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：香川県）

成果報告書

請負事業者：高松商工会議所

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、高松商工会議所が「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。
香川県内の中小企業70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）
- 標的型攻撃メール訓練

2. 背景・目的

2.1. 背景

近年、サプライチェーン全体の中で対策が弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化している。

今年度に入り、 NEC、三菱電機等が高度なサイバー攻撃を受けていたことが明らかとなったが、サイバー事案に対する社会的関心は非常に高く、これへの対応は、ステークホルダ等とのコミュニケーション等を間違えると会社の経営そのものに深刻な影響を与え得るという意味で経営問題そのものである※とされている。

昨年度の「中小企業向けサイバーセキュリティ事後対応実証事業」（以下、「昨年度事業」と言う。）では、地域・企業規模に関わらず、中小企業もサイバー攻撃の対象となっていることが判明した。多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも発生している。

※経済産業省「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取り組みの方向性について」

2.2. 目的

これらに対応していくためには、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定着させていく必要がある。

私ども高松商工会議所は、地域の総合経済団体として、本実証事業において、高松を中心とした香川県内の中小企業のセキュリティ向上を図っていきたいと考えている。

3. 実証事業の概要

3.1. 実証対象の選定

実証地域⇒高松市を中心とする香川県内

香川県とは･･･

- 香川県は四国の玄関口であり、全国の企業の支社・支店が所在する
- 四国の中心都市（四国 4 県の県内総生産のうち人口当たりの金額は 4 県で最も高い）
- 「卸売業、小売業」など第三次産業事業所が全体の 80%超
- 売上高においては、「卸売業、小売業」に次いで「製造業」が多い

高松市とは･･･

- 香川県の県庁所在地であり、県内人口の約 44%を占める
- 県内の事業所数の約 47%が同市内に集中しており、県内の経済の中心地
- 卸売・小売業が全事業所数の 27.5%、宿泊・飲食サービス業が 12.1%と、県全体の産業構造と似通った業種割合

四国の経済の中心地である香川県において、その中核である高松市を中心とした地域は、サイバーセキュリティ対策の必要性が高い地域と考えられる。

個人情報等の機密すべき情報が多い業種が多く所在していることから、実態を早期に把握し、不足している部分への対策も急務と言える。

また、県全体の産業構造と似通った業種割合であることから、高松地域の結果を県下全域に応用して考えることもできる。そして、四国経済の中心市であるからこそ、四国全体のサイバーセキュリティの実態を見通すための土台となるデータ※として応用できると考える。

※高松商工会議所にて確認する限り、高松市、香川県、四国における中小企業のサイバーセキュリティに関する先行研究は無い。

3.2. スケジュール

事業期間：2020 年 9 月 8 日～2021 年 1 月 25 日

実証期間：2020 年 10 月 1 日～12 月末日

	事業全般 （高松商工会議所）	UTM （キヤノン MJ、NTT）	標的型メール訓練 （STNet）
8 月 28 日（金）	参加事業所募集開始・事業広報		
9 月 1 日（火）	高松 CCI HP にて事業内容等掲載		
9 月 8 日（火）	プレスリリース		
9 月 12 日（土）			
9 月 13 日（日）			
9 月 14 日（月）			
9 月 15 日（火）	説明会開催 セキュリティ対策状況・意識等調査		
9 月 16 日（水）		⑥設置前調査・設置	⑦訓練実施打合わせ
⋮		↓	↓
9 月 30 日（水）		↓	↓
10 月 1 日（木）		実証	訓練実施
⋮		↓	↓
12 月 25 日（金）		↓	↓
⋮		↓	↓
12 月末日		↓	↓
1 月 5 日（火）		レポート提出（報告会前）	レポート提出（報告会前）
1 月 8 日（金）			
1 月 13 日（水）	報告会開催 実証後アンケート・意識調査		
⋮			
1 月 25 日（月）	事業成果報告書提出締め切り日		

3.3. 実証参加企業

説明会等による参加企業の募集を実施（表 1）

対象：高松市内を中心に県内に本社・支社等を構える中小企業	
日　　時	9 月上旬
場　　所	高松商工会議所会館（高松市番町二丁目 2 番 2 号）
回　　数	1 回以上
実施内容	① SECURITY ACTION および中小企業の情報セキュリティ対策ガイドライン 8 の普及に向けた周知啓発活動および活用促進に向けた必要なフォローアップを実施。 ② 簡易のセキュリティ診断（「5 分でできる！情報セキュリティ自社診断」またはアンケート）を行い、参加企業の現状のセキュリティレベルを把握する。
備　　考	① 開催にあたって、あらかじめ開催概要や開催スケジュール等を含む実施計画を作成し、IPA との協議により決定する。また、チラシを作成の上、参加企業を募集。 ② 新型コロナウイルス感染症の感染防止の観点から、必要に応じて、オンラインでの説明会を行う。
対象：高松市内を中心に県内に本社・支社等を構える中小企業 特に前述の説明会への参加企業	
日　　時	9 月上旬まで
手　　法	チラシを作成の上、 ① 高松商工会議所会員のメーリングリスト先への送付（2984 事業所） ② FAX 等での案内（104 事業所） ③ 高松商工会議所経営指導員による巡回 ④ プレスリリースを実施 掲載：9 月 16 日四国新聞 9 月 25 日ビジネス香川ホームページ https://www.bk-web.jp/post.php?id=2050 10 月 1 日ビジネス香川誌面※ホームページと同様
募 集 数	50 社以上（70 社目標）
理　　由	① サイバーセキュリティのレベルに応じた検証を行う最低ロットの想定 UTM：40 社分、標的型訓練メール：30 社分 ② 実証事業終了後への継続性 「実証事業期間のみ機器を設置しただけ」とならないよう、実証事業終了後も、ベンダーが十分なフォローをすることができる範囲。

参加企業数および業種・規模

最終での実証参加企業数は 70 社となった。

業種別では、「製造業」「卸売業・小売業」が多く、全体の半数を占める。募集時に、 IT ・ IoT をよく活用している業種であると考え、特に案内・募集に注力したためだと考えられる。また上記2業種においては取引先との情報のやり取りが他業種に比べ比較的多いと想定され、そのためサイバーセキュリティへの関心が高いとも考えられる。

また規模は、従業員数 100 人以下の企業が 7 割近くを占め、資本金 3,000 万円以下の企業が半数となった。

参加企業業種別（表 2）

業種	事業所数	割合
D 建設業	5	7.1%
E 製造業	18	25.7%
G 情報通信業	5	7.1%
I 卸売業・小売業	18	25.7%
J 金融業・保険業	10	14.3%
K 不動産業・物品賃貸業	1	1.4%
L 学術研究・専門技術サービス業	3	4.3%
N 生活関連サービス業・娯楽業	1	1.4%
O 教育学習支援業	1	1.4%
P 医療・福祉	3	4.3%
R サービス業（他に分類されないもの）	4	5.7%
T 分類不能の産業	1	1.4%
総計	70	100.0%

参加企業従業員数別（表 3）

従業員数	事業所数	割合
1~5 人	11	15.7%
6~10 人	7	10.0%
11~20 人	7	10.0%
21~50 人	11	15.7%
51~100 人	12	17.1%
101~200 人	16	22.9%
201~300 人	3	4.3%
301 人以上	3	4.3%
総計	70	100.0%

参加企業資本金別（表 4）

資本金	事業所数	割合
1,000 万円未満	19	27.1%
1,000 万～3,000 万円未満	17	24.3%
3,000 万～5,000 万円未満	11	15.7%
5,000 万～1 億円未満	10	14.3%
1 億円以上	6	8.6%
その他学校法人等	7	10.0%
総計	70	100.0%

3.4. 実施内容

3.4.1. 実証の目的

【中小企業のセキュリティ実態の把握】

実施概要

①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構築

②中小企業向けのサイバー保険の在り方を検討するために必要な情報を収集

③参加した中小企業に対して結果をフィードバックすることで、ネットワークセキュリティに対する意識向上を図る

【サイバー攻撃の実態把握】

①ネットワークセキュリティ機器（以下「UTM」という。）を設置による分析

検出したセキュリティインシデントの情報を収集

中小企業がさらされているサイバー攻撃の実態を把握

②中小企業のニーズに応じたサポート体制の検証

機能・サポート体制・掛け付け支援においてあえて差異を付与

実証期間終了後に中小企業へのヒアリングし、最も効果的であった内容を把握

3.4.2. 実証内容

【ネットワークセキュリティ機器 UTM の設置による分析】

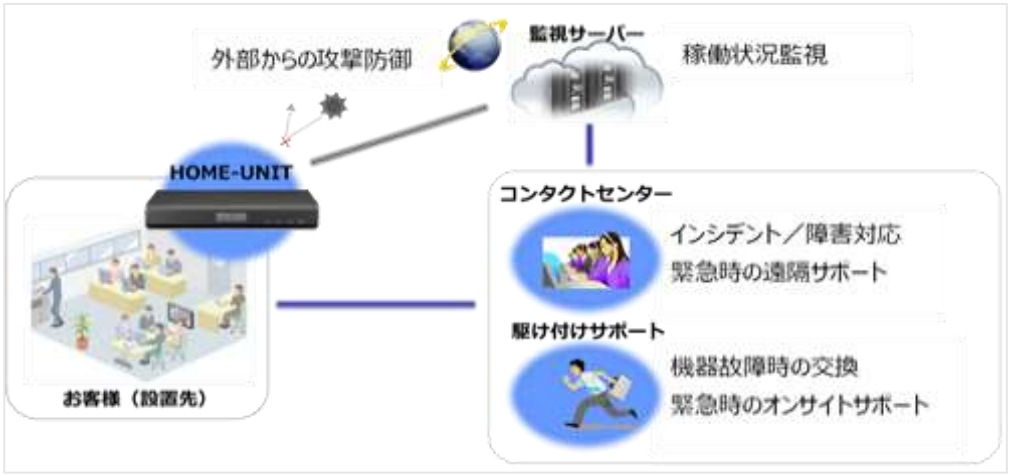
キヤノンマーケティングジャパン　HOME ネットワークセキュリティサービス

実証内容詳細

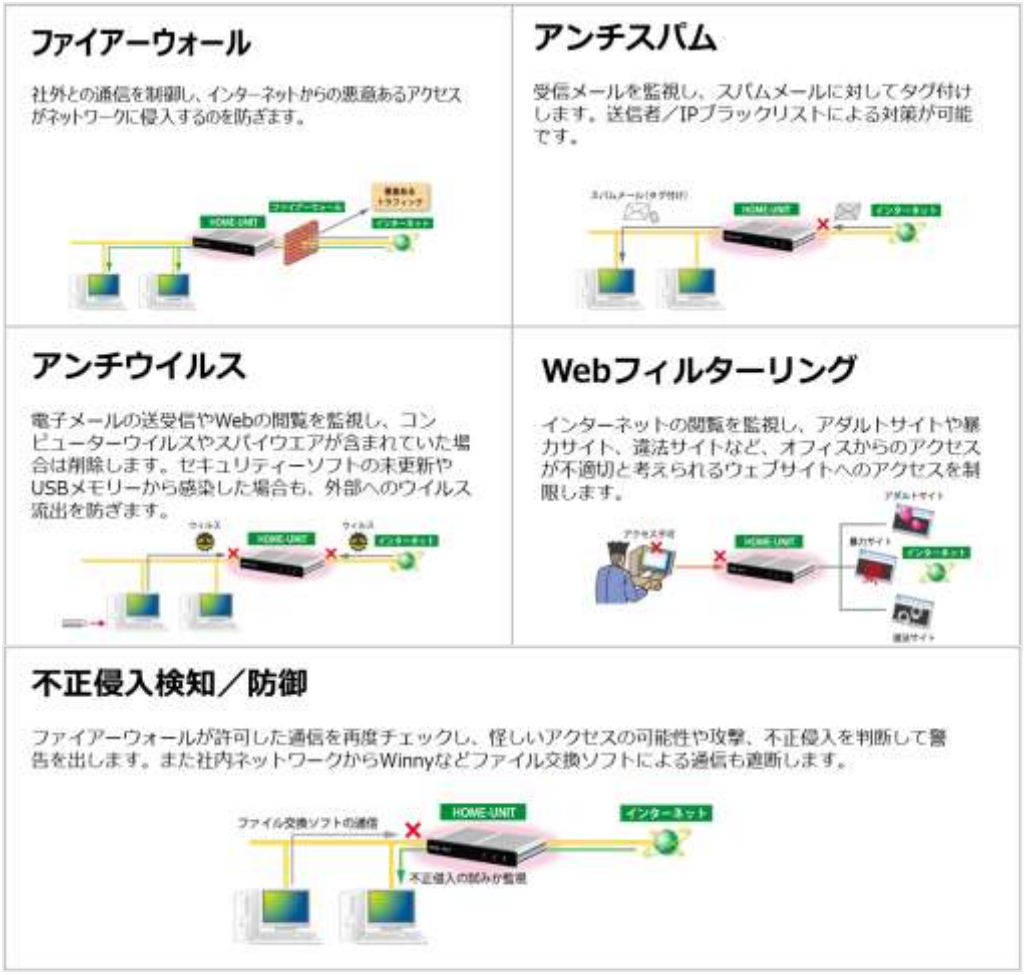
実証参加企業に UTM（HOME-UNIT）を設置し、通信ログを収集、レポート配信。

正常稼働を監視し、障害発生時にはコンタクトセンターから遠隔サポートおよび保守委託拠点から駆け付けサポートを実施。

実証内容イメージ （図 1）



UTM（HOME-UNIT）の主な機能 （図 2）



サポート内容詳細（表 5）

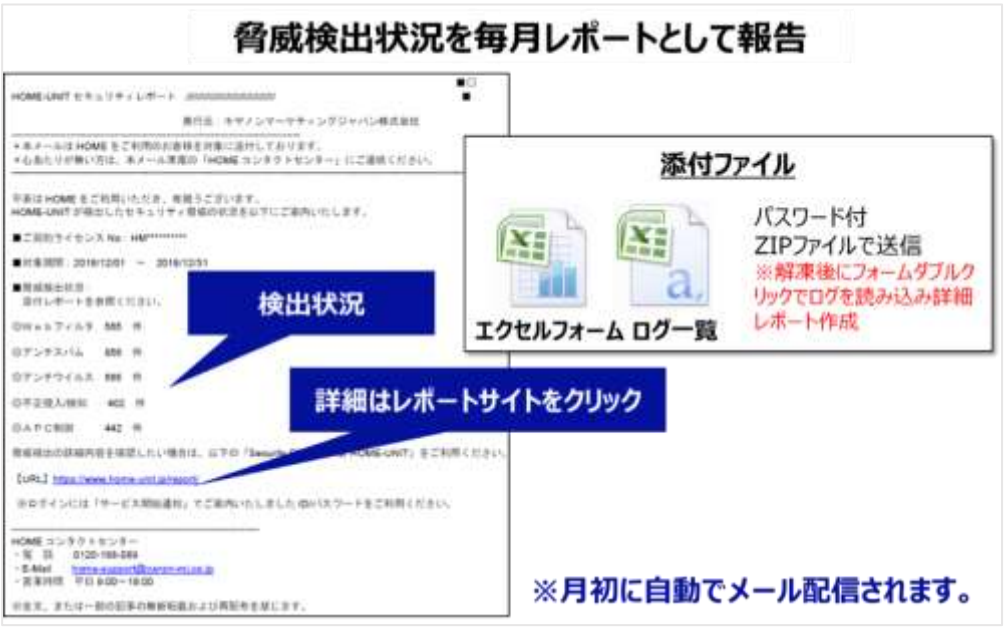
機能		提供内容	
監視	インシデント発生時の連絡	内　　容	以下のセキュリティ脅威イベント発生時のシステム管理者への電話連絡 ・HOME-UNIT 本体電源断および通信異常　・セキュリティアラートの異常時
		提供方法	電話および電子メール
		提供時間	平日 9:00～18:00
	レポート機能	内　　容	HOME-UNIT にて取得する脅威ログの検知状況をまとめたレポートの提供
		提供方法	電子メール
		提供時間	月 1 回配信
対処	セキュリティに関する問合せ対応	内　　容	・HOME－UNIT の設置環境や設定情報の変更などの各種セキュリティ機能 ・セキュリティレポートに関するご質問
		提供方法	電話
		提供時間	平日 9:00～18:00
	インシデント発生時の遠隔支援	内　　容	・セキュリティインシデント発生時のネットワーク端末の調査 ・マルウェア等感染状況の確認および駆除・復旧支援 ・HOME-UNIT が取得するログ解析
		提供時間	平日 9:00～18:00
	インシデント発生時の現地支援	内　　容	OS リカバリ、ネットワーク再構築支援
		提供時間	平日 9:00～17:30
	機器の故障時の交換対応	内　　容	オンサイトによる機器交換作業
		提供時間	平日 9:00～17:30

セキュリティ防御機能一覧（表 6）

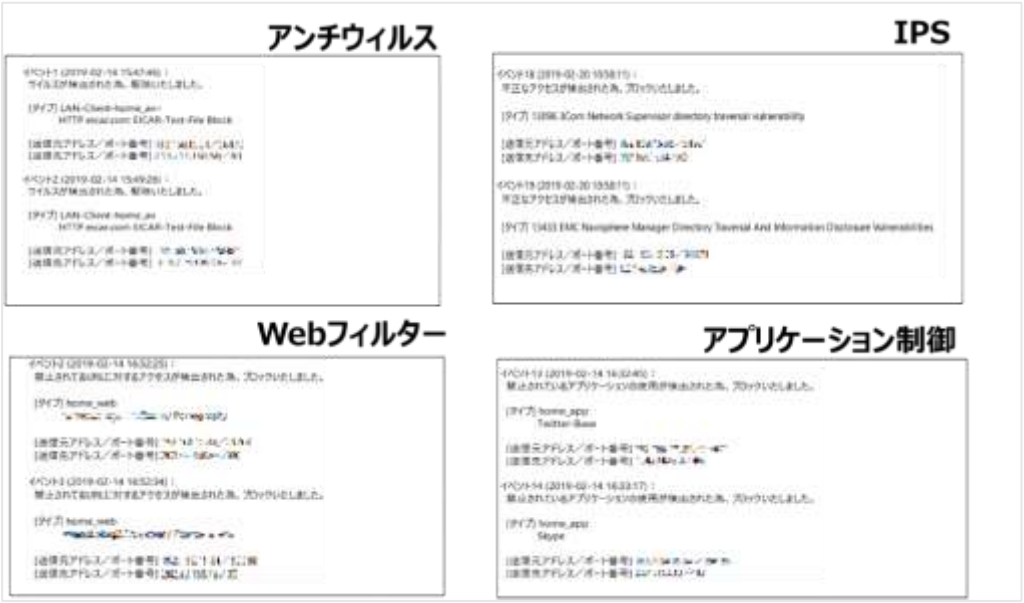
機能	提供内容
アンチウイルス検知	電子メールの送受信や Web の閲覧を監視し、コンピューターウイルスやスパイウエアが含まれていた場合は削除。セキュリティソフトの未更新や USB メモリーから感染した場合も、外部へのウイルス流出を防ぐ。※ヒューリスティック機能およびサンドボックス内蔵
アンチスパム検知	受信メールが「迷惑メール」に該当する、フィッシング詐欺被害に繋がる URL が含まれるなどの検知。送信者／IP ブラックリストによる対策が可能。※当該メールには[SPAM]のタグ付けがされる。
侵入防御（IPS）検知	ファイアウォールが許可した通信を再度チェックし、OS やアプリケーションを対象とした外部からの攻撃や社内からのセキリティリスクがある通信を検知、ブロック。また社内ネットワークから Winny などファイル交換ソフトによる通信も遮断。

DoS/DDoS 攻撃検知	実証参加企業のサーバ環境や端末に対して大量のデータやリクエストを検知・制御。 ※「外部からの攻撃」といった外部要因だけではなく、実証参加企業のネットワーク環境や、回線利用状況により検知される場合もあり。
URL フィルタリング	業務効率の低下や、マルウェア感染・犯罪被害に繋がる不正技術を利用した脅威サイトへのアクセスを検知、ブロック。※申し込み状況により、ブロックされるサイトの種類は異なる。
アプリケーションコントロール（APC）検知	実証参加企業が指定した、情報漏洩や業務効率低下に繋がるアプリケーションの利用を検知、ブロック。

セキュリティレポート詳細-1 （図 3）



セキュリティレポート詳細-2 （図 4）



レポートサイト （図 5）

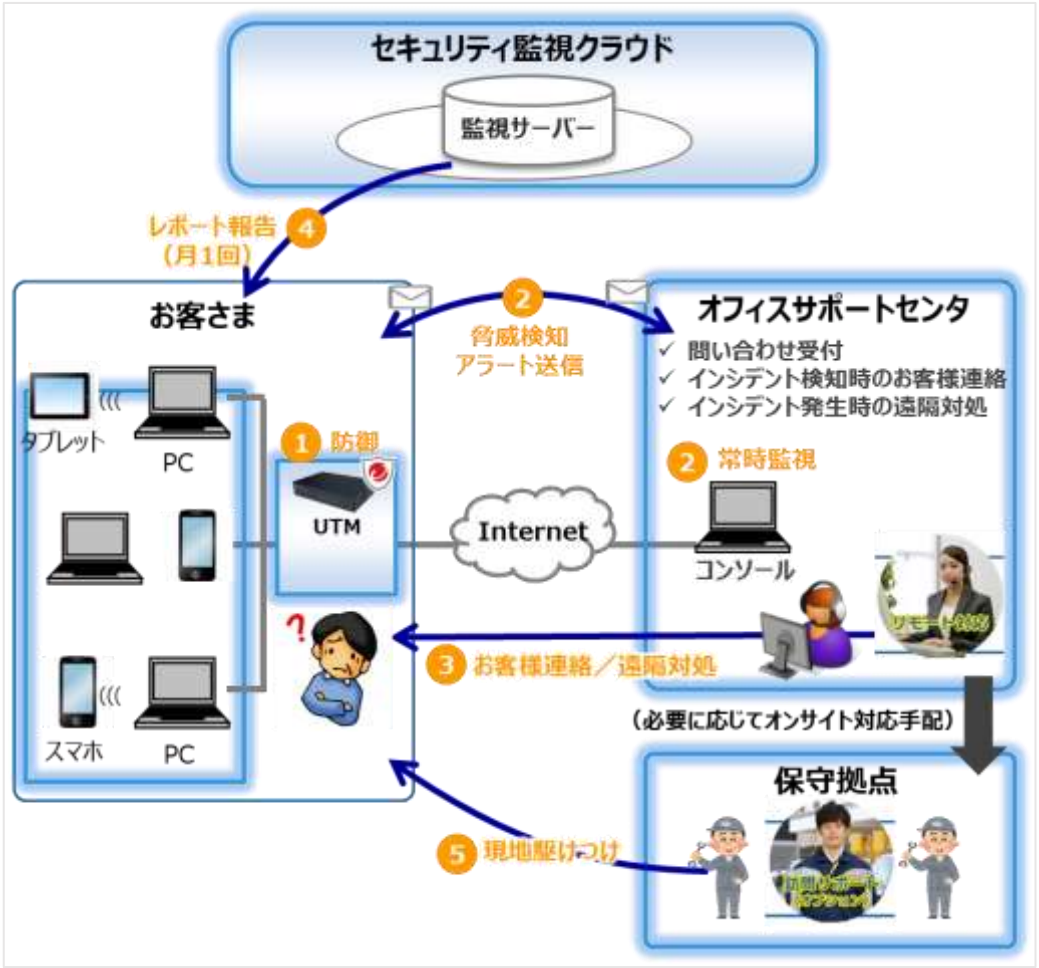
HOME-UNIT が検出した脅威を集計。
当月と過去 5 か月分の脅威検出状況をグラフで表示可

NTT 西日本　セキュリティおまかせプラン

実証内容詳細

実証参加企業にセキュリティ対策機器（UTM※）を設置し、UTM 通信ログを収集する。

実証内容イメージ （図 6）



サポート内容詳細（表 7）

機能		提供内容	
監視	インシデント発生時の連絡	内　　容	以下のセキュリティ脅威イベント発生時のシステム管理者への電話連絡 ・C＆C サーバ通信検知時　・UTM 電源断
		提供方法	電話および電子メール
		提供時間	電子メールによる連絡：24 時間 365 日 電話による連絡：9:00～21:00（年末年始を除く）
	レポート機能	内　　容	セキュリティ脅威の検知状況をまとめたレポートの提供
		提供方法	電子メール
		提供時間	月 1 回配信
対処	セキュリティに関する問合せ対応	内　　容	・セキュリティ全般に関する問合せ対応 ・提供するセキュリティ対策機器やアンチウイルスソフトの機能問合せ
		受付方法	電話
		提供時間	電話による連絡：9:00～21:00（年末年始を除く）
	インシデント発生時の遠隔支援	内　　容	・セキュリティインシデント発生端末の探索支援 ・マルウェア等感染状況の確認およびセキュリティツールによる駆除支援 ・未知のウイルス対策ソフトに対する専用ツールでのログ取得支援・解析 ・提供するセキュリティ対策機器やアンチウイルスソフトの設定支援
		提供時間	電話による連絡：9:00～21:00（年末年始を除く）
	インシデント発生時の現地支援	内　　容	OS リカバリ支援
		提供時間	9:00～17:00（年末年始を除く）
	故障時の交換対応	内　　容	UTM の訪問による故障交換対応
		提供時間	24 時間 365 日

セキュリティ防御機能一覧（表 8）

機能	提供内容
不正プログラム対策	UTM 本体でのエンジン検索とクラウドデータを利用した検索を使い分け、高い不正プログラム検出率を維持しながら高スループットを実現。
メールセキュリティ対策	E-mail レピュテーションと UTM 本体のエンジンを利用し、不正プログラム付メール、スパムメールをブロック。また、コンテンツフィルタリングにより、不適切なメールを検知。
機械学習型検索（添付ファイル）	メール攻撃で侵入する添付ファイルを、AI 技術を利用して特徴を元に判断することで、従来の検出技術では検出できなかった未知のマルウェアにも迅速に対処。
クラウドサンドボックス	必要に応じて不審なメールの添付ファイルの解析を実施。

Web レピュテーション	約 16 億 URL の情報を持つトレンドマイクロ社のデータベースを利用して、接続先 URL をリアルタイムに評価。
URL フィルタリング	約 80 のカテゴリで URL をフィルタリング。ブラックリスト/ホワイトリストの設定も可能。
E-mail レピュテーション	スパムメール対策として使用。受信メールメッセージの IP アドレスを検証して、スパムおよびフィッシングの送信元を特定し阻止。
アプリケーションコントロール	1,000 以上のアプリケーションをサポートし、利用可否を制御。
侵入防御（IPS）	6,500 を超えるルールにより脆弱性対策が可能。
ファイアウォール	攻撃をブロックし、適切なアプリケーショントラフィックのみを通過。
コンテンツフィルタ	メールのコンテンツフィルタリングを実施。

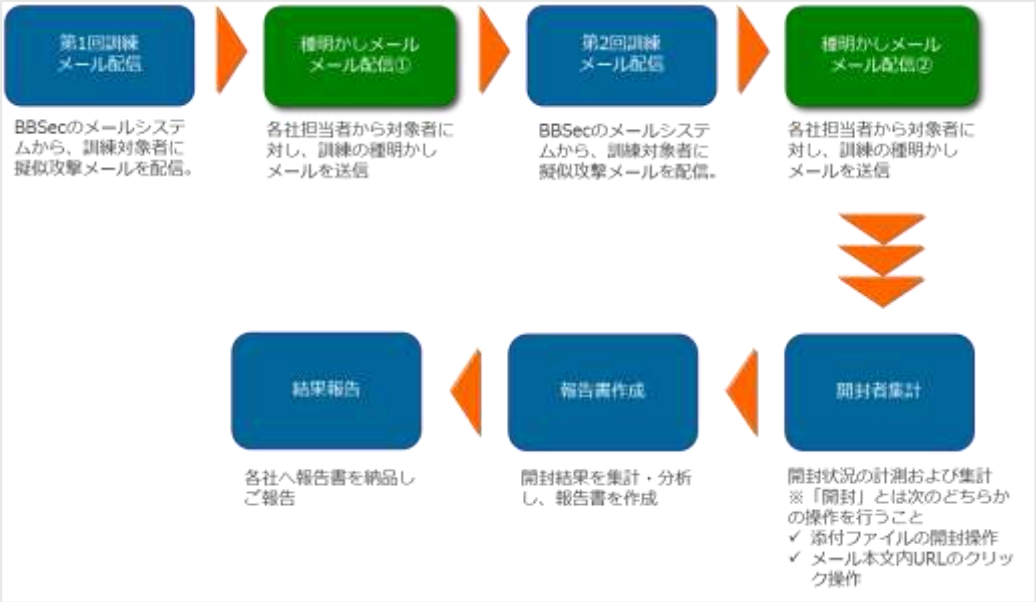
【セキュリティ対策の実態把握】

<u>STNet　標的型メール訓練サービス</u>

実証内容詳細

今回は 30 の企業・団体に対して標的型攻撃メール訓練を実施。同訓練は、各企業・団体の対象者に対し株式会社ブロードバンドセキュリティ（以下「BBSec」という。）から擬似攻撃メールを配信し、メール内の URL リンク、または添付ファイルの開封者をカウントして結果を報告するものである。擬似攻撃メールは期間を通じて各企業・団体それぞれに対し 2 回配信している。

標的型メール訓練サービススキーム （図 7）



※メール文面サンプル （図 8）

件名： 総務企画部 <announcement@office-information.com>
送信アドレス： テレワーク導入についてのアンケート

本文

各位

新型コロナウイルス感染症（COVID-19）や開催延期となった
東京オリンピック・パラリンピックへの対策としてテレワークでの業務
が推奨されています。
これらのことから、当社では積極的にテレワークを推進していきます。

つきましては皆さまのご意見を伺いたく、下記のURLよりアンケートにご協力下さい。
※急なお願いで申し訳ありませんが、○月○日（○曜日）までにご回答をお願いいたします。

[訓練用URL]

以上

総務企画部 ○○

4. 実施結果

4.1. 説明会の開催（表 9）

日　　時	2020 年 9 月 15 日（火） 14 時～16 時	
場　　所	高松商工会議所 およびオンライン配信（Zoom）※感染症拡大防止策のため	
出 席 者	34 社/39 名 （高松商工会議所にて 18 社/20 名、オンラインにて 16 社/19 名）	
講 演 会	テ ー マ	サイバーセキュリティの基礎（特定非営利活動法人 ITC かがわ）
説 明 会	テ ー マ	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）
	テ ー マ	サイバーセキュリティお助け隊事業概要説明（高松商工会議所）
	テ ー マ	情報セキュリティ自社診断の実施（高松商工会議所）
個別相談会	本事業における実証内容の説明（希望者のみ） ネットワークセキュリティ機器（UTM）設置 キヤノンマーケティングジャパン（株） 西日本電信電話（株） 香川支店 標的型メール訓練 （株）STNet	
ｱﾝｹｰﾄ内容	①独自アンケート 計 11 問 （説明会もしくは実証参加申込時に回答、73 社） サイバーセキュリティに対する意識および対策に関して・・・6 問 本事業および実証内容について・・・5 問 ②新！5 分でできる情報セキュリティ自社診断 （説明会もしくは実証参加申込時に回答、69 社）	

説明会の開催内容については、下記 URL 等より実施の様子を撮影した動画を閲覧可能。

説明会開催後、本実証事業への参画を検討される方への説明や、サイバーセキュリティ対策の啓発として、Web にて動画を配信。

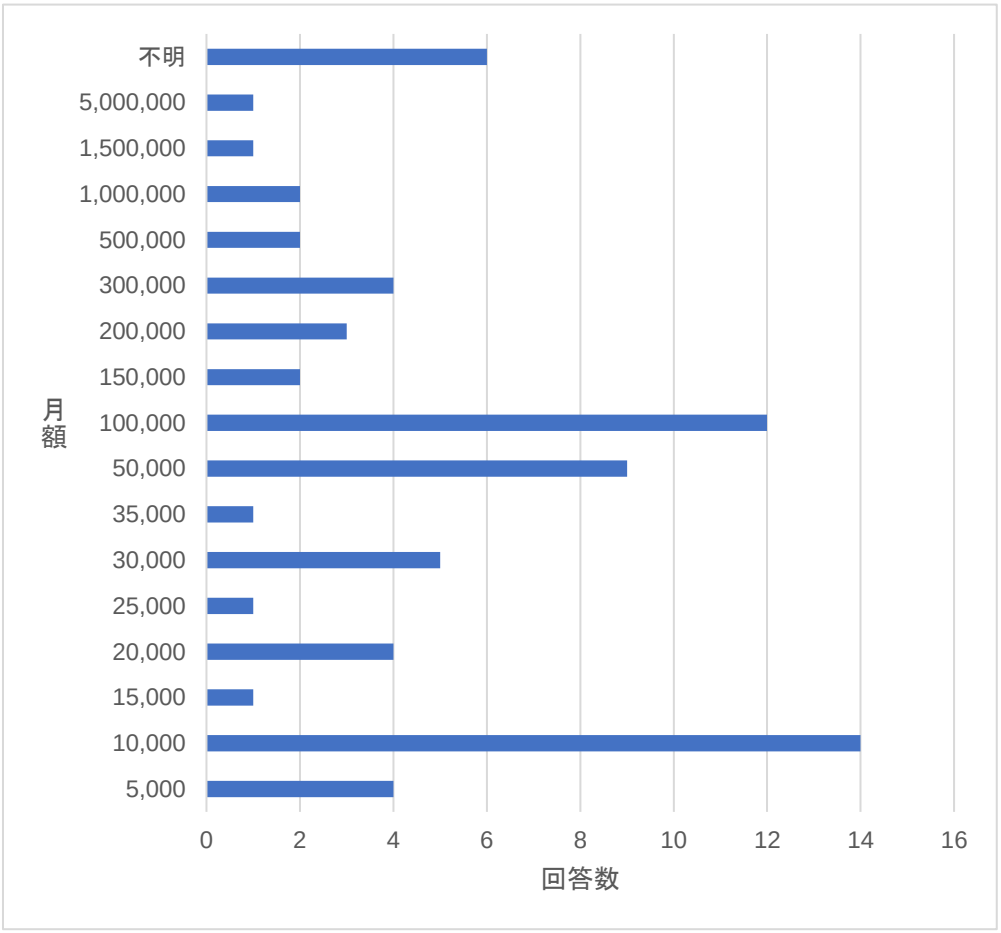
高松商工会議所：YouTube、https://youtu.be/SuLJS_EKYOk （2021/1/20 参照）

4.2. 実態把握結果

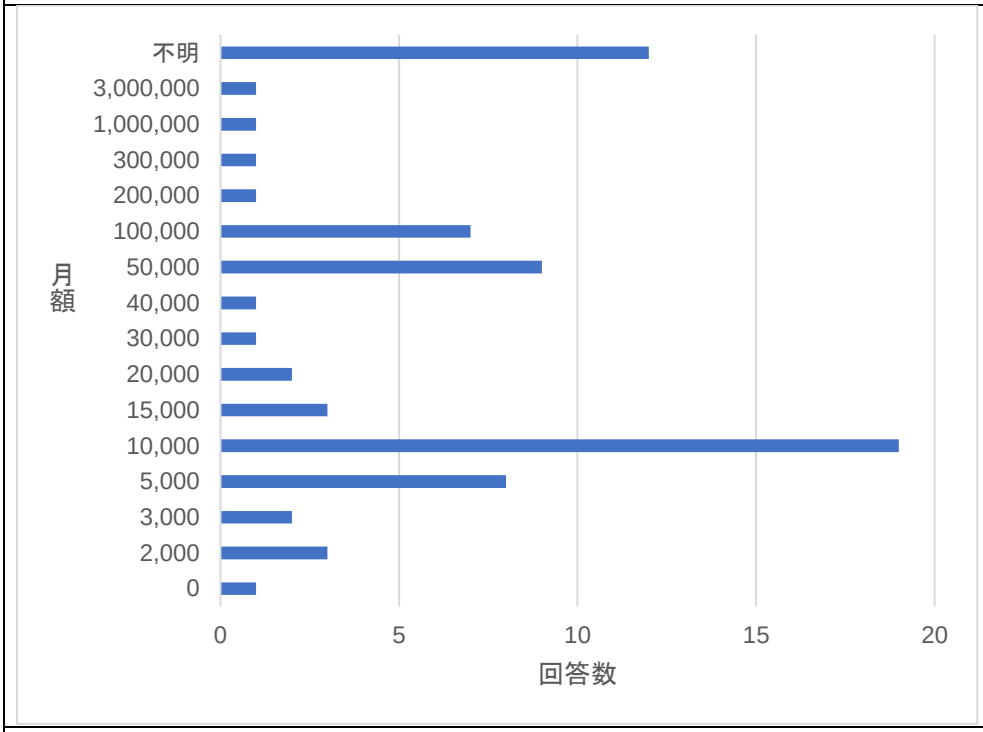
説明会時実施アンケート/72 社回答 （表 10）

①「サイバー攻撃」や「サイバーセキュリティ」について		
回答内容	回答数	割合
理解している	14	19.4%
知っている	41	56.9%
聞いたことはある	17	23.6%
総計	72	100.0%
②現在何らかのサイバーリスクに対する対策を行って		
回答内容	回答数	割合
いる	53	73.6%
いない	19	26.4%
総計	72	100.0%
③これまでサイバー攻撃を受けたことが		
回答内容	回答数	割合
ある	21	29.2%
無い	51	70.8%
総計	72	100.0%
④サイバー攻撃によって実害が発生したことが		
回答内容	回答数	割合
ある	9	12.5%
無い	63	87.5%
総計	72	100.0%

⑤サイバーセキュリティ対策に係る費用は、



⑥サイバーセキュリティ対策費用として、月額いくらなら積極的に取り入れたいと思いますか？



⑦本事業を知ったきっかけは何ですか？

回答内容	回答数	割合
IPA サイト	2	2.8%
お助け隊メンバーの紹介	30	41.7%
各種関連団体の紹介	28	38.9%
知人や友人等の紹介	9	12.5%
その他	3	4.2%
総計	72	100.0%

⑧本事業にどんなことを期待しますか？

回答内容	回答数	割合
セキュリティ対策の妥当性の確認	13	15.1%
セキュリティの向上	38	44.2%
セキュリティ対策助言の入手	14	16.3%
セキュリティ関連情報の入手	7	8.1%
セキュリティ製品/サービスの利用	12	14.0%
その他	2	2.3%

⑨実証に参加いただける場合、希望されるのはどちらですか？

回答内容	回答数	割合
なりすまし等の悪意あるメールに対する社員の対応力やリスクレベルを把握し、対策・改善を行いたい	32	44.4%
自社へのサイバー攻撃を把握し、必要な対策を知りたい	36	50.0%

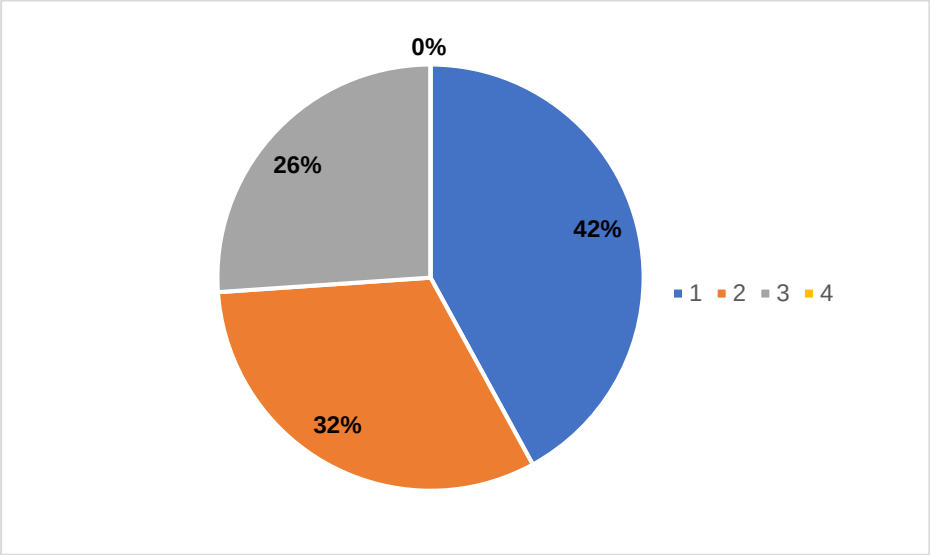
両方	4	5.6%
総計	72	100.0%
⑩貴社へのサイバー攻撃状況の把握や対策をされる場合、サポートとして重視されるのはどちらですか？		
回答内容	回答数	割合
遠隔操作による復旧支援	26	36.1%
充実したコールセンター機能	35	48.6%
両方	11	15.3%
総計	72	100.0%

分析結果

回答した企業の内、「サイバー攻撃」や「サイバーセキュリティ」という言葉を聞いたことが無いという企業は無く、理解や対策に繋がっているか否かの差はあるが、サイバーセキュリティ対策への関心はあると推察できる。しかしながら、実際に攻撃を受けたり、被害を被ったりしたという認識のある企業は多くなく、サイバー攻撃が身近なものだという実感は薄いと考えられる。

また、サイバーセキュリティ対策を導入する上での検討金額は、中央値は 10,000 円以下、さらに「不明」と回答した企業も 10 社以上あった。本実証事業へ期待する内容への回答からも、自社のセキュリティ向上は行いたいが、どのような対策があるのか、またその妥当性を確認する術が無いために、投資しづらいのではないかと考える。

説明会時実施「5 分でできる！情報セキュリティ自社診断」/69 社回答 （**図 9**）



分析結果

回答した企業の内、「49 点以下」が 4 割以上を占めた。20 点以下となった企業も複数あり、対策を実施していないことに加え、担当者が自社のセキュリティ対策状況を把握していない項目が多かったために点数が伸びなかったと考えられる。まずは、本実証事業を機に関心を持ち、自社の把握と対策の実施が行えるよう支援を行う必要がある。

一方、100 点には届かなかったものの、90 点以上の企業が 3 社あり、サイバーセキュリティ対策への関心が高く、対策を実施していた。本実証事業への参加により、対策の妥当性の確認や、多重防衛の必要性を理解するきっかけとなったと考える。

実証前訪問時ヒアリング （表 11）

Q.実証へ参加した理由や、設置する上で不安に思うことはありますか？
＜参加理由＞ ・先日 emotetに感染した為、2 度とこの様な事は起こしたくないので実証に参加したい。 ・セキュリティ対策や UTM の内容をよく知りたい。 ・今後どのくらいのレベルのセキュリティ対策が必要か把握したい。 ・実際なりすまし等の悪意あるメールに悩まされているため、セキュリティ対策をしたい。 ・セキュリティに関して社内研修を実施しているが、教育の効果が出ているかどうか確認したい。 ・社員のセキュリティ意識を確認したい。また実証をもってこれからの対策を考えたい ・メールや Web は業務に欠かせないもので、それを扱うリスクについて社員に知ってもらいたい。 ・今現在何らかのサイバー攻撃を受けているかの確認、および現在セキュリティレベルでどの程度のサイバー攻撃なら守られているのかを把握したい。 ・なりすましメールが実際に届いたことがあり、他人事ではないと思った ・セキュリティ対策にどのような方法があるか知りたい。 ・UTM を実際に導入してみて、妥当性や動作検証をしたい。 ＜不安に思うこと＞（⇒は回答内容） ・自社のネットワークの構成を十分に把握していないが、UTM 設置の工事はベンダーに行ってもらえるのか。 ⇒本事業では事前調査、設置等はベンダーが行う。そのため事前に調査を実施する。 ・UTM を設置するとインターネット回線が遅くなるのか。 ⇒接続端末数によっては遅くなることもある。まずはベンダーが事前調査を行い、UTM が設置できるか、回線が遅くなる場合はどの程度なのかを伝えるる。 ・事務所が離れているが、UTM は複数台設置した方がよいのか。 ⇒企業内のネットワーク構成によっては、1 台でカバーできる場合もある。ベンダーが事前調査を行い確認する。

分析結果

自社の実態を把握したいという意向の企業が多く、本実証事業での実証結果を見て、どの程度の対策が必要なのかを検討する企業が多いと考えられる。また、限られた経費の中で、自社に必要な対策を知りたいという思いを抱えていると推察できる。さらに、これまで独自で研修や対策を行ってきたが、その効果、妥当性を図りたいという企業もあり、対策の導入後も随時相談を行える窓口や機会を設ける必要がある。

報告会開催時実施アンケート/45 社回答 （表 12）

1.セキュリティ担当者の有無についてお教えください。		
回答内容	回答数	割合
専任者がいる	7	15.6%
兼任しかいない	26	57.8%
1 人もおらず経営層が直轄	9	20.0%
1 人もおらずIT業者等に外注	0	0.0%
業務マニュアルがあるのでどの社員でも担当出来る	0	0.0%
専任者以外に分かる社員がおらず業務マニュアルもない	2	4.4%
答えたくない/不明	1	2.2%
総計	45	100.0%
2. サイバーセキュリティ対策の相談先の有無についてお教えください。		
回答内容	回答数	割合
あり	30	66.7%
無し	14	31.1%
答えたくない/不明	1	2.2%
総計	45	100.0%
3. インシデント（事故につながるような出来事）発生時の相談先についてお教えください。		
回答内容	回答数	割合
あり	27	60.0%
無し	18	40.0%
答えたくない/不明	0	0.0%
総計	45	100.0%
4. 取引先からのセキュリティ対策の要求についてお教えください。（例：SECURITY ACTION を宣言していないと取引できないと言われた等）		
回答内容	回答数	割合
取引の要件化とされつつある	1	2.2%
指示されつつある	4	8.9%
依頼されつつある	13	28.9%
答えたくない/不明	27	60.0%
総計	45	100.0%
5. 過去（本実証事業以前）サイバー攻撃を受けたことがありましたか？（複数回答可）		
回答内容	回答数	割合
HP 接続不能・改竄	3	5.7%
標的型攻撃メール/ビジネスメール詐欺	20	37.7%
ランサムウェア（暗号化・身代金）	5	9.4%

導入したシステムや製品にウイルス等が混入	1	1.9%
その他攻撃	8	15.1%
答えたくない/不明	16	30.2%
総計	53	100.0%
6. 過去（本実証事業以前）サイバー攻撃によって被害を受けたことがありましたか？（複数回答可）		
回答内容	回答数	割合
情報漏えい被害	3	6.7%
システムダウン被害	0	0.0%
データ損壊被害	5	11.1%
金銭拠出被害	0	0.0%
流通途絶被害	0	0.0%
答えたくない/不明	37	82.2%
総計	45	100.0%
7. 現在、サイバー攻撃対策としてどのような対策を実施されていますか？（複数回答可）		
回答内容	回答数	割合
アンチウイルスソフト	33	25.0%
ファイアウォール	24	18.2%
UTM	14	10.6%
その他 IT ベンダー提供サービス	4	3.0%
データのパスワード設定	11	8.3%
データの暗号化	6	4.5%
物理的管理の徹底（PC・USB の持ち出し禁止等）	14	10.6%
社員教育・研修	14	10.6%
専門人材育成	1	0.8%
ISMS・CSMS の取得	0	0.0%
SECURITY ACTION	3	2.3%
サイバー保険	3	2.3%
取引先との情報管理契約	2	1.5%
サプライチェーンでの規定等の制定・参画	0	0.0%
その他対策を実施	1	0.8%
実施していない	2	1.5%
総計	132	100.0%
8. 現在、情報セキュリティ対策にかけている月額の費用はいくらですか？（サイバー保険費用を含む。情報システム担当者の人件費を除く）		
回答内容	回答数	割合
月額 1,000 円未満	1	2.2%
月額 1,000 円～3,000 円	3	6.7%

月額 3,001 円～5,000 円	3	6.7%
月額 5,001 円～10,000 円	7	15.6%
月額 10,001 円～15,000 円	5	11.1%
月額 15,001 円以上	18	40.0%
対策は行っていない（0 円）	3	6.7%
答えたくない/不明	5	11.1%
総計	45	100.0%

9. サイバー攻撃による被害でより脅威と感じるのはどちらですか？

回答内容	回答数	割合
事業中断（データ復旧や原因調査、再発防止策に係る費用が発生）	8	17.8%
情報漏えい（第三者への賠償費用が発生）	7	15.6%
事業中断・情報漏えいの両方	29	64.4%
答えたくない/不明	1	2.2%
総計	45	100.0%

10. 現在、サイバー保険へ加入されていますか？

回答内容	回答数	割合
加入している	7	15.6%
加入していない（必要性を感じていないため）	2	4.4%
加入していない（予算がないため）	4	8.9%
加入していない（満足する内容のものがないため）	1	2.2%
加入していない（自社に適した補償内容や保険料が分からない）	16	35.6%
加入していない（その他）	11	24.4%
答えたくない/不明	4	8.9%
総計	45	100.0%

11. 本実証事業に参加いただいたことで、今後、サイバーセキュリティ対策の実施内容や費用に変化はありますか？（情報システム担当者の人件費を除く）

回答内容	回答数	割合
現在と変わらない	25	55.6%
現在の対策内容（設置機器や保険内容）等を検討し、費用削減を検討	4	8.9%
新たな対策の実施（機器の設置、社員研修の実施、保険への加入）等、費用の増額を検討	16	35.6%
総計	45	100.0%

12. 今後、サイバー保険へ加入するとした場合、月額いくらであれば検討されますか？

回答内容	回答数	割合
月額 1,000 円未満	2	4.4%
月額 1,000 円～3,000 円	4	8.9%
月額 3,001 円～5,000 円	7	15.6%

月額 5,001 円～10,000 円	12	26.7%
月額 10,001 円以上	2	4.4%
答えたくない/不明	18	40.0%
総計	45	100.0%
13. 今後、サイバーセキュリティに関する保険のご案内を希望されますか？		
回答内容	回答数	割合
希望する	12	26.7%
希望しない	21	46.7%
答えたくない/不明	12	26.7%
総計	45	100.0%
14. 今後、貴社が情報セキュリティ対策をするきっかけとして考えられるものをお教えください。（複数回答可）		
回答内容	回答数	割合
自社がサイバー攻撃を受けた時	28	18.1%
同業他社がサイバー攻撃を受けた時	18	11.6%
取引先がサイバー攻撃を受けた時	14	9.0%
取引先からの要請	25	16.1%
国や自治体からの要請	18	11.6%
金融機関からの勧め	10	6.5%
補助金・助成金申請時の要件化	18	11.6%
ベンダーからの提案	11	7.1%
同業他社の対策強化情報	9	5.8%
税理士・弁護士からの勧め	3	1.9%
不明/答えたくない	1	0.6%
総計	155	100.0%
15. サービスの実施結果や UTM 検知状況報告等、レポートの分かりやすさはいかがでしたか？		
回答内容	回答数	割合
分かりやすかった	30	66.7%
閲覧したが、専門用語が多く分かりづらい	10	22.2%
閲覧していない	1	2.2%
担当者から報告を受けている	4	8.9%
総計	45	100.0%
16. UTM 設置や標的型メール訓練の実施にあたり、コールセンターやベンダー担当者へ相談されましたか？されなかった場合、理由をお教えください。		
回答内容	回答数	割合
相談した	23	51.1%
相談していない（相談するような事項がなかったため）	14	31.1%

相談していない（何を相談すればいいか分からなかったため）	4	8.9%
相談していない（相談したかったが連絡先が分からなかったため）	0	0.0%
相談していない（その他）	4	8.9%
実証事業に参加していない	0	0.0%
総計	45	100.0%

17. お助け隊の実証サービスは満足いただけましたか？

回答内容	回答数	割合
非常に満足	14	31.1%
満足	27	60.0%
どちらともいえない	4	8.9%
不満	0	0.0%
非常に不満	0	0.0%
実証には参加していない	0	0.0%
総計	45	100.0%

18. お助け隊の実証に参加してよかったと思う点がございましたらお教えください。（複数回答可）

回答内容	回答数	割合
自社へのサイバー攻撃・情報流出等が防げた	2	3.4%
自社へのサイバー攻撃動向が把握できた	14	24.1%
自社のサイバーセキュリティやネットワーク環境を把握・改善することができた	11	19.0%
自社の社会的信用が向上した	0	0.0%
社員のサイバーセキュリティ意識・知識が向上した	30	51.7%
良かったと思う点はない	0	0.0%
その他	1	1.7%
総計	58	100.0%

19. 今回参加いただいたサービスが有料となった場合、いくらくらいの価格（税込）であれば導入されますか？※UTM 設置は【月額】、標的型メール訓練は【2回配信】

回答内容	回答数	割合
1,000 円未満	2	4.4%
1,000 円～3,000 円	5	11.1%
3,001 円～5,000 円	6	13.3%
5,001 円～10,000 円	12	26.7%
10,001 円～15,000 円	6	13.3%
15,001 円以上	4	8.9%
有料なら利用しない	4	8.9%
答えたくない/不明	6	13.3%
総計	45	100.0%

20. 今後セキュリティ対策に関するサービスについて、求めることは何でしょうか（複数選択可）		
回答内容	回答数	割合
高くても包括的な対策をしてくれる商品・サービス	11	16.2%
安くて限定された箇所のみ対策をする商品・サービス	24	35.3%
相談窓口	18	26.5%
いざというときの保険	10	14.7%
その他	1	1.5%
答えたくない/不明	4	5.9%
総計	68	100.0%
21. テレワークを実施していますか？		
回答内容	回答数	割合
実施している	13	28.9%
実施体制は整っているが、現在は実施していない	14	31.1%
実施していない	18	40.0%
総計	45	100.0%
22. テレワーク等、社外で業務を行うことについて、どのようなリスクを感じますか？（複数回答可）		
回答内容	回答数	割合
社外で業務用パソコンを利用するための技術的な対策がとれていない	18	17.5%
私用パソコンの業務利用	13	12.6%
USB メモリーの利用	10	9.7%
フリーWi-Fi への接続	15	14.6%
私用スマートフォンの業務用パソコンへの接続	9	8.7%
オンラインストレージ等ファイルツールの利用	7	6.8%
フリーメールの利用	6	5.8%
Web 会議サービスのセキュリティが不安	5	4.9%
セキュリティ強化によるパフォーマンスの低下	6	5.8%
パソコンの紛失・破損	14	13.6%
総計	103	100.0%
23. （テレワークを実施している事業所様）実施にあたり何かしらのセキュリティ対策を行いましたか？（複数回答可）		
回答内容	回答数	割合
リモートツールの導入	9	22.5%
VPN の導入	10	25.0%
テレワーク用端末を配備	7	17.5%
リモートデスクトップの導入	5	12.5%
資料の社外持ち出しルール等の徹底	5	12.5%
シンクライアント端末の導入	0	0.0%

その他	4	10.0%
総計	40	100.0%

24. 貴社でのサイバーセキュリティ対策を行う上での課題、本事業へのご意見・ご感想等ございましたら、自由にご記入ください。

回答内容
・一人でもリテラシーが低いと低い方に引っ張られるので、全体の底上げが必要。 ・現在は実施していませんが、今後もしテレワークを本格的に実施するようになったら、社員のサイバーセキュリティに対する教育が今以上に必要だと感じている。 ・実施が急務であるが、経費面でオーナーへの説得が必要。具体例を複数知りたい。 ・社員のセキュリティ意識向上に繋がった。ありがとうございました。 ・上層部のセキュリティ意識がまた希薄なところがあり、費用負担が発生するとなると見えないものに投資することになるので説明等に注力しないといけない。 ・今回サイバーセキュリティお助け事業に参加したことにより、社員の普段何気なく利用しているメールにも危険があるということを意識付けできたことは効果があったと思う。 ・全くセキュリティ対策を行っていない会社などは、今回の事業を有意義なものにできたのではないかと思う。自社でももう少しセキュリティ対策について考えようと思った。 ・費用増を経営層に提案するのが難しく、対策が進めにくい。 ・本事業に参加できて非常に良かったと感じている。今後もいろいろと情報提供頂ければと思う。 ありがとうございました。 ・予想以上にウイルスが入りこんでいる実態が分かった。データ分析しないといつまで放置になるので良い機会であると思っている。継続的にこの事業はして頂ければさらに興味あるいは勉強になるのではと思う。

分析結果

専任者が不在の企業が多いこと等から、サイバーセキュリティ対策の検討が十分に行えていない、関連情報を得にくい状況であることが考えられる。支援体制として相談窓口を設けたり、ツール紹介・セミナーの開催など情報提供を行うことで、よりサイバーセキュリティ対策の実施および啓発が図られると考える。

また、費用については、担当者が必要性を理解していても、導入のために必要となる経営層への説明に苦慮しているという意見が散見される。セキュリティ機器・保険ともに、導入しやすい価格に設定することに加え、その必要性、対策の有効性を経営者に訴える必要がある。実証の感想や「5 分でできる！情報セキュリティ自社診断」の結果から、本実証事業のように中小企業が導入のきっかけとしやすい事業があることで、関心を持つ機会、対策を始める導入となることが分かる。

サイバーセキュリティ対策については、ほとんどの実証参加企業が、既に何かしらの対策を行っていたが、アンチウイルスソフトなど1つの対策で十分と考えていた、との意見があった。セキュリティ機器の設置といったハード面だけでなく、社員教育、インシデント発生時の報告体制などソフト面での対策など、複数の防御体制を構築することが課題であると考える。

4.3. 実証の実施結果

4.3.1. セキュリティ対策機器（UTM）によるサイバー攻撃の状況把握

実証期間中に設置したセキュリティ対策機器（UTM）により以下のサイバー攻撃を検知した。

キヤノンマーケティングジャパン HOME ネットワークセキュリティサービス

実証期間・参加企業数 （表 13）

期間	2020 年 10 月～12 月（設置期間は各社ごとに異なる）
対象企業	16 社
検知企業	16 社

検知したサイバー攻撃 （表 14）

i	アンチウイルス検知	8
ii	スパムメール検知	8,465
iii	IPS 検知	134
iv	DoS/DDoS 攻撃検知	33,151
v	URL フィルタリング	5,401
vi	アプリケーションコントロール（APC）検知	0

本実証参加企業※3 位まで （表 15）

順位	アラート種別	検知率	検知件数
1 位	DoS/DDoS 攻撃検知	70.3%	33,151
2 位	アンチスパム検知	17.9%	8,465
3 位	URL フィルタリング	11.4%	5,401
弊社の実証参加企業においては、全体傾向よりさらに DoS 攻撃数が多い状況となった。これは、一部の実証参加企業の設置環境のネットワーク端末の通信が影響しているものと見られ、外部からの攻撃が極端に多いとは限らないが、全体傾向と比較しても上位に位置した。			

参考：日本国内に稼働する同一機種の検知傾向値を参照※3 位まで（表 16）

順位	アラート種別	検知率	検知件数
1 位	URL フィルタリング	47.0%	—
2 位	DoS/DDoS 攻撃検知	32.5%	—
3 位	アプリケーションコントロール（APC）検知	12.7%	—

アンチスパム検知　分析（表 9 の詳細）

アンチスパムを検知した件数の上位 3 位までで全体の 67%に相当した。送信元アドレスの多くはショッピングサイト、インターネット通販事業者からのメールがスパムメールと判定されている。インターネット通販を日常的に利用している企業においては検知される可能性が高い。ただ、検知された一部のアドレスは不審なドメインも散見され、フィッシングサイトへ誘導するようなメールの可能性もある。

DoS/DDoS 攻撃検知　分析（表 9 の詳細）（表　17）

分類 A	分類 B	分類 C	分類 D
32,096	21	19	21
分類 A：プライベート IP アドレス、IPv6 のリンクローカルアドレス			
同一セグメント内での通信と見られる社内の通信が DoS 攻撃として検知された。検知されたシグニチャのほとんどが「RSTPROT_DETECTOR」であった。当該シグニチャは社内のネットワーク輻輳などによりセッションが正常に確立しない場合やデータ通信量が多い場合も検知。			
分類 B：Apple 社の IP アドレス／Google や Yahoo!などの検索エンジンなどと見られる IP アドレス			
検知されたシグニチャのほとんどが「RSTPROT_DETECTOR」であった。当該シグニチャは社内のネットワーク輻輳などによりセッションが正常に確立しない場合にも検知される。			
分類 C：プロバイダやネットワーク機器・サーバ管理会社などから割り振られる IP アドレスなど			
プロバイダが端末に割り振った IP アドレスからのアクセス。通信元がサイバー攻撃の踏み台にされている場合もあるため、不審な通信元の可能性もある。			
分類 D：外部からの攻撃遮断			
overlapped_fragment を検知、ネットワークへの侵入を試みるパケットをブロックした。IP パケットに対するフィルタリング機能を、先頭のフラグメントパケットでしか行わない製品／機器が存在することを利用して、IP パケットのフラグメントオフセットが重複するようにフラグメント化したパケットを送信する攻撃。これにより、2 番目以降のフラグメントパケットが内部ネットワーク上のホストに到達するおそれがある。			

URL フィルタリング　分析（表 9 の詳細）

URL フィルタリング検知は全ての実証参加企業において検知された。その多くは、アダルト／兵器・武器／ショッピングなどカテゴリされたサイトへのアクセスであったが、一方でマルウェア／フィッシングサイト／違法ソフトへのアクセスが約 1 割見られ、サイバー攻撃の入り口となる有害なサイトへのアクセスを制御している。

侵入防御(IPS)検知　分析

侵入防御(IPS)検知件数は 134 件と比較的少ないものの、検知された実証参加企業の割合は 60%を超えた。

主な内容は以下のとおりである。（表 18）

[BUFFER OVERFLOW]	21 件
攻撃対象のコンピューターに許容量以上のデータを送り付け、誤作動を起こさせる攻撃を検知、遮断	
[CONFIG ERROR WEB-MISC Admin_files access]	24 件
http アクセスする際に、URL に「/admin_files」が存在したため検知、遮断。攻撃を受けた場合、サーバの情報漏洩等の可能性がある。	
[UNKNOWN GNU Bourne Again Shell(Bash) Remote Code Execution]	59 件
Linux などの UNIX 系 OS で使用されるオープンソースプログラム「Bourne Again shell(bash)」コマンドシェルに存在する脆弱性を利用した攻撃を検知、遮断。	
[BACKDOOR/TROJAN gh0st rat Trojan Horse]	1 件
感染した Windows コンピューターをリモートで制御するために使用されるリモート アクセス/管理ツール （RAT） をインストールするためのバックドアをブロック。	

コールセンター等への相談・対応内容、掛け付け支援の内容 （表 19）

対応種別	件数	相談・インシデント等対応状況
コンタクトセンター	1 件	セキュリティ機器設置等の問合せ
	1 件	セキュリティレポート内容の問合せ
駆け付け	2 件	機器設置等のトラブル対応
	1 件	その他(操作指導や説明等フォロー)

NTT 西日本 セキュリティおまかせプラン

実証期間・参加企業数 （表 20）

期間	2020 年 9 月 28 日(月)～12 月 31 日(木)
対象企業	24 社
検知企業	19 社

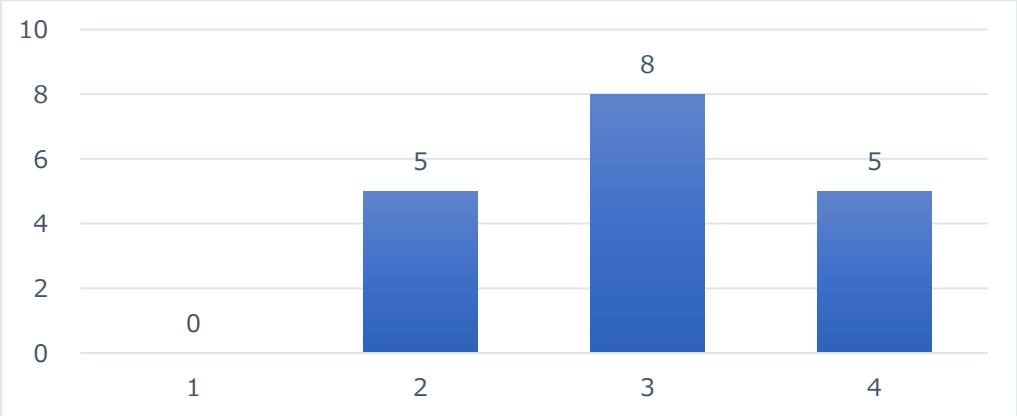
検知したサイバー攻撃 （表 21）

i	不正プログラム検知	18
ii	IPS 検知	705
iii	Web サイトブロック	140
iv	スパムメール検知	43,887
v	ランサムウェア検知	27

不正プログラム探知

不正な通信、プログラムによる攻撃を検知する。どのような通信が行われているか判別し、内部感染を早期に発見する。

不正プログラム検知　月別状況　（表 22）



IPS 検知

IPS とは「不正侵入防御システム」の略称で、利用中のシステムの脆弱性を狙った攻撃等ネットワークを介した攻撃をブロックする。（表 23）

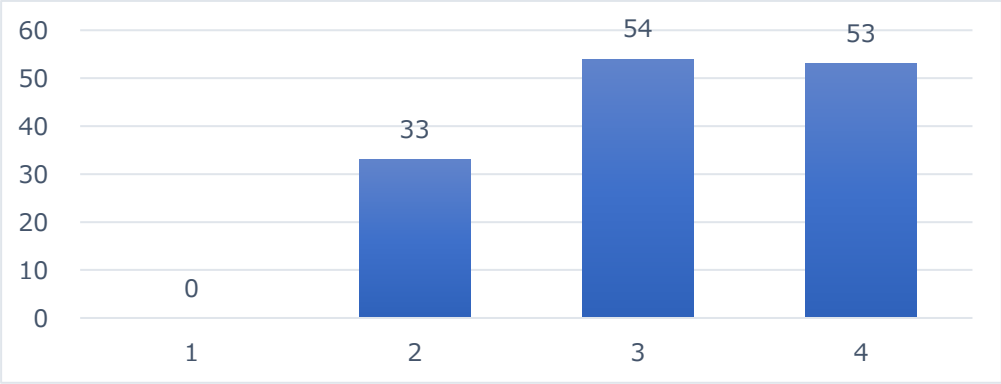
No	不正プログラム検知内容	累積件数
1	request_9028.xls	4
2	notice-8558.xls	4
3	請求書.doc	3
4	faktur 10.2020-VS711...	2
5	Invoice_576810_67148.xlsm	1
6	SEO-Pricelist.html	1
7	841982.xls	1
8	BIZ_04G48W9MVBTL8YG_RL_10162019.doc	1
9	1_Total_New _Invoices...	1

IPS 検知　内訳　（表 24）

No	IPS 検知内容	件数
1	4043309056:TCP Land:MISC:RFC 793	378
2	1133253:WEB Remote Command Execution via Shell Script -1.h:msf; CVE-2016-unknown	88
3	1050015:WEB Cross-site Scripting -34:CVE-2011-2133; CVE-2014-4116; CVE-2017-7309	71
4	1058626:WEB Generic XXE Information Disclosure -1:CVE-2018-10613; CVE-2018-3600; EDB-32623; CVE-2013-5014; CVE-2013-6447; CVE-2013-6429; CVE-2014-0002	34
5	1136426:WEB Remote Command Execution via Shell Script -3:msf; CVE-2016-unknown	27

6	1056055:WEB PHP CGI Argument Injection:CVE-2012-1823; msf	25
7	1132663:FILE Windows PDF Remote Code Execution Vulnerability （CVE-2016-3203）:CVE-2016-3203; MS16-068;ZDI-16-369	15
8	1136426	13
9	1133254:WEB Remote Command Execution via Shell Script -1.b:msf; CVE-2016-unknown	12
10	1056916:EXPLOIT HP Universal CMDB Server Axis2 Default Credentials Remote Code Execution:http://retrogod.altervista.org/9sg_ca_d2d.html; CVE-2010-unkn	7
11	1136521	4
12	1134610:WEB Dasan GPON Routers Command Injection -1.1 （CVE-2018-10561）:CVE-2018-10561; CVE-2018-10562	4
13	1133679:SSL OpenSSL ChaCha20-Poly1305 and RC4-MD5 Integer Underflow -2 （CVE-2017-3731）:CVE-2017-3731	3
14	4043309087:Bad TCP Flag:MISC:RFC 791	3
15	1057783:FILE Microsoft Office PNG File Handling Buffer Overflow （CVE-2013-1331）:CVE-2013-1331; MS13-051	3
16	1056167:WEB Cross-site Scripting Attempt -12:CVE-2012-0296	3
17	1111071:FILE Microsoft Word Global Array Index heap overflow -1 （CVE-2008-4026）:CVE-2008-4026	3
18	1055299:ICMP Microsoft Windows TCP-IP Stack ICMP Sequence Denial of Service （CVE-2011-1871）:CVE-2011-1871;CVE-2011-2013	2
19	1055299	2
20	1055396:WEB Cross-site Scripting -9:CVE-2010-0817;CVE-2011-1976;CVE-2011-2260;CVE-2011-2710;CVE-2012-0017;CVE-2012-0551;CVE-2012-0719;CVE-2012-1859;CV	2
21	1051723:VIRUS Eicar test string -1:http://www.eicar.org/anti_virus_test_file.htm	1
22	1112775:EXPLOIT Adobe Photoshop CS4 ABR File Processing Buffer Overflow -3 （CVE-2010-1296）:CVE-2010-1296; APSB10-13; ZSL-2010-4940; SA39934; BID:40389	1
23	1056281:FILE Photodex ProShow Producer 5.0.3256 load File Handling Buffer Overflow （BID-54264）:CVE-2012-unknown; EDB-19563; BID-54264; msf	1
24	1054837:WEB Remote File Inclusion /etc/passwd:BID:65874; CVE-1999-0262; CVE-2007-1277; CVE-2011-0405;CVE-2011-0518; CVE-2011-4716; CVE-2012-5192; CVE	1
25	1059406:SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -1 （CVE-2014-0160, Heartbleed）:CVE-2014-0160; msf	1
26	1050700:WEB Cross-site Scripting （document.cookie） attempt:CVE-2010-1663; CVE-2012-0007; CVE-2012-0010;CVE-2012-1861; CVE-2013-6039; CVE-2013-1942; C	1

Web サイトブロック　（表 25）



Web サイトブロック 内訳 （表 26）

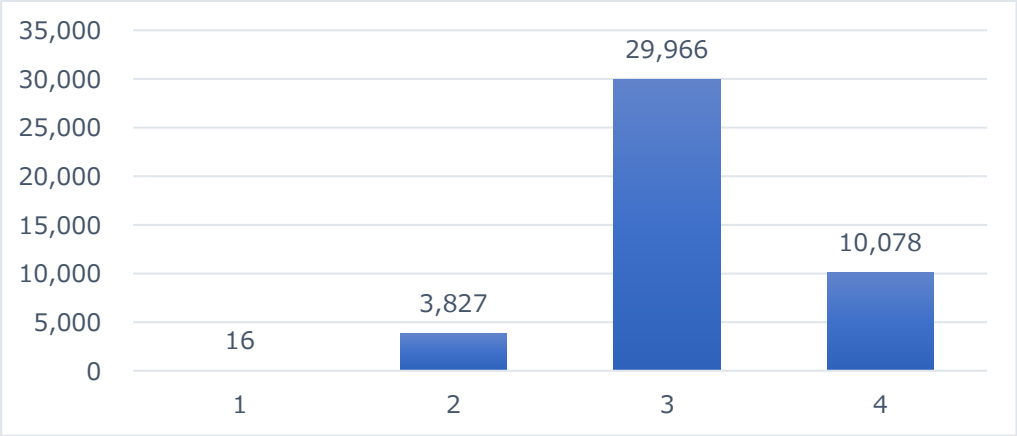
No	Web サイトブロック内容	件数
1	log.theby.in	58
2	www.5ipikapika.com	6
3	d24ak3f2b.top	6
4	useurmind.com	4
5	click.mnmnck.com	4
6	gda6-75.waste-pat.com	4
7	peachtrackercn.com	2
8	www.bettyslash.jp	2
9	csiag.xyz	2
10	saipure.shop	2
11	www.tow nofmountainvi...	2
12	sexydb.xyz	2
13	www.masksjp.xyz	2
14	gassite.xyz	2
15	libhigashimatsuyama.shop	2
16	e81q-33.cheatintroduction.net	2
17	h3r2r-al.stretch-range.com	2
18	cosmic-tools.de	1
19	funcouncil.fun	1
20	greenfinanceobservat...	1
21	shoping.valueress.to...	1
22	triga-it.de	1

23	www.blue-hot.com	1
24	eservice.appfavorite...	1
25	hotelsinfo.top	1
26	baby-potato.tokyo	1
27	mimiko-1023-go.tokyo...	1
28	chgkfdgfko.com	1
29	iyfsearch.com	1
30	www.cr.mufg.marinaw r...	1
31	fangpenlin.xyz	1
32	carehoter.com	1
33	infoscience.xyz	1
34	law yermon.fun	1
35	team-yellow .de	1
36	www.farmacianuovafer...	1
37	aucsupplementcafe.xy...	1
38	www.w intercoatsjp.co…	1
39	8w tkfxiss1o2.com	1
40	verycheapl.com	1
41	r1258178.imusby.com	1
42	onnhot.shop	1
43	raanlymq.shop	1
44	haveulot.store	1
45	tare.pro	1
46	buyworths.top	1
47	manuqas.com	1
48	www.downjackatjp.com	1
49	hotelsbeing.xyz	1
50	buying.iceshyme.shop	1
51	polimer.xyz	1
52	mailprinter.xyz	1
53	topstuff.xyz	1

スパムメール検知

スパムメールは宣伝目的のものからフィッシングサイトへの誘導やウイルスへの感染を引き起こすものもある。受信者の意向を無視して一方的に送付される迷惑メールを検出する。

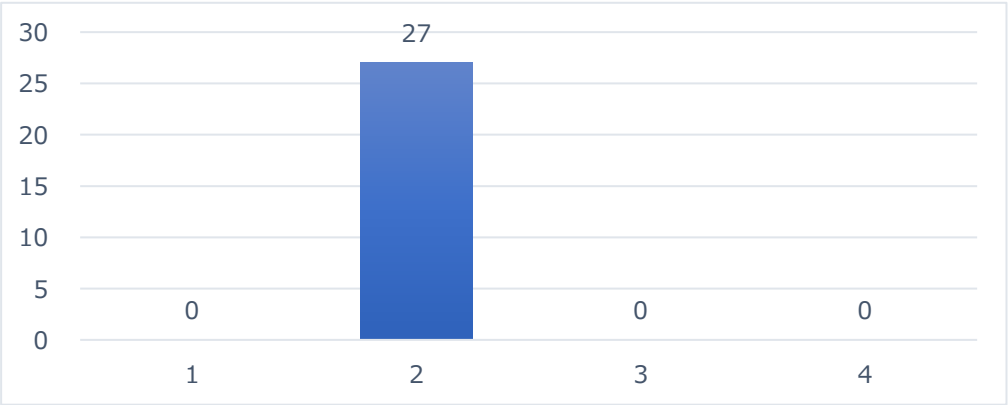
スパムメール検知　月別状況　（表 27）



ランサムウェア検知

ランサムウェアとは PC 内のファイルを暗号化、もしくはロックすることで使用できない状況に追いこみ、元に戻すことと引き換えに「身代金」（Ransom）を要求する不正プログラム。2017 年には「WannaCry」と呼ばれるランサムウェアが世界で流行し、多くの被害をもたらした。

ランサムウェア検知　月別状況　（表 28）



コールセンター等への相談・対応内容 （表 29）

対応種別	件数	相談・インシデント等対応状況
コールセンター対応	1 件	UTM の設定変更依頼を受領し、サポートセンターにて遠隔で対応を実施
その他訪問対応	3 件	・過電流による UTM 機器故障のため、装置取り替えを実施 ・インターネットへの接続が断続的に切断されるため、切り分けのため訪問（実証参加企業資産のルーター故障） ・インターネットへ接続でき無いため、切り分けのため訪問（アクセス回線不良）

4.3.2. セキュリティ対策の実態把握

STNet 標的型メール訓練サービス

参加企業数 （表 30）

実施社数	30 社
対象者数	第 1 回 4,155 名
	第 2 回 4,156 名

開封結果

標的型攻撃メール訓練での平均開封率は、第 1 回 13.8%、第 2 回 10.4%であり、今回の参加企業・団体全体の開封率は第 1 回、第 2 回ともに平均を上回る結果となった。その反面、第 1 回と第 2 回では一定の改善が見られ、訓練を実施したことによる教育効果が表れていると判断できる。

今回実施した訓練は継続的に行うことで、その効果を高めることが可能である。今回の参加企業・団体で今までに標的型攻撃メール訓練の実施経験が少ない、もしくは初めて実施した企業・団体が多い場合は、今後も同様の訓練を継続的に行うことで改善できる可能性が高いと思われる。

実施回別開封率および改善率（表 31）

第 1 回配信			第 2 回配信			改善率① 開封率比較	改善率② 開封件数比較
対象者	開封者	開封率	対象者	開封者	開封率		
4,155	746	18.0%	4,156	523	12.6%	5.4%	29.9%

※改善率①とは （第 1 回開封率 － 第 2 回開封率）

※改善率②とは （第 1 回開封者 － 第 2 回開封者）÷ 第 1 回開封者

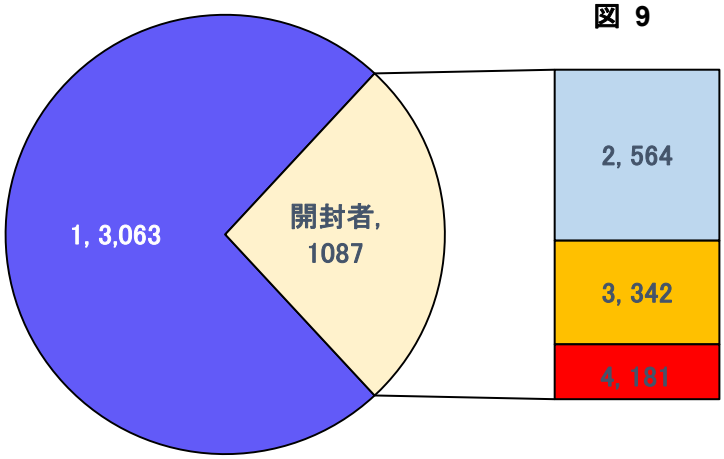
※「開封」とは 次のどちらかの操作を行うこと

- 添付ファイルの開封操作
- メール本文内 URL のクリック操作

全体学習効果分析

対象者全体の約 4 人に 1 人は開封しているという結果になった。攻撃者は様々な手法でメールを送り付けて開かせようとするので、訓練でも色々な文面や形態で実施することが肝要だ。

図 9



開封結果および学習効果率（表 32）

第 1 回訓練のみ		第 2 回訓練のみ		両方とも開封	
開封者	開封率	開封者	開封率	開封者	開封率
564	13.6%	342	12.6%	181	4.4%
対象者数	学習効果率※1	開封者※2		非開封者	
		開封者	開封率	非開封者	非開封率
4,150	75.7%	1,087	**26.2%**	3,063	73.8%

学習効果率 ※1　第 1 回のみ開封者数 ÷ 第 1 回開封者数

開封者 ※2　第 1 回訓練のみ開封者数 + 第 2 回訓練のみ開封者数 + 両方とも開封者数

※訓練対象者の退職等により、訓練対象者数と学習効果分析の対象者数は一致しない場合あり。

文面の話題に関連した傾向 （表 33）

配信回	文面（タイトル）	採用社数	対象者	開封者	平均開封率
1 回目	社内アンケートに関するご協力のお願い	11	1377	211	15.3%
	JavaScript などに関する注意喚起	5	622	88	14.1%
	テレワーク導入についてのアンケート	5	733	130	17.7%
	あなたのアカウントがロックされました	3	335	59	17.6%
2 回目	テレワーク導入についてのアンケート	8	1615	346	21.4%
	あなたのアカウントがロックされました	5	228	13	5.7%
	外部監査の実施について	3	460	45	9.8%
	給与支払日変更について	3	68	6	8.8%
	JavaScript などに関する注意喚起	3	194	12	6.2%

1 回目、2 回目ともにテレワークに関連する文面が比較的開封率が高い傾向にある。興味深いのは、2 回目にテレワークに関する文面を選択した企業・団体（8 社）において、1 回目からの改善率が全体平均の 5.4%（P.6 改善率参照）を上回った企業は 8 社中 1 社しかない。つまり一般的に開封率が下がる傾向にある 2 回目において改善状況が芳しくない結果となっている。これは新型コロナの影響で全国的にテレワークに取り組む企業・団体が増えたことと無関係ではないと思われる。

4.4.　報告会等による成果の周知（表 34）

日　　時	2020 年 1 月 13 日（火） 14 時～16 時	
場　　所	高松商工会議所およびオンライン配信（Webex）	
出　席　者	31 社/32 名 （高松商工会議所にて 3 社/4 名、オンラインにて 28 社/28 名）	
報　告　会	テ　ー　マ	令和 2 年度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：香川県）報告会
	登 壇 者 （発言順）	（株）STNet キヤノンマーケティングジャパン（株） 西日本電信電話（株）高松商工会議所
質 疑 応 答	①現在、サイバー保険はどんなものがあるのか。 →日本商工会議所のビジネス総合保険の特約および UTM 等機器の付帯保険について説明。 ②UTM の検知結果において、キヤノンマーケティングジャパンは DoS/DDoS 攻撃が多いとのことだが、NTT 西日本の検知結果項目に DoS/DDoS 攻撃の記載が無い。DoS/DDoS 攻撃は検知しないのか。 →同一 UTM ではないため検知結果項目名が異なっているが、NTT 西日本の UTM でも DoS/DDoS 攻撃は検知している。IPS 検知件数に含まれている。	
ご　案　内	内　　容	中小企業サイバーセキュリティ対策促進事業について
	登 壇 者	四国経済産業局地域経済部
セ　ミ　ナ　ー	テ　ー　マ	中小企業のための情報セキュリティセミナー
	登 壇 者	セキュリティプレゼンター
アンケート内容	① 独自アンケート （報告会後、実証参加企業より回答、44 社） サイバーセキュリティ対策状況（人材面）について･･･3 問 取引先からのセキュリティ対策の要求について･･･1 問 サイバー攻撃の有無および対策状況・費用について･･･5 問 サイバー保険について･･･3 問 今後のサイバーセキュリティ対策について･･･3 問 実証に対する満足度について･･･5 問 テレワークについて･･･3 問 サイバーセキュリティ対策を行う上での課題について･･･1 問 ② 新！5 分でできる情報セキュリティ自社診断 （報告会後、実証参加企業より回答、28 社）	

※コロナ対策のため、オンラインを併用して開催。

5. 考察

5.1. 実証参加企業におけるサイバー攻撃の実態

5.1.1. ネットワークセキュリティ機器 UTM の設置による分析

（1）既にメールアドレスが流出している場合、攻撃対象となりやすい

NTT による検証では、不正プログラム検知は全てメールによる検知であった。元々Emotet 等に悩まされているユーザーで検知しており、既にメールアドレスが流出し、攻撃対象であったと推測される。

（2）Land 攻撃の脅威

NTT による検証では、I PS 検知は半数以上を Land 攻撃（DoS 攻撃の一手法で、宛先 IP アドレス/TCP ポート番号と、送信元 IP アドレス/TCP ポート番号とを同一にした TCP 接続要求を大量に送り込み、サービスを停止させる手法の攻撃）が占め、旧来からの攻撃が続いている。また、特定の 1 社で約 55%を占めており、「固定 IP の利用」、「サーバの公開」、「リモート接続」等はないことから、外部からの標的とされそうな原因は見受けられない状況であるが、必要に応じ状況確認をしておく必要がある。

（3）11 月のスパムメールについては、「Emotet」および「IcedID」等の攻撃か

11 月に検知数が大幅増。JPCERT/CC 等から注意喚起されている、「Emotet」および「IcedID」等の攻撃があったと推測される。

（4）不正 URL によるセキュリティリスク

ランサムウェア検知は、1 社のみ特定の日に 1 つの Web サイトに対して検知しており、利用ユーザーが不正と思われる URL にアクセスしようとした結果である。

（5）都心部だけでなく、地方においても、また業種問わずセキュリティリスクは顕在化

短い実証期間ながら、NTT による検証では、24 社中 19 社は、何らかの検知をしており、地方においても、また業種に関わらず、サイバー攻撃を受け、インシデントが発生する可能性があることを改めて認識した。

5.1.2. セキュリティ対策の実態把握

（1）サイバーセキュリティに対する危機意識の醸成・深化・浸透を

本実証の被験対象には、地域有数の事業規模のある企業も多数含まれる。そのような中、当県の実証メール開封率は、他地域で実施されたそれと比して、開封率が高い（セキュリティリスクが高い）傾向にあることがある。当県の実態としては、危機意識の醸成・深化・浸透のための啓発がより強度なレベルで必要であると言える。

（2）継続的な訓練に効果がある

1 回目、2 回目ともに他地域と比して高い開封率であったが、2 回目の訓練の結果より一定の改善が見られていることから、1 回目の訓練の結果を受け、被験企業の経営陣・管理者に意識的な変化があったこと、社員教育の実施により被験企業全体のセキュリティ対策に関するボトムアップが図られていると推察できる。3 回目、4 回目と実施すことで開封率は逓減すると想定され、継続的な訓練が効果を有すると思料する。

（3） 時事・トレンドを踏まえた攻撃への対象が求められる

テレワークを盛り込んだメールの開封率が高いことから、経営陣・管理者は時事・トレンドを組み込んだ攻撃を想定し社員教育を図ること、あるいは標的型メール識別のポイントに関する全社的な理解を浸透させる必要があると考えられる。

5.2. 中小企業におけるセキュリティ対策を進める上での課題（表 35）

① 関心・検討のきっかけづくりが必要
実証に参加し、現状を把握できたことで、早急に対策の検討・導入を進める実証参加企業があったことを踏まえ、情報セキュリティセミナーをはじめとした啓発活動の実施が必要である。 なお、高松商工会議所においては高松商工会議所行動計画（令和 2 年～6 年）における基本目標①「IT・ IoT の実装による生産性向上」に基づき、IT・ IoT の実装と並行し、サイバーセキュリティについても実施事業内にて浸透を図って行いきたい。また、将来的に高松商工会議所独自のサイバーセキュリティ対策サービスを検討することも視野に入れたい。
② 商品・サービス利用料が高価である
サイバーセキュリティ対策の導入検討に値する価格として 10,000 円以内という結果が示された。 これを実現するためには、 i. 事業規模・使用状況に合わせた機器の選択を可能とすること（ネット回線接続状況：～10 台、～30 台、～50 台、～100 台） ii. コスト高となる過剰なサービスを見直し（24 時間 365 日対応可能なコールセンターのオプション） iii. 将来的な保険補償範囲の適正化（既存商品における UTM に自動付帯される保険が過剰・不足している） iv. 将来的な最適保険商品の開発（中小企業にとって導入しやすい価格と過不足無いサイバー保険の商品開発） を検討する必要がある。 また、ベンダーとしても、商品開発に係るコスト、商品バリエーションが増えることによる管理コストが増えることから、地域特性を重視した各々の商品を地域ごとに保有するよりは、対中小企業向け商品として、全国共通モデル（お助け隊ブランド商品）によるスケールメリットを取りに行く（推奨する）方が望ましいと言える。
③ 相談窓口が無い
必要な対策が分からない、自社の状況を把握したいが方法が不明との声に対応し、高松商工会議所などの支援機関、セキュリティ簡易診断の紹介等、入り口となる支援を行う。また、機器導入にあたっては、最低限の機能として、インシデント・事故が発生した際の相談窓口等のサービスやサイバー保険の付帯をするべきである。

5.3.　中小企業において必要なセキュリティ対策

5.3.1.　UTM の継続的設置および設置常態企業の普遍化

本実証では、実証期間が短いながらも、被験企業において少なくない数の攻撃が探知された。重要な情報資産を守るためにも、インシデントの発生を未然に防ぐ効果の期待できる UTM を自社においては継続的に設置し、かつ同社とサプライチェーンを構成する企業においても設置が常態化していることが望まれる。

5.3.2.　継続的な訓練による社員全員の危機意識の底上げ

標的型メール訓練の結果を見ても分かるように、反復により一定の効果が得られる。経営陣・管理者のみならず、社員全員がセキュリティリスクに目を向けるための、継続的訓練などの社内での仕組みづくりが必要である。

5.3.3.　セキュリティ担当者の設置の普遍化

30 名以下の小規模企業においては IT 担当者、セキュリティ担当者というように明確な役割を持つ人格が不在である傾向にある。これは、経営陣の危機意識の欠如を示唆しており、またインシデント発生時の初動にも大きく影響する。経営陣の啓発とともに、社内インフラとしてのセキュリティ担当者の設置を推奨・支援していく必要がある。

5.4.　中小企業におけるセキュリティ対策の効果

本実証においても、実証参加後にその効果を感じ、UTM を自費で継続して設置することを決めた企業がおり、設置までは至らない企業も実証後のアンケートによりセキュリティ対策に係る意識レベルに改善が見られた。よって、5.3 の対策に取り組むことにより

① 中小企業のセキュリティリスクへの理解と危機意識が高まり、
② 中小企業全体のセキュリティ対策の底上げを図ることができ、
③ ひいてはそのサプライチェーンを構成する大企業を含む日本の企業全体における情報資産の保護に繋がる

と言える。

6. 実証を踏まえたビジネス化に向けた検討

6.1. サイバー保険の活用

6.1.1. サイバー保険の必要性・認識

一般的なサイバー保険では、情報漏洩などの重大インシデントに対する第三者賠償とインシデント発生時の原因調査、データ復旧などの各種対応費用を保険で補償するものとなっているが、今回アンケート回答した企業の 66%がサイバー攻撃による被害で「第三者賠償」と「各種対応費用」をともに脅威を考えており、保険に対するニーズは一定あるものと推察することができた。

しかしながら、「サイバー保険の必要性」にて保険に対するニーズは一定あるものと判断できたものの、実際の加入率は 16%となっており、また、「加入していない」と回答した企業の 48%が「自社に適した補償内容や保険料が分からない」理由によるものであることから、現時点では多くの中小企業が保険加入までに至らない潜在的なニーズとなっている状況と推察される。

◆サイバー攻撃による被害でより脅威と感じるのはどちらですか？（表 36）

事業中断（データ復旧や原因調査、再発防止に係る費用が発生）	16%
情報漏えい（第三者への賠償費用が発生）	16%
事業中断・情報漏えいの両方	66%
答えたくない/不明	2%

◆現在、サイバー保険へ加入されていますか？（表 37）

加入している	16%
加入していない（自社に適した補償内容や保険料が分からない）	36%
加入していない（必要性を感じていないため）	5%
加入していない（満足する内容のものがないため）	2%
加入していない（予算がないため）	7%
加入していない（その他）	25%
答えたくない/不明	9%

サイバーセキュリティ対策における優先順位

サイバーセキュリティ対策において求めるものとして「保険」と回答した割合は 26%であることから、重大インシデント発生時のリスクファイナンス機能を有する保険の重要性の認識が低いと考えられ、事後対応の観点からのセキュリティ対策に対する意識醸成が必要であると考える。

このことより、サイバー保険の普及には補償額、補償範囲、保険料水準といった保険設計面での検討だけでなく、サイバー保険の必要性をどのように訴求していくか検討することも重要であると考える。

◆今後セキュリティ対策に関するサービスについて求めるもの（複数回答）（表 38）

安くて限定された箇所のみ対策をする商品・サービス	35%
高くても包括的な対策をしてくれる商品・サービス	16%

相談窓口	26%
いざという時の保険	15%
その他	1%
答えたくない/不明	6%

6.1.2. サイバーセキュリティ対策に対するコスト

サイバーセキュリティ対策において「答えたくない/不明」を除く有効回答の 92%が何かしらのセキュリティ対策を講じており、半数が月額 1 万円以上の費用負担をしている結果となった。

また、サイバー保険においては「答えたくない/不明」を除く有効回答の 90%が月 1 万円以内で検討する結果となった。

この結果によりサイバーリスクが一定認識されてきていることが考えられるが、現在のコスト以上の費用負担は難しいという意見も複数あることから、中小企業が継続して利用可能なサービス（保険）を幅広く展開していくためには、必要最低限のサービス（保険）を基本サービス（保険）とし、以外についてはオプションとして位置付け提供していくサービス（保険）体制を構築する必要があると推察する。

◆現在、情報セキュリティ対策にかけている月額の費用（表 39）

（サイバー保険費用を含む。情報システム担当者の人件費を除く）

1,000 円未満	2%
1,000 円～3,000 円	7%
3,001 円～5,000 円	7%
5,001 円～10,000 円	16%
10,001 円～15,000 円	11%
15,001 円以上	39%
対策は行っていない（0 円）	7%
答えたくない/不明	11%

◆今後、サイバー保険へ加入する場合、減額いくらであれば検討しますか？（表 40）

1,000 円未満	5%
1,000 円～3,000 円	9%
3,001 円～5,000 円	16%
5,001 円～10,000 円	25%
10,001 円以上	5%
答えたくない/不明	41%

6.1.3. サイバーリスクにおける意識醸成

上記考察で挙げたサイバー保険におけるニーズの顕在化、必要性の訴求といった課題の対策として、損害保険会社が提供する無料診断サービス等の活用を検討する。

今回の実証事業に加えて、この対策を実施することによりサイバー保険加入の必要性の認識を高め、サイバー保険加入率の向上を実現させる。

6.1.4. 実施検討中のサービス

サイバーセキュリティリスク診断
サイバー攻撃対策として考慮すべき「組織的」「人的」「物理的」「技術的」な対策を中心としてサイバーリスクへの対応状況を診断し、サイバー攻撃が生じた場合の「予想損失額」をリスクシナリオに基づき算出
Web アプリ簡易診断
企業 Web アプリおいて 3 つのカテゴリ（暗号通信確認、サーバ設定に関する不備、既知の脆弱性）、15 項目の必要最低限の脆弱性を簡易かつ迅速に検出

6.1.5. 保険組成

上記考察で挙げた中小企業が負担するコストの課題を踏まえ、サイバー保険を広く普及させるために、セキュリティサービス提供企業全てに必要最低限の補償とした保険を自動付帯し、企業ごとのリスク実態に合わせて不足する補償を上乗せの個別加入により補完する保険組成を検討する。

① セキュリティサービスへのサイバー保険自動付帯

サイバー保険自動付帯の組成においては、UTMなどのハード機器に保険を付帯する方式が一般的となっているが、セキュリティサービス運営において必須である管理サポートサービスに保険を付帯することも検討する。

補償内容については、必要最低限の第三者賠償と掛け付け費用などの初動費用、フォレンジック費用（50 万円～100 万円程度）での組成を検討しており、セキュリティサービス全体において検討可能な価格帯に応じた保険料に設定する。

② 上乗せカバーの補償

前述の無料診断サービスを活用することにより、企業ごとのリスク実態に合わせたカスタマイズした補償内容の保険設計が可能となる。保険料については、セキュリティサービス加入企業に限定し、割引率の高い団体保険制度を立ち上げることも検討していく。

また、スケールメリットがあり保険料の割引率が高い全国制度商品の展開も検討しているが、①サイバー保険自動付帯の補償と重複となってしまう課題があることから今後一定の整理が必要と判断する。

6.2. 中小企業向けセキュリティのビジネス化に向けた課題・検討

（課 題 ①）関心を持つきっかけが無い（啓発が必要である）

（検討内容）高松商工会議所行動計画に基づき、会員事業所の IT 化と並行したサイバーセキュリティ対策の必要性の周知を行う。具体策として、セミナーの開催や部会委員会における講演会、勉強会を実施する。

（課 題 ②）中小企業が負担できるコストに比して実売価格が高い

（検討内容）今回使用した UTM については、オプション等の取り外し、事業所のネット回線接状況による申し込みプランの変更によるコスト削減を行う。

新商品開発については、IPA が今後検討することとされている「お助け隊サービス」ブランドの要件に適合するような費用や機能等の検討を実施する。

販売窓口自体を増やす（香川県全域の中小企業へ案内する場合、各商工会議所・商工会と連携する等）ことにより見込販売数増加が図れ、商品に含まれる固定費部分が薄まり、結果商品単価の低廉化を実現することができる。

（課 題 ③）インシデント発生時等の相談・支援窓口がない、あるいはわかりづらい

（検討内容）「相談サービス＋保険による補償」のパッケージ化商品の開発

既存の商品は、UTM 設置と簡易保険がセットになったものが主流である。ただ、課題①に示すように、UTM の設置に至るにはまだまだ啓発による危機意識と対策意識の喚起が必要である。

そこで、UTM の設置を絶対条件としない新サービス（例えば、Ⓐ事業所内のネットワーク環境の事前調査とⒷ平常時の相談窓口とインシデント発生時にⒶの事前調査に基づいた原因調査や支援をセットにしたもの）と、発生した被害に対する保険を組み合わせた商品の開発を検討する。

一方、UTM を設置している企業に対するサービスとしては、設置しっぱなしになり、企業側に設置していること自体の認識がない事例が見られたことを踏まえ、UTM 設置ベンダーがモニタリングレポートを定期的に報告し、企業側に設置している認識を持たせるとともに、インシデント発生時には UTM 設置ベンダーが第一の相談窓口として活用されるような認知体系の構築が必要である。

また、モニタリングレポートを踏まえた対策の提案・導入や、多重防衛として有効な対策の紹介等、現在ベンダー側が営業的側面から行っている支援策についても、当然に UTM 設置・モニタリングに含まれるサービスとして組み込むことで、サイバーセキュリティ対策を推し進められるのではないかと考える。

7. 総括

香川県において、中小企業のサイバーセキュリティの実態に関する目ぼしい調査はこれまでになく、またそれは高松商工会議所の知る限り四国地域においても同様であった。そこで、本実証事業では、四国経済の核である香川県高松市を中心とし、当該地域のサイバーセキュリティ対策について調査をすることで、俯瞰的に四国地域の実態を把握するための足掛かりとするべく取り組んだものである。

実証結果については前述のとおりであり、当該地域の中小企業の実態を一定、明らかにすることができたと考える。総括としてここで述べるべき成果としては、実証用機器の設置やサービス実施に先立ち、説明会の開催による集団的、損害保険会社・ベンダーによる個別的啓発により、中小企業へのセキュリティ対策の意識醸成を図れたことを述べたい。本実証事業により、被験者となった 70 企業のほか、実証参加の検討依頼などで総数にして 100 社を超える企業に、サイバーセキュリティの必要性を説くことができた。この意味で、中小企業の課題とされるセキュリティリスクに関心を持つきっかけをつくることに、大きく資するものであると言える。また、企業にとっては、UTM 導入や標的型メール訓練実施に係るコストを金銭的負担なく取り組めるということが大きな切り口となり、事業参画を決めた実証参加企業も往々にしてあったが、結果として、啓発が実現したことで、UTM の継続設置を決めた実証参加企業も少なからずあり、標的型メール訓練により経営陣が会社全体のセキュリティリスクの理解を得て、対応策を検討することにも繋がった。

実態把握に関する実証事業は、来年度以降は実施されないと聞き及んでいるが、実証後の課題にも挙げたとおり、商品サービスのコストが課題となり、かつ本実証事業による試験的な UTM やサービスの導入より、結果として啓発活動が効果的に行えたことを踏まえれば、試験的導入に関する継続的な支援は中小企業のサイバーセキュリティ対策の全体的な底上げに繋がると思料する。

さて、今後について、高松商工会議所では、総合経済団体・中小企業等の支援機関として、本実証事業の結果を元に、ベンダー・損害保険会社と継続的に連携し、お助け隊ブランド化に合わせた商品造成を検討していくほか、セキュリティ対策の必要性を周知する啓発活動を行い、IT 化/導入の推進および相談機能の強化を合わせて進めていく所存である。

以上