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）
－ 成果報告書（全体版） －

2020年4月21日

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

目　次

1. 背景・目的

IoT や AI といった技術により実現される「Society5.0」「Connected Industries」では、サイバー空間とフィジカル空間が密接に関わることにより、サイバー攻撃がフィジカル空間へ及ぼす影響が大きくなる。また、「Connected Industries」を始めとするネットワーク化の進展は、企業間のつながりなど様々な形のつながりを生むため、悪意のある者にとって新たな攻撃の機会となるおそれがある。さらに、攻撃の手法も進化しており、サイバー攻撃の脅威はあらゆる産業活動に潜むようになっている。

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

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。

一方で、中小企業がサイバーセキュリティに関して困ったときに気軽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するサービスに対するニーズはあるが、サービス提供側が、中小企業の被害実態や、中小企業支援に必要な人材スキル等の把握ができていないため、現状は中小企業のニーズに合った製品、サービスが提供されていない。

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、中小企業のサイバーセキュリティの被害実態等を把握することで、これら中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らかにする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. 事業実施の概要

2.1. 実証事業の内容

本事業は、地域の中小企業を対象として、地域の団体、セキュリティ企業、保険会社が実施体制を組み、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、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、中小企業に必要なセキュリティ対策サービスの内容、及び民間による中小企業向けのセキュリティ簡易保険サービスのあり方を検討した。

以下に実証事業の地域ごとの実施概要図を示す。

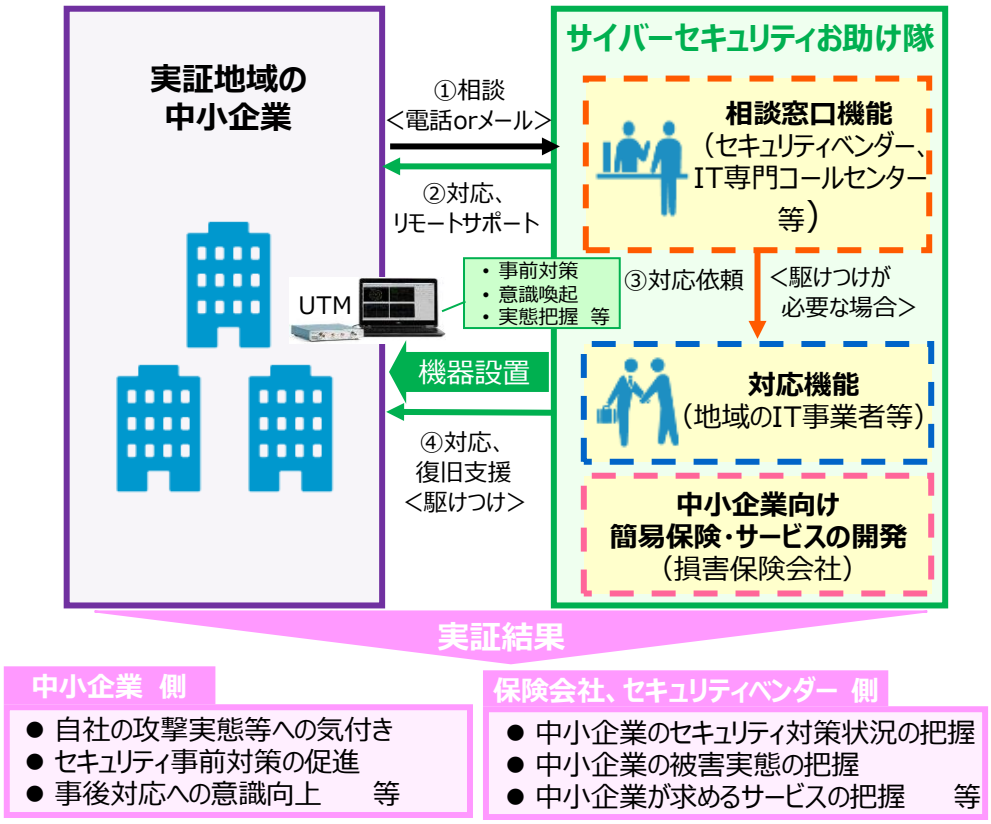


図 1 実証事業の地域ごとの実施概要図

2.2. 実証参加状況

本事業は、公募により全国 8 地域で請負事業者を選定し、請負事業者が事業主体となって実施体制を組織し、8 地域 19 府県の中小企業に実証事業の周知及び参加を呼びかけることで、計 1,064 社の中小企業が本事業に参加した。

以下に対象地域[2]、事業主体と実施体制、実証参加企業数を示す。

対象地域	事業主体	実施体制	実証参加企業数
①宮城、岩手、福島	株式会社デジタルハーツ	損害保険ジャパン日本興亜株式会社、株式会社アライブ、地元関係団体多数	111社
②新潟	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、東京海上日動リスクコンサルティング株式会社	148社
③長野、群馬、栃木、茨城、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	112社
④神奈川	SOMPOリスクマネジメント株式会社	損害保険ジャパン日本興亜株式会社、日本PCサービス株式会社、株式会社コムネットシステム、株式会社サイバーセキュリティクラウド、株式会社ラック、学校法人岩崎学園	150社
⑤石川、富山、福井	株式会社PFU	アイパブリッシング株式会社、損害保険ジャパン日本興亜株式会社　金沢支店、北陸先端技術大学院大学、PFU西日本株式会社	120社
⑥愛知	MS&ADインターリスク総研	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、NTTアドバンステクノロジ株式会社、綜合警備保障株式会社、デロイトトーマツサイバー合同会社	201社
⑦大阪、京都、兵庫	大阪商工会議所	東京海上日動火災保険株式会社、日本電気株式会社、キューアンドエー株式会社	112社
⑧広島、山口	株式会社日立製作所	損害保険ジャパン日本興亜株式会社、SOMPOリスクマネジメント株式会社、株式会社日立システムズ、広島県情報産業協会	110社
※対象地域の北から順に記載			**計 1,064社**

表 1 実証参加状況一覧

[2] 対象地域は採択した各事業主体の提案に基づき設定した。なお、本事業の実効性を高めるため、提案採択後、次の対象地域の拡大を行った。（③埼玉県 ⑤富山県、福井県 ⑧山口県）

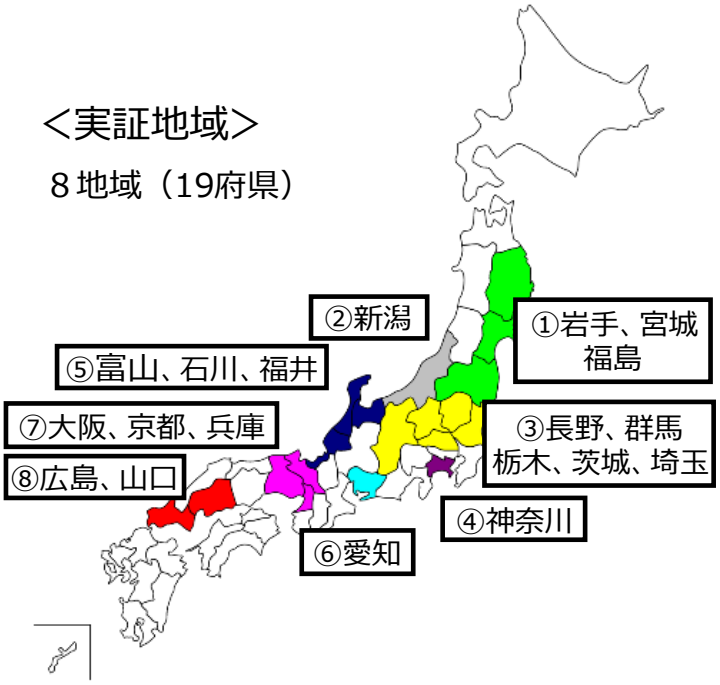

＜実証地域＞
８地域（19府県）
②新潟
①岩手、宮城
福島
⑤富山、石川、福井
⑦大阪、京都、兵庫
③長野、群馬
栃木、茨城、埼玉
⑧広島、山口
④神奈川
⑥愛知

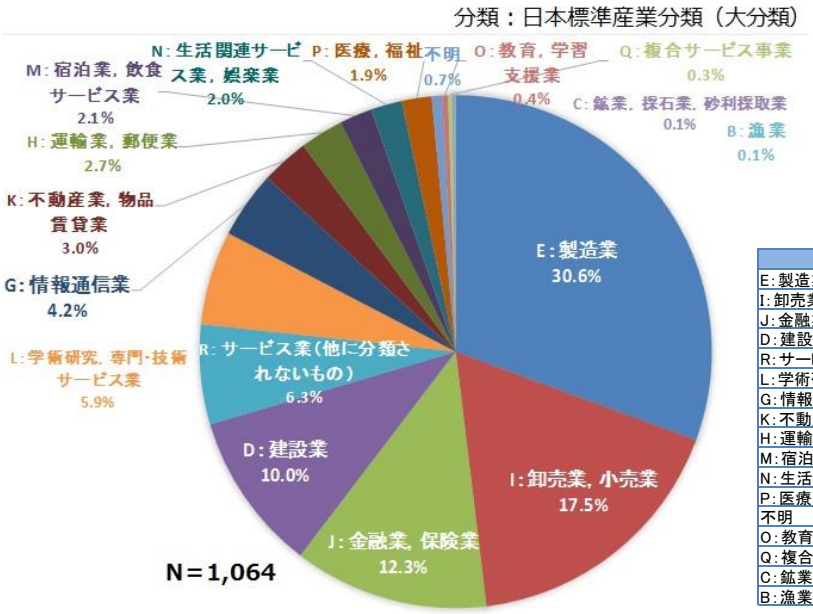
図 2 実証の対象地域

2.3.　実証参加企業の属性

本事業の実証参加企業 1,064 社の属性は以下のとおりであった。

（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 30.6%、次いで卸売業・小売業が 17.5%、金融・保険業が 12.3%であった。

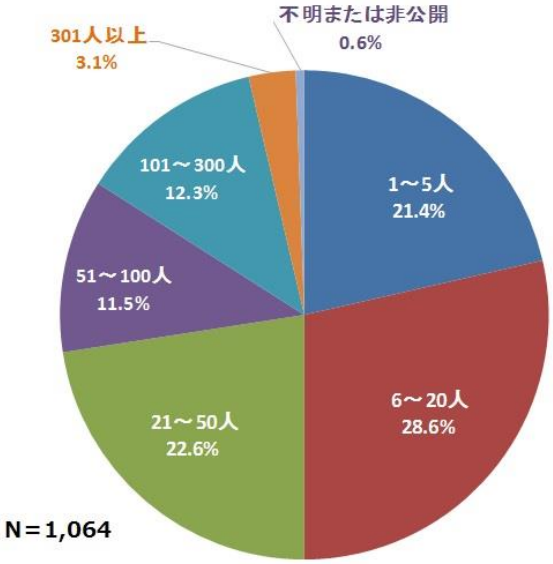


産業分類(大)	社数
E：製造業	326
I：卸売業，小売業	186
J：金融業，保険業	131
D：建設業	107
R：サービス業（他に分類されないもの）	67
L：学術研究，専門・技術サービス業	63
G：情報通信業	45
K：不動産業，物品賃貸業	32
H：運輸業，郵便業	29
M：宿泊業，飲食サービス業	22
N：生活関連サービス業，娯楽業	21
P：医療，福祉	20
不明	7
O：教育，学習支援業	4
Q：複合サービス事業	3
C：鉱業，採石業，砂利採取業	1
B：漁業	1

図 3 業種別一覧

（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、6~20 人が 28.6%、次いで 21~50 人が 22.6%、 1~5 人が 21.4%であった。



従業員層	従業員数
1～5人	228
6～20人	304
21～50人	240
51～100人	122
101～300人	131
301人以上	33
不明または非公開	6

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、対象地域の中小企業に対して実証事業の周知及び参加呼びかけ等を行うことを目的に説明会を実施した。説明会は、事業開始、中間報告、成果報告の各段階で延べ 96 回開催し、1,642 社、1,956 名の参加を得た。併せて、当該説明会の参加者に対しサイバーセキュリティに関する普及啓発を行い、中小企業のセキュリティ対策に関する意識向上を図った。また、中間報告会、成果報告会においては、実証事業で収集した中小企業におけるサイバー攻撃の実態などに関する情報のフィードバックを行った。

以下に各事業主体が実施した説明会・報告会の開催数と参加状況を示す。

事業主体	事業説明会			中間報告会			成果報告会		
	回数	社数	人数	回数	社数	人数	回数	社数	人数
①株式会社デジタルハーツ	4	40	52	1	25	26	1	22	23
②東日本電信電話株式会社	4	121	121	1	14	17	1	81	130
③富士ゼロックス株式会社	11	124	125	5	26	33	9	46	54
④SOMPOリスクマネジメント株式会社	6	52	52	5	19	27	3	27	36
⑤株式会社PFU	10	162	209	3	33	41	3	32	46
⑥MS&ADインターリスク総研株式会社	10	263	295	2	72	76	2	73	84
⑦大阪商工会議所	1	69	80	1	116	127	1	79	86
⑧株式会社日立製作所	5	109	170	1	15	17	1	22	29
合計	51	940	1,104	19	320	364	21	382	488

総計	回数	91	社数	1,642	人数	1,956

表 2 事業説明会の実施状況

2.5. 実証参加企業募集に関する状況

本事業は、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他、対象地域の事業主体の工夫により、以下の取組みを行った。

事業主体	参加企業募集のためのその他の取組み
①株式会社デジタルハーツ	・自社及び地場企業による開拓（55社）、地域団体からの紹介先同行訪問（110社） ・地方銀行からの紹介、大手自動車メーカー及び大手製紙会社のサプライチェーン企業へのアプローチ（具体的な参加企業獲得には至らず） ・ダイレクトメール（約9,700通）、アンケートによる勧誘活動（77社） ・地元有力新聞の事業紹介記事の掲載
②東日本電信電話株式会社	・自社支店の顧客への個別訪問による集客（営業担当者約40名） ・地域企業（Sier、電気工事会社等）の協力による選定ユーザへの訪問説明 ・メールマガジンを活用した集客（会員：約4,000名）
③富士ゼロックス株式会社	・テレアポ募集：コール約750件、うちアポ90件（約12%）、うち設置30社（約4%） ・製造業へのダイレクトメール配信、商工会議所等のメルマガ配信等（5社設置） ・販売会社の営業チャネル、地域ITベンダーによる集客活動（55社設置） ・大手自動車メーカーの地域工場、電機メーカー、精密機器メーカーのサプライチェーン中核企業に対するアプローチ（2社設置）
④SOMPOリスクマネジメント株式会社	・募集説明会を複数回追加開催 ・店頭チラシ設置（地域金融機関、地方公共団体、中小企業関連団体） ・グループの代理店網を活用した中小企業への参加呼び掛け （大手自動車メーカー及び一次サプライヤー企業については協力を得ることができず）
⑤株式会社PFU	・新聞メディアへの記事掲載（3紙） ・地域行政などの関係機関、団体への働きかけ（48団体） ・地域販社の協力による個社訪問活動（61社）
⑥MS&ADインターリスク総研株式会社	・グループ傘下の損害保険会社2社の対象地域の社員及び代理店による中小企業への呼び掛け（参加175社） ・地域メディア（新聞社、テレビ局）、行政機関・商工会議所等の協力による周知
⑦大阪商工会議所	・会議所の広報誌（3万社×3回）、ホームページ掲載、ダイレクトメール（1,324社）等 ・プレス発表（新聞5紙掲載、テレビ報道3回） ・会議所に関係する企業のTel後訪問（61社） （サプライチェーン上位企業から取引先に事業案内する取組みを依頼したが奏功せず）
⑧株式会社日立製作所	・商工会議所会員へのダイレクトメール9,000通、地域の情報産業協会及び自社顧客へのメルマガ配信 ・商工会議所会報、地元誌へのセキュリティ関連記事の掲載 ・個別訪問14社、ミニセミナー4回/21社、オンラインセミナー8回/11社

表 3 参加企業募集のためのその他の取組み

これらの取組みを実施する上で、各事業主体からは以下のような状況が報告された。

- ホームページへの掲載やダイレクトメールのみでは、事業内容をうまく説明できず参加に結び付かなかった。
- 事業主体の担当者や地場ベンダーの直接訪問による説明が一番効果があった。

・サプライチェーン上流企業からの紹介は、上流企業側の下請代金支払遅延等防止法の優越的地位の乱用[3]に抵触するとの懸念等から、上手く機能しなかった。

以上のことから、中小企業に対してサイバーセキュリティ対策の重要性を理解してもらうためには、信頼関係をベースとした対面での説明が必要あることがうかがえる。また、サプライチェーン上位企業からのアプローチは制約があることが分かった。

[3] 下請代金支払遅延等防止法（昭和 31 年法律第 120 号 第 4 条 1 項 6 号 に規定する「役務の利用強制」

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に対して、中小企業向けサイバーセキュリティ事後対応支援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。

（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[4]機器、EDR[5]ソフト等）を実証参加企業に設置（727 社）することで行った。

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		
		(設置数)	内訳	社数
①株式会社デジタルハーツ	111	81	ネットワークセンサー	81
②東日本電信電話株式会社	148	148	UTM機器	148
③富士ゼロックス株式会社	112	101	UTM機器	101
④SOMPOリスクマネジメント株式会社	150	110	UTM機器	38
			クラウド型WAF	0
			EDRソフト	72
⑤株式会社PFU	120	97	PC脅威検知ツール	97
⑥MS&ADインターリスク総研株式会社	201	55	据置型UTM	27
			クラウド型UTM	28
⑦大阪商工会議所	112	112	UTM機器	112
⑧株式会社日立製作所	110	23	UTM機器	10
			EDRソフト	13
計	**1,064**	**727**		

表 4 セキュリティ機器等によるサイバー攻撃の実態把握

[4] 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。

[5] 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。

（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、各事業主体が実証参加企業等（1,716 社）[6]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	実証参加企業数	アンケート等によるセキュリティ対策状況等の把握		
		(延べ数)	内訳	社数
①株式会社デジタルハーツ	111	40	参加企業アンケート	40
②東日本電信電話株式会社	148	390	セキュリティ対策アンケート	243
			標的型攻撃メール訓練	147
③富士ゼロックス株式会社	112	49	セキュリティ意識調査アンケート	49
④SOMPOリスクマネジメント株式会社	150	34	サイバーリスク簡易診断	18
			WEBアプリ簡易診断	16
⑤株式会社PFU	120	353	セキュリティ意識調査①	185
			セキュリティ意識調査②	37
			セキュリティベンチマーク診断	86
			公開サーバ脆弱性診断	45
⑥MS&ADインターリスク総研株式会社	201	377	事前アンケート	193
			サイバーセキュリティ演習	63
			事後アンケート	121
⑦大阪商工会議所	112	357	第1回説明会アンケート	69
			第2回説明会アンケート	118
			中間アンケート	65
			最終アンケート	105
⑧株式会社日立製作所	110	116	簡易セキュリティアセスメント	107
			現場セキュリティアセスメント	9
計	**1,064**	**1,716**		

表 5 アンケート等によるセキュリティ対策状況等の把握

6 アンケート等の実施先には、事業説明会の参加企業等、一部実証参加企業以外のものを含む。

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.　検知及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及び監視の仕組みを構築し、相談受付及び対応体制と共に、検知及び監視した結果がサイバーインシデント[7]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（事後体制支援体制）。

以下に事業主体ごとのセキュリティ機器等による検知及び監視の仕組みと実証結果を示す。

（1）株式会社デジタルハーツ（宮城、岩手、福島）

【セキュリティ機器】

＜ネットワークセンサー＞「Starlight」（Stellar Cyber 社）

【検知及び監視の仕組み】

監視対象ネットワークに設置したネットワークセンサーからのトラフィック情報を収集し、クラウド上のインシデント分析・管理システムへログデータを送信して分析、具体的な対応を行う。

【実証結果】

Starlight 上では多数のアラートを検知したが、分析・優先度付け（トリアージ）の結果、具体的対応が必要なセキュリティインシデントは確認されなかった。ただし、機器による検知以外の事象確認で、駆け付け対応を 2 件実施した（Emotet[8]感染対応）。

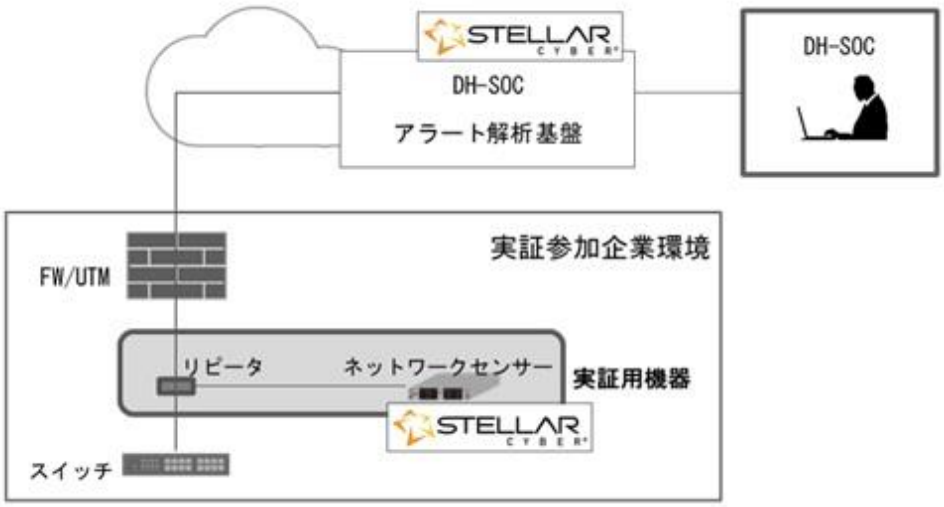


図 5 検知及び監視の仕組み（デジタルハーツ）

7 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。

8 Emotet（エモテット）：情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大が試みられる。

（２）東日本電信電話株式会社（新潟）

【セキュリティ機器】

＜UTM＞専用 BOX（「おまかせサイバーみまもり」サービス）

【検知及び監視の仕組み】

事前にユーザーのネットワーク環境の全件調査の上、UTM 機器を設置。セキュリティ監視により、ユーザー端末がマルウェア[9]感染の可能性がある場合、感染の確認及び駆除支援等を実施する。

【実証結果】

不正プログラム検知は、約 30%が Internet Speed Tracker ツールバー（接続速度テストアプリ）をインストールしたことにより、アドウェア[10]に感染したケースであった。

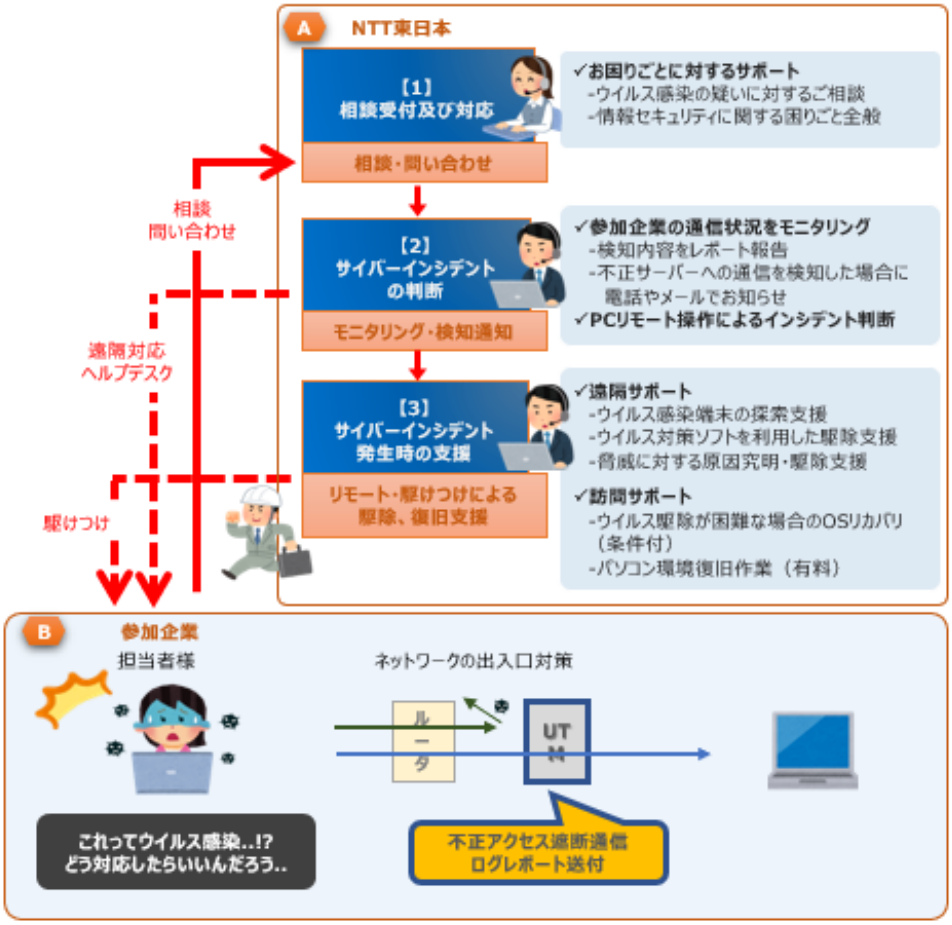


図 6 検知及び監視の仕組み（東日本電信電話）

9 マルウェア：コンピュータの正常な利用を妨げたり、不正に動作させる意図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。

10 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、ユーザー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。

（３）富士ゼロックス株式会社（長野、群馬、栃木、茨城、埼玉）

【セキュリティ機器】

＜UTM＞「beat-box」（富士ゼロックス）

【検知及び監視の仕組み】

外部からの不正アクセスは、UTM 機器がポートを遮断。ネットワークオペレーションセンターが遠隔監視で通信ログデータを収集し、異常と判断した場合は、コンタクトセンターが状況把握と対応を行う。

【実証結果】

検知した不正な通信検知数は合計で 6,757,458 件、1 日あたりに換算すると約 603 件/台となった。特にランサムウェア[11]「WannaCry[12]」の通信等、危険性が高い不正通信を 2 件検知、通信をブロックの上、追加調査を行った。

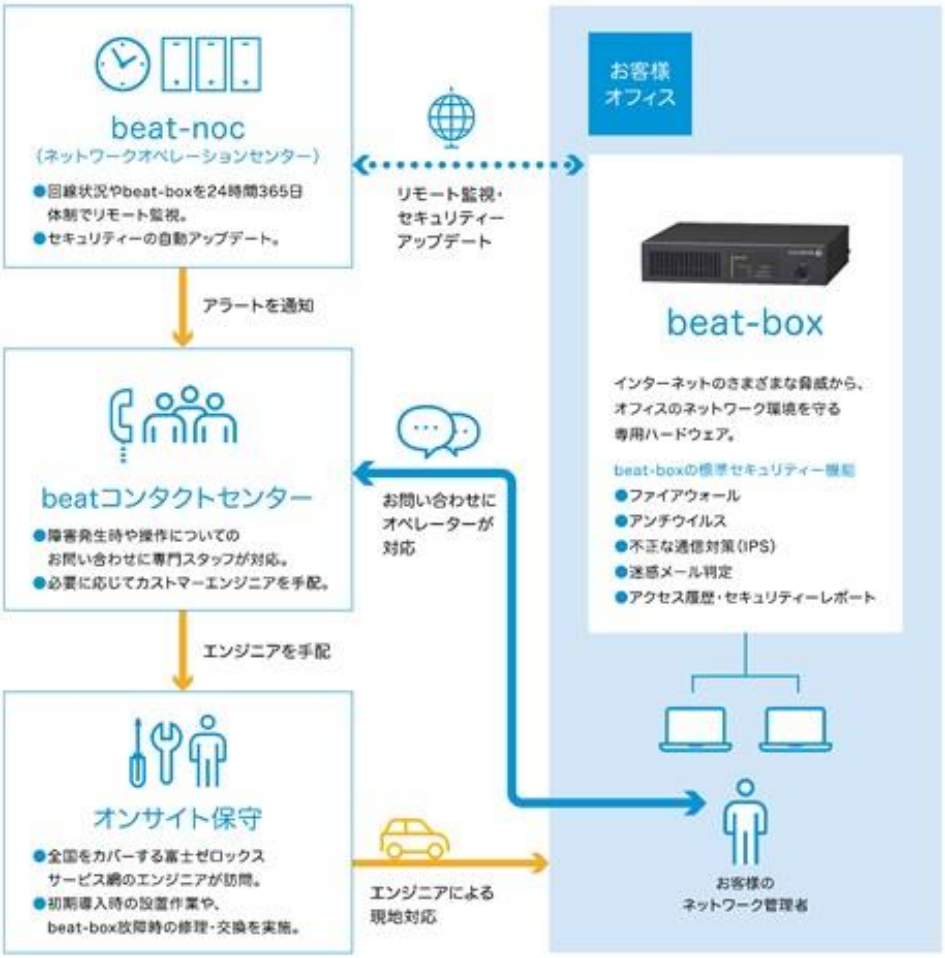


図 7 検知及び監視の仕組み（富士ゼロックス）

11 ランサムウェア：マルウェアの一種で、感染したコンピュータを正常に利用できないような状態に置き、復元のために「身代金」（Ransom）を要求する。

12 WannaCry（ワナクライ）：Microsoft Windows を標的としたワーム型ランサムウェアで、 感染したコンピュータの身代金として暗号通貨ビットコインを要求する。

（４）ＳＯＭＰＯリスクマネジメント株式会社（神奈川）

①UTM 機器

【セキュリティ機器】

＜UTM＞「Firebox M370」（Watchguard 社）

【検知及び監視の仕組み】

UTM 機器のセンサー（IPS[13]機能及び URL フィルタリング[14]機能）からのアラートに係るログデータを「セキュリティログ自動分析システム」に送信し分析することで、セキュリティインシデントを検出する。

【実証結果】

UTM 機器設置 38 社において、4 件の緊急度「高」のアラートを発信し、このうち 1 件は社内から外部への「不正な IP アドレスへの通信」であったため、駆け付け支援を行い不正プログラムの駆除を実施した（残り 3 件は UTM 機器で防御）。

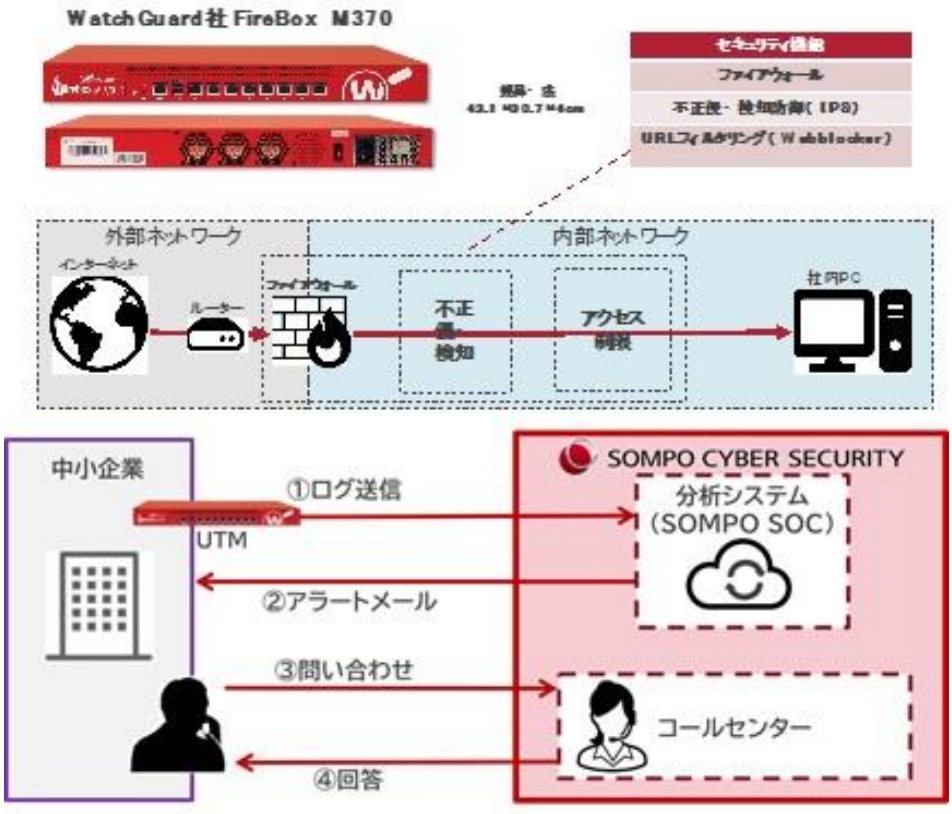


図 8 検知及び監視の仕組み（ＳＯＭＰＯリスクマネジメント①）

※クラウド型ＷＡＦは、中小企業が自ら DNS サーバーの設定変更を行うができない等の理由で、サービス提案を行った 12 社の全てが導入不可となった。

13 IPS（Intrusion Prevention System）：侵入防止システム

14 URL フィルタリング：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こと

②EDR ソフト

【セキュリティ機器】

＜EDR＞パソコン監視分析サービス

【検知及び監視の仕組み】

EDR ソフト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】

EDR ソフト導入 72 社のうち、1 週間以上監視の 67 社の約 50%で不正プログラムが検出された。このうち 1 件については緊急度「高」のアラートを発信し、リモートアクセスでの駆除対応を実施した。また、不正プログラムを配布するサイト等へのアクセスが多く確認された。

図 9 検知及び監視の仕組み（ＳＯＭＰＯリスクマネジメント②）

（５）株式会社ＰＦＵ（石川、富山、福井）

【セキュリティ機器】

＜PC 脅威検知ツール＞「SecureAnywhere Business」（WEBROOT 社）

【検知及び監視の仕組み】

ファイアウォールや UTM 機器等のセキュリティ対策をすり抜けた脅威をツール上で検知、重要度や確度の低い脅威を分析担当が絞り込んだ上で参加企業へ報告する。

【実証結果】

Emotet をはじめ、3 件のマルウェアを検知、分析担当が確度が高く重要性が大きい脅威として参加企業の担当者へ通報した。Emotet の脅威については、導入していたウイルス対策ソフトでは駆除できなかったため、駆け付け対応で最新の駆除ソフト持ち込み駆除した。

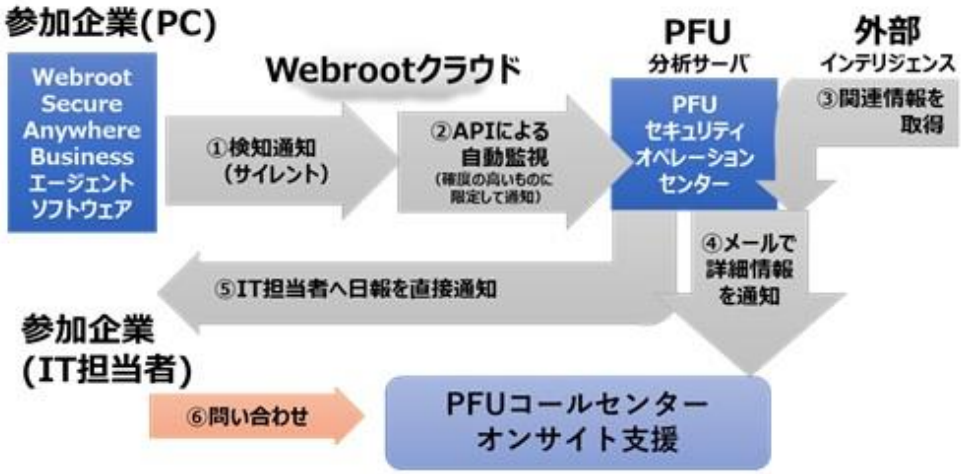


図 10 検知及び監視の仕組み（PFU）

（６）ＭＳ&ＡＤインターリスク総研株式会社（愛知）

①据置型 UTM

【セキュリティ機器】

＜据置型 UTM＞「SonicWall TZ300 TotalSecure」(SonicWall)

【検知及び監視の仕組み】

実証参加企業にて、ルータと HUB（または PC）の間に据置型 UTM 機器を挟み込む形で設置する。据置型 UTM 機器で検知したアラートは、コールセンターでサイバーインシデント等の判断、駆け付け要否判断等を行う。

【実証結果】

ポートスキャン[15]による偵察行為（疑いを含む）が検知したアラート全体の 9 割強（14,478 件）を占めた。また、不正サイトへのアクセスブロック（ボットネット[16]通信）は 89 件だった。

図 11 検知及び監視の仕組み（ＭＳ&ＡＤインターリスク総研①）

②クラウド型 UTM

【セキュリティ機器】

＜クラウド型 UTM＞「MRB-Cloud」（ALSOK）

【検知及び監視の仕組み】

クラウド上の UTM を介してインターネットに接続することでセキュリティ機能を利用できるサービス。自動アラート通知機能の代わりに、週次レポートを電子メールで送信し、利用者の能動的アクションを促す。

【実証結果】

検知された外部から内部への不正通信（130,621 回）のすべてが偵察活動であった。URL フィルタリングでは合計で 2,347,474 件のブロックを検知した。Web 通信以外の外部への危険な通信のブロック（振る舞い検知）は、Android 端末が使用することの多い通信ポート（5228/TCP）も多く検知されており、社内ネットワークの無線環境に許可されていないスマートフォンやタブレットが接続され、通信がブロックされている。

15 ポートスキャン：ネットワークに接続されているサーバーに外部から特定のデータを送信して、それに対応する応答を調べることで、サーバーで動作しているサービスのバージョンや OS などを特定する。

16 ボットネット：サイバー攻撃により乗っ取っとられた多数のコンピュータで構成されるネットワークのことで、乗っ取られたコンピュータは外部から遠隔操作される「操り人形」と化し、サイバー攻撃の踏み台とされてしまう。

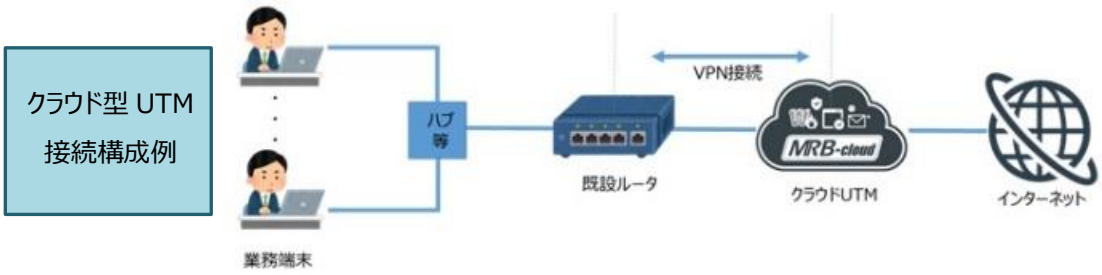


図 12 検知及び監視の仕組み（ＭＳ＆ＡＤインターリスク総研②）

（７）大阪商工会議所（大阪、京都、兵庫）

【セキュリティ機器】

＜UTM＞簡易 UTM 機器（NEC）

※既存 UTM 機器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

【検知及び監視の仕組み】

実証参加企業ネットワークのブロードバンドルータと社内 LAN の間に UTM 機器を接続。接続はボタンを押下するだけで使用可能とし、PC やネットワーク機器の設定変更は不要としている。UTM 機器で検知したログを解析し、端末等がマルウェアに感染している可能性がある場合などは、重要アラートとして実証参加企業へメールで通知する。企業側でアラート対処できない場合は、相談窓口での問合せ対応を行い、、必要に応じて、お助け実働隊（地域 IT 事業者）が駆け付け対応を行う。

【実証結果】

外部からの攻撃は、64 社で検知・遮断した（攻撃の探索活動であるポートスキャンは除く）。1 日あたり 30 件以上の外部攻撃がある 2 社に関しては、現地調査を実施した結果、グローバル IP アドレスが付与され外部からアクセス可能な機器が設置されていた。外部への不正通信を検知した 31 社のうち、企業内の端末がマルウェアに感染し被害が発生していると考えられるアラートを 7 社（7 件）で検知し、対処の結果、3 社にてマルウェアを検出・駆除した。

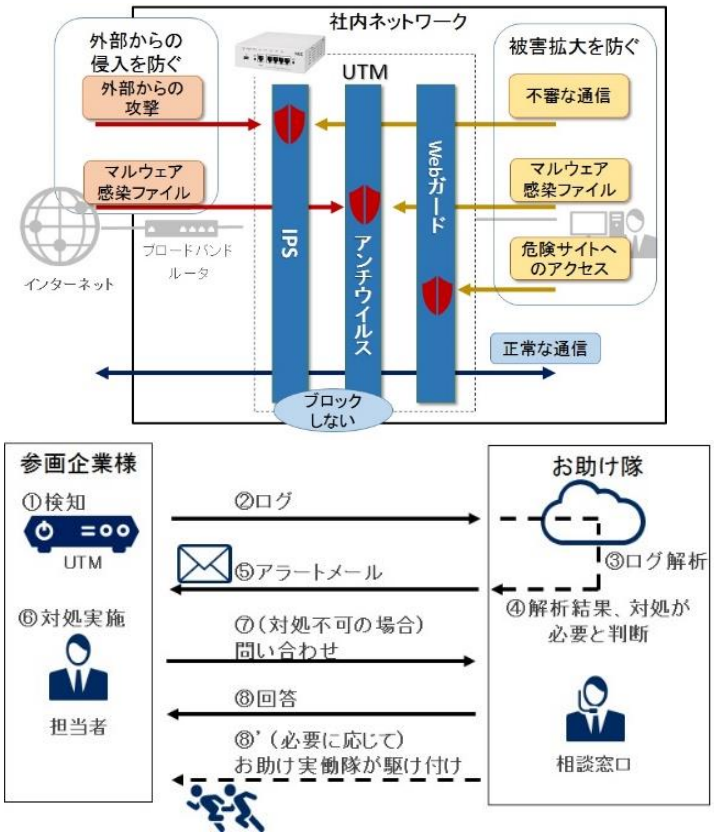


図 13 検知＆監視の仕組み（大阪商工会議所）

（８）株式会社日立製作所（広島、山口）

①UTM 機器

【セキュリティ機器】

＜UTM＞「Sophos XG115」（SOPHOS 社）

【検知及び監視の仕組み】

実証参加企業のネットワーク上に UTM 機器を設置し、インターネット経由でインシデントのリモート監視を実施する。UTM 機器から送信される検知アラート監視について、技術者が検知内容を確認し、検知内容の解説と実証参加企業での対応の必要性等をメールで連絡する。

【実証結果】

インシデント件数は 48,061 件、1 社あたり平均約 67 件/日、駆け付け支援は発生 0 件。

図 14 検知及び監視の仕組み（日立製作所①）

②EDR ソフト

【セキュリティ機器】

＜EDR＞「Cisco AMP for Endpoints」（Cisco 社）

【検知及び監視の仕組み】

監視対象 PC へ EDR ソフトをインストールし、インターネット経由でインシデントのリモート監視を行う。EDR ソフトから送信される検知アラートを技術者が確認し、検知内容の解説と実証参加企業での対応の必要性等をメール等で連絡する。

【実証結果】

インシデント件数は、アドウェア検知が 2 件、駆け付け支援は発生 0 件。

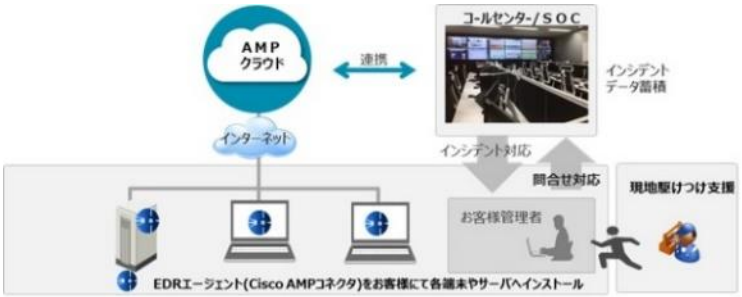


図 15 検知及び監視の仕組み（日立製作所②）

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を各事業主体が構築したセキュリティ機器等による検知及び監視の仕組みにより収集した。

サイバー攻撃の手法は進化しているため、攻撃を検知するアラートも各種存在する。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正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、収集したアラート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
①外部からの不正アクセス検知及び防御（外→内）	外部からの不正アクセス通信を検知・遮断し、バッファーオーバーフロー[17]や SQL インジェクション[18]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
②内部不正プログラム検知及び防御（内⇔外）	ボットネットとの通信など、マルウェア感染等による内部から外部への不正通信や不正プログラムが含まれる通信を検知、感染を早期発見し防御
③不正サイトへのアクセスブロック（内→外）	内部端末から、予め登録したセキュリティ上のリスクがある不正サイトへの接続をブロック（URL フィルタリング）
④マルウェアの検知及び無害化	メール添付ファイルや Web からのダウンロードファイルに含まれるウイルス、ランサムウェア、アドウェア等の検知と無害化
⑤エンドポイントでのアラート検知	パソコン端末にインストールした EDR ソフト等で不正プログラムの検知や不正サイトへのアクセスを検知

表 6 サイバー攻撃に関するアラート種別

17 バッファーオーバーフロー：攻撃対象のコンピュータに許容量以上のデータを送りつけて誤動作を起こさせる攻撃

18 SQL インジェクション：データベースと連動した Web サイトの脆弱性を狙ったサイバー攻撃手法の一つで、データベースに命令する SQL 文を不正操作して、保存されている個人情報などを盗み取る攻撃

（1）UTM 機器等によるアラート検知結果（アラート種別①～④）

アラート種別のうち、UTM 機器等により検知したアラートは以下のとおりであった。

※各事業主体で構築した検知及び監視の仕組みより、アラート検知に関する設定が同一ではないため、特記事項については脚注に記す。

事業主体		UTM 設置数	①外部からの不正アクセス検知及び防御	②内部不正プログラム検知及び防御	③不正サイトへのアクセスブロック	④マルウェアの検知及び無害化
デジタルハーツ（ネットワークセンサー）		81	1,277[19]	804	－[20]	－[21]
東日本電信電話（UTM）		148	965,262	1,015	4,197	1
富士ゼロックス（UTM）		101	93,824	6,757,458[22]	3,213,734	317
SOMPO リスクマネジメント（UTM）		38	511[23]	843	6,755	－[24]
MS&AD インターリスク総研	（据置型 UTM）	27	18,140	255	－[25]	905
	（クラウド型 UTM）	28	130,621	40,018	2,347,474	8
大阪商工会議所（UTM）		112	19,100[26]	692	2,168,065[27]	775
日立製作所（UTM）		10	48,061	0	－[28]	31

表 7 URL 機器等によるアラート検知結果

（2）EDR ソフト等によるアラート検知結果（アラート種別⑤）

アラート種別のうち、EDR ソフト等により検知したアラートは以下のとおりであった。

事業主体	EDR インストール数	⑤エンドポイントでのアラート検知	
		不正プログラムの検知	不正サイトへのアクセス検知
SOMPO リスクマネジメント（EDR ソフト）	72	1,142	4,987
PFU（PC 脅威検知ツール）	97	87	－
日立製作所（EDR ソフト）	13	2	－

表 8 EDR ソフト等によるアラート検知結果

19 デジタルハーツ：既存の FW/UTM を通過したアラートを検知、ポートスキャンは含めない

20 デジタルハーツ：URL フィルタリングの設定無し

21 デジタルハーツ：マルウエア検知の設定無し

22 富士ゼロックス：不正通信の検知には特定アプリ（迷惑ソフト等）による意図せぬ外部通信を含む

23 SOMPO リスクマネジメント：ポートスキャンは既存 FW の機能にてブロックする設定のため検知数に含めない

24 SOMPO リスクマネジメント：今回実証ではマルウエア検知機能は使用していない

25 MS&AD インターリスク総研：今回実証では URL フィルタリング機能は使用していない

26 大阪商工会議所：ポートスキャンは攻撃の探索活動であるため検知数に含めない

27 大阪商工会議所：アダルトサイトと危険なサイトへのアクセス数（検知した通信は UTM では遮断しない）

28 日立製作所：今回実証では URL フィルタリング機能は使用していない

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） 外部からの不正アクセス検知及び防御（外→内）

デジタルハーツ（ネットワークセンサー：Starlight）	
検知数	1,277（内訳：IP/Port Scan 等(1,192)、Brute-Forced 攻撃(2)、SYN Flood 攻撃(83)）
検知内容	ブルートフォース攻撃（総当たり攻撃）を 2 件、DoS 攻撃手法である SYN フラッド攻撃を 83 件検知した。なお、単月 1 社で 6 万件を超えるおびただしいアラートを検知したが、これは実証参加企業の POS レジ不具合による FTP サーバーとのアクセスによるものと判明したため、検知数から除外している。
東日本電信電話（UTM：専用 BOX）	
検知数	965,262（不正侵入検知（IPS））
検知内容	不正侵入検知の 9 割近くが 1 社の検知数だった。当該企業の環境を調査したが、「固定 IP アドレスの利用」、「サーバーの公開」、「リモート接続」等の環境は無く、外部から標的となる原因は見受けられない状況であった。当該企業は食品販売業であるため、販売拡大に向けて、雑誌の Web 広告や twitter など様々広告サイト、ツールを利用していることが攻撃を受ける要因であると推測される。
富士ゼロックス（UTM：beat-box）	
検知数	93,824（内訳：ping(83,910)、port-scan(9,914)）
検知内容	外部から ping または port-scan によるアクセスを受けた回数は合計 93,824 件で、UTM 機器 1 台 1 日あたりに換算すると約 14 件／台となった。ping は 103 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、半数以上の 51%を占めた。他方、port-scan は 63 ヶ国からのアクセス履歴を検知。米国、ルーマニア、中国の 3 ヵ国で、44%を占めた。
SOMPO リスクマネジメント（UTM：Watchguard Firebox M370）	
検知数	511（不審な通信の検知・防御） ※ポートスキャンを含まない
検知内容	不審な通信の検知・防御（IPS）にアラートを 511 件確認した。IPS 検知の上位 3 位は、Microsoft Office の初期化されていないメモリ使用の脆弱性（164 件）、LNK のリモートでコードが実行される脆弱性（109 件）、複数の MicrosoftWindows 製品における任意のコードが実行される脆弱性（67 件）であった。
MS&AD インターリスク総研（据置型 UTM：SonicWall TZ300 TotalSecure）	
検知数	18,140（内訳：DoS 攻撃(601)、IPS アラート(72)、ポートスキャン(17,467)）
検知内容	外部からの不正アクセス検知（防御を含む）は、ポートスキャンによる偵察行為（疑いを含む）が大多数を占めたが、脆弱性を突く侵入攻撃である IPS アラートも 72 件検知した。

MS&AD インターリスク総研（クラウド型 UTM：MRB-Cloud）	
検知数	130,621（内訳：ポートスキャン TCP23（telnet）(80,268)、TCP22（ssh）(17,832)、TCP80（http）(17,345)、ICMP(15,176)）
検知内容	クラウド型 UTM において検知された、外部から内部への不正通信のすべてがポートスキャンによる偵察活動であった。ポート別のスキャン件数は、TCP23 番ポート(telnet)を使用した通信が最も多く、次いで TCP22 番ポート(ssh)、TCP80 番ポート(http)、ICMP の順となっている。
大阪商工会議所（UTM：簡易 UTM 機器）	
検知数	19,100（内訳：IPS(18,325)、アンチウイルス(775)） ※ポートスキャンを含まない
検知内容	外部からの攻撃が 1 日あたり 30 件以上ある 2 社を現地調査を実施した結果、グローバル IP アドレスを付与され、外部からアクセス可能な機器が設置されていた。また、別企業も UTM のログからグローバル IP を使用し、外部から直接アクセス可能な機器があった。グローバル IP を付与して、外部からアクセス可能な機器があると攻撃は多くなる傾向がある。
日立製作所（UTM：Sophos XG115）	
検知数	48,061（ネットワークに関するセキュリティ監視）
検知内容	インターネット出入り口の監視の結果、既知の脆弱性を不正利用する試みが多数検出された。上位 3 位は、Samba の既知の脆弱性を不正利用する試み(45,007)、サーバーlogin の null ポインターの逆参照の脆弱性を不正利用する試み(1,938)、OS-LINUX Red Hat の NetworkManager の提供スクリプトの脆弱性を不正利用する試み(823)であった。

表 9 外部からの不正アクセス検知及び防御の状況

【考察】

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、実証参加の中小企業に対しても数多く行われていることを確認した。「ポートスキャン」により、企業のシステムで利用しているサービスのバージョンや OS などが特定された場合、そのサービスや OS の脆弱性を突いた不正アクセス等に発展するリスクがあるため、最新のセキュリティパッチを適用する等の対策を講じる必要がある。

また、ネットワーク内にグローバル IP アドレスを付与した端末が設置されるなど、外部からアクセス可能な環境がある場合は、多種多様な攻撃を受けるリスクがあるため、外部からのアクセスは必要な通信のみ許可することや、対象ソフトウェアのバージョンアップ等により、外部アクセス環境の脆弱性対応を行う必要がある。

（２） 内部不正プログラム検知及び防御（内⇔外）

デジタルハーツ（ネットワークセンサー：Starlight）	
検知数	804（内訳：Command & Control(119)、DGA(266)、DNS Tunneling 攻撃(419)）
検知内容	DNS のリクエスト・レスポンスを利用して、DNS のフリをした C&C サーバーと通信を行う手法である DNS トンネリング攻撃の疑いのある通信として、複雑な DNS クエリを検出しているアラートを 419 件検知した。このうち、10%を占める 42 個のドメインは、マルウェアなどで疑似乱数を使用した DGA と組み合わせて、ボットネットへの通信として一時的に利用されていたドメインである可能性が高いと思われる。
東日本電信電話（UTM：専用 BOX）	
検知数	1,015（内訳：不正プログラム検知(1,011)、C&C サーバー検知(4)）
検知内容	不正プログラム検知は、Internet Speed Tracker ツールバー（接続速度テストアプリ）をインストールしたことにより、アドウェアである「InternetSpeedTrackerAuto.exe_0」が動作したケースが約 30%を占めた。C＆C サーバーへのアクセス検知は、検知数が少ないものの 4 件検知した。
富士ゼロックス（UTM：beat-box）	
検知数	6,757,458（不正な通信（IPS）検知）
検知内容	検知した不正通信の約 7 割は、Baidu IME の通信であった。Baidu IME は入力中の文字情報を中国の Baidu 社のサーバーに送信し、変換精度を高める機能を利用した際に検出されため、意図せぬ情報送信で機密漏洩のリスクがある。また、WannaCry の C&C サーバーとの通信等、危険性が高い不正通信を 2 件検知、通信をブロックの上、追加調査を行った。
SOMPO リスクマネジメント（UTM：Watchguard Firebox M370）	
検知数	843（ボットネットへのアクセス）
検知内容	不審な URL への接続の検知のうち、ボットへ攻撃の指令を出すサーバーへのアクセスを 843 件検知した。ボット化した端末から指令を受けに行こうとしている可能性があり、ブロックしていなければ、ボットとして勝手にインターネットへの攻撃に加担してしまうリスクがあった。
MS&AD インターリスク総研（据置型 UTM：SonicWall TZ300 TotalSecure）	
検知数	255（内訳：内部不正アクセス検知(166)、不正サイトブロック（IP フィルタリング）（89)）
検知内容	ポートスキャン攻撃の結果として、内部からの不正アクセスを 166 件検知及び防御した。また、ボットネット通信による、不正サイトへのアクセスを IP フィルタリング機能により 89 件ブロックした。

MS&AD インターリスク総研（クラウド型 UTM：MRB-Cloud）	
検知数	40,018（Web 通信以外の外部への危険な通信のブロック（振る舞い検知））
検知内容	Web 通信以外の外部への危険な通信を振る舞い検知でブロックした。UDP53 番ポート（DNS）を使用した通信が最も多く検知されたが、TCP 5228 番ポートを使用した通信も多く検知された。TCP 5228 番ポートは Android 端末が使用することの多い通信であり、社内ネットワークの無線環境に、業務用または私物のスマートフォンやタブレットが接続され、通信がブロックされている可能性が高い。
大阪商工会議所（UTM：簡易 UTM 機器）	
検知数	692（内訳：IPS(683)、アンチウイルス(1)、Web ガード(8)）
検知内容	外部への不正通信で検知遮断したもののうち、40 件でエンドポイントにてウイルススキャンを実施し、6 件のマルウェアを検出した。また、外部へのメールに添付されたファイルで 1 件のマルウェアを検出、対象端末でウイルススキャンを実施したところ、Emotet が検出され駆除した。Web ガードでは、フィッシングサイトや閲覧によりマルウェア感染する有害サイトへのアクセスを検知し通信を遮断した。
日立製作所（UTM：Sophos XG115）	
検知数	0（C&C /ボットネット防止）
検知内容	C＆C/ボットネット防止機能でのアラート検知は 0 件であった。

表 10 内部不正プログラム検知及び防御の状況

【考察】

不正プログラムは、一般的にコンピュータに害を及ぼすプログラムの総称であり、インターネットを介して意図せぬ通信を行うなど、ユーザーにとって不正な動作が発生するおそれがある。不正プログラムによる外部への不正通信は、どんな通信が行われているか検知することで、不正プログラムへの内部感染を早期に発見し、対処する必要がある。

本事業の実証では、マルウェア感染や特定アプリ（迷惑ソフト等）による、意図せぬ外部への不正通信を数多く検知及び遮断した。特に C&C サーバー[29]への不正通信を検知し、対象端末のウイルススキャンを実施したところ、マルウェアやランサムウェアを検出した例が多かった。

また、外部へのメールに添付されたファイルでマルウェアを検出、対象端末でウイルススキャンを実施したところ、Emotet が検出され駆除したケースも報告されている。

[29] 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

（３） 不正サイトへのアクセスブロック（内→外）

東日本電信電話（UTM：専用 BOX）	
検知数	4,197（Web サイトアクセスブロック）
検知内容	不正サイトへのアクセスブロックについても、不正侵入検知（IPS）と同様にほぼ 1 社（食品販売業）が検知数を独占している状況であった。なお、原因については特定できていない状況である。
富士ゼロックス（UTM：beat-box）	
検知数	3,213,734（Web フィルタリング）
検知内容	実証期間中にブロックした Web サイト数は合計で 3,213,734 件で、UTM 機器 1 台 1 日あたりに換算すると約 388 件／台となった。危険性が高いと判断した（ブロック済）コンテンツの内訳は、87%はオンラインストレージ利用であり、次いで 7%が SNS に対するブロックであった。
SOMPO リスクマネジメント（UTM：Watchguard Firebox M370）	
検知数	6,755（不審な URL への接続の検知・防御（除く：ボットネットへのアクセス）
検知内容	インストールすると不要な広告を出す仕組みの迷惑ソフトによる不正サイトへのアクセスや、アクセスすると不正なプログラムが実行されるように改ざんされた可能性のあるサイト等への接続をブロックした。
MS&AD インターリスク総研（クラウド型 UTM：MRB-Cloud）	
検知数	2,347,474（URL フィルタリング）
検知内容	URL フィルタリングによるブロックでは、「シェアウェア／フリーウェア」及び「コンテンツ配信」のブロック件数が非常に多くなっている。Web サイトの中にある広告表示のブロックなども、それぞれを 1 件とカウントしているため、この 2 カテゴリーは、サイト内のコンテンツのブロック数が多くなったものと思われる。
大阪商工会議所（UTM：簡易 UTM 機器）	
検知数	2,168,065（Web サイトアクセス状況のうち、アダルトサイト(2,159,153)、危険なサイト(8,912)）
検知内容	Web サイトアクセス状況のうち、アダルトサイト（ポルノ、アダルトサイト、ギャンブル等）、危険なサイト（フィッシング詐欺、マルウェア、危険アプリケーション等）が 2,168,065 件であった。なお、今回実証では、検知した通信は UTM では遮断をしない設定とした。

表 11 不正サイトへのアクセスブロックの状況

【考察】

不正サイトへのアクセス等により有害なプログラムが仕込まれたウイルスに感染させ、金融機関のログイン情報やクレジットカード情報などを摂取するフィッシング詐欺等の被害が発生している。

本事業の実証でも、不正な Web サイトへのアクセスを数多く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。また、オンラインストレージ、SNS などへのアクセスを多く検知したが、業務上許可されていないアクセスは、内部不正や不注意による情報漏洩のリスクとして懸念される。

（4） マルウェアの検知＆無害化

東日本電信電話（UTM：専用 BOX）	
検知数	1（ランサムウェア）
検知内容	身代金要求型ウイルスであるランサムウェアの侵入を 1 件検出し、防御した。
富士ゼロックス（UTM：beat-box）	
検知数	317（FTP/HTTP ウイルススキャン(45)、ウイルスメール受信(272)）
検知内容	Web 経由でダウンロードされたウイルス検知数は 45 件で、多くは意図しない広告の表示、他ソフトウェアのインストール、ブラウザのハイジャック等が行われる可能性があるグレイウェア（マルウェアと断定はできないプログラム）であった。一方、ウイルス添付メールの受信数は272 件で、特定の企業 1 社に 100 件のウイルスメールが集中しており、調査の結果、当該企業の取引先のメールサーバーがハックキングされ、メールアドレスが漏洩したことにより、マルウェア付きメールが送付されていることが判明した。
MS&AD インターリスク総研（据置型 UTM：SonicWall TZ300 TotalSecure）	
検知数	905（スパイウェア(255)、ウイルス(650)）
検知内容	マルウェアの検知及び無害化は、スパイウェアが 255 件、ウイルスが 650 件であった。
MS&AD インターリスク総研（クラウド型 UTM：MRB-Cloud）	
検知数	8（Web ダウンロードファイル） ※軽微との判断により事業主体が作成した報告書には未記載
検知内容	外部からダウンロードしたファイルを確認し、8 件のマルウェアを検知、無害化を行った。
大阪商工会議所（UTM：簡易 UTM 機器）	
検知数	775（マルウェア）
検知内容	検知及び駆除したマルウェアの 88%は、文書ファイルなどに仕込まれたマクロ感染型ウイルスであった。また、端末内のファイルを暗号化して身代金を要求するランサムウェアを 16 件検知及び駆除した。
日立製作所（UTM：Sophos XG115）	
検知数	31（マルウェア） ※事業者報告書には未記載
検知内容	IPS で検知した 172 件のアラームをサンドボックス機能にて確認し、31 件をマルウェアとして検知、無害化を行った。

表 12 マルウェアの検知＆無害化の状況

【考察】

ランサムウェアは、パソコン内のファイルを暗号化して使用できない状況にし、元に戻すことと引き換えに「身代金」（Ransom）を要求する不正プログラムである。企業が感染すれば、業務に必要な重要なファイルが暗号化されて、事業継続が困難になるような影響

を及ぼしかねない。本事業の実証でも、多くのランサムウェアを検知及び無害化し、被害を未然に防ぐことができた。

また、本業務の実証では、文書ファイルなどに仕込まれたマクロ感染型ウイルスを多数検知及び無害化している。実例としては、実証参加企業の取引先がウイルスに感染し、2か月で 100 件のウイルスメールが送られた事例も報告されている。

（5）エンドポイントでのアラート検知

SOMPO リスクマネジメント（EDR ソフト）	
検知数	6,129（不正プログラムの検知(1,142)、不正サイトへのアクセス検知(4,987)）
検知内容	EDR ソフトを導入した企業の 49%で不正プログラムが検知された。このうち、広告表示により収入を得る目的のアドウェアや使い方によっては悪用されるリスクウェアを 397 件、トロイの木馬型マルウェアを 145 件検知した。このうち 1 件については、緊急度「高」のアラートと判定し、リモートアクセスでの駆除対応を実施した。一方、不正サイトへのアクセスは 4,987 回検知した（内訳：不正サイト 452 回、フィッシングサイト 146 回、悪意のあるサイト 4,095 回、安全と言えないサイト 294 回）。
PFU（PC 脅威検知ツール）	
検知数	87 (不正プログラムの検知)
検知内容	パソコン上の脅威検知ツールにより、検知したマルウェアは 87 件であった。このうち 3 件は、確度が高く重要性が大きい脅威として当該企業に通報を行い、Emotet については当該企業が導入していた既存のウイルス対策ソフトでは駆除できなかったため、駆け付け対応で最新の駆除ソフトを持ち込むことで駆除を行った。
日立製作所（EDR ソフト）	
検知数	2（不正プログラムの検知）
検知内容	エンドポイント監視での検知したアラートは 2 件だが、いずれも悪性(低)のアドウェアと判断され、駆け付け対応にいたるインシデントにはならなかった。

表 13 エンドポイントでのアラート検知の状況

【考察】

EDR は、パソコン端末等にインストールするクライアントソフトと、それを一括管理するサーバー等から構成され、サイバー攻撃の痕跡等から攻撃の兆候等の検知を行い、マルウェアの駆除等の処置を講じる。

本事業の実証では、EDR ソフト等を使用してエンドポイントでのアラート検知を行ったところ、相当数の不正プログラムや不正サイトへのアクセスを検知し、マルウェアの駆除等を行った。

3.2.4. 相談・インシデント等対応状況

本事業の実証では、各事業主体毎に実証に関する相談受付及び対応体制（コールセンター）構築した。また、検知したアラートは、各事業主体があらかじめ定義した判定基準等[30]により、サイバーインシデントであるかの判断の上、電話及びリモートによるインシデント対応を行い、必要に応じて訪問によるインシデント対応（駆け付け対応）を行った。

実証の結果、全国 8 地域合計で 128 件のインシデントが発生し、そのうち駆け付け対応が 18 件発生した。

以下にコールセンター対応及びインシデント等対応の状況を示す。

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	741 件	実証参加に関する問合せ	64 件
		セキュリティ機器設置等の問合せ	432 件
		セキュリティ対応の相談	113 件
		その他	132 件
インシデント等対応	**128 件**	**電話及びリモートによるインシデント対応 ※**	**110 件**
		訪問によるインシデント対応（駆け付け対応）	**18 件**
その他訪問対応	68 件	機器設置等のトラブル対応	19 件
		その他（セキュリティ機器の導入･設置支援等）	49 件

※電話及びリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む

表 14 コールセンター対応及びインシデント対応等の状況

30 大阪商工会議所の取組み例：検知内容に重要度を定義し、実証参加企業が対処の必要性が一目でわかり、駆け付け発動判断ができるように判定基準を設定

3.2.5. 駆け付け対応事例

本事業の実証の結果、訪問によるインシデント対応（駆け付け対応）を行った 18 事例の発生事象と対処状況を以下に示す。

No.	01	発生日	2019 年 11 月 19 日		
地域	岩手県	業種	製造業	従業員数	6～20 名
概要	Emotet 感染による偽装メールの受信				
発生事象	事業主体が同社を装ったメールを受信したことから、発信元である同社がマルウェアに感染している疑いがあり、企業社内外への情報漏えい等のおそれがあるため、駆け付け対応を実施した。				
対処状況	電話対応で対象端末の隔離、対象端末以外の端末の初期化を指示し、企業側にて実施。訪問対応で対象端末のログ分析等を実施した結果、Emotet 感染により、悪性 PowerShell コマンドが実行されていることを確認。抜き取られたアドレス情報から不正メール送信に悪用されている可能性があると推測。PowerShell を禁止設定にする対策などの対応方法を指示した。				

No.	02	発生日	2019 年 12 月 12 日		
地域	宮城県	業種	学術研究，専門・技術サービス業	従業員数	6～20 名
概要	悪質サイトへ誘導すると思われる広告のブロック対応				
発生事象	実証参加企業から、「誤って偽通知をクリックしたら、怪しい広告通知がデスクトップ上に表示される様になった」との相談が、コールセンターに入った。概要から判断して、社内の PC がマルウェアに感染した恐れがあるため、駆け付け対応を実施した。				
対処状況	訪問対応の結果、悪質サイトへ誘導する広告表示の通知を誤って許可してしまったことにより、意図しないポップアップ広告が表示されるようになったことを確認。ブラウザ広告に記載のアクセス先ドメインに対してブラウザのブロック設定を行い、再起動後、再度広告が出ないことを確認した。また、不審なプログラム、不審なブラウザ拡張機能などが、混入していないことの確認を行った。				

No.	03	発生日	2020 年 1 月 14 日		
地域	埼玉県	業種	卸売業，小売業	従業員数	6～20 名
概要	ランサムウェアへの感染の疑いがある通信の検知				
発生事象	ランサムウェア WannaCry の C&C サーバーとの通信を検知、ブロックしている状況が判明。社内 PC が感染している可能性が高く、追加調査が必要と判断し、駆け付け対応を実施した。				
対処状況	対象企業でウイルススキャンを行うが送信元端末は特定できなかった。訪問調査でネットワーク構成を確認し、不正通信の IP が無線ルーターであることを特定。ヒアリングにより、社長の家族が個別に持ち込んだ無線ルーターであることが判明、当該無線ルーターに接続した全端末のウイルススキャン実施を指示。セキュリティ上のリスクがあるので、今後は私物のルーターや端末等を社内ネットワークに繋がないよう指導した。				

No.	04	発生日	2020 年 2 月 4 日		
地域	群馬県	業種	サービス業（他に分類されないもの）	従業員数	21～50 名
概要	マルウェアへの感染の疑いがあるサイバー攻撃の通信を検知				
発生事象	社内から社外 Web サーバーや FTP サーバーの脆弱性を突くサイバー攻撃の通信を検知、ブロックしている状況が判明。社内 PC がマルウェアに感染し、意図せず他社サーバーを攻撃させられていて、サイバー攻撃の踏み台になっている可能性が高いため、追加調査が必要と判断し、駆け付け対応を実施した。				
対処状況	不正通信の発信源の当該端末として、業務用 PC1 台を発信元 IP から特定した。当該端末は 1 月度にもランサムウェアである WannaCry の C&C サーバーとの通信も検知・ブロックしていることが判明し、ウイルススキャンを実施したが、マルウェア等の検知はされず、当該 PC の初期化、OS の再インストールを実施するよう指示した。なお、当該 PC の利用ユーザーにヒアリングしたところ、以前、偽ウイルス対策ソフトを誤ってインストールしたことがあるとのことであった。PC 初期化後に不正通信は発生していない。				

No.	05	発生日	2020 年 2 月 4 日		
地域	群馬県	業種	サービス業（他に分類されないもの）	従業員数	21～50 名
概要	標的型攻撃によるウイルスメール受信の増加を検知				
発生事象	10～12 月度で特定企業 1 社にウイルスメール 100 件が集中し、継続的にブロックしている状況が判明。検知数が多いため追加調査が必要と判断し、駆け付け対応を実施した。				
対処状況	該当企業の取引先会社のメールサーバーが不正アクセスを受けてメールアドレスが漏えいし、それが使用されて、賞与支払い、請求書支払い等を装うなりすましメールで標的型攻撃を受けていたことが判明した。標的型攻撃の対象になっていることを通知し、ウイルスメールは UTM 機器でブロックしている状況ではあるが、被害拡大がないように社員へ注意喚起した。				

No.	06	発生日	2019 年 12 月 20 日		
地域	神奈川県	業種	サービス業（他に分類されないもの）	従業員数	51～100 名
概要	不正な IP アドレスへの通信の検知				
発生事象	過去に複数のマルウェアの通信先として使われた IP アドレス宛ての通信を検知。該当企業に確認したところ、ウイルス対策ソフト未導入の WindowsXP パソコンにて通信をしたことが判明し、マルウェア駆除のため駆け付け対応を実施した。				
対処状況	当該端末は、Windows XP でしか動作しないソフトウェア利用のためのもので、インターネットに常時接続していない認識であったことから、ウイルス対策ソフトが導入されていなかった。今回、社内プリンタ使用のために社内 LAN に接続したことで、意図せずインターネットに接続されていたことが判明した。当該端末に対しウイルススキャンを実施、ワームやトロイの木馬、迷惑ソフト等計 25 ファイルの不正プログラムを発見したため駆除を実施した。				

No.	07	発生日	2019 年 12 月 12 日		
地域	石川県	業種	製造業	従業員数	101～200 名
概要	マルウェア「Emotet」感染を検知				
発生事象	パソコン上の脅威検知ツールが Emotet を検知、事業主体の SOC で対象企業に連絡、該当端末をネットワークから抜線した。対象企業で導入していたウイルス対策ソフトでは駆除ができなかったため、駆け付け対応で最新の駆除ソフトを持ち込み駆除した。				
対処状況	該当端末は初動対応でネットワークから切り離していて、事業者の SOC からリモート対応でウイルス駆除ができなかったため、訪問対応により USB 型のウイルス対策ソフトで駆除を行った。調査依頼により、ネットワークから抜線されていない他の PC をリモート対応で検査したが、問題は発見されなかった。				

No.	08	発生日	2019 年 9 月 4 日		
地域	愛知県	業種	製造業	従業員数	21～50 名
概要	特定端末からのボットネットとの不正通信を検知				
発生事象	特定の端末からボットネットとの不正通信を検知。お助け隊コールセンターより連絡するも、対象企業側で当該端末の特定をできず。端末の特定を目的に駆け付け対応を実施した。				
対処状況	訪問対応時点で、対象企業側で端末は特定できていたが、自動で社内ネットワークの接続端末一覧を作成する機器（SECURIE）を設置し、社内に存在する機器の見える化を行った。不正通信は、社内の無線 LAN に接続された社員の私物スマートフォンが発信元であったため、フォレンジックツールによる情報取得は行わなかった。				

No.	09	発生日	2019 年 10 月 31 日		
地域	愛知県	業種	サービス業（他に分類されないもの）	従業員数	1～5 名
概要	業務に使用する PC への詐欺ソフトのインストール				
発生事象	従業員が自宅で業務に使用している PC に詐欺ソフトをインストールしてしまい、キャッシュカード情報などの入力画面が消えなくなった、との問合せがお助け隊コールセンターに入電、当該企業の要請により駆け付け対応を実施した。				
対処状況	フォレンジックツールにより必要情報を取得、情報を解析した結果、詐欺ソフト「Onesafe PC Cleaner」が 9 月 20 日にインストールされていることが判明。詐欺ソフトの概要、インストールされた経緯、アンインストール方法等をレポートにまとめて提出し、当該企業で詐欺ソフトのアンインストールを実施した。				

No.	10	発生日	2019 年 11 月 25 日		
地域	愛知県	業種	金融業，保険業	従業員数	21～50 名
概要	ステルス・スキャン[31]攻撃の疑いのある通信を連日検知				
発生事象	社内 5 台の端末から、ステルス・スキャン攻撃手法の 1 つである TCP Xmas スキャンのアラートを連日検知した。当該端末がマルウェアに感染し、マルウェアが指令サーバーに接続して命令を受け取り、通信を発生している可能性があるため、お助け隊コールセンターより対象企業に連絡するも、当該端末を特定できず。端末の特定及び当該端末からの情報取得を目的に駆け付け対応を実施した。				
対処状況	訪問調査でパケットキャプチャを実施、通信の発信元は PC2 台、プリンタ 2 台、不明 1 台と判明。PC2 台からフォレンジックツールによる情報取得を実施した。取得した情報を解析、アラートを発生させた通信の接続先 IP アドレス約 40 件を評価したが、不正な通信の発信元となる不正なプログラム等の問題は見つからなかった。対象企業に、既知の悪意のあるサイトへの接続が無い旨の調査結果レポートを提出した。				

No.	11	発生日	2019 年 8 月 29 日		
地域	大阪府	業種	製造業	従業員数	21～50 名
概要	リモートアクセス型トロイの木馬[32]への感染の疑いのある通信を検知				
発生事象	マルウェア（リモートアクセス型トロイの木馬（RAT））に感染の疑いのある通信を検知し、同マルウェアによる情報の窃取、改ざん、破壊、端末の遠隔操作・停止などが発生する可能性があることから、駆け付け対応を実施した。				
対処状況	不正通信の疑いのある送信元 PC と通信先 PC に対して、当該企業で導入しているウイルス対策ソフトとは別の対策ソフトを使用し、ウイルススキャンを実施したが、ウイルスは検出されなかった。過検知と判定。				

No.	12	発生日	2019 年 9 月 13 日		
地域	大阪府	業種	製造業	従業員数	21～50 名
概要	ファイアウォールの脆弱性に対する攻撃の疑いがある通信を検知				
発生事象	ファイアウォール製品の脆弱性の悪用により、情報漏洩、端末の遠隔操作・停止、マルウェアへの感染などが発生する可能性があることから駆け付け対応を実施した。				
対処状況	確認の結果、該当するファイアウォール製品は発見できなかった。アラート対象の通信元 PC と通信先 PC に対してウイルススキャンを実施したが、ウイルスは検出されなかった。過検知と判定。				

31 ステルススキャン：サイバー攻撃を行う対象となるコンピュータの状態を調べるポートスキャンの手法の一つで、相手に記録（ログ）を取られずに調査を行う手法のこと

32 リモートアクセス型トロイの木馬（Remote Access Trojan, RAT）： 無害なプログラムを装ってコンピュータ内に侵入するマルウェアであるトロイの木馬のうち、侵入したコンピュータをリモートアクセスを可能な状態にする機能を持つもの

No.	13	発生日	2019 年 9 月 27 日		
地域	大阪府	業種	製造業	従業員数	51～100 名
概要	特定端末からの毎回規則性のある BASIC 認証（基本認証）[33]通信を検知				
発生事象	admin などの類推されやすいパスワードを使用した BASIC 認証を試みる通信が、特定端末から毎週定期的に規則性のあるアクセスを繰り返す事象を検知したことから、不正プログラムの感染が疑われ、状況調査のため駆け付け対応を実施した。				
対処状況	BASIC 認証通信の送信元 PC の不明なプログラムのインストール状況確認、ウイルススキャンを実施したが、不正プログラム及びウイルスは検出されなかった。過検知と判定。（送信先機器のパスワードを複雑性を持たせた強度の強いパスワードへ変更）				

No.	14	発生日	2019 年 11 月 5 日		
地域	大阪府	業種	学術研究，専門・技術サービス業	従業員数	6～20 名
概要	オンライン銀行詐欺ツール型マルウェアへの感染の疑いがある通信を検知				
発生事象	オンライン銀行詐欺ツール型マルウェア(UPATRE/DYRE）への感染の疑いがある通信を検知し。当該マルウェアに感染したシステムでは、攻撃者が外部からインターネットバンキングの利用情報を狙うマルウェアなど複数のマルウェアをダウンロードすることが可能となるため、駆け付け対応を実施した。				
対処状況	検知した IP アドレスはルーターであったため、ルーター配下にある全 PC でウイルススキャンを実施した結果、2 台の PC でウイルスを検出し駆除した。				

No.	15	発生日	2019 年 11 月 15 日		
地域	大阪府	業種	製造業	従業員数	21～50 名
概要	ボットネットマルウェアの感染の疑いがある外部への通信を検知				
発生事象	インスタントメッセンジャーなどを介して個人情報などを搾取するボットネットマルウェア（Dorkbot)の感染の疑いがある外部への通信を検知したため、駆け付け対応を実施した。				
対処状況	１回目の訪問対応では、検知した端末の MAC アドレスと合致する PC は発見できなかった。対象企業から、親族が経営する別会社の端末が自社ネットワークつながっていることが分かったとの連絡があり、２回目の訪問対応で送信元 PC を特定した。調査の結果、不要なフリーソフトが外部への通信を発信していることが判明したため、アンインストールを実施した。また、当該 PC に対し、ウイルススキャンを実施したところ、474 件のウイルスを検出し駆除した。				

[33] BASIC 認証（基本認証）通信：強度の弱いパスワードを使用し、相手先のルーター等へのログインを試みる通信

No.	16	発生日	2019 年 12 月 17 日		
地域	大阪府	業種	建設業	従業員数	21～50 名
概要	送信メールの添付ファイルからウイルス（Emotet）を検知				
発生事象	送信メールに添付されたファイルにウイルスが含まれていることを検知、送信元端末がマルウェアに感染しているおそれがあるため、駆け付け対応を実施した。				
対処状況	訪問対応により、当該端末のウイルススキャンを実施し、Emotet を検知し駆除、感染ファイルを含むメールを削除した。他に有害な侵入物がないか検査し、問題ないことを確認した。ヒアリングの結果、メール添付の Word ファイルを開いてしまったことが原因らしいとのことであった。				

No.	17	発生日	2019 年 12 月 27 日		
地域	大阪府	業種	建設業	従業員数	21～50 名
概要	リモートアクセス型トロイの木馬への感染の疑いがある通信を検知				
発生事象	マルウェア（リモートアクセス型トロイの木馬（RAT））に感染の疑いのある通信を検知し、同マルウェアによる情報の窃取、改ざん、破壊、端末の遠隔操作・停止などが発生する可能性があることから、駆け付け対応を実施した。				
対処状況	対象企業でウイルススキャンを実施し検出無しとのことだったが、フルスキャンでは無く、2016 年のパターンファイルによる検査であった。最新パターンファイルでのフルスキャンの実施しようとしたが、対象企業から「パターンファイルをアップデートすると、業務システムが動かなくなるおそれがあるのでしたくない」との意向があり、実施を断念した。業務システムへの影響が無いことを確認の上、当該端末がインターネットに接続できないように DNS 設定を無効化して対処した。				

No.	18	発生日	2020 年 1 月 23 日		
地域	大阪府	業種	製造業	従業員数	21～50 名
概要	リモートアクセス型トロイの木馬への感染の疑いがある通信を検知				
発生事象	マルウェア（リモートアクセス型トロイの木馬（RAT））に感染の疑いのある通信を検知し、同マルウェアによる情報の窃取、改ざん、破壊、端末の遠隔操作・停止などが発生する可能性があることから、駆け付け対応を実施。				
対処状況	対象企業で送信元 PC のウイルススキャンを実施したが、マルウェア等の検出は無かった。送信元 PC のイベントログから、アラート発生時の起動アプリケーションから、送信先 IP を確認したところ、大手広告会社の関連会社のものと思われる IP であった。過検知と判定。				

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、事業主体ごとに実証参加企業等へのアンケートによる状況調査、脆弱性診断等による調査を行い、セキュリティ対策状況等を把握した。併せて、実証参加企業のセキュリティに関する意識の向上を図るためセキュリティ訓練等を実施した。

※本項では事業主体の略称を以下のように記す。

【事業主体の略称】
①株式会社デジタルハーツ（略称：DH）
②東日本電信電話株式会社（略称：NTT 東）
③富士ゼロックス株式会社（略称：FX）
④SOMPO リスクマネジメント株式会社（略称：SOMPO）
⑤株式会社 PFU（略称：PFU）
⑥MS&AD インターリスク総研株式会社（略称：MS&AD）
⑦大阪商工会議所（略称：大商）
⑧株式会社日立製作所（略称：日立）

3.3.1. アンケートによる状況調査

本事業では、各事業主体が実証開始の前後や事業説明会の開催時に、実証参加企業等へのアンケート調査を行い、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のセキュリティ対策状況等の確認結果を示す。

＜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）

- 導入しているセキュリティ対策は、ウイルス対策ソフト 90%、出入り口対策 20%弱、社員教育 20%弱、サイバーリスク保険加入は 3%である。（NTT 東）
- パスワード設定や ID 管理等の「アクセス制御管理」についての達成度は高い。（SOMPO）
- 組織的及び技術的安全管理措置については、一定の対応ができている。（SOMPO）
- 「リスク管理」、「通信ネットワーク管理」、「インシデント対応」及び「教育訓練・改善」については達成度が低い。（SOMPO）
- サイバーセキュリティ対策の状況として、「（外部に）セキュリティ相談窓口がある」が 57%、「マルウェアの侵入などを検知する仕組みがある」が 65%で、取引 IT ベンダーとの関係やアンチウイルスソフト導入がある程度進んでいる。（PFU）
- UTM 導入率 27%（実証参加企業以外も含む）、実質的にはファイアウォール的な運用しかしていない企業や「入れっぱなし」の企業も散見。（大商）
- 情報システム担当者を配置：41%（専任 9%、兼任 32%）（大商）
- アンチ ウイルスソフトの導入率は 87%である。（大商）
- パターンマッチ型アンチウイルスソフトの導入率は 80%前後と高いが、パターンに依存しないアンチウイルスなどの新しいウイルスの検知防御に対応できていない。（日立）

表 15 自社で実施しているセキュリティ対策

【考察】

ウイルス対策ソフトは 80～90%の中小企業で導入が進んでいるが、UTM 機器等は 20～30%しか導入が進んでいない。また、情報システムの専任者を置く中小企業は少なく、「リスク管理」「通信ネットワーク管理」「インシデント対応」「教育訓練・改善」に関するアンケート項目についての達成度が低い。

また、サイバー保険加入が 3%との結果もあり、サイバー保険の普及が進んでいない。

＜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）

- サイバーセキュリティ対策経費は年間 50 万円未満が 7 割。（DH）
- お助け隊サービス有料化の妥当月額は 5000 円未満が 7 割。（DH）
- 今後のセキュリティ対策費用見込みは月額 5,000～10,000 円が約 4 割と最多。（NTT 東）
- セキュリティ対策にかけることができる月額費用は平均 5.8 万円（年間 70 万円）。従業員 1 人あたり月額 988 円。（PFU）
- セキュリティ機器にかける費用は月額 1 万円未満が最も多い（4 割弱）ものの、月額 1 万～3 万円の層も 3 割弱存在する。（MS&AD）
- セキュリティ製品導入の決め手は、「自社のネットワークにマッチするかどうか」「性能・精度」と回答した企業が 5 割近くおり、必ずしも低価格であるとは言えない。（MS&AD）
- サイバーセキュリティに係る年間経費は、実証参加企業では 3 分の 1 以上が年 1 万円未満、年 11 万円以上は 20%にすぎない。（大商）

表 16 情報セキュリティ対策にかける費用

【考察】

情報セキュリティ対策にかける費用は、年間 6 万円（月額 5 千円）から年間 70 万円（月額 5.8 万円）まで幅がある回答となったが、総じてかけられる費用は高いとは言えない。ただし、一部ではセキュリティ製品導入の決め手は、「必ずしも低価格であるとは言えない」との回答もあった。

＜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）

- 自社のセキュリティについて専門家を交えて検討したい企業が半数以上。（DH）
- ビジネスメール詐欺は約 3 割の企業が被害、中小企業も標的になっている。（NTT 東）
- インシデント発生時の相談先については、相談先がないと回答した企業が全体の 4 割弱、自社のみで対応することは困難。（NTT 東）
- 自社内で発生したサイバー攻撃を 31%の組織が認識。認識しているサイバー攻撃 TOP3：ランサムウェア 8 件、Web サーバーの侵害(改ざん)7 件、なりすましメール 5 件。（PFU）
- 7 割以上の企業がサイバーセキュリティ体制の構築をしていない状況。（MS&AD）

・整備されている文書・規程としてポリシーが最も多かった（28.0%）が、何も整備していない企業は過半数存在。（MS&AD）
・事後対応のニーズについて、「電話や遠隔 PC 操作による相談」「IT 事業者等の駆け付けによる相談」など、実効性ある初動対処へのニーズが高い。（大商）
・情報の流出を防止する（出口対策）の実装率が低いため、マルウェア感染後の情報流出のリスクは高い。（日立）
・セキュリティ対策を実施していない主な理由として、検討をしていない、もしくは対策自体を知らないとの回答が最も多い。（日立）
・入口対策としてインターネット（Web サイト）へのアクセス時にユーザー認証などのアクセス制限が適用されていないケースがあった。（日立）
・出口対策では、ファイルサーバーのアクセス権が未設定、かつ、重要な情報に対するファイル単位の暗号化などのセキュリティ制限についても未実施。（日立）

表 17 情報セキュリティ対策を進める上での課題

【考察】

約 3 割の中小企業が自社内のサイバー攻撃を認識している中、約 7 割の中小企業がサイバーセキュリティ体制の構築をしていないことが確認された。マルウェア感染後の情報流出を防ぐ出口対策の実施がされていない中小企業が多く、セキュリティに関する文書・規程が整備していない企業も過半数存在したとの結果もあった。

一方で、「インシデント発生時に自社のみで対応することは困難だが相談先がない」、「自社のセキュリティについて専門家を交えて検討したい」との回答があり、専門家への相談ニーズがある。

＜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）

・関係先、取引先とのセキュリティ対策を確認したが、関心事にはならず、意見交換すら行っていない実態が分かった。しかし、一部企業では、取引先から問合せやガイドラインが提示されている。（FX）
・取引企業からセキュリティ対策が要件に含まれている企業 42%。製造業(その他)、医療・福祉、金融業・保険業が多い傾向。（PFU）
・「取引先からサイバー攻撃対策を求める意思表示の有無」は「その動向はない」が概ね過半数である一方で、「取引先の要件化とされつつある」も 33%あり、サプライチェーンの中での取組みが一部では行われている。（日立）

表 18 セキュリティ対策について取引先からの要求の有無

【考察】

サプライチェーン上流企業から中小企業に対するセキュリティ対策の要求は、過半数が「その動向はない」と回答しているものの、30%～40%で取引企業からセキュリティ対策が要件に含まれているとの回答がある。一部の企業では取引先から問合せやガイドラインが提示されており、製造業、医療・福祉、金融業・保険業からの要請が多い との報告もあった。

3.3.2. 脆弱性診断等による調査

本事業では、事業主体の取組み内容により、実証参加企業の公開 WEB サイトへの脆弱性診断等を行い、セキュリティ対策状況等を把握した。

以下に脆弱性診断等によるセキュリティ対策状況等の確認結果を示す。

◇WEB アプリ簡易診断
・問合せフォームを設置している WEB サイトもある中で、「暗号通信に関する脆弱性」に対する対応が不十分であるケースが多かった。（SOMPO）
・WEB サイト開設後のセキュリティ対応が十分でなく、診断対象である WEB サイトの全てにおいて、クロスサイトスクリプティングやクリックジャッキングを防ぐための対策が講じられていないことが判明した。（SOMPO）
◇公開サイト脆弱性診断
・意識が向上した：12 件、意識は向上しなかった：8 件（PFU）

表 19 脆弱性診断等によるセキュリティ対策状況等の確認結果

【考察】

問合せフォームを設置している WEB サイトもある中で、WEB サイトの脆弱性に対するセキュリティ対応が十分でなく、クロスサイトスクリプティング[34]やクリックジャッキング[35]等のサイバー攻撃を仕掛けられるおそれがあることが確認された。

3.3.3. セキュリティ訓練等

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、標的型メール訓練及びサイバーセキュリティ演習を実施した。

以下にセキュリティ訓練等の実施結果を示す。

◇標的型攻撃メール訓練（NTT 東）
・147 社 198 名に対して、標的型攻撃メール訓練を実証前後の計 2 回実施。
・1 回目開封率約 20%、2 回目約 14%まで減少、実際に疑似メールの受信を抜き打ちで体験することで巧妙なメールの手口を知り、攻撃への警戒心・注意の意識が高まった。
・定期的かつ継続的な訓練で、組織全体での意識向上やモチベーション維持が必要。
◇サイバーセキュリティ演習（MS&AD）
【午前】講習(座学式)、【午後】演習(設問回答式) （3 回開催／参加 63 社）
＜演習シナリオ＞ 以下の 3 問のシナリオについて実施
攻撃シナリオ①：標的型攻撃の発覚・初動・復旧・対策等について（設問数 11／正答率 80%）
攻撃シナリオ②：ランサムウェアの発覚・初動・復旧・対策等について（設問数 7／正答率 87%）
攻撃シナリオ③：内部不正の発覚・初動・復旧・対策等について（設問数 5／正答率 77%）

表 20 セキュリティ訓練等の実施結果

34 クロスサイトスクリプティング：SNS や EC サイトなどの動的な WEB ページの脆弱性を悪用して、不正なスクリプトを挿入して実行させるサイバー攻撃手法

35 クリックジャッキング：WEB ページのボタンやリンクの上に透明な不正ページを重ねて表示させ、これを利用者がクリックすると意図しない動作をさせるサイバー攻撃手法

【考察】

実体験に近いセキュリティ訓練や演習を実施することで担当者の意識の向上に資することが確認できた。また、組織全体での意識向上やモチベーション維持の観点から継続的に実施することの重要性が確認できた。

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）」[36]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。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」及び「中小企業の情報セキュリティ対策ガイドライン」[37]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 SA 宣言数

本事業の実証参加企業 1,064 社のうち、「SECURITY ACTION」一つ星を宣言した企業は 149 社（14.0%）、二つ星を宣言した企業は 43 社（4.0%）、計 192 社（18.0%）であった。[38]

（2）SA の認知度

各事業主体において、本事業の事業説明会及び報告会を中心に「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うかがえた。

一方で、サイバーセキュリティの必要性と重要性を認識しても「何から取り組めばいいかわからない」という中小企業の声が多いことから、各事業主体からは、SA 制度をもっと活用することで「基本的対策から取り組むことができ、取引先など対外的な PR に資する」との意見が複数あった。

---

36 https://www.ipa.go.jp/security/security-action/

37 https://www.ipa.go.jp/security/keihatsu/sme/guideline/

38 対象である SECURITY ACTION 宣言事業者は、中小企業者が大部分を占めるが、一部企業以外の法人、個人事業主等の小規模事業者が含まれる。

3.3.5. 実証参加企業への訪問ヒアリング

本事業の実証参加企業のうち、13 社から協力をいただき、訪問ヒアリングにより、実証参加企業が実施した実証内容、制度・施策に対する意見、これまでの取組みと今後についてまとめた事例集を作成した。

以下に、訪問ヒアリング先企業一覧を示す。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	事例コメント
A 社	宮城県	情報通信業	約 80 名	約 7,000 万円	システム管理室を立上げ、情報セキュリティ対策を組織全体で推進
B 社	宮城県	情報通信業	約 20 名	約 1,000 万円	監視装置の導入によりネットワーク監視を常時実施できることに安心感
C 社	新潟県	電気通信工事業	約 20 名	約 1,600 万円	実証参加を機に情報セキュリティ対策を組織全体で進めていける体制を検討
D 社	新潟県	保険代理業	約 20 名	約 500 万円	体制構築、ツールの導入など、必要な費用をかけて対策実施を検討
E 社	埼玉県	製造業	約 130 名	約 1,700 万円	情報セキュリティはお客様の信頼を得る差別化要素と考え、取組みを強化
F 社	神奈川県	サービス業	約 100 名	約 1,000 万円	実証事業でインシデントを検知し従業員のセキュリティに関する知識不足を再認識
G 社	石川県	製造業	約 80 名	約 5,600 万円	組織全体の脆弱性や脅威を監視するサービスの有効性を実感
H 社	石川県	製造業	約 170 名	約 6,500 万円	取引先からの要求が高まるなか、業界平均を踏まえたセキュリティ対策を推進
I 社	愛知県	製造業	約 50 名	約 3,000 万円	実証参加を通じて監視装置の有効性を認識
J 社	愛知県	サービス業	約 20 名	約 1,000 万円	監視装置の導入により不審な通信の検知の重要性を認識
K 社	大阪府	製造業	約 90 名	約 3,000 万円	本事業と並行して情報セキュリティポリシーの策定も実施
L 社	大阪府	製造業	約 40 名	約 3,500 万円	実証参加を通じて社内ネットワークの可視化を実現
M 社	広島県	サービス業	約 370 名	約 2,000 万円	監視装置の導入により正常な運用を確認でき安心感

表 21 訪問ヒアリング先企業一覧

【取組み事例の構成】

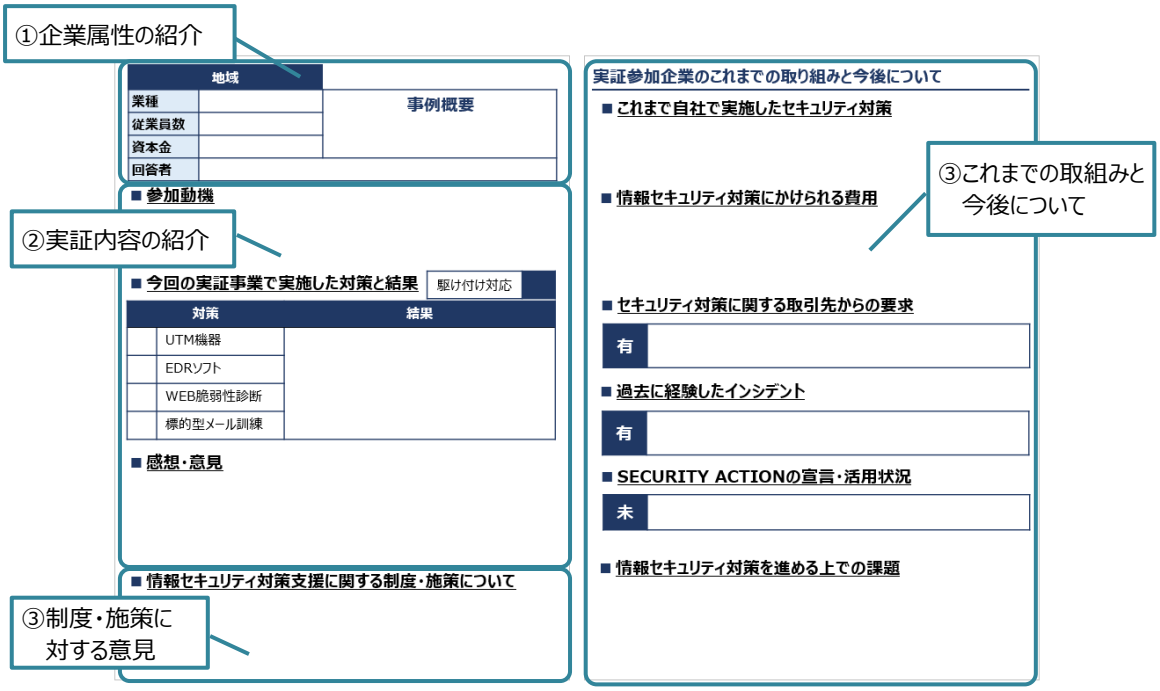


図 16 「サイバーセキュリティお助け隊 実証参加企業事例集」構成

①企業属性の紹介

実証参加企業が所在する「都道府県」、「業種」、「従業員数」、「資本金」、ヒアリングに対応した「回答者」の立場に加え、事例概要を記載している。

②実証内容の紹介

本事業への「参加動機」、「今回の実証事業で実施した対策と結果」及び、「感想・意見」について記載している。

③制度・施策に対する意見

本事業に限らず、中小企業の情報セキュリティ対策支援に関する制度・施策についての意見を記載している。

④これまでの取組みと今後について

実証参加企業が「これまで自社で実施したセキュリティ対策」、「情報セキュリティ対策にかけられる費用」、「セキュリティ対策に関する取引先からの要求」の有無、「過去に経験したインシデント」の有無、「SECURITY ACTION の宣言・活用状況」及び、今後「情報セキュリティ対策を進める上での課題」を記載している。

4. 実証結果を踏まえた検討の実施

4.1. 中小企業に必要な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状況を示す。

事業主体	実証結果	セキュリティ対策のサービス検討
①株式会社デジタルハーツ	・専任の IT 管理者が不在で、ネットワーク構成が把握できていない中小企業が多い。 ・具体的にどのような対策を講じるべきかわからないため、予算化するかの議論に至っていない。 ・サービス提供者側のスキルとして、インシデント発生時には高い知識が要求されるものの、現状把握、月次報告作成等の大半を占める業務は基本的知識で対応可能。	・ネットワーク構成の書面化、UTM 導入等を検討段階から伴走型でサポートするサービスを提供。 ・セキュリティ対策強化による、取引先への信頼性向上や事業継続に係るリスク軽減等のメリットを可視化する。 ・Web サイトによる情報発信やセキュリティに関する説明会等を継続し、企業及び地域の信頼を得る。 ・特定エリアに集約された複数企業に対して一括してサービスを提供することにより、効率化、低価格化を図ることができる。
②東日本電信電話株式会社	・中小企業の大半が、ウイルス対策ソフト（エンドポイント対策）は導入しているが、UTM の導入はしていない。 ・システム管理者や IT の専任担当者は少なく、社長や他の業務に従事している社員が兼務しているケースが多い。 ・ネットワーク及びシステム環境の構築にコスト面や利便性を優先するケースが多く、情報漏洩等により発生する多大な被害についての意識が薄いため、セキュリティを考慮した環境の構築や運用ができていない。	・「多層防御」の観点からも、中小企業においても UTM 等による出入り口対策の導入やセキュアな通信環境の構築が必要。 ・支援にあたっては、対象企業のシステムや業務形態等を理解・把握し、業務上のセキュリティリスク及び対策の提示を、定期的かつ継続的に行うことが望ましい。 ・システム導入等のアドバイスができるよう、現地または遠隔で実施可能な環境及び人材を準備する。 ・中小企業への UTM の普及には、サイバーセキュリティのリスク対策としての価値を理解してもらうために、訪問により丁寧な説明を行い、トライアル等で効果を実感してもらうことが重要である。
③富士ゼロックス株式会社	・セキュリティ対策の低価格化へのニーズが高いが、費用感が定まっておらず、具体的な負担可能額は不明。 ・中小企業のネットワーク環境は多様であり、管理された状態でないことが多い。そのため、有事における事後支援でのシス	・セキュリティ対策の費用負担を必要最低限にする方策として、事業形態や取引先の要請に応じたセキュリティ対策のランク化を行い、ランク値に応じた製品・サービス・保険を選択できるようにすることで、多様性ある中小企業を広くカバーできるようになる。

事業主体	実証結果	セキュリティ対策のサービス検討
	テム復旧費用等について、定額サービスでの提供は難しい。 ・サイバー攻撃への危機感は高まっているが、人手や知識不足のため、具体的な対策は進んでいない。	・UTM 等の導入には、リモート監視によるアラート検知や、専門家による診断及び対策支援を併せて提供するサービスが良い。 ・現状のセキュリティ対策サービスの主なコストは人件費であるため、ビッグデータや人工知能（AI）に処理を代替させること等で、低価格化を図ることができる。
④SOMPO リスクマネジメント株式会社	・中小企業は自社がサイバー攻撃の被害を受けることの想像ができていないことが多く、重大なリスクとしての認識が不十分。 ・中小企業では、リスク管理、通信ネットワーク管理、インシデント対応及び教育訓練・改善について、達成度が低い。 ・情報システム部門や専任担当者をおいている中小企業は少なく、多くが情報システムの導入、保守、運用等をシステムベンダーに依存、丸投げしていた。	・地方の中小企業においては、地場の IT ベンダーとセキュリティベンダーが連携した協力体制を構築するなどの取組みが有効。 ・中小企業にセキュリティ上のリスクを認識してもらうには、実際のセキュリティ事故事例を紹介することで、自社にも起こり得ることを想起してもらうことが有効。 ・中小企業向けのインシデント対応支援を円滑にするために、サイバー保険とセキュリティ対策とを一体化したサービスとして、普及に向けた推進がなされることが望ましい。
⑤株式会社 PFU	・中小企業の経営層がサイバーセキュリティ対策の重要性を認識していない、情報システム担当者がいないなど、セキュリティ対策を行う体制が整っていない。 ・中小企業は、セキュリティ対策に割り当てられる費用は限られている。 ・地域の IT 会社には、情報セキュリティの提案ができる人材が不足している。	・セキュリティ対策サービスの普及には、販売側のサイバーセキュリティに関するスキル向上が必要だが、専門スキルをなるべく排除した分かり易い商品仕立てにすることの両面が重要となる。 ・中小企業の担当者がインシデント等の報告書を見て理解し、サーバー保守業者に対処を依頼できるように、報告書は専門用語を排して分かり易いものに改善する必要がある。
⑥MS&AD インターリスク総研株式会社	・アンケート結果から、セキュリティ対策強化に投資や手間をいとわない中小企業が一定数存在することが分かった。 ・実証申込み後に、既設 UTM の存在が判明し、UTM 設置を断念した企業がおり、既に導入していたにもかかわらず、活用できていない事例である。 ・セキュリティ対策を次のステップに進めるための選択肢が多く、中小企業が自らセキュリティサービスを選択することは、知識量や情報量から難しい。	・セキュリティ対策サービスは、リスクアセスメントとサイバー保険、監視と駆け付け、文書作成とセキュリティ人材派遣など、いくつかのサービスを組み合わせて提供することが有効と考えられる。 ・中小企業のセキュリティ対策ロードマップを明確にし、中小企業が自社に最適なセキュリティサービスを選べるようにすることが求められる。 ・セキュリティ関係文書や体制が整っていない企業が、高度なセキュリティ機器を導入しても活用されないことが想定されるため、セキュリティ対策に関するコンサルティングが必要となる。
大阪商工会議所	・サイバー攻撃が可視化され、何らかの対処が必要であることを実証参加の中小企業に一定程度認知させることができ	・UTM で可視化される、サイバー攻撃やウイルスの感染を放置すると、どのような被害に繋がるかという事例を具体的に示した上で、更なるニーズ

事業主体	実証結果	セキュリティ対策のサービス検討
	た。また、駆け付けによる初期対応でウイルス駆除等がなされ、被害拡大防止に繋がったケースも確認できた。 ・UTM の設置に関して、約 7 割の企業が自力で UTM を設置できたが、設置できた企業においても、攻撃の検知がゼロであった企業があり、必ずしも適切な箇所に UTM が設置されていなかった可能性がある。 ・実証参加企業へのサイバー攻撃を UTM で検知し防御していたにも関わらず、状況を確認できるポータルサイトの内容が理解しづらく、その効果が企業に十分に伝わっていなかった。	把握が必要。 ・中小企業においてセキュリティ対策の有力な手段となる UTM 機器の「導入の手軽さ」、「運用の手軽さ」を実現するために、設置環境の配下に端末が無いなど、不適切な箇所に接続された UTM を検出できる機能追加が必要となる。 ・サイバー攻撃の検知・防御状況を確認できるポータルサイトやアラート通知メールについて、中小企業が見てもデータの参照方法や、その意味するところが理解できるように改善し、次のアクションをどうすればよいか判断できるように通知方法の見直しが必要となる。
⑧株式会社日立製作所	・中小企業では、ネットワークの環境、利用アプリケーション等の情報が管理されていないケースが多い。 ・中小企業におけるウイルス対策ソフトの導入は進んでいるが、未知のウイルスに対応できるセキュリティ製品を利用している中小企業は少なく、セキュリティ製品の機能を知らないことも要因として考えられる。	・中小企業にセキュリティ製品を効率よく導入普及させるためには、セキュリティ製品の導入前に、現状調査サービスにてネットワーク環境の可視化をする必要がある。 ・サプライチェーン全体への攻撃への備えとして、取引先からのセキュリティ対策の要請の動きは、今後さらに顕著になってくると予想される。取引先からの調査や対策依頼がある場合、対応要員の確保や担当社員の育成が課題となる。

表 22 中小企業に必要なセキュリティ対策サービスの検討

4.2. 中小企業向けの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、中小企業が利用し易いセキュリティ簡易保険サービス(サイバー保険)のあり方について検討を行った。

以下に各事業主体のセキュリティ簡易保険サービスの検討について示す。

事業主体	実証結果	セキュリティ保険サービスの検討
①株式会社デジタルハーツ	・「サイバー保険を知らない」とのアンケート回答が大半となっていることから、まずはサイバー保険の内容の周知を徹底する必要がある。 ・セキュリティ製品に保険を付帯するなど、効率的なセキュリティサービスの開発が考えられる。	・サイバー保険の周知のために、中小企業と信頼関係のある地場企業と連携した啓発活動を行うことが有効である。 ・中小企業の実態に即した安価な保険サービスとして、以下について今後検討する必要がある。 ①加入しやすい安価なサイバー保険 ②セキュリティ製品へのサイバー保険の付帯
②東日本電信電話株式会社	・実証参加企業のサイバー保険の認知度は約 20%、導入企業は 2%と低い水準であった。自社の実態を踏まえた必要な対策を図る「サイバーリスクマネジメント」への対応の遅れが保険の付保率が低い要因の一つと考える。 ・サイバー保険の商品検討においては「提供方法」と「補償とコスト水準とのバランス」を念頭におくことが不可欠。	・UTM 等のセキュリティ製品に保険を付帯することで、自動的に補償が得られる等、一連のセキュリティ対策として、手配されることが望ましい。 ・保険の補償内容は、「復旧にかかる費用負担」が最もニーズが高いことから、賠償責任ではなく復旧費用を担保することが実態に即している。 ・セキュリティ製品に付帯する保険では補償が限られるため、企業のリスクに応じて不足する補償を上乗せできる保険が求められる。
③富士ゼロックス株式会社	・中小企業のサイバー保険の運用においては、損害賠償以外にも、調査・対策等の様々な費用がかかる。 ・アンケートの結果、サイバー攻撃で想定される影響には「わからない」とする回答が大多数を占めることから、中小企業では未だサイバー保険の費用負担イメージが確立されていない。 ・サイバー保険について、自動車保険の等級制度のような仕組みを適用することは難しい。特に中小企業は企業ごとにセキュリティリスクが異なるため、母数が大きい自動車保険と同様にリスク量を決める事は現実的ではない。	・サイバー保険を設計するために、中小企業側で発生する必要な調査コスト及び対策コスト等について、継続検討する必要がある。 ・中小企業にとっては、セキュリティ製品及びサービスの提供事業者が契約者となり、保険会社の提供するサイバー保険を付帯する商品付帯型の保険が導入しやすいと考える。 ・商品付帯型の保険が普及すれば、モニタリングでインシデント発生の経緯や被害状態を把握し、高リスクの被保険者（中小企業）には、リスクレベルに応じた保険を追加提案することができる。 ・サイバー保険は火災保険のような個別査定が必要であり、中小企業の個別のリスク量に応じた補償額（支払い限度額）が設定されるべき。
④SOMPO リスクマネジメント株式会社	＜サイバー保険として備えるべき要件＞ ・インシデント対応費用（調査費用、不正プログラム駆除費用等）が補償されること	・中小企業向けサイバー保険については、事故が生じた際のリスク移転（リスク・ファイナンス）の機能だけでなく、インシデントが発生した後にスムーズな調査等の手配を行うための与信（クレジット）

事業主体	実証結果	セキュリティ保険サービスの検討
	・保険金の支払だけでなくインシデント対応サービスの提供や斡旋を合わせて提供されること ・中小企業が加入可能な保険料設定であること ・中小企業が実際に入手可能であること	の機能が重要な位置付けとなっている。こうした観点から、中小企業向けサービスにあっては、セキュリティ対策サービスへの商品付帯契約として、サイバーリスクに関してプレ・インシデントからポスト・インシデントまでを一元的にカバーできるような提供形態が望ましい。
⑤株式会社PFU	・アンケートでは、情報漏洩等により引き起こされる損害賠償の大きさから、サイバー保険の必要性を直感的に感じる傾向にあるが、サイバー事故の発生頻度が想像し難いため、保険加入までは踏み切れていないと考えられる。 ・インシデント対応（調査・復旧）については、損害賠償と比べてかかる費用をイメージしやすいため、費用対効果の感覚を得やすいが、莫大な費用発生までには至らないという感覚を持たれている可能性がある。	・中小企業向けのサイバー保険の形態として、「セキュリティ対策サービス＋保険付帯」とすることで、保険検討のきっかけとなり、サービス提供ベンダーとしても、インシデント初動対応から情報漏洩調査までシームレスに対応できることから、費用が無いため調査ができないといった状況に陥らず、十分なサポートが可能となる。 ・保険費用を抑える条件として、「セキュリティ対策を講じていること」や「過去に漏洩事故がないこと」などを事前チェックすることにより、サービスの加入条件や免責事項等を明確にすることが考えられる。
⑥MS&ADインターリスク総研株式会社	・現在は、民間損害保険各社がそれぞれ独自にサイバー保険を販売し、事故データや損害額、損害調査方法などの情報共有が図られていない。 ・国や公的機関とも連携し、サイバー事故の事例、損害額、損害調査方法、脅威情報の共有などの体制が構築されれば、事故・脅威情報の共有によるサイバーセキュリティ対策への世論形成・普及促進が進むものと考えられる。	・お助け隊と同等品質を持つセキュリティサービスに対して、損害保険会社の共同保険により高品質で最低限の保険を組成し、商品付帯方式でサイバー保険を付帯する。共同保険とすることによって事故データの共有を実現することが可能となる。 ※共同保険方式でない場合、事故データの共有には契約者・被保険者の同意が必要となる。共同保険によって保険会社間で共有する事故データの内容については調整が必要である。
⑦大阪商工会議所	・中小企業においては、重大インシデントに対して損害賠償責任、フォレンジック費用等を幅広く補償する一般的なサイバーリスクに関する保険の普及率が未だ低い状況である。これは、中小企業にサイバーリスクに対する意識の低さや保険料水準の高さが要因であると考えられる。 ・サイバー攻撃は日々進化し、それに合わせて、保険の発動要件が定期的に変動するという事象が発生し、保険商	・実際に大きな被害が発生した事案や、外部調査費用、データ復旧費用を把握できるような事例をより多く集約して示すことで、サイバー保険の必要性を訴求するとともに、中小企業にとって必要な補償額の基準等が明らかになることが望ましい。 ・中小企業が加入しやすい保険料水準を安定的に提供するには、中小企業が自らウイルス対策ソフトの更新などの最低限の対策を日常的に実施することや、事前のリスク診断、最新のサイバーリスク対策に関する情報収集を適時適切に行っていくことが望ましい。

事業主体	実証結果	セキュリティ保険サービスの検討
	品設計が複雑になる可能性がある。 ・本実証では、中小企業向けの保険発動要件やその基準、免責、保険料・保険金の額などを検討する上で、ややサンプル数が少なかった。	・中小企業向けの簡易的なサイバー保険の実現に向けて、引き続きデータや知見の収集を継続し、中期的に軌道修正を続けていく必要がある。
⑧株式会社日立製作所	・アンケートから、約 3 割の中小企業がセキュリティ対策が取引先の要件化とされつつあると回答している。そのため、取引先からはセキュリティ対策状況の開示を求められた場合に、サイバー保険加入の証左として取引先に提示できる証明書の発行や、診断レポートの提供といった付帯サービスのニーズも高まってくる可能性がある。	・中小企業において、サイバー保険の普及を図るためには、サイバー保険の補償範囲や保険料水準並びに付帯サービスといった保険設計の観点だけでなく、保険の必要性を訴求するアプローチやプロモーションの工夫も必要であると考えられる。 ・UTM 等のセキュリティサービスを導入している場合に、サイバー保険で大幅な割引を適用する、セキュリティサービスにサイバー保険を自動的にセットするなど、相乗効果を促進するような保険の設計や加入スキームの検討が期待される。

表 23 中小企業向けのセキュリティ簡易保険サービスの検討

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①】「SOMPO SOC」（SOMPO リスクマネジメント）
（「UTM 監視・検知サービス」の後続サービス）

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。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ー（Syslog サーバー）経由で SOMPO リスクマネジメント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。
特長	◇豊富な分析知見と高度ログ自動分析エンジン 24 時間 365 日セキュリティログを収集し、大企業向け SOC サービスで得られる脅威情報から新たに生成される分析ルールを適用させた高度自動分析エンジンにより、高品質なセキュリティ監視サービスを提供する。
費用	◇リーズナブルな費用 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となる。 （参考） 「セキュリティ監視サービス」（販売予定価格）　※分析ログ容量５Ｇの場合 ・初期費用：152,000 円（税抜）　・初年度月額利用料金：16,000 円（税抜） ・初年度費用合計：344,000 円（税抜） ・次年度以降月額利用料金 17,000 円（税抜）・年間合計 204,000 円（税抜） ※ＵＴＭを新たに購入する場合の「ＵＴＭ運用管理サービス」は別途要
保険	◇サイバー保険を自動付帯 「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：損害保険ジャパン日本興亜）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 24 ビジネス化事例①（SOMPO リスクマネジメント）

（２）【ビジネス化事例②】「SOMPO SHERIFF」（SOMPO リスクマネジメント）
（「パソコン監視分析サービス」の後続サービス）

概要	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、SOMPO リスクマネジメントの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、早期に駆除する。
特長	◇ウイルス感染による脅威を早期検知（緊急アラート） パソコン上のさまざまな挙動ログを SOMPO リスクマネジメントの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・分析することで、従来のウイルス対策ソフトで検知されない未知のウイルスも含めて、緊急性の高いウイルス感染の脅威を検知し、緊急アラートメールで通知する。 ◇検知したウイルスを早期分析・駆除（脅威ハンティング機能） 緊急アラートで通知した脅威ファイル及び被疑ファイルについては、専門のセキュリティエンジニアがリモートアクセスにより早期に分析・駆除する。 ◇面倒な設定や調整（チューニング）は不要 パソコンの挙動ログを収集するための EDR をインストールするだけで、サービス利用者の通常業務に支障をきたさない。また、サービス利用者側でのルール設定や機器の調整（チューニング）等の作業を生じさせない仕組みにしたことにより、中小企業では困難である専任のエンジニア等の要員手配が不要である。 ◇定期的なレポートでパソコンのリスクを“見える化” 定期的にセキュリティレポートを提供する。当該レポートは、ウイルス感染状況のほか、不正なプログラムサイト、フィッシングサイト等へのアクセス状況、セキュリティレベルの低い Wi-Fi への接続状況、USB の接続状況などのリスクを“見える化”するとともに、ソフトウェアのインストール状況やハードディスクの故障予兆などの従業員によるパソコンの利用状況を明らかにすることで、サービス利用者のセキュリティ対策の検討に資するものとなっている。
費用	◇リーズナブルな費用 パソコンを常時監視・分析し、ウイルス感染時の事後対応までを中小企業が自力で行うのは、人件費その他のコスト負担が大きく、現実的に困難である。「SOMPO SHERIFF」の導入により、監視・分析から駆除までのリスクマネジメントに係る費用を大幅に抑えることが可能である。 （参考） 初期費用：35,000 円（税抜）、月額利用料金：1 台当たり 1,800 円（税抜）
保険	◇サイバー保険を自動付帯 「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）を自動付帯している。ウイルス感染の分析・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 25 ビジネス化事例②（SOMPO リスクマネジメント）

（３）【ビジネス化事例③】「商工会議所サイバーセキュリティお助け隊サービス」
（大阪商工会議所）

概要	「日本の中小企業ならびにサプライチェーンをサイバー攻撃から守る」「中小企業がサイバーセキュリティにより事業継続力と企業価値を高めることを支援する」をビジョンに、大阪商工会議所が事業実施主体となって、NEC、東京海上日動、キューアンドエー、NEC ネクサソリューションズなど各分野のリーディングカンパニー、そして地域で機動的に活躍している地場の IT 事業者などとタッグを組み、大阪市内を中心とする京阪神の中小企業向けに利用しやすいサービスを提供する。
特長	◇訴求ポイント 「総合性」・・・セキュリティ機器、ネットワーク監視、相談窓口、駆け付け、保険がパッケージ化されたワンストップ性 「目的」・・・利潤でなく政策実現 「安価」・・・年 10 万未満。初期費用ゼロ。※機器設置支援は自己負担 「簡便」・・・導入・運用が簡便（情報システム担当者不在でも利用可能） 「会社の価値を高める」・・・同サービスの利用が第三者認証に近いような“取引先を安心させる”要素になるよう、ブランディング推進 「ＢＣＰ対策」・・・事後対応力の向上に資するもの 「付随教育機能も充実」・・・関連セミナーの開催、最新セキュリティー情報の提供、SECURITY ACTION の宣言支援
費用	◇サービス提供価格 月額 6 千円～8 千円程度での設定を検討 （簡易 UTM 設置は費用は受益者負担 15,000 円（交通費込・税別）予定
保険	◇簡易的な保険（全員加入型）※以下の内容で検討中 ・中小企業が設置している UTM で不正アクセス等の発生やそのおそれを検知。 ・検知後に大阪商工会議所が紹介する IT 事業者が訪問のうえ初動対処等を行う。 ・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を支払う。 （インシデントの原因特定や、情報漏洩の際の費用補償は、別途上乗せ保険の加入が必要） ◇上乗せ保険（任意加入型） （東京海上日動の主に以下を補償するサイバーリスクに関する保険の提供を予定） ①【賠償】サイバー・情報漏洩事故 サイバー攻撃などに起因して法律上の損害賠償責任を負担することによって被る損害 ②【費用】サイバー・情報漏洩事故対応費用 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負担するサイバー・情報漏洩事故対応費用

表 26 ビジネス化事例③（大阪商工会議所）

5. 中小企業のセキュリティ対策の実態と今後の課題

本事業の実証により把握された中小企業のセキュリティ対策の実態と、今後の中小企業のセキュリティ対策の向上のための取組み課題について、「サイバー攻撃と防御」、「組織的セキュリティ対策」、「人的リソース」、「サイバー保険」の４つの観点から取りまとめた。

（1）サイバー攻撃と防御

【対策の実態】

中小企業も業種や規模を問わず例外なくサイバー攻撃を受けており、ウイルス対策ソフト等の既存対策だけでは防ぎきれない

本事業では、実証参加企業に設置したUTM機器等により、ボットネットとの通信などマルウェア感染等による外部への不正通信や不正プログラムが含まれる通信を数多く検知及び遮断した。中には駆け付け対応によってウイルス駆除等を行い、被害拡大防止に繋がったケースも報告されている。また、アンケート調査の結果から、約8割強の中小企業でウイルス対策ソフトが導入されているが、サイバー攻撃を検知及び防御できるUTM機器等は2割強しか導入が進んでいない状況が確認できた。これらのことから、中小企業も業種や規模を問わず例外なくサイバー攻撃を受けており、ウイルス対策ソフト等の既存対策だけではセキュリティ対策として十分ではないことが確認された。

なお、今回の実証を行った事業主体の中には、中小企業におけるUTM機器の「導入の手軽さ」と「運用のし易さ」の実現を目指し、実証用に用意した自動設定による簡易UTM機器の設置を通じ実証に取り組む事業主体がいたが、それでも約3割の中小企業が自力では設置できなかったとの報告がなされている。

【今後の課題】

中小企業における導入・運用に適したUTM機器等セキュリティ機器の開発と普及促進

「多層防御」の観点からUTM機器等による出入り口対策の導入やセキュアな通信環境の構築が重要だが、現在のUTM機器等については、導入の前提として一般的にネットワーク管理者などの情報システム担当者が社内にいる企業を想定したものが多く、中小企業が自ら導入し運用することは困難である。また、中小企業がセキュリティ対策にかけられる費用は総じて高いとは言えないため、費用的な観点からもセキュリティ機器の導入を行うことは難しい。

今後、中小企業へのサイバー攻撃を検知及び防御するUTM機器等のセキュリティ機器を普及促進するためには、導入・運用に係るコストの低廉化と併せて、中小企業でも導入・運用し易い機器開発及びサポート体制の構築が重要である。

（2）組織的セキュリティ対策

【対策の実態】

自社のネットワーク環境について把握できている中小企業は少なく、IT ベンダーに丸投げ状態も見受けられる

アンケート調査の結果から、約 3 割の中小企業が自社に対するサイバー攻撃を認識している一方で、約 7 割の中小企業においてはサイバーセキュリティ体制を構築できていない状況が確認された。本事業においても、多くの実証参加企業が自社のネットワーク環境について把握できておらず、情報システムの導入、保守、運用等を IT ベンダーに依存し、丸投げしていた状況もあった。この結果、UTM 機器等のセキュリティ機器を導入する際、機器設置が円滑に行えない、あるいは設置を断念するなどの弊害が発生するケースが見受けられた。

【今後の課題】

外部の支援を適切に活用するため、中小企業自らが実施すべき取組みや必要性を理解するための継続的な意識啓発が重要

セキュリティ対策を自ら実施する場合に限らず、外部支援を活用する場合であっても、自社のネットワーク環境やシステム環境を把握しておくことが求められる。全てを IT ベンダー任せにせず、必要最低限の知識の習得や社内の状況を自ら把握することが重要であり、中小企業の経営者はこれを認識する必要がある。

このため、中小企業の経営者に対して、サイバー攻撃の実態やウイルス感染による被害などの事例を具体的に示すことで、セキュリティへの意識向上を図るとともに、まずは自社のネットワーク環境や対策状況の把握などの実施できることから取組みをスタートさせ、必要最低限の対策を講じることの必要性を理解してもらうための継続的な啓発活動が重要である。

（3）人的リソース

【対策の実態】

中小企業では人的リソースが不足していることにより IT 専任者がいる割合が低く、日常的なセキュリティ対策に取り組むことができていない

アンケート調査の結果から、情報システムの専任者を置く中小企業は少なく、人的リソース不足から社長や他の業務に従事している社員が兼務しているケースが多いことが確認できた。また、セキュリティに関する専門知識を得る機会が少なく、ウイルス感染等の注意喚起情報も行き届いていないことが多いこともあり、日常的なセキュリティ対応ができていない中小企業が多い。

【今後の課題】

人的リソース不足を補うため、外部専門家による伴走型支援サービスの活用検討と普及促進

人的リソースが不足している中小企業においては、自社のシステム環境や業務環境等を理解している外部専門家による伴走型支援サービスの活用を検討することが望ましい。例えば、外部専門家の支援を通じたネットワーク構成の書面化、UTM 機器等の導入及び運用支援など、一連のセキュリティ支援をワンパッケージ化した伴走型サービスを有効に活用することの検討と普及促進が重要である。

（4）サイバー保険

【対策の実態】

中小企業においてサイバー保険の認知度は低く、普及が進んでいない

アンケート調査の結果から、もしもの時の備えとなるサイバー保険について、多くの中小企業が「必要である」と肯定的であったが、サイバー保険そのものの認知度は約 2 割と低く、普及が進んでいない状況が確認できた。

サイバー保険の認知度が低く普及が進まない理由としては、具体的な事故事例や損害額等の情報が少なく、中小企業が自分事として捉える意識が希薄なこと、損害賠償やインシデント対応にかかる費用感がわからず費用対効果が理解できない等が挙げられる。

【今後の課題】

費用対効果の可視化、中小企業でも加入しやすいサイバー保険の実現

中小企業においてサイバー保険の重要性を認識してもらうためには、具体的な事故事例や損害額等の情報提供が有効であるが、現状は損害保険会社間での情報共有が十分ではなく、中小企業に対して統一的かつ有効な情報提供がなされていない。中小企業へのサイバー保険の普及を促進するためには、損害保険各社が保有する情報の集約及び共有を図るための効果的な仕組みを構築し、サイバー保険に加入することによる費用対効果を可視化し、中小企業に提示することが有効である。

また、中小企業における加入のし易さの観点からは、セキュリティ製品にあらかじめサイバー保険を付帯することが有効である。ただし、付帯保険については一般的に補償範囲が限られるため、損害補償等については上乗せ保険などの検討が重要である。

6. 全体のまとめ

本事業は、IPA が公募により全国 8 地域で請負事業者を選定し、請負事業者が事業主体となって実施体制を組織することで、地域の中小企業に実証への参加を呼びかけ、計 1,064 社の中小企業が実証に参加した。このうち、727 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及び防御を実施し、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、従来からの攻撃手法である外部からの不正アクセスに加え、ボットネットとの通信など不正プログラムによる内部から外部への不正通信を数多く検知及び遮断した。また、全国 8 地域において合計 128 件のインシデントが発生し、そのうち駆け付け支援を 18 件実施した。中には駆け付け支援により、ウイルス駆除等を行ったことで被害拡大を防止できたケースもあり、中小企業においても業種や規模を問わず例外なくサイバー攻撃を受けている実態が明らかになった。

一方、実証参加企業以外も含めた延べ 1,716 社を対象に実施したアンケート等によるセキュリティ対策状況等の確認結果では、サイバー攻撃を検知及び防御する機能を持つ UTM 機器等のセキュリティ機器は 2 割強しか導入が進んでおらず、既に導入している場合であっても有効活用できていないケースがあることが確認された。また、セキュリティ対策を進める上での課題として、約 3 割の中小企業が自社内のサイバー攻撃を認識しているものの、これを大きく上回る約 7 割がサイバーセキュリティ体制の構築ができていない状況であることが確認された。

これらは、中小企業における人的リソースなどの経営資源が不足していることに加え、中小企業を巡るサイバーセキュリティの脅威や事業に及ぼす影響等に関して経営者の理解が不足しており、自分事として捉えていない可能性があることが推察される。このため、中小企業の経営者に対して、サイバー攻撃やウイルス感染による被害などに関する身近な事例を具体的に示すなど、セキュリティ対策への理解を促すための継続的な啓発活動が重要である。

本事業において実証参加の募集活動を行った際、地域によっては事業説明会やウェブ等による告知だけでは、目標とする実証参加企業数を確保することが難しく、事業主体の創意工夫により追加的な募集活動を実施した。当該活動は中小企業と日常的に付き合いがあり、信頼関係が構築されている地域の公的機関や商工団体、業界団体等と連携したことで、効率的・効果的に実証参加企業を集めることができた。このような事例から、中小企業の経営者に対してサイバーセキュリティの必要性や実証事業の重要性等を効果的に訴求するためには、対象地域の地域特性や産業特性等を十分に考慮した上で、セキュリティ関連のみならず地域コミュニティを形成する様々な企業、機関、団体等との連携が有効であるといえる。

また、今回の実証結果を踏まえたサイバーセキュリティ対策の観点では、サイバー攻撃を検知及び防御する UTM などのセキュリティ機器等の有効性は疑う余地がなく、今後の普及

促進を図ることが重要である。そのため、中小企業でも導入・運用しやすいUTMなどのセキュリティ機器等の開発とサポート体制の構築が求められる。中小企業が扱いやすいセキュリティ機器等の提供と専門家による伴走型支援などの必要なサポートをワンパッケージで提供することは、人的リソースが不足する中小企業において有効である。併せて、セキュリティ対策にかけられるコストに制約があるため、中小企業に求められる必要最低限のサポートを検討することで支援内容のスリム化を図り、提供する支援サービスに係る価格の低廉化を図る必要がある。

また、インシデント発生など有事の備えとなるサイバー保険の普及に向けては、中小企業にとって身近なサイバー事故の事例や損害額等の情報に加え、サイバー保険適用による必要コストや補償額等を具体的に提示することで費用対効果の可視化を図るなど、サイバー保険の有効性を理解してもらうための取組みを検討することが必要である。併せて、セキュリティ機器等にサイバー保険を付帯する保険商品を開発するなど、中小企業が導入しやすいサイバー保険のあり方検討も引き続き重要である。なお、付帯保険については一般的に補償範囲が限られるため、事故損害に見合った適当な保障額を設定する上乗せ保険の検討も必要である。

上述した一連の取組みを推進する上では、今般の地域毎あるいは個社毎の検討では保有しているサイバー攻撃のデータや事故データなどの情報量に限りがあり、検討が難しいことも想定される。そのため、今般実証を行ったサービスのビジネス化を促すための取組みとして、今後、実証に取り組む事業主体等がコンソーシアムを形成するなど、今後のビジネス化に向けた必要な情報共有や検討を実施することができる仕組みの構築が有効であり、中小企業のサイバーセキュリティ対策の促進に向けた今後の課題の一つとして検討を行う必要がある。

以上