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：滋賀県、奈良県、和歌山県）

成果報告書

請負事業者：大阪商工会議所

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、大阪商工会議所が「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。

滋賀県、奈良県、和歌山県内の中小企業 53 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。

- セキュリティ監視機器（UTM）による防御・SOC による監視
- テレワークツールの提供
- アンケート
- 簡易セキュリティ診断

2. 背景・目的

2.1 背景

2.1.1 現状認識

大阪商工会議所では、昨年度のサイバーセキュリティお助け隊実証事業を踏まえて、東京2020 オリンピック・パラリンピック開催に伴うサイバー攻撃の増大に備えるため、全国の他チームに先駆けて、内容、費用ともに中小企業が利用しやすいサービスの開発を実現し、本年 4 月からビジネス化したサービスを開始した。

ところが、新型コロナウイルスの感染拡大の影響を受け、東京オリンピック・パラリンピックは延期され、企業はセキュリティに不安を抱えながらも、事業を継続するため、テレワークを導入せざるを得ない状況となった。大阪商工会議所が 6 月に実施した「中小企業のテレワークについての緊急アンケート調査」（※）から、その様子は明らかである。

多くの中小企業は、感染拡大の第 2 波襲来という不安の中、先が読めないことから、セキュリティを当面取り組むべき課題と捉えづらく、サプライチェーンのサイバーセキュリティ強化のために考案された「お助け隊サービス Ver.1.0」の普及が進まない状況が続いていた。

大阪商工会議所は、ビジネス化した「お助け隊サービス Ver.1.0」の課題を洗い出し、with コロナの時代でも、多くの中小企業が喜んでサービスを利用できる「お助け隊サービス Ver.2.0」の開発を目指し、「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」を実施することにした。

※大阪商工会議所「中小企業のテレワークについての緊急アンケート調査」
https://www.osaka.cci.or.jPChousa_Kenkyuu_Iken/press/

2.1.2 令和元年度実証で生み出した「お助け隊サービス Ver.1.0」の現状・課題

現状の「お助け隊サービス Ver.1.0」には以下の課題があると考えた。

① IT 化に遅れがある非大都市の中小企業において、セキュリティを普及させるための分析や販路が不十分。
② with コロナや非大都市、交通の便の悪い地域ではインシデント発生時の支援を提供できていない。
③ セキュリティ対策まで考慮できずにテレワークを始めた中小企業へのセキュリティ対策が現状のお助け隊サービスだけでは十分でない。

2.2 目的

現状の課題解決のため、以下の令和 2 年度実証事業では、以下の取り組みを行う。

① 中小企業へのアクセスの充実した団体を通じて、中小企業に適した上記の仕組みを提供できる体制が必要であることから、中小企業と密接な繋がりのある地域展開窓口と連携し、広範囲にわたるセキュリティ普及・促進を図る。

② インシデント時の初期対応を駆け付けではなく、リモートで実施する仕組みが必要であることから、インシデント時の初期対応における駆け付け作業をリモートで実施。

緊急事態宣言の発令時や交通の便の悪い地域などにおいて、インシデント発生時の支援を安定的かつ実効性ある形で提供できる手法や体制について、実証で様々な手法を試行し、一定のプロトタイプを作ること。こうした検証作業は、多数かつ多彩な中小企業において現場レベルでの検証が不可欠である。しかし、この種の検証は、サービス利用料を収受しサービス仕様書や利用規約に拘束される環境下で行うことは適切でないため、実証という環境下において、実証参加企業の協力意思の下に行うこと。

③ 社外へ重要データを持ち出し情報漏洩に繋がらないようセキュアにテレワークができる仕組みが必要であることから、中小企業に UTM を設置し、不正アクセスの　予防と、インシデントを検知する。更にテレワークを行う仕組みを提供し、社外への重要データ持ち出しによる情報漏洩を防ぐ。

緊急事態宣言や外出自粛に伴い、準備不足のまま急遽テレワークを導入しセキュリティに不安を抱える企業も多いことを踏まえ、テレワークという新しい業務形態に対応した with コロナ時代のセキュリティサービスが必要となっている。更に、新規で追加するべき機能、削減しても差し支えない機能などを改めて検証することにより、サービスのスリム化や代替の可能性を探ることも必要である。“セキュリティ一点張り”では中小企業のセキュリティ意識向上を図ることは難しいことが令和元年度実証で明らかになったこともあり、新たに、テレワークなど時代の要請を満たすツールも新たに取り入れ、これを切り口に据えることによる新手法で中小企業がセキュリティに関心を抱くことを促進する。これらの点につき、非大都市におけるテレワークの実情と課題およびニーズについて確認すること。

3. 実証事業の概要

3.1 実証対象（地域／産業分野）の選定とその理由

実証対象は、滋賀県・奈良県・和歌山県（以下、滋賀・奈良・和歌山と表記）とする。

・令和元年度実証で、サプライチェーン上位の大企業にヒアリングした際、これら 3 県に取引先を数多く有する企業が少なくなかった。

・これら 3 県は、産業機械、家電、プラスチック、化学、鉄鋼などを中心に高い技術力を有する中小企業が集積する地域であり、大阪、名古屋、東京などの、サイバーセキュリティ上の重要な情報を取り扱う産業セクターに連なるサプライチェーンを構成している。

・非大都市にもサイバー攻撃があることは、令和元年度実証における全国 8 地域の成果報告書が示すとおりである。

・実効性の観点では、実証実施中に不測の事象が発生した場合でも、訪問フォローができる範囲内であり、特段支障は無い。

・実証参加企業募集という観点では、大阪商工会議所が事務局を担う関西商工会議所連合会の管内にあり、全 18 の加盟商工会議所とは日頃から接点があるため、説明会の共催をはじめ実証参加企業募集活動への協力が得られやすい。また、地域の金融機関（地方銀行や信用金庫）とも接点があり、実証およびその後のビジネス化に向けても広報面での協力が得られやすい。

・サイバーインシデント時の支援提供を担う「お助け実働隊地域 IT 事業者（後述）」を確保できる地域でもある。

図 3-1 実証対象（地図）

3.2 スケジュール

図 3-2　スケジュール

3.3　実証参加企業など

3.3.1 実証参加企業などの目標数

滋賀県・奈良県・和歌山県で合計 50 社・団体

3.3.2 実証参加企業などの定義

本実証事業の仕様書に定義される中小企業などであり、本実証で使用する UTM が設置され、オンラインになった中小企業など

3.3.3 実証参加企業の募集の手法および結果

(1) 募集方針

・ 商用サービスを地元京阪神以外の地域の中小企業に（同じように安価に）提供していくには、いわゆる代理店（IT ベンダーなど）と契約し拡販する手法は必ずしも妥当ではないと考える。

・ そこで、令和 2 年度実証において、各地の商工会議所・商工会や地域金融機関などを「地域展開窓口」（詳細後述）と位置づけ、今後の商用サービスの拡販結節点としての有効性や課題を検証（実証参加企業の募集手法と募集実績から推察）した。

(2) 募集手法および募集手法別の募集実績

表 3-1 募集手法および募集手法別の募集実績

募集手法		募集実績			
個別打診・一本釣り	地域展開窓口の個別打診	10	19%	33	62%
	お助け実働隊地域 IT 事業者の個別打診 （3 者）	8	15%		
	大阪商工会議所事務局の個別打診 （2 者）	5	9%		
	大阪商工会議所の会員である 3 県の企業およびプライバシーマーク認定企業への封書直送&テレマーケティング 封書直送 261 件 → テレマーケティング 135 件	4 奏効率(テレマ)3%	8%		
	コンソーシアム側関係者の個別打診 （2 者）	3	6%		
	サプライチェーン上流企業の紹介 （1 社）	3	6%		
広報	地域展開窓口（商工会議所・商工会・商工会連合会）での会報同梱チラシ・配架チラシ 奈良商工会議所 2700 枚、生駒商工会議所 300 枚、橿原商工会議所 2000 枚、大和高田商工会議所 1300 枚、守山商工会議所 1300 枚、その他約 400 枚 計約 8000 枚	5 奏効率 0.06%	9%	17	32%
	地域展開窓口（商工会議所・商工会・商工会連合会）でのメール・FAX・セミナーなど	3	6%		

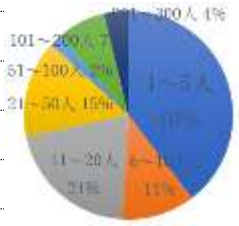
募集手法		募集実績			
	地域展開窓口の提供 DM(各地商工会議所会員)による大阪商工会議所または各地商工会議所からの直送チラシ 大津商工会議所 1759 件、生駒商工会議所 880 件、和歌山商工会議所 3436 件　計 6075 件	6 奏効率 0.1%	11%		
	大阪商工会議所事務局独自収集母集団への直送チラシ 1254 件(3 県)	2 奏効率 0.16%	4%		
	地域展開窓口(地元金融機関など)でのチラシ配架 各金融機関などで 2000 枚配架	1 奏効率 0.05%	2%		
その他	日経新聞で経済産業省の記事(お助け隊掲載)を見て検索、IPA の SECURITY　ACTION 登録企業向けメルマガ、名古屋商工会議所のお助け隊の情報入手	3	6%	3	6%
プレス発表	大阪経済記者クラブ、大津市政記者クラブ、 奈良県政・経済記者クラブ、橿原市役所市政記者クラブ、和歌山市市政記者クラブ	—	—	—	—
合計		**53**		**53**	

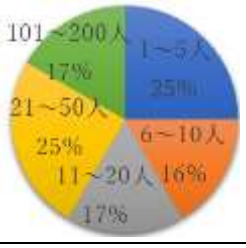
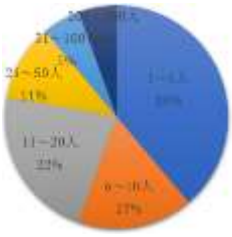
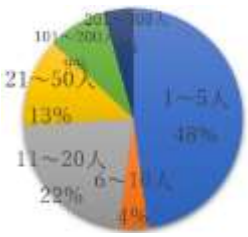
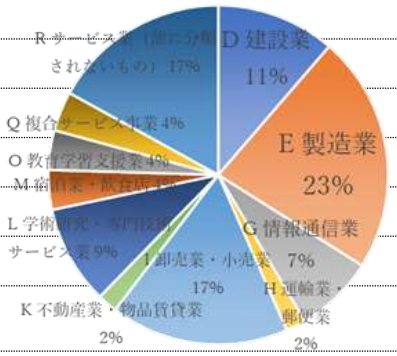
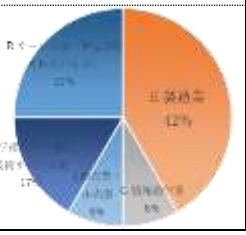
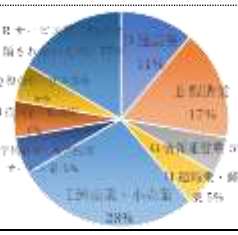
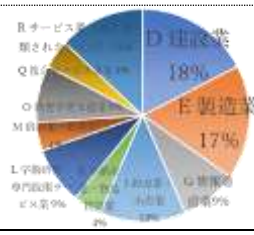
3.3.4 実証参加企業などの概要

(1) 実証参加企業などの構成

表 3-2　実証参加企業などの構成

		滋賀県		奈良県		和歌山県		合計
参加企業などの数		12(23%)		18(34%)		23(43%)		53
市郡町村別		大津市	2	生駒市	5	和歌山市	9	
		守山市	2	橿原市	5	田辺市	6	
		草津市	2	奈良市	3	紀の川市	2	
		東近江市	2	大和高田市	1	西牟婁郡	2	
		高島市	1	香芝市	1	海南市	1	
		湖南市	1	高市郡明日香村	1	日高郡	1	
		米原市	1	北葛城郡	1	有田市	1	
		愛知郡	1	磯城郡	1	東牟婁郡	1	
従業員数の規模別	従業員数の平均値	30.8 人						
		37.4 人		24.2 人		32.5 人		
	従業員数の中央値	10 人						
		14.5 人		9.0 人		6.0 人		
	1～5 人	21(40%)						
	6～10 人	6(11%)						
	11～20 人	11(21%)						
	21～50 人	8(15%)						
	51～100 人	1(2%)						
	101～200 人	4(8%)						
	201～300 人	2(4%)						
	1～5 人	3 (25%)		7(39%)		11(48%)		
	6～10 人	2(17%)		3(17%)		1(4%)		
	11～20 人	2(17%)		4(22%)		5(22%)		
	21～50 人	3(25%)		2(11%)		3(13%)		
	51～100 人	0		1(6%)		0		
	101～200 人	2(17%)		0		2(9%)		
	201～300 人	0		1(6%)		1(4%)		



		滋賀県	奈良県	和歌山県	合計
					
業種別	D 建設業	6(11%)			
	E 製造業	12(23%)			
	G 情報通信業	4(8%)			
	H 運輸業・郵便業	1(2%)			
	I 卸売業・小売業	9(17%)			
	K 不動産業・物品賃貸業	1(2%)			
	L 学術研究・専門技術サービス業	5(9%)			
	M 宿泊業・飲食店	2(4%)			
	O 教育学習支援業	2(4%)			
	Q 複合サービス事業	2(4%)			
	R サービス業（他に分類されない）	9(17%)			
	D 建設業	0	2(11%)	4(17%)	
	E 製造業	5(42%)	3(17%)	4(17%)	
	G 情報通信業	1(8%)	1(6%)	2(9%)	
	H 運輸業・郵便業	0	1(6%)	0	
	I 卸売業・小売業	1(8%)	5(28%)	3(13%)	
	K 不動産業・物品賃貸業	0	0	1(4%)	
	L 学術研究・専門技術サービス業	2(17%)	1(6%)	2(9%)	
	M 宿泊業・飲食店	0	1(6%)	1(4%)	
	O 教育学習支援業	0	0	2(9%)	
	Q 複合サービス事業	0	1(6%)	1(4%)	
	R サービス業（他に分類されない）	3(25%)	3(17%)	3(13%)	
					

3.4 実施内容

3.4.1 事業の全体像

(1) 「助ける側」のコンソーシアムの組成

・ 大阪商工会議所は公益な地域経済団体であり、サイバーセキュリティお助け隊実証事業やそこで生み出された商用サービス提供を自己完結的に実施することはできない。

・ よって、技術面およびセキュリティ機器の提供は本分野において我が国のリーディングカンパニーの一つである日本電気（株）（NEC）に、相談受付の提供は IT に強いコールセンターとして定評あるキューアンドエー（株）に、保険の提供は我が国でサイバー保険を先駆的に事業化した東京海上日動火災保険（株）に依頼してコンソーシアムを組成した。

・ コンピュータウイルスや不正アクセスなどによるサイバーインシデントを一種の“病”と捉えるなら、当コンソーシアムが「サイバーセキュリティお助け隊」における“大病院”的存在であり、セキュリティ機器である UTM が“マスク”“体温計”に相当する。

(2) 地域支援体制の構築

・ 昨今のサイバー攻撃・インシデントの増加を踏まえると、全ての案件を“大病院”が対応するわけにはいかない。よって地域ごとに“町医者”“救急隊”が必要である。

・ しかし“町医者”“救急隊”（情報処理安全確保支援士やセキュリティ系 IT ベンダー）は小規模な主体であるケースが多いので、一般的に広報力も弱く、その存在は（同じ市内であったとしても）ユーザーたる中小企業に知られていないケースも多い。

・ 中小企業からすれば、サイバーインシデントについて相談したり、対応を発注したりできる信頼ある“町医者”“救急隊”が身近にいない（知らない）ので、インシデント（の存在を認知し得たとしても）を放置したり、自己流の解決を試みたり、単なるパソコンの不調と思ってしまうケースもあり、被害の実害化、実害の拡散化をもたらしかねない。

・ とりわけ大都市圏以外の地方都市にあっては、サイバーセキュリティ解決に係る需要と供給はともに低調に推移しており、需要が少ない（インシデントの存在に気付いていない）ため供給も育たず、供給が少ない（セキュリティ系 IT ベンダーなどの存在が見えていない）ため需要も興らないという“鶏と卵”の問題が常態化していると考えられる。

・ よって、非大都市圏を含め日本各地に、中小企業がサイバーインシデントに気付く仕組みと、“町医者”“救急隊”が一定の基準と手法のもとに囲い込まれ（お墨付きが与えられ）地元中小企業の知るところとなり、頼りにされる存在になるような仕組み作りが必要であり、かつ“大病院”と円滑に連携していくことが、各地域におけるサイバーセキュリティ対策支援体制構築の要諦の一つと考えられる。

(3) サイバーセキュリティお助け隊の成否のカギを握る「お助け実働隊地域 IT 事業者」

- 前項の例え話で言うところの“町医者”“救急隊”には、各地域で地域密着的に活躍している情報処理安全確保支援士や地域 IT 事業者などを想定した（これを便宜上「お助け実働隊地域 IT 事業者」と呼ぶ）。

- 地域 IT 事業者は必ずしもセキュリティ系 IT ベンダーには限定しなかった。なぜなら地方都市においてセキュリティ一本で、もしくはセキュリティに軸足を置いて事業展開している IT 事業者は極めて僅少だからである。

- お助け実働隊地域 IT 事業者は、技術力に加え、中小企業の経営者などとのコミュニケーション能力が求められるため、情報処理安全確保支援士と中小企業診断士の資格を併せ持つ方が適任との認識のもとに、これらスペックを有する事業者の情報収集と信頼関係構築に努めた。

- お助け実働隊地域 IT 事業者には、令和元年度実証同様「所定サイバーインシデント駆け付け・初動対処」と「簡易 UTM 設置支援」のうちいずれか一方または両方の対応を依頼した。

表 3-3　お助け実働隊地域 IT 事業者の役割

	所定 UTM 設置支援	所定サイバーインシデント初動対処
役割	所定 UTM の設置、撤去	所定のサイバーインシデントが発生した場合の①初動対処、②状況判断、③暫定対処　など
要求スキルなど	◎ネットワーク・ネットワーク製品、ICT 関係のハードウエア製品の知識と実務経験を有する IT 事業者、IT に強い電気工事業者、情報処理安全確保支援士　など	◎UTM 設置支援の要求スキルを備えていること ◎サイバー攻撃・マルウエア感染などに係る状況判断（他のインシデントとの判別）、現場レベルの暫定対処（ネットワーク切り離し、エンドポイントセキュリティのフルスキャン、OS クリアインストール、その他顧客の IT 環境や意向に応じた対処）ができる IT 事業者、情報処理安全確保支援士　など
	◎大阪商工会議所と所定の契約が締結できること ◎所定の技術的対応力、顧客対応力があり、大阪商工会議所などと緊密に連携し、所定の仕様と実証参加企業の意向に基づき業務を履行すること ◎第三者に再請負すること無く、委託業務の全部を自己完結的に対応できること	

表 3-4　お助け実働隊地域 IT 事業者の一覧

お助け実働隊地域 IT 事業者の一覧							
	所在地	対応可能エリア			曜日	時間	プロフィール
		滋賀	奈良	和歌山			
1	米原市	全域			全	1000～1800	情報処理安全確保支援士、IT コーディネータ。製造業での勤務経験を踏まえ、IPA の「情報セキュリティマネジメント指導事業」の専門家として中小企業への訪問指導経験あり。
2	奈良市		全域		土日祝を除く	0900～1700	県内で初めて「プライバシーマーク」付与認定を取得。情報処理安全確保支援士も在籍。信頼・安心をモットーに時代の変革に対応するコンピューターシステムやソリューションを提供。
3	奈良市		全域		土日祝を除く	1000～1800	クラウドコンピューティングで中小企業の経営革新と儲ける力向上を支援。中小企業診断士・情報処理安全確保支援士・ITコーディネータなどの有資格者が中小企業のクラウドサービスの選択と導入、運用を支援
4	和歌山市			全域	土日祝を除く	1000～1800	情報処理安全確保支援士、情報セキュリティ監査人補、IT ストラテジスト、IPA 登録セキュリティプレゼンター、中小企業診断士
5	田辺市			御坊市以南	全	0900～1700	パソコン機器の管理・運用。出張メンテナンス、ネットワーク構築、セキュリティ対策など。
6	京都市	県南部	県北部		全	0900～2100	情報処理安全確保支援士、情報処理技術者（ネットワーク・情報セキュリティ）、IT コーディネータ、クラウド、AI、IPA セキュリティプレゼンター登録。IT 全般に関する管理・運用・導入・構築・コンサル・保守など。
7	高槻市	JR沿線最寄駅から徒歩圏エリア	近鉄奈良線最寄駅から徒歩圏エリア		日を除く	0900～2100	情報処理安全確保支援士、IT サービスマネージャー、システム監査技術者、IT ストラテジスト、プロジェクトマネージャー、1 級販売士、中小企業診断士
8	豊中市	全域	全域	全域	要相談	0900～1930	地元商工会議所 IT 支援推進室アドバイザー、パソコントラブルサポート
9	貝塚市	相談	相談	田辺市以北	祝を除く	1000～1600	パソコンや IT 駆け付けサポート 20 年。大阪府下なら最短 60 分以内で駆け付け。ネットワークやセキュリティの提案、ホームページや Web・印刷物デザインの専門家も常駐。

(4) 「商工会議所サイバーセキュリティお助け隊サービス」の成否のカギを握る「地域展開窓口」

・ 商工会議所は商工会議所法に基づく地域経済団体であり、原則として、その活動領域は所在市の市内に限定される。よって、実証参加企業募集はもとより、商用化サービスの拡販においても、他市で事業展開する場合は、各地域の官・公・民の各機関などによる協力が不可欠である。

・ 本実証事業においては、各地域の中小企業に接点のある各地商工会議所、商工会、商工会連合会、地域金融機関、地域有力企業、行政機関などに「地域展開窓口」としての機能を依頼した。実際に協力を得られたのは下記のような組織である（順不同・敬称略）。

> 関西サイバーセキュリティネットワーク（近畿経済産業局、近畿総合通信局、関西情報センター）、大津商工会議所、奈良商工会議所、大和高田商工会議所、生駒商工会議所、橿原商工会議所、和歌山商工会議所、滋賀県商工会連合会、奈良県商工会連合会、和歌山県商工会連合会、天理市、滋賀銀行、南都銀行、紀陽銀行、奈良信用金庫、奈良中央信用金庫、大和信用金庫、大阪ガス、近鉄グループホールディングス、東京海上日動の支店（一部）および代理店（一部）、日本電気の各支店（一部）

・ 「地域展開窓口」には、案内チラシの会報などへの同梱、配架、メールマガジン・FAX・公式ウエブサイトなどでの広報、地元記者クラブでの共同プレス発表、中小企業への個別打診、中小企業の個別紹介などの協力を得た。（募集結果は別記）

(5) 本実証事業の目的および事業スキームの検討・構築

・ 本実証事業の目的は、令和元年度実証で生み出し令和2年4月より商用化している「商工会議所サイバーセキュリティお助け隊サービス（Ver.1.0）」を同Ver.2.0として発展させることである。

・ 「商工会議所サイバーセキュリティお助け隊サービス（Ver.1.0）」の基本的なスキームは以下のとおりであり、これら全てがパッケージ化され、安価（全国いずれかの商工会議所・商工会の会員なら月額6,600円、非会員なら同8,250円）かつ短い契約期間（1年）で大阪商工会議所が中小企業向けに提供しているものである。

①NECが令和元年度実証時に開発した「設置（導入）」と「運用」が容易で「郵送」により送付できる「国産」のUTMの貸与（お守り）
②NECによる「24時間365日」の遠隔監視（見守り）
③アラートメールでの「お知らせ」とユーザーごとのサービスポータルでの「閲覧」による（見える化）
④ITに強いコールセンター（相談窓口）
⑤所定サイバーインシデント時の「お助け実働隊地域IT事業者」による初動対処（駆け付け）
⑥駆け付け経費にあてがう簡易サイバー保険（補償）
⑦サイバーセキュリティに関する最新情報の提供（意識喚起）

・ しかし、令和元年度から2年度にかけて、新型コロナウイルスの感染拡大に伴い社会経済情勢の大きな変容が生じた。「商工会議所サイバーセキュリティお助け隊サービス」の目玉サービスである所定サイバーインシデント時の「駆け付け」についても、緊急事態

宣言などの発令下にあっては、助ける側のお助け実働隊、助けられる側のユーザー中小企業のいずれかもしくは両方が訪問による駆け付けを固辞するかもしれない。またかかる環境下でなくても、今後サービスを現行の京阪神エリア以外にも提供していく中で、山間部など交通の不便な場所に立地するユーザーから利用希望が寄せられるかもしれず、かかるユーザーをその立地を理由として見捨てるわけにはいかない。

- そこで、本実証事業では、リモートツールなどを利用した遠隔でのサイバーインシデント対応の可能性（ニーズ、手法、課題および課題解決法）につき検証を加えることとした。

- また本実証事業において、サイバー攻撃の入口となりかねないテレワークを安全に行えるツール（画面転送型）の提供を行い、実証期間中の試用を通じて、そのニーズや課題についても検証を行うこととした。

- 更には、サイバー攻撃やサイバーセキュリティに係る現状の実態や今後の対策ニーズなどにつき、滋賀・奈良・和歌山と、京阪神など大都市圏との間の有意差を探るとともに、地域特有の課題について検証することとした。

- そのため、実証参加企業に対し、サイバー攻撃の実態やセキュリティ対策の実情、ニーズに係るアンケート調査を行うとともに、「簡易セキュリティ診断」を行う。

- あわせて、今後の商用化サービスの拡販を見据え、その手段としての地域支援体制および「地域展開窓口」の構築・確立自体も本実証事業の目的とするところであり、信頼関係構築からスタートして定期的な意見交換や情報交換の機会を意識的に設け、ウイン・ウインの関係性の在り方を模索する機会とする。

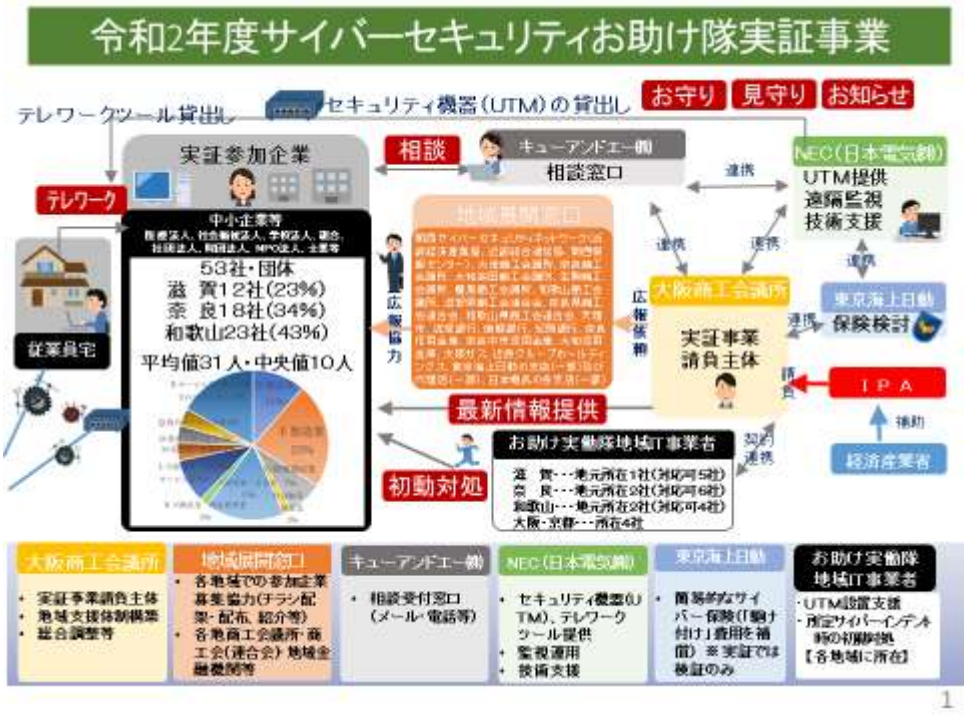


図 3-3　サイバーセキュリティお助け隊実証事業（滋賀・奈良・和歌山）概要図

3.4.2 UTM による防御・SOC による監視（「お守り」「見守り」「お知らせ」）の概要

本実証事業において、使用する UTM の諸元や設置方法、セキュリティ機能や運用手法について、詳細を記載する。

3.4.2.1 簡易 UTM による防御と観測（把握）

(1) UTM の諸元

本実証事業では、NEC の既存 UTM をベースに、中小企業が容易に設置、運用できるよう設計・製造（令和元年度実証において開発・検証）した以下のスペックの UTM を使用した。

表 3-5　実証で使用した UTM のスペック

項目		仕様
WAN インタフェース	ポート数	1 ポート
LAN インタフェース	ポート数	4 ポート
無線 LAN インタフェース	アンテナ	内蔵アンテナ
	規格	IEEE802.11n
		IEEE802.11g
		IEEE802.11b
電源（AC アダプタ）		AC100V～240V 50/60Hz
動作保証環境		温度：0～40℃　湿度：10～90%
消費電力		35VA（21W）以下
外形寸法（WHD）		約 174×195×40 mm
本体質量		0.9 kg以下
設置方法		横置き、縦置き
セキュリティ機能	不正侵入防止検出/防止（IDS/IPS）	ネットワークに対する攻撃を認識／防止
	アンチウイルス	ホームページ閲覧時やメール受信、その他のアプリケーションの通信を監視し、ダウンロードするファイルにウイルスが混入していないかをチェックし、発見時には無害化
	Web ガード	フィッシングサイトなどの詐欺サイトや、閲覧によりマルウエア感染の可能性がある危険なサイトへのアクセスをガードする
	URL フィルタリング ※本実証では使用しない	サイトの URL をカテゴリごとに登録し、登録済みカテゴリに対してアクセス禁止などの制御

項目		仕様
	URL キーワードフィルタリング ※本実証では使用しない	Web 閲覧において、予めユーザーが設定した特定の文字列を URL に含むページのアクセスをブロック
	アプリケーションガード ※本実証では使用しない	チャットアプリ、ファイル交換ソフト、SNS サイト、動画サイトなど、アプリケーションの通信を検出し、制御
	ファイアウオール ※本実証では使用しない	お客様のネットワーク環境（イントラネット）とインターネットの境目（エッジ）に設置し、その間の通信をポート制御することで、イントラネットからインターネット接続を損なわず、インターネットからお客様のネットワーク環境のアクセスを制限

・本実証では、UTM をインターネット接続機器（ONU やブロードバンドルーターなど、PPPoE を終端している機器。以下、ブロードバンドルーターと記載）と監視対象端末（パソコンやモバイル機器など）の間に設置する想定とした。

・既存の UTM は、約 100 台の端末を監視でき、中小企業にとって十分であると考え、選定した。また、100 台を超えた場合、通信速度が遅くなる可能性があるため、募集の際にも条件として考慮した。

・WAN インタフェースに関して、中小企業では、ブロードバンドルーターやキャリアとの回線は複数無いと想定し 1 ポートの既存 UTM をベースとした。複数のブロードバンドルーターが存在する場合、業務でよく利用する回線を対象とする方針とした。

・LAN インタフェースに関して、仮にブロードバンドルーターが 4 ポート以上ある場合は、別途ハブを用意してもらう前提とした。

・ブロードバンドルーターの無線機能を使用している場合、端末からの通信はブロードバンドルーター配下に設置した UTM は経由しないため、UTM による監視はできない。そのため、ブロードバンドルーターの無線機能は無効にし、UTM の無線機能を使用する必要がある。ブロードバンドルーターの無線機能ではなく、別の無線 LAN アクセスポイントを用意している場合は、無線 LAN アクセスポイントとブロードバンドルーターの間に UTM を設置することで、無線 LAN アクセスポイントの設定や配下に接続されている端末の設定変更無しで監視できる。

(2) UTM の設置方法

中小企業の実態を把握するため、ブロードバンドルーターと監視対象端末の間に UTM を設置し、企業 LAN とインターネットの通信を監視した。また、UTM の動作は「ブリッジ」モードとした。これは、実証参加企業のネットワーク構成を極力変更しないこと、万一 UTM で問題が発生した場合でも業務停止を最小限にするためである。

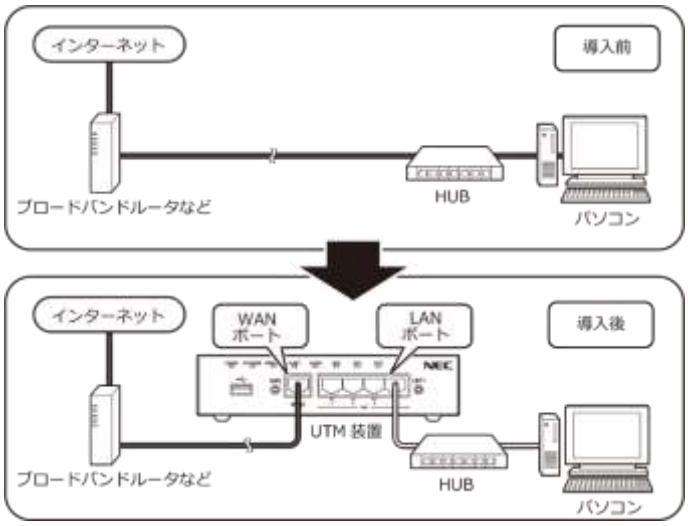


図 3-4　ブロードバンドルーターなどの配下に HUB などを設置している場合の UTM 接続位置

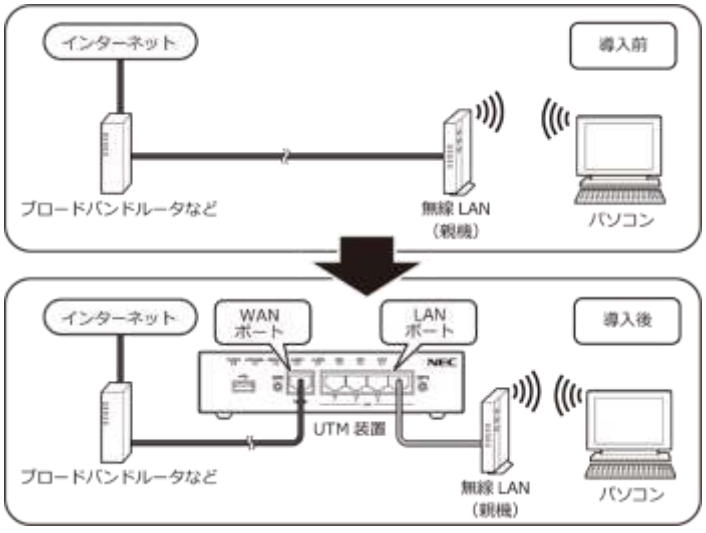


図 3-5　ブロードバンドルーターなどの配下に無線 LAN（親機）を使用している場合の UTM 接続位置

(3) セキュリティ機能

UTM では、下記の 3 種類のセキュリティ機能を使用した。また、「URL フィルタ」および「アプリケーションガード」は、昨年度の実証結果および企業への業務影響を考慮し、実証では設定しないこととする。以降、各セキュリティ機能は表の略称にて記載する。

表 3-6　使用した UTM のセキュリティ機能一覧

セキュリティ機能	略称	説明
不正侵入防止	IPS	通信データ内の攻撃コードなどの異常なデータが含まれていることを検知し、防御する機能。 予め登録された侵入手口のパターンとマッチングさせることで、検知・遮断を実現し、ネットワークに対する攻撃に対して防御する。
アンチウイルス	AV	マルウエアや危険なコードが含まれるファイルを検知した場合に内容を書き換え、無害化する機能。 ホームページの閲覧やメール受信、その他のアプリケーションの通信を監視し、ダウンロードまたはアップロードするファイルにマルウエアが混入していないかをチェックする。ダウンロードまたはアップロードするファイルにマルウエアが混入している場合、ファイルの内容を書き換えてファイルを無害化する。
Webガード	WG	フィッシングサイトや、閲覧によってマルウエア感染を起こすなどの有害なWebサイトへのアクセスを遮断する機能。予め定義されている有害なWebサイトに対するアクセスを検知し、通信を遮断する。
URLフィルタ ※本実証では使用しない	UF	予め用意されている、Webサイトのカテゴリに該当するWebサイトへのアクセスを検知する。
アプリケーションガード ※本実証では使用しない	APG	ファイル交換ソフトや動画共有アプリ、メッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションを利用した際の通信を検知する。

(4) 運用手法

UTM では、下記の運用手法を用いた。

・ UTM のセキュリティ機能のうち、IPS、AV、WG で検知した通信を遮断することにより、外部からの攻撃（不正アクセスやマルウエアの侵入）や、外部への不正通信（マルウエア感染などによる企業内部から外部への被害拡大）を防ぐ。即ち、「攻撃の被害化」と「被害の実害化」を防ぐ。

・ UTM が攻撃通信を防御、検知したアラート情報をクラウドで収集する。

・ IPS、AV、WG で検知、遮断した際、実証参加企業の管理者に通知を行い、注意を促す。通知方法は、企業内部から外部（インターネット）への不正通信（以下、外部への不正通信と記載）を検知・防御したか、外部（インターネット）から企業内部への攻撃（以下、外部からの攻撃と記載）を検知・防御したかにより異なる。
  - 外部への不正通信を検知・防御した場合は、既に実証参加企業内の端末がマルウエアに感染しているなど被害が発生している可能性があり、実証参加企業側で対処が必要と考え、ログの記録に加え、重要アラートとして実証参加企業の管理者あてにメール通知を行い、対処を促す。
  - 外部からの攻撃を検知・防御した場合は、UTM で事前に防いでいることから、実証参加企業側での対処は不要であり、ログの記録を行い各実証参加企業閲覧用サービスポータルサイト（以下、ポータルサイト）から確認することとし、メール通知は行わない。事前に防いだことをメール通知すると、メール数が非常に多くなり、実証参加企業が開封すらしなくなる恐れがあるためである。
  - 内部の脆弱性は、パスワードが脆弱なこともあり注意喚起のため、検知・防御した場合は、ログの記録に加え、重要アラートとして実証参加企業の管理者あてにメール通知を行い、対処を促す。

・ マルウエアへの感染が疑われるアラートをクラウドで自動判定し、検知したアラートの内容および実証参加企業が実施する必要がある対処内容を記載し、「重要アラート」として、実証参加企業あてにメール通知した。通知は、1 時間に 1 回、検知したアラートをまとめて通知を行った。同種のアラートが繰り返し発生した際に大量のメールが発生し、重要なメールが埋もれてしまい対処されない可能性を考慮したためである。

・ 各セキュリティ機能と検知内容と説明、通知方法の関係は以下のとおりである。

表 3-7　セキュリティ機能とアラートメール通知方法

略称	検知した通信	説明	ログ記録・ポータル表示	メール通知
IPS	外部からの攻撃	インターネットからイントラネットへの通信データ内に攻撃コードなどの異常なデータが含まれていることを検知し、通信を遮断	○	—
	外部への不正通信	社内の端末がマルウエアに感染したことによるインターネットへの不正通信を遮断	○	○（※1）
	内部の脆弱性	ルーターあてなど内部の通信で、脆弱なパスワード（デフォルトのパスワードを使用など）を使用したHTTP Basic 認証の通信を検知・遮断	○	○
AV	外部からの攻撃	エンドユーザーによるメール受信、その他のアプリケーションの通信を監視し、ダウンロードするファイルにウイルスが含まれていることを検知し、ファイルの内容を書き換え無害化	○	—
	外部への不正通信	エンドユーザーによるメール送信、その他のアプリケーションの通信を監視し、アップロードするファイルにウイルスが含まれていることを検知し、ファイルの内容を書き換え無害化	○	○
WG	外部への不正通信	マルウエアによる攻撃者が用意した外部サーバーへの通信や、エンドユーザーによるウェブ閲覧によってマルウエア感染を起こすなどの有害な Web サイトに対するアクセスを検知し通信を遮断	○	○
UF	外部の Web サイトへのアクセス	予め用意されているWebサイトのカテゴリに該当するWebサイトへのアクセスを検知	○	—
APG	外部へのアプリケーションを使用した通信	ファイル交換ソフトや動画共有アプリ、メッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションを利用した際の通信を検知	○	—

重要度	説明
★★★　（高）	マルウエア感染の可能性が高い（所定サイバーインシデント初動対処の対象＝簡易サイバー保険発動対象）
★★☆　（中）	マルウエア感染の可能性が考えられる
★☆☆　（低）	マルウエア感染の可能性は低い
無し	マルウエア感染の可能性は極めて低い （アラートメール通知はしない）

※1：ユーザーによる対処不要なアラートはメール通知しない

・ 以下のログ情報を UTM で取得し、ポータルに掲載している。
  - アクセス先 IP アドレス/ポート番号
  - アクセス元 IP アドレス/ポート番号
  - 企業 LAN 側の端末 MAC アドレス
  - プロトコル
  - 脅威名、脅威 ID（IPS の場合）
  - ウイルス名、ウイルス ID、ファイル名、メールタイトル、メールの日時（AV の場合）
  - アクセス先、URL（WG、UF の場合）
  - アプリケーション名（APG の場合）

3.4.3 所定サイバーインシデント初動対処とリモートお助けの実施方法の概要

(1) 所定サイバーインシデント初動対処の全体概要

・ アラート通知メールのうち、重要度★★★メールを送信した実証参加企業は、所定サイバーインシデント初動対処（駆け付けお助けまたはリモートお助け）の対象とする。

・ 所定サイバーインシデント初動対処（駆け付けお助けまたはリモートお助け）はお助け実働隊地域 IT 事業者が行う。実証参加企業の出入りの IT 事業者などによる支援は想定していない。なお、お助け実働隊地域 IT 事業者は原則として相談窓口から実証参加企業にお助け実働隊地域 IT 事業者リストを渡し、実証参加企業自身が選択し、アポイント日時も当該 2 者間で決定することを原則とするが、例外的に事務局が間に入って調整することもある。

・ 駆け付けお助けかリモートお助けかは、相談窓口または事務局が、該当実証参加企業に対し、両方のメリット、デメリットを説明した上で、原則として実証参加企業が選択する。

(2) 駆け付けお助けの意義

・ リアルの「駆け付け」は、所定サイバーインシデント時（上記★★★メール送信時＝保険発動事由を満たす深刻度）に現地訪問して初動対処を行うことであり、これが実証ならびに商用のセキュリティサービスの目玉と言えるアピール点である。

・ 緊急事態宣言下での中小企業のテレワーク実施率が全国的にあまり高くないことも勘案すると、中小企業は良くも悪くも“リアル”“対面”“アナログ”“現場”を重視・評価する傾向ある。よって、困ったときに専門家が駆け付けてくれる安心感はサービスの強い訴求要素と言えよう。

・ 実際のところ、多数のインシデント現場に同席した経験から言えば、中小企業の中には、

ウイルス対策ソフトがパソコン画面のどこをクリックすれば“出てくるのか”すら分かっていない企業がある。それどころか、無料試用期間が終了しているウイルス対策ソフトを“入っている”と勘違いしているケースも少なくない。Windows アップデートをしていない中小企業が、ウイルス対策ソフトのパターンファイルの最新化をしているとも考えにくい。よしんばウイルス対策ソフトを（有効に）入れており、かつ最新化（自動更新される場合を含む）されているとしても、フルスキャン実施にたどり着くのは容易なことではない。IT 事業者が“普通はできるはず”と考える作業も“知っていて当然”と考える IT 用語も、中小企業には高いハードルであるという点を今一度改めて認識する必要性がある。よって「駆け付け」は中小企業への寄り添いという点では、必要不可欠なサービス種目と言える。

(3) リモートお助けの意義と実施の流れ

・ 緊急事態宣言の発令時や交通の便の悪い地域などにおいて、インシデント発生時の支援を安定的かつ実効性ある形で提供できる手法

・ リモートお助けは、以下の流れで実施する

表 3-8　リモートお助け実施方法

実施対象	・ 重要度：★★★のアラートメール ・ 今年度実証では、重要度：★★☆のアラートの中でも、個別調査の結果、必要に応じて初動対処を実施した。
実施方法	・ 遠隔コミュニケーションツール ・ 電話 ・ メール
実施タイミング	・ 重要度：★★★のアラートメール発報時 ・ 重要度：★★☆のアラートメール発報後、個別調査の結果、お助け対象と判断されたタイミング

・リモートお助けの有効性確認は、以下を対象に実施した。

表 3-9　リモートお助け有効性確認方法

実施対象	・ インシデント対応企業 ・ お助け実働隊地域 IT 事業者
実施方法	・ インシデント対応企業：アンケート ・ お助け実働隊地域 IT 事業者：ヒアリング
実施タイミング	・ インシデント対応完了後

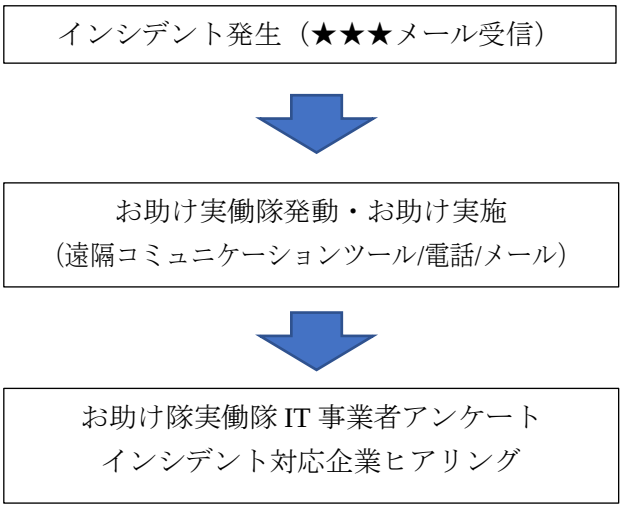


図 3-6　リモートお助け有効性確認実施フロー

・電話やメールでの支援で解決できない場合に遠隔コミュニケーションツールを使用し、動画などを確認しながら支援をすることを想定する。それでもなお解決しない場合や、実証参加企業が希望する場合は、訪問お助けを実施する。

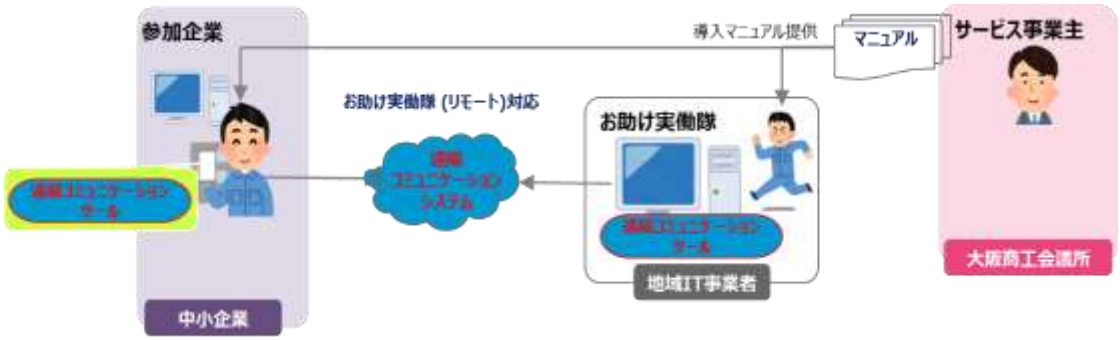


図 3-7　リモートお助け概要図

3.4.3.2 非大都市でのリモートツールを用いたインシデント対応支援の有効性確認を計測する観点

リモートお助け実施後のお助け隊実働隊 IT 事業者アンケート、インシデント対応企業ヒアリング結果から、非大都市でのリモートツールを用いたインシデント対応支援の有効性を確認する。

アンケート・ヒアリングは以下の観点で実施する。

表 3-10　リモートお助け隊に関するアンケートの観点

1. お助け実働隊地域 IT 事業者	
1-1	リモートお助けのみでのインシデント解決有無
1-2	リモートお助けの対応時間の変化
1-3	リモートお助け時のツールの利用環境・利用方法
1-4	リモートツールでの実施作業・状況把握可否
1-5	お助け実働隊地域 IT 事業者視点で感じたリモート対応のメリット/デメリット
2. インシデント対応企業観点	
2-1	中小企業視点で感じたリモート対応のメリット/デメリット
2-2	現場へ駆け付けた場合はどのような事例だったか

3.4.4 テレワークツールの概要

3.4.4.1 目的

with コロナ時代を鑑みて、テレワークを余儀なくされる中小企業に対し、社外に情報を持ち出すことを防ぎ”セキュリティリスクを低減”するための「テレワークツール」を提供する。テレワーク環境におけるセキュリティ脅威の実態把握とテレワークツールによるセキュリティリスク低減効果の確認を目的とする。

3.4.4.2 テレワーク実証の実施方法

テレワーク実証は、以下を対象に実施した。

表 3-11　テレワーク実証実施方法

実施対象	テレワーク実証参加企業
実施方法	テレワークツール提供
実施タイミング	実証開始時（テレワークツール希望時のみ）

テレワーク実証では、テレワーク環境におけるセキュリティ脅威の実態把握、テレワークツール効果測定の 2 つを実施した。それぞれ以下を対象に実施した。

表 3-12　テレワーク環境におけるセキュリティ脅威の実態把握方法

実施対象	実証参加全企業
実施方法	アンケート
実施タイミング	実証開始時

表 3-13　テレワークツール効果測定方法

実施対象	テレワーク実証参加企業（希望企業）
実施方法	アンケート （テレワークツールを利用し、実施前後の回答があった企業のみ有効回答とする）
実施タイミング	テレワーク実証実施前後

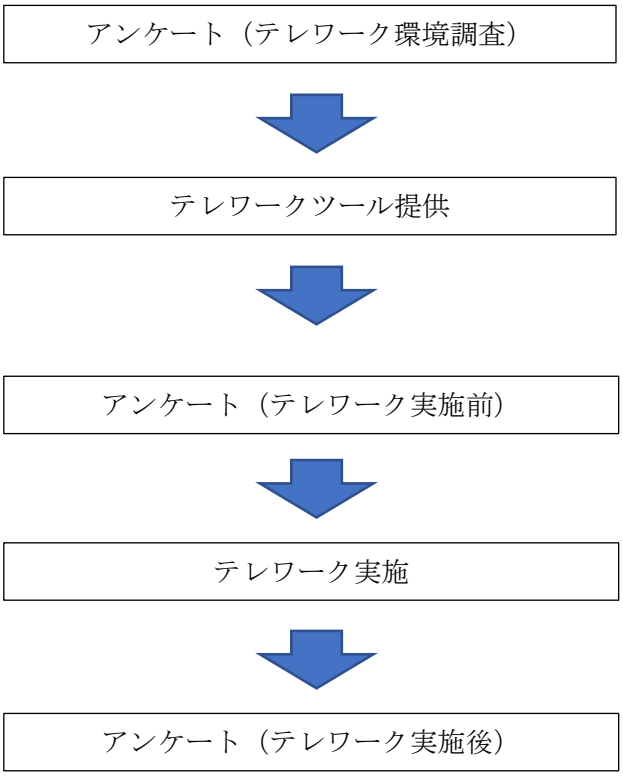


図 3-8　テレワーク実証フロー

テレワーク環境調査は実証参加全企業を対象に実施した。

テレワーク効果測定は、既にテレワークツールを導入しているか否かに関わらず、テレワークツールを希望する企業に対してテレワークツールを提供し、テレワークツール利用前後でアンケートを行った。

3.4.4.3 セキュリティ脅威の実態把握およびテレワークの効果測定アンケート観点

テレワーク環境におけるセキュリティ脅威の実態把握は、テレワーク環境調査アンケートをもとに確認する。

テレワークツール効果測定は、テレワークツール実施前後のアンケートをもとに持ち出しの有無を確認する。

アンケートは以下の観点で実施する。

表 3-14　テレワークに関するアンケート観点

1. テレワーク環境におけるセキュリティ脅威の実態把握	
1-1	重要書類の保管
1-2	重要書類の持ち出し管理
1-3	重要な電子データのアクセス管理
1-4	重要な電子データの持ち出し管理
1-5	テレワーク時の実施場所
1-6	テレワーク時の使用回線
1-7	テレワーク時の社内ネットワークへの接続方法
1-8	テレワーク時の使用端末
1-9	テレワーク時に使用している端末のセキュリティ対策
2. テレワークツール効果測定	
2-1	1 週間の重要情報の持ち出し回数（実施前後比較）
2-2	データ持ち出し方法（実施前後比較）
2-3	持ち出し理由（実施前後比較）

3.4.4.4 情報漏洩に繋がらないセキュアなテレワークの仕組みを提供

本実証で提供するテレワークツールには、RemoteView を選定した。RemoteView は、外出先のモバイル端末から、会社の PC にセキュアにアクセスし、遠隔操作することができるリモートアクセスサービスである。

RemoteView を使用した接続までの流れは以下のとおりである。

1. 操作したい PC（会社 PC）にエージェントを事前にインストールする。
2. 自宅や外出先など遠隔地 PC でブラウザ※を起動し、専用サイトにログインする。
3. RemoteView Server が、遠隔地からのログインを認証し、遠隔接続が開始される。

※スマートフォンやタブレットからは専用アプリで接続

遠隔地の PC と操作される PC 間は SSL 通信を適用し、相互通信されるデータには AES 256bit の標準暗号化処理号体系を使用している。画面転送により業務データを自宅や外出先に持ち出さないセキュアな業務環境を構築可能である。

図 3-9　テレワークツール概要図

3.4.5 現在におけるセキュリティ実態把握のための簡易なセキュリティ診断の概要

3.4.5.1 目的

実証対象地域における現在のセキュリティ対策の実態を把握するために、簡易なセキュリティ診断を実施する。

簡易セキュリティ診断結果を通して、自社のセキュリティ対策の取り組み状況を客観的に確認することで、重点的に取り組まなければならない課題を把握し、実証対象地域企業のサイバーセキュリティに関する意識向上・普及啓発に繋げることを目的とする。

3.4.5.2 簡易セキュリティ診断の実施方法

簡易セキュリティ診断は、以下の企業を対象に実施した。

表 3-15　簡易セキュリティ診断実施方法

実施対象	事業説明会参加企業（オンライン参加企業含）
実施方法	「紙」または「Web」
実施タイミング	事業説明会内で実施（所要時間：15 分程度）

事業説明会は、会場での参加だけでなく、オンラインでの説明会参加企業に対応するため、実施方法としては「紙」と「Web」の 2 種類を準備した。

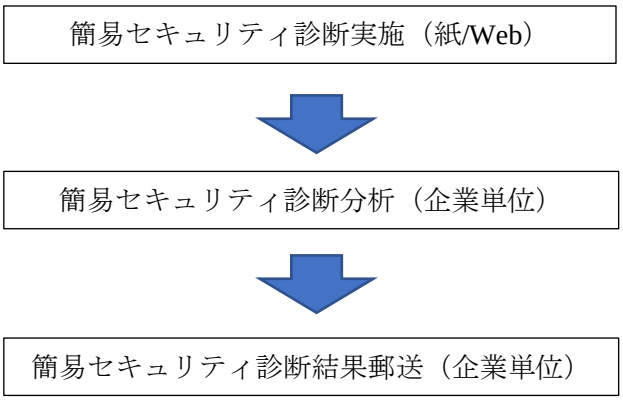


図 3-10　簡易セキュリティ診断実施フロー

簡易セキュリティ診断の回答内容は、企業単位に分析を行い、分析結果（PDF 形式）を後日各企業へ郵送する。

分析出力結果にはレーダーチャートを使用し、どのような分野を重点的に取り組まなければならないかを視覚的に分かりやすくした。

3.4.5.3 簡易セキュリティ診断項目

簡易セキュリティ診断の構成は以下のとおりである。

回答方式を選択式とし、回答内容を独自に点数化したものと「評価基準」を照合することで「総合判定」「カテゴリ別判定」を行う方式である。

カテゴリ 4 はカテゴリ 1～3 の項目のうち、「情報セキュリティ 5 か条」に該当する項目を評価し、自社の「SECURITY ACTION（一つ星宣言）」達成状況も合わせて確認できるようにした。

表 3-16　簡易セキュリティ診断項目構成

カテゴリ	項目数
1. 組織的セキュリティの取り組み	11 項目
2. 情報システム／ネットワークセキュリティの取り組み	10 項目
3. リモートワークセキュリティの取り組み	4 項目
4. SECURITY ACTION（一つ星宣言）	（6 項目）*1
計	25 項目

*1：項目数は内数

表 3-17　回答方式と選択肢

回答方式	選択式（4 択）		
選択肢（*1）	◎	できている	ない
	△	一部できていない	不明
	×	できていない、不明	ある
	ー	対象外	対象外

*1：選択肢は設問によって 2 パターンの回答がある

表 3-18　評価基準

判定	自己評価	内容
A（良く対策できている）	80%以上	全ての項目で望まれる対応ができている
B（更なる改善を推奨）	65%以上	全ての項目で何らかのセキュリティ対策を行っているが、更なる改善が必要な項目がある
C（見直しが必要）	30%以上	一部のセキュリティ対策は行われているが、対策が不十分な項目が残っている
D（全面的に見直しが必要）	30%未満	早急なセキュリティ対策が必要な状態

表 3-19　簡易セキュリティ診断項目（カテゴリ 1）

1. 組織的セキュリティの取り組み		
1-1	情報セキュリティに関する脅威や攻撃の手口について最新情報の収集	○
1-2	他者に推測されにくい「複雑さ」を確保したパスワード設定ルールの採用とパスワード使い回しの禁止	○
1-3	適切ではない人が重要情報にアクセスできないように、アクセス権の定期的な見直し実施	○
1-4	組織として許可されたソフトウエアの使用	
1-5	無線 LAN や外部ネットワーク入口の設置場所や数の把握・管理	
1-6	PC や媒体、重要文書（図面など）や媒体を社外に持ち出すときのルール（盗難や紛失対策）の策定と周知	
1-7	添付ファイル付きメール送付時のパスワード付与などのルール策定と運用	○
1-8	原則、私物媒体の業務使用の禁止	
1-9	私物の媒体を業務で使用することを許可する場合、社有品と同などのセキュリティ対策の策定と周知	
1-10	取引先から自社セキュリティ対策への取り組み状況のヒアリングや具体的な対策実施要望の有無	
1-11	社内に情報システム部門（IT 資産や IT システムを管理する部門）の設置、もしくは専任担当者の配置	

○：「SECURITY ACTION（一つ星宣言）」該当項目

表 3-20　簡易セキュリティ診断項目（カテゴリ 2）

2. 情報システム／ネットワークセキュリティの取り組み		
2-1	コンピュータウイルスから情報システムを保護するためのウイルス対策ソフト導入と新種ウイルスにも対応できるよう定義ファイルの常時最新化	○
2-2	セキュリティ修正パッチ公開の都度、情報システムの OS やソフトウエアに対する適用の実施	○
2-3	業務に関係の無いサイトへのアクセスを行わせない仕組みの導入	
2-4	自社が外部に公開するサービス（電子商取引、オンライン取引、外部向けのホームページやシステム／サービスなど）に対して、不正アクセスの防止、なりすましの防止、否認の防止、脆弱性対応などの対策実施	
2-5	インターネットを介したウイルス感染や SNS に対する書き込みなどのトラブルへの対策実施	
2-6	情報システムに対し、アクセスログやイベントログなどの取得と、必要に応じた保護（改ざんなどを防止）と活用の準備	
2-7	通信ネットワークを流れる重要なデータを脅威から守るために、必要に応じて暗号化などの対策実施	
2-8	外部からの脅威に対する、社内のネットワークの保護	
2-9	インシデント（情報システム障害、ウイルス感染など）の対応手順の策定と周知	
2-10	過去の情報セキュリティに関連する問題（未遂を含む）発生の有無	

○：「SECURITY ACTION（一つ星宣言）」該当項目

表 3-21　簡易セキュリティ診断（カテゴリ 3）

3. リモートワークセキュリティの取り組み	
3-1	外出時、必要のない情報資産（取引先の連絡先リスト、社員名簿など）の社外持ち出し有無
3-2	原則、私物の PC やスマホなどのリモートワーク使用の禁止
3-3	私物の PC やスマホをリモートワークで使用することを許可する場合、社有品と同などのセキュリティ対策の策定と周知
3-4	会社のメールを個人の携帯、スマホ、PC などへの転送の有無

○：「SECURITY ACTION（一つ星宣言）」該当項目

4. 実施結果

4.1 説明会の開催結果

4.1.1 事業説明会の開催結果

・ 説明会は新型コロナウイルス感染症の感染拡大防止のため、受講可能人数を制限（定員の 1/2～1/3）して実施した。このため同一会場で 2 回転ずつ実施した。

・ この時点では感染再拡大（第三波）が深刻化していなかったため、リアル開催をメインと位置づけ、ライブによるオンライン配信は行わず、オンライン受講希望者に対しては、リアル開催を録画したものを動画コンテンツ化し当該コンテンツの視聴先 URL を後日案内し、後日各自でアクセスして受講する形を採った。

表 4-1　事業説明会概要（滋賀県）

開催日時	令和 2 年 10 月 1 日（木）　（1）13:00～14:20　（2）15:00～16:20
場所、形態	びわ湖大津プリンスホテル（リアル開催）
参加者数	（1）3 社 4 人　（2）5 社 6 人　計 8 社 10 人
アジェンダ	① with コロナ時代における中小企業のテレワークとセキュリティ（日本電気（株）） ②中小企業における情報セキュリティ対策支援のご紹介（ライブ配信）（IPA） ③サイバーセキュリティお助け隊事業と参加中小企業などのメリット（大阪商工会議所） ④簡易セキュリティ診断
開催結果	・4 社の実証への参加が得られた（うち 1 社は収録動画を見て） ・アンケートで受講企業でのサイバー攻撃と対策状況などが把握できた

表 4-2　事業説明会概要（奈良県①）

開催日時	令和 2 年 10 月 2 日（金）　（1）13:15～14:35　（2）15:00～16:20
場所、形態	奈良商工会議所（リアル開催）
参加者数	（1）4 社 4 人　（2）6 社 6 人　計 10 社 10 人
アジェンダ	① with コロナ時代における中小企業のテレワークとセキュリティ（（株）ブルーオーキッドコンサルティング） ②中小企業における情報セキュリティ対策支援のご紹介（録画放映）（IPA） ③サイバーセキュリティお助け隊事業と参加中小企業などのメリット（大阪商工会議所） ④簡易セキュリティ診断
開催結果	・6 社の実証への参加が得られた ・アンケートで受講企業でのサイバー攻撃と対策状況などが把握できた

表 4-3　事業説明会概要（奈良県②）

開催日時	令和 2 年 10 月 6 日（火）　（1）13:15～14:35　（2）15:00～16:20
場所、形態	橿原商工会議所（リアル開催）
参加者数	（1）6 社 6 人　（2）3 社 3 人　計 9 社 9 人
アジェンダ	①　with コロナ時代における中小企業のテレワークとセキュリティ （（株）ブルーオーキッドコンサルティング） ②中小企業における情報セキュリティ対策支援のご紹介（録画放映） （IPA） ③サイバーセキュリティお助け隊事業と参加中小企業などのメリット（大阪商工会議所） ④簡易セキュリティ診断
開催結果	・9 社の実証への参加が得られた ・アンケートで受講企業でのサイバー攻撃と対策状況などが把握できた

表 4-4　事業説明会概要（和歌山県）

開催日時	令和 2 年 10 月 7 日（水）　（1）13:00～14:20　（2）15:00～16:20
場所、形態	ホテルグランヴィア和歌山（リアル開催）
参加者数	（1）3 社 3 人　（2）8 社 9 人　計 11 社 12 人
アジェンダ	①with コロナ時代における中小企業のテレワークとセキュリティ（日本電気（株）） ②中小企業における情報セキュリティ対策支援のご紹介（録画放映） （IPA） ③サイバーセキュリティお助け隊事業と参加中小企業などのメリット（大阪商工会議所） ④簡易セキュリティ診断
開催結果	・8 社の実証への参加が得られた（うち 2 社は収録動画を見て） ・アンケートで受講企業でのサイバー攻撃と対策状況などが把握できた

図 4-1　説明会の様子

4.2 実態把握結果

4.2.1 中小企業などの実態把握結果

(1) アンケートなどによる実態把握

① 滋賀県・奈良県・和歌山県の中小企業などがさらされているサイバー攻撃の実態（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）

表 4-5 サイバー攻撃の有無

①－1 サイバー攻撃の有無（複数回答有）	※参考 令和 2 年度成果報告会（実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
HP接続不能/大量メール受信	3（7%）	1（2%）	6（6%）
標的型攻撃メール/ビジネスメール詐欺	22（52%）	24（48%）	25（24%）
ランサムウエア（暗号化・身代金）	4（10%）	2（4%）	8（8%）
導入したシステムや製品にウイルスが混入	1（2%）	0（0%）	6（6%）
その他攻撃	4（10%）	2（4%）	8（8%）
分からない	13（31%）	19（38%）	被害と合わせ 58（55%））

①－2 サイバー攻撃の有無（複数回答有）	令和 2 年度実証参加企業 2020 年 10 月		
	滋賀県 n＝12 平均 37.4 人・中央 14.5 人	奈良県 n＝18 平均 24.2 人・中央 9.0 人	和歌山県 n＝20 平均 32.5 人・中央 6.0 人
HP接続不能/大量メール受信	0	1（6%）	0
標的型攻撃メール/ビジネスメール詐欺	7（58%）	10（56%）	7（35%）
ランサムウエア（暗号化・身代金）	0	0	2（10%）
導入したシステムや製品にウイルスが混入	0	0	0
その他攻撃	0	0	2（10%）
分からない	3（25%）	7（39%）	9（45%）

表 4-6　サイバー攻撃被害の有無

②－1 サイバー攻撃被害の有無 （複数回答有）	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
情報漏洩被害	3（7%）	0（0%）	2（2%）
システムダウン被害	2（5%）	0（0%）	0（0%）
データ損壊被害	4（10%）	3（6%）	5（5%）
金銭拠出被害	1（2%）	0（0%）	0（0%）
流通途絶被害	1（2%）	0（0%）	0（0%）
分からない	26（62%）	33（66%）	攻撃と合わせ（58（55%））

②－2 サイバー攻撃被害の有無 （複数回答有）	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
情報漏洩被害	0	0	0
システムダウン被害	0	0	0
データ損壊被害	1（8%）	1（6%）	1（5%）
金銭拠出被害	0	0	0
流通途絶被害	0	0	0
分からない	7（58%）	15（83%）	11（55%）

② 滋賀県・奈良県・和歌山県の中小企業などにおけるサイバーセキュリティ対策状況（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）

表 4-7　情報システム担当者の有無

③－1 情報システム担当者の有無	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
専任者がいる	7（17%）	3（6%）	9（9%）
兼任者しかいない	22（52%）	17（34%）	34（32%）
1 人もおらず経営層が直轄	9（21%）	22（44%）	52（50%）
1 人もおらず IT 業者に外注	3（7%）	7（14%）	10（10%）
回答無し	1（2%）	1（2%）	—

③－2 情報システム担当者の有無	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
専任者がいる	0	1（6%）	2（10%）
兼任者しかいない	5（42%）	7（39%）	5（25%）

1 人もおらず経営層が直轄	4(33%)	9(50%)	9(45%)
1 人もおらず IT 業者に外注	3(25%)	1(6%)	3(15%)
回答無し	0	0	1(5%)

表 4-8　情報システム関係の業務マニュアルの有無

④－1 情報システム関係の業務マニュアルの有無	※参考 令和 2 年度成果報告会 (実証参加企業以外) 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 (回答率 50/53=94%) 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 (回答率 105/112=94%) 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
担当者以外に分かる社員がおらず業務マニュアルも無い	26(62%)	40(80%)	—
業務マニュアルがあるのでどの社員でも対応できる	10(24%)	0(0%)	—
回答無し	6(14%)	10(20%)	—

④－2 情報システム関係の業務マニュアルの有無	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
担当者以外に分かる社員がおらず業務マニュアルもない	10(83%)	14(78%)	16(80%)
業務マニュアルがあるのでどの社員でも対応できる	0	0	0
回答無し	2(17%)	4(22%)	4(20%)

表 4-9　サイバー対策年間経費（正社員情シス担当者人件費を除く）

⑤－1 サイバー対策年間経費(正社員情シス担当者人件費を除く)	※参考 令和 2 年度成果報告会 (実証参加企業以外) 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 (回答率 50/53=94%) 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 (回答率 105/112=94%) 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人	
5 万円未満	現在 11(26%) 今後 8(19%)	現在 32(64%) 今後 18(36%)	36(35%) 27(26%) 13(12%)	76(72%)
5～10 万	現在 9(21%) 今後 9(21%)	現在 8(16%) 今後 20(40%)	8(8%)	
11～20 万	現在 10(24%) 今後 8(19%)	現在 5(10%) 今後 5(10%)	9(9%)	
21～50 万	現在 3(7%) 今後 4(10%)	現在 4(8%) 今後 4(8%)	4(4%) 3(3%)	7(7%)

51 万以上	現在 6(14%) 今後 8(19%)	**現在 0(0%)** **今後 2(4%)**	2(2%) 2(2%)	4(4%)
回答無し	現在 3(7%) 今後 5(12%)	**現在 1(2%)** **今後 1(2%)**	1(1%)	

⑤−2 サイバー対策年間経費 (正社員情シス担当者人件費を除く)	令和 2 年度実証参加企業 2020 年 10 月		
	滋賀県 n＝12 平均 37.4 人・中央 14.5 人	**奈良県 n＝18** 平均 24.2 人・中央 9.0 人	**和歌山県 n＝20** 平均 32.5 人・中央 6.0 人
5 万円未満	**現在 8(67%)** **今後 7(58%)**	**現在 12(67%)** **今後 6(33%)**	**現在 12(60%)** **今後 5(25%)**
5〜10 万	**現在 2(17%)** **今後 2(17%)**	**現在 3(17%)** **今後 8(44%)**	**現在 3(15%)** **今後 10(50%)**
11〜20 万	**現在 1(8%)** **今後 0(0%)**	**現在 2(11%)** **今後 3(17%)**	**原罪 2(10%)** **今後 2(10%)**
21〜50 万	**現在 1(8%)** **今後 3(25%)**	**現在 1(6%)** **今後 1(6%)**	**原罪 2(10%)** **今後 0(0%)**
51 万以上	**現在 0(0%)** **今後 0(0%)**	**現在 0(0%)** **今後 0(0%)**	**現在 0(0%)** **今後 2(10%)**
回答無し	**現在 0(0%)** **今後 0(0%)**	**現在 0(0%)** **今後 0(0%)**	**現在 1(5%)** **今後 1(5%)**

表 4-10　サイバー攻撃対策のセキュリティ実施状況

⑥−1 サイバー攻撃対策のセキュリティ実施状況 (複数回答有)	※参考 令和 2 年度成果報告会 (実証参加企業以外) 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 (回答率 50/53=94%) 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 (回答率 105/112=94%) 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
アンチウイルスソフト	38(90%)	**46(92%)**	91(87%)
EDR・振る舞い検知	3(7%)	**—**	—
OS プロテクト型セキュリティ	1(2%)	**—**	—
ファイアウオール	20(48%)	**14(28%)**	40(38%)
UTM	22(52%)	**実証 UTM 除く 1(2%)**	実証 UTM 除く 8(8%)
その他 IT ベンダ提供のセキュリティサービス	3(7%)	**1(2%)**	3(3%)
データのパスワード設定	8(19%)	**6(12%)**	16(14%)
データの暗号化	7(17%)	**3(6%)**	6(6%)
物理的管理の徹底	7(17%)	**0(0%)**	6(6%)
社員教育・研修	17(40%)	**6(12%)**	14(14%)
専門人材育成	3(7%)	**0(0%)**	1(1%)
ISMS(ISO/IEC27001・27002)・CSMS	2(5%)	**0(0%)**	0(0%)
SECURITY ACTION	6(14%)	**4(8%)**	11(11%)
サイバー攻撃損害保険	3(7%)	**1(2%)**	0(0%)
取引先との情報管理契約	2(5%)	**2(4%)**	3(3%)

サプライチェーンでの規定などの制定・参加		0(0%)	1(1%)
特に実施していない	0(0%)	2(4%)	3(3%)

⑥－2 サイバー攻撃対策のセキュリティ実施状況 （複数回答有）	令和2年度実証参加企業　2020年10月		
	滋賀県　n＝12 平均37.4人・中央14.5人	奈良県　n＝18 平均24.2人・中央9.0人	和歌山県　n＝20 平均32.5人・中央6.0人
アンチウイルスソフト	10(83%)	17(94%)	19(95%)
EDR・振る舞い検知	—	—	—
OSプロテクト型セキュリティ	—	—	—
ファイアウオール	4(33%)	3(17%)	7(35%)
UTM	0	1(6%)	0
その他ITベンダ提供のセキュリティサービス	0	1(6%)	0
データのパスワード設定	1(8%)	4(22%)	1(5%)
データの暗号化	1(8%)	0	2(10%)
物理的管理の徹底	0	0	0
社員教育・研修	2(17%)	3(17%)	1(5%)
専門人材育成	0	0	0
ISMS(ISO/IEC27001・27002)・CSMS	0	0	0
SECURITY　ACTION	2(17%)	2(11%)	0
サイバー攻撃損害保険	0	1(6%)	0
取引先との情報管理契約	1(8%)	1(6%)	0
サプライチェーンでの規定などの制定・参加	0	0	0
特に実施していない	1(8%)	0	1(5%)

表 4-11　テレワーク実施状況

⑦－1 テレワーク実施状況	※参考 令和2年度成果報告会 （実証参加企業以外） 2021年1月 n=42 関西を中心とする中小企業	令和2年度実証参加企業 2020年10月 n=50 （回答率50/53=94%） 滋賀・奈良・和歌山 平均30.8人・中央10.0人	令和元年度実証参加企業 2020年1月 n=105 （回答率105/112=94%） 大阪・京都・兵庫 平均29.3人・中央11.5人
実施している （部分実施を含む）	—	17(34%)	—
実施していない	—	32(64%)	—
回答無し	—	1(2%)	—

⑦－2 テレワーク実施状況	令和2年度実証参加企業　2020年10月		
	滋賀県　n＝12 平均37.4人・中央14.5人	奈良県　n＝18 平均24.2人・中央9.0人	和歌山県　n＝20 平均32.5人・中央6.0人
実施している （部分実施を含む）	4(33%)	7(39%)	6(30%)
実施していない	8(67%)	11(61%)	13(65%)
回答無し	0	0	1(5%)

表 4-12　テレワーク未導入の理由

⑧－1 テレワーク未導入の理由 （複数回答有）	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
テレワークできない業務内容	—	21（66%）	—
コミュニケーションが取りづらい	—	3（9%）	—
費用対効果	—	1（3%）	—
セキュリティが心配	—	6（19%）	—
対応できる人材がいない	—	8（25%）	—
労務管理ルール	—	4（13%）	—
必要性を感じない	—	7（22%）	—
その他	—	1（3%）	—

⑧－2 テレワーク未導入の理由 （複数回答有）	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
テレワークできない業務内容	5（42%）	8（44%）	8（40%）
コミュニケーションが取りづらい	0	2（11%）	1（5%）
費用対効果	0	1（6%）	0
セキュリティが心配	1（8%）	4（22%）	1（5%）
対応できる人材がいない	1（8%）	5（28%）	2（10%）
労務管理ルール	1（8%）	2（11%）	1（5%）
必要性を感じない	2（17%）	1（6%）	4（20%）
その他	1（8%）	0	0

表 4-13　取引先からサイバー攻撃対策を求める意思表示の有無

⑨－1 取引先からサイバー攻撃対策を求める 意思表示の有無	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
取引要件とされつつある	6（14%）	2（4%）	4（6%）
指示されつつある	4（10%）	5（10%）	3（5%）
依頼されつつある	8（19%）	7（14%）	7（11%）
その動向は無い	23（55%）	35（70%）	51（77%）
回答無し	1（2%）	1（2%）	1（2%）

⑨－2 取引先からサイバー攻撃対策を求める	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人

意思表示の有無			
取引要件とされつつある	0	2(11%)	0
指示されつつある	1(8%)	2(11%)	2(10%)
依頼されつつある	3(25%)	2(11%)	2(10%)
その動向は無い	8(67%)	12(67%)	15(75%)
回答無し	0	0	1(5%)

表 4-14　サイバーセキュリティ対策を進める上での課題

⑩－1 サイバーセキュリティ対策を進める上での課題 (複数回答可)	※参考 令和 2 年度成果報告会 (実証参加企業以外) 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 (回答率 50/53=94%) 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 (回答率 105/112=94%) 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
コストの高さ・費用対効果	24(57%)	34(68%)	—
経営者・従業員の意識	26(62%)	20(40%)	—
面倒さ・可用性の低減	12(29%)	17(34%)	—
脅威が分からない・見えない	11(26%)	17(34%)	—
対策すべき内容・程度や対策商品が分からない	12(29%)	14(28%)	—
信頼できる IT ベンダがいない	7(17%)	9(18%)	—
対策している事実の効果的な対外 PR	6(14%)	—	—
その他	0(0%)	2(4%)	—

⑩－2 サイバーセキュリティ対策を進める上での課題 (複数回答可)	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
コストの高さ・費用対効果	8(67%)	14(78%)	12(60%)
経営者・従業員の意識	3(25%)	9(50%)	8(40%)
面倒さ・可用性の低減	3(25%)	6(33%)	8(40%)
脅威が分からない・見えない	4(33%)	7(39%)	6(30%)
対策すべき内容・程度や対策商品が分からない	4(33%)	6(33%)	4(20%)
信頼できる IT ベンダがいない	3(25%)	4(22%)	2(10%)
対策している事実の効果的な対外 PR	—	—	—
その他	1(8%)	1(6%)	0

③　滋賀県・奈良県・和歌山県の中小企業におけるサイバーセキュリティ対策に係るニーズの実態（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）

表 4-15　サイバーセキュリティお助け隊実証に期待すること

⑪-1 サイバーセキュリティお助け隊実証に期待すること （複数回答可）	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2020 年 1 月 n=105 （回答率 105/112=94%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
セキュリティの向上	—	30（60%）	—
自社のセキュリティ対策の妥当性確認	—	21（42%）	—
セキュリティ対策への助言の入手	—	21（42%）	—
セキュリティ関連情報の入手	—	12（24%）	—
セキュリティ製品・サービスの利用	—	8（16%）	—
その他	—	1（2%）	—

⑪-2 サイバーセキュリティお助け隊実証に期待すること （複数回答可）	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
セキュリティの向上	7（58%）	11（61%）	12（60%）
自社のセキュリティ対策の妥当性確認	7（58%）	9（50%）	5（25%）
セキュリティ対策への助言の入手	6（50%）	8（44%）	7（35%）
セキュリティ関連情報の入手	4（33%）	5（28%）	3（15%）
セキュリティ製品・サービスの利用	5（42%）	3（17%）	0
その他	0	0	1（5%）

表 4-16　サイバーインシデント発生時に必要となること

⑫-1 サイバーインシデント 発生時に必要となること	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2019 年 11 月 n=66 （回答率 66/112=59%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
電話や遠隔 PC 操作による相談・ウイルス除去などの簡易処置対応	20（48%）	28（56%）	48（73%）
IT 事業者などの駆け付けによる相談・ウイルス除去など簡易処置対応	18（43%）	23（46%）	31（47%）
感染した PC の初期化・クリーンナップ対応	18（43%）	22（44%）	26（39%）
感染した PC の買い替え対応	4（10%）	4（8%）	2（3%）
影響範囲や原因の調査	19（45%）	18（36%）	27（41%）
従業員へのサイバーセキュリティ教育	14（33%）	23（46%）	10（15%）
再発防止のためのセキュリティ強化	22（52%）	13（26%）	27（41%）
インシデントによる損害を補償するサイバー保険加入	10（24%）	3（6%）	6（9%）
その他	0（0%）	1（2%）	—

⑫-2 サイバーインシデント 発生時に必要となること	令和 2 年度実証参加企業　2020 年 10 月		
	滋賀県　n＝12 平均 37.4 人・中央 14.5 人	奈良県　n＝18 平均 24.2 人・中央 9.0 人	和歌山県　n＝20 平均 32.5 人・中央 6.0 人
電話や遠隔 PC 操作による相談・ウイルス除去などの簡易処置対応	5（42%）	14（78%）	9（45%）
IT 事業者などの駆け付けによる相談・ウイルス除去など簡易処置対応	6（50%）	7（39%）	10（50%）
感染した PC の初期化・クリーンナップ対応	6（50%）	9（50%）	7（35%）
感染した PC の買い替え対応	1（8%）	1（6%）	2（10%）
影響範囲や原因の調査	7（58%）	5（28%）	6（30%）
従業員へのサイバーセキュリティ教育	4（33%）	4（22%）	5（25%）
再発防止のためのセキュリティ強化	6（50%）	10（56%）	7（35%）
インシデントによる損害を補償するサイバー保険加入	0	2（11%）	1（5%）
その他	0	0	1（5%）

表 4-17　ウイルス対策ソフトで（最新バージョンにした上で）ウイルスの駆除を自社で行うことができるか

⑬ウイルス対策ソフトで（最新バージョンにした上で）ウイルスの駆除を自社で行うことができるか	※参考 令和 2 年度成果報告会 （実証参加企業以外） 2021 年 1 月 n=42 関西を中心とする中小企業	令和 2 年度実証参加企業 2020 年 10 月 n=50 （回答率 50/53=94%） 滋賀・奈良・和歌山 平均 30.8 人・中央 10.0 人	令和元年度実証参加企業 2019 年 11 月 n=66 （回答率 66/112=59%） 大阪・京都・兵庫 平均 29.3 人・中央 11.5 人
社員の誰かはできると思う	29（70%）	―	―
どの社員もできないと思う	8（19%）	―	―
分からない	4（10%）	―	―
無回答	1（2%）	―	―

4.2.2 簡易セキュリティ診断による実態把握結果

4.2.2.1 診断実施実績

簡易セキュリティ診断の実施実績は以下のとおりである。なお、簡易セキュリティ診断は実証参加企業の一部および実証不参加企業（事業説明会に出席した中小企業のうち結果的に実証に参加しなかった中小企業）を対象に行った。

表 4-18　簡易セキュリティ診断実施実績（地域別）

実施企業数	滋賀	16 社	28%
	奈良	19 社	33%
	和歌山	22 社	39%
	合計	57 社	

表 4-19　簡易セキュリティ診断実施実績（事業所規模別）

事業所規模	実施企業数	
1～5 人	21 社	37%
6～10 人	5 社	9%
11～20 人	11 社	19%
21～50 人	9 社	16%
51～100 人	3 社	5%
101～200 人	5 社	9%
201～300 人	2 社	4%
300 人以上	1 社	1%
合計	57 社	

表 4-20　簡易セキュリティ診断実施実績（業種別）

業種	実施企業数	
A 農業・林業	0 社	0%
B 漁業	0 社	0%
C 鉱業・採石業・砂利採取業	0 社	0%
D 建設業	4 社	7%
E 製造業	13 社	23%
F 電気・ガス・熱供給・水道業	0 社	0%
G 情報通信業	5 社	9%
H 運輸業・郵便業	3 社	5%
I 卸売業・小売業	8 社	14%
J 金融業・保険業	0 社	0%
K 不動産業・物品賃貸業	1 社	2%
L 学術研究・専門技術サービス業	7 社	12%
M 宿泊業・飲食店	1 社	2%
N 生活関連サービス業・娯楽業	0 社	0%
O 教育学習支援業	1 社	2%
P 医療・福祉	0 社	0%
Q 複合サービス事業	2 社	4%
R サービス業（他に分類されないもの）	12 社	21%
S 公務（他に分類されるものを除く）	0 社	0%
T 分類不能の産業	0 社	0%
合計	57 社	

4.2.2.2 診断結果集計（診断実施企業全体）

(1) 総評

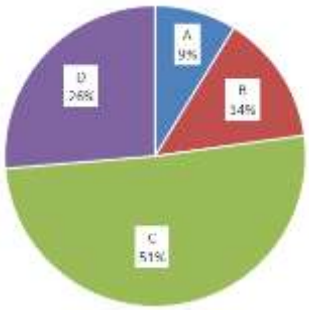


図 4-2　全体（総評）

(2) カテゴリ別

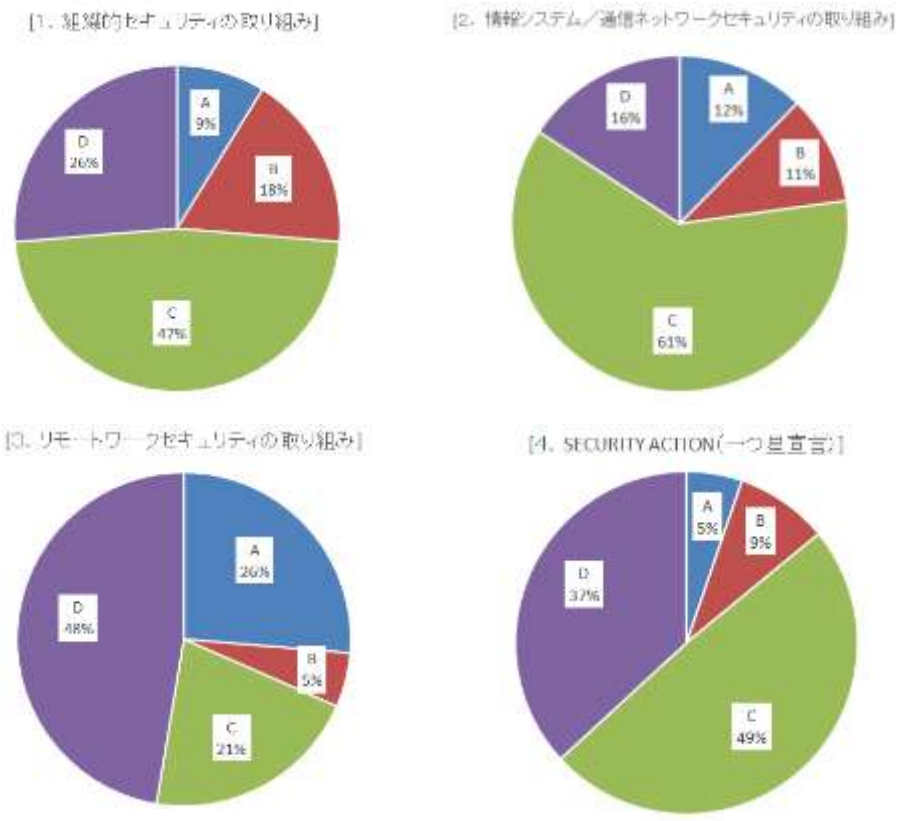
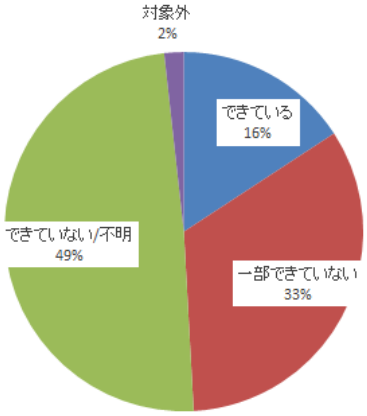


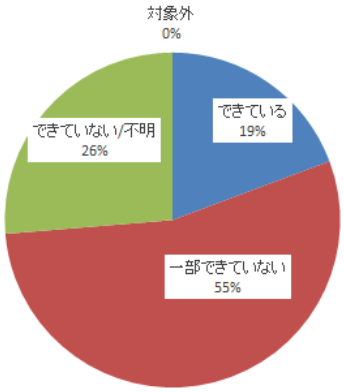
図 4-3　全体（カテゴリ別）

(3) 項目別

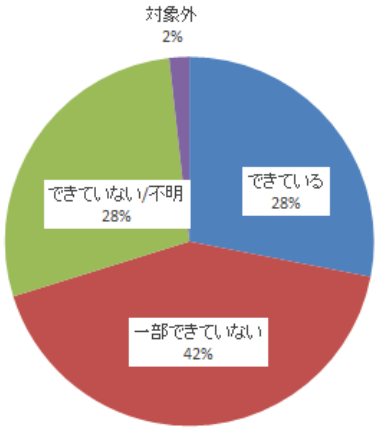
[Q1-1]
情報セキュリティに関する脅威や攻撃の手口について
最新情報の収集



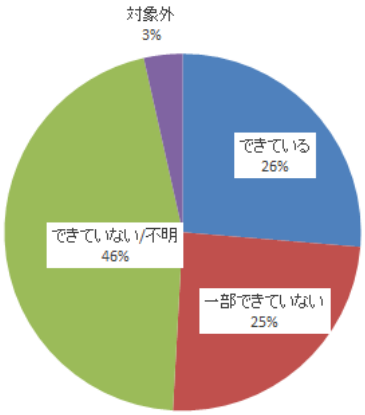
[Q1-2]
他者に推測されにくい「複雑さ」を確保した
パスワード設定ルールの採用と、パスワード使い回しの禁止



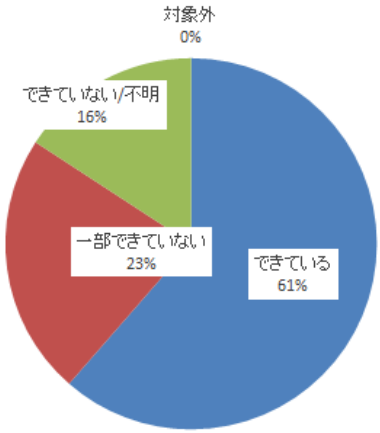
[Q1-3]
適切ではない人が重要情報にアクセスできないように
アクセス権の定期的な見直し実施



[Q1-4]
組織として許可されたソフトウェアの使用



[Q1-5]
無線LANや外部ネットワーク入口の設置場所や
数の把握・管理



[Q1-6]
PCや媒体、重要文書(図面など)や媒体を社外に
持ち出すときのルール(盗難や紛失対策)の策定と周知

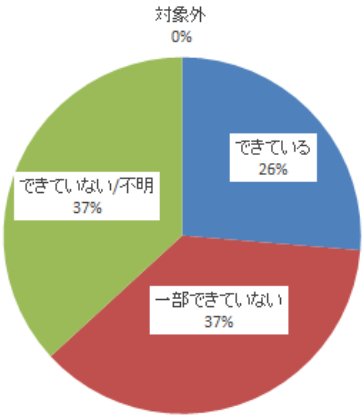
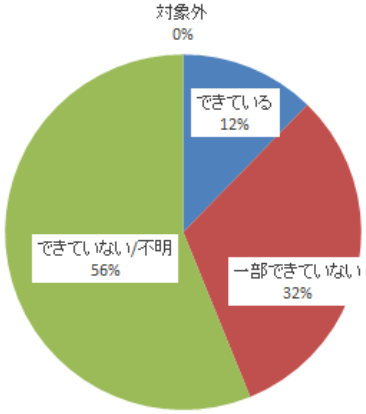
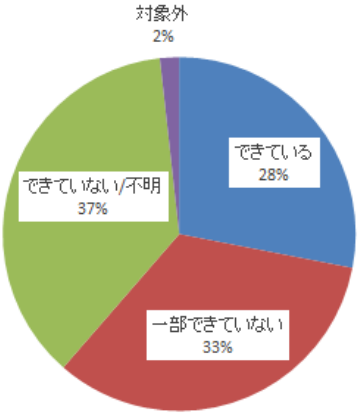


図 4-4　全体（項目別）[1/5]

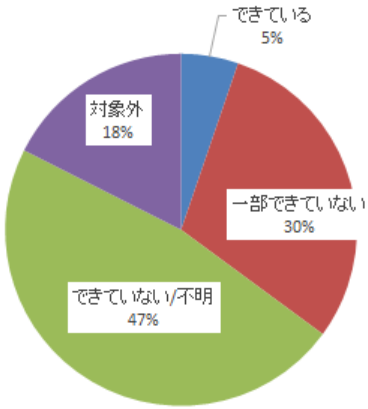
[Q1-7]
添付ファイル付きメール送付時のパスワード付与等のルール策定と運用



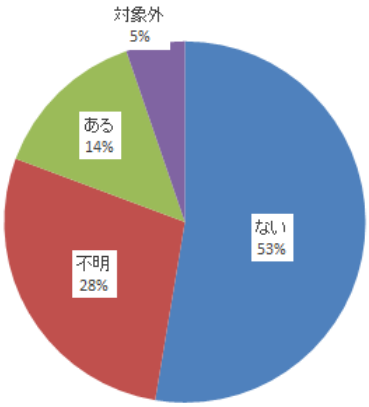
[Q1-8]
原則、私物媒体の業務使用の禁止



[Q1-9]
私物の媒体を業務で使用することを許可する場合社有品と同等のセキュリティ対策の策定と周知



[Q1-10]
取引先から自社のセキュリティ対策への取り組み状況のヒアリングや具体的な対策実施要望の有無



[Q1-11]
社内に情報システム部門(IT資産やITシステムを管理する部門)の設置、もしくは専任担当者の配置

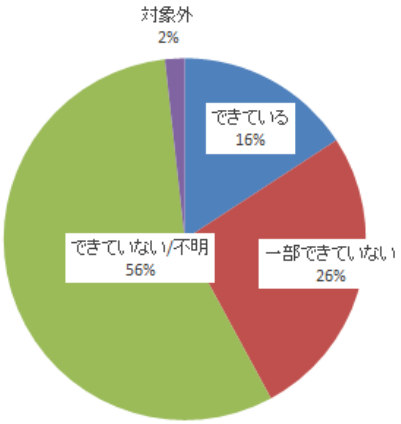
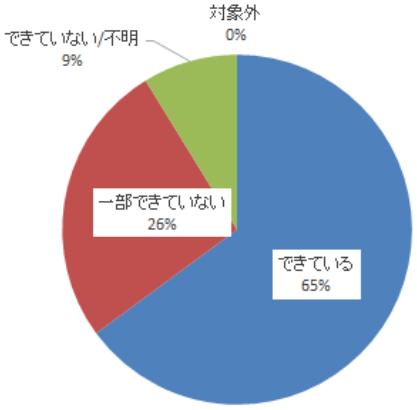
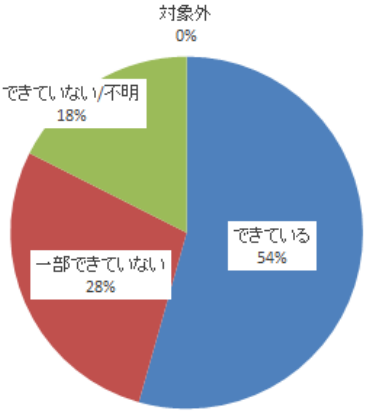


図 4-5　全体（項目別）[2/5]

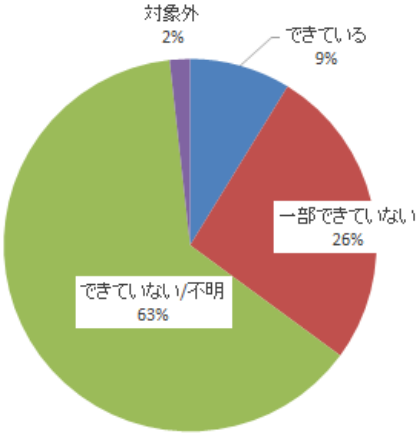
[Q2-1]
コンピュータウイルスから情報システムを保護するための
ウイルス対策ソフト導入と新種ウイルスにも対応できるよう
定義ファイルの常時最新化



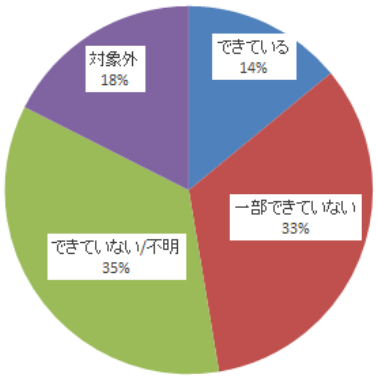
[Q2-2]
セキュリティ修正パッチ公開の都度、情報システムの
OSやソフトウェアに対する適用の実施



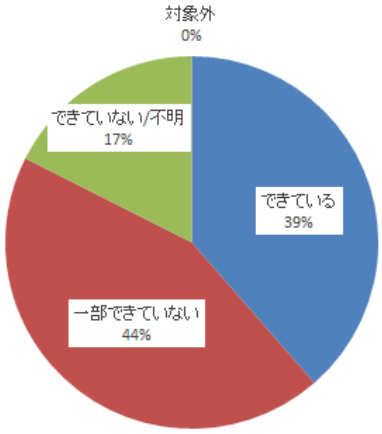
[Q2-3]
業務に関係の無いサイトへのアクセスを
行わせない仕組みの導入



[Q2-4]
自社が外部に公開するサービス(電子商取引、オンライン取引、外部向
けのホームページやシステム／サービスなど)に対して、不正アクセスの
防止、なりすましの防止、否認の防止、ぜい弱性対応などの対策実施



[Q2-5]
インターネットを介したウイルス感染やSNSへの書き込みなどの
トラブルへの対策実施



[Q2-6]
情報システムに対し、アクセスログやイベントログなどの取得と、
必要に応じた保護(改ざんなどを防止)と活用の準備

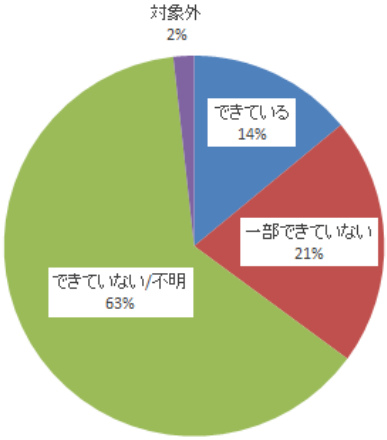
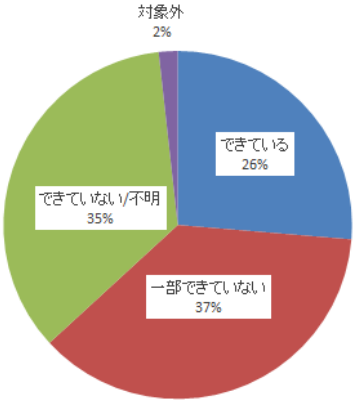
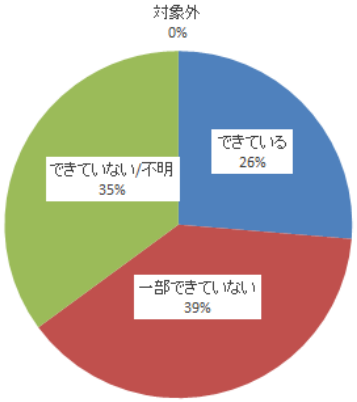


図 4-6　全体（項目別）[3/5]

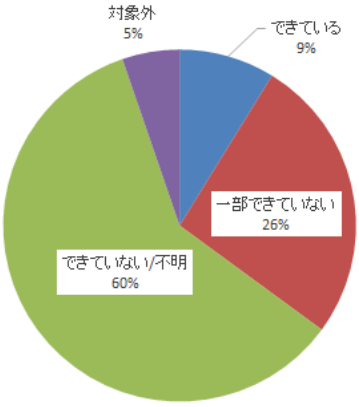
[Q2-7]
通信ネットワークを流れる重要なデータを脅威から守るために、必要に応じて暗号化などの対策実施



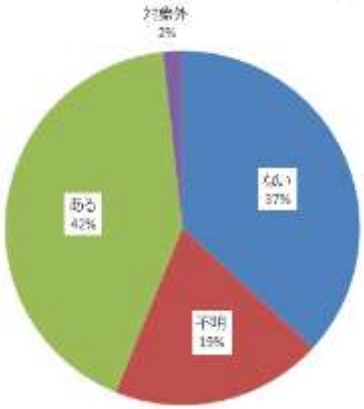
[Q2-8]
外部からの脅威に対する、社内のネットワークの保護



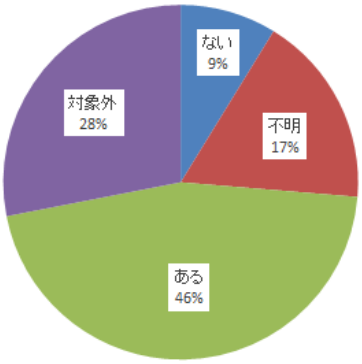
[Q2-9]
インシデント(情報システム障害、ウイルス感染など)の対応手順の策定と周知



[Q2-10]
過去の情報セキュリティに関連する問題(未遂含む)発生の有無



[Q3-1]
外出時、必要のない情報資産(取引先の連絡先リスト、社員名簿等)の社外持ち出し有無



[Q3-2]
原則、私物のPCやスマホなどのリモートワーク使用の禁止

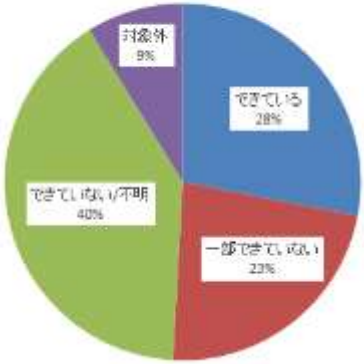


図 4-7　全体（項目別）[4/5]

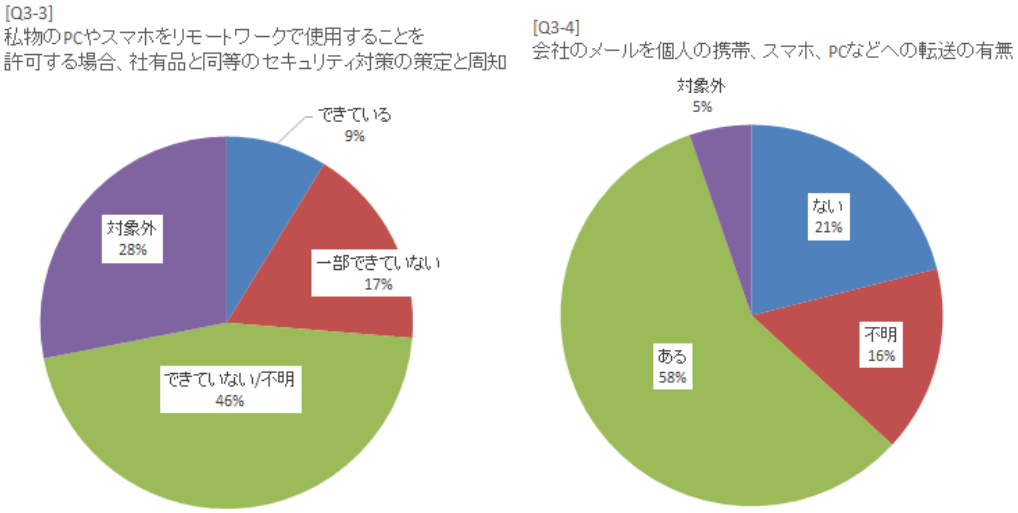

[Q3-3]
私物のPCやスマホをリモートワークで使用することを
許可する場合、社有品と同等のセキュリティ対策の策定と周知
できている
9%
一部できていない
17%
できていない/不明
46%
対象外
28%
[Q3-4]
会社のメールを個人の携帯、スマホ、PCなどへの転送の有無
ない
21%
不明
16%
ある
58%
対象外
5%

図 4-8　全体（項目別）[5/5]

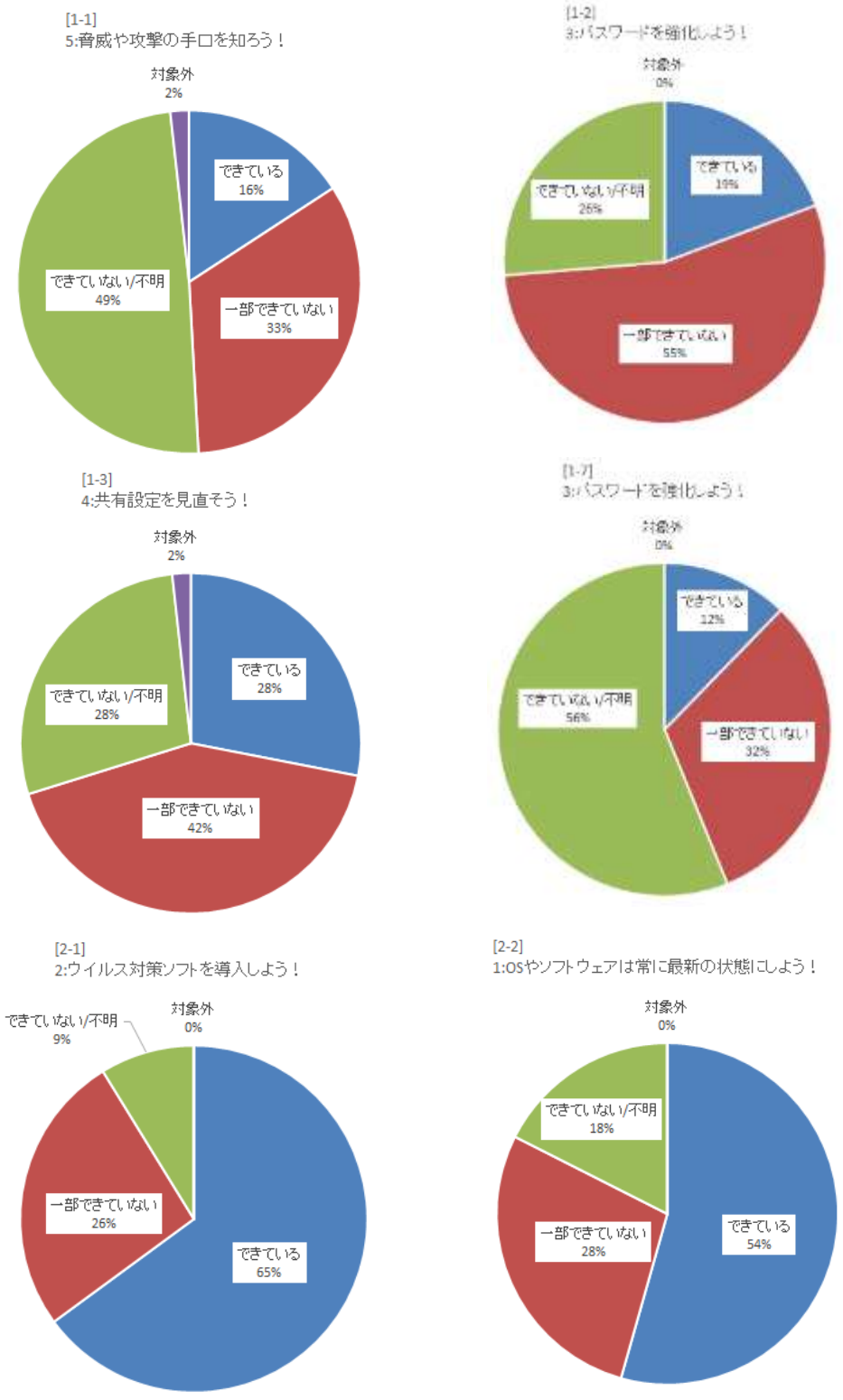


図 4-9　全体（SECURITY ACTION 関連項目）

4.2.2.3 診断結果集計（地域別）

(1) 地域内訳

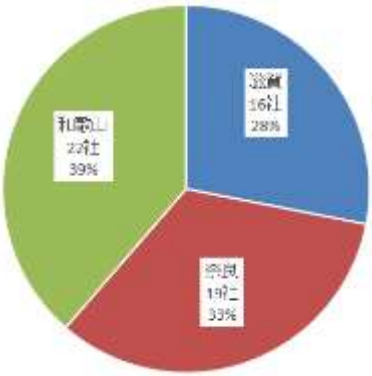


図 4-10　地域内訳

(2) 総評

図

(3) カテゴリ別

図 4-12　カテゴリ別（1. 組織的セキュリティの取り組み）

図 4-13　カテゴリ別（2.　情報システム／通信ネットワークセキュリティの取り組み）

図 4-14　カテゴリ別（3. リモートワークセキュリティの取り組み）

図 4-15　カテゴリ別（4. SECURITY ACTION（一つ星宣言））

4.2.2.4 診断結果集計（事業所規模別）

(1) 事業所規模内訳

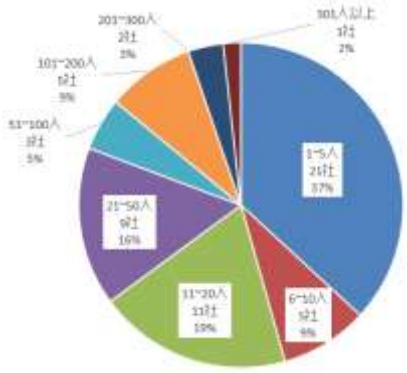


図 4-16　事業所規模内訳

(2) 総評

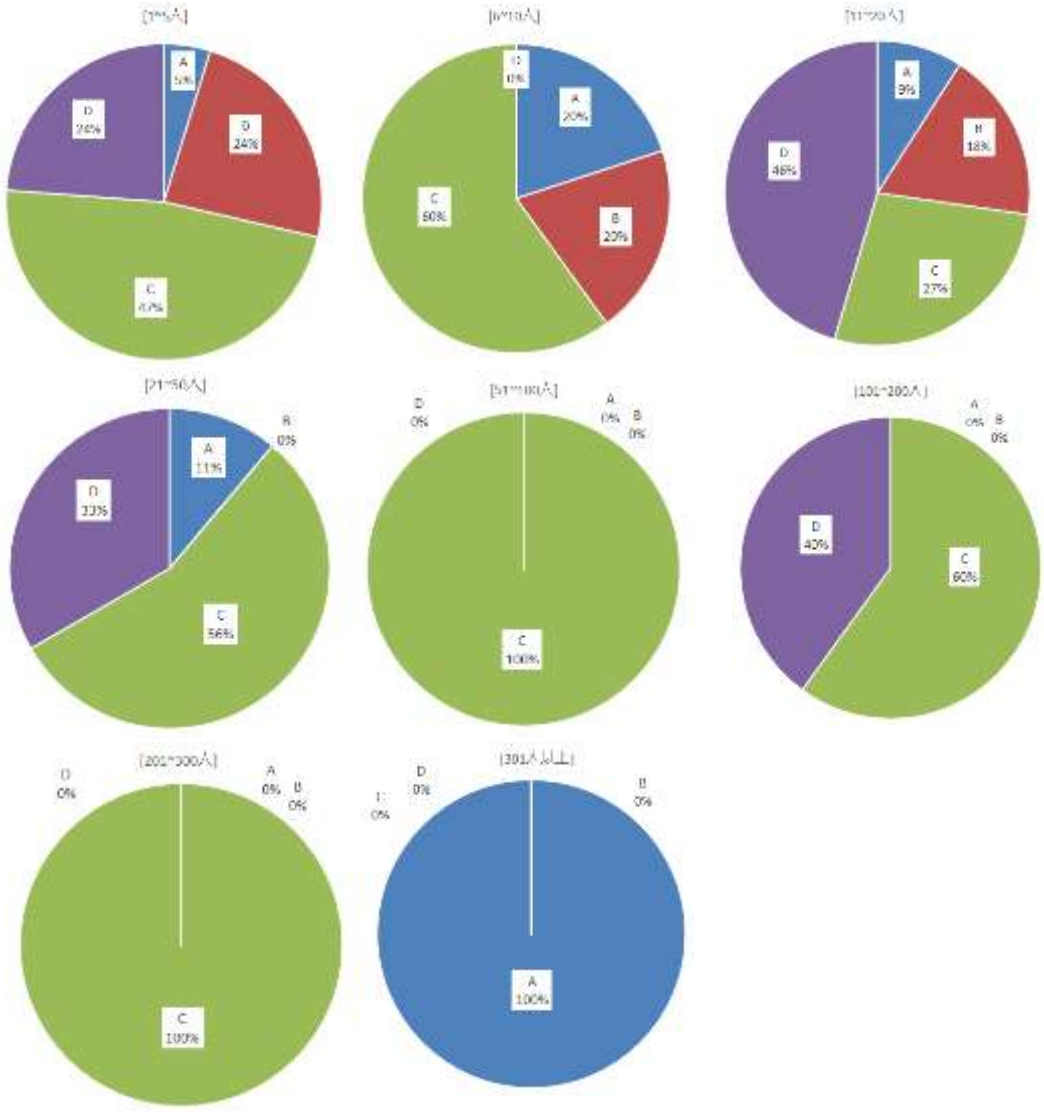


図 4-17　事業所規模別（総評）

4.2.2.5 診断結果集計（業種別）

(1) 業種内訳

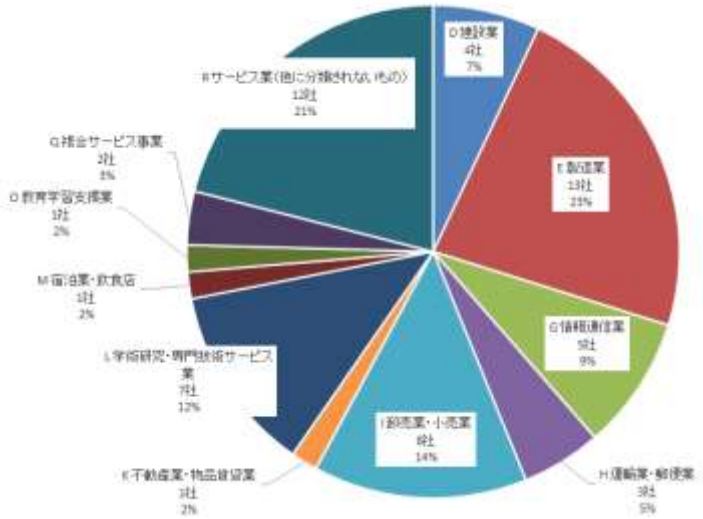
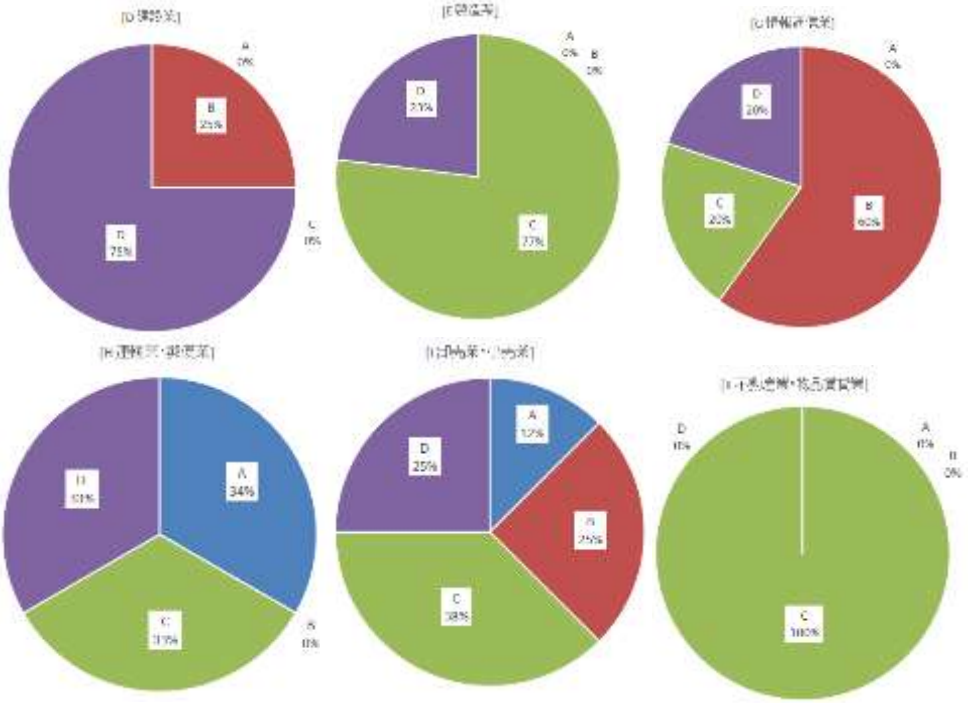


図 4-18　業種内訳

(2) 総評



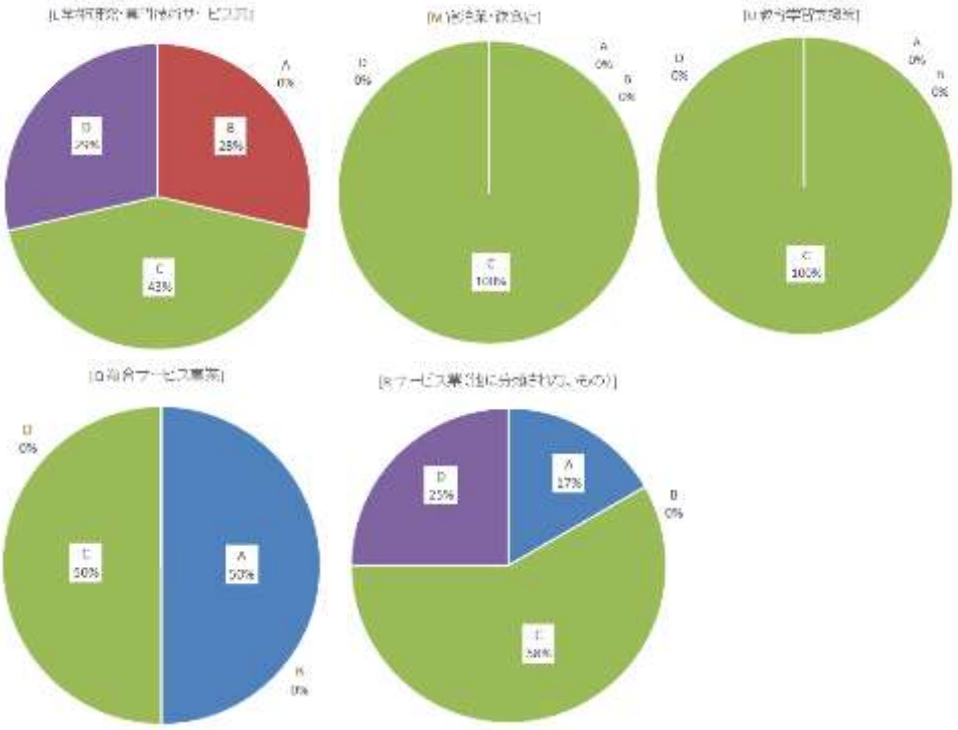


図 4-19 業種別（総評）

4.3 実証実施結果

4.3.1 UTM による防御・SOC による監視（「お守り」「見守り」「お知らせ」）結果

4.3.1.1 設置容易な UTM

- 令和元年度実証においては、NEC が中小企業でも設置および運用が容易にできる UTM を開発し、商用化サービス（主なユーザーは京阪神の中小企業）においても、設置の容易さは既にその真価を発揮しており、本サービスにおける有力なアピール点となっている。

- よって、UTM の設置の容易さは令和 2 年度実証においては主たる検証対象ではない。しかし、京阪神と滋賀・奈良・和歌山に地域差があるか否かを確認してみた。

- 令和 2 年度実証は実施期間が短いこと、また、令和元年度実証の実施結果から UTM 送付後すぐには設置せず長期間放置する実証参加企業も少なくないことが予め分かっていたため、UTM 送付後ほどなくして大阪商工会議所より各実証参加企業に直接連絡を取り、プッシュ型でお助け実働隊地域 IT 事業者による「訪問設置支援」を案内し、設置日時のアポイントを積極的に取得することとした。

- その結果、54 社（最終的にオンラインにならなかった 1 社含む。当該 1 社は「実証参加」

の定義を満たさないため、実証参加企業数からは除外）中 25 社（46%）に「訪問設置支援」を行った。即ち自社設置率は 54%である。

・ 上記対策を実施し、UTM 到着からアクティベーション（UTM 有効化）までに要した日数は以下となった。

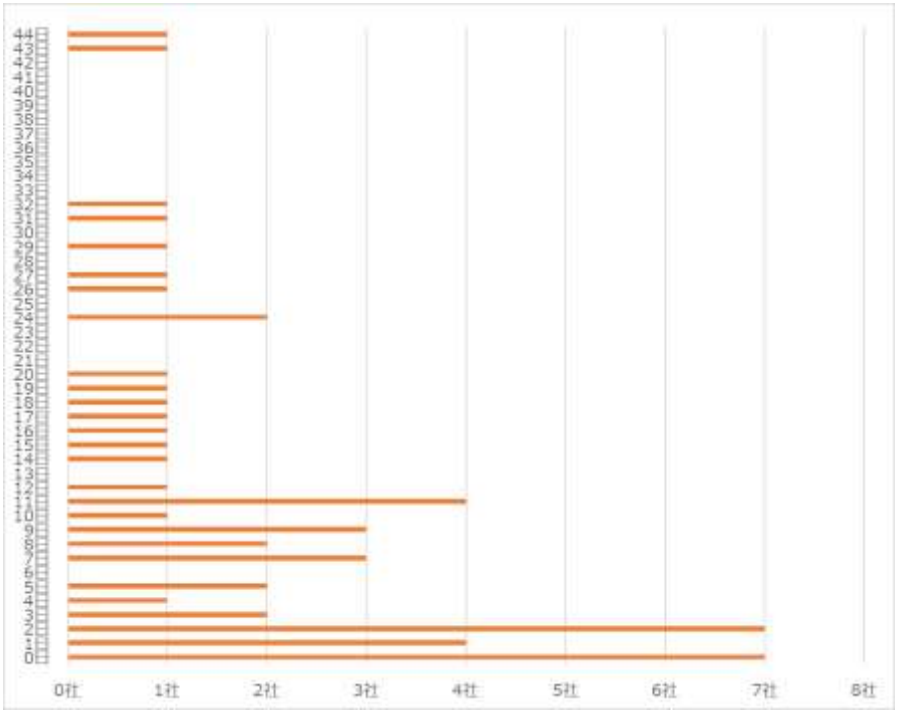


図 4-20　UTM 到着からアクティベーション（UTM 有効化）までに要した日数

・ 自社設置率 54%は、令和元年度実証（大阪・京都・兵庫）の自社設置率 69%（自社設置時間：「容易」回答集団で平均値 20 分、中央値 10 分、「困難」回答集団で平均値 77 分、中央値 60 分）と比較して 15%も低く、UTM が両実証で同じものである以上、上記経緯を勘案したとしても、少し開きが目立つ。

・ なお、下記はあるお助け実働隊地域 IT 事業者から示された所見であり、この種のコメントは令和元年度実証でも散見されたところである。

> 2 件訪問しましたが、ONU 直下か CTU 直下に UTM を接続しようとして、IP などのネットワーク設定ができずに NG となりルーター配下に設置しました。ONU 直下か CTU 直下は DHCP にて IP 設定を取得できない場合は、空いている IP を探して想定できる設定を実施しましたが、上手くいかず、もし、上手く接続できたとしても確実に将来にわたって機能するとは保証できないので、DHCP か IP を完全に把握して管理されている企業のみで設定できるように思います。DHCP で IP をつかめた多くのお客様は比較的簡単に UTM

設置できたと思います。つかめなかったお客様がお助け隊の出番となりますが、IP 設定などネットワーク設計を把握していないお客様が大半なので、各機器の説明書や契約書など関連書類も無い場合が多いので、お助け隊の仕事としては、ONU、CTU、ルーター、WiFi 設備、経路を全体に見て、設置可能ないくつかのポイントを有効順に見つけ出し、そのポイントに設置できる、できないを見極めることにありそうです。設置できるベストなポイントは物理的に考えるとルーターの前のよう思いますが、そのポイントだと、DHCP で構成できれば OK なのですが、不可の場合は、情報不足で手動設定は困難なケースが多いと思います。ただ、論理的にはルーターの後が UTM の意味合いを考えるとベストとは思います。ルーターにもファイアウオールやフィルタリング・簡易 UTM があるので、それをすり抜けてきたもののみを当 UTM で捕捉できるからです。そのような観点でアドバイス頂ければ有難いです。

4.3.1.2 UTM による観測結果

(1) 所在地別

所在地別の UTM 観測結果は以下のとおりである。

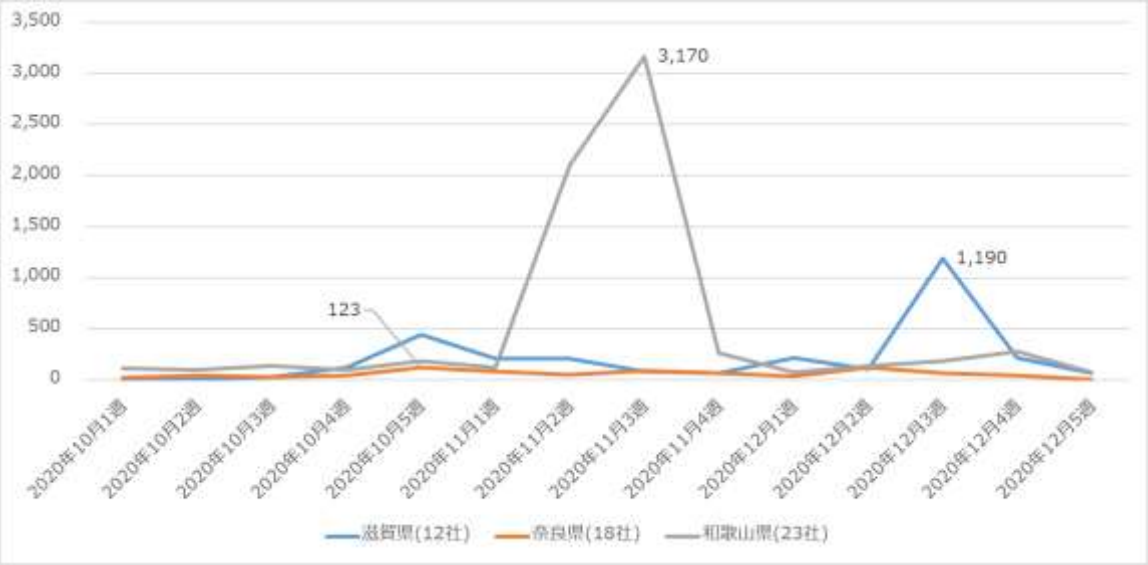


図 4-21　UTM 脅威検知数の推移（AV/IPS/WG）（所在地別）

図 4-22　UTM 脅威検知数の推移（AV）（所在地別）

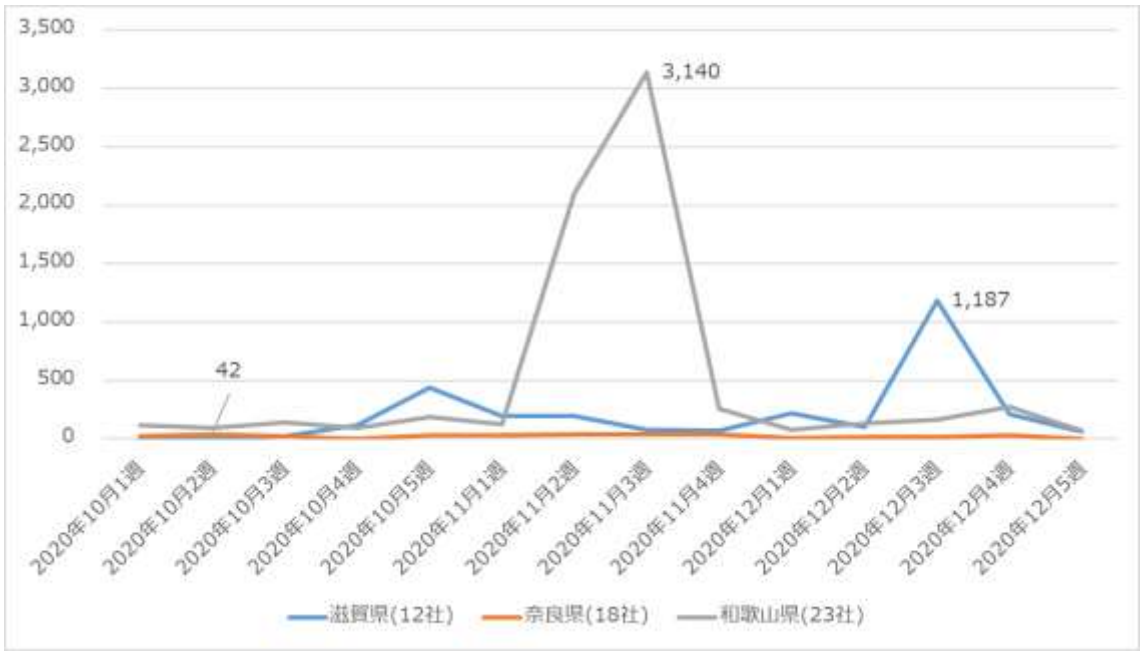


図 4-23　UTM 脅威検知数の推移（IPS）（所在地別）

図 4-24　UTM 脅威検知数の推移（WG）（所在地別）

(2) 企業別

企業別の UTM 観測結果は以下のとおりである。

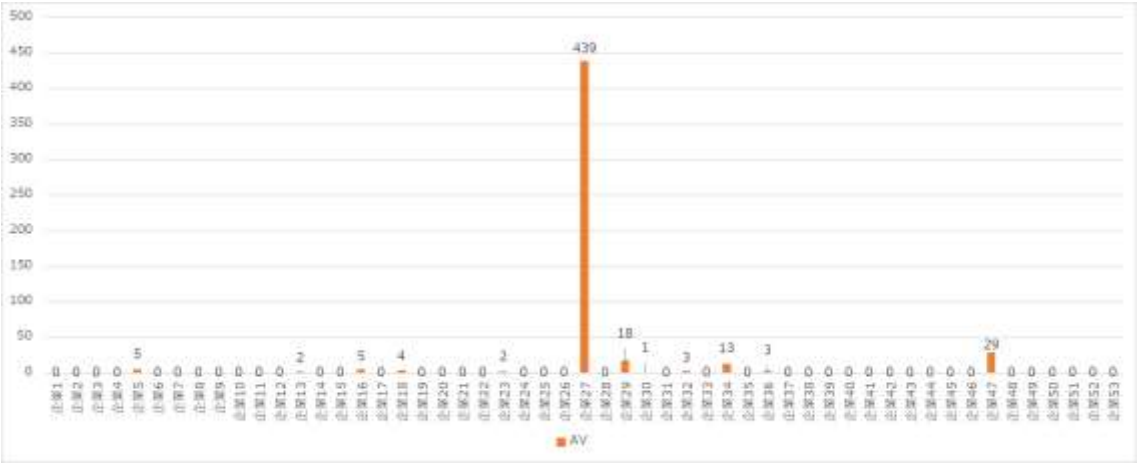


図 4-25　UTM 脅威検知数（AV）（企業別）

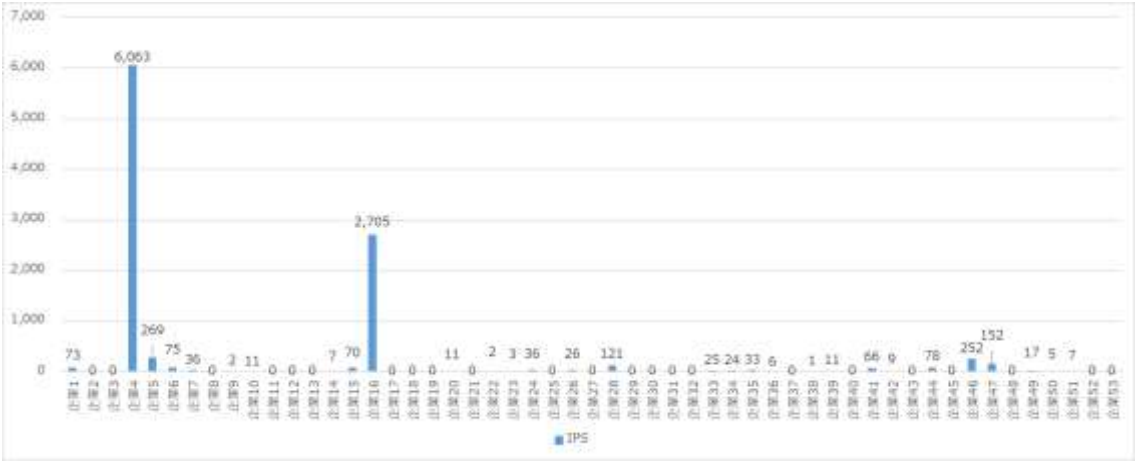


図 4-26　UTM 脅威検知数（IPS）（企業別）

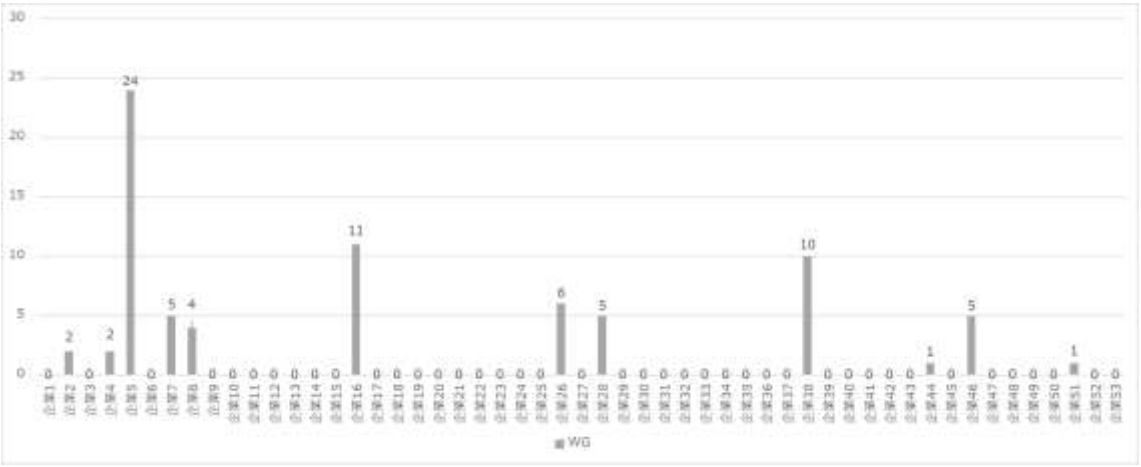


図 4-27　UTM 脅威検知数（WG）（企業別）

(3) 事業所規模別

事業所規模別の UTM 観測結果は以下のとおりである。

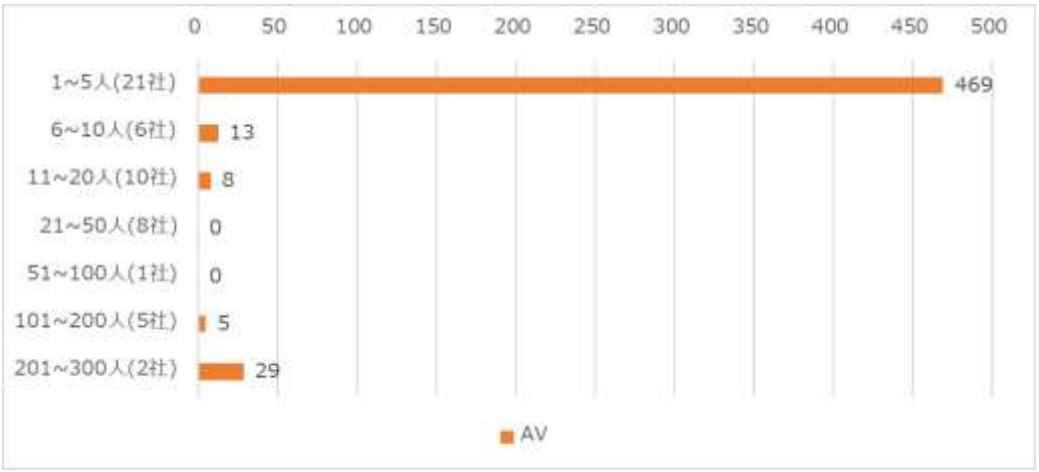


図 4-28　UTM 脅威検知数（AV）（事業所規模別）

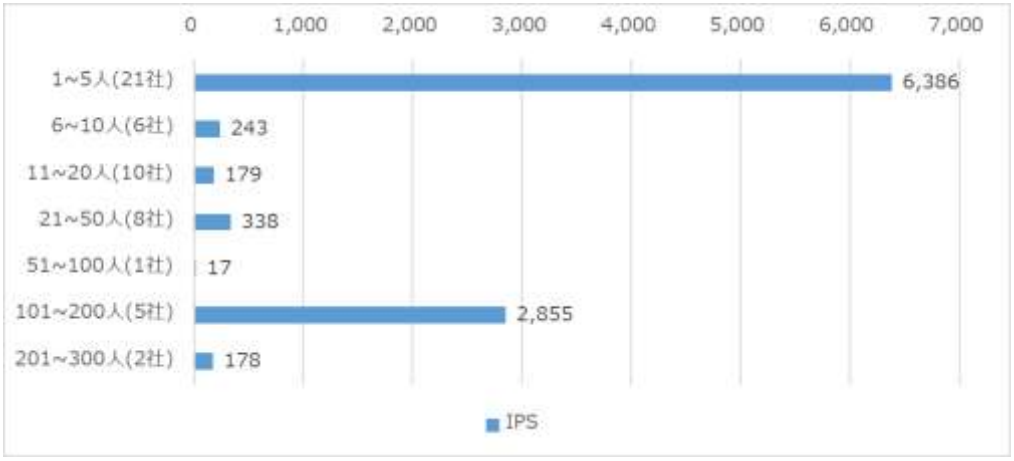


図 4-29　UTM 脅威検知数（IPS）（事業所規模別）

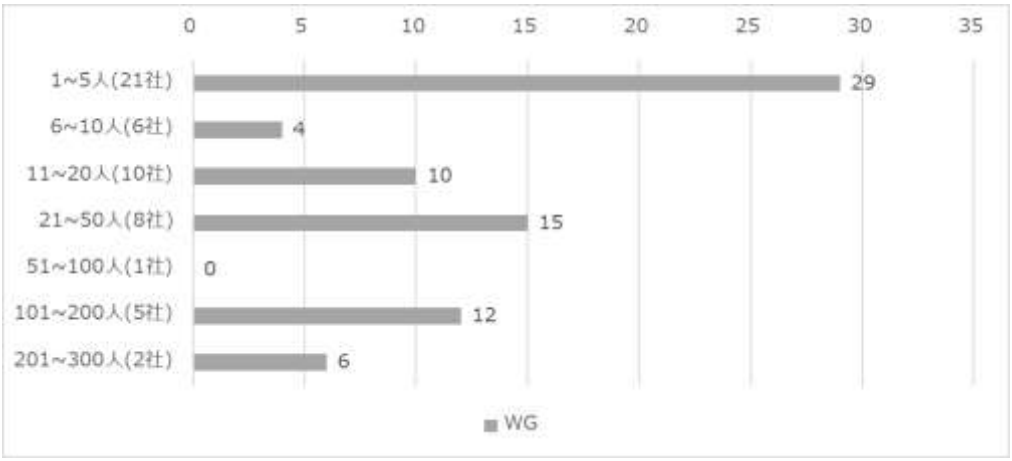


図 4-30　UTM 脅威検知数（WG）（事業所規模別）

(4) 業種単位

業種別の UTM 観測結果は以下のとおりである。

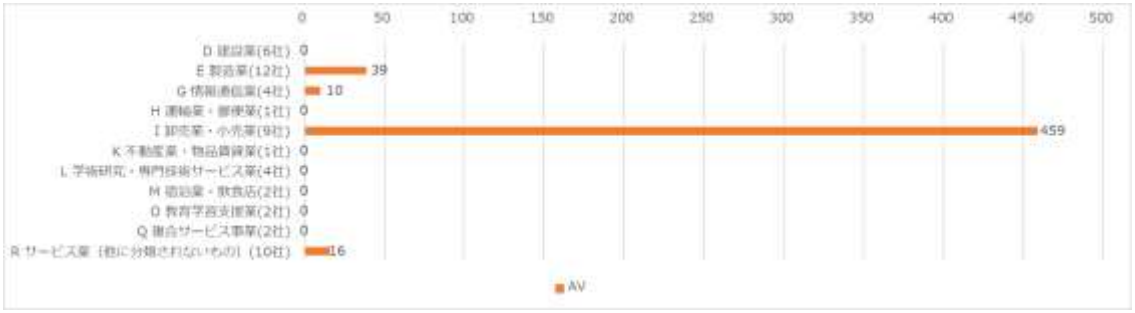


図 4-31　UTM 脅威検知数（AV）（業種別）

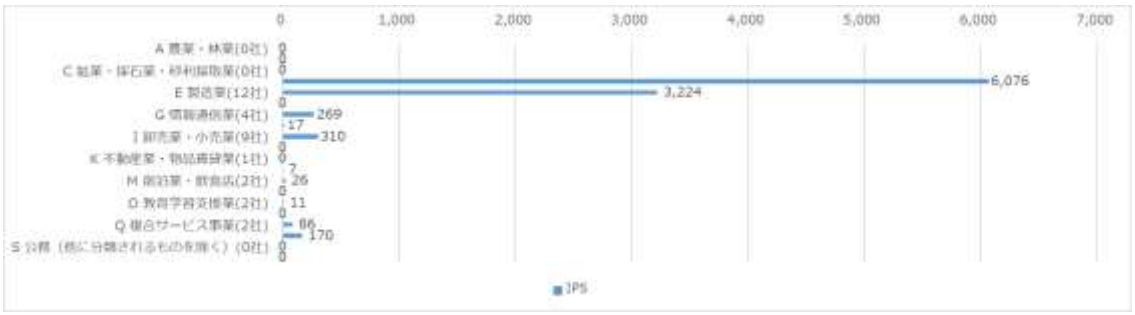


図 4-32　UTM 脅威検知数（IPS）（業種別）

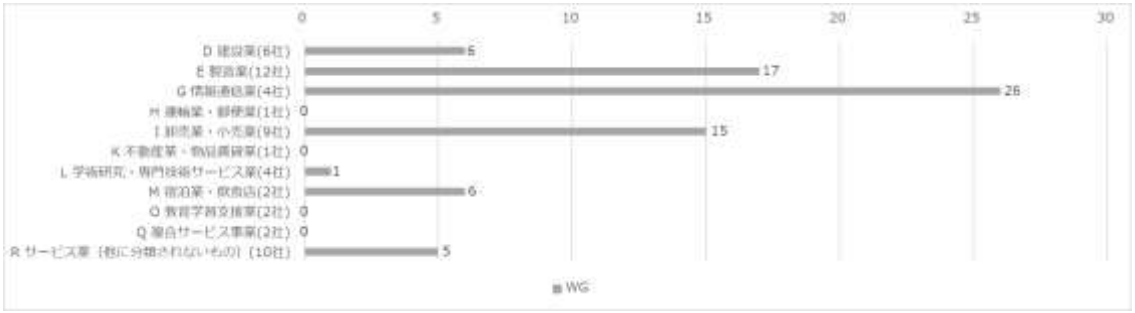


図 4-33　UTM 脅威検知数（WG）（業種別）

(5) UTM 機能別

UTM 機能別の UTM 観測結果は以下のとおりである。

表 4-21　UTM 機能別 重要度検知数

機能	件数（件）	重要度（件）			
		★★★（高）アラートメール発報	☆★★（中）アラートメール発報	☆☆★（低）アラートメール発報	重要度なし（*1）
AV	524	0	0	524	0
IPS	10,196	0	70	677	9,449
WG	76	0	76	0	0
合計	10,796	0	146	1,201	9,449

*1：即時遮断しユーザー影響が無い脅威はユーザー通知対象外（アラートメール不発報）

機能ごとの通信方向を分類した監視結果は以下のとおりである。

表 4-22　UTM 機能の通信方向別検知数

検知した通信	機能	件数	社数
外部からの攻撃	IPS	7,906	22
	AV	524	12
外部への不正通信	IPS	2,091	15
	AV	0	0
	WG	76	12
内部の脆弱性	IPS	199	3
合計		10,796	—

・ 表 3-22 につき、「外部からの攻撃」を UTM が防いだことで、重複を除き 30 社を防御した（「被害の攻撃化」を阻止）。また「外部への不正通信」「内部の脆弱性」を防いだことで、重複を除き 23 社を防御した（「被害の実害化」を阻止）。53 社の実証参加企業のうち 71%に相当する 38 社（重複を除く）を防御し得たことは令和 2 年度実証の最大の直接的成果と言える。（令和元年度実証は 110 社中 67%に相当する 74 社を防御）

機能ごとに検知された脅威トップ 10 は以下のとおりである。トップ 10 より順位が低い脅威については、検知数が少ないため、記載は省略する。

表 4-23　UTM の AV 機能による脅威検知数トップ 10

	脅威	件数（件）	割合（%）
1	Trojan.Multi.Generic.4	196	37.4
2	Hacktool.MSOffice.Generic.3	93	17.7
3	Trojan.Script.Generic.a	57	10.9
4	Trojan.MSIL.Agensla.i	24	4.6
5	Trojan.Win32.Generic.4	20	3.8
6	Trojan.MSIL.Injects.4	18	3.4
7	Trojan.Win32.Malicious.4	18	3.4
8	Trojan.Script.Generic.4	15	2.9
9	Trojan.MSOffice.Alien.4	13	2.5
10	Trojan.MSOffice.SAgent.4	12	2.3

表 4-24　UTM の IPS 機能による脅威検知数トップ 10

	脅威	件数（件）	割合（%）
1	Cross Site Script attack	1,964	19.3
2	JSIG-WEB SQL-Union-ALL-Select-1	1,697	16.6
3	JSIG-WEB:SQL-Union-ALL-Select-3	1,662	16.3
4	Possible SQLMAP SCAN -2	1,571	15.4
5	Brute Force attack	457	4.5
6	JSIG-WEB:Netgear-SetuPCGI-Cmd-Exec	447	4.4
7	RealNetworks Helix RTSP two simultaneous long get request buffer overflow	275	2.7
8	HTTP Basic Auth Null Password Login attempt	241	2.4
9	HTTP Basic Auth Default Password Login attempt (admin) -2	179	1.8
10	PHPCGI Remote File Include attempt	163	1.6

表 4-25　UTM の WG 機能による脅威検知数トップ 10

脅威		件数（件）	割合（%）
1	infopicked.com	26	34.2
2	images2.imgbox.com	19	25.0
3	eu.dspultra.com/api/submit_form_request	15	19.7
4	poPCash.net	5	6.6
5	p238000.infopicked.com/adServe/domainClick	3	3.9
6	apps.identrust.com/roots/dstrootcax3.p7c	2	2.6
7	beta.infopicked.com/aS/feedclick	2	2.6
8	infopicked.com/aS/feedclick	2	2.6
9	poPCash.net/world/go/134600/426377	1	1.3
10	usd.mnason-hec.com/zcvisitor/81cdf7c5-210e-11eb-82b2-12fb7b68362b/e6eb32c0-57f0-11e6-9404-0aaf54648f79	1	1.3

4.3.2 相談窓口の運用結果

(1) 相談窓口の概要

① 役割・機能

・ 実証参加企業での UTM 設置やインシデント発生時の支援として相談窓口を設置した。状況が不明瞭な実証参加企業の話を聞くことで、不安を受け止める役割を果たしている。インシデント発生時には状況を把握し、対象 PC のネットワークからの切り離しやウイルスのスキャンなど初動対応を案内。被害拡大防止の役割を担っている。

② 運用手法

・ 専用フリーダイヤルにて、土日祝日を除く 9：00～18：00 の時間帯を受付時間とした。コールセンターは専用席を用意、1 名を専任の担当者として電話・メールによる受付を行い、リモートサポートも含め、実証参加企業に寄り添ったサポートを提供した。

(2) 相談窓口での対応状況

① 電話・メールによる相談の内容・傾向・件数【事例紹介を含む】

表 4-26　各月の電話問合せ推移

項目	9 月	10 月	11 月	12 月	累計
入電件数	3 件	23 件	32 件	6 件	64 件
応答件数	3 件	22 件	30 件	5 件	60 件
応答率	100%	95.7%	93.8%	83.3%	93.2%

表 4-27　各月のメール問合せ推移

項目	9 月	10 月	11 月	12 月	累計
メール問合せ数	0 件	4 件	5 件	1 件	10 件

表 4-28　問合せ内容毎の解決方法（累計）

解決方法 / お問い合せ内容	電話	メール（※1）	窓口リモート	駆け付け案内	累計
UTM 関連	22 件（81%）	0 件（0%）	1 件（4%）	4 件（15%）	27 件
ポータルサイト関連	8 件（100%）	0 件（0%）	0 件（0%）	0 件（0%）	8 件
アラート関連	4 件（100%）	0 件（0%）	0 件（0%）	0 件（0%）	4 件
セキュリティ関連	1 件（100%）	0 件（0%）	0 件（0%）	0 件（0%）	1 件
その他	12 件（100%）	0 件（0%）	0 件（0%）	0 件（0%）	12 件

※1：表 3-27「各月のメール問合せ」に記したメール問合せ件数（10 件）と表 3-28「問合せ内容毎の解決方法（累計）」のメールの欄に記した件数（0 件）が一致しない理由は、問合せはメールにて受け付けたが、スピーディーかつ着実な課題解決を目指し、解決は電話や窓口リモートにて行ったためである。

・ 問合せの 8 割が電話による相談、残り 2 割がメールによる相談となっている。電話による相談が過半数とはなるが、営業時間内に問合せすることが難しい企業や電話ではなくメールによるやり取りを希望される企業があり、結果としてメールでの問合せも一定の割合を占めた。

・ 問合せ内容は UTM 設置時の問合せが最も多く、実証参加企業のうち約 20%から問合せを受けている。内容としては「配線位置が分からない」「配線したがアクティベーションができない」「UTM ID の登録ができない」などとなっている。またポータルサイト関連についても設置時と同タイミングでの入電が多く、「ポータルへのログイン方法が分からない」「ポータルのログイン情報を忘れた」などが主なものである。一方、UTM 設置後は、問合せ数が減少していき、問合せ内容もアラート関連やセキュリティ関連へ変化している。

・ 実証参加企業自身で UTM の設置が完了しないケースとして、ほとんどが配線位置を誤っており、PPPoE セッション（プロバイダ情報）が設定された機器（ルーターなど）よりも手前に UTM を接続しているため、UTM の通信がインターネット上に接続できない状態となっていた。特に、無線機能内蔵ルーター設置においては、PPPoE セッション（プロバイダ情報）設定の有無を把握されておらず、UTM 直下に無線ルーターを設置し、アクティベーションが完了しないケースがあった。

・ 相談窓口にて、実証参加企業担当者と配線の確認や取り付け依頼を行うものの、「自社のネットワーク環境を把握していない」「ネットワーク環境が複雑で確認が難しい」との申告から配線の案内に時間がかかるケースや担当者のリテラシーが不足し「電話案内

にて作業を行えるか不安」との理由で、最初から駆け付け設置を希望されるケースもあった。

・ UTM 設置後のトラブルとして周辺機器や共有フォルダのアクセス不具合が発生するケースがあったが、UTM 起因によるものではなく、設置前から発生していた不具合が原因による症状であった。実証参加企業側では不具合が UTM 起因によるものかの判断が難しく、相談窓口を活用した設置サポートの重要性を再認識した。

・ 今回の実証を通じて設置マニュアルをより分かりやすい表記にすることや、ユーザー環境パターンによる設置事例などを追加することのような工夫が必要であることが分かる。また、アラート発生時に迅速に対応できるよう、実証参加企業においても定期的なアラートチェックを含めてセキュリティに関する意識向上が必要であると感じる。

② 各関係者の連携

相談窓口では問合せを受けた際に、登録・設置に関する内容かトラブルかを判断し、各関係者と以下のように連携を行った。

・ **ポータルサイト登録、UTM 設置に関する対応**
  - 電話またはリモートで対応し、解決に至らないケースは駆け付け提案を行い、実証参加企業が希望する場合はお助け実働隊地域 IT 事業者に環境情報などの情報共有を行った。

・ **UTM 設置後のトラブルやインシデント対応**
  - 電話またはリモートで対応し、解決に至らないケースは NEC にエスカレーションを行い、対応方針を仰ぎ、それをもとに実証参加企業への回答を行った。駆け付け対応の場合は、お助け実働隊地域 IT 事業者に情報共有を行っている。

・ **イレギュラー対応が発生した場合**
  - この場合は再販事業者である大阪商工会議所へ対応依頼行い、その上で実証参加企業へ回答を行った。

(3) 実証相談窓口に対する参加企業の評価

表 4-29　実証相談窓口に対する参加企業の評価

<table>
<tr><th colspan="5">相談窓口の対応は良かったか</th></tr>
<tr><td rowspan="4">とても良かった</td><td>先方の指示･助言･用語が的確･理解しやすかった</td><td>8</td><td rowspan="4">17
(57%)</td><td rowspan="7">23
(77%)</td></tr>
<tr><td>当方の状況･要望を把握･理解してもらえた</td><td>4</td></tr>
<tr><td>解決までの時間が短かった</td><td>2</td></tr>
<tr><td>その他</td><td>3</td></tr>
<tr><td rowspan="3">良かった</td><td>先方の指示･助言･用語が的確･理解しやすかった</td><td>2</td><td rowspan="3">6
(20%)</td></tr>
<tr><td>当方の状況･要望を把握･理解してもらえた</td><td>2</td></tr>
<tr><td>解決までの時間が短かった</td><td>1</td></tr>
</table>

	その他	1		
普通		7	7 (23%)	7 (23%)
悪かった	(略)	0	0%	0%
とても 悪かった	(略)	0	0%	

4.3.3 テレワークツールの利用実績・効果測定の結果

4.3.3.1 テレワークツール利用実績

テレワークツールの申込実績、利用実績は以下のとおりである。

表 4-30　テレワークツール申込み、利用実績

テレワークツール申込企業数	テレワークツール利用企業数
28 社（実証申み企業中：約 50%）	5 社（テレワークツール申込企業中：約 17%）

4.3.3.2 セキュリティ脅威の実態把握結果集計

アンケートにてテレワークの実施有無、重要情報に対するセキュリティポリシー、テレワーク環境の確認を行った。なお、アンケート結果の単位は社数である。

(1) テレワーク実施有無

テレワーク実施有無について、実証参加企業のうち、37 社からアンケートの回答があった。アンケート結果は以下のとおりである。

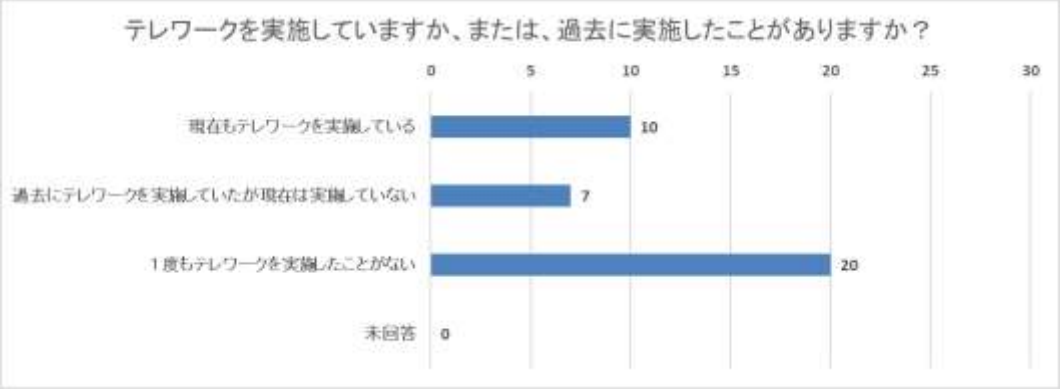


図 4-34　テレワーク実施有無

(2) 重要情報に対するセキュリティポリシー

重要情報に対するセキュリティポリシーについて、実証参加企業のうち、37 社からアンケートの回答があった。アンケート結果は以下のとおりである。

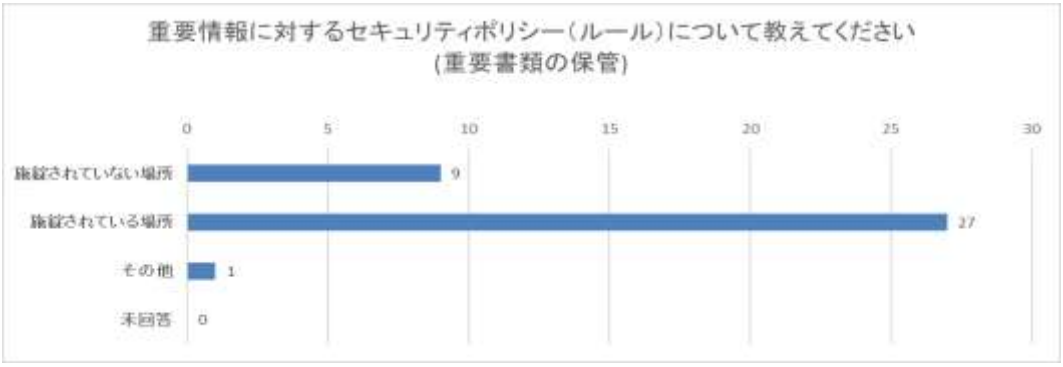
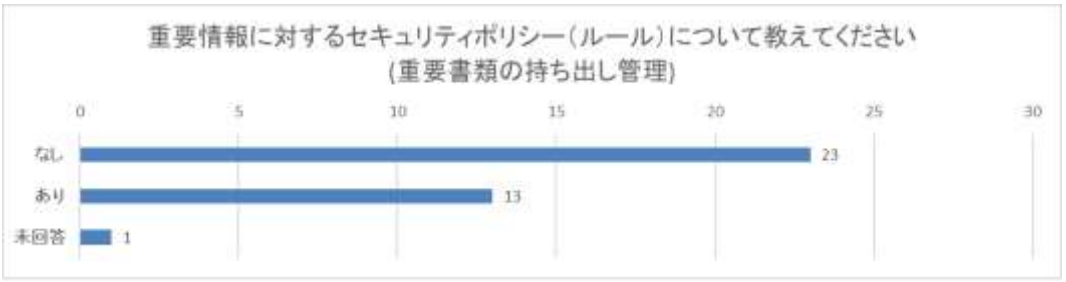


図 4-35　重要書類の保管



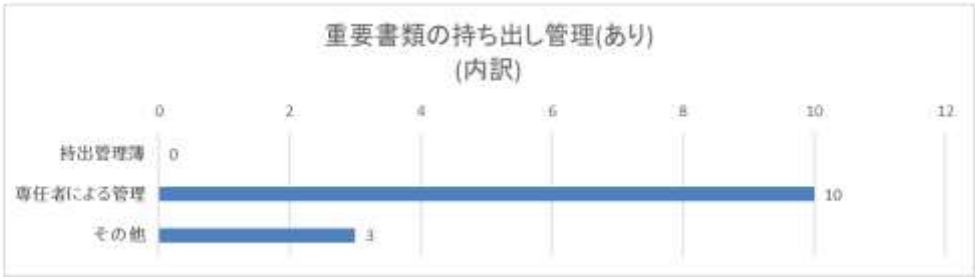


図 4-36　重要書類の持ち出し管理

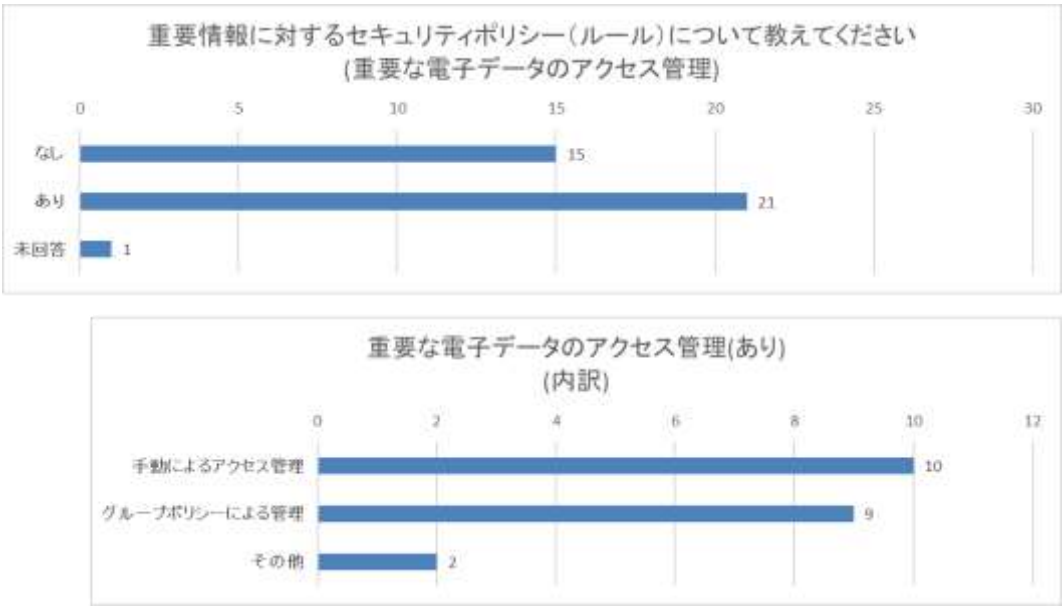


図 4-37　重要な電子データの持ち出し管理

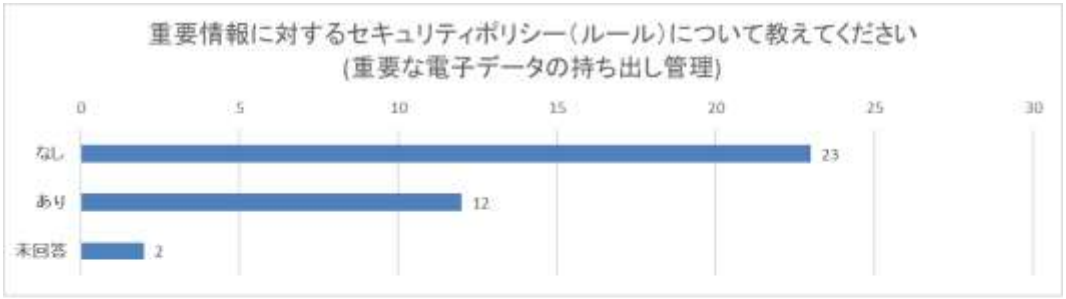


図 4-38　重要な電子データの持ち出し管理

(3) テレワーク環境

実証参加企業のうち、一度でもテレワークを実施したことがあると回答した 17 社にテレワーク環境についてのアンケートを実施した。アンケート結果は以下のとおりである。

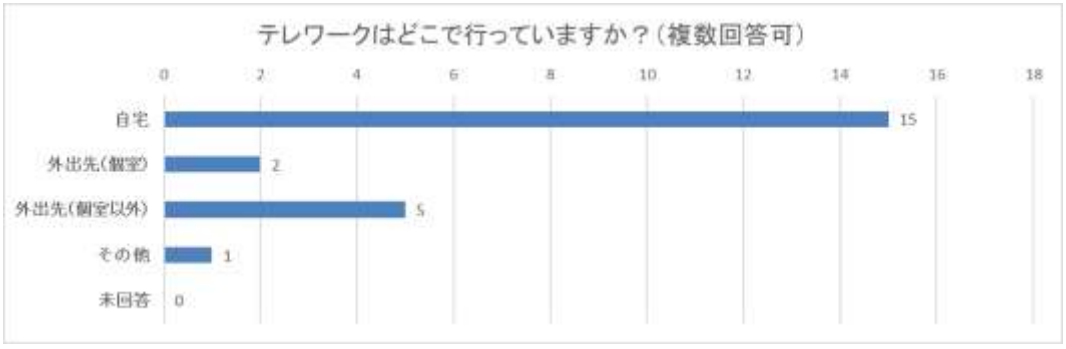


図 4-39　テレワーク時の実施場所

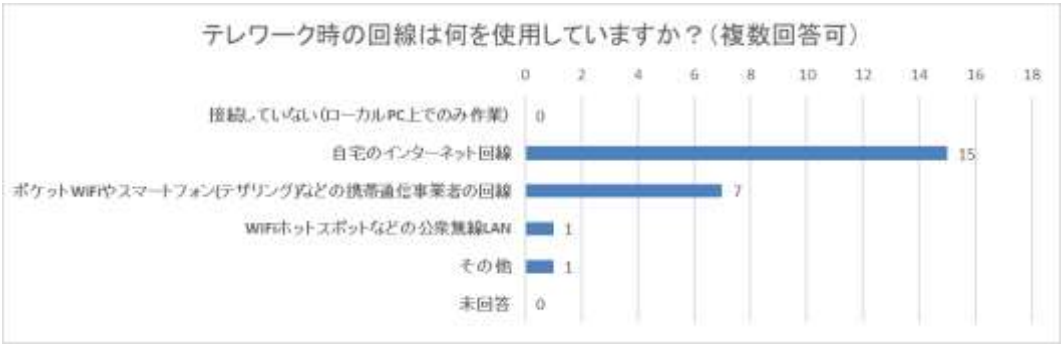


図 4-40　テレワーク時の使用回線

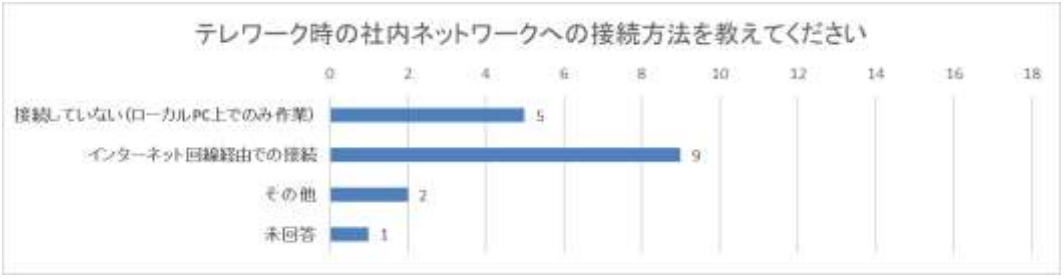


図 4-41　テレワーク時の社内ネットワークへの接続方法

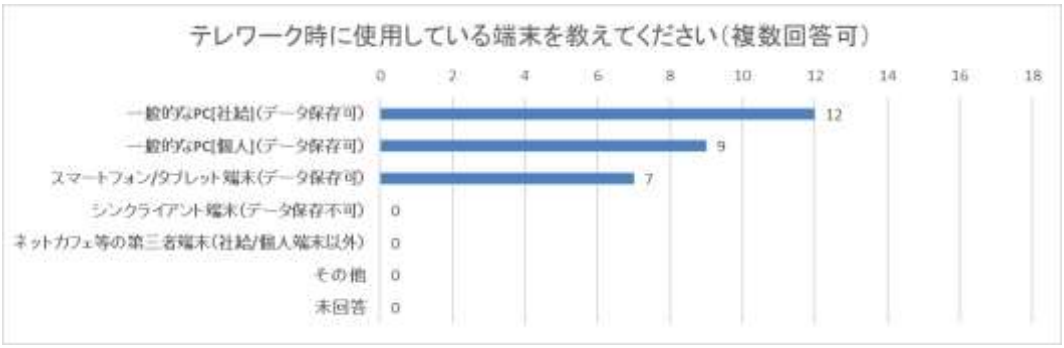


図 4-42　テレワーク時の使用端末

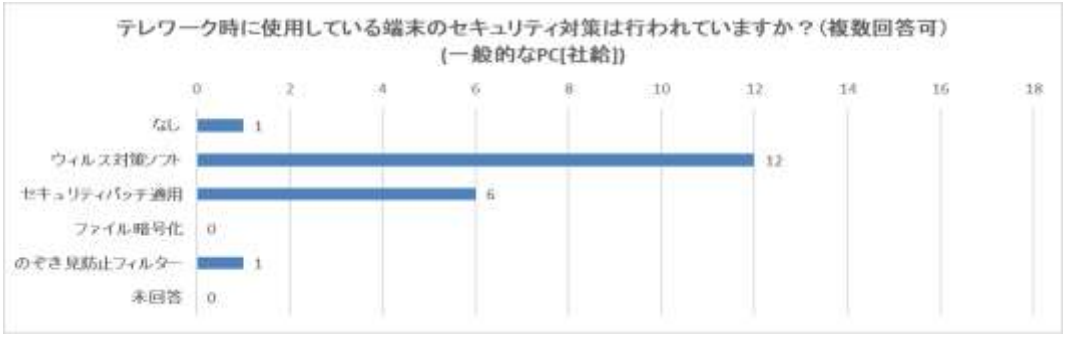


図 4-43　テレワーク時に使用している端末のセキュリティ対策（一般的な PC[社給]）

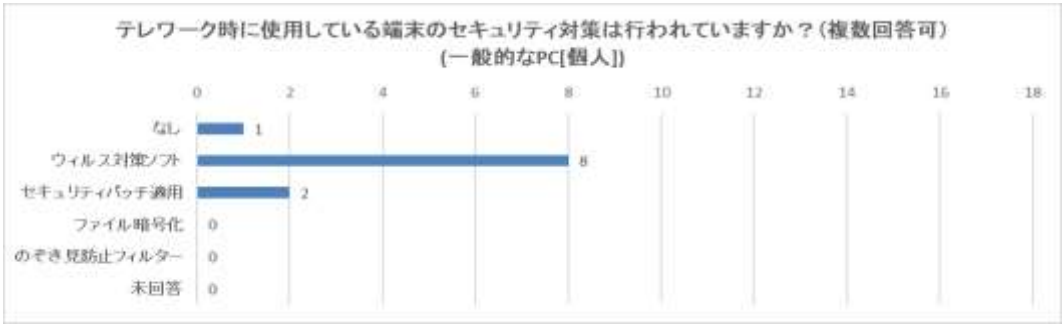


図 4-44　テレワーク時に使用している端末のセキュリティ対策（一般的な PC[個人]）

図 4-45　テレワーク時に使用している端末のセキュリティ（スマートフォン/タブレット端末）

4.3.3.3 テレワークツール利用前後の重要情報持ち出し比較

アンケートにてテレワークに係るツール利用前後の重要情報持ち出しについて確認を行った。また、テレワークツール利用企業にテレワークツールの評価、テレワークツール未使用企業に理由の確認を行った。なお、アンケート結果の単位は社数である。

(1) テレワークツール利用前後比較事例

実証期間中にテレワークツールを使用した企業 5 社のテレワークツールアンケートの前後比較事例は以下のとおりである。

表 4-31　テレワークツール利用前後比較事例

	アンケート項目	利用前	利用後
A 社	持ち出し回数	5回以下	0回
B 社	持ち出し回数	テレワーク未実施	0回
C 社	持ち出し回数	アンケート未回答	0回
D 社	持ち出し回数	5回以下	5回以下
	持ち出し方法	紙、メール、その他(one drive)	メール、その他(one drive)
	持ち出し理由	その他(急ぎの作業やメール対応のため)	在宅勤務のため テレワークツール利用より容易だから
E 社	持ち出し回数	5回以下	5回以下
	持ち出し方法	USBメモリ/HDD	USBメモリ/HDD
	持ち出し理由	外出先で作業が必要なため	外出先で作業が必要なため テレワークツールでは複数名で画面の共有ができないから

(2) テレワークツールへの評価

実証期間中にテレワークツールを使用した企業 5 社にテレワークツールの評価についてアンケートを行った。アンケート結果は以下のとおりである。

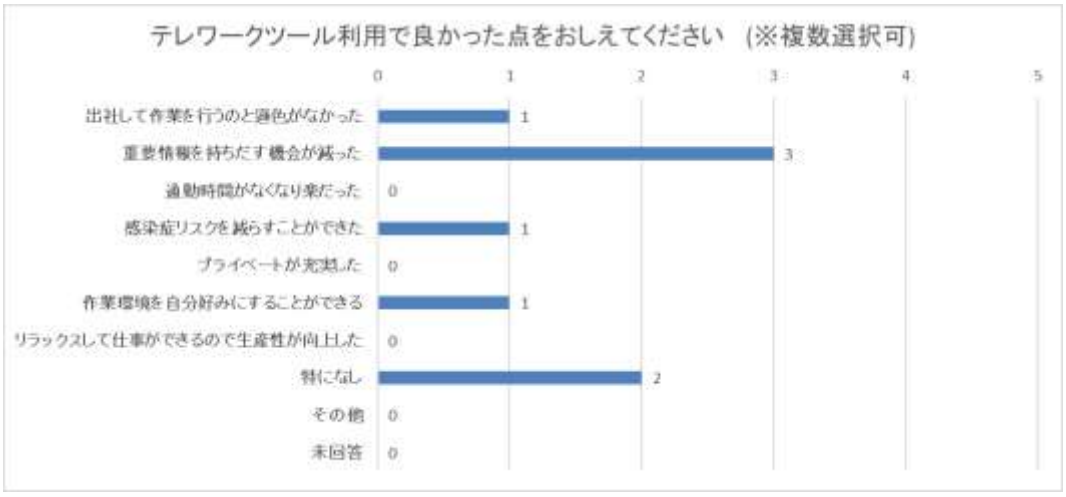


図 4-46　テレワークツール利用で良かった点

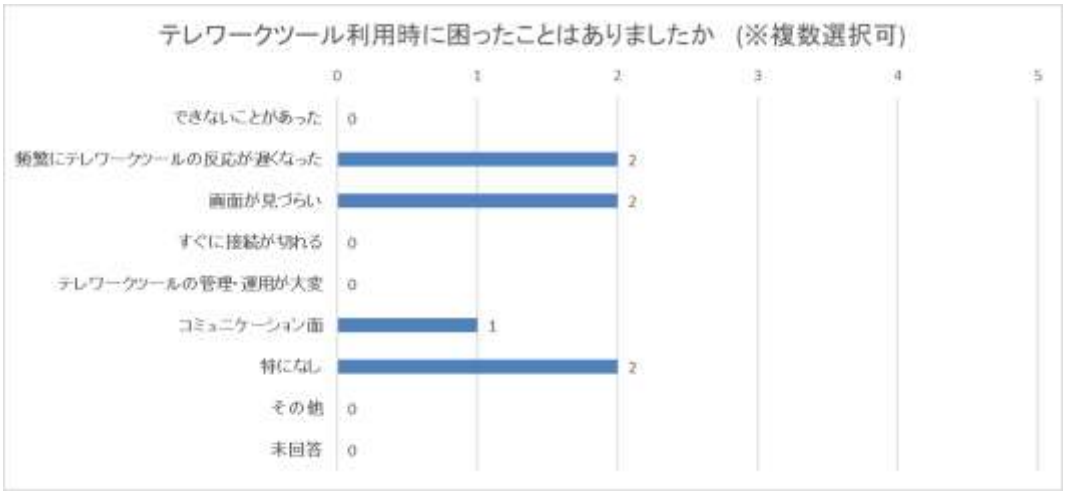


図 4-47　テレワークツール利用時に困ったこと

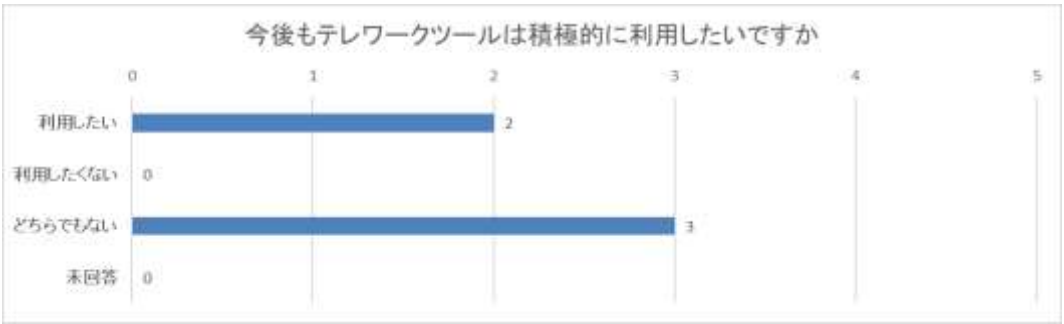


図 4-48　今後もテレワークツールを積極的に利用したいか

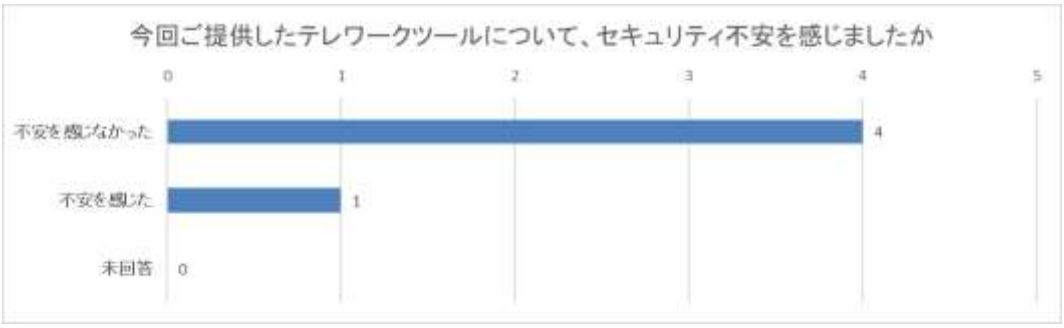


図 4-49　テレワークツールにセキュリティ不安を感じたか（利用企業）

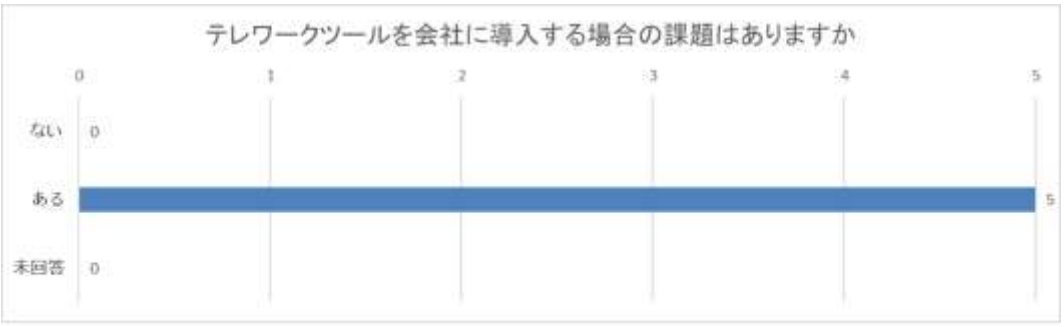


図 4-50　テレワークツールを会社に導入する場合の課題

(3) テレワークツール未使用企業へのアンケート

実証期間中に行ったリモートワークツールの利用状況ヒアリングでも、テレワークツールの利用率が低いことが判明していた。そのためテレワークツールを利用しない企業に向けたアンケートを追加で行い、17 社から回答があった。

図 4-51　テレワーク実証に申し込んだ理由

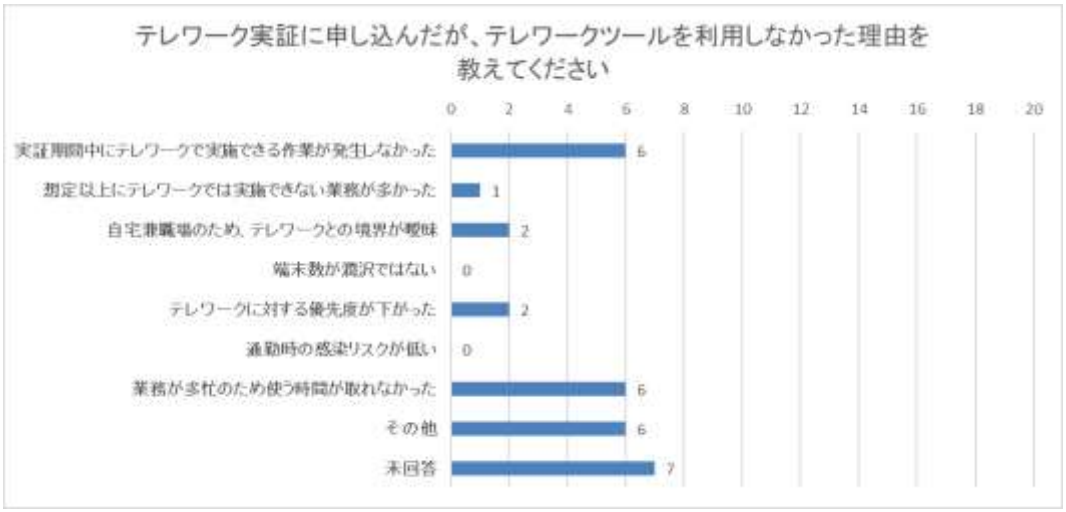


図 4-52　テレワークツールを利用しなかった理由

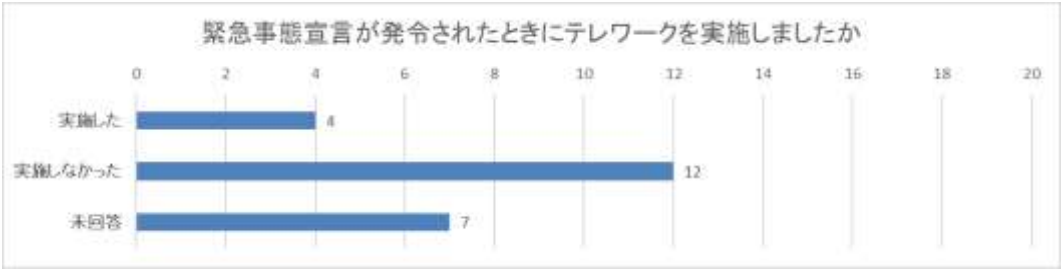


図 4-53　2020 年 4 月の緊急事態宣言発令時のテレワーク実施有無

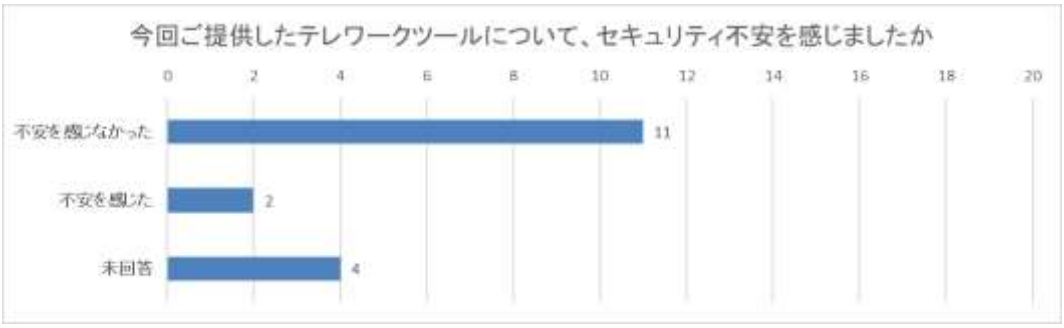


図 4-54　テレワークツールにセキュリティ不安を感じたか（未使用企業）

(4) with コロナ時代に対応するためのテレワークの必要性

実証終了後、with コロナ時代に対応するためのテレワークの必要性について実証参加企業 53 社へアンケートを行った。アンケート結果は以下のとおりである。

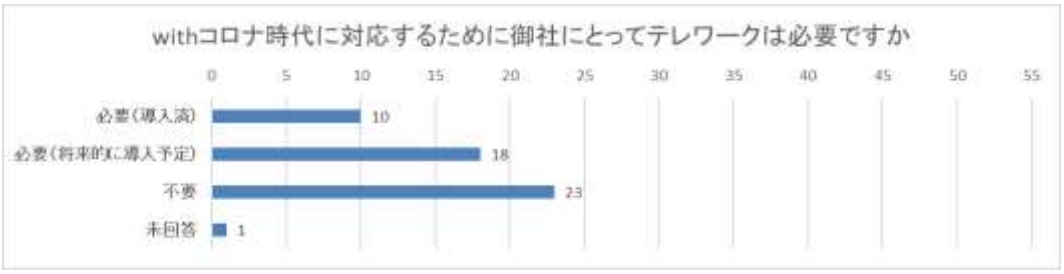


図 4-55　with コロナ時代に対応するためにテレワークは必要か

4.3.4 所定サイバーインシデント初動対処（「駆け付け」「リモートお助け」）結果

(1) 所定サイバーインシデント初動対処実施事例

・ 令和 2 年度実証は期間も短かったため、所定サイバーインシデント対応は 2 件しか発生しなかった。しかも、うち 1 件は実証参加企業が駆け付けお助けを希望したため、リモートお助けは 1 件しか発生しなかった。

表 4-32　所定サイバーインシデント初動対処　実施事例

	A社	B社
UTM 検知機能	IPS	Web ガード
アラート概要	マルウエアへの感染の疑いがある通信を UTM で検知	本サービスにおいて有害サイトとして登録されたサイトにアクセスしており、Web ガードで遮断
アラート日時	10 月 1 日【UTM 設置 5 日後】	11 月 26 日【UTM 設置 28 日後】
初動対処日時	10 月 2 日【1 日後に駆け付け】	12 月 3 日【7 日後に駆け付け】

初動対処手法	リモートお助け	駆け付けお助け
対処概要	・UTM が検知した「脅威検出通知（IPS）」をきっかけとして相談を受け、駆け付けを実施。 ・フルスキャンを実施。終了まで数時間を要するため、対応は翌営業日に持ち越しで合意。 ・フルスキャンの結果、複数の脅威を確認。 ・本脅威の駆除処理は問題なく完了。（詳細別記）	・UTM が検知した「脅威検出通知（Web ガード）」を個別調査し、駆け付けを実施。 ・お助け実働隊からリモートお助けを提案したが、実証参加企業の要望によりリモートお助けを実施せずに訪問お助けを実施 ・社内には検知した端末の MAC アドレスと合致する PC が見つからず、タブレットが被疑端末であることを特定。 ・該当タブレットにウイルス対策ソフトがインストールされていないためインストールを実施。 ・ウイルススキャンを実施したがウイルスは検出されず、タブレット内のアプリもしくはソフトウエアがバックグラウンドにてアクセスしたものと推定し、経過観察を促しクローズ。
対処結果	ウイルスを検知し、駆除	ウイルス検出なし
検出マルウエアなど	・脅威（高）の Hacktool：3 件 ・脅威（重大）の Trojan：3 件	―
初動対処時間	移動時間：リモートのためなし 作業時間：235 分	移動時間：往路 60 分 作業時間：120 分

⑵ 「リモートお助け」によるインシデント対応の実施事例

表 4-33　リモートお助け事例

	実証参加企業 甲社による実施内容	お助け実働隊地域 IT 事業者 による実施内容
10/1　（木）	アラートメール受信 【Trojan　Agent outbound connection-2】	
10/2　（金） 16:00	初動対処要請電話	
10/2（金） 17:00-17:30		電話でウイルス定義ファイル最新化方法を説明
	ウイルス定義ファイル最新化	

	実証参加企業 甲社による実施内容	お助け実働隊地域 IT 事業者 による実施内容
		電話でフルスキャンの設定と実施方法および駆除方法を説明
10/2（金） 17:30-18:30	LAN 線を抜きフルスキャン	
		フルスキャン実施中の画面コピーの採取方法を説明
	フルスキャン実施中の画面コピーをメール送信	
		フルスキャン実施中の画面コピーを受領し方向性の確認
	終了まで数時間要するため対応は翌営業日に持ち越しで合意	
10/5（月） 10:00-11:00	フルスキャン後「脅威が見つかりました」の画面コピー採取。「操作の開始」ボタン押下 【Hacktool および Trojan 計 6 件のマルウエアを駆除】	
10/5（月） 15:00-16:00	電話にて駆除処理が完了していることの連絡を受け状況確認。メールにて画面コピーの採取・送付依頼	
	電話にて該当 PC の再起動支援	
10/6（火） 14:00-15:00		「見守りサービスポータル」にて 2020/10/5（月） 14:54:30 以降は本マルウエアに関するアラートが止まっていることを確認
10/6（火） 16:00-17:00		トレンドマイクロ「脅威データベース」にてウイルス名とその挙動確認、WindowsDefender のログを効率的に取得するためのイベントビューアの活用方法を下調べ

	実証参加企業 甲社による実施内容	お助け実働隊地域 IT 事業者 による実施内容
		電話にてフルスキャン前後のウイルス定義ファイルのバージョンを確認するためイベントビューアより、 Windows Defender に関する「evtx ファイル」などエビデンス取得の依頼を行い、メールにて操作方法提示・説明
10/7（水） 17:00-17:30	PC 上でイベントビューアより Windows Defender に関する「evtx ファイル」を PC 上で取得しメール送付	
10/7（水） 17:30-17:35		「evtx ファイル」をメール受領。各種 Defender の操作ログを確認しバージョンなどを取得
10/7（水） 17:35-17:40	電話にて本マルウエアに関するアラートが止まっていることを「見守りサービスポータル」で社長と一緒に確認し一旦完了報告	
10/8（木） 11:00-12:00	電話にて追加の画面コピーなどの送付依頼やエビデンスの確認	
聴取 40 分＋下調べ 50 分＋作業 80 分＋完了報告 30 分＋その他 35 分 ＝合計 235 分		

(3) リモートお助けを実施したお助け実働隊地域 IT 事業者へのヒアリング

表 4-34　リモートお助けを実施したお助け実働隊地域 IT 事業者へのヒアリング

①	リモートお助けでインシデントが解決しましたか？ ☑解決した　□解決しなかった(訪問お助けに切り替え)
②	リモートお助けは作業時間短縮に効果あると感じましたか？ ☑感じた　□感じなかった

③	仮に訪問お助け（駆け付け）を行っていたとすると、どれくらい時間がかかったと予想されますか？ 移動時間：往路だけで 240 分程かかっていたと思われる。 現地作業時間： 400 分程かかっていたと思われる。
④	リモートお助け時のツールの利用環境・利用方法を教えて下さい 利用者様… ☑被疑端末（PC/スマートフォン/タブレット） ☐被疑端末とは別 PC ☐被疑端末とは別スマートフォン/タブレット お助け隊… ☑PC ☑スマートフォン/タブレット 利用方法… ☐リモートツールの画面共有機能 ☐リモートツールのリモート操作機能 ☐スマートフォンなどのカメラ付き端末での映像共有 ☐視覚的情報の共有無し（電話での口頭指示のみ） ☑その他（電話、メール、「見守りサービスポータル」）
⑤	リモートツール（本件の場合、電話、メール、「見守りサービスポータル」）でチャレンジして実施できた作業を教えて下さい ☐LED 点灯状態確認 ☐ケーブル接続確認 ☐ケーブル挿抜、接続先変更 ☑被疑端末の画面確認 ☑ログの収集と確認 ☐コマンド操作（CLI）と結果確認 ☐ブラウザ操作（GUI）と結果確認 ☐正常性確認 ☐部品や機器交換 ☐その他（ ）
⑥	リモートツール（本件の場合、電話、メール、「見守りサービスポータル」）で現地の状況を把握できましたか？ ☑十分できた ☐一部できた ☐できなかった
⑦	リモートお助けはどのようなインシデントの場合に効果があると思いますか？ ☐目視確認が必要な事象（LED 点灯状態、ケーブル接続状態など） ☑エラーメッセージ内容など事象を正確に把握する必要がある事象 ☐文章で表現が難しい事象（画面表示、物理的な状態） ☑その他（**他社で頻出の対処実績のあるマルウエアの駆除対応**）
⑧	リモートお助けで最低限必要と感じた情報や設備は何ですか？ ☐システム構成図 ☐ネットワーク構成図 ☑IP アドレス一覧 ☑導入ソフトウエア一覧 ☑その他（**本サービスで発生検知済みのマルウエア一覧と各々の過去解決策のパターンを記載した FAQ が欲しい**）

⑨ リモートお助けは積極的に使いたいですか？

☑利用したい

☑リモートで対応するため、移動にかかる時間が短縮できた

☐世の中の動向などにより外出が困難な場合でも対応が可能だと感じた

☐画面越しで確認が行え、利用者様に適切な指示が行えた

☑対応を通し、利用者様と信頼関係が築けた

☑その他（**バージョン最新化やフルスキャン時に作業中断し無駄な待ち時間を回避し別日に実施可能**）

☐利用しない

☑電話でほとんど対応できる（画面越しで確認が必要な項目が少ない）

☐自身が直接操作を行えないため、逆に伝えるのに時間がかかる

☐作業ミスなどのリスクや責任分界点が不明瞭なため、慎重に時間をかけて作業を行う必要がある

⑩ リモートお助けで良かった点、悪かった点を教えて下さい

良かった点

☑現地まで出向かずに済む

☑問題解決までの時間が早くなった

☐現地から収集できる情報の量と精度が上がった

☑その他（**地方都市などの場合は移動時間が削減できる、フルスキャン待ちの時間が削減できる**）

悪かった点

☑利用者様にやってほしいことが伝わらない

☑試したいことをすぐに試せない（遠隔で指示してやって頂く必要がある）

☐シビアなタイミングでの操作ゆえ必要な調査ができない

☐複数の操作を同時に実施することが困難

☐画面がブレてよく見えない（手ブレなど）

☐全体状態など俯瞰した確認がしづらい（映像がつぶれる）

☐物理的な確認がしづらい（ケーブルを手繰るなど）

☑その他（**電話代をかなり要する。メッセンジャーや Zoom などに変えることが課題。緊急時は電話が一番迅速。作業日が複数に分割される**）

(4) インシデント対応を実施した実証参加企業などへのヒアリング

・ インシデント対応を実施した本実証参加企業（中小企業など）における、インシデント対応に関する評価・所感、インシデント発生前後での意識の変化、求めたい最低限の支援内容・費用、サイバー保険のニーズなどは下記のとおり。

表 4-35　インシデント対応を実施した実証参加企業などへのヒアリング（リモートお助け）

リモートお助け＜電話やリモートツールによる支援＞（甲社）	
リモートお助けで良かった点	□事象をリアルタイムに映像で確認してもらえる ☑初動対応が早い
リモートお助けで困ったこと	☑情報の伝達に時間がかかる □オペレーション1つ1つの確認に時間がかかる □リモートお助けのために時間が拘束されてしまう □お助け隊の作業を代理で行う必要があり、作業ミスが怖かった □作業ミスの責任分界点が曖昧
リモートお助けは積極的に利用したいか	□利用したい ☑利用したくない
駆け付けお助けは積極的に利用したいか	☑利用したい 利用したくない
トラブル解決までの時間は満足か	□とても満足　☑満足　□普通　□不満　□とても不満
リモートお助けを通じて社員のセキュリティ意識に変化があったか	□無かった ☑あった
お助け隊に最低限実施してほしい支援内容	☑1次対応（ウイルス駆除・PC初期化など） □原因特定 ☑再発防止策の提案
インシデントなどの突発的な問題対処で費用が発生した場合にかけられる費用	☑5万円以下 □10万円以下 □50万円以下 □100万円以下 □101万円以上
インシデントで発生する突発的な費用などのリスクに備えるサイバー保険はセキュリティサービスのメニューに必要か	☑必要 □不要 □どちらとも言えない

表 4-36　インシデント対応を実施した実証参加企業などへのヒアリング（訪問お助け）

訪問お助け＜駆け付け支援＞（乙社）	
訪問お助けで良かった点	☑事象を直接現場で確認してもらえる ☑情報の伝達をスムーズに行える ☑専門家に対応して頂けるので安心できる ☐自ら対応するより、トラブル解消までの時間が早い ☑トラブルの内容や対処方法を知ることができて勉強になった
訪問お助けで困ったこと	☐駆け付けまでに時間がかかる ☐作業を任せてしまい、状況を把握できない ☐予想以上に調査作業の対応が発生した ☑特に無し ※引き続き、リモートではなく、訪問お助けが頼りになります
リモートお助けは積極的に利用したいか	☐利用したい ☑利用したくない
駆け付けお助けは積極的に利用したいか	☑利用したい ☐利用したくない
トラブル解決までの時間は満足か	☐とても満足　☑満足　☐普通　☐不満　☐とても不満
駆け付けお助けを通じて社員のセキュリティ意識に変化があったか	☐無かった ☑あった
お助け隊に最低限実施してほしい支援内容	☑1次対応（ウイルス駆除・PC初期化など） ☑原因特定 ☐再発防止策の提案
インシデントなどの突発的な問題対処で費用が発生した場合にかけられる費用	☑5万円以下 ☐10万円以下 ☐50万円以下 ☐100万円以下 ☐101万円以上
インシデントで発生する突発的な費用などのリスクに備えるサイバー保険はセキュリティサービスのメニューに必要か	☐必要 ☐不要 ☑どちらとも言えない

4.4 報告会などによる事業成果の周知（成果報告会の開催結果）

表 4-37　成果報告会概要

開催日時	令和 3 年 1 月 15 日（金）
場所、形態	（1）大阪マリオット都ホテル（リアル開催） （2）YouTube Live（ライブによるオンライン配信）
参加者数	（1）21 人（社数：19 社）　（2）98 人（社数：オンライン開催のため不明） 計 119 人（うち 8 人が滋賀・奈良・和歌山）
アジェンダ	第一部　お助け隊実証で観測されたサイバー攻撃紹介 （大阪商工会議所、日本電気（株）） ①事業概要および 3 県の中小企業におけるサイバーセキュリティの実態 ②3 県の中小企業で実証中に観測されたサイバー攻撃の実例と脅威 第二部　中小企業報セキュリティ対策支援のご紹介 （IPA セキュリティプレゼンター） SECURITY ACTION、中小企業の情報セキュリティ対策ガイドライン 第三部　サイバー攻撃の実際と中小企業にとってその実現可能な対策 （神戸大学大学院工学研究科 教授） 
開催結果	・アンケートで受講企業でのサイバー攻撃と対策状況などが把握できた ➢ 集計結果は表 3-5～表 3-11 参照 ➢ 「商工会議所サイバーセキュリティお助け隊サービス」を ➢ 「利用したい」……6 社、「説明を聞きたい」……10 社 ・本実証事業参加企業以外（119 人のうち 115 人）にも本実証の概要と実証での収集情報、SECURITY ACTION などの説明ができ、広い地域の中小企業のサイバーセキュリティ意識向上に寄与できた。（波及効果） ➢ 「SECURITY ACTION」宣言を検討したい……8 社 ➢ 「中小企業の情報セキュリティ対策ガイドライン」を読んでみたい…31 社

開催結果	➢ 本実証でのサイバー攻撃実態「想像以上に多かった」…25 社（60%） **自由記述意見（講師の説明で印象に残った点など）** ・ サイバーお助け隊の活動、サービス提供、従業員の認識の甘さ、経営層への情報セキュリティの資産としての考え方が参考になった。 ・ SECURITY ACTION 宣言というものが会社の価値を上げそうだということが分かった。 ・ セキュリティ対策は、利益を生み出す・保証する・守るための最善の方策である。安全無くして生産無し。 ・ サイバーセキュリティ対策は、利益を生むための、言い換えれば、利益を保証し、守るための最善の方策。サイバーセキュリティは価値であり、それを生み出す投資である、という説明。 ・ 社内でなく社外から体制を問われる、見られる、という視点 ・ テレワークにおける VPN の脆弱性という言葉が印象的でした。VPN の機器やソフトウエアの脆弱性があることを認識して対応したい。OS を最新化していないなど、運用する人間のセキュリティ意識によるものは認識しているので今後も引き続き注意していきたい。 ・ 専門の人・お金が無くても社員のわずかな知識・注意で対応できる。 ・ 大阪商工会議所の方の「他県でも事業展開したい」という言葉に期待を感じました。（昨年度の大商様の事業報告書を拝読し、サービス利用者目線の真摯な姿勢に感銘を受け、別地域から今回の報告会に参加させて頂きました。パートナー企業様である NEC 様の UTM、各種サービス込みの月額 6,600 円は、名古屋商工会議所様請負の今年度実証事業参加者である私にとっては、非常に魅力的に感じました。地域密着型のお助け実働隊地域 IT 事業者サービスとの関係もあり、他地域への面的展開は容易ではないとの理解もありますが、名商様のパートナー企業様の提示価格は月額 1 万円を超えており、かつ顧客ケアの点でも満足できませんでした。同一地域内での複数の事業者による正当な価格競争が展開されることをサービス利用者としては期待します） ・ 1 人情シスどころかゼロ情シス（という説明が印象的だった） ・ 攻撃の件数（が印象的だった） ・ 脆弱性を突いた侵入ルートが多くなってきているのだと実感した。 ・ 体制の整備からまず行い、UTM の導入を検討する。 ・ セキュリティソフトと UTM では、防御力は雲泥の差という表現。 ・MBS（毎日放送）のテレビ取材があり（放映日は未定）仮に放映された場合は本実証事業の成果報告や啓発が更に広く波及する可能性がある。

5. 考察

5.1 実証参加企業におけるサイバー攻撃および対策などの実態

5.1.1 アンケートによる実態把握に係る考察

(1) 滋賀県・奈良県・和歌山県の中小企業などがさらされているサイバー攻撃の実態（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）に係る考察

① サイバー攻撃の有無

・ 表 3-5 のとおり、滋賀・奈良・和歌山では「標的型攻撃メール・ビジネスメール詐欺」のようなメール系の攻撃を経験している実証参加企業が 48%と非常に多く、日常的な脅威に常に直面していると言える。ランサムウエアは 4%と比較的少ない。また「分からない」が 38%を占めており、脅威を見える化してくれるセキュリティ機器の導入が進んでいないことが伺われる。(今回の実証では原則として UTM 未設置企業を対象としたため、回答母集団のうちのほとんどが UTM 未設置企業であるため、このような結果になっている点には留意する必要がある)

・ 令和元年度実証（大阪・京都・兵庫。以下、京阪神と略す）と比較すると「標的型攻撃メール・ビジネスメール詐欺」の 48%は、令和元年度の 24%と割合的に 2 倍も多く、調査時期が約 9 ヶ月間後であることも勘案しても非常に高い水準であると言えよう。両者の母集団は、規模（従業員数）がほぼ同じであり、業種別構成も令和元年度実証において製造業、サービス業の比率がやや多いほかはあまり変わらないため（以下同）、規模や業種の違いによるものとも言い難い。では、地域的特性に起因するものかと言うと、他の攻撃種のデータに有意差が見られない（そもそもサンプル数が少なすぎて統計的判断を下すことができない）ことから、それも断定的には言い切れない。

・ 滋賀・奈良・和歌山の 3 県（表中の「①-2」）では有意差は無い。

② サイバー攻撃被害の有無

・ 表 3-6 のとおり、滋賀・奈良・和歌山では、令和元年度実証同様に「分からない」が一番多く 66%を占めており、「攻撃」の「分からない」の 38%を遥かに上回っている。「被害」については、ランサムウエアなど目に見えるものでもない限り、一般の中小企業では特定しようも無く、したがって、各被害種ともに回答に 0 が並んでいる。唯一回答されているのがデータ損壊被害の 3 社（6%）である。無回答企業も多いが、これらはほぼ全て「分からない」に分類して差し支えなかろう。それを合わせると実質的に 9 割以上が「分からない」のが実態と言えよう。

・ 滋賀・奈良・和歌山の 3 県（表中の「②-2」）は回答母数が少なすぎて分析不能である。

(2) 滋賀県・奈良県・和歌山県の中小企業などにおけるサイバーセキュリティ対策状況（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）に係る考察

③ 情報システム担当者の有無

・ 表 3-7 のとおり、滋賀・奈良・和歌山では、「専任者がいる」が 6%、「兼任者がいない」が 34%、「1 人もおらず経営層が直轄」が 44%、「1 人もおらず IT 事業者に外注」が 14%であった。いわゆる「ゼロ情シス」が約 6 割を占めていることを含め、令和元年度実証の京阪神との有意差は見られない。IT 業者外注率は和歌山と滋賀が、京阪神および奈良と比較してやや高い傾向が読み取れる。但し、成果報告会受講企業（実証参加企業を除く。大阪を中心とする関西の中小企業）は「ゼロ情シス」は 3 割未満であり、明らかに実証参加企業とは異なる母集団であると考えられる。

・ 滋賀・奈良・和歌山の 3 県（表中の「③-2」）については、滋賀県の IT 業者外注率がやや高いほかは有意差は見られない。

④ 情報システム関係の業務マニュアルの有無

・ 表 3-8 のとおり、滋賀・奈良・和歌山では「担当者以外に分かる社員がおらず業務マニュアルも無い」が 80%を占めており、「業務マニュアルがあるのでどの社員でも対応できる」は 0 であった。これは表 3-7 のとおり専任者がほとんどいないことと一定の関係性があると考えられる。片手間で任されている兼任者は、業務マニュアルを作成する能力も時間的余力も当事者意識も稀薄なのかもしれない。今後は IoT 機器などが増加することが予想されるため、セキュリティを含めた IT のブラックボックス化が懸念される。

・ 滋賀・奈良・和歌山の 3 県（表中の「④-2」）での有意差は無い。

⑤ サイバー対策年間経費（正社員の情報システム担当者の人件費を除く）

・ 表 3-9 のとおり、現在においては、滋賀・奈良・和歌山では、額が増えるほどその構成比が低くなっており、「5 万円未満」64%と一番多く、次いで「5～10 万円」が 16%となっており、全体の 8 割が年 10 万円以下である。この傾向は令和元年度の京阪神とほぼ同様である。但し、成果報告会の受講企業群だけは、企業によって額が分散しており、具体的行動の点でも実証参加企業群とは異なっている。

・ 同じ質問につき、今後については、滋賀・奈良・和歌山では、「現在 5 万未満」と回答した企業のうち 4 割が増額を検討しているものの、その行き先はほとんどが「今後 5～10 万円」であることが推定される。これは 11 万円以上の各金額帯の割合がそれぞれほとんど変化していない（「11～20 万円」が 10%→10%、「21～50 万円」が 8%→8%、「51 万円以上」が 0%→4%）ことから読み取れる。各レイヤーにおいて一部には“顔ぶれ”の交代はあろうが、概ねは、現状において一番お金をかけていない「現状 5 万円未満」のうち 4 割が「さすがにもう少し増額しよう。でも 5 万円以内」というのが実情であろう。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑤-2」）での有意差は無い。

⑥ サイバー攻撃対策のセキュリティ実施状況

・ 表 3-10 のとおり、滋賀・奈良・和歌山では、令和元年度実証の京阪神と比較して、アンチウイルスソフトのような最低限の対策は 92%と高割合となっている。令和元年度実証の京阪神の 87%より高いのは、地域差というより経年（約 9～10 ヶ月）に伴う改善と考えられる。ファイアウオール、UTM、物理的管理の徹底、SECURITY ACTION などは、滋賀・奈良・和歌山の方が、経年によるアドバンテージ（上記）が若干あるにもかかわらず、京阪神よりも実施率が低く（ファイアウオール 28%＜38%、UTM2%＜8%、物理的管理の徹底 0%＜6%、SECURITY ACTION 8%＜11%）、大差とまでは言えないものの、これは若干の地域差と言えるかもしれない。なお、成果報告会の受講企業群だけは、UTM 設置率が 5 割を超えており、中小企業を十把一絡げに捉えてはいけないことが分かる。（そもそも本実証の参加対象は原則的に UTM 未設置企業である点に留意する必要がある）

・ 「サイバー攻撃損害保険」の付保率は１社（2%）しか無く、令和元年度実証の京阪神同様に非常に低い水準であり、地域差も経年差も見られず、少なくとも、実証参加企業においては全く普及していないことが分かる。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑥-2」）では、奈良の「パスワード設定」が 22%と他の 2 県および京阪神と比べてやや高割合なほかは、有意差は見られない。

⑦ テレワーク実施状況

・ 表 3-11 のとおり、滋賀・奈良・和歌山では、テレワークを「実施（部分実施を含む）している」が 34%、「実施していない」が 64%であった。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑦-2」）では、実施率は奈良が 4 割、和歌山が 3 割と若干の地域差が見られる。

⑧ テレワーク未導入の理由

・ 表 3-12 のとおり、滋賀・奈良・和歌山では、テレワーク未導入の理由として「テレワークできない業務内容」が一番多く 66%を占め、次いで「対応できる人材がいない」が 25%で続いている。「セキュリティが心配」は 19%であり、セキュリティを心配してテレワークを導入しないという企業は必ずしも多くはないことが分かる。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑧-2」）では、奈良において「セキュリティが心配」（22%）、「対応できる人材がいない」（28%）が他の 2 県に比べてやや高いこと、滋賀、和歌山において「（テレワークの）必要性を感じない」がそれぞれ約 2 割と奈良（6%）に比して少し高いことを除いては大差は見られない。滋賀、和歌山でテレワークの必要性が感じられていない理由の一つとしては、電車での通勤より自家用車での通勤の方が多いと考えられることが挙げられる。

⑨ 取引先からサイバー攻撃対策を求める意思表示の有無

・ 表 3-13 のとおり、滋賀・奈良・和歌山では、「取引先からサイバー攻撃対策を求める意

思表示の動向が無い」が 70%を占めており、「取引要件とされつつある」は 4%と非常に低く留まっている。しかし「指示されつつある」「依頼されつつある」の合計は全体の約 4 分の 1（24%）あり、まだまだ少数派とはいえ、サプライチェーンでの取り組みが進みつつあることが伺える。令和元年度実証の京阪神と比べると、滋賀・奈良・和歌山は「指示されつつある」「依頼されつつある」がやや多く、「取引先からサイバー攻撃対策を求める意思表示の動向が無い」がやや少ない傾向にある。これだけを見る限り、滋賀・奈良・和歌山では、京阪神より、サプライチェーンでのサイバーセキュリティの取り組みが進んでいるように受け取ることもできようが､大差ではないことも勘案すると、これは地域差というよりは 9 ヶ月間の経年差と捉えることもできる。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑨-2」）は回答母数が少なすぎ分析不能である。

⑩ サイバーセキュリティ対策を進める上での課題

・ 表 3-14 のとおり、滋賀・奈良・和歌山では、「コストの高さ・費用対効果」が課題として一番大きく 68%を占めている。次いで「経営者・従業員の意識」（40%）、「面倒さ・可用性の低下」（34%）、「脅威が分からない・見えない」（34%）と続く。「対策すべき内容・程度や対策商品が分からない」「信頼できる IT ベンダーがいない」といったサプライヤー側の問題に係る課題も一定数ある。

・ こうした課題を踏まえると、中小企業サイバーセキュリティ対策支援には、「安価さ」「（導入・運用の）簡便さ」「（脅威やその防御効果の）見える化」「お任せ型」「信頼できる主体によるサービス提供」などがソリューションのキーワードとして浮上する。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑩-2」）での有意差は無い。

(3) 滋賀県・奈良県・和歌山県の中小企業におけるサイバーセキュリティ対策に係るニーズの実態（令和元年度実証での大阪府・京都府・兵庫県の実証参加企業との比較を含め）に係る考察

⑪ サイバーセキュリティお助け隊実証に期待すること

・ 表 3-15 のとおり、「セキュリティの向上」が一番多く 60%を占めている。これは本実証事業の募集時期である 9 月に「Emotet」が再流行したこと、実証参加企業のほとんどが UTM 未設であったこと、などから、本実証事業がまさに“渡りに舟”のタイミングとなり「とにもかくにも眼前の脅威をブロックしたい」という動機付けが働いたことが推察される。次いで「自社セキュリティ対策の妥当性確認」「セキュリティ対策への助言の入手」がいずれも 42%と高率で並んでおり、これは、自社のセキュリティに関するアセスメントやアシスタントが得られる機会が滋賀・奈良・和歌山においてやや少なからんことが推定される。

・ これらニーズは、大阪商工会議所が本実証事業で提供する UTM を軸とした「お守り」「見守り」「お知らせ」「相談」ならびに別途実施する「簡易セキュリティ診断」などの検証サービス機能が、必要かつ十分なソリューションを提示し得るところのものであり、

後述のとおり、本実証事業が令和元年度実証に比して総合満足度が高かったのは、まさに上記ニーズに対するミスマッチが少なかったからと考えられる。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑪-2」）での有意差は無い。

⑫ サイバーインシデント発生時に必要となること

・ 表 3-16 のとおり、滋賀・奈良・和歌山では、「電話や遠隔 PC 操作による相談・ウイルス除去などの簡易処置対応」「IT 事業者などの駆け付けによる相談・ウイルス除去などの簡易処置対応」「感染した PC のクリーンナップ対応」などが令和元年度実証の京阪神同様に上位に挙げられており、これらニーズも、前質問同様に、大阪商工会議所が本実証事業で提供する「相談」「駆け付け」などの検証サービス機能で対応可能である。

・ 令和元年度実証の京阪神との特異的な差異としては、滋賀・奈良・和歌山においては「従業員へのサイバーセキュリティ教育」へのニーズが 46%あるのに対し京阪神は 15%しかない点、逆に「再発防止のためのセキュリティ強化」へのニーズは 26%しかないのに対し京阪神は 41%もある点などが挙げられる。前者については、滋賀・奈良・和歌山では支援機関や IT ベンダーなどによるセキュリティセミナーや関係イベントなどの情報発信・啓発の機会が比較的少ないと考えられること、後者については、別記のとおり、ファイアウオールや UTM の導入率が滋賀・奈良・和歌山では京阪神よりやや低いことに伴いインシデントの見える化も若干遅れていることなどにより“痛い経験”の経験値もやや少ないことなどに起因しているのかもしれない。

・ 滋賀・奈良・和歌山の 3 県（表中の「⑫-2」）での有意差は無い。

⑬ ウイルス対策ソフトで（最新バージョンにした上で）ウイルスの駆除を自社で行うことができるか

・ 表 3-17 のとおり、本質問項目は、成果報告会の受講企業のみに聞いた。表 3-7 のとおり、このレイヤーは「ゼロ情シス」が 3 割未満であるなど、比較的 IT リテラシーが高いと考えられる企業群である。

・ それでも「社員の誰かはできると思う」が 70%に留まっており、「どの社員もできないと思う」も約 2 割ある。このことから、比較的 IT リテラシーが高いと考えられる企業群においても、お助け実働隊地域 IT 事業者による初動対処支援のニーズは幾分かありそうである。事実、表 3-16 においても「IT 事業者などの駆け付けによる相談・ウイルス除去などの簡易処置対応」のニーズが 43%もあり、実証参加企業群とあまり変わらない。

5.1.2 簡易セキュリティ診断による実態把握に係る考察

(1) 全体（総評）

・ 「C（見直しが必要）」が 51%、「D（全面的に見直しが必要）」が 26%であり、計 77%の企業がセキュリティ対策に課題を抱えており、非大都市部の中小企業もサイバーセキュリティリスクにさらされていることは明らかである。

(2) 全体（カテゴリ別）

・ カテゴリ 1～3 の全てにおいて、約 7 割強が「C（見直しが必要）」「D（全面的に見直しが必要）」で占められており、あるカテゴリにリスクの偏りがあるわけではなく、全体的に対策が不足している。

・ 「3. リモートワークセキュリティの取り組み」において、「D（全面的に見直しが必要）」が 48%と、診断実施企業の約半分はリモートワークを実施するための準備ができておらず、多くの企業は令和 2 年 3 月の緊急事態宣言以降もリモートワークが実施できていない、もしくは準備不足のままリモートワークを実施せざるを得ない状況であると推測される。

・ 一方で「3. リモートワークセキュリティの取り組み」において、「A. 良く対策できている」も 26%と約 3 割存在し、他のカテゴリと比べると、実施率は高めであることから、一定数の企業では緊急事態宣言以前、もしくは緊急事態宣言をきっかけに優先度を上げて対応した可能性も考えられ、リモートワークに関しては、非大都市部の中小企業が一律で必要としているものではなく、企業の業種や業務内容などが導入の条件に関連しているものと考えられる。

・ 「4. SECURITY ACTION（一つ星宣言）」は「情報セキュリティ 5 か条」の達成状況を評価したものだが、「A. 良く対策できている」が 5%に留まり、ほとんどの企業ではサイバーセキュリティ対策の基本部分が実施できていないことが浮き彫りになった。中小企業のサイバーセキュリティ対策を行う上では、「情報セキュリティ 5 か条」に関わる対策から優先的に着手することが望ましいと考えられる。

(3) 全体（項目別）

・ 「情報セキュリティに関する脅威や攻撃の手口についての情報収集（1-1）」ができている企業は診断実施企業の 16%に留まり、半数は「できていない/不明」という結果であった。情報収集の実態は、企業側が能動的に実施する必要があるため、情報システム担当者を置くことが難しい中小企業には敷居が高い可能性が考えられる。（情報システム部門や専任担当者の配置ができている診断実施企業は 16%（Q1-11））

・ 情報収集に関して中小企業全体の底上げを行うためには、メールマガジンなどによる定期的な情報配信など、不特定対数の企業が受動的に情報を集められる仕組みを検討する

余地がある。但し、情報量が多すぎると受け取っても活用されない（見ない）可能性もあるため、配信する情報の重要度・量・頻度のバランスを考慮しておく必要がある。

・ 「パスワード設定ルール（Q1-2,Q1-7）」、「アクセス権の定期的な見直し（Q1-3）」「情報の持ち出し管理（Q1-6）」などの IT 技術だけでは解決できない「組織内の運用ルールの策定や運用」ができている企業も 3 割未満に留まっている。情報セキュリティに関する一定の知識が必要な運用ルールの策定は企業側にとっては大きな負担であることが想定される。パスワード設定ルールやアクセス権の定期的な見直しなど、企業に対して依存度が低いルールに関しては、共通ルールとしてマニュアルや指針を策定し、中小企業に提供することができれば、企業側の負担を軽減する一助となるかもしれない。

・ 「私物媒体の業務利用禁止（Q1-8）」「私物 PC/スマホの業務利用禁止（Q3-2）」では 7 割の企業で私物の業務利用が認められた。「私物を業務利用する上でのセキュリティ対策の実施（Q1-9,Q3-3）」についても対策を実施できている企業は 1 割未満に留まり、多くの診断実施企業が情報漏洩リスクを抱えた状態で業務を行っている実態が明らかになった。事業所規模が小さい企業（診断実施企業のうち 37 社（65%）が 20 人未満の企業）では、業務用 PC などの IT リソースを潤沢に用意できないなどの理由が考えられるが、いかなる理由であれ、私物を利用するのであれば、セキュリティ対策は必須である。本実証では「テレワーク」を前提としたリモート接続ツールの提供であったこともあり、テレワークができない業務内容などの理由から、テレワークの実施が低調に終わったが、リモート接続ツールを「データを持ち出さないためのツール」として活用するなど、視点を変えることで、私物利用をサイバーセキュリティリスクから守るソリューションとしてのニーズはあるかもしれない。

・ 「外部の脅威からの社内ネットワーク保護（Q2-4,Q2-8）」「インターネット利用に関するリスク対策（Q2-3,Q2-5）」についても 3～4 割程度の診断実施企業でしか対策ができておらず、サイバーセキュリティ対策を包括的に実施可能なサイバーセキュリティお助け隊サービスの潜在ニーズは存在すると推察される。

・ IPA と中小企業関係団体が自発的な情報セキュリティ対策を促す取り組みとして推進している「SECURITY ACTION」の「一つ星宣言」に定義されている「情報セキュリティ 5 か条」は以下のとおりである。

表 5-1　情報セキュリティ 5 か条

1	OS やソフトウエアは常に最新の状態にしよう！
2	ウイルス対策ソフトを導入しよう！
3	パスワードを強化しよう！
4	共有設定を見直そう！
5	脅威や攻撃の手口を知ろう！

IPA：「SECURITY ACTION」、https://www.ipa.go.jp/security/security-action/index.html
（2021/1/6 参照）

・ 「情報セキュリティ5か条」の達成状況という観点では、「1.OSやソフトウエアは常に最新の状態にしよう！」は「できている（54%）」、「2.ウイルス対策ソフトを導入しよう！」は「できている（65%）」であり、約6割前後の診断実施企業で脆弱性やウイルスに対して危機感を持っており、対策を講じていることが分かった。しかしながら、「3.パスワードを強化しよう！」「4.共有設定を見直そう！」「5.脅威や攻撃の手口を知ろう！」に関しては、「できている」が2割～3割程度に留まっていた。

・ OSのパッチ適用やウイルス対策ソフトの定義ファイル最新化は、インターネットに接続された環境があれば、製品側で自動的に実施されることもあり、比較的実施率が高い結果になったものと考えられる。

・ パスワードの強化や共有設定の見直しなどは、組織としての運用が必要な項目であるため、実施率が低い結果になったものと推測される。

・ 「過去に情報セキュリティに関する問題の発生有無(Q2-10)」については「ある」が42%、「インシデントの対応手順の策定と周知（Q2-9）」については「できていない/不明」が60%となっており、情報セキュリティインシデントの発生経験はあるものの、インシデント対応手順が整備されていない実態が明らかになった。「サイバーセキュリティお助け隊サービス」によるインシデント対応やサイバー保険による補償は非大都市部の中小企業にとっても重要な意味を持つサービスであると考える。

(4) 地域別（総評）

・ 各地域ともに「A（良く対策できている）」は10%前後であり、地域ごとに割合の差はあるものの、地域差に起因する要因は認められず、どの地域の中小企業もサイバーセキュリティリスクにさらされているということ以外に特徴的な分析結果は得られなかった。

(5) 地域別（カテゴリ別）

・ カテゴリ別に見ても、地域ごとに割合の差はあるものの、割合の差は地域差に起因する要因は認められず、簡易セキュリティ診断を実施した企業ごとの取り組みの差に起因するものと推察される。

(6) 事業所規模別（総評・カテゴリ別）

・ 総評・カテゴリ別ともに、事業所規模ごとの母数が小さい値になり、事業所規模ごとの母数に含まれる企業の診断結果がより濃く分析結果に反映されてしまった。また、事業所規模間の母数の乖離が大きいため、事業所規模単位での単純比較もできず、有効な分析ができないと判断した。

(7) 業種別（総評・カテゴリ別）

・ 事業所規模別と同様、総評・カテゴリ別ともに、業種ごとの母数が小さい値になり、業種ごとの母集団に含まれる企業の診断結果がより濃く分析結果に反映されてしまった。また、業種間の母数の乖離が大きいため、業種単位での単純比較もできず、有効な分析ができないと判断した。

5.1.3 UTM の観測結果に係る考察

(1) 所在地別に対する今年度の考察

・ UTM 脅威検知数の推移（AV/IPS/WG）で地域別に確認すると、和歌山県が 11 月 2,3 週にかけて検知数が突出していることが確認できる。また、滋賀県においても 12 月 3 週に検知数が突出していることが確認できる。この検知のほとんどは、特定の 2 社で IPS により検知された脅威である。和歌山県の企業に対して、個別にヒアリングを実施したところ、グループウェアサービスを提供していることが判明した。また、検知数が突出しているグローバル IP（141.98.80.xx）は日本国外のものがほとんどであるため実際の攻撃にさらされていたと考えられる。滋賀県の企業に関しても、ヒアリングは実施できていないが、同様の理由が想定される。（「図 4-21　UTM 脅威検知数の推移（AV/IPS/WG）（所在地別」、「図 4-23　UTM 脅威検知数の推移（IPS）（所在地別」参照）

・ UTM 脅威検知数の推移（AV）で地域別に確認すると、奈良県が 10 月 5 週、12 月 2 週に検知数が突出している。この検知はいずれも特定の 1 社で検知されており、脅威の内容はトロイの木馬ウイルスと想定されるものが多く検知された。この企業に対してヒアリングは実施できていないが、取引にメールが多く活用されている企業と想定される。（「図 4-22　UTM 脅威検知数の推移（AV）（所在地別」参照）

・ UTM 脅威検知数の推移（WG）で地域別に確認すると、和歌山県が 11 月 3 週に検知数が突出していることが確認できる。この検知は特定の 1 社で検知されており、アドウエアと呼ばれる広告を目的とするソフトウエアの配布や、アドウエアの通信先となるサイトの一つである。（「図 4-24　UTM 脅威検知数の推移（WG）（所在地別」参照）

・ 結論として、今年度の実証において脅威検知は特定の地域ではなく、特定の企業で多く検知されることが確認できた。また、検知件数の多少に関わらずどの地域も攻撃を受けていることが確認できた。

(2) 企業別に対する今年度の考察

・ UTM 脅威検知数の推移（AV）で企業別に確認すると、1 社のみ検知数が突出していることが確認できる。（「図 4-25　UTM 脅威検知数（AV）（企業別」参照）

・ UTM 脅威検知数の推移（IPS）で企業別に確認すると、2 社のみ検知数が突出している

ことが確認できる。（「図 4-26　UTM 脅威検知数（IPS）（企業別」参照）

・ UTM 脅威検知数の推移（WG）で企業別に確認すると、1 社のみ検知数が 20 件を超えてしていることが確認できる。（「図 4-27　UTM 脅威検知数（WG）（企業別」参照）

・ 結論として、昨年度と同様に今年度の実証における脅威検知では、全企業が平均的に脅威を検知しているのではなく、特定の企業で多く検知していることが確認できた。AV は送信先 IP アドレスが複数にわたって継続的に記録されているため、特定の端末で検知されていないことが確認できた。また、IPS は特定の企業が特定の日に集中して検知している傾向が確認された。但し、攻撃を検知した日に法則性は確認できなかった。

(3) 事業所規模別に対する今年度の考察

・ UTM 脅威検知数の推移（AV）で事業所規模別に確認すると、1～5 人の規模で検知数が突出していることが確認できる。（「図 4-28　UTM 脅威検知数（AV）（事業所規模別）」参照）

・ UTM 脅威検知数の推移（IPS）で事業所規模別に確認すると、1～5 人、101～200 人の規模で検知数が突出していることが確認できる。（「図 4-29　UTM 脅威検知数（IPS）（事業所規模別」参照）

・ UTM 脅威検知数の推移（WG）で事業所規模別に確認すると、1～5 人の規模で検知数が 20 件を超えていることが確認できる。（「図 4-30　UTM 脅威検知数（WG）（事業所規模別」参照）

・ 結論として、上記の事業所規模別の検知数を押し上げているのは特定の企業であり、これを除いた件数で分析すると事業所規模に起因した傾向は見られなかった。

(4) 事業所規模別に対する昨年度との比較

・ 令和元年度実証と今年度実証では実証期間および実証参加企業数などに差異があるため、件数による比較だと業種や事業所規模に偏りが出る。そのため、令和元年度実証と今年度実証において、実証に参加した企業の業種や事業所規模の割合に対して、脅威を検知した企業の検知比率に注目して分析を行った。その結果は以下のとおりである。また、令和元年度実証および今年度実証で一部の業種および事業所規模において母数が小さい値となり、検知比率の妥当性を示しにくい結果となったため、それらは分析対象から除外した。

表 5-2　脅威検知（AV/IPS/WG 合計）と事業所規模の傾向［昨年度］

事業所規模	参加社数（112 社）	事業所規模別参加比率	脅威検知社数（88 社）	検知比率	備考
1~5 人	35 社	30%	24 社	27%	
6~10 人	20 社	18%	14 社	16%	
11~20 人	12 社	11%	11 社	13%	
21~50 人	28 社	25%	24 社	27%	
51~100 人	12 社	11%	10 社	12%	
101~200 人	3 社	3%	3 社	3%	*1
201~300 人	2 社	2%	2 社	2%	*1

*1：参加社数の母数が少ないため対象外

表 5-3　脅威検知（AV/IPS/WG 合計）と事業所規模の傾向［今年度］

事業所規模	参加社数（53 社）	事業所規模別参加比率	脅威検知社数（38 社）	検知比率	備考
1~5 人	21 社	40%	11 社	29%	
6~10 人	6 社	11%	6 社	16%	
11~20 人	10 社	19%	7 社	18%	
21~50 人	8 社	15%	7 社	18%	
51~100 人	1 社	2%	1 社	3%	*1
101~200 人	5 社	9%	4 社	11%	
201~300 人	2 社	4%	2 社	5%	*1

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の事業所規模に注目すると、脅威検知（AV/IPS/WG 合計）と事業所規模の傾向では、昨年度は参加比率に対する検知比率で突出した値は見受けられなかったが、今年度は 6～10 人において検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の事業所規模への偏りは確認できなかった。

表 5-4　脅威検知（AV）と事業所規模の傾向［昨年度］

事業所規模	参加社数（112 社）	事業所規模別参加比率	脅威検知社数（34 社）	検知比率	備考
1~5 人	35 社	30%	9 社	26%	
6~10 人	20 社	18%	4 社	12%	
11~20 人	12 社	11%	4 社	12%	
21~50 人	28 社	25%	10 社	29%	
51~100 人	12 社	11%	5 社	15%	
101~200 人	3 社	3%	1 社	3%	*1
201~300 人	2 社	2%	1 社	3%	*1

*1：参加社数の母数が少ないため対象外

表 5-5　脅威検知（AV）と事業所規模の傾向［今年度］

事業所規模	参加社数（53 社）	事業所規模別参加比率	脅威検知社数（12 社）	検知比率	備考
1~5 人	21 社	40%	6 社	50%	
6~10 人	6 社	11%	1 社	8%	
11~20 人	10 社	19%	3 社	26%	
21~50 人	8 社	15%	0 社	0%	
51~100 人	1 社	2%	0 社	0%	*1
101~200 人	5 社	9%	1 社	8%	
201~300 人	2 社	4%	1 社	8%	*1

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の事業所規模に注目すると、脅威検知（AV）と事業所規模の傾向では、昨年度は 21～50 人、51～100 人において検知比率がやや高く見受けられるが、今年度は 1～5 人、11～20 人において検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の事業所規模への偏りは確認できなかった。

表 5-6　脅威検知（IPS）と事業所規模の傾向［昨年度］

事業所規模	参加社数（112 社）	事業所規模別参加比率	脅威検知社数（79 社）	検知比率	備考
1~5 人	35 社	30%	20 社	25%	
6~10 人	20 社	18%	13 社	16%	
11~20 人	12 社	11%	9 社	11%	
21~50 人	28 社	25%	22 社	28%	
51~100 人	12 社	11%	10 社	13%	
101~200 人	3 社	3%	3 社	4%	*1
201~300 人	2 社	2%	2 社	3%	*1

*1：参加社数の母数が少ないため対象外

表 5-7　脅威検知（IPS）と事業所規模の傾向［今年度］

事業所規模	参加社数（53 社）	事業所規模別参加比率	脅威検知社数（30 社）	検知比率	備考
1~5 人	21 社	40%	5 社	17%	
6~10 人	6 社	11%	5 社	17%	
11~20 人	10 社	19%	6 社	20%	
21~50 人	8 社	15%	7 社	23%	
51~100 人	1 社	2%	1 社	3%	*1
101~200 人	5 社	9%	4 社	13%	
201~300 人	2 社	4%	2 社	7%	*1

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の事業所規模に注目すると、脅威検知（IPS）と事業所規模の傾向では、昨年度は参加比率に対する検知比率で突出した値は見受けられなかったが、今年度は 6～10 人、21～50 人において検知比率がやや高いことが見受けられる。また、101～200 人において昨年度は母数が少ないため分析対象外だが、今年度は検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の事業所規模への偏りは確認できなかった。

表 5-8　脅威検知（WG）と事業所規模の傾向［昨年度］

事業所規模	参加社数（112 社）	事業所規模別参加比率	脅威検知社数（5 社）	検知比率	備考
1~5 人	35 社	30%	0 社	0%	
6~10 人	20 社	18%	0 社	0%	
11~20 人	12 社	11%	0 社	0%	
21~50 人	28 社	25%	3 社	60%	
51~100 人	12 社	11%	1 社	20%	
101~200 人	3 社	3%	1 社	20%	*1
201~300 人	2 社	2%	0 社	0%	*1

表 5-9　脅威検知（WG）と事業所規模の傾向［今年度］

事業所規模	参加社数（53 社）	事業所規模別参加比率	脅威検知社数（12 社）	検知比率	備考
1~5 人	21 社	40%	4 社	33%	
6~10 人	6 社	11%	1 社	8%	
11~20 人	10 社	19%	2 社	17%	
21~50 人	8 社	15%	2 社	17%	
51~100 人	1 社	2%	0 社	0%	*1
101~200 人	5 社	9%	2 社	17%	
201~300 人	2 社	4%	1 社	8%	*1

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の事業所規模に注目すると、脅威検知（WG）と事業所規模の傾向では、昨年度は 21～50 人、51～100 人において検知比率がやや高く見受けられる。また、101～200 人において昨年度は分析対象外だが、今年度は検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の事業所規模への偏りは確認できなかった。

(5) 業種別に対する今年度の考察

・ UTM 脅威検知数の推移（AV）で業種別に確認すると、卸売業・小売業で検知数が突出していることが確認できる。（「図 4-31　UTM 脅威検知数（AV）（業種別」参照）

・ UTM 脅威検知数の推移（IPS）で業種別に確認すると、建設業、製造業で検知数が突出していることが確認できる。（「図 4-32　UTM 脅威検知数（IPS）（業種別」参照）

・ UTM 脅威検知数の推移（WG）で業種別に確認すると、情報通信業で検知数が 20 件を超えてしていることが確認できる。（「図 4-33　UTM 脅威検知数（WG）（業種別」参照）

・ 結論として、上記の業種別の検知数を押し上げているのは特定の企業であり、これを除いた件数で分析すると業種に起因した傾向は見られなかった。

(6) 業種別に対する昨年度との比較

・ 令和元年度実証と今年度実証では実証期間および実証参加企業数などに差異があるため、件数による比較だと業種や事業所規模に偏りが出る。そのため、令和元年度実証と今年度実証において、実証参加企業の業種や事業所規模の割合に対して、脅威を検知した企業の検知比率に注目して分析を行った。その結果は以下のとおりである。また、令和元年度実証および今年度実証で一部の業種および事業所規模において母数が小さい値となり、検知比率の妥当性を示しにくい結果となったため、それらは分析対象から除外した。

表 5-10　脅威検知（AV/IPS/WG 合計）と業種の傾向［昨年度］

業種	参加社数（112 社）	業種別参加比率	脅威検知社数（88 社）	検知比率	備考
D 建設業	8 社	**7%**	7 社	**8%**	
E 製造業	44 社	**39%**	35 社	**40%**	
G 情報通信業	0 社	**0%**	0 社	**0%**	*1
H 運輸業・郵便業	1 社	**1%**	1 社	**1%**	*1
I 卸売業・小売業	21 社	**19%**	15 社	**17%**	
K 不動産業・物品賃貸業	0 社	**0%**	0 社	**0%**	*1
L 学術研究・専門技術サービス業	0 社	**0%**	0 社	**0%**	*1
M 宿泊業・飲食店	3 社	**3%**	3 社	**3%**	*1
O 教育学習支援業	0 社	**0%**	0 社	**0%**	*1
Q 複合サービス事業	0 社	**0%**	0 社	**0%**	*1
R サービス業（他に分類されないもの）	35 社	**31%**	27 社	**31%**	

*1：参加社数の母数が少ないため対象外

表 5-11　脅威検知（AV/IPS/WG 合計）と業種の傾向［今年度］

業種	参加社数（53 社）	業種別参加比率	脅威検知社数（38 社）	検知比率	備考
D 建設業	6 社	11%	4 社	11%	
E 製造業	12 社	22%	9 社	23%	
G 情報通信業	4 社	7%	4 社	11%	
H 運輸業・郵便業	1 社	2%	1 社	3%	*1
I 卸売業・小売業	9 社	17%	9 社	23%	
K 不動産業・物品賃貸業	1 社	2%	0 社	0%	*1
L 学術研究・専門技術サービス業	4 社	7%	1 社	3%	
M 宿泊業・飲食店	2 社	4%	1 社	3%	*1
O 教育学習支援業	2 社	4%	1 社	3%	*1
Q 複合サービス事業	2 社	4%	2 社	5%	*1
R サービス業（他に分類されないもの）	10 社	19%	6 社	15%	

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の業種に注目すると、脅威検知（AV/IPS/WG 合計）と業種の傾向では、今年度は卸売業・小売業において検知比率がやや高いことが見受けられる。また、情報通信業において昨年度は母数が 0 のため分析対象外だが、今年度は検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の業種への偏りは確認できなかった。

表 5-12　脅威検知（AV）と業種の傾向［昨年度］

業種	参加社数（112 社）	業種別参加比率	脅威検知社数（34 社）	検知比率	備考
D 建設業	8 社	7%	4 社	12%	
E 製造業	44 社	39%	19 社	55%	
G 情報通信業	0 社	0%	0 社	0%	*1
H 運輸業・郵便業	1 社	1%	0 社	0%	*1
I 卸売業・小売業	21 社	19%	3 社	9%	
K 不動産業・物品賃貸業	0 社	0%	0 社	0%	*1
L 学術研究・専門技術サービス業	0 社	0%	0 社	0%	*1
M 宿泊業・飲食店	3 社	3%	0 社	0%	*1
O 教育学習支援業	0 社	0%	0 社	0%	*1
Q 複合サービス事業	0 社	0%	0 社	0%	*1
R サービス業（他に分類されないもの）	35 社	31%	8 社	24%	

*1：参加社数の母数が少ないため対象外

表 5-13　脅威検知（AV）と業種の傾向［今年度］

業種	参加社数（53 社）	業種別参加比率	脅威検知社数（12 社）	検知比率	備考
D 建設業	6 社	11%	0 社	0%	
E 製造業	12 社	22%	4 社	33%	
G 情報通信業	4 社	7%	3 社	25%	
H 運輸業・郵便業	1 社	2%	0 社	0%	*1
I 卸売業・小売業	9 社	17%	3 社	25%	
K 不動産業・物品賃貸業	1 社	2%	0 社	0%	*1
L 学術研究・専門技術サービス業	4 社	7%	0 社	0%	
M 宿泊業・飲食店	2 社	4%	0 社	0%	*1
O 教育学習支援業	2 社	4%	0 社	0%	*1
Q 複合サービス事業	2 社	4%	0 社	0%	*1
R サービス業（他に分類されないもの）	10 社	19%	2 社	17%	

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の業種に注目すると、脅威検知（AV）と業種の傾向では、昨年度は建設業、製造業において検知比率がやや高く見受けられるが、今年度は製造業、卸売業・小売業において検知比率がやや高いことが見受けられる。また、情報通信業において昨年度は母数が 0 のため分析対象外だが、今年度は検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の業種への偏りは確認できなかった。

表 5-14　脅威検知（IPS）と業種の傾向［昨年度］

業種	参加社数（112 社）	業種別参加比率	脅威検知社数（79 社）	検知比率	備考
D 建設業	8 社	7%	6 社	8%	
E 製造業	44 社	39%	31 社	39%	
G 情報通信業	0 社	0%	0 社	0%	*1
H 運輸業・郵便業	1 社	1%	1 社	1%	*1
I 卸売業・小売業	21 社	19%	14 社	18%	
K 不動産業・物品賃貸業	0 社	0%	0 社	0%	*1
L 学術研究・専門技術サービス業	0 社	0%	0 社	0%	*1
M 宿泊業・飲食店	3 社	3%	3 社	4%	*1
O 教育学習支援業	0 社	0%	0 社	0%	*1
Q 複合サービス事業	0 社	0%	0 社	0%	*1
R サービス業（他に分類されないもの）	35 社	31%	24 社	30%	

*1：参加社数の母数が少ないため対象外

表 5-15　脅威検知（IPS）と業種の傾向［今年度］

業種	参加社数（53 社）	業種別参加比率	脅威検知社数（30 社）	検知比率	備考
D 建設業	6 社	11%	3 社	11%	
E 製造業	12 社	22%	8 社	27%	
G 情報通信業	4 社	7%	1 社	3%	
H 運輸業・郵便業	1 社	2%	1 社	3%	*1
I 卸売業・小売業	9 社	17%	6 社	20%	
K 不動産業・物品賃貸業	1 社	2%	0 社	0%	*1
L 学術研究・専門技術サービス業	4 社	7%	1 社	3%	
M 宿泊業・飲食店	2 社	4%	1 社	3%	*1
O 教育学習支援業	2 社	4%	1 社	3%	*1
Q 複合サービス事業	2 社	4%	2 社	7%	*1
R サービス業（他に分類されないもの）	10 社	19%	6 社	20%	

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の業種に注目すると、脅威検知（IPS）と業種の傾向では、昨年度は参加比率に対する検知比率で突出した値は見受けられなかったが、今年度は製造業において検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の業種への偏りは確認できなかった。

表 5-16　脅威検知（WG）と業種の傾向［昨年度］

業種	参加社数（112 社）	業種別参加比率	脅威検知社数（5 社）	検知比率	備考
D 建設業	8 社	7%	1 社	20%	
E 製造業	44 社	39%	3 社	60%	
G 情報通信業	0 社	0%	0 社	0%	*1
H 運輸業・郵便業	1 社	1%	0 社	0%	*1
I 卸売業・小売業	21 社	19%	1 社	20%	
K 不動産業・物品賃貸業	0 社	0%	0 社	0%	*1
L 学術研究・専門技術サービス業	0 社	0%	0 社	0%	*1
M 宿泊業・飲食店	3 社	3%	0 社	0%	*1
O 教育学習支援業	0 社	0%	0 社	0%	*1
Q 複合サービス事業	0 社	0%	0 社	0%	*1
R サービス業（他に分類されないもの）	35 社	31%	0 社	0%	

*1：参加社数の母数が少ないため対象外

表 5-17　脅威検知（WG）と業種の傾向［今年度］

業種	参加社数（53 社）	業種別参加比率	脅威検知社数（12 社）	検知比率	備考
D 建設業	6 社	11%	2 社	17%	
E 製造業	12 社	22%	3 社	25%	
G 情報通信業	4 社	7%	2 社	17%	
H 運輸業・郵便業	1 社	2%	0 社	0%	*1
I 卸売業・小売業	9 社	17%	2 社	17%	
K 不動産業・物品賃貸業	1 社	2%	0 社	0%	*1
L 学術研究・専門技術サービス業	4 社	7%	1 社	8%	
M 宿泊業・飲食店	2 社	4%	1 社	8%	*1
O 教育学習支援業	2 社	4%	0 社	0%	*1
Q 複合サービス事業	2 社	4%	0 社	0%	*1
R サービス業（他に分類されないもの）	10 社	19%	1 社	8%	

*1：参加社数の母数が少ないため対象外

・ 母数が一定数以上の業種に注目すると、脅威検知（WG）と業種の傾向では、昨年度は建設業、製造業において検知比率がやや高く見受けられるが、今年度は建設業において検知比率がやや高いことが見受けられる。また、情報通信業において昨年度は母数が 0 のため分析対象外だが、今年度は検知比率がやや高いことが見受けられる。しかし、突出した検知比率の差異ではないため、昨年度と比較しても特定の業種への偏りは確認できなかった。

(7) UTM 機能別に対する今年度の考察

・ 今年度実証で検知されたアラートについて、マルウエア感染の可能性が高い重要度：★★★（高）は検知されなかった。マルウエア感染の可能性が考えられる重要度：☆★★（中）は 146 件検知された。マルウエア感染の可能性が低い重要度：☆☆★（低）は 1,201 件検知された。今年度実証において、重要度：★★★（高）が検知されなかった理由は、実証期間の短さと、シグネチャの精度向上が想定される。

・ また、AV における外部からの攻撃は 524 件、外部への不正通信は 0 件、IPS における外部からの攻撃は 7,906 件、外部への不正通信は 2,091 件、内部の脆弱性は 199 件検知された。令和元年度実証と比較して、IPS,WG による外部への不正通信の検知数が比較的多いが、この理由はクロスサイトスクリプティングである。攻撃者が標的の Web サイトの脆弱性を悪用し、不正なコンテンツを埋め込み Cookie 情報を盗んでしまう脅威であり、検知した企業は注意が必要である。また、WG についてもアドウエア関連サイトや画像アップロードサイトに企業が通信したと想定され、検知した企業は怪しいサイトは閲覧しないよう注意が必要である。

・ アンチウイルス機能による通信の遮断で、最も多かった脅威は「Trojan.Multi.Generic.4」である。当該脅威は、アンチウイルス機能による全遮断数の 4 割程度を占め、実証参加企業 53 社のうち 5 社で検知された。「Trojan.Multi.Generic.4」は、トロイの木馬と呼ばれる形式のウイルスで、ウイルス感染した端末から情報を盗み出してしまう。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ アンチウイルス機能による通信の遮断で、2 番目に多く見受けられた脅威は「Hacktool.MSOffice.Generic.3」である。当該脅威は、アンチウイルス機能による全遮断数の 2 割程度を占め、実証参加企業 53 社のうち 2 社で検知された。「Hacktool.MSOffice.Generic.3」は、ウイルス、ワーム、トロイの木馬などを生成し、他の端末をハッキングする疑いのあるファイル送受信の通信を検知したものである。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ アンチウイルス機能による通信の遮断で、3 番目に多く見受けられた脅威は「Trojan.Script.Generic.a」である。当該脅威は、アンチウイルス機能による全遮断数の 1 割程度を占め、実証参加企業 53 社のうち 1 社で検知された。「Trojan.Script.Generic.a」

は、最も多かった脅威と同様に、トロイの木馬と呼ばれる形式のウイルスであり、銀行口座番号などの個人情報や秘匿情報を窃取されてしまう。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ 不正侵入防止機能による通信の遮断で、最も多かった脅威は「Cross Site Script attack」である。当該脅威は、不正侵入防止機能による全遮断数の 2 割程度を占め、実証参加企業 53 社のうち 13 社で検知された。「Cross Site Script attack」は、Web アプリケーションの脆弱性などを利用したクロスサイトスクリプティングという攻撃である。クロスサイトスクリプティング攻撃では、攻撃者が標的の Web サイトの脆弱性を悪用し、不正なコンテンツを埋め込み Cookie 情報を盗んでしまう。攻撃者は、盗んだ Cookie 情報を不正アクセスなどに悪用してしまう。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ 不正侵入防止機能による通信の遮断で、2 番目に多く見受けられた脅威は「JSIG-WEB SQL-Union-ALL-Select-1」である。当該脅威は、不正侵入防止機能による全遮断数の 2 割程度を占め、実証参加企業 53 社のうち 1 社で検知された。「JSIG-WEB SQL-Union-ALL-Select-1」は、SQL Injection を用いた攻撃で、Web アプリケーションなどに対してセキュリティ上の不備を意図的に利用し、想定しない SQL 文を実行させることで、データベースシステムから個人情報などを不正に入手する脅威である。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。同企業への個別ヒアリングを実施したところ、グループウェアサービスを提供していることが判明した。

・ 不正侵入防止機能による通信の遮断で、3 番目に多く見受けられた脅威は「JSIG-WEB:SQL-Union-ALL-Select-3」である。当該脅威は、不正侵入防止機能による全遮断数の 2 割程度を占め、実証参加企業 53 社のうち 1 社で検知された。「JSIG-WEB:SQL-Union-ALL-Select-3」は、2 番目に多かった脅威と同様に、SQL Injection を用いた攻撃で、Web アプリケーションなどに対してセキュリティ上の不備を意図的に利用し、想定しない SQL 文を実行させることで、データベースシステムから個人情報などを不正に入手する脅威である。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。この企業も同一の企業であり、ヒアリングの結果、グループウェアサービスを提供していることが判明した。

・ Web ガード機能による通信の遮断で、最も多かった脅威は「infopicked.com」である。当該脅威は、Web ガード機能による全遮断数の 3 割程度を占め、実証参加企業 53 社のうち 2 社で検知された。「infopicked.com」は、アドウエアと呼ばれる広告を目的とするソフトウエアの配布や、アドウエアの通信先となるサイトの一つである。当該サイトを閲覧することでマルウエア感染した端末から個人情報や企業情報を盗んでしまい、不正に悪用されてしまう可能性がある。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ Web ガード機能による通信の遮断で、2 番目に多く見受けられた脅威は「images2.imgbox.com」である。当該脅威は、Web ガード機能による全遮断数の 3 割程度を占め、実証参加企業 53 社のうち 3 社で検知された。「images2.imgbox.com」は、画像アップロードサイトの一つである。当該サイトは攻撃にもよく利用されていたサイトであり、閲覧することでマルウエア感染した端末から個人情報や企業情報を盗んでしまい、不正に悪用されてしまう可能性がある。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

・ Web ガード機能による通信の遮断で、3 番目に多く見受けられた脅威は「eu.dspultra.com/api/submit_form_request」である。当該脅威は、Web ガード機能による全遮断数の 2 割程度を占め、実証参加企業 53 社のうち 2 社で検知された。「eu.dspultra.com/api/submit_form_request」は、1 番目に多かった脅威と同様に、アドウエアと呼ばれる広告を目的とするソフトウエアの配布や、アドウエアの通信先となるサイトの一つである。当該サイトを閲覧することでマルウエア感染した端末から個人情報や企業情報を盗んでしまい、不正に悪用されてしまう可能性がある。本脅威を UTM で遮断することで、情報漏洩リスクが低減できたと考えられ、本実証の直接的成果と言える。

(8) UTM 機能別に対する昨年度との比較

・ 昨年度と今年度の実証において、アンチウイルス機能（AV）、不正侵入防止機能（IPS）、Web ガード（WG）機能で通信を遮断した件数脅威トップ 3 は以下のとおりである。また、昨年度および今年度において、黄色のセルは同じ脅威である。

表 5-18　UTM の AV 機能による昨年度との比較

順位（位）	昨年度	今年度
1	Trojan.MSOffice.SAgent.4	Trojan.Multi.Generic.4
2	Trojan.MSWord.Generic.4	Hacktool.MSOffice.Generic.3
3	Hacktool.MSOffice.Generic.3	Trojan.Script.Generic.a

・ アンチウイルス機能による全体の通信の遮断を通して、「Trojan」が付くトロイの木馬ウイルスがかなり多く見受けられる。その割合は、アンチウイルス機能による検知の 8 割を占めている。検知されているファイルの種類は、Word や Excel ファイルといった Office ファイルから PDF ファイルまで様々だが、令和元年度実証および今年度実証におけるセキュリティ脅威の主流の一つであると想定される。

・

表 5-19　UTM の IPS 機能による昨年度との比較

順位（位）	昨年度	今年度
1	SCAN SIPVicious User-Agent Detected	Cross Site Script attack
2	EXPLOIT Netcore Router Udp 53413 Backdoor	JSIG-WEB SQL-Union-ALL-Select-1
3	Cross Site Script attack	JSIG-WEB:SQL-Union-ALL-Select-3

・ 不正侵入防止機能による全体の通信の遮断を通して、「クロスサイトスクリプティング」に関係する攻撃がかなり多く見受けられる。その割合は、不正侵入防止機能による検知の 2 割を占めている。令和元年度実証および今年度実証におけるセキュリティ脅威の主流の一つであると想定される。

表 5-20　UTM の WG 機能による昨年度との比較

順位（位）	昨年度	今年度
1	visITmarrakech.es	infopicked.com
2	www.topsystem.jp	images2.imgbox.com
3	www.retail9ventures.com	eu.dspultra.com/api/submit_form_request

・ Web ガード機能においてトップ 3 に共通の脅威は見受けられなかった。今年度は Web ガード機能による全体の通信の遮断を通して、アドウエアに関係するサイトを用いた攻撃がかなり多く見受けられる。その割合は、Web ガード機能による検知の 5 割を占めている。アドウエア関連のサイトへ誘導し、ウイルス感染を試みる手法は、本実証事業におけるセキュリティ脅威の主流の一つであると想定される。

(9) まとめ（脅威の傾向）

・ 結論として、今年度も昨年度と同様に特定の企業が大量の脅威を検知したが、これは各企業が提供するサービスを狙ったものであることが確認された。そのため、外部に公開しているサービスを自社に持っている企業は特に地域や規模、業種に関わらず継続したセキュリティ対策を実施する必要がある。

・ 脅威の多少に関わらず昨年度も今年度も実証参加企業の約 70%が何らかの脅威を検知しており、大都市・非大都市のいずれの企業もセキュリティリスクにさらされていることに違いは無い。また、実証期間が短く、現在脅威が検知されていない企業も今後攻撃の対象になる可能性も十分考えられるため、継続的なセキュリティ対策が求められる。

(10) まとめ（規模の傾向）

・ 結論として、サイバー攻撃の脅威は大都市・非大都市では特定の事業所規模に依存すると判断できる明確な差異は見受けられなかった。令和元年度実証も今年度実証も事業所規模別参加比率に対する検知比率を確認したところ、突出した値ではない。実証期間や実証参加企業数などの実証の構成要素が異なる点も影響したと考えられる。

(11) まとめ（業種の傾向）

・ 結論として、サイバー攻撃の脅威は大都市・非大都市では特定の業種に依存すると判断できる明確な差異は見受けられなかった。令和元年度実証も今年度実証も業種別参加比率に対する検知比率を確認したところ、突出した値ではない。実証期間や実証参加企業数などの実証の構成要素が異なる点も影響したと考えられる。

(12) まとめ（全体）

・ サイバー攻撃の脅威は大都市と非大都市で傾向や業種、事業所規模に明確な差異は見受けられなかった。昨年度と今年度で、実証期間や実証参加企業数などの実証の構成要素が異なる点も影響したと考えられる。

・ しかし、攻撃者は企業のセキュリティ対策を待つこと無く、常に企業を狙っている。今年度の実証参加企業の 70%が何らかの脅威を検知しており、更に特定の企業で脅威が集中して検知された。この脅威の明確なきっかけは不明なため、いつ、どの企業においても脅威にさらされる可能性がある。そのため継続的にセキュリティ対策を行う必要がある。

・ また、世間一般的なトレンドとして Emotet が挙げられる。本実証において Emotet そのものは検知されなかったが、Emotet と攻撃パターンが類似する脅威（Word、Excel などの MS-Office で作成されたファイルを基点）を確認することができた。Emotet とは、標的のメールに関する情報を収集した上で、Word ファイルや Excel ファイルなどをなりすましメールで送付し、感染を拡大させるマルウエアのことを示す。UTM において無害化されていなかった場合、検知された企業に限らず、取引先やサプライチェーン含めて感染した可能性もあり、UTM の導入効果があった。

5.1.4 テレワークアンケートに係る考察

(1) 総評

・ 現状のテレワーク時のセキュリティ対策状況について、一部意識的に対策を講じている企業もあったが、重要情報の持ち出しポリシーやテレワーク環境が整備されていないままテレワークを実施している企業が多数であることが分かった。

・ テレワークツールの利用実績は、テレワーク申込企業の 17%（5 社）と非常に低い結果となったが、テレワークツールを使用した企業 3 社では持ち出し回数が 0 回になるなど、セキュリティ対策としての有効性は確認できた。

(2) セキュリティ脅威の実態把握

・ 実証開始時のテレワークの実施有無について、アンケート回答企業のうち、テレワークを 1 度でも利用したことがあると回答した企業は約 4 割強に止まった。現在もテレワークを実施していると回答した企業は 3 割以下であり、本実証参加企業ではテレワーク実施率が低いという結果となった。

・ 重要書類に対するセキュリティポリシーに関して、7 割の企業が重要書類は施錠されている場所に保管していると回答した。しかし、重要書類の持ち出し管理を行っていると回答した企業は約 3 割強に留まっている。そのうち、持ち出し管理の方法は約 7 割強が「専任者による管理」であった。以上の結果から、重要書類が担当者の一存で社外に持ち出されていることが多いと考えられる。重要書類に対してセキュリティ意識が十分でないと言わざるを得ず、書類の紛失・盗難による情報漏洩リスクについて啓発が必要である。

・ 重要電子データに対するセキュリティポリシーについては、アクセス管理を行っていると回答した企業は約 6 割弱であった。重要電子データの持ち出し管理をしていると回答した企業は約 3 割であり、そのうち専任者による管理が約 7 割、その他パスワードによるロック、上司への事前報告などの回答があった。このことから、電子データに対しては、書類へのセキュリティ意識より更に低く、改善が急務である。

・ テレワークを実施したことがある 17 社のうち、テレワークの実施場所について、自宅で行っていると回答した企業が 9 割弱（15 社）と最も多かった。また外出先の個室と回答した企業が 2 社、コワーキングスペースと回答した企業が 1 社で、多くは適した場所でテレワークを実施していることが分かった。一方で、個室以外の外出先でテレワークを実施していると回答した企業も 3 割弱（5 社）あり、作業時の背後や離席時などに情報を覗き見られる危険など、公共の場でのテレワーク実施は危険であることを注意喚起していかなければならない。

・ テレワーク時の回線については、自宅のインターネット回線を利用していると回答した企業が 9 割弱（15 社）と最も多かった。次いでポケット WiFi やスマートフォン（テザリング）などの携帯通信事業者の回線が 4 割強（7 社）であった。自宅の WiFi 環境は安全と考えられがちだが、通信経路の暗号化方式が適切（WPA2）であること、ファームウェアを最新の状態に保つことなど、考慮すべき事項が多いことは認識しておく必要がある。

・ 社内ネットワークへの接続方法については、VPN 接続利用や、既に別の画面転送型のテレワークツールを利用している企業もあり、一部のセキュリティ意識の高い企業ではテレワーク時のセキュリティ対策が進められている。一方で社内ネットワークに接続せずに、ローカル PC にデータを保存してテレワークを実施している企業も 3 割弱と少なくないことも明らかとなった。

・ テレワーク時に使用している端末について、約 7 割（12 社）が一般的な社給 PC を利用していると回答し、5 割強（9 社）が一般的な個人 PC、4 割強（7 社）がスマートフォン/タブレット端末を利用していると回答した。いずれもテレワーク端末にデータ保存が可能であり、データ保存不可であるシンクライアント端末を使用していると回答した企業は無かった。ローカル PC へのデータ保存は端末紛失時のリスクが最も高く、特に厳格なセキュリティ意識を持つことが必要になる。

・ テレワーク時に使用している端末のセキュリティ対策については、社有 PC を使用していると回答した企業のうち、12 社全社がウイルス対策ソフトを導入していると回答した。個人 PC を使用していると回答した 9 社についても、9 割弱（8 社）でウイルス対策ソフトを導入していると回答があり、PC へのウイルス対策ソフト導入は当たり前に行われていることが分かった。一方で、セキュリティパッチの適用は社給 PC 利用企業のうち 5 割（6 社）。個人 PC 利用企業では 2 割強（2 社）に止まっている。ウイルス対策ソフト導入に比べてセキュリティパッチ適用は実施率が低く、対策が急務である。

(3) テレワークツールの有効性

・ 実証期間が短かったこともあり、本実証で提供したテレワークツールを利用した企業はわずか 5 社に止まったが、テレワークツールを利用した 5 社のうち、3 社については実証期間中の重要情報持ち出しが 0 回と効果が見られた。数少ない事例ではあるが、テレワークツールがセキュリティ対策として有効であることが実証された。

・ テレワークツールを利用した企業のうち、残り 2 社は 5 回以下の持ち出しが発生している。持ち出しが発生した理由として、Zoom などの遠隔コミュニケーションツールが整備されていない企業では画面共有ができないなどのコミュニケーションの障壁が生じたことが挙げられる。また、テレワークツールを利用するよりも従来どおりデータを持ち出すことの方が容易なためとの回答もあり、セキュリティよりも業務優先ともとれる回答が見受けられた。テレワークを実施するにあたり、その他のツールの整備やセキュリティルールの整備、社員へのセキュリティ教育を行うことが課題として挙げられる。

・ テレワークツールを利用して良かった点について､｢重要情報を持ち出す機会が減った」と回答した企業が 3 社あり、その他に「出社して作業を行うのとそん色が無かった」とテレワークツールを評価する声や、「感染リスクを減らすことができた」という新型コロナ対策として効果があったという意見も見られた。またテレワークツールを使用した 5 社のうち、4 社は「テレワークツールにセキュリティ不安は感じない」と回答し、1 社は「便利すぎるがゆえに不安もあった」と回答があった。

・ テレワークツールを申し込んだが、実証期間中にテレワークツールを利用しなかった企業にテレワーク実証に申し込んだ理由をアンケートしたところ、「テレワークツールに興味があった」が 7 割と最多回答であり、次いで「緊急事態宣言以前から自社へテレワーク導入の必要性を感じていた」が 2 割強の回答があった。このことからテレワークツールに対する関心がある企業は多いと推測できる。

・ しかし、テレワークツールを利用しなかった理由としては、「実証期間中にテレワークで実施できる作業が発生しなかった」、「業務が多忙のため使う時間が取れなかった」という回答が多く､その他として､｢テレワークに必要な周辺準備ができていなかった」、「テレワークツールの使用方法が難しかった」という回答もあった。関心はあるが業務多忙のためテレワークの導入は後回しになっている企業が多いものと思われる。また、テレワークツールの使用方法が難しいとの意見について、テレワークツールの仕組みをより分かりやすく説明した上で、普及を進めることも必要と思われる。

・ 実証終了後に全実証参加企業向けに with コロナ時代に対応するためにテレワークが必要かアンケートを行ったところ、2 割が「必要（導入済み）」、3 割強が「必要（将来的に導入予定）」と回答した。一方で、テレワークの導入が「不要」と回答した企業は 4 割を上った。理由として「職種がテレワークに合わない」、「現場作業が必要なため」という回答があった。これについて、実証参加企業では、製造業やサービス業の企業の参加が多く、工場などの現場作業やお客様への対面での接客をメインとしている企業ではテレワークを今後も導入しないと考えている企業が多いことが分かる。また、「少人数のため」、「出勤が可能だから」がと言う理由も見られた。これについては、実証期間中の 10 月～12 月の対象 3 県では、新型コロナウイルスの日別感染者数拡大がなだらかであり、非大都市の中小企業では、新型コロナウイルス対策としてのテレワークの緊急性が下がっていることが分かる。しかし、2020 年末から全国的に新型コロナウイルスの感染が急拡大していることからも、テレワークの必要性が再度高まるのではないかと考えられる。

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

5.2.1 実証参加企業の募集に係る考察（地域展開窓口との連携に係る考察を含む）

・ 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を考察するにあたっては、それ以前の問題として、中小企業においてセキュリティの意識が高まっていることが前提となるし、セキュリティ対策サービスの存在自体が“人口に膾炙する”存在となる必要性がある。よって実証参加企業にせよ、商用サービスのユーザー企業にせよ、いかに意識を高め、心を開いてもらった上で、いかに効果的に周知を行っていくかがカギとなる。ここでは、今後、商用サービスの拡販も見据え、本実証事業での募集手法と募集結果につき考察する。

・ 本実証事業の主要な目的の一つである各地商工会議所・商工会（連合会）や地域金融機関、地域有力企業などとの連携（今後の商用サービスの拡販結節点候補としての地域展開窓口との連携）については、表 2-1 のとおりの結果となった。

・ 募集手法を「人」を介した「個別打診（一本釣り）」と、「広報媒体（チラシ・メール・ウエブ・メディアなど）」を通じた「広報」に大別すると、本実証事業においては前者が 62%、後者が 28%であった。一方、大阪商工会議所の地元エリアを対象に行った令和元年度実証ではその比率（分類法がやや異なるのが）は前者が 44%、後者が 56%であった。この比較によると、令和 2 年度実証の滋賀・奈良・和歌山にあっては、広報的手法よりも個別打診の方が主体であったことが分かる。特に「地域展開窓口の個別打診」「お助け実働隊地域 IT 事業者の個別打診」だけで 35%を占めている。

・ これは、滋賀・奈良・和歌山では県の面積が広く、各都市が散在していることにより、広報の効率、浸透率が悪いこと（とりわけ大阪商工会議所にとってそれら地域は完全な“アウェイゲーム”であるため広報のパス自体が僅少であった）、また、地方においては、人的繋がりが重要であることなどによるものと推察される。

・ 大阪商工会議所の滋賀・奈良・和歌山の会員企業（市外特別会員）の一部、および 3 県のプライバシーマーク取得企業の一部に対し、チラシなどを事前に送付した上でテレマーケティングを行った結果、奏効率は 3%であった。令和元年度実証もごく少数の特定母集団に対しテレマーケティングを行いその奏効率は 4%であったので大差は無い。

・ 各地商工会議所・商工会でのチラシの会報同梱・配架などの奏効率は 0.06%、各地地域金融機関でのチラシ配架の奏効率は 0.05%であった。一方、チラシ（単独）直送の奏効率は 0.1%（各地商工会議所会員企業）～0.16%（大阪商工会議所独自収集母集団）であり、チラシの場合、同梱・配架よりも単独直送の方が約 2 倍効果が高かった。なお、チラシは封書で送付するのではなく、厚紙に印刷しそれ自体を郵便物として裸で送付（表面上部にあて先を印字)する形式としたため､開封率というバリアを未然にクリアした。

・ 奏効率では優れている直送案内方式の課題は、いかにあて名情報を取得するかという点にある。この点、今回は国の実証事業として実施したため、各地商工会議所・商工会からの提供を受けることができた（各地商工会議所・商工会も本実証事業の協力につき稟議の上、機関決定しているケースが多いと考えられる）が、商用サービスに移行しても同じように情報提供協力が得られるかどうかは未知数である。そのため、商用サービス移行後も各地商工会議所・商工会には地域展開窓口として主体的に関わってもらう必要があり、その動機付けは、事業収入（販売手数料）というよりは、中小企業のサイバーセキュリティの重要性に対する意識の如何であると考えられる。

・ 最後に、実証事業参加寄与率の 6%のうち以下のような例もあった。①お助け隊実証に係る経済産業省の取り組みに関する日本経済新聞の記事を見て応募した企業、②SECURITY ACTION 登録企業向けの IPA のメルマガを見て応募した企業、③令和 2 年度実証の他の請負主体である名古屋商工会議所のお助け隊実証の情報を得て応募した企業。これらの存在も大変重要であり、マスメディアを通じた国策の周知広報や意識向上、我が国の情報セキュリティの総本山とも言える IPA 自体による広報、そして、お助け隊実証が 2 年越しに行われ延べ 23 地域・産業分野で実施されたことに伴う“全国的な広がりと機運醸成と相乗効果”の成果と言えよう。要するに、各事業主体がその限られたリソースを精一杯用いて各々単独で“竹槍戦術”のごとく広報・啓発していても一向に埒が明かず、とてもじゃないが国家を背景とするような攻撃者から中小企業を守れるはずも無く、国および IPA が強いリーダシップを発揮し、各事業主体が緊密に連携して、官民そして産業全体（大企業・中小企業）で一丸となってサイバーセキュリティの普及を行っていくべきであると言えよう。その意味でも「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）」の一刻も早い実質的活動開始が期待されるところである。

5.2.2 実証参加企業の IT リテラシーの課題に係る考察

(1) UTM 自社設置率から推定する滋賀・奈良・和歌山の中小企業の IT リテラシー

・ 先述のとおり、本実証事業において、UTM の自社設置率は 54%であり、令和元年度実証（大阪・京都・兵庫）の自社設置率 69%と比較して（UTM が両実証で同じものであるにもかかわらず）15%低い。

・ この要因として（事務局によるお助け実働隊地域 IT 事業者の訪問設置支援の積極的案内を勘案したとしても）、滋賀・奈良・和歌山の中小企業などが大阪・京都・兵庫に比べて、ネットワーク構成図の有無、ネットワーク環境のブラックボックスぶり、担当者（専任・兼任）の有無やその IT リテラシーなどの点で、やや心許ない状態にあることが仮説として浮上する。ネットワークのブラックボックスぶりや担当者の IT リテラシーなどは定量的に調査していないので正確なところは分からないため、別の視点で下記のとおり考察を続ける。

(2) お助け実働隊地域 IT 事業者による簡易 UTM 設置支援

・ 下記はお助け実働隊地域 IT 事業者にとっての UTM 設置難易度を、令和元年度実証、令和 2 年度実証にわたり定点観測したアンケート調査したものである。UTM は両実証で同じものである。またお助け実働隊地域 IT 事業者のレベルもほぼ同じと考えられる。

表 5-21　お助け実働隊地域 IT 事業者にとっての UTM 設置難易度

お助け実働隊地域 IT 事業者にとっての UTM 設置の難易度				
		令和 2 年度実証 滋賀・奈良・和歌山		令和元年度実証 大阪・京都・兵庫
UTM の設置場所	分かりやすかった	17（77%）		84%
	分かりにくかった	5（23%）	＞	16%
UTM の設置設定の難易度	容易だった	14（64%）		69%
	困難だった	8（36%）	＞	31%

・ 本表から読み取れるお助け実働隊地域 IT 事業者の感想も勘案すると、滋賀・奈良・和歌山の方が、大阪・京都・兵庫より、設置位置、設置・設定ともに若干ではあるが難易度が高い。有意差とまでは言えないかもしれないが、滋賀・奈良・和歌山においては、ネットワーク構成図の有無、ネットワーク環境のブラックボックスぶり、担当者（専任・兼任）の有無やその IT リテラシーなどの面で、大阪・京都・兵庫より若干心許ないところがあると言えるかもしれない。

5.2.3 実証参加企業のサイバーセキュリティ意識の課題に係る考察

・ 中小企業のサイバーセキュリティに係る意識を定量的に把握することは困難である。何か別の切り口や指標によって間接的に伺い知るしか方法がなかろう。本実証事業では、UTM が観測した「自社へのサイバー攻撃に対する印象」を聞いたところ、下記のとおりの反応であった。

表 5-22　自社へのサイバー攻撃に対する印象

UTM が検知した（アラートメールでお知らせした） 自社へのサイバー攻撃に対する印象 n=53		
自社への サイバー攻撃の量	想像以上に多かった	8（15%）※最小
	想像していた程度だった	11（21%）
	想像していたほどは多くなかった	18（34%）※最大
	無回答	16（30%）
自社への サイバー攻撃の質	想像以上に酷かった	1（2%）※最小
	想像していた程度だった	14（26%）
	想像していたほどは酷くなかった	20（38%）※最大
	無回答	18（34%）

・ 本集計結果についての論評は難しいが、「想像以上に多かった」「想像以上に酷かった」と回答した割合がいずれも最小であり、「想像していたほどは多くなかった」「想像していたほどは酷くなかった」と回答した割合がいずれも最大であった。

・ 本実証に参加し UTM を設置したことに伴い、良くも悪くもサイバー攻撃の実態（と言っても網羅的でも 100%でもなく、極めて短期間でもあるが）が、警戒を促す方向ではなく、安心（もしくは軽視）する方向に“見える化”されてしまった感が否めない。

・ 本実証事業は令和元年度実証に比して実証期間自体が短く、実際のところ、表 4-4 のとおり、「アラート通知メールが来なかった」のも 15 社（28%）あった（アラート通知メールの着信に気付いていないケースを含む）ため、攻撃の量を「想像していたほどは多くなかった」と 18 社（34%）が感じても至極当然の受け止め方と言えよう。

・ 実証が始まった 9 月の時点では UTM の設置がほとんど進んでおらず、多くの実証参加企業が 10 月中旬～11 月中旬にかけて UTM を設置した。もし仮に実証がもう 1～2 ヶ月早くスタートしていたとしたら、「Emotet」が猛威を振るった令和 2 年 7 月後半から 10 月初旬に UTM がその攻撃を検知・防御する体験をすることができたものと思われる。また、皮肉なことに「IcedID」のごとき原理的に UTM を通過する圧縮ファイル型のサイバー攻撃が増えたのも本実証事業たけなわの時期であり、本実証を通じて UTM の効果実感することや、サイバーセキュリティ意識を大きく高める効果は、一定程度、見られたものの、限定的であったと言わざるを得ない。

5.2.4 簡易型保険などを通じた中小企業のサイバーセキュリティの普及向上に係る考察

(1) 現状の課題

・ 実証参加の 53 社のうち 6 社（約 11%）が商用化サービスの採用意思を示したアンケート結果を踏まえると、企業のサイバーリスク対策への認識・優先順位は依然として高いとは言い難い実態があるものと考えられる。他方で、サイバーインシデントが発生する可能性は UTM による検知結果が示すとおり、依然高い水準となっている。これらを踏まえると、簡易型保険の上乗せ保険（サイバーリスク保険）を届けるプロセス（損害保険会社・保険代理店による中小企業訪問活動）の中に中小企業にとっての BCP の観点においても、中小企業のサイバーセキュリティへの危機認識を同時に高めるプロセスを含むことが一層必要になってくる。

（参考）

商工会議所とは経営相談事業の一環である会員事業者への BCP 策定支援としてワークショップの開催支援、ビジネス総合保険制度の加入促進と合わせ BCP 策定支援を行っている。これらは会員事業者の経営基盤強化とともに政府の防災基本計画に掲げる「企業防災の促進」にも資する。但し、現実的には、一部を除いて BCP、サイバーセキュリティ、サイバーリスク保険に造詣のある保険代理店は極めて少ないのが実情であり、そのような人材の育成が急務である。

(2) 今後の対応

・ まず、令和元年度実証では、中小企業におけるサイバーセキュリティ・サイバーリスクに関する意識の低さやサイバー保険料水準の高さを踏まえて、中小企業向けには段階的に保険の必要性を訴求していくことが必要と考え、まずはインシデントへの対処を促す簡易的な補償を提供し、次に一般的なサイバーリスクに関する保険のニーズを高めていくことが必要との仮説に至った。

・ 次に、令和 2 年度実証では、中小企業のリモート環境を考慮しつつ、損害保険会社および保険代理店のリスクソリューション（サイバーリスク保険を含めた総括的な BCP コンサル）の提供の一環として、お助け隊サービスを届けるためのツール整備や奈良、滋賀、和歌山の社員代理店向けの勉強会を開始しており、令和 2 年度実証参加の中小企業に、保険代理店が商用化サービスの加入勧奨を担っていく予定である。しかしながら、保険代理店訪問による商用化サービスの加入勧奨については、緊急事態宣言の状況を踏まえた慎重な対応が必要となり、当面は実施困難な状況にある。

（参考）令和元年度実証終了段階の保険を通じたサイバーセキュリティ普及のシナリオ

ステップ1：

実証参加企業全社に対し、インシデント発生時に5万円程度の補償を提供し、簡易処置・診断を提供することで、サイバー攻撃に対する初動対応の重要性を理解させ、万が一の際の被害について考えさせるという“行動変容”を促す。

→保険機能として、実証参加企業間で薄く広くリスク分担する仕組み（補償）を構築する。

ステップ2：

ステップ1の簡易処置・診断を通じて「重大事案」の発生を早期に検知し、真に対応が必要な場合に本格的な対処（フォレンジックなど）へと繋げる仕組みを構築。本格的な対処には数百万円から数千万円の費用負担が必要となり、加えて賠償リスク（サプライチェーンへの影響）の懸念も早期に顕在化することから、各自がオプション（任意）でも保険に加入し、簡易的な保険だけでは対応できない対処費用や損害賠償責任に備えられる仕組みを構築する。

→既存の中小企業向けサイバーリスクを補償する保険へ誘導

5.2.5 相談窓口に係る考察

- **回答時間の短縮**
  即答できない事象は NEC へエスカレーションをし回答を行ったが、事象によっては実証参加企業へ追加ヒアリングが必要となり、確認に時間を要したケースもあった。実証で得た事例をナレッジ化することで回答時間の短縮を図り、窓口に対する CS 向上に繋げる必要がある。

- **リモート対応活用**
  今回の実証では、ネットワーク環境や固定 IP アドレスの把握にリモートが活用され、お客様の正確なネットワーク環境や設定情報の確認に有効であった。迅速に対応を行うため、トラブル対応やインシデント対応に対して、積極的にリモート提案を行う必要がある。

- **分かりやすさ・伝わりやすさ・聞きやすさ**
  中小企業の担当者の中には ICT・セキュリティ分野のリテラシーが高くない方もいるため、トラブルの状況を正確に伝えられない可能性がある。その場合でも、窓口では少ない情報から発生状況を正確に把握し、なおかつ「専門用語」を使わずに、できるだけ噛み砕いた言葉で説明やサポートを行い、企業担当者へのストレスをかけない窓口対応を目指す。

- **よろず相談**
  今回実証では UTM 設置やインシデント対応に関する相談だけではなく、PC やタブレッド端末、プリンタのトラブルなどについても相談を受けている。相談内容により簡単なアドバイスや、メーカーやプロバイダへの誘導を行っている。専属のサポート契約が無く、どこに問合せをして言いか分からない中小企業ユーザーに対しては、相談ができる窓口があることで不安を取り除く役割を担える。

5.2.6 テレワーク利用効果と課題に係る考察

- **テレワークルールやテレワーク環境整備が不十分**

  重要情報の持ち出しポリシーやテレワーク環境が整備されていないままテレワークを実施している企業が多数であり、本実証開始前の仮説どおりセキュリティ対策まで考慮できずにテレワークを始めた中小企業が多いという課題が浮き彫りになった。テレワークに関するルールを策定し、社員へのセキュリティ教育を行った上でテレワークを行っていくことが望まれる。

  特に、テレワーク実施時の端末セキュリティが不十分の企業が目立つ。アンケート回答企業全社が、社給、私有に関わらずデータ保存可の端末を使用しており、端末にデータを保存してテレワークを実施している企業も少なくないことが分かった。持ち出し管理を徹底していない企業で、データを保存した端末の紛失や盗難があった場合は情報漏洩に直結するため、持ち出しを発生させないテレワークの仕組みを構築していくことは継続課題として挙げられる。

- **テレワークツールのニーズが少ない**

  一方で、本実証参加企業ではテレワークツールのニーズが少ないことが明らかになった。中小企業では現場作業を行っていることや、対面での接客が必要なためにテレワークを導入できない業種・職種も多い。更に、テレワークに関心があっても業務優先となり、導入が進まないという課題があることも分かった。中小企業でテレワークが可能な業務について、引き続き調査をした上でテレワークツールの商用サービス導入を検討する必要があると考える。

5.2.7 簡易セキュリティ診断結果から見える課題に係る考察

- **情報セキュリティに関する脅威や攻撃に関する情報収集が実施できていない**
  情報セキュリティに関するルールの策定や運用が実施できていない
  情報セキュリティ対策の検討を行う上では、情報セキュリティに関するある程度の知識や情報が必要不可欠である。しかし、非都市部の中小企業も大都市部の中小企業と同様に、情報システム部門や専任担当者を置くことができない、もしくは兼任者が片手間で対応しているのが実態であり、情報セキュリティ対策が後回しになっていることが考えられる。また、ルールの策定や情報収集は、組織が能動的に取り組む必要があり、形になるまでには相応の時間を要する点も導入の妨げになっていると考えている。

- **私物の媒体や PC/スマートフォンを利用する際のセキュリティ対策が不十分**
  理想としては、私物の媒体や PC/スマートフォンの業務利用は禁止することが望ましいが、事業所規模が小さい企業は限られた IT リソースの中で業務を遂行している可能性があり、リモートワークを行う際には、私物を使用せざるを得ない企業も存在していると推察する。その場合は、私物に対するセキュリティ対策は必須となり、情報紛失や情報漏洩対策を行う必要がある。

- **情報セキュリティに関する知識を持った人材が少ない**
  情報セキュリティ対策を組織として機能させるためには、組織内に有識者がいることが望ましい。
  令和元年度の実証結果から立ち上げた「サイバーセキュリティお助け隊サービス」の提供により、「問合せ窓口」や「駆け付け対応」といった分野では「情報システム部門や専任担当者」の役割を支援できているが、「ルール策定」といった分野の役割はカバーできていない。
  IPA から啓発されている「中小企業の情報セキュリティ対策ガイドライン」にも雛形やサンプルが公開されているが、情報セキュリティに対する人材が不足している中小企業にとっては、汎用的に作成された雛形では活用が困難である可能性があり、「ルール策定」を支援する対策が必要と考えられる。

5.3 中小企業において必要なセキュリティ対策

5.3.1 発注元大企業などが取引先中小企業に求めるサイバーセキュリティ対策に係る考察

・ 実証参加企業と日頃からメールなどで情報のやり取りをしている発注元大企業、持株会社、業界の結節点的組織が、実証参加企業を含む取引先中小企業などに求めるサイバーセキュリティ対策の優先順位や実施レベルなどは下記のとおりであった。

表 5-23　発注元大企業などが取引先中小企業に求めるサイバーセキュリティ対策

		発注元大企業			持株会社	業界の結節点的組織	
		A社	B社	C社	D社	E社	F社
取引先などのサイバーセキュリティやサイバー攻撃の状況を把握しているか		担当者もあまり把握していない	担当者が概ね把握	（無回答）	担当者もあまり把握していない	担当者もあまり把握していない	担当者もあまり把握していない
取引先などのサイバーセキュリティの対策	早急に求めたい・実施したいこと	口頭や文書での注意喚起	口頭や文書での注意喚起、社内規定の整備・社員教育訓練の実施、セキュリティ契約の締結、セキュリティ診断の実施	社内規定の整備・社員教育訓練の実施	ない	（無回答）	口頭や文書での注意喚起、セキュリティ契約の締結
	今後ぜひ求めていきたい・実施していきたいこと	口頭や文書での注意喚起	サイバー保険加入、SECURITY ACTION 自己宣言、代三者認証の取得、情報システム担当者の配置	実態把握のためのセキュリティ診断の実施、SECURITY ACTION 自己宣言	セキュリティ契約の締結、自社セキュリティ基準の採用・準拠	SECURITY ACTION 自己宣言	実態把握のためのセキュリティ診断の実施、サイバー保険加入、自社セキュリティ基準の採用・準拠
	今後できれば求めていきたい・実施していきたいこと	口頭や文書での注意喚起、情報システム担当者の配置	自社セキュリティ基準の採用・準拠	第三者認証の取得	SECURITY ACTION の自己宣言、第三者認証の取得	（無回答）	社内規定の整備・社員教育訓練の実施
取引先などのサイバーセキュリティのツール	早急に求めたい・実施したいこと	ファイルの暗号化・パスワード設定・バックアップ	端末のウイルス対策ソフト、端末の EDR、出入口のファイアウオール、出入口の UTM、ファイルの暗号化・パスワード設定・バックアップ	端末のウイルス対策ソフト、出入口のファイアウオール、ファイルの暗号化・パスワード設定・バックアップ	端末でのウイルス対策ソフト	（無回答）	端末のウイルス対策ソフト、端末の EDR、出入口のファイアウオール
	今後ぜひ求めていきたい・実施していきたいこと	端末のウイルス対策ソフト	SOC（遠隔監視）サービス、駆け付けサービス、安全なテレワークツール	出入口の UTM、安全なテレワークツール	ない	端末のウイルス対策ソフト、出入口のファイアウオール	出入口の UTM、ファイルの暗号化・パスワード設定・バックアップ、安全なテレワークツール
	今後できれば求めていきたい・実施していきたいこと	端末のウイルス対策ソフト	（無回答）	SOC（遠隔監視）サービス	端末の EDR、出入口のファイアウオール、出入口の UTM、SOC（遠隔監視）サービス、駆け付けサービス	（無回答）	SOC（遠隔監視）サービス
取引先などのサイバーセキュリティに今後求めていきたいが足枷となる点		取引先などに求める事項や明確な基準が分からない	特に無い	取引先などの意識が低い、取引先などに求める事項や明確な基準が分からない	取引先などの意識が低い、取引先などの IT 力が低い、取引先などの資金力が低い、取引先に人材がいない、取引先などに求める立場にない	特に無い	取引先などの IT 力が低い、取引先などの資金力が低い、取引先などに人材がいない
取引先などがサイバー攻撃被害を受けその被害が貴社にも及ん	過去の貴社の対処	どういう対処になるか分からない	（無回答）	（無回答）	何も求めなかった（Emotet による不審メール）	（無回答）	何も求めなかった
	今後の貴社の対処	どういう対処になるか分からない	損害賠償請求	損害賠償請求	取引停止	再発防止に向けた改善	何も求めない、損害賠償請求、取引停止

だ場合							

・ 「取引先などのサイバーセキュリティやサイバー攻撃の状況の把握」の状況については、多くが「担当者もあまり把握していない」と回答しており、サプライチェーンでのサイバーセキュリティ対策の難しさが浮き彫りになった。

・ 「取引先などに求めるサイバーセキュリティ対策」の優先度・実施レベルとしては、「早急に求めたい」こととして「口頭や文書での注意喚起」「セキュリティ契約の締結」「セキュリティ診断の実施」など、窓口担当者が事務レベルで経費をかけずに即刻実行できるような対策が並ぶ。「今後ぜひ求めたい」「今後できれば求めたい」こととしては、「SECURITY ACTION の自己宣言」「自社セキュリティ基準の採用・準拠」「社内規定の整備・社員教育訓練の実施」などのように全社的対応が必要で少々時間の要する対策が挙げられている。

・ 「取引先などに求めるサイバーセキュリティのツール」の優先度・実施レベルとしては、「早急に求めたい」こととして、「端末でのウイルス対策ソフト」「出入口でのファイアウオール」「ファイルの暗号化・パスワード設定・バックアップ」など、既存のパソコンやルーターなどで対応できることが挙げられているほか、「端末での EDR」を求める企業などもあり、攻撃の巧妙化、未知の脅威の増加などを踏まえたものと思われる。「今後ぜひ求めたい」「今後できれば求めたい」こととしては、「出入口での UTM」「SOC（遠隔監視）サービス」「駆け付けサービス」など、別途セキュリティ機器の手配や IT ベンダーなどとの契約が必要となるものが比較的多い。こうしたプラスαの技術的対策を、個別に吟味し、発注し、支払いし、運用し、資産管理していくのは中小企業にとっては大変であることから、「サイバーセキュリティお助け隊」などのパッケージサービスが課題解決の有効な選択肢となろう。

・ 「取引先などのサイバーセキュリティに今後求めていきたいが足枷となる点」は、「取引先などの意識が低い」「取引先などの IT 力が低い」などが挙げられている。こうした課題に対しては各地商工会議所・商工会が地域ごとに中小企業などにサイバーセキュリティセミナーや小規模事業者経営改善資金融資などを粘り強く継続的に行うことにより支援していくほかない。また「取引先などの資金力が低い」「取引先に人材がいない」といった課題に対しては、サイバーセキュリティお助け隊実証事業など「公助」によるイニシアティブのもと、各コンソーシアムが地域ごとに支援体制を構築し「共助」の仕組みを整備するとともに、実証を通じて事業化した安価・簡便なセキュリティサービスを実用化することにより、中小企業による「自助」を後押しすることが必要となろう。更には、「取引先などに求める事項や明確な基準が分からない」といった課題に対しては、大企業と中小企業がサイバーセキュリティに関して情報共有や相互連携する場を設け、産業分野にとらわれない（あるいは産業分野ごとに）サイバーセキュリティ対策に係る基準・行動指針・規定の雛形のようなものを作成・普及していくことが有効であり、そうした活動を有効に進める上でも、令和 2 年 11 月に設立された「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）」には大いに期待を寄せたいところである。

・ 「取引先など（中小企業）がサイバー攻撃被害を受けその被害が貴社（発注元大企業など）にも及んだ場合の貴社の対処」は、あくまで案件内容や相手先によってその対処内容は異なるものと思われるが、本アンケートの回答は、「何も求めない」という心許ない対応と、「損害賠償請求」「取引停止」も辞さないという劇薬的な対処とに二分され、いずれも中小企業にとっては看過できない反応と言える。「損害賠償請求」や「取引停止」に対しては、サイバー保険、しかも費用保険といった簡易保険ではなく、本格的な賠償保険により対応するほかなく、また「再発防止に向けた改善」に関しても、フォレンジック調査などに対応できるようなサイバー保険への加入が何より重要であることが伺われる。

5.3.2 アンケートから浮かび上がった中小企業において必要と考えられるセキュリティに係る考察

・ 滋賀・奈良・和歌山と京阪神の地域差……ほとんど有意差は見られなかった。
・ 昨年度と今年度の経年差……ほとんど有意差は見られなかった。
・ 滋賀・奈良・和歌山の地域差……ほとんど有意差は見られなかった。

・ 滋賀・奈良・和歌山ならびに京阪神の中小企業において必要と考えられるセキュリティに係るキーワードは下記のとおり総括できよう。

① 攻撃・被害の「見える化」と社員の意識向上につき大幅な改善が必要であること
② ゼロ情シスが多く、マニュアルも無く、人材・時間が圧倒的に不足していること
③ 金銭的に「年 10 万円の壁」を超えられないこと
④ テレワーク不実施の不動の理由あり、テレワークを実施しないことでテレワーク起因のサイバーインシデントリスクも必ずしも高くなく、対策ニーズも低いこと
⑤ サプライチェーンでの取り組み進展が鈍いこと
⑥ 相談や初動対処へのニーズは比較的高いこと

5.3.3 所定サイバーインシデント初動対処（「駆け付けお助け」「リモートお助け」）に係る考察

(1)「駆け付けお助け」に係る考察

・ 本案件は「Web ガード」の有害サイトアクセス検知に伴う★★アラートメールであり、通常、所定サイバーインシデント初動対処の対象となる★★★アラートメールより深刻度は低いものの、政策的見地から対処を行うこととし、大阪商工会議所から実証参加企業に「駆け付けお助け」と「リモートお助け」のいずれを希望するか確認した。その結果、「リモートお助け」では対応できないとのことだったので「駆け付けお助け」を実施した。

・ 「駆け付けお助け」はアラートメール発報の 7 日後に実施した。これは、令和元年度実証において、「駆け付けお助け」当日中に行われたのが 38%、数日中が 38%だったことと比較すると、やや対応が遅いが、深刻度があまり高くなかったこと、実証参加企業側の意識がさほど高くなかったことなどによるものである。

・ 駆け付け先となった同企業の所在地は、京阪神の大都市圏のような都会ではないものの、県の中でも比較的大きな市の、しかも鉄道駅から徒歩圏内（山間部などではなく市街地中心部）であり、駆け付けを行ったお助け実働隊地域 IT 事業者も同じ県内の事業者であり、来訪が困難だったわけでもない（片道 60 分）ことから、「7 日後」という遅めの対応となった原因に地理的条件は考慮する必要は無い。

・ 本案件の場合、UTM が検知した IP アドレス、MAC アドレスの端末が見つからなかった。その後、社員が社長私有のタブレットの存在を示唆した。しかしながら、アラートに係る通信の時刻は深夜であり、当該タブレットは社内には無かったはずである点も指摘された。ところが社長の自宅は社屋に隣接しており、自宅からの通信を無線 LAN ルーター経由で UTM が検知したものと推定した。そこで社長にタブレット持参を依頼し、確認したところ、MAC アドレス、IP アドレスともに一致し、被疑端末が特定された。

・ 同タブレットにはウイルス対策ソフトが入っていないことが判明。無料版のウイルス対策ソフトをインストールしようとしたが、お助け実働隊地域 IT 事業者がタブレット端末の取り扱いに慣れていなかったため時間を要し、結果的に全体で 120 分を要した。

・ 以上のことから、本案件においては、①シャドーIT（IT 資産管理）の問題（令和元年度実証でも課題となった）、②シャドーIT が経営層の私有のものである場合には対処にあたり色々な意味で慎重さを要すること、③無線接続のタブレット端末の場合は所定サイバーインシデント初動対処時に当該端末が対処現場に存在していないケースも想定されること（被疑端末が特定・現認できないリスク）、④端末にウイルス対策ソフトが入っていないこと（定義ファイルの最新化以前の問題）、⑤お助け実働隊地域 IT 事業者がタブレット端末の扱いに不慣れであるケースも想定されること、などの課題が浮かび上がった。とりわけ②～⑤は令和 2 年度実証により新たに得た課題意識である。

(2)「リモートお助け」に係る考察

・ まずもって、本案件はUTM設置のわずか5日後に発生したことが特筆すべき点である。よって、UTM 設置（実証参加）前からマルウエアに感染していた可能性が高く、本実証事業を機にいち早く課題解決に繋がった点は、実証参加企業側にとってもセキュリティ上、良かったことであるし、本実証事業の実施意義という点からも大きな成果と言える。

・ 本案件は、マルウエア感染の疑いのある通信を「IPS」にて検知したものであり、深刻度は★★アラートメール相当であった。通常、所定サイバーインシデント初動対処の対象となる★★★アラートメールより深刻度は相対的に低いものの、実証参加企業側の意識が高く、実証参加企業側の希望により、お助け実働隊地域IT事業者による所定サイバーインシデント初動対処の実施となった。

・ 相談を受けたお助け実働隊地域IT事業者が「リモートお助け」と「駆け付けお助け」の両手法を提示したところ、当該お助け実働隊地域IT事業者が、実証参加企業の所在する県内ではなく隣県に事業所を構える事業者であったこともあり、また、実証参加企業側は本案件を比較的深刻な案件と受け止めたこともあり、「リモートお助け」を実施することとなった。

・ 「リモートお助け」はアラートメール発報の翌日（金曜日）に開始され、専ら電話により、ウイルス対策ソフトによるウイルスの検知および駆除を実証参加企業側に指示する形で行われた。お助け実働隊地域IT事業者がリモートデスクトップなどでPCを遠隔操作することや遠隔コミュニケーションツールなどでリアルタイムで支援をする手法は用いず、主に実証参加企業がキャプチャ撮影した画像をメール送信し、その画像を見て次の指示をする手法で初動対処が行われた。ウイルス対策ソフトは定義ファイルの最新化からスタートしたこともあり全体としてはかなり時間を要することになった。またフルスキャンには更に長時間を要することが予見されたため、一旦支援は打ち切り、フルスキャンは翌営業日（土日を挟み月曜日）に支援することとなった。

・ 翌営業日である月曜日の午前に、お助け実働隊地域 IT 事業者が実証参加企業からフルスキャン結果のキャプチャ画像をメール受信し、それを見ながら駆除作業を電話で指示し、駆除が終了したのが同日の夕方。その後の安全確認作業などは更にその翌日の火曜日までおよび、evtxファイルなどのエビデンス取得を経て、支援が完全に終了したのは、更にその翌日の水曜日となった。クローズまで足掛け 5～6 日を要したことになる。なお、実際にお助け実働隊地域IT事業者が支援に携わった時間の合計は235分間である。

・ この「リモートお助け」につき、お助け実働隊地域IT事業者側は、作業時間短縮に効果があったと感じており、もし仮に「駆け付けお助け」を実施していたら、移動だけで240分、現地作業400分を要していただろうと推定している。現地作業は、一般的にはフルスキャンが一番時間を要するものであり、この時間は、お助け実働隊地域IT事業者にとっても、実証参加企業側にとっても手持ち無沙汰な時間となる。この時間の節減には「リモートお助け」は有効と言えよう。また、対処実績が多い頻出のマルウエア駆除には「リモートお助け」は一定の有効性を持つだろう。

・ 本案件の場合、幸いなことに、電話で対応できる範囲内であった。しかし、現地でのネットワーク接続状況の確認を要する場合や、コマンド操作（CLI）やブラウザ操作（GUI）とその結果確認を行う必要がある場合などは、電話では上手くできない可能性がある。また被害の及んでいる範囲などの調査は事実上困難だろう。

・ また対応可能な範囲内のインシデントであったとしても、お助け実働隊地域 IT 事業者側としては、①利用者にやってほしいことが伝わらない点、②試したいことをすぐに試せない点、③電話代をかなり要する点、④作業日が複数日に分割される点などが限界点であると指摘している。

・ 本案件の場合、ウイルス対策ソフトの定義ファイルを最新化してからすぐにフルスキャンを実施したのではなく、土日を挟んで 3 日後にフルスキャンを実施している。この 3 日間の間にマルウエアが悪性通信を続けることや、LAN 内に感染拡大をするリスクもある。ランサムウエアの場合、一刻も早い駆除が望ましかろう。一方で UTM が不審なアウトバウンド通信をブロックするため数日程度であれば、フルスキャンを先延ばしにしても、外部の C&C サーバーのごとき悪性サイトへの情報などの送信は防ぐことはできる。この点、UTM の有無も初動対処の手法や迅速さに関係するため、総合的な観点から対処方法が決定される必要性がある。

・ 実証参加企業側は、本案件に係る「リモートお助け」に対し、初動対処が早かった点では評価をしているものの、情報伝達に時間がかかる点を課題として挙げており、総合的には「リモートお助け」を今後は使いたくない、と回答している。

(3) 所定サイバーインシデント初動対処を受けた実証参加企業の反応

・ 実証参加企業側は、「リモートお助け」を受けた企業も「駆け付けお助け」を受けた企業も、お助け実働隊地域 IT 事業者による初動対処を受けたことで「社員のセキュリティ意識に変化があった」と回答しており、これは実証の成果と言える。

・ また、お助け実働隊地域 IT 事業者に実施してほしい対処内容として、「ウイルス駆除などの 1 次対応」「原因特定」「再発防止策の提案」などを望んでいる。

・ 所定サイバーインシデント初動対処など突発的な問題対処にかけられる費用については、2 社とも 5 万円以下と回答している。また当該突発費用に備えるサイバー保険（賠償責任保険のような本格的保険ではない費用保険）の要否については、1 社は必要と回答、もう 1 社はどちらとも言えないと回答している。

5.3.4 簡易セキュリティ診断結果から見える課題に係る考察

(1) 情報セキュリティルール策定支援と情報配信

「情報システム部門や専任担当者」を置くことができない多くの中小企業全体に対して一定の効果を得られ、かつ、事業所規模や業種が異なる企業に対しても適用できる対策が求められる。

そのため、情報セキュリティ対策は以下の 2 階層に分割して検討する。

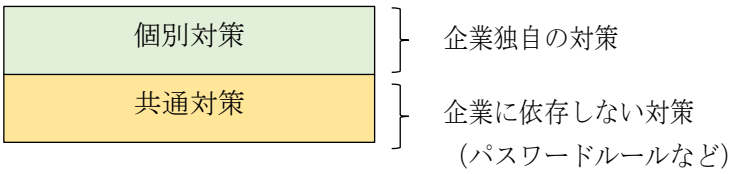


図 5-1　情報セキュリティ対策の階層分割

「SECURITY ACTION」の「情報セキュリティ 5 か条」に挙げられている「パスワードの強化」「共有設定の見直し」など、企業に依存しない共通的な対策を「サイバーセキュリティ共通ルール」として定義し、「サイバーセキュリティお助け隊サービス」利用企業に提供する。つまり、IPA から啓発されている「中小企業の情報セキュリティ対策ガイドライン」の雛形やサンプルの内容から、優先度が高い項目を抜粋し、具体的なルールまでの定義を支援する対策である。

本来企業内の「情報システム部門や専任担当者」が実施する「ルール策定」業務の一部を肩代わりすることが可能となり、中小企業の負荷軽減効果を期待できる。

本対策は「情報システム部門や専任担当者」が実施する業務の代行という観点で考えれば、人的対策にもなり得る。

(2) セキュリティ情報の配信

「情報システム部門や専任担当者」が不在の中小企業が、能動的にセキュリティ情報の収集を行うことは困難である。

そのため、中小企業がセキュリティ情報を可能な限り受動的に情報収集できる仕組みを構築できることが望ましい。

配信した情報が企業側で有効活用されるかという別の課題は存在するが、それはセキュリティ情報を得られた後の課題であり、中小企業がセキュリティ情報を「入手できていない（していない）」というそれ以前の課題をクリアすることが先決である。

セキュリティ情報を受動的に収集する仕組みとしては「メールマガジンによる配信」が有力候補となり得よう。但し、「情報システム部門や専任担当者」が不在の中小企業が、配信された情報を活用するためには、情報セキュリティの知識が無くても理解できるような工夫（注釈を付ける、検索しやすく分類して配信するなど）をしておくことが、活用段階にスムーズに移行するためには理想的であろう。

もう一つの候補としては、各種情報へ到達できるよう、情報リンクサイトを提供する案で

ある。情報収集が大変な要因は、情報が 1 か所に集まっていないことである。製品ベンダーや情報提供サイトが各々でパッチ情報やサポート終了情報などを公開しており、フォーマットも様々であるため、情報を探す側が「情報にたどり着くまで」の負担が大きいと考えられる。情報リンクサイトを提供することで「情報にたどり着くまで」の負担を軽減することが可能となり、企業側が実施する能動的なアクションを減らす効果が期待できる。

(3) リモート接続ツールの活用範囲の拡張

本実証では「テレワーク」を前提としたリモート接続ツールの提供であったこともあり、テレワークができない業務内容などの理由から、テレワークの実施が低調に終わった。

しかし、今回採用したリモート接続ツールは「画面転送型」の仕組みを採用しており、社外へのデータ持ち出しは一切発生しない。このリモート接続ツールを「テレワークツール」だけでなく「データを持ち出さないためのツール」として活用することで、私物媒体は利用不要となり、私物PCやスマートフォンを使用してもデータ持ち出しのリスクは発生しない。使用するツールの活用方法の視点を変えることによって、私物利用をサイバーセキュリティリスクから守るソリューションとしての検討の余地はある。

5.3.5 直近のサイバーリスクのトレンドと保険を含めた対策の必要性に係る考察

- 経済産業省サイバーセキュリティ課およびIPAより、昨今の不正アクセス実態に関する事例および対策に関する発信が直近で中小企業向けになされているとおり、Emotetやランサムウエア（※）などの被害が急拡大している。特にランサムウエアの深刻さおよび頻度の高まりにおいてロンドン、欧州、米国におけるサイバーリスク保険の収益性が悪化している。これにより2021年度のサイバーリスク関連の再保険レートが15%～30%程度上昇する見込みである旨が大手再保険ブローカーのレポートには記載がされている。本件は、本実証に直接的に影響するものではないが、中小企業におけるサイバーリスク保険の普及が進めば、本邦においても再保険の活用シーンが増える可能性が考えられることや、海外発のマルウエアに関連する情報として決して無視できないトレンドと考えられる。

  （参考）【サイバー犯罪による全世界の年間被害額】
  米国のサイバーセキュリティ企業である、サイバーセキュリティベンチャーズ社の推計によると、全世界のサイバー犯罪による年間被害額は2015年に3兆ドル（≒330兆円）であったが、2021年には6兆ドル（≒660兆円）に達すると予想している。2019年度の日本の実質GDPは約539兆円であることを鑑みると、いかに大きな金額であるかが分かる。

  （参考）【ビジネスメール詐欺（BEC）による被害】
  2019年10月にFBIが公表した内容によると、2016年～2019年の3年間で、被害額は260億ドル（≒2兆8,600億円）、被害件数は16万6,349件にも上ることが分かっている。

（参考）【ランサムウエアによる全世界の被害額】

米国のサイバーセキュリティ企業である、サイバーセキュリティベンチャーズ社の推計によると、全世界のランサムウエアによる被害額は2019年は115億ドル（≒1兆2,650億円）であったが、2021年には200億ドル（≒2兆2,000億円）に達すると予想している。ランサムウエアの被害額も急増する見込みであり、引き続き大きな脅威となっている

・ 次に、IPA による「情報セキュリティ 10 大脅威」の直近 3 年の推移に着目した。これは、前年に発生した社会的に影響が大きかった情報セキュリティにおける事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約 140 名のメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものであり、本実証前にあたる 2018 年度を含む直近 3 年間から、下記傾向が読み取れる。いずれもサイバーリスク保険の担保危険そのものである。

＜出典：IPAの情報セキュリティ10大脅威＞

IPA（https://www.ipa.go.jp/security/vuln/10threats2020.html）（2021/1/18 参照）

・ **「内部不正による情報漏洩」**

内部不正とは、従業員や委託作業員などが不正に内部情報を持ち出し、第三者に販売することや悪用することである。2018 年：8 位→2019 年：5 位→2020 年：2 位と順位を上げており大きな脅威となっている。委託先業者の管理体制がずさんであることも多く、サプライチェーン管理と合わせて対策を検討すべき脅威である。

・ **「ビジネスメール詐欺（BEC）」**

BEC とは、経営者や取引先企業の担当者になりすまし、メールで送金指示を出し、実際に攻撃者の口座へ送金させる詐欺の手口である。2018 年：3 位→2019 年：2 位→2020 年：3 位と近年高順位を維持しており、継続的に大きな脅威となっている。世界的に猛威を振るっている脅威であり、海外の取引先や新規取引先とやり取りを行う際は特に注意すべき脅威である。

・ **「サプライチェーン攻撃」**

サプライチェーン攻撃とは、系列企業や取引先、委託先企業など含めたサプライチェーン全体における弱点を突き、サプライチェーン全体に被害を拡大させる攻撃手口である。2019 年：4 位（初登場）→2020 年：4 位と、2019 年に初登場してから、引き続き高順位をキープしている。国内企業においても、海外子会社の技術的な脆弱性を突かれ、本社システムにまで侵入され、情報漏洩が発生してしまった事案が報告されている。サプライチェーンが複雑化し、また IT やテクノロジーの利活用が増々高まっていくことを鑑みると、今後、より大きな脅威となることが想定されるため、すぐにでも対策を検討すべき脅威である。

・ 「ランサムウエア」

ランサムウエアとは、コンピュータウイルスの一種で、ランサムウエアに感染すると PC に保存されているファイルが暗号化され、攻撃者は暗号化解除や復旧と引き換えに金銭を要求するもの。

2018 年：2 位→2019 年：3 位→2020 年：5 位と、順位を下げているが、2019 年にも海外において複数工場が停止に追い込まれ、数十億円規模で被害が発生しているなど、引き続き、世界的に猛威を振るっている。

5.4 中小企業におけるセキュリティ対策の効果（実証の効果）

5.4.1 実証参加企業が本実証の中で実際に行った具体的対処・改善などに係る考察

・ 本実証事業の重要な目的の一つが実証参加企業の「意識変革」「行動変容」である。これらも定量的に把握することが困難な性質のものだが、一つの切り口として、下記のとおり、UTM 検知に伴って自動送信されるアラート通知メールに基づき、実際に能動的な対処を実施したか否かを調査した。

表 5-24　アラート通知メール記載対処の実施有無

アラート通知メール記載の対処は実施したか（複数回答可）		
対処・改善など	件数	備考
ウイルス対策ソフトでスキャンしウイルスが検出され駆除	4 (8%)	
ウイルス対策ソフトでスキャンしたがウイルスが不検出	8 (15%)	
OS をクリアインストールした	0	
怪しいソフトやアプリなどを削除･アンインストールした	2 (4%)	
社員に注意喚起した	11 (21%)	
その他	1 (2%)	ルーターの設定を見直した
実施しなかった	17 (32%)	UTM が防御したので対処せず ・特に必要と感じられなかったため（3） ・UTM がウイルスを遮断したとの連絡だったので対処は不要だった（2） 経過観察とした ・重大インシデントが無くアラートは要観察とした ・有害サイト閲覧は数日で止んだため保留 UTM の過検知

		・アラート発報に基づきチェックしたが過検知だった アラート通知の問題 ・対処法が曖昧で分からない 参加企業側の事情によるもの ・設定が煩雑なためしなかった
アラート通知メールが来なかった	15 (28%)	

・ アラート通知メールに基づき何らかの対処を実施したのは（「実施しなかった」「アラート通知メールが来なかった」から引き算で算出し）40%割（21 社）であった。令和元年度実証ではこの比率が 34%（35 社）であったため、若干ではあるが良好である。全体としては少数派ではあるが、4 割の実証参加企業が具体的な行動を能動的に実施したことは大きな成果である。

・ 「ウイルス対策ソフトでスキャンしたがウイルスが不検出」であったものは 8 件あり、UTM の過検知（False Positive）である可能性も高く、UTM の精度向上という点でも大変貴重なデータである。通常、商用サービスにおいては、発報したアラート通知の正確性を追跡調査することはしないし、アラート通知の助言に基づき実際に対処をしたか否かなどの追跡調査も行わない。よって、実証であってこそ入手できた貴重なデータと言える。

・ 但し「ウイルス対策ソフトでスキャンしたがウイルスが不検出」を、そのまま UTM の過検知（False Positive）と判断することは速断とも言える。令和元年度実証では OS のアップデートが行われていない PC やウイルス対策ソフトのパターンファイルが最新化されていない状態でスキャンを実施したケースもあった。こうした場合、仮にウイルスが入り込んでいても「検出無し」で表示される場合も少なくない。また令和元年度実証により生み出した商用サービスのユーザー企業において、OS もウイルス対策ソフトのパターンファイルも最新の状態でスキャンしたが「検出なし」とされたが、UTM が明らかにウイルスを検知していたことから念のため「EmoCheck」で確認したところ、検出されたケースも実際にあった。更には、ウイスルスキャンをいわゆるクイックスキャンで済ませているケースも散見される。よって「不検出」の 8 社は中期的な経過観察が必要であり、決して UTM を過小評価したり、安心したりするのは禁物である旨を伝達する必要性があるが、この種の伝達が実務的には誠に難しいのである。

・ 「社員に注意喚起した」が 11 社（21%）あった点も重要な成果と言える。情報システム担当者や経営層のみならず、サイバーセキュリティ意識を社員に浸透させていくことは何よりも重要であるが、なかなかそういった機会というものは到来しないのが現実である。何かをきっかけにするしか無いが、そのきっかけを本実証事業が提供し得たことは大きな意義である。

・ 「実施しなかった」のうち 5 社は UTM が防御したがゆえである。これこそ、人手も時間も不足がちな中小企業における“お任せ型”統合脅威管理サービスの存在意義であるが、

これはUTMの効果を実感しにくくする要素にもなり得る。つまり“お任せ型に伴う安心感”と“ほったらかしに伴う意識低下”は表裏一体の関係性にある。だから、アラート通知メールはプッシュ型連絡手段として、後者に堕することが無いよう、前者を強調するものであり続ける必要がある。その意味では「対処法が曖昧で分からない」といった本実証事業で得た“ユーザーの厳しい声”は真摯に受け止め、改善に努めなければならない。

5.4.2 実証参加企業が感じた満足度と効果に係る考察

- 実証参加企業による総合的な満足度は下記のとおりであった。

表 5-25　お助け隊実証のサービスの満足度

お助け隊実証のサービスに満足したか			
	令和2年度 滋賀・奈良・ 和歌山 n=53	備考	令和元年度 京阪神 n=105
はい	37 (70%)	攻撃を防御してくれた ・セキュリティが強化された ・ウイルスが入らないようにして頂けて大変有難かった ・特に困ったことが無かった 攻撃の実態が分かった ・サイバー攻撃や脅威を見える化できた（2） ・マルウエアや危険サイトへのアクセスの見える化ができた ・認識できていなかった脅威が見つかった 自社のセキュリティ状況を把握できた ・自社のサイバーセキュリティ状況を把握できた（2） 安心感があった ・サイバー攻撃情報を頂戴するなど安心感があった（2） ・すごく安心感があった。同じような営業を断ることができた ・セキュリティ対策やインシデントの助言で不安が解消された ・セキュリティが高まったと思えた ・見た目には分からないが守られているという意識を持てた ・セキュリティが向上できたと思う 対応が良かった ・UTM設置のサポートまでしてもらえて大変助かりました ・設置時に事務局・相談窓口でアドバイスを頂けた ・異常検知だけでなく設置を含め分からないことに対応頂けた UTMを知った・UTM導入のきっかけになった ・UTMの運用を理解できた ・セキュリティに関する機材に興味が持てた ・UTMの導入を検討していたため使用感を確かめられ良かった 情報を入手できた ・セキュリティ情報の提供が有難かった（2） ・今まで分からなかった情報を得ることができた ・リアルタイムでウイルス情報を提供頂ける 意識・知識が高まった ・サイバーセキュリティ意識の向上になった（3）	56（53%）
いいえ	0		5（5%）

どちらとも言えない	16 (30%)	効果の実感できなかった ・効果の実感が無かった（5） ・サイバー攻撃の対応が不明・未解決 ・個人事業主なのでパソコンにセキュリティがあればいい ・特にセキュリティが向上した兆しが無い ・UTM 設置・設定に時間がかかり実際に動いていた期間が短すぎて判断できない 攻撃・被害・問題が無かった ・サイバー攻撃が少なかった ネット環境などへの支障があった ・結局ネットが重い気がして外してしまうことが多かった 参加企業側の事情によるもの ・工場なので上手く活用できなかった ・多忙のため活用できなかった	42（40%）
無回答	0		2（2%）

・　実証参加企業による「参加して良かったと点」は下記のとおりであった。

表 5-26　お助け隊実証に参加し良かった点

お助け隊実証に参加し良かった点（複数回答可）			
内容	令和 2 年度 滋賀･奈良･和歌山 n=53	備考	令和元年度 京阪神 n=105
自社へのサイバー攻撃動向が把握できた	26 (49%)	・アラートメールが届くことで把握ができる（3） ・傾向の把握、他社比較が参考になった ・今まで見えなかった部分が見える化できた ・ウイルスメールの危険度が分かった ・要注意のメールやサイトの傾向や情報が得られた ・UTM 検知情報やウイルス除去の情報が有難い ・サイバー攻撃やスパムメールが巧妙になり自社では判断できないことがあった ・取引先のサイトが危険な状態であったことが理解できた ・簡単な操作でセキュリティを施せたのが良かった ・サイバー攻撃の数値化ができた ・情報漏洩は無かったので安心した ・お助け隊の駆け付けなどにより、より見えてきた	22 (21%)
社員のサイバーセキュリティ意識・知識が向上した	16 (30%)	・少々サイバーセキュリティの知識が身に付いた ・普段の業務 PC でのアクセスする意識が共有できた ・説明会で最新の知識を得ることができた。 ・社内からの通知が多く社員の意識向上になった ・携帯電話のセキュリティが低い点につき理解が深まった ・実際に異常が感知されたため安全意識が高まった ・セキュリティ対策を社内で検討した ・PC を置いてある部屋を施錠するようになった	22 (21%)
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	12 (23%)	・通信ログをこまめに見るようになった ・自社でできていること、できていないことがはっきりした ・内部で特に問題が無いことが確認できた ・現状の PC 管理台帳では PC を特定することは困難であることが判明した ・WiFi の常時接続を止めた ・来年度、情報セキュリティ計画を策定することになった ・情報セキュリティに関する取り組みができた ・不要なサイトへのアクセス遮断	19 (18%)

自社へのサイバー攻撃・情報流出などが防げた	10 (19%)	・実感は無いが防げていると思う ・攻撃内容が見える化され回避・遮断によって安心できた ・PC,NAS からの不審なアクセスが確認できた。今後の対策に役立てたい	18 (17%)
自社の社会的信用が向上した	5 (9%)	・セキュリティをしていることで信頼感が増した	6 (6%)
その他	7 (13%)	・不明な点を相談することができた ・適時情報を頂けたのが良かった ・UTM が問題なく動いているので良かった ・目で見えないものなので守られている安心感がある ・多忙のため活用できなかった ・FW 側アクセスなど必要無いサイトをブロックしてくれることが非常に良い ・他からの攻撃を防止できる点で良いと思った ・簡易セキュリティ診断結果により今後取り組むべき内容が明らかになった	23 (22%)
良かったと思う点は無い	1 (2%)	・特に使わなかった	18 (17%)

・　本実証事業における効果の代表的なものは下記事例のとおりであった。

表 5-27　本実証事業における効果

会社	実証の効果
O 社 滋賀県 製造業 101～200 人	・テレワークツールは将来的に導入を予定しているが、今回の実証でツールが貸与され実際に使ってみることができ、使いやすかった。 ・セキュリティの実施、インシデントへの助言で不安が解消された。 ・攻撃内容が見える化され、回避・遮断によって安心できた。 ・傾向の把握、他社比較が参考になった。 ・自社でできていること、できていないことがはっきりした。 ・商用サービスは利用したい。パッケージで非常に分かりやすく価格も安価と感じたため、他の拠点分も含め利用したい。
P 社 奈良県 サービス業 201～300 人	・自社のセキュリティ状態が分かった。例えば、現状の当社の PC 管理台帳では PC を特定することは困難であることが判明した。 ・今まで見えなかった部分が見える化できて良かった。 ・社内からの通知が多く社員の意識向上になった。 ・商用サービスは前向きに考えているが、内部で調整して最終的に判断したい。
Q 社 和歌山県 製造業 201～300 人	・サイバー攻撃の数値化ができた。 ・今まで分からなかった情報を得ることができた。 ・不要なサイトへのアクセス遮断。 ・UTM の必要性を感じるため、商用サービスは利用したい。
R 社 滋賀県 製造業 1～3 人	・アラートメールに基づきウイルス対策ソフトでスキャンした結果、ウイルスが検出され駆除した ・セキュリティが高まったと思えた。 ・相談窓口の対応はとても良く、丁寧に連絡を頂いた。 ・実証の期間が短すぎ商用サービスに残るか否か判断しにくい。

S 社 奈良県 建設業 11～20 人	・簡易セキュリティ診断の結果により今後取り組むべき対策が明らかになった。 ・セキュリティが必要なことは理解できたが、期間が短すぎ、UTM 設置による効果は実感できず、導入については緊急性を感じていない。
T 社 和歌山県 サービス業 11～20 人	・UTM 導入を検討していたため使用感を確かめることができた。 ・来年度、情報セキュリティ計画を策定することになった。 ・テレワークは、方針として導入しないこととなった。

- 満足度は 70%であり令和元年度実証の 53%を大きく上回った。「不満足」も令和元年度実証では 5%あったのに対して令和 2 年度実証では 0 となり、「良かったと思う点が無い」も令和元年度実証の 17%に対して令和 2 年度実証は 2%まで下がり、大幅な改善があった。また、令和元年度実証と比して実証期間が短かった（約半分）にもかかわらず「どちらとも言えない」が令和元年度の 40%よりむしろ低く 30%であった。

- この改善の理由は実際のところよく分からない。自由記述コメントも令和元年度で見られたようなコメントばかりである。事務運営面や顧客サービス面は令和元年度実証の経験により様々な面でスムーズかつきめ細やかに実施できたと思われるが、17 ポイントも評価を押し上げる要素ではなかろう。

- UTM のスペックは令和元年度実証とほぼ同などのものであるため、「お守り」「見守り」サービスの部分が評価を上げた要因とは考えにくい。一方、アラート通知メールである「お知らせ」は、その記述を令和元年度（大変、評判が悪かった）から改善している点などが幾分か評価されたことと推定される。「相談」は先述のとおり令和元年度同様に非常に満足度が高い。「初動対処（駆け付けお助けまたはリモートお助け）」は件数が 2 社しか無く（当該企業からの評価は高いものの）全体の満足度を押し上げる数量ではない。

- 令和元年度実証には無かった「テレワークツール」も別記のとおり誠に残念ながら実利用企業は 5 社と非常に少なく（当該企業からの評価は高いものの）全体の満足度を押し上げる要素にはならない。いまひとつ令和元年度実証に無かった「簡易セキュリティ診断」は満足度を押し上げる役割を担った可能性があるが、自由記述コメントにはほとんど登場しないことから、これも全体評価の押し上げ要因としては限定的と言える。

- 畢竟、総合満足度が令和元年度との比較において向上した理由を明確なエビデンスをもって総括することはできない。よって、以降は推定になるが、滋賀・奈良・和歌山にあっては、中小企業を対象としたサイバーセキュリティのセミナーやサービス、支援機関、支援施策、実証事業の類いなども、もともと少ないのではなかろうか。少ない中、本実証事業がサイバーセキュリティ対策を検討することや UTM を無料体験する貴重な機会となったのではなかろうか。このことが評価されたのかもしれない。

それは表 4-6 において「自社へのサイバー攻撃動向が把握できた」が 49%（26 社）であり令

和元年度実証の 21%（22 社）に比して 2 倍以上高いこと、「社員のサイバーセキュリティ意識・知識が向上した」が 30%（16 社）であり令和元年度実証の 21%（22 社）に比して 10 ポイント近く高いことからも間接的に伺える。

・ もしそうであるならば、大阪商工会議所が地域展開窓口の力を借りながら“背伸び”して非大都市圏である滋賀・奈良・和歌山の 3 県で本実証事業を実施した意義は大きく、効果も小さくなかったと言えよう。

5.4.3 UTM の防御効果に係る考察

・ 令和 2 年度実証の実証参加企業の 70%が何らかの脅威を検知しており、更に特定の企業で脅威が集中して検知された。よって、UTM の AV、IPS、WG による 3 機能により、幅広く脅威を検知・遮断でき、非大都市においても機能の有効性を確認できた。また、UTM の検知アラートがきっかけとなり、内在していたセキュリティリスクを駆除することにも成功した。

・ 直接的な防御効果ではないが、古いバージョンのソフトウエアを使用していることが検知できた。令和元年度実証は InternetExplorer を、令和 2 年度実証は Adobe Flash player（2020 年 12 月 31 日でサポート終了）を検出しており、古いバージョンのソフトウエアは脆弱性が発見されても修正されることが無いため、UTM を通した企業へのセキュリティ向上に貢献した。

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 実証結果を踏まえた検討

(1) 簡易型保険の在り方

① 令和元年度実証を踏まえた簡易的な保険（全員加入型）の概要

・ 中小企業が設置しているUTMで不正アクセスなどの発生やその恐れを検知。検知後に大阪商工会議所が紹介するお助け実働隊地域IT事業者が訪問の上、初動対応などを行う。上記駆け付け対応にかかる費用につき5万円を限度に保険金でお支払いする。

② 令和2年度実証からの考察

・ 令和2年度実証においては既存の保険発動となる事例は1件も無かった。
（参考）商用化の簡易型保険における保険請求は1件（支払保険金48,000円）である。

・ アンケート結果によればサイバーリスク保険の必要性を認識している中小企業は 10%に満たず、保険の優先順位は引き続き低いままと考えられる。また、サイバーセキュリティにかける経費は年間5万円以下との回答が大半を占め、サイバーリスク保険料についても同様の予算枠内で検討される可能性が高い。

・ アンケート結果によれば、29社/53社（約55%）の中小企業が将来的にテレワークの導入を検討している。よって、テレワーク環境に応じた補償（含む保険約款の記載文言）の在り方への対応は今後とも念頭に置く必要がある。新型コロナウイルスにより駆け付け対応が物理的に困難となっている状況を鑑みて、4 月の保険更改までに補償の変更を検討していく。

③ 令和2年度実証を踏まえた簡易保険の在り方

・ 令和2年度実証においては保険事故に繋がるインシデント発生は無く、商用化サービスに付帯されている簡易型保険の請求は1件（損害率は約5%）と、悪い実績とは言えないものの、運用から1年経過をしていないことから、大数の法則が働くと認識するには時期尚早と考えることもできる。

・ 今後、中小企業における請求可能回数（現在は1中小企業あたり年間1回）や1回あたりの支払限度額の拡充、その他リモート・テレワーク環境において必要な初動対応費用などを簡易型保険で補償することの是非について検討を継続しつつ、中小企業に賦課しやすい保険料水準を維持していく。

(2) サイバーリスク保険（いわゆる 2 階部分保険）について

① 令和元年度実証における考察

・ 駆け付けによる初期対応だけでは、根本的な問題が解決しないケースも想定される。その際、中小企業には更に高度な対応が求められることになり、上乗せ保険が必要となる。実証参加企業へのヒアリングでも、お助け隊（簡易的な保険）で対応できる範囲と、上乗せ保険で対応できる範囲につき説明（以下、図表参照。）した際には上乗せ保険のニーズも一定程度確認することができた。但し、これは中小企業であっても相当数のサイバー攻撃を受けている事実を個別に説明したことで、リスクを具体的に認識し上乗せ保険の必要性を認識したことによるものと推測される。

表 6-1 （参考）簡易型保険と上乗せ保険の関係図

起こり得る代表事例	お助け隊を導入していた場合	被害事例	上乗せの保険でできること
不正なプログラム（ウイルスなど）の送付などの攻撃	UTM により攻撃をブロック	被害無し（ウイルスの感染の恐れ無し）	（お助け隊で対応完了）
	UTM で不正アクセス検知。IT 事業者が駆け付け、初期対応を実施。（フルスキャンによりハードディスク上のファイルと実行中のプログラムをチェックし、確認できたウイルスを可能な範囲で除去。）	被害無し（ウイルスの感染も除去）	（お助け隊で対応完了）
		被害無し（ウイルスの感染の恐れが残っている）	【費用】 IT 事業者の駆け付けによる初期対応でウイルスの除去や感染源の特定などができなかった場合の追加費用を補償。
		社内のネットワークの稼働が停止	【費用】 稼働停止の原因の調査と、原因に対する復旧費用を補償。
		社内データが消失	【費用】 データが消去した場合の復元などの費用を補償。
		社内の顧客情報データが流出	【費用（含む賠償）】 データが流出した顧客に対する見舞金、プライバシーの侵害による賠償請求を補償。
		自社になりすまし、取引先にウイルスを送付し、取引先のデータを消失。	【賠償】 取引先のデータ消失による損害賠償責任や、データを復元するための費用に対する損害賠償責任を補償。
		端末の乗っ取りにより、取引先を攻撃し、取引先のネットワークを切断。	【賠償】 ネットワークの切断に伴う損害賠償責任を補償。

② 令和 2 年度実証を踏まえたサイバーリスク保険展開の方向性

（参考）2020 年度の現状

・ 2020 年度は商用化サービス導入の中小企業向けに、東京海上日動社が日本商工会議所の団体制度として中小企業向けに提供する「超ビジネス保険（サイバー補償条項）」の提供を予定していた。
※本保険は、商工会議所の団体割引により通常より最大で 33%割安となっており、サイバーインシデントの発生により大きくは以下 2 点の補償をするもの。
  - 【賠償】サイバー・情報漏洩事故（最大 3 億円）
    サイバー攻撃などに起因、法律上の損害賠償責任を負担することにより被る損害
  - 【費用】サイバー・情報漏洩事故対応費用（最大 3000 万円）
    セキュリティトラブルへの対応やサイバー・情報漏洩事故に起因する訴訟対応を行うために被保険者が負担する初動対応対応費用を補償

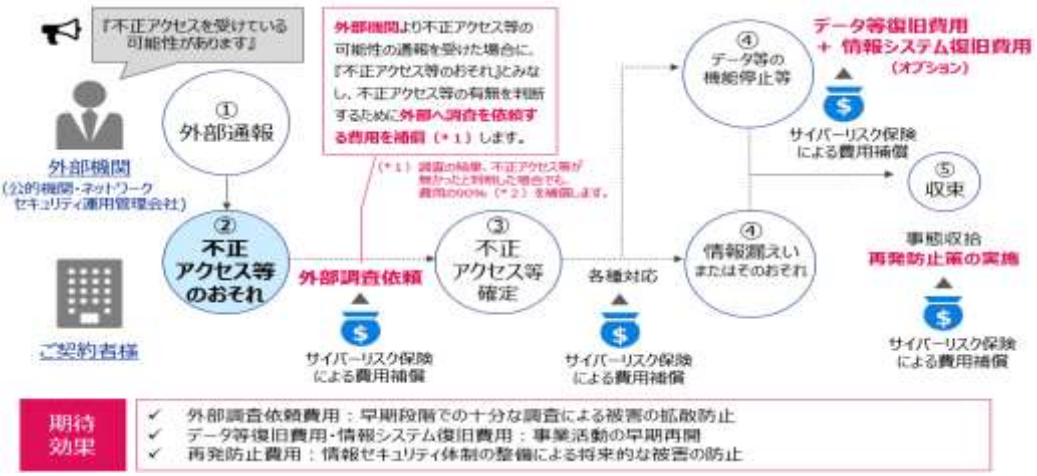
・ しかしながら、2020 年 4 月の緊急事態宣言発出や新型コロナによる損害保険会社および代理店の活動量の制限により、当初の目論見は外れ、想定どおりの活動は実施できなかった。

③ 令和 2 年度実証を踏まえて

・ 各種インシデント発生による新聞報道や IPA の情宣、改正個人情報保護法などにより中小企業にとってサイバーリスク保険を目にする機会は飛躍的に向上したと考えられる。また、アンケート結果においては半数以上が実証参加におけるアドバンテージに「自社のサイバー攻撃動向を把握できた」と回答している。

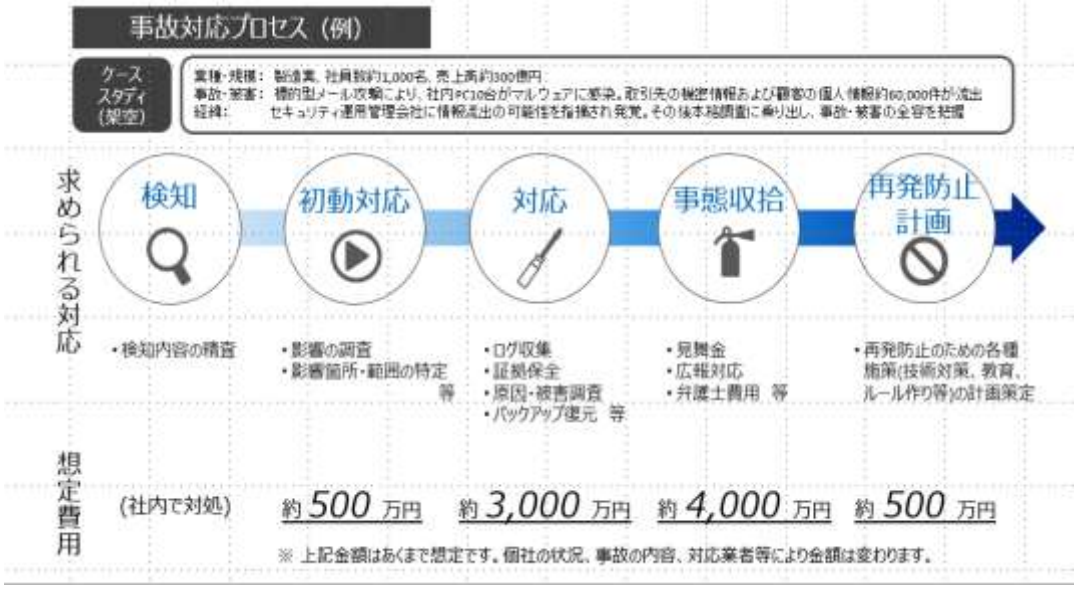
・ 他方で、商用化サービスにおける保険請求があった事例は Emotet によるものであった。初動対応 3 時間程度で駆除が完了したものの、Emotet を駆除しきれない場合は感染した中小企業を起点にサプライチェーンに Emotet が流出し情報漏洩や影響を及ぼす可能性を否定できない。

・ 加えて、自社の営業継続にも支障が出る可能性が考えられ、企業が所有する財物に物理損害が生じないような、サイバーインシデントがトリガーになる事業休止に対応する保険はサイバーリスク保険（含む上述の超ビジネス保険のネットワーク中断条項）しか存在しない。



・ 上図のようにお助け隊サービスで処理が完結しなかった場合は甚大な外部への調査依頼やゆくゆくはデータ復元（夜間残業代金ほか）などが発生することが想定される。

図 6-2　（参考）お助け隊サービスの初動対応で済まない場合に発生する費用と保険の対応



(3) 簡易型保険やサイバーリスク保険が果たす意義

・ 上述のとおり、本実証成果および 2020 年における不正アクセスなどの外部環境変化を考慮すれば、中小企業のサイバーセキュリティを真に普及向上させる上においては、セキュリティ体制構築に向けた中小企業の意識向上と並行して本格的な補償のサイバーリスク保険の普及が必要と考えられる。これらを実現するには中小企業の事業リスクに身近な商工会議所および保険代理店（損害保険会社）による BCP 策定支援機能と連動した形でのワンパッケージとして伝播される形が極めて有効な手段であると考察する。（裏を返せば、そのような機能を担保できる他の主体は国内にはほぼ存在しないのではないか）

・ よって、緊急事態宣言が再発出される環境下ではあるものの、大阪商工会議所および損害保険会社、保険代理店によるサイバーセキュリティサービスを伝播するための準備を簡易保険のバージョンアップとともに図っていく。

※代理店が活用しやすいようフローチャート

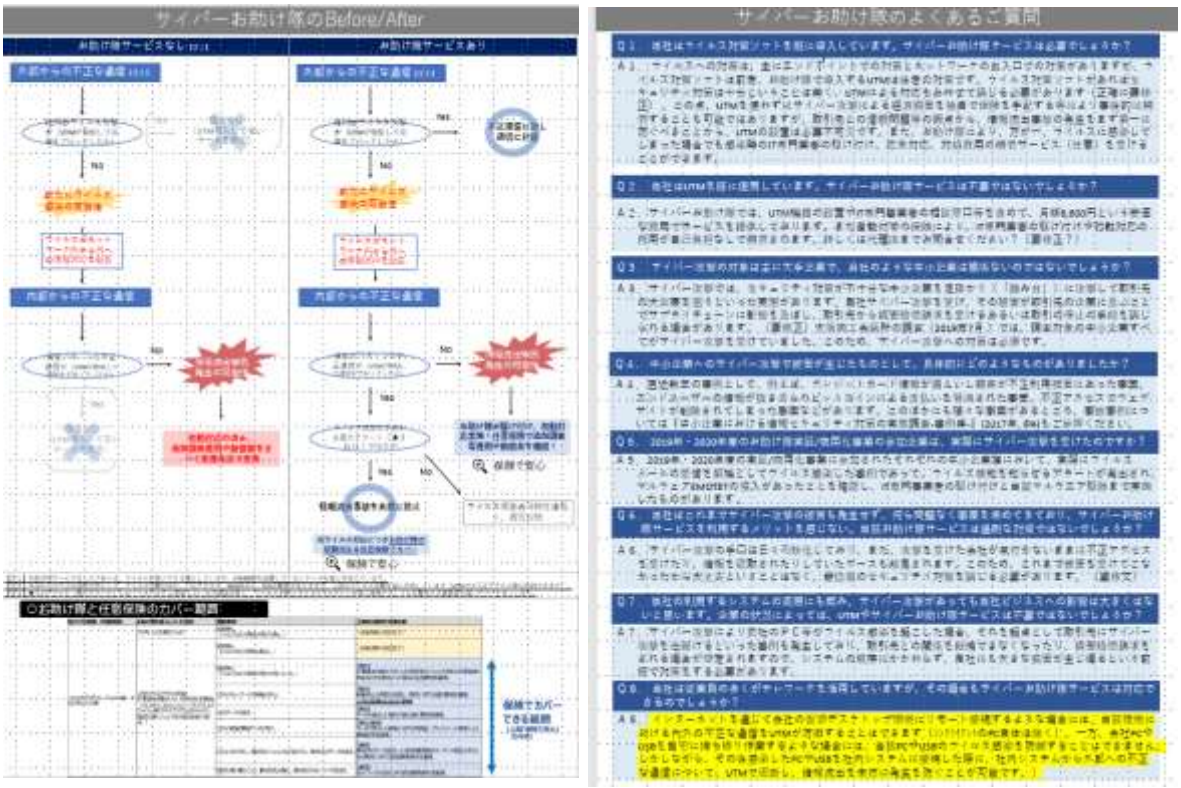


図 6-3　（参考）保険代理店が中小企業訪問時に使用するお助け隊サービスの企画書（ドラフト版）

6.2 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

6.2.1 UTM と SOC の改善（「お守り」「見守り」「お知らせ」）

・ 本実証事業において、問合せの約 35%が、UTM の設置場所に関する問合せであった。そのため、実証中の問合せ内容をもとに、設置場所に関する UTM の設置マニュアルの改善を行う。マニュアルを見ることで、UTM の正しい設置場所がどの企業でもすぐに分かる内容となるよう、マニュアルを作成する。それにより、企業自身の設置コスト削減や、サービス運用コスト削減（問合せ件数、問合せ対応に掛かる時間）の削減を図る。

・ 本実証事業の問合せ内容をもとに、UTM の脅威を検知するシグネチャの改善を行う。シグネチャを改善することで、UTM の過検知を減らし、企業に対して通知されるメールの件数を減らす。それにより、サービス運用コスト削減（問合せ件数、問合せ対応に掛かる時間）の削減を図る。

・ 今回の実証事業では、期間が 3 ヶ月と短かったこともあり、UTM の各機能の必要性およびオプションや価格の再検討までは至らなかった。今後実証参加企業による意見やセキュリティ情勢を考慮し、UTM の価格や機能に関するスリム化の検討を継続する。

6.2.2 テレワークツールの取り扱い

・ 本実証事業においては、テレワークツールの利用が 5 件であり、テレワークツール申込企業のうち 17%の利用、実証参加企業全体で見るとわずか 9%の利用となった。

・ 「with コロナ時代に対応するために御社にとってテレワークは必要ですか？」の問いに対して、「不要」と回答した企業が 23 社と、実証参加企業中 43%を占める結果となった。テレワークツール利用によって重要情報の持ち出しをなくすことができた事例もあり、テレワークツールはテレワーク時のセキュリティ対策として有効ではあるが、本実証の結果のみから判断すると、ニーズが低いと言わざるを得ない。

・ 以上のことから、商用サービス（Ver.2.0）においては、テレワークツールを導入することは見送る。しかし、テレワークにおいて多くのセキュリティリスクが伴うことは明らかであり、本実証を通して環境が整っていないままテレワークを実施する中小企業が多いことも明らかになったため、引き続きテレワークセキュリティ対策のサービスについて検討を続けていく。

6.2.3 所定サイバーインシデント初動対処の改善（「駆け付け」「リモートお助け」）

- 本実証事業においては、初動対処の対象となる所定サイバーインシデントが 2 件発生し、1 社はリモートお助けを受け入れ（甲社）、1 社は入口論で拒否した（乙社）。

- リモートお助け拒否の理由は、乙社自身が自身の IT リテラシーの低さを理由として挙げている。また、受け入れた甲社も「今後はリモートお助けを積極的に使いたくない」と回答しており、その理由として「情報伝達に時間がかかる」ことを挙げている。

- 以上のことから、本実証事業から得られた知見だけをもとに判断すると、リモートお助けを積極的に評価することはできない、という結論を下さざるを得ない。

- そうではありながらも、緊急事態宣言下にあってもインシデント対応は発生しうるし、山間部まで駆け付けることは現実的にできない。よって、商用サービス（Ver.2.0）においては、本実証事業を踏まえつつも、状況により、リモートお助けの手法をユーザー側に案内・提案し、ユーザーおよびお助け実働隊地域 IT 事業者の双方が合意した場合は、引き続きリモートお助けを実施し、試行錯誤により検証作業を継続していく予定である。

- 経験値を積むことで、様々な工夫や改善点が見いだされ、早晩フォーマットが形成されるであろう。また、リモートに係る技術や各種ツールはコロナ禍を契機として IT ベンダーなどにより積極的に開発・リリースが進むと考えられるし、5G の進展によりリアルタイム性も向上するであろう。時代の風を機敏に感じ取り、サービスの守備範囲と価値を高めていきたい。

6.2.4 実証参加企業の商用サービスへの残留率

・ 実証参加企業に、暫定で、現商用済みサービス（Ver.1.0）のサービス概要と価格感を伝えた上で商用サービス利用をするか否かを聞いたところ下記のとおりであった。

表 6-2　商用サービスへの残留率

商用サービスを利用するか				
内容	令和 2 年度 滋賀･奈良･ 和歌山 n=53	備考	令和元年度 京阪神 n=105	
利用する	6 (11%)	・今後も継続して監視していきたいと思います ・パッケージで非常に分かりやすく価格も安価 ・この現状のままセキュリティを強化していきたい ・お助け実働隊がセットになっており魅力を感じる ・UTM の必要性を感じる	12 (11%)	結果的に商用サービス利用に至ったのは45／112（40%）
迷っている	20 (38%)	・本社と相談する ・実証の期間が短すぎた。もう少し使ってから判断したい	36 (34%)	
分からない			17 (16%)	
無回答			1 (1%)	
利用しない	27 (51%)	・VPN ルーター導入済 ・ウイルスソフトで対処可能 ・データの活用方法が分からなかった ・コスト的に高い ・小規模事業者なのでウイルスの侵入は無いと思うが、将来的には必要だ。 ・対策が必要なことは理解しているがそこまでの緊急性を感じていない	39 (37%)	

・ 上記のとおり、53 社中 6 社（11%）が商用サービス利用を決めており、迷っている企業が 20 社（38%）である。令和元年度実証では、実証参加 112 社のうち結果的に商用サービスを利用することになったのは 45 社（令和 3 年 1 月現在）であり、商用サービス残留率は 40%である。しかし令和元年度実証においても実証終了時点では上記のとおりの 12 社（11%）しか残留を希望していなかったが、その後の「Emotet」の大流行などもあり「迷っている」「分からない」「利用しない」としていた企業からも申し込みがあり、結果的に 45 社（40%）まで積みあがった。この率が高いのか低いのかを判断することは困難であるが、コンソーシアムの目標は 50%であったことから、コロナ禍に伴うユーザー側の経費節減・緊縮財政の風潮や、大阪商工会議所側としても当初予定していた販売・営

業活動がほとんどできていない状況を勘案すると、そこそこの成績とも言える。

・ 令和 2 年度実証においても、実証終了時点において、参加企業の商用サービス利用意向は、令和元年度実証とほぼ同じである。懸念されるのは、先述のとおり、令和 2 年度実証の「総合満足度」や「参加して良かった点」は令和元年度実証に比して大幅に改善されているにもかかわらず、商用サービスへの残留率に関しては、令和元年度実証とほぼ同じという点である。即ち“満足はしたけど、買いません”ということにほかならない。商用サービスを「利用しない」理由も、自由記述コメントを見る限り、令和元年度実証のそれと内容的にはほとんど変わりが無く、「高い」「ウイルス対策ソフトで十分」「必要性は分かるが緊急性を感じない」の 3 点に集約され、これらはいずれも「効果実感は無い」ということと裏表の関係性であり、これは令和元年度実証とほぼ同じ総括である。

・ 令和 2 年度の実証参加企業の規模（従業員数）は平均値も中央値も令和元年度実証とほぼ同じであることに鑑みると、滋賀・奈良・和歌山の 3 県の中小企業にあっては、大阪など大都市圏以上に、セキュリティに係る経費支出が更に一層厳しいのかもしれないという抽象的な仮説以上はここでは見い出せない。

・ 効果実感の課題解決策を含む販売促進策については、コンソーシアム内でも相当な時間をかけて試行錯誤や深い議論を重ね、様々な関係機関などとも接触してきており、微細な改善は随時実行を加えているものの、販促上効果を持つようなキラーコンテンツはいまだ見い出せておらず、それは既存商用サービスのユーザー数の伸び悩みにも表れている。残念ながら、本実証事業においても、販促上効果を持つようなキラーコンテンツを見い出すには至らなかったが、幾多のヒントは得ることができた。

6.2.5 中小企業サイバーセキュリティ対策支援体制の構築

(1) 地域における支援体制構築のカギを握るお助け実働隊地域 IT 事業者

・ 今回契約した 9 事業者のお助け実働隊地域 IT 事業者が全て最低 1 回は出動した。

うち 1 社（UTM 設置支援と所定サイバーインシデント初動対処の両方を体験）は、その現場作業の困難さに照らし、現行の支払対価では採算が合わない旨を指摘している。しかし、同社は本実証事業ならびに商用サービスに対し必ずしも否定的な印象を持つには至っていない。他のお助け実働隊地域 IT 事業者も概ね今後の商用サービスでも引き続き事業参画を得られそうである。

・ また表 5-3 のとおり、実証参加企業（ユーザー）側の評価も高かった。

表 6-3　お助け実働隊地域 IT 事業者の対応についてのアンケート

<table>
<tr><th colspan="5">お助け実働隊地域 IT 事業者の対応は良かったか</th></tr>
<tr><td rowspan="4">とても
良かった</td><td>先方の指示・助言・用語が的確・理解しやすかった</td><td>8</td><td rowspan="4">15
(58%)</td><td rowspan="9">良かった
23
(89%)</td></tr>
<tr><td>当方の状況・要望を把握・理解してもらえた</td><td>4</td></tr>
<tr><td>解決までの時間が短かった</td><td>2</td></tr>
<tr><td>その他</td><td>1</td></tr>
<tr><td rowspan="4">良かった</td><td>先方の指示・助言・用語が的確・理解しやすかった</td><td>2</td><td rowspan="4">8
(31%)</td></tr>
<tr><td>当方の状況・要望を把握・理解してもらえた</td><td>4</td></tr>
<tr><td>解決までの時間が短かった</td><td>1</td></tr>
<tr><td>その他</td><td>1</td></tr>
<tr><td colspan="2">普通</td><td>3</td><td>3（12%）</td><td>3（12%）</td></tr>
<tr><td>悪かった</td><td>（略）</td><td>0</td><td>0%</td><td rowspan="2">0%</td></tr>
<tr><td>とても
悪かった</td><td>（略）</td><td>0</td><td>0%</td></tr>
</table>

・ 以上より、本実証事業を機に、滋賀・奈良・和歌山を含む関西のほぼ全域に「駆け付けお助け」または「リモートお助け」のいずれかを展開できる支援体制が構築することができたと言える。これは令和 2 年度実証の成果と言える。

・ とはいえ、商用サービスとしての「商工会議所サイバーセキュリティお助け隊サービス」は、コンソーシアムおよびお助け実働隊地域 IT 事業者の全てにとって、持続可能なものでなくてはならない。“赤字だが、大阪商工会議所へのお付き合い（社会貢献）で参画する”では、せいぜい 2～3 年しかもたない。

・ 一方、表 2-1 のとおり、お助け実働隊地域 IT 事業者が少なくとも 8 社の実証事業参加に寄与して下さった。今後は、協力を得られる範囲内で、一定のインセンティブのもと、地域支援体制の担い手と地域拡販の結節点としての両方の役割を担う方向で関係性を築いていきたい。

・ また、各地域における需給バランスということにも目配せが必要ではあるが、お助け実働隊地域 IT 事業者に、地元の別のセキュリティベンダー、IT 事業者、情報処理安全確保支援士の紹介を受けるなどして、地域ごとにお助け実働隊地域 IT 事業者を複数事業者確保し、所定サイバーインシデント初動対処の安定供給を図るとともに、当該地域ごとに（あるいは県単位などの広域的に）お助け実働隊地域 IT 事業者の小さなコミュニティ（エコシステム）のようなものを形成しサイバーセキュリティに関する情報交換や若

手人材育成、地場中小企業へのセキュリティ意識向上に資する取り組みなども進めていくことができれば、なお理想的と言える。こうした取り組みには次項で述べる地域展開窓口（各地商工会議所・商工会など）との連携が不可欠となろう。

⑵ 長期にわたり持続可能なサービスとする上でのカギを握る地域展開窓口

・ 本実証事業で初めて地域展開窓口という概念と実体を構築した。実証においては実証参加企業の募集、そして商用サービスにおいては地域におけるサイバーセキュリティ普及やサービス拡販の結節点としての協力を期待している。

・ しかし、商工会議所、商工会、地域金融機関、地域有力企業などは、地域経済を支援する立場にあるものの、他の多くの分野と異なり、サイバーセキュリティに関しては、支援を担えるだけの人材も事業経験も不足気味である。

・ 1 月 14 日に地域展開窓口連絡会議を開催したところ、説明する側（商工会議所や地域金融機関）が、UTM を含め、実証概要を地元中小企業に分かりやすく説明するだけの予備知識が無いことにより「十分な協力ができず申し訳なかった」旨の総括を得るケースが多かった。説明を試みてくれたものの、中小企業から「一体何のことか、よく分からない」という反応が返ってきたそうであり“底辺”を底上げする必要性を指摘している。分かりやすい広報ツールを作成すべきとの意見もあった。説明する側の経営指導員や融資担当者向けに事前レクチャーを希望する声も複数あった。地域展開窓口も中小企業も「理念だけでは動かない」とのことであり、今後の課題となろう。

・ 大阪商工会議所としては、今後、支援機関としての関西の商工会議所・商工会や地域金融機関などにおける意識向上と各地域における中小企業の意識向上の両方を同時に進めてゆかねばならない。コロナ禍にあっては、思惑通りには進まないだろうが、まずは商工会議所・商工会、地域金融機関担当者向けにサイバーセキュリティやお助け隊サービスに関する簡単なレクチャーの場を設けてくれるよう粘り強く働きかけを続けること、定期的な情報交換などの場を設けていき、サイバーセキュリティお助け隊のファンとなってくれるような職員を増やしてゆくこと、などを目指したい。

6.2.6 「商工会議所サイバーセキュリティお助け隊サービス Ver.2.0」に向けて（総括）

「お助け隊サービス Ver.1.0」は、月額利用料金 6600 円（税込）という画期的な低価格を実現し、2020 年 4 月からサービス提供を開始した。緊急事態宣言下という厳しい状況での船出だったとはいえ、販売状況は芳しくない。大企業に協力依頼し、取引先中小企業への説明機会を何度となく提供されたが、なかなか成果には結びつかず、いくつかの課題も見えてきた。

本実証では、1.1.2.で記したとおり、以下の 3 点を課題とした。

① IT 化に遅れがある非大都市の中小企業において、セキュリティを普及させるための分析や販路が不十分。
② with コロナや非大都市、交通の便の悪い地域ではインシデント発生時の支援を提供できていない。
③ セキュリティ対策まで考慮できずにテレワークを始めた中小企業へのセキュリティ対策が現状のお助け隊サービスだけでは十分でない。

②、③については、残念ながら本実証ではサンプル数が不十分で、現段階で「Ver.2.0」として、サービス内容を改善し、新年度からサービス提供するには至らなかった。

ただ、①については、実証スタート時は、地域展開窓口を担った各機関ともサイバーセキュリティへの関心が必ずしも高くなかったのが、1 月 14 日の会議では、今後の協力について、積極的な発言が挙がり、近畿一円でのサービス拡販に期待ができる結果となった。

昨年来、高市早苗・前総務大臣や日本商工会議所の三村明夫・会頭といった方々に、大阪商工会議所の「お助け隊サービス」について説明する機会に恵まれたが、いずれの方からも、実証から商用化したことには一定の評価をしつつも、大阪、近畿に留まらず、全国への展開に期待する声を得た。

もちろん 350 万社と言われる全国の中小企業全てに大阪商工会議所のサービスを提供できるものではないため、サプライチェーン・サイバーセキュリティ・コンソーシアムの活動に合わせ、他の実証事業参加チームと協力し、1 社でも多くの中小企業にお助け隊サービスを提供していきたい。

以上