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：岩手県、宮城県、福島県）

成果報告書

請負事業者：株式会社デジタルハーツ

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

目次

サマリー

本報告書は、株式会社デジタルハーツ（以下「デジタルハーツ」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。

岩手県、宮城県、福島県内の中小企業 56 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。

- 環境調査
- 標的型攻撃メール訓練
- 脆弱性診断（簡易）
- ユーザーサポート（インシデント発生時の駆けつけ支援を含む）
- UTM 監視
- MDR 付き EDR
- 脆弱性診断（詳細）

1. 背景・目的

1.1 背景

デジタルハーツは、令和元年度のサイバーセキュリティお助け隊事業において岩手県・宮城県・福島県での実施主体として実証事業（以下「昨年度事業」という。）を実施した。

当初は実証参加企業の獲得に苦労したが、地域経済団体からの紹介などを通じて徐々に現地での信頼を得られるようになった。同地域では、サービスの品質や技術力もさることながら、一過性の取り組みではなく長期にわたってしっかりと東北に根付いて実施することが高く評価されることが分かった。

また、昨年度事業の実施に当たって、監視装置の設置などのソリューションを提供する以前の問題として自社ネットワーク環境の現状把握もままならない中小企業が多数を占めていた現状を踏まえると、まず共通事項として簡易な現状把握を実施した上で、各社の置かれた状況に応じた個別のソリューションを提供することが必要であることが分かった。

こうした昨年度事業から得られた示唆や、実証事業内容（仕様書）に記載されている背景・目的を踏まえ、①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、②中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを目指して、今年度のサイバーセキュリティお助け隊事業（以下「今年度事業」という。）を行うこととした。

1.2 目的

昨年度事業では、①サイバーインシデント実態の可視化、②地域のサイバー対策強化、③中小企業向けサイバーセキュリティ対策の事業化という３つの基本コンセプトに沿って実施した。このうち、①サイバーインシデント実態の可視化については、専門性の高さから中小企業の理解を得ることは容易ではなく、基本的な内容の普及啓発を粘り強く実施していくことが重要であることが分かった。また、②地域のサイバー対策強化に関しては、事業説明会などにおいて公的機関からの関連政策の紹介などに対して参加者から良い反応が得られたことから、今後も公的機関が関与する取り組みとして継続的に行っていく必要があることが分かった。③中小企業向けサイバーセキュリティ対策の事業化に当たっては、セキュリティセンサーの設置といったハードウェア提供のみならず、ネットワーク環境の現状把握や有事の駆けつけ対応などのサービス提供も含めたサービス全体でのビジネスモデルを検討する必要があることが分かった。

こうした昨年度事業の成果を踏まえつつ、今年度は、①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観点から、事業説明会および報告会の開催や情報ポータルサイトの更新を通じた啓発活動を行う。また、②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観点か

ら、50 社の実証参加企業を獲得し、複数のサービス・製品の提供を通じて必要なサービスの水準や要するコストなどの把握を行い、実証終了後の有償サービスを設計することを目的として、今年度事業を行うこととした。

2. 実証事業の概要

2.1 実証対象（地域／産業分野）の選定

昨年度事業では、以下に示す理由により岩手県・宮城県・福島県の 3 県を対象とすることとしたが、現在も引き続き同地域は経済規模としては小さいもののサプライチェーン上の重要な位置づけであることに変わりは無く、2019 年 10 月に発生した台風 19 号では大きな被害が発生しており復興の途上にある。また、新型コロナウィルスの感染者は他地域と比較して低く抑えることができているが、今後の経済活動の再開を見据えると新しい生活様式を実践するためにも IT 技術の活用は不可避であり、それと一体的なサイバーセキュリティ対策を早急に進めていく必要がある。一方で引き続き東北地域は経済規模が小さいことから民間企業の視点からはどうしても規模の経済が働く大都市圏を中心にサービス提供が検討されがちになり、公費を投入しなければ同地域にサイバーセキュリティ対策の意識を根付かせることは難しい。

デジタルハーツは昨年度事業を通じて同地域における一定の信頼関係を構築しており、今年度も継続して実証事業を実施することにより同地域の面的なサイバーセキュリティ対策の底上げが可能となることから、今年度においても引き続き同一地域（岩手県・宮城県・福島県）を実証地域として選定することとした。

①サプライチェーン上の重要性

東北地域は、首都圏や名古屋、大阪といった主要都市と比較すると経済圏としては小さいものの、自動車産業や電子部品産業などにおけるサプライチェーン上の重要な位置づけとなっている。サイバー攻撃はサプライチェーン上の脆弱な組織が攻撃対象となりやすいことを踏まえれば、東北地域の中小企業におけるサイバーインシデントの実態把握を軽視することはできない。

例えば、岩手県および宮城県内にはトヨタ東日本の生産工場があり、年間約５０万台の自動車が生産されている。これに伴い、多くの自動車部品メーカーなどが東北にて生産に携わっていることから、同地域におけるサプライチェーン上のリスクマネジメントを強化する必要がある。また、業種別の全国シェアでは、東北地域は電子部品・デバイス・電子回路の比率が高くサイバーインシデントのリスクが高いことが見込まれる。東北地域の中でも、宮城県は流通の要衝として東北地域内の卸売業シェアの約 50%を占めているなど、重要な位置を占めている。

②地域内のサイバー対策強化

多くの中小企業には IT の専門的知識を有する人材が不足しており、経営者が自らネットワーク構築・運用業務を行っているケースも多い。こうした場合、IT に関するトラブルが発生した場合にサイバー攻撃が原因か否かの判定が難しく、思い切った IT 活用に踏み切ることができない原因にもなっていると考えられる。

特に、東北地域は首都圏からの地理的アクセスも良く、東日本大震災からの復興も今なお国家的に重要な課題であるところ、IT 活用を進めていくことでさらなる経済成長が見込まれることから、デジタル化は喫緊の課題である。一方で、十分かつきめ細かな情報が提供されていないことから、IT 導入補助金の利用実績も少なく、IT 活用やサイバー対策に踏み切れていない現状がある。

③中小企業向けサイバーセキュリティ対策の事業化

民間企業の視点からはどうしても規模の経済が働く大都市圏を中心にサービス提供が検討されがちである一方で、サイバー攻撃はサプライチェーン上の脆弱な組織から狙われる可能性があることを踏まえれば、こうした規模の経済が働きづらい地方において優先的に公費による実証を行いサービス検討に必要な情報を収集すべきである。一方で、予算の範囲内で実証事業を行うためには、関係団体との連携や駆けつけサポートなどを効率的に行うためにも首都圏からの交通アクセスの良い場所を選定する必要がある。

以上の理由により、仙台市を中心的なエリアとして設定し、交通アクセスをかんがみて岩手県および福島県も視野にいれた事業とした。

2.2 スケジュール

以下のスケジュールで実証事業を実施した。2020 年 10 月 30 日（木）までに目標とする 50 社超の参加を獲得し、3 カ月程度の実証を行った。

2020 年 8 月 28 日（金）以降	随時、個別説明・勧誘活動を実施
2020 年 8 月 28 日（金）	一般社団法人宮城県損害保険代理店業協会主催セミナー
2020 年 9 月 1 日（火）以降	随時サービス導入を実施
2020 年 9 月 11 日（金）	盛岡工業クラブ主催セミナー
2020 年 9 月 17 日（木）	一般社団法人宮城県損害保険代理店業協会主催セミナー
2020 年 10 月 14 日（水）	損保ジャパンセミナー
2020 年 10 月 22 日（木）	損保ジャパンセミナー
2021 年 1 月 8 日（金）	実証参加企業に対する月次報告の送付（実証終了）
2021 年 1 月 19 日（火）	成果報告会
2021 年 1 月 25 日（月）	報告書提出

2.3 実証参加企業

昨年度事業において実証参加動機を質問したアンケート結果では、「知人、関係者の紹介」が最多回答となり、「現状対策の客観的な意見を聞くため」という回答も多く寄せられた。また、昨年度の獲得手段別の企業数に関しては、自社・地場企業での開拓や地域団体からの紹介が中心であった。

Q.参加動機は何ですか？（複数回答）

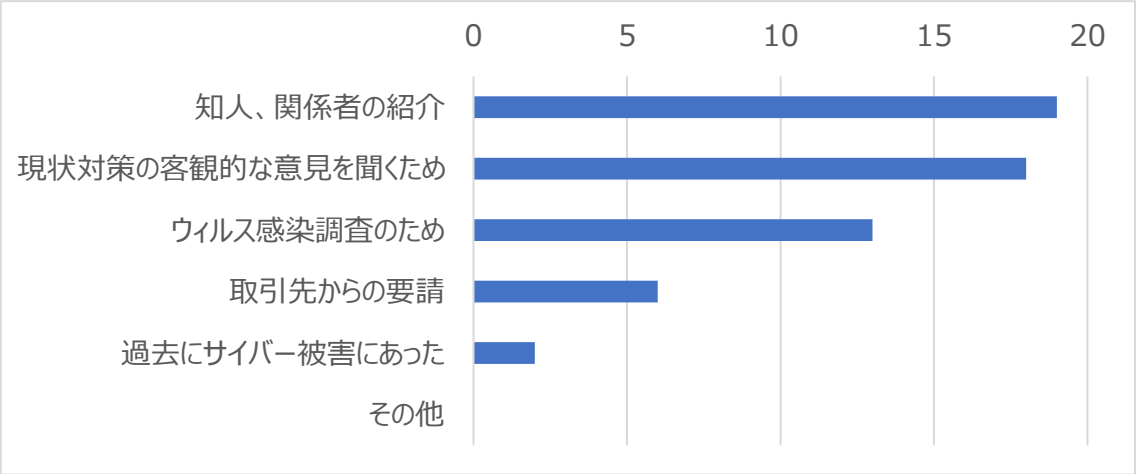

図 1：参加動機（昨年度）

	アプローチ	申込		機器設置		
	企業数	企業数	申込率	企業数	設置率	構成比
自社および地場企業での開拓	55	49	89.1%	40	81.6%	49.4%
地域団体からの紹介	110	29	26.4%	17	58.6%	21.0%
ダイレクトメール	99,500	19	1.9%	13	68.4%	16.0%
セミナー	77	14	18.2%	11	78.6%	13.6%
合計		111	ー	81	73.0%	100.0%

表 1：獲得手段別の企業数（昨年度）

こうした昨年度の状況を踏まえると、説明会などで幅広く周知する形で短期間に実証参加企業を獲得することは難しいことから、地場企業および地域団体からの協力を中心として速やかに実証参加企業 50 社を開拓していく方針とした。

具体的には、実証参加企業は、事業説明会、デジタルハーツによる募集活動、パートナー企業による募集活動を通じて獲得した。その結果は以下の表のとおりとなった。

獲得手段		アプローチ	申込	申込率	構成比
事業説明会の実施		19	1	5.3%	1.7%
デジタルハーツでの募集活動		42	21	50.0%	35.6%
パートナー企業での募集活動	株式会社 NTT 東日本-東北	9	8	88.9%	13.6%
	株式会社アライブ	31	29	93.5%	49.2%
	マンパワーグループ株式会社	1	0	0.0%	0%
合計		102	59	54.9%	100%

表２：獲得手段別の企業数（今年度）

デジタルハーツ、およびパートナー企業での募集活動は、実証対象企業へのメールでの告知と地場の担当営業にて地道な個別勧誘活動を行った。また、地場経済団体との協力活動は、共同組合仙台卸商センターによる会員企業へメール告知と、盛岡工業クラブおよび一般社団法人宮城県損害保険代理店業協会による会合を通じて募集を行った上で、デジタルハーツが個別企業に事業説明、および実証参加を希望する企業へのクロージングを行った。

その結果、今年度実証を通じた実証参加企業の募集結果は以下のとおりとなった。

内容		計画数（社）	実績数（社）				達成率（%）
			9 月	10 月	11 月	類計	
1	参加検討企業数		18	83	1	102	
2	参加申込企業数		30	28	1	59	
3	実証参加企業数	50	30	25	1	56	112.0

表３：実証参加企業の募集結果

以下に示すとおり実証参加企業は宮城県が中心となり、資本金・従業員数・業種は多岐にわたる企業から参加を得ることができた。

都道府県別	社数
岩手県	8
宮城県	43
福島県	5
総計	56

資本金別	社数
1000 万円未満	18
1000 万～3000 万円未満	23
3000 万～5000 万円未満	6
5000 万～1 億円未満	7
1 億～3 億円未満	2
総計	56

従業員数別	社数
1～5 人	9
6～10 人	8
11～20 人	12
21～50 人	14
51～100 人	5
101～200 人	6
201～300 人	1
301～900 人	1
総計	56

業種別	社数
D.建設業	6
E.製造業	10
H.運輸業,郵便業	2
I.卸売業・小売業	9
L.学術研究,専門・技術サービス業	6
M.宿泊業,飲食店	2
N.生活関連サービス業,娯楽業	1
P.医療,福祉	2
R.サービス業（他に分類されないもの）	17
T.分類不能の産業	1
総計	56

表 4：実証参加企業の内訳

2.4 実施内容

以下に示す共通サービスおよび個別サービスを提供した。

（1） 共通サービス：実証に参加する全ての企業に対して、以下のサービスを提供した。

① 環境調査

- 実証開始時に、以下の項目に沿って、書面、Web サイト、電話などを通じたヒアリングにて調査を実施。
  - 基本情報：業種、売上高、従業員数、拠点所在地などの基礎情報を確認。
  - セキュリティに対する意識調査：セキュリティの管理体制や選任担当者の有無を確認するとともに、社内での立場（経営層、情報システム部門、一般社員）ごとのセキュリティに関する意識を調査。
  - セキュリティ対策状況調査：現状導入しているセキュリティサービスや対策の状況を確認する。併せて SECURITY ACTION の取得有無を確認。
  - 社内ネットワーク環境の現状調査：社内のネットワーク構成、システム構成、端末の台数、ネットワーク回線の種類などを確認し、併せてそれらがドキュメント化されて

管理されているかを調査。

- 個別サービス選定：現状把握の結果を踏まえ、個別サービスとして提供する対策を選定。

② 標的型攻撃メール訓練

- 実証期間中に、NTT 東日本が提供する「標的型攻撃メール訓練」にて「標的型攻撃メール」を疑似体験する訓練サービスを実施。
- 実証参加企業の従業員が、ウイルス対策だけでは完全に防ぐことは難しいと言われている「標的型攻撃メール」への対策として“不審なメールを開かない”という意識がどの程度あるかの現状把握を実施。
- この標的型攻撃メールは、開封すると警告メッセージが表示され、情報セキュリティ意識の向上を促す内容とする。メール開封結果、標的型攻撃メール訓練の実施日時、送付したメール本文の内容、開封情報のグラフ、他社比較、今後の情報セキュリティ対策に関するアドバイスについてもレポート。

③ 脆弱性診断（簡易）

- 対象企業の Web サイトに情報漏えいやページの改ざんに繋がる脆弱性(弱点)が無いか、不正なサイトへのリンクが埋め込まれていないかを NTT 東日本が提供する「Web セキュリティ診断サービス」ツールにより診断。
- 診断結果については、診断完了後にメールで通知。
- 診断結果を踏まえ、個別対応が必要な場合は④ユーザーサポートにて実施する。なお、⑦脆弱性診断（詳細）を実施する場合は、診断内容が重複することから、このサービスは実施しない。

④ ユーザーサポート（インシデント発生時の駆けつけ支援を含む）

- 対象企業からの社内インフラに関する相談へのサポートおよび各個別サービスでの監視、診断結果に対するサポートを提供。
  対応時間：平日 9:00～21:00
  ・各共通・個別サービスに関するサポート・サービスに関する質問対応
  ・導入した機器のサポート
  ・セキュリティ監視に関する問合せ
  ・ウイルス除去やリカバリをサポート
  ・未知の脅威に対する駆除支援
  ・インシデント発生時の緊急駆けつけサポート

(2) 個別サービス：共通サービスで行った環境調査の内容を踏まえ、以下のサービスの中から適切と思われる内容を選択して提供。

⑤ UTM 監視

- NTT 東日本が提供する「おまかせサイバーみまもり」を活用し、UTM 機器（トレンドマイクロ社 Cloud Edge など）を対象企業のネットワークに設置し、セキュリティ対策を

強化するとともに、通信状況をモニタリングする。不正通信を行った場合など、インシデント発生の際には原因究明・環境復旧をサポート。

- 提供するネットワークセキュリティ機能

機能名	機能概要
不正アクセスブロック（不正プログラム対策/Web サイトアクセスブロック）	・不正 Web サイト、不正 URL へのアクセスをブロックすることにより不正プログラムによる感染やフィッシング詐欺の被害を未然に防止 ・万が一感染した場合も、不正な通信やプログラムによる攻撃を検知し、内部感染を早期に発見
不正侵入対策	・設定により許可された通信のみを通過させ、さらにその中から悪意ある侵入や攻撃を検知し、遮断
メールセキュリティ対策	・メールに含まれる不正プログラムの検知やスパム（迷惑）メールを判定
URL 指定によるアクセス制御	・アクセス許可されたカテゴリから特定のサイトのみをブロック ・ブロックされたカテゴリから、特定のサイトのみをアクセス許可
アプリケーション利用制限	・特定のアプリケーションからの通信を制限

表 5：UTM が提供するセキュリティ機能

- モニタリング状況報告は、月 1 回のレポート配信を行い、脅威の侵入や不正サイトへのアクセスをブロックした状況を見える化。グラフなどで視覚的な状況情報を提供し、必要な情報セキュリティ対策を明確化。

⑥ MDR 付き EDR

- 対象企業の各クライアント端末に EDR（Endpoint Detection and Response）のエージェントをインストールし、常時監視により適切な対応を支援する MDR（Managed Detection & Response）サービスを提供。
- EDR：Sophos 社の Intercept X Advanced with EDR を使用。同エージェントはディープラーニングテクノロジーを活用しており、広範なマルウェア検出が可能となっており、疑わしいファイルの DNA を 同社の脅威分析センター（SophosLabs） によって分類されたマルウェアサンプルと比較することで、攻撃の可能性を幅広くかつ専門的に分析することができる。SophosLabs は脅威の状況を常に完全可視化するために、常時、攻撃の新機能やサイバー犯罪の新技術を探索し、毎日 40 万件に上る過去に検出されたことが無いユニークなマルウェア攻撃を追跡、解体、分析している。Intercept X Advanced with EDR を使用することで、ラテラルムーブメント（内部感染行動）が実行されているかどうかを確認し、業界で最も高度なエンドポイント保護ソリューションである Intercept X のランサムウェア対策機能とエクスプロイト対策機能を活用して、複数のエンドポイントへの感

染を阻止できる。本 EDR は、少数のライセンスから安価に利用可能なため、他の EDR と比較して中小企業などへの導入が適している可能性があると判断し、本実証に採用することとした。

- MDR：エンドポイントにおけるインシデントのアラートをデジタルハーツセキュリティチームで受信、専門知識を持つアナリストが解析し、エンドポイントの隔離や、マルウェア除去などの脅威除去支援、再発防止施策支援により、脅威侵入後の対応をサポートする。また、インシデントの内容、危険度、対応方法などを、分かりやすい形にまとめて報告。
  - アラート解析：受信したアラートに関するインシデントのログを解析し、危険度の判定と早期対応に必要な情報を提供。
  - 脅威の封じ込め：エンドポイントのネットワーク隔離を遠隔、または自動で実施。
  - 脅威除去・回復支援：マルウェアの駆除やセキュリティパッチ情報の提供など、再発を抑止しエンドポイントに残存する脅威の除去を支援。
  - 脅威ハンティング：組織内に侵入・潜伏している未検知の脅威を検出。
  - 月次レポート：セキュリティ侵害検知状況、脅威ハンティング実施結果、最新のセキュリティ関連情報のレポートを月 1 回提供。

⑦　脆弱性診断（詳細）

- 多数の個人情報を保有する企業、EC サイトを運営する企業、ネイティブアプリケーションを公開している企業に対して、ウェブサイトまたはネイティブアプリケーションに対する脆弱性診断またはプラットフォームのネットワーク診断を実施。
- 使用する診断ツール（Burp Suite や Nessus など）は対象企業のコンディションにより調整し、併せて手動による診断も実施。
- 書面での事前確認ヒアリング後、電話により詳細を調整し、作業計画の作成、および検査実施を実施。診断結果は、診断後速やかに報告するが、危険度の高いものについては速報通知を実施。

3. 実施結果

3.1 説明会の開催

事業説明会は下記のとおり計 5 回実施した。

説明会は、地域のサイバーセキュリティの意識向上を図る観点から中堅企業以上の企業や自治体等も含めた対象に幅広く行った。このため、中小企業の実態把握のためのアンケートについては、事業説明会参加者ではなく、個社別での説明した企業を含め、参加申込をした中小企業に対して実施した。

(1)　一般社団法人宮城県損害保険代理店業協会主催セミナー

同協会が定期的に開催する勉強会にウェビナー形式にて登壇。参加者は同協会に所属する会員となる。

① 2020 年 8 月 28 日（金）　BCP 勉強会

開催結果：参加者 26 名。うち、申込獲得は 0 件。質疑応答は無かった。

② 2020 年 9 月 17 日（木）　サイバーセキュリティセミナー

開催結果：参加者 19 名。うち、申込獲得は 0 件。質疑応答は無かった。

(2)　盛岡工業クラブ主催セミナー

同クラブが定期的に開催する定例懇談会にウェビナー形式にて登壇。参加者は同クラブに所属する会員となる。

① 2020 年 9 月/11 日（金）　第 116 回定期懇親会

開催結果；参加者 39 名。うち、申込獲得は 0 件。質疑応答は特に行われなかった。

(3)　中小企業向け情報セキュリティ対策 Web セミナー

損害保険ジャパン株式会社の主催により、中小企業向け情報セキュリティ対策 Web セミナーを 2 回実施した。

図 2：募集チラシ（10/14 開催分）

① 2020 年 10 月 14 日（水）岩手県・宮城県を中心とした中小企業を対象としたセミナー

- ビデオメッセージによる挨拶（3 分）
  損害保険ジャパン株式会社
- 「世界の潮流から考えるサイバーセキュリティと事業活動への影響」（60 分）
  明治大学理工学部　教授
- 「中小企業における IT 導入に向けた支援策」（15 分）
  経済産業省東北経済産業局地域経済部情報政策室
- 「サイバーセキュリティお助け隊 in 東北のポイント」（15 分）
  デジタルハーツ

参照：事業説明資料は「（別添１）事業説明資料」を参照のこと

開催概要（画面キャプチャ）は以下のとおり。

図 3：司会進行：損害保険ジャパン株式会社

ビデオメッセージによる挨拶：損害保険ジャパン株式会社

図 4 ：講演：明治大学　教授

図 5：政策支援策の紹介：経済産業省　東北経済産業局

図 6：実証事業の紹介：株式会社デジタルハーツ

開催結果：8 名の参加を得た。特段の質問などは行われなかった。参加者のうち 1 社から申込を獲得した。

② 2020 年 10 月 22 日（木） 福島県を中心としたセミナー

開催概要：内容は同一のため画面キャプチャは省略する。

開催結果：12 名の参加を得た。特段の質問などは行われなかった。参加者のうち 1 社から申込を獲得した。

3.2 実態把握結果

実証参加申込企業 59 社に対して実施した実態把握調査の結果は以下のとおりとなった。

（1） IT 資産管理に関する調査

半数以上の企業が自社の IT 資産を書面で把握していない実態が明らかとなった。

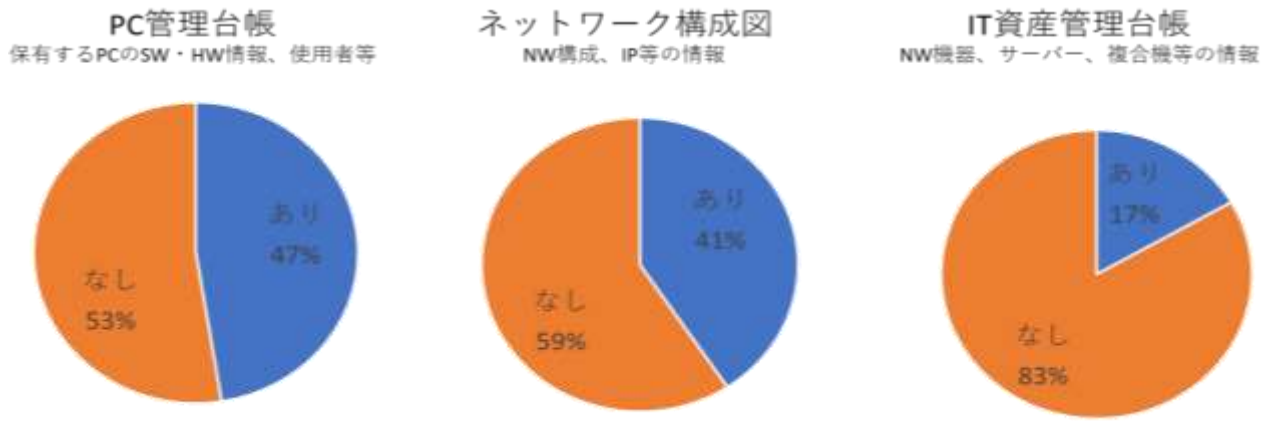

図 7：IT 資産管理に関する調査結果（n=59）

(2)　セキュリティ対策に関する現状調査

申込時点で出入口対策（UTM 設置）を行っている企業は 22%にとどまった。ウイルス対策ソフトは 91%の企業が導入していたが、監視付き EDR を導入している企業はいなかった。

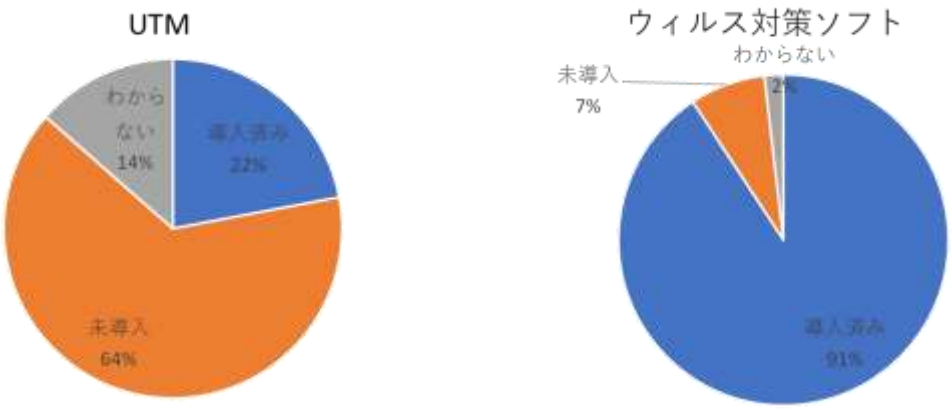

図 8：セキュリティ対策に関する調査結果（n=59）

(3)　サイバーセキュリティに対する意識調査

「何を導入すべきか？」が最も大きな課題となり、次いで人員面、コスト面となった。強化点については対策以前に社内ルール・教育面が必要と考えている企業が多かった。

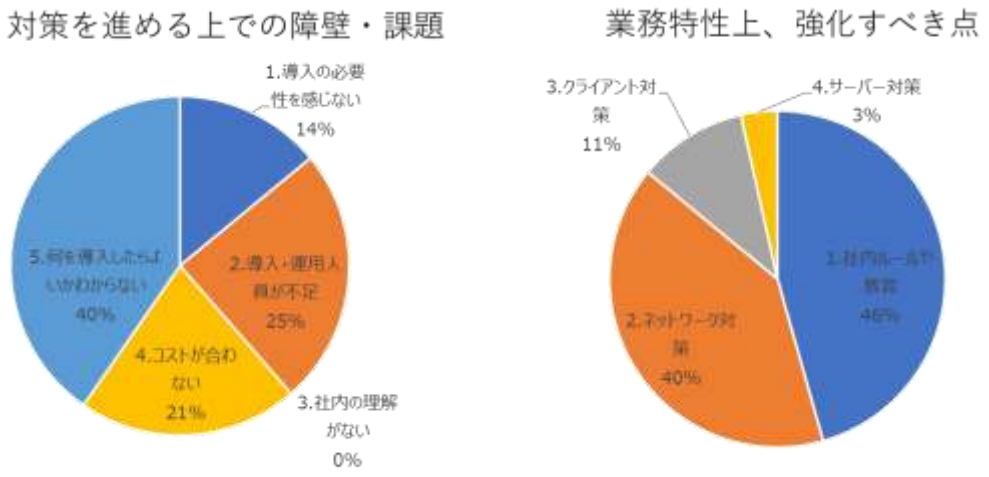

図 9：サイバーセキュリティに対する意識調査結果（n=59）

（4）　実証参加企業への個別ヒアリング結果

承諾を得た 4 社に対して 1 時間程度の個別ヒアリングを実施した。その結果として以下のような意見が寄せられた。

① 参加動機

・ 昨年から emotet の流行が気になっており、セキュリティには興味があった。
・ PC やサーバーの入れ替えを実施したタイミングであり良い機会だと考えた。
・ 社内従業員への注意喚起を行いたかった。
・ 経済団体からの紹介があり、参加しようと考えた。

② 業界特有の事情

・ 国際標準取得の関係で取引先から要求があり、何らかのセキュリティ対策を考える必要があった。
・ 過去に他社で情報漏えいがあり、取引先から対策の要望があった。

③ 新型コロナウィルス対策の影響

・ リモートワークは増加しており、クラウドサーバーやチャットツールの利用を始めるに伴い、従業員の適切な利用などセキュリティ面の懸念が拡大した。
・ 取引先や他の支店との会議がオンラインミーティングに切り替わった。取引先からもセキュリティ対策面を聞かれる機会が増えた。

④ セキュリティ対策を支援する制度の活用状況

・ IPA ガイドラインが記載されているガイドブックを活用して社内のルールを定めている。
・ 制度があることを知らなかった。

⑤ デジタル化に対する関心事項

・ 基幹システムを入れ替えるプロジェクトが動いている。生産設備の効率化に対する投資は社長の理解も得やすいが、セキュリティはコストと受け止められ社内理解が難しい。
・ 事業所ごとに業務や顧客が異なるため、事業所単位で導入したいシステムを検討して、本社で取りまとめるという体制をとっている。
・ ウェブサイトのリニューアルを検討している。

⑥ サイバー保険への関心

・ 最低限の対策を講じていれば、それ以上は不要と考えている。
・ 金額と補償内容によっては検討したい。
・ 過去に不正侵入らしきものがあり、システム部門が保険に加入した。より充実した内容のものも保険会社から提案されており検討中。

3.3 情報ポータル

本実証事業の紹介、問合せ窓口、サイバーセキュリティに関する情報提供等を行うポータルサイトを今年度事業の内容に更新して公開した。

URL　　：https://www.cyber-otasuke.jp/
更新日　：2020 年 8 月 28 日

情報ポータルは、本実証事業の内容を機器設置企業のみに閉じたものとすることなく、広く地域の意識啓発を目的として設置した。サービス内容や説明会の案内・開催資料の掲載をするほか、IPA 等が発信する情報を掲載することにより、東北地域の中小企業がサイバーセキュリティに関して情報収集する際の起点となるものとすることを心がけた。また、本活動を実証期間中に限定することなく、今後も継続して情報発信等を行っていくためのプラットフォームとして位置づけることを目的とした。

ただし、東北地域の中小企業はインターネットからの情報収集はあまり積極的に行っていない実情を踏まえれば、サイバーセキュリティに関するセミナーや、東北地域でのマルウェア感染事例など、具体的に関心がある情報をきっかけに、情報ポータルサイトでその詳細や対策を知ることができる、といったリアルコンテンツとの連動性が非常に重要となる。また、こうした取組は短期的に効果が出るものではなく、継続して発信していくことによる累積効果が期待されるものであるため、実証事業の終了後も、自主的に運営して地元経済団体等の活動と連携していく方針とした。

図 10：情報ポータルサイトページ（トップ）

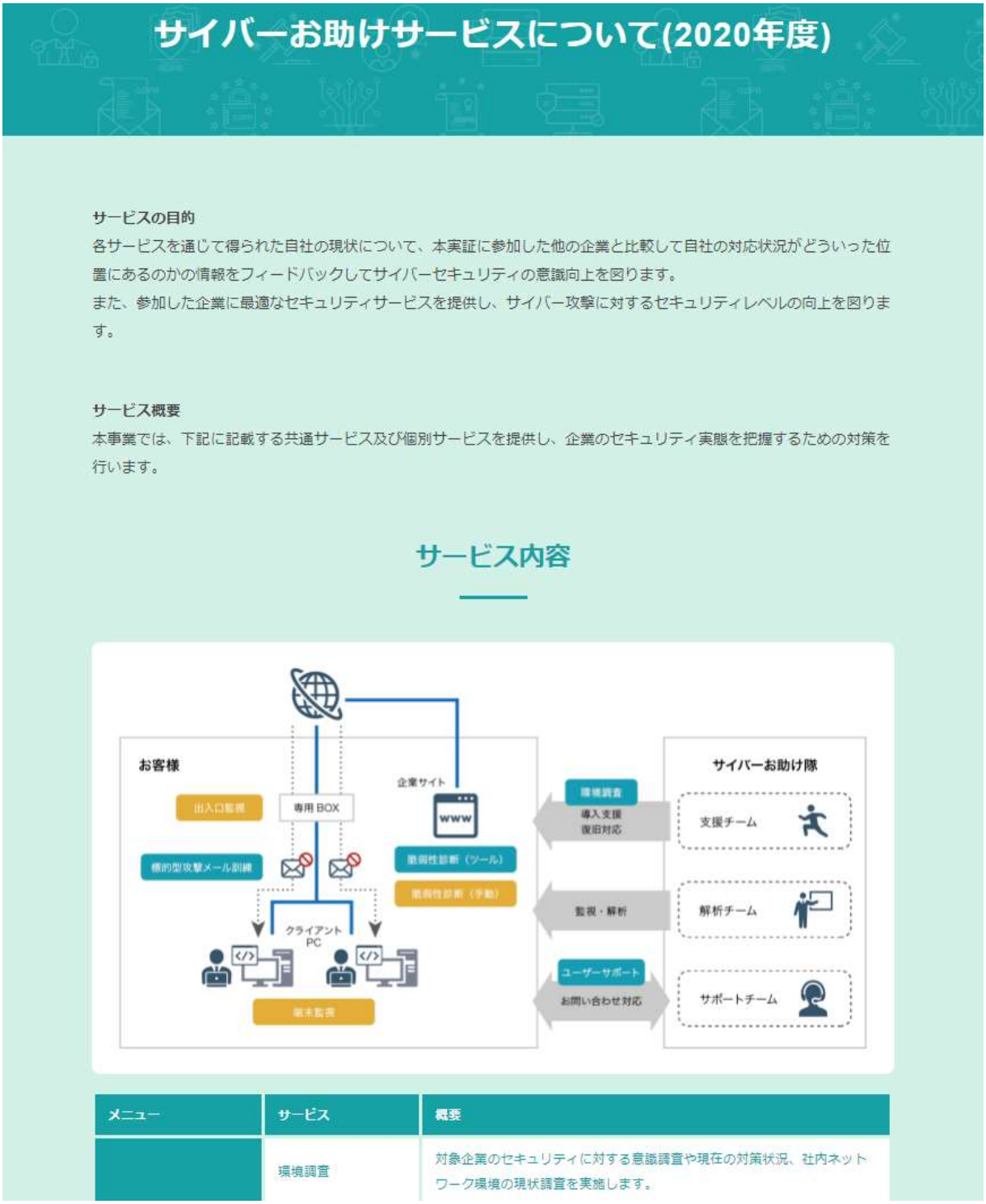

図 11：情報ポータルサイトページ（サービス）

(1)　情報ポータルで提供した情報（2020 年 8 月 28 日～2021 年 1 月 19 日）

イベント情報：事業説明会やセミナーなどの開催告知　1 件

セキュリティニュース：脆弱性情報、注意喚起　8 件

実証情報：実証結果など　1 件

(2)　アクセス状況（2020 年 8 月 28 日～2021 年 1 月 19 日）

ユニークユーザー数：1214

セッション数：1596

ページビュー数：3025

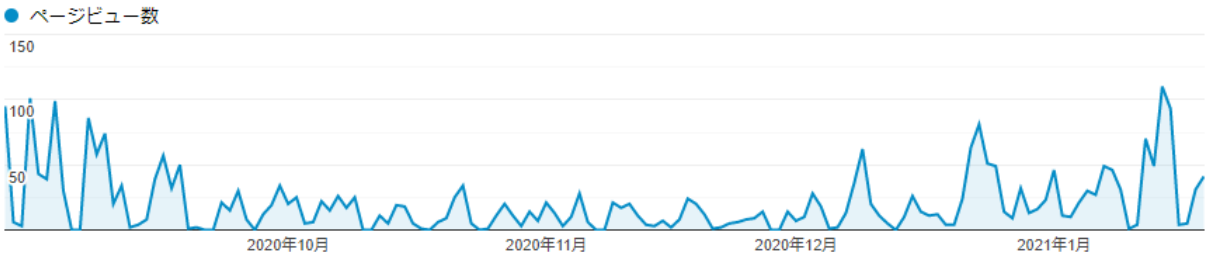

図 12；情報ポータルのページビュー推移（日別）

ページビュー推移は、実証参加を募集した 8 月後半から 9 月にかけてアクセスが増加し、また成果報告会の申し込みを開始した 12 月中旬から 1 月にかけてアクセスが増加した結果となった。昨年の傾向も踏まえてポータルサイトへ能動的にアクセスされることは現状ではまだ少ないと想定されたため、重要なセキュリティ情報はメールでの情報提供を行うこととで補完した。

3.4 実証の実施結果

(1)　共通サービスの結果

① 標的型攻撃メール訓練

実証参加企業 56 社に対して、事前に入手したメールアドレスに対して偽装メールを送信し、添付されたファイルや記載された URL へのアクセスを検知した。検知内容を各企業の担当者へレポート形式で報告し、社内での注意喚起を行ってもらうものとした。

内容	実施企業数	送信数	開封検知数	検知率
第 1 回（10 月実施）	42	543	13	2.4%
第 2 回（11 月実施）	56	884	77	8.7%
第 3 回（12 月実施）	56	856	25	2.9%
合計	—	1429	90	6.3%

表 6：標的型攻撃メール訓練の実施結果

【メール内容】

1 回目：取引先を名乗る企業よりセキュリティアップデートを促す URL リンクへ誘導するメール

2 回目：健康管理センターを名乗る団体から新型コロナウィルス健康調査アンケートの URL へ誘導するメール

3 回目：定期会議参加者を名乗る担当者より議事録送付として PDF 閲覧を誘導するメール

特に開封率が高くなった第 2 回に関して、導入台数別に開封企業数を整理した結果、20-50 名の企業では開封率が 100%という高い結果が得られた。20 名以上の従業員を有する企業においては、教育が行き届かず標的型攻撃メールの被害を受けるリスクが高いことが分かった。

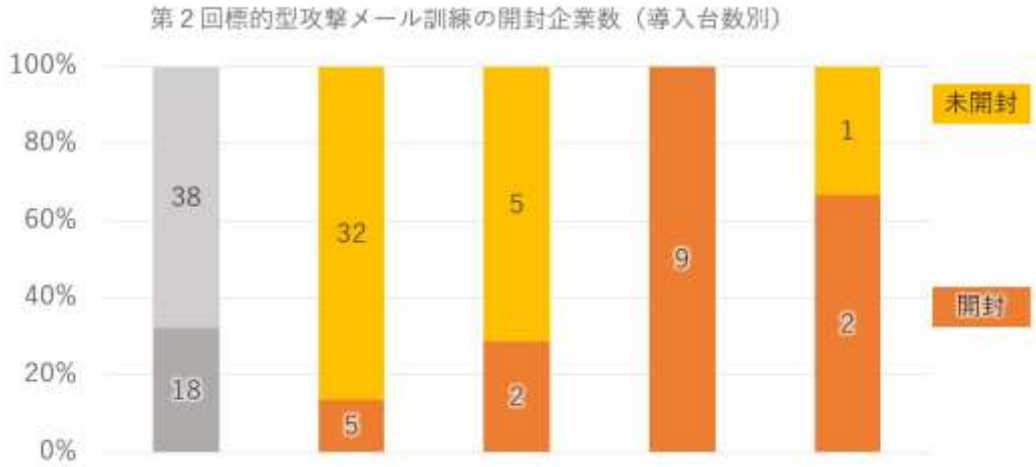

図 13：第 2 回標的型攻撃メールの開封企業数（導入台数別）

② Web セキュリティ診断

実証参加企業のうち 43 社が指定した自社 Web サイトを対象に、ツールによる自動診断を行った結果、3 社において合計 6 件の脆弱性が発見された。

検知内容	検知数
OS コマンドインジェクション	1
クロスサイト・スクリプティング	2
ディレクトリインデックス	3
合計	6

表 7：Web セキュリティ診断の実施結果

(2) 個別サービスの結果

① サイバー攻撃に関するアラート種別と検知状況

実証参加企業のうち UTM 導入の申し込みは 25 社となり、そのうち 19 社への導入が完了した。導入できなかった 6 社については、先方都合による導入前キャンセルが 3 社、導入作業時に他社 UTM の既設が発覚し導入を見送ったケースが 3 社となる。また導入完了後にネットワーク遅延により撤去を行った企業が 3 社発生した。

EDR 導入の申し込みは 29 社となり、そのうち 24 社への導入が完了した。導入ができなかった 5 社については、先方都合による導入前キャンセルが 3 社、導入作業時に既存のアンチウイルスソフトをアンインストールできない状況だったため、導入を見送ったケースが 2 社発生した。

実証期間中に検知されたアラートは下図のとおりとなった。

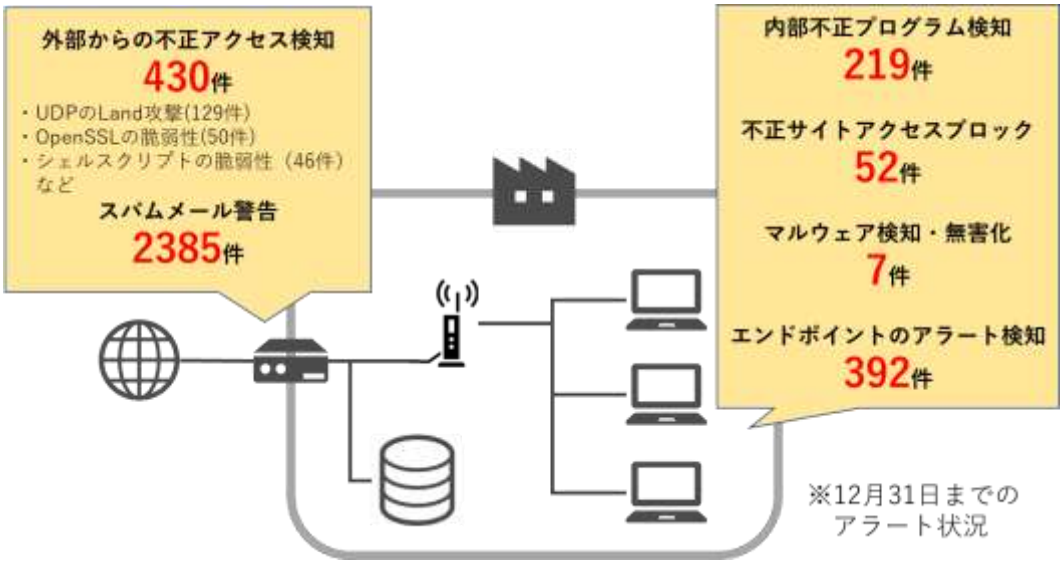

図 14：UTM および EDR によるアラート検知件数

実証期間中に検知されたアラート件数を、地域・資本金・従業員数別に整理したところ、下図のとおりとなった。

・UTM、EDR ともに岩手県での検知が多く、福島県での検知が少ない結果となった。

・UTM、EDR ともに資本金 5000 万円～1 億円未満の企業群での検知が多い結果となった。

・UTM について従業員 21-50 人の企業群、EDR について従業員 21 人以上の企業群での検知が多い結果となった。

約 3 カ月の短い期間での観測であり、かつ、サンプル数が少ないため一概には言えないが、地域や企業規模により変動が見られ、一定以上の規模の企業において相対的にアラート件数が多く検出される結果となった。

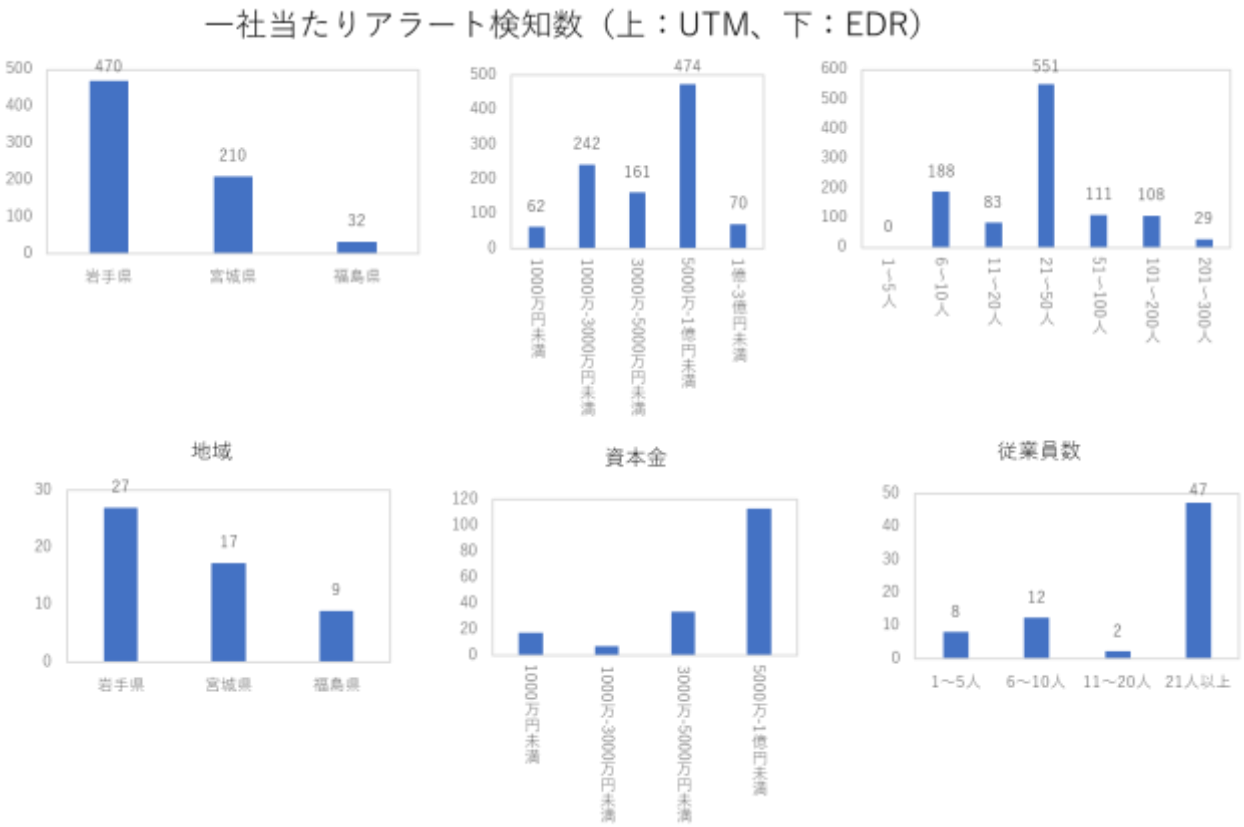

図 15：地域・資本金・従業員数別の 1 社当たりアラート検知件数

② 脆弱性診断（詳細）の結果

実施対象 5 社に対して、自社 Web サイトをデジタルハーツのエシカルハッカーにて手動診断を行った結果、いずれの Web サイトにおいても何らかの脆弱性が発見された。発見された脆弱性は Web サイト制作会社などと協議し対応を検討するよう依頼した。

危険度	内容	検知数	A	B	C	D	E
1.critical	xmlrpc.php が有効となっている	1	1				
2.high	サポート切れソフトウェアの使用	1	1				
	メールヘッダインジェクション	1		1			
	WordPress における XML-RPC の悪用	1			1		
3.mid	Cookie のセキュア属性不備	1		1			
	xmlrpc.php が有効となっている	1				1	
	クロスサイト・スクリプティング（蓄積型）	1		1			
	脆弱性のある Bootstrap の使用	1		1			
	脆弱性のある JQuery の使用	2		1	1		
	脆弱性のある lazysizes の使用	1		1			
	認証なしにアクセス可能な非公開情報	1			1		
	脆弱性のあるソフトウェアの使用	1					1
4.low	クリックジャッキング　等	18	4	3	1	6	4
5.info	php のバージョン露出　等	12	3	3	2	3	1
総計		43	**9**	**12**	**6**	**10**	**6**

表 8：脆弱性診断（詳細）の実施結果

(3)　コールセンター対応およびインシデント対応などの結果

実証参加企業 56 社からの実証期間中の問合せなどは以下のとおり行われた。

対応種別	総計	相談・インシデントなど対応状況	発生件数
コールセンター対応	59 件	実証参加に関する問合せ	7 件
		セキュリティ機器設置などの問合せ	37 件
		セキュリティ対応の相談	5 件
		その他	10 件
インシデント対応	0 件	電話およ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（駆けつけ）	0 件
その他訪問対応	5 件	機器設置などのトラブル対応	5 件
		その他（セキュリティ機器の導入・設置支援など）	0 件

表 9：コールセンター対応およびインシデント対応などの結果

「実証参加に関する問合せ」は、デジタルハーツ Web サイトを見て参加検討をしている企業からの問合せである。

「セキュリティ機器設置などの問合せ」の内訳としては、EDR に関する問合せ 22 件、UTM に関する問合せが 8 件、脆弱性診断に関する問合せが 7 件となり、主に導入日程調整に関する内容

となる。UTM の日程調整は NTT 東日本が直接導入企業と行っていたため、EDR と比較して問合せ件数が少ない結果となった。

「セキュリティ対応の相談」は、導入したセキュリティサービスの不調と思われる相談が 3 件、不審メールに関する対応相談が 2 件となった。

「その他」は、実証参加申込後の法人番号確認のための問合せ 10 件となる。

「機器設置などのトラブル対応」は、EDR 導入後に既存アプリケーションが利用できなくなった事案対応の問合せが 2 件、EDR 導入後に PC 動作が重くなった事案対応の問合せが 1 件、UTM 導入後に社内ネットワーク遅延、または切断発生した事案対応の問合せが 2 件となる。

3.5 報告会などによる事業成果の周知

以下のとおり、成果報告会を行った。

開催日時	2021 年 1 月 19 日（火）15:00-17:00
場所、形態	オンライン・オフラインのハイブリッド形式で実施。 会場：TKP ガーデンシティ PREMIUM 仙台西口ホール 8A
参加申込者数	54 名（オフライン 7 名、オンライン 47 名）
参加者数	34 名（オフライン 5 名、オンライン 29 名）
アジェンダ	15:00～15:05　開会、注意事項等の説明 15:05～15:35　「デジタル化関連予算の紹介」（経済産業省東北経済産業局） 15:35～15:45　「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） 15:45～16:15　「中小企業のための情報セキュリティセミナー～できるところからはじめよう！！コストをかけずに SECURITY ACTION！！～」（IPA セキュリティプレゼンター） 16:15～16:45　「サイバーセキュリティお助け隊　成果報告」（デジタルハーツ）

表 10：成果報告会の議事次第

参照：登壇資料は「（別添 2）成果報告会登壇資料」を参照のこと

サイバーセキュリティお助け隊 in 東北 成果報告会
兼 中小企業のための情報セキュリティセミナー
開催のお知らせ

独立行政法人情報処理推進機構が主催する「令和２年度中小企業サイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）」にて、デジタルハーツが2020年9月～12月に岩手県、宮城県、福島県で行った実証を通じて明らかになった実態と、今後の中小企業のサイバーセキュリティ対策の在り方について報告させて頂きます。
また、独立行政法人情報処理推進機構が主催する「中小企業のための情報セキュリティーセミナー」を同時開催致します。
参加をご希望の方は下記に記載のWEBサイトよりお申込みください。

日時

2021年1月19日（火）
15:00～17:00　※開場は14:30

会場

TKPガーデンシティPREMIUM仙台西口　ホール8A（８階）
宮城県仙台市青葉区花京院1-2-15　ソララプラザ

対象

中小企業向けサイバーセキュリティに興味・関心のある方であればどなたでも参加可能

定員

現地会場30名/オンライン80名

参加費用

無料

主催（共同開催）

株式会社デジタルハーツ
独立行政法人情報処理推進機構（IPA）

スケジュール

15:00～15:05　開会、注意事項等の説明
15:05～15:35　「(仮)デジタル化関連予算の紹介」
　経済産業省東北経済産業局　情報政策室　係長 土屋一樹　様
15:35～15:45　「(仮)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」
　独立行政法人情報処理推進機構　セキュリティセンター
15:45～16:15　「中小企業のための情報セキュリティセミナー～できるところからはじめよう！！コストをかけずにSECURITY ACTION！！～」
　サイバーセキュリティ専門家の方
16:15～16:45　「サイバーセキュリティお助け隊　成果報告」
　株式会社デジタルハーツ 事業推進本部 副本部長 畑田康二郎
16:45～17:00　質疑応答

お申込み方法

下記のWEBサイトよりお申込みください。

www.cyber-otasuke.jp/entry210119/

お助け隊 東北　検索

【お申込み・ご参加時の注意事項】
・現地会場へのご参加の場合は、マスク着用の上ご来場をお願い致します。
・ご入場の際、検温及び手のアルコール消毒を実施させて頂きます。体温が37.5度以上の場合は入場をお断りさせて頂く場合がございます。
・新型コロナウィルス感染拡大の状況によっては、オンラインのみの開催とする可能性がある旨、ご了承ください
・オンラインでのご参加の場合、ビデオ会議ツールは「cisco webex」を利用致します。参加方法についてはお申込み後、別途メールでご案内させて頂きます。
・ビデオ会議に参加するための端末やネット回線については、参加者様にて各自ご用意お願いいたします。
・終了後、簡単なオンラインアンケートオを実施させて頂きますのでご協力の程お願いいたします。
・内容やスケジュールについて予告なく変更される場合がございますので予めご了承ください。

DIGITAL HEARTS

お問合せ先：株式会社デジタルハーツ サイバーセキュリティお助け隊 運営事務局
東京都新宿区西新宿三丁目20番2号 東京オペラシティビル41階 担当：吉葉、大久保
mail:otasuke_r2cs@digitalhearts.com tel:0570-098-098 fax:03-3379-2054

図 17：参加募集チラシ

成果報告会への参加者に対してアンケートを行った結果、22 名から有効な回答を得ることができた。そのうち 18%が過去にサイバー攻撃を受けてことがあり、約 8 割の回答者がここ数年間でサイバーセキュリティに対する意識が向上していることが分かった。また、本実証事業のような取り組みに対する期待について質問したところ、製品やサービスの提供よりも、助言や情報提供などの伴走型支援に対するニーズが高いことが分かった。

成果報告会に対する理解度は約 7 割、満足度は約 9 割と高い評価を得ることができた。

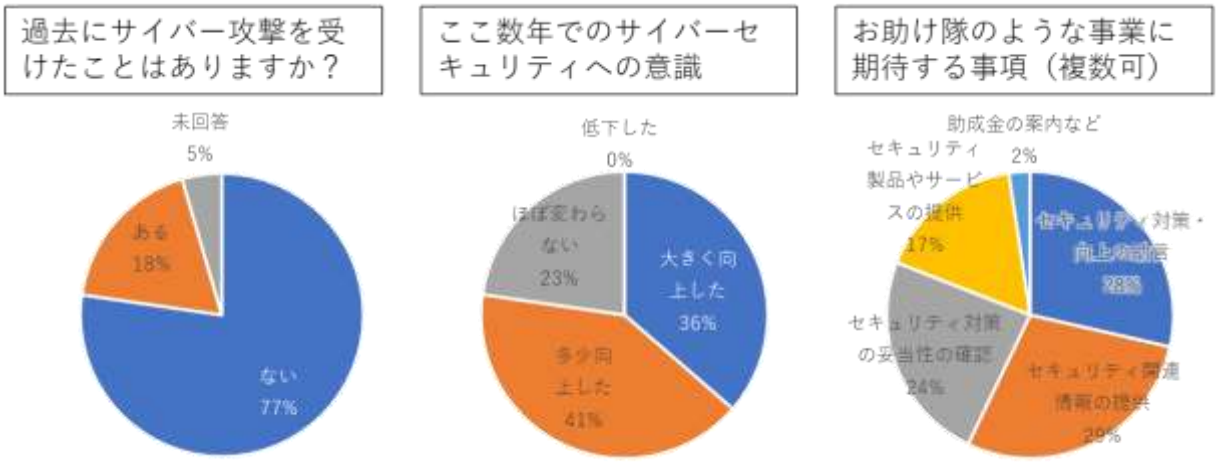

図 18：サイバーセキュリティに関する意識調査（n=22）

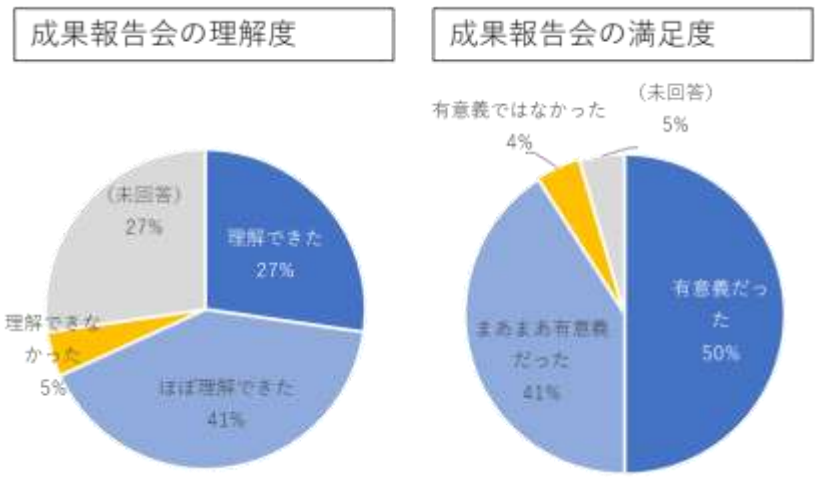

図 19：成果報告会の理解度・満足度（n=22）

4. 考察

4.1 実証参加企業におけるサイバー攻撃の実態

今回は約 3 カ月間という短期間の実証であったため、駆けつけ支援が必要なインシデントが発生することは無かった。

43 社に行った Web セキュリティ診断により 3 社から 6 件の脆弱性が検出された。また、デジタルハーツのエシカルハッカーによる手動診断では 5 社から 42 件の脆弱性が検出された。特にそのうち 1 件は、既に攻撃に利用された可能性がある緊急性の高い脆弱性であった。中小企業のウェブサイトの多くは、過去に構築したまま何ら見直しが行われていない状況であり、脆弱性に対する対応が行われないまま放置されている例が数多く見られた。

標的型攻撃メール訓練に関して、1429 件の送付に対して 90 の開封（6.3%）が行われる結果となった。特に、導入台数 20-50 台の企業 9 社が全て開封するなど、一定以上の従業員を有する中小企業において標的型攻撃メールのリスクが高いことが確認された。

4.2 中小企業におけるセキュリティ対策を進める上での課題

(1)　サービス導入時の課題

今回は昨年度実証を踏まえ個別勧誘を重点的に行った結果、速やかに実証参加企業を獲得することができたが、参加申込後、実際にサービスを開始するまでに長い時間を要した。その原因として、セキュリティ専任の担当者がいない中で実証参加申込企業の半数以上が IT 資産を把握できておらず、現状を把握できていないために導入に時間を要するケースが多く見受けられた。例えば UTM 設置のために現地調査に行った際、既に他社製品が導入されているケースがあった。このほか、EDR を導入する際に既存のアンチウイルスソフトの再インストールに必要なシリアルキーを紛失していることが判明し、導入作業が進まないケースが多くあった。特に EDR に関しては実証参加企業側でインストール作業を行うことは難しく、約半数の企業で訪問の上で導入することとなった。

(2)　サービス導入後の課題

EDR の導入後、PC スペックの問題で PC 動作が遅くなってしまい、撤去せざるを得ないケースがあった。このほか、業務上必要なアプリケーションがポリシー設定上使えなくなるケースがあった。ポリシー設定は導入コストを圧縮するため全社で汎用性のあるポリシーを一律適用したが、商

用化に当たっては設定のカスタマイズが必要であることが分かった。

UTM 運用においては、SOC などで集中管理を行うコンソール機能が無かったため、導入企業ごとのコンソールにそれぞれログインして監視を行う必要があり、運用工数がかさんだ。今回の実証では企業数や実施期間が決まっているため人的リソース補強で対応できたが、商用化に当たっては運用面の効率化を踏まえたプロダクトが必須であることが分かった。

月次報告の送付に関して、パスワード別送でファイル送付を 1 件ずつ行う運用にしたため、月初の送付作業に多くの工数を要した。商用化に当たっては連絡作業の効率化が必須となる。

12 月の月次報告において、セキュリティインシデントには分類されないものの注意が必要な事項として、12 社（EDR 監視企業の 50%）に対して以下の事項を指摘した。

① 疑わしい挙動をするマルウェア（悪意のある動作をするソフトウェア）や業務上不要と考えられるアプリケーションの自動除去（6 件）
② スパムURLやマルウェアのダウンロードに繋がるサイトへのアクセス自動ブロック （4件）
③ 非推奨ブラウザ、バージョンの古いブラウザの使用（2 件）

これらは従業員が業務 PC でフリーゲームなどをダウンロードして利用しているなどセキュリティリスクを高める行為であり、かつシステム管理者が従業員の PC 利用状況（アプリケーションのインストールなど）を把握できていないという問題が浮き彫りになったと言える。サイバーセキュリティ対策を進めていく上では、こうした実態を踏まえ社内に適切な体制を構築する必要があると言える。

4.3 中小企業において必要なセキュリティ対策

(1)　伴走型の支援の必要性

セキュリティ対策は、機器の設置やソフトウェアのインストールといった対応では不十分であり、IT 資産の書面化、セキュリティポリシーの策定・運用、従業員に対する継続的なトレーニング、インシデント発生時の迅速な対応などが求められている。一方で、多くの中小企業においてセキュリティの専任者は不在であり、手探りで対応を行っている状況。このため、担当者の悩みに寄り添って現実的な対応を指南する伴走型の支援が必要である。

(2)　自社の現状を可視化する必要性

セキュリティのレポートを送付しても、中小企業側には十分な知識がなく時間もない中で正確に読み解くことは難しい。ウェブ診断やメール訓練、UTM、EDR などの情報を分かりやすく把握できる一元的な情報把握方法が必要である。

(3)　守りのコストではなく攻めの投資

生産設備への投資は惜しまないが、セキュリティ投資はコストであり費用をかけることができないという声が多数あげられた。一方で、参加動機の多くに、取引先からの求めがあり対応を行わなければならないという声も多く寄せられた。こうした現状を踏まえ、セキュリティ対策をしっかり行っているということをアピールできれば取引の拡大に繋がることから、セキュリティ投資を積極的に行う動機付けとなる。単に安全を提供するだけでなく、取引の拡大に繋がるサービス提供を行う必要がある。

4.4 中小企業におけるセキュリティ対策の効果

実証参加企業への個別インタビューなどを通じて、中小企業においてセキュリティ対策に取り組む動機や導入時の課題など、個別の論点についてある程度の実態が明らかになった。参加時のアンケートでも従業員教育に対する関心の高さがうかがえたが、実証を通じても従業員教育に繋がる施策に関しては概ね良い反応が得られた。一方で監視レポートに関しては専門的な内容も含まれるため、レポートに対する反応は薄かった。なかなかセキュリティ対策の効果を実感しづらいという声も多かった。

項目	要点
参加動機	取引先からの要請（行政機関、電力系団体、自動車メーカー） サイバー犯罪被害に関する報道 セキュリティ専任ではない中で、どこまで取り組むべきかが分からない。 従業員からの情報漏えいが怖い。コロナでリモート拡大。
導入の手間	UTM：訪問設置の日程調整が困難。申込 29 社中 5 社（17%）は、訪問時に他社製品を確認したことなどを理由にキャンセル。(自社の現状が把握できていない) EDR：インストーラを送付して作業を依頼するだけでは進まない。訪問して実施したケースも多数。申込 25 社中 3 社（12%）は、既存アンチウイルスソフトのパスワードが分からないからサービス終了後に元に戻せないことを懸念してキャンセル。
従業員教育	メール訓練は複数の実証参加企業から好評。時事ネタ（コロナ関連メール）の開封率が高い。EDR が、業務 PC でフリーソフト（ゲーム）のダウンロードを検知・自動削除した事例。
脆弱性	ウェブサイトが改ざん可能な状態で放置されている（特に WordPress） 手動で診断した全ての企業において修正すべき脆弱性を検出。 IE の継続利用、古いバージョンの OS の利用なども見られた。
商用化に向けて	継続的な従業員教育に対する課題を感じている企業は多い。 UTM や EDR のセキュリティレポートに関しては関心が低い。 生産設備への投資は惜しまないが、セキュリティへの投資に躊躇。

表 11：個別インタビューなどを通じて得られた示唆のまとめ

5. 実証を踏まえたビジネス化に向けた検討

5.1 サイバー保険の活用

サイバー保険には、サイバー被害に伴う保険金の支払い機能だけではなく、調査・緊急対応、緊急時広報、コールセンター対応など緊急的に発生する業務を必要に応じてコーディネートする機能も含まれており、サイバーインシデントが発生した際にはお助け隊事業者にとって有益なものとなるが、平時におけるサイバー攻撃の監視まで行うものではない。このため、本実証のような実態の可視化と一体となり、被害発生時の経済面の補償および事業復旧のための体制整備支援を行うことが求められている。また、平時から、いざ有事が発生した場合の被害を最小化するとともに、速やかな事業継続を目指すという観点では、BCP に近いものであり、自然災害などと同様に、保険も組み入れた対策を自社で予め検討し、定期的な訓練・研修によりアップデートしていく必要がある。

保険の観点での対応方法としては、

・加入しやすい安価なサイバー保険の検討

・セキュリティ商材へのサイバー保険付帯の検討

になるが、アンケート結果を見ると、「対応を進める上での障壁・課題」において、「導入・運用人員の不足」と「コストが合わない」の合計が約 50%であることが分かる。コストに見合うような、つまり中小企業が加入しやすい水準の、保険付帯のセキュリティサービスが期待されており、まずはセキュリティ意識を高める意味および間口を広げる意味でも、保険付きセキュリティ商材を検討しつつ、併せて上乗せのセキュリティサービスあるいは保険の導入を働きかけることでセキュリティに強固な企業を増やしていきたい。具体的には、「シンプルサイバー」など既存の保険商品と本実証で得られた中小企業の実態を踏まえて損保ジャパンと具体的に検討していく。

また、「参加の動機」にて 30%が「取引先からの要請」となっており、個社だけでなく取引先またサプライチェーンの観点など多面的な周知が必要かつ有用と考える。

5.2 中小企業向けセキュリティビジネス化に向けた課題・検討

本実証を踏まえ、中小企業などの実態やニーズに応じた必要なセキュリティ対策サービスとして検討する上では、①複雑で分かりにくいサービスについてまず「初めの一歩」を踏み出せる分かりやすい内容であること、②スムーズな導入を行うことができるものであること、③対策の効果が分かりやすいものであること、といった点を留意する必要があることが明らかになった。

対象となる中小企業についてカスタマージャーニーマップに即して考えた場合、その必要性を強く認識してもらうためにも国全体での PR 活動が必要となる。この点については 2020 年に立ち上がったサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の活動が期待される。加えて、同コンソーシアム事務局を担う IPA ではお助け隊サービス審査登録制度の運営を行うこととされているところ、問題意識を持った中小企業が必要な対策について調べる段階で的確にお助け隊登録サービスに関する情報が届けられることが期待される。

その上で、自主サービスにおいては中小企業へのスムーズな導入に向けた地場企業との連携や、これまで実証で得られた経験に基づききめ細かいケアが求められる。加えて、サイバーセキュリティ対策の効果を実感してもらうためにも、分かりやすく現状を把握できるための「ダッシュボード」を提供し、セキュリティ専任ではない担当者であっても状況を簡単に把握できるための方策が必要と考える。

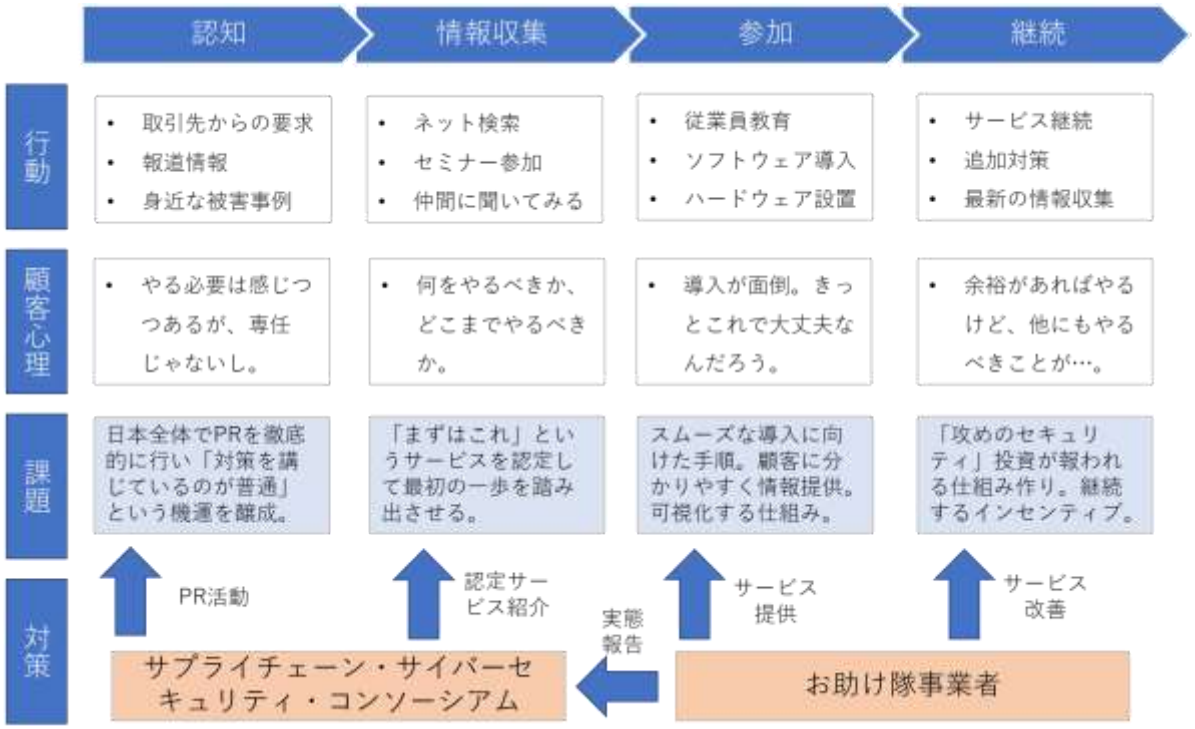

図 20：サービス化に向けたカスタマージャーニーマップ

本実証を通じて、特に「初めの一歩」として実施すべきサービスは常時監視機能付き EDR であると考えた。サービス提供に際しては、最低限、以下の内容を備えたものとして、PC1 台当たり 2000 円以下の価格帯で提供する方向で検討する。

①窓口機能：サービス導入・運用における各種相談への対応を行う窓口の設置

②導入サポート：地場企業との連携または遠隔サポートによる、スムーズな導入に向けたサポート体制の構築

③監視・緊急支援機能：システムによる 24 時間自動監視・サイバー攻撃の検知・隔離・復旧の仕組みを提供。懸念がある場合には状況確認などを実施して安全・安心を提供。万が一サイバーセキュリティインシデントが発生した場合は、速やかな対応についても支援。

④簡易サイバー保険：インシデント発生に伴う経済的被害を一定程度カバーする簡易なサイバー保険の提供

こうした自主サービスを提供するに当たって、本実証に対応したお助け隊チームを引き続き自主サービスの提供チームとして維持し、自主サービスの拡大を目指す。自主サービス提供に当たってのマーケティングとしては、3 カ月の実証期間ではデータ収集としては不十分であるため、実証終了後も希望する企業には一定期間無料の形で継続してサービスを提供しつつ監視ログデータを収集し、顧客獲得に向けての材料を得ることを検討している。その上で、一定の情報に立脚したサイバーセキュリティ対策の必要性を訴えることにより、有償でのサービス利用を求めていくこととしたい。支援体制については今回の実証事業に従事したメンバーを自主サービス提供の人員として確保することにより、これまでのノウハウを活用した支援体制の提供を検討している。

また、これらはあくまでも最低限のサービスであり、特に今回の実証で複数の実証参加企業から好評を得た標的型攻撃メール訓練、多くの脆弱性が検出された脆弱性診断、その他 UTM などについてはオプションサービスとしての提供を検討する。その際、それぞれのサービスをバラバラに提供しても、顧客視点からは複雑なものとなりかねないため、一元的に情報を管理できるダッシュボードを提供することによりユーザーの視点で分かりやすいサービス提供を行うことを目指す。こうしたパッケージ型のサイバーセキュリティサービスについては、可能な限り速やかに提供するための検討を行う。

以上