特定非営利活動法人
ITCちば経営応援隊

【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～

２０２４年3月２３日

特定非営利活動法人 ITC ちば応援隊

2023 テーマ研究 チーム

＜目次＞

はじめに

１.テーマ選定の背景と本研究の目的

２.サイバーセキュリティお助け隊サービスとは

３.調査研究結果

４.実証実験結果と考察（事例研究）

おわりに

・別紙：調査資料「お助け隊サービス比較一覧表 2023」

【研究メンバー（役割・氏名・関係保有資格)】

- リーダー　　：松下正夫（ITC、情報セキュリティ内部監査人）
- サブリーダー：川名正幸（ITC、システム監査技術者、公認システム監査人）
- メンバー　　：高山和子（ITC、税理士、行政書士）
- メンバー　　：田島彰二（ITC、PMP、ITIL(F)、電気通信主任技術者）
- メンバー　　：木村 敦 （ITC、iCDコンサルタント、PMP、ｼｯｸｽｼｸﾞﾏ･ﾌﾞﾗｯｸﾍﾞﾙﾄ）
- メンバー　　：鈴木克彦（ITC、厚労省認定ITマスター、スマートSMEサポーター）

本報告書は各項を上記メンバーで分担して執筆した。

はじめに

ITC ちば経営応援隊では、昨年度に引き続き、IPA が公開する「サイバーセキュリティお助け隊サービス」の調査・分析・評価を研究テーマと定めて活動を実施した。

今年度の研究対象は、2024 年 1 月 16 日時点で IPA ホームページに公開されていた 55 サービスの内、基本的にサービスが全国で展開され詳細な情報が提供者のホームページ等で公開されている 30 のサービスとし、昨年度調査した 10 サービスに加え新たに 20 サービスを調査対象範囲に加えて実施することとした。

昨年度は、「最適なサービスの選択肢」に至るアプローチとして、企業環境やニーズに関して典型的な３つのケースを想定し、各ケースでの最適なサービスを選定し明示することができたが、個々の企業のケースにおいてより客観的な選択肢の提示ができないかという課題を残すこととなった。

今年度は、これらの課題を解決するため、以下の２つのアプローチを試行した。

１つ目は、各サービス評価基準の数値化である。お助け隊サービスは一定の基準を満たしたサービスであるが、特に中小・小規模事業者ユーザーにとって重要と思われるサービス要素の評価基準を設定し、各サービスの「更なる付加価値」として数値化することとした。

２つ目は、個別企業へのサービス候補選択の提案や経営者とのディスカッションに際し、企業の環境や経営者のニーズを反映する方法として、評価項目に「個別企業の重みづけ」をできるようにしたこと。例えば、とにかく価格重視という経営者の場合は、価格項目に２倍の重みづけを、万一の事故の際の補償重視の経営者の場合は保険項目に２倍の重みづけする、といった運用ができるようにした。

以上のように２年間通じて本テーマに関する研究を進めた結果、お助け隊サービスの選択に際して、専門家や支援機関担当者と経営者や IT 責任者がひざを交えてディスカッションするための一つのアプローチ方法を整理することができたと考えている。

それが具体的にどのような内容なのか、実際に現場で使えるものなのか等については、是非、読者の皆様に評価して頂き忌憚のないコメントを頂ければと思う。

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 1345 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。

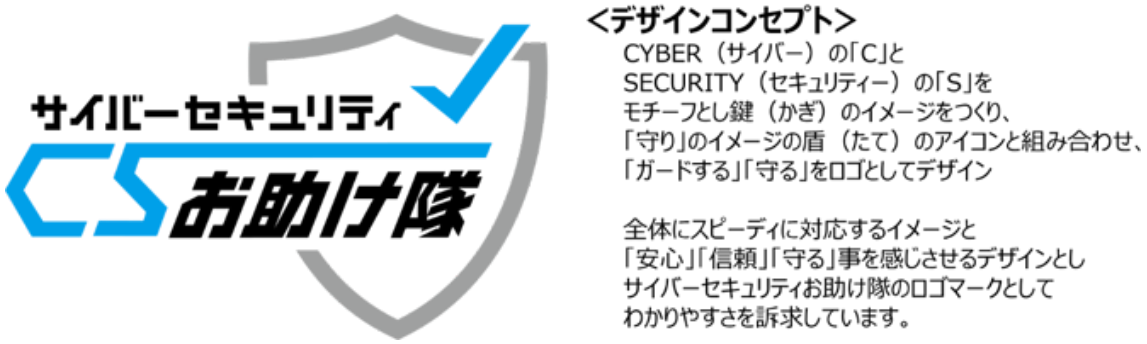
主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク及び／又は端末を**24時間見守る仕組み**を提供
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・運用できる簡単さ	**専門知識がなくても導入・運用できるような工夫**
簡易サイバー保険	突発的に発生する駆付け費用等を補償する**サイバー保険**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）** ・併用型：**これらの和に相当する価格を超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

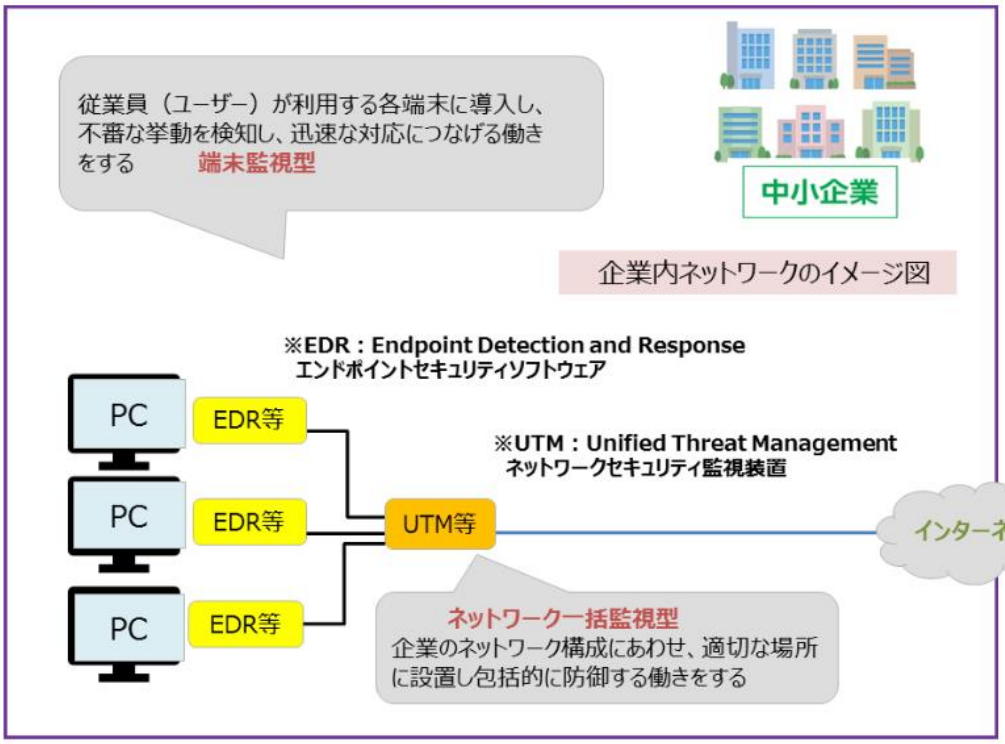
企業のネットワーク構成に合わせて適切な場所に設置しネットワークを包括的に防御する働きをし、事務所の中でネットにつながっている端末すべてを監視する。

※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

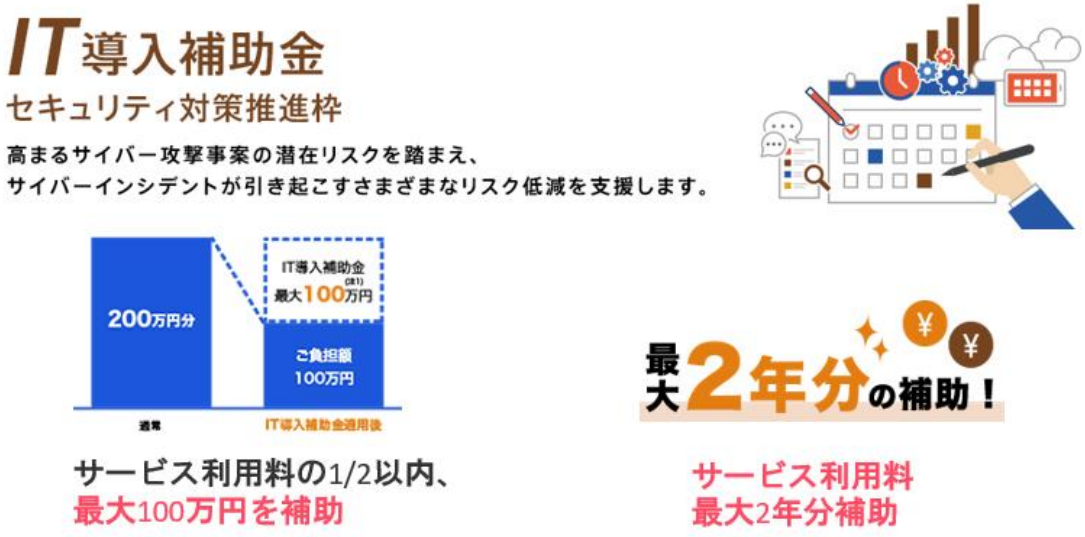
・支援機関（最寄りのよろず支援拠点、商工会議所、商工会）や専門家（IT コーディネータ等）を活用する。
・直接ＩＴ導入事業者に連絡することも可能だが、支援機関や信頼できる専門家を利用して必要なセキュリティを相談しながらの導入が望ましい。
・この機会を利用して、社内で IPA が推進する SECURUTY ACTION（中小企業の自己宣言）等を利用し、社内でのセキュリティ知識を向上することも必要である。

【参考】IT 導入補助金 2024 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、サイバー攻撃の増加に伴う潜在的なリスクに対処するため、サイバーインシデントに関する様々なリスク低減策を支援。IT 導入補助金 2024 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５万円以上100万円以下を1/2以内補助、IT ツールの導入費用及び、サービス利用料の最大２年分補助が受けられる。

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。

（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 2024 の申請（令和 5 年度補正サービス等生産性向上 IT 導入支援事業の場合）については、以下のサイトから確認できる。

IT導入補助金2024

⇒ https://it-shien.smrj.go.jp/

「通常枠」をはじめとして、「セキュリティ対策推進枠」など 5 つの枠があるので、自社の目的に合致した「枠」の補助金サービスを選択して申請する。

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 2023 年 12 月末時点では 55 のサービスが登録されている。

参照 URL : https://www.ipa.go.jp/security/sme/otasuketai-about.html

テーマ研究では、これらのサービスについて以下の 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 3-1 に示す 29 のサービスを調査の対象とした。

連番	登録番号	サービス名称	事業者名	監視対象	調査担当
2	2020-002	防検サイバー	MS＆ADインターリスク総研株式会社	端末	川名
3	2020-003	PCセキュリティみまもりパック	株式会社PFU	端末	田中
4	2020-004	EDR運用監視サービス「ミハルとマモル」	株式会社AGEST	端末	高山
5	2020-005	SOMPO SHERIFF	SOMPOリスクマネジメント株式会社	端末	川名
6	2021-001	ランサムガード	株式会社アイティフォー	端末	松下
9	2022-002	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	端末	高山
10	2022-003	セキュアエッジMDR99	セキュアエッジ株式会社	端末	松下
12	2022-005	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	端末	川名
13	2022-007	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	端末	田中
15	2022-009	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	端末	高山
18	2022-018	AXIS総合セキュリティパック（端末監視コース）	株式会社アクシス	端末	田島
20	2022-020	データお守り隊	株式会社アクト	端末	木村
21	2022-022	SecurityFREEレスキュー隊 for PC監視	株式会社ソフトクリエイト	端末	鈴木
22	2023-001	サイバープロテクション（CP）	株式会社ブロードバンドセキュリティ	端末	木村
連番	**登録番号**	**サービス名称**	**事業者名**	**監視対象**	**調査担当**
1	2020-001	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	ネットワーク	松下
8	2021-006	CSPサイバーガード	セントラル警備保障株式会社	ネットワーク	田中
11	2022-004	Cloud Edge運用支援 EasySOC Plus パック	株式会社大塚商会	ネットワーク	田中
14	2022-008	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	ネットワーク	田中
19	2022-019	beat/solo 見守りサービス	富士フイルムビジネスイノベーションジャパン株式会社	ネットワーク	田中
23	2023-007	セキュリティお助けパック（ネットワーク）	バリオセキュア株式会社	ネットワーク	鈴木
25	2023-013	スマートセキュリティ	株式会社ビープラス	ネットワーク	松下
26	2023-017	おまかせサイバーみまもり(Lightプラン)	東日本電信電話株式会社	ネットワーク	川名
27	2023-018	おまかせサイバーみまもり(Standardプラン)	東日本電信電話株式会社	ネットワーク	川名
連番	**登録番号**	**サービス名称**	**事業者名**	**監視対象**	**調査担当**
7	2021-003	セキュリティ見守りサービス「＆セキュリティ＋」	株式会社BCC	併用	川名
16	2022-016	AXIS総合セキュリティパック（ネットワーク＆端末監視コース）	株式会社アクシス	併用	田島
17	2022-017	AXIS総合セキュリティパック（小規模ネットワーク＆端末監視コース）	株式会社アクシス	併用	田島
24	2023-008	セキュリティお助けパック（ネットワーク）	バリオセキュア株式会社	併用	鈴木
28	2023-019	おまかせサイバーみまもり(Lightプラン) おまかせアンチウイルスEDRプラス	東日本電信電話株式会社	併用	川名
29	2023-020	おまかせサイバーみまもり(Standardプラン) おまかせアンチウイルスEDRプラス	東日本電信電話株式会社	併用	川名

【表 3-1】調査対象としたお助け隊サービスの一覧（監視対象別）

3.2 調査項目の検討

当調査は昨年度に続き 2 回目となるが、昨年のまとめにおいては、最適なサービスの選択として【表 3-2】に示すように、3 ケースを想定した選択肢に留まり、点数等の数値化による分かりやすい評価をまとめるには至らなかった。

	企業の環境やニーズ
A	社内に対応できる人間がいないので、ある程度の費用が掛かっても、しっかり任せられるサービスを選択したい。
B	ある程度は自社で対応できるので、費用の安さを重要視し、サービスの内容は即時通知さえあれば、作業支援のレベルでよい。
C	費用最優先で、最安金額のサービスを選択したい。万一の異常発生時には、別途有料サービスで対応してもよい。

【表 3-2】昨年度のテーマ研究における最適なサービスの選択肢

今回の調査に当たっては、この点を課題とし、何等かの数値化(点数化)による比較を行うことを目標とし、以下の考え方とアプローチですすめることとした。

[考え方とアプローチ]

- ✓ 数値化に当たっては、比較の基準を明確にし、主観による偏りをできる限り減らすことで、客観性を高める。
- ✓ 数値化の意味を、お助け隊サービスの最低要件は満たした上での、更なる付加価値部分と位置付ける。
- ✓ 各自が調査したサービスの内容を、「評価ワークシート」を用いて、テーマ研究会としての付加価値点数付けを行う。
- ✓ 上記のテーマ研究会の点数評価に、企業ごとの環境やニーズを反映した重みづけを行い、個別企業としての点数評価が可能なワークシートとする。
- ✓ 企業の経営者や IT 担当者との間で、各企業の環境やニーズの把握を行ったうえで、個別企業の点数評価がされたワークシートを作成し、提案やディスカッションの参考資料として活用する。

尚、各サービスの調査内容については、前回からの継続性を考慮し変更しないものの、これまで参考程度に見ていた 2 つの視点を新たに追加し、以下の 7 項目とした。

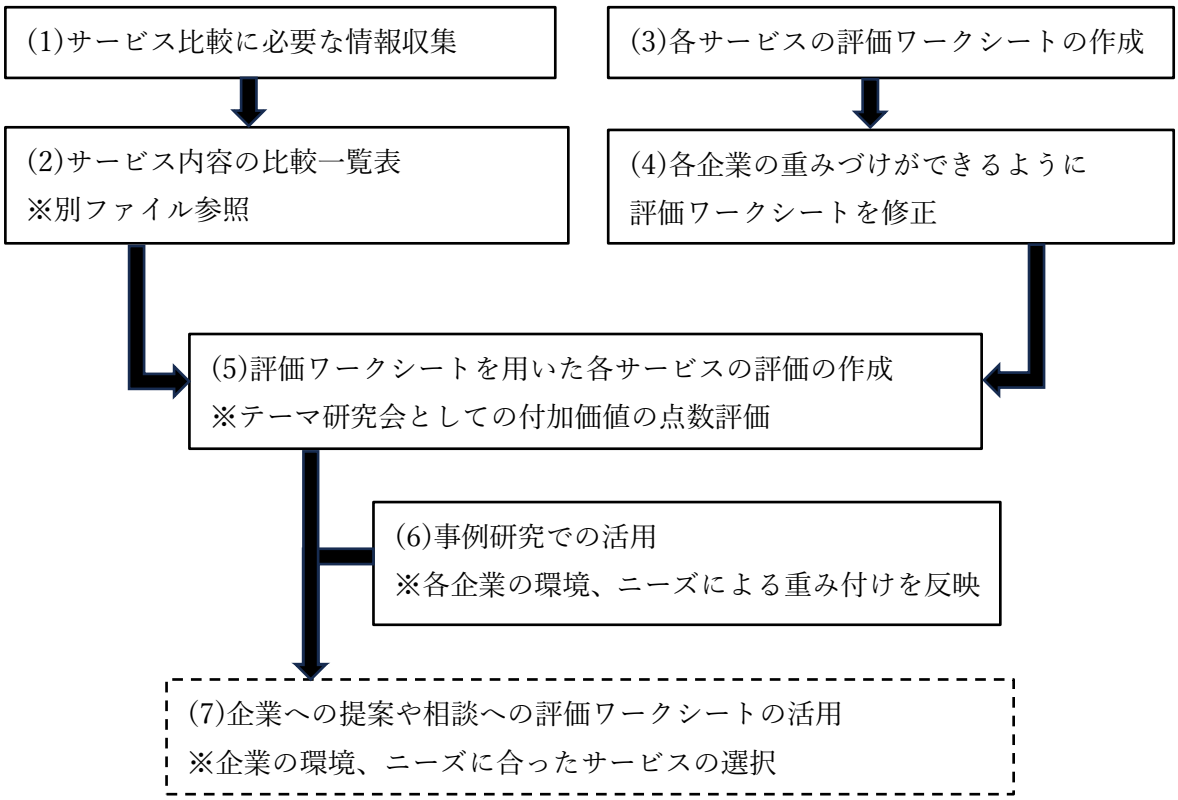
【評価項目】

①. サービス提供力 **<追加>**
②. 既存システムへの影響（システムの環境や構成への適合性）
③. 平常時の対応レベル
④. 異常発生時の対応家レベル
⑤. 費用一式
⑥. 保険
⑦. 導入実績 **<追加>**

3.3 調査結果サマリー

前述の「考え方とアプローチ」に従い、以下の図 3-1 に示す流れで、調査から評価を行った。

以下に、順を追ってその内容と評価結果を説明する。尚、「(6)事例研究での活用」については次章で述べる。



【図 3-1】調査と評価の進め方

3.3.1. サービス比較に必要な情報収集と比較一覧表の作成

情報収集は、IPA の Web ページの情報に加えて、対象サービスの Web ページに掲載されている情報を中心に行ったが、サービス提供会社により公開されている情報にバラツキが大きく、比較一覧表を埋めるために問い合わせ窓口に電話するなど、可能な限りの情報入手を試みた。問い合わせにおいては、情報収集の目的を伝え、直接のビジネス案件に結びつくものでないものの情報提供に協力いただき、我々の質問にも丁寧に受け答えをしていただくことが多かった。

尚、昨年度調査対象としたサービスについても、その後の変更点が無いかを含め再度調査し、販売代理店や実績の増加など、更新された情報を一覧表に反映した。

収集した情報は、昨年度と同じフォームを用いて比較一覧表を作成し、分析のための基本情報とした。

3.3.2 評価ワークシートの作成

今年度の活動の中で、最も検討を要したのは、「数値による(より可視化された)分かりやすい比較」という課題について、評価の基準と用いる共通ツール(ワークシート)を考えることであった。

特に配慮したのは、評価において、各自の主観をできるだけ減らした客観的評価とするための工夫であり、各評価項目について、「付加価値があると認める評価基準」と「評価基準とした理由」を明確にした。

評価項目		評価基準
1	サービス提供力	サービス対象地域として全国の主要都市をカバーしている。
		自社の拠点だけでなく、販売代理店など顧客との接点(相談窓口)を増やして、サービスのサポート体制を整えている。
2	既存システムへの影響	【端末型(EDR)】 以下の3点から既存の端末構成に対する制約が少なく、幅広い端末で利用可能。 ①.Windows以外の端末(MAC, Linux)もサポート対象としている。 ②.現在サポート対象外の旧バージョンもサポート対象としている。 ③.PCに導入済みのウイルス対策ソフトとコンフリクトしない。
		【ネットワーク型(UTM)】 ①.既存のシステム(ネットワーク)環境に影響を与えずに導入でき、機能を補完し合って使える。 ②.システム(ネットワーク)環境に修正を要しても、既存の機器が不要となり、コストを削減(抑制)できる。
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。
		定期的報告(レポートやメール)が週次に送付される。
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。
		駆け付け対応の時間帯が24時間365日可能である。
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※ネットワーク一括監視型:月額1.1万円以下 ※端末監視型:月額2.2千円/台以下 ※併用型:上記の和を超えないこと
		初期費用などの追加費用がない。
6	保険	損害賠償も補償の対象となっている。
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。
		補償金額の上限が200万円/年以上である。
7	導入実績	使用されているUTM機器やEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。

【表 3-3】評価項目の評価基準

評価項目		評価基準とした理由
1	サービス提供力	工場や事業所などが離れた地域にある場合を想定し、全国の主要都市をサービス対象としていることを評価の対象とした。
		販売代理店を含めた拠点数が多いことが、顧客がお助け隊サービスについての身近な相談窓口を見つけることに繋がり、サービスの提供力の一つとして評価基準に加えた。
2	既存システムへの影響	既存のPC環境を変更せずにサービスが利用可能なことは、企業にとって有効な選択肢となることから、左記の評価基準の3項目を評価基準とした。
		ファイアウォール等の機器を既に導入済みの企業においても、更に境界防御の機能強化やコスト削減(抑制)を図れる視点から、左記の2点の評価基準を設定した。
3	平常時の対応レベル	企業側に担当できる要員や体制がある場合や、気になる事象があった場合に、何時でも状況を確認できるという視点から、評価基準とした。
		企業側が日常の管理負荷を掛けなくても、サービス提供側から定期的な状況報告が欲しいという視点で、「最低週次」を目安として評価基準に加えた。
4	異常発生時の対応レベル	異常検知時の初動対応スピードの重要性から、評価基準に加えた。
		同上。特に異常発生時に、何時でも相談窓口が開いていることは、専門家がいない中小企業にとっては有用な評価基準となる。
		駆け付けサービス自体は、お助け隊サービスの基本要件なので、あるだけでは特別の加点要素にはならない。また、お助け隊サービスの要件としては「リモート対応も可」としているものの、何時でも駆け付けてくれる安心感は、重要な評価ポイントと言える。(追加費用の有無は問わない)
		スキル等の面で対応要員がいない中小企業にとって、復旧までの支援は有用性が高く、評価基準に加える。(追加費用の有無は問わない)
5	費用一式	年額換算費用が、IPAが定めるお助け隊サービスの要件(基準)の金額から40%以上低いことを評価基準とする。
		利用に当たって必須となる初期費用などの追加費用がない点を評価基準に加える。 ※選択理由の重要ポイントであることから、配分点数を10点とする。
6	保険	セキュリティ事故における損害賠償費用は中小企業にとって大きな負担となることから、有効な補償機能であり、評価基準に加える。
		駆け付けサービスの費用補償は、IPAの基本要件であるが、被害拡大防止や原因究明だけでなく、復旧までの広範囲をカバーしていることは、有効な補償機能であり、評価基準に加える。
		万一の場合の中小企業の費用負担を軽減させる意味からも、補償金額を「200万円」を目安として評価基準に加える。
7	導入実績	使用されている機器/ソフト類の提供元が明記されていることで、お助け隊サービスとしての信頼性や実績の裏付けとなる情報を得ることが可能なことから、評価基準に加える。
		導入実績数や、具体的な導入事例の情報が公開されていることは、顧客からのフィードバックも含めサービス品質が高く、サービス内容に自信を持っていると言えることから、評価基準に加える。

【表 3-4】評価基準とした理由

これらの調査項目と基準が整理できたことを踏まえて、具体的なワークシートの作成を行った。作成に当たっては、各自が調査した情報をもとに点数評価を試行する中で、各項目の配分点数決めなど、全体のバランスを考えながらメンバー間の意見集約を行った。

こうしてできた我々なりの評価を、企業との間でお助け隊サービスの紹介や、相談を受けた際に、そのまま伝えるだけでは企業の環境やニーズにマッチしないことから、ワークシートを一工夫して、我々の評価に企業側の視点や思いを反映できる仕掛けを追加するという 2 段階評価を考えた。

でき上がったワークシートの外観は表 3-5 の通りだが、各評価項目に企業の重みづけができる欄を設けることで、企業が特に重視する項目の点数が、より高くなるようにワークシートを修正した。これにより、お助け隊サービスを選定する際に、企業の環境やニーズを反映しながら、より適切なアドバイスが可能になると考える。

尚、このワークシート使う際の重みづけできる項目は、最大 3 項目程度として評価項目の点数にメリハリが付くようにすることが望ましい。

この「重みづけ」という考え方を持ち込んだことで、ワークシートを様々な場面で自分なりにアレンジして、汎用的に活用することができる。例えば、企業との会話の中で、『既存の IT ベンターとの関わりから候補となるサービスはほぼ決まっている』ということがよくある。その場合、ワークシートの評価項目の内、サービス提供力や実績の評価項目を重みづけすることで、該当のサービスは合計点数も高くなるはずで、そうした結果になれば、そのサービスを選択することは適切な判断と言える。

逆に、もしそれでも合計点数が上回る別のサービスがあった場合は、単なる取引関係で判断してよいのかという指摘にもつながり、より選択肢を拡げた判断材料を提供できる。

お助け隊サービスの選定時の評価ワークシートVer.2　(注1) 評価点⇒評価基準を満たすものに配分点数を与える

お助け隊サービス名称：xxxxxxxxx　　(注2) 重みづけ⇒不要:0、必要:1、重要:2

提供事業者：xxxxxxxxx　　※「重要:2」は最大3項目程度とする

7項目

	評価項目	配分点数	評価基準	テーマ研究会の評価 配分点数	評価点(注1)	コメント	合計点数	導入検討企業の評価 重みづけ(注2)	コメント	企業の評価点	合計点数	評価基準の採用理由と配分についての注釈
1	サービス提供力	10		5	0		0	0		0	0	
				5	0							
2	既存システムへの影響	15		15	0		0				0	
				15						0		
3	平常時の対応レベル	10		5	0					0	0	
				5	0			0		0		
4	異常発生時の対応レベル	20	4項目	5	0			0		0		
				5	0		0	0		0	0	
				5	0			0		0		
				5	0			0		0		
5	費用一式	20	倍の配点	10	0			0		0		
				10	0		0	0		0	0	
6	保険	15		5	0			0		0		
				5	0		0	0		0	0	
				5	0			0		0		
7	導入実績	10	テーマ研究会としてのベース評価	5	0			0		0		
				5	0		0	0		0	0	
	合計点数⇒	100		115	0		0			0	0	

顧客のニーズ/要件を反映

併用型は、EDR, UTMの両サービスを評価

顧客のニーズ/要件を反映した評価

(注3) 併用型(EDR+UTM)のサービスについては、配分点数の合計が115点になる。

評価に際してのコメント	

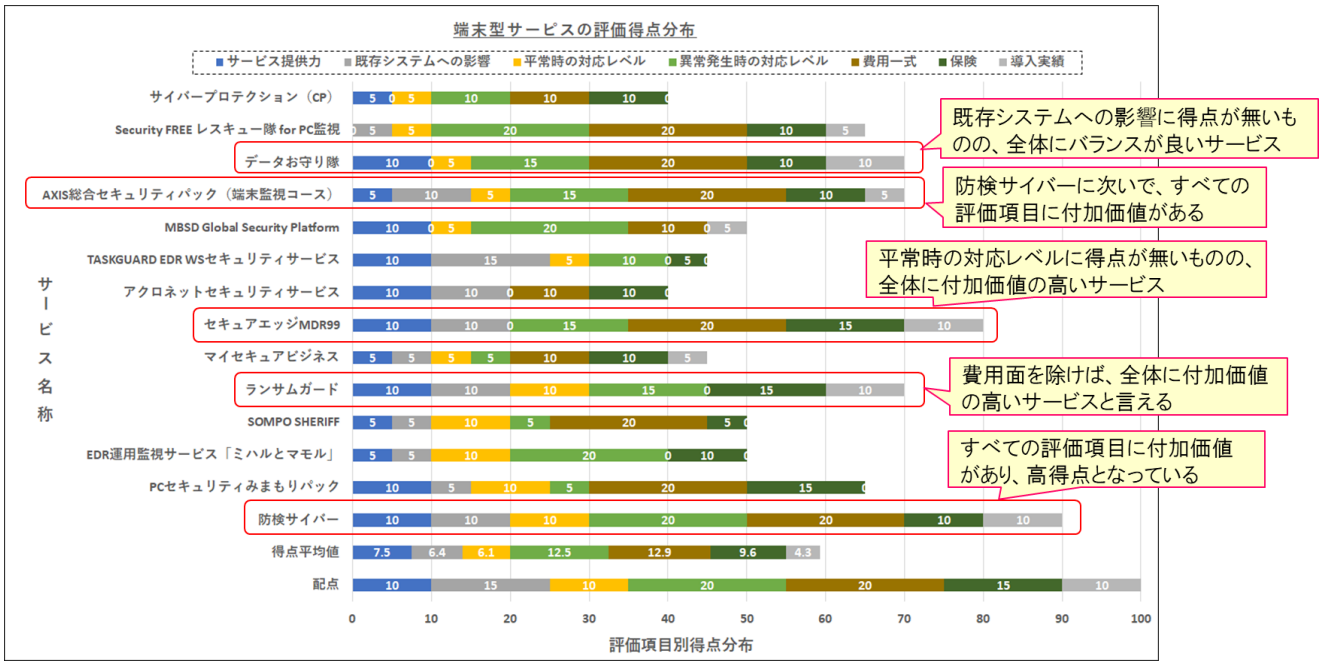
【表 3-5】評価ワークシートの外観

3.3.3 評価ワークシートを用いた各サービスの評価

ワークシートを用いて、各サービスについて我々なりの点数評価を行い、別紙の通り比較項目別の一覧表にまとめたが、当報告書の中では、監視対象別(端末、ネットワーク、併用の各タイプ別)に、特徴となる点を見ていくことにする。

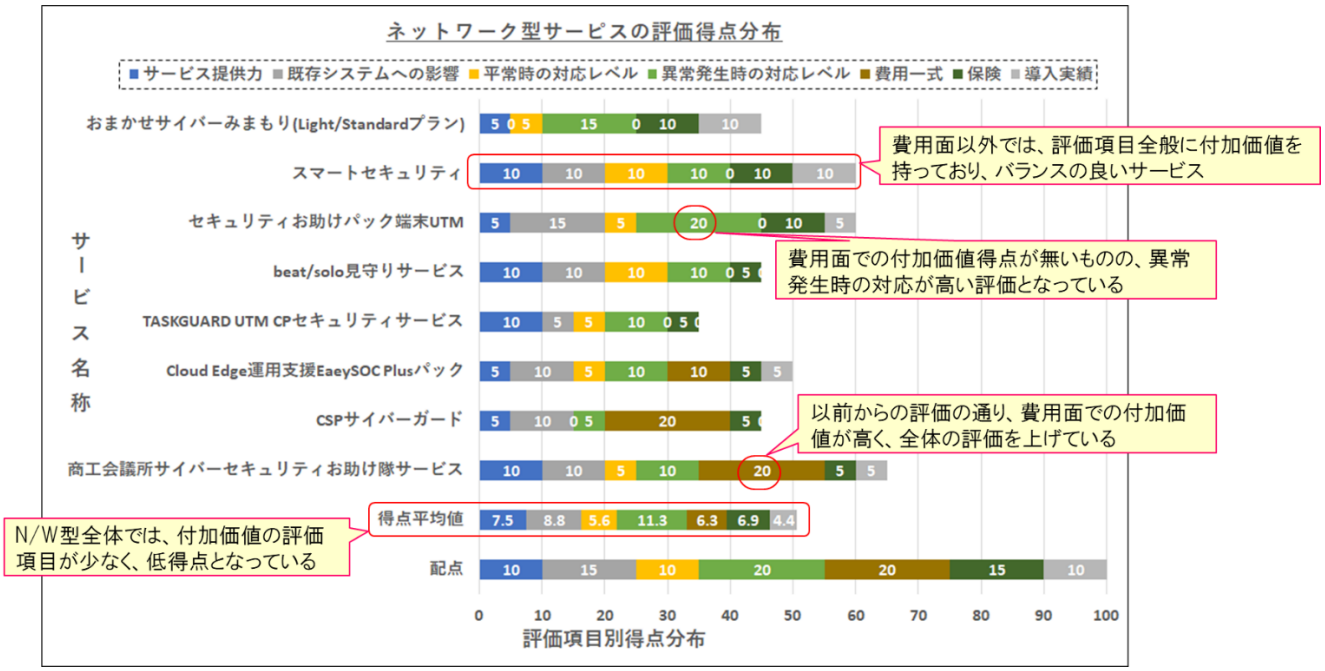
尚、ネットワーク型の連番 26,27 と併用型の連番 28,29 は、使用する UTM の性能(接続端末数)に違いがあるだけのため、以降の比較では同一のサービスとして取り扱うことにした。

図 3-2 の端末型サービスでは、ネットワーク型や併用型のサービスと比べて、全体的に付加価値点数が高く、特に高得点のサービスには、吹き出しに示すような特徴が見て取れる。



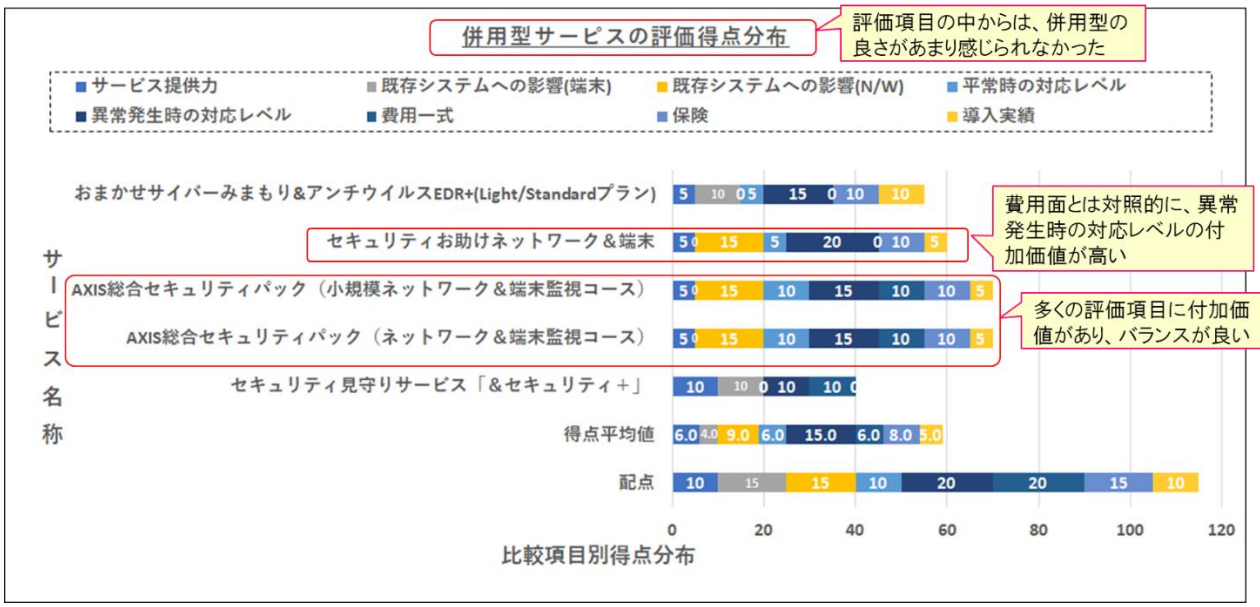
【図 3-2】端末型サービスの評価点数分布

ネットワーク型のサービスは、全体的に付加価値の得点が低く、吹き出しに示したように、UTM の使用料である費用面での得点が低いサービスが多く見られる。



【図 3-3】ネットワーク型サービスの評価点数分布

併用型サービスについては、端末型とネットワーク型の両方の対策が取れる良さがあるものの、付加価値得点としてさほど高い得点ではなく、今回の評価では併用型のメリットがあまり感じられなかった。



【図 3-4】併用型サービスの評価点数分布

以上の通り各タイプ別の得点分布の特徴を見てきたが、これを表 3-6 として、一覧表にまとめ、また比較項目ごとの特徴を整理した。

付加価値としての得点(合計)	配点	対象サービスの平均値	対象サービスの最高得点	対象サービスの最低得点
端末型	100点	59.3点	90点	40点
ネットワーク型	100点	50.6点	65点	35点
併用型	115点	59.0点	70点	40点
併用型	100点換算	51.3点	60.1点	34.8点

比較項目	端末型	N/W型	併用型(100点換算)	(注)%の数値は、各比較項目ごとの平均値÷配点x100%
サービス提供力	75.0%	75.0%	52.2%	併用型には、販売代理店のあるサービスが少ないことが数値の差になっている。
既存システムへの影響	42.9%	58.3%	37.7%	全体として低い数値だが、端末型/併用型は、複数OSに対応するサービスが少ないことがN/W型との数値の差になっている。
平常時の対応レベル	60.7%	56.3%	52.2%	大きな差は無いが、端末型が週次レポートや、適宜情報確認できる機能を持つサービスが多いことが、比較的数値が高い要因と言える。
異常発生時の対応レベル	62.5%	56.3%	65.2%	即時通知や24時間365日の窓口対応は多くのサービスで行っているが、駆付け対応が24時間365日可能なサービスはごく少数だった。
費用一式	64.3%	31.3%	26.1%	最も得点の差が出た項目で、EDRを割安な費用設定となっているサービスが多いのに対し、UTM費用を低く抑えているサービスは少ない。
保険	64.3%	45.8%	46.4%	N/W型は、補償金額が少額のサービスが多く、損害賠償費用を対象としているサービスも少ないことが大きな差となっている。
導入実績	42.9%	43.8%	43.5%	どのサービス型も、ほぼ同程度の数値になっており、実績についての情報開示は低水準と言える。
合計	59.6%	50.6%	53.0%	

【表 3-6】各監視タイプ別の付加価値得点一覧表

比較のもう一つの視点として、「各サービスが付加価値の基準をどの程度満たしたか」について、表 3-7, 8, 9 に星取表として整理し、今回設定した基準の妥当性を検証してみた。

各監視タイプの特徴は吹き出しのコメントにあるとおりだが、共通の特徴として、駆け付け対応の時間帯(24 時間 365 日)の評価基準を満たしているサービスが少ないことが挙げられる。ただ、お助け隊サービスの要件としては、既にリモートでの対応が認められており、費用との兼ね合いもあることから、今後はリモート対応の機能をどこまで高められるかが、付加価値として求められる点かもしれない。

○:評価基準を満たしている、●:評価基準を満たしていない

	評価項目	評価基準	○数	●数	連番 2	3	4	5	6	9	10	12	13	15	18	20	21	22
1	サービス提供力	全国の主要都市をカバーしている。	13	1	○	○	○	○	○	○	○	○	○	○	○	○	●	○
		販売代理店など顧客との接点(窓口)が多い。	8	6	○	○	●	●	○	●	○	○	○	○	●	○	●	●
2	既存システムへの影響	既存の端末構成に対する制約が少なく、幅広い端末で利用可能。	11	3	○	○	○	○	○	○	○	○	○	●	○	●	○	●
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	11	3	○	○	○	○	○	○	●	●	○	○	●	○	○	○
		定期的報告(レポートやメール)が週次に送付される。	6	8	○	○	○	○	○	●	●	●	●	●	○	●	●	●
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	12	2	○	●	○	○	○	○	○	●	○	○	○	○	○	○
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	8	6	○	●	○	●	○	●	○	●	●	○	○	○	○	●
		駆け付け対応の時間帯が24時間365日可能である。	4	10	○	●	○	●	●	●	●	●	●	○	●	●	○	●
		マルウェアの駆除や復旧までの支援が得られる。	11	3	○	○	○	●	○	●	○	●	○	○	○	○	○	○
5	費用一式	年額換算費用が、IPA要件(基準)の60%以下である。	9	5	○	○	●	○	●	○	○	○	●	●	○	○	○	●
		初期費用などの追加費用がない。	9	5	○	○	●	○	●	●	○	●	●	○	○	○	○	○
6	保険	損害賠償も補償の対象となっている。	10	4	○	○	●	●	○	○	○	○	●	●	○	○	○	○
		費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象	9	5	●	○	○	○	○	●	○	●	○	●	●	○	○	○
		補償金額の上限が200万円/年以上	8	6	○	○	○	●	○	○	○	○	●	●	○	●	●	●
7	導入実績	提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	6	8	○	●	●	●	○	●	○	●	●	●	○	○	○	●
		導入実績数や具体的な事例紹介の情報が、Webなどで公開されている。	6	8	○	●	●	●	○	○	○	●	●	○	●	○	●	●
			合計	○数	15	11	10	8	13	8	13	6	7	9	11	12	11	7
				●数	1	5	6	8	3	8	3	10	9	7	5	4	5	9

今後はリモート対応が主体？

更なる情報開示が望まれる

【表 3-7】端末型サービスの評価得点分布

○:評価基準を満たしている、●:評価基準を満たしていない

	評価項目	評価基準	○数	●数	連番 1	8	11	14	19	24	26	27
1	サービス提供力	全国の主要都市をカバーしている。	7	1	○	○	○	○	○	●	○	○
		販売代理店など顧客との接点(窓口)が多い。	5	3	○	●	●	○	○	○	○	●
2	既存システムへの影響	既存の端末構成に対する制約が少なく、幅広い端末で利用可能。	7	1	○	○	○	○	○	○	○	●
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	7	1	○	●	○	○	○	○	○	○
		定期的報告(レポートやメール)が週次に送付される。	2	6	●	●	●	●	○	●	○	●
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	8	0	○	○	○	○	○	○	○	○
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	2	6	●	●	●	●	●	○	●	○
		駆け付け対応の時間帯が24時間365日可能である。	1	7	●	●	●	●	●	○	●	●
		マルウェアの駆除や復旧までの支援が得られる。	7	1	○	●	○	○	○	○	○	○
5	費用一式	年額換算費用が、IPA要件(基準)の60%以下である。	3	5	○	○	○	●	●	●	●	●
		初期費用などの追加費用がない。	2	6	○	○	●	●	●	●	●	●
6	保険	損害賠償も補償の対象となっている。	3	5	●	●	●	●	●	○	○	○
		費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象。	8	0	○	○	○	○	○	○	○	○
		補償金額の上限が200万円/年以上	0	8	●	●	●	●	●	●	●	●
7	導入実績	提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	4	4	○	●	○	●	●	●	○	○
		導入実績数や具体的な事例紹介の情報が、Webなどで公開されている。	3	5	●	●	●	●	●	○	○	○
			合計	○数	10	6	8	7	8	10	11	9
				●数	6	10	8	9	8	6	5	7

即時アラートはあるが、24時間365日対応は少ない

UTMの導入初期費用が必要なサービスが多い

復旧までの対応が保障されているが補償金額は少ない

【表 3-8】ネットワーク型サービスの評価得点分布

○:評価基準を満たしている、●:評価基準を満たしていない

	評価項目	評価基準	○数	●数	連番 7	16	17	25	28
1	サービス提供力	全国の主要都市をカバーしている。	4	1	○	○	○	●	○
		販売代理店など顧客との接点(窓口)が多い。	2	3	○	●	●	○	●
2	既存システムへの影響(端末)	既存の端末構成に対する制約が少なく、幅広い端末で利用可能。	2	3	○	●	●	●	○
	既存システムへの影響(N/W)	既存の端末構成に対する制約が少なく、幅広い端末で利用可能。	3	2	●	○	○	○	●
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	4	1	●	○	○	○	○
		定期的報告(レポートやメール)が週次に送付される。	2	3	●	○	○	●	●
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	0	○	○	○	○	○
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	0	○	○	○	○	○
		駆け付け対応の時間帯が24時間365日可能である。	1	4	●	●	●	○	●
		マルウェアの駆除や復旧までの支援が得られる。	4	1	●	○	○	○	○
5	費用一式	年額換算費用が、IPA要件(基準)の60%以下である。	3	2	○	○	○	●	●
		初期費用などの追加費用がない。	0	5	●	●	●	●	●
6	保険	損害賠償も補償の対象となっている。	4	1	●	○	○	○	○
		費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象。	2	3	●	●	●	○	○
		補償金額の上限が200万円/年以上	2	3	●	○	○	●	●
7	導入実績	提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	3	2	●	○	○	●	○
		導入実績数や具体的な事例紹介の情報が、Webなどで公開されている。	2	3	●	●	●	○	○
			合計	○数	6	11	11	10	10
				●数	11	6	6	7	7

駆け付け対応の24時間365日対応以外は基準を満たしている項目が多い

UTMの導入初期費用が必要なサービスが多い

損害賠償を補償対象としているサービスが多い

【表 3-9】併用型サービスの評価得点分布

以上の各タイプの評価基準の達成度合いをまとめると、表 3-10 の通りとなる。

総括としては、ネットワーク型の基準達成度合いが若干低いものの、どのサービス形態(監視対象別)においても、50%～60%程度の基準を満たしており、今回の付加価値得点としての基準設定は、妥当な範囲と言える。

また今後は、以下の変化を踏まえて、「サービスの付加価値」の評価基準も、適宜見直しを図る必要がある。

1) 今後更にお助け隊サービスの登録数が増え、その内容も多様になることが考えられる。
2) 企業のニーズや環境面での求められる要件が変化する。
3) 後述の事例研究や、今後の具体的な案件の中で、新たな評価基準の必要性が出てくる。

○:評価基準を満たしている、●:評価基準を満たしていない

星取表	端末型		ネットワーク型		併用型		合計	
	個数	比率	個数	比率	個数	比率	個数	比率
○	141	62.9%	69	53.9%	48	56.5%	258	59.0%
●	83	37.1%	59	46.1%	37	43.5%	179	41.0%
合計	224	100%	128	100%	85	100%	437	100%

【表 3-10】星取表のまとめ

3.3.4　評価のまとめ

後述の事例研究にもある通り、評価ワークシートを用いた「数値による比較評価」が試行でき、当初の目標を達成することができた。

今後、お助け隊サービスに関する企業からの相談や提案活動の場で、企業のニーズや環境を認識合わせできるツールとしての活用いただけれとありがたい。

一方で、今回設定した基準の妥当性(星取表の○の比率)は認められるものの、個々の基準の配点や、満たすための条件設定などについては、再考の余地がある。

①. 今回は基準ごとに基本 5 点の配点とし、費用の項目のみ 10 点としたが妥当か。

②. 個々の基準設定のバラツキは妥当か。

※「いずれかを満たせば 5 点」、「満たしている内容ごとに 5 点ずつ加点」等々

また、昨年度の報告書でも触れたが、比較評価に有用な公開情報はまだ少なく、特に以下の点で更なる開示が欲しい。

①. サービスで使用される機器やソフトウェアの仕様、サービスの提供元(製造/開発/運用管理)

②. お助け隊サービスとしての実績と事例紹介

比較の最後に、今回対象としたサービスの中で、我々のチームとして付加価値点数の高かったサービスを一覧にまとめた。

比較は公開情報など、我々が入手できたものによるものであり、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、あくまでも参考としてご覧いただきたい。

尚、今回各メンバーが事例研究として各企業の環境、ニーズによる重み付けを反映した比較を行ったが、その結果については次章で紹介する。

監視対象	連番	サービス名称	事業者名	得点	調査担当者のコメント（一部抜粋）
端末	2	防検サイバー	MS&ADインターリスク総研株式会社	90	ある程度自社にて運用管理できる(したい)場合には、機能や実績面の評価が高く、有力な候補となる。
	6	ランサムガード	アイティフォー	70	初期費用や1台単価が少し割高だが製品実績はあり保証金額も高め。事故発生時の対処は早いが基本リモート対応なので復旧可能かどうか要確認
	10	セキュアエッジMDR99	セキュアエッジ株式会社	80	自動で監視・検知・隔離・駆除まで実施。補償金額もある程度ある。駆け付けはあまり期待できないが、比較的安価なお任せサービスである。
	18	AXIS総合セキュリティパック（端末監視コース）	株式会社アクシス	70	初期費用無料で、サポートはかなりの範囲実施。
	20	データお守り隊	株式会社アクト	70	MITRE社の評価で世界トップクラスの検知・防御率であるSentinel Oneがベースのサービスで情報提供にも協力的。
ネットワーク	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	65	価格を抑えるため保険補償額は最小限。各地の商工会議所やIT事業者と連携して駆付けサービスを充実。事故時の現場復旧対応に力を入れた。
	24	セキュリティお助けパック端末UTM	パリオセキュア株式会社	60	中小規模事業所に最適化されたネットワークセキュリティ機器の提供・運用支援に加え、ウイルス駆除支援と、ウイルス感染により発生した損害を補償。
	26	スマートセキュリティ	(株)ビープラス	60	IT導入補助金を意識して初期一括導入費が高い(44万円)パックにしているが、補償は1請求100万円まで、駆け付けは解決するまで無償でサポートと手厚い。
併用	16 17	AXIS総合セキュリティパック（N/W＆端末監視コース）	株式会社アクシス	70	初期費用は高いが(UTM代11万円)かなり高度なサポートまで可能 ※No.17は小規模ネットワークを対象にしたサービスで内容は同じ。
	25	セキュリティお助けネットワーク＆端末	パリオセキュア株式会社	60	上記(ネットワーク)の提供サービスに、端末セキュリティを強化するEDR/EPP機能を付加し、より安心なサイバー攻撃対策を実現。

【表 3-11 付加価値得点の高かったお助け隊サービス】

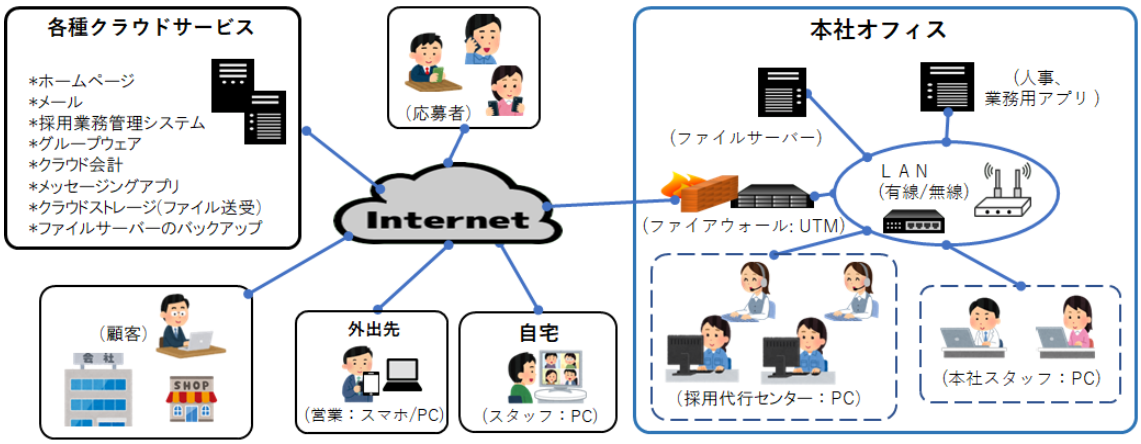
4．実証実験結果と考察（事例研究）

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紹介する。

4.1 事例（作成者：川名）

【企業の状況】

業種　：　サービス業(企業の人材採用支援)
拠点数　　：　1 箇所
PC 台数と OS　：　約 40 台（Windoes10, 11）
PC の持ち出し　：有（営業活動、自宅でのテレワーク）
ウイルス対策ソフト　　：有（PC、UTM）
ネットワーク対策　　：有（UTM を設置済）
外部から社内への接続　：有
万が一の際の対応：日常のシステム運用管理やユーザーサポートを行うチーム(兼務)が対応する。ユーザーサポート面での IT スキルは比較的高いが、インフラ技術面での専門的知識はなく、UTM の管理は IT ベンダーに依頼。



【提案したサービス】

現在の UTM による防御機能に加えて、端末側に EDR 機能を有するお助け隊サービスの導入し、セキュリティ対策の強化を図る。

【選定理由】

事業継続(BCP)について関心が高く、万一のサイバーインシデント発生時の初動・緊急対応を強化したい意向があり、またクラウドサービス活用による情報システムの構成や環境変化に、UTM だけでは対処できていない状況がある。

①. UTM では、ネットワークを流れるメール添付のパスワード付き zip ファイルや、https 対応により SSL で暗号化されたデータは監視できない。
②. UTM 設置の主目的であった、サーバーに対する外部からの防御が、クラウドサービスの積極的活用の結果、防御対象がわずかになった。
③. 社外や自宅で使用されている PC は、UTM を経由せずに直接インターネットにアクセスして、クラウドサービスを使用している。

これらの状況を踏まえ、EDR の導入について、以下の要件を重視して選定を行った。

①. IT チームの対応力が高いことから、万一のインシデント発生時の即時通知や、24 時間 365 日対応可能な相談窓口など対応スピードを重視する。
②. 平常時の効率的な運用管理の点から、事業会社からの週次レポートに加え、各種の情報を必要に応じて適宜入手できることを重視する。
③. 採用支援という個人情報を取り扱う事業であることから、万一のインシデント発生時における損害賠償補償の手厚さを重視する。
④. 導入実績が多数あり、サービスの信頼性を重視する。

また、評価シートにおける企業側の重みづけとして、以下の 3 項目を 2 倍評価とした。

①. 異常検知時に即時にメール通知や管理端末へのアラート表示がある。
②. 異常検知時の窓口対応(リモート対応)が 24 時間 365 日可能である。
③. 損害賠償も補償の対象となっている。

【検討結果】

自らが調査を担当した損保系の 2 社と、東京都の情報セキュリティマネジメント指導業務で関係のある 1 社の計 3 社のお助け隊サービスを候補とした。

企業による重みづけを加えた比較の結果、候補 A が最有力候補となった。

候補		評価点	コメント
A	防検サイバー （MS&ADインターリスク総研）	100	機能、費用、実績等、全体にバランスが良く高評価となった。
B	SOMPO SHERIFF （SOMPOリスクマネジメント）	50	機能や実績での評価が低かったが、無料体験版で稼働環境や機能の確認が可能。
C	ランサムガード （アイテイフォー）	80	費用の低評価が、候補Aと比べた差となった。

【参考：ワークシートの評価点】

：企業の重みづけとして、2倍とした項目

		サービス名称		防検サイバー				SOMPO SHERIFF				ランサムガード			
		提供会社		MS&AD				SOMPOリスクマネジメント				アイティフォー			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	1	5	5	5	1	5	5	5	1	5	5
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	0	0		0	0	0		5	0	0	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10	5	1	5	5	10	1	10	10
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	10	5	1	5	10	5	1	5	10
		定期的報告(レポートやメール)が週次に送付される。	5	5	1	5		5	1	5		5	1	5	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	30	5	2	10	10	5	2	10	25
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	2	10		0	2	0		5	2	10	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	5	1	5		0	1	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5		0	1	0		5	1	5	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	1	10	20	10	1	10	20	0	1	0	0
		初期費用などの追加費用がない。	10	10	1	10		10	1	10		0	1	0	
6	保険	損害賠償も補償の対象となっている。	5	5	2	10	15	0	2	0	0	5	2	10	20
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0		0	1	0		5	1	5	
		補償金額の上限が200万円/年以上である。	5	5	1	5		0	1	0		5	1	5	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	10	0	1	0	0	5	1	5	10
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	5	1	5		0	1	0		5	1	5	
	合計点数⇒		115	90		100	100	45		50	50	70		80	80

4.2 事例（作成者：鈴木）

＜事例１＞

【企業の状況】

業種　：　製造業

拠点数　　：　1 箇所

PC 台数と OS　：　10 台（OS 名称）　営業　WIN11　現場・事務　WIN10

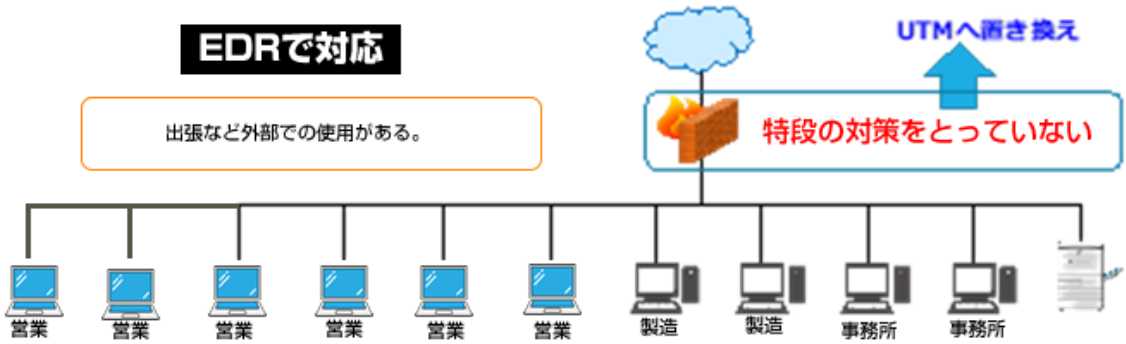
PC の持ち出し　：有（営業）

ウイルス対策ソフト　　：有（全数インストール済）PC

ネットワーク対策　　：有　（UTM）

外部から社内への接続　：有

万が一の際の対応：内容社内に対応できる人の無、頼める IT ベンダーの無



【提案したサービス】

UTM と端末を両方セキュリティ対応し、さらに、補償がついたサービスを導入する。

【選定理由】

セキュリティに対して、まだ知識もなく、ただ、事業者として導入していないのが困るために初段階として導入をする。

① 対外的にセキュリティ対応を示せるもの

② 社内のセキュリティへのリテラシーが低いために全体的セキュリティ対応できる

③ 事故発生したときに、できるだけ会社に金銭的負担をかけない補償がついたもの

これらの状況を踏まえ、導入について、以下の要件を重視して選定を行った。

①. **費用**　総合的にコストがかからないものを選定する。

②. **機能**　社内、社外両方のセキュリティを網羅したサービスを選定する。

③. **補償**　ユーザーに何かしらの障害を起こす場合を考えて、全体網羅したサービスを選定する。

【検討結果】

以下の３つのお助け隊サービスを候補とし、企業による重みづけを加えた比較の結果、候補Ｂが最有力候補となった。

候補		評価点	三社比較での順位
A	セキュリティ見守りサービス「 &セキュリティ＋ 」（株式会社BCC）	40	費用 1位 機能 3位 補償 3位 ※費用が安い分、機能、補償もそれに準じたものになっており、費用対効果は低いと評価した。
B	AXIS総合セキュリティパック（ネットワーク&端末監視コース）（株式会社アクシス）	75	費用 2位 機能 2位 補償 1位 ※月額費用は安価だったが、初期費用が高いため費用の評価は低くなったが、機能は全体網羅され、補償は一番厚かった。
C	ランサムガードセキュリティお助けパック（ネットワーク&端末）パリオセキュア株式会社	55	費用 3位 機能 1位 補償 2位 ※高機能であるが、費用もそれに準じて高額になる。補償も充実しているが、Bよりを上回らなかった。

		提供会社		株式会社BCC				株式会社アクシス				パリオセキュア株式会社			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	1	5	10	5	1	5	5	0	1	0	15
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	1	5		0	0	0		15	1	15	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10	0	0	0	15	5	1	5	5
		【ネットワーク型(UTM)】 ①.既存のシステム(ネットワーク)環境に影響を与えずに導入でき、機能を補完し合って使える。 ②.システム(ネットワーク)環境に修正を要しても、既存の機器が不要となり、コストを削減(抑制)できる。	15	0	0	0		15	1	15		0	0	0	
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	0	1	0	0	5	1	5	10	5	1	5	10
		定期的報告(レポートやメール)が週次に送付される。	5	0	1	0		5	1	5		5	1	5	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	1	5	10	5	1	5	15	5	1	5	10
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	1	5		5	1	5		5	1	5	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	0	1	0		0	0	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	0	1	0		5	1	5		0	1	0	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	1	10	10	10	1	10	10	5	1	5	10
		初期費用などの追加費用がない。	10	0	1	0		0	0	0		5	1	5	
6	保険	損害賠償も補償の対象となっている。	5	0	0	0	0	5	1	5	15	0	1	0	5
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0		5	1	5		0	1	0	
		補償金額の上限が200万円/年以上である。	5	0	1	0		5	1	5		5	1	5	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	0	1	0	0	5	1	5	5	0	1	0	0
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	0	1	0		0	1	0		5	0	0	
	合計点数⇒		115	40		40	40	75		75	75	60		55	55

＜事例 2＞（作成者：鈴木）

【企業の状況】

業種　：　情報通信業

拠点数　　：シェアオフィス活用（5 か所）

PC 台数と OS　：　5 台（Win11）

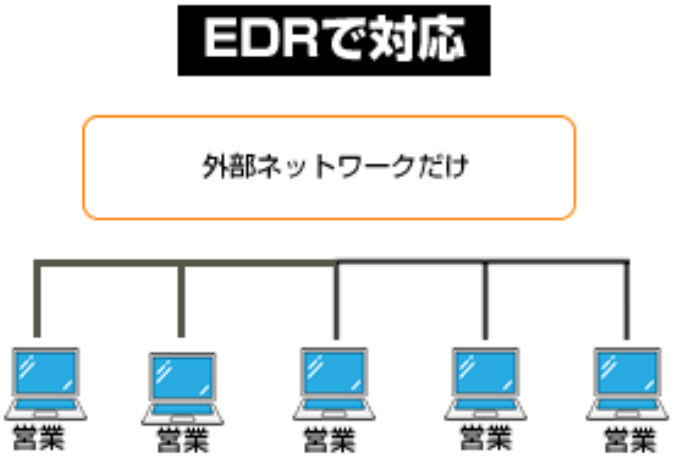
PC の持ち出し　：有（営業・テレワーク）

ウイルス対策ソフト　　：有（全数インストール済）PC

ネットワーク対策　　：無（シェアオフィス活用）

外部から社内への接続　：無（クラウド活用）

万が一の際の対応：社内に対応できる人のあり（そんなに詳しくない)、頼める IT ベンダーの無



【提案したサービス】

シェアオフィスや自宅、外部での PC 作業が多いため、EDR 機能有した端末お助け隊サービスの導入し、セキュリティ対策のを強化する。

【選定理由】

シェアオフィスや配布の Wifi でビジネス展開を行い、作業も行ってきたが、クライアントから、情報セキュリティの取り組みについてリクエストが増えたためにそれに対応する。

①. シェアオフィスでは、そのオフィス内でのセキュリティに課題がある。特に自社からクライアントに感染させない対応が必要である。

②. 自社でも社員のセキュリティリテラシーの向上は必要だが、まずは、外部にシステムでのセキュリティ対応を示していく。

③. 事故が起こった時の補償のついたサービス。

【検討結果】

以下の３つのお助け隊サービスを候補とし、企業による重みづけを加えた比較の結果、候補Ｂが最有力候補となった。

候補		評価点	コメント
A	防検サイバー（MS&ADインターリスク総研）	90	機能１位、費用１位、補償１位とすべてで他社を上回った
B	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)	45	機能3位、費用3位、補償3位とすべてで他社を下回った
C	ランサムガード (アイテイフォー)	70	機能2位、費用2位、補償3位と候補Aを上回れなかった

		サービス名称		防検サイバー				TASKGUARD EDR WS セキュリティーサービス				ランサムガード			
		提供会社		MS&AD				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				アイティフォー			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	1	5	10	5	1	5	10	5	1	5	10
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	1	5		5	1	5		5	1	5	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10	15	1	15	15	10	1	10	10
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	10	5	1	5	5	5	1	5	10
		定期的報告(レポートやメール)が週次に送付される。	5	5	1	5		0	1	0		5	1	5	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	1	5	20	5	1	5	10	5	1	5	15
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	1	5		0	1	0		5	1	5	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	5	1	5		0	1	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5		5	1	5		5	1	5	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	1	10	20	0	1	0	0	0	1	0	0
		初期費用などの追加費用がない。	10	10	1	10		0	1	0		0	1	0	
6	保険	損害賠償も補償の対象となっている。	5	5	1	5	10	0	1	0	5	5	1	5	15
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0		5	1	5		5	1	5	
		補償金額の上限が200万円/年以上である。	5	5	1	5		0	1	0		5	1	5	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	10	0	1	0	0	5	1	5	10
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	5	1	5		0	1	0		5	1	5	
	合計点数⇒		115	90		90	90	45		45	45	70		70	70

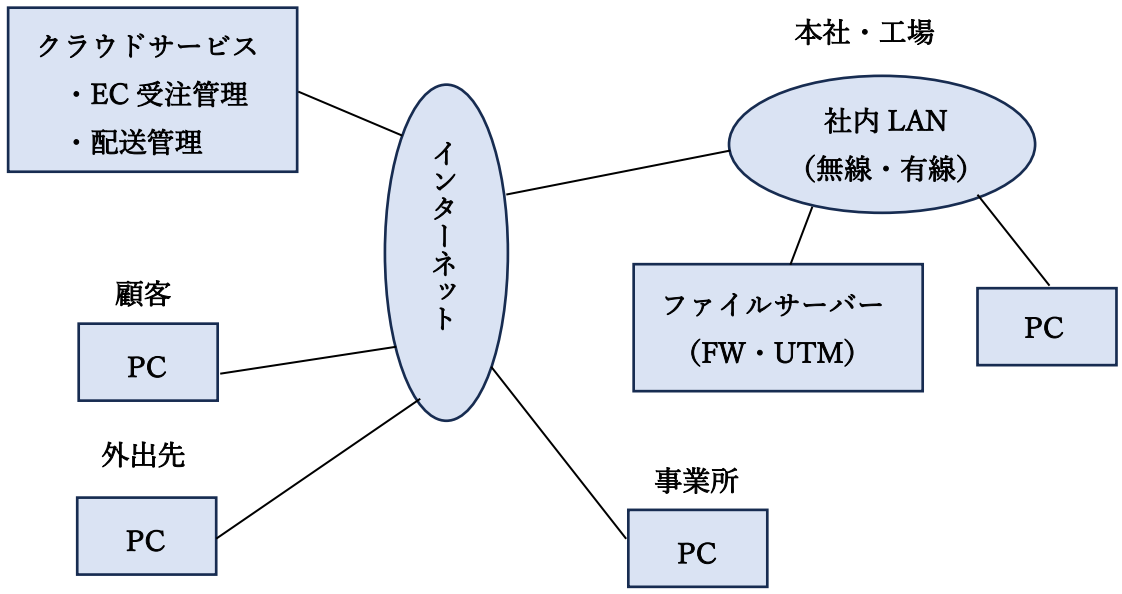
4.3 事例（作成者：木村）

＜事例１＞

【企業の状況】

業種　　：製造業（エンドユーザーの個人情報取り扱い有り）
拠点数　　：２か所（本社・工場、及び、都内に事業所が１カ所）
PC 台数と OS　　：15 台（OS 名称） WIN11、WIN10
PC の持ち出し　　：有（展示会や商談で）
ウイルス対策ソフト　：有（全数インストール済）
ネットワーク対策　　：有
外部から社内への接続：有
万が一の際の対応　　：社内に対応できる人：無、頼める IT ベンダー：無

ネットワーク構成図



【提案したサービス】

ファイルサーバー用途で UTM がパッケージされた共有ストレージを使っているので、端末 EDR としてコストパフォーマンスに優れたサービスを選定した。

【選定理由】

機微な個人情報を扱うこともあり、UTM だけでは不十分と判断し、端末 EDR を導入して情報セキュリティ対策を強化したい。

EDR 型の導入について、以下の要件を重視して選定を行った。

①.自社に合ったサービスかの見極めのために、まずは月額費用が安価であること

②.インシデント発生時の即時通知があり、24 時間 365 日対応可能な相談窓口など対応スピードが速いこと

③.インシデント発生時における損害賠償補償が手厚いこと

【検討結果】

以下の 4 つのお助け隊サービスを候補とし、企業による重みづけを加えた比較の結果、候補 A が最有力候補となった。

候補		評価点	コメント
A	防検サイバー（MS&ADインターリスク総研）	115	機能、費用、実績等、全体にバランスが良く高評価
B	セキュアエッジMDR99（セキュアエッジ株式会社）	105	平常時・異常発生時の対応レベルがAよりやや低評価
C	AXIS総合セキュリティパック（株式会社アクシス）	100	保険の対象範囲がA、Bよりやや低評価
D	データお守り隊（株式会社アクト）	95	上記に加えてサポートOS対象範囲がやや低評価

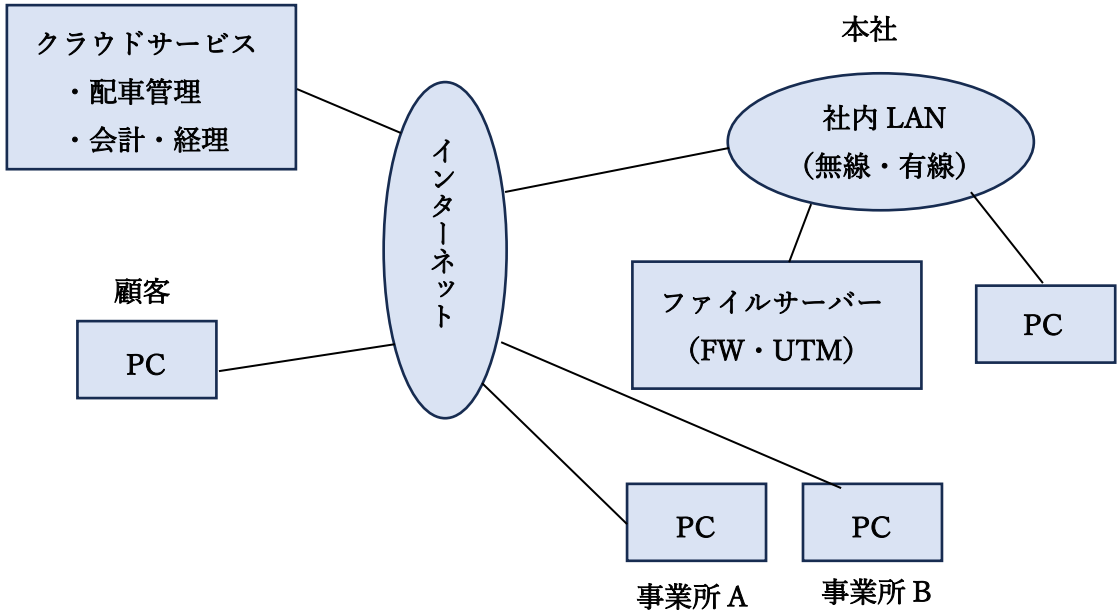
		サービス名称		防検サイバー					セキュアエッジMDR99				AXIS総合セキュリティパック（端末監視コース）				データお守り隊			
		提供会社		MS&AD					セキュアエッジ株式会社				株式会社アクシス				株式会社アクト			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数		研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	0	0	0		5	0	0	0	5	0	0	0	5	0	0	0
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	0	0			5	0	0		0	0	0		5	0	0	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10		10	1	10	10	10	1	10	10	0	1	0	0
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	10		0	1	0	0		1	0	5	5	1	5	5
		定期的報告(レポートやメール)が週次に送付される。	5	5	1	5			0	1	0		5	1	5		0	1	0	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	30		5	2	10	25	5	2	10	25	5	2	10	25
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	2	10			5	2	10		5	2	10		5	2	10	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	5	1	5			0	1	0		0	1	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5			5	1	5		5	1	5		5	1	5	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	2	20	40		10	2	20	40	10	2	20	40	10	2	20	40
		初期費用などの追加費用がない。	10	10	2	20			10	2	20		10	2	20		10	2	20	
6	保険	損害賠償も補償の対象となっている。	5	5	2	10	15		5	2	10	20	5	2	10	15	5	2	10	15
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0			5	1	5		0	1	0		5	1	5	
		補償金額の上限が200万円/年以上である。	5	5	1	5			5	1	5		5	1	5		0	1	0	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	10		5	1	5	10	5	1	5	5	5	1	5	10
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	5	1	5			5	1	5		0	1	0		5	1	5	
	合計点数⇒		115	90		115	115		80		105	105	70		100	100	70		95	95

＜事例２＞（作成者：木村）

【企業の状況】

業種　　：運送業
拠点数　　：３か所（本社、及び、２つの事業所）
PC 台数と OS　　：10 台（OS 名称） WIN11
PC の持ち出し　　：無
ウイルス対策ソフト　：有（全数インストール済）
ネットワーク対策　　：有
外部から社内への接続：無
万が一の際の対応　　：社内に対応できる人：有、頼める IT ベンダー：有

ネットワーク構成図



【提案したサービス】

基幹システム導入時から UTM がパッケージされたファイルサーバーを使っているので、端末 EDR としてコストパフォーマンスに優れたサービスを選定した。

【選定理由】

UTM だけでは不十分と判断し、端末 EDR を導入して情報セキュリティ対策を強化したい。

EDR 型の導入について、以下の要件を重視して選定を行った。

①.自社に合ったサービスかの見極めのために、まずは月額費用が安価であること

②.インシデント発生時の即時通知があり、24 時間 365 日対応可能な相談窓口などの対応スピードが速いこと

③.インシデント発生時における損害賠償補償が手厚いこと

④.AI 等の先進的な技術を導入した革新的サービスであること

【検討結果】

以下の 4 つのお助け隊サービスを候補とし、企業による重みづけを加えた比較の結果、点数的には候補 A が最有力候補となったが、選定理由④を満たすサービスが D であることから、新しもの好きな社長は D の導入を考えている。

候補		評価点	コメント
A	防検サイバー（MS&ADインターリスク総研）	115	機能、費用、実績等、全体にバランスが良く高評価
B	セキュアエッジMDR99 (セキュアエッジ株式会社)	105	平常時・異常発生時の対応レベルがAよりやや低評価
C	AXIS総合セキュリティパック (株式会社アクシス)	100	保険の対象範囲がA、Bよりやや低評価
D	データお守り隊 (株式会社アクト)	95	上記に加えてサポートOS対象範囲がやや低評価だがAIを使った検知・分析あり

		サービス名称		防検サイバー					セキュアエッジMDR99				AXIS総合セキュリティパック（端末監視コース）				データお守り隊			
		提供会社		MS&AD					セキュアエッジ株式会社				株式会社アクシス				株式会社アクト			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数		研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	0	0	0		5	0	0	0	5	0	0	0	5	0	0	0
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	0	0			5	0	0		0	0	0		5	0	0	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10		10	1	10	10	10	1	10	10	0	1	0	0
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	10		0	1	0	0		1	0	5	5	1	5	5
		定期的報告（レポートやメール）が週次に送付される。	5	5	1	5			0	1	0		5	1	5		0	1	0	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	30		5	2	10	25	5	2	10	25	5	2	10	25
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	2	10			5	2	10		5	2	10		5	2	10	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	5	1	5			0	1	0		0	1	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5			5	1	5		5	1	5		5	1	5	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	2	20	40		10	2	20	40	10	2	20	40	10	2	20	40
		初期費用などの追加費用がない。	10	10	2	20			10	2	20		10	2	20		10	2	20	
6	保険	損害賠償も補償の対象となっている。	5	5	2	10	15		5	2	10	20	5	2	10	15	5	2	10	15
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0			5	1	5		0	1	0		5	1	5	
		補償金額の上限が200万円/年以上である。	5	5	1	5			5	1	5		5	1	5		0	1	0	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	10		5	1	5	10	5	1	5	5	5	1	5	10
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	5	1	5			5	1	5		0	1	0		5	1	5	
	合計点数⇒		115	90		115	115		80		105	105	70		100	100	70		95	95

4.4 事例（作成者：田島）

＜事例１＞

【企業の状況】

業種　　：　製造業(半導体製造装置)

拠点数　：　1 箇所

PC 台数と OS　　：　約 5 台（Windoes10, 11）

PC の持ち出し　　：有（営業活動、自宅でのテレワーク）

ウイルス対策ソフト　　：有（PC）

ネットワーク対策　　：無

外部から社内への接続　：無

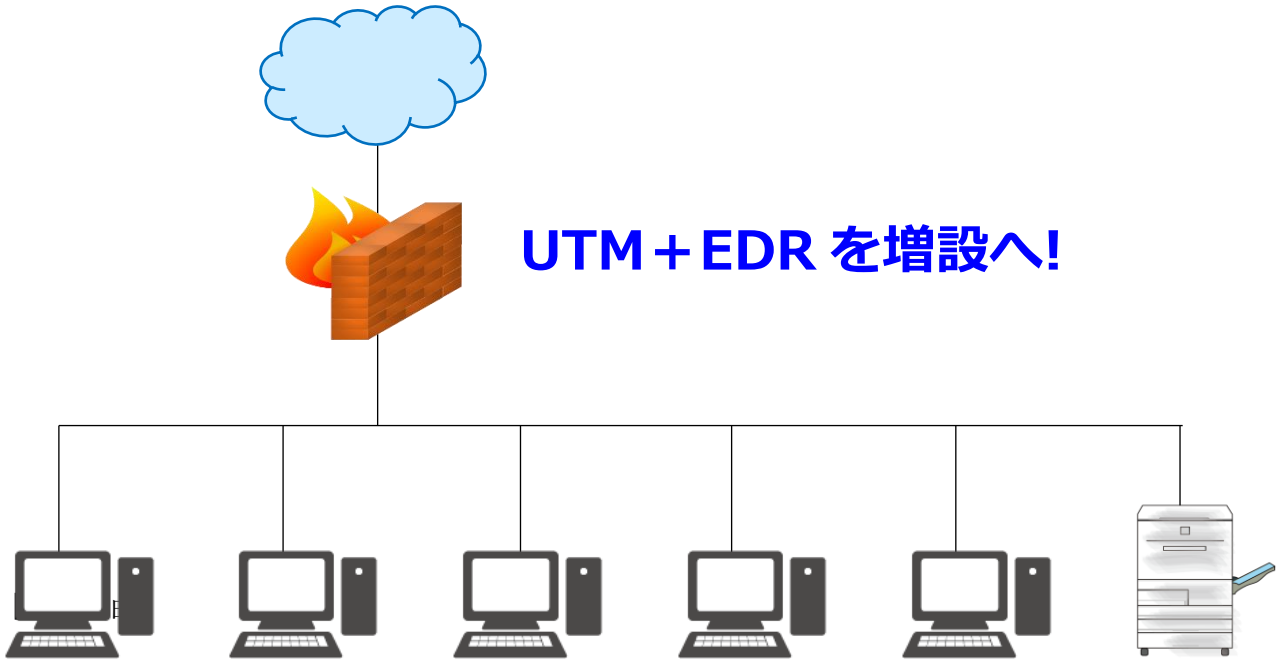
万が一の際の対応：日常のシステム運用管理やユーザーサポートを行うチーム(兼務)が対応する。ユーザーサポート面での IT スキルは比較的高いが、インフラ技術面での専門的知識はなく、UTM の管理は IT ベンダーに依頼。

【提案したサービス】

UTM の防御機能に加えて、端末側に EDR 機能を有するお助け隊サービスの導入し、セキュリティ対策の強化を図る。

【選定理由】

半導体製造関連設備のため海外からの発注も多く、その際の秘密保持条件等が厳しい（取引停止、厳重賠償契約がある）ことに加え、海外からのアタックもあり、緊急に厳重な対策を取る必要に迫られていた。ただし、厳しい経営・経済条件でもあり、できる限りの機密性を限られた経済条件で（それなりのコスト価格の中で）実現する必要があるとのこと。また、商工会議所の会員のためその属性が活かせることも選定の条件。



順番	候補	評価点	コメント
A	商工会議所サイバーセキュリティ お助け隊サービス	65	
B	防検サイバー （MS&AD インターリスク総研）	90	評価点数的には高いが　運用を実施するには この会社には不向き（運用者の技術力不足）
C	AXIS 総合セキュリティパック（ネットワーク＆端末監視コース）	70	評価点数的には高いが　価格の面で 少し高すぎる　（初期費、月次運用費の面から）

・特殊装置で秘密が漏れると事業が成り立たない！
（外国からのアタックがあるほど最近の H 業界では必要な装置）
＝＞UTM+EDR　型が必須
・費用的には　まあなんとか出せる範囲にしたく、、
・商工会議所会員のメリットも出したく
＝＞そんなに儲かってはいないが多少の金額負担は OK

【検討結果】

使用料金、使用形態、運用形態を考慮して以下の３つのサービスを提案し、コスト見合いで決定していただくことになった。お助け隊サービスを候補とした。

企業による重みづけを加えた比較の結果、候補 A が最有力候補となった。

		サービス名称		商工会議所サイバーセキュリティお助け隊				防検サイバー				AXIS総合セキュリティパック（N&T）			
		提供会社		大阪商工会議所				MS&AD				株式会社アクシス			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	1	5	5	5	1	5	5	5	1	5	5
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	0	0		5	0	0		0	0	0	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10	10	1	10	10	15	1	15	15
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	5	5	1	5	10	5	1	5	10
		定期的報告(レポートやメール)が週次に送付される。	5	0	1	0		5	1	5		5	1	5	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	15	5	2	10	30	5	2	10	25
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	0	2	0		5	2	10		5	2	10	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	0	1	0		5	1	5		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5		5	1	5		5	1	5	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	1	10	20	10	1	10	20	10	1	10	10
		初期費用などの追加費用がない。	10	10	1	10		10	1	10		0	1	0	
6	保険	損害賠償も補償の対象となっている。	5	5	2	10	10	5	2	10	15	5	2	10	15
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0		0	1	0		0	1	0	
		補償金額の上限が200万円/年以上である。	5	0	1	0		5	1	5		5	1	5	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	5	5	1	5	10	5	1	5	5
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	0	1	0		5	1	5		0	1	0	
	合計点数⇒		115	65		70	70	90		100	100	70		85	85
	総合コメント			価格を抑えるため保険補償額は最小限(年間30万円）各地の商工会議所やIT事業者と連携して駆け付けサービスを充実。事故時の現場復旧対応に力を入れた.				ある程度自社にて運用管理できる(したい)場合には、機能や実績面の評価が高く、有力な候補となる。				初期費用は高いが（UTM代１１万円）かなり高度なサポートまで可能			

＜事例２＞（作成者：田島）

【企業の状況】

業種　　：　教育・コンテンツ製造業(低学年向け)

拠点数　：　３箇所

PC 台数と OS　　：　約２０台（Windows 11）

PC の持ち出し　　：有（教育活動、自宅でのテレワーク）

ウイルス対策ソフト　　：有（PC）

ネットワーク対策　　：無

外部から社内への接続　：有

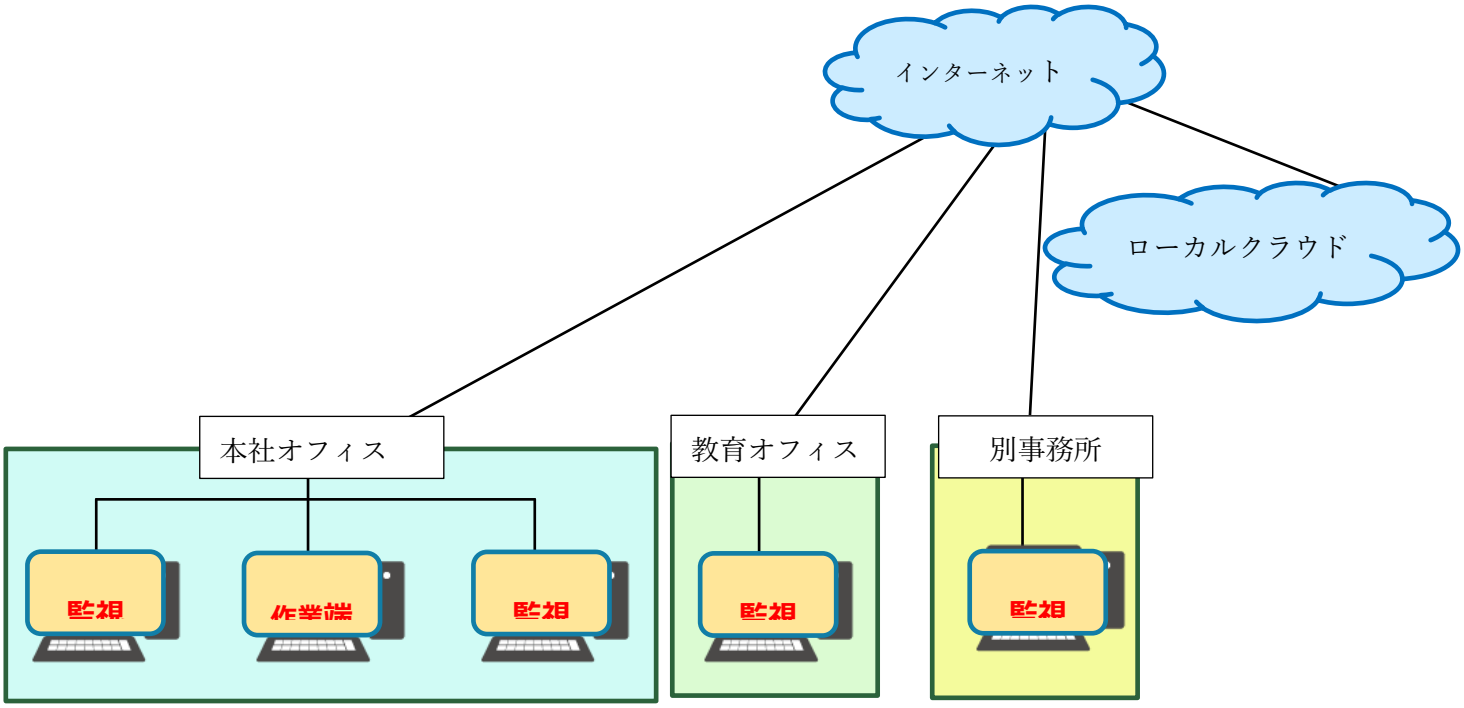
万が一の際の対応：日常のシステム運用管理やユーザーサポートを行うチームがいない。秘匿情報は限られていて、切り離しが可能。

【提案したサービス】

コスト面がゆとり無く、最低コスト対応と、多少の余裕対応を併用して提案。最終的には、年度末直前に判断。

【選定理由】

児童教育コンテンツを作成、使用、教育実習で実践し、それを各種の教育事業者に提供するビジネスモデル。それらのコンテンツを改善、確認し、改良を加えながら展開する。このためコンテンツの最新系を保存し、展開先を秘匿するだけのセキュリティで十分。このためこれらの情報のみをその都度の経済状況で分離することから機密保持は開始する予定。また、商工会議所の会員のためその属性が活かせることも選定の条件。



【選定理由】

・売上とコストがギリギリで当面は多額の月額の出費は無理
　＝＞現状、先々で対応が異なっても致し方ない
・秘密にすべき（各種客先、自社コンテンツ）情報の取り扱いは微量膨大ではない
　=>個別に保存可能
・商工会議所会員
　＝＞商工会議所会員のメリットが出れば

【検討結果】

　今年度の決算次第で　まずは端末型で個別を守り、余裕が見えてきた段階で
UTM+EDR に展開することになりそう。

順番	候補	評価点	コメント
A	商工会議所 サイバーセキュリティお助け隊サービス	65	
B	「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）」	45	評価点数的には高いが　運用を実施するには この会社には不向き（運用者の技術力不足）

		サービス名称		商工会議所サイバーセキュリティお助け隊				マイセキュアビジネス			
		提供会社		大阪商工会議所				NTTコミュニケーションズ			
	評価項目	評価基準	配分点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数	研究会の評価点	企業の重みづけ	重みづけ反映評価点	合計点数
1	サービス提供力	全国の主要都市をカバーしている。	5	5	1	5	5	5	1	5	5
		自社の拠点だけでなく、販売代理店など顧客との接点（相談窓口）を増やして、サービスのサポート体制を整えている。	5	5	0	0		0	0	0	
2	既存のシステム環境への影響	既存の端末構成に対する制約が少ない。 ①.Windows以外の端末もサポート対象。 ②.サポート対象外の旧バージョンもサポート対象。 ③.導入済みのウイルス対策ソフトとコンフリクトしない。	15	10	1	10	10	5	1	5	5
3	平常時の対応レベル	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	5	5	1	5	5
		定期的報告(レポートやメール)が週次に送付される。	5	0	1	0		0	1	0	
4	異常発生時の対応レベル	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	15	5	2	10	10
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	0	2	0		0	2	0	
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	0	1	0		0	1	0	
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5		0	1	0	
5	費用一式	年額換算費用が、以下のIPA要件(基準)の60%以下である。 ※端末監視型：月額2.2千円/台以下	10	10	1	10	20	10	1	10	10
		初期費用などの追加費用がない。	10	10	1	10		0	1	0	
6	保険	損害賠償も補償の対象となっている。	5	5	2	10	10	5	2	10	15
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	0	1	0		0	1	0	
		補償金額の上限が200万円/年以上である。	5	0	1	0		5	1	5	
7	導入実績	使用されているEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	1	5	5	0	1	0	5
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	0	1	0		5	1	5	
	合計点数⇒		115	65		70	70	45		55	55

総合コメント	価格を抑えるため保険補償額は最小限(年間30万円）各地の商工会議所やIT事業者と連携して駆け付けサービスを充実。事故時の現場復旧対応に力を入れた.	初期費用がすくなく月次使用料が格安のためすすめやすい。ほかのセキュリティソフトも共有できるため、現在の環境を変えずに試しで使用しやすい

4 .5 事例（作成者：高山）

【企業の状況】

業種　　：製造業

拠点数　　：4 箇所（工場 3 箇所）

PC 台数と OS　　：50 台（WIN10）

PC の持ち出し　　：有(営業、自宅でのテレワーク)

ウイルス対策ソフト　：有(PC、UTM)

ネットワーク対策　　：有(UTM 設置済)

※現在のＵＴＭ

有①アンチウイルスソフト

有②ファイアウォール

有③アプリケーション制御

有④リモートアクセス　ＶＰＮファイアウォール

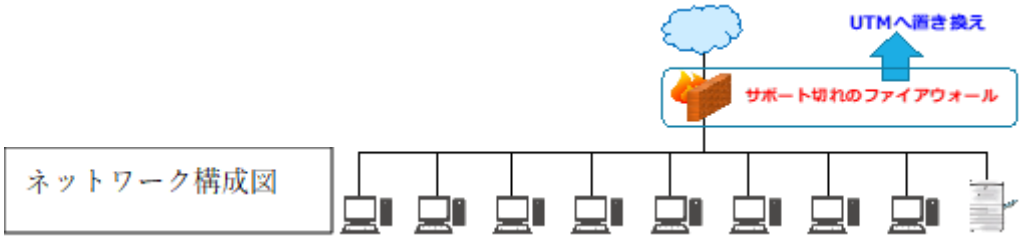
外部から社内への接続：有（工場から）

万が一の際の対応　　：内容　社内に IT チームを組織化中であるが、現在は推進する従業員が進んで行っている。

頼めるＩＴベンダーもあるが、あまりＩＴベンダーとの関係がよくない

【提案したサービス】

お助け隊サービス名称（大阪商工会議所）



【選定理由】

EDR も選定を考慮したとき、PC スペックの問題で（ほかの業務ソフト運用でも不具合あり）現状でも動きが遅い PC があり EDR を入れることが懸念されている。

事務所内での PC がほとんどのため、UTM をいれる大阪商工会議所のサービスであると個別の PC のスペックはかかわらないため導入が可能である。

【企業での検討結果】

セキュリティについて大切なことを認識しているが、企業内の IT 化（ＰＣ入れ替え、業務ソフトとバックヤードソフトの変更）が急務のため、PC 入れ替えの前に対策できる UTM で安価な大阪会議所のお助け隊が選定された。

商工会議所	105 点	採用　点数も高く希望条件にあった
防検サイバー	60 点	不採用　EDR のため希望にあわない
AXIS	100 点	不採用　実績の点で不採用

		提供会社		大阪商工会議所					三井物産セキュアディレクション株式会社					株式会社アクシス				
評価項目	配分点数	評価基準	配分点数	研究会の評価点	企業の重み付け	重み付け反映評価点	合計点数	コメント	研究会の評価点	企業の重み付け	重み付け反映評価点	合計点数	コメント	研究会の評価点	企業の重み付け	重み付け反映評価点	合計点数	コメント
サービス提供力	10	全国の主要都市をカバーしている。 ※主要都市に自社の拠点が無くても、サービス対象地域としていればよい。 ※島しょ部を除く	5	5	1	5	10		5	1	5	10		5	1	5	5	
		自社の拠点だけでなく、販売代理店など顧客との接点（開設窓口）を増やして、サービスのサポート体制を整えている。	5	5	1	5		申請約12 会社24	5	1	5			0	1	0		
既存のシステム環境への影響(導入検討の前提となるシステム要件) ※端末とネットワークの保有型サービスについては、既存を評価し、結果として配分点数は他の30点とする。(30点とする妥当性については、別途検討する)	15	【端末型(EDR)】 以下の3点から既存の端末構成に対する制約が少なく、幅広い端末で利用可能。 ①Windows以外の端末(MAC、Linux)もサポート対象としている。 ②現在サポート対象外の旧バージョンもサポート対象としている。 ③PCに導入済みのウイルス対策ソフトとコンフリクト(競合してPCが動かなくなる)しない。	15	0	0	0	30		10	0	0	0		0	0	0	30	
		【ネットワーク型(UTM)】 ①既存のシステム(ネットワーク)環境に影響を与えずに導入でき、機能を補完し合って使える。 ②システム(ネットワーク)環境に修正を要しても、既存の機器が不要となり、コストを削減(抑制)できる。	15	15	2	30		ウイルスソフトは必要	0	2	0			15	2	30		
平常時の対応レベル	10	監視状況を常時、企業側の管理端末やレポートで確認できる。	5	5	1	5	10	チェック出来る	5	1	5	10		5	1	5	10	
		定期的報告(レポートやメール)が遅滞なく送付される。	5	5	1	5		異常時のレポートのみ	5	1	5			5	1	5		
異常発生時の対応レベル	20	異常検知時に即時にメール通知や管理端末へのアラート表示がある。	5	5	2	10	20	重要アラート時には30分遅	5	2	10	25		5	2	10	20	
		異常検知時の窓口対応(リモート対応)が24時間365日可能である。	5	5	1	5		平日日中のみ	5	1	5			5	1	5		
		駆け付け対応の時間帯が24時間365日可能である。 ※現地に駆け付けるまでの時間は対象外とする。	5	0	1	0		重要アラート時は関係事業者が駆け付け	5	1	5			0	1	0		
		被害拡大阻止や原因究明だけでなく、マルウェアの駆除や復旧までの支援が得られる。	5	5	1	5		駆け付けて実施	5	1	5			5	1	5		
費用一式	20	年経換算費用が、以下のIPA要件(基準)の60%以下である。 ※ネットワーク装置視型：月額1.1万円以下 ※端末監視型：月額2千円/台以下 ※併用型：上記の和を超えないこと	10	10	1	10	20	台当月額6,000円 台当月3,200円	0	1	0	0		10	1	10	10	
		初期費用などの追加費用がない。	10	10	1	10		伝播する機台160,000円	0	1	0			0	1	0		
保険 ※中小企業の費用負担を軽減する意味から、評価基準を3点あげて配分点数を高めた。	15	損害賠償も補償の対象となっている。	5	0	1	0	5	ない	5	1	5	10		5	1	5	15	
		駆け付けサービスの費用補てんにおいて、マルウェアの駆除や復旧までの支援費用が対象となっている。	5	5	1	5		最大4時間まで	5	1	5			5	1	5		
		補償金額の上限が200万円/年以上である。	5	0	1	0		ない	0	1	0			5	1	5		
	10	使用されているUTM機器やEDRソフト、監視サービスなどの提供会社の情報が明記され、仕様や性能、実績などの情報が得られる。	5	5	2	10	10	UTMはNEC製	0	2	0	5		5	2	10	10	
		お助け隊サービスとしての導入実績数や具体的な事例紹介などの情報が、Webなどで公開されている。	5	0	1	0		ない	5	1	5			0	1	0		
合計点数＝	100		115	80		105	105		65		60	60		75		100	100	

おわりに

２年間にわたって私共のテーマ研究活動にご協力いただいた、サイバーセキュリティお助け隊サービス提供者の皆様、また、昨年度のテーマ研究成果報告の場で私たちの提案を受け止め、暖かく励ましていただき、中小企業・小規模事業者の皆様のために更なる「お助け隊サービス」の募集・拡充を推進しておられる IPA セキュリティセンターの皆様に心から敬意と謝意を表します。