サプライチェーン全体で サイバーセキュリティ対策強化を

～サイバーセキュリティお助け隊サービスの活用～

MS＆ADインターリスク総研株式会社
リスクコンサルティング本部 リスクマネジメント第三部
危機管理・サイバーリスクグループ
マネジャー上席コンサルタント
槇 健介（まき けんすけ）

要旨

- サイバーセキュリティお助け隊サービス制度は、サイバーセキュリティ対策が遅れがちな中小企業が利用しやすいサービスを、独立行政法人情報処理推進機構（IPA）が審査・登録する制度である。
- 基準の改訂や拡大を経て、新たに高度な機能を追加したサービス類型である2類サービスが追加された。
- サプライチェーン全体での取り組みの推奨や、IT導入補助金など補助金制度との連携により、経済産業省はじめ政府機関や業界団体により普及が推進されている。
- 発注者を含めたサプライチェーン全体でサイバーセキュリティ対策を強化するための制度活用イメージ等について情報提供するとともに、制度普及のために期待される施策について述べる。

1 サイバーセキュリティお助け隊サービス制度の概要

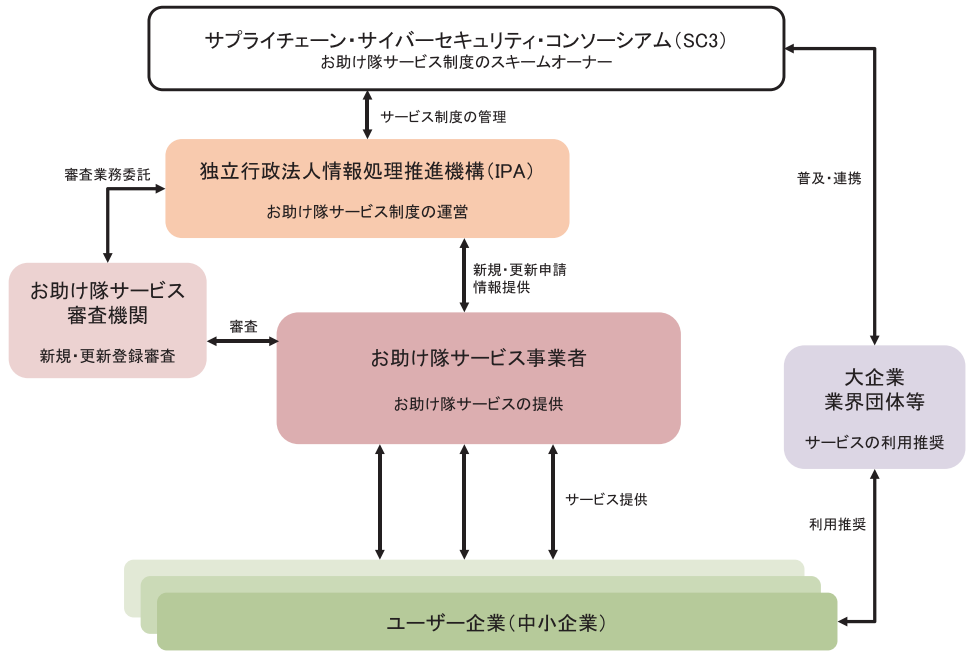
サイバーセキュリティお助け隊サービス（以下、「お助け隊サービス」）制度は、その前身となるサイバーセキュリティお助け隊実証事業から発展した。この実証事業は、中小企業におけるサイバーセキュリティに対する意識を高め、その実態に適した対策を検証し、使いやすいサービスを実現することを目指して、2019年から2年間実施された。

この実証事業を通じて創設されたお助け隊サービス制度は、SC3（サプライチェーン・サイバーセキュリティ・コンソーシアム：産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的とした組織）がスキームオーナーとして制度を統括し、IPAが制度運営を担い、お助け隊サービス基準を満たした民間事業者のサービスを審査し、登録している（次頁図1）。この制度は2021年3月に最初の五つのサービスとともに開始され、2024年5月現在で57のサービスが登録されている。

お助け隊サービスは、中小企業のサイバーセキュリティ対策を支援するための相談窓口、異常の監視、事案発生時の初動対応（駆付け支援等）および簡易サイバー保険といったサービスを提供している。これらのサービスは、中小企業の事業環境の実情に基づいて、安価かつ効果的なワンパッケージにまとめられ、確実に提供されることを基本コンセプトとしている。

さらに、国の補助金制度であるIT導入補助金に「サイバーセキュリティお助け隊サービス推進枠」という専用の補助金枠が設けられており、経済産業省もこのサービスの普及を後押ししている。

主なユーザーとなる中小企業は、経済産業省やIPAが認めた、中小企業が必要最小限備えるべき対策を満たしたサービスの中から、自社に合ったものを選び、安心して利用することができる。



【図1】お助け隊サービス制度のスキーム概要　（MS&ADインターリスク総研作成）

2 お助け隊サービス基準

(1)サービス基準

お助け隊サービス基準（次頁表1）とはセキュリティサービスを提供する事業者が満たすべき基準である。これは過去3回改訂され、2024年5月現在「2.0版」が最新となっている。直近の改訂では、現行サービスよりも高度な監視機能やセキュリティサービスを必要とする中規模以上の中小企業のニーズに対応するため、「2類サービス」が新たに設けられた。これは主に価格要件を緩和し、現行サービスを基盤に監視機能の強化や定期的なコンサルティングの実施など、サービスを拡充したもの。「2類サービス」の創設に伴い、現行サービスは「1類サービス」とされた。

なお、「2類サービス」を提供するためには、「1類サービス」の提供が必須とされている。「2類サービス」は、「1類サービス」の上位プランという位置付けであり、既に提供・運用している「1類サービス」に高度なサービスが付加された形となる。現行基準において「2類サービス」のみを提供する事業者は存在しない。

(2)サービス基準のポイント

お助け隊サービス基準は、セキュリティサービスを提供する事業者が満たすべき基準であるが、ユーザーである中小企業がサービスを選定する際の「判断材料」という観点で、お助け隊サービス基準の主なポイントについて、表1に基づき解説する。

①サービス機能

表1の「1. 相談窓口」～「6. ワンパッケージ提供」は、お助け隊サービスの機能そのものであり、ユーザー自社内運用に関わる内容であるため、ユーザーは自社に導入する前に、特に確認することを推奨する。

お助け隊サービスとして登録されている以上、基準を満たしていることは間違いないのだが、個々のユーザーにとっての使いやすさや、ユーザーが求めるサービスレベルであるかどうかは確認が必要となる。サービス提供事業者によっては試用期間を設けて、サービスの導入テストが可能な場合もある。

また、基準では定められていない項目として、例えば「保管されるログの範囲や保存期間」「他のセキュリティツールとの併用可否」「対象となるデバイスの仕様」など、同じお助け隊サービスであってもサービスによって異なるため、事前に確認することを推奨する。

②価格

表1の「8. 価格」において、サービス提供事業者が提供するサービス価格の上限値を定めており、最低契約台数や最長契約期間についても上限（あるいは下限）を定めている。こうしたサービス基準において、価格要件が設定されていることは稀で、

お助け隊サービス制度の特徴といえる。

お助け隊実証事業を通じて、主なユーザーとなる中小企業にとってサイバーセキュリティ対策を進める上で、サービス価格（コスト）が大きな判断要素であったことから、サービス基準の中に価格要件が設定された経緯がある。

価格要件が設定されることは、ユーザーにとって低コストで導入できる利点がある一方、より高い機能を求めるユーザーにとっては、サービス内容が物足りない場合がある。また、サービス提供事業者側にとっては、より高い機能を盛り込みたくても、価格要件の存在により費用対効果を考慮するとサービスレベルを制限せざるを得ないジレンマが生じている。

こうした状況を受けて、より高度な機能等を追加し、価格要件を部分的に撤廃した「2類サービス」が導入された経緯がある。

ユーザーは、お助け隊サービスの導入検討時には、価格に見合ったサービスであるかどうか事前に確認することを推奨する。

③信頼性

表1の「9. サービス提供実績」「12. 情報共有」「13. 事業継続性」「15. 法令遵守」などは、サービス提供事業者やサービスの信頼性に関する基準である。これらの基準はユーザーからしてみれば、サービス提供事業者が当然満たすべき内容が大半であろう。

サービス提供事業者は、ＩＰＡへの新規審査または更新審査の際に、これらの信頼性を裏付ける資料を提出することが義務付けられている。

【表1】お助け隊サービス基準

No.	要件	概要	1類	2類
1	相談窓口	一元的な問い合わせ窓口がある	○	○
2	異常の監視	24時間監視・検知・通知する	○	○
3	緊急時の対応支援	技術者による緊急時の対応支援を行う	○	○
4	導入・運用の簡単さ	専門知識なく導入・運用できる工夫がある	○	○
5	簡易サイバー保険	初動対応の費用を補償する簡易サイバー保険が付帯されている	○	○
6	ワンパッケージ提供	上記1～5の機能を一元的に購入可能	○	○
7	拡充要件（2類）	1類サービスに加えて以下のいずれかを拡充すること • 監視対象端末の増加 • クラウドサービスの監視 • 異常監視機能の追加 • 月1回以上提供するサービスの拡充	－	○
8	価格	初期費用は50万円以下 ネットワーク一括監視型月額1万円以下 端末監視型1台あたり月額2,000円以下 ※最低契約台数は1台、年数は2年以内	○	－
		ユーザー概況に照らして相応かつ妥当な額 ※最低契約台数は1台、年数は2年以内	－	○
9	サービス提供実績	類似のサービスを提供・運用した実績がある	○	－
		1類サービスを提供・運用した実績がある	－	○
10	1類サービスの継続	1類サービスを提供し続けること	－	○
11	2類サービスの妥当性・適時性	2類サービスの内容がユーザーにとって適正・妥当・タイムリーであること	－	○
12	情報共有	IPAにアラートの統計情報等の提供を行う	○	－
		IPAが求める高度な情報等の提供を行う	－	○
13	事業継続性	サービス提供に必要な要員や品質管理能力、安定した財政基盤等を有する	○	○
14	2類サービスの安定性・継続性	2類サービスの品質を維持すること	－	○
15	法令遵守	法令および本基準を遵守する	○	○
16	サプライチェーン・リスク対応	2類サービスを構成する製品等におけるサプライチェーン・リスク対応を行う	－	○

※表1の項番は、IPAお助け隊サービス基準を基に項目を統合しているため、IPAのホームページ記載のサービス基準の項番と異なる。

（出典:IPAお助け隊サービス基準を基に、MS&ADインターリスク総研作成）

④2類サービス独自の基準

表1の「7. 拡充要件（2類）」が、2類サービスの主な機能を定めている。サービス基準における正確な表記は次のとおり。

> **第3章 お助け隊サービス（2類サービス）の基準に関する事項**
> **1. 要件**
> **⑸拡充要件**
> 現に提供中の1類サービスに加えて、以下のアからウのいずれか1つ以上を満たす拡充を行ったサービスを提供すること。
> ア ネットワーク監視の場合、又は端末監視との併用の場合、監視対象端末が増加していること。なお、自社が提供する1類サービスの監視可能端末が50端末未満の場合は50端末以上へ増加すること。
> イ 上記アを満たしたネットワーク監視と端末監視の併用へ変更又はクラウドサービスを対象とした異常監視の仕組みを追加すること。
> ウ 別途定める「サイバーセキュリティお助け隊サービス2類詳細ガイドライン」に従い異常監視の機能を追加すること。
> エ 常時利用を想定するセキュリティサービス又は各月とも少なくとも1回以上は提供することとなるセキュリティサービスを、新たに追加すること。

2類サービスは、1類サービスを基盤として、監視対象の拡大（「ア：端末数」、「イ：範囲」、「ウ：機能」）あるいは「エ：月1回以上提供するセキュリティサービスの追加されたもの」とされている。このうち、「エ」はサービス提供事業者によって独自色が出やすいサービスとなる。

本稿執筆時点では、新たに2類サービスとして登録されたサービスは公表されていないが、今後2類サービスが拡大し、より多くの企業においてお助け隊サービスの利用が進むことを期待したい。

3 サプライチェーンでの取り組み

⑴政府のメッセージ

政府（経済産業省と公正取引委員会の連名）は、サプライチェーン全体でサイバーセキュリティ対策を行うことを求めるメッセージとして、2022（令和4）年10月28日付「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」において、次のように述べている。

- サプライチェーンを構成する中小企業がサイバー攻撃を受けることによって全体の事業活動に支障がでる
- 特に発注者側はサプライチェーン全体でのサイバーセキュリティ対策強化に取り組んでほしい
- 中小企業等へのサイバーセキュリティ対策には「サイバーセキュリティお助け隊サービス」等を活用してほしい
- 発注者側はサイバーセキュリティ対策を求める以上、中小企業側のコスト増加を考慮すべきである
- 合理的な理由なくサイバーセキュリティ対策商品の購入や利用を強制することは禁止する

こうしたメッセージが政府から発信されることは、特に発注者側にとってどのようなスタンスで中小企業等に対策を求めるべきかについての判断基準の参考となる。

政府には、サプライチェーン全体でのサイバーセキュリティ対策を普及させるため、継続的にこうしたメッセージを発信することが望まれる。

⑵サプライチェーン全体で活用するメリット

サプライチェーン全体のサイバーセキュリティ対策を強化するために、中小企業がお助け隊サービスを活用するメリットを大きく五つに整理した。これらは、自社の対策を強化したい中小企業にとってのメリットでもあるが、対策を強化してほしい発注者側にとってもサプライチェーン全体で一斉に対策レベルを底上げする際の参考としてほしい。

①24時間365日の監視と防御

サプライチェーンの各企業がお助け隊サービスを利用することで、UTM（Unified Threat Management：複数のセキュリティ機能を統合し集中的にネットワーク管理を行うこと）やEDR（Endpoint Detection and Response：ユーザーが利用するパソコンやサーバーにおける不審な挙動を検知し、迅速な対応を支援するセキュリティツール）による24時間365日の監視と防御を受けられる。これにより、サプライチェーン全体で不正アクセスやサイバー攻撃の早期検出と迅速な対応が可能となる。

②専門家へのアクセス

お助け隊サービス利用企業には、サイバー攻撃や異常な活動が検出された際に、サイバーセキュリティの専門家に電話やメールで相談できる窓口が提供される。これにより、各企業が迅速かつ適切な対策を講じることができ、サプライチェーン全体のリスク管理が強化される。

③情報共有と脅威検知

サプライチェーン内の各企業がお助け隊サービスを活用する

ことで、最新のサイバー攻撃情報やセキュリティ事故情報の提供を受けられる。サービス提供事業者側は同じサプライチェーン上で脅威情報を検知した場合、脅威情報を直ちに横展開し、早期に対処することが可能となる。

④サイバー保険とインシデント対応

お助け隊サービスには必ずサイバー保険が付帯されている。サイバーインシデントが発生した場合には、保険を利用して専門家の駆けつけ対応を受けることができる。これにより速やかに事業継続対応を図ることが可能となる。

⑤経済産業省とIPAのサポート

経済産業省とIPAが推奨し、サプライチェーンの各企業が利用しやすいように設計されている。IT導入補助金等の制度の利用が可能であり、中小企業が効果的にサイバーセキュリティ対策を導入できるよう支援する仕組みが構築されている。

これらの対策により、サプライチェーン全体で一貫したサイバーセキュリティ対策を実施し、リスクを低減することが期待される。

4 補助金制度

政府はお助け隊サービス普及のため、2022年3月からお助け隊サービスを補助金制度に取り入れ、IT導入補助金の対象とした。2022年7月にセキュリティ対策推進枠が新たに創設された。

本稿執筆時点で利用可能な「IT導入補助金2024」の概要は表2のとおりである(表2のほかにインボイス枠も存在するがここでは割愛する)。

「セキュリティ対策推進枠」は表2のとおり、お助け隊サービス専用の補助金枠となっている。補助金の申請手続きは少々煩雑であるが、補助金を加味するとユーザーは実質半額でお助け隊サービスを導入することができる。

なお、お助け隊サービス単体では通常枠やインボイス枠の申請要件を満たさないが、それぞれの枠の申請要件を満たすツールを導入する際に、同時にお助け隊サービスを申請すると、申請時に加点要件となる場合や、サービス料を合算して補助を受けられる場合もある。

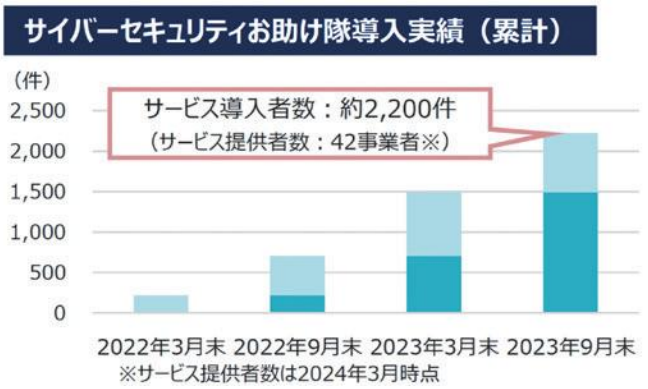
その他の補助金制度においては、2023年度ものづくり補助金における加点要件とされるなど、補助金制度とお助け隊サービスを組み合わせることで、ユーザーは政府による支援が受けられる。

こうした制度は全国の中小企業への導入を後押しするものであり、継続した国の支援が期待される。

5 お助け隊サービス制度の展望

(1)お助け隊サービスの普及実績

経済産業省が公表しているお助け隊サービス導入実績(2023年9月末時点)は、約2,200件である。国内の中小企業数を考慮すると、まだ導入企業数は少ないといえる(図2)。



【図2】お助け隊サービスの導入実績
(出典:経済産業省「第8回産業サイバーセキュリティ研究会　事務局説明資料」)

【表2】IT導入補助金2024におけるセキュリティ対策推進枠

枠	通常枠		セキュリティ対策推進枠
補助額	5万円～150万円未満	150万円～450万円以下	5万円～100万円
機能要件	1プロセス以上	4プロセス以上	独立行政法人情報処理推進機構が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているいずれかのサービス
補助率	1/2以内		1/2以内
対象経費	ソフトウェア購入費、クラウド利用費(クラウド利用料最大2年分)、導入関連費		サービス利用料(最大2年分)

(出典:IT導入補助金2024ポータルサイトを基にMS&ADインターリスク総研作成)

⑵お助け隊サービス普及に向け期待される施策

お助け隊サービス制度を日本全国に普及させるためには、制度を所管するIPAが中心となり、サービス提供事業者とともに普及施策に取り組むことが必要である。より一層の普及促進を期待し、MS&ADインターリスク総研として以下八つの普及施策を提言する。

①教育とトレーニングの提供

中小企業の経営者や従業員に対して、サイバーセキュリティの重要性を理解させるための教育プログラムを実施する。ウェビナー、ワークショップ、オンラインコースなどを活用して、実際のサイバー攻撃事例や対策方法を紹介し、サイバーセキュリティ対策の重要性を浸透させる。

②補助金や助成金の周知

サイバーセキュリティ対策に関する費用を補助するために、経済産業省や地方自治体が提供する補助金や助成金の情報を広く周知し、中小企業がこれらの資金を活用してお助け隊サービスを導入できるよう支援する。

③成功事例の共有

お助け隊サービスを導入して成功した中小企業の事例を収集し、成功事例として広く共有する。これにより、他の中小企業も導入のメリットを具体的に理解しやすくなる。

④パートナーシップの構築

サプライチェーン中核企業や業界団体と協力し、サイバーセキュリティの重要性を啓発する。これにより、業界全体でサイバーセキュリティ対策が促進され、中小企業への普及が進む。

⑤地方との関係強化

地方での説明会やセミナーを開催し、地域の中小企業に直接お助け隊サービスの利点を説明する。地方イベントの開催により、地域のITベンダーとの連携を強化し、現地でのサポート体制を充実させる。

⑥簡単な導入手順とサポート

サービスの導入手順を簡素化し、初期設定や運用に関するサポートを充実させる。分かりやすいマニュアルやサポート窓口を提供することで、技術的なハードルを下げる。

⑦インセンティブの提供

早期導入企業に対する割り引きや特典を提供することで、導入を促進する。また、紹介プログラムを導入し、既存ユーザーが新しいユーザーを紹介することで報酬を得られる仕組みを作る。

⑧広報活動の強化

サイバーセキュリティの重要性やお助け隊サービスのメリットを広く宣伝するために、ソーシャルメディア、メールマーケティング、新聞、ラジオなど多様なメディアを活用した広報活動を展開する。

これらの施策を組み合わせることで、中小企業に対する「サイバーセキュリティお助け隊サービス」の普及を効果的に推進することが望まれる。MS&ADインターリスク総研でもお助け隊サービスの一つである「防検サイバー」を提供しており、引き続き普及に努めたい。

以上

参考文献・資料等

1) 独立行政法人情報処理推進機構　サイバーセキュリティお助け隊サービス制度
<https://www.ipa.go.jp/security/sme/otasuketai/index.html>（最終アクセス2024年5月20日）
2) 独立行政法人情報処理推進機構　サイバーセキュリティお助け隊サービス基準（2.0版）
<https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf>（最終アクセス2024年5月20日）
3) 経済産業省・公正取引委員会　サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて
<https://www.meti.go.jp/policy/netsecurity/hontai_1028.pdf>（最終アクセス2024年5月20日）
4) 令和5年度補正サービス等生産性向上IT導入支援事業 IT導入補助金2024
<https://it-shien.smrj.go.jp/>（最終アクセス2024年5月21日）
5) 全国中小企業団体中央会　ものづくり補助金総合サイト
<https://portal.monodukuri-hojo.jp/index.html>（最終アクセス2024年5月20日）
6) 経済産業省　第8回産業サイバーセキュリティ研究会事務局説明資料
<https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/008_03_00.pdf>（最終アクセス2024年5月21日）