仕様書

Ⅰ　一般仕様

1.　件　　名

SOC サービスの運用

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、「当機構」）では、情報セキュリティに関わるインシデント疑いに対する調査やインシデントへの対応等に迅速な対応が求められるため、当機構が収集するセキュリティログ等を一元管理、検知する SIEM（Security Information and Event Management）を導入し、既設ファイアウォール機器のログ監視と合わせて SOC（Security Operation Center）サービスを運用するための設備・機器を、株式会社ラックのサービス「JSOC xPDR」および「JSOC MSS」で令和 7 年 10 月に構築した（12 月構築完了予定）。

本件では、構築した環境を用いた SOC サービスを 24 時間 365 日体制で運用し、当機構のサイバー攻撃への即応体制を高度化し、セキュリティ対策レベルを向上させることを目的とする。

3.　履行期限

令和８年１月１日　～　令和８年３月３１日　（３ヶ月）

4.　作業場所

受注者が管理・運用する SOC サービス提供の専用監視センター

5.　作業内容　（詳細はⅡ技術仕様による。）

（1）SOC サービスの提供（アラート監視、初期対応、当機構担当者への報告等）

（2）実施報告書の提出

6.　必要な能力・資格

受注者は、以下の要件を満たしていること。なお、認証や登録が有効な期間等が有る場合において本件の納期内に期限を迎える場合は更新の予定があることを示すこと。

① ISMS(ISO27001)の認証を取得又は同等以上の情報セキュリティ対策を実施していること。なお、ISMS(ISO27001)は、本業務内容及び本業務を実施する部門を対象として認証を取得していること。

② 一般財団法人日本情報経済社会推進協会（JIPDEC）が付与するプライバシーマークを取得していること。

③ 日本国内において、24 時間 365 日のセキュリティ監視サービスを複数年にわたり現在まで継続して実施していること。

④ 本件で連携する SOC サービスは IPA（独立行政法人情報処理推進機構）が公開する「情報セ

キュリティサービス基準適合サービスリスト」の「セキュリティ監視・運用サービス」に登録されていること。

⑤ 当機構の SOC 環境の構築または運用実績を有すること。

7. 提出図書

下記の書類を提出すること。

No.	図書名	提出時期	様態	確認
1	連絡体制表	契約後速やかに	電子版	要
2	実施報告書	作業実施翌月 15 日迄に毎月提出 ※ただし作業実施が本件履行期限最終月の場合は当機構担当者と事前に調整のうえ当月末迄に提出すること	電子版	要
3	再委託承諾願 （当機構指定様式）	契約後速やかに ※下請負等がある場合に提出のこと。	電子版	要

（提出先）

情報基盤管理部　IT セキュリティ課

（提出方法）

当機構担当者と協議の上、決定する。

8. 検査条件

I 章 5 項及び II 章に示す作業完了後、I 章 7 項及び II 章 6 項に定める提出書類の確認並びに仕様書に定めるところに従って業務が実施されたと当機構が認めたときをもって検査合格とする。

9. その他

① 受注者は、当機構が量子科学技術の研究・開発を行う機関であり、高い技術力及び高い信頼性を社会的に求められていることを認識するとともに、当機構の規程等を順守し、安全性に配慮しつつ業務を遂行しうる能力を有する者を従事させること。

② 受注者は、当機構の情報セキュリティポリシーを遵守すること。

③ 受注者は、本件で取得した当機構の情報を、当機構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。

④ 受注者は、本件で取得した当機構の情報を、当機構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。

⑤ 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、当機構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。

⑥ 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。

⑦ 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、速やかに当機構担当者に連絡し、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。

⑧ 受注者は、当機構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当機構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。

⑨ 受注者は、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、当機構の許可無く当機構外部に持ち出してはならない。

⑩ 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。

⑪ 本件で作成された著作物（マニュアル、コンピュータプログラム等）の所有権は、当機構に帰属するものとする。

⑫ 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当機構に提出し、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、当機構に対しすべての責任を負うこと。

⑬ 仕様書及び詳細仕様書に疑義が生じた場合は、当機構担当者と協議の上決定するものとする。

10. 総括責任者

受注者は本契約業務を履行するに当たり、受注者を代理して直接指揮命令する者（以下、「総括責任者」という。）及びその代理者を選任し、次の任務に当たらせるものとする。

（1）受注者の従事者の労務管理及び作業場での指揮命令

（2）本契約業務履行に関する当機構との連絡及び調整

（3）従事者の規律秩序の保持並びにその他本契約業務の処理に関する事項

11. グリーン購入法の推進

本契約において、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、ＯＡ機器等）が発生する場合は、これを採用するものとする。

12. 協議

本仕様書に記載されている事項及び本仕様書に記載のない事項について疑義が生じた場合は、当機構と協議のうえ、その決定に従うものとする。

II　技術仕様

1．一般事項

受注者は、当機構のセキュリティ機器が収集するログやアラートから脅威を分析し、危険度等に応じて一次対応の実施や当機構担当者への速やかな報告を行うこと。

2．セキュリティ監視対象

(1)　当機構が運用する SIEM 環境

当機構が運用するクラウドサービスのログを収集している。

- Microsoft Entra ID
- Microsoft Entra ID Protection
- Microsoft Defender XDR
  （Microsoft Defender for Endpoint、Microsoft Defender for Office 365 含む）
- Intune
- Azure Activity
- Azure Bastion
- Azure Firewall
- Azure Application Gateway
- Azure Web Application Firewall

上記のほか、当機構担当者と受注者で協議の上追加されたログ等が対象に加わることがある。

(2)　当機構が運用するファイアウォール機器

- Palo Alto 社製 PA-5220

3．SOC サービス

以下の作業を実施すること。

(1)　SOC サービスは日本国内で運用され、サービス運営のために保有するデータの保存場所も日本国内であること。

(2)　24 時間 365 日、当機構が連絡可能な SOC サービスを運用すること。

(3)　当機構が監視状況を把握することができる WEB ポータルを運用すること。

(4)　WEB ポータルのダッシュボード上で各種のイベントやアラートへの対応状況等が確認できること。

(5)　WEB ポータルへの接続には、多要素認証や IP アドレス制限等により接続元を厳に制限できること。

(6)　当機構向けの WEB ポータル環境は、他の利用者の環境と論理的もしくは物理的に分割されていること。

(7)　SOC サービスの中で検知されるインシデントに対し、危険度をリスクレベルとして Informational, Medium, High, Critical などといった 4 段階以上で定義されていること。

(8)　SOC サービスにより「2. セキュリティ監視対象」のセキュリティ監視を行うこと。

(9)　SOC サービスは、自動分析・自動対処・自動通知等の自動化を取り入れ、迅速な対応を実現すること。特に、重大なセキュリティインシデントを検知した際には Microsoft365 のアカウントの自動停止や端末の自動遮断等のインシデント初動対応を実施すること。

(10) クラウドサービスにおけるセキュリティインシデント等の検知能力向上のために、クラウドサービスの脅威インテリジェンスに加え、受注者独自のサイバー脅威インテリジェンス情報、QST 独自のサイバー脅威インテリジェンス情報を SOC サービスに適用すること。

(11) 当機構で発生するインシデントの詳細分析を行うため、アドバイザー、アラート助言、マルウェア調査、アクセス先調査、トリアージ支援、インシデントハンドリング支援、フォレンジック、危機管理対応といった支援を受注者の専門チームが実施すること。(5 作業時間/月を想定)

(12) SOC サービスで検知されるインシデントの取り扱いにおいては、対象機器の定義したリスクレベルをそのまま用いるのではなく、通信内容やログを分析することにより攻撃が成功、又はその可能性が高いかどうかを判断し、当該判断を加味したリスクレベルの定義と、それに基づく運用を行うこと。詳細については当機構と受注者にて別途定めることとする。

(13) 当機構のファイアウォールの監視において、緊急または重要なセキュリティインシデントが発生した場合、当機構担当者に代わり不正な通信の遮断設定や端末の通信遮断設定等を当機構のファイアウォールに対して実施すること。

なお、実施にあたり監視システム等と当機構のファイアウォールとの接続で仮想プライベートネットワークを用いる場合は Site-to-Site で行うこと。その接続に必要となる機器および運用維持にかかる費用は本件に含めること。

(14) 定義した危険度の分析基準において不正アクセスの成功の可能性が高い又は成功した場合、セキュリティインシデントと判断してから速やかに受注者より当機構に緊急連絡を行うこと。詳細については当機構と受注者にて別途定めることとする。

6．実施報告書の作成と提出

II 技術仕様書 3 で実施した作業の内容を 1 ヵ月ごとに整理、資料化し実施報告書として翌月 15 日迄（ただし作業実施が本件履行期限最終月の場合は当機構担当者と事前に調整のうえ当月末迄）に提出すること。

様式等詳細については契約後速やかに当機構担当者と協議のうえ決定することとする。

必要に応じて打合せの実施に応じること。

（要求者）

部課（室）名：本部　情報基盤管理部　IT セキュリティ課

氏　　名：大竹　淳

（別紙様式１－１）

選定理由書

１．件名	SOC サービスの運用
２．選定事業者名	株式会社ラック
３．目的・概要等	QST では、情報セキュリティに関わるインシデント疑いに対する調査やインシデントへの対応等に迅速な対応が求められるため、当機構が収集するセキュリティログ等を一元管理、検知する SIEM（Security Information and Event Management）を導入し、既設ファイアウォール機器のログ監視と合わせて SOC（Security Operation Center）サービスを運用するための設備・機器を、株式会社ラックのサービス「JSOC xPDR」および「JSOC MSS」で令和 7 年 10 月に構築を開始した（12 月構築完了予定）。 本件では、構築した環境を用いた SOC サービスを 24 時間 365 日体制で運用し、当機構のサイバー攻撃への即応体制を高度化し、セキュリティ対策レベルを向上させることを目的とする。
４．希望する適用条項	契約事務取扱細則第２９条第１項第１号ヲ (特定の業者以外では販売、提供することができない物件を購入、借用、利用するとき)
５．選定理由	本件は、令和 7 年 9 月に一般競争入札で株式会社ラックに委託して構築した SIEM および SOC 環境を用いて令和 8 年 1 月より SOC サービス運用を行うものである。 SIEM および SOC 環境における分析・検知・自動対処といった各種機能は株式会社ラックが独自に設計および実装したものであり、それらを用いて SOC サービスを適切かつ安定的に運用するためには、開発元である株式会社ラックによる継続的な技術支援が必要不可欠である。 また、SOC サービスを利用するにあたっては、構築された環境と密接に連携して監視する必要があり、開発元以外の事業者による運用では機能の完全な利活用やインシデント等発生時の迅速な対応等が困難である。 よって SOC サービスの利用は、株式会社ラックを選定先とする。