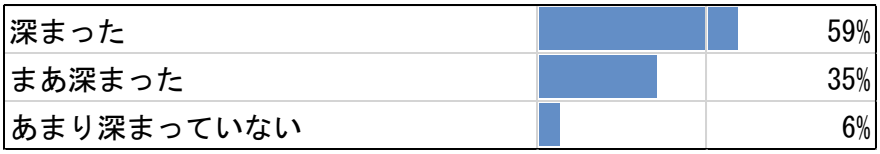

図 3.2- 48　Q8 の結果（n=17）

9. 標的型攻撃メール訓練は必要だと思うか

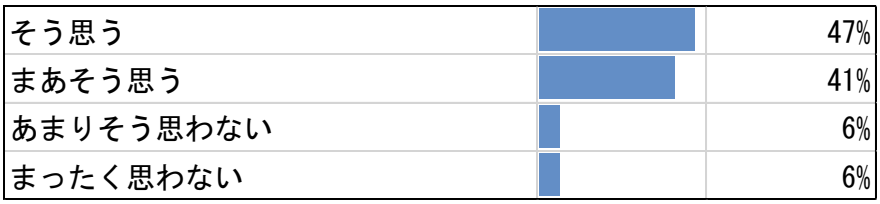

図 3.2- 49　Q9 の結果（n=17）

10. 今回の訓練についての感想等

- 抜き打ちテストは、今後も自分達が引っかからないためにも不定期に実施していただけるとありがたい。
- 以前も「標的型攻撃メール訓練」をほぼ全員に試したことがある。その時に、注意喚起をしたが、まだ怪しいメールを開く人がいる。
- 社員にもやらせたい
- 送信者名、社内メールなのに社名を入れている、そもそもパッチが古い等、メール内容が微妙におかしいところがリアリティを感じた。訓練時に参考にしたい。
- 試験メールと同時に対応方法まで予行演習があると良いと思う。
- 通販サービスや金融機関等を騙った同様のメールが最近頻繁に送られてくる。
- 職場内での啓発活動として、十分な意義があった。
- 会社としてこの種のメールは開けないように徹底しているので、そうでない会社には訓練の有

効性が高いと思うが、弊社の場合にはそういうものという認識をすることも難しかったと思う。
・ 不審なメールだったので、とっさに削除した。

訓練を実施した企業の情報セキュリティに対する認識が高いことから、インシデント時の対応率（連絡／ネットワーク切断等）が高く、また前向きな感想／改善要望が多い結果となったと考える。体験することで具体的なイメージができるようになるため、セキュリティに対する意識啓発ツールとしては一定の効果があると考えている。訓練視点では、予め従業員に対する教育の実施や対応体制の構築を行った後に、対象企業の実態に即した訓練内容を検討した上で実施すべきと考える。

また Emotet 等の流行で、標的型攻撃メール自体の見極めはより困難となっており、訓練の意義はメール見極めや開封率低減から、その後の連絡等の対応へ移行していると考える。

3.3 実証の実施結果

3.3.1 中小企業のセキュリティ診断

本実証事業では、以下 2 つ観点から、3 つのセキュリティ診断を実施した。

- 情報セキュリティの対策レベル

・ 3.2.2②情報セキュリティレベルの数値化（5 分でできる！情報セキュリティ自社診断）で記述のとおり、実証参加企業 53 社の情報セキュリティ対策に関する入門レベルについて、4 つのレベルで診断した。基本対策ができていない（49 点以下）企業は約 2 割であった（表 3.2-3 参照）。
・ 3.2.2③セキュリティ対策状況で記述のとおり、実証参加企業 53 社のより詳細なセキュリティ対策レベルについて 4 つのレベルで診断した。上記と比較すると、より詳細なセキュリティ対策レベルでは、約 7 割の企業でセキュリティリスクが高い状況にあると判定された（表 3.2-4 参照）。

- UTM モニタリングから見たセキュリティリスク

・ 後述する 3.3.3 中小企業のサイバー被害の実態把握において、UTM モニタリングのログ分析結果から、実証参加企業 36 社のセキュリティリスクについて診断した。UTM を設置した企業のうち 8 割以上の企業において、セキュリティリスクがあると判定された（表 3.3-3 参照）。

3.3.2 サイバーセキュリティに関する相談の受付および対応

表 3.3-1 に、本実証事業に関連するコールセンター対応およびインシデント対応等を示す。

対応種別	総計	相談・インシデント等対応状況	発生件数
コールセンター対応	7 件	実証参加に関する問合せ	0 件
		セキュリティ機器設置等の問合せ	2 件
		セキュリティ対応の相談	1 件
		その他	4 件
インシデント対応	1 件	電話およびリモートによるインシデント対応	1 件
		訪問によるインシデント対応（駆け付け）	0 件
その他訪問対応	5 件	機器設置等のトラブル対応	4 件
		その他(セキュリティ機器の導入･設置支援等)	1 件

表 3.3- 1　コールセンター対応およびインシデント対応等の状況サマリー

実証参加企業から連絡を受けたコールセンター対応は 7 件、詳細は以下のとおり。

- セキュリティ機器設置等の問合せ：リモートアクセス等の設定方法に関する問合せ
- セキュリティ対応の相談：Web フィルタリングに関する問合せ
- その他：ネットワークやメール送受信等に関する問合せ

電話対応によるインシデント対応は 1 件で、UTM 以外に起因する通信環境の不具合が原因であり、セキュリティ事故ではなかった。その他訪問対応は 5 件で、メール送受信や Web アプリケーションの使用に関するトラブル対応であった。

3.3.3 中小企業のサイバー被害の実態把握

(1) UTM のログデータ分析

期間中に発生した全セキュリティ・アラート結果を示す。各アラート種別の検知状況、サイバー攻撃の動向等の観点から、中小企業におけるサイバー攻撃被害の実態について報告する。

アラート種別	件数	説明	備考
①外部からの不正アクセス検知および防御（外→内）	17,958 件	外部からの不正アクセス通信を検知・遮断し、バッファーオーバーフローや SQL インジェクション等のソフトウェアやネットワークの脆弱性を突いた攻撃を防御	ping/port-scan の検知数
②内部不正プログラム検知および防御（内⇔外）	139,109 件	ボットネットとの通信等、マルウェア感染等による内部から外部への不正通信や不正プログラムが含まれる通信を検知、感染を早期発見し防御	内部からの不正通信履歴（内→外の IPS 検知ログ）
③不正サイトへのアクセスブロック（内→外）	364,413 件	内部端末から、予め登録したセキュリティ上のリスクがある不正サイトへの接続をブロック(URL フィルタリング)	コンテンツフィルタログ
④マルウェアの検知および無害化	6 件	メール添付ファイルや Web からのダウンロードファイルに含まれるウイルス、ランサムウェア、アドウェア等の検知と無害化	・メール受信 ・HTTP・FTP ウイルスチェック履歴
⑤スパムメールの検知	8,566 件	受信したメールに含まれるスパムメールの検知	スパムメール履歴

表 3.3- 2 UTM モニタリングの全セキュリティ・アラートの結果

①外部からの不正アクセス検知および防御（外→内）

- ping/port-scan

結果を、下図 3.3-1 に示す。調査期間中に外部から ping または port-scan によるアクセスを受けた回数は合計で 17,958 件（ping：15,945 件、port-scan：2,013 件）。UTM 端末 1 台で 1 日あたりに換算すると約 17 件/台となった。日別で多少のばらつきはあるが、大きな変動は見られなかった。

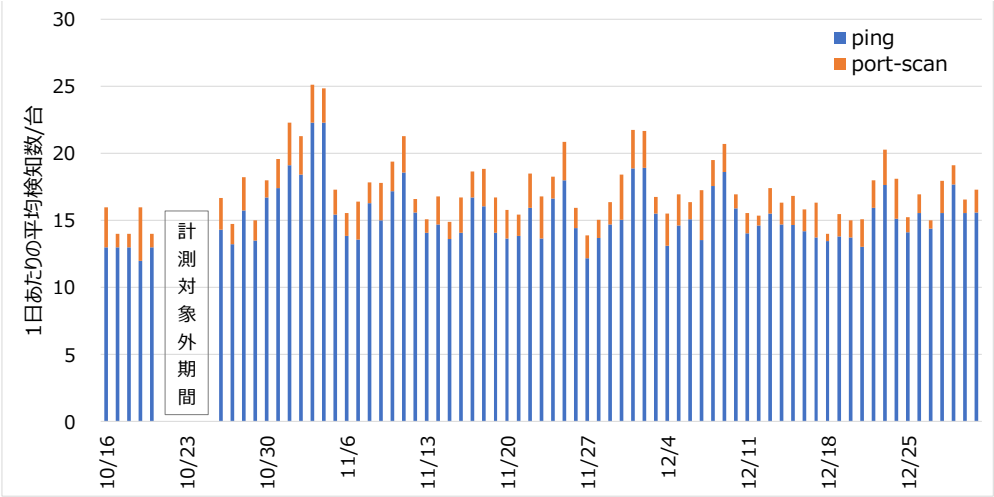

図 3.3- 1　ping/port-scan 履歴の日別データ

ping は 74 ヶ国からのアクセス履歴を検知。その大半は US（米国）、CN（中国）の 2 ヶ国からのアクセスであり、約 6 割を占めた（図 3.3-2 参照）。他方、port-scan は 35 ヶ国からのアクセス履歴を検知。US（米国）、RO（ルーマニア）の 2 ヶ国で、49%を占めた（図 3.3-3 参照）

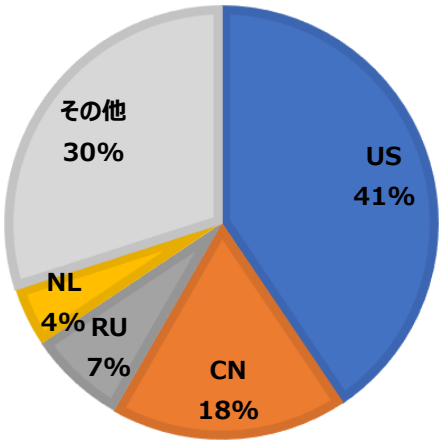

図 3.3- 2　ping の国別比率

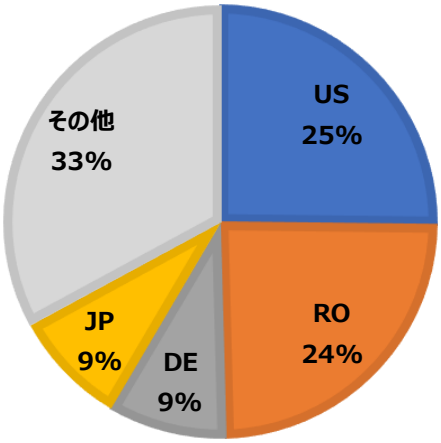

図 3.3- 3　port-scan の国別比率

②内部不正プログラム検知および防御（内⇔外）

・　不正通信履歴（IPS 検知ログ）

実証企業で検知した不正な通信検知数は合計で 139,109 件、1 日あたりに換算すると約 86 件/台となった。

不正通信の内訳を下図 3.3-4 に示す。今回検知した通信の約 8 割は、Dropbox の通信であった。会社情報を個人のアカウントに移して持ち出す等のリスクがあるため、社内ルールをしっかり整備した上で利用することが重要である。次に、Baidu IME の通信が 14%であった。意図せぬ情報送信で機密漏えいのリスクがあるとして、2013 年に内閣サイバーセキュリティセンター：NISC から注意喚起されている。昨年度実証事業と同じく、調査対象の約 1/3 にあたる 10 台から通信を検知しており、“意図しない情報送信”等のリスクがある状況といえる。また TeamViewer といったリモートアシスタンス（遠隔地の PC へ接続する通信）の信号も検知しており、情報漏えいのツールになり得る危険性があるため、注意が必要である。

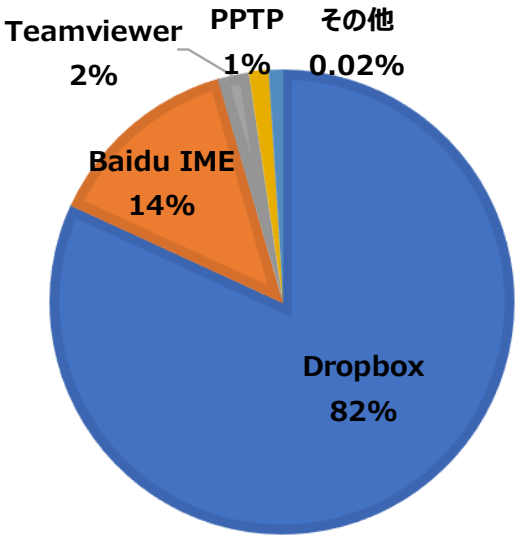

図 3.3- 4　不正通信（IPS）検知ログの内訳

③不正サイトへのアクセスブロック（内→外）

・　コンテンツフィルタログ

調査期間中にブロックした Web サイト数は合計で 364,413 件、1 日あたり約 191 件/台。危険性が高いと判断した（ブロック済み）コンテンツの内訳を下図 3.3-5 に示す。32%は SNS 利用であり、調査対象の約 1/5 にあたる 8 台からの通信であった。次いで 28%がオンラインストレージに対するブロックであり、調査対象の約 2 割にあたる 7 台から通信があった。また 18%は Web アプリケーション利用によるものであり、これら SNS やオンラインストレージ等へのアクセスは、業務上許可されていない場合は、内部不正や不注意による情報漏えいリスクが懸念される。

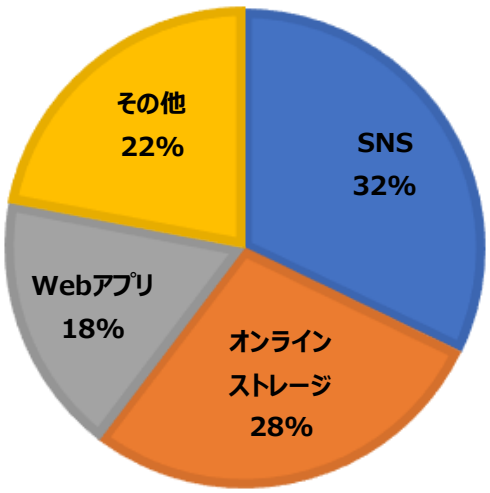

図 3.3- 5　コンテンツフィルタログの内訳

④マルウェアの検知および無害化

・　HTTP/FTP ウイルスチェック履歴

実証期間中の FTP/HTTP ウイルススキャンにより検知されたウイルスは 0 件。Web 経由でダウンロードされたウイルスは確認されなかった。

・　メール受信ウイルスチェック履歴

図 3.3-6 に、メール受信ウイルスチェック履歴の日別データを示す。

実証期間中のウイルスメール受信数は 6 件（約 0.01%、全メール受信数 75,330 件）。10 月に埼玉県で請求書を装うなりすましメールを 1 件、12 月には千葉県でウイルス感染している可能性のある報告書が添付されたメールが 3 日間に渡って同じ企業に送付されるのを確認、いずれも UTM でブロックした。こうした手口によるウイルスメールは昨年度実証事業でも複数件見られており、今後も注意が必要である。

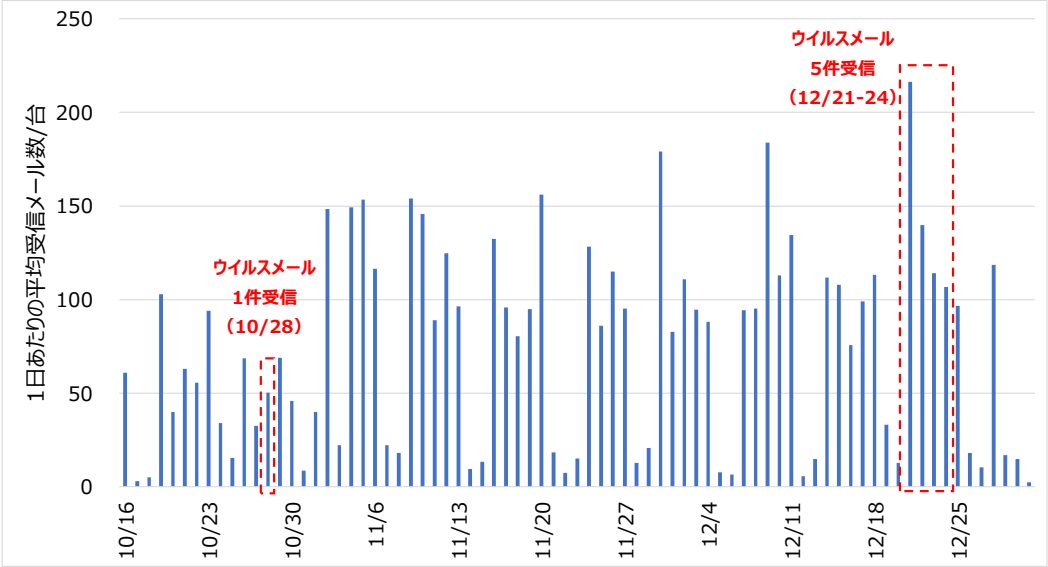

図 3.3- 6　メール受信ウイルスチェック履歴の日別データ

・　メール送信ウイルスチェック履歴

実証期間中のメール送信ウイルスは 0 件（全送信メール 10,269 件）。実証企業の社内 PC からのウイルス付きメール送信は確認されなかった。

⑤スパムメールの検知

・　スパムメール履歴

以下、スパムメールの判定履歴を示す。図 3.3-7 に示すとおり、調査期間中に受信したスパムメール数は、8,566 件（全メール受信数 75,330 件の 11%）であった。1 日あたり約 8 件/台のスパムメールを受信しており、日ごとのばらつきはあるものの、大きな傾向変動は見られなかった。

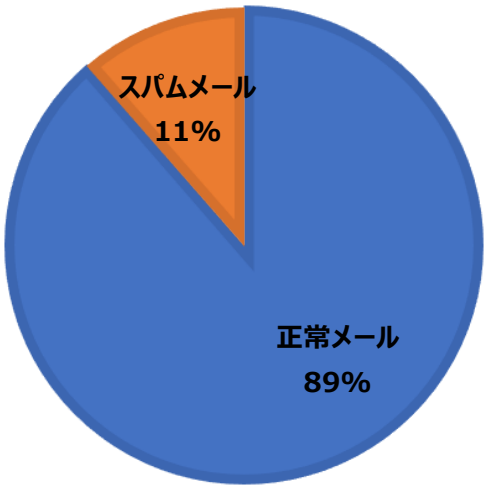

図 3.3- 7　受信メールに占める正常メールとスパムメールの比率

(2) 実証参加企業のセキュリティリスク診断

UTM のログから、実証参加企業のセキュリティリスクについて、以下の観点で診断した。

1. 期間中にウイルスを検知したか
2. 情報漏えいに繋がるリスクのあるツール（Baidu, Dropbox, P2P）を利用しているか
3. 情報流出に繋がるリスクのあるサイト（オンラインストレージ、SNS）へアクセスしているか

リスク	判定条件	実証参加企業の割合
高	1 に該当する	8%（3 社）
↑	2 かつ 3 に該当する	8%（3 社）
↓	2 または 3 に該当する	67%（24 社）
低	いずれにも該当しない	17%（6 社）

表 3.3- 3　UTM ログ分析から判定したセキュリティリスクの診断結果（n=36）

表 3.3-3 に示すとおり、今回の実証事業で UTM を設置した企業で 1、2、3 いずれにも該当しない企業は 2 割以下で、残りの 8 割以上の企業はセキュリティリスクがあると判定された。

(3) 脅威シナリオ

UTM のログ分析結果から、昨年度同様、中小企業においても以下のようなサイバー攻撃等の脅威に晒されていることを確認した。

脅威シナリオ	内容	頻度	影響度
標的型攻撃（なりすまし）による被害	企業や民間団体そして官公庁等、特定の組織から重要情報を窃取することを目的とした標的型攻撃。 攻撃者はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織の PC をウイルスに感染させる。その後、組織内部へ潜入し、組織内部の侵害範囲を拡大しながら重要情報や個人情報を窃取する。	低	関係する会社から情報が盗み取られた場合等、継続的に標的にされる可能性が高く、被害が大きく拡大する可能性が高い。
内部不正による情報漏えい	組織の従業員や元従業員等、組織関係者による意図的な機密情報の漏えい、悪用等の不正行為。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失等により、組織に多大な損害を与える。	高	クラウド等の利用により、外部に大量データを保持することがあり、そのデータ流出によっては、被害が大きくなる可能性が高い。
不注意による情報漏えい	情報管理に対する意識の低さや確認漏れ等に起因する、従業員による個人情報や機密情報の漏えい。漏えいした情報が悪用される等の二次被害も懸念される。	高	Web サービスに組み込まれている API から情報が窃取される可能性があり、信頼できるか否かの判断が随時必要である。

表 3.3- 4　本実証事業で確認した脅威シナリオ

3.3.4 サイバーインシデント対応

実証期間中のインシデント処理を表 3.3-4 に示す。

アラート種別	件数	インシデント対応	
		オンライン対応	オンサイト対応
①外部からの不正アクセス検知および防御（外→内）	17,958 件	全件ブロック	0 件
②内部不正プログラム検知および防御（内⇔外）	139,109 件	18,713 件ブロック（他は記録のみ）	0 件
③不正サイトへのアクセスブロック（内→外）	364,413 件	全件ブロック	0 件
④マルウェアの検知および無害化	6 件	全件ブロック	0 件
⑤スパムメールの検知	8,566 件	全件通知	0 件

表 3.3- 5　全インシデント処理

スパムメールは、自動判別結果を通知する処理、不正な通信やウイルスメール等は、通信をブロック処理（ポート遮蔽）もしくは記録処理（経過観察）をしている。どちらもオンライン対応が基本である。実証期間中、オンサイト対応（駆け付け支援）が必要なインシデントは発生しなかった。

3.4 報告会等による実証事業成果の周知

3.4.1 開催概要・結果

成果報告会の概要と結果を表 3.4-1 に示す。

開催日時	2021/1/13　14:00～15:30	2021/1/14　14:00～15:30
場所 **形態**	埼玉県 オンライン（Zoom）	千葉県 オンライン（Zoom）
協力	柏商工会議所	春日部商工会議所 所沢商工会議所
参加企業（人数）	18 社（19 人）	19 社（20 人）
アジェンダ	・ はじめに（開催挨拶）　5 分 ・ 実証事業実施結果（富士ゼロックス）　35 分 ➢ 本事業の取り組み概要 ➢ 中小企業の実態把握結果 ➢ 中小企業におけるサイバーセキュリティの脅威 ➢ 中小企業におけるサイバーセキュリティ対策 ・ 令和 2 年度中小企業サイバーセキュリティ対策促進事業のご紹介（経済産業省　関東経済産業局）　15 分 ・ 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）　15 分 ➢ SECURITY ACTION ➢ 中小企業の情報セキュリティ対策ガイドライン ・ その他（連絡事項、アンケート）　20 分	

表 3.4- 1　成果報告会の概要と結果

成果報告会では、以下の募集活動を実施した。
- 地域の商工会議所による募集（FAX、メルマガ、HP 掲載　等）
- 富士ゼロックス各販売会社の営業・カスタマーエンジニア（以下、CE）による個別訪問による募集
- 富士ゼロックスホームページによる告知
- IPA ホームページによる告知
- 地域の IT コーディネーターを通じた勧誘
- 本実証事業で協力関係にある損害保険会社（東京海上日動火災保険）を通じた勧誘

1/13 に埼玉県、1/14 に千葉県の企業を対象とし、新型コロナウイルス感染症対策を考慮し、オン

ラインによる成果報告会（Zoom）を実施した。2 回の説明会参加企業は合計 37 社（39 名）であった。

実証事業説明会同様、千葉県、埼玉県とも商工会議所の協力を得て、HP 掲載、FAX、メルマガ、チラシ配布等で各県下の中小企業へ幅広く開催を告知したが、報告会への参加企業数は、目標（20 社/回）の 9 割程度であった。

3.4.2 参加者の反応

報告会の参加者および実証参加企業への実証事業参加後アンケート結果（n=18）を以下に示す。

Q1. 報告会または本実証事業を通じて、サイバーセキュリティ対策の必要性を感じましたか。

図 3.4- 1　Q1 の結果（n=18）

Q1-1. Q1 で YES の場合、必要と感じるセキュリティ対策についてお聞かせください。（複数選択可）

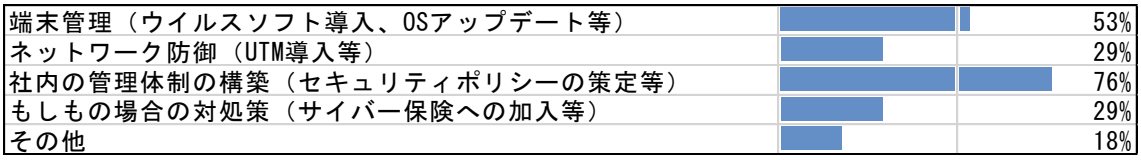

図 3.4- 2　Q1-1 の結果（n=17）

Q1-2. Q1 で YES の場合、セキュリティ対策にかけられる月額費用の上限をお聞かせください。

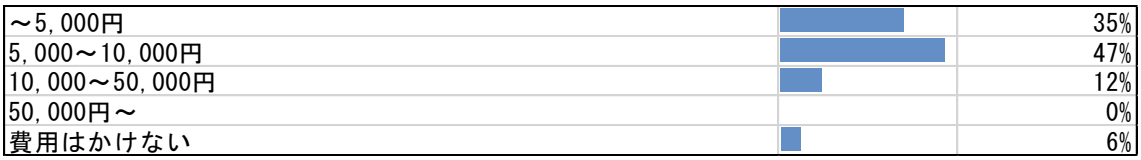

図 3.4- 3　Q1-2 の結果（n=17）

サイバーセキュリティの必要性を感じた企業は 9 割以上に達した。必要と感じた対策内容は、「社内管理体制の構築」が最も多く、次いで「端末管理」であった。「その他」は、パスワード管理、バックアップ等である。また、対策にかけられる月額費用の上限は、1 万円以内の回答が約 8 割を占めている。

Q2. 報告会または本実証事業に参加して、専門家等による外部支援の必要性を感じましたか。

図 3.4- 4　Q2 の結果（n=18）

Q2-1. Q2 で YES の場合、必要と感じる支援内容についてお聞かせください。（複数選択可）

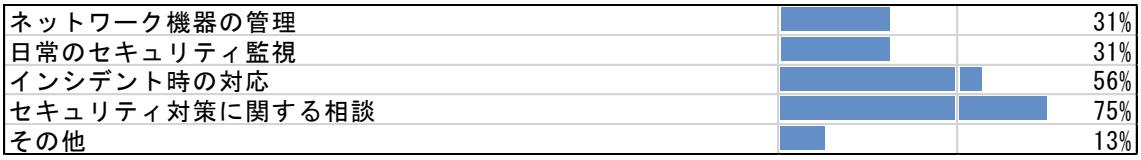

図 3.4- 5　Q2-1 の結果（n=16）

約 9 割の企業が専門家による外部支援の必要性を感じており、相談できる専門家の存在が重要であることが分かった。支援内容は「セキュリティに対する相談」が最も多く、次いで「インシデント時の対応」であった。「その他」は、セキュリティログの相談、定期的な研修や情報提供であった。

Q3. 報告会または本実証事業に参加して、サイバー保険の必要性を感じましたか。

図 3.4- 6　Q3 の結果（n=18）

Q3-1. Q3 で YES の場合、必要と感じる保険内容についてお聞かせください。（複数選択可）

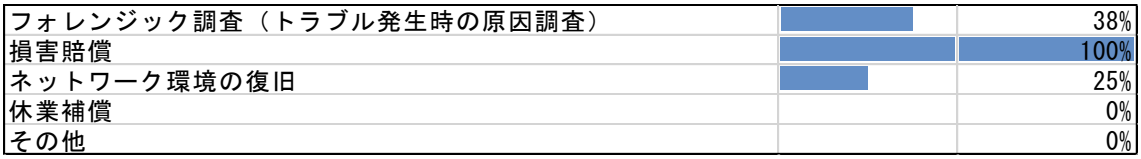

図 3.4- 7　Q3-1 の結果（n=8）

サイバー保険の必要性を感じた企業は約 4 割であった。必要と回答した全企業で、「損害賠償」を必要な保険内容として挙げている。

Q4. 取引先（業務委託元）から、セキュリティ対策を要求されたことがありますか。

図 3.4- 8　Q4 の結果（n=18）

Q4-1. Q4 で YES の場合、要求内容についてお聞かせください。（複数選択可）

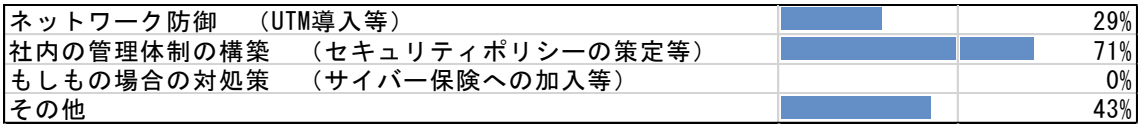

図 3.4- 9　Q4-1 の結果（n=7）

取引先からセキュリティ対策を依頼された企業は約 4 割であった。要求内容は「社内の管理体制の構築」が多く、「その他」は、Web サイトのセキュリティ対策、業務システムのセキュリティ対策等であった。

Q5. テレワークを実施している、または導入する予定がありますか。

図 3.4- 10　Q5 の結果（n=18）

Q5-1. Q5 で YES の場合、セキュリティ対策の課題についてお聞かせください。（複数選択可）

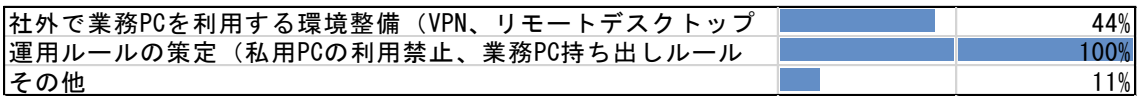

図 3.4- 11　Q5-1 の結果（n=9）

テレワークを実施、または導入予定の企業は半数であった。対策の課題としては、いずれの企業も「運用ルールの策定」を挙げている。

自由記述：

- サイバーセキュリティの取り組みについてとても参考になった。（千葉県教育学習支援業）
- セキュリティに関する自分の知らない知見が無料で得られた。（千葉県建設業）
- 自社のセキュリティレベルを客観的に確認できた。（埼玉県製造業、千葉県サービス業）
- サイバーセキュリティがどのようなものか理解できた。(千葉県生活関連サービス業・娯楽業)
- 多くの中小企業でセキュリティ診断調査をする機会が多くなってほしい。（埼玉県製造業）
- 社内規則の確認ができた。（千葉県教育学習支援業）

3.4.3 成果報告会での気づき

アンケート結果から、9 割以上の企業で“サイバーセキュリティ対策の必要性を感じた”との回答があり、本実証事業の報告内容については、中小企業のサイバーセキュリティに対する意識変革に繋がると確信した。

多くの中小企業で専門家等の外部支援を必要としていて、セキュリティ機器を設置するだけでは十分ではなく、伴走支援できる仕組みが必要である。

もしもの場合に備えるためのサイバー保険については、業種や情報システムへの依存度等のビジネス形態によるところが大きいと考えられる。本実証事業で実施した予想損失額シミュレーション等を通して、保険の必要性について一定の訴求効果はあったと考えている。

重要性を認識しても「何から取り組めばいいか分からない」という中小企業の声はまだ多いため、サイバーセキュリティに対する意識変革を促す必要がある。具体的な取り組みとして、IPA が公開している SECURITY ACTION（一つ星：情報セキュリティ 5 か条、二つ星：情報セキュリティ自社診断）等を浸透させていく活動を、地域側の支援体制も含めて官民協業で進めていくこと等が重要である。

4. 考察

実証事業を通じた考察を以下に示す。

4.1 実証参加企業におけるサイバー攻撃の実態

実証参加企業へのサイバー攻撃の実態について整理する。

本年度の実証事業期間（2020 年 9 月からの約 4 ヶ月間）では、富士ゼロックスが担当した実証企業でのセキュリティ事故に関するインシデント（Web 改ざん、DDoS 攻撃、ウイルス感染等）は発生していない（2021 年 1 月 10 日時点）。しかしながら設置した UTM モニタリングでの分析結果を見ると、ポートスキャンやウイルスメール受信等の外部からのサイバー攻撃については、昨年度と同程度に多く発生しており、常にインシデントは起こりうる状態にあるといえる。

また、外部通信を記録した IPS ログやコンテンツフィルタログを見ると、利用に注意を要する Web サイトとの交信が発生しており、経営者や管理者が意図しない方法で利用されている場合は、利用者の情報が第三者へ流出している（抜き取られている）可能性について疑われる。このような状況は、近年の Web サービス（業務アプリケーション、業務クラウド）の利用拡大の中では避けられないため、実際の利用方法等については利用者側で細心の注意を払うことが必要である。

一方、標的型攻撃等の巧妙な手口によるウイルス感染や情報窃取については、中小企業の現場での判別が極めて難しいため、政府のサイバーセキュリティ機関や民間のセキュリティベンダーからの情報提供に頼ることになる。関連企業の被害状況等にも注意を払いながら対策を講じる等の自衛策が求められる。

4.2 中小企業におけるセキュリティ対策を進める上での課題

本実証事業で得られた結果を基に、中小企業における課題について整理する。

4.2.1 IT 専門人材の不足

中小企業には、IT 環境（端末、ネットワーク、アプリケーション等）を管理できる人材が足りていない。実証参加企業でも、実態調査の段階で IT ネットワークやセキュリティ管理に時間を割けないという現場担当者も多く、本実証事業で派遣した IT コーディネーターの支援が必要と回答する企業が多くあった。

4.2.2 サイバーセキュリティ対策に関する知識不足

日々進化するサイバー攻撃に対して、本実証事業でアプローチした企業からは「サイバー攻撃を受けていることの実感がない」「被害を受けたとしても業務への影響は小さい」という回答が見られる等、中小企業側の危機意識は依然として十分とはいえない。原因としては、中小企業の知識不足があり、サイバーセキュリティ分野の動向、自社が受けている外部からのサイバー攻撃の実態について把握できていない状態といえる。サイバーセキュリティに関する情報が、中小企業に行き届いていないことの現れであり、中小企業が自分事としてサイバーセキュリティ対策の必要性を感じるよう、引き続き情報提供していく必要がある。

4.2.3 クラウド利用の拡大への対策遅れ

OneDrive やDropbox 等のファイル共有サービス等、中小企業でのクラウド利用率が高まっている。取引先からの要請や他企業での実績等を理由に利用している企業もあるが、自社での管理体制の策定等が不十分なままに利用しているケースが多いと考えられる。近年では、定期的なデータバックアップをクラウド上に配置する等のプライベートクラウド的な利用も増えており、通信データ量も膨大になるため、必ずしも会社側で管理しきれないことを前提にした対策が求められる。

4.2.4 リスクを軽視した不適切な運用

スマートフォンや SNS の利用普及により、中小企業の職場には通信可能な個人端末が持ち込まれるケースが増えているが、それらを管理する人的リソースがないのが中小企業の実態である。結果、社内ネットワークに個人端末が接続されることになり、業務に関係のない Web サイトへのアクセスや Web サービスが利用されることで、社内ネットワークがウイルス感染する等のリスクとなる。他で感染した端末が職場に持ち込まれた結果、それが感染源となる例もあるため、厳密なガイドライン等を整備する必要がある。

4.2.5 インシデント発生に対する準備不足

もしものインシデント発生を想定して、その被害を最小限にくい止めるための対策検討ができている中小企業は非常に少ない。現在保有している情報資産がどのくらいあるか、顧客の個人情報が流出する危険性はないか、業務停止での取引先への影響はどのくらいか、原因調査からネットワーク復旧の費用はどのくらいかかるか等、個別の中小企業では対応しきれない多くの検討項目があり、外部の専門家の支援は不可欠といえる。

4.3 中小企業において必要なセキュリティ対策

中小企業の現状課題（4.2）を踏まえて、本実証事業で検討したセキュリティ対策と実証参加企業での結果について記載する。

4.3.1 専門家派遣による理解促進と伴走支援

IT 専門人材の不足（4.2.1）およびサイバーセキュリティ対策に関する知識不足（4.2.2）の課題解決を目的に、地域で活動している IT コーディネーターを実証参加企業へ派遣し、専門家と実証参加企業との直接対話できる機会を設けることで、理解促進と伴走支援を推進した。

結果、実証参加企業の相談相手として、理解不足を補うことができ、多くの実証参加企業から高い評価を受けることができた。一方で、実証参加企業の個別状況（業務内容、情報資産、IT ネットワーク環境、セキュリティ体制、経営者や担当者の知識や理解レベル等）に合わせて、サイバーセキュリティ対策を最適化する伴走支援には、多大な時間（1 社あたり数日を要する）がかかることが分かった。今回の実証事業期間では、各社で重点すべきセキュリティ対策についてアドバイスする支援に留まった。

4.3.2 事前診断プログラムの提供

サイバーセキュリティ対策に関する知識不足（4.2.2）、リスクを軽視した不適切な運用（4.2.4）およびインシデント発生に対する準備不足（4.2.5）の課題解決を目的にしてセキュリティ対策、およびサイバー保険設計に必要となる事前診断プログラムを提供した。具体的には、IT ネットワークやサイバー攻撃に詳しくない中小企業でも対応できるように、実態調査の質問票を再設計した。また、実証参加企業の個別状況に合わせて、サイバー攻撃による想定損害額をシミュレーションできる Web ツールも提供した。

結果、実証参加企業が回答しやすくなり、セキュリティ対策に必要となる情報収集については一定の成果を得ることができた。一方で、事前診断プログラムの実施については、実証参加企業まかせにすることの困難性も見えてきた。理由は、担当者の知識不足やモチベーション欠如があり、事前診断の質問項目に回答できる内部情報を持ち合わせていないという実情がある。

4.3.3 UTM モニタリングレポートを通じた理解促進と必要性訴求

サイバーセキュリティ対策に関する知識不足（4.2.2）、クラウド利用の拡大への対策遅れ（4.2.3）およびリスクを軽視した不適切な運用（4.2.4）の課題解決のため、実証参加企業への UTM モニタリングレポートを通じて、サイバー攻撃の実態に関する理解の訴求と個別状況に応じたセキュリティ対策の必要性の訴求を実施した。

結果、UTM モニタリングレポートで、実証参加企業が受けている個別のサイバー攻撃の実態を可視化、企業ごとにセキュリティ対策の必要性を訴求することができた。一方で、近年増えているクラウド利用の拡大に伴うセキュリティ対策の遅れやリスクを軽視した不適切な運用についての実態把握はできたが、具体的な対策については課題が残った。今後、管理リソースが不足している中小企業の実態に合った具体策を検討する必要がある。

4.4 中小企業におけるセキュリティ対策の効果

4.3 での実証結果を踏まえて、セキュリティ対策で期待される効果について記述する。

4.4.1 自己診断＆学習プログラムへの進化

外部からの一時的支援のままでは、時間的かつ金銭的な面で限界がある。本実証において、IT コーディネーターによる専門家派遣および事前診断プログラム提供等で中小企業側のサイバー攻撃の理解促進、危機感の醸成とセキュリティ対策の必要性訴求、具体策検討に繋がる事前プログラム診断により一定の成果は得られているが、さらなる効果のためには、自己診断＆学習プログラムへの進化が必要であると考える。

今後、診断する側の情報取得を目的にするだけでなく、調査される側が（質問項目や解説を通して）自ら学び進められるようにすることが重要である。調査される側がサイバー攻撃への危機感を高め、セキュリティ対策に取り組めるように促す等、中小企業側にとっての自助努力の範囲を最大限に拡大させる仕掛けにしていく必要がある。Web での学習プログラムにすることで、知識レベルに応じたステップ教材を用意すること、業界別の事例を紹介すること等も、学習効果を高める施策として追加することが好ましいと考えている。

4.4.2 モニタリング結果と対策提案の連動

UTM モニタリングレポートを通じた理解促進と必要性訴求については、中小企業ごとに実態把握等の効果が期待できるが、測定結果を理解するレベルで留まることが課題である。「現状から追加施策が必要である」「求めるレベルに対して必要な施策を提案する」等、結果に応じた対策を提案できることが望ましいと考える。

現状、診断結果を基に中小企業と面談し、個別で追加すべきセキュリティ対策を検討するには専門家を必要とするが、支援パターンを学習させたエキスパートシステム（人工知能）等を構築できれば、モニタリングレポートから対策提案までを連動させることが可能になると考える。さらには、地域での専門家育成および専門家派遣のための予算確保という問題解消にも繋げられる。

4.4.3 伴走支援する外部リソースの活用

本実証事業活動を通じて、IT コーディネーター等の専門家による伴走支援を求める中小企業側の要請に対応することも重要である。理由は、従業員が少ない企業では、IT ネットワーク環境やセキュリティ対策へ選任を配置することは極めて難しく、たとえ初期に万策を講じたとしても、システムの老朽化や巧妙化する外部攻撃には対応できなくなるためである。

外部リソースによる伴走支援（アウトソーシング）は、中小企業側の経済的負担が大きな問題となるため、IT ベンダーが、総合的なセキュリティ対策までを組み込んだサービスを提供することが理想である。不足する対策（もしもの場合の対策、損害補償等）については、サイバー保険を組み合わせ設計することで、中小企業側の費用負担を最小限にすることが期待されている。

5. 実証を踏まえたビジネス化に向けた検討

本実証事業で得られた結果を基に、実証を踏まえた中小企業等向けのサイバーセキュリティ対策支援サービスのビジネス化について検討する。

5.1 サイバー保険の活用

サイバー保険のあり方、マーケティング方法について報告する。

5.1.1 サイバー保険のあり方

近年、サイバー攻撃は手口が巧妙化しており、強固なセキュリティを構築してもサイバーリスクを完全に排除することは困難である。今後は人工知能等を悪用することで、攻撃件数はさらに増加することが懸念されており、中小企業においてもセキュリティ事故は必ず起こりうるという認識のもと、インシデント発生時の対処方法、費用、（自社が加害者となってしまう場合の）責任範囲、等についての検討が急務となっている。

中小企業の経営を圧迫しない保険料で留めるためには、企業ごとの個別リスクに応じた保険適用が必須であると考える。必要最小限の賠償のみを保険でカバーするという基本思想のもと、企業ごとに個別に検討していく。具体的には、事業規模、業務内容、保有している情報資産、等についての情報を棚卸し、シミュレーションによる最適化等を行い、サイバーリスクに対応できるようにする必要がある。

また、分かりやすいリスクアセスメントへ修正することの重要性も明らかになってきた。実際、今回の実証では通常のサイバー保険加入時に利用されている質問票や Web での損失額シミュレーションツールを提供したにもかかわらず、自力で実施できた実証参加企業はわずかであり、一般的な中小企業には取り掛かり難いという声が多くあった。中小企業側の知識不足の問題も含まれるが、セキュリティ対策サービスを提供する IT ベンダーと共同して、保険プログラムを再設計していくのが好ましいと考える。

具体的には、UTM 等の製品付帯として、基本的な保険を提供することが重要であると考える。製品付帯とすることで、製品を提供する IT ベンダー側で、お客様の知識レベルに応じた対応がとりやすくなると考える。また、製品側に UTM のようなモニタリング機能が存在することにより、お客様側でのネットワーク利用状態の経時変化を追跡でき、外部からの攻撃レベルが高まる（リスクが高くなる）状態になったタイミングで、追加となる保険プログラムへ移行させる等の検討が可能になる。

5.1.2 サイバー保険のマーケティング方法

サイバー保険のマーケティング方法は、業界団体やサプライチェーン単位での対策導入が効果的であると考える。自社だけでなく、サプライチェーンの関係先からの拡散被害が増加していること、その対策として取引先規定にセキュリティ要件を取り込む動き等があるためである。一般的に、セキュリティ被害は自社だけでないという認識が高まっており、業務の関係先を含め、共通してセキュリティ対策レベルを高めることが、極めて有効であると考える。また、取引関係性の中で対策レベルを共通化させることにより、保険でカバーすべき内容についてのガイドラインが作成されることで、中小企業での判断を容易にできる効果も期待できる。

業界団体やサプライチェーン単位での動きを誘導するには、国レベルでの政策として流れを作っていくことが不可欠である。様々な業界が同時進行で検討を始めることで、中小企業にも波及し得る大きな経済効果になるということが重要であり、中小企業が自主的にセキュリティ対策に取り組み、サイバー保険の加入増にも反映されていくことが期待できる。

また、5.1.1 で言及したセキュリティ関連商品付帯での保険提供も効果的なマーケティング策である。近年、中小企業においても IT ツール・製品は必須要件になっているため、それらを提供する地域の IT ベンダーとの連携により、全国の中小企業をカバーできるようになる。課題としては、中小企業の費用負担が少なく、製品付帯として最大限の保険内容が組み込まれるようにすることであり、中小企業側で手がかからないマネージドサービスの実現が期待される。

5.2 中小企業向けセキュリティビジネス化に向けた課題・検討

中小企業の実態に応じたセキュリティサービスの支援内容やマーケティング方法について報告する。

5.2.1 中小企業等の実態やニーズに応じたセキュリティ対策サービスの内容（対応範囲や費用等）

今回の実証を通じて、多くの中小企業で「セキュリティ対策の必要性は理解しているものの、どのように実施すれば良いのか分からない」という苦手意識の強さが明白になった。そのため、これからの中小企業向けセキュリティサービスでは、できる限り中小企業側の手を煩わせないマネージドサービスを提供するのが好ましいと考える。具体的には、図 5.2-1 に示すようなセキュリティ機能全体をプラットフォームにして、不足している専門人材やスキルの補完、整備が遅れている IT 環境のケア、通信状況の常時監視、インシデント発生時の対応等を、各中小企業の必要性に応じて提供できる仕組みである。プラットフォーム全体としてコストを下げるビジネススキームを実現させていくべきと考える。サイバー保険適用部分については、セキュリティプラットフォームでカバーする基本保険と、損害保険会社に受け渡す任意保険とを連携させるスキームを組み合わせる予定である。

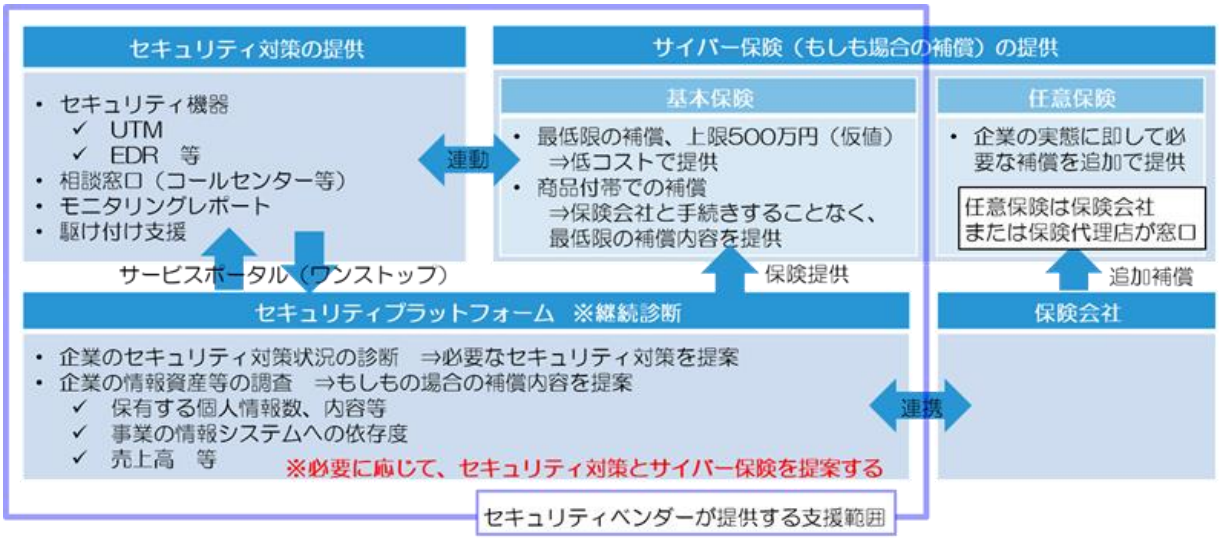

図 5.2- 1　中小企業向けのセキュリティ対策支援サービスの実現イメージ

- セキュリティプラットフォーム
  企業のセキュリティ対策状況、保有する情報資産等を簡易診断し、実態に即したセキュリティ対策とサイバー保険を提案する
- セキュリティ対策の提供
  診断結果に応じて、企業ごとに必要なセキュリティ対策を提供する
- サイバー保険（もしもの場合の補償）の提供
  基本保険…最低限必要な補償（フォレンジック調査費用や賠償責任等）のみを低コストで提供する。商品付帯としてセキュリティベンダーが提供することで導入しやすくする
  任意保険…企業ごとの状況に応じて必要な補償内容を追加で提供する（窓口は損害保険会社または保険代理店）

上記の支援サービスを構築するため、サイバー保険に関する補償内容等について、引き続き検討していく計画である。実証終了後は、以下の支援内容からのスモールスタートを予定している。

・セキュリティ対策状況等の簡易診断と対策の案内
・UTM によるセキュリティ対策
・UTM 障害発生時のオンライン・オンサイト（駆け付け）対応
・費用は 1 万円以下／月　※最小構成での費用、別途オプション機能あり

5.2.2 中小企業等の実態やニーズに応じたマーケティング方法や支援体制

マーケティング方法は、セキュリティプラットフォームを前面にしたマネージドサービスで、中小企業側に訴求していくのが好ましいと考える。IT ツール等の導入によりセキュリティを担保しようとする旧来型サービスではなく、中小企業側で不足しているセキュリティ機能を必要に応じて補完する、セキュリティサービスサプライヤーとしてのブランド化が重要と考える。

5.2.3 実証終了後の中小企業等向けサイバーセキュリティ対策支援サービス提供の可能性

マネージドセキュリティサービスのプラットフォームとして、図 5.2-2 に示した「IT Expert Service」を検討している。中小企業側で IT 人材への投資をせずに、効果的な IT 活用を加速させることを狙いにしている。

現状のシステム構成や運用ルール等を明確にした上で、中小企業の課題を特定し、最新テクノロジーや業界のトレンドを十分に考慮したセキュリティ対策の導入計画を立案する。日常的な問合せを担当する Service Desk に加え、IT インフラのメンテナンスとリモート監視・復旧を行う NOC により、障害発生時にも迅速な対応を実現させる。また、セキュリティ監視状況や IT 運用の情報を基にサイバー攻撃からの防御レベルを定期レビューし、その継続的改善までを担うことによって、中小企業の活動の安心・安全を確保することができると考えている。

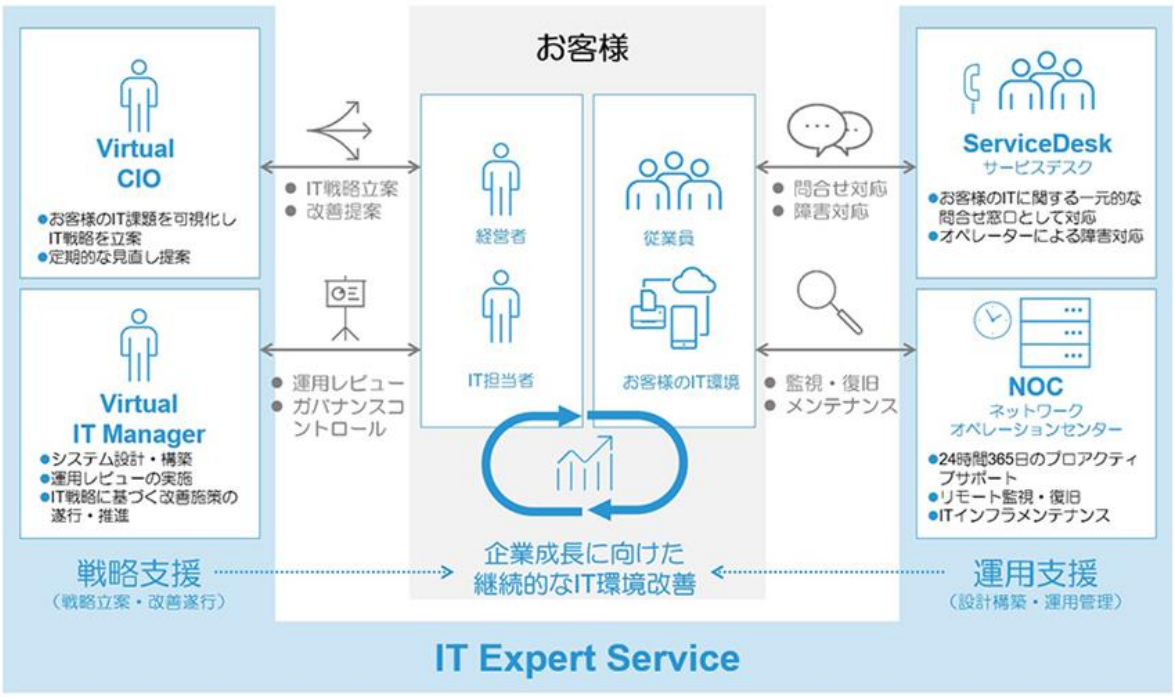

図 5.2- 2　IT Expert Service の概要