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
別冊　情報セキュリティサービス表示の考え方

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

１．背景

（１）情報セキュリティサービス審査登録制度の抱える課題

経済産業省が公表した「情報セキュリティサービス基準」に基づき、平成 30 年度より運用が開始された情報セキュリティサービス審査登録制度は、情報セキュリティサービスに関する専門的な知見を有する人材を確保することが困難な企業等において、信頼に足るサービスを選定するための手段として普及と活用が期待されているが、今後の普及と活用に向けて抱えている課題として、以下の２点が挙げられる。

① 利用者にとってのわかりやすさの改善の必要性

情報セキュリティサービス基準は、「情報セキュリティ監査サービス」、「脆弱性診断サービス」、「デジタルフォレンジックサービス」、「セキュリティ監視・運用サービス」の４種類のサービスによって構成されている。これらが「情報セキュリティサービス」という一括りでなく、４種類の独立したサービスとして定義されているのは、それぞれのサービスの提供に用いている技術や方法論が異なることから、適切なサービスかどうかの審査基準がサービス毎に異なっていることによっている。

一方で、企業等のサービスの利用者が情報セキュリティサービスを利用しようとして、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、「リスト」という。）を参照するとき、サービスを通じて行いたいことと、４種類のサービスの名称とは必ずしも一致するとは限らない。例として、自社で利用している情報システムが脆弱性に対して適切に対策されているかどうかの診断を行いたい場合、「脆弱性診断サービス」に対応するリストに掲載されているサービスから選択すればよいので問題ないが、自社で実施している情報セキュリティ対策が適切かどうかを総合的に検証したい場合、情報セキュリティマネジメントの適切性を検証するのであれば「情報セキュリティ監査サービス」の利用が、技術的な対策のうち脆弱性対策を検証するのであれば「脆弱性診断サービス」の利用がそれぞれ適切であって、２種類のリストが参照対象となる。また、外部からのサイバー攻撃で被害が生じているかどうかを専門家に確認してもらいたい場合、インシデントレスポンスに相当するサービスを、「デジタルフォレンジックサービス」のリストの中から選択することになる。このように、現状の情報セキュリティサービス基準を構成するサービスの名称は、目的とするサービスを選ぶというための手段という観点からはわかりやすいとは言えない。

② 品質の高いセキュリティサービスを提供する事業者とのマッチングの改善

現在の情報セキュリティサービス基準は、必要最低限の品質を確保しているサービスであればリストに登録可能としているため、より質の高いサービスを提供している事業者が同リストにおいて差別化を図ることが困難であり、低価格のサービスが有利になるとの意見がある。品質の高いサービスを有利に扱うためには、品質の高いサービスのみが適合可能な基準を設ける

ことが考えられる。しかしながら、情報セキュリティサービスはITを用いて行われる何らかの業務について、その情報セキュリティ対策を提供するためのものであり、サービス自体の絶対的な価値を判断することは困難である。「品質が高い」サービスとは、「情報セキュリティ対策のレベルが高い」ことであるとは限らず、サービスを利用する企業等の利用者のニーズに近いものが品質が高いサービスであると考えられる。ゆえに、サービスを利用する企業にとって品質の高いサービスを提供可能とすることは、リストに掲載されたサービスと企業のニーズとのマッチングを容易にすることに相当する。

（２）課題解決の方向性

（１）における課題の特徴を踏まえると、情報セキュリティサービス審査登録制度の普及と活用を今後一層促進していくためには、リストに掲載されているサービスが有する特徴を、サービス利用者にとってわかりやすい形で表示する手段を提供することが適切であると考えられる。その手段として、次表に基づき「カテゴリ」を定義することが考えられる。

表 1　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、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。**

（３）カテゴリを用いた情報セキュリティサービスの表示に求められる条件

カテゴリを用いて情報セキュリティサービスを表示する場合、課題解決の趣旨を踏まえ、カテゴリは次の条件を満足させることが求められる。

① カテゴリ表示要件を満たすかどうかの基準が明確であること

カテゴリを表示可能かどうかは、現在の情報セキュリティサービス基準と同様、審査登録機関による適合性の審査に基づいて決定される。よってカテゴリ表示要件として規定される内容は、適合性を容易に審査できるよう、曖昧性を含まないことが求められる。

② カテゴリの名称からサービスの特徴をイメージしやすいこと

カテゴリは利用者によるサービスの選定を支援するために設けられるものであり、その名称はサービスの特徴をイメージしやすいものであることが望ましい。

③ 中立性

カテゴリの名称は、特定のサービスを連想させるようなものであってはならず、サービスを提供する事業者に対して中立的である必要がある。

２．カテゴリによるサービスの表示例

有識者による会議体での検討結果をもとに、１．に示した背景を踏まえて作成したカテゴリのイメージを次ページ表に示す。

表 2　カテゴリのイメージ

注）ここに記載しているカテゴリはいずれも説明のための例示であり、将来的に導入されるカテゴリは改めて検討される予定である。

サービス名称	カテゴリ名称	カテゴリの定義	カテゴリ表示要件		審査用エビデンス
情報セキュリティ監査サービス	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。	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
			イ　サービス提供に関する手順の規定	監査項目及び手順書が整備されていること	当該サービスの監査項目及び手順書
脆弱性診断サービス	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）。	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員が参加した案件の診断実施計画書、報告書等
			イ　サービス仕様の明示	診断実施計画にゴール設定に基づく攻撃シナリオ及び脆弱性を利用した攻撃の実施を含むこと	当該サービスの仕様を定義した文書
	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。	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
			イ　サービス提供に関する手順の規定	以下の内容を含む要員向け手順書が整備されていること: ・検出できる脆弱性の範囲 ・構成情報のヒアリング ・機器の預かり証の発行	当該サービスの手順書又は提案書、報告書のサンプル
デジタルフォレンジックサービス	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。	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
	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。**	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
			イ　サービス提供に関する手順の規定	以下の内容を含む要員向け手順書が整備されていること ・インシデント発生状況のヒアリング実施方法 ・被害拡大を防止するための初動対応に関する実施方法 ・調査対象となる電子記録媒体の	当該サービスの提案書、調査報告書のサンプル インシデント発生状況のヒアリング項目に関するテンプレート 初動対応に関する対応手順書

サービス名称	カテゴリ名称	カテゴリの定義	カテゴリ表示要件		審査用エビデンス
				証拠保全の実施方法 ・証拠保全及び保全後のデータに対する調査解析の実施方法	証拠保全及び調査解析を行うための手順書
	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。**	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
			イ　サービス提供に関する手順の規定	以下の内容を含む要員向け手順書が整備されていること ・顧客へ貸与するファストフォレンジックツールの使用方法 ・顧客が使用するEDR製品を利用したファストフォレンジックの実施方法 ・顧客のファストフォレンジック対象の環境のヒアリング	ファストフォレンジックツールまたはEDRを利用した対応手順書
	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。**	ア　実施体制の整備	サービス提供体制に1名以上の経験者を含むこと	当該要員の業務経歴
			イ　サービス提供に関する手順の規定	以下の内容を含む要員向け手順書が整備されていること ・コンフリクトチェックに関する規定とのその確認方法 ・弁護士など外部の調査対応者に対する電子データのレビュー環境の提供方法 ・EDRM（The Electronic Discovery Reference Model）の各工程におけるサービスの提供方法	当該サービスの提案書 サービス提供のための社内体制に関する資料 電子データレビュー環境の使用手順書 コンフリクトチェックに関する規定と確認のための手順書 EDRMの各工程に対する対応ポリシーと仕様書