経済産業省

サイバーセキュリティお助け隊サービスについて

商務情報政策局

サイバーセキュリティ課

医療機関におけるお助け隊サービス導入事例①
～無床、職員約20名の診療所～

「サイバー被害にあった」ことがセキュリティ対策のきっかけに！外部からの攻撃をシャットアウトしてくれるという信頼感とセキュリティ対応の定期レポートで安心感が格段に向上！

導入のきっかけ

過去に小さなセキュリティインシデントを経験しました。また、医療機関でのセキュリティインシデントの報道等もあり、危機感を持っていました。そこで、院内でセキュリティに関するルールを定め、さらにUTMの設置を検討しましたが、1台100万円～150万円の導入費用に加え、月額数千円～1万円の運用費がかかるものもあることを知り、高額なのであきらめかけていたところ、「お助け隊サービス」の存在を知り、すぐに導入を決めました。

導入したサービス

お助け隊サービスの「ネットワーク監視」サービスを導入し、 UTM （統合脅威管理）※機器を設置しています。

※UTMとは、複数の異なるセキュリティ機能を1台の機器に統合して、機器の管理や運用の負担を低減すると共に、集中的なネットワークの脅威管理を実現する、セキュリティ機能を集約した機器です。

お助け隊サービスの良いところ

外部からの攻撃をシャットアウトしてくれるという信頼感と、定期的レポートによって異常な攻撃がなかったことを確認できる安心感があります。

医療機関におけるお助け隊サービス導入事例②

～複数拠点を持つ約280床、職員約250人の病院～

組織における「DX推進の取組の一環」としてサイバーセキュリティお助け隊サービスを導入！
内部PCの状況や外部通信が可視化され、状況把握に活用！

導入のきっかけ

数年前から、内部にDXワーキングを組織し、セキュリティ確保について進めています。DXワーキングの顧問の方からサイバーセキュリティ対策について推奨され、UTMの導入を検討している中で、以前から付き合いがある事業者がお助け隊サービスの提供事業者であったこともあり、お助け隊サービスを導入することにしました。

導入したサービス

お助け隊サービスの「ネットワーク監視」サービスを導入し、 UTM （統合脅威管理）※機器を設置しています。

※UTMとは、複数の異なるセキュリティ機能を1台の機器に統合して、機器の管理や運用の負担を低減すると共に、集中的なネットワークの脅威管理を実現する、セキュリティ機能を集約した機器です。

お助け隊サービスの良いところ

安価で、既存システムの大掛かりな変更なく導入できる利便性が良いところ。月に１回のレポートで、このパソコンが危ない、この部署が危ないということや、外部クラウドストレージへの通信状況等、ネットワーク全体の動きや注意点を可視化できるようになり、院内のセキュリティ対策の状況把握に役立っています。

サイバーセキュリティお助け隊サービスの種類

サイバーセキュリティお助け隊サービスには、監視種別とサービス価格によって、複数の種類があり、それぞれに登録されたサービスがあります。

ネットワーク監視（１類）

社内ネットワークに監視製品（UTM等）を設置し、ネットワーク通信を監視します。

サービス例(価格は税抜き)

初期費用:20,000円、月額費用:8,800円、初年度費用:125,600円
監視可能端末数:20台

併用（１類）

ネットワーク監視と端末監視を併用し、ネットワークとPCの両方を監視します。

サービス例(価格は税抜き)

初期費用:198,000円、月額：ネットワーク監視10,000円＋　端末監視2,000円/台、初年度費用※：342,000円～、監視可能端末数:30台　※監視対象PC1台の場合

端末監視（１類）

PCへ監視製品（EDR等）をインストールし、個々のPCの通信や挙動を監視します。

サービス例(価格は税抜き)

初期費用:0円、月額費用:750円/台、初年度費用※:9000円~
※監視対象PC1台の場合

２類

お助け隊サービス1類をベースに監視機能の強化や定期的なコンサルティングの実施、監視端末数の拡充等を要件とした類型

サービス例(価格は税抜き)

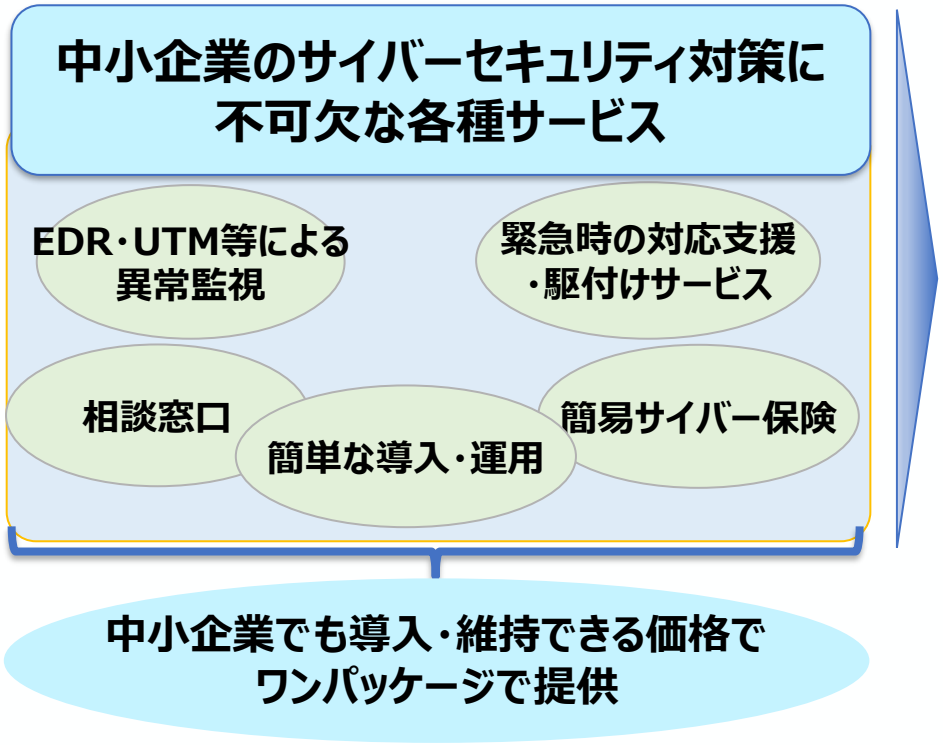
初期費用:65,900円～、ネットワーク監視22,500円＋端末監視600円/台、初期費用※:343,100円～、監視可能端末数:100台　※監視対象PC1台の場合

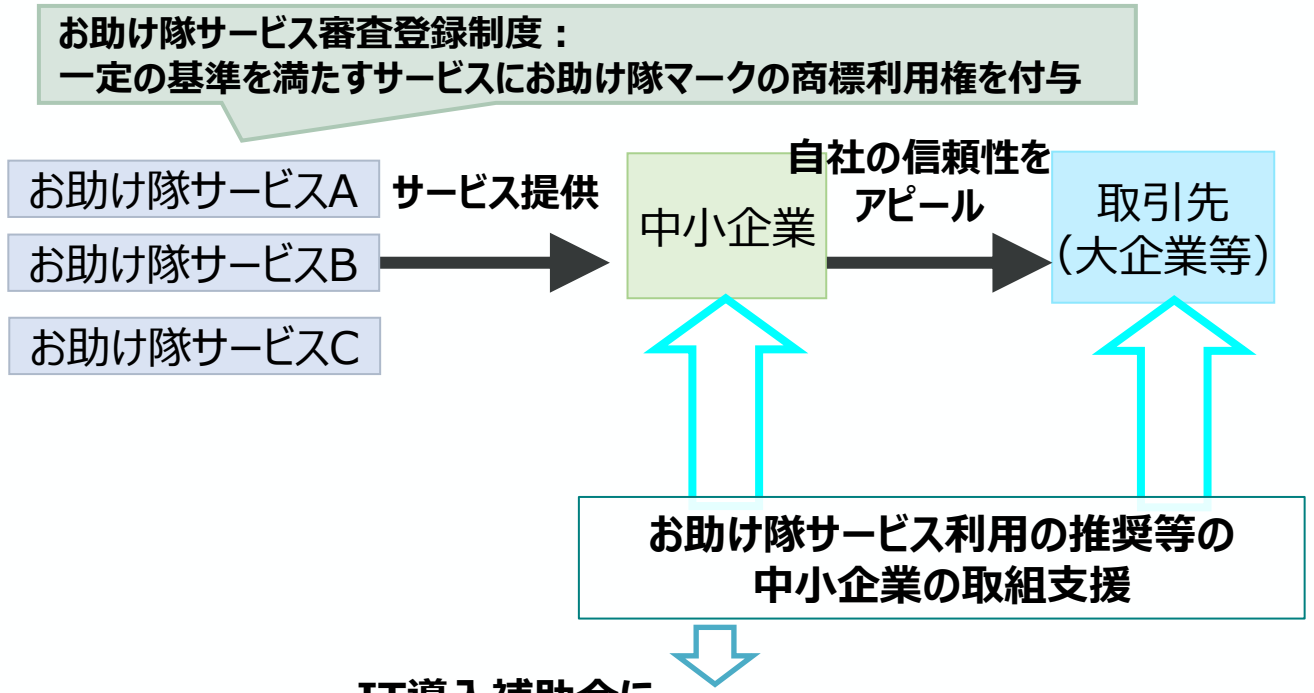
IPAホームページでは、お助け隊サービスの価格や提供地域を監視種別ごとに一覧としてまとめています。

https://www.ipa.go.jp/security/otasuketai-pr/hikaku/index.html

サイバーセキュリティお助け隊サービス

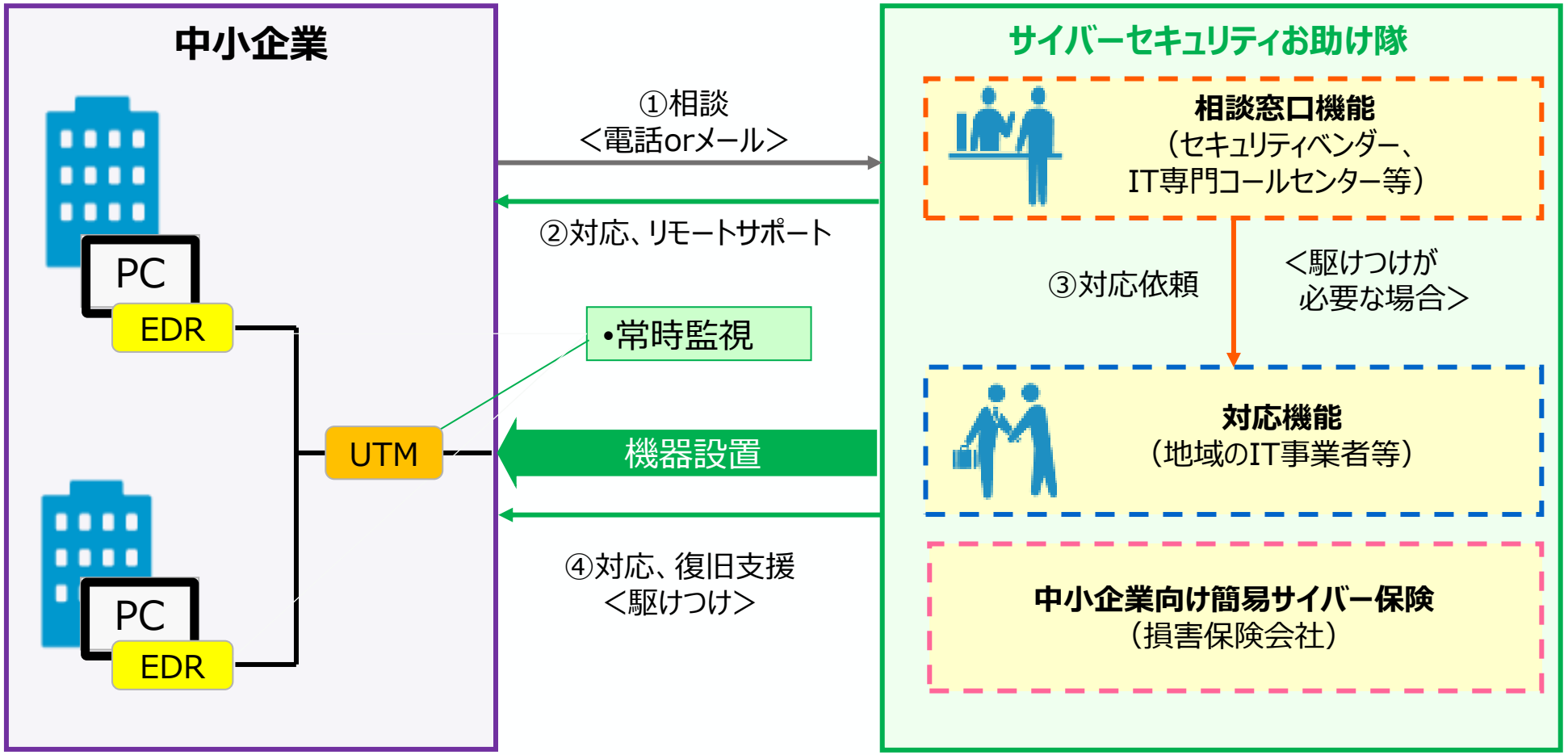
- 中小企業に対するサイバー攻撃への対処として不可欠なサービス（見守り、駆付け、保険）をまとめた、民間の事業者から提供されるサービス。**中小企業が利用しやすい安価で提供。**
- IT導入補助金「セキュリティ推進枠」でお助け隊サービス**導入費用を補助**（補助率：1/2）。





お助け隊サービスの提供イメージ

- 中小企業にUTM（ネットワーク監視機器）、EDR（端末監視機器）のセキュリティ監視ツールを設置し常時の異常監視を行うとともに、①相談窓口による導入・運用に関するユーザーからの各種相談の受け付け、必要に応じて②リモートでの支援や③駆けつけ支援などを実施。



サイバーセキュリティお助け隊サービス　事業者・登録サービスリスト

全国各地域の中小企業にとって選択・利用可能な**「サイバーセキュリティお助け隊サービス」のリスト**。40事業者がサービスを登録・提供中（2024年11月時点）。

	事業者名(サービス名称)
1	**大阪商工会議所** （商工会議所サイバーセキュリティお助け隊サービス）
2	**ＭＳ＆ＡＤインターリスク総研株式会社** （防検サイバー）
3	**株式会社ＰＦＵ** （PCセキュリティみまもりパック）
4	**ＳＯＭＰＯリスクマネジメント株式会社** （SOMPO SHERIFF）
5	**株式会社アイティフォー** （ランサムガード）
6	**富士ソフト株式会社** （オフィスSOCおうちSOC）
7	**株式会社BCC** （セキュリティ見守りサービス「＆セキュリティ＋」）
8	**中部事務機株式会社** （CBM ネットワーク監視サービス）
9	**中部電力ミライズ株式会社** （中部電力ミライズ　サイバー対策支援サービス） （中部電力ミライズサイバー対策支援サービス エンドポイントセキュリティ） （中部電力ミライズサイバー対策支援サービス デュアル防御）
10	**セントラル警備保障株式会社** （ＣＳＰサイバーガード）
11	**株式会社コハマ** （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） （ネットワークセキュリティ見守り隊）
12	**セキュアエッジ株式会社** （セキュアエッジＭＤＲ９９）
13	**株式会社大塚商会** （Cloud Edge運用支援EasySOC Plus　パック）
14	**コスモテレコム株式会社** （ビジネスサポートサービス） （ビジネスサポートサービスS7）

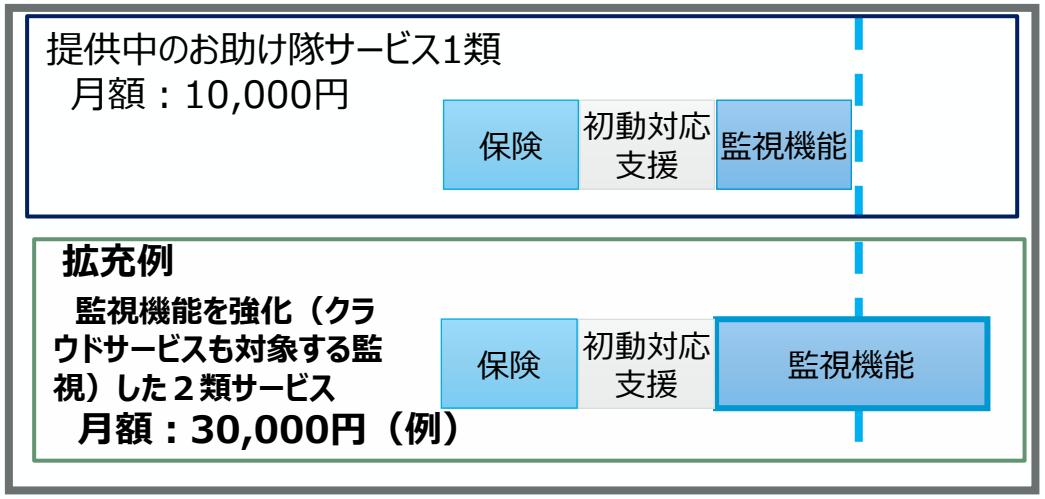
	事業者名(サービス名称)
15	**京セラドキュメントソリューションズジャパン株式会社** （TASKGUARD UTM CP セキュリティーサービス）
16	**三井物産セキュアディレクション株式会社** （MBSD Global Security Platform（略称：MGSP））
17	**ラディックス株式会社** （ラディックスお助け隊サービス） （ラディックスお助け隊サービスPlus）
18	**株式会社四日市事務機センター** （YONJINサイバーセキュリティ UTM） （YONJINサイバーセキュリティ UTM&EDR）
19	**株式会社ハイテックシステム** （TSOCエンドポイントパッケージ）
20	**株式会社アクシス** （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 －小規模ネットワーク＆端末監視コース －端末監視コース
21	**富士フィルムビジネスイノベーションジャパン株式会社** （beat/solo 見守りサービス）
22	**株式会社アクト** （データお守り隊）
23	**株式会社ケーオウエイ** （サイバーセキュリティお助けパック）
24	**株式会社ソフトクリエイト** （SecurityFREEレスキュー隊 for PC監視）
25	**グローバルセキュリティエキスパート株式会社** （サイバードラレコ）
26	**株式会社ブロードバンドセキュリティ** （サイバープロテクション（CP））
27	**ステラグループ株式会社** （ステラお助け隊サービス）

	事業者名(サービス名称)
28	**田中工業株式会社** （小規模/中規模ネットワークセキュリティパッケージ） （ネットワークパトロール（S）/（M））
29	**バリオセキュア株式会社** （セキュリティお助けパック（ネットワーク）） （セキュリティお助けパック（ネットワーク＆端末））
30	**タクテックス株式会社** （タクテックスセキュリティサービス） （タクテックスセキュリティサービス＆PC見守り隊サービス）
31	**株式会社CISO** （CISO EDR+マネジメントサービス）
32	**株式会社ワールドスカイ** （お助け侍）
33	**株式会社ビープラス** （スマートセキュリティ）
34	**株式会社アクト** （アクトサイバーサポート）
35	**東日本電信電話株式会社** （おまかせサイバーみまもり） （おまかせサイバーみまもり　おまかせアンチウイルスEDRプラス）
36	**Sエナジーユニオン** （S E security）
37	**FIRAセキュリティ** （FIRAネットワーク監視サービス）
38	**日本通信機器株式会社** （Security Net Keeper Plus）
49	**株式会社奈良事務機** （奈良事務機サイバー攻撃見守りサービス（ベーシック）） （奈良事務機サイバー攻撃見守りサービス）
40	**株式会社清芳屋** （セイホウヤ　ネットワークセキュリティ見守り隊サービス） （セイホウヤ　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）

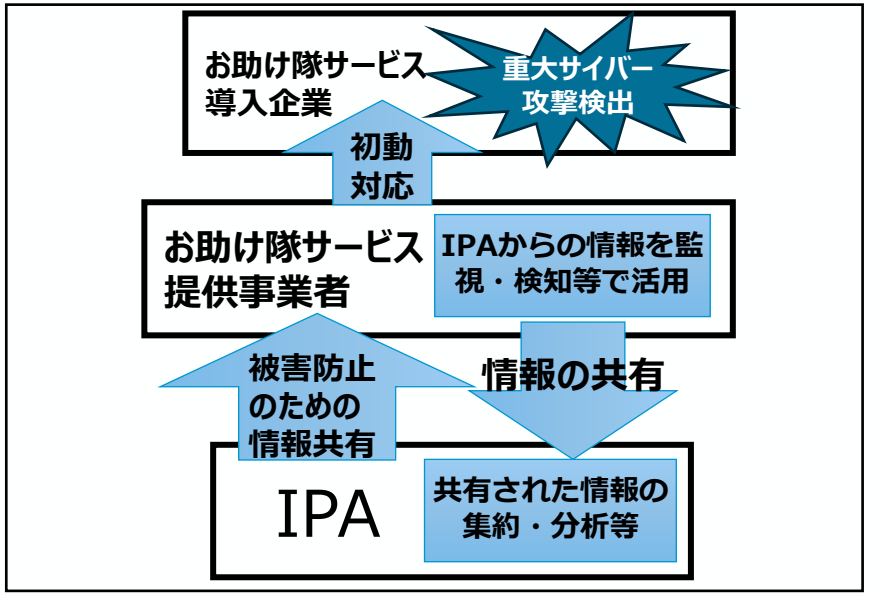
サイバーセキュリティお助け隊サービスの新たな類型（２類）について

- 現行のお助け隊サービス（１類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであるところ、**中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（２類）の検討を実施。**
- 現行のお助け隊サービスのコンセプトは維持しながら、**価格要件を緩和しつつ、提供中のお助け隊サービス１類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として、基準の改定を実施**（2024年３月15日に公開）。
- **令和６年度以降、２類サービスの基準への適合性審査を開始し、適合した２類サービスを登録、公表予定。**厚生労働省等の**関係機関や業界団体とも連携しながら、お助け隊サービスの更なる普及、促進を図る。**

2類のイメージ



IPAとの情報共有イメージ



（参考）IT導入補助金による「サイバーセキュリティお助け隊サービス」の導入支援

- 「通常枠」及び「インボイス対応類型」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」をメインツールと組み合わせて申請することが可能。この際、「サイバーセキュリティお助け隊サービス」を申請する事業者については、**申請採択における審査時に加点対象**になっている。
- 2022年８月から、新たに「セキュリティ対策推進枠」を創設。**「サイバーセキュリティお助け隊サービス」のみでの補助金申請が可能**になっている。

IT導入補助金2024概要

メインツールと組み合わせて、**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」**を申請可能。

「サイバーセキュリティお助け隊サービス」のみで申請可能。

	通常枠	インボイス枠 インボイス対応類型	セキュリティ対策推進枠
要件	業務効率化やDXの推進等に資するITツールを導入	インボイス制度に対応した会計・受発注・決済の機能を有するITツール及びそのためのハードウェアを導入	サイバーセキュリティお助け隊サービスを導入
補助上限	ITツールの業務領域が 1～３まで：5万円～150万円 4以上：150万円～450万円	ITツール： １機能：～50万円 ２機能以上：50万～350万円 PC・タブレット等：～10万円 レジ・券売機等：～20万円	5万円～100万円
補助率	中小企業：１/２	～50万円以下：3/4 (小規模事業者：4/5) 50万円～350万円：2/3 ハードウェア購入費：1/2	中小企業：1/2
対象経費	ソフトウェア購入費、 クラウド利用料（最大2年分）、 導入関連費	ソフトウェア購入費、 クラウド利用料（最大2年分）、 導入関連費、 ハードウェア購入費	**サイバーセキュリティお助け隊サービス利用料（最大2年分）**
	オプションとして**「サイバーセキュリティお助け隊」を申請した場合、利用料の1年分（「サイバーセキュリティお助け隊」導入は加点要素）**		

IT導入補助金のインボイス枠(電子取引類型)、複数社連携IT導入枠においては、サイバーセキュリティお助け隊サービスは補助等の対象外である。

（参考）サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「**ランサムウェア攻撃**」やセキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「**サプライチェーンの弱点を悪用した攻撃**」により、甚大な影響が生じている。また国家支援型の攻撃集団等が特定の企業を執拗に狙う「**標的型攻撃**」も大きな課題。
- 社会のデジタル化は進展する一方、AI等のデジタル技術の発展や地政学情勢の不安定化の影響もあり、**サイバー攻撃は今後ますます増加するとともに高度化・複雑化していくおそれ**。

情報セキュリティ10大脅威 2024

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	内部不正による情報漏えい等の被害
4位	標的型攻撃による機密情報の窃取
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	不注意による情報漏えい等の被害
7位	脆弱性対策情報の公開に伴う悪用増加
8位	ビジネスメール詐欺による金銭被害
9位	テレワーク等のニューノーマルな働き方を狙った攻撃
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2024.1.24>

デジタル技術の発展によるサイバーリスクの増加の例

■　情報システムの利用拡大やクラウド等の活用拡大、インターネットに接続されるIoT製品の急増（2019年：231億台⇒ 2024年：399億台）など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

■　スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成AI ツールも登場**。

□　NICTER において2023年に観測した**サイバー攻撃関連通信数は増加傾向**であり、約6,197億パケット（2018年の約３倍）。中でも、**IoT機器を狙った攻撃関連通信が多い**。

□　フィッシング対策協議会によると、2023年における**フィッシングの報告件数は100万件超**（2019年の約20倍まで増加）。

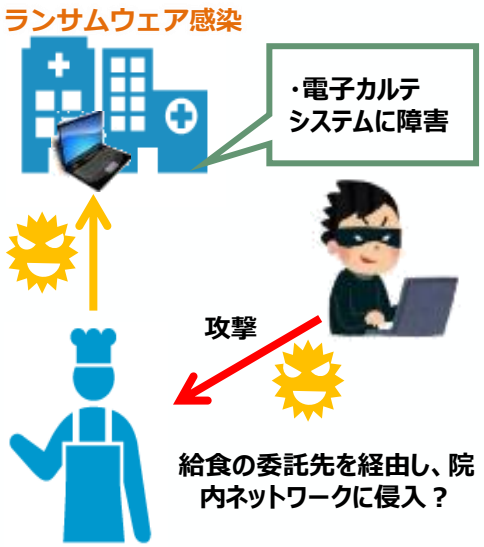
<出典：総務省「令和５年度版情報通信白書データ集」、(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2024」解説書、(国研)情報通信研究機構「NICTER観測レポート2023」、フィッシング対策協議会「月次報告書」 等>

（参考）取引先を通じたサイバー攻撃の被害の事例

- 国内の公立病院や大手自動車会社において、直接サイバー攻撃の標的とされない場合であっても、**取引先に対するサイバー攻撃により、操業を停止するケース**が発生。

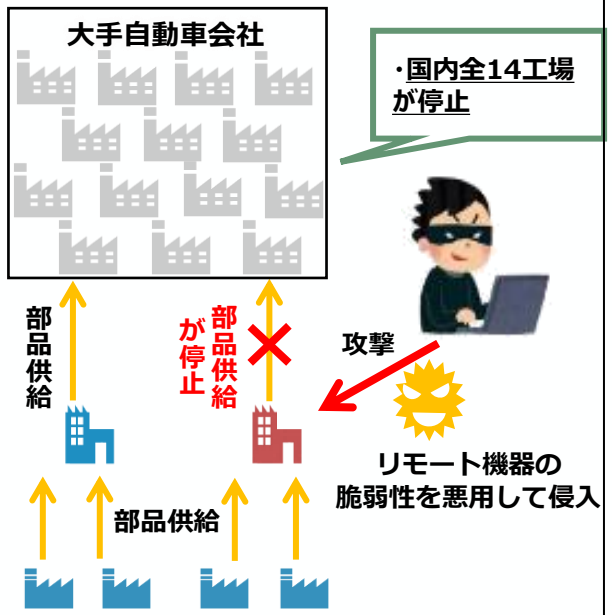
事例①

- 2022年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生**し、**緊急以外の手術や外来診療が一時停止する等**通常診療ができない状況に。
- **病院の給食を委託していた業者のサーバーからウイルスが侵入**した可能性が高いとみられている。
- ２ヶ月超にわたり通常診療を見合わせ。



事例②

- **大手自動車会社の取引先企業**のサーバー等がランサムウェアに感染。更なる感染拡大を防ぐため、**全サーバをネットワークから切断し、全てのシステムを停止し、受注困難**になった。
- 大手自動車会社は、部品供給の停止により、**全国の工場で生産が困難**になったため、1日間の稼働停止を余儀なくされ、 約1万台強の生産に影響。



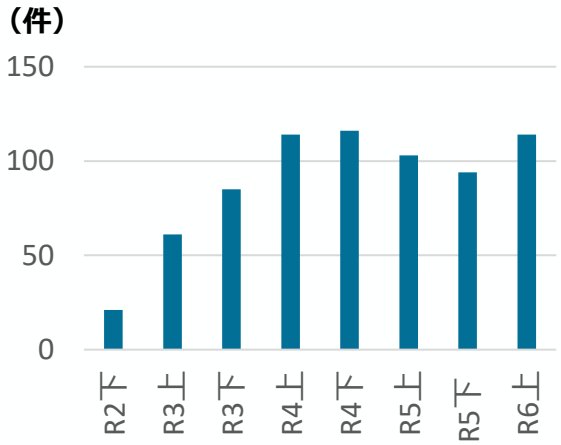
（参考）中小企業に対するサイバー攻撃の現状

- 近年、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、**中小企業自身**及びその**取引先である大企業等への被害が顕在化**している。
- 過去に取引先等がサイバー攻撃の被害を受け、**自社に被害が及んだ経験があると回答した企業は２割**。

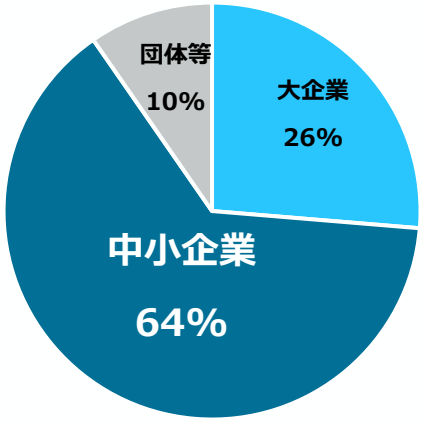
中小企業に対するランサムウェア攻撃が増加

- サイバー被害（ランサムウェア被害）は右肩上がりに増加。
- 被害件数114件の内訳は、大企業が30件（26%）に対して、中小企業は73件（64%）と6割を占める。

企業・団体等における ランサムウェア被害の報告件数



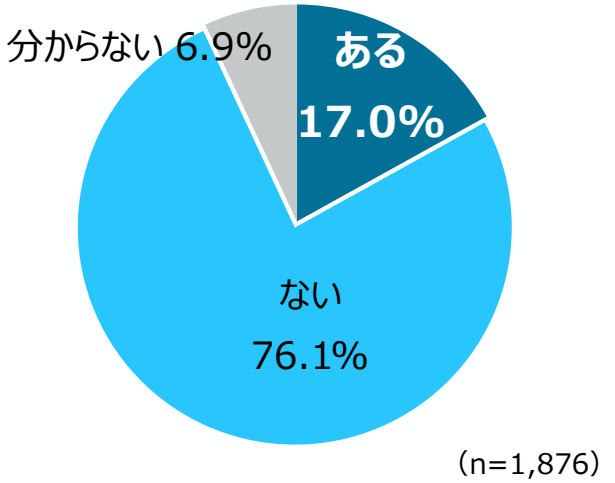
ランサムウェア被害企業等の 規模別件数



<出典：令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について>

取引先等を経由したサイバー攻撃被害の経験

過去に取引先等がサイバー攻撃の被害を受け、それが自社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



出典：令和３年度企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査

（参考）中小企業へのサイバー攻撃状況 ～サイバーセキュリティお助け隊実証事業の結果～

- 1,064社が参加した実証期間中に、全国８地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。

・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

＜実証参加の成果（参加中小企業のアンケート結果より）＞

- アラート通知が実際にあり、**他人事ではないとの意識につながった**。（大阪府・建設業）
- 参加することで、情報セキュリティ対策を実施していることを、**外向けにアピールできる**のが良い。（新潟県・電気通信工事業）
- 総務担当がセキュリティを兼務していることもあり、**ワンパッケージでやってくれると非常に助かる**。（石川県・製造業）