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（地域：愛知県）
成果報告書

請負事業者：MS&AD インターリスク総研株式会社

目次

本編

本編

I. 本実証事業の概要

1. 背景・目的

IoT 技術の進展等によりサイバー攻撃の脅威が高まっている中、特に中小企業においてサイバーセキュリティに対する意識が低く、対策が遅れているケースが見受けられる。本事業は、サイバー攻撃はあらゆる産業活動に潜み、サプライチェーンの構成員である中小企業において、その対策が経営を左右しかねず、本実証事業において中小企業におけるサイバーセキュリティ意識向上を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を検証、実現させていくことを目的としている。

2. 本事業の概要

上記をふまえ、本実証事業の参加企業（以下「参加企業」という。）200 社程度において、サイバーセキュリティ対策レベル別にカテゴリー分けをし、カテゴリー（レベル）に応じて、セキュリティ体制構築支援や演習等を実施した。（具体的には、参加企業につき、以下のようにサイバーセキュリティに関する①コールセンターや駆けつけ隊などの支援体制構築、②サイバーセキュリティセミナーや演習など意識向上、③UTM 設置による実態把握、④アンケートによる実証モニタリング、⑤成果報告、を実施）

（1） **実施内容・スケジュール**

実施した内容・スケジュールは表 1 のとおり。

【表 1】実証事業のスケジュールとメニュー　（◎：利用可能、○：任意で利用可能、－：対象外）

実施内容		利用可能な参加企業カテゴリー			実施スケジュール					
		A	B	C	7 月	8 月	9 月	10 月	11 月 12 月	1 月
1	愛知県お助け隊専用コールセンター	◎	◎	○	25 日	←	→			
2	駆けつけ隊によるサポート	◎	◎	○	25 日	←	→			
3	UTM 機器によるサイバー攻撃の検知 据置型 UTM	◎	◎	－	25 日	←	→			
	クラウド UTM	◎	◎	－	25 日	←	→			
4	サイバー保険（UTM 付帯）の付保	◎	◎	－	25 日	←	→			
5	セキュリティ体制構築支援 （B 群・C 群向け基礎セミナー）	○	◎	◎		28 日 29 日				
6	サイバー演習（A 群向け）	◎	－	－			24 日			
	サイバー演習（B 群向け）	－	◎	－				23 日 24 日		
7	サイバーセキュリティセミナー 兼中間報告会	◎	◎	◎				16 日		
8	成果報告会	◎	◎	◎						15 日 16 日

（２） **実施対象**

愛知県に本社のある、中小企業基本法に定める中小企業者・小規模企業者を対象とした。

なおネット接続環境があることを原則とし、UTM 設置に応じることができる企業を中心として、何らかの理由で UTM が設置できなかった企業については、セミナー・各種説明会/報告会への参加を認めた。

提案書記載の「セキュリティ対策レベル」（図１）に基づき、事前アンケート回答内容を踏まえて、図２のとおりカテゴリー分けを実施し、選定結果通知を発信。選定結果発信時の振り分け状況は表２のとおり。

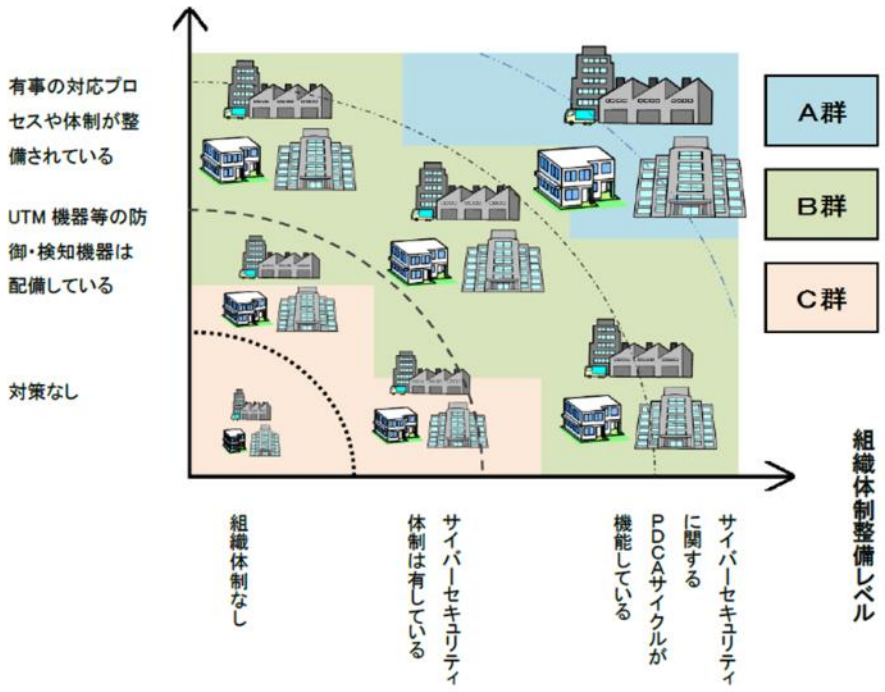
実証地域の選定理由は、愛知県は日本を代表する製造業者やエネルギー関連事業者が本社を構え、そのサプライチェーン企業群が集積する、いわゆる企業城下町である。MS&AD インターリスク総研株式会社（以下「MS&AD インターリスク総研」という。）と同じく MS&AD インシュアランスグループ傘下の、三井住友海上火災保険株式会社（以下、「三井住友海上火災保険」という。）とあいおいニッセイ同和損害保険株式会社（以下「あいおいニッセイ同和損害保険」という。）の愛知県における二社合算の市場占有率は実に約 43.7%である。（2019 年３月末、※主要損保六社の損害保険一般種目合計）

また、サイバー保険を含む新種保険分野についても同様に市場占有率は約 44.2%となっている。（2019 年３月末、主要損保六社の新種保険分野合計）

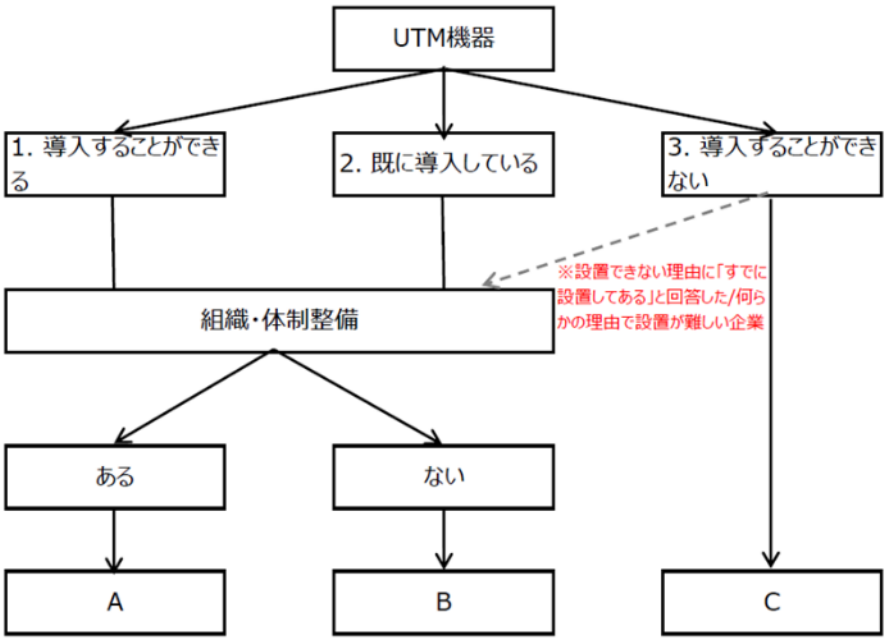
当該地域における No1 損保グループとしての強みを十分に活かしうる、本実証事業を実施するうえでの最適な環境と考え、愛知県を選定した。

※　　主要損保六社…三井住友海上火災保険、あいおいニッセイ同和損害保険、東京海上日動火災保険株式会社、損害保険ジャパン日本興亜株式会社、日新火災海上保険株式会社、共栄火災海上保険株式会社

【図 1】セキュリティ対策レベル（MS&AD インターリスク総研提案書より抜粋）



【図 2】カテゴリー分け基準（MS&AD インターリスク総研作成）



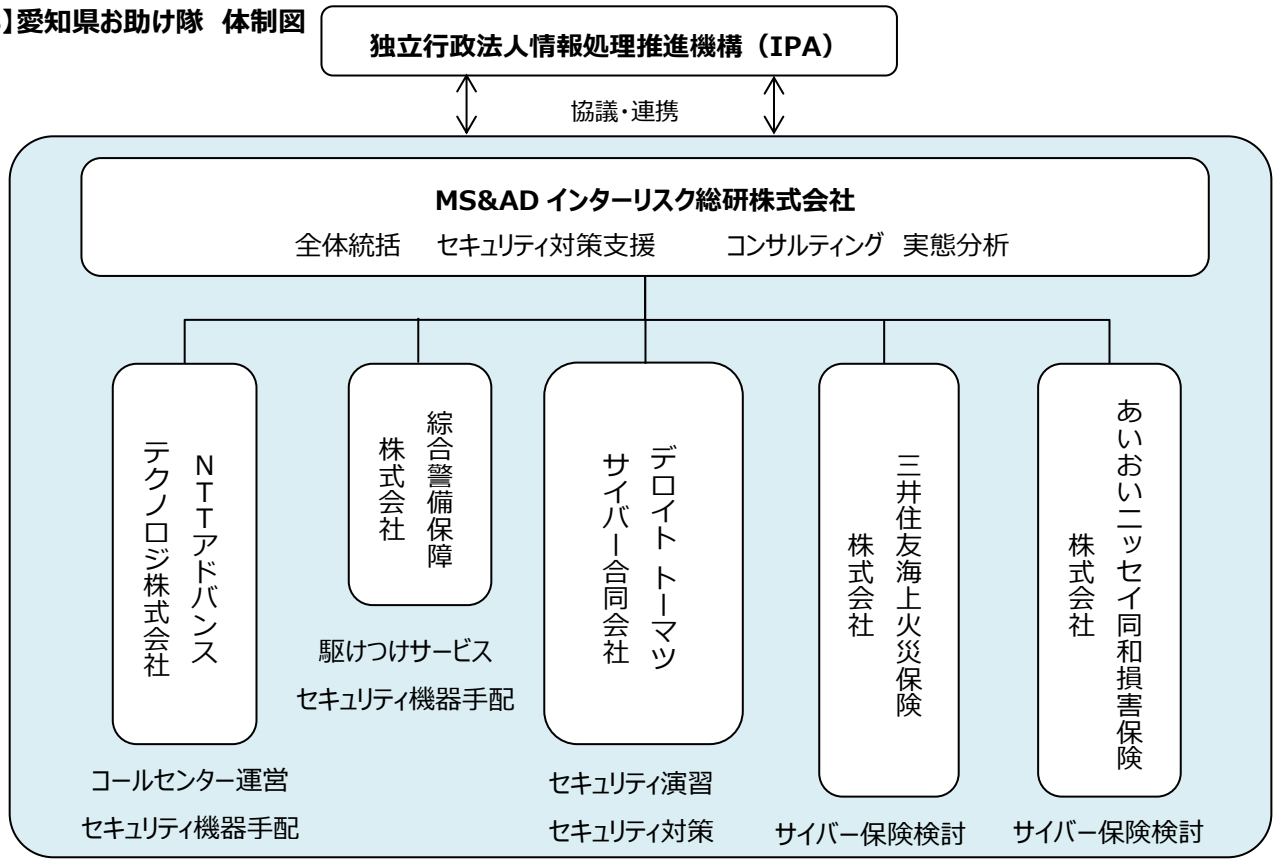
【表 2】カテゴリー・UTM 手配振り分け結果（7 月 24 日 18 時時点）※最終的に辞退した企業を含む

カテゴリー	UTM			
	据置型	クラウド型※「予定」含む	手配なし	手配要否別途確認
A 群	3	10	2	8
B 群	38	81	1	27
C 群	-	-	5	-

（3） **実施体制**

MS&AD インシュアランスグループのシンクタンクである、MS&AD インターリスク総研を主体に、各専門分野についてそれぞれ我が国の有力事業者へ再請負し、一丸となった対応を行った。

【図 3】愛知県お助け隊　体制図



（4） **実施内容と成果物**

【表 3】実施内容と成果物（※提案書の「実施内容・役割分担」の表を一部準用して作成）

実施項目	実施内容	成果物	該当項目
１．１． 事業説明会の開催	募集説明会の開催	・申込み 201 社、正式参加 193 社の集客を実施。 ・計 10 回説明会を開催し、延べ 408 社が参加。 ・SECURITY ACTION 宣言の取得促進、中小企業の情報セキュリティ対策ガイドラインの活用について呼びかけを実施。	Ⅱ.3.(1)
	開始説明会の開催		Ⅱ.3.(2)
	中間報告会・成果報告会の開催		Ⅱ.3.(3) Ⅱ.3.(4)
１．２． 中小企業の実態把握	事前アンケート	・実態調査、意識調査を実施。193 社から回答を受け、分析を実施。	Ⅱ.2
	カテゴリー分け	・レベルに応じて A.B.C 群へ振り分けを実施。	Ⅰ.2.(1) Ⅱ.1 表 6
	UTM 機器の配備	・据置型 UTM とクラウド型 UTM を手配、実態調査を実施。	Ⅱ.1 表 6 Ⅱ.4.(1)～(5)
	セキュリティ体制構築支援	・サイバーセキュリティ体制が整っていない企業を中心に、体制構築のポイントを中心とするセミナーを計 4 回開催。	Ⅱ.5
	セキュリティセミナー	・中間報告会と同時開催。	Ⅱ.3.(3)
１．３． 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	コールセンターの設置	・サイバーセキュリティに関する相談窓口としてコールセンターを設置し、参加企業への相談対応を実施。	Ⅱ.7
	駆けつけ隊の設置	・サイバーセキュリティに関する有事の際の対応を行う駆けつけ隊を設置。計 3 回出動した。	Ⅱ.8
	リモート監視	・据置型 UTM、クラウド型 UTM 設置先のデータを収集。	Ⅱ.4.(3) Ⅱ.4.(4)
１．４． サイバーセキュリティ演習の実施	セキュリティ演習	・A 群、B 群向けに実践的な演習を計 3 回開催。 ・演習フォローアップとして 6 社と対面ヒアリングを実施。	Ⅱ.6.(1) Ⅱ.6.(2)
１．５． 地域実証の実施	継続サービス検討	・実証終了後の継続サービスについて検討を行った。	Ⅱ.4.(3) Ⅱ.4.(4) Ⅲ.3.(1)
	事後アンケート ヒアリング	・事後アンケートは 121 社から回答受け、分析を実施。 ・事後ヒアリングは 5 社と対面ヒアリングを実施。 ・実証事業の効果、中小企業のニーズ把握を行った。	Ⅱ.9 Ⅱ.10
１．６． 実証結果を踏まえた検討の実施 １．７． 成果報告書の作成	サイバー保険の検討	・中小企業が加入しやすいサイバー保険について検討を行った。	Ⅱ.12 Ⅲ.1.(1)～(4)
	実証結果を分析	・各メニューについて実態、課題などについて分析を実施。	–
	あるべきサービス提供の検証	・中小企業にとって必要と考えられるセキュリティ対策サービスの検討を行った。	Ⅲ.2.(1)～(4) Ⅲ.3.(2)
	成果報告書の作成	・成果報告書レビューWG での承認を得た。	–

II. 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結果

今回の事業で実施した事項は以下のとおり。それぞれの項目について実施概要と結果を報告する。

【表 4】実証事業で実施した事項と概要

No	項目	概要	参加数等
1	参加企業の集客	愛知県お助け隊を周知し実証事業参加企業を集客した。	201 社
2	事前アンケート	事前アンケートにより参加する中小企業の実態把握を行った。	回答 193 社
3	説明会の開催	実証事業に関して計 10 回の説明会を開催した。	延べ 408 社
4	UTM 機器の手配	据置型とクラウド型の UTM を手配した。	接続完了 55 社
5	セキュリティ体制構築支援セミナーの開催	サイバーセキュリティ体制が整っていない企業を中心に、体制構築のポイントを中心とするセミナーを計 4 回開催した。	103 社
6	サイバーセキュリティ演習の開催	A 群、B 群向けに実践的な演習を計 3 回開催した。	参加 63 社 ヒアリング 6 社
7	コールセンターの設置	サイバーセキュリティに関する相談窓口としてコールセンターを設置した。	インバウンド 6 社 アウトバウンド 9 社
8	駆けつけ隊の設置	サイバーセキュリティに係る相談・有事の際の対応を行う駆けつけ隊を設置した。	駆けつけ 3 社
9	事後アンケート	実証事業の効果の確認や中小企業のニーズ把握を行った。	回答 121 社
10	事後ヒアリング	参加企業の生の声を確認するため対面ヒアリングを行った。	5 社
11	SECURITY ACTION の普及促進	SECURITY ACTION 宣言の取得促進の呼びかけを行った。	増加 27 社
12	サイバー保険の検討	中小企業が加入しやすいサイバー保険について検討を行った。	–

１．参加企業の集客（募集説明会、その他両損保の営業網など）

提案書に記載のとおり、MS＆AD インシュアランスグループ傘下の三井住友海上火災保険とあいおいニッセイ同和損害保険の愛知県下の営業社員および代理店ネットワークを基軸として、対象となる中小企業に本実証事業への参加呼び込みを行った。

MS&AD インターリスク総研ホームページにお助け隊専用ページを設け、QR コードによる読み込みで遷移できるようにする等、申込み方法を簡素化する工夫を行った。さらに、愛知県お助け隊を広く周知をするため、愛知県の中小企業に関連するメディアや行政、商工会議所等の協力を得て、下記対応を実施した。

- 中部経済産業局のメールマガジン配信
- 中部経済産業局記者クラブへのチラシ投げ込み
- 名古屋商工会議所会員へのメール周知
- 名古屋経済記者クラブへのチラシ投げ込み
- 愛知県庁中小企業部からのメールマガジン配信
- 中部経済新聞、中日新聞への記事掲載依頼
- テレビ局（テレビ愛知、東海テレビ、名古屋テレビ放送、CBC テレビ、中京テレビ、NHK 名古屋）への取材依頼　等
- その他（地元の有力企業、サプライチェーン上流企業）の紹介　等

しかし、これらの周知手段を通じて申込みがあったのは少数派であり、あまり効果はみられなかった。

下表５のとおり、大半が三井住友海上火災保険およびあいおいニッセイ同和損害保険の愛知県下の営業社員および代理店ネットワークによる集客により呼び込んだものである。結果、201 社より web 申込みを受け、うち 193 社から事前アンケートの提出を受け、十分な集客をすることができた。最終的なカテゴリー・UTM 手配振り分け結果を下表６に示す。

【表 5】実証事業紹介ルート

No	紹介ルート	正式参加企業数 （事前アンケート提出済企業のみ）
1	あいおいニッセイ同和損害保険からの紹介	91 社
2	三井住友海上火災保険からの紹介	84 社
3	MS&AD インターリスク総研からの紹介	4 社
4	独立行政法人情報処理推進機構からの案内	4 社
5	経済産業省からの案内	3 社
6	地元有力企業・サプライチェーン上流企業からの紹介	2 社
7	愛知県庁からの案内	1 社
8	小牧商工会議所の HP	1 社
9	その他（得意先からの案内、募集説明会に参加など）	3 社
計		193 社

【表 6】カテゴリー・UTM 振り分け結果

No	実証事業参加状況	企業数	備考
1	正式申込企業数（web 申込完了企業数）	201 社	
2	事前アンケート提出済み企業数	193 社	ア
3	実証事業辞退企業数	12 社	イ
4	（実証終了時）参加企業数	181 社	ア－イ

No	カテゴリー	企業数	UTM 手配状況	企業数
1	A 群	25 社	現行利用・手配なし	18 社
			据置型 UTM	1 社
			クラウド型 UTM	6 社
2	B 群	149 社	現行利用・手配なし	79 社
			据置型 UTM	28 社
			クラウド型 UTM	42 社
3	C 群	7 社	現行利用・手配なし	7 社
合計		181 社	合計	181 社

２．事前アンケートによる実態把握

参加申込みと並行して、事前アンケートにより参加する中小企業の実態把握を行った。

設問は大きく分けて下記の５つに分類される。愛知県お助け隊の参加企業の実態として、最終的には193社から回答を得ることができた。

- IT 化の状況調査（PC 台数含む）
- サイバーセキュリティ体制の現状把握（組織体制、文書など）
- 過去サイバーセキュリティに関する事故発生状況調査
- サイバー保険に関する意識調査
- UTM 機器設置に関する情報調査

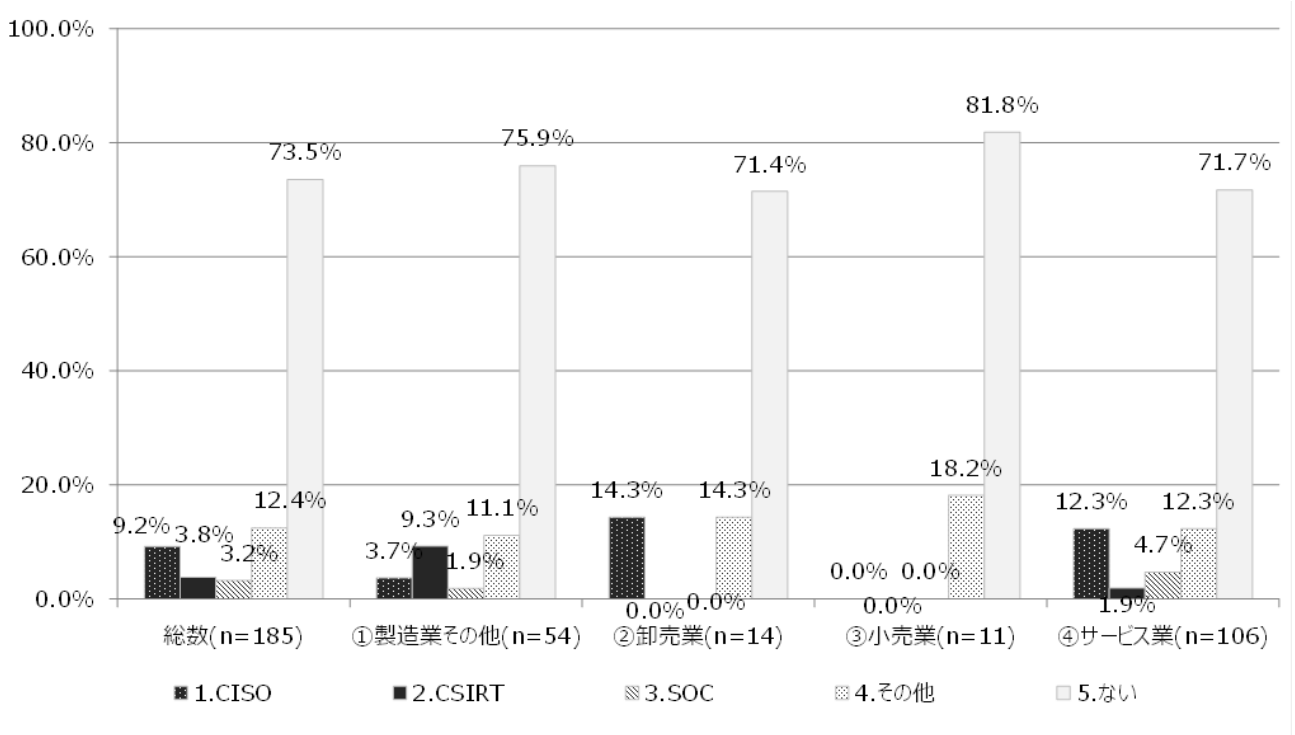
なお前述（Ⅰ．２（２））のとおり、事前アンケートの回答に基づき、カテゴリー分け・UTM 配備振り分けを行った。

本アンケートにより判明したアンケート結果の概略は以下のとおり。

- 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
- 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
- 最も被害が大きかったサイバーセキュリティに関する事故としては、マルウェアが挙げられた（37.5%）
- サイバー保険に加入済の企業は少なく（11.8%）、保険に加入していない理由（複数選択可能）としては「保険があることを知らなかった」という理由が最も多く（33.8）、「保険料が高い」という理由は最下位であった（13.8%）

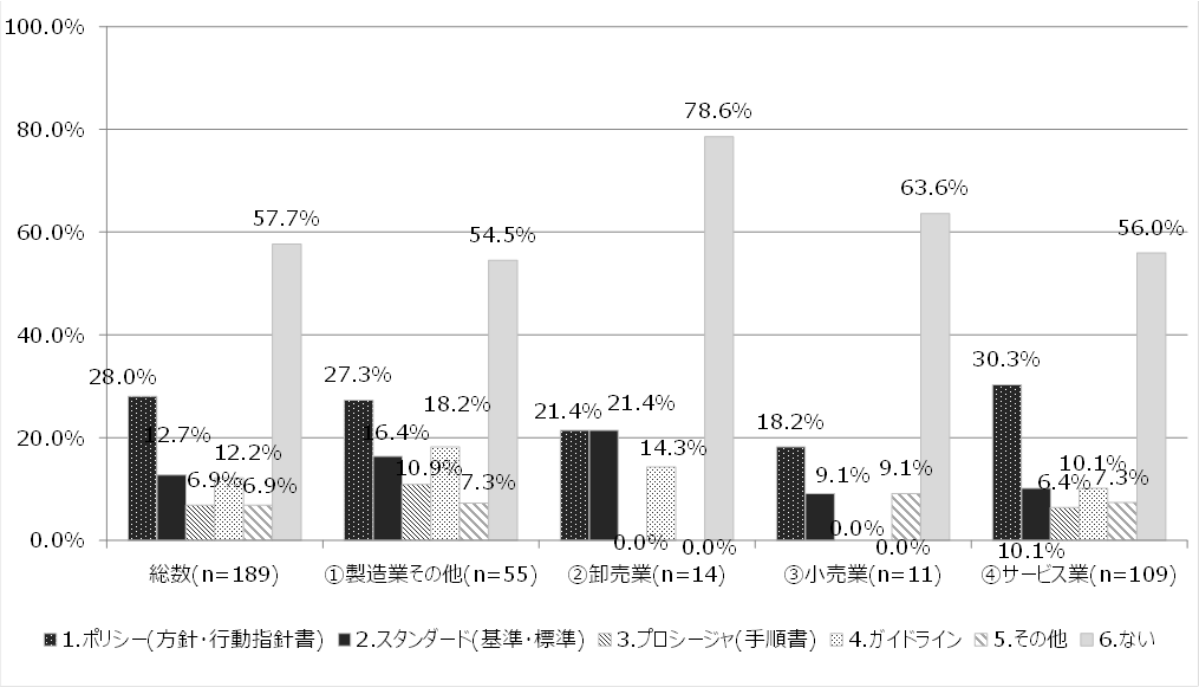
１）　設置されているサイバーセキュリティ体制に関する設問

【グラフ 1】 業種別　設置されているサイバーセキュリティ体制



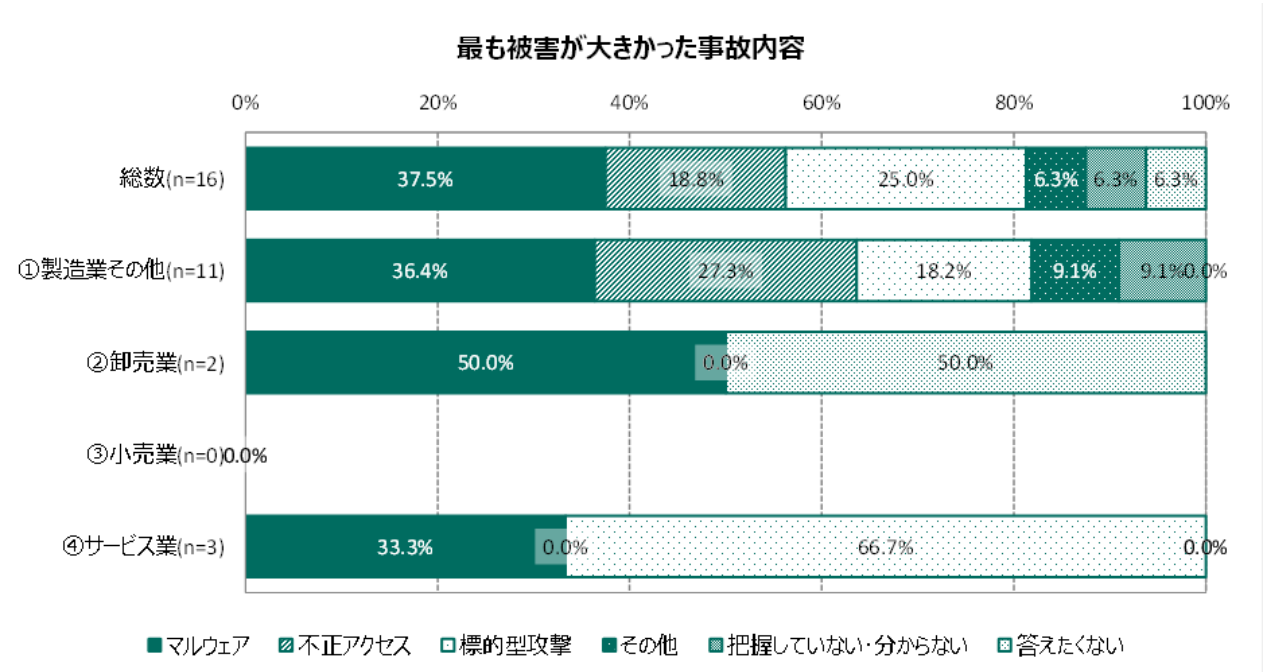
２）　整備されているセキュリティに関する文書・規程に関する設問

【グラフ 2】 業種別　整備されているセキュリティ文書・規程



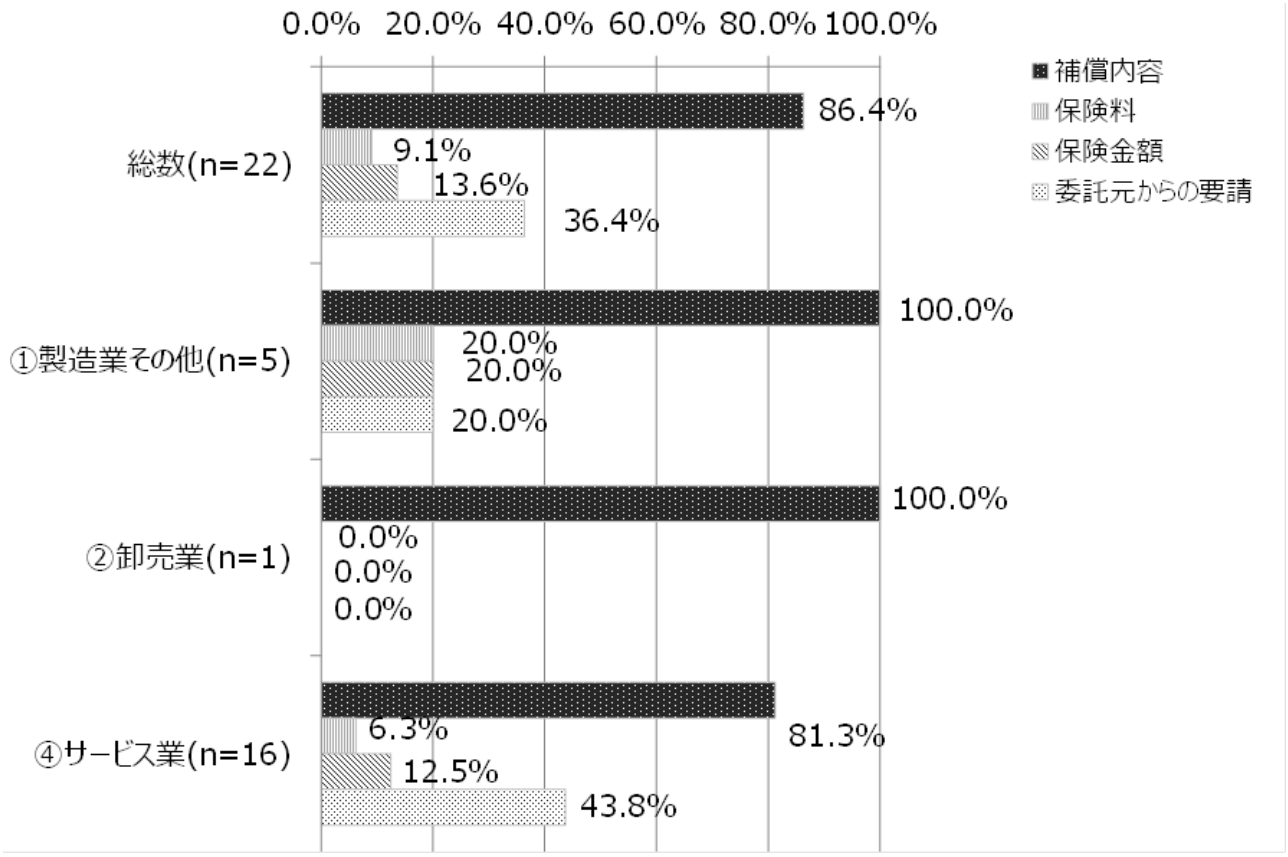
３）　過去にサイバーセキュリティに関する事故が発生した企業のうち、最も被害が大きかったサイバーセキュリティに関する事故に関する質問

【グラフ 3】 業種別　過去のサイバーセキュリティ事故



４）　サイバー保険への加入の決め手に関する質問

【グラフ４】 業種別　サイバー保険加入の決め手



３．説明会

（１） 募集説明会

実証事業への参加呼び込みのため、募集説明会を４回開催した。実証事業の概要と申込方法をわかりやすく解説し、呼び込みを行った。下表７とは別に非公式ではあるが、三井住友海上火災保険とあいおいニッセイ同和損害保険の営業社員や代理店および対象となる企業向けに、名古屋地区、豊橋地区、岡崎地区にて説明会を開催し、呼び込みを行った。

【プログラム】

「中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について」 経済産業省/独立行政法人情報処理推進機構（以下「IPA」という。）

「愛知県お助け隊の概要と参加申込方法について」 MS&AD インターリスク総研

「据置型 UTM 機器について」 NTT アドバンステクノロジ株式会社（以下「NTT アドバンステクノロジ」という。）

「クラウド型 UTM 機器について」 （綜合警備保障株式会社）（以下「ALSOK」という。）

【表 7】募集説明会概要

No	日時	会場	参加社数
1	2019 年 6 月 19 日（水）10:30～12:30	TKP ガーデンシティ PREMIUM 名古屋ルーセントタワー	136 社
2	2019 年 6 月 19 日（水）14:00～16:00		
3	2019 年 6 月 24 日（月）10:30～12:30		
4	2019 年 6 月 24 日（月）14:00～16:00		

（２） 開始説明会

開始説明会を開催。実証事業のキックオフミーティングの位置づけとして、お助け隊で提供するメニュー、参加規約を案内。全体のスケジュールを示し、お助け隊の全体像を説明した。

事前アンケート結果に基づき、開始説明会前に参加企業にメールにて通知を行っていたが、カテゴリーおよび UTM 手配を把握していない企業が多く、改めて案内。後日資料やカテゴリーを全企業に再度書面で通知を行った。

SECURITY ACTION 自己宣言を呼びかけた。

【プログラム】

「中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について」 IPA

「愛知県お助け隊　実証事業開始にあたって」 MS&AD インターリスク総研、NTT アドバンステクノロジ、ALSOK、デロイトトーマツサイバー合同会社（以下「デロイトトーマツサイバー」という。）

「サイバーセキュリティに関する最新動向」 MS&AD インターリスク総研

【表 8】開始説明会概要

No	日時	会場	参加社数
1	2019 年 7 月 25 日（木）10:30～12:30	TKP ガーデンシティ PREMIUM 名駅西口	127 社
2	2019 年 7 月 25 日（木）14:00～16:00		

（３） 中間報告会

事前アンケートの取りまとめ結果の報告。参加企業数やカテゴリー分けの状況、UTM 手配状況報告。実証事業で発生したインシデントやコールセンター対応事例の報告を行った。サイバーセキュリティセミナーとしてサイバーセキュリティに関する最新情報共有のパートを設けた。

SECURITY ACTION のチラシを配布し、自己宣言を呼びかけた。欠席した全企業に対しても SECURITY ACTION のチラシを送付し、自己宣言を呼びかけた。「セキュリティマネジメント指導事業」や「中小企業の情報セキュリティ対策ガイドライン」の活用についても呼びかけた。

【プログラム】

「お助け隊実証事業（愛知県）中間報告」 MS&AD インターリスク総研、NTT アドバンステクノロジ、ALSOK、デロイトトーマツサイバー

「サイバーセキュリティセミナー」 MS&AD インターリスク総研

「中小企業における情報セキュリティ対策支援のご紹介」 IPA

【表 9】中間説明会概要

No	日時	会場	参加社数
1	2019 年 10 月 16 日（水）10:30～12:30	TKP ガーデンシティ PREMIUM 名駅西口	72 社
2	2019 年 10 月 16 日（水）14:00～16:00		

（4） **成果報告会**

実証事業の総括として事後アンケート結果、事後ヒアリング結果を中心に、実証事業で得られたデータや UTM 検知事例、駆けつけ事例を紹介。実証事業を通じて MS&AD インターリスク総研含むコンソーシアムで検討した中小企業向けサイバーセキュリティサービスや保険のあるべき形について報告を実施。UTM を導入した企業向けに継続・返却方法を案内した。

SECURITY ACTION のチラシ、および「中小企業の情報セキュリティ対策ガイドライン」を配布し活用を呼びかけた。

【プログラム】

「中小企業における情報セキュリティ対策支援のご紹介」 経済産業省/ IPA

「愛知県お助け隊　事業成果報告」 MS&AD インターリスク総研

「愛知県お助け隊　事業成果報告、継続サービスのご案内」 NTT アドバンステクノロジ、ALSOK、デロイトトーマツサイバー

「サイバー犯罪の情勢と対策」 愛知県警察本部

「その他サービスのご案内」

「よろず相談」MS&AD インターリスク総研

【表 10】成果報告会概要

No	日時	会場	参加社数
1	2020 年 1 月 15 日（水）13:00～17:00	TKP ガーデンシティ PREMIUM 名古屋ルーセントタワー	73 社
2	2020 年 1 月 16 日（木）13:00～17:00		

４．UTM 機器の配備等による中小企業の実態把握結果

（１） UTM 手配可否の事前確認（事前アンケートによる振り分け）

前述のとおり、事前アンケートにおいて、本実証事業で UTM を導入するにあたり、「PC 台数」「UTM 導入可否」「据置型 UTM 設置可否」「クラウド UTM 導入可否」に関する質問を行い、回答に従って据置型 UTM とクラウド型 UTM の振り分けを行った。詳細は後述する。

（２） UTM 配備について

据置型 UTM とクラウド型 UTM の 2 種類を用意し、事前アンケートの回答結果に従って手配を進めた。

当初の振り分け後、実際に導入するにあたり、「既に UTM 導入済みであることが判明」、「既存システム・ネットワークへの影響の懸念」等により、UTM 導入を断念するケースが発生した。

当初配備予定 148 社に対し、実証期間内に接続完了に至ったのは 55 社であった。

接続完了に至った企業の大半が電話支援・現地支援のいずれか、もしくは両方の支援を受けながら接続完了に至っており、「支援なしで接続完了に至った企業」はわずか 3 社である。

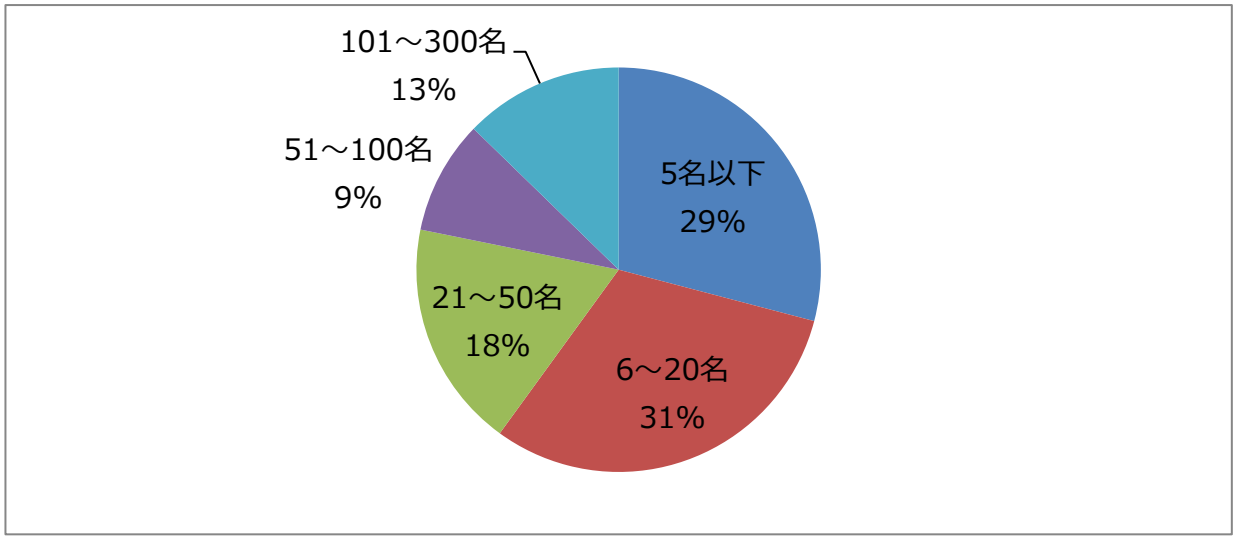
UTM 手配に関する諸課題については、それぞれ据置型 UTM とクラウド型 UTM のパートで詳述する。

【表 11】UTM 配備について※最終的に辞退した企業を含む

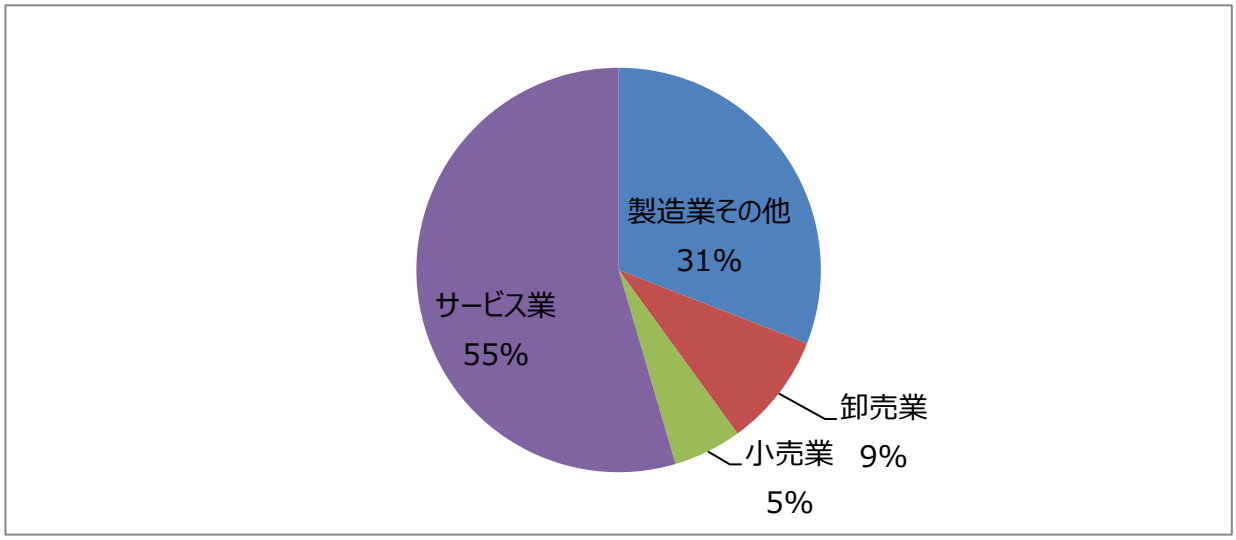
※下記は一社が複数に該当するケース（例：設置支援を実施し、既設 UTM が判明した結果、実証事業を辞退した企業）等が含まれる。

	当初配備予定	接続完了（実証終了時）
据置型	48 社	27社
	（うち実証事業辞退 3 社）	
	（うち設置支援を要した企業 36 社）	
	（うちネットワーク構成等の問題により設置断念した企業 8 社）	
	（うち既設 UTM が判明し設置断念した企業 3 社）	
クラウド型	100 社	28 社
	（うち実証事業辞退 7 社）	
	（うち設置支援を要した企業 46 社）	
	（うちネットワーク構成等の問題により設置断念した企業 13 社）	
	（うち既設 UTM が判明し設置断念した企業 9 社）	
計	148 社	55 社
	（うち実証事業辞退 10 社）	
	（うち設置支援を要した企業 82 社）	
	（うちネットワーク構成等の問題により設置断念した企業 21 社）	
	（うち既設 UTM が判明し設置断念した企業 12 社）	

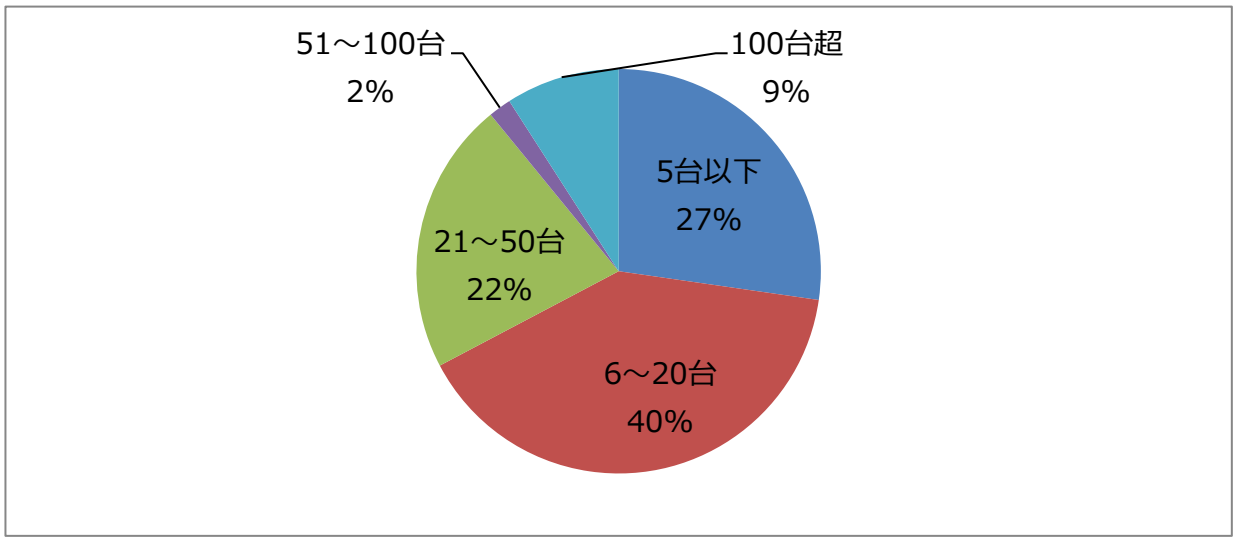
【グラフ 5】 接続完了企業の従業員数別割合（n=55）



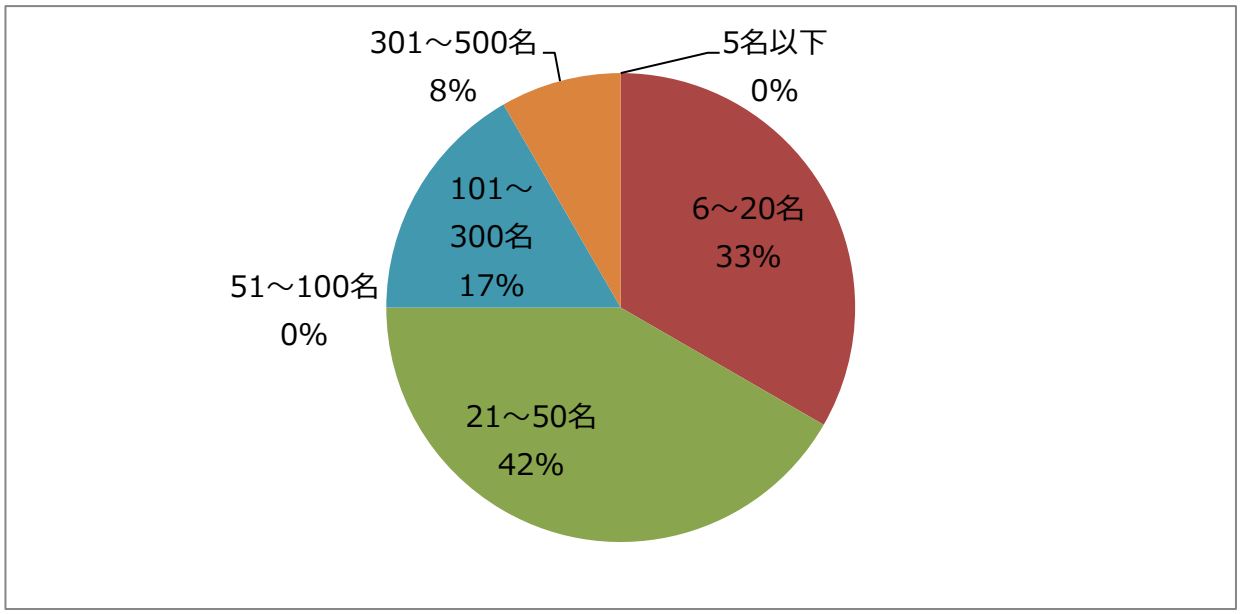
【グラフ 6】 接続完了企業の業種別割合（n=55）



【グラフ 7】 接続完了企業の PC 台数別割合（n=55）



【グラフ 8】 既設 UTM が判明した（既設 UTM の存在を知らなかった）企業の従業員数別割合（n=12）
※既に辞退した企業を含む



（3） **据置型 UTM**

本実証事業では NTT アドバンステクノロジにおいて、据置型 UTM「Sonic Wall TZ300」の手配を実施した。以下に据置型 UTM の概要を説明する。

① 据置型 UTM（Sonic Wall TZ300）の機能概要

【表 12】据置型 UTM の機能

No	仕様・機能	TZ 300
1	保護する PC 同時接続台数の目安	30 台
2	CPU	800MHz (x2)
3	Firewall スループット	750 Mbps
4	Full DPI スループット(すべてのセキュリティ機能を有効化)	100 Mbps
5	最大消費電力	12.0W
6	アンチウイルス/アンチスパイウェア	○
7	不正侵入防御(IPS)	○
8	URL フィルタリング	○
9	アンチスパム	×
10	アプリケーションの制御	○
11	アプリケーションの可視化	○
12	地域 IP フィルタ/ボットネットフィルタ	○

② **据置型 UTM の設置作業**

据置型 UTM を受け取った企業はルータと HUB（または PC）の間に据置型 UTM を挟み込む形で設置する。これにより、据置型 UTM に収容されている各種機器をサイバー空間における様々な脅威から、保護することができる。

【図 4】据置型 UTM 接続イメージ

③ **据置型 UTM 手配の流れ**

(ア) 事前ヒアリングシートの配布（NTT-AT）
(イ) 事前ヒアリングシートの返送（配備対象企業）
(ウ) 据置型 UTM への設定作業（NTT-AT）
(エ) 据置型 UTM を利用企業へ発送（NTT-AT）
(オ) 据置型の受領・設置（配備対象企業）→ 電話およびオンサイト支援（NTT-AT）
(カ) 設置後の接続確認（NTT-AT）

④ 据置型 UTM 手配企業について

据置型 UTM を手配した企業は下表 13 のとおり。（27 社）

【表 13】据置型 UTM 手配企業（※接続完了日順）

No	業種	従業員数	接続完了日
1	サービス業	5 名以下	2019/8/8
2	サービス業	6～20 名	2019/8/9
3	製造業その他	51～100 名	2019/8/19
4	サービス業	6～20 名	2019/8/19
5	製造業その他	21～50 名	2019/8/20
6	製造業その他	51～100 名	2019/8/20
7	サービス業	5 名以下	2019/8/23
8	製造業その他	6～20 名	2019/8/26
9	製造業その他	101～300 名	2019/9/2
10	サービス業	5 名以下	2019/9/2
11	サービス業	5 名以下	2019/9/9
12	製造業その他	21～50 名	2019/9/17
13	サービス業	6～20 名	2019/9/17
14	サービス業	5 名以下	2019/9/24
15	製造業その他	5 名以下	2019/10/3
16	製造業その他	51～100 名	2019/10/3
17	サービス業	6～20 名	2019/10/4
18	サービス業	5 名以下	2019/10/4
19	サービス業	5 名以下	2019/10/7
20	サービス業	6～20 名	2019/10/7
21	小売業	6～20 名	2019/10/7
22	サービス業	21～50 名	2019/10/8
23	小売業	6～20 名	2019/10/9
24	サービス業	6～20 名	2019/10/11
25	サービス業	6～20 名	2019/10/23
26	サービス業	6～20 名	2019/12/17
27	サービス業	5 名以下	2020/1/14

据置型 UTM 手配企業の設置台数遷移は下表 14 のとおり。

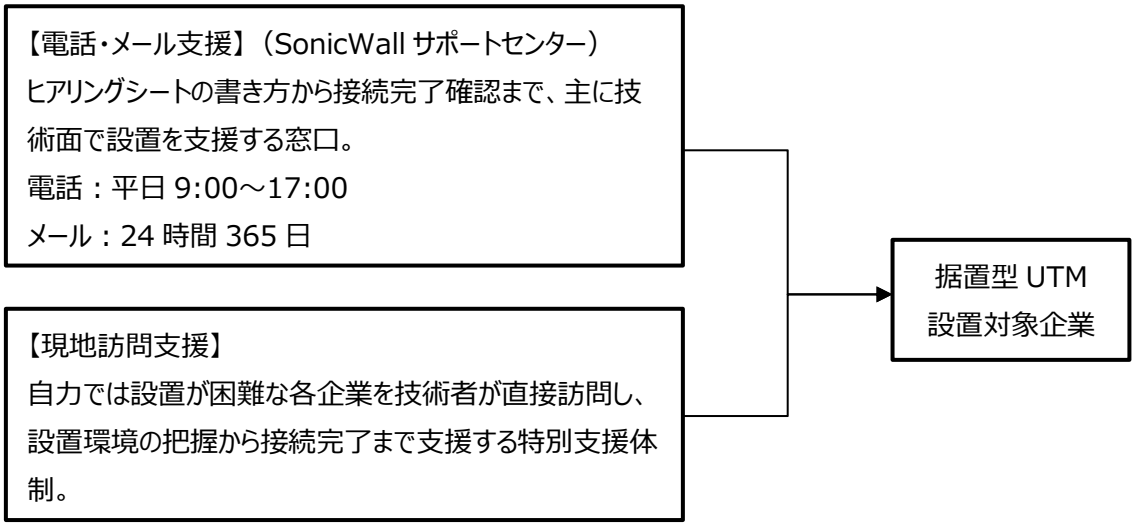
【表 14】据置型 UTM 設置台数推移

据置型 UTM 配備	8 月	9 月	10 月	11 月	12 月	1 月
配備対象	42	42	31	29	29	29
機器発送予定	0	1	0	0	0	0
機器発送済み	12	10	4	3	2	1
接続完了	10	14	24	25	26	27
未完了	20	17	3	1	1	1
導入サポート	41	17	27	3	1	1

⑤ 据置型 UTM 導入のためのサポート体制について

据置型 UTM を対象企業に導入するにあたり、以下の体制でサポートを行った。

【図 5】据置型 UTM サポート体制



⑥　据置型 UTM で検知したデータ

本実証事業の期間中（７月 25 日~1 月 31 日）に、据置型 UTM を配備した企業において検知されたデータについて示す。

【表 15】据置型 UTM で検知したデータ

分類	攻撃種別	小計	合計
外部からの不正アクセス検知（防御含む）	DoS 攻撃	601	18140
	IPS アラート	72	
	ポートスキャン攻撃	14478	
	ポートスキャン攻撃の可能性	2989	
内部からの不正アクセス検知（防御含む）	ポートスキャン攻撃	166	166
マルウェアの検知＆無害化	スパイウェア	255	905
	ウイルス	650	
不正サイトへのアクセスブロック	ボットネット通信	89	89
異常通信ブロック	フラグメンテーション攻撃	1	1

【グラフ 9】 据置 UTM で検知したデータ割合

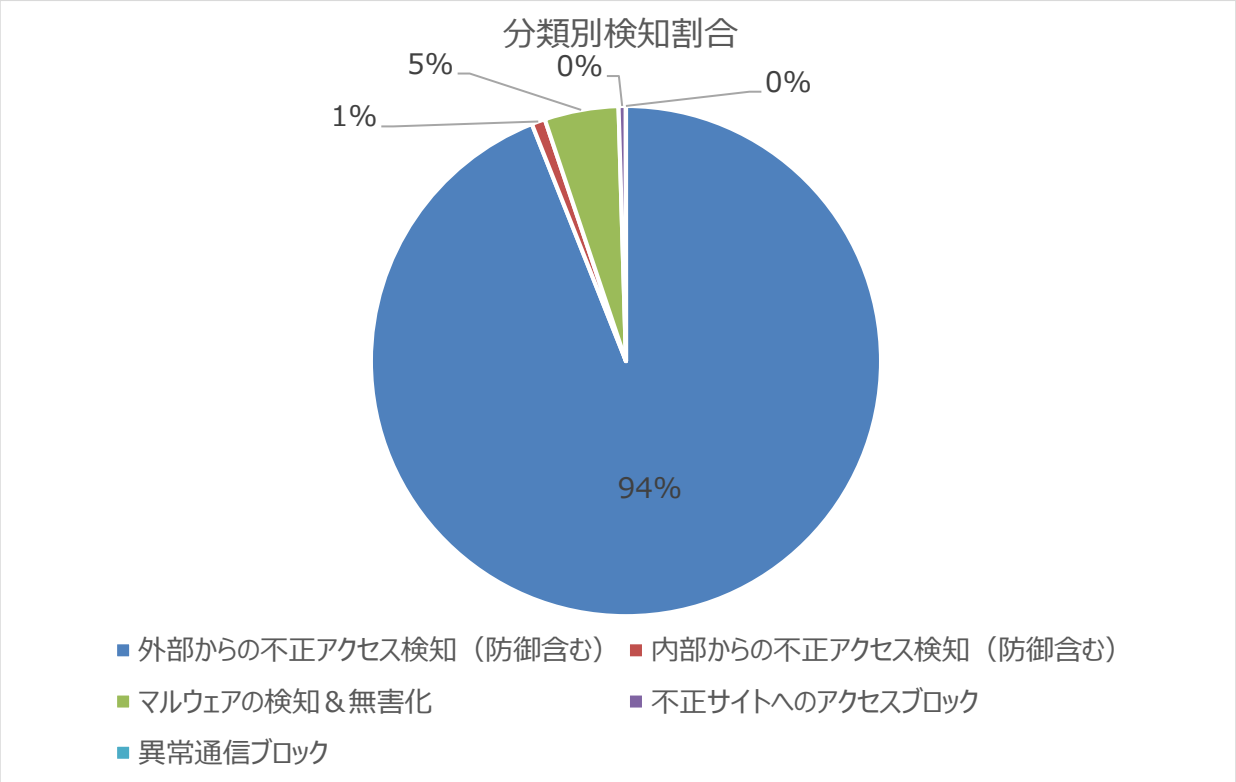


表１５およびグラフ９のとおり、ポートスキャンによる偵察行為（疑いを含む）が検知したアラート全体の９割強を占めた。

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 などを特定された場合、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恐れがある。最新のセキュリティパッチを適用することが経済合理性の観点からも中小企業にとって有効なセキュリティ対策であると考えられる。

⑦ 据置型 UTM 手配に関する諸課題

据置型 UTM 設置を断念したケースには以下のような原因があった。

(ア) 機器の継ぎ足し等により不適切な構成となっている。
(イ) 1 台の PC が有線と無線の両方に接続している。
(ウ) 高所や壁面内に機器や配線が隠蔽されてあり状態を確認できない。
(エ) 担当者自身が構成を把握していない。
(オ) 担当者の認識していない UTM が既に設置してあった。
(カ) 据置型 UTM に関する前提知識がなく、改めて UTM 導入について説明をしても、必要性を感じてもらえなかった。

据置型 UTM の設置に時間がかかったケースには以下のような原因があった。

(ア) ISDN 回線を使っており、光回線への切替まで保留。
(イ) Windows7→10 への入れ替え予定があり保留。
(ウ) 業務繁忙により対応する時間がない。
(エ) 担当者へのコンタクトが困難。

逆に担当者へのコンタクトに問題がなく、一定の知識レベルがあるケースでは導入がスムーズに進んだ。

⑧ UTM 設置に関する必要な人材

据置型 UTM の設置にあたっては、設置担当者が自社のネットワーク構成を把握し、ネットワークの基礎知識（社内 LAN の設定が自力でできるレベル）ならびにセキュリティに関する基礎知識（UTM が持つ機能の概要が理解できるレベル）を備えていることが望ましい。そういった知識が備わっていない場合には、企業のネットワークに合わせて予め設定を施した UTM 機器および設置のための詳細な手順書が必須である。

上記条件が揃わない場合には、有識者のオンサイト支援や手厚い電話サポート等のコストがかかり、かつ業務繁忙等によりコンタクトや対応が困難な企業には、さらなる対応コストが積算される。

- 設置対象企業の増減とコストの関係
  - 設置対象企業が増えるとコストも増える項目
    - ✧ 設置／回収サポート（電話およびオンサイト）
  - 設置対象企業が増えてもとコストが変わらないまたは減る項目
    - ✧ 据置型 UTM 本体費用
    - ✧ ライセンス費用
    - ✧ 遠隔監視費用

（4）クラウド型 UTM

本実証事業では ALSOK において、クラウド型 UTM「MRB-Cloud」の手配を実施した。以下にクラウド型 UTM の概要を説明する。

① クラウド型 UTM（MRB-Cloud）の機能概要

MRB-Cloud は、クラウド上にある 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である。以下にクラウド型 UTM の仕様および検知内容をまとめる。

(ア) クラウド型 UTM（MRB-Cloud）の仕様

【表 16】クラウド型 UTM の機能

No	項目	概要
1	製品名	MRB-Cloud
2	開発元	株式会社テクノル
3	脅威データベース	WEBROOT 社の脅威データベースである ”BrightCloud Thread Intelligence®”を使用する。

(イ) クラウド型 UTM の提供機能

【表 17】クラウド型 UTM の提供機能

No	機能	説明
1	ファイアウォール機能	必要な通信を自動的に通すステートフルインスペクションファイアウォール方式を採用しており、お客様による任意のポート開閉などの設定はできない。
2	ウイルスチェック機能	Web 閲覧時およびメール受信時にウイルスチェックを行う。
3	迷惑メール判定機能	メールの送信元サーバの IP アドレスを脅威データベースを基に判定する。迷惑メールと判定した場合、件名に文字列"Virus"を付加する。
4	URL フィルタリング機能	Web サイトのカテゴリーによる制限と独自のスコアによる危険度評価を組み合わせて、閲覧制限を行う。フィルタリングの強度は強・中・低・無の 4 段階から選択可能。
5	IP フィルタリング機能	危険な IP アドレスへのアクセスをブロックする。
6	ふるまい検知機能	Web 閲覧以外の外部向け通信をすべて監視し、危険なサイトへアクセスする通信をブロックする。
7	レポートメール機能	毎週月曜日に 1 週間の稼働レポートを送信する。
8	L2TP 機能	OS 標準搭載の VPN 接続機能を利用して MRB-Cloud に接続することで、出先でのインターネット利用も保護することが可能。

(ウ) アラートおよび監視機能について

クラウド型 UTM は、自動でアラートを発出し利用者に通知する機能を持たない。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可能にしている。週次レポートは、毎週月曜日に登録されたメールアドレスに対して、過去 1 週間分の検知内容を掲載している。以下にレポートメールの例を示す。

【図 6】クラウド型 UTM の週次レポートメール例

株式会社〇〇〇 御中
　　ご担当者 様

　平素MRBｰ cloudをご利用いただきまして、誠にありがとうございます。
先週の稼働状況をお知らせいたします。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
1.ウイルスブロックログ
　ー ウェブ閲覧時 x回
　ー ウイルスメール送受信 x回
　ー 週間合計　　x回

2.URLフィルタブロックログ
　ー 週間合計　　xxx回
　ー ブロックカテゴリTOP5
　　27ギャンブル
　　37有料サイト
　　44不審なサイト
　　15デッドサイト
　　34ゲーム
　ー ブロックPC TOP5
　　1.xxx.xxx.xxx.xxx
　　2. xxx.xxx.xxx.xxx
　　3. xxx.xxx.xxx.xxx
　　4. xxx.xxx.xxx.xxx
　　5. xxx.xxx.xxx.xxx

3.IPフィルタブロックログ
　ー 週間合計　　xxx回
　ー ブロック先IPアドレスTOP5
　　1. xxx.xxx.xxx.xxx
　　2. xxx.xxx.xxx.xxx
　　3. xxx.xxx.xxx.xxx
　　4. xxx.xxx.xxx.xxx
　　5. xxx.xxx.xxx.xxx
　ー ブロックPC TOP5
　　1. xxx.xxx.xxx.xxx
　　2. xxx.xxx.xxx.xxx
　　3. xxx.xxx.xxx.xxx
　　4. xxx.xxx.xxx.xxx
　　5. xxx.xxx.xxx.xxx

4.迷惑メール判定
　ー メール総数　 x通
　ー 迷惑メール判定数 x通

5.HWリソース情報
　ー CPU稼働率80%以上 x回
　ー メモリ利用率80%以上　　x回

各項目の詳細説明については、下記URLの「レポートメールの説明」をご覧ください。
https://www.mrb-security.jp/support/download

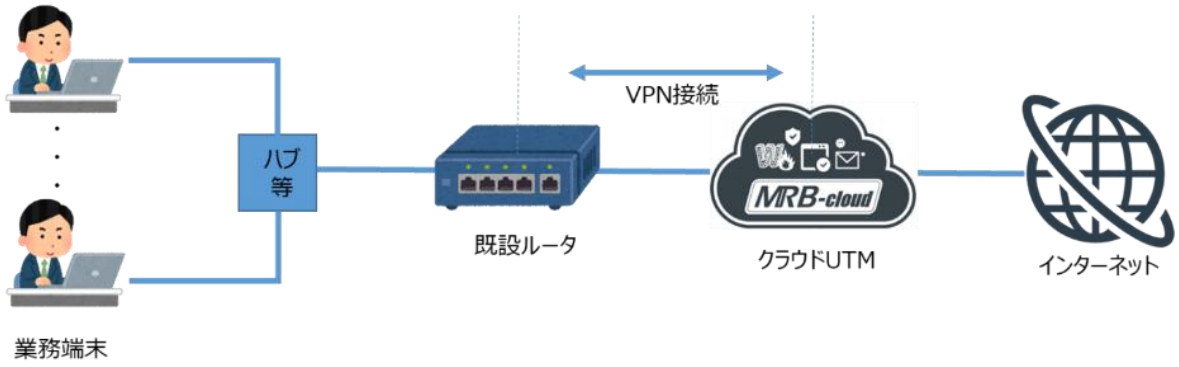
② クラウド型 UTM の接続作業

クラウド型 UTM への接続作業は、参加企業が自ら実施することとした。

(ア) VPN 設定機能を持つルータを使用している企業

VPN 設定機能を持つルータを使用している企業では、既設ルータにクラウド型 UTM に接続するためのコンフィグを追加することで、クラウド型 UTM の利用が可能となる。接続構成例を以下に示す。

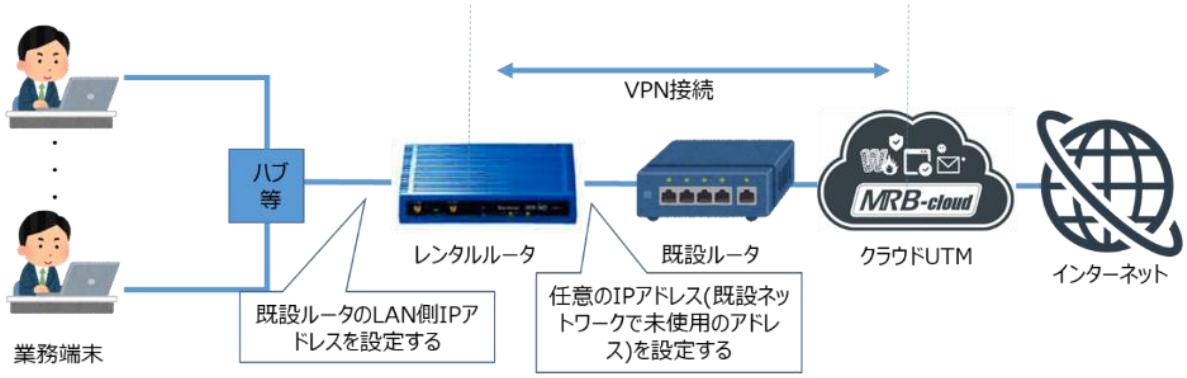
【図 7】クラウド型 UTM への接続構成例（レンタルルータなし）



(イ) VPN 設定機能を持たないルータを使用している企業

VPN 設定機能を持たないルータを使用している企業に対しては、レンタルルータの貸出を実施し、以下の構成で接続することを標準として推奨した。

【図 8】クラウド型 UTM への接続構成例（レンタルルータ有り）



レンタルルータを既設ルータの下部（LAN 側）に接続することとし、レンタルルータの LAN 側ポートに既設ルータの LAN 側 IP アドレスを設定し、既設ルータの LAN 側ポートの IP アドレスを任意の IP アドレスに変更する。各業務端末のデフォルトゲートウェイ等ネットワーク設定の変更を発生させないため、これを推奨設定とした。

③ クラウド型 UTM 手配の流れ

クラウド型 UTM の手配は、以下の手順で実施した。

(ア) クラウド型 UTM の手配において必要な項目を記載する「MRB-Cloud 登録申請書」を配備対象企業に対して送付（ALSOK）

(イ) 「MRB-Cloud 登録申請書」に必要事項を記載し ALSOK に返送（配備対象企業）

(ウ) 「MRB-Cloud 登録申請書」の記載内容を基にクラウド側に登録作業を実施（ALSOK）

(エ) 登録作業完了後、クラウド型 UTM 利用証を送付。このとき、VPN 設定のできないルータを利用している企業に対して、レンタルルータを発送する。（ALSOK）

(オ) クラウド型 UTM への接続作業（ルータ等の設定変更）を実施（配備対象企業）

- クラウド型 UTM を配備できる企業側の条件

  VPN 設定機能を持つルータを使用、また、その暗号化方式で IKEv2、AES256 に対応していること。

  なお、VPN 設定機能を持たないルータを使用している企業に対しては、クラウド型 UTM に接続するための VPN 設定を事前に入れ込んだレンタルルータの貸出を実施した。

  また、レンタルルータの設置に伴い新規に HUB が必要になる企業で、HUB の用意ができない企業に対しては、HUB の貸出を実施した。

【図 9】クラウド型 UTM レンタルルータ外観

④ クラウド型 UTM 手配企業について

接続完了企業の内訳。本実証事業期間中に 28 社がクラウド型 UTM への接続を完了した。

接続が完了している企業の一覧は下表 18 のとおり。

【表 18】クラウド型 UTM 手配企業（※接続完了日順）

No	業種	従業員数	接続完了日
1	製造業その他	51～100 名	2019/8/30
2	製造業その他	51～100 名	2019/9/18
3	製造業その他	21～50 名	2019/9/18
4	卸売業	21～50 名	2019/9/18
5	卸売業	21～50 名	2019/9/23
6	製造業その他	101～300 名	2019/10/2
7	製造業その他	101～300 名	2019/10/2
8	卸売業	21～50 名	2019/10/2
9	卸売業	21～50 名	2019/10/2
10	サービス業	21～50 名	2019/10/7
11	サービス業	5 名以下	2019/10/11
12	サービス業	5 名以下	2019/10/23
13	サービス業	5 名以下	2019/10/31
14	サービス業	21～50 名	2019/11/5
15	サービス業	5 名以下	2019/11/5
16	サービス業	6～20 名	2019/11/5
17	製造業その他	101～300 名	2019/11/6
18	サービス業	6～20 名	2019/11/11
19	卸売業	6～20 名	2019/11/19
20	サービス業	5 名以下	2019/11/20
21	サービス業	5 名以下	2019/11/20
22	サービス業	6～20 名	2019/11/26
23	製造業その他	101～300 名	2019/11/29
24	製造業その他	5 名以下	2019/11/29
25	サービス業	6～20 名	2019/12/10
26	小売業	101～300 名	2019/12/12
27	サービス業	6～20 名	2019/12/12
28	製造業その他	101～300 名	2019/12/24

クラウド型 UTM の配備状況の推移（企業数、PC 台数）

【表 19】クラウド型 UTM 設置台数推移

クラウド型 UTM 配備	8 月	9 月	10 月	11 月	12 月	1 月
配備対象	88	81	59	49	48	48
レンタルルータ手配	11	26	26	23	23	19
申込書受付	20	12	7	4	4	0
開始案内送付済	14	25	22	10	6	0
接続完了	1	9	13	24	28	28
未完了	53	35	17	11	10	1
現地導入支援回数	0	1	7	22	1	0

⑤ クラウド型 UTM 導入のためのサポート体制について

サポートセンターの活用状況

対応期間　　：7月 25 日~1月 31 日

対応時間　　：平日　09:00~17:00

受けた問合せの件数　　：76 件

クラウド型 UTM 接続のための問い合わせ窓口として ALSOK 情報警備監視センターによる問い合わせ対応を実施した。また、ALSOK のみならず MRB-Cloud の開発元である株式会社テクノルのサポートセンターも活用し、参加企業からの問い合わせに対応した。

・現地設定支援の実施

本実施事業においては、クラウド型 UTM の利用のために発生するネットワーク機器の設定変更等の作業は、すべて参加企業が自身の責任の下、実施する。なお、現地での設定支援を希望する企業には、有償の設定支援プラン（1 回 50,000 円を想定）を用意した。

現地設定支援では、ネットワーク構成の確認、既設ルータの設定変更、レンタルルータの設置、配線のつなぎこみ作業、クラウド型 UTM の接続動作確認を実施した。また、本支援では、既に「MRB-Cloud 登録申請書」を提出済みの企業だけでなく、申請書を未提出の企業 4 社に対しても支援を実施した。

⑥ クラウド型 UTM で検知したデータ

本実証事業の期間中（7月 25 日~1 月 31 日）に、クラウド型 UTM を配備した企業において検知されたデータについて示す。

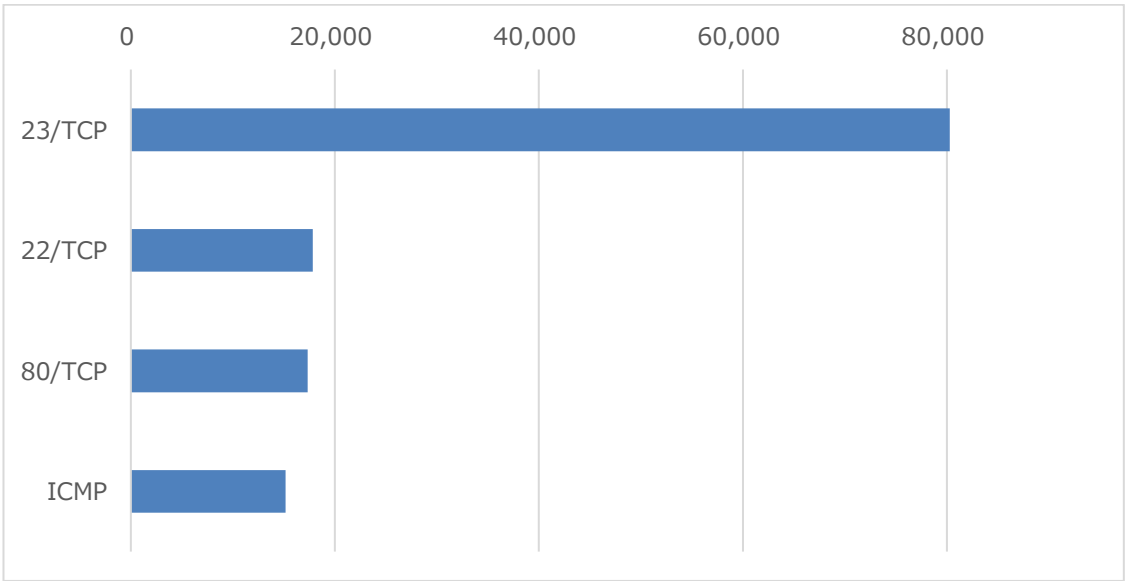
・外部→内部の通信

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偵察活動であった。以下にポート別のスキャン件数を示す。なお、クラウド型 UTM については、UTM の基盤のグローバル IP の検知状況である。

【表 20】クラウド型 UTM で検知したデータ（ポート別のスキャン件数）

No.	ポート番号/プロトコル	検知件数
1	23/TCP	80,268
2	22/TCP	17,832
3	80/TCP	17,345
4	ICMP	15,176
合計		130,621

【グラフ 10】クラウド型 UTM で検知したデータ割合（ポート別のスキャン件数）



実証事業期間中に合計で 130,621 回の不正な通信を検知している。中でも、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。

また、Web サイト閲覧時およびメール受信時のウイルスチェックにおいて検知されたケースは 8 件発生している。

・URL フィルタリング

URL フィルタリングでは、ユーザがフィルタリングの強度を高・中・低・無の 4 段階から任意で選択することができる。各段階でブロックされるカテゴリーの数が異なるほか、WEBROOT 社の” BrightCloud Thread Intelligence®”のスコアとの組み合わせでフィルタリングを行う。

フィルタリングの各強度においてブロックの対象となるカテゴリーを示す。

【表 21】フィルタリング強度「低」のブロックリスト

オークション	マリファナ	フィッシングサイト
ショッピング	ハッキング	プロキシサイト
カルト/オカルト	ゲーム	スパイウェアサイト
ドラッグ/麻薬	武器	ヌード
アダルト/ポルノ	有料サイト	非合法/違法
軍事	狩り/釣り	コンテンツ配信
SNS	グリーティングカード	音声および映像コミュニケーション
デッドサイト	水着/下着	ボットネット
株式/投資	不審なサイト	妊娠中絶
出会い系	人種差別	スパムソース
性教育	オンラインストレージ	動的コンテンツ
宗教	暴力	パークドメイン
個人サイト/ブログ	キーロガー/モニターツール	画像/動画検索
ストリーミング	Web 広告	ファッションと美容
仕事検索	不正行為（盗作など）	レクリエーション
ギャンブル	グロテスク	自動車/バイク
シェアウェア/フリーウェア	Web メール	レピュテーション
P2P	マルウェアサイト	

【表 22】フィルタリング強度「中」のブロックリスト

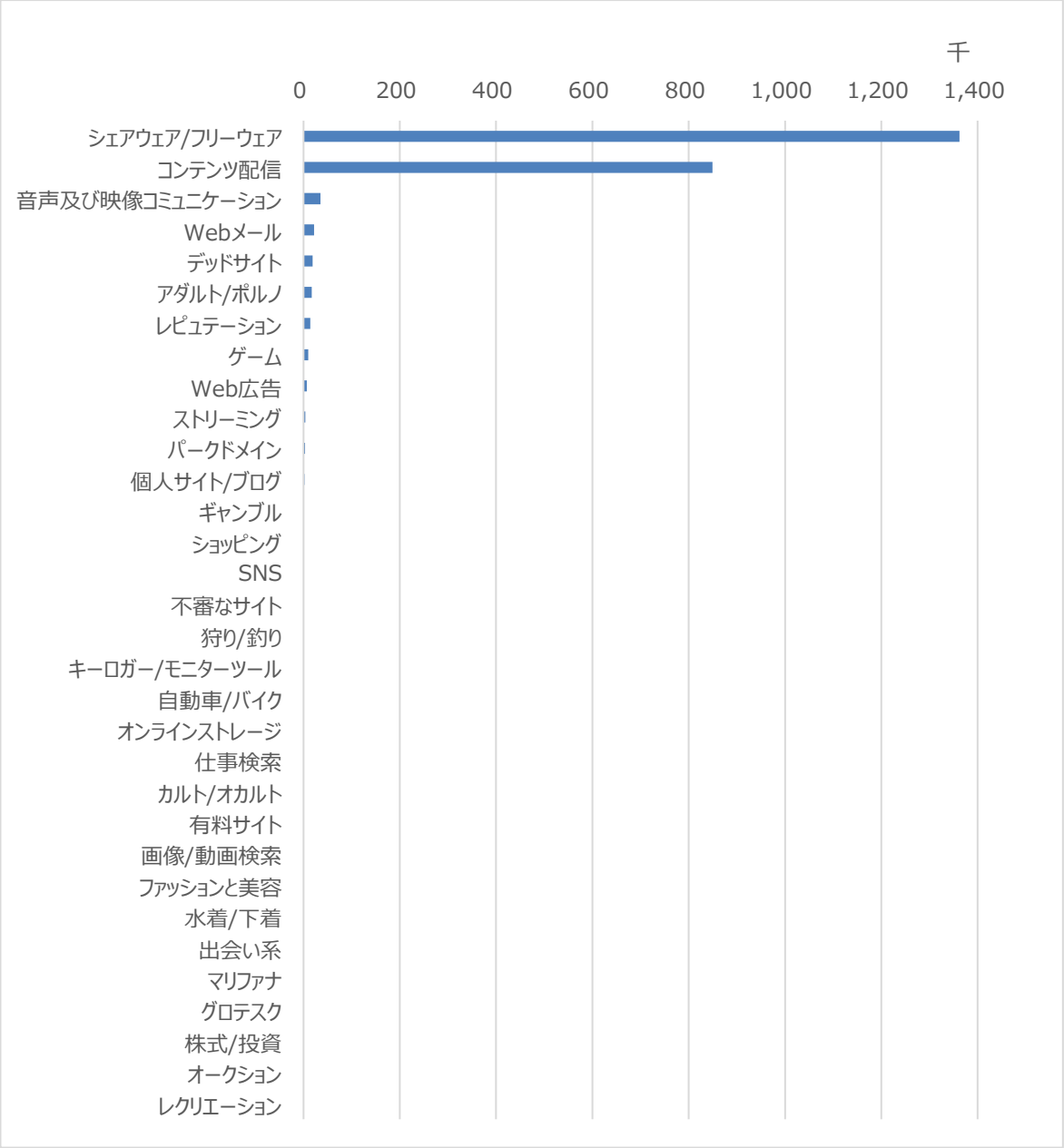
オークション	マリファナ	フィッシングサイト
ショッピング	ハッキング	プロキシサイト
カルト/オカルト	ゲーム	スパイウェアサイト
ドラッグ/麻薬	武器	ヌード
アダルト/ポルノ	有料サイト	非合法/違法
軍事	狩り/釣り	コンテンツ配信
SNS	グリーティングカード	音声および映像コミュニケーション
デッドサイト	水着/下着	ボットネット
株式/投資	不審なサイト	妊娠中絶
出会い系	人種差別	スパムソース
性教育	オンラインストレージ	動的コンテンツ
宗教	暴力	パークドメイン
個人サイト/ブログ	キーロガー/モニターツール	画像/動画検索
ストリーミング	Web 広告	ファッションと美容
仕事検索	不正行為（盗作など）	レクリエーション
ギャンブル	グロテスク	自動車/バイク
シェアウェア/フリーウェア	Web メール	レピュテーション
P2P	マルウェアサイト	

【表 23】フィルタリング強度「高」のブロックリスト

オークション	マリファナ	フィッシングサイト
ショッピング	ハッキング	プロキシサイト
カルト/オカルト	ゲーム	スパイウェアサイト
ドラッグ/麻薬	武器	ヌード
アダルト/ポルノ	有料サイト	非合法/違法
軍事	狩り/釣り	コンテンツ配信
SNS	グリーティングカード	音声および映像コミュニケーション
デッドサイト	水着/下着	ボットネット
株式/投資	不審なサイト	妊娠中絶
出会い系	人種差別	スパムソース
性教育	オンラインストレージ	動的コンテンツ
宗教	暴力	パークドメイン
個人サイト/ブログ	キーロガー/モニターツール	画像/動画検索
ストリーミング	Web 広告	ファッションと美容
仕事検索	不正行為（盗作など）	レクリエーション
ギャンブル	グロテスク	自動車/バイク
シェアウェア/フリーウェア	Web メール	レピュテーション
P2P	マルウェアサイト	

それぞれのカテゴリーにおけるブロック件数は以下のとおり。

【グラフ 11】URL フィルタリング検知状況

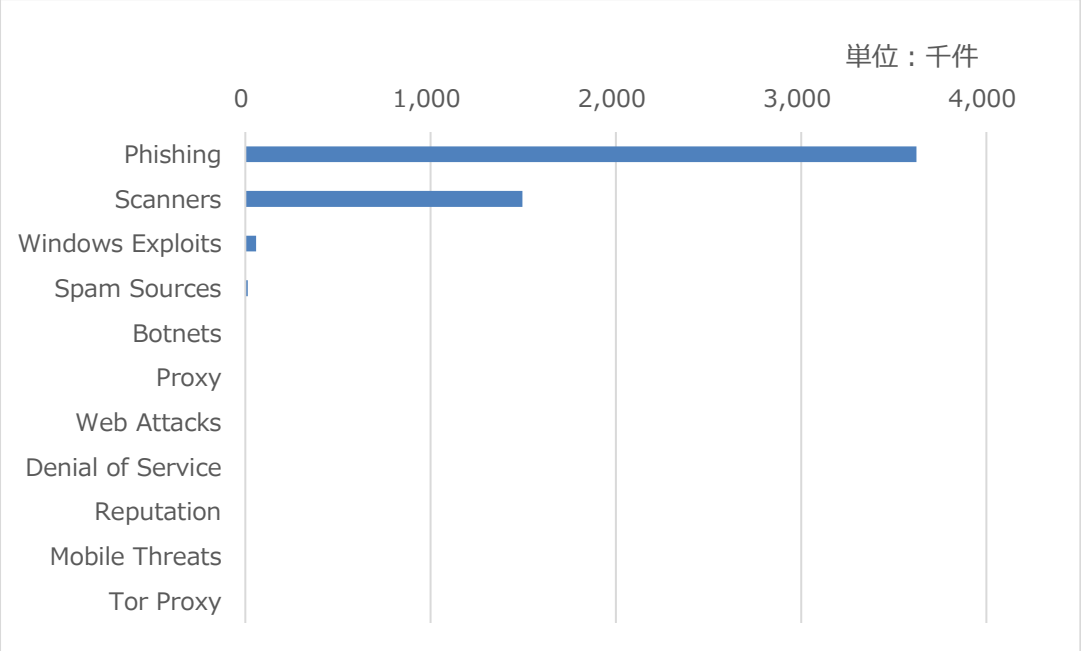


合計で 2,347,474 件のブロックを検知しており、「シェアウェア/フリーウェア」および「コンテンツ配信」のブロック件数が他のカテゴリーと比べて非常に多くなっている。クラウド型 UTM では、Web サイトの中にある広告表示のブロックなどもそれぞれを 1 件とカウントするため、この 2 カテゴリーはサイト内のコンテンツのブロックが嵩んだものと思われる。

・IP フィルタリング

クラウド型 UTM では Web 通信については、Web サイトのカテゴリーでアクセスをブロックする URL フィルタリング他に、IP アドレスをベースとしてブロックをする IP フィルタリングが存在する。以下に実証事業期間中に検知した IP フィルタリングによるブロック件数を示す。

【グラフ 12】IP フィルタリング検知状況



【表 24】IP フィルタリング検知状況

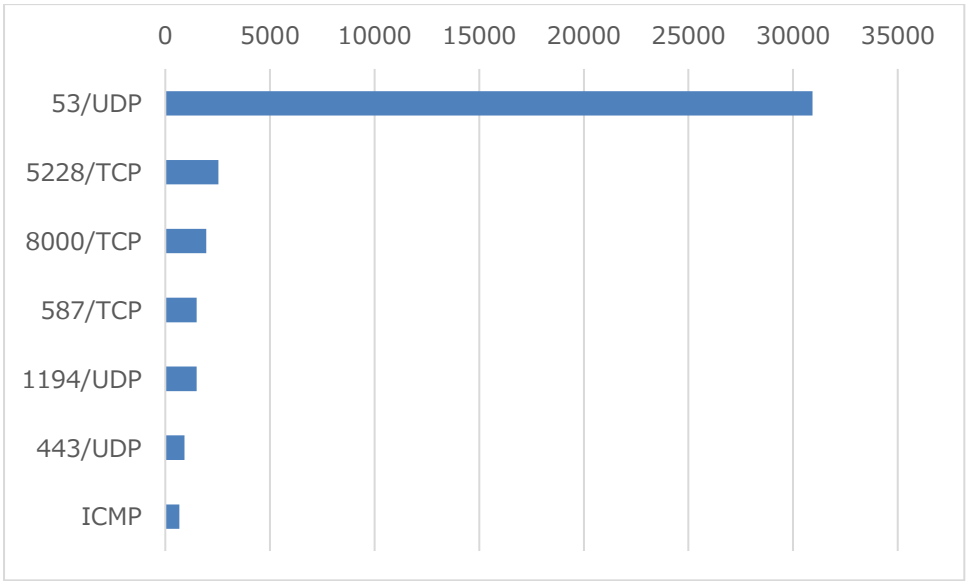
No	種別	検知件数
1	Phishing	3,621,981
2	Scanners	1,495,432
3	Windows Exploits	57,632
4	Spam Sources	13,123
5	Botnets	3,701
6	Proxy	1,921
7	Web Attacks	0
8	Denial of Service	0
9	Reputation	0
10	Mobile Threats	0
11	Tor Proxy	0

Phishing および Scanners に区分される IP アドレスへの通信が他の区分よりも多く検知された。

・振る舞い検知

Web 通信以外の外部への危険な通信のブロックは振る舞い検知としてカウントされる。

【グラフ 13】振る舞い検知状況



UDP53 番ポート（DNS）を使用した通信が最も多く検知された。また、TCP 5228 番ポートを使用した通信も多く検知されている。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。

⑦ クラウド型 UTM 手配に関する諸課題

本実証事業におけるクラウド型 UTM の手配を通して確認された諸課題について以下に述べる。

本実証事業では、クラウド型 UTM 手配予定先 23 社に対して計 33 回の現地支援を実施した。現地支援を実施した企業はすべて保有 PC 台数が 50 台以下の企業であり、「サービス業」が全体の 77%を占めた。現地訪問において確認された状況として、23 社すべてが、ネットワークの保守のために特定のベンダーと契約をしていない状況であった。これに伴い、管理者が自社のネットワーク構成を正しく把握できていないケースがみられた。また、各企業に設置されているルータについて、管理用ログイン ID およびパスワードを管理者が把握していないケースも多く、初期設定のログイン ID とパスワードでログインできてしまう企業が 21 社、パスワードの変更を行っていた企業は 2 社のみであった。

クラウド型 UTM の手配を断念したケースの詳細

クラウド型 UTM の手配について、配備対象は合計で 100 社に及んだが、実証事業からの辞退、UTM 手配なしへの区分変更、据置型 UTM 手配への切替が多数発生し、最終的にクラウド型 UTM の配備対象企業は 48 社となった。UTM 手配なしへの区分変更および据置型 UTM 手配への切替において確認された主なケースの詳細を以下に示す。

(ア) UTM 手配なしに区分変更したケース

・お客様都合によるもの

導入のための社内承認が得られなかった

既にネットワークベンダーと保守契約を締結している企業において、クラウド型 UTM を利用するための機器設定変更作業費の支出について社内承認が得られなかったケースがみられた。また、担当者の独断で実証事業に申込みを行ったが、新たなセキュリティ対策を試行することに対する社内承認を得られなかった、などのケースがみられた。

ネットワーク等の工事を予定しているが実証事業期間中に実施できない見込みとなった

実証事業に参加する以前から社内ネットワークの変更工事を予定し、工事終了後にクラウド型 UTM への接続を計画していたが、都合により工事が延期になり、実証事業期間中に終了の見込みが立たなくなってしまったケースがみられた。また、Windows7 のコンピュータの Windows10 への入替作業の時期と実証事業期間が重複するため、手配なしへの変更を希望するケースも見られた。

・担当者の異動によるもの

事業所が愛知県外を含む複数拠点存在する企業において、ネットワーク担当者が愛知県外に異動してしまったため、UTM 手配を辞退したケースがみられた。

・環境または技術的要因によるもの

使用しているネットワークサービスの仕様によるもの

ネットワーク事業者がサービス提供を行っている閉域網サービスにおいて、その使用によりクラウド型 UTM に対して VPN 設定を個別に設定することができない、というケースがみられた。

IKEv2、AES256 に未対応の VPN ルータを使用して、かつ拠点間 VPN を構築している

VPN 設定機能を持つルータを使用しているが IKEv2、AES256 に未対応の機種を利用中で、かつ拠点間 VPN を利用しているケースがみられた。この場合、レンタルルータを使用することで、既設ルータの LAN 側ポートの IP アドレスが変更になり、VPN が利用できなくなるため、クラウド型 UTM の利用を見送ったケースがみられた。

企業が把握しているネットワーク構成と現地で確認できたネットワーク構成に大きな相違がある

現地支援として訪問したところ、企業側のネットワーク担当者は拠点間 VPN を構築している認識であるものの、目視で確認できる範囲のネットワーク機器には拠点間 VPN の設定の確認がとれず、ルータの設定変更を見送るケースがあった。

VPN 設定機能を持たないルータの無線 LAN に全 PC が接続されている

VPN 設定機能を持たないルータを使用していて、かつそのルータの無線 LAN に事務所内の全業務端末が接続されているケースがみられた。この場合、ルータの下部にレンタルルータを設置しても、レンタルルータを通過する通信が存在しないため、クラウド型 UTM で通信を検知することができない。

UTM が既に設置済みであることが判明した

実証事業への申込み後に、自社のネットワーク構成を再確認したところ、既に UTM が導入されていることが判明したケースがみられた。また、現地支援として訪問のうえネットワーク構成を確認したところ、既に UTM が設置されていることが確認されたケースもみられた。

・物理的環境要因

レンタルルータを貸出企業において、既存のルータが壁掛けかつ高所に設置されており、レンタルルータを設置するスペースが無いケースがあった。

(イ) 据置型 UTM 手配に変更したケース

・企業側の希望によるもの

クラウド型 UTM の利用のためには、既設ルータ等のネットワーク機器の設定変更が必要となるが、既存システムへの影響を考慮し、これらの機器の設定変更を望まない企業があった。これらの企業に対しては、透過モードを搭載している据置型 UTM に手配変更した。

⑧ UTM 設置に関する必要な人材

クラウド型 UTM を利用するためには既設ルータの設定変更が必須となる。本実証期間中に観測された状況から、中小企業では、IP アドレスを変更するといった簡単な設定であっても、実施が難しいことがわかった。企業が利用するルータの種類は様々であり、これを電話によるサポートのみで完結するには多くの時間とコストを要する。これを踏まえて、現地のネットワークベンダーとの連携もしくは自社による現地設定支援体制を構築することが望ましい。

しかしながら、現地支援によりルータの設定変更を行うことで、当該企業のネットワークにおける責任分界点が不明確になり、障害発生時の責任の所在があやふやになることが懸念されることから、現地支援体制を構築する際には、契約内容も含めて、責任分界点の明確化が必要である。

（5） UTM 手配の課題解決策

上記のとおり、本実証事業において、据置型 UTM およびクラウド型 UTM 手配にあたっては想定していたよりも、多くの課題があった。

課題の解決策として下記が挙げられる。

【中小企業側が備えるべき要件】

- UTM 設置担当者が自社のネットワーク構成を把握していること（管理者用 ID、パスワード含む）
- ネットワークの基礎知識（社内 LAN の設定が自力でできるレベル）を備えていること
- セキュリティに関する基礎知識（UTM が持つ機能の概要が理解できるレベル）を備えていること
- 新たなセキュリティ対策（UTM 導入含む）のための社内承認を得ること
- 自社のセキュリティ対策状況を把握していること（既設 UTM の有無の把握含む）
- 自社のネットワーク構成を正しく把握している特定の保守ベンダーと契約していること（外部リソース）
- 追加でセキュリティ対策を導入できるネットワーク構成となっていること（変更できること）
- ルータの所在不明、設定変更が容易でない、等の物理的環境要因をなくすこと

【手配側が備えるべき要件】

- 企業のネットワークに合わせて予め設定を施した UTM 機器および設置のための詳細な手順書
- 有識者によるオンサイト支援（現地設定支援）
- 電話サポート体制（平日 9 時～17 時に限らない体制構築）
- 現地のネットワークベンダーとの連携
- 当該企業のネットワークにおける責任分界点の明確化（障害発生時の責任の所在）

- 様々なネットワーク構成を持つ企業側にとって導入が用意な機器・サービスの開発
- 複数の選択肢の提示

【実証事業においてはやむを得ない事情】

- ネットワーク等の工事等のタイミングが合わなかった
- 担当者の異動によるもの
- 使用しているネットワークサービスの仕様によるもの（据置型、クラウド型とは仕様がアンマッチ）
- 企業側の希望によるもの（既設ネットワーク機器の設定変更による既存システムへの影響を考慮）

5．セキュリティ体制構築支援セミナー

サイバーセキュリティ体制が十分でない（サイバーセキュリティ組織体制が整っていない）B 群および C 群（A 群は任意参加）を対象として、開催。サイバーセキュリティ組織体制を構築することが対策の第一歩であることを解説するためのセミナーを開催。9 割以上が体制構築のきっかけになったと回答、50%以上が SECURITY ACTION を宣言するとの回答を得る極めて満足度の高いセミナーであった。

「SECURITY ACTION 自己宣言」、「セキュリティマネジメント指導事業」、「中小企業の情報セキュリティ対策ガイドライン」の活用について呼びかけた。

【表 25】セキュリティ体制構築支援セミナー概要

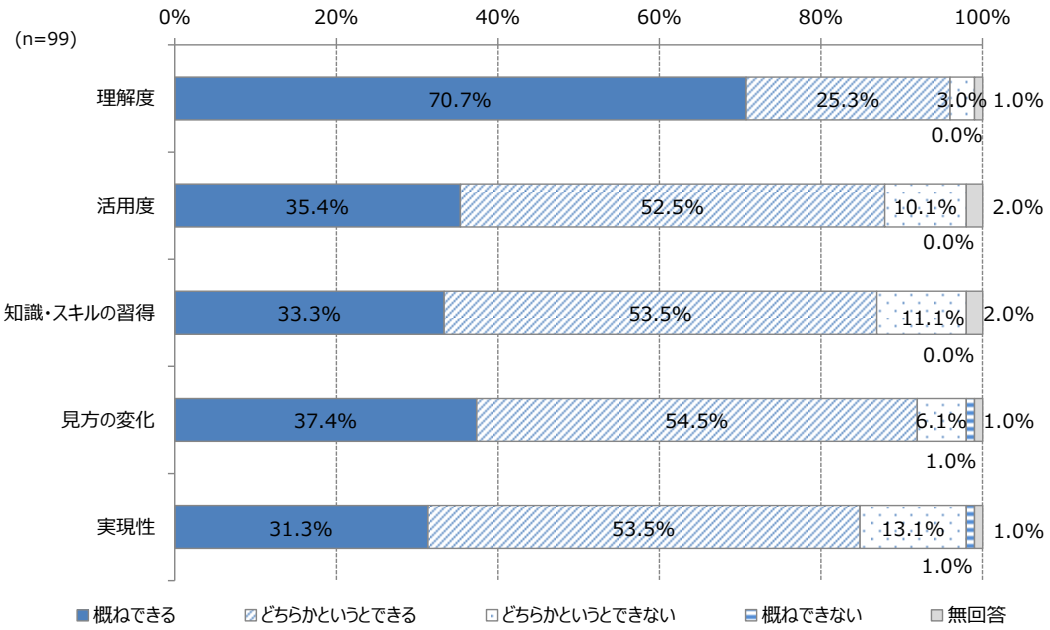
No	日時	会場	参加数
1	2019 年 8 月 28 日(水) 13:30-14:30	TKP ガーデンシティ PREMIUM 名古屋ルーセントタワー	103 社
2	2019 年 8 月 28 日(水) 15:30-16:30		
3	2019 年 8 月 29 日(木) 13:30-14:30		
4	2019 年 8 月 29 日(木) 15:30-16:30		

① 実施結果（アンケート結果）

セミナー終了時に実施したアンケート結果は以下のとおり。

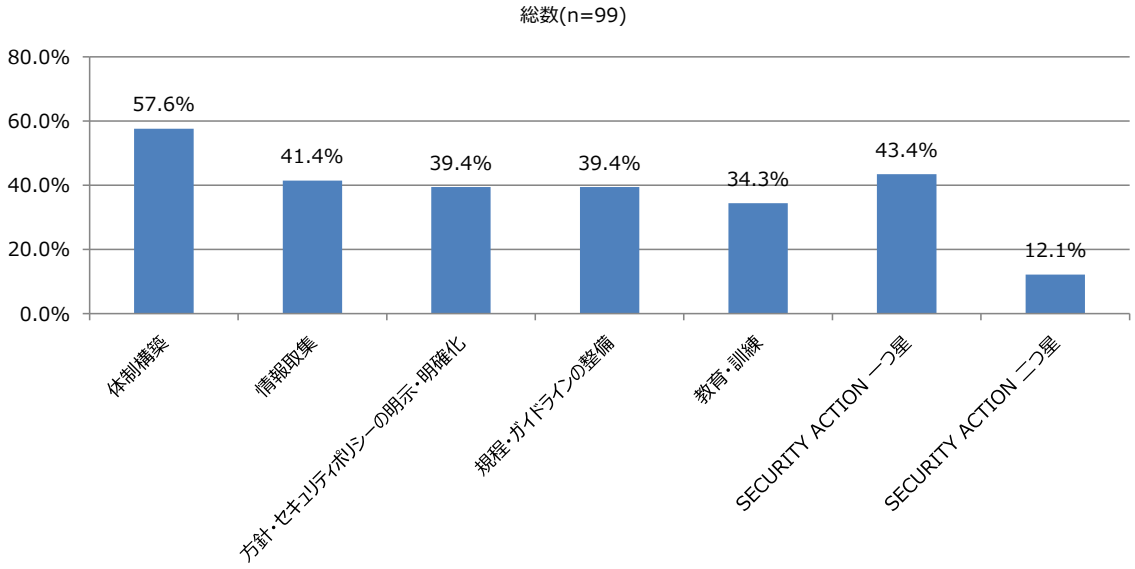
（ア）セミナーに関する事項

【グラフ 14】セミナーに関する事項



（イ）今後活用したい知識やスキル

【グラフ 15】今後活用したい知識やスキルについて



６．サイバーセキュリティ演習の実施結果

各参加企業のサイバーセキュリティ体制およびサイバーセキュリティルール構築の動機付けを目的として演習を実施した。また、参加企業における具体的なサイバーセキュリティ対策状況を把握するために、演習参加企業のうち 6 社に対してヒアリングを実施した。実施内容および結果は以下のとおり。

（１）サイバーセキュリティ演習

①　実施内容

内容　：　【午前】講習(座学式)、【午後】演習(設問回答式)

講師　：　デロイトトーマツサイバー

参加社数(全体)　：　参加 63 社、不参加 113 社

【表 26】サイバーセキュリティ演習概要

No	日時	会場	参加数
1	2019 年 9 月 24 日(火)　10:00-17:00（A 群向け）	TKP ガーデンシティ PREMIUM 名古屋新幹線口	63 社
2	2019 年 10 月 23 日(水)　10:00-17:00（B 群向け）		
3	2019 年 10 月 24 日(木)　10:00-17:00（B 群向け）		

②　設問正答率

午後のサイバー攻撃演習における設問正答率は以下のとおり。

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

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

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

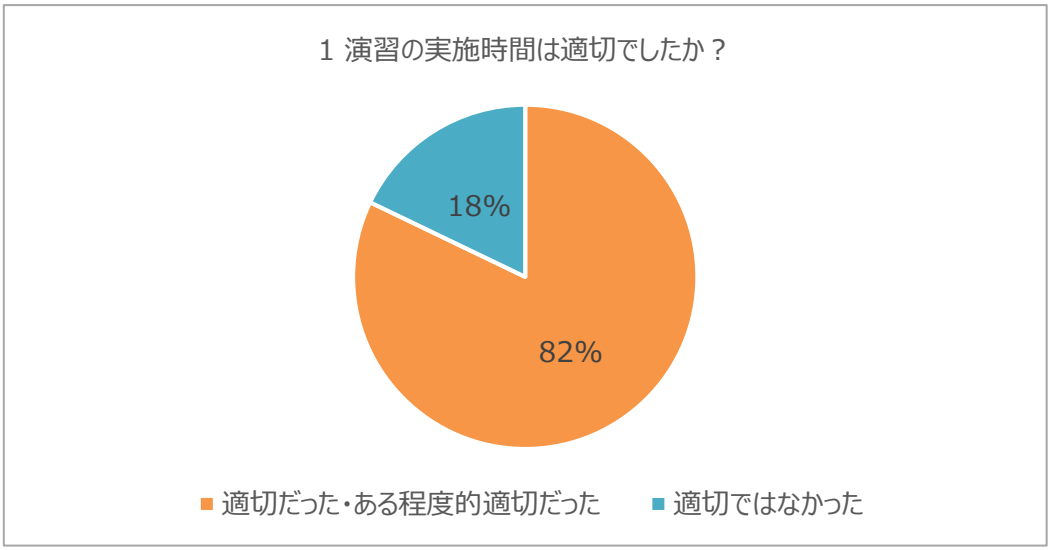
【表 27】サイバーセキュリティ演習　設問正答率

グループ	攻撃シナリオ① 設問数１１	攻撃シナリオ② 設問数 7	攻撃シナリオ③ 設問数 5
A 群(n=6)	82%	86%	83%
B 群(n=55)	78%	85%	75%
全体平均(n=61)	80%	87%	77%

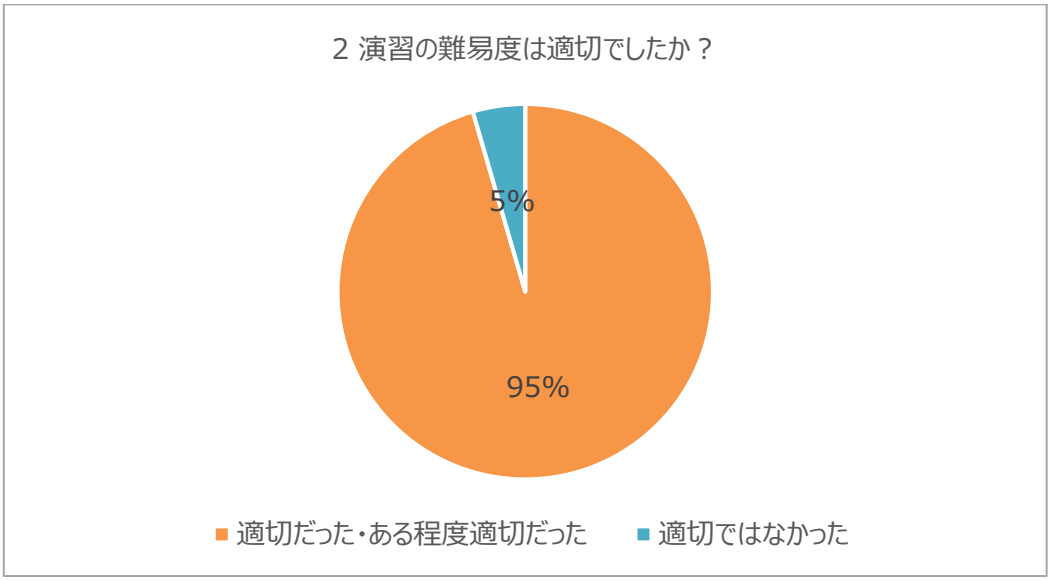
③　アンケート結果

演習後に実施したアンケート結果は以下のとおり。(参加企業のうち 2 社は無回答。)

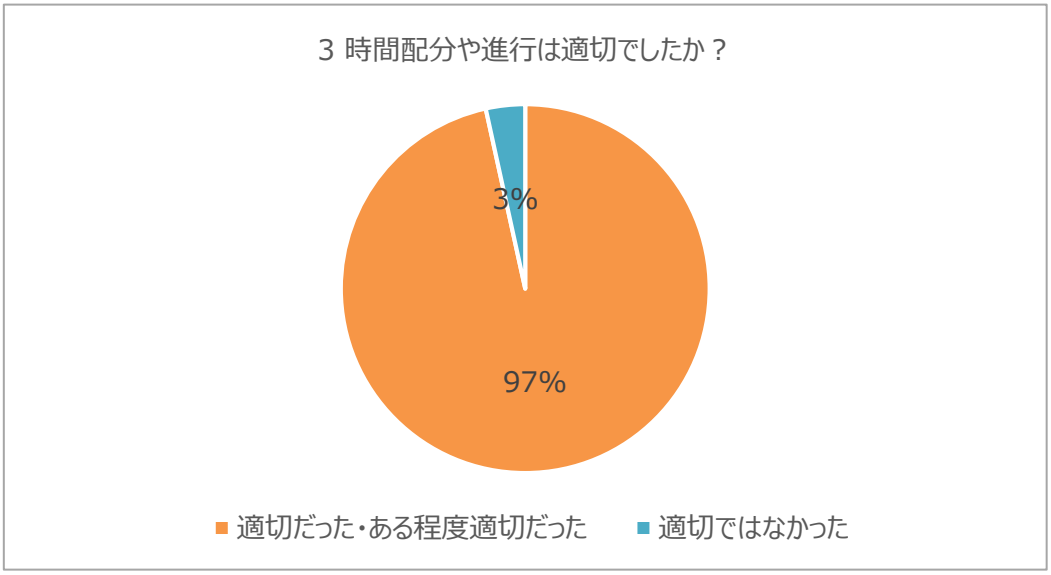
【グラフ 16】演習の実施時間について（n=61）



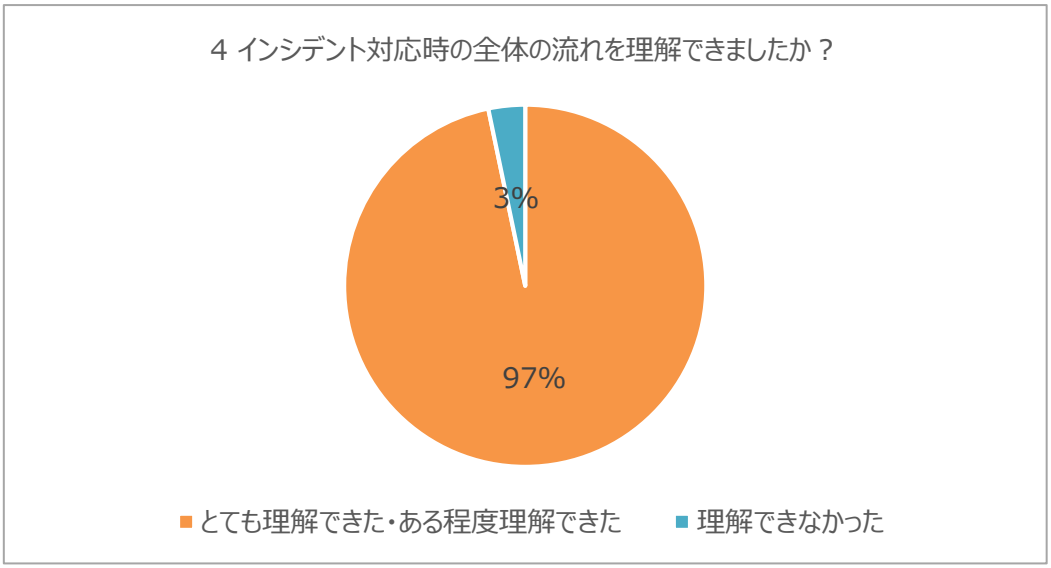
【グラフ 17】演習の難易度について（n=61）



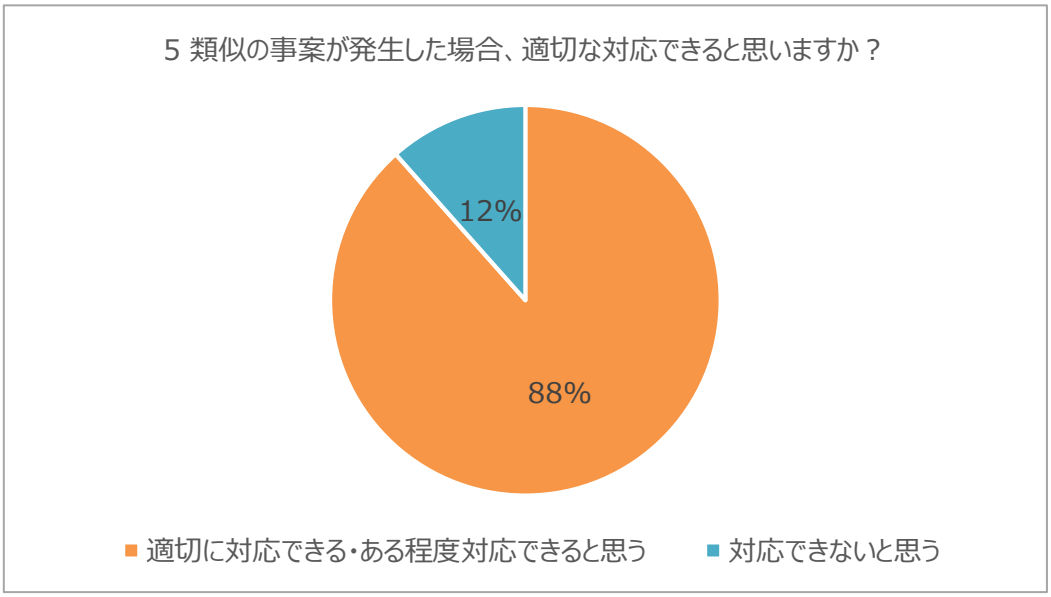
【グラフ 18】演習の時間配分について（n=61）



【グラフ 19】演習の理解度について（n=61）



【グラフ 20】類似事案が発生した場合の対応について（n=61）



④　参加社の声(一部)

演習後アンケートにおける自由記入欄に回答いただいた内容は以下のとおり。

- ９月参加者
  - 冷静な判断を行う必要があると感じた
  - ウイルス等の危険性について、上層部含め、認識不足、整備不足であるため、会社全体で対策をしていかなければいけないと思った
  - 社内での注意喚起、教育が課題と感じた
  - ネットワーク以外の媒体でデータのバックアップを取っておきたいと思った
  - 現在、個人情報の取り扱いについて、誰でも外部に持ち出せる状況になっている点を改善していきたい
  - 専門家、ベンダーとの連携を強化していきたいと思った　等

- 10 月参加者
  - 現在、アクセス権限の整理があいまいになっているため、再構成しなければならないと感じた
  - 経営者がサイバーセキュリティリスクを軽視しているのでいかに参加させるのかが課題であると思った
  - サイバーインシデントに対する自社の準備ができていないことを痛感した
  - AD サーバ、PC ログ収集解析ツールを導入したい
  - 取組体制を見直したいと思う
  - 社内のルール作り、勉強の実施が必要と感じた　等

（2）**演習後フォローアップヒアリング**

①　実施内容

時期：10 月 17 日～11 月 7 日

対象：サイバーセキュリティ演習参加企業のうち 6 社（下表 28）

内容：セキュリティ対策の現状と課題認識、本実証事業に係る意見・要望等

【表 28】サイバーセキュリティ演習　フォローアップヒアリング実施先

No	会社名	業種	従業員数	ヒアリング実施日
1	α社	製造業その他	101～300 名	2019/10/17
2	β社	卸売業	21～50 名	2019/10/28
3	Θ社	卸売業	51～100 名	2019/10/30
4	Δ社	サービス業	6～20 名	2019/10/30
5	E社	製造業その他	21～50 名	2019/11/7
6	Z社	製造業その他	101～300 名	2019/11/7

② セキュリティ対策の現状と課題認識の傾向

【表 29】サイバーセキュリティ演習 フォローアップヒアリングまとめ

大分類	中分類	現状	課題認識
組織/人	現状のセキュリティ体制	・セキュリティ/IT 担当者は一人のみまたは少数である。	・セキュリティ/IT の知見を持ったリソースが存在せず、新たに雇用する予算的余裕がない。 ・セキュリティ対策の持続可能性が低い。(担当者が高齢化しており、後継者がいない)
	経営層の関与・理解度	・経営層が予算承認等で関与はするが、セキュリティ/IT に係る理解度は低い。	・必要な対策について、経営層が判断できない。 ・経営層に対して説明する側の理解度が低いため、訴求力が低い。
ルール/プロセス	セキュリティポリシー/規程の策定状況	・ポリシーは存在するが、文書化された規程は存在しない。	・どの程度の規程を作成する必要があるのか判断できない。 ・規程の展開が行き届かない。 ・規程の運用(改訂)に係るリソースが十分ではない。
	インシデント発生時の対応	・インシデント対応の手順は存在せず、対応が場当たり的になっている。	・対応手順が定められていない。 ・ベンダー相談ができない部分の判断ができない。 ・スピーディな対応ができない場合がある。
技術	講じている技術的対策	・アンチウイルスソフトは導入されている。 ・従業員の PC ログインは管理されていない。	・PC/サーバのアップデートができない。 ・バックアップ媒体が破損したとき、データが消失する可能性がある。 ・社内のネットワークが把握できていない。
	セキュリティ監視状況	・日常的な監視は行っていない。	・監視を行えるリソースが存在しない。 ・ネットワーク構成を把握できていないため、UTM の導入ができない。

③ 本実証事業に係る意見・要望等

- コールセンター/お助け隊に対する意見・要望等
  - お助け隊は 24 時間 365 日の対応ができ、スピーディ(1 時間以内)な対応が可能であれば望ましい。
  - お助け隊が安価で利用可能であれば望ましい。
  - コールセンターに問い合わせ可能な内容を明確に周知してほしい。
  - コールセンター側で個社の状況を把握した方に問い合わせ可能であれば助かる。
  - コールセンターにはベンダーに相談できない内容を相談できれば助かる。

- その他情報セキュリティ全般に係る事項
  - 最低限このレベルまで対策を講じるべき、という基準が欲しい。
  - 個社の状況を把握したうえで、第三者視点でアドバイスを提供できる外部専門家は助かる。(IPA の支援士派遣サービス)
  - 定期的な情報収集の場として、セミナー/ワーキンググループがあれば助かる。

7．コールセンター

① コールセンター概要

【表 30】コールセンター概要

No	項目	内容
1	受付方法	電話およびメール
2	電話番号	0120-xxx-xxx（フリーダイヤル）
3	受付時間	（電話）平日 9:00～17:00（受付時間外はガイダンスによる案内） （メール）24 時間 365 日
4	設置回線数	2 回線
5	実稼働時間	平均 5～10 分/日
6	要員構成	専任 1 名＋補助 1 名
7	コールセンター 対象業務	・サイバーセキュリティに関する相談（コールセンター） ・有事の際の対応受付窓口　等（コールセンター） ・サイバーインシデント等の判断、駆けつけ要否判断等（コントロールセンター） （対象外業務：公序良俗に反する内容、本実証事業の目的にそぐわない内容　等）
8	コールセンター 利用実績	インバウンド　6 件 アウトバウンド　9 件 ※詳細は以下②、③のとおり

※コールセンター（相談受付窓口等）とコントロールセンター（サイバーインシデント等の判断、駆けつけ要否判断等）は一体で設置をした。

② コールセンター利用状況

運用期間中、コールセンターに相談が寄せられたのは以下の **6 件**

【表 31】コールセンター対応内容（インバウンド）

No	相談	対応
1	Windows update の方法について 照会日　：2019 年 9 月 26 日 照会者　：A社	手動による Windows update の方法を説明し、処理が進んでいることを確認した。
	最近、報道等で公表されている Windows10(IE)の脆弱性に関する対応について、Windows パッチが自動更新されないが、どうすればよいか。	
2	怪しいソフトをインストールしてしまった 照会日　：2019 年 10 月 29 日 照会者　：B社	詐欺ソフトウェアのインストールであるため、駆けつけ隊を手配。 データ取得後に当該ソフトウェアのアンインストール実施を推奨、追って電話にて、PC の動作およびアンチウイルス等で特に問題は起きていないことを確認した。
	従業員が自宅で使っているパソコンに One Safe PC Cleaner というソフトが入っている。 パソコンを会社に持ってきてもらいネットで調べてみるとマルウェアと書いてあるのを見つけたが、ウイルスチェックするも引っかからず。更に調べるとソフトを削除するためのアプ	

No	相談	対応
	リをダウンロードするために個人情報を入力する画面になったため、怪しいと思ってやめた。	
3	Windows update の方法について 照会日　：2019 年 11 月 7 日 照会者　：C社 PCを立ち上げたら「この処理を終わらせましょう」というメッセージが表示された。	Windows のアップデートを適用していない場合に表示されるメッセージであることならびに以下を回答。 「今すぐ再起動」ボタンを押すことによりWindowsのアップデートが開始されますが、時間がかかることとアップデート後のバージョンに対応していないアプリケーションは動かなくなる可能性があります。 アップデートを実行されるようでしたら、事前に重要なファイルをバックアップしておくことをおすすめ致します。
4	Emotet について 照会日　：2019 年 12 月 18 日 照会者　：D社 ここ最近、社員複数名が不審なメールを受信している。Emotet 感染のニュースもあるので、気になってかけた。内容はそれぞれ異なり、不審メールの受信者が以前他のメールでやり取りした内容を一部切り取り・貼り付けられたものも含まれており、情報漏洩しているのではと感じる。	以下をヒアリング。 ・添付ファイルはついているか？⇒word ファイルがついているメールもあるし、リンクとなっている場合もある。 ・添付ファイルやリンクを開いてしまった人はいますか？⇒いない。 ・差出人は取引先ですか？⇒身に覚えのない多数のドメインからのメールになっている。 ・メールの特徴を教えてください？⇒退職者や現職の名前が入っている。引用されている文章は全く関係がない文章タイトルが「賞与」となっているものがある。「取り急ぎ」と書かれているものもある。 ・気になっていることはありますか？⇒内部から内部宛のメールもあって気持ちが悪い。⇒ヘッダはどうなっていますか？社外から届いていませんか？⇒ヘッダを見たところ社外から届いている。⇒これについては社内の感染は低いものと思われますと回答 【その他ご案内したこと】 IPA に Emotet の特集ページがあることをお知らせ。 また、念のため、メールを受信した端末についてはフルスキャンを推奨とご案内した。（まだ、フルスキャンは未実施とのこと） 内部感染の可能性は低いものと考えられ、IPA の特集ページを見ていただき今後も注意していただくこととフルスキャンの実施をご案内し、クローズ。
5	ウイルスメールを開いてしまった（Emotet に感染した可能性）がある。 照会日　：2019 年 12 月 18 日 照会者　：E社	コールセンターより以下を確認および推奨。 １．感染端末はその後増えていないか。 →全部で 7,8 台。本社 2 台と福岡 5,6 台。LAN ケーブルは抜いている。 ２．被害先を保全するためにメーラーのアドレス帳を控

No	相談	対応
	複数台のパソコンがウイルスメールを受信した。 添付ファイルがあり、開いてしまった。 すぐに LAN ケーブルを抜いて隔離したが、不審なメールを受信していない他のパソコンから外部へメール送信されていた。 メールは過去そのパソコンで受信したメールに返信する形で送っているよう。 取引先から感染の疑い連絡を受ける。 翌日、以下の追加相談あり。 「なりすましメールが送信され続けている。どうにかする方法はないか？」 12 月 24 日 コールセンターから状況をヒアリング。	えておく。 ３．メールアカウントのパスワードを変更 ４．OS リカバリ ５．現在特定された PC 以外のものも念の為にウイルススキャンをかける。 ※追加の相談先として JPCERT/CC の窓口をご案内。 まずは案内した方法でやってみますとのこと。 お助け隊としては一次対応完了とし、復旧は先方待ち。 以下のとおり回答した。 「メールは御社とは関係のないところから送信されているため、基本的には止められない。昨日ご案内して控えていただいているアドレス帳の連絡先に御社のなりすましメールが送信されていることを注意喚起するのが、現実的な対応。」 「現在、業務は落ち着いている。最終的に感染した PC は 7 台。OS リカバリ中で感染した人には代替 PC で業務をしてもらっている。なりすましメールに関する外部からの問い合わせは減ったが、なくなってはいない。」 →また何かあればご連絡ください。とお伝えして本件クローズ。
6	怪しいメールが届く。 照会日　：2019 年 12 月 19 日 照会者　：Ｆ社 社内のドメインから社員宛にメールが届く。複数人に届いている。内容は同じ。「A さん→B さん、C さん、D さん」のような形。 内容は請求書の送付のお願いなど。どのメールも内容は同じだと思う。身に覚えはない。 一昨日くらいから発生。社員には無視してほしいと伝えてあるが、お助け隊のことを思い出して、相談してみた。	コールセンターより以下を確認および推奨。 メールの差出人について、外部から来ているものであれば A さんを騙って出されたものである可能性が高いとご案内。 なお、A さんから転送した貰ったメールの件名は、Virus Removed というように書かれており、添付ファイルも doc ファイルではなく txt ファイルがついているとのこと⇒電子メールスキャナによって無害化されている可能性あり メールの文面については IPA が注意喚起しているもの（「賞与支払届」や「請求書の件です」）と似ているが少し違っている⇒文面は変化することがあることをお知らせした。 その後の電話で外部のドメインからであることがわかったとのこと。 ⇒内部感染の可能性は低くなりますので、IPA や JPCERT/CC の注意喚起に従って、今後もご対応いただければとご案内。

③ UTM でのアラート検知起因のコールセンター対応

運用期間中、UTM でアラートを検知し、コールセンターで対応したのは以下の**9件**

【表 32】コールセンター対応内容（アウトバウンド）

No	検知アラート	対応
1	ボットネットとの通信 G 社 初回検知日： 2019 年 8 月 26 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　該当端末のネットワーク（有線 LAN・無線 LAN）から切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン ウイルス対策ソフトで検知できない場合は、端末の初期化を推奨。あわせて駆けつけ隊の要否を確認。 ⇒駆けつけ隊を希望されたため駆けつけを要請。 ⇒駆けつけ隊到着前に該当端末のメーカーを特定し、連絡。 Apple 社製のスマートフォンかパソコンの可能性。
2	ポートスキャン（TCP Xmas Tree Attack） H 社 初回検知日： 2019 年 9 月 2 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　TCP Xmas Tree Attack を行うツール等の利用有無 ②　該当端末のネットワーク（有線 LAN・無線 LAN）からの切り離し ③　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 追加調査をし、以下のとおり回答・クローズ。 「複数の箇所で検出されているため詳細調査を実施した結果、 特定通信先においては危険性がないものであると判明しました。 そのため、本アラートへの対応については実施しないで結構です。 また今後、同様のアラートの場合は通知も行いません。」
3	ボットネットとの通信 I 社 初回検知日： 2019 年 9 月 25 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　検知機器のネットワーク（有線 LAN・無線 LAN）から切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 先方で iPhone や ipad（私物持ち込み）に心当たりがあるとのこと。コールセンターからは駆けつけ調査はできかねるが、可能なら該当の端末で不正通信が検知された日時に行われた操作の確認を推奨。
4	ポートスキャン（TCP Xmas Tree Attack） J 社 初回検知日： 2019 年 10 月 2 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　TCP Xmas Tree Attack を行うツール等の利用有無 ②　該当端末のネットワーク（有線 LAN・無線 LAN）から切り離し ③　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 連日の検知があったため、駆けつけ隊の要否を確認。

No	検知アラート	対応
		⇒駆けつけ隊を希望されたため駆けつけを要請。 駆けつけ隊による調査結果は後述するが、追加調査でのパケットキャプチャを実施。（先方合意済み） パケットキャプチャの結果、以下を調査結果として報告し、クローズ。 「調査結果がでましたのでお知らせします。 【調査結果報告】 通信先を分析しましたところでは既知の悪意のあるサイトへの接続は認められませんでした。また、現時点では通信（スキャン）は UTM でブロックされていますので、外部への影響も発生していないと考えられます。 【現在まで調査しました内容】 ・ウイルススキャンソフトによるウイルス（マルウェア）検出はありませんでした。 ・ALSOK による現地端末の調査でも異常は検出されませんでした。 ・アラートを発生させた通信の接続先 IP アドレスを管理している団体を確認したところ Google でした。（悪意のあるサイトである可能性は低い） ・アラートを発生させた通信には内部情報は含まれていませんでした。（情報漏洩目的の通信であるとは断定できませんでした） ・マルウェアに感染し、マルウェアが指令サーバに接続して命令を受け取り、通信を発生している可能性を確認するために UTM で可能な限りの接続先 IP アドレスを取得、取得できた IP アドレス約 40 件を評価したところでは、問題は見つかりませんでした。 【今後につきまして】 「Google 関連のドメインに対する」TCP Xmas Tree スキャンについてはアラートメールをお送りしません。なお、他のアラートが発生した場合には従来とおり通知致します。」
5	ボットネットとの通信 K 社 初回検知日： 2019 年 10 月 29 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　該当端末のネットワーク（有線 LAN・無線 LAN）から切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 外部の業者が持ち込んだ Mac であることが判明。 先方で無線 AP へのアクセス制限をかけることで対応済み。
6	ボットネットとの通信 L 社 初回検知日： 2019 年 12 月 5 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　該当端末のネットワーク（有線 LAN・無線 LAN）から切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 該当端末は従業員の方が使われている私物スマホ（Android 端末および iPhone）。それらの端末は社内ネットワークに接続させていた。 コールセンターからは送信先の IP アドレスが海外の企業が管理するドメインであることを伝えた。 さらに上記状況より、担当者に以下を伝えた。 ・従業員の方が使われたスマホで海外の企業に接続するアプリを利用されている可能性が高い。

No	検知アラート	対応
		・スマホのフォレンジック調査は実証事業の範囲では行えない。 ・念の為、該当の端末でウスキャンを実施してほしい。 ・私物のスマホを社内ネットワークに接続させない。 ・新たに情報があれば追ってご連絡する。
7	ポートスキャン（TCP Xmas Tree Attack） M 社 初回検知日： 2019 年 12 月 23 日	端末利用者に対し、当該通信が意図して行った通信であるか否かの確認を依頼。また、以下の実施を推奨。 ①　該当端末のネットワーク（有線 LAN・無線 LAN）からの切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン 以下のお問い合わせあり。 「MAC アドレス：c8:1f:66:xx:xx:xx の端末がデスクトップパソコン（Windows10）、 MAC アドレス：54:e1:ad:xx:xx:xx の端末がノートパソコン（Windows10）で、どちらも社内で使用しているもので、 ウイルス感染の様子等はなく、現在も普段と同様に使用しています。 当該時間帯のパソコン操作においても、特に思い当たるところはありませんでした。 原因として何が考えられますでしょうか？」 追加調査をし、以下のとおり回答・クローズ。 「当方にて追加調査を実施した結果、特定した通信先においては危険性がないものであると判明しました。 そのため、本アラートに対する貴社での対応は不要です。 また今後、同様のアラートの場合は通知も行いません。」
8	ボットネットとの通信 N 社 初回検知日： 2019 年 12 月 26 日	当該通信が意図して行ったものではない場合、マルウェア感染の恐れがあるため、以下の対応を推奨。 ①当該端末上のウイルス対策ソフト定義ファイルの最新化 ②当該端末をネットワーク（有線 LAN・無線 LAN）から切り離し ③　ウイルス対策ソフトによるフルスキャンの実施 以下の対応を行いクローズ。 担当者に電話連絡してヒアリングを実施 【ヒアリング結果】 当該端末をウイルススキャンしたところでは何も検出されなかったとのこと。 また、現在、PC の入れ替え時期となっており当該 PC は NW から切断されている状態でもう戻す予定はないとのこと。
9	ボットネットとの通信 J 社 初回検知日： 2020 年 1 月 17 日	当該通信が意図して行ったものではない場合、マルウェア感染の恐れがあるため、以下の対応を推奨。 ①　検知機器のネットワーク（有線 LAN・無線 LAN）から切り離し ②　ウイルス対策ソフトの最新定義ファイルを使用しフルスキャン

No	検知アラート	対応
		以下の対応を行いクローズ。 担当者に電話連絡してヒアリングを実施 【ヒアリング結果】 私物のスマートフォンや PC を社内の Wi-Fi に接続させているとのことで、端末特定が困難。 上記状況より、担当者に以下を伝えた。 ・私物についても社内の端末と同じセキュリティを担保する。 ・私物の機器にウイルススキャンソフトを入れる。 ・私物の機器と会社のネットワークを分ける。 ・会社のネットワークに私物の機器を接続させない。

④ コールセンター利用促進に向けた取り組み

コールセンター（電話およびメール）の利用促進に向け、以下の対応を行ったが大きな効果は得られなかった。その理由は以下コールセンターの諸課題に記載。

- 開始説明会で配布したしおりへの掲載
- 中間報告会での利用促進・再説明
- 事務局からの利用促進メールの発信（チラシ付き）

⑤ コールセンターの諸課題

運用期間全体を通じてコールセンターの活用は少なかった。活用が少なかった原因は事後ヒアリングや事後アンケート結果を踏まえて、以下であると想定される。

- 相談するような困り事がなかった。
- 何を相談してよいか（できるのか）わからなかった。
- 相談することに抵抗感があった。

コールセンターの活用が少なかった一方で、何らかのマルウェアや脆弱性がメディア等で話題になると、それに関する相談が一時的に集中する。そのような不均一な稼働要素と稼働の平準化の課題は必ず発生すると考えられ、対応リソースを効率良く活用するためには相談窓口の機能を持たせるだけではなく、一定の稼働が発生する定常業務の機能を持たせることも必要である。

情報が複数の組織に分散される場合、組織間での情報連携は必須であり、緊急対応が必要な事案であれば、さらにその重要度は増す。連携手段は電話、メール、システム等を併用しながら、相互に状況を確認し合うこと（プロアクティブな行動）が円滑な連携を促進する。

また、対応側が複数の組織から構成される場合、些細なことや利用企業の情報などで何気ない日ごろのコミュニケーションを図っておくことも緊急時の連携をスムーズに行うためには重要なことである。

コールセンターが利用企業側のシステムあるいはネットワーク構成等を対応しながら把握することは困難であるため、企業側にベンダーや SIer がついている場合には、事前に開示できる範囲の情報を共有しておくことで、いざという時の対応がスムーズになると考えられる。

⑥ コールセンターのあるべき姿、そのために必要な体制や国の支援

コールセンターは困っている利用企業からの相談に「耳を傾けること」が、高度な専門知識やスキルを持つことよりも優先される。

コールセンターでの対応には、技術的な専門用語をいかに相手にわかる言葉に置き換えて伝えるかが重要である。利用者と高度な専門スキルを持った技術者が直接対話するよりも、オペレーターを通じた対話の方が結果的に利用満足度は高くなると考えられる。

上記より、コールセンターのフロントには相談ごとに耳を傾け、利用者に理解できる言葉でコミュニケーションが図れるオペレーターとバックヤードに高度な専門スキルを持つ技術者が控える体制が望ましいと考える。

コールセンターは稼働が平準化しない一方で体制は維持しておく必要があり、稼働率に関わらず、設備や人材に一定のコストがかかり続ける。さらに利用者目線では相談は無償であることが前提になっているため、設置事業者側の負担が大きい。コールセンター設置事業者には運用を維持するためのコストを国が支援する仕組みがあると設置へのモチベーションとなる。

８．駆けつけ隊

本実証事業では ALSOK において、駆けつけ隊を実施した。以下に駆けつけ隊の概要を説明する。

①　駆けつけ隊概要

駆けつけ隊とは、サイバーセキュリティに係る相談・有事の際の対応のため、コールセンターからの要請に基づき、ALSOK が現地へ駆けつけ、対応の支援を行うものである。

現地対応では、一次調査に必要となる PC の情報の確保を行う。1 次調査結果は 1 週間を目安に当該企業に対して回答する。

【表 33】駆けつけ隊概要

No	項目	内容
1	対応内容	マルウェア感染が疑われる PC のファストフォレンジック 内部不正が疑われる PC の証拠保全およびファストフォレンジック
2	対応時間	平日　09:00~17:00
3	対応機種	OS が Windows の PC。ただし、メーカーサポートが終了
4	対応要員	ALSOK の愛知県内 4 事業所（名古屋支社、尾張支社、岡崎支社、豊橋支社）に所属する社員
5	出動実績	3 件　※詳細は下表 34 のとおり

② **駆けつけ隊出動事例**

本実証事業期間中に **3 件**の出動を実施した。以下に出動の事例を示す。

【表 34】駆けつけ隊　出動事例

No	駆けつけ出動事例	対応
1	G 社 出動日： 9 月 4 日	据置型 UTM の配備先で、特定の端末から不正な通信先への通信を検知。 お助け隊コールセンターより連絡し、担当者と会話をするも当該端末を特定できず。 端末の特定を目的に駆けつけ隊の出動を実施。 駆けつけ実施時点で、担当者によって端末は既に特定されていたが、自動で社内ネットワークに接続されている端末の一覧を作成する機器を設置し、社内に存在する機器の見える化を行った。 不正通信な通信は社内の無線 LAN に接続された社員の私物スマートフォンだったため、フォレンジックによる情報取得は実施しなかった。
2	B 社 出動日：10 月 31 日	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、との問い合わせがお助け隊コールセンターに入電されたもの。 要請により駆けつけを実施し、フォレンジックツールにより必要情報の取得。 取得したデータを ALSOK 情報警備監視センターにて解析した結果、9 月 20 日に詐欺ソフトである「Onesafe PC Cleaner」がインストールされたことを確認。 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、11 月 8 日に提出した。 なお、当該企業において詐欺ソフトのアンインストールを実施するも、PC の動作が重く、画面上に多くのウィンドウが開く症状は改善せず。当該企業の担当者による調査の結果、詐欺ソフトとは別に「Intel(R) Security Assist」のプロセスが 100 以上起動していることが確認され、これをアンインストールすることで症状が治まった。
3	J 社 出動日：11 月 25 日	据置型 UTM の配備先で、5 台の端末からポートスキャンを検知。 お助け隊コールセンターより連絡し、担当者と会話をするも当該端末を特定できず。 端末の特定および当該端末からの情報取得を目的に駆けつけを実施した。 駆けつけを実施して調査を実施し、不正な通信の発信元は、PC2 台、プリンタ 2 台、不明 1 台であった。PC2 台よりフォレンジックツールによる情報取得を行った。 取得した情報を ALSOK 情報警備監視センターで解析するも、不正なプログラム等通信の発信元となるプログラムの特定に至らなかった。判明した状況を整理し、レポートを 12 月 9 日に提出した。

③ **駆けつけ隊の諸課題**

本実証事業を通じて確認された駆けつけ隊の諸課題については以下のとおり。

（ア）対応機種（Windows のみ。Mac、スマホ、複合機に対応できない）

本実証事業での駆けつけ隊による情報取得は OS が Windows の PC に限定した。これは、中小企業における業務端末は、OS が Windows の PC であるとの想定によるものである。しかしながら、駆けつけ事例の中には、不正な通信の発信元がスマートフォンであるケースや複合機が発信元であるケースも発生しており、対応機種の拡大について検討が必要と思われる。

しかしながら、対応 OS や機種を拡大した場合には、駆けつけ時の対応により高度な専門知識を要する場合や専用のツールを用意する必要がある場合があり、その教育費用やツールの準備にはコストが発生する。これらはそのまま駆けつけ隊の出動費用に反映されることも想定されることから、コストと対応範囲のバランスについては検討が必要である。

(イ) 端末特定

本実証事業では、駆けつけ隊の出動条件の一つを「該当の端末が特定できていること」としていた。しかしながら、これまでの出動実績では、中小企業の IT 資産管理が十分になされていないケースが散見され、担当者が端末を見つけられない、見つけるための IT スキルを持っていない、ネットワークが DHCP で構成されている、などの諸課題がある。駆けつけ隊においても端末特定の支援をメニューに組み込む検討が必要と考えられる。

しかし、企業のネットワーク構成によっては端末特定に長時間を要する場合がある。長時間の拘束は駆けつけ隊員の稼働コストになりうる。例えば DHCP を利用している企業において、検知から駆けつけまでに期間が空いた場合、駆けつけ時には検知時とは異なる IP アドレスが付与されているケースが考えられる。この場合には、MAC アドレスなど一意の端末情報が取得できていることなどが、駆けつけに付随するサービスの条件となる。

(ウ) 対応範囲の拡大

本実証事業では、フォレンジックツールによる情報取得によって、当該 PC で「何が起きているのか」「なぜそうなったのか」「どう対応すればよいのか」を明らかにすることを主眼にサービスを行った。これは専門会社への取次ぎやサイバー保険適用時のエビデンス取得のためでもあるが、中小企業の担当者は原因調査よりも早期復旧を望むケースも多い。これは中小企業が予備の PC を持ち合わせていないなどの理由に起因するものと考えられる。調査期間の短縮や簡易な対応についての検討が必要と考えられる。

また、本実証事業の参加企業の中には保守ベンダーとの契約を交わしている企業も存在しているが、このような企業においてインシデントが発生した際に、駆けつけ隊と保守ベンダーによる情報の連携、作業区分および責任範囲の明確化も今後の課題となる。

(エ) コールセンターとの連携

本実証事業では、コールセンターを NTT-AT が担当し、駆けつけ隊を ALSOK の事業所社員が担当し、駆けつけ隊の出動には異なる会社間での連携が必要であった。これについては、事前に十分に連絡のフォーマットやフローについて話し合っていた結果、駆けつけ隊の出動に大きな障害となる問題は発生しなかった。

9．事後アンケート結果

事後アンケートによりお助け隊設置に関する中小企業のニーズや意見を確認した。
設問は大きく分けて下記の３つの分類。それぞれ参加する中小企業の実態について 121 社から回答を得た。

- 体制整備に関する設問（社内体制構築、文書の作成、従業員教育、SECURITY ACTION 宣言等）
- UTM 機器・コールセンターに関する質問（UTM や EDR、コールセンターの活用、セキュリティ費用等）
- 愛知県お助け隊メニュー・今後の体制に関する質問（お助け隊メニュー、次年度事業、中小企業向けサービス等）

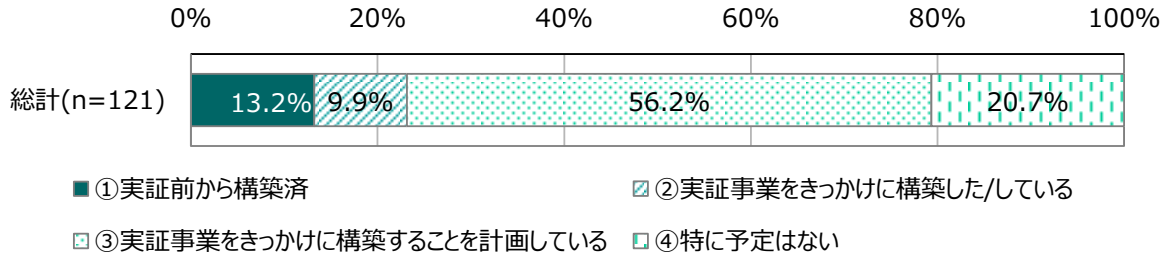
特筆すべき内容としては、下記のような結果が見て取れる。

- 本実証事業によって組織体制構築（8 割弱）、文書整備（6 割強）のきっかけになった
- 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 万の層も 3 割弱おり、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」と回答した企業の合計は 5 割近くであり、必ずしも低価格であることが決め手であるとは言えない
- セキュリティマネジメント指導業務のような寄り添ったサポート、「防御～検知～対応」をカバーするサービス、自社のネットワークを評価するサービスなど、個別対応を求める意見も多い

これらの結果を踏まえると、中小企業とひとくくりにしてもセキュリティ強化に投資や手間をいとわない企業は一定数おり、第三者による評価を求める声も多いということが言える。

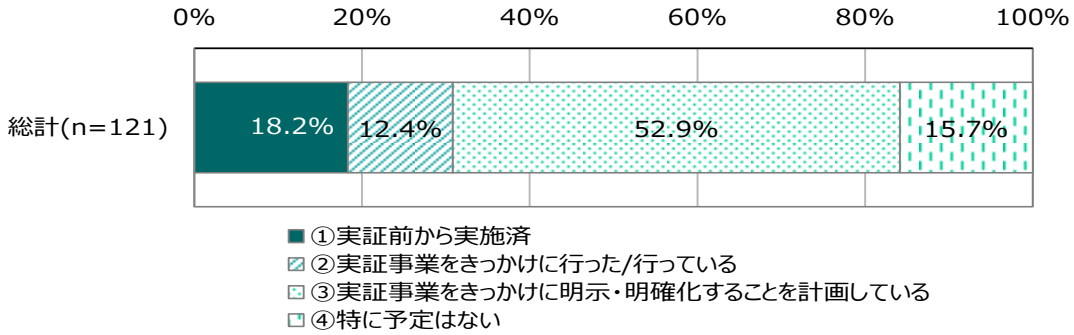
1）サイバーセキュリティに関する組織体制構築に関する質問

【グラフ 21】サイバーセキュリティに関する組織体制構築について



2）方針・セキュリティポリシーの明示・明確化に関する質問

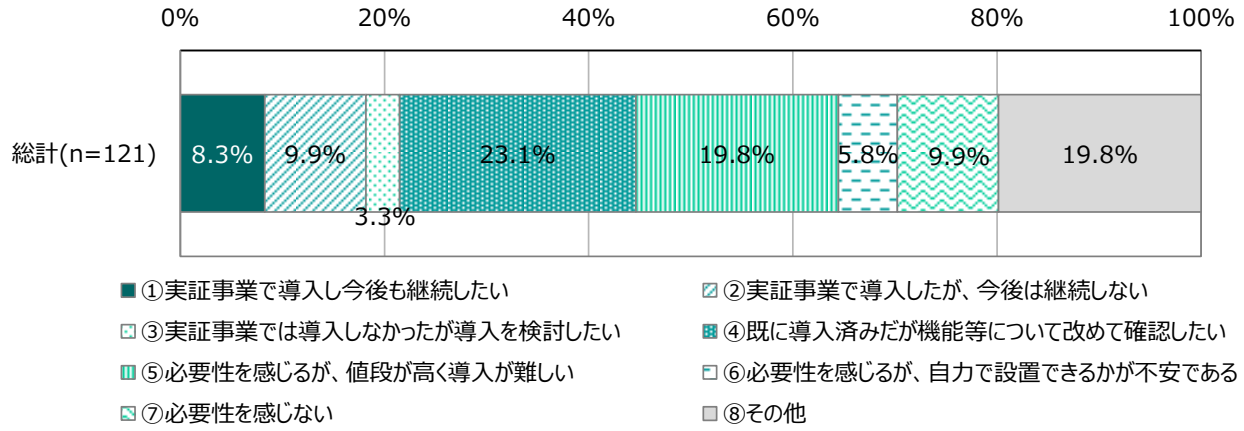
【グラフ 22】方針・セキュリティポリシーの明示・明確化について



3）UTM 機器の導入に関する質問

※「⑧その他」には“（今回は）導入できなかった”・“既に導入済である”等の回答があった。

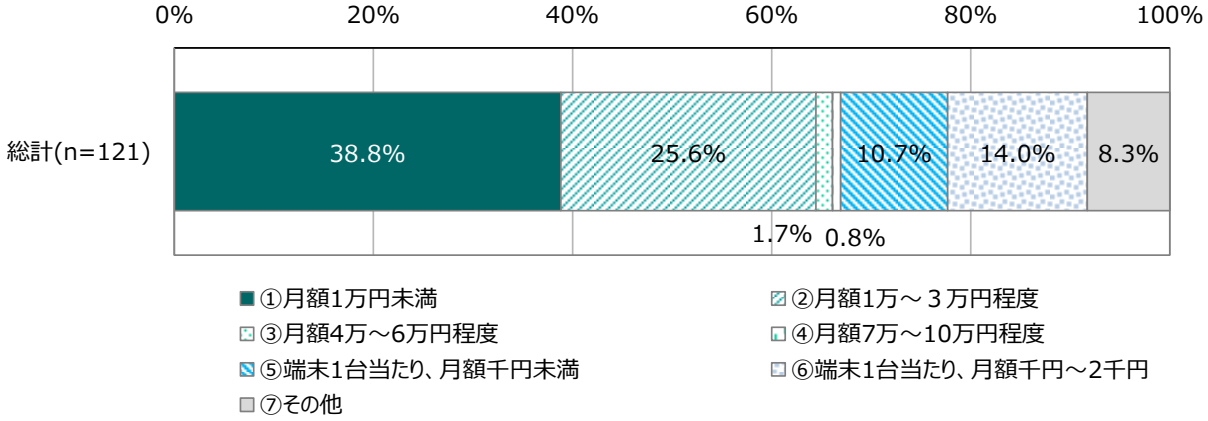
【グラフ 23】UTM 導入について



4）セキュリティ機器（UTM 機器、エンドポイントセキュリティ機器等）に関する質問

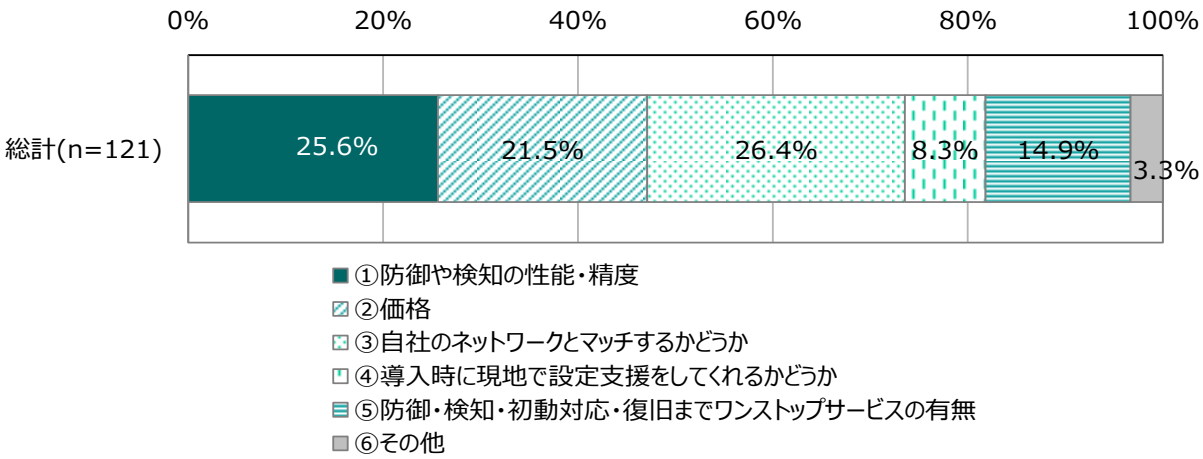
※「⑦その他」には“必要があれば金額関係なく導入を検討”・“継続的な費用負担があるものの導入は難しい”等の回答があった。

【グラフ 24】セキュリティ機器の価格について



5）セキュリティ機器導入にあたって最も決め手となるものに関する質問

【グラフ 25】セキュリティ機器導入の決め手について



6）中小企業にとって、サイバーセキュリティ体制向上のため必要なサービスに関する質問（自由記述）

※下記は抜粋

【表 35】中小企業にとってサイバーセキュリティ体制向上のために必要なサービスについて

No	Q.中小企業にとって、サイバーセキュリティ体制向上のため必要なサービスは何だと思いますか？	分類
1	公平な立場での、対策状況モニタリングと評価。弱点・課題の提供。	プラットフォーム
2	なんでも１１０番的な相談室があれば気楽に相談できてよいと思う。	プラットフォーム
3	定額年会費のみで使えるサービス。	プラットフォーム
4	警備会社やインターネット企業ではなくサイバーセキュリティに特化した法人部隊の起業。定期的な初期段階での攻撃の種類や情報の配信。	プラットフォーム
5	「情報セキュリティマネジメント指導事業」での個別指導はとても良かった。そのようなサービスが今後も継続されて、尚且つセキュリティアクションの星で外部機関からの評価があってもよいのではないかと思います。	個別コンサル
6	よくわかりませんが、弊社のように人数が少なく理解ができていない会社にとっては、かなり手取り足取りで指導していただけると助かります。	個別コンサル
7	サイバーセキュリティの脅威および対策の啓蒙。各個別企業に合ったセキュリティ対策の提案	個別コンサル
8	担当者が顔の見える形でセキュリティ体制について相談させていただくサービスがあると、より安心でき会社としてもセキュリティの脆弱な部分についてわかるため、よいかと思います。	個別コンサル
9	ネットワーク構築時のアドバイス等が必要だと思います。	個別コンサル
10	体制構築にあたり、相談できる窓口があるとよいと思う。	個別コンサル
11	個別のコンサルティング。	個別コンサル
12	サイバーセキュリティシステム構築のためのサポート。	個別コンサル
13	中小企業での被害状況や対処費用等の情報共有	情報共有
14	最新情報の案内、助成金等の情報、セキュリティーベンダーの紹介。	情報共有
15	同様のサービスを提供している各社の費用比較や機能比較、実績比較など、中小企業にとっては、その情報を集めるだけでも手間がかかります。ニュートラルな情報発信があればよいのかと思います。	情報共有
16	無料セミナーや短時間セミナー等を開催してほしい。又日々時間に制限がある者が多いと思われるのでＥラーニング等があれば学びやすい。	情報共有
17	最低限のレベルを明確にして欲しい。	情報共有
18	まだまだ各々の危機意識は正直低いと思われる部分がありますので、広告などメディアを通じてもっと注意喚起をしていただければ意識改革につながるのではないかと考えております。	情報共有
19	日常業務の多さに、セキュリティにまで時間を割けないのが実状です。毎月、ポイントを絞ったプログラムで一年を通じてやると、ある程度セキュリティ水準が上がるといったようなサービスだとやりやすいのかと思います。	情報共有
20	期間が短すぎたので、年間計画で設定サポート者を派遣していただき、実験開始前までに接続を確立してほしい。	製品・サービス
21	個別事案に対応できる柔軟なサポートと価格の安さ。	製品・サービス
22	手軽に導入できるもの。	製品・サービス
23	ＵＴＭの内容を報告する形態が一番重要だと思います。	製品・サービス
24	一般的には、導入が丸投げできるものがよいと思う。 自社はＲＰＡを使用しているのでしっかりした説明が欲しかった。	製品・サービス

No	Q.中小企業にとって、サイバーセキュリティ体制向上のため必要なサービスは何だと思いますか？	分類
25	ちょっとしたことでもすぐに問い合わせできる窓口と導入しようと思える価格。	製品・サービス
26	添付ファイルを開かなくて済むような作業環境構築の推奨。低ＩＴリテラシー作業者の教育が先決。ＵＴＭで防止するならネット遮断のセットアップを出張でやるべきです。	製品・サービス
27	設置コストが低く、最低限度のセキュリティを担保できる商材。	製品・サービス
28	低価格で導入支援・保守・訪問サポートまで一括で受けられるサービス。	製品・サービス
29	自社のセキュリティレベルを測定（点数で）できるサービス。	製品・サービス
30	業種ごとに　何をどのように守るのかを具体化できかつコストに見合ったセキュリティサービスがあるとよい。	製品・サービス
31	中小企業には人員的にセキュリティチームを構築することが困難な所もあります。「ＵＴＭ・サイバー保険・事故対応」までをセットにした商品開発がされればセキュリティ環境をつくるハードルが下がるのではないでしょうか。	製品・サービス
32	比較的廉価でどのような時間帯（２４時間体制）で対応可能なサービス。	製品・サービス
33	プロバイダ、回線業者の段階で、ウイルスなど明らかな脅威はとりのぞいてほしい。	製品・サービス
34	外部からの試験的な不正アクセス実験。	製品・サービス
35	普段の何も起きていない状態を「問題ない」と確認できるサービス。	製品・サービス
36	ワンストップサービス。	製品・サービス
37	セキュリティソフトや機器の導入程度の簡単さでもっと全体に同一の仕組みを一斉展開する。	製品・サービス
38	各会社の規模およびレベルに対しての体制つくり。	体制構築
39	ガイドラインの策定と推進・補助。	体制構築
40	社内体制の整備、構築がまず必要、役割を決め実行すること。	体制構築
41	中小企業が自社で対応できる限界（ヒト、カネ、ノウハウ）が認識できれば保険の必要性にも目が向く。	体制構築
42	規模に応じて体制は大きく異なると思います。規程のサンプルもある程度の規模を想定したものになっているように思えます。規模に応じたサンプルがあるとよいと思います。	体制構築
43	安価で簡素な体制が確立できるようなサービス。	体制構築

１０．　事後ヒアリング結果

事後ヒアリングにより中小企業の実態やニーズを確認した。対象企業は、お助け隊メニューを特に活用している企業を中心に、5 社に対して実施した。

【表 36】事後ヒアリング実施先

（★印は IPA 同席）

No	会社名	業種	従業員数	ヒアリング実施日
1	G 社★	製造業その他	21～50 名	2019/12/16
2	O 社★	製造業その他	101～300 名	2019/12/16
3	P 社	卸売業	21～50 名	2019/12/16
4	I 社★	製造業その他	51～100 名	2019/12/17
5	K 社★	サービス業	6～20 名	2019/12/17

共通ヒアリング項目は下記 5 点である。

- お助け隊実証事業の参加目的・動機について
- 実証事業に参加したことによる目的の達成
- 実証事業の各メニューについて意見・感想
- 中小企業にとって「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）」
- 中小企業が利用しやすいサイバー保険について

なお個別ヒアリング項目は、企業の特性に応じたものとした。

ヒアリングを行った結果、特筆すべき内容は下記のとおり。

- ネットワークに不安を感じている企業が多い、自社のネットワーク構成をチェック・評価する機能を求める
- セキュリティに費用を投資してもよいと考えている企業も多い
- 自社ですべてをまかなうことは想定しておらず、最低限自社で整えるべきセキュリティ体制と、外部委託で対応すべきセキュリティサービスとを分けて考えている。

上記これらの結果や事後アンケートの結果を踏まえると、信頼できるサービスやベンダーを活用したセキュリティ体制構築が重要であり、価格はどちらかといえば安い方がよいが、“ただ安ければよい”というものではないという事業者の意識があることがうかがえる。

【表 37】事後ヒアリング　まとめ

大分類	中分類	ヒアリング回答	キーワード
実証事業について	参加目的・動機	・情報収集、サイバーセキュリティ体制強化 ・UTM 無償導入 ・サプライチェーン企業からの紹介	情報収集 UTM サプライチェーン
	目的の達成	・体制構築から実践的な演習まで幅広いセミナーは有意義だった ・実際にアラーム検知、駆けつけ対応してもらい活用できた ・他社の取組の情報を聞けたことが有意義だった	情報収取 他社情報共有 アラーム・駆けつけ
	メニューについて	・実践的なサイバー演習は有意義だった ・UTM 導入は安心感あるが、性能・精度については検証が必要 ・（セキュリティマネジメント指導業務の個別指導は有益だった）	実践的な演習 UTM の性能 個別指導
中小企業向けサービス人材スキル保険	サービス、人材、スキル	・内部の体制強化と外部委託の使い分け（検知・監視は外部） ・中小企業側にも最低限の知識は必要 ・様々なシステムソリューションから自社にマッチするものを選択	内部と外部 自社にマッチ
	サイバー保険	・サイバー保険の補償内容が十分に理解できない ・セキュリティ対策が追いついておらず、保険の検討に至っていない ・保険にセキュリティサービスが付属していたらありがたい	補償内容がわからない 保険付帯サービス
	自社のネットワーク構築	・自社ネットワークは独自に構築している ・自社ネットワークを評価、検証してほしい ・自社ネットワークを把握できていない	自社ネットワークの評価、検証
	国に期待するサービス	・公平性の保てる機関による情報集約、情報発信 ・他社取り組みなどの情報交換の場が欲しい ・SECURITY ACTION の活用推進	情報発信 情報交換 SECURITY ACTION
サプライチェーンセキュリティ対策コスト	サプライチェーン企業からの要求	・セキュリティに関するアンケートや推奨ソフトの案内はある ・取引条件にセキュリティ要件は入っていない（セキュリティに限らずの責任関係は契約書に明記）	取引要件ではない
	セキュリティ対策コスト	・安ければいいというものではない、コストに見合った性能も重要 ・自社に必要なセキュリティ製品、サービスに対しては必要コストとして投資すべきと考えている（安くても性能が悪ければ意味がない）	安ければいいというものではない

１１． SECURITY ACTION 取得状況

7 月末（実証事業開始時点）、9 月末時点（8 月のセキュリティセミナー後）、11 月末時点（中間報告後）、1 月末時点（実証終了後）

【表 38】SECURITY ACTION 宣言企業推移

SEURITY ACTION	7 月末	9 月末	11 月末	1 月
一つ星	14 社	24 社	35 社	34 社
二つ星	3 社	6 社	6 社	10 社
計	17 社	30 社	41 社	44 社
増加数	**－**	**13 社** ↗	**11 社** ↗	**3 社** ↗
累計増加数	**－**	**13 社**	**24 社**	**27 社**

※web 申込と事前アンケート提出の両方を実施した 193 社の内数。途中辞退した企業を含む。

説明会等で呼びかけを行い、チラシ配布なども行い、SECURITY ACTION 取得を呼びかけた。

MS&AD インターリスク総研および三井住友海上火災保険、あいおいニッセイ同和損害保険は SECURITY ACTION 普及賛同企業に申請、登録された。MS&AD インターリスク総研においては、SECURITYACTION 取得のためのサービスメニュー『「SECURITY ACTION」宣言支援コンサルティング』開発し、サービス実装している。

１２． サイバー保険（中小企業向け）の検討

提案書に記載のとおり、MS&AD インシュアランスグループの、MS&AD インターリスク総研・三井住友海上火災保険・あいおいニッセイ同和損害保険の三社が連携し、本実証事業を踏まえたサイバー保険（中小企業向け）の検討を行った。

検討により出た意見や論点は以下のとおり。

【既に実施している内容】

- セキュリティ商品・サービス付帯サイバー保険による普及
- 総合賠償責任保険に特約としてサイバー補償特約を付帯
- Lucideus 社とのリスクアセスメントツールの共同開発
- MS&AD インターリスク総研・三井住友海上火災保険・あいおいニッセイ同和損害保険の SECURITY ACTION 普及賛同企業

【中小企業のニーズに応じた検討が必要な内容】

- サイバー保険の補償内容、保険料水準
- サイバー保険の事故事例、事故データの集積、分析
- 販売チャネル
- 販売方式（商品付帯、特約付帯、サイバー保険単体による販売など）
- 販売ツール（パンフレットや提案書、保険料計算ツールなど）の充実化
- MS&AD インターリスク総研のサービスメニューの充実化（MSSP 事業者との協業）
- SECURITY ACTION の項目と併せたサイバー保険販売強化策の検討

実証事業参加企業の意見やニーズとしては、下記の意見が多かった。

【ポジティブな意見】

- サイバー保険の必要性を理解し、見積もりを取ってみたら意外と安かったので、加入しようと思う
- サイバー保険に付随したワンストップサービスがあるとよい
- まずは体制構築が先決だが、経営陣のセキュリティへの理解が進めばサイバー保険の検討をしやすくなる

【ネガティブな意見】

- サイバー保険の補償内容がわからない、パンフレットなどがわかりづらい
- 自社のネットワーク構成やセキュリティ体制構築が不十分な中、リスクヘッジとしてサイバー保険の検討にまで至らない
- 補償内容や必要性を十分に理解していない状況で高いか安いかの判断ができない

これらを踏まえると、単にサイバー保険の保険料を下げることや補償内容を削減することが、求められる中小企業向けサイバー保険の検討において適切とは言えない。

サイバー保険の必要性を理解してもらうには、中小企業におけるセキュリティ体制構築や中小企業間の情報共有体制の構築が必要である。

一方で、保険会社の立場としては、サイバー保険の補償内容をわかりやすくすること、企業の実態に合わせたカスタマイズを可能とすること、付随するサービスを検討することなどが考えられる。

議論の中で、特に重要と考えられるのは、「事故データの共有」である。現状はサイバー保険の普及が進んでいないゆえに、事故事例・データが少なく、中小企業へのニーズ喚起・リスク喚起への障壁となっている。

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、適切な情報発信によるサイバーセキュリティ世論形成により普及促進が進むものと考えられる。

近年のグローバル化を踏まえれば、海外の事例や海外拠点へのサイバー攻撃のリスクも増えており、我が国一丸となった情報共有と、それと連動した事故未然防止の情報発信体制の構築が急務であると考える。

サイバー保険のあるべき姿の提案として、共同保険による事故情報の共有体制をつくり、情報の蓄積を図ることが考えられる。

１３． 実施結果から読み取れる課題（参加企業側）

実証事業各メニューを通じて中小企業のニーズや課題を確認することができた。各メニューで挙げられたニーズや課題は下表 39 の対応表のとおり。

【表 39】中小企業のニーズ・課題対応表

No	項目	該当項目
1	事前アンケートによる実態把握	Ⅱ.2
2	据置型 UTM 手配に関する諸課題	Ⅱ.4.(3)⑦
3	（据置型）UTM 設置に関するコスト・必要な人材	Ⅱ.4.(3)⑧
4	クラウド型 UTM 手配に関する諸課題	Ⅱ.4.(4)⑦
5	（クラウド型）UTM 設置に関するコスト・必要な人材	Ⅱ.4.(4)⑧
6	UTM 手配の課題解決策	Ⅱ.4.(5)
7	（サイバーセキュリティ演習） 参加者の声（一部）	Ⅱ.6.(1)④
8	（サイバーセキュリティ演習） フォローアップヒアリングまとめ	Ⅱ.6.(2)②表 29
9	（サイバーセキュリティ演習）本実証事業に係る意見・要望等	Ⅱ.6.(2)③
10	コールセンターの諸課題	Ⅱ.7.⑤
11	駆けつけ隊の諸課題	Ⅱ.8.③
12	事後アンケート結果	Ⅱ.9.表 35
13	事後ヒアリング結果	Ⅱ.10.表 37
14	サイバー保険の検討	Ⅱ.12

表 39 に対応するニーズや課題を、下記のとおり 23 項目に整理・集約した。

1. セキュリティ業務(企画・調達・運用)を担う人材が不足している
2. 経営層・従業員のセキュリティに係る意識が低い
3. 標的型サイバー訓練を実施してほしい
4. セキュリティ文書の整備状況がばらついている
5. 外部専門家が訪問し、アドバイスしてほしい
6. 相談先が「懇意にしているベンダー」に限られている
7. 講じるべき技術的対策がわからない
8. 安全にバックアップを取れない
9. IT 環境(NW、サーバ等)を把握できていない
10. セキュリティ監視を担える人材が不足している
11. 有事の際にスピーディに対応できる人材が不足している
12. 実際の具体例（偽メールからの被害、ランサムウェア等）および具体的な対策方法を提供してほしい
13. 情報共有の場、または E ラーニング等を提供してほしい
14. インシデント発生時等のセキュリティに係る相談窓口、助成金、セキュリティーベンダー等の紹介をしてほしい
15. サイバー保険に入っていない
16. サイバー保険の補償内容がわからない
17. 自社のセキュリティ体制が構築できていない状態で保険に加入するべきかどうかの判断に至らない
18. UTM 導入は安心感あるが、性能・精度については検証が必要
19. 内部の体制強化と外部委託の使い分けが重要だと感じている（内製できない検知・監視は外部を想定）

20. 様々なシステムソリューションの中で自社に費用対効果的に適切なものの選択が難しい(必要な対策に対する適切な費用が判断できない)
21. 保険にセキュリティサービスが付属していたらありがたい
22. 公平性の保てる機関による情報集約、情報発信、他社取り組みなどの情報交換の場が欲しい
23. SECURITY ACTION を推進したいと感じているが、自社単独では難しい

III.　実証結果を踏まえた検討の実施

１．中小企業が利用しやすいサイバー保険のあり方

本実証事業を通じて得た情報をもとに中小企業が利用しやすいサイバー保険のあり方について下記のとおり検討した。

（１）　「商品付帯サイバー保険」

企業向けのセキュリティソフトやクラウドサービスなどにサイバー保険が自動的に付帯されているもの（被保険者はそれらを購入した企業）。昨今では様々な商材にサイバー保険が付帯されている。

今回の実証事業においても、据置型 UTM およびクラウド型 UTM に商品付帯サイバー保険を手配した。

補償内容は下記のとおり設定した。（開始説明会資料より抜粋）

【表 40】本実証事業で付帯した商品付帯サイバー保険の概要

項目	内容
補償内容	本実証事業で提供する UTM 機器あるいはサービスが接続するネットワークの所有・使用または管理に関連して発生した事故 ※　ネットワークに起因しない事故（書類の紛失など）は対象外です。
保険期間	保険責任開始日：対象商品等を保険契約者から提供され、かつ契約者が提供するリモートサポートサービスが開始したとき時 保険責任終了日：保険期間の終了もしくは対象商品等にかかわるサービスを解約した日のいずれか早い日の午後１２時まで
支払限度額	賠償損害　　１被保険者あたり３００万円 費用損害　　１被保険者あたり１００万円
免責金額	なし

商品付帯サイバー保険の中小企業のメリットとして下記が挙げられる。

① 保険の加入手続きが不要

② 「おまけ」なので保険料負担無し

③ 「対策」と「保険」を一度に手配可

サイバー保険を広く普及させ、いざという時の最低限の補償として加入していることは中小企業にサイバーインシデントが発生した場合に重要なリスクヘッジとなる。ただし課題として、付帯される保険は中小企業が自社のリスク実態に合わせて設計するものでなく、「サイバープロテクター」「サイバーセキュリティ保険」などの汎用商品の簡易版となり、補償内容は商材ごとに異なるため、対策としてはこれのみでは不十分である。

【表 41】一般的な保険契約と商品付帯方式の違い

	一般的な保険契約	商品付帯方式
保険契約者	購入した事業者	商品・サービス・認証を提供する事業者
被保険者	購入した事業者	該当商品・サービス・認証を購買した事業者
補償内容	個別に設定	一律

（２）　「中小企業向けパッケージ型賠償責任保険に特約でセット」

ＰＬ保険などの中小企業にとって必要な賠償責任保険をパッケージにした保険商品に「特約（オプション）」としてサイバー保険をセットすることができる（売上高 100 億円以下の企業のみ対象）。

パッケージ型賠償責任保険に特約でセットする場合の、中小企業のメリットとして下記が挙げられる。

① 詳細な告知書を提出する必要無し
② 他の賠償責任保険とセットで検討可能
③ わかりやすいシンプルな補償内容

（３）　「サイバー保険加入前のリスクアセスメントツール提供（パイロット実施）」

簡易な 20 問程度の質問に回答することで自社のサイバーセキュリティ体制を可視化（スコア化）できるサービスを、MS&AD インターリスク総研と米国・インドを拠点とする Lucideus 社とで共同開発した。自社のサイバーセキュリティ対策状況の把握や、どのような部分を改善する必要があるのか、客観的な状況を把握することができる。

本サービスはサイバー保険そのものではないが、サイバー保険加入にあたって自社のサイバーセキュリティ対策状況を把握することで、サイバー保険加入のきっかけとなるツールである。

（４）　「事故データ共有体制の構築（案）」

Ⅱ．１２でサイバー保険について検討の中で、特に重要と考えている「事故データの共有」体制の構築を提案する。

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。

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。

下図のようにお助け隊品質を持つセキュリティサービスに認証を付与する際に、お助け隊コンソーシアムに賛同する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。

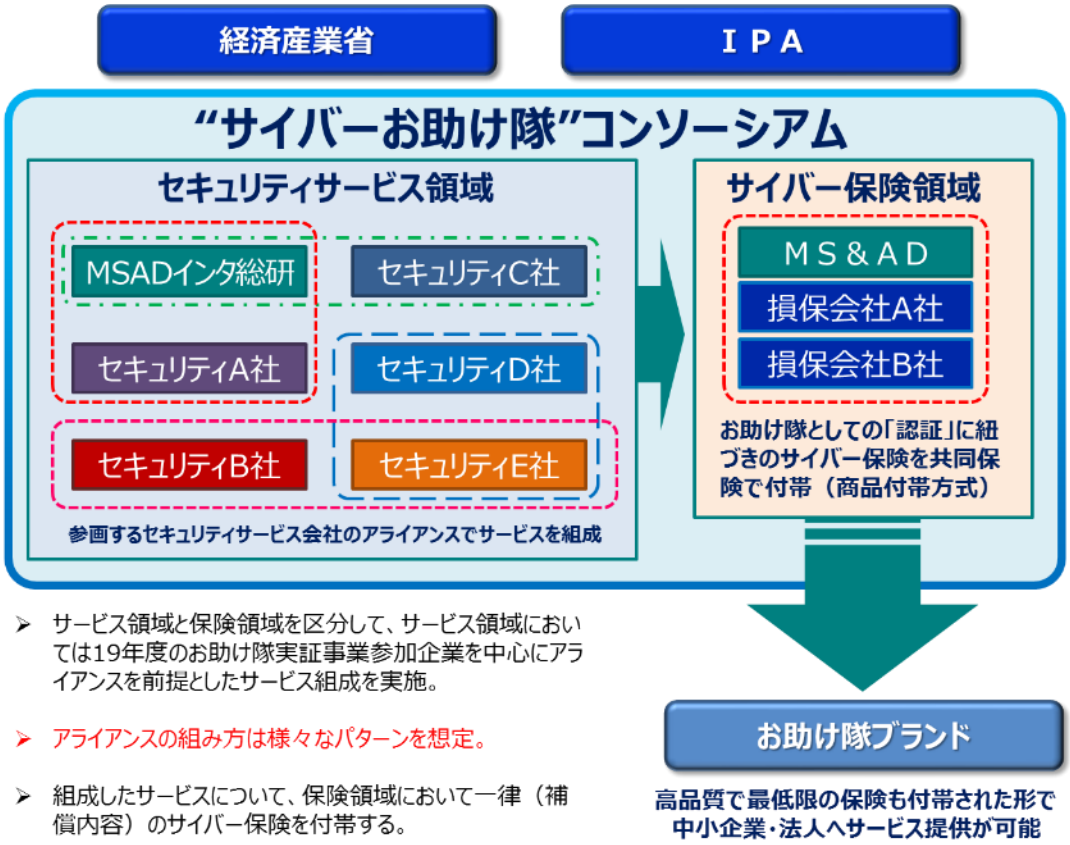
※共同保険方式でない場合、事故データの共有には契約者・被保険者の同意が必要となる。

※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。

また、共同保険方式とすることで、お助け隊ブランドのセキュリティ製品・サービスとして認証されれば、一律サイバー保険が付帯され、補償内容も同一となる。これにより、認証されたセキュリティサービスに付帯するサイバー保険は一律の内容となり、中小企業にとってわかりやすく安心感のある顧客本位の制度を実現することができる。

さらに将来的に、国や IPA その他公的機関とも事故データ等を共有することで、サイバーセキュリティ強化に関する政策立案等への活用が期待される。

【図 10】サイバーセキュリティお助け隊コンソーシアム　認証と保険

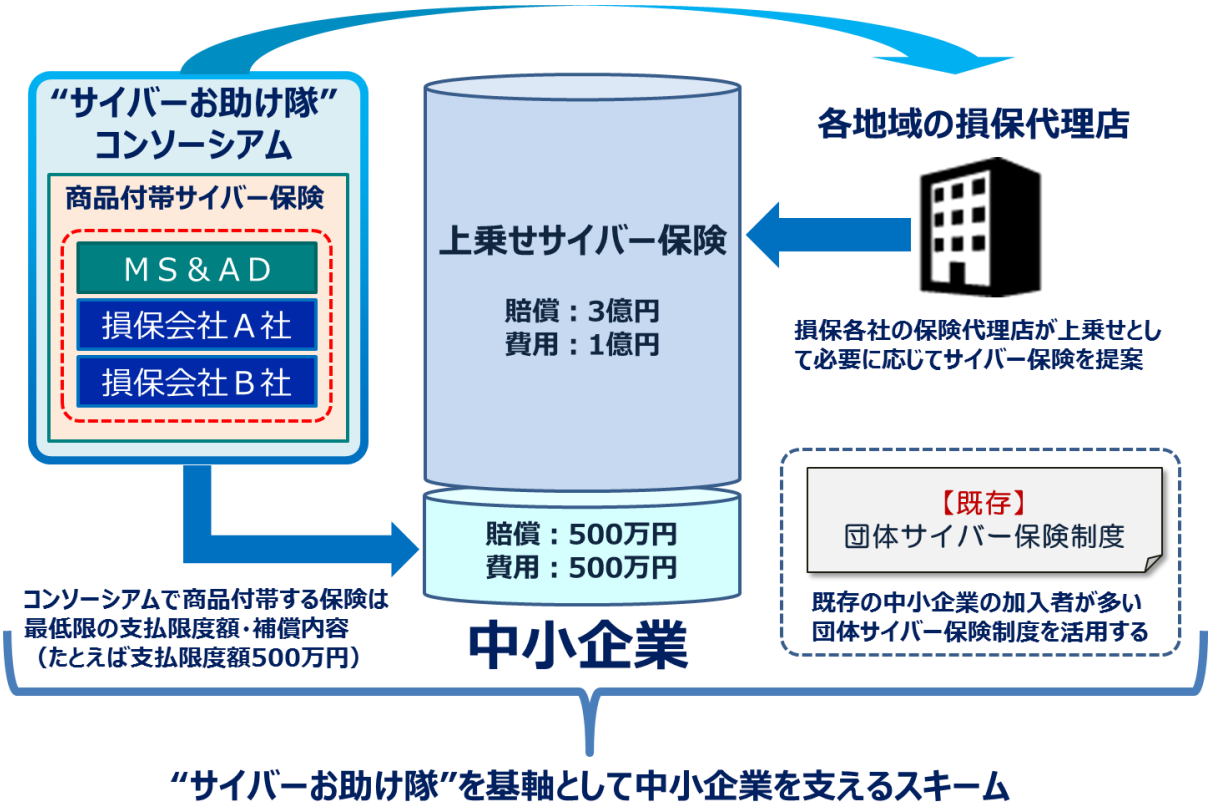


一方で、商品付帯サイバー保険の補償内容だけでは十分でない企業も見込まれる。その場合には、商品付帯サイバー保険の上乗せ補償として補償内容や免責金額を設定することにより、商品付帯サイバー保険と重複せずにサイバー保険に任意で加入することができる。

特に中小企業向けの保険制度として既存の「中小企業の加入者が多い団体サイバー保険制度」を活用し、上乗せ補償として加入することができるように保険制度の変更の検討をする必要がある。

【図 11】事故データ共有体制の構築

※下図の保険支払限度額の金額設定は一例であり、中小企業のニーズや業種に応じて設定する必要がある。



本制度設計によるメリットは主に下記４点となる。

① 「お助け隊」ブランドの付加価値

「サイバーセキュリティお助け隊コンソーシアムとして認証するサービス」を利用するメリットの一つとして、複数の保険会社が共同で運営するサイバー保険の提供を標榜することが可能となり、ブランド価値の向上に寄与する。

② 統一化された補償内容（事故対応）

商品付帯方式を採用することで、「サイバーセキュリティお助け隊コンソーシアム」のもとに提供されるサイバー保険の補償内容が統一化される。現在は、例えば保険会社によってサイバー保険約款に記載される「事故日」の定義が異なるなど、顧客にとってわかりにくい状態となっている。万が一の事故の際にも、購買しているサービスにかかわらず、統一化された補償内容での事故対応が可能となり、中小企業にとってわかりやすく安心感のある顧客本位の制度となる。

③ 事故情報の共有

共同保険の商品付帯方式とすることで、参画する保険会社間で事故情報を共有することができ、中小企業向けのサイバー保険開発に際して有益な事故情報を効率的に蓄積することができる。これにより高品質かつニーズに合った保険商品開発の促進につながる。

④ 十分な保険キャパシティの確保

共同保険の商品付帯方式とすることで、複数の保険会社による保険キャパシティの提供が可能となり、多数の中小企業を補償する保険制度として、安定した運用が可能となる。

※サイバーセキュリティは事故が同時多発的に発生する集積リスクがあるため、上記例では支払限度額 500 万円としているが 1 年間で 5000 社に事故があった場合の最大総支払額は 250 億円となり、それを 1 保険会社だけで提供することは難しく、共同保険とするメリットになる。

なお、上述の共同保険を前提とした商品付帯方式での制度構築については、統一された補償内容の提供や事

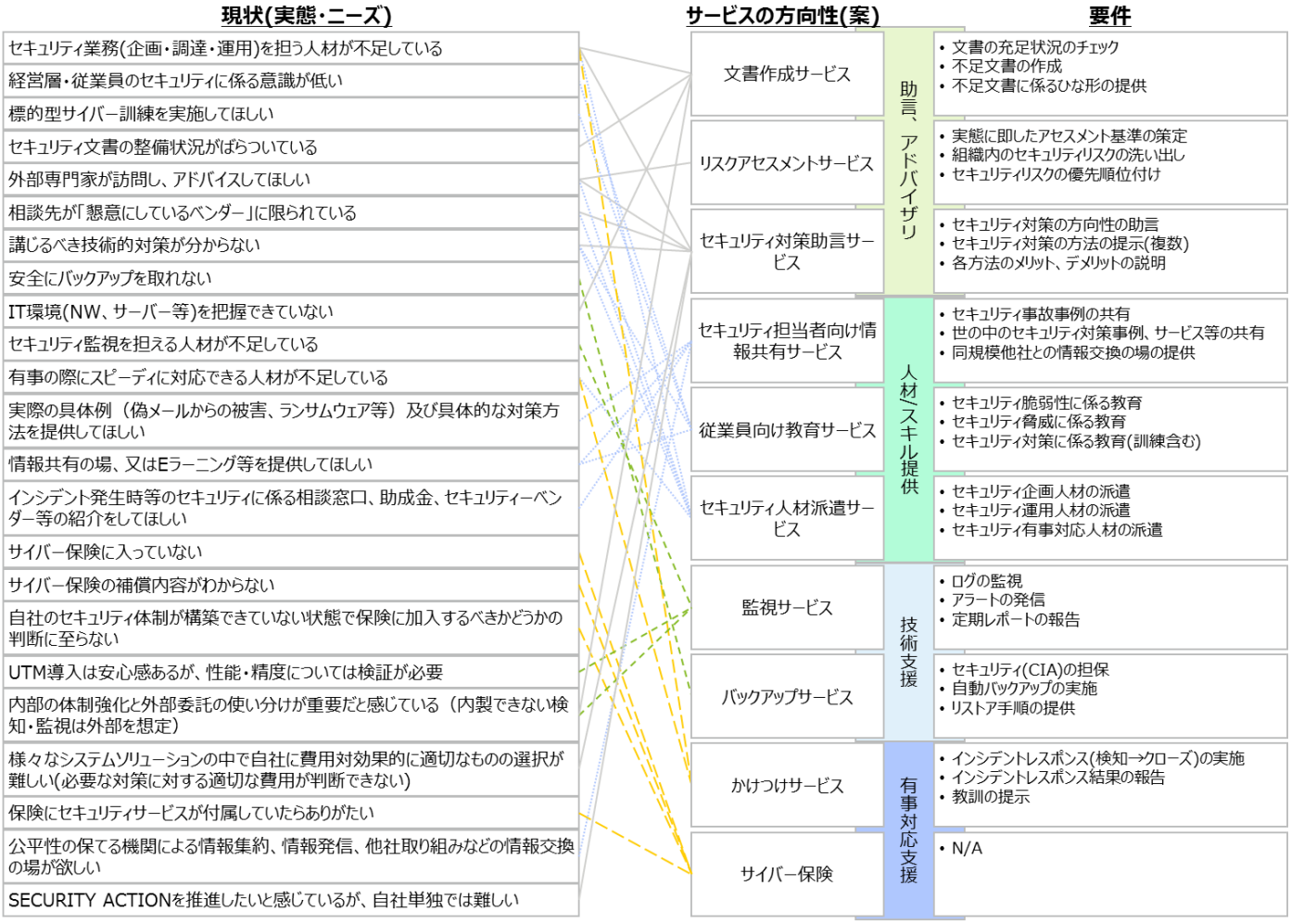
故情報の共有などを目的とした場合の手法の一案であり、他に当該目的を実現しうる手法（例えばお助け隊コンソーシアムが中心となり参画する各保険会社のサイバー保険に一定の標準形を作る、加えて事故情報を一元的に集約する機能を持たせるなど）が現実的であれば、必ずしも上述の手法にこだわる必要はない。

2．中小企業向けセキュリティ対策サービス案

（1）　サービス

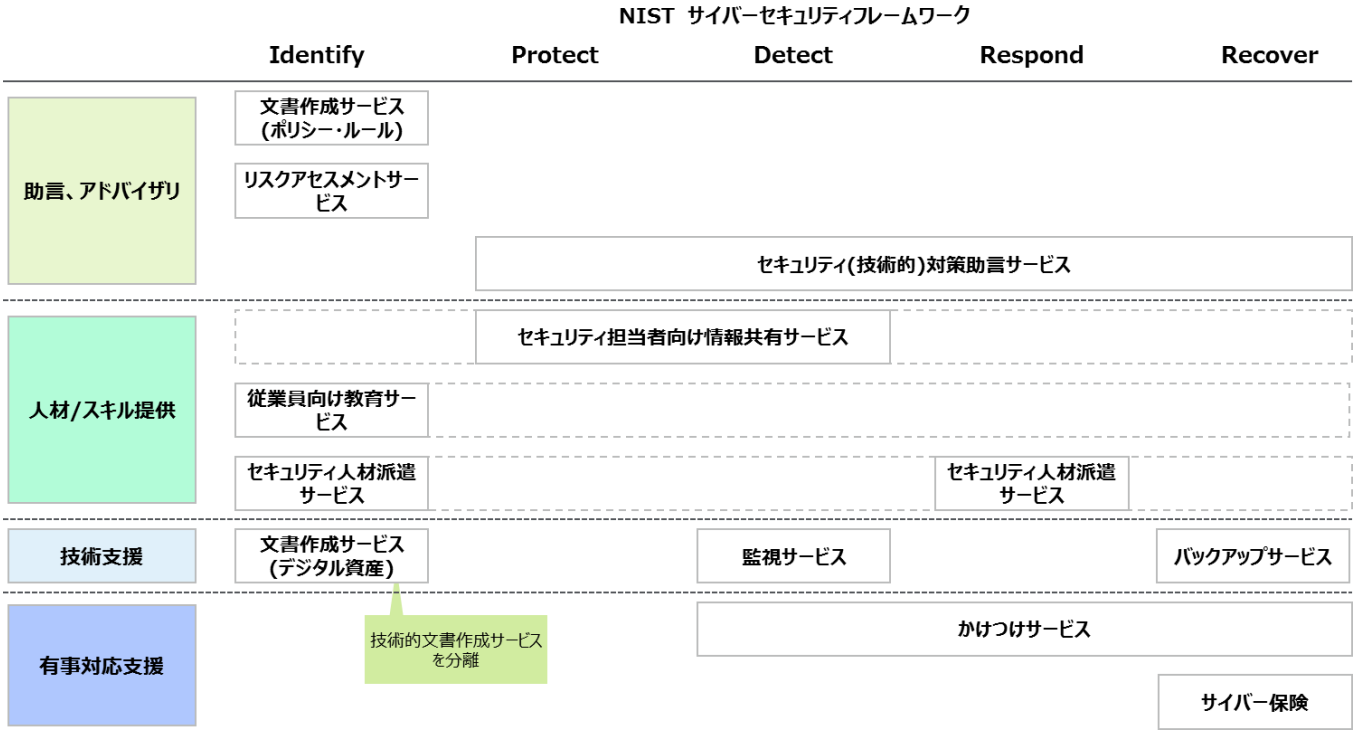
Ⅱ．１３で整理した課題に基づき、中小企業にとって必要と考えられるセキュリティ対策サービスを下記のとおり検討した。

【図 12】中小企業向けセキュリティ対策サービスの方向性



さらに、考えられるセキュリティ対策サービスを NIST サイバーセキュリティフレームワークに落とし込むと下記のとおりとなる。

【図 13】中小企業向けセキュリティ対策サービスと NIST サイバーセキュリティフレームワーク



今回の実証事業の提案書に、下記のとおり中小企業のセキュリティ対策に関する仮説を立てていた。

＜提案書記載の仮説＞

「組織体制や文書の整備を進め、セキュリティ意識が向上することで、次のステップとしてサイバー保険の手配や UTM 機器等の導入を始めとするセキュリティ対策が進展する」

今回の実証事業参加企業からの意見として「自社のセキュリティ体制が構築できていない状態で保険に加入するべきかどうかの判断に至らない」という課題が挙がったことからもわかるように、本仮説は一定正しいと考えられる。

また、セキュリティ意識が高い・対策の必要性を認識している企業の意見として出た「自社に必要なセキュリティ製品、サービスに対しては必要コストとして投資すべきと考えている（安くても性能が悪ければ意味がない）」が表しているように、中小企業の中にもセキュリティ強化に投資や手間をいとわない企業は一定数おり、第三者による評価を求める声も多い。

一方で、UTM を導入したいとの意向を踏まえ実際に設置を進めたところ「既設 UTM の存在が判明し、設置を断念した企業」が 12 社もいるなど、セキュリティ製品・サービスを導入していたにもかかわらず活用できていないケースも散見された。

愛知県では組織体制整備レベル・セキュリティ対策レベルに応じて A 群～C 群にカテゴリー分けを行った。しかし、レベルを向上する基準（文書・規定整備、アセスメント、組織体制整備等）と SECURITY ACTION とが必ずしも紐づいておらず、関係性をより明確にすべきだったと考える。

B 群企業の中でもサイバーセキュリティに関する意識が高い層（特に、サイバーセキュリティに関する意識が高く「SECURITY ACTION 二つ星」に近いと考えられる層）の抱える課題（ネットワークの把握、相談先に迷うなど）や UTM 手配、事後アンケート、事後ヒアリング等を通じて、次のステップに進むためのセキュリティサービスの選択肢（図 12）が多く、当該企業の置かれた環境に応じて選択する必要があることがわかった。ただし、中小企業が選択をすることは知識

量や情報量から難しく、コンサルティングやガイドラインなどの整備が求められている。

一方で、「中小企業向けセキュリティ対策サービスの方向性（案）」で提示したサービスにおいて、いくつかのサービスをまとめて提供しているケースもある。例えば、「リスクアセスメントサービス」と「サイバー保険」はサイバー保険の引受申請を行う際に同時に実施されることが多い。また、お助け隊実証事業の枠外であるが、実証事業説明会にて案内したところ好評であった、IPA のセキュリティマネジメント指導業務は「文書作成サービス」「セキュリティ人材派遣サービス」の機能を併せ持つ。

さらに今回の実証事業後には「監視サービス」と「駆けつけサービス」を組み合わせたサービスが提供されると考えられる。

それ以外に IPA の公表している情報セキュリティサービス基準適合サービスリストを活用することで、図 12 にてマッピングされたサービスは、既に存在するサービスで実現可能なものも多いが、コストも含めて自社に合ったサービスを見つける負担が依然残る。

今後は、SECURITY ACTION 二つ星の次のステップをガイドラインとして明確化し、お助け隊ブランドとしてガイドラインに即した製品・サービスを認証する仕組みが求められる。これにより中小企業のセキュリティ対策のロードマップがより明確化され、中小企業が自社に最適なセキュリティサービスを選ぶ一助となる。

（2） スキル・人材

参加企業の意見として「中小企業には人員的にセキュリティチームを構築することが困難」という意見がある一方、「内部の体制強化と外部委託の使い分け（検知・監視は外部）」「中小企業側にも最低限の知識は必要」といった中小企業側にも最低限の体制整備・知見が必要と認識している企業も多い。

UTM のパートにおいて、中小企業側が備えるべき要件として下記を挙げた中でも特に以下の点が重要である。

- UTM 設置担当者が自社のネットワーク構成を把握していること（管理者用 ID、パスワード含む）
- ネットワークの基礎知識（社内 LAN の設定が自力でできるレベル）を備えていること
- セキュリティに関する基礎知識（UTM が持つ機能の概要が理解できるレベル）を備えていること
- 自社のセキュリティ対策状況を把握していること（既設 UTM の有無の把握含む）

これらを支援するために IPA のセキュリティマネジメント指導業務のように、専門家が個社に相談・指導をすることがよいと挙げる企業も多く、外部に求める知見は情報処理安全確保支援士等の専門性が高い人材を求めていることがわかる。

中小企業にサービスを提供する側に必要なスキル・人材としては、技術的な面（ネットワークおよび IT システムのセキュリティ）に関する知識が幅広く必須であり、また、図 12 で提示した「中小企業向けセキュリティ対策サービスの方向性（案）」の各サービスに関する幅広い知識が求められる。それらの人材として情報処理安全確保支援士が最適であるが、IPA の HP 内で確認可能な「情報処理安全確保支援士検索サービス」によると、資格保持者は約 18,000 人存在するものの、勤務地住所を“関東”と公開している方が多く、情報処理安全確保支援士がいわゆる都心に集中しているように見受けられる。全国でサービス提供を実現するためのリソースを一定数確保するには更なる資格保持者が必要であり、都心以外の地域にも資格保持者をさらに増やしていくためには、本資格の維持に係る費用（講習費用等）負担に対する公的な補助を行う等の対策が一つの方法であると考える。

中小企業側は IT パスポート試験の取得を目指すことでスキル取得の第一歩を進めていく必要がある。

（3） 無関心層への対応

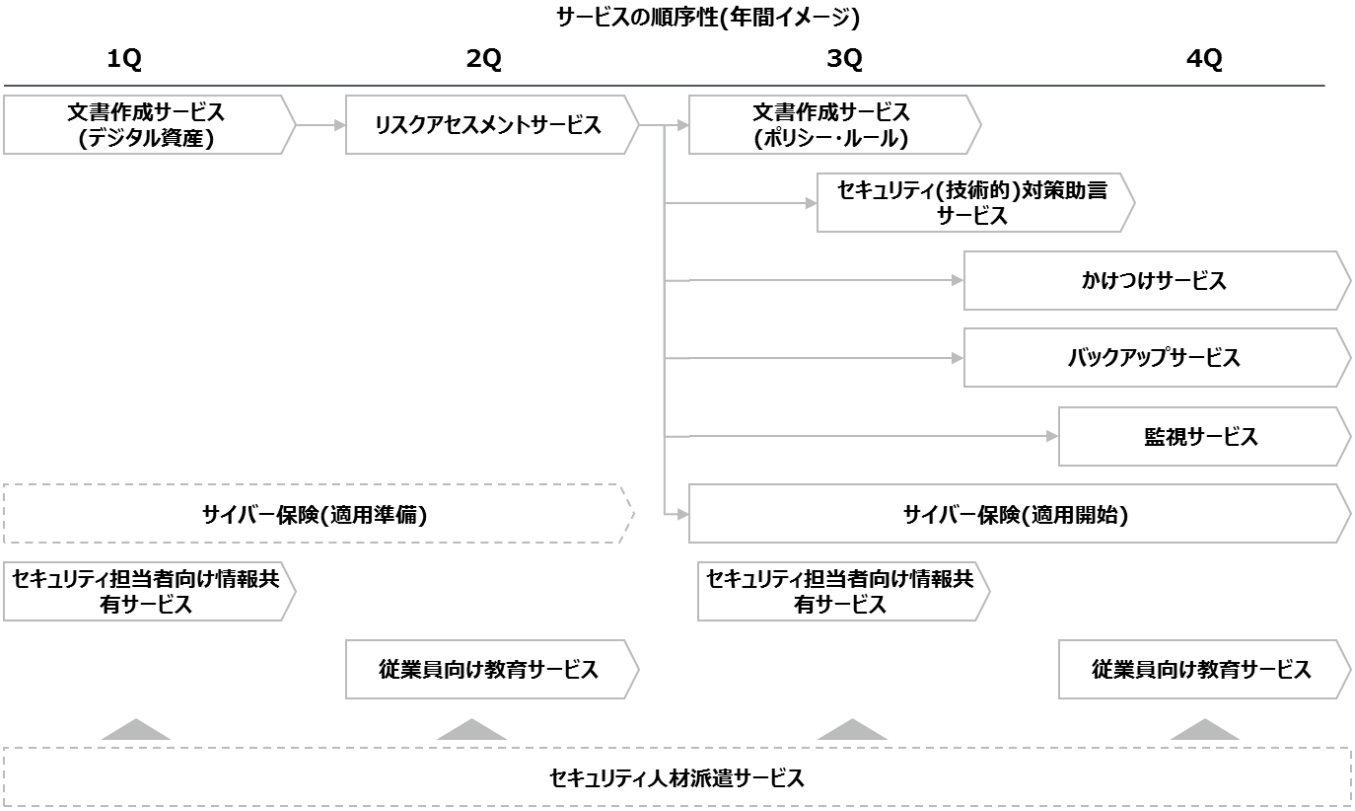
中小企業側が備えるべきスキル・人材以前の問題として、今回実証事業で痛感した「無関心層」への対応が挙げられる。一定数の企業が実証事業への参加を宣言したものの、セミナーへの参加をほとんどせず UTM 手配においても関心を示さないなど、本実証事業への関心を示さなかった。これらの層に対しては対策サービス導入、スキル・人材以前の問題として、サイバーセキュリティへの関心を持ってもらうため、業界団体や融資をする地銀などから「SECURITY ACTION 取得」や「お助け隊ブランドとして認証された製品・サービスを利用していること」を呼びかけ、取引や融資の際に中小企業にとって有利となるような契約条件を標準とすること等でセキュリティへの関心を高める活動などが効果的であると考えられる。

（４）　参考：サービスの順序性

また、対策サービスの組み合わせについては順序があり、セキュリティの文書も体制も整っていない企業が、高度な機器を導入しても活用されないことが想定される

そこで本サービスの順序性について検討した内容を下記に示す。

【図 14】中小企業向けセキュリティ対策サービスの順序性



３．実証終了後のサービス提供の可能性

（１）　実証終了後のサービス継続について

本実証事業で提供した据置型 UTM およびクラウド型 UTM、コールセンターや駆けつけ隊については UTM の付随サービスとして一部連携体制や機能に変更があるものの、原則として継続サービスとして提供する。

①　据置型 UTM

【図 15】据置型 UTM の継続サービスについて

実証事業終了後のUTM提供

実証事業終了後は以下のサービスを有償で提供する。

・本体のみ

メーカー標準サポート
- 技術支援 - カスタマーサポートセンターの利用（受付時間： 平日9:00～18:00）
- WEBによるサポートの提供
- 交換品先出しセンドバック保守（受付時間： 平日9:00～18:00）
- ファームウェアアップグレード

以下の1年間ライセンス
- -ゲートウェイアンチマルウェア/侵入防御/アプリケーション
- -コントロール/コンテンツフィルターサービス
- -地域IPフィルタ/ボットネットフィルタ

・本体＋遠隔監視

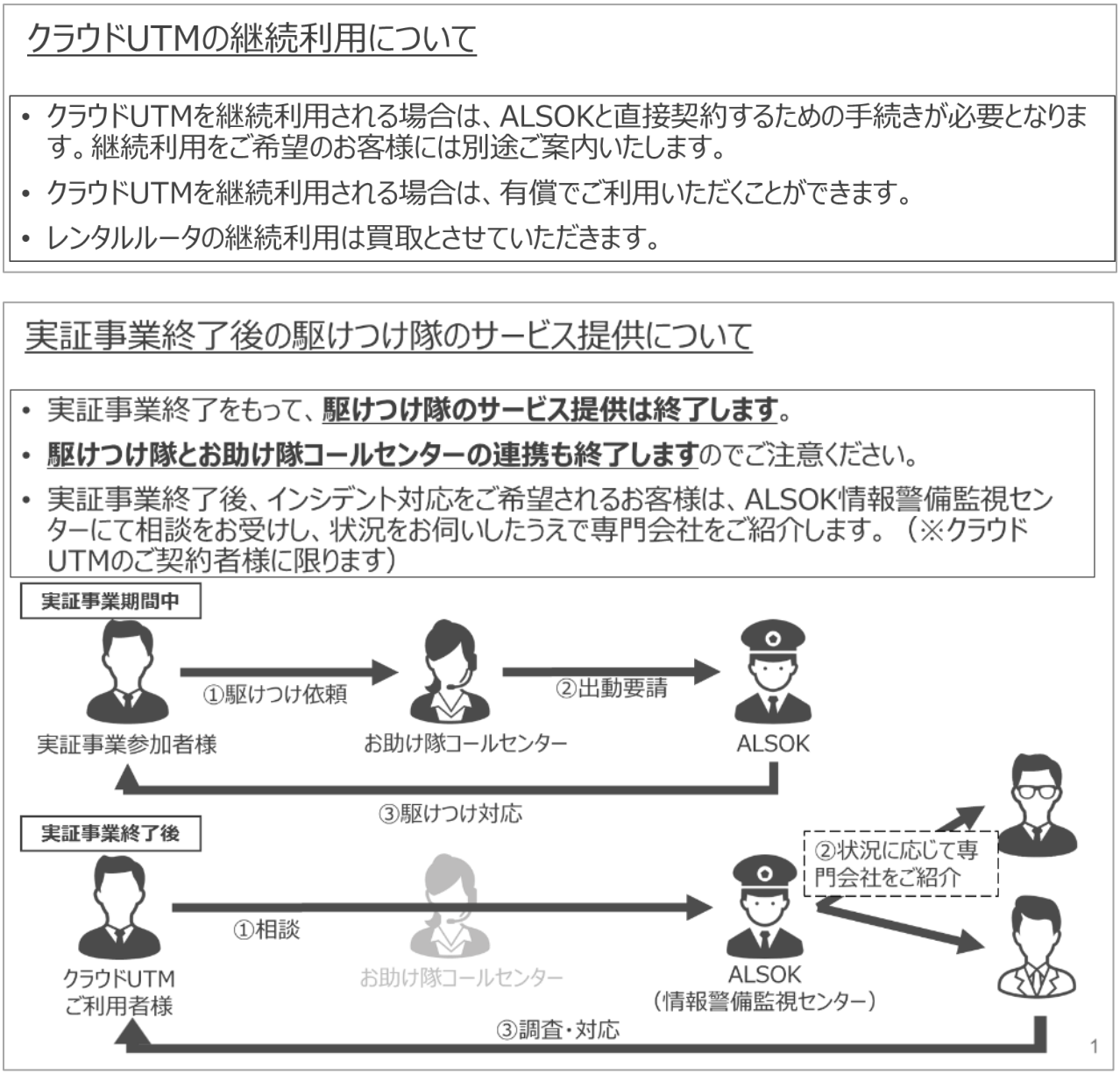
初期設定費用
メーカー標準サポート
- 技術支援 - カスタマーサポートセンターの利用（受付時間： 平日9:00～18:00）
- WEBによるサポートの提供
- 交換品先出しセンドバック保守（受付時間： 平日9:00～18:00）
- ファームウェアアップグレード

以下の1年間ライセンス
- -ゲートウェイアンチマルウェア/侵入防御/アプリケーション
- -コントロール/コンテンツフィルターサービス
- -地域IPフィルタ/ボットネットフィルタ

SonicWall遠隔監視（対応時間：平日9:00～17:00）

② **クラウド型 UTM**

【図 16】クラウド型 UTM の継続サービスについて



（２） 支援体制の必要性

上記のとおり、今回の実証事業で提供したサービスを継続するだけでは、Ⅲ． ２（１）で述べたとおり、中小企業の置かれた環境すべてには対応しきれない。そのため、より広範囲な支援体制が求められる。

具体的には、本章で述べた以下 5 点が必要とされる。

① **事故データ共有体制の構築（高品質かつニーズに合った保険商品開発）**

② **SECURITY ACTION 二つ星の次のステップのガイドライン（セキュリティ対策のロードマップの明確化）**

③ **お助け隊ブランドとして製品・サービスを認証する仕組み（最適なセキュリティサービスの選択支援）**

④ **「情報処理安全確保支援士」普及策**

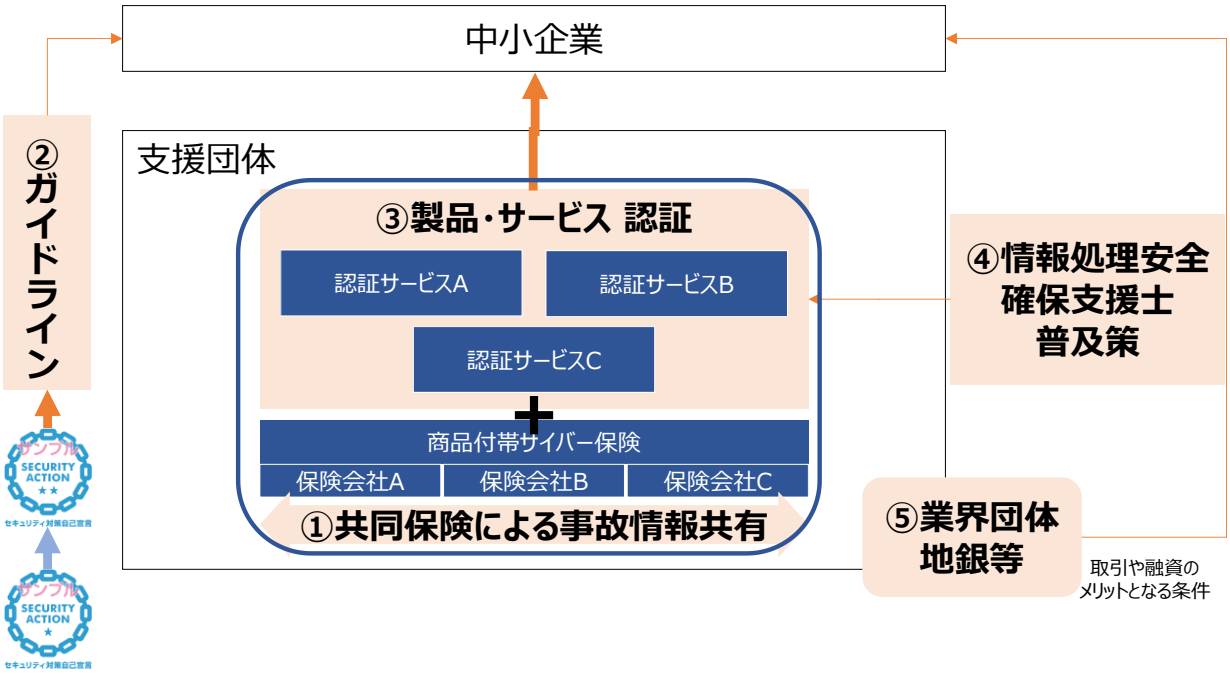
⑤ **取引・融資条件への組み込み（無関心層の底上げ）**

このような体制構築に向けて、本実証事業（8 地域）に参加した企業を中心として検討を継続することが望ましいと考

える。また、図 17 の青枠で囲んでいる「①+③」については、次年度実証事業で検討を進めることによって、本支援体制の構築が加速されると考える。

これらを実現する支援体制を整理すると下図のようなイメージになる。

【図 17】中小企業向け支援体制の必要性について



以上