

仕様書

1. 件名 脆弱性管理クラウドの導入及び整備

2. 目的

国立研究開発法人量子科学技術研究開発機構（以下「QST」という。）では、情報システムの安定運用及び情報セキュリティ確保のため、各種情報システムに係る脆弱性管理を実施している。一方で、対象となる情報システムやその構成要素は多岐にわたり、それらに関する脆弱性情報等を継続的かつ網羅的に把握・管理することは容易ではなく、対応の属人化や管理負荷の増大が課題となっている。また、近年はサイバー攻撃の高度化・巧妙化が進み、脆弱性を悪用した被害の発生リスクが高まっていることから、継続的かつ適切な脆弱性管理が求められている。

本件では、脆弱性管理クラウド（以下「本システム」という。）を導入し、情報システムの構成情報を一元的に収集・管理するとともに、脆弱性情報との照合によるリスクの把握、リスク評価及び優先順位付け並びに対応状況管理を実施するための脆弱性管理環境を整備し、情報システムの構成情報の可視化、脆弱性管理業務の効率化、対応状況の適切な把握及び情報セキュリティ水準の向上を図ることを目的とする。

3. 仕様

別紙「詳細仕様書」を参照のこと。

4. 納品物

下記を電子媒体にて提出すること。

2026年11月30日(月)まで

(ア) 利用マニュアル（オンラインで提供している場合には、当該マニュアル等の参照条件及び参照方法を示す文書を作成し提出すること。）

(イ) サポートやサービス利用に必要な連絡先窓口情報を含む情報やライセンス情報等、一式

2027年3月31日(水)まで

(ウ) 詳細仕様書 4.9) に示す報告書

5. 納入期日及び利用期間

納入期日

2026年11月30日（月）

利用期間

2026年12月1日（火）から 2027年3月31日（水）まで

6. 納入場所

国立研究開発法人量子科学技術研究開発機構

本部 情報基盤管理部 IT セキュリティ課

千葉県千葉市稲毛区穴川 4－9－1

7. 必要な能力・資格等

受注者及び本システムは、以下の要件を満たしていること。認証又は登録に有効期間がある場合は、本システムの利用期間中、当該認証又は登録を有効に維持すること。

- (ア) 本システムが、ISMAP クラウドサービスリストに登録されていること。技術審査資料に登録番号及び登録対象範囲を明示すること。
- (イ) 本システムに係る脆弱性管理サービスが、経済産業省「情報セキュリティサービス基準」適合認定を受けていること。
- (ウ) 本システムの提供を対象範囲に含む ISMS (ISO/IEC 27001 又は JIS Q 27001) 認証を取得していること。

8. 検査

「3. 仕様」に定める作業が完了し、かつ「4. 納品物」に定める納品物が納入されたことを QST が確認したことをもって、検査合格とする。

9. その他

- (ア) 受注者は、QST の情報セキュリティポリシーを遵守すること。
- (イ) 受注者は、本件で取得した QST の情報を、QST の許可なしに本件の目的以外に利用してはならない。本件の終了後においても同様とする。
- (ウ) 受注者は、本件で取得した QST の情報を、QST の許可なしに第三者に開示してはならない。本件の終了後においても同様とする。
- (エ) 本件の履行に当たり、受注者は従業員又はその他の者によって、QST が意図しない変更が加えられることのない管理体制を整えること。
- (オ) 本件の履行に当たり、情報セキュリティ確保の観点で、受注者の資本関係・役員等の情報、本件の実施場所、業務を行う担当者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報を求める場合がある。受注者は、これらの要求に応じること。
- (カ) 本件に係る情報漏えいなどの情報セキュリティインシデントが発生した際には、速やかに Q S T 担当者に連絡し、その指示の元で被害拡大防止・原因調査・再発防止措置などを行うこと。
- (キ) 受注者は、Q S T から本件で求められる情報セキュリティ対策の履行状況を Q S

Tからの求めに応じて確認・報告を行うこと。またその履行が不十分である旨の指摘を受けた場合、速やかに改善すること。

- (ク) 受注者は、本件の履行に必要な場合を除き、機器、コンピュータプログラム、データ及び文書等について、QST の許可なく QST 外部に持ち出してはならない。なお、本システムへの情報送信については、詳細仕様書及び本システムの利用条件に基づくものとする。
- (ケ) 受注者は、本件の終了時に、本件で取得した情報を削除又は返却すること。また、取得した情報が不要となった場合も同様とする。
- (コ) 本件の履行により受注者が新たに作成した成果物の著作権その他の権利の取扱いは、QST と受注者との協議又は契約条件に定めるところによる。ただし、受注者又は第三者が従前から保有する権利及び本システムの標準マニュアル等を除く。
- (サ) 本件の履行に当たり、その業務の一部を再委託するときは、軽微なものを除き、あらかじめ再委託の相手方の住所、氏名、再委託を行う業務の範囲、再委託の必要性及び金額等について記載した書面を QST に提出し、承諾を得ること。その際受注者は、再委託した業務に伴う当該相手方の行為について、QST に対しすべての責任を負うこと。
- (シ) 仕様書及び詳細仕様書に疑義が生じた場合は、QST 担当者と協議の上決定するものとする。

以上

(要求者) 本部 情報基盤管理部 IT セキュリティ課
田井治 浩之

詳細仕様書

本詳細仕様書は、「脆弱性管理クラウドの導入及び整備」において調達する本システムの機能、初期導入支援、運用設計支援及び関連作業に係る要求事項を定めるものである。受注者は、本書に示す要件を全て満たすクラウドサービスを提供するとともに、導入及び初期設定に必要な作業を実施すること。本書の要件を満たすために必要なライセンス、オプション及び作業に係る費用は、全て契約金額に含めること。

1. 基本要件

以下の要件を全て含むシステムを整備すること。

- 1) 本システムはクラウドサービスとして提供され、QST の利用者が Web ブラウザから管理画面を利用できること。
- 2) 管理画面は原則として日本語表記とすること。
- 3) QST が指定する情報システム並びに当該情報システムを構成するホスト、サーバ、ネットワーク機器、クラウド環境その他の IT 資産（以下「登録資産」という。）を登録・変更できること。登録数は 150 以上とし、必要に応じて有償で追加できること。

※登録資産の算定方法は、ホスト、サーバ及びネットワーク機器等については機器等ごと、クラウド環境については AWS アカウント、Microsoft Azure サブスクリプション又は Google Cloud プロジェクト等ごとを基本とする。ただし、スキャン方法又は登録方法により算定方法が異なる場合は、技術審査資料において具体的な算定方法及び制限事項を明示すること。

- 4) チーム管理機能を有し、登録可能チーム数は 100 以上であること。
- 5) 利用可能ユーザー（管理者・一般ユーザーを含む）数は 500 以上であること。
- 6) 本システムの操作ログを監査ログとして出力し、確認可能であること。
- 7) 登録資産の構成情報、脆弱性、EOL 及び対応状況について、管理画面、API 又はファイル出力により取得できること。技術審査資料において、取得可能な情報、取得方法及び出力形式を明示すること。
- 8) Microsoft Entra ID と連携し、シングルサインオンによる認証が可能であること。
- 9) Microsoft EntraID と連携しないユーザーも登録可能であること。その場合、認証にはパスワード認証方法を含む多要素認証に対応していること。

2. 脆弱性管理機能の要件

以下の機能を有すること。

①登録資産のソフトウェア構成の一元管理機能

- 1) オンプレミス環境及びパブリッククラウド環境の双方を対象として、登録資産の

構成情報及び脆弱性等のリスク情報を一元的に管理できること。

- 2) ホスト、OS、ミドルウェア、ソフトウェア、ライブラリ、コンテナイメージ、ネットワーク機器及びクラウド資産等を管理対象として登録できること。
- 3) Microsoft Azure、AWS 及び Google Cloud のクラウド環境と連携し、クラウド上のホスト、コンテナ及びソフトウェアの構成情報及び設定情報を一括して把握できること。
- 4) 3) のクラウド連携による自動収集が困難な機器（ネットワーク機器、ハイパーバイザー、商用ミドルウェアその他）について、製品名及びバージョン等を手入力又は CSV で登録できること。
- 5) 3) のクラウド環境との連携により取得した設定情報に基づき、アクセス制限、管理権限、セキュリティグループ等の設定不備を検知する CSPM（※）機能を有すること。

※Cloud Security Posture Management の略。クラウドサービスの設定ミスを自動で検知し、セキュリティ体制を継続的に最適化するソリューションを指す。

- 6) SBOM を利用して、情報システム及びソフトウェアの構成情報並びに脆弱性を管理できること。また、SPDX 形式及び CycloneDX 形式の SBOM について、エクスポートが可能であること。
- 7) 登録資産毎に重要度を設定可能であること。
- 8) 登録資産毎に外部からのアクセス可否を設定可能であること。

②脆弱性情報の自動照合及びリスクの自動評価機能

- 1) 国内外の脆弱性情報（※）を日次で収集し、セキュリティアナリストが分析・精査した情報を登録するデータベースを有すること。また、当該データベースと登録資産の構成情報を自動的に照合し、潜在的なリスクを検知できること。

※NVD、JVN、IPA、JPCERT/CC、GitHub Security Advisories、ソフトウェア公式サイト等。

- 2) OSS の利用状況を管理画面上で可視化し、OSS ライセンス違反のリスクがある箇所を検知できること。
- 3) 検知したリスクに対し、登録資産の重要度、CVSS ベーススコア、外部からのアクセス可否、攻撃コード（PoC）の流通の有無及び CISA KEV への登録状況等の観点から判定し、対処優先度を 4 段階以上に自動分類できること。
- 4) 判定結果を管理画面で確認でき、対処優先度及び EOL 期限等の条件に応じて通知できること。通知方法、通知条件及び通知先の設定範囲を技術審査資料に明示すること。
- 5) EOL 期限については、期限切れ及び期限到来前の複数段階で表示でき、各段階に応じて自動通知できること。また、期限到来前の通知時期を設定できること。

③組織管理機能及び対応状況管理機能

- 1) セキュリティ部門及び登録資産管理部門等のチームを登録し、チーム単位で管理対象及び対応状況を管理できること。
- 2) チームは2階層以上で管理でき、複数の組織又はチームに係る構成情報及びリスクを上位の管理チームが参照・管理できること。また、将来的に有償オプション等により3階層以上へ拡張可能であること。なお、当該拡張に係る費用は本件の契約金額に含めないものとする。
- 3) 検出された脆弱性等に対して、担当者、対応予定日、ステータス及びコメントを登録し、対応履歴を管理できること。また、その対応状況を一覧で確認できること。

3. 初期導入及び整備作業

本システムの導入に際し、以下を実施すること。

- 1) サービス環境、組織、チーム、利用者、権限、通知及びスキャンに係る初期設定を実施し、又はQSTによる設定を支援すること。
- 2) QSTが指定する初期対象について、構成情報登録・収集を支援し、脆弱性、EOL、OSSライセンス及びクラウド設定リスク等の検出結果をQSTと共同で確認すること。
- 3) 緊急性の高い脆弱性等を対象に、影響確認、優先順位付け、ステータス変更及びコメント記録を含む一連の対応管理手順を試行すること。
- 4) 定期スキャン、通知、脆弱性リスクの確認及び対応状況管理を含む定常的な脆弱性管理の運用ルールの設定を支援すること。
- 5) リモートホストスキャン等の実施に当たり踏み台サーバが必要となる場合は、必要となる台数、OS、CPU、メモリ、ストレージ、通信要件及び設定内容を技術審査資料に明示すること。踏み台サーバを動作させるための基盤はQSTが用意し、受注者は必要なソフトウェアの提供及びQSTによる導入設定の技術支援を行うこと。

4. 技術支援及び運用支援

本システムの利用期間中、以下の技術的支援を行うこと。

- 1) 本システムの利用期間中、日本語によるテクニカルサポート窓口を提供すること。
- 2) テクニカルサポートは、サービスの仕様、利用方法、設定方法及びトラブル発生時の対応支援を対象とすること。
- 3) サポート受付時間は原則として平日10:00～17:00を含む時間帯とし、連絡方法及びサポート範囲を技術審査資料に明示すること。
- 4) 本システムによるリスク評価及び対処優先度の判定についてQSTと協議し、設

定の調整を支援すること。

- 5) 本システムにより検知された個別のリスクを分析し、QST におけるリスクの状況を取り纏めた報告及び対応方針の提案を行うこと。
- 6) QST における脆弱性管理に係る運用フロー及び評価基準の策定を支援すること。
- 7) QST が指定する情報システムの重要度を評価し、当該評価結果を踏まえた脆弱性への対処優先順位及び対応ルールの策定を支援すること。
- 8) 本システムを利用した脆弱性管理の導入から定常運用への移行に向け、QST に対する継続的な助言及び支援を行うこと。
- 9) 2027 年 3 月下旬までに運用報告を行い、本項 4) ～8) の内容を含む報告書を取り纏め提出すること。

以上。