サイバーセキュリティお助け隊サービス基準

（２．０版）

独立行政法人情報処理推進機構

令和６年 ３月 １５日

目次

第１章　総則

１．サイバーセキュリティお助け隊サービスのコンセプト・目的

サイバーセキュリティお助け隊サービスは、中小企業等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）及び簡易サイバー保険等のサービスを中小企業等に、その事業環境の実情に則した内容で、安価かつ効果的なワンパッケージにまとめて確実に提供することを基本コンセプトとする。

本基準は、上記お助け隊サービスの内容を明確化し、提供する個々のサービスごとに独立行政法人情報処理推進機構（IPA）が「サイバーセキュリティお助け隊サービスマーク」の使用を許諾するにあたり充足すべき基準を定めることで、幅広い中小企業等において無理なく各社相応のサイバーセキュリティ対策を導入・運用することを支援するとともに、サプライチェーン全体のセキュリティの底上げを図ることを目的とする。

２．定義

本基準における以下各号の用語の意味は、次に定めるところによる。

（１）「１類サービス」とは本基準第２章所定の基準に適合するサービスをいい、「１類事業者」とは同章に従って１類サービスを提供する事業者（次号で定義する２類サービスの全部又は一部も併せて提供する事業者を除く。）をいう。

（２）「２類サービス」とは本基準第３章所定の基準に適合するサービスをいい、「２類事業者」とは本基準に従って１類サービス及び２類サービスの双方を提供する事業者をいう。

（３）「お助け隊サービス」とは、文脈に応じて、１類サービスのみ又は１類サービスと２類サービスを併せたサービスをいう。

（４）「実施主体」とは、以下のアとイのいずれか又はその両方を満たした事業者をいう。

ア　本章の「１．サイバーセキュリティお助け隊サービスのコンセプト・目的 」に記載したお助け隊サービスの基本コンセプトにおいて想定する導入対象者（以下「ユーザー」といい、文脈に応じて潜在顧客を含む。）と締結するサービス契約に基づいて、当該ユーザーにお助け隊サービスを提供する事業者。

イ　別途定める「サイバーセキュリティお助け隊サービス申請届出ガイドライン」に従って、次号で定義する再販協力会社と協業しかつその言動に責任を負う事業者。

（５）「再販協力会社」とは、上記（４）イ 所掲の申請届出ガイドラインに従い、自己の名と責任において、自らユーザーと締結するサービス契約に基づき当該ユーザーにお助け隊サービスを提供する事業者をいう。

（６）「パートナー」とは、お助け隊サービスを構成する製品（UTM 等）・サービス（駆付け等）・保険の内の全部又は一部を特定の実施主体（１者）のみに提供する事業者をいい、パートナーごとに実施主体１者が一意に定

まる。

（７）「チーム」とは、実施主体、及び当該実施主体にお助け隊サービスを構成する製品（UTM 等）・サービス（駆付け等）・保険の内の全部又は一部を提供する全てのパートナーから構成される集合体をいい、実施主体ごとに一意に定まる。

（８）「ネットワーク監視」とは、UTM（Unified Threat Management・統合脅威管理）等のネットワークセキュリティ監視装置を用い、少なくとも次のアからウの機能を実装したユーザーのネットワーク通信の異常監視をいう。

ア　外部からの不審アクセス等の脅威を検知する機能。

イ　内部からの不正通信等を検知する機能。

ウ　検知した脅威等を防御する機能。ただし、次号で定義する端末監視による防御機能と組み合わせる場合、この機能の実装は要件としない。

（９）「端末監視」とは、EDR（Endpoint Detection and Response）等のエンドポイントセキュリティソフトウェアを用い、少なくとも次のアとイの機能を実装したユーザーの端末内部の挙動の異常監視をいう。

ア　端末を常時監視し、異常や不審な挙動を検知する機能。

イ　検知した異常等を防御する機能（お助け隊サービスと連動して一体的に機能するその他の防御機能も含む。）。ただし、ネットワーク監視による防御機能と組み合わせる場合は、この機能の実装は要件としない。

（１０）「ユーザー概況」とは、ユーザーの業種、業態、事業規模（人的規模を含む。）、業績規模、経営状況、システム構成の規模・内容、システム要員の規模とレベル、サイバーセキュリティ対策へのニーズの規模・必要性・緊急性等の、ユーザーの属性を含めた総合的な事業環境をいう。

（１１）「オプションサービス」とは、お助け隊サービスの提供に併せて別途追加で提供するサービスをいう。

（１２）「登録サービス」とは、お助け隊サービスを構成する製品（UTM 等）・サービス（駆付け等）・保険等をまとめたサービスであり、かつ別途定める「サイバーセキュリティお助け隊サービス申請届出ガイドライン」に従って登録を受けたサービスをいう。

（１３）「サイバーセキュリティお助け隊サービスマーク」とは登録サービスの提供に際して使用することを目的として IPA が制定し使用許諾するマークをいう。同マークの詳細な使用許諾条件及び注意事項等は、別途「サイバーセキュリティお助け隊サービスマーク使用規約」で定める。

第２章　お助け隊サービス（１類サービス）の基準に関する事項

１．要件

１類サービス及び／又は１類事業者は、次に掲げる全ての要件を満たすものであること。

（１） 相談窓口

ユーザーからのお助け隊サービスに関する次に掲げる全ての問合せを受け付ける窓口が一元的に設置又は分かりやすく案内されていること。

ア　お助け隊サービスの内容、価格、及び申込方法等に関する問合せ

イ　UTM の設置方法等、契約後にお助け隊サービスを導入する際の問合せ

ウ　アラートの解釈等、お助け隊サービス利用中の技術的な問合せ

エ　価格調整等の営業的な問合せ

（２） 異常の監視

次のいずれかの仕組みを含む異常監視サービスを提供すること。

ア　【ネットワーク監視の場合】ユーザーのネットワークを２４時間見守り、攻撃を検知・通知する仕組み（UTM 等のツールと異常監視サービスから構成）

イ　【端末監視の場合】ユーザーの端末（PC やサーバ）を２４時間見守り、攻撃を検知・通知する仕組み（EDR 等のツールと異常監視サービスから構成）

なお、異常監視サービスが上記ア、イのいずれの仕組みを含むものであっても、検知した異常に応じて、

・ セキュリティ上重大なインシデントの場合は即時（６０分以内を目標）

・ また、防御機能により十分な対策を行ったインシデント、あるいはインシデント対応が不要なアラートについては、後日のレポート（週１回）等により

各々、ユーザーに通知すること。

（３） 緊急時の対応支援

ユーザーから要請された場合、サービス契約に基づき、当該ユーザーの指定する場所に技術者を派遣して緊急時の対応支援（駆け付け支援）を行うこと（ユーザーの合意を得て、リモートによる対応支援も可とする。）。

なお、異常監視の仕組み導入時の初期対応を除き、サービス契約に基づく駆付け支援は少なくとも年１回（簡易サイバー保険を活用する場合を含む。）、ユーザーの費用（駆付け支援の実施に必要又は相当と認める諸経費を除く。）負担無しに提供されるものとする。

（４） 中小企業等でも導入・運用できる簡単さ

IT やセキュリティの専門知識のないユーザーでも導入・運用できるような工夫が凝らされていること。

（５） 簡易サイバー保険

インシデント対応時に突発的に発生する各種コストを補償するサイバー保険が付帯されていること。なお、サイバー保険の補償内容（補償対象となる事項、補償回数、補償限度額、免責金額等）とユーザーにおいて自己負担が生じる場合は、サービス契約に明記するとともに、ユーザーにと

って分かりやすい説明資料を別途用意すること。

（６） 上記要件のワンパッケージ提供

上記（１）～（５）の要件が原則として一つの契約で提供可能となること。ただし、保険契約の締結等や法令等によりやむを得ない場合は複数の契約によることも可とするが、その場合にあってはユーザーにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること。また、異常の監視装置の製造メーカーと型式、サービス提供の所在国及び把握している場合はデータ保存先のサーバー所在国をサービス契約に記載すること。

（７） 中小企業等でも導入・維持できる価格等

上記（６）によりワンパッケージで提供されるお助け隊サービスの価格等については、次のアからカの全てを満たすこと。

ア　幅広い中小企業等において無理なく導入可能であることが望ましいため、初期導入費用、各種実費等、契約締結に当たってユーザーが一時的に支払うべき費用をサービス契約に明記する。また、その合計価格（次のイで定める月額価格は含めない）は以下の金額を超えないこと。

・【ネットワーク監視の場合】５０万円（税抜き）。
・【端末監視の場合】端末数によらず５０万円 （税抜き）。
・【上記の両者を併用する場合】これらの和に相当する価格である１００万円（税抜き）。

イ　お助け隊サービスの月額価格は以下の金額を超えないこと。

・【ネットワーク監視の場合】月額１万円（税抜き）。
・【端末監視の場合】端末１台あたり月額２，０００円（税抜き）。

なお、上記の両者を併用する場合は、合計額が月額１万円（税抜き）以下と端末１台あたり月額２，０００円（税抜き）以下の両方を満たすこと。

ウ　端末１台から契約可能とすること。

エ　最低契約期間は２年以内であること。

オ　初期費用、契約期間等の協議事項についての合意内容をサービス契約に明記するとともに、口頭又は書面によりユーザーに分かりやすく説明すること。

カ　途中解約した場合の違約金やユーザー側の契約解除の権利等をサービス契約に明記するとともに、口頭又は書面によりユーザーに分かりやすく説明すること。

（８） 中小企業等向けセキュリティサービス提供実績

IPA 実施事業「中小企業向けサイバーセキュリティ事後対応支援実証事業」、若しくは「令和２年度中小企業向けサイバーセキュリティ対策支援体制構築事業」に参加していたこと、又は類似のサービスを中小企業等向けに実質的に提供・運用した実績があること。

（９） 情報共有

お助け隊サービスを提供する事業者等及び／又は同サービスの制度運用等に関わる組織・機関等の相互間での情報共有が同制度の円滑かつ永

続的・発展的な運用・運営等に資すると認めて、IPA から「サイバーセキュリティお助け隊情報共有ガイドライン」に従った情報提供の要請を受けた場合、同ガイドラインに従って、少なくともアラートの統計情報を含めた情報の提供に応じること。

（１０） 事業継続性

お助け隊サービスの安定的・継続的な提供に必要な要員の確保、品質管理等の社内体制整備、企業としての安定した財政基盤、経理処理能力の保持等を維持するとともに、別途定める「サイバーセキュリティお助け隊サービス審査登録機関基準」所定の登録機関から要請を受けた場合は、かかる状況を証する資料等を同基準に従って提出等すること。なお、お助け隊サービスの安定的・持続的な提供が困難となる事情若しくはそのおそれが生じた場合又はその他必要若しくは有用と認めた場合には、上記基準に従って速やかに報告すること。

（１１） 法令等の遵守

実施主体及びこれと協業する再販協力会社並びに当該実施主体についてサービスを提供するパートナーは法令及び本基準を遵守すること。

２．更新・その他

（１） 登録の更新

登録サービスは、「サイバーセキュリティお助け隊サービス申請届出ガイドライン」に従って、本基準の適合性に関し２年毎に更新審査を受けること。

（２） サービス内容の変更

実施主体は、自己又は協業する再販協力会社が提供する登録サービスの内容・構成等を変更する場合は、「サイバーセキュリティお助け隊サービス申請届出ガイドライン」に従って事前に届け出ること。ただし、上記ガイドラインに再度の申請等の手続を必要とする旨の規定がある場合は、当該規定に従うこと。

（３） 登録の取消し等

実施主体及びこれと協業する再販協力会社並びに当該実施主体についてサービスを提供するパートナーのいずれか、又は上記各事業者が提供する登録サービスのいずれかに、本基準に適合せず若しくはその強い疑いがある場合、IPA は、当該実施主体に対し是正又は改善のために必要又は有効な措置を講ずべきことを指示又は勧告することができる。なお、相当の期間を定めての是正指示に応じない場合、IPA は 次の措置を講じることができる。

ア　サイバーセキュリティお助け隊サービス審査登録機関基準に従い、是正指示対象となった事業者が提供する全部若しくは一部の登録サービス、又は是正指示対象となった登録サービスについて、その登録を取り消す措置。

イ　お助け隊サービス制度に対する社会の信頼の保持に必要と認めた場合は、「サイバーセキュリティお助け隊サービス」の呼称の使用禁

止、その他上記信頼の保持に必要又は適切と認める広報的措置。

（４） 各種調査等への協力

お助け隊サービスを提供している実施主体は本基準遵守状況やその傾向、又は社会経済情勢等に照らしての本基準内容の社会的妥当性の調査・検証等のために、「サイバーセキュリティお助け隊サービス審査登録機関基準」所定の登録機関から協力要請を受けた場合、誠実にこれに対応するとともに、自社についてサービスを提供する全てのパートナー又は再販協力会社が上記協力要請に誠実に対応することとなるように事前に適切な措置を講じておくものとする。

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

２類サービス及び／又は２類事業者は、次に掲げる全ての要件を満たすものであること。

（１） 第２章の「１．要件」の（１）から（６）、（１０）及び（１１）各記載の要件

（２） 中小企業等でも導入・維持できる価格等

第２章の「１．要件」の（６）によりワンパッケージで提供されるお助け隊サービスについて、次のアとイを満たすこと。

ア　２類サービスの提供価格の合計は、ユーザー概況に照らして相応かつ妥当な額であること。

イ　第２章の「１．要件（７）」の「ウ、エ、オ、カ」各記載の要件。

（３） １類サービスの提供実績

１類サービスの提供・運用実績が「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」に定める要件を満たすこと。

（４） 情報共有

２類サービスのニーズとシーズの現況及びその動向等の把握、並びにその動向等に全ての２類事業者が迅速・適切・公平に適応できる事業環境整備等のために IPA が必要又は有用と認めて都度指定する情報については、全ての２類事業者は、IPA が別途定める「サイバーセキュリティお助け隊サービス情報共有ガイドライン」に従って、当該情報を遅滞なく IPA に提供するものとする。なお、個人情報保護法その他個人情報保護に関する法令の適用を受ける個人情報の提供については、当該法令の定め（強行規定に限る。）が優先する。

（５） 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。

（６）１類サービスの継続

１類サービスを構成する或るサービスが、上記（５）に従って拡充されて２類サービスとして提供されることとなる場合であっても、当該拡充された２類サービスが提供されている限り、拡充前の１類サービスは、拡充前の内容のまま引き続き１類サービスとして提供されること。

（７）監視の変更

１類サービスで採用中の監視の変更は、ネットワーク監視と端末監視の併用への変更のみとすること。

（８）２類サービスの妥当性及び適時性

以下のアとイを満たすこと。

ア　ユーザーに対するサービス契約の提案内容が、ユーザー概況に照らして適正・妥当かつタイムリーであること。

イ　ユーザーと締結したサービス契約の内容が、ユーザー概況に照らして適正・妥当かつタイムリーであること。

（９）２類サービス提供事業の安定性・継続性

以下のアからウを全て満たすこと。

ア　２類サービスに含まれる登録サービスの提供中はいつでも、お助け隊サービスの提供に関してユーザーから問合せ・契約締結の意向等を受けた場合、遅滞なく誠実に対応すること。

イ　２類サービスに含まれる登録サービスの提供中は、既存ユーザーへの積極的なサポート（２類サービスの提供内容をユーザー概況に応じてユーザーごとに更に充実させるための適切妥当な推奨活動を含む）や、新規ユーザーの積極的な開拓に努めること。

ウ　２類サービスに含まれる登録サービスの提供中は、常に２類サービスの品質維持及びサービスレベルの向上に向けての研鑽に努めること。

（１０）サプライチェーン・リスク対応

２類事業者はお助け隊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※について可能な限り努めること。

また、IPA は、お助け隊サービス制度に対する社会の信頼の保持に必要と認めた場合、２類サービスへ申請されたお助け隊サービスを構成する製品等を対象に、サプライチェーン・リスク対応の観点から外部機関等へ照会又は調査依頼を行い、助言等を受けるものとする。

※　本基準においては、お助け隊サービスの用に供する情報システム環境に潜在する様々なリスクの内、主に不正行為が介在するリスクへ

の対応を指す。政府統一基準適用個別マニュアル群「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」参照。

２．更新・その他

（１） 第２章の「２.更新・その他」の（１）から（４）各記載の要件を全て満たすこと。

（２） 登録上限数

２類サービスとして提供可能な登録サービスの上限数は別途定める「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」に従うこと。

（３） 比較表

ユーザーの求めがある場合、当該ユーザーに提供中の１類サービスと２類サービスの差分が分かる比較表を遅滞なく提示すること。

（４） オプションサービスの提供

オプションサービスの提供は、理由の如何を問わず、２類サービス提供の対価に一切影響を与えないものとする。

附則

１．推奨事項

中小企業等におけるサイバーセキュリティ対策の導入・運用の更なる利便性向上等を図る趣旨のもと、お助け隊サービスの提供にあたっては以下の事項を推奨する。

（１） 独自のオプションサービス提供

お助け隊サービスの他に、さらなるセキュリティ対策の導入・レベルアップ等を考える企業のためのオプションサービスを用意すること。

例：・事前アセスメント等の簡易コンサルティングサービス
・ネットワーク監視の更なる強化のための仕組み
・デジタルフォレンジック等より広い範囲のコストを補償するサイバー保険

（２） 日本発の技術・製品の活用

日本特有のサイバー攻撃動向に対してより高精度で対応するため、日本発の技術やそれを用いた製品・サービスを活用すること。

（３） ネットワーク監視の場合

ネットワーク監視によりサービスを提供する場合、ネットワーク通信全体を監視できるよう監視機器の設置する場所等を考慮すること。

（４） 端末監視の場合

端末監視によりサービスを提供する場合、当該機能は少なくとも重要情報を取り扱う端末には導入すること。

２．改定

IPA は、本基準第１章「１．サイバーセキュリティお助け隊サービスのコンセプト・目的」記載の目的に照らし必要又は適切と認めた場合、必要に応じて各方面の意見を求めた上で、相当の予告期間をおいて本基準の内容を改定することがある。改定に伴う経過措置は、改定後の内容の中で定める。