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：熊本県）

# 成果報告書

請負事業者：西日本電信電話株式会社

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

# 目次


**1. はじめに ..... 1**

1.1. プロジェクト概要および目的 ..... 1

1.2. サマリー ..... 1

1.2.1. 実証事業実施期間 ..... 1

1.2.2. 実証参加企業数 ..... 1

**2. 実証事業概要 ..... 2**

2.1. 実証事業の概要 ..... 2

2.2. スケジュール ..... 3

2.3. 実証地域の選定 ..... 3

2.4. 実証参加企業 ..... 3

2.5. 実施内容（詳細） ..... 5

**3. 実施結果 ..... 10**

3.1. 実証事業説明会の開催 ..... 10

3.2. アンケート内容 ..... 12

3.3. 中小企業の ICT 実態アンケート調査結果 ..... 15

3.4. 実証参加企業のセキュリティ対策事前アンケート調査結果 ..... 23

3.5. 標的型攻撃メール訓練およびインシデント対応アンケート結果 ..... 29

3.6. UTM およびエンドポイントによる対策結果 ..... 34

3.7. 実証参加企業への実証事業終了時アンケート結果 ..... 39

3.8. サイバーセキュリティに関する相談の受付および対応結果 ..... 42

3.9. 実証事業報告会実証事業報告会 ..... 43

**4. 分析・考察 ..... 45**

4.1. 実証参加企業におけるサイバー攻撃の実態 ..... 45

4.1.1. セキュリティ対策機器（UTM）によるサイバー攻撃防御の状況 ..... 45

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 ..... 45

4.2.1. セキュリティ対策実施に向けた外部からのアプローチの増強 ..... 45

4.3. 中小企業において必要なセキュリティ対策 ..... 46

4.3.1. 標的型攻撃メール訓練による社員のセキュリティ意識の実態 ..... 46

4.4. 中小企業におけるセキュリティ対策の効果 ..... 46

4.4.1. 実証事業期間中のサイバーセキュリティ脅威が企業に及ぼす影響 ..... 46

**5. 実証を踏まえたビジネス化に向けた検討 ..... 48**

5.1. サイバー保険の活用.....48
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.....49

# 1. はじめに

本報告書は、西日本電信電話株式会社（以下「NTT 西日本」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。

熊本県内の中小企業 105 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。

- セキュリティ対策機器（UTM）の設置
- エンドポイントセキュリティの設置
- アンケート調査
- 標的型攻撃メール訓練

## 1.1. プロジェクト概要および目的

地域密着のサイバーセキュリティ対策支援の体制を、大手 SIer と地元 IT 企業、地元団体の強みを組み合わせて効果的に構築し、地元中小企業等へのサイバーセキュリティ対策の浸透を支援する。

## 1.2. サマリー

### 1.2.1. 実証事業実施期間

・実証事業実施期間　　2020 年 9 月 16 日（水）～2021 年 1 月 25 日（月）
・実証事業説明会（第 1 回）　2020 年 9 月 25 日（金）
・実証事業説明会（第 2 回）　2020 年 10 月 14 日（水）
・実証参加企業のサイバーセキュリティ対策利用可能期間
　　2020 年 9 月 16 日（水）～2020 年 12 月 31 日（木）
・実証事業報告会　　2021 年 1 月 15 日（金）

### 1.2.2. 実証参加企業数

熊本県内の中小企業など　105 社

## 2. 実証事業概要

### 2.1. 実証事業の概要

・サイバーセキュリティ相談窓口と情報共有網の構築

本実証事業を熊本県全域に周知させるため、（一社）熊本県サイバーセキュリティ推進協議会を主軸に「熊本サイバーセキュリティお助け隊実行委員会」を編成し、サイバーセキュリティ対策相談窓口を開設した。実証参加企業の募集においては、熊本商工会議所、肥後銀行、くまもと機械電子情報連携推進機構といった地域の有力企業や団体との連携体制を構築しており、説明会では、SECURITY ACTION および中小企業の情報セキュリティ対策ガイドラインの普及に向けた周知啓発活動、活用促進においては熊本県警察本部生活安全部サイバー犯罪対策課の協力も得て啓発効果の高い内容にした。また、サイバーセキュリティに関する損害補償においては東京海上日動火災保険（株）熊本支店との協力体制を構築し、熊本県内で起こるサイバーセキュリティ相談窓口、実証参加企業の拡大、啓発活動、インシデントに対する事後対応といった部分で包括的に活動可能な総合窓口を用意することで速やかな対応が可能な体制を整えた。

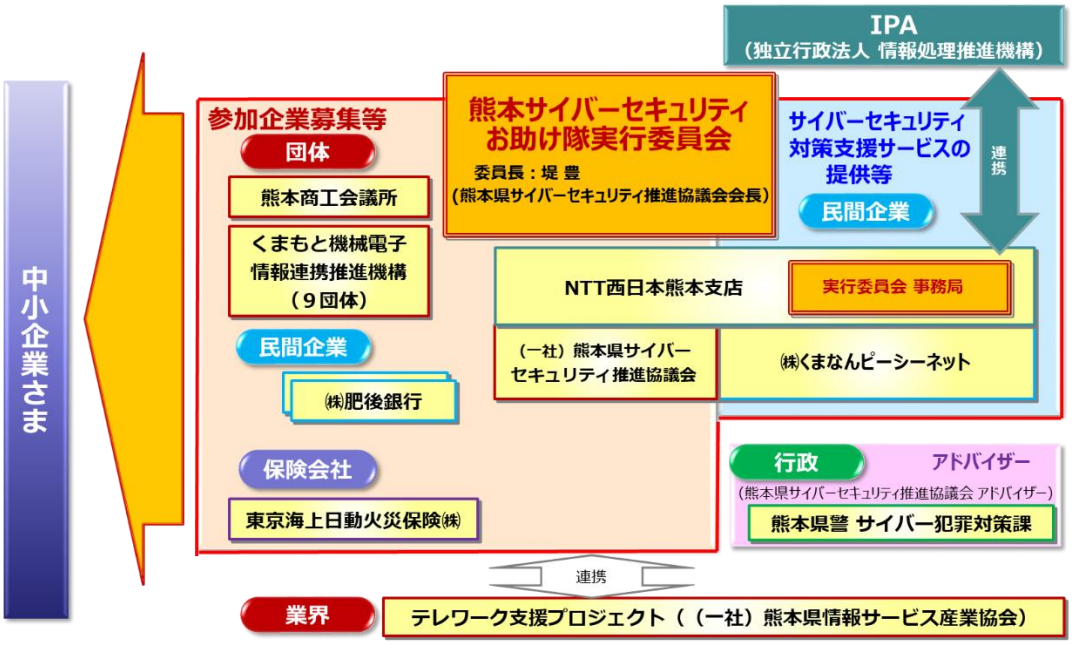



図 1：実証事業実施体制

・UTM を使った簡易 SOC サービスによる地域企業の監視サービス

大企業が設置するセキュリティ監視する拠点、いわゆる SOC（Security Operation Center）の機能を中小企業でも利用できるように、大手 SIer が共用型の SOC サービス提供を開始している。この大手 SIer サービスに地域 IT 事業者のサービスや地域団体の活動を組み合わせて地域に合った CSIRT まで活動を高めながら、SIer だけではリーチできなかったユーザー層にもサイバーセキュリティ対策の普及啓発を推進することを目指して実証事業を実施した。

実証事業を実施した「熊本お助け隊実行委員会」に参加する企業が提供するセキュリティサービスの中から、中小企業が導入しやすく、実証後も継続しやすいサービスを組み合わせて提供した。これにより中小企業のセキュリティ対策における人材不足、機器導入負担を軽減し、主たる目的であるサ

イバー攻撃の脅威に対し持続性のある効果を確認できた。

・セキュリティ対策実態調査、かけつけ体制、データ復旧サービス
「セキュリティ事故は起こるものである」ということを前提に熊本県内の中小企業に対し、UTM等で検知したインシデントに対応する、いわゆるインシデントレスポンスチームを結成した。これにあたり地域の中小企業のセキュリティ対策の現状を把握し、従業員のサイバーセキュリティ対策意識を含めた社内環境の脆弱性アンケート調査を併用してUTMで防ぐことができない潜在的なリスクの洗い出しも実施した。また、インシデント発生後にデータアクセスができなくなったパソコンに対するデータ復旧サービスも加えることで実証参加企業の事業継続性を高める内容とした。

## 2.2. スケジュール

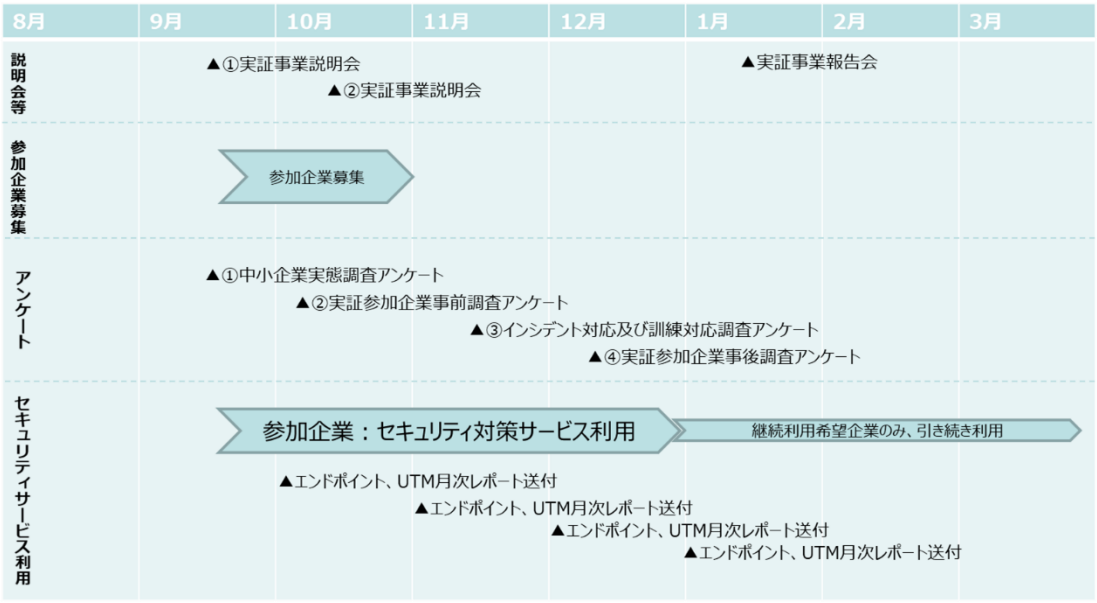



図 2：スケジュール

## 2.3. 実証地域の選定

熊本県内全域を対象に実証参加企業を募集した。

## 2.4. 実証参加企業

・実証事業説明会参加企業数
第 1 回説明会（9/25）　51 社
第 2 回説明会（10/14）　32 社
計 83 社

・実証参加企業数
105 社

なお、実証参加企業の法人種別、業種、資本金、従業員数の内訳については、図 3～6 のとおりである。

| n= | 会社 | 個人事業主 | 医療法人社会福祉法人 | 学校法人 | 商工会・都道府県商工会連合会及び商工会議所 | 中小企業団体 | 組合・連合会 | 財団法人、社団法人 | 特定非営利活動法人業 | その他 |
|---|---|---|---|---|---|---|---|---|---|---|
| 実証参加企業 (105) | 83.8% | 4.8% | 4.8% | 1.0% | 1.0% | - | 2.9% | - | 1.0% | 1.0% |

図 3：法人種別

| | 実証参加企業 (n=105) |
|---|---|
| 農業、林業 | 4.8% |
| 漁業 | - |
| 鉱業、採石業、砂利採取業 | 2.9% |
| 建設業 | 14.3% |
| 製造業 | 1.0% |
| 電気・ガス・熱供給・水道業 | - |
| 情報通信業 | 1.9% |
| 運輸業、郵便業 | 4.8% |
| 卸売業・小売業 | 14.3% |
| 金融業、保険業 | 1.9% |
| 不動産業、物品賃貸業 | 4.8% |
| 学術研究、専門・技術サービス業 | 6.7% |
| 宿泊業、飲食店 | 1.0% |
| 生活関連サービス業、娯楽業 | 6.7% |
| 教育学習支援業 | 1.0% |
| 医療、福祉 | 17.1% |
| 複合サービス事業 | 3.8% |
| サービス業（他に分類されないもの） | 6.7% |
| 公務（他に分類されるものを除く） | - |
| 分類不能の産業 | 6.7% |

図 4：業種

| n= | 1千万円以下 | ～3千万円以下 | ～5千万円以下 | ～1億円以下 | ～3億円以下 | ～10億円以下 | それ以上 |
|---|---|---|---|---|---|---|---|
| 実証参加企業 (105) | 80.0% | 8.6% | 6.7% | 3.8% | 1.0% | - | - |

図 5：資本金

| n= | ～5人 | ～10人 | ～20人 | ～50人 | ～100人 | ～200人 | ～300人 | ～400人 | ～500人 | ～600人 | ～700人 | ～800人 | ～900人 | ～1000人 | 1001人以上 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 実証参加企業 (105) | 25.7% | 15.2% | 20.0% | 21.9% | 9.5% | 5.7% | - | 1.0% | - | - | - | - | - | - | 1.0% |

図 6：従業員数

・実証事業報告会参加企業数
31 社

## 2.5. 実施内容（詳細）

・広報活動
実証事業 Web ページ開設、新聞広告、協議会等の媒体への記事提供を通じて実証事業の公報活動を実施した。

実証事業 Web ページ URL：https://otasuke.kumamoto-sec.jp/index.html

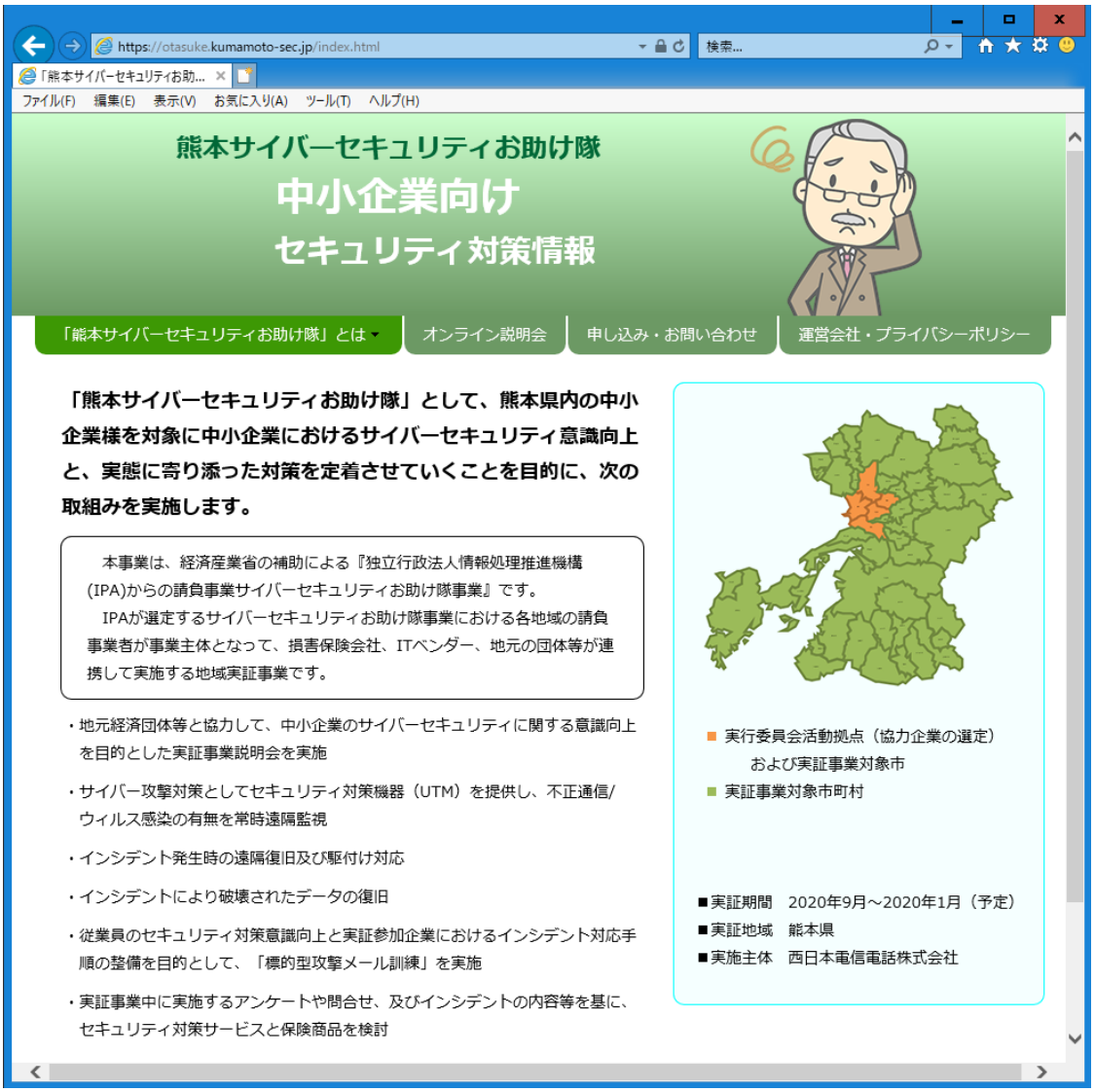



図 7：実証事業ホームページ（2021/1/15 参照）


図 8：熊本日日新聞（2020/9/18）朝刊広告

図 9：熊本商工会議所会報誌「商工ひのくに」P6-P7

図 10：熊本商工会議所会報誌「商工ひのくに」P8-P9

・実証参加企業に提供するセキュリティ機器とサービス

実証参加企業に対して、セキュリティ対策の導入支援と運用支援を実施した。導入支援では、アンケートおよび実証参加企業のセキュリティ対策機器設置状況などを確認し、セキュリティ対策を短期間で導入できるように支援した。また、運用支援では、導入した UTM とエンドポイントのアラート状況を常時監視し、有事の際に必要な支援（遠隔支援、駆付け支援、データ復旧支援）を行えるようにした。

UTM は「Unified Threat Management」の略で、ネットワークの出入り口に設置し、ウイルス、不正アクセス等のセキュリティの脅威からネットワークを複合的・網羅的に守るための機器であり、本実証事業では NTT 西日本の「セキュリティおまかせプラン　プライム」の UTM「Cloud Edge」を使用した。Cloud Edge は、クラウドサンドボックスと AI を採用しており、未知の脅威に対しても対応が可能である。添付ファイルがウイルスなのか判別できない場合、添付ファイルを必要に応じてクラウド上に隔離された「サンドボックス」で試し実行し、ふるまいを解析し、危険なものはブロックすることができる。「サンドボックス」とは添付ファイルがウイルスであったとしてもクラウド上に隔離された場所なので、万が一破壊活動が発生しても実運用しているネットワークに影響しない機能である。

業務用パソコンのエンドポイントセキュリティには、同じく NTT 西日本の「セキュリティおまかせプラン　プライム」のエンドポイントセキュリティツールを使用した。

・常時監視とサポート体制

実証参加企業に対して、常時監視とサポート体制を提供した。不正なサーバーとの通信や様々なウイルス攻撃は、オフィスサポートセンターより常に監視し、万が一の異常発生時には電話やメールで連絡し、問題解決をサポートする体制とした。また、ウイルス感染によるデータ暗号化など、やむを得ない事態における OS 初期化やバックアップデータのリストアが必要な際には、実証参加企業のオフィスを訪問して復旧支援する体制とした。さらに、必要な場合にはウイルス感染したハードディスクからのデータ復旧を支援内容に含めた。

遠隔サポート体制：

電話による受付・お知らせ　9:00～21:00（年末年始 12/29～1/3 除く）

メールによるお知らせ　24 時間 365 日

訪問サポート体制：

OS 初期化支援対応　9:00～21:00（年末年始 12/29～1/3 除く）

ハードディスクデータ復旧体制：

遠隔サポート実施後に、ハードディスクデータ復旧が必要な場合に

（株）くまなんピーシーネットに持込みで実施

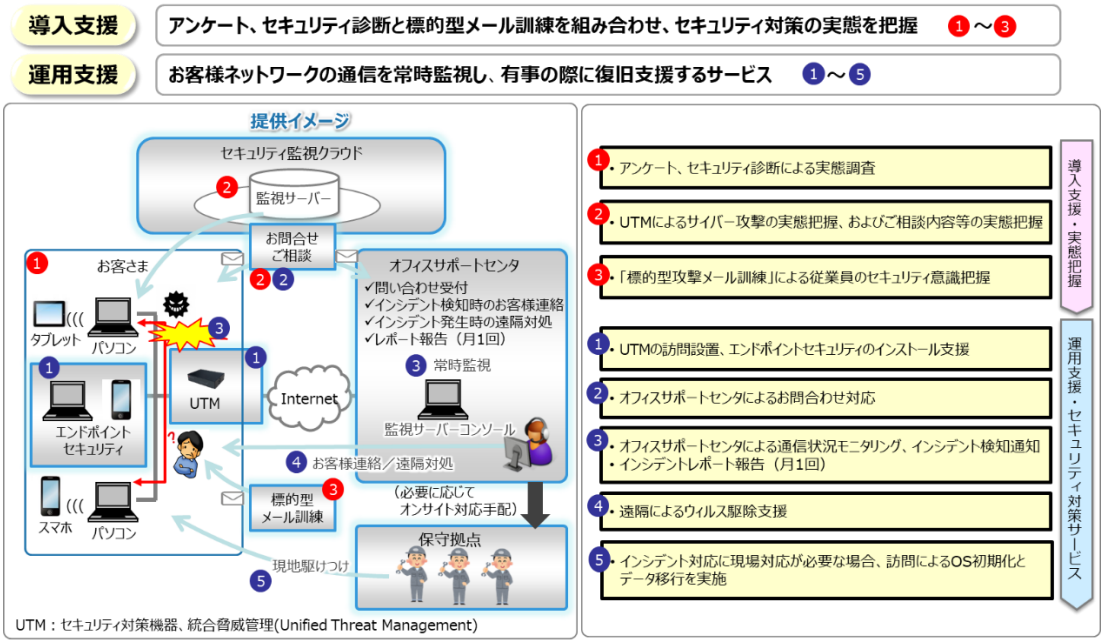



図 11：提供するセキュリティ対策支援

# 3. 実施結果

## 3.1. 実証事業説明会の開催

・第 1 回説明会

| | |
|---|---|
| 開催日時 | 2020 年 9 月 25 日（金） 13:30 ～ 16:00 |
| 場所、形態 | NTT 西日本 熊本支店<br>集合セミナーとオンラインセミナーの併用 |
| 参加者数 | 51 社（56 名） |
| アジェンダ | ① 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について（IPA）<br>② コロナ禍におけるサイバー犯罪の現状と対策（熊本県警本部 生活安全部 サイバー犯罪対策課）<br>③ サイバー攻撃におけるリスク（東京海上日動火災保険（株）熊本支店）<br>④ サイバーパトロール事例紹介（（一社）熊本県サイバーセキュリティ推進協議会）<br>⑤ 中小企業サイバーセキュリティ対策支援体制構築事業「熊本サイバーセキュリティお助け隊」の概要説明（NTT 西日本熊本支店） |

・第 2 回説明会

| | |
|---|---|
| 開催日時 | 2020 年 10 月 14 日（水） 14:30 ～ 17:00 |
| 場所、形態 | NTT 西日本 熊本支店<br>集合セミナーとオンラインセミナーの併用 |
| 参加者数 | 32 社（34 名） |
| アジェンダ | ① 中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について（経済産業省 商務情報政策局）<br>② コロナ禍におけるサイバー犯罪の現状と対策（熊本県警本部 生活安全部 サイバー犯罪対策課）<br>③ サイバー攻撃におけるリスク（東京海上日動火災保険（株）熊本支店）<br>④ サイバーパトロール事例紹介（（一社）熊本県サイバーセキュリティ推進協議会）<br>⑤ 中小企業サイバーセキュリティ対策支援体制構築事業「熊本サイバーセキュリティお助け隊」の概要説明（NTT 西日本熊本支店） |

実証事業説明会は、十分な新型コロナ対策を実施したうえで集合セミナーとオンラインセミナーを併用して実施した。

実証事業説明会および実証事業内容を個別説明した中小企業に対して実施したアンケートの結果、アンケートへの協力得た 147 社のうち 105 社の中小企業から実証事業参加意向を獲得することができた。アンケートの詳細は「3.2 アンケート内容」で記載する。


図 12：実証事業説明会の模様

### 3.2. アンケート内容

アンケートは主に次の 4 回に分けて実施した。

① ICT 実態アンケート調査
② 実証参加企業のセキュリティ対策事前アンケート調査
③ 標的型攻撃メール訓練およびインシデント対応アンケート調査
④ 実証参加企業への実証事業終了時アンケート調査

それぞれ、主に次の目的で実施した。

・ICT 実態調査アンケート
実証事業説明会への実証参加企業や実証事業内容を個別説明した中小企業を対象に実施し、中小企業の ICT 導入状況や実証事業への参加意向を確認する。また、全国の中小企業のサンプリングアンケートを併用し、熊本県内の中小企業の ICT 活用実態について特徴を確認する。

・実証参加企業事前調査アンケート
実証事業への参加を意思決定した中小企業を対象に実施し、実証事業への期待やセキュリティ対策状況を確認する。

・標的型攻撃メール訓練およびインシデント対応アンケート
標的型メール訓練の対応状況をベースとして、インシデントが発生した際の対応状況を確認する。

・実証参加企業への実証事業終了時アンケート
実証事業へ参加することでセキュリティ対策に対する考えなどに変化があったか、実証事業後のセキュリティ対策要望などを確認する。

＜第 1 回＞ ICT 実態アンケート調査
調査対象: 【1】実証事業説明会参加企業および実証事業の個別説明を受けた企業
【2】全国一般の中小企業において「経営者・役員」または「IT・情報システム部門」に所属する人 ※個人事業主を除く
調査方法: インターネット調査
調査時期: 【1】2020 年 9 月 27 日（日）～11 月 20 日（金）
【2】2020 年 11 月 25 日（水）～28 日（土）
有効回答数: 【1】147 サンプル
【2】225 サンプル
調査実施機関:株式会社マクロミル

＜第 2 回＞ 実証参加企業のセキュリティ対策事前アンケート調査
調査対象: 実証参加企業
調査方法: インターネット調査
調査時期: 2020 年 10 月 16 日（金）～12 月 18 日（金）
有効回答数: 104 サンプル
調査実施機関:株式会社マクロミル

＜第 3 回＞ 標的型攻撃メール訓練およびインシデント対応アンケート結果
調査対象: 実証参加企業
調査方法: インターネット調査
調査時期: 2020 年 11 月 6 日(金)～12 月 18 日(金)
有効回答数: 90 サンプル
調査実施機関:株式会社マクロミル

＜第 4 回＞ 実証参加企業への実証事業終了時アンケート
調査対象: 実証参加企業
調査方法: インターネット調査
調査時期: 2020 年 11 月 18 日(水)～12 月 18 日(金)
有効回答数: 82 サンプル
調査実施機関:株式会社マクロミル

なお、第 1 回:ICT 実態アンケート調査の回答企業の法人種別、業種、資本金、従業員数の内訳については図9～12のとおりである。

| n= | 会社 | 個人事業主 | 医療法人社会福祉法人 | 学校法人 | 商工会・都道府県商工会連合会及び商工会議所 | 中小企業団体 | 組合・連合会 | 財団法人、社団法人 | 特定非営利活動法人業 | その他 |
|---|---|---|---|---|---|---|---|---|---|---|
| 説明会参加企業(熊本) (147) | 78.2% | 4.8% | 5.4% | 1.4% | 0.7% | - | 4.8% | 0.7% | 1.4% | 2.7% |
| 一般(全国) (225) | 94.7% | - | 1.8% | 0.9% | - | 0.4% | 0.4% | 0.4% | 1.3% | - |

図 13：法人種別

| | 説明会参加企業（熊本）<br>(n=147) | 一般（全国）<br>(n=225) |
|---|---|---|
| 農業、林業 | 2.7% | 0.9% |
| 漁業 | - | - |
| 鉱業、採石業、砂利採取業 | 1.4% | - |
| 建設業 | 18.4% | 7.6% |
| 製造業 | 11.6% | 12.4% |
| 電気・ガス・熱供給・水道業 | 0.7% | 1.3% |
| 情報通信業 | 5.4% | 31.6% |
| 運輸業、郵便業 | 3.4% | 2.2% |
| 卸売業・小売業 | 12.2% | 11.1% |
| 金融業、保険業 | 6.1% | 1.8% |
| 不動産業、物品賃貸業 | 4.1% | 6.2% |
| 学術研究、専門・技術サービス業 | 1.4% | 2.7% |
| 宿泊業、飲食店 | 1.4% | 0.4% |
| 生活関連サービス業、娯楽業 | 3.4% | 1.8% |
| 教育学習支援業 | 2.0% | 0.9% |
| 医療、福祉 | 13.6% | 1.8% |
| 複合サービス事業 | 1.4% | 0.9% |
| サービス業（他に分類されないもの） | 8.2% | 13.8% |
| 公務（他に分類されるものを除く） | 1.4% | 0.4% |
| 分類不能の産業 | 1.4% | 2.2% |

図 14：業種

| | n= | 1千万円以下 | ～3千万円以下 | ～5千万円以下 | ～1億円以下 | ～3億円以下 | ～10億円以下 | それ以上 |
|---|---|---|---|---|---|---|---|---|
| 説明会参加企業（熊本） | (122) | 59.8% | 15.6% | 9.8% | 9.0% | 3.3% | 1.6% | 0.8% |
| 一般（全国） | (213) | 39.0% | 22.5% | 11.3% | 15.0% | 9.4% | 1.4% | 1.4% |

図 15：資本金

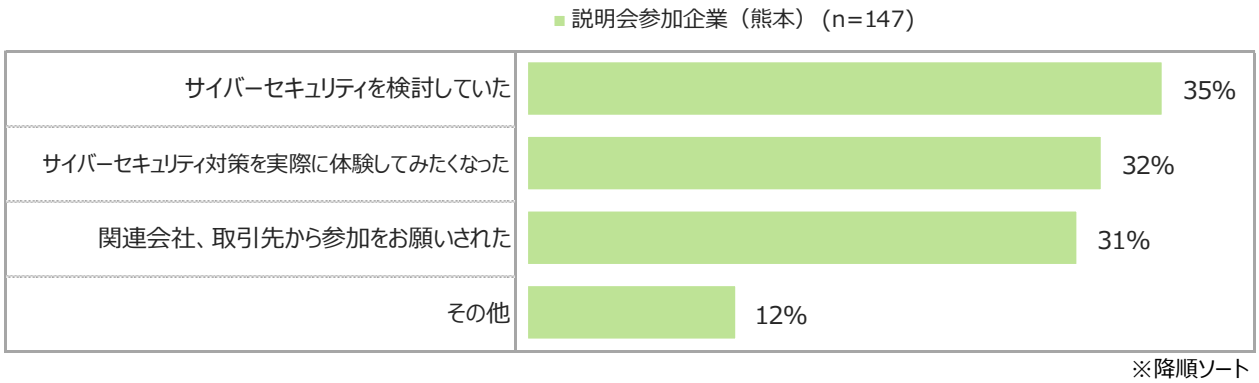
| | n= | ～5人 | ～10人 | ～20人 | ～50人 | ～100人 | ～200人 | ～300人 | ～400人 | ～500人 | ～600人 | ～700人 | ～800人 | ～900人 | ～1000人 | 1001人以上 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 説明会参加企業（熊本） | (147) | 18.4% | 13.6% | 15.6% | 21.1% | 9.5% | 12.2% | 4.1% | 0.7% | 0.7% | 0.7% | - | 1.4% | - | - | 2.0% |
| 一般（全国） | (225) | 26.2% | 10.2% | 8.4% | 10.7% | 12.4% | 9.8% | 9.8% | 3.1% | 1.8% | 0.9% | - | 0.9% | 0.4% | 1.8% | 3.6% |

図 16：従業員数

### 3.3. 中小企業の ICT 実態アンケート調査結果

本章では、本実証事業の説明会参加企業（熊本）および一般の企業（全国）に対して行った ICT 実態アンケート調査の結果を報告する。

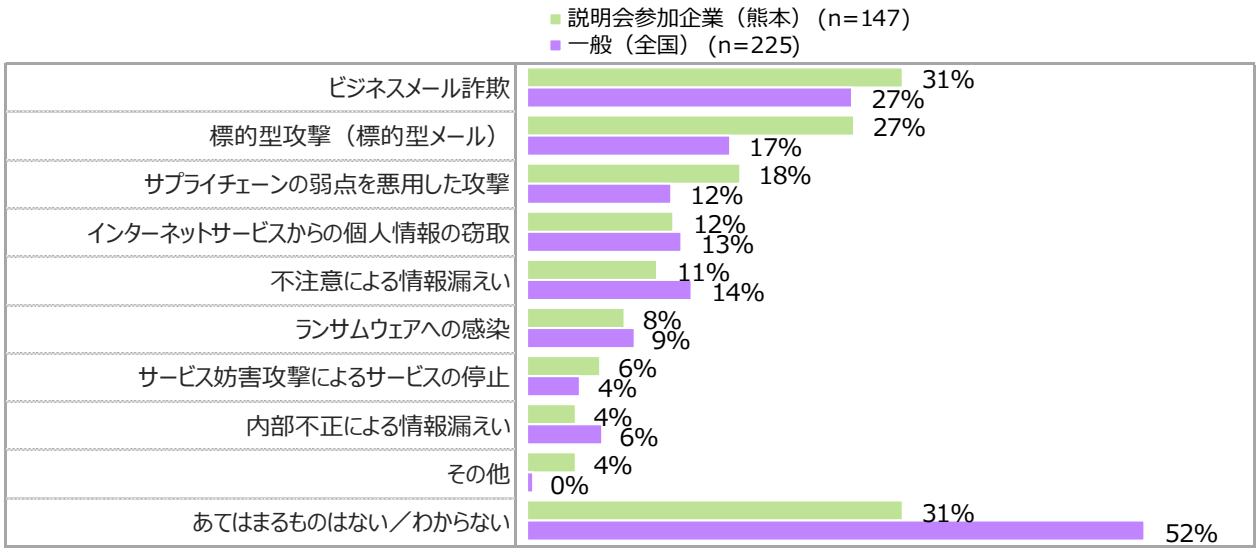
説明会への参加を決めた理由は、「サイバーセキュリティを検討していた」が最も高く、次いで「サイバーセキュリティ対策を実際に体験してみたくなった」が挙がっている。多くの説明会参加企業が、サイバーセキュリティを今後強化していきたい意向を持って参加している。




※降順ソート

図 17：説明会の参加を決めた理由（複数回答）

企業が今まで経験したセキュリティ脅威としては「ビジネスメール詐欺」「標的型攻撃（標的型メール）」が上位で、メールを介したセキュリティ脅威が大きくなっている。次いで「サプライチェーンの弱点を悪用した攻撃」を経験している企業が多くなっている。



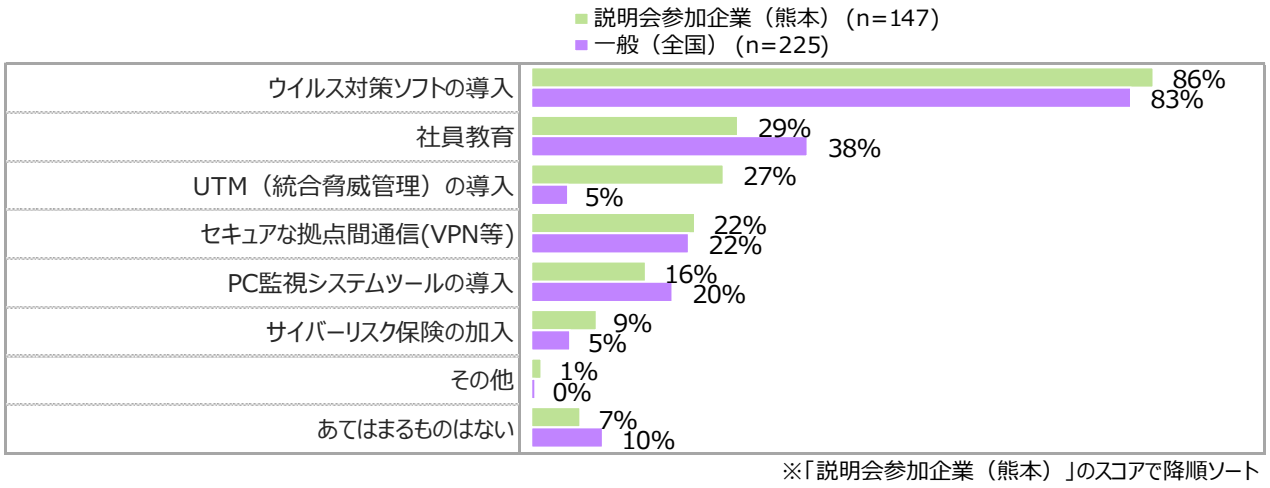

※「説明会参加企業（熊本）」のスコアで降順ソート

図 18：今まで経験したセキュリティ脅威（複数回答）

現在導入されているセキュリティ対策としては、「ウイルス対策ソフトの導入」が 8 割以上と突出している。次いで「社員教育」が高いが、説明会参加企業（熊本）で 29%、一般（全国）で 38%にとどまる。

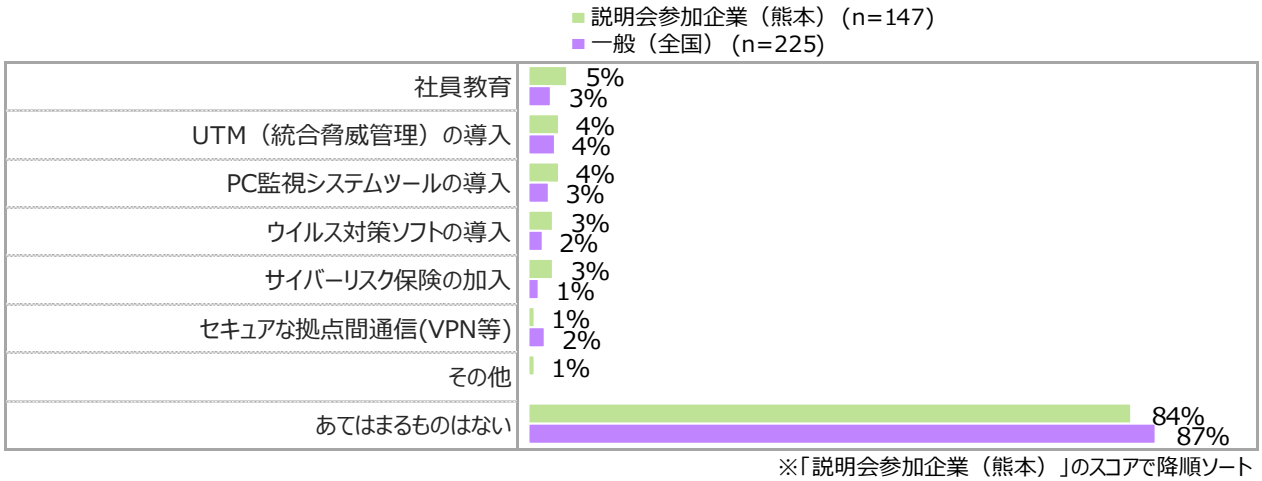
また、過去には行っていたが、現在行っていない（中止した）セキュリティ対策はそれほど多くないものの、各種システム・ツールの導入や社員教育を見合わせた企業も存在する。

その理由として「満足な効果が得られなかった」「コスト面で負荷になった」が多く挙げられている。




※「説明会参加企業（熊本）」のスコアで降順ソート

図 19：現在導入されているセキュリティ対策（複数回答）




※「説明会参加企業（熊本）」のスコアで降順ソート

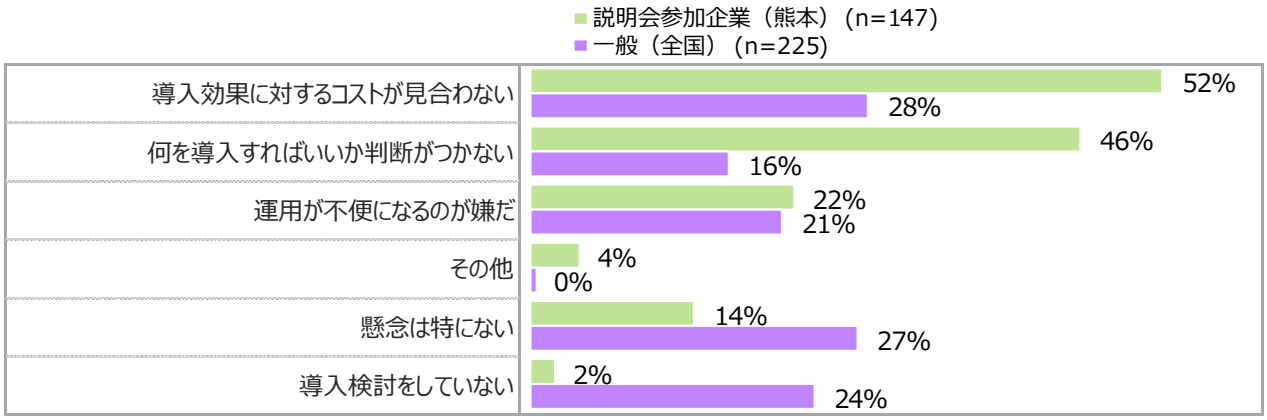
図 20：過去には行っていたが、現在行っていない対策（複数回答）

※過去行っていたが、現在行っていない対策がある方ベース

| | | n= | コスト面で負荷になった | 満足な効果が得られなかった | 通常業務へ影響が出た | その他 |
|---|---|---|---|---|---|---|
| ウイルス対策ソフトの導入 | 説明会参加企業（熊本） | (5) | 40% | 60% | - | - |
| | 一般（全国） | (4) | 25% | 100% | 50% | - |
| UTMの導入 | 説明会参加企業（熊本） | (6) | 50% | - | 50% | - |
| | 一般（全国） | (8) | 50% | 75% | 25% | 13% |
| 社員教育 | 説明会参加企業（熊本） | (8) | 38% | 13% | 13% | 38% |
| | 一般（全国） | (7) | 14% | 57% | 43% | 14% |
| PC監視システムツールの導入 | 説明会参加企業（熊本） | (6) | 50% | 33% | 17% | - |
| | 一般（全国） | (6) | 50% | 50% | - | - |
| セキュアな拠点間通信(VPN等) | 説明会参加企業（熊本） | (1) | 100% | - | - | - |
| | 一般（全国） | (5) | 40% | 60% | 40% | - |
| サイバーリスク保険の加入 | 説明会参加企業（熊本） | (5) | 80% | - | - | 20% |
| | 一般（全国） | (3) | 67% | - | - | 33% |
| その他 | 説明会参加企業（熊本） | (1) | - | - | - | 100% |
| | 一般（全国） | (0) | - | - | - | - |

図 21：対策を辞めた理由（複数回答）

今後のセキュリティ対策の導入を検討する際、「導入効果に対するコストが見合わない」が最大の懸念点である。また、説明会参加企業（熊本）では「何を導入すればいいか判断がつかない」も高く、コストも含めてそれぞれの企業に合ったセキュリティ対策の提案が必要となっている。




※「説明会参加企業（熊本）」のスコアで降順ソート

図 22：セキュリティ対策の導入検討における懸念点（複数回答）

セキュリティに関する情報源としては「取引先ベンダー」「IT 情報誌、IT 情報サイト」の存在が大きくなっている。「IPA 等の公的 Web サイト」は 2 割弱が利用している。
一方で、情報収集を行っていない企業も、3 割以上に上り、セキュリティに関する身近な情報源を把握していない企業の割合が高くなっている。

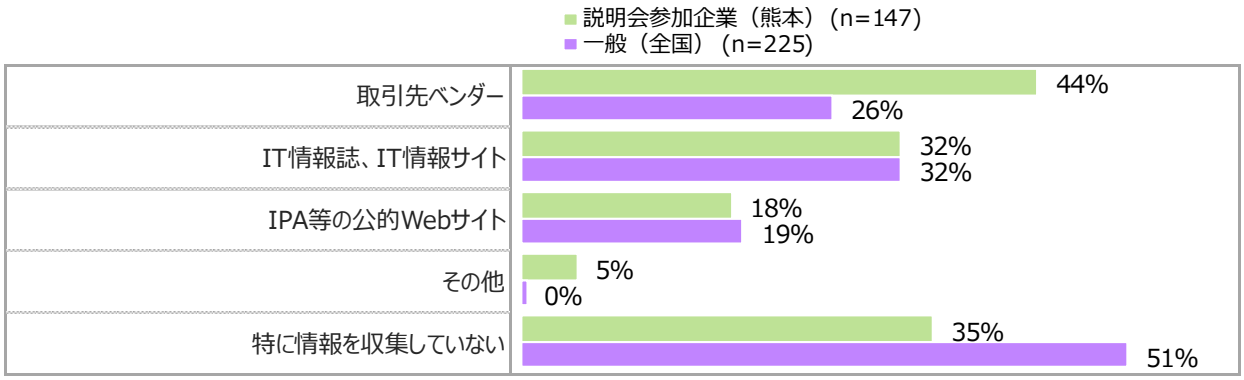



図 23：セキュリティに関する情報源（複数回答）

企業におけるセキュリティ体制や対策状況について、「社内でセキュリティ対策を任せている担当者がいる」のは 5 割程度、「社外でセキュリティのことを任せている専門業者がいる」のは 3 割程度となっており、社内に担当者を置いている企業が多い。セキュリティ対策として実施率が高いのは、Wi-Fi 接続のアクセス制限、PC 利用ポリシーの設定、ファイルの持ち出し制限などである。概ね一般（全国）よりも説明会参加企業（熊本）における実施率が低く、セキュリティ対策の普及の遅れが指摘される。

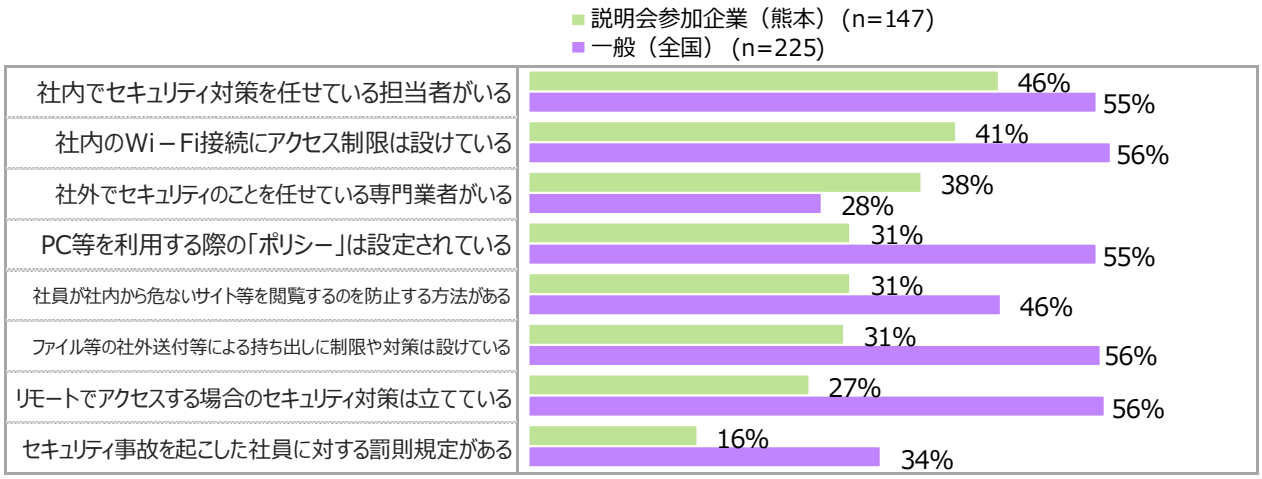



図 24：セキュリティ体制や対策状況についてあてはまるもの（複数回答）

テレワークの導入率は、一般（全国）では 5 割弱に達しているのに対し、説明会参加企業（熊本）では 2 割台にとどまる。説明会参加企業（熊本）では導入未検討の割合が高いが、次いで「一部導入しているが、まだ課題があり追加の対策が必要」「導入を検討しているが、導入の目処はついていない」の割合が高く、導入済み／導入検討中の企業における課題感も大きくなっている。

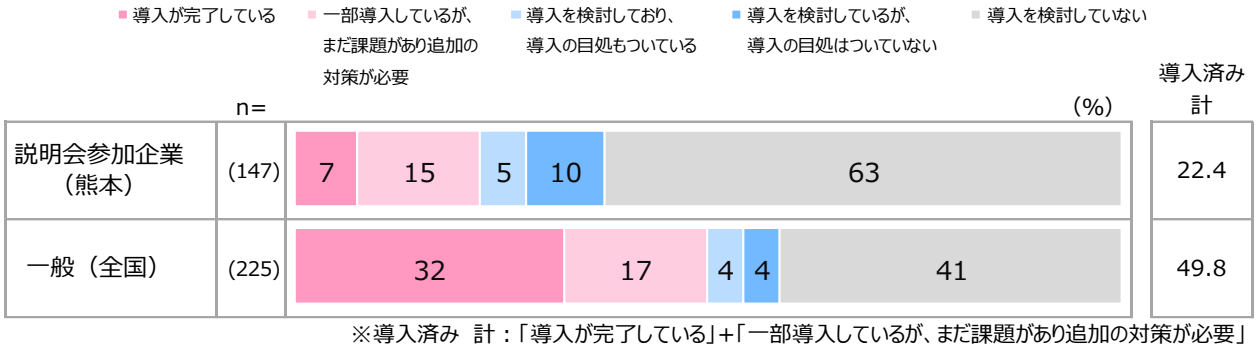



図 25：テレワークの導入状況

テレワークを導入している企業では「自宅からリモートを利用し、社内 PC へアクセス」「自宅 PC から VPN 装置を経由し社内ネットワークへ接続」がボリュームゾーンである。しかし、説明会参加企業（熊本）では「USB や書類等で社内情報を持ち帰り、自宅で作業」といったアナログな方法で実施している割合も 24%と高く、セキュリティ面での課題が残る。

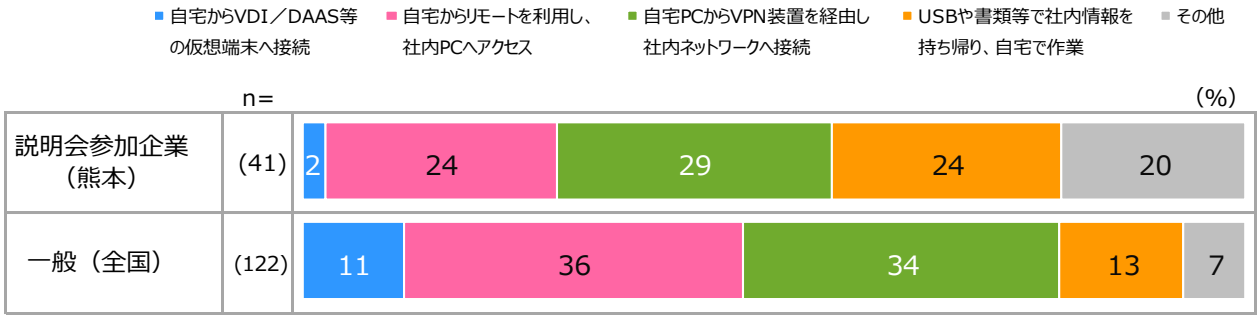



図 26：テレワークで導入している（導入予定の）システム

テレワークの導入に至っていない理由としては「業務上、テレワークでは対応不可能な業務がある」「テレワークを導入する必要性を感じない」が高く、業務による事情、必要性に対する意識の低さが要因として大きくなっている。テレワークを推進するには、具体的な導入方法やコストなどの課題以前に、どういった業務がテレワーク化できるのか、テレワークを導入することでどんなメリットがあるのか、といった視点での提案が必要と考えられる。

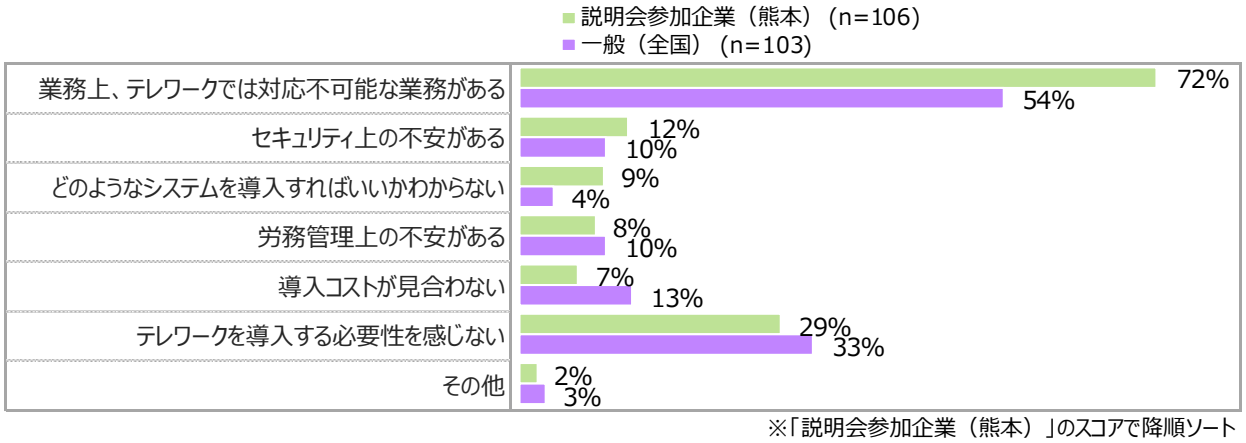



図 27：テレワークの導入に至っていない理由（複数回答）

PC・OS・アプリなどの更新方法について「ルールが決まっておらず、管理ができていない」が 3 割以上を占める。特に説明会参加企業（熊本）で 4 割近くに上る。また、ルールが決まっている企業では「システム管理者が更新・管理をおこなっている」「システム管理者が管理し、パソコン等のユーザー自身が更新をおこなっている」の割合が高いが、ルール通りに運用できていない層も存在する。

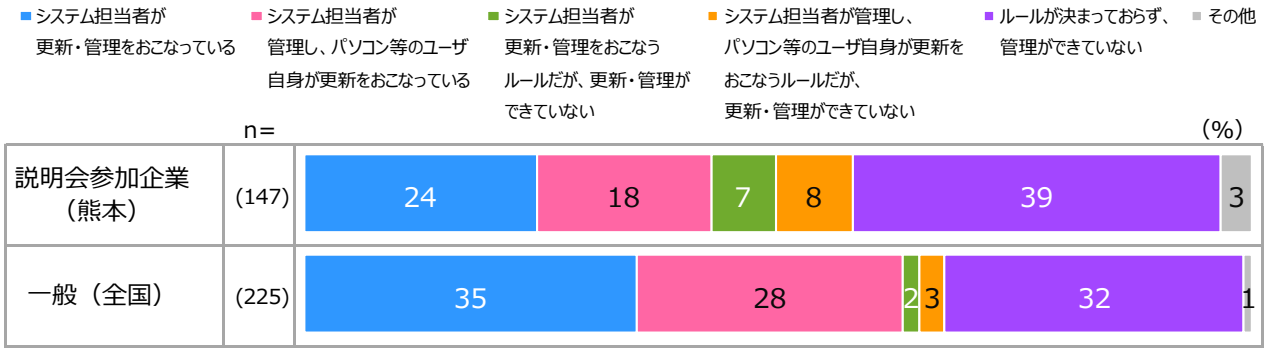



図 28：PC・OS・アプリなどの更新の管理方法

利用されている業務システムは経理、勤怠管理、Web 会議などが上位で、何らかの業務システムを導入している企業が計 7 割前後である。

また、取引先とのシステム連携している企業は 1 割前後で、割合としては少ない。

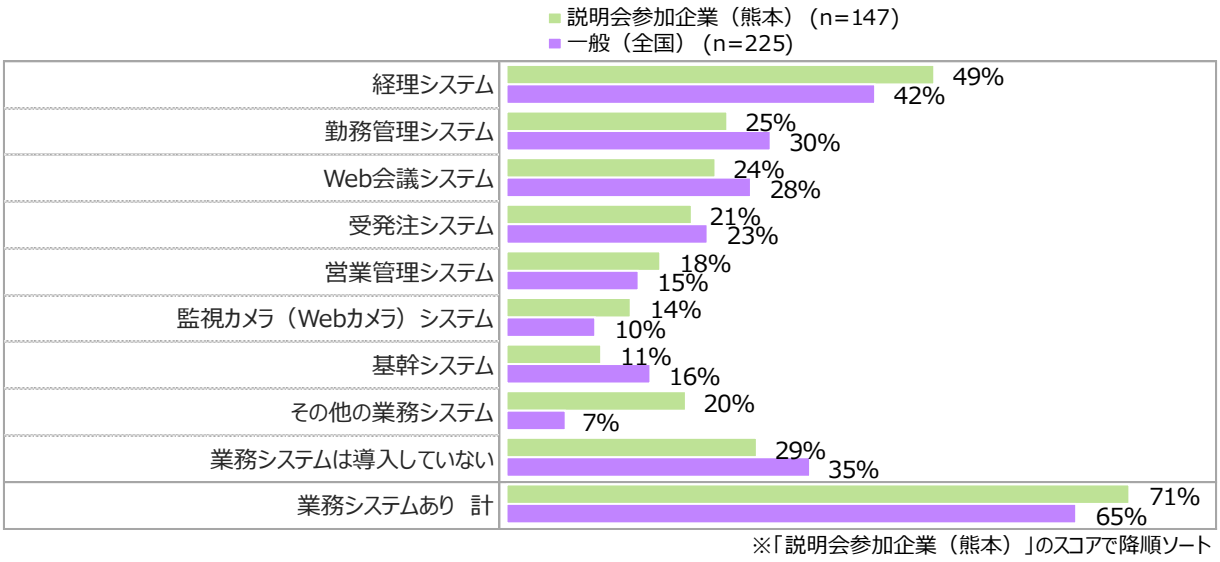



図 29：利用している業務システム（複数回答）

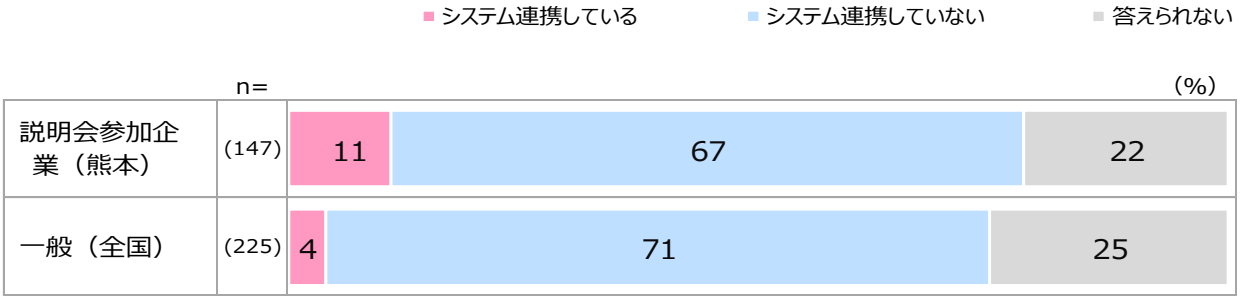
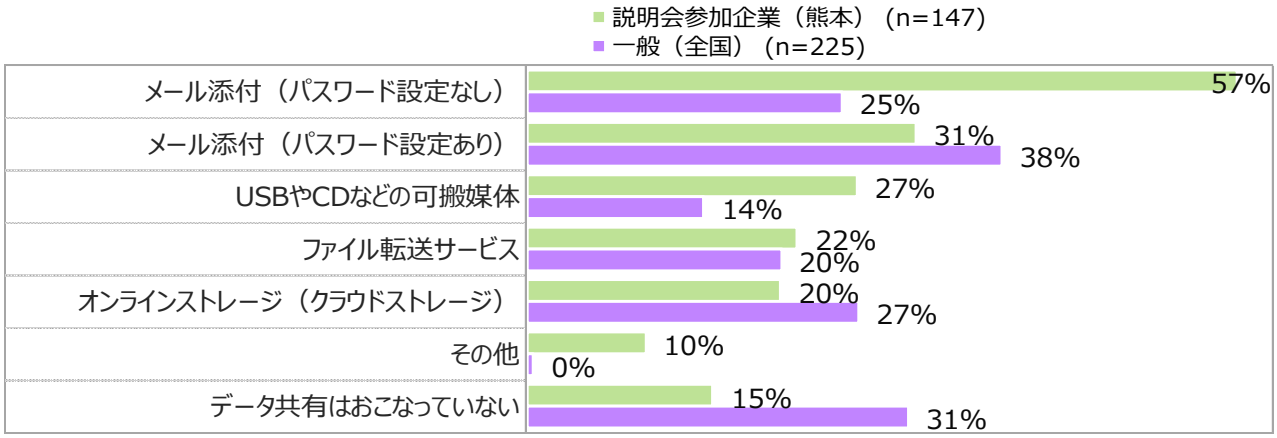



図 30：取引先とのシステム連携の有無

外部とのデータ共有の方法について、説明会参加企業（熊本）では「メール添付（パスワード設定なし）」が 5 割以上と突出。次いで「メール添付（パスワード設定あり）」「USB や CD などの可搬媒体」が続き、既存のデータ共有方法が使われ続けている状況である。一方、一般（全国）では「メール添付（パスワード設定あり）」「オンラインストレージ」「メール添付（パスワードなし）」が上位となっている。

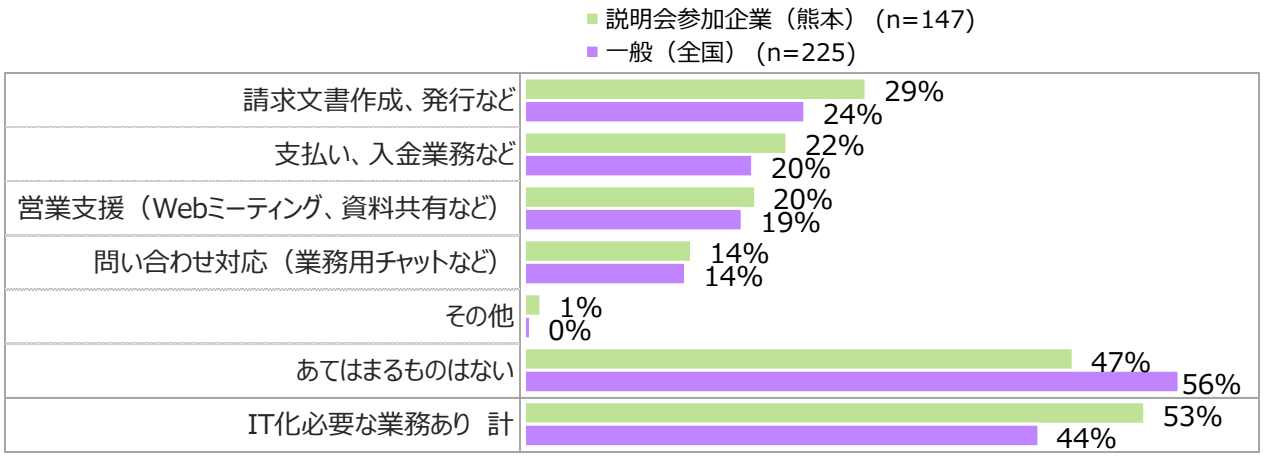



※「説明会参加企業（熊本）」のスコアで降順ソート

**図 31：外部とのデータ共有方法（複数回答）**

今後 IT 化が必要な業務としては「請求文書作成、発行など」「支払い、入金業務など」といった経理関連の業務が上位となっている。

何らかの IT 化必要な業務のある企業が 5 割前後であり、IT 化の推進が期待される。




※「説明会参加企業（熊本）」のスコアで降順ソート

**図 32：今後 IT 化が必要な業務（複数回答）**

### 3.4. 実証参加企業のセキュリティ対策事前アンケート調査結果

本章では、本実証事業の実証参加企業に対して事前に行ったアンケート調査の結果を報告する。

本実証事業への参加を決めた理由としては「サイバーセキュリティ向上の効果が期待できそうだから」が最も高い。次いで「無料期間中だけでも利用してみたかったから」「試験的に運用してみて、効果があれば今後導入したいから」が挙がっており、無料によるトライアルへのハードルの低さから参加を決めた企業が多く、本実証事業がセキュリティ対策導入のきっかけとして有効であったことが分かる。

具体的に期待していることとしては「悪意のあるウイルスの外部からの遮断」が最も高く、ウイルス感染のリスクを減らしたいというニーズが最も大きい。次いで「悪意のあるメールの外部からの遮断」「脅威検知内容のレポート報告」に対する期待が高くなっている。

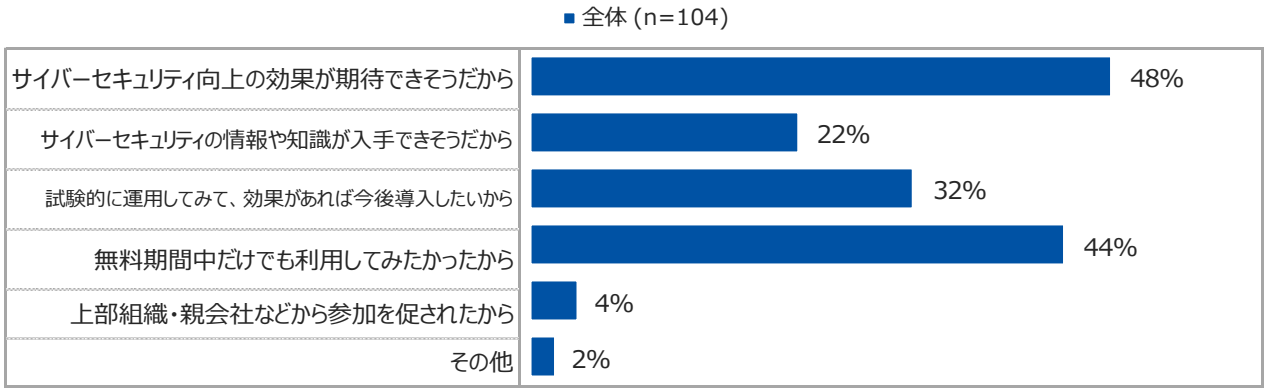
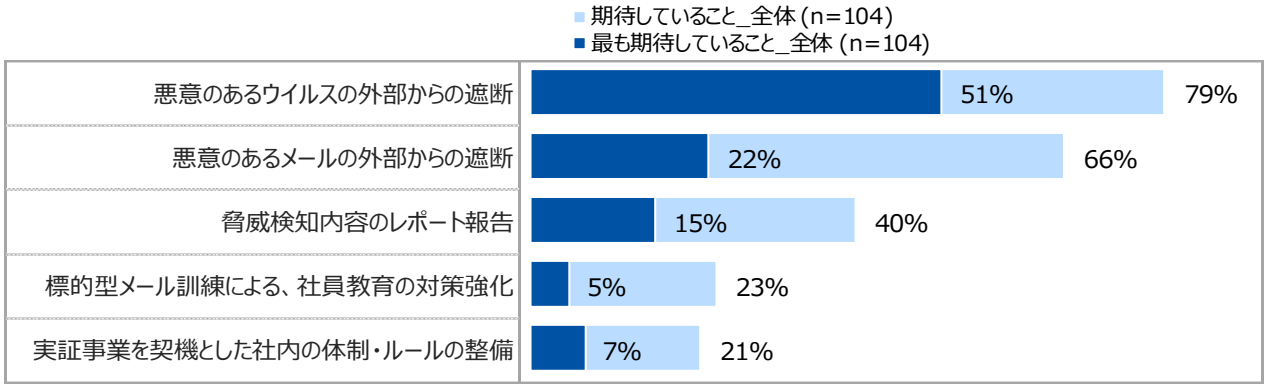


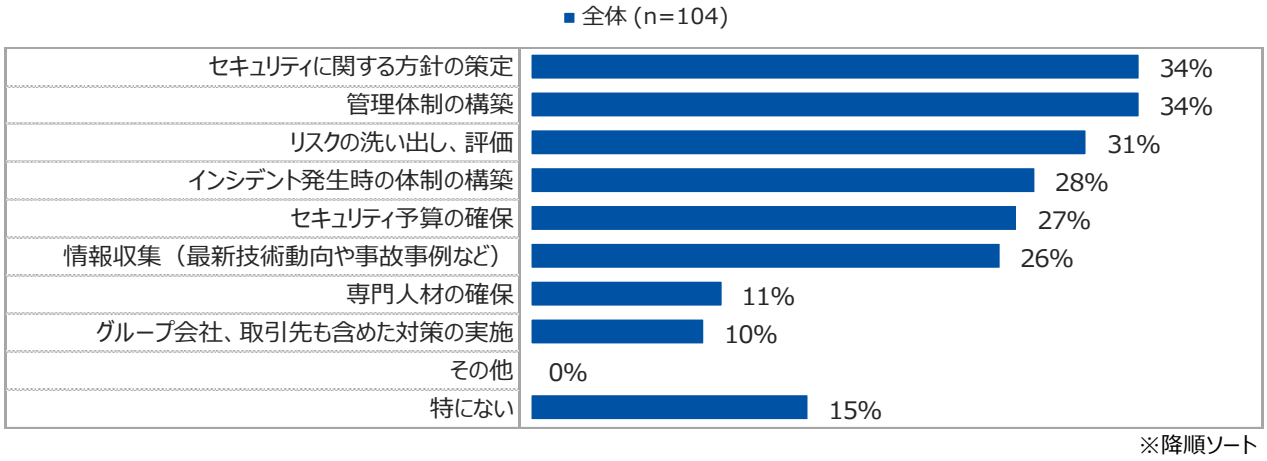

図 33：本実証事業への参加を決めた理由（複数回答）




※「期待していること_全体」のスコアで降順ソート

図 34：本実証事業で期待していること

実証事業実施前時点でのサイバーリスクの課題として「セキュリティに関する方針の策定」「管理体制の構築」など全体的な方針・体制を整えることが課題と感じている企業が多くなっている。




※降順ソート

図 35：サイバーリスクに関する課題：事前（複数回答）

自社がサイバー攻撃を受けるリスクがあると思うかについては、75%がリスクありと回答しており、リスクを自分事として受け止めている企業が多くなっている。

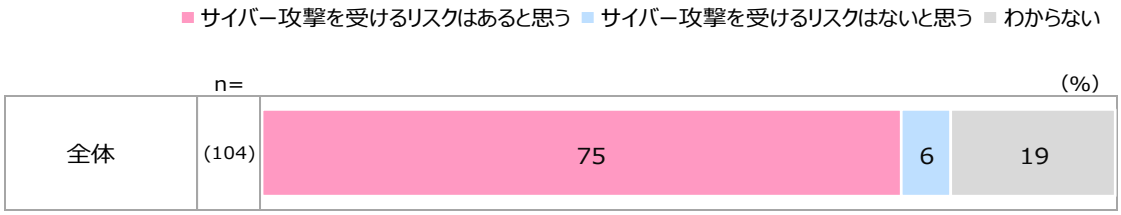



図 36：サイバー攻撃を受けるリスクがあると思うか：事前

現在のサイバーセキュリティ対策の年間予算としては「全くかけていない」が 38%。最も割合が高いのは「12 万円未満（月額 1 万円未満）」で 45%を占めており、全体の 8 割以上が年間予算なし～12 万円未満となっている。

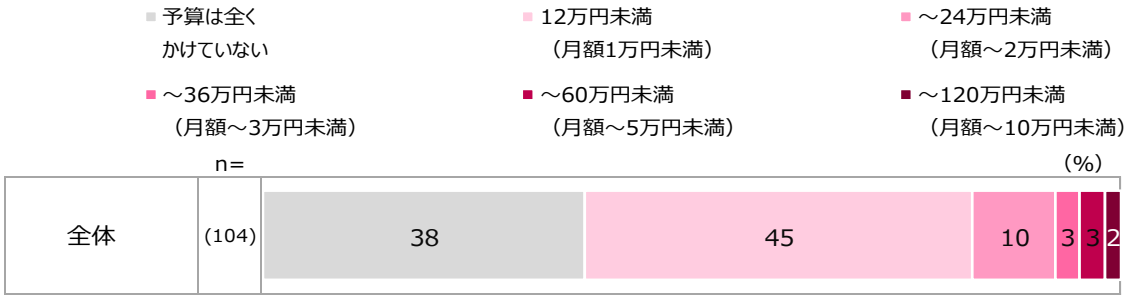



図 37：現在のサイバーセキュリティ対策予算

セキュリティ事故（インシデント）が発生した場合の最高被害額の想定については、100 万円以下がボリュームゾーンで中央値は 100 万円。一方で、100 万円より大きい金額を想定している企業も半数存在する。

サイバーセキュリティ保険の加入率は 1 割、加入検討層を含めても 2 割に満たない結果である。

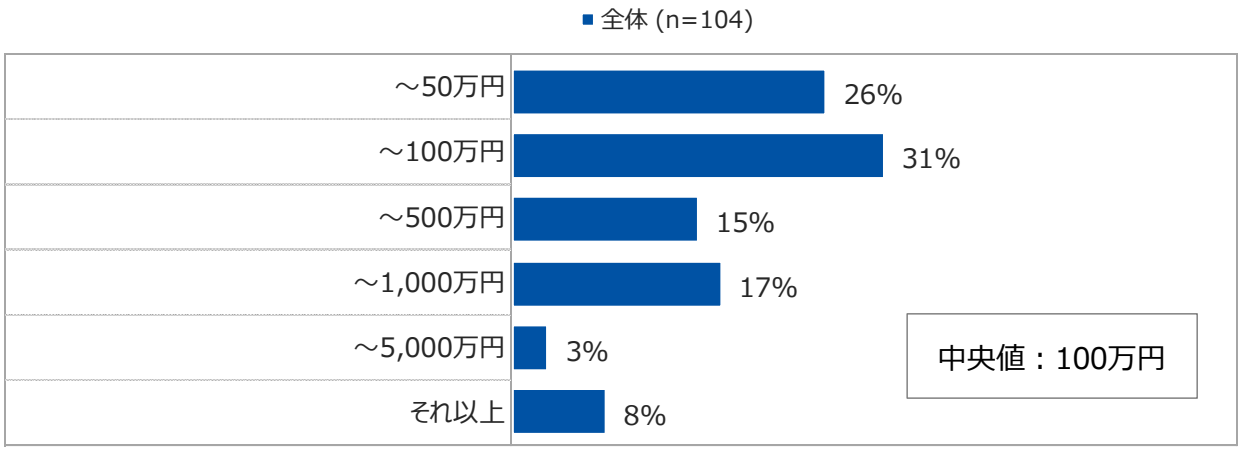
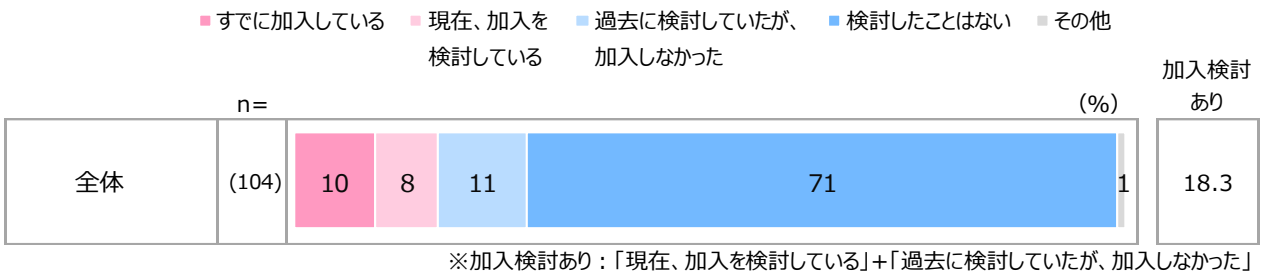



図 38：セキュリティ事故が発生した場合の最高被害額の想定（数値回答）




※加入検討あり：「現在、加入を検討している」+「過去に検討していたが、加入しなかった」

図 39：サイバーセキュリティ保険への加入・検討状況

セキュリティ事故が発生した場合の相談窓口は「取引先ベンダー」が 55%と最も高いが、「相談できる窓口は無い」も 3 割以上で、ベンダーとの取引が無い場合は相談先がほとんど無い状態である。

一方で、セキュリティ事故が発生した場合「自社内に有スキル者がいるため、解決可能である」と考えているのは全体の 4%にとどまり、多くの企業が外部の助けを必要としている。

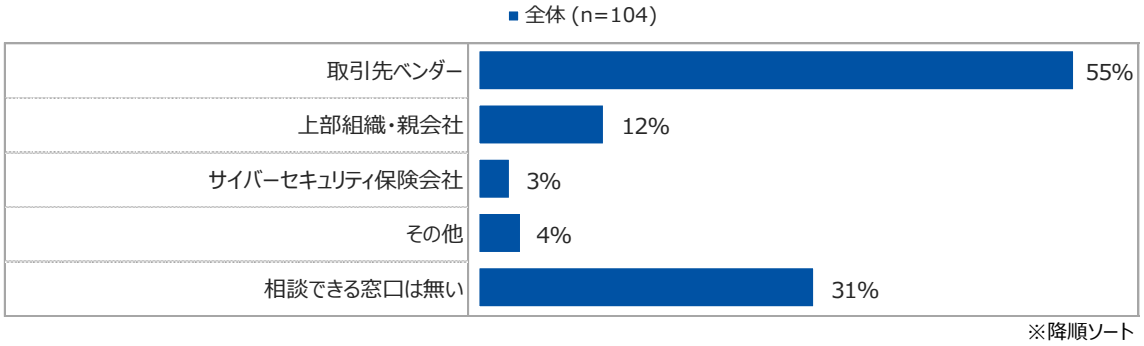



図 40：セキュリティ事故発生時の相談窓口（複数回答）

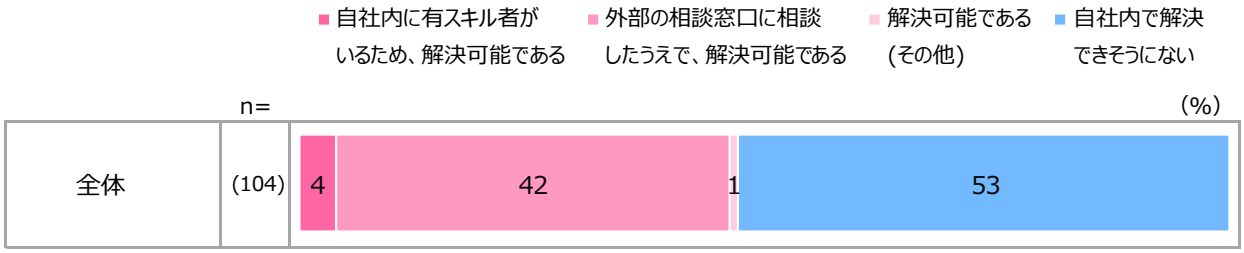
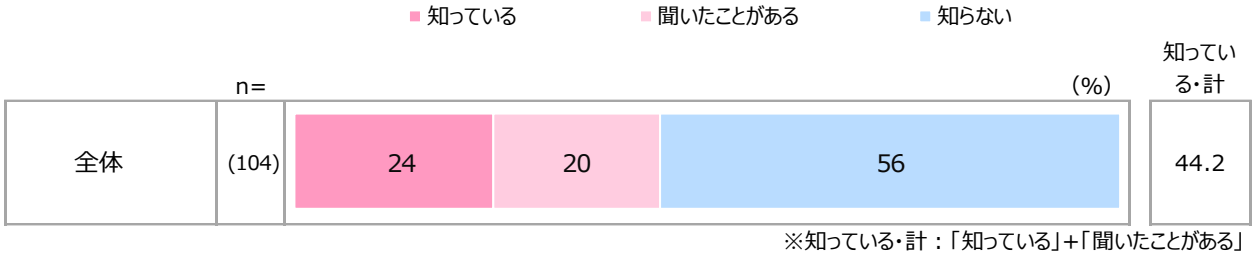



図 41：セキュリティ事故が発生した場合、自社内で解決可能か

実証事業参加前に「UTM（統合脅威管理）」を知っていたのは 44%で、知らなかった層が過半数である。

UTM の導入について、「検討または導入」に至っているのは 2～3 割程度で、未検討層や UTM 自体を認知していない層が大部分となっている。




※知っている・計：「知っている」+「聞いたことがある」

図 42：UTM の認知状況


※検討または導入・計：「すでに導入している」～「提案は受けていないが、現在導入を検討している」

図 43：UTM の導入・検討状況

セキュリティに関して、社員向けに何らかの啓発活動を行っているのは実証参加企業（熊本）では38%、一般（全国）では54%で、実証参加企業での実施率が低くなっている。

実施内容で特に差が大きいのは「社員への定期的なセキュリティ研修の実施」「入社時のセキュリティ研修の実施」「セキュリティに関する理解度チェックやテストの実施」であり、定期的な／決まったタイミングでの研修実施や、実際に社員が理解しているかまでを確認することができていない企業が、実証参加企業では多くなっている。

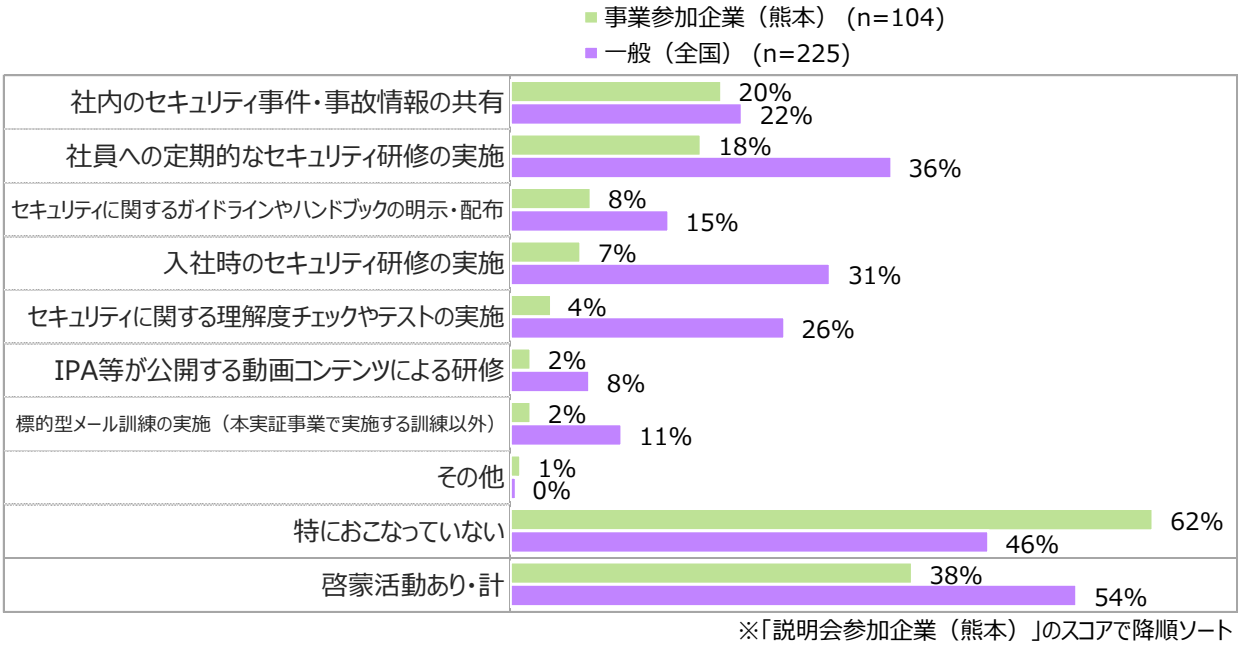



図 44：社員向けに行っている啓発活動（複数回答）

セキュリティ担当者の育成・スキルアップの取り組みについても、実証参加企業（熊本）は一般（全国）に比べて実施率が低くなっている。特に「情報セキュリティに関する講習の受講」において差が大きくなっている。

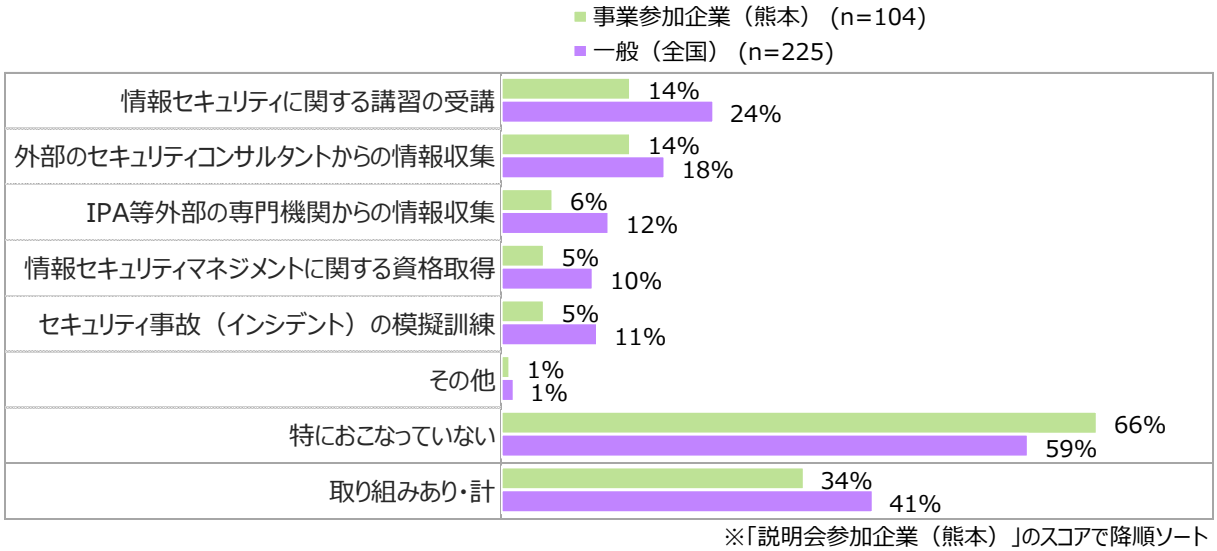



図 45：セキュリティ担当者の育成・スキルアップの取り組み（複数回答）

### 3.5. 標的型攻撃メール訓練およびインシデント対応アンケート結果

本章では標的型攻撃メール訓練およびインシデント対応に関するアンケート調査結果について報告する。

まず標的型攻撃メール訓練について、事前に社員へ予告を行っていた企業は実証参加企業の 2 割である。

結果、添付ファイルを開いたケースがあったのは全体の 2 割で、送付件数 10 件のうち、平均 0.5 件が開封されている。また、不審なメールとして報告があったケースがあったのは全体の 3 割半ばである。

不審なメールとして報告があったケースのうち、添付ファイルを開いていたケースはわずかであり、添付ファイルを開いたケースよりも割合が少なくなっている。すなわち添付ファイルを開いたにもかかわらず報告がされなかったケースが多かったことが推察される。

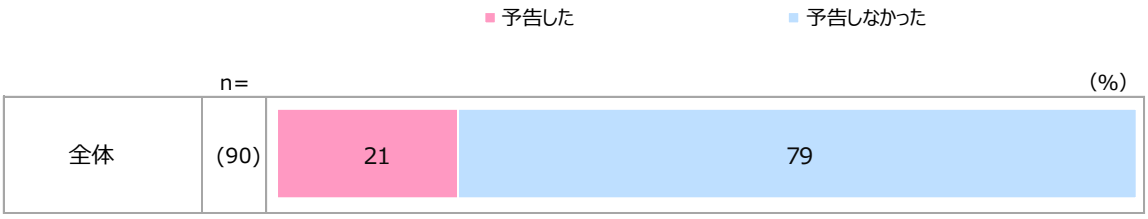



図 46：社員への予告の有無

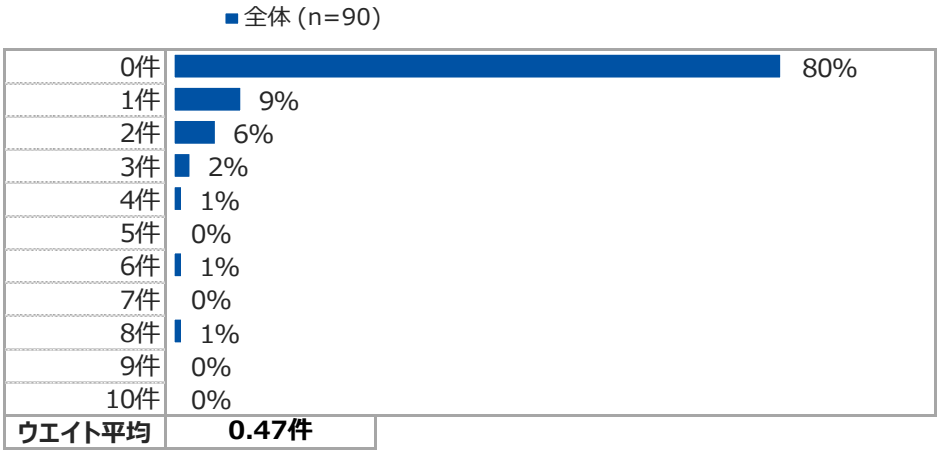



図 47：添付ファイルを開いた件数

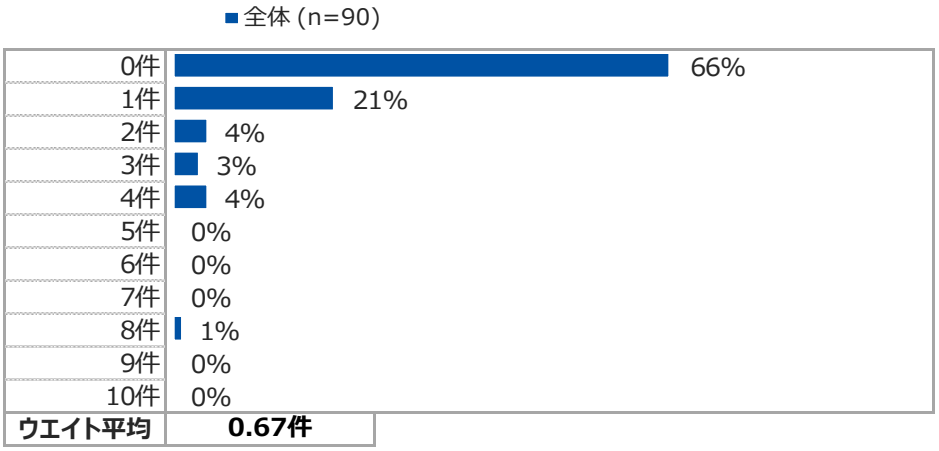



図 48：不審なメールとして報告があった件数

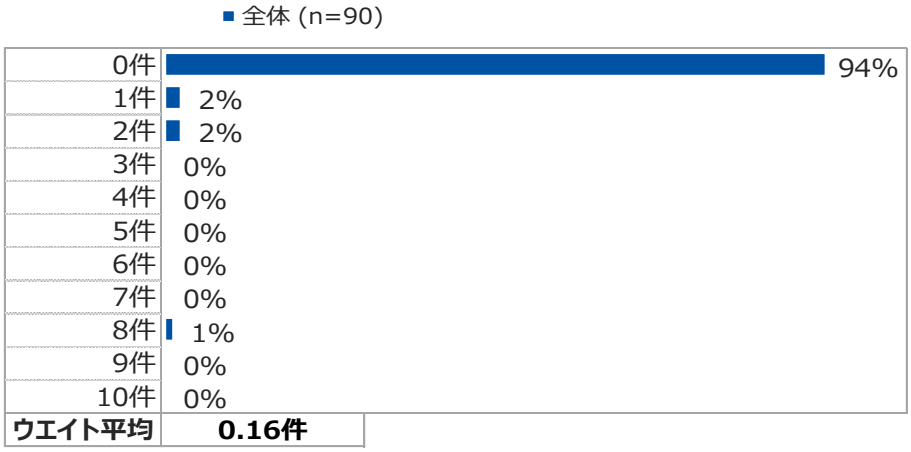



図 49：不審なメールとして報告があったケースのうち、添付ファイルを開いていた件数

訓練前後に不審なメールへの対応方法に関する研修を実施したのは全体の 2 割にとどまる。

訓練により、社員のセキュリティ対策意識が向上したと感じている企業が 6 割以上と、一定の効果は感じられている。

また、今後の訓練の実施意向は「定期的に実施したい」が 33%、「訓練は必要だが、一度でよいと思う」が 38%で、訓練の必要性は伝わったものの、繰り返し実施することの必要性を伝えることが今後の課題となる。

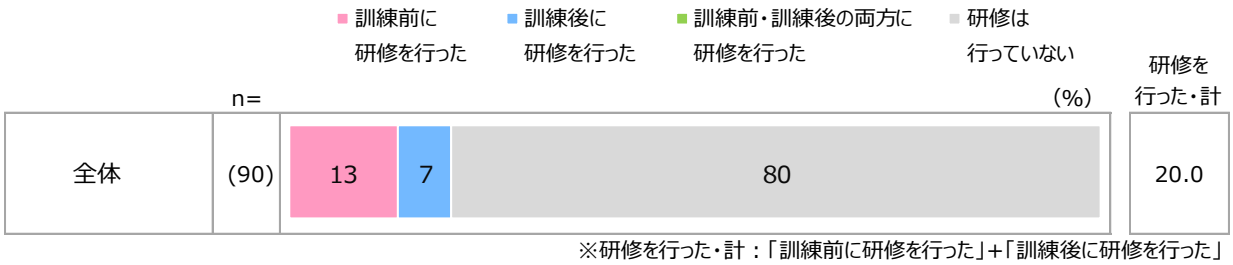



図 50：不審なメールへの対応方法に関する研修の実施有無

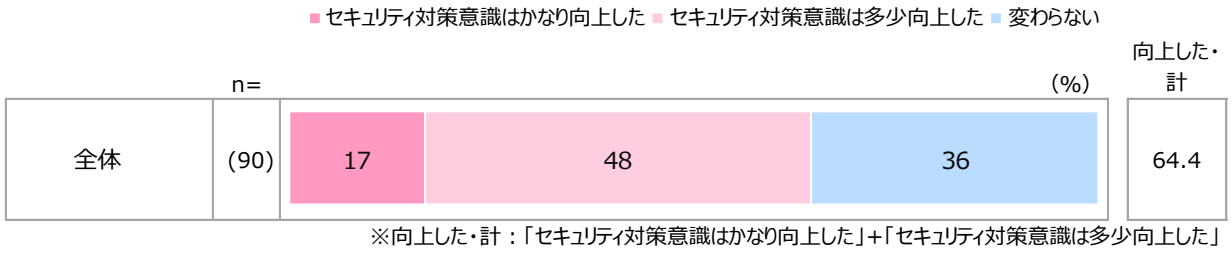



図 51：訓練により、社員のセキュリティ対策意識は向上したと思うか

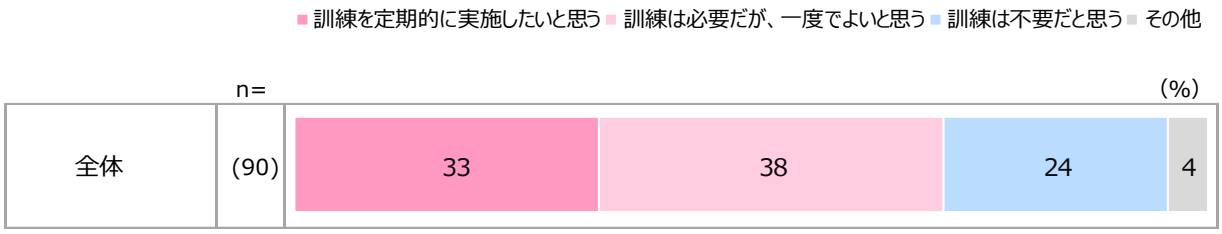



図 52：定期的な訓練の実施意向

ここからはインシデント対応に関する調査結果を報告する。
回答企業のうち、インシデント対応が実際に行われた企業は 3%（3 件）であった。

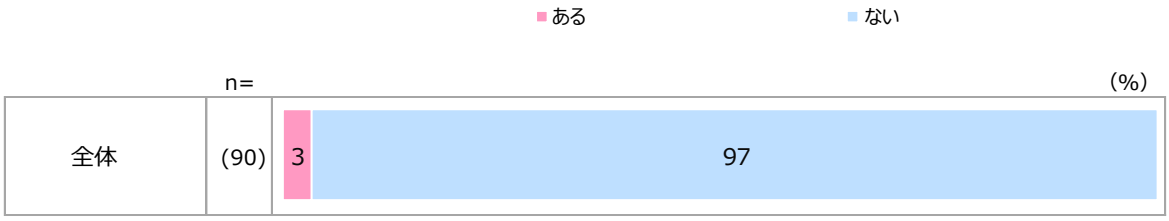



図 53：インシデント対応の有無

発生したインシデントについて、「過去に同様の経験がある」「過去に同様の経験はない」が同率。
オペレーターの対応は「分かりやすかった」の評価が 100%であった。
インシデント対応には、現地駆付けまたは電話による対応が行われた。

※インシデント対応ありの方ベース

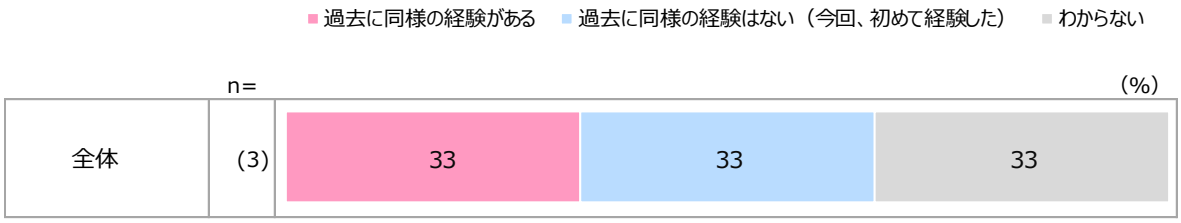
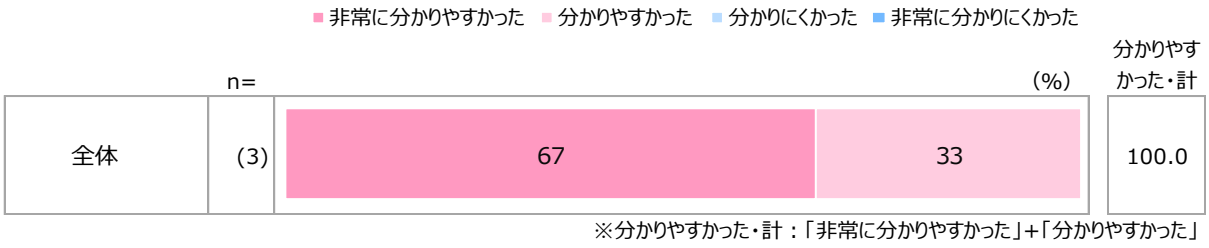



図 54：インシデントについて、過去に同様の経験があったか

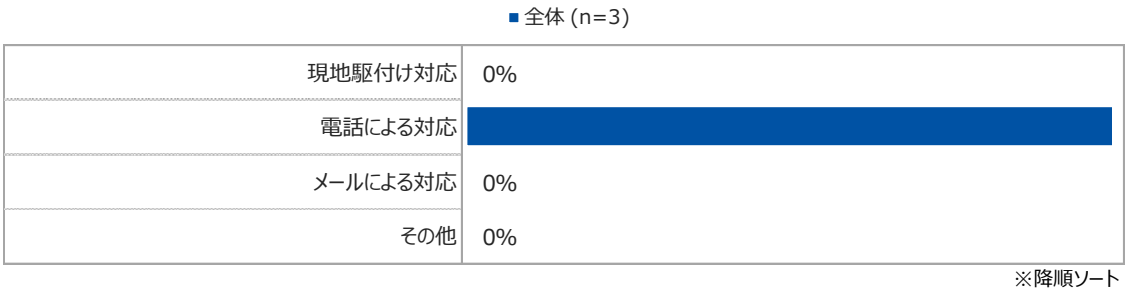
※インシデント対応ありの方ベース




※分かりやすかった・計：「非常に分かりやすかった」+「分かりやすかった」

図 55：オペレーター対応の評価

※インシデント対応ありの方ベース




※降順ソート

図 56：インシデント対応の方法

データの復旧作業について「完全に復旧できた」「復旧できなかった」「復旧作業は無かった」に分かれており、復旧できた企業においては想定よりも早いスピードで復旧できたと評価されている。

※インシデント対応ありの方ベース

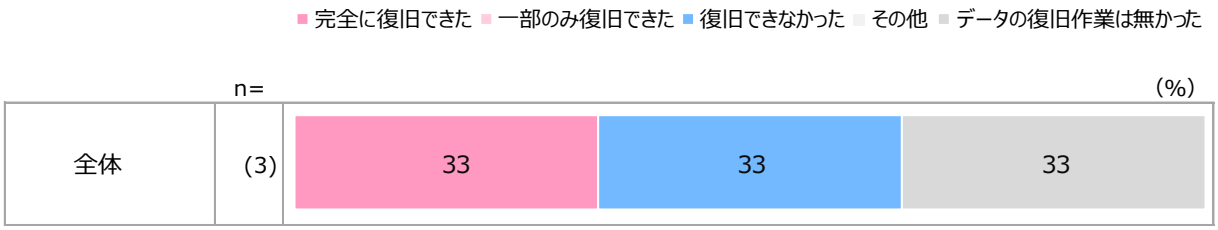



図 57：データ復旧の可否

※データ復旧作業ありの方ベース

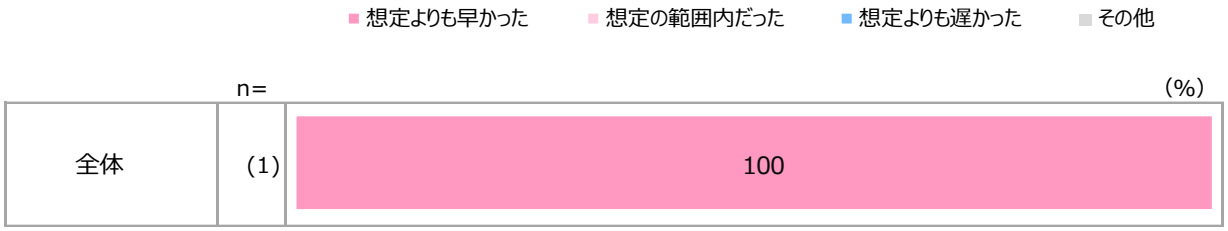



図 58：データ復旧の早さ

### 3.6. UTM およびエンドポイントによる対策結果

UTM およびエンドポイントで防御された脅威の情報は、翌月 1 日に実証参加企業に送付した。これにより、実証参加企業は、システムにより自動的に防がれた脅威情報を確認することができる。


TREND MICRO | Worry Free™ Business Security Services

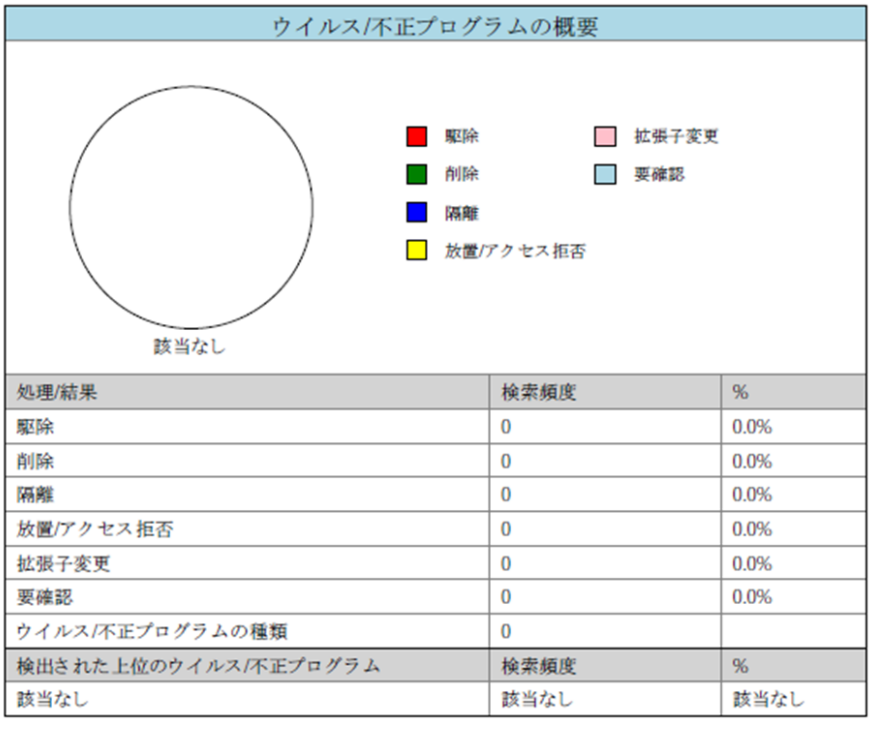
【 セキュリティおまかせプラン月次レポート 】
( エンドポイント )

開始:2020年12月1日 00:00:00JST
終了:2021年1月1日 00:00:00JST
生成日時: 2021年1月1日 00:06:16JST
含まれるグループ: すべてのデバイス

目次

ウイルス/不正プログラムの概要
スパイウェア/グレーウェア概要
ウイルス/不正プログラムが検出されたエンドポイント (サーバを除く) の上位5件
ウイルス/不正プログラムが検出されたサーバの上位5件
検出されたネットワークウイルスの上位10件
ネットワークウイルスが検出されたエンドポイントの上位10件
スパイウェア/グレーウェアが検出されたエンドポイント (サーバを除く) の上位5件
スパイウェア/グレーウェアが検出されたサーバ上位5件
Webレピュテーション違反のあったエンドポイントの上位10件
挙動監視違反のあったプログラムの上位5件
挙動監視違反のあったエンドポイントの上位10件
デバイスコントロール違反のあったプログラムの上位5件
デバイスコントロール違反のあったエンドポイントの上位10件
URLフィルタ違反のあったカテゴリ上位5件
URLフィルタ違反のあったエンドポイントの上位10件

図 59：エンドポイント月次レポート例 1/4


ウイルス/不正プログラムの概要



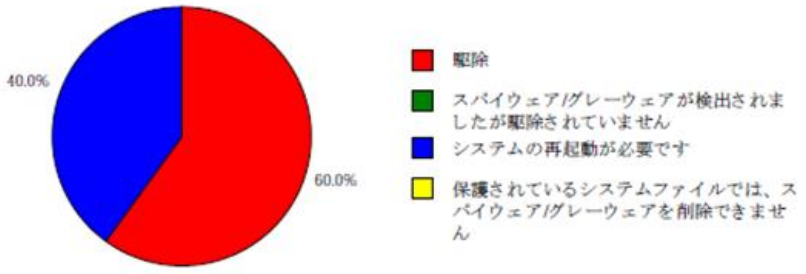
該当なし

駆除
削除
隔離
放置/アクセス拒否
拡張子変更
要確認

| 処理/結果 | 検索頻度 | % |
|---|---|---|
| 駆除 | 0 | 0.0% |
| 削除 | 0 | 0.0% |
| 隔離 | 0 | 0.0% |
| 放置/アクセス拒否 | 0 | 0.0% |
| 拡張子変更 | 0 | 0.0% |
| 要確認 | 0 | 0.0% |
| ウイルス/不正プログラムの種類 | 0 | |
| 検出された上位のウイルス/不正プログラム | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

図 60：エンドポイント月次レポート例 2/4

## スパイウェア/グレーウェア概要




| 処理/結果 | 検索頻度 | % |
|---|---|---|
| 駆除 | 9 | 60.0% |
| スパイウェア/グレーウェアが検出されましたが駆除されていません | 0 | 0.0% |
| システムの再起動が必要です | 6 | 40.0% |
| 保護されているシステムファイルでは、スパイウェア/グレーウェアを削除できません | 0 | 0.0% |
| スパイウェア/グレーウェアの種類 | 15 | |

| 検出された上位のスパイウェア/グレーウェア | 検索頻度 | % |
|---|---|---|
| PUA.Win32.MyWebSearch.AE.component | 8 | 53.3% |
| PUA.Win32.MyWebSearch.GF.component | 1 | 6.7% |
| PUA.Win32.MyWebSearch.SMTB3 | 1 | 6.7% |
| PUA_MyPCBackup.GC | 1 | 6.7% |
| PUA.Win32.MyWebSearch.IL.component | 1 | 6.7% |

| ウイルス/不正プログラムが検出されたエンドポイント (サーバを除く) の上位5件 | | |
|---|---|---|
| エンドポイント | 検出した脅威 | % |
| 該当なし | 該当なし | 該当なし |

| ウイルス/不正プログラムが検出されたサーバの上位5件 | | |
|---|---|---|
| エンドポイント | 検出した脅威 | % |
| 該当なし | 該当なし | 該当なし |

| 検出されたネットワークウイルスの上位10件 | | |
|---|---|---|
| ネットワークウイルス | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

図 61：エンドポイント月次レポート例 3/4

| ネットワークウイルスが検出されたエンドポイント の上位10件 | | |
|---|---|---|
| エンドポイント | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| スパイウェア/グレーウェアが検出されたエンドポイント (サーバを除く) の上位5件 | | |
|---|---|---|
| エンドポイント | 検出した脅威 | % |
| dan-PC | 13 | 86.7% |
| user01-pc | 2 | 13.3% |

| スパイウェア/グレーウェアが検出されたサーバ上位5件 | | |
|---|---|---|
| エンドポイント | 検出した脅威 | % |
| 該当なし | 該当なし | 該当なし |

| Webレピュテーション違反のあったエンドポイント の上位10件 | | |
|---|---|---|
| エンドポイント | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| 挙動監視違反のあったプログラムの上位5件 | | |
|---|---|---|
| プログラム | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| 挙動監視違反のあったエンドポイント の上位10件 | | |
|---|---|---|
| エンドポイント | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| デバイスコントロール違反のあったプログラムの上位5件 | | |
|---|---|---|
| プログラム | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| デバイスコントロール違反のあったエンドポイント の上位10件 | | |
|---|---|---|
| エンドポイント | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

| URLフィルタ違反のあったカテゴリ 上位5件 | | |
|---|---|---|
| URLカテゴリ | 検索頻度 | % |
| 該当なし | 該当なし | 該当なし |

図 62：エンドポイント月次レポート例 4/4

Cloud Edge Cloud Console

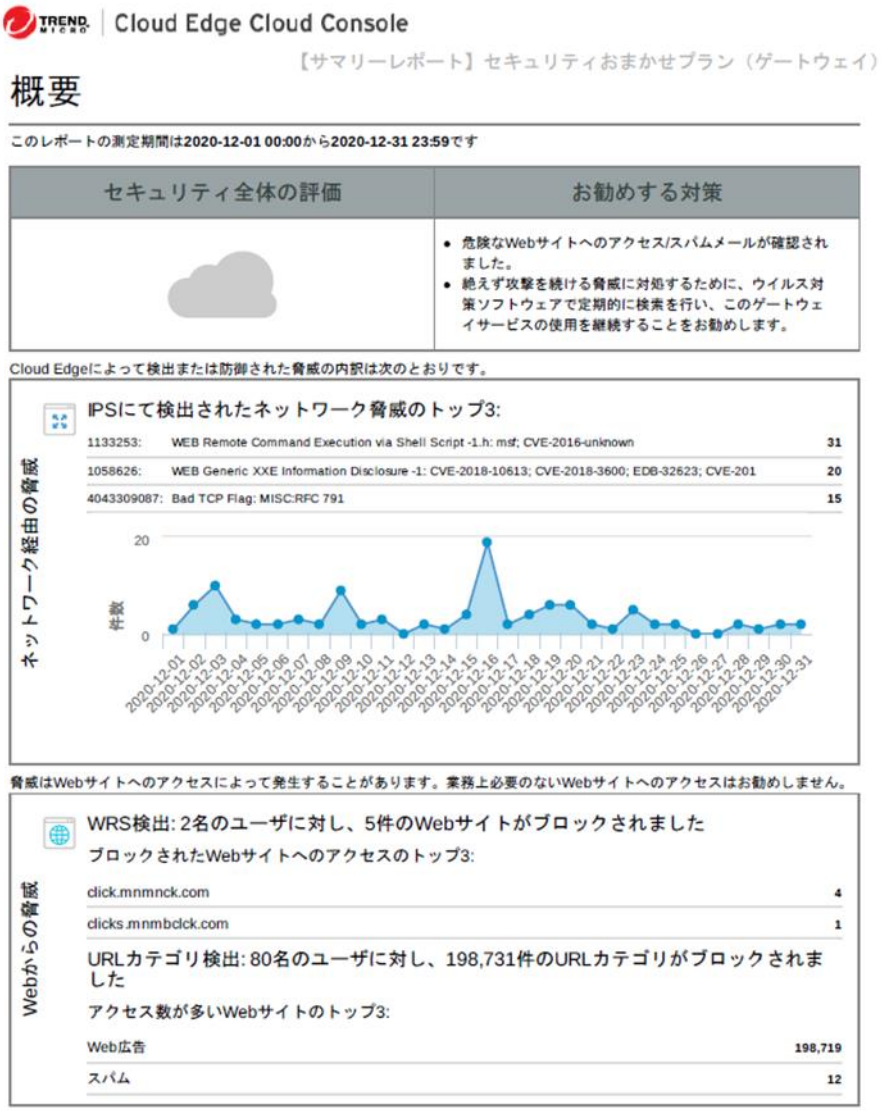
【サマリーレポート】セキュリティおまかせプラン（ゲートウェイ）

# 【サマリーレポート】セキュリティおまかせプラン（ゲートウェイ）

生成者: ACT_kaitsu
生成日: 2021-01-01 06:09
レポート期間: 過去1か月間 (2020-12-01 00:00 - 2020-12-31 23:59)

概要 2

図 63：UTM サマリーレポート例 1/3



Cloud Edge Cloud Console

【サマリーレポート】セキュリティおまかせプラン（ゲートウェイ）

## 概要

このレポートの測定期間は2020-12-01 00:00から2020-12-31 23:59です

| セキュリティ全体の評価 | お勧めする対策 |
| --- | --- |
| | • 危険なWebサイトへのアクセス/スパムメールが確認されました。<br>• 絶えず攻撃を続ける脅威に対処するために、ウイルス対策ソフトウェアで定期的に検索を行い、このゲートウェイサービスの使用を継続することをお勧めします。 |

Cloud Edgeによって検出または防御された脅威の内訳は次のとおりです。

ネットワーク経由の脅威

IPSにて検出されたネットワーク脅威のトップ3:

| | | |
| --- | --- | --- |
| 1133253: | WEB Remote Command Execution via Shell Script -1.h: msf; CVE-2016-unknown | 31 |
| 1058626: | WEB Generic XXE Information Disclosure -1: CVE-2018-10613; CVE-2018-3600; EDB-32623; CVE-201 | 20 |
| 4043309087: | Bad TCP Flag: MISC:RFC 791 | 15 |



脅威はWebサイトへのアクセスによって発生することがあります。業務上必要のないWebサイトへのアクセスはお勧めしません。

Webからの脅威

WRS検出: 2名のユーザに対し、5件のWebサイトがブロックされました

ブロックされたWebサイトへのアクセスのトップ3:

| | |
| --- | --- |
| click.mnmnck.com | 4 |
| clicks.mnmbclck.com | 1 |

URLカテゴリ検出: 80名のユーザに対し、198,731件のURLカテゴリがブロックされました

アクセス数が多いWebサイトのトップ3:

| | |
| --- | --- |
| Web広告 | 198,719 |
| スパム | 12 |

図 64：UTM サマリーレポート例 2/3

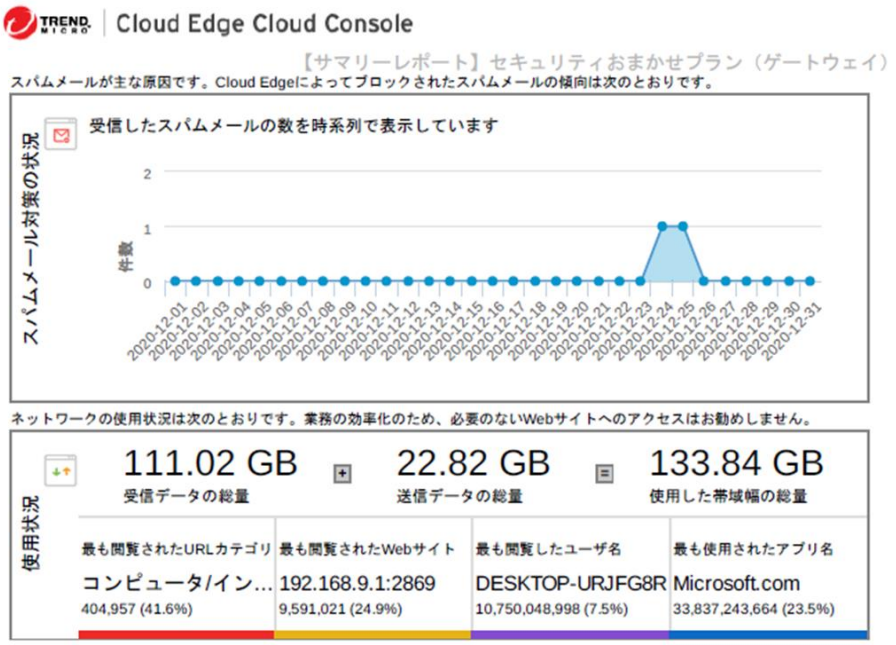



図 65：UTM サマリーレポート例 3/3

## 3.7. 実証参加企業への実証事業終了時アンケート結果

本章では、実証事業の終了時のアンケート調査結果を報告する。

脅威検知レポートについて、「満足」「やや満足」が 57%で半数以上が満足と回答した。
特に役立った内容として「インターネットセキュリティ」「セキュリティ全体の評価」「ウイルス/不正プログラムの概要」が上位に挙がっている。

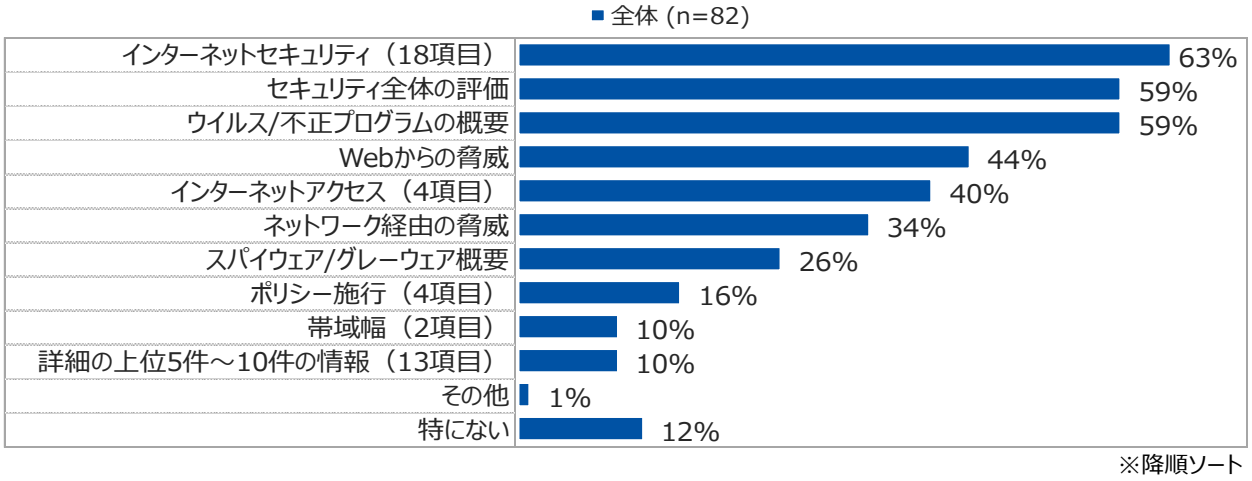



図 66：脅威検知レポートの役立った内容

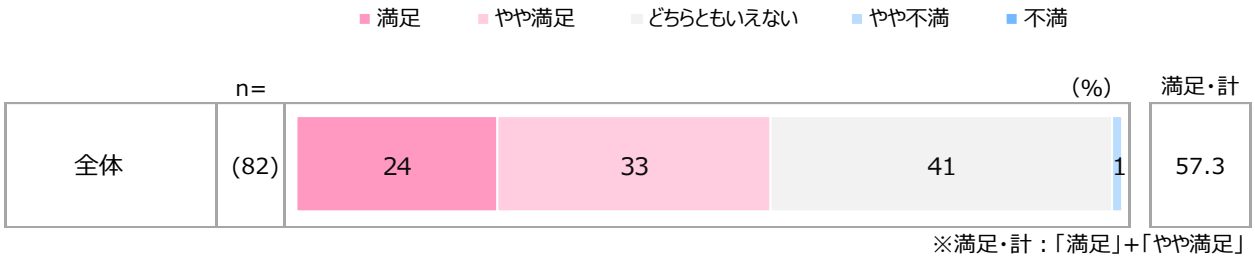



図 67：脅威検知レポートの評価

本実証事業で効果を感じたこととして「悪意のあるメールの外部からの遮断」「脅威検知内容のレポート報告」が上位で、ともに実証参加企業の 4 割以上が効果を感じている。

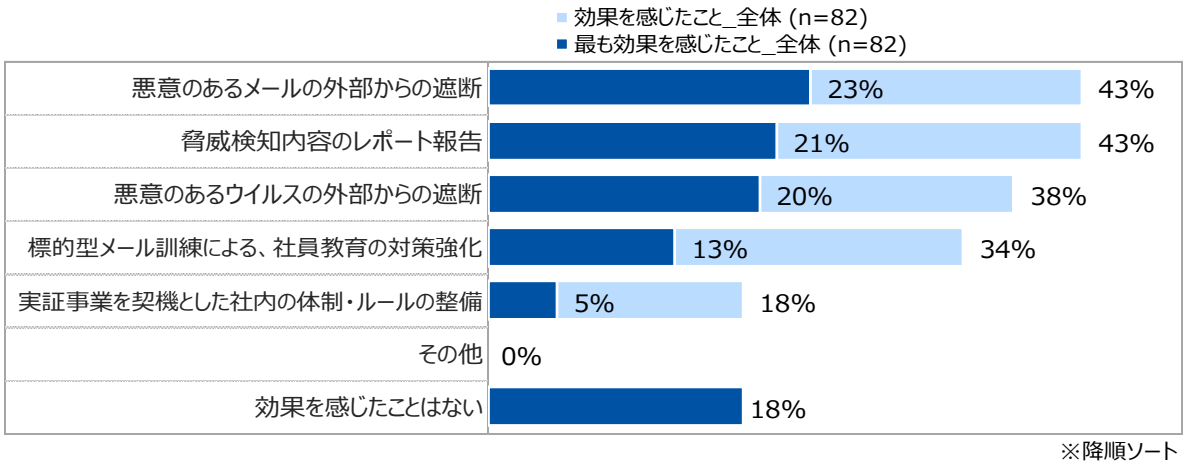



図 68：本実証事業で効果を感じたこと

サイバーリスクに関する課題感として、実証事業終了後では「インシデント発生時の体制の構築」「セキュリティ予算の確保」が上位に挙がっており、インシデント発生時の対応や、予算確保といった具体的な動きについて関心が高まっている。

サイバー攻撃に対するリスクについては、「あると思う」が 73%である。

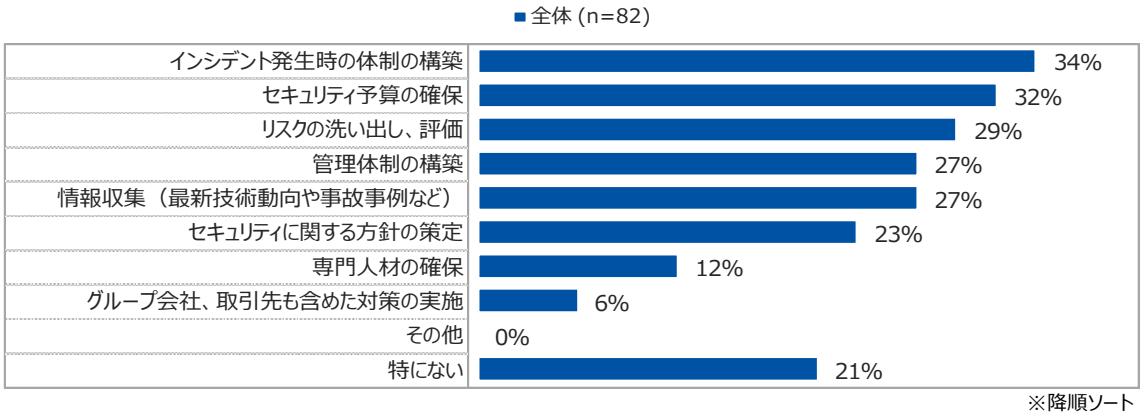



図 69：サイバーリスクに関する課題：事後（複数回答）

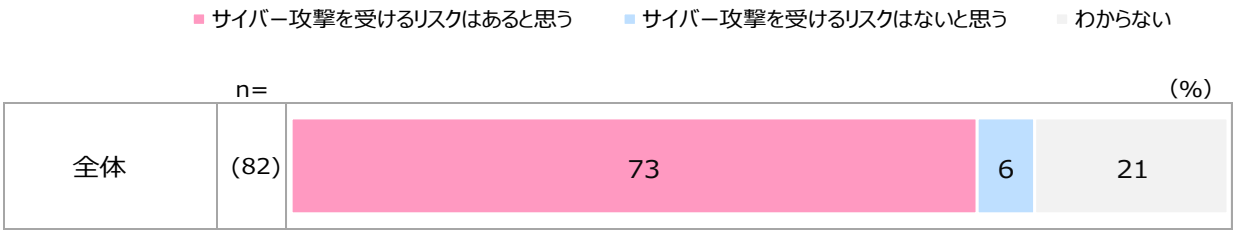



図 70：サイバー攻撃を受けるリスクがあると思うか：事後

今後用意したいサイバーセキュリティ対策の年間予算については「12 万円未満（月額 1 万円未満）」が 46%で最も高く、次いで「～24 万円未満（月額～2 万円未満）」が続いている。「全くかけない」は 16%にとどまり、低予算でも費用をかけて対策したいと考えている企業が多くなっている。

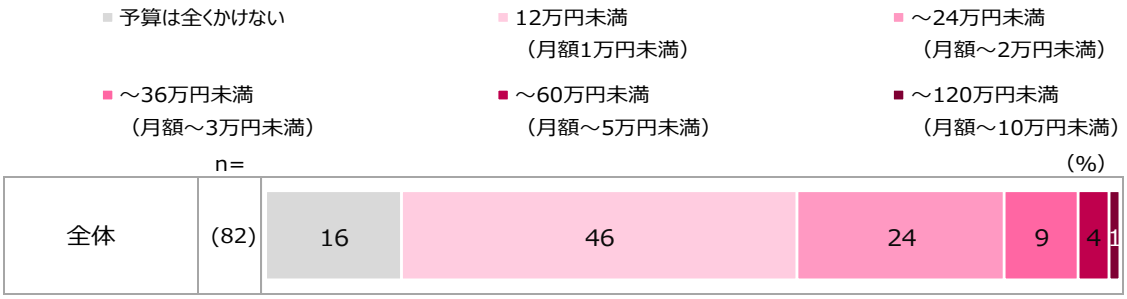
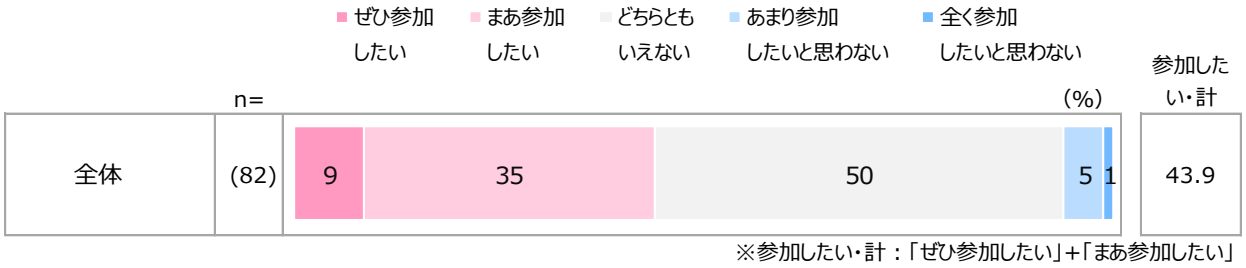



図 71：今後のサイバーセキュリティ対策予算

今後、同様の実証事業を行った場合に参加したいかについては「ぜひ参加したい」「まあ参加したい」を合わせて 4 割以上がリピート参加を希望している。

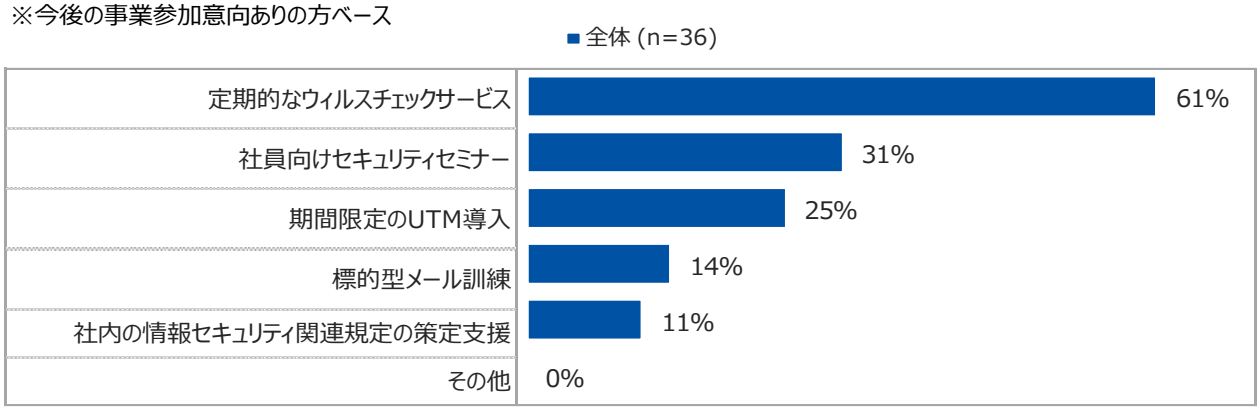
その際に期待する内容としては「定期的なウイルスチェックサービス」が突出して高く、次いで「社員向けセキュリティセミナー」「期間限定の UTM 導入」が挙げられている。




※参加したい・計：「ぜひ参加したい」+「まあ参加したい」

図 72：今後の実証事業参加意向

※今後の事業参加意向ありの方ベース




※降順ソート

図 73：今後の実証事業で希望する内容

今回の実証事業で提供したサービスを、実証事業終了後も継続して利用を希望する意向は 18%であった。なお、最終的な個社別のサービス継続意向確認では、アンケートで「分からない／決まっていない」と回答した企業からも継続意向を確認できたため、53 社が有償でのサービス利用継続を決めた。

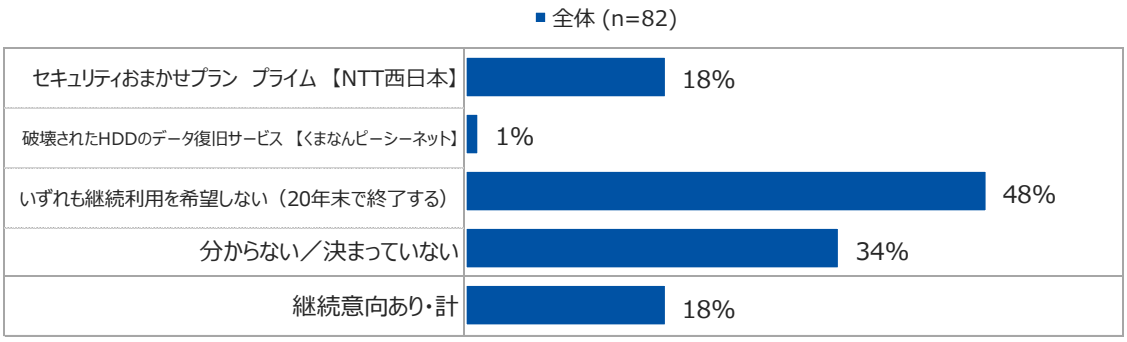



図 74：継続して利用したいサービス

### 3.8. サイバーセキュリティに関する相談の受付および対応結果

実証事業に関する問合せなどをコールセンターで受け付けた。実証事業への参加を検討するための情報収集の連絡を 22 件受付けており、そのうち 5 件が実証事業に参加した。

インシデント対応として電話およびリモート対応を実施するのは次の 3 つの場合である。

1）C&C コールバック検出数の超過した場合

※C&C サーバー （Command and Control server）：ボットネットに指令を送るサーバーとの不正通信の検出

2）オフライン UTM が一定期間（24 時間）以上検出された場合

3）ウイルス対策において自動解決ができない場合

実証事業においては、UTM が一定期間オフラインであることを検知した場合にセンターから電話連絡して UTM の使用を正常状態に戻す支援を行うことを 3 件実施している。

その他のインシデント対応については、実証事業においては発生しなかった。

| 対応種別 | 総計 | 相談・インシデント等対応状況 | 発生件数 |
|---|---|---|---|
| コールセンター対応 | 22件 | 実証参加に関する問合せ | 22件 |
| | | セキュリティ機器設置等の問合せ | 0件 |
| | | セキュリティ対応の相談 | 0件 |
| | | その他 | 0件 |
| インシデント対応 | 3件 | 電話及びリモートによるインシデント対応 | 3件 |
| | | 訪問によるインシデント対応（駆付け） | 0件 |
| その他訪問対応 | 105件 | 機器設置等のトラブル対応 | 0件 |
| | | その他（セキュリティ機器の導入・設置支援等） | 105件 |

図 75：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

### 3.9. 実証事業報告会実証事業報告会

実証事業報告会を 1 回実施した。当初、実証事業報告会の実施は NTT 西日本熊本支店において集合開催を予定していたが、新型コロナ対策緊急事態宣言（熊本県独自を含む）の影響下であったため、IPA SECURITY ACTION セミナーとの共同開催によるオンラインの実証事業報告会とした。

| | |
|---|---|
| 開催日時 | 2021 年 1 月 15 日（金）　14:00　～　16:40 |
| 場所、形態 | オンラインセミナー |
| 参加者数 | 31 社（31 名） |
| アジェンダ | ① 広がるテレワーク環境とセキュリティ対策の強化～最近のサイバーセキュリティ攻撃の動向～（トレンドマイクロ（株））<br>② セキュリティ被害状況とサイバーリスク保険について（東京海上日動火災保険（株）　熊本支店）<br>③ 中小企業向け情報セキュリティ対策支援事業のご紹介（IPA）<br>④ 熊本サイバーセキュリティお助け隊 活動結果報告（熊本サイバーセキュリティお助け隊 事務局（NTT 西日本 熊本支店））<br>⑤ 中小企業のための情報セキュリティセミナー （有限会社 Biz Assist（ビズアシスト）） |

報告会実施後に実施したアンケートにおいて、「取引先からセキュリティ対策を要求されたことがある」企業は半数あり、取引条件としてのセキュリティ対策の必要性が浸透していることが分かる。

また、実証事業報告会への参加目的を確認したところ、「自社のセキュリティ対策向上のため」と回答した企業が 33%あり、「自身の知識向上のため」と合わせると 75%が情報セキュリティの情報収集のために参加していた。

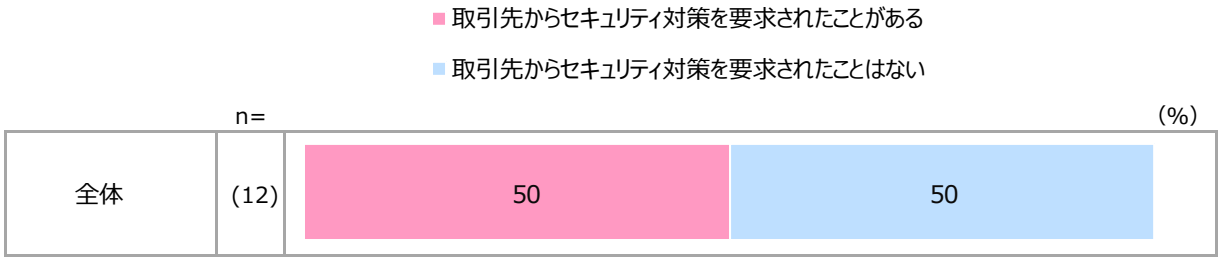



図 76：取引先からのセキュリティ対策の要求

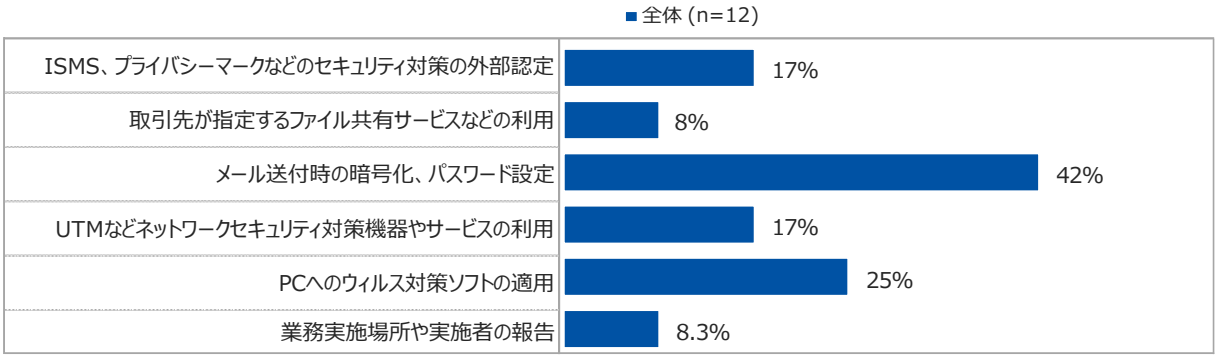



図 77：要求されたセキュリティ対策の内容

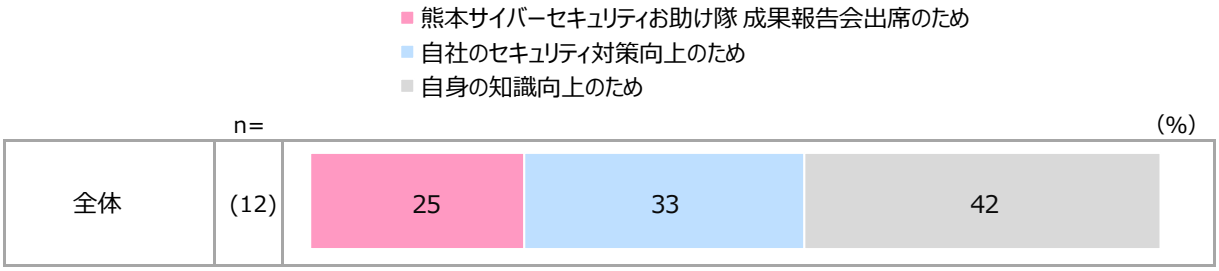



図 78：実証事業報告会への参加目的

# 4. 分析・考察

## 4.1. 実証参加企業におけるサイバー攻撃の実態

### 4.1.1. セキュリティ対策機器（UTM）によるサイバー攻撃防御の状況

スパイウェアの駆除/無効化および WRS ブロックは、実証参加企業数が増えた 10 月からは毎月発生した。WRS ブロックとは、Web レピュテーションサービス （WRS） により、危険な可能性のある Web サイトにユーザーがアクセスする前に URL を調べ、危険があると判断した場合にアクセルをブロックすることである。

代表的なウイルスとしては、EMOTED によると考えられる Trojan が検出された。

また、ADW/PUA といった、フリーソフトウェアなどにバンドルされ、同時にダウンロード/インストールされている可能性が高いグレイウェアも検出されている。

WRS では偽の通販サイト、詐欺サイト、フィッシングサイトなどへのアクセスをブロックしており、実証参加企業の社員教育が必要と考えられる。

なお、実証事業期間中に検出されたインシデントはシステムで自動対応できており、駆付け対応は発生しなかった。

| | | | 9月 | | 10月 | | 11月 | | 12月 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 利用社数（社） | 1 | | 43 | | 100 | | 105 | |
| | | | | % | | % | | % | | % |
| エンドポイント | ウィルス/不正プログラム 駆除/無効化 | 件数(件) | 0 | | 43 | | 0 | | 0 | |
| | | 台数(台) | 0 | | 4 | | 0 | | 0 | |
| | | 社数(社) | 0 | 0% | 3 | 7% | 0 | 0% | 0 | 0% |
| | スパイウェア 駆除/無効化 | 件数(件) | 0 | | 25 | | 8 | | 17 | |
| | | 台数(台) | 0 | | 3 | | 3 | | 4 | |
| | | 社数(社) | 0 | 0% | 3 | 7% | 3 | 3% | 3 | 3% |
| クラウドエッジ サマリーレポート | WRSブロック | 件数(件) | 0 | | 15 | | 88 | | 195 | |
| | | 台数(台) | 0 | | 8 | | 24 | | 46 | |
| | | 社数(社) | 0 | 0% | 6 | 14% | 17 | 17% | 29 | 28% |
| | その他の脅威 ブロック | 件数(件) | 0 | | 4 | | 21 | | 36 | |
| | | 社数(社) | 0 | 0% | 3 | 7% | 5 | 5% | 9 | 9% |

図 79：UTM およびエンドポイントによる防御件数

## 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. セキュリティ対策実施に向けた外部からのアプローチの増強

実証事業に参加した中小企業の 9 割以上は、熊本サイバーセキュリティお助け隊実行委員会に属する企業の既存顧客リストから集中的にアプローチして実証事業への参加を促した。実証事業を紹介する Web ページや広報をきっかけに中小企業が自らセキュリティ対策の導入を決めるケースは実証事業においても少ない結果となった。

よって、中小企業のセキュリティ対策実施には、地域 IT ベンダー等が積極的に営業活動を行うことが不可欠であると考えられる。多くの地域 IT ベンダー等が中小企業に対してセキュリティ対策サービスの提供や販売を行うことで、対策を行う中小企業を増やすことが可能となるため、地域の中小企業を営業対象とする企業がセキュリティ対策サービスの普及を目的とした協力体制を築くことが効果的と考えられる。

## 4.3. 中小企業において必要なセキュリティ対策

### 4.3.1. 標的型攻撃メール訓練による社員のセキュリティ意識の実態

システムによるハード面のセキュリティ対策と合わせて、体制や社員のセキュリティ意識などソフト面のセキュリティ対策を進める事が重要であるが、標的型攻撃メール訓練の実施において、社員教育とセキュリティ体制の 2 つのポイントに課題があることが明らかになった。

社員教育について、標的型攻撃メール訓練を実施するにあたり、事前に社員に対して、社員が不審なメールを受信した際の望ましい行動を示しておくことが社員のセキュリティ意識向上に効果的である。しかしながら、アンケート結果で示したとおり標的型攻撃メール訓練を実施する前後で社員に対してセキュリティ研修を行っていない企業が約 80%であった。

これは、事前アンケートで確認した社員のセキュリティ意識を向上するための啓発活動を「特に行っていない」と回答した企業が 63%あったこととも連動しており、中小企業に対してこれまでと同じ取組姿勢では、社員のセキュリティ意識向上のための啓発活動を増やすことが困難であることを示していると考えられる。

セキュリティ体制について、標的型攻撃メール訓練を組織的に実施することができたかを分析することで有効性を確認できる。実証事業期間内に社内の担当者が経営者もしくはセキュリティ責任者の合意を得て訓練メール送信を行ったと考えられる企業数は 13 社であった。訓練メールを送信した 60 社のうち、47 社は 1 通のみの送信であった。一部ヒアリングを行ったところ、実証事業として攻撃型メール訓練の利用を促したものの、実証事業期間内では訓練実施の準備を実施できなかったため、1 通だけ試しに送信した状態であると考えられる、

また、今後の訓練の実施意向について、訓練は一度でよいと思っている層も 3 割以上存在し、訓練を繰り返し行う必要性が十分に伝わっていない。

今後は、訓練を継続して実施することや、訓練と合わせて研修を実施することで訓練の効果を高めることも含めて、標的型攻撃メール訓練の意義を中小企業に伝えていくことが課題となる。

中小企業においては、情報セキュリティに関する体制が整理されておらず、社員教育等のセキュリティ意識向上に課題があることが明らかになった。

| 実証事業参加企業数（社） | 訓練メール送信企業数（社） | 訓練メール送信数が 2 以上の企業数（社） |
|---|---|---|
| 105 | 60 | 13 |

**図 80：標的型攻撃メール訓練実施企業数**

## 4.4. 中小企業におけるセキュリティ対策の効果

### 4.4.1. 実証事業期間中のサイバーセキュリティ脅威が企業に及ぼす影響

実証事業期間中において、実証参加企業にはシステムによるハード面のセキュリティ対策としてネットワークに UTM を設置し、業務用パソコンにエンドポイントセキュリティツールを設定した。また、体制や社員のセキュリティ意識などソフト面のセキュリティ対策を促進するため。標的型攻撃メール訓練を実施した。

さらに、インシデント発生時の対応をサポートする体制として、遠隔サポート体制と派遣サポート体制を準備した。

ICT 実態アンケート調査の結果から、メールを介した攻撃や、サプライチェーンの弱点を悪用した攻撃といったセキュリティ脅威を経験している企業は多く、中小企業におけるサイバーセキュリティ強化の取り組みは喫緊の課題である。

しかし、現在導入されているセキュリティ対策はウイルス対策ソフトが中心となっており、PC・OS・アプリ更新管理の徹底、社員向け研修の実施、可搬媒体を使った外部へのデータ持ち出し禁止といった、基本的な対策すら取られていない企業が多いのが実情である。

実証事業参加前の事前アンケートでは、セキュリティ対策における費用に加え、「何を導入すればいいか判断がつかない」という悩みが大きく、導入を判断するためのリテラシー不足や、セキュリティ対策に関する情報源、相談できる窓口が不足している状況が推察された。

今回の実証事業を経て、実証参加企業の意識の変化が見られたポイントを 3 点挙げる。

・サイバーリスクに対する課題の具体化
実証事業実施前の時点では、サイバーリスクの課題として「セキュリティに関する方針の策定」「管理体制の構築」など、全体的な方針・体制を整えることに課題感を持っていた企業が多いのに対し、実証事業終了後では「インシデント発生時の体制の構築」「セキュリティ予算の確保」など具体的な対策への関心が高まった。

・UTM の認知、導入意向の向上
実証事業実施前には、セキュリティ対策はウイルス対策ソフト中心であり、UTM を未認知／未検討の層が大半であった。
実証事業終了後のアンケートでは「悪意のあるメールの外部からの遮断」を始めとした UTM の効果が評価され、「脅威検知レポート」に対する満足度も高く、外部脅威を入口でブロックする UTM の重要性の理解が進んだと言える。実際に、実証事業終了後にも UTM の継続利用を希望する企業も存在しており、企業のセキュリティレベル向上への寄与が期待できる。

・サイバーセキュリティ対策に対する許容コストの拡大
サイバーセキュリティ対策の年間予算「なし」の層が、実証事業実施前では 38%に対し、実証事業終了後は 16%まで縮小した。
実証事業終了後では年間～24 万円までが 70%をしめる年間予算のボリュームゾーンとなっており、低予算であっても費用をかけて対策したいと考える企業が増加したと言える。
実証事業参加のきっかけとして、無料でハードル低くセキュリティ対策を試せることが大きな要因となっていたが、本実証事業を活用して実際に利用して効果を実感できたことが、許容コストの拡大に繋がったと考えられる。

# 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

実証事業のアンケートを通じて、実証参加企業の約 7 割の企業が実際にサイバー攻撃を受けるリスクがあると思うと回答し、また約 8 割がサイバーリスクに関して何らかの課題を認識していることが分かった。

本実証事業に参加した企業は、県内他企業と比べても比較的サイバーセキュリティに対する意識レベルが高い母集団であることが推察されるが、セキュリティ対策に大きなリソースを投下している大企業であってもサイバー攻撃の被害を 100%回避することが不可能であることを考えると、サイバー攻撃のリスクを感じている企業が未だ 6 割程度というのはまだまだ正しいリスク認識が浸透していない結果であると考える。

一方、東京海上日動火災保険（株）におけるサイバーリスク関連保険の普及率は、既往 1 年間で約 20%増と、全国的には認知が広がっていると考えられるものの、首都圏の企業が牽引しており、熊本県において現時点では普及率はほぼ横ばいである。県内企業におけるサイバーリスクに対する認知度がまだ低いことが原因の一つと考えられ、損害保険会社の持つ代理店ネットワーク等を活用しながら、サイバーリスクに対する県内企業の認識を高めてゆく必要があると考える。

本実証事業を通して、まずは実証事業に参加した各企業に対し、改めて東京海上日動火災保険（株）の保険代理店を通して、サイバーリスクに対する経済的な備えの一環として、サイバーリスク保険を広く案内してゆく。

なお、実証事業後のアンケートにおいて、サイバーセキュリティ対策にかけても良いと考える予算については、約半数の企業が 12 万円未満、25%弱の企業が 12～24 万円未満と回答している。東京海上日動火災保険（株）の提供するサイバーリスク関連の保険商品は、中堅規模以上の企業を対象とした「サイバーリスク保険」と、中小企業を対象とした「超ビジネス保険（サイバー補償）」に大別されるが、前述アンケート結果を鑑みると、より安価な保険料で加入が可能な「超ビジネス保険」を中心に案内をしていくことで、県内企業へより広くリスクヘッジ策を展開することに繋がると考える。「超ビジネス保険」は商工会議所等商工団体の会員向けに保険料割引制度を適用しており、商工団体が推進する県内企業向け BCP（Business Continuity Plan＝事業継続計画）策定支援において、サイバーリスクを事業継続上のリスクシナリオとして含むことを検討する。

最後に、自動車保険や火災保険のように、リスクがイメージしやすく保険加入が進んでいる分野と比較しても、サイバーリスクは目に見えず、今回の実証事業に参加した企業ですら十分にリスク認識が出来ているとは言い難い現状を鑑みると、前述のような保険代理店ネットワークを活用した個別の展開ではスピード感に課題があると考える。サイバーリスク保険の認知度を飛躍的に高め、県内企業のサイバーリスクへの対策に寄与するためには、サイバー関連商品・サービスへ保険をバンドルさせ、商品・サービス購入者全員に対して補償を提供する等の方法も検討していく。

## 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

実証参加企業の 105 社のうち、53 社は既にビジネス化している NTT 西日本のセキュリティサービス（セキュリティおまかせプラン　プライム : 月額 16,500 円～）を有償で継続利用する意向を得た。実証事業への参加理由として「無料期間中だけでも利用してみたかったから」、「試験的に運用してみて、効果があれば今後導入したいから」と回答した企業が約半数であったことを鑑みると、多くの企業にセキュリティ対策に必要性を実感し、継続利用の意思表示を得られたと考えている。

しかしながら、実証参加企業の約半数では、本実証事業終了後は本対策を継続しないとの結果となっており、更なるサイバーセキュリティ対策を推進する必要がある。

実証事業で使用したサービスを継続利用しない理由としては、次の理由が考えられる。

・導入の必要性に納得していない。
・費用対コストに納得していない
・サービス提供者に納得していない

実証事業終了時アンケート結果からも、「サイバー攻撃を受けるリスクがあると思うか」という設問に対して「サイバー攻撃を受けるリスクはないと思う」と「わからない」の合計が 27%存在する。セキュリティ対策の必要性を啓発する活動はこれからも必要である。

また、「今後のサイバーセキュリティ対策予算」について、46%は年間 120,000 円未満を回答しており、実証事業で使用したサービス（年間 198,000 円～）よりも低額のコストを希望している。

サービス提供者に関しては、実証事業なので今回はサービス提供者にこだわらずに使用したが、情報システムは他に相談したい事業者が存在するなど、他のサービスと比較検討したいという意見もあり、実証事業で使用したサービスの継続利用は見送っている。

セキュリティサービスは安価であれば利用されるといった簡単なものではないことは、無償でサービスを利用できる実証参加企業を募集することが安易にはいかなかったことからも明らかであるため、既にビジネス化しているサービスの低廉版を検討するだけでなく、熊本県内の中小企業へのサイバーセキュリティ対策の啓発活動や関連サービスの提供、事後対応などについて、その分野の専門企業が連携して提供することをさらに検討していく。

本実証事業の推進にあたって結成した「熊本サイバーセキュリティお助け隊」の委員会およびタスクフォースを原型として、（一社）熊本県サイバーセキュリティ推進協議会の部会として存続させることも含めて検討を進める。本実証事業でサービス提供を担当した企業だけでなく、熊本県内の ICT 関連企業全体で、中小企業の ICT 促進とサイバーセキュリティ対策に必要なサービスを準備していくことで、前述のサイバーセキュリティ「超ビジネス保険」による補償範囲とも組み合わせて、中小企業がより自社に適したサービスを利用できるようにしていく。

また、今回実証事業報告会を IPA の SECURITY ACTION 啓発セミナーと同時開催としたように、お助け隊実証事業の枠組みだけでなく、IPA の SECURITY ACTION も組み合わせ、中小企業のセキュリティ体制整備も合わせて啓発していくことで、適切に運用されるセキュリティ対策の浸透を中小企業に対して進めていく。

以上