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：沖縄県）

成果報告書

請負事業者：沖電グローバルシステムズ株式会社

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

目次

1. サマリー

本報告書は、沖電グローバルシステムズ株式会社（以下「沖電グローバルシステムズ」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。

沖縄県内の中小企業 102 社を対象に、以下のサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- セキュリティ対策機器（UTM）
- クラウド WAF
- EISS（簡易 EDR）
- 簡易セキュリティ診断

2.　本実証事業の全体概要

近年サイバー攻撃の手法は進化しているとともに、その被害の対象が大企業ではなく中小企業にまで広がっている状況がある。

そのため、本実証事業ではサイバーセキュリティ対策支援サービスの提供を行うことで、地域の中小企業に対しサイバーセキュリティに関する意識向上を図るとともに、実施済み対策や意識、ニーズなどの実態を把握し、その地域特性・産業特性などを考慮したマーケティング方法や支援内容をスリム化しコスト低減した中小企業向けのサイバーセキュリティ対策支援サービスの検討を行うことを目的にした実証事業であり、当該実証などの成果を報告するものである。

2.1.　背景・目的

IoT 技術や AI 技術などの技術が注目を浴びているように近年ビジネスと ICT の結びつきが強くなってきているとともに中小企業のサイバー攻撃からの被害が顕在化してきている状況にある。その中でもサプライチェーン全体の中で対策が弱い中小企業を足掛かりに大企業などへの攻撃も増加してきており、中小企業自体のセキュリティ対策の強化は我が国の産業全体を守る上で非常に重要な課題となっている。

そのような中にありながら、多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うということすら想定していないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも多く発生している。

それらの原因としては、中小企業の持つサイバーセキュリティに対する情報やサイバーセキュリティ対策支援サービスに触れる機会の乏しさの他、中小企業のニーズにマッチした製品・サービスの乏しさなどが考えられる。

そのため、本実証事業では中小企業に対するサイバーセキュリティ対策支援サービスの試用やアンケート調査などを通し、サイバーセキュリティに対する意識向上及び中小企業のニーズにマッチしたサイバーセキュリティ対策の構築・定着を目的とする。

2.2.　実証地域の選定

本実証事業の地域実証は、「沖縄県」を選定して実施した。

2.2.1.　地域の選定理由及び妥当性

① 開業率が全国トップクラス

「中小企業白書」で公開されている 2017 年、2018 年度の都道府県別開廃業率の最新統計では沖縄県が開業率第 1 位で本実証事業のターゲット層である中小企業が多い地域である。

② 主要産業が観光業である

沖縄県は日本有数の観光地である。

観光業は元々個人情報の取り扱いが多く、過去に大手企業も複数の個人情報漏洩の　　インシデントを起こしている状況がある。

しかし、インシデント発生時の影響が大きい産業でありながらも、個人事業主や中小規模企業が多く、セキュリティ対策意識があったとしても実際に対策を講じるだけの体力が乏しい状況にある。

コロナウィルスの悪影響の大きい産業であるが、コロナウィルスの終息後に回復基調へ移った際のことを想定し、今のうちにセキュリティ対策の導入及び産業全体としてのセキュリティ対策意識の向上を図ることを目的とする。

③ 地理的特性

日本の最南端のエリアであり、国防を担うだけでなく、アジアの中心としての物流拠点になりつつある地域である。

また、島嶼地域である沖縄は本土と違い、社会インフラの他県との広域融通が難しいという特性があり、全て自前で調達をしなければいけないという状況がある。

そうした観点で、安定的な供給を目的取引先のセキュリティ対策及び意識をより向上させたい、という目的から沖縄電力グループには実証参加企業の募集に関する協力も得て、実証を推進した。

3. 事業概要

本実証事業では、中小企業に対する IT ベンダーによるサイバーセキュリティ対策支援サービス提供と専門的なアドバイスなどを実施する支援体制を構築し、同時にアンケート調査やヒアリングを実施し、中小企業のサイバーセキュリティ対策の実態を把握し、実態に即したサービス内容や支援体制などを明らかにすることにより中小企業が活用しやすいサイバーセキュリティサービスの創出を目指した検討を行う。

3.1. 全体像

5 つの仕掛け（4 種類のセキュリティ対策支援サービスの提供+アンケート）で中小企業の実態把握を進めた。

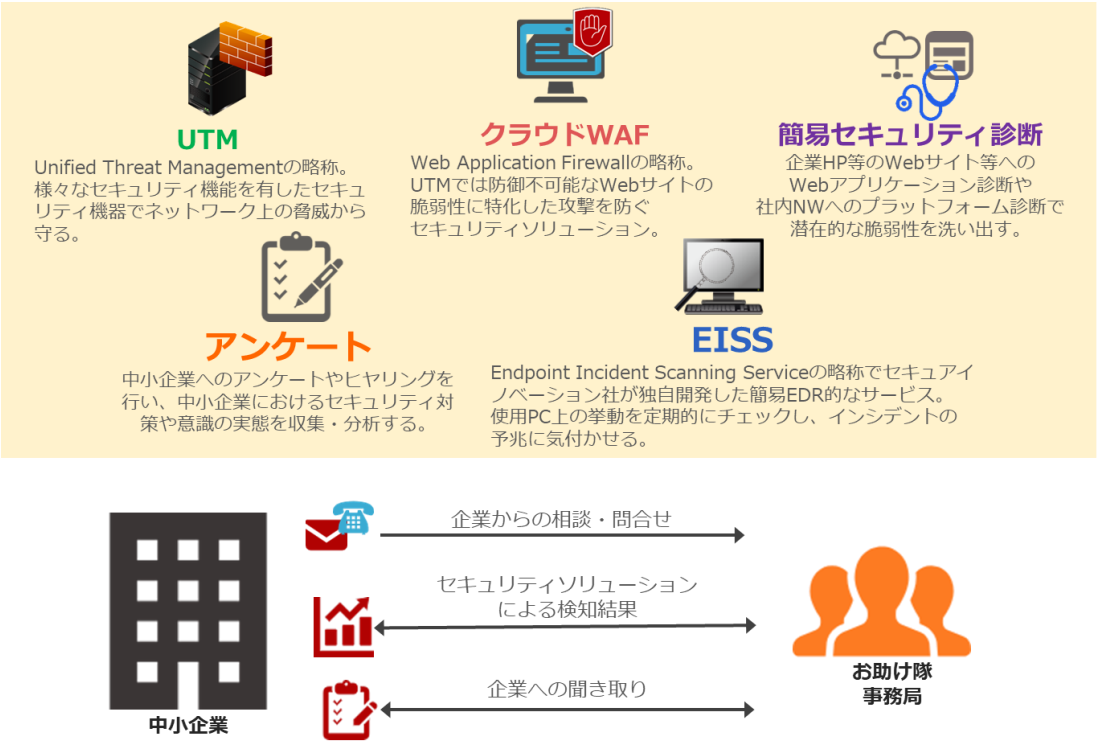
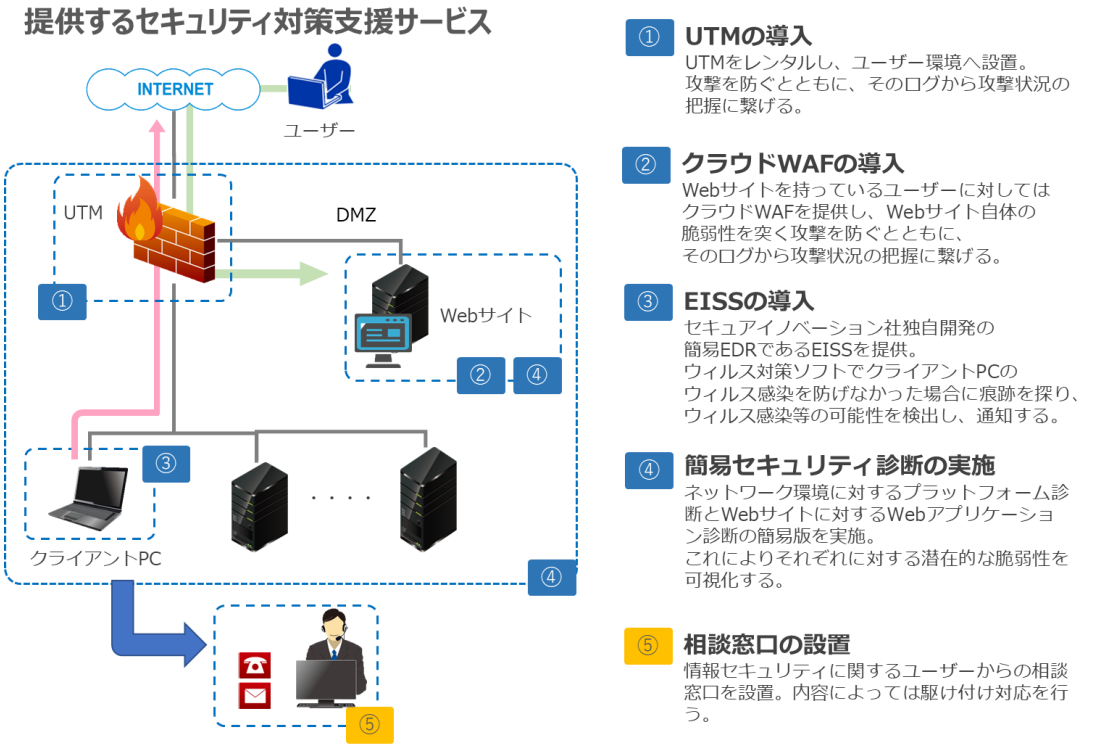


図 1：5 つの仕掛けによる実態把握

多層防御を図ることが可能なように各分野のサービスを用意するが、全てのサービスを提供するのではなく、サービス個別での申込みを受け付けることとし、実証参加企業ごとに必要なサービスを提供した。



【イメージ】参加事業社の状況に応じた提供内容

	AVソフト導入済み	Webサイト所有	UTM導入済み	UTM	クラウドWAF	EISS	簡易診断	アンケート
A社	○	○	○	×	○	○	○	○
B社	○	○	×	○	○	○	○	○
C社	○	×	×	○	×	○	○	○
D社	×	×	×	○	×	○	×	○

図 2：提供するセキュリティ対策支援サービス

アラート通知や実証参加企業からの相談・問合せをインシデントのトリガーとし、ヘルプデスクで段階的に原因を切り分けて各チームへ対応を指示し、事象によっては必要に応じて現地への駆け付け支援をする体制を構築した。

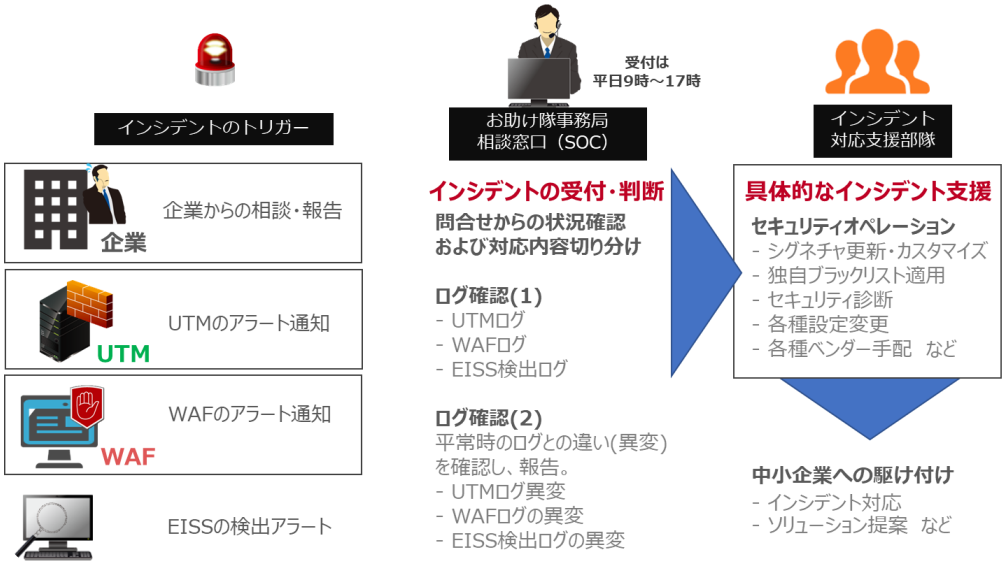


図 3：サイバーセキュリティ事後対応支援体制

3.2.　提供サービス

3.2.1.　UTM

設置機器

実証参加企業に設置する UTM はウォッチガード・テクノロジー・ジャパン株式会社の「Firebox シリーズ」を使用した。

機器の型番は固定せずに実証参加企業へのヒアリング結果から規模に応じた機器を選択して提供。ライセンスに関しては原則的に「Basic Security ライセンス」としたが、一部の企業に関しては検証のために「Total Security ライセンス」を適用し提供した。

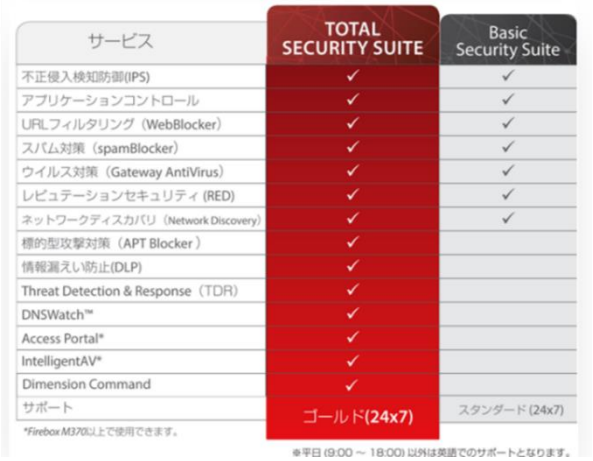


図 4：使用する UTM とそのライセンス

有効にしたセキュリティ機能

機能名	機能概要
不正侵入検知・防御（IPS）	継続的に更新されるシグネチャを使用して、主要プロトコルのトラフィックをスキャンしスパイウェア、SQL インジェクション、クロスサイトスクリプティング、及びバッファオーバーフローなどのネットワーク脅威に対するリアルタイムの保護。
レピュテーションセキュリティ（RED）	複数の脅威フィードからデータを収集し、不正なサイトやボットネットに対するリアルタイム保護機能を提供するとともに、セキュリティインスペクションによる Web アクセスのオーバーヘッドを大幅に軽減する、強力なクラウドベースの Web レピュテーションサービス。
スパムメール対策（Spam）	スパムメール及びフィッシングメールをリアルタイムかつ連続的に検知し、保護。WatchGuard SpamBlocker は、高速かつ効率的に検査を行い、1 日に最大 40 億件のメッセージを検査するとともに、メッセージの言語、形式、内容に関わらず効果的な保護を提供。
ゲートウェイウィルス対策（GAV）	継続的に更新されるシグネチャを活用して、既知のスパイウェア、マルウェア、トロイの木馬、ワーム、ローグウェア、マルウェアの亜種も含め、複合型の脅威を識別しブロック。 ヒューリスティック分析エンジンによる疑わしいデータ構造や 行動を追跡することで、未知のウィルスの侵入もブロック。
APT Blocker ※一部の企業のみ	次世代型サンドボックスを使用して、ランサムウェア、ゼロデイ脅威、更に新たな回避型の高度なマルウェアなどの高度な攻撃を的確に検知し阻止。
IntelligentAV ※一部の企業のみ	マシンラーニングエンジンを活用し、進化し続けるゼロデイ マルウェアをより確実に防御。脅威が拡散される数か月前に脅威を予測し、強力なプロアクティブな保護が可能。

表 1：使用した UTM のセキュリティ機能

UTM の設置

事前にメール電話などで状況をヒアリングした後に、手戻りによる時間のロスを避けるためにエンジニアが機器を持参して設置を行った。

今回、離島地域である石垣市、宮古島市へも往訪し、設置を行うケースもあった。

設定モード

実証参加企業の既存のネットワーク環境を変更せずに済むようトランスペアレントモードで設置をした。

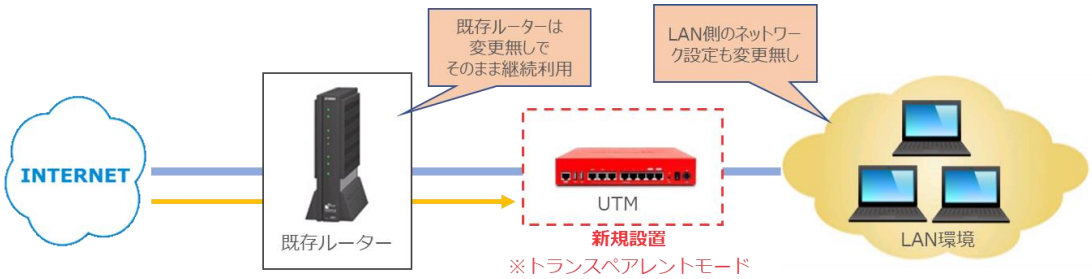


図 5：UTM の設定モード

▼メリット

・既存ルーターの設定を UTM に移植することなく設置が可能なため、設定が容易。

・UTM 故障時に一時的に機器を取り外すことでインターネット接続の復旧可能。

その他、設定変更や監視に関してはリモート接続により実施する形を取った。

攻撃検知時のアラート

実証参加企業の運用負担の軽減を考慮し、UTM で攻撃を検知した際は実証参加企業へ直接アラート通知をするのではなく、一度 SOC 側にてアラートを受けて検知内容を精査し、対応が必要な場合にのみ通知をする形を取った。

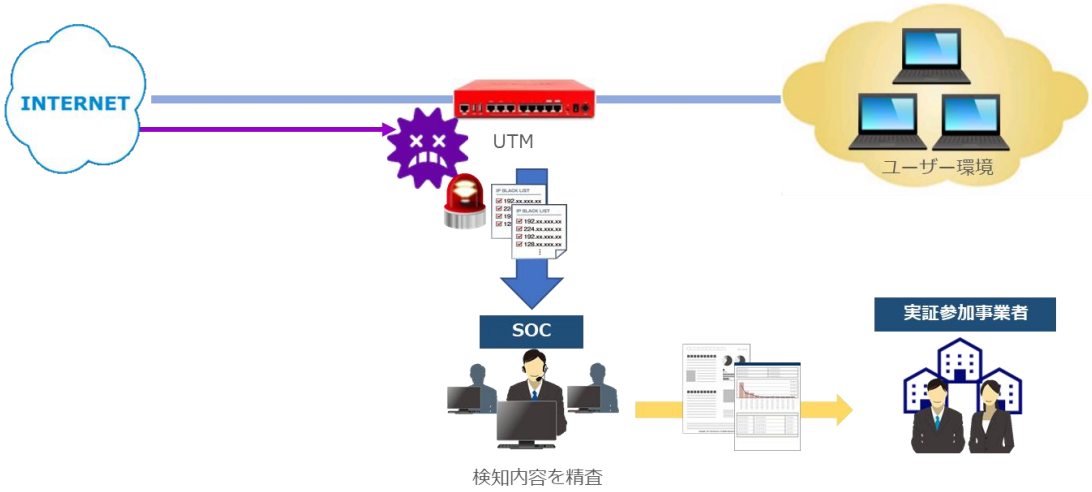


図 6：アラート検知時フロー

3.2.2.　クラウド WAF

提供サービス

実証参加企業へは株式会社セキュアイノベーションのクラウド WAF サービスである「secuWAF」を提供。実証参加企業へは検出ログの閲覧機能などを有した管理画面を付与した。

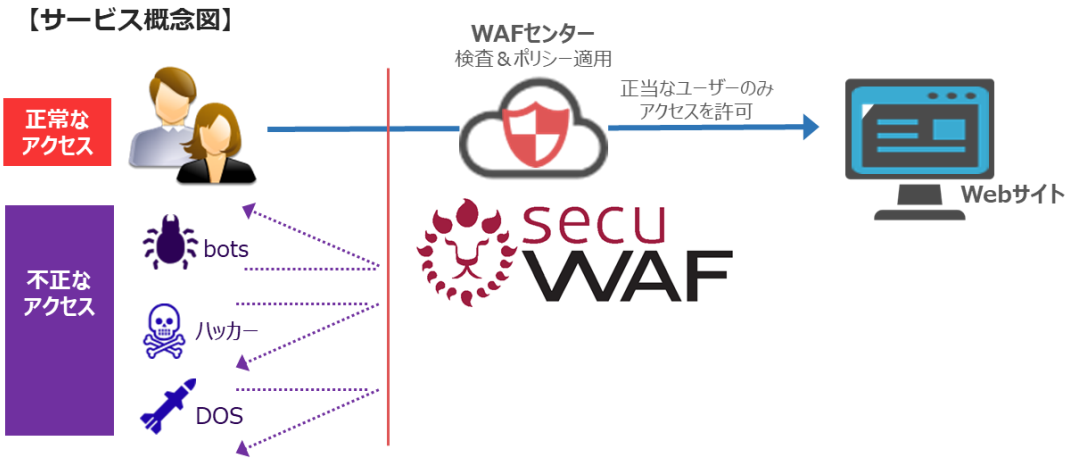


図 8：クラウド WAF（secuWAF）のサービス概念図

図 9：クラウド WAF（secuWAF）のユーザー管理画面

導入方法

ユーザー環境に対しての設定変更は不要で、保護対象となる Web サイトドメインの DNS 設定変更のみで適用が可能で比較的簡易な導入手法である。

3.2.3. EISS

EISS の製品概要

実証参加企業に対しては、株式会社セキュアイノベーションの「EISS（Endpoint Incident Scanning Service の略称で株式会社セキュアイノベーション社の造語。）」を提供した。

EISS は、エンドポイント（Windows パソコン）における操作や生成ファイルなどのログ情報を記録・保持し、マルウェア感染後に発生する活動かどうかを定期的に分析し、情報漏洩などの被害に繋がる可能性に気付かせ、早期の事後対処アクションに繋げるもので、予防のためのウィルス対策ソフトとは異なり、感染後の事後対処に効果のある簡易 EDR 製品である。

そのため、導入済みのウィルス対策ソフトと干渉することなく導入が可能であり、併用することで効果的な製品である。

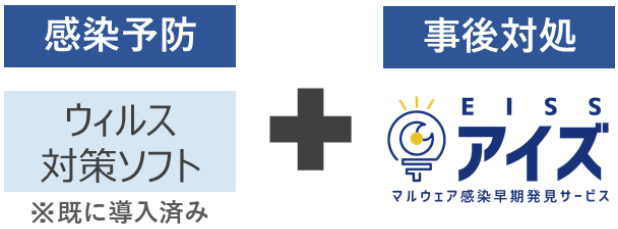


図 10：既存 AV ソフトとの併用

EISS の導入方法

エージェントをインストールすることで導入が可能だが、そのエージェントのダウンロードサイトからのダウンロードもしくは、SOC からのファイル送付にて配布する。

エージェント自体はサイレントインストールにて実行されるため、導入の手間はわずかである。

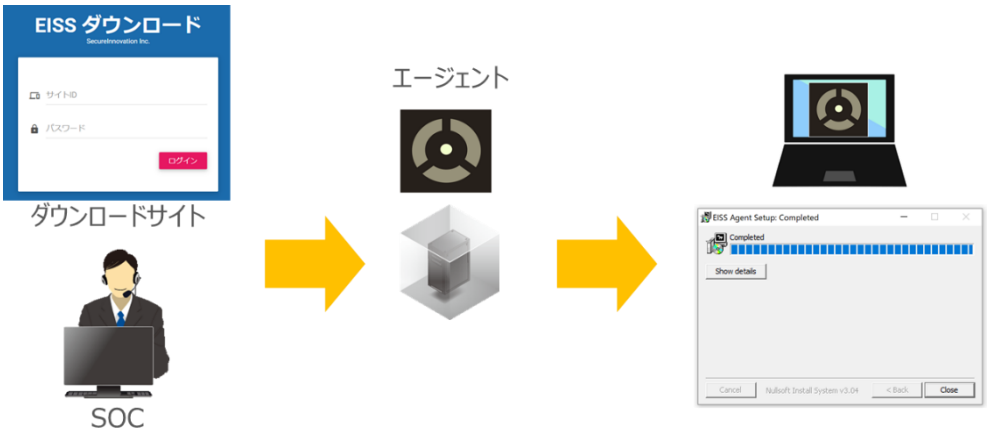


図 11：エージェントの配布とインストール

処理・運用のイメージ

エンドポイント（Windows パソコン）から必要な情報（以下、「ログなど」と呼ぶ）を定期収集し、クラウド上の分析基盤でログなどを分析し、同時にそのログなどは一定期間保管される。

ログなどの分析はマルウェアそのものではなく、マルウェアの挙動自体に着目し、分析を行い、SANS や JPCERT/CC などの公的機関が危険な兆候だと示すものなどを検知する。

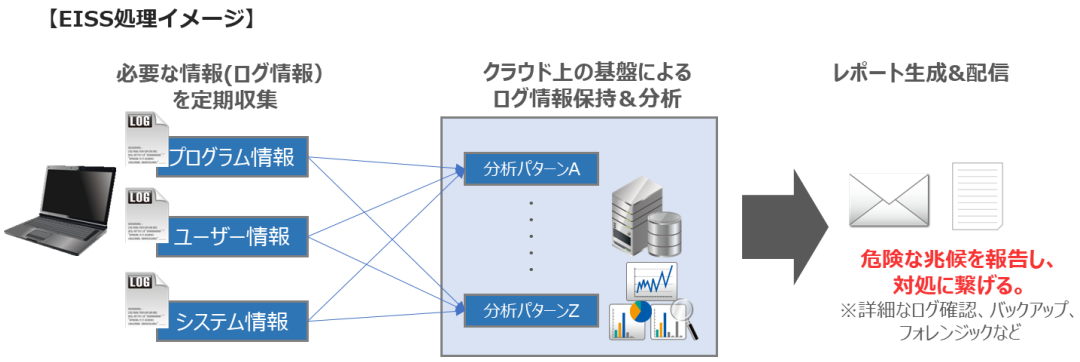


図 12：EISS の処理イメージ

3.2.4. 簡易セキュリティ診断

簡易セキュリティ診断の概要

自社の潜在的なセキュリティリスクを把握させ、セキュリティ対策を具体的に検討するきっかけを与えることを目的に簡易診断を実施した。

自社のホームページやサービスサイトなどの作り自体に脆弱性がないかをチェックする Web アプリケーション診断と、利用中のサーバーやネットワーク機器などの設定や利用状況に脆弱性がないかをチェックするプラットフォーム診断の 2 種類の診断を用意した。

いずれも対象を制限した簡易的なものであるが、診断ツールとセキュリティエンジニアによる手動での診断を併用した形で診断を実施した。

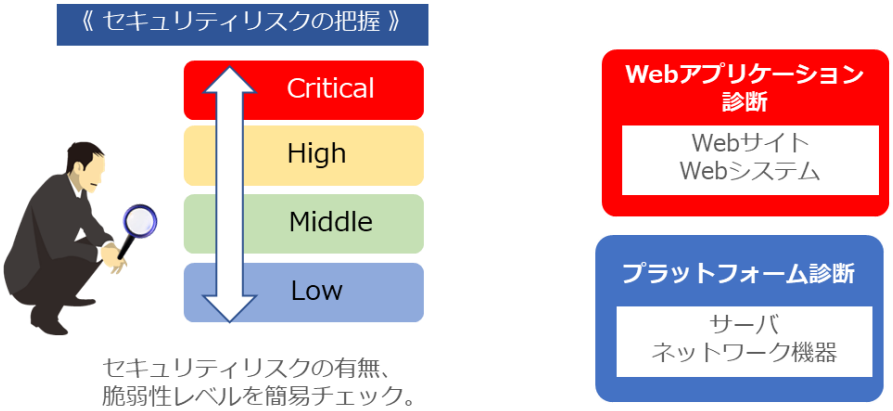


図 13：セキュリティ診断の意義と種類

診断手法

外部からの攻撃を想定し、リモート接続による診断を実施。

実際の攻撃者の手法と同様の攻撃手法で疑似アタックを行い、脆弱性の有無とその危険性を診断した。

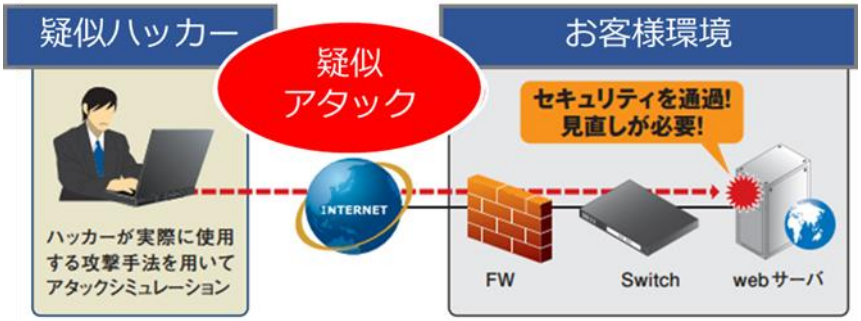


図 14：セキュリティ診断のサービス概念図

診断結果

診断完了後には診断結果報告書を提示。

診断結果報告書には脆弱性の有無や危険度レベルだけではなく、修正方法のヒントまでも含め、その報告書への質疑対応も行った。

※具体的な修正対応自体は本実証事業の対応の中には含めず、質疑対応に留めた。

3.2.5. ヘルプデスク

開設内容

実証参加企業からの相談を適切な対処に繋げるためのヘルプデスク機能として事務局の他にコールセンターも設けた。

応対手法としては専用電話ダイヤルの他、メールアドレスを設け、相談窓口の電話応対の開設時間は、本実証事業の実証参加企業である一般的な中小企業の営業時間帯や今後の中小企業向けサービスとして検討していくことを考慮して、土日祝日を除く、平日午前 9 時から午後 5 時までとした。

3.3. スケジュール

下記の全体スケジュールで本実証事業を実施した。

	9月	10月	11月	12月	1月
募集告知					
個別事業者訪問					
ラジオCM					
事業説明会の開催					
事業説明会（会場開催）					
事業説明会（ウェビナー開催）					
成果報告会					
中小企業の実態把握					
セキュリティサービス提供					
1.UTM					
2.WAF					
3.EISS					
4.簡易セキュリティ診断					
5.セキュリティ相談支援窓口					
インシデント対応支援					
アンケート/ヒアリングによる実態把握					
簡易サイバー保険のあり方の検討					
中小企業向けセキュリティ対策サービスの検討					
成果報告書の作成					

表 2：全体スケジュール

3.4. 実施体制

実証エリアである沖縄県内で活動をする組織で共同事業運営体を整備し、また、告知には沖縄県内の各公的機関の協力も得て、地域一丸の体制で実施した。

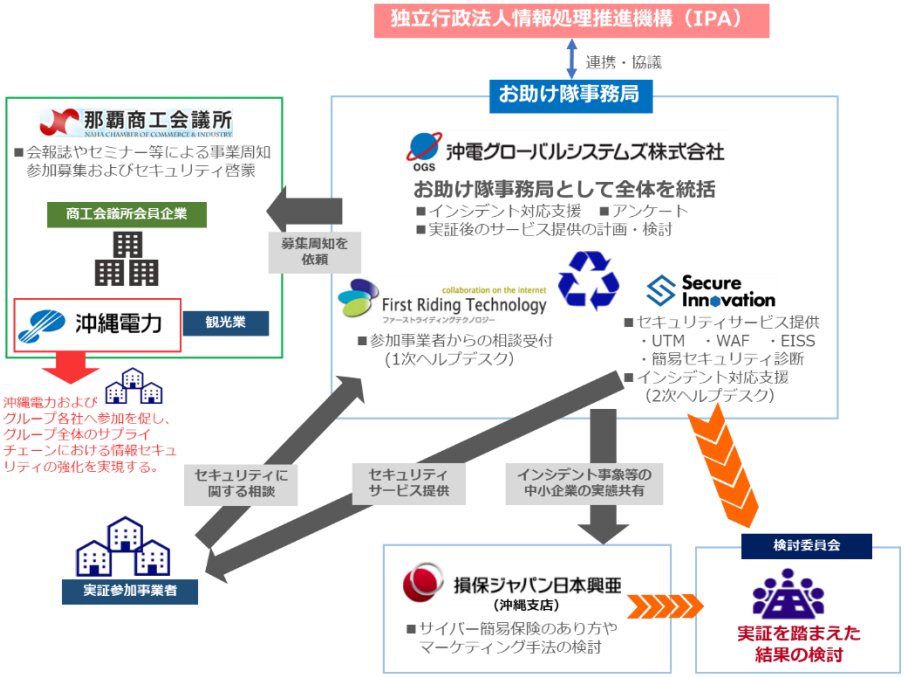


図 15：実施体制の全体スキーム

3.5.　実証参加企業数

実証参加申込企業数は 116 社で、そのうち実際にサービス提供を行ったユニークな提供社数は 102 社であった。

提供サービス	申込 総件数	申込件数	未提供・提供 不可件数	提供済み 件数
UTM	116 社	29 社	14 社	15 社
クラウド WAF		30 社	22 社	8 社
EISS		84 社	16 社	68 社
簡易セキュリティ診断		60 社	13 社	47 社

※　企業ごとに申込んだサービスが異なるため、提供済み件数は延べ件数となっており、ユニーク提供社数と異なるものになっている。

表 3：実証参加企業数とサービス提供済み件数

▼実証参加企業の属性

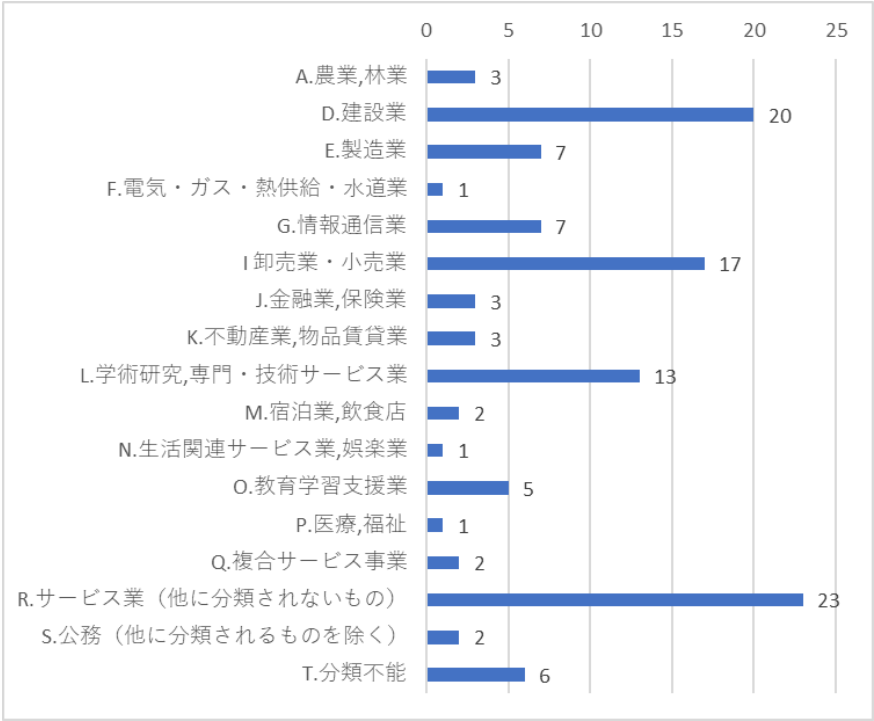


図 16：実証参加企業の属性（業種）

考察：当初は沖縄地域の主要産業である観光業の企業をメインターゲットの 1 つと想定していたが、コロナウィルスの影響が直撃し、実証への参加どころではない状態になり、乏しい結果となった。

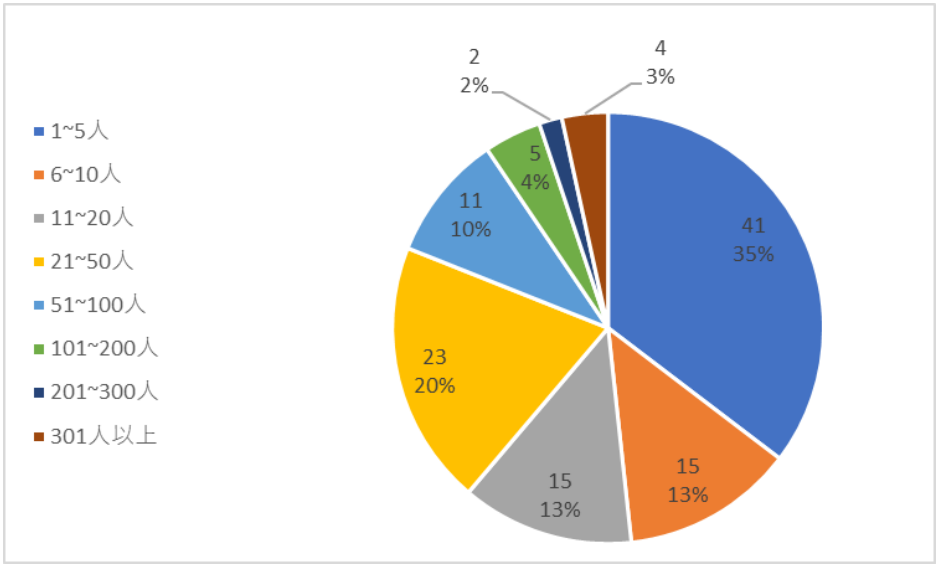


図 17：実証参加企業の属性（従業員数）

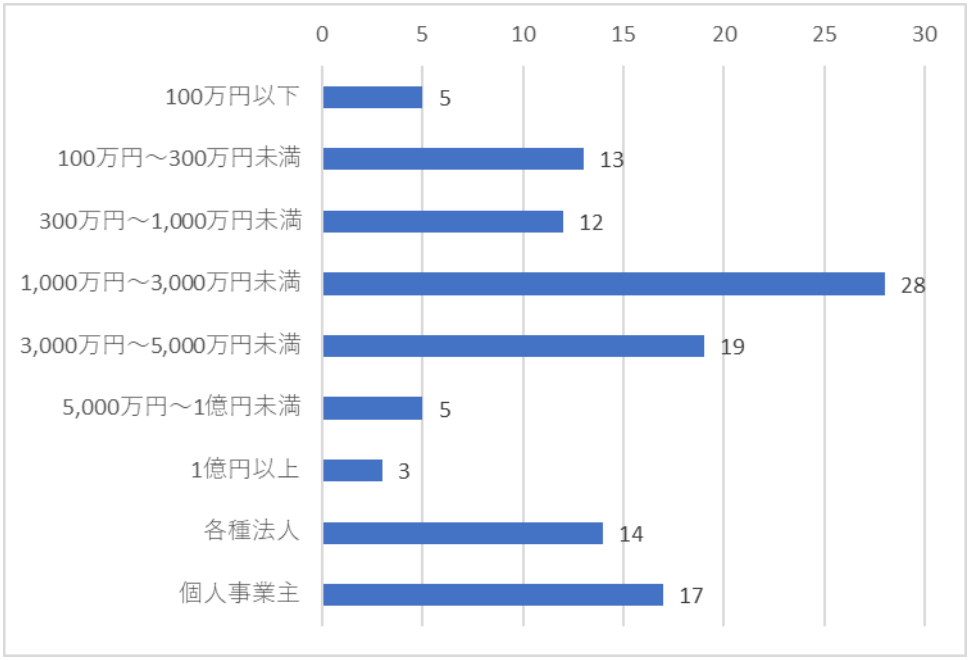


図 18：実証参加企業の属性（資本金額）

申込済みでありがらも未提供となった企業に関してはそれぞれ以下のような理由が挙げられる。

▼未提供・提供不可の理由

■UTM

・ 現地調査をした際になって初めて既設の UTM 機器の存在が判明した。
・ 導入作業時のテストでは問題はなかったが、導入後になってインターネットが繋がらないという事象が発生。
① 現地での調査の結果、上位 NW 機器の設定との干渉が怪しまれたが、当該上位 NW 機器の保守ベンダーの協力を得られず調査を断念し、結局設置済みの UTM 機器を取り外した。
② 同じ部署の端末でもインターネットが使える端末と使えない端末がある、という状況であると聞き、端末依存の可能性が考えられたため、現地調査を打診したが、業務影響の解消を最優先するという判断のもと、UTM 機器の即時取り外しを指示された。

■クラウド WAF

・ 申込み後のヒアリング及び調査の結果、レンタルサーバーや CMS サービス等、　現在の利用サービスの中で WAF 機能を有していて既に利用済みであった。利用可能な状態でありながらも未使用の場合は、有効化することを案内した。
・ 導入時に、DNS 設定の設定追加やネームサーバーの変更、サブドメインの追加等、ユーザー側での実施が必要な作業があるが、以下のような理由でこれらの対応を実施してもらえない。
① 必要な設定情報を伝えても実施してもらえない。
② 設定ミスで不具合が発生し、影響の大きさから切戻しをして未設定状態。
③ ネームサーバーの変更も必要なケースでは、変更による運用上の手間・影響を考慮し、導入を取りやめるという判断になった。
④ サブドメインサイトの新規構築やリダイレクト設定が必要なケースでは、運用会社の協力が得られない事象や、運用上の影響から経営判断として導入を取りやめた。

■EISS

・ パソコンへインストールしてもらう必要のある EISS エージェントを提供してもインストールを実行してもらえない。
・ インストールが上手くいかない事象が発生した場合に事象解消のための情報提供を依頼しても、その情報提供の返答がなされない。
・ EISS が動作保証しているのが Windows OS のみとなっており、実証参加企業のパソコンが動作保証対象外の Mac OS であった。

■簡易セキュリティ診断

・ 診断対象環境の保守管理会社（担当）から診断作業の許諾を得られない。
・ ログインアカウント情報など、診断に必要な情報提供を依頼しても情報提供がなされない。
・ Web サイトを新規構築後に診断をする予定だったが、構築自体の進捗が悪く、実証期間内での実施が難しい。（コロナウィルスの影響による作業遅れや作業自体の保留が原因）

その他、実証へ参加しない企業へヒアリングをしたところ、以下のような意見があった。

▼参加しない理由に関するコメント

・ 実証期間が十分な長さではなく、導入時の手間と比べて効果があるのか疑問。
・ 社内を通す上手い理由が考えられず、上長（社長）への決裁を通せない。
・ 保守をお願いしている会社（担当）が参加不要だと言っている。
・ 実証終了後に有償になった際に、その予算を捻出する企業体力がない。
・ 本実証事業の対応をするのに社内人員の手が回らない。
・ 自社の企業規模では現状の対策で十分だと感じているため。
・ 取引先からセキュリティ対策の要請がない状況であるため必要性を感じていない。
・ 自社と同規模・同業他社での被害を聞いていないので必要性を感じない。
・ 変化があった際の拒絶反応がとても大きい組織であり、新たなものを導入した際の業務への影響が心配なため。

4.　実証参加企業の募集

実証参加企業募集のための以下のアプローチを行った。

4.1.　事業説明会

事業説明会としては 8 回を実施した。

会場開催の説明会に関しては、沖縄本島内でも南部と中部に分け、更に離島エリアもカバーする目的で離島の中でも規模の大きい石垣市と宮古島市も対象に全 5 回開催した。

会場開催の説明会もオンラインで視聴できるよう Web 公開していたが、日程上の理由で事業説明会へ参加できない企業へ向けに全 3 回のウェビナー形式説明会を開催した。

事業説明会では、事業内容の説明とサイバーセキュリティの普及に向けた啓発を行った。サイバーセキュリティについて身近に感じてもらうため、沖縄県警サイバー犯罪対策課の担当官にも登壇（※沖縄本島の那覇会場 2 回、中部会場）を依頼し、企業を取り巻くサイバー犯罪の状況について紹介してもらった。

今回離島でも開催したが、企業総数自体が少ないため説明会への参加数は乏しかったが、複数の企業から実証への参加申込みがあり、参加率としては高く、効果的であったと考える。

4.2.　個別対応（メール・電話・訪問）

所有している取引先・関係先で構成される募集先リストに対し、電話やメールでの案内の他、訪問を許された相手先には個別訪問をして本実証事業への参加呼び掛けを行った。

今回の募集先には、沖縄電力グループの孫請け企業（サプライチェーン）も含めた。

▼個別対応の件数

募集先リストへの電話　約 200 件

募集先リストへの DM約 1,800 通

募集先リストへの訪問　約 50 件

※沖縄電力の孫請けリストへのアプローチ件数：約 30 件

4.3.　会報誌へのチラシ封入

各会員組織への会報誌にチラシ封入をして、本実証事業の告知を行った。

▼チラシ封入数

那覇商工会議所会員への会報誌：4,570 部

AIKATA（※）会員への会報誌：90 部

※沖縄県内の企業で構成されるビジネスマッチングや相互サポートを目的とした会員制のビジネスプラットフォーム組織

4.4.　その他、メディアなど

4.4.1.　ホームページ

「沖縄サイバーセキュリティお助け隊」として事務局で専用ホームページを開設し、本実証事業に関する申込受付や情報提供を行った。

また、沖縄県産業振興公社や那覇商工会議所のホームページにも本実証事業に関する情報を掲載する協力を得た。

■専用ホーム開設日　2020 年 9 月 7 日（月）
■URL：https://www.okinawa-cyber-otasuketai.com/

図 19：お助け隊ホームページ TOP ページ

4.4.2.　メルマガ・SNS など

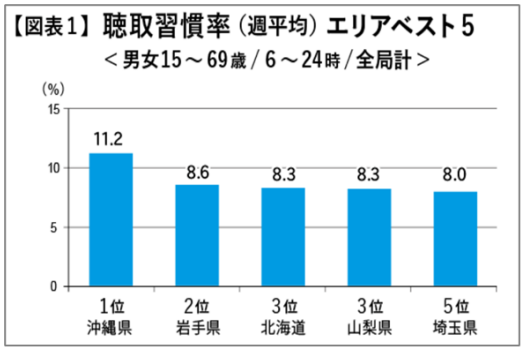
コンソーシアム構成企業である株式会社セキュアイノベーション社の公式 SNS（Facebook）での告知の他、那覇商工会議所や沖縄総合事務局、沖縄県産業振興公社、ISCO（沖縄 IT イノベーション戦略センター）など沖縄県内の各団体の協力を得て、メルマガ配信で募集告知を行った。

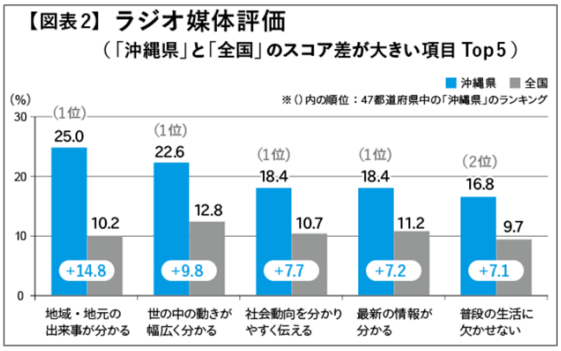
■メルマガ配信数
沖縄県総合事務局：4,570 通
那覇商工会議所：約 800 通 ISCO：約 1,200 通
沖縄県産業振興公社：約 8,100 通

4.4.3.　ラジオ

沖縄県はマイカー通勤が多く、ラジオ聴取率が非常に高いエリアとされており、そこへ着目しラジオ CM なども活用し告知を行った。

結果として、ラジオを聞いて問合せを受けたケースも複数発生しており、問合せや申込みにまでは至らずとも取引先や関係者から「ラジオを聞いたよ」という声も挙がっており、沖縄地域においてはラジオ媒体での告知は有効なものだったと分析する。

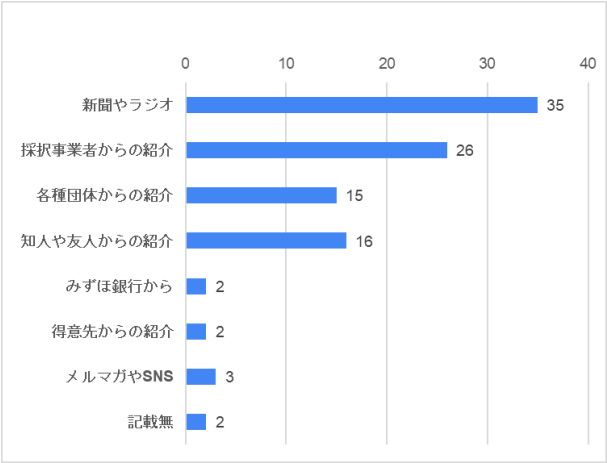




株式会社ビデオリサーチ（2017年10月調査）

図 20：ラジオ CM の効果性

図 21：本実証事業を知ったきっかけを教えてください（複数回答）



考察：新聞やラジオといったメディアの告知が有効であったことが分かった。

エフエム沖縄

・ラジオ CM

期間　：2020 年 9 月 14 日（月）～2020 年 10 月 30 日（金）

放送数：20 秒×57 本

・番組内告知①

日程　：2020 年 10 月 2 日（金）10：10～

番組名：Fine!

番組内容：県内で生放送している情報発信番組

発信内容：事業概要や背景、説明会実施内容、問合せや申込みについて

・番組内告知②

日程　：2020 年 10 月 19 日（月）　17：00～

番組名：ForPM

番組内容：県内で生放送している情報発信番組

発信内容：事業概要や背景、説明会実施内容、問合せや申込みについて

RBC-i ラジオ

・ラジオ CM

期間　：2020 年 9 月 14 日（月）～2020 年 10 月 30 日（金）

放送数：20 秒×57 本

・番組内告知③

日程　：2020 年 9 月 28 日（月）　12：50～

番組名：ミュージックシャワー

番組内容：県内で生放送している情報発信番組

発信内容：事業概要や背景、説明会実施内容、問合せや申込みについて

4.4.4.　新聞・ニュース

募集説明会の開催に関しては沖縄県内の地元 2 紙（琉球新報：2020 年 9 月 13 日（日）、沖縄タイムス：2020 年 10 月 10 日（土））にも取り上げられ、2020 年 10 月 2 日（金）開催の第 2 回目の事業説明会に関しては、QAB 琉球朝日放送のニュースでも報じられた。

4.5.　実証参加企業の募集活動における課題考察

当初の目論見では沖縄地域の主要産業であり、個人情報も日常的に取り扱う観光業の企業をメインターゲットの 1 つに考えていたが、コロナウィルスによるビジネスへの影響をダイレクトに受けてしまい、実証へ参加するどころではない企業が数多くおり、最終的に観光業の企業の参加は乏しいという結果になってしまったことは大きな誤算であった。

次に、今回は多くの目に触れる目的でメディア掲載も行い、公的機関や団体などからも告知を行ったが、準備・計画期間が十分でなかったこともあり、一度に複数のチャネルでの同時告知となったため逆に情報を目立たせることができず、埋もれてしまった可能性がある。この点はチャネルごとに時期をずらしていく工夫が必要であったと考える。

また、実際に参加へ至ったケースの多くは訪問や電話などの個別対応であったことから、メディア媒体やメルマガ告知は広域に周知するという意味では効率的ではあるが確実性が十分でないという結果も示された。

いずれの告知に関しても、事業説明会の参加を促すもののみならず、個別での相談会や説明会などの個別対応へ誘導するアプローチも必要であったと考える。

5.　事業説明会の開催

5.1.　開催結果

開催結果は以下のとおり。

開催形式	開催日・開催会場	申込 企業数	申込 人数	参加 企業数	参加 人数	実証事業 参加企業数
会場開催	9 月 15 日（火）：那覇会場①	13 （2）	14（2）	12（2）	13（2）	7
ウェビナー	9 月 29 日（火）：オンライン①	2（2）	2（2）	2（2）	2（2）	0
会場開催	10 月 2 日（金）：中部会場	10	11	7	12	3
ウェビナー	10 月 5 日（月）：オンライン②	9（9）	5（5）	5（5）	5（5）	1
会場開催	10 月 6 日（火）：石垣会場	3	3	3	3	2
会場開催	10 月 8 日（木）：宮古島会場	7	10	6	9	2
会場開催	10 月 23 日（金）：那覇会場②	27 （12）	35 （13）	23 （11）	30 （13）	5
ウェビナー	11 月 9 日（月）：オンライン③	0	0	0	0	0
	合計	71	80	58	74	20

※（　）内はオンライン参加数

表 4：説明会の開催結果

会場開催（計 5 回）

■第 1 回事業説明会（那覇会場）

日時：2020 年 9 月 15 日（火）　14：30～15：30（14：00 開場）
場所：おきでんふれあいホール
▼アジェンダ
14：30～14：35　開会挨拶
14：35～15：00　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）
15：00～15：15　企業と取り巻くサイバー犯罪の状況について（沖縄県警サイバー犯罪対策課）
15：15～15：30　お助け隊事業内容説明（セキュアイノベーション）

図 22：事業説明会の実施風景（第 1 回開催）

■第 2 回事業説明会（中部会場）

日時：2020 年 10 月 2 日（金）　14：30～15：30（14：00 開場）
場所：ミュージックタウン音市場
▼アジェンダ
14：30～14：35　開会挨拶
14：35～15：00　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）
15：00～15：15　企業と取り巻くサイバー犯罪の状況について（沖縄県警サイバー犯罪対策課）
15：15～15：30　お助け隊事業内容説明（セキュアイノベーション）

図 23：事業説明会の実施風景（第 2 回開催）

■第 3 回事業説明会（石垣会場）

日時：2020 年 10 月 6 日（火）　14：30～15：30（14：00 開場）
場所：石垣市商工会　商工会ホール
▼アジェンダ
　14：30～14：35　開会挨拶
　14：35～15：00　お助け隊事業概要案内（沖電グローバルシステムズ）
　15：00～15：30　お助け隊提供サービス説明（セキュアイノベーション）

図 24：事業説明会の実施風景（第 3 回開催）

■第 4 回事業説明会（宮古島会場）

日時：2020 年 10 月 8 日（木）　14：00～15：00（14：00 開場）
場所：ホテルアトールエメラルド宮古島
▼アジェンダ
　14：00～14：05　開会挨拶
　14：05～14：30　お助け隊事業概要案内（沖電グローバルシステムズ）
　14：30～15：00　お助け隊提供サービス説明（セキュアイノベーション）

図 25：事業説明会の実施風景（第 4 回開催）

■第 5 回事業説明会（那覇会場）

日時：2020 年 10 月 23 日（金）　14：30～15：30（14：00 開場）
場所：おきでんふれあいホール
▼アジェンダ
14：30～14：35　開会挨拶
14：35～15：00　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（代読：沖電グローバルシステムズ）
15：00～15：15　企業と取り巻くサイバー犯罪の状況について（沖縄県警サイバー犯罪対策課）
15：15～15：30　お助け隊事業内容説明（セキュアイノベーション）

図 26：事業説明会の実施風景（第 5 回開催）

ウェビナー形式開催（計 3 回）

■第 1 回お助け隊提供サービスオンライン説明会

日時：2020 年 9 月 29 日（火）　14：00～14：30
14：00～14：30　お助け隊事業概要、提供サービス説明（セキュアイノベーション）

■第 2 回お助け隊提供サービスオンライン説明会

日時：2020 年 10 月 5 日（月）　16：00～16：30
16：00～16：30　お助け隊事業概要、提供サービス説明（セキュアイノベーション）

■第 3 回お助け隊提供サービスオンライン説明会

日時：2020 年 11 月 9 日（月）　13：00～13：30
13：00～13：30　お助け隊事業概要、提供サービス説明（セキュアイノベーション）

5.2.　事業説明会に関する課題考察

いずれか都合の良い日程で参加が可能なように開催日とエリアを複数に分けて開催したが、告知した数と比較すると参加数は芳しくない結果であった。中小企業のサイバーセキュリティに対する意識・関心が想定を下回るものであったと考えるが、開催告知の段階でセキュリティ対策の必要性をしっかり訴求しておくべきであった。

また、説明会自体についてはコロナウィルスの影響を考慮し、説明会の開催時間を 1 時間以内に留めるようにしたため、詳細に説明をしていく時間を取らなかったこともあり、セキュリティに対する意識・知識に乏しい参加者にとっては説明不足な内容で短時間での理解が困難であった可能性もある。実際に事業説明会への参加者からも、「我々のような中小企業にはこうした説明会では厳しいのではないか」という意見もあった。

事業説明会への参加者から実際に本実証事業への参加へ繋がる参加率に関しては実際に訪問して個別で募集を行う方がより確実性が高いという結果も出ているが、個別対応の場合はヒアリングと同時に相手の反応を見ながらの説明や質疑応答が可能であったので当然の結果と言える。中小企業のサイバーセキュリティに対する意識・知識がまだまだ乏しい現状を考慮すると、それらの中小企業に対しては日頃の情報提供及び個別での寄り添いが必要であるという課題も明確になった。

6.　成果報告会の開催

6.1.　開催結果

実証参加企業のみを対象にせず、オープンな形での広く募集を行う形で開催した。

募集に関しては、那覇商工会議所や沖縄県総合事務局などの各機関に協力のもとでメルマガでの周知の他、沖縄県内の地元紙（沖縄タイムス：2021 年 1 月 13 日（水））でも告知を行った。

■成果報告会

日時：2021 年 1 月 15 日（金）　14：30～16：00（14：00 開場）

場所：沖縄県立図書館ホール

開催日	申込 企業数	申込 人数	参加 企業数	参加 人数	実証事業 参加企業数
2021 年 1 月 15 日（金）	14（7）	16（7）	15（7）	17（7）	9

※（）内はオンライン参加数

表 5：成果報告会時の開催結果

▼アジェンダ

14：30～14：40　開会挨拶（IPA）

14：40～15：10　SECURITY ACTION（イージーコンプ）

・SECURITY ACTION

・中小企業の情報セキュリティ対策ガイドライン

15：10～15：50　お助け隊実証事業実施成果（セキュアイノベーション）

・本実証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

15：50～16：00　サイバーセキュリティ保険について（損保ジャパン）

16：00～16：10　事務連絡（サイバーお助け隊事務局）

図 27：成果報告会の実施風景

6.2.　成果報告会に関する課題考察

コロナウィルスの感染拡大により緊急事態宣言が再度発令された影響もあって、参加者数は芳しいものではなかった。

しかしながら参加者からは以下のようなコメントがあったり、個別で話を聞きたいという要請もあったりしたため、参加者にとって良い情報提供ができたものと考える。

▼参加者コメント

- 事例が聞けて参考になって良かった。
- 他社も同じなのだということが分かって安心した。
- アンケートの分析結果がとても分かりやすくて良かった。
- 社内でセキュリティ対策を強化するようにどうやって説明するか考えたい。
- 結局自社はいくら対策コストを掛けたら良いかは分からなかったが、対策をしないとマズいという認識は持てた。

アンケートを含めたこうした情報共有は中小企業へセキュリティへの関心・意識を持ってもらうために非常に重要な手段となるはずであるため、定期的に実施することを検討していく。

7.　中小企業の実態把握

7.1.　実施概要

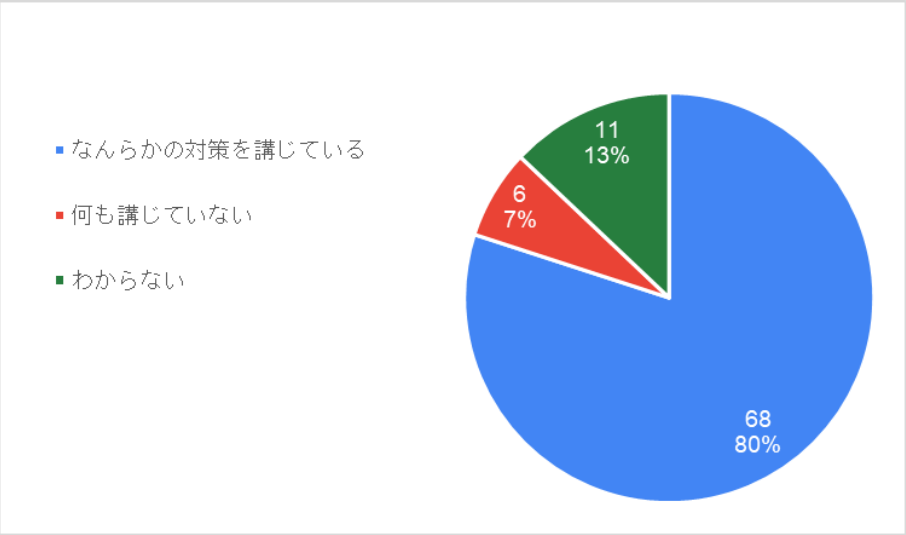
セキュリティ対策支援サービスの提供結果及び中小企業へのアンケートの他、ヒアリングや問合せ内容の各結果から中小企業の実態について考察をする。

7.2.　アンケート結果

7.2.1.　アンケート結果

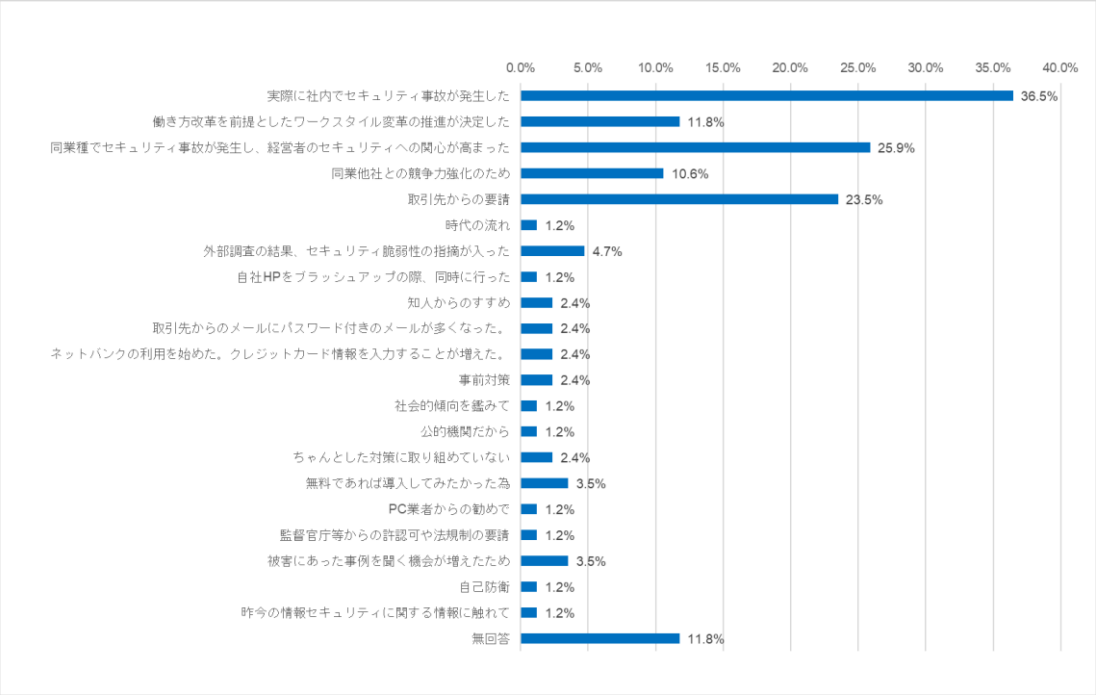
説明会への参加者及び本実証事業への参加者に対して、書面及び Web でのアンケートを実施した。以下にその結果を示す。

図 28.　現在勤務先では何らかの情報セキュリティ対策を講じていますか。（n=85）



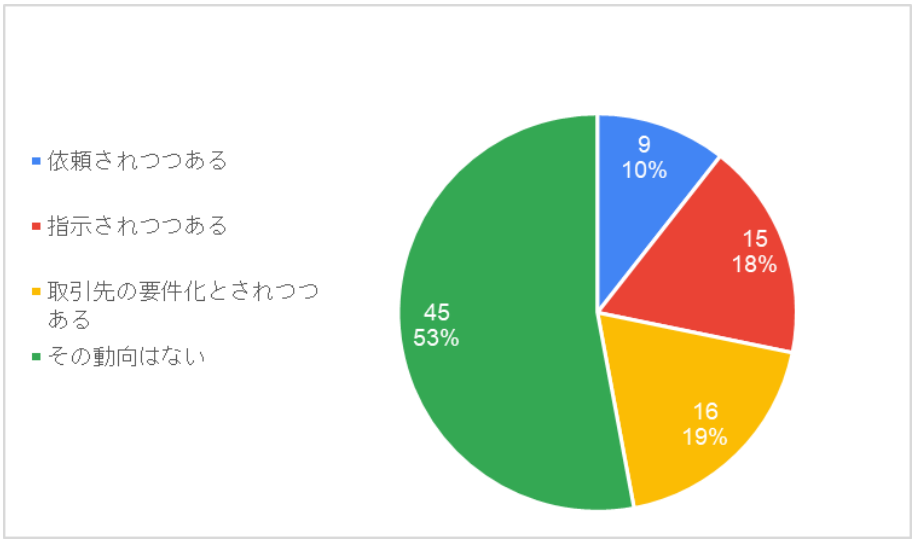
考察：本実証事業に関心がある方を対象にしていることもあり、何かしらの対策は講じているという回答が多かったものと考える。

図 29. 勤務先において、情報セキュリティ対策に取り組むきっかけとなった理由について、ご自身のお考えに近いものをお選びください。（n=85）



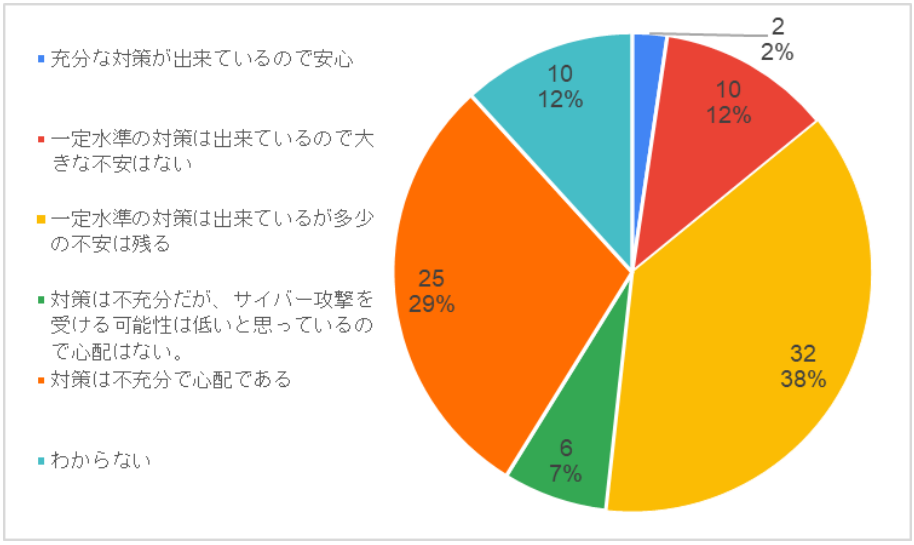
考察：社内や同業他社におけるセキュリティインシデントの発生や取引先からの要請など、他人事から自分事になったことがきっかけになっている。

図 30. 取引先からのサイバー攻撃対策を求める要請の有無について教えてください。（n=85）



考察：半数ほどの企業に対応の必要性が出てきている状況がうかがえた。

図 31. 勤務先のセキュリティ対策の充実度はどのように感じていますか？（n=85）



考察：約 90%が自社のセキュリティ対策に不安を抱えている状況がうかがえた。

図 32. 勤務先で導入済みのセキュリティ対策を教えてください（n=85）

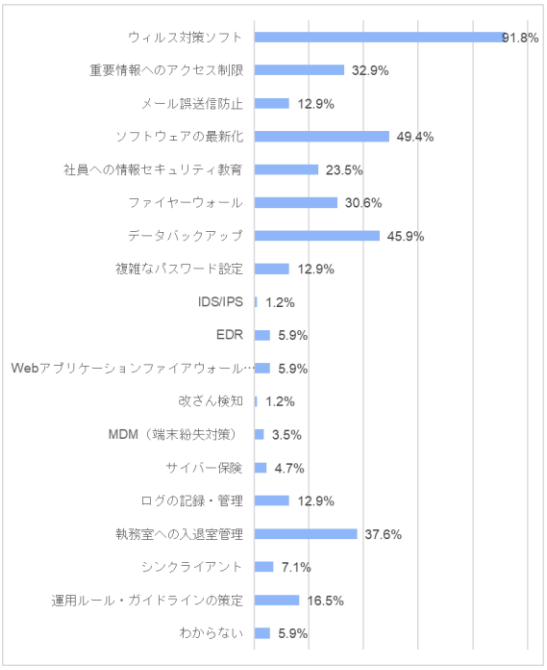
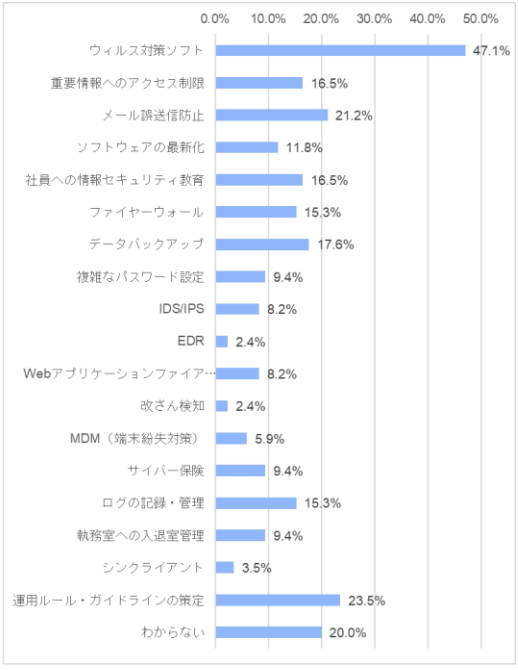
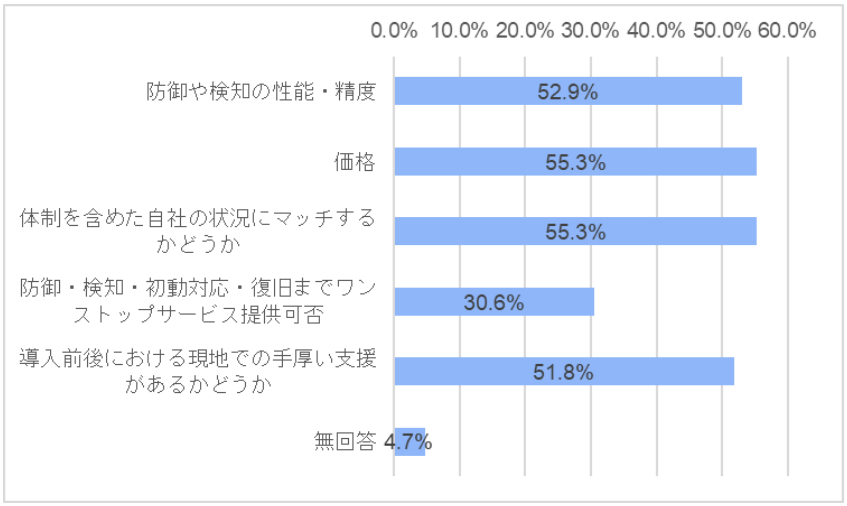


図 33. 勤務先で検討したことがあるセキュリティ対策を教えてください（複数回答）（複数回答）（n=85）



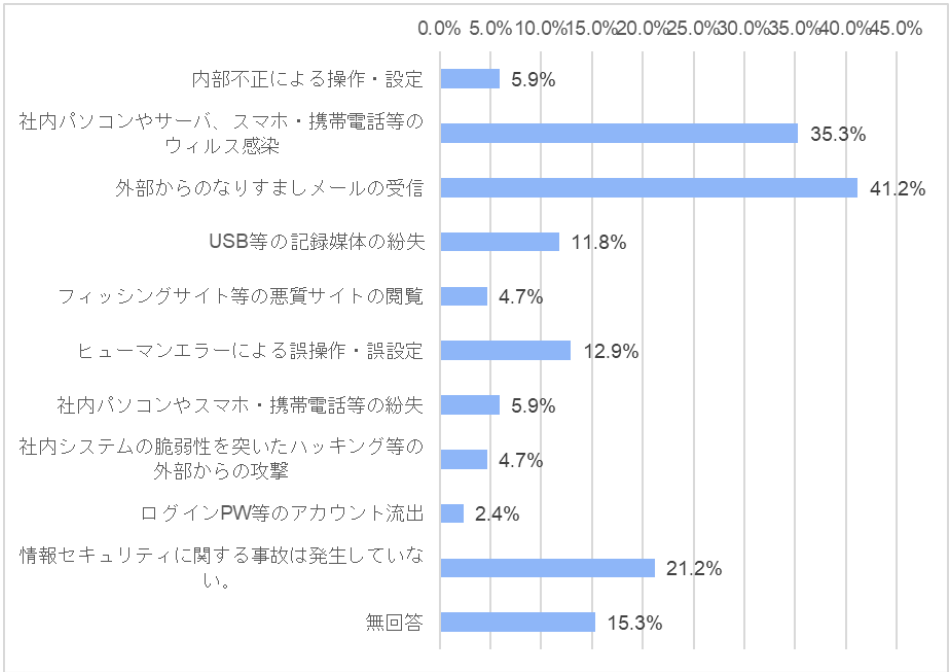
考察：セキュリティ対策ソリューションの導入・検討は議題に挙がるが、根本的に重要となる運用ルール・ガイドライン策定といったアナログな準備に関する対応への意識が希薄であることが考えられる。

図 34. セキュリティ対策製品・サービスを導入する上で重要視したいことを教えてください。（複数回答）（n=85）



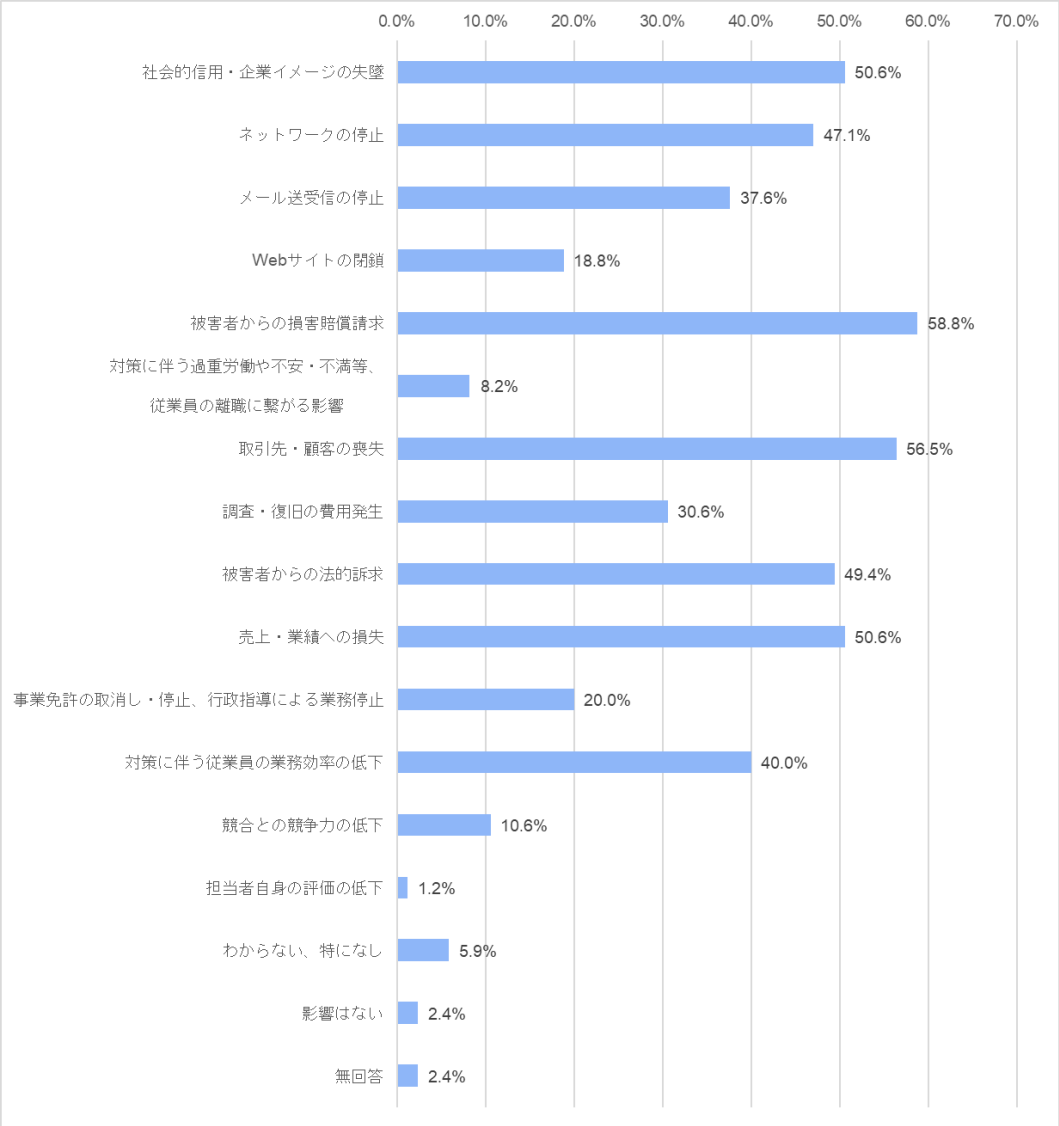
考察：性能や価格といったところは当然な要素だが、現地での手厚いサポートにも価値を見出していることがうかがえる。

図 35. 勤務先において発生したことのあるセキュリティに関する事故の理由について近いものをお選びください。（複数回答）（n=85）



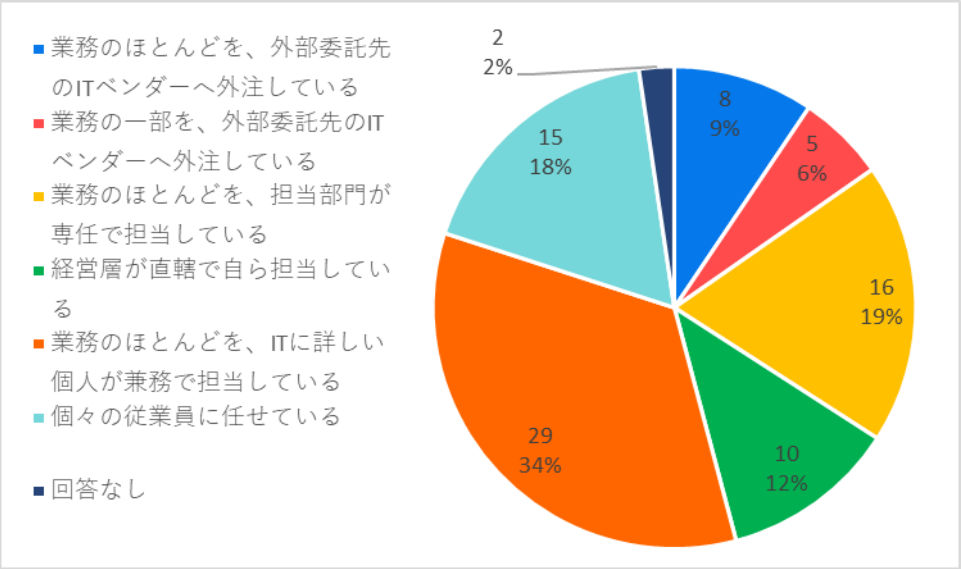
考察：セキュリティ事故の発生がないのは 2 割程度（=8 割程度は何らかの事故が起きている）という状況がうかがえた。

図 36. 勤務先の状況を踏まえ、情報セキュリティ事故に関してご自身が心配しているものをお選びください。（複数回答）（n=85）



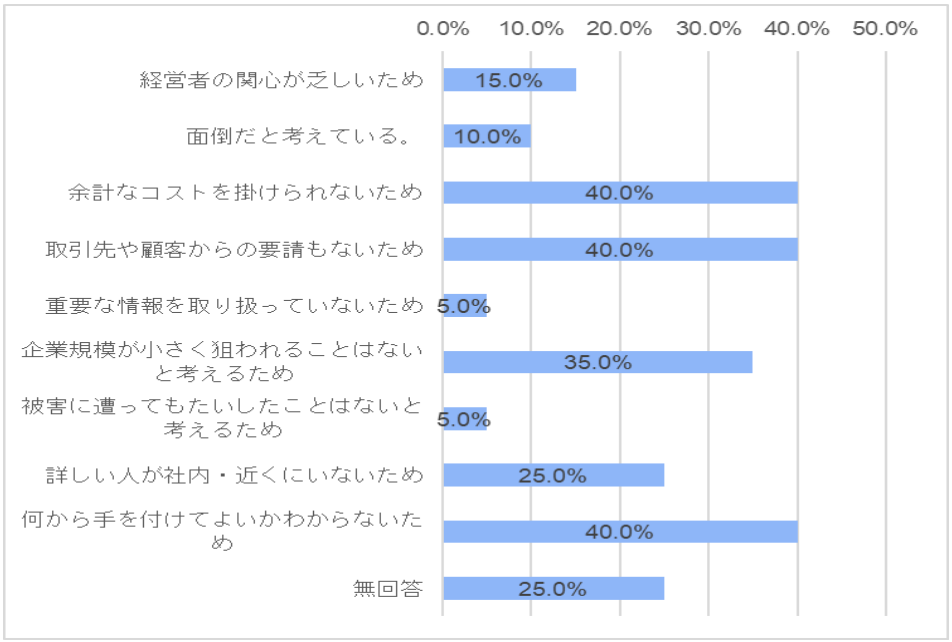
考察：やはり事業継続に関するリスクについて懸念していることがうかがえた。

図 37. 現状の社内 IT 環境を運用する人員について最も近いものをお選びください。



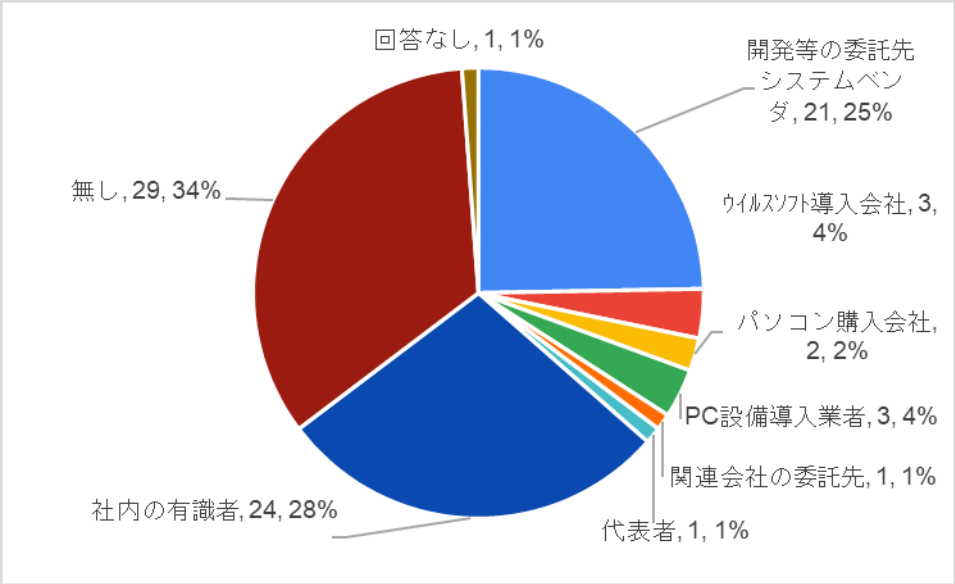
考察：外部へのアウトソーシングを活用できているのは約 15%程度で、自社で対応しようとしている状況がうかがえる。

図 38. 情報セキュリティ対策を講じていないのはどういった理由からだとお考えでしょうか。（複数回答）（n=20）



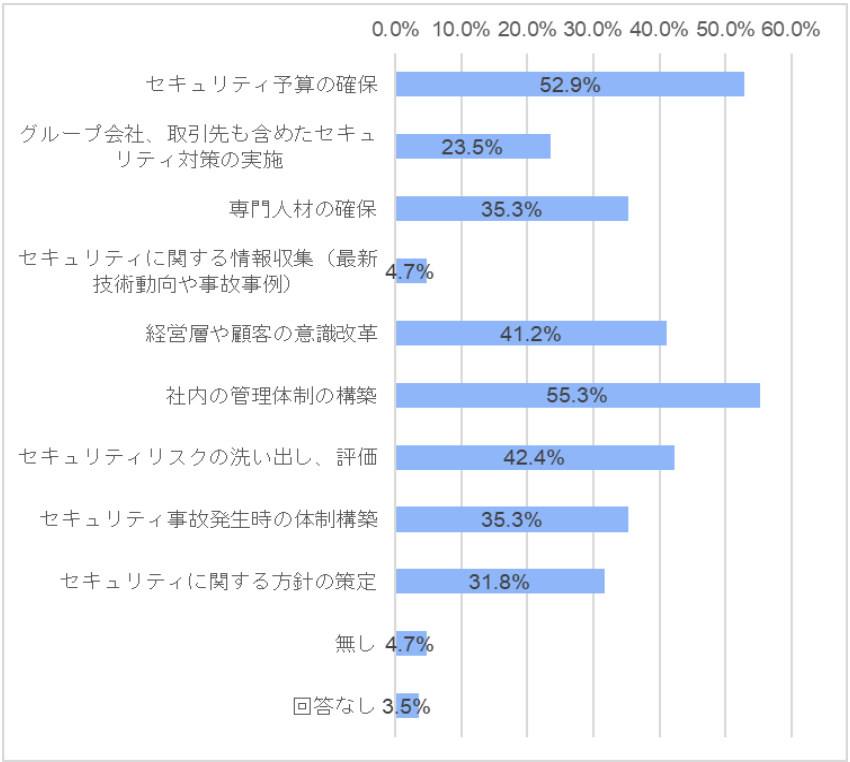
考察：重要な情報資産がなく自社が狙われることはない、被害は小さい、というように中小企業が置かれている状況を理解できていない様子がうかがえる。

図 39. セキュリティ事故発生時の相談先はありますか ？（n=85）



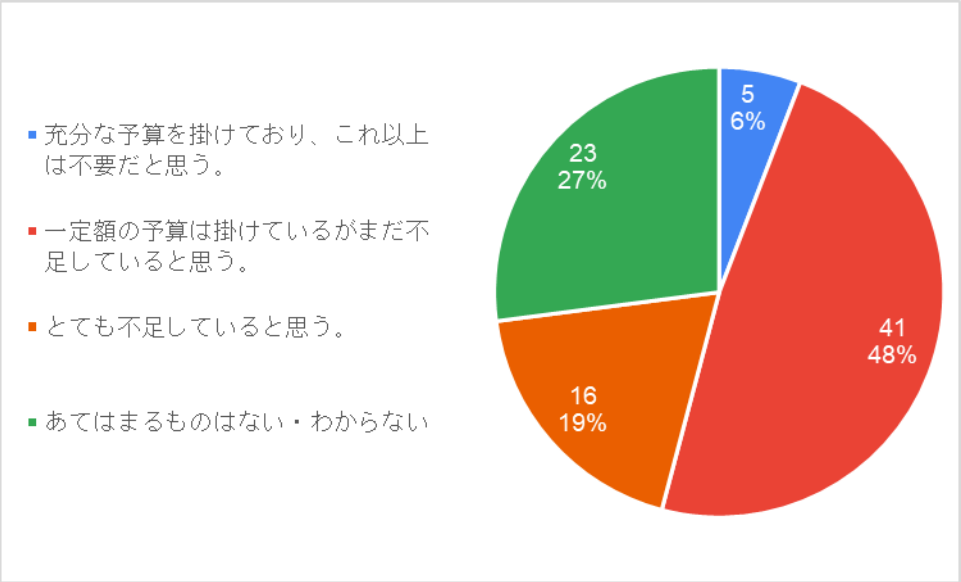
考察：相談先すらないのが約 30％で外部の相談先を有しているのが約 35％という結果であった。

図 40. サイバーリスク関して課題だと感じているものを教えてください。（複数回答）（n=85）



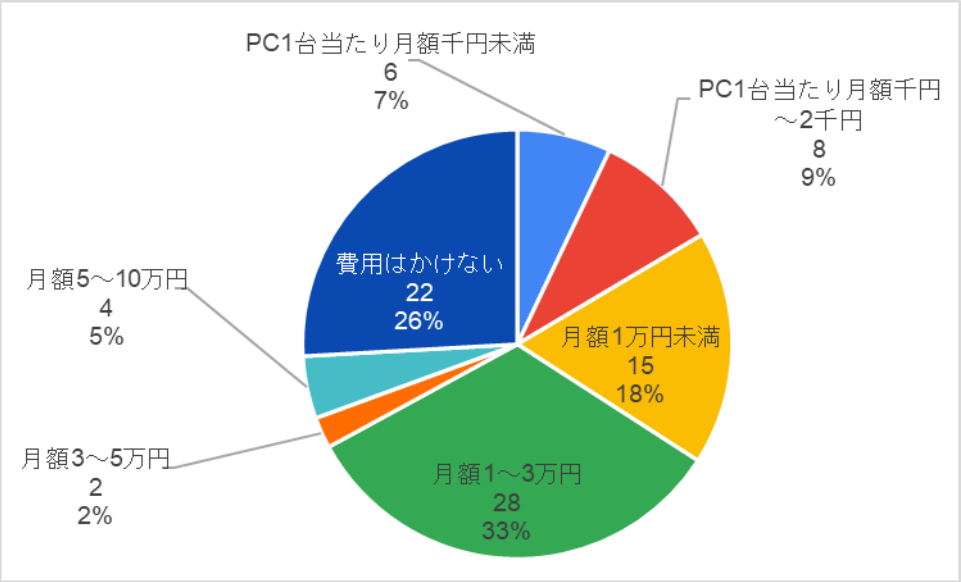
考察：課題は多岐にわたるが、管理体制の構築の部分に関しては属人的で組織的な対応に課題を感じているものと推察する。

図 41. 勤務先における現状のセキュリティ対策予算についてお考えをお聞かせください。（n=85）



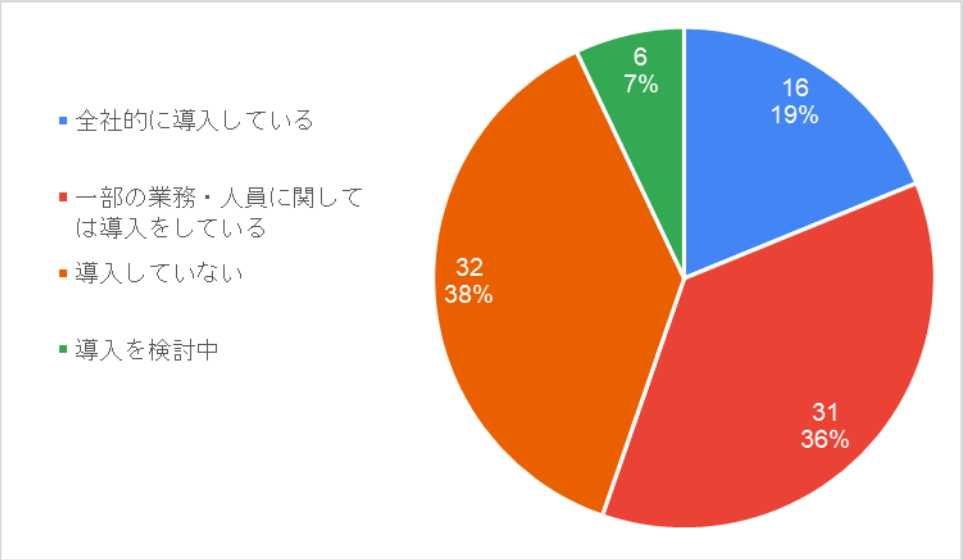
考察：ほとんどの企業（95%）が不足を感じていることが分かった。

図 42. 勤務先のセキュリティ対策経費としてはどの程度の経費を掛けることができるとお考えでしょうか。（n=85）



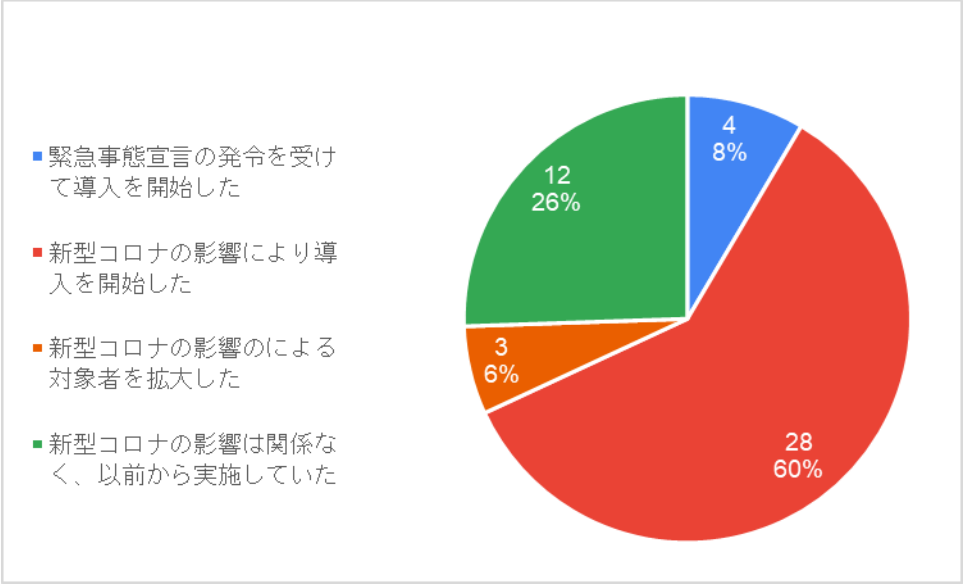
考察：月額 3 万円以上という回答は全体の 7%で、多くの中小企業にとっては月額 1～3 万円（理想は 1 万円以下）が現実的な予算だと推測する。

図 43. テレワークの導入状況について教えてください。(n=85)



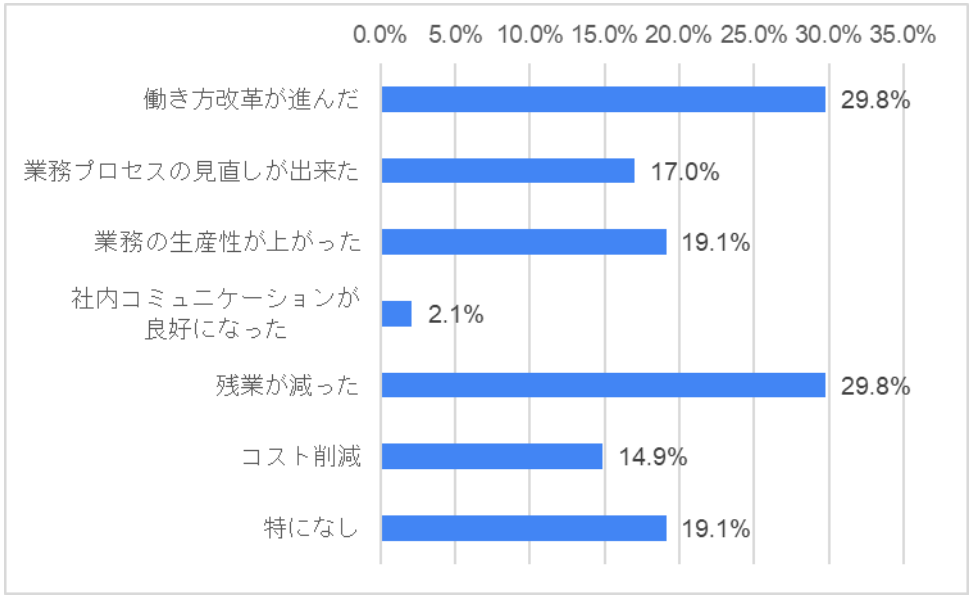
考察：セキュリティ対策に比較的関心がある企業へのアンケートとはいえ、半数以上はテレワークを導入していることがうかがえた。

図 44. テレワークの導入時期について教えてください。(n=47)



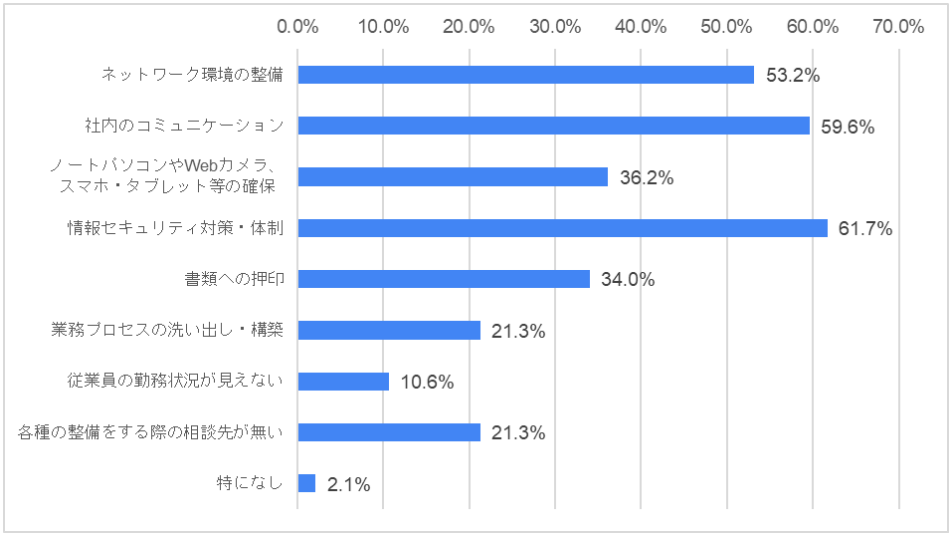
考察：コロナウィルスの影響がある前からの導入企業は 25%となっており、やはりコロナウィルスは働き方へ変化を与える大きな転機となっている。

図 45. テレワークによって感じた効果を教えてください。（複数回答）（n=47）



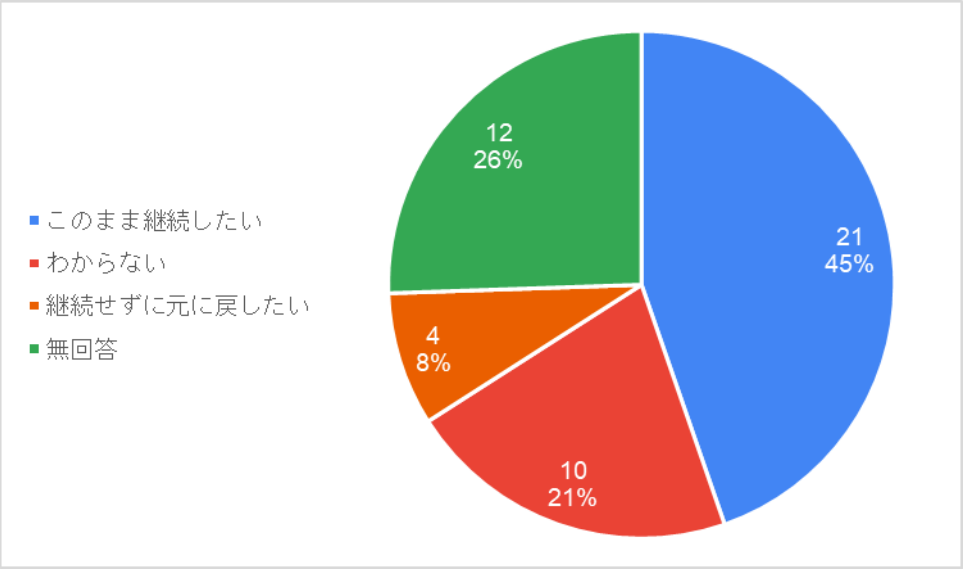
考察：「特になし」が約 20%という結果になっており、約 80%が何らかの効果を感じていることがうかがえる。残業が減ったという結果も出ているが、サービス残業が増えたという声も。

図 46. テレワークを導入する際に生じた課題を教えてください。（複数回答）（n=47）



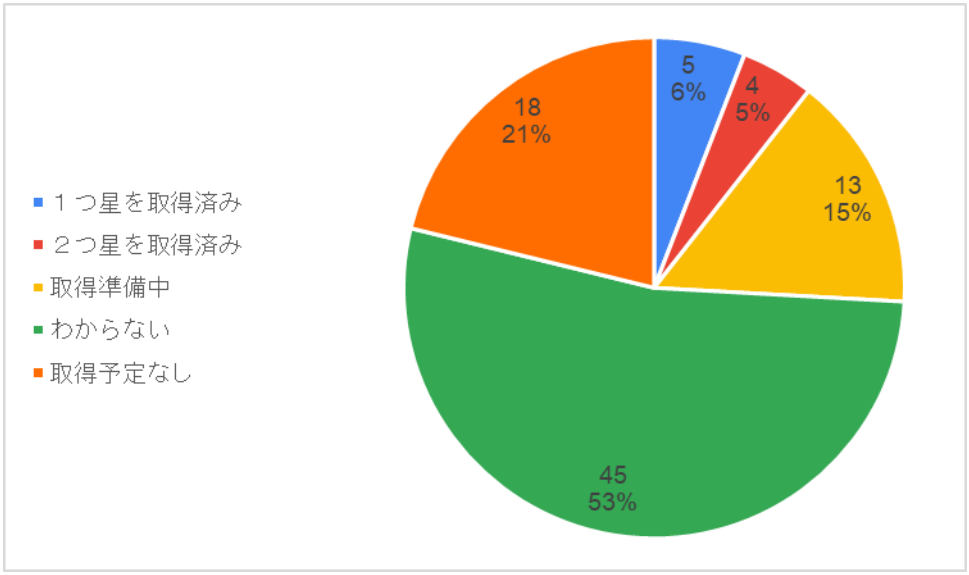
考察：様々な課題が生じた中で、やはりセキュリティ対策は大きな課題となっていたことがうかがえる。

図 47. 新型コロナ収束後もこのままテレワークの導入を継続したいとお考えですか？（n=47）



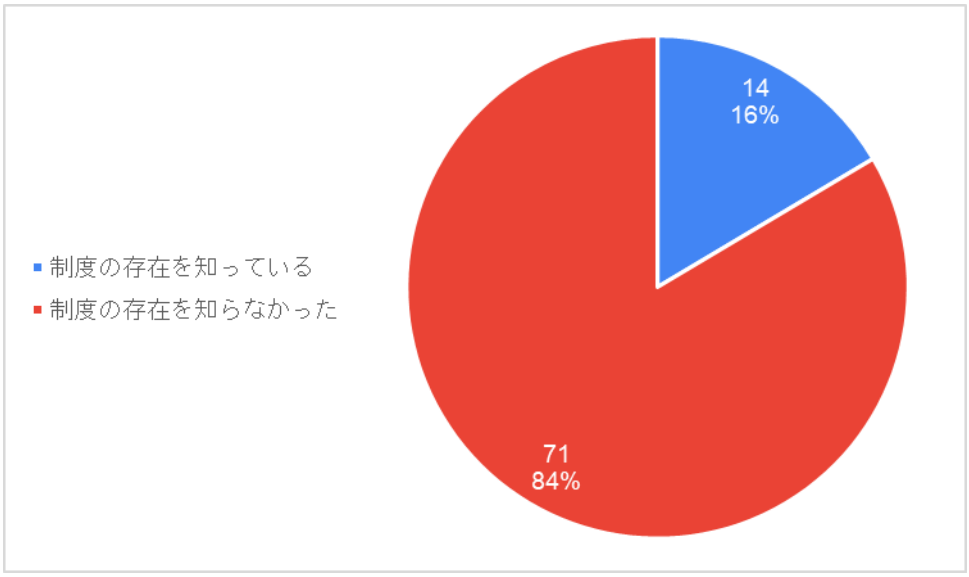
考察：元に戻したいと考えているのは 10%以下という結果で、やはりテレワークは新しい働き方として定着していくものと予想される。

図 48. SECURITY ACTION の取得状況を教えてください。（n=85）



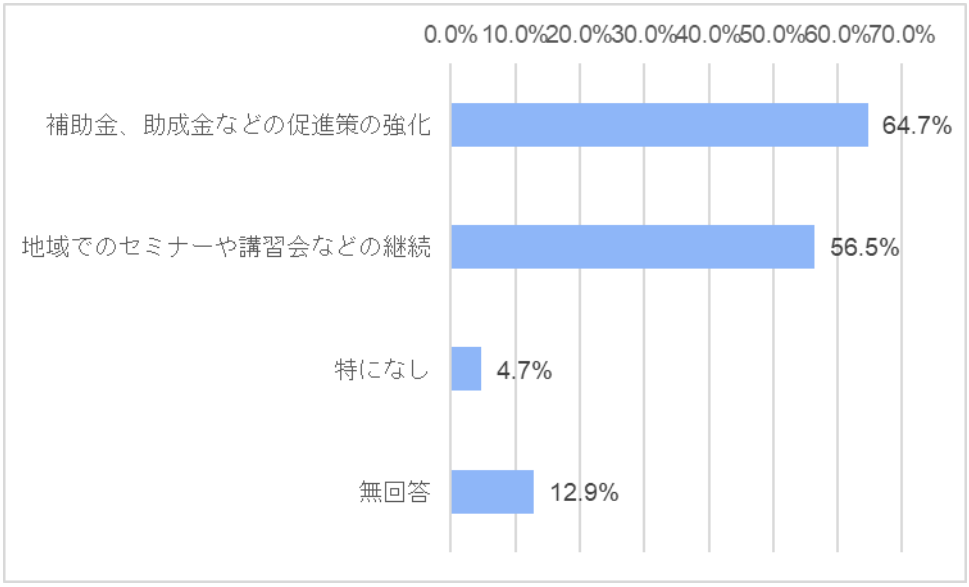
考察：取得済みは約 10%という結果であった。分からないという回答を含め、取得段階にない企業が 75%を占めているため、今後の普及活動が必須な状況となっている。

図 49. 「SECURITY ACTION」制度を知っていましたか？（n=85）



考察：存在を知らないという回答が 80%超となっており、認知度がまだまだ低い状況であり、制度の認知度を上げることでおのずと「SECURITY ACTION」の取得も広がるものと考える。

図 50. セキュリティ対策に関して政府に期待することを教えてください。（複数回答）（n=85）



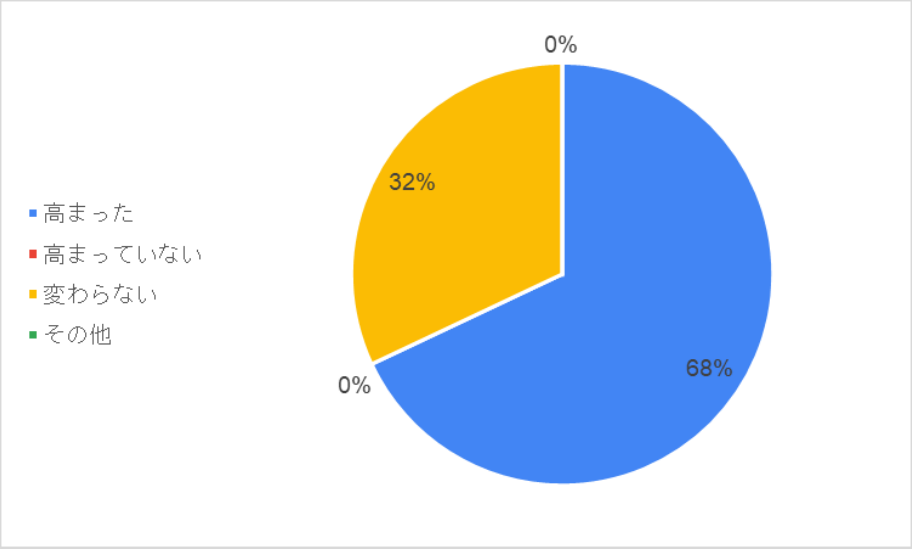
考察：コスト負担軽減のための支援を求める声が大きいことがうかがえる。

7.2.2. アンケート結果（実証後の変化）

本実証事業へ参加後の意識などの変化を捉える目的で成果報告会への参加者及び本実証事業への参加者に対して、書面及び Web でのアンケートを実施した。

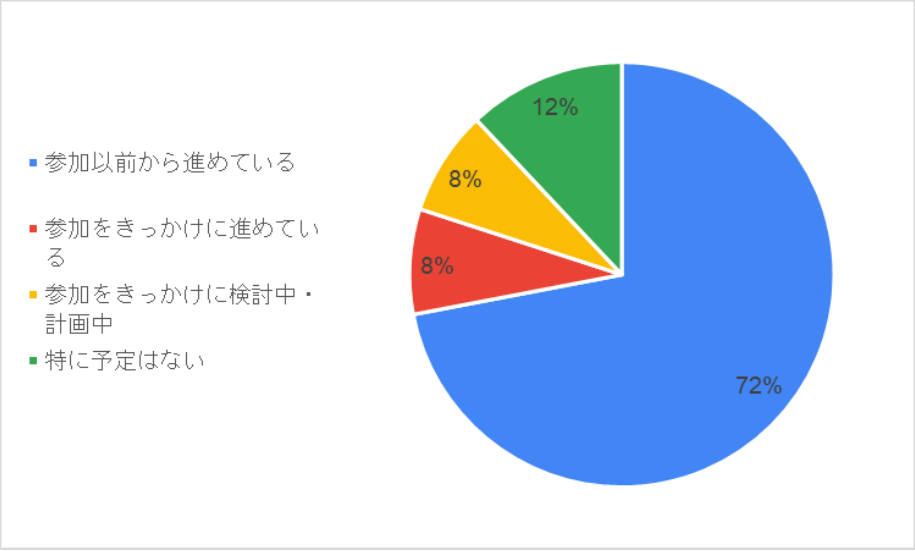
以下にその結果を示す。

図 51. セキュリティ対策に関する意識は高まりましたか？（n=25）



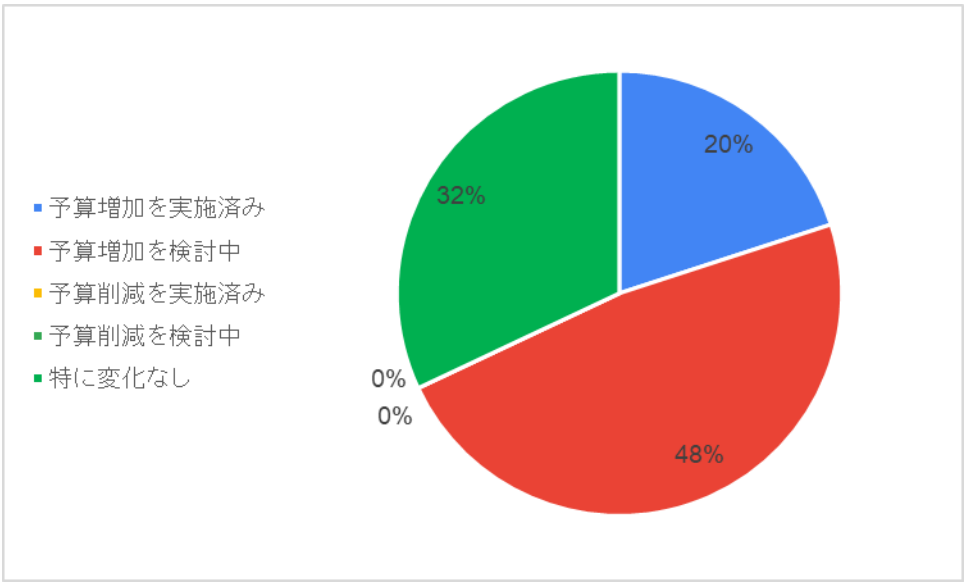
考察：7 割近くの企業が「意識が高まった」という回答をしており、本実証事業による成果がうかがえる。

図 52. セキュリティ対策・体制の強化をしましたか？（n=25）



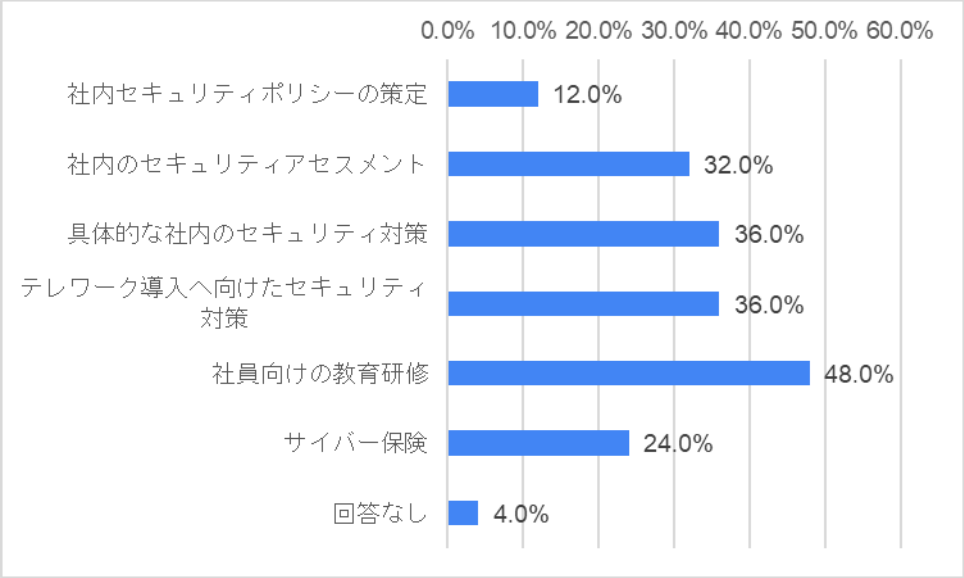
考察：7 割近くの企業が以前から対策を進めていた企業であり、本実証事業に参加していること自体が意識の高さを示していると考える。

図 53. 勤務先における現状のセキュリティ対策予算についてお考えをお聞かせください。(n=25)



考察：7 割近くの企業が予算増の動きをしており、本実証事業による意識の高まりがうかがえる。

図 54. 改めて特に相談したいと思うことはありますか？（複数選択）(n=25)



考察：特に社員教育のニーズが高いため、まずはその部分のニーズを満たすことで、次の具体的なセキュリティ対策へ繋がるものと考える。

7.2.3. ヒアリング結果コメント

実証参加企業への個別対応など本実証事業への募集活動において、企業からのヒアリングしたコメントについて、それぞれの分野に分けて示す。

種別	コメント
組織	◆セキュリティの知見を持った人材の確保が難しく、そもそも新規雇用の余力も乏しい。 ◆経営層の関与が求められていることは理解できるが、知識が乏しく理解度が低いため、実際はとても難しい。 ◆全てを把握している担当者がいると助かるが、退職してしまう際のリスクが恐ろしい。 ◆セキュリティ事故発生を想定した費用は年度予算に組み込んでおらず、緊急費となるので発生してしまうことを想像すると恐ろしい。 ◆セキュリティ事故が想定被害額の算出が難しいので、何か参考になるような他社情報が欲しい。 ◆セキュリティ対策は売上を生むような投資コストではないので予算に組み入れるのが難しい。セキュリティ対策をしていることが売上アップなど、直接的なメリットがあるようになると予算も確保しやすい。
社内ルール運用	◆自社では難しいので親会社に全て指針や規定を作ってもらいたい。 ◆社内向けに口頭や文書での注意喚起はあるものの、具体的な対策措置の要件や指示が曖昧 ◆整備すべきパターンが無数にあると捉えていて、どの部分のルール・規定を作成すべきか分からない。 ◆セキュリティ製品やサービスを導入するのは良いが、結局導入した後に何かあった際にこちらで実施すべきことが不明で、本来はトレーニングが必要なはずだがなかなか難しい。 ◆社内ルール・ポリシーを策定すること自体に専門性が必要でハードルが高い。
技術	◆相談をしてもベンダーに対応外と言われて困るケースがある。 ◆ベンダーから次々に新しいサービスを提案されて、何が良い対策なのか分からなくて困る。 ◆全部ベンダー任せなのできちんと理解している担当者が社内に不在。 ◆そもそも導入時に専門用語が難解でやりとりが多くなってしまい、ベンダー側も含めて双方ストレスになっていると思う。
コスト	◆似たようなサービスが色々あるが違いが分からず、そのためコストの妥当性も分からない。

	◆導入するサービスの優先順位が不明。 ◆成果報酬や使用した分だけ支払うようなサービスが望ましい。 ◆「これは料金追加です」と言われるケースが多く、最初から含めた金額提示や提供内容の明確化をしっかりしてほしい。
取引先	◆契約書や仕様書でセキュリティに関する言及はあるが、具体的な方法やレベル感が不明で困る。 ◆セキュリティ対策を講じるためのコスト負担を取引先に求めて良いものか悩ましい。

表 6：個別ヒアリング結果

セキュリティ対策を実行する段階だけでなく、社内ルールや方針、予算策定といった計画段階においても人材不足の影響が出ている様子がうかがえた。

優秀な人材や新しい機能等を獲得するためのコストは競争力を生むための戦略コストという認識はあるはずだが、セキュリティ対策については戦略コストという理解にはなっておらず、むしろ自社のみがコストを掛けることはできないと考えているような様子がうかがえた。

そうした意味で他社事例を継続的に共有していくことは意味が大きいと考える。

7.2.4. アンケート結果からの全体評価

ヒト・カネ・情報が不足しているという点に関しては想定通りであったが、セキュリティインシデントが発生したことがあると認識している企業は想定以上に多く、驚きの結果であった。加えて、外部への相談先がなく困っている状況や身近な相談先を求めていることも見て取れたため、そういった意味でお助け隊事業のニーズの高さを再確認することができた。

一方、企業個々の課題はそれぞれながら、セキュリティ対策の必要性を感じている企業と感じていない企業の意識の差が大きい状況も感じとられ、その部分を埋めるために本来必要な情報提供が大きく不足している現状も確認ができた。今後もテレワークが継続導入されることが予想される中で特にセキュリティ対策の入口となる SECURITY ACTION やリスクヘッジとして最後の拠り所となるサイバー保険の認知度の低さは大きな課題であり、この点を解消することで、中小企業におけるセキュリティ対策全体の底上げに繋がるものと考える。

7.3.　サービスごとの提供結果

7.3.1.　UTM

設置件数

29 社の申込みがあったが、実際に設置ができたのは 18 社であった。申込みのあった企業の内 2 社については導入後に不具合が発生し、導入後の取り外しを行った。

申込件数	未提供・提供不可件数	提供件数
29 社	14 社	15 社

表 7：申込み件数とサービス提供件数（UTM）

■導入後に取り外しを行った理由

・ 導入時は通常にインターネットが利用可能だったが、途中から利用不可になった。ヘルプデスクから指示を行い、再起動を試みてもらうと一旦不具合は解消されるが、一定期間経過後に再び利用不可となってしまう状態が発生。現地へ駆け付け調査をしたところ、原因は既設の上位ネットワーク機器の設定が影響していると推測されたが、調査のための保守ベンダーとの調整が難航したため、実証参加企業の判断として「業務影響を考慮し、即時取り外す」という結論となった。
・ 導入翌日に、インターネットが利用可能な端末と利用不可な端末がある、という問合せが入った。導入当日の試験ではその事象の報告は受けていなかったが、同一ネットワーク内で発生している事象であるという報告であったため、端末依存の可能性も想定し、切り分けのために訪問を打診した。しかし、業務優先をしたいという実証参加企業の判断で即時取り外しを行った。

■申込みがありながらも設置に至らなかった企業の理由

・ 実際に設置のために訪問したところ、既に別の UTM 機器の存在が判明した。
・ 訪問日の調整をするものの担当者が現業で多忙につき、日程の確定ができない。
・ 訪問日の調整をするもののコロナウィルスの影響で訪問を自粛してほしい、という要請があり、日程の確定ができない。
・ 最終的な上長の決裁が取れず、進めることができない。
・ 導入作業時のテストでは問題はなかったが、導入後になってインターネットが繋がらないという事象が発生。
    ① 現地での調査の結果、上位 NW 機器の設定との干渉が怪しまれたが、当該上位 NW 機器の保守ベンダーの協力を得られず調査を断念し、結局設置済みの UTM 機器を取り外した。
    ② 同じ部署の端末でもインターネットが使える端末と使えない端末がある、という状況であると聞き、端末依存の可能性が考えられたため、現地調査を打診したが、業務影響の解消を最優先するという判断のもと、UTM 機器の即時取り外しを指示された。

検知内容とその考察

UTM で検知したアラートは全てブロックしており、本実証期間内においてインシデントは発生しなかった。

検知数としては、社内にサーバー機器などを設置しておらず、更に設置期間も比較的短期間であるため検知数自体は多くないという結果であったが、それでもほぼ全ての業種において、フィッシングサイトのような不正な Web サイトや評価の低い（危険度が高い）Web サイトへのアクセスへのブロックが発生していた。

これらの不正サイトは近年巧妙さを増しているため、どのような業種・規模においても無意識にアクセスしまう状況が想定される。不正サイトへアクセスすることによる被害の拡大が考えられることから、重要情報の取り扱いはないと認識している中小企業にとっても UTM の有効性は訴求できるものと考えられる。

ちなみに、「その他」で検出した内容に関しては、内から内の不正通信を検出したものだが、詳細確認の結果、業務通信であることが推測され、過検知として判定している。

【アラート種別と検知内容】

No	業種	外部からの不正アクセス検知及び防御（外→内）	内部不正プログラム検知及び防御（内⇔外）	不正サイトへのアクセスブロック（内→外）	マルウェアの検知及び無害化	エンドポイントでのアラート検知	その他
1	A 農業・林業						2
2	L 学術研究・専門技術サービス業			6			3
3	S 公務（他に分類されるものを除く）			6			3
4	R サービス業（他に分類されないもの）			39	8		6
5	A 農業・林業			4			5
6	L 学術研究・専門技術サービス業			17			18
7	D 建設業			64			3
8	A 農業・林業						
9	E 製造業			47			4
10	D 建設業			14			5
11	L 学術研究・専門技術サービス業						
12	K 不動産業・物品賃貸業			4			
13	O.教育学習支援業			1			
14	R.サービス業（他に分類されないもの）			2			
15	Q.複合サービス事業			3			

表 8：UTM のアラート検知件数

アラート種別	概要
外部からの不正アクセス検知及び防御（外→内）	外部からの不正アクセス通信を検知・遮断し、バッファオーバーフローや 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及び防御（内⇔外）	ボットネットとの通信など、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→外）	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）
マルウェアの検知及び無害化	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ィルス、ランサムウェア、アドウェア等の検知と無害化
エンドポイントでのアラート検知	パソコン端末にインストールした EDR ソフト等で不正プログラムの検知や不正サイトへのアクセスを検知
その他	

表 9：UTM の検知アラートの種別

7.3.2. クラウド WAF

提供者数

30 社の申込みがあったが、実際に導入ができたのは 8 社であった。

申込件数	未提供・提供不可件数	提供件数
30 社	22 社	8 社

表 10：申込件数とサービス提供件数（クラウド WAF）

22 社については申込みがありながらも以下のような理由で導入に至らなかった。

■申込みがありながらも設置に至らなかった企業の理由

- 申込み後のヒアリング及び調査の結果、レンタルサーバーや CMS サービス等、現在の利用サービスの中で WAF 機能を有していて既に利用済みであった。利用可能な状態でありながらも未使用の場合は、有効化することを案内した。
- 導入時に、DNS 設定の設定追加やネームサーバーの変更、サブドメインの追加等、ユーザー側での実施が必要な作業があるが、以下のような理由でこれらの対応を実施してもらえない。
  ① 必要な設定情報を伝えても実施してもらえない。
  ② 設定ミスで不具合が発生し、影響の大きさから切戻しをして未設定状態。
  ③ ネームサーバーの変更も必要なケースでは、ネームサーバーの変更により当該 Web サイトのドメインと同一ドメインで稼働している他サービスへの影響の大きさや運用の手間を考慮し、導入を取りやめるという判断になった。
  ④ 既存運用への影響を小さくしながらクラウド WAF を適用させるためにサブドメインサイトの新規構築やリダイレクト設定が必要となったが、運用会社の協力を得られない事象や、継続的な運用への影響から経営判断として導入を取りやめた。

※一部の企業については、予期せぬ影響の発生を承諾の上で事務局側で設定変更を行い、導入した事例もある。

検知内容とその考察

クラウド WAF 側で有している検出ポリシーに基づき、Web サイトへの攻撃を合計 27,099 件検知してブロックをしたが、いずれの Web サイトも少なからず攻撃があった。
攻撃の種類を大別すると、「コマンドインジェクション」のような直接的な攻撃と「スキャナ/プロキシ/スパムボット検知」のような更なる攻撃に繋げるための偵察行為にあたるような攻撃があるが、偵察行為にあたる攻撃が大半を占める結果となった。

この偵察行為に関しては、もし当該サーバーに脆弱性があり乗っ取り等に成功されてしまった場合、踏み台として大企業へのサイバー攻撃や DDos 攻撃に悪用されてしまうと中小企業が被害者ではなく、加害者として求償される可能性すら否定できない状況にある。

そのため、直接的な攻撃を防ぐというクラウド WAF の有効性は当然ながら、偵察行為を防ぐという部分においても事業継続性の観点でも有効であるものと考える。

また、今回のクラウド WAF 導入の結果、以下のようなコメントもあり、間接的な効果もあったと考える。

■利用者コメント

・ 悪意のあるアクセス（攻撃）が可視化されることで具体的に知れて良かった。
・ こんなに海外からの不正なアクセスがあるなんて驚いた。海外からの利用は必要ないので海外からのアクセスを拒否したい。
・ たまたま被害に繋がっていないだけのはずなので恐ろしい。Web サイトに脆弱性があったら怖いので脆弱性検査をしっかり行いたい。

【検出ポリシーごとの検出件数】

検出ポリシー	概要	検出件数
コマンドインジェクション検知	ユーザーからの入力が OS のコマンド中の一部または全部として実行される場合、意図しないシステムコマンドが実行される脆弱性	144
ディレクトリアクセス検知	予想外のアクセス制限エリアについてのパス文字列を構成することができるようになってシステムの情報流出やサービスの障害を誘発する脆弱性	222
アプリケーション脆弱性検知	公開されているアプリケーションの各種脆弱性の情報によってホームページ改ざん及び攻撃経由地として用いられる可能性がある脆弱性	363
脆弱なページアクセス検知	ファイル名を推測してファイル名を見つけ出せることで、該当ファイルへ直接に要求してハッキングに必要なサービス情報を取得するような事象や、攻撃者の SQL インジェクションや総当り攻撃などの様々な形態の攻撃の口実を与える脆弱性	484
スキャナ/プロキシ/スパムボット検知	主要プロキシツール、ウェブ脆弱性スキャナ、スパムボットを使ったアクセスで脆弱性を収集する行為で、収集された情報から更なる攻撃の口実を与える脆弱性	23431

システムファイルアクセス検知	システムファイルや DB の重要テーブル等へ直接アクセスし重要情報やデリケートな情報を収集し、攻撃において必要な情報として用いられる脆弱性	306
HTTP メソッド制限検知	不要な HTTP メソッドを用いて悪意のあるファイルがアップロードされる事象や、重要なファイルが削除される可能性がある脆弱性	342
HTTP 異常リクエスト検知	セキュリティシステムを迂回するために、標準ルールに反するリクエストでウェブサーバーにアクセスする包括的な攻撃方法	857
エラーページクローキング	ウェブサーバーにカスタマイズしたエラーページを指定しない場合、表示されたエラーメッセージによって攻撃に必要な情報が流出される脆弱性	2512

表 11：検出ポリシーごとの検出件数

7.3.3. EISS

提供者数

84 社の申込みがあったが、68 社へ提供し、導入端末の合計数は 523 端末であった。

申込件数	未提供・提供不可件数	提供件数
84 社	16 社	68 社

表 12：申込件数とサービス提供件数（EISS）

16 社については申込みがありながらも以下のような理由で導入に至らなかった。

■申込みがありながらも設置に至らなかった企業の理由

・ パソコンへインストールしてもらう必要のある EISS エージェントを提供しても　インストールを実行してもらえない。
・ インストールが上手くいかない事象が発生した場合に事象解消のための情報提供を依頼しても、その情報提供の返答がなされない。
・ EISS が動作保証しているのが Windows OS のみとなっており、実証参加企業のパソコンが動作保証対象外の Mac OS であった。

アラート検知数とその考察

アラート種別	台数
セキュリティリスクはみられません。	408 台
セキュリティリスクの疑いがあります。	13 台
セキュリティリスクの恐れがあります。	100 台
合計	521 台

分析結果として「セキュリティリスクの疑いがあります。」「セキュリティリスクの恐れがあります。」というアラートが出た端末数は 113 端末であったが、いずれも詳細確認をした結果、過剰検知と判定しマルウェア感染をした端末の検出には至らなかった。

【過剰検知理由の例】

・ 通常の業務使用で発生したものであった。
・ 詳細確認の結果、攻撃の恐れとは断定できないものであった。
・ ユーザーが登録しているプログラム（プロセス）に依存した挙動であった。
・ 該当端末で使用中のセキュリティ製品によっては挙動が変わり、当該ケースでは攻撃の恐れまでには至らないと判断される挙動であった。
・ 当該端末のユーザーによる初期化時によるログと判明したため。

感染したマルウェアが動作した際の挙動は利用者が通常業務での使用状態でも発生し得ることから、一般的な中小企業ではその点の切り分けが難しく、専門的にチェックをして問題がないかを「潰す」という行為は有益なものだと考える。

また、検知ルールの一部に Excel 等のマクロが自動有効化されている場合に検知するようなものもあり、昨今大流行している Emotet のようなマクロを介したマルウェアへの予防対策としても役立つものであった。

また、今回は幸いにもマルウェア感染が認められた端末は発見されなかったが、実証参加企業からは以下のようなコメントもあり、間接的な効果もあったと考える。

■利用者コメント

・ マルウェア感染の「恐れ」をチェックしていくことで、日頃の意識付けになる点は非常に良かった。
・ 実際にマルウェア感染をしてしまった場合の対処が不安なので、バックアップや OS の最新状態のチェックなど、対策・準備を考えたい。
・ 日常的な業務上のパソコンの使用に際して、他にも危険なものがないか教えてもらうようなサービスになると良い。

7.3.4. 簡易セキュリティ診断

提供者数

60 社の申込みがあったが、47 社に対して診断を行った。

簡易セキュリティ診断については、Web アプリケーション診断とプラットフォーム診断を用意し、実証参加企業の要望に応じてどちらか片方もしくは両方提供をしたため、申込みをした企業数と提供件数が異なるものとなっている。

診断の種類	申込件数	未提供・提供不可件数	提供件数
Web アプリケーション診断	45 社	12 社	33 社
プラットフォーム診断	31 社	8 社	23 社

表 13：申込件数とサービス提供件数（簡易セキュリティ診断）

Web アプリケーション診断	ブラウザで閲覧・利用する Web アプリケーションに関して XSS（クロスサイトスクリプティング）や SQL インジェクションのような脆弱性がないかを検査する。
プラットフォーム診断	ネットワーク機器や OS、サーバー、ミドルウェアに脆弱性がないか、設定に問題がないかを検査する。

表 14：セキュリティ診断の種類

脆弱性の検出内容とその考察

診断内容・対象を絞った形での簡易診断でありながら危険度の高い脆弱性が検出された結果となったため、範囲を広げて実施すると更に脆弱性が検出されるものと推測される。

診断結果については、実証参加企業へ報告して改善対応を促し、考えられる危険性や修正方法などについて質疑応答の対応をした。

【Web アプリケーション診断】

■検出した危険度毎の企業数

緊急	1社
高	1社
中	15社
低	16社

■検出した脆弱性項目と数量

緊急	脆弱性を含む製品の使用	1件
高	SQLインジェクション	1件
中	平文通信	18件
	クロスサイトスクリプティング	12件
	セッション管理不備	14件
	クロスサイトリクエストフォージェリ	7件
	メールヘッダーインジェクション	1件
低	セキュリティ設定の不備	153件
	過度な情報漏えい	35件
	クロスサイトスクリプティング	30件
	不適切なエラー処理	14件
	脆弱性を含む製品の使用	10件
	セッション管理不備	2件

表 15：脆弱性の検出結果（Web アプリケーション診断）

直接的な攻撃に繋がるものではなく危険度はさほど高くないと判断されるものになるが、ほぼ全ての Web サイトにおいて、「セキュリティ設定の不備」が認められた。

実証参加企業が公開する Web サイトのほとんどはクラウド上に構築されているが、クラウドサービスには AWS（アマゾンウェブサービス）の責任共有モデルが例になるような、利用者自身の責任の下でケアしていく必要がある範囲があり、この「セキュリティ設定の不備」に関わる部分もそういた範囲に含まれるものが多く含まれるため、開発者側に一定の知識・意識が身についていれば安心・安全に使用することができるが、実態としてあまりそこまでの対応には至っていないことが判明した。

また、最も危険度が高い「脆弱性を含む製品の使用」に関しては、既知の脆弱性が報告されている古いバージョンの Bash シェルを使用しているために検出されたものであったが、早々に修正をするように提案をした。

【プラットフォーム診断】

■検出した危険度毎の企業数

緊急	3社
高	4社
中	11社
低	6社

■検出した脆弱性項目と数量

緊急	アプリケーションのバージョンがサポート切れ	5件
高	アプリケーションの脆弱性	42件
中	証明書の不備	23件
	不要と思われるサービスポートの開放	19件
	アプリケーションの設定不備	2件
低	弱い暗号化プロトコルの使用	32件
	非暗号化プロトコルの使用	3件

表 16：脆弱性の検出結果（プラットフォーム診断）

危険度の高いものとして、「アプリケーションのバージョンがサポート切れ」が検出されたが、UNIX や FreeBSD といった OS 及び PHP などのミドルウェアに関して、既にサポート切れになっているバージョンで利用している状況があった。企業によっては、バージョンアップの必要性を知っていながら運用上の理由で意図的にそのままの状態にしてあるケースもあるが、確認をしたところ無意識に古いままの状態で使用している状況であったため、この基礎的に重要な対応に関して定期的にフォローする伴走的なサービス・支援のニーズもあるものと推測する。

また、全般的な傾向として、比較的規模の大きい企業と比べると「不要と思われるサービスポートの開放」の検出が多くなっている印象があり、中には管理画面まで到達可能な状態になっているケースもあり、パスワードリスト攻撃などのブルートフォースアタックをされると即時不正ログインを受ける可能性があるものも検出された。

7.3.5. ヘルプデスク・駆け付け対応

対応件数

事務局およびヘルプデスクには専用の電話番号とメールアドレスを用意し、相談窓口として対応を行った。

【対応種別と件数】

対応種別	総計	相談・インシデント等対応状況	件数
事務局 コールセンター対応	24 件	セキュリティ機器設置等の問合せ	8 件
		セキュリティ対応の相談	34 件
		その他	14 件
インシデント対応	0 件	電話及びリモートによるインシデント対応	0 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	19 件	機器設置等のトラブル対応	3 件
		その他（セキュリティ機器の導入・設置支援等）	21 件

表 17：問合せ対応種別と件数

対応事例

提供サービスに関しての問合せがほとんどであったが、導入後になって初めて対応の必要性が判明したものや実証参加企業側の「気のせい・勘違い」という内容もあった。

【問合せ例】

■セキュリティ機器設置等の問合せ

① UTM 導入後にメールが送れなくなった。
② UTM 導入したらインターネットが遅くなった気がする。
③ UTM 導入後に今まで閲覧できていたサイトが閲覧できなくなった。
④ UTM 導入後にデータのダウンロードができなくなった。

■セキュリティ対応の相談

① 診断結果の見方、アラート通知内容の見方について教えてほしい。
② 診断結果に対する修正方法の相談
③ 各サービスの必要性に関する質問

■その他

① 仮に Emotet に感染してしまった場合の対応について
② Emotet に感染したことを調べる方法について
③ 診断時にメールがたくさん届くけど問題ないのか。
④ DNS の設定方法について教えてほしい。
⑤ EISS のインストールが上手くいかない。

【駆け付け対応例】

機器の導入・設置以外に以下のようなトラブル対応で駆け付け対応を行った。

① UTM 導入後に正常動作していたものが、インターネット接続不可となった。エンジニアが駆け付けて現状を確認したところ、上位に別の社内ネットワーク環境が存在し、そちら側の設定と干渉をしている状況が判明。

<対応>

解消へ向けて上位ネットワークを管理しているベンダーへ連携するも、調整が難航したため、UTM を抜線して切り離しをし、UTM 導入前の状態に切り戻した。

② UTM 導入後に社内サーバーへのアクセスがタイムアウトする、という報告を受け、エンジニアが駆け付けて現状を確認。

<対応>

対象サーバー宛の通信は UTM 機能をバイパスするように設定変更を行い解消。

7.4. その他、実証参加企業へのヒアリング内容

アンケートへの回答とは別に個別訪問や問合せなどのやりとりの中でヒアリングした意見・感想を記載する。

- 実証へ参加したことをきっかけにセキュリティ対策への関心や意識付けができたと思う。社員への教育も検討していきたいと思った。
- 攻撃が可視化され、実際に攻撃を受けていることが認識できて良かった。他人事ではないことが分かったが、他社がどうなのかが気になりだした。
- こんなに不正通信（攻撃）が多いものとは認識していなかった。海外からこんなに来ているのには驚いた。
- 既存の保守ベンダーへの連絡等、調整事が多くて大変だった。たらい回しされた感じもしたので、極力 1 つの会社に全部対応を任せたい。
- システム開発会社だが、技術要素が全く違うため、この脆弱性はきっと自社では検出できなかったので非常に助かった。今回は簡易診断だったが、きちんとした形の診断を受けることも検討したい。
- ウィルス対策ソフト以外の対策があることを知れて良かった。
- 丁寧に説明をしてくれたはずだと思うが、導入時の説明が専門的過ぎて難しかった。これは自分達だけなのか。やはり社内に専門担当を置く必要性を感じた。
- 無償期間が短く、効果が分かりにくかったので、もう少し長い期間で効果を見たかった。
- 何かあった際の相談先になるので、沖縄県内にこうしたサービス提供者がいることが心強くて安心感がある。
- こうしたサービスが無償で受けられるのは良いが、無償期間が終わった後の金額がどの程度になるかが気になる。中小企業が捻出のできる価格帯だと良いが。
- 最終的には各企業で決める必要あることは頭では理解しているが、参考としてだけでも対応すべき対策の順序をはっきり示してほしい。

7.5. サービス提供上の課題考察

サービス提供全体を通して、散見した事象や挙がった意見などから、それぞれのサービスに対する課題をまとめると以下のとおりである。

サービス	コメント・課題
UTM 機器設置	自社 NW 環境に関する情報不足があり（把握している技術担当が社内に乏しい)、その影響から現地調査に時間を必要とする場合や、設置後の想定外の挙動が発生する。
	多くの企業にとってはレポート内容が難解であるため、レポートの分かりやすさ向上が必要。
	物理的な環境や業務、使用しているアプリケーションなど、企業によって個別の要求事項があり、デフォルト設計で導入ができず、独自設計／設定を必要とするケースが少なくなく、初期導入時の作業量が大きくなる。
クラウド WAF	ネームサーバーや DNS 設定変更といったどうしても必要な利用者側の作業があり、利用者側のスキルによっては作業協力が得られない。
	設定変更方法に関して一般的な方法は案内できるが、利用サービスによって異なるため具体的な案内が困難である。
EISS	ウィルス対策ソフトとの違いを認識してもらうのに苦労した。
	レポート受領後の対応が分かりにくい、何をしたら良いか分からないという声があり、その後の推奨対応まで示す必要がある。
	エージェントをインストールするのであれば、マルウェア感染以外に、バージョンアップが必要なものなど、予防のために有効な通知が拡充されると良い。
	エージェントインストールがハードルになっている状況もあったので、より簡単に専門知識が一切不要で無意識に導入できるものが望ましい。
簡易 セキュリティ 診断	サーバーやサイトの保守管理会社から許諾してもらえないので、入口を下げるために許諾を不要とするレベルの簡易診断にする。
	診断結果に応じた修正対応までカバーするプランが望ましい。

表 18：サービスごとの課題考察

いずれのサービスも Web サイト・システムやネットワーク等の情報セキュリティ以外の一定の知見を必要とするため、それに対応できる人員体制が整備されていないとスムーズな導入が難しい状況であった。一方、社内に不在であっても外部ベンダーとアウトソーシング契約をする形で人員体制が整備されている場合もあるが、その外部ベンダー自身が情報セキュリティに関する理解・知識が乏しい状況だと同様にスムーズな導入は困難であった。

また、一般的に Web サイト・システムとネットワークの分野は畑違いであるため、双方の知見を有した人員が配置された人員体制を構築できる中小企業は稀であることが考えられるため、そうした企業に対してはセキュリティベンダーが包括的な支援を行うサービスが有効なものと考えられる。

8.　セキュリティ簡易保険サービスのあり方について

本実証事業を通じて得た情報をもとに検討委員会を開催し、中小企業が利用しやすいセキュリティ簡易保険サービスの内容や定着のためのマーケティングについて検討をした。

サイバー保険自体の課題としては、その認知度の低さ、導入手続きの煩雑さ、価格の大きさ・不透明さが考えられるが、認知度については本実証事業の結果からも推測できるため、その必要性とともに認知度を上げることが最優先事項であると考える。

次に、導入手続きの煩雑さについては、現在は告知書の内容が簡略化された保険商品も開発しているが、それでもなお煩雑である印象は払しょくできていない。その点においてもセキュリティ対策サービスに保険が自動附帯される形が望ましいと考える。

しかしながら、自動附帯保険はその特性上、補償金額が大きくできず、更にセキュリティ対策サービス提供社側の観点からすると、持続可能で低価格なサービスの実現を優先に考えると保険の発動条件や補償金額は限定的にせざるを得ない。

そのため、大きな補償を得ることに主眼を置かず、インシデント検知から初動対応までをシームレスでスピーディーに行うことを目的としたものにすることが理にかなっているものと考える。具体的には安心感を得るための駆け付け対応費用の他、沖電グローバルシステムズの通常業務においても比較的頻繁に相談があるウィルス駆除といったところが候補になるものと考える。

また、この自動附帯されるセキュリティサービスの保険料の負担はセキュリティ対策サービス提供事業者となるため、仮に自動附帯されたサービスを提供した際に利用ユーザーのうち 1 社でも多大な費用の掛かるインシデントが発生してしまった場合は翌年度以降に負担する保険料金が大幅に上がることになり、結果的にサービスとしての収支を圧迫し採算が取れずに、安価なセキュリティ対策サービスの提供がストップしてしまう状況に陥ってしまうことが考えられる。このような状態は、自動車の自賠責保険のように半ば強制的に加入させるような制度を設けることができれば回避できる可能性はあるはずだが、現状は困難である。ただ、このセキュリティ対策サービスが安定的に提供できなくなってしまう状況は双方にとって望ましいことではないため、まずはサービス加入条件や免責事項を事前に明確にすることが肝要であると考える。

一方、サプライチェーンリスクという観点では、上位サプライヤーにセキュリティ対策サービスの費用の負担を望む声もあり、上位サプライヤーからは一定の負担は仕方ないという声も上がっており、そういった意味でも下位サプライヤーのために上位サプライヤーが加入するサイバー保険商品の造成もサプライチェーン全体の対策強化に繋がるものと考える。

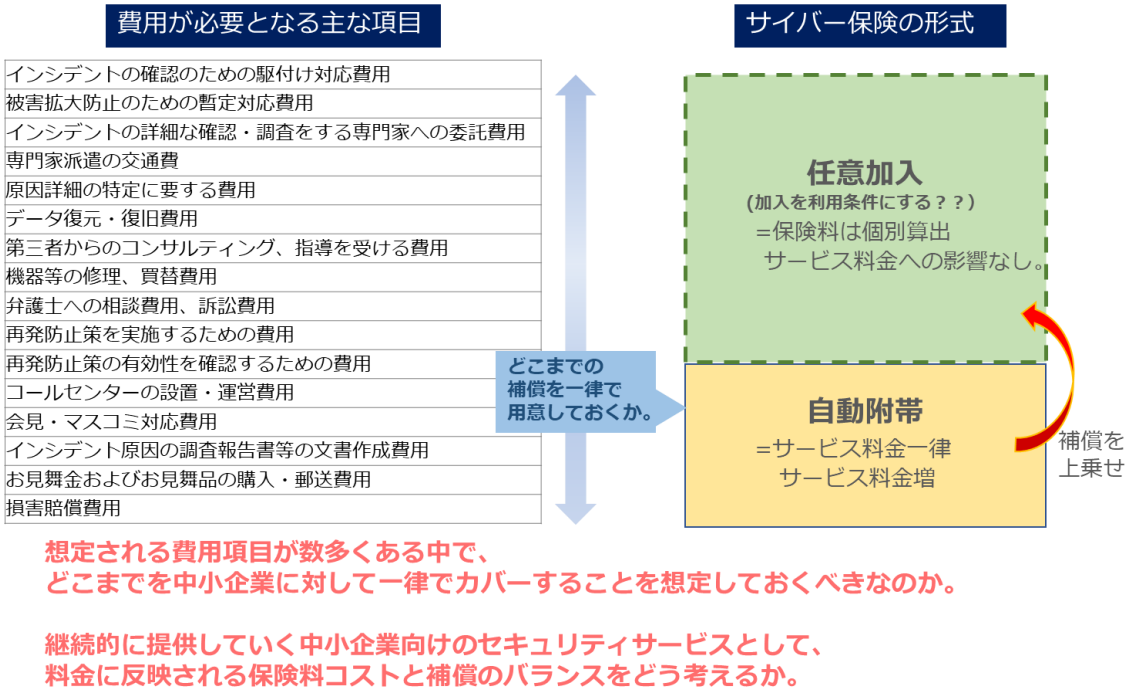
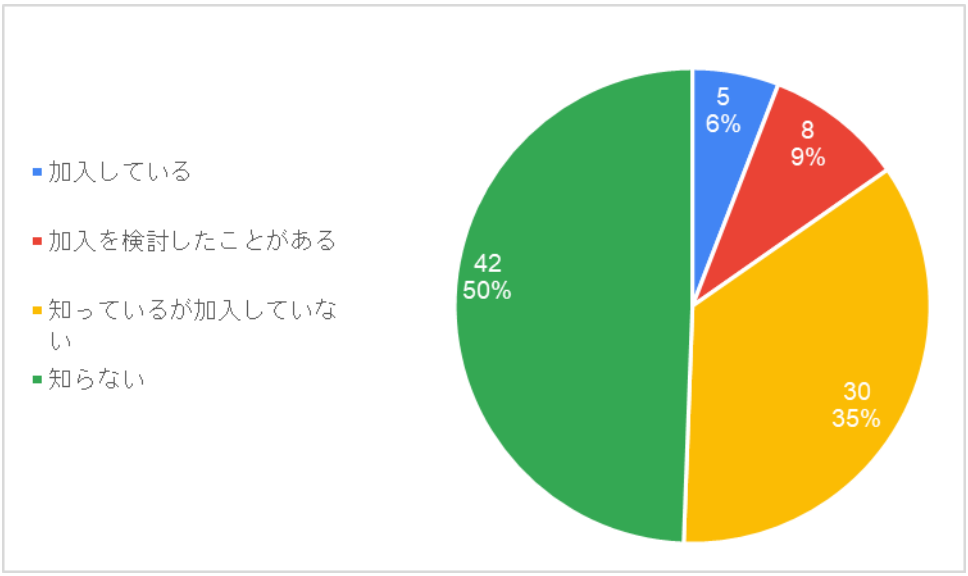


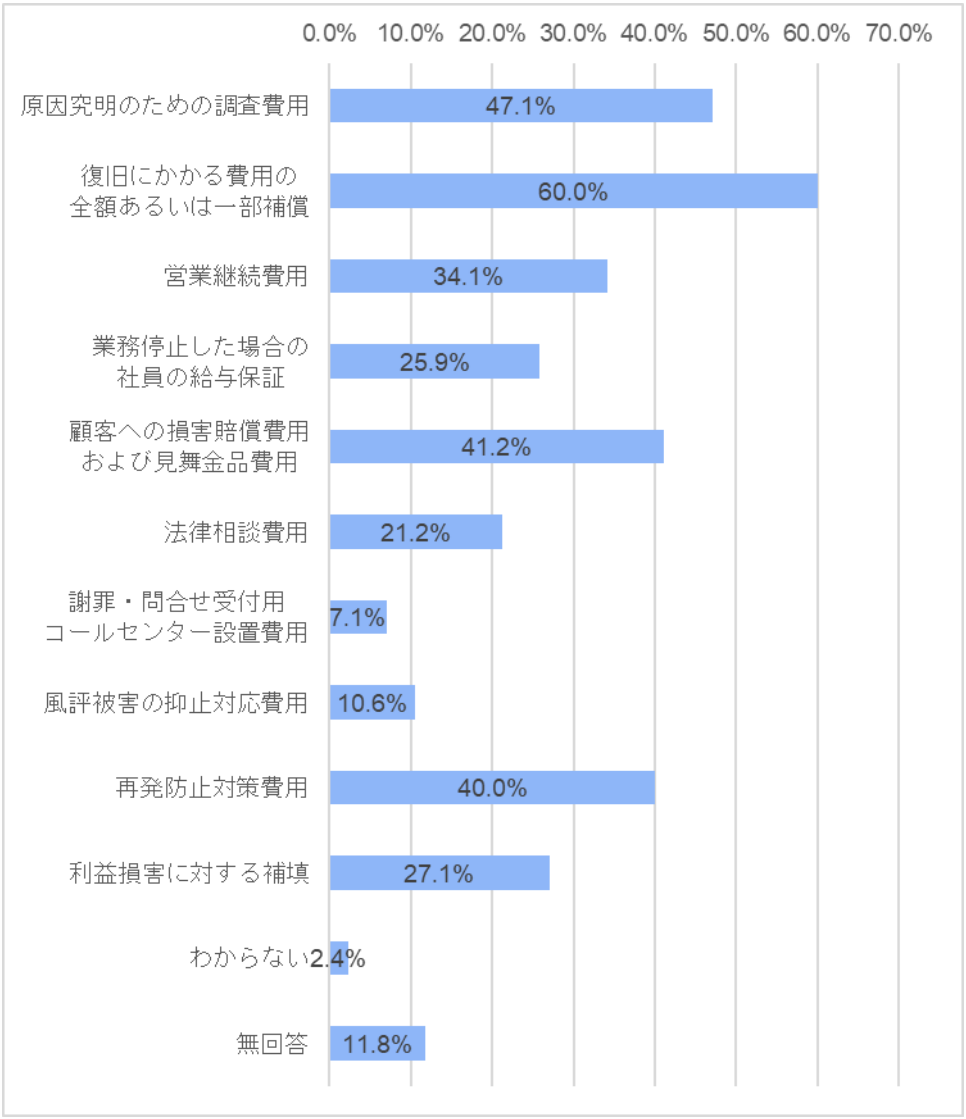
図 55.サイバー保険の自動附帯の考え方

図 56. サイバー保険に加入していますか？ （n=25）



考察：半数がサイバー保険を認知しておらず、普及が先決な状況

図 57. サイバー保険の補償として必要だと感じるものは何ですか？（複数回答）　（n=25）



考察：コストは掛けられないと考えている中でも復旧や再発防止など、事業継続のための補償へのニーズは高い。

9.　本実証事業の結果を踏まえた中小企業向けセキュリティ対策サービスについて

9.1.　中小企業に必要な対策の考察・提言

課題の再確認と解決へ向けた方向性

ここで改めて中小企業の実態から導き出された課題と課題解決へ向けた方向性の整理をする。

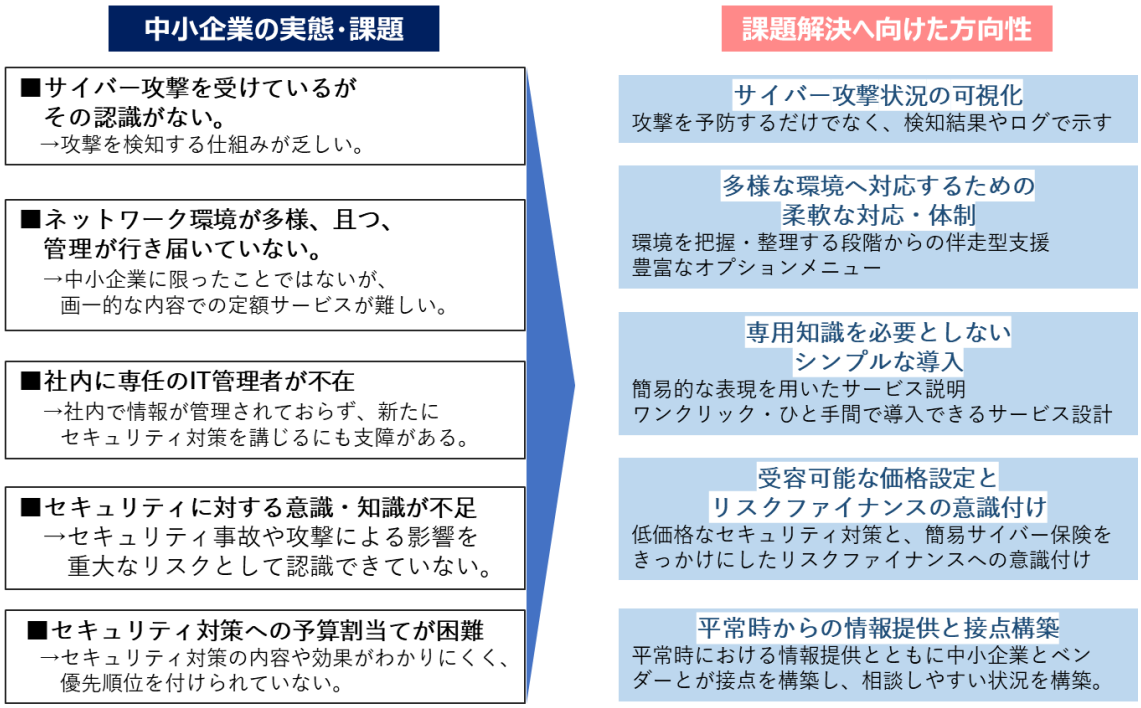


図 58.課題と課題解決の方向性

中小企業に必要なセキュリティ対策と政府への要望

本実証の結果を踏まえ、中小企業に必要なセキュリティサービスの方向性に対する考察と政府への要望を提言する。

【中小企業に必要なセキュリティサービスの方向性】

■価格

アンケートの結果から中小企業の大部分が受容可能な価格帯として月額１万円～３万円といった価格帯だと考えられる。ただし、同時にサービス提供側の採算性も確保する必要があるため、標準で提供するサービスはある程度制限されたものにせざるを得ず、その代わりにオプションサービス等を設け、不要なものが排除された必要なサービスのみを選択できるようにすることが望ましい。

■サイバー保険によるリスクファイナンス

100%安全とは言い切れるような万全な対策が存在しない状況下において、サイバー保険によりリスクファイナンスを講じるのが有効な手段と言えるが、中小企業の企業体力や検討の手間を考慮すると、ある一定の補償の範囲で自動附帯している状態が望ましい。

しかしながら、この補償の範囲の設定はサービス提供側の採算性に影響を与え、継続的なサービス提供を見据えると慎重に設定すべきである。

■平易でシンプルな表現

「ウィルス対策ソフトは、パソコン側で指名手配犯の写真を持っていて、入ってきた人の顔を 1 つ 1 つ写真と見比べ指名手配犯を侵入させないようにするようなものです」というように中小企業がインプットする情報は、可能な限り平易な表現を駆使した形でのサービス説明や疑問を増やさないようにシンプルな表現に留め、実施してもらいたいアクションは具体的に 1 つ 1 つコマ切れにしてアナウンスする等、専門用語を減らすことを意識することが望ましい。

■導入／手続き

各セキュリティ対策の目的や効果について中小企業が理解しやすくするために、その機能やコンセプトをシンプルにする工夫が必要である。

また、セキュリティ対策によって導入手続きが異なるのは致し方ないが、それにより中小企業側の作業も増えるため、理想的なのはオールインワン型・ワンストップ型のサービスであるが、可能な限り導入手続きが少ないようにする工夫が必要である。

■セキュリティリスクの可視化

セキュリティ費用対効果やリスク認識させるとともにセキュリティに対する意識を高めるために管理画面や定期的なレポート、アラートなど、サイバー攻撃を受けている状況を可視化する機能があることが望ましい。

■サービス領域

企業のネットワーク環境の構成管理や事前調査、リスクアセスメントなど、セキュリティ対策を講じる前の段階から支援に入り、そこから実際のセキュリティ対策の提供とその後の運用まで付き合う伴走型の支援が必要だと考える。

本実証においても「沖縄でこうしたセキュリティ対策サービスを提供している企業があると安心」という声もあったように、この伴走型支援に関しては、顔が見え気兼ねなく相談ができて、中小企業も安心できる地域のベンダーが担うことでより効果が高まるものと考える。

■平常時からの接点構築

セキュリティに対する意識や情報不足を補うためにも平常時からの情報提供が必要で、更にインシデントが発生して初めて問合せをして対応が走るという状況である場合はスムーズな対応が難しいことが予想される。

伴走型支援の効果を最大限にするためにも中小企業とサービス提供側は平常時から接点を持っておくことが望ましいと考えるため、まずは簡易的なサービスからでも利用してもらい地域内で

の接点を広げることで、地域全体のセキュリティ対策強化の足掛かりなるはずである。そういった意味で「サイバーお助け隊」ブランドは非常に有効的であるものと考える。

■免責事項の明確化と読み合わせ

中小企業向けには伴走型支援としてより一歩踏み込んだ支援が必要となるが、サービス提供社側の過失によりネットワークの停止やアプリケーションの動作不良といった中小企業への不都合が発生する可能性は排除できない。または、精一杯支援をしても要望に応えられないケースも考えられる。そうした場合のために免責事項を明確にし、すり合わせをすることで事前にトラブル回避を行い、双方安心して伴走型支援が進められるよう準備をすることが望ましい。

【政府への要望】

■セキュリティ対策を講じることのメリット

「セキュリティ対策コストは投資コストにならない」という意見も出てきている状況がある。既に SECURITY ACTION の宣言が IT 導入補助金の申請における必須要件となっているが、それ以外にも税制面や調達時の優遇など、セキュリティ対策を講じることが企業の業績やビジネス面に対してプラスに働くような施策を講じてはどうか。

これが浸透することでサプライチェーン全体のセキュリティ強度も高まり、ひいては産業全体の強化に繋がるものと考える。

■セキュリティインシデント被害状況に関する情報開示

ニュースで公開されるようなセキュリティインシデントは有名企業のものばかりであるため、中小企業の多くはまだ他人事のように受け取っている。自社や競合他社、同規模企業でセキュリティインシデントが発生したことがセキュリティ意識を芽生えさせるきっかけになるため、中小企業の事例を数多く情報開示してはどうか。

インシデント発生時の対応費用や損失額はもちろん、インデントが発生してしまった中小企業を追跡調査することによる現在の状況等、中小企業のセキュリティ意識を高めるには非常に魅力的な情報になると予想されるため、現在の力を入れている SECURITY ACTION の周知活動と並行するとより効果的なものになると考える。

■中小企業のコスト負担の軽減措置

既に様々な補助金が存在する状態ではあるが、例えば IT 導入支援金の補助対象にセキュリティ対策サービス・製品を拡充してはどうか。

中小企業においてはその企業ごとの個別要件があり、初期導入に手間取るケースが少なくないが、極小企業に関してはそうした個別要件が少なく手間が少なく導入可能なケースも多い。また、例えば UTM 等はパソコンやタブレットと同等金額で購入できるものも存在しており、コスト負担が小さくなれば導入件数も増えるものと推測する。

9.2. 今後のビジネス化の見通しについて

本実証終了後は、実証事業を通じて得た知見や構築した体制を活用し、沖電グローバルシステムズ株式会社が主体となり、株式会社セキュアイノベーション、ファーストライディングテクノロジー株式会社と連携し、『沖縄サイバーお助け隊サービス』として継続的なサービスの提供を予定しており、既に本実証事業の実証参加企業から数件の継続依頼が入ってきている状況である。

提供予定のサービスの内容について

【1】UTM 監視運用サービス

■概要：

- UTM 機器のレンタルと運用監視サービスをセットにしたサービスで、UTM 機器は利用者の事業規模に応じてスペックは変動させる。
- UTM からの監視ログはクラウド上の SOC 基盤で自動収集し、その内容を分析し、　　検知結果の通知を行う。
- アラート通知に関しては、中小企業の負担軽減を考慮し、SOC 側で一旦精査をし、対応が必要になると判断したもののみを通知する形を取る。
- その他、ログ保管（1 ヶ月）やバージョンアップ対応といった対応も含める。

■提供料金：

- 最低料金を初期料金 10,000 円／月額料金 10,000 円で設定。
- この金額内で UTM 機器レンタルと標準運用を提供する。
- UTM 機器のスペックや運用作業のオプション付与で料金変動していく形を取る。
- 初期料金については、導入時に必要な作業が異なってくるが、オプションとして対応をしていく。

【2】クラウド WAF

■概要：

- （株）セキュアイノベーションの「secuWAF」を提供する。
- 利用者は管理画面から攻撃状況の確認や簡易的な WAF ポリシーの変更も可能。
- 上位プランでは簡易改ざん検知機能を標準提供し、改ざんされ悪意のあるスクリプトを埋め込まれて加害者になってしまうような攻撃への対策も行う。

■提供料金：

- WAF を経由する総トラフィック量に応じたプランになっており、10GB／月間で初期料金 0 円／月額料金 10,000 円で設定。
- 上位プランは 15,000 円（20GB）、30,000 円（50GB）というような価格帯で提供。
- 通常プランでサイト入れ放題になっており、低価格で複数サイトの保護が可能。

【3】EISS（アイズ）※簡易 EDR

■概要：

・（株）セキュアイノベーションの「EISS」を提供する。
・ウィルス対策ソフトと併用して利用することができる簡易 EDR。
・クライアント PC へインストールした EISS エージェントが定期的にクライアント PC における操作や生成ファイルなどのログ情報クラウド上へアップ。
・クラウド上の EISS 基盤にてマルウェアが感染した際の挙動との類似性を分析し、マルウェア感染が疑われる端末を通知する。
・現在はマルウェア感染の疑いのみを通知するものだが、今後はソフトウェアのバージョンチェックなど PC 自体の利用状態のチェックも加えていく予定。

■提供料金：

・1 端末あたり年間 1,800 円の価格を設定し、5 端末からの利用が可能。
・標準的なメールサポートは附帯しているが、ウィルス駆除やログ保管期間の延長、デジタルフォレンジックなどは別オプションとしており、導入のハードルを下げている。

【4】簡易セキュリティ診断

■概要：

・Web アプリケーション診断（5 画面まで）とプラットフォーム診断（グローバル IP1 つ）を用意し、どちらかを選択してもらう。
・再診断や診断報告会は含まないが、診断結果に対する問合せ対応や修正対応に関する質疑応答といった診断後フォローまでを提供する。

■提供料金：

・1 回 100,000 円で設定。
・診断対象を増加や再診断、診断報告会などは別オプションで提供。

サイバー保険の自動附帯について

サイバー保険の自動附帯に関しては検討をしているが、現時点では補償内容や条件を確定できておらず、提供料金への影響も小さくないことから附帯させていない状況である。

ただし、（株）セキュアイノベーションがサイバー保険の募集人資格を有しているため、サイバー保険の任意加入についてはセットで提案を行う。

ビジネス化・拡大に対する課題

既にビジネス化の決定はしているが、並行して検討・対応を進めるべき課題を記載する。

■セキュリティ対策の重要性についての啓発

中小企業の多くは実害に直面していないため、その重要性をまだまだ理解していない。そのためビジネスへの影響やリスクといった危機感を醸成するような観点からの情報提供を強化するなど、

サイバー保険も含めたセキュリティ対策の効果を啓発していく必要がある。

■「サイバーお助け隊」の地域での認知度向上

潜在的に困っている中小企業も存在していることが予想され、本実証の中でも「地域にこうした支援体制・サービスがあると助かる」「こうした企業があることが知らなかった」というようなコメントもあり、地域にこうした体制があることの認知度を上げていくことで一気にビジネスが拡大する可能性がある。

■申込企業の環境状況の把握と、それに伴う初期導入費用・サービス条件の設定

企業ごとにネットワーク環境や利用状況が異なるという実態がある中、それをどのように把握するか、という点がサービス提供側の初期導入時の稼働を抑えるためには非常に重要な要素である。

『都度見積』を極力減らすことが利用者獲得に繋がるのは明らかであるため、初期導入費用を定額にしていくための条件・ルール作りが必要となる。

■アラート内容やサービス説明などついて平易な言葉での説明・表現

本実証の中でも度々意見が挙がったが、専門用語を極力用いない形での説明や案内が必要。難解な表現はそれこそがセキュリティ対策への関心を削ぐことに繋がるため、テキスト内及び口頭での表現を簡易にしていくことが非常に重要である。

■サービスの拡充（バックアップやウィルス駆除などのオプションサービス）

企業ごとに多様な要求があり、発生するインシデント自体が多様なこともあるが、 オールインワンのサービスにしてしまうと、どうしても高額な利用料金の設定になってしまうため、オプションプランを明示しておくことが望ましいと考える。

今後提供していくサービスとの連携においては、バックアップサービスやリストアサービス、ウィルス駆除といったサービスの必要性を考えているが、中小企業の多様な状況を想定すると、それ以外のサービスメニューの検討も必要である。

■サイバー保険の自動附帯

利用者側の利便性からサイバー保険の自動附帯の効果は当然認められるものだが、任意加入の場合の保険料負担者が利用者側になるのに対し、セキュリティ対策サービスへの自動附帯とした場合はそのサービス全体に掛かるため、その保険料はサービス提供社側のコストに組み込まれ、採算性に影響するものになる。

そのため、保険事故が頻発されないようにするとともに、採算性を継続的に保てる形で保険の補償範囲と発動条件を策定しなければならないが、厳しく設定をしてしまうと補償内容が足りず、せっかくの保険が形式的なものになってしまうため、慎重に設定をしていく必要がある。

10. まとめ

中小企業が抱えるセキュリティ対策への課題はある程度事前の想定のとおりであったが、特にセキュリティ人材の不足は深刻である。セキュリティ人材が存在していれば、比較的安価なコストである程度の対策を講じることも可能となり、様々な検討も可能になるが、その課題解決が困難な状況もあり、何かあった際に相談ができる、駆け付けてくれる体制といったその地域内の第三者のサポートは必要不可欠なものだと考える。

本実証を通じた結果として、「8.本実証事業の結果を踏まえた中小企業向けセキュリティ対策サービスについて」でサービス提供社側の課題とは別に政府への要望を示したが、セキュリティ対策サービスを提供する民間企業として解決していくべき道筋が見え、それを前進させる必要があるのは当然なことながら、一方、中小企業に置かれている現状においては、まだまだ民間主導だけでは困難な部分も残っており、そうしたことから政府の協力との両輪で推進していく必要があるものと考える。