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：防衛・航空宇宙産業（関東地方、中部地方、関西地方））

成果報告書

請負事業者：株式会社PFU

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

目次

1　サマリー

本報告書は、株式会社 PFU（以下「PFU」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。
防衛・航空宇宙産業に関わる中小企業今後参入を検討する中小企業 50 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。

- セキュリティ意識調査アンケート
- セルフアセスメント「情報セキュリティ整備状況診断」
- 社内パソコンの脆弱性診断
- パソコン上の脅威検知
- 工場の IT 機器見える化
- 機密性の高いデータ共有

2　背景・目的

中小企業の実態を踏まえ、サイバーセキュリティ事後対応支援体制の整備と実証を通じた成果を今後の中小企業向けサービスへフィードバックする。

2.1　背景

サイバー攻撃の状況

サプライチェーン全体の中で対策が弱い中小企業を対象とするサイバー攻撃やそれに伴う大企業などへの被害が顕在化してきている。

令和元年 大阪商工会議所の調査では、大企業・中堅企業 118 社のうち 25%が「取引先がサイバー攻撃被害を受け、影響が自社に及んだ経験がある」と回答。

中小企業の現状

IT やサイバーセキュリティに関する知識が乏しく、サイバー攻撃に遭っていることに気付かず被害が拡大するケースも多く発生。スキル・人手不足の課題もある。

サービス提供側の現状

中小企業のニーズに合った製品、サービスが提供されていない。中小企業の被害実態や、中小企業支援に必要な人材スキルなどの把握ができていない。

令和元年度 「サイバーセキュリティお助け隊事業」を実施。現状は、中小企業への意識喚起が不十分、中小企業のニーズに合った製品、サービスが提供されてない状況。

- 地域特性・産業特性の考慮が必要
- 導入負荷を下げる必要がある
- セキュリティに関する普及啓発が必要
- 事後対策だけでなく事前対策も必要
- サービス購入費用が許容可能であること

防衛･航空宇宙産業の現状

サプライチェーンリスクの問題への対処の必要性

- 防衛・航空宇宙産業のサプライチェーンへ参加できなくなる中小企業が多数発生
- 中小企業の不参加による我が国の防衛・航空宇宙産業の競争力の低下

防衛・航空宇宙産業は、国家機密などの窃取・損壊や他国による同産業の発展を目的とした知的財産の窃取など、標的にされやすく重点的に保護すべき産業である認識がある。

本産業における動向として、米国では米国政府機関が調達する製品や技術を開発・製造する企業に対して求められる情報・サイバーセキュリティを担保するため NIST CSF（※1）に則ったセキュリティ対策ガイドライン「NIST SP800-171（※2)」の遵守が義務化されており、我が国においても同レベルのサイバーセキュリティ準拠が求められている。

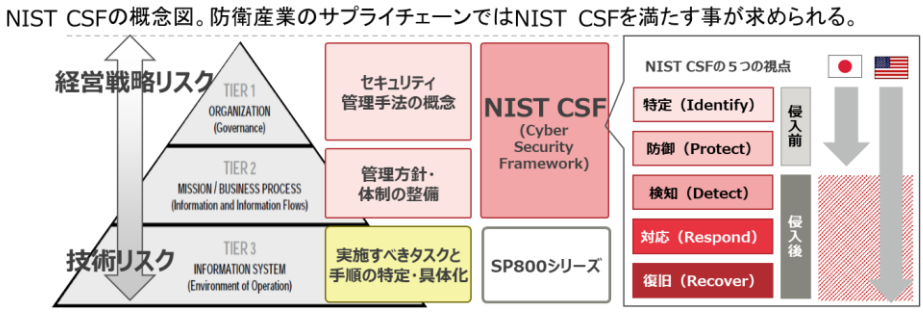
取引先の上位企業は必要なサイバーセキュリティ対策ができても、下請けとなる中小企業はリソ

ース・コスト・スキルなどの課題があり対応が困難であると考えられる。

今回、本産業に関わる中小企業へのサイバーセキュリティ普及啓発・実態調査により、今後この産業で求められる対策レベルとのギャップを明らかにすることで、中小企業が利用可能な対策サービスの検討を行う。

＜参考情報＞

米国では米国防総省が 2018 年 1 月から、契約業者に対して NIST（アメリカ国立標準技術研究所）が定めた厳格な NIST CSF（※1）に則ったセキュリティ対策ガイドライン「NIST SP800-171（※2)」の遵守を義務化



NIST SP800-37 を元に作成

図 2-1. NIST CSF の必要性

※1 NIST CSF サイバーセキュリティを「特定（Identify)」、「防御（Protect)」「検知（Detect)」、「対応（Respond)」、「復旧（Recover)」の 5 段階で考える枠組み。

※2 NIST SP 800-171：NIST が定めたセキュリティ対策ガイドライン。 米国政府機関が調達する製品や技術を開発・製造する企業に対して求められる情報・サイバーセキュリティを担保するためのもの。

2.2 目的

本事業の実施目的

中小企業におけるサイバーセキュリティの意識向上を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを目的とする。

防衛・航空宇宙産業におけるサイバー攻撃対策の必要性とサイバー攻撃被害は経営を直撃することを中小企業の経営層に理解してもらうとともに、セキュリティ対策の導入負荷を低減しテレワークにも対応する PC ソフト導入型のサービスを用いて事後対応支援を実証し、安価で普及可能なサービスの検討を行う。

【令和 2 年度 実施内容】

①対策の必要性が高い産業分野を選定して実証する（防衛・航空宇宙産業）
②サイバーセキュリティ対策の必要性を説明して意識を喚起する
③事後対応支援体制の構築・実証により被害状況や対策状況などの実態を把握する
④継続的なサービスの検討、サイバー保険のありかたを検討する
⑤サイバーセキュリティ対策の普及に向け、実証成果をまとめて報告する

令和元年度のお助け隊事業で明らかになった中小企業の実態・ニーズを踏まえ、中小企業に定着するサービスを実施できる体制を整備し実証に取り組む。

3　実証事業の概要

3.1　実証対象（産業分野）の選定

サイバーセキュリティの対応が重要である防衛・航空宇宙産業を支えるサプライチェーンである関連する中小企業に向けた実証事業を行い、実態把握とともに、業界への啓発が必要と考える。

防衛・航空宇宙産業に関わる中小企業および今後参入を検討する中小企業を対象に実証を行った。

対象となる産業を絞ることから対象企業母数が制限されるため、実証地域の選定においては、有効な実証データを確保するために必要な実証参加企業数を確保できることを主眼に置き地域を選定した。

関東地方：福島県、栃木県、東京都、群馬県、埼玉県、神奈川県
中部地方：三重県、愛知県、岐阜県、静岡県、長野県
関西地方：兵庫県、京都府、滋賀県、大阪府

防衛・航空宇宙産業のサプライチェーンは全国に分布しているが、募集対象中小企業母数の確保、募集活動ができる期間などを考慮し、主要な産業クラスターが形成されている地域、主要なサプライチェーン上位の企業が所在している「中部地方」、「関東地方」「関西地方」を選定した。

3.2　スケジュール

表 3-1. 実施スケジュール

	9 月	10 月	11 月	12 月	1 月
事業説明会の開催	6 回	9 回	10 回		
・ オンライン 25 回	5 回	9 回	10 回		
・ オフライン 1 回(名古屋)	1 回				
中小企業の実態把握		1 回目	2 回目		
・意識調査					
・情報セキュリティ整備状況診断					
監視・駆け付け対応					
・コールセンター					
・パソコン脅威検知					
・パソコン脆弱性監視					
・駆け付け対応支援					
・工場の IT 機器見える化					
・機密性の高いデータ共有					
成果報告会					1/15
・ オンライン 1 回					●

実施期間：2020 年 9 月 15 日～2021 年 1 月 31 日
うち監視・駆け付け対応（事後対応支援）期間：2020 年 9 月 15 日～2021 年 1 月 24 日

3.3　実証参加企業

54 社の実証参加申込みを得たが、4 社からは実証参加の取りやめを受けた。不参加理由を「4.1.1.7 不参加理由」に記載。

表 3-2. 実証参加状況

実証参加状況		活動成果	社数
実証参加企業数		実態把握	54 社
	監視サービス辞退企業数（不参加理由の収集）	実態把握	4 社
	監視サービス実施企業数（実機調査による）	実態把握	50 社

3.4　実証内容

3.4.1 参加募集方法

産業特化の募集を行う必要があるため、関係する団体を中心に募集活動を展開する。また、対象とする産業のサプライチェーン全体へのサイバーセキュリティ対策効果が見込めることから取引先企業への働きかけも同時に実施する。

対象地域を広く取り、産業特化により減少した対象企業母数を補う方法としており、産業絞り込みに加えてエリア拡大により行政との連携方法に工夫が必要となる。行政との連携については、ほかのお助け隊事業者の実証地域と重なることも考慮し、中部･関東･近畿経済産業局との連携をまず図り、防衛・航空宇宙産業に関わる協力先となる団体などの情報連携を行い、市・町・村・商工会議所への総当たり的な募集協力については控え、本実証の周知をする範囲に留める方向で考えている。

広大なエリアでの募集および事後対応支援の工夫点として、全 8 回のウェビナー活用や説明会動画コンテンツのサイト掲載により、定期開催／オンデマンドなどの手法を取り入れ、時間が取れない中小企業においても参加機会が得られるように工夫し、広大なエリアに対する短期募集ができるように実施する。

表 3-3. 募集ターゲット（計画時）

主な働きかけ先	実証対象地域														
	三重	愛知	岐阜	静岡	長野	福島	栃木	東京	群馬	埼玉	神奈川	兵庫	京都	滋賀	大阪
中部地域の航空機クラスター特区	●	●	●	●	●										
関東エアロスペース・プロモーション・プログラム					●	●	●	●							
埼玉航空・宇宙産業参入支援										●					
まんてんプロジェクト											●				
関西航空機産業プラットフォーム NEXT												●	●	●	●
サプライチェーン大手企業への働きかけ（約 10 社）					●		●	●	●			●	●	●	●

3.4.2 募集施策（全体）

中部・関東・近畿経済産業局の協力および本実証事業請負会社※の関係先などを通じて以下の行政・団体にアプローチし募集活動を進めた。

表 3-4. 募集施策

アプローチ先	募集活動内容
日本防衛装備工業会（JADI）	約 70 社へメルマガ発信
栃木航空宇宙懇話会（TASC）	同団体向けウェビナー説明会(2 回) 同団体の研究会で事業説明を実施(1 回)
公益財団法人 長野県テクノ財団	数十社の航空機関連の中小企業へメルマガ配信
浜松商工会議所	協同でセミナー開催
東京商工会議所	会員企業へメルマガ配信
名古屋商工会議所 産業振興部 ものづくりイノベーションユニット	セミナーを開催（大手・団体などを含み 100 社参加） 補足：名古屋商工会議所（愛知県、岐阜県、三重県を担当）の実証参加企業と重複しないように開催
全国航空機クラスター・ネットワーク（NAMAC）	約 900 社へメルマガ配信
東京エリアのものづくり企業コミュニ	約 70 社へメルマガ配信

アプローチ先	募集活動内容
ティ（TMAN）	
ぐんま航空宇宙産業振興協議会（Hizuru）	会員約 150 社へのメルマガ配信
公益財団法人 埼玉県産業振興公社	同団体の研究会で約 20 社にウェビナー説明
公益財団法人 三重県産業支援センター（MASIP）	15 社にウェビナー説明
愛知県航空宇宙産業ネットワーク	同団体の研究会で説明（会場約 10 社、ウェビナー）
協同組合 SOLAE（静岡航空宇宙産業プロジェクト）	定例会でチラシを配布（約 10 社）
中部航空宇宙産業技術センター（C-ASTEC）	メルマガ配信
サプライチェーン大手企業へのサプライヤーの参加協力依頼	積極的な協力を得られず。サプライヤーが強要と捉える募集方法ができないことや、中小企業デジタル化などで既にサプライヤーに多くの協力を求めている時期と重なったためサプライチェーン大手企業が積極的に動きづらい状況にあったため。
エンジンフォーラム神戸（航空機産業のイベント）	イベント会場にて関係団体に協力を得て会場で募集
中小企業への直接アプローチ（本実証事業請負会社の関係先※）	約 20 社

※ PFU、富士通株式会社、株式会社エヴァアビエーション

3.4.3 事業説明会の計画

Zoom Webinar によるオンライン事業説明会を下記の内容で 8 回開催を計画した。

表 3-5. 事業説明会の開催内容

時間	内容	講演者
5 分	開催挨拶と趣旨説明	PFU
20 分	セキュリティ脅威と対策の必要性について米国（NISTCSF など）や 国内（防衛省）の検討状況などの最新状況	株式会社エヴァアビエーション
20 分	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などの支援事業について	IPA
40 分	本実証事業の説明 1） パソコン上の脅威検知、脆弱性監視 2） 工場の IT 機器見える化 （iNetSec SF)） 3） エヴァアビエーションの提供サービス セルフチェック（情報セキュリティ整備状況診断))、海外動向など情報共有サイト 4） 機密性の高いデータの共有（Fort#Forum）	PFU 株式会社エヴァアビエーション 富士通株式会社
5 分	参加申込み方法について	PFU

事業説明会に参加できない方に向けて、スライド写真と説明による冊子説明や、講演ビデオを Web サイトで公開し、逐次閲覧できる環境作りも実施した。

図 3-6. 事業説明の資料公開サイトの写し

3.4.4 実態把握の方法

適切なサイバーセキュリティ事後対応支援体制を構築するため「防衛・航空宇宙産業における中小企業がさらされているサイバー攻撃の実態」と「現在のセキュリティ対策状況」を調査・収集する。

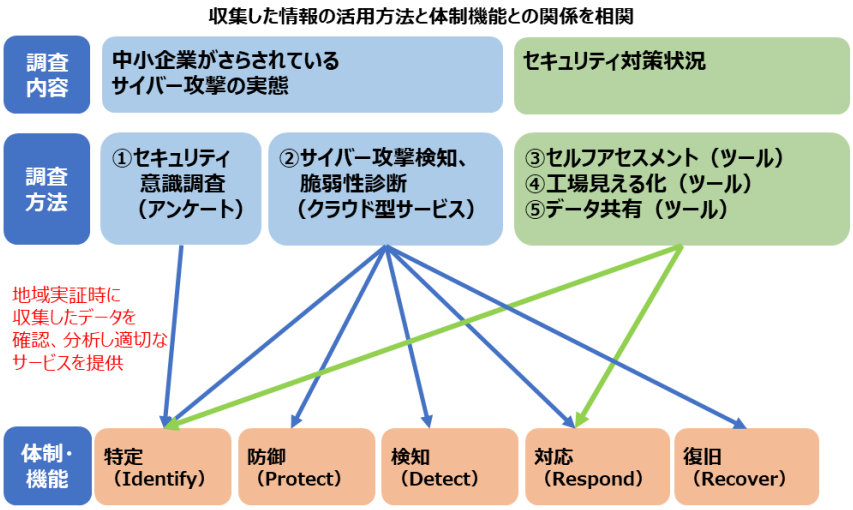


図 3-1. 中小企業の実態把握方法

以降の項で、図中の①～⑤について詳説する。

3.4.5 セキュリティ意識調査アンケート（①）

防衛産業が求めるセキュリティ対策の実態やニーズを調査する。
実態把握するための設問は下記のとおり。

1.　サイバー攻撃対策の状況
1-1.セキュリティに関する困りごとがあった際に相談できる窓口はお持ちですか 1-2.PC の OS やソフトウェアは常に最新状態に保つ仕組みはお持ちですか 1-3.マルウェアの侵入などのサイバー攻撃を検知する仕組みはお持ちですか 1-4.PC がマルウェアに感染している疑いがあった場合に、それを分析する仕組みはお持ちですか 1-5.サイバー攻撃の被害があった場合の対応を規定化していますか 1-6.サイバー攻撃の被害状況の調査や復旧に向けた対応を進める仕組みはありますか
2.　セキュリティに対する意識
2-1.自社がサイバー攻撃被害に遭う可能性があると考えていますか 2-2.脆弱性診断やサイバー保険など、セキュリティ対策を実施されていますか 2-2-1.セキュリティ対策を実施している場合どのようなセキュリティ対策を行っていますか 2-3.それらセキュリティ対策は十分だと思いますか（自社に適していると思いますか） 2-4.セキュリティ対策にかけることができる費用はどの程度お考えですか 2-4-1.現在かけている費用（これまでに掛けられている費用） 2-4-2.今後かけられる費用（今後予定されている費用） 2-4-3.お助け隊サービスを仮に継続した場合に、このサービスにかけられる費　用 2-5.情報セキュリティ対策を進める上での課題、阻害要因はどのようなものがありますか 2-6.現在、テレワークを実施されていますか 2-6-1.テレワークされている場合、社外利用時のセキュリティ対策は行っていますか 2-6-2.テレワークの導入を進める上での課題はどのようなものがあります　　か 2-7.工場を保有していますか 2-7-1.保有している場合、IP 通信を行う機器は接続されていますか 2-7-2.工場ネットワークは社内ネットワークと接続されていますか 2-7-3.工場ネットワークに接続されている機器は把握・管理されていますか 2-7-4.工場ネットワークでセキュリティ対策は意識されていますか 2-7-5.意識されている場合、どのような対策を行っていますか
3.　サプライチェーン
3-1.「防衛産業」または「航空宇宙産業」という名目で特別な対策は要求されましたか 3-1-1.要求された場合、どのような要求がありましたか 3-2.取引先企業とデータの受け渡しなどはありますか

3-2-1.受け渡しがある場合、機密情報をやり取りされていますか 3-2-2.社内で何人ぐらいの方が機密情報のやり取りをされますか 3-2-3.受け渡しがある場合、どのような方法で行っていますか 3-2-4.取引先企業とデータの受け渡しを行う企業は複数ありますか 3-2-4-1.複数ある場合はどの程度の企業数とやり取りを行いますか 3-2-5.取引先企業とのデータの受け渡しにおいてセキュリティ対策など意識していますか 3-2-5-1.意識している場合、どのような点を意識していますか 3-2-6.意識していない場合、どのような理由が考えられますか
4. サイバー攻撃被害の実態
4-1.自社内でサイバー攻撃を認識したことはありますか 4-1-1.どのような被害に遭いましたか 4-1-2.その際はどのような対応をしましたか 4-2.自社内で保有する情報が漏えいした場合、どの程度の被害が出ると想定していますか 4-3.セキュリティ対策を進める上でどのようなサービスがあるとメリットを感じますか 日々の監視 復旧サービス 被害に対する補償 現地駆け付け支援 4-4.情報漏えいが発生した場合、取引先、お客様、市場などに対してどのような対応をとる可能性がありますか
5. サイバー保険
5-1.サイバー保険の存在を知っていますか 5-2.サイバー保険に加入していますか 5-3.加入した理由／加入していない理由は何ですか 5-4.既存のサイバー保険やサービスの価格帯は高いと思いますか 5-5.サイバー保険として妥当だと思う保険料（月額）は幾らですか 5-6.サイバー攻撃の被害にあった場合は多額の費用が必要となるケースがありますか、どのような費用が保険で補償されるとメリットを感じますか
6. そのほかご意見・ご要望がございましたら、ご自由にご記入ください

3.4.6 セルフアセスメント「情報セキュリティ整備状況診断」(③)

アメリカ国防総省（DoD)）が NIST SP 800-171（セキュリティ基準を示すガイドライン）を防衛産業に関わる全ての企業に遵守させる目的で創設されたものの、その施策が企業において十分浸透できなかった経緯がある。それは SP 800-171 には 110 項目のガイドラインがあり、中小企業では全てを実施することは大変負荷がかかる点、またその遵守状況は自己申告で良いことと、実施していない項目については達成目標日を申告するだけで DoD は受注会社としての要件をクリアしたこととしていたためである。そこで SP 800-171 を全企業へ必須とするべく、2020 年 1 月に CMMC-AB という非営利法人を立ち上げ、5 つのレベルにプロセス(手順）とプラクティス(実施）を設定した。請負会社は受注案件内容によって必要レベルを第三者機関に認められれば、DoD の受注対象企業となるという仕組みである。

今回、航空・防衛産業に携わる企業においては、2021 年以降の受注案件によってはその対象となる可能性があり、CMMC Level 1 の 17 項目が達成されているかを確認するためにセルフアセスメントを設定した。

また IPA が従来から設定している組織的な情報セキュリティ対策ガイドラインである「新 5 分でできる！情報セキュリティ自社診断」の 25 問と併せ、重複する部分を含めると合計 35 項目のセルフアセスメントとして設定し、セキュリティ対策整備状況を把握する。

本実証事業では、回答内容に対して、コンサルタントが改善点のコメントを返すとともに、不明点の Q&A を受け付ける。　さらに、SECURITY ACTION の一つ星、二つ星の宣言方法を案内することで、SECURITY ACTION を促進する。

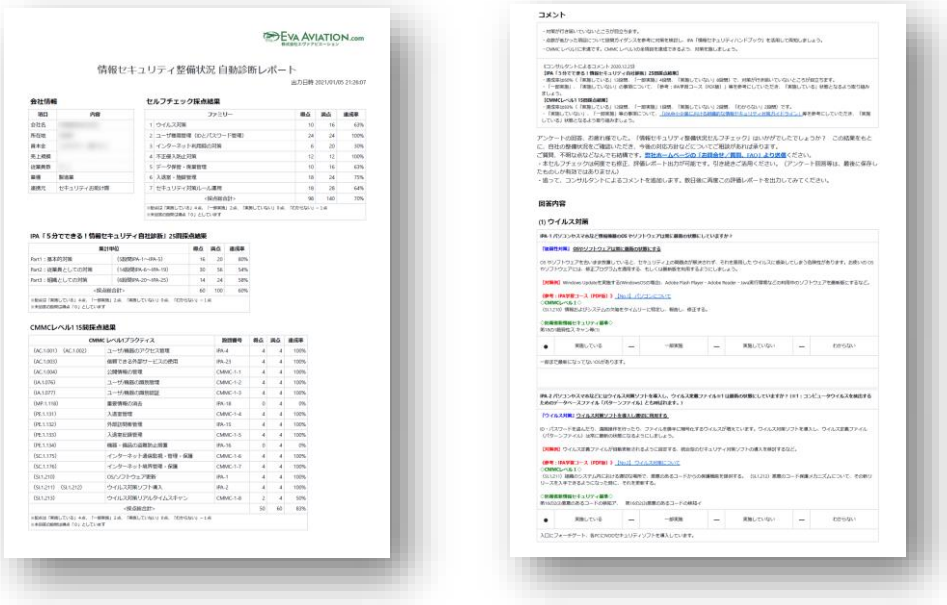


図 3-2. 個社へ送付した診断結果レポートの写し（例）

付与するコメント例：

・対策が行き届いていないところが目立ちます。 ・点数が低かった項目について設問ガイダンスを参考に対策を検討し、IPA「情報セキュリティハンドブック」を活用して周知しましょう。 ・CMMC レベル 1 に未達です。CMMC レベル 1 の全項目を達成できるよう、対策を施しましょう。
《コンサルタントによるコメント》 **【IPA「5 分でできる！情報セキュリティ自社診断」25 問採点結果】** ・達成率は 66%（「実施している」12 設問、「一部実施」9 設問、「実施していない」4 設問）で、対策が行き届いていないところが目立ちます。 ・「一部実施」、「実施していない」の事項について、「参考：IPA 学習コース（PDF 版）」などを参考にしていただき、「実施している」状態となるよう取り組みましょう。 **【CMMC レベル 1 15 問採点結果】** ・達成率は 57%（「実施している」7 設問、「一部実施」3 設問、「実施していない」5 設問、「わからない」2 設問）です。 ・「実施していない」の CMMC-1-2（ユーザー/機器の識別管理）、CMMC-1-3（ユーザー/機器の識別認証）、CMMC-1-5（入退室記録管理）、CMMC-1-6（インターネット通信監視・管理・保護）、CMMC-1-7（インターネット境界管理・保護）などの事項について、「IPA 中小企業における組織的な情報セキュリティ対策ガイドライン」（https://www.ipa.go.jp/security/manager/know/sme-guide/sme-security_guidline.html）の 4.2（物理的セキュリティ）、4.3（情報システムおよび通信ネットワークの運用管理）、4.4（情報システムのアクセス制御の状況および情報システムの開発、保守におけるセキュリティ対策）などを参考にしていただき、「実施している」状態となるよう取り組みましょう。

実態把握するための設問は下記のとおり。

（1: IPA-1） パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
（2: IPA-2） パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？
（3: CMMC-1-8）パソコンやスマホなどについてウイルス対策ソフトで、定期的にスキャンするとともに、外部からのファイルをリアルタイムスキャンしていますか？
（4: IPA-5） 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
（5: CMMC-1-2） システムを利用できるユーザー、装置などを特定し、ID を発行し、付与していますか？
（6: IPA-3） パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
（7: CMMC-1-3） ユーザー、装置などがシステムを利用できるようにする前に、ユーザー、装

置などの ID をパスワードなどにより認証していますか？
（8: IPA-4） 重要情報に対する適切なアクセス制限を行っていますか？（重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。）
（9: CMMC-3-1） 特権アカウントを利用する場合や、リモートアクセスを行う場合、ユーザーがシステムを利用できるようにする前に、多要素認証を行っていますか？（多要素認証とは複数の要素（記憶情報、所持情報、生体情報）を用いた認証方式）
（10: CMMC-3-2） 秘密情報を含む媒体へのアクセスを管理し、社外への送信/輸送時も、許可された者だけがアクセスできるようにしていますか？
（11: IPA-6） 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
（12: IPA-7） 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
（13: IPA-8） 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
（14: IPA-10） インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
（15: CMMC-1-1） ニュースリリースなど外部公表する情報を管理、制限し、契約情報を含む可能性のある情報を、公開 Web サイトなどに掲載許可しないようにしていますか？
（16: IPA-9） 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
（17: CMMC-1-6） 社内システムをインターネット接続する場合、ファイアウォール、Web プロキシなどを利用して、送受信される情報を監視・管理・保護していますか？
（18: CMMC-1-7） 外部に公開する Web サーバー、メールサーバーなどがある場合、内部ネットワークから分離された DMZ セグメントに配置していますか？
（19: IPA-11） パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
（20: IPA-12） 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は 机上に放置せず、書庫などに安全に保管していますか？
（21: IPA-13） 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
（22: IPA-18） 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
（23: IPA-14） 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
（24: CMMC-1-4） 社内施設（事務所、工場など）や社内システム・装置のアクセス（入室、利用）を許可した人に限定していますか？
（25: IPA-15） 関係者以外の事務所への立ち入りを制限していますか？
（26: IPA-16） 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしています

か？
（27: IPA-17） 事務所が無人になる時の施錠忘れ対策を実施していますか？
（28: CMMC-1-5） 社内施設（事務所、工場など）や機器に、いつ誰がアクセス（入室、利用）しているか記録を残していますか？
（29: IPA-19） 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
（30: IPA-20） 従業員にセキュリティに関する教育や注意喚起を行っていますか？
（31: IPA-21） 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
（32: IPA-22） 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
（33: IPA-23） クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
（34: IPA-24） セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
（35: IPA-25） 情報セキュリティ対策（上記 IPA-1 ～ IPA-24 など）をルール化し、従業員に明示していますか？

3.4.7 社内パソコンの脆弱性診断（②）

PFU 製の iNetSec Inspection Center（PC 脆弱性検査ソフトウェア）を実証参加企業の PC に導入することで、PC からの検査結果を自動的に監視し、PC 上の脆弱性に関する是正箇所を含めた報告書を作成し週報として実証参加企業へメールする。

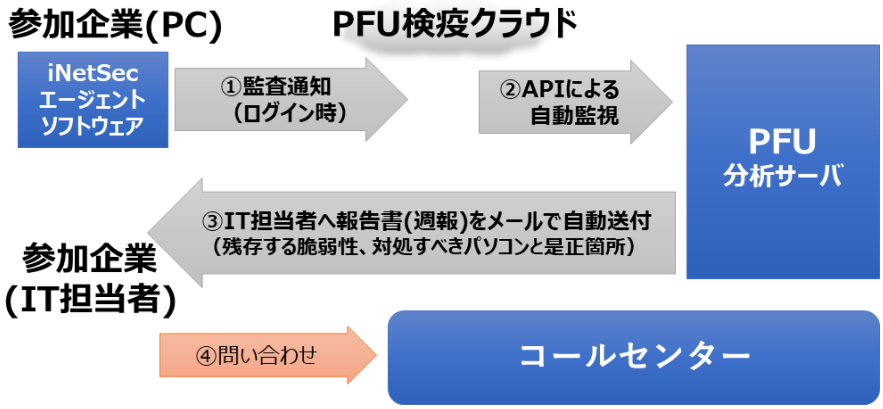


図 3-3. パソコン上の脆弱性監視サービス提供イメージ

日々社員の画面に脆弱性に関する問題点を通知することで善処を施す機能があるが、実証参加企業によっては管理者だけに通知してほしいとの要望が多数ある。本実証事業では、実証参加企業ごとに PC 利用者への通知をする／しないについて選択できるようにした。

多くの企業では管理者に送付する週次報告書（問題のあるパソコンと、改善点を列挙）の送付のみを希望されている。これは、日々社員に通知することで管理者が介在しなくとも善処の指導を行う予定であったが、社員からの問合せを受けることで、業務に支障が出てしまうことを懸念される管理者が多かったためと考える。

3.4.8 パソコン上の脅威検知（既存対策をすり抜けたマルウェア感染の実態）（②）

実証参加企業の PC に WEBROOT 社 SecureAnywhere Business を導入し、クラウド上で管理する方式でサービスを提供した。ソフトウェアは、通常のアンチウイルスソフトの機能に加えて、未知の脅威を識別でき、クラウド上から隔離操作（処置）ができる機能がある。

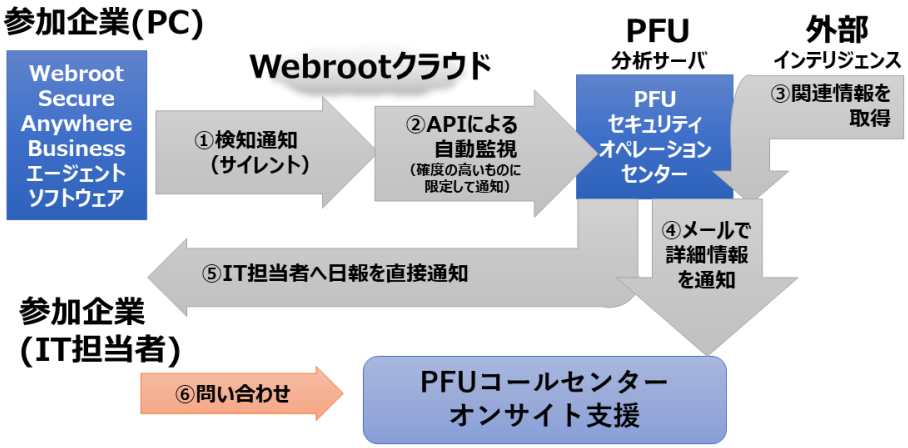


図 3-4. パソコン上の脅威検知サービス提供イメージ

本実証事業の「脅威の検知数」に関しては、社内と社外ネットワークの境界位置で行うファイアウォールや UTM 装置などで防御されなかった検知数となる。さらに、パソコン上においても、既存のセキュリティ対策製品が検出・対処された脅威は件数に含まれず、**全ての既存対策をすり抜けた脅威の検知数を報告している。**

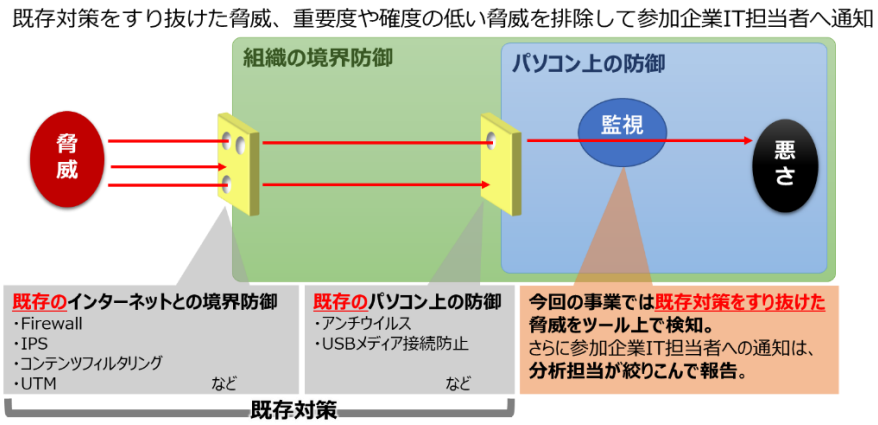


図 3-5. PFU サービスの脅威検知位置

さらに、既存対策と同居する本実証事業で使用する検知ツールは、確度や重要度の異なる多くの通知を行っている。これらの通知を全て実証参加企業に転送せず、大手・中堅企業で培った知見を活かし、**重要度が低い警告のフィルタリング、外部インテリジェンスを活用して低い確度をフィルタリング、さらに分析担当の知見でフィルタリングし、実証参加企業 IT 担当者の負担を軽減**している。実証参加企業には、**対処の緊急度を 2 段階に分け、可及的速やかに対処を要するか否か分けて報告**を行った。

図 3-6. PFU サービスの脅威警告における抑制

3.4.9 工場の IT 機器見える化（④）

工場を保持する企業において IT 機器の「見える化」を希望する 5 社に対して、一定期間（2 週間程度）センサー装置を設置することで、意図しない IT 機器（私物機器など）の接続状況を検出し、併せて工場管理者へ管理状況についてアンケートを行うことで、工場への管理体制状況を検証する。

図 3-7. 工場の IT 機器見える化のセンサー設置イメージ

別途、次のヒアリングを実施する。

1.オフィス系ネットワークと、工場系のネットワークで管理者は分かれていますか？分かれている場合、お互いの管理状況を把握されていますか？
2.工場系のネットワークに保守用回線など外部からアクセス可能なネットワークは繋がれていますか？
3.工場系ネットワークに想定していない機器が接続されていたことがありますか？ある場合、どのような機器が接続されていましたか？
4.工場側において、セキュリティインシデントが過去に発生したことがありますか？ある場合、どのようなインシデントでしたか？
5.今回、工場の IT 機器見える化として、サービスを提供させていただきますが、自動で見える化して管理したい機器は、どんなものがありますか？（たとえば、PLC、DCS、IoT-GW など）
6.ネットワークに接続されている機器は、どんな情報が知りたいですか？（たとえば、バージョン／ファーム／製造年、ネットワーク構成／機器状態、サポート情報／脆弱性情報など）
7.先ほどの質問で、機器の知りたい情報のお話をしました。現在は、それらをどのように管理されていますか？ （たとえば、都度、セキュリティを見ているご担当者（脆弱性管理）から、工場のライン担当様へご案内されるなど）
8.アンチウイルス製品を導入できない機器があるなど、セキュリティ面で気になる機器はございますか？
9.業者などが、保守用 PC の持ち込みを行い接続されるケースでは、現在どのように管理されておりますか？ （利用申請・承認したパソコンのみ接続を許可するなど）

3.4.10 機密性の高いデータ共有（⑤）

NIST SP800-171 に準拠する「データ共有」サービス（富士通 Fort#Forum）を提供して機密性の高いデータ共有に関して体感してもらう。

・二要素認証
・アクセス記録
・クラウド経由のデータ共有
・ファイルの暗号化
・受け渡し後も、アクセス制御を維持（著作権管理技術）

また、アンケートによるデータ受け渡しの実態把握を実施する。
設問は下記のとおり。

1．御社は、情報を守る上で、以下のシステムの機能を採用されていますか。 （採用されているものにチェックください） □ 二要素認証（パスワードと生体、など組み合わせ） □ データの暗号化 □ データへのアクセス履歴記録 □ 機密情報取扱者権限の明確化
2．情報の保護のために以下のシステムの機能を導入する上で、障壁はどの程度ですか。「高い」「それ程高くない」「低い」からお答えください。 ・ 二要素認証（パスワードと生体、など組み合わせ） ・ データの暗号化 ・ データへのアクセス履歴記録 ・ 機密情報取扱者権限の明確化
3．お取引先との間、社内での情報（契約書、製品仕様、図面など、機微情報を含んだ文書）共有はどのような手段でされていますか。（下記、該当にチェックください） □ 紙、媒体などを郵便、手渡し □ メールで暗号化し送付、受信（送付先と、メール以外で、事前に取り決めたパスワードで暗号） □ メールで暗号化し送付、受信（送付先に、メールで都度、暗号化したパスワードを送付） □ システムまたはクラウド上でのファイル共有 □ そのほか（ご記載ください）
4．お取引先との間、社内での情報（契約書、製品仕様、図面など、機微情報を含んだ文書）共有をクラウド上（国内クラウド）で行うのに抵抗はありますか。（下記、該当にチェックください） □ 無い □ 多少ある □ 大いにあり □ そのほかのコメント

5．前記載の機能を備えた、機微情報の保管、社内外の方とのセキュアな情報共有のサービスが Fort#Forum ですが、利用価格がどの程度でしたら使っても良いと思いますか。（1 名、月額） （下記、該当にチェックください） □ 5,000 円 □ 4,000 円 □ 3,000 円 □ 2,000 円 □ 1,000 円 □ 1,000 円以下
6．もし、情報の保護、お取引との情報共有のために Fort#Forum のようなクラウドサービスを使うとしたら、当てはまる下記の利点、懸念などにチェックしてください。 □ 業務の効率化に寄与する（情報共有の簡素化） □ 機微情報を安全に保護できて情報漏えいの心配が少なくなる □ クラウドに機微な情報を上げるのが不安 □ 既存のシステムへのセキュリティ強化への投資が軽減される □ 既存のシステムへの投資に加えて、クラウドサービス利用の投資が負担になる □ そのほかのコメント □ 1,000 円以下

3.4.11　機能ごとの体制構築

PFU 内の各作業を行う部門内に本実証事業を実施する体制を構築する。

前記機能間の運用フローを構築した。

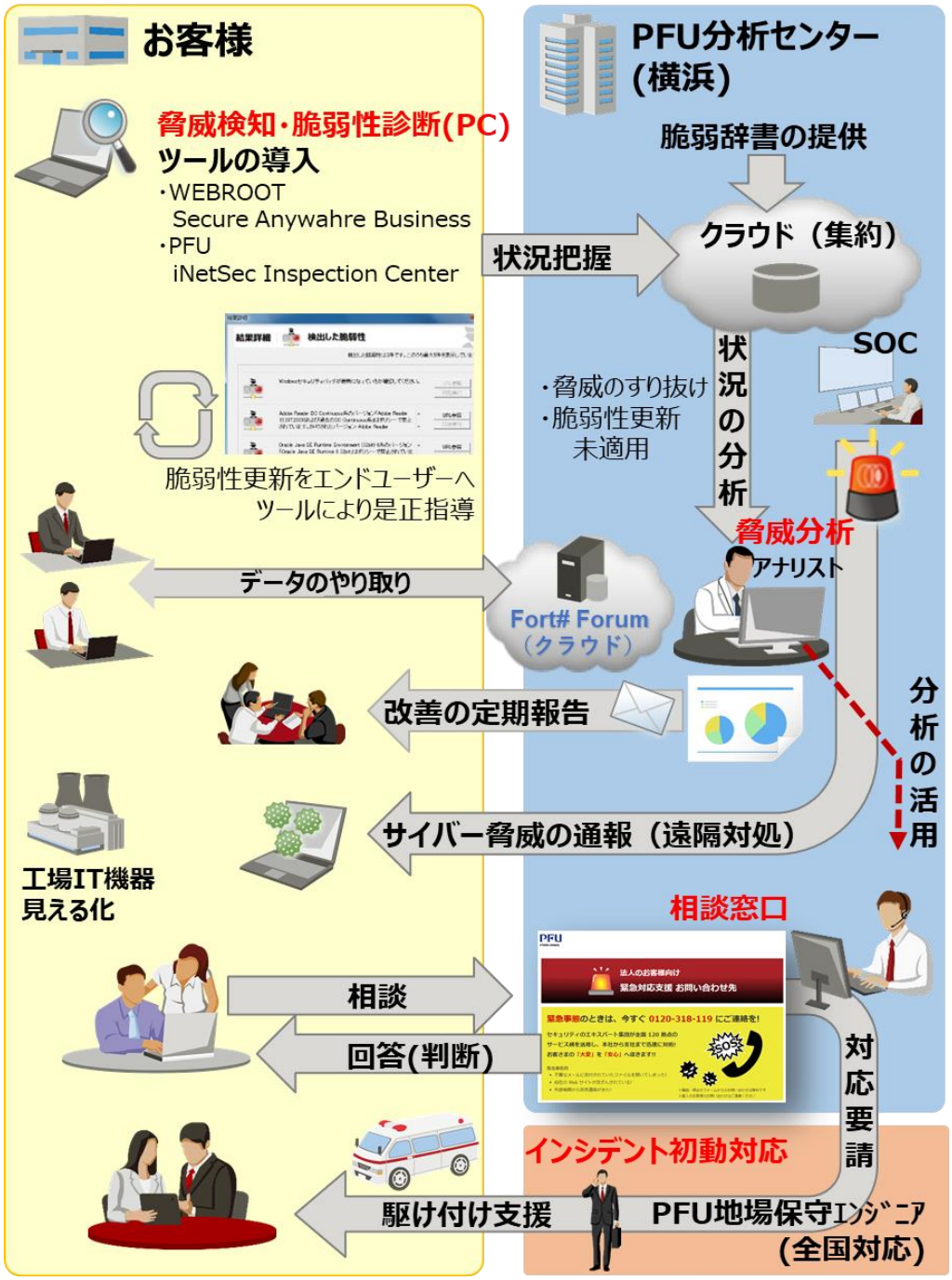


図 3-8. 機能間の運用フロー

3.4.11.1相談窓口体制

①必要なスキル

1. 一般的なビジネススキル（電話応対・メール作成）
   ＋PC スキル＋セキュリティに関する知識
   ・日本コンタクトセンター検定 オペレーション
   ・CompTIA A+, Network+, Security+
2. 技術的なサービス内容や脅威内容に関して回答を実施するスキル
   ・CISSP（実証参加企業からの質疑対応・事業説明など）
   ・情報処理安全確保支援士（登録セキスペ）（サービス実行の対応）

②必要な人数

サービス開設時間：9～17 時（12～13 時を除く）

サービス開設日：　平日のみ（土日祝日・夏季冬季の PFU 休暇日を除く）

1. コールセンター：4 名　（常時 2 名、必要に応じて応援 2 名）
2. サービス実行部隊：4 名（常時 2、必要に応じて応援 2 名）

3.4.11.2パソコンの脆弱性検知と報告

必要なスキルと人数

完全に自動化されており、特別なスキルは必要としない。

3.4.11.3パソコンの脅威検知と報告

①必要なスキル

パソコン上での検知および外部インテリジェンスを活用した脅威の確度を確認する部分は、システム化されており、特別なスキルや対応者は不要であるが、最後に、過去の知見から実証参加企業に報告すべきか最終判断するために、外部インテリジェンスを活用した脅威の分析スキルが必要。

②人数

分析担当 1 名。

3.4.11.4工場の IT 機器見える化診断と報告

①必要なスキル

工場ネットワークへの設置ヒアリング、設置・撤収作業では、現地のネットワーク環境に応じた設置作業が行えるネットワークエンジニアスキルが必要。

センサー装置が収集した機器種別情報から報告書をまとめ、セキュリティに影響がある項目のコンサルタントコメントを付記できるスキルが必要。

②人数

設置担当 1 名

分析担当 1 名

※今回は同一のシステムエンジニアが担当

3.4.11.5機密性の高いデータ共有の教育と体験

①必要なスキル

全体プログラム作成、実施のために、米国 Exostar 社のサービス（マイクロソフトの SharePoint ベース）の知識、米国の情報セキュリティ基準項目に関する知識、IT 全般にわたる基礎知識。

そのほか教育資材（マニュアル、教育動画）作成スキル、講習プログラム構成、講習実施のためのスキルが必要。

②人数

全体プログラム構成、実施責任者 1 名。

教育実施担当者 1 名（25 社に対して、都度メールで説明、オンラインでの説明を実施。）

3.4.11.6駆け付け対応支援（インシデント初動対応）

①現地駆け付け対応要員へ指示する SOC 側に必要なスキル

脅威・脆弱性に対する回答スキル

・CompTIA A+, Network+, Security+

②現地駆け付け要員のスキル

一般的な PC 操作・顧客対応スキルに関する知識。

最新のオフラインアンチウイルスソフトを持ち込んで実施すること、必要に応じてセキュリティオペレーションセンター技術員からの遠隔指示により、作業を実施できるスキルを必要とする。

・CompTIA A+, Network+, Security+

③現地駆け付け要員の人数

サービス開設時間：9～17 時（12～13 時を除く）

サービス開設日：　平日のみ（土日祝日・夏季冬季の PFU 休暇日を除く）

駆け付け隊：県ごとに 1 名待機（必要に応じて増員、最大時は地域に 2 名）

3.4.11.7そのほか（契約からサービス開始までの事務局体制）

①必要なスキル

・一般的なビジネススキル（電話応対・メール作成）

・必要に応じて法務部門に個別相談（個別、秘密保持契約など）

②必要な人数

サービス開設時間：9～17 時（12～13 時を除く）

サービス開設日：　平日のみ（土日祝日・夏季冬季の PFU 休暇日を除く）

受付業務：2 名　（ダブルチェック）

③契約からサービス開始までの流れ

1．参加企業に事業説明会への参加、訪問による説明により事業内容の把握をしてもらい、参加企業から仮申込みを行ってもらう。この時点で、今後やり取りする添付ファイルのパスワードも合わせてオフラインで回答してもらう。

2．申込みをした実証参加企業に対して、サービス仕様書の提示を行い、サービス利用条件（契約書）への署名、サービスヒアリングシート（ソフトウェアを実行するための実証参加企業環境の調査）、意識調査アンケートを渡し、実証参加企業に回答してもらう。

3．サービスヒアリングシートに従い、インストールモジュールの作成（実証参加企業の環境設定済）を作成し、実証参加企業へ送付する（ファイルは 1 で得たパスワードで暗号化）。

4．送付したモジュールのインストール後、実証参加企業から連絡をもらい、PFU の遠隔監視サービスの対象となったか回答する。

3.4.11.8そのほか（インストールモジュール作成と送付の事務局体制）

①必要なスキル

手順書に従い、実証参加企業から回答してもらったサービスヒアリングシートに従い、個社ごとの設定を行ったインストールモジュール作成を行う。特別なスキルは不要。

②必要な人数

サービス開設時間：9～17 時（12～13 時を除く）

サービス開設日：　平日のみ（土日祝日・夏季冬季の PFU 休暇日を除く）

作成業務：1 名（依頼時 5 分程度）

確認業務：1 名（依頼時 5 分程度）…ダブルチェック

4　実施結果

4.1　説明会の開催

4.1.1 募集

4.1.1.1 説明会の結果

コロナ禍の中、業界団体からメルマガ・声かけによるオンライン説明会への参加を呼びかけるも、オンライン開催は 48 社中 21 社の実証参加に留まり十分に参加者を募ることができなかった。その後、個社説明（訪問を含む）へのアプローチが必要と判断し、個社説明にて 22 社の実証参加を得た。

結果、54 社の実証参加申込を受けたが、4 社辞退となり、最終的に 50 社の実証参加に至った。

表 4-1. 事業説明会の参加状況および実証参加申込数

開催日	説明会の参加社数（参加人数）	実証申込社数	備考
9/15（火）（オンライン）	1 （1）	1	
9/17（木）（オンライン）	1 （1）	1	
9/23（水）（オンライン）	3 （3）	2	
9/25（金）（オンライン）	1 （1）	0	
9/28（月）（オフライン:名古屋）	78 （100）	2	
9/29（火）（オンライン）	1 （1）	0	
10/1（木）（オンライン）	1 （1）	1	
10/6（火）（オンライン）	1 （1）	0	
10/8（木）（オンライン）	0 （0）	0	
10/13（火）（オンライン/追加）	1 （2）	0	
10/15（木）（オンライン/追加）	3 （3）	2	
10/20（火）（オンライン/追加）	7 （7）	0	
10/22（木）（オンライン/追加）	5 （6）	3	
10/27（火）（オンライン/追加）	3 （4）	1	
10/27（火）（IPA セミナー）	（25 社中 12 社）	1	IPA のセキュリティプレゼンター勉強会での個社説明
10/27（火）（IPA セミナー）	（35 社中 35 社）	0	IPA の講習能力養成セミナー内にて参加者へ説明
10/29（木）（オンライン/追加）	2 （2）	1	
11/4（水）（オンライン/追加）	2 （5）	1	
11/6（金）（オンライン/追加）	2 （3）	1	
11/9（月）（オンライン/追加）	3 （3）	1	

開催日	説明会の参加社数（参加人数）	実証申込社数	備考
11/10（火）　（オンライン/追加）	2　（2）	0	
11/11（水）　（オンライン/追加）	1　（1）	0	
11/12（木）　（オンライン/追加）	2　（2）	1	
11/17（火）　（オンライン/追加）	4　（4）	0	
11/19（木）　（オンライン/追加）	0　（0）	0	
11/24（火）　（オンライン/追加）	2　（2）	2	
11/26（木）　（オンライン/追加）	0　（0）	0	
Web サイトの講演資料で直接検討（個社訪問による説明）	45　（45）	32	
合計	171　（200）	54	

9 月 15 日～11 月 26 日に開催したオンライン説明会は、下記のコンテンツで実施した。

14:00 開会挨拶と趣旨説明（PFU）

14:05 セキュリティ脅威と対策の必要性について

米国（国防総省、NIST など）や国内（防衛省）の検討状況などの最新状況

（株式会社エヴァアビエーション）

14:25 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）

14:50 本実証事業の説明

1） パソコン上の脅威検知、脆弱性監視（PFU）

2） 工場の機器見える化（PFU）

3） エヴァアビエーションの提供サービス

情報セキュリティ整備状況診断、

海外動向等情報共有サイト（株式会社エヴァアビエーション）

4） 機密性の高いデータの共有（富士通株式会社）

15:30 質疑応答（質疑終了後に終了）

9 月 28 日（月）に名古屋商工会議所から名商 DX サポートプログラムの一環で実施した、防衛・航空宇宙産業向け中小企業セミナーを、下記のコンテンツで実施した。

15:30 ご挨拶（名古屋商工会議所）

15:35 航空宇宙・防衛産業分野の情報セキュリティ最前線

～サプライヤー企業が押さえるべき最新動向と対策～

（株式会社エヴァアビエーション）

16:25 中小企業が踏み出す初めの一歩

～サイバーセキュリティお助け隊事業のご紹介～

・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）

・サイバーセキュリティお助け隊の事業説明（PFU）

17:00 質疑応答（質疑終了後に終了）

4.1.1.2 募集施策タイプ別の実証参加効果

表 4-2. 募集施策別の実証参加申込数

募集施策	実証参加社数
エヴァアビエーション社（防衛・航空宇宙産業関連）	8
展示会（エンジン神戸）	6
富士通株式会社（防衛・航空宇宙産業関連）	5
あいちなごや研究会	4
IPA Web サイト	3
全国航空機クラスター・ネットワーク（NAMAC）	2
名古屋のオフラインセミナー	2
栃木航空宇宙懇話会（TASC）	1
日本舶用工業会	1
近畿経済産業局	1
名古屋商工会議所	1
チラシ	1
PFU 公開サイト	1
不明	17
合計	54

4.1.1.3 県別の実証参加社数

対象地域から満遍なく参加しているが、特に東京都、愛知県、兵庫県からの参加が多かった。

表 4-3. 実証参加企業の県別企業数

所在地	社数
東京都	14（-2）
愛知県	8
兵庫県	8
静岡県	5
栃木県	4
神奈川県	3
埼玉県	3（-1）
長野県	2
千葉県	1
群馬県	1
新潟県	1
三重県	1
岐阜県	1
京都府	1
大阪府	1（-1）
総計	**54（-4）**

※東京都、埼玉県、大阪府は実証参加取りやめた企業に-1 を記載

4.1.1.4 業種別の実証参加率

防衛・航空宇宙産業に関わりのある業種を対象としたことから、**製造業**に偏っている。

表 4-4. 実証参加企業の業種別の割合

業種別	参加割合
E. 製造業	**58%**
G. 情報通信業	13%
L. 学術研究、専門・技術サービス業	9%
I. 卸売業・小売業	8%
T. 分類不能の産業	6%
H. 運輸業、郵便業	2%
R. サービス業	2%
T. 分類不能の産業（航空・IT コンサルティング）	2%

4.1.1.5 規模別の実証参加率

小規模から中堅まで各規模の企業が参加している。

表 4-5. 実証参加企業の規模別の割合

従業員数	参加割合
1~5	10%
6~10	10%
11~20	6%
21~50	20%
51~100	24%
101~200	26%
201~300	2%
301~	2%

4.1.1.6 防衛・航空宇宙産業の関係性

防衛･航空宇宙産業に該当、または取引している割合は 90%であり、今後検討している割合は 6%、そのほかが 4%であった。

表 4-6. 防衛・航空宇宙産業との関係性

関係	参加割合
自社が防衛・航空宇宙産業に該当	**15%**
取引がある	**75%**
取引を検討中	3%
取引に興味がある	3%
取引は無い	4%

4.1.1.7 不参加理由

実証事業申込を受けた後に不参加となった企業および事業説明会時点で不参加を表明された企業について、アンケート回答および電話によるヒアリングから得られた不参加理由を下記に集約した。

【メリットなし】　4 件

- 別ベンダーで似たサービスを展開しており、メリットを感じず、年末で忙しいこともあり、辞退する
- メリットを感じないため参加取りやめ
- 既に資産管理ソフトなどの導入が済んでおり二重投資となる
- 現在も UPS やサーバー配信のシステムを導入しており、ベンダーからの提案があり、上層部と相談の上で辞退

【工数理由】 3件

- 社内にセキュリティについて詳しいものがいないので、参加が難しいです
- 年度内、対応が立て込んでしまい、現地でセキュリティ構築など担当するメンバーが他作業にアサインされて作業できなくなり、構築やセキュリティに対して時間を割くことが困難なため、今回は辞退したい。来年度改めて、こういった事業があれば参加させてほしい
- 現状セキュリティ関係にまでは手が回らないため

【事業期間が短い】 3件

- ツールをインストールおよびアンインストール期間を考えると、無償期間が短く有意性が感じられなかったため

【他お助け隊事業者のサイバーセキュリティお助け隊へ参加】 1件

- 他お助け隊事業者が行う、サイバーセキュリティお助け隊（地域版）に参加するため

【当初から実証参加予定なし（団体からの声かけに対応)】 1件

- 航空産業のお客様ともやり取りがあったので興味本位で説明会へ参加したが、事業への参加は考えておらず、またの機会に考えたい。

【コロナ禍】 1件

- コロナ禍の影響も有り、今回は見送りたい

4.1.2 事業説明会のアンケート結果

事業説明会後の電子メールによるアンケートへの回答は、9社から得られた。
10点満点の設問は、ネットプロモータースコア（NPS）により算出した。

1. 本実証事業へのご参加を検討頂けますか。
   1）実証事業に参加します 4社
   2）興味があり検討します 2社
   3）実証事業には参加しません 3社
   - 3か月弱しかなく、あれこれ準備が無駄（使わないツールのセットアップ、アンインストール）
   - 無償期間が短く有意性が感じられなかったため
   - 終了時期に近いため
   - コロナ禍の影響も有り、今回は見送りたい

2. 本事業説明会に参加頂いたきっかけについて教えてください。

1）IPA のサイトを見て　0 社

2）PFU のお知らせサイトを見て　0 社

3）その他の団体から紹介　8 社

- 栃木航空宇宙懇話会（TASC） … 3 社
- 日本舶用工業会
- 全国航空機クラスター・ネットワーク（NAMAC）
- 飯田航空宇宙プロジェクト
- 取引会社
- 本実証事業の運営元企業

3. 本説明会の音声・映像は十分理解できる品質でしたか。

NPS：-13%

- 画像は良かったが音声の大きさにばらつきがあった
- 時折、音声が乱れる
- 発表者により音量にばらつきがあった
- 音量にばらつきあり
- 音声の大きさを統一していただけるとありがたい
  （音声が「小さい」から「大きい」に変化する際、いきなり大音量となっていた）

4.「セキュリティ脅威と対策の必要性について」の内容はご理解いただけましたか。

NPS: ±0%

- 既知の内容が多かった
- 前回の結果が興味深く参考になった

5.「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」の内容はご理解いただけましたか。

NPS: ±0%

- ２月以降の支援の有償・無償の扱い、有償の場合の金額などが不明であった
- すっきりとまではいかないが、分かったように思う

6.「本実証事業の説明」の内容はご理解いただけましたか。

6-1. PFU からの事業説明（パソコンの脆弱性・脅威検知、工場の IT 機器見える化）。

NPS: +12%

- 資料が分かりやすかった
- 分かりやすかった気がする
- 少々声が聞き取りづらく、画面を確認する時間がやや少なかった

6-2. エヴァアビエーションからの説明（セキュリティチェック）。

NPS: -7%

- 聞き取りやすかったが、画面を確認する時間がやや少なかった
- なんとなくわかった

6-3. 富士通からの説明（機密性の高いデータの共有）。

NPS: -25%

- なんとなくわかった
- 概要は理解できましたが、実際の運用環境の紹介があればなお分かり易いと思います
- 内容の規模が大きすぎた
- 少々声が聞き取りづらく、画面を確認する時間がやや少なかった

7. その他、事業説明会で何かご意見・ご感想を記載してください。

- 重複する内容が一部にあったため、内容を整理して 1 時間程度にしていただけるとありがたい
- NIST に対応出来るパソコンの導入と、サイバー保険の加入の必要性は十分理解しており、昨年、防衛省と取引があるすべての企業は、NIST SP800-171 と同等のセキュリティレベルを持つ必要があるとの報道を受け、弊社では Windows 7 のサポート終了を鑑み、NIST に準拠した PC に入替を行っており、製造拠点では構築している。ただし、セキュリティ対策の重要性は十分に理解していても、中小企業にとってサイバー攻撃等の目に見えない物に対する設備に対し、慎重になるため、国等からの何らかの強制力のある指導により導入せざるを得ない状況にした方が対策は進むと考える
- 推測ではあるが、対象地域毎に支援事業の団体が決まっており、今回は PFU が担当されていると考える。今回のサイバーセキュリティ対策支援体制構築事業に関して、事業団体（PFU）を選択した理由について、何らかの説明があったほうがよい。変な先入観が無くなると考える

4.1.3 対象外企業からの参加対応

中小企業に向けた事業であることが伝わっておらず、参加申込を受けて、調査したところ定義に合わないため断った企業が 8 社あった。（製造業で資本金 3 億 10 万円など）

4.2　実態把握結果

4.2.1 セキュリティ意識調査アンケート（①）

意識調査アンケートは、2 回に分けて行ったアンケートを集約し、さらに深堀してアンケートを 2 回目に実施し、下記に回答結果を集約した。

参考までに、昨年度北陸地域で実施した中小企業向けサイバーセキュリティお助け隊事業で得られたデータを項目単位で「【令和元年お助け隊】」を記載する。昨年存在しない項目は省略する。

4.2.1.1 集計対象の母数

集計対象となる回答母数は下記のとおり。

表 4-7. 意識調査アンケートの母数

アンケート	母数となる回答企業数
1 回目（9～12 月） ※2 回目を重なる期間あり	50 社
1 回目（11～12 月）	32 社

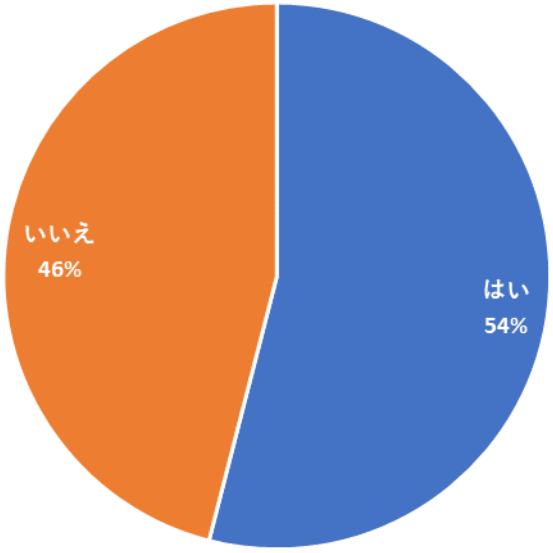
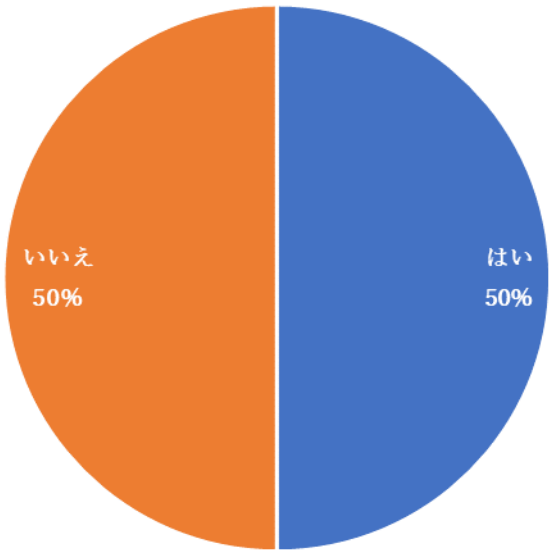
表 4-8. 意識調査アンケートの業種別割合

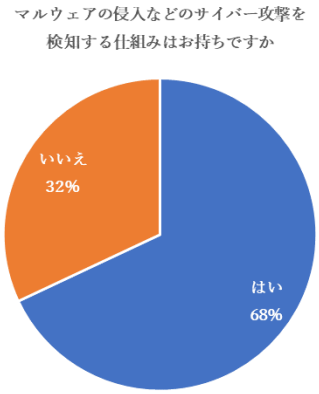
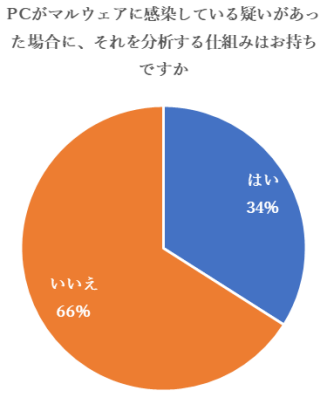
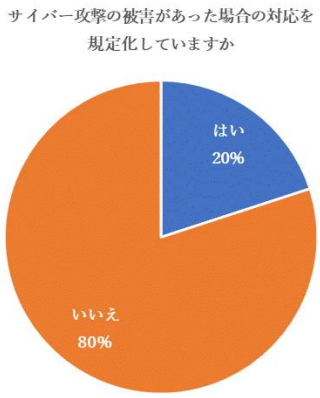
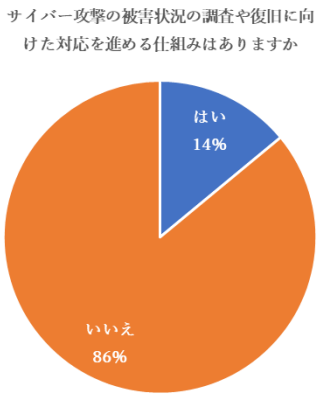
業種	1 回目（事業開始時）	2 回目（事業終了時）
E. 製造業	28 社　(46%)	17 社
G. 情報通信業	6 社　(12%)	6 社
H. 運輸業、郵便業	1 社　(2%)	1 社
I. 卸売業・小売業	4 社　(8%)	2 社
L. 学術研究、専門・技術サービス業	4 社　(8%)	3 社
R. サービス業	2 社　(4%)	1 社
T. 分類不能の産業	5 社　(10%)	2 社

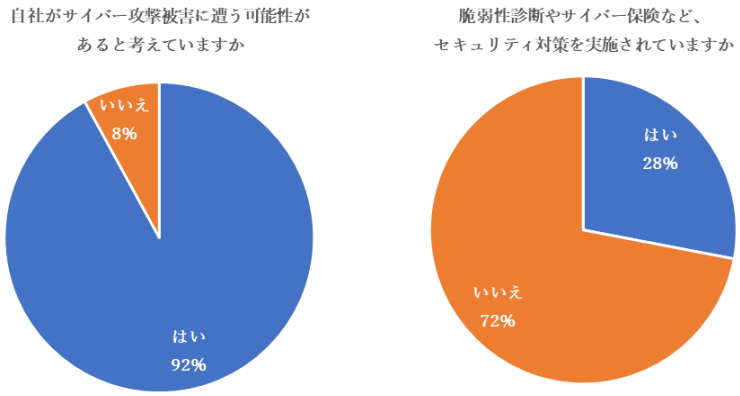
【令和元年お助け隊】製造業は若干少なく 40.7%だった。

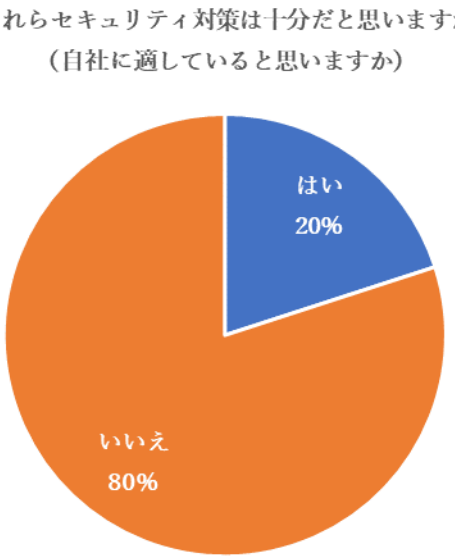
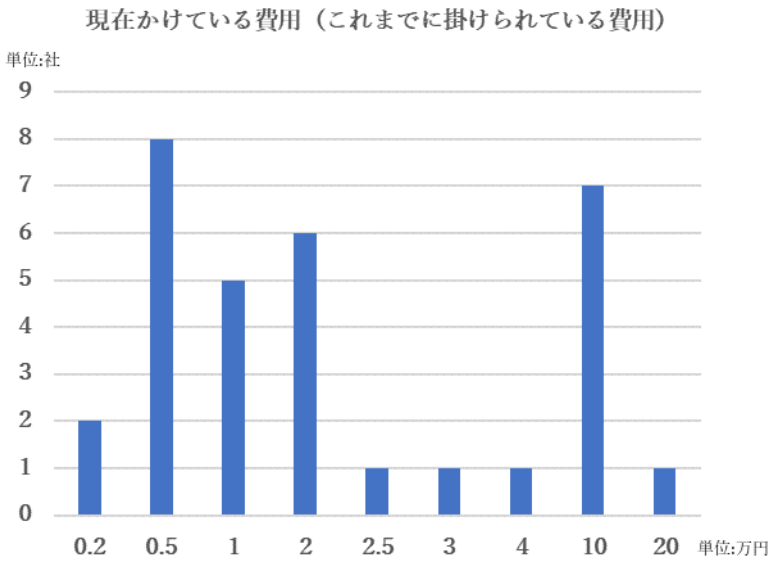
4.2.1.2 傾向

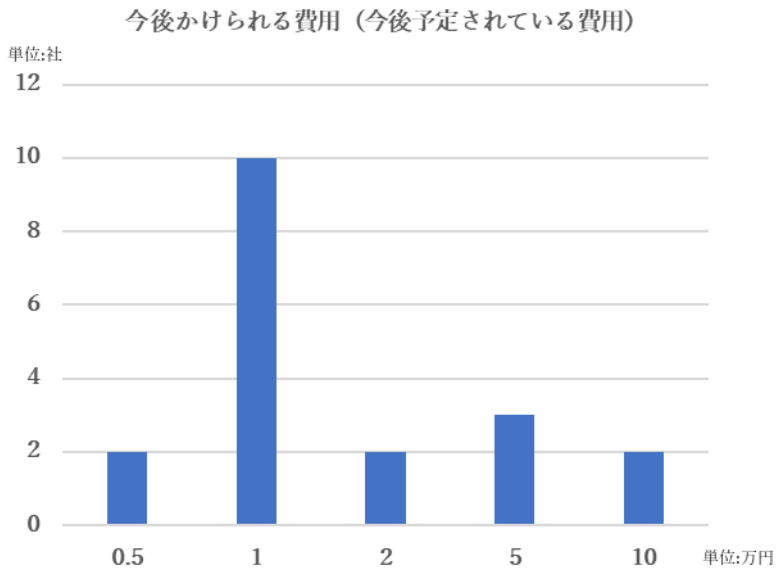
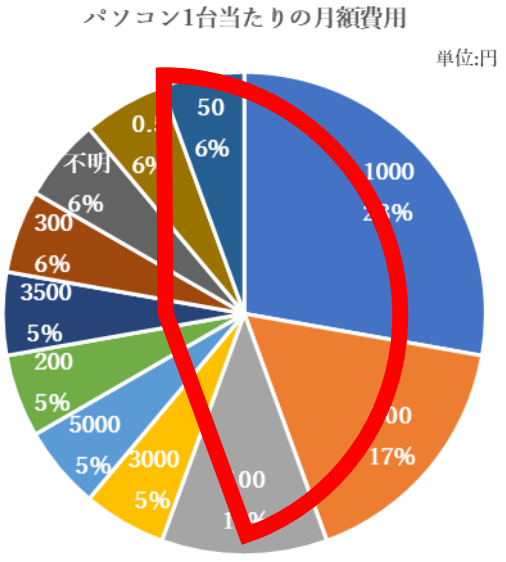
表中のパーセンテージは、特に断りがないものは、設問に「はい」「持っている」「実施している」「行っている」と肯定する企業の割合を表している。表による説明では、縦軸の業種は、件数の多いもの順でソートした。

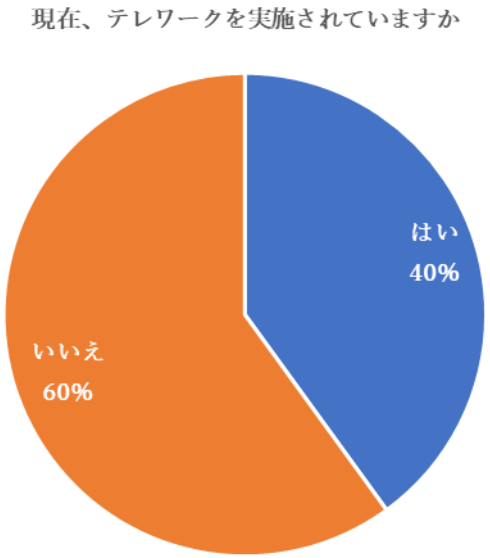
1	サイバー攻撃対策の状況
1-1	セキュリティに関する相談窓口を持っていると答えた企業は 54%である。 【令和元年お助け隊】ほぼ同じ 57%であった。 
1-2	PC の OS やソフトウェアを最新状態に保つ仕組みを導入している 企業は 50%である。 【令和元年お助け隊】ほぼ同じ 56%であった。 

1-3 1-4	マルウェアやサイバー攻撃を検知する仕組みは、過半数の会社が導入しているが、その後に分析する仕組みを導入している企業は 1/3 程度である。 【令和元年お助け隊】ほぼ同じ、検知する仕組み 65%、分析する仕組み 28%であった。  
1-5 1-6	サイバー攻撃に対する規定化や調査・復旧に関する項目は総じて低く、被害状況の調査や復旧対応の仕組みについて、あると回答した 企業は僅か 14%である。 【令和元年お助け隊】ほぼ同じ、規定化 17%、対応を進める仕組み 18%であった。  

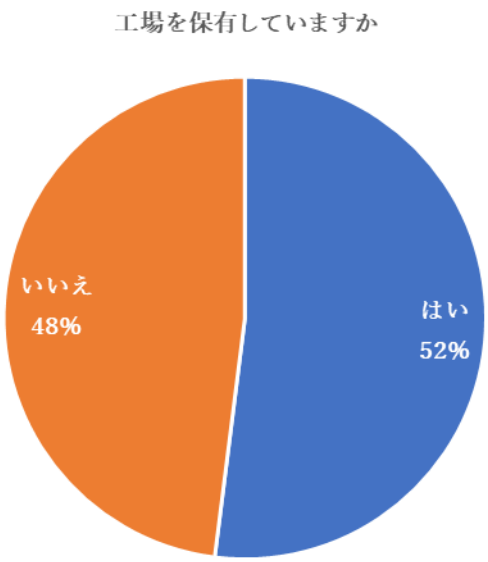
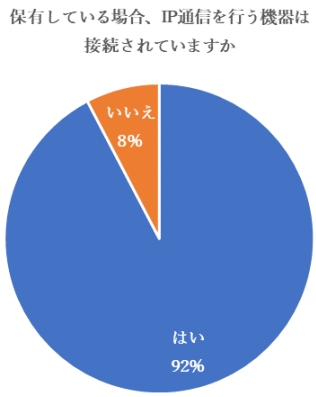
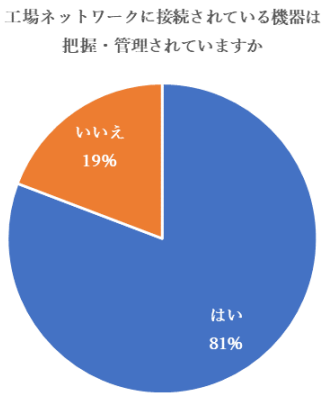
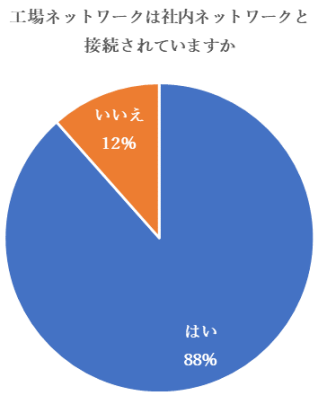
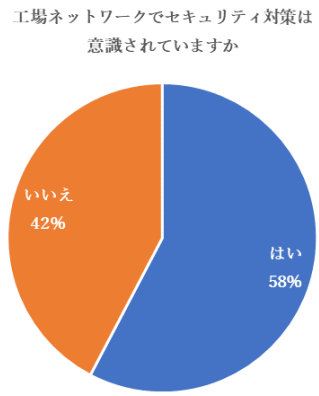
<table>
<tr><td>2</td><td>セキュリティに対する意識</td></tr>
<tr><td>2-1
2-2</td><td>9 割以上の企業で、自社がサイバー攻撃の被害に遭う可能性があると回答。しかし、脆弱性診断やサイバー保険などの対策を採っている企業は 28%に留まった。
【令和元年お助け隊】ほぼ同じ、被害に遭う可能性 85%、脆弱性診断やサイバー保険などの対策 24%であった。
 
</td></tr>
<tr><td>2-2-1</td><td>対策している企業の対策内容は以下のとおりである。
<table>
<tr><td rowspan="5">リスク低減策</td><td>教育</td><td>• ISMS の規定作成とその遵守
• 機密情報保護マニュアルの制定
• IPA 情報の定期的チェック
• e ラーニング</td></tr>
<tr><td>防御</td><td>• アンチウイルスソフトの導入・定期的なスキャン
• UTM の導入
• ファイアウォールの設置
• 社内ネットワークから外部接続不可
• WSUS （Windows Server Update Services）</td></tr>
<tr><td>監視</td><td>• ログ収集
• 資産管理システム</td></tr>
<tr><td>制限</td><td>• USB の使用制限</td></tr>
<tr><td rowspan="2">リスク移転策</td><td>外部</td><td>• サイバー保険へ加入
• セキュアネットワークアウトソーシングサービス
• 保守契約</td></tr>
</table>
【令和元年お助け隊】
主なものは、エンドポイントセキュリティ（アンチウイルスソフトウェア）:25 件、UTM:12 件、ファイアウォール：5 件、サイバー保険：5 件、脆弱性診断：3 件、IT 資産管理（デバイス制御）：3 件、バックアップ：2 件、専門業者とコンサルティング契約：2 件、OS・アプリケーションの脆弱性更新：2 件など。</td></tr>
</table>

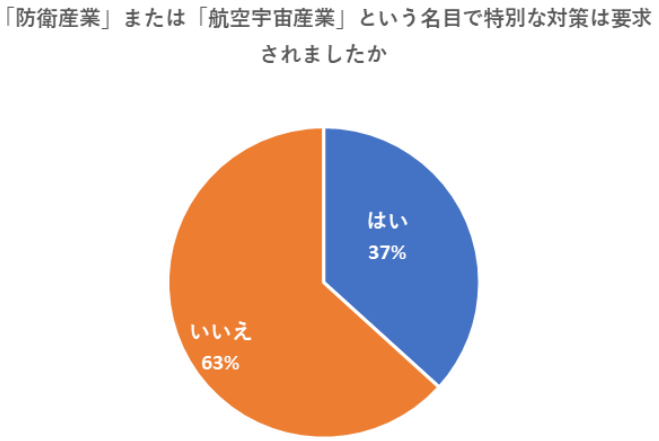
2-3	現在のセキュリティ対策が十分ではない（自社に適していない）と答えた企業は 80%である。 【令和元年お助け隊】ほぼ同じ、十分でない企業は 83%であった。 
2-4-1	現在、セキュリティ対策にかけている費用として、5000 円~2 万円が多く、従業員規模が大きいところで 10 万円という結果である。 【令和元年お助け隊】平均 5.8 万円であった。 

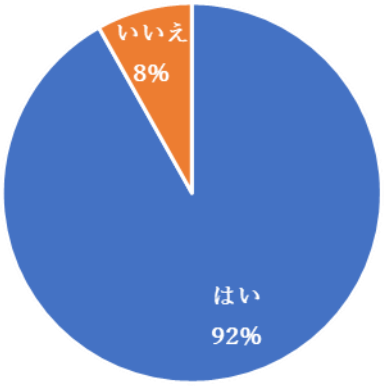
2-4-2	今後、セキュリティ対策にかけられる費用として、 従業員規模問わず 1 万円が最も多いという結果である。 
2-4-3	お助け隊サービスを継続する場合に 1 台あたり幾らまでかけられるかについて以下のような回答が得られた。500 円~1000 円までの割合が半数近くを占めている。 【令和元年お助け隊】ほぼ同じ、月額 643 円であった。 

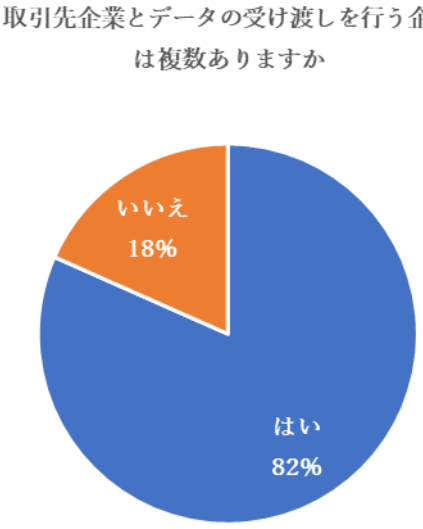
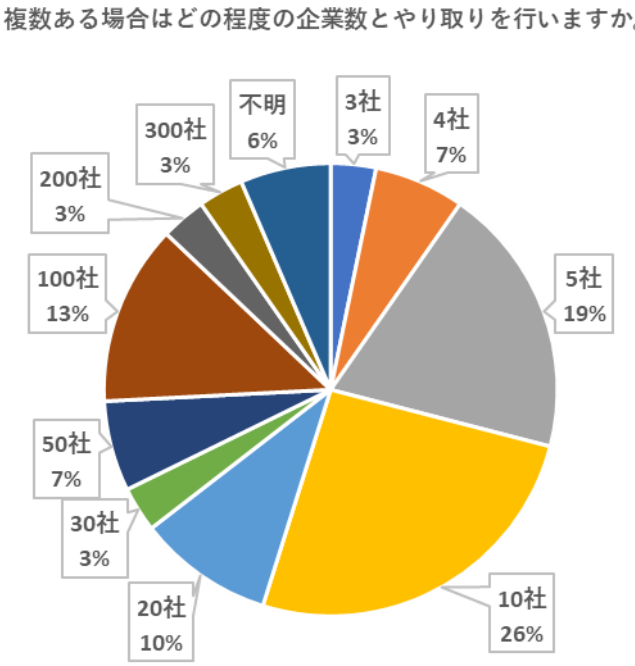
<table>
<tr><td>2-5</td><td>情報セキュリティ対策を進める上での課題や阻害要因として、以下の回答があった。
<table>
<tr><td>教育</td><td>• 運用についての社員への教育と認識
• マイコンなどのセキュリティ対策に対する知識不足
• どこからマルウェアなどが侵入して来るか不安
• リスクのイメージが小さく感じる</td></tr>
<tr><td>コスト</td><td>• セキュリティ対策のコスト
• 旧式機材のリプレース
• 専任の担当者を置けない</td></tr>
<tr><td>仕組み</td><td>• セキュリティ事故発生後、復旧までを速やかに行う仕組み
• リモートワークの増大
• 機密情報の管理</td></tr>
<tr><td>ガイドライン</td><td>• 規定の整備、仕組み、体制、知識
• どこまで対策すればいいかわからない
• 会社の規模や業務内容に合わせて、具体的にどのような対策をしたら良いのか示してくれる Play Book が無い</td></tr>
<tr><td>業務効率</td><td>• 業務効率の低下
• セキュリティ対策ソフトに対する信頼性</td></tr>
</table></td></tr>
<tr><td>2-6</td><td>テレワークを実施している企業は 40%である。
 
</td></tr>
</table>

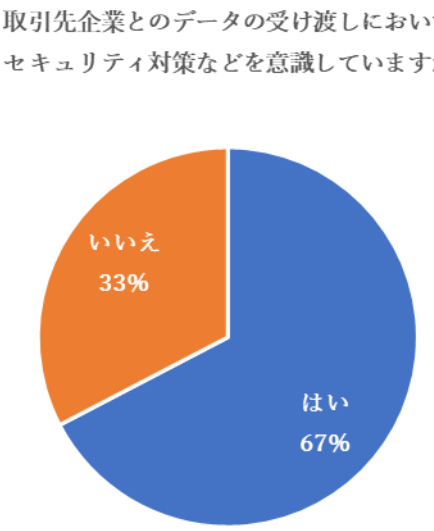
<table>
<tr><td>2-6-1</td><td>テレワークされている場合の社外利用時のセキュリティ対策について、以下の回答があった。
<table>
<tr><td>特定</td><td>• リモートデスクトップ接続で、各種認証に電子証明書とパスワード認証を併用</td></tr>
<tr><td>防御</td><td>• アンチウイルスソフトの導入
• VPN の導入
• 暗号化
• データ保管場所のセキュリティ確保</td></tr>
<tr><td>制限</td><td>• MAC アドレスによるアクセス制限
• MDM
• データレス PC
• テレワーク実施場所の限定
• リモートデスクトップ専用環境の使用
• 公衆無線 LAN の使用禁止</td></tr>
<tr><td>監視</td><td>• システムログの収集</td></tr>
<tr><td>外部</td><td>• クラウドサービスでのファイル共有
• サイバー保険</td></tr>
</table></td></tr>
<tr><td>2-6-2</td><td>テレワークの導入を進める上での課題として、以下の回答があった。
<table>
<tr><td>紛失対策</td><td>• 機器の紛失対策
（PC 暗号化、管理者によるリモートワイプ）</td></tr>
<tr><td>漏えい対策</td><td>• 情報漏えい検知・対策
• 社外取り扱いデータの管理と方法
• 情報記憶媒体による情報流出
• 自宅の Wi-Fi セキュリティに対する不安
• ネットワーク関連のセキュリティの実装</td></tr>
<tr><td>環境整備</td><td>• 通信環境の改善
• テレワーク用の環境が未構築</td></tr>
<tr><td>ガイドライン/ポリシー</td><td>• セキュリティ対策レベルに統一性が無い
• 運用ルール整備と徹底、教育
• セキュリティに関する規定がない
• どのようにセキュリティ対策したら良いかわからない</td></tr>
<tr><td>人事評価</td><td>• コミュニケーション・作業実績の評価</td></tr>
</table></td></tr>
</table>

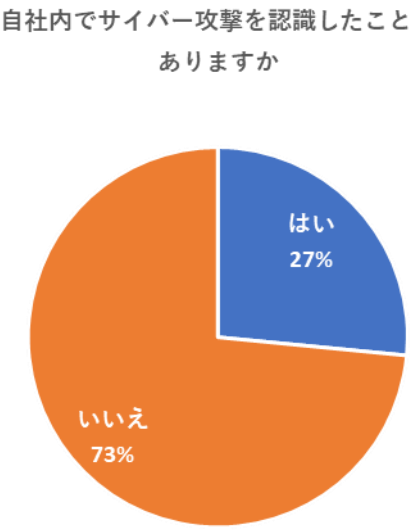
2-7	工場を保有している企業は 60%である。 
2-7-1 2-7-3	工場を保有している殆どの企業で、IP 通信を行う機器が 接続されており、機器の把握や管理をしていると回答。  
2-7-2 2-7-4	工場と社内のネットワークが独立していない企業が多く、 工場ネットワークのセキュリティ対策を意識していないと 答えた企業が 42%ほどあった。  

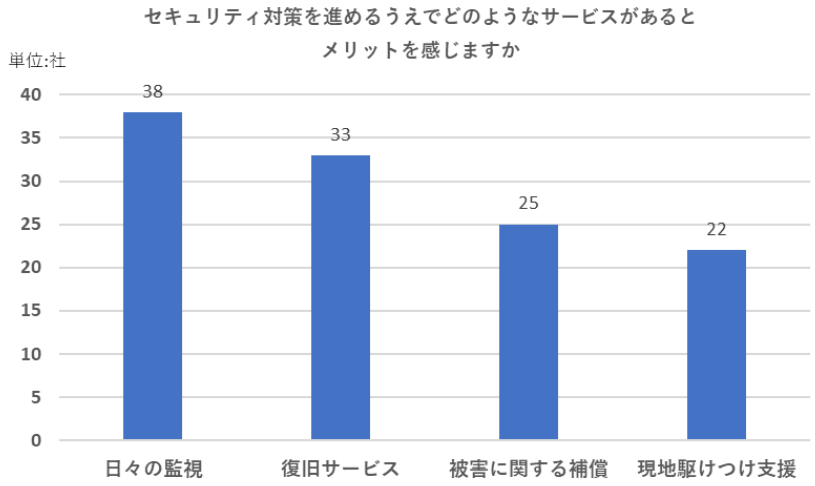
<table>
<tr><td>2-7-5</td><td>工場ネットワークのセキュリティ対策として、以下の回答があった。<table>
<tr><td>防御</td><td>• 統合型ゲートウェイセキュリティ（UTM） ×2 件
• アンチウイルスソフトの導入
• エンドポイント・ソフト更新管理</td></tr>
<tr><td>制限</td><td>• 資産管理
• 外部メディアの制限
• スタンドアローンでの運用</td></tr>
<tr><td>監視</td><td>• ログ収集・分析
• システム監視ソフトウェア
• 毎月 1 回の定期的な診断</td></tr>
<tr><td>外部</td><td>• セキュアネットワークアウトソーシングサービス</td></tr>
<tr><td>秘匿化</td><td>• 秘密情報が特定される名称などの略化、暗号化</td></tr>
<tr><td>教育</td><td>• e ラーニング</td></tr>
</table></td></tr>
<tr><td>3</td><td>サプライチェーン</td></tr>
<tr><td>3-1</td><td>防衛産業、航空宇宙産業という分野に対して対策を要求されたのは
38%の企業。業種、規模で割合が偏るといった事態は見られない。
【令和元年お助け隊】ほぼ同じ、一定レベルのセキュリティ対策が要件に含まれているケースは 42%であった。
 
</td></tr>
</table>

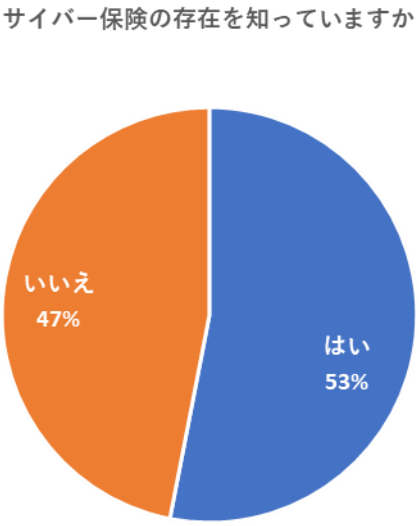
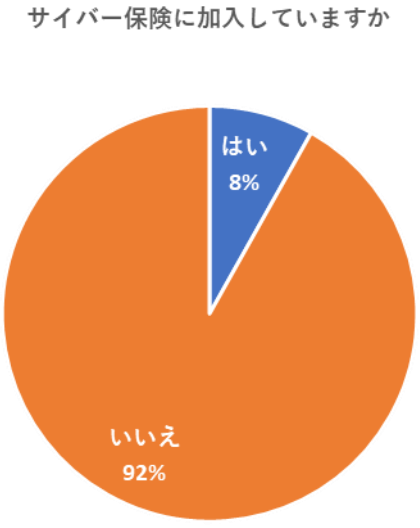
3-1-1	要求された対策として「知るべき人にだけ知らせる」（Need to know の原則）、「アクセス権は必要最小限の範囲でのみ認められるべき」（Least privilege の原則）が要求されている。 防衛・航空宇宙産業では、機密情報を扱う上で、クローズなネットワーク環境も要求されているケースもある。 ・機密保持、情報の**保管・閲覧・複製の制限** ・社内においても機密情報へ**アクセスできる人員を管理（制限）**する ・暗号化、**部外者の立ち入り制限**、データ情報の管理 ・高度な機密情報を扱う場合は**完全オフライン環境**で行う
3-2	データの受け渡しがあるのは 90%の企業である。 今回実証参加した企業の殆どがデータの受け渡しを行っている。 
3-2-1	職種の割合上、図面や部品のデータが多い。それ以外は、余り記載がなく契約書や納品情報が機微と記載された企業も少なかった。 ・**機体、部品、配合表などのデータ**（12 社） ・個人や顧問先のセンシティブ情報など ・契約書、納品資料
3-2-2	規模の大きな企業ほどデータのやり取りを行う人数が全体数に比較して少ない。全体数が少ない企業は全員がやり取りを行っている。業種ごとで偏りはない。製造業でもほぼ全員がやり取りを行っている企業もある。 ※小さい会社ほど全社員に教育が必要

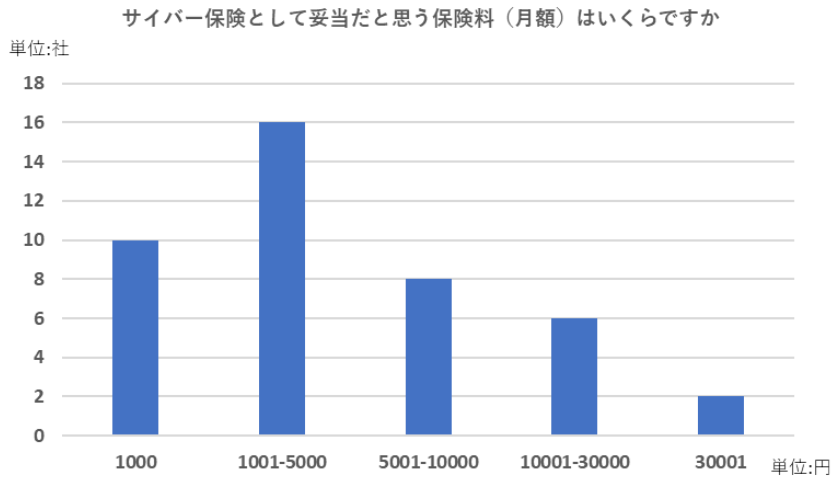
3-2-3	一番多く使用されていたのは電子メールであり、暗号化やパスワード設定しているところも見られた。機微なデータは、手渡しをされているとの意見もあった。 ・メール　×34 件 ・手渡し　×11 件 ・ストレージサービス　×10 件 ・郵便　×4 件
3-2-4	複数の企業とデータのやり取りをするのは 82%である。殆どの企業が複数の企業とやり取りを行っている。 
3-2-4-1	殆どの企業が 10 社、20 社の企業とやり取りを行っていると回答している。 

3-2-5	データの受け渡しにおいてセキュリティ対策を意識しているのは全体の 67%である。3 分の 1 の企業が受け渡し時に対策を行っていない。 
3-2-5-1	意識している 67%は、メールを使用する際のパスワードの設定、暗号化が主に行われている。機微情報などは手渡しをするという対策を行っている企業もある。ストレージサービスではアクセス制限を行っている。 ・パスワード設定、メール暗号化　×24 件 ・手渡し　×2 件 ・ストレージサービスでのアクセス制限　×1 件
3-2-6	意識していない 33%は、主に見られたのは運用が煩雑になる、運用方法がわからないといった意見。時間とコストがかかると考えている企業も一部ある。意識していない、重要なデータのやり取りをしていないと認識しているという意見もあった。 ・運用が煩雑になる ・コストが増える ・意識していなかった ・知識と技術が足らず、周知徹底に至らない

4	サイバー攻撃被害の実態
4-1	サイバー攻撃を認識したことがあるのは全体の 27%である。規模、分野ともに偏りがあるわけではないため、どの分野でもサイバー攻撃を受ける可能性があると言える。 【令和元年お助け隊】ほぼ同じ、31%であった。 
4-1-1	認識した被害の内容は下記のとおり。 ・ ランサムウェア ・ トロイの木馬 ・ バックドア ・ Emotet ・ サーバーへの攻撃 ・ 実害はないが迷惑メールを受信 【令和元年お助け隊】 ランサムウェア：8 件、Web サーバーの侵害（改ざん）：7 件、メール乗っ取り（なりすましメール）：5 件、マルウェア付きメールの開封：4 件、迷惑メールが届く：4 件、フィッシングメール：3 件、被害・攻撃はない：3 件、マルウェア感染拡大（共有フォルダ）：2 件、サービス妨害攻撃（DoS）：2 件、標的型メール：2 件であった。
4-1-2	その際の対応は下記のとおり。 【実害ない場合の対応内容】 ・ 削除 ・ 無視 ・ 攻撃を確認したが、ルーターで止まっていた 【実害がある場合の対応内容】 ・ バックアップから復旧したのち駆除対策 ・ 収まるまで待つしかなかった ・ 初期化した

4-2	自社内で保有する情報が漏えいした場合、どの程度の被害が出ると想定されているか確認した。多かった意見は取引停止・契約解除・信頼損失という意見である。さらにその後に売上減退、損害賠償に発展することを認識している企業も見られる。最悪のケースとして倒産があり得る企業もあった。 回答内容は以下のとおりである。 • 取引停止 ×6 件 • 契約解除 ×5 件 • 信頼損失 ×5 件 • 売上減退 ×3 件 • 補償金の支払い、損害賠償 ×3 件 • 倒産 ×2 件
4-3	セキュリティ対策を進める上でメリットを感じるサービスとしては、日々の監視が 76%、復旧サービスが 66%、被害に関する補償が 50%、現地駆け付け支援が 44%の企業がメリットを感じると答えている。日々の監視は多くの企業でメリットを感じているが、現地駆け付け支援は余りメリットを感じられていない。 【令和元年お助け隊】ほぼ同じ、監視サービス：54%、復旧サービス：49%、被害に対する補償（サイバー保険）：29%　（駆け付けサービスは設問なし） 
4-4	情報漏えいが発生した場合、取引先、客先、市場などに対して行う対応としては、報告謝罪、賠償、情報公開、再発防止と続くが、数は少ないものの最後に書かれている原因調査も報告や再発防止に必要となる。 ・ 報告謝罪 ×21 件 ・ 損害賠償 ×9 件 ・ 情報公開 ×5 件

	・ 再発防止措置の実施 ×3 件 ・ 市場へ報告 ×2 件 ・ 各所と協議 ×2 件 ・ 原因調査 ×1 件
5	サイバー保険
5-1	サイバー保険の存在を知っているのは 53%であり、約半数は認知していない。 【令和元年お助け隊】33%であったため、昨年より認知が進んでいる。 
5-2	サイバー保険に加入しているのは 8%であり、存在を知っている割合と比較してもとても少ないことがわかる。 

5-3	加入している理由として挙がったのは取引先から求められた、万が一のためという意見である。加入していない理由として主に挙げられているのは、保険の詳細がわからないといった意見である。 • 加入している理由 ➢ 万が一の訴訟、賠償対応 ➢ 取引先から求められたため • 加入していない理由 ➢ 保険の詳細がわからない ➢ 必要性を感じない ➢ 先に社内のセキュリティを向上させたい ➢ 予算がない
5-4	既存のサイバー保険やサービスの価格について把握していない、高いという意見が多かった。補償金を考慮すると高いと感じないという意見もあった。別の保険に組み込まれているため単体での金額は把握できていないという意見もあった。 【令和元年お助け隊】高い：46%、わからない：39%、高くない：15%であった。
5-5	サイバー保険の妥当だと思う保険料は 1000 円以下が 24%、1001-5000 円が 38%、5001-10000 円が 19%、10001-30000 円が 14%、30000 円以上が 5%となっている。 

5-6	どのような費用が保険で補償されるとメリットを感じるか尋ねたところ、多く挙がっていたのが損害賠償、復旧、弁護士の費用についての補償があるといいという意見である。 • 損害賠償費用 • 事故対応費用 • 設備機器更新費用 • 復旧費用 • 弁護士依頼料 • 費用全額 • 被害、訴訟、補償にかかる費用

4.2.2 セルフアセスメント「情報セキュリティ整備状況診断」(③)

IPA「5 分でできる! 情報セキュリティ自社診断」の 25 問に加え、NIST SP800-171、CMMC ベストプラクティスレベル 1、防衛省の管理基準に基づいたヒアリング項目を加え、実証参加企業のセキュリティ対策整備状況を診断した。これにより、セキュリティ対策の現状と今後、防衛・航空宇宙産業において求められる要件とのギャップを分析する。

実証参加企業 50 社が情報セキュリティ整備状況診断を実施した。

4.2.2.1 従業員数別の得点分布

従業員数別に満点を 100%とした得点の分布をプロットした。

明確な傾向は見られなかった。

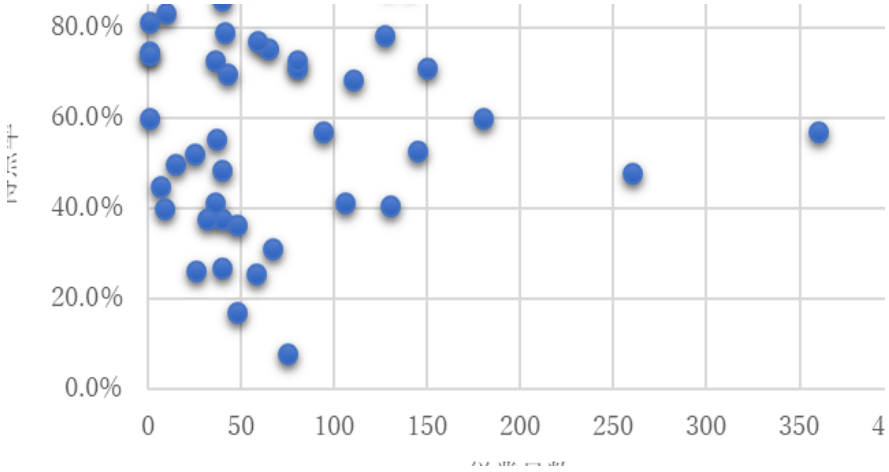


図 4-9. 従業員数別の得点分布

4.2.2.2 設問種別ごとの平均得点

設問の種別ごとに合計得点を、満点に対する比率として下記に集計した。

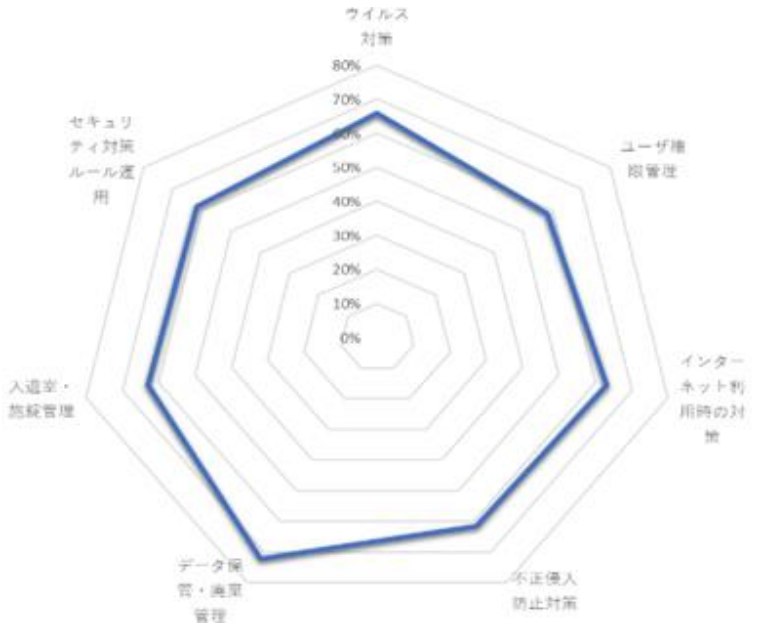


図 4-10. 設問種別ごとの平均得点

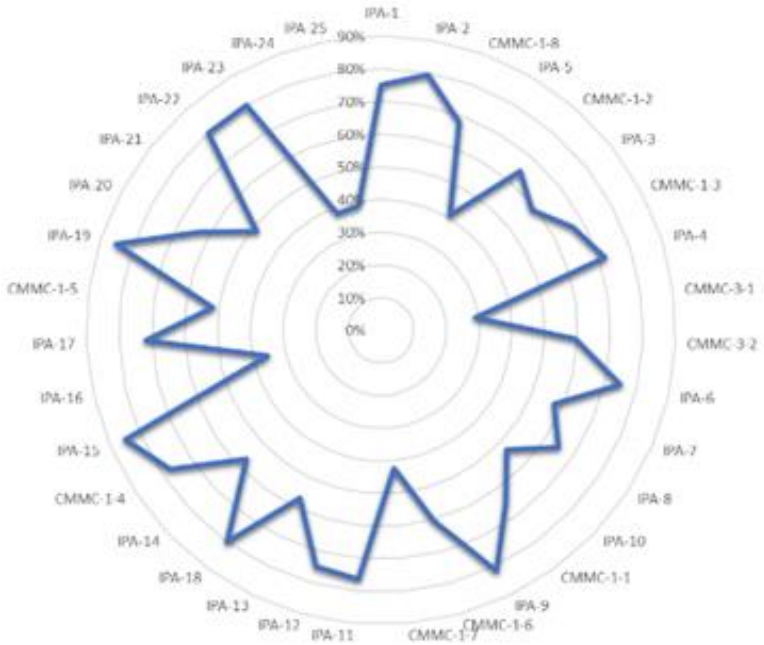


図 4-11. 設問ごとの平均得点

全平均得点は、63.3%であった。なお、種別ごとの平均からは特段の傾向は見えないが、項目ごとにはバラつきが見られた。以下に設問ごとの回答分布により傾向を考察する。

4.2.2.3 各設問の回答比率

参考までに、昨年度北陸地域で実施した中小企業向けサイバーセキュリティお助け隊事業で得られた「5 分でできる! 情報セキュリティ自社診断」に関するデータを、「実施」列のパーセンテージの下段「昨年」として記載する。「CMMC」の項目は昨年存在しないため省略する。

表 4-12. 各設問の回答比率

設問番号（CMMC L1 対象か否か）	設　問	実施	一部実施	未実施	不明	未回答
種別「ウイルス対策」						
IPA-1（L1 対象）	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	58% 昨年 52%	34%	6%	0%	2%
IPA-2（L1 対象）	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？　（※1：コンピューターウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。）	68% 昨年 74%	24%	4%	2%	2%
CMMC-1-8（L1 対象）	パソコンやスマホなどについてウイルス対策ソフトで、定期的にスキャンするとともに、外部からのファイルをリアルタイムスキャンしていますか？	56%	26%	12%	4%	2%
IPA-5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	28% ★ 昨年 19%	28%	38%	4%	2%
種別「ユーザー権限管理（ID とパスワード管理）」						
CMMC-1-2（L1 対象）	システムを利用できるユーザー、装置などを特定し、ID を発行し、付与していますか？	56%	18%	22%	2%	2%
IPA-3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	44% ★ 昨年 29%	34%	12%	8%	2%
CMMC-1-3（L1 対象）	ユーザー、装置などがシステムを利用できるようにする前に、ユーザー、装置などの ID をパスワードなどにより認証していますか？	54%	26%	14%	2%	4%
IPA-4（L1 対象）	重要情報※2 に対する適切なアクセス制限を行っていますか？　（※2 ：重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。 ）	58% 昨年 45%	30%	6%	4%	2%
CMMC-3-1	特権アカウントを利用する場合や、リモートアクセスを行う場合、ユーザーがシステムを利用できるようにする前に、多要素認証※を行っていますか？（※：複数の要素（記憶情報、所持情報、生体情報）を用いた認証方式）	16% ★	26%	56% ★	0%	2%
CMMC-3-2	秘密情報を含む媒体へのアクセスを管理し、社外への送信/輸送時も、許可された者だけがアクセスできるようにしていますか？	48% ★	24%	24%	2%	2%
種別「インターネット利用時の対策」						
IPA-6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	64% 昨年 51%	24%	8%	4%	0%
IPA-7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	50%	18%	26%	6%	0%

設問番号（CMMC L1 対象か否か）	設　問	実施	一部実施	未実施	不明	未回答
		昨年 24%				
IPA-8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	44%★ 昨年 11%	42%	14%	0%	0%
IPA-10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？	34% ★ 昨年 21%	38%	26%	0%	2%
CMMC-1-1（L1 対象）	ニュースリリースなど外部公表する情報を管理、制限し、契約情報を含む可能性のある情報を、公開 Web サイトなどに掲載許可しないようにしていますか？	56%	20%	18%	4%	2%
種別「不正侵入防止対策」						
IPA-9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	80% 昨年 54%	6%	8%	6%	0%
CMMC-1-6（L1 対象）	社内システムをインターネット接続する場合、ファイアウォール、Web プロキシなどを利用して、送受信される情報を監視・管理・保護していますか？	58%	8%	28%	6%	0%
CMMC-1-7（L1 対象）	外部に公開する Web サーバー、メールサーバーなどがある場合、内部ネットワークから分離された DMZ セグメントに配置していますか？	46% ★	2%	34%	18%	0%
種別「データ保管・廃棄管理」						
IPA-11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	62% 昨年 59%	30%	6%	2%	0%
IPA-12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は　机上に放置せず、書庫などに安全に保管していますか？	60% 昨年 28%	30%	10%	0%	0%
IPA-13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	40% ★ 昨年 19%	34%	26%	0%	0%
IPA-18（L1 対象）	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	70% 昨年 51%	20%	10%	0%	0%
種別「入退室・施錠管理」						
IPA-14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	40% ★ 昨年 24%	34%	26%	0%	0%
CMMC-1-4（L1 対象）	社内施設（事務所、工場など）や社内システム・装置のアクセス（入室、利用）を許可した人に限定していますか？	66%	22%	12%	0%	0%
IPA-15（L1 対象）	関係者以外の事務所への立ち入りを制限していますか？	74% 昨年 61%	22%	4%	0%	0%
IPA-16（L1 対象）	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	26% ★ 昨年 15%	20%	50% ★	2%	2%
IPA-17	事務所が無人になる時の施錠忘れ対策を実施していますか？	64%	16%	20%	0%	0%

設問番号（CMMC L1 対象か否か）	設　問	実施	一部実施	未実施	不明	未回答
		昨年 47%				
CMMC-1-5（L1 対象）	社内施設（事務所、工場など）や機器に、いつ誰がアクセス（入室、利用）しているか記録を残していますか？	42% ★	20%	38%	0%	0%
種別「セキュリティ対策ルール運用」						
IPA-19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	76% 昨年 54%	18%	6%	0%	0%
IPA-20	従業員にセキュリティに関する教育や注意喚起を行っていますか？	48% ★ 昨年 21%	30%	22%	0%	0%
IPA-21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	38% ★ 昨年 25%	22%	38%	2%	0%
IPA-22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	72% 昨年 30%	18%	6%	4%	0%
IPA-23（L1 対象）	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？	74% 昨年 44%	14%	8%	4%	0%
IPA-24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	32% ★ 昨年 11%	14%	50% ★	4%	0%
IPA-25	情報セキュリティ対策（上記 IPA-1 ～ IPA-24 など）をルール化し、従業員に明示していますか？	30% ★ 昨年 11%	18%	50% ★	2%	0%

4.2.2.4 診断結果の傾向

昨年度、北陸地域で実施した中小企業向けサイバーセキュリティお助け隊事業で得られた「5 分でできる! 情報セキュリティ自社診断」に関するデータと比較したところ、IPA-2 のウイルス対策に関する設問以外、防衛・航空宇宙産業では全ての項目で昨年より実施率が高い。

しかしながら、設問回答の中で、「実施している」回答比率が 50%に達していないもの（★を記載）が 35 項目中、43%の 15 項目が該当した。以下の傾向が見られる。

- 外部への秘密情報持ち出し時の対策が不十分
- パスワード管理が不十分
- 事務所内の物理的安全管理対策が不十分
- 情報セキュリティに関する仕組みが未整備

各傾向の概要を以下に示す。

(1) 外部への秘密情報持ち出し時の対策が不十分

外部への秘密情報をメール送信する場合、外部へ紙媒体などで秘密情報を持ち出す場合のセキュリティ対策が採られていない。

- ✓ 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護することをしていない（IPA-8）
- ✓ インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていない（IPA-10）
- ✓ 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていない（IPA-13）
- ✓ 秘密情報を含む媒体へのアクセスを管理し、社外への送信/輸送時も、許可された者だけがアクセスできるようにしていない（CMMC-3-2）

(2) パスワード管理が不十分

パスワード管理が不十分で、多要素認証の導入が行われていない。

- ✓ パスワードは破られにくい「長く」「複雑な」パスワードを設定していない（IPA-3）
- ✓ 特権アカウントを利用する場合や、リモートアクセスを行う場合、ユーザーがシステムを利用できるようにする前に、多要素認証を行っていない（CMMC-3-1）

(3) 事務所内の物理的安全管理対策が不十分

事務所内の物理的安全管理対策がとられておらず、事務所内は安全なエリアとして捉えている傾向にある。

- ✓ 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていない（IPA-14）
- ✓ 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていない（IPA-16）
- ✓ 社内施設（事務所、工場など）や機器に、いつ誰がアクセス（入室、利用）しているか記録を残していない（CMMC-1-5）

(4) 情報セキュリティに関する仕組みが未整備

社内の情報セキュリティに関する仕組み作りを行っておらず、セキュリティ事故発生時対応手順、情報セキュリティに関するルールが未整備で、従業者へのセキュリティ教育も実施していない。

- ✓ 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みができていない（IPA-5）
- ✓ 従業員にセキュリティに関する教育や注意喚起を行っていない（IPA-20）
- ✓ 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていない（IPA-21）
- ✓ セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていない（IPA-24）
- ✓ 情報セキュリティ対策（上記 IPA-1 ～ IPA-24 など）をルール化し、従業員に明示していない（IPA-25）

4.2.2.5 個社ごとへの指導と結果

実施した各社には、実施結果とともに、コンサルタントによるコメントを付して、各社にフィードバックした。以下にその例を示す。

※点数は、「実施している」4 点、「一部実施」2 点、「実施していない」0 点、「わからない」-1 点　※未回答の設問は 0 点とした。

① 「設問の種別ごと」の採点

表 4-13. 設問の種別ごとの採点

設問の種別		得点/満点	達成率
1	ウイルス対策	8/16	50%
2	ユーザー権限管理（ID とパスワード管理）	12/24	50%
3	インターネット利用時の対策	20/20	100%
4	不正侵入防止対策	4/12	33%
5	データ保管・廃棄管理	12/16	75%
6	入退室・施錠管理	16/24	67%
7	セキュリティ対策ルール運用	12/28	43%
合計		84/140	60%

② IPA「5 分でできる! 情報セキュリティ自社診断」25 問の採点

表 4-14. IPA「5 分でできる! 情報セキュリティ自社診断」25 問の採点

設問の種別	得点/満点	達成率
Part1:基本的対策（IPA-1~5 の 5 問）	10/20	50%
Part2:従業員としての対策（IPA-6~19 の 14 問）	46/56	82%
Part3:組織としての対策（IPA-20~25 の 6 問）	10/24	42%
合計	66/100	66%

③ 「CMMC レベル 1」15 問のプラクティスごとの採点

表 4-15. CMMC レベル 1 のプラクティスごとの採点

CMMC レベル 1 プラクティス	得点/満点	達成率
AC.1.001, AC1.002: ユーザー/機器のアクセス管理 （IPA-4）	4/4	100%
AC.1.003: 信頼できる外部サービスの使用 （IPA-23）	4/4	100%
AC.1.004: 公開情報の管理 （CMMC-1-1）	4/4	100%
IA.1.076: ユーザー/機器の識別管理 （CMMC-1-2）	0/4	0%
IA.1.077: ユーザー/機器の識別認証 （CMMC-1-3）	0/4	0%
MP.1.118: 重要情報の消去 （IPA-18）	4/4	100%
PE.1.131: 入退出管理 （CMMC-1-4）	4/4	100%
PE.1.132: 外部訪問者管理 （IPA-15）	4/4	100%
PE.1.133: 入退室記録管理 （CMMC-1-5）	0/4	0%
PE.1.134: 機器・備品の盗難防止措置 （IPA-16）	2/4	50%
SC.1.175: インターネット通信監視・管理・保護 （CMMC-1-6）	0/4	0%
SC.1.176: インターネット境界管理・保護 （CMMC-1-7）	0/4	0%
SI.1.210: OS/ソフトウェア更新 （IPA-1）	2/4	50%
SI.1.211, SI.1.212: ウイルス対策ソフト導入 （IPA-2）	2/4	50%
SI.1.213: ウイルス対策リアルタイムスキャン （CMMC-1-8）	4/4	100%
合計	34/60	57%

4.2.2.6 SECURITY ACTION の促進

本実証事業に参加されている 50 社中、取得状況は下記のとおり。

残念ながら促進の結果としては+3 社にとどまっている。これはアンケート回答が 12 月末に集中し、本コンサルタントからの回答を得てからの行動として、集計時点でのアクションが得られなかったと考える。

表 4-16. SECURITY ACTION の宣言状況

	一つ星	二つ星
実証参加時	10 社	6 社
12 月末時点	13 社 （+3 社）	6 社

4.2.3 社内パソコンの脆弱性診断（②）

4.2.3.1 サポート切れ / サポート切れ間近な OS の利用率

サポート切れとなるバージョンは半年単位で増えているが、現在も使い続けている状況を報告する。 初めに 2020 年 12 月末時点で Windows 7 や Windows 8.1 に加え、Windows10 内のバージョン（半期アップデート）においてもサポート切れになるバージョンが存在する。成果報告会で啓発するとともに、状況を下記に取りまとめた。

表 4-17. OS バージョンのサポート期限

OS バージョン	サポート期限	
Windows 7	サポート期限切れ	
Windows 8.0	サポート期限切れ	
Windows 8.1	サポート期限切れ	
Windows 8.1 延長サポート	2023/1/10	
Windows 10	Home/ Pro/ Pro Education/ Pro for Workstation/ IoT Core	Enterprise/Education/IoT Enterprise
Version 1809	サポート期限切れ（2020/11/10）	2021/05/11
Version 1903	サポート期限切れ （2020/12/08）	
Version 1909	2021/05/11	2022/05/10
Version 2004	2021/12/14	
Version 20H2 （Microsoft 推奨）	2022/05/10	2023/05/09
4.2.3.2 Windows Server 2008	サポート期限切れ （2020/01/14）	
Windows Server 2012	2023/01/10	
Windows Server 2016	2027/01/10	
Windows Server 2019	2029/01/09	

※Windows 7 を 1 年ごとに最大 3 年セキュリティ更新を受けられる ESU （Extended Security Update を除く）

※Windows 10 Enterprise および IoT Enterprise の長期間サポート（LTSB/LTSC）エディションを除く

※参考 URL

- Microsoft：Microsoft ライフサイクル ポリシー, https://docs.microsoft.com/ja-jp/lifecycle/ （2020/12/28）
- Microsoft：Windows 7 ESU に関する FAQ, https://docs.microsoft.com/ja-jp/troubleshoot/windows-client/windows-7-eos-faq/windows-7-extended-security-updates-faq （2020/12/28）
- Microsoft：Windows 10 リリース情報, https://docs.microsoft.com/ja-jp/windows/release-information/ （2020/12/28）
- Microsoft：Windows Server 2008 と Windows Server 2008 のサポート Windows Server 2008 R2, https://docs.microsoft.com/ja-jp/troubleshoot/windows-server/windows-server-eos-faq/end-of-support-windows-

server-2008-2008r2 （2020/12/28）

12 月末時点において、監視サービスを利用する企業 50 社、監視対象のパソコン 502 台で稼働している OS バージョンについて、Windows Management Instrumentation （WMI）インタフェースを通して得られた OS バージョンを列挙した。**サポート期限切れとなっている OS が 72 台（14.3%）、半年以内にサポート切れとなる OS が 149 台（29.7%）利用されていた。**

表 4-18. パソコン上の OS バージョン

OS バージョン名	台数
Microsoft Windows NT 6.0.6001 Service Pack 1 （Vista）	1
Microsoft Windows NT 6.1.7601 Service Pack 1 （Windows 7）	6
Windows 7 Service Pack 1 （Build 7601） 32bit	12
Windows 7 Service Pack 1 （Build 7601） 64bit	6
Windows 10.0 （Build 17134） 64bit （Version 1803）	1
Windows 10.0 （Build 17763） 64bit （Version 1809）	2
Windows 10.0 （Build 18362） 64bit （Version 1903）	23
Windows 10.0 （Build 18363） 32bit （Version 1903）	20
Windows 10.0 （Build 18363） 64bit （Version 1909）	149
Windows 10.0 （Build 19041） 32bit （Version 2004）	4
Windows 10.0 （Build 19041） 64bit （Version 2004）	73
Windows 10.0 （Build 19042） 32bit （Version 20H2）	3
Windows 10.0 （Build 19042） 64bit （Version 20H2）	25
Windows 10.0 （Build 21277） 64bit （Insider Preview Version）	1
Windows 10.0 32bit （※）	11
Windows 10.0 64bit （※）	156
Windows Server 2008 Service Pack 1 （Build 7601） 64bit	1
Windows Server 2012 （Build 9200） 64bit	1
Windows Server 2012 （Build 9600） 64bit	6
Windows Server 2016 （Build 14393） 64bit	1

※167 台（33.6%）は Windows10 の OS バージョンまで取得できなかった機器

セキュリティ更新プログラムが提供されない OS を使い続けることは、攻撃者に狙われやすく、抵抗力がとても低い状態であるため、実証参加企業に向けて、脆弱な OS を使用中のコンピューター名を列記した週報を送付して注意喚起を行った。

Windows パソコン上では「Winver」コマンドを実行することで OS バージョンを確認することができる。Windows 10 であっても、半期アップデートを 3 回（1 年半）適用していないと、未サポートとなってしまうため注意が必要である。業務上サポート切れの Windows 7 を使い続けている場合は、メール受信や、Web サイトの閲覧は行わず、社内ネットワークから隔離することを強く推奨したい。

4.2.3.3 脆弱性更新の適用状況（Windows Update で対応可能なもの）

Microsoft Windows OS や Microsoft Office など OS の更新メカニズムで対応ができる脆弱性について報告する。横軸は日付（10～12 月）、縦軸は脆弱性を検知したパソコン 130 台。Windows へのログイン時に検査を行い、脆弱性を検出した日に「赤点」を掲載した。**5 割は更新プログラムの適用に時間がかかっている**。

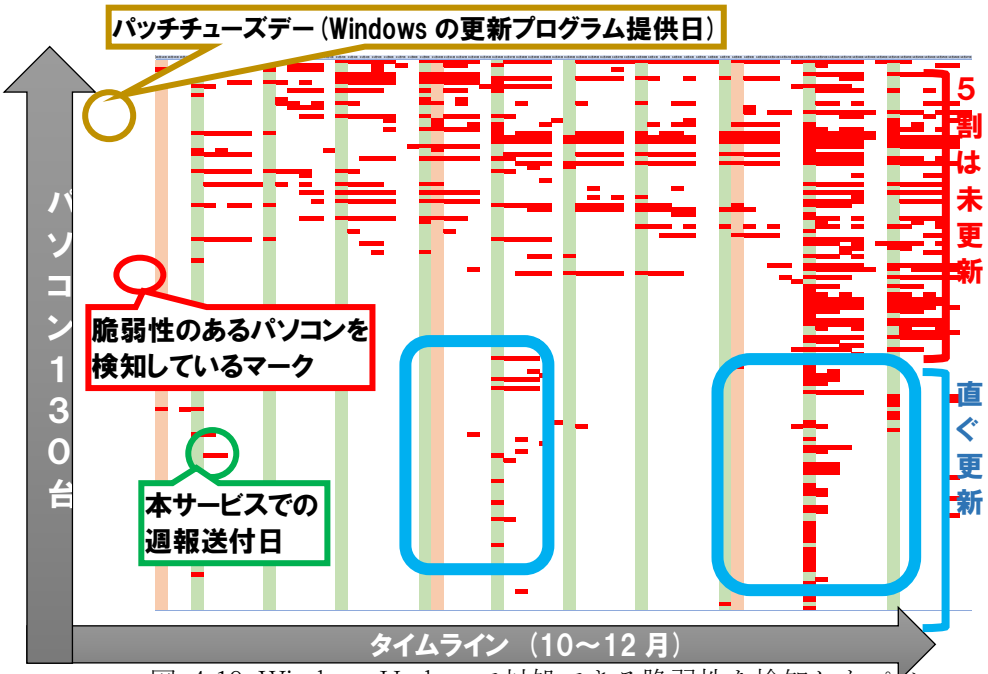


図 4-19. Windows Update で対処できる脆弱性を検知したパソコン

4.2.3.4 脆弱性更新の適用状況（Windows Update で対応不可能なもの）

Adobe Reader, Adobe Flash や Oracle Java のようなサードパーティアプリケーション「ごと」に更新が必要な脆弱性について報告する。横軸は日付（10～12 月）、縦軸は脆弱性のあるパソコン 84 台。Windows へのログイン時に検査を行い、脆弱性を検出した日に「赤点」を掲載した。3 割は更新プログラムの適用に時間がかかっている。

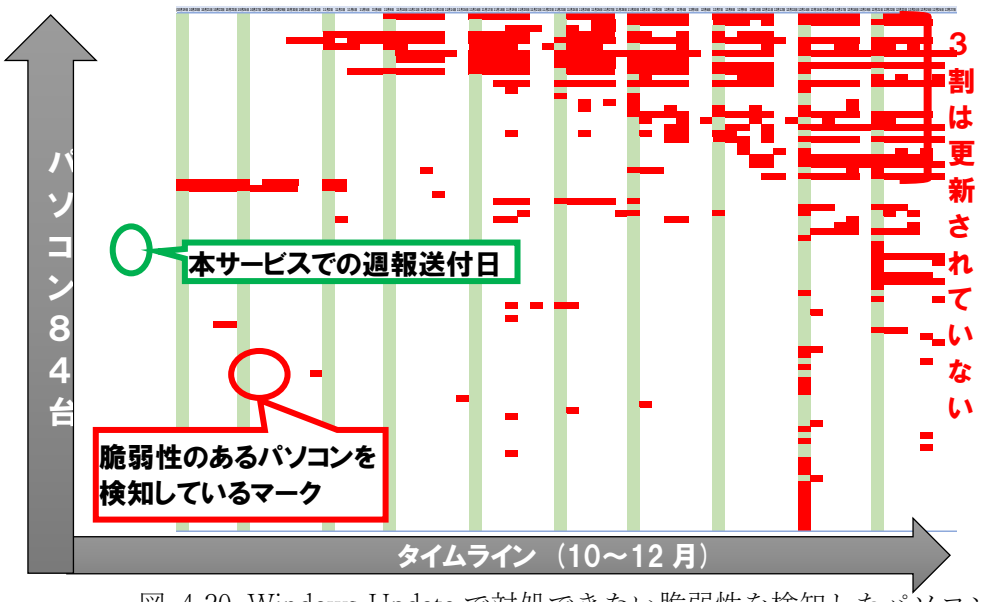


図 4-20. Windows Update で対処できない脆弱性を検知したパソコン

4.2.4 パソコン上のセキュリティソフトの既存対策状況

12 月末時点において、監視サービス実施企業 50 社、監視対象のパソコン 502 台に導入されているセキュリティソフト名について、Windows Management Instrumentation （WMI）インタフェースを通して得られた名称で列挙した。6 割強が、Windows 10 標準搭載の Windows Defender を利用されている。Windows 10 に移行したことで、標準でもセキュリティ対策が施されている点がセキュリティ確保に貢献しているものと考えられる。

表 4-21. パソコン上の既存セキュリティ対策の導入状況

セキュリティ対策の製品名	台数	割合
Windows Defender	328	65%
ESET Security	35	7%
ウイルスバスター クラウド	29	6%
CylancePROTECT	24	5%
ノートン 360	23	5%
McAfee Endpoint Security	14	3%
（名称不明）	12	2%
マカフィー　ウイルススキャン	9	2%

セキュリティ対策の製品名	台数	割合
ウイルスセキュリティ	5	1%
トレンドマイクロ ウイルスバスター コーポレート	5	1%
ESET Endpoint Antivirus 6.2.2033.1	3	1%
ESET Endpoint Antivirus	2	0%
Trend Micro Apex One	2	0%
Microsoft Security Essentials	2	0%
ノートン インターネット セキュリティ	1	0%
ビジネスセキュリティクライアント	1	0%
ノートン セキュリティ	1	0%
常時安全セキュリティ 24	1	0%
スーパーセキュリティ ウイルス対策	1	0%
Symantec Endpoint Protection	1	0%
Kaspersky Endpoint Security for Windows	1	0%
α Scan II	1	0%
（名称不明）	1	0%
合計 （12 月末時点）	**502**	

4.2.5 パソコン上の脅威検知（既存対策をすり抜けたマルウェア感染の実態）（②）

前記、「3.4.8 パソコン上の脅威検知（既存対策をすり抜けたマルウェア感染の実態）（②）」で説明したとおり、他お助け隊事業者と検知位置の違いにより、既存対策をすり抜けた脅威、かつ確度や重要度が高いと分析担当が判断するものを絞り込んで報告するため、相対的に検出数は少なくなっている。

下記は、本実証事業期間内に検知したマルウェアであるが、前記メカニズムにより IT 担当者が疲弊しないよう、確度が高く重要性が大きい脅威と、対応する優先度は低いものの好ましくないアプリケーション（アドウェア、ダウンローダーなど）を区別して担当者へ通報を行った。次が報告した脅威の一覧である。

本実証事業期間内では、緊急度を要するマルウェア（遠隔操作型、破壊型、身代金型）は、既存対策で排除されており、パソコン内で残っているものは検知されなかった。

パソコン内で対処されず残っていた脅威は、業務上好ましくないアドウェア、ダウンローダーと呼ばれるものであり、その後、脅威に繋がる可能性はあるが、緊急に対処が必要なものではなかった。

(1) 確度が高く重要性が大きい脅威

報告なし（既存対策で同日内に対処済）

(2) 対応する優先度は低いものの好ましくないアプリケーション

下記、1766 件 193 種 9 マルウェアグループの報告を行った。

表 4-22. パソコン上で脅威検知されたマルウェアグループ名

マルウェアグループ名	件数	説明
Pua.Mindspark	173	・ ブラウザにツールバーを追加 ・ ブラウザからキーワードを検索すると、意図しない検索エンジンに問合せる ・ この問合せの結果、メジャーな検索エンジンで は表示されないような広告されることがあり、この 広告を経由してマルウェアが配信される可能性がある ※類似名称について 「Pua.My.Websearch」は好ましくないアプリケーションとして検知。「W32.Mywebsearch」はその中でもマルウェア的な挙動を確認している。
Pua.My.Websearch	2	
W32.Mywebsearch	2	
Adware.NewDotNet	1	
Pua.Opencandy	1	・ アプリケーションのインストーラーに広告を含み、推奨される任意の他アプリケーションがインストールされる ・ 予期していないアプリケーションが追加で導入される懸念がある
W32.Adware.Gen	11	・ 一般的に広告が表示されるアプリケーションであり、業務で意図的に使っていなければ削除することも検討
W32.Malware.Gen	1	・ 挙動がウイルスに近いため検出した ・ 誤検知の可能性もあるが、業務上使う必要があるアプリケーションであるか判断が必要
W32.Adware.Installcore	1	・ 別のソフトウェアをインストールするダウンローダーと呼ばれるソフトウェアの 1 つ ・ アドウェアというのはユーザーの望まない広告表示活動を行うものであり、『あなたの PC の速度が低下しています』や『あなたの PC でエラーが見つかりました』といったメッセージと合わせて『これを改善するにはここをクリック』のような広告を表示することが多い
W32.Riskware.Avremover	1	・ アンチウイルス製品を導入する前に、他社アンチウイルス製品を削除するために使うツール ・ 意図して行うものでなければ、アンチウイルス製品が削除される懸念がある

4.2.6 駆け付け対応支援

実証参加企業の PC がマルウェアに感染し、実証参加企業自身で対処できないと判断した場合、駆け付け対応要員が実証参加企業事業所に駆け付けて状況調査やマルウェア駆除支援などの初動対応支援を実施する。また、初動対応支援により、さらに詳細な影響範囲の調査や安全宣言に向けた復旧作業などが必要な場合には、本実証事業の対象外での活動となるが、高度な分析調査を行うことができる技術員を派遣し対応する。

4.2.6.1 脅威に対する出動

本実証事業期間では、**脅威に対する出動要請は 0 件**であった。これは前記、パソコン上の脅威検知でも説明したとおり、**至急対応が必要な脅威は検知されておらず、現場でのインシデントも発生していなかった**と考える。

4.2.6.2 その他の出動

実証参加企業に困りごとのヒアリングを行ったところ、IT に詳しい担当がおらず、**現地での導入作業の支援依頼が 7 社**あった（有償製品であれば付き合いのあるベンダーによる対応が可能）。

依頼内容

・業務多忙でインストール作業を行えていない。訪問して対処してもらえると助かる。（類似 4 件）
→ IT 担当者とは異なる事業所で、現地の端末所有者と共に作業を実施。

・社内には、IT に詳しいものがおらず、業者から購入したものは業者に頼むことができるが、今回の件は別件となるため依頼が難しく、送ってもらったツールの導入を実施できていない。手伝ってもらえると助かる。（類似 2 件）
→ 現地で総務担当者と一緒に作業を実施。

・手順書に従いインストールを試みたが、正しく動作しない。コールセンターによる電話対応受けたが状況が改善しない（類似 1 件）。
→ 訪問対応したところ、特別な対応なく、インストール終了。（原因不明）

4.2.7 工場の IT 機器見える化（④）

IoT 機器などが接続可能な工場においては、不審な機器や意図せず接続された機器により可用性・完全性が失われる可能性がある。本実証事業では、IT 機器を検知するツールを工場ネットワークに 2 週間、設置し、接続されている機器を把握することにより、リスクの見える化を図る。

※参考：会社プロフィール（設置企業 6 社）

A 社）製造業、従業員 26 名、資本金 1000 万円、保有パソコン 12 台
B 社）製造業、従業員 360 名、資本金 2000 万円、保有パソコン 200 台
C 社）製造業、従業員 80 名、資本金 9500 万円、保有パソコン 100 台
D 社）製造業、従業員 139 名、資本金 2000 万円、保有パソコン 171 台
E 社）製造業、従業員 36 名、資本金 3000 万円、保有パソコン 48 台
F 社）製造業、従業員 48 名、資本金 2300 万円、保有パソコン 28 台

4.2.7.1 工場ネットワークで見つかった機器種別

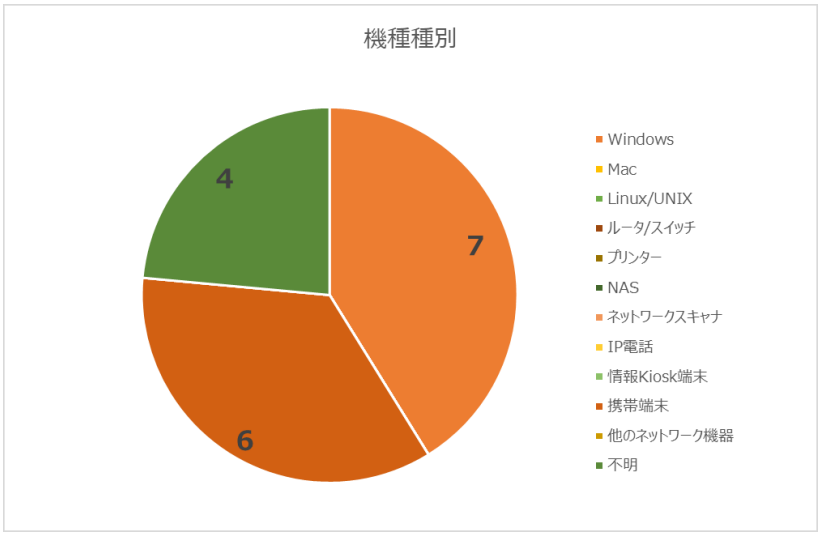


図 4-23. 工場ネットワークで検知された機器種別（A 社）

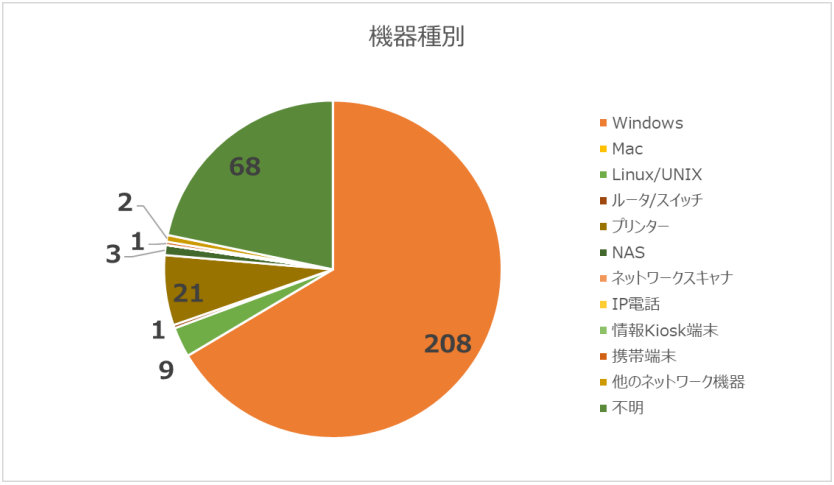


図 4-24. 工場ネットワークで検知された機器種別（B 社）

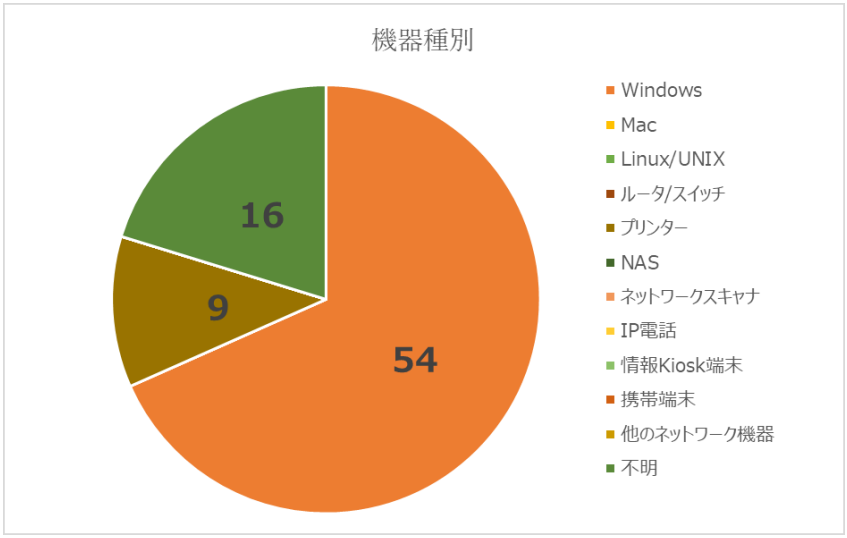


図 4-25. 工場ネットワークで検知された機器種別（C 社）

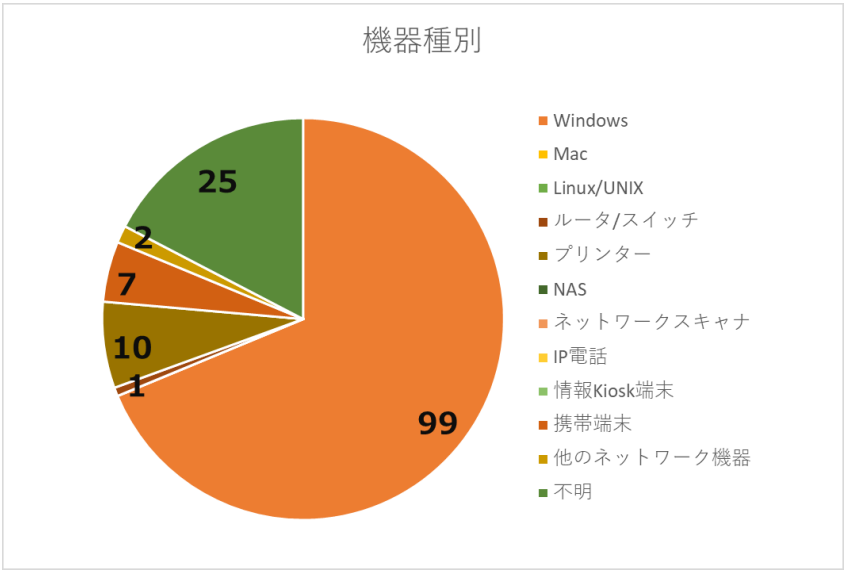


図 4-26. 工場ネットワークで検知された機器種別（D 社）

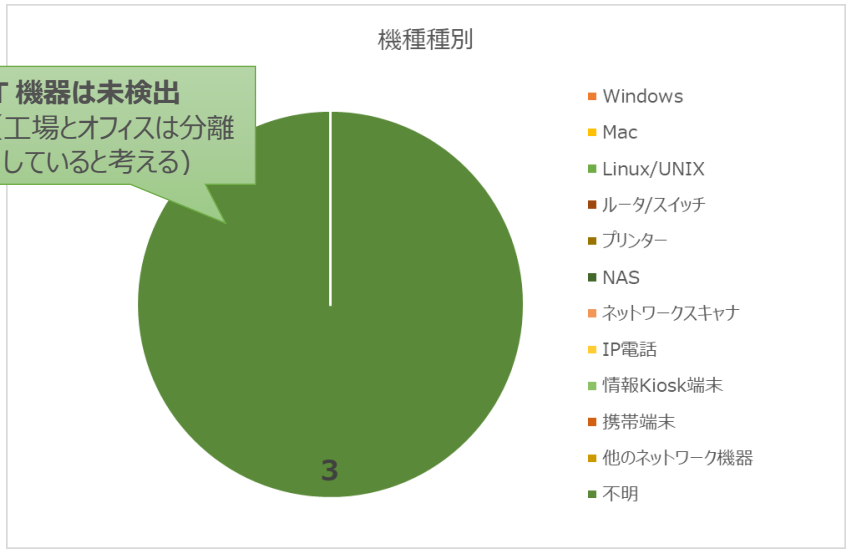


図 4-27. 工場ネットワークで検知された機器種別（E 社）

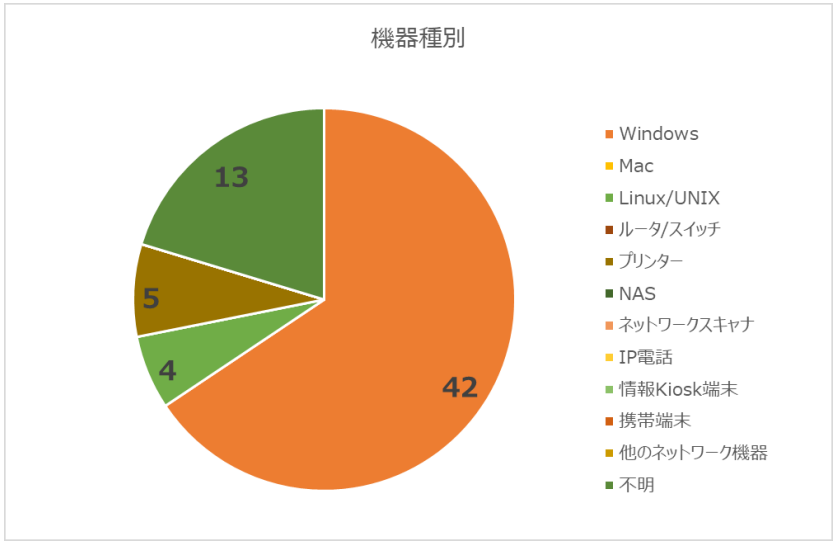


図 4-28. 工場ネットワークで検知された機器種別（F 社）

1 社を除き、いずれの会社も、Windows パソコンが大部分を占めており、ネットワークプリンター（複合機）なども存在することから、**オフィスと工場のネットワークが分離されておらず大量の Windows パソコンが検知されていると考えられる**。後述するヒアリング結果からも、**ネットワークを分離していないとの回答**もある。攻撃者の踏み台になりかねないオフィス内のパソコンと、**セキュリティ更新がしづらい生産設備が通信可能な同一ネットワーク上に存在することは好ましくない**と考えられる。

4.2.7.2 Windows のバージョン種別

表 4-29. Windows のバージョン種別

OS 種別	A 社	B 社	C 社	D 社	E 社	F 社
Windows 2000	8	8	1	0	0	0
Windows 2000 Server	2	2	0	0	0	0
Windows XP	0	1	3	0	0	10
Windows 7	1	2	7	2	0	4
Windows 8	0	1	0	0	0	0
Windows Server 2003	0	2	0	0	0	0
Windows Server 2008	0		0		0	1
Windows Server 2008 R2	0	1	0	1	0	0
Windows Server 2012	0	0	0	0	0	1
Windows Server 2012 R2	0	9	3	3	0	0
Windows Server 2016	0	2	0	4	0	0
Windows10	3	151	45	72	0	26
（期間内に未取得）	3	29	0	17	0	0
合計	7	208	54	99	0	

Windows 7 や、Windows Server 2008 は既に**サポート期限切れ**となっており、ネットワーク上で運用することは**危険**と言える。後述ヒアリング結果からも、**オフィスで使っているものでは、業務ソフトの関係から、工場は専用機器の関係から更新ができないと回答**がある。

4.2.7.3 ネットワークプリンター種別

表 4-30. ネットワークプリンター種別

機器種別	A 社	B 社	D 社	C 社	E 社	F 社
Brother MFC-J6997CDW （最新ファーム: 2020/10/15）	0	1	0	0	0	0
Brother DCP-L2550DW series （最新ファーム: 2020/12/25）	0	1	0	0	0	0
Brother DCP-7065DN （最新ファーム: 2019/02/14）	0	1	0	0	0	0
Canon MB5100 series 1.120 （最新ファーム: 2020/12/10）	0	1	0	0	0	0
EPSON PX-M5080F Series （最新ファーム: 2020/10/20）	0	1	0	0	0	0
EPSON LP-S7160	0	2	0	0	0	0

機器種別	A社	B社	D社	C社	E社	F社
（最新ファーム: 2020/3/31）						
EPSON LP-S6160 （最新ファーム: 2020/3/31）	0	5	0	0	0	0
EPSON EW-M630T Series （最新ファーム: 2020/11/24）	0	1	0	0	0	0
EPSON VP-2300 （最新ファーム: 不要）	0	0	0	1	0	0
FUJI XEROX DocuPrint P350 （最新ファーム: 2019/10/11） ※2017 年にセキュリティ更新あり	0	0	0	1	0	0
FUJI XEROX DocuPrint C3450 （最新ファーム: 2020/11/20）	0	0	0	1	0	0
FUJI XEROX DocuCentre-IV C2260 （最新ファーム: 不要）	0	0	1	0	0	1
FUJI XEROX DocuCentre-IV C2263 （最新ファーム: 不要）	0	0	1	0	0	0
FUJI XEROX DocuCentre-IV C2275 （最新ファーム: 不要）	0	0	0	1	0	0
FUJI XEROX DocuCentre-IV C3375 （最新ファーム: 不要）	0	0	1	0	0	0
FUJI XEROX DocuCentre-IV C4470 （最新ファーム: 不要）	0	0	1	0	0	0
FUJI XEROX DocuCentre-IV C5570 （最新ファーム: 不要）	0	0	1	0	0	0
FUJI XEROX DocuCentre-IV C5575 （最新ファーム: 不要）	0	0	0	1	0	0
FUJI XEROX DocuCentre-V C2275 （最新ファーム: 不要）	0	0	0	0	0	2
FUJI XEROX DocuCentre-VI C2264 （最新ファーム: 不要）	0	0	0	0	0	1
FUJI XEROX DocuWide3037 （最新ファーム: 不要）	0	0	0	0	0	1
RICOH MP C4504 JPN （最新ファーム: 機器上で要調査）	0	1	0	0	0	0
RICOH MP C3504 JPN （最新ファーム: 機器上で要調査）	0	1	0	0	0	0

機器種別	A社	B社	D社	C社	E社	F社
RICOH MP C3503 （最新ファーム：機器上で要調査）	0	0	2	0	0	0
RICOH MP C2503 JPN （最新ファーム：機器上で要調査）	0	1	0	2	0	0
RICOH MP W7100 （最新ファーム：機器上で要調査）	0	0	1	0	0	0
RICOH imagio MP C4001 （最新ファーム：機器上で要調査）	0	1	0	0	0	0
RICOH imagio MP C3302 （最新ファーム：機器上で要調査）	0	1	0	0	0	0
RICOH imagio MP C2802 （最新ファーム：機器上で要調査）	0	1	0	0	0	0
RICOH IM C6000 JPN （最新ファーム：機器上で要調査）	0	1	0	0	0	0
SHARP MX-3110FN （最新ファーム：保守契約要）	0	0	0	1	0	0
SHARP MX-3111F （最新ファーム：保守契約要）	0	0	0	1	0	0
OKI C332 （最新ファーム：2020/10/21） **※2019 年にセキュリティ更新あり**	0	1	0	0	0	0
OKI C811 （最新ファーム：不要）	0	0	0	1	0	0
合計	0	21	9	10	0	5

検知したネットワークプリンター（複合機）のファームウェアバージョンは、明らかではないが、これら機器にも**ファームウェアの更新版が提供されている**。明確にセキュリティ更新プログラムとの記載は少なく、ソフトウェアのバグとの記載しかないため危険性は判断できないが、**機器ごとの計画的に更新を行う（または自動更新機能を持つ機器を利用）することが推奨**される。

※ファームウェアバージョンは 2020 年 12 月 PFU による調査

4.2.7.4 携帯デバイスと推察される種別

表 4-31. 携帯デバイスと推察される種別

機器種別	A社	B社	C社	D社	E社	F社
Android	2	1	0	7	0	0
iOS	4	0	0	0	0	0
合計	6	1	0	7	0	0

Android デバイスは、ファームアップデートがメーカー任せであり、2 年程度でファーム更新されないケースが多いため注意が必要。

4.2.7.5 そのほかのネットワーク機器

表 4-32. そのほかのネットワーク機器

機器種別	A 社	B 社	C 社	D 社	E 社	F 社
IntraGuardian	0	0	0	1	0	0
SmartUPS	0	2	0	1	0	0
BUFFALO.INC	0	0	0	0	1	0
A2 CORPORATION	0	0	0	0	1	0
Lantronix	0	0	0	0	1	0
合計	0	2		2	3	0

※IntraGuardian は不正端末接続防止ソリューション

4.2.7.6 ヒアリング結果

工場ネットワークについてヒアリングした結果は下記のとおり。

表 4-33. 工場ネットワークについてのヒアリング結果

1.**オフィス系ネットワークと、工場系のネットワークで管理者は分かれて**いますか？ 分かれている場合、お互いの管理状況を把握されていますか？
→ **管理者は同一であり、殆どの会社ではオフィスと工場でネットワークを分離していない** **【ネットワークは分離 （管理者不在）】** A 社） オフィス系ネットワークと工場系ネットワーク自体は**分かれているが、ネットワークの管理者がおらず**、これから体制を作ろうとしている。 **【ネットワークは分離せず （管理者同一）】** B 社）工場とオフィスが同じネットワークであり、管理者は分かれていない。**総務系の部署が全て管理**している。 C 社）管理者は分かれていない。**品質保証部が全てのネットワークを管理**している。 D 社）分かれていない。**システム課が管理**している。 E 社）オフィス系と工場系が**同一のネットワーク**であり、管理者は**分かれていない**。 F 社）**ネットワークは分かれていない**。**現場の担当者と IT 担当者の 2 名**体制で管理している。
2.工場系のネットワークに保守用回線など**外部からアクセス可能なネットワークは繋がれていますか**？
→ **設問 1 でオフィスと工場のネットワークが殆ど分離されておらず（オフィスで遠隔マルウェアに感染すると工場にも波及）、またオフィス用途で VPN 接続しているケースも半数ある。**

【外部からの接続あり】

A 社） 外部からアクセス可能な保守用回線などは存在していないが、**現在 VPN 回線の構築を計画**している。

B 社）**以前は、基幹系サーバーのメンテナンスなどでリモートから VPN** でアクセス可能であったが、今は提供していない。

C 社）外部から設備（デマンド監視装置）自体に**保守用のモバイル回線**がある。**メーカーと保守契約**を結んでおり、定期点検などの際に独自モバイル回線から 1～2 台がアクセスしている。

F 社）外部から **VPN 接続している営業用の端末が 10 台**ほどある。

【外部からの接続はない】

D 社）繋がれておらず、**外部からのアクセスは不可**となっている。

E 社）外部から工場系ネットワークに**アクセスはできない**。

3.工場系ネットワークに**想定していない機器が接続されていたこと**がありますか？ある場合、どのような機器が接続されていましたか？

→ **管理者の意識として、想定外の機器が接続されるケースは、殆どない（1 社のみ）**

【ない】

A 社） 認識している範囲で、想定していない機器が接続されていたことは**ない**。

C 社）想定していない機器が接続されたことは**ない**。普段ネットワークに接続されている機器は、一般的な Windows 製品。また、マシニングセンター内には組み込み OS（Windows Embedded など）の機器が存在する。

D 社）接続されていたことはない。**ISMS 認証を取得**しており、セキュリティ対策は行っている。スマホなど**私物端末は接続不可**となっている。

E 社）想定してない機器が接続されたことは**ない**。

F 社）想定してない機器が接続されたことは**ない**。

【ある】

B 社）個人で**持ち込んできた端末など**、想定していない機器が接続されていたことはよく**ある**。機器は、Windows の**端末や無線のアクセスポイントなど**。

4.工場側において、**セキュリティインシデントが過去に発生**したことがありますか？ ある場合、どのようなインシデントでしたか？

→ **殆どはインシデントの経験なし（1 社のみあるが感染理由は不明）**

【ない】

A 社） 認識している範囲で、過去にセキュリティインシデントが発生した事例は**ない**。

B 社）ライセンスの使用に関するインシデントがあったが、情報漏えいなどのセキュリティインシデント発生の事例は**ない**。

C 社）発生したことは**ない**。

D 社）セキュリティインシデントが発生したことは**ない**。　※USB を紛失し、その後発見したという事例はある。なお、USB を PC に接続するのは権限のある者のみとしている。

E 社）セキュリティインシデントの発生事例は**ない**。

【ある】

F 社）**サーバー2 台がトロイの木馬に感染（2014 年）**。
感染対象の機器は抜線を行い隔離している状況。
感染の原因は不明。

5.今回、工場の IT 機器見える化として、サービスを提供させていただきますが、自動で見える化して**管理したい機器**は、どんなものがありますか？
（たとえば、PLC、DCS、IoT-GW など）

→ 全てを管理したいが 2 社。Windows 機器が 1 社。そのほか 3 社は特になし（台帳で管理できるレベル）

【種別に関わらず全て】

A 社）　ONU からネットワークに飛んでいる機器は**全て見える化して管理**したい。

F 社）ネットワーク繋がっている**機器は全て管理**したい。

【Windows 機器】

E 社）**Windows OS が入った端末を管理**したい。

【特になし】

B 社）特に**なし**。

C 社）自動で管理したい機器は特に**ない**。マシニングセンター内に **PLC などの制御機器**はあるが、機器の台数もそれ程多くないので**手動の管理で十分**と感じている。

D 社）現在のところなし。現状、制御機器の管理はツールではなく**台帳（Excel）で管理**している。

6.ネットワークに接続されている機器は、**どんな情報が知りたい**ですか？
（たとえば、バージョン／ファーム／製造年、ネットワーク構成／機器状態、サポート情報／脆弱性情報など）

→ **ほぼ、OS バージョンや脆弱性情報を把握したい。課題としては、組み込み OS の制御機器は、サポート切れは機器の更改が必要となるため高額な点である。**

A 社） OS の**脆弱性情報**を知りたい。

B 社）一年前に Windows10 への切り替えが行われたが、漏れている端末もあったため **OS のバージョン情報**が知りたい。バージョン情報の取得や Windows アップデートは、資産管理ツールの導入を検討しているが、まずは現状**ネットワークに接続されている機器の存在**を全て知りたい。

C 社）**例示されている情報は全て**知りたい。

追加質問）制御機器の OS は最新化されているか。

→**組み込み系 OS のためアップデート**する場合は、**機器自体の入れ替えが必要**だが高額なため（1 台 1000 万円くらい）**最新化できていない**。

D 社）**バージョン情報**が知りたい。（Windows Update のバージョンなど。） バージョンは最新ものを適用するようにしており、**旧バージョンの端末はネットワークに接続していない**。

E 社）Windows が最新のバージョンに更新されているか確認するため、**バージョン情報や脆弱性を管理**したい。

F 社）Windows の**バージョン情報**を知りたい。

7.先ほどの質問で、機器の**知りたい情報**のお話をしました。現在は、それらを**どのように管理**されていますか？ （たとえば、都度、セキュリティを見ているご担当者（脆弱性管理）から、工場のライン担当様へご案内されるなど）

→ **1 社資産管理ツールを導入されておられるが使いこなせていないとのこと。そのほかは Excel などの台帳で管理する程度であるが、セキュリティやネットワークを管理する人材がいない点。ツールで把握するにも電断中の機器は情報を収集できない点を挙げられている。**

A 社） セキュリティやネットワークを管理している専門部署が存在しないため、**管理できていない**。

B 社）**ツールを定期的に実行し機器の情報を収集**・チェックしているが、**電源が落ちている端末の情報が拾えない**、または一部の情報が拾えないなど課題はある。

C 社）**Excel ファイルで管理**している。

D 社）**LanScope Cat を導入**しているが、いまいち**使いこなせていない**。バージョン管理ではなくメール管理（誰がいつどのメールを送信したか）に使用している。

E 社）**エクセルなどの表**で管理している。

F 社）**エクセルで帳票**を作り管理している。（端末の数は 80 台ほど）

8.アンチウイルス製品を導入できない機器があるなど、**セキュリティ面で気になる機器**はございますか？

→ **セキュリティチェックが口頭確認で確実性がないこと。専用機器の OS が古い点。制御機器に対策ソフトを入れられず UTM やインストール不要な外部製品に頼りたいが高額な点。**

A 社） 工場のネットワークに**古い Windows OS 機器（Windows 7）が 1 台ある**こと。

B 社）デバイスの数や種類が多く、FW や **UTM などのセキュリティ製品**を導入したいが**予算的に苦しい**。端末には中小企業向けのウイルスバスターを導入。今後はクラウドで管理できる製品への切り替えを検討中。

C 社）**制御機器にアンチウイルス製品が入れられない**こと。**インストール不要**の製品（マカフィー）の紹介があったものの、**更新料が高額**であったため、導入はできていない。

D 社）ネットワークに接続していない機器は各部署で管理している。**セキュリティチェック**を行ったことは報告させているが、**確実に行ったか実態は把握できていない**。

E 社）**専用機械の Windows OS が古い**こと

F 社）特に**ない**。

9.業者などが、**保守用 PC の持ち込みを行い接続**されるケースでは、現在どのように管理されておりますか？ （利用申請・承認したパソコンのみ接続を許可するなど）

→ **持ち込み機器に対して特に気にしていないが 1 社あるものの、ほぼ接続申請を必要としている。1 社はセキュリティ対策がされているかを条件としている。**

A 社） ネットワークに繋げる際は事前に**担当者の承認が必要**。

B 社）持ち込む機器は**事前に申請が必要**。ウイルス対策ソフトの**パターンファイルが最新化**されているか、**OS がアップデート**されているか**確認**している。

C 社）持ち込み PC をネットワークに接続する場合は、**事前に利用申請が必要**で IP アドレスを払い出している。

D 社）**利用申請**としているが今まで利用したケースは**殆どない**。（保守で PC を接続することはない。）

E 社）業者が持ち込んだ PC などの管理は**特にしていない**。

F 社）業者などが保守用 PC を**持ち込みケースはなく**、ネットワークに接続されている PC は**社員端末のみ**。

4.2.8 機密性の高いデータ共有（⑤）

業務でのデータ共有には情報漏えいのリスクが潜んでいる。実証参加企業のデータ共有に関する運用ヒアリングし、現状のセキュリティ課題を調査する。また、NISTSP800-171 準拠したデータ共有を専用のツールを使い体験してもらう。

データ共有サービスを実際に導入して体験した企業が 16 社、導入は行わないがデータ共有サービスを利用した場合の効果について対面または電話説明を行いアンケートに回答した企業が 11 社となった。

4.2.8.1 ヒアリング結果

① 御社は、情報を守る上で、以下のシステムの機能を採用されているか

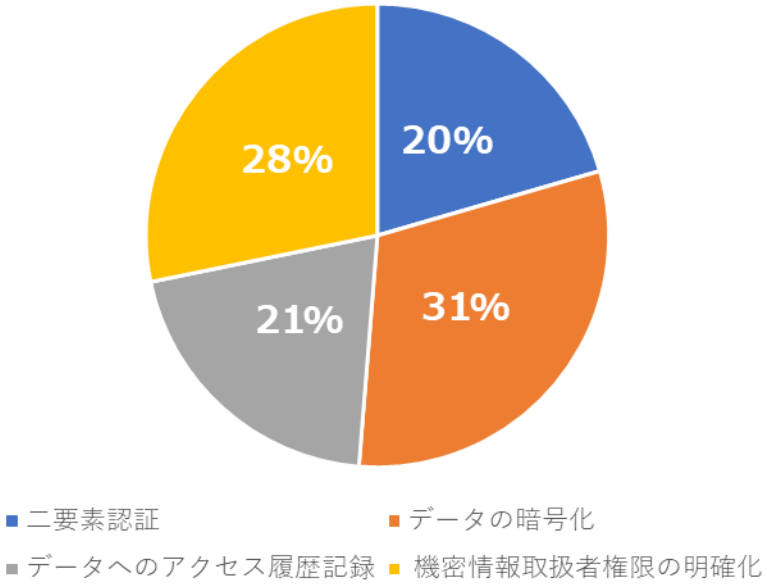


図 4-34. 情報を守るために利用している機能

意外にも、どの種別のセキュリティ対策も採用されていた。しかし、他の諸機関実施の調査結果と同じく、二要素認証を採用されている企業が若干少ないという結果となった。

② 情報保護のために以下のシステムの機能を導入する上で、障壁はどの程度ですか（「高い」「それ程高くない」「低い」から選択）

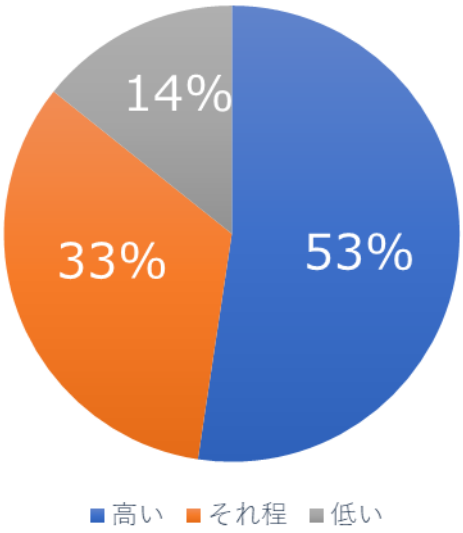


図 4-35. 二要素認証（パスワードと生体、など組み合わせ）の導入障壁

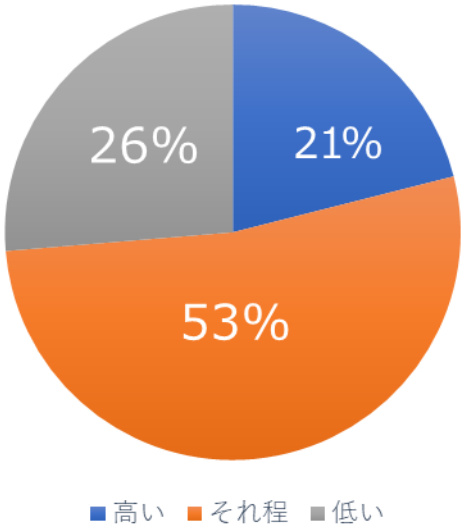


図 4-36. データ暗号化の導入障壁

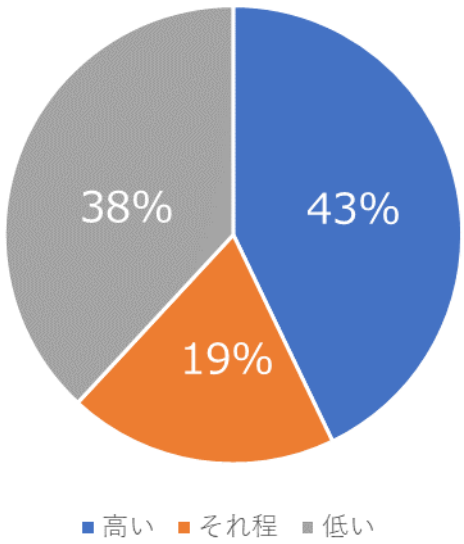


図 4-37. データへのアクセス履歴記録の導入障壁

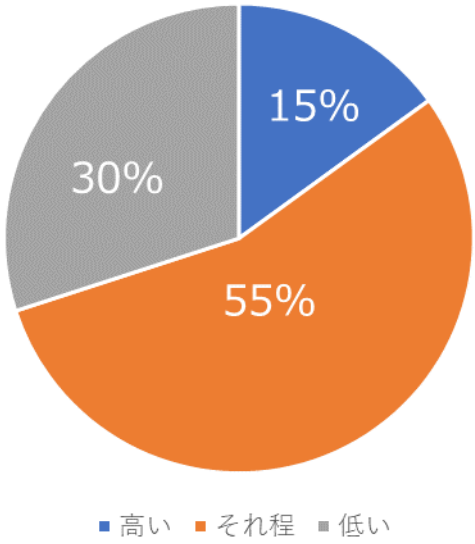


図 4-38. 機密情報取扱者権限の明確化の導入障壁

二要素認証導入は他の対応と比較して、ハードルが高いとの結果が出た。(設問 1 を裏付けたもの。) また、アクセス履歴管理についても、システムでの対応となると難しいことから、ハードルが高いと回答した企業が多かった。

関連する実証参加企業からの回答

- Cloud に関しては BoxCryptor と呼ばれるソフトを使用しています。 End to End での暗号化がなされており、 Cloud 側で漏えいしても暗号化されているファイルであり、復号するためのキーは私のコンピューターにしか無いと聞いています。

・ Email での送信に関しては、都度 zip などで暗号化しています。 S/MIME は近いうちに導入する予定です。
・ パソコンのディスクは暗号化されており、バックアップ（TimeMachine）も暗号化されています。

③ 取引先との間、社内での情報（契約書、製品仕様、図面など、機微情報を含んだ文書）共有はどのような手段でされているか

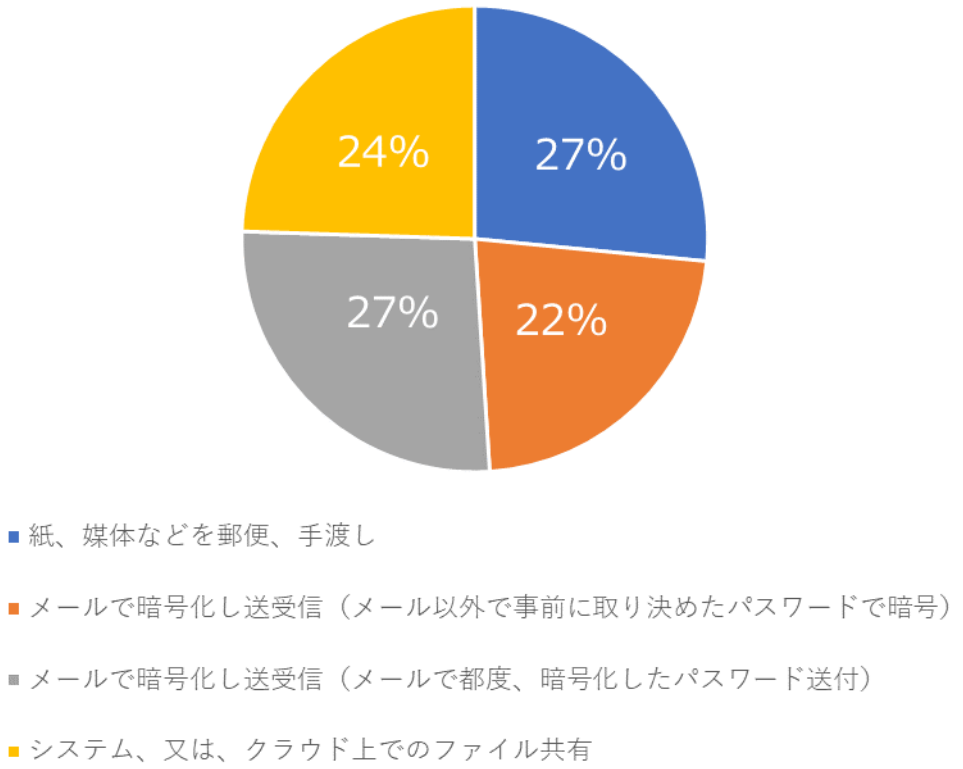


図 4-39. 取引先、社内での状況共有の手段

多数は、紙などの媒体で手渡し、郵便で送付。システム、クラウドで情報共有される企業も多く、クラウド利用についての抵抗が意外と低い結果となった。

④ 取引先との間、社内での情報（契約書、製品仕様、図面など、機微情報を含んだ文書）共有をクラウド上（国内クラウド）で行うのに抵抗はあるか（社数）

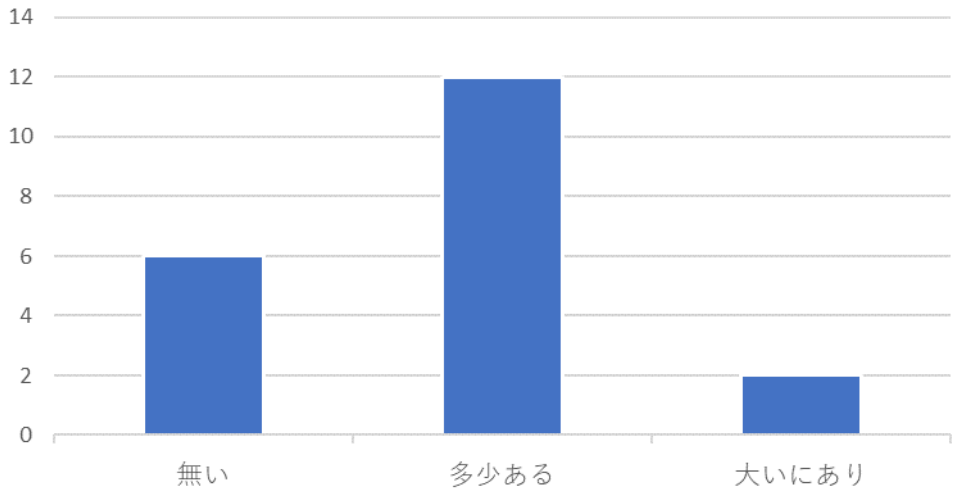


図 4-40. 取引先、社内での状況共有をクラウドで行うことへの抵抗感

前設問のとおり、大きくクラウドに抵抗がある企業は殆ど無いとの結果が出た。但し、大いにありを回答した企業も少数ではあるがあった。「クラウドに格納したデータなどの守秘・原本性などの担保について心配」、とのコメントがあった。

⑤ 前記載の機能を備えた、機微情報の保管、社内外の方とのセキュアな情報共有するサービス「機密性の高いデータ共有（Fort#Forum）」として提供しているが、このようなサービスは、利用価格としてどの程度なら使っても良いと考えるか
（月額 1 名の料金を選択した社数）

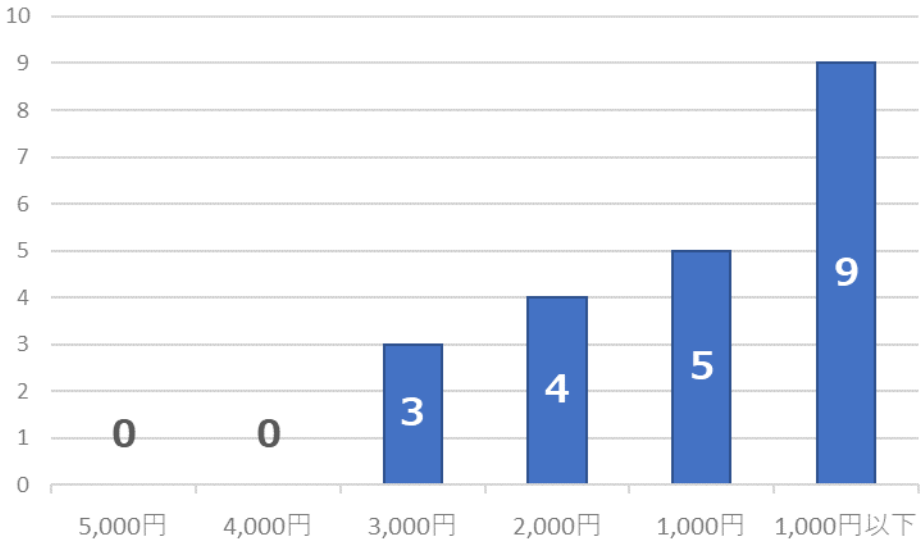


図 4-41. 機密性の高いデータ共有サービスの費用感（月額 1 人あたり）

Fort#Forum サービスの利用価格感については、予想通り 1,000 円/月額以下と回答された企業が多かったが、これは、まだ、セキュリティ基準対応を詳細に検討されている企業が少ないからと思われる。2,000 円以上と回答された企業も少なく無いという結果も出た。

⑥ もし、情報の保護、取引先との情報共有のために「機密性の高いデータ共有（Fort#Forum）」のようなクラウドサービスを使う場合、下記の利点、懸念などで当てはまる項目があれば選択

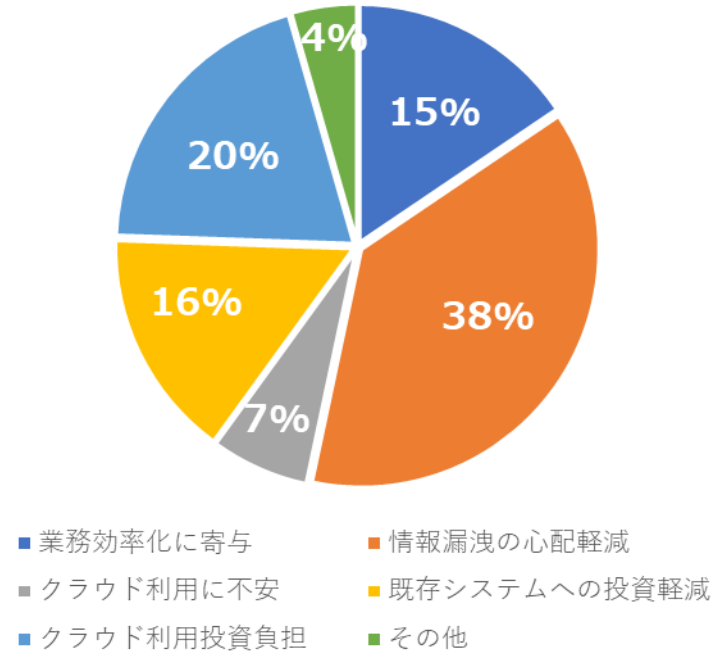


図 4-42. 機密性の高いデータ共有サービスの利点・懸念点

情報漏えいの心配が少なくなるとの回答が多く、サービスの訴求効果があったと思われるが、「追加の投資が発生する」との回答も多く、コストメリットの訴求が必要。 （オンプレでの基準対応とクラウドの比較が必要）

「一般論としてセキュリティレベルが担保できるクラウドは相応な価値があると考える。半面、セキュリティレベルを高めることについて、機微情報のクラウド利用についての社会的な認知は低く、特に中小規模の企業・団体はコスト面でも厳しいといった見解が大勢と思う。」といった中小企業への適合性について十分な検討が必要とのコメントもあった。

4.3　実証の実施結果

4.3.1 サービス実施中の注意喚起・啓発

実証事業に参加されている実証参加企業に向けて下記の注意喚起を実施した。

発信日	内容
2020/10/16	月例の脆弱性更新プログラムの適用について（注意喚起） ・Microsoft 製品の脆弱性対策について（2020 年 10 月） ・Adobe Flash Player の脆弱性対策について（APSB20-58）（CVE-2020-9746） ・Office 2010 のサポート終了について
2020/10/20	SECURITY ACTION「二つ星」宣言に向けて（啓発） ・中小企業のための情報セキュリティセミナー ～できるところからはじめよう !! コストをかけずに SECURITY ACTION !!～ ・令和 2 年度中小企業の情報セキュリティマネジメント指導業務
2020/11/13	月例の脆弱性更新プログラムの適用について（注意喚起） ・Microsoft 製品の脆弱性対策について（2020 年 11 月） ・Adobe Acrobat および Reader の脆弱性対策について（APSB20-67）（CVE-2020-24435 など） ・Oracle Java の脆弱性対策について（CVE-2020-14803 など） 以下情報レベルのお知らせ ・新しいセキュリティ更新プログラム ガイドでの脆弱性情報の詳細 ・Adobe Flash Player の削除を行うパッチをリリース 以下続く脅威への追加喚起 ・Windows SMBv3 クライアント/サーバーのリモートでコードが実行される脆弱性（CVE-2020-0796） ・Netlogon の特権昇格に関する脆弱性 （CVE-2020-1472） への早急な対応を
2020/12/01	Fortinet 社製品（注意喚起） ・Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 （CVE-2018-13379） の影響を受けるホストに関する情報の公開について
2020/12/08	月例の脆弱性更新プログラムの適用について（注意喚起） ・Microsoft 製品の脆弱性対策について（2020 年 12 月） ・Adobe Acrobat および Reader の脆弱性対策について（APSB20-75）（CVE-2020-29075） ・Windows 10 Version 1903 のサービス終了

	・Adobe Flash Player サポート終了情報ページ ・Adobe Flash Player のサポート終了に関する最新情報 以下情報レベルのお知らせ ・ランサムウェアによるサイバー攻撃について ・2020 年最悪なパスワード Top200 が報告されています ・中小企業において目指す Security By Design 以下続く脅威への追加喚起 ・Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379） の影響を受けるホストに関する情報の公開について（注意喚起）
2020/1/18	月例の脆弱性更新プログラムの適用について（注意喚起） ・2021 年 1 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 – JPCERT/CC ・Adobe Acrobat および Reader の脆弱性対策について（APSB20-75）（CVE-2020-29075） - IPA 以下情報レベルのお知らせ ・第 1 回九州サイバーセキュリティシンポジウム - KYUSEC ・セキュリティの「インシデント対応」を体験しませんか？ ～セキュリティの「サイバーインシデント演習 in 大阪」を開催～ - 近畿経済産業局 ・緊急事態宣言（2021 年 1 月 7 日）を踏まえたテレワーク実施にかかる注意喚起 - NISC ・監査人の警鐘- 2021 年 情報セキュリティ十大トレンド ・「中小規模製造業者の製造分野における DX 推進ガイド活用」徹底討論セミナー - IPA ・テレワークを行う際のセキュリティ上の注意事項 - IPA ・2020 セキュリティ十大ニュース発表 - JNSA ・テレワークのセキュリティに関するアンケート調査結果の中間報告を公開 - IPA ・NIST SP800-207（2020 年 8 月）ゼロトラスト・アーキテクチャの日本語訳を公開 ・最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取り組みの強化に関する注意喚起を行います- 経済産業省 以下続く脅威への追加喚起 ・シスコの複数の製品に脆弱性、中小企業向けルーターなど ・Adobe Flash Player が 2020 年 12 月末をもってサポート終了 - NISC

	・SolarWinds 社製 SolarWinds Orion Platform ソフトウェアに関する政府機関などへの注意喚起の発出について - NISC

4.3.2 運営で得られた課題と対策

4.3.2.1 募集における課題と対策

・ **メルマガによる募集が進まない**

働きかけ先の県関係者よりコロナ関連の情報が数多く発信されており埋もれている可能性を指摘される。

・ **サプライチェーン大手企業の協力が思うように得られない**

サプライチェーン大手企業 3 社の情シス部門に周知協力依頼を行うも、その後調達部門に依頼内容が伝達されサプライヤーへの周知についてバトンが渡される、国の事業であることや本実証事業の意図・意思がうまく伝わらない。また、サプライヤーが強要と捉える募集活動ができないことや中小企業デジタル化などで既にサプライヤーに多くの協力を求めている時期と重なったこともありサプライチェーン大手企業が積極的に動きづらい状況となった。

→ 対策「中小企業と直接対話することに専念」

・ ウェビナーによる事業説明会参加後に実証参加の意思を示されなかった企業に対して直接対話を申し入れ、実証参加における不安を取り除く活動を展開した。航空機産業のイベント「エンジンフォーラム神戸」に出向いて関係団体との直接対話から中小企業の紹介を受けて説明を行った。関係団体の研究会などにも積極的に現地参加して直接対話を進めた。

・ このように中小企業 1 社 1 社のサイバーセキュリティ対策の現状や課題認識を共有し、実証事業の有効性と実証参加への不安を解消することで実証参加企業数の改善が進んだ。

4.3.2.2 契約からサービス開始

(1) 契約作業の課題と対策

・ 参加申込後に、契約書類へのサイン、サービスヒアリングシートの記載に時間がかかった。
  ✓担当者からの申込みでは、社内手続き（役員）への承認に時間がかかる
  ✓会社役員（代表）からの申込みでは、業務多忙で記載する時間がない
・ 業界団体からの依頼であることから申し込んでみたが参加に消極的
  ✓セキュリティ関係の整備まで手が回らないため取りやめ
  ✓短期事業であることから参加取りやめ

(2) サービス開始に必要なヒアリングの課題

・ 中小企業の経営者・担当者に対する設問として技術的ハードルが高い質問内容があったため、ヒアリングシートの未記入が多く、再依頼行った
  ✓プロキシの有無とは？

✓ゲートウェイ IP アドレス、ネットワークマスクとは？

・ 日頃は付き合いのある IT 機器ベンダーに作業を行ってもらっている

✓プロキシの有無や設定など、ネットワーク環境についてわからない

✓ベンダーの納品する商品ではないため、本実証事業への理解がなく回答に時間がかかる

・ クラウド業者への提出物に英語表記の記載が必要だった

✓英語の住所・電話番号の記載に慣れておらず記載できない

（事務局で記載した上で、記載内容の確認を行ってもらう形に変更）

4.3.2.3 インストールモジュール作成時と送付時の課題

・ 個社ごとに作成するインストールモジュールの再作成

✓個社ごとにコンフィグレーションしたモジュールを作成しているが、サービスヒアリングシートに記載されている確度が低く、動作できないケースでは作り直しが発生（前記理由で聞かれてもわからないケースがあることからトライアンドエラー方式で提供）

・ 個社ごとに作成したインストールモジュールをクラウド経由で再送付

✓ダウンロードに 2 週間の送付期限を設けていたが、2 週間のダウンロード期限では足りないケースがある。

4.3.2.4 インストールモジュール導入時の課題

・ zip ファイル展開後に、展開先フォルダからインストーラー起動のみで、自動インストールされるものを提供し、写真入りの手順書も添付したが、IT に詳しくなく難しそうとのことで、現地インストール対応を実施した

✓クラウドからのダウンロードが脅威と捉え、作業していなかった

✓zip ファイルを展開せず、圧縮フォルダ内で実行（付随ファイルが展開されておらずインストールに失敗）

✓実行中に黒い画面（コマンドプロンプトが 20 秒くらい）が表示されるが、途中で閉じてしまった

✓インストール作業そのものを社外ベンダーに任せているため、実行できず

4.3.2.5 セキュリティツールの課題

導入後のツールに関する課題は特に指摘はない。

4.3.2.6 相談窓口の課題

(1) 対応人数の結果

実証参加される企業が一挙に増えず、徐々に参加されたことで、想定通りの対応を行うことができ、人数に対する課題はなかった。

(2) 問合せ内容

表 4-43. 問合せ件数

対応月	対応件数	参考） 対象社数
10 月	7 件	11 社
11 月	12 件	33 社
12 月	25 件	50 社
合計	44 件	

表 4-44. コールセンター対応、インシデント対応件数

対応種別	アラート種別	発生件数	特記事項
コールセンター対応	実証参加に関する問合せ	25	動作確認を含む
	セキュリティ機器設置などの問合せ	14	インストール相談を含む
	セキュリティ対応の相談	2	サービスに関する相談含む
	そのほか	3	
	計	44	
インシデントなど対応	電話およびリモートによるインシデント対応	0	
	訪問によるインシデント対応（駆け付け）	0	
	計	0	
そのほか訪問対応	機器設置などのトラブル対応	1	インストール失敗の調査
	そのほか	6	ツールの導入支援
	計	7	
	総計	51	

相談窓口の対応詳細

【コールセンター対応】

- 実証参加に関する問合せ

「ツール導入が終わったので動作確認を依頼したい」(25 件)

- セキュリティ機器設置などの問合せ

「正常にインストールされない」(6 件)
「端末入れ替えや終息に伴うアンインストール要望」(3 件)
「動作が遅くなったことによるアンインストール要望」(3 件)
「ツールがインストールされた一覧が欲しい」(1 件)
「当初予定していた PC より多く導入しても良いか」(1 件)

- セキュリティ対応の相談

「脆弱性監査サービスで警告画面が出ている」(1 件)
「セルフチェックサービスのアカウント取得方法について」(1 件)

- そのほか

「マイクロソフトボリュームライセンスというメールが届いた」(3 件)

【そのほか訪問対応】

- 機器設置などのトラブル対応

「どうしても導入できない端末があるため調査訪問」(1 件)

- そのほか

「業務多忙でインストール作業を行えていない。訪問して対処してもらえると助かる。(4 件)
「社内には、IT に詳しいものがおらず、業者から購入したものは業者に頼むことができるが、今回の件は別件となるため依頼が難しく、送ってもらったツールの導入を実施できていない。手伝ってもらえると助かる。」(2 件)

4.3.2.7 問合せを減らすための仕組み

(1) 客先からの問合せをインシデント管理システムに自動取り込み
→ メールでの問合せを自動で取り込み、受付手続きの簡素化

(2) 回答内容のデータベース化とナレッジの共有
→ 同一内容は、コールセンター内で折り返し回答を実施
- インストールの正しい手順
- トラブルシューティングおよびヒアリングガイド
- Windows 更新プログラムの適用方法、各種ログの採取方法

→ コールセンター内で問合せ内容・回答の定期的な棚卸しと勉強会を実施

(3) インストールモジュールやインストール手順書の改版（事業部）
→ バッチ形式から、実行ファイル形式（EXE）によるモジュールインストールに変更し、権限昇格（UAC）の自動表示など、権限操作を簡素化。またそれに合わせた写真入りの手順書を改版し

わかりやすくした。

(4) お客様に送付するレポートに対処法も併せて記載（事業部）

→ Windows やアプリケーションの更新方法を明記することで、それに関する問合せがゼロとなった。

4.3.2.8 パソコンの脆弱性報告の課題

サービス中に指摘を受けた課題はない。

4.3.2.9 パソコンの脅威報告の課題

(1) 脅威検知の報告レベルの通知方法が妥当であるか

→ 対応の緊急度に応じて、至急対応が必要なものと、望ましくないアプリケーション（業務上意図して使っていない場合は対処を行うべき）の 2 段階に分けて通知を行ったが、望ましくないアプリケーションとは言え、その後に脅威レベルが上がる可能性もあるため通知を行うようにしたが、通知不要との意見もあり、緊急度はなくとも対処を考慮すべき点の説明が必要と考える。

(2) 診断ツールの情報のみでは悪意のあるマルウェアであるか判断できないケースが地域実証中に発生するか

→ 特に指摘はなかった。

(3) 一般企業向けに実施した昨年北陸事業と、防衛・航空宇宙産業の差異

→ 昨年は脅威レベルの高いもの（Emotet など）も通知があったが、防衛・航空宇宙産業に向けた本実証事業期間では、既存対策で対処されており、脅威レベルの高いものは残存していなかった。

4.3.2.10 マニュアルによる効率化が行えるか

一番作業工数のかかる客先対応の大半を、本実証事業に関する各種作業フローを手順化し、マニュアル化したことで入社 1 年目の担当者でも作業を実施することができた。

4.3.2.11 駆け付け対応支援（インシデント初動対応）の課題

(1) 地域実証中にこのような対処が必要となる件数

本実証事業では高いレベルの脅威は 0 件であり、駆け付け要請も 0 件であった。

(2) 初動対応の総時間

0 時間。

4.3.2.12 セルフアセスメント「情報セキュリティ整備状況診断」の課題

(1) 回答手続きの煩雑さ

ログインまでのガイダンスに顧客情報を取得するプロセスを含んで行った。このプロセスが少々煩雑になったことで、入力までたどり着けない企業が数社あった。

- 中小企業の中でも家族経営をされている企業に多く、パソコン全般は総務を担当している方がせざるを得なかったことが一因として挙げられる。
- 今回はセキュリティ意識を高める取り組みであるため、ユーザー登録や**認証の仕組みにも慣れてもらうことも重要**と考え、2 段階認証など少し高度な要求を行ったことが**難易度を上げた**と

考える。

→ Excel に設問を記載し、Excel への回答記載を電子メールで返信してもらう方式に切り替えた。

(2) 設問の難易度

今回の入力対象社のペルソナを、航空防衛産業に関わる下請けの中でも海外の取引についても後々関わることになる企業を考えて設定していた。実際に今回の入力結果については、2 つの顧客傾向がある。

① 従来から航空・防衛に深く携わっており、下請け企業としてではなく、自らも積極的に海外ビジネスを拡大したい会社については、既に 35 項目については達成しているため、セルフアセスメントは確認レベルで行った。

このような企業は ISO 9100 認証を取得しており、日頃から情報セキュリティへの関心や対応に敏感な企業である。

質問内容にも精通し、対策としてはある程度できている企業が多い。

コンサルタントによるアドバイスについても、従前から理解しているあるいは指摘されたことを直ぐに行動に移すことができる知識と労力がある。

② 「CMMC」というキーワードを聞いたことも無い。情報セキュリティ施策については、第三者のシステム管理会社に委託、あるいはクラウドサービスに依存しているため、自ら重要性は把握しているものの、その内容については考えていなかった。

まず、**質問そのものがわからないケース**、さらに質問は理解できても、**自社の対応がどこまでできているかを把握していないケース**（担当が不在）。

→ Excel シートにヒアリング項目として作り直したものを活用し、PFU 技術員が各社を**訪問し、1 対 1 で質問内容を説明しながら例示しながらヒアリングする方式**に変更した。

4.3.2.13 機密性の高いデータ共有の課題

今回、利用の体験をしてもらったサービスは、直接的に NIST SP800-171 のセキュリティ基準項目への対応を目的としたものであり、基準対応を主眼に置いているユーザーでないと利点を見出すことが難しかった。

・ 機微な情報を扱うサービスであり、実証をしてもらうための環境整備に時間がかかり、ユーザーに負担となる。そのため、実証してもらえないケースが多かった。（今回は、米国のサービスであったために、余計、手間が大きかった）

→ 基準対応に加えて、オンプレで対応した場合よりも、クラウドを活用した利便性、コストメリットをより訴求する。

→ 個別、各企業様に実証環境を構築するのではなく、まとめて環境を準備する、あるいは、簡易的にデモ環境を用意して、体験してもらう方法を検討する。

→ 日本でサービスを構築し、柔軟に実証環境を整備する。

4.4　報告会などによる事業成果の周知

9～12 月に実施した本実証事業から得られた知見を、実証参加企業へフィードバックする場を設けた。

4.4.1 報告会の県別参加企業数

表 4-45. 成果報告会参加企業の県別企業数

所在地	組織数　（人数）
東京都	8 組織　（9 名）
愛知県	5 組織　（5 名）
栃木県	3 組織　（3 名）
岐阜県	1 組織　（1 名）
大阪府	1 組織　（2 名）
兵庫県	1 組織　（2 名）
神奈川県	1 組織　（1 名）
新潟県	1 組織　（1 名）
千葉県	1 組織　（1 名）
合計	22 社　（25 名）

4.4.2 報告会の開催概要

開催日　　：　2021 年 1 月 15 日（金）（14:00～15:40）
場所・開催方法：オンライン形式（Q&A チャット機能による随時質問の受付）

下記の内容を実施した。

表 4-46. 成果報告会の開催内容

時間	内容	講演者
5 分	ご挨拶	PFU
20 分	SECURITY ACTION 制度および情報セキュリティ対策ガイドラインのご紹介	IPA
45 分	成果報告	PFU
15 分	サイバー保険の概要と今後の方向性について	損害保険ジャパン株式会社
15 分	今後の事業展開について	PFU

4.4.3 報告会のアンケート結果

4.4.3.1 本実証事業へ参加して良かったこと

SECURITY ACTION の「5 分でできる! 情報セキュリティ自社診断」を初めとした情報セキュリティ整備状況診断のサービスを通し、自社の対策漏れや、他社を含めた対策の弱いところが数値的に見え、今後どのようにすべきか理解できたと考える。

意識調査アンケートから得られた他社の対策状況、サプライチェーンの期待値、対策への費用感などが理解を深めてもらった。

これらを通じて、サイバーセキュリティに対する意識改革に繋ぐことができたと考える。

回答内容

- 弊社は ISMS を取得運用しており、ある程度セキュリティ面は強化していると思っていましたが、**漏れていた部分があり改善でき**て良かったです
- 当社の現状での問題点が見えたことと、今回の報告会で**他社の状況を知ることもでき**良かった
- 見守り隊の商品化サービスについて興味があり、導入検討をして行きたいと思います
- **具体的数字が示されて理解でき**ました、思ったより参加企業が少なく感じました
- インシデントが起きていないことが確認できました、**今後どのようにすべきか**についても、少しわかりました
- 社内にある **PC のセキュリティ対策状況をある程度把握すること**ができた、結果として、深刻な問題が無いことがわかった
- 情報の共有を始めとして、**修正改善すべきところ**もあったので勉強させていただきました
- **サプライチェーンの中で期待されるセキュリティ**の概要に触れられた
- 社内 PC の**具体的なセキュリティチェック項目**が見えた
- 社内の**制度、規則としてどのようにすべきか**の指針を見ることができた
- 情報セキュリティの**最新情報や、他社の動向**が把握できて良かった
- このようなサービスをご提供されていることがわかったこと
- 世の中の**「相場」がわかり**ました

4.4.3.2 本実証事業で改善が必要なこと

中小企業は、社長があらゆることを実施しており、このような多忙な中でも参加しやすくなるような、仕組みが求められていた。中小企業での課題と言える。

結果の共有に関しては、報告会だけではなく、個社毎に Web 会議を用いた対面指導を行う場を持つべきとの意見をもらった。事業説明でよろず相談窓口としたコールセンターを説明していたが、活用されていなかったと言える。

導入環境においては、OS の再起動にも時間がかかる状況もあり、本実証事業で追加のツールを導入してもらったことで、業務に支障が出てしまうケースが指摘されている。　このようなスペックにおいても業務に負荷をかけないようなツール作りを、ツール開発側へ共有して行く必要がある。

本実証事業のタイトルが固く、参加の敷居が高かったとの意見もあった。今後の事業で考慮が必要と考える。

回答内容

- また来年もやっていただければと思います
- 見守りソフトにより、**パソコンの挙動が重く**なってしまうという問合せがありました
- 顧客からの案内が無ければ、**本実証事業の存在を知ることができなかった**、名称なども含め、何となく**敷居の高い**ものであるかのように感じて躊躇してしまう
- 今後の事業展開の説明において、今回導入したチェックソフトの導入だけ（駆け付けは別料金）の**安価なものも**、ご用意いただき、まずは敷居を下げて利用者を増やした方が良いように思います
- 途中から　今回のモジュールが原因かどうかわかりませんが、**殆どの PC から削除**しました。何故かそれで直りました。
- 改善ポイントは、**テスト台数を幾通りかに絞ってやって行く方が良い**のかも知れないと思いました、企業によって台数が違うので、統計をとる際は有効ではないかと
- 今日の説明にもありましたように、**中小企業は社長がなんでもしている**ところが多いので、そのような方でも対応できるようにするべきだと思いました
- 今回は貴重な時間をお助け隊事業者の皆様にいただいているので、少し甘えて、アンケートだけではなく**対面（電子的に）で、直接ダメ出しをしていただく**ことにより、さらに貴重な情報が得られるのではないでしょうか？
- 費用をかけてどこまでセキュリティ強化をすれば良いか、**具体的なトラブル事例などで情報を展開いただく**と、より必要性が理解できたと思います

4.4.3.3 報告会への意見

全体的に数値化した報告に好感度を持ってもらえたが、目標値に対してどうだったかも説明が必要と意見があった。情報セキュリティ整備状況診断では良し悪しの数値を色付けして説明できたが、ツールでの実態把握でも、提示できれば良かったと言える。

サイバー保険の理解は促進できたが、今後の事業展開の中でサイバー保険までワンパッケージとした価格を提示したものの、サイバー保険の説明で価格感の提示がなかったことが残念と感じられていた。

回答内容

- **数字で報告**いただいて具体的に内容がよくわかりました
- 細かな資料は僅かに読みづらさを感じました、資料をいただけるとのことで、十分に補足されるものと考えております
- サイバー**保険の概要を理解することができ**、有意義でした
- サイバー保険の説明で、**概算価格も提示をしていただけるとなお良かった**と思います。
- サイバー保険は、必要ではあると思いますが、現状どうなのか？というところです
- お助け隊については大変興味があります
- 事前に資料をいただけるとなお良かったと思います
- 実証参加企業の数も含め、**具体的な数値での解説**で、非常にわかりやすかったです
- 成果報告は、似通ったものも多かったです
- 大変勉強になりました、ありがとうございました
- 成果については**数値化されており良かった**のですが、それで十分な効果があったのか、**目標に対してどうだったのかなど判断がしづらかった**

5　考察

5.1　実証参加企業におけるサイバー攻撃の実態

防衛・航空宇宙産業という名目で特別な対策を要求された企業は、特に業種、規模で割合が偏ることもなく 38%程度あった。要求された対策として「知るべき人にだけ知らせる」（Need to know の原則）、「アクセス権は必要最小限の範囲でのみ認められるべき」（Least privilege の原則）に関するものであった。しかしながら、秘密情報を管理する上で行うアクセス管理回りは、半数が実施できていないという回答がある。

被害に遭う可能性は 90%の企業が感じているが、脆弱性診断やサイバー保険など、一段階進めた対策は 28%の実施に留まっていた。

実証参加企業へのヒアリングでは、過去にサイバー攻撃を認識している企業は 27%であった。認識されている被害は、身代金を請求するランサムウェア、取引先に迷惑をかける Emotet のような目に見えるものから、目に見えないバックドアも回答にあった。

本実証事業期間（3 か月）の間に、これら既存対策（ゲートウェイ対策製品やパソコン内の既存セキュリティ対策ソフト）で対処されなかったマルウェアは、緊急度の高いものは無く、PUA（好ましくないアプリケーション）程度に限り検知されていた。内容は、アドウェア（広告を経由してマルウェアが配信されるかも知れないもの、追加でアプリケーションが導入されることでマルウェアが混入する恐れのあるもの）、他社アンチウイルス製品を削除するために使うツールなど、1766 件、193 種、9 つのマルウェアグループとなっていた。

パソコンに導入されているセキュリティ対策ソフトを調査したところ、Windows 10 の導入が進んだことで、無料の Windows Defender が OS に標準搭載され、65%は OS 標準対策でカバーされている。Windows7 が多かった昨年と異なり、既存対策により対処が行われており、対処漏れと言える程の脅威は検知されていない。

工場に限定してセキュリティインシデントを確認したところ、殆どの企業では経験がなく、唯一経験していた 1 社も感染原因までは調査していないとのこと。

データの受け渡しを行っている企業は、92%と殆どの企業で行われており、製造業が大半ということもあり「図面」や「部品データ」の記載が多く見られた。受け渡している取引先は、概ね 10～20 社であった。

このような機密データの受け渡しに関わる担当者は、大規模な会社は一部の人が担当しているが、小規模な会社は全員が関わっている状況である。小さい会社ほど全社員への教育が重要と言える。

セキュリティを意識して受け渡しをしている企業は 67%であり、残りの 33%の方は、運用が煩雑になると利便性に重点を置かれていることや、コスト増加の懸念があった。また、何すれば良いのかわからないため意識もなく、社内への周知もできないといった回答もあった。

受け渡し手段は、暗号化した電子メールに加え、機微な情報は手渡しをしていた。電子メールで暗号化した情報を送る場合も、半数は都度暗号パスワードを送っている状況であり、セキュリティ対策としては高いとは言えない。

クラウドでの送受信は、抵抗感も低く、今後はクラウド経由での授受が増えて行くものと考えられる。

5.2　中小企業におけるセキュリティ対策

CMMC L1 は要件 17 項目全てに適合しない限り認定されない。今回のセキュリティ対策整備状況診断を受けた 50 社中、適合したのは 5 社（10%）であった。

そのほか 3 項目以内を達成すれば CMMC L1 に適合可能という企業も 5 社（10%）あった。不足していた事項は、システムのユーザー管理に関するものや、多要素認証の適用、ファイアウォールの設定などのシステム環境などに不適合項目が見られた。

これらの結果より、未実施の項目に絞って対策を行えば、一定の水準になりうる企業もあることから、適切な指導を併せて行い、無駄なく効率的にセキュリティ対策のレベルアップを行うこともできることが判明した。このようなセルフチェックの効果が期待できると考える。

セキュリティ意識調査から得られた対策状況として、セキュリティ対策が不十分と感じている企業は、とても高い 80%もあった。

PC の OS やソフトを最新に保つ仕組みは 50%程度に留まっており、実証参加されたパソコンを実際に調査したところ Windows Vita、Windows 7、Windows 10 Version1903 以下、Windows Server 2008 といったサポート切れ OS が 14.3%見つかった。また、半年以内にサポート切れとなるため、計画的に更新が必要となる Windows 10 Version1909 も 29.7%見つかっており、さらにパソコン上の脆弱性更新に関する適用状況を監視したところ、およそ半数は数週間経っても脆弱性が解消されず危険な状況にあった。

今回は、製造業の参加が多いこともあり、60%の企業で工場を保有している。この工場のネットワークに想定外の機器が接続される可能性について確認したところ、1 社を除き無いと回答している。しかし、工場を保有している企業の 88%が、工場とオフィスのネットワークは繋がっていると回答があった。実際に、6 社の工場ネットワークにセンサー装置を設置させていただき、繋がれている IT 機器の探索を行ったところ、工場の制御機器用だけではないものの、Windows2000、 Windows 2000 Server、Windows XP、Windows 7、Windows 8、Windows Server 2003、 Windows Server 2008、Windows

Server 2008 R2 といった、サポートが切れている OS が 14%も見つかった。メールや Web 閲覧をするマルウェア感染しやすいオフィスから、これら脆弱なパソコン（専用装置を含む）へ波及する懸念が高い。

また、工場内ネットワークについて把握したいことをヒアリングしたところ、台帳で管理できる程度の企業も多いが、繋がれている機器を把握したいという意見。さらに機器の脆弱性について把握したいとの意見もあった。しかし、サポート切れの専用機器は、ハードの更改が必要となるため、脆弱対策とは言え、高額となることが課題との回答もあった。

持ち込み機器の接続に関しては、概ね事前申請を求めている。その中で 1 社のみセキュリティ対策（脆弱性更新やセキュリティ対策製品の導入）まで確認を行ってから接続を許可していた。

意識調査アンケートでは VPN により外部からオフィス内に接続を行っており、前記のとおり、工場ネットワークとオフィスネットワークが接続されている環境下では、よりリスクが高くなっている。安全性の異なるネットワーク境界に、何かしらの対策を導入し、ネットワークへの不要な機器の接続を防止することが望まれる。

個人所有のパソコンを利用する際の、セキュリティ対策を明確にしている企業は 38%程度に留まっている。脆弱かつマルウェアが混入したパソコンが接続されるリスクがある。

5.3　中小企業において必要なセキュリティ対策

セキュリティに関する相談窓口を持っている企業は 54%程度であり、専門家の意見を得られる環境作りが必要と言える。また、社内のセキュリティポリシー（ルール作り）は 20%程度であり、SECURITY ACTION の更なる推進が必要と言える。

製造業が多いということもあるが、中小企業では脅威の検知から復旧を最優先に求められている。

サイバー保険を知っている企業は半分程度で、加入している企業は僅か 8%だった。サイバー保険に加入している理由としては、万が一の訴訟や賠償に加え、取引先から求められたためという意見があった。逆に、加入していない理由としては、社内セキュリティを優先的に向上させたい、予算がないといった「コスト」的な面に加え、保険の詳細がわからない、必要性を感じないといったものがあった。

5.4　中小企業におけるセキュリティ対策の効果

脆弱性を対処することで攻撃者へのハードルを高めることができる。しかし、セキュリティ対策にかけることができる費用は、月額 1 万円程度が多く、お助け隊サービスを継続する場合も、パソコン 1 台あたり月額 500～1000 円が半数を占めている現状から、効果な対策を導入することは困難と言える。

サイバー保険は、どのようなものか理解が進んでいない現状もあり、周知徹底が求められるが、月額の 1000～5000 円が期待されていることから、万が一の時、取引先への報告を含めた初動を行える部分を提供することで、まずは効果を周知した上で、低価格に始めることで利用への壁が低くなるものと期待される。

工場ネットワークとオフィスネットワークが分離されていない実態が見えてきた。工場ネットワークが脆弱性に対処できない専用機器もあり、オフィスネットワークと接続する場合であっても、オフィスネットワークから必要な通信に限定してマルウェアが伝播しないようにすること。さらに工場ネットワーク側に、メールや Web 閲覧をさせないような通信制限も行うことや、持ち込み機器を気軽に接続されないようにすることで、リスクを減らすことができる。

機密データの受け渡しでは、小さい会社では全員が関わっているため、小さい会社ほど全社員への啓発が効果を上げるものと考える。

6　実証を踏まえたビジネス化に向けた検討

6.1　サイバー保険の活用

6.1.1 セキュリティ簡易保険サービスに関するマーケティング方法の検討

実証参加企業にセキュリティ意識調査アンケートにより、サイバー保険に関する下記内容のアンケート調査により情報を収集した。

- サイバー保険の存在を知っていますか
- サイバー保険に加入していますか
- 加入した理由／加入していない理由は何ですか
- 既存のサイバー保険やサービスの価格帯は高いと思いますか
- サイバー保険として妥当だと思う保険料（月額）は幾らですか
- サイバー攻撃の被害にあった場合は多額の費用が必要となるケースがありますか、どのような費用が保険で補償されるとメリットを感じますか

上記アンケートで得た結果をもとに事項より今後のサイバー保険の検討を行う。

6.1.2 中小企業向けのサイバー保険検討

サイバー保険に関するアンケート結果からサイバー保険の認知度は 53%、サイバー保険に加入している企業は 8%であった。仮に、サイバー保険の認知度が 100%であっても 17%の企業しかサイバー保険に加入しない計算になる。残る 83%の企業はいくつかの理由により保険には加入しない。

まず強化すべきはサイバー保険の認知向上であるが、アンケート結果のサイバー保険に加入しない主な理由について解決策を検討する。

表 6-1. サイバー保険へ加入しない理由

加入しない理由	サイバー保険加入促進施策
保険の詳細がわからない	・顧客が理解できる説明／わかりやすさ 損害保険会社のサイバー保険商品の改善、説明等の工夫、保険外交員への教育促進など。
予算がない	・安価な保険商品の検討 令和元年度、令和２年度のサイバーセキュリティお助け隊事業のデータをもとに再度の見直し実施。サイバーセキュリティお助け隊の監視・駆け付けサービス内容分析により、どの程度リスク低減に貢献できるか IT サービスベンダーと損害保険会社が協力して数値化に取り組むことで低価格化ができる可能性がある。
セキュリティ向上が先決	・監視サービスへの簡易サイバー保険付帯 次項にて具体的な今後の対応を説明する。

必要性を感じない	・サイバー攻撃の怖さ実態の啓発を継続 国・産業・IT ベンダー全体での啓発・施策の継続が必要。

6.1.3 監視サービスへの簡易サイバー保険付帯

6.1.3.1 監視サービス付帯の簡易サイバー保険の位置づけ

下図のイエローゾーン（中間の黄色帯）は監視サービスで検知したマルウェア種別や潜伏期間などにより初動対応にかかる労力は想定しづらい。中小企業向けに低コストで最低限必要なサービスを目指すにあたっては初動対応のコストが算出しづらく、リスクを多く見込むとサービス高額化となり、リスクを排除するために初動対応の対応範囲を限定すると不満足なサービスになる要因となる。この課題を緩和する役割がサービス付帯のサイバー保険の位置づけであり、ある程度の初動調査の幅がもてるようになる。

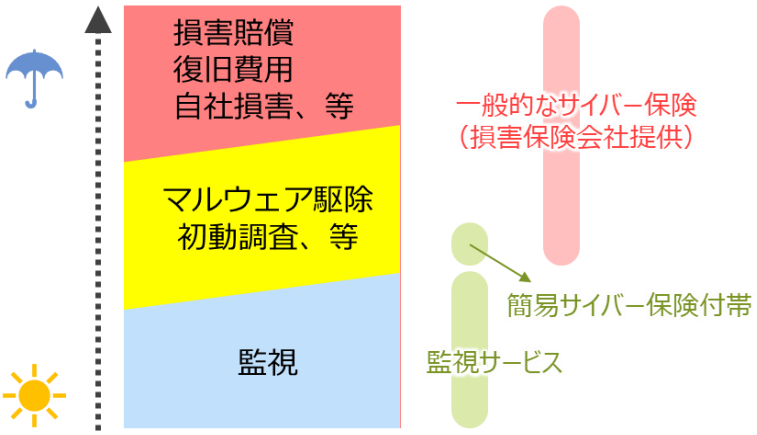


図 6-2. 5.1.2.1　監視サービス付帯の簡易サイバー保険の位置づけ

6.1.3.2 監視サービス付帯の簡易サイバー保険の制約

サービス付帯の保険は監視・駆け付けサービスの景品的な位置づけとされるため補償額には上限がある。そのため初動対応でできることはこの制限による補償金額の範囲となり、PFU ができることや顧客が求めることには必ずしも合致しない。

PFU が提供するサービスでは、主に感染が拡大している可能性がある場合の調査、情報漏えいの形跡がないか調査するための補填として活用することを検討している。

6.2　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

6.2.1 セキュリティ対策サービスのマーケティング方法や支援体制について

6.2.1.1 防衛・航空宇宙産業の市場規模（マーケティング）

防衛・航空宇宙産業の中小企業母数は、防衛装備品の生産に参加する企業 約 3,480 社（※1）、航空機クラスター企業 約 900 社（※2）などから全国で約 5,000 社前後と推測する。産業を縛らずに中小企業数をみれば埼玉県の 16 万社、千葉県の 12 万社と比べても防衛・航空宇宙産業の企業数は市場規模的には大きくない。

※1 情報： H.23（社）日本防衛装備工業会の情報より

※2 全国航空機クラスター・ネットワークホームページの情報より

6.2.1.2 防衛・航空宇宙産業の市場性とビジネス化に向けた検討（マーケティング）

アンケート結果より、防衛・航空宇宙産業の中小企業は、昨年北陸地域の中小企業よりも対策レベルや意識レベルは若干高い数値となっているが、機密性の高い情報を取り扱う産業分野であること、米国との取引に関係し影響を受ける可能性があることなどを考慮しておきたい。

今後の米国の動向（対策の義務化）により国内企業においても取引に関わる限り対策強化が必要となることが想定されるため、サプライチェーン全体での対応検討が求められてくる。

今後の防衛・航空宇宙産業における中小企業のサイバーセキュリティ対策普及に向けては、中小企業だけにフォーカスせずサプライチェーン全体の対策をどう底上げするか、その一連の対応の中で中小企業向け「お助け隊」サービスをどう位置づけるのかは重要と考える。

6.2.1.3 中小企業のサイバーセキュリティ強化に向けた課題と対応

令和元年度（北陸）・本年度（防衛・航空宇宙産業）の実証において共通することは、ウイルス対策やファイアウォール・UTM などの製品を導入していることが対策されているか否かの判断基準となっており、侵入を前提とした事後対応の必要性が浸透していないと感じる。

どのような最新技術の製品を導入してもそれを回避する攻撃手法により侵入が行われ、最新技術の製品をもってしても専門技術者（または AI など）が侵入の徴候を数百・数千のアラートから分析する必要があることが理解されなくてはならない。本実証においては「既存対策をすり抜けた脅威に対応する事後対応支援」というように、なるべく平易な言葉でそれを説明するように心がけた。

今後のマーケティング活動として、地域経産局および主要な業界団体に対して本実証結果をフィードバックすることで業界内へのサイバーセキュリティ強化の意識喚起を行う。

6.2.1.4 今後の支援体制について

防衛・航空宇宙産業に向けたサイバーセキュリティ強化支援については、今後の米国動向などを考慮し、動向を踏まえた対応ができるよう本実証事業サービス提供事業者は引き続き連携体制を維持する。

直近のサービス提供については、産業に関わらず中小企業共通の対策となる、サイバーセキュリティ脅威から中小企業の事業継続をサポートする「監視・駆け付け対応に加え簡易保険を付帯したサービス」（仮称「お助け隊サービス」とする）を提供する。

また、産業特性を考慮したコンサルティングサービスやサプライチェーンの企業間でやり取りされる機密データの共有サービスは本実証で得られた中小企業のニーズを踏まえ今後のビジネス化を継続検討する。

ビジネス化に向けては、防衛・航空宇宙産業のプライム企業が求める対策についての意見確認とサービスへの反映を進めて行く必要があると考える。

表 6-3. ビジネス化の検討状況

提供サービス	中小企業向け商品	備考
①仮称「お助け隊サービス」（監視＋駆け付け支援＋簡易保険付帯）	本実証で提供したサービス内容で提供 提供時期：2021 年 2 月頃	既存の対策をすり抜けた脅威について、侵入を前提とした事後対応支援として提供することで中小企業の事業継続をサポートする。
②セルフアセスメント ＊サービス化継続検討 ＊米国の規定などの産業特性を考慮したサービス	コンサルティングサービスとして、関連情報や教育などを加えた形での提供を検討。 提供時期：2021 年度	セルフアセスメントは現状認識の入口であり、中小企業がとるべき対策を、個々の会社のリスク／要件ベースに整理する相談窓口が必要。
③機密性の高いデータ共有 ＊サービス化継続検討 ＊米国の規定などの産業特性を考慮したサービス	中小企業にも対応できるサービスを検討 提供時期：2021 年度	プライム企業と連携しながら、サプライチェーンを構成する中小企業に合わせて仕様、価格の検討を行っていく。
④工場の IT 機器見える化 ＊個別対応とする	個別対応	見えた課題に対する改善サービスを提供することが本質であるため、工場に持ち込み機器に対する運用アドバイス、事務所と工場のネットワーク分離など個別に対応する。

次項で「①お助け隊サービス（監視＋駆け付け支援＋簡易保険付帯）」について説明する。

6.2.2 仮称「お助け隊サービス」（監視＋駆け付け支援＋簡易保険付帯）

6.2.2.1 中小企業に向けたサービスとして事後対応支援をワンストップで提供

① ワンストップサービスの概要

中小企業が導入しやすいように必要なツールや支援サービスが全てパッケージ化された商品として提供。

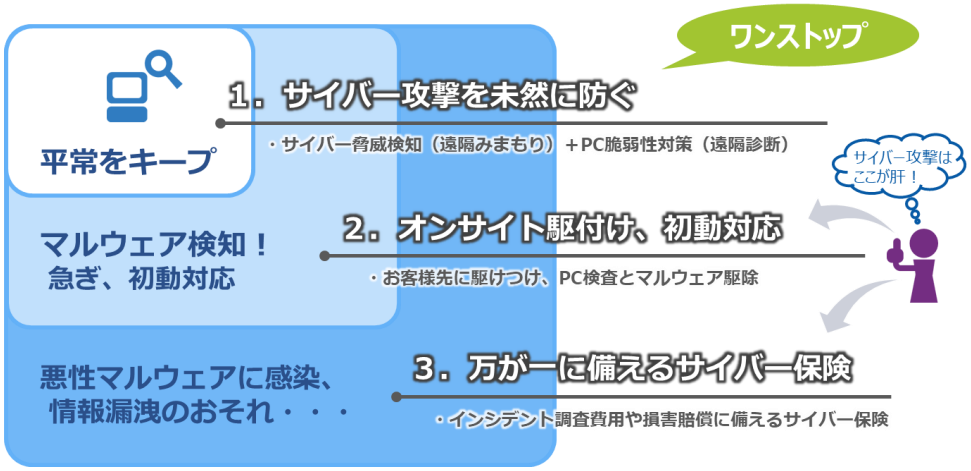


図 6-4. ワンストップサービスの概要

② エンドポイント型のサービス採用理由

テレワークで利用する PC もサービス適用対象とでき、また、リモートからマルウェア隔離などの操作ができるため、利用者の負担軽減、問題対処の時間短縮に優れているため。

③ 提供価格の検討

アンケート結果をもとに価格設定するが、PC1 台あたり月額 500～1,000 円程度で提供する。

6.2.2.2 サービス内容

表 6-5. サービス内容

サービス内容	概要
導入支援	サービス開始に向けて提供ソフトウェアの導入作業を支援するサービス。
PC のサイバー攻撃脅威検知と情報通知	ソフトウェア「WEBROOT 社製 SecureAnywhere Business」の利用と、遠隔監視した脅威情報は 1 日 1 回メールにて報告。
PC 脆弱性監査と週次レポート報告	ソフトウェア「PFU 製 iNetSec Inspection Center」の利用と、Windows の OS バージョンや、主要ソフトウェアのセキュリティパッチ適用状況などを検査し週次で報告。
問合せ対応	電話や E-Mail にて利用者の問合せに対応。
オンサイト初動対応支援	客先へ駆け付け、感染状況調査やマルウェア駆除支援などの初動対応支援について全国エリアを対象に実施。

サービス内容	概要
簡易サイバー保険 （サービス付帯）	サイバーインシデントや情報の漏えいの恐れに起因する賠償責任（損害）や「端末調査」および「情報漏えい調査」の費用に対して保険金が支払われる。補償額の上限は年間 200 万円程度に設定。
ベンチマーク診断（年 1 回）	利用者の対策状況を幅広い観点で診断。匿名化し集計した後に他社の水準と比較して自社の状況を確認できるように共有、今後の対策検討に役立ててもらう。

6.2.2.3 サービス提供で得られた知見の取り扱いと活用

本サービスで使用する iNetSec、WEBROOT で得られる IP アドレスや脆弱性、感染マルウェアなどの情報を収集し集計したのち匿名化する。匿名化した情報はセキュリティ対策のためのデータ分析、製品改良（新製品開発を含む）、講演などで使用する。

6.2.2.4 実証事業を通じた工夫や改良点

表 6-6. 実証事業を通じた工夫や改良点

サービス内容	工夫、改良点
導入支援	実証事業では手順書による顧客作業として進めたが、多忙で作業に着手できない、PC 環境に依存する問題で手順通りに作業が進まないなどの課題が明らかになり有償サービスを用意する方向で検討する。本サービスは初期費用として一括支払いを申し受けるサービスとする。
PC のサイバー攻撃脅威検知と情報通知サービス	コストのスリム化と顧客の負荷軽減を目的に、WEBROOT 社のエンドポイント製品と外部インテリジェンスを活用した PFU 独自の分析システムを構築。過検知や緊急性の低いアラートを除去した緊急性の高いアラートに絞り通知する。令和元年度に北陸で実証した際には緊急アラートのみに絞ったが、緊急対処の必要性は低くとも業務上好ましくないプログラムなどの情報はある程度ほしいという顧客要望に対応した。但し、顧客ごとにスキルや意識が異なるため、中小企業向けの通知内容や通知量に対する最適化は継続する。
PC 脆弱性監査と 週次レポート報告サービス	令和元年度の北陸実証では月次報告としていたが本年度は週次報告に変更。報告内容についても具体的な対処がわかりやすいフォーマットに変更したことで脆弱性の改善を行うお客様が増加した。

6.2.2.5 サービスに付帯するサイバー保険

サービスに付帯するサイバー保険は、補償額上限が年間 200 万円程度までとし、サイバー攻撃の疑いがあり詳細な調査が必要となった際の費用補填の位置づけとする。サイバー攻撃による金銭的被害は巨額の損害賠償への対応だけではなく、そこに至るまでの調査に数百万の費用が必要となる。

それ以上の補償を求める利用者には損害保険会社が提供する一般的なサイバー保険に加入してもらうよう誘導する。

【想定される保険適用ケース】

- 感染が拡大している可能性がある

「適用例：影響調査」

高度技術者による調査・対応方針検討後、十数台の PC 調査や調査現場の切り盛りなどであわせて 100 万円前後が初見で必要となる。

- 情報漏えいの形跡がないか調査したい（悪性のマルウェアに感染）

「適用例：被疑端末の解析調査（デジタルフォレンジック）」

PC1 台の調査で 1～200 万円程度必要。一概には言えないが、中小企業規模の場合は 1 インシデントで平均 1～400 万円程度の調査費用になる場合が多いと想定される。