サイバーセキュリティお助け隊サービス基準 1.2版改定にかかる主な内容

No.	サービス基準改定の主な内容	改定の内容	
		1.1版	1.2版
1	**収集データ保管の制約** (対応の方向性) サービス基準改定で、クラウドサービス利用時のデータ保存先の所在国について、サービス規約等に記載してユーザーと合意する必要がある旨を明確化。	「原則として（１）～（５）の機能をユーザーが個別に契約することなく，一元的に契約可能であること。ただし，法令等やむを得ない事情がある場合は個別契約も可とするものの，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。」（第2章1.(6)）	「原則として（１）～（５）の機能をユーザーが個別に契約することなく，一元的に契約可能であること。ただし，法令等やむを得ない事情がある場合は個別契約も可とするものの，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・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所在国についてサービス規約等に記載すること。**」（第2章1.(6)）
2	**製品・サービスの制約** (対応の方向性) サービス基準改定で、異常の監視装置の製造メーカーやサービス提供の所在国について、サービス規約等に記載してユーザーと合意する必要がある旨を明確化。	同上	同上
3	**緊急時の駆付け対応支援にかかる要件の明確化** (対応の方向性) ①サービス基準改定で、リモートによる支援が可能な場合は、ユーザーの合意が必要である旨を明確化。	「ユーザーと合意したサービス規約等に基づき，ユーザーから要請された場合， ユーザーの指定する場所に技術者を派遣することにより，緊急時の対応支援を行うこと（リモートによる対応支援が可能な場合には，リモートによる対応支援も可とする）。」（第2章1.(3)）	「ユーザーと合意したサービス規約等に基づき，ユーザーから要請された場合， ユーザーの指定する場所に技術者を派遣**（駆付け支援）し，緊急時の対応支援を行うこと**（リモートによる対応支援が可能な場合には，**ユーザーからの合意を得て，**リモートによる対応支援も可とする）。 ・・・
4	**緊急時の駆付け対応支援にかかる要件の明確化** (対応の方向性) ②サービス基準改定で、緊急時の対応支援は、簡易サイバー保険の活用する場合も含めて、年２回はユーザーの自己負担が生じないようにする必要がある旨を明確化。 ただし、移動に要する交通費については許容（ユーザー負担可）とする。	同上	・・・ **また，緊急時の対応支援は，簡易サイバー保険を活用する場合を含めて，異常の監視の仕組みの導入に伴う初期対応に必要な駆付け支援を除き,少なくとも年１回はユーザーの自己負担が生じないようにすること。ただし,駆付け支援を行うための移動に要する交通費などの諸経費は除くことができる。**」（第2章1.(3)）
5	**簡易サイバー保険の対象明確化** (対応の方向性) サービス基準改定で、サイバー保険の補償範囲をサービス規約に記載し、かつ、ユーザーが分かりやすい説明資料を用意する必要がある旨を明確化。	「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，当該保険は初動対応（駆付け支援等）の費用を補償するものであることとし，ユーザーにおける自己負担が生じる場合及びその範囲についてはサービス規約等に記載するとともに，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。」（第2章1.(5)）	「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）及びユーザーにおいて自己負担が生じる場合，サービス規約等に記載するとともに，別途ユーザーにとって分かりやすい説明資料を用意すること。**」（第2章1.(5)）
6	**UTMの性能、監視機能要件の詳細化** (対応の方向性) サービス基準改定で、プリンターなどのオフィス機器の監視は基準においては求めない旨を明確化。	「（１）ネットワーク一括監視型 お助け隊サービスのうち，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てユーザーのネットワーク通信の異常を監視する形態のものをいう。」(第1章 2.(1))	（１）ネットワーク監視型 ・・・

No.	サービス基準改定の主な内容	改定の内容	
		1.1版	1.2版
7	**UTMの性能、監視機能要件の詳細化** (対応の方向性) サービス基準改定で、セキュリティ監視機器の最低限実装すべき機能を記載し明確化。	「（１）ネットワーク一括監視型 お助け隊サービスのうち，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てユーザーのネットワーク通信の異常を監視する形態のものをいう。」(第1章 2.(1))	「・・・ お助け隊サービスのうち，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てユーザーのネットワーク通信の異常を監視する形態のものをいう。 **少なくとも以下の機能を実装すること。** **ア　外部からの不審アクセス等の脅威の検知** **イ　内部からの不正通信等の検知** **ウ　検知した脅威等の防御** **ただし,端末監視型の仕組みの防御機能と組み合わせて提供する場合は,ネットワーク監視型における防御機能の実装は要件として求めない。**」(第1章 2.(1)) 「（3）ネットワーク監視型のサービスの提供 **ネットワーク監視型の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。**」(附則 1.(3))
8	**EDRの性能、監視機能要件の詳細化** (対応の方向性) サービス基準改定で、セキュリティ監視機器の最低限実装すべき機能を記載し明確化。	「（２）端末監視型 お助け隊サービスのうち，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てユーザーの端末内部の挙動の異常を監視する形態のものをいう。」(第1章 2.(2))	「（２）端末監視型 お助け隊サービスのうち，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てユーザーの端末内部の挙動の異常を監視する形態のものをいう。 **少なくとも以下の機能を実装すること。** **ア　端末を常時監視し，異常や不審な挙動の検知** **イ　検知した異常等の防御（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も含む）** **ただし,ネットワーク監視型の仕組みの防御機能と組み合わせて提供する場合は,端末監視型における防御機能の実装は要件として求めない。**」(第1章 2.(2)) 「（４）端末監視型のサービスの提供 **端末監視型のサービスを提供する場合，少なくとも重要情報を取り扱う端末には導入すること。**」(附則 1.(4))
9	**インシデントを検知した場合の通知** (対応の方向性) サービス基準改定で、何らかのインシデントを検知した場合、遅滞なくユーザーに通知する必要がある旨を明確化	「（２）異常の監視の仕組み 次のいずれかを含む異常監視サービスを提供すること。 ア　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）（ネットワーク一括監視型の場合） イ　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）（端末監視型の場合）」（第1章 1.(2)）	「（２）異常の監視の仕組み 次のいずれかを含む異常監視サービスを提供すること。 ア　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）（ネットワーク一括監視型の場合） イ　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）（端末監視型の場合） **なお ,いずれの異常監視サービスであっても検知した異常に応じ，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）,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）等によりユーザーに通知すること。**」 （第1章 1.(2)）
10	**初期費用の金額、対象制約の要否** (対応の方向性) サービス基準改定で、初期費用の上限金額を明記し、明確化。	「ウ　初期費用，契約年数等の契約にかかる条件をサービス規約等に記載するとともに，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。 エ　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規約等に記載するとともに，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」(第2章 1.(7))	「ウ　初期費用，契約年数等の契約にかかる条件をサービス規約等に記載するとともに，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。 **エ　初期費用の金額は,幅広い中小企業において無理なく導入可能な価格であることが望ましいため,必要な場合であっても,最大で以下の金額を上回らないこと。** **ネットワーク監視型の場合・・　50万円以下（税抜き）** **端末監視型の場合・・　端末数によらず50万円以下（税抜き）** **併用型の場合・・　これらの和に相当する価格(100万円（税抜き）)を超えない価格であること。** **オ**　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規約等に記載するとともに，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。」(第2章 1.(7))

No.	サービス基準改定の主な内容	改定の内容	
		1.1版	1.2版
12	**販売方法の見直し** (対応の方向性) サービス基準改定で、実施主体の記載を見直し、実施主体が中小企業と契約を行わないケースも許容	「(3)実施主体 お助け隊サービスに関する契約を中小企業と行う事業者であり、お助け隊サービス審査登録機関への申請等を行う者をいう。」(第1章 2.(3))	「(3)実施主体 お助け隊サービスに関する契約を中小企業と行う事業者**又は再販協力会社を通じてお助け隊サービスを提供する事業者であり，**お助け隊サービス審査登録機関への申請等を行う者をいう。」(第1章 2.(3))
13	**販売方法の見直し** (対応の方向性) サービス基準改定で、「再販協力会社」の定義を追加	―	**「(4) 再販協力会社** **実施主体が提供するお助け隊サービスに関する契約を中小企業と行う事業者をいう。**」(1章 2.(3)) 「(10)事業継続性 お助け隊サービスの提供に必要な要員の確保，品質管理等の社内プロセス整備，企業としての安定した財政基盤，経理処理能力等を有し，それらを審査登録機関に対して示せること。なお，お助け隊サービスの提供が困難となる事情が生じた場合，その他必要な場合には，IPA及び審査登録機関に対しその旨速やかに報告を行うこと。**また ,再販協力会社によるお助け隊サービスの提供が困難となる場合は,実施主体がその責任を負うこと。**」(第2章　1.(10)
14	**販売方法の見直し** (対応の方向性) サービス基準改定で、「再販協力会社」を含む届出運用を追記。	―	**「(2) サービス内容の変更** **実施主体は，お助け隊サービスの提供内容に変更が生じた場合は，IPAが別に定めるガイドライン等に従い，速やかに届け出ること。ただし，変更内容によっては改めて申請を要する場合があるが，これに従うこと。」**（第2章 2.(3)
15	**サービスの登録取り消し規定の要否　（法令違反などの重大な違法行為があった場合）** (対応の方向性)	―	「（11) サービス基準の遵守 **実施主体は，日本の法令及び本基準が定める事項を遵守すること。**」（第2章 1.(11)） 「（３）サービスの取消し **再販協力会社も含め本基準に逸脱した場合，又はその強い疑いがあり，お助け隊サービス制度に対する社会的信頼保持等の観点から必要と考えられる場合，IPA は実施主体に対し是正のために必要な措置を講ずべきことを指示することができる。この場合，相当の期間を定めて是正のための機会を与えるが，是正に応じない際には，IPAはそのサービスのかかる登録を取り消す場合がある。**」（第２章 3.(3)）
16	**【その他】** (形式的・修辞的な修正)	―	基準全体を通して平仄等の観点から、形式的・修辞上の修正を行った。