我が国産業の情報セキュリティ向上に向けた
情報セキュリティサービスの高度化方策に関する調査報告書

令和元年 6 月

経済産業省

商務情報政策局サイバーセキュリティ課

目　次

１．目的

ＩＴの利活用が我が国産業競争力の強化に不可欠となる一方で、サイバー攻撃の激化等に伴い、サイバーセキュリティ対策の重要性はますます高まりつつある中、サイバーセキュリティ対策には高度な専門性が必要であるため、事業会社の多くは情報セキュリティサービスを活用せざるを得ない状況にある。適切な情報セキュリティサービスの選択に資するため、経済産業省は、平成２９年度に情報セキュリティサービス基準及び情報セキュリティサービスに関する審査登録機関基準を策定し、当該基準に基づく審査登録制度（以下「審査登録制度」という。）を平成３０年度から開始した。

我が国産業の情報セキュリティ水準を高めるためには、産業界のニーズに合ったより良い情報セキュリティサービスが提供されることが必要である。審査登録制度は、このための第一歩として、市場として受け入れられる水準を維持する情報セキュリティサービスを明示するものである。そして、審査登録制度の普及を推進すると共に、産業界のニーズに合ったより良い情報セキュリティサービスの情報を明確に把握し、利用者に当該情報を提供することが望ましい。

審査登録制度普及の鍵は、情報セキュリティサービス基準に基づき、情報セキュリティサービスに関する審査登録機関基準に規定する審査登録機関（以下「審査登録機関」という。）が行う審査を基に、独立行政法人情報処理推進機構が開示する、情報セキュリティサービス基準適合サービスリスト（以下「基準適合サービスリスト」という。）の信頼性にある。審査登録制度では、審査登録機関がサーベイランスを通じて申請内容の信頼性を高めることが求められている。このために、基準適合サービスリストに掲載されているサービスについてサンプリングを行い、サーベイランスを実施することが必要である。

また、審査登録制度の更なる普及、発展のために、より良い情報セキュリティサービスの情報をどのように付け加えるかについて検討することが必要である。このため、利用者が情報セキュリティサービスを利用する際の問題点等の現状を把握し、より良い情報セキュリティサービスとは何かを明確にした上で、その評価を行う主体、及び評価結果の開示のあり方等を検討し、具体的な施策を明らかにする。

本調査は、上記の２つの事業を行うことを通じて、情報セキュリティサービスの高度化の具体策を検討することを目的として実施したものである。

２．事業の概要

以下に、本事業の全体に関わる内容について、その概要を示す。

２．１ 実施内容

「１．目的」を達成するために以下（１）～（３）の事業を実施した。

（１）基準適合サービスリストに掲載されたサービスに対するサーベイランス

基準適合サービスリストに掲載されたサービスのうち、提供する事業者が異なるサービスを４件選択し、申請書類に記載された内容に係る事実が存在することを調査した。調査の内容は以下のとおりである。

① 技術要件

次の２点について、申請内容に基づく実態の確認を行う。

ア　専門性を有する者が申請のとおり在籍しているか。

イ　サービス仕様が申請のとおり明示されているか。

② 品質管理要件

次の３点について、申請内容に基づく実態の確認を行う。

ア　品質管理者が申請のとおり割当てられているか。

イ　品質管理マニュアルが申請のとおり整備されているか。

特に、以下の内容が申請のとおりであるか。

（ア）サービス提供プロセスの管理

（イ）アウトプットの管理

ウ　品質の維持・向上に関する手続きが申請のとおり導入されているか。

（ア）品質の維持・向上に関する手続きが申請のとおり行われているか

（イ）情報セキュリティサービスに従事する者に対して、情報セキュリティサービス基準の附則に定める教育又は研修等のいずれかを申請のとおり実施又は受講させているか。

（ウ）申請のとおりに、顧客の情報を保護するための手続を設け、運用するとともに、当該手続について情報セキュリティサービスを行った案件の担当者以外による監査（内部監査又は外部監査）を実施することにより実効性を確保しているか。

調査に当たっては、サーベイランス対象サービスの選定、事実認定の基準、調査の方法、報告書の内容等について、情報セキュリティサービスに知見のある技術的専門家を含めたメンバー６名によるワーキンググループを２回設け、検討した。

（２）より良い情報セキュリティサービスの情報提供のあり方

基準適合サービスリストに基づいて、より良い情報セキュリティサービスを明示する方法について検討し、そのための制度について取りまとめた。検討の内容は以下のとおりである。

① 情報セキュリティサービスの利用における現状把握

情報セキュリティサービスの利用者が、サービスを利用、選択等する上での現状の課題を明らかにし、課題を解決するために必要な情報、制度は何かについて検討した。

② より良い情報セキュリティサービスを評価する指標とその伝え方の検討

「より良い情報セキュリティサービス」の概念を検討し、サービスの質や顧客満足度などの評価指標を検討した。さらに、より良さを具体的に伝える方法について、表彰、定性的な表現、数値的評価（レーティング）など複数案を想定し、その長所及び短所を評価し、推奨する方法を検討した。

③ より良い情報セキュリティサービスの評価方法のあり方の検討

上記②で取りまとめた評価指標を具体的に測るための情報の収集方法及び評価方法について複数案を作成し、評価の質（公平性や信頼性）や実行可能性等の観点から評価したうえで、望ましい方向を検討した。

検討に当たっては、審査登録制度の検討に係ったメンバー等の有識者９名で構成される検討会を３回開催し、実施した。

２．２ 実施体制

本事業の実施体制を次図に示す。事業のうち、情報セキュリティサービス事業者のサーベイランスについては、情報セキュリティサービス審査登録機関である特定非営利活動法人日本セキュリティ監査協会の支援を得て実施した。

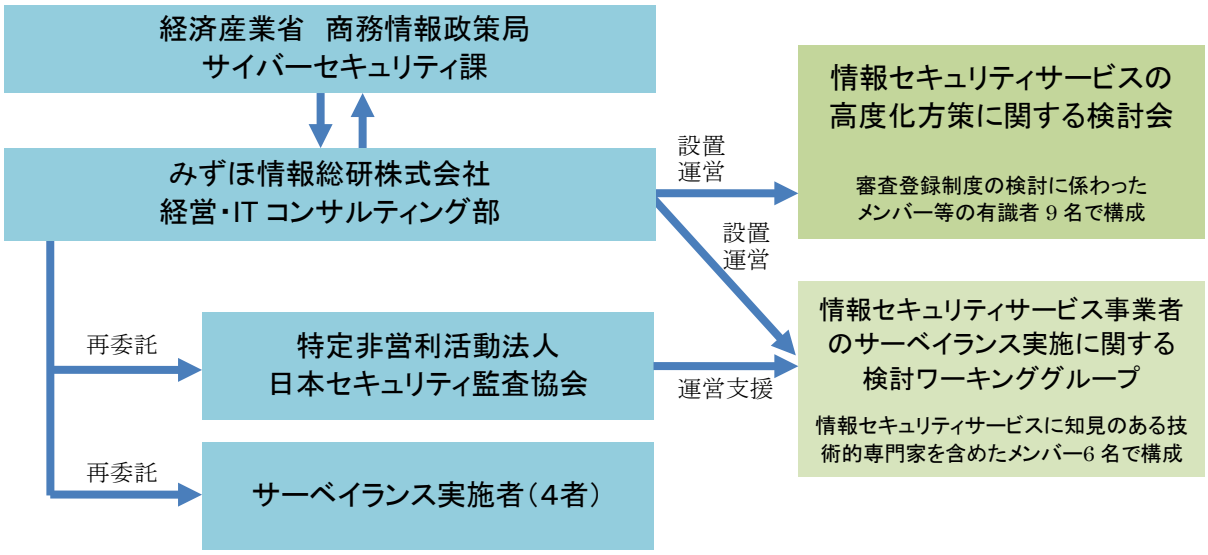


図 1　本事業の実施体制図

２．３ 実施スケジュール

本事業は以下のスケジュールにて実施した。

表 1　実施スケジュール

作業項目		平成 30 年												平成 31 年								
		9 月			10 月			11 月			12 月			1 月			2 月			3 月		
		上	中	下	上	中	下	上	中	下	上	中	下	上	中	下	上	中	下	上	中	下
(1) 基準適合サービスリストに掲載されたサービスに対するサーベイランス	実施方法検討			■	■	■	■	■	■													
	サーベイランス実施者公募・選定											■	■	■	■	■						
	サーベイランス実施																■	■	■	■		
	ワーキンググループ開催								■	①	■								■	②	■	
(2) より良い情報セキュリティサービスの情報提供のあり方	関連調査実施			■	■	■	■															
	関係機関ヒアリング							■	■	■			■	■	■			■	■	■		
	検討会開催									■	①	■			■	②	■			■	③	■
報告書作成・納入																					■	▼

各作業項目の網掛け部分において実施。
①②③は検討会・WG（それぞれ第1～3 回）開催時期。▼は成果物の納入期日。

２．４ 会議体による検討経緯

本事業の実施に際しては、事業内容に合わせて次の２つの会議体を設置し、それぞれ次のような議論を行った。

（１）情報セキュリティサービス事業者のサーベイランス実施に関する検討ワーキンググループ

サーベイランスの実施方法と実施結果の妥当性について審議するため、情報セキュリティサービス事業者のサーベイランス実施に関する検討ワーキンググループ（以下、「WG」という。）の会合を開催した。

表 2　構成員一覧（◎＝座長）

対象者名(敬称略)	所　属
大木 榮二郎◎	工学院大学 名誉教授
川名 正幸	アイティーム(個人事業主)
神林 彰	富士ゼロックス株式会社 CP&RM 部 情報セキュリティセンター センター長
高橋 正和	株式会社 Preferred Networks 情報セキュリティ最高責任者 セキュリティアーキテクト
丸山 司郎	株式会社ベネッセインフォシェル 代表取締役社長
湯淺 墾道	情報セキュリティ大学院大学 情報セキュリティ研究科 教授

表 3　開催状況

時期	回	概要
平成 30 年 11 月 22 日	第 1 回	①本ワーキンググループの開催要綱について ②本ワーキンググループにおける検討内容について
平成 31 年 3 月 6 日	第 2 回	①サーベイランス実施結果についての審議

（２）情報セキュリティサービスの高度化方策に関する検討会

より良い情報セキュリティサービスの情報提供のあり方について審議するため、表５の構成員にて表６の要領にて情報セキュリティサービスの高度化方策に関する検討会（以下、「検討会」という。）の会合を開催した。

表 4　構成員一覧（◎＝委員長）

対象者名	所　属
阿部　恭一	ANA システムズ株式会社品質・セキュリティ監理室エグゼクティブマネージャ
川口　洋	株式会社川口設計　代表取締役
小松　靖直	日本商工会議所　情報化推進部　部長
小屋　晋吾	一般社団法人コンピュータソフトウェア協会（CSAJ）セキュリティ委員会副委員長
佐藤　元彦	伊藤忠商事株式会社 IT 企画部技術統括室 ITCCERT 上級サイバーセキュリティ分析官
下村　正洋	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）事務局長
土居　範久◎	慶應義塾大学　名誉教授
永宮　直史	特定非営利活動法人日本セキュリティ監査協会（JASA）事務局長
宮下　清	一般社団法人日本情報システム・ユーザ協会（JUAS）常務理事

表 5　開催状況

時期	回	概要
平成 30 年 12 月 7 日	第１回	①本検討会の開催要綱について ②本検討会における検討内容について
平成 31 年 1 月 22 日	第２回	①情報セキュリティサービスにおけるカテゴリの考え方について
平成 31 年 3 月 13 日	第３回	①情報セキュリティサービスにおけるカテゴリの考え方について ②次年度以降の進め方について ③その他

３．基準適合サービスリストに掲載されたサービスに対するサーベイランス

平成 30 年 6 月に公開が開始された基準適合サービスリストの掲載サービスを対象として、その申請内容に事実との齟齬がないかどうかを検証するためのサーベイランスを実施した結果について示す。

３．１ サーベイランス仕様の検討

本年度事業において実施したサーベイランスの仕様は次の通りである。

（１）対象

平成 30 年 6 月までに基準適合サービスリストに掲載された 46 事業者とした。

（２）実施件数

サービスの種類による実施上の課題を把握する観点から、現在登録対象となっている 4 サービスから 1 件ずつ、合計 4 件について実施した。

（３）実施方法

既存の情報セキュリティサービス審査登録機関において計画している実施方法に準じる形で実施した。

３．２ サーベイランスの実施経緯

サーベイランスを実施手順は次の通りである。

（１）サーベイランス項目案（チェックリスト）の作成

第１回 WG における議論を踏まえて、サーベイランス項目を作成した。

（２）サーベイランス実施者の公募と選定

平成 30 年 12 月 12 日～26 日まで、本事業受託者の公開ウェブページにて実施者の公募を行った。上記公募の結果、９者の応募があり、すべての応募者が要件を満たしていた。応募者のサーベイランス対象分野に関する要望をもとに、同条件の応募者を対象に抽選を行った結果、1 月 10 日に４者に依頼することを決定し、1 月 11 日に全応募者に採否を通知した。

（３）サーベイランス対象サービスの選定

３．１（１）の条件を満たすサービスから無作為抽出の結果、４サービスを平成 30 年度のサーベイランス対象とすることに決定し、12 月 21 日に各サービスの提供事業者に通知した。

（４）サーベイランスの実施

事業者への事前説明、関係者間での秘密保持契約の締結の後、サーベイランス実施者によるサーベイランスを実施し、3 月 4 日までにすべてのサーベイランスを完了させた。これには次の内容を含む。

- 書面によるエビデンス資料の確認（概ね１～数日間）
- 品質管理者へのインタビューによる品質管理基準の順守状況の把握（約半日程度）

３．３ サーベイランス結果

サーベイランスの結果、対象となった４サービスとも申請内容との齟齬は検出されず、申請内容が適正であったことが確認され、それらの結果は WG にて了承された。

３．４ 今後に向けた考慮事項

前述の通り、本事業にて実施したサーベイランスにおいて不適合が生ずることはなかったが、今後の実施に際しては次の点に留意する必要がある。

（１）秘密保持契約の締結に要する日数の考慮

サービス提供事業者が大手事業者の場合、法務担当者による契約書の確認に１週間以上を要す

ることがある。本事業で実施するサーベイランスの場合、秘密情報の開示が必要となるのはサーベイランス対象サービスの提供事業者のみであり、当該事業者が用意している秘密保持契約書の様式を用いて契約を締結することで、契約に要する期間を短縮することができる場合もあるため、今後の実施に際しては考慮することが望ましい。

（２）サーベイランスの実施時期の考慮

本事業では第４四半期にサーベイランスを実施することとなったが、この時期を繁忙期とする事業者も多く、品質管理者へのインタビュー日程の調整に苦労するなどの事例もみられた。可能であれば、第２～３四半期において実施するほうが、サービス提供実施者における負担を減らすことができると期待される。

（３）エビデンスの電子化への対応

多くの事業者においてペーパーレス化が進展した結果、サーベイランスにおいてエビデンスとして審査対象となる文書が電子化され、書面としての確認を行うことができず、現地で端末を用いて閲覧せざるを得ない場合が増えてきている。これに伴い、現在半日程度で想定している現地調査の工数が今度増大する可能性が見込まれる。

４．より良い情報セキュリティサービスの情報提供のあり方

基準適合サービスリストに基づいて、より良い情報セキュリティサービスを明示する方法について検討し、そのための制度について取りまとめた。検討の内容は以下のとおりである。

４．１ 情報セキュリティサービス利用における現状の把握

情報セキュリティサービスの利用者が、サービスを利用、選択等する上での現状の課題を明らかにし、課題を解決するために必要な情報、制度は何かについて検討した。

（１）情報セキュリティサービス審査登録制度の概要

平成 30 年 2 月 28 日にセキュリティサービスが最低限の品質を維持するために満たすべき『情報セキュリティサービス基準』及び『情報セキュリティサービス基準に関する審査登録機関基準』を経済産業省にて公表した。独立行政法人情報処理推進機構ではこれらの基準を踏まえて、同年 6 月に「情報セキュリティサービス基準適合サービスリスト」を公表した。同リストを利用することで、中小企業等のように社内に情報セキュリティサービスに関する専門的な知見をもつ人材がいない企業であっても一定の品質維持向上が図られているサービスを選択することが可能になった。同リストを用いたサービス利用のイメージを次図に示す。

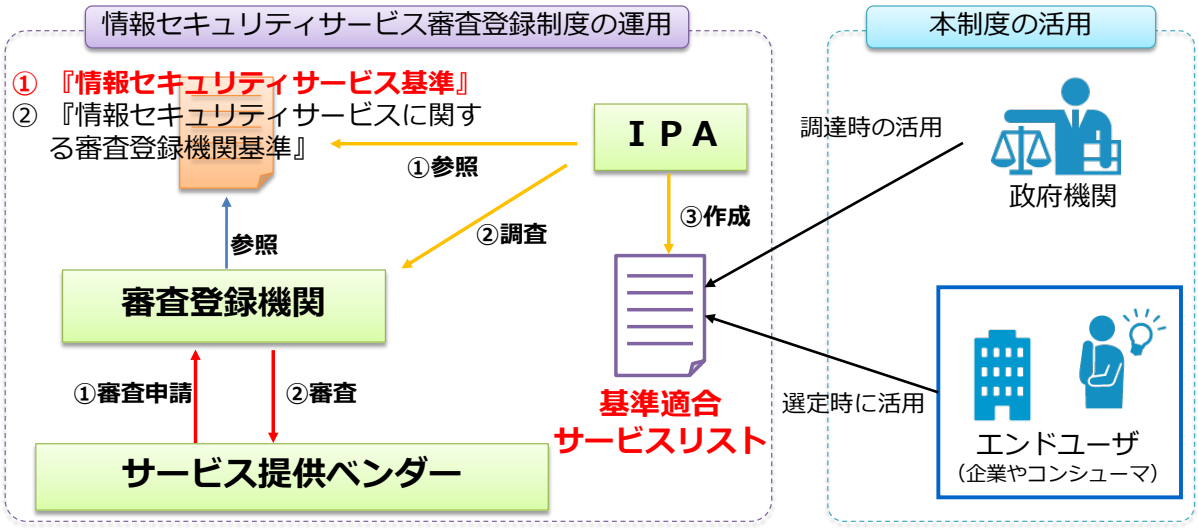


図 2　情報セキュリティサービス審査登録制度の概要

（２）情報セキュリティサービス利用における問題点

（１）の取組を通じて一定の品質を維持・向上している情報セキュリティサービスの選択が可能となった一方で、２．４（２）に示した検討会での審議を通じて、情報セキュリティサービスの利用に関して、次のような課題が指摘されている。

- 現状では、４種類のサービス毎に基準を満たすものが登録順に列挙されているのみであり、サービス内容の特徴を比較・確認するには各社のウェブサイトを参照したり、問い合わせをしたりする必要がある。
- 実際のサービスの中には、制御系システムに特化していたり、レッドチームによる疑似攻撃を含む脆弱性診断を行ったりするなどの特徴により、通常のサービスよりも高い価格設定を行っているサービスも存在するが、サービスベンダにおいてこうした付加価値を基準適合サービスリスト上で示そうとしても、その手段はサービス名称程度に限定されるため、サービスの差別化を図ることが難しい。
- 基準適合サービスリスト上に掲載されているサービスの名称は、サービスの内容が同一であっても各社で異なっていることがある。
- 中小企業やこれまで情報セキュリティサービスを利用したことがない企業にとっては、基準適合サービスリストに挙げられているサービスの名称になじみがなく、自社で相談したい内容がどこにあるのかわかりにくい。

（３）サービスの利用側のおける現状と要望

情報セキュリティサービスにおける（２）で示された意見について、制度を利用する企業側の関係者へのヒアリング調査を通じて、次の意見を得た。

① 重要インフラ関連企業

- 同じ脆弱性診断でも、情報系と制御系では留意すべき点も異なる。制御系に強い事業者であることがわかるとよい。
- 脆弱性診断、監視・運用には制御系向けのカテゴリを設けてはどうか。金融基幹系も同様に別扱いではないか。
- 脆弱性診断とペネトレーションテストでは必要なスキルに大きな差があるので、同一のカテゴリで扱うのは不適切である。また制御系のペネトレーションテストの場合はまた別のスキルが必要となる。
- 制御系ではレガシー環境を未だに用いている場合は多い。こうしたレガシー環境に関する知見・経験が豊富で、その危険性に応じたサービス提供ができるのであれば、それをアピールしてもらえると選定時の参考になる。
- デジタルフォレンジックに関して、自社で攻撃を受けて、被害を受けたかどうかがわから

ない時の「かけこみ相談」「緊急相談」に相当するサービスがわかるとよい。サービス名称だけではデジタルフォレンジックの対象が情報系かネットワーク系かもわからない。

- 品質が高くても新規受注の余力が無いのでは困る。即時対応可能かどうかがわかるとありがたい。
- サービスの価格イメージを示してもらえると良いが、規模・環境等に大きく依存するため価格イメージの提示が難しいのも理解している。
- サービスに「よろず相談」が含まれていることを重視している。専門的知見をもたないユーザはサービスの切り分けもできない。
- サービス提供を通じて本番業務を止めてしまうようなトラブルを起こす事業者に関する情報は、現状では ISAC などを通じて口コミで共有する程度であるが、それが事業者の評価を下げるような形で可視化できるとよい。

② 中小企業

- ほとんどの中小企業は、このようなサービスの利用までたどりつかないのが現状である。また費用の負担能力もない（ただし、IT に立脚したベンチャー企業は例外）。
- 中小企業向けの営業はコストがかかるため、中小企業向けのサービスを扱っているベンダの営業はユーザ企業からの相談を待つスタイルにならざるを得ない。よって、中小企業に何らかのアクションを促すような取り組みが必要。
- 中小企業の利用も可能というマークや列をリストに設けてもよいのではないか（旅館やレストランの「おひとり様も歓迎」のイメージ）。
- 特に規模の小さな企業については、情報セキュリティサービスを自分で利用するのではなく、情報セキュリティサービスが組み込まれた SaaS 型の IT サービスを利用する形になるのではないか。

こうした指摘を踏まえて、制度のさらなる普及のためには、基準適合サービスリストに掲載されたサービスがどのようなものかをわかりやすく伝えるための方策が必要と考えられる。

（4）サービスの提供側による現状認識

（3）と同様に、ベンダへのヒアリング調査を通じて、次の回答を得た。

- サービスレベルの違いはサービサーの能力の差よりも顧客側の事情（予算、要件）に依存することが多く、顧客の要求事項に応じて、それに合ったサービスを提供している。
- 金融系以外の顧客は、業務上の重要度に応じて高度なサービスを利用しようとするモチベーションが低い。
- 脆弱性診断は、診断ツールの出力結果をそのまま提示するだけでよいので安く提供してほしい、というニーズもある。

４．２ より良い情報セキュリティサービスを評価する指標とその伝え方の検討

「より良い情報セキュリティサービス」の概念を検討するとともに、より良さを具体的に伝える方法についての比較を行う。

４．２．１ 候補となり得る指標の例示と比較

社会においてサービスを比較するために用いられている指標について、それぞれの導入事例、利点と欠点を整理した結果を次ページの表に示す。

表 6　社会で実施されているサービスの評価方法の比較

分類	評価方法・指標	概要	サービスの評価例	利点	欠点
人（個人）が評価する	利用者レビュー（利用者満足度）	サービスの利用経験者が当該サービスの品質等について段階的に評価し、その平均値を評価値とする。	・ホテルやレストランのユーザレビュー	・実際に利用した利用者の意見に基づくため、実態を反映したものとなる可能性が高い。	・利用社数が少ないサービスの場合、十分なサンプルが集まらず、評価が偏る恐れがある。 ・不正なレビューを完全に排除することが難しい。
人（グループ）が評価する	有識者（専門家）レビュー	情報セキュリティ分野の有識者（専門家）が当該サービスの品質等について段階的に評価し、その平均値を評価値とする。	・政策評価（事業（プロジェクト）評価、制度評価、追跡評価など）	・一般にどこが優れているかの説明が併記されることが多く、利用者にとってわかりやすい。	・専門家の主観に左右されたり、サービス提供者の意図が伝わらなかったりする恐れがある。 ・大手事業者を評価する場合に、中立的な有識者の確保が困難。
	表彰	サイバーセキュリティの普及等の社会的効果への貢献の高いサービスを表彰する。	・NISC表彰 ・経済産業省情報処理月間表彰	・表彰されたサービスは、社会的に認められたものであることが明確である。	・条件を満たすサービスが複数あっても、表彰対象数の上限があると表彰されないサービスが生じる恐れがある。
ある基準を満たしているかどうかで評価する	適合性の有無	ある条件に適合しているかどうかの判定を行う。	・CSマーク ・PCIDSS認定	・目的に応じて複数の条件についての適合性の有無を示すことで、目的に応じた選定に用いることが可能。	・つねに適合しているか否かの0/1で判定され、中間的な段階の表現ができない。
測定可能な数値で評価する	費用対効果（コストパフォーマンス）	費用あたりの効果（あるいはサービス単位あたりの費用）を定量化して評価値とする。	・相見積もり	・サービスの投資に見合う効果をわかりやすく把握することが可能。	・情報セキュリティサービスの場合は効果の定量化が非常に難しい。
	性能試験結果	性能のうち定量的に比較可能なものについて評価値とする。	（サービスについては該当なし？）	・客観性をもつ機関が実施することで、公平な比較が実現可能。	・性能試験がサービスの一部の性能しか表象していない場合、誤解が生ずる恐れがある。
	市場シェア（占有率）分析	ある市場（マーケット）における各サービスの利用状況を定量的に比較する。	・ガートナー、IDC、富士キメラ等の市場調査レポート	・市場原理に基づく利用者による評価を把握することが可能。	・客観的なデータの入手が困難 ・営業力などサービスの本質以外の要素に左右されやすい。

４．２．２ 類似サービスに対する評価の事例

情報セキュリティサービスに類似したサービスを評価する制度として、現在運用されている事例について調査した結果を以下に示す。

（１）米国における FedRAMP 制度

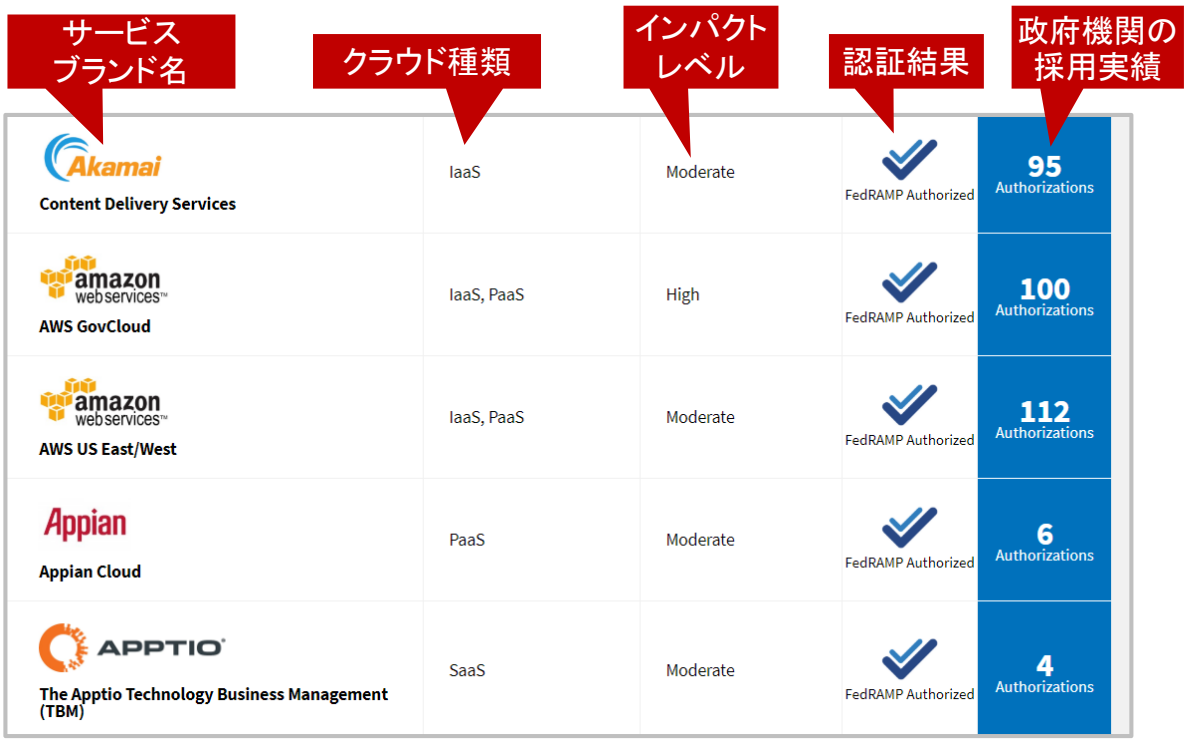
クラウドコンピューティングサービスを対象とする米国連邦政府の調達要件に関する認定制度として知られている。政府内で運用されているが、適合性の評価は民間の評価機関が行う。対象機関のいずれか１機関で認定されると、すべての対象機関で認定対象となる点が事業者にとってのメリットとなっている。

同制度では、政府機関による利用に適した品質について、下表に示す４種類の「インパクトレベル」を定義している。

表 7　米国における評価事例（FedRAMP）

<table>
<tr><th>インパクトレベル</th><th>定義（機密性/完全性/可用性が損なわれた場合の影響）</th><th>管理策例１
（ペネトレーションテスト）</th><th>管理策例２
（モバイル機器の接続）</th></tr>
<tr><td>低位SaaS</td><td>ログイン情報以外の個人識別情報を格納しないSaaSアプリケーション</td><td rowspan="2">不要</td><td>不要</td></tr>
<tr><td>低位</td><td>限定的な悪影響を及ぼすことが予想されうる情報を扱うクラウドサービス</td><td rowspan="3">モバイル機器の使用条件を定め、条件を満たす機器についてのみ、組織内システムへの接続を許可する</td></tr>
<tr><td>中位</td><td>重大な悪影響を及ぼすことが予想されうる情報を扱うクラウドサービス</td><td rowspan="2">必要と判断したシステムについて、一定頻度で実施</td></tr>
<tr><td>高位</td><td>致命的または壊滅的な悪影響を及ぼすことが予想されうる情報を扱うクラウドサービス</td></tr>
</table>

このインパクトレベルへの適合性について、民間の第三者評価機関による評価の結果を FedRAMP のウェブサイト上で表示することで、クラウドサービスを利用しようとする公的機関が参考にできるようにしている。この表示例を次ページに示す。



https://marketplace.fedramp.gov/#/products

図 3　FedRAMP サイトにおけるインパクトレベルの表示例

（２）Kantara Initiative

Kantara Initiative は ID 標準化団体の相互連携を目的とするグローバルなオープンコミュニティである。ID 認証方法に関して、Identity Assurance Framework（IAF）を定義し、その中でユーザの識別に求められる信頼性に応じて４段階の“Assurance Level（保証レベル）”を定義している。これは、NIST SP 800-63-2「電子認証ガイドライン」に準拠しており、Kantara Initiative の定める基準をもとに、サービス認定機関が評価を実施する。ユーザに相当する認証連携を行う機関（政府機関等）は、このようにして公表される保証レベルに応じてサービスの提供可否を決定することができる。レベルの定義を次表に示す。

表 8　Assurance Level（保証レベル）

保証レベル	定義	例	クレデンシャル管理
AL 1	サービスで扱うIDに秘匿性や信頼性が不要なサービスや、コンテンツの暗号化が不要なサービス	ニュースサイトへのユーザ登録	PINとパスワード
AL 2	サービスで扱うIDに秘匿性や信頼性が求められるサービス	受取人の住所変更手続き	１要素認証：認証プロトコルを通じたトークンの検証制御
AL 3	サービスで扱うIDに高度な秘匿性や信頼性が求められるサービス	ネット証券のアカウントへのアクセス	多要素認証：ソフトウェアトークン、ハードウェアトークンまたはワンタイムパスワードの組合せ
AL 4	サービスで扱うIDにきわめて高度な秘匿性や信頼性が求められるサービス	規制医薬品の処方または百万ドルの銀行振込	多要素認証かつハードトークンを組合せ、認証プロセスと暗号プロトコルを結合

４．２．３ 情報セキュリティサービスにおける望ましい評価の方法

表６に示した評価方法のうち、４．２．２に示した２件の事例はいずれも「ある基準を満たしているかどうかで評価する（適合性の有無）」による評価を採用している。情報セキュリティサービスは、

- サービスの品質を定量的に表現することが困難
- 利用者（人）による主観的な評価になじまない

といった特徴をもつことから、上述の事例と同様、適合性の有無によって評価することが適切と判断される。

４．３ より良い情報セキュリティサービスの評価方法のあり方の検討

４．２で取りまとめた評価指標を具体的に測るための情報の収集方法及び評価方法について、評価の質（公正性や信頼性）や実行可能性の観点から評価した上で、望ましい方向について検討した。

４．３．１ サービスの特徴を表示するための概念（カテゴリ）

４．２．３において、「ある基準を満たしているかどうかで評価する（適合性の有無）」方法が適切であるという結論が得られたこと、及び検討会において情報セキュリティサービスの利用者向けによりわかりやすい指標を提供する必要があるとの意見が示されたことを踏まえ、情報セキュリティサービスにおけるサービスの特徴を表示するための方法として、次表に基づき「カテゴリ」を定義する。

表 9　情報セキュリティサービスに関する「カテゴリ」の定義

カテゴリ	**情報セキュリティサービスの利用者がサービスを選定時にサービスの種類等を絞り込みするために必要な情報について、基準適合サービスリストで表示可能な内容を規定するもの。**
カテゴリ表示要件	**個別の情報セキュリティサービスについてカテゴリの表示を認めるための要件。ある情報セキュリティサービスが本要件を満たしているかどうかは情報セキュリティサービス審査登録機関によって審査され、適合すると判定されたサービスのみについて、カテゴリの表示が可能となる。**

カテゴリは情報セキュリティサービスの利用者向けに表示の利便性を高めるために導入する新たな概念であり、現行の情報セキュリティサービス基準を維持したままでの導入が可能である。一方で、利用者のニーズは多様であり、前項で提案するカテゴリが利用者にとって真に使いやすいかどうかは、制度を運用していく中で明らかになっていくものと考えられる。そこで、現状において想定されているカテゴリ表示要件（案）を本報告書の別冊に示すものの、審査登録制度へのカテゴリの導入は、試行的な検討を行いつつ、見直しを前提として推進していく必要がある。将来的にはカテゴリを利用することによって、情報セキュリティサービスの利用者が自社のニーズに近いサービスを容易に選定できるようになることを目標とする。このようなカテゴリ活用の考え方を次ページ図に示す。

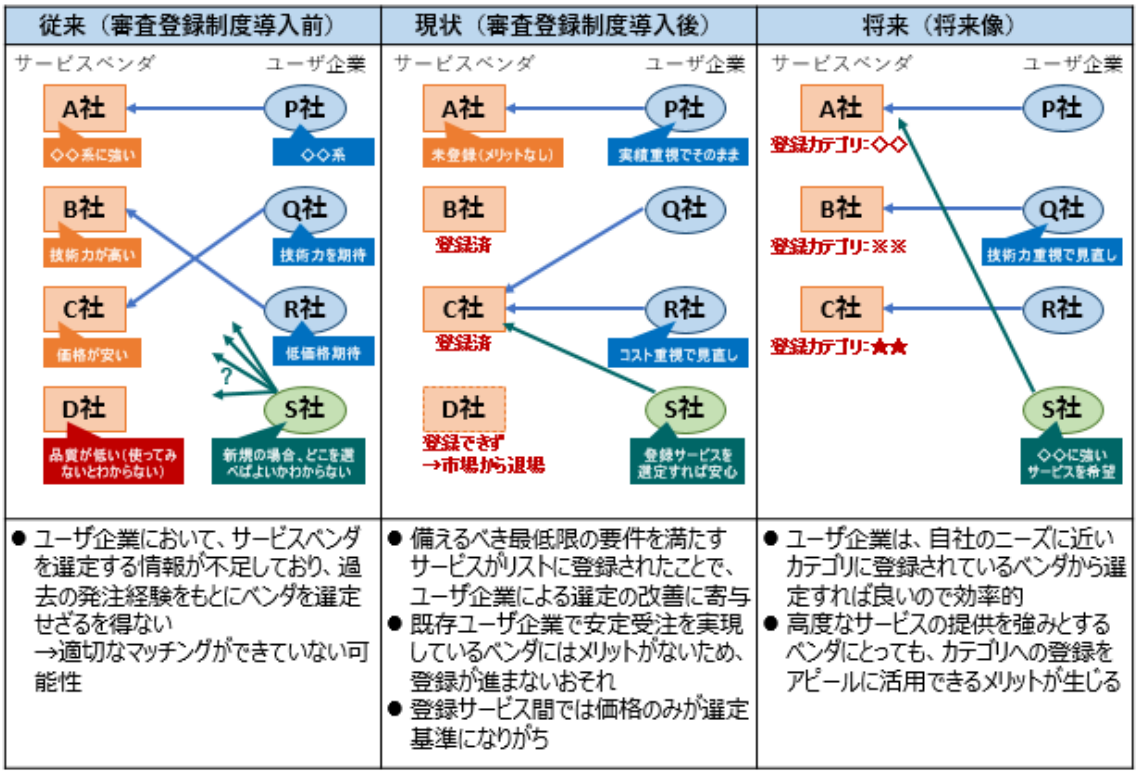


図 4　情報セキュリティサービス審査登録制度におけるカテゴリ活用の考え方

具体的なカテゴリのイメージとしては、検討会における議論を踏まえ、次表のような例が考えられる。詳細は本報告書の別冊を参照。

表 10　カテゴリの例

サービスの種類	カテゴリ例	カテゴリの定義
情報セキュリティ監査	PCIDSS 準拠性監査	PCIDSS において求められるセキュリティ対策要件への適合状況についての情報セキュリティ監査を行うサービス。
脆弱性診断	ペネトレーションテスト	その組織が持つすべて又は指定されたシステム全体を対象として、実際の攻撃者が使用しているツールや脆弱性、ソーシャルエンジニアリングなどを利用して、明確な意図を持った攻撃者が一定期間内にその目的を達成できるかの調査を行う（Web アプリケーション単体やプラットフォーム単体のテストではなく、また網羅的に脆弱性の調査を行うわけではない）。
	IoT 機器向け脆弱性診断	ハードウェア（PC、サーバー、通信機器を除く）と一体で運用される情報システムを対象に、その所定の動作の妨害や、不正な侵入及びアクセスに至る可能性のある脆弱性の有無を確認するサービス。

サービスの種類	カテゴリ例	カテゴリの定義
デジタルフォレンジック	不正調査	情報漏えい・窃取・持ち出し、不正経理他、各種の不正が疑われる際にデジタルフォレンジック専門事業者が不正の有無や事実（証拠）を明らかにするサービス。
	インシデント対応	デジタルフォレンジックを用いて各種セキュリティインシデントやサイバー攻撃等の事実確認、被害範囲の特定、内外への報告書作成等を行うサービス。
	ファストフォレンジック	サイバー攻撃等のセキュリティ侵害が発生した際に早急な原因究明、侵入経路や不正な挙動を把握するため、専用のデータ収集ツールや EDR (Endpoint Detection and Response)利用して必要最小限のデータを抽出及び確認し、解析するサービス。
	訴訟対応支援	裁判（刑事・民事）等の訴訟を前提とした証拠及び事実の収集や捜査機関または弁護士、第三者委員会等へのサポートを目的としたデジタルフォレンジックを用いたサービス。なお、米国訴訟における電子証拠開示（eディスカバリ）対応を目的としたサービスを含む。

４．３．２ 他の取組との連携

審査登録制度におけるカテゴリの導入は、次に示す取組との組合せを通じて、相乗効果によりさらに有効に機能することが期待される。

（１）民間のソリューション検索サービスとの連携

審査登録制度で扱う情報は、制度の利用者からは審査を経たものであると認識されるため、審査を経ない多様な情報を掲載することは不適切である。しかしながら、情報セキュリティサービスを利用する企業等にとっては、サービスの選定に際して基準適合サービスリストに掲載されている情報以外に、当該サービスの特色や、営業地域などについても考慮したいと考えるのは自然である。そこで、こうした情報を参照できる民間のソリューション検索サービスと連携し、検索したサービスが基準適合サービスリストに掲載されているかどうかをリンク等で簡単に確認できるようにすることで、利便性に審査登録制度による信頼性の付加価値を提供するなどの効果が期待できる。

（２）他政策における要件ないし推奨としての活用

カテゴリを導入することは、情報セキュリティサービスを利用する企業のみならず、政策を推進する公的機関等にも好ましい効果を及ぼすことが期待される。具体的には、中小企業等で IT 機器やサービスの利活用を促進するための補助金を提供する際に、そのサイバーセキュリティ対策のためのサービスの併用を条件とする場合において、カテゴリの名称を指定することで、条件と指定が容易になる。また、サイバーセキュリティ対策に関する普及啓発を行うにあたっても、リスクに応じたサービスを推奨する際に、カテゴリの名称を用いて解説することで、理解を容易にする効果が期待できる。

４．３．３ 制度の見直しによって期待される効果

前ページまでに示した見直しや普及に関する取組を通じて、審査登録制度の普及、展開に関する次のような効果が期待される。

（１）サービスを利用したい企業等とのマッチングの改善

情報セキュリティサービスを利用する企業にとって、カテゴリに表示された内容を通じて自社で利用したいサービスであることが理解しやすくなることで、ユーザ企業とサービスとのマッチングの改善が期待される。ただし、カテゴリで表現可能かな情報には限界があるため、４．３．３（１）に示した通り、民間のソリューション検索サービスとの併用により、より効果を高めることが可能となる。

（２）制度の魅力の向上

（１）による効果を通じて、基準適合サービスリストに掲載されたサービスが積極的に選定される傾向が強まることで、サービスを提供するベンダにおいて、審査登録制度に登録するメリットが高まることが見込まれる。この結果、これまでよりも規模の小さな事業者や、地域でサービスを提供する事業者による登録が増えるなどにより、情報セキュリティサービス市場において、基準適合サービスリストに掲載されたサービスの占める割合が高まり、審査登録制度のプレゼンスやインパクトの向上が期待される。

４．４ 今後の方向性

４．４．１ 課題に対するアクションの考え方

これまでの検討を踏まえ、審査登録制度をさらに普及、展開させるための取組の方向性として、検討会における議論をもとに、次のような課題について、その解決に向けたアクションに取り組むことが提案されている。

（１）課題１：制度の認知度が低い

制度発足から間もないこともあって、現状においては特に情報セキュリティサービスを利用するユーザ企業における本制度の認知度の低さが、制度の効果が発揮されない最大の要因となっている。そこで、企業において情報セキュリティサービスの調達を行う担当者や、最高情報セキュリティ責任者（CISO）、経営層などが、本制度を認知するように次のような取組を行うことが考えられる。

① セミナー等の機会を活用した普及啓発活動の実施

経済産業省やその関係機関において、全国でサイバーセキュリティ対策に関する普及啓発セミナー等を開催する際に、あわせて本制度の紹介を行うことで、サイバーセキュリティ対策に関心をもつユーザの認知度を効果的に高めることができるものと期待される。

② 「情報セキュリティサービスマーク」表示の推進

審査登録機関では、本制度について次図のようなマークを定め、登録事業者が自社のウェブページ等の対外公表物に、当該サービスが情報セキュリティサービス基準に適合することを示す手段として同マークを掲載することを認めている。このマークが掲載されているサービスは情報セキュリティサービス基準に適合するサービスであるということが周知されることで、ユーザへの本制度の認知度が向上すると期待できることから、基準適合サービスリストに掲載されているベンダに当該マークの積極的な表示を促すことが考えられる。

図 5　情報セキュリティサービスマーク

（２）課題２：登録のメリットが不十分

情報セキュリティサービスを提供するベンダにおいて、審査・登録のための費用を負担しても、

それに見合うメリットが十分に感じられない。（1）に示した制度の認知度が低いことによるところが大きいが、改善のために次のようなアクションが考えられる。

① 政府機関を対象とするセキュリティ基準での参照の拡大

政府機関が実施すべき情報セキュリティ対策を定める「政府機関の情報セキュリティ対策のための統一基準群」においては、平成 30 年度版の「政府機関等の対策基準策定のためのガイドライン」において、外部事業者に情報セキュリティ監査を委託する場合に、本制度の基準適合サービスリストを参照することが示されている。同ガイドラインに記載されることにより、様々な政府機関におけるサービス調達の際の調達要件もしくは推奨事項となることが期待され、ベンダにとっての本制度への登録のインセンティブとなることから、情報セキュリティ監査以外のサービスについても参照されるように関係機関への働きかけを行うことが考えられる。

② 本制度の利用に関する働きかけの実施

①は政府機関向けのガイドラインを対象としたものであるが、他にも特定業界や業務向けの情報セキュリティ基準やガイドラインを策定・運用している公的機関や民間団体が存在する。こうした機関等に対し、情報セキュリティサービスを利用する場合の選定に際して、本制度の利用を働きかけることで、それぞれの基準やガイドライン等で参照され、同様にベンダにとってのインセンティブとなるような効果が得られるものと期待される。

例えば、現状においては①に示す「政府機関等の対策基準策定のためのガイドライン（内閣サイバーセキュリティセンター）」の他、以下の制度・ガイドライン等にて、基準適合サービスリストが参照されている。

- 地方公共団体における情報セキュリティ監査に関するガイドライン 平成 30 年 9 月 25 日版（総務省）
- 「革新的データ産業活用計画」認定申請のご利用の手引き（コネクテッド・インダストリーズ税制）（経済産業省）
- 小さな中小企業と NPO 向け情報セキュリティハンドブック Ver.1.00（内閣サイバーセキュリティセンター）
- 中小企業の情報セキュリティ対策ガイドライン 第３版（独立行政法人情報処理推進機構）

（3）課題３：対象サービスが限定的

現行の情報セキュリティサービス基準において審査及び登録が可能なサービスは４種類にとどまっているが、これは適切な品質のサービスを提供可能かどうかの審査を行うための要件がサービスの特徴に応じて異なることを踏まえ、基準とすべき内容が相対的に明確なサービスを選定したことによるものである。次に例示するようなサービス等、これら４種類以外のサービスに対し

てもニーズは存在している。

① セキュリティアセスメントサービス

情報セキュリティコンサルティングサービスには多様なサービスが含まれ、その実施に必要な要件も同様に多様であるため、一定の品質を確保するサービスに求められる要件を明確化することは容易ではない。その中で、コンサルティング業務の一要素に相当するセキュリティアセスメントサービスについては、組織の特徴に応じてセキュリティ上の脅威に関するリスクアセスメントを行うことの重要性が高いのと同時に、アセスメントに必要なスキル等を明確化することが比較的容易であることから、情報セキュリティサービス基準の対象として追加することが可能と考えられる。

② セキュリティ教育サービス

情報セキュリティ分野を対象とする教育サービスとしては、専門人材の育成サービスのほか、経営層や一般を対象とする教育サービスなど、多様なサービスが含まれる。いずれにしても、教育サービスについては、一定の品質を確保するための要件は、教育に関するスキルと情報セキュリティに関する専門性のそれぞれに関する知識やスキル、経験等を明確化することが比較的容易であることから、①と同様に情報セキュリティサービス基準の対象として追加することが可能と考えられる。

（4）課題４：ユーザ企業にとってわかりにくい

情報セキュリティサービスは一般になじみのない専門的な技術をもとに提供されることから、一般のユーザにとってわかりにくいことはある程度避け得ないことであるが、今後の制度の普及に向けて、次のような改善策が考えられる。

① カテゴリの導入を通じた改善

４．３．１にて示したカテゴリの導入は、制度の利用者にとって理解しやすい名称の使用などの工夫を行うことで、わかりやすさの改善につながるものと期待される。

② 民間のソリューション検索サービス等の相互連携

４．３．２（1）にて示した民間のソリューション検索サービスとの連携により、本制度の審査対象情報に含まれない営業地域などの条件など、制度の利用者の希望に応じたサービスの選択と、本制度による信頼性の付加価値との併せ持つ選定が可能となることが期待される。

４．４．２ 基準適合サービスリストにおける表示ルールについて

審査登録機関より、情報セキュリティサービス基準適合サービスリストにおけるサービス名称がもたらす混乱の恐れについて指摘があり、次のような改善の方向性が検討されている。

（１）懸念される問題

現在の情報セキュリティサービス基準には登録するサービス名称についてのルールがない。この結果、次のような問題と思われる事例があり、利用者の混乱を招く恐れがあることが指摘されている。

① 問題と思われる事例（情報セキュリティ監査サービス）

- 情報セキュリティ監査の名称ではなく、コンサルティングや支援サービスなどの名称で登録されている
- 事業者のホームページにおけるサービスの名称では監査サービスが分かりにくい
  －サービスに関する表示がない
  －他のサービスの一部として埋もれてしまっている

② 問題と思われる事例（デジタルフォレンジックサービス）

- インシデントレスポンスや緊急対応という名称が多い

（２）対応の方向性

（１）の問題を踏まえ、サービス名称については、対象サービスが基準の範囲内であることが明確になるような名称に関するルールを明確にすることが適切と考えられる。ルールのイメージを次表に示す。

表 11　サービス名称に関するルールのイメージ

1. **審査登録制度におけるサービス名称は、情報セキュリティサービス基準に示されたサービス（以下、基準対象サービス）であることが明確になるように表示する**
2. **基準対象サービスが複数のサービスを含む総合サービスの一部として提供している場合には、サービス名称の後に（　）で総合サービスの名称を記載する**
3. **サービス名称に複数のサービスが列挙されている場合、基準対象サービス以外の表示をしてはならない**
4. **登録名称と申請登録者が、ホームページ等で公開する名称は一致させる**

このガイドラインを適用することによる、サービス名称の例示のイメージを次ページ表に示す。

表 12　ガイドラインによる例示のイメージ

	望ましい表示例	望ましくない表示例
1	助言型情報セキュリティ監査サービス（セキュリティプロフェッショナルサービスの一部として実施）	セキュリティプロフェッショナルサービス
2	情報セキュリティ監査サービス	セキュリティポリシー策定支援サービス、 リスクアセスメントサービス、 CSIRT 構築支援サービス、 情報セキュリティ監査サービス、 セキュリティ教育サービス
3	デジタルフォレンジックサービス（インシデント対応支援サービスの一部として実施）	インシデント対応支援サービス

５．まとめ

本事業では、審査登録制度に対する信頼度と利便性の向上を通じ、更なる普及、発展を実現させるため、パイロット登録事業者に対するサーベイランス実施と、より良い情報セキュリティサービスの可視化のあり方について検討した。本事業で実施した成果は、今後の制度運用を通じて、我が国における情報セキュリティサービスの普及を通じた安全性の向上に寄与することが期待される。