サイバー攻撃検知及びインシデント発生時の初期対応等に関する支援業務
仕　様　書

1. 件名

サイバー攻撃検知及びインシデント発生時の初期対応等に関する支援業務

2. 目的

本件は、国立研究開発法人日本原子力研究開発機構（以下、「機構」という）に対するサイバー攻撃の兆候を迅速に検知し、攻撃等によるインシデント発生時には初期対応、封じ込め、原因分析、復旧支援など一連の対応を適切に実施するため、外部の SOC（セキュリティオペレーションセンター）サービスを活用して、機構の情報資産の保護とセキュリティ水準の維持・向上を図るものである。

3. 作業場所

本業務の作業場所等は、以下のとおりとする。

(1) 主たる作業場所は、機構および受注者が構築・運用する SOC とする。

(2) 本業務のデータ処理を行う設備は、いずれも日本国内に所在するデータセンターに限定すること。

(3) 作業場所またはデータ処理設備の所在地を変更する場合は、あらかじめ機構へ書面にて申し出ること。

4. 期間

令和 8 年 2 月 1 日から令和 9 年 3 月 31 日 （14 ケ月間）

但し、契約締結から令和 8 年 1 月 30 日までの期間に「6. 導入準備作業」を行うものとする。

5. 監視対象機器および利用環境

機器・サービス名	台数または対象範囲
Active Directory（オンプレミス）	1 台
Entra ID	7,600 ユーザー
i-FILTER	13,000 台
Microsoft Defender for Endpoint	7,600 ユーザー
VPN 装置	2,700 ユーザー

6. 導入準備作業

支援業務の円滑な開始に向け、以下の導入準備作業を実施すること。

(1) 現状把握と要件整理

① 受注者は、支援業務の詳細を事前に機構と綿密に調整すること。

② 監視対象機器の IP アドレス、ホスト名、ユーザー数などの詳細情報を受領し、連携方

式を確定すること。

(2) 運用設計書の作成

① 各監視対象に関するログ種別、送信方式、監視項目、通知ルール、エスカレーションルートなどを整理し、機構の確認を得て、「運用設計書」として納品すること。

※7.(9)②で定める CSIRT 通報の窓口対応を含めること。

② 支援業務の期間中は、必要に応じて「運用設計書」を改版すること。なお、改版の回数は無制限とすること。

(3) ログ連携構築と接続テスト

① 機構指定の接続ポイント(Syslog 中継機器、API エンドポイント等)と SOC 側の受信基盤を安全な暗号化通信方式で接続し、ログの送信確認試験を実施すること。

② ログ取得のためのエージェントが必要となる場合には、機構が対象端末へのエージェント導入を実施する。受注者は導入に必要な技術的支援を行い、連携後のログ取得に支障がないことを確認すること。

(4) 通信要件とログの取り扱い

① ログ連携は、TLS 通信を利用した Syslog または HTTPS 等、安全な通信方式により実施すること。

② ログ保存期間は最低 1 年間とし、必要に応じて CSV 形式での抽出に対応すること。

③ 機器ごとにログ連携方式を定義し、構成図により明示すること。

7. 支援業務内容

(1) 常時監視と有人対応

支援業務は、24 時間 365 日有人監視を行うこと。

(2) イベント分析と一次対処

検知されたセキュリティイベントに対し、内容を平易な日本語に翻訳し、影響範囲の封じ込めを目的とした一次対処を実施すること。エンドポイントに対しては、EDR を用いたリモート操作により隔離対応を行うこと。

(3) 一次通報

重大なインシデントが発生した場合、検知から 30 分以内に電話および電子メールにて通報を行うこと。通報先は機構が指定した連絡先とし、全ての通報内容を記録すること。

(4) 端末隔離の運用方針

次の 3 つのポリシーから選択すること。

① 無許可による自動隔離

② 許可後に隔離

③ 隔離を実施しない

※誤検知による隔離を考慮して有人の窓口を常設すること。

(5) 隔離端末の復旧対応

隔離された端末については、機構の指示に基づきリモートで復旧を行うこと。

(6) 二次通報と恒久的対処支援

インシデントの発生後、原因の究明、影響範囲の分析、再発防止策の提案を実施すること。なお、調査においては周辺ログも確認を行うこと。

(7) 誤検知・過検知の判断

対象イベントが正当な通信である可能性がある場合は、機構の業務内容を踏まえたうえで判断を行い、ホワイトリストへ登録または提案を行うこと。

(8) 報告

検知および対応の実績を取りまとめた月次レポートを提出すること。また、月次もしくは四半期に報告会を開催し、インシデントの傾向、セキュリティ情勢、今後の対応方針などを共有すること。

(9) 技術支援・情報提供

以下の付帯サービスを提供すること。

① EDR のホワイトリスト登録（登録の提案も可）とその管理

② CSIRT 通報の窓口対応

(a) CSIRT 窓口として機構職員等からの通報を 24 時間 365 日体制で電話一次受付を行うこと。

(b) SOC サービス以外の対応は機構が定める取次先へエスカレーションを行うこと。

(c)エスカレーション先への対応に関しては、機構と手順書や運用フローをマニュアル化する支援を行うこと。

③ 機構からの相談に応じたセキュリティ全般の助言を実施

④ インシデント発生時の周辺機器ログの確認と分析及び SOC サービス対象外の機器における不審挙動への対応支援

⑤ 上記④に基づく、デジタルフォレンジック等の有事対応の支援

(a) 有事対応の作業内容を検討・整理し、機構へ助言すること。

(b) 必要に応じて、有事対応を本契約に関連する緊急契約として、別途締結するので、これに対応できること。

⑥ 運用設計書の更新と内容変更に伴う運用変更の支援

⑦ SOC サービスからの通報基準や優先度調整の柔軟な変更対応

8. クラウドサービス利用に関する事項

本業務においてクラウドサービスを利用する場合は、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたサービスを用いること。やむを得ず ISMAP 未登録のクラウドサービスを利用する必要がある場合には、事前に機構と協議し、必要なセキュリティ対策とリスク評価を実施すること。

9. 技術力に係る要件等（総合評価項目）

(1)必要な資格等

① 本業務において提供されるSOCサービスは、独立行政法人情報処理推進機構（IPA）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。

また、本業務に必要な他のサービスも「情報セキュリティサービス基準適合サービスリスト」に登録されていることが望ましい。【加点項目】

② サービス提供における専門性および信頼性の確保するため、Microsoft が認定する「Specializations」資格のうち、Security カテゴリに該当する要件を保有していることが望ましい。【加点項目】

③ 本業務の従事者のうち少なくとも 1 名以上は、下記のいずれかの資格を取得していること。

(a)情報処理安全確保支援士

(b)公認情報システムセキュリティ専門家（CISSP）

(c)情報セキュリティスペシャリスト試験の合格者

(d)テクニカルエンジニア（情報セキュリティ）試験の合格者

また、上記資格を有する従事者が複数名いることが望ましい。【加点項目】

(2)業務の実施体制に関する事項

①業務責任体制（統括責任者名、総括責任者代理名、業務担当者名、業務担当者の実績・保有資格、統括責任者と業務担当者の役割分担、機構との連絡体制）を提示すること。なお、効果的な人員体制となっていることが望ましい。

②過去に類似業務を行った実績があること。または、類似業務に求められる知見・技術力を有していること。なお、長期に渡る類似業務の実績を有することが望ましい。

（類似業務の目安：24 時間 365 日の有人監視を伴う SOC サービスにおいて、Active Directory や EDR、クラウド型メールフィルタなど複数機器を対象とし、エンドポイント数が 概ね 4,000 台以上の環境での常時監視・一次対応・通報・月次報告等を一体的に提供した実績を目安とする。）

(3)サプライチェーン・リスクに関する事項

① 情報システムの運用・保守工程において、機構の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。

② 情報システムに機構の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、機構と連携して原因を調査し、排除するための手順及び体制（例えば、運用・保守業務におけるシステムの操作ログや作業履歴等を記録し、発注先から要求された場合には提出させるようにするなど）を整備していること。また、当該手

順及び体制が妥当であることを証明するための書類を提出すること。

③ 受注者は、本業務の遂行における情報セキュリティ対策の履行状況を確認するために、機構が情報セキュリティ監査の実施を必要と判断した場合は、機構が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報セキュリティ監査を受け入れること。（機構が別途選定した事業者による監査を含む）。

④ 受注者は、本業務の全部を一括して、第三者に再委託してはならない。また、受注業務における総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託してはならない。ただし、本契約の適正な履行を確保するために必要な範囲において、この契約の一部（仕様書に示す業務の主たる部分を除く。）を第三者に再委託（再々委託以降の委託を含む。以下同じ。）する場合は、受注者は、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託する業務の範囲、再委託の必要性について記載した書面を機構に提出すること。

⑤ 前項は、受注者が再委託先を変更する場合その他の事由により、機構から承認を受けた内容を変更する場合において準用する。

⑥ 再委託を行う場合、受注者は、再委託先の資本関係・役員の情報、本契約の実施場所、従事者の所属・専門性（情報セキュリティに係る資格・研修等）・業務経験実績及び国籍についての情報を記した書類をあらかじめ機構に提出すること。

⑦ 受注者は、知的財産権、情報セキュリティ（機密保持を含む。）及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施すること。

10．支給物品及び貸与品

(1) 本業務を行うために必要な規則等のドキュメントは、機構が受注者に貸与する。貸付等にあたっては、機構監督員に申し出て、事前に許可を受けること。

(2) 受注者は、貸与品について、借用品管理票を作成し、善良な受注者としての注意義務を持って、適正に管理しなければならない。貸与品を保管する場合は、施錠のできる書庫等に保管することとし、常時施錠しなければならない。なお、貸与品を保管する場合は、施錠のできる書庫等の写真を提出すること。

(3) 受注者が、貸与品を運搬する場合、その経費は受注者の負担とする。

(4) 受注者は、貸与品について、機構から返還の指示があった場合、必要がなくなった場合、又は契約が終了したときは、速やかに返還しなければならない。電子データは、速やかに削除すること。

11. 提出図書

No.	名称	提出期限	部数	確認
1	作業計画書	契約締結後、速やかに	1	不要
2	委任又は下請負届（本業務の一部を再委託する場合）	契約締結後、速やかに	1	要
3	運用設計書	運用業務開始前まで	1	要
4	サポート体制表	運用業務開始前まで	1	要
5	作業報告書	作業後速やかに	1	不要
6	打合せ議事録	打合せ後速やかに	1	要
7	検査要領書	検査実施の 2 週間前まで	1	要
8	検査成績書	検査後速やかに	1	要
9	月次報告書	翌月 1 日まで （ただし、1 日が土日祝日にあたる場合は翌営業日まで）	1	要

※1 上記に加えて受注者の資本関係・役員の情報、本契約の実施場所、従事者の所属・専門性（情報セキュリティに係る資格・研修等）・業務経験及び国籍についての情報を記した書類をあらかじめ機構に契約後速やかに提出すること。

なお、機構がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、機構と迅速かつ密接に連携し体制の見直しを図ること。また、提出した内容に変更が生じた場合は、その都度提出すること。

※2 カラーを使用する場合は、白黒でも印刷できるよう配慮すること。

12. 提出場所

茨城県那珂郡東海村大字白方 2 番地 4
日本原子力研究開発機構　原子力科学研究所
システム計算科学センターサイバーセキュリティ統括室

13. 検収条件

(1) 導入準備作業に関する検収・支払い

以下のすべての要件を令和 8 年 1 月 30 日までに満たすこと。

① SOC サービスを利用可能な環境を構築し、検査要領書に基づく検査に合格すること。なお、検査に用いる検査要領書は受注者が作成し、事前に当機構に提出して確認を得ること。

② 「11.提出図書」のうち月次報告書を除く全ての図書を「12.提出場所」に提出すること。

③　導入準備作業についての請求書を送付すること。

(2)　支援業務に関する検収・支払い

①　検収は月次報告書の提出および内容確認、並びに請求書の受領をもって行うものとする。

②　支援業務にかかる費用の支払いは、令和 8 年 2 月 1 日から令和 9 年 3 月 31 日(14 ケ月間)の 14 等分した金額を月額として毎月後払いとする。初回の月次報告書および請求書は、令和 8 年 2 月分の業務を対象とし、令和 8 年 3 月に提出すること。

14. 適用規程等

(1)　平成 12 年法律第 100 号「国等による環境物品等の調達の推進に関する法律」

(2)　情報セキュリティ管理規程

(3)　情報システムセキュリティ対策基準

15. 情報セキュリティ強化に係る特約条項

本業務における情報セキュリティの確保については、別紙 1「情報セキュリティ強化に係る特約条項」に定められたとおりとする。

16. 特記事項

(1)　受注者は機構が原子力の研究・開発を行う機関であるため、高い技術力及び高い信頼性を社会的にもとめられていることを認識し、機構の規程等を遵守し安全性に配慮し業務を遂行しうる能力を有する者を従事させること。

(2)　受注者は業務を実施することにより取得した当該業務及び作業に関する各データ、技術情報、成果その他のすべての資料及び情報を機構の施設外に持ち出して発表もしくは公開し、または特定の第三者に対価をうけ、もしくは無償で提供することはできない。ただし、あらかじめ書面により機構の承認を受けた場合はこの限りではない。

(3)　受注者は異常事態等が発生した場合、機構の指示に従い行動するものとする。また、契約に基づく作業等を起因として異常事態等が発生した場合、受注者がその原因分析や対策検討を行い、主体的に改善するとともに、結果について機構の確認を受けること。

17. グリーン購入法の推進

(1)　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。

(2)　本仕様に定める提出図書(納入印刷物)については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

別紙1

情報セキュリティ強化に係る特約条項

受注者（以下「乙」という。）は、本契約の履行に当たり、情報セキュリティの強化のため、契約条項記載の情報セキュリティに係る遵守事項に加え、以下に特約する内容を遵守するものとする。

（情報セキュリティインシデント発生時の対処方法及び報告手順）

第１条 乙は、情報セキュリティインシデントが発生した際の対処方法（受注業務を一時中断することを含む。）及び発注者（以下「甲」という。）に報告する手順について整備しておかなければならない。

（情報セキュリティ強化のための遵守事項）

第２条 乙は、次の各号に掲げる事項を遵守するほか、甲の情報セキュリティ強化のために、甲が必要な指示を行ったときは、その指示に従わなければならない。

(1) この契約の業務を実施する場所を、情報セキュリティを確保できる場所に限定し、それ以外の場所で作業をさせないこと。

(2) 業務担当者に遵守すべき情報セキュリティ対策について教育・訓練等を受講させるとともに、業務担当者には甲の情報セキュリティ確保に不断に取り組み、甲の情報及び情報システムの保護に危険を及ぼす行為をしないよう誓約させること。また、業務担当者の異動・退職等の際には異動・退職後も守秘義務を負うことを誓約させ、これを遵守させること。

(3) 暗号化を要する場合は、「電子政府推奨暗号リスト」に記載された暗号化方式を実装し、暗号鍵を適切に管理すること。

(4) 甲の承諾のない限り、この契約に関して知り得た情報を受注した業務の遂行以外の目的で利用しないこと。

(5) 甲が提供する情報を取り扱う情報システムへの不正アクセスを検知・抑止するために、ログを取得・監視し全ての業務担当者についてシステム操作履歴を取得すること。

(6) 甲が提供する情報を格納する装置、機器、記録媒体及び紙媒体について、業務担当者のみがアクセスできるよう施錠管理や入退室管理を行い、セキュアな記録媒体の使用や使用を想定しないUSBポートの無効化、機器等の廃棄時・再利用時のデータ抹消など想定外の情報利用を防止すること。

(7) 情報システムの変更に係る検知機能やログ解析機能を実装し、外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時には、多要素主体認証を要求する

とともに定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時の脆弱性対策を行うこと。

(8) システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施するとともに、システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと。

(9) 委任をし、又は下請負をさせた場合は、当該委任又は下請負を受けた者に対して、業務担当者が遵守すべき情報セキュリティ対策についての教育・訓練等を行うこと。

(10) 契約条項に基づき甲が乙に対して行う情報セキュリティ対策の実施状況についての監査の結果、情報セキュリティ対策の履行が不十分である場合には、甲と協議の上改善を行い、甲の承諾を得ること。

(11) 契約の履行期間を通じて前各号に示す情報セキュリティ対策が適切に実施されたことの報告を含む検収を受けること。また、本契約の履行に関し、甲から提供を受けた情報を含め、本契約において取り扱った情報の返却、廃棄又は抹消を行うこと。