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：長野県、群馬県、栃木県、茨城県、埼玉県）

成果報告書

請負事業者：富士ゼロックス株式会社

目次

概要

本事業は、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、中小企業のサイバーセキュリティ対策支援（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に関する悩み、対策のニーズ、サイバー攻撃・被害の実態等を把握するとともに、中小企業が必要とするサイバーセキュリティ製品・サービスの再定義、インシデントが発生した際の支援体制等を検討するための実証事業である。

富士ゼロックス株式会社（以下「富士ゼロックス」という。）は本事業請負事業者として活動したので、以下に事業完了を報告する。

1.1 はじめに

近年、サイバー攻撃の手法は進化しており、中小企業においても、リスクマネジメントの一環として捉え、サイバーセキュリティの意識啓発や対策整備を進めなければならない。

1.1.1 背景

2018年7月閣議決定のサイバーセキュリティ戦略で指摘されているように、IoTやAI技術により“Society5.0”“Connected Industries”が加速的に実現されつつある。サイバー空間がフィジカル空間のビジネスへ及ぼす影響も大きくなり、様々な産業領域においてサイバーセキュリティ対策整備が必須要件になりつつある。しかしながら中小企業においては、サイバーセキュリティ対策整備が未だ不十分であり、中小企業の経営者および社員の意識改革、更にはサプライチェーン全体への影響に配慮した検討や対策徹底が求められる。

1.1.2 目的

本事業の目的は、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浸透・定着させていくことである。

活動内容は、以下の通りである

１）中小企業でのサイバー攻撃、サイバーセキュリティ対策の実態把握

２）中小企業向けサイバーセキュリティ事後サービス検討

1.1.3 実証プロセスの流れ

下図1.1-1に、本事業での実証プロセスを示す。説明会開催による意見交換、アンケート回答集計などでの実態把握および通信ログ分析結果から、中小企業が晒されているサイバー攻撃の脅威シナリオを見出す。その脅威シナリオ対策として、中小企業での課題・ニーズを明確にした後に、地域側での基盤整備の必要性、セキュリティ製品・サービスの進化、保険プログラムの開発必要性などについて検討し、考察・提言を行う。

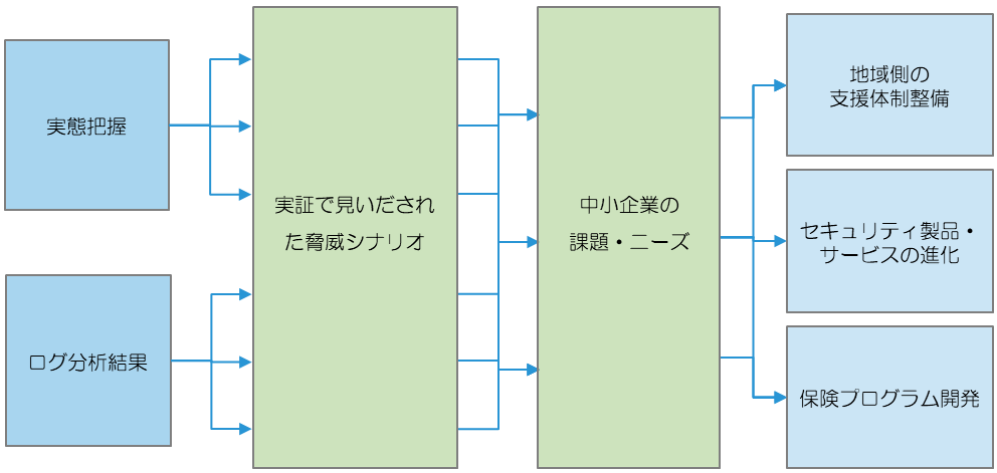


図 1.1-1　本事業での実証の流れ

1.2 事業内容

1.2.1 活動ステップ

本事業は、下図1.2-1に示す4つのステップで実施した。

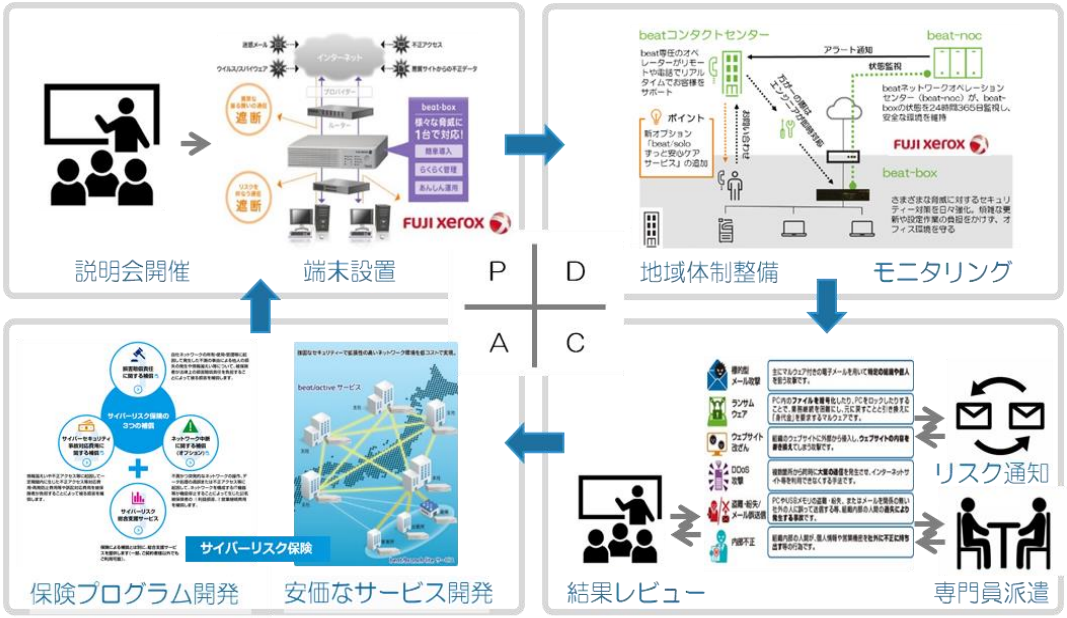


図 1.2-1　本事業での活動実施内容

【本事業の4つのステップ】

①事業説明会の実施と実証企業の募集、UTM端末設置（Plan）

②モニタリングの実施、リモートでの監視・管理等の支援体制整備（Do）

③ログ分析評価、インシデント対応、結果報告会などの開催（Check）

④脅威シナリオ等の考察および中小企業向け製品サービスの検討（Action）

①事業説明会の実施と実証企業の募集、UTM端末設置

実証企業を募集する目的で、各県下で事業説明会を実施。経済産業省関東経済産業局、自治体や商工会議所等への協力要請、富士ゼロックス販売会社からの訪問説明、テレアポ（電話勧誘）等を実施することで、中小企業へ広く声掛けを行った。実証企業には、随時UTM端末設置を進めて、通信ログのモニタリングを始めた（※UTM：Unified Threat Management）。

②リモートでの監視・管理等の支援体制整備

24時間365日遠隔監視するネットワークオペレーションセンター（以下、noc）とコンタクトセンターにより、リモートでの監視・管理を実施。通信ログデータを収集し、各社ごとのログ分析結果を通知、必要に応じて遠隔サポート、スタッフ派遣を実施した。PC等の使用状況、管理体制、セキュリティ対策の情報を収集し、発生事象に応じた再発防止策についての検討を進めた。

③ログ分析評価、インシデント対応、結果報告会などの開催

実証中に発生した重大リスクについては、原因究明に向けて追跡調査を実施し、実証企業やセキュリティに関心のある中小企業等へ情報提供するために、中間報告会および最終報告会を開催した。その際に、中小企業におけるサイバーセキュリティ対策の課題や具体的要請について、参加者との意見交換を実施した。

④脅威シナリオ等の考察および中小企業向け製品サービスの検討

③で得られた情報をもとに、中小企業が晒されているサイバー攻撃による脅威シナリオを立案した。サイバーセキュリティ対策に求められる課題や具体的要求を明確化。サイバー保険も含めた今後のサイバーセキュリティ製品・サービスの在り方についての検討を進めた。

1.2.2 本事業で対象とする地域

本事業の対象地域は、茨城県、栃木県、群馬県、長野県、埼玉県の5県とした。事業開始時点（6月）では、茨城県、栃木県、群馬県、長野県の4県を対象としたが、9月時点で埼玉県を追加地域とした。選定理由については下記に示す通りである。

茨城県、栃木県、群馬県、長野県の選定理由

北関東甲信地域4県には、生産製造拠点や技術開発拠点としている企業およびサプライチェーンが多く存在し、サイバーセキュリティ対策の必要性が高い地域と判断した。さらに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とする）拠点網を活用して、参加企業を募ることが十分可能であると判断し、実証対象地域として選定した。

埼玉県を追加した理由

埼玉県はサプライチェーンのコア企業が多く、前出地域と同様にサイバーセキュリティ対策が必要な中小企業が集積していること、事業開始後に埼玉県の中小企業から本事業への問い合わせが数多くあったこと等の理由から、本事業のニーズが高いと判断し、早期の目標達成、効果的な実証実現に向けてIPAに地域追加申請を行い、9月より埼玉県での事業実施の許可を得た。

1.3 本事業でのセキュリティ対策

以下、本事業のセキュリティ対策において採用した製品やサービスおよびリスク検知の方法等について説明する。

1.3.1 使用するUTM端末

本事業で使用するUTM端末は、富士ゼロックスの商品・サービスである“beat”を採用した。さまざま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。同端末は、中小企業向けに国内で開発製造されたものであり、すでに多数の中小企業に採用されている。

※“beat”機能詳細は、別紙：各種データ・資料に掲載した説明を参照

1.3.2 UTM端末の監視機能

UTM端末“beat”の主な機能は以下の通り。

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

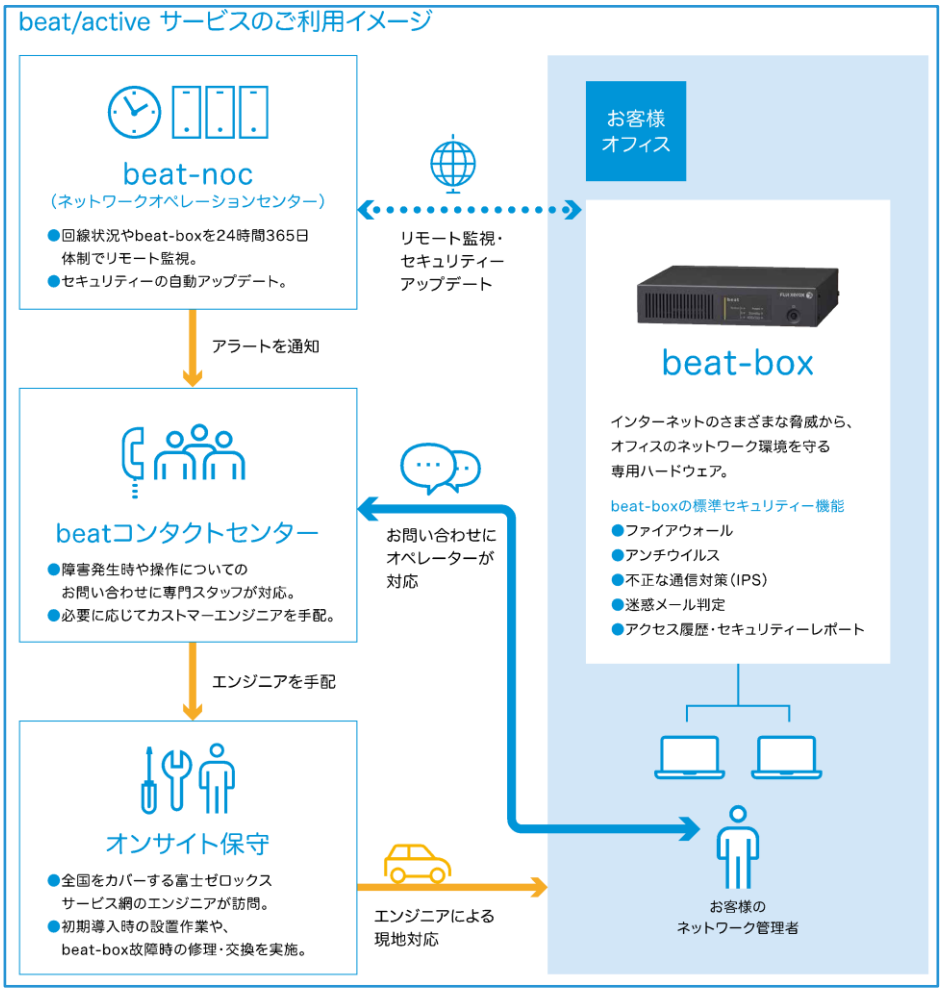


図 1.3- 1　設置するUTMが提供するセキュリティ機能（利用イメージ）

1.3.3 監視レポート配信

UTM端末の監視機能により収集したデータ結果は月次で集計・分析し、グラフ等で可視化したレポートを実証企業ごとに提供した。

1.3.4 エンドポイント管理機能

エンドポイント管理を実施として“beat”のオプション機能である“ITあんしんサポート”を提供した。ネットワーク上にあるパソコンなどの情報資産の管理実態について調査した。

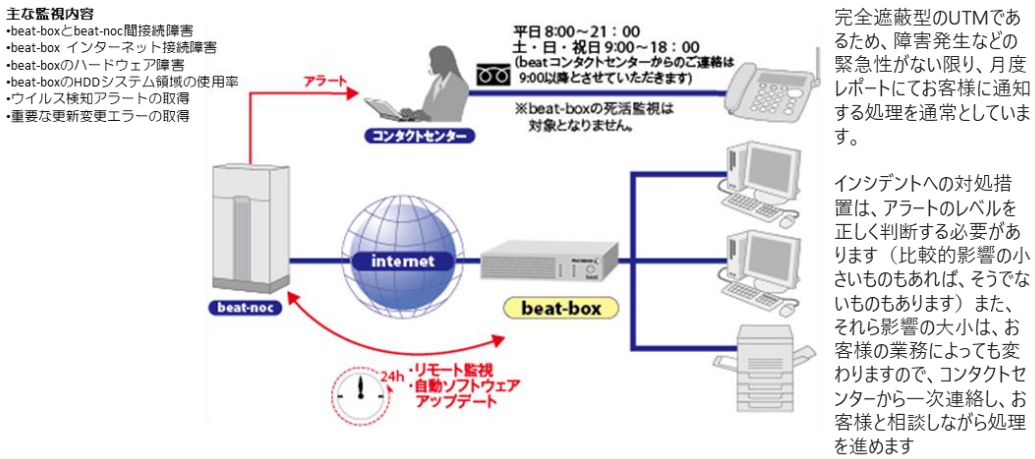
1.3.5 インシデント処理

下表1.3-1に、インシデント発生時の一次措置を示した。本実証に用いた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
不正な通策（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、シグネチャ毎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。ウィ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つけて通過（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 1.3- 1　インシデントへの一次措置

二次措置は（下図1.3-2）、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。



完全遮蔽型のUTMであるため、障害発生などの緊急性がない限り、月度レポートにてお客様に通知する処理を通常としています。

インシデントへの対処措置は、アラートのレベルを正しく判断する必要があります（比較的影響の小さいものもあれば、そうでないものもあります）また、それら影響の大小は、お客様の業務によっても変わりますので、コンタクトセンターから一次連絡し、お客様と相談しながら処理を進めます

図 1.3-2　インシデント対応の流れ

1.4 活動スケジュールと支援体制

1.4.1 事業期間

本事業は、2019年6月より2020年１月末までの約８か月間を活動期間とした。

1.4.2 活動スケジュール

当初の活動スケジュールを、下図1.4-1に示す。

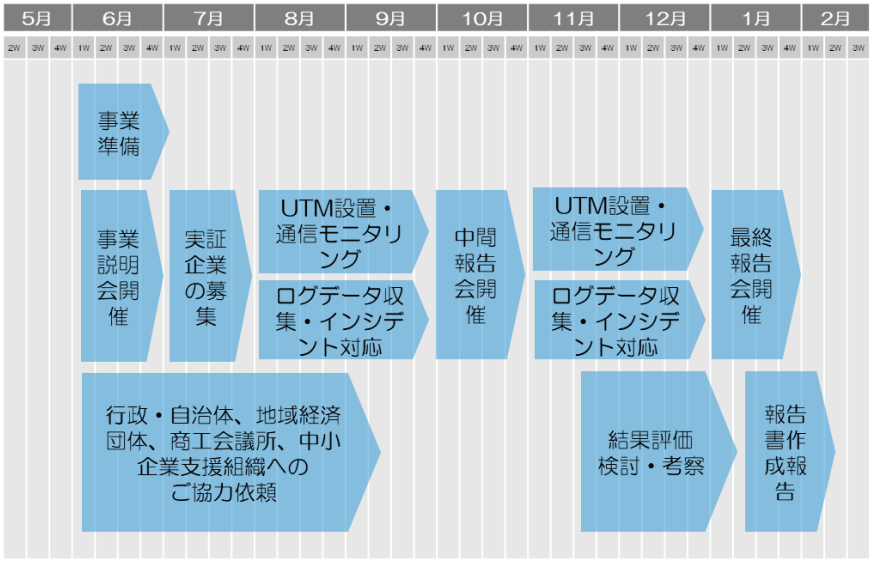


図 1.4- 1　活動スケジュール（計画時、変更前）

実際の活動では、実証企業の募集活動が11月まで長引いたため、下図1.4-2の活動スケジュールで進めた。募集継続しながらも、段階的にUTM設置・モニタリング、ログデータ評価・インシデント対応、報告会開催（中間・最終）結果評価・考察等を進める方式とした。

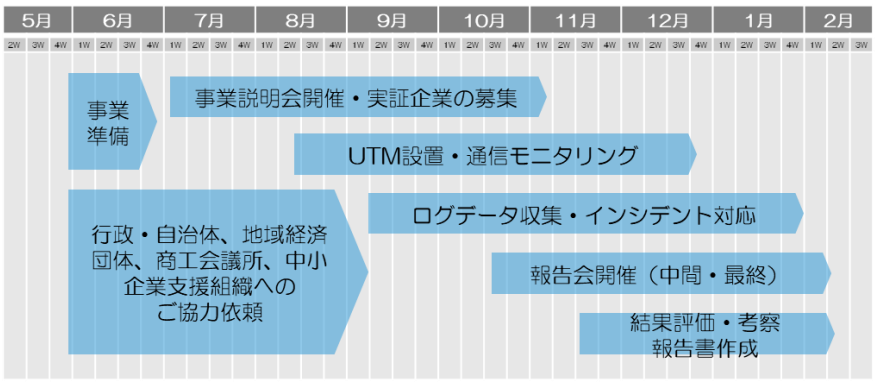


図 1.4-2　活動スケジュール（実績、変更後）

1.4.3 支援体制の構築

下図1.4-3に、実証企業への支援体制図を示す。実証企業からの相談受付および対応、インシデントか否かの判断、インシデント発生時の支援活動、という3段階での対応とした。

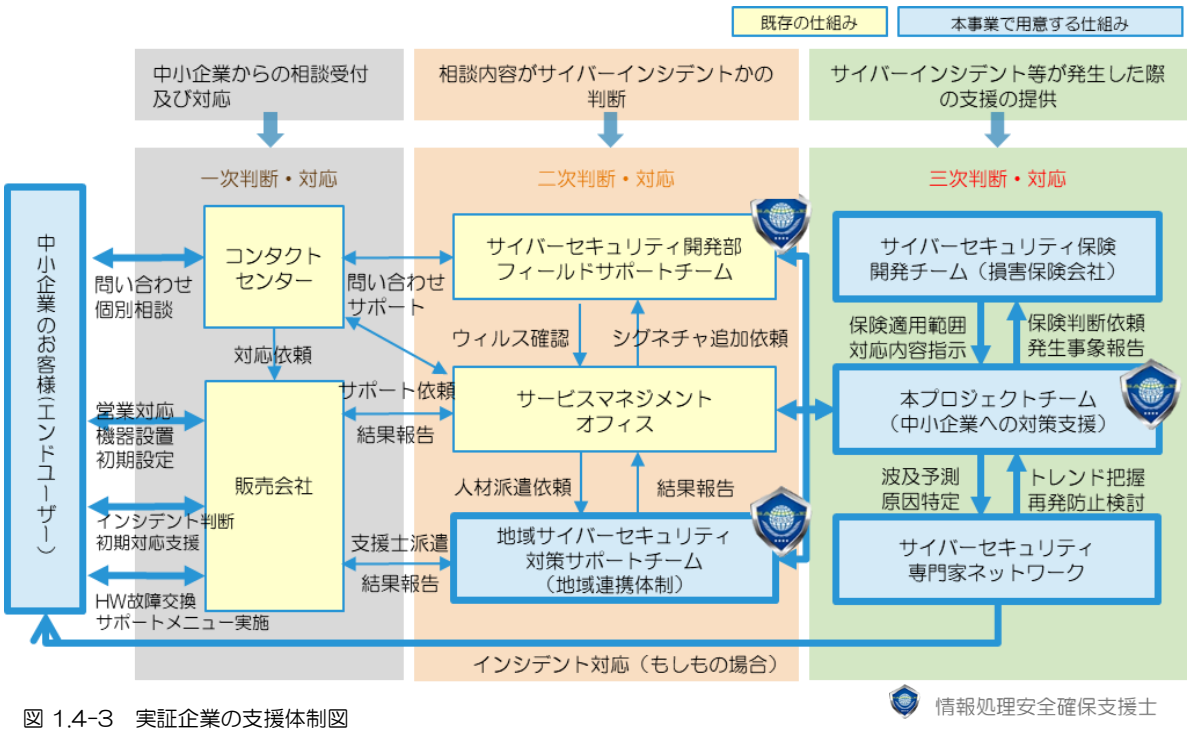


図 1.4-3　実証企業の支援体制図

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、サイバーセキュリティ開発部、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。サイバーセキュリティ開発部のフィールドサポートチームには、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、実証企業からの問い合わせに対応する役割を担わせた。

② 本事業での独自体制

本プロジェクトチーム、地域サイバーセキュリティ対策サポートチーム、サイバーセキュリティ保険開発チーム、サイバーセキュリティ専門家ネットワークは、本事業のために、新たな体制を組んだ。本プロジェクトチーム、地域サイバーセキュリティ対策サポートチームには、情報処理安全確保支援士を配置した。前者は、実証企業でのサイバー攻撃リスクを判定する役割、後者は、専門知識が必要となる販売会社からの問い合わせに対応する役割を担った。

活動結果

2.1 実証企業の募集

事業説明会への勧誘および本事業への参加依頼活動は以下の通り。

①提案時に予定した勧誘施策

・テレアポの実施

・経済産業省関東経済産業局、自治体、商工会議所等への協力要請

②事業開始後に追加した勧誘施策

・富士ゼロックス各販売会社の営業・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およびDMによる告知

・地域ITベンダーを通じた勧誘

・本事業で協力関係にある保険会社を通じた勧誘

・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

2.1.1 事業説明会の実施

以下、事業説明会の実施結果について記述する。

【アジェンダ】

・中小企業でのサイバーセキュリティ対策の必要性および普及に向けた国等の支援事業について（IPA）

・サイバーセキュリティお助け隊の支援内容について

開催結果

事業説明会の開催結果を表2.1-1に示す。茨城県4回、栃木県4回、群馬県1回、長野県2回の合計11回開催し、説明会参加企業は124社、そのうち実証事業への参加合意（UTM端末設置）は9社のみであった。

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、募集活動の段階で十分に訴求しきれなかったことが、事業説明会の勧誘活動が難航した要因と考えている。

開催地	日程	場所	開催告知	参加企業 (参加人数)	申込み	設置	設置率
栃木	7月22日	栃木ITセミナー 協力：FX栃木	①メルマガ（宇都宮商工会議所）	10 (10)	2	2	20%
栃木	7月24日	大手自動車製造会社社内 協力：大手自動車製造会社	①サプライチェーン	19 (19)	6	0	0%
茨城	7月26日	水戸商工会議所 協力：水戸商工会議所	①FAX（水戸商工会議所会員企業3400枚）	1 (1)	1	1	100%
栃木	8月30日	栃木県産業技術センター 協力：栃木県	①チラシ配布 ②FAX（県庁）	30 (30)	0	0	0%
長野	9月2日	上田商工会議所 協力：関東経済産業局、上田商工会議所	①チラシ配布 ②工業部会参加メンバーへの声掛け	20 (20)	3	3	15%
茨城	9月3日	茨城県中小企業振興公社 協力：茨城ITコーディネータ協会	①メルマガ（中小企業振興公社） ②HP告知（中小企業振興公社）	25 (25)	0	0	0%
長野	9月5日	長野県中小企業振興センター 協力：長野ITコーディネータ協会		3 (3)	0	0	0%
栃木	9月18日	宇都宮商工会議所 協力：栃木県	①FAX（県庁） ②メルマガ（県庁） ③チラシ配布	8 (9)	1	1	13%
茨城	10月9日	日立商工会議所 協力：大手電機メーカー	①サプライチェーン	6 (6)	2	2	33%
茨城	10月10日	土浦商工会議所 協力：大手電機メーカー	①サプライチェーン	2 (2)	0	0	0%
群馬	10月21日	太田商工会議所 協力：FX群馬	①サプライチェーン	0	0	0	-
			合計	124 (125)	15	9	7%

表2.1-１　事業説明会の開催結果　　※「FX」は富士ゼロックスの略称

事業説明会への参加者等の反応

・サプライチェーンまで含めたサイバーセキュリティレベルの向上が必要と認識した（7/24栃木の担当者）

・本事業の賛同の声はあるものの、中小企業の興味が低く、説明会開催は効果的ではない。個別で中小企業への訪問を推奨する（7/26水戸商工会議所の担当者）

・これまであまり意識してこなかったサイバーセキュリティの重要性を認識できた（9/2上田商工会議所の参加者）

・ネットワークやサイバーセキュリティについて、相談できる相手ができた（9/3茨城県中小企業振興公社の参加者）

・ウイルスソフトを入れているが、UTMとの違いがわからない。UTM端末は必要なのか疑問を感じた（9/18宇都宮商工会議所の参加者）

・中小企業でのサイバーセキュリティ対策は喫緊の課題と認識した。本事業をきっかけに県庁としても積極的に後援していきたい（9/18栃木県庁の担当者）

・サプライチェーン全体でのサイバーセキュリティ対策レベルを向上させる必要性を認識した（10/9開催の担当者）

事業説明会開催での気づき

中小企業のサイバーセキュリティに対する意識・関心は、想定を下回るものであった。サイバーセキュリティに関するリスク認識が低く、本事業に関するさらなる啓発が必要であると感じた。また、自社がUTM端末を設置しているかどうかわからない、ウイルスソフトとUTMの違いがわからない等のコメントが多くあり、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。

2.1.2 テレアポによる募集

テレアポによる勧誘と募集結果は以下の通り。

【テレアポの勧誘プロセス】

・本プロジェクトを中心に中小企業（テレアポ先）のリスト化
・テレアポ（電話連絡）での本事業説明、実証参加の勧誘
・関心を持った中小企業へ、富士ゼロックス各販売会社の営業もしくはCEが面談を申し込み。
・訪問面談にて、より事業詳細について説明、実証参加を依頼

【テレアポの活動結果】

対象範囲：4県合計で、約750件の中小企業を対象とした
実施期間：2019年6～8月にかけて実施
アポ獲得：90件（約12%）
設置合意：30社（約4%）

2.1.3 地域関係者への募集協力依頼

地域での説明会開催への勧誘および実証企業の募集を目的に、商工会議所などの地域関係者への協力依頼をした。以下に、主な依頼履歴を示す。

主な6～7月度の依頼履歴

・茨城県、栃木県、群馬県、長野県の富士ゼロックス各販売会社：本事業の協力要請
・日本商工会議所経由で各県下の地域商工会議所：本事業の協力要請
・各県下の地域商工会議所：本事業説明会の開催依頼およびメルマガや会報へのチラシ折り込み等の広報活動を要請

主な8月度の依頼履歴

・関東経済産業局：茨城県、栃木県、群馬県、長野県の関係機関へ声掛け要請
・中小企業庁：ミラサポのメルマガで配信要請
・富士ゼロックス各販売会社：中小企業への勧誘を要請
・各県の東京事務所：県庁および所管組織への声掛けを要請

主な9月度の依頼履歴

・富士ゼロックス各販売会社：中小企業への勧誘強化を要請
・各県庁の東京事務所：県庁および所管組織への声掛け継続を要請

主な10月度の依頼履歴

・富士ゼロックス各販売会社：中小企業への勧誘強化を要請

2.1.4 富士ゼロックス各販売会社営業・CE訪問による募集

以下、富士ゼロックス各販売会社営業・CE訪問による実証企業の募集結果を示す。

【販売会社営業・CE訪問での募集プロセス】

・中小企業のリストを作成し、訪問のアポイント

・販売会社営業・CEが面談にて本事業説明し、経営者の関心度を確認、実証参加同意を獲得

・現地調査を行い、UTM端末が設置可能であれば申込書回収、設置手配

【販売会社営業・CE訪問での募集結果】

・5県で43社の申込件数を獲得

・直接面談で、中小企業側の心配事や不明点確認のもと、詳細に事業説明して不安を解消するプロセスが非常に重要であった

【工夫したポイント】

改めて過去勧誘活動のレビューを実施し、実証参加に戸惑っている中小企業が多いことが判明した。そのため、富士ゼロックス各販売会社営業・CEが主体となり、中小企業に直接面談して事業趣旨等を詳細に説明し、理解を促すことを周知徹底させたことで、参加企業数アップにつなげた。

2.1.5 WEB掲載・DM配信等による募集

以下、WEB 掲載・DM 配信などの情報ツールによる募集結果を示す

WEB掲載：

・6月末に本事業内容の説明および説明会参加予約サイト（Web申し込みページ）を開設。7/25富士ゼロックスホームページに事業内容および説明会への参加を促す広報リリースを発信

DM配信：

・中小企業家同友会会員より、対象となる製造業360社（茨城県41社、栃木県12社、群馬県142社、長野県165社）にDM配信にて、本実証事業へ参加勧誘

メルマガ配信：

・関東経済産業局、長野県庁、栃木県庁、茨城県中小企業振興公社、中小企業庁ミラサポ等の各メルマガ会員企業に情報配信を実施

FAX：

・商工会議所主催の説明会やセミナー等の案内時にあわせて本実証事業へ参加勧誘FAXの送信

その他：

・群馬県警察本部経由、群馬県中小企業等サイバーセキュリティ支援連絡会にて事業説明

以上のように、告知・募集の情報ツールについては、ホームページ、DM、メルマガ、FAX等を活用した。関心のあった中小企業には、追加で電話、メール、面談等で勧誘および事業趣旨説明を実施したが、実証参加の申込みは5件のみとなった。情報ツール主体での募集では、事業趣旨、内容、意義を詳細に伝えることができなかった。

2.1.6 地域ITベンダーによる募集

以下の手順で、地域ITベンダーによる募集を進めた。

①地域ITベンダー所有の中小企業リストへの勧誘

②直接面談にて、中小企業へ事業内容を説明（サイバー攻撃によるリスク、サイバーセキュリティ対策の必要性を訴求）

③主に経営者および情報システム部門の人脈での関心度、実証への参加意向を確認

【地域ITベンダーによる活動結果】　実証参加：12社獲得

地域密着型ITベンダー経由による募集効果は高かった。理由は、普段の営業活動を通じた信頼関係が土台にあり、経営者が前向きに検討してくれたためと考える。

2.1.7 保険会社による募集

保険会社に、地域支社取引先の中小企業の紹介を依頼。保険会社側で、対象となる取引先を選定。個別説明会開催にて、実証参加を募った。

【保険会社による活動結果】　実証参加：2社獲得

保険会社からの紹介効果は高かった。母数が24社と少なかったため、2社の獲得に留まった。

2.1.8 サプライチェーンによる募集

サプライチェーンのコア企業に対するアプローチを実施した。大手自動車製造会社（栃木）（群馬）、大手電機メーカー（茨城）、大手光学機器メーカー（埼玉）等へコンタクトして、サプライチェーン単位でサイバーセキュリティ対策に取り組む必要性について提案訴求、関連するサプライヤーへの情報提供（事業説明会への参加、実証への協力）を依頼した。

【サプライチェーンによる活動結果】　実証参加：2社獲得

サプライヤー（の中小企業）で、セキュリティ対策の重要性は認められたが、実証協力とはならなかった。コア企業からの旗振りでの実証企業数の増加を期待したが、下請法等の観点で積極的な勧誘は困難であることが分かった。

サプライヤー側の中小企業から「現状で取引継続できているなか、追加対策がなぜ必要なのか」というコメントが多くあり、コア企業側が感じているサイバー攻撃への危機意識（サイバーセキュリティ対策の緊急性）が、サプライヤー側に浸透できてないと感じた。

2.1.9 参加申込みの進捗と結果

7～12月の参加申込み企業数の推移を図2.1-1に示す。7～8月は、各県、自治体、商工会議所等へ協力依頼して事業説明会を開催、個別には、テレアポで事業説明するなどで対応したが、募集活動は難航した。

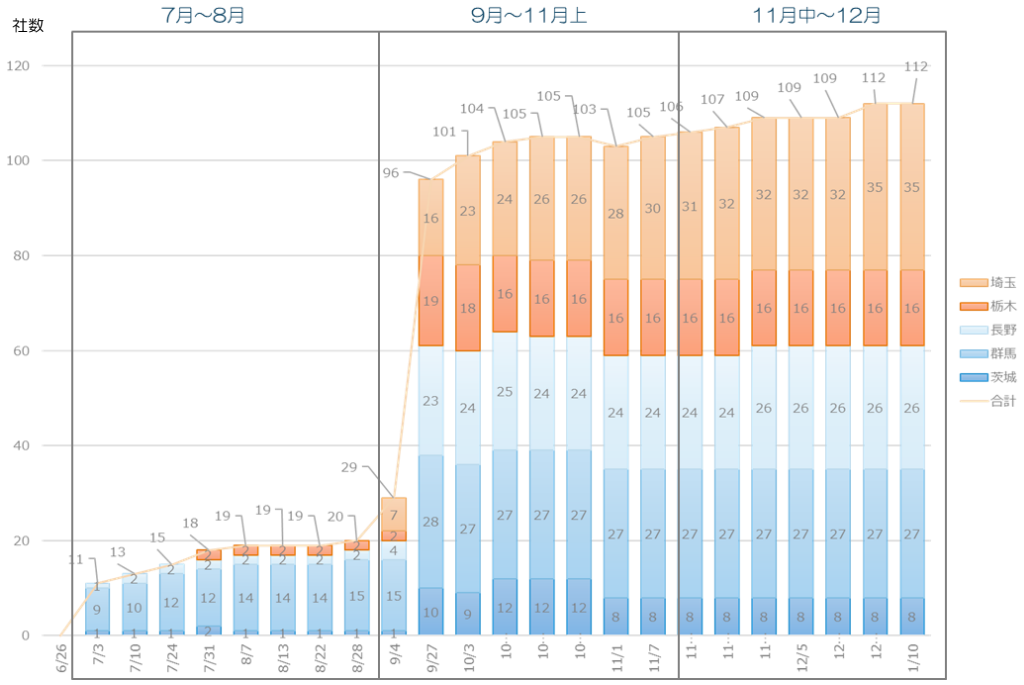


図 2.1-１　参加申込み企業数の推移

9～10月は、8月までの活動レビューから、富士ゼロックス各販売会社の営業・CEへ指示を出し、面談時に中小企業の心配事や不明点を明確にするプロセスの徹底を図った。さらに、プロジェクトメンバーが主体となり、各県下の中小企業に直接事業説明する機会を増やした結果、100社以上の中小企業から参加申込みを獲得することができた。最終的に、参加企業は112社に達したが、UTM端末の設置による実証に参加した中小企業（以下「実証企業」という。）は101社となった。理由は、2.2 UTM端末設置で記述する。

実証企業を地域別にみると（下図2.1-2参照）、埼玉県33件、群馬県24件、長野県23件、栃木県15件、茨城県6件である。業種別では（下図2.1-3参照）約半数の52社が製造業である。また従業員数別では（下図2.1-4参照）約半数の45社が従業員数10名以下の小規模事業者である。

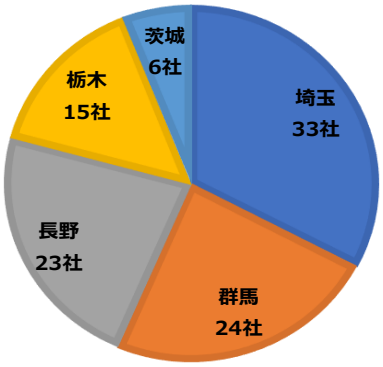


図 2.1-２　実証企業の地域

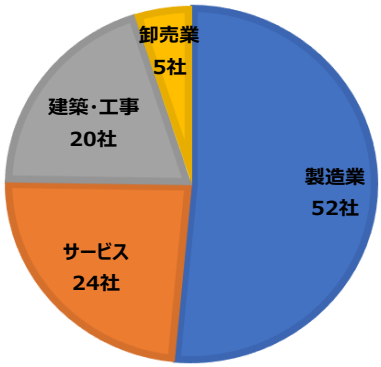


図 2.1-３　実証企業の業種

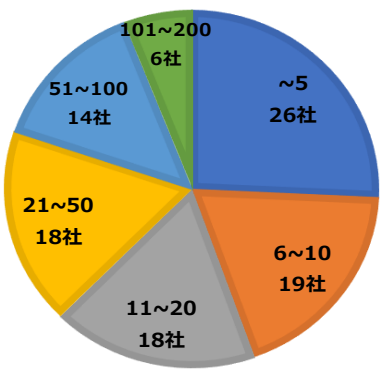


図 2.1-４　実証企業の従業員数

募集手段ごとの内訳は下記の通り。事業説明会は５県（茨城県、栃木県、群馬県、長野県、埼玉県）で実施したが、実証企業の獲得は9社に留まった。またWeb掲載・DM配信は掲載期間を長くしても5社と少なかった。他方、テレアポ、富士ゼロックス各販売会社からの営業・CE訪問、地域ITベンダーからの個別訪問により、合計で85社獲得した。それら訪問では、職場のIT環境・管理状態を相互に確認すること、ネットの利用状況やサイバー攻撃リスクに対する危機感等について意見交換することで、中小企業が感じている不安を解消できたことが効果的であったと考える。

- 説明会での勧誘： 9社設置（15社申込み、うち6社は設置不可）
- WEB掲載、DM配信：5社設置（DMでは約360社への声掛）
- テレアポ勧誘・訪問： 30社設置（750社声掛、90社個別訪問）
- 販社営業・CE訪問： 43社設置（約200社への個別訪問）
- 地域ITベンダーの紹介： 12社設置（約60社への個別訪問）
- 保険会社からの紹介： 2社設置（約24社への説明会開催）

県別の募集手段内訳を、下図2.1-5に示す。いずれの県においても、テレアポ、富士ゼロックス各販売会社営業・CE訪問、地域ITベンダーが個別訪問することで、実証企業の獲得に至ったことが分かる。

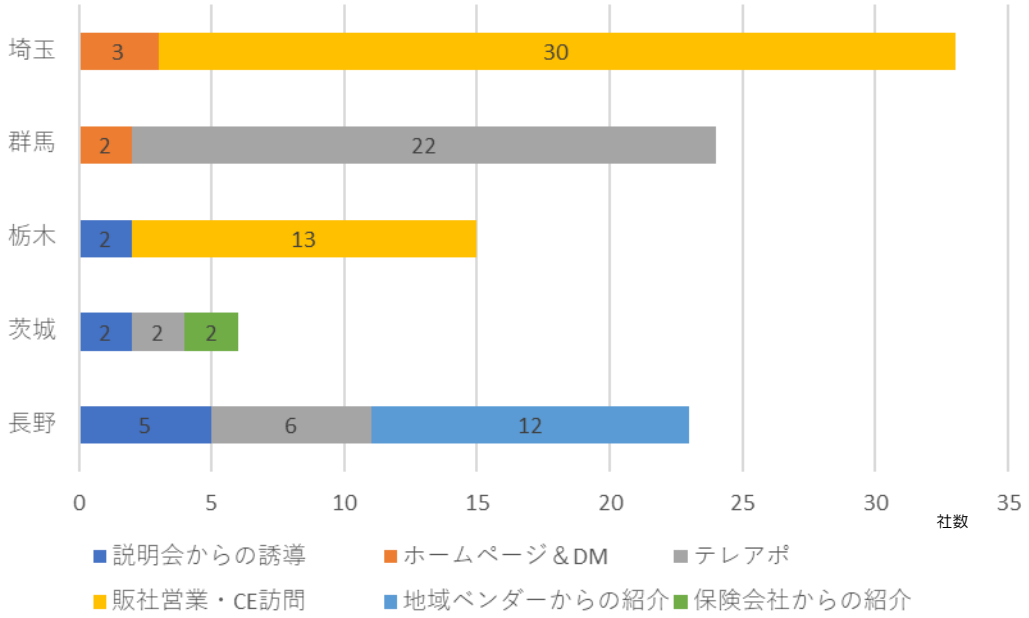


図 2.1-５　実証企業の募集手段内訳（県別）

2.2 UTM端末設置

以下に、UTM端末設置での活動について記述する。

2.2.1 現地調査での困難性

申込みのあった実証企業を個別訪問して、改めて経営者、情報システム管理責任者に対して事業趣旨および実証内容について説明の上、当該中小企業のネットワーク環境を調査し、設置可否を判断したが、設置不可となる事案が数多く発生した。その理由は下記の通り。

【主な設置不可理由】

- 別会社のUTM端末を確認（既設済み）
- ネットワーク構成上の問題（外部とVPN接続を組んでおり、専用機器を取り外せない等）

既設済みUTM端末の認識がなかったという理由で設置不可となる事案は20件以上あった。自社のセキュリティ環境について組織として把握できていない、という中小企業の実態が判明した。VPNなど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）に設置不可となった。

2.2.2 設置後の問題

UTM端末設置後の運用段階においても、いくつか問題が発生した。

【設置後の課題】

- 業務上必要な、以前閲覧できていたサイトにアクセスできない　※UTMにより遮断される
- 業務システム（レジ、社内放送など）動作に影響を及ぼす

1つ目は、実証企業が利用するWebサイト側の問題である。実証企業には、危険なサイトであることを十分に通告した上で、セキュリティレベルを下げる等の設定変更を施した。2つ目は、レガシーシステムとの適合問題である。設定変更だけでは対応できず、業務を優先する場合は、設置したUTM端末を撤去することになった。

残念ながら、本事業での端末設置による実証に参加できなかった中小企業が多く発生したが、それら中小企業には、危険な通信発生や外部サイトへのアクセスによる脅威、またはレガシーシステム刷新の必要性が認識され、サイバーセキュリティに関する啓発は大いに図られたと考えている。

2.2.3 設置数の月別推移

以下に、UTM端末設置活動の月度推移について記述する。

7月～8月は、参加合意いただいた20数社の実証企業へ効率的な設置プロセス対応に向けて、各県下へ経験豊富な設置導入専門員を増員した。9月～12月は、特に10月に発生した台風19号の影響によりスケジュール変更を余儀なくされた。一部の実証企業での設置は11月以降となった。そのため、本来8月で終了する予定だった設置導入専門員を、9月以降も継続投入し対応した。

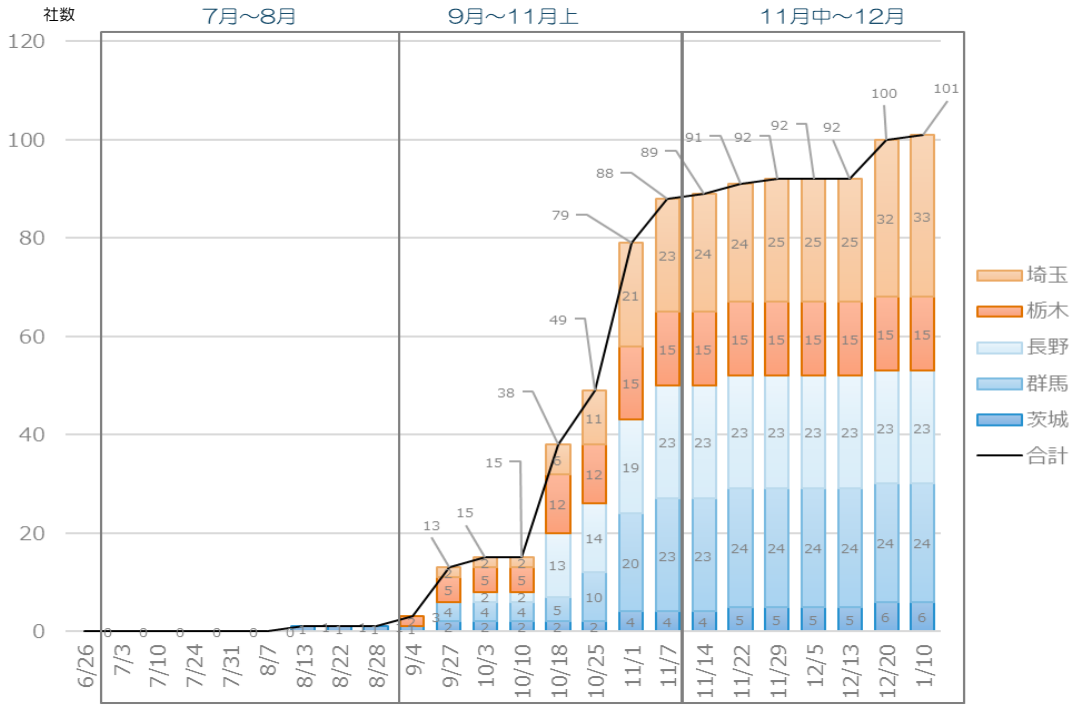


図 2.2- 1　実証企業への UTM 設置数の推移

2.3 監視とログ収集

以下、実証企業に設置したUTM端末での監視とログ収集について報告する。

2.3.1 UTM開通・稼働状況

期間中、実証企業に設置したUTM端末の故障・不具合レポートはなかった。稼働状況についても、nocによるリモート監視にて、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、実証企業101社の通信ログは正常に収集できたと判断する。

2.3.2 コールセンターへの問い合わせ

下表2.3-1に、実証事業に関連するコールセンターへの問い合わせ内容を示す。

コールセンター受付	**30**
実証実験に関して	0
セキュリティ機器設置に関して（お客様）	3
セキュリティ対応の相談	16
その他	11
インシデント等対応	**3**
電話およびリモート	3
訪問	0
機器設置等のトラブル対応	0
その他	0

表 2.3.- 1　コールセンターへの問い合わせ内容

問い合わせは合計30件。セキュリティ対応の相談は16件で、内訳はWebフィルタリングの設定、メール送受信に関する不具合、LAN設定トラブル等であった。その他11件はネットワークに関する相談であり、内訳はiCloud設定、Wi-Fi機器との接続方法、停電時の取り扱い等であった。インシデント等対応の問い合わせは、通信ネットワークの設定対応であり、セキュリティ事故ではなかった。

2.3.3 実証企業へのレポート発行（月次レポート）

UTM端末の通信ログは、実証企業ごとに月次で集計・分析、サイバー攻撃の実態を可視化し、図2.3-1に示すレポートにてフィードバックした。このレポートにより、セキュリティの専門家でなくても全体状況が把握でき、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てもらった。

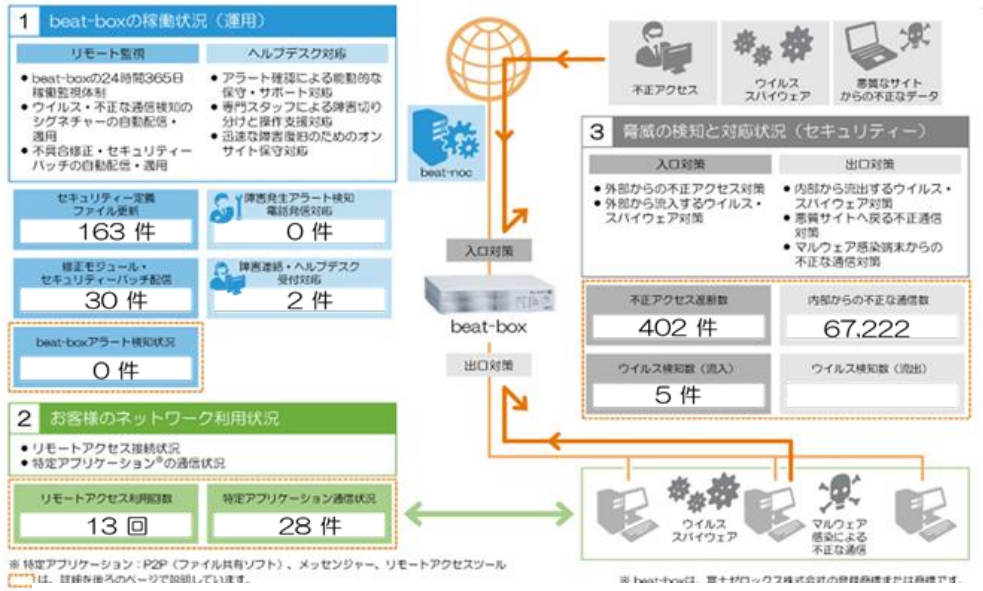


図 2.3- 1　月次レポートの内容（例）

2.3.4 ネットワーク上の端末調査（エンドポイント管理）

実証企業でのネットワーク上の端末調査の結果を、下表2.3-2に示す。

		A社	B社	C社
監視対象PC		13台	2台	5台
総合判定		見直し・対策が必要	問題無し	見直し・対策が必要
ハードウェア診断				
	PC経年数	1年未満（1） 4～5年（10） 5年以上（2）	2～3年（2）	2～3年（2） 5年以上（3）
	ハードディスク使用率	～30%（10） ～50%（1） ～70%（1） ～100%（1）	～10%（1） ～30%（1）	～10%（1） ～30%（3） ～50%（1）
ソフトウェア診断				
	OSバージョン	win10（1） win７（12）	win10（2）	win7（5）
	officeバージョン	Ver2016（1） Ver2013（11） Ver2010（1）	365（1） Ver2016（1）	365（1） Ver2007（3）
セキュリティ診断				
	ウィルス対策状況	実施済み（12） 未実施（1）	実施済（2）	実施済（4） 未実施（1）
	スパイウェア対策	実施済み（12） 未実施（1）	実施済（2）	実施済（5）
	ファイアウォール設定	実施済み（13）	実施済（2）	実施済（4） 未実施（1）

表 2.3.- 2　IT ネットワーク環境調査の結果（3 社）

上表、IT環境を調査した3社中2社では、セキュリティ上重要なOSバージョンやウイルス対策が不十分であり、見直し・対策が必要と判別された。本実証は、UTM端末によるゲートウェイセキュリティを主眼としたが、中小企業にはエンドポイント側のIT環境の調査・対応についても、必要と考えられる。

2.4 ログデータ分析

以下、実証企業101社のUTM端末のログデータ分析の集計・分析結果を示す。

調査概要を下表2.4-1、期間中の全セキュリティ・アラート結果を下表2.4-2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	実証企業にUTM端末を設置、調査期間中に収集したログ情報の分析
調査対象	実証企業101社
調査期間	2019/9/5 ～ 2020/1/31　※UTM端末ごとに調査開始日は異なる
調査項目	ping/port-scan履歴 不正な通信（IPS）検知ログ HTTP/FTPウイルスチェック履歴 メール受信ウイルスチェック履歴 メース送信ウイルスチェック履歴 スパムメール判定履歴 コンテンツフィルタログ

表2.4- 1　ログデータ分析による調査概要

対策項目	監視項目	発生件数（合計）	内容
外部からの不正アクセス防止対策（ファイアウォール機能）	外→内のping/port-scan履歴	93,824件	・外部からping又はport-scanによるアクセスを受けた履歴 ・アクセスの日時、アクセス（ping/port-scan）の種別、送信元IPアドレス
不正な通信対策（IPS：不正侵入防止システム）	不正な通信(IPS)検知ログ（内→外、内→外→内を含む）	6,757,458件	・IPS（Intrusion Prevention System）が検出した、不正な通信の履歴 ・検知日時、送信元IPアドレス、送信先IPアドレス、送信先ポート、ツール名、検知モジュール、シグネチャーID、アクション
ウイルス・スパイウェア対策	HTTP・FTPウィルスチェック履歴	45件	・HTTP通信・FTP通信に対するウィルスチェック履歴 ・通信日時、アクセス元のIPアドレス、WebサイトのURL又はIPアドレス、ウィルス名
	メール受信ウィルスチェック履歴	272件	・受信したメールに対するウィルスチェック履歴 ・受信日時、宛先メールアドレス、件名、ウィルス名
	メール送信ウィルスチェック履歴	0件	・送信したメールに対するウィルスチェック履歴 ・送信日時、送信元メールアドレス、件名、ウィルス名
スパムメール対策	スパムメール判定履歴	141,935件	・受信したメールの日単位の総数と、その中に含まれるスパムメール判定されたメール数 ・受信日、メール（NORMAL/SPAM）の種別、メール数
WEBフィルタリング対策	コンテンツフィルタログ	3,213,734件	・有害なWebサイトや業務上必要のないWebサイトへのアクセス履歴 ・アクセス日時、アクセス元PCのIPアドレス、フィルタリング結果（アクセスの許可/禁止/警告/）、アクセス許可/制限の理由、アクセス先WebサイトのURL、アクセス先Webサイトの所属カテゴリー、適用されたルールのID

表 2.4- 2　全セキュリティ・アラートの結果

2.4.1 ping/port-scan

結果を、下図2.4-1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93,824件（ping：83,910件、port-scan：9,914件）。UTM端末1台で1日あたりに換算すると約14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い。

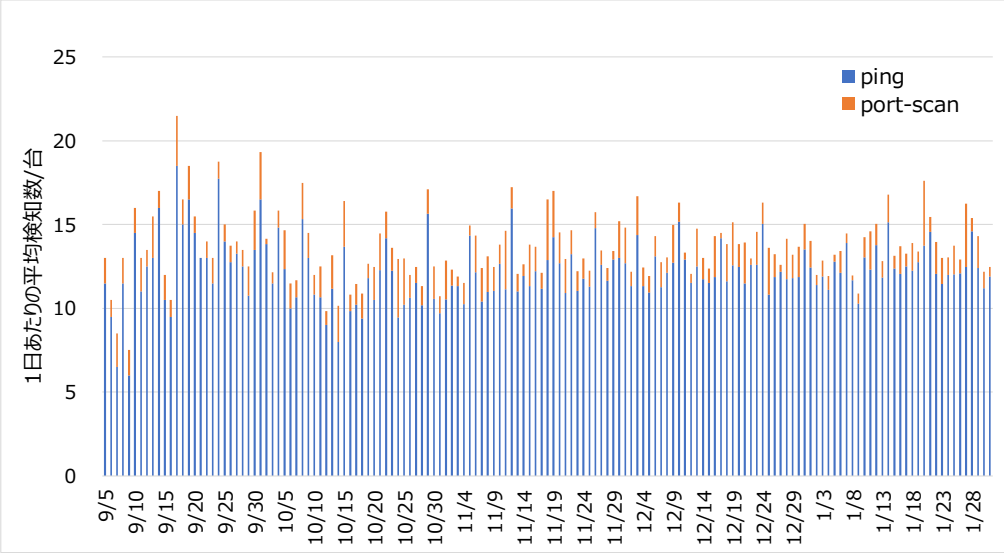


図 2.4- 1　ping/port-scan 履歴の日別データ

pingは103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、半数以上の51%を占めた（図2.4-2参照）。他方、port-scanは63ヶ国からのアクセス履歴を検知。US（米国）、RO（ルーマニア）、CN（中国）の3ヵ国で、44%を占めた（図2.4-3参照）。

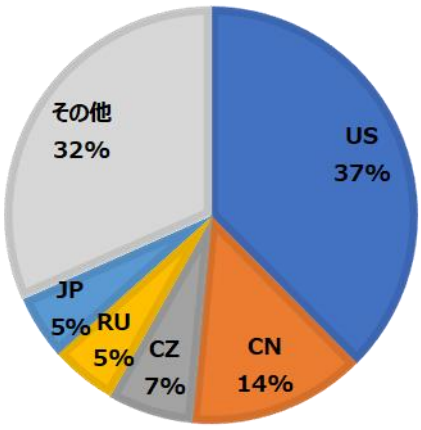


図 2.4- 2　ping の国別比率

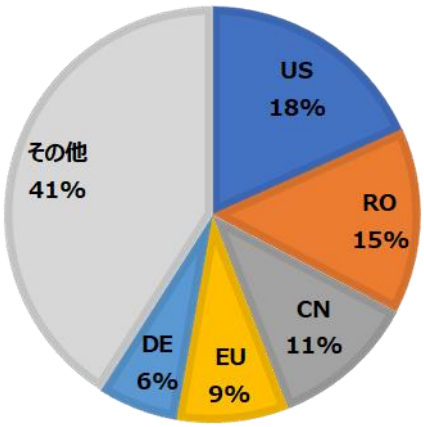


図 2.4- 3　port-scan の国別比率

2.4.2 不正な通信（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6,757,458件、1日あたりに換算すると約603件/台となった。

不正通信の内訳を下図2.4-4に示す。今回検知した不正通信の約7割は、Baidu IMEの通信であった。調査対象の約1/3にあたる33台から通信を検知。“意図しない情報送信”などのリスクが高いといえる。次に、マルウェアの配布に使われる危険性があるP2Pソフトの通信が13%、会社情報を個人のアカウントに移して持ち出す危険性があるDropboxの通信が12%など、要注意レベルの通信が続いた。TeamViewer、VNC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）は、調査対象の約1/5にあたる22台で検知された。リモートアシスタンスは、外部サーバーへの情報持ち出しが可能であり、内部不正による情報漏洩のツールになり得る危険性があり、注意が必要である。

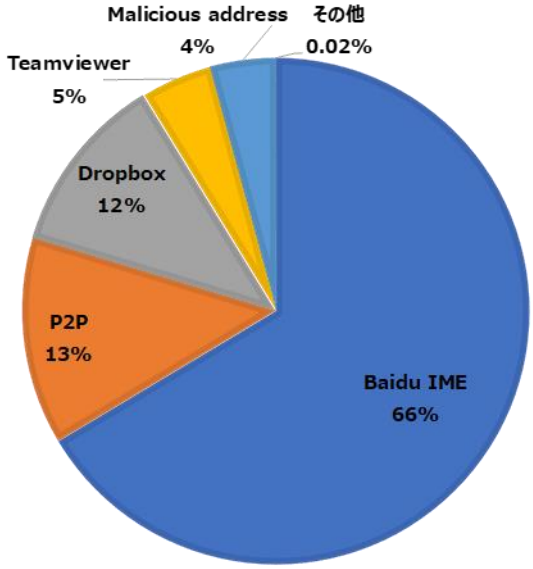


図 2.4- 4　不正通信（IPS）検知ログの内訳

※“Baidu IME”は、入力中の文字情報を中国のBaidu社のサーバーに送信し、変換精度を高める機能を利用した際に検出される。意図せぬ情報送信で機密漏洩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。

その他（0.02%）には、危険性が高い（急ぎ対応が必要、セキュリティインシデントにつながる可能性の高い）不正通信を検知した。その内訳は、下記の通り。

1）WannaCryのC&Cサーバーとの通信を検知、ブロック（埼玉県X社、群馬県Y社）
→社内PCがランサムウェアであるWannaCry感染の可能性
2）外部サーバーへの攻撃に関する通信を検知、ブロック（群馬県Y社）
→社内PCがマルウェア感染の可能性

本実証では、これらを重大リスクと判断して、追加調査を実施。詳細は2.6.3以降で報告する。

2.4.3 FTP/HTTPウイルススキャン

FTP/HTTPウイルススキャンの結果を、下表2.4-3に示す。

検知数	ウイルス名
10件	GrayWare/Win32.Puasson(0x2fdb273)ASMalwS
10件	RiskWare[WebToolbar]/Win32.MyWebSearch.z(0x380c)ASBOL
10件	GrayWare/Win32.Presenoker(0x2cfcdf8)ASMalwS
5件	Unknown(ASMalwGH:910999)
3件	Trojan[DDoS]/Linux.Agent.ak(0x2e202)ASELF
2件	GrayWare/Win32.ProductKey.dj(0x1458437)
2件	Unknown(ASMalwGH:1009009)
2件	GrayWare/Win32.Presenoker(0x2d1dc6f)ASMalwS
1件	GrayWare/Win32.Slimware.a(0x170)ASCommon

表 2.4- 3　検知した HTTP・FTP ウイルス

Web経由でダウンロードされたウイルス検知数は合計45件、多くはフリーソフトである。意図しない広告の表示、他のソフトウェアのインストール、ブラウザのハイジャック等が行われる可能性があり、グレイウェア（マルウェアと断定はできないプログラム）と呼ばれる。

以下、今回検知したウイルスについて補足説明する。

10件：GrayWare/Win32.Puasson(0x2fdb273)ASMalwS

スマートフォン用のユーティリティであり、意図せぬ広告などを表示。

HTTPS://BLOG.MALWAREBYTES.COM/DETECTIONS/VSCREENSHOT-COM/

10件：RiskWare[WebToolbar]/Win32.MyWebSearch.z(0x380c)ASBOL

AdWareの一種であり、imgfarm自体はブラウザ上にポップアップを表示するなど、特定のサイトにリダイレクトを行う動作をする。また、その過程において、ブラウザのプラグインなど意図しないものをインストールされる現象が報告されている。

HTTPS://MALWAREFIXES.COM/THREATS/IMGFARM-COM/

10件：GrayWare/Win32.Presenoker(0x2cfcdf8)ASMalwS

2件：GrayWare/Win32.Presenoker(0x2d1dc6f)ASMalwS

lavasoftのソフトウェア自体は無償のセキュリティソフトであり、ウイルスではない。インストールすると意図しない広告の表示、他のソフトウェアのインストール、ブラウザのハイジャックが行われるとの報告があり、マルウェアの一種と捉えることができる。※グレーな扱いとなっている。

HTTPS://WWW.MALWARERID.JP/MALWARE/WEB-COMPANION/

5件：Unknown(ASMalwGH:910999)

2件：GrayWare/Win32.ProductKey.dj(0x1458437)

2件：Unknown(ASMalwGH:1009009)

nirsoftのソフトウェアは一種のユーティリティソフトであり、プロダクトキーを表示するなど、パスワードのリカバリを行うことができる。ハックツールとして、複数のアンチウイルスベンダーがマルウェアとして検出する。また、その特徴からマルウェアに同梱されるケースもある。

HTTPS://WWW.SYMANTEC.COM/SECURITY-CENTER/WRITEUP/2017-053107-3147-99

HTTPS://WWW.TRENDMICRO.COM/VINFO/JP/THREAT-ENCYCLOPEDIA/MALWARE/SPYW_PRODKI

HTTPS://WWW.SOPHOS.COM/JA-JP/THREAT-CENTER/THREAT-ANALYSES/ADWARE-AND-PUAS/NIRSOFT.ASPX

3件：Trojan[DDoS]/Linux.Agent.ak(0x2e202)ASELF

脆弱性のあるLinuxモジュールのダウンロードをブロック。

1件：GrayWare/Win32.Slimware.a(0x170)ASCommon

Slimwareは、Microft Windowsの最適化ツールとして公開されている。他のソフトウェアのインストール、意図せぬ設定の変更などの報告があり、マルウェアの一種と捉えることができる。

HTTPS://WWW.MICROSOFT.COM/EN-US/WDSI/THREATS/MALWARE-ENCYCLOPEDIA-DESCRIPTION?NAME=PUA:WIN32/SLIMWARE

2.4.4 ウイルスメール受信

下図2.4-5に、ウイルスメール受信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272件（約0.05%、全メール受信数582,330件）。下図2.4-5の通り、特定企業に集中してウイルス添付メールが届く結果となった。

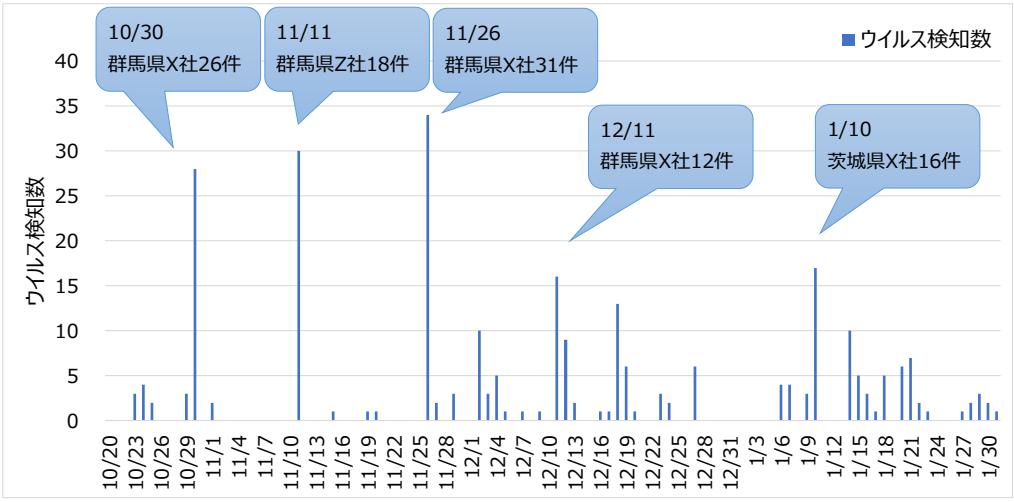


図2.4- 5 メール受信ウイルスチェック履歴の日別データ

実証企業の群馬県X社では、3か月で100件（35件/10月度、31件/11月度、34件/12月度）のウイルスメールを集中していたことから、追加調査を実施した。結果、群馬X社の関係会社のメールサーバーがハックされメールアドレスが漏洩したことが判明した。詳細は2.6.3以降で報告する。

2.4.5 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133,804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。

2.4.6 スパムメール判定履歴

以下、スパムメールの判定履歴を示す。

下図2.4-6に示す通り、調査期間中に受信したスパムメール数は、141,935件（全メール受信数582,330件の約24%）であった。

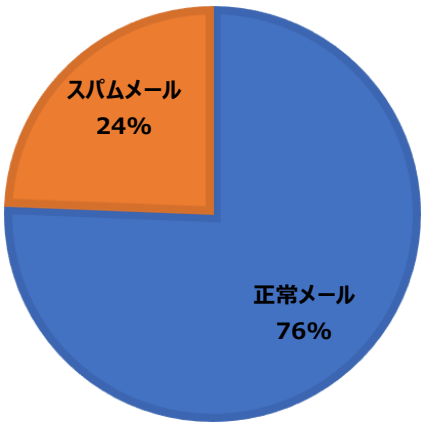


図 2.4- 6 受信メールに占める正常メールとスパムメールの比率

下図2.4-7にスパムメール判定履歴の日別データを示す。受信するスパムメール数は1日あたり約17件/台であり、週末は少なく、月曜日に多くのスパムメールを受信する傾向がある。

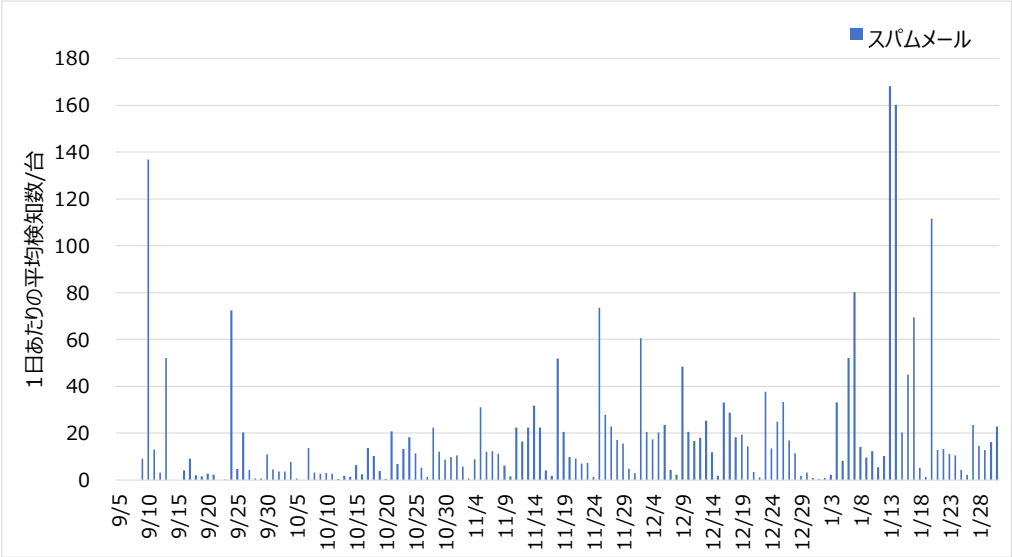


図 2.4- 7 スパメール判定履歴の日別データ

2.4.7 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3,213,734件、1日あたり約388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2.4-8に示す。87%はオンラインストレージ利用であり、調査対象の約1/5にあたる20台（1日あたり約320件/台）からの通信であった。次いで7%がSNSに対するブロックであり、調査対象の約3割にあたる28台（1日あたり約30件/台）から通信があった。これらオンラインストレージ、SNSなどへのアクセスは、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洩のリスクとして懸念される。

その他６%は、業務外URL（違法ソフト、ゲーム、チャット、ポルノ、他）であった。調査対象UTMの約80%にあたる78台（1日あたり約18件/台）から、この業務外URLの通信が確認されている。未だ情報漏えいリスクにつながっていないが、急ぎの検討・改善が必要である。

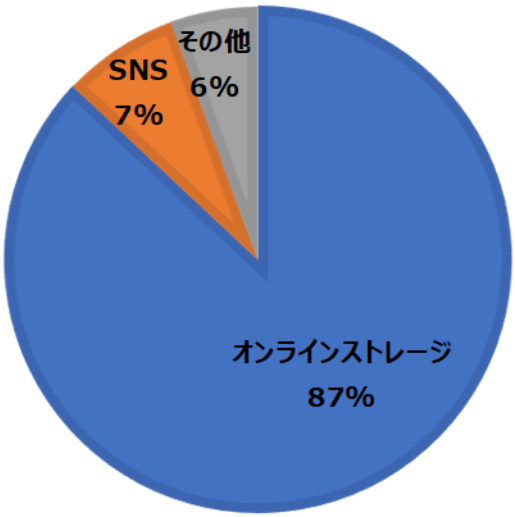


図 2.4- 8 コンテンツフィルタログの内訳

2.5 分析結果からの特徴抽出

以下、リスクランク別分析での特徴抽出の結果を示す。

リスクランクの定義は、下記の4段階とした。レベル４（即時対応）はサイバー攻撃による重大リスクであり、実証企業への駆け付け支援の判断基準にもしている。※駆け付け支援詳細は、2.6インシデント対応を参照。

４：即時対応　…駆け付け支援の対象

３：要観察　…長期間継続する場合はリスク低減措置を検討

２：許容範囲　…現状維持で可

１：低リスク　…問題なし

2.5.1 IPSでのリスクランク別分析

IPS検知ログは、下記定義にてリスクランク化した。

リスクランク	定義
４：即時対応	悪質なマルウェア感染の可能性がある内部からの通信をブロック
３：要観察	グレイウェアに起因する内部からの通信、または非推奨のソフトウェアに起因する内部からの通信をブロック
２：許容範囲	SNS,オンラインストレージ等 社内ポリシーによっては許可される通信を検知
１：低リスク	上記いずれの通信も検知無し

※グレイウェア：マルウェアやスパイウェアに類する。破壊活動やセキュリティ上危険な活動を特に行うものではなく、不正プログラムと見なすのが難しいソフトウェアの総称。BAIDU IMEなどもこれに含む。非推奨のソフトウェア：P2Pソフトや脆弱性が指摘されているソフトウェアなど、他のマルウェアを引き込む可能性があるソフトウェア

IPSリスクランクの内訳を、図2.5-1に示す。即時対応が必要なランク4が2%、要観察のランク3が33%、許容範囲のランク2が29%、低リスクのランク1は37%となった。

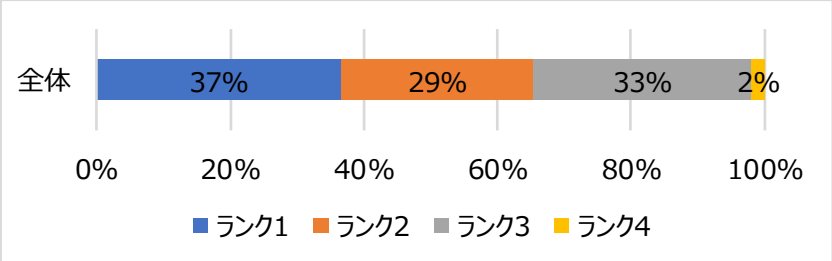


図 2.5- 1　IPS リスクランクの内訳

次に、IPSリスクランクを従業員数別でみた結果を図2.5-2に示す。従業員数が増加するにつれて高リスク（ランク3以上）の割合が増加し、従業員数21～50人で最もリスクが高く、従業員数が50人以上になるとリスクが低下する傾向がみられる。

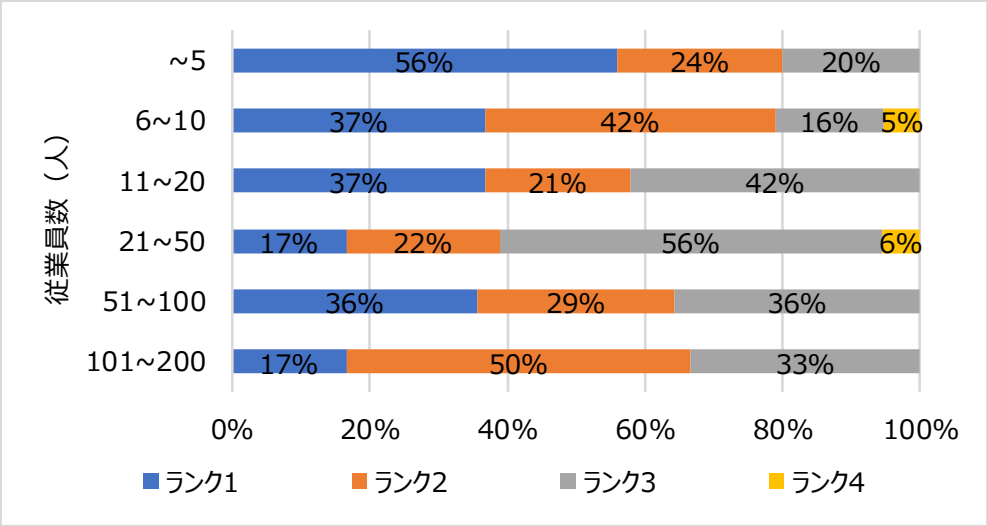


図 2.5- 2　IPS リスクランクの内訳（従業員数別）

2.5.2 スパムメールでのリスクランク別分析

スパムメールは、下記定義にてリスクランク化した。

リスクランク	定義
4：即時対応	スパムメールの検出数が急激に増加
3：要観察	スパムメールの検出数が 240 件以上
2：許容範囲	スパムメールの検出数が 240 件未満
1：低リスク	スパムメールの検知無し

※ランク2,3の判定値は、本実証結果の中央値とした。
※ランク4の判定値は、直近3か月の変動分で判定（検出数の平均値と標準偏差で算出）、今回ランク4は該当なし

スパムメールのリスクランクの内訳を、図2.5-3に示す。低リスクのランク1の企業は4%しかない。要観察のランク3、許容範囲のランク2はともに48%となった。

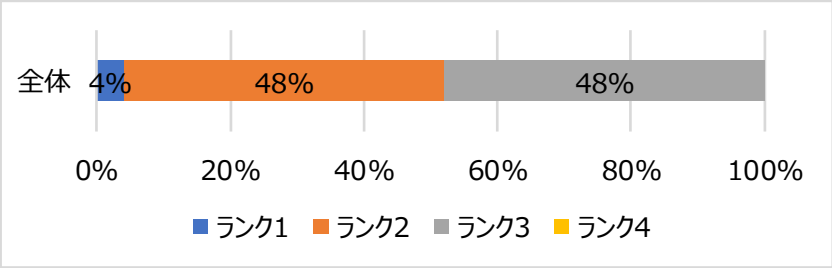


図 2.5- 3　スパムメールリスクランクの内訳

次に、従業員数別でみた結果を、図2.5-4に示す。高リスク（ランク3以上）の割合は51～100人で高く、次いで11～20人が高くなる。

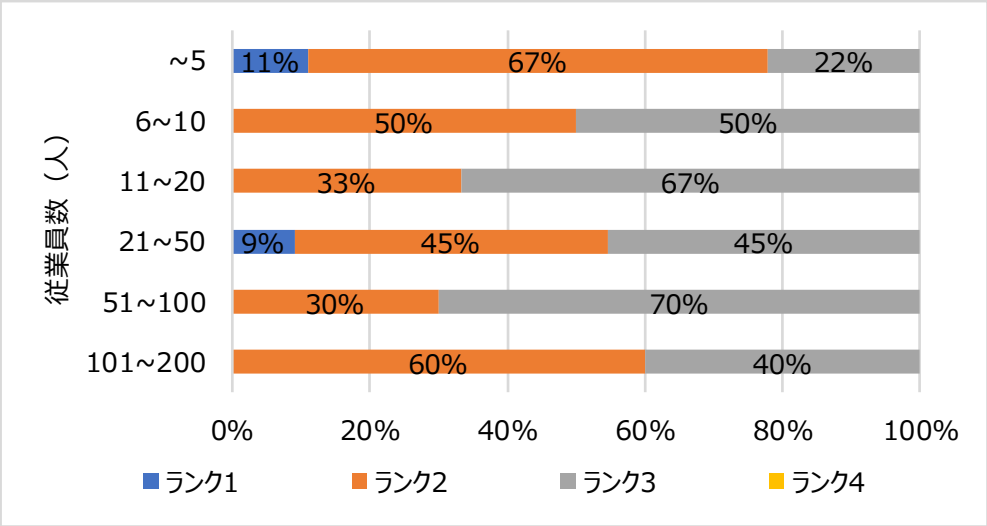


図 2.5- 4　スパムメールリスクランクの内訳（従業員数別）

2.5.3 ウイルスメールでのリスクランク別分析

ウイルスメールは、下記定義にてリスクランク化した。

リスクランク	定義
４：即時対応	送信メールにおいてウイルスを検知
３：要観察	ウイルス検出数が５件以上
２：許容範囲	ウイルス検出数が５件未満
１：低リスク	ウイルス検知無し

※ランク2,3の判定値は、本実証結果の中央値とした。
※ランク4の判定値は、危険性あるウイルスをブラックリスト化して判定。今回ランク4は該当なし

ウイルスリスクランクの内訳を、図2.5-5に示す。低リスクのランク1が大半で75%を占め、要観察のランク3が14%、許容範囲のランク2は11%となった。

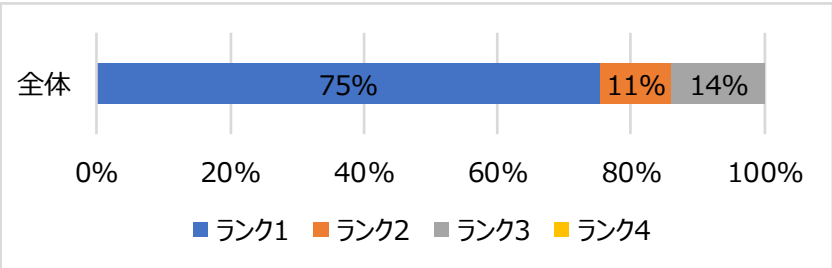


図 2.5- 5　ウイルスリスクランクの内訳

従業員数別でみた結果を、図2.5-6に示す。高リスク（ランク3以上）の割合は51～100人で高く、次いで11～20人が高くなる。

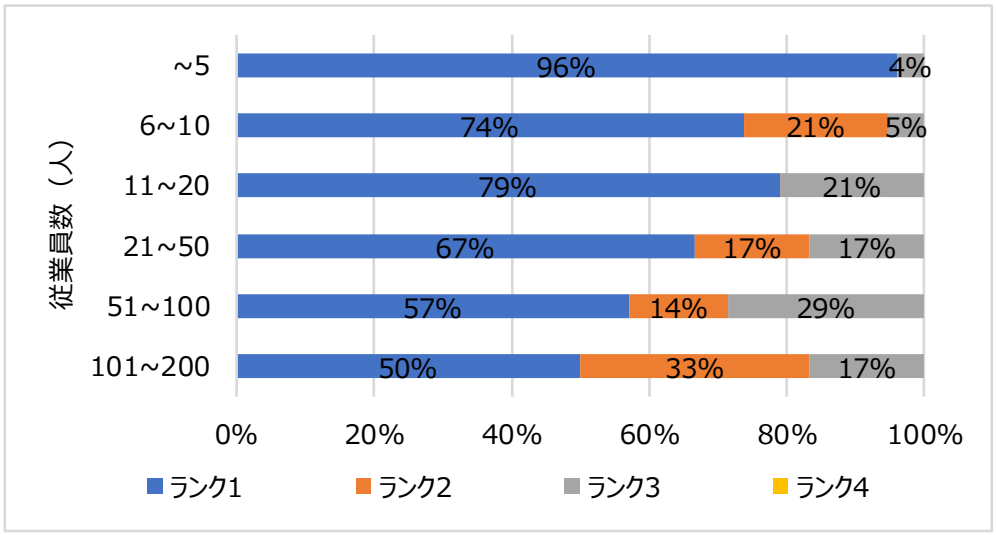


図 2.5- 6　ウイルスリスクランクの内訳（従業員数別）

2.5.4 ping/port-scanでのリスクランク別分析

ping/port-scanは、下記定義にてリスクランク化した。

リスクランク	定義
4：即時対応	ping/port-scan の合計検出数が急激に増加
3：要観察	ping/port-scan の合計検出数が 1200 件以上
2：許容範囲	ping/port-scan の合計検出数が 100 件以上 1200 件未満
1：低リスク	ping/port-scan の合計検出数が 100 件未満

※ランク2,3の判定値は、本実証結果の中央値としている。
※ランク4の判定値は、直近3か月の変動分で判定（検出数の平均値と標準偏差で算出）、今回ランク4は該当なし

ping/port-scanリスクランクの内訳を、図2.5-7に示す。低リスクのランク1の企業は3%しかない。要観察のランク3が58%、許容範囲のランク2が39%となった。

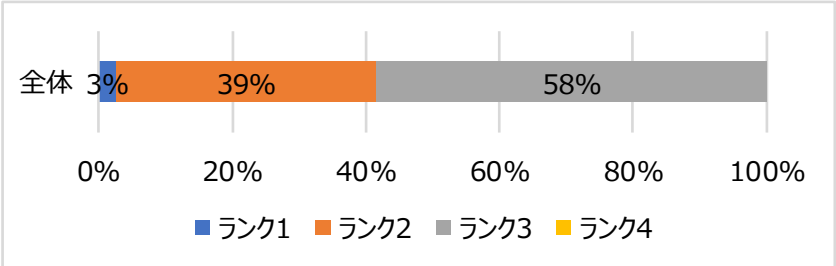


図 2.5- 7　ping/port-scan リスクランクの内訳

従業員数別でみた結果を、図2.5-8に示す。高リスク（ランク3以上）の割合は、従業員数21～50人規模で最も高くなっている。

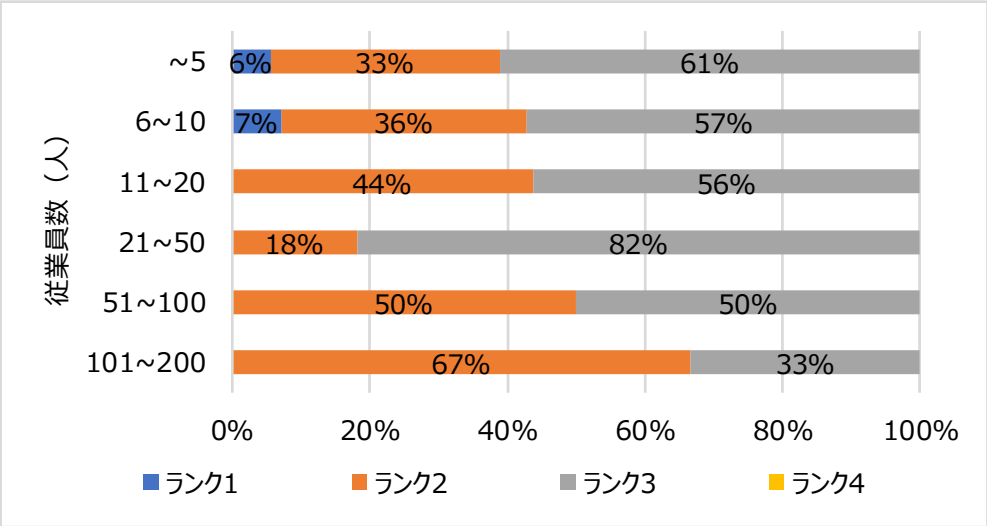


図 2.5- 8　ping/port-scan リスクランクの内訳（従業員数別）

2.5.5 コンテンツフィルタでのリスクランク別分析

コンテンツフィルタは、下記定義にてリスクランク化した。

リスクランク	定義
4：即時対応	業務と関連のないサイトへのアクセス数が急激に増加
3：要観察	業務と関連のないサイトへのアクセス数が 450 件以上
2：許容範囲	業務と関連のないサイトへのアクセス数が 450 件未満
1：低リスク	業務と関連のないサイトへのアクセス検知無し

※ランク2,3の判定値は、本実証結果の中央値としている。
※ランク4の判定値は、直近3か月の変動分で判定（検出数の平均値と標準偏差で算出）、今回ランク4は該当なし

コンテンツフィルタリスクランクの内訳を図2.5-9に示す。低リスクのランク1の企業は23%で、要観察のランク3は40%、許容範囲のランク2は38%となった。

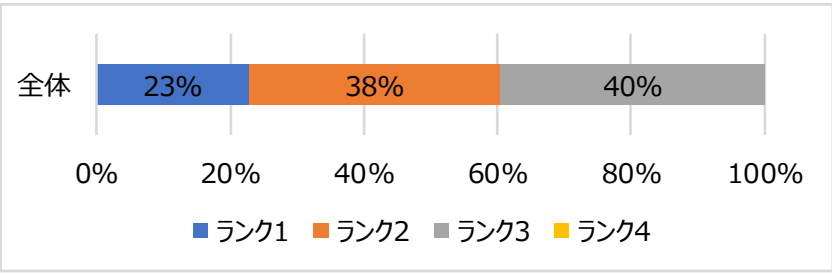


図 2.5- 9　コンテンツフィルタリスクランクの内訳

従業員数別でみた結果を、図2.5-10に示す。従業員数が増加するにつれて高リスク（ランク3以上）の割合が増加し、従業員数51～100人、101～200人で高くなっている。

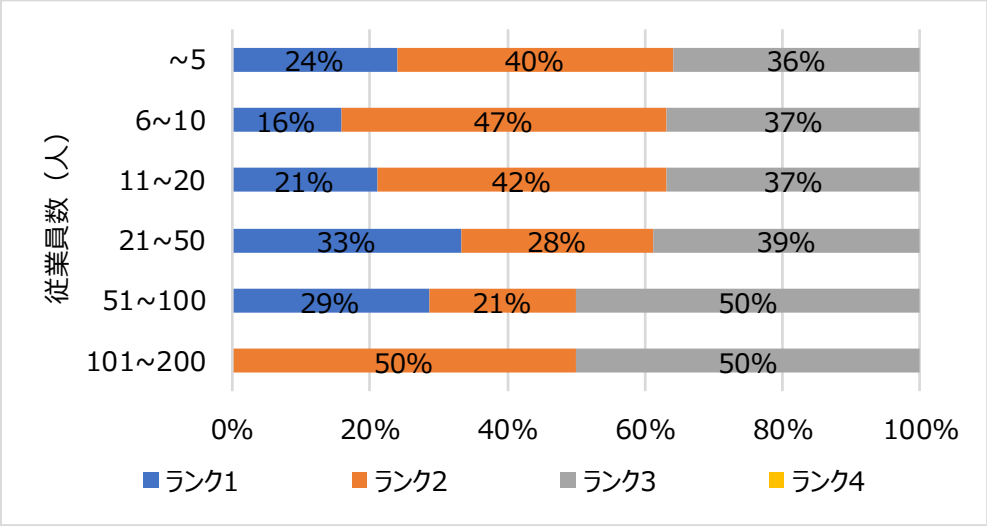


図 2.5- 10　コンテンツフィルタリスクランクの内訳（従業員数別）

以上、2.5.1～2.5.5のリスクランクの特徴をまとめると、高リスク（ランク3以上の要観察、即時対応）の割合は、従業員数11～20人、21～50人、51～100人で高く、10人以下、100人以上で低い、という傾向がみられた。つまり、従業員数11～100人（中規模）の中小企業は、セキュリティ対策をより必要としている企業群であるといえる。

その原因には、企業規模が大きくなるにつれて、ガバナンスが効きにくくなること、PC等のITネットワーク環境の管理運用ができていないこと等で、セキュリティレベルが低くなっている可能性が考えられる。他方、100名以上の規模になると、システム管理者を任命する余裕が生まれ、それら課題への対策が講じられていると推測できる。

2.6 インシデント対応

以下、本実証事業中に対応した全インシデント処理について示す。

2.6.1 インシデント処理の内容

実証期間中のインシデント処理を、下表2.6-1に示す。

対策項目	監視項目	発生件数（合計）	インシデント対応	
			オンライン対応	オンサイト対応
外部からの不正アクセス防止対策（ファイアウォール機能）	外→内のping/port-scan履歴	93,824件	全件ブロック	0件
不正な通信対策（IPS：不正侵入防止システム）	不正な通信(IPS)検知ログ（内→外、内→外→内を含む）	6,757,458件	4,770,889件をブロック※1（他は記録のみ）	2件
ウイルス・スパイウェア対策	HTTP・FTPウィルスチェック履歴	45件	全件ブロック	0件
	メール受信ウィルスチェック履歴	272件	全件ブロック	0件
	メール送信ウィルスチェック履歴	3,213,734件	―	0件
スパムメール対策	スパムメール判定履歴	93,824件	全件通知※2	0件
WEBフィルタリング対策	コンテンツフィルタログ	6,757,458件	全件ブロック	0件

表 2.6- 1　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。ただし本実証事業では、2.6.3で検知された重大リスク3件のうち、2件でオンサイト対応（駆け付け支援）を実施した。詳細は2.6.4で記述する。

2.6.2 コールセンターへのインシデント通知

危険性あるウイルスメールや不正な通信等は、一次措置となるUTM端末側のブロック機能（ポート遮蔽）により自動的に防御される。そのため、実証企業からコールセンターへのインシデント通知は発生しなかった。

他方、重大リスク（3件）が、nocでのリモート監視側で確認された。インシデントにつながる可能性のある事案であり、それら詳細と対応について、以下に記述する。

2.6.3 重大リスクの検知

実証企業の通信ログ監視にて、重大リスクとして選別されたものは下記3件。いずれも危険なサイバー攻撃であり、検知直後よりUTM端末で通信ブロックすることに加え、実証企業へ連絡して、対応措置を実施した。

・埼玉県X社：ランサムウェア感染　※潜在状態での検知
・群馬県Y社：マルウェア感染　※外部への攻撃拡散行為あり
　　ランサムウェア感染　※潜在状態での検知
・群馬県X社：標的型攻撃によるウイルスメール受信　※3か月継続

2.6.4 重大リスクの追加調査（インシデント対応）

以下、2.6.3で見いだされた重大リスク3件について、追加調査した結果を報告する。

———

対応１【埼玉県X社：ランサムウェア感染】

———

12月度にランサムウェアであるWannaCryのC&Cサーバーとの通信を検知、ブロックしている状況が判明。社内PCが感染している可能性が高く、追加調査が必要と判断。

対処内容（時系列）：

・不正通信の発信源企業とIP（1台分）を特定
・X社に電話で「該当端末を特定し、AVフルスキャンとWindowsセキュリティパッチの更新状況確認」を依頼するも端末を特定できず　※AV:アンチウイルス
・X社に訪問してNetwork構成を確認し、不正通信のIPが無線ルータであることを特定。本無線ルータにつないでいる端末が疑わしいと推測
・X社にヒアリングした結果、社長の家族が個別に持ち込んだ無線ルータであると判明。

プライベート端末の接続はセキュリティ上リスクがあることを説明、以下2点依頼した。

・プライベートのルータや端末等をつながないよう指導すること
・今回の無線ルータで使用した可能性のある全端末にAVフルスキャンを実施すること

経過観察：

1月度に不正通信は発生していない　⇒1月末にて対応完了。

———

対応２【群馬県Y社：マルウェア感染】

———

12月度に社外WebサーバーやFTPサーバーの脆弱性を突くサイバー攻撃の通信を検知、ブロックしている状況が判明。社内PCがマルウェアに感染し、サイバー犯罪の踏み台にされている（他社サーバーを攻撃させられている）可能性が高く、追加調査が必要と判断した。

対処内容（時系列）：

・不正通信の発信源企業とIP（3台分）を特定

・Y社に訪問し、情報システム責任者に「該当端末を特定し、AVフルスキャン」を依頼　※AV:アンチウイルス

・3つのIPのうち、該当端末を特定できたのは業務用PC1台。残り2台は、社内無線LANに社員がプライベート端末を自由に接続できる環境（DHCP）であるため、それらの端末である可能性がある。プライベート端末の接続はセキュリティ上リスクがあることを説明した。

・特定したPC1台は、1月度にランサムウェアであるWannaCryのC&Cサーバーとの通信も追加で検知、ブロックしていることが判明。AVフルスキャンを実施したがウイルスは検出されず。当該PCはOSを再インストールして初期化対応を依頼した。

・当該PCを利用している社員にヒアリングしたところ、以前、「セキュリティに問題があるので対策ソフトをインストールすることを勧める」といった内容のメールを受け、その通りに何らかソフトをインストールしていたことが判明した。

・不審メールの添付ファイルを開く等の行為はセキュリティ上リスクがあることを説明した。

経過観察：

PC初期化後に不正通信は発生していない　⇒1月末にて対応完了。

———

対応３【群馬県X社：標的型攻撃によるウイルスメール受信の増加】

———

10～12月度でウイルスメール100件を集中検知し、継続的にブロックしている状況が判明。検知数が多いため追加調査が必要と判断した。

対処内容（時系列）：

・X社と取引のある会社のメールサーバーがハックされたことによりメールアドレスが漏洩し、複数アドレスからマルウェア付きメールが送付されていたことがわかった。

・メール内容は賞与支払い、請求書支払い等を装うなりすましメールであり、標的型攻撃を受けていたことが判明した。

・X社に攻撃対象になっていることを通知し、UTM端末でブロックしている状況ではあるが、被害拡大がないように社員へ注意喚起した。

経過観察：

1月度にウイルスメールは発生していない　⇒1月末にて対応完了。

2.7 脅威シナリオ

以下、実証企業の通信ログデータ分析および検知された重大リスクから見いだされた、4種類の脅威シナリオ（ランサムウェアによる被害、標的型攻撃による被害、内部不正による情報漏えい、不注意による情報漏えい）について説明する。

2.7.1　ランサムウェアによる被害

PC（サーバー含む）やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、復旧に金銭を支払うように脅迫するランサムウェアと呼ばれるウイルスへの感染が確認されている。組織においては、業務を遂行する上で必要な情報を暗号化された場合、事業継続に支障がでるおそれがある。また、脅迫に従った場合、金銭的な被害も発生する。頻度は少ないが、データをロックされて業務停止に追い込まれることが多く、取引会社等に納品できなくなる等、影響度は極めて高い。

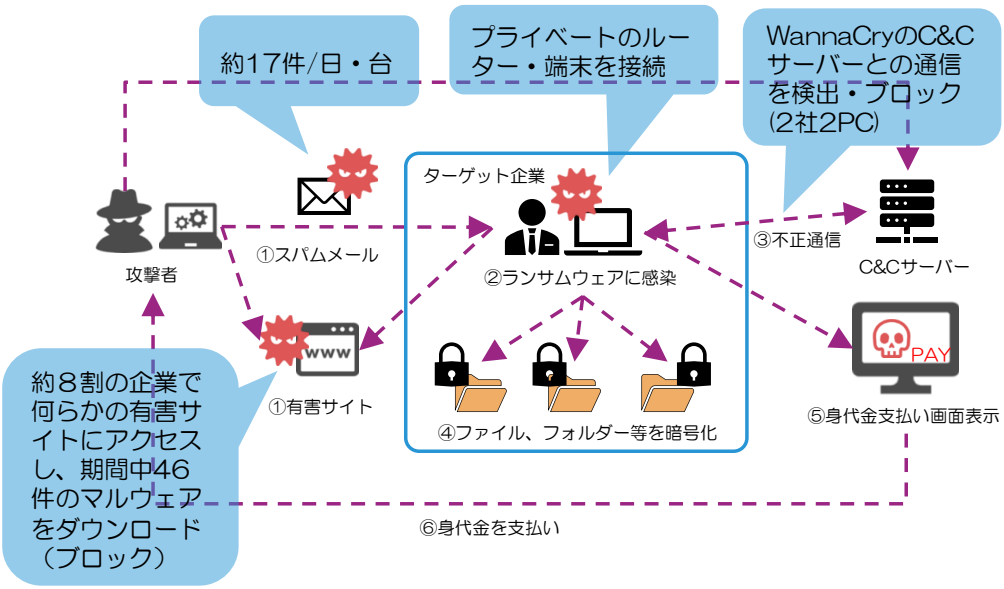


図 2.7- 1 ランサムウェアによる被害と実証結果

【攻撃手順】

①スパムメール、または有害サイトを利用してランサムウェアを配布

②PCがランサムウェアに感染

③外部（C&Cサーバー）と通信して不正ファイルを実行

④⑤⑥ファイル、フォルダー等を暗号化し、身代金支払い画面が表示され、被害者による身代金の支払いが行われる

【考えられる対策案】

・Webフィルタリング、アンチウイルス、アンチスパム機能によりマルウェアを検知、駆除する

・IPS/IDS機能により不審な通信を検知、ブロックする

・マルウェアを端末側で検知し、端末を隔離する
・スパムメール訓練等による社員教育を実施する
・プライベートのルータや端末等の使用を禁止する
・重要データはバックアップを取得しておく

2.7.2　標的型攻撃による被害

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が発生している。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。頻度は低いが、関係する会社から情報が盗み取られた場合をきっかけに攻撃標的化され、被害も大きく拡がる可能性が高い

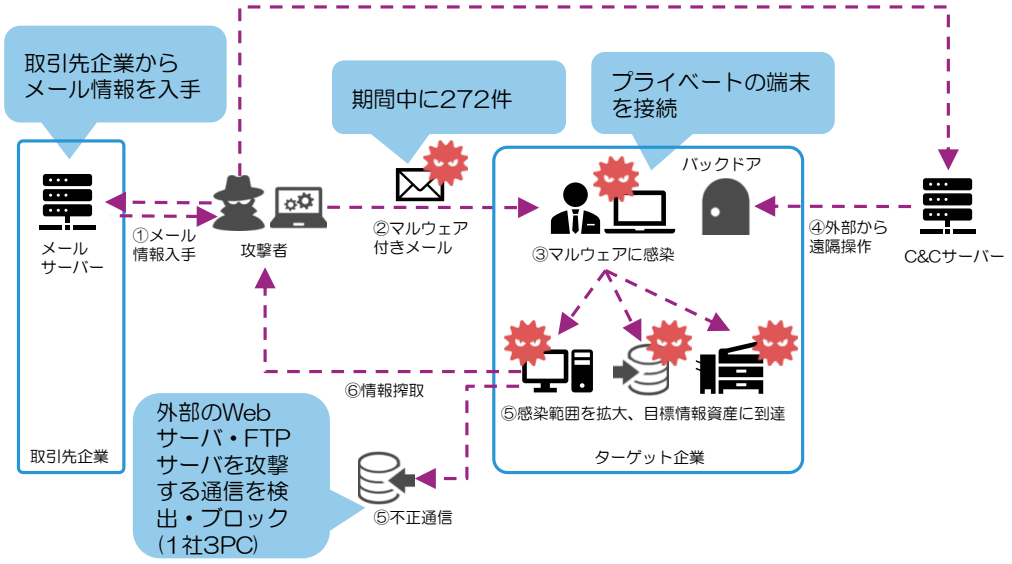


図 2.7- 2　標的型攻撃による被害と実証結果

【攻撃手順】

①ターゲット企業への攻撃の成功率を上げるため、取引先企業等のメールサーバーを攻撃し、メール情報を入手

②取引先企業になりすまし、メールへの返信を装う形でマルウェア付き、もしくはURL付きのメールを送りマルウェアが侵入

③～⑥外部からの遠隔操作から更なる感染拡大による情報漏えい、またはランサムウェアによる身代金攻撃等の被害が発生

【考えられる対策案】

・アンチウイルス、アンチスパム機能でマルウェアを検知・駆除する
・IPS/IDS機能により不審な通信を検知、ブロックする
・マルウェアを端末側で検知し、端末を隔離する

・標的型メール訓練等による社員教育を実施する
・プライベートのルータや端末等の使用を禁止する

2.7.3　内部不正による情報漏えい

　従業員や元従業員等の組織関係者による機密情報の漏えい、悪用等の不正行為が発生している。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。頻度は高く、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、甚大な被害になる可能性がある

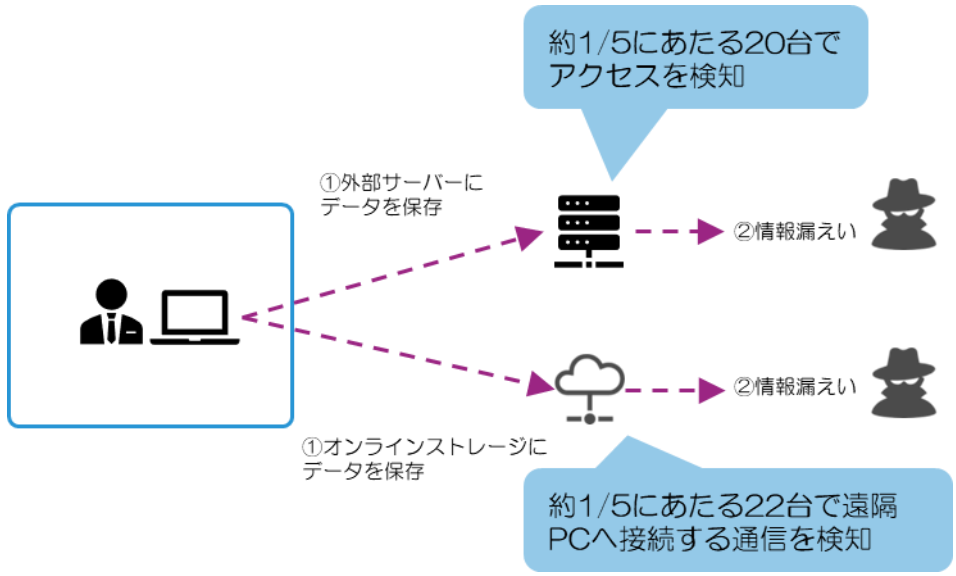


図 2.7-３　内部不正による情報漏えいと実証結果

【発生順】
①従業員が（業務上許可されていない）オンラインストレージや外部サーバーに機密情報を保存
②外部に機密情報を持ち出し、または機密情報が漏えい

【考えられる対策案】
・セキュリティポリシーを策定する
・システムの操作履歴を監視する
・コンプライアンスに関する社員教育を実施する

2.7.4　不注意による情報漏えい

　組織や企業では、情報管理に対する意識の低さや確認漏れ等により、従業員による個人情報や機密情報の漏えいが後を絶たない。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。頻度は高く、Webサービスに組み込まれたAPIからも情報が盗み取られる可能性があり、信頼できるサービスか否かの判断が随時必要である。

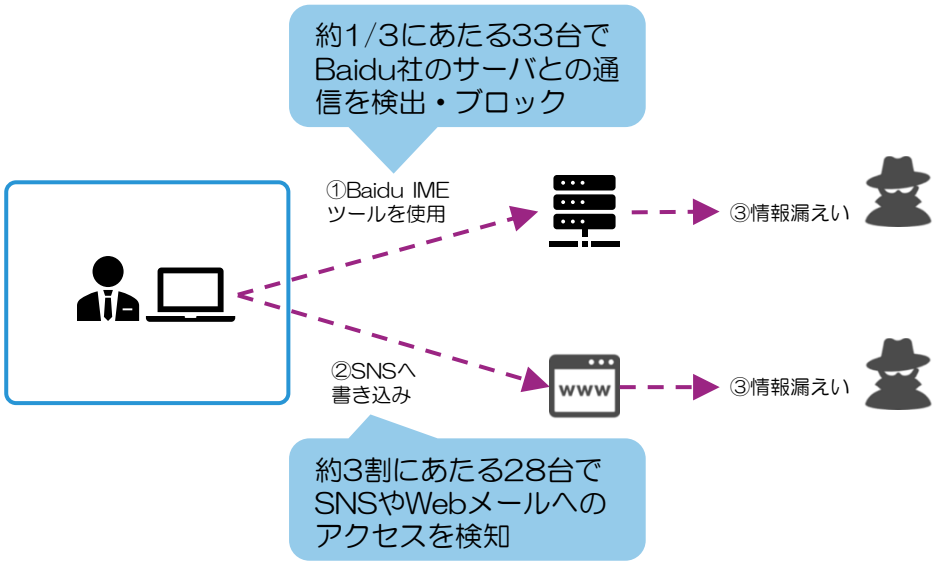


図 2.7- 4　不注意による情報漏えいと実証結果

【発生順】

① 従業員がBaidu IMEツールを使用

② 従業員がSNSに機密情報を書き込み

③ 外部に機密情報が漏えい

【考えられる対策案】

・セキュリティポリシーを策定する

・利用しているシステムの情報を監視する

・サイバーセキュリティに対する意識啓発の教育を実施する

2.8 中間報告会の実施

以下、中間報告会の実施結果について報告する。

2.8.1 中間報告会の開催結果

実証企業でのログ分析結果、中小企業のサイバー攻撃被害の実態に関する報告を目的として、中間報告会を企画・開催した。アジェンダは、下記の3項目とした。

- サイバーセキュリティ対策の普及に向けた国等の支援事業について（IPA）
- UTM端末ログ分析結果の報告
- 中小企業向けサイバー保険の在り方について

中間報告会の開催結果を、下表2.8-1に示す。実証地域の5県で各1回ずつ開催。参加数は合計26社、うち実証企業の参加は埼玉県2社のみとなった。実証企業の少なさについては、富士ゼロックスからの声掛け、販売会社の営業・CEによる開催チラシの配布に効果がみられなかったこと等が原因である。群馬県では参加社数が0社、茨城県では参加社数が1社のみとなった。それら参加社数の少なさには、台風19号の被害による開催日程変更が大きく影響した。

開催地	日程	場所	開催告知	**参加企業（参加人数）**	**実証参加企業**
長野	11月18日	諏訪市公民館 協力： 岡谷商工会議所 諏訪商工会議所 下諏訪商工会議所 茅野商工会議所 諏訪圏ものづくりネットワーク	①月度会報誌へのチラシ折込 ②電話勧誘 ③WEB告知	**9 (9)**	**0**
栃木	12月13日	栃木県産業交流センター 協力：栃木県	①FAX配信 ②電話勧誘 ③WEB告知 ④チラシ配布	**5 (9)**	**0**
群馬	12月16日	前橋商工会議所 協力：FX群馬	①電話勧誘 ②WEB告知 ③チラシ配布	**0**	**0**
埼玉	12月17日	ランド・アクシス・タワー 協力：FX埼玉	①電話勧誘 ②WEB告知 ③チラシ配布	**11 (14)**	**2**
茨城	12月19日	土浦商工会議所 協力：FX茨城	①電話勧誘 ②WEB告知 ③チラシ配布	**1 (1)**	**0**

表 2.8- 1　中間報告会の開催結果

2.8.2 中間報告会開催での参加者の反応

以下、中間報告会で得られた参加者の反応を示す

アンケート結果（n=19、1社2名以上の回答も含む）

回答率は（約58%、26社中15社）。95%が“参考になった”“とても参考になった”との回答。ウイルス対策については約9割で実施しているが、不正アクセス対策まで実施している割合は約4割と低い。セキュリティ事故は、約2割で経験している。サイバー保険については約7割が“知らない”、さらに保険加入している企業は0社との回答だった。

（自由記述）

・中小企業でもサイバー攻撃を受けていることがわかった

・サイバーセキュリティについて考える必要性を感じた

・エモテット被害に対する対応策を知りたい（栃木参加者、対応済み）

・従業員の意識が低く、持ち出し用PCを社内LANに勝手につないだりする等、ルールを守らないので、エンドポイントのケアをしっかりしたいと考えている（埼玉参加者）

・サイバー保険の普及状況を知りたい（茨城参加者）

・チラシの手渡し、FAX等で積極的に報告会への参加を勧誘したが、思うように参加者を集められなかった。県内企業のサイバーセキュリティに対する意識の低さを感じた（後援いただいた栃木県庁の職員）

・中間報告会のログ分析結果を聞いて、サイバーセキュリティ対策の普及活動を継続していく重要性を再認識した（栃木県庁の職員）

・「商工会議所にもサイバーセキュリティの相談窓口を作ること」「地域のセキュリティスペシャリスト相談員をリスト化し、もしもの場合の地域支援体制を作ること」が必要だと感じた（岡谷商工会議所の職員）

2.8.3 中間報告会開催での気づき

各地域で中間報告会の集客活動は難航した。最初の事業説明会同様に、中小企業でのサイバーセキュリティに対する意識は低いと感じた。報告会に参加した企業からは、「中小企業でもサイバー攻撃を受けていることを初めて知った」「サイバーセキュリティ対策の必要性を初めて認識した」という感想が多くあり、説明会を開催することの必要性は大いにあると確信した。

また、アンケート回答のほぼ全員から“参考になった”“とても参考になった”との回答を得ていることから、中小企業側の（サイバーセキュリティの必要性に関する）意識変革が徐々にできつつあると感じた。県庁職員や地域商工会議所の担当者から「報告会の説明を聞いて重要性を再認識した」「商工会議所にもサイバーセキュリティの相談窓口を作る必要があると思う」等の意見がでており、サイバーセキュリティ対策普及には、地域側（の支援体制）と連携推進していくことが重要であると感じた。

2.9 最終報告会の実施

以下、最終報告会の実施結果について報告する。

2.9.1 最終報告会の開催結果

今回の実証事業でわかった中小企業のサイバー攻撃被害等の実態に関する報告を目的として、最終報告会を開催した。

- 中小企業におけるサイバーセキュリティ対策支援事業のご紹介（IPA）
- 中小企業におけるサイバー攻撃の実態について
- 中小企業がとるべきサイバーセキュリティ対策

最終報告会の開催日程を、下表2.9-1に示す。

開催地	日程	場所	開催告知	参加企業（参加人数）	実証参加企業
埼玉	1月22日	春日部商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 （事前レポート勉強会実施）	**9 (10)**	**0**
群馬	1月22日	高崎商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 ④会員企業にLINEで参加呼びかけ （商工会議所）	**3 (3)**	**3**
埼玉	1月23日	さいたま商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 （事前レポート勉強会実施）	**7 (12)**	**0**
埼玉	1月27日	所沢商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 （事前レポート勉強会実施）	**5 (5)**	**0**
埼玉	1月28日	川越商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 （事前レポート勉強会実施）	**10 (10)**	**1**
埼玉	1月29日	蕨商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 （事前レポート勉強会実施）	**4 (5)**	**0**
茨城	1月29日	水戸商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 ④会員企業にFAXで参加呼びかけ（商工会議所）	**1 (1)**	**0**
栃木	1月30日	とちぎ産業交流センター 協力：栃木県	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布 ④SUBARU栃木製作所様へ連絡	**5 (6)**	**0**
長野	2月14日	上田商工会議所 協力：同上	①実証参加企業へ電話による直接勧誘 ②WEB告知 ③チラシ配布	**2 (2)**	**1**

表 2.9- 1　最終報告会の開催結果

実証地域の5県において、群馬県、茨城県、栃木県、長野県で各1回ずつ、埼玉で5回の合計9回開催。参加は合計46社、うち実証企業の参加は5社となった。最終報告会ではこれまでの開催告知に加えて、実証参加企業に対しては電話での直接勧誘を行ったが効果は限定的であった。全

ての実証参加企業に対しては、1月末での実証終了に伴い、今回の実証結果について個別に報告するフォロー活動を実施した。

2.9.2 最終報告会での参加者の反応

以下、最終報告会で得られた参加者の反応を示す。

アンケート結果（茨城県、栃木県、群馬県、長野県：n=13　※1社2名以上の回答も含む）

回答率は（100%、11社中11社）。92%が“参考になった”“大変参考になった”との回答。ウイルス対策については100%で実施しているが、不正アクセス対策まで実施している割合は約2割と低い。セキュリティ事故は、約4割で経験している。サイバー保険については約6割が“知らない”、さらに保険加入している企業は0社との回答だった。

アンケート結果（埼玉県：n=34　※1社2名以上の回答も含む）

回答率は（約86%、30社中35社）。報告会を聞いて、約9割が“自社がサイバー攻撃を受けるリスクはあると思う”と回答。報告会を聞いて、“改めてサイバーセキュリティ対策を検討したい”との回答が約7割だった。

（自由記述）

・IPAのガイドライン、SECURITY ACTIONがあり、他社へのアピール方法があることを知ることができた（群馬参加者）

・社内に専門家がいないので、実際にインシデントが発生した場合の問い合わせ先がわからない不安がある（群馬参加者）

・今回の報告書を参考にして社員に重要性を伝えたい（群馬参加者）

・ウイルス被害の事例はわかったがもう少し具体的な情報を知りたかった（群馬参加者）

・UTMが自社の状態をモニタリングするツールとて有用であることがわかった（栃木参加者）

・少なくともヒューマンエラーによる脅威はなくしたい（栃木参加者）

・実際にサイバー攻撃を受けている実態が分かり、サイバーセキュリティ対策の重要性を再認識した（水戸商工会議所の職員）

・UTMでも防ぎきれない脅威に対する対策方法を知りたい（埼玉参加者）

・スパムメールのリスク等を心配している。社内ルールの整備についても相談したい（埼玉参加者）

・情報漏えい対策等、社員に説明するきっかけが作れた。また自社が加害者にならないための行動が必要だと改めて思った（埼玉参加者）

・早速「情報セキュリティ5か条」を社内で実施したい（長野参加者、実証企業）

2.9.2 最終報告会での気づき

実証企業へ直に電話勧誘する等で積極的に開催告知をしたが、集客活動は難航した。最終報告会に参加した企業からは“自社がサイバー攻撃を受けるリスクはあると思う”（約9割）“改めてサイバーセキュリティ対策を検討したい”（約7割）との回答があり、報告内容については、中小企業のサイバーセキュリティの必要性に関する意識変革につながると確信した。

しかしながら、重要性を認識しても「何から取り組めばいいかわからない」という中小企業の声は多い。そのような中小企業にむけて、IPAが公開しているSECURITY ACTIONの取組み（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）を紹介しているが「最適な施策であるが、今回の報告会で説明して初めて知った」という声がほとんどであった。

以上から、サイバーセキュリティに対する意識変革を促すとともに、具体的な取り組みであるSECURUTY ACTION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が重要であると考える。

2.10 アンケート回収結果

以下、実証企業のアンケート調査結果を示す。

2.10.1 中小企業のサイバーセキュリティに対する意識、および現状確認

調査目的：実証企業のサイバーセキュリティに対する意識調査
調査対象：実証企業（101社）
調査方法：郵送、FAX、電話等
有効回収数：49、回収率：49%

Q1：本実証事業への参加を決めた理由をお選びください

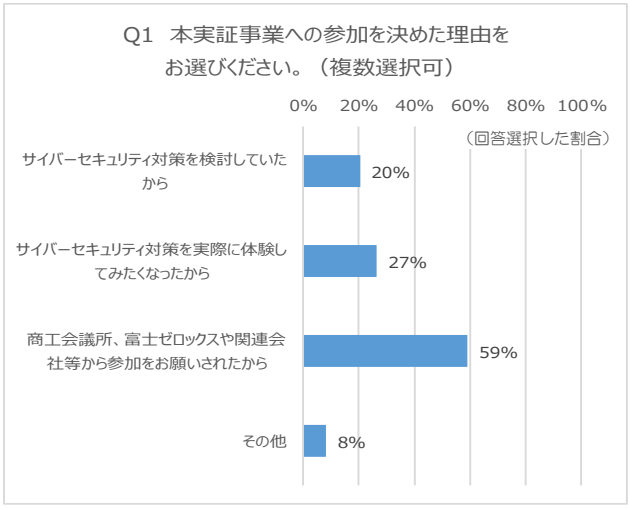


図 2.10- 1　実証参加の理由

約2割がセキュリティ対策を検討、約3割が体験してみたかったと回答していることから、中小企業側のセキュリティ対策ニーズは少なからずあるといえる。しかしながら、約６割が声をかけられたことでの参加と答えており、まだ積極的にセキュリティ対策を導入する意識にはない（優先順位は低い）と考えられる。

Q2：UTMを導入するにあたって気になったことをお選びください

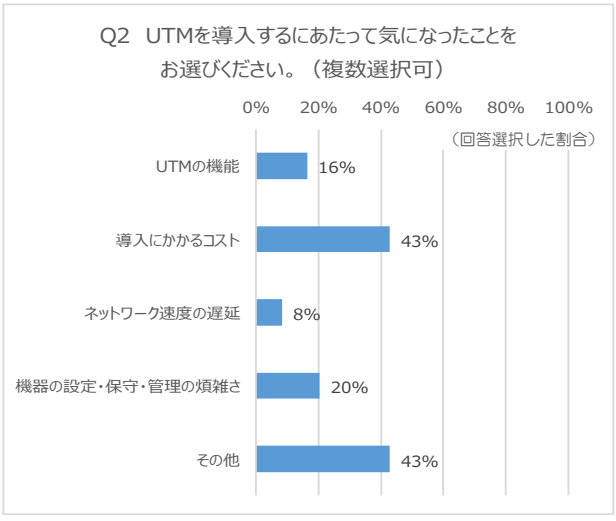
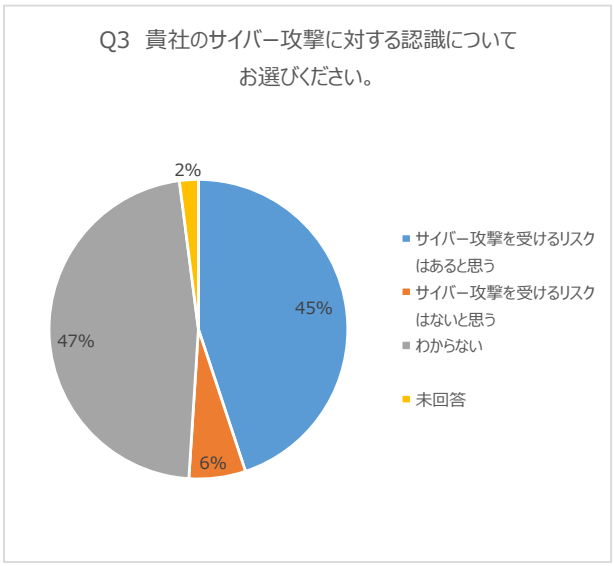


図 2.10- 2　UTM 端末導入での懸念点

UTM端末導入の懸念点は、約4割の企業がコスト負担について、続いて約2割が機器の設定・保守・管理の煩雑さを指摘している。その他では“そもそもわからない”が多く、UTM端末の機能・必要性について理解できていない企業が多い、といえる。

Q3:貴社のサイバー攻撃に対する意識をお選びください



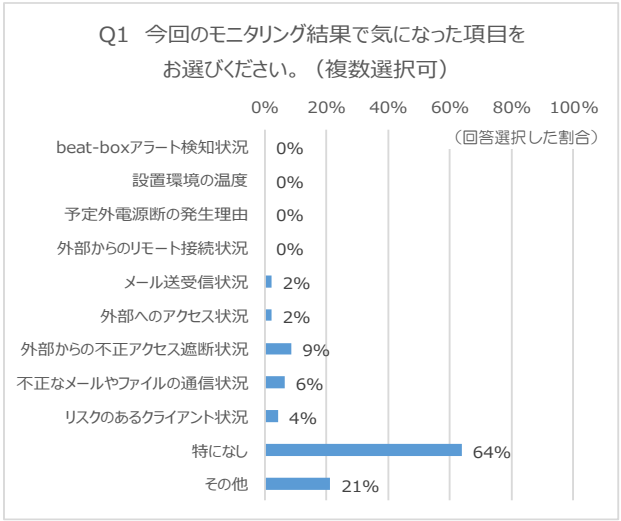
“サイバー攻撃のリスクはない”“わからない”“未回答”が合わせて5割以上あり、サイバーセキュリティ対策の緊急性については、十分に浸透していないと考えられる。残り5割弱は、サイバー攻撃を受けるリスクはあると認識している。

図 2.10- 3　サイバー攻撃に対する意識調査

2.10.2 ログ分析結果の感想および意識の変化

調査目的：実証企業のログの分析結果に対する意識調査
調査対象：実証企業（101社）
調査方法：郵送、FAX、電話等
有効回収数：47、回収率：47%

Q1:今回のモニタリング結果で気になった項目をお選びください



モニタリングにより収集した通信ログの分析結果を説明しているが、未だ自分事には感じられず、興味喚起＆危機醸成ができていない状況である。

図 2.10- 4　モニタリング（ログ分析結果）で気になった項目

Q2:貴社でサイバーセキュリティ事故が発生した場合、想定される影響についてお答えください

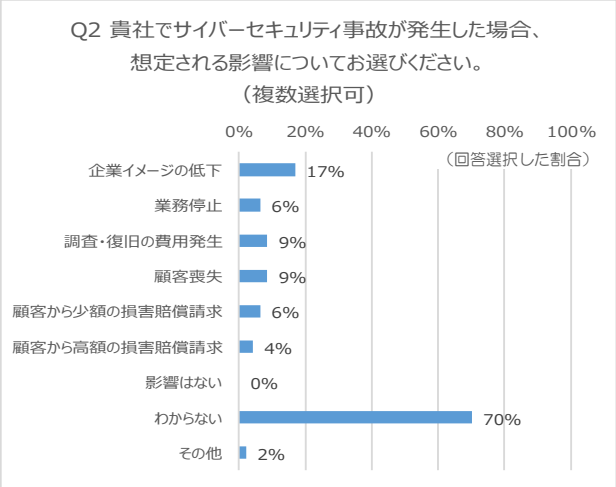


図 2.10- 5　サイバーセキュリティ事故発生で想定される影響

サイバーセキュリティ事故により想定される影響について、7割が分からないと答えており、サイバー攻撃を理解するための基礎知識が不足して、脅威シナリオが周知されにくいことが分かる。

Q3：貴社でサイバーセキュリティ事故が発生した場合、必要なサポートについてお聞かせください

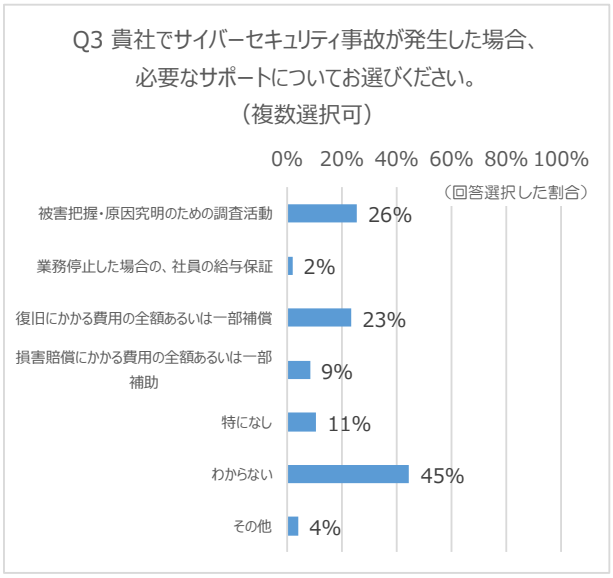


図 2.10- 6　サイバーセキュリティ事故発生時に必要となるサポート

サイバーセキュリティ事故が発生した場合に必要となるサポートについて、5割近くが分からないと答えており、多くの中小企業では、サイバー攻撃（による被害）を想定した備えができていないことがわかる。一方、3割近くが被害状況の把握、原因究明のための調査活動に関するサポートが必要と回答している。

2.10.3 サイバーセキュリティ対策の継続必要性と要望

調査目的：実証企業のサイバーセキュリティに対する意識調査
調査対象：実証企業（101社）
調査方法：郵送、FAX、電話等
有効回収数：47、回収率：47%

Q1：サイバーセキュリティ対策の継続は必要と思いますか？

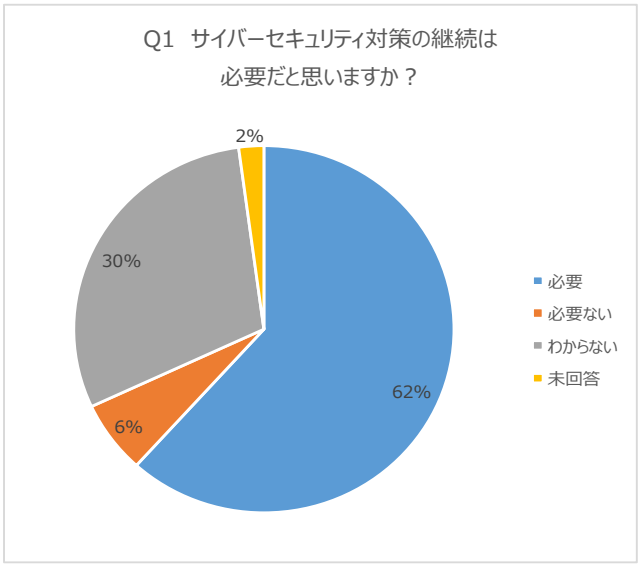


図 2.10-７ サイバーセキュリティ対策の継続必要性

今回の実証を通じて、約6割がサイバーセキュリティ対策は必要と回答（危機意識の醸成）。しかしながら、残り4割は“分からない”“必要ない”と回答するなど、さらなる中小企業への情報提供や共感を促す施策が必要であると考える。

Q2：Q1で“必要”と回答された方へ、継続利用で期待する条件をお選びください

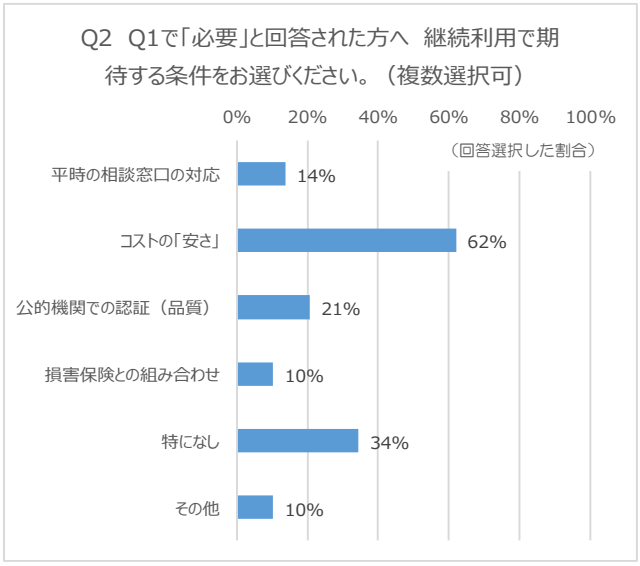


図 2.10-８ サイバーセキュリティ対策の継続利用で期待する

必要であると答えた人の約6割が、コストを安くしてほしいとの回答である。中小企業の多くが経済的支援を要望する、という結果が得られた。

Q3：サイバーセキュリティ対策に関して政府に期待することをお選びください

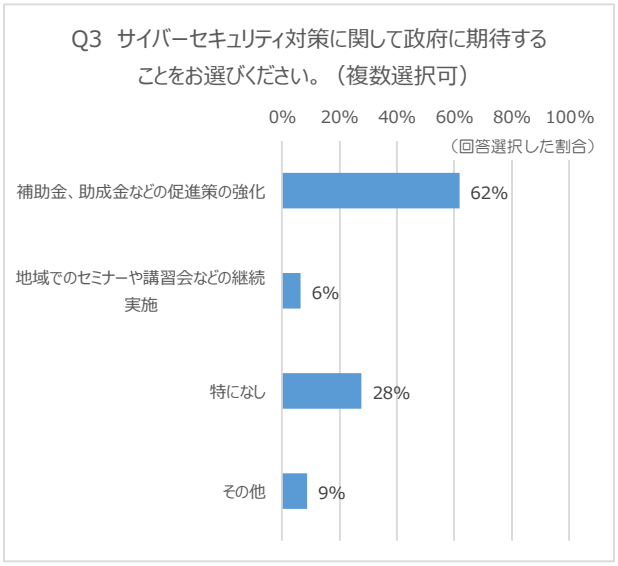


図 2.10- 9　サイバーセキュリティ対策で政府に期待すること

政府施策に対する支援として、補助金や助成金に対する期待は大きく、セミナーや講習会への要望は少なかった。

2.10.4 サイバーセキュリティ対策への意識の高まり

――――

調査目的：実証企業のサイバーセキュリティに対する意識調査

調査対象：実証企業（101社）

調査方法：郵送、FAX、電話等

有効回収数：40、回収率：40%

――――

Q1　業務上の支障はなかったか、不便さはどうか

- 支障はない（23）
- 色々なホームページにつながらなくなった（3）
- インターネットアクセスのレスポンスが低下した（3）
- わからない（1）

――――

　UTM端末設置により、少なからず業務に支障が出ていたようである。普及促進につなげていくためには、これら不満を解消させていく必要がある。

Q2　社員の皆さんの反応はどうか（意識の変化はあったか）

- 意識変化は特にない（17）
- 反応を確認していない（10）
- つながらないホームページがあり困っている（2）
- 多少の意識啓発につながっている（1）

・良い（1）

———

中小企業側への意識啓発（の効果）は低かったようである。

Q3　関係先、取引先でのセキュリティ対策は進められているか（意見交換してみたか）

・意見交換していない（27）
・わからない（9）
・「Windows7使うな」等、色々指摘されるが業務アプリが対応していない（1）
・取引先から問い合わせはある（1）

———

周辺企業とのセキュリティ対策を確認したが、関心事にはならず、意見交換すら行っていない実態が分かった。しかしながら、一部企業では、取引先から問い合わせやガイドラインが提示されているようであり、さらに要請が高まることで、セキュリティ対策の普及促進が加速すると考える。

Q4　セキュリティスペシャリスト（診断士）の支援を必要とするか

・検討したことがない（11）
・必要と感じていない（4）
・わからない（2）

———

セキュリティスペシャリスト（診断士）の情報提供を行ったものの、具体的なアクションについての知識が無い状態であり、現時点でのニーズは低い。

2.10.5 サイバーセキュリティ対策継続のための要件

———

調査目的：実証企業のサイバーセキュリティ対策に対する意識調査
調査対象：実証企業（101社）
調査方法：郵送、FAX、電話等
有効回収数：40、回収率：40%

———

Q1　今後、サイバーセキュリティにかけられる費用（総額）はいくらぐらいか

・検討したことがない（14）
・わからない（12）
・数千円/月（6）
・安ければ安いほどいい（4）
・効果があれば少しはいいが1万円/月は高い（1）
・1万円以内/月（1）

・5000円/月（１）
・費用はかけたくない（1）

———

セキュリティ対策費用については“安ければよい”“わからない”という声が大半であり、具体的に検討されていない実態がわかる。身近な対策であるPCウイルスソフトとUTM端末を比較する声は多く、UTM端末がサイバー攻撃に対して効果的である理解促進ができていない。さらなる情報提供や理解促進が必要である。

Q2　もしも被害にあった場合のことを考えて、サイバー保険は必要かどうか

・わからない（16）
・検討したことがない（9）
・必要（6）

———

サイバー保険については、“わからない（脅威シナリオについての知識が不足）”“検討したことが無い（被害想定が考えられない”等の声が大半となった。必要とした6社は、すでに検討し始めていた背景があり、「なにかしら導入したい」というコメントであった。

Q3　全般的な感想（やってよかったか、悪かったか）

・わからない（14）
・良かった（12）
・大変良かった（3）
・不便である（2）
・大変良かった。継続利用を検討している（１）

———

全般的な感想としては、半数に“やってよかった”と感じてもらえているが、残りの半数は“分からない”“不便である”等の回答となった。

2.10.6 実証参加への感想（良かった点、悪かった点）

良かった点：

・あまり意識していなかったサイバーセキュリティの重要性について、説明してもらえたこと
・ネットワークの現状を調べてもらえたこと（IT管理者がいないため）
継ぎ足しで複雑化していたネットワーク（配線、接続機器）を整理してもらえたこと
・ネットワークの使い方（内部要因）にもリスクが潜んでいることが分かったこと
・ネットワークやサイバーセキュリティについて、相談できる相手ができたこと

———

悪かった点：

・申し込み後、調査から設置まで、かなりの時間を要したこと（想定外だった）
・設置時に、ネットワークが切断され、一次的に利用できなくなったこと（想定外だった）
・設置までの契約等の手続きが長かったこと（とても面倒だった）
・時間をかけて検討したが、設置できないという結果になったこと（時間が無駄になった）

2.11 関係者との協議、情報交換

以下、様々な関係者と協議、情報収集した結果について記述する。

2.11.1 地域側の関係者との協議

本事業で関係いただいた地域行政、自治体、商工会議所、地域経済団体、地域ITベンダーと意見交換して、サイバーセキュリティ対策のための継続的な地域支援について検討した。地域での普及促進のためには、普段からの情報共有が必要であること、支援施策を中小企業の目線で考えることの指摘があった。具体的には、下記の2項目（５つの課題）への対応である。

【中小企業側の課題】：危機感の無さ、IT環境整備の遅れ、知識・人材の不足
【対策支援での課題】：身の丈に合わないコスト負担、中小企業側の多様性

危機感の無さ

中小企業の多くは、サイバー攻撃による被害（事業停止や費用請求）や周辺他社への被害拡散・損害賠償の実感がない。情報が足りていないために、想像もできないという回答が多い。

IT環境整備の遅れ

中小企業のITネットワークが老朽化、最新システムへ更新できていない状況である。人材不足で管理・整備するリソースが充てられていない、IT導入補助金などの経営支援策が進められているが、すべての中小企業には行き届いてはいない等の課題がある。

知識・人材の不足

中小企業が、身近に相談できる（寄り添い、支援する）相談員が足りていない。経営指導役である中小企業診断士、ITコーディネータに加えて、情報処理安全確保支援士（登録セキスペ）の認知・活用を広げていく必要がある。

身の丈に合わないコスト負担

中小企業側には、費用負担する余裕はない。サイバーセキュリティ領域で、何を対策化すべきかの必要最低限を明確にしなければならない。「製品・サービスが高額すぎる」との意見も多く、中小企業向けとしての最適化は今後の課題である。

中小企業側の多様性

中小企業の多くで、サイバーセキュリティ対策の大切さについては理解しているが「何から着手すれば良いか、具体策が分かりにくい」と回答している。しかしながら、中小企業側の多様性が高く（事業の規模や業務内容でITネットワークが大きく異なる）、共通での支援施策が展開できないという難しさがある。

2.11.2 社外セキュリティ専門家との協議、情報交換

本事業の結果について、近年のサイバー攻撃に見られる一般的な動向、大企業などの中小企業以外のサイバーセキュリティ対策との比較等について、社外セキュリティ専門家（大手セキュリティベンダー技術者、情報セキュリティ分野の学術専門家等）へ第三者意見をヒアリングしたので、その結果を記述する。

本実証のデータをみると、外部からのサイバー攻撃については、大企業と中小企業に違いは感じられなかった。インターネットに接続した状態であれば、皆が同じ条件で攻撃を受けることの覚悟が必要であり、セキュリティの穴があれば、いつでもどこからでも侵入される危険性があるといえる。また、標的型攻撃での情報漏えいが確認されており、サプライチェーン全体へ攻撃拡散してしまう可能性が高く、至急の対策が必要であると考える。

中小企業からのアンケート回答や意見交換から、中小企業側で（サイバー攻撃を受ける）穴を空けていることの自覚がないこと、その危機感や責任意識が低いこと等も明らかになった。防御策がとられていないことで、中小企業の社員が直にサイバー攻撃に晒されることになる。現状、社員までサイバー攻撃の予備知識が共有されていないことが多く、不意な操作等でウイルス感染しやすく、被害が発生しても対処できない（被害が拡大しやすい）という状況へ発展しやすいと考える。

普及促進のポイントは、中小企業（の社員）にとって自分事化できる脅威シナリオである。サイバーセキュリティ対策の一般論だけでなく、中小企業のどこにリスクが潜んでいるのか、どんな行動により（知らず知らずのうちに）情報が漏えいする危険性があるのか等について、より具体的な例を使って中小企業（の社員）へ周知させなければならない。ランサムウェア等による業務停止や金銭要求などの実被害を事例紹介することも効果的と考える。

技術的な面では、UTM端末設置により、サイバー攻撃の可視化とリスク検知・防御ができたと考えており、UTM端末設置は中小企業にとっても有効であると感じた。ネットワーク上で経過観察や、駆け付け支援等の対処の実施についても、知識・リソース不足で対策を講じられない中小企業にとっては必要な支援となる。しかしながら、手厚いサービスはコスト高になり、中小企業には費用負担が難しくなるので、いかにコストが安くできるのかも検討しなければならない。

費用負担の面では、社会側でサイバーセキュリティの共通基盤整備を進めることも重要である。社会側の基盤整備で、個別の中小企業がかかる費用を少なくできると良い。セキュリティに関する専門的判断などは、今後、人工知能活用も進められていくのではないかと考える。

製品・サービスの面では、中小企業をひとくくりにせず、いくつかのカテゴリー分け（情報資産別、リスク別）が重要である。中小企業が保有している情報資産の価値や情報漏えいによる取引先会社へ及ぼす影響など、社会での責任範囲に応じたセキュリティ対策として、投資が行われるべきである。なお、サイバー攻撃に対して穴をあけていることの（中小企業側の）責任範囲が明確になっていないことは、社会的な問題であり、早急に検討・改善されるべきと考える。

2.11.3 保険会社との協議、情報交換

中小企業むけのサイバー保険について、保険会社と協議した結果を記述する。

保険運用には、損害賠償以外にもかかる様々な費用（調査・対策等）について検討しなければならない。今回の実証企業101社での実被害は発生しておらず、UTM端末によるリモート監視およびリスク検知の段階で対処することで、実被害につながるインシデント発生が、かなり防御されることが分かった。中小企業のサイバー保険にとって、調査・対策（にかかる費用）が重要な要素になることが部分的に確かめられたと言える。

賠償額の検討では、中小企業ごとの査定（リスク量の算出）が必要となる。中小企業ごとの調査結果や対策状況に応じたシミュレーション、内部の情報資産の棚卸、サプライチェーンに広げた被害シミュレーションも実施しなければならない。さらには、これからのサイバー攻撃がどうなっていくのか、使用しているセキュリティ製品・サービスの種類や機能は何か、正しくアップデートされているかなどについて確認する等、いかに正しく保険運用にするかついて、詳細検討していかなければならない。

短期的な対策としては、サイバーセキュリティの製品・サービス（を提供しているITベンダー）側を包括して引受ける、商品付帯型の保険を組み込むのが好ましいと見立てている。それら製品・サービスによるモニタリングにより、インシデント発生の経緯や被害状態を把握する仕組みにもなり、モニタリングで高リスクの被保険者（中小企業）が見つかれば、そのリスクレベルに対応した保険商品を追加提案することができ、被保険者にとっての付加価値につながる。

他方、保険営業側では、中小企業向けサイバー保険が低価格であることにも検討が必要である。保険商品を販売する営業（代理店）のインセンティブを高くできないこと、個別に調査費用をかけると採算性が取れなくなる等の問題がある。

なお、自動車保険の等級制度のような仕組みは、サイバー保険に適用することは難しい。企業により大きく異なるサイバーリスク量を、母数が大きく異なる自動車保険と同様にテーブルを作成してリスク量を決める事は現実的ではないためである。そのため、サイバー保険は（火災保険のような）個別査定が必要であり、中小企業個別のリスク量に応じた補償額（支払い限度額）が設定されるべきと考える。

海外のサイバー保険の例では、セキュリティ被害にあった企業が、翌年に他社のサイバー保険に乗り換える事例も発生している。保険料の増額を避けた行動であり、日本のサイバー保険制度の在り方については、これから様々なケースにもとづいた議論が必要である。

サプライチェーンに関する保険については、大企業発でサプライチェーン末端の中小企業までをカバー範囲とする保険設計は技術的に可能であり、多くの開発余地が残っていると考えている。企業間での調達基準や取引先選定基準が厳しくなっていく可能性があり、将来的には、取引で発生する中小企業側の損害賠償責任を明確にしていくことには意味がある。

考察・提言

3.1 実証企業でのサイバー攻撃の実態

以下、実証により見えてきた中小企業へのサイバー攻撃の実態について考察を示す。

実態１：中小企業へサイバー攻撃のリスクが拡大している

重大リスクの発生頻度は101社中の3社（約3%）であった。平均2か月のデータ取得期間であったことから、単純計算で6倍の12ヶ月に換算すると約18%となる。つまり、年間では中小企業5社あたり1社が被害を受ける可能性を示唆している。この結果は、一部サンプリングでの推測値ではあるが、5社あたり1社が被害を受けるという確率は非常に高く、中小企業へサイバー攻撃のリスクが拡大していることがわかる。

実態２：サイバー攻撃（感染している状態）に気づけていない

標的型攻撃が検知された。その標的型攻撃は10月に突然発生し、その後12月までの3か月間、100通をこえるウイルスメールが送付されていた。対象となった実証企業はそのサイバー攻撃に気づかず、その攻撃起点になっていた関連会社（最初に被害があった会社）からの通知もないという状況であった。相互に認知できていない（結果、対処できない）状態は非常に危険であり、それら企業から漏えいした情報によって、連鎖的に被害拡大する可能性がある。

実態３：自らがサイバー攻撃の加害者にされている可能性がある

自社の（内部PCの）ウイルス感染により、他社へ攻撃を仕掛けている重大リスクが確認できた。不意な操作によるウイルス感染で、自社がサイバー攻撃の加害者になってしまう事案であるが、その実証企業では、そのウイルス感染に気づかずに通常業務を継続していた。近年のサイバー攻撃では、自らが攻撃の起点にされる可能性もあり、起きうる可能性を考えて対策を講じなければならない。

実態４：UTMでは防御しきれないリスクが増加している

中小企業が様々なWebサイトへアクセスして、グレイウェアのダウンロードやクラウドサービスを利用している実態が明らかになった。ユーザーが意図して利用するグレイウェアやクラウドサービスについては、UTM端末では必ずしも防御できない。そのため、利用する側の中小企業（の社員）のセキュリティ意識が問われることになるが、セキュリティ意識が低い場合には、いつでもウイルス感染や情報漏えいというリスクが起こりうる。今回の実証企業では、それら社員の利用実態について、把握できているという経営者は極めて少なかった。

実態５：もしもの場合の対処ができない

危険性の高いランサムウェア（WannaCRY）の通信を検知して、駆け付け支援を実施した。その駆け付け支援が無かった場合には、PCロックで業務停止され、さらに金銭要求まで発展したかもしれない。他方、実証企業側はランサムウェアの感染に気づいておらず、富士ゼロックスか

らの駆け付け支援で、初めて感染状況を知ることになったが、感染を知らされても、いかに処置したらよいのかわからないという状況であった。

3.2 中小企業で必要となるサイバーセキュリティ対策

以下、本実証を通じて明らかになった中小企業で必要となるサイバーセキュリティ対策について考察する

対策１：サイバー攻撃の危機感を醸成する情報提供

中小企業側のサイバー攻撃に対する危機意識の低さが顕著にみられた。通信ログの分析評価結果や脅威シナリオを示しても、サイバーセキュリティについて自分事で考えられる実証企業側の担当者は極めて少なく、その担当者が対策導入を内部提案しても、会社（経営）側が動きださない場合も多かった。サイバー攻撃がより深刻化しつつあるなか、緊急性のある経営施策であることの認知・理解を高められるような情報提供を、経営者側にも強化していかなければならない。

対策２：知識・人材の不足をカバーする支援措置

中小企業のITネットワーク環境が多様かつ老朽化している実態が判明した。そのため、サイバーセキュリティ対策の導入段階から、現状のITネットワーク環境を正しく診断、中小企業の個別事情に即した施策や手順を的確に絞り込む必要があると考える。現状のリスクはどのくらいか、何をしなければならないのか、どのような運用になるのかまで、サイバーセキュリティ対策導入から運営管理までを伴走支援できる専門家（支援者）の配備が求められている。

対策３：コスト負担を軽減させる支援措置

UTM監視サービスが継続困難であるとの回答が多くあり、その主な理由は「価格が高すぎる」であった。サイバーセキュリティ対策の必要性は十分に理解・評価できても、費用が払えないという中小企業側の経営事情の反映である。これら中小企業の声に応えるべく、民間側でのサイバーセキュリティ製品・サービスにかかるコスト見直しを検討しているが、中小企業への共通基盤整備を目的として、政府側からの補助金など費用面での支援措置も必要と考える。

対策４：サイバーセキュリティ対策のアウトソーシング支援

中小企業側には知識・人材の不足という根本的問題があり、たとえ高度な製品・サービスを導入しても、運用段階で使いこなせない（課題が残る）ことが明確になった。その解決策としては、サイバーセキュリティ対策をアウトソーシングするという新しい観点での製品・サービスの再設計が必要であると考えている。初期のネットワーク調査から、セキュリティレベルのアセスメント、UTM端末でのモニタリング監視、もしもの場合の駆け付け支援までをパッケージにして提供するイメージである。ネットワークセンター側にサイバーセキュリティの専門家を配置すれば、リモート診断段階でインシデント原因を特定させ、初期対応で何が求められるのかを的確に判断することもできる。結果、駆け付け支援等で専門員を過剰派遣することが減少され、トータルコスト削減につながり、中小企業側にかかる費用負担を軽減できるようになる。

対策５：経営支援策としての体系化

サイバーセキュリティ対策（にかかる費用）が、中小企業経営にとっての必要な投資に考えられていないこと・優先順位が低いこと等が分かった。従来の情報セキュリティ対策（情報資産管理）のイメージが強く、自社被害に対する防衛策との考えに留まり、自社からの被害拡大で損害賠償にまで発展するかもしれないとの考えには至らなかった。「経験しないとわからない」「実感がわかない」というのが、中小企業のリアルな声である。今後、調達基準や取引先選定基準にサイバーセキュリティ要件が加味されていくかもしれないなど、中小企業経営支援の中で必須の取り組みとして体系化され、広く認知促進が図られるべきと考える。

3.3 地域側での連携体制、支援側の人材スキルについて

以下、本実証を通じて明らかになった地域側での連携体制、支援側の人材スキル等について考察・提言する

地域支援１：地域支援団体との連携による活動拡大

地域との交流機会（事業説明会、中間報告会、最終報告会）を通じて、サイバーセキュリティ対策に関する中小企業の意識が高められたと実感している。最初の事業説明会で興味を示さなかった脅威シナリオに対して、事業後半の説明会では（自分事として）具体的な対策をどうすればよいかの質問が来るようになったためである。しかしながら、地域には未だ多くの中小企業が存在しており、地域支援団体との連携で活動を拡大させ、サイバーセキュリティ対策の緊急性や必要性を広く訴求していかなければならないと考える。

地域支援２：もしもの場合に駆け込みできる地域相談窓口

中小企業が自立して、サイバーセキュリティ対策を進められない実態が判明した。ITネットワーク管理者がいない中小企業にとっては、サイバーセキュリティ対策を追加独自検討すること自体に無理があると考える。さらに対策具体化の段階では、人手不足などの諸事情、時間的都合や予算的都合等も考慮する必要があり、地域側で伴走支援できる体制が必要であり、商工会議所などへ相談窓口を設置するのが望ましいと考える。東京オリンピック・パラリンピックに向けて、サイバー攻撃による被害拡大の可能性が高まるため、早急な対応が求められている。

地域支援３：専門家によるリモート診断、ワンストップの仕組み化

実証を通じて、攻撃手段の巧妙さ（サイバー攻撃されていることの実感が全くない）、感染ウイルスの多様さ（簡単には特定できない）という実態が判明し、それらを特定するためには、高度なセキュリティ専門家によるリモート診断が必要になると感じた。各地にもれなく高度専門家を配置することは不可能であるため、ネットワークセンター側に配置、リモート診断を通じて各地対応するのが望ましいと考える。また、その専門家による判定結果に応じて、セキュリティ対策チームが派遣されるなどのワンストップ対応を仕組み化できれば、中小企業が期待する迅速な対応が実現できる。

地域支援４：ITベンダーとの連携、セキュリティ人材育成

中小企業のネットワーク管理の一端を、地域ITベンダーが担っている実態が判明した。中小企業側からITベンダーへ明示的にネットワーク管理を委託している状況ではないが、情報端末や業務システムを導入した際のITネットワーク環境を設定変更した痕跡が確認できており、サイバー攻撃を誘引する原因をつくっている可能性も否定できない。今後は、ITベンダー側の責任として、中小企業のIT導入の際には、サイバーセキュリティ対策検討までを含めて支援するのが理想である。その支援にあたるエンジニアには、ITネットワーク構築の知識に加えて、サイバーセキュリティ対策の知識を習得させるなどの教育徹底が図られるべきと考える。

3.4 保険連動プログラムの検討

以下、中小企業向け保険連動プログラム（サイバー保険の在り方）について考察・提言する。

保険検討１：追加コストに関する与件整理

保険設計をするために必要な中小企業側で発生する追加コストに関する情報が十分には得られておらず、今後も継続検討しなければならない。検討すべきコスト構造は４つ、①調査コスト、②対策コスト、③それ以外のコスト（損害賠償を除く）、④契約上で発生するグレーなコストである。実証企業に限らず、既存サービスのユーザーにも対象範囲を広げていくことができれば効果的である。なお、損害賠償発生時に必要となる支払限度額も含め、本実証事業で十分にニーズを拾い切れたとは言えない状況であり、引き続きの検証が必要と考える。

保険検討２：中小企業側の費用負担イメージ確立

サイバー攻撃の見える化ができた一方で、“攻撃に対する認識”“想定される影響”“発生時の必要なサポート”のいずれも“わからない”との意見が、回答の大多数を占めていた。中小企業では、未だサイバーセキュリティ対策検討がなされておらず、インシデント発生時の支援必要性要否についてイメージできずに状態である。結果、サイバー保険についての費用負担イメージが未だ確立されていないといえる。

保険検討３：最低限度と任意手配という2種類の保険設計

中小企業で発生しうるインシデント事案を確認できたが、事故の実態（事例の共有）、事故発生時の取引に与える影響、事故発生後の初期対応、選択肢となる任意保険の活用についての情報は未だ得られていない。最低限度の保証を国の制度等で守られるべきとする一方で、事業内容や取引関係性をふまえて、中小企業自らが必要とする補償額（追加購入をすべき任意手配保険）についても準備検討を進めるべきと考える。ただし上記2を踏まえると、現時点における中小企業の保険加入方法は、UTM全設置先が加入する“基本”領域に加え、その上乗せとして中小企業が個別に加入可否、および加入時の補償額を選択する“任意”領域の2層構造の検討が必要であることが、実証事業を通じて確認できたといえる。

保険検討４：製品・サービスへの商品付帯（団体保険の検討）

セキュリティの製品機能やサービス内容に応じて、インシデント発生のリスクが変動することが分かった、そのため、製品・サービスを介した商品付帯型の保険を立ち上げることで、中小企業のニーズを踏まえた補償内容、および保険料を柔軟に設計・検討をする事が可能となると考える。商品・サービスを提供する側の事業者が契約者となり、保険会社の提供するサイバー保険を付帯する仕組みである。

保険検討５：サプライチェーンでの保険設計

重要産業のサプライチェーンにおいて、中小企業側のサイバーセキュリティ対策が問題視され始めたことが分かった。今後、中小企業側において、大企業からの契約要求で明確に定義されていないような所謂“グレー”な自己負担発生することも予想できるため、それら想定しうる各種コストについて、可能な範囲で保険への転嫁を図れるかについて検討する余地があると考える。

保険検討６：国による制度設計

中小企業におけるサイバーセキュリティ対策の独自対策が難しい状況であることが判明した。しかしながら中長期的には、中小企業競争力の強化および中小企業発リスクマネジメント浸透の観点から、中小企業の自力自走を目指した仕組み化が必要である。検討に時間はかかったとしても、国に因る制度設計は必要であると考える。

3.5 中小企業向けサイバーセキュリティ製品・サービスの在りかた

以下、中小企業向けサイバーセキュリティ製品・サービスの在りかたについて考察・提言する。

製品・サービス検討１：コスト構造に関する与件整理

中小企業から低価格化への要請が強いことが判明したが、それらのコスト構造を最適化するための情報が未だ十分に得られておらず、具体的な価格設計は次年度以降の課題として残った。問題は、中小企業側の費用感が定まっていないことである。富士ゼロックスの製品・サービスは初期設置費用（6万円）および月額サービス費用（1万2800円）等の価格設定をしているが、いくらまでなら負担可能なのかの質問に対して、正確に回答できない中小企業がほとんどであった。

製品・サービス検討２：ネットワーク監視、リスク分析サービス：

ネットワーク監視やリスク分析には、中小企業からの期待が大きいことが分かった。これまでは、個別での価格設定をしてこなかったが、これからの製品・サービス設計での中心的機能になると思われ、期待されている品質に応じた価格化をしていきたい。現状の主なコストは人件費であるため、ビッグデータ＆人工知能（AI）の処理へ代替させること等で、低価格化が図れる可能性がある。

製品・サービス検討３：駆け付けサービス

駆け付けサービスについても、中小企業からの期待が大きいことが分かった。中小企業側の経営者および担当者共に、サイバー攻撃による重大リスクを自ら感知することができないこと、インシデント発生に対しても、どのように対処したらよいかわからないこと等の実態があり、今後さらに駆け付け支援のニーズが高まると考える。駆け付け支援を実施する場合、移動費・人件費

がかかるため、事前にリモート診断で原因を特定しておくなど、システム面での仕組み整備も重要になると考える。

製品・サービス検討３：システム復旧サービス

中小企業のITネットワークが多様であること、必ずしも管理された状態でないことが判明しており、事後支援でのシステム復旧費用等について定額サービスの対応は難しいと感じた。駆け付け支援と連動させた追加費用の随時見積もり、あるいはサイバー保険でカバーする保証範囲を広げる等の対応が必要になる。

製品・サービス検討４：製品・サービス体系の最適化

今後のサイバーセキュリティ製品・サービス体系として、3つの方向性を見出した。価格重視で“どこまで低価格にできるのか”、高度化するサイバー攻撃への対策を考えたサービス品質重視で“いかに防御するのか、リスクを減らすのか”、損害賠償や復旧費をベースに考える“もしもの備え、いかに対策するのか”である。中小企業にとっては、これら3つからなる商品・サービスを、それぞれの経営事情や業務プロセス、取引関係先からの要望、さらにはリスクの起こりやすさに合わせて、組み合わせ設計できるのが望ましいと考える。

最後に、上記3つの方向性を統合した製品・サービス化のモデルとして、下図3.5-1の示したマネージドセキュリティを検討すべきと考える。サイバーセキュリティ対策の運用管理アウトソーシング（事前対応から事後対応まで）と、ツール導入・環境整備、サイバー保険とを組み合わせ、全体をマネージドセキュリティとして統合させることで、中小企業側の多様な要請に応えることができる。社会や取引先から求められる中小企業のサイバーセキュリティ対策のレベルを担保しつつ、個別の経営状況に応じた機能の最適化（費用の最小化）と、経営者や社員にかかる負荷の最小化が期待できる。

なお、より多くの中小企業へ広げていくためには、ツール導入・環境整備の共通化や標準化、専門家が活躍するアウトソーシング領域の拡大、サイバー保険の普及拡大を目指す必要があると考える。社会インフラ側では、ログデータ共有、認証・認定基盤などのセキュリティ共通基盤整備されることが望ましいと考える。

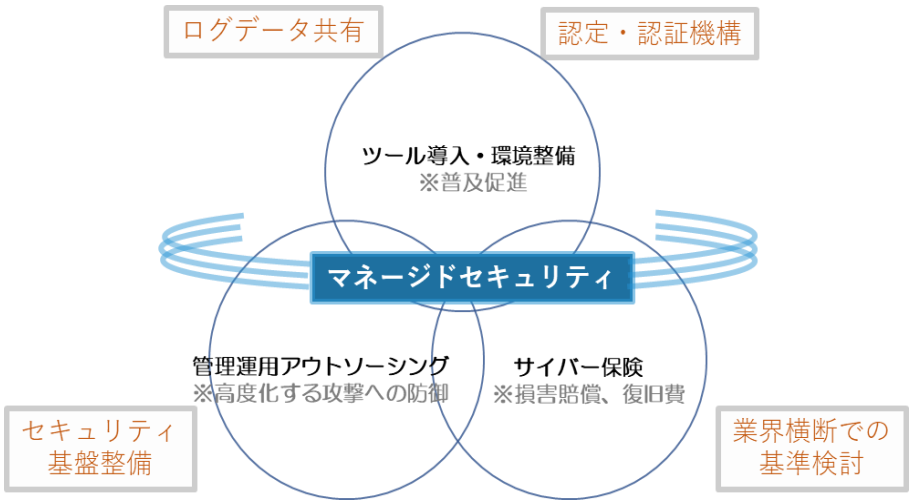


図 3.5- 1　サイバーセキュリティ対策の製品・サービスの在りかた

まとめ

本年度の事業活動を通じて、サイバー攻撃が既に中小企業へ拡がっていること、実被害につながる重大リスクが発生していることを確認できた。そして、中小企業側での（サイバー攻撃への）危機感は高まっている一方で、人手や知識の不足のために具体的な対策実施が進まないという困難さも明確になった。金銭的負担を懸念する声も多くあり、必要最低限となる製品・サービスへの再設計が求められるが、リスク検知やインシデント対応を重視する意見も多くあり、それら費用をいかにカバーするのかは、さらなる課題として残った。さらに、もしもの備えとなる保険適用については、多くの中小企業が“必要である”と肯定的であったが、保険商品設計に必要となる保証範囲等の詳細検討が足りておらず、さらなる情報収集が必要であることが分かった。

以下、本事業での活動内容を総括する。

本事業は、経済産業省・IPAが主導する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）であり、富士ゼロックスは請負事業として、北関東エリアの5県（茨城県、栃木県、群馬県、長野県、埼玉県　※埼玉県は9月度に追加）にて、8か月間（2019年6月～2020年1月）の活動を行った。

事業前半では、各県下関係者への協力依頼（訪問回数、のべ60回以上）、中小企業への事業説明会（11回開催、124社参加）、実証企業の募集を実施した。実証企業数101社（12月末時点）となり、当初目標100社を達成することができた。

事業中間では、それら実証企業へUTM端末を設置して、通信ログ記録するとともに、24時間365日でのリモート監視を実施した。危険性あるサイバー攻撃を感知した場合には、UTM端末にて通信を遮断するとともに、必要に応じて実証企業への通知を実施した。それら実証企業には、緊急の対策実施を促すとともに、必要に応じて駆け付け支援、原因特定、復旧支援、再発防止などの措置を行った。

その後、UTM端末から通信ログデータを回収して、データアナリストによる集計・分析・評価を実施。実証企業ごとのサイバー攻撃の実態を可視化するとともに、リスク度（攻撃されやすさ）についての診断を実施して、その結果を実証企業へフィードバックした。

事業後半では、通信ログ分析・評価の結果について、各県下にて中間報告会（5回開催、26社参加）、最終報告会（9回開催、46社参加）を開催した。さらに、本事業で協業いただいた関係者と協議して、中小企業が注意すべきサイバー攻撃についての脅威シナリオを立案し、中小企業むけのサイバーセキュリティ製品・サービスの在りかた、およびサイバー保険の必要性についての検討を行った。

以下、検討結果について総括する。

中小企業でのサイバーセキュリティ対策の遅れが、大きな問題になりつつある。実証企業では危険性の高い外部攻撃（標的型攻撃、ランサムウェア）が観測されており、自社被害だけでなく、関連会社への被害拡散にもなりかねない状況であった。他方、中小企業は、依然として危機意識が低く、サイバーセキュリティ対策は促進されづらい状況である。攻撃者に侵入されている段階でも、巧妙化している手口に気づく手段・知識が不足しており、長く放置されることで被害が深刻化してしまう可能性が高い。

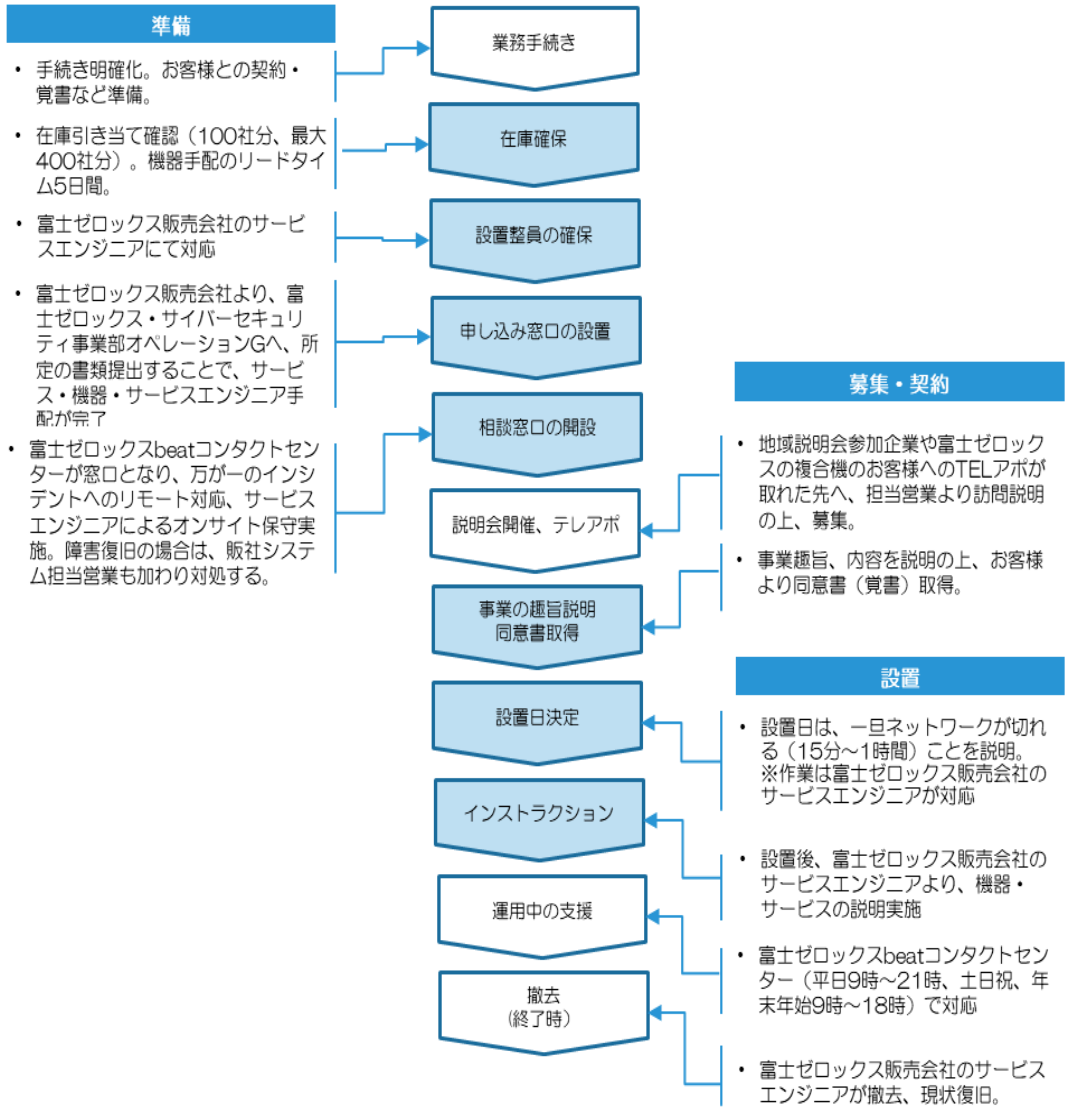
さらに中小企業では、内部要因（内部不正や意図しない操作）の危険性も高まっており、社内での管理統制の改善が求められる。理由は、最近のIT進化に伴って多様なWebサイト閲覧やクラウドアプリが業務利用されるようになったためであり、それらからのウイルス感染や情報漏えいが生じやすい状態にある。さらに、管理外のモバイル端末（個人PC、スマートフォン）の持ち込みが増えており、それらによる不正通信の増加や、それらが感染源となる社内外へのウイルス拡散が危惧される。

今後の対策推進では、人材や知識が足りていない中小企業に、サイバー攻撃のリスク検知やインシデント対応までを担わせることには無理がある。まずは各地域の商工会議所などに相談窓口を設けるのが良く、合わせて中小企業には通信ログ記録・防御ができるUTM等の導入、リモート監視でのリスク検知や専門家による診断や対策支援を整備していくのが良い。次に、中小企業側の費用負担を必要最低限にする検討が重要である。この点で、機能限定で画一的に低価格にするのではなく、事業形態や取引関係先の要請に応じたサイバーセキュリティのランク化が導入されるべきと考えている。それらランク値に応じた製品・サービス・保険を選択させることで、多様性ある中小企業を広くカバーできるようになる。

最後に、ウイルス感染や情報漏えいなどのサイバー攻撃による被害を永続的に抑止し続けることは不可能であり、それぞれのリスク度に応じた中小企業向けのサイバー保険は整備されるべきである。しかしながら現状は、中小企業で（保証範囲等の）明確な考えが整理できていないことから、まずは、サイバーセキュリティ対策を提供している製品・サービス側からのアプローチで、その保証範囲の拡張となる（商品付帯での）保険提供から着手するのが良いと考える。

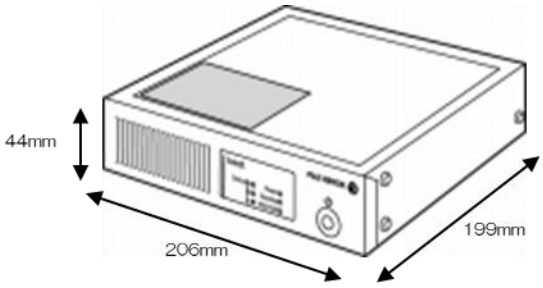
別紙：各種データ・資料

別紙１　契約手続き、UTM設置プロセスの流れ

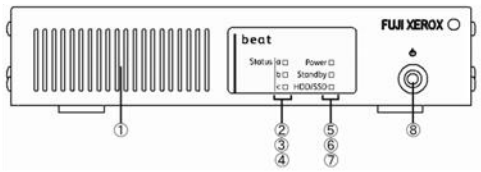


補図　1　UTM の契約手続きから、設置プロセス、撤去までの流れ

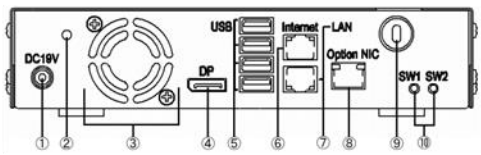
別紙２　UTM端末の外観、機能



■本体カラー：黒
■インターフェイス：10/100 BASE-TX / 1000 BASE-T × 3
■電源/電源アダプター：AC 100-240 V ±10 %、 50/60 Hz ±1 Hz
■消費電力：最大約70 W
■サイズ：W205 × D199 × H44 mm（ゴム足、クランプなど、突起を含みません）
■本体質量：約1.4 kg
■動作環境：温度5~35 ℃、湿度20~80 %（結露なきこと）
■基準適合：RoHS指令準拠、VCCI ClassB、高調波抑制対策 JIS C 61000-3-2 準拠



①給気口
②③④ステータスインジケーター
⑤電源インジケーター
⑥スタンバイインジケーター
⑦ハードディスクインジケーター
⑧電源スイッチ



①電源ジャック
②クランプ
③排気口
④ディスプレイポート
⑤USBポート
⑥イーサネットポート（Internet）
⑦イーサネットポート（LAN）
⑧イーサネットポート（Option）
⑨セキュリティースロット
⑩メンテナンス用スイッチ

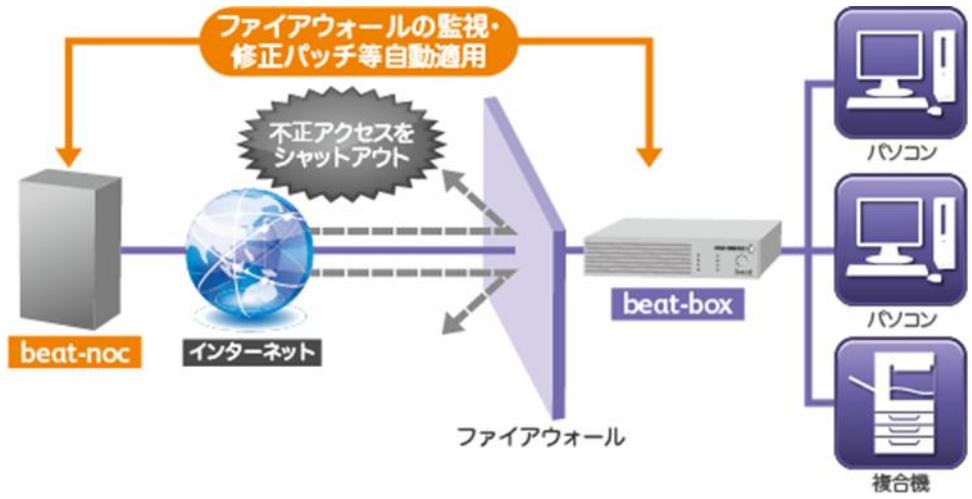
補図 2　セキュリティ機材：UTM 端末　（富士ゼロックス製　BEAT）

別紙３　UTM端末の仕様詳細

項目		内容
利用可能回線		FTTH、ADSL等のブロードバンド回線
アンチウイルス	有効/無効切替	無（有効のみ）
	対象	メール送受信（POP3、SMTP、サブミッションポート）、Web閲覧（HTTP、FTP） ※対象のプロトコルであってもポート番号や、ファイルの種類、容量によってはウイルススキャンの対象にならない場合があります。
	利用エンジン	Antiy Labs社製
不正な通信対策（IPS）	有効/無効切替	有（不正な通信対策の初期値は有効、対象の通信の初期値は有効、対象のアプリケーションの初期値は無効）
	対象の通信 ※対象の通信は変更になる場合があります。	DDoSサーバ/クライアント間の通信
		DoS攻撃・バッファオーバーフローを狙った攻撃
		バックドアによる通信・トロイの木馬による通信
		FTP、POP、SMTPなど様々なサービスの脆弱性を突く攻撃
		プロトコルアノマリ攻撃
	対象のアプリケーション ※対象のアプリケーションは変更になる場合があります	P2P ： Winny、eMule(eDonkey)、Cabosなど
		メッセンジャー ： ICQなど
		リモートアクセス ： VNC、pcAnywhereなど
	利用エンジン	株式会社MCセキュリティ製
迷惑メール判定	有効/無効切替	有（初期値は無効）
	主な機能	自動判定機能
		迷惑リストおよび許可リスト判定機能
		レポート表示機能
	利用エンジン	Cloudmark社製
ファイアウォール	有効/無効切替	無（有効のみ）
メールアドレスおよび利用者数		標準60　※オプションのbeat/active 利用者追加サービスにより10単位で440まで追加し、500まで登録可能。
利用者管理機能	主な機能	利用者、メールアドレスの追加・削除やパスワードの変更など
	利用者アカウント(メールアドレス)文字制限	最初の文字は英数字でなければなりません。全体の文字数は2文字～31文字でなければなりません。
		beatで始まるアカウント名、および下記のアカウント名は使用できません。 .htaccess、adm、admin、alias、apache、bin、daemon、dbus、default、ftp、games、gdm、gopher、haldaemon、halt、ident、lp、mail、mailer-daemon、mailnull、named、mqueue、news、ncsd、nfsnobody、nobody、ntp、operator、pcap、postgres、postmaster、qmaild、qmaill、qmailp、qmailq、qmailr、qmails、radvd、rcp、root、rpc、rpcuser、rpm、shutdown、smmsp、squid、sweep、sync、tomcat、tomcat4、tty、uucp、vcsa、vpasswd、vpasswd.cdb、wnn、www、xfs
接続クライアント数の上限		お客さまネットワーク設定に依存。推奨は最大250台程度。
レポート参照		現在のインターネット接続/過去の不正な通信・禁止アプリケーション検知回数/アンチウイルスの定義ファイルバージョン
表示機能		イーサネットポート情報
その他表示・設定機能		パケットフィルター設定/不正な通信対策設定/ネットワーク接続設定
週間稼働状況レポート		不正な通信対策/http・ftpウイルスチェック/メールウイルスチェック/迷惑メールチェック
プライバシーマーク・ログ機能		利用可能なログ一覧 利用者管理履歴、メール送信履歴、メール受信履歴、メール送信ウイルスチェック履歴、メール受信ウイルスチェック履歴、FTPアクセス履歴、beat-box責任者管理履歴、RAS接続履歴、Webアクセス履歴、HTTPウイルスチェック履歴、FTPウイルスチェック履歴、不正な通信対策履歴、パケットフィルター履歴、beat設定ページ、高度な設定のアクセス履歴、DHCP履歴、認証失敗履歴、外部からのアクセス履歴

補表 1　セキュリティ機材：UTM 端末（富士ゼロックス社製　BEAT）の機能詳細

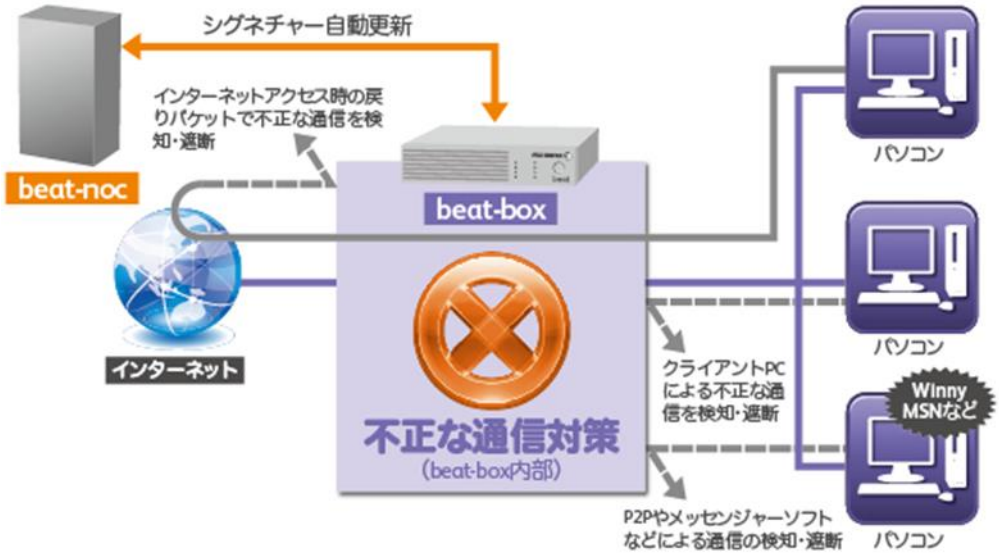
別紙４　UTM端末による監視機能



補図 ３　BEAT サービス：セキュリティ機能（１）

外部からの不正アクセス防止対策（ファイアウォール機能）

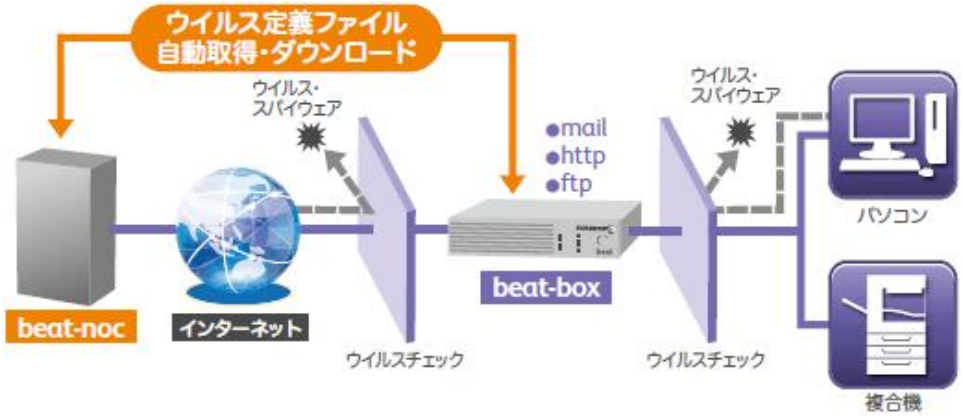
独自技術のファイアウォールが不正アクセスをシャットアウト。インターネット上から UTM 端末の存在を隠し、ハッカーによる攻撃の危険性を回避。ソフトウェアの脆弱性を補強する修正パッチの自動適用や、攻撃への対策が beat-noc 経由で随時実施されるので、管理者の負担も軽減されます。



補図 ４　BEAT サービス：セキュリティ機能（２）

不正な通信対策（IPS：不正侵入防止システム）

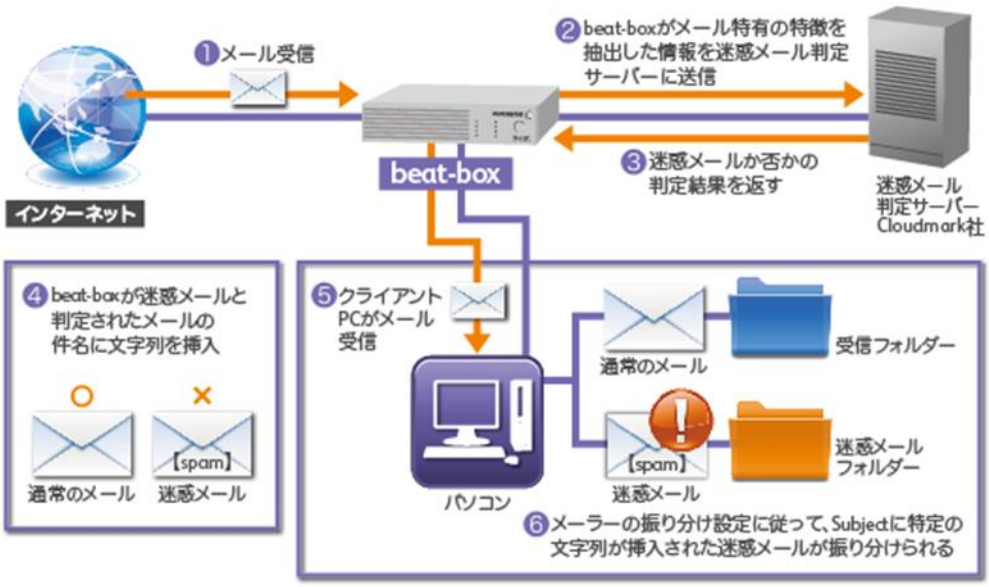
通過する通信パケットの内容や振る舞いを検査し、不正な通信を検知して遮断。さらに、違法性のない場合でも情報漏えいやウイルス感染などのリスクのあるアプリケーションの通信も遮断します。次々と発生する新たな脅威に対しては、beat-noc が新種の不正な通信やアプリケーションに対応するためのシグネチャーファイルを自動でダウンロードし最適な状態に保ちます。



補図 5　BEAT サービス：セキュリティ機能（3）

ウイルス・スパイウェア対策

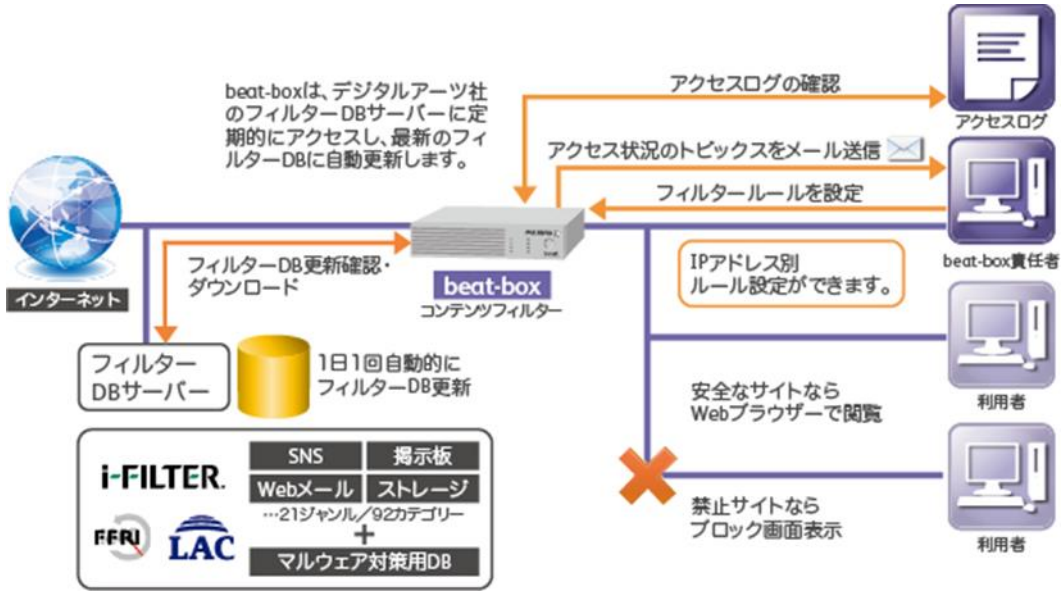
メールや Web アクセス時のウイルスやスパイウェアを、インターネットの出入り口で自動検出。最新のウイルス定義ファイルを beat-noc 経由にて 24 時間リモートで自動適用して、新種ウイルスにもスピーディーに対応します。



補図 6　BEAT サービス：セキュリティ機能（4）

迷惑メール対策

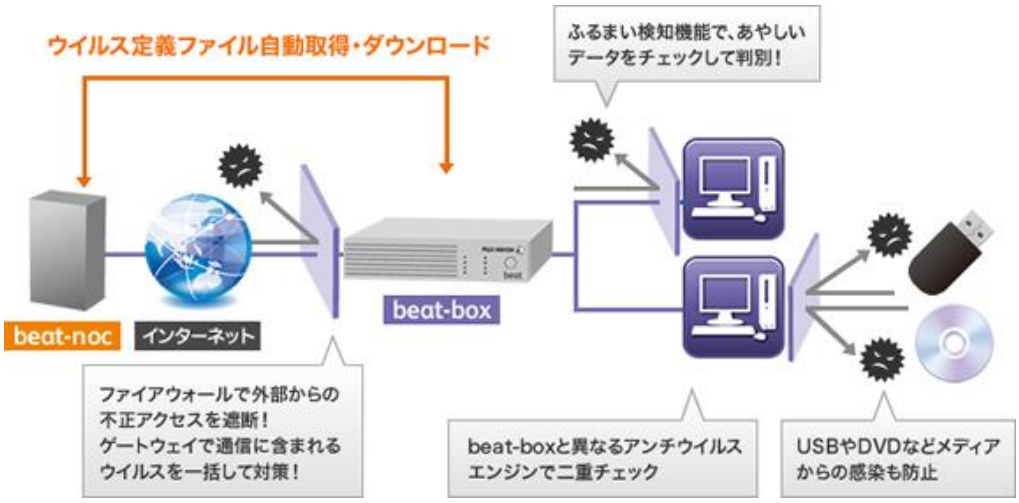
外部から受信する迷惑メールを自動判定。迷惑メールと判定された場合は、メールの件名に特定の文字列が追加されます。利用者は簡単に対処でき、メールチェック負担による業務効率の低下も防ぎます



補図 7　BEAT サービス：セキュリティ機能（5）

WEB フィルタリング対策

業務上不要な Web サイトへのアクセスを制限するサービスをオプションで提供します。情報漏えいのリスクを低減するとともに、私的利用から発生するタイムロスをなくして業務効率を向上します。



補図 8　BEAT サービス：セキュリティ機能（6）

PC ウイルス対策

クライアント PC 用アンチウイルスソフトを提供しています。各クライアント PC にアンチウイルスソフトをインストールすることでウイルス対策を二重化し、USB や DVD などのメディアからのウイルス侵入を防止することで、より強固なセキュリティ環境を実現します。

別紙５　エンドポイント管理サービスの内容

パソコンやネットワーク機器を一元管理
インストール済みソフトウェアやセキュリティ対策状況など、
複数のパソコンやネットワーク機器の情報を一元管理します。

私物USB/スマートフォンの利用制限
紛失や漏洩のリスクがある私物のUSB
デバイスの利用を制限。USBストレー
ジやポータブルデバイス、SDカードな
どの使用を禁止する。ホワイトリスト
の作成・登録も可能。

Windowsの自動更新制御
Windowsの自動更新の設定を「自動的
にインストールする」への変更・制御
が可能。これによりWindows等のアッ
プデート漏れを防ぐことができる。

アプリケーション制御
指定アプリケーションの起動を禁止す
ることが可能。これにより、P2Pソフ
トなどの情報漏洩のリスクがあるアプ
リケーションの起動を禁止でき、リス
クを低減できる。

補図　９　IT ネットワーク診断・管理サービスの内容