# 【テーマ研究報告書】

# 中小企業におけるサイバーセキュリティ対策等に有効な無償・安価ツールの研究

## ～サイバーセキュリティお助け隊サービスの研究～

２０２３年3月３１日

特定非営利活動法人 ITC ちば経営応援隊

テーマ研究 チーム１

# はじめに

本テーマ研究は、独立行政法人情報処理推進機構（以下 IPA）が選定した「サイバーセキュリティお助け隊サービスの 10 件（研究開始時に選定済みで、全国展開のサービス、情報がホームページ等に公開されているものを対象とした）」の中味を調査・分析・評価し、その検討結果をもって我々ＩＴコーディネータがセキュリティ対策を支援している中小企業、小規模事業者（以下、中小企業等　という）に適したサービスを提案するという取り組みである。

メンバーで分担を決め、意気込んで調査を開始したものの、各サービス提供企業のホームページや問合せから得られる公開情報は限られており、かつ掲載されている情報も各社ばらばらで難解な表現が多く、機能や内容を整理し比較するには相当な苦労を要した。

一方、提案先の企業においても、IT 機器を利用するネットワーク環境等には様々な条件や制約があり、一律に安易な決めつけや選択ができない状況であることも認識した。

とはいえ、今回のメンバー5 名には、慎重派、大胆派、緻密派、率直派など様々なタイプが揃っており、技術面のみならず費用や使い易さなど様々な切り口で自由なディスカッションや判断、評価を行いながら、中小企業等の立場に立つということを第一に考えた上で、分かりやすさという点を大切に、かなり思い切った割り切りをもって成果物をまとめることとした。

私たちの研究成果が、サイバーセキュリティの脅威に対処が求められている中小企業、小規模事業者の方々や、それらを支援する皆様に少しでもお役に立つことを願うと同時に、本研究成果を更にブラッシュアップするために、我々の知見のなさや調査不足などに起因する改善・修正点に関する厳しい指摘も大いに歓迎することを付け加えておきたい。

# ＜目次＞

# 1．テーマ選定の背景と本研究の目的

## 1.1 中小企業における情報セキュリティ対策の状況認識

昨今、サイバー攻撃は、企業規模など相手を問わずランダムな波状攻撃を仕掛けてきており、セキュリティ対策に「十分な費用や、人的資産」を掛ける余裕がない中小・小規模事業者においては、大半の事業者がいつ被害を受け事業存続の危機に陥っても不思議ではない状況となっている。

特に、ネットワークを中心とした、サプライチェーン上の様々な脅威に対する技術的対策の強化が、中小・小規模事業者において喫緊の課題になっている。

## 1.2 サイバーセキュリティお助け隊サービスに対する認識

情報セキュリティ対策は、「組織的対策」、「人的対策」、「物理的対策」、「技術的対策」の４つの分野※1で整理される。

中でも「技術的対策」は、サイバー対策には欠かせないものであるが、製品の選定・導入など企業の費用負担増と直結し、且つ専門的な知識が要求されるため、企業側の立場に立った信頼できる専門家による適切なアドバイスが求められる分野である。

２０２１年３月から、IPA がウイルス対策ソフト導入の次のステップとして「サイバーセキュリティお助け隊サービス」を選定し、中小・小規模事業者に推奨していることは非常に有効な施策であるが、サービスメニューが多数リストアップされる中で、どのサービスが個々の企業に最適かどうかの選択を企業独自で行うのは困難なのが実情である。

## 1.3 ＩＴＣちば経営応援隊の活動の状況認識

ITC ちば経営応援隊は、昨年度まで、IPA のセキュリティ対策普及事業の受託や千葉県地域 SECUNITY における企業支援活動などにおいて、IPA の「5 分でできる情報セキュリティ自社診断」や「中小企業の情報セキュリティ対策ガイドライン」等を使用し、主に、ITC プロセスの”上流工程”の指導助言を実施してきた。

しかし、今後セキュリティ対策の一貫した支援を行うためには、支援企業(主に小規模企業者）の実情に合った「安価で、専門知識がなくとも運用可能」なツールやサービスの導入を含めた”下流工程”の提案・支援が是非とも必要だと考える。

ゆえに今回の研究成果物を「千葉県地域 SECUNITY」参加団体・企業等に、セキュリティツール導入の際の選択肢として活用・提案できるものにすることを目的とする。

【目的】「サイバーセキュリティお助け隊サービス」の調査分析を行い、評価した結果をもって実際の支援活動の中で活用する。

※1.参考：情報セキュリティ対策の 4 領域　　※JNSA ホームページから引用

情報セキュリティ対策は、「組織的対策」、「人的対策」、「物理的対策」、「技術的対策」の 4 つの領域に分類される。

- 組織的対策：ルール作り、ルールを守る取り組み、ルールが守れる PDCA（それにプラス、技術と人への資金手当）
- 人的対策：個別の場で従業員一人ひとりの規則遵守（コンプライアンス)、判断、目配り気配り、運用と管理
- 物理的対策：オフィスへの入退室・施錠管理、PC など情報機器や USB メモリ・紙などの記録媒体の管理（移動・輸送・廃棄も含め）
- 技術的対策：ウイルス対策ソフトやファイアウォールなどの正しい配置と運用による防御、ならびに常時監視、定期チェックによる検知・発見

## 2.サイバーセキュリティお助け隊サービスとは

中小企業もサイバー攻撃に晒されている。IPA が実施したサイバーセキュリティ対策実証事業（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）では、中小企業約 1,100 社に対して、社内アクセスの侵入を試みる不審なアクセス検知数が、181,536 件認められ、ランサムウェアやトロイの木馬などのウイルスを検知し無害化した件数は 1,345 件、対象を怠った場合の想定被害額が 5,000 万円になる案件も確認された。

ウイルス対策ソフトだけでは、このようなサイバー攻撃を防ぐことはできない。サイバー攻撃に対して、人材や予算が限られる中小企業でできる効果的な対策の一つが、「サイバーセキュリティお助け隊サービス（以下、お助け隊サービスという。）」の活用である。相談、見守り、駆けつけ、保険など中小企業のセキュリティ対策に不可欠なサービスが、使い易く、安価でワンパッケージにセットされている“優れもの”だ。

このお助け隊サービスは、IPA が中小企業向けのセキュリティサービスを満たす基準（図 1）を制定し、その基準を満たしているかどうかを審査するサービス登録審査機関により、適合性を認められ審査基準（【図 2-1】）をクリアしたサービスが「サイバーセキュリティお助け隊サービス」として登録され、マーク（【図 2-2】）を付与されて、後述する中小企業庁事業「IT 導入補助金」では、お助け隊サービス利用料が支援対象に選定されている。

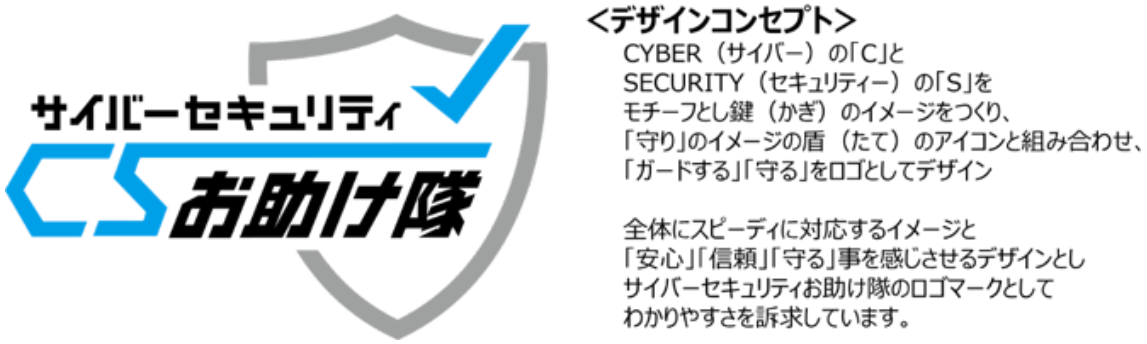
| 主な要件 | 概要 |
|---|---|
| 相談窓口 | ユーザーからの**相談を受け付ける窓口**を設置／案内 |
| 異常の監視の仕組み | ネットワーク及び／又は端末を**24時間見守る仕組み**を提供 |
| 緊急時の対応支援 | インシデント発生などの**緊急時には駆け付け支援** |
| 中小企業でも導入・運用できる簡単さ | **専門知識がなくても導入・運用できるような工夫** |
| 簡易サイバー保険 | 突発的に発生する駆付け費用等を補償する**サイバー保険** |
| 中小企業でも導入・維持できる価格 | ・ネットワーク一括監視型：**月額１万円以下（税抜き）**<br>・端末監視型：**月額2,000円以下／台（税抜き）**<br>・併用型：**これらの和に相当する価格を超えないこと**<br>※端末1台から契約可能であることが条件 |

現在登録されているお助け隊サービスは、登録審査において、左記要件がすべて満たされている。

リモートでの対応支援も可とする。

表の出典：IPA2022年度セキュリティプレゼンターカンファレンス資料より

【図 2-1】お助け隊サービス審査基準




【図 2-2】サイバーセキュリティお助け隊サービスマーク

## 2.1 サイバーセキュリティお助け隊サービスを選定するポイント

次に、中小企業が自社に合ったお助け隊サービスを選定するポイントを考えてみよう。

お助け隊サービスは、（図 3：企業内ネットワークのイメージ図）のように大きく「端末監視型」と「ネットワーク一括監視型」に分類される。

従って、まず対象企業にとって、端末に対してのセキュリティが必要か、あるいはネットワーク全体へのセキュリティが必要か、またはその両方かを判断する必要がある。

### 1）端末監視型

このサービスの特徴は、従業員(ユーザー)が利用する各端末に導入することで、不審な挙動を検知した場合に迅速なレスポンスがあり、対策につなげる働きをすることである。

※EDR : Endpoint Detection and Response

エンドポイント（端末）にセキュリティソフトをインストールする。

＜選定するケース例＞

企業の事務所以外に自宅でのテレワークや遠隔地の工場等でも端末を利用しており、事務所一か所の UTM 設置だけでは対応ができず、端末単位でのセキュリティ対策を選択する場合。

### 2）ネットワーク一括監視型

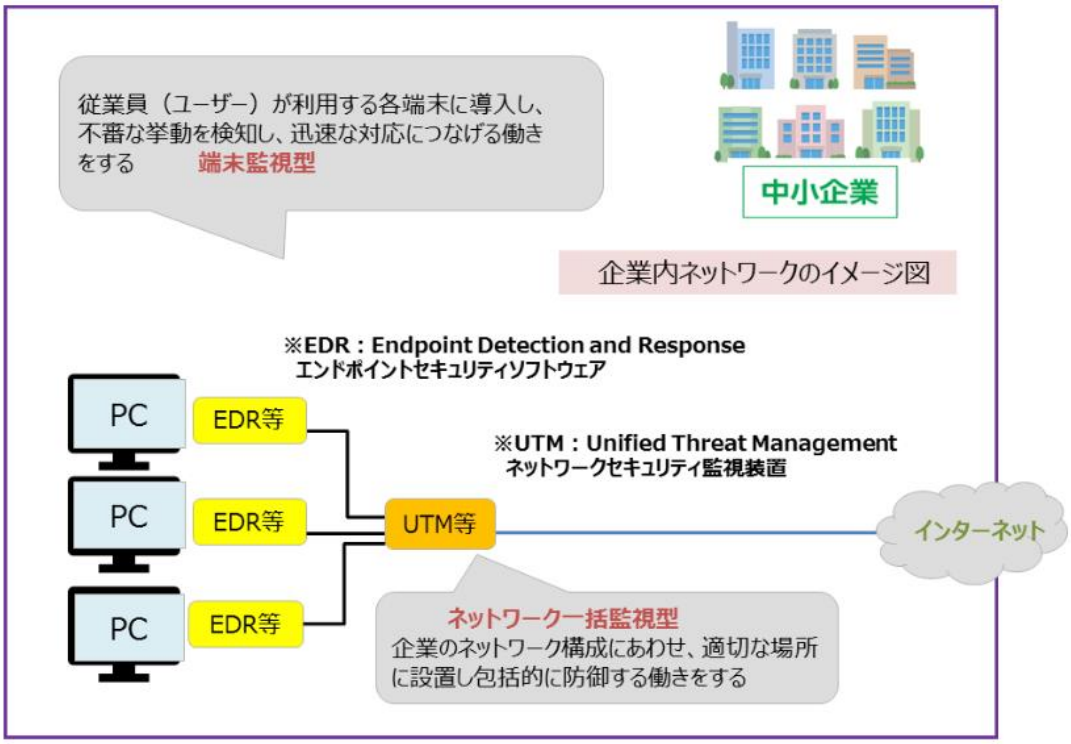
企業のネットワーク構成に合わせて適切な場所に設置しネットワークを包括的に防御する働きをし、事務所の中でネットにつながっている端末すべてを監視する。

※UTM : Unified Threat Management（ネットワークセキュリティ監視装置）を設置する。

＜選定するケース例＞

事務所以外では端末を使用していない場合。UTM により外部からの社内ネットワークへの入り口を抑えることによりセキュリティ対策を行う。

［　企業内ネットワークのイメージ図　］




※出典：IPA「サイバーセキュリティお助け隊サービス」ホームページ

【図 2-3】企業内ネットワークのイメージ

## 2.2 サイバーセキュリティお助け隊サービス選定の際の課題と解決方法

### 1）選定の際の課題

・中小企業には、社内にＩＴに詳しい人材がいないことが多い。
・システムはベンダーに任せていて機器の内容がわからないことが多い。

### 2）解決方法例

・支援機関（最寄りのよろず支援拠点、商工会議所、商工会）や専門家（IT コーディネータ等）を活用する。
・直接ＩＴ導入事業者に連絡することも可能だが、支援機関や信頼できる専門家を利用して必要なセキュリティを相談しながらの導入が望ましい。
・この機会を利用して、社内で IPA が推進する SECURITY ACTION（中小企業の自己宣言）等を利用し、社内でのセキュリティ知識を向上することも必要である。

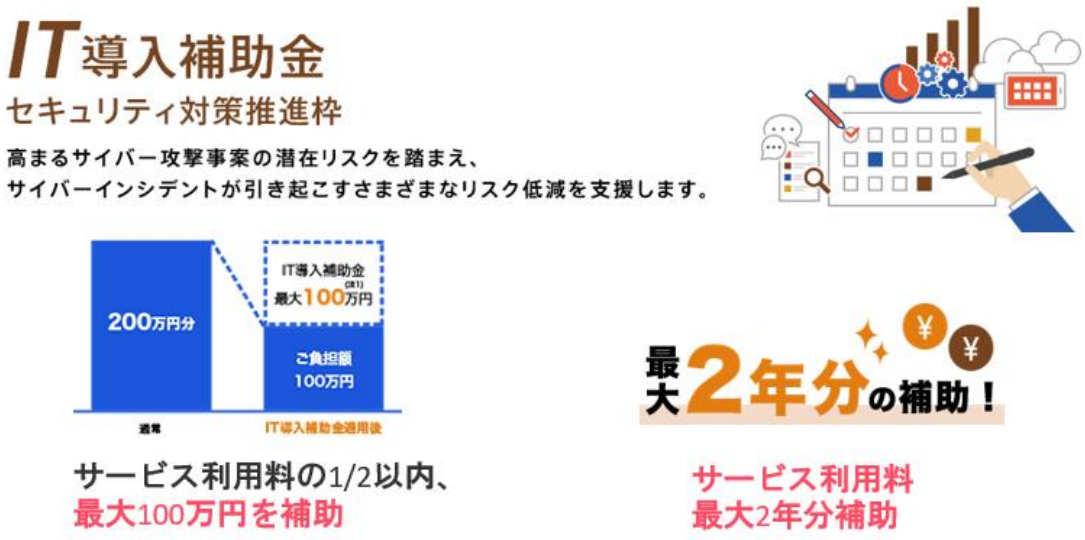
### 【参考】IT 導入補助金 2022 セキュリティ対策推進枠の紹介と申請手順

本補助金事業は、高まるサイバー攻撃事案の潜在リスクを踏まえ、サイバーインシデントが起き起こすさまざまなリスクの低減を支援するもの。

IT 導入補助金 2022 では、サイバーセキュリティお助け隊サービスのサービス利用料の 1/2 以内で最大 100 万円補助、サービス利用料最大 2 年分補助が受けられた。

但し、IPA が公表するサイバーセキュリティお助け隊サービスリストに掲載されているサービスのうち、IT 導入補助金事業において IT 導入支援事業者が提供し、かつ事務局に事前登録されたサービスであることが必要。（2023 年度事業では要確認）

（参 考）




※出典：中小企業庁ホームページ

本 IT 導入補助金を使ってサイバーセキュリティ対策実施を目指す中小企業に対しては、IT コーディネータが専門家として当該企業に見合ったサービスの選定支援を行うことが必要であり、以下に、企業が IT 導入補助金を申し込む際の申請と選定の手順例と留意点を示す。

**＜申請と選定の手順例＞**


サイバーセキュリティお助け隊サービスについては、IPA のホームページに詳しい記載がある。https://www.ipa.go.jp/security/otasuketai-pr/

1，IPA が公表する「サイバーセキュリティお助け隊サービスリスト」を確認する。
サービスリスト：https://www.ipa.go.jp/security/otasuketai-pr/index.html#service_title
2，支援機関（最寄りのよろず支援拠点、商工会、商工会議所）や IT コーディネータ等の専門家に経営課題や課題解決のための IT ツールを相談する。但し、この相談は必須ではなくご自身で直接 IT 導入支援事業者への連絡をすることも可能。
3，導入したい IT ツールを決定し IT 導入支援事業者に連絡をし、申請に必要な情報をヒアリングして申請を完了する。
4，審査を得て採択されればＩＴツールを導入・活用できる。
5，IT 導入補助金の申請にあたって（2022 年度の場合で 2023 年度は要確認）
「通常枠」及び「デジタル化基盤導入枠」において、オプションとして「サイバーセキュリティお助け隊サービス」をメインの IT ツールと組み合わせて申請することが可能。
「通常枠」及び「デジタル化基盤導入枠（デジタル化基盤導入類型)」については、オプションとして「サイバーセキュリティお助け隊サービス」を選定すると、補助事業者の採択にかかる審査において、加点対象となる。
また、新たに設置された「セキュリティ対策推進枠」では、「サイバーセキュリティお助け隊サービス」をメインの IT ツールとした申請(「サイバーセキュリティお助け隊サービス」単品での申請)が可能となる。

# 3．調査研究結果

## 3.1 調査対象サービスの選定

お助け隊サービスは、2021 年 3 月に 5 つのサービスが登録されて以降、順次追加され 2022 年 12 月末時点では【表 3-1】の通り 27 種類のサービスが登録されている。

※追記：2023 年 3 月に、6 事業者、8 種類のサービスが新たに追加された旨の発表があった。

| | サービス名（事業者名） |
|---|---|
| 1 | 商工会議所サイバーセキュリティお助け隊サービス（大阪商工会議所） |
| 2 | 防検サイバー（ＭＳ＆ＡＤインターリスク総研株式会社） |
| 3 | PCセキュリティみまもりパック（株式会社ＰＦＵ） |
| 4 | EDR運用監視サービス「ミハルとマモル」（株式会社AGEST） |
| 5 | SOMPO SHERIFF（ＳＯＭＰＯリスクマネジメント株式会社） |
| 6 | ランサムガード（株式会社アイティフォー） |
| 7 | オフィスSOCおうちSOC（富士ソフト株式会社） |
| 8 | セキュリティ見守りサービス「＆セキュリティ＋」（株式会社BCC） |
| 9 | CBM ネットワーク監視サービス（中部事務機株式会社） |
| 10 | 中部電力ミライズ　サイバー対策支援サービス（中部電力ミライズ株式会社） |
| 11 | ＣＳＰサイバーガード（セントラル警備保障株式会社） |
| 12 | PCお助けパック　PC定期侵害調査プラン（沖電グローバルシステムズ株式会社） |
| 13 | ネットワークセキュリティ見守り隊＆PCセキュリティ見守り隊サービス（株式会社コハマ） |
| 14 | マイセキュア ビジネス（NTTコミュニケーションズ株式会社） |
| 15 | セキュアエッジＭＤＲ９９（セキュアエッジ株式会社） |
| 16 | Cloud Edge運用支援EasySOC Plus パック（株式会社大塚商会） |
| 17 | アクロネットサイバーセキュリティサービス（株式会社アクロネット） |
| 18 | ビジネスサポートサービス（コスモテレコム株式会社） |
| 19 | TASKGUARD EDR WS セキュリティーサービス（京セラドキュメントソリューションズジャパン株式会社） |
| 20 | TASKGUARD UTM CP セキュリティーサービス（京セラドキュメントソリューションズジャパン株式会社） |
| 21 | MBSD Global Security Platform（略称：MGSP）（三井物産セキュアディレクション株式会社） |
| 22 | ラディックスお助け隊サービス（ラディックス株式会社） |
| 23 | MRⅡ Plus（株式会社テクノル）　2022年11月追加分は対象外とした |
| 24 | ネットワークセキュリティ見守り隊（株式会社コハマ） |
| 25 | ＹＯＮＪＩＭサイバーセキュリティ ＵＴＭ（株式会社四日市事務機センター） |
| 26 | ＹＯＮＪＩＭサイバーセキュリティ ＵＴＭ ＆ ＥＤＲ（株式会社四日市事務機センター） |
| 27 | TSOCエンドポイントパッケージ（株式会社ハイテックシステム） |

出典：IPA2022年度セキュリティプレゼンターカンファレンス資料より

【表 3-1】お助け隊サービスの一覧

この内、当チームの活動がスタートした 2022 年 7 月の段階で登録されていた 18 種類のサービスを調査対象として、以下の 2 点から絞り込みを行った。

① 千葉県をはじめ関東、全国地域をカバーしていること。

② 調査の情報源として、ホームページ等に内容の説明が掲載されていること。

その結果、【表 3-2】に示す 10 種類のサービスを取り上げることになり、分担して各サービスのホームページや問い合わせ先から情報収集を行った。

| 番号 | サービス名称 | 事業者名 | 再販協力会社/法人：数 | サービス対象地域 | 監視対象 | 調査担当 |
|---|---|---|---|---|---|---|
| 1 | 商工会議所サイバーセキュリティお助け隊サービス | 大阪商工会議所 | 商工会議所：6<br>株式会社：6 | 全国(離島など一部地域除く) | ネットワーク一括監視(UTM) | 松下 |
| 2 | 防検サイバー | MS＆ADインターリスク総研株式会社 | 株式会社：4 | 全国 | 端末監視(EDR) | 川名 |
| 3 | PCセキュリティみまもりパック | 株式会社PFU | 株式会社：75<br>有限会社：3<br>合同会社：1 | 全国 | 端末監視(EDR) | 田中 |
| 4 | EDR運用監視サービス「ミハルとマモル」 | 株式会社AGEST | - | 全国 | 端末監視(EDR) | 高山 |
| 5 | SOMPO SHERIFF | SOMPOリスクマネジメント株式会社 | - | 全国 | 端末監視(EDR) | 結城 |
| 6 | ランサムガード | 株式会社アイティフォー | 株式会社：2 | 全国(現時点では、関東、中部、関西、九州、沖縄県に限定) | 端末監視(EDR) | 松下 |
| 8 | セキュリティ見守りサービス「＆セキュリティ＋」 | 株式会社BCC | 株式会社：13 | 全国 | 併用 | 川名 |
| 11 | CSPサイバーガード | セントラル警備保障株式会社 | - | 東京･神奈川･千葉･埼玉<br>※順次全国に拡大予定 | ネットワーク一括監視(UTM) | 田中 |
| 14 | マイセキュア ビジネス | NTTコミュニケーションズ株式会社 | - | 全国 | 端末監視(EDR) | 高山 |
| 16 | Cloud Edge運用支援 EasySOC Plus パック | 株式会社大塚商会 | - | 北海道地方、東北地方、関東地方、中部地方、関西地方、中国地方、九州地方(一部地域を除く) ※順次全国に拡大予定 | ネットワーク一括監視(UTM) | 結城 |

【表 3-2】調査対象としたお助け隊サービスの一覧

### 3.2 調査項目の検討

調査に当たっては、中小企業等の立場になって、「自社にとって何が最適なサービスか」の視点から検討を行い、お助け隊サービスに求めることを以下にまとめた。

- ✓ 自社の情報システム環境(システム構成)において導入可能なこと
- ✓ 現在の情報ネットワークと事業/組織の状況から見て、急がれる対策であること
- ✓ 導入が容易で導入後も継続的に運用が可能なこと
- ✓ 必要な費用が妥当なものであること
- ✓ 保険によるリスク移転により、費用や責任の負担軽減が図れること

一方で、前章の通り、登録されているお助け隊サービスは、審査基準として挙げられている要件がすべて満たされていることから、それらの要件と照らし合わせて、更に具体的に掘り下げ、調査するサービスの比較項目を【表 3-3】に示す 5 項目とした。

お助け隊サービスの審査基準を踏まえた、具体的な比較項目

①. 自社の情報システムの環境や構成への適合性と優先度
*ハードウェア、ソフトウェアの使用条件や、導入にあたっての留意事項について

②.平常時の監視
*相談窓口の対応時間帯と、監視状況のフィードバック(情報提供)の内容について

③.異常発生時の対応
*異常検知時の通知の即時性と方法について
*緊急対応のサービス時間帯と支援内容について

④. 導入・運用の費用
*導入時の初期費用と運用時の年額換算費用について

⑤. 保険の適用範囲
* 駆付け対応以外も含めた、補償される対象と金額について

【表 3-3】お助け隊サービスの審査基準を踏まえた、具体的な比較項目

### 3.3 調査結果サマリー

調査に当たっては各サービスを共通の視点で比較するため、情報収集する際のワークシートを作成し、その調査結果をもとに 10 種類のサービスの一覧表を作成した。

詳細は添付ファイル(【別紙】調査資料：お助け隊サービス比較一覧表.xlsx)を参照いただくとして、この報告書では、「②.平常時の監視」、「③.異常発生時の対応」、「④.導入・運用の費用」、「⑤.保険の適用範囲」の 4 つの項目について、一覧表から見えたことをコメントすると共に、サービス内容とその有用性を比較してみた。

尚、比較項目「①.自社の情報システムの環境や構成への適合性と優先度」については、比較できる共通情報が端末の稼働環境(OS の種類)に限られるなど、得られた技術情報がまちまちで、企業規模やシステム構成面から企業への適合性をまとめて比較することが難しかった。

これについては、次章の「実証実験結果と考察（事例研究)」で、システムの環境や構成、企業の規模などを想定したモデルケースを設定し、最適と思われるサービスの選択肢としてまとめているので、そちらを参照していただきたい。

また、比較はあくまでも公表されている情報をもとにまとめたものであり、各サービスの優劣を評価したものではなく、また最新情報が正しく反映されているとは限らないことから、もし調査に不備や誤りがあった場合はご容赦いただきたい。

#### 1) 平常時の監視

平常時の重要な比較ポイントとして、相談窓口の対応時間帯と、監視状況のフィードバック(情報提供)の内容を取り上げて比較を行った。

その結果、相談窓口の対応時間帯に大きな差はなかったが、平日の日中時間帯に限られており、流通・サービス業界をはじめ、土日・祭日に情報システムを稼働している業種の企業は、相談対応の曜日が限られることに留意する必要がある。

また、サービス事業者からの定期的な状況報告に加え、利用者側の管理端末から、様々な情報を閲覧可能なサービスもあるが、企業側の担当者が日常の運用管理の中で、そのサービス機能を使いこなせるかの見極めも必要になる。

尚、【表 3-4】以降の比較表では、有用性が高いと思われるサービス内容に網掛けを行っている。

| 基準となる要件（全サービス対応） | サービス内容の詳細（比較のポイント） | 対応しているサービス | 不明/調査中 |
|---|---|---|---|
| ✓ 相談窓口設置 | ✓ 平日日中対応：電話、メール | ①、②、⑤、⑧、⑯ | ④、⑥、⑭ |
| | ✓ 休日・夜間対応：電話 | 無し | |
| ✓ 24時間監視 | ✓ 常時情報確認(レポート入手)可能 | ①、②、⑭、 | ③、⑪、⑧ |
| | ✓ 定期的報告(レポート)送付：日次 | 無し | |
| | ✓ 定期的報告(レポート)送付：週次 | ⑤、⑥ | |
| | ✓ 定期的報告(レポート)送付：月次 | ④、⑯ | |

| | 番号 | サービス名称 ※事業者名 |
|---|---|---|
| 端末 | ② | 防検サイバー ※MS＆AD |
| | ③ | PCセキュリティみまもりパック ※PFU |
| | ④ | ミハルとマモル ※AGEST |
| | ⑤ | SOMPO SHERIFF ※SOMPO |
| | ⑥ | ランサムガード ※アイティフォー |
| | ⑭ | マイセキュア ビジネス ※NTT Com |
| ネットワーク | ① | 商工会議所お助け隊サービス ※大阪商工会議所 |
| | ⑪ | CSPサイバーガード ※セントラル警備保障 |
| | ⑯ | Cloud Edge運用支援 ※大塚商会 |
| 併用 | ⑧ | セキュリティ＋ ※BCC |

【表 3-4】サービス内容の比較ポイント（平常時の監視）

### 2） 異常発生時の対応

異常時の重要な比較ポイントとして、異常検知時の通知の即時性とその方法や、緊急対応のサービス時間帯と支援内容を取り上げて比較を行った。

結果としては、【表 3-5】に示す通り、多くはメールやアプリによる即時通知を行っているが、中には通知に時間を要するものもあり、緊急対応のサービス時間帯も、平常時の監視のように全日 24 時間ものは少なかった。

尚、現場への駆け付けに要する時間(翌営業日等)と具体的な支援内容については、残念ながら詳細な情報が得られず、同条件での比較ができなかった。

一方で、2021 年 7 月に改定されたサービスの審査基準では、緊急時の対応支援として「リモートによる対応支援が可能な場合には，リモートによる対応支援も可とする」となったことから、異常発生現場が遠隔地の場合、現場への駆け付けよりも迅速な対応が図れることも想定でき、サービス選定における選択肢となり得る。

従って実際のサービス選定時には、自社の環境や緊急事態時の状況を具体的に想定(シミュレーション)して、最適な対応が取れるサービスを選択することが望まれる。

| 基準となる要件（全サービス対応） | サービス内容の詳細（比較のポイント） | 対応しているサービス | 不明/調査中 |
|---|---|---|---|
| ✓ 専門知識無くても導入運用できる工夫 | ✓ 自動メール通知：即時 | ①、⑤、③、⑪、⑭ | ④ |
| | ✓ 管理端末アラート表示：即時 | ②、⑤ | |
| | ✓ 自動メール通知：30分以内 | ⑥、⑧ | |
| | ✓ 自動メール通知：1日1回 | ⑯ | |
| | ✓ 検知時の窓口対応:24時間365日 | ②、③ | |
| ✓ 駆付けによる対応支援(リモート対応を含む) | ✓ 駆付け対応時間帯：24時間365日 | ②、⑥ | |
| | ✓ 駆付け対応時間帯：翌営業日以降 | ⑧ | |
| | ✓ 作業支援以上の対応：原因究明 | ①、② | |
| | ✓ 作業支援以上の対応：駆除、復旧 | ①、②、⑯ | |

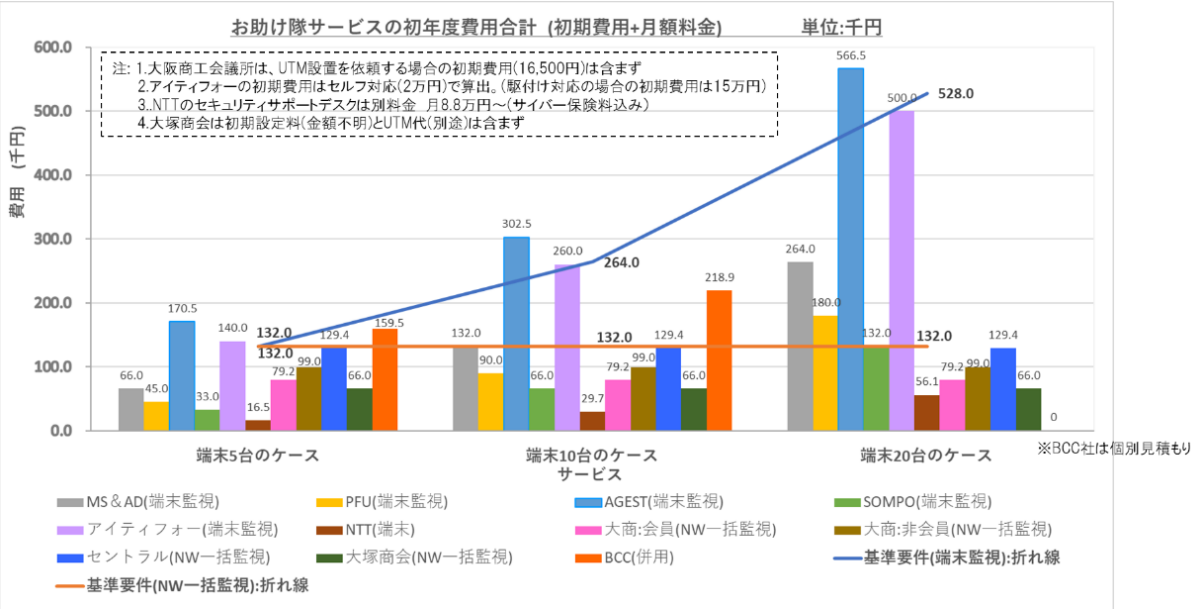
| | 番号 | サービス名称 ※事業者名 |
|---|---|---|
| 端末 | ② | 防検サイバー ※MS＆AD |
| | ③ | PCセキュリティみまもりパック ※PFU |
| | ④ | ミハルとマモル ※AGEST |
| | ⑤ | SOMPO SHERIFF ※SOMPO |
| | ⑥ | ランサムガード ※アイティフォー |
| | ⑭ | マイセキュア ビジネス ※NTT Com |
| ネットワーク | ① | 商工会議所お助け隊サービス ※大阪商工会議所 |
| | ⑪ | CSPサイバーガード ※セントラル警備保障 |
| | ⑯ | Cloud Edge運用支援 ※大塚商会 |
| 併用 | ⑧ | セキュリティ＋ ※BCC |

【表 3-5】サービス内容の比較ポイント（異常発生時の対応）

### 3） 導入・運用の費用

費用に関しては、端末監視型、ネットワーク監視型、併用型それぞれで基準が異なることから、端末台数を 5 台、10 台、20 台の 3 ケースを設定した上で、各サービスの導入時の初期費用と、運用時の年額換算費用との合計金額(初年度費用)を算出した。

また、目安としてサービスの審査基準で示されている金額をもとに、同様の合計金額(初年度費用)を算出し、各サービスと比較した。




【図 3-1】サービス内容の比較ポイント（導入・運用の費用）

結果を【図 3-1】のグラフで見ると、当然のことながら、端末監視型の費用は台数単位となるため、ネットワーク一括監視型と比べ高額になりやすく、特に初期導入費用がある一部のサービスでは、折れ線で示した基準要件の金額を飛び出ている。

但し全体で見ると、ほとんどのサービスは基準金額を下回っていることから、更に有用性を明確化するため、【表 3-6】での比較のポイントでは、初年度費用が基準要件の 60%以下となるサービスを網掛けしている。

尚、端末監視型において最安となる「マイセキュアビジネス」のサービスは、異常発生時のサポートが別料金のため、比較における取り扱いに注意が必要となる。

また端末とネットワークの両方の対策が必要な場合は、併用型のサービスも検討の対象となり、端末台数が 5 台、10 台の場合を見ると、いずれも基準金額(端末監視型＋ネットワーク一括監視型の合計金額)を下回る割安な選択肢となる。

※併用型での端末 20 台のケースは個別見積もりとなることから、金額比較ができなかった。

| 基準となる要件（全サービス対応） | サービス内容の詳細（比較のポイント） | 対応しているサービス | 不明/調査中 |
|---|---|---|---|
| ✓ ネットワーク一括監視型（月額1.1万円以下） | ✓ 年額換算費用が基準の60%以下 | ①、⑯ | |
| | ✓ 初期費用などの追加費用無し | ①、⑪ | |
| ✓ 端末監視型（月額2.2千円/台以下） | ✓ 年額換算費用が基準の60%以下 | ②、③、⑤、⑭ | |
| | ✓ 初期費用などの追加費用無し | ②、③、⑤ | |
| ✓ 併用型（上記の和を超えないこと） | ✓ 年額換算費用が基準の60%以下 | ⑧ | |
| | ✓ 初期費用などの追加費用無し | | |

| | 番号 | サービス名称 ※事業者名 |
|---|---|---|
| 端末 | ② | 防検サイバー ※MS＆AD |
| | ③ | PCセキュリティみまもりパック ※PFU |
| | ④ | ミハルとマモル ※AGEST |
| | ⑤ | SOMPO SHERIFF ※SOMPO |
| | ⑥ | ランサムガード ※アイティフォー |
| | ⑭ | マイセキュア ビジネス ※NTT Com |
| ネットワーク | ① | 商工会議所お助け隊サービス ※大阪商工会議所 |
| | ⑪ | CSPサイバーガード ※セントラル警備保障 |
| | ⑯ | Cloud Edge運用支援 ※大塚商会 |
| 併用 | ⑧ | セキュリティ＋ ※BCC |

【表 3-6】サービス内容の比較ポイント（導入・運用の費用）

### 4） 保険の適用範囲

リスク移転の対策となる保険については、【表 3-7】に示す通り、補償金額に大きな差が見られ、特に端末監視サービスの多くに、駆付け対応の費用だけでなく損害賠償費用の保障が付加されているのが目立った特徴と言える。

個人情報が漏洩した際の損害賠償など有用性が高いように思えるが、当然ながらランサムウェア感染による身代金は補償の対象にはならない。

また補償される駆付け対応費用は、駆け付ける要員の人件費と交通費だけなのか、以下の事故対応費用が一部でも含まれているのかなど、詳細な適用条件を十分に理解しておくことが必要である。

※事故対応費用：事故原因調査費用、サーバー復旧作業、再発防止策費用、法律相談費用など、様々な費用が想定される。

| 基準となる要件（全サービス対応） | サービス内容の詳細（比較のポイント） | 対応しているサービス | 不明/調査中 |
|---|---|---|---|
| ✓ 駆付け費用等を補償<br>※駆付け費用と損害賠償を合わせた上限金額 | ✓ 損害賠償も補償の対象とする | ②、③、④、⑥、⑭ | |
| | ✓ 補償金額の上限：20万円/年まで | ⑧ | |
| | ✓ 補償金額の上限：30万円/年まで | ①、⑪ | |
| | ✓ 補償金額の上限：40万円/年まで | ⑯ | |
| | ✓ 補償金額の上限：100万円/年まで | ⑤ | |
| | ✓ 補償金額の上限：200万円/年まで | ③、④ | |
| | ✓ 補償金額の上限：300万円/年まで | ⑥ 損害賠償も補償の対象としているサービスは補償金額の上限も高い。 | |
| | ✓ 補償金額の上限：600万円/年まで | ②、⑭キャンペーン期間（2023年8月）限定 | |

| | 番号 | サービス名称 ※事業者名 |
|---|---|---|
| 端末 | ② | 防検サイバー ※MS＆AD |
| | ③ | PCセキュリティみまもりパック ※PFU |
| | ④ | ミハルとマモル ※AGEST |
| | ⑤ | SOMPO SHERIFF ※SOMPO |
| | ⑥ | ランサムガード ※アイティフォー |
| | ⑭ | マイセキュア ビジネス ※NTT Com |
| ネットワーク | ① | 商工会議所お助け隊サービス ※大阪商工会議所 |
| | ⑪ | CSPサイバーガード ※セントラル警備保障 |
| | ⑯ | Cloud Edge運用支援 ※大塚商会 |
| 併用 | ⑧ | セキュリティ＋ ※BCC |

【表 3-7】サービス内容の比較ポイント（保険の適用範囲）

### 3.4 調査結果のまとめ（サービス選定の考え方）

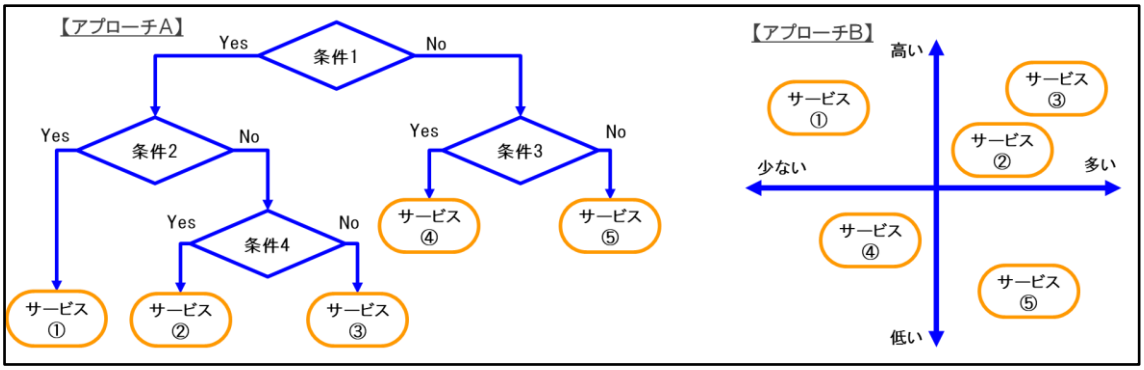
改めて、ここまでの 4 つの比較ポイントを整理してみると、すべての項目で突出して有用性が高く、「このサービスを選んでおけば間違いがいない」ベストなサービスは見当たらなかった。

一方で、「結局どのサービスを選択したら良いんだ」という質問に、テーマ研究として何等かの結論を出すことが必要と考え、どのようなまとめ方がよいか検討した。

検討に当たっては、当初この種の比較でよく用いられる【図 3-2】に示すような 2 つのアプローチを試みたが、比較の要素が多元的であり、また Web により提供される情報が、均一なレベルで収集できなかったことから、いずれも断念した。

アプローチＡ：求めるサービスの要件(条件)を順に選んでいく中で、該当するサービスが枝分かれし、最終的に最適なサービスに至るアプローチ

アプローチＢ：2 つの異なる比較ポイントを縦・横軸の 4 象限の分布図で示し、最適なものを選択するアプローチ




【図 3-2】サービス内容の比較ポイント（導入・運用の費用）

このような検討を経た上で、中小企業等にとっての最適なサービスの選択方法を、改めて以下の 2 点から整理し【表 3-8】にまとめた。

① 中小企業等のニーズや置かれた状況により最適な選択肢は異なることを踏まえ、代表的なケースを 3 通り想定する。

ケースＡ：自社の要員での対応が難しく、ある程度の費用を掛けても対応を任せられるサービスを選択したい。

ケースＢ：即時通知と的確な情報があれば、ある程度自社で対応できるので、作業支援レベルの費用が安いサービスを選択したい。

ケースＣ：最小限の費用で対応できるサービスを選択したい。万一の事故発生時の対応費用は、その時に判断する。

② 4 つの比較ポイントの中で、「異常発生時の対応」と「導入・運用の費用」を最重視する。

| | 企業のニーズや置かれた状況 | 監視対象 | | 選択サービス ※事業者名 | 選択理由 |
|---|---|---|---|---|---|
| A | 自社の要員での対応が難しく、ある程度の費用を掛けても対応を任せられるサービスを選択したい。 | 端末監視 | ② | 防検サイバー<br>※MS＆AD | ✓ 即時通知が管理端末へのアラート表示のみだが、検知時の窓口や駆付けのサービスが24時間365日対応であり、原因究明から復旧までを任せられる。<br>✓ 費用も基準の60%以下と割安感がある。 |
| | | ネットワーク一括監視 | ① | 商工会議所お助け隊サービス<br>※大阪商工会議所 | ✓ 異常発生時にメールで即時通知があり、駆付けサービスでも原因究明から復旧までを任せられる。<br>✓ 費用も会員企業であれば基準の60%程度と低額。 |
| B | 即時通知と的確な情報があれば、ある程度自社で対応できるので、作業支援レベルの費用が安いサービスを選択したい | 端末監視 | ⑤ | SOMPO SHERIFF<br>※SOMPO | ✓ 端末監視では費用が2番目に安い。<br>✓ 駆付けサービスは作業支援に限られるが、異常発生時はメールと管理端末の両方に即時通知あり。 |
| | | ネットワーク一括監視 | ① | 商工会議所お助け隊サービス<br>※大阪商工会議所 | ✓ このケースでも、他の⑪、⑯と比べ有利性が高い。<br>✓ ⑯のサービスは、初期設定料とUTM代の金額が不明なことから、必ずしも最安とは言えない。 |
| C | 最小限の費用で対応できるサービスを選択したい。万一の事故発生時の対応費用は、その時に判断する。 | 端末監視 | ⑭ | マイセキュア ビジネス<br>※NTT Com | ✓ 万一異常が発生した際のサービスは別途有料となるが、費用負担を最少に抑えたい企業が、何等かの監視対策を取りたい場合の選択肢になる。 |

【表 3-8】企業のニーズや置かれた状況を踏まえた最適なサービスの選択例

今回は、限られた 10 種類のサービスの中からの選択を試みたが、他のお助け隊サービスについても、今後得られる情報量が増え、またサポート地域も全国レベルに拡大されてくれれば、同様に前述の「4 つの比較ポイント」と上記の「中小企業等の視点での 3 ケース」で比較・評価できればと思う。

尚、個々の企業が実際にサービスを選択する際には、情報システムの環境や構成面で制約が無いかなど、技術面からのクロスチェックを行った上で最終判断することが必須であり、次章の実証実験の事例を併せて参考に願いたい。

# 4．実証実験結果と考察（事例研究）

情報セキュリティ対策を支援中の中小企業に対してお助け隊サービスの利用を提案した事例を考察とともに紹介する。

## 4.1 事例 1（ネットワーク一括監視型の事例）

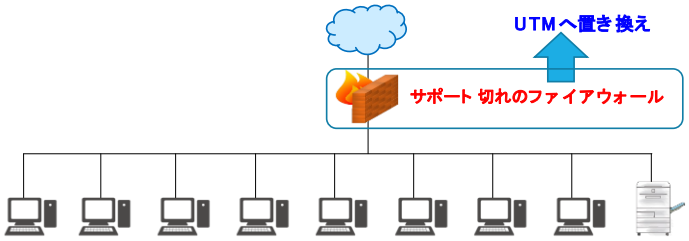
【企業の状況】

| | |
|---|---|
| 業種 | ：製造業 |
| 拠点数 | ：1 箇所 |
| PC 台数と OS | ：8 台（Windows 10, Windows 11） |
| プリンタ台数 | ：1 台 |
| PC の持ち出し | ：なし |
| ウイルス対策ソフト | ：導入済み |
| ネットワーク対策 | ：ファイアウォールを設置しているが、サポート切れ |
| 外部から社内への接続 | ：なし |
| 万が一の際の対応 | ：社内に対応できる人はいないが、頼める IT ベンダーがある |

【提案したサービス】

商工会議所サイバーセキュリティお助け隊サービス（大阪商工会議所）

【選定理由】




利用しているファイアウォールのサポートが切れており、機器故障による通信障害が発生するリスクがある。このことから、ファイアウォールの新機種への移行が必要であると判断した。そこで、UTM へ置き換えることで、ネットワーク対策のレベルを上げることにした。表 3-8 で最適と判断した上記サービスを提案した。

【企業での検討結果】

お助け隊サービスでは、万が一の際の対応に対応範囲に制限が出る可能性があると考え、社内の IT 環境を一括して見てもらっている IT ベンダーが提供する UTM（駆け付け対応あり）を利用することにされた。損害賠償の補償はないが、取り扱っている情報の重要度から損害賠償の可能性は低いと判断された。

### 4.2 事例 2（端末監視型の事例）

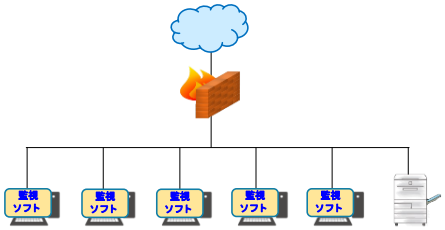
【企業の状況】

| | |
|---|---|
| 業種 | ：製造業 |
| 拠点数 | ：1 箇所 |
| PC 台数と OS | ：5 台（Windows XP, Windows 10, Windows 11） |
| プリンタ台数 | ：1 台 |
| PC の持ち出し | ：なし |
| ウイルス対策ソフト | ：導入済み |
| ネットワーク対策 | ：ファイアウォールを設置ずみで、サポート期間中 |
| 外部から社内への接続 | ：なし |
| 万が一の際の対応 | ：社内に対応できる人はいないが、頼める IT ベンダーがある |

【提案したサービス】

マイセキュア ビジネス（NTT コミュニケーションズ株式会社）

【選定理由】




利用しているアプリケーションの関係で Windows XP を使用せざるを得ない状況である。Windows XP をネットワーク分離することを検討したが、Windows XP からも印刷できる必要があり、分離には相当の費用がかかることが判明した。

そこで Windows XP をサポートしているサービスを探したところ、上記のサービスだけが対応していた。

【導入結果】

本事例では提案したサービスを導入されたが、導入にあたって以下のような問題があった。

- 導入手順書が、IT に詳しくない人にはわかりにくく、インストールに手助けが必要
- 保険のキャンペーン登録がサービス開始の案内等にはなく、サービスを選定した者でないとキャンペーンがあることに気づかない
- キャンペーン登録には MAC アドレスが必要だが、入力時は区切り記号を取ることの説明がない
- MAC アドレスの確認方法の説明に、サポート対象の Windows XP の記載がない
- インストールでエラーが発生した際問い合わせフォームでは画面のキャプチャを登録できず、折り返しの連絡を待たなければいけない

### 4.3 事例 3（端末監視型の事例）

【企業の状況】

| | |
|---|---|
| 業種 | ：製造業 |
| 拠点数 | ：5 箇所（在宅を含む） |
| PC 台数と OS | ：20 台（Windows 10, Windows 11） |
| プリンタ台数 | ：5 台 |
| PC の持ち出し | ：あり |
| ウイルス対策ソフト | ：導入済み |
| ネットワーク対策 | ：ファイアウォールを設置していない |
| 外部から社内への接続 | ：なし |
| 万が一の際の対応 | ：社内に対応できる人はいなく、頼める IT ベンダーもない |

【提案したサービス】

防検サイバー（MS＆AD インターリスク総研株式会社）　または
マイセキュア ビジネス（NTT コミュニケーションズ株式会社）

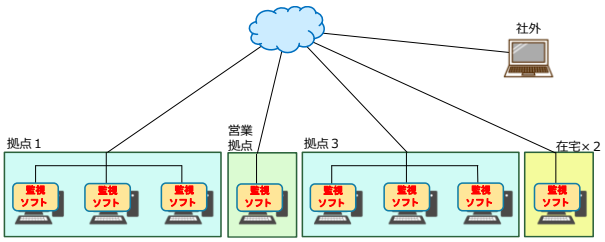
【選定理由】

ネットワーク一括監視型を利用すると、UTM の設置箇所が複数になり費用が嵩む。また、社員の自宅に設置するのは困難である。さらに、社外へ持ち出している間の対策はできない。

そこで、端末監視型のサービスを提案することにした。万が一の際に対応できる人が社内にいないことから、表 3-8 の類型 A に該当することから「防検サイバー」を提案した。ただし、他にも対策が必要な事項があったため、費用を抑える場合の対策として類型 C の「マイセキュア ビジネス」もあわせて提案した。

【企業での検討結果】

他の対策を優先させるため、お助け隊サービスの利用については、継続検討事項とされた。




【その他】

小規模事業者では、ウイルス対策ソフトはクライアント型であり、管理サーバーが導入されていないケースが多い。この状況で端末監視型サービスを導入した場合、ウイルスは一括監視されないがマルウエアは一括監視される状況が発生する。このことから、ウイルスを含めて一括監視されるサービスが望ましいと感じた。

# おわりに

中小企業等の立場に立ち、「お助け隊サービス」を技術面のみならず費用や使い易さなど様々な切り口で評価し、分かりやすく紹介したいという思いをもって調査研究を進めてきた。しかし、本報告書は様々な意味において通過点に過ぎない。

「お助け隊サービス」は、2023 年 2 月末時点で 35 種類のサービスが登録されており、「お助け隊サービス基準」も基準の明確化のため 2023 年 4 月に改訂が予定されている。

したがって本報告書の内容も、今後、新たな情報に基づいた改訂が必要であり、中小企業等への更に分かりやすい説明のために、導入事例の追加等も必要だと考えている。

また、IPA においては、「お助け隊サービス」に関する、より詳しい情報の紹介や一覧表での整理・分析が公開されてきており、利用者が最適なサービスを選択できるための検討が着実に進められている。

われわれはＩＴコーディネータとして、中小企業等に寄り添ったサイバーセキュリティ対策を進めるため、今一度、現場感覚を研ぎ澄まし、経営者が、経営の視点から最も適切なサービスの選択を行えるために、より分かりやすい選択肢や参考になる事例を提供できるよう、更に弛みない研鑽を積んでいきたい。

・研究メンバー（役割・氏名・関係保有資格）

- リーダー　　：松下正夫（情報セキュリティ内部監査人）
- サブリーダー：川名正幸（システム監査技術者、公認システム監査人）
- サブリーダー：田中孝典（情報処理安全確保支援士、システム監査技術者 ）
- メンバー　　：高山和子（税理士、行政書士）
- メンバー　　：結城健一（システム監査技術者、公認情報システム監査人（CISA））

本報告書は各項をメンバーで分担して執筆した。