新規申請事業者様向け説明会資料

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（IPA）　セキュリティセンター
普及啓発・振興部　　普及啓発グループ

目次

本資料の一部では「サービス基準からの抜粋」を用いて説明をしています。
サービス基準の全文を掲載するものではありません。

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即した内容で、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。

相談窓口
異常の監視
初動対応（駆付け支援等）
簡易サイバー保険

本基準は、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。

サイバーセキュリティ
お助け隊

第１章　総則
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。

（４）「実施主体」とは

サービス基準からの抜粋

ア　お助け隊サービスの基本コンセプトにおいて想定するユーザー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　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。

第１章　総則
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。

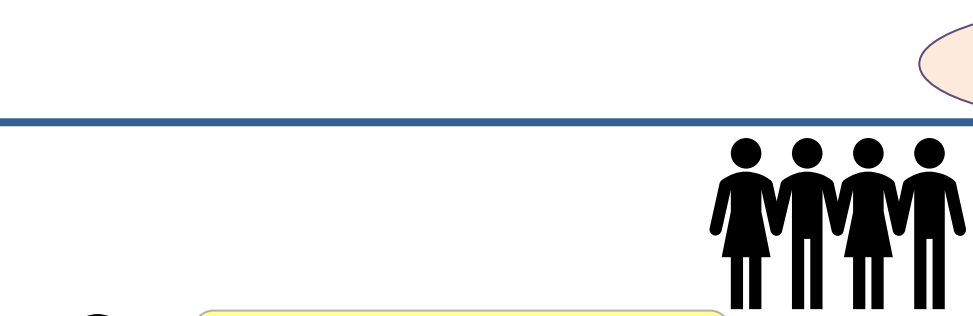
（６）「パートナー」とは

サービス基準からの抜粋

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。



複数の事業者で構成

第１章　総則
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。

（８）「ネットワーク監視」とは

サービス基準からの抜粋

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の検知をする機能。
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、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。

UTM等

端末監視との併用で
補完できればOK

第１章　総則
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。

（９）「端末監視」とは

サービス基準からの抜粋

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。

EDR等

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。

ネットワーク監視との
併用で補完できればOK

第１章　総則
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。

（１０）「ユーザー概況」とは

サービス基準からの抜粋

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。

第１章　総則
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。

サービス基準からの抜粋

（１３）「サイバーセキュリティお助け隊マーク」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。

登録サービスに対して使用ＯＫ

サイバーセキュリティ
お助け隊

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求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、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

お問合せには速やかな対応を

お答えいたします!

どうしたらいいの？

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

24時間見守り　重大なインシデントに対応

（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。

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

緊急時の駆付け支援

（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。**

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（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。

チームによるサポート体制の整備

例えば、このような…

- ◆ 監視のための機器の設置方法などを簡潔に紹介した動画の作成・提供
- ◆ 相談窓口では、メール・電話に加えリモートデスクトップによるサポートを提供
- ◆ 監視のための機器等のアップデートなどを遠隔で行い、中小企業側の業務負担を軽減する
- ◆ インストール作業が簡単に行えるインストーラーの配布
- ◆ 専用の問合せ窓口を設置
- ◆ 情報提供や問合せ対応のための、ユーザー専用のダッシュボードの作成・提供
- ◆ サービス導入前に、既導入ソフトとの相性確認などの「無料セキュリティ診断」サービスの提供

など

おまかせください　！

よく、わからないんです..

第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（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範囲（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。**

説明が大事です！

サイバー保険でカバーされるもの
駆付けの回数　期間　適用範囲
ユーザーの自己負担となるもの

対象期間は？

何回まで？

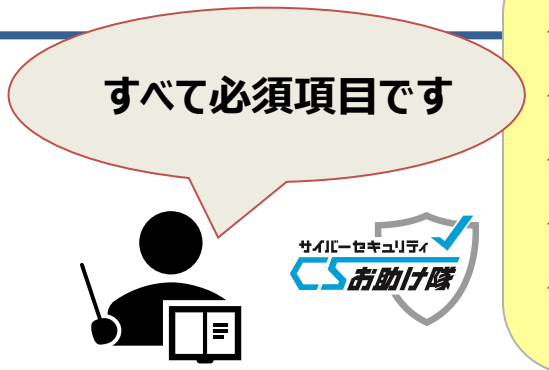
駆付けの交通費は？

第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（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**一つの契約で契約可能**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形式、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。



ワンパッケージで提供

- ✓ **(1)相談窓口**
- ✓ **(2)異常の監視の仕組み**
- ✓ **(3)緊急時の対応支援**
- ✓ **(4)中小企業でも導入・運用できる簡単さ**
- ✓ **(5)簡易サイバー保険**

第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（７）中小企業でも導入・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）**

第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

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。

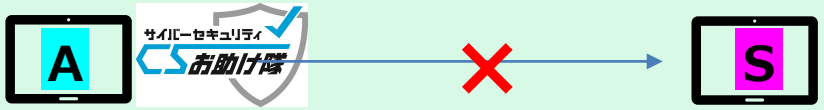
ウ　**端末１台から契約可能**とすること。

端末の契約は
１台からでもＯＫ

お助け隊サービスのガイダンス

契約台数にかかわらず、**同一のお助け隊サービスにおいて提供される**
セキュリティ機器は、同一の製品により提供される必要があります。

例：〇台以上の契約の場合には、セキュリティ機器を別の機器へアップグレードするといった
　　ことはできない。



第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

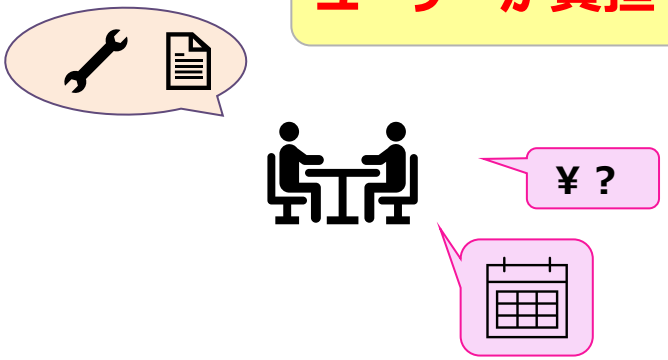
エ　最低契約期間は**２年以内**であること

説明は分かりやすく！

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。

ユーザーが負担する費用を明確に表示



第２章　お助け隊サービスの基準に関する事項
１　　要件

本お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（８）中小企業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向けに実質的に提供・運用した実績がある**こと。

実績の有無は、申請時に提供される情報から実態を踏まえて総合的に判断

実績の目安としては…

お助け隊サービスのガイダンス

「サイバーセキュリティお助け隊サービスと類似のサービスを30社以上の中小企業に提供・運用した、製品のみならず運用サポート等も合わせて提供した」 などが目安の一例

製品のみを数百社以上の中小企業に提供した実績があってもそれだけでは実績要件を満たすことにはなりません。

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

事業者連絡会での情報共有

（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」に従った情報共有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

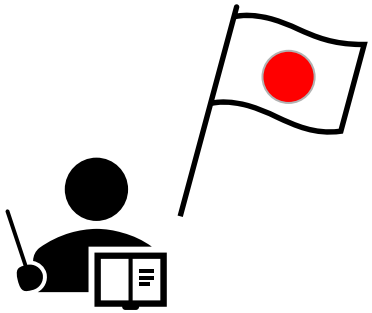
お助け隊サービスの安定的・継続的な提供に必要な要員の確保、**品質管理等の社内体制整備**、企業としての**安定した財政基盤**、**経理処理能力の保持等**を維持するとともに別途定める「サイバーセキュリティお助け隊サービス審査登録機関基準」所定の登録機関から要請を受けた場合は、かかる状況を証する資料等を同基準に従って提出等すること。なお、お助け隊サービスの安定的・持続的な提供が困難となる事情若しくはそのおそれが生じた場合又はその他必要若しくは有用と認めた場合には、上記基準に従って速やかに報告すること。

第２章　お助け隊サービスの基準に関する事項
１　　要件

お助け隊サービスは、次に掲げる全ての要求を満たすものであること。

（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。



第２章　お助け隊サービスの基準に関する事項
１　　更新･その他

サービス基準からの抜粋

（１）登録の更新

登録サービスは、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、事前に届け出ること。

登録時のサービス内容を勝手に変えることはできません。

登録を継続する場合は更新審査が必要

サービス基準の要件にかかる変更については再申請が必要

第２章　お助け隊サービスの基準に関する事項
１　　更新･その他

（３）登録の取り消し等

サービス基準からの抜粋

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、**本事業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な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）審査登録機関への協力

登録機関からの協力要請を受けた場合、誠実にこれに対応すること。

付則
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。

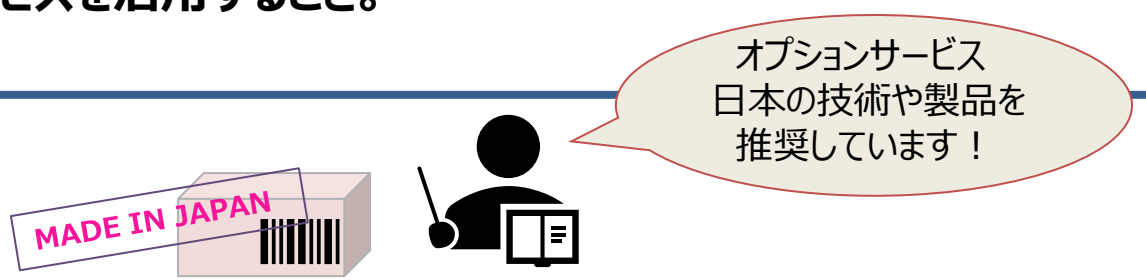
（１）独自のオプションサービス提供

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。



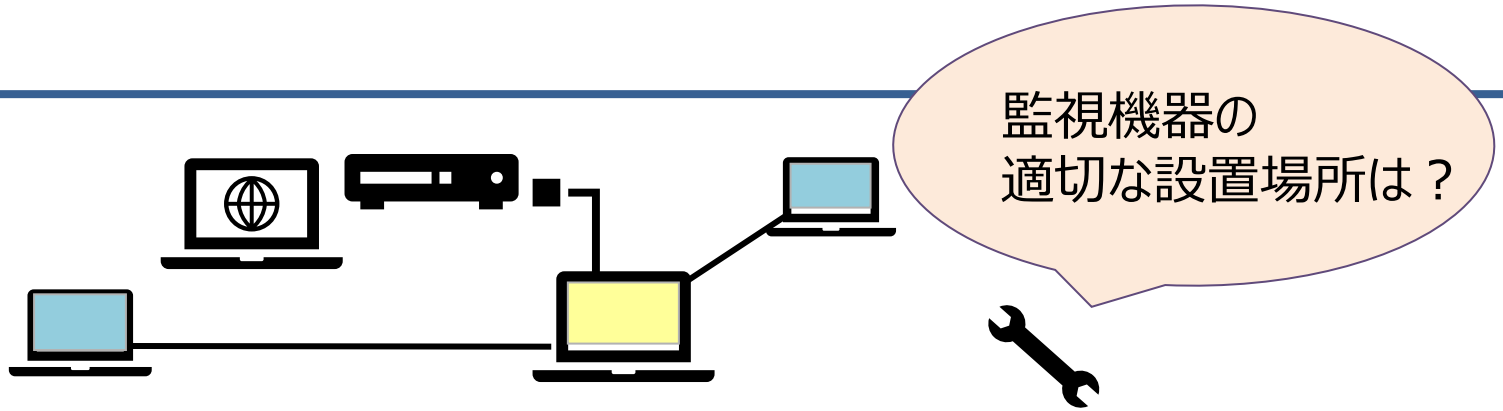
付則
1　推奨事項

（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。



付則
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。


サイバーセキュリティ
CSお助け隊