IPA 情報処理推進機構

中小企業向けサイバーセキュリティ事後対応支援事業
（サイバーセキュリティお助け隊）
成果報告書（概要版）

2020年４月

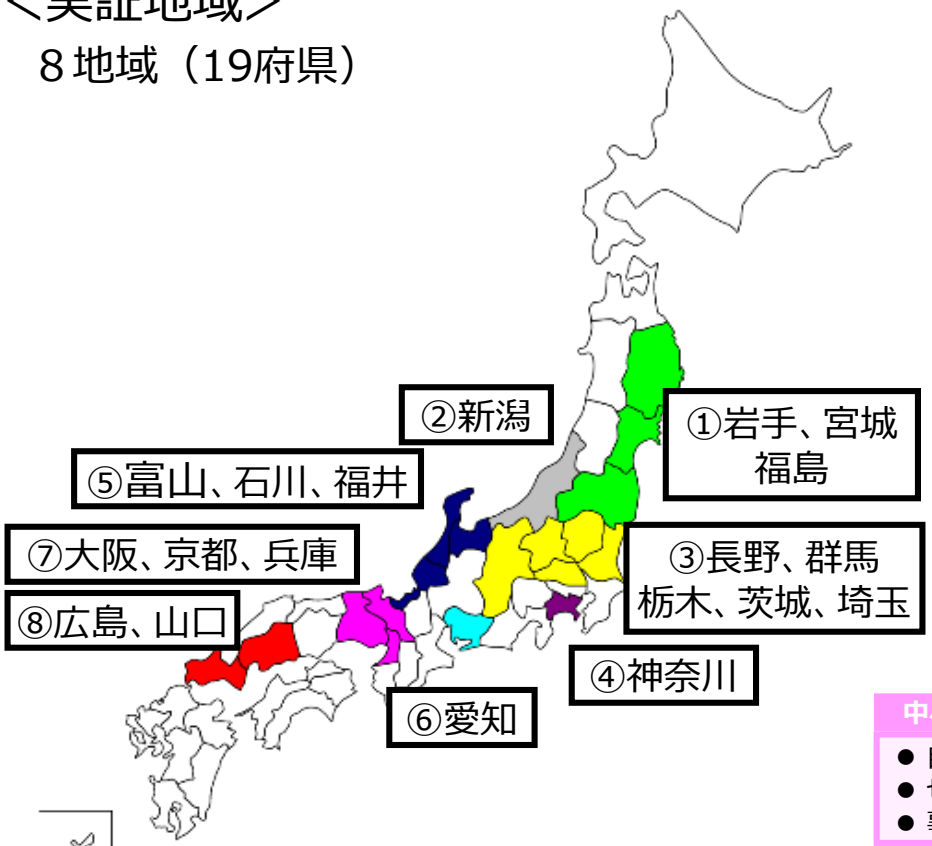
独立行政法人情報処理推進機構
セキュリティセンター

事業実施の概要

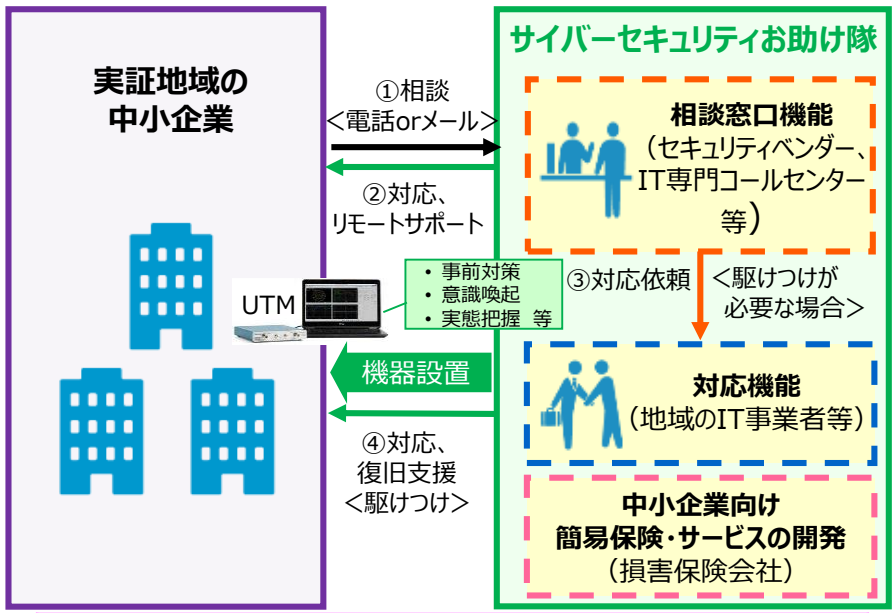
- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社が実施体制を組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**中小企業に必要なセキュリティ対策サービス**の内容、及び民間による**中小企業向けのセキュリティ簡易保険サービス**のあり方を検討した。

＜実証地域＞

８地域（19府県）



＜実証のイメージ＞



実証結果

中小企業　側

- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側

- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

実証参加状況

- 全国**8地域**で請負事業者が事業主体となって実施体制を組織し、対象地域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。

対象地域 （対象地域の北から順に記載）	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）

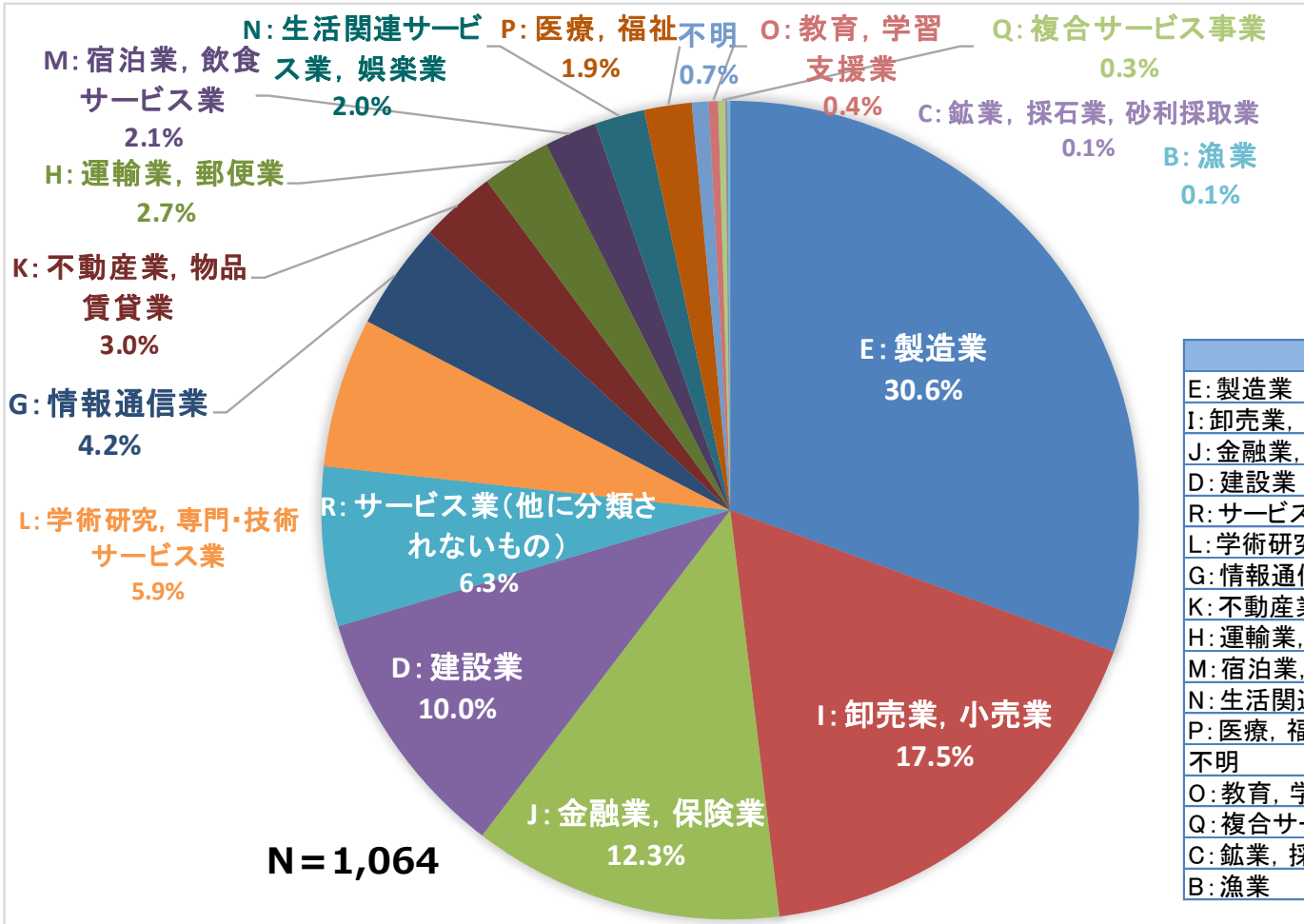
計 1,064社

実証参加企業の属性

- 実証参加企業1,064社の業種別内訳は、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。

<業種別一覧>

分類：日本標準産業分類（大分類）



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

事業説明会の実施状況

- 実証参加企業の募集及びサイバーセキュリティに関する普及啓発のため、事業開始、中間報告、成果報告の各段階で事業説明会を延べ**91回**開催し、1,642社、1,956名の参加を得た。

＜事業説明会の実施状況＞

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

実証参加企業募集に関する状況

- 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、各種の取組みを行った。

＜参加企業募集のためのその他の取組み＞

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 ・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、電機メーカー等のサプライチェーン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
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）
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

セキュリティ状況等の実態把握

- 実証参加企業1,064社に対して、セキュリティ機器等による**サイバー攻撃の実態把握**（727社）、及びアンケート等による**セキュリティ対策状況等の把握**（1,716社）を行った。

＜セキュリティ状況等の実態把握＞

事業主体	実証参加企業数	中小企業のセキュリティ状況等の実態把握					
		セキュリティ機器等によるサイバー攻撃の実態把握			アンケート等による対策状況等の把握		
		(設置数)	内訳	社数	(延べ数)	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	40	参加企業アンケート	40
②東日本電信電話株式会社	148	148	UTM機器	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	101	UTM機器	101	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	110	UTM機器	38	34	サイバーリスク簡易診断	18
			クラウド型WAF	0		WEBアプリ簡易診断	16
			EDRソフト	72			－
⑤株式会社PFU	120	97	PC監視ソフト	97	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	55	据置型UTM	27	377	事前アンケート	193
			クラウド型UTM	28		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	112	UTM機器	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	23	UTM機器	10	116	簡易セキュリティアセスメント	107
			EDRソフト	13		現場セキュリティアセスメント	9
計	**1,064**	**727**			**1,716**		

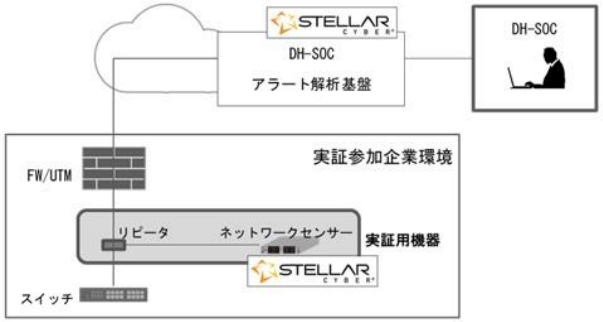
※アンケート等の実施先には、事業説明会の参加企業等、一部実証参加企業以外のものを含む。

検知及び監視の仕組みと実証結果

● 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た。

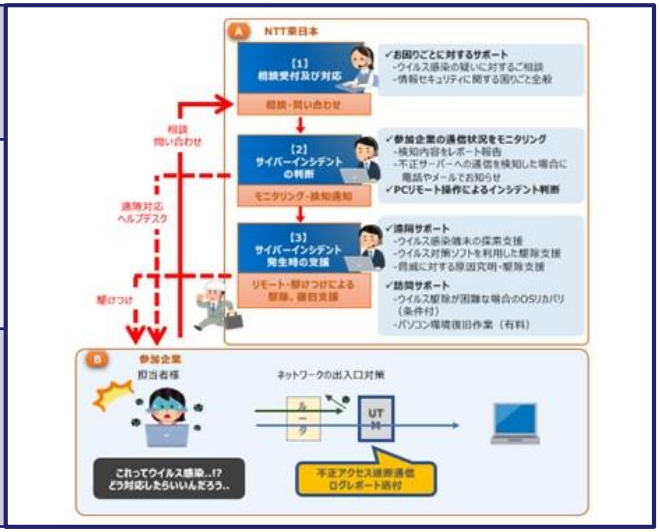
①株式会社デジタルハーツ （対象地域：宮城、岩手、福島）

セキュリティ機器	＜ネットワークセンサー＞ 「Starlight」（Stellar Cyber 社）
検知＆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ベントは確認されなかった。ただし、検知以外の事象確認で、駆け付け対応を2件実施した（Emotet感染対応）。



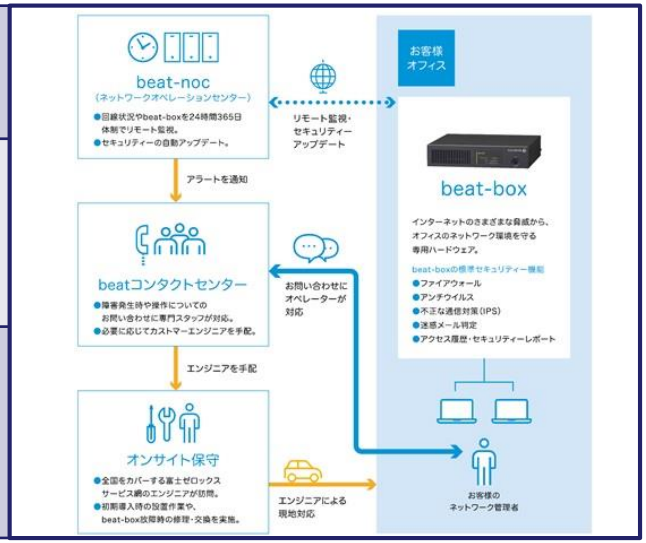
②東日本電信電話株式会社 （対象地域：新潟）

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＆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、ユーザ端末がマルウェア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、アドウェアに感染したケースであった。不正メール検知に関しては、約1/3の企業で検知されている。



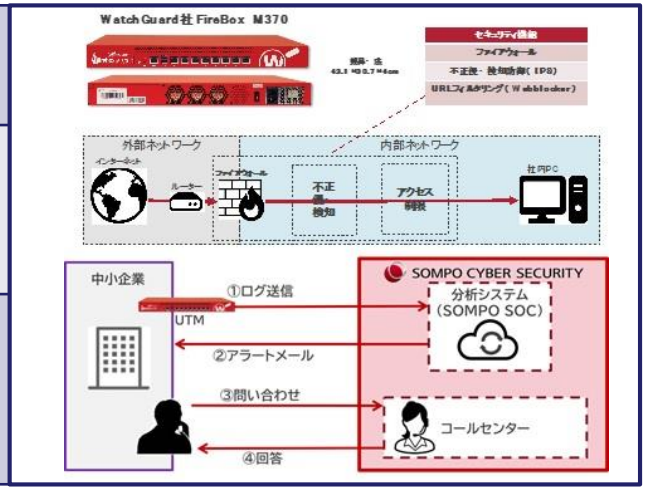
③富士ゼロックス株式会社　（対象地域：長野、群馬、栃木、茨城、埼玉）

セキュリティ機器	＜UTM＞ 「beat-box」（富士ゼロックス）
検知＆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。



④-1 SOMPOリスクマネジメント株式会社　（対象地域：神奈川）

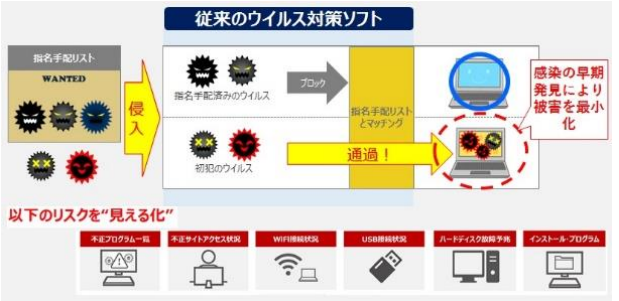
セキュリティ機器	＜UTM＞ 「Firebox M370」（Watchguard社）
検知＆監視の仕組み	UTM機器のセンサー（IPS機能及びURLフィルタリング機能）からのアラートに係るログデータを「セキュリティログ自動分析システム」に送信し分析することで、セキュリティインシデントを検出する。
実証結果	UTM機器設置38社において、4件の緊急度「高」のアラートを発信し、このうち1件は社内から外部への「不正なIPアドレスへの通信」であったため、駆け付け支援を行い不正プログラムの駆除を実施した（残り3件はUTM機器で防御）。



※クラウド型ＷＡＦは、中小企業が自らDNSサーバの設定変更を行うこと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。

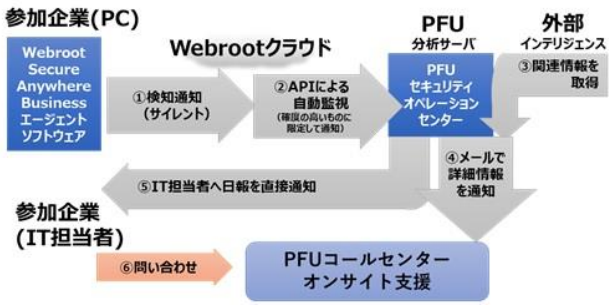
④-2 SOMPOリスクマネジメント株式会社　（対象地域：神奈川）

セキュリティ機器	＜EDR＞ パソコン監視分析サービス
検知＆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。



⑤株式会社PFU　（対象地域：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＆監視の仕組み	ファイアウォールやUTM機器等の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、導入していたウィ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。

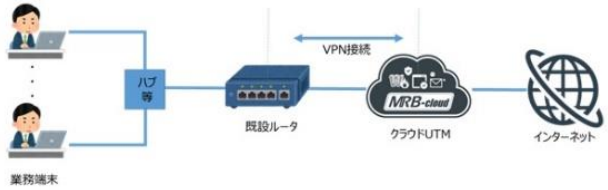


⑥ MS&ADインターリスク総研株式会社　（対象地域：愛知）

セキュリティ機器	＜据置型UTM＞「SonicWall TZ300 TotalSecure」(SonicWall) ＜クラウド型UTM＞「MRB-Cloud」（ALSOK）
検知＆監視の仕組み	＜据置型UTM＞ 実証参加企業にて、ルータとHUB（またはPC）の間に据置型UTMを挟み込む形で設置する。据置型UTM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、駆けつけ要否判断等を行う。 ＜クラウド型UTM＞ 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促す。
実証結果	＜据置型UTM＞ ポートスキャンによる偵察行為（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（ボットネット通信）は89件だった。 ＜クラウド型UTM＞ 検知された外部から内部への不正通信（130,621回）のすべてが偵察行為であった。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。

＜据置型UTM接続構成例＞

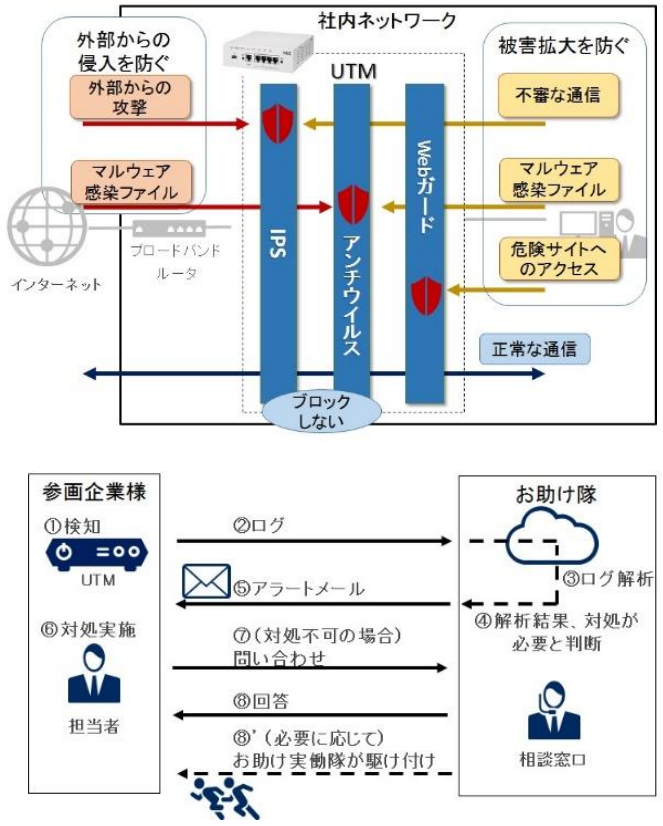
＜クラウド型UTM接続構成例＞



＜クラウド型UTM接続構成例＞
（レンタルルータ有）

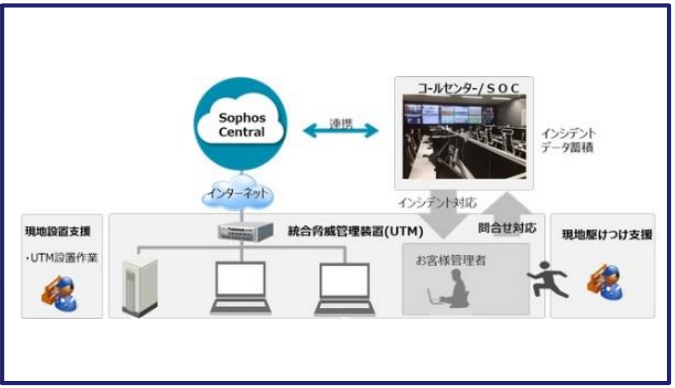
⑦大阪商工会議所　（対象地域：大阪、京都、兵庫）

セキュリティ機器	＜UTM＞ 簡易UTM機器（NEC） ※既存UTMをベースに中小企業が容易に設置、運用できるよう設計・製造
検知＆監視の仕組み	実証参加企業のネットワーク内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エ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。



⑧ 株式会社日立製作所　（対象地域：広島、山口）

セキュリティ機器	＜UTM＞ 「Sophos XG115」（SOPHOS社）
検知＆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。駆け付け支援が必要なインシデントは発生0件。



セキュリティ機器	＜EDR＞ 「Cisco AMP for Endpoints」（Cisco社）
検知＆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、駆け付け支援が必要なインシデントは発生0件。

アラート検知等の結果

- 実証の結果、UTM機器等により、サイバー攻撃に関する様々なアラートを検知及び防御した。アラート種別ごとの検知状況の取りまとめは以下のとおり。

＜サイバー攻撃に関するアラート種別と検知状況＞

アラート種別	アラート種別の説明	アラート検知状況
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やSQLインジェクション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、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。
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	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 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。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。
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）	**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。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	身代金要求型のマルウェアである**「ランサムウェア」を多く検知及び無害化**し、被害を未然に防ぐことができた。また、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。
⑤エンドポイントでのアラート検知	パソコン端末にンストールした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	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る。EDRソフト等により、相当数の**不正プログラムや不正サイトへのアクセス痕跡**等を検知し、マルウェアの駆除等の処置を行った。

相談・インシデント等対応状況

- 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）を構築し対応した。
- 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。

＜コールセンター対応及びインシデント対応等の状況＞

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

※電話およ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

主な駆け付け対応事例

地域	群馬県	業種	サービス業	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	当該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。				

地域	神奈川県	業種	サービス業	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。				

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。				

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。				

セキュリティ対策状況等の把握

- 事業主体毎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。

＜アンケートによる状況調査＞

調査ポイント	セキュリティ対策状況
現在、自社で実施しているセキュリティ対策	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。
情報セキュリティ対策にかける費用	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。
情報セキュリティ対策を進める上での課題	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。
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。

＜脆弱性診断等による調査＞

診断方法	セキュリティ対策状況
・WEBアプリ簡易診断 ・公開サイト脆弱性診断	問合せフォームを設置しているWEBサイトもある中で、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 やクリックジャッキング 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。

＜セキュリティ訓練等＞

訓練方法	セキュリティ訓練結果
・標的型攻撃メール訓練 ・サイバーセキュリティ演習	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。

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ていない

- ◆ 実証では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等を数多く検知及び遮断
- ◆ ウイルス対策ソフトは約8割強導入されているが、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

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
- ◆ UTM機器等の導入・運用に係るコストの低廉化と併せて、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

（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

- ◆ 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割の企業においてはセキュリティ体制を構築できていない
- ◆ 自社のネットワーク環境について把握できておらず、UTM機器等の導入設置が円滑に行えない等、弊害が発生するケースがあった

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

- ◆ 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
- ◆ 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することが必要

（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
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

◆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

◆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

◆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の有効活用の検討と普及促進が重要

（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
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

◆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

◆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

◆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

全体のまとめ

- 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**が、**検知及び防御のための対策や社内体制の構築ができていない**企業が多いことが確認された。
- 人的リソースの不足やコストに制約がある中小企業に、必要なセキュリティ対策を促すためには、「継続的な意識啓発」、「導入・運用しやすい対策機器やサイバー保険の開発」、「専門家の伴走型支援を含むワンパッケージ化」、「コスト低廉化」が重要であり、これらを効果的に推進するため**地域コミュニティとの連携促進**や**ビジネス化に向けた情報共有の仕組みの構築**が有効。

中小企業のセキュリティ状況等の実態

◆業種や規模を問わず、内外に向けた不正通信等を数多く検知
◆計128件のインシデントが発生し、うち駆け付け対応を18件実施
◆サイバー攻撃を検知及び防御できるUTM機器等の導入は2割強のみ
◆約7割の企業においては社内のセキュリティ体制構築ができていない
◆サイバー保険の認知度は低く、普及が進んでいない

対策普及に向けた取組みの方向性

◆セキュリティ対策への理解を促す継続的な意識啓発
◆導入・運用しやすいUTM等セキュリティ機器の開発及び普及促進
◆セキュリティ機器と専門家による伴走型支援のワンパッケージ化を検討
◆中小企業に求められる支援サービスのスリム化によるコストの低廉化
◆加入しやすいサイバー保険の開発と普及促進

取組み推進のポイント

◆地域特性や産業特性等を十分に考慮し、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

◆実証サービスのビジネス化を促すため、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