意見招請を実施する案件

【意見招請番号：２】

案件名	日本学生支援機構セキュリティ運用監視業務委託

直近の調達内容

契約件名	日本学生支援機構セキュリティ運用監視業務委託
調達方式	一般競争入札（総合評価落札方式）
入札公告日	平成30年11月14日
競争参加資格	本件の一般競争入札に参加できる者は、以下の条件をすべて満たしている者とする。 （１）予算決算及び会計令第70条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。 （２）予算決算及び会計令第71条の規定に該当しない者であること。 （３）平成28・29・30年度文部科学省競争参加資格（全省庁統一資格）において、「役務の提供等」の「Ａ」の等級に格付けされた、「関東・甲信越地域」の競争参加資格を有する者であること。なお、当該競争参加資格については、平成30年３月30日付け号外政府調達第59号の官報の競争参加資格の資格に関する公示の別表に掲げる申請受付窓口において随時受け付けている。 （４）本機構理事長から取引停止を受けている期間中でないこと。 （５）「暴力団員による不当な行為の防止等に関する法律」（平成３年法律第77号）に規定するところの暴力団員及びその構成員、準構成員又はその関係者でないこと。 （６）受託者及び再委託先は、一般財団法人日本経済社会推進協会又は海外の認定機関により認定された審査機関による情報セキュリティマネジメントシステム（ISMS）の取得又はこれに類する情報セキュリティ管理体系を確立していること。 （７）受託者は、本件と同等以上のシステム規模のセキュリティ運用監視業務について、１者以上の受託実績を有すること。
提出書類等及び提出期限	（１）一般競争入札参加申込書（本機構所定様式）　１部 （２）入札書　１部（本機構所定様式　作成に当たっては「入札参加者心得」に従うこと。） （３）委任状　１部（本機構所定様式　代理人が入札する場合のみ。） （４）資格審査結果通知書（全省庁統一資格）の写　　１部 （５）ISMS(Information Security Management System)又はこれに類する情報セキュリティ管理体系を確立していることを証する書類（情報セキュリティに関する認証（「ISO/IEC27001（ISMS））を受けている場合は、その認定証の写しで可）　１部 （６）実績証明書（本機構所定様式）　１部 競争参加資格（７）を有することを証明するための書類として、「実績証明書」を作成し、その裏づけとなる契約書、仕様書等の写しを添付すること。なお、保管期間を経過した等の理由により、裏づけとなる契約書・仕様書等の書類が調えられない場合は、「確約書」（本機構所定様式）を作成のうえ「実績証明書」と併せて提出すること。 （７）提案書　　正本１部、副本６部

	平成31年1月11日　午後5時
開札日	平成31年1月21日　午後3時
業務履行期間	平成31年4月1日　～　令和4年3月31日

日本学生支援機構
セキュリティ運用監視業務委託
調達仕様書

2018 年 10 月

独立行政法人　日本学生支援機構

1　調達の目的

1.1　調達件名

日本学生支援機構セキュリティ運用監視業務委託

1.2　調達の背景および目的

独立行政法人日本学生支援機構（以下、当機構）は、「サイバーセキュリティ基本法」および「政府機関等の情報セキュリティ対策のための統一基準群」に則り、情報資産を守るべく、入口出口対策、標的型メール対策、エンドポイントセキュリティ、ウイルス対策等、多岐にわたる情報セキュリティ対策機器を導入してきた。

一方、外部からの攻撃が複雑化・巧妙化しており、未知の攻撃も日々生まれている中、防御側も情報セキュリティ対策機器を導入しただけではすぐに陳腐化してしまうため、日々の運用監視、最新のセキュリティ対策を施していくことが重要である。しかしながら、これらを行うためには多大な技術、知識を要するとともに、昼夜問わず行われてくる攻撃に対応するには、時間を問わず体制を確保することが必要不可欠と考え、2018 年度には外部事業者へ委託を行ったところである。

本調達では、継続的に対応すべく、技術者による遠隔監視拠点の利用をはじめ、専門的知見を有するサポート業務を外部委託することにより、セキュリティインシデント発生時や、インシデントレスポンス、フォレンジック等を昼夜問わず対応可能な体制とし、対応力を強化することを目的とする。

1.3　調達における基本方針

本調達における基本方針を以下に示す。

- 当機構が運用する情報セキュリティ対策機器とそれらが保護すべき機器の監視とセキュリティインシデント発生有無の検知、発生時の対応から解決までを一本化した調達とする。
- 本調達は複数事業者が導入した機器等で構成される、マルチベンダー環境となっており、それらに対する役務も含まれている。スムーズに業務が開始できるよう、各事業者からの引き継ぎ、事前設計と現地調査、運用の主体的な実行も役務として含めることとする。
- 特定のベンダー、メーカー、技術等に固執せず、当機構の情報資産を確実に守ることに主眼を置く。
- 安定的、効率的なシステム運用基盤を確立し、職員の負荷低減につなげることを基本とする。
- スケジュール（進捗）、品質、コスト及びセキュリティ等に関して、適切な工程管理を行う。

・ 当機構の IT システムのライフサイクルを鑑みて、サイバーセキュリティの状況変化にも柔軟に対応できることとする。

1.4 用語の定義

本仕様書および業務実施における用語とその意味は以下の通りである。

・ A系ネットワーク
当機構で運用している基幹業務システムである奨学金業務システム等、個人情報、機密情報を取扱うシステムへ接続可能な基幹業務系ネットワークの総称。機密性が高い情報を保存することが可能で、当機構の大部分が所属する。原則としてインターネットへの接続はできず、情報系ネットワーク（B系ネットワーク）とは論理分離されている。

・ B系ネットワーク
業務、事務を取扱う業務端末が接続された情報系ネットワークの総称。このネットワークに接続される機器はインターネットにアクセスが可能であり、インターネット上のウェブサイトを閲覧する、インターネットを経由して電子メールを送受信する、個人情報を含まない情報を保存する資料を保存する等が可能である。原則として個人情報、機密情報を取扱うシステムへの接続はできず、基幹業務系ネットワーク（A系ネットワーク）とは論理分離されている。

・ インシデント共有システム
発生したセキュリティインシデント情報、ネットワーク障害情報、構成管理対象ドキュメントを当機構および関連事業者と共有するためのシステム。現行システムは2018年度セキュリティ運用監視事業者がクラウド上に構築し、インターネットを介してアップロード、ダウンロードによる授受を行っている。

・ インシデントハンドリング
セキュリティインシデント発生時から解決までの一連の活動。

・ JASSO-CSIRT
情報セキュリティリスクを適切に管理するための組織。緊急時の対処において、関係各所と連携し被害を局所化する、日常的に各事業者（受託者含む）と情報共有して脆弱性の排除における取り組みや有事に備えた体制を構築する。

・ JASSO Online Storage（JOS）
インターネットと機構の内部にて情報をやり取りすることが可能なストレージシステム。当機構と外部組織が大容量のファイルを送受信するために使用する、セキュリティを確保したストレージ。受託者と当機構は、本システムを使用してデータの授受を行う。略してJOS（ジェイオーエス）。

・ インシデントマネジメント

インシデント発生を防ぐべく、防御策や啓発活動等、事前の対応を含めた業務。本調達における受託者の主要業務の一つ。

・ インシデントレスポンス
発生したセキュリティインシデントへの対応。

・ インターネットシステム
インターネットとの通信を行うシステム。DNSサーバー、メールサーバー、Proxyサーバー、NTPサーバー、外部公開用ウェブサーバー等で構成される。

・ 機構内ネットワーク
IP-VPN網で接続された拠点間通信網。データセンターを中心に、各拠点を接続する。主回線と副回線で冗長化がされており、障害発生時等に自動的に切り替わる。

・ 拠点
本部、支部、日本語教育センター、コールセンター等、機構の役職員が執務を行う全国18ヵ所の事務所。

項番	拠点名	住所
1	本部	神奈川県横浜市緑区長津田町4259 S-3
2	市谷事務所	東京都新宿区市谷本村町10-7
3	青海事務所	東京都江東区青海2-2-1
4	駒場事務所／関東甲信越支部	東京都目黒区駒場4-5-29
5	グローバル人材育成部	東京都千代田区霞ヶ関3-2-2 （文部科学省内）
6	東京日本語教育センター	東京都新宿区北新宿3-22-7
7	大阪日本語教育センター	大阪府大阪市天王寺区上本町8-3-13
8	北海道支部	北海道札幌市中央区大通西３丁目１１番地北洋ビル10階
9	東北支部	宮城県仙台市青葉区一番町2-4-1 仙台興和ビル10階
10	東海北陸支部	愛知県名古屋市中区錦1-4-16 日銀前ＫＤビル3階
11	近畿支部	大阪府大阪市北区西天満4-11-22　阪神神明ビル8階
12	中国四国支部	広島県広島市中区西白島町16-8 ソレイユ白島2階
13	九州支部	福岡県福岡市中央区大名2丁目9番27号野村

		不動産赤坂センタービル3階
14	市谷事務所分室	東京都新宿区内 ※詳細は受託者にのみ開示する
15	文教団体年金基金	東京都新宿区内 ※詳細は受託者にのみ開示する
16	データセンター	東京都特別区内 ※詳細は受託者にのみ開示する
17	コールセンター（名古屋）	愛知県名古屋市内 ※詳細は受託者にのみ開示する
18	コールセンター（松山）	愛媛県松山市内 ※詳細は受託者にのみ開示する

- 事務系システム
  役職員が事務業務を行うためのシステム。グループウェア、文書決裁及び決裁済文書管理システム等。
- 奨学金業務システム
  機構の基幹業務である学資金の貸与および返還の各業務を行うためのシステム。JSAS（Jasso Scholarship Application System、ジェイサス）と呼称する。
- 情報資産
  情報（電磁的に記録されたものに限る）及び情報を管理する仕組み（情報システム及びシステム開発，運用及び保守のための資料等）の総称。
- 情報システム
  情報処理及び通信に係るシステムをいう。
- 情報セキュリティ対策機器
  情報資産の外部流出や破壊等から保護することを目的とした機器。ファイアウォール、サンドボックス解析装置等。
- 情報セキュリティポリシー
  情報資産の情報セキュリティ対策について総合的・体系的かつ具体的にまとめたもの。対策基準や実施手順などを含む。
- シンクライアント
  最小限の機能を持つクライアント端末から、ネットワークを介して OS の機能を提供する。当機構の職員が利用する端末の多くはシンクライアント型であり、総数としては約 700 台。
- セキュリティインシデント
  当機構の運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故、情報システムの運用におけるセキュリティ上の問題として捉えられる事象。

・ 相関分析システム
サーバーやネットワーク機器等から集められたログをセキュリティの観点で分析するシステム。本調達では受託者が導入する。
・ データセンター
当機構の主要機器を設置している施設。場所は東京都特別区にあり、セキュリティの理由により受託者にのみ詳細を開示する。
・ ネットワーク再構築
従来のネットワーク基盤から、仮想ネットワークにて構成する基盤への移行、切り替え業務を指す。データセンターの中心となる基盤を構築するのが、データセンターネットワーク再構築事業者。その基盤と連携して各拠点およびデータセンターへの一部を担当するのが拠点ネットワーク再構築事業者である。
・ ファットクライアント
OS、記憶媒体等、各種機能をローカル側に備えたクライアント端末。主にB系端末として使用し、総数としては約400台。
・ フォレンジック
当機構の情報資産を対象とし、証拠保全及び調査、分析が可能な状況とする。本調達では受託者を中心にフォレンジック（証拠保全）を行い、その後にフォレンジック調査を実施する。
・ 不正侵入検知・防御システム
次世代ファイアウォール、ロードバランサー、アンチスパム装置にて構成される、外部からの不正侵入やスパムメール等を検知、防御するだけでなく、内部からの通信においても通信内容により細かな制御を実現する。仮想ネットワーク制御機器より動的制御が可能。
・ 不正接続防止サーバー
ネットワークに接続された端末を自動的に検知し、不正に接続された端末の通信を遮断する機能を有したサーバーおよびソフトウェア。
・ ログ収集システム用サーバー
ネットワーク機器、セキュリティ機器からログを収集し、一元管理する機能を有したサーバーおよびソフトウェア。

2　調達の概要

2.1　本調達の内容

本調達の調達内容を以下に示す。これらは主な項目を記載したものであり、詳細については別項「業務要件」等に定める。

2.1.1 運用監視業務

- 情報セキュリティ対策機器の運用監視業務
- 当機構におけるセキュリティインシデントの監視、対応業務
- 業務に必要となる機器の導入、保守および運用監視
- 対象機器の設定変更および付帯作業
- 対象機器の構成管理および付帯作業
- 各種資料作成、提供
- ヘルプデスク

2.1.2 運用開始、終了時対応

- 関連事業者からの聞き取り、引き継ぎ
- 次期事業者への引き継ぎ

2.1.3 技術支援

- 会議への出席
- 技術的な質問、相談、助言
- 情報提供
- 当機構および他組織への説明

2.1.4 その他

- 当機構が必要と定めるもの

2.2　本調達の範囲

2.2.1保護すべき対象

当機構が取扱う情報資産すべてを保護すべき対象とする。

2.2.2業務開始時の対象機器

当機構にて稼動しており、本調達の対象となる機器を「別紙 1.対象機器一覧」に示す。それぞれの機器に対して、別項の「業務要件」にて記載する業務を実施すること。これらは契約の範囲内で、随時、契約ベンダーのサポートを受けられる状態であるため、積極的に活用し、別項「業務要件」にて記載する業務を実施すること。

なお、ここで記すものはあくまで主要機器である。実際の機器と差異があった場合は、当機構と調整とする。また、運用期間中に移設や入替、機器の増減が発生する場合があるため、同等規模の台数であれば本調達範囲内で同様に対応すること。また、一般にセキュリティ機器とみなされない機器・システムについて、後述のインシデントハンドリング業務を遂行するうえで、必要と認められる場合は、業務を実施する対象とすること。

2.2.3受託者導入機器

下記については、当機構には存在しないため、最低限必須と考えられるものを明記している。その他、業務に必要な機器等があれば、受託者にて導入すること。

なお、これらは当機構への納品物ではない。従って、受託者にて運用、保守等を行い、運用期間満了後に受託者にて撤去をすること。

必要機器例

項番	機器
1	SOC と接続する回線、ネットワーク機器（閉塞網、ルータ等）
2	相関分析システム（SIEM）
3	作業用端末
4	自動監視用システム
5	構成管理システム

2.3　作業スケジュール

・　受託者決定から運用期間の前日までを準備期間とし、運用期間中における業務実施に向けてSOCの立上げや、機器の導入、当機構、関連事業者への聞き取り、運用

ルールの合意等を行うこと。
- 運用開始時に本調達に定める内容がすべて提供できるよう準備を行うこと。
- 本調達以外の関連事業者のスケジュールについて何らかの原因による遅延等が発生した場合、当機構と協議の上、受託者は該当業者と調整し、本番運用開始に極力影響のないよう業務を遂行すること。
- 運用開始に影響することが予見された場合には、当機構に報告し、対応の指示を仰ぐこと。スケジュール調整が受託者だけでは困難な場合は、当機構および関連事業者を交え、別途協議する場を設ける。

2.4　運用・業務委託

2.4.1 期間

- 運用期間
  2019 年 4 月 1 日（水）～2022 年 3 月 31 日（木）

  以下に期間中のより詳細な日程を示す。

- 納入成果物の提出、運用開始準備期限
  2019 年 3 月 15 日（金）
- 受入検査
  2019 年 3 月 18 日（月）～2019 年 3 月 25 日（月）
- 運用期間
  2019 年 4 月 1 日（月）～2022 年 3 月 31 日（木）

2.4.2 形態

- 本調達は業務委託とする。
- 費用については運用期間中に定額での月払いとする。
- 受託者が導入する機器等は納品対象外であり、当機構への資産とはしない。
- その他詳細は契約書等にて定める。

2.4.3 完了通知

- 受託者は業務を完了した際に、直ちにその旨書面を以て当機構へ通知すること。

2.4.4 **その他**

- 運用期間中に障害の多発や、拠点およびシステムの追加等により業務量の増加や役務の規模が拡大した場合においても、原則として費用の変更は発

生しないものとする。ただし、受託者の自助努力により対応可能な範囲を超過する場合は、協議のうえ決定とする。その対応可能な範囲は事前に定量化するものとし、想定していなかった等が無いよう、提案書へ明記すること。

2.5　納入物

納入物の詳細は以下を参照すること。なお、各納入物品はすべて当機構の協議を以て承認を得ること。

2.5.1 納入成果物

2.5.1.1　　運用期間前の納入成果物

運用期間前における納入成果物と納入期限を以下に記す。これらは必要最低限を記したものであるため、必要に応じて納入物を追加すること。なお、納入期限は初回納入におけるものであり、プロジェクトの状況により随時改訂し、原則として受入検査時に最終版を納入すること。

項番	成果物	初回納入期限	概要
1	成果物一覧	受託者決定後 2 週間	本調達で対象となる役務、納入成果物の一覧。
2	基本計画書	受託者決定後 2 週間	プロジェクトの実施方針、スケジュール、体制、推進計画、予定工数を記載する。
3	要件定義書	受託者決定後 2 週間	定義された実施すべき業務を整理し、記載する。
4	現地調査計画書	受託者決定後調整	現地にて事前調査を行うにあたり、その内容や日程等、計画を記載する。
5	現地調査結果報告書	受託者決定後調整	現地調査の結果を記載する。
6	基盤設計書	受託者決定後 3 週間	ハードウェア、ソフトウェアの論理設計、物理設計、全体構成を記載する。 ※受託者が導入する機器のみ
7	用語集・表記規約	受託者決定後 2 週間	プロジェクト全体で用いる用語の説明や、表記の規約を記載する。
8	各種構成図	受託者決定後調整	ハードウェア構成図、配線図、ラック搭載図、機器諸元等を各事業者より入手あるいは記載し、一元化された構成図を作成する。

9	構成管理手順書	受託者決定後調整	構成管理の手順を記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
10	詳細設計書	受託者決定後調整	設計値、設定値、設定根拠を各事業者より入手あるいは記載し、一元化された設計書を作成する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
11	運用設計書	受託者決定後調整	運用の体制、運用に係るスケジュール、運用項目、監視項目の一覧、データ及びシステムのバックアップについて記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
12	保守手引書	受託者決定後調整	保守体制、運用窓口や運用条件、障害時のフロー等をまとめた運用資料。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
13	監視手引書	受託者決定後調整	監視体制、対応窓口、障害時のフロー等をまとめた運用資料。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
14	操作手順書	受託者決定後調整	全機器の電源操作や設定手順、障害対応等、運用に必要となる手順を記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
15	スケジュール	受託者決定後 1 週間	基本計画書として提出されるスケジュールに対し、進捗状況を記載する。
16	課題管理表	受託者決定後 1 週間	実施にあたり判明した課題を随時記載し、情報の連携を図る。
17	協議の記録等	協議、会議後 1 週間	協議、会議（運用報告会含む）の実施記録と議事及びその際に提出された資料を記載する。
18	付属マニュアル類	受入検査前	機器等に付属するマニュアルとメディア類。 ※受託者が導入する機器のみ
19	業務改善実施報告書	改善実施前随時	業務改善を実施するにあたり、その内容と効果を記載する。

20	業務改善結果報告書	改善実施後調整	業務改善を実施したことによる結果、効果を記載する。
21	体制図	受託者決定後 1 週間	運用開始に向けた体制、運用期間中の体制（SOC 人員含む）を記載する。
22	工数実績表	受入検査前	受託者決定後から運用開始までの各工程にかかった工数を工程ごとに記載する。
23	サービスレベル合意書	受入検査前	当機構と関連事業者の保守内容を調査・分析し、システムごとのサービスレベル(システム稼働率、RPO, RTO 等)を定義し文書。それに準じて OLA を設定すること。

2.5.1.2　　運用期間中の納入成果物

運用期間中における納入成果物と納入期限を以下に記す。これらは必要最低限を記したものであるため、必要に応じて納入物を追加すること。なお、納入物はプロジェクトの状況変化や内容の変更を反映し、最新の情報に随時改訂すること。

項番	成果物	納入時期	概要
1	成果物一覧	発生時調整	本調達で対象となる役務、納入成果物の一覧。
2	基本計画書	発生時調整	プロジェクトの実施方針、スケジュール、体制、推進計画、予定工数を記載する。
3	要件定義書	発生時調整	定義された実施すべき業務を整理し、記載する。
4	現地調査計画書	発生時調整	現地にて事前調査を行うにあたり、その内容や日程等、計画を記載する。
5	現地調査結果報告書	発生時調整	現地調査の結果を記載する。
6	基盤設計書	随時	ハードウェア、ソフトウェアの論理設計、物理設計、全体構成を記載する。 ※受託者が導入する機器のみ
7	用語集・表記規約	発生時調整	プロジェクト全体で用いる用語の説明や、表記の規約を記載する。
8	各種構成図	発生時調整	ハードウェア構成図、配線図、ラック搭載図、機器諸元等を各事業者より入手あるいは記

			載し、一元化された構成図を作成する。
9	構成管理手順書	発生時調整	構成管理の手順を記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
10	詳細設計書	発生時調整	設計値、設定値、設定根拠を各事業者より入手あるいは記載し、一元化された設計書を作成する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
11	運用設計書	発生時調整	運用の体制、運用に係るスケジュール、運用項目、監視項目の一覧、データ及びシステムのバックアップについて記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
12	保守手引書	発生時調整	保守体制、運用窓口や運用条件、障害時のフロー等をまとめた運用資料。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
13	監視手引書	発生時調整	監視体制、対応窓口、障害時のフロー等をまとめた運用資料。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
14	操作手順書	発生時調整	全機器の電源操作や設定手順、障害対応等、運用に必要となる手順を記載する。受託者導入機器以外も対象とし、必要に応じて他事業者から入手すること。
15	作業計画書	運用報告会 3 営業日前	中長期的な作業がある場合、WBS を作成し、進捗状況を記載する。
16	課題管理表	運用報告会 3 営業日前	実施にあたり判明した課題を随時記載し、情報の連携を図る。
17	協議の記録等	協議、会議後 1 週間以内	協議、会議（運用報告会含む）の実施記録と議事及びその際に提出された資料を記載する。
18	保守実施報告書	発生時調整	保守対応における実施内容、事象、影響等を記載する。

19	業務改善実施報告書	改善実施前随時	業務改善を実施するにあたり、その内容と効果を記載する。
20	業務改善結果報告書	改善実施後調整	業務改善を実施したことによる結果、効果を記載する。
21	体制図	発生時調整	運用開始に向けた体制、運用期間中の体制（SOC 人員含む）を記載する。
22	工数実績表	月間定例会議 3 営業日前	各業務にかかった工数を業務ごとに記載する。期間は前月初日～末日を対象とし、毎月提出する。
23	サービスレベル評価書	月間定例会議 3 営業日前	サービスレベル合意書に基づいて業務が遂行されているかの評価を記載する。

2.5.2 納入形式

2.5.2.1 受入検査前（準備期間中）の納入形式

- 紙（会議出席者数分）
- 電子データ（メールでの提出）
- MS Word 2010、MS Excel 2010、MS PowerPoint 2010で読み込み、編集が可能なものであること。PDFやVisio等、その他のファイル形式については機構と協議とし、成果物の内容によっては許容する。

2.5.2.2 受入検査時の納入形式

- 紙媒体正副1 式ずつ（バインダー綴じ。計2 式）
- 電子媒体（CD-R 又はCD-RW、DVD±R 又はDVD±RW 等） 正副1 式ずつ（計2 式）
- MS Word 2010、MS Excel 2010、MS PowerPoint 2010で読み込み、編集が可能なものであること。PDFやVisio等、その他のファイル形式については機構と協議とし、成果物の内容によっては許容する。
- 構成管理資料については、その内容に応じて調整とする。

2.5.2.3 運用期間中の納入形式

- 紙（会議出席者数分）
- 電子データ（メールでの提出）
- MS Word 2010、MS Excel 2010、MS PowerPoint 2010で読み込み、編集が可能なものであること。PDFやVisio等、その他のファイル形式につ

いては機構と協議とし、成果物の内容によっては許容する。
- 構成管理資料については、その内容に応じて調整とする。

2.5.3 納入場所
- 納入成果物は当機構市谷事務所へ納入すること。
- その他の納入物については調整の上、決定とする。

2.5.4 検査・検収

2.5.4.1 受入検査
- 受託者は、納入期限までに役務実施準備、当機構への納入を終え、当機構による受入検査を受けなければならない。
- 検査が可能な状態になった時点で、当機構へその旨を申し出ること。
- 当機構は、検査期間内に、受託者による業務遂行が可能であるか、納入物が適正な内容であるか等を判定し、妥当と判断された場合に受入検査の合格とする。
- 検査の結果、対象の一部が不合格となった場合には、受託者はただちに必要な修正、改善を行った後に、別途指定する期限（原則、検査期間内）までに再度提供すること。
- 受託者は、当機構からの質問や指摘、検査への対応を行うとともに、当機構の指示に従うこと。また、当機構からの修正および改善要求があった場合には、適切に対応すること。
- 検査にかかる受託者の作業および対応に要する費用は、一切を本調達の範囲に含めること。また、必要に応じて再検査を求める場合があることから、変更となったものは資料等により常に履歴を管理し、最新状態を保つこと。
- 外的要因等、受託者の責によらず、検査期間に間に合わない場合は、ただちに当機構へ報告し、提供開始時期の変更等、対応を協議する。ただし、その際は可能な限り運用面に配慮した措置を受託者にて検討、実施すること。

2.5.4.2 検収
- 受託者は、継続的に提供されるサービス、役務等は全て当機構による検収を受けなければならない。
- 当機構は、受託者による業務が契約通りに履行されているか、納入物が適正な内容であるか等を判定し、妥当と判断された場合に検収の合格とする。
- 検収の結果、対象の全部または一部が不合格となった場合には、受託者は

ただちに必要な修正、改善を行った後に、別途指定する期限までに再度提供すること。

- 検収は運用期間中、定期的に行う。原則として毎月月末に実施するが、状況によってはその限りではなく、同月内に複数回行うこともあるので留意すること。
- 受託者は、当機構からの質問、検収への対応を行うとともに、当機構の指示に従うこと。また、当機構からの修正および改善要求があった場合には、適切に対応すること。
- 外的要因等、受託者の責によらず、検収期間に間に合わない場合は、ただちに当機構へ報告し、提供開始時期の変更等、対応を協議する。ただし、その際は可能な限り運用面に配慮した措置を受託者にて検討、実施すること。

2.6　撤去

- 受託者が導入した機器については、本調達の運用期間が満了した際に、当機構の求めに応じて各拠点から当該機器等の撤去を行うこと。
- 撤去に際し、個人情報や機密情報の漏えいを防止するため、現地にてデータ消去装置等により記録された全ての情報を復元できない状態とすることに加え、その結果を記したデータ消去証明書を提出すること。なお、運用期間中の機器の故障による交換においても同様とする。

3　前提条件

3.1　業務における基本方針

- JPCERTコーディネーションセンター（JPCERT/CC）が公開している「CSIRT ガイド」に記載されているインシデントマネジメントの思想のもと、当機構の組織運営に危険を及ぼしかねないセキュリティリスクを排除する。
- 複数の事業者が導入したものが混在しているため、本件受託者に対応を集約・一元管理することで、対応の煩雑さを無くし、迅速な問題解決を図る。
- 高度化・複雑化するセキュリティの脅威へ迅速に対応すべく、安定的、効率的な運用とする。
- 高い専門性が要求されることに加え、規模も大きいため、それらへ対応できる強固な体制とする。
- 遠隔監視、設定作業、トリアージ等が可能なSOCと、インシデントレスポンス、フォレンジックおよび当機構職員と連携して迅速な対応や意思疎通を目的としたオンサイト対応可能な機構専任の人員を含む体制とする。
- 運用監視業務の委託のみならず、セキュリティ対策における検討や課題の洗出し、運用改善等もあわせて行うことで当機構職員へかかる負担を低減する。

3.2　作業場所

- 受託者は、本調達仕様書に基づく作業について、特に当機構の指示が無い限り、受託者の各拠点とそれに付随する場所で行うものとし、事前に当機構の承認を得ること。
- インシデントハンドリング、インシデントレスポンスや、機構が作業場所を指示した場合は、SOCで対応が可能であっても当機構市谷事務所あるいはデータセンター、状況によっては現地にて作業を実施すること。
- 当機構を交えた打合せ、会議等については、原則として当機構市谷事務所で行うものとする。

3.3　関連事業者と役割分担等

本調達の範囲内においては、多くの関連事業者が存在する。本調達の受託者はそれを踏まえ、関連事業者との連携の上、役務を実施すること。

3.3.1 業務開始時の関連事業者

3.3.1.1　セキュリティ運用監視事業者（本件受託者）

・ 本調達における要件実現にかかる役務を実施する。
・ インシデントハンドリング、インシデントレスポンス等、セキュリティに関連する対応を主体的に実施する。
・ 当機構の監督下、本調達内で実施する作業に関して各事業者と主体的に調整を行い、他事業者と協調して役務を実施する。
・ 特にネットワーク運用監視事業者、JASSO-CSIRTとは密接な連携を行い、業務を遂行する。

3.3.1.2　2018 年度セキュリティ運用監視事業者

・ 本調達と同等の役務を2019年3月31日まで実施する。
・ 受託者は、当機構の業務影響、サービスの低下等が無いよう、当該事業者から業務を引き継ぐこと。

3.3.1.3　ネットワーク運用監視事業者（別途調達予定）

・ ネットワーク基盤とその構成機器の保守・運用監視を実施する。
・ 当機構および受託者からの対応指示、連携が可能なNOC（Network Operations Center）を有し、遠隔での常時監視およびネットワークに関する作業全般を担う。
・ セキュリティインシデント等が発生した際は、当該事業者、JASSO-CSIRTと連携して対応にあたる。

3.3.1.4　CSIRT 運用支援事業者

・ 当機構における情報セキュリティリスクに係るガバナンス体制の運用を支援する。
・ 現状の情報セキュリティに関する規程、情報セキュリティリスク、体制を分析し、JASSO-CSIRTの運用に向けて積極的な助言を行う。
・ 本件受託者、セキュリティ運用監視事業者との密接な連携を行い、業務を遂行する。

3.3.1.5　データセンターネットワーク再構築事業者

・ 2017年～2018年に、データセンター内のネットワーク基盤の再構築を実施した。
・ ネットワーク機器や付帯システムの導入、設置を行い、ハードウェア・ソフトウェアの保守を実施する。
・ インターネットシステムの基盤を担っており、各種システムの統合監視

も同事業者のシステムにて行っている。

3.3.1.6　　拠点ネットワーク再構築事業者

・　2017年～2018年に、各拠点のネットワーク基盤の再構築を実施した。
・　ネットワーク機器のみならず、機構内ネットワークの副回線も同事業者にて開通、提供している。
・　ネットワーク機器や付帯システム（不正接続防止、ファイル受渡サーバー等）の導入、設置を行い、ハードウェア・ソフトウェアの保守を実施する。

3.3.1.7　　青海事務所ネットワーク機器提供、保守事業者

・　青海事務所ネットワークを構成する機器、および運用サービスを提供する。
・　拠点ネットワーク再構築事業者への既存設定の提供、および拠点ネットワーク再構築事業者が実施する移行作業のコンティンジェンシープランに参画する。
・　移行作業、切戻し作業の作業体制に参画し、当機構、システム導入事業者の指示に基づき、作業を実施する。

3.3.1.8　　機構内ネットワーク事業者

・　2018 年から順次、機構内ネットワークを開通、提供している。
・　市谷事務所、データセンターをはじめとする当機構の各拠点間を接続する VPN 回線と、ONU、ルータ等を含めた、回線を使用するための物品提供から保守を提供、運用する。
・　当該事業者が提供する回線を「主回線」と位置づける。拠点ネットワーク再構築事業者が敷設したバックアップ用途の回線は「副回線」と呼称する。

3.3.1.9　　データセンター事業者

・　奨学金業務システムをはじめ、当機構の業務の中枢を担う機器を設置するデータセンターを運営する。
・　ラック、電源、空調等のハウジングが可能な設備系、サービスを提供する。
・　インターネット回線、ルータも同事業者が提供する。
・　本調達にて監視回線等を敷設する場合、この事業者が用意したデータセンターへ設置する。

3.3.1.10　不正侵入検知・防御システム提供、保守事業者

・ 次世代ファイアウォール、ロードバランサー、アンチスパム装置を導入、提供する。
・ インターネットの出入口に配置され、外部からの不正侵入や内部からの不正通信の遮断、スパムメールフィルタ等の当該事業者が導入した機器は、ネットワーク再構築事業者が導入した機器と連携し、セキュリティインシデントが発生した端末の遮断等を行う。

3.3.1.11　ログ収集システム提供、保守事業者

・ ログ収集システムのハードウェア、ソフトウェアを導入、提供する。
・ Proxyサーバー、メールサーバー等のログが蓄積されるため、障害の切り分け等で本システムの操作が必要となる場合は、当該事業者と調整する。

3.3.1.12　インターネットシステム保守事業者

・ インターネットとの通信を行うシステム(外部公開 Web サーバー、DNS サーバー、メールサーバー、Proxy サーバー)を運用、保守する。
・ ハードウェアの構築、導入とは別事業者であるが、部品交換等が必要となった場合は、当該事業者を通じて保守コールをする。

3.3.1.13　奨学金業務システム用インフラ基盤提供事業者

・ 奨学金業務システムのハードウェア、ソフトウェアの構築から導入、保守、稼動維持を提供する。
・ 受託者は、当該事業者が構築するシステムへ組み込み、業務が可能なようにすること。
・ 2018 年 7 月～2019 年 3 月上旬に各種試験、2019 年 3 月に現行の奨学金業務システムから切替を行う予定である。

3.3.2 関連事業者との調整

3.3.2.1　関連事業者への依頼や調整事項

・ 受託者は、関連事業者への依頼や調整等について、当機構の承認を得て実施すること。
・ 当機構からの要求により関連事業者を交えた会議を実施する場合があるので留意すること。
・ 依頼や調整等 に関して、必ず証跡を残すこととし、当機構に無断で意

思決定を行わないこと。

- 関連事業者への依頼や調整等は、認識の齟齬が無いよう明瞭かつ正確な表現をすること。また、突発的な依頼は行わず、余裕のある日程を確保すること。
- 本調達仕様書に記載する関連事業者は調達時点で判明しているものである。記載されていない事業者（本調達の運用期間中に追加や変更となるもの）、他組織（所管省庁、監査法人等）であっても、同様に対応すること。

3.3.2.2　関連事業者からの依頼や調整事項

- 受託者は、関連事業者からの依頼や調整等について、当機構の承認を得たものに対して、必要となる調整作業を支援すること。特にセキュリティに関することは、受託者にて主体的に対応すること。
- 当機構からの要求により関連事業者を交えた会議を実施する場合があるので留意すること。
- 依頼や調整等 に関して、必ず証跡を残すこととし、当機構に無断で意思決定を行わないこと。
- 本調達仕様書に記載する関連事業者は調達時点で判明しているものである。記載されていない事業者（本調達の運用期間中に追加や変更となるもの）、他組織（所管省庁、監査法人等）からであっても、同様に対応すること。

3.3.3 関連事業者との責任分界点

- セキュリティインシデント発生時等、緊急を要する事態においては、受託者が各事業者よりも権限を有するものとする。当機構と同等の立場として各事業者へ指示を出すことに加え、状況によっては自らが作業も行うこと。
- 本案件の役務の実施にあたり、必要となる情報について、各事業者への聞き取りや、現地調査、コンフィグ分析等を受託者主導で実施すること。
- 当機構が保有する機器の設定変更の要否の調査および判断は、当機構を交えて受託者主導で実施すること。
- サーバー類のアプリケーションの改修やネットワーク機器の設定変更は発生しないものとするが、やむを得ず必要となる変更については当機構および各事業者への説明を実施すること。あわせて変更時のサポートを実施すること。
- 本調達にて他社の機器、システム等に対して、互いの稼働に影響を与えないことの調査および作業について、関連事業者と協力して、受託者主導で

実施すること。

- 電源、ネットワークケーブル等、他事業者の機器、機材へ接続する必要があるものは、受託者主導で対向機器を含めた影響調査を実施および説明のうえ、接続、稼動確認を実施すること。
- 調査の結果、関連事業者または受託者にて追加費用が発生し、当機構にて費用負担が発生する場合は、当機構を交えた協議とする。

4　業務要件

本調達の業務における要件を以下に示す。

4.1　業務における全体憲章

- 本業務の対象となるシステムは機構の業務における中枢的な役割を担う機器である。特定の組織、団体のみならず、一般の利用者へ向けたものであり、かつ国内外へも広く利用されている。そのことを意識して業務にあたること。
- 本調達と並行して各機器の移設および切り替え、基幹業務システムの更改も行われるものであるため、受託者は必要な情報等に関わる内容について、全体の整合性を確保するための支援を行い、必要に応じて関係業者等の成果物のレビューを実施するなどの対応を行うこと。
- 限られた納期の中でプロジェクトを完遂させる必要があることから、プロジェクトの特性を踏まえながら、手戻りが発生するリスクについて十分に監視・評価を実施しながら、プロジェクトを推進すること。一方で、受託者の進捗の遅れが後続工程の作業遅れに直結し、関係事業者の稼動の遅れに至るリスクがあることから、確実な進捗管理や関係業者との綿密なコミュニケーションを通じた課題・リスクへの先を見越した対応が求められる点について留意すること。
- 工期においては効率性を確保した作業推進が求められることから、本調達以外の影響も作業計画の策定や課題・リスクの早期の抽出・対応、次期工程に向けた早期の作業計画の策定といった対応が求められる。そのため本対応に当たっては、受託者のノウハウを結集したプロジェクト計画・運営を図ること。
- 機構および対外的な情勢により、期日どおりのドキュメントの作成完了が困難であったり、機器等の導入完了が困難であったりする場合には、後続工程への影響を早期に分析の上、対応方針について当機構と協議の上、決定すること。
- 機構に報告する内容については、信憑性が確認できるように、報告書の裏付けとなるエビデンス等の情報を添付する等の対応を実施することとし、文書管理標準として管理プロセスを整備の上、確実に実施すること。
- 業務実施にあたっては機構の負担を軽減することを念頭に置き、情報の提供依頼やヒアリングシートへの記入等を一方的に行うのでなく、受託者にて最大限の努力をすること。

4.2　業務基本要件

- 平日、休日問わず、24 時間対応が可能であること。
- 必ずしも常駐する必要はなく、SOC で対応出来る作業は SOC で実施することも許容する。ただし、作業の影響（故意か否か問わず）でネットワークが切断される懸

念がある場合や、障害発生時の立会い、復旧対応等については、その対応の開始から終了までオンサイトで対応すること。
- セキュリティインシデント発生時等、緊急時にオンサイトで対応すること。
- 作業を行った場合、作業実施後にすべての作業内容等を監査できるよう、作業のログ等を取得および保管し、当機構の要求に応じて提出をすること。なお、その作業に機器等が必要な場合、受託者の負担により用意すること。
- ログは 3 年間保管すること。なお、保管期間の 3 ヶ月前に当機構へその対象を報告し、削除する場合は可否の照会を行うこと。
- 修理、保守、交換、廃棄等により破棄又は交換する機器及び資料について、その機器及び資料に記録されている当機構の情報が外部に漏えいすることを防ぐための処置を施すこと。なお、この対応に必要な作業、資源については受託者の負担とする。
- 作業については、特に明確な取り決めが無い限りは、事前に機構の承認をもって実施すること。
- 当機構のみならず、関連事業者からの問合せ、依頼、指示についても同様に対応すること。
- 運用監視業務の品質評価を目的として、当機構と関連事業者の保守内容を調査・分析し、システムごとのサービスレベル(システム稼働率、RPO, RTO 等)を定義した後、それに準じて OLA を設定すること。

4.3　業務実施計画

4.3.1 実施準備

- 業務実施にあたり、必要な情報を実機からの取得や各業者へのヒアリング等により、受託者にて主体的に収集すること。ただし、各事業者の対応は当機構が締結している保守契約の範囲での対応となるため、留意すること。
- 業務実施にあたり、システムの構築が必要な場合は、受託者にてその仕組みを提案し導入すること。

4.3.2 対応計画

- 各種のセキュリティリスクを想定し、当機構および関連事業者への報告や通知、対応、障害復旧の手順、体制、役割分担、連絡方法などの対応計画を策定し、その対応手順、フローを作成すること。
- 下記インシデント発生時に 2 時間以内の駆け付けを目標としてオンサイト対応を受託者が行う旨を計画に盛り込むこと。
  ＜駆け付けが必要なインシデント＞

(a) 重大なセキュリティインシデントに至る可能性がある出来事の発生、もしくは発生が疑われる時。
(b) 情報漏洩や、それにつながる可能性のある予兆活動の発生時。
(c) ウイルス感染や不正アクセスによるホームページの改ざんの発生、もしくは発生が疑われる時。
(d) 当機構で情報漏えいの発生、もしくは発生が疑われる時。
(e) 委託先、関連事業者のシステムへの不正アクセス及び情報漏洩時。
(f) サイバー攻撃に起因すると考えられる Web サイトアクセス不具合時。
(g) 警察や政府機関もしくは、外部からのセキュリティインシデントに関する通報が入った時。
(h) ログ取り込み対象機器及びその他の機器からセキュリティアラートが発せられた時。
(i) 当機構内でマルウェア感染が疑われる時。
(j) その他、当機構もしくは受託者が必要と認める時。

- セキュリティインシデント発生時等、緊急を要する事態での対応を想定し、当機構と同等の立場として各事業者へ指示を出せるよう、計画を立案すること。
- PDCA サイクルの手法により、業務を適宜見直して改善を行うこと。なお、その内容、結果は当機構に報告すること。

4.4 インシデントハンドリング業務

4.4.1 業務対象

- 「別紙 1.対象機器一覧」のインシデントハンドリング業務に「○」と記載されている機器、システム

4.4.2 検知、連絡受付

- 当機構の役職員と当機構システムの運用・保守事業者（調達仕様書記載外の運用・保守業者等を含む）を対象として問合せ窓口業務を提供すること。
- セキュリティに関する問合せ（不審なメールの受信、見慣れない画面の表示等）、連絡などを一元的に受付け、一次応答を行い、必要に応じて当機構や関連事業者への対応を依頼すること。
- 当機構で稼動しているセキュリティ対策機器、ソフトウェアにて検知されたセキュリティアラートを一元的に把握、管理し、セキュリティインシデントの発生有無を監視すること。監視については、マンパワーでの対応を主とするのではなく、監視品質や精度の向上のために、人工知能、機械学習機能を有する検知システムを活用すること。
- 採用する人工知能・機械学習機能については、導入後学習期間がなくても、

即時、セキュリティインシデントの効果ある監視が開始できること。また、管理負荷軽減のため、エージェントを使用しないで監視可能であること。

- SOC により遠隔で監視が可能な仕組みとし、セキュリティリスクの対応優先度を機械学習により識別のうえ、自動的に知らせる仕組みを有すること。
- ネットワークを遮断する必要がある事態が発生した際は、ゲートウェイと連携して自動遮断する機能を有することとし、タイムリーに検知したことを認識できる体制にすること。
- ネットワーク内での正常時とのふるまいの違いを学習するのではなく、約5分以内に更新されているグローバルなレピュテーション情報に関するビッグデータを保有し、不正な C&C サーバーとのアクセスに関する学習を行えること。
- 検知アルゴリズムまたは検知エンジンは、ブラックボックスにならないよう、論文等により公表されていること。
- セキュリティリスク等が発生した際に、当機構および当機構が指定する個別のシステム管理責任者に第一報の連絡を行うこと。その後、影響度合いにより、返答、指示等を待たず、トリアージ、レスポンスを実施すること。
- 相関分析システム（SIEM）およびセキュリティ機器、ソフトウェア等からのアラートを受け、状況を把握し、セキュリティリスク等が発生した際に、当機構および影響する個別のシステム管理責任者に第一報の連絡を行うこと。その後、影響度合いにより、返答、指示等を待たず、トリアージ、フォレンジック、レスポンスを実施すること。
- その他監視が必要なものについては、それらの監視内容、監視方法、監視体制、異常検知時の連絡方法等を提案し、監視を行うこと。

4.4.3 トリアージ

- セキュリティインシデントの発生あるいはその疑いがあるものに対して、復旧の必要性の判断と復旧作業をする対象や優先順位を決定すること。
- セキュリティインシデントは、転送データ、接続パターン、接続状況等の観点からリスクレベルを判断して優先順位を決定すること。判断の遅れを防ぐため、人工知能（機械学習機能）を有する検知システムによるリスク分析結果などを活用すること。
- 実施にあたって、中心メンバーとなって当機構と同等の立場で主体的に対応すること。
- 当機構等に対応要員を派遣する前提で対応するものとし、その手配と調整を行うこと。
- 対応にあたり、必要に応じて、個別のシステム管理責任者及び当機構への協

力を要請すること。
- 原則として別項の対応計画にて合意されたガイドラインに基づいた判断とするが、それに固執せず臨機応変に実施すること。

4.4.4 フォレンジックおよび調査
- セキュリティインシデントの発生あるいはその疑いがあるものに対して、証拠保全及び調査、分析が可能な手段を講ずること。また、必要に応じて当機構の担当者に証拠保存の指示を具体的に行うこと。
- スキルに依存して分析時間に差が出ないよう、人工知能、機械学習機能を有する検知システムによる分析結果などを活用すること。
- セキュリティインシデントの発生有無、被害状況等を調査、分析すること。
- 調査の方針、状況等を個別のシステム管理責任者及び当機構に報告および書類を作成すること。
- 経営層（理事長、理事、役員等）、関係機関（文部科学省、内閣サイバーセキュリティセンター、情報処理推進機構等）、その他当機構が指定する組織、団体向けへの説明の同行と、報告書等の書類を作成すること。
- 実施にあたって、中心メンバーとなって当機構と同等の立場で主体的に対応すること。
- 当機構等に対応要員を派遣する前提で対応するものとし、その手配と調整を行うこと。
- 原則として別項の対応計画にて合意されたガイドラインに基づいた判断とするが、それに固執せず臨機応変に実施すること。
- 対応にあたり、必要に応じて、個別のシステム管理責任者及び当機構への協力を要請すること。

4.4.5 インシデントレスポンス
- セキュリティインシデントの発生あるいはその疑いがあるものに対して、ネットワークからの遮断、隔離等、被害を拡大しない措置を講ずること。フォレンジック後の対応を想定しているが、不要と判断される場合は、フォレンジックを行わずに本作業が実施できるように、導入済みの不正侵入検知・防御システム、サイバー攻撃対策製品等と連携すること。
- 個別のシステム管理責任者及び当機構への応策の内容の説明及び実施に必要な調整を行い、復旧作業を実施すること。
- 原因、復旧作業、再発の防止策等を個別のシステム管理責任者及び当機構に報告および書類を作成すること。根本的な対策が取れない場合は暫定的な復旧策を検討・提案すること。

- 経営層（理事長、理事、役員等）、関係機関（文部科学省、内閣サイバーセキュリティセンター、情報処理推進機構等）、その他当機構が指定する組織、団体向けへの説明の同行と、報告書等の書類を作成すること。
- 実施にあたって、中心メンバーとなって当機構と同等の立場で主体的に対応すること。
- 当機構等に対応要員を派遣する前提で対応するものとし、その手配と調整を行うこと。
- 原則として別項の対応計画にて合意されたガイドラインに基づいた判断とするが、それに固執せず臨機応変に実施すること。
- 対応にあたり、必要に応じて、個別のシステム管理責任者及び当機構への協力を要請すること。

4.5　構成管理業務

4.5.1 業務対象

- 「別紙 1.対象機器一覧」の構成管理業務に「○」と記載されている機器、システム

4.5.2 システム構成管理

- 当機構に設置済みの各機器の構成、設定値を各事業者より入手し、各種情報を履歴管理すること。
- セキュリティ対策等の各種ドキュメントを各事業者より入手し、入手した各種情報については、一元化された資料を作成し、履歴管理すること。
- 構成や設定の変更を行う都度、その情報をドキュメントに反映し、常に最新の状態を保つこと。
- 構成管理対象ドキュメントのファイル毎に、更新日時、変更点等の履歴を管理するとともに、変更前の古いファイルを保存し、どのような変更を経て最新のファイルになったか確認できるようにすること。
- 構成管理対象ドキュメントのファイルが更新された際、当機構および当機構の指定する関連事業者に、自動でメールにて更新の連絡を行うこと。

4.5.3 インシデント、問合せ管理

- 発生したインシデント、脅威を事案毎に記録・管理し、状況が常に把握できる仕組みとすること。なお、管理された情報は当機構の要求に応じて、その都度提出、報告が可能なこと。
- 問合せ内容を FAQ の形式に取りまとめて、当機構へ提供すること。この FAQ はグループウェア等で、当機構内に公開する。情報システムに精通した者ばかりではないため、万人にわかりやすい平易な内容とすること。

・ 受け付けた問合せ内容を記録し、回答状況を管理すること。また、記録の集計、分析を行うこと。

4.6 相関分析業務

4.6.1 業務対象

・ 「別紙 1.対象機器一覧」の相関分析業務に「○」と記載されている機器、システム

4.6.2 機器機能要件

4.6.2.1 機能要件

・ 異種のログを統合的に検索したり、相互に関連付けて分析したりするため、様々なログに散在する情報を組み合わせて分析を行うことができること。
なお、以下の検索速度を目安として有すること
(a) 50,000 件/秒（密データ）
(b) 5,000 件/秒（疎データ）
・ 任意のソースからログと機器の情報を収集し、インデクス化できること。
・ セキュリティインシデント発生時の侵入ルートの調査やアプリケーションの故障対応等が可能な情報を取り込み、リアルタイムで検索、分析が可能であること。
・ 認証ログ、アクセスログ、操作ログ等の各種ログを相互に関連付けて検索が可能であること。
・ 別途導入済みのログ収集システムと連携し、転送されるログを取り込めること。
・ 取り込んだログをリアルタイムに動的に変化するレポートとして作成が出来ること。
・ 取り込んだログの絞り込みを行う際、マウスオーバー及びタイムラインバーによる検索条件設定が可能なこと。
・ 作成したレポート、ダッシュボード上をクリックすることで、詳細ログにドリルダウン可能なこと。
・ 受託者が開発し適用実績のある検知ルール群をまとめたテンプレートを用意し、有効なものであれば適用すること。
・ 対象が増加しても遅延なく動作すること。
・ インシデント発生時のキャプチャデータを証拠として保全すること。
・ イベントを検出した際に、メール通知や外部コマンド実行などの機能を有すること。

4.6.2.2　　ハードウェア要件

- ラックマウント型であること。
- 台数は 1 台以上であること。
- データセンターが用意した EIA 規格に準拠した 19 インチラック(奥行き 1,000㎜)に搭載可能であること。
- AC100V または 200V の電源に対応すること。
- 提案時点で販売、提供されている最新の機種を採用すること。採用しない場合には、その理由を示すこと。
- 他の事業者においても市場で調達可能な製品であり、受託者が独占的に供給するものでないこと。
- 中古（再利用品）ではなく新品であること。
- ラックマウントにキット類等が必要な場合には、併せて納入すること。
- その他要求要件を満たすために、導入が必要な機器等があれば受託者にて提案し本調達費用に含めること。

4.6.3 導入作業要件

4.6.3.1　　構築作業

- 別項「機能要件」に記すすべての動作が実行可能なよう設定および構築作業を行うこと。
- 必要に応じて、各事業者より必要な情報（標準のログフォーマット、転送元の構成等）を入手し、作業を行うこと。
- セキュリティアセスメントに基づく、ログ相関分析によるログ監視内容や、イベントに応じた自動遮断ポイントの提案および関連機器の設定変更作業などを実施すること。
- 各種要件を満たすための最適な設定値を検討し、設定作業を実施すること。
- 設定値については事前に当機構と調整の上、決定とすること。

4.6.3.2　　機器設置作業

- 各物品を指定された方法、ルートで所定の位置へ搬入すること。
- 機器を車両で運搬して搬入する場合、機器設置場所となるデータセンターは、車両の大きさや重量、駐車スペース、作業可能時間帯に制限がある。そのため、近隣の駐車場を利用して搬入する可能性も考慮すること。

- データセンターへの事前発送や受け取りは出来ないため、持ち込みにより搬入すること。
- 機器が破損しないよう緩衝材や箱等で梱包し、その部材は搬入後に受託者にて持ち帰り、処分すること。
- 全ての機器に対して、ラックへ搭載、設置したうえで耐震固定を施すこと。
- 既存機器との LAN ケーブルや電源ケーブル等の接続、当機構所有機器への挿しこみは受託者の責任、負担にて実施すること。
- 既存機器の撤去は、本調達では実施しないものとする。
- 休日や深夜早朝に実施する可能性も考慮すること。

4.6.3.3　　導入、試験

- 作業実施前に、正手順と切戻し手順を記載した作業手順書、動作試験実施要領を記載した試験項目書、および、移行完了条件を提出し、当機構と合意を得ること。
- 導入作業は、関連事業者と作業に係る全ての調整を行い、当機構の承諾を受けた上で、当機構業務に影響がない時間帯に実施すること。なお、作業 1 回につき、1 回以上の予備日を予め、用意しておくこと。
- 作業実施にあたり、導入前後に試験を実施すること。
- 導入後の動作試験を実施した結果が想定と異なった場合は、直ちに当機構に報告すること。その後、業務・サービス影響を把握して、当機構に報告すること。なお、その後の作業続行の可否は、当機構と協議の上、決定する。

4.6.4 運用・保守要件

4.6.4.1　　運用要件

- 収集したログに対して、セキュリティインシデントの発生またはその兆候があった際に、分析・対処を行うこと。また、マルウェアについては､別途契約済みのセキュリティベンダー等へ検体を依頼すること。
- 必要に応じて、相関分析ルールを追加し同様の兆候の監視を強化すること。
- 別項「インシデントハンドリング」の実施に際し、本システムを活用して対応にあたること。
- 導入後も当機構が有用と判断したものは、本システムへ取り込み、分析を行えるように設定すること。

- レピュテーション情報や脅威検知モデルの情報は、随時、自動的に最新の情報が反映されるようにすること。

4.6.4.2　ハードウェア・ソフトウェア保守要件

- 故障発生の有無を平日、休日問わず、24 時間監視すること。
- 別の監視センター等で監視する場合は、SOC と滞りなく状況を連携すること。
- 必要に応じて詳細ログの調査や情報収集を行い、根本原因の調査を実施すること。
- 障害受付から 5 時間以内を目標に、オンサイトにて部品交換等、復旧作業を行うこと。
- ソフトウェアの修正プログラム対応、バージョンアップ対応を実施すること。なお、安定運用を鑑み、バージョンアップについて当機構と事前に協議すること。
- 納入した機器に対して作業を行った場合、事後にすべての作業内容等を監査できるよう、作業のログ等を取得し、保管すること。なお、その作業に機器等が必要な場合、受託者の負担により用意すること。
- 修理、保守、交換、廃棄等により破棄又は交換する機器及び資料について、その機器及び資料に記録されている当機構の情報が外部に漏えいすることを防ぐための処置方法（データを読み出せないようにする処理、資料の消却）については、当機構と協議して決定すること。なお、この対応に必要な作業、資源については受託者の負担とする。
- ハードウェア及びソフトウェアに精通した保守要員により、運用期間中におけるアフターサービス、修理、部品提供等を速やかに行い得る総合的な体制を確保していること。

4.7　コンサルテーション業務

4.7.1 技術的な問合せへの対応、提案

- 技術的な問合せに対して、回答すること。
- 当機構の規程の策定、改訂、対応フローの策定に対して、内容のレビューや、推奨される内容の提案等、支援、助言すること。
- 当機構のシステムの見直しの企画、検討等に対して、推奨される内容を提示する等、支援すること。
- 日々の運用で発見した課題を分析し、改善提案を行うこと。
- 次期事業者へ業務説明、引き継ぎを実施すること。
- 当機構が提供するレピュテーション情報を元に、当機構のセキュリティレベルを維持・向上するための既存セキュリティ機器およびネットワーク機器への設定変更を提案し、承認が下りた後に設定の追加・変更を行うこと。また、変更後は適宜構成情報を更新すること。

4.7.2 情報提供

- 悪意のあるウェブサイトやマルウェアの解析拠点(事業所および解析要員)を日本含め世界に複数拠点持ち、国内外の最新のマルウェアについての情報を提供すること。
- ソフトウェア等製品の脆弱性に関連する情報(脆弱性の名称、公表日、共通脆弱性識別子(CVEID)、共通脆弱性評価システム(CVSS)の基本値・現状値、信頼性、対象ソフトウェア名およびバージョン、影響、攻撃シナリオ・エクスプロイト情報、緩和策)を提供すること。
- マルウェアに関連する情報(マルウェアの名称、発見日、マルウェアの種類、影響度を示す指標、普及度を示す指標、影響を受けるソフトウェアおよびバージョン、動作内容(ファイル、レジストリ書き込み、通信先 IP アドレスやドメイン情報など)、駆除方法、緩和策)を提供すること。
- 不正な IP アドレスに関連する情報(初観測日、最新観測日、危険度を示す指標、位置情報、攻撃の種類)を提供すること。
- 不正なドメイン・URL に関連する情報(初観測日、最新観測日、危険度を示す指標、Whois 情報、攻撃の種類)を提供すること。
- 上記のうち重要であると判断されたものについては直ちに情報を提供し、修正プログラム適用計画を提出すること。（最低頻度は 1 ヶ月に 1 回）

5　プロジェクト運営

5.1　プロジェクト管理

5.1.1 プロジェクト実施計画

- 受託者は、実施計画書等、別項「納入物」に示す書類を作成し、当機構による承認を得ること。
- 期限までに確実に作業を完了するために、プロジェクトは適切に管理されなければならない。このためプロジェクト計画では、本調達の作業を完遂させるうえで必要となる作業を漏れなく洗い出すこと。
- 特別な事由が無い限り、段階的な開始、スモールスタート、縮退体制での運用は認めない。運用期間中においては業務レベルが低下することなく提供できるように計画すること。
- 実施計画書を変更する必要が生じた場合は、速やかに改定する計画を策定し、当機構と調整を行い、承認を得ること。

5.1.2 プロジェクト管理の実施

- 受託者は、計画書に基づき、適切にプロジェクトの進捗管理、課題・問題管理、構成・変更管理、リスク管理、情報セキュリティ管理を行うこと。
- 受託者の責によらない要因でスケジュールについて何らかの原因による遅延等が発生した場合、当機構と協議の上、受託者はその起因となる者と調整し、本番運用に極力影響のないよう業務を遂行すること。
- 業務に影響することが予見された場合には、当機構に報告し、対応すること。

5.1.3 会議体

5.1.3.1　　キックオフミーティング

- 本プロジェクトの開始に際して、受託者主導により実施すること。
- 実施計画書一式を提出し、必要となる情報及び資料を用意し、当機構へ口頭での説明とともに書面で提出すること。
- 受託者決定後5営業日以内に実施すること。

5.1.3.2　　進捗報告

- 進捗状況、課題等報告を、受託者主導により実施すること。
- 必要となる報告を、当機構へ口頭での説明とともに書面で提出すること。

・ 初回はキックオフミーティング開催後1週間以内に開催し、以後の周期は原則として1週間に1回とする。ただし、状況によって隔週または不定期での開催とする。
・ 原則として提供開始までの期間とする。

5.1.3.3 運用報告会

・ 運用におけるインシデント等の発生状況、問合せ件数、課題等報告を、受託者主導により実施すること。
・ 必要となる報告を、当機構へ口頭での説明とともに書面で提出すること。
・ 初回は運用開始後１ヶ月以内に開催し、以後の周期は原則として１ヶ月に１回とする。ただし、状況によって隔週または不定期での開催とする。
・ 原則として運用終了までの期間とする。

5.2 体制

5.2.1 運用開始に向けた対応体制

運用開始までの期間、下記の体制を維持すること。

5.2.1.1 運用開始に向けての実施体制

・ 運用開始に向けて本調達作業を実施するものを業務従事者とし、SOCのオペレーター、オンサイト作業者、エンジニア、保守員等を含む、運用開始に関係する人員すべてを対象とする。
・ 業務従事者の最小限の体制として、統括責任者（業務全体を統括する責任者）、実施責任者（業務完了まで継続して本調達を実施できる者であり、業務の実施にあたっての責任者）、実施者（実施責任者の配下に属し、個々の作業を行う者。）、アカウント管理者（契約担当）からなる実施体制を運用開始まで常にとり、本調達作業を履行すること。なお、これらは併任しないこととする。
・ 受託者の責によるもののみならず、当機構や関連事業者に起因するものや、不測の事態等により、本件受託者へ発生しうるリスクへの対応が可能なよう、十分な体制を確保すること。
・ 各種作業については、業務従事者が2名以上立会うこととし、窓口となって対応すること。
・ 誠実な対応と判断されない場合（言動、態度等）や、業務遂行上不利益（ミスの多発、隠匿等）と当機構が判断した場合、即日、代替要員の確保等、体制の変更を行うこと。なお、その際は業務への影響を最小限に

抑える措置を受託者負担により講ずるものとする。

- 受託者都合により業務従事者を変更する場合は、遅くとも14営業日前に申し出て当機構の承認を得ること。なお、その際は業務への影響を最小限に抑える措置を受託者負担により講ずるものとする。
- 体制を変更する場合は、当機構の承認を得るとともに、更新した体制図を提出すること。

5.2.1.2　運用開始に向けての業務従事者の資格

- 統括責任者は下記をすべて満たしていること。
  (a) 経済産業省情報処理技術者試験のプロジェクトマネージャ試験の合格者あるいはPMI(プロジェクトマネジメント協会)が認定するPMP(プロジェクトマネジメントプロフェッショナル)の資格を取得し維持していること。
  (b) 情報処理安全確保支援士あるいは情報セキュリティスペシャリストに合格していること。
  (c) セキュリティ関連の実務経験（インシデントハンドリング等。CSIRT構築支援やコンサルティングは含まない。）を3年以上有すること。

5.2.2運用期間中の対応体制

運用期間中、下記の体制を維持すること。

5.2.2.1　運用期間中の実施体制

- 運用期間中、本調達作業を実施するものを運用業務従事者とし、SOCのオペレーター、オンサイト作業者、エンジニア、保守員等を含む、運用期間中に関係する人員すべてを対象とする。
- 運用業務従事者の最小限の体制として、運用統括責任者（業務全体を統括する責任者）、運用実施責任者（業務完了まで継続して本調達を実施できる者であり、業務の実施にあたっての責任者）、運用実施者（実施責任者の配下に属し、個々の作業を行う者。）、アカウント管理者（契約担当）からなる実施体制を運用終了まで常にとり、本調達作業を履行すること。なお、これらは併任しないこととする。
- 運用業務従事者は、機構専任の人員を含む体制とし、アカウント管理者を除く2名以上は緊急時を含むオンサイト対応が可能な人員とする。
- 受託者の責によるもののみならず、当機構や関連事業者に起因するものや、不測の事態等により、本件受託者へ発生しうるリスクへの対応が可

能なよう、十分な体制を確保すること。

- 各種作業については、運用業務従事者が2名以上立会うこととし、窓口となって対応すること。
- 誠実な対応と判断されない場合（言動、態度等）や、業務遂行上不利益（ミスの多発、隠匿等）と当機構が判断した場合、即日、代替要員の確保等、体制の変更を行うこと。なお、その際は業務への影響を最小限に抑える措置を受託者負担により講ずるものとする。
- 受託者都合により運用業務従事者を変更する場合は、遅くとも1ヶ月前に申し出て当機構の承認を得ること。なお、その際は業務への影響を最小限に抑える措置を受託者負担により講ずるものとする。
- 体制を変更する場合は、当機構の承認を得るとともに、更新した体制図を提出すること。

5.2.2.2　　運用期間中の運用業務従事者の資格

- 運用統括責任者は下記をすべて満たしていること。
    (a) 経済産業省情報処理技術者試験のプロジェクトマネージャ試験の合格者あるいはPMI(プロジェクトマネジメント協会)が認定するPMP(プロジェクトマネジメントプロフェッショナル)の資格を取得し維持していること。
    (b) 情報処理安全確保支援士あるいは情報セキュリティスペシャリストに合格していること。
    (c)セキュリティ関連の実務経験(インシデントハンドリング等。CSIRT構築支援やコンサルティングは含まない。)を3年以上有すること。

6　情報セキュリティ

6.1　情報セキュリティにおける基本要件

・　本業務は、国の行政機関等のサイバーセキュリティに関する対策の基準となる「政府機関等の情報セキュリティ対策のための統一基準群（平成 30 年度版）」（以下「統一基準群」という。）に準拠した情報セキュリティ対策を行うこと。また、統一基準群の見直しが実施された場合は、その内容を適切に反映し、セキュリティ対策の見直しを行うこと。

・　機構における奨学生及び返還者の個人情報の取扱いに関しては、独立行政法人等における個人情報の保護に関する法律やガイドラインに準拠して行うこと。

6.2　情報セキュリティ遵守における実施方針

・　受託者は、本調達の導入から運用期間中、情報セキュリティを確保するための監査体制を、別項目のプロジェクト管理とは別に組織し、継続的に維持すること。なお、これらは業務従事者とは併任しないこととする。

・　情報セキュリティ対策と方針、体制を提出し、当機構の承認を得ること。不十分であると判断された場合には、速やかに追加対策等の是正措置を行うこと。

6.3　情報セキュリティにおける要員管理

・　受託者は統一基準群や独立行政法人等における個人情報の保護に関する法律やガイドラインに準拠した情報セキュリティを確保するためのセキュリティポリシィや体制を整備すること。また、本体制は、定期的に要員等に対して監査を行い、機構に対して情報セキュリティや個人情報に関する対応状況等を報告すること。

・　受託者は要員に対し、「秘密保持及び個人情報保護に関する誓約書」あるいは類する誓約書に誓約をさせること。業務委託開始、実施時はもとより、退任後、業務委託終了後も責任を負うものとする。

・　受託者は要員に対し、稼働開始時を含め、定期的な情報セキュリティ対策や個人情報保護に関する研修の受講を義務付け、統一基準群や個人情報保護法等を遵守させること。

・　統一基準群や個人情報保護法等の遵守ができない場合の責任の所在及び処罰の内容が明確化され、周知徹底されていること。

6.4　施錠管理

・　業務履行のための施設及び作業スペースには、統一基準群や独立行政法人等における個人情報の保護に関する法律やガイドラインに準拠のうえ、入退出管理を的確に行うために必要な措置を講ずること。

- 業務履行のための施設及び作業スペースで従事する者は、常時、ID カード等を他者に見やすいように着用すること。
- 業務履行のための施設及び作業スペース内への適切でない私物の持込を制限する措置を講ずること。
- 業務履行のための施設及び作業スペースで従事する者以外の者が入室する場合は、事前に所定の手続きを取り、証跡を保存、管理すること。

6.5　情報管理

- 本業務で扱ういかなる情報も、紛失、改ざん、破壊及び漏洩等が行われないように適切に管理すること。
- 本業務で使用する情報設備及び機器は関係者以外の者がアクセスできない環境を構築すること。
- 本業務で使用する情報設備及び機器は、すべて最新のウイルス対策及びその他必要な情報セキュリティ対策を施すこと。
- 本業務での情報の送受信は必要な情報セキュリティ対策を講じた方法で行うこと。
- 過失、故意を問わず、業務履行時及び作業時において発生した印刷物（プリンター、コピー機に限らず、メモ用紙等を含む）の外部持出しを禁ずる措置を講ずること。

6.6　個人情報保護

- 本業務で受託者が知り得ることになった奨学生番号、氏名、住所、連絡先等の個人情報（以下、個人情報）は、独立行政法人等における個人情報の保護に関する法律やガイドラインに準拠して取扱わなければはならない。業務受託終了後も同様とする。
- 受託者は会社全体として個人情報の保護に関する法律やガイドラインに準拠した運用・教育を行い、適切な文書管理・情報管理を行うこと。

6.7　内部監査

- 定期的に受託者内部にて監査を行い、当機構に対しセキュリティの対応状況を報告すること。
- 監査内容は、統一基準群に準拠したものであること。
- 情報セキュリティ対策の履行状況を確認するために、受託者は当機構からの求めに応じて、情報セキュリティ対策の実施状況に関わる報告を速やかに提出すること。

6.8　当機構による監査対応

・　本業務の遂行において、情報セキュリティ対策の履行状況や個人情報の保護状況を確認するために、受託者は機構からの求めに応じて、情報セキュリティ対策の実施状況や個人情報の取扱いに係る運用状況を速やかに報告すること。
・　受託者は、機構からの求めに応じて、業務実施場所等に関する監査対応に応じること。

6.9　その他

・　情報セキュリティ上の重大な問題の発生が予見された、若しくは発生した場合や、当機構から指摘された場合は、速やかにその内容と対策案を報告のうえ、当機構の指示に従うこと。
・　情報セキュリティ事故が発生した場合は、直ちに当機構に報告し、あらかじめ定められた一次対応を行うこと。また、原因分析および再発防止策を検討し、対応状況についても逐一、当機構に報告すること。

7　特記事項

7.1　要求仕様

- 本仕様書の要件は、原則としてすべて必須の要求要件であるが、経済的又は技術的に優れた代替方法による提案を行うことを妨げない。ただし、要件の実現が困難な場合に限り、同等の機能を有する仕組みや、要件と同じ結果をもたらす代替提案を許容する。なお、代替提案を行う場合は、本仕様書に記載された仕様との差分を明らかにした上で、その代替提案を採用することによる影響範囲・メリット、デメリット等を明確にすること。また、代替提案を採用することにより生じる追加作業および費用については、一切を本調達に含めること。
- 全ての要件は当機構が必要とする最低条件を示しており、これを満たしていないとの判断がなされた場合には、不合格となり、落札決定の対象から除外する。
- 使用許諾ライセンスや関連法令に違反すると認められたときには、要件を満たしていないと判断する。

7.2　再委託

- 再委託を許諾するが、いずれの場合においても運用期間中の対応窓口と、本調達仕様書に定める要求要件の履行に際しての責任は受託者が負うこと。
- 受託者は秘密保持、情報セキュリティ、知的財産権等に関して本仕様書が定める受託者の責務を再委託先業者も負うよう、必要な処置を実施し、当機構に報告し承認を得ること。
- 第三者に再委託する場合においても、作業実施期間中は受託者が会議等に出席すること。また、再委託先が作成した資料を提出する際や作業を実施する際も受託者が事前確認を行うだけでなく、その場に立会うこと。
- 詳細については入札資料一式として配布される『委託業務の再委託について』の記載について従うこと。

7.3　受託者要件

7.3.1 受託者資格

- 受託者、再委託先とも、一般財団法人日本経済社会推進協会または海外の認定機関により認定された審査機関による、情報セキュリティマネジメントシステム（ISMS）を取得していること。ただし、社内に同等の情報セキュリティ管理体制の構築及び運用を確立している場合はその限りではない。その場合は、ISMS と同等である根拠が明確に判別可能な資料を入札時に添付すること。
- ワーク・ライフ・バランス等推進の取組みとして、以下のいずれかの認定を

受けていることが望ましい。

（1）女性の職業生活における活躍の推進に関する法律（女性活躍推進法）に基づく認定（えるぼし認定企業）

（2）次世代育成支援対策推進法に基づく認定（くるみん認定企業・プラチナくるみん認定企業）

（3）青少年の雇用の促進等に関する法律に基づく認定（ユースエール認定）

7.3.2受託者実績

・ 受託者が本件と同等以上のシステム規模のセキュリティ運用監視業務について、1者以上の受託実績を有すること。

7.3.3その他

・ 一元的に対応できる体制を備えていること。
・ 本調達に関連する者（受託者、再委託先、リース会社、回線キャリア等）が日本国内に営業所を有し、日本語による対応が行えること。

7.4 受託者責任

・ 本調達仕様書に定める要求要件の履行に際し、誠意を持って実施するとともに、責任を負うこと。
・ 受託者は、受託者が作成し当機構が承認した計画に従い、進捗管理を行うこと。
・ 実施において是正の必要がある場合は、その原因と対策を明らかにし、速やかに是正の計画を当機構へ報告するとともに、是正の実施、評価を行うこと。
・ 受託者の責により当機構の業務に影響が出た場合は、その回復に要した費用等は受託者が負担すること。
・ 当機構が提供する電子情報については、厳重に管理しデータの複写等は最低限に抑えること。また、役務終了後、速やかにデータの削除を行うこと。
・ 提案書等にて記載した認定資格等について、認定の取消などによって記載した内容と異なる状況となる可能性が予見された際や、認定が取り消された場合には、速やかに当機構へ届け出ること。

7.5 瑕疵担保責任

・ 当機構は、成果物に瑕疵があるときは、受託者に対して相当の期間を定めてその瑕疵の修補を請求し、又は修補に代え若しくは修補とともに損害の賠償を請求することができる。
・ 受託者が負うべき責任は、検査・検収に合格したことをもって免れるものではない。

- システムを正常に使用した状態で障害が発生した場合において、原因が受託者の責に帰する場合には、システムが正常に稼働するように対応すること。なお、対応完了後には、現象・原因・対処内容等を報告書として提出すること。
- 詳細は契約書にて取り交わすものとする。

8　付帯事項

8.1　秘密保持

8.1.1 情報の管理

- 受託者は本調達および業務に関して、全ての作業におけるデータの取扱いについては、機密情報管理を徹底すること。
- その他詳細は別項「情報セキュリティ」を参照のこと。

8.1.2 第三者への提供、開示

- 受託者は、本調達に係る業務の実施により知り得た情報（個人情報を含む）を契約履行期間中か否かに係らず、当機構の承諾なしに第三者に提供、開示又は漏えいしてはならない。但し、既に公開されている情報および公知となった情報についてはこの限りではない。

8.2　契約の変更、延長

- 当機構より契約変更または延長を行う場合、その起点となる2ヶ月前までに申出があった場合は、2ヶ月以内で1ヶ月単位の契約変更、延長ができること。またこの場合、延長前と同じ契約内容を同等の費用またはそれ以下で提供できること。
- 契約の終了12ヶ月前、6ヶ月前に当機構へ書面等で通知すること。6ヶ月前までに当機構から延長や満了の申し出が無い場合は、不達の可能性があるため、必ずその意思を確認し、証跡をとること。
- 契約延長に際し、保守延長の費用や保守延長が出来ない機器の交換費用等について、当機構が別途費用を負担する想定である。従って、契約延長を前提とした費用を本調達の入札金額に計上しないこと。

8.3　提案書の提出

- 入札に先立って提案書を提出するものとする。
- 提案内容が要件を満たしているか否かの判定は、本調達についての技術審査会において、仕様書を含む入札説明書で求める提案資料の内容を審査して行う事とする。
- 本調達仕様書は要件を記載したものであるため、当機構にとって有用であるものは、要件の実施に加えて、その内容を積極的に提案すること。
- 提出された内容等について、問合せ等を行う場合があるので誠実に対応すること。
- 説明が不十分なものや、根拠が不明確等、評価が困難であると当機構で判断した場合は、要求要件を満たしていない資料とみなし不合格とするので十分留意して

作成すること。

- 受託者の自助努力により、費用低減における具体的な施策を提案書に添付すること。
- その他、詳細は「提案依頼書」、「提案書作成要領」を参照のこと。

8.4　業務に係る検査職員、監督職員

- 検査職員　情報部　情報管理課　課長
- 監督職員　情報部　情報管理課　情報セキュリティ対策係長

次の資料は機密保持のため削除いたしました。

「別紙１．　対象機器一覧」

「資料閲覧について」及び
「資料閲覧希望者一覧（別紙１）」
「秘密保持誓約書（別紙２）」

日本学生支援機構セキュリティ運用監視業務委託
提案依頼書

2018 年 10 月

独立行政法人　日本学生支援機構

目次

1 調達概要

1．1 件名

日本学生支援機構セキュリティ運用監視業務委託

1．2 調達の目的

独立行政法人日本学生支援機構（以下、当機構）は、「サイバーセキュリティ基本法」および「政府機関等の情報セキュリティ対策のための統一基準群」に則り、情報資産を守るべく、入口出口対策、標的型メール対策、エンドポイントセキュリティ、ウイルス対策等、多岐にわたる情報セキュリティ対策機器を導入してきた。

一方、外部からの攻撃が複雑化・巧妙化しており、未知の攻撃も日々生まれている中、防御側も情報セキュリティ対策機器を導入しただけではすぐに陳腐化してしまうため、日々の運用監視、最新のセキュリティ対策を施していくことが重要である。しかしながら、これらを行うためには多大な技術、知識を要するとともに、昼夜問わず行われてくる攻撃に対応するには、時間を問わず体制を確保することが必要不可欠と考え、2018 年度には外部事業者へ委託を行ったところである。

本調達では、継続的に対応すべく、技術者による遠隔監視拠点の利用をはじめ、専門的知見を有するサポート業務を外部委託することにより、セキュリティインシデント発生時や、インシデントレスポンス、フォレンジック等を昼夜問わず対応可能な体制とし、対応力を強化することを目的とする。

1．3 調達範囲

「日本学生支援機構セキュリティ運用監視業務委託」調達仕様書に記載のとおりとする。

2 提案依頼事項

提案書は、別紙に示す「提案書作成要領」に従い作成すること。

3 提案手続

3．1 提案書提出に関する事項

応札者は、提案書を別紙に示す「提案書作成要領」に従い作成し、機構に提出すること。

3．2 選定方法

本調達の落札者は、総合評価落札方式により決定する。

3．3 選定基準

本調達の落札者を決定するための選定基準は､別紙に示す総合評価基準書によるものとする。

4 留意事項

（1）提案書の作成及び提出等に係る費用は、入札参加者の負担とする。

（2）提案書提出にあたり、以下の場合は無効とし提出した入札参加者は本調達において失格とする。

ア．提案書の提出先、提出期限に適合しないもの。

イ．「提案書作成要領」に記載する提案書の書式に示された条件に適合しないもの。

ウ．虚偽の内容が記載されているもの。

（3）機構における提案書の取扱いについては、以下のとおりとする。

ア．提出された提案書は、本調達における提案書の評価以外は使用しない。

イ．提案書の提出後機構の判断により補足資料の提出を求めることがあるので、速やかに対応すること。

ウ．提出された提案書は返却しないこととする。

（4）その他関連事項については、以下のとおりとする。

ア．本調達のために作成した提案書及び関連資料については、機構の許可なく公表及び他の目的に使用しないこと。

イ．提案書の提出は、１者につき１案のみとする。

ウ．提案書内の記述について、特許権など日本国の法令に基づいて保護される第三者の権利の対象となっているものを使用した結果生じた責任は、作成者（入札参加者）が負うものとする。

提案書作成要領

本調達における提案書作成要領は次のとおりである。

1. 提案書の提出

1.1. 入札に際して、提案書作成要領に基づき作成した提案書を提出すること。
1.2. 提出部数は下記のとおりとする。
- 正本　　：１部
- 正本の写し：６部

2. 提案書の体裁、書式

2.1. 提案書は以下の内容が記載された構成とする。
- 提案書本紙（１冊目）
  表紙
  目次
  第１章　要求要件に対する実施提案
  総合評価項目書
  第２章　総合評価項目に対する具体的提案
  補足、別添資料　※任意
  証明書類　※調達仕様書で定められた場合
- 提案書別紙（２冊目）
  提案の概要

2.2. 各項目にタグ等で目印をつけること。
2.3. 頁毎に取り外しが可能な状態でドッチファイル等に編綴すること。
2.4. 「Ａ４版縦、横書き、左綴じ」「Ａ４版横、横書き、上綴じ」のいずれかで作成すること。なお、頁や章毎に混在することが無いよう、どちらかの書式に統一すること。ただし、提案書本紙の補足、別添資料については、Ａ３版を使用することも可とする。その場合は、Ａ４版の大きさに折り込むこと。
2.5. 各項目に対しての提案内容は項番順に記載すること。
2.6. 各頁にはフッターに頁番号を記載すること。
2.7. 文字は注記等を除き、原則として 10 ポイント以上の大きさとすること。
2.8. 多色刷りを可とするが、色の使いすぎによる視認性の低下や、モノクロ複写・印刷することにより内容がわからなくなる等が無いよう配色等に留意すること。

2.9. 使用する言語及び通貨は、日本語及び日本国通貨とすること。

3. 提案書の記載

3.1. 外装

- 提案書本紙、提案書別紙とも、表面と背表紙から、提案書の件名、提案者（応札者）の社名を判別できるようにすること。

3.2. 表紙

- 当機構宛てのものであること、提案書の件名、提案者（応札者）の住所、会社、代表者、提出する日付を記載すること。
- 正本のみ、会社名に社印、代表者名には代表印を押印すること。

3.3. 目次

- 本紙、別紙に添付すること。
- 項目とページ番号を記載すること。

3.4. 第１章　要求要件に対する実施提案

- 調達仕様書に記載する要件を満たすかどうかについての実施提案を記載すること。
- 左側に調達仕様書の要件、右側に提案者の回答を記載すること。
- 全てに対してそれぞれ対応する形（いわゆる一問一答形式）とし、何を満たすかを明記すること。例えば「1 日に 1 回、当機構へ提示連絡を行うこと。」に対しては、「左記の要件通り実施します。」ではなく、「1 日に 1 回、機構に対して定時連絡を行います。」といった形で記載をすること。
- 一定数以上の数値を要求する要件への提案については、提案する機器やサービスが有する具体的な数値を記載すること。例えば「クロック周波数が 3.2Ghz 以上の CPU を搭載すること。」に対しては、「3.2Ghz 以上の CPU を搭載します。」ではなく、「○○社の××モデル（3.6Ghz）の CPU を搭載します。」といった形で実装する部品の具体的な数値を記載すること。

3.5. 総合評価項目書

- 総合評価基準書の別紙にある総合評価項目書に対して、上部の※印欄に会社名、頁番号に提案書の第２章　総合評価項目に対する具体的提案の頁番号を記入すること。

3.6. 第２章　総合評価項目に対する具体的提案

- 総合評価項目とそれに対する提案を紐付けて記載し、提案内容がどの項目に向けたものか判別できるように作成すること。なお、この際に付番をする項番については、調達仕様書ではなく、総合評価項目の番号とする。
- 提案者の考え方やアピールポイント、強みを記載すること。それに伴って文書

を補完するためのイメージやイラスト、グラフの使用は可能とする。また、応札者が当機構への提案に際して使用する目的での許諾がとれた範囲での引用や転載も可能とするが、出典元および許諾されたものである旨を記載すること。

3.7. 補足、別添資料

- 第２章　総合評価項目に対する具体的提案への直接的な提案ではなく、同章への提案内容に対する理解を深めるための内容のみを添付すること。
- 様式は特に定めない。

3.8. 提案書に添付する事項

- 運用開始に向けた体制とそれぞれの関連性を記した図を添付すること。
- 運用後の体制とそれぞれの関連性を記した図を添付すること。
- 運用開始までの作業内容とスケジュール（線表）を添付すること。
- 調達仕様書「受託者資格」に記載されている事項について、証明書等のコピーを添付すること。
- 別項「受託者実績」に記載されている事項について、証明書等のコピーを添付すること。
- 本調達の実施にかかる作業内容と、それにかかる工数を人日ベースで記載した一覧表を作成し、実現可能な根拠を添付すること。
- 更新時期の関係で証明書等が提出時に期限が超過している場合は、更新前の証明書と、その理由を証明できる旨の説明を添付すること。

3.9. 提案の概要

- 提案内容の要約を簡潔明瞭に記載すること。
- 「詳細は本紙を参照」等、他の資料を参照させず、同紙内で完結させること。

4. 参考

第１章　要求要件に対する実施提案の様式例

項番	要求要件	提案内容
4	ハードウェア要件	
4.1	管理用サーバー	
	クロック周波数が3.2Ghz以上のCPUを搭載すること。	○○社の××モデル（3.6Ghz）のCPUを搭載します。
	○○○	○○○
	○○○	○○○
4.2	クライアント	
	○○○	○○○

5	役務要件	
5.1	ユーザー管理機能	
	1日に1回、当機構へ定時連絡を行うこと。	1日に1回、機構へ定時連絡を行います。
	○○○	○○○
	○○○	○○○

「日本学生支援機構セキュリティ運用監視業務委託」調達

提案書の総合評価基準書

2018 年 10 月

独立行政法人日本学生支援機構

本資料は、「日本学生支援機構セキュリティ運用監視業務委託」の調達に係る提案書の評価基準について述べたものである。

機能及び技術等の評価は、「日本学生支援機構セキュリティ運用監視業務委託　調達仕様書」及び別紙「総合評価項目書」に基づき以下のとおり評価を行う。

１．落札方式

（１）次の各要件に該当する入札者のうち、「２．総合評価の方法」によって得られた数値の最も高い者を落札者とする。

(a) 入札価格が、予定価格の制限の範囲内であること。

(b) 仕様書において明らかにした要件をすべて満たしているか、代替提案により同等以上の内容での提案であること。

(c) 仕様書に記載された技術要件を一つでも満たさない場合は、「不合格」とし、評価対象外とする。

（２）上記（１）の最も高い数値の者が複数あるときは、当該者にくじを引かせて落札者を定める。

２．総合評価の方法

（１）総合評価は、価格点（入札価格の得点）に技術点（提案書による基礎点＋加点）を加えて得た数値により行う。

価格点（830 点満点）＋技術点（830 点満点）

（２）価格点の評価方法については、次のとおりとする。

価格点は、入札価格を予定価格で除して得た値を「１」から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

ただし、入札価格が予定価格を上回った者については、評価対象外とする。

価格点＝（1－入札価格／予定価格）×830 点　※小数点以下切り捨て

（３）技術点の評価方法については、次のとおりとする。

「技術点」は、「基礎点（150 点)」に「加点（最高 680 点)」を加えて得た値（830 点満点）とする。

技術点＝基礎点（150 点）＋加点（最高 680 点）

(a) 基礎点について

上記１．（１）の（b）で示される要件に該当する者を「合格」とし、区分に応じて配分した「基礎点」を与える。

区分 評価	最重要	重要	普通
最低限の要求要件を満たしている	20 点	10 点	5 点

(b) 加点について

別紙「総合評価項目書」で示す各評価項目をその重要度に応じ 3 つの評価区分および評価点（最重要…80 点、重要…40 点、普通…20 点）に区分し、提案内容の優劣について以下の「加点基準」に基づいた 5 段階の評価に応じる割合で付与する。

（加点基準）

提案書で示された各評価項目の記述内容について、以下のような観点も考慮し、総合的に評価を行う。

① 本調達の目的・背景等を正しく理解し、提案内容に具体的に反映されている。

② 提案内容の妥当性、実現可能性について、他の選択肢との比較検討や結論に至る検討過程が具体的に明示されている。

5 段階の評価は以下のとおりとする。

評価	割合
５（特に優れている）	１００％
４（優れている）	７５％
３（特に良い）	５０％
２（良い）	２５％
１（標準である）	０％

なお、女性の職業生活における活躍の推進に関する法律（女性活躍推進法）に基づく認定（えるぼし認定企業）、次世代育成支援対策推進法（次世代法）に基づく認

定（くるみん認定企業・プラチナ認定企業)、青少年の雇用の促進等に関する法律に基づく認定における加点基準については下記の通りとする。

・女性の活躍推進法に基づく認定企業の評価（えるぼし認定企業）
1 段階目：40 点
2 段階目：60 点
3 段階目：80 点
行動計画策定済み：20 点

・次世代法に基づく認定企業の評価（くるみん認定企業・プラチナくるみん認定企業）
くるみん認定：40 点
プラチナくるみん認定：80 点

・若者雇用促進法に基づく認定企業の評価（ユースエール認定企業）
ユースエール認定：80 点

※いずれも認定を満たしていない場合、加点無しとする。
※複数の認定等を受けている企業等については、最も配点が高い認定について評価点とする。
（例えば、配点 80 点の場合、くるみん認定とユースエール認定を受けている時は、配点の高い、ユースエール認定の 80 点を評価点とする。）
※えるぼし認定企業の認定については以下の５つの評価項目により認定されるが、評価においては「③労働時間等の働き方」に係る基準を満たすことを必須とする。
＜えるぼし認定に係る評価項目＞
①採用 ②継続就業 ③労働時間等の働き方 ④管理職比率 ⑤多様なキャリアコース
※行動計画策定済については、常時雇用する労働者の数が 300 人以下の事業主に限る。

別紙 総合評価項目書

※会社名		【入札参加者は※欄を記入すること。】					
提案依頼項目	評価項目	区分	基礎点	加点	加点評価	評価点点数	※提案書頁番号
1．業務要件							
1	「業務実施計画」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。また、その内容が「業務における全体憲章」を意識されたものであるか。	最重要	20	80			
2	「インシデントハンドリング業務」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。また、その内容が「業務における全体憲章」を意識されたものであるか。	最重要	20	80			
3	「構成管理業務」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。また、その内容が「業務における全体憲章」を意識されたものであるか。	重要	10	40			
4	「相関分析業務」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。また、その内容が「業務における全体憲章」を意識されたものであるか。	最重要	20	80			
5	「コンサルテーション業務」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。また、その内容が「業務における全体憲章」を意識されたものであるか。	重要	10	40			
2．プロジェクト運営							
1	「プロジェクト管理」について、その内容と実現方法が簡潔明瞭に記載されており、当機構にとって有効な提案となるものは、その提案意図と狙い、効果が図等を交えて具体的かつわかりやすく記載されているか。	重要	10	40			
2	「体制」について、資質がある者が適切に配置されているかが判断でき、かつ当機構にとって有効な提案となっているか。	普通	5	20			
3．その他							
1	提案書全体において、「調達の目的」が理解されており、当機構の現状の環境や問題点等を踏まえた具体的な提案内容となっているか。	最重要	20	80			
2	提案書全体において、役務を実施するにあたり、想定される課題やリスク、それに対する対策が具体的に明記しているか。	最重要	20	80			
3	関連事業者と役割分担等について、本業務を円滑に進めるための関連事業者の役割が理解されており、その連携手法が具体的に明記しているか。	普通	5	20			
4	添付資料として要求している「受託者の自助努力により、費用低減における具体的な施策」について、実現性があり、かつ当機構にとって有効な提案となっているか。	重要	10	40			
5	以下のいずれかの認定を受けているか。 ・女性の職業生活における活躍の推進に関する法律（女性活躍推進法）に基づく認定（えるぼし認定企業）を受けていること。 ・次世代育成支援対策推進法（次世代法）に基づく認定（くるみん認定企業・プラチナ認定企業）を受けていること。 ・青少年の雇用の促進等に関する法律に基づく認定を受けていること 〈加点基準〉 ・女性の活躍推進法に基づく認定企業の評価（えるぼし認定企業） 1段階目：40点 2段階目：60点 3段階目：80点 行動計画策定済み：20点 ・次世代法に基づく認定企業の評価（くるみん認定企業・プラチナくるみん認定企業） くるみん認定：40点 プラチナくるみん認定：80点 ・若者雇用促進法に基づく認定企業の評価（ユースエール認定企業） ユースエール認定：80点 ※いずれも認定を満たしていない場合、加点無しとする。 ※複数の認定等を受けている企業等については、最も配点が高い認定について評価点とする。 （例えば、配点80点の場合、くるみん認定とユースエール認定を受けている時は、配点の高い、ユースエール認定の80点を評価点とする。） ※えるぼし認定企業の認定については以下の５つの評価項目により認定されるが、評価においては「③労働時間等の働き方」に係る基準を満たすことを必須とする。 ＜えるぼし認定に係る評価項目＞ ①採用 ②継続就業 ③労働時間等の働き方 ④管理職比率 ⑤多様なキャリアコース ※行動計画策定済については、常時雇用する労働者の数が300人以下の事業主に限る。	－	－	80			