（参考資料）１．サイバーセキュリティの設問趣旨（１/３）

本公募の応募フォームにおける「サイバーセキュリティ」に係る設問の趣旨について、以下にご説明します。

設問設置の背景※1	➢ 近年、産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まり、企業においてOSS※2を含むソフトウェアの利用が広がっております。 ➢ サイバー空間とフィジカル空間の融合が進む一方、ソフトウェアの脆弱性が企業経営に大きな影響を及ぼすなど、セキュリティ脅威が増大しています。このため、セキュリティを強化するためのソフトウェア管理が重要になりますが、ソフトウェアサプライチェーンが複雑化し、OSSの利用が一般化する中で、自社製品において利用するソフトウェアであっても、どのようなソフトウェアコンポーネントが含まれているのかを把握することが重要です。
目的	➢ 技術カタログ掲載にあたり、機能的な観点に留まらず、サイバーセキュリティ、ソフトウェアサプライチェーン管理の観点で製品・サービスの情報をご提供いただくことを目的としています。

※1：出典：経済産業省
「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引」にもとづき作成
※２：OSSとは、ソフトウェアのソースコードが無償で公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェアのことである。OSS の概念及び志向は、世界中のユーザーがソースコードを共有の知的財産として扱い、修正や改良を重ねながらより良いソフトウェアへと磨き上げていくことである。
出典：経済産業省
「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」より抜粋

（参考資料）１．サイバーセキュリティの設問趣旨（２/３）

セキュリティ認証取得や脆弱性対策、データの取扱いに関する設問、およびソフトウェアサプライチェーン管理についての設問から、製品・サービスに関する網羅的なセキュリティ情報をご提供いただくことを目的としています。

質問セクション	カテゴリ	設問名	趣旨
サイバーセキュリティ	セキュリティ認証の取得	組織/法人のサイバーセキュリティ管理に関する認証について【必須】	製品・サービスについて、システムの適切な設計と正しい実装に関する第三者認証の情報をご提供いただくことを目的としています。 併せて、組織として取組んでいるセキュリティ対策情報もご提供いただくことを目的としています。
		製品・サービスにおける「ISO/IEC 15408認証」、「CCDS認証」の取得状況について【必須】	
		「ISO/IEC 15408認証」における、取得しているCCのレベル（EAL）及び対象のProtection Profile（PP）について【必須】	
		「CCDS認証」における、下記のサイバーセキュリティ認証について【必須】	
		その他製品・サービスに関する認証【任意】	
	脆弱性への対策	サイバーセキュリティにおける脆弱性検査の実施状況について【必須】	外部からの不正アクセスやデータの改ざん等の脆弱性について、製品・サービスに対して具体的に実施している脆弱性検査の内容の情報をご提供いただくことを目的にしています。
		国内外発刊のガイドラインに準拠した脆弱性検査について【必須】	
		脆弱性検査の具体的な実施内容について【必須】	
		脆弱性検査の実施に関する検討状況について【必須】	
		脆弱性検査を実施していない理由について【必須】	
	業務データの取扱い	取扱い業務データの保存国【必須】	クラウドサービスに保存される業務データ（個人の機密データを含む）が安全に取扱われ、外部への漏洩・改ざん等のリスクへの対応状況について、情報をご提供いただくことを目的としています。
		取扱い業務データの機密性確保に関する対策【必須】	

（参考資料）１．サイバーセキュリティの設問趣旨（３/３）

セキュリティ認証取得や脆弱性対策、データの取扱いに関する設問、およびソフトウェアサプライチェーン管理についての設問から、製品・サービスに関する網羅的なセキュリティ情報をご提供いただくことを目的としています。

質問セクション	カテゴリ	設問名	趣旨
サイバーセキュリティ	ソフトウェアサプライチェーン管理の対策	ソフトウェアが有している機能【任意】	重要なソフトウェア※1とみなされる機能の有無について、情報をご提供いただくことを目的としています。
		ソフトウェアおよびソフトウェアを実行するためのプラットフォームに対する保護対策【任意】	ソフトウェアに対して不正アクセスや不正利用から保護する対策の内容について、情報をご提供いただくことを目的としています。
		ソフトウェアを実行するためのプラットフォームで使用されるデータに対する対策【任意】	取り扱うデータの機密性確保等に関する対策の内容について、情報をご提供いただくことを目的としています。
		ソフトウェア・コンポーネントの管理について【任意】	ソフトウェアにて、どのようなOSSを活用しているのかを適切に把握する重要性から、ソフトウェア・コンポーネントの管理、ソフトウェア・コンポーネントに関するインベントリ（ソフトウェア部品表；SBOM：software bill of materials） の作成有無及びソフトウェアの保護対策について、情報をご提供いただくことを目的としています。
		ソフトウェア・コンポーネントに関するインベントリの作成有無について【任意】	
		ソフトウェアの特定と維持管理による保護対策【任意】	
		ソフトウェアを実行するためのプラットフォームに対するインシデントに関する対策【任意】	セキュリティ・インシデント（脆弱性の検知を含む）に関し、効果的な対応を実施するための対策の内容について、情報をご提供いただくことを目的としています。
		セキュリティのリテラシーを向上させる対策【任意】	セキュリティに関わるリスクを低減させる観点等から、貴法人内にて実施しているセキュリティのリテラシーを向上させる対策の内容について、情報をご提供いただくことを目的としています。
		ソフトウェア開発におけるベストプラクティスな手法の実施状況【任意】	セキュリティ・バイ・デザインや品質担保の観点から、ソフトウェアの開発手法について、情報をご提供いただくことを目的としています。

※1：出典：NIST（National Institute of Standard and Technology）「Critical Software」
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory

（参考資料）２．認証の概要

本公募の応募フォームにおいて「サイバーセキュリティ」に係る設問の選択肢に記載されている各認証の概要を以下に示します。

● 認証名・概要

No	認証名	概要説明
1	ISO※1/IEC※2 27001（情報セキュリティ）認証	組織における情報セキュリティマネジメントシステム（ISMS）に関する国際規格である。情報の機密性・完全性・可用性の3つをバランスよくマネジメントし、情報を有効活用するための枠組みを示す。
2	ISO/IEC 27017（クラウドサービスセキュリティ）認証	クラウドサービスに関する情報セキュリティ管理策のガイドライン規格である。クラウドサービスに対応した情報セキュリティ管理体制を構築するための枠組みを示す。
3	ISO/IEC 27701（プライバシー情報）認証	プライバシー情報マネジメントシステムに関する国際規格である。プライバシー情報を保有する組織における情報セキュリティマネジメントシステムの要求事項に加え、個人情報の処理によって影響を受けかねないプライバシーを保護するための要求事項及びガイドラインを規定する。ISO/IEC 27001及びISO/IEC 27002のアドオン（拡張）規格として位置づけられている。
4	JIS※3 Q 15001（個人情報保護）認証	組織が個人情報を適切に管理するためのマネジメントシステムの要求事項を定めたJIS規格（日本産業規格）である。個人情報を取り扱う組織に適用可能な個人情報保護マネジメントシステムの要求事項を規定する。
5	ISO/IEC 15408（CC）認証	情報技術セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されていることを評価するための国際標準規格である。
6	CCDS認証	IoT機器に必要とされるセキュリティ要件の認証である。 認証は、CCDS（Connected Consumer Device Security Council：一般社団法人重要生活機器連携セキュリティ協議会）が独自に策定したガイドラインに基づいて実施している。 ・IoT機器セキュリティ要件ガイドライン2023年度版（CCDS-GR01-2023） ・IoT機器セキュリティ要件ガイドライン2021年度版（CCDS-GR01-2021） ・IoT機器セキュリティ要件ガイドライン2019年度版（CCDS-GR01-2019）

※1　International Organization for Standardization
※2　International Electrotechnical Commission
※3　Japanese Industrial Standards