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

中小企業向けサイバーセキュリティ事後対応支援実証事業（地域名：新潟県）

成果報告書

請負事業者：東日本電信電話株式会社

目次

1. サマリー

本報告書は、東日本電信電話株式会社（以下「NTT 東日本」という。）が「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」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。

新潟県内の中小企業 148 社を対象に、セキュリティ診断、アンケート、UTM 通信ログ、一元対応窓口への問合せ、標的型攻撃メール訓練の結果から、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。

＜実証の結果に基づく新潟県内の中小企業の傾向＞

- サイバーリスクの脅威や事業に及ぼす影響についての知識に乏しい。
- システム管理者やシステム専任担当が不在であることが多い。
- セキュリティ機器（UTM）の設置には提供側のサポートが不可欠。
- どの企業も漏れなく不正アクセス攻撃を受けている。
- 本実証事業がきっかけとなり、参加企業の約半数が、UTM を本格導入（継続利用）となった。

＜中小企業の課題＞

- サイバーリスクとサイバーセキュリティ対策の全体像を理解すること。
- 事業への影響、サプライチェーンへの影響を考慮し、計画的なリスク対策に取り組むこと。

＜中小企業のサイバーセキュリティ対策＞

- 中小企業の ICT 環境や業務環境を把握している第三者が、事前事後を含めたサイバーセキュリティ全体についてのアドバイスを行うなど外部のサポートが必要であり、セキュリティ機器単体ではなく総合的なサイバーリスク対策のサポートを提供する必要がある。

2. サイバーセキュリティ対策の現状

近年、IoT や AI、ビッグデータなどの台頭により新しい価値を創造するようなビジネスイノベーションやデジタルトランスフォーメーションが注目されている。

企業の規模に関わらず、企業内部・外部に対するサイバーセキュリティに取り組むことが重要であり、取り組みを進める上では経営層のサイバーセキュリティ知識や能力の向上が重要となっている。

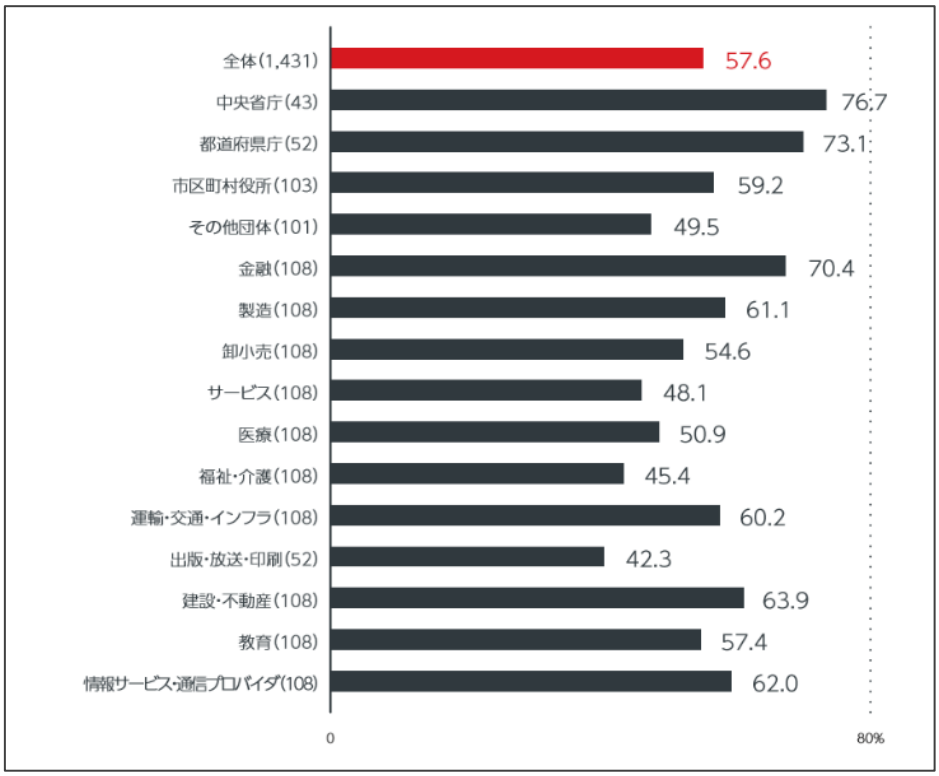
＜セキュリティインシデントによる被害状況＞

トレンドマイクロ株式会社（以下「トレンドマイクロ」という。）の「法人組織におけるセキュリティ実態調査 2019 年版」によればセキュリティインシデントを経験した割合は 57.6%となり、半数以上がインシデントを経験している深刻な状況となっている。

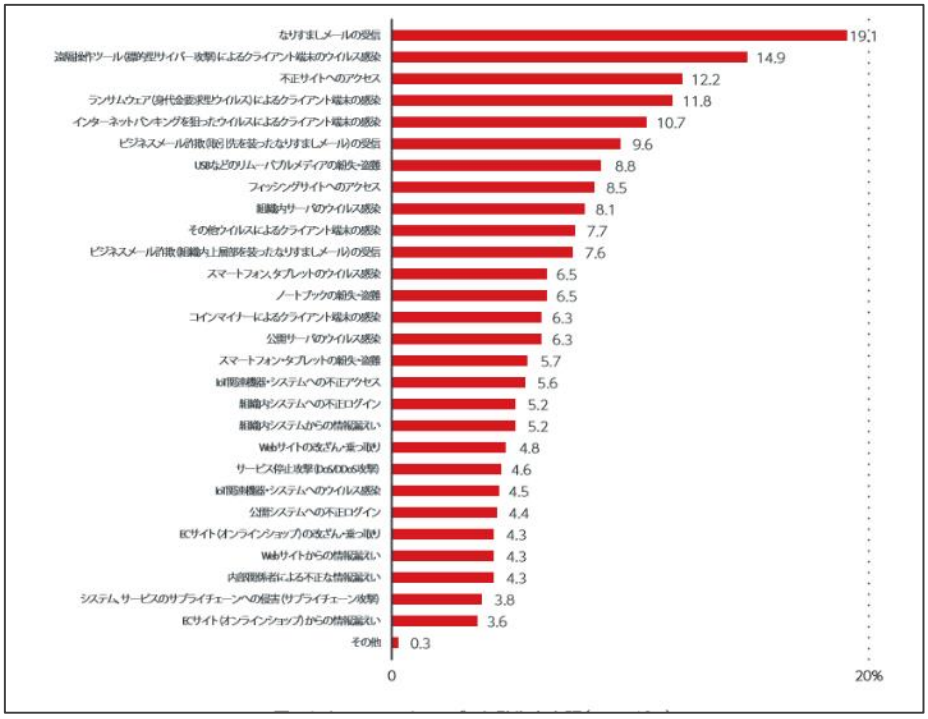
セキュリティインシデント発生率が最も高かったのは「なりすましメールの受信」で 19.1%、次いで「遠隔操作ツールによるクライアント端末のウイルス感染」が 14.9%で続いている。その中でも、重大被害による年間平均被害総額は約 2.4 億円となっており、4 年連続 2 億円を超える結果となっている。

中小規模の組織でも年間平均被害総額は 1 億円を超えており、セキュリティインシデントはこうした組織の事業継続にも大きな影響を与える深刻なリスクとなっている。

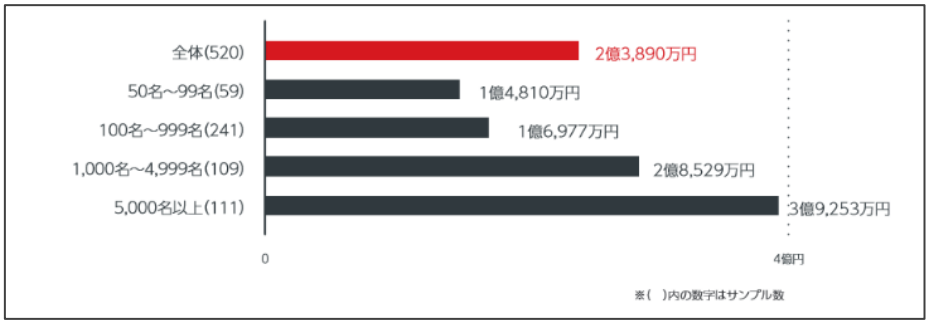
【図 1】セキュリティインシデント発生率（業種別）



【図 2】セキュリティインシデント発生率内訳



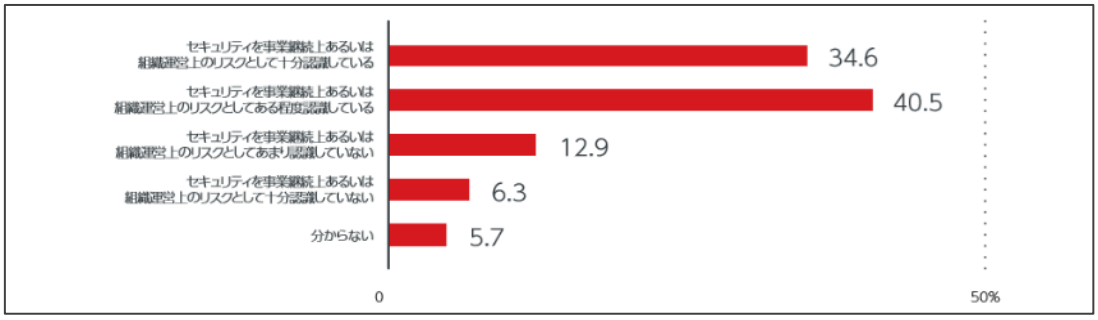
【図 3】重大被害による年間平均被害額（規模別）



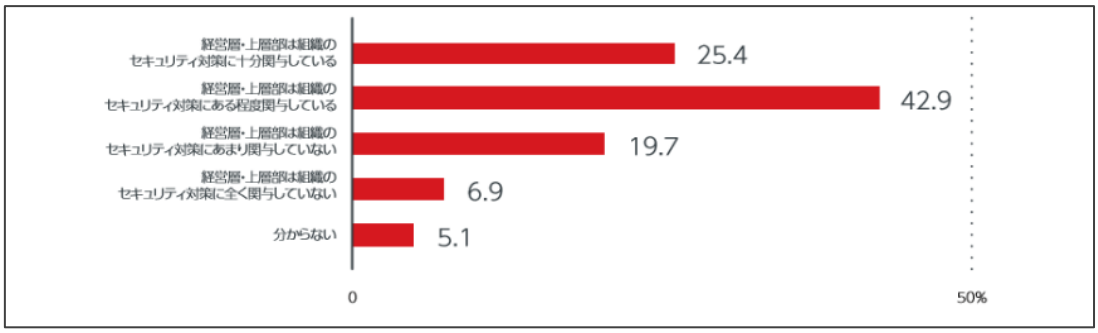
＜情報セキュリティに関する経営層のリスク認識および関与度＞

法人組織における情報セキュリティに関する経営層・上層部のリスク認識については「セキュリティを事業継続上あるいは組織運営上のリスクとして十分認識している」と回答した割合は、34.6%、セキュリティに十分関与している経営層・上層部の割合は 25.4%に留まり、未だ多くの法人組織で十分な関与がない状況となっている。

【図 4】情報セキュリティに関する経営層・上層部のリスク認識



【図 5】情報セキュリティに関する経営層・上層部の関与度



規模別で見た場合には、組織規模に比例して、経営層・上層部における「セキュリティを事業継続上あるいは組織運営上のリスクとして十分認識している」割合は増加している。5,000 名以上の組織の割合は、99 名以下の組織の割合の約 2.7 倍となっており、大きく差がついていることが明らかとなった。

【図 6】セキュリティに関する経営層・上層部のリスク認識（規模別）

経営層・上層部のリスク認識	全体 (1,431)	50名～99名 (254)	100名～999名 (707)	1,000名～4,999名 (251)	5,000名以上 (219)
セキュリティを事業継続上あるいは組織運営上のリスクとして十分認識している	34.6	20.5	30.6	41.8	55.7
セキュリティを事業継続上あるいは組織運営上のリスクとしてある程度認識している	40.5	45.7	41.7	40.6	30.1
セキュリティを事業継続上あるいは組織運営上のリスクとしてあまり認識していない	12.9	17.7	14.1	8.8	8.2
セキュリティを事業継続上あるいは組織運営上のリスクとして十分認識していない	6.3	7.5	7.1	5.6	3.2
分からない	5.7	8.7	6.5	3.2	2.7

※単位は%、( )内の数字はサンプル数

図36:セキュリティに関する経営層・上層部のリスク認識(規模別) 低 高

セキュリティ対策への経営層・上層部の関与度を見た場合でも、リスク認識と同様の傾向が見られており、経営層・上層部がセキュリティ対策に十分に関与している割合は 5,000 名以上の組織が 99 名以下の組織の約 2.3 倍となっている。
このことから、中小規模の組織では、経営層・上層部のセキュリティに対する意識の大きな変化が求められていると考えられる。

【図 7】セキュリティ対策への経営層・上層部の関与度（規模別）

経営層・上層部の関与度	全体 (1,431)	50名～99名 (254)	100名～999名 (707)	1,000名～4,999名 (251)	5,000名以上 (219)
経営層・上層部は組織のセキュリティ対策に十分関与している	25.4	17.7	21.2	31.5	40.6
経営層・上層部は組織のセキュリティ対策にある程度関与している	42.9	45.7	42.7	42.6	40.6
経営層・上層部は組織のセキュリティ対策にあまり関与していない	19.7	19.3	22.2	19.1	12.8
経営層・上層部は組織のセキュリティ対策に全く関与していない	6.9	11.0	7.5	4.8	2.7
分からない	5.1	6.3	6.4	2.0	3.2

※単位は%、( )内の数字はサンプル数

低 高

出典（図 1～7）：トレンドマイクロ「法人組織におけるセキュリティ実態調査 2019 年版」

3. 実証事業概要

(1) 実証の概要

アンケートによる企業のサイバーセキュリティ対策の実態把握

セキュリティ対策機器によるサイバー攻撃の状況及び相談内容等の実態把握

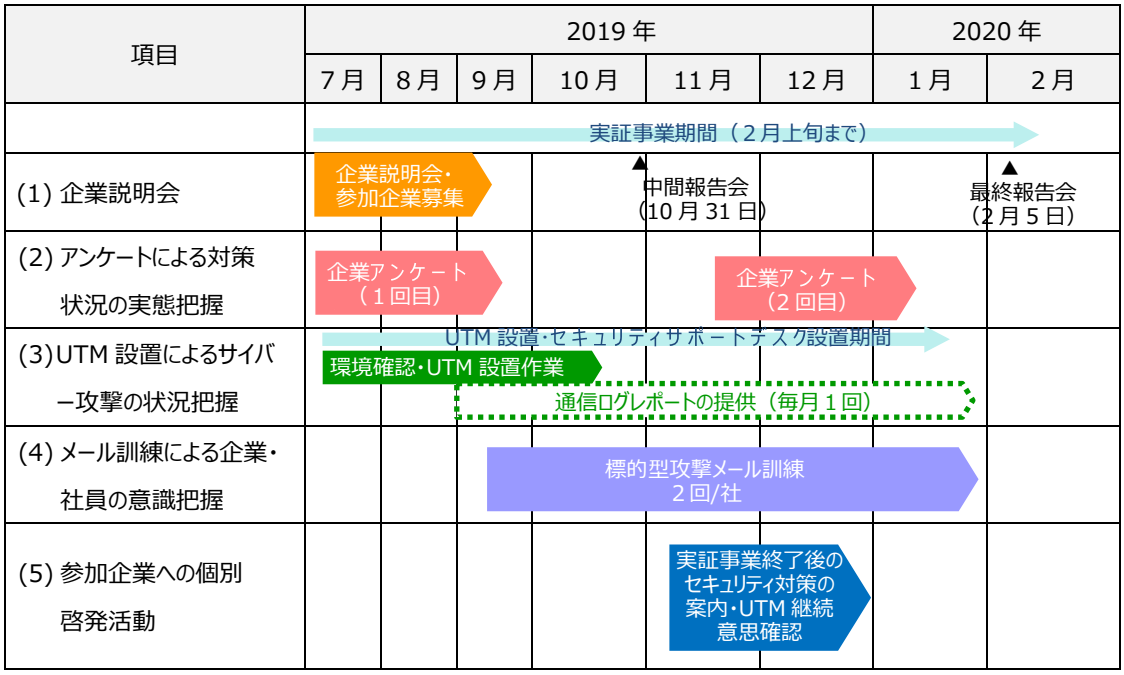
「標的型攻撃メール訓練」による企業・社員のサイバーセキュリティ意識把握

(2) 実証の目的

中小企業が継続して利用可能なサービスの提供を実現するための、サービスおよび保険商品の組成を検討すること。

(3) スケジュール

【図 8】実証スケジュール



(4) 実証地域の選定

① 実証地域

新潟県

② 実証地域選定理由

＜地方圏での実施選定理由＞

啓発機会や専任人材が少ない地方エリアにて本実証を実施することにより、大都市圏のみならず様々な地域でのモデル化ができると考え、地方圏を選定。

地方圏を選定するにあたり、以下を想定。

■ 東名阪等大都市圏と地方圏を比較した場合、サイバーセキュリティセミナー等の啓発機会や、サイバーセキュリティ支援企業数（技術者の要員数）は少ない。

■ 地方圏においても、重要産業、企業が多数存在しているため、地方も含めて対策を実施することが日本全体のサイバーセキュリティ対策向上につながる。

＜新潟県の実施選定理由＞

以下の理由により、地方圏の中で新潟県を選定。

■ 東日本の地方圏の中で新潟県は比較的事業所数が多く、日本の“ものづくり”を支える製造業の割合が全国平均を上回っている。

■ 三条、燕地域では金属製品、長岡地域では生産用・業務用機械器具、上越・妙高地域では電子部品・デバイスが盛んであり県内のすべてのエリアについて“ものづくり”が盛んである。

■ 長岡市エリアにおいては自動車・バイクのメーターの製造が盛んで、特にバイクメーター国内シェアは 9 割弱、世界シェアは 3 割ほどを占める。

(5) 参加企業

① 説明会による募集

新潟県内の各企業が所属する団体・協会と連携した事業説明会※を 4 回実施。

※事業説明会概要

＜開催日程（場所）＞

6 月 25 日（火）：糸魚川会場

6 月 26 日（水）：上越会場

6 月 27 日（木）：中越会場

8 月 27 日（火）：新潟会場*追加開催

＜説明会集客方法＞

I. 地域団体、連携する法人団体への勧奨による集客

■ 公益財団法人日本電信電話ユーザ協会、新潟商工会議所、ほか

II. NTT 東日本新潟支店（新潟・長岡・上越）及び東京海上日動火災保険株式会社（以下「東京海上日動」という。）の顧客基盤への勧奨による集客

III. 地域開催セミナーを活用した集客

IV. メールマガジンを活用した集客（新潟会員：約 4,000 名）

＜説明会内容＞

I. サイバーセキュリティセミナー（有識者講演、デモ展示等）

■ サイバーセキュリティ脅威と対策の必要性について

■ サイバーセキュリティの事故事例、有効な対策について

■ SECURITY ACTION 及び中小企業のサイバーセキュリティ対策ガイドラインの普及に関する内容等

II. 本実証事業の趣旨説明、参加募集

② NTT 東日本の顧客基盤を活かした募集

日頃からリレーションがあり、ネットワーク環境を把握している（＝セキュリティ対策が万全でないことを把握している）ユーザを中心に選定し、セキュリティ対策の普及啓発活動の一環として、本実証事業の内容や意義の説明（個別訪問）を実施した。上記活動を、営業担当者約 40 名で約 3 ヶ月間（6 月～8 月）に亘り、実施した。

＜参加企業募集において注力した点＞

実証事業終了後のセキュリティ対策機器の継続利用を促進できるよう、セキュリティ対策導入の必要性が高いと思われるユーザ（業務上の個人情報取り扱い有無、サプライチェーン、NW 環境等）を選定し、本実証事業におけるトライアルを通して導入の必要性を実感いただいた。

③ 地域の企業との連携による募集

NTT 東日本と取引のある地域の企業（SIer、電気工事会社等）と連携し、地域の企業が日頃からリレーションがあり、ネットワークに関する対策が万全でないと思われるユーザを選定いただき、選定したエンドユーザへ本実証事業の内容を説明し、参加いただいた。上記活動を、地域の企業 4 社と約 3 ヶ月間（6 月～8 月）実施した。

＜参加企業募集において注力した点＞

■ 連携する地域の企業を選定する際、以下の点をポイントに選定した。
  -地域に根付いた企業であり、エンドユーザとのリレーションが深く、ネットワーク環境を把握している
  -中小企業を顧客としている
■ 地域の企業に本実証事業の趣旨を理解いただくため、地域の企業に対する概要説明会を実施した。
■ 地域の企業とエンドユーザへ同行訪問し、本実証事業の内容や意義の説明を実施した。

④ 参加企業数・内訳

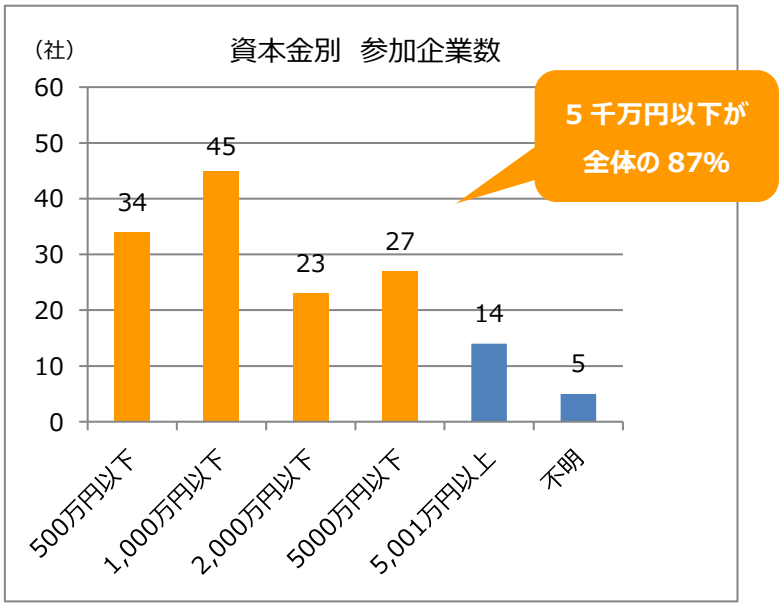
＜参加企業数＞

148 社

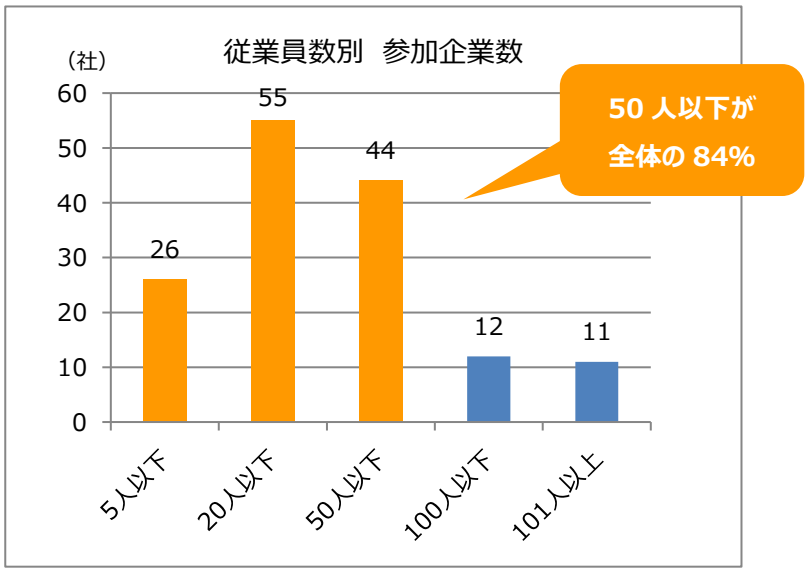
参加企業はすべての実証（意識調査・UTM 設置・標的型攻撃メール訓練）に参加している。ただし、標的型攻撃メール訓練についてはモバイルキャリアのメールアドレスのみ所有の企業が訓練対象外となり 148 社中、147 社が参加した。

規模別、業種別の内訳は図 9～11 の通りであった。

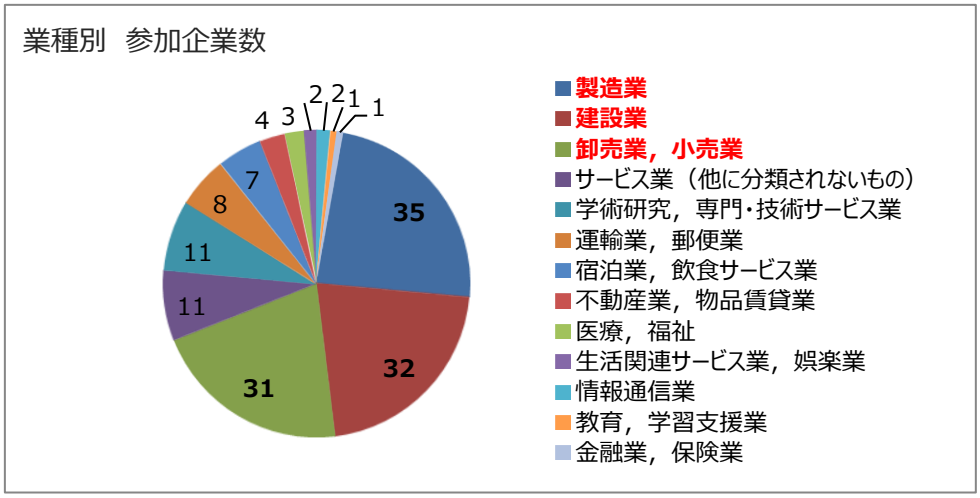
【図 9】資本金別 参加企業数



【図 10】従業員数別 参加企業数



【図 11】業種別 参加企業数



(6) 実証内容（詳細）

下記①～③の観点で中小企業の実態を収集・分析し、今後のサービスの在り方や普及啓発等を含めた提言として取りまとめる。

【表 1】収集する情報と活用方法

収集する情報	収集するための 具体的な手段	データ活用方法（調査内容）
① 企業のサイバーセキュリティ対策における実態	■実証前後のアンケートによる意識調査	■中小企業のサイバーセキュリティ対策の現状把握 ■実証開始時の中小企業におけるサイバーセキュリティに対する意識調査 ■サイバーセキュリティ脅威に対する事前対策・事後対応（復旧・補償）、企業内啓発策の導入・実施に向けての障壁把握（金銭的要因、技術的要因） ■実証後の企業における社員意識の変化 新たな保険サービスについて検討する素材
② 企業に対するサイバー攻撃等の脅威及び対応状況の実態	■UTM 通信ログ ■一元対応窓口に対する問合せ内容の応対記録	■UTM のログから見える脅威のアタックとブロック状況 ■参加企業からの問合せ内容、頻度、傾向 ■サイバーセキュリティ支援人材に必要なスキルレベル サイバーセキュリティ対策のサービス内容・価格帯の検討
③ 標的型攻撃メールに対する社員意識の実態	■標的型攻撃メール訓練	■標的型攻撃メール訓練開封率（実証前後比較） ■標的型攻撃メール訓練実施とサイバーセキュリティ脅威状況のフィードバックによる意識変化（実証前後比較）

① 企業のサイバーセキュリティ対策における実態

アンケートによる実証開始時の中小企業におけるサイバーセキュリティに対する意識調査

② 企業に対するサイバー攻撃等の脅威及び対応状況の実態

実証参加企業にセキュリティ機器（UTM※）を設置し、UTM 通信ログを収集する。

※NTT 東日本のセキュリティインシデント監視・復旧支援サービス「おまかせサイバーみまもり」

「おまかせサイバーみまもり」の機能は表 2～3、図 12～14 参照。

【表 2】おまかせサイバーみまもりの機能

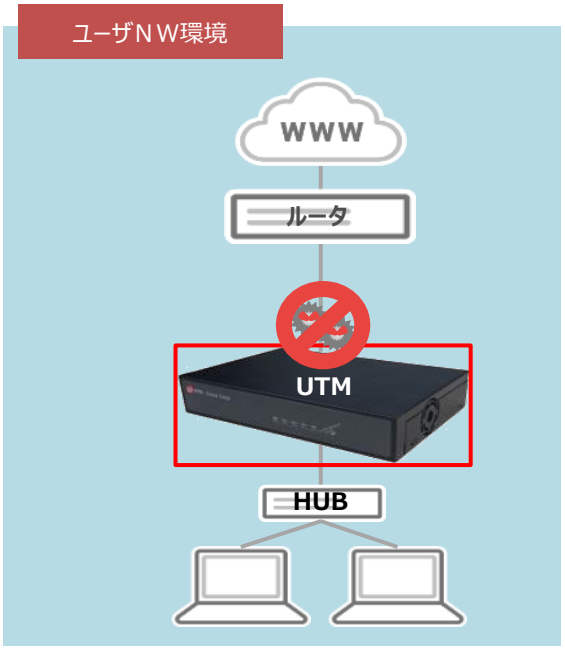
分類	機能概要
1．専用 BOX	■おまかせサイバーみまもりを利用するために必要となる宅内端末 ■契約者のネットワーク内に設置し、セキュリティ脅威の防御や、通信状況の通知等を実施
2．問合せ対応	■セキュリティ全般に関する問合せについて、セキュリティサポートデスクにて対応を実施
3．セキュリティ監視	■専用 BOX 配下のサポート対象機器による C&C サーバへの通信を監視し、検知した場合にはメールおよび電話にて契約者に連絡を実施
4．専用 BOX 遠隔設定変更	■セキュリティサポートデスクにて、Web サイトブロックの設定・変更を実施
5．遠隔サポート	■問合せ対応やセキュリティ監視により、ユーザ端末がマルウェア感染の可能性がある場合に、感染の確認及び駆除支援等を実施 ■機器の故障が疑われる場合に、切り分け作業の支援を実施
6．訪問サポート	■遠隔サポートによりユーザの状況が改善しないまたは遠隔サポートが完結しない場合にユーザ先に訪問し、作業を実施 ■東日本エリアは、9:00～19:00 対応 ■西日本エリアは、9:00～17:00 対応
7．レポート配信 （月次レポート・サマリーレポート）	■専用 BOX で収集したログをもとに、月 1 回月次レポートをメールにて送付 ■見やすく分かりやすくまとめたサマリーレポートを月 1 回メールにて送付
8．機器故障対応	■専用 BOX 故障時に日中帯（9:00～17:00）にオンサイトで機器交換を実施
9．24 時間機器故障対応 （オプション）	■専用 BOX 故障時に 24 時間 365 日オンサイトで機器交換を実施

【表 3】おまかせサイバーみまもりのセキュリティ機能

機能名		機能概要
不正アクセスブロック	不正プログラム対策	不正な通信、プログラムによる攻撃を検知。どこから、どこに、どんな通信が行われているか判別し、内部感染を早期に発見。C&C サーバ通信の検知、Shellshock など脆弱性を狙う攻撃などに対応。
	Web サイトアクセスブロック	不正 Web サイト、不正 URL へのアクセスを止めることにより不正プログラムによる感染、フィッシング詐欺被害を未然に防止 。

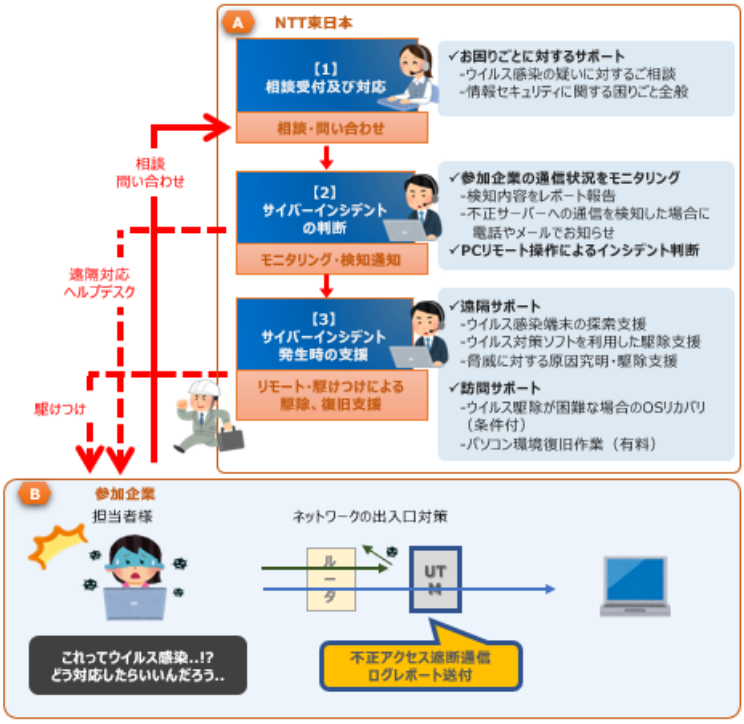
機能名		機能概要
不正侵入対策	ファイアウォール	攻撃のみをブロックし、適切なアプリケーショントラフィックだけを通過する機能。
	IPS （不正侵入防御）	ポリシールールで許可されたトラフィックを調べ侵入する脅威、セキュリティホールなど悪意ある攻撃がないかを確認し、セキュリティを強化。
メールセキュリティ対策		メールに含まれる不正プログラムの検知やスパム（迷惑）メールを判定。検知・処理されたメールは、件名に、不正プログラムは「ウイルス駆除済み」、スパムメールは「スパムメール」を付与し、送信。
URL 指定によるアクセス制御		URL を指定し、アクセス許可されたカテゴリから、特定のサイトのみをブロック（ブラックリスト）したり、ブロックしたカテゴリから、特定のサイトのみをアクセス可能（ホワイトリスト）とする。
アプリケーション利用制限		アプリケーションの利用制限を行う機能。日本独自のアプリケーションを含む 1,000 以上のアプリケーションをサポート。

【図 12】セキュリティ機器構成（イメージ図）



【図 13】支援体制（イメージ図）

企業からの相談・問合せに対する一元対応窓口を設置し、各種困りごとインシデント判断・遠隔駆除を実施。



【図 14】実証拠点

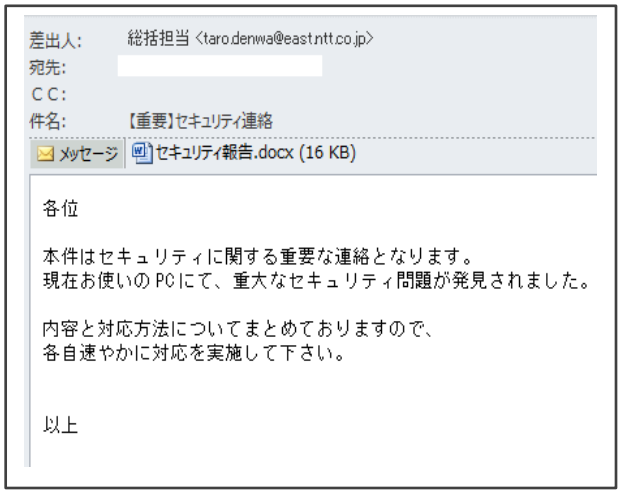
現地駆けつけが必要な場合には県内の各 7 拠点から対応。
（拠点：新潟・三条・長岡・上越・南魚沼・新発田・佐渡）

③ 「標的型攻撃メール訓練」による参加企業社員のサイバーセキュリティ意識把握

■ 参加企業の社員宛に訓練用の標的型攻撃メールを配信し（メール本文は図 15 参照）、組織ごとに添付ファイルの開封者数、開封率を各企業に報告する。

■ 参加企業社員の標的型攻撃メールに対する対応の有無、傾向を調査する。

【図 15】標的型攻撃メール訓練　本文サンプル



4. 実証開始時のアンケート結果

中小企業のサイバーセキュリティ対策の現状把握、実証開始時の中小企業における社員のサイバーセキュリティに対する意識調査を目的に実証開始時にアンケートを実施した。（実証前後の比較を行うため実証後にも同種のアンケートを実施する）

(1) アンケート内容

＜対象者＞ 説明会参加企業・実証参加企業

＜回答数＞ 243 社

＜実施日＞ 6 月 1 日～9 月末の期間で実施

＜実証開始時アンケート内容＞

Q1.サイバーセキュリティ対策に関心をお持ちですか

1. すぐにでも、検討しようと思った
2. とても関心があり、いずれ検討しようと思った
3. 関心はあるが、検討するかは分からない
4. 関心はない

Q2.セキュリティ対策に際しての、あなたご自身の立場をお教えください（ひとつだけ）

1. 社内への導入を承認する立場
2. 社内への導入を提案する立場
3. 社内で利用する立場
4. その他（ ）

Q3.オリンピック開催に向けてセキュリティリスクが高まっていることをご存知ですか

1. よく知っていて、対策も打っている
2. よく知っているが対策は未実施
3. あまり知らない
4. 聞いたことがない

Q4.ご存知のセキュリティ脅威がございましたらお答え願います（いくつでも）

1. 標的型攻撃による被害
2. ビジネスメール詐欺による被害
3. ランサムウェアによる被害
4. サプライチェーンの弱点を悪用した攻撃の高まり
5. 内部不正による情報漏えい
6. サービス妨害攻撃によるサービスの停止
7. インターネットサービスからの個人情報の窃取

8. IoT 機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい

Q5.貴社で被害のあるセキュリティ脅威がありましたらお答え願います（いくつでも）

1. 標的型攻撃による被害
2. ビジネスメール詐欺による被害
3. ランサムウェアによる被害
4. サプライチェーンの弱点を悪用した攻撃の高まり
5. 内部不正による情報漏えい
6. サービス妨害攻撃によるサービスの停止
7. インターネットサービスからの個人情報の窃取
8. IoT 機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい

Q6.貴社で導入しているセキュリティ対策をお教えください（いくつでも）

1. ウイルス対策ソフト
2. 出入り口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. サイバーリスク保険
8. その他（　　）

Q7.今後、以下のセキュリティ対策を実施することを検討していますか（いくつでも）

1. ウイルス対策ソフト
2. 出入り口対策
3. 社員教育
4. セキュリティ管理者の設置
5. セキュアな無線環境
6. セキュアな拠点間通信
7. サイバーリスク保険
8. その他（　　）

Q8.今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか

1. 5000 円～10000 円
2. 10000 円～5 万円
3. 5 万円～
4. 費用はかけない

Q9.サイバーリスクに関して、貴社の課題を教えてください

1. セキュリティに関する方針の策定
2. 管理体制の構築
3. リスクの洗い出し、評価
4. グループ会社、取引先も含めた対策の実施
5. セキュリティ予算の確保
6. 専門人材の確保
7. インシデント発生時の体制の構築
8. 情報収集（最新技術動向や事故事例）
9. その他（ ）
10. なし

Q10.インシデント発生時の相談先はありますか

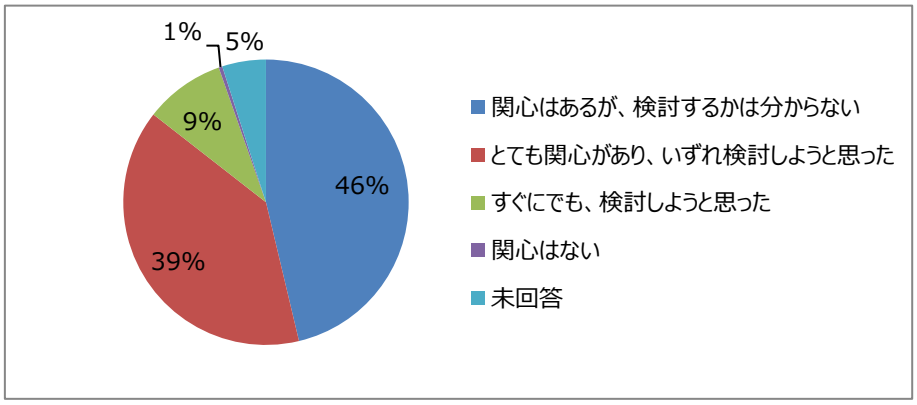
1. システムベンダ
2. その他（ ）
3. なし

(2) アンケート結果（集計）

① サイバーセキュリティ対策への関心

サイバーセキュリティへの関心があると回答した企業は 243 社中 229 社と全体の 94%を占めているが、「すぐにでも、検討しようと思った」と答えた企業は 9%に留まった。

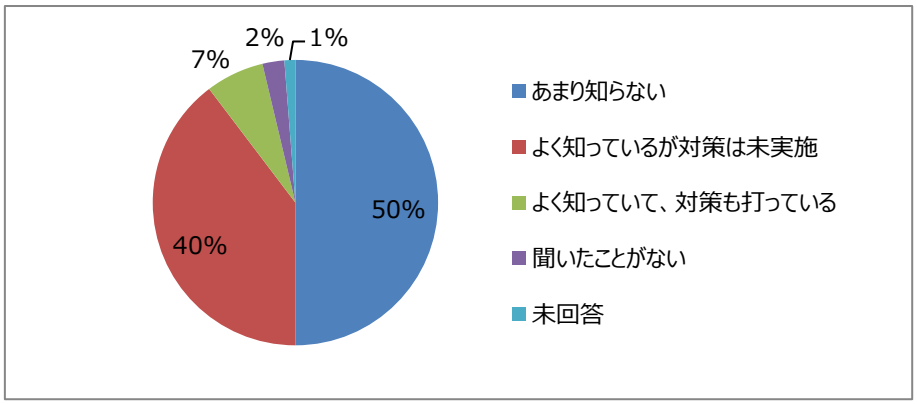
【図 16】Q1.サイバーセキュリティ対策に関心をお持ちですか



② オリンピック開催に向けたサイバーセキュリティリスクの高まり

オリンピック開催に向けてサイバーセキュリティリスクが高まっていることの認知度は低く、約半数の企業が「あまり知らない」または「聞いたことがない」と回答、「よく知っていて、対策も打っている」と回答した組織は 7%に留まった。地理的に東京から距離があることから、首都圏と比べて対策の必要性を感じている企業が少ないと推察される。

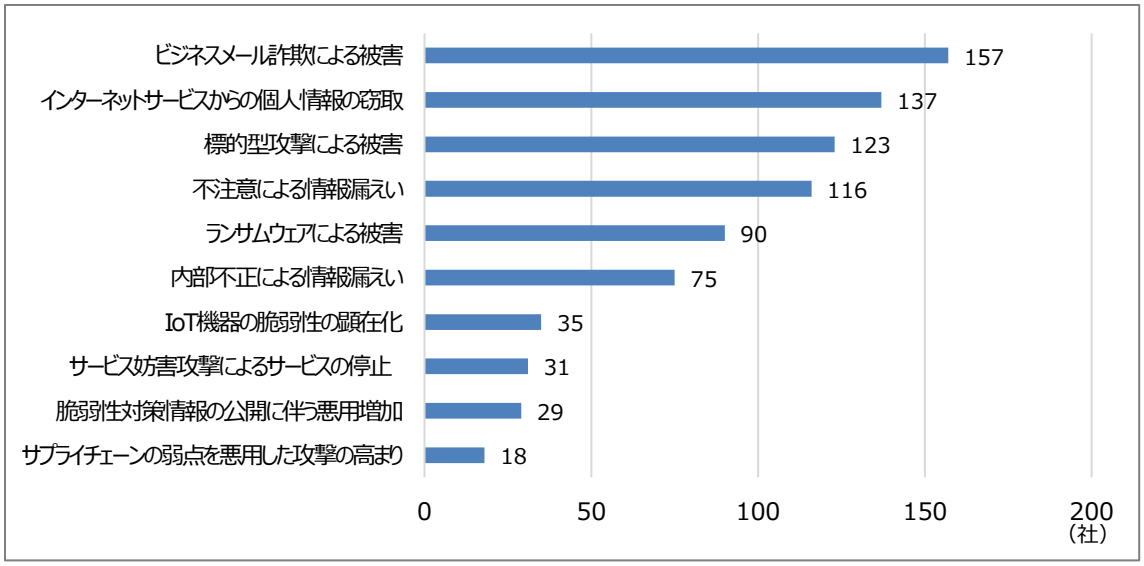
【図 17】Q3.オリンピック開催に向けてセキュリティリスクが高まっていることをご存知ですか



③　脅威の認識

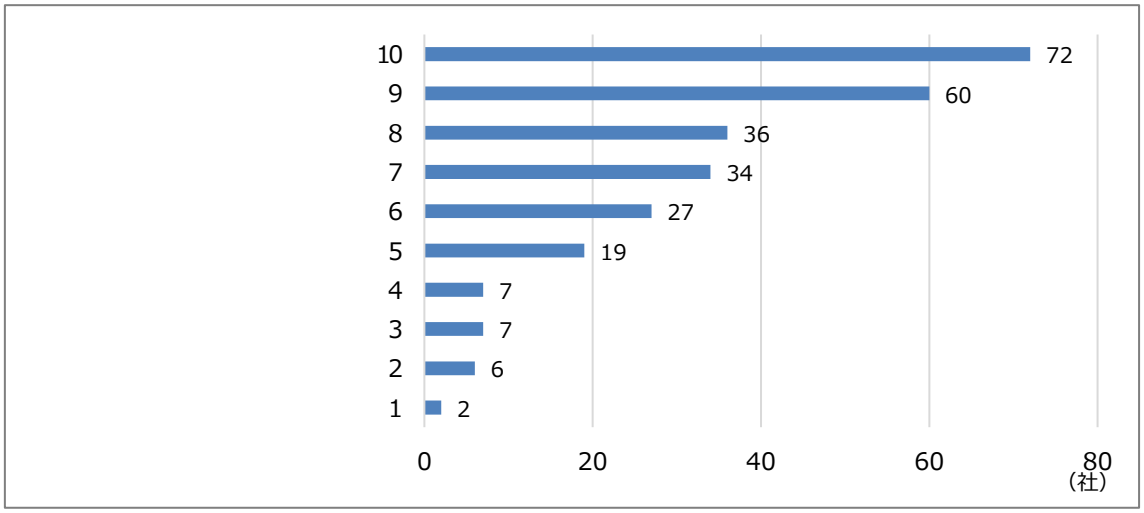
独立行政法人情報処理推進機構（以下「IPA」という。）が毎年発表する「10 大脅威」の中で、知っているサイバーセキュリティ脅威の 1 位は「ビジネスメール詐欺による被害」であった。近年被害が急増しており、「10 大脅威」の順位は、2017 年のランク外から 2018 年が 3 位、2019 年が 2 位とランクアップしている。被害額が高額となる事例が報道されたこともあり認知度が高まっていることがうかがえる。次いで、「インターネットサービスからの個人情報の窃取」、「標的型攻撃による被害」と続いている。「サプライチェーンの弱点を悪用した攻撃の高まり」は 18 社、全体の約 7%に留まった。

【図 18】Q4.ご存知のセキュリティ脅威がございましたらお答え願います。（いくつでも）



自社に被害がある脅威の 1 位は、知っているセキュリティ脅威と同様「ビジネスメール詐欺による被害」で、72 社、全体の約 3 割の企業が被害にあっていた。次いで「不注意による情報漏えい」「インターネットサービスからの個人情報の窃取」と続いている。

【図 19】Q5.貴社で被害のあるセキュリティ脅威がありましたらお答え願います。（いくつでも）



【表 4】＜参考資料＞情報セキュリティ 10 大脅威 2019（組織編）

順位	組織向け脅威
1 位	標的型攻撃による被害
2 位	ビジネスメール詐欺による被害
3 位	ランサムウェアによる被害
4 位	サプライチェーンの弱点を悪用した攻撃の高まり
5 位	内部不正による情報漏えい
6 位	サービス妨害攻撃によるサービスの停止
7 位	インターネットサービスからの個人情報の窃取
8 位	IoT 機器の脆弱性の顕在化
9 位	脆弱性対策情報の公開に伴う悪用増加
10 位	不注意による情報漏えい

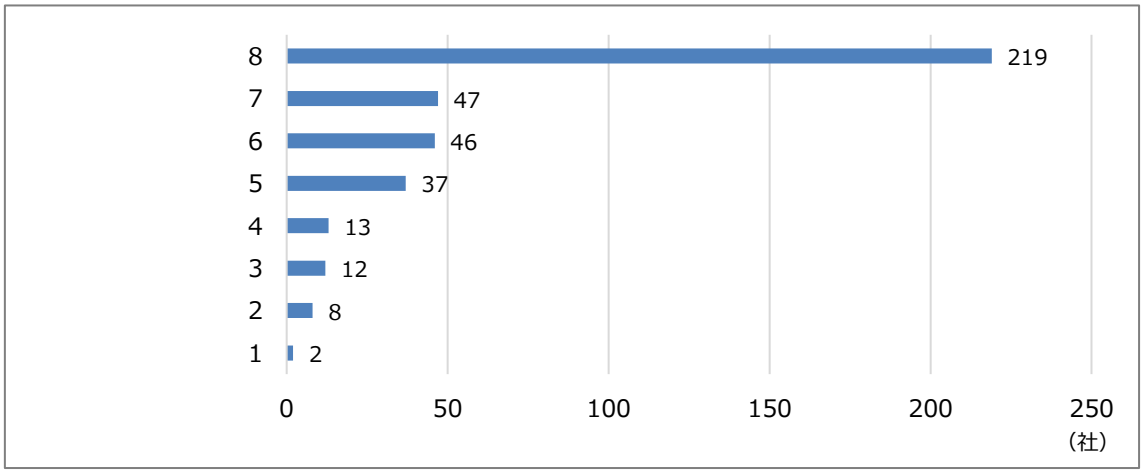
出典：IPA「情報セキュリティ 10 大脅威 2019」

https://www.ipa.go.jp/files/000072668.pdf

④　導入しているセキュリティ対策

導入しているセキュリティ対策は、1 位が「ウイルス対策ソフト」で 219 社、全体の約 9 割が導入している。次いで、「出入り口対策」「社員教育」と続くが、どちらも全体の 2 割弱に留まっている。「サイバーリスク保険」の加入は 8 社、全体の 3%であった。

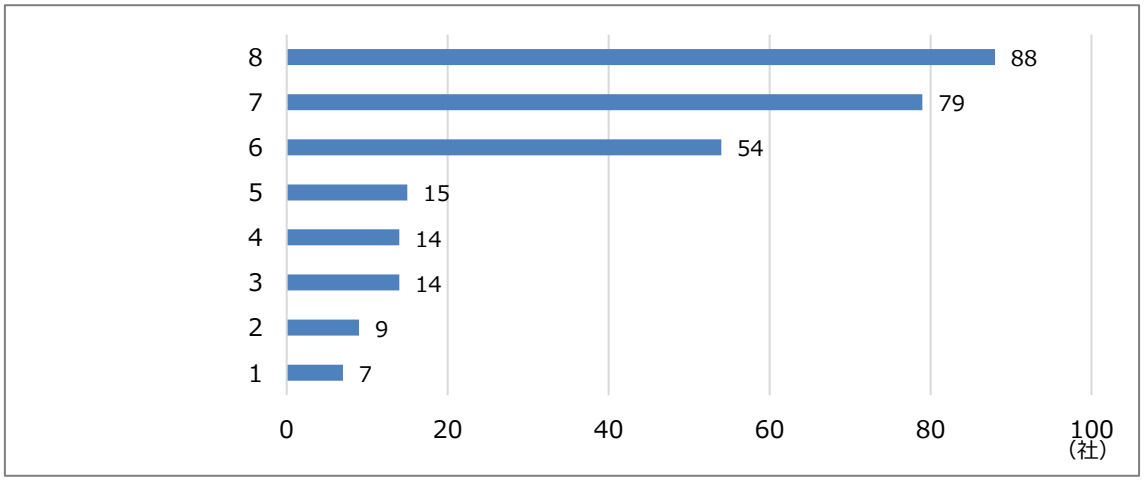
【図 20】Q6.貴社で導入しているセキュリティ対策をお教えください。（いくつでも）



⑤　検討しているセキュリティ対策

検討しているセキュリティ対策は、1 位が「出入り口対策」で 88 社であった。「サイバーリスク保険」の加入を検討している企業は 9 社であった。（「ウイルス対策ソフト」の回答には、新規の導入だけでなく無料ソフトから有料ソフトへの切り替えの検討や適用範囲の拡大、バージョンアップ等のニーズを含む。）

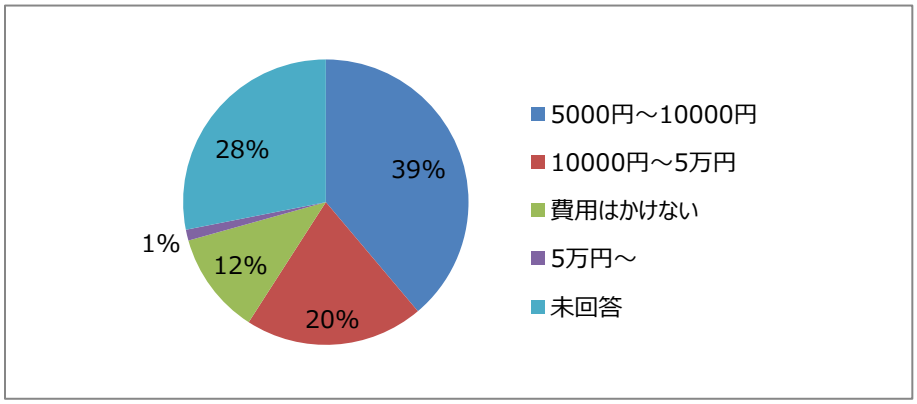
【図 21】Q7.今後、以下のセキュリティ対策を実施することを検討していますか（いくつでも）



⑥　セキュリティ対策にかける費用見込み

今後セキュリティ対策にかける月額費用の見込みは、5,000 円～10,000 円が 39%、次いで 10,000 円～5 万円が 20%であった。「費用はかけない」と回答した企業が全体の 12%、28 社あった。

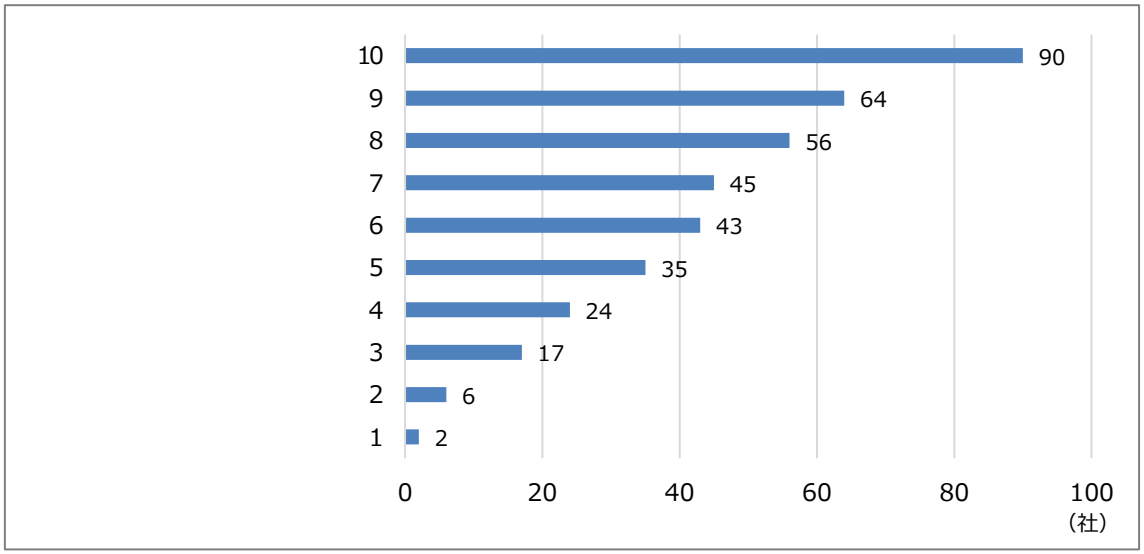
【図 22】Q8.今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。



⑦　サイバーリスクに関する課題

サイバーリスクに関する課題は、1 位が「管理体制の構築」で 90 社、全体の 4 割弱であった。次いで、「セキュリティ予算の確保」「セキュリティに関する方針の策定」と続いている。

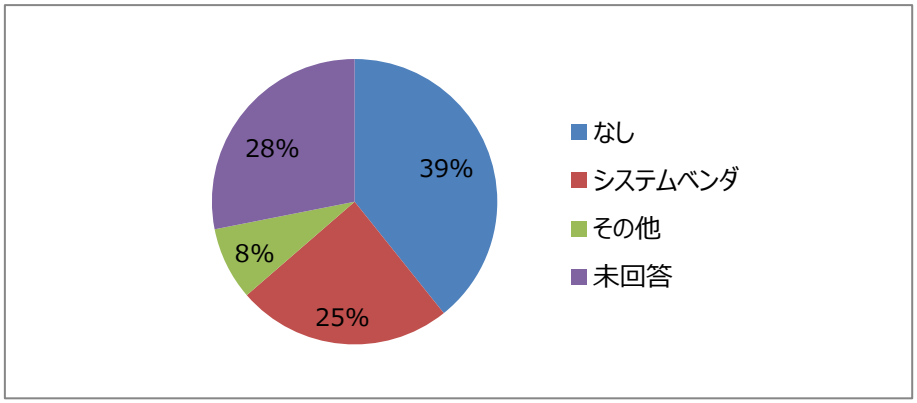
【図 23】Q9.サイバーリスクに関して、貴社の課題を教えてください（いくつでも）



⑧　インシデント発生時の相談先

インシデント発生時の相談先がないと回答した企業が 95 社、全体の 4 割弱であった。

【図 24】Q10.インシデント発生時の相談先はありますか？



(3) 考察

サイバーセキュリティ対策への関心は高いが、すぐにでも検討をしようと思ったと回答した企業は少ない。関心は持っているものの優先順位が低いことが推察される。一方、本実証への参加希望は想定以上に多く、外部からの情報提供や本事業のような無料で実施できる機会など、きっかけがあれば検討が進む可能性がある。

脅威の認識については、知っている脅威・被害のある脅威ともにビジネスメール詐欺が最も多かった。ビジネスメール詐欺は 2017 年 12 月に大手航空会社が偽メールにより約 3 億 8400 万円の被害に遭うなど各種報道がされている。また、警察庁、IPA、一般社団法人全国銀行協会等がビジネスメール詐欺の手口や対策を公表し注意喚起を行っている。

ビジネスメール詐欺は、企業の経営幹部や取引先企業等になりすましてメールで送金の指示や請求書の送金先口座変更を行い、金銭を詐取するものである。海外との取引が利用されるケースが多かったが、日本語を使用するケースも発生しており、企業規模や海外との取引有無、個人情報の保有有無に関わらず標的となる。本アンケートでも約 3 割の企業が被害にあっており中小企業も標的になっていることがわかる。

検討している対策は出入り口対策が 1 位であり、ウイルス対策ソフト導入済みの企業が次に導入する対策としてあげていると推察される。今後サイバーセキュリティ対策にかける費用の見込みは 5,000～10,000 円が約 4 割と一番多かった。

インシデント発生時の相談先については、相談先がないと回答した企業が全体の 4 割弱であった。インシデント発生時に自社のみで対応することは困難であり、相談先がない、または相談先を認識できていない企業が多いことは課題である。

5. 実証期間中のサイバーセキュリティ脅威についての結果と考察

UTMのログから見える脅威のアタックとブロック状況、参加企業からの問合せ内容・頻度・傾向、サイバーセキュリティ支援人材に必要なスキルレベルを把握することを目的に、UTM を設置し、ログの収集・分析を行うとともに、一元対応窓口に対する問合せ内容の応対記録の集計・分析を行った。

(1) セキュリティ対策機器（UTM）の設置における課題

① 本事業における UTM 設置方法

＜設置工事前＞

UTM 設置にあたり、事前にユーザのネットワーク環境の全件調査実施

↓

HUB 要否、LAN ケーブルの不足数確認

↓

設置前の状況を写真撮影および資料化

↓

端末台数等によりスペック/プランの選定

＜設置工事時＞

調査結果をもとに、事前の設定シートを作成し、クラウド側を設定。

↓

設置工事時に設定内容の流し込み（クラウド型）

↓

設置工事時通信断発生、参加企業通信断了承時間内で設置工事実施

↓

設置後のインターネット等通信の正常性確認実施

＜運用＞

24 時間訪問修理サポートの提供（遠隔サポート/訪問サポート）

② 設置における課題

- UTM 設置には、ユーザのネットワーク環境および構成を把握し、ユーザ環境下での UTM 正常動作を確認する必要がある。そのため、ユーザからのサービス申込み～現場調査～提供まで最短約 1 ヶ月が必要となる。（本実証事業においては、実証終了後の UTM 撤去や通信トラブル発生時の現状復旧が必要であると想定し、実証事業参加企業 148 社に対し現場調査および設置前後のユーザ環境資料の作成を実施した。）
- 事前調査時および設置工事時、ユーザの立会いが必要なため、ユーザに対して拘束時間が発生する。

- 設置工事時、通信断が発生するため、業務に支障をきたすので、設置工事時間の調整が必要である。
- 中小企業には IT リテラシーの高い人材が乏しく、セキュリティ対策機器設置にあたり、IT ベンダの支援が必要である。
- IT ベンダによる導入支援に伴い、設置工事費のユーザ負担が必要である。

(2) セキュリティ対策機器（UTM）によるサイバー攻撃の状況

実証期間中設置したセキュリティ対策機器（UTM）により以下のサイバー攻撃を検知した。

実証期間　2019 年 8 月～12 月
対象企業数　148 社
検知した攻撃

① 不正プログラム検知
② 不正侵入検知（IPS）
③ 不正メール検知
④ Web サイトアクセスブロック
⑤ C&C サーバ検知
⑥ ランサムウェア検知

① 不正プログラム検知

＜機能＞

不正な通信、プログラムによる攻撃を検知。どんな通信が行われているか判別し、内部感染を早期に発見。

＜脅威＞

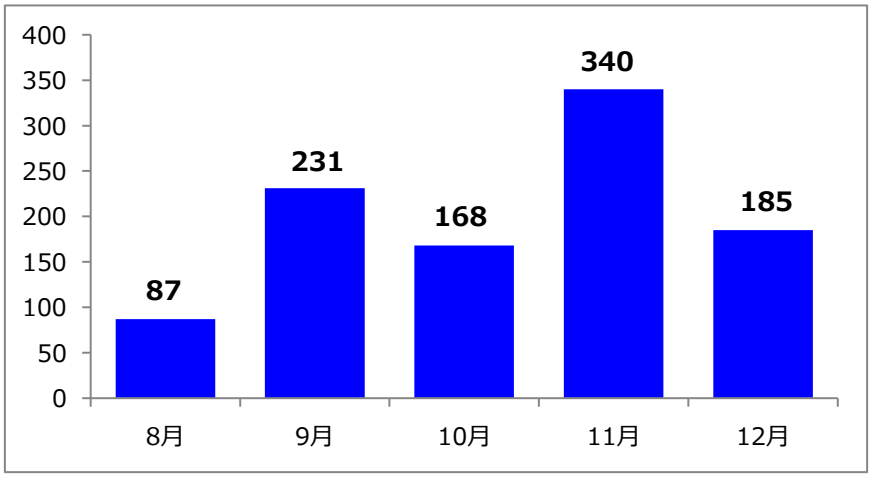
コンピュータに害悪をおよぼすプログラムであり、不正な操作、インターネットに対して情報を送り出す。

【表 5】不正プログラム検知件数（累計）

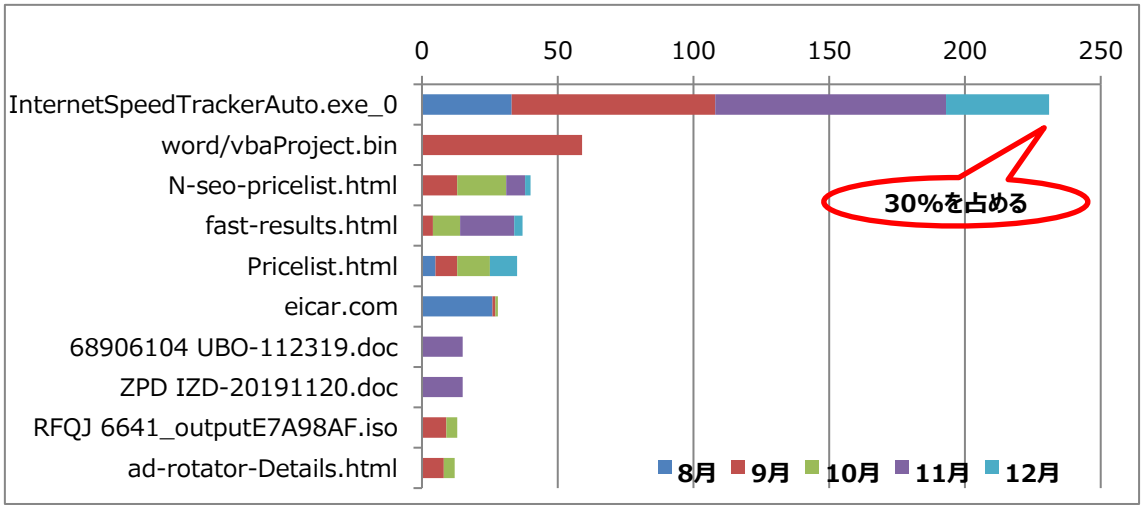
（件）

参加企業検知数合計	1,011
1 企業あたり	6.8
1 日あたり	6.6

【図 25】不正プログラム検知 （月別推移）



【図 26】不正プログラム検知 トップ 10（累計）



② 不正侵入検知（IPS）

＜機能＞

ソフトウェアやネットワークの脆弱性をついた攻撃と疑われる通信を検知・ブロック。

＜脅威＞

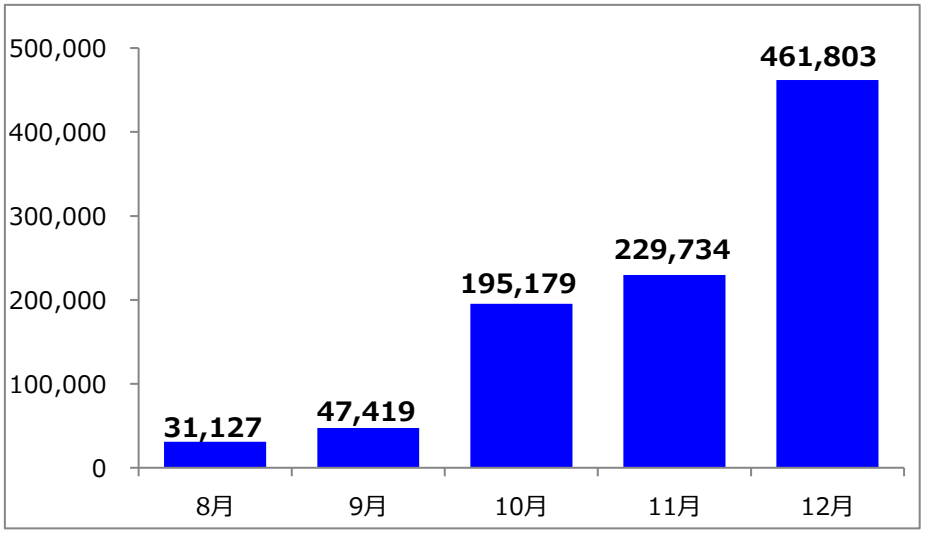
ソフトウェアやネットワークが抱えるサイバーセキュリティ上の問題点である脆弱性を利用した、システムの乗っとりや機密情報の漏えい。

【表 6】不正侵入検知件数（累計）

（件）

参加企業検知数合計	965,262
1 企業あたり	6,522
1 日あたり	6,309

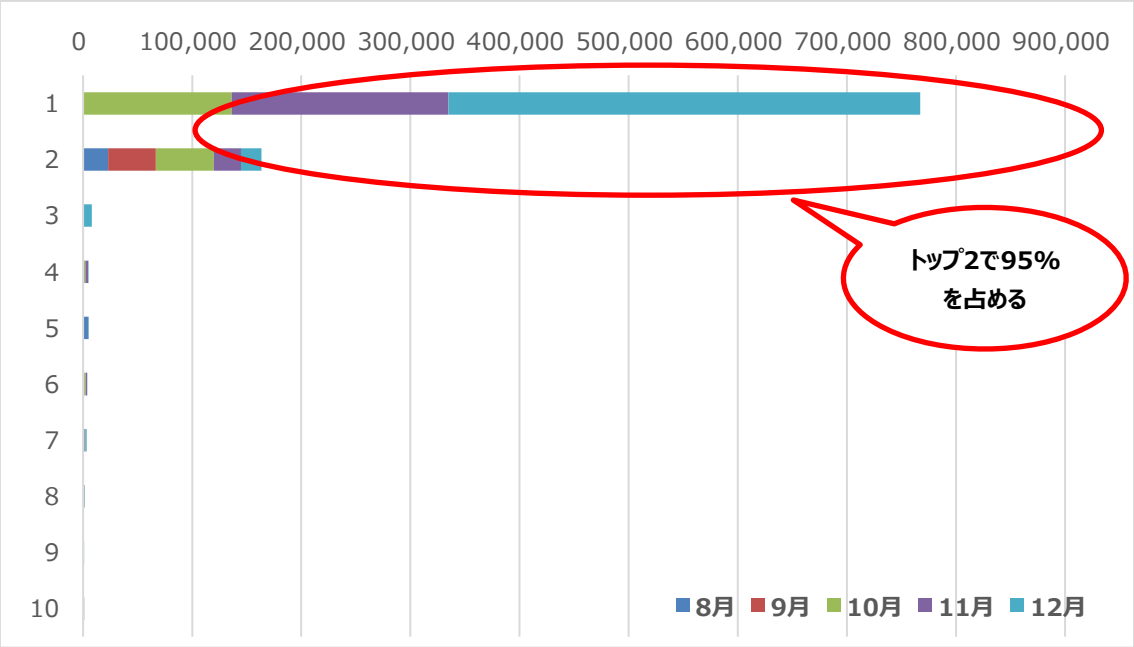
【図 27】不正侵入検知（IPS）　（月別推移）



【表 7】不正侵入検知（IPS）　トップ 10（累計）

	不正プログラムファイル名	累計件数
1	1135775:SMB Windows SMBv2 Information Disclosure Vulnerability (CVE-2019-0703):CVE-2019-0703	767,275
2	4043309056:TCP Land:MISC:RFC 793	163,436
3	1130586:SSL OpenSSL TLS DTLS Heartbeat Information Disclosure -8 (CVE-2014-0160, Heartbleed):CVE-2014-0160	7,912
4	4043309087:Bad TCP Flag:MISC:RFC 791	5,012
5	1133851:EXPLOIT Genivia gSOAP XML parser Buffer Overflow (CVE-2017-9765):CVE-2017-9765	4,960
6	1055397:DNS Microsoft DNS Server NAPTR Record Sign Extension Memory Corruption (CVE-2011-1966):CVE-2011-1966; MS11-058	3,857
7	1133859:WEB Squid Squoison Host Header Cache Poisoning -2 (CVE-2016-4553):CVE-2016-4553	3,211
8	1055299:ICMP Microsoft Windows TCP-IP Stack ICMP Sequence Denial of Service (CVE-2011-1871):CVE-2011-1871;CVE-2011-2013	1,636
9	1133662:SSL OpenSSL DHE and ECDHE Parameters NULL Pointer Dereference -2 (CVE-2017-3730):CVE-2017-3730	1,058
10	1049193:SHELLCODE x86 NOOP - 1	964

【図 28】不正侵入検知（IPS） トップ 10（累計）



③ 不正メール検知

＜機能＞

メールに含まれる不正プログラムの検知やスパム（迷惑）メールを判定。検知・処理されたメールは、件名に、不正プラグラムは「ウイルス駆除済み」、スパムメールは「スパムメール」を付与し、送信。

＜脅威＞

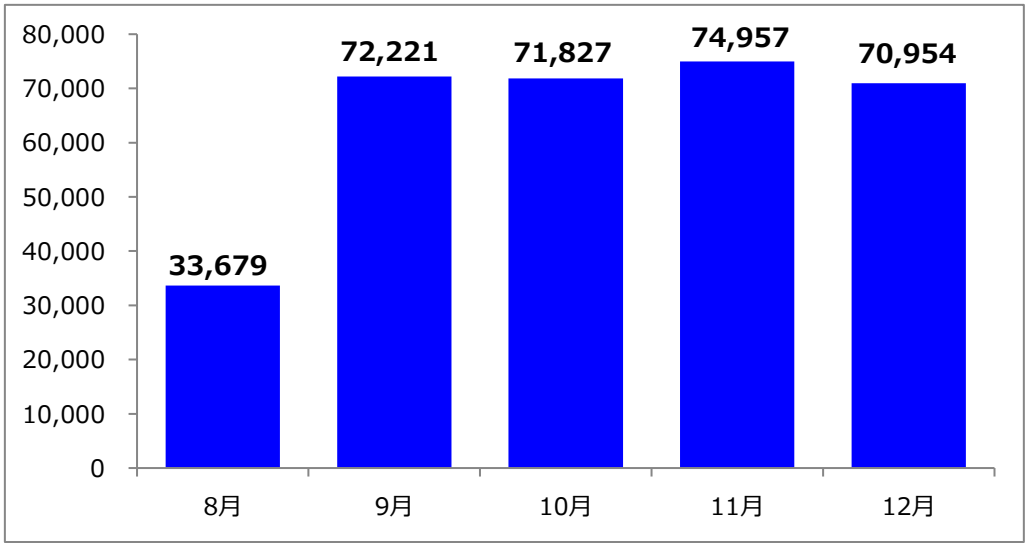
宣伝広告目的で、ユーザの同意なしに勝手に送られてくるメールやウイルスが添付されていたり、アクセスのみで感染に至る URL が記されている「標的型攻撃メール」に感染し情報漏えい等の被害が発生。

【表 8】不正メール検知件数

（件）

参加企業検知数合計	323,638
1 企業あたり	2,187
1 日あたり	2,115

【図 29】不正メール検知件数（月別推移）



④　Web サイトアクセスブロック

＜機能＞

不正な Web サイトへのアクセスを阻止することにより、不正プログラムを実行することによる脅威への感染、フィッシング詐欺被害等を未然に防止。

＜脅威＞

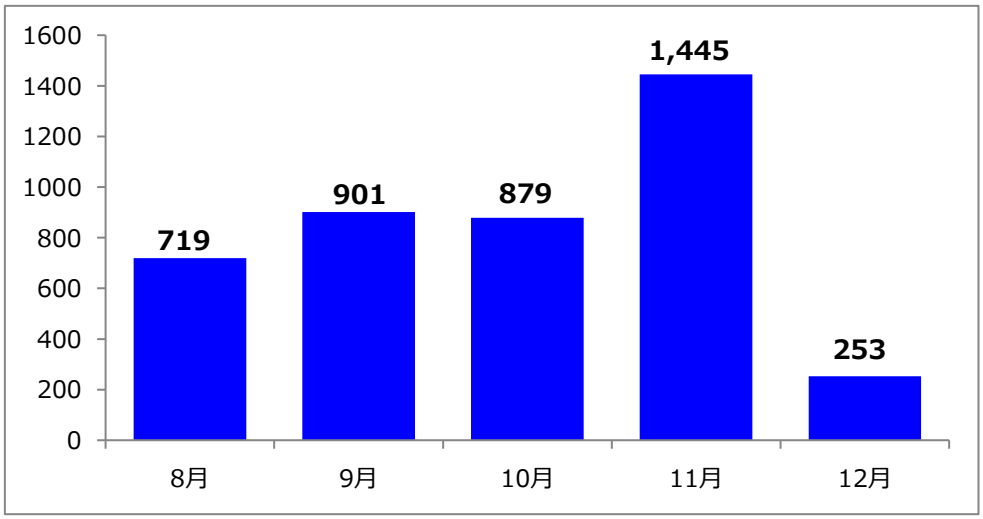
有害なプログラムが仕込まれたウイルス（ランサムウェア等）に感染、金融機関のログイン情報やクレジットカード情報などを取得するフィッシング詐欺、インターネットバンキング等の暗証番号などを取得され、不正に他所へ送金されるオンライン詐欺の被害が発生。

【表 9】Web サイトアクセスブロック件数

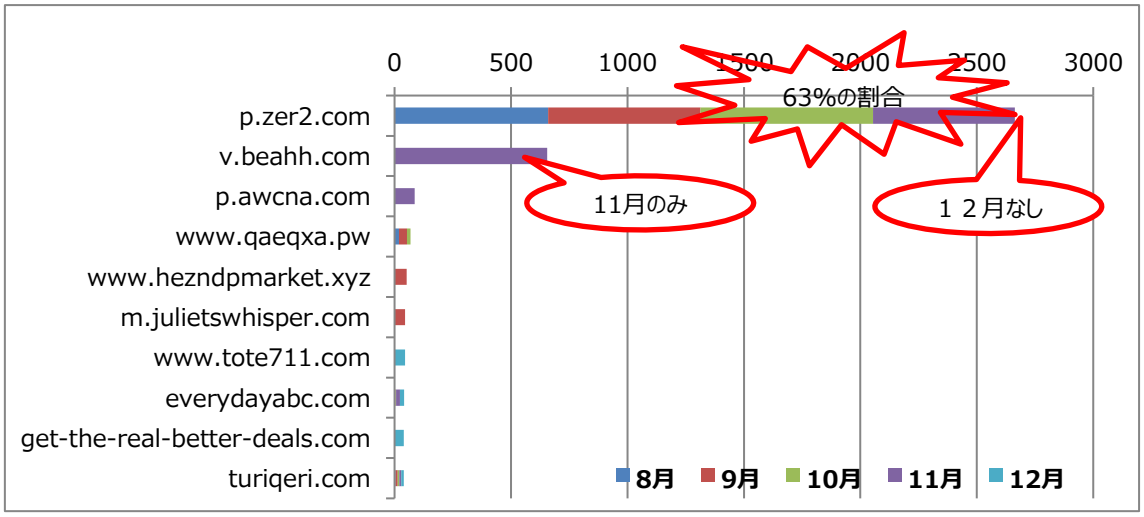
（件）

参加企業検知数合計	4,197
1 企業あたり	28.4
1 日あたり	27.4

【図 30】Web サイトアクセスブロック（月別推移）



【図 31】Web サイトアクセスブロック トップ 10（累計）



⑤　C&C サーバ検知

＜機能＞

C&C サーバ（command and control server）接続を検知・ブロックし、IP アドレスにより、どのユーザが C&C サーバへの通信を実施しているか把握する。

＜脅威＞

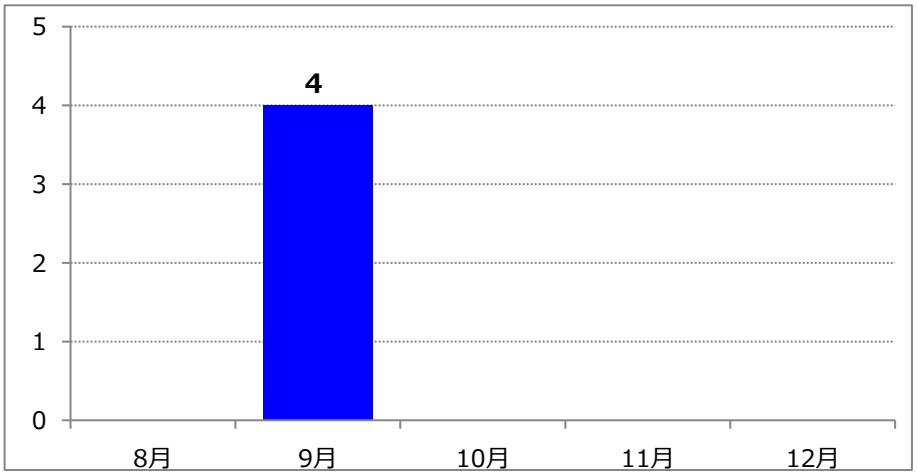
外部から侵入して乗っ取ったコンピュータを踏み台にして制御したり命令を出したりする役割を担うサーバコンピュータであり、通信が発生した場合、特定の Web サイトへ負荷を与える DDoS 攻撃やサーバから、重要な機密情報を抜き取りなどの被害が発生。

【表 10】C&C サーバ検知件数

（件）

参加企業検知数合計	4
1 企業あたり	0.005
1 日あたり	0.026

【図 32】C&C サーバ検知　（月別推移）



⑥　ランサムウェア検知

＜機能＞

ランサムウェアの侵入を検出しブロックした件数と、あて先となっていたユーザを把握する。

＜脅威＞

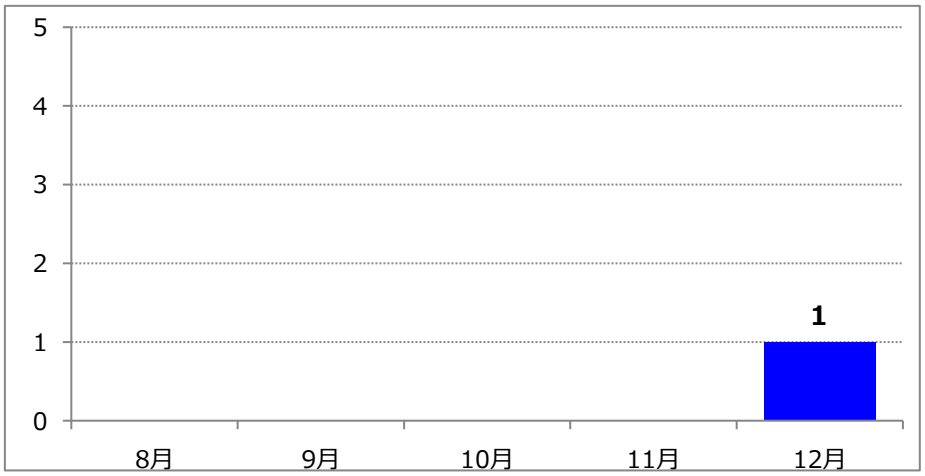
PC 内のファイルを暗号化したりロックすることで使用できない状況に追いこみ、元に戻すことと引き換えに「身代金」（Ransom）を要求する不正プログラム。

【表 11】ランサムウェア検知件数

（件）

参加企業検知数合計	1
1 企業あたり	0.001
1 日あたり	0.007

【図 33】ランサムウェア検知　（月別推移）



＜考察＞

不正プログラム検知は、Internet Speed Tracker ツールバー（接続速度テストアプリ）をインストールしたことにより「InternetSpeedTrackerAuto.exe_0」に感染したケースが約３０％も占めたと推測される。また 11 月は「Emotet」の影響により他の月と比較して検知数が伸びていると推測される。不正侵入検知（IPS）は、9 割近くが 1 社の検知数であり、ユーザ環境を調査したものの「固定 IP アドレスの利用」、「サーバの公開」、「リモート接続」などの環境がないことから、外部からの標的とされそうな原因は見受けられない状況である。ただし食品業者であるため、販売拡大に向けて、雑誌の Web 広告や twitter など様々な広告サイト、ツールを利用していることが要因であると推測される。UTM の継続ユーザであることから今後も調査を進めていく。

不正メール検知に関しては、約 1/3 の企業が検知されており、検知数の多いユーザは毎月同等の数値である。

Web サイトアクセスブロックについても不正侵入検知（IPS）と同様にほぼ 1 社が検知数を独占している状況であり、当該企業の UTM 契約解除により 12 月は極端に検知数が下がっている。なお原因については特定できていない状況である。

C＆C サーバ検知、ランサムウェア検知は、検知数が少ないものの首都圏、大企業だけはなく、新潟県域及び中小企業にも感染する可能性があることが改めて認識した。

(3) 一元対応窓口（サポートデスク）への相談・対応内容

実証期間中、一元対応窓口（サポートデスク）には、以下の問合せがあり対応を行った。

【表 12】一元対応窓口相談件数（内訳）

問合せ内容	件数
①セキュリティ機器設置の問合せ	30 件
②セキュリティ対応相談	24 件
③その他	10 件
合計	64 件

①セキュリティ機器設置の問合せ

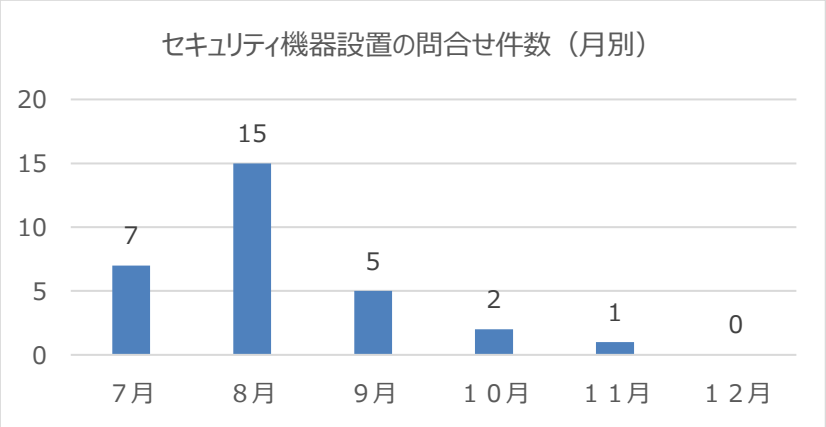
＜主な内容＞

- ネット、メールのアクセスが不可
- スパムメールの増加
- 月次レポートの見方について教えてほしい

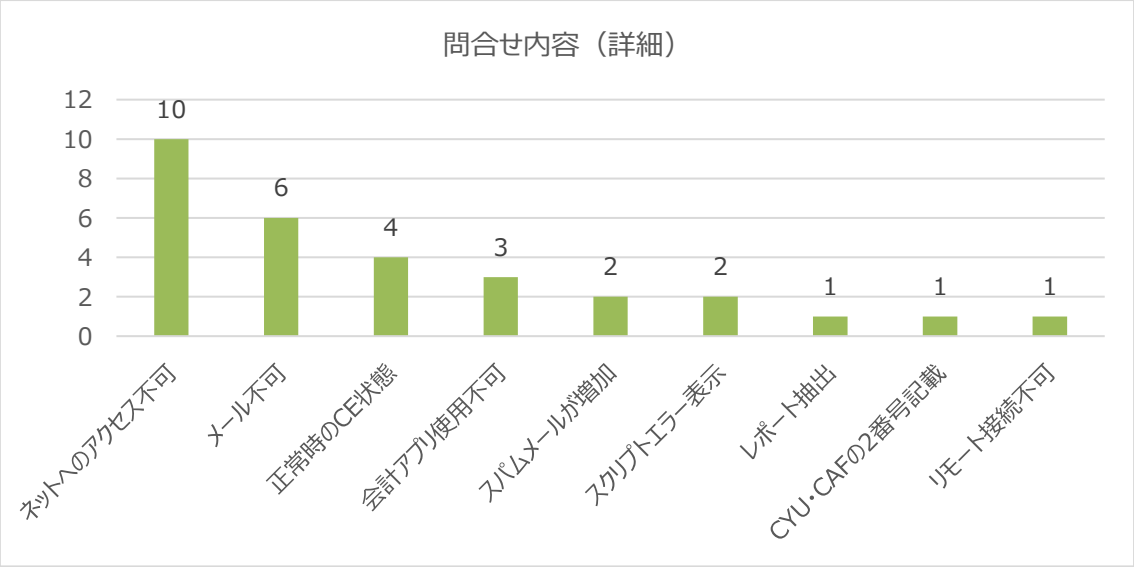
＜対応状況＞

- リモートからアクセスリストの変更及び電源 OFF/ON による再起動で復旧
- 「スパム」タグが付与されたことにより、急増したように見えることを電話説明、現地営業担当対応
- レポートの見方について、現地 SE 担当が対応

【図 34】セキュリティ機器設置の問合せ件数（月別）



【図 35】セキュリティ機器設置の問合せ内容（詳細）



②サイバーセキュリティ対応相談

＜主な内容＞

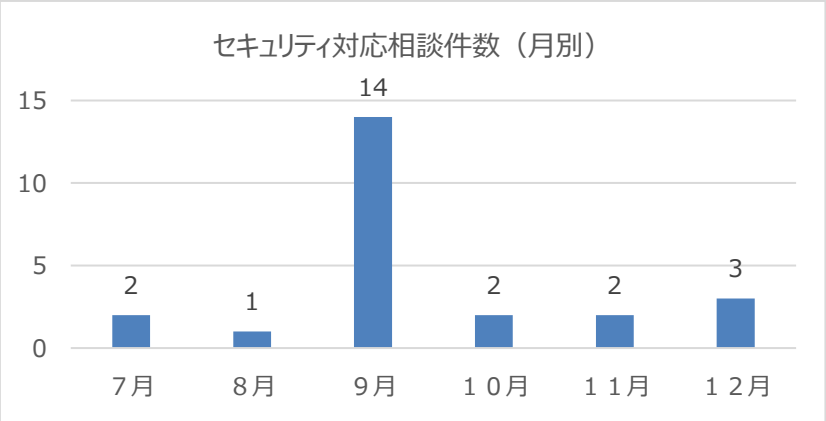
- 特定ポートを空けてほしい
- URL ブロックを解除してほしい
- 月次レポートを紛失してしまったので再送してほしい
- C&C アラート（C&C ウイルスソフト感染）をサポートセンターが検知

＜対応状況＞

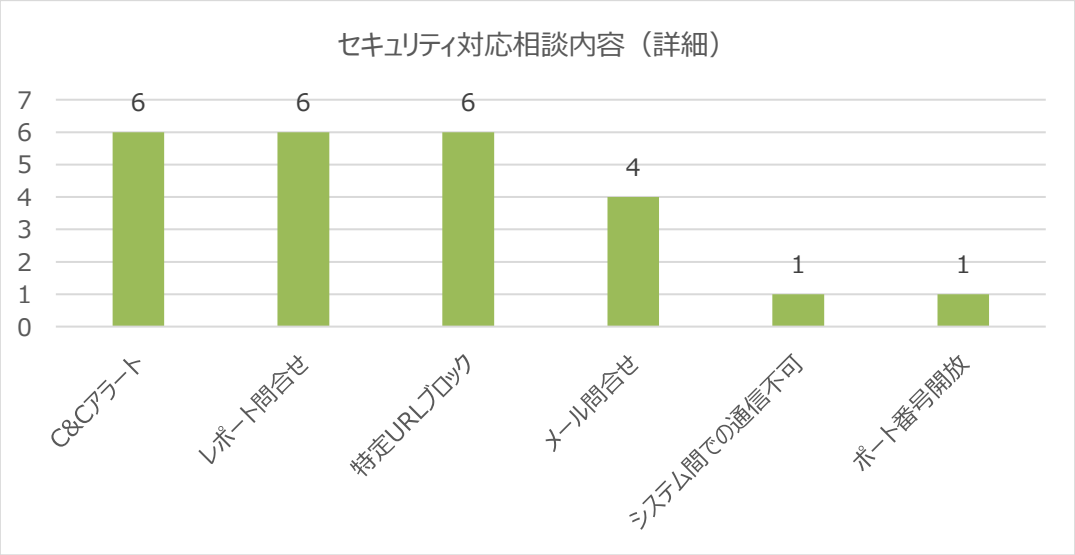
- リモートから IPS ルールの見直し、特定ポート（8080）のポリシー変更を実施
- 特定の URL アクセス解除、取引先との業務で使用している VPN 通信等は、現地に営業、SE 担当が駆付け、ユーザと相談の上指定された URL、ポートの解放実施
- 管理コンソールから確認が可能なことを説明

■ サポートセンターから C&C サーバにアクセスしている状況を報告し、IP アドレスから NAS サーバから発信されていることから、NAS サーバの隔離及び NAS サーバ内のデータをアンチウイルスソフトで駆除することを指摘

【図 36】セキュリティ対応相談件数（月別）



【図 37】セキュリティ対応相談内容詳細



(4) 標的型攻撃メール訓練による社員のサイバーセキュリティ意識

① 標的型攻撃メール訓練の内容

標的型攻撃メール訓練の開封率を比較することによる社員のサイバーセキュリティ意識変化の調査を目的に、標的型攻撃メール訓練を実証前後の計 2 回実施した。

1 回目の開封率は約 20%と 5 人に 1 人が開封した。NTT 東日本のグループ会社が全国で実施した実績である「参考平均開封率」は 13.07%である。これと比較すると、約 7%上回っている。2 回目の開封率は 14%と 1 回目より 7%改善し参考平均に近づいたが、2 回目の開封者のうち 2 回ともに開封

した件数が半分を占めている。

＜対象＞

147 社 198 名（実証参加企業 148 社のうち 1 社についてはモバイルキャリアのメールアドレスのみ所有のため訓練対象外。）

＜配信期間＞

1 回目

メール送信日時：2019 年 9 月 18 日 10：00

開封確認期間：2019 年 9 月 18 日 10：00～9 月 27 日 13：00

2 回目

メール送信日時：2019 年 12 月 13 日 16：00

開封確認期間：2019 年 12 月 13 日 16：00～12 月 25 日 17：00

＜配信本文＞

【図 38】配信本文（1 回目）：取引先からの資料共有と偽り、本文記載の URL に誘導する手口


差出人: eigyo@japan-news-com.jp　　送信日時: 2019/09/18 (水) 10:23
宛先: ntt_cybersecurity_helpteam-ml@east.ntt.co.jp
ＣＣ:
件名: 打合せの議事録のご送付

NTT東日本　新潟支店　様

お世話になっております。

先日に実施した打合せの議事録を作成しました。
内容などに問題がないか、ご確認のほど、よろしくお願い致します。
http://japan-news-com.jp/3d8aee44b6f6a2d/2848/index.html?url=1936e6cf

議事録の内容につきまして
修正事項がございましたらご連絡をお願いいたします。

以上、宜しくお願い致します。

【図 39】配信本文（2 回目）：取引先からの見積書と偽り、本文記載の URL に誘導する手口

差出人: eigyo@japan-news-com.jp　　送信日時: 2019/12/13 (金) 16:20
宛先: ntt_cybersecurity_helpteam-ml@east.ntt.co.jp
ＣＣ:
件名: 御見積のご送付

NTT 東日本　新潟支店　様

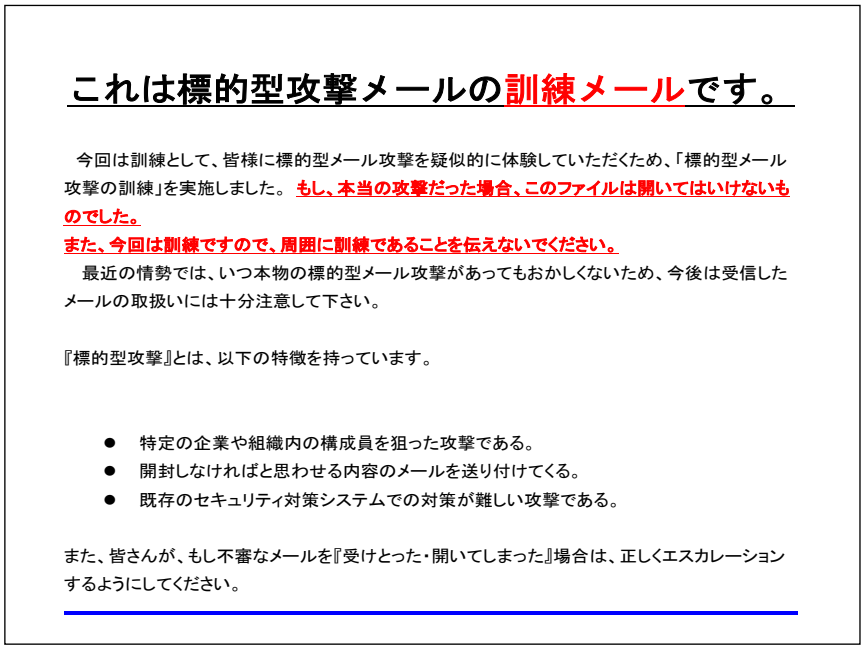
お世話になっております。

先日ご依頼頂いた内容について、見積書を作成しましたのでお送りいたします。
内容などに問題がないか、ご確認のほど、よろしくお願い致します。
http://japan-news-com.jp/7cf05952f30e430/3439/index.html?url=1936e6cf

見積の内容について、問題ないかご確認をお願いいたします。
ご不明な点がございましたらご連絡をお願いいたします。

以上、宜しくお願い致します。

【図 40】URL 開封時画面（共通）



これは標的型攻撃メールの訓練メールです。

今回は訓練として、皆様に標的型メール攻撃を疑似的に体験していただくため、「標的型メール攻撃の訓練」を実施しました。**もし、本当の攻撃だった場合、このファイルは開いてはいけないものでした。**
また、今回は訓練ですので、周囲に訓練であることを伝えないでください。
最近の情勢では、いつ本物の標的型メール攻撃があってもおかしくないため、今後は受信したメールの取扱いには十分注意して下さい。

『標的型攻撃』とは、以下の特徴を持っています。

- 特定の企業や組織内の構成員を狙った攻撃である。
- 開封しなければと思わせる内容のメールを送り付けてくる。
- 既存のセキュリティ対策システムでの対策が難しい攻撃である。

また、皆さんが、もし不審なメールを『受けとった・開いてしまった』場合は、正しくエスカレーションするようにしてください。

② 標的型攻撃メール訓練結果

メール訓練（1 回目・2 回目）の実施の結果、平均開封率は下がっているものの、2 回ともに開封した件数が半分を占めている。

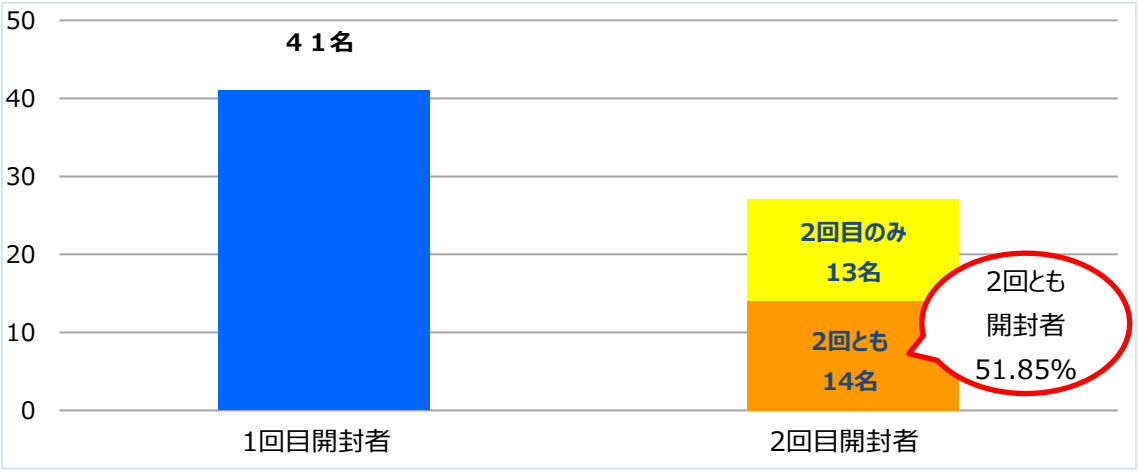
【図 41】標的型攻撃メール訓練開封結果

1 回目

人員数	開封者数	未開封者数	開封率
198	41	157	20.71%

2 回目

人員数	開封者数	未開封者数	開封率
198	27	171	13.64%

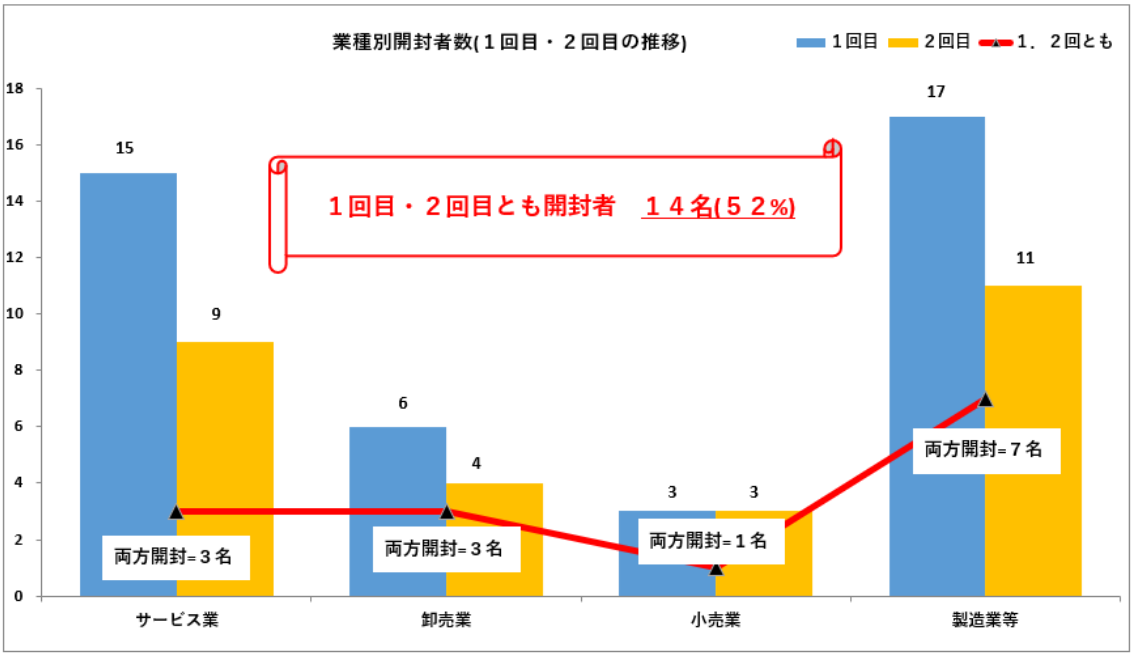


【表 13】標的型攻撃メール訓練結果（業種別）

		1 回目		2 回目		1・2 回とも*	
業種名	人員数	開封者数	開封率	開封者数	開封率	開封者数	開封率
サービス業	50	15	30.00%	9	18.00%	3	33.33%
卸売業	30	6	20.00%	4	13.33%	3	75.00%
小売業	25	3	12.00%	3	12.00%	1	33.33%
製造業等	93	17	18.28%	11	11.83%	7	63.64%
全体	198	41	20.71%	27	13.64%	14	51.85%

*分子＝1・2 回とも開封/分母＝2 回目に開封

【図 42】標的型攻撃メール訓練業種別開封者数

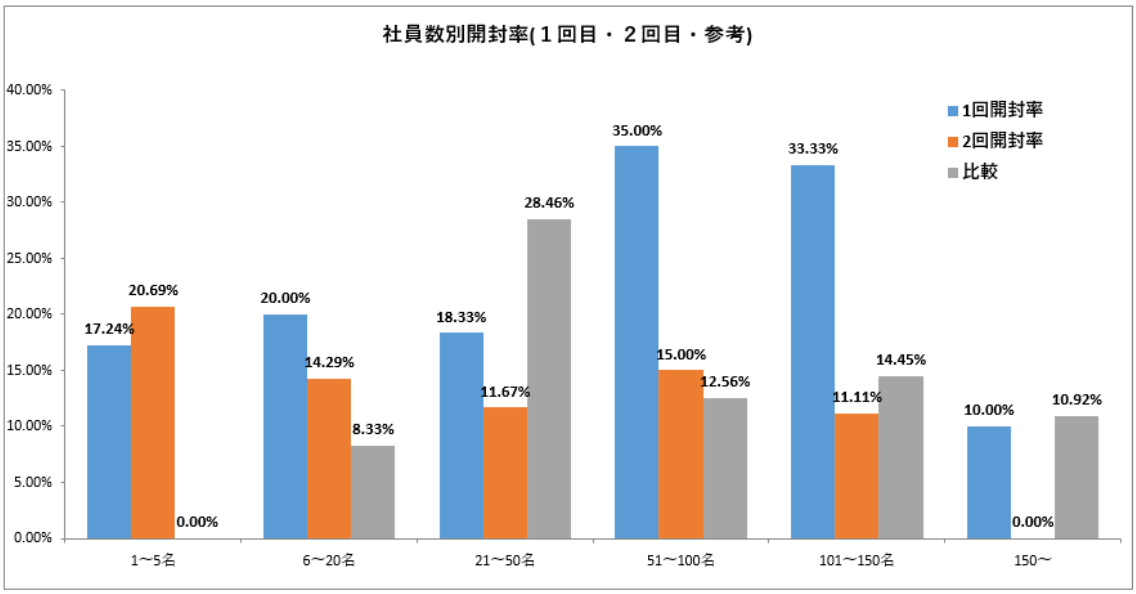


【表 14】標的型攻撃メール訓練結果（規模（社員数）別）

規模別（社員数）	開封率			参加会社数	参加人数	開封数	
	1 回	2 回	参考平均*			1 回目	2 回目
1～5 名	17.24%	20.69%	0.00%	25	29	5	6
6～20 名	20.00%	14.29%	8.33%	55	70	14	10
21～50 名	18.33%	11.67%	28.46%	44	60	11	7
51～100 名	35.00%	15.00%	12.56%	12	20	7	3
101～150 名	33.33%	11.11%	14.45%	5	9	3	1
150～	10.00%	0.00%	10.92%	6	10	1	0
合計	20.71%	13.64%	–	147	198	41	27

*サービスの開発ベンダである NTT 東日本のグループ会社が実施した実績の平均開封率

【図 43】標的型攻撃メール訓練社員数別開封者数



③　標的型攻撃メール訓練を体験した方の声

【表 15】標的型攻撃メール訓練を体験した方の声

メール開封状況		体験した方の声
メールを開封した	1 回目	■ 元請会社との打ち合わせ後、議事録を待っていたところにそれに似た内容の訓練メールが来たため開封してしまった。 ■ 何のメールかわからなかったが、特に危ないとは思わず開封してしまった。
	1・2 回とも	■ 無意識に開封してしまった。 複数で共有しているアドレスのため、自分に関係あるのかを確認してしまった。 ■ メールに日時等を指定する文章があり、返事をする必要があると思って開封してしまった。
1 回目は開封したが、 2 回目は開封しなかった		■ 開封してしまった前回の訓練メールと類似する点があり、怪しいと思い開封しなかった。 ■ 最初は無用心に開封してしまったが、さすがに一回目で学習した。
メールを開封しなかった		■ 誰も身に覚えのないアドレスからのメールだったため、開封しなかった。 普段から知らない送り主や名前が明記されていないメールは開かないようにしている。 ■ 日頃より社内の IT 担当者がメールの危険性を周知しており、無関係のメールは開封しないようにしている。 普段から用心深く、“怪しいメール”が届くと社内エスカレーションするようにしている。

④　考察

全 2 回の標的型攻撃を想定したメール訓練を実施し、当初約 20%の開封率から、約 14%まで減少した。今回の実証では、実際に疑似メールの受信を抜き打ちで体験することで巧妙なメールの手口を知り、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。

今回 2 回の訓練を実施したが、四半期に 1 回など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。また、疑似メールの訓練実施だけでなく、怪しいメールについては開封前に社内で共有・エスカレーションするルールを決めるなど個人だけで対処せず、企業・部署など全体での対策を講じる必要がある。

(5) 実証期間中のトピック（Emotet）

2019 年 10 月 Emotet の感染が急増した。これを受けて JPCERT コーディネーションセンターは、「マルウェア Emotet の感染に関する注意喚起」を出している。

（https://www.jpcert.or.jp/at/2019/at190044.html）

トレンドマイクロの資料によると、10 月の国内における Emotet 検出が 1,700 と前月の 20 倍近くに増加している。11 月に入り減少傾向であるが９月以前と比べて高水準であり再び攻撃が拡大するリスクがあり注意が必要である。

【図 44】国内における EMOTET 検出状況

出典：トレンドマイクロ「国内で拡大する EMOTET の脅威」

＜Emotet の感染フロー＞

添付ファイル（不正マクロを含む Word 等）付きメールが着信し、添付ファイルを開き「コンテンツを有効化」することで Emotet がダウンロードされる。感染後、メールの内容、メールアドレス等のデータを収集され、データが不正サーバに送信される。

＜Emotet の拡散＞

収集したデータをもとに Emotet を仕込んだスパムメールを発信することで拡散する。

（図 45 参照）

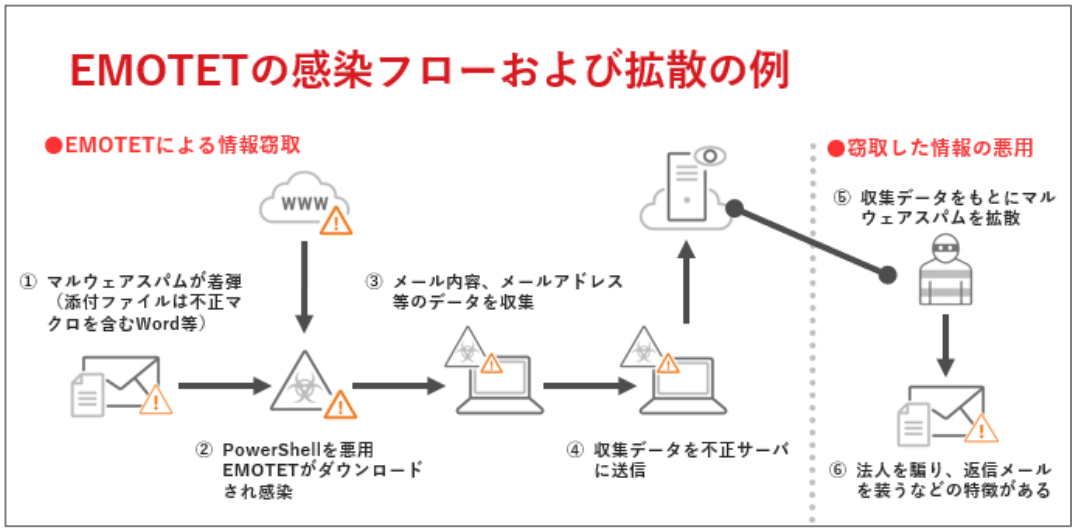
＜Emotet の主な機能＞

- マルウェア「TRICKBOT」やランサムウェア「RYUK」等をダウンロードし感染させる
- リモートからコマンドの実行が可能（遠隔操作）
- 複数のメールクライアントのユーザ名、パスワード等を窃取
- スパムメールの送信

- 端末内のデータ、コンピュータ名、OS バージョン、動いているプロセス情報等を窃取
- 利用者アカウントの認証情報窃取
- ネットワーク内での感染拡大

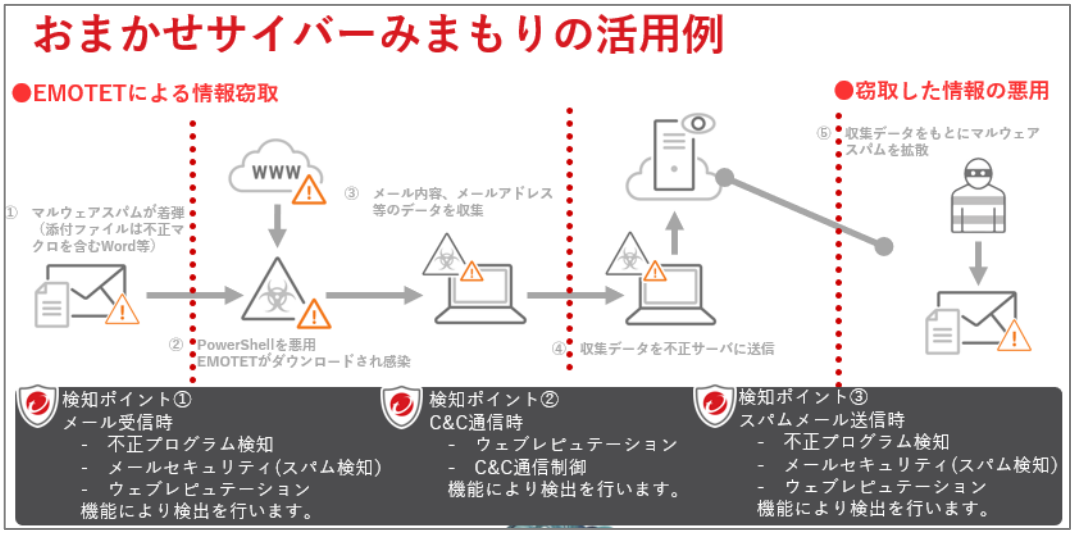
出典：トレンドマイクロ「国内で拡大する EMOTET の脅威」

【図 45】Emotet の感染フローおよび拡散の例



出典：トレンドマイクロ「国内で拡大する EMOTET の脅威」

【図 46】「おまかせサイバーみまもり」による Emotet の検出



出典：トレンドマイクロ「国内で拡大する EMOTET の脅威」

(6) 実証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（企業活動継続リスク等）

① 対応費用の発生

サイバーセキュリティ脅威が発生した場合、対応にかかる費用は以下が考えられる。

【表 16】サイバーセキュリティ脅威が発生した場合の対応費用（例）

費用項目		具体例	脅威例
初動対応費用 復旧・再発防止費用	社外委託費用	■ 専門調査機関に依頼する調査費用 ■ データ・システム復旧費用	不正アクセス マルウェア感染
	社内超過人件費	システム担当者等が初動～システム復旧までにかかる超過勤務時間分の人件費	
取引先対応費用	社外委託費用	（取引先数が多い場合）コールセンター設置費用	情報漏えい
	社内超過人件費	取引先対応にかかる担当者等の超過勤務時間分の人件費	
訴訟・賠償費用		■ 弁護士費用 ■ お詫び費用（お詫び状の発送・金券の配布など） ■ 賠償金支払い	情報漏えい

② 企業活動継続に及ぼす影響

サイバーセキュリティ脅威の発生によりシステム等が停止した場合、企業活動への影響は以下が考えられる。

【表 17】システム停止が企業活動に及ぼす影響（例）

停止するシステム等の種類	企業活動に及ぼす影響（例）
基幹システム	■ 発注・生産・販売・会計等業務の停止 ■ システムが利用できず、アナログで対応することによる業務効率の悪化
制御システム	■ 受注停止による売上減 ■ 納期遅れによる信用の低下、契約打ち切り
EC サイト	■ EC サイト停止期間中の売上減 ■ 顧客離れによる売上減

③　サプライチェーンに及ぼす影響

サイバーセキュリティ脅威が発生した場合、サプライチェーンに及ぼす影響は以下が考えられる。

- 自社を踏み台に発注元の大企業が攻撃を受ける
- システムの停止により期限までに製品を納品できない
- マルウェア感染した製品を納品する
- 発注元より預かった情報が漏えいする

(7) 中間報告会

本実証の中間報告会を以下の通り実施した。

＜開催日時＞

2019 年 10 月 31 日（木）15：00～17：00

＜開催場所＞

新潟駅前会場（新潟駅前貸し会議室）

＜参加者数＞

17 名

＜集客方法＞

- 支店営業担当者による誘引（チラシ配布）
- 参加企業に向けたメールの案内

＜プログラム＞

第 1 部「中小企業向けサイバーセキュリティセミナー」

- 忍び寄るサイバー犯罪の脅威 その手口と対策について
  講師：トレンドマイクロ
- サイバーセキュリティ対策サービスのご紹介
  講師：NTT 東日本
- サイバーリスク保険のご紹介
  講師：東京海上日動

第 2 部「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」中間報告

- 実証結果から見る、新潟県内のサイバーセキュリティの脅威状況について
  講師：NTT 東日本
- 中小企業における情報セキュリティ対策支援のご紹介
  講師：IPA

(8) 最終報告会

本実証の最終報告会を以下の通り実施した。

＜開催日時＞

2020 年 2 月 5 日（水）15：00～17：15

＜開催場所＞

新潟駅前会場（新潟駅前ホテル）

＜参加者数＞

130 名（定員 130 名）

＜集客方法＞

- 参加企業に向けたメールの案内
- 支店営業担当者による誘引（チラシ配布）
- 東京海上日動ユーザへの案内
- メルマガ利用の新潟県内の企業への案内

＜プログラム＞

第 1 部「中小企業向けサイバーセキュリティセミナー」

- 開会挨拶
  NTT 東日本
- 忍び寄るサイバー犯罪の脅威 その手口と対策について
  講師：トレンドマイクロ
- サイバー犯罪の実態
  講師：新潟県警察本部

第 2 部「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」最終報告

- 実証結果から見る。新潟県内のサイバーセキュリティの脅威状況について（実証事業最終報告）
  講師：NTT 東日本
- 中小企業向けサイバーセキュリティ対策と保険サービスについて
  講師：NTT 東日本・東京海上日動
- 中小企業における情報セキュリティ対策支援のご紹介
  講師：IPA

6. 実証後のアンケート結果

サイバーセキュリティ脅威に対する事前対策・事後対応（復旧・補償）、企業内啓発策の導入・実施に向けての障壁把握（金銭的要因、技術的要因）、実証後の企業における社員意識の変化を調査することを目的に実証後にアンケートを実施した。本アンケートに基づき次項以降に、中小企業に必要な対策、マネジメント、保険について考察する。

(1) アンケート内容

＜対象者＞実証参加企業

＜回答者数＞　124 社（148 社に依頼したうちの回答数）

＜実施期間＞　11 月下旬～1 月上旬

＜実証後アンケート内容＞

Q1.　実証事業期間終了後もサイバーセキュリティ対策に関心をお持ちですか
1.　すぐにでも、検討しようと思った
2.　とても関心があり、いずれ検討しようと思った
3.　関心はあるが、検討するかは分からない
4.　関心はない

Q2.　セキュリティ対策に際しての、あなたご自身の立場をお教えください。（ひとつだけ）
1.　社内への導入を承認する立場
2.　社内への導入を提案する立場
3.　社内で利用する立場
4.　その他（　　）

Q3.　オリンピック開催に向けてセキュリティリスクが高まっていることをご存知ですか
1.　よく知っていて、対策も打っている
2.　よく知っているが対策は未実施
3.　あまり知らない
4.　聞いたことがない

Q4.　ご存知のセキュリティ脅威がございましたらお答え願います（いくつでも）
1.　標的型攻撃による被害
2.　ビジネスメール詐欺による被害
3.　ランサムウェアによる被害
4.　サプライチェーンの弱点を悪用した攻撃の高まり
5.　内部不正による情報漏えい
6.　サービス妨害攻撃によるサービスの停止

7. インターネットサービスからの個人情報の窃取
8. IoT 機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい

Q5. 貴社で過去実際に被害やインシデントがありましたらお答え願います（いくつでも）
1. 標的型攻撃による被害
2. ビジネスメール詐欺による被害
3. ランサムウェアによる被害
4. サプライチェーンの弱点を悪用した攻撃の高まり
5. 内部不正による情報漏えい
6. サービス妨害攻撃によるサービスの停止
7. インターネットサービスからの個人情報の窃取
8. IoT 機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい

Q6. 貴社で脅威に感じているリスクがあると思うものがありましたらお答え願います（いくつでも）
1. 標的型攻撃による被害
2. ビジネスメール詐欺による被害
3. ランサムウェアによる被害
4. サプライチェーンの弱点を悪用した攻撃の高まり
5. 内部不正による情報漏えい
6. サービス妨害攻撃によるサービスの停止
7. インターネットサービスからの個人情報の窃取
8. IoT 機器の脆弱性の顕在化
9. 脆弱性対策情報の公開に伴う悪用増加
10. 不注意による情報漏えい
11. その他（ ）

Q7. 実証期間中にご利用いただきましたセキュリティ対策（UTM・メール訓練）以外で、貴社で導入しているセキュリティ対策をお教えください（いくつでも）
1. ウイルス対策ソフト
2. 出入り口対策（UTM 等）
3. 社員教育（e-ラーニング・社内外の研修参加等）
4. セキュリティ管理者の設置

5. セキュアな無線 LAN 環境（Wi-Fi）
6. セキュアな拠点間通信
7. サイバーリスク保険
8. データレスな PC 環境
9. HP など Web のセキュリティ脆弱診断
10. MDM（モバイル端末管理）

Q8. 上記（Q7）で出入り口対策を導入していない方にお聞きします
導入に至らない理由があればお答えください（いくつでも）

1. 必要だと感じないから
2. 対策することについて知らなかった
3. 必要だとは思うが価格がおりあわない
4. 導入するための知識がない
5. 導入するための担当者がいない
6. 相談するシステムベンダがいない
7. その他（ ）

Q9. 上記（Q8）で「必要だが価格がおりあわない」と答えた方にお聞きします
どのくらいの価格であれば導入を検討できますか

1. 4,999 円以下
2. 5,000 円～9,999 円以下
3. 10,000 円～14,999 円
4. 15,000 円以上
5. 不明

Q10. 今後、以下のセキュリティ対策を実施することを検討していますか（いくつでも）

1. ウイルス対策ソフト
2. 出入り口対策（UTM 等）
3. 社員教育（e-ラーニング・社内外の研修参加等）
4. セキュリティ管理者の設置
5. セキュアな無線 LAN 環境（Wi-Fi）
6. セキュアな拠点間通信
7. サイバーリスク保険
8. データレスな PC 環境
9. HP など Web のセキュリティ脆弱診断
10. MDM（モバイル端末管理）

Q11. 今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか。

1. 5000 円～10000 円
2. 10000 円～5 万円
3. 5 万円～
4. 費用はかけない

Q12. 現在、セキュリティ対策について相談できる相手はいますか

1. いる
2. いない

Q13. 上記（Q12）で（1）いると答えた方にお聞きします
相談相手はどのような方ですか

1. システムベンダ
2. 社外の有識者（税理士や電話業者、詳しい知人）
3. その他（　　）

Q14. インシデント発生した際に、ご相談できる相手はいますか

1. いる
2. いない

Q15. 上記（Q14）で（1）いると答えた方にお聞きします
相談相手はどのような方ですか

1. システムベンダ
2. 社外の有識者（税理士や電話業者、詳しい知人）
3. その他（　　）

Q16. 現在貴社で業務上当てはまるものについてご解答願います（いくつでも）

1. ファイル共有やデータ保管のため、USB の使用をしている
2. 従業員が私用の PC・タブレットを利用し業務にあたっている
3. 有事の際を想定し、データのバックアップを実施し復旧または対処できるようにしている
4. お客様情報や機密情報の持ち出しの際には社内で管理簿をつけている

Q17. 標的型攻撃メールの擬似訓練を実施し、なりすましメールの脅威について意識の変化はありましたか

1. 脅威を感じ、意識に変化があった
2. 脅威は感じたが、意識に変化はない

3. 特になにも感じない

Q18. 貴社のお取引企業様より、取引をする上でのセキュリティ対策の方針の要件やルールの提示はありますか
例 1：業務提携や発注・請負契約をする際の条件として、全 PC に出入り口対策の実施とウイルスソフトを導入しておりセキュリティ対策を実施
例 2：データの持ち出しや流出を防ぐために USB の利用を禁止　等
1. ある
2. ない
3. 不明

Q19. 情報漏えいやシステム停止などのインシデントが発生した場合の対応（役割・手順・連携先等）を決めていますか
1. 決めている
2. 決めていない
3. 検討中

Q20. 情報漏えいやシステム停止などのインシデントが発生した場合の事業への影響（影響の範囲、対応にかかる費用や労力、売上への影響等）を想定していますか。想定しているものにチェックしてください。
1. 影響の範囲（親会社・サプライチェーンなど）
2. 対応にかかる費用（システム復旧等）
3. 対応にかかる労力（人件費）
4. 売上・事業への影響
5. その他（　　）

Q21. 情報漏えいやシステム停止などのインシデントが発生した場合にかかる費用の予算を確保または検討していますか
1. 予算を確保している
2. 今後予算を確保する予定
3. 保険に加入している
4. 保険の加入を検討している
5. していない

Q22. サイバーリスクに備えた保険があることを知っていますか
1. 知っていた
2. 知らなかった

Q23. サイバーリスクに備えた保険について、どのようなサービスがあれば検討ができますか

1. セキュリティ対策追加費用の補填
2. インシデント発生時のお見舞金
3. 復旧費用に関わる費用負担
4. 原因特定に向けた調査費用
5. UTM や標的型攻撃メール訓練機能の提供ができるオプション

Q24. 本実証事業の参加を通じて、サイバーセキュリティに関する意識は変わりましたか

1. 大きく意識が向上した
2. 少し意識が向上した
3. 特に変わらない

Q25. SECURITY ACTION（セキュリティ対策自己宣言）を知っていますか

1. 知っており、宣言している
2. 知っているが、宣言していない
3. 知らない

Q26. Q25 で＜1.知っており、宣言している＞とお答えいただいた方にお聞きします
どこまで宣言されておりますか

1. 一つ星登録済み
2. 二つ星登録済み

Q27. Q25 で＜2.知っているが、宣言していない／3.知らない＞とお答えいただいた方にお聞きします
今後宣言される予定はありますか

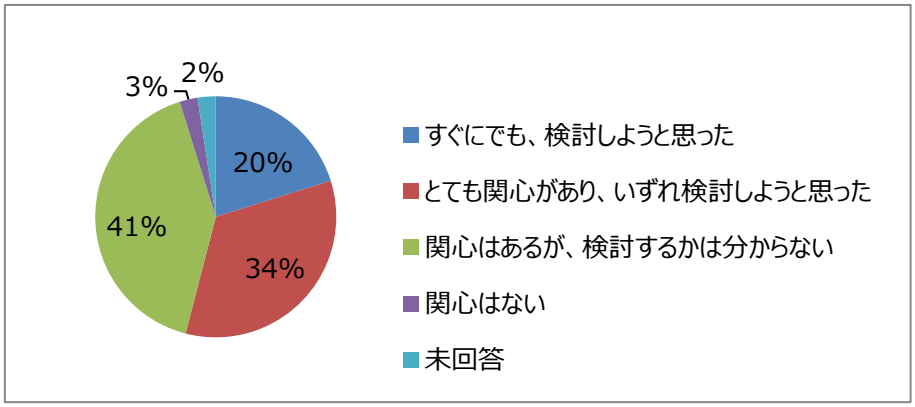
1. 一つ星登録まで実施したい
2. 二つ星登録まで実施したい
3. 登録しない

(2) アンケート結果（集計）

① サイバーセキュリティ対策への関心

サイバーセキュリティへの関心があると回答した企業は 124 社中 118 社と全体の 95%を占めた。すぐにでも、検討しようと思ったと回答した企業は全体の 20%であった。

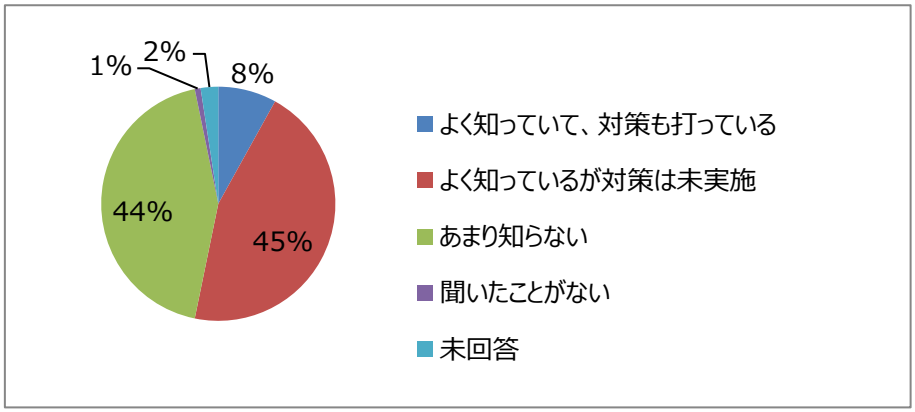
【図 47】Q1.実証事業期間終了後もサイバーセキュリティ対策に関心をお持ちですか



② オリンピック開催に向けたセキュリティリスクの高まり

オリンピック開催に向けてサイバーセキュリティリスクが高まっていることの認知度は低く、約半数の企業が「あまり知らない」または「聞いたことがない」と回答、「よく知っていて、対策も打っている」と回答した組織は 8%に留まった。

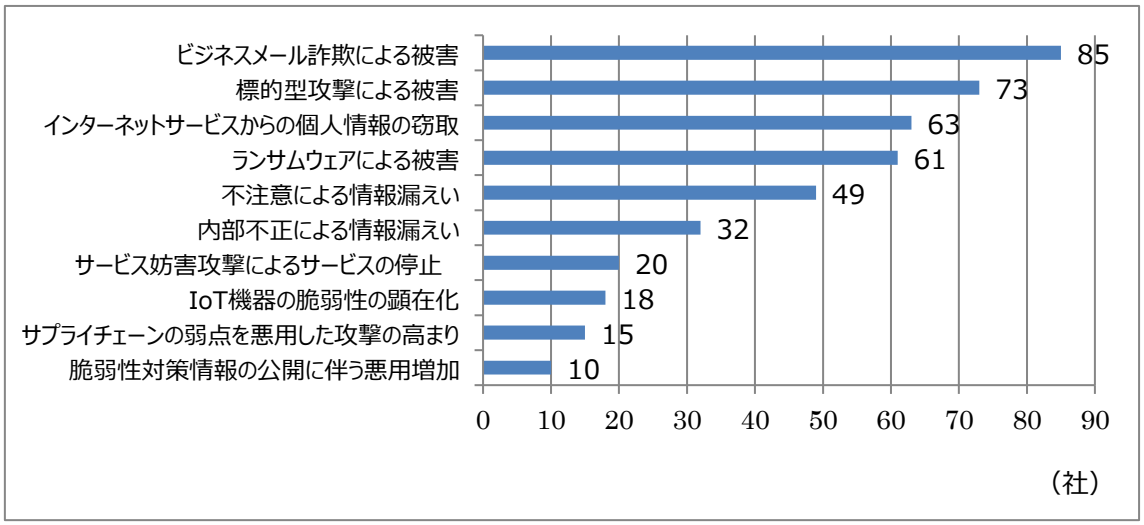
【図 48】Q3.オリンピック開催に向けてセキュリティリスクが高まっていることをご存知ですか



③　脅威の認識

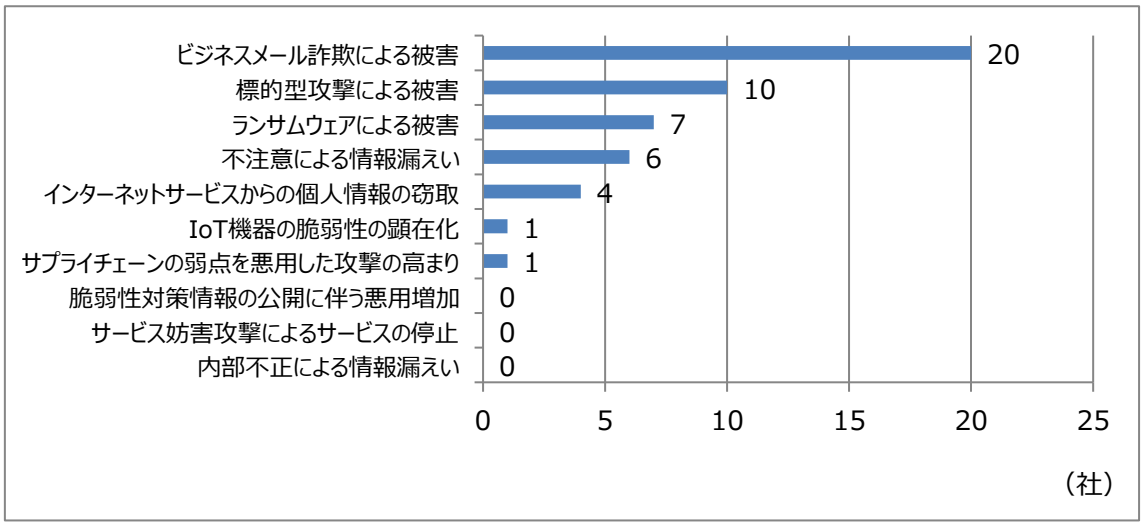
IPA が毎年発表する「10 大脅威」の中で、知っているセキュリティ脅威の 1 位は「ビジネスメール詐欺による被害」であった。次いで、「標的型攻撃による被害」、「インターネットサービスからの個人情報の窃取」と続いている。

【図 49】Q4.ご存知のセキュリティ脅威がございましたらお答え願います（いくつでも）



自社に被害がある脅威の 1 位は、知っているセキュリティ脅威と同様「ビジネスメール詐欺による被害」であった。次いで「標的型攻撃による被害」「ランサムウェアによる被害」と続いている。

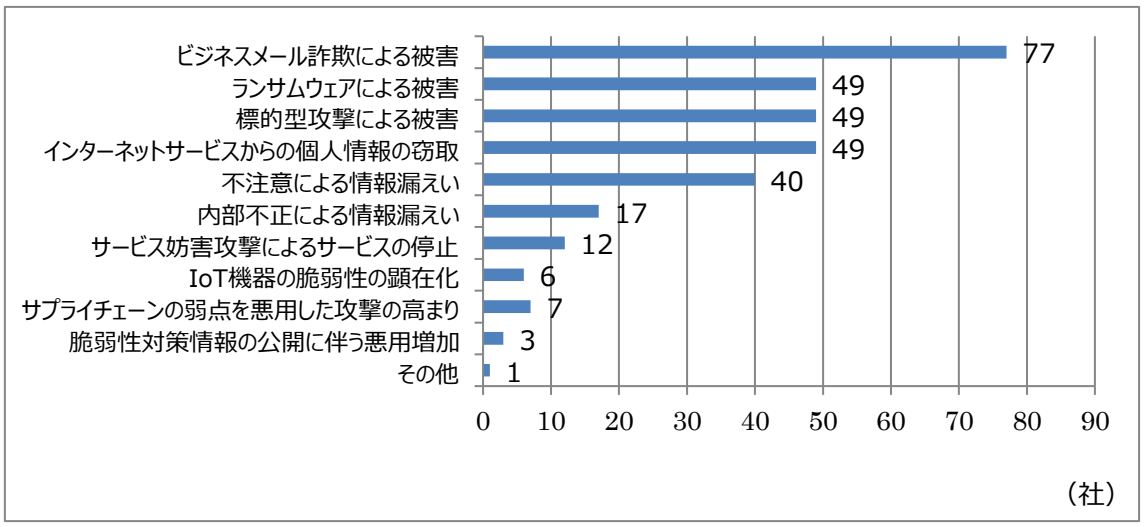
【図 50】Q5.貴社で被害のあるセキュリティ脅威がありましたらお答え願います（いくつでも）



脅威に感じているリスクの 1 位は、同じく「ビジネスメール詐欺による被害」であった。次いで、「ランサムウェアによる被害」「標的型攻撃による被害」、「インターネットサービスからの個人情報の窃取」が同数となっ

ている。

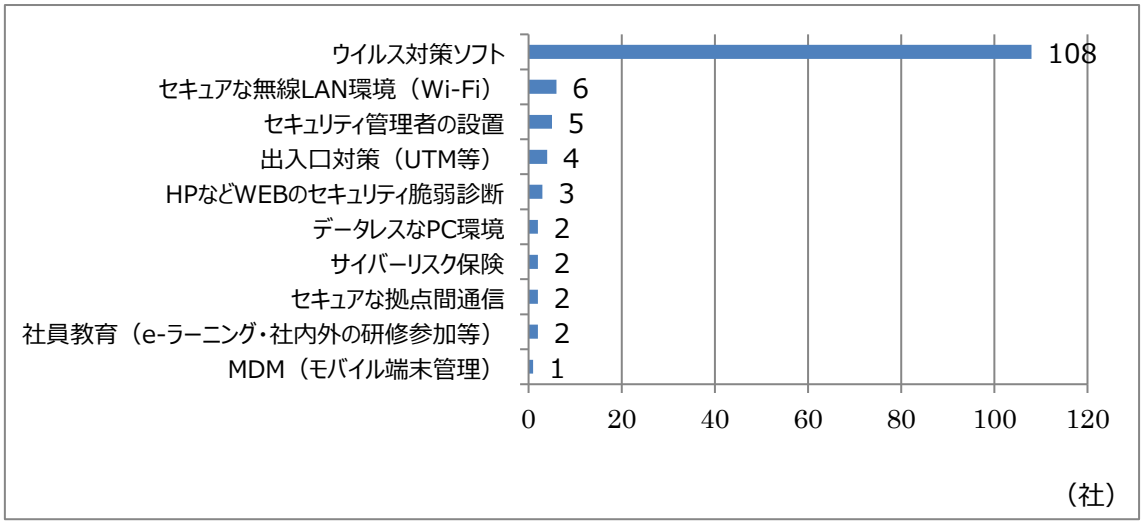
【図 51】Q6.貴社で脅威に感じているリスクがあると思うものがありましたらお答え願います（いくつでも）



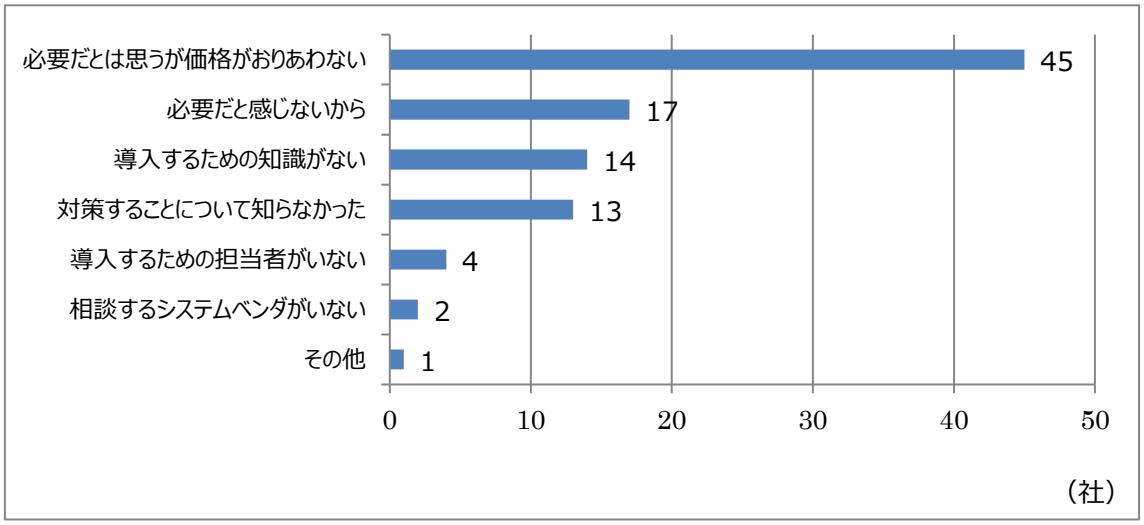
④　導入しているセキュリティ対策

導入しているセキュリティ対策（実証期間中に利用いただいたセキュリティ対策を除く）は、1 位が「ウイルス対策ソフト」で 108 社、全体の約 90%が導入している。次いで、「セキュアな無線 LAN 環境」「セキュリティ管理者の設置」と続くが、どちらも全体の 5%以下に留まっている。「出入り口対策（UTM 等）」を導入している企業は 4 社にとどまった。導入していない理由の 1 位は「必要だとは思うが価格がおりあわない」で 30%以上を占めている。導入を検討できる価格帯は 4,999 円以下が半数を占め、次いで 5,000～9,999 円が 30%弱であった。

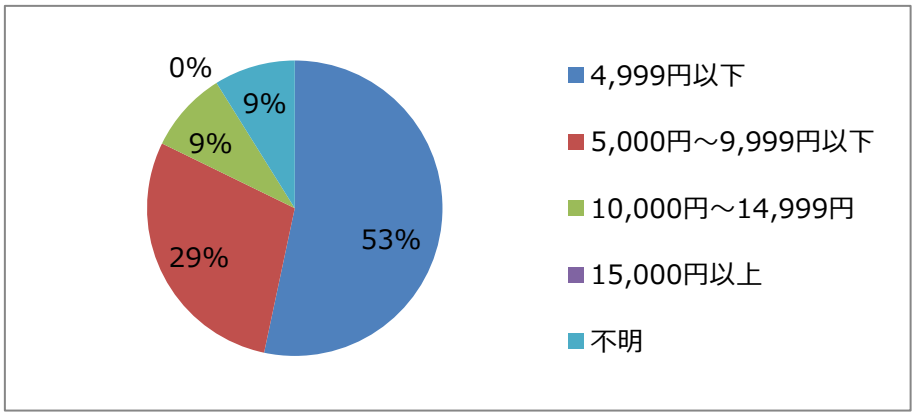
【図 52】Q7.実証期間中にご利用いただきましたセキュリティ対策（UTM・メール訓練）以外で、貴社で導入しているセキュリティ対策をお教えください（いくつでも）



【図 53】Q8.出入り口対策を導入していない方にお聞きします
導入に至らない理由があればお答えください（いくつでも）



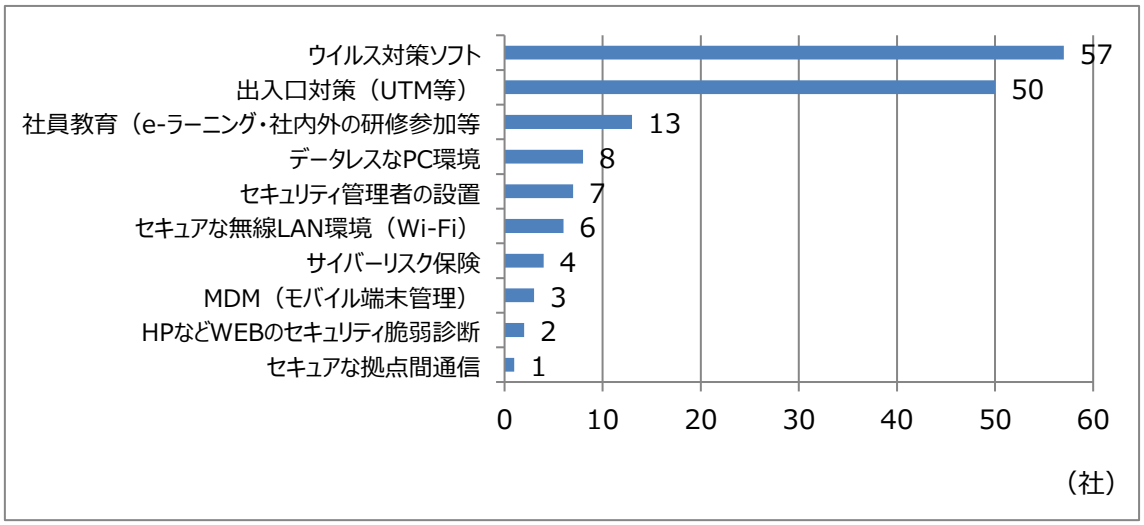
【図 54】Q9.「必要だが価格がおりあわない」と答えた方にお聞きします
どのくらいの価格であれば導入を検討できますか



⑤　検討しているセキュリティ対策

検討しているセキュリティ対策は、1 位が「ウイルス対策ソフト」次いで「出入り口対策」であった。（「ウイルス対策ソフト」の回答には、新規の導入だけでなく無料ソフトから有料ソフトへの切り替えの検討や適用範囲の拡大、バージョンアップ等のニーズを含む。）

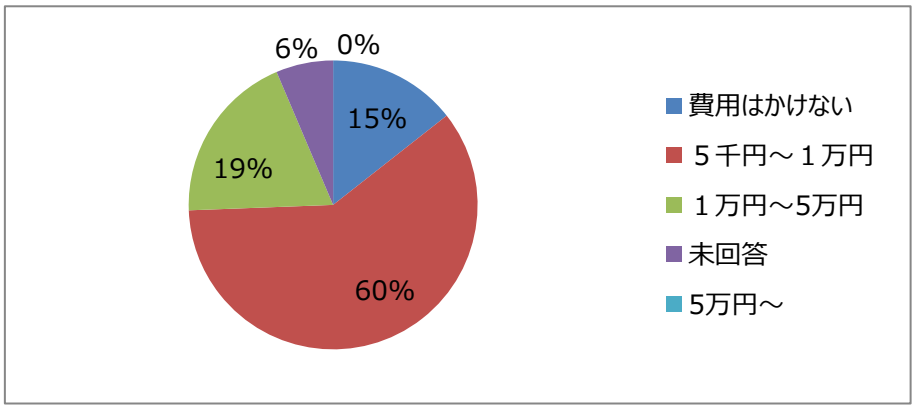
【図 55】Q10.今後、以下のセキュリティ対策を実施することを検討していますか（いくつでも）



⑥　セキュリティ対策にかける費用見込み

今後セキュリティ対策にかける月額費用の見込みは、5,000 円～10,000 円が 60%、次いで 10,000 円～5 万円が 20%弱であった。「費用はかけない」と回答した企業が全体の 15%、18 社あった。

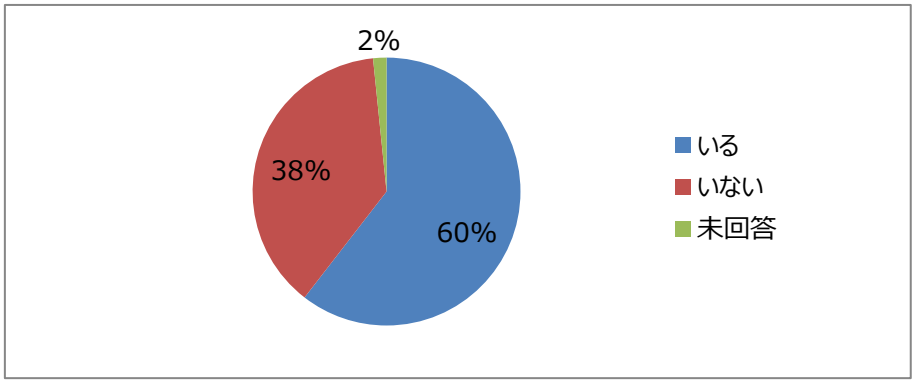
【図 56】Q11.今後セキュリティ対策にかける月額費用はいくらぐらいを見込んでいますか



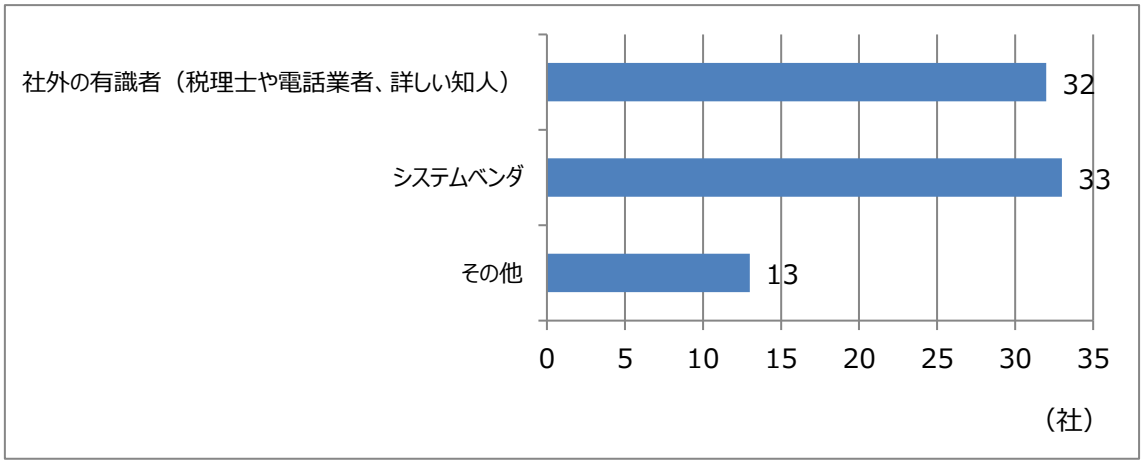
⑦　サイバーセキュリティに関する相談先

セキュリティ対策に関する相談相手がいると答えた企業は 60%、相談相手がいないと回答した企業が 38%であった。インシデント発生時の相談相手がいると答えた企業といないと答えた企業が約半数ずつであった。相談先は主に社外有識者またはシステムベンダであった。

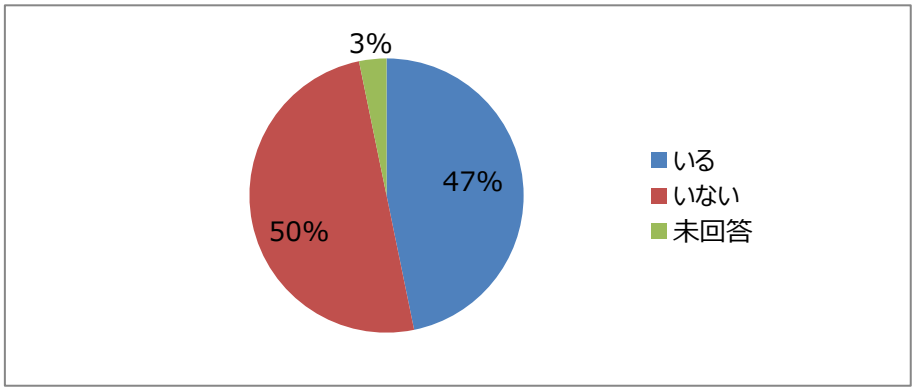
【図 57】Q12.現在、セキュリティ対策について相談できる相手はいますか



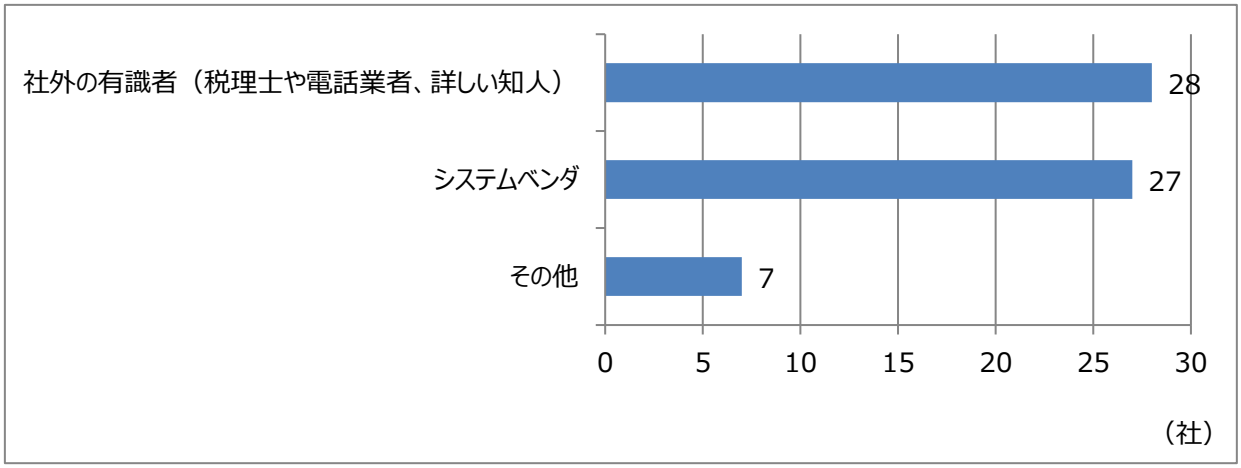
【図 58】Q13.「Q12」で「いる」と答えた方にお聞きします・相談相手はどのような方ですか



【図 59】Q14.インシデント発生した際に、ご相談できる相手はいますか



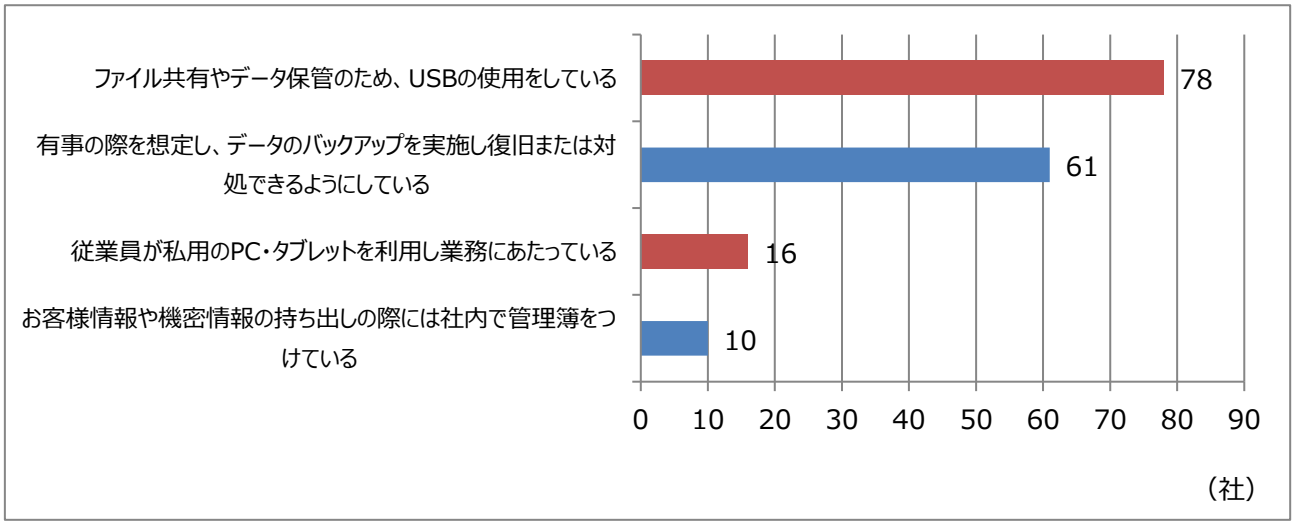
【図 60】Q15.「Q14」で「いる」と答えた方にお聞きします
相談相手はどのような方ですか



⑧　業務におけるサイバーリスク

業務においてサイバーリスクが高いと考えられる対応として、USB の使用について「使用している」と回答した企業が 78 社で全体の 63%、私用 PC やタブレットの利用は 16 社で全体の 13%であった。サイバーリスクを軽減する対応として「有事を想定し、データのバックアップを実施し復旧または対処できるようにしている」と回答した企業は 61 社で全体の 49%、取引先情報や機密情報の持ち出し管理を行っているのは 10 社で全体の 8%であった。

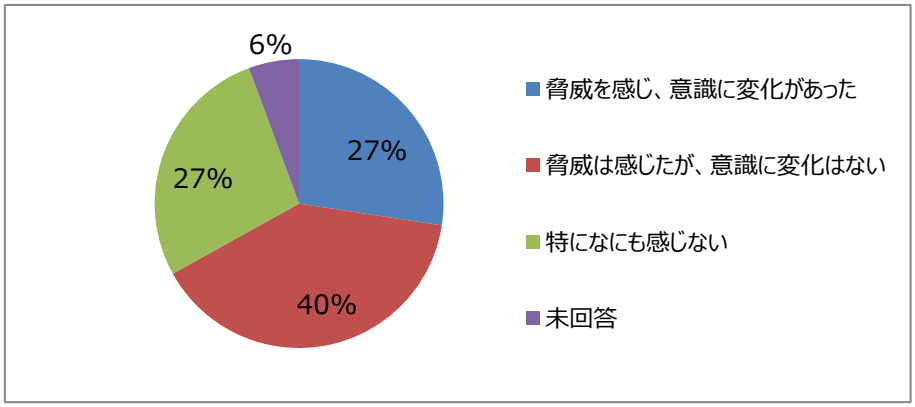
【図 61】Q16.現在貴社で業務上当てはまるものについてご回答願います（いくつでも）



⑨　標的型攻撃メール訓練実施後の意識の変化

標的型攻撃メール実施後、「脅威を感じ、意識に変化があった」と回答したのは 34 社で全体の 27%、「脅威を感じたが意識に変化はない」と回答したのが 49 社で全体の 40%であった。

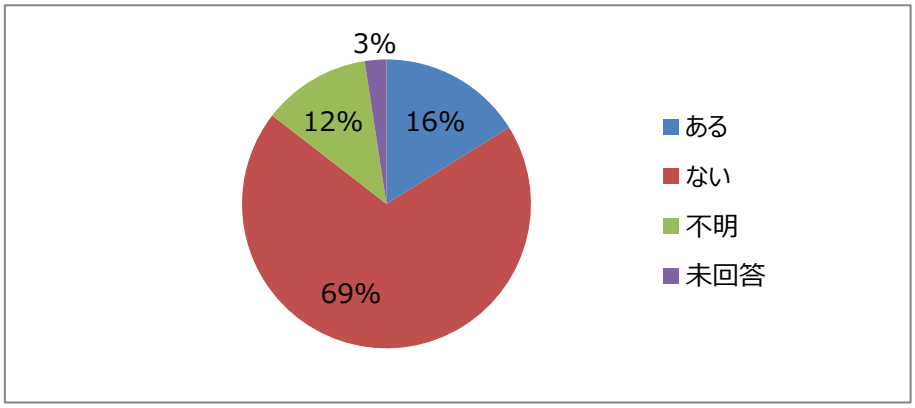
【図 62】Q17.標的型攻撃メールの擬似訓練を実施し、なりすましメールの脅威について意識の変化はありましたか



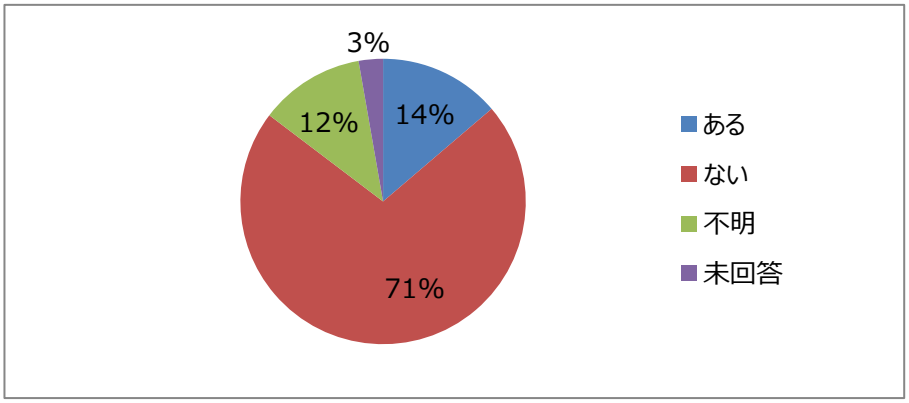
⑩　取引先からの要求

取引先企業から、セキュリティ対策の方針の要件やルールの提示が「ある」と回答した企業が 20 社で全体の 16%、「ない」と回答した企業が 86 社で全体の 69%であった。企業規模で比較すると、従業員数 50 名以下の企業のほうが、「ない」と回答した割合が高い。

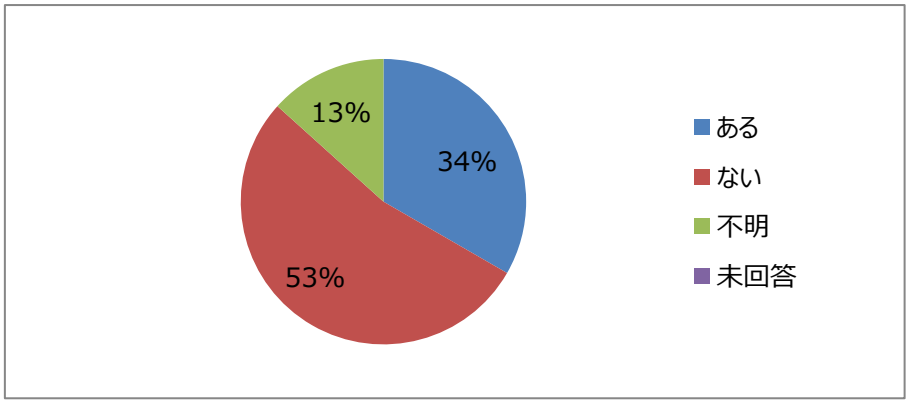
【図 63】Q18.貴社のお取引企業様より、取引をする上でのセキュリティ対策の方針の要件やルールの提示はありますか



【図 63-1】従業員 50 名以下企業の回答



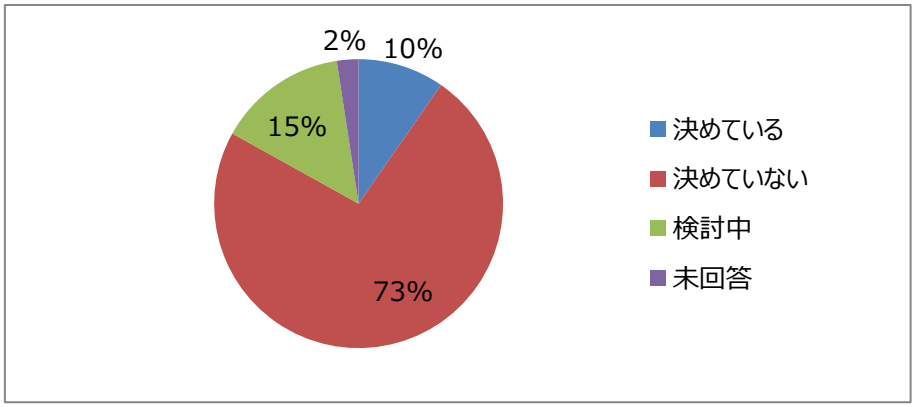
【図 63-2】従業員 51 名以上企業の回答



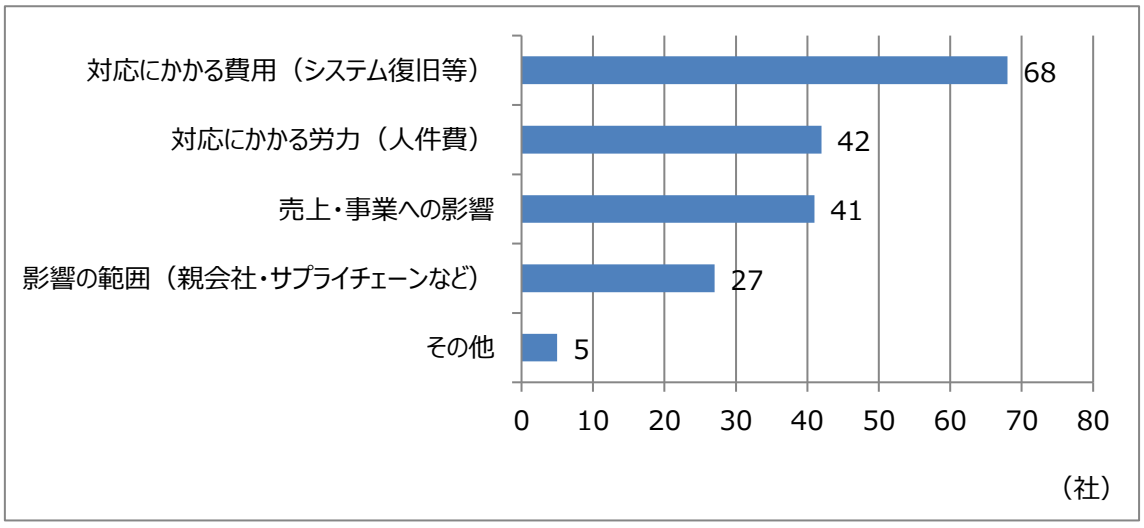
⑪　インシデント発生時の対応準備

インシデントが発生した場合の対応を決めていないと回答した企業が 91 社と全体の 73%であった。インシデント発生時の事業への影響を想定しているものの 1 位は「対応にかかる費用」、次いで「対応にかかる労力」「売上・事業への影響」であった。インシデント発生時にかかる費用の予算を確保している企業は 1 社、保険に加入している企業が 2 社、保険を検討している企業は 2 社にとどまった。90%を超える企業が予算の確保または検討をしていないと回答した。

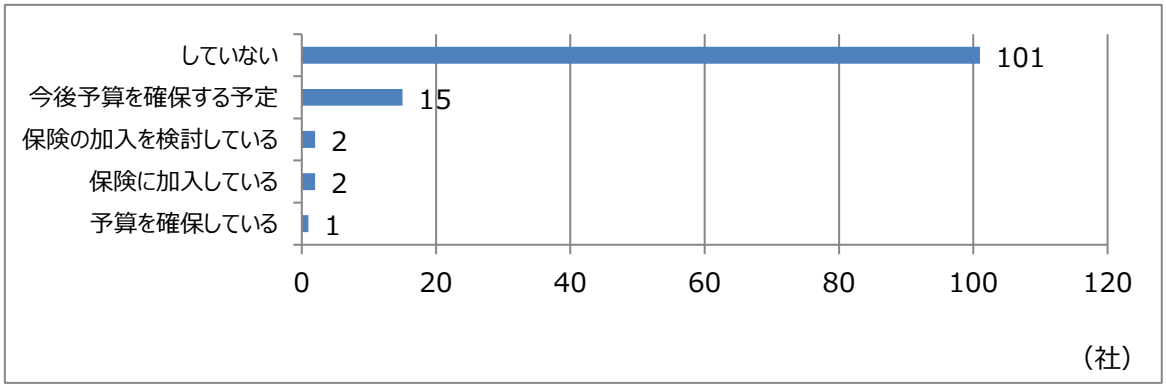
【図 64】Q19.情報漏えいやシステム停止などのインシデントが発生した場合の対応（役割・手順・連携先等）を決めていますか



【図 65】Q20.情報漏えいやシステム停止などのインシデントが発生した場合の事業への影響（影響の範囲、対応にかかる費用や労力、売上への影響）を想定していますか
想定しているものにチェックしてください



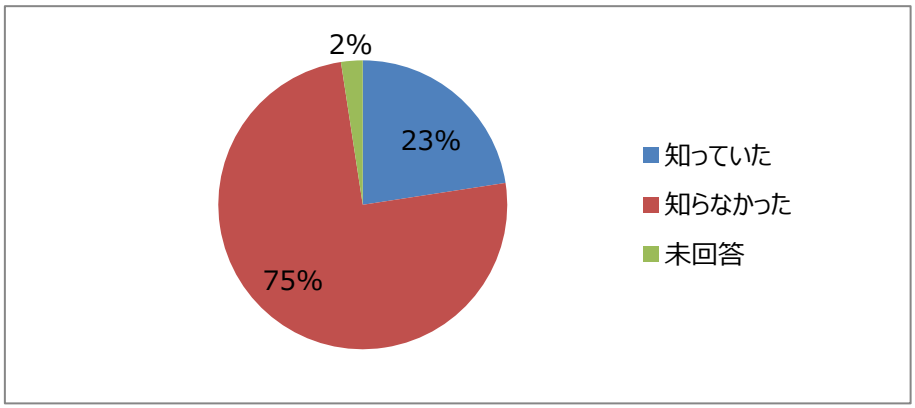
【図 66】Q21.情報漏えいやシステム停止などのインシデントが発生した場合にかかる費用の予算を確保または検討していますか



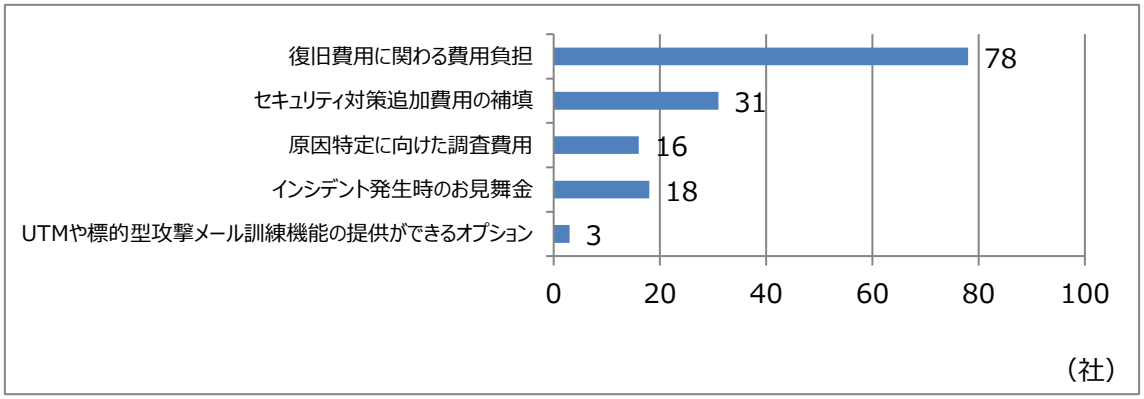
⑫　サイバーリスク保険について

サイバーリスクに備えた保険について、知っていると回答した企業は 28 社で全体の 23%、知らないと回答した企業は 90 社で全体の 75%であった。保険について、どのようなサービスがあれば検討できるかについては、「復旧費用に関わる費用負担」が 1 位、次いで「セキュリティ対策追加費用の補填」であった。

【図 67】Q22.サイバーリスクに備えた保険があることを知っていますか



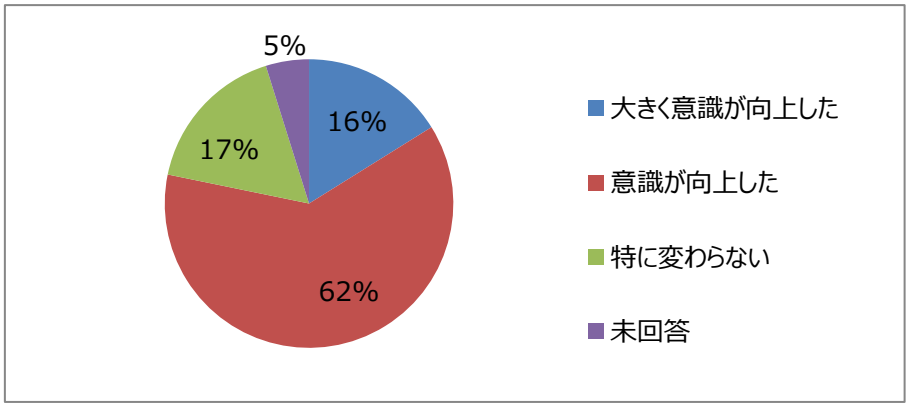
【図 68】Q23.サイバーリスクに備えた保険について、どのようなサービスがあれば検討ができますか



⑬　実証を通じた意識の変化

約 8 割の企業が、実証事業を通じてセキュリティ意識の向上が見られた。

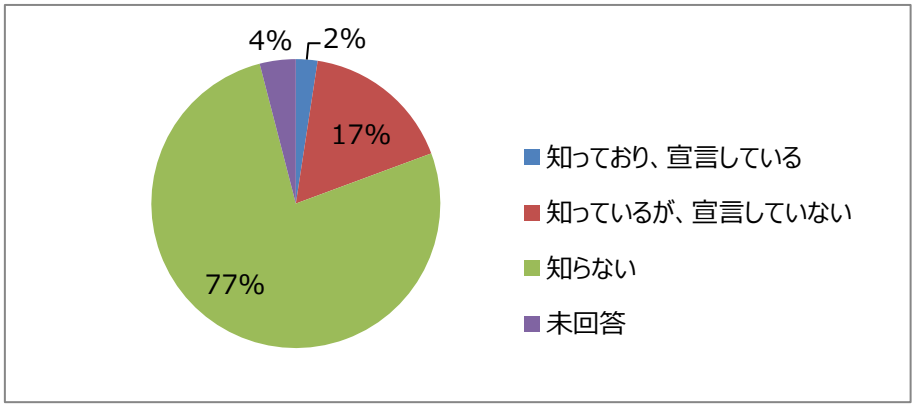
【図 69】Q24.本実証事業の参加を通じて、サイバーセキュリティに関する意識は変わりましたか



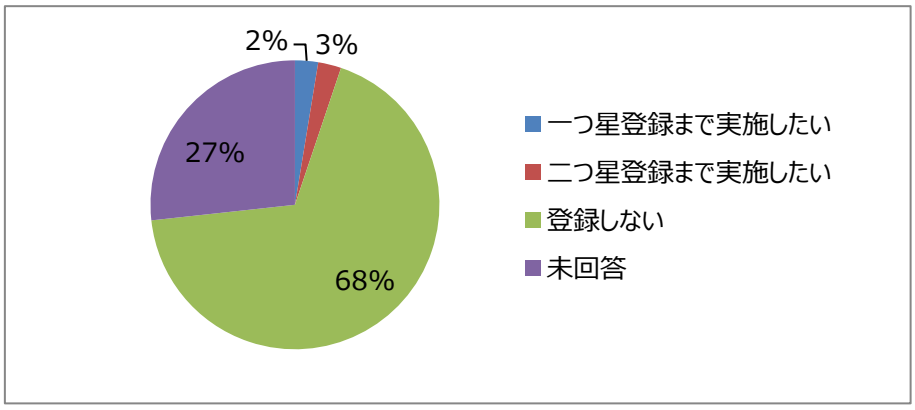
⑭　SECURITY ACTION について

SECURITY ACTION について知っている企業が 24 社で全体の 19%、そのうち一つ星を登録している企業は 3 社、二つ星を登録している企業はなかった。登録していない企業のうち、登録を希望する企業は 6 社であった。

【図 70】Q25.SECURITY ACTION（セキュリティ対策自己宣言）を知っていますか



【図 71】Q26.＜2.知っているが、宣言していない／3.知らない＞とお答えいただいた方にお聞きします。今後宣言される予定はありますか



(3) 考察（サイバー脅威に対する対策実施の障壁等）

実証実験後アンケート項目のうち、Q1・2・3・4・5・7・10・11・14 は事前アンケートと同種の質問項目である。実証前後の変化を確認するために行ったものであるが、回答に大きな変化は見られなかった。新たに追加したアンケート項目の回答結果より、中小企業のサイバーリスクの現状と対策実施の障壁等を以下の通り考察した。

＜対策実施の障壁＞

今回の実証において設置した UTM 等出入り口対策の導入に至らない理由について、「必要だとは思うが価格がおりあわない」と答えた企業が未導入企業の半数近くを占めた。検討可能な価格帯は 4,999 円以下が半数以上を占めており、中小企業にとって費用負担が導入の障壁となっていると考えられる。「必要だと感じない」または「対策することについて知らなかった」と回答した企業が約 3 割であった。これらの企業は、自社のリスクを正しく認識していない可能性があり、サイバーリスクについて理解を深める必要がある。「導入するための知識がない」「導入するための担当者がいない」「相談するシステムベンダがいない」との回答もあり、サイバーセキュリティ人材のいない企業にはサポートや相談できる先が必要である。

本実証において UTM を利用いただいた企業のうち、継続して利用する企業が半数近くであったことから、有用性の理解と導入のサポートにより導入検討が進む可能性があると考えられる。

＜インシデント発生を想定した対策状況＞

サイバー脅威に対する対策は出入り口対策をはじめとした技術的対策だけでなく、インシデント発生を想定した体制作りやインシデント発生にかかる費用の準備が必要となる。インシデント発生時の対応準備については、7 割以上の企業が「決めていない」と回答した。インシデント発生時にかかる費用を確保または検討している企業は少数であった。インシデント発生時の相談先も半数の企業が「ない」と回答している。まずは、サイバーインシデントが発生することを前提に被害の想定や必要な対応の検討が必要であることを知ってもらうことが重要と考えられる。また、サイバーリスクに備えた保険の存在を知らない企業が 7 割以上であったことから、保険についても必要性や役割を理解する機会が必要である。

＜業務におけるサイバーリスク＞

中小企業が業務を行う上でサイバーリスクを軽減する対応ができているかについて、USB の利用、取引先情報持ち出し管理、バックアップの取得、私用 PC の利用の 4 つの観点で確認した。

USB を使用していると回答した企業が 6 割以上であったが、USB の使用には、次のような危険性がある。

- 情報の持ち出しが容易であり、紛失、盗難のリスクが高い
- 内部犯行による情報の持ち出しに利用される可能性がある
- USB 経由でマルウェア感染する危険性がある

取引先情報や機密情報の持ち出し管理を行っている企業は 1 割未満であった。管理を行わないことによ

り、以下のような危険性がある。

- 紛失や盗難に気付くことが遅れる
- 紛失や盗難の際に流出した情報の範囲がわからない
- 自由に持ち出しができることから内部犯行（故意による持ち出し）を行いやすい

有事を想定したバックアップの取得とデータ復旧への備えについては、ランサムウェア対策や自然災害等によるシステムへの被害対策として必要であるが、実施している企業は 5 割以下であった。

私用 PC・タブレットの利用については、2 割以下と少なかったが、私用 PC・タブレットは会社支給のものと比較してサイバーセキュリティが弱く、利用する場合にはしっかりとしたルールとサイバーセキュリティ意識が必要となる。

いずれの観点からも中小企業の業務におけるリスクが高いことがうかがえるが、原因としてこれらの業務におけるサイバーリスクを理解していないケースもあると想定される。まずはリスクを正しく認識し、対策についての理解、ルール作りを含めた対策の導入とステップアップする必要があるが、特に日常業務における取組においては従業員ひとりひとりがリスクに対する意識を高めルールを順守することが重要となる。そのためには定期的な従業員教育が必要である。

＜取引先からの要求について＞

取引先企業から、情報セキュリティ対策の方針の要件やルールの提示が「ない」と回答した企業が 7 割となっており、「仕入・委託先」「受注・受託先（売り先）」におけるサイバーセキュリティ対策について把握していないことが考えられる。また、企業へのインタビューの結果から、口頭や文書での注意喚起はあるものの、具体的な対策措置の要件や指示が曖昧であり、受け手となる企業の自己判断で運用されているのが実態と考えられる。（ヒアリング企業：製造業、従業員 50 名以下）

この結果から中小企業においてはサイバーセキュリティ対策の方針の要件やルールの提示について発注企業側が運用上での関与・管理していないケースが多く、相互で意識の統一が図れていないと考えられる。今後のさらなるサイバーセキュリティ対策の普及に向けては、発注企業側が受注企業側に明確な基準を明示すべきであり、その基準としては、IPA の「SECURITY ACTION 二つ星」またはそれに準ずる基準（発注企業の情報セキュリティポリシー等）を活用するべきと考える。このような営みを継続することにより、中小企業等受注側企業もセキュリティの重要性を認識し国内全体の安全性を高めることにつながると思われる。

＜サイバーリスクマネジメントについて＞

導入または検討しているサイバーセキュリティ対策については、技術的な対策の回答数が多く、社員教育やセキュリティ管理者の設置などマネジメントに関わる回答は少ない。情報漏えいやシステム停止などのインシデントが発生した場合の事業への影響について、対応にかかる費用の想定をしている企業は 5 割強、対応にかかる人件費や売上・事業への影響を想定している企業は 3 割強、自社だけでなく親会社やサプライチェーンなど影響の範囲を想定している企業は 2 割である。サイバーセキュリティ対策は、予防としての事前の対策とインシデントが発生した場合を想定した事後の対策がある。また、ウイルス対策ソフト

や出入り口対策等の技術的対策だけでなく、組織としての対策（対策方針の策定、社内ルールの策定、従業員教育等）、従業員としての対策（社内ルールの順守、ウイルス感染や盗難等への注意）にも取り組む必要がある。中小企業においては、サイバーセキュリティの全体像を理解し計画的な取り組みを実施できていないことが推察される。自社の事業内容や規模、リスク実態にあわせて計画的に取り組み改善を続けるためのサイバーリスクマネジメントが必要である。

＜SECURITY ACTION について＞

中小企業のサイバーリスクマネジメントのガイドラインとして、「中小企業情報セキュリティガイドライン」（IPA）がある。

ガイドラインのステップとしては、

Step1 セキュリティ 5 か条の実行

Step2 情報セキュリティ自社診断

Step3 自社のリスクに応じた対策規定の作成と運用・改善

Step4 継続的な改善

とあり、Step1 の宣言が SECURITY ACTION の一つ星、Step2 の実施と Step3 の公開が SECURITY ACTION の二つ星の要件となる。

アンケートにおいて、SECURITY ACTION について知っている企業は 20%に留まった。宣言しているまたは予定のある企業はさらに少数であるが、SECURITY ACTION の二つ星に取り組むことで中小企業がサイバーセキュリティの全体像を把握するきっかけとなる可能性がある。また、社内外に宣言することで、社外には取引先からの評価基準の１つとなり、社内のサイバーセキュリティ意識向上につながるものと考える。

7. 中小企業に必要な対策の考察（ファシリティ面・人材面）

実証を通じて、中小企業のファシリティ面・人材面において以下の傾向と課題があるとの気付きを得た。

＜ファシリティ面＞

- アンケート結果から、現状、中小企業の大半がウイルス対策ソフト（エンドポイント対策）の導入に留まっているが、「多層防御」の観点からも、UTM 等による出入り口対策の導入やセキュアな通信環境の構築が必要である。ただし、価格面における障壁を解消するために、IT ベンダが中小企業向けに価格や機能を抑えた新たなサービスの開発や、必要なセキュリティ対策にかかるコストの妥当性を訴求しなければならない。

＜人材面＞

- 中小企業にはシステム管理者や IT リテラシーの高い専担の従事者が少なく、社長や他の業務に従事している社員が兼務しているケースが多い。情報セキュリティに知見のあるシステム専担者を設けることが望ましいが、専担者を設けられない場合には、中小企業がセキュリティ対策機器導入後のアフターフォローを任せられる IT ベンダ・サービスを選定することが必要である。アフターフォローを実施するにあたっては、中小企業が導入しているシステムやネットワーク環境はもちろんのこと、業務形態を理解・把握し、業務フローにそったセキュリティリスクの訴求と対策措置の提示ができるとともに、定期的かつ継続的に中小企業の支援をすることができる IT ベンダ等が望ましい。
- その他機器の更改やシステム導入などのタイミングでアドバイスができる人材を現地または遠隔支援ができる環境で準備することが望ましい。

中小企業は、コスト面や利便性を優先したネットワーク及びシステム環境を構築し運用しているケースが多いが、情報漏えい等から発生する多大な被害についての意識が薄いため、セキュリティを考慮した環境の構築や運用ができていない。このような意識を改革することを含め、第三者が総合的にセキュリティに関する提案をすることが重要であると考察する。

8. サイバー保険の在り方

中小企業が継続して利用可能な保険商品を検討するにあたり、実証において「対策の実態」と障壁となる「要因」について明確にした。内容をふまえ、理論的に必要と考える保険商品（補償内容、コスト水準）と物理的に導入可能な保険商品とのギャップを埋めるための検討を行う。

(1) 実証をふまえた中小企業の保険手配の実態と課題

参加企業のうち導入している対策に保険をあげた企業は 2%と非常に低い水準にあり、普及の遅れが顕在化した。要因は下記の通りと考察する。

① サイバーリスクマネジメントにおける課題

サイバーリスク保険の認知度は約 20%にとどまり、75%は知らなかったと回答している。サイバーセキュリティ対策においては技術的な対策のみならず、保険によるリスクの移転等、リスクに応じた対応計画を策定する必要があるが、組織的、人的な態勢の整備が十分ではなく、保険を含めた総合的な計画策定が適切になされていないため、利活用が遅れていると推察される。セキュリティの全体像を把握し自社の実態をふまえた必要な対策を図る「サイバーリスクマネジメント」の対応の遅れが付保率の低い要因の一つと考える。

② 対策コストにおける課題

アンケートにおいてセキュリティ対策導入を検討できる価格帯は 10,000 円以下が全体の 75%を占め、限られたコストでセキュリティ対策全般を検討せざるを得ない実態が明確となった。事後の対策である「サイバーリスク保険」までコストが配分されず、優先順位が後位となっていると考察する。

上記考察により、継続して利用可能な保険商品の検討においては「提供方法（どのように届けるか）」と、「補償とコスト水準とのバランス」を念頭におくことが不可欠であることが明確となった。保険利用の検討が十分行われない中でも、無理なく、無意識に手配がなされている状態の創出と、真に必要な補償の丁寧な提案活動の二軸を並行して行うことが肝要であると考える 。

(2) 中小企業向けサイバーリスク保険の在り方について

上記を含めた実証結果に基づき、中小企業の実態に即した保険の在り方は下記の通りと考える。

① 保険サービスについて

セキュリティ対策は予防としての事前の対策とインシデント発生後の事後の対策を総合的に導入する必要がある。保険についても保険単体で検討するのではなく、セキュリティ対策と一体となり対策の一環として検討する必要がある。導入ニーズの高い「ウイルス対策ソフト」や「出入り口対策（UTM）」等のセキュリティ商材に保険を付帯し、セキュリティ商材を導入することで自動的に補償が得られている等、一連のセキュリティ対策として無意識のうちに手配されることが望ましい。補償の内容は「復旧にかかる費用負担」が最もニーズが高く全体の 63%を占めた実態をふまえ、賠償責任ではなく復旧費用を担保することが実態に即していると推察する。

一方で、検討可能な価格帯とのバランスからセキュリティ商材に付帯できる補償は最小限となると考えられるため、企業のリスク実態に合わせて不足する補償をサイバーリスク保険の上乗せ加入により手配を

することを推奨する。その際、保険料の高さが障壁になると考えられることから、業種や企業規模等それぞれのニーズに合致した柔軟なプランニングを行うことで補償と保険料に納得いただけるようにすることが望ましいと考える。

② サイバーリスク保険の販売体制について

企業がサイバーリスク保険を手配する際には、業務環境やリスクの実態をふまえ、それに即した保険を手配する必要がある。実証においては、東京海上日動の代理店販売網と連携、セキュリティ、保険の両軸で協働しリスクコンサルティングを行ったが、今後の保険サービスを考察する上でもこの取組は有用であったと考える。

9. まとめ

サイバーセキュリティ対策は事前の対策と事後の対策をセットで考える必要がある。1 つの対策をすれば十分というものではなく、その企業の業務内容とリスク実態に応じた総合的な対策が必要である。

本実証において事前の対策として実施した UTM の設置は、システム担当者が不在であることが多い中小企業が自力で設置することが難しく、ネットワークを把握した上で設置し、アフターフォローを行う必要があった。同様に、企業のサイバーセキュリティ全体を見る上でも当該企業の ICT 環境や業務環境を把握していることが重要であり、これらを把握している第三者が相談に乗りアドバイスをすることがサイバーセキュリティ対策の普及に必要であると考える。

さらに、有事の際には、ネットワークを理解した上でリモートサポートや駆付けを行えることがリスク軽減に資する。

中小企業への普及には、「UTM による出入り口対策の導入」だけでなく、「総合的なサイバーリスク対策のサポート」としての価値を理解いただくために、訪問し丁寧に説明を行いトライアル等でリスクを実感してもらうことが重要である。