令和２年度中小企業サイバーセキュリティ対策支援体制構築事業

（サイバーセキュリティお助け隊事業）

（実証対象：青森県、秋田県、宮城県、山形県）

成果報告書

請負事業者：東北インフォメーション・システムズ株式会社

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

目次

サマリー

本報告書は、東北インフォメーション・システムズ株式会社（以下「TOiNX」という。）が「令和２年度中小企業サイバーセキュリティ対策支援体制構築事業」において実施した実証内容を報告するとともに、結果に基づき中小企業のサイバーセキュリティ対策について提言するものである。

宮城県、山形県、秋田県、青森県内の中小企業 40 社を対象に、以下のサイバーセキュリティ対策サービスを提供し、それぞれの結果から、中小企業のサイバーセキュリティ対策の実態を把握し、今後中小企業が継続的に利用可能なサービスおよび保険について検討を実施した。

- 簡易なセキュリティ診断
- 中小企業等からのサイバーセキュリティに関する相談の受付および対応
- セキュリティ対策機器（UTM）
- 標的型攻撃メール対応訓練
- 脆弱性診断
- 制御システム簡易リスクアセスメント

1. 背景・目的

1.1 背景

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。また、同会議所が同年 5 月に公表した調査では、大企業・中堅企業 118 社に「取引先がサイバー攻撃被害を受け、影響が自社に及んだ経験があるか」を調査したところ、25%の企業が経験ありと回答した。

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

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

そのため、上述のような中小企業の実態・ニーズを踏まえ、損害保険会社、IT ベンダー、地元の団体等が連携して中小企業セキュリティ対策支援体制を構築し、中小企業の実態やニーズをよりきめ細かく把握することで、その実態に即したサービス内容やこれに必要な人材、体制等を明らかにし、中小企業の実態やニーズに合致した持続可能なセキュリティ対策支援体制を構築することで、中小企業のセキュリティ対策強化を図る必要がある。

1.2 目的

本実証事業は、令和 2 年度においても引き続き、「2.4. 実施内容」を通じて、中小企業におけるサイバーセキュリティの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定着させていくことを目的として、持続可能な中小企業サイバーセキュリティ対策支援体制を構築する。

2. 実証事業の概要

2.1 実証対象（地域／産業分野）の選定

TOiNX および再委託先の本社または営業所の所在地である「宮城県」「山形県」「秋田県」「青森県」の 4 県を実証対象地域とした。

表 1　本提案実施企業の所在県

本提案実施企業	所在県	備考
TOiNX 本社	宮城県	
株式会社ハイテックシステム（以下、HTS） 本社	山形県	再委託先
株式会社アキタシステムマネジメント（以下、ASM） 本社	秋田県	再委託先
TOiNX 青森営業所	青森県	

昨年度のサイバーセキュリティお助け隊事業で実施した東北の県は「岩手県」「宮城県」「福島県」である。この 3 県以外の東北の県は中小企業の実態やニーズを把握できていない。本提案では、東北地域から空白地帯である中小企業の実態を把握するために、昨年度実施していない「山形県」「秋田県」「青森県」を実証対象地域に選定した。なお、宮城県は昨年度も実施しているが、「産業特性」の観点から対象地域に加えている。

昨年度のサイバーセキュリティお助け隊の成果報告書で「専門家の伴走型支援を含むワンパッケージ化」が重要であるとまとめられている。IT が発達した現在でも、すべてを遠隔で伴走型の支援を行うことは困難であると考える。「人」の顔が見え、安心・信頼していただけるサービスが必要である。これは中小企業の所在地の「地場企業」であることが大きな利点になる。本提案では、東北に根を下ろした地場企業が結束してサービスを提供する。東北の企業が東北地域を実証地域とすることに意義があると考える。

TOiNX は東北 6 県と新潟県に事業所がある東北電力および東北電力企業グループ各社へ SOC・CSIRT 支援サービスを提供している。また、HTS は、東北地域を中心に SOC サービスを提供している。

また、産業特性の観点から、情報システム産業のサプライチェーンを重点対象産業とした。対象企業の所在地は、宮城県になる。

そして、中小企業における制御システムのセキュリティ対策の実態を把握するために、製造業も重点対象産業とした。

これ以降、文章が冗長になるため、本文中は「サイバーセキュリティお助け隊事業」を「お助け隊」の略称で表記する。

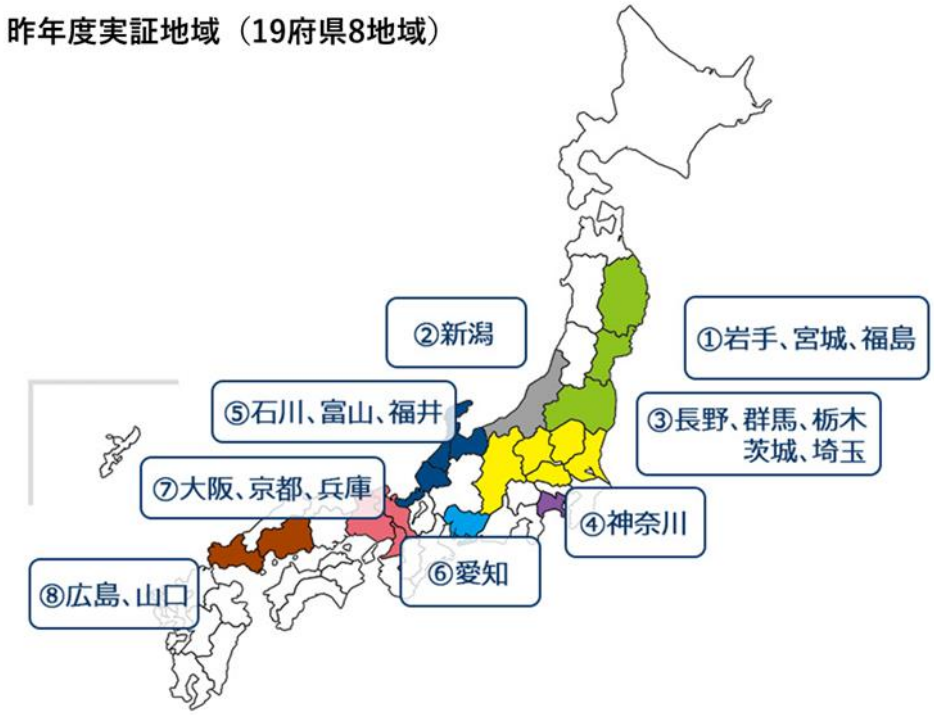


図 1 昨年度実証地域

図 2 本提案実証地域

2.2 スケジュール

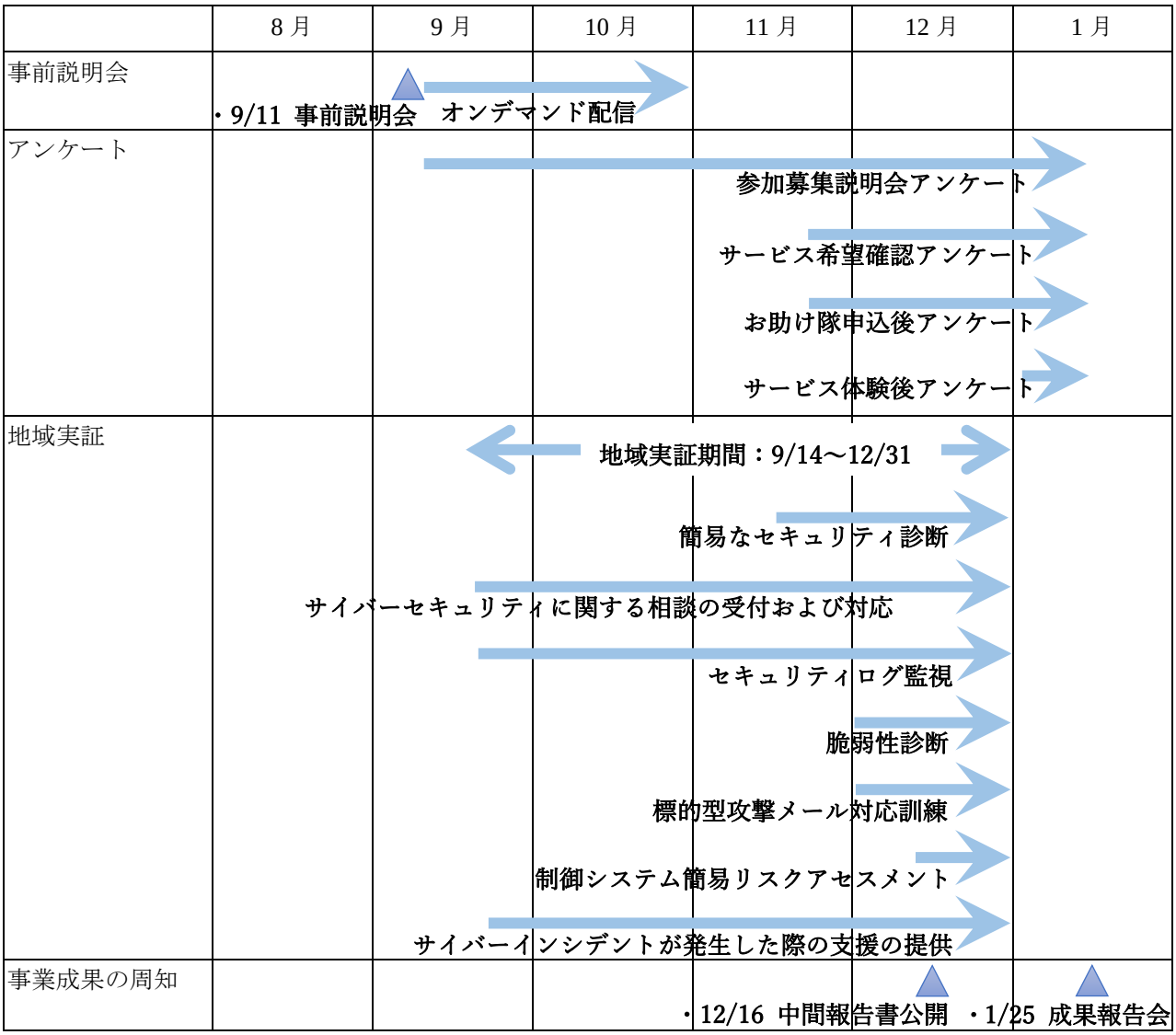


図 3 スケジュール

2.3 実証参加企業

2.3.1 募集活動

参加募集説明会の実証参加企業を募集するために、次を実施した。

- TOiNX のホームページに、実証参加企業募集説明会のページを公開した。
- 2020 年 9 月 9 日に東北経済産業局から次の協会の担当者に参加募集説明会の周知の協力依頼をした。
    - 青森県情報サービス産業協会
    - 秋田県情報産業協会
    - 山形県情報産業協会
- 青森県情報産業サービス協会へ、会員企業であるサンコンピュータから協力依頼をした。
- 秋田県情報産業サービス協会へ、会員企業であるアキタシステムマネジメントから協力依頼をした。
- 秋田商工会議所に、参加募集説明会のパンフレットを置いた。
- 山形銀行に「サイバーセキュリティお助け隊事業」と「参加募集説明会」の情報を提供した。
- 2020 年 9 月 10 日に東北経済産業局から、次の協会の会員に参加募集説明会の周知をした。
    - 一般社団法人宮城県情報サービス産業協会

次の企業の既存顧客を訪問し、サイバーセキュリティお助け隊事業の説明、参加募集説明会の案内、事業参加の依頼を行った。

- TOiNX：6 社
- 株式会社ハイテックシステム：18 社
- 株式会社アキタシステムマネジメント：3 社

参加募集説明会への参加企業数が想定を下回った。その後、申し込みが少なく、目標数に到達しなかったため、次の企業の既存顧客を訪問し、サイバーセキュリティお助け隊事業の説明、事業参加の依頼を行った。

- TOiNX：13 社
- 株式会社ハイテックシステム：15 社

結果として、以下のように実証参加企業の募集を達成することができた。

表 2 実証参加企業数

分類	小分類	達成企業数
地域	青森県	4 社
	秋田県	4 社
	山形県	22 社
	宮城県	10 社
合計		40 社
目標企業数		40 社

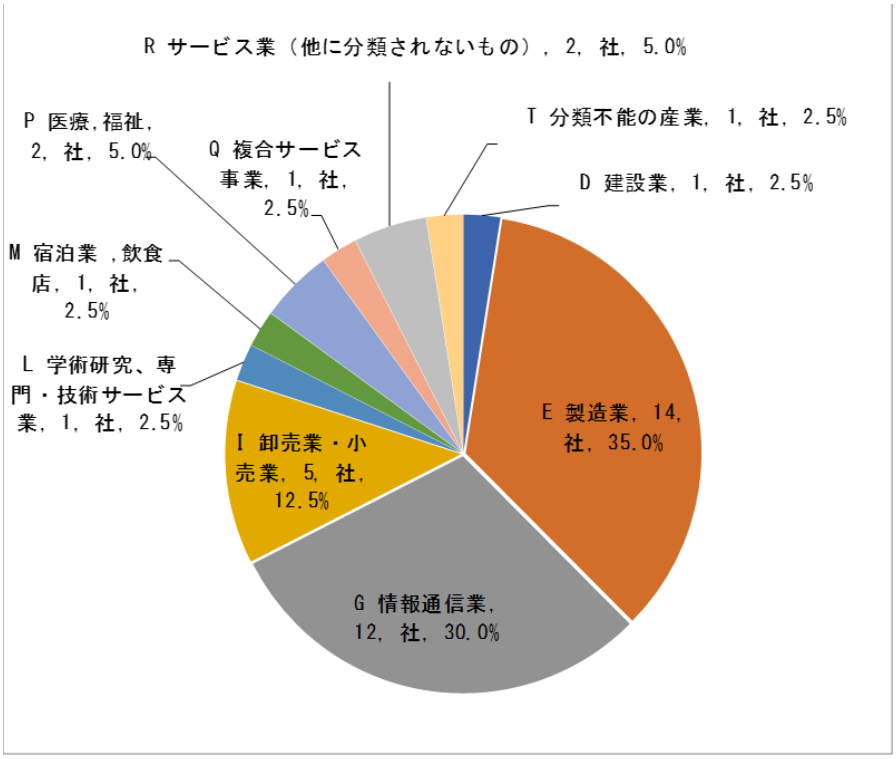
2.3.2 実証参加企業概要

（1） 業種の構成

表 3 業種別 実証参加企業数

業種分類	社数
D 建設業	1
E 製造業	14
G 情報通信業	12
I 卸売業・小売業	5
L 学術研究、専門・技術サービス業	1
M 宿泊業 ,飲食店	1
P 医療,福祉	2
Q 複合サービス事業	1
R サービス業（他に分類されないもの）	2
T 分類不能の産業	1
総計	40

図 4 業種別 実証参加企業数（n=40）



(2) 資本金の構成

表 4 資本金別 実証参加企業数

資本金	社数
5000 万円以下	31
1 億円以下	8
1 億円以上	1
総計	40

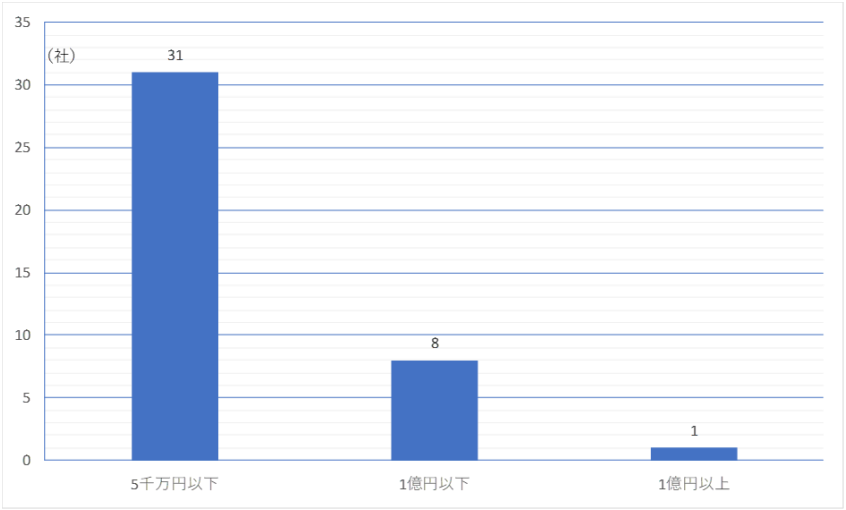


図 5 資本金別 実証参加企業数（n=40）

（3） 従業員数の構成

表 5 従業員数別 実証参加企業数

従業員数	社数
1～5 人	2
6～10 人	4
11～20 人	5
21～50 人	8
51～100 人	13
101～200 人	5
201～300 人	1
301 人以上	2
総計	40

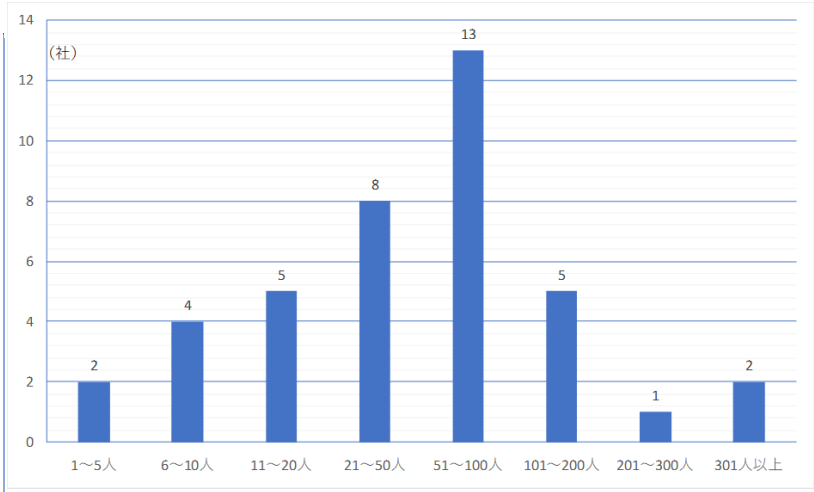


図 6 従業員数別 実証参加企業数（n=40）

（4） 実証参加企業エリアの分布

実証参加企業 40 社

青森県 4 社 秋田県 4 社 山形県 22 社 宮城県 10 社

図 7 実証参加企業のエリア分布

2.4 実施内容

2.4.1 中小企業等の実態把握

（1）セキュリティ実態を把握するための措置

表 6 セキュリティ実態把握サービス一覧

サービス名称	概要	実証参加企業数
a.セキュリティログ監視	UTM を設置し、ログを分析する。 NW 可視化ツールを導入し、インシデント対応支援を行う。	40 社
b.脆弱性診断	インターネットに公開されているサーバー（Web サイト等）の脆弱性診断を行う。	3 社
c.標的型攻撃メール対応訓練	疑似的な攻撃メールを訓練対象者に送付し、攻撃を体験する訓練を行う。URL リンクのクリックまたは添付ファイルの開封有無を集計する。	18 社
d.制御システム簡易リスクアセスメント	工場などの制御システムを利用している企業のセキュリティ対策状況を確認し、どのようなリスクがあるかを評価する。	2 社

各サービスの詳細を次に記す。

（a） セキュリティログ監視

UTM（Fortinet 社 FortiGate）を実証参加企業に設置し、ログを監視することで、中小企業のセキュリティ実態を把握した。また、HTS が開発した「WatchManBox MR」もすべての実証参加企業に導入した。

セキュリティログ監視で提供するサービスの詳細を下表に記す。

表 7 セキュリティログ監視一覧

機器・サービス	機能項目	機能内容
セキュリティログ監視	・通信ログ監視・分析 ・インシデント解析 ・インシデント対応支援	・24 時間 365 日ログ監視 ・インシデント通知（メール、24 時間 365 日） ・インシデント対策のコンサルティング ・月次セキュリティ分析レポート
UTM（ForitGate）	・インシデント検知 ・通信制御 ・通信ログ管理	【入口対策機能】 ・アンチウイルス ・不正侵入防止（IPS） 【出口対策機能】 ・アプリケーションコントロール ・SandBox（攻撃のプロアクティブな防御）
WatchManBox MR	・ユーザー環境調査（現状把握） ・エンドポイント監視 ・端末検知	・ネットワーク構成図自動作成 ・リモート接続（VPN） ・脆弱性診断機能（簡易型） ・無許可端末検知機能 ・マルウェア検知機能（ハニーポット） ・死活監視機能（Active Monitoring） ・3D グラフィック表示機能 ・リストアップ機能（CSV 出力）＆資産管理 ・Syslog 収集＆転送機能

(b) 脆弱性診断

インターネット上に公開している Web システム等に対して、プラットフォームと Web アプリケーションの脆弱性診断を実施した。このサービスを提供することにより、中小企業の次の実態を把握した。

脆弱性診断は、脆弱性を狙った攻撃に耐えうるかを検査するサービスである。診断ツールを使った診断のほか、手動による診断を用いて脆弱性の検出および評価を行った。各サービスの診断内容を次に記す。

a. プラットフォーム脆弱性診断

プラットフォーム脆弱性診断サービスは、通信機器・サーバーOS・ミドルウェアを対象に、既知の脆弱性の有無や設定の不備などを診断した。本サービスでは、ポートスキャンツール「nmap」と診断ツール「Nessus Professional」を利用した脆弱性診断を行った。脆弱性診断を行うことにより、既知の脆弱性や設定の不備を検出することができる。

b. Web アプリケーション脆弱性診断

個別に開発したアプリケーションに対して、攻撃者の立場で悪用可能な脆弱性の有無を診断した。攻撃者よりも先に脆弱性を把握することにより、被害を受ける前に対策を実施することができる。Web アプリケーション脆弱性診断ツールとして「Vex （Vulnerability Explorer)」を使用した。

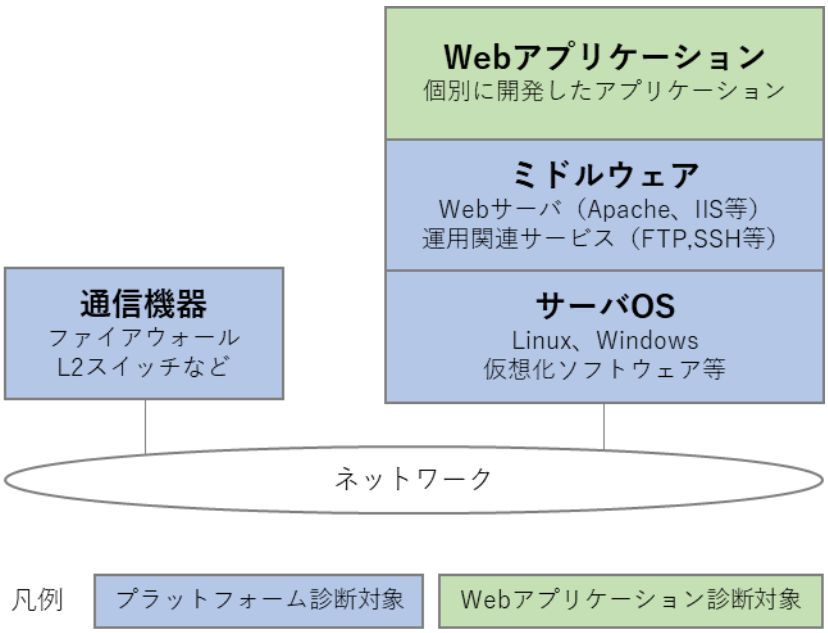


図 8 脆弱性診断対象イメージ図

（c） 標的型攻撃メール対応訓練

標的型攻撃メール対応訓練は、標的型攻撃を模したメール（以下、訓練メール）を実証参加企業指定のメールアドレスへ送信し、訓練メールを受信した際の訓練対象者の対応について訓練するものである。

このサービスを提供することにより、中小企業の次の実態を把握できる。

・標的型攻撃を受けた場合に攻撃が成功する可能性

一般的に机上の教育だけでは、効果は限定的である。本訓練では、標的型攻撃を模した訓練メールを訓練対象者に送ることにより､肌で感じてもらう(実感する)ことができた｡頭だけでなく「体」で覚えることが重要である。

攻撃者は添付ファイルを開かせようとする。添付ファイルを開かなければ、多くの標的型攻撃を防ぐことができる。本訓練により『安易に電子メールの「添付ファイルを開かない」ことを習慣づける』事で､実際に標的型攻撃を受けても､攻撃が成功する確率を低減することができたと考える。

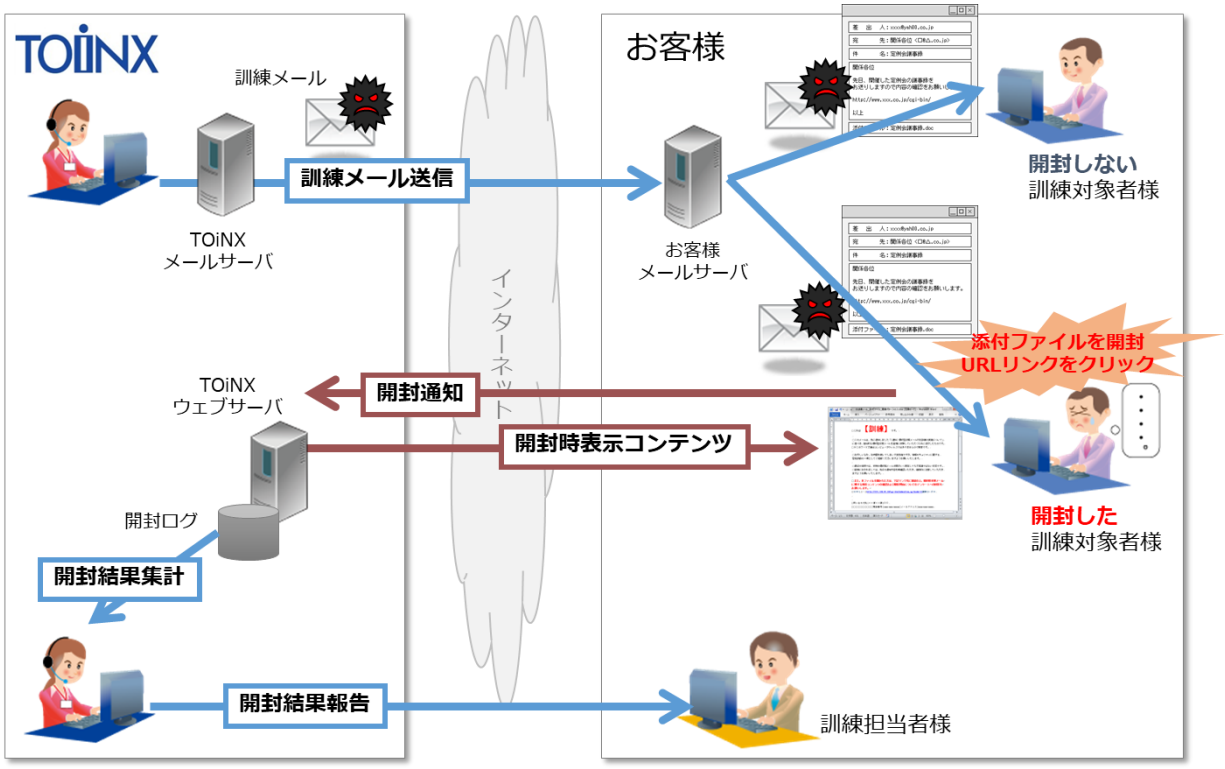


図 9 標的型攻撃メール対応訓練イメージ図

訓練メールには、注意喚起されている不特定多数に対する攻撃で実際に使われた文面を使用した。開封結果報告は、訓練対象者毎に開封有無と開封がある場合はその時間を報告した。

(d) 制御システム簡易リスクアセスメント

制御システムに対する脅威の動向や「表 8 制御システムリスクアセスメントに関わる各種ガイドライン」等を参照し、制御システムに対する典型的なサイバー攻撃シナリオを「

表 9 制御システムに対する典型的なサイバー攻撃シナリオ」のように整理した。さらに、各サイバー攻撃シナリオに対するセキュリティ対策が実施されているかという観点でチェックリストを作成し、リスクアセスメントを実施した。

表 8 制御システムリスクアセスメントに関わる各種ガイドライン

発行元	資料名
IPA	制御システムのセキュリティリスク分析ガイド
NIST	Cyber Security Framework（CSF）
NIST	SP 800-30（リスクアセスメント実施の手引き）
JESC	電力制御システムセキュリティガイドライン
JESC	スマートメーターシステムセキュリティガイドライン

表 9 制御システムに対する典型的なサイバー攻撃シナリオ

No.	サイバー攻撃シナリオ	選択
1	外部記憶媒体や外部持込 PC からのマルウェア感染	○
2	不正な攻撃用端末接続による中間者攻撃	
3	情報系システムを介した攻撃	
4	リモート接続端末を用いた攻撃	
5	制御系ネットワークにおける不正操作	○
6	無線 LAN に係わる攻撃	
7	機器に対する電磁波攻撃	
8	計測機器への攻撃	
9	外部インフラからの供給途絶による機能不全	
10	サプライチェーンリスク	
11	建屋への物理攻撃による機能不全	
12	安全系システムへの攻撃	
13	ログへの攻撃	
14	時刻同期システムの不具合による障害	
15	バックアップシステムや予備品への攻撃	
16	外部ネットワーク上のリソースへのサイバー攻撃	

ドイツ連邦政府情報セキュリティ庁（BSI）が作成・公開した「産業用制御システムのセキュリティ -10 大脅威と対策 2019-」（IPA 翻訳版）に記載されている制御システムに対する最新の 10 大脅威（表 10）によると「リムーバブルメディアや外部機器経由のマルウェア感染」や「インターネットおよびイントラネット経由のマルウェア感染」、「ヒューマンエラーと妨害行為」等が上位となっており、内部犯行に関わる脅威が高まっているものと想定される。

表 10　産業用制御システムのセキュリティ 10 大脅威（2019 年）

順位	脅威
1 位	リムーバブルメディアや外部機器経由のマルウェア感染
2 位	インターネットおよびイントラネット経由のマルウェア感染
3 位	ヒューマンエラーと妨害行為
4 位	外部ネットワークやクラウドコンポーネントへの攻撃
5 位	ソーシャルエンジニアリングとフィッシング
6 位	DoS / DDoS 攻撃
7 位	インターネットに接続された制御機器
8 位	リモートアクセスからの侵入
9 位	技術的な不具合と不可抗力
10 位	スマートデバイスへの攻撃

このような制御システムに対する脅威の動向をふまえ、今回提案する制御システム簡易リスクアセスメントにおいては、表 9 に記載したサイバー攻撃シナリオのうち内部犯行と関連が大きいと考えられる以下の 2 シナリオを選定した。さらに、シナリオごとに作成しているチェックリストから 3 つのチェック項目を選定することにより、簡易的なリスクアセスメントを実施した。

・外部記憶媒体や外部持込 PC からのマルウェア感染（No.1）

・制御系ネットワークにおける不正操作（No.5）

上記シナリオごとに選定したチェックリストは下表のとおりである。

表 11 サイバー攻撃シナリオ チェックリスト

サイバー攻撃シナリオ	チェック項目
外部記憶媒体や外部持込 PC からのマルウェア感染	許可された外部記憶媒体（USB メモリ等）のみが利用可能であること
	許可された外部持込 PC のみが利用可能であること
	許可された USB ポート、LAN ポートのみが利用可能であること
制御系ネットワークにおける不正操作	オペレータごとに ID/パスワードが設定されていること
	オペレータごとに操作ログを取得、収集していること
	重要な操作時には 2 人以上でのダブルチェックが行われていること

各チェック項目に対し、「文書調査」「ヒアリング」「現場確認」の 3 ステップでチェックを行った。

・文書調査

セキュリティに関わる文書調査により、チェックリストの各チェック項目が文書の観点から満たされているか否かのチェックを行う。

・ヒアリング

担当者へのヒアリングにより、チェックリストの各チェック項目が運用の観点から満たされているか否かのチェックを行う。

・現場確認

製造ラインやサーバールーム等の現場確認により、チェックリストの各チェック項目が運用の観点から満たされているか否かのチェックを行う。

表 12 サイバー攻撃シナリオ チェック結果 記入表

サイバー攻撃 シナリオ	チェック項目	チェック結果		
		文書	運用	総合
外部記憶媒体や外部持込 PC からのマルウェア感染	許可された外部記憶媒体（USB メモリ等）のみが利用可能であること			
	許可された外部持込 PC のみが利用可能であること			
	許可された USB ポート、LAN ポートのみが利用可能であること			
制御系ネットワークにおける不正操作	オペレータごとに ID/パスワードが設定されていること			
	オペレータごとに操作ログを取得、収集していること			
	重要な操作時には 2 人以上でのダブルチェックが行われていること			

チェック結果はチェックリストのチェック項目ごとに以下の観点で記載した。

○：対策がなされている

△：対策がなされているが、一部改善事項がある

×：対策がなされていない

「総合」欄のチェック結果の記載基準は以下のとおりである。

○：「文書のチェック結果が○である」かつ「運用のチェック結果が○である」

△：「文書のチェック結果が○である」かつ「運用のチェック結果が△である」、または「文書のチェック結果が△である」かつ「運用のチェック結果が○である」、または「文書のチェック結果が△である」かつ「運用のチェック結果が△である」

×：「文書のチェック結果が×である」かつ「運用のチェック結果が×である」

「シナリオ」欄のチェック結果の記載基準は以下のとおりである。

○：各チェック項目のチェック結果（「総合」欄）がすべて○である

△：各チェック項目のチェック結果（「総合」欄）に 1 つ以上△が含まれ、残りが○である

×：各チェック項目のチェック結果（「総合」欄）に 1 つ以上×が含まれる

チェックの結果「△」または「×」であった項目に関しては、対策例を含めて報告した。

また、組織的な対策の状況を確認するため、電力制御システムセキュリティガイドラインを参照し、「組織」「文書化」「運用・管理のセキュリティ」「セキュリティ事故の対応」の観点での要求項目からチェックリストを作成し、簡易的なリスクアセスメントを実施した。

表 13 組織的対策チェックリスト

区分	チェック項目
組織	経営層が制御システムにおけるセキュリティ対策に関わる体制構築に関わっていること
	制御システムにおけるセキュリティ管理責任者が任命されていること
	制御システムセキュリティに関わる教育を計画し、実施していること
文書化	制御システムセキュリティに関わる情報を文書化していること
運用・管理のセキュリティ	セキュリティ区画が明確になっていること
	セキュリティ区画には許可された者のみがアクセス可能となるセキュリティ対策がなされていること
	セキュリティ区画への入退室者の台帳を作成していること
セキュリティ事故の対応	セキュリティ事故発生時の対応体制と手順が明確になっていること
	セキュリティ事故発生時の対応に関わる周知や訓練を行っていること

(2) アンケート

次の情報を収集することを目的に Web アンケートを実施した。

①中小企業が置かれている状況

②サイバー攻撃とセキュリティ対策に関する認識と意識

③中小企業等がさらされているサイバー攻撃の実態

④セキュリティ対策関連サービスに関するニーズ（マーケティング）

⑤サイバーセキュリティ保険の認識と意識（加入状況含む）

⑥支援サービスの期待

⑦支援サービスの評価（満足度、効果）

⑧実証後提供サービスの意見、要望

アンケートは次のタイミングで行った。計画では中間報告時に実施する予定のアンケートがあったが、中間報告の実施時期が予定より遅くなったため、「サービス体験後」アンケートと名称を変えて実施した。

- 参加募集説明会時
- お助け隊参加申込後
- サービス希望確認
- サービス体験後
- 成果報告会時

(3) インシデント対応支援を実施した企業のヒアリング

8 社に対して、次のテーマで状況確認と意見交換を行った。

表 14 ヒアリングテーマ

テーマ	内容
インシデント対応について	・お助け隊参加前のインシデント対応方法 ・お助け隊のサービスの有効性 ・実証終了後のお助け隊のサービス利用
セキュリティ対策の実施状況について	・セキュリティ担当者の割り当てと人材育成 ・インシデント対応に関する予算、セキュリティ対策全体の予算 ・サイバーセキュリティ保険（内容、価格）
IT の大規模開発の分散した場所での業務について（※）	・事務所での開発の課題（障壁）と実現可能性 ・テレワーク形式の開発の課題（障壁）と実現可能性 ・希望する開発形態
今後のセキュリティ対策について	・希望するセキュリティサービス

※IT 関連企業のみヒアリング

2.4.2 地域実証の実施内容

(1) 地域実証の実施内容

次のサービスを提供した。

①簡易なセキュリティ診断

②中小企業等からのサイバーセキュリティに関する相談の受付および対応

③機器、ソフトウェア、サービス等による中小企業等の実態把握のための措置

④サイバーインシデントが発生した際の支援の提供

中小企業がサービスを体験することにより、サービスの必要性の評価、サービス内容・品質の満足度、サービスの在り方等の改善要望について、体験に基づくフィードバックを得ることができた。このフィードバックを元に実証終了後のサービスを検討した。

地域実証の体制図を下図に記す。

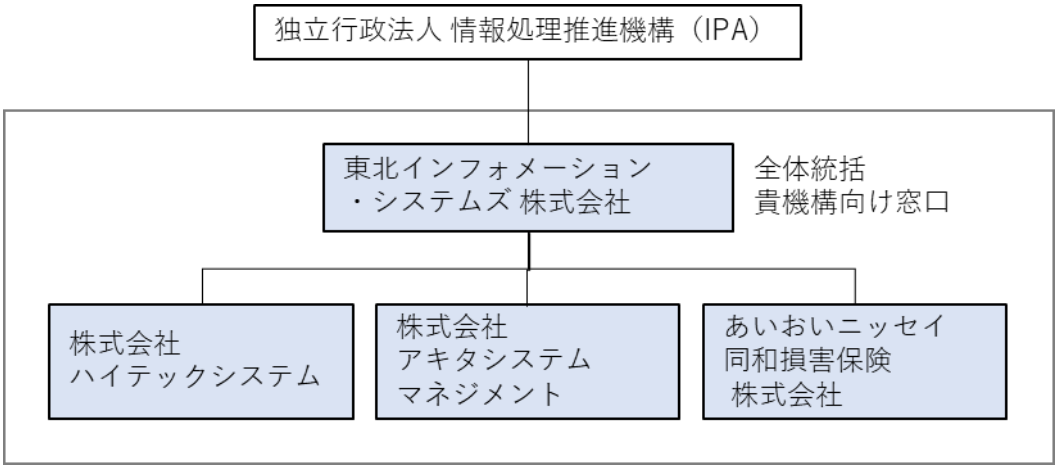


図 10 体制図

(a) ①簡易なセキュリティ診断

「簡易なセキュリティ診断」を次の手法で実施した。

i. IPA ツール活用

IPA の「5 分でできる！情報セキュリティ自社診断」を利用した。IPA が持っているデータと比較することで、中小企業と他企業の差を東北地域内だけでなく、他地域と比較できる。昨年度「5 分でできる！情報セキュリティ自社診断」を利用していた事業者があった。「5 分でできる！情報セキュリティ自社診断」を中小企業が利用することで PR になり、IPA のデータも増える。

また、組織的セキュリティ対策を確認するために IPA の「情報セキュリティ対策ベンチマーク」を利用した。こちらも、利点は「5 分でできる！情報セキュリティ自社診断」と同じである。

ii. 情報システム向けセキュリティ対策調査

具体的な情報システム向けセキュリティ対策の実施状況を調査するアンケートを行った。アンケートの内容は「表 21 サービス体験後アンケートの設問と回答選択肢」の Q13～Q21、「表 23 テレワークに関するアンケートの設問と回答選択肢」を参照。

（b）伴走型支援パッケージ

「②中小企業等からのサイバーセキュリティに関する相談の受付および対応」、「③a.セキュリティログ監視」「④サイバーインシデントが発生した際の支援の提供」を組み合わせたサービスは、昨年度のお助け隊の成果報告書で、対策普及に向けた取り組みの方向性のひとつである「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（以下、伴走型支援パッケージ）」に該当すると考えた。伴走型支援パッケージの体制図を下図に記す。

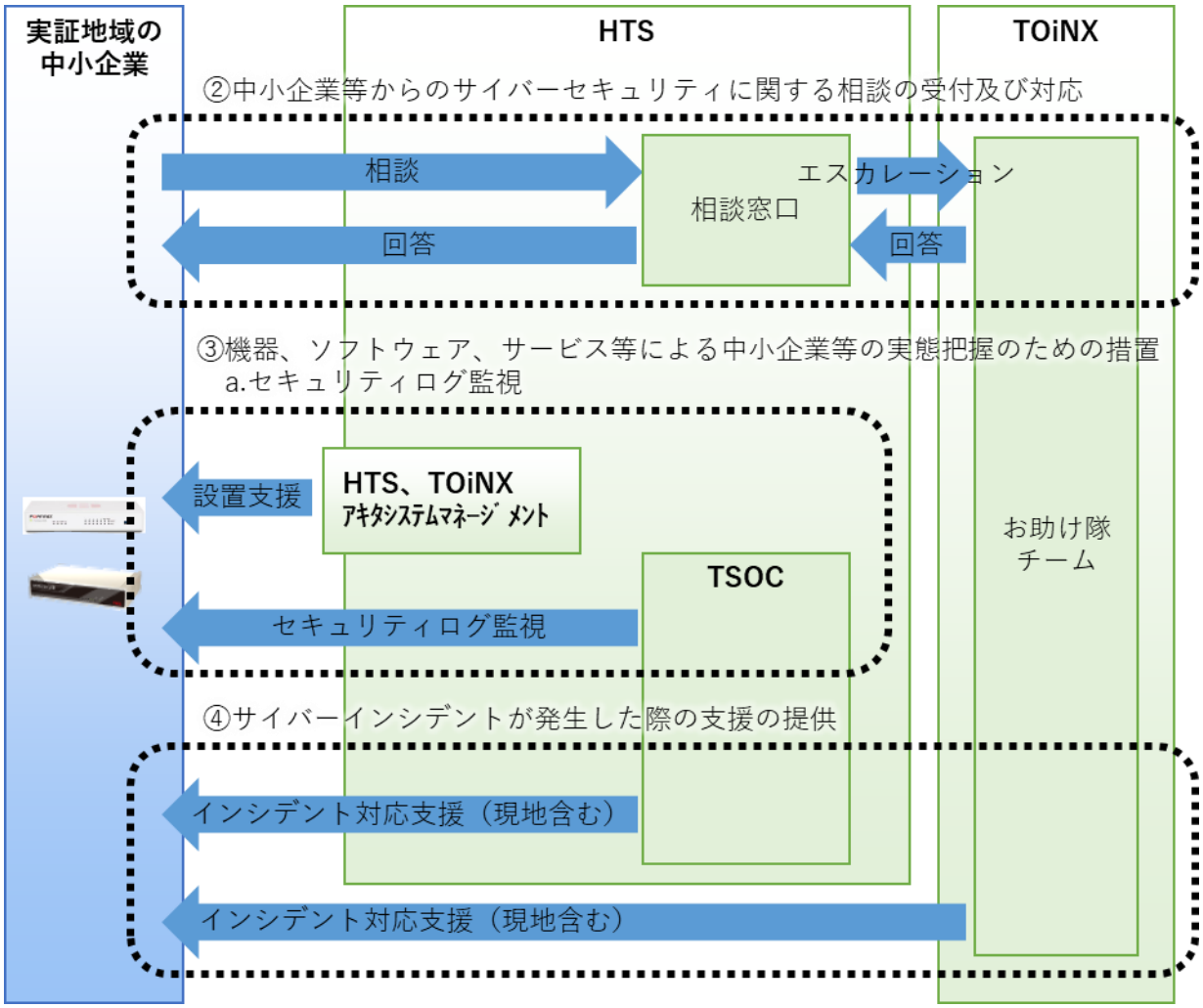


図 11 セキュリティログ監視関連体制図

次にそれぞれの支援サービスの内容の詳細を記す。

②中小企業等からのサイバーセキュリティに関する相談の受付および対応

相談の受付および対応は、2 段階に分けて行った。SOC サービスを提供する HTS が窓口となり、問合せ先を一本化した。受け付けた後は、問合せの内容により、下表の役割分担で対応を行った。

表 15 問合せ役割分担

企業名	役割	対応分野
HTS	・問合せ窓口 ・インシデント一次対応 ・TOiNX へのエスカレーション	・セキュリティ機器設置等の問合せ ・インターネット接続障害（インターネットが繋がらない等）の問合せ ・UTM で検知した内容に関する問合せ ・セキュリティインシデントに関する問合せ全般（ウイルス感染、不正侵入、情報漏洩、情報改ざん等）
TOiNX	・インシデント二次対応 ・インシデント以外の問合せ対応	・ウイルス感染後の調査や復旧に関する問合せ ・セキュリティ対策全般に関する問合せ ・セキュリティ関連制度に関する問合せ（SECURITY ACTION 等） ・お助け隊事業に関する問合せ ・制御システムセキュリティに関する問合せ

図 12 問合せ受付フロー

③機器、ソフトウェア、サービス等による中小企業等の実態把握のための措置

セキュリティログの監視は、HTS の SOC（以下、TSOC）が 24 時間 365 日行う。インシデントを検知した場合は、電子メールにて実証企業へ通知した。

また、セキュリティログを分析した結果をレポートに取りまとめ、月に一回レポートを提供した。

セキュリティログ監視の全体像を下図に記す。

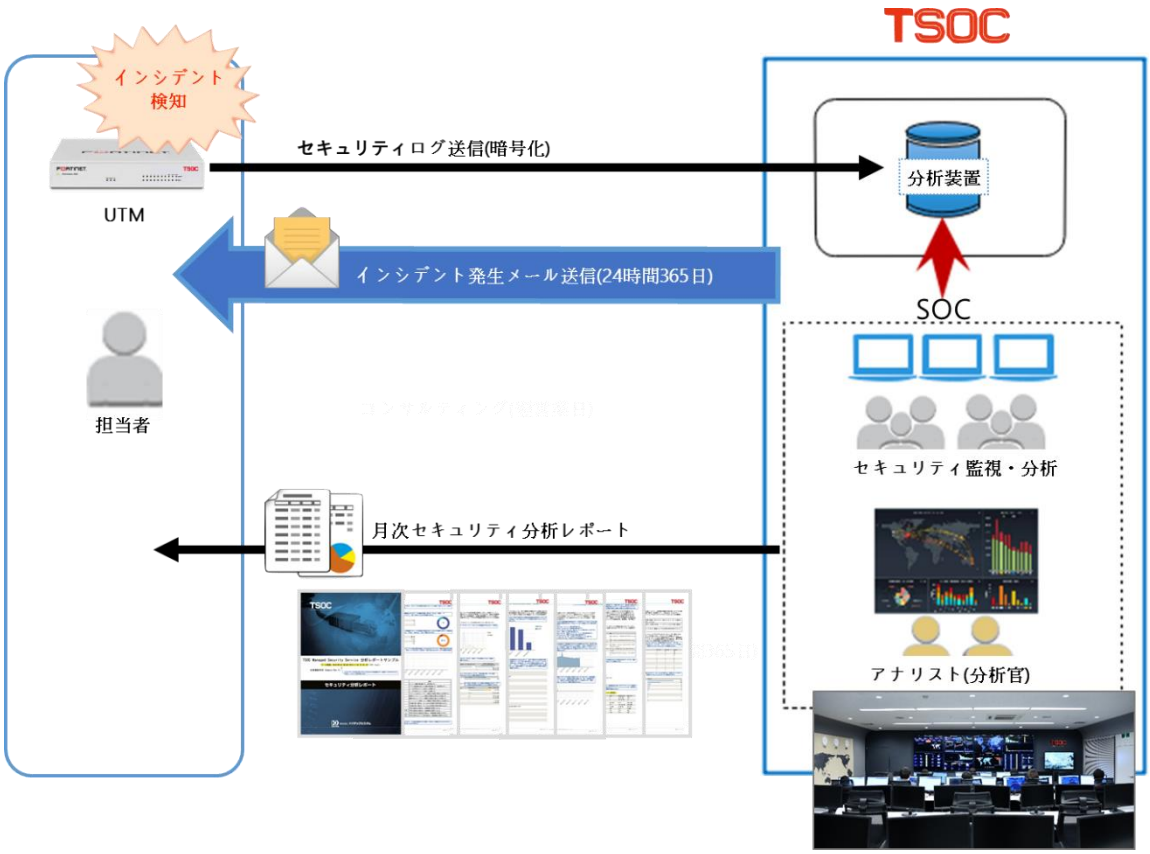


図 13 セキュリティログ監視

④サイバーインシデントが発生した際の支援の提供

サイバーインシデントは発生していないが、マルウェア感染が疑われる事例があった。TOiNX、HTS が連携して調査を行った。

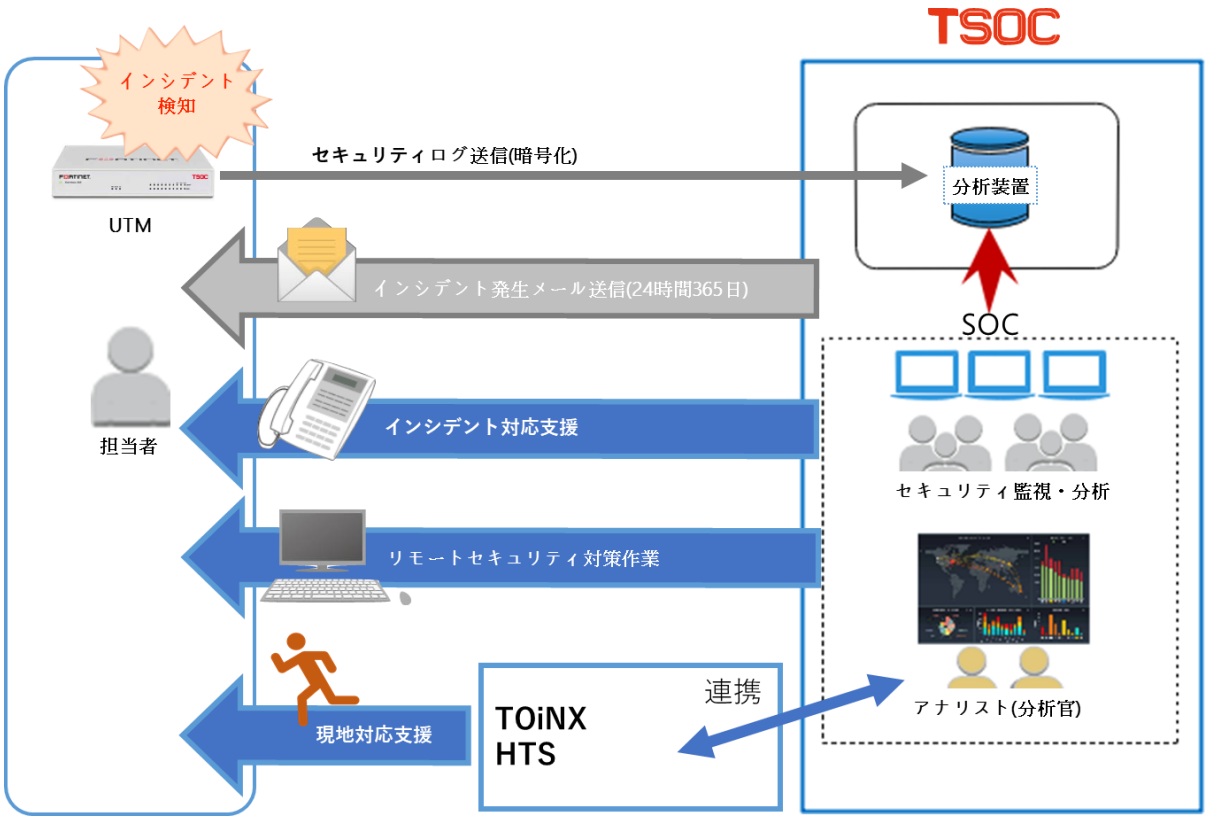


図 14 サイバーインシデント発生時対応

3. 実施結果

3.1 説明会の開催

3.1.1 参加募集説明会

表 16 参加募集説明会の概要

項目	内容
開催日時	2020 年 9 月 11 日（金）13:30 – 16:30 （2020 年 9 月 14 日（月）10:00 よりオンデマンド配信）
場所、形態	オンライン
参加者数	18 名（14 社）
アジェンダ	1. 開会挨拶（TOiNX） 2. サイバーセキュリティお助け隊事業概要（TOiNX） 3. 実証サービス内容（TOiNX） 4. 中小企業向けのセキュリティに関する制度・ガイドライン（ToiNX） 5. 中小企業の IT 管理者・利用者の視点から見た情報セキュリティ対策 （株式会社ハイテックシステム）

オンライン形式で実証参加企業の募集を行った。

参加募集説明会への参加数が想定よりも少なく中小企業のサイバーセキュリティへの関心が低いことがうかがえた。しかし、参加企業の実証事業参加率は 7 割弱（18 社中 12 社）と高い数値であり、サイバーセキュリティの必要性を理解してもらえる内容であったと考えられる。また、参加募集説明会開催時にはアンケートを実施しており、結果については後述の「3.2.1 アンケートによる実態把握結果」を参照。

図 15 事前説明会配信風景

図 16 事前説明会事務局

3.2 実態把握結果

3.2.1 アンケートによる実態把握結果

次のアンケートを実施した。アンケートの実施結果は「4 考察」を参照。

表 17 実施アンケート一覧

アンケート名称	実施期間	対象企業数	回答数	回答率
参加募集説明会アンケート	9 月 11 日～1 月 15 日	42 社	32 社	76%
お助け隊参加申込後アンケート	11 月 20 日～1 月 15 日	40 社	30 社	75%
サービス希望確認アンケート	11 月 20 日～1 月 15 日	40 社	29 社	73%
サービス体験後アンケート	1 月 5 日～1 月 15 日	40 社	21 社	53%
成果報告会アンケート	1 月 14 日～1 月 18 日	20 社	18 社	90%
テレワークに関するアンケート	1 月 14 日～1 月 18 日	40 社	13 社	33%

各アンケートの設問と回答の選択肢は次のとおり。

表 18 参加募集説明会アンケートの設問と回答選択肢

設問	回答選択肢
Q4. 本実証事業を知ったきっかけを教えてください。	IPA サイト
	採択事業者の紹介
	商工会議所等の紹介
	各種関連団体の紹介
	知人・友人等の紹介
	その他
Q5. サイバーセキュリティお助け隊事業に期待する事項を教えてください （複数選択）	セキュリティ対策の妥当性確認
	セキュリティの向上
	セキュリティ対策助言の入手
	セキュリティ関連情報の入手
	セキュリティ製品・サービスの利用
	その他
Q6. 貴社についてご回答ください。業種	農業、林業
	漁業
	鉱業、採石業、砂利採取業
	建設業
	製造業
	電気・ガス・熱供給・水道業
	情報通信業
	運輸業、郵便業
	卸売業・小売業
	金融業、保険業
	不動産業、物品賃貸業
	学術研究、専門・技術サービス業
	宿泊業、飲食店
	生活関連サービス業、娯楽業
	教育学習支援業
	医療、福祉

	複合サービス事業
	サービス業（他に分類されないもの）
	公務（他に分類されるものを除く）
	分類不能の産業
Q7. 貴社についてご回答ください。資本金	3 億円以下
	1 億円以下
	5000 万円以下
Q8. 貴社についてご回答ください。従業員数	1～5 人
	6～10 人
	11～20 人
	21～50 人
	51～100 人
	101～200 人
	201～300 人
	301 人以上
Q9. サイバーセキュリティ体制についてご回答ください。セキュリティ担当者	専任
	兼任
	アウトソース（他社サービス利用、委託）
	明確にきまっていない
Q10. サイバーセキュリティ対策の相談先	あり
	なし
Q11. インシデント発生時の相談先	あり
	なし
Q12. 取引先からのセキュリティ対策の要求	あり
	なし
Q13. サイバー攻撃の被害有無	あり
	なし
Q14. セキュリティ対策の年間予算（人件費を除く）	1000 万円以上
	1000 万円未満
	500 万円未満
	100 万円未満
Q15. サイバー攻撃とセキュリティ対策に関する認識	している

について「SECURITY ACTION」を宣言されていますか	していない
Q16. サイバー攻撃に遭い、事業継続に影響する被害を受ける可能性があると思いますか	思う
	思わない
	わからない
Q17. 自社のセキュリティ対策状況の自己評価をご回答ください	十分
	不十分
	わからない
Q18. サイバー攻撃の状況について不審メールを受信したことがありますか	ある
	ない
Q19. ウイルス（ランサムウェアを除く）に感染したことがありますが	ある
	ない
Q20. ランサムウェアに感染したことがありますか	ある
	ない
Q21. 情報漏洩の疑いがあること等によりフォレンジック調査を外部に依頼したことがありますか	ある
	ない
Q22 セキュリティ対策について　セキュリティ対策導入の障壁･課題に該当する項目を選択してください（複数選択）	費用を捻出することが困難
	人的リソースが不足
	対策を検討する要員の知識が不足
	セキュリティ対策の効果が不明

表 19 お助け隊参加申込後アンケートの設問と回答選択肢

設問	回答選択肢
Q1. 回答いただく方の組織の立場をお答えください。	1. 経営層
	2. 管理職
	3. 一般職
Q2. サイバーセキュリティお助け隊事業に参加いただいた動機・理由をお答えください。（複数選択）	① セキュリティサービスを体験したい
	② セキュリティ対策水準を向上させたい
	③ セキュリティ要員の負荷を軽減したい
	④ セキュリティ対策に取り組んでいくきっかけとしたい
	⑤ 無償だから
Q3. 地域実証（提供するサービス）に	① UTM によるサイバー攻撃防御

期待することを回答ください。 （複数選択）	② UTM によるサイバー攻撃の実態把握
	③ 可視化ツール（WatchManBox MR）を活用したインシデント遠隔支援
	④ セキュリティインシデント発生時の駆け付け対応
	⑤ セキュリティに関する相談対応
	⑥ 簡易セキュリティ診断による自社セキュリティ対策実施状況の評価
	⑦ 標的型攻撃メール対応訓練によるリスク把握および意識向上
	⑧ Web アプリケーション診断による公開 Web の脆弱性検出
	⑨ 制御システム簡易リスクアセスメントによるリスクの見える化
Q4. サイバーセキュリティ保険に加入していますか。	加入している
	加入していない
Q5. ※設問 Q4 で「加入している」と回答された方 加入した理由をお答えください。	（自由記述）
Q6. ※設問 No4 で「加入していない」と回答された方 加入していない理由をお答えください。	① サイバーセキュリティ保険の存在を知らない
	② 自社に必要ないと思う
	③ サイバーセキュリティ保険のメリットが分からない
	④ 自社のサイバー攻撃を受けるリスクを把握していない
	⑤ 保険の加入手続きが面倒
	⑥ 価格面で加入に至っていない
	⑦ 保険の加入方法が分からない
Q7. サイバーセキュリティ保険の補償範囲のご希望を教えてください。 どちらの補償を希望されますか？	① 損害賠償
	② 費用損害
	③ どちらも
Q8. どのような事象の補償を希望されますか？ （複数選択）	① 他人の情報の漏えいまたはそのおそれ。ただし、ネットワーク上に存在する電子情報の漏えいに起因するものに限る（本実証事業と同条件）
	② クレジットカードの電子情報漏えい
	③ 個人情報の電子情報漏えい
	④ マルウェアの調査・対応（外部への調査、ランサムウェアによるファイル暗号化対応費用など）

	⑤ 紙や外部記憶媒体などの「物」に記録された他人の情報の紛失・盗難
Q9. サイバーセキュリティ保険にかけても良い価格を教えてください。補償範囲により価格が変動しますが、支払うことが可能だと思われる価格を選択してください。	① 3,000 [円/月]程度 （ 36,000 [円/年]程度）
	② 5,000 [円/月]程度 （ 60,000 [円/年]程度）
	③ 10,000 [円/月]程度 （120,000 [円/年]程度）
	④ 15,000 [円/月]程度 （180,000 [円/年]程度）
	⑤ 20,000 [円/月]程度 （240,000 [円/年]程度）
	⑥ わからない

表 20 サービス希望確認アンケートの設問と回答選択肢

設問	回答選択肢
Q1. 「Web アプリケーション脆弱性診断」の希望有無を回答ください。	1.希望しない
	2.希望する
Q2. Q1 で「希望する」と回答された方は、診断対象の URL を記載してください。	（自由記述）
Q3. Q1 で「希望する」と回答された方は、診断対象ページ数（概数で可）を記載してください。	（自由記述）
Q4. Q1 で「希望する」と回答された方は、診断の希望日時があれば教えてください。ただし、11 月 23 日～12 月 25 日の平日日中（9:00-17:00）の期間内でご指定下さい。	（自由記述）
Q5. 「制御システム簡易リスクアセスメント」の希望有無を回答ください。	1.希望しない
	2.希望する
Q6. 簡易リスクアセスメントを希望する制御システムの概要（どのような処理を行っているか）を記載してください。	（自由記述）

表 21 サービス体験後アンケートの設問と回答選択肢

設問	回答選択肢
Q1. セキュリティログ監視（UTM による脅威防御）および対応支援サービスの満足度を回答ください。	1.満足
	2.やや満足
	3.どちらでもない
	4.やや不満
	5.不満

	6.サービスを受けていない
Q2. サイバーセキュリティ保険サービスの満足度を回答ください。	1.満足
	2.やや満足
	3.どちらでもない
	4.やや不満
	5.不満
	6.サービスを受けていない
Q3. 標的型攻撃メール対応訓練サービスの満足度を回答ください。	1.満足
	2.やや満足
	3.どちらでもない
	4.やや不満
	5.不満
	6.サービスを受けていない
Q4. Web アプリケーション脆弱性診断サービスの満足度を回答ください。	1.満足
	2.やや満足
	3.どちらでもない
	4.やや不満
	5.不満
	6.サービスを受けていない
Q5. 制御システム簡易リスクアセスメントサービスの満足度を回答ください。	1.満足
	2.やや満足
	3.どちらでもない
	4.やや不満
	5.不満
	6.サービスを受けていない
Q6. サービス全体（総合評価）の満足度を回答ください。	1. 満足
	2. やや満足
	3. どちらでもない
	4. やや不満
	5. 不満
Q7. サイバーセキュリティお助け隊参加の目的を達成できましたか。	1. 達成できた
	2. 一部達成できた

	3. 達成できなかった
Q8. サイバーセキュリティお助け隊で改善して欲しいこと。	（自由記述）
Q9. 事業参加に伴うセキュリティ意識の変化を回答ください。 ・経営層	1. 向上した
	2. やや向上した
	3. 変わらない
Q10. 事業参加に伴うセキュリティ意識の変化を回答ください。 ・情報システム担当	1. 向上した
	2. やや向上した
	3. 変わらない
Q11. 事業参加に伴うセキュリティ意識の変化を回答ください。 ・一般社員	1. 向上した
	2. やや向上した
	3. 変わらない
Q12. 公的機関（国、地方自治体）に期待することをご回答ください。	1. 補助金・助成金
	2. セミナーや講習会等の教育・啓発
	3. セキュリティに関する情報提供
Q13. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・パソコンに対する対策（モバイル用パソコンを含む） －ウイルス対策（Windows Defender を含む）	1. 実施している
	2. 実施していない
	3. わからない
Q14. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・パソコンに対する対策（モバイル用パソコンを含む） －情報漏洩防止対策（外部へのファイル持出し時の暗号化や遮断等）	1. 実施している
	2. 実施していない
	3. わからない
Q15. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・パソコンに対する対策（モバイル用パソコンを含む） －USB 接続機器利用制限	1. 実施している
	2. 実施していない
	3. わからない
Q16. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・パソコンに対する対策（モバイル用パソコンを含む） －ハードディスク暗号化	1. 実施している
	2. 実施していない
	3. わからない
Q17. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・ネットワークで実施する対策	1. 実施している
	2. 実施していない
	3. わからない

－ファイアウォール	
Q18. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・ネットワークで実施する対策 －UTM（セキュリティ対策統合型ファイアウォール）	1. 実施している 2. 実施していない 3. わからない
Q19. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・ネットワークで実施する対策 －パソコン以外のウイルス対策 次を含みます。 ネットワーク上に設置した UTM 以外の製品 インターネットサービスプロバイダの サービス クラウドのウイルス対策サービス	1. 実施している 2. 実施していない 3. わからない
Q20. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・ネットワークで実施する対策 －Web コンテンツフィルタリング UTM のみの場合は、こちらは選択しないでください。	1. 実施している 2. 実施していない 3. わからない
Q21. サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況 ・ネットワークで実施する対策 －侵入検知/防御装置（IDS/IPS） UTM のみの場合は、こちらは選択しないでください。	1. 実施している 2. 実施していない 3. わからない
Q22. 参加をきっかけに実施した追加のセキュリティ対策 ない場合は「なし」と回答ください。 参加後に「SECURITY ACTION」を宣言された場合は、その旨を記載ください。	（自由記述）
Q23. 参加をきっかけに実施する予定のセキュリティ対策 ない場合は「なし」と回答ください。	（自由記述）
Q24. お助け隊事業で提供した以外に希望するサービスがあれば回答ください。	（自由記述）

表 22 成果報告会アンケートの設問と回答選択肢

設問	回答選択肢
Q1. セキュリティ対策が必要であると感じましたか？	1. はい
	2. いいえ
Q2. 今後のセキュリティ対策検討に役立つ内容でしたか？	1. はい
	2. いいえ
Q3. 紹介したサービスを利用したいと感じましたか？	1. はい
	2. いいえ

表 23 テレワークに関するアンケートの設問と回答選択肢

設問	回答選択肢
Q1. テレワークを実施していますか？	1. 実施していない
	2. 実施している
Q2. テレワークを「実施していない」企業様にお聞きします。 テレワークを実施されていない理由を教えてください	1. 必要ないため
	2. テレワークを実施する機器がないため
	3. セキュリティ対策が実施できない（間に合わない）ため
	4. テレワークによるセキュリティ事故が懸念されるため
	5. その他
Q3. 「その他」と回答された方に伺います。 実施されていない理由をご回答ください。	（自由記述）
Q4. テレワークを「実施している」企業様にお聞きします。 以下の設問にご回答をお願いします。 どの程度の従業員の方がテレワークを実施していますか？	1. ごく一部（10%以下）
	2. 一部（30%以下）
	3. 半分
	4. 全員
Q5. テレワークの運用ルールを定めていますか？	1. はい
	2. いいえ
Q6. 個人所有機器（BYOD）の利用を許可していますか？	1. はい
	2. いいえ
Q7. テレワークのためのセキュリティ対策について実	1. VPN による社内ネットワークへの接続

施している対策をご回答ください。 （複数選択）	2. VDI（仮想デスクトップ）による社内機器への接続
	3. パソコンのハードディスク暗号化（盗難・紛失対策）
	4. パソコンをインターネットに接続しない（ローカルに保存したファイルを編集するのみ）
Q8. テレワークの課題がありましたらご回答ください。	（自由記述）

3.2.2 ヒアリングによる実態把握結果

次のテーマでヒアリングを 8 社に実施した。ヒアリングの結果を次に記す。

（1）インシデント対応について
（2）セキュリティ対策の実施状況について
（3）IT の大規模開発の分散した場所での業務について
（4）今後のセキュリティ対策について

(1) インシデント対応について

インシデント対応は、実際に被害を受けていないため、課題として認識している企業は少ない。セキュリティ対策が進んでいないことで、不審メールが届くことが「当たり前」になっており、従業員の意識は高いと思われる。

サイバーセキュリティお助け隊は有効であったとの回答が多かった。セキュリティ対策を取り組んでいく「きっかけ」にしていただけたと感じる。

インシデント対応に関するヒアリングの回答の詳細を次に記す。なお、類似の回答は、一つのみ記載した。

ａ．インシデント対応

- セキュリティ対策を進めなければならないと感じているが、過去に被害を受けていないため、実施できていない。
- 過去にマルウェア感染したことがないので、対応を行ったことがない。
- 今までなかったので大丈夫だろうという意識がある。
- 電子メールは、不特定多数の顧客を相手にしているので、開かざるを得ない
- 不審なメールが届いたら、周りに聞いている
- 不審メールは普段から多いので慣れている
- Emotet の攻撃メールが届いたが、昨年度の日付だったので不審に思い、送信元に連絡し、送っていないことが判明し、削除した。

b. サイバーセキュリティお助け隊の有効性

- お助け隊がなければこのようなセキュリティ対策は実施しなかった。
- UTM が大事とあらためて思った。いろんなものを試す価値がある。何もなければ試していなかった
- UTM により、目に見える形で状況を把握できた。
- 見える化できた事象を教育・注意喚起に活用できる。
- UTM により実態に色々気付くことができた
- 啓発、勉強になった。

(2) セキュリティ対策の実施状況について

取引先からセキュリティ対策を実施するよう要請されている。内容は業界によって異なるが、IT 関連業界が最も要求水準が高いようである。

セキュリティ対策は、ウイルス対策ソフトをすべての企業で導入しているが、それ以外は企業により差異がある。大企業と比較すると、技術的対策の導入は進んでいない。

セキュリティ体制は企業により差があった。IT 関連企業はセキュリティ体制が明確になっていたが、それ以外の業種の企業は、明確になっていない企業が多かった。セキュリティの相談先は IT を導入した事業者であることが多かった。

セキュリティ対策の実施状況に関するヒアリングの回答の詳細を次に記す。なお、類似の回答は、一つのみ記載した。

a . 取引先からセキュリティ対策の要請

- 大手企業の取引先からのセキュリティ対策を要求される。しかし、何をどこまでやれば良いか明確な要求事項がない
- 自治体の取引には、有償アンチウイルス利用、サポートが終わった製品を利用しないことが求められる
- IT 系の開発は、取引先全部からセキュリティ対策の実施を求められる。

b. セキュリティ対策実施状況

- セキュリティ対策の実施状況は、ウイルス対策ソフトと教育のみ。
- セキュリティ対策予算は、ウイルス対策ソフト、UTM、資産管理ソフトである。予算を増やす予定はない。
- セキュリティ対策予算は、ウイルス対策ソフト、Web コンテンツフィルタリング、USB 接続制限である。
- セキュリティ対策予算は、ソフトウェアの維持、継続更新である。
- セキュリティ対策の有効性評価が難しい。
- セキュリティ対策は、個人情報保護法ができたときおよび取引先からのセキュリティ対策の要求があったときから取り組んできた。

c. セキュリティ体制

- セキュリティ体制は明確になっていない。
- セキュリティ担当者は社長である。引継ぎしたいと考えている。
- セキュリティ体制は、担当が２人で、情報セキュリティ委員会を設置している。

・　セキュリティ人材育成は、セキュリティ管理者向けの研修を定期的に受けている。
・　セキュリティインシデント発生時に一緒に対応して育てている。
・　セキュリティ対策の相談先は、製品ベンダー、メーカーである。
・　ウイルス対策ソフトのサポートに入っているが、価格が高い。

(3) IT の大規模開発の分散した場所での業務について

顧客の業種により、分散した場所での開発が難しい場合がある。テレワーク形式の開発の技術的な課題はないと回答した企業が多かった。

IT の大規模開発の分散した場所での業務に関する IT 関連企業 3 社へのヒアリングの回答の詳細を次に記す。なお、類似の回答は、一つのみ記載した。

・　電力関連、金融の開発は、クローズド環境で行うケースが多く、持ち帰りはできない案件がほとんどである。なお、専用線で接続し、決まったクライアントで開発する場合もある。
・　クローズド環境の場合、メールやチャットが使えない。連絡は電話のみとなる。
・　テレワーク形式の開発に技術的な問題はない。
・　できるのであればテレワークを推進したい。
・　持ち帰ることができる開発は、テレワークを含めて様々な場所で実施している。
・　開発のフェーズによって、実施するセキュリティ対策を変えている場合がある。（VDI での接続を許可するか、しないか等）
・　クラウド上で開発している案件もある。ただし、2 要素認証＋グローバル IP アドレス制限の対策を講じている。

(4) 今後のセキュリティ対策について

サイバーセキュリティ保険の有効性は認識しているが、情報がないと回答した企業が多かった。

「セキュリティ対策費用の捻出が難しい」こと、「人的リソースがない」こと、「要員の知識が不足している」ことが、セキュリティ対策を進めていく上での共通の課題であった。

今後の計画を立案できていない企業が多かった。セキュリティ対策の必要性を認識しているが、何をすれば良いかわからないため実施できていない企業が多かった。

今後のセキュリティ対策に関するヒアリングの回答の詳細を次に記す。なお、類似の回答は、一つのみ記載した。

ａ．サイバーセキュリティ保険
・　知らなかった。
・　情報がない。情報をもらえれば検討する。
・　積極的に活用したい
・　価格が高いので加入していない
・　データが消えた、暗号化された場合、お金では戻せないのではないか。

ｂ．今後の計画
次がセキュリティ対策を進める上での課題であるとの回答だった。
・　セキュリティ対策費用の捻出が難しい
・　人的リソースがない

・　要員の知識が不足している
・　今のところ、セキュリティ人材の育成計画はない
・　今のところ、追加するセキュリティ対策の計画はない
・　IT を便利に使えれば良いと思っている。しかし、具体的なビジョンがない。
・　セキュリティ対策の今後の計画を立てなければならないと考えている
・　セキュリティ対策は、何をしたら良いかわからない
・　費用対効果がわからないため費用を出しにくい
・　どれくらいの費用が妥当なのかわからない。目安となる金額があったら教えて欲しい

c．希望するセキュリティサービス
・　セキュリティに関する（攻撃等）情報提供サービス。社内への通知に利用したい
・　啓発活動に該当するサービス。今は IPA の注意喚起を利用している。
・　セキュリティ対策に関する年に数回の相談対応
・　UTM を複数拠点に設置できるパッケージが良い。
・　UTM だけでなく、クライアントのセキュリティ対策のセットが良い。
・　資本関係のあるグループ企業にまとめてセキュリティ対策を提供しているような、大きな規模のセキュリティシステムを参加企業が利用できる形態が望ましい
・　IT 機器の導入からシステムの運用まですべてアウトソース。どちらかだけだと、IT の障害か攻撃か切り分けができない。

3.3 実証の実施結果

地域実証の結果をサービス別に記す。

3.3.1 簡易なセキュリティ診断

次の 2 つの実施結果を記載する。
・5 分でできる！情報セキュリティ自社診断
・情報セキュリティ対策ベンチマーク

(1)　5 分でできる！情報セキュリティ自社診断

表 24 5 分でできる！情報セキュリティ自社診断 選択肢

選択肢	
1	実施している
2	一部実施している
3	実施していない
4	わからない

表 25 5 分でできる！情報セキュリティ自社診断

質問内容	実証参加企業-最も実施できている企業（最大）	実証参加企業-最も実施できていない企業（最小）	お助け隊参加企業-平均	IPA-平均
1-1 アップデート	1	2	1.3	1.5
1-2 ウイルス対策	1	1	1.0	1.5
1-3 パスワード	1	3	1.8	2
1-4 アクセス制限	1	2	1.3	2
1-5 情報共有	1	3	1.8	2.5
2-6 電子メール受信	1	2	1.3	1.8
2-7 電子メール送信	1	3	1.8	2.2
2-8 添付重要情報の保護	1	3	1.7	2.5
2-9 無線 LAN	1	1	1.3	2
2-10 インターネット	1	3	1.5	2.5
2-11 バックアップ	1	1	1.2	2
2-12 保管	1	3	1.4	2.2
2-13 盗難対策	1	3	1.8	2.3
2-14 利用者限定	1	2	1.5	2.5
2-15 立ち入り監視	1	3	1.4	2
2-16 盗難防止	1	3	1.8	2.5
2-17 施錠管理	1	1	1.5	2
2-18 破棄	1	3	1.4	2
3-19 社内規定周知	1	3	1.3	2
3-20 意識教育	1	3	1.6	2.2
3-21 個人所有	1	3	1.5	2.5
3-22 取引先	1	2	1.3	2
3-23 外部サービス	1	2	1.3	2
3-24 事故対応	1	3	1.5	2
3-35 対応の明確化	1	3	1.8	2.8

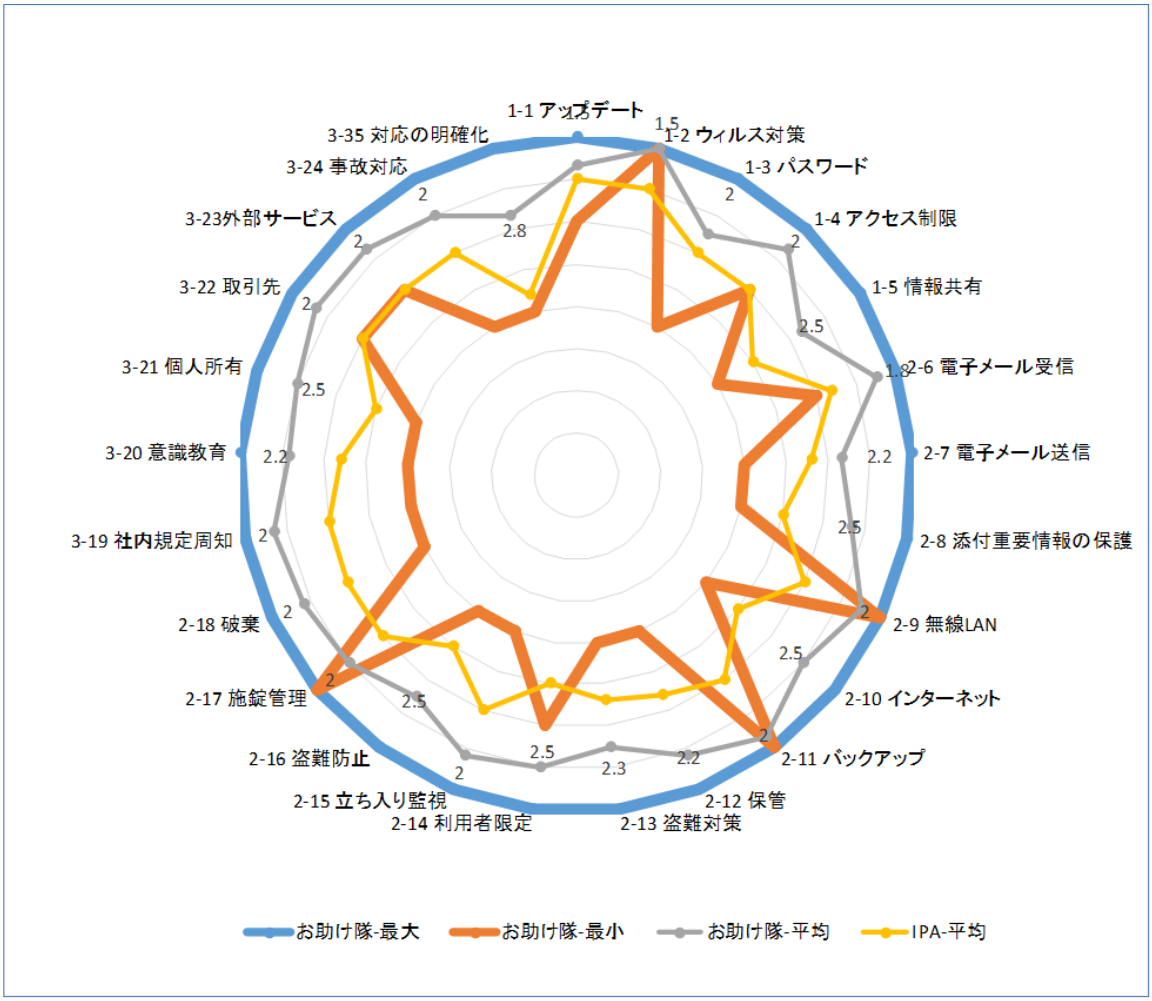


図 17 5分でできる自社診断レーダーチャート（n=12）

（2） 情報セキュリティ対策ベンチマーク

表 26 情報セキュリティ対策ベンチマーク 選択肢

選択肢	
1	方針やルールを定めておらず、実施されていない。
2	方針やルールの整備、周知を図りつつあるが、一部しか実現できていない。
3	方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。
4	経営層の指示と承認の下に方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている。
5	4.に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している。

表 27 情報セキュリティ対策ベンチマーク

質問内容	実証参加企業-最も実施できている企業(最大)	実証参加企業-最も実施できていない企業（最小）	実証参加企業-平均	IPA-平均
1.情報セキュリティ管理規定	4	2	3.5	3.1
2.情報セキュリティに対する組織的な取り組み	4	2	3.4	3
3.情報セキュリティ推進体制	4	1	3.4	3.1
4.重要資産の重要度分類	4	1	3.1	3
5.重要情報の業務工程ごとの安全対策	4	2	3.3	3.1
6.業務委託契約	4	1	3.3	3.2
7.従業者との契約	4	1	3.5	3.3
8.従業者への教育	4	1	3.3	3.1
9.建物や安全区画の物理的セキュリティ	4	2	3.3	3.2
10.第三者アクセス	4	1	3.3	3.1
11.情報機器の安全な設置	4	2	3.3	3.1
12.書類、記憶媒体の適切な管理	4	2	3.3	3.1
13.実稼働環境の情報セキュリティ対策	4	2	3.2	3.1
14.システム運用におけるセキュリティ対策	4	2	3.3	3.1
15.バックアップ	4	1	3.0	3.2
16.不正プログラム対策	4	3	3.7	3.7
17.情報システムの脆弱性対策	4	2	3.3	3.4
18.通信ネットワークの保護策	4	1	3.3	3.2
19.記憶媒体の紛失、盗難対策	4	1	3.1	3.2
20.情報（データ）へのアクセス制御	4	1	3.3	3.3
21.業務アプリケーションに対するアクセス制御	4	1	3.5	3.3
22.ネットワークのアクセス制御	4	2	3.5	3.3
23.業務システム開発時のセキュリティ考慮	4	1	3.1	3
24.ソフトウェアの導入・開発時のセキュリティ管理	4	1	3.2	3
25.情報システムの障害対策	4	2	3.2	3.1
26.情報セキュリティ事故対応手続き	4	1	2.8	3
27.事業継続への取り組みの実施	4	1	2.4	3

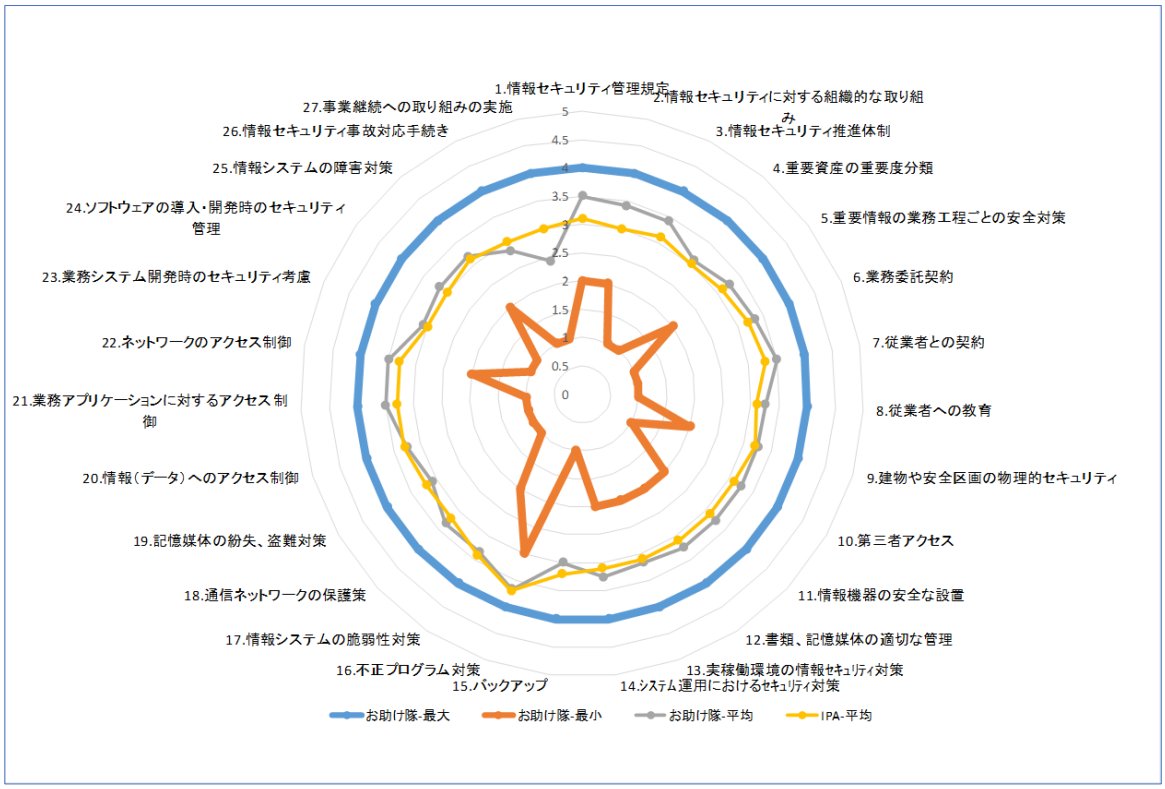


図 18 情報セキュリティ診断レーダーチャート（n=12）

3.3.2 中小企業等からのサイバーセキュリティに関する相談の受付および対応

コールセンター対応およびインシデント対応等の状況は下表のとおりである。

表 28 コールセンター対応およびインシデント対応等の状況サマリー

対応種別	総計	相談・インシデント等対応状況	件数
コールセンター対応	9 件	実証参加に関する問合せ	1 件
		セキュリティ機器設置等の問合せ	4 件
		セキュリティ対応の相談	0 件
		その他	4 件
インシデント対応	0 件	電話およびリモートによるインシデント対応	0 件
		訪問によるインシデント対応（駆け付け）	0 件
その他訪問対応	42 件	機器設置等のトラブル対応	2 件
		その他（セキュリティ機器の導入・設置支援等）	40 件

表 29 コールセンター対応およびインシデント対応等の状況詳細

対応種別	相談・インシデント等対応状況	内容
コールセンター対応	実証参加に関する問合せ	UTM 設置について VPN 接続する必要はあるか。別途料金はかかるか。
	セキュリティ機器設置等の問合せ	UTM 設置時のネットワーク構成に関する相談
		UTM の設定をできるか。またその方法について
		「不正アクセスを検知しブロックしました」というレポートの内容について
		IPS 検知の危険度「High」以下の防御設定はどうなっているか
	その他	お助け隊事業を継続した場合の料金の発生タイミングはいつか
		トライアル参加後の費用はどの程度かかるのか
		簡易なセキュリティ診断実施方法について
		自動通知メールが届くが大丈夫であるか
その他訪問対応	機器設置等のトラブル対応	機器設置時の初期不良対応
		設置した機器と SOC の通信不良対応
	その他（セキュリティ機器の導入・設置支援等）	機器設置対応：40 社

3.3.3 機器、ソフトウェア、サービス等による中小企業等の実態把握のための措置

セキュリティログを監視し、脅威を検知・防御した件数は下表の通りである。

表 30 脅威分類別検知件数

脅威分類 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
外部からの不正アクセス検知および防御（外→内）	6	63	41	110
内部不正プログラム検知および防御（内→外）	0	0	0	0
マルウェアの検知および無害化	19	54	42	115
合計	25	117	83	225

外部からの不正アクセス検知および防御（外→内）を 110 件、マルウェアの検知および無害化を 115 件検知した。攻撃の種別毎の検知数については後述の表参照。

また、「内部不正プログラム検知および防御（内→外）」の検知・防御があったが、調査の結果、誤検知であると判断したため、件数を「0」とした。

脅威分類の定義は下表のとおりである。

表 31 脅威分類の定義

脅威分類	定義
外部からの不正アクセス検知および防御（外→内）	インターネット（外部）から組織内部のネットワークに対しての攻撃（不正アクセス）の検知および防御
内部不正プログラム検知および防御（内→外）	組織内部機器から攻撃者サーバーや標的への攻撃に対する通信の検知および防御
マルウェアの検知および無害化	Web サイトアクセスや電子メール等のネットワーク経由で侵入するマルウェアの検知および無害化

なお、次は本実証では取得できない脅威であるため、報告から除外した。

表 32 本報告対象外の脅威分類

脅威分類	除外した理由
不正サイトへのアクセスブロック	Web コンテンツフィルタ機能を提供していない
エンドポイントでのアラート検知	エンドポイントの検知ソフトを提供していない

a．外部からの不正アクセス検知および防御（外→内）

攻撃の種類別の検知件数を下表に記す。

表 33 外部からの不正アクセス検知および防御数

攻撃種別 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
Bladabindi.Botnet	2	4	2	8
D-Link.Realtek.SDK.Miniigd.UPnP.SOAP.Command.Execution	0	1	0	1
Eir.D1000.Modem.CWMP.Command.Injection	3	7	21	31
Gh0st.Rat.Botnet	1	6	3	10
ip_dst_session	0	36	0	36
OpenSSL.Heartbleed.Attack	0	1	15	16
udp_dst_session	0	7	0	7
udp_flood	0	1	0	1
合計	6	63	41	110

上記の表は外部からの不正アクセス検知および防御数で検知した攻撃種別になる。

DoS 攻撃により、システムの速度を低下させたり、クラッシュさせたりする、ip_dst_session やリモート攻撃を行う Eir.D1000.Modem.CWMP.Command.Injection が多いことが分かる。

ｂ．内部不正プログラム検知および防御（内→外）

内部ネットワーク上のパソコンから内部不正プログラムの存在が疑われる通信を検知したが、調査した結果、誤検知であると判断した。

ｃ．マルウェアの検知および無害化

表 34 マルウェア検知および無害化件数

経路 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
電子メール	9	33	25	67
Web サイト接続	10	21	17	48
合計	19	54	42	115

表 35 電子メール経路のマルウェア検知

攻撃種別 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
MSIL/Kryptik.YEJ!tr	1	0	0	1
MSOffice/CVE_2017_11882.95A0!tr	0	3	0	3
VBA/Agent.A664!tr	4	11	0	15
VBA/Agent.AVL!tr	0	0	0	0
HTML/IFrame.3EB!tr	0	0	1	1
Malicious_Behavior.SB	0	4	0	4
Malware_Generic.P0	0	2	4	6
MSIL/GenKryptik.EXPH!tr	0	0	3	3
MSIL/Kryptik.ZBU!tr	0	0	4	4
PDF/Spam.2761!tr	0	0	2	2
VBA/Agent.3411!tr	1	0	0	1
VBA/Agent.LXMF!tr	0	0	2	2
VBA/Agent.UMA!tr.dldr	2	0	0	2
VBA/Agent.VAR!tr.dldr	0	0	2	2
VBA/Agent.VEF!tr	0	0	1	1
W32/Injector.ENXJ!tr	0	5	0	5
W32/Kryptik.HCGI!tr	0	0	2	2
W32/Kryptik.HHEK	0	0	4	4
W32/Kryptik.HHGY!tr	0	4	0	4
W32/Kryptik.HHRG!tr	0	4	0	4
合計	8	33	25	66

表 36 Web サイト経路のマルウェア検知

攻撃種別 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
JS/RefC.G!tr	9	13	5	27
JS/EvilCursor.B!tr	0	3	0	3
Riskware/UwS_SlimDrivers	0	5	0	5
HTML/Refresh.BC!tr	1	0	0	1
Riskware/Agent	0	0	12	12
合計	10	21	17	48

非常に多くの攻撃種別を検知したことが上の電子メールや Web サイト接続の攻撃種別の表から分かる。

3.3.4 サイバーインシデントが発生した際の支援の提供

サイバーインシデントが発生した際の支援の提供は、0 件だった。

表 37 サイバーインシデントが発生した際の支援の提供件数

分類 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
サイバーインシデントが発生した際の支援の提供	0	0	0	0

3.3.5 標的型攻撃メール対応訓練

（1） 実施概要

（a） 目的

標的型攻撃メールによる被害が顕在化している状況を踏まえ、標的型攻撃メールを体感することにより、システム利用者の情報セキュリティ意識の向上および標的型攻撃メール（不審メール）の組織的な知識と対応力の向上を図ることを目的として、申し込みがあった 18 社に対して標的型攻撃メール対応訓練を実施した。

（b） 訓練対象者

対象企業より提供されたリストに基づき、423 名の訓練対象者に対して訓練を実施した。

（c） 実施手順

疑似攻撃メールとして、Microsoft Word ファイルをパスワード付き ZIP 形式に圧縮して添付したメール（以下「訓練メール」という）を訓練対象者に送付した。

（d） スケジュール

下記のスケジュールでメール送信を実施した。

表 38 訓練対象者数

送信日	訓練対象企業	訓練対象者
2020 年 12 月 9 日	15 社	321 名
2020 年 12 月 23 日	3 社	102 名
全体	18 社	423 名

（e） 訓練メール内容

表 39 訓練メール内容文面（添付ファイル型）

送信者表示名 <送信元アドレス>	attacker@yah00co.jp
宛先表示名	お客さま各位<訓練対象者のメールアドレス>
件名	Fwd:
本文	協力会社各位 お世話になっております。 標記の件、20_12 に皆様にお送りしたご案内に修正事項がございます。 以下に要点を記載いたしますのでご確認の程お願いいたします。 お心当たりがある業者様は取り急ぎご連絡いただきますようお願いいたします。 今後の手続きについてご案内いたします。 日時：202012 月 09 添付ファイル名：TVKHENDWW4 202012 月 09.zip パスワード：[YYtZRh] この度は当方の不手際でご迷惑をお掛けし、大変申し訳ありません。
添付ファイル名	TVKHENDWW4 202012 月 09.zip ※Word 文書をパスワード付き Zip で圧縮。パスワードはメール文面を参照。

(f)　集計対象期間

表 40 開封ログ集計期間

送信日	集計開始日時	集計終了日時
2020 年 12 月 9 日	2020 年 12 月 09 日 10:00	2020 年 12 月 13 日 23:59
2020 年 12 月 23 日	2020 年 12 月 23 日 10:00	2020 年 12 月 27 日 23:59

(g)　集計対象者

訓練対象者のうち、正常に訓練メールを送信できた方を集計対象者とした。

(h)　開封者

集計対象者のうち、訓練メールに添付されているファイルを開封し、TOiNX サーバーに開封ログが記録された方を開封者とした。

(i)　開封率

以下の式で算出した開封者の割合を開封率とした。

開封率 [%] ＝ 開封者 [名] ÷ 集計対象者 [名] × 100

※開封率は小数点第 2 位を四捨五入する。

(2)　訓練結果

(a)　開封結果概要

訓練結果概要を下記に示す。

表 41 開封結果概要

訓練対象者数	423 名
送信エラー数	0 名
集計対象者数	423 名
開封者数	7 名
開封率	1.7%

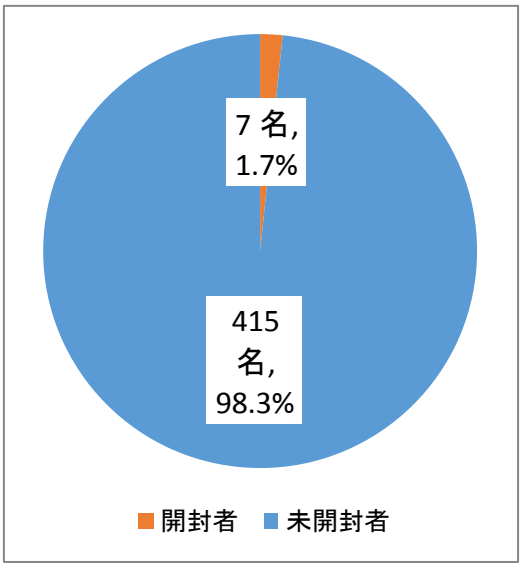


図 19 開封結果

(3) 開封結果の分析

開封結果（全体）の開封率は 1.7%となり、ラック社が実施、公表した事例（11.5%）よりも低い結果となったことから、訓練対象者が情報セキュリティに関するリテラシーを身につけており、標的型攻撃への対応力を備えているものと推察される。

今回の訓練では実際に訓練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、脅威・リスクを意識することでメールによる攻撃への警戒心・注意の意識が高まったと考えられる。

標的型攻撃では業務や組織に関連する内容や人間の心理的な側面を利用した手法が攻撃に利用されることが多く、注意が必要である。また、一部のシステム利用者への攻撃が成功するだけでも被害が拡大する可能性があるため、組織全体のセキュリティを向上させることが重要となることから、定期的かつ継続的な訓練を実施することで、脅威に対する意識を向上・維持することが必要だと考える。加えて、個人が不審メールを見分けるだけでなく、組織内で情報共有を行い、事前に定めておいたルールに則った連絡や行動をとれるかが重要であることから、企業・部署など組織全体での対策を講じる必要がある。

株式会社ラック: :「セキュリティ診断レポート 2018 秋」、
https://www.lac.co.jp/lacwatch/pdf/20180926_sec_report_vol3.pdf（2021/01/15 参照）.
過去から継続して訓練を実施している 139 組織，41.8 万人を対象とした 2017 年度の平均開封率がおよそ 11.5%であったという統計値が発表されている。（グラフから読み取った概数）

3.3.6 脆弱性診断

脆弱性診断を 3 社に対して実施した。危険度の高い脆弱性は検出されなかった。脆弱性に関する内容であるため、詳細は開示しない。

検知した件数を下表に示す。件数は 3 社で検知した件数の合計である。

表 42 Web アプリケーション脆弱性診断 脆弱性検出件数

危険度	件数
High	0
Medium	0
Low	0
Info	12

表 43 Web アプリケーション脆弱性診断 脆弱性検出件数

危険度	件数
High	0
Medium	10
Low	2
Info	14

表 44 セキュリティ診断 危険度判定基準

危険度	想定される被害の例
High	・リモートからのシステムの完全制御 ・全面的な情報漏えい、情報改ざん ・全面的なシステム停止を伴うサービス拒否（DoS） ・任意の命令実行
Medium	・部分的な情報漏えい、情報改ざん ・部分的なシステム停止を伴うサービス拒否（DoS） ・クロスサイトスクリプティング ・その他、High に該当するが再現性が低いもの
Low	・攻撃をするための条件が複雑であるもの ・その他、Medium に該当するが再現性が低いもの
Info	・検出項目単体では被害に繋がらないが、将来的な脆弱性につながる可能性のあるもの ・よりセキュアなアプリケーションを構築する上で改修の検討が必要なもの

3.3.7 制御システム簡易リスクアセスメント

2 社に対して実施した。現地確認とヒアリングの結果、サイバー攻撃により大きな被害が懸念される状況ではなかった。

インシデントの発生確率は低い状況だが、ルールの定義等のセキュリティマネジメント（管理）に関する対策が十分でなかったため、改善策を提案した。

3.4 報告会等による実証事業成果の周知

3.4.1 中間報告

実証結果の中間状況をとりまとめた PDF 形式の報告書をポータルサイトへ掲載し、情報のフィードバックを行った。情報の掲載日は 2020 年 12 月 16 日である。

中間報告の内容を下表に記す。

表 45 中間報告概要

項目	内容
情報提供日	2020 年 12 月 16 日（水）
提供方法	ポータルサイトに PDF 形式の中間報告書を公開
連絡方法	電子メールで実証参加企業にポータルサイトに公開したことを連絡
報告書の内容	1. サイバー攻撃の状況 （1） IPS-攻撃検知件数 （2） IPS-検知攻撃種別 （3） マルウェア検知-経路別防御数 （4） マルウェア検知-検知マルウェア種別 （5） サイバー攻撃の動向 2. セキュリティ対策実施状況 （1） サイバー攻撃の被害概況 （2） セキュリティ対策実施概況 （3） アンケート結果 （4） 簡易なセキュリティ診断結果 （5） SECURITY ACTION 宣言状況

「サイバー攻撃の状況」では 11 月までのセキュリティログ監視の情報を統計的にまとめたデータを開示し、実際に検知した攻撃、サイバー攻撃の動向を示した。「セキュリティ対策実施状況」ではアンケートや簡易なセキュリティ診断の結果、SECURITY ACTION 宣言状況から実証参加企業のセキュリティ対策実施状況を報告した。

3.4.2 成果報告会

表 46 成果報告会概要

項目	内容
開催日時	2021 年 1 月 13 日（水） （2021 年 1 月 14 日（木）17:00 よりオンデマンド配信）
場所、形態	オンライン（ツール：Zoom）
参加者数	20 社（18 社）
アジェンダ	1. 開会挨拶（東北経済産業局） 2. サイバーセキュリティお助け隊事業について（IPA） 3. サイバーセキュリティお助け隊成果報告（ToiNX） 実証するサービス内容について 4. 中小企業のため情報セキュリティセミナー（ちば経営応援隊） 5. サイバー攻撃被害事例と対策（ToiNX）

実証事業の総括として実証事業から得られたデータやアンケート結果から実際にどのような攻撃が行われているのか、実証参加企業のセキュリティ対策状況を説明した。また、実証事業の結果からセキュリティ対策を進める上での課題を考察し、必要なセキュリティ対策を提示した。特にお金をかけずにできるセキュリティ対策として、SECURITY ACTION 宣言や「中小企業の情報セキュリティガイドライン」の実践を具体的に紹介した。

実証終了後のサービスについて、その内容を説明した。

図 20 成果報告会撮影風景

図 21 成果報告会事務局

成果報告会後に実施したアンケートの結果を次に記す。

a．セキュリティ対策の必要性

表 47 「セキュリティ対策が必要であると感じましたか？」の回答

選択肢	回答数
はい	18 社
いいえ	0 社

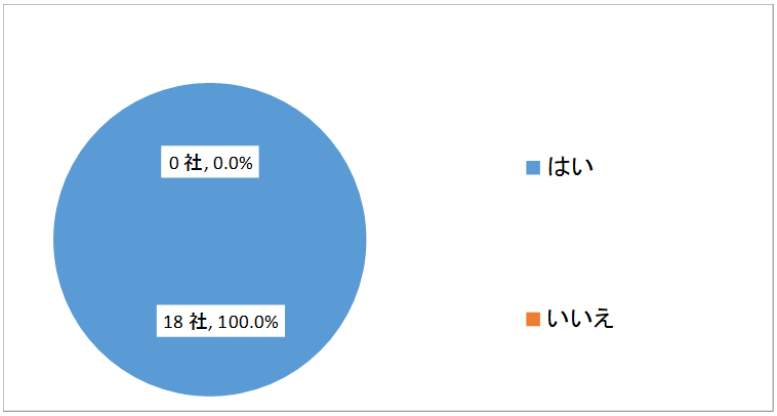


図 22 セキュリティ対策の必要性（n=18）

b．今後のセキュリティ対策検討有無

表 48 「今後のセキュリティ対策検討に役立つ内容でしたか？」の回答

選択肢	回答数
はい	17 社
いいえ	1 社

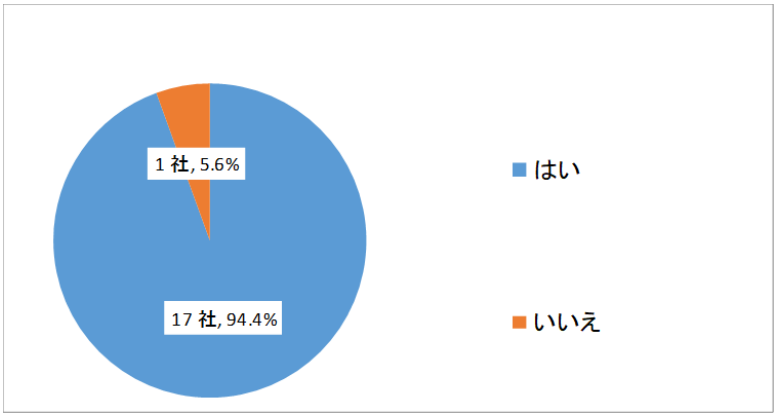


図 23 今後のセキュリティ対策検討有無（n=18）

4. 考察

お助け隊実証事業で得られた事実から現状（AS IS）を整理し、あるべき姿（TO BE）を考察した。なお、この分析結果およびお助け隊の実証を踏まえてビジネス化を検討した結果は、「5 実証を踏まえたビジネス化に向けた検討」を参照。

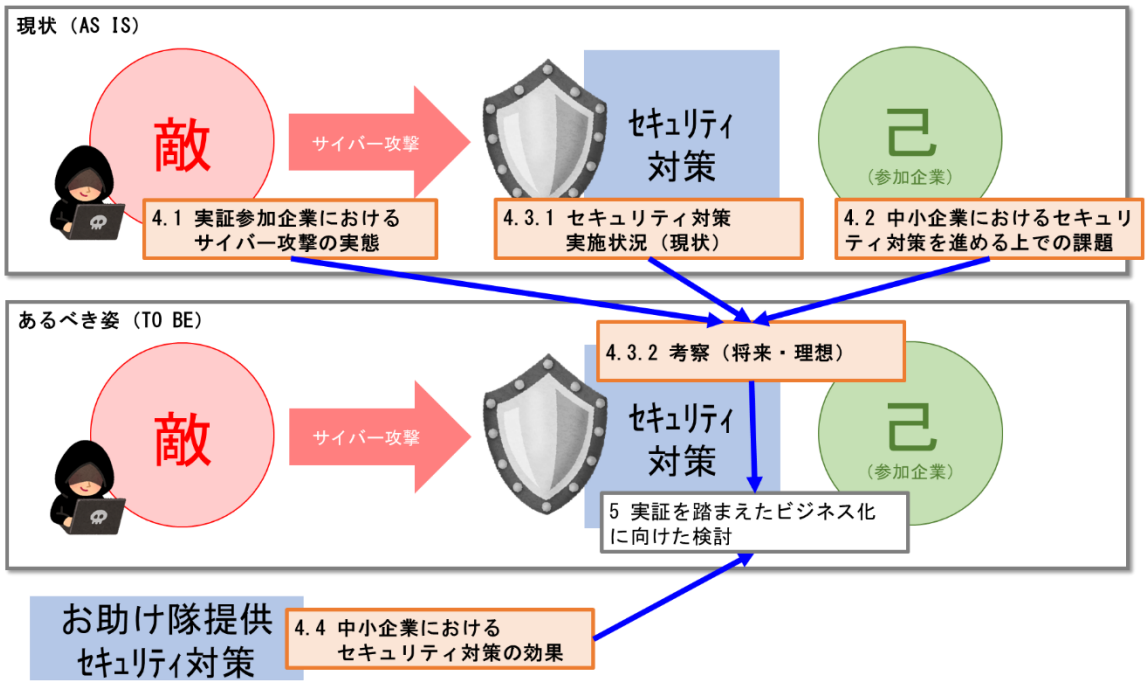


図 24 考察の全体像

4.1 実証参加企業におけるサイバー攻撃の実態

4.1.1 セキュリティログ監視結果

(1) 全体

UTM で多数のサイバー攻撃を検知・防御した。

表 49 サイバー攻撃検知・防御件数

脅威分類 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
外部からの不正アクセス検知および防御（外→内）	6	63	41	110
内部不正プログラム検知および防御（内→外）	0	0	0	0
マルウェアの検知および無害化	19	54	42	115

「内部不正プログラム検知および防御（内→外）」の検知・防御があったが、調査の結果、誤検知であると判断したため、件数を「0」とした。

(2) 外部からの不正アクセス検知および防御（外→内）

外部公開機器（インターネットから接続可能な機器）に対する攻撃を 110 件検知・防御した。外部公開機器（インターネットから接続可能な機器）は、常に攻撃を受けている。

ほとんどの機器は、インターネットからの攻撃をファイアウォール等で防御している図 25 の上のパターン（ファイアウォール等で内部ネットワークへの通信を遮断）となる。このような構成であれば、内部の機器はインターネットから直接攻撃を受けることはない。本実証において、ほとんどの実証参加企業の UTM をファイアウォールの内側に設置したため、攻撃は届かない。

インターネットから接続可能な機器が内部にある実証参加企業は、ファイアウォール等でその機器への通信を許可しているため、実証参加企業内部ネットワークの外部公開機器に対してインターネットから攻撃が届いた。この攻撃を UTM で検知・防御した件数が 110 件だった。

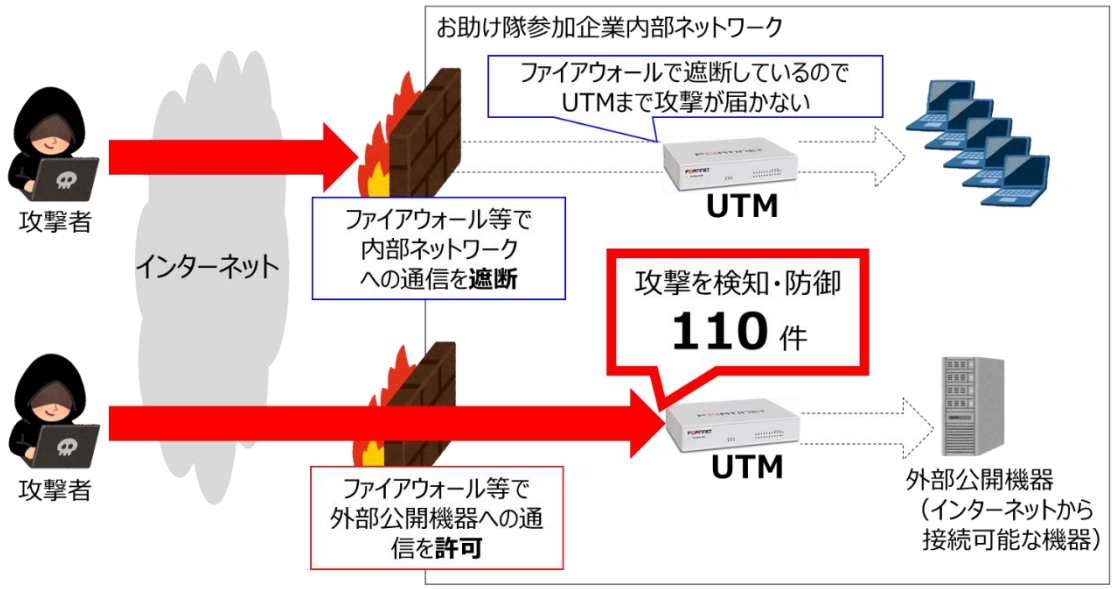


図 25 外部からの不正アクセス検知および防御（外→内）

(3) 内部不正プログラム検知および防御（内→外）

内部不正プログラムが疑われる通信を検知したが、調査の結果、誤検知と判断した。したがって、内部不正プログラムを検知および防御した件数は、0 件である。

もしも、マルウェアに感染した場合、攻撃者のサーバーへの通信や正規サイト（攻撃対象）への攻撃が行われる場合がある。

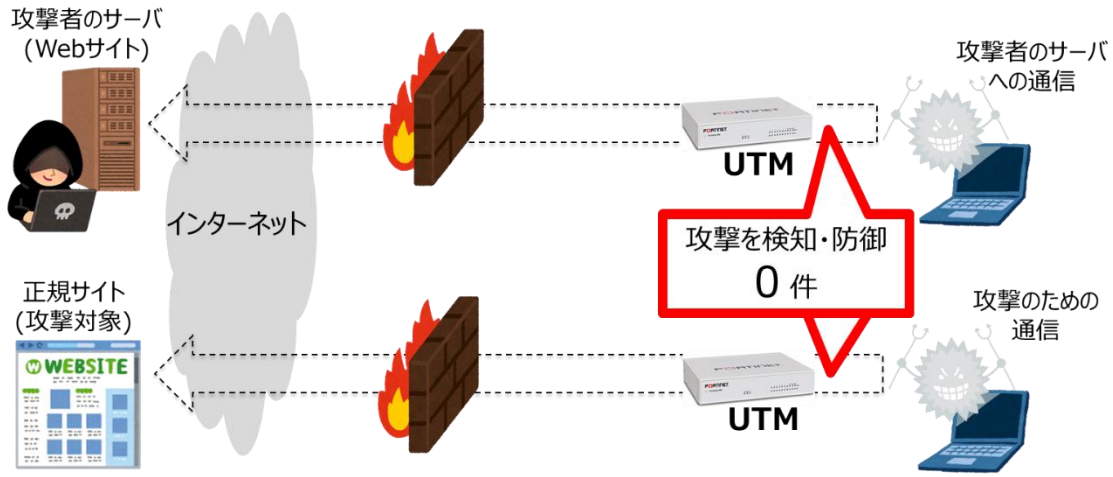


図 26 内部不正プログラム検知および防御（内→外）

(4) マルウェアの検知および無害化

Web サイト経由で送られたマルウェアを 48 件検知・防御した。
電子メール経由で送られたマルウェアを 67 件検知・防御した。

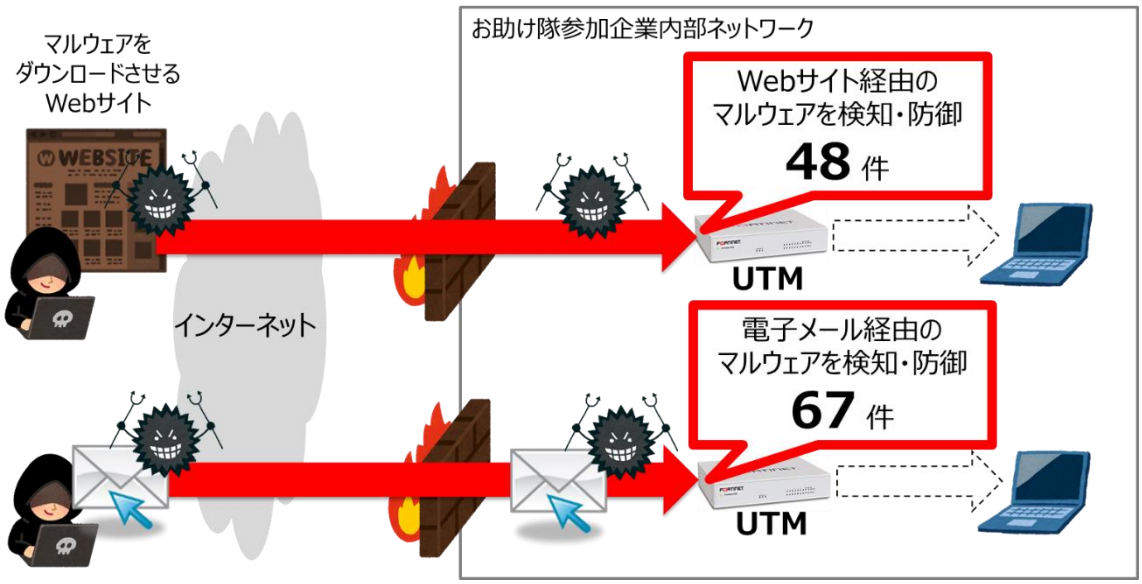


図 27 マルウェアの検知および無害化

4.1.2 アンケート結果

「サイバー攻撃の実態」に関するアンケートの結果、次の傾向であった。

- 「不審メールを受信」91%
- 「サイバー攻撃の被害あり」9%
- 「ランサムウェアを除くウイルスの感染あり」16%
- 「ランサムウェア感染あり」6%
- 「フォレンジック調査を外部へ依頼あり」3%

不審メールの受信は全体の 90%（32 社中 29 社）とほとんどの企業で受信しているが、サイバー攻撃の被害に遭ったことがあると回答した企業は全体の 9%（32 社中 3 社）とそれほど多くない。

アンケート結果の詳細を下表と下図に記す。

a．サイバー攻撃の被害有無

表 50 サイバー攻撃の被害有無

選択肢	回答数
あり	3 社
なし	29 社

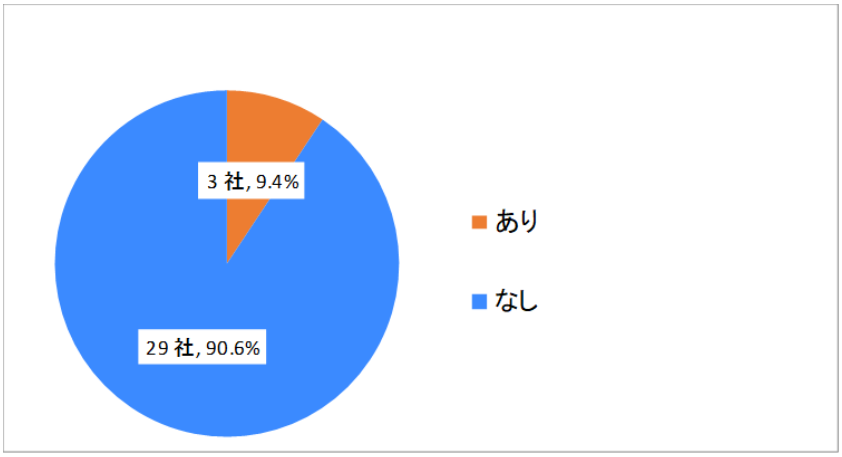


図 28 サイバー攻撃の被害有無（n=32）

b．サイバー攻撃の状況（不審メールの受信）

表 51 サイバー攻撃の状況（不審メールの受信）

選択肢	回答数
ある	29 社
ない	3 社

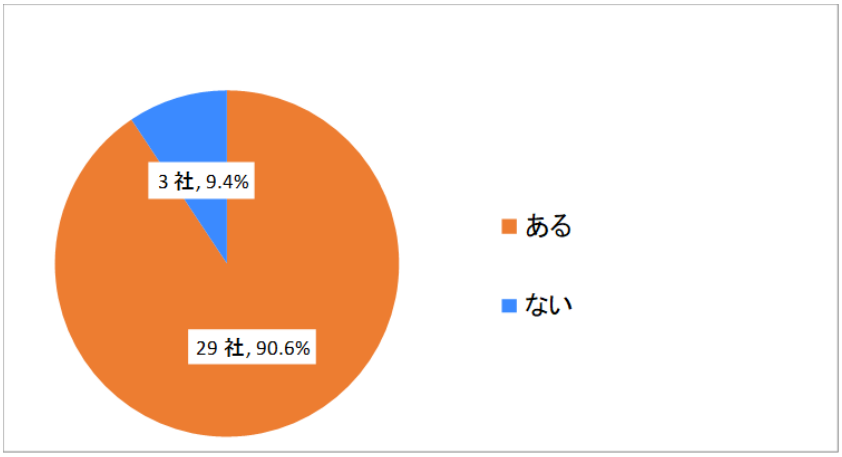


図 29 サイバー攻撃の状況（不審メールの受信）（n=32）

c．ウイルス（ランサムウェアを除く）に感染

表 52 ウイルス（ランサムウェアを除く）に感染

選択肢	回答数
ある	5 社
ない	27 社

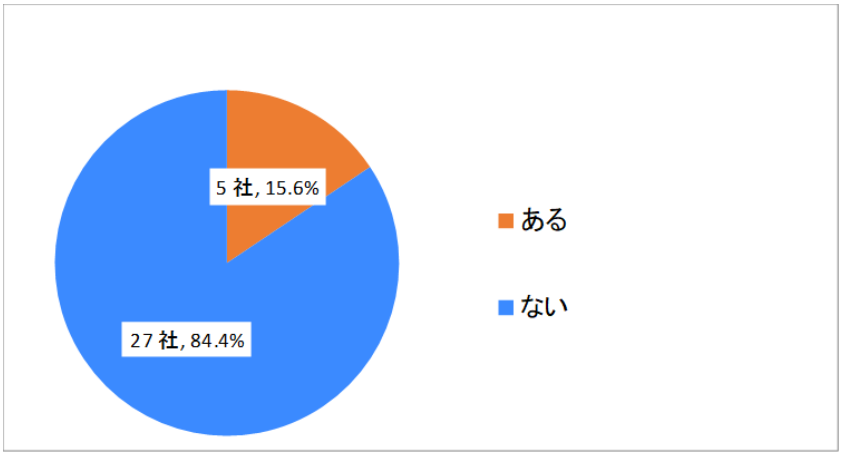


図 30 ウイルス（ランサムウェアを除く）に感染（n=32）

d．ランサムウェアに感染

表 53 ランサムウェアに感染

選択肢	回答数
ある	2 社
ない	30 社

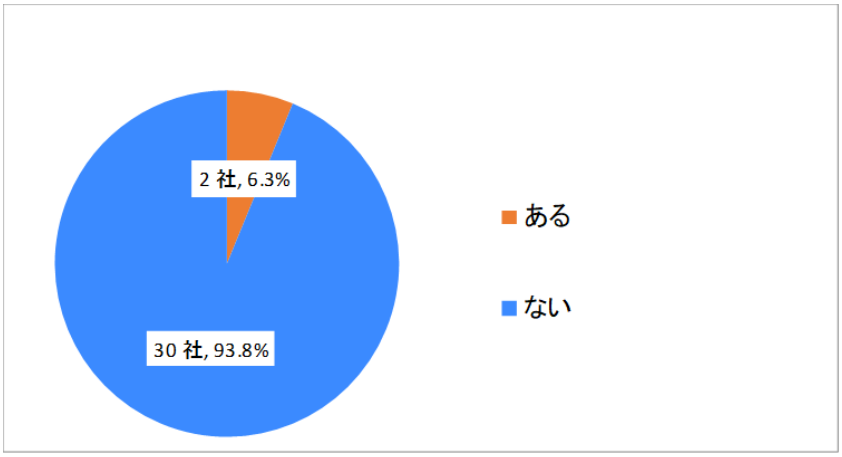


図 31 ランサムウェアに感染（n=32）

e．フォレンジック調査を外部へ依頼

表 54 フォレンジック調査を外部へ依頼

選択肢	回答数
ある	1 社
ない	31 社

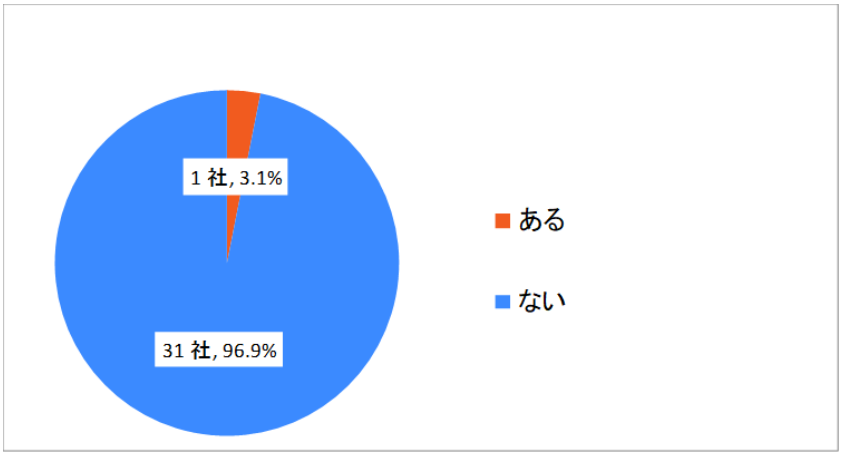


図 32 フォレンジック調査を外部へ依頼（n=32）

4.1.3 駆け付け対応・相談対応・ヒアリング結果

インシデント発生による駆け付け対応とサイバー攻撃に関する相談対応は、0 件だった。

表 55 駆け付け対応・相談対応件数

分類 ＼ 月 カッコ内は監視対象企業数	10 月 （26 社）	11 月 （38 社）	12 月 （40 社）	合計
インシデント発生による「駆け付け対応」	0	0	0	0
サイバー攻撃による「相談対応」	0	0	0	0

また、ヒアリングの結果、サイバー攻撃を懸念している企業はあったが、具体的な問題・課題がある企業はなかった。

ヒアリングをした際に、Emotet の攻撃メールを受信したが、本文中の日付が一年前だったため、不審に思い、送信元に連絡したところ、そのメールを送信していないとの回答があり、被害に至らなかったとの事例があった。

アンケートの結果からも不審メールを受信していることを認識している企業が多くの割合を占めていることから、サイバー攻撃がないから被害を受けていないのではなく、様々な要因で被害が発生しているものと思われる。なお、標的型攻撃だと思われる事例はなかった。

インシデント発生による「駆け付け対応」とサイバー攻撃による「相談対応」がなかった。これは、サイバー攻撃の被害がなかったことが原因だと思われる。下表の理由で被害が発生しなかったものと推察する。

表 56 サイバー攻撃の被害がなかった理由（推測）

No	理由	根拠	備考
1	監視対象が小規模	・実証参加企業の従業員数合計が約 4,000 人である。	小規模であるほど、リスクが顕在化する確率が小さくなる。
2	監視期間が短い	・監視対象期間が、約 3 ヶ月間であった。	過去を含めても被害を受けていない企業の割合が多い。
3	お助け隊の UTM により攻撃を防御した	・「4.1.1 セキュリティログ監視結果」を参照	
4	電子メール、Web サイト閲覧の利用が限定的	・ブルーカラーの業務が多い（IT 関連企業を除く） ・業務上の外部とのやり取りは特定の人だけの企業が多い。	マルウェアの主たる感染経路は「電子メール」「Web サイト閲覧」である。
5	セキュリティ対策が十分でないが故に、不審メールに対する免疫力がある。	・ヒアリングで、左記の意見があった。普段からたくさんの不審メールがメールボックスに届くため、日常的に気を付けていると思われる。	

4.1.4 考察（サイバー攻撃状況の実態）

サイバー攻撃状況の実態は次であると推測する。

サイバー攻撃を受けているが、リスクの発生可能性は低い状態である。

サイバー攻撃を受けていることを確認できたが、お助け隊期間中のインシデント発生はなく、過去にサイバー攻撃による被害を受けた実証参加企業は一部だった。実証参加企業のリスクの発生確率は低いと考えられる。リスクの発生確率が低い要因は、「4.1.3 駆け付け対応・相談対応・ヒアリング結果」で示したとおり、次であると推測する。

- 監視対象が小規模
- 監視期間が短い
- お助け隊の UTM により攻撃を防御した
- 電子メール、Web サイト閲覧の利用が限定的
- セキュリティ対策が十分でないが故に、不審メールに対する免疫力がある。

ヒアリングの際に、セキュリティ対策を進めなければならないと感じているが、過去に被害を受けていないため、実施できていないとの回答があった。リスクの発生可能性が低い場合、「リスク保有」が妥当な判断となる。

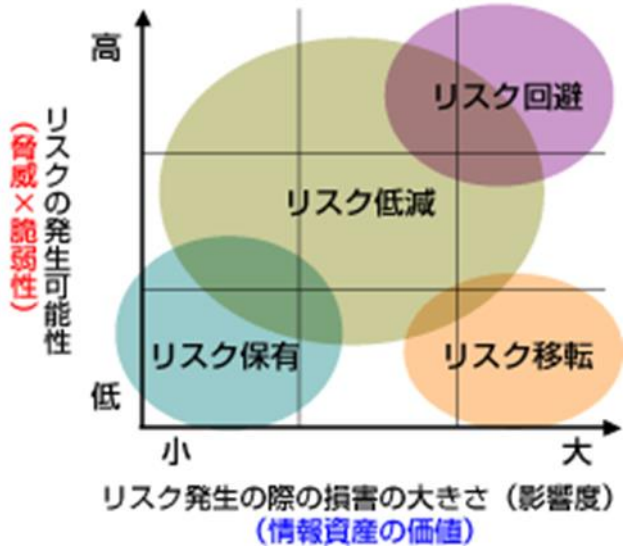


図 33 リスクへの対応（概念図）

IPA：情報セキュリティマネジメントと PDCA サイクル
https://www.ipa.go.jp/security/manager/protect/pdca/risk.html（2021/01/15 参照）.

過去であれば、セキュリティ対策を実施しない（リスク保有）が適切な判断になった可能性があるが、ランサムウェアのように業務遂行に致命的な影響を与える攻撃が多くなっている。ランサムウェアの影響が致命的なのは、リスク移転（サイバー保険）で金銭的な補償を得られても、業務遂行ができなくなることである。

サイバー攻撃が拡大・巧妙化している状況から「リスクの発生可能性」は今後高くなり、それにつれて「リスク発生の際の損害の大きさ」は今後大きくなると思われる。これは、大企業だけでなく、中小企業も同様であると予測される。

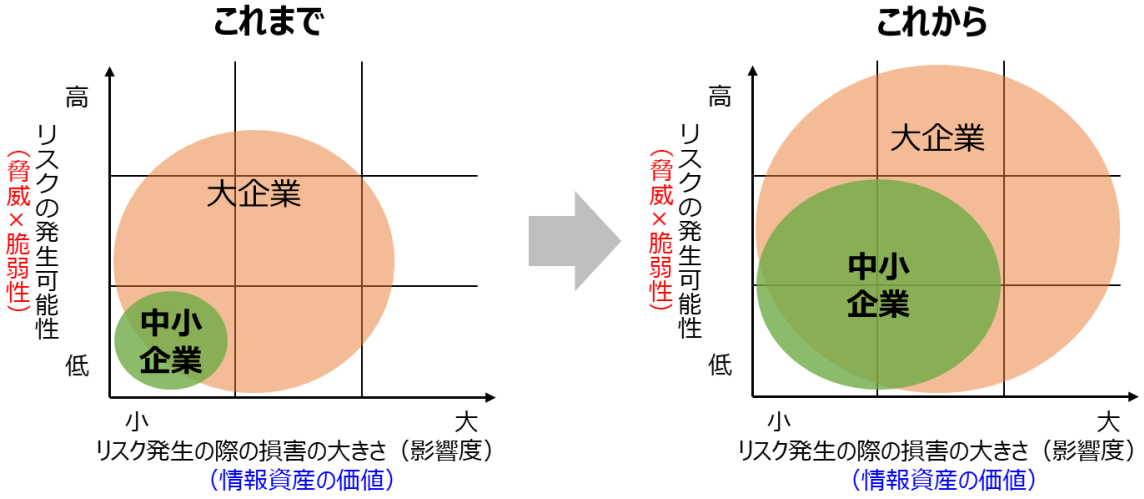


図 34 今後のリスクの発生可能性と影響度の予測

4.2 中小企業におけるセキュリティ対策を進める上での課題

4.2.1 アンケート結果

「セキュリティ対策を進める上での課題」に関するアンケートの結果、次の傾向であった。

- サイバーセキュリティ体制で「専任」9%、「兼任」38%、「明確にきまっていない」44%
- サイバーセキュリティ対策の相談先「あり」53%
- インシデント発生時の相談先「あり」53%
- 取引先からのセキュリティ対策の要求「あり」53%
- サイバー攻撃に遭い、事業継続に影響する被害を受ける可能性が「あると思う」56%
- セキュリティ対策の年間予算は「100 万円未満」94%
- 自社のセキュリティ対策状況の自己評価は「不十分」69%
- セキュリティ対策導入の障壁・課題で「費用を捻出することが困難」69%、「人的リソースが不足」78%、「対策を検討する要員の知識が不足」81%

自社のセキュリティ対策について約 70%の企業が「不十分」であると回答しており、約 80%の企業が十分なセキュリティ対策を構築できていないというアンケート結果は、セキュリティ対策のコストや人員の問題が障壁となっていると推測される。

アンケート結果の詳細を下表と下図に記す。

a．サイバーセキュリティ体制

表 57 サイバーセキュリティ体制

選択肢	回答数
専任	3 社
兼任	12 社
アウトソース（他社サービス利用、委託）	3 社
明確にきまっていない	14 社

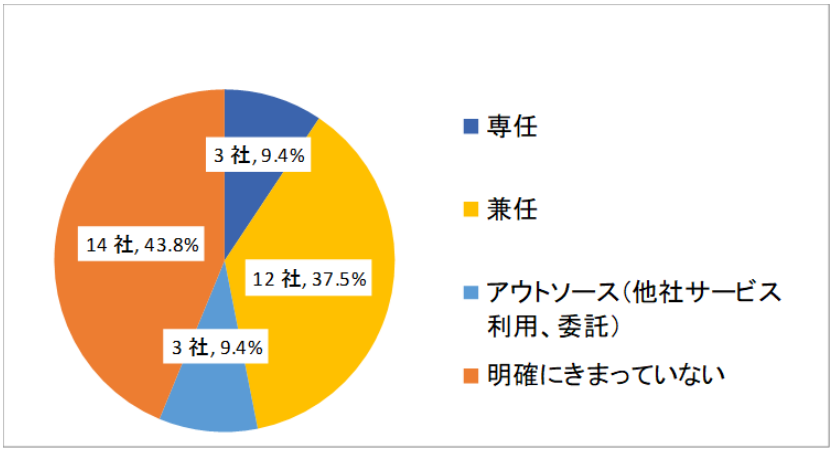


図 35 サイバーセキュリティ体制（n=32）

b．サイバーセキュリティ対策の相談先

表 58 サイバーセキュリティ対策の相談先

選択肢	回答数
あり	17 社
なし	15 社

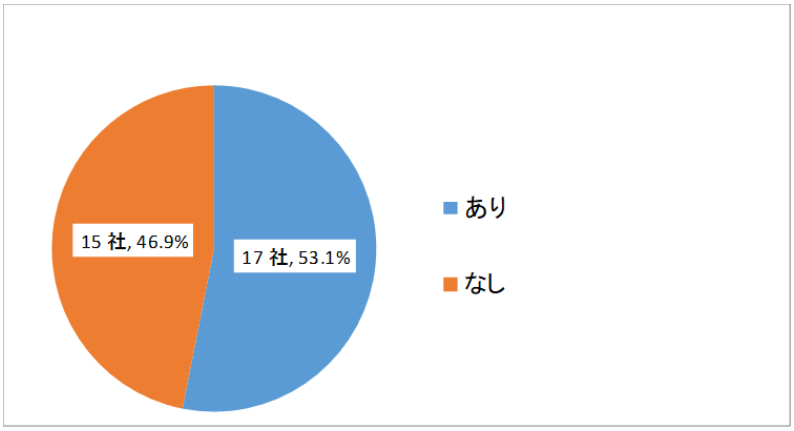


図 36 サイバーセキュリティ対策の相談先（n=32）

c．インシデント発生時の相談先

表 59 インシデント発生時の相談先

選択肢	回答数
あり	17 社
なし	15 社

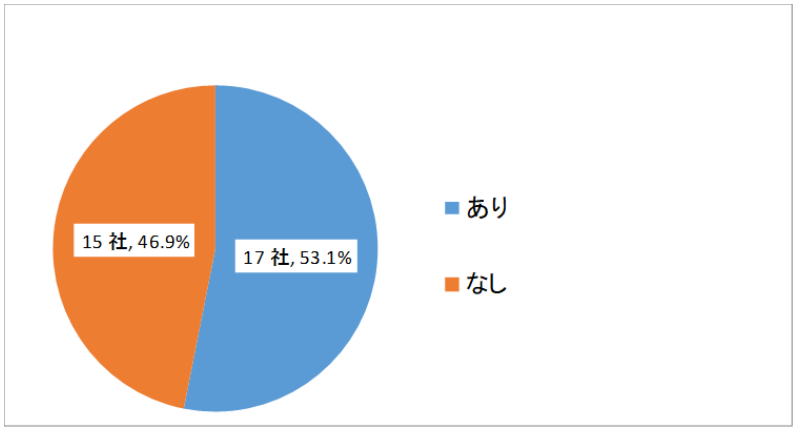


図 37 インシデント発生時の相談先（n=32）

d．取引先からのセキュリティ対策の要求

表 60 取引先からのセキュリティ対策の要求

選択肢	回答数
あり	17 社
なし	15 社

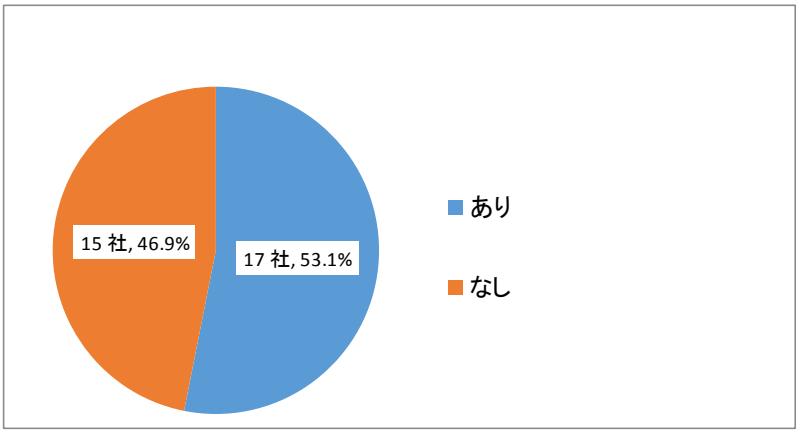


図 38 取引先からのセキュリティ対策の要求（n=32）

e．サイバー攻撃に遭い、事業継続に影響する被害を受ける可能性

表 61 事業継続に影響する被害を受ける可能性

選択肢	回答数
思う	18 社
思わない	2 社
わからない	12 社

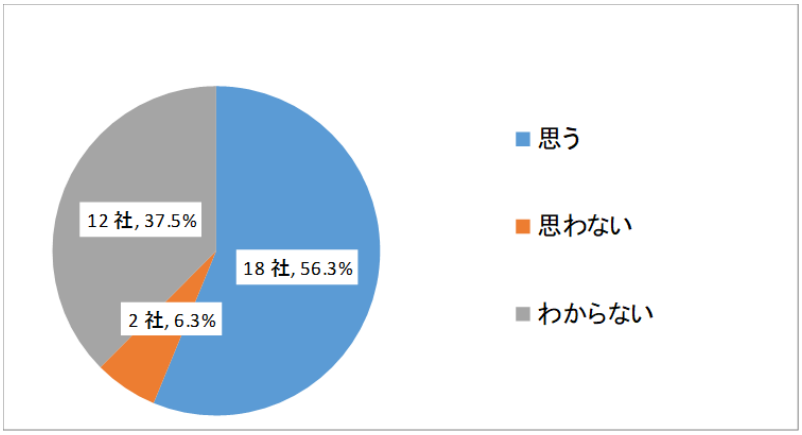


図 39 事業継続に影響する被害を受ける可能性（n=32）

f．セキュリティ対策の年間予算（人件費を除く）

表 62 セキュリティ対策の年間予算（人件費を除く）

選択肢	回答数
1000 万円以上	0 社
1000 万円未満	0 社
500 万円未満	2 社
100 万円未満	30 社

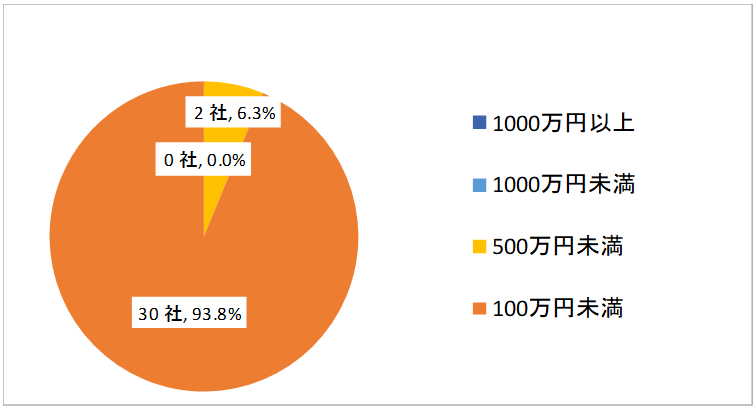


図 40 セキュリティ対策の年間予算（人件費を除く）（n=32）

g．自社のセキュリティ対策状況の自己評価

表 63 自社のセキュリティ対策状況の自己評価

選択肢	回答数
十分	4 社
不十分	22 社
わからない	6 社

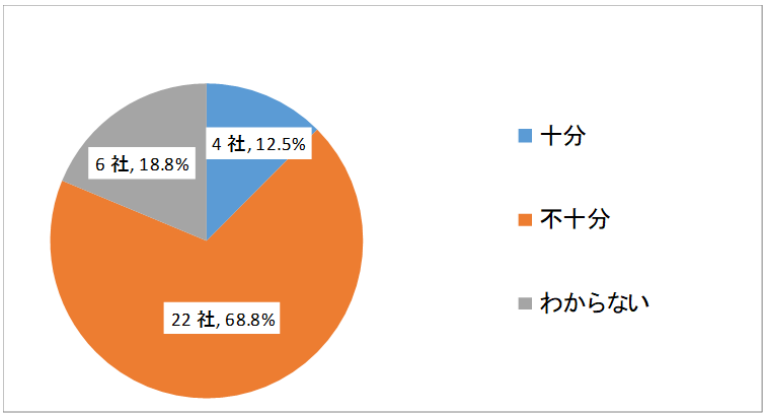


図 41 自社のセキュリティ対策状況の自己評価（n=32）

h．セキュリティ対策導入の障壁・課題

表 64 セキュリティ対策導入の障壁・課題

選択肢	回答数
費用を捻出することが困難	22 社
人的リソースが不足	25 社
対策を検討する要員の知識が不足	26 社
セキュリティ対策の効果が不明	12 社

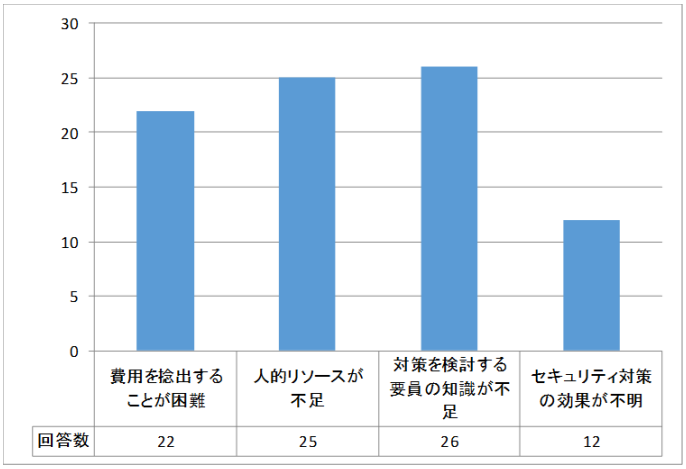


図 42 セキュリティ対策導入の障壁・課題（n=32）

i．サイバーセキュリティお助け隊事業に参加いただいた動機・理由

表 65 お助け隊事業に参加いただいた動機・理由

選択肢	回答数
①セキュリティサービスを体験したい	17 社
②セキュリティ対策水準を向上させたい	11 社
③セキュリティ要員の負荷を軽減したい	4 社
④セキュリティ対策に取り組んでいくきっかけとしたい	10 社
⑤無償だから	15 社

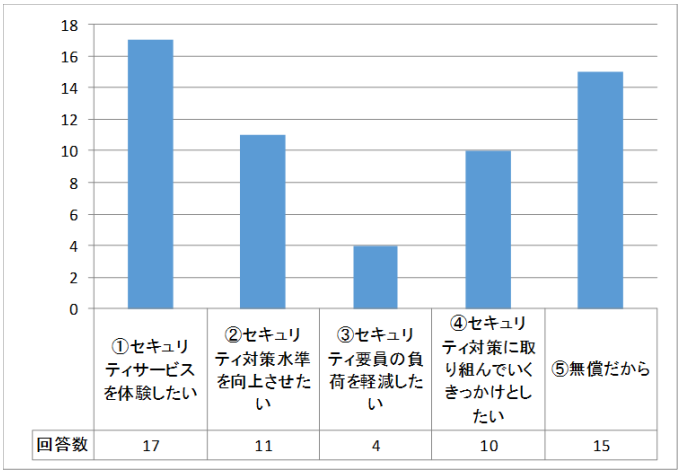


図 43 お助け隊事業に参加いただいた動機・理由（n=29）

ｊ．地域実証（提供するサービス）に期待すること

表 66 地域実証（提供するサービス）に期待すること

選択肢	回答数
①UTM によるサイバー攻撃防御	17 社
②UTM によるサイバー攻撃の実態把握	19 社
③可視化ツール（WatchManBox MR）を活用したインシデント遠隔支援	8 社
④セキュリティインシデント発生時の駆け付け対応	9 社
⑤セキュリティに関する相談対応	8 社
⑥簡易セキュリティ診断による自社セキュリティ対策実施状況の評価	10 社
⑦標的型攻撃メール対応訓練によるリスク把握および意識向上	10 社
⑧Web アプリケーション診断による公開 Web の脆弱性検出	9 社
⑨制御システム簡易リスクアセスメントによるリスクの見える化	3 社

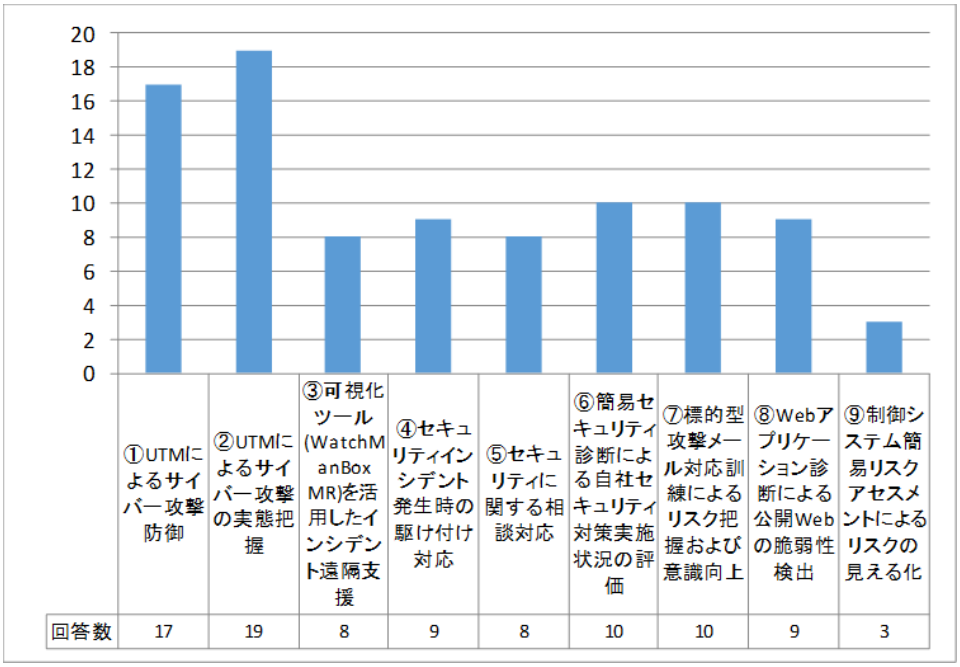


図 44 地域実証（提供するサービス）に期待すること（n=29）

k．本実証事業を知ったきっかけ

表 67 本実証事業を知ったきっかけ

選択肢	回答数
IPA サイト	0 社
採択事業者の紹介	19 社
商工会議所等の紹介	0 社
各種関連団体の紹介	4 社
知人・友人等の紹介	3 社
その他	6 社

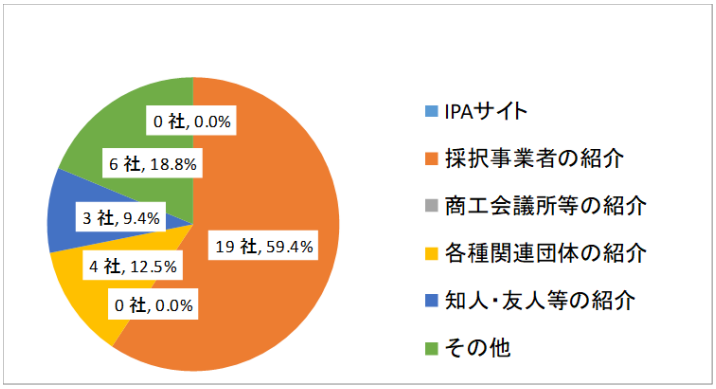


図 45 本実証事業を知ったきっかけ（n=32）

l．サイバーセキュリティお助け隊事業に期待する事項

表 68 サイバーセキュリティお助け隊事業に期待する事項

選択肢	回答数
セキュリティ対策の妥当性確認	17 社
セキュリティの向上	23 社
セキュリティ対策助言の入手	14 社
セキュリティ関連情報の入手	11 社
セキュリティ製品・サービスの利用	11 社
その他	2 社

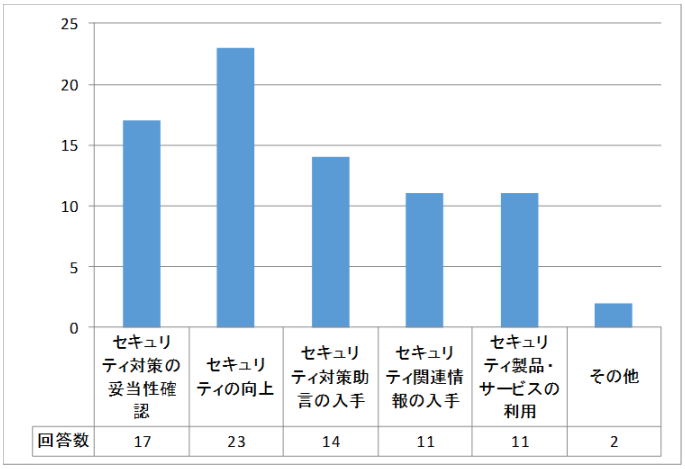


図 46 サイバーセキュリティお助け隊事業に期待する事項（n=32）

m. 「SECURITY ACTION」を宣言（お助け隊参加前）

表 69 「SECURITY ACTION」を宣言

選択肢	回答数
している	2 社
していない	30 社

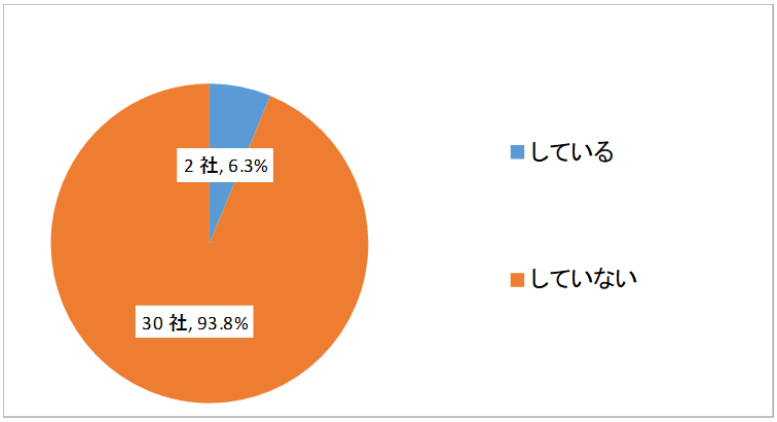


図 47 「SECURITY ACTION」を宣言（n=32）

n. 回答者の組織の立場

表 70 回答者の組織の立場

選択肢	回答数
経営層	9 社
管理職	9 社
一般職	11 社

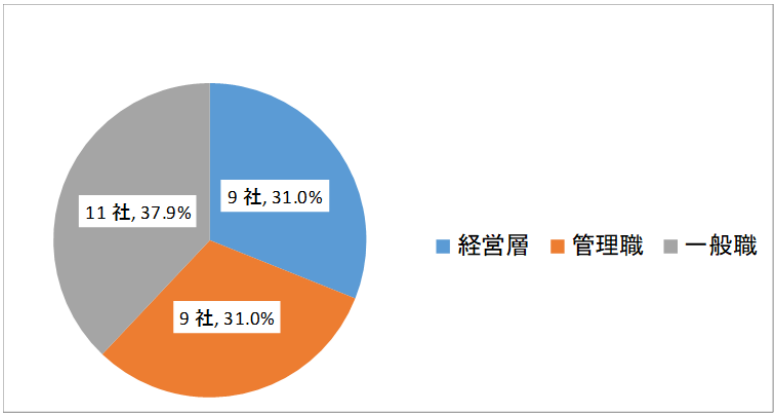


図 48 組織の立場（n=29）

4.2.2 相談対応・ヒアリング結果

ヒアリングを行った結果、アンケート結果と同様に次がセキュリティ対策を進める上での課題であるとの回答だった。

・セキュリティ対策費用の捻出が難しい
・人的リソースがない
・要員の知識が不足している

セキュリティ対策費用については「費用対効果がわからないため費用を出しにくい」「どれくらいの費用が妥当なのかわからない。目安となる金額があったら教えて欲しい」との意見があった。セキュリティ対策の難しい側面である。資産価値を算出し、リスクの発生確率を想定し、被害額を算出した上で、妥当なセキュリティ対策費用を捻出することが望ましいが、知識・経験がない人が適切な結果を出すことは難しい。

また、情報収集と分析ができておらず「何をしたら良いかわからない」と回答した企業が複数あった。IPA を含む公的機関や民間企業からもインターネット上に多くの情報が公開されているが、情報収集の人的リソースがないことと、情報収集の方法がわからないため、能動的に情報収集できていない実態が浮かび上がった。

経営層(多くが代表取締役)がひとりでセキュリティ対策を考えて実施している例があった。また、職位が高く、IT に詳しい人がひとりで対応している例もあった。セキュリティのための体制を構築できていないことがうかがえる。

昨年度のお助け隊の報告であったように、IT に関して分かる人がおらず、外部の業者に任せており、社内に分かる人材がいない事例があった。セキュリティだけでなく、IT の人材もいないことが課題である。

なお、以前は、パソコンに詳しい人が対応を行っている場合が多かった。しかし、IT の利用が多様化し、パソコンだけの知識では対応が難しい状況である。

4.2.3 考察（セキュリティ対策を進めていく上での課題）

セキュリティ対策を進めていく上での課題は次であると考える。

・「お金」「人」「情報」がない
・セキュリティ対策が十分でない

セキュリティに関するアンケートやヒアリングの結果から、次の状況であると推察する。

図 49 セキュリティ対策を進めていく上での中小企業の課題

(1) お金がない（投資ができない）

セキュリティ対策はお金を生まない。マイナスの費用（ネガティブコスト）を低減するものである。中小企業の規模でお金を生まないセキュリティ対策に投資することは簡単ではない。また、妥当なセキュリティ対策費用を算出することは簡単ではない。これらの理由から、セキュリティに投資できていないと考えられる。

まれにしか発生しない事象への対応は難しい。これはリスクの特性であり、リスクマネジメントの難しさである。被害を経験していなければ、投資の判断が難しい。

(2) 人がいない

セキュリティ対策投資には人的資源への投資が含まれる。中小企業は人的リソースに余裕がないことが多いこと、セキュリティ人材が不足していることから、セキュリティ技術・知識を持つ人材を確保・育成することは簡単ではない。また、セキュリティに限らず、環境への配慮など、企業に求められる責務が増えている。しかし、直接収入がない間接業務への人的投資は難しく、片手間でやらざるを得ない状況だと推察する。また、すべての作業が規模に比例して小さくなるのではなく、固定的な費用が発生する。これは、大企業よりも規模が小さい中小企業の方が、相対的に影響が大きい。どの中小企業も苦慮している課題だと推察する。

(3) 情報がない

能動的に収集しなければ、セキュリティに関する情報を得ることは難しい。セキュリティの担当者が明確になっていなければ、情報収集ができない。

また、ヒアリングの結果、SECURITY ACTION をお助け隊に参加することで初めて知ったと回答する企業が多かった。公的機関、民間ともに様々なセキュリティの啓発・普及活動を行っているが、中小企業に届いていない可能性がある。

(4) セキュリティ対策が不十分

前述した課題のうち、「情報」と「お金」がなければセキュリティ対策の実施は難しい。しかし、セキュリティ対策を決定・実施するためには「人」が最も重要な要素であると考える。

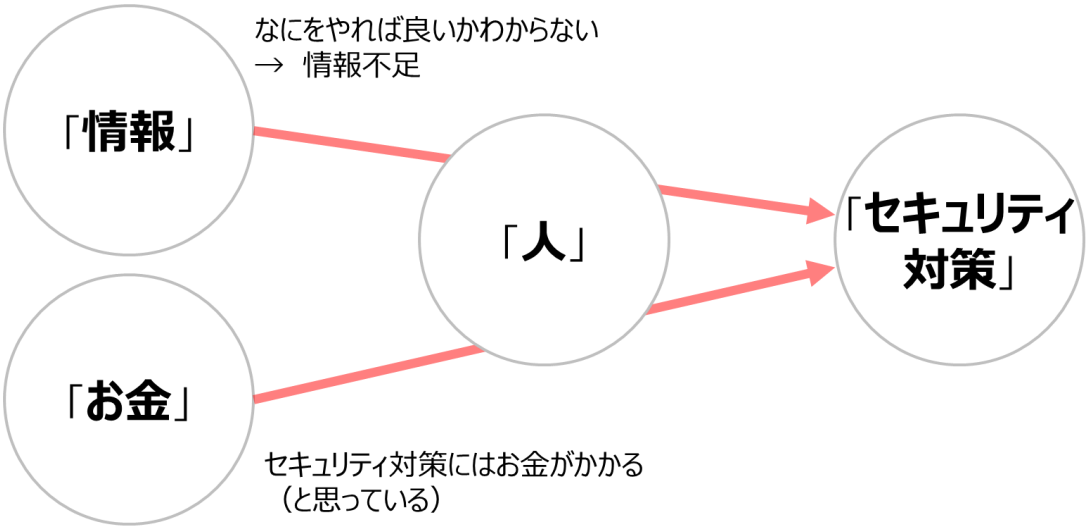


図 50 セキュリティ対策実施の課題

セキュリティ対策において「なにをやれば良いかわからない」状態、つまり情報が不足していると、セキュリティ対策が実施できない。また、お金がないとセキュリティ対策が実施できない部分がある。なお、人的リソースが必要になるが、お金がなくてもできる対策は多くある。

ここで、もし情報とお金があったとしても、セキュリティ対策を決定し、実施するのは「人」である。「人」がいなければ、セキュリティ対策の意思決定と実行ができない。セキュリティ対策はアウトソーシングできるが、意思決定はアウトソーシングできない。

昨年度のお助け隊の結果および TOiNX の提案でも、「伴走型支援」サービスが必要であると結論づけていた。しかし、アンケートの結果、約半数の企業でセキュリティ担当者が不明確である。伴走する相手がいなければ、伴走型支援サービスを提供できない。

20 年前のインターネット黎明期は、ウイルス対策ソフトを入れて、ファイアウォールを導入すれば多くのリスクを低減できた。それにも関わらず、当時ファイアウォールとウイルス対策ソフトを導入することは当たり前ではなく、実施しない企業もあった。文化として定着していなかった。これは、今は当たり前になったシートベルトと民間の自動車保険と同様である。

サイバー攻撃が拡大・巧妙化しているというのは、言い方を変えるとサイバー空間の治安が悪くなったということである。そのため自衛のための対策を実施しなければならない。一番簡単な回避策は、インターネットを利用しない（治安の悪いところに行かない）ことである。しかし、インターネットを利用せずに業務を行うことは難しくなっており、今後、クラウドサービスの利用が増え、ますますインターネットの必要性が増すと考えられる。

アンケートの結果、約 7 割の企業が自社のセキュリティ対策が不十分であると自己評価している。上記の状況のため、セキュリティ対策が進んでいないことがうかがえる。

セキュリティ対策の現状と課題は、「4.3 中小企業において必要なセキュリティ対策」に記す。

4.3 中小企業において必要なセキュリティ対策

4.3.1 セキュリティ対策実施状況（現状）

(1) アンケート結果

「必要なセキュリティ対策」に関するアンケートの結果、次の傾向であった。

- パソコンに対するウイルス対策で「実施している」100%
- 情報漏洩防止対策（外部へのファイル持出し時の暗号化や遮断等）を「実施している」60%
- USB 接続機器利用制限を「実施している」35%
- ハードディスク暗号化を「実施している」50%
- ネットワークで実施する対策でファイアウォールを「実施している」80%
- UTM（セキュリティ対策統合型ファイアウォール）を「実施している」55%
- パソコン以外のウイルス対策を「実施している」60%
- Web コンテンツフィルタリングを「実施している」35%
- 侵入検知/防御装置（IDS/IPS）を「実施している」20%
- サイバーセキュリティ保険加入有無で「加入している」10%
- 「Web アプリケーション脆弱性診断」の希望で「希望する」21%
- 「制御システム簡易リスクアセスメント」の希望で「希望する」4%

パソコンに対するウイルス対策は、すべての企業で実施済みであるが、UTM、パソコン以外のウイルス対策、Web コンテンツフィルタリング、侵入検知/防御装置（IDS/IPS）などネットワークで実施する対策は 40%以下にとどまった。

アンケート結果の詳細を下表と下図に記す。

a．サイバーセキュリティお助け隊事業参加前のセキュリティ対策実施状況

・パソコンに対する対策（モバイル用パソコンを含む）

－ウイルス対策（Windows Defender を含む）

表 71 パソコンに対する対策

選択肢	回答数
実施している	21 社
実施していない	0 社
わからない	0 社

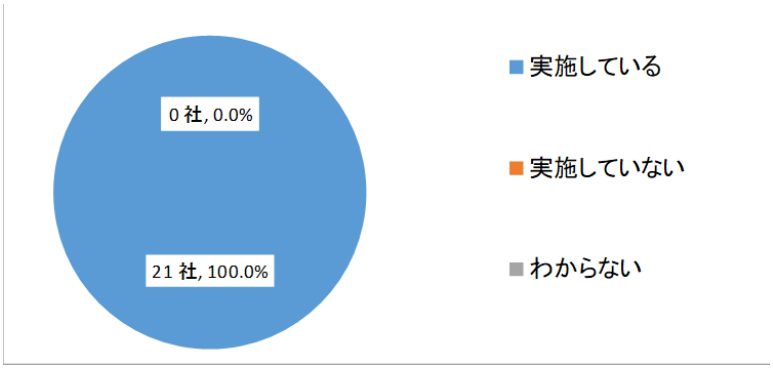


図 51 パソコンに対する対策（n=21）

・情報漏洩防止対策（外部へのファイル持出し時の暗号化や遮断等）

－ウイルス対策（Windows Defender を含む）

表 72 情報漏洩防止対策

選択肢	回答数
実施している	12 社
実施していない	9 社
わからない	0 社

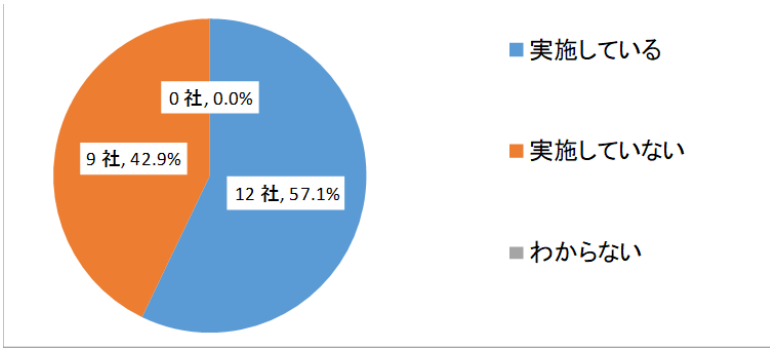


図 52 情報漏洩防止対策（n=21）

－USB 接続機器利用制限

表 73 USB 接続機器利用制限

選択肢	回答数
実施している	7 社
実施していない	14 社
わからない	0 社

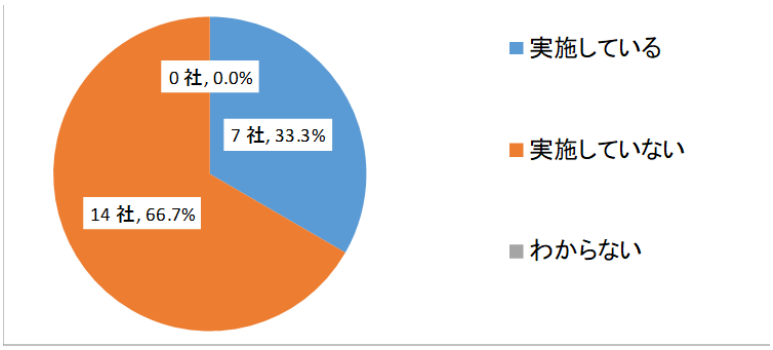


図 53 USB 接続機器利用制限（n=21）

－ハードディスク暗号化

表 74 ハードディスク暗号化

選択肢	回答数
実施している	10 社
実施していない	11 社
わからない	0 社

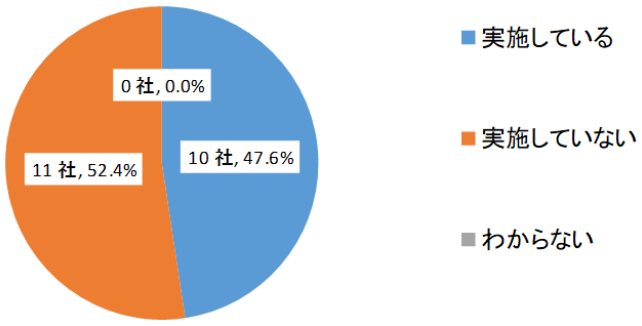


図 54 ハードディスク暗号化（n=21）

・ネットワークで実施する対策
－ファイアウォール

表 75 ファイアウォール

選択肢	回答数
実施している	17 社
実施していない	3 社
わからない	1 社

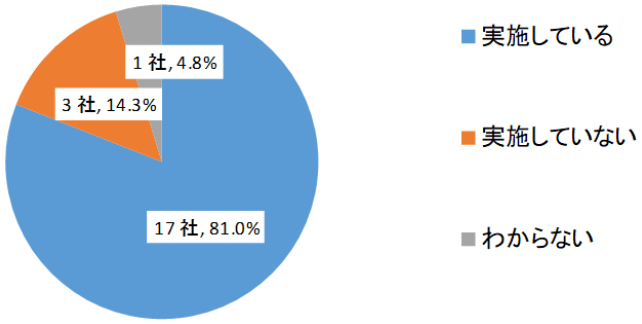


図 55 ファイアウォール（n=21）

－UTM（セキュリティ対策統合型ファイアウォール）

表 76 UTM（セキュリティ対策統合型ファイアウォール）

選択肢	回答数
実施している	12 社
実施していない	9 社
わからない	0 社

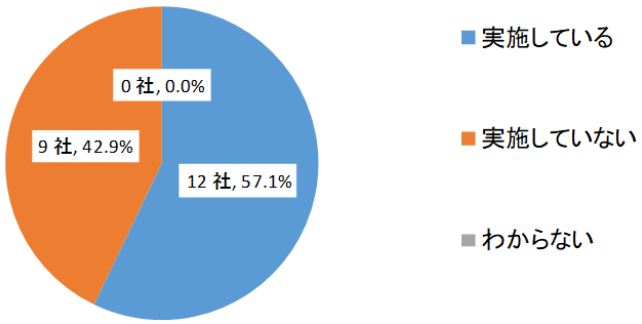


図 56 UTM（セキュリティ対策統合型ファイアウォール）（n=21）

－パソコン以外のウイルス対策

次を含みます。

ネットワーク上に設置した UTM 以外の製品

インターネットサービスプロバイダのサービス

クラウドのウイルス対策サービス

表 77 パソコン以外のウイルス対策

選択肢	回答数
実施している	12 社
実施していない	7 社
わからない	2 社

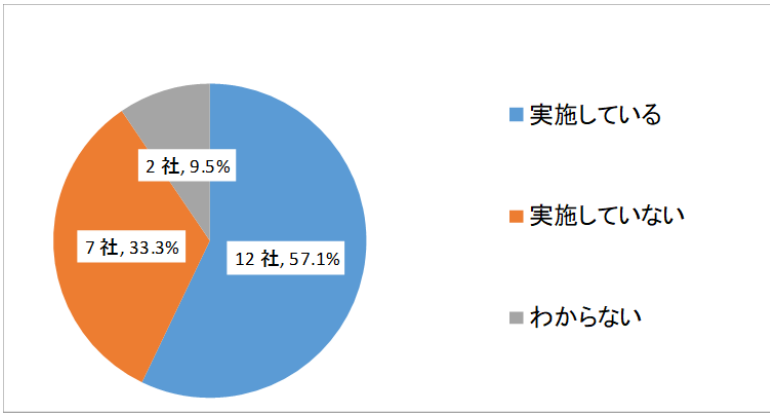


図 57 パソコン以外のウイルス対策（n=21）

－Web コンテンツフィルタリング

表 78 Web コンテンツフィルタリング

選択肢	回答数
実施している	8 社
実施していない	11 社
わからない	2 社

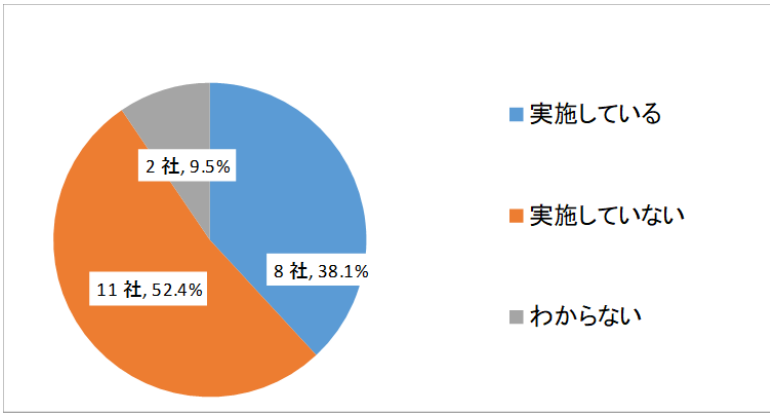


図 58 Web コンテンツフィルタリング（n=21）

－侵入検知/防御装置（IDS/IPS）

表 79 侵入検知/防御装置

選択肢	回答数
実施している	4 社
実施していない	13 社
わからない	4 社

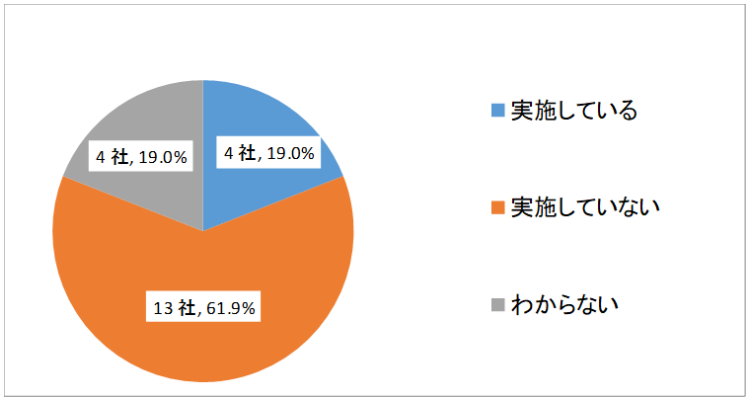


図 59 侵入検知/防御装置（n=21）

b．テレワークのアンケート結果

・テレワークの実施有無

表 80 テレワークの実施有無

選択肢	回答数
実施していない	6 社
実施している	7 社

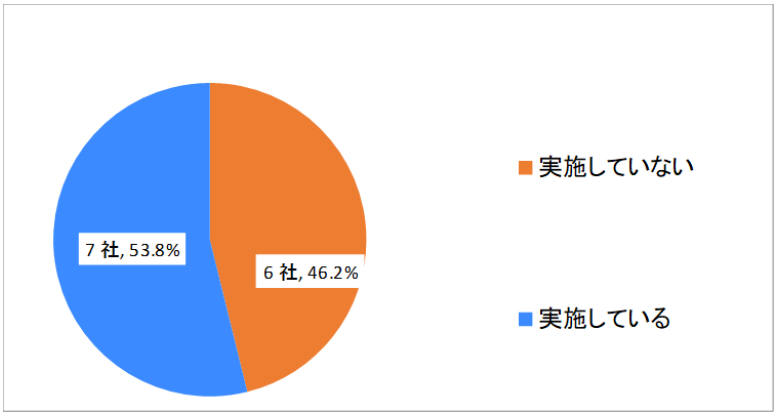


図 60 テレワークの実施有無（n=13）

・テレワークを実施していない理由

表 81 テレワークを実施していない理由

選択肢	回答数
必要ないため	2 社
テレワークを実施する機器がないため	0 社
セキュリティ対策が実施できない（間に合わない）ため	0 社
テレワークによるセキュリティ事故が懸念されるため	0 社
その他	4 社

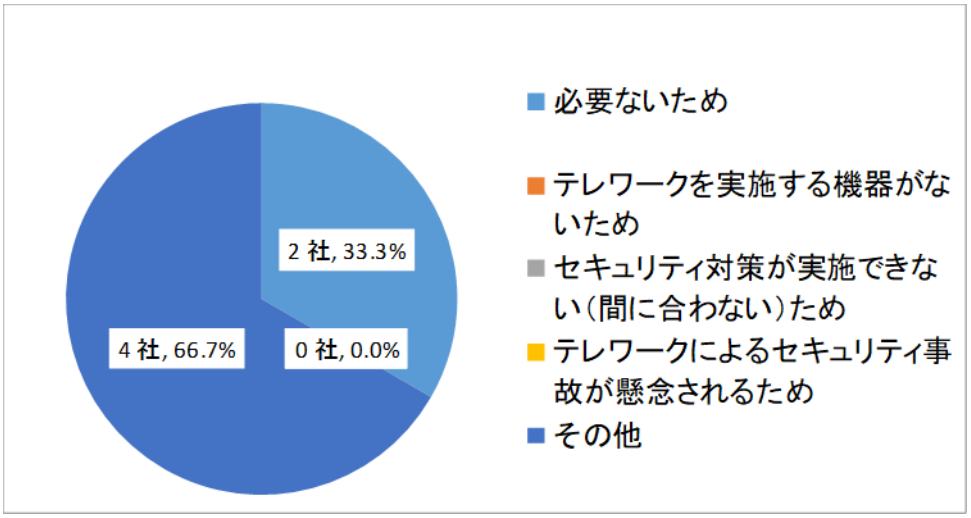


図 61 テレワークを実施していない理由（n=6）

・「その他」と回答された理由

表 82 「その他」と回答された理由

内容
店頭販売が主な為
テレワークできる商売じゃない
サービス業なのでテレワークを実施できない
業態がテレワークに馴染まないため

・テレワーク実施の割合

表 83 テレワーク実施の割合

選択肢	回答数
ごく一部（10%以下）	4 社
一部（30%以下）	2 社
半分	1 社
全員	0 社

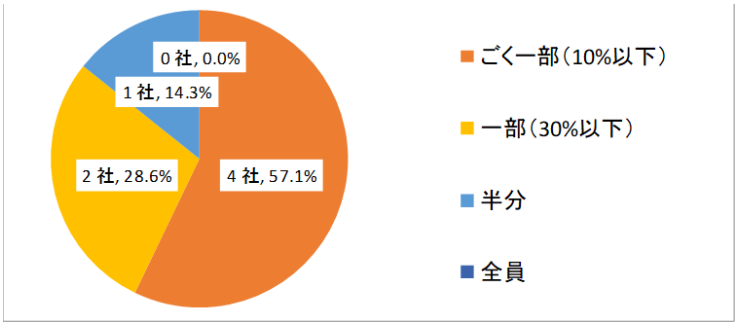


図 62 テレワーク実施の割合（n=7）

・テレワークの運用ルールの有無

表 84 テレワークの運用ルールの有無

選択肢	回答数
はい	5 社
いいえ	2 社

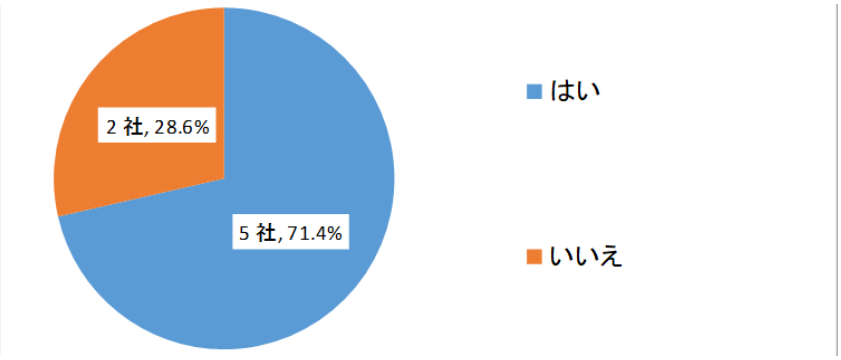


図 63 テレワークの運用ルールの有無（n=7）

・個人所有機器（BYOD）の利用有無

表 85 個人所有機器（BYOD）の利用有無

選択肢	回答数
はい	4 社
いいえ	3 社

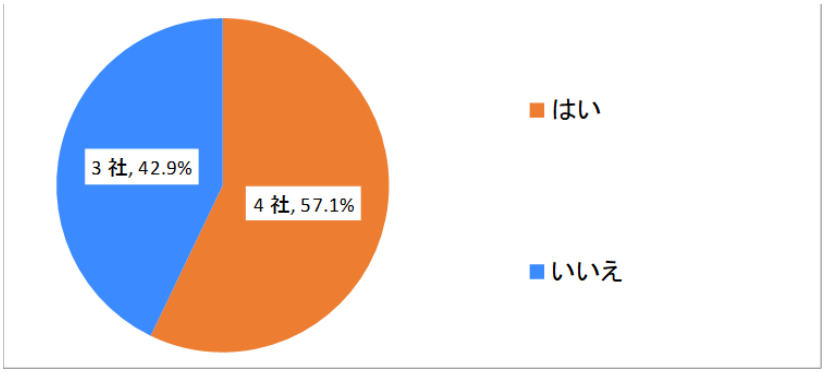


図 64 個人所有機器（BYOD）の利用有無（n=7）

・テレワークのためのセキュリティ対策

表 86 テレワークのためのセキュリティ対策

選択肢	回答数
VPN による社内ネットワークへの接続	5 社
VDI（仮想デスクトップ）による社内機器への接続	3 社
パソコンのハードディスク暗号化（盗難・紛失対策）	4 社
パソコンをインターネットに接続しない（ローカルに保存したファイルを編集するのみ）	0 社

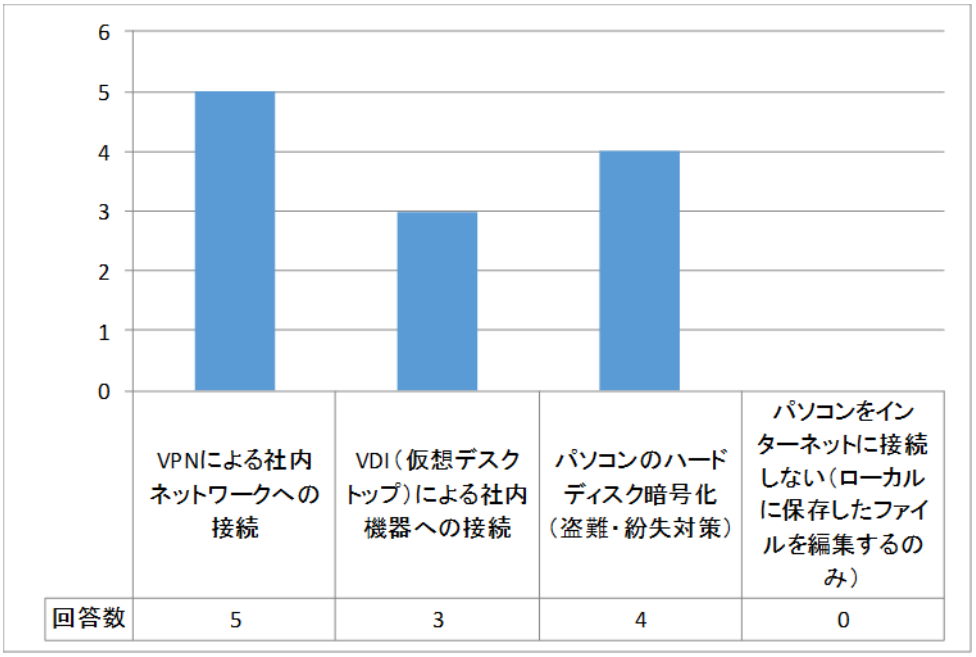


図 65 テレワークのためのセキュリティ対策（n=7）

・テレワークの課題

表 87 テレワークの課題

内容
生産性と効率の悪化が避けられない、コスト増、リーダークラスの負担が激増する
他部署とのコミュニケーション
現状利用しているサービス（NTT 東日本-IPA「シン・テレワークシステム」）の無償提供終了後のサービス検討

c．サイバーセキュリティ保険加入有無

表 88 サイバーセキュリティ保険加入有無

選択肢	回答数
加入している	3 社
加入していない	26 社

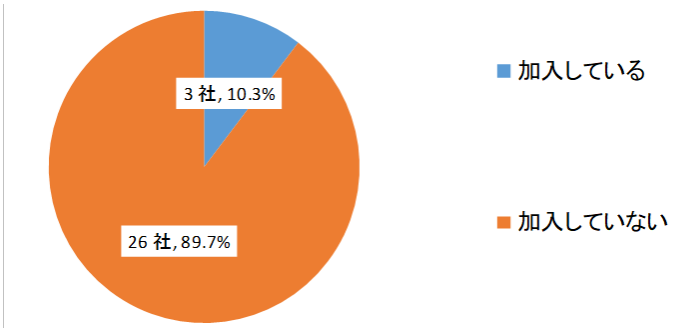


図 66 サイバーセキュリティ保険加入有無（n=29）

d．「Web アプリケーション脆弱性診断」の希望

表 89 Web アプリケーション脆弱性診断

選択肢	回答数
希望しない	22 社
希望する	6 社

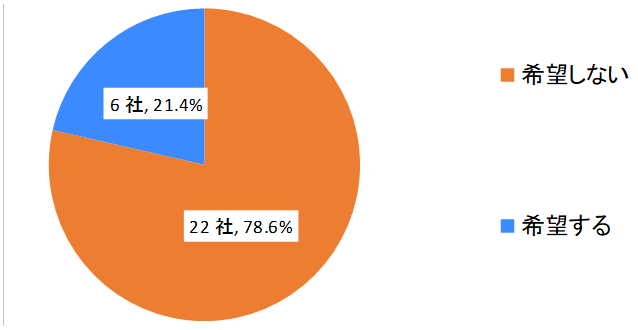


図 67 Web アプリケーション脆弱性診断（n=28）

e. 「制御システム簡易リスクアセスメント」の希望

表 90 制御システム簡易リスクアセスメント

選択肢	回答数
希望しない	27 社
希望する	1 社

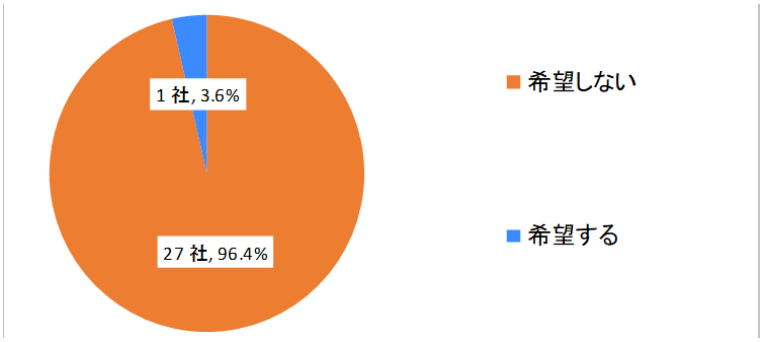


図 68 制御システム簡易リスクアセスメント（n=28）

(2) 簡易なセキュリティ診断結果（現状）

「5 分でできる！情報セキュリティ自社診断」の結果、実証参加企業の平均は、IPA が公表する統計平均よりも高かった。対策を実施できている企業と、実施できていない企業の間に大きな差が見られた。

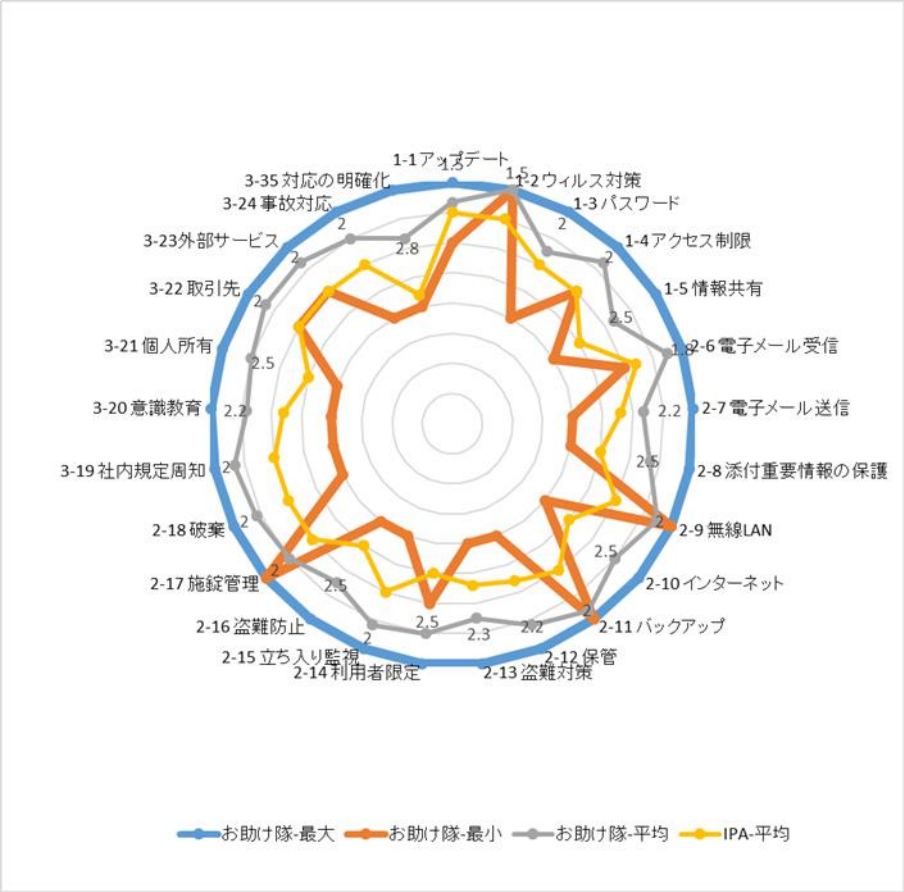


図 69 5 分でできる！情報セキュリティ自社診断（n=12）

「情報セキュリティ対策ベンチマーク」の結果、実証参加企業の平均は、IPA が公表する統計平均とほぼ同じだった。こちらも、対策を実施できている企業と、実施できていない企業の間に大きな差が見られた。

図 70 情報セキュリティ対策ベンチマーク（n=12）

(3) 相談対応・ヒアリング結果（セキュリティ対策実施状況）

ヒアリングの結果、セキュリティ対策を実施しなければならないことを認識しているが何をどこまでやれば良いかわからないと回答する企業が多かった。「4.2.3 考察（セキュリティ対策を進めていく上での課題）」に記載したとおり、「情報がない」ことでセキュリティ対策が進んでいない企業が多いと思われる。

また、ヒアリングの結果、セキュリティ対策を強化する計画がある企業は少なかった。人材育成を計画している企業も少なかった。

セキュリティ対策の費用は、ウイルス対策ソフトだけの企業が多くあった。規模が小さい企業はパソコンの数が少ないため、多くの費用はかからない。現状の費用が小さいため、追加対策のコストが大きく見える可能性がある。

希望するセキュリティ対策を確認したところ、次の回答があった。「人」「情報」に関するニーズがあることがうかがえる。

・セキュリティに関する情報を提供するサービス
・年に数回、相談できるサービス

4.3.2 考察（中小企業において必要なセキュリティ対策）

中小企業において必要なセキュリティ対策を検討した。検討した結果の要旨を次に記す。なお、ここでは中小企業の立場で必要なセキュリティ対策について考察した。そのため、中小企業が実施すべき事項が含まれる。実証終了後に提供するサービスの検討結果は「5. 実証を踏まえたビジネス化に向けた検討」に記載した。

実施すべき基本的なセキュリティ対策は企業規模に関わらず変わらない。セキュリティ対策を進めるためには、体制の構築が必要である。次に、お金をかけずに実施できるセキュリティ対策を含め、不足しているセキュリティ対策を実施することが望ましい。

必要なセキュリティ対策は、大企業であっても、中小企業であっても変わらない。なぜなら、セキュリティ対策は、資産の機密性・完全性・可用性を確保することが目的であり、中小企業も資産を保持している。言い換えれば、リスクマネジメントである。起きて欲しくない事象が起きることを想定して、事前および事後の対策を実施することである。

適切なセキュリティ対策は、保有資産や事業特性等により異なる。唯一の正解はない。しかし、セキュリティ対策を検討する上での原理・原則、方法論は共通である。組織的セキュリティ対策は「IPA 中小企業の情報セキュリティ対策ガイドライン」、防御・対応のセキュリティ対策は「米国国立標準技術研究所 重要インフラのサイバーセキュリティを改善するためのフレームワーク（以下、NIST CSF）」を指標に用いて、中小企業の将来像（あるべき姿）を考察する。

(1) 現状の考察

アンケートとヒアリング結果から、実証参加企業の現状は下表であると推測する。なお、以下に記載する事項の多くを実施できている実証参加企業がある。半数を目安に実施できていない場合に、対策を実施できていないと整理した。

表 91 サイバーセキュリティ経営ガイドライン 指示事項別中小企業の現状（推測）

サイバーセキュリティ経営ガイドライン指示事項	中小企業の現状
指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定	セキュリティポリシーを定めていない企業がある
指示 2 サイバーセキュリティリスク管理体制の構築	セキュリティ担当者が明確になっていない企業が約半数
指示 3 サイバーセキュリティ対策のための資源（予算、人材等）確保	多くの企業は年 100 万円以下の予算規模 人的リソースを割り当てられていない
指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	リスクがあることは認識しているが、具体的なリスクは想定できておらず計画を立てられていない
指示 5 サイバーセキュリティリスクに対応するための仕組みの構築	体制・技術的対策とも構築できていない企業が多い
指示 6 サイバーセキュリティ対策における PDCA サイクルの実施	体制・計画がないため、PDCA サイクルを回せていない企業が多い
指示 7 インシデント発生時の緊急対応体制の整備	インシデント発生時の緊急対応体制を整備できていない企業が多い
指示 8 インシデントによる被害に備えた復旧体制の整備	インシデントによる被害に備えた復旧体制を整備できていない企業が多い
指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策および状況把握	取引先からセキュリティ対策を要求されている 自社よりもサプライチェーンの下流側の企業は少ない
指示 10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用および提供	情報収集できていない。情報収集する担当を割り当てられていない。

会社により状況は異なるが、すべてをすぐに実現することは困難である。他の対策の前提となる指示 1・指示 2 を実現できなければ、それ以外の指示事項を適切に実施することは困難である。

表 92 NIST CSF 機能別中小企業の現状（推測）

機能	カテゴリー	中小企業の状況
識別	資産管理	資産管理、リスクアセスメントをできていない企業が多い
	ビジネス環境	
	ガバナンス	
	リスクアセスメント	
	リスクマネジメント戦略	
	サプライチェーンリスクマネジメント	
防御	アイデンティティ管理とアクセス制御	ファイアウォールとウイルス対策ソフト以外の対策を実施できていない企業がある
	意識向上およびトレーニング	
	データセキュリティ	
	情報を保護するためのプロセスおよび手順	
	保守	
	保護技術	
検知	異常とイベント	ウイルス対策ソフトの検知状況の確認など、現状を見える化できている企業は少ない
	セキュリティの継続的なモニタリング	
	検知プロセス	
対応	対応計画の作成	対応体制は十分でない インシデント発生時の相談先がある企業は半数程度 相談先の多くは、情報システムを導入した事業者
	コミュニケーション	
	分析	
	低減	
	改善	
復旧	復旧計画の作成	バックアップを取得できているが、復旧計画を作成できていないと思われる
	改善	
	コミュニケーション	

資産管理・リスクアセスメントができていないため、個別の適切なセキュリティ対策を立案することは困難であると思われる。

60%以上が実施している防御対策は、ファイアウォールとウイルス対策ソフトに留まっている。

多くの企業が検知・対応ができておらず、防御対策を実施しているのみである。

(2) 中小企業において必要なセキュリティ対策

現状のセキュリティ対策実施状況を踏まえて、優先的に実施すべきセキュリティ対策を考察した。結論を次に記す。もちろんこの対策だけ実施すれば良いのではない。環境が激しく変化するため、セキュリティ対策はマネジメントしなければならない。継続的な取組が必要である。

a . SECURITY ACTION 二つ星を宣言（情報セキュリティ基本方針を定める）
b . セキュリティの責任者、担当者を任命
c . 不足している防御対策を実施

a. SECURITY ACTION 二つ星を宣言

サイバーセキュリティ経営ガイドライン「指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定」は、SECURITY ACTION 二つ星を宣言すること、つまり「情報セキュリティ基本方針を定める」ことで達成できる。何のためにセキュリティ対策を実施するかを明確にし、経営層が承認することがスタートラインとなる。

b. セキュリティの責任者・担当者を任命

アンケートの結果、セキュリティ担当者が明確になっていない企業が約半数であることなどから、サイバーセキュリティ経営ガイドライン「指示 2 サイバーセキュリティリスク管理体制の構築」を達成できていない企業が多いと思われる。

「4.2.3 考察（セキュリティ対策を進めていく上での課題）」に記載したとおり、「人」がいないことが課題であり、この課題を解決することが最も重要であると考える。セキュリティに関する知識・技術がなくても、責任者・担当者を割り当てなければならない。

中小企業において、専任の対象者を割り当てることは難しいため、多くの場合兼務になると思われる。サイバー攻撃の対策は IT とは切り離せない。IT の担当との兼任が良いと考えられる。しかし、IT の担当者も明確になっておらず、導入事業者に丸投げの場合もある。セキュリティだけでなく IT も自社に知識・技術を持った人を保有することが困難な企業が多いと思われる。

自社だけで有効な体制を構築することは困難であるため、IT を導入した地場事業者への包括的な運用アウトソーシングにする等、範囲をセキュリティに限定しないことで、有効な体制を築ける可能性があると考える。

また、サイバーセキュリティ経営ガイドライン「指示 7 インシデント発生時の緊急対応体制」を構築することが望ましいが、中小企業で十分な体制を構築することは難しいと考える。こちらもアウトソーシングや外部サービス利用を検討することが望ましい。ただし、CSIRT の機能をすべてアウトソーシングすることはできない。会社の意思決定、外部、社内の窓口の機能は自社で実現しなければならない。

この考察を踏まえたビジネスモデルの検討結果は、「5. 実証を踏まえたビジネス化に向けた検討」を参照。

c．不足している防御対策を実施

NIST CSF の機能別に不足していると思われる対策を考察する。

(a) 識別

ヒアリングなどからの推測になるが、資産管理ができていないと推測される。また、制御リスク簡易リスクアセスメントで、情報システムの状況を確認した結果などからリスクアセスメントも実施していない企業が多いと推察する。

資産管理、リスクアセスメントは重要な対策だが、IT とセキュリティの知識・経験が少ない場合は、実施に多くの時間が必要になると思われる。

セキュリティアセスメントを実施すべきだが、短期的にはリスクシナリオに基づくリスクマネジメント戦略を検討することが良いと考える。まずは、中小企業においてもリスクが高い「ランサムウェアにより情報が暗号化され、情報システムが利用できなくなる」脅威の事前対策を検討することが推奨される。この対策の基本は、バックアップである。バックアップは、NIST CSF では「復旧」に該当する。復旧に関しては、(d) 復旧を参照。

(b) 防御

60%以上が実施している防御対策は、ファイアウォールとウイルス対策ソフトに留まっている状況から、先に防御対策を強化すべきと考える。

防御対策で費用対効果が高いのは、UTM である。防御対象が小規模であれば、機器およびライセンスが安価であり、UTM 配下の機器をすべて防御できるため、機器一台当たりの単価が安くなる。

また「情報セキュリティ 5 か条」に示されている「1.OS やソフトウェアは常に最新の状態にしよう！」「4.共有設定を見直そう！」などのお金をかけずにできる対策も効果がある。これらの対策実施状況は確認できていないが、セキュリティ体制が構築されていない状況から実施できていないことが懸念される。

(c) 検知・対応

標的型攻撃を完全に防ぐことが難しいため、NIST CSF で示されているように「検知・対応・復旧」の重要性が増している。

ヒアリングの結果などから、ウイルス対策ソフトの検知状況を確認していない企業、UTM を導入している企業でもログの確認をしていない企業があることから、検知できる仕組みを構築できていないと思われる。

約半数の企業がアンケートでインシデント対応の相談先があると回答しており、ヒアリングの結果、情報システムを導入した事業者であることが多かった。一定水準の対応は可能だと推察するが、セキュリティの専門企業ではないため、標的型攻撃のような高度な攻撃の対応は難しいと思われる。相談先がない企業を含め、十分な対応体制ではないと推測する。

なお、検知・対応は、防御対策が有効に機能していることが前提である。もし、防御機能が十分でない場合、「検知・対応・復旧」を行わなければならないインシデントが増えるため、対応コストが大きくなる。

（d） 復旧

「5 分でできる！情報セキュリティ自社診断」の「2-11 バックアップ」の回答結果の平均が「1.2」であった。選択肢は「1 実施している」「2 一部実施している」である。

「情報セキュリティ対策ベンチマーク」の「15.バックアップ」の回答結果の平均は「3.0」であった。選択肢は「3 方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。」である。

この結果から、バックアップは実施されていると思われる。しかし、アンケートやヒアリングで確認できなかったが、他のセキュリティ対策の実施状況から、復旧計画を作成できていない企業が多いと思われる。

4.4 中小企業におけるセキュリティ対策の効果

4.4.1 アンケート結果

地域実証のサービスごとの効果有無をアンケートで確認した結果を記載する。
「必要なセキュリティ対策」に関するアンケートの結果、次の傾向であった。

- 全体の満足度は、「満足」と回答した企業は 76%（21 社中 : 16 社[満足 5 社+やや満足 11 社]）、「不満」と回答した企業は 14%（21 社中：3 社[不満 3 社+やや不満 0 社]）
- セキュリティログ監視（UTM による脅威防御）および対応支援の満足度は、「満足」と回答した企業は 71%（21 社中 : 15 社[満足 6 社+やや満足 9 社]）、「不満」と回答した企業は 10%（21 社中：2 社[不満 2 社+やや不満 0 社]）
- サイバーセキュリティ保険の満足度は、「満足」と回答した企業は 19%（21 社中：4 社[満足 2 社+やや満足 2 社]）、「不満」と回答した企業は 0%（21 社中：0 社[不満 0 社+やや不満 0 社]）
- 標的型攻撃メール対応訓練の満足度は、「満足」と回答した企業は 67%（18 社中 : 12 社[満足 7 社+やや満足 5 社]）、「不満」と回答した企業は 11%（18 社中：2 社[不満 2 社+やや不満 0 社]）
- Web アプリケーション脆弱性診断の満足度は、「満足」と回答した企業は 36%（11 社中 : 3 社[満足 2 社+やや満足 1 社]）、「不満」と回答した企業は 9%（11 社中 : 1 社[不満 1 社+やや不満 0 社]）
- 制御システム簡易リスクアセスメントの満足度は、「満足」と回答した企業は 22%（9 社中 : 2 社[満足 1 社+やや満足 1 社]）、「不満」と回答した企業は 23%（9 社中：2 社[不満 1 社+やや不満 1 社]）
- サイバーセキュリティお助け隊参加の目的の達成度は、「達成できた」と回答した企業は 29%（21 社中 6 社）、「一部達成できた」と回答した企業は 52%（21 社中 11 社）、「達成できなかった」と回答した企業は 19%（21 社中 4 社）

全体の満足度は約 76%の企業が「満足」と回答している。また、お助け隊参加の目的の達成度は、「達成できた」と回答した企業は 29%、「一部達成できた」と回答した企業は 52%であり、効果の程度に差があると思われるが、80%以上の実証参加企業に効果があったと評価できる結果だったと思われる。

アンケート結果の詳細を下表と下図に記す。

a．満足度：全体（総合評価）

表 93 全体（総合評価）

選択肢	回答数
満足	5 社
やや満足	11 社
どちらでもない	2 社
やや不満	0 社
不満	3 社

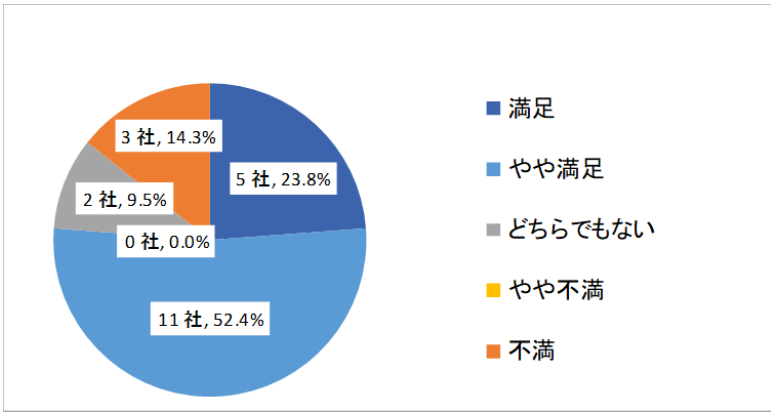


図 71 全体（総合評価）（n=21）

b．満足度：セキュリティログ監視（UTM による脅威防御）および対応支援

表 94 セキュリティログ監視（UTM による脅威防御）および対応支援

選択肢	回答数
満足	6 社
やや満足	9 社
どちらでもない	4 社
やや不満	0 社
不満	2 社
サービスを受けていない	0 社

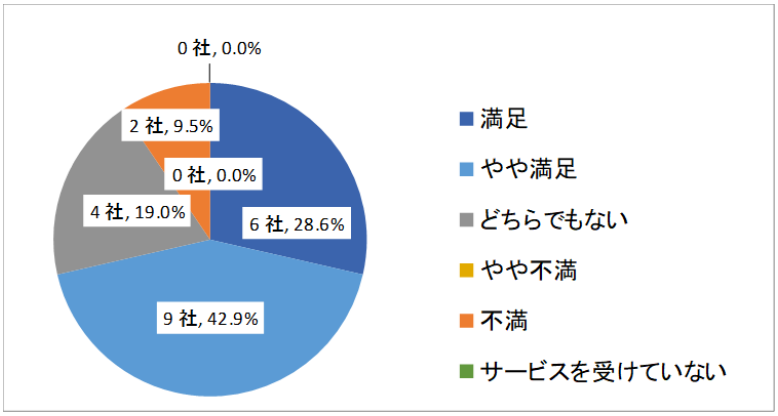


図 72 セキュリティログ監視（UTM による脅威防御）および対応支援（n=21）

c．満足度：サイバーセキュリティ保険

表 95 サイバーセキュリティ保険

選択肢	回答数
満足	2 社
やや満足	2 社
どちらでもない	17 社
やや不満	0 社
不満	0 社
サービスを受けていない	0 社

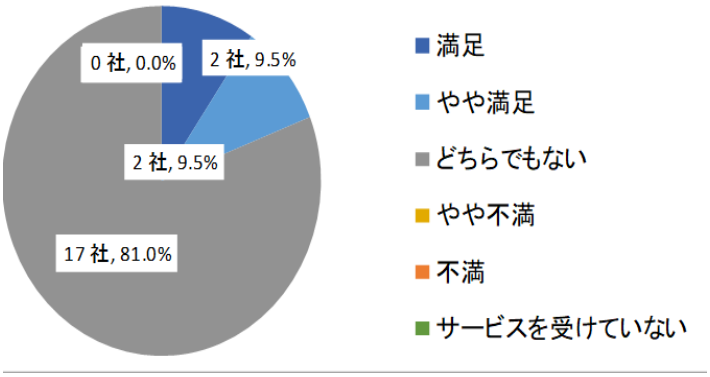


図 73 サイバーセキュリティ保険（n=21）

d．満足度：標的型攻撃メール対応訓練

表 96 標的型攻撃メール対応訓練

選択肢	回答数
満足	7 社
やや満足	5 社
どちらでもない	4 社
やや不満	0 社
不満	2 社
サービスを受けていない	3 社

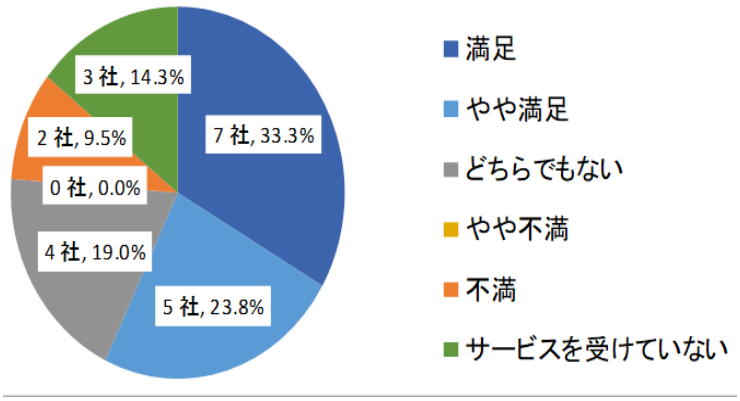


図 74 標的型攻撃メール対応訓練（n=21）

e．満足度：Web アプリケーション脆弱性診断

表 97 Web アプリケーション脆弱性診断

選択肢	回答数
満足	2 社
やや満足	2 社
どちらでもない	6 社
やや不満	0 社
不満	1 社
サービスを受けていない	10 社

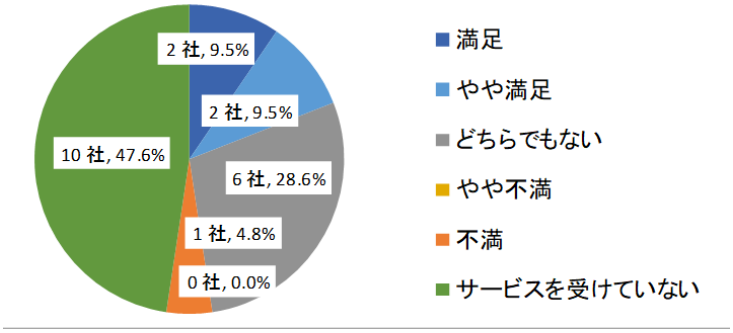


図 75 Web アプリケーション脆弱性診断（n=21）

f．満足度：制御システム簡易リスクアセスメント

表 98 制御システム簡易リスクアセスメント

選択肢	回答数
満足	1 社
やや満足	1 社
どちらでもない	5 社
やや不満	1 社
不満	1 社
サービスを受けていない	12 社

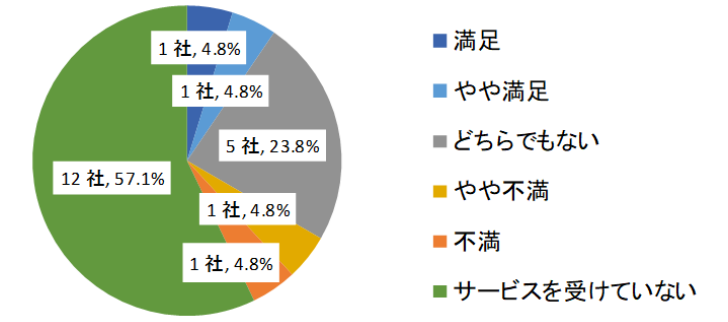


図 76 制御システム簡易リスクアセスメント（n=21）

g．改善して欲しいこと

表 99 改善して欲しいこと

内容
標的型攻撃メール対応訓練において、件名および差出人名があからさますぎて訓練となりうるのか疑問が残った。
期間が短すぎるため評価が困難
FortiGate を設置すると、拠点のパソコンからインターネットへのアクセス速度が極端に低下し、業務に支障を来した。そのため、ほとんどお助け隊サービスを受けられていない。

h．サイバーセキュリティお助け隊参加の目的の達成度

表 100 お助け隊参加の目的の達成度

選択肢	回答数
達成できた	6 社
一部達成できた	11 社
達成できなかった	4 社

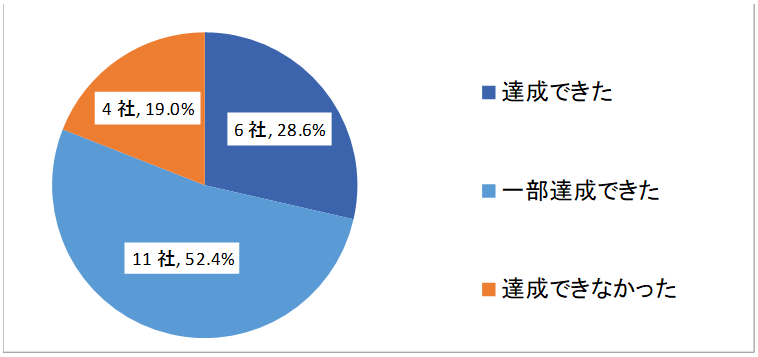


図 77 お助け隊参加の目的の達成度（n=21）

i．事業参加に伴うセキュリティ意識の変化

表 101 事業参加に伴うセキュリティ意識の変化

選択肢	回答数		
	経営層	情報システム担当	一般社員
向上した	4 社	7 社	3 社
やや向上した	9 社	6 社	8 社
変わらない	7 社	8 社	10 社
わからない	1 社	0 社	0 社

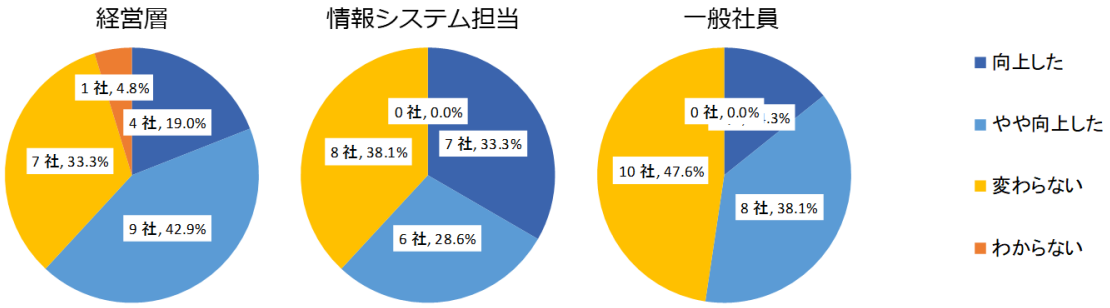


図 78 事業参加に伴うセキュリティ意識の変化（n=21）

j．参加をきっかけに実施した追加のセキュリティ対策

表 102 参加をきっかけに実施した追加のセキュリティ対策

内容
SECURITY ACTION 宣言

k．参加をきっかけに実施する予定のセキュリティ対策

表 103 参加をきっかけに実施する予定のセキュリティ対策

内容
UTM 設置
ネットワーク検疫システムの導入検討
予定のみ。具体策は検討中

l．お助け隊事業で提供した以外に希望するサービス

表 104 お助け隊事業で提供した以外に希望するサービス

内容
特になし

4.4.2 効果があったと評価できる事例

お助け隊を実施することにより効果があったと評価できる事例を記載する。

(1) アンケート結果

ａ．達成度

達成度に関するアンケート結果から、多くの実証参加企業で程度の差はあると思われるが、達成できた企業の割合が多いことから、効果があったと推察する。

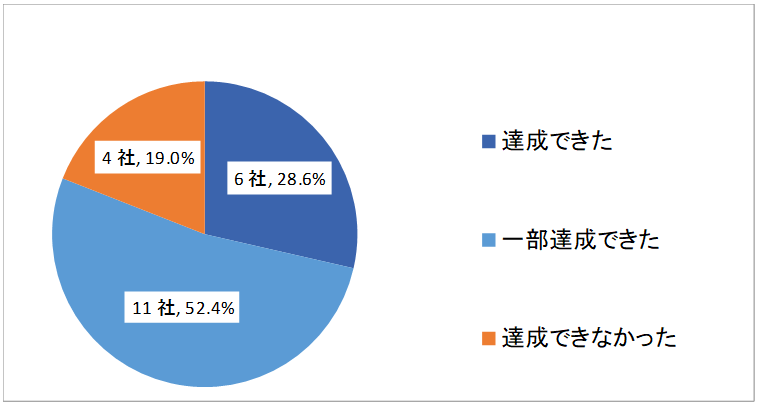


図 79 お助け隊参加の目的の達成度（n=21）（再掲）

選択肢	回答数
①セキュリティサービスを体験したい	17 社
②セキュリティ対策水準を向上させたい	11 社
③セキュリティ要員の負荷を軽減したい	4 社
④セキュリティ対策に取り組んでいくきっかけとしたい	10 社
⑤無償だから	15 社

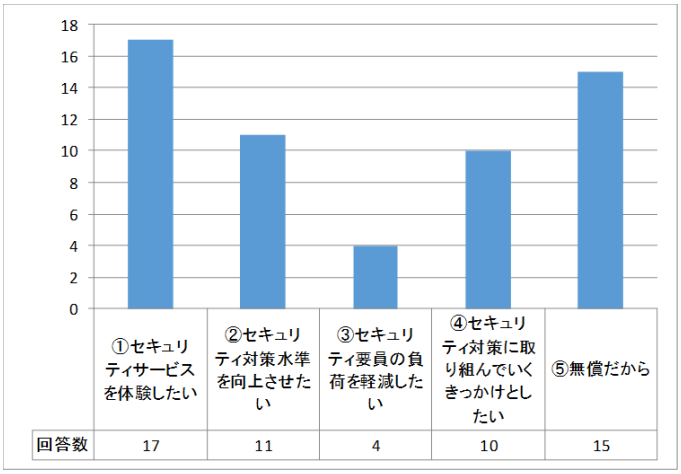


図 80 お助け隊事業に参加いただいた動機・理由（n=29）（再掲）

b. 意識の変化

アンケートに回答した企業の半数以上が、経営層、情報システム担当、一般社員ともに、向上したまたはやや向上したと評価している。意識向上に寄与できたと考える。

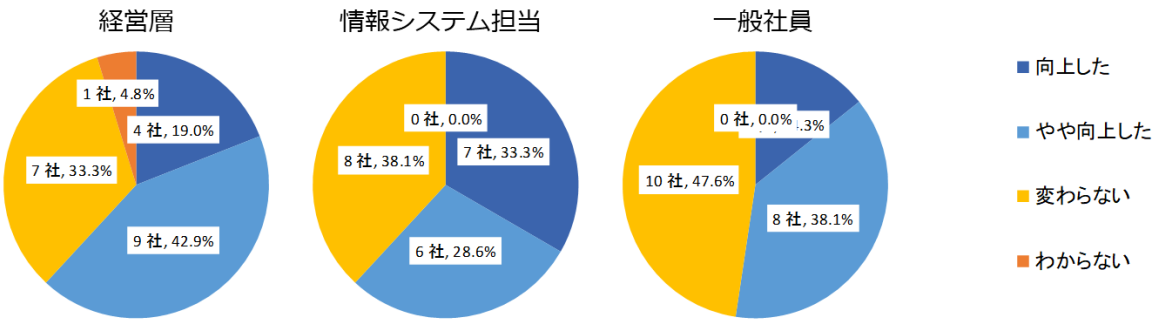


図 81 事業参加に伴うセキュリティ意識の変化（n=21）

(2) ヒアリング結果

ヒアリングの結果、効果があったと考えられる次のコメントを得た。

- UTM により、目に見える形で状況を把握できた。
- 見える化できた事象を教育・注意喚起に活用できる。
- インシデントは発生しなかったので体験できなかったが、いざというときに助かると思う。
- UTM が大事だとあらためて思った。いろんなものを試す価値がある。
- お助け隊がなければこのようなセキュリティ対策は実施しなかった。
- 啓発、勉強になった。
- UTM により実態に色々気付くことができた

(3) SECURITY ACTION 宣言企業数

アンケートの「参加をきっかけに実施した追加のセキュリティ対策」で「SECURITY ACTION 宣言」と回答した企業があったように、お助け隊参加後に「SECURITY ACTION 宣言」をした企業があった。

表 105 SECURITY ACTION 宣言企業数

宣言	一つ星 （A）	二つ星 （B）	合計 （C=A+B）	比率 （D=C/40）
企業数	4	2	6	15%

4.4.3 考察（セキュリティ対策の効果）

セキュリティ対策は何をすれば良いかわからない企業にとって、お助け隊の参加はセキュリティ対策に取り組む良いきっかけになったと考えられる。

「4.4.2 効果があったと評価できる事例」に示した通り、次の効果があった。

・意識が向上した
・サイバー攻撃を見える化できた
・SECURITY ACTION 宣言をするなど、セキュリティ対策に取り組むきっかけになった。

一方、満足度が低い企業もあった。原因についてはこれから分析するが、サービス品質や内容の改善が必要な部分があると考えられる。

4.5 産業構造別考察

4.5.1 情報システム産業のサプライチェーン

情報システム産業の実証参加企業は、簡易なセキュリティ診断の結果、ほとんどの企業が良い評価だった。また、ヒアリング等からも基本的なセキュリティ対策を実施していることがうかがえる結果だった。

ヒアリングしたすべての企業が、すべての案件でセキュリティ対策の実施を要求されるとの回答だった。これは、情報システム産業が「情報」を扱う業種であり、サイバー攻撃を受けた際の影響が大きいこと、業界全体のセキュリティ意識が高いことが一因だと思われる。TOiNX も情報システム産業の企業であり、扱う情報の重要度に応じたセキュリティ対策実施が委託する条件になっている。取引先からのセキュリティ対策を要求されているため、セキュリティ対策が進んでいると考えられる。

また、ほとんどの開発業務をテレワークで行っている企業があった。開発業務は物理的な制約を受けないことが多いため、セキュリティの課題を解決できれば、テレワークを推進しやすい。新型コロナウイルスが流行する前から取り組んでいる企業が多かった。特にクラウド上で動作させるアプリケーションの開発は、データをローカルパソコンに置かずに開発している。

しかし、非常に機微な情報を取り扱う「電力」や「銀行」などの開発は、物理的にクローズされた環境で行っている。

4.5.2 中小規模の製造業

大企業で制御システムを狙ったサイバー攻撃が発生しているが、制御システム簡易リスクアセスメントを実施した中小企業は、サイバー攻撃の被害に遭っていない。また、制御システム（制御機器）は、ネットワークに接続されておらず、スタンドアロンで動作しているため、サイバー攻撃を受けた場合でもすぐに全体に影響する事象が発生する可能性は低い状態である。

今後、制御システムへのサイバー攻撃のリスクが大きくなると思われるので、被害が発生する前にセキュリティ対策を進めることが推奨される。

情報システムにおいては、特に他の中小企業と大きく異なる点はなかった。

5. 実証を踏まえたビジネス化に向けた検討

5.1 サイバー保険の活用

次のプロセスでサイバー保険の活用を検討する計画とした。しかし、保険設計の結果、一律でサービス費用が高くなること、保険商品の制約からオプションにできないことから、低価格でサービスを提供することができなくなるとの結論に達した。そのため、商品付帯型ではなく、顧客の企業規模・業種・希望に合わせて設計する損害保険会社の商品を提供する方針とした。そのため、「再調査」「保険再設計」は実施していない。

図 82 サイバー保険検討プロセス

5.1.1 マーケティング（アンケート、ヒアリング結果）

サイバーセキュリティ保険に入っていない割合が高い。その理由として「サイバーセキュリティ保険の存在を知らない」回答の割合が高かった。ヒアリングした際も、サイバー保険の内容を知らないと回答する企業が多かった。

しかし、サイバーセキュリティ保険の有用性は認識しており、サイバー保険に入りたいと考えている企業が多かった。

アンケート結果を次に示す。

ａ．サイバーセキュリティ保険に加入していない理由

表 106 サイバーセキュリティ保険に加入していない理由

選択肢	回答数
①　サイバーセキュリティ保険の存在を知らない	12 社
②　自社に必要ないと思う	2 社
③　サイバーセキュリティ保険のメリットが分からない	4 社
④　自社のサイバー攻撃を受けるリスクを把握していない	6 社
⑤　保険の加入手続きが面倒	1 社
⑥　価格面で加入に至っていない	7 社
⑦　保険の加入方法が分からない	2 社

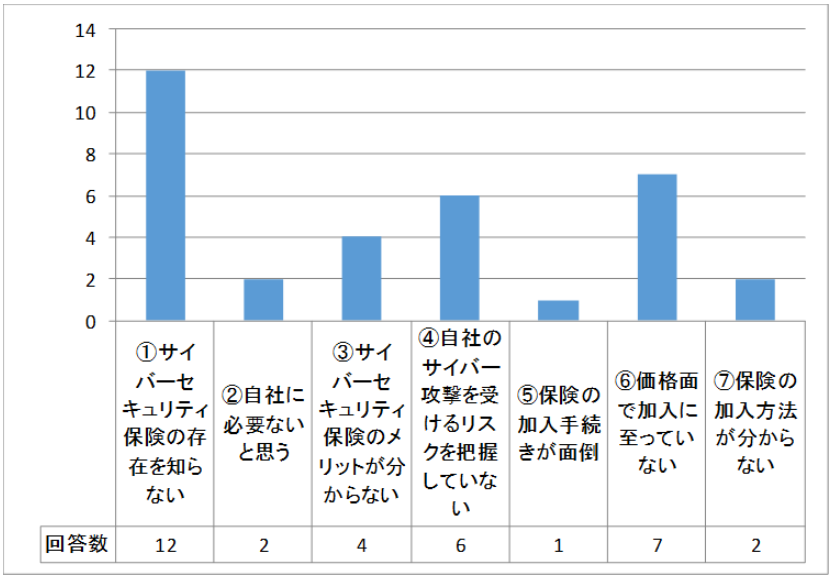


図 83 サイバーセキュリティ保険に加入していない理由（n=29）

b．サイバーセキュリティ保険の補償範囲の希望

表 107 サイバーセキュリティ保険で希望する補償範囲

選択肢	回答数
損害賠償	4 社
費用損害	3 社
どちらも	22 社

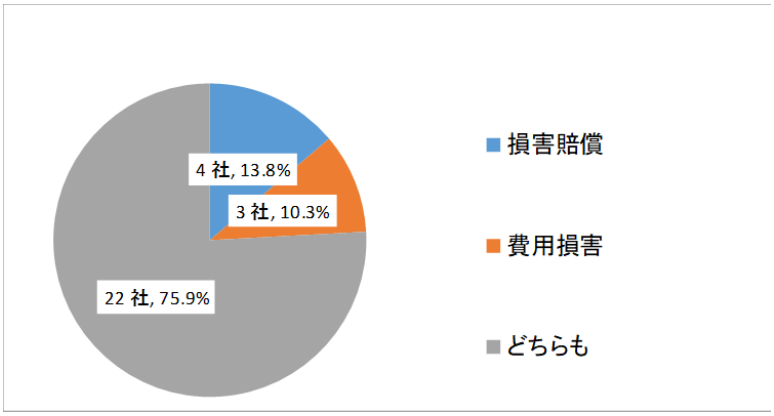


図 84 サイバーセキュリティ保険で希望する補償範囲（n=29）

ｃ．サイバーセキュリティ保険の補償を希望事象

表 108 サイバーセキュリティ保険の補償を希望事象

選択肢	回答数
①他人の情報の漏えいまたはそのおそれ。ただし、ネットワーク上に存在する電子情報の漏えいに起因するものに限る（本実証事業と同条件）	19 社
②クレジットカードの電子情報漏えい	7 社
③個人情報の電子情報漏えい	17 社
④マルウェアの調査・対応（外部への調査、ランサムウェアによるファイル暗号化対応費用など）	14 社
⑤紙や外部記憶媒体などの「物」に記録された他人の情報の紛失・盗難	7 社

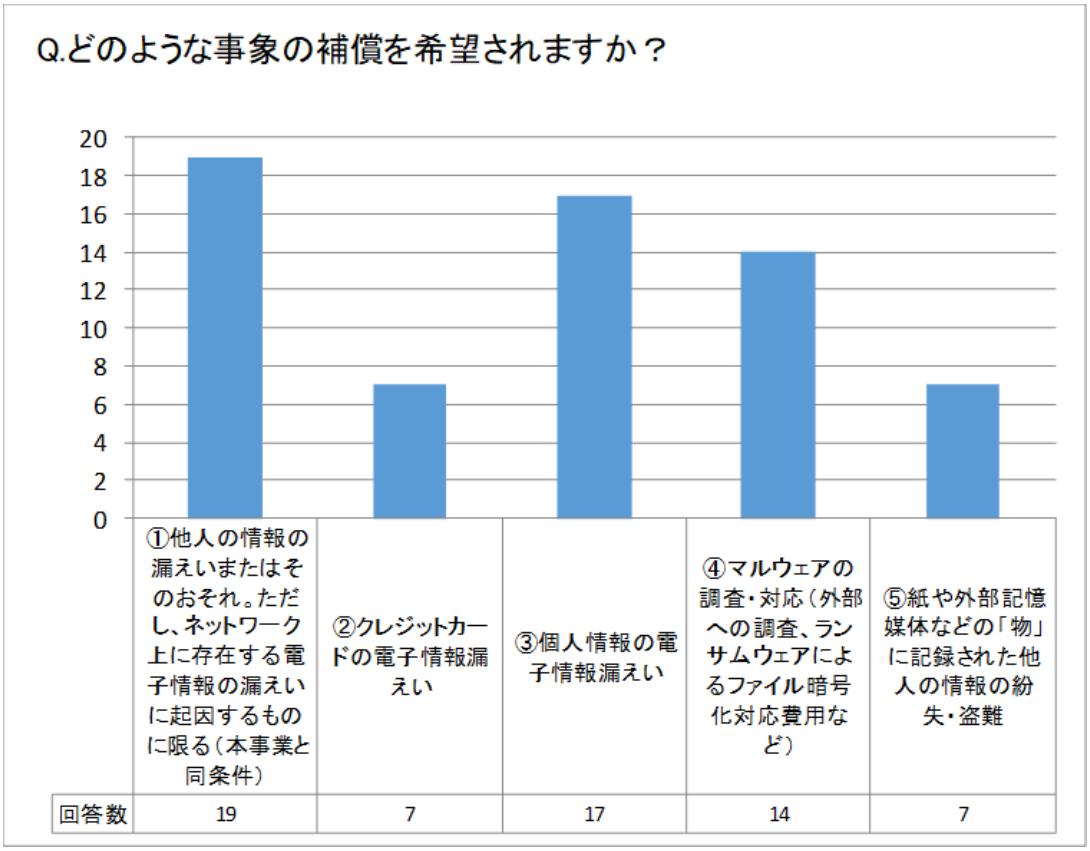


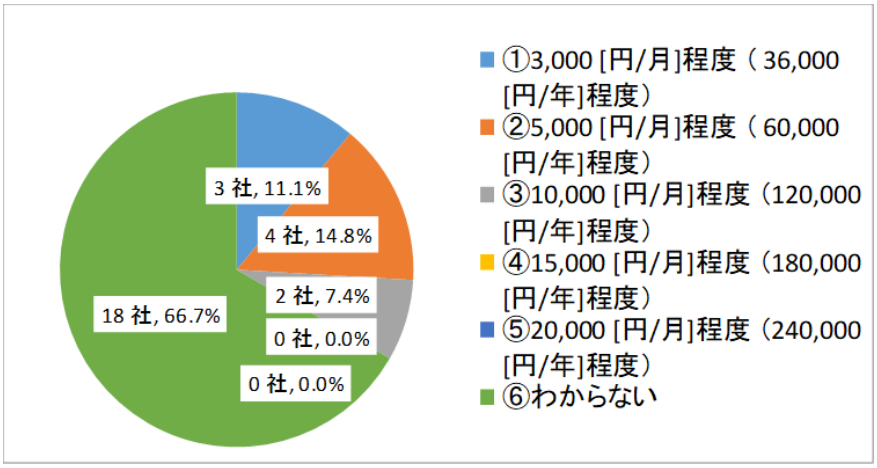
図 85 サイバーセキュリティ保険の補償を希望事象（n=29）

d．サイバーセキュリティ保険にかけても良い価格

表 109 サイバーセキュリティ保険にかけても良い価格

選択肢	回答数
① 3,000 [円/月]程度 （ 36,000 [円/年]程度）	3 社
② 5,000 [円/月]程度 （ 60,000 [円/年]程度）	4 社
③ 10,000 [円/月]程度 （120,000 [円/年]程度）	2 社
④ 15,000 [円/月]程度 （180,000 [円/年]程度）	0 社
⑤ 20,000 [円/月]程度 （240,000 [円/年]程度）	0 社
⑥ わからない	18 社

図 86 サイバーセキュリティ保険にかけても良い価格（n=29）



5.1.2 保険設計

保険設計をした結果、次の結論となった。

商品付帯型のサイバー保険としない。 企業毎の規模やニーズに合わせて保険内容を変更できる、個別見積・個別契約の損害保険会社の商品を提供する。

お助け隊の地域実証のサイバー保険は、セキュリティログ監視サービスの付帯保険とした。サイバー保険の内容は次の通り。

表 110 お助け隊 サイバー保険内容

項目	内容
支払限度額	200 万円（賠償損害・費用損害共有）
対象となる損害	（1）賠償損害 ①損害賠償金 ②争訟費用 ③権利保全行使費用 ④訴訟対応費用 （2）費用損害 事故原因・被害範囲調査費用
対象事由 ・補償内容	対象製品の監視対象ネットワークの所有、使用または管理に起因する次の事由に起因する損害に限る。 ・他人の情報の漏えいまたはそのおそれ。ただし、ネットワーク上に存在する電子情報の漏えいに起因するものに限る。 ・クレジットカード情報の漏えいに起因する損害（例：カード会社からの不正利用、再発行費用等にかかる求償等）は補償対象外とする。 ・費用損害については「事故原因・被害範囲調査費用」のみ補償する。

実証終了後も付帯保険とすることを前提にサイバー保険内容を設計した。まず、一般的なサイバー保険の価格は「企業の売上規模」「扱っている情報等」「セキュリティ対策実施状況」で変動する。

商品付帯型のサイバー保険の設計をしたところ、次の課題があることが分かった。

表 111 商品付帯型保険の課題

項目	課題
補償内容	顧客が保有する情報資産や業務内容にかかわらず、一律固定
補償金額	顧客が保有する情報資産や業務内容にかかわらず、一律固定
保険価格	リスクの発生確率と情報資産の価値（損害の大きさ）が企業により異なることから、個別見積と比較すると相対的に価格が高くなる企業が発生する可能性がある。
販売	商品付帯の場合、選択式にできない。商品と必ずセットになる。

また、「5.2 中小企業向けセキュリティビジネス化に向けた課題・検討」において、価格をできるかぎり抑える方針となった。この場合、選択式にできず必ずセットになる保険商品の販売制約があるため、商品付帯型にすると基本価格が高くなる。価格を下げるためには、補償内容を限定しなければならない。

お助け隊で提供したサイバー保険は、実証事業費用の枠内に収めるため、補償内容を限定し、価格を下げた。お助け隊はサイバー保険の体験が目的であるため、これで問題なかったと考える。しかし、発生確率が低く、損害が大きいリスクに対するセキュリティ対策がリスク移転であるため、大きな損害を補償できなければ意味がない。

5.1.3 普及啓発

次の内容の電子メールを実証参加企業に 2021 年 1 月 5 日に送信し、情報提供を行った。

サイバー保険に関する情報をご提供します。

一般社団法人 日本損害保険協会様がサイバー保険について
わかりやすい解説資料を公開しています。次の URL を参照ください。

「サイバー保険」ホームページ
【URL】https://www.sonpo.or.jp/cyber-hoken/

※以下は同サイトのコンテンツ

サイバー保険とは
【URL】https://www.sonpo.or.jp/cyber-hoken/about/

お役立ち情報（動画・チラシ・リンク集）
【URL】https://www.sonpo.or.jp/cyber-hoken/useful/

青森・秋田・山形・宮城地域のサイバーセキュリティお助け隊事業で、
商品付帯型のサイバーセキュリティ保険を提供させていただいている
あいおいニッセイ同和損保の「サイバーセキュリティ保険」の紹介サイトでは
具体的な保険料例などを公開しています。
なお、この保険は、サイバーセキュリティお助け隊事業で提供している保険とは
異なる保険の紹介であることにご留意ください。

あいおいニッセイ同和損保「サイバーセキュリティ保険」紹介サイト
【URL】https://www.ad-cybersecurity.com/

また、成果報告会の実証終了後のサービス紹介の中で、サイバー保険の内容を説明した。

5.1.4 ビジネス化に向けた検討結果

セキュリティ対策が不十分であると認識している企業のサイバー保険に対するニーズは大きい。また、実態把握の結果、サイバー攻撃の被害を受けた経験がある企業は限定的である。発生確率が低いリスクに備えるためには、サイバー保険が有効なセキュリティ対策である。

業種により大きく異なるが、セキュリティ事故の損害額は近年大きくなっている。補償範囲を限定した場合、自動車の自賠責保険のように、補償が足りず別の保険が必要になることが懸念される。中小企業の状況に見合った、適切なリスク移転のセキュリティ対策となる保険サービスにしなければならない。

商品付帯型にすることで、保険の販売の資格がなくても販売できること、顧客が強く意識しなくても保険サービスを受けられることの利点はあるが、中小企業の立場で考えると、企業ごとの規模やニーズに合わせて保険内容を変更できる、個別見積・個別契約のサイバー保険を提供することが最善であるとの結論に達した。

お助け隊の商品付帯型サイバー保険サービスを提供した「あいおいニッセイ同和損保」の保険商品「サイバーセキュリティ特約セット包括職業賠償責任保険」の概要を次に記す。

表 112 サイバーセキュリティ特約セット包括職業賠償責任保険

項目	内容
費用損害	
対象となる事由	【ベーシック】 ①他人の情報の漏えいまたはそのおそれ ②情報システムの所有・使用もしくは管理または電子情報の提供に起因する事故による他人の業務の阻害、他人の電子情報の喪失等 【ワイド】 ③サイバー攻撃に起因する対人・対物事故 ④サイバー攻撃に起因する②または③のおそれ サイバー攻撃調査費用
対象となる損害	【ベーシック】 事故対応費用、法律相談費用、事故原因・被害範囲調査費用、コンサルティング費用、社告宣伝活動費用、見舞金・見舞品購入費用 【ワイド】 クレジット情報モニタリング費用、被害拡大防止費用、公的調査対応費用、再発防止費用、情報システム等復旧費用、サイバー攻撃調査費用
損害賠償	
対象となる事由	【ベーシック】 ①他人の情報の漏えいまたはそのおそれ ②情報システムの所有・使用もしくは管理または電子情報の提供に起因する事故による他人の業務の阻害、他人の電子情報の喪失等 【ワイド】 ③サイバー攻撃に起因する対人・対物事故 国外訴訟
対象となる損害	損害賠償金のほか、事故発生の際に適切な対応を行うための費用、訴訟・調停・和解・示談などの対応の費用を支払う。 ■法律上の損害賠償金:法律上の損害賠償責任に基づく賠償金 ■争訟費用:訴訟にかかった費用等 ■権利保全行使費用:権利の保全や行使に必要な手続きをするためにかかった費用等 ■訴訟対応費用:書類の作成など、訴訟に関する諸費用等

5.2 中小企業向けセキュリティビジネス化に向けた課題・検討

次のプロセスで「中小企業向けセキュリティビジネス化」を検討した。事前マーケティングのアンケートに期限内に回答しない企業があり、計画よりも長い期間となった。「実証終了後のサービス内容検討」の後に、「支援経験後マーケティング」と「意見交換」を行う予定だったが、最後の実証参加企業の決定が 11 月末までずれ込んだため「支援経験後マーケティング」の実施が大幅に遅れた。そのため、ヒアリングに合わせて「意見交換」を実施し、サービス内容を見直した。このプロセスを並行して実施したことから、「意見交換」と「サービス内容見直し」の結果を含めて「実証終了後のサービス内容検討」に記載した。なお、ビジネスモデルの検討結果とサービス内容の検討結果は項を分けて記載した。

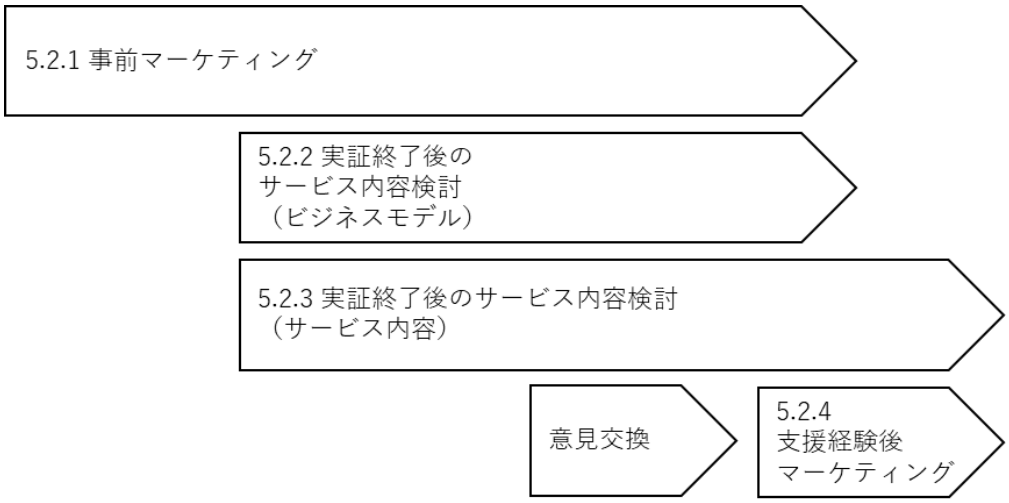


図 87 中小企業向けセキュリティビジネス化を検討するプロセス

また、下図に示すとおり、実証の結果得られた情報を元に検討した考察結果を考慮して実証終了後のサービス内容を検討した。

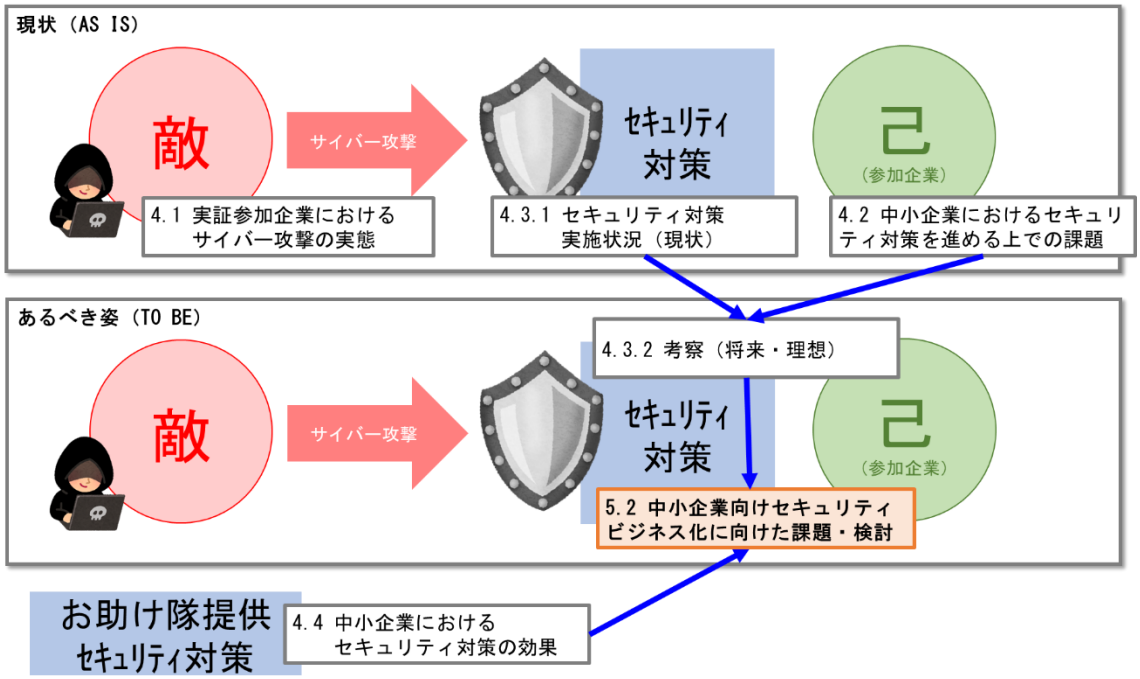


図 88 実証終了後サービス内容検討の考慮事項

実証結果の考察の要旨を下表に記す。

表 113 考察の要旨

タイトル	考察の要旨
4.1 実証参加企業におけるサイバー攻撃の実態	・サイバー攻撃を受けているが被害を受けた企業は限定的 ・リスクの発生確率が小さい（現時点）
4.2 中小企業におけるセキュリティ対策を進める上での課題	・「お金」「人」「情報」がないこと ・「人」の課題解決が重要
4.3.1 セキュリティ対策実施状況（現状）	・防御対策が不十分な企業が多い ・検知・対応が不十分
4.3.2 考察（中小企業において必要なセキュリティ対策　将来・理想）	・体制整備（セキュリティの責任者、担当者を任命） ・不足している防御対策を実施
4.4 中小企業におけるセキュリティ対策の効果	・実証参加企業にとって、お助け隊参加による効果があった ・セキュリティ対策に取り組むきっかけになった

5.2.1 事前マーケティング（ニーズ調査）

アンケート結果およびヒアリング結果を分析し、中小企業は次の状況に置かれているとの仮説を立てた。

表 114 中小企業が置かれている状況の仮説

No	置かれている状況	根拠となるアンケート・ヒアリング結果
1	UTM を導入していない企業が多くある。	・お助け隊に期待すること ・セキュリティ対策実施状況
2	セキュリティ対策にかけられる費用が少ない	・ほとんどの企業で年間投資額が 100 万円以下 ・独自のアンケートで、最も多かったセキュリティ対策にかけられる費用の回答が 20,000 [円/月] 一番安い選択肢だったため、安いほど良いと考えている可能性がある
3	UTM を設置しても自社で運用できない	・情報システムの運用をアウトソーシングしている企業が多い ・セキュリティ担当者が明確に決まっていない企業が半数 ・担当者のスキルが足りないことを課題と認識している企業が多い
4	何からセキュリティ対策を実施すれば良いかわからない	ヒアリングの回答

中小企業が置かれている状況の仮説およびアンケートとヒアリングの結果から、中小企業には次のニーズがあるとの仮説を立てた。

表 115 中小企業のニーズの仮説

No	課題分類	ニーズ・要望	理由
1	お金	できるだけ安価が良い	・セキュリティ対策に投資できるお金が少ない ・価格の妥当性の評価が困難（高価格は受け入れられない）
2	人	セキュリティに関して相談できるサービスが欲しい	・人がいない、知識がないことの解決策になる ・ヒアリングで希望があった
3	人	UTM 設置支援	・知識のある人がいない
4	人	UTM の維持管理を依頼したい	・知識のある人がいない
5	情報	セキュリティ情報提供	・情報を持っていない ・情報を収集する人がいない
6	対策	UTM を導入したい	・お助け隊に期待することで UTM が一番多かった
7	対策	状況を見える化したい	・ヒアリングの結果、見える化できたことが成果との回答あり
8	対策	Web セキュリティ診断、制御システム簡易リスクアセスメントのニーズは限定的	・サービス希望アンケートで希望する企業が少なかった

5.2.2 実証終了後のサービス内容検討（ビジネスモデル）

中小企業向けセキュリティサービスのビジネスモデルを検討した結果を次に記す。

実証の結果の考察を踏まえ次のビジネスモデルを仮定した。なお、将来構想を含むモデルである。

表 116 中小企業向けセキュリティサービスのビジネスモデル

項目	内容
顧客	・セキュリティ対策が進んでいない東北地域の中小企業
提供する価値	・セキュリティ対策実施に関する「人」「情報」の不足解消 ・不十分なセキュリティ対策の強化 ・結果して、サイバー攻撃による被害低減
提供方法	・セキュリティ責任者・担当者の支援 ・技術的セキュリティ対策サービス提供
利益を確保する方法	・核となるサービスを年間契約とし、継続的に料金を徴収 ・一定数以上の顧客を確保

これは中小企業がすべてを外部に頼らないビジネスモデルである。組織的対策は内部の人しかできない（ルール策定・周知・指導等）。伴走支援するが、中小企業にしっかり走ってもらうことを目指している。セキュリティ対策は変化するため、見直していかなければならない。中小企業のセキュリティ体制が土台となる。

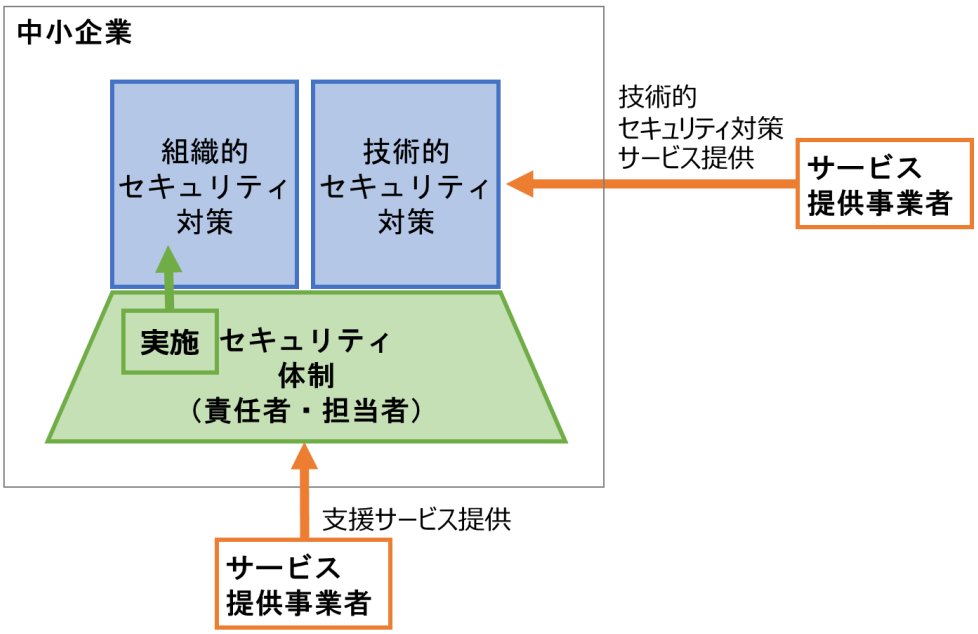


図 89 ビジネスモデル

このビジネスモデルが成立するために必要な条件とそのように考えた理由を下表に記す。

表 117 ビジネスモデルが成立するために必要な要件

No	ビジネスモデルが成立するために必要な条件	理由
1	中小企業の経営者にセキュリティの意識を高く持ってもらうこと	セキュリティ対策の効果は論理的に説明しきれない部分があり、主観的な判断が必要になる。担当者からのボトムアップでセキュリティ対策を推進することは簡単ではない。
2	中小企業においてセキュリティ対策を推進する体制が整備されていること	セキュリティレベル向上には、中小企業の責任者と担当者の行動が必須である。
3	中小企業の体力（売上）に見合った価格で提供できること	アンケートやヒアリング等から、セキュリティ対策の投資が難しいことが課題である。
4	単体のサービスでなく、包括的なサービスとすることで、全体の収入を増やすこと	少ない売り上げで、持続可能なサービスを提供することは困難である。なお、中小企業のセキュリティ投資は大きく増えないと想定した。
5	セキュリティ以外のサービスと組み合わせることで、全体の収入を増やすこと	

これらの要件を満たすために必要なことを検討した。検討結果を下表に示す。

表 118 ビジネスモデルが成立する要件を実現する手法

No	要件を満たすために必要なこと	ビジネスモデルが成立するために必要な条件の該当要件番号
(1)	啓発活動	No1、No2
(2)	価格低減	No3
(3)	セキュリティサービスの拡充	No4
(4)	セキュリティ以外のサービスの組み合わせ	No5

(1) 啓発活動

国や IPA、民間企業で、セキュリティに関する普及啓発活動を行っている。情報システムのセキュリティを確保することは事業継続の一つの要素であることが多くの企業に浸透してきたと感じる。しかし、大企業は当たり前になったが、中小企業には十分に浸透していないと感じる。

「中小企業の経営者にセキュリティの意識を高く持ってもらうこと」を実現するためには、継続的に啓発活動を行う以外に方法がない。なお、個人情報保護法のように国の制度による強制力を伴った手法もあるが、ここでは検討から除外した。

まずは、経営者向けにセミナーなどを開催して、セキュリティ対策の必要性を認識してもらい、セキュリティ体制を構築してもらわねばならない。さらに、セキュリティ責任者と担当者向けのセミナーなどによる啓発活動が必要である。

民間企業だけでは、すべての中小企業へのアプローチは困難である。国・地方公共団体・各種地場団体などと連携して啓発活動を行うことが望ましい。アンケートの結果、半数程度の企業が公的機関の「セミナーや講習会等の教育・啓発」に期待している。現在も多くのセミナーなどが国の予算等で実施されている。今後も継続して実施することを希望する。

表 119 公的機関（国、地方自治体）に期待すること

選択肢	回答数
補助金・助成金	15 社
セミナーや講習会等の教育・啓発	10 社
セキュリティに関する情報提供	14 社

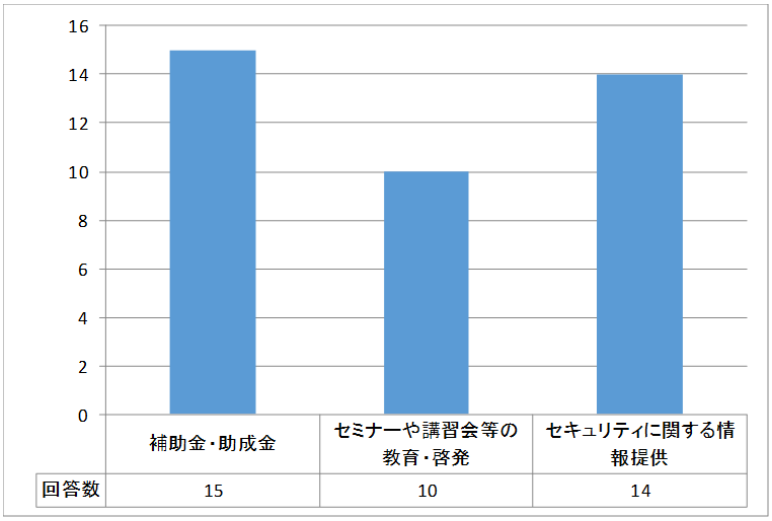


図 90 公的機関（国、地方自治体）に期待すること（n=21）

また、地域コミュニティを作り、中小企業間で情報交換することも有効である。こちらも国が実現に向けた検討を行っている。なお、実現には、核となる企業または人材の確保が課題であると考える。

ヒアリングを実施した企業の経営層の意識は高く、やらなければならないと感じている。情報がないだけである。中小企業に届くような啓発活動の仕組みが必要であると感じる。

(2) 価格低減

価格を低減するためには、次の 2 つの手段がある。

・共通の仕様のサービスを多くの顧客に提供する（コストの案分）
・サービス範囲や内容を限定する、または分ける

UTM の「監視・通知」サービスは、共通化・自動化が可能なため、規模による価格低減効果が得られやすい。

しかし、「インシデント対応」は状況に応じて、人が動かなければならない。SOC の対応を自動化する仕組み（SOAR）が出てきているが、実現には高いコストがかかる。ただ、今後 SOC に限らず、自動化などによって人的コストを削減することはサービス提供事業者にとって必須要件になると考える。

また、現地への「駆け付け対応」は人的コストが高いサービスである。特に、東北のように広い地域で安価にサービスを提供することは簡単ではない。安価にするためには、遠隔でインシデント対応を完結させることが望ましい。遠隔でインシデント対応を行うためには、EDR 機能を持つ製品などを利用することがひとつの選択肢である。UTM だけでは調査・対応ができない。ただし、すべてのパソコンに EDR を入れると価格が高くなる。既存のウイルス対策ソフトとの入れ替えなどを含めた

統合的なセキュリティ対策の提案が必要である。
できるだけ遠隔で対応するサービスを提供することにより、中小企業が支払わなければならない費用を低減することを目指す。

上記のとおり、セキュリティ対策サービスは、「人」が動かなければならない部分が多いため、規模の価格低減効果を得られにくいサービスが含まれる。だが、すぐに自動化や新規サービス提供は難しい。実証終了後に提供するサービスは、価格を低減するために、基本とオプションに分け、基本部分をできるだけ安価にし、ニーズに合わせてサービスを追加できるようなメニュー体系とする方針とした。

(3) セキュリティサービスの拡充

セキュリティの製品やサービスの有効性・費用対効果の評価は難しい。攻撃内容・方法が多様であり、変化するためである。これは中小企業だけでなく、セキュリティ専門企業でも同じである。そのため、品質ではなくブランドで選ばれることが多い。しかし、実際には同じ価格でも品質の差が大きい。
この課題の解決策として、品質の高い様々なセキュリティ対策を実現するサービスをパッケージ化して提供するビジネスモデルが考えられる。これは、資本関係のあるグループ企業に統一的なセキュリティ対策を提供するモデルと同じである。ヒアリングの結果、このようなサービス提供形態を希望する企業があった。

お助け隊での防御対策は「UTM」による不正通信の防御だった。アンケートの結果、UTM を設置していない企業が多い。UTM 配下の機器を防御でき、費用対効果が高いため、UTM を基本サービスとする方針とした。
その一方、アンケートなどで把握できたセキュリティ対策の状況から一般的に実施している企業が多い「USB 接続機器の利用制限」や「ハードディスク暗号化」などの対策を実施していない企業が多い。上記で示したようにパッケージ化して提供することが考えられる。

また、UTM だけではインシデント発生時の調査が難しい課題がある。「駆け付け対応」に変わるサービス提供のための EDR も合わせて提供することが望ましいサービスである。

さらに、今後、クラウドの利用が主になると、セキュリティ対策もクラウドから提供する形態が多くなると思われる。この形態であれば、より中小企業に対してサービスを提供しやすくなる。

このように、複数のセキュリティ対策をパッケージとして提供できれば、中小企業のセキュリティ対策向上に寄与できると考えられる。ただし、価格を安くできることが必要である。

(4) セキュリティ以外のサービスの組み合わせ

実証の結果、リスクの発生確率が低い状態であることがわかった。サイバー攻撃の増加・巧妙化により、リスク発生確率が増加すると思われるが、発生確率が低ければ、リスク低減のためのセキュリティ対策に投資するよりも、サイバー保険を利用することが適切である。この場合、リスク低減のためのセキュリティ対策の費用は大きく増えないと思われる。セキュリティ以外の情報システムの開発・運用等と組み合わせることで、トータルの提供コストを下げながら、品質の高いサービスを提供することができる可能性がある。

また、インシデント対応は、情報システムの状態を把握している必要がある。情報システムの運用とセキュリティ対策サービスを組み合わせて提供することは有効である。

運用を地場のベンダーにアウトソーシングしている企業がある。運用の役務をセキュリティベンダーが行うのではなく、地場ベンダーと連携することが望ましい。

なお、前述した地域コミュニティをこの枠組みで行うことも有効であると考える。

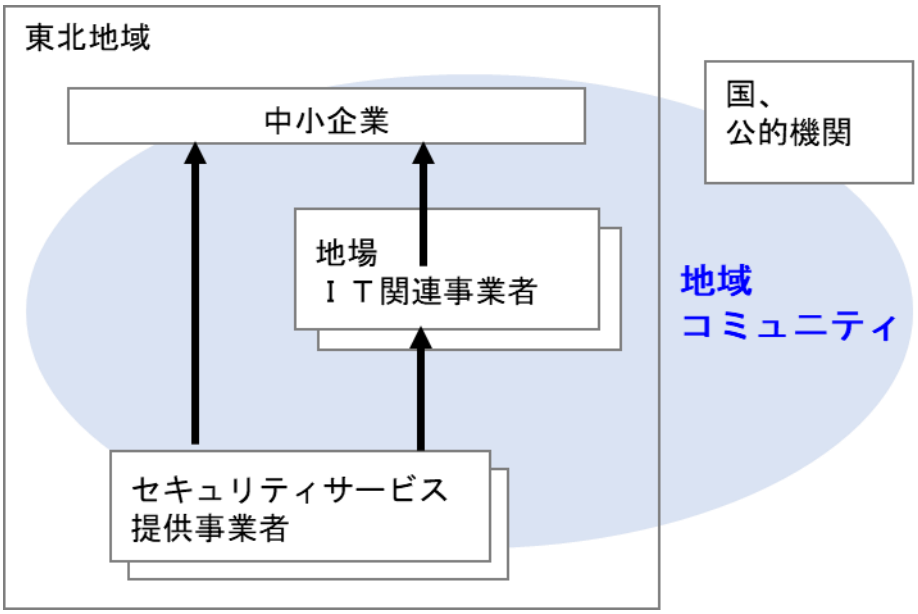


図 91 地場 IT 関連事業者との連携イメージ

5.2.3 実証終了後のサービス内容検討（サービス内容）

ビジネスモデルの検討結果を踏まえ、具体的なサービス内容を検討した結果を次に記す。

(1) セキュリティログ監視とインシデント対応支援

お助け隊の「セキュリティログ監視とインシデント対応支援」には、次のサービスが含まれていた。

ａ. UTM 設置支援
ｂ. UTM リモートメンテナンス
ｃ．相談受付および対応
ｄ．セキュリティログ監視およびインシデント対応支援（リモート）
ｅ．駆け付け対応

それぞれのサービスについて、実証終了後のサービスを検討した結果を次に示す。

ａ. UTM 設置支援

人がいないこと、人がいても技術がないこと、ネットワーク構成を把握できていないなど資産を管理できていないことから、設置支援のニーズが大きいと考えられるため、サービスメニューに入れる。（人の課題解決）

設置支援にかかる作業量は、企業により大きく異なる。標準パターンを 2 つ程度に絞ることで、費用を低減できる。また、監視以外のセキュリティ機能の設定をする場合のヒアリングや設定は、オプションとする。

ｂ. UTM リモートメンテナンス

「ａ. UTM 設置支援」と同様に、中小企業の人の課題があるため、自社で運用できる企業は限定的である。したがって、UTM をリモートでメンテナンスするサービスをオプションサービスとして提供する。

JPCERT/CC から出された「複数の SSL VPN 製品の脆弱性に関する注意喚起」のように、脆弱性を放置すると大きな影響が発生する可能性があるため、適宜バージョンアップが必要である。これを中小企業が適切に実施することは難しいと考えられるため、バージョンアップ作業はオプションサービスとせずに、基本サービスに含める。

なお、バージョンアップ以外の、顧客の個別要望に基づくセキュリティ機能の設定変更作業（VPN 接続、URL コンテンツフィルタリングなど）はオプションサービスの範囲とする。

ｃ．相談受付および対応

実証期間中の個別の相談は少なかった。サイバー攻撃の被害がなかったこと、本サービスの周知が十分でなかったことが要因だと思われる。しかし、ヒアリングで相談対応を望まれる企業があった。アンケートの結果から「要員の知識不足」を課題にあげた企業が多いことから、相談対応のニーズがあると思われるので、メニューに入れることとした。また、ビジネスモデルの仮説を実現するために

も重要なサービスとなる。

また、セキュリティ情報の提供を要望される企業があった。アンケートやヒアリング結果から能動的に情報収集ができていないことがうかがえる。中小企業のセキュリティ対策向上にはセキュリティ情報の提供が有効だと考えられる。セキュリティ情報提供もメニューに加えることとした。

ｄ．セキュリティログ監視およびインシデント対応支援（リモート）

UTM を設置していない企業にとっては不足しているセキュリティ対策を強化する有効な手段であることから、セキュリティログ監視を基本サービスとして位置付けることが良いとの結論に至った。

また、インシデント検知時のメール通知、防御できていないと思われる通信を検知した際の初動対応の提案、月次レポートも満足度が高かった要因と考えられるため、お助け隊と同様にサービスに含める。

ｅ．駆け付け対応

お助け隊期間中の駆け付け対応はなかったが、あれば何かあった時に支援してもらえるので安心できるとの意見があった。駆け付け対応のニーズはあると考えられる。しかし、次の理由により、基本サービスには含めずに、駆け付けを実施する際のスポット契約とすることとした。

・実証の結果から、駆け付けが必要になるインシデントの発生確率が低いと思われる。
・東北を対象地域とした場合、非常に広い範囲であるため、移動に伴う旅費交通費と工数が多くかかるため、費用が高くなる。
・基本サービスに含めると価格が高くなり、発生確率が低いものの対価として受け入れられないと思われる。

昨今の EDR 製品は、リモートで多くの対応ができる機能を備えている。今後はリモートで対応することを前提としたサービスを提供することが、顧客とサービサーの両社にとってメリットが大きいと考える。実証終了後すぐにこのようなサービスは提供できないが、サービスの企画検討を進める。

(2) 標的型攻撃メール対応訓練

標的型攻撃メール対応訓練は、今回の仕様のように共通の内容で複数の企業に疑似攻撃メールを送信することでサービス提供価格を下げることが可能である。

サービス内容について、満足との回答が多かったので、お助け隊のサービス提供と同様の内容で、オプションサービスとして提供することとした。

(3) 公開 Web サイト脆弱性診断

想定よりも申込数が少なかった。個別に Web サイトを構築している中小企業が少ないと思われる。また、本サービスは規模を増やすことで安価にできるサービスではない。仕様を変えることで価格を下げることができるが限定的である。

したがって、公開 Web サイト脆弱性診断は、個別見積・個別サービス提供することとした。

(4) 制御システム簡易リスクアセスメント

サービス希望のアンケートを取ったが申し込みがなかったため、個別に声がけし 2 社に対してサービス提供した。

最近は国から、特に重要インフラ事業者に対して制御システムのセキュリティを確保するよう周知したり、様々な分野でガイドラインが作られたりしているが、ここ数年の動きである。制御システムのセキュリティへの関心が高まってきているが、大企業でも取り組み始めたばかりであることが多い。中小企業の制御システムに対する取り組みはこれからであると思われる。

しかしながら、制御システム簡易リスクアセスメントを提供した企業のセキュリティ意識は非常に高く、これまで被害に遭っていないため実施していなかったが、今回のサービスをきっかけに、取り組むとのことだった。

このサービスも規模を増やすことで安価にできるサービスではないこと、対象が制御システムを保持する企業に限定されることから、個別見積・個別サービス提供することとした。

(5) 環境調査・エンドポイント監視・端末検知（WatchManBox_MR）

本実証実験では、ハイテックシステム社製の WatchManBox__MR をトライアル企業のセキュリティ状況把握（環境調査、エンドポイント監視、端末検知）の為に、導入したが、トライアル企業の中には、自動ネットワーク構成図作成や、無許可端末検知、3D グラフィック表示機能などの機能を利用する企業があった。お助け隊のサービス提供と同様の内容で、オプションサービスとして提供することとした。

5.2.4 支援経験後マーケティング

お助け隊のサービスを体験した後の満足度のアンケート結果を下図に記す。なお、サービスを受けていないと回答した企業を除いた比率を示した。

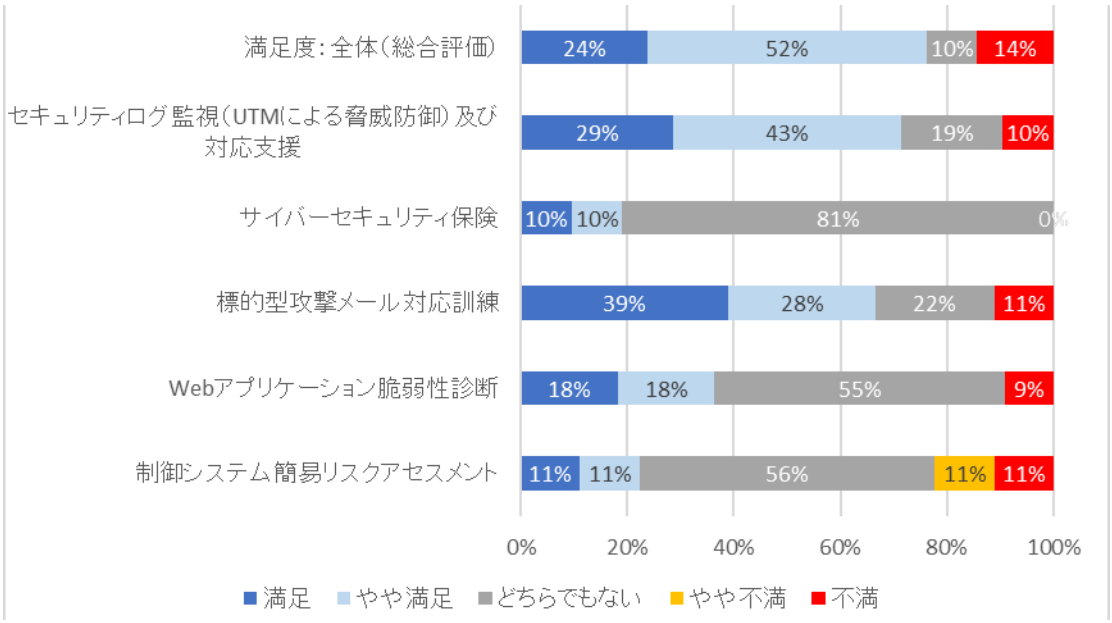


図 92 満足度アンケート結果

基本サービスとオプションサービスメニューに入れた「セキュリティログ監視および対応支援」「標的型攻撃メール対応訓練」は「満足」「やや満足」を足した割合が約 70%程度だった。満足度が高いサービスがメニューに入っているため、見直しの必要はないと判断した。

個別見積・個別サービス提供とした「サイバーセキュリティ保険」「Web アプリケーション脆弱性診断」「制御システム簡易リスクアセスメント」の満足度は高くなかった。「サイバーセキュリティ保険」はインシデントが発生していないので評価できなかったため「どちらでもない」の割合が高かったと考えられる。「Web アプリケーション脆弱性診断」「制御システム簡易リスクアセスメント」の原因は分析できていないが、サービスを実施した企業より多い企業が回答していることが影響している可能性がある。

成果報告会で実証終了後のサービスを紹介した。その後のアンケート結果を下図に示す。評価が分かれる結果となった。この結果についてはまだ分析できていない。このような結果になった原因を分析し、サービスの見直しにつなげる。

表 120 紹介したサービスの利用有無

選択肢	回答数
利用したい	5 社
価格が高い	3 社
サービス内容が求めるものと異なる	3 社
利用しない	7 社

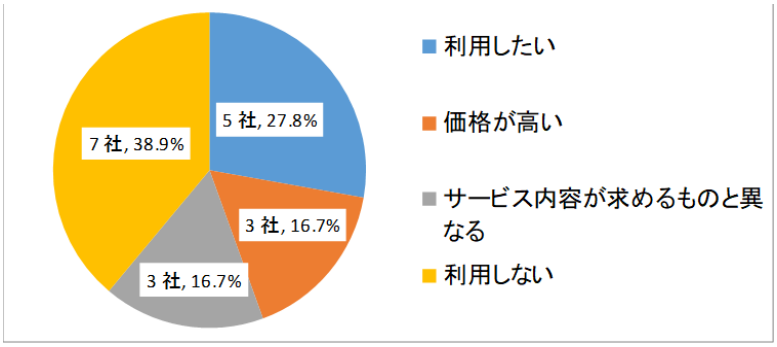


図 93 紹介したサービスの利用有無（n=18）

5.2.5 実証終了後に提供するサービス内容

下図の方針でメニューを組み立てた。お助け隊で提供したサービスの検討結果を踏まえて「基本」「オプション」「個別見積・個別契約」に分ける方針とした。

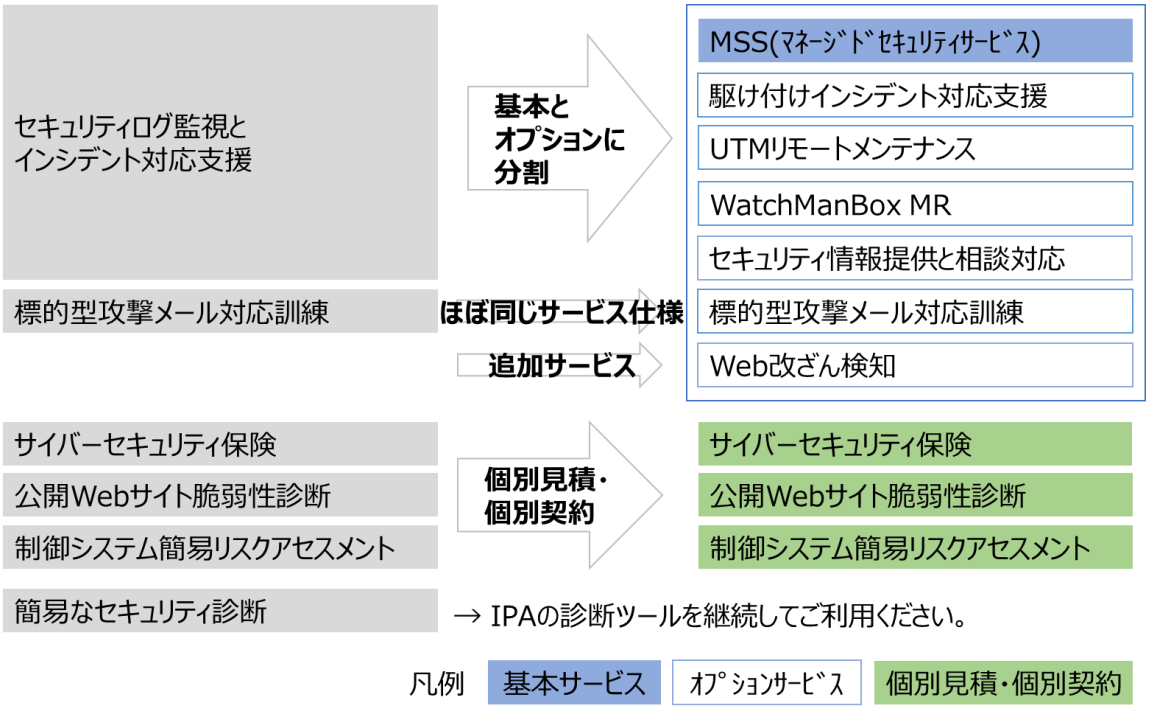


図 94 実証終了後のサービス内容

本実証事業の検討結果を踏まえて決定した「実証終了後に提供するサービスメニュー」を下表に示す。

表 121 実証終了後に提供するサービス内容

区分	サービス		契約期間	備考
基本サービス	MSS デバイス数 [1～ 40]	UTM 機器本体	導入時	実証参加企業は無償 買い取り又はリース 保守費用を含む
		UTM 設置支援		
		セキュリティ監視	年間	UTM 保守費用を含む
	MSS デバイス数 [41～ 100]	UTM 機器本体	導入時	実証参加企業は無償 買い取り又はリース 保守費用を含む
		UTM 設置支援		
		セキュリティ監視	年間	UTM 保守費用を含む
オプションサービス	UTM 初期設定カスタマイズ		導入時	
	UTM リモートメンテナンス		スポット	
	駆け付けインシデント対応支援		スポット	
	セキュリティ情報提供		年間	
	セキュリティ対策サポート		スポット	
	標的型攻撃メール対応訓練		スポット	5 月に実施
	Web 改ざん検知	初期設定	導入時	
		監視	年間	価格は監視対象 URL 数による

以上