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）
- 成果報告書（全体版） -

2021年５月

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

目 次

別紙１　サイバーセキュリティお助け隊 実証参加企業事例集

1. 背景・目的

近年、サプライチェーン全体の中で、セキュリティ対策の弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業等への被害が顕在化してきている。具体的には、令和元年 7 月に大阪商工会議所より公表された調査結果によると、30 社の中小企業を調査したところ、30 社全てでサイバー攻撃を受けていたことを示す不審な通信が記録されていた。[1] また、同会議所が同年 5 月に公表した調査では、大企業・中堅企業 118 社に「取引先がサイバー攻撃被害を受け、影響が自社に及んだ経験があるか」を調査したところ、25%の企業が経験ありと回答した。[2]

多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも多く発生している。また、多くの中小企業は IT やサイバーセキュリティに関する知識が乏しく、IT に関するトラブルが発生した際にシステムの不具合が原因なのか、サイバー攻撃が原因であるか自社で判断することは困難である。

こうした状況を踏まえ、経済産業省と独立行政法人情報処理推進機構（IPA）は、令和元年度にトラブル時に相談できる窓口や、サイバー攻撃に遭った際に事後対応を支援するサービス（事後対応支援）を提供する体制構築を目指し、全国 8 地域で「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊事業）」（以下「サイバーセキュリティお助け隊事業」という。）を実施した。1,064 社の中小企業が参加し、実証に取り組んだ結果、延べ 128 件のインシデント対応支援が発生し、そのうち 18 件の駆けつけ支援を実施した。[3]しかしながら、令和元年度のサイバーセキュリティお助け隊事業では、地域特性・産業特性等の考慮が必要であること、人手不足により機器設置対応が困難であり導入負荷を下げる必要があること、セキュリティに関する普及啓発が必要であること、事後対応だけでなく事前対策も必要とする中小企業も多いこと、サービス購入費用が中小企業にとって許容可能な価格である必要があること等が明らかになり、現状は、中小企業への意識喚起が不十分であるとともに、中小企業のニーズに合った製品、サービスが提供されてない状況であることが確認された。

そこで、経済産業省と IPA は、令和 2 年度においても令和元年度の実証の結果を踏まえて、中小企業の実態やニーズをよりきめ細かく把握することで、その実態に即したサービス内容やこれに必要な人材、体制等を明らかにし、中小企業の実態やニーズに合致した持続可能なセキュリティ対策支援体制を構築することで、中小企業のセキュリティ対策強化を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを目的に本事業を実施した。

[1] http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190703cyber.pdf
[2] http://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/190510sc.pdf
[3] https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

2. 事業実施の概要

2.1. 実証事業の内容

本事業では、地域と産業分野の中小企業を対象として、損害保険会社、IT ベンダー、セキュリティ企業、地域の団体等が実施体制を組み、実証事業（サイバーセキュリティお助け隊）を実施した。

また、本事業の実施を通じて、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズ把握を行い、中小企業等に必要なセキュリティ対策の内容（対応範囲や費用等）、マーケティング方法や支援体制、中小企業等向けのサイバーセキュリティ対策の一つとして提供するセキュリティ簡易保険サービスのあり方、実証終了後のサービス提供の可能性を検討した。

以下に実証事業の実施概要図を示す。

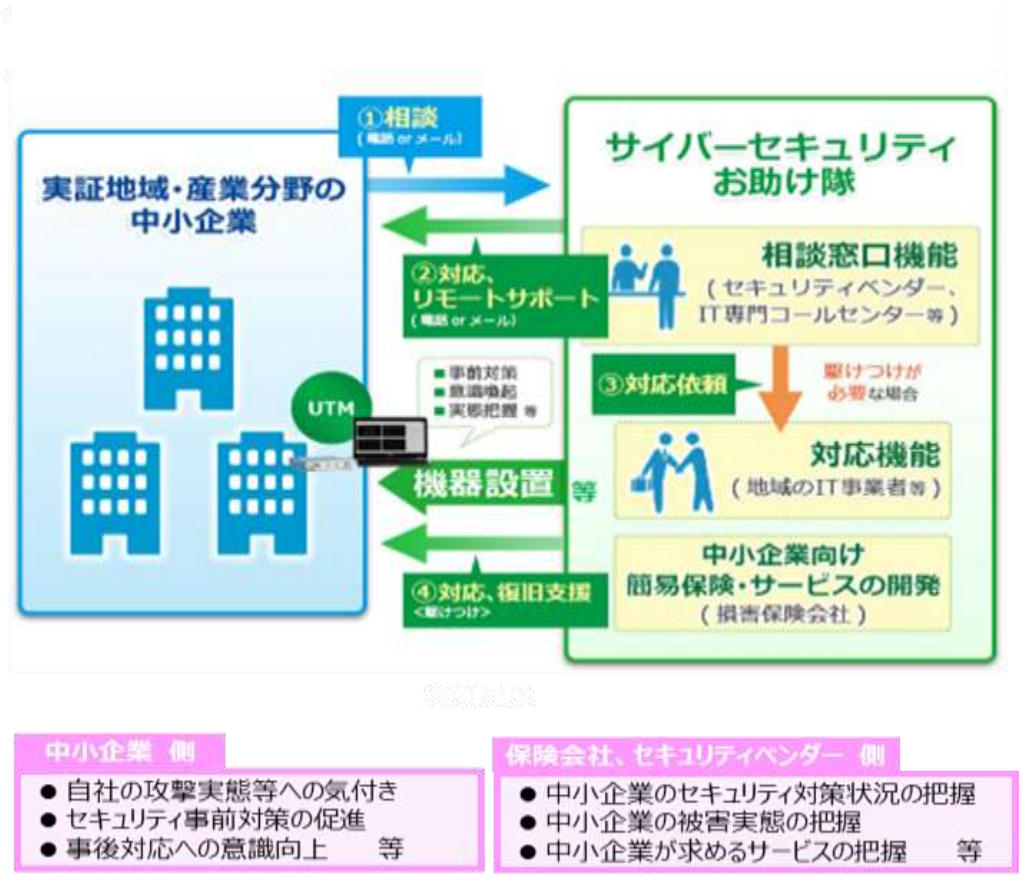


図 1 実証事業の実施概要図

2.2. 実証参加状況

本事業は、公募により全国 13 地域・2 産業分野でサイバーセキュリティお助け隊の請負事業者（事業主体）を選定し、事業主体がそれぞれ実施体制を組織することにより実施された。事業主体が中小企業に実証事業を周知し、参加を呼びかけた結果、**計 1,117 社**の中小企業が本事業に参加した。

以下に、実証が行われた対象地域/産業、事業主体と実施体制、実証参加企業数を示す。

対象地域/産業	事業主体	実施体制	実証参加企業数	
			計画	実績
①北海道	東日本電信電話株式会社	東京海上日動火災保険株式会社	100	**143**
②宮城、山形、秋田、青森	東北インフォメーション・システムズ株式会社	株式会社ハイテックシステム、株式会社アキタシステムマネジメント、あいおいニッセイ同和損害保険株式会社	40	**40**
③岩手	富士ソフト株式会社	東京海上日動火災保険株式会社	70	**71**
④岩手、宮城、福島	株式会社デジタルハーツ	損害保険ジャパン株式会社、東日本電信電話株式会社	50	**56**
⑤千葉、埼玉	富士ゼロックス株式会社	東京海上日動火災保険株式会社	50	**60**
⑥千葉	ＳＯＭＰＯリスクマネジメント株式会社	ちばぎんコンピューターサービス株式会社、株式会社千葉銀行、株式会社ラック、損害保険ジャパン株式会社	50	**66**
⑦岐阜を中心とする中部エリア（岐阜、愛知、三重、静岡）	MS&AD インターリスク総研株式会社	中部電力株式会社、株式会社中電シーティーアイ、中部電力ミライズ株式会社、三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社	50	**76**
⑧愛知、岐阜、三重	名古屋商工会議所	株式会社日立システムズ、西日本電信電話株式会社、東京海上日動火災保険株式会社、損害保険ジャパン株式会社	100	**140**
⑨滋賀、奈良、和歌山	大阪商工会議所	日本電気株式会社、東京海上日動火災保険株式会社、キューアンドエー株式会社	50	**53**
⑩香川	高松商工会議所	株式会社 STNet、キヤノンマーケティングジャパン株式会社、株式会社青柳、四国オフィスオートメーションシステム株式会社、四国特機株式会社、西日本電信電話株式会社、損害保険ジャパン株式会社、東京海上日動火	70	**70**

対象地域/産業	事業主体	実施体制	実証参加企業数	
			計画	実績
		災保険株式会社		
⑪福岡を中心とする九州圏（福岡、佐賀、長崎、熊本、大分、宮崎）	株式会社 BCC	日本電気株式会社、東京海上日動火災保険株式会社、ＮＥＣフィールディング株式会社	50	**54**
⑫熊本	西日本電信電話株式会社	株式会社くまなんピーシーネット、東京海上日動火災保険株式会社、一般社団法人熊本県サイバーセキュリティ推進協議会	100	**105**
⑬沖縄	沖電グローバルシステムズ株式会社	株式会社セキュアイノベーション、ファーストライディングテクノロジー株式会社、損害保険ジャパン株式会社、那覇商工会議所、沖縄電力株式会社	100	**102**
⑭防衛・航空宇宙産業（関東地方、中部地方、関西地方）	株式会社 PFU	株式会社エヴァアビエーション、損害保険ジャパン株式会社、富士通株式会社	50	**50**
⑮自動車産業（静岡県、広島県等）	東京海上日動リスクコンサルティング株式会社	東京海上日動火災保険株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社、NTT セキュリティ・ジャパン株式会社、NTT コムソリューションズ株式会社、ジェイズ・コミュニケーション株式会社	30	**31**
		合計	**960**	**1,117**

※対象地域の北から順に記載

表 1 実証参加状況一覧

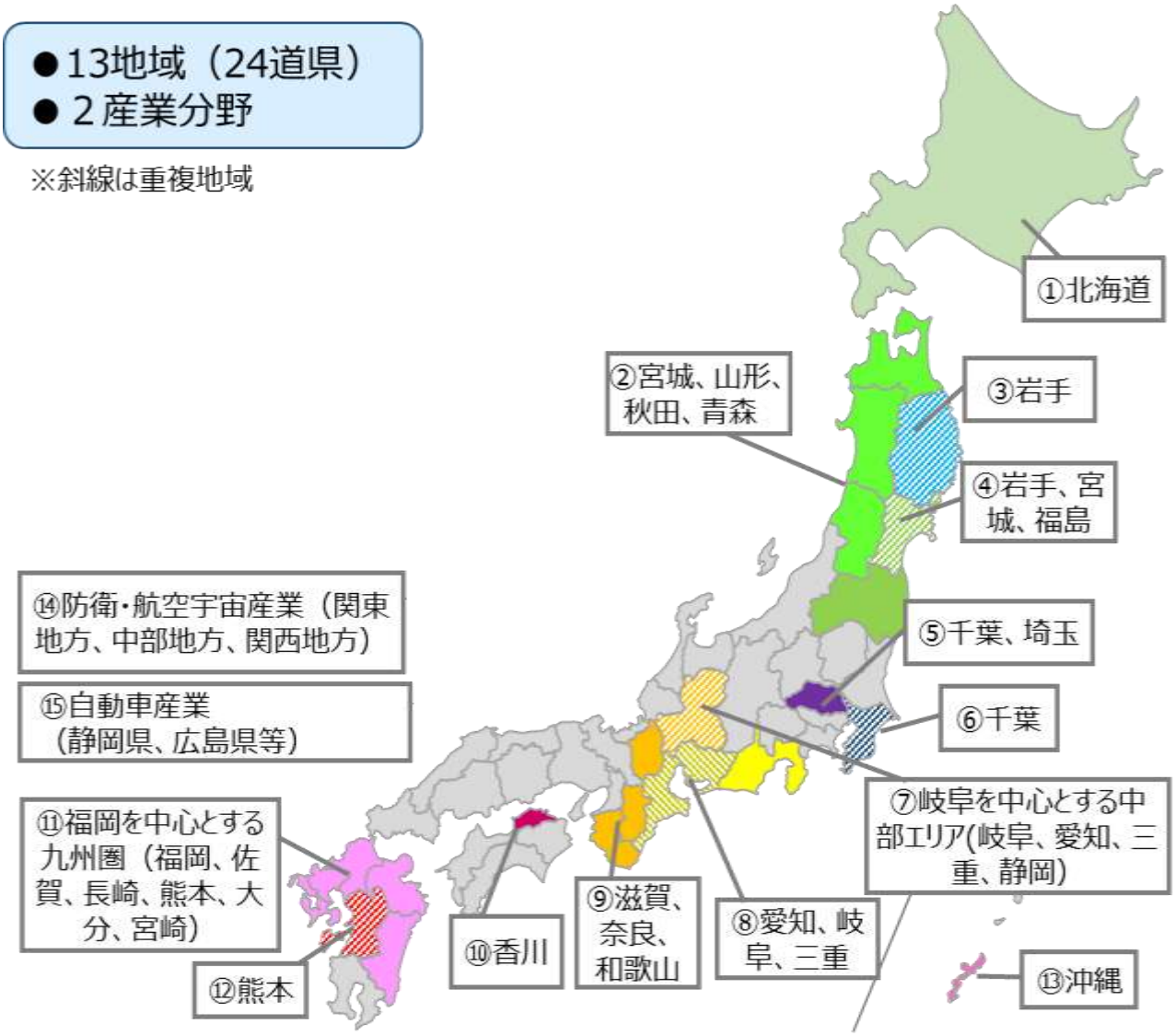


図 2 2020 年度の実証地域

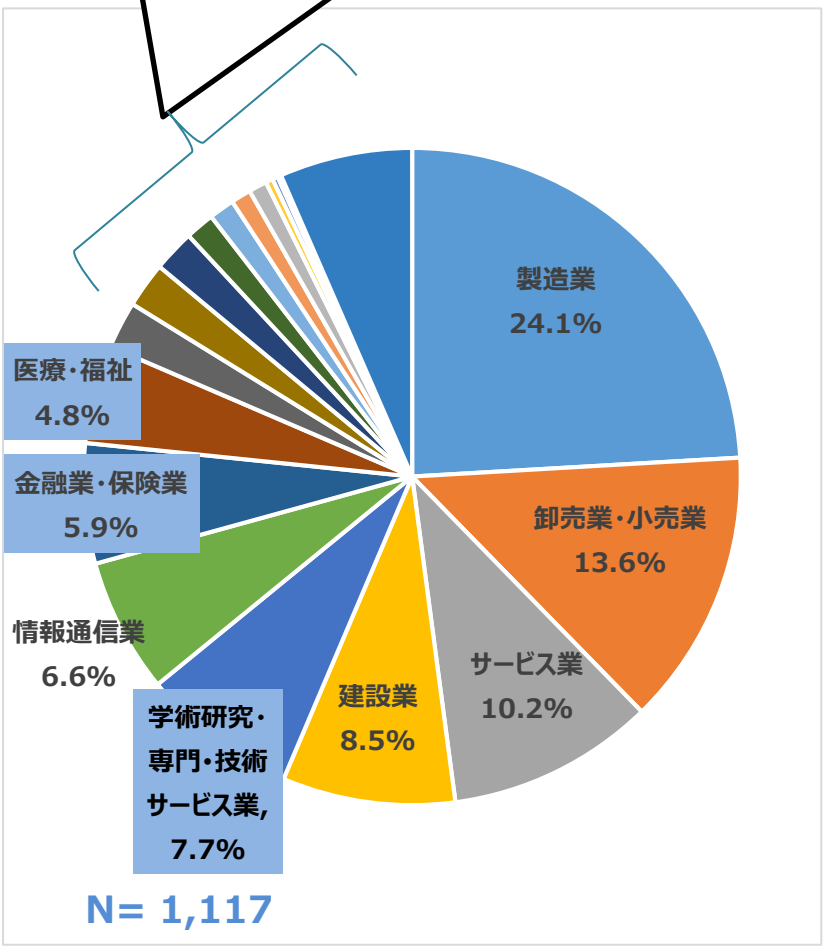
2.3.　実証参加企業の属性

本事業の実証参加企業 1,117 社の属性は以下のとおりであった。

2.3.1.　実証参加企業の業種

実証参加企業の業種別内訳は、「製造業」が 24.1%（269 社）、次いで「卸売業・小売業」が 13.6%（152 社）や「サービス業」10.2%（114 社）など様々な業種より参加があった。

不動産業・物品賃貸業　2.3%、宿泊業・飲食店　2.2%、
運輸業・郵便業　2.1%、教育学習支援業　1.4%、
複合サービス事業　1.3%、生活関連サービス業・娯楽業　1.0%、
農業・林業　0.9%、電気・ガス・熱供給・水道業　0.4%、
鉱業・採石業・砂利採取業　0.3%、公務　0.2%
分類不能の産業　6.5%



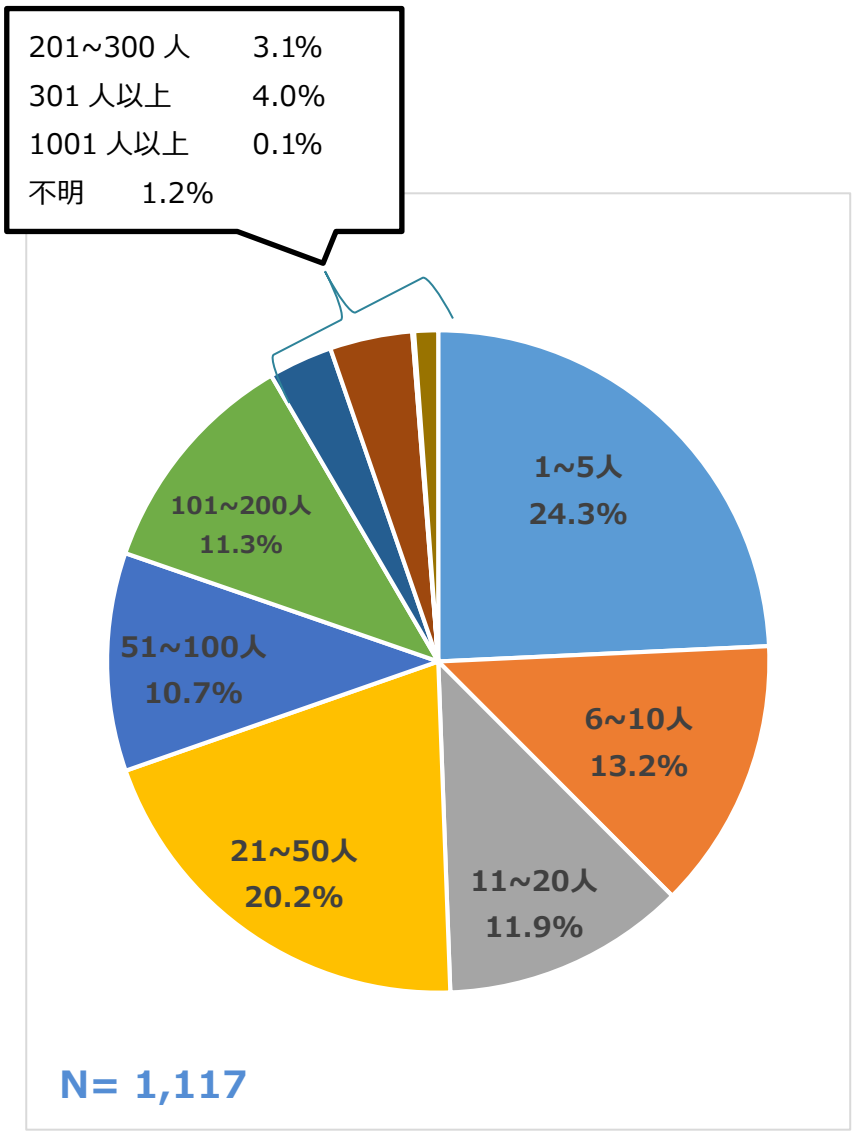
分類:日本標準産業分類(大分類)

業種分類	社数
製造業	269
卸売業・小売業	152
サービス業	114
建設業	95
学術研究・専門・技術サービス業	86
情報通信業	74
分類不能の産業	73
金融業・保険業	66
医療・福祉	54
不動産業・物品賃貸業	26
宿泊業・飲食店	25
運輸業・郵便業	23
教育学習支援業	16
複合サービス事業	14
生活関連サービス業・娯楽業	11
農業・林業	10
電気・ガス・熱供給・水道業	4
鉱業・採石業・砂利採取業	3
公務	2
総計	**1117**

図 3 業種別一覧

2.3.2. 実証参加企業の従業員規模

実証参加企業の従業員数別内訳は、300 人未満が 94.7%であり、「1～5 人」が 24.3%（271 社）、次いで「21～50 人」が 20.2%（226 社）であったものの、「201～300 人」も 3.1%（35 社）含まれるなど多様性があった。



従業員規模	社数
1～5人	271
6～10人	148
11～20人	133
21～50人	226
51～100人	119
101～200人	126
201～300人	35
301人以上	45
1,001人以上	1
不明	13
総計	1,117

図 4 従業員数別一覧

2.4. 事業説明会の実施状況

本事業では、実証に参加する中小企業の募集を行うことと、SECURITY ACTION[4]および中小企業の情報セキュリティ対策ガイドライン[5]の普及に向けた周知啓発活動を目的に、9/7 から 11/26 までに延べ 105 回の事業説明会が事業主体により開催され、その結果 955 名の参加を得た。新型コロナウイルス感染症の影響により集合形式の説明会自体が敬遠された地域も多くあったため、事業主体によっては、オンライン形式のみ、集合形式＋オンライン形式の併用など、様々な形式で開催された。

以下に各事業主体が実施した事業説明会の開催数と参加状況を示す。

事業主体	開催回数	参加社数	参加人数
東日本電信電話	3	24	29
東北インフォメーション・システムズ	1	14	18
富士ソフト	8	50	56
デジタルハーツ	5	不明注)	104
富士ゼロックス	2	23	25
ＳＯＭＰＯリスクマネジメント	2	4	4
MS&AD インターリスク総研	10	19	27
名古屋商工会議所	5	136	136
大阪商工会議所	8	38	41
高松商工会議所	1	34	39
BCC	20	50	59
西日本電信電話	2	83	90
沖電グローバルシステムズ	8	58	74
PFU	25	126	155
東京海上日動リスクコンサルティング	5	46	98
合計	**105**	**705+α**	**955**

注）オンライン開催により社数を把握できなかった

表 2 事業説明会の実施状況

[4] https://www.ipa.go.jp/security/security-action/
[5] https://www.ipa.go.jp/security/keihatsu/sme/guideline/

2.5. 実証参加企業募集に関する状況

本事業では、実証事業への参加を促進するために、事業説明会の開催のほか各事業主体により以下のような取組みが行われた。

事業主体	参加企業募集のためのその他の取組み
東日本電信電話	・商工会議所、法人団体等の各団体の発行する情報誌やメールマガジンを活用した募集 ・自社の顧客基盤への勧奨による募集 ・地方銀行、保険会社の顧客基盤への勧奨による募集
東北インフォメーション・システムズ	・地域行政機関、商工会議所、団体等の協力による周知 ・地方銀行の協力による周知 ・自社の顧客への個別訪問による参加依頼（6 社）
富士ソフト	・地域の行政機関、各経済団体、各商工会議所などの協力による周知（案内チラシの送付、ダイレクトメール配信等） ・保険会社の代理店網を活用した中小企業への参加呼びかけ ・地元有力新聞への広告を掲載および事業紹介記事の掲載 ・個別訪問による参加依頼 実証参加企業の半数以上が個別訪問をきっかけとした参加であった。
デジタルハーツ	・自社およびパートナー企業による開拓（ダイレクトメール配信と地場の営業担当による個別訪問による参加依頼） ・地域の経済団体等の協力による周知（ダイレクトメール配信、会合での事業紹介）
富士ゼロックス	・自社販売会社の顧客への個別訪問による参加依頼 ・地域の IT コーディネーターを通じた周知 ・保険会社の代理店網を活用した中小企業への参加呼びかけ ・サプライチェーンのコア企業からの紹介によるサプライチェーン企業へのアプローチ
ＳＯＭＰＯリスクマネジメント	・個別訪問による参加依頼（169 社） ・会報誌による情報発信（7,000 社） ・メールマガジンを活用した情報発信（3,000 社）

事業主体	参加企業募集のためのその他の取組み
MS&AD インターリスク総研	・地域電力会社の取引先企業を中心に個別訪問による参加依頼 ・県警や業界団体の協力による周知 ・ダイレクトメール配信による勧誘活動
名古屋商工会議所	・Pit-Nagoya 参画企業の取引があるサプライチェーン企業に対するアプローチ ・地域コミュニティ団体の協力によるアプローチ ・損保会社の顧客基盤へのアプローチ
大阪商工会議所	・商工会議所会員への案内チラシの送付およびテレマーケティング ・商工会議所関係企業への個別訪問による参加依頼 ・地域 IT ベンダーによる個別訪問による参加依頼 ・サプライチェーン上流企業からの紹介 ・会議所の広報誌、ダイレクトメール配信、FAX、セミナー開催等 ・店頭チラシ設置（地域金融機関、商工会議所等） ・プレス発表
高松商工会議所	・商工会議所会員のダイレクトメール配信（1984 社） ・商工会議所会員の FAX 送信（104 社） ・個別訪問による参加依頼 ・地元有力新聞の事業紹介記事の掲載
BCC	・地域の経済団体、各商工会議所などの協力による周知（FAX 配信、ダイレクトメール配信） ・個別訪問による参加依頼
西日本電信電話	・地元有力新聞への広告掲載 ・協議会等の媒体への記事提供 ・商工会議所の情報誌

事業主体	参加企業募集のためのその他の取組み
沖電グローバルシステムズ	・個別対応（ダイレクトメール・電話・訪問）による参加依頼 （ダイレクトメール:約 1,800 通、電話:約 200 件、訪問:50 件） ・商工会議所、法人団体等の各団体の発行する情報誌による告知 ・地域行政などの関係機関、団体による SNS、メールマガジンを活用した募集 ・ラジオ CM、事業紹介による告知 ・地域メディア（地元新聞社、テレビ局）による事業紹介の掲載
PFU	・地域の行政機関、各経済団体、各商工会議所などの協力による周知（メールマガジン配信、セミナー開催、チラシ配布等） ・業界開催イベント会場での募集 ・サプライチェーン大手重工メーカーの協力によるサプライチェーン企業へのアプローチ ・個別訪問による参加依頼（約 20 社）
東京海上日動リスクコンサルティング	・大手自動車メーカの取引先サプライヤー企業が加盟する協同組合の協力による募集活動（チラシ配布、ダイレクトメール配信） ・サプライヤー企業の経営者への電話による勧奨等の募集活動

表 3 参加企業募集のためのその他の取組み

2.6. 成果報告会の実施状況

本事業では、実証参加企業および実証地域の中小企業等を対象に、本事業の成果報告を行うことと、SECURITY ACTION および中小企業の情報セキュリティ対策ガイドライン及に向けた周知啓発活動を目的に、延べ 22 回の成果報告会が開催され、その結果 648 名の参加を得た。

以下に各事業主体が実施した成果報告会の開催数と参加状況を示す。

事業主体	開催回数	参加社数	参加人数
東日本電信電話	3	19	46
東北インフォメーション・システムズ	1	18	20
富士ソフト	3	25	26
デジタルハーツ	1	不明注)	34
富士ゼロックス	2	37	39
ＳＯＭＰＯリスクマネジメント	1	9	10
MS&AD インターリスク総研	1	38	63
名古屋商工会議所	1	29	29
大阪商工会議所	1	不明注)	119
高松商工会議所	1	31	32
BCC	2	41	56
西日本電信電話	1	31	31
沖電グローバルシステムズ	1	15	17
PFU	1	22	25
東京海上日動リスクコンサルティング	2	74	101
合計	**22**	**389 +α**	**648**

注）オンライン開催により社数を把握できなかった

表 4 成果報告会の実施状況

3. 事業内容（全体）

3.1. セキュリティ状況等の実態把握

本事業では、実証事業に参加する中小企業から、中小企業向けサイバーセキュリティ事後対応支援体制の構築のために必要な情報（中小企業がさらされているサイバー攻撃の実態、セキュリティ対策状況等）を収集し、セキュリティ状況等の実態把握を行った。

3.1.1. セキュリティ機器等によるサイバー攻撃の実態把握

サイバー攻撃の実態把握は、各事業主体が選定したセキュリティ機器（UTM[6]機器、EDR[7]ソフト等）を実証参加企業に設置（延べ 1.190 社）することにより行った。

以下に各事業主体が実施したサイバー攻撃の実態把握のための取組みを示す。

事業主体	実証参加企業数	セキュリティ機器等によるサイバー攻撃の実態把握	
		内訳	設置社数（延べ数）
東日本電信電話	143	UTM 機器	134
東北インフォメーション・システムズ	40	UTM 機器	40
富士ソフト	71	ネットワークセンサー	71
デジタルハーツ	56	UTM 機器	22
		MDR 付き EDR ソフト	24
富士ゼロックス	60	UTM 機器	36
ＳＯＭＰＯリスクマネジメント	66	UTM 機器	59
		EDR ソフト	51
MS&AD インターリスク総研	76	UTM 機器	50
		EDR ソフト	50
名古屋商工会議所	140	UTM 機器	29
		Defender 監視ツール	6
		Web 対策ツール	41
		メール対策ツール	7

[6] UTM（Unified Threat Management）：複合的なセキュリティ機能を導入して脅威から統合的に保護する手法。

[7] EDR（Endpoint Detection and Response）：端末での脅威を検知してインシデント対応等を支援する手法。

事業主体	実証参加企業数	セキュリティ機器等によるサイバー攻撃の実態把握	
		内訳	設置社数（延べ数）
大阪商工会議所	53	UTM 機器	53
高松商工会議所	70	UTM 機器（キヤノン）	16
		UTM 機器（NTT 西日本）	24
BCC	54	UTM 機器	54
		EDR ソフト	42
西日本電信電話	105	UTM 機器	105
		EDR ソフト	105
沖電グローバルシステムズ	102	UTM 機器	15
		クラウド WAF	8
		簡易 EDR	68
PFU	50	PC の脅威検知	50
東京海上日動リスクコンサルティング	31	UTM 機器	30
合計	**1,117**		**1,190**

表 5 セキュリティ機器等によるサイバー攻撃の実態把握

3.1.2. アンケート等によるセキュリティ対策状況等の把握

セキュリティ対策状況等の把握は、各事業主体が実証開始・終了時や事業説明会・成果報告会開催時に、実証参加企業等にアンケート等を実施することで行った。

以下に各事業主体が実施したアンケート等によるセキュリティ対策状況等把握のための取組みを示す。

事業主体	アンケート等による中小企業の実態把握方法	
	名称	回答社数
東日本電信電話	実証開始時アンケート（事業説明会開催時も含む）	73
	実証終了時アンケート	43
	成果報告会開催時アンケート	7
東北インフォメーション・システムズ	事業説明会開催時アンケート	32
	実証開始時アンケート	30
	サービス希望確認アンケート	29
	サービス体験後アンケート	21
	成果報告会開催時アンケート	18
	テレワークに関するアンケート	13
富士ソフト	事業説明会・成果報告会開催時アンケート	90
デジタルハーツ	実証開始時アンケート（実証参加者）	59
	成果報告会開催時アンケート	22（名）
富士ゼロックス	事業説明会開催時アンケート	8
	標的型メール訓練後アンケート	14
	実証終了時アンケート（成果報告会開催時も含む）	18
ＳＯＭＰＯリスクマネジメント	セキュリティに関する事前アンケート	65
	セキュリティに関する事後アンケート	12
MS&AD インターリスク総研	実証事業の効果検証アンケート	51
	成果報告会開催時アンケート	42
	事後ヒアリング	5
名古屋商工会議所	事業説明会開催時アンケート	136
	成果報告会開催時アンケート	29
大阪商工会議所	実証開始時アンケート（実証参加者）	50
	テレワークアンケート	37
高松商工会議所	事業説明会開催時アンケート	72
	成果報告会開催時アンケート	45

事業主体	アンケート等による中小企業の実態把握方法	
	名称	回答社数
BCC	サイバーセキュリティに関するアンケート	43
	成果報告会開催時アンケート	39
西日本電信電話	ICT 実態調査アンケート（2 回実施）	147
		225
	参加企業のセキュリティ対策事前アンケート	104
	標的型攻撃メール訓練およびインシデント対応アンケート	90
	実証終了時アンケート	82
沖電グローバルシステムズ	実証開始時アンケート（実証参加者）	85
	実証終了時アンケート（成果報告会開催時も含む）	25
PFU	事業説明会開催時アンケート	9
	セキュリティ意識調査アンケート（2 回実施）	50
		32
	データ共有に関する運用ヒアリング	11
	成果報告会開催時アンケート	13
	工場ネットワークについてのヒアリング	6
東京海上日動リスクコンサルティング	セキュリティ実態把握アンケート（セキュリティセミナー）	64
	事業終了時アンケート（成果報告会開催時も含む）	69

表 6 アンケート等によるセキュリティ対策状況等の把握

3.1.3. 脆弱性診断等によるセキュリティ対策状況等の把握

脆弱性診断等によるセキュリティ対策状況の把握は、各事業主体が実証参加企業等（959 社） にセキュリティ診断等を実施することで行った。

以下に各事業主体が実施した脆弱性診断等によるセキュリティ対策状況等把握のための取組みを示す。

事業主体	脆弱性診断等によるセキュリティ対策状況等の把握	
	診断方法	実施社数
東日本電信電話	Web セキュリティ診断	108
東北インフォメーション・システムズ	脆弱性診断	3
	制御システム簡易リスクアセスメント	2
富士ソフト	簡易セキュリティ診断	71
デジタルハーツ	脆弱性診断（簡易）	43
	脆弱性診断（詳細）	5
富士ゼロックス	専門家によるヒアリング	53
ＳＯＭＰＯリスクマネジメント	公開情報の外部評価	57
MS&AD インターリスク総研	簡易セキュリティ診断	53
名古屋商工会議所	簡易セキュリティアセスメント	140
大阪商工会議所	簡易セキュリティ診断	57
高松商工会議所	簡易セキュリティ診断	72
BCC	セキュリティ簡易診断アセスメント	48
沖電グローバルシステムズ	Web アプリケーション診断	33
	プラットフォーム診断	23
PFU	情報セキュリティ整備状況診断	50
	社内 PC の脆弱性診断	50
東京海上日動リスクコンサルティング	外部診断	30
	内部診断（社内 PC の脆弱性診断）	31
	マルウェア対策診断	30
合計		959

表 7 脆弱性診断等によるセキュリティ対策状況等の把握

3.1.4. 標的型メール訓練によるセキュリティ対策状況等の把握

セキュリティ訓練によるセキュリティ対策状況の把握は、各事業主体が実証参加企業等（370 社） に標的型メール訓練を実施することで行った。

以下に各事業主体が実施したセキュリティ訓練等によるセキュリティ対策状況等把握のための取組みを示す。

事業主体	実施社数
東日本電信電話	140
東北インフォメーション・システムズ	18
デジタルハーツ	56
富士ゼロックス	15
MS&AD インターリスク総研	51
高松商工会議所	30
西日本電信電話	60
合計	**370**

表 8 セキュリティ訓練等によるセキュリティ対策状況等の把握

3.2. セキュリティ機器等によるサイバー攻撃実態把握

3.2.1. 検知および監視の仕組みと実証結果

本事業では、事業主体ごとにセキュリティ機器等によるサイバー攻撃の検知および監視の仕組みを構築し、相談受付および対応体制と共に、検知および監視した結果がサイバーインシデント[8]等であるか判断する体制、サイバーインシデント等が発生した際の支援体制を併せて構築した。

以下に事業主体ごとのセキュリティ機器等による提供サービス内容、設置社数、検知および監視の仕組みとその実証結果を示す。

(1) 東日本電信電話（実証対象：北海道）

セキュリティ機器	＜UTM＞「おまかせサイバーみまもり」サービス」	**設置社数（延べ数）**	**134** 社
提供内容	UTM 機器を設置し、通信監視・ログ把握による不正アクセス等の状況を把握する。 各企業のセキュリティ対策状況に応じた、更に必要となる対策を個別にレコメンド提供する。 一元窓口（サポートデスク）による各種困りごと受付、インシデント判断、遠隔・訪問サポートを行う。		
実証結果	不正侵入（IPS[9]）は実証参加企業の約 80%で検知し、スパムメールは実証参加企業の約 69%で検知した。 ランサムウェアを実証期間内で 129 件検知した参加企業もあり、集中的にサイバー攻撃を受けている企業も存在していることが確認された。		

表 9 UTM によるセキュリティ対策状況等の確認結果（東日本電信電話）

[8] サイバーインシデント：ネットワークへの不正侵入やマルウェア感染、Web サーバーの改ざんなどのサイバー攻撃等により、セキュリティ上のリスクが発現・現実化した事象のこと。

[9] IPS(Intrusion Prevention System)：侵入防止システム

図 5 検知および監視の仕組み（東日本電信電話）

(2) 東北インフォメーション・システムズ（実証対象：青森県、秋田県、宮城県、山形県）

セキュリティ機器	＜UTM＞ FortiGate（Fortinet 社製） WatchManBox MR（株式会社ハイテックシステム社製）	**設置社数（延べ数）**	**40** 社
提供内容	UTM を設置し、ログを監視・分析を行う。 インシデントを検知した場合は、電子メールにて実証企業へ通知し、インシデント対応支援を行う。 セキュリティログを分析した結果をレポートに取りまとめ、月に一回レポートを提供する。		
実証結果	外部からの不正アクセスは、110 件検知し、防御した。 マルウェア[10]を 115 件検出し、駆除した。 ・Web サイト経由で送られたマルウェア:48 件 ・電子メール経由で送られたマルウェア:67 件		

表 10　UTM によるセキュリティ対策状況等の確認結果（東北インフォメーション・システムズ）

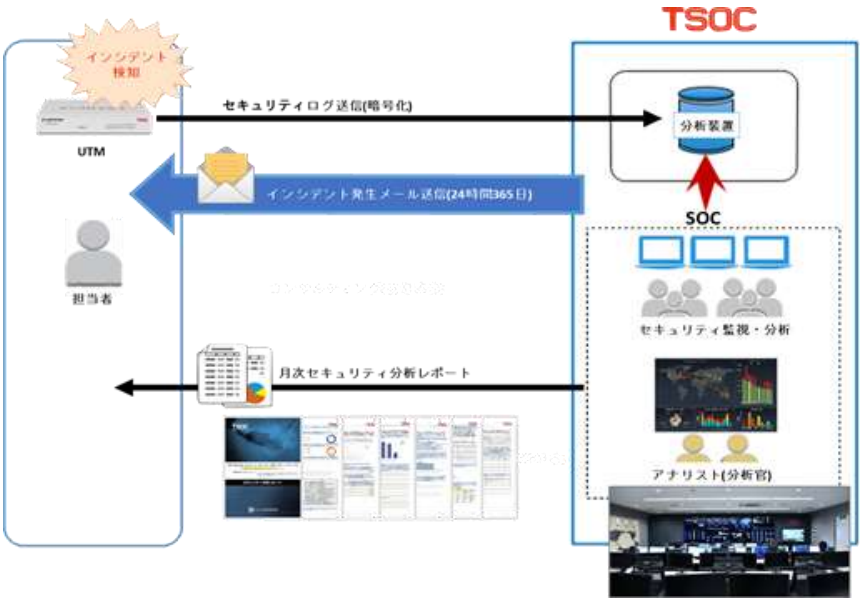


図 6 検知および監視の仕組み（東北インフォメーション・システムズ）

10 マルウェア：コンピュータの正常な利用を妨げたり、不正に動作させる目的で作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる。

(3) 富士ソフト（実証対象：岩手県）

セキュリティ機器	＜ネットワークセンサー＞ オフィス SOC および おうち SOC	**設置社数（延べ数）**	**71** 社
提供内容	対象企業の IT 環境内に、ネットワークセンサーを設置し、対象企業のオフィス環境およびテレワーク環境におけるネットワーク挙動をセキュリティ監視システムとアナリストにて、監視、分析する。セキュリティ監視システムにて検出したアラートをアナリストが分析した結果、通報が必要と判断したものをインシデントとして、対象企業に通知し、インシデント対応支援を行う。		
実証結果	水面下で侵攻するサイバー攻撃の状況をセキュリティ監視システムにて観測・収集し、AI 基準で洗い出した結果、合計 3,539 件のアラートを検出した。この結果を基に専門家による分析を行い、7 件通報が必要と判断し、インシデントとして対象企業に通報し、リモートでの対処を実施した。 ・迷惑メールに分類されるソフトウェアの利用痕跡を検出（アドウェア[11]感染）。通報し削除等の対応を実施した。 ・フィッシングサイトへアクセスした痕跡を検出。通報し、利用者の特定と情報入力していないかの確認と対策を実施した。 ・不審な IP アドレスからインターネット上の公開端末に URL スキャンが実施され、レスポンスを返していたことを検出（不正な URL スキャンへの応答）。通報し、公開している端末のログイン履歴確認と脆弱性対策を実施した。		

表 11 ネットワークセンサーによるセキュリティ対策状況等の確認結果（富士ソフト）

[11] アドウェア：広告を表示する機能を持つソフトウェアだが、ユーザの意思とは無関係にインストールされ、広告を強制的に表示する迷惑ソフトや、無断で情報を収集して提供元などに送信するスパイウェアもある。

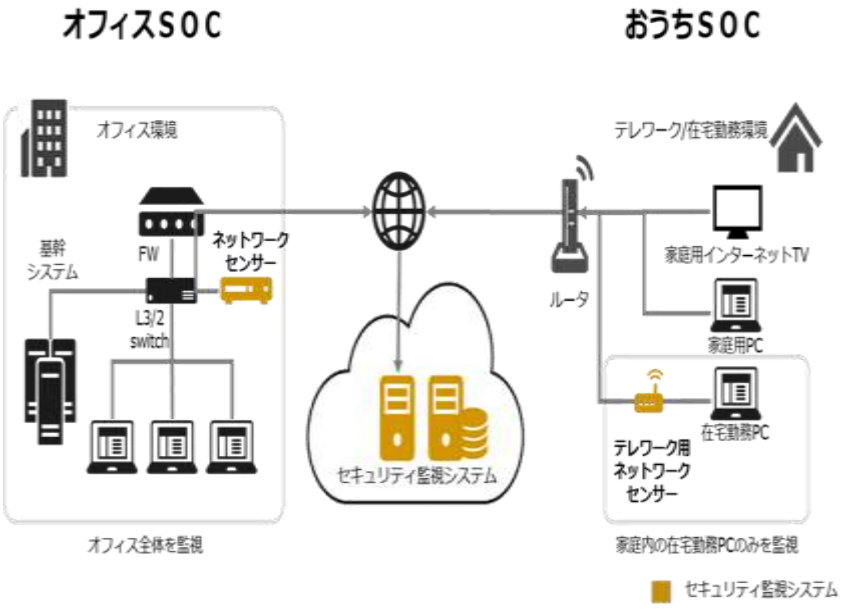


図 7 検知および監視の仕組み（富士ソフト）

(4) デジタルハーツ（実証対象：岩手県、宮城県、福島県）

① UTM 機器

セキュリティ機器	＜UTM＞ Cloud Edge（トレンドマイクロ社）+「おまかせサイバーみまもり」サービス（NTT 東日本）	**設置社数（延べ数）**	**22** 社
提供内容	対象企業のネットワークに UTM を設置し、セキュリティ対策を強化するとともに、通信状況をモニタリングする。 不正通信を行った場合などのインシデント発生の際には原因究明・環境復旧のサポートを行う。		

表 12 UTM によるセキュリティ対策状況等の確認結果（デジタルハーツ）

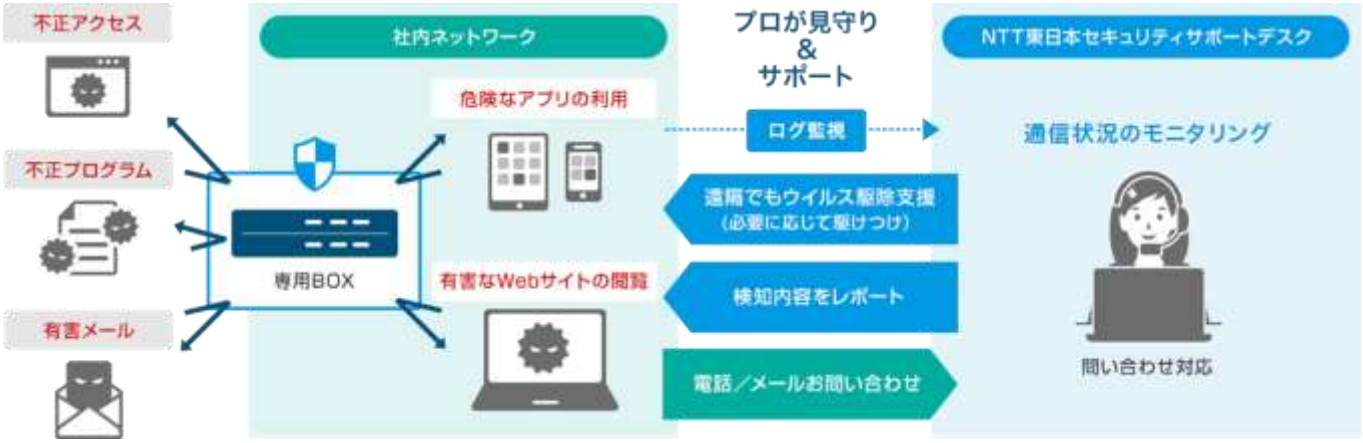


図 8 UTM の検知および監視の仕組み（デジタルハーツ）

② EDR ソフト

セキュリティ機器	<EDR> Intercept X Advanced with EDR（Sophos 社）	**設置社数（延べ数）**	**24** 社
提供内容	対象企業の各クライアント端末に EDR クライアントをインストールし、常時監視により適切な対応（専門家の解析、脅威除去支援、再発防止施策支援）を行う。		

表 13 EDR によるセキュリティ対策状況等の確認結果（デジタルハーツ）

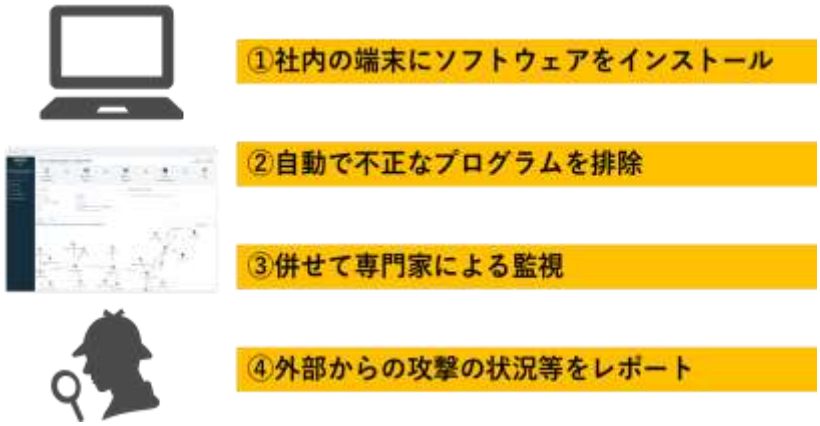


図 9 EDR の検知および監視の仕組み（デジタルハーツ）

【実証結果】

アラート件数は、下図のとおりであった

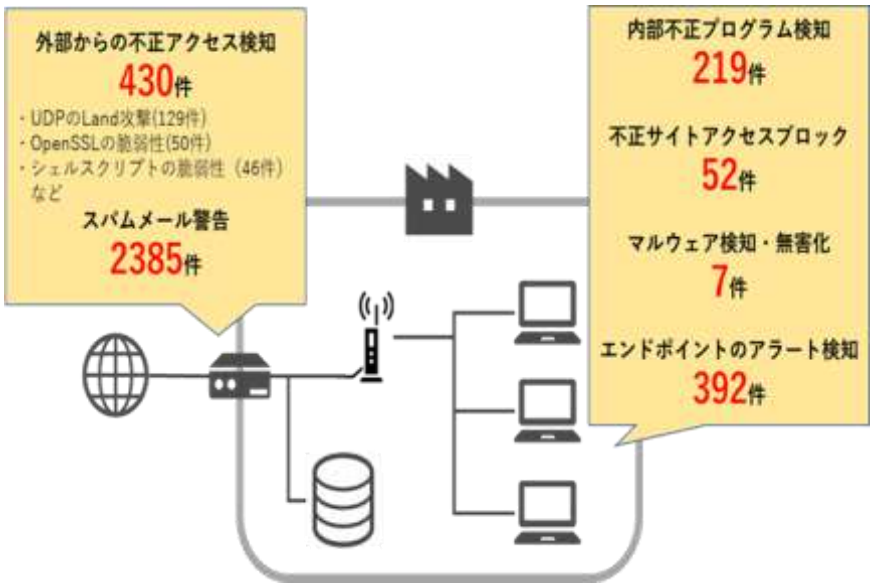


図 10 アラート件数一覧（デジタルハーツ）

(5) 富士ゼロックス（実証対象：千葉県、埼玉県）

セキュリティ機器	＜UTM＞ beat-box（富士ゼロックス社）	**設置社数（延べ数）**	**36** 社
提供内容	実証参加企業に UTM 端末を設置し、調査期間中に収集したログ情報を分析し、グラフ等で可視化したレポートを実証参加企業に提供する。 異常を検知した場合は、ポート完全遮蔽により不正通信をブロックし、コンタクトセンターにて情報把握と対応を行う。		
実証結果	・検知した ping/port-scan は、78 ヵ国から合計 17,958 件、1 日あたり約 17 件/台の偵察行為を受けていた。 ・不正と考えられる内部から外部への通信検知数は 139,109 件、1 日あたり約 86 件/台に上った。 ・ブロックした Web サイト数は 364,413 件、1 日あたり約 191 件/台、外部へのアクセスをブロックした。 ・10 月に埼玉県で請求書を装うなりすましメールを 1 件、 12 月には千葉県でウイルス感染している可能性のある報告書が添付されたメールが 3 日間に渡って同じ企業に送付される事象が確認された。（いずれも UTM で防御） ・全受信メール中、約 11%でスパムメールを検知、1 日あたり約 8 件/台のスパムメールを受信していた。		

表 14 UTM によるセキュリティ対策状況等の確認結果（富士ゼロックス）

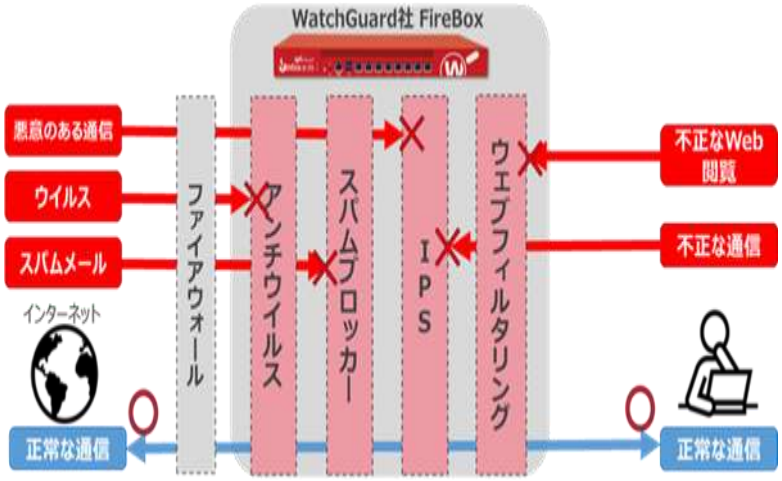
図 11 検知および監視の仕組み（富士ゼロックス）

⑹　ＳＯＭＰＯリスクマネジメント（実証対象：千葉県）

①　UTM 機器

セキュリティ機器	＜UTM＞ Firebox シリーズ（Watchguard 社）	設置社数（延べ数）	59 社
提供内容	UTM 機器のセンサー（ファイアウォール機能、IPS 機能、ウェブフィルタリング機能[12]、スパムフィルタ機能およびアンチウイルス機能）によりセキュリティインシデントを検出する。また、ログを「セキュリティログ自動分析システム」に送信し分析し、3 段階のランク付けを行い可視化する。		
実証結果	トロイの木馬、アドウェアといったウイルス侵入を、約 14%の企業で検出され、駆除した。 スパムメールの侵入を、約 73%の企業で検知され、防御した。 不正侵入（IPS）は約 32%の企業で検知され、防御した。 悪意のある Web サイトへの接続を、約 88%の企業で検知され、防御した。 UTM の不正侵入（IPS）では検出できなかった**「不正な IP アドレスへの通信」が成立していること**を SOC 機能[13]にて検知し、緊急度「高」のアラートを発信し、**リモートによる支援**を実施した。		

表 15 UTM によるセキュリティ対策状況等の確認結果（ＳＯＭＰＯリスクマネジメント）



[12] ウェブフィルタリング機能：有害な Web サイトや危険性のある Web サイトへのアクセスを制限または拒否する機能

[13] SOC(Security Operation Center)： ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対策のアドバイスを行う組織

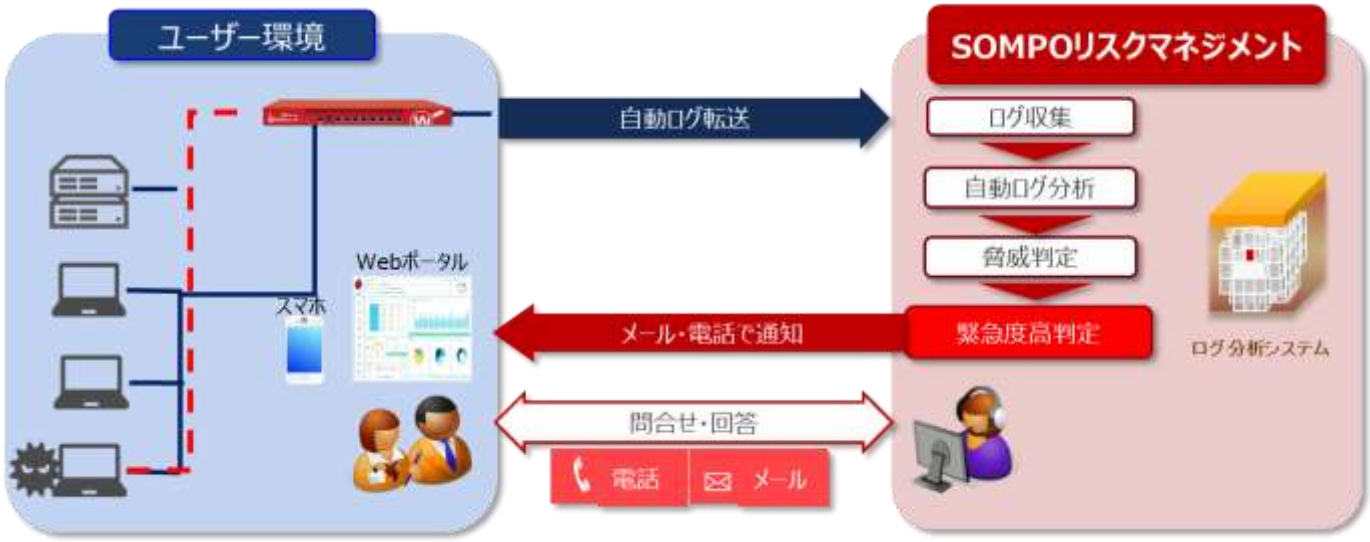


図 12 検知および監視の仕組み（ＳＯＭＰＯリスクマネジメント）

② EDR ソフト

セキュリティ機器	＜EDR＞ エンドポイントセキュリティ対策ソフトウェア（ＳＯＭＰＯリスクマネジメント社）	**設置社数（延べ数）**	**51** 社
提供内容	エンドポイントセキュリティ対策ソフトウェアを用いて、パソコンの挙動ログを収集し、セキュリティエンジニアが分析することで、不正プログラムの感染などのセキュリティインシデントを検出する。		
実証結果	不正プログラムが 75%の企業で検出され、駆除した。 不正なプログラムを配布しているサイトといった不正なサイトへのアクセスについても 47%の企業で検出され、防御した。 **ブラウザ・ハイジャッカー**[14]を検知し、駆除方法を案内したが自力で対応出来なかったため、**リモートで駆除**を実施した。		

表 16 EDR によるセキュリティ対策状況等の確認結果（ＳＯＭＰＯリスクマネジメント）

[14] ブラウザ・ハイジャッカー：ユーザーの Web ブラウザの設定をユーザーの意思とは無関係に変更したり、有害サイトの広告やページを表示したり、ツールバーをインストールしたりするウイルスの一種

図 13 検知および監視の仕組み（ＳＯＭＰＯリスクマネジメント）

(7) MS＆AD インターリスク総研（実証対象：岐阜県を中心とする中部エリア）

① UTM 機器

セキュリティ機器	＜UTM＞ CloudEdge（トレンドマイクロ社）	設置社数（延べ数）	50 社
提供内容	UTM の提供、監視サービス、各種照会が可能なコールセンター、有事の駆けつけをワンストップで提供する。 ・異常通信や振る舞いを検知・駆除する。 ・脅威検知内容をレポート化して参加企業に報告する。（月 1 回）		
実証結果	・UTM 設置してすぐに「C&C コールバック（C&C サーバ[15]との通信）」と見られる通知を検知、防御し、リモートによるインシデント対応を実施した。 ・IPS（侵入防御システム）にて検知、防御が必要な通信を多数検知（約 8 万件）し、中小企業においてもサイバー攻撃の標的とされていることが確認された。 ・スパムメール対策機能による検知・駆除は、計 23 万件にものぼった。 ・ランサムウェアを 1 社で検知したものの、UTM で防御しており、感染被害はなかった。		

表 17 UTM によるセキュリティ対策状況等の確認結果（MS＆AD インターリスク総研）

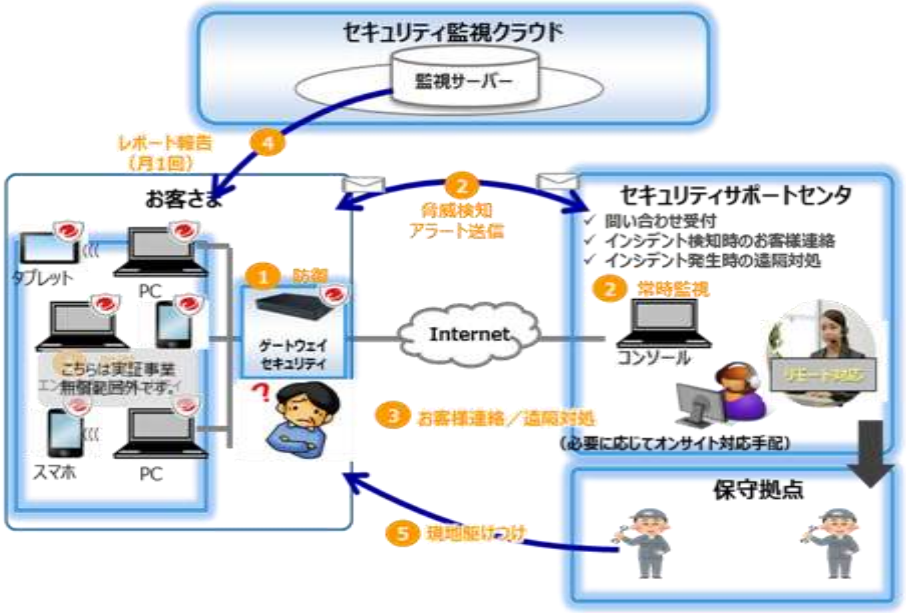


図 14 検知および監視の仕組み（MS&AD インターリスク総研）

[15] C&C サーバー（command and control server）：外部から侵入して、乗っ取ったコンピュータを踏み台にして制御したり命令を出したりする攻撃側のサーバー。

② EDR ソフト

セキュリティ機器	＜EDR＞ 防検サイバー（MS&AD インターリスク総研）	設置社数（延べ数）	50 社
提供内容	EDR 導入による端末の遠隔監視、ログ保存、AI とアナリストによる防御・検知機能を提供し、コールセンターによる問い合わせ窓口の設置および異常と判断した場合の駆けつけ支援を行う。		
実証結果	「不審なコマンド実行」や「不審なプロセス起動」を合計 1 万件検知したが、アナリストによる調査の結果、大半が過検知によるものであった。 サポートが終了したメンテナンスされないソフトウェア（プラグイン）の振る舞いを検知したため、注意喚起を行った。		

表 18 EDR によるセキュリティ対策状況等の確認結果（MS＆AD インターリスク総研）

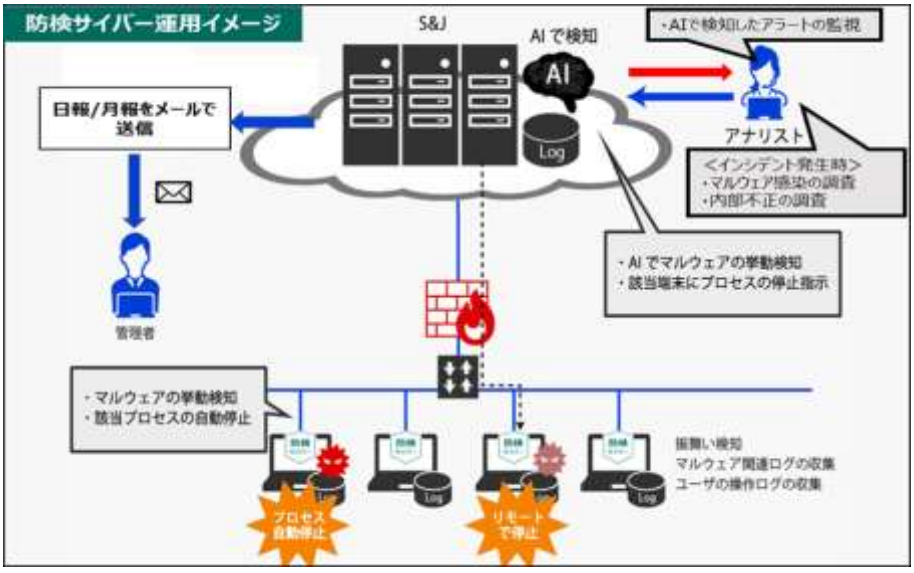


図 15 検知および監視の仕組み（MS&AD インターリスク総研）

(8) 名古屋商工会議所（実証対象：愛知県、岐阜県、三重県）

① UTM 機器

セキュリティ機器	<UTM> CloudEdge（トレンドマイクロ社）	設置社数（延べ数）	29 社
提供内容	導入企業のネットワーク上に統合脅威管理装置（UTM）を設置し、不正通信を抑止、インシデントのリモート監視を行う。インシデント発生時にはコールセンターからの遠隔サポートを行う。また、UTM による防御状態について毎月レポートを送付する。		
実証結果	不正サイトへのアクセスを合計で 400 万件超、検知・防御した。 これは導入企業 1 社 1 日平均で 500 件超の検知数であり、中小企業においても日々サイバー攻撃の脅威にさらされている実態を確認した。 マルウェアの検知・駆除で 19 件、不正アクセス検知・防御で 576 件の防御実績があった。		

表 19 UTM によるセキュリティ対策状況等の確認結果（名古屋商工会議所）

図 16 検知および監視の仕組み（名古屋商工会議所）

② Web 対策ソフト

セキュリティ機器	＜Web 対策ツール＞ i-FILTER（デジタルアーツ社）	**設置社数（延べ数）**	**41** 社
提供内容	導入企業の監視対象 PC へ i-FILTER（Agent）をインストールし、危険サイト閲覧を防止する。i-FILTER は、Web フィルタリングソフトに当たるが、マルウェア等の通信先である不正サイトへの通信において、ブラウザーを使用しない場合でも遮断することが可能である。		
実証結果	不正サイトへのアクセスを合計 624 件、検知・防御した。 そのほとんどが、「違法ソフト・反社会的サイト」であった。 導入企業の 75%の企業は、ブロック数は 10 回以下であったが、1 部の企業ではブロック数が 200 回近くに上る企業もあった。		

表 20 Web 対策ソフトによるセキュリティ対策状況等の確認結果（名古屋商工会議所）

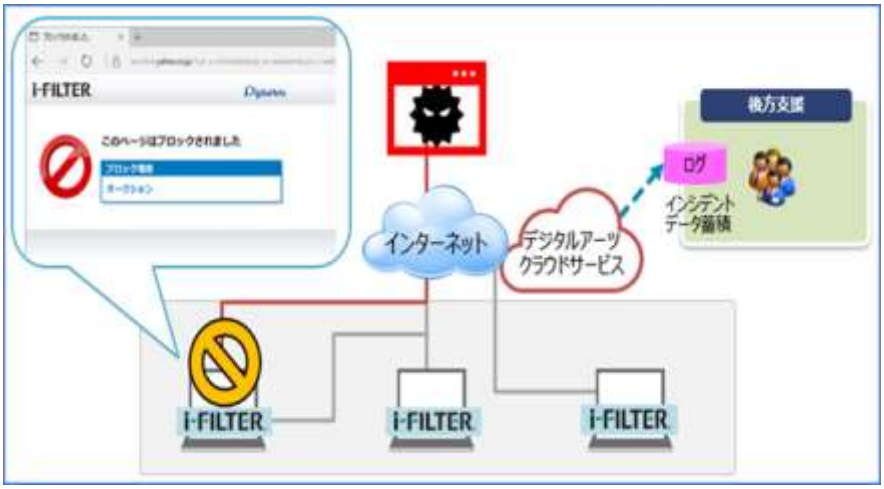


図 17 検知および監視の仕組み（名古屋商工会議所）

③　メール対策ソフト

セキュリティ機器	＜メール対策ツール＞ m-FILTER@Cloud（デジタルアーツ社）	**設置社数（延べ数）**	**7** 社
提供内容	メール受信時に「送信元」「添付ファイル」「本文・URL」の偽装判定を行い、安全なメールだけを受信する。 危険なメールは隔離およびメール無害化を実施する。		
実証結果	セキュリティインシデントとして、標的型攻撃メール（疑い）の検知はなかったが、スパムメール受信を 60 件検知し、防御した。		

表 21　メール対策ソフトによるセキュリティ対策状況等の確認結果（名古屋商工会議所）

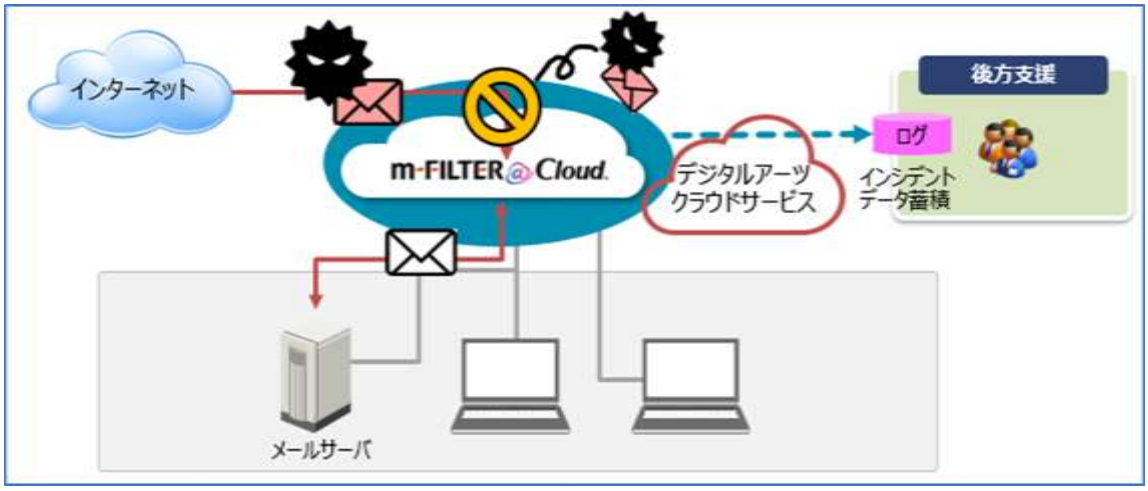


図 18 検知および監視の仕組み（名古屋商工会議所）

(9) 大阪商工会議所（実証対象：滋賀県、奈良県、和歌山県）

セキュリティ機器	＜UTM＞ 簡易 UTM 機器（NEC 社）	**設置社数（延べ数）**	**53** 社
提供内容	UTM をインターネット接続機器と監視対象端末（PC,モバイル機器など）の間に設置し、企業 LAN とインターネットの通信を監視する。 感染が疑われる場合、「重要アラート」として参加企業へメール通知し、駆けつけ支援又はリモート支援を行う。		
実証結果	「外部からの攻撃」を約 56%（30 社）の企業において検知・防御した。 「外部への不正通信」「内部の脆弱性」を 43%（23 社）の企業において検知・防御した。 UTM がトロイの木馬を検知し、アラート通知。アラート通知をきっかけに、当該企業から相談を受け、リモート支援を実施し、フルスキャンを実施した結果、内在していた別の脅威を検出し、合わせて駆除した。		

表 22 UTM によるセキュリティ対策状況等の確認結果（大阪商工会議所）

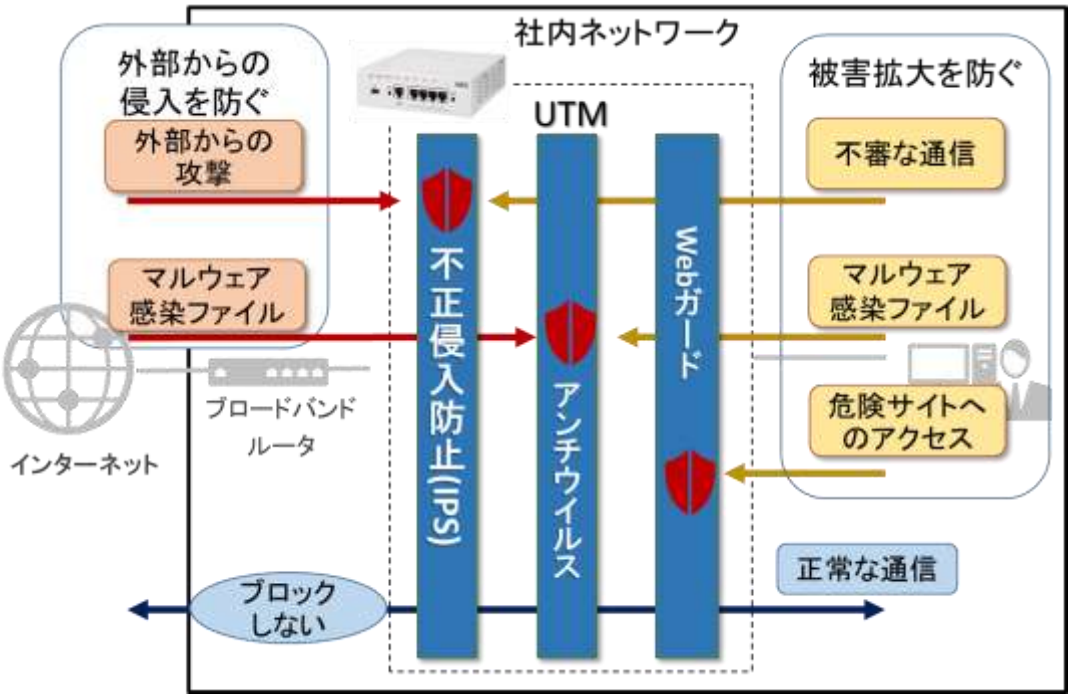


図 19 検知および監視の仕組み（大阪商工会議所）

(10) 高松商工会議所（実証対象：香川県）

① UTM 機器①

セキュリティ機器	＜UTM①＞ HOME ネットワークセキュリティサービス（キヤノンマーケティングジャパン社）	**設置社数（延べ数）**	**16** 社
提供内容	実証参加企業に UTM を設置し、通信ログを収集、レポート配信する。 正常稼働を監視し、障害発生時にはコンタクトセンターから遠隔サポートおよび保守委託拠点から駆け付けサポートを行う。		
実証結果	DoS/DDoS 攻撃が 70%の企業で検知され、防御した。 スパムメールが 18%の企業で検知された。その多くはショッピングサイト、インターネット通販事業者からのメールがスパムメールと判定されていたが、一部不審なドメインも散見され、フィッシングサイトへ誘導するようなメールの可能性もあった。 URL フィルタリング検知は、全ての参加企業において検知された。その多くは、アダルト／兵器・武器／ショッピングなどのサイトへのアクセスであったが、マルウェア／フィッシングサイト／違法ソフトへのアクセスが約 1 割見られた。		

表 23 UTM①によるセキュリティ対策状況等の確認結果（高松商工会議所）

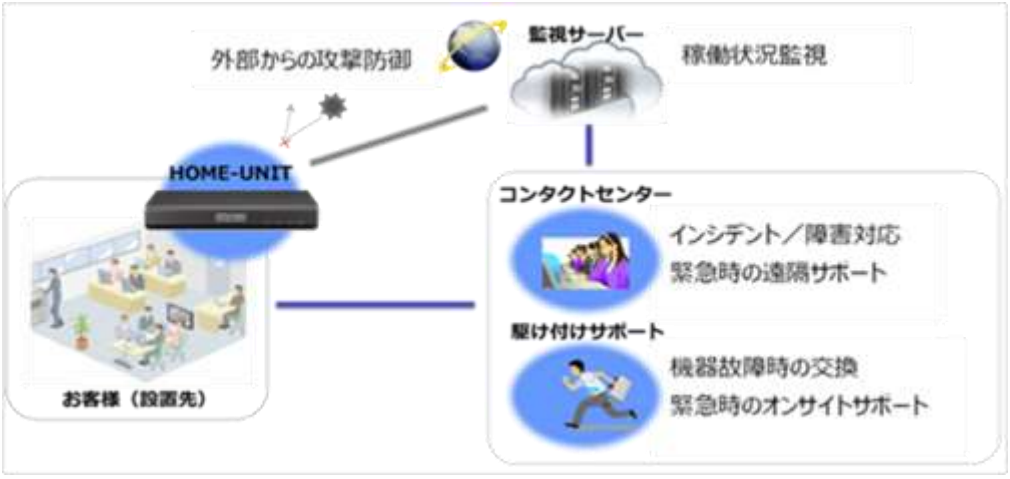


図 20 検知および監視の仕組み（高松商工会議所）

② UTM 機器②

セキュリティ機器	＜UTM②＞ セキュリティおまかせプラン（NTT 西日本社）	設置社数（延べ数）	24 社
提供内容	実証参加企業に UTM を設置し、通信ログを収集する。 セキュリティ脅威の検知状況をまとめたレポートを送付する。（月 1 回） インシデント検知時はサポートセンタから連絡し、必要に応じて現地駆けつけ対応を行う。		
実証結果	ランサムウェアが 27 件検知され、防御したが、1 社のみ特定の日に 1 つの Web サイトにて検知されていた。 スパムメールが計 43,887 件検知されたが、11 月に検知数が大幅に増えており※1、JPCERT/CC 等から注意喚起されている、「Emotet」および「IcedID」等の攻撃があったと推測される。		

表 24 UTM②によるセキュリティ対策状況等の確認結果（高松商工会議所）

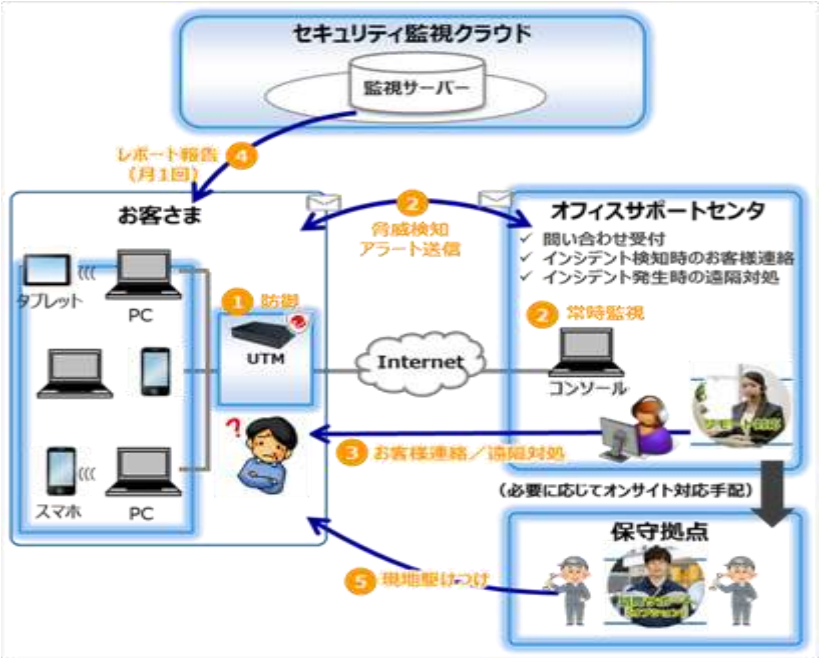


図 21 検知および監視の仕組み（高松商工会議所）

(11) BCC　（実証対象：福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県）

①　UTM 機器

セキュリティ機器	＜UTM＞ サイバーセキュリティ見守りサービス（NEC 社）	**設置社数（延べ数）**	**54** 社
提供内容	中小企業が容易に設置および運用できるよう設計した UTM で通信を監視し、不正な通信の遮断やウイルスの無害化、有害 Web サイトへのアクセス遮断を行う。 サイバーインシデントと判断された場合、相談窓口がリモートサポートによる対応もしくは駆け付け対応を行う。		
実証結果	UTM により外部からの攻撃や外部への不正通信を検知および遮断した社数は、24 社 特定の 1 社にて、UTM 設置後、毎日 10 件程度検知された。※1 検収件数が突出している 2 社は、「情報通信業」であった。 「アドウェア」に分類されるマルウェアを 1 件検知し、駆けつけ対応により駆除を行った。ヒアリングした結果、不正プログラムはインターネットからダウンロードしたフリーソフトであったことが判明した。		

表 25　UTM によるセキュリティ対策状況等の確認結果（BCC）

②　EDR ソフト

セキュリティ機器	＜EDR＞ エンドポイント監視サービス Type-Y（NEC 社）	**設置社数（延べ数）**	**42** 社
提供内容	実証への参加企業のエンドポイント端末にエージェントソフトを導入し、常時エージェントを監視する。異常を検知した際に通知を行い、対処を行う。 パターンファイルに依存しない振る舞い検知型のマルウェア対策エンジンにより、未知のマルウェアを防御することが可能である。		
実証結果	・検知総数は 229 件あり、そのうち対応が必要な要注意検知（マルウェアの疑いがある検知）があった社数は 20 社であり 48%を占めた。 ・要注意検知数が最も多かった業種は「教育学習支援業」であり、62%を占めた。組織に属さない利用者に端末を貸し出して利用する機会もあり、組織のポリシーに則った利用がされない可能性が高いためと思われる。		

表 26　EDR によるセキュリティ対策状況等の確認結果（BCC）

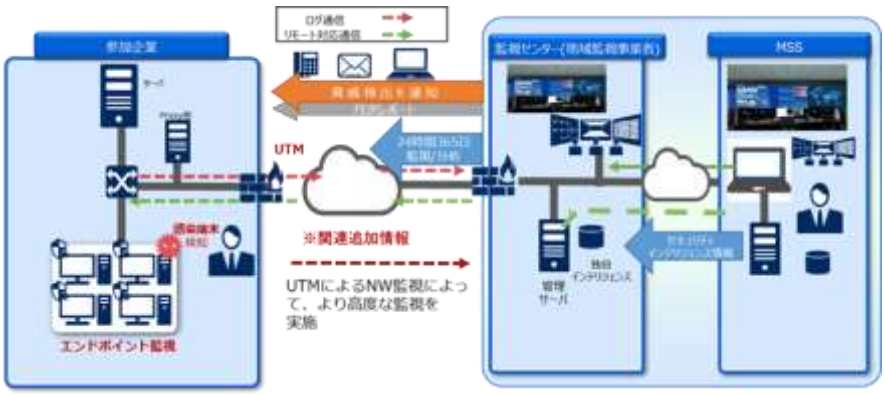


図 22 検知および監視の仕組み（BCC）

(12) 西日本電信電話（実証対象：熊本県）

① UTM 機器

セキュリティ機器	＜UTM＞ CloudEdge（トレンドマイクロ社）	**設置社数（延べ数）**	**105** 社
提供内容	導入した UTM のアラート状況を常時監視し、有事の際に必要な支援（遠隔支援、駆付け支援、データ復旧支援）を行う。 未知の脅威に対しても対応が可能であり、ウイルスなのか判別できない場合、必要に応じてクラウド上に隔離された「サンドボックス」で試し実行し、ふるまいを解析し、危険なものは UTM で防御する。		
実証結果	スパイウェアの駆除/無効化および Web フィルタリングは、参加企業数が増えた 10 月からは毎月発生した。 Web フィルタリングでは、偽の通販サイト、詐欺サイト、フィッシングサイトなどへのアクセスを防御しており、参加企業の社員教育が必要と考えられる。		

表 27 UTM によるセキュリティ対策状況等の確認結果（西日本電信電話）

② EDR ソフト

セキュリティ機器	＜EDR＞ セキュリティおまかせプラン プライム（NTT 西日本）	**設置社数（延べ数）**	**105** 社
提供内容	エンドポイントセキュリティツールを導入した端末のアラート状況を常時監視し、有事の際に必要な支援（遠隔支援、駆付け支援、データ復旧支援）を行う。 エンドポイントセキュリティでは、ウィルス検知・駆除等を実施する。		
実証結果	代表的なウイルスとしては、EMOTED と考えられるトロイの木馬が検出された。 ADW/PUA といった、フリーソフトウェアなどにバンドルされ、同時にダウンロード/インストールされている可能性が高いグレイウェアも検出された。		

表 28 EDR によるセキュリティ対策状況等の確認結果（西日本電信電話）

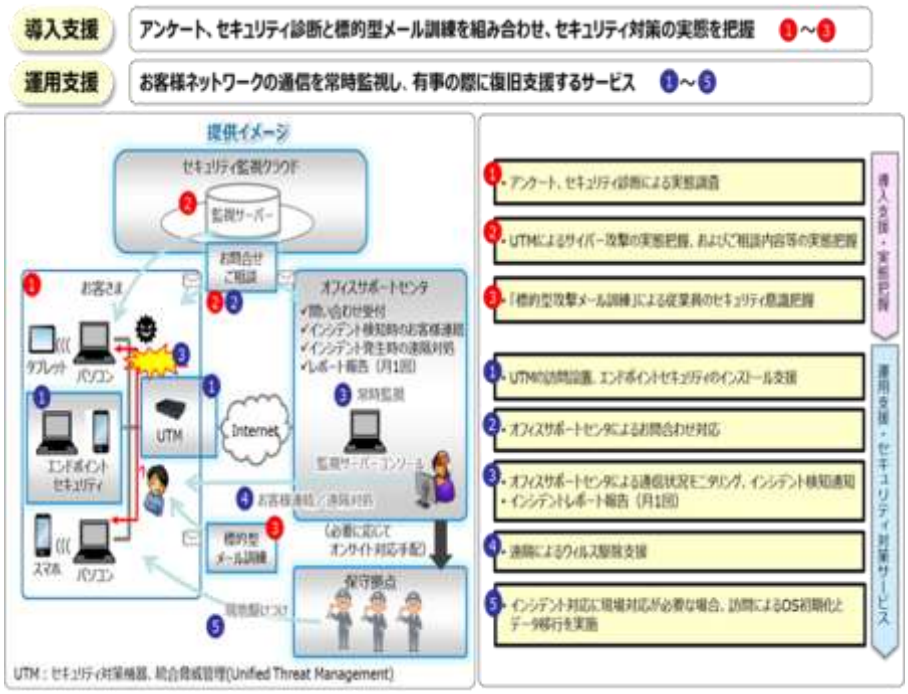


図 23 検知および監視の仕組み（西日本電信電話）

(13) 沖電グローバルシステムズ （実証対象：沖縄県）

① UTM 機器

セキュリティ機器	＜UTM＞ Firebox シリーズ（Watchguard 社）	設置社数（延べ数）	15 社
提供内容	UTM 機器を設置し、不正な通信や不正アクセスやスパムメール、危険な Web サイトへの誘導等のサイバー攻撃を検知・防御する。UTM で攻撃を検知した際は参加企業へ直接アラートを通知するのではなく、一度 SOC 側にてアラートを受けて検知内容を精査し、対応が必要な場合にのみ通知する。		
実証結果	フィッシングサイトのような不正な Web サイトや評価の低い（危険度が高い）Web サイトへのアクセスを検知・防御した。 無意識に不正サイトへアクセスしている様子もあり、UTM の有効性が確認された。		

表 29 UTM によるセキュリティ対策状況等の確認結果（沖電グローバルシステムズ）

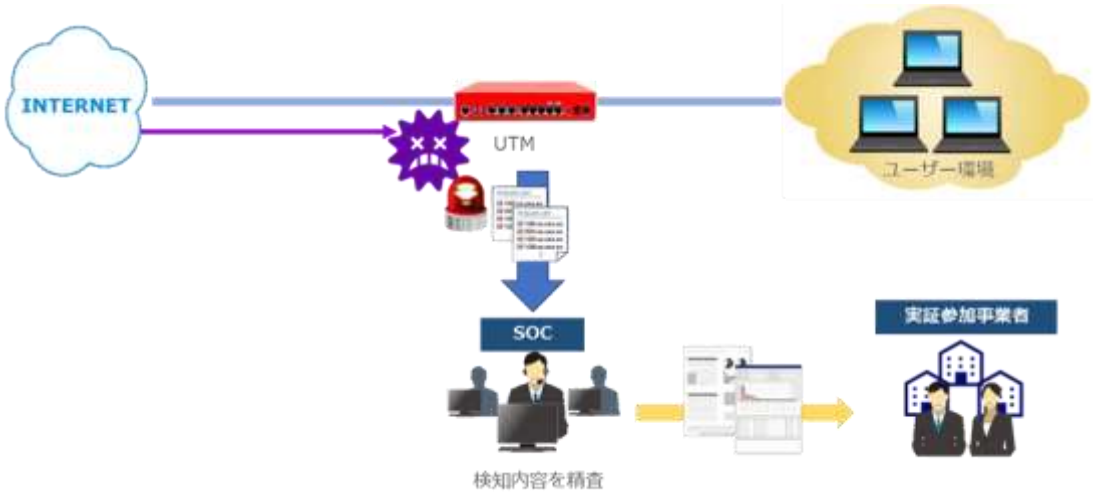


図 24 検知および監視の仕組み（沖電グローバルシステムズ）

② クラウド型 WAF

セキュリティ機器	＜クラウド型 WAF[16]＞ secuWAF（セキュアイノベーション社）	設置社数（延べ数）	8 社
提供内容	Web サイトの改ざんやクレジットカード情報の搾取等のサイバー攻撃を WAF センターで検査し、正当なユーザのみ Web サイトのアクセスを許可する。		
実証結果	クラウド型 WAF 側で有している検出ポリシーに基づき、Web サイトへの攻撃を合計 27,099 件検知してブロックをした。 導入した全ての Web サイトにおいて少なからず攻撃があることが判明した。 攻撃の種類を大別すると、偵察行為にあたる攻撃が大半を占める結果であった。		

表 30 クラウド型 WAF によるセキュリティ対策状況等の確認結果（沖電グローバルシステムズ）

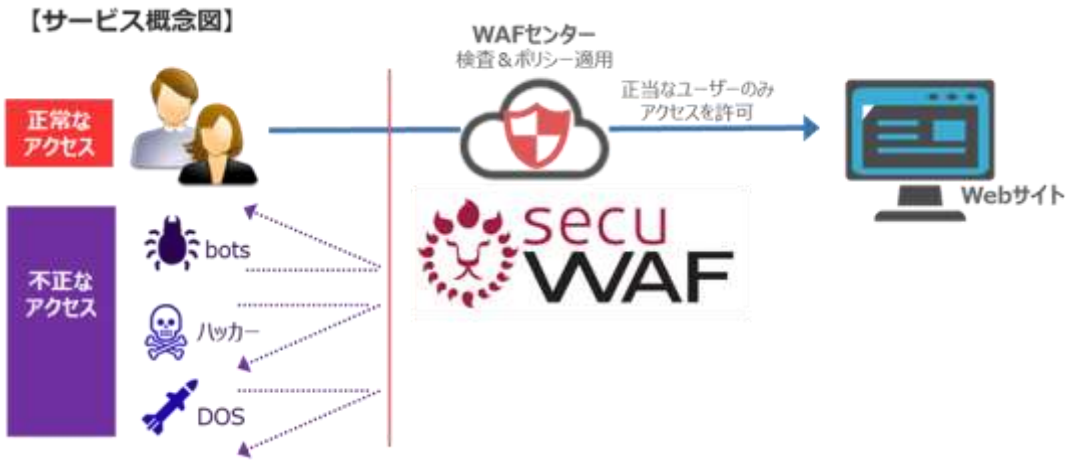


図 25 検知および監視の仕組み（沖電グローバルシステムズ）

16 WAF(Web Application Firewall)：ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するセキュリティ対策。ファイアウォールや IPS(不正侵入防止システム)では防御することができない攻撃を検知・遮断する。

③　EDR ソフト

セキュリティ機器	＜簡易 EDR＞ EISS（セキュアイノベーション社）	**設置社数（延べ数）**	**68** 社
提供内容	エンドポイント（Windows パソコン）における操作や生成ファイルなどのログ情報を記録・保持し、マルウェア感染後に発生する活動かどうかを定期的に分析し、情報漏洩などの被害に繋がる可能性に気付かせ、即時対応を行う。		
実証結果	「セキュリティリスクの疑いがあります。」「セキュリティリスクの恐れがあります」というアラートが出た端末数は 113 端末であった。 詳細確認をした結果、過剰検知と判定しマルウェア感染をした端末の検出には至らなかった。		

表 31　簡易 EDR によるセキュリティ対策状況等の確認結果（沖電グローバルシステムズ）

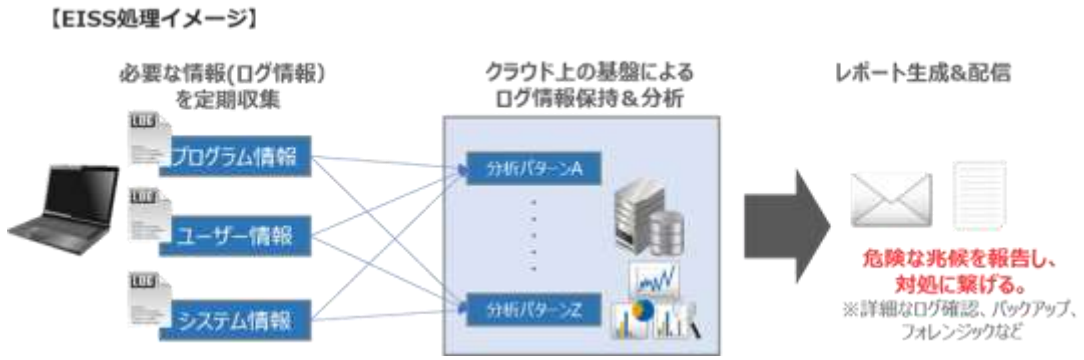


図 26 検知および監視の仕組み（沖電グローバルシステムズ）

(14) PFU （実証対象：防衛・航空宇宙産業（関東地方、中部地方、関西地方））

セキュリティ機器	＜PC の脅威検知ツール＞ 「SecureAnywhere Business」（WEBROOT 社）	**設置社数（延べ数）**	**50** 社
提供内容	参加企業の PC に WEBROOT 社 SecureAnywhere Business を導入し、クラウド上で管理する方式でサービスを提供する。ソフトウェアは、通常のアンチウイルスソフトの機能に加えて、未知の脅威を識別でき、クラウド上から隔離操作（処置）ができる機能を有している。 参加企業の PC がマルウェア等に感染し、参加企業自身で対処できないと判断した場合、駆け付けて状況調査やマルウェア駆除支援などの初動対応支援を行う。		
実証結果	アンチウィルスなどの既存対策をすり抜けた脅威として、業務上好ましくないアドウェア、ダウンローダーと呼ばれるものが、**1,766 件検出**された（緊急に対処は必要でなかったものの、その後、 脅威に繋がる可能性はあるもの）。		

表 32 PC の脅威検知ツールによるセキュリティ対策状況等の確認結果（PFU）

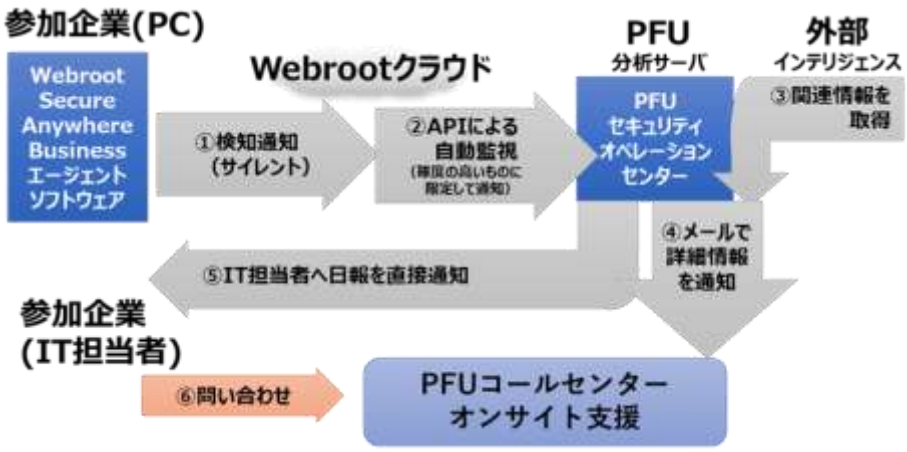


図 27 検知および監視の仕組み（PFU）

(15) 東京海上日動リスクコンサルティング（実証対象：自動車産業（静岡県、広島県等））

セキュリティ機器	以下の 2 パターンの監視機器を設置 <UTM> Cloud Edge（トレンドマイクロ社） <ネットワークセンサー>StellarCyber （StellarCyber 社）	**設置社数（延べ数）**	**30** 社（※1）
提供内容	UTM 機器を設置し、企業内の通信状態をモニタリングし、有害サイトへのアクセス等の不正な通信や不正アクセスを検知、必要に応じて自動で遮断を行う。 セキュリティインシデント発生時は、トラブル相談窓口を通じて状況を確認し、リモートサポートにて事象の解決を行う。また、リモートサポートによる解決が困難と判断した場合は、現地への駆け付け対応を行う。		
実証結果	検知された不正プログラム、ランサムウエアの数は、合計 32 件であり、特定企業において検知が多かった。 URL フィルタリング機能にて、有害または業務に無関係の通信として、約 1900 万件のアクセスを防御した。そのうち、99%は Web 広告で、Web 広告以外でのアクセスブロック数は、1,612 件であった。1,612 件うち、詐欺サイトへ誘導されるケースが 75%と大半であった。 インシデントと判断し、リモート支援を 2 件行った。 うち、1 件は StellarCyber による通信の監視にて C&C 通信と思われる不正アクセスを検知し、当該端末をネットワークから切り離し、ウイルススキャンの実施を行った。 実際に通信を行っている端末の特定、疑わしい通信の特定については、当該企業の業務都合等の理由により、詳細調査を行えず、特定できていない。		

※1 StellarCyber 3 社、CloudEdge27 社

表 33 UTM によるセキュリティ対策状況等の確認結果（東京海上日動リスクコンサルティング）

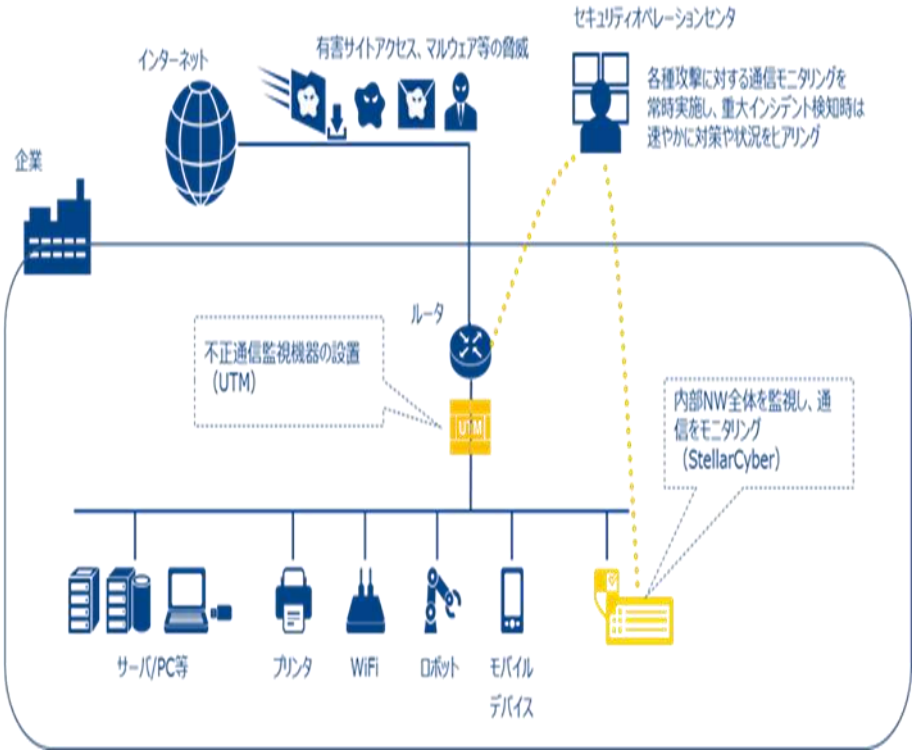


図 28 検知および監視の仕組み（東京海上日動リスクコンサルティング）

3.2.2. 実証による検知等の結果

本事業では、サイバー攻撃に関する様々なアラート等が、各事業主体が構築したセキュリティ機器等による検知および監視の仕組みにより確認された。

サイバー攻撃の手法は進化しており、これに対応するために攻撃を検知するアラート等も多数の種別が存在する。本事業の実証では、中小企業がさらされているサイバー攻撃の実態を把握するために、従来からの攻撃手法である外部からの不審なアクセスへの対応に加え、不正プログラムによる内部から外部への不正通信の実態にも着目し、以下のアラート種別により、アラート等の検知状況の取りまとめを行った。

アラート種別	アラート種別の説明	主なアラート検知状況
①外部からの不審なアクセス検知および防御（外→内）	外部からの不審なアクセス通信を検知・遮断し、バッファーオーバーフローや Web クロスサイトスクリプティング等のソフトウェアやネットワークの脆弱性をついた攻撃を防御	外部からの**サイバー攻撃の探索活動である「ポートスキャン」が数多く行われている**ことを確認した。また、**直接的な攻撃**である「バッファーオーバフロー」「クロスサイトスクリプティング」「Dos 攻撃」等の攻撃も**数多く検知および遮断**した。また、PC をリモートで制御するためのツールをインストールするためのバックドアを検知、ブロックする事例もあり、新たな脅威も確認された。
②内部からの不正通信や不正プログラム検知および防御（内⇔外）	マルウェアの侵入が疑われる内部から外部への不正通信や不正プログラムの存在が疑われる通信を検知、感染を防御	不正プログラムの存在が疑われる通信を数多く検知し、防御した。特に **C&C サーバへの通信**と考えられる不審な通信先へのアクセスを**検知および防御**した。同一企業で約 4,000 件発生した事例については、リモートによるインシデント対応を実施し、処置した。
③不正および不許可サイトへのアクセスブロック（内→外）	予め登録したセキュリティ上のリスクがある不正サイトや業務上許可されていない Web サイトへの接続をブロック（URL フィルタリング）	ほぼ全ての企業において、不正サイトへのアクセスを検知し、ブロックした。**特定企業に突出して発生する**傾向も見られた。また、業務上許可されていない Web サイトだけでなく、**偽の通販サイト、詐欺サイト、フィッシングサイト**などへのアクセスもブロックしており、**社員教育が必要**と考えられる。
④マルウェアの検知および無害化	メール添付ファイルや Web からのダウンロードファイルに含まれるウイルス、ランサムウェア、アドウェア等の検知と無害化	身代金要求型のマルウェアである**「ランサムウェア」を多く検知および無害化**した事例が数多く見られた。また、ウィルスが仕組まれていると思われる報告書を添付した、なりすましメールが 3 日間にわたって同じ企業に送付される事例も発生した。
⑤エンドポイントでのアラート検知および処置	パソコン端末にインストールした EDR ソフト等で不正プログラムの検知および防御や不正サイトおよび不許可サイトへのアクセスブロック	EDR ソフト等により、相当数の**ランサムウェア**や**トロイの木馬**などの不正プログラムや不正サイトおよび不許可サイトへのアクセス痕跡等を検知し、ウィルスの駆除やブロック等の処置を行った。
⑥その他のアラート検知	スパムメールの検知や内部の脆弱性を検知	スパムメール検知では、導入した企業の 7 割超の企業で何らかの迷惑メールを受信していた。多くは広告メールであったが、**フィッシングサイトへ誘導するような悪意のあるメール**もあり、注意が必要である。内部の脆弱性では、バ

		ージョンの古いソフトウェアの使用や、不正アクセスを試みようとする疑いのあるコードが見つかるなど **Web サイトの脆弱性**が複数確認された。

(1) ネットワーク一括監視型（UTM 機器等）による検知結果（アラート種別①～④）

アラート種別のうち、ネットワーク一括監視型（UTM 機器等）により検知したアラート等は以下のとおりであった。

事業主体	設置社数	①外部からの不審なアクセス検知および防御（外→内）	②内部からの不正通信や不正プログラム検知および防御（内⇔外）	③不正および不許可サイトへのアクセスブロック（内→外）	④マルウェアの検知および無害化	その他
東日本電信電話（UTM）	134	19,650	18,993	710	299	59,182
東北インフォメーション・システムズ （UTM）	40	110	0	–	115	–
富士ソフト（ネットワークセンサー）	71	2,121	1,348	70	–	–
デジタルハーツ（UTM）	22	430	219	52	7	2,385
富士ゼロックス（UTM）	36	17,958	139,109	364,413	6	8,566
SOMPO リスクマネジメント （UTM）	59	490	–	118,141	52	67,080
MS&AD インターリスク総研 （UTM）	50	78,659	4,168	361	97	236,842
名古屋商工会議所（UTM）	29	576	26	4,286,363	19	60[17]
大阪商工会議所（UTM）	53	7,906	2,091	76	524	199
高松商工会議所（UTM①）	16	134	33,151	5,401	8	8,465
高松商工会議所（UTM②）	24	705	18	140	27	43,887
BCC（UTM）	54	25,698	118	66	90	25
西日本電信電話（UTM）	105	–	–	298	61	–
沖電グローバルシステムズ （UTM）	15	–	49	207	8	–
沖電グローバルシステムズ （クラウド型 WAF）	8	27,099	–	–	–	–
東京海上日動リスクコンサルティング （UTM）	30	–	3,587	19,301,698	32	–

[17] スパムメールブロックは、メール対策ツールで実施し、60 件のスパムメール(疑い)の受信を検知した。

表 34 ネットワーク一括監視型（UTM 機器等）による検知結果

⑵ 端末監視型（EDR ソフト等）による検知結果（アラート種別⑤）

アラート種別のうち、端末監視型（EDR ソフト等）により検知したアラート等は以下のとおりであった。

事業主体	設置社数	⑤エンドポイントでのアラート検知および処置
デジタルハーツ（EDR ソフト）	24	392
ＳＯＭＰＯリスクマネジメント（EDR ソフト）	51	4,122
MS&AD インターリスク総研（EDR ソフト）	50	10,723
名古屋商工会議所（Defender 監視ツール/Web 対策ツール）	54	624
BCC（EDR ソフト）	42	229
西日本電信電話（EDR ソフト）	105	93
沖電グローバルシステムズ（EDR ソフト）	68	0
PFU（PC の脅威検知ツール）	50	1,766

表 35 端末監視型（EDR ソフト等）による検知結果

- 事業主体によりセキュリティ機器や環境設定が異なるため、検知件数にバラツキはあるものの、導入したほとんどの中小企業で何らかのアラートが検知されており、**その業種や規模を問わずサイバー攻撃の脅威にさらされている実態が明らかとなった。**
- アラート種別やアラート内容も多岐に渡ることもあり中小企業自らこれを管理することは困難であり、セキュリティの専門家の活用が求められるといえる。

3.2.3. アラート種別ごとの検知状況

本事業の実証で検知した、アラート種別ごとの検知状況は以下のとおりであった。

(1) 外部からの不審なアクセス検知および防御（外→内）

外部からの不審なアクセスとしては「ポートスキャン」や DoS/DDoS 攻撃の件数が多いことが確認できた。

東日本電信電話（UTM）	
検知数	19,650 （内訳：通信が IPS 機能で定義されたルールにマッチした件数）
検知内容	10 月に最も検知の多かったルールは、1 社に集中して見られたが、11 月には該当社数が 6 社と増え、累計検知回数が 12,412 回に及んだ。 10 月に該当社数が 18 社で累計マッチ回数が 130 件と第 2 位だったルールは、11 月第 4 位、12 月第 8 位と複数月に渡り多く検知した。
東北インフォメーション・システムズ（UTM）	
検知数	110
検知内容	公開サーバまたはアクセスポイントに対して DoS 攻撃等の攻撃を検知した。 システムの速度を低下させたり、クラッシュさせたりする、ip_dst_session やリモート攻撃を行う Eir.D1000.Modem.CWMP.Command.Injection を多く検知した。
富士ソフト（ネットワークセンサー）	
検知数	2,121 （内訳：ブルートフォース攻撃 （1,399）、ポートスキャン（569）、URL スキャン（152）、SYN Flood 攻撃の検知（1））
検知内容	ブルートフォース攻撃（総当たり攻撃）、ポートスキャン、URL スキャン、SYN Flood 攻撃をそれぞれ検知した。 その中で、不審な IP アドレスからの当該企業のインターネット上に公開している端末への URL スキャン通信に成功応答したことを検出した。この成功応答により、Web サイトに存在する脆弱性が晒された状態となり、本格的な攻撃により不正アクセスや情報漏えいなどの被害を受けたり、他の攻撃の踏み台として悪用される可能性があるため、通報し、公開している端末のログイン履歴確認と脆弱性対策を実施した。
デジタルハーツ （UTM）	
検知数	430
検知内容	主な攻撃は、UDP の Land 攻撃（129 件）、OpenSSL の脆弱性 （50 件）、シェルスクリプトの脆弱性（46 件）等であり、いずれも検知後に攻撃をブロックした。

富士ゼロックス （UTM）	
検知数	17,958 （内訳：ping/port-scan の検知数）
検知内容	ping：15,945 件、port-scan：2,013 件が検知され、UTM 端末 1 台で 1 日あたりに換算すると約 17 件/台となった。日別で多少のばらつきはあるが、大きな変動は見られなかった。 また、ping は 74 ヶ国からのアクセス履歴を検知。その大半は米国、中国の 2 ヶ国からのアクセスであり、約 6 割を占めた。 他方、port-scan は 35 ヶ国からのアクセス履歴を検知。米国とルーマニアの 2 ヶ国で 49%を占める結果となった。
ＳＯＭＰＯリスクマネジメント（UTM）	
検知数	490 （内訳:WEB クロスサイトスクリプティングの通信（64）、WEB クロスサイトスクリプティング（cookie 盗難）の試みの通信（33）、バッファオーバーフローの脆弱性を狙った通信（21）、Web ディレクトリトラバーサル[18]の脆弱性を狙った通信（16）、Web シェルスクリプトによるリモートコマンド実行を狙った通信（131）、脆弱性をスキャンするツールによるスキャニングのための通信（67）、PHP CGI 引数インジェクションの通信（18）、その他）
検知内容	導入した企業の約 3 割の 19 社で、合計 490 件もの不正通知をブロックした。 標的である企業に直接損害を与えるものだけでなく、企業のウェブサイトのユーザに被害をもたらす攻撃もあった。
MS&AD インターリスク総研（UTM）	
検知数	78,659 （内訳：IPS （侵入防御システム）による検知）
検知内容	IPS（侵入防御システム）にて、防御が必要な通信を多数検知した。 中小企業においても、攻撃通信の標的となることが再確認できた。
名古屋商工会議所（UTM）	
検知数	576 （内訳：外部からの不正アクセス検知および防御）
検知内容	UTM による防御が無かった場合実際に感染していた可能性もあり、中小企業における脅威およびその対策の重要性を把握できた。
大阪商工会議所（UTM）	
検知数	7,906 （内訳：IPS（外⇒内））
検知内容	外部からの不正アクセスは即時遮断し、ユーザ影響がないためアラート対象外となる。 遮断上位 3 種は、JSIG WEB SQL Union ALLSelect（3,359 件）、Cross Site Script attack（1,964 件）、Possible SQLMAP Scan（1,571 件）であった。

18 ディレクトリトラバーサル：ファイル名の先頭に「../」などの上位のディレクトを意味する文字列を用いることにより、公開を意図していないファイルに不正にアクセスする攻撃

高松商工会議所（UTM①）	
検知数	134 （内訳：IPS 検知）
検知内容	侵入防御（IPS）検知件数は 134 件と比較的少ないものの、検知した企業の割合は 60%を超えている。 バッファオーバーフロー攻撃、UNIX 系 OS で使用されるプログラムのコマンドシェルに存在する脆弱性を利用した攻撃、コンピュータをリモートで制御するために使用されるリモートアクセス／管理ツール（RAT）をインストールするためのバックドアを検知し、ブロックした。
高松商工会議所（UTM②）	
検知数	705 （内訳：IPS 検知）
検知内容	TCP Land 攻撃（378 件）、クロスサイトスクリプティング（71 件）などの攻撃を検知し、ブロックした。
BCC（UTM）	
検知数	25,698 （内訳：IPS 検知）
検知内容	設置台数増加とともに件数も増加するが、月別で見ると件数は増減しており、検知傾向や特異点などは見られなかった。
沖電グローバルシステムズ （クラウド型 WAF）	
検知数	27,099 （内訳：クラウド型 WAF の検出ポリシーに基づく検知）
検知内容	クラウド型 WAF にて、Web サイトへの攻撃を合計 27,099 件検知してブロックをした。導入企業の Web サイトのいづれでも少なからず攻撃を検知した。 攻撃の種類を大別すると、「コマンドインジェクション」のような直接的な攻撃と「スキャナ/プロキシ/スパムボット検知」のような更なる攻撃に繋げるための偵察行為にあたるような攻撃があるが、偵察行為にあたる攻撃が大半を占める結果となった。

表 36 外部からの不審なアクセス検知および防御の状況

(2) 内部からの不正通信や不正プログラム検知および防御（内⇔外）

不正プログラムの存在が疑われる不正な外部通信を多数検知した。特に C&C サーバへの不正通信（C&C コールバック）と考えられる不審な通信先へのアクセスを検知および防御した。同一企業で約 4,000 件発生した C&C コールバック事例については、リモートによるインシデント対応を実施し、処置した。

東日本電信電話（UTM）	
検知数	18,993 （内訳：禁止アプリケーション検知（18,384）、C&C サーバへの通信（609））
検知内容	「禁止アプリケーションの検知」件数は、ポリシー設定で禁止したアプリケーションからの通信要求が検知された件数を示し、期間中 18,384 検知した。 「C&C サーバへの通信」は、10 月、12 月は検知されなかったが、11 月に 609 件（1 社あたり 4.6 件）検知した。
東北インフォメーション・システムズ（UTM）	
検知数	0
検知内容	内部ネットワーク上のパソコンから内部不正プログラムの存在が疑われる通信を検知したが、調査した結果、誤検知であると判断したため、検知数からは除外している。
富士ソフト（ネットワークセンサー）	
検知数	1,348 （内訳：既知の C&C サーバへの通信の検知（1,049）、DNS トンネリング攻撃（298）、異常なプロセスの実行（1））
検知内容	C&C 通信と考えられる不審な通信先へのアクセスを検知した。 一部、迷惑ソフトに分類されるソフトウェアの利用痕跡を検出した。 当該ソフトウェアは、有償ソフトウェアのダウンロードを促す広告ポップアップを表示の上、トロイの木馬の関連であるサイトに通信を行っていることが確認されており、セキュリティ対策が不十分な端末では、マルウェア感染、データ漏洩・破壊されるなどの被害を受ける可能性があるため、通報し、迷惑ソフトの削除等の対策を行った。 また、エクスプロイトの異常なプロセスの実行が 1 件検知された。
デジタルハーツ（UTM）	
検知数	219 （内訳：ポリシー設定で禁止したアプリケーションからの通信要求が検知された件数）
検知内容	いずれも検知後にブロックした。傾向や動向については特に読み取れなかった。

富士ゼロックス（UTM）	
検知数	139,109 （内訳：IPS 検知ログ）
検知内容	IPS が検知した不正な通信検知数は、UTM1 台で 1 日あたり換算すると約 86 件となった。 検知した通信の約 8 割は Dropbox の通信であった。 次に、意図せぬ情報送信で秘密漏えいのリスクがあるとして、2013 年に内閣サイバーセキュリティセンター：NISC から注意喚起されている「Baidu IME」の利用が 14%であった。 また、TeamViewer というリモートアシスタンス（遠隔地の PC へ接続する通信）の信号も検知した。
MS&AD インターリスク総研（UTM）	
検知数	4,168 （内訳：C&C コールバック）
検知内容	C&C コールバックを UTM 設置によりブロックした。11 月～12 月の 4,126 件の検知は、1 企業において発生していたため、当該企業へ通報し、リモートによるインシデント対応を実施。 WindowsXP 端末により発生していることを特定。当該端末を買い替えたことにより、以後検知されなくなった。1 月に別企業でも発生した。
名古屋商工会議所（UTM）	
検知数	26 （内訳：不正アクセス検知・防御
検知内容	Web サイトにアクセスした際に不正なサイトであることを動的に検知し、ブロックした件数が 26 件あった。
大阪商工会議所（UTM）	
検知数	2,091 （内訳：IPS（内⇒外））
検知内容	アラート上位は、 HTTP Basic Auth Default Password Login attempt （guest） （241 件） HTTP Basic Auth Default Password Login attempt （admin） （179 件）。
高松商工会議所（UTM①）	
検知数	33,151 （内訳：DoS/DDoS 攻撃検知）
検知内容	検知数のほとんどが同一セグメント内の通信と見られる社内の通信を DOS 攻撃として検知した。社内のネットワーク輻輳などにセッションが正常に確立しない場合やデータ通信量が多い場合も検知するため、過検知であると推察される。 ネットワークへの侵入を試みるパケットを検知・ブロックした。

高松商工会議所（UTM②）	
検知数	18　（内訳：不正プログラム検知）
検知内容	2020 年 10 月に 5 件、11 月に 8 件、12 月 5 件の計 18 件不正な通信、プログラムによる攻撃を検知し、内部感染を早期に発見した。
BCC（UTM）	
検知数	118　（内訳：IPS 検知）
検知内容	設置台数とともに検知数も増加した。
沖電グローバルシステムズ（UTM）	
検知数	49　（内訳：内から内への不正通信）
検知内容	内から内への不正通信を 49 件検知したが、詳細確認の結果、業務通信であることが推測され、過検知として判定した。
東京海上日動リスクコンサルティング（UTM　または　ネットワークセンサー）	
検知数	3,587　（内訳：不正通信の検知）
検知内容	マルウェアの混入が疑われる P2P アプリケーションの通信を検知・遮断し、不正通信やウイルス感染の発端となる通信を 3,587 件検知し、ブロックした。 定の P2P アプリケーションによる通信を多く検知した。 C&C コールバックの検知はなかった。

表 37　内部からの不正通信や不正プログラム検知および防御の状況

(3) 不正および不許可サイトへのアクセスブロック（内→外）

不正な Web サイトへのアクセスをブロックすることにより、不正プログラムが実行される脅威等を未然に防止した。多くのユーザで発生するアクセスブロックであるが、事業主体によっては特定のユーザにおいて発生するケースも見られた。業務上許可されていない Web サイトへのアクセスも多数見られた。

業務上許可されていない Web サイトへのアクセスを通じた情報漏えいのリスクは当然高いことが想定される。

東日本電信電話（UTM）	
検知数	710 （内訳：不正サイトの検知（710））
検知内容	2020 年 10 月から 12 月の間の「不正サイト」を検知した件数は、10 月は 18 件、11 月は 441 件、12 月は 251 件であった。月別の変化を 1 社あたりマッチ件数でみると、2020 年 11 月の多さが際立っているが、月別の変化を 1 社あたりの検知件数でみると、顕著な差ではなかった。
富士ソフト（ネットワークセンサー）	
検知数	70 （内訳：フィッシングサイトへのアクセス（69）、マルウェア配布サイトへのアクセス（1））
検知内容	フィッシングサイト、マルウェア配布サイトへのアクセスとして 70 件のアラートを検知・ブロックした。一部、フィッシングおよびマルウェアに関連するサイトとして確認されているサイトへアクセスした痕跡を検出したため、通報し、使用者を特定、フィッシングサイトに情報入力していないか等の確認と対策を行った。
デジタルハーツ（UTM）	
検知数	52（内訳：Web レピュテーション機能により、危険とされる URL への HTTP リクエストまたは TLS ネゴシエーション等が検知された回数）
検知内容	いずれも検知後にブロックした。特定企業に突出して発生する傾向が見られた。
富士ゼロックス（UTM）	
検知数	364,413（内訳：コンテンツフィルタログ）
検知内容	危険度が高いと判断し、ブロックした Web サイト数は、UTM 1 台で 1 日あたりに換算すると約 191 件あった。 ブロックしたコンテンツのうち、32%は SNS 利用であり、次いで 28%がオンラインストレージに対するブロック、18%は Web アプリケーション利用によるものであった。

ＳＯＭＰＯリスクマネジメント（UTM）	
検知数	118,141
検知内容	55 社中 52 社と約 9 割の企業で検知した。 最も多かったのはゲームサイトへのアクセス（42,723 件）、次いで Facebook へのアクセス（16,068 件）、成人/アダルトコンテンツサイトへのアクセス（13,603 件）であった。
MS&AD インターリスク総研（UTM）	
検知数	361 （内訳：Web レピュテーション）
検知内容	件数は少ないが組織としてアクセスに適さないウェブサイトへの通信を確認した。 機械的なフィルタリングによりマルウェア感染リスクを低減できると思われる。
名古屋商工会議所（UTM）	
検知数	4,286,363 （内訳：不正 URL へのアクセス（4,286,363））
検知内容	予め指定した不正 URL へのアクセスを約 400 万件ブロックした。99.99%が広告サイトであり、重大なインシデントを危惧するものではなかったが、ごく一部ではあるが詐欺サイトやフィッシングサイトへのアクセスをブロックしたケースもあった。
大阪商工会議所（UTM）	
検知数	76 （内訳：Web ガード（76））
検知内容	検知数を地域別に確認したところ、和歌山県で 11 月 3 週に検知数が突出した。 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った。
高松商工会議所（UTM①）	
検知数	5,401
検知内容	URL フィルタリング検知は全ての事業者において検知された。その多くは、アダルト／兵器・武器／ショッピングなどカテゴリされたサイトへのアクセスであったが、一方でマルウェア／フィッシングサイト／違法ソフトへのアクセスが約 1 割見られ、サイバー攻撃の入り口となる有害なサイトへのアクセスを制御した。

高松商工会議所（UTM②）	
検知数	140
検知内容	2020 年 10 月に 33 件、11 月に 54 件、12 月 53 件の計 140 件の Web サイトへのアクセスをブロックした。
BCC（UTM）	
検知数	66 （内訳：Web ガード（66））
検知内容	検知の最も多かった企業では動画サイトを見ていたとの報告があり、それが原因の可能性が高いが、業務に影響は無かったとのことであった。
西日本電信電話（UTM）	
検知数	298 （内訳：Web レピュテーション）
検知内容	偽の通販サイト、詐欺サイト、フィッシングサイトなどへのアクセスをブロックした。
沖電グローバルシステムズ（UTM）	
検知数	207
検知内容	ほぼ全ての業種において、フィッシングサイトのような不正な Web サイトや評価の低い（危険度が高い）Web サイトへのアクセスへのブロックが発生した。
東京海上日動リスクコンサルティング（UTM　または　ネットワークセンサー）	
検知数	19,301,698
検知内容	有害または業務に無関係の通信として、約 1900 万件のアクセスをブロックした。 そのうちの 99%以上は Web 広告が占めていた。 Web 広告以外でブロックした URL カテゴリ比率を集計した結果は、詐欺サイト（75%）、スパム（13%）、フィッシング（7.5%）と詐欺サイト[19]へ誘導されるケースが多かった。

表 38　不正および不許可サイトへのアクセスブロックの状況

[19] 詐欺サイト：個人または団体から信用を得た上で金銭などをだまし取ろうとする Web サイト

(4) マルウェアの検知および無害化

身代金要求型のマルウェアであるランサムウェアの検知および無害化の事例が多く見られた。また、請求書を装うなりすましメールやウイルス感染の可能性のある報告書が添付されたメールが 3 日間に渡って同じ企業に送付される事例があり、いずれも UTM でブロックすることができた。

東日本電信電話（UTM）	
検知数	299 （内訳：ランサムウェア検知（223）、不正プログラム/スパイウェア検知（76））
検知内容	「ランサムウェアの検知」は、10 月 6 件、11 月 67 件、12 月 150 件と、徐々に増加した。 不正プログラム／スパイウェア検知は、「load-scripts.php」が全体の 7 割弱を占め、次いで「COMPANY PROFILE.doc」が続いた。「COMPANY PROFILE.doc」は、同時期に検知した社数が 4 社あり、該当社数が複数存在したのが特徴的で、本実証参加以外の企業も含め広く流通した可能性があると思われる。 また、「COMPANY PROFILE.doc」に類似した「COMPANY PROFILE.doc,RFQ.exe」が検知されているほか、名称は異なるものの「Fattura_」で始まる表計算関連ファイル（拡張子が.xls や.xlsm）を複数検知した。 表計算関連ファイルのように業務上利用頻度が高いと思われるファイルに不正プログラムが含まれることが確認された。
東北インフォメーション・システムズ（UTM）	
検知数	115
検知内容	Web サイト経由マルウェア防御 48 件、電子メール経由マルウェア防御 67 件検知し、無害化した。 USB メモリ経由の感染が少なくなり、Web サイト閲覧と電子メールがマルウェアの主たる感染経路になっていた。非常に多くの攻撃種別を検知した。
デジタルハーツ（UTM）	
検知数	7（内訳：メールセキュリティ機能により、添付ファイルがマルウェアであると検知されたメールの数）
検知内容	いずれも検知後にブロックした。傾向や動向については特に読み取れなかった。
富士ゼロックス（UTM）	
検知数	6（内訳:HTTP・FTP ウイルススキャンによる検知（0）、メール受信ウィルススキャンによる検知（6））

検知内容	Web 経由でダウンロードされたウィルスは確認されなかった。 メール受信ウィルススキャンによるウイルスメール受信数は、全メール受信数:75,330 件に対して 6 件検知した。 10 月に埼玉県で請求書を装うなりすましメールを 1 件、12 月には千葉県でウイルス感染している可能性のある報告書が添付されたメールが 3 日間に渡って同じ企業に送付されるのを確認した。いずれも UTM でブロックしたため、被害を未然に防ぐことができたが、こうした手口によるウイルスメールは昨年度事業でも複数件検出されており、今後も注意が必要である。
ＳＯＭＰＯリスクマネジメント（UTM）	
検知数	52
検知内容	トロイの木馬 46 件、アドウェア 6 件検知した。導入企業 59 社のうち、8 社において検知した。 本実証では、UTM のパフォーマンス低下により導入企業の業務に支障が出ることを避けるため、1MB 未満のウイルスのみ監視対象とした。
MS&AD インターリスク総研（UTM）	
検知数	97 （内訳:ウィルス/不正プログラム（63）、ランサムウェア（34））
検知内容	ウイルス・不正プログラム、ランサムウェアを検知した。 ランサムウェアの検知は、1 企業において発生したものであった。UTM によりブロックしており感染被害を防ぐことが出来た。
名古屋商工会議所（UTM）	
検知数	19 （内訳：マルウェアの事前検知・駆除）
検知内容	マルウェアの事前検知・駆除が 19 件できた。
大阪商工会議所（UTM）	
検知数	524 （内訳：アンチウィルス（内⇔外））
検知内容	検知数を地域別に確認したところ、奈良県が 10 月 5 週、12 月 2 週に検知数が突出していた。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。
高松商工会議所（UTM①）	
検知数	8 （内訳：アンチウイルス検知）

検知内容	社内ネットワークとインターネット間の通信で確認されたマルウェアを 8 件検知、ブロックした
高松商工会議所（UTM②）	
検知数	27 （内訳：ランサムウェア検知）
検知内容	ランサムウェアの検知は、1 社のみ特定の日に 1 つのサイトに対して検知した。利用ユーザが不正と思われる URL にアクセスした結果であった。
BCC（UTM）	
検知数	90 （内訳：アンチウィルス）
検知内容	検知の多くがトロイの木馬の疑いのあるファイルの送受信である。メール添付ファイルでの検知がほとんどであり、検知したファイルは全て無害化されている。検証終盤の 12 月中旬以降にファイル転送での検知も 11 件確認された。
西日本電信電話（UTM）	
検知数	61 （内訳：その他の脅威ブロック）
検知内容	その他の脅威 （ランサムウェア、メールからの不正プログラム）を 10 月に 4 件、11 月に 21 件、12 月に 36 件検知、ブロックした。
沖電グローバルシステムズ（UTM）	
検知数	8
検知内容	UTM のウイルス対策機能にて、8 件のマルウェアを検知、ブロックした。
東京海上日動リスクコンサルティング（UTM または ネットワークセンサー）	
検知数	32
検知内容	不正プログラム、ランサムウェアを 32 件検知したが、UTM にてブロックしており駆け付け対応にいたるインシデントには発展しなかった。

表 39 マルウェアの検知および無害化の状況

(5) エンドポイントでのアラート検知および処置

EDR 等によるエンドポイントでのアラート検知では、ランサムウェアやトロイの木馬などの不正プログラムを多く検知し、駆除した。但し、過検知の場合も多く見られた。また、不正サイトおよび不許可サイトへのアクセスの痕跡を検知し、防御した。

デジタルハーツ（EDR ソフト）	
検知数	392
検知内容	・ランサムウェアを 1 件検知（ただし誤検知）したが、それ以外は IE のセーフブラウジング侵害や EDR システム認証エラー等のため経過観察対象であった。 ・疑わしい挙動をするマルウェア（悪意の動作をするソフトウエア）や業務上不要と考えられるソフトウェアを 6 件検知し、自動除去した。 ・スパム URL やマルウェアのダウンロードに繋がるサイトへのアクセスを 4 件検知し、アクセスをブロックした。 ・非推奨ブラウザ、バージョンの古いブラウザの使用を 2 件検知した。
ＳＯＭＰＯリスクマネジメント（EDR ソフト）	
検知数	4,122
検知内容	75%の企業においてアドウェアやリスクウェア等の不正プログラムが検知されているが、危険度の高い不正プログラムは確認できなかった。
MS&AD インターリスク総研（EDR ソフト）	
検知数	10,723 （内訳: 不審なプロセス起動（122）、不審な通信（40）、不審なファイル生成（6）、不審なコマンド実行（10,407）、不審な API 実行（146）、不審な常駐プログラム登録（5））
検知内容	EDR 設置後 1 か月間に検知した「不審なコマンド実行」や「不審なプロセス起動」は大半が過検知によるものであった。導入から 1 ヵ月間は AI の学習期間のため、検知はするものの過検知が多くなる傾向があるが、その中でも、サポートが終了したメンテナンスされないソフトウェア（プラグイン）の振る舞いを検知しているケースもあり、導入企業に対する注意喚起になった。
名古屋商工会議所（Defender 監視ツール/Web 対策ツール）	
検知数	624 （内訳:Defender 監視ツール（0）、Web 監視ツール（624））

検知内容	不正サイトのブロックが 624 件であった。平均的ではなく、一部企業におけるブロック実績が多かった。
BCC（EDR ソフト）	
検知数	229
検知内容	要注意検知　90 件、過検知　139 件であった。要注意検知のうち、最も多かったのはマルウェア（46 件）であった。
西日本電信電話（EDR ソフト）	
検知数	93　（内訳:ウイルス・不正プログラム駆除/無効化（43）、スパイウェア駆除／無効化（50））
検知内容	代表的なウイルスとしては EMOTED によると考えられるトロイの木馬を検出した。 また、ADW/PUA といった、フリーソフトウェアなどにバンドルされ、同時にダウンロード/インストールされている可能性が高いグレイウェアも検出した。
沖電グローバルシステムズ（EDR ソフト:EISS）	
検知数	0
検知内容	セキュリティリスクの疑いがあるというアラートが発生した端末は、113 端末あった。 詳細確認をした結果、いづれも過剰検知であると判定したため、検知数からは除外している。 マルウェア感染をした端末の検出には至らなかった。
PFU（PC の脅威検知ツール）	
検知数	1,766
検知内容	緊急度を要するマルウェア（遠隔操作型、破壊型、身代金型）は、既存対策（ファイアウォール、アンチウイルスなど）で排除されており、既存対策をすり抜けた脅威は検知されなかった。 対応する優先度は低いものの**業務上好ましくないアドウェア、ダウンローダーと呼ばれるアプリケーション**は、**1,766 件**（193 種/9 マルウェアグループ）検知し、報告した。

表 40　エンドポイントでのアラート検知および処置の状況

(6) その他のアラート検知

スパムメール検知では、導入した企業の 7 割超の企業で何らかの迷惑メールを受信していた。多くはショッピングサイト、インターネット通販事業者からの広告メールであったが、フィッシングサイトへ誘導するような悪意のあるメールもあり、注意が必要である。古いバージョンのソフトウェアを使用している事例や、不正アクセスを試みようとする疑いのあるコードが見つかるなどの事例も見られ、Web サイトの脆弱性が検知された。

東日本電信電話（UTM）	
検知数	59,182 （内訳：スパムメール検知:59,182）
検知内容	「スパムメール」は、宣伝広告目的で、ユーザの同意なしに勝手に送られてくる迷惑メールで、アクセスのみで感染に至る URL が記されている場合は誤ってアクセスすることで情報漏えい等につながる脅威がある。 2020 年 10 月から 12 月の間の「スパムメール」を検知した件数は、10 月は 516 件、11 月は 36,903 件、12 月は 21,763 件であった。月別の変化を 1 社あたり検知件数でみると、2020 年 11 月の多さが目立つ結果となった。
デジタルハーツ（UTM）	
検知数	2,385 （内訳:スパムメール警告 （2,385））
検知内容	「スパムメール警告」は、期間中 2,385 件検出した。
富士ゼロックス（UTM）	
検知数	8,566 （内訳:スパムメール受信 （8,566））
検知内容	調査期間中に受信したスパムメール数は、8,566 件（全メール受信数 75,330 件の 11%）であった。UTM 端末 1 台で 1 日あたりに換算すると約 8 件のスパムメールを受信している。 日別で多少のばらつきはあるが、大きな変動は見られなかった。
ＳＯＭＰＯリスクマネジメント（UTM）	
検知数	67,080 （内訳:スパムメールフィルター （8,566））
検知内容	導入した企業の 7 割超の企業で何らかの迷惑メールを受信していることを確認した。 検知したスパムメールをブロックするだけでなく、分類でタグ付けし通知した。 ・既知のスパムメール送信者から送られた迷惑メールと確定しているメール:26,279 ・新たなスパム攻撃に関連があると思われるメール：351 ・既知のスパムメール送信者からのメールではないが、迷惑メールである可能性のあるメール:40,450

MS&AD インターリスク総研（UTM）	
検知数	236,842 （内訳：スパムメール対策）
検知内容	スパムメール対策は最も多く検知したもので、無数に飛び交うメールは危険なものが多く、中小企業においてもサーバー被害のきっかけになり得ることを示していると思われる。
名古屋商工会議所（メール対策ツール）	
検知数	60 （内訳：標的型攻撃メール（疑い）の受信（0）、スパムメール（疑い）の受信（60））
検知内容	標的型攻撃の疑いのあるメール受信は、0 件、スパムメールの疑いのあるメール受信は 60 件であった。導入社数は 7 社。また、導入時の問題点として中小企業は取引先がフリーメールを使用していることが多く、導入したメール対策ツールの初期設定ではフリーメールは、一旦保留され、承認処理が必要であるため、導入作業の負担が多くなってしまった。
大阪商工会議所（UTM）	
検知数	199 （内訳：内部の脆弱性）
検知内容	古いバージョンのソフトウェアを使用していることが検知された。 昨年度の実証では InternetExplorer の使用を、今年度は Adobe Flash player（2020 年 12 月 31 日でサポート終了）を検出した。 古いバージョンのソフトウェアは脆弱性が発見されても修正されることがないため、使用し続けることはセキュリティリスクとして懸念される。
高松商工会議所（UTM①）	
検知数	8,465 （内訳：スパムメール検知）
検知内容	アンチスパムを検知した件数の上位 3 位までで全体の 67%に相当した。送信元アドレスの多くはショッピングサイト、インターネット通販事業者からのメールがスパムメールと判定された。 インターネット通販を日常的に利用している事業者においては検知される可能性が高い。ただ、検知された一部のアドレスは不審なドメインも散見され、フィッシングサイトへ誘導するようなメールの可能性もあった。
高松商工会議所（UTM②）	
検知数	43,887 （内訳：スパムメール検知）
検知内容	スパムメール検知は、受信者の意向を無視して一方的に送付される迷惑メールを検出し、2020 年 10 月に 3,827 件、11 月に 29,966 件、12 月 10,078 件のスパムメールを検知した。

BCC（UTM）	
検知数	25 （内部の脆弱性）
検知内容	Null パスワードによるログインが出来る脆弱性をついた攻撃（バッファオーバーフロー／無認証ログイン）を 21 件検知、Web 通信の中に Basic 認証を使い、不正アクセスを試みようとする疑いのあるコードを 4 件検知した。

表 41 その他のアラート検知の状況

3.3. アンケート等によるセキュリティ対策状況等の把握

本事業では、お助け隊事業者がそれぞれ実証参加企業等へのアンケート等による状況調査、脆弱性診断等による調査を行い、中小企業におけるセキュリティ対策状況等を把握した。

3.3.1. アンケート調査結果

本事業では、各事業主体が実証開始・終了時や事業説明会・成果報告会開催時に、実証参加企業等へのアンケート調査やヒアリング調査を行い、セキュリティ対策状況等を把握した。以下にアンケートにおける主な調査ポイントごとにセキュリティ対策状況等の確認結果を示す。

※本項では、お助け隊事業者の略称を以下のように示す。

①東日本電信電話（略称：NTT東）
②東北インフォメーション・システムズ（略称：TOiNX）
③富士ソフト（略称：FSI）
④デジタルハーツ（略称：DH）
⑤富士ゼロックス（略称：FX）
⑥ＳＯＭＰＯリスクマネジメント（略称：ＳＯＭＰＯ）
⑦MS&ADインターリスク総研（略称：MS&AD）
⑧名古屋商工会議所（略称：名商）
⑨大阪商工会議所（略称：大商）
⑩高松商工会議所（略称：高松商）
⑪BCC（略称：BCC）
⑫西日本電信電話（略称：NTT西）
⑬沖電グローバルシステムズ（略称：OGS）
⑭PFU（略称：PFU）
⑮東京海上日動リスクコンサルティング（略称：TRC）

(1) 調査ポイント１ 現在、自社で実施しているセキュリティ対策
（自社で導入したセキュリティ製品やサービス、社内体制や教育実施等）

- 現在実施しているセキュリティ対策の上位は、「ウイルス対策ソフト」「重要ファイルのバックアップ」「出入口対策」であり、情報窃取・漏えいの脅威に対する対策は大半の企業で導入済み。（NTT 東）
- サイバーセキュリティ対策に対しての課題は顕在化しているが、具体的に何を対策すればよいのか、どこまで対策すればよいのかといった意見が多数。（FSI）
- 情報セキュリティ対策が行き届いていない企業（５分できる！情報セキュリティ自社診断”で 69 点以下の企業）が８割であり、４割以上の企業は情報セキュリティに関するルールがなく、対応方針を組織外に宣言している企業はゼロ。（FX）
- IT 資産に関する情報は半数以上が管理なされていない状況。（DH）
- UTM は約 20%しか導入が進んでいないが、ウイルス対策ソフトは 90%以上が導入済み。（DH）

- ウイルスソフト対策は 9 割近くの企業が実施している。（FX）
- 半数の企業では、情報セキュリティに関するルールがない。また、対応方針を組織外に宣言している企業は 3 割未満。（FX）
- 9 割以上の企業では、インシデント発生時に対応できる体制がない。（FX）
- ウイルス対策ソフトの導入率は高いが、それ以外の対策（データバックアップ、UTM、ファイアウォール）も一定水準で導入されている。（ＳＯＭＰＯ）
- 基本の対処はできているが、社内教育や周知が弱い。（BCC）
- ウイルス対策ソフトは 100%近い中小企業で導入されているが、UTM は半数を切っている。（NTT 西）
- 実施状況が低い部分として、次の部分が特徴的。①セキュリティポリシーやセキュリティ規定、②セキュリティを任せる専門業者との関係構築、③社員の情報システムの利用管理・制限。（NTT 西）
- OA 系のネットワークに接続されるパソコンについては、最新 OS のアップデートや、セキュリティパッチの適用といった基本的なセキュリティ対策の取組みは実施されつつある。しかしながら、FA 系のネットワークに接続されている、もしくはスタンドアロンの設備制御用パソコンや PLC については、OS バージョンアップやパッチ適用の影響で接続する設備の制御ができなくなる危険性があるため、古い OS が残存していたり、セキュリティパッチへの適用が進んでいないケースが多い。（TRC）

表 42 アンケート調査結果　調査ポイント 1

【考察】

ウイルス対策ソフトは**9割程度**の中小企業で導入されているが、**UTM**の導入は**２割程度**しか進んでいない。セキュリティポリシーやルールの策定、インシデント対応体制の構築等の組織的な対応は遅れている。また、IT資産に関する情報については半数以上が管理されていない。

オフィス系については基本的なセキュリティ対策は実施されているものの、工場系では古いOSの残存やセキュリティパッチ適用が進んでいない状況が見られた。

⑵　調査ポイント2　情報セキュリティ対策にかける費用

（現在かけている費用、今後かけられる費用、お助け隊サービスを継続した場合の費用等）

- 経費も十分には掛けられないため必要最低限の対策のみを実施している傾向が見受けられる。（FSI）
- セキュリティ対策の検討額として中央値 10,000 円（月額）が判明したが、あくまで検討額であり、実際に導入を促すためには金額だけでなく、導入が必要と感じられることが必要。（高松商）
- セキュリティ対策費用は、半数近くの企業が 50 万円／年以下。（BCC）
- サイバー攻撃を受けるリスクについて「ないと思う」との回答が 6.6 %であるのに対して、セキュリティ対策には「予算は全くかけていない」が 37.7 %、「12 万円未満（月額 1 万円未満）」が 45.3%であった。リスクが「ある」と自覚している企業においてもセキュリティ対策に予算はかけられていない。（NTT 西）
- セキュリティ対策予算について、「まだ不足」「とても不足」と考えるのは約 70%。しかし、セキュリティ対策に対して「費用はかけない」と考えるのは 39.5%。（OGS）
- 半数の企業が月額 PC1 台あたり 500 円～1000 円で対策したいと考えている。（PFU）

表 43 アンケート調査結果　調査ポイント 2

【考察】

サイバー攻撃を受けるリスクは認識されているものの、セキュリティ対策について予算は全くかけていない、あるいは最低限のみ対策費用をかけているという企業が多かった。支払可能な金額は、**月額1万円程度**の回答が多かった。

(3)　調査ポイント3　情報セキュリティ対策を進める上での課題

（現在のセキュリティ上の課題、何が解決すれば取組みが進むのか等）

- 「管理体制の構築」、「セキュリティ対策専門人材の確保」、「インシデント発生時の体制の構築」で 47%を占め、体制面の整備が中小企業の大きな課題。（NTT 東）
- 「情報収集（最新技術動向や事故事例）」が 12%と一定程度あり。（NTT 東）
- セキュリティ対策が進まない理由は、主にサイバーセキュリティ担当者が明確となっていない、費用を捻出することが困難、人的リソースが不足、対策を検討する要員の知識不足であった。（TOiNX）
- 傾向として、情報セキュリティ担当者は他の業務と兼務するケースが多く、専門部署として確立した企業は非常に少ない。（FSI）
- サイバーセキュリティに関するリスクがあることは認識されているが、実施にインシデントが発生したことがない企業が多く、実感として捉えにくいといった意見も見受けられた。（FSI）
- 「何を導入すべきか」が最も大きな課題となり、次いで人員面、コスト面となった。強化点については対策以前に社内ルール・教育面が必要と考えている企業が多い。（DH）
- セキュリティ担当を専任が行っているのは約 8%と低い。（ＳＯＭＰＯ）
- 過去サイバー攻撃を受けたと認識している事業者は約 10%と少数だが、Emotet やランサムウェアによる攻撃を受けていた。対策を講じるきっかけとしては、自社や自社にとって身近な組織が実際にサイバー攻撃を受けることが影響しやすい。（ＳＯＭＰＯ）
- セキュリティ専任者がいるのは 50%以下である。（BCC）
- 社員のセキュリティ教育、セキュリティ担当者の育成のどちらも「特に行っていない」が 60 %以上であり、セキュリティに関する社員育成が組織的に行われていない。（NTT 西）

表 44 アンケート調査結果　調査ポイント 3

【考察】

中小企業におけるセキュリティ対策の課題は**専門人材の不足**（兼任が多い）、社員や専門人材に対する**教育**がなされていない、**費用**がかかるといった点が挙げられた。何を対策すべきかわからないという課題もある。情報収集（最新技術動向や事故事例）に対するニーズも見られた。

セキュリティ対策を講じるきっかけとしては、自社や身近な組織が実際にサイバー攻撃を受けることの影響が大きい。

(4)　調査ポイント4　セキュリティ対策について取引先からの要求の有無

（サプライチェーン対策の観点で、上流企業が取引先に対しての要求状況等）

- 過去に取引先企業から義務付けられた対策の上位 3 項目は「ウイルス対策ソフト」「社員教育」「セキュリティポリシー策定」。（NTT 東）
- 取引先からセキュリティ対策の要求があるのは 4 割弱。（大商）
- 半数近くの企業が取引先からセキュリティ対策を要求されている。（BCC）

- 取引先からのサイバー攻撃対策の要請があるのは約 32%。（OGS）
- 昨年度、取引企業から一定レベルのセキュリティ対策が要件に含まれるケースがあった企業は約 4 割、「防衛」または「航空宇宙産業」という名目で特別な対策が要求されたのは 4 割弱。（PFU）
- （実証対象である自動車産業において）取引先からサイバーセキュリティ対策について要求があるのは 8 割近くに達する。（TRC）

表 45 アンケート調査結果 調査ポイント 4

【考察】

取引先からのセキュリティ要求については、30%～50%弱が要求ありという状況であった。防衛または航空宇宙産業での特別な要求は見られないが、**自動車産業**においては**8割近くの企業が取引先からセキュリティ対策に関する要求を受けて**いた。

(5) 調査ポイント5 テレワークの導入を進める上での課題
（テレワーク利用のセキュリティ対策や運用ルールの整備状況等）

- 岩手県ではテレワーク率が非常に低く、オフィスでの業務をスタンダードとする IT 環境となっており、サイバー攻撃対策傾向にもその傾向が現れている。（FSI）
- テレワークを導入していると回答したのは 2 割弱。リモートツールやテレワーク用端末配備等技術的な対策が取れていないためサイバーリスクへの懸念がある。（ＳＯＭＰＯ）
- テレワークに関する課題としては「ネットワーク環境の整備」（57.1%）、「情報セキュリティ対策・体制」（42.9%）が挙げられている。（OGS）

表 46 アンケート調査結果 調査ポイント 5

【考察】

中小企業におけるテレワークの実施率はそれほど高くないという結果であった。テレワークを実施している中小企業におけるセキュリティ上の課題としては、リモートツールの未整備、私物端末の利用、ネットワーク環境の未整備等の**技術的な対策**が挙げられていた。

3.3.2. 脆弱性診断等によるセキュリティ対策状況等の把握

本事業では、事業主体ごとに、希望する中小企業に対して、①インターネット上に公開している自社のホームページやサービスサイト等に情報漏えいやページの改ざんに繋がる脆弱性（弱点）がないかを診断する「**外部診断（Web アプリケーション診断）**」、②社内 PC 上に脆弱性がないかを診断する「**社内 PC 脆弱性診断**」、又は③参加企業に対してヒヤリング等を行い、その結果を分析しセキュリティ対策レベルを診断する「**簡易セキュリティ診断**」等の診断サービスを実施した。

以下に脆弱性診断等の実施結果の概要を示す。

・**外部診断（Web アプリケーション診断）**を計 278 社に実施した結果、クロスサイトスクリプティング[20]、ディレクトリインデックス[21]、OS コマンドインジェクション[22]といった危険度の高い脆弱性が合計 **116 件**確認され、**技術的支援**を実施した。 ・**社内 PC の脆弱性診断**は、計 81 社に実施した結果、セキュリティリスクが高い脆弱性が合計 **15 件**確認され、技術的支援を実施した。 ・**簡易セキュリティ診断**においても、多くの事業主体において参加企業の**約 7 割**の企業で**セキュリティリスクが高い状況にあると判定**された。

表 47 脆弱性診断等の実施結果

3.3.3. 標的型メール訓練によるセキュリティ対策状況等の把握

本事業では、事業主体の取組み内容により、実証参加企業のサイバーセキュリティに関する意識の向上を図るため、標的型メール訓練を実施した。

以下に標的型メール訓練の実施結果の概要を示す。

・**標的型メール訓練**においては、開封率は 1 割～3 割程度と実施内容によりバラバラであったが、**開封率 0 の企業はなかった**ことを踏まえれば、この点でのセキュリティリスクは残ると言わざるを得ない。 ・標的型メール訓練により、社員のセキュリティ対策意識が向上したと感じている企業が 6 割以上と一定の効果は得られたものの、それでも「一度で良い」と考えている企業も多く、**繰り返し実施することの必要性を伝えることが課題**。

表 48 標的型メール訓練の実施結果

[20] 「クロスサイトスクリプティング」とは、Web サイト利用者のブラウザに悪意のあるスクリプト(簡易プログラム）を送り込み、実行させることを許してしまう脆弱性

[21] 「ディレクトリインデックス」とは、Web コンテンツを格納するディレクトリ(フォルダ）配下のファイルが一覧表示されてしまう脆弱性

[22] 「OS コマンドインジェクション」とは、悪意のあるリクエスト(OS への命令）により、不正に操作されてしまう脆弱性

3.3.4. SECURITY ACTION の周知状況と実績

IPA では、2017 年 4 月から中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度である「SECURITY ACTION（略称：SA）」[23]の運用を開始し、多くの中小企業が情報セキュリティ対策に取り組んでいる（一つ星：情報セキュリティ 5 か条、二つ星：情報セキュリティ自社診断）。

本事業においても、各地域の実施主体が、実証参加企業を中心に地域の中小企業に対して、「SECURITY ACTION」および「中小企業の情報セキュリティ対策ガイドライン」[24]の普及に向けた周知啓発活動を行った。

(1) 実証参加企業の「SECURITY ACTION」宣言数

本事業の実証参加企業 1,117 社のうち、「SECURITY ACTION」一つ星を宣言した企業は 172 社（15.0%）、二つ星を宣言した企業は 48 社（4.0%）、計 220 社（19.0%）であった。[25]

以下に事業主体ごとの実証参加企業の「SECURITY ACTION」宣言数を示す。

事業主体	一つ星宣言 企業数	二つ星宣言 企業数
東日本電信電話	14	0
東北インフォメーション・システムズ	5	2
富士ソフト	9	4
デジタルハーツ	8	2
富士ゼロックス	24	12
ＳＯＭＰＯリスクマネジメント	8	1
MS&AD インターリスク総研	17	3
名古屋商工会議所	17	2
大阪商工会議所	8	5
高松商工会議所	12	2
BCC	11	2
西日本電信電話	9	1
沖電グローバルシステムズ	10	4
PFU	15	7
東京海上日動リスクコンサルティング	5	1
合計	**172**	**48**

表 49 実証参加企業の「SECURITY ACTION」宣言数

[23] https://www.ipa.go.jp/security/security-action/

[24] https://www.ipa.go.jp/security/keihatsu/sme/guideline/

[25] 対象である SECURITY ACTION 宣言事業者は、一部本実証事業参加企業以外、本事業の事象参加申込後に参加取り消しした企業も含まれる。

(2) 「SECURITY ACTION」制度の認知度

各事業主体において、本事業の事業説明会および報告会を中心に「SECURITY ACTION」制度の周知啓発活動を行った。説明会アンケート等を確認すると、「今回の説明会で初めて SA 制度を知った」とのコメントが多くあり、実証参加企業において「SECURITY ACTION」制度の認知度が高くない状況が昨年度に引き続き確認された。

一方で事業主体からは、「SECURITY ACTION」制度はセキュリティ対策に取り組むきっかけに有効であり、「SECURITY ACTION」等を浸透させていく活動を、地域側の支援体制も含めて官民協業で進めていくことが重要であるという意見が複数挙がった。

また、認知度が高くない理由として、「SECURITY ACTION」の実効性やメリットが把握しづらいのではないか、認知度を高める方法として、「IT 導入補助金の申請の必須要件になっているように、税制面や調達の優遇などビジネス面にプラスに働くような施策を講じてはどうか」という意見があった。

3.3.5. 実証参加企業へのヒヤリング

本事業の実証参加企業のうち、7 社から協力を得てヒヤリングを行い、参加動機、実施内容、得られた効果、今後についてまとめた事例集を作成した。

以下に、ヒヤリング先一覧を示す。なお、各企業の具体的な事例の内容については、別紙「サイバーセキュリティお助け隊 実証参加企業事例集」に記載する。

	地域	業種	従業員数	資本金
A 社	愛知県	卸売業	101～200 名	1 億円以下
B 社	広島県	製造業	201-300 名	1 億円以下
C 社	福島県	卸売業・小売業	6 名	600 万円
D 社	埼玉県	製造業	16 名	1,000 万円
E 社	千葉県	製造業	10 名強	3,000 万円
F 社	岩手県	製造業	201 名～300 名	5,000 万円
G 社	長野県	製造業	21～50 名	3,000 万円以下

表 50 ヒヤリング先企業一覧

3.4. 相談・インシデント対応ほか技術的支援の状況

本事業の実証では、事業主体ごとに実証に関する相談受付および対応等の実施体制（コールセンター）を構築し対応した。セキュリティ機器による検知、および脆弱性診断等の結果に基づき、**合計 293 件のインシデント対応ほか技術的支援を行った**。

他方で、セキュリティ機器の導入・設置支援等のための訪問対応が 257 件と多く、2019 年度事業と同様に、中小企業において**セキュリティ監視機器の自力での設置が困難**な状況も確認された。

対応種別	総数	相談・インシデント等対応状況	発生件数
コールセンター対応	616	実証参加に関する問合せ	78
		セキュリティ機器設置等の問合せ	285
		セキュリティ対応の相談（各サービスの製品情報・必要性の相談、表示内容の見方、操作・設定方法等の運用に関する問合せ）	56
		その他	197
インシデント対応ほか技術的支援	293	電話およびリモート等によるインシデント対応ほか技術的支援（※）	291
		訪問によるインシデント対応（駆け付け対応）	2
その他訪問対応	283	機器設置等のトラブル対応	26
		その他（セキュリティ機器の導入・設置支援等）	257

※「電話およびリモート等によるインシデント対応ほか技術的支援」には、訪問によるインシデント対応の一次対応を含む

表 51 コールセンター対応およびインシデント対応ほか技術的支援等の状況

3.5. インシデント対応事例

本事業の実証では、新型コロナウイルス感染症拡大の影響もあり、リモートにより管理可能なサービスの提供が多く行われ、インシデント発生に際しても概ねリモートによる支援対応が実施された。

インシデント対応事例として主な 4 事例の発生事象と対処状況を以下に示す。

項目	内容
発生日	2020年11月24日 (最初に要注意検知が発生した日)
発生事象	UTM サービスを導入した企業において、同一ホストにて断続的に**要注意検知が発生していることが確認**されたため、お助け隊事業者が駆けつけ支援を実施。
対処状況	現地にて取得した資料から、検知日時の前後で不審な動作がないか、レジストリやイベントログを確認した。また、ハッシュ値から本検知名のマルウェアは「アドウェア」に分類することが判明。 **対象のマルウェアと判定されたプログラム**は、インターネットからダウンロードしたフリーソフトであったことが判明、**駆除を実施**した。

表 52 インシデント対応事例 1

項目	内容
発生日	2020 年 12 月下旬
発生事象	UTM サービスを導入した企業において、PC の「ウィルス対策ソフト」を導入済みであったものの、直近 1 カ月の間に**「不正な IP アドレスへの通信（※）」が成立していることが確認**されたため、緊急度「高」のアラートを発報、支援を実施した。 （※）直近 1 カ月の間にマルウェアの通信先になっていたことが確認されている IP アドレスへの通信
対処状況	担当者に確認したが、当該通信が検知された時点の作業内容は覚えておらず、意図した通信であったかは不明であった。 当該 IP アドレスはホスティング業者のもので複数のドメインに紐付いており、マルウェアが通信をする際に当該 IP アドレスを経由したと考えられる。 UTM の機能では検出できなかったリスクを SOC 機能により補足できた事例である。 接続元端末を LAN から分離した上、ウィルス対策ソフトでのフルスキャンを実施した結果、何も検知されなかったため、再びアラートが発報されるまで様子を見ることし、案件クローズとした。 本件では、被害は確認されていないが、仮に情報漏えい等の被害に至っていた場合の**被害試算額**は、**54,760,000 円**であった。

表 53 インシデント対応事例 2

項目	内容
発生日	2020 年 10 月 1 日 【UTM 設置 5 日後】
発生事象	UTM サービスを導入した企業において、**マルウェアへの感染の疑いがある通信を UTM で検知**、リモート支援により駆除を実施。
対処状況	該当端末（PC）を LAN から分離した上でフルスキャンを実施した結果、**Hacktool およびトロイの木馬、計 6 件のマルウェアを発見したため駆除を実施**した。

表 54 インシデント対応事例 3

項目	内容
発生日	2020 年 12 月 11 日（対応完了日）
発生事象	EDR サービスを導入した企業において、**不正プログラム「ブラウザハイジャッカー」**を EDR で検知、駆除方法を案内
対処状況	駆除方法を案内したが自力で対応出来なかったため、**お助け隊がリモート支援により駆除を実施**した。

表 55 インシデント対応事例 4

3.6. 実証参加企業から寄せられた声

本事業の実証参加企業のアンケート結果より、多くの声が寄せられた。大別すると以下のとおり。

自社へのサイバー攻撃動向が把握できた

・傾向の把握、他社比較が参考になった。
・サイバー攻撃の数値化ができた
・要注意のメールやサイトの傾向や情報が得られた。
・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。
・自社の現時点での弱点が分かった。その対応策についてのアドバイスが得られた。

社員のサイバーセキュリティ意識・知識が向上した

・サイバーセキュリティの知識が身に付いた。
・説明会で最新の知識を得ることができた。
・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。
・自社のセキュリティ面での改善に向けて、およそ何をすれば良いかを明確にすることができた。

自社へのサイバー攻撃・情報流出等が防げた

・攻撃内容が見える化され回避・遮断によって安心できた。
・PC、NAS からの不審なアクセスが確認できた。
・セキュリティ対策を行っていることで自社の社会的信用が向上した。
・何かあった時に駆け付け支援してもらえるので安心できる。

経営層に今後のセキュリティ対策提案がしやすくなった

・セキュリティレベルが客観的に審査されることにより、経営層に今後のセキュリティ対策提案がしやすくなった。
・情報セキュリティ計画を策定することになった。
・サイバーセキュリティ対策について自社のやり方が正しいか、全体を俯瞰してコンサルティングするサービスをしてほしい。

4. 実証結果を踏まえた検討の実施

4.1. 中小企業向けに必要なサイバーセキュリティ対策サービスの内容

本事業の実証結果を踏まえ、各事業主体において、中小企業の実態やニーズに応じた必要なセキュリティ対策サービスの内容（対応範囲や費用等）や求められる人材スキル（スキルレベルや規模感等）を検討した。

以下に各事業主体の中小企業向けセキュリティ対策サービスの検討結果を示す。

事業主体	実証結果	セキュリティ対策のサービス検討
東日本電信電話	・社内やテレワーク先で利用するためのツールとして手軽に導入・運用できる Microsoft365 に代表される SaaS サービスを活用し、メール、ストレージ、コミュニケーションツールを利用する企業が増加。 ・Emotet や IcedID 等に代表される新種、亜種マルウェアを活用した未知脅威の攻撃が拡大。セキュリティ対策のベースとなる GW型セキュリティ、エンドポイント型セキュリティ対策といった基本となる多層防御だけでは防ぎきれず、実際に取引先がマルウェア感染したという事例も散見。	クラウドアプリケーション向けのセキュリティ対策： ・SaaS 型サービスはその構成上、元々企業が用意している社内防御機能（UTM、FW 等）が働かないケースが増えるため SaaS 型サービスに特化したセキュリティ対策が必要。 エンドポイントセキュリティ対策の強化： ・EDR、MDR 等の技術やサービスを活用した未知脅威検知や早期発見、対処を実現するセキュリティ対策の強化が必要。
東北インフォメーション・システムズ	・パソコンに対するウイルス対策は、すべての企業で実施済みであるが、UTM、パソコン以外のウイルス対策、Web コンテンツフィルタリング、侵入検知/防御装置（IDS/IPS）などネットワークで実施する対策は 40%以下にとどまった。	・以下の対策を実施するだけでなく、環境が激しく変化するため、セキュリティ対策はマネジメントしなければならず、継続的な取組が必要である。 ➢ SECURITY ACTION 二つ星を宣言（情報セキュリティ基本方針を定める）。 ➢ セキュリティの責任者、担当者を任命。 ➢ 不足している防御対策を実施。
富士ソフト	・簡易セキュリティ診断のオフィス環境の調査結果は、全国全業種平均と比べ「破棄、施設管理、社内規定周知」では、平均より高水準だが、「事故対応、対策の明確化、インターネット」は、平均より低い状況であった。 ・簡易セキュリティ診断の在宅/テレワーク環境の調査結果は、「対策の明確化、無線 LAN、ルータ対策」面での対策が低い状況であった。 ・中小企業でも約 32%が「何らかのサイバー攻撃を受けたことがある」との回答があり、また、セキュリティ監視システムを使用したサイバー攻撃の実態把握において 7 件のインシデントに対し通報を実施した。大企業と同様に、サイバー攻撃のリスクにさらされていることが分かる結果となった。	・実証で明らかとなったセキュリティ監視サービスの課題（設置マニュアルの改善、通報フォローの検討など）を改善し、セキュリティサポートパッケージとして提供することを検討する。 ・ユーザ企業向け： – 簡易セキュリティ診断＋セキュリティ健康診断 – セキュリティ監視（SaaS 型） – 相談窓口 – リモート支援 – 駆け付け支援 ・ 地域 IT 事業者向けに、営業/運営ツール、紹介資料などの整備をする。
デジタルハーツ	・多くの中小企業においてセキュリティの専任者は不在であり、手探りで対応を行っている状	・担当者の悩みに寄り添って現実的な対応を指南する伴走型の支援が必要である。

事業主体	実証結果	セキュリティ対策のサービス検討
	況であった。 ・ セキュリティのレポートを送付しても、中小企業側には十分な知識や時間がない中で正確に読み解くことは難しい。 ・ 生産設備への投資は惜しまないが、セキュリティ投資はコストでありお金をかけることができないという声が多数あげられた。 ・ 参加動機の多くに、取引先からの求めがあり対応を行わなければならないという声も多く寄せられた。	・ ウェブ診断やメール訓練、UTM、EDR などの情報を分かりやすく把握できる一元的な情報把握方法が必要である。 ・ セキュリティ対策をしっかり行っているということをアピールできれば取引の拡大に繋がることが、セキュリティ投資を積極的に行う動機付けとなる。単に安全を提供するだけでなく、取引の拡大に繋がるサービス提供を行う必要がある。
富士ゼロックス	・ 多くの中小企業で「セキュリティ対策の必要性は理解しているものの、どのように実施すればよいのか分からない」という苦手意識の強さが明白になった。	・ 中小企業向けセキュリティサービスでは、できる限り中小企業側の手を煩わせないマネージドサービスを提供するのが好ましい。 ・ セキュリティ機能全体をプラットフォームにして、不足している専門人材やスキルの補完、整備が遅れている IT 環境のケア、通信状況の常時監視、インシデント発生時の対応等を、各中小企業の必要性に応じて提供できる仕組みが必要。
ＳＯＭＰＯリスクマネジメント	・ セキュリティ対策を講じるきっかけになる「自社へのサイバー攻撃の認識」や「取引先からの対策実施の要請」については、ほとんどの企業が実際に経験したことがなく、セキュリティ対策を実施する意識の醸成は十分とは言えない。 ・ 情報資産の管理までを一任出来る取引ベンダーの存在が、一定のセキュリティ水準の維持を可能にしている一方で、セキュリティ意識が醸成されにくい環境を作り出している可能性がある。 ・ セキュリティの担当者の専任者は少なく、兼務による担当者がほとんどで且つ 1 人の場合が多い。 ・ 担当者以外の従業員のリテラシーが低いことが、セキュリティ対策導入時や導入後の担当者の負荷を大きいものにし、新たな対策導入を検討する際のネックになっている可能性がある。	・ 中小企業等に対して多様な攻撃が高頻度で行われていることから、中小企業等においても、従来のウイルス対策ソフトによるエンドポイント対策に加えて、ネットワークの境界に設置して配下のネットワークを複数の機能で監視・検知する UTM サービスなどの境界防御を目的とする対策の導入が必要。 ・ テレワーク等により社外でパソコン等をネットワークに接続する機会が増えれば、社内ネットワークの外側で攻撃を受ける可能性が高くなる。ウイルス対策ソフトでは安全に隔離等の処理ができないものも存在することが確認されているため、ウイルス対策ソフトの機能を補完する対策として、パソコン等への EDR サービスの導入も必要である。
MS&AD インターリスク総研	・ セキュリティ対策にかける費用に余裕がない。 ・ 適切なセキュリティ対策といえる製品・サービスがわからない。 ・ セキュリティ対策を担う人材がいない。	・ 中小企業にとって最も重要なのはコスト面であることから適合する製品・サービスを展開していくことが必要。 ・ 中小企業が「まず関心を持ち→知識を付け→使い勝手を確認しながら→自社の規模や取り巻く環境から最適なサービスを見つけていく行動」につなげることが重要。 ・ 恒常的に多忙で限られた経営資源でやりくりしている中小企業においてセキュリティ専門人材を育成していくことは至難である。そこで管理サービス付きサイバーセキュリティサービスによってアウトソースすることでその不足を補うことが最適と考えられる。 ・ アウトソースするにしても目利き力のない中小企業においては、「お助け隊サービス」のような制度が必要。

事業主体	実証結果	セキュリティ対策のサービス検討
名古屋商工会議所	・リスクを把握できていない、知識不足。 ・安全性と利便性のトレードオフへの理解が不足。 ・セキュリティ対策の予算が低い（月額 1 万円以下）。 ・導入作業時におけるリスクがある。 ・セキュリティ要員の人材不足 ・マルウェアに対する対策が不十分（従来型のアンチウイルス対策のみ）。 ・出口対策が不十分。	・セキュリティ対策を考えるにあたり以下の 3 つの方針を検討した。 – 出口対策・マルウェア対策。 – セキュリティ知識が無くとも導入判断できる。 – 費用対効果が見込める。 ・下記のセキュリティ対策を推奨する。 – UTM の導入。 – エージェント型 Web 対策ツールの導入（従業員数および対策すべき PC が少ない企業の場合）。
大阪商工会議所	・今年度の参加企業の 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。 ・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。 ・私物の媒体や PC および 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。 ・情報セキュリティに関する知識を持った人材が少ない。	・UTM と SOC の改善： ➢ UTM 設置マニュアルの改善 ➢ UTM の脅威を検知するシグネチャの改善による過検知の減少 ➢ UTM の価格や機能に関するスリム化。 ・テレワークツールの取り扱い： 現段階では必要性の認識は低いものの、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、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となったため、テレワークセキュリティ対策のサービスについて継続検討する。
高松商工会議所	・関心・検討のきっかけがない。 ・商品・サービス利用料が高価である（サイバーセキュリティ対策の導入検討に値する価格は、月額 1 万円以下）。 ・相談窓口が無い。	・関心を持つきっかけづくり（啓発活動の実施が必要）。 ・コスト高となる過剰なサービスを見直しなどのコスト削減の検討。 ・最低限の機能として、インシデント・事故が発生した際の相談窓口等のサービスやサイバー保険の付帯をするべきである。 ・継続的な訓練による社員全員の危機意識の底上げ ・経営陣の啓発とともに、社内インフラとしてのセキュリティ担当者の設置を推奨・支援していく必要がある。
BCC	・九州地域のセキュリティ意識や対策レベルが全国と比較して低い。 ・セキュリティサービス導入に手間取った。 ・より安価でインシデント発生時の対応支援までカバーしたサービスへのニーズあり。 ・今回提供したセキュリティサービスにより多くのマルウェア検知や不正通信遮断を確認でき、サービス導入による一定の効果が認められた。	・サービス導入時の容易性については、改善の必要性が高い。 ・エンドポイントとネットワークの両面をカバーした安価かつ簡便な中小企業向けサイバーセキュリティ対策サービスが必要。
西日本電信電話	・実証事業を経て、実証参加企業の意識の変化が見られた。 – サイバーリスクに対する課題の具体化。 – UTM の認知、導入意向の向上。 – サイバーセキュリティ対策に対する許容コストの拡大(「予算なし」が 38%から 16%に下がった)。	・実証参加企業の約半数の企業でセキュリティ対策の必要性を実感し、継続利用の意思表示を得られた。 ・他方で実証事業終了後はセキュリティ対策は継続しない結果となっており、更なるサイバーセキュリティ対策を推進する必要がある。継続利用しない理由と対応先は以下のとおり。 ➢ 導入の必要性に納得していない。

事業主体	実証結果	セキュリティ対策のサービス検討
		「サイバー攻撃を受けるリスクはないと思う」と考えている企業が一定数おり、セキュリティ対策の必要性を啓発する活動が引き続き必要。 ➢ 費用対コストに納得していない。 セキュリティサービスは安価であれば利用されるといった簡単なものではないことは明らかであるため、既にビジネス化しているサービスの低廉版を検討するだけでなく、サイバーセキュリティ対策の啓発活動や関連サービスの提供、事後対応などについて、その分野の専門企業が連携して提供することをさらに検討していく。 ➢ サービス提供者に納得していない 熊本県内の ICT 関連企業全体で、中小企業の ICT 促進とサイバーセキュリティ対策に必要なサービスを準備していくことで、サイバー保険による補償範囲とも組み合わせて、中小企業がより自社に適したサービスを利用できるようにしていく。
沖電グローバルシステムズ	・ サイバー攻撃を受けているがその認識がない。 ・ ネットワーク環境が多様で、且つ管理が行き届いていない。 ・ 社内に専任の IT 管理者が不在。 ・ セキュリティに対する意識および知識が不足。 ・ セキュリティ対策への予算割当てが困難。	・ サイバー攻撃状況の可視化。 ・ 多様な環境へ対応するための柔軟な対応および体制 ・ 専門知識を必要としないシンプルな導入。 ・ 受容可能な価格設定とリスクファイナンスの意識付け。 ・ 平常時からの情報提供と接点構築。
PFU	・ 小規模な会社の場合、機密データ(図面、部品)の受け渡しに、一部の担当だけでなく、全員が関わっている。 ・ セキュリティ対策整備状況診断を実施した 50 社中、CMMC L1 レベルに適合したのは 5 社（10%）のみ。 ・ システムのユーザ管理に関するものや、多要素認証の適用、FW の設定などのシステム環境などに不適合項目が見られた。 ・ PC の OS やソフトを最新に保つ仕組みは 50%程度に留まる。 ・ 意識調査アンケートでは VPN により外部からオフィス内に接続を行っており、工場ネットワークと分離されていない環境下では、よりリスクが高くなっている。	・ 機密データの受け渡しでは、小規模な会社では全員が関わっているため、全社員への啓発が重要。 ・ 未実施の項目に絞って対策を行えば、一定の水準になりうる企業もあることから、適切な指導を併せて行い、無駄なく効率的にセキュリティ対策のレベルアップを行うこともできる。 ・ 工場ネットワークとオフィスネットワークが接続されている環境下では、よりリスクが高くなっているため、安全性の異なるネットワーク境界に、何かしらの対策を導入し、ネットワークへの不要な機器の接続を防止することが望まれる。 ・ セキュリティに関する専門家の意見を得られる環境作りが必要。
東京海上日動リスクコンサルティング	・ セキュリティに対する全社的な課題認識の不足(IT 部門と FA 系部門の連携)。 ・ セキュリティ対策における人的リソースの不足。 ・ セキュリティ標準として何をどこまで規定すべきかが不明確。	・ 業界団体や組合、OEM メーカー等と連携して普及促進をすることで、経済的で簡易に提供できる仕組みを構築する。 – 中小企業の経営者向け啓発活動。 – サプライチェーンの業界団体や組合、OEM メーカー主導によるセキュリティ標準の策定。CS/SU 規則の

事業主体	実証結果	セキュリティ対策のサービス検討
	・ 不正アクセスの検知など、サイバー攻撃への一歩踏み込んだ対策が不十分（FA ネットワーク）。 ・ 自社の取引先に対するセキュリティ状況の把握が出来ていない。	施行への対応。 – セキュリティ対策レベルの把握および対策に向けたセキュリティ診断の定期的な実施。 – 中小企業が経済的に利用できるセキュリティ監視および侵入防御サービスの提供(UTM+SOC サービス)。 – 中小企業のセキュリティ担当者が気軽に相談できる窓口の整備

表 56　中小企業向けセキュリティ対策サービスの検討結果まとめ

4.2. 中小企業向けのサイバーセキュリティ簡易保険サービスのあり方

本事業の実証結果で得られた結果をもとに、各事業主体において、中小企業が利用しやすいセキュリティ簡易保険サービスのあり方について検討を行った。

- サイバー保険に対する認知度は 50%程度のところもあるなど、認知度が上がっていることが確認できたが、**サイバー保険に加入している企業**は、**10%未満と極めて低い水準**であった。
  その理由としては、サイバーリスクは目に見えないため、**必要性を感じていない**という声が多かった。一方で、必要性は認識しているものの加入しない理由としては「**予算がない**」という意見が多かった。

- 上記を踏まえ各事業主体で検討した結果、①**サイバー保険は製品やサービスの付帯保険として提供する**ことで中小企業にとって加入しやすい価格帯とする、そして②インシデントが発生した場合の賠償費用やフォレンジック等の本格的な調査・対処費用については、**任意保険として提供する**という考え方が多数であった。
- 他方で、中小企業によって**必要な補償範囲は異なる**ため、企業の規模やニーズに合わせて保険内容を変更することが出来る個別契約のサイバー保険の提供が望ましいという意見もあった。

表 57 中小企業向けのサイバーセキュリティ簡易保険サービスのあり方の検討結果まとめ

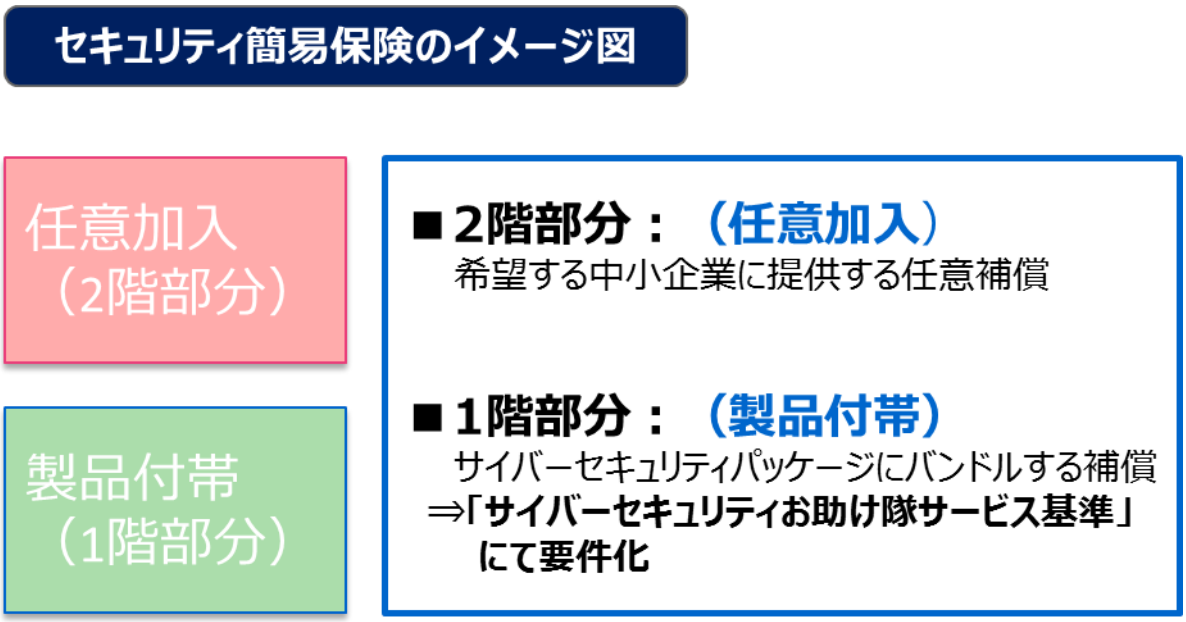


図 29 セキュリティ簡易保険のイメージ図

4.3. 実証終了後のサービス提供の可能性

本事業の実証結果を踏まえ、各事業主体において、実証終了後のサービス提供の可能性を検討した。

以下にビジネス化の事例として、本実証を通じて得た知見などに基づき事業主体が開発したサービス例を示す。

(1) 【ビジネス化事例】 大阪商工会議所

項目	内容
概要	• 「お助け隊サービス Ver.1.0」は、月額利用料金 6600 円（税込）という低価格を実現し、2020 年 4 月からサービス提供を開始した。 • 2020 年度は、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であった課題を解決し、地域展開窓口を担って頂いた各機関から今後の協力について積極的な発言を頂き、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。
費用	• サービス提供価格 月額 6,600 円（商工会議所会員） 月額 8,250 円（非会員）
保険	• 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・情報漏えい事故（最大 3 億円） サイバー攻撃等に起因、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・情報漏えい事故対応費用（最大 3000 万円） セキュリティトラブルへの対応やサイバー・情報漏えい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 • 2020 年度は、新型コロナ等により想定通りの活動は実施できなかったが、今後については、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（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されることから、大阪商工会議所および保険会社、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。

表 58 ビジネス化事例①（大阪商工会議所）

⑵ 【ビジネス化事例】 ＳＯＭＰＯリスクマネジメント 「SOMPO SOC」

項目	内容
概要	• ネットワーク内の監視対象機器のセキュリティログをクラウド上に自動で収集・分析し、不正アクセス等の重要なセキュリティインシデントを検知するサービス。（2020 年 2 月販売開始） • 企業側のネットワーク環境に設置された UTM のログをログ転送サーバ（Syslog サーバ）経由で同社の分析システムに送信し、分析結果をアラート通知する「セキュリティ監視サービス」と「UTM（Syslog サーバーを含む。）運用管理サービス」で構成される。
費用	・ 大企業向けサービスをベースに新たに開発した監視分析システムをクラウド上で稼働させることで、専門のアナリストがいなくても高度で高品質なセキュリティ常時監視サービスをリーズナブルな価格で提供することが可能である。
保険	・ 「SOMPO SOC」で検知したマルウェア感染やスキャン通信の対応に特化した専用のサイバー保険（引受保険会社：損害保険ジャパン株式会社）を自動付帯している。損害賠償責任だけでなく、ウイルス検索費用やウイルス駆除費用、オンサイト対応費用、データ保護費用、OS クリーンインストール費用等の各種費用損害についても当該サイバー保険の保険金が充当される。 （参考）保険金額：300 万円 ※ただし、1 事故当たり 30 万円を限度とする。

表 59 ビジネス化事例②（ＳＯＭＰＯリスクマネジメント：「SOMPO SOC」サービス）

⑶ 【ビジネス化事例】 ＳＯＭＰＯリスクマネジメント「SOMPO SHERIFF」サービス

項目	内容
概要	・ 地域実証でも利用した EDR によって従来のウイルス対策ソフトでは防ぐことができずに侵入してきたウイルス感染による脅威を早期に検知し、検知した脅威については、データ解析システムと専門のセキュリティエンジニアが調査・分析の上、緊急アラートメールでサービス利用者に通知し、早期駆除を可能にするサービス。
費用	・ 初期費用 35,000 円、月額 1 台あたり 1,800 円
保険	・ 「SOMPO SHERIFF」で検知した緊急性の高いウイルス感染の対応に特化した専用のサイバー保険（引受保険会社：損害保険ジャパン日本興亜株式会社）を自動付帯している。検知したウイルスの分析・駆除費用については当該サイバー保険の保険金が充当されるため、分析・駆除に必要な追加費用負担が不要となり、円滑に対処することが可能となるため、サービス利用者にとっては更なる安心を得ることができる。 （参考）保険金額：300 万円 ※ただし、被疑ファイル分析・脅威ファイル駆除に係る費用については、1 アラート当たり 16,000 円を限度とする。

表 60 ビジネス化事例③（ＳＯＭＰＯリスクマネジメント：「SOMPO SHERIFF」サービス）

(4) 【ビジネス化事例】MS&AD インターリスク総研：「エンドポイント監視サービス（EDR）」

項目	内容
概要	エンドポイントセキュリティ（EDR）セキュリティ監視サービス 防検サイバー 巧妙化するサイバー攻撃の手口に対して、防御だけではなく、脅威の侵入を素早く検知し、被害を最小限に止める「次世代エンドポイントセキュリティ（EDR）」と 24 時間 365 日の監視サービスを提供する「管理セキュリティサービス」がパッケージとなったサービス ・ 検知モード/防御モードの 2 種類を提供 ➢ 検知モードではマルウェアの挙動を検知・分析し、貴社の端末管理者、端末ユーザーへアラートを送信する。 ➢ 防御モードでは検知に加え、脅威があると判断した場合、自動で当該プロセスの停止や実行ファイルの隔離といった防御を行う。 ・ 端末に導入する防検サイバーエージェントと、管理サーバーの AI&アナリストによる多角的な監視でマルウェアを検知する。 ・ マルウェア関連の詳細ログは保存され、過去にさかのぼりインシデント調査が可能
費用	＜検知モード＞ 年額 1 台あたり 9,600 円 ＜防御モード＞ 年額 1 台あたり 12,000 円
保険	サイバーセキュリティ保険を付帯 （補償内容） 防検サイバーを導入した端末の所有・使用または管理に関連して発生した事故 （支払限度額） 賠償損害 導入端末あたり 50 万円（1 事故） 費用損害 導入端末あたり 50 万円（1 事故） ※支払限度額は導入端末数に応じて積算されるが、被保険者あたり 3,000 万円が上限 （免責金額） 賠償 無し、費用 １０万円

表 61 ビジネス化事例④ （MS&AD インターリスク総研：「エンドポイント監視サービス（EDR）」）

5. 全体のまとめ

本事業は、IPA が公募により全国 13 地域、2 産業分野で事業主体を選定し、事業主体が実施体制を組織することで実施された。事業主体が、説明会や個社訪問等を通じて地域の中小企業の参加を促すことで、計 1,117 社の中小企業が本事業に参加した。このうち、**延べ 1,190 社に UTM 機器などのセキュリティ機器等を設置**することで、サイバー攻撃に関する様々なアラートの検知および防御を実施し、中小企業におけるサイバー攻撃の実態把握を行った。

その結果、外部からの不審なアクセス、不正プログラムによる内部から外部への不正通信等を検知および遮断した。また、セキュリティ機器による検知、および脆弱性診断等の結果に基づき、**合計 293 件のインシデント対応ほか技術的支援が発生**し、そのうち電話およびリモート等によるインシデント対応ほか技術的支援を 291 件、**訪問によるインシデント対応（駆け付け対応）を 2 件実施**した。

インシデント対応ほか技術的支援は、2020 年度は新型コロナウィルス感染症拡大の影響もあり、当初からリモートによる管理可能なサービス提供が多く行われたこともあり、概ねリモートによる支援対応となった。

セキュリティ機器の導入・設置に関して自力で設置することが出来ず、お助け隊事業者が直接訪問し、設置支援等を 257 件実施した。**中小企業においては、自力でのセキュリティ機器設置はハードルが高く、導入マニュアルの拡充の必要性と共に駆けつけ支援が必要**である実態も確認された。

中小企業の参加募集については昨年度と同様、地域の団体や企業・ベンダー等と連携した募集活動が効果的であった。今年度は、コロナ禍により中小企業においてもセキュリティ対策の余裕がないことも想定されたことに加え、企業の参加募集については対面での説明会が実施できず、募集に苦労したケースも見られた。一方、オンラインのメリットを活用しオンデマンドでの配信を行うなど、視聴機会を増やすことで実証参加につなげた事例もあった。

中小企業におけるセキュリティ対策の課題は専門人材の不足（兼任が多い）、社員や専門人材に対する教育がなされていない、費用がかかるといった点が挙げられた。**セキュリティ対策を講じるきっかけとしては、自社や身近な組織が実際にサイバー攻撃を受けること**が影響しやすい。中小企業において、専門人材を確保することは困難であるため、外部の専門家からのサポートや、業界団体や地域の中小企業団体・ベンダー等の**身近なところから他社の事例を得られる等、外部からの情報提供が有効**と考えられる。

取引先からのセキュリティ要求については、3～5割弱程度が求められている状況であるが、自動車産業においては8割近くの企業がセキュリティ対策に関する要求を受けていた。

中小企業におけるテレワークの実施率はそれほど高くなかったが、テレワークに取り組む企業におけるセキュリティ上の課題としては技術的な対策が挙げられていた。今後、中小企業においてもテレワークの推進とともに技術的な対策についての情報提供やセキュリティ製品・導入支援が必要になると考えられる。

中小企業に望まれるセキュリティ製品・サービスについては、**導入を容易とするための最小限の内容・価格の低減が望まれる。**実証においては、UTM の設置においてネットワーク状況が不明、担当者の日程確保が困難など、設置に負荷を要する製品については導入がなかなか進まず、複数回の訪問対応が必要となる事例もあった。アンケート調査においても、**中小企業がセキュリティ対策費用としてかけられるのは月額 10,000 円程度との回答もあり**、負荷がかから

ず低価格で提供可能なサービスが望まれる。

セキュリティ対策においてカバーできない部分は、サイバー保険において対応するのが有効と考えられるが、今年度においてもサイバー保険の認知度は低い状況であった。サイバー保険の契約に関しても、認知度が低い現状を鑑みると、**最低限の保証内容を製品・サービスへ付加する形が効果的**であると考えられ、付加的なサービスが追加の契約にする等の方法が有効と考えられる。

今回の実証を通じて、複数の事業主体によって具体的なサービス提供が検討されており、今後地域の中小企業団体等や、セキュリティサービス提供者等が連携し、中小企業に向けたサービスが広がることが期待される。

以上