資料１－２

# 国立研究開発法人科学技術振興機構
# JST セキュリティ監視運用業務
# 民間競争入札実施要項（案）

令和元年６月

国立研究開発法人科学技術振興機構

# 目次

国立研究開発法人科学技術振興機構　JST セキュリティ監視運用業務
民間競争入札実施要項（案）

# 1　趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のため、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、国立研究開発法人科学技術振興機構（以下「当機構」という。）は「公共サービス改革基本方針」（平成 24 年 7 月 20 日閣議決定）別表において民間競争入札の対象として選定された「JST セキュリティ監視運用業務」（以下「本業務」という。）について、公共サービス改革基本方針に従って、民間競争入札実施要項を定めるものとする。

# 2　JST セキュリティ監視運用業務の詳細な内容及びその実施に当たり確保されるべき質に関する事項

(1) JST セキュリティ監視運用業務の概要

ア　対象となる JST セキュリティ監視運用業務の概要

(ア) JST セキュリティ監視運用業務の経緯と目的

本業務は、当機構の総合的なセキュリティ対策のため、セキュリティ機器、ネットワーク機器、接続回線のセキュリティ監視とセキュリティインシデント対応をおこなうものである。

当機構のネットワーク環境は、ルータ、スイッチングハブ等のネットワーク機器と、IPS、ファイアウォール、WAF 等のセキュリティ機器、及びサーバ類、端末で構成されている。

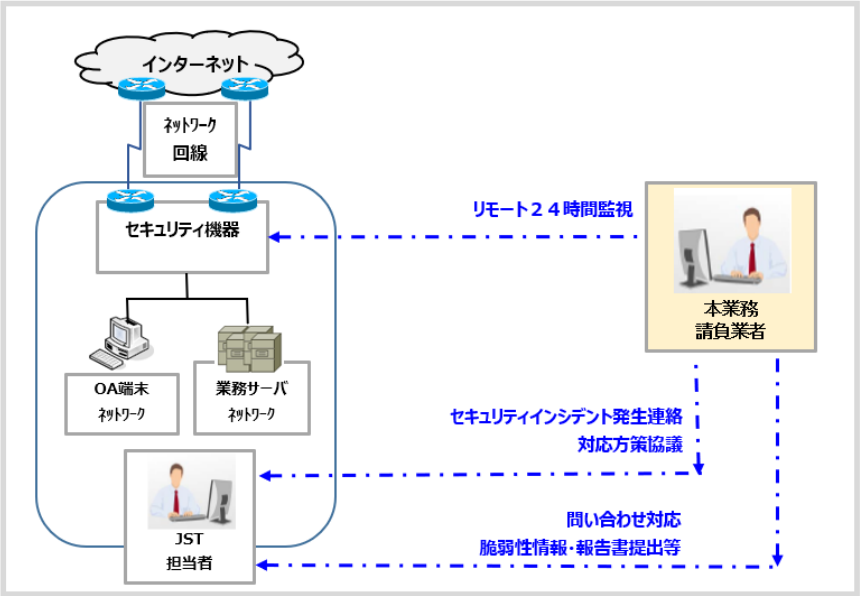
当機構の主な事業はインターネットを通じて情報発信を行っていることから、インターネット接続環境は 24 時間安定稼動する必要がある。

また、当機構の中期目標には「政府の情報セキュリティ対策における方針を踏まえ、適切な情報セキュリティ対策を推進する。」とあり、外部からのサーバへの攻撃や、端末への標的型攻撃など、様々な脅威への対応や、24 時間のセキュリティ機器のログ監視とセキュリティインシデントが発生した際の速やかな対応が求められている。

これらを総合的に解決するため、インターネット接続環境及びセキュリティ機器等の監視を行い、問題が発生した場合の速やかなインシデント対応が可能な環境と体制を整える。

(イ) JST セキュリティ監視運用業務の構成

図 1 に業務概要図を示す。




◆セキュリティ監視
・セキュリティログの監視
・サンドボックスが検出した
マルウェアの分析
・セキュリティインシデント
への対応
・特に重要なインシデント
発生時の現場対応
・ブラックリストIPアドレス
の登録
・脆弱性情報の報告
・脆弱性情報に基づくサーバ
の緊急公開停止

◆報告書等の作成

◆その他
・問い合わせ対応
・月次報告会の開催
等

**図１　業務概要図**

(ウ) JST セキュリティ監視運用業務の対象

当該業務対象機器は、表１(a),(b)の通り。

各機器の機種、ハードウェア構成、設定、ログの取得方法等は、入札前は所定の手続きに沿って申請を行った応札予定者に対し一部をマスクした上で、開札後には秘密保持契約締結後に請負者にマスクしていないものを開示する。

なお、使用しているネットワークプロトコルのアドレスファミリーはIPv4 のみである。

**表１　当該業務対象機器**

**(a) 東京本部**

| 機器名称 | 台数 | 補足 |
|---|---|---|
| IPS 機能付きファイアウォール#1 | 2 台 | 物理的にはアクティブ-スタンバイの 2 台構成だが、論理的にはそれらを 4 つに分割している |
| IPS 機能付きファイアウォール#2 | 2 台 | アクティブ-スタンバイの 2 台構成 |
| WAF | 2 台 | 負荷分散機能を兼ねる。物理的にはアクティブ-スタンバイの 2 台構成だが、論理的にはそれらを 2 つに分割している |
| アンチウイルスソフトウェア管理サーバ | 2 台 | |
| 認証サーバ | 4 台 | |

| | | |
|---|---|---|
| DNS サーバ | 2 台 | 構内ゾーンに対する権威サーバ、それ以外については別の DNS サーバへのフォワーダとして動作している |

### (b) 日本科学未来館

| 機器名称 | 台数 | 補足 |
|---|---|---|
| IPS 機能付きファイアウォール#2 | 2 台 | アクティブ-スタンバイの 2 台構成 |
| 認証サーバ | 2 台 | |
| DNS サーバ | 2 台 | 構内ゾーンに対する権威サーバ、それ以外については別の DNS サーバへのフォワーダとして動作している |

イ　対象業務の内容

請負者が実施する業務の内容は、次のとおりであり、その詳細は、別添 1.「JST セキュリティ監視運用業務仕様書（案）」（以下、「仕様書」という。）を基本とする。

(ア) セキュリティ監視

セキュリティログを受信、分析する業務。

請負者はそれらに関して定期的な報告を行う他、異常が認められた場合には当機構担当者に連絡等を行い、必要に応じてインシデント対応を行う。

(a) セキュリティログの監視

セキュリティ監視機器が出力する全てのログを 24 時間体制で受信し、当機構にとって危険度が高いものを検出すること。

危険度は次のように定義する。

| | |
|---|---|
| 危険度 3 | マルウェアが侵入している、公開サーバのコンテンツ等が書き換わっている、又は何らかの情報が漏えいしており緊急対応が必要である |
| 危険度 2 | 危険度 3 の状態であると確認はできていないが、その可能性が高く、早急な確認が必要である |
| 危険度 1 | 攻撃が成功した可能性は低いが、経過を観察する必要がある |
| 危険度 0 | 問題ない通信とは言い難いが、直ちに対応の必要はない |

請負者はログを世界中から収集した最新の脆弱性情報、マルウェア情報、悪意のある通信先情報、攻撃者情報、攻撃手法情報を統合し、相関的な分析を行うこと。それにより、機器単一のログを調査するだけではわからない侵入、マルウェアへの感染、改ざん、情報の流出等の攻撃を検出すること。分析に用いるルールを日々更新し、可能な限

りゼロデイ攻撃と標的型攻撃も検出すること。ログの上では遮断できている攻撃やマルウェアであっても、それが遮断できなかった攻撃等によって 2 次的に引き起こされた可能性も考慮すること。

危険度 0 ～ 3 までの全ての事象に関して当機構に報告すること。報告には以下の内容を含めること。なお、トラフィックログなど接続・遮断に関する情報のみ記録されるものについては当機構と協議の上で事象毎の報告内容を定めること。

・検出日時
・検出対象
・分析結果
・推奨する対処方法

攻撃の成功又はその可能性が高い事象を検出した場合は、下記「(ｱ)(c)セキュリティインシデントへの対応」を実施すること。

(b) サンドボックスが検出したマルウェアの分析

ファイアウォールのサンドボックス機能がマルウェアとして検出したファイルについて、その判定の妥当性を確認すること。サンドボックス機能が出力したログにマルウェアと判定されたものがあり、かつアンチウイルスソフトにより駆除が行われていない場合は、請負者はサンドボックス機能がファイルの安全性を評価した結果を示した専用の Web サイトを用いて、本当にマルウェアであるかどうかをログ受信後原則 30 分以内に独自に判定すること。それが難しい場合は中間報告を実施すること。

サンドボックス機能の判定の通りマルウェアであると判断した場合は、「(ｱ)(c)セキュリティインシデントへの対応」を行うこと。マルウェアではないと判断し、かつ当機構のドメインの公開サーバ上でそのファイルが見つかった場合、誤検知が発生しないようファイアウォールのメーカーに判定変更を要求する手続きを実施すること。

(c) セキュリティインシデントへの対応

セキュリティインシデントとは、請負者がセキュリティ監視の結果発見した、又は当機構担当者が申告したセキュリティ上の事案のうち、対応を必要とするものを指す。

請負者はセキュリティインシデント発生時には、被害の拡大防止を最優先とすること。

危険度 3 の事態発生時には、請負者は当機構担当者の判断を仰ぐことなく、30 分以内に問題の PC 等又はサーバの通信を遮断する措置をとること。対応実施後は速やかに当機構担当者に連絡し、検出したログの内容、日時、攻撃の種類、確認できている被害、被害 IP アドレスと加害 IP アドレス、推奨する対応等を明確に説明すること。

危険度 2 のインシデントの場合は、その検出後 30 分以内に当機構担当者に連絡し、遮断対応の要否を確認すること。遮断実施の判断になった場合は、その後 30 分以内に前述のものと同様の遮断対応を完

了すること。
なお、当機構担当者が独自に危険度 3 又は 2 の発生を検知し請負者に申告することがある。請負者はそれを受け、当機構担当者が提示する情報を基に遮断が必要と判断された場合は 30 分以内に前述の遮断対応を完了すること。さらに、当機構担当者と協調して攻撃の詳細を調査し、被害の拡大防止のために推奨する対応等を助言すること。

この対応は、月に 2 回を想定している。

(d) 特に重要なインシデント発生時の現場対応
当機構担当者は、特に重要なセキュリティインシデント発生時には請負者に当機構内でのサポートを要請する。請負者はそれに応じ適切なスキルを持った人員 2 名程度を手配して当機構内にてインシデントの調査、被害拡大防止、証拠保全等のサポート業務に従事させること。このサポート業務の開始は平日の日中とするが、状況により夜間及び休日におよぶ可能性がある。
この対応は 1 年で 2 回（1 回あたりの作業工数 64 人/時間）を想定している。

(e) IP アドレスブラックリストの登録
請負者は収集した最新の IP アドレス評価情報を基に、各平日に 1 回通信を遮断すべき IP アドレスリストを更新すること。そのリストが含む IP アドレスとの通信を遮断するよう JST 担当者が指定する機器に設定を行うこと（ただし、 調査の結果、遮断すべき IP アドレスリストに更新が発生しなかった場合は、対象機器への設定は不要)。また、通信遮断設定が行われているが遮断の必要がなくなった IP アドレスについては、精査した上でリストからの削除を行うこと。
請負者は IP アドレスの評価情報を複数の情報源から得て、それらから適切に遮断すべき又は遮断の必要がなくなった IP アドレスのリストを作成すること。当機構担当者から遮断対象の IP アドレス追加の依頼があった場合は、それも遮断対象に含めること。
当機構担当者から IP アドレスの遮断設定削除の依頼があった場合、その IP アドレスの通信先としての危険度を検討し、十分低いと判断した場合はその対応を行うこと。検討した結果に関わらず、その判断の根拠を当機構担当者に説明すること。

(f) 脆弱性情報の報告
当機構担当者が指定する機器やソフトウェアについて広く脆弱性に関する情報を収集し、危険度・緊急度の高い脆弱性については、遅滞なく当機構担当者に報告すること。

(g) 脆弱性情報に基づくサーバの緊急公開停止
請負者は収集している脆弱性情報の中に、当機構担当者が指定する Web サイトに該当するものを発見した場合、その影響度を評価すること。評価の結果が情報漏えいやデータ・コンテンツの改ざん、利用者

の通信内容盗聴などがすぐにでも発生する可能性が高いとなった場合は、当機構担当者の判断を仰ぐことなく、速やかに該当する Web サイトを、ネットワーク機器の設定を変更して公開停止とする対応を実施すること。対応実施後は当機構担当者に連絡し、脆弱性の内容や停止した Web サイトなどを明確に説明すること。緊急性が高くない場合は、当機構担当者に連絡し、公開停止の要否を確認すること。いずれの場合も、該当の脆弱性情報の公表から 1 日以内にこれらの対応を完了させること。

Web サイトが脆弱性の影響を受けるかどうかの判断には、Web サイトが搭載されている各サーバのインストール済みソフトウェアバージョン一覧を得る当機構が導入している仕組みを使った結果も加味すること。

(イ) 報告書等の作成

請負者は下記に定める通り報告書等を納めること。

(a) 計画書

当該業務スケジュール、体制、連絡窓口、会議体等、セキュリティログ監視及び機器の設定手順等を明確に記すこと。体制では責任者を明確にすること。当該業務において有用な資格等を保持している要員については、それを付記すること。再委託を行っている場合はその内容も記載すること。また、作成した計画書、運用手順書、報告書等の作成と更新及び承認等についての文書・記録管理手順と、当機構からの貸与品の管理手順も含めること。契約期間中、計画書は適宜修正すること。

(b) 情報システムセキュリティ管理手順書

請負者の当該業務実施環境について、当機構の情報セキュリティポリシーに従い管理手順書を作成すること。

(c) 日次報告書

当該日のセキュリティ監視に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。

・セキュリティインシデントが発生している場合はその状況

・各セキュリティ監視機器が出力したログの統計情報(全ログ件数、ファイアウォールのポリシーによって遮断した通信の上位 10 位以内、IPS で検知しているイベントの上位 10 位以内、WAF が検知しているイベントの上位 10 位以内)

・サンドボックス機能がマルウェアと判定したファイルがあった場合は、その解説(「(ア)(b) サンドボックスが検出したマルウェアの分析」で行った対応、独自に行った判定の根拠、メーカーへの判定変更手続を行った場合はその状況を含めること)

・アンチウイルスソフトウェアがマルウェアと判定したファイルがあり、注意事項又は何らかの推奨する対応がある場合は、その内容

・特筆すべきログがある場合はその解説(ログの意味、注意を要する理由、推奨する対応を含めること)

(d) 月次報告書

当該月の当該業務に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。

・実施した当該業務の内容とかかった工数
・課題管理表
・サービスレベル報告。「(2)イ サービスレベルの遵守」に定めるサービスレベルと比較し、実績がどうであったかを報告すること。逸脱している項目については改善計画を立案し、その内容を記すこと
・当該月の日次報告書の内容をまとめたもの
・当該月全体でのセキュリティログの統計情報
・当該月のログの傾向や、請負者が収集している様々な情報を総合して分析した結果から導出した当機構全体のセキュリティレベル評価。それが十分なレベルでないならば、その原因と推奨する対策

(e) 改善提案書

当該業務のあらゆる面からコスト削減、効率向上、統制とセキュリティ強化等の改善が可能な点を洗い出し、その改善案を提示すること。改善案には実施した場合の効果と、実施にかかる費用の概算も記すこと。

(ウ) その他

(a) 問い合わせ対応

納品物や当該業務に関すること、及び脆弱性、マルウェア、攻撃者、攻撃手法等のセキュリティに関する当機構担当者からの問い合わせに回答すること。一次回答は1営業日以内に行うこと。

問い合わせは1年に40回程度を想定している。

(b) 停電対応

当該業務の対象機器が設置されている東京本部と日本科学未来館のビルは、例年それぞれ2月と12月に法定電源点検が行われる(実施時期は変わり得る)。これによる停電時に、請負者が持ち込んだ機器に何らかの作業が必要になる可能性がある。その場合は、請負者の負担で適切に対応を行うこと。

(c) ログの調査

当機構担当者からの依頼に基づき、受信しているセキュリティログの調査を行うこと。回答は2営業日以内に行うこと。指定する宛先への通信が、指定する期間に行われていたかどうか、行われていたとしたらいつ、どの送信元からだったかの調査などである。調査対象となるログは6ヶ月前までとする。

この調査依頼は月に2回程度発生を想定している。

(d) 月次報告会

毎月初めから 6 営業日以降 10 営業日以内又は当機構担当者と同意した日に、前月の月次報告書を説明する会を開催すること。9 月と 3 月に開催の報告会では改善提案書についても説明すること。報告会の質疑応答の内容は議事録を作成し、報告会の 3 営業日後までに当機構担当者に送付すること。

ウ　請負業務の引継ぎ

（ア）現行請負者又は当機構からの引継ぎ

当機構は、本業務を受注した請負者への引継ぎが円滑に実施されるよう、現行請負者及び請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者（又は当機構）から業務の引継ぎを受けるものとする。引継ぎ期間は本業務開始日前 4 ヶ月間を想定している。なお、その際の事務引継ぎに必要となる経費のうち、現行請負者に発生した経費は現行請負者の負担、当機構に発生した経費は当機構の負担、請負者に発生した経費は請負者の負担となる。

（イ）請負期間満了の際の引継ぎ

当機構は、本業務の次回請負者への引継ぎが円滑に実施されるよう、本業務を受注した請負者及び次回請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の終了に伴い請負者が変更となる場合には、本業務を受注した請負者は、当該業務の開始日までに、業務内容を明らかにした書類等により、次回請負者に対し、引継ぎを行うものとする。

なお、その際の事務引継ぎに必要となる経費のうち、本業務を受注した請負者に発生した経費は本業務を受注した請負者の負担、当機構に発生した経費は当機構の負担、次回請負者に発生した経費は次回請負者の負担となる。

(2) 確保されるべき対象業務の質

ア　業務内容

2(1)イ～ウに示す業務を適切に実施すること。

イ　サービスレベルの遵守

本業務が目標とするサービスレベルを以下の表 2 に示す。内容の詳細は調達仕様書を参照すること。

請負者はこれらの遵守のため、常に各項目を測定、記録し、サービスレベルが適切な範囲に収まっているかを確認すること。下記の目標値は、天災や大規模停電等による障害及び計画停止の場合は除く。

**表 2　サービスレベル**

| 項目 | 目標値 | 内容 |
|---|---|---|

| | | |
|---|---|---|
| 納品物の納期遵守 | 100%納期遵守 | 納品物の納期遵守率 |
| セキュリティログ受信損失 | 0.01%以下 | 請負者による分析が行われずに失われたセキュリティログの時間の割合。月に 5 分以内のログ損失 |
| 当機構担当者からのセキュリティインシデント発生の申告を受けてからの初動対応 | 30 分以内 | 当機構担当者からのセキュリティインシデント発生の連絡受付後に、遮断対応を完了するまでの時間 |
| サンドボックスが検出したマルウェアの判断時間 | 30 分以内 | サンドボックスのマルウェア検出のログを受信してから独自の判断を完了するまでの時間 |
| 危険度 3 のセキュリティインシデント発生時の初動対応 | 30 分以内 | 危険度 3 のセキュリティインシデント発生時に、その検知から通信遮断対応を完了するまでの時間 |
| 危険度 2 のセキュリティインシデント発生時の初動対応 | それぞれ 30 分以内 | 危険度 2 のセキュリティインシデント発生時に、その検知から JST 担当者に連絡を行うまでの時間、及び遮断対応実施の判断からその実施完了までの時間 |
| セキュリティログ保存損失 | 少なくとも 6 ヶ月分の損失 0% | 保存しているセキュリティログの損失 |
| 脆弱性情報に基づくサーバの緊急公開停止 | 1 日以内 | 脆弱性情報公表後からサーバの緊急公開停止を実施し当機構担当者に連絡するまで、又は当機構担当者に連絡し指示のあった対応を実施完了するまでの時間 |

ウ　サービスレベルアグリーメントの締結

運用支援の効率化、品質向上及び円滑化を図るため、上記イに示すサービスレベルに対して別添 4 のサービスレベルアグリーメント（案）（以下「SLA」という。）を締結すること。

(3) 創意工夫の発揮可能性

本業務を実施するに当たっては、以下の観点から請負者の創意工夫を反映し、公共サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。

ア　セキュリティ監視運用業務の実施全般に対する提案

請負者は、当該業務のあらゆる面からコスト削減、効率向上、統制/セキュリティ強化等の改善が可能な点を洗い出し、その改善案を改善提案書として半期毎に提出すること。改善案には実施した場合の効果と、実施にかかる費用の概算も記すこと。

(4) 契約の形態及び支払

ア　契約の形態は、業務請負契約とする。

イ　当機構は、業務請負契約に基づき、請負者が実施する本業務について、契約の履行に関し、仕様書に定めた内容に基づく監督・検査を実施するなどして適正に実施されていることを確認した上で、適正な支払請求書を受領した日から起算して翌月末までに、契約金額を支払うものとする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、又は達成できないおそれがある場合、当機構は、確保されるべき対象業務の質の達成に必要な限りで、請負者に対して本業務の実施方法の改善を行うよう指示することができる。請負者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を速やかに当機構に提出するものとする。業務改善報告書の提出から１ヶ月の範囲で、業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、当機構は、請負費の支払いを行わないことができる。なお、請負費は、本件業務開始以降のサービス提供に対して行われるものであり、請負者が行う準備行為等に対して、請負者に発生した費用は、請負者の負担とする。

(5) 法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、アからウに該当する場合には当機構が負担し、それ以外の法令変更については請負者が負担する。

ア　本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設

イ　消費税その他類似の税制度の新設・変更（税率の変更含む）

ウ　上記ア及びイのほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

## ３　実施期間に関する事項

業務請負契約の契約期間は、令和元年 11 月 29 日から令和 5 年 3 月 31 日までとする。

## ４　入札参加資格に関する事項

(1) 法第 15 条において準用する法第 10 条各号（第 11 号を除く。）に該当する者でないこと。

(2) 予算決算及び会計令（昭和 22 年勅令第 165 号）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、特別な理由がある場合に該当する。

(3) 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。

(4) 平成 31・32・33 年度又は令和 01・02・03 年度当機構競争参加資格または全省庁統一資格の「役務の提供等」Ａ及びＢ等級に格付され競争参加資格を

有する者であること。

(5) 会社更生法（平成 14 年法律第 154 号）に基づき更生手続開始の申立てがなされている者又は民事再生法（平成 11 年法律第 225 号）に基づき民事再生手続開始の申立てがなされている者については、手続開始の決定後に一般競争参加資格の再認定を受けていること。

(6) 当機構からの取引停止、及び各府省庁等における物品等の契約に係る指名停止措置要領に基づく指名停止を受けている期間中の者でないこと。

(7) 法人税並びに消費税及び地方税の滞納がないこと。

(8) 労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

(9) 調査研究や各工程の調達仕様書の作成に直接関与した事業者及びその関連事業者（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社、同一の親会社をもつ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）でないこと。

(10) 調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行う CIO 等の属する又は過去 2 年間に属していた事業者でないこと。または、CIO 等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が 2 年に満たない場合に限る。）でないこと。

(11) 単独で対象業務を行えない場合は、又は、単独で実施するより業務上の優位性があると判断する場合は、適正に業務を実施できる入札参加グループを結成し、入札に参加することができる。その場合、入札書類提出時までに入札参加グループを結成し、入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。また、入札参加グループの構成員は、上記(1)から(3)及び(5)から(10)までの資格を満たす必要があり、他の入札参加グループの構成員となり、又は、単独で参加することはできない。さらに、入札参加グループの構成員は、セキュリティ監視の体制（人員、設備等）を有する者が下記（13）の資格を、セキュリティ監視機器を導入する者が（14）の資格を、セキュリティ監視要員を手配する者が（17）及び（18）の資格を、最新のセキュリティ関連情報を収集する者が（19）の資格を、それぞれ満たす必要がある。なお、入札参加グループの代表者及び構成員は、入札参加グループの結成に関する協定書（又はこれに類する書類）を作成し、提出すること。

（注）入札参加グループとは

本業務の実施を目的に複数の事業者が組織体を構成し、本業務の入札に参加する者のことを指す。

(12) 別に定める入札説明書に記載の提出期限までに提案書等を提出した者であること。

(13) 契約期間中 24 時間常時複数名によるセキュリティ監視が可能な体制（人員、設備等）があること。監視要員の人数、保有資格、業務経験、交代スケジ

ュールは適切であること。

(14) 本業務で取り扱うセキュリティ監視機器又は同等の製品について、そのログを監視する業務の受注実績があること。

(15) ISO9001 に準拠、又は同等の品質管理を実施していること。同等の品質管理とは、品質管理方針、品質管理体制を制定し、文書管理、記録の管理などについて、文書化した手順により実行していること及び内部監査を実施していることをいう。

(16) ISO/IEC27001 又は JIS Q 27001 に準拠、又は同等の情報セキュリティ管理を実施していること。同等の情報セキュリティ管理とは、情報セキュリティ方針、情報セキュリティ管理体制を制定し、リスクアセスメント、リスクアセスメントに基づく管理策、内部監査、教育を実施していることをいう。

(17) セキュリティ監視を行う要員には、セキュリティの専門家を含んでいること。専門家であるとは、下記の資格のいずれかを有することを指す。

・情報処理安全確保支援士

・CISSP(Certified Information Systems Security Professional)

・GIAC(Global Information Assurance Certification)

(18) 当該業務を請け負う部門には、下記のいずれかの資格を持つ者、または本業務と類似した業務実施経験を 3 年以上有する者が在籍しており、本業務の実施体制に含んでいること。

・PMI(Project Management Institute)認定 PMP(Project Management Professional)

・情報処理推進機構認定プロジェクトマネージャ

・Expert Certificate in IT Service Management (ITIL Expert)

(19) 常に最新のセキュリティ関連情報を世界中から収集していること。収集した情報を当該業務で活用できる体制を確立していること。

## ５　入札に参加する者の募集に関する事項

(1) スケジュール

| | |
|---|---|
| 入札公示：官報公示 | 令和元年８月下旬 |
| 入札説明会（2 回実施予定） | ８月下旬 |
| 質問受付期限 | ９月上旬 |
| 資料閲覧期限 | ９月下旬 |
| 提案書提出期限 | 10 月中旬 |
| 提案書の審査 | 10 月下旬頃 |
| 入札書提出期限 | 10 月下旬頃 |
| 開札及び落札予定者の決定 | 11 月上旬頃 |
| 契約締結 | 11 月下旬頃 |

（なお、現在の運用計画書・手順書等については、民間競争入札に参加する予定の者から要望があった場合、別に定める入札説明書に記載された手続きを踏まえた上で入札時に閲覧可能である。）

(2) 入札書類

入札参加者は、次に掲げる書類を別に定める入札説明書に記載された期日及び方法により提出すること。

ア　入札説明後の質問受付

入札公告以降、当機構において入札説明書の交付を受けた者（当機構ホームページから入札説明書をダウンロードした者を含む）は、本実施要項の内容や入札に係る事項について、入札説明会後に、当機構に対して質問を行うことができる。質問は原則として電子メールにより行い、質問内容及び当機構からの回答は原則として別に定める入札説明書に記載された URL から閲覧できるウェブサイトに掲載することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ　入札参加希望届出書

本入札に参加を希望する者は、別に定める入札説明書に記載された期限までに入札参加希望届出書を FAX により提出すること。原本送付は不要。

※ 本届出書未提出の者であっても入札に参加することは可能だが、各種連絡事項の通知は本届出書を提出した者に対してのみ行う場合があるので留意のこと。

ウ　提案書等

別添２　「JST セキュリティ監視運用業務 提案書作成要領（案）」に示した各要求項目について具体的な提案（創意工夫を含む。）を行い、各要求項目を満たすことができることを証明する書類

エ　参考見積書

形式は指定しない。但し、一式表記は不可とする。項目毎に単価×数量等を示すこと。

オ　定価証明書
　参考見積書積算において定価の設定がある項目については、人件費単価証明書、製品定価証明書、料金表等価格の確認できる資料を提出すること。なお、製品単価証明書等に記載する標準価格等は、カタログ標準価格（当該標準価格等がカタログ標準価格以外のものである場合は、当該標準価格等をカタログ標準価格として設定するとした場合にカタログ標準価格に含まれるものを含む。以下「カタログ標準価格等」という。）に限定されるものとし、当該製品の設置等に係る費用のうち、通常カタログ標準価格等に含まれない費用は含まないものとする。

カ　入札書
　入札金額（入札参加者が消費税及び地方消費税に係る課税事業者であるか免税事業者であるかを問わず、契約期間内の全ての請負業務に対する報酬の総額の 110 分の 100 に相当する金額）を記載した書類

キ　委任状
　代理人に委任したことを証明する書類
　ただし、代理人による入札を行う場合に限る。

ク　競争参加資格審査結果通知書の写し
　平成 31・32・33 年度又は令和 01・02・03 年度当機構競争参加資格または全省庁統一資格の「役務の提供等」Ａ及びＢ等級に格付けされた競争参加資格を有する者であることを証明する審査結果通知書の写し

ケ　法第 15 条において準用する法第 10 条に規定する欠格事由のうち、暴力団排除に関する規程について評価するために必要な書類

コ　法人税並びに消費税及び地方消費税の納税証明書（直近のもの）
　４(8)に該当する場合、社会保険料納入確認書等（直近のもの）

サ　主たる事業概要、従業員数、事業所の所在地、代表者略歴、主要株主構成、他の者との間で競争の導入による公共サービス改革に関する法律施行令（平成 18 年 7 月 5 日政令第 228 号）第 3 条に規定する特定支配関係にある場合は、その者に関する当該情報

シ　入札参加グループによる参加の場合は、入札参加グループ内部の役割分担について定めた協定書又はこれに類する書類

ス　指名停止等に関する申出書
　各府省庁等から指名停止を受けていないことを確認する書類

セ　誓約書
　本請負を完了できることを証明する書類

## ６　JST セキュリティ監視運用業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す。なお、詳細は別添 3「JST セキュリティ監視運用業務 総合評価基準書（案）（以下「総合評価基

準書」という。)」を基本とする。

(1) 評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。なお、技術の評価に当たっては、入札プロセスの中立性、公正性等を確保するため、当機構の CIO に意見を聴くものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（総合評価基準書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

価格点と技術点の配分

価格点の配分：技術点の配分　＝　1：1

| 総合評価点　＝　価格点（840 点満点）＋ 技術点（840 点満点） |
|---|

(2) 合否決定方法

提出された提案書に記載された内容が、別添 3「総合評価基準書」の評価項目において必須項目と定められた要求要件を全て満たしている場合に「合格」とし、一つでも欠ける場合は「不合格」とする。

(3) 総合評価点

ア　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。

| 価格点　＝　（1－入札価格÷予定価格）×　840 点 |
|---|

イ　技術点の評価は以下のとおりとする。

(ア) 全ての仕様を満たし、「合格」したものに「基礎点」として 210 点与える。

(イ) 「合格」した提案書について、総合評価基準書に基づき、総合評価委員会の委員ごとに加点部分の評価を行う。各委員の評価結果を委員会で確認し、事実誤認等があれば各委員において訂正する。なお、各委員が行う加点部分の評価は、以下の評価基準及び得点に基づき点数化する。確定した各委員の採点結果の平均値（小数点以下切り捨て）を算出し、「加点」とする。

評価基準及び得点

| 評価 | 評価基準 | 得点 |
|---|---|---|
| S | 実績の場合は、A 評価を満たし、かつ、記載された根拠が本業務の効果的・効率的な実施に資すると判断できるものであること。<br>提案の場合は、A 評価を満たし、かつ、その実効性、有効性が優れておりその根拠が客観的に示されていること。 | 配点×１．０ |
| A | 実績の場合は、B 評価を満たし、かつ、それが | 配点×０．７ |

| | | |
|---|---|---|
| | 本業務の効果的・効率的な実施に資する根拠が記載されていること。<br>提案の場合は、B 評価を満たし、かつ、その手順や方法等がより具体的（実効性、有効性等の根拠を含む）であること。 | |
| B | 評価の観点に示した内容が記載されている。 | 配点×０．３ |
| C | 評価の観点に示した内容が記載されていない。 | 配点×０ |

(ウ) 「基礎点」と「加点」の合計点を「技術点」とする。

| 技術点　＝　基礎点（210 点）　＋　加点（630 点満点） |
|---|

(4) 落札者の決定

ア　総合評価基準書に示す全ての要求要件を満たし、入札者の入札価格が国立研究開発法人科学技術振興機構調達契約及び前渡資金の取扱事務細則第 9 条の規定に基づき、当機構が作成した予定価格の制限の範囲内であり、かつ、「総合評価落札方法」によって得られた数値の最も高い者を落札者とする。ただし、落札者となるべき者の入札価格が予定価格に１０分の６を乗じて得た額に満たない場合は、入札の結果を保留する。この場合、入札参加者は当機構の行う事情聴取等の調査に協力しなければならない。

イ　調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

（会計法第 29 条の６第１項ただし書き抜粋）
相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるとき

ウ　落札者となるべき者が２人以上あるときは、抽選で落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わって抽選を行い、落札者を決定するものとする。

エ　契約担当者等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記イにより落札者を決定する場合には別に書面で通知する。なお、当機構では総合評価方式（加算方式）において、総合評価点の内訳は公表していないため予め了承のこと。

(5) 落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当者等が、正当な理由があると認めたときはこの限りでない。

ア　落札者が、契約担当者等から求められたにもかかわらず契約書の取り交わしを行わない場合

イ　入札書の金額と入札金額内訳書の金額が符合しない場合
　落札後、入札者に入札金額内訳書を記載させる場合がある。入札金額内訳金額が入札金額と符合しないときは、入札した金額で入札したものとみなすため、入札内訳金額の補正を求められた入札者は、直ちに入札書の金額に基づいてこれを補正しなければならない。

(6) 落札者が決定しなかった場合の措置
　初回の開札で予定価格の制限の範囲内で入札した者がいないときは、直ちに再度の入札を行うものとする。なお、初度の入札に参加しなかった者及び初度の入札が無効となった者は、再度入札に参加できないものとし、入札を辞退した者及び無効入札者は退席するものとする。初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行ってもなお落札者が決定しなかった場合は、原則として、入札条件等を見直した後、再度公告を行う。
　なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、自ら実施する等とし、その理由を官民競争入札等監理委員会（以下、「監理委員会」という。）に報告するとともに公表するものとする。

## ７　JST セキュリティ監視運用業務に関する従来の実施状況に関する情報の開示に関する事項

(1) 開示情報
　対象業務に関して、以下の情報は別紙 1 「従来の実施状況に関する情報の開示」のとおり開示する。

ア　従来の実施に要した経費

イ　従来の実施に要した人員

ウ　従来の実施に要した施設及び設備

エ　従来の実施における目標の達成の程度

オ　従来の実施方法等

(2) 資料の閲覧
　前項イ、ウ、エ、オの詳細な情報は、民間競争入札に参加する予定の者から要望があった場合、所定の手続を踏まえた上で入札時に閲覧可能とする。

　また、民間競争入札に参加する予定の者から追加の資料の開示について要望があった場合は、当機構は法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

## ８　JST セキュリティ監視運用業務の請負業者に使用させることがで

## きる当機構の施設・設備等に関する事項

(1) 当機構の施設・設備等の使用

請負者は、当機構と協議し承認された本業務の遂行に必要な当機構の施設、設備等を適切な管理の下、無償で使用することができる。

(2) 使用制限

ア　請負者は、本業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　請負者は、あらかじめ当機構と協議した上で、当機構の業務に支障を来さない範囲内において、施設内に運用管理業務の実施に必要な設備等を持ち込むことができる。

ウ　請負者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ　請負者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、請負者の責任と負担において速やかに復旧するものとする。

## ９　JST セキュリティ監視運用業務請負者が、当機構に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の本業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項

(1) 本業務請負者が当機構に報告すべき事項、当機構の指示により講じるべき措置

ア　報告等

(ア) 請負者は、調達仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を当機構に提出しなければならない。

(イ) 請負者は、請負業務を実施したとき、又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに当機構に報告するものとし、当機構と請負者が協議するものとする。

(ウ) 請負者は、契約期間中において、(イ)以外であっても、必要に応じて当機構から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

(ア) 当機構は、請負業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第 26 条第 1 項に基づき、請負者に対し必要な報告を求め、又は当機構の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(イ) 立入検査をする当機構の職員は、検査等を行う際には、当該検査が法第 26 条第 1 項に基づくものであることを請負者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

当機構は、請負業務の適正かつ確実な実施を確保するために必要と認めるときは、請負者に対し、必要な措置を採るべきことを指示することができる。

(2) 秘密を適正に取り扱うために必要な措置

ア　請負者は、本業務の実施に際して知り得た当機構の情報等（公知の事実等を除く）を、第三者に漏らし、盗用し、又は請負業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第 54 条により罰則の適用がある。

イ　請負者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負者からの文書による申出を当機構が認めた場合に限り、第三者へ開示できるものとする。

ウ　請負者は、当機構から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成 15 年法律第 57 号）、独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針（平成 16 年 9 月 14 日総管情第 85 号総務省行政管理局長通知）、当機構の個人情報保護規則等に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　請負者は、以下の情報セキュリティ管理事項を遵守すること。

(ア) 当機構の「情報セキュリティポリシー(情報セキュリティ規程及び関連例規、情報セキュリティ手引書、情報システムセキュリティ管理手順書(ガイドライン))」「JST システム運用・保守管理ガイドライン」に準拠し、当該業務を実施すること。これらの資料は、入札時に入札説明書記載の方法に従い申し込むことによって応札を希望する事業者に開示する。

(イ) 当機構の情報セキュリティポリシーに則り、当該業務にかかる「情報システムセキュリティ管理手順書」を作成して、適宜修正・更新を行うこと

(ウ) 情報データの管理台帳を作成し、情報データのライフサイクルをトレースすること。

(エ) セキュリティ管理責任者を設定し、責任・権限を明確化すること。

オ　アからエまでのほか、当機構は、請負者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

(3) 契約に基づき請負者が講じるべき措置

ア　請負業務開始

請負者は、セキュリティ監視業務の開始日（令和２年４月１日）から確実に業務を開始すること。

イ　権利の譲渡

請負者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による当機構の事前の承認を得たときは、この限りではない。

ウ　権利義務の帰属等

(ア)本業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、請負者は、その責任において、必要な措置を講じなくてはならない。

(イ)請負者は、本業務の実施状況を公表しようとするときは、あらかじめ、当機構の承認を受けなければならない。

エ　瑕疵担保責任

(ア) 当機構は、成果物の引渡し後に発見された瑕疵について、引渡し後１年間は、請負者に補修を請求できるものとし、補修に必要な費用は、全て請負者の負担とする。

(イ) 成果物の瑕疵が請負者の責に帰すべき事由によるものである場合は、当機構は、前項の請求に際し、これによって生じた損害の賠償を併せて請求することができる。

オ　再委託

(ア) 請負者は、本業務の実施に当たり、その全部を一括して再委託してはならない。

(イ) 請負者は、本業務の実施に当たり、その一部について再委託を行う場合には、原則として、あらかじめ提案書において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。

(ウ) 請負者は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先等を明らかにした上で、事前に書面により当機構の承認を受けなければならない。

(エ) 請負者は、(イ)又は(ウ)により再委託を行う場合には、請負者が当機構に対して負う義務を適切に履行するため、再委託先の事業者に対し前項「(2)秘密を適正に取り扱うために必要な措置」及び本項「(3)契約に基づき請負者が講じるべき措置」に規定する事項その他の事項について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取することとする。

(オ)(イ)から(エ)までに基づき、請負者が再委託先の事業者に業務を実施させる場合は、全て請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、請負者の責に帰すべき事由とみなして、請負者が責任を負うものとする。

カ　契約内容の変更

当機構及び請負者は、本業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第 21 条の規定に基づく手続を適切に行わなければならない。

キ　機器設定変更等の際における民間事業者への措置

実施期間中、以下のことがあり得る。これらの変更があったとしても、請負者はサービスレベルを落とすこと無く継続的に当該業務を遂行すること。ただしそれらにより請負者の設備や体制等に増強等が必要である場合は、当機構と請負者が協議して契約を変更することができる。

(ア) 当該業務対象機器の設定変更、機能の追加あるいは削除、ソフトウェアのバージョン変更、機種の変更、何らかの原因によりログが著しく増大したとき

(イ) 機器の追加/撤去を含むネットワーク構成の物理的/論理的な変更が生じるとき

(ウ) セキュリティ対策の強化等により業務内容に変更が生じたとき

(エ) 当機構の組織変更や人員増減に伴う利用者数の変動等により業務量に著しい変動が生じたとき

ク　契約の解除

当機構は、請負者が次のいずれかに該当するときは、請負者に対し請負費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、請負者は当機構に対して、契約金額から消費税及び地方消費税を差し引いた金額の 100 分の 10 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、当機構の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負者は、当機構との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

(ア) 法第 22 条第 1 項イからチまで又は同項第 2 号に該当するとき。

(イ) 暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。

(ウ) 暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。

(エ) 再委託先が、暴力団若しくは暴力団員により実質的に経営を支配され

る事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。

(オ) 再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

ケ　談合等不正行為

請負者は、談合等の不正行為に関して、当機構が定める「談合等の不正行為に関する契約一般条項」に従うものとする。

コ　損害賠償

請負者は、本業務の実施に当たり請負者の故意又は過失により当機構に損害を与えたときは、当機構に対し、その損害について賠償する責任を負う。ただし、当該損害が当機構の責に帰すべき事由による場合はこの限りではない。また、当機構は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。なお、当機構から請負者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

サ　不可抗力免責・危険負担

民間事業者は、上記事項にかかわらず、不可抗力により請負事業の全部若しくは一部の履行が遅延又は不能となった場合は当該責任を負わないものとする。

当機構及び請負者の責に帰すことのできない事由により契約期間中に物件が滅失し、又は毀損し、その結果、当機構が物件を使用することができなくなったときは、請負者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

シ　金品等の授受の禁止

請負者は、本業務の実施において、金品等を受け取ること、又は、与えることをしてはならない。

ス　宣伝行為の禁止

請負者及び本業務に従事する者は、本業務の実施に当たっては、自ら行う業務の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

セ　法令の遵守

請負者は、本業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

ソ　安全衛生

請負者は、本業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

タ　記録及び帳簿類の保管

請負者は、本業務に関して作成した記録及び帳簿類を、本業務を終了し、又は中止した日の属する年度の翌年度から起算して５年間、保管しなければならない。

チ　契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、当機構と請負者との間で協議して解決する。

## 10　JST セキュリティ監視運用業務請負者が本業務を実施するに当たり第三者に損害を加えた場合において、その損害の賠償に関し契約により本業務請負者が負うべき責任に関する事項

本業務を実施するに当たり、請負者又はその職員その他の本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

(1) 当機構が国家賠償法第１条第１項等の規定に基づき当該第三者に対する賠償を行ったときは、当機構は請負者に対し、当該第三者に支払った損害賠償額（当該損害の発生について当機構の責めに帰すべき理由が存する場合は、当機構が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

(2) 請負者が民法（明治 29 年法律第 89 号）第 709 条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について当機構の責めに帰すべき理由が存するときは、請負者は当機構に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

## 11　JST セキュリティ監視運用業務に係る法第７条第８項に規定する評価に関する事項

(1) 本業務の実施状況に関する調査の時期

当機構は、本業務の実施状況について、総務大臣が行う評価の時期（令和3年12月を予定）を踏まえ、本業務開始後、毎年12月に状況を調査する。

(2) 調査項目及び実施方法

表２に示したサービスレベルの各項目について、請負者から提出される月次報告書及び請負者が開催する月次報告会により調査を行う。

(3) 意見聴取等

当機構は、必要に応じ、本業務請負者から意見の聴取を行うことができるものとする。

(4) 実施状況等の提出時期

当機構は、令和4年2月を目途として、本業務の実施状況等を総務大臣及び監理委員会へ提出する。

なお、調査報告を内閣総理大臣及び監理委員会に提出するに当たり、CIO 補佐官及び外部有識者の意見を聴くものとする。

## 12　その他業務の実施に関し必要な事項

(1) JSTセキュリティ監視運用業務の実施状況等の監理委員会への報告

当機構は、法第26条及び第27条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

(2) 当機構の監督体制

本契約に係る監督は、主管部署自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督責任者は以下のとおり。

業務に係る監督責任者：情報基盤事業部長

契約に係る監督責任者：契約部長

(3) 本業務請負者の責務

ア　本業務に従事する請負者は、刑法（明治40年法律第45号）その他の罰則の適用については、法令により公務に従事する職員とみなされる。

イ　請負者は、法第54 条の規定に該当する場合は、１年以下の懲役又は50万円以下の罰金に処される。

ウ　請負者は、法第55条の規定に該当する場合は、30万円以下の罰金に処されることとなる。なお、法第56条により。法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第55条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

エ　請負者は、会計検査院法（昭和22年法律第73号）第23条第１項第７号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第25条及び第26条により、同院の実地の検査を受けたり、同院から直接又は当機構に通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

(4) 著作権

ア　請負者は、本業務の目的として作成される成果物に関し、著作権法第27条及び第28条を含む著作権の全てを当機構に無償で譲渡するものとする。

イ　請負者は、成果物に関する著作者人格権（著作権法第18条から第20条までに規定された権利をいう。）を行使しないものとする。ただし、当機構が承認した場合は、この限りではない。

ウ　ア及びイに関わらず、成果物に請負者が既に著作権を保有しているもの（以下「請負者著作物」という。）が組み込まれている場合は、当該請負者著作物の著作権についてのみ、請負者に帰属する。

エ　提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負者が当該著作物の使用に必要な費用の負担及び使用許諾契約等

に係る一切の手続きを行うものとする。

(5) JSTセキュリティ監視運用業務の仕様書

本業務を実施する際に必要な仕様は、仕様書に示すとおりである。

別紙１

# 従来の実施状況に関する情報の開示（案）

## １　従来の実施に要した経費

（単位：千円）

| | | | 平成28年度（4月～3月） | 平成29年度（4月～3月） | 平成30年度（4月～3月） |
|---|---|---|---|---|---|
| | 人件費 | 常勤職員 | ー | ー | ー |
| | | 非常勤職員 | ー | ー | ー |
| | 物件費 | | ー | ー | ー |
| | 請負費等 | 役務 | 84,700 | 127,100 | 127,100 |
| | | 機器・回線等料 | ー | ー | ー |
| | | その他 | ー | ー | ー |
| 計(a) | | | 84,700 | 127,100 | 127,100 |
| 参考値(b) | 減価償却費 | | ー | ー | ー |
| | 退職給付費用 | | ー | ー | ー |
| | 間接部門費 | | ー | ー | ー |
| (a)＋(b) | | | 84,700 | 127,100 | 127,100 |

（注記事項）
国立研究開発法人科学技術振興機構（以下、「当機構」という。）では、民間競争入札の対象であるJSTセキュリティ運用監視業務（以下、「当該業務」という）を請負契約により実施している。
平成28年度は、平成28年 4月から平成29年3月までの契約額(税抜)である。
平成29年度は、平成29年 4月から平成30年3月までの契約額(税抜)である。
平成30年度は、平成30年 4月から平成31年3月までの契約額(税抜)である。

## ２ 従来の実施に要した人員

（単位：人）

| | 平成28年度（4月～3月） | 平成29年度（4月～3月） | 平成30年度（4月～3月） |
|---|---|---|---|
| （請負者における当該業務従事者） | | | |
| 当機構のセキュリティ対応状況に関連する情報のため非公開。民間競争入札に参加する予定の者から要望があった場合、入札公告時に入札説明書記載の方法に従い申し込むことによって閲覧可能。 | | | |

（業務従事者に求められる知識・経験等）

当該業務を実施する組織・部門には、下記のいずれかの資格を持つ者が在籍しており、体制に含まれているか又は組織・部門として資格を取得していること。
- PMI(Project Management Institute)認定PMP(Project Management Professional)
- 情報処理推進機構認定プロジェクトマネージャ
- ITIL Foundation Certificate in IT Service Management

セキュリティ監視を行う要員には下記の資格のいずれかを有する者が含まれていること。
- GCIA(GCIA Certified Intrusion Analyst)
- CISSP(Certified Information Systems Security Professional)

（平成28年度）

| 作業項目 | 回数時間(h) | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 計 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 監視 | | | | | | | | | | | | | | |
| 機器の死活監視 | 回数 | 12 | 9 | 11 | 14 | 11 | 12 | 12 | 4 | 4 | 4 | 6 | 4 | 103 |
| | 時間 | 0.2 | 0.2 | 0.2 | 0.2 | 0.2 | 0.2 | 0.2 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 1.9 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 機器の性能監視 | 回数 | 4 | 5 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 52 |
| | 時間 | 4 | 5 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 52 |
| 機器の異常監視 | 回数 | 294 | 220 | 261 | 355 | 247 | 253 | 262 | 249 | 210 | 166 | 258 | 290 | 3065 |
| | 時間 | 6.7 | 6.2 | 6.4 | 7.3 | 6.4 | 6.4 | 6.5 | 6.3 | 6.1 | 5.7 | 6.2 | 6.8 | 77 |
| 障害対応 | 回数 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 3 |
| | 時間 | 8 | 0 | 0 | 0 | 0 | 0 | 8.5 | 0 | 0 | 0 | 0 | 0.5 | 17 |
| セキュリティ監視 | | | | | | | | | | | | | | |
| セキュリティログの監視 | 回数 | 236 | 226 | 225 | 180 | 216 | 195 | 293 | 214 | 310 | 161 | 212 | 647 | 3115 |
| | 時間 | 224 | 214 | 219 | 175 | 203 | 193 | 290 | 212 | 397 | 182 | 232 | 628 | 3169 |
| サンドボックスが検出したマルウェアの分析 | 回数 | 2 | 1 | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 3 | 2 | 1 | 20 |
| | 時間 | 6 | 3 | 9 | 3 | 3 | 6 | 6 | 3 | 3 | 9 | 6 | 3 | 60 |
| セキュリティインシデントへの対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 特に重要なインシデントへの駆けつけ | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 20 | 20 |
| 運用 | | | | | | | | | | | | | | |
| 機器の設定変更 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 機器のソフトウェアアップデート | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 定期ログ確認 | 回数 | 30 | 31 | 30 | 31 | 31 | 30 | 31 | 30 | 31 | 31 | 28 | 31 | 365 |
| | 時間 | 45 | 46.5 | 45 | 46.5 | 46.5 | 45 | 46.5 | 45 | 46.5 | 46.5 | 42 | 46.5 | 548 |
| ブラックリストIPアドレスの登録 | 回数 | 5 | 7 | 8 | 5 | 4 | 6 | 4 | 4 | 4 | 4 | 4 | 5 | 60 |
| | 時間 | 7.5 | 10.8 | 9.5 | 8.3 | 4.8 | 4.7 | 4.3 | 9.7 | 3.6 | 6.2 | 6.5 | 7.6 | 83.5 |
| IPSのシグネチャアップデート | 回数 | 2 | 3 | 3 | 6 | 5 | 4 | 4 | 3 | 2 | 4 | 2 | 4 | 42 |
| | 時間 | 10 | 4.2 | 4.4 | 8 | 6.4 | 4.3 | 4.1 | 4.9 | 2.1 | 6.6 | 3.1 | 5.1 | 63.2 |
| 脆弱性情報の報告 | 回数 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 52 |
| | 時間 | 12 | 12 | 15 | 12 | 15 | 12 | 12 | 15 | 12 | 12 | 12 | 15 | 156 |
| 納品物の作成 | | | | | | | | | | | | | | |
| 計画書 | 回数 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 4 | 9 |
| | 時間 | 1 | 0 | 0.5 | 0 | 0 | 1 | 0 | 2 | 0 | 0 | 3 | 4 | 11.5 |
| 情報システムセキュリティ管理手順書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 運用手順書 | 回数 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 4 |
| | 時間 | 20 | 20 | 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 62 |
| 日次報告書 | 回数 | 20 | 19 | 22 | 20 | 22 | 20 | 20 | 20 | 19 | 19 | 20 | 22 | 243 |
| | 時間 | 60 | 60 | 60 | 60 | 60 | 60 | 60 | 60 | 57 | 57 | 60 | 66 | 720 |
| 月次報告書 | 回数 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |
| | 時間 | 85 | 73 | 78 | 72 | 73 | 73 | 71 | 71 | 72 | 72 | 72 | 72 | 884 |
| 改善提案書 | 回数 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 2 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 14 | 0 | 0 | 0 | 0 | 0 | 14 | 28 |
| 年次報告書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 3 |
| その他 | | | | | | | | | | | | | | |
| 問合せ対応 | 回数 | 7 | 6 | 3 | 7 | 4 | 2 | 5 | 4 | 2 | 2 | 4 | 6 | 52 |
| | 時間 | 21.5 | 20 | 7 | 12.2 | 6 | 2 | 18.5 | 5.5 | 9 | 8 | 7 | 6 | 123 |
| 停電対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2.3 | 0 | 2.3 |
| ログの調査 | 回数 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 2 | 5 | 11 |
| | 時間 | 15 | 15 | 0 | 4 | 0 | 0 | 6 | 0 | 0 | 0 | 4 | 7.5 | 51.5 |
| 月次報告会 | 回数 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 11 |
| | 時間 | 0 | 6 | 6 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 65 |

（平成29年度）

| 作業項目 | 回数<br>時間(h) | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 計 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 監視 | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 機器の死活監視 | 回数 | 4 | 5 | 4 | 6 | 7 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 54 |
| | 時間 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 1.2 |
| 機器の性能監視 | 回数 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 52 |
| | 時間 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 52 |
| 機器の異常監視 | 回数 | 217 | 281 | 280 | 255 | 186 | 110 | 85 | 62 | 31 | 31 | 63 | 60 | 1661 |
| | 時間 | 6.1 | 6.7 | 6.6 | 6.5 | 5.8 | 5.2 | 5 | 4.8 | 4.6 | 4.6 | 36 | 4.8 | 96.7 |
| 障害対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 0 | 0 | 0 | 0 | 0.8 |
| セキュリティ監視 | | | | | | | | | | | | | | |
| セキュリティログの監視 | 回数 | 156 | 251 | 1076 | 1049 | 501 | 394 | 577 | 330 | 577 | 683 | 784 | 804 | 7182 |
| | 時間 | 160 | 297 | 950 | 932 | 416 | 334 | 531 | 345 | 531 | 702 | 816 | 864 | 6878 |
| サンドボックスが検出したマルウェアの分析 | 回数 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 5 |
| | 時間 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 4 | 4 | 0 | 0 | 20 |
| セキュリティインシデントへの対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 2 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 8 | 18 | 0 | 0 | 26 |
| 特に重要なインシデントへの駆けつけ | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 2 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 16 | 8 | 0 | 0 | 24 |
| 運用 | | | | | | | | | | | | | | |
| 機器の設定変更 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 機器のソフトウェアアップデート | 回数 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| | 時間 | 0 | 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 25 |
| 定期ログ確認 | 回数 | 30 | 31 | 30 | 31 | 31 | 30 | 31 | 30 | 31 | 31 | 28 | 31 | 365 |
| | 時間 | 45 | 46.5 | 45 | 45 | 45 | 45 | 46.5 | 45 | 46.5 | 46.5 | 42 | 46.5 | 545 |
| ブラックリストIPアドレスの登録 | 回数 | 16 | 20 | 22 | 20 | 22 | 20 | 21 | 20 | 20 | 19 | 20 | 22 | 242 |
| | 時間 | 17.9 | 29.2 | 32.4 | 22.5 | 20.2 | 17.1 | 23 | 22.5 | 16.2 | 25.3 | 21.2 | 23.7 | 271 |
| IPSのシグネチャアップデート | 回数 | 4 | 7 | 4 | 5 | 5 | 5 | 7 | 4 | 2 | 5 | 3 | 2 | 53 |
| | 時間 | 5.9 | 12 | 6.3 | 5.2 | 4.5 | 4.9 | 6.1 | 5.4 | 2.4 | 6.5 | 4.6 | 2.5 | 66.3 |
| 脆弱性情報の報告 | 回数 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 49 |
| | 時間 | 12 | 15 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 147 |
| 納品物の作成 | | | | | | | | | | | | | | |
| 計画書 | 回数 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 6 |
| | 時間 | 2 | 0 | 0 | 0 | 2 | 2 | 2 | 3 | 0 | 2 | 0 | 0 | 13 |
| 情報システムセキュリティ管理手順書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 運用手順書 | 回数 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| | 時間 | 0 | 3 | 25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 28 |
| 日次報告書 | 回数 | 20 | 20 | 22 | 19 | 22 | 20 | 20 | 20 | 20 | 20 | 19 | 21 | 243 |
| | 時間 | 60 | 60 | 66 | 57 | 66 | 60 | 60 | 60 | 60 | 60 | 57 | 63 | 729 |
| 月次報告書 | 回数 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |
| | 時間 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 72 | 864 |
| 改善提案書 | 回数 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 1 | 3 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 24 | 28 |
| 年次報告書 | 回数 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 2 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 4 | 7 |
| その他 | | | | | | | | | | | | | | |
| 問合せ対応 | 回数 | 1 | 3 | 4 | 6 | 4 | 3 | 3 | 6 | 4 | 3 | 1 | 6 | 44 |
| | 時間 | 2 | 6 | 6 | 9 | 10 | 3.3 | 6.5 | 7.6 | 19 | 2.5 | 0.5 | 12.5 | 84.9 |
| 停電対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.7 | 0 | 0.7 |
| ログの調査 | 回数 | 1 | 2 | 0 | 3 | 2 | 1 | 2 | 4 | 3 | 1 | 1 | 4 | 24 |
| | 時間 | 2 | 3 | 0 | 6 | 6 | 1.5 | 4.5 | 5.5 | 17 | 6 | 0.5 | 11.5 | 63.5 |
| 月次報告会 | 回数 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |
| | 時間 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 72 |

（平成30年度）

| 作業項目 | 回数<br>時間(h) | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 | 計 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **監視** | | | | | | | | | | | | | | |
| 機器の死活監視 | 回数 | 4 | 4 | 4 | 4 | 62 | 4 | 4 | 4 | 5 | 5 | 8 | 15 | 123 |
| | 時間 | 0.1 | 0.1 | 0.1 | 0.1 | 0.6 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.2 | 1.8 |
| 機器の性能監視 | 回数 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 4 | 52 |
| | 時間 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 4 | 52 |
| 機器の異常監視 | 回数 | 71 | 63 | 92 | 61 | 152 | 30 | 36 | 52 | 33 | 41 | 54 | 67 | 752 |
| | 時間 | 4.5 | 4.8 | 4.7 | 4.8 | 5.5 | 4.2 | 4.5 | 4.4 | 4.3 | 4.4 | 4.1 | 4.6 | 54.8 |
| 障害対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **セキュリティ監視** | | | | | | | | | | | | | | |
| セキュリティログの監視 | 回数 | 380 | 667 | 495 | 174 | 346 | 394 | 608 | 456 | 403 | 512 | 504 | 456 | 5395 |
| | 時間 | 405 | 691 | 511 | 241 | 423 | 334 | 631 | 443 | 554 | 611 | 618 | 434 | 5896 |
| サンドボックスが検出したマルウェアの分析 | 回数 | 0 | 2 | 0 | 0 | 1 | 0 | 6 | 2 | 1 | 2 | 2 | 2 | 18 |
| | 時間 | 0 | 8 | 0 | 0 | 4 | 0 | 23 | 4 | 0.4 | 1 | 2.5 | 3.2 | 46.1 |
| セキュリティインシデントへの対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 特に重要なインシデントへの駆けつけ | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **運用** | | | | | | | | | | | | | | |
| 機器の設定変更 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 機器のソフトウェアアップデート | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 定期ログ確認 | 回数 | 30 | 31 | 30 | 31 | 31 | 30 | 31 | 30 | 31 | 31 | 28 | 31 | 365 |
| | 時間 | 45 | 46.5 | 45 | 46.5 | 46.5 | 45 | 46.5 | 45 | 46.5 | 46.5 | 42 | 31 | 532 |
| ブラックリストIPアドレスの登録 | 回数 | 20 | 21 | 21 | 19 | 17 | 17 | 22 | 12 | 8 | 7 | 9 | 10 | 183 |
| | 時間 | 22 | 28.7 | 18.6 | 14.5 | 11.8 | 12.3 | 16 | 17.6 | 17.2 | 15.9 | 16.2 | 19.4 | 210 |
| IPSのシグネチャアップデート | 回数 | 4 | 3 | 3 | 3 | 3 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 32 |
| | 時間 | 4.7 | 3 | 4.1 | 3.3 | 3.3 | 2 | 2.6 | 1.5 | 3.3 | 3.1 | 2 | 1.7 | 34.6 |
| 脆弱性情報の報告 | 回数 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 4 | 4 | 1 | 41 |
| | 時間 | 12 | 12 | 12 | 12 | 12 | 12 | 2 | 12 | 11.6 | 12 | 12 | 2 | 124 |
| **納品物の作成** | | | | | | | | | | | | | | |
| 計画書 | 回数 | 0 | 2 | 0 | 1 | 0 | 2 | 2 | 1 | 1 | 0 | 2 | 2 | 13 |
| | 時間 | 0 | 3 | 0 | 2 | 0 | 3 | 5 | 2 | 2 | 0 | 4 | 4 | 25 |
| 情報システムセキュリティ管理手順書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 運用手順書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 日次報告書 | 回数 | 20 | 19 | 21 | 21 | 23 | 18 | 22 | 20 | 19 | 19 | 19 | 20 | 241 |
| | 時間 | 60 | 57 | 63 | 63 | 69 | 54 | 69 | 64 | 68.1 | 71.2 | 58 | 60 | 756 |
| 月次報告書 | 回数 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |
| | 時間 | 72 | 72 | 72 | 72 | 72 | 72 | 82 | 79 | 82 | 77 | 71 | 87 | 910 |
| 改善提案書 | 回数 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 2 | 3 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 18 | 0 | 0 | 0 | 0 | 0 | 12 | 30 |
| 年次報告書 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 5 |
| **その他** | | | | | | | | | | | | | | |
| 問合せ対応 | 回数 | 2 | 3 | 3 | 2 | 4 | 1 | 2 | 8 | 3 | 4 | 5 | 6 | 43 |
| | 時間 | 2 | 2.5 | 5.7 | 2 | 10.5 | 2 | 8.7 | 29.7 | 16.2 | 30 | 18 | 28.2 | 156 |
| 停電対応 | 回数 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 時間 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ログの調査 | 回数 | 2 | 2 | 2 | 2 | 4 | 3 | 2 | 4 | 2 | 1 | 1 | 2 | 27 |
| | 時間 | 2 | 2 | 5.5 | 2 | 10.5 | 6.5 | 5 | 15 | 3 | 13.2 | 2 | 7 | 73.7 |
| 月次報告会 | 回数 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 12 |
| | 時間 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 72 |

（注記事項）

## 3 従来の実施に要した施設及び設備

当機構
【施設】
施設名称：当機構内
使用場所：当該業務対象機器の設置場所（オンサイト作業時のみ）

【設備】
当機構貸与
当該業務対象機器の設置場所に入るためのカード

請負者が用意するもの
【施設】
当該業務実施場所（当該業務はリモート作業である）

【設備】
監視機器、セキュリティログを収集・分析する機器、運用対象機器を操作する機器、請負者と当機構との間の
接続回線・接続機器（請負者と当機構側の両端）、当該業務に使用するソフトウェア・ツール等。

外部拠点
外部拠点に設置されているセキュリティ機器に関する情報を含むネットワーク構成図は、入札公告時に入札説明書
記載の方法に従い申し込むことによって応札を希望する事業者に開示する。

## 4 従来の実施における目的の達成の程度

| | 平成28年度（4月～3月） | | 平成29年度（4月～3月） | | 平成30年度（4月～3月） | |
|---|---|---|---|---|---|---|
| | 目標・計画 | 実績 | 目標・計画 | 実績 | 目標・計画 | 実績 |
| 納品物の納期厳守 | 100%納期遵守 | 82.1% | 100%納期遵守 | 92% | 100%納期遵守 | 100% |
| 監視パケット損失 | 0.01%以下 | 0% | 0.01%以下 | 0% | 0.01%以下 | 0% |
| セキュリティログ受信損失 | 0.01%以下 | 0% | 0.01%以下 | 0% | 0.01%以下 | 0% |
| セキュリティインシデント通知時間 | 30分以内 | 対象事案なし | 30分以内 | 対象事案なし | 30分以内 | 対象事案なし |
| サンドボックスが検出したマルウェアの確認時間 | 30分以内 | すべて30分以内で対応 | 30分以内 | すべて30分以内で対応 | 30分以内 | 対象事案なし |
| セキュリティインシデント発生時の初動時間 | 30分以内 | 対象事案なし | 30分以内 | すべて30分以内で対応 | 30分以内 | 対象事案なし |
| 機器の設定変更依頼から開始までの時間 | 3時間以内 | すべて3時間以内で対応 | 3時間以内 | 対象事案なし | 3時間以内 | 対象事案なし |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 機器のソフトウェアアップデート依頼から開始までの時間 | 3時間以内 | 対象事案なし | 3時間以内 | 25時間かかった事案が1件 | 3時間以内 | 対象事案なし |
| IPSのシグネチャリリースからアップデート開始までの時間 | 1営業日以内 | すべて1営業日以内で対応 | 1営業日以内 | すべて1営業日以内で対応 | 1営業日以内 | すべて1営業日以内で対応 |
| セキュリティログ保存損失 | 少なくとも6ヶ月分を損失0% | 0% | 少なくとも6ヶ月分を損失0% | 0% | 少なくとも6ヶ月分を損失0% | 0% |
| （注記事項） | | | | | | |

## 5 従来の実施方法等

| |
|---|
| 従来の実施方法（業務フロー図等）<br><br>実施要項「2.(1)ウ 対象業務の内容」に示すとおり。より詳細に記載された運用手順書は、民間競争入札に参加する予定の者から要望があった場合、入札公告時に入札説明書記載の方法に従い申し込むことによって閲覧可能。 |
| （注記事項） |

別添 1

# JST セキュリティ監視運用業務
# 仕様書（案）

令和元年 6 月
国立研究開発法人科学技術振興機構

# 目次

# 1　発注要件

## (1) 発注内容

### ア　案件名

JST セキュリティ監視運用業務

Monitoring, Managing and Operating Security Devices

### イ　発注概要

本件は国立研究開発法人科学技術振興機構の総合的なセキュリティ対策のため、セキュリティ機器やサーバ機器、関連ソフトウェアが生成するログを監視し、セキュリティインシデント発生の際にはその対応を行う業務を調達するものである。

### ウ　用語定義

JST

国立研究開発法人科学技術振興機構の略称。

当該業務

本仕様書に定める業務。

JST 担当者

当該業務に関する JST 側の担当者。

請負者

本件を受注した業者。再委託を行っている場合は再委託先も含む。

セキュリティログ

JST のセキュリティ機器が出力するログ。「2(3)ア①　セキュリティログの監視」に列挙しているログ。

セキュリティ監視業務

当該業務のうち、セキュリティログを受信、分析する業務。請負者はそれらに関して定期的な報告を行う他、異常を認めた場合には JST 担当者に連絡等を行い、必要に応じてインシデント対応を行う。

平日

日本の祝日及び年末年始(12 月 29 日から 1 月 3 日まで)を除く月曜日から金曜日。

営業日

営業日は平日を数えるものとする。例:金曜日の翌営業日は月曜日。

セキュリティインシデント

請負者がセキュリティ監視の結果発見した、又は JST 担当者が申告したセキュリティ上の事案のうち、対応を必要とするもの。詳細は後述する。

## (2) 発注条件

### ア　契約期間

契約期間は契約締結日(令和元年 11 月 29 日見込み)から令和 5 年 3 月 31 日までとする。

なお、引継ぎ等の準備は令和 2 年 3 月 31 日までとし 、セキュリティ監視業務は令和 2 年 4 月 1 日から令和 5 年 3 月 31 日まで とする。

請負者は契約期間開始から遅滞なく本書で定めるサービスレベルで当該業務ができるよう体制と環境を構築すること。

### イ　選定条件

請負者は次の要件をすべて満たすこと。

① 請負者は契約期間中 24 時間常時複数名によるセキュリティ監視が可能な体制(人員、設備等)があること。監視要員の人数、保有資格、業務経験、交代スケジュールは適切であること。

② 請負者はセキュリティ監視機器又は同等の製品について、そのログを監視する業務の受注実績があること。

③ 請負者は ISO9001 に準拠又は同等の品質管理体制を実施していること。同等の品質管理体制とは、品質管理方針、品質管理体制を制定し、文書管理、記録の管理などについて、文書化した手順により実行していること及び内部監査を実施していることを言う。

④ 請負者は ISO/IEC27001 又は JIS Q 27001 に準拠した管理若しくは同等の情報セキュリティ管理を実施していること。同等の情報セキュリティ管理を実施しているとは、情報セキュリティ方針、情報セキュリティ管理体制を制定し、リスクアセスメント、リスクアセスメントに基づく管理策、内部監査、教育を実施していることを言う。

⑤ 請負者のセキュリティ監視を行う要員には、セキュリティの専門家を含んでいること。専門家であるとは、下記の資格のいずれかを有することを指す。

- 情報処理安全確保支援士

- CISSP(Certified Information Systems Security Professional)
- GIAC(Global Information Assurance Certification)

⑥ 請負者の当該業務を請け負う部門には、下記のいずれかの資格を持つ者、または本業務と類似した業務実施経験を 3 年以上有する者が在籍しており、本業務の実施体制に含んでいること。

- PMI(Project Management Institute)認定 PMP(Project Management Professional)
- 情報処理推進機構認定プロジェクトマネージャ
- Expert Certificate in IT Service Management (ITIL Expert)

⑦ 請負者は常に最新のセキュリティ関連情報を世界中から収集していること。収集した情報を当該業務で活用できる体制を確立していること。

## ウ　言語

請負者は JST 担当者への連絡を日本語で行うこと。納品物の報告書等も日本語で作成すること。ただし、システム的に生成する日次の報告書等は英語でもよい。その場合であっても、請負者は JST 担当者からの求めがあれば、その内容について日本語で解説すること。

## エ　業務実施場所

当該業務はリモート作業とする。請負者が当該業務を行う場所は、原則として請負者の負担で用意すること。ただし、必要に応じ JST 内での作業はあり得る。JST のサーバ室へ入室する際には、入退室記録等の手順に従うこと。

当該業務対象機器の設置場所は下記の通り。会議等の開催場所は、原則として東京本部とする。

［東京本部］

〒102-8666 東京都千代田区四番町 5-3

国立研究開発法人科学技術振興機構 東京本部

［日本科学未来館］

〒135-0064 東京都江東区青海 2-3-6

日本科学未来館

### オ　貸与品

JST 担当者は請負者に必要に応じ次のものを貸与する。請負者は貸与品の管理責任者を定め、紛失や破損のないよう留意すること。万一、紛失等が発生した場合は、速やかに JST 担当者に報告し、指示に従うこと。第三者への貸与は禁ずる。

契約満了時又は不要になった場合は速やかに返却すること。電子データはすべて消去すること。

- 当該業務対象機器の設置場所に入館するためのカード
- 当該業務対象機器に関する設計書等の資料、設定情報及びログデータのサンプル等
- 情報セキュリティ規程及び関連規則
- 情報システムセキュリティ管理手順書(「2(3)イ② 情報システムセキュリティ管理手順書」)

### カ　開示資料

本件に関する開示資料は、入札前は所定の手続に沿って申請を行った応札予定者に対し一部をマスクした上で、開札後には秘密保持契約締結後にマスクしていないものを請負者に開示する。資料は「4 開示資料一覧」に列挙している。

### キ　当該業務環境・ツール等

当該業務に使用する請負者側の環境(監視機器、セキュリティログを収集・分析する機器、請負者と JST との間の接続回線・接続機器(請負者側と JST 側の両端)、当該業務に使用するソフトウェア及びツール等)は、請負者の負担で用意すること。セキュリティログは少なくとも 6 ヶ月前にさかのぼって調査が可能なように、JST にあるものとは別に請負者の環境にも保存すること。なお、「2(2)ウ JST 内への機器設置」にあるように、必要であれば JST 内への機器の設置は可能である。前述の JST のものとは別にとしているセキュリティログの保存は、その機器で行ってもよい。

これらの準備にかかる費用は、月額費用とは分けて初期費用として計上すること。

### (3) 当該業務条件

#### ア　工数・課題管理

請負者は計画書等に従い確実に当該業務を実施し、その実績を定量的に記録すること。記録を行う作業単位は、工数と実績を評価する上で適切であること。可能であれば、作業件数とその稼働時間の両方を記録すること。請負者はこの記録に基づき、必要であれば要員の増員、配置の変更等を適切に計画すること。

当該業務遂行中に発生した課題については課題管理表を作成し、課題の内容、発生日、完了日、対応者、対応結果等を記録すること。業務遂行に支障をきたす重大な課題、懸念等が発生した場合は、速やかに JST 担当者に報告すること。

なお、2017 年 10 月から契約中の「JST セキュリティ監視運用業務」において、その請負者が報告した業務内容と作業工数は、開示資料として閲覧できる。

#### イ　連絡体制

請負者は 24 時間 365 日当該業務を実施するための体制を整えること。JST 担当者からのインシデント発生の申告、問い合わせ等を受け付ける連絡窓口を設けること。

請負者がインシデント発生時等に連絡する JST 担当者の連絡先は、受注後に開示する。連絡先は優先度を付けた複数の電話番号とメールアドレスの一覧である。連絡が必要となった場合は、請負者はその一覧に従い連絡を実施すること。電話での場合は、連絡が取れるまで一覧中の電話番号に少なくとも 2 巡は連絡を試みること。電話での連絡ができたかどうかにかかわらず、一覧中のすべてのメールアドレスに必要な情報を送信すること。

#### ウ　変更への対応

すべての当該業務の対象となる機器で、契約期間中に設定の変更、機能の追加あるいは削除、ソフトウェアのバージョン変更、機種の変更、何らかの原因によるログの増大又は機器の追加、撤去を含むネットワーク構成の物理的、論理的な変更等(なお、これらの変更作業は当該業務の範囲内ではない。)があり得る。これらの変更があったとしても、請負者はサービスレベルを落とすことなく継続的に当該業務を遂行すること。それらにより請負者の設備や体制等に増強等が必要となる場合は、JST 担当者と協議すること。

### (4) 納品・検収要件

#### ア　納品物

請負者は下記に定める報告書等を所定の期日までに納品すること。

納品形態を電子データとしているものは、基本的には指定する宛先への電子メールでの送付とするが、JST 担当者が認めた場合は、請負者が用意した Web サイトへの掲載としてもよい。Web サイトによる納品の場合は、JST 担当者以外が閲覧することができないよう、適切な認証、暗号化の仕組みを盛り込むこと。その仕組みの妥当性について、事前に JST 担当者の了承を得ること。

電子データとして納める電子ファイルは、内容の変更が可能な形式にすること。電子データは納品時点における最新のパターンファイルを実装したアンチウイルスソフトウェアによるチェック実施後に納品すること。

① 受注時、随時納品物

| 項番 | 納品物 | 納品形態 | 部数 |
|---|---|---|---|
| 1 | 計画書 | 電子データ、書類 | 各 1 |
| 2 | 情報システムセキュリティ管理手順書 | 電子データ、書類 | 各 1 |

② 日次納品物

| 項番 | 納品物 | 納品形態 | 部数 |
|---|---|---|---|
| 1 | 日次報告書 | 電子データ | 1 |

③ 月次納品物

| 項番 | 納品物 | 納品形態 | 部数 |
|---|---|---|---|
| 1 | 月次報告書 | 電子データ | 1 |

④ 半期納品物

| 項番 | 納品物 | 納品形態 | 部数 |
|---|---|---|---|
| 1 | 改善提案書 | 電子データ、書類 | 各 1 |

**イ　納品日**

請負者は各納品物を次に指定する期日までに納めること。

① 受注時、随時納品物

受注日の翌営業日から起算して 10 営業日以内とする。ただし、契約期間中に変更があった場合は、更新版を随時納め、JST 担当者の承認を得ること。

② 日次納品物

日本時間で当該日の翌日午前中までとする。ただし、請負者が希望すれば、送付は平日のみでも可とする。その場合は、本来休日に送付するべきだった分（金曜、土曜、日曜、祝日の分）は、直後の営業日の午前中に送付すること。

③ 月次納品物

日本時間で当該月の翌月の 10 営業日までとする。

④ 半期納品物

9 月末と 3 月末までとする。

**ウ　納入場所・担当者**

請負者は納品物を次の住所に納品すること。電子データ送付先の電子メールアドレスは、受注後に開示する。

〒102-8666 東京都千代田区四番町 5-3

国立研究開発法人科学技術振興機構 情報基盤事業部

**エ　検収**

検収は JST 担当者が次のすべてを確認、承認することにより完了とする。

① 計画した当該業務をすべて実施し、実績報告をしていること。

② 報告書の形式及び内容が正しいこと。

③ すべての納品物が指定の媒体、数量、形式となっていること。

④ すべての納品物の記載内容及び情報が妥当であること。

なお、JST 担当者が納品物の内容について修正、追加を依頼した場合は、速やかに対応し再納品すること。

**(5) その他の前提条件**

**ア　再委託**

請負者は本業務のすべてを一括して再委託してはならない。一部を再委託する場合は、原則として、あらかじめ提案書に再委託先に委託する業務の範囲、再委託を行うことの合理性と必要性及び再委託先の履行能力並びに報告徴収、個人情報の管理

及びその他運営管理の方法(以下「再委託先等」という。)について記載しなければならない。

契約締結後にやむを得ない事情により再委託を行う場合には、請負者は再委託先等を明らかにした上で、事前に JST の承認を得なければならない。

再委託においては、JST に対して負う義務を適切に履行するため、請負者は再委託先の事業者に対し必要な措置を講じさせるとともに、再委託先から必要な報告を徴収することとする。また、再委託先の事業者が行う業務はすべて請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由は、請負者の責に帰すべき事由とみなして、請負者が責任を負うものとする。

### イ　要員の準備

当該業務開始時から円滑に業務を実施するよう、請負者の各要員は当該業務に必要な知識と技術の習得、運用手順書の熟知に努めること。

### ウ　要員の交代

請負者側の都合により要員交代の必要がある場合は、JST に対して事前に通知するとともに、充分な業務引継ぎを行い、滞りなく業務を遂行すること。また、計画書に記載している体制を修正すること。

### エ　引継ぎ

当該業務の契約満了時、別契約の請負者との間で業務の引継ぎを行う必要がある場合は、本契約の請負者は新規業者が円滑に当該業務を開始できるよう最大限協力すること。JST は円滑な引継ぎのために現行請負者及び請負者に対して必要な措置を講ずるとともに、適切に引継ぎが行われているかを監督し、その完了を確認する。

本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者又は JST から業務の引継ぎを受けるものとする。引継ぎ期間は本業務開始日前の 4 ヶ月を想定している。

本業務の終了に伴い請負者が変更となる場合には、請負者は当該業務の開始日までに業務内容を明らかにした書類等により、次回請負者に対し引継ぎを行うこと

いずれの場合でも、引継ぎに必要となる経費は、現行請負者に発生した経費は現行請負者の負担、JST に発生した経費は JST の負担、引継ぎを受ける請負者に発生した経費は引継ぎを受ける請負者の負担とする。

当該業務で JST のために作成した相関分析の分析ルール等は、可能な限り新規業者に引継ぐこと。ただし、請負者が事業継続上特に秘匿したい情報は除外してよい。

# 2　当該業務要件

## (1) 当該業務概要

### ア　本案件の目的

JST のネットワーク環境は、様々なネットワーク機器とセキュリティ機器、サーバ類、端末及びそれらにインストールしたソフトウェアが構成している。当該業務に関するネットワークの概要図は開示資料に含めている。

中長期計画において JST は「ICT を適切に活用し業務の効率化を推進する」としている。昨今のインターネットを活用した情報発信、情報収集は、業務に多大な効率化の恩恵を与えたが、悪意を持つ者にとってもそれは同様である。そのような者はインターネット上のあらゆるところから任意の時間に攻撃を試みることができ、その手法は様々な者が随時開発、公開している。ひとたび悪意を持つ者にネットワーク環境への侵入を許せば、それは JST が保有する国民の財産である様々な情報資産を重大な脅威にさらすことになる。そのような場合に備え、同じく中長期計画で「情報システムに対するサイバー攻撃への防御力、攻撃に対する組織的対応能力の強化に取り組む」とも掲げている。本件は JST ネットワーク環境のセキュリティ監視を行い、攻撃等発生時の速やかなインシデント対応が可能なシステムと体制を整え、組織的対応能力の強化を行うものである。

### イ　セキュリティログ監視対象

請負者が当該業務でセキュリティログ監視を行う対象とする機器を「表 1 セキュリティログ監視対象（東京本部）」と「表 2 セキュリティログ監視対象（日本科学未来館）」に示す。表に記載の通り、対象機器は大きく東京本部所属のものと日本科学未来館所属のものに分かれている。請負者はそれぞれのログを適切に収集できるよう収集用機器や回線を設計、構築すること。それぞれの機器のログを請負者の環境に送付するための設定作業等は、JST 担当者が行う。

各機器の機種、ハードウェア構成、設定、監視対象となるログのサンプルとその 1 日当たりのサイズ、ログの取得方法等は開示資料に記す。

なお、使用しているネットワークプロトコルのアドレスファミリーは IPv4 のみである。

**表 1 セキュリティログ監視対象（東京本部）**

| 機器名称 | 台数 | 補足 |
|---|---|---|
| IPS 機能付きファイアウォール#1 | 2 台 | 物理的にはアクティブ-スタンバイの 2 台構成だが、論理的にはそれらを 4 つに分割している |
| IPS 機能付きファイアウォール#2 | 2 台 | アクティブ-スタンバイの 2 台構成 |

| | | |
|---|---|---|
| WAF | 2 台 | 負荷分散機能を兼ねる。物理的にはアクティブ-スタンバイの 2 台構成だが、論理的にはそれらを 2 つに分割している |
| アンチウイルスソフトウェア管理サーバ | 2 台 | |
| 認証サーバ | 4 台 | |
| DNS サーバ | 2 台 | 構内ゾーンに対する権威サーバ、それ以外については別の DNS サーバへのフォワーダとして動作している |

表 2 セキュリティログ監視対象(日本科学未来館)

| 機器名称 | 台数 | 補足 |
|---|---|---|
| IPS 機能付きファイアウォール | 2 台 | アクティブ-スタンバイの 2 台構成 |
| 認証サーバ | 2 台 | |
| DNS サーバ | 2 台 | 館内ゾーンに対する権威サーバ、それ以外については別の DNS サーバへのフォワーダとして動作している |

(2) 当該業務環境

ア　当該業務環境における条件

請負者の当該業務環境は「3(1) サービスレベル」に定めるサービスレベルを保証できる構成とすること。

請負者の環境が、JST 以外の受注先業務の環境を共有する場合は、JST 用の機器と JST 以外用の機器は物理的又は論理的に分離し、JST と他組織との間で請負者を介した通信、情報の移動ができないようにすること。適切にファイアウォールやアンチウイルスゲートウェイなどを設置し、セキュリティを確保すること。なお、セキュリティログ監視に用いる機器がインターネットと通信することは、ソフトウェアやデータのアップデート又は当該業務に直接関連する場合を除いて禁ずる。

請負者は自らの当該業務環境の詳細について、事前に JST 担当者の承認を得ること。

イ　回線

請負者は自身の負担で当該業務に用いる環境と JST を接続する回線を用意すること。回線は東京本部及び日本科学未来館のそれぞれに敷設すること。

回線は 24 時間の監視が可能なもので、当該業務実施に十分な帯域を有すること。「3(1)サービスレベル」に定めるサービスレベルを達成するよう複数回線の敷設、回線切断時の自動切替えの仕組み導入などの方策をとること。なお、サービスレベル及びセキュリティを維持しているのであれば、インターネット VPN を用いてもよい。

JST との接続回線は JST 以外への通信に用いてはならない。やむを得ず他用途と共用する場合は論理的に分離し、JST との間で行われるべき通信が他の回線へ漏えいすること及び JST 向け回線に不要な通信が入り込むことを防止する対策を施すこと。

インターネット VPN を用いる場合は、適切なアクセス制御、認証、暗号化を設定すること。通信には、あらかじめ JST 担当者が許可した固定 IP アドレスを用いること。インターネット VPN として用いる回線を、VPN 確立のためではないインターネット宛ての通信に用いることは禁ずる。

請負者は利用する回線について、その種別、サービスレベル/セキュリティの担保に関する施策をあらかじめ JST 担当者に開示し承認を得ること。

### ウ　JST 内への機器設置

JST 内へ請負者の機器を設置する必要がある場合は、その用途を明確にし、JST 担当者の承認を得た上で行うこと。機器には所有者を明示すること。JST 担当者がその機器にセキュリティ対策が必要と判断した場合は、適切な対策を施し、その内容について承認を得ること。

## (3) 当該業務内容

請負者は次の業務を実施すること。

各業務で JST 担当者への連絡を実施した場合は、その日時と連絡した内容を記録すること。その記録を月次報告書に記載すること。

### ア　セキュリティ監視業務

① セキュリティログの監視

請負者はセキュリティ監視機器が出力するすべてのログを常に受信し、JST にとっての危険度が高いものを検出すること。危険度は次のように定義する。

| | |
|---|---|
| 危険度 3 | マルウェアが侵入している、公開サーバのコンテンツ等が書き換わっている、又は何らかの情報が漏えいしており緊急対応が必要である |
| 危険度 2 | 危険度 3 の状態であると確認はできていないが、その可能性が高く、早急な確認が必要である |
| 危険度 1 | 攻撃が成功した可能性は低いが、経過を観察する必要がある |
| 危険度 0 | 問題ない通信とは言い難いが、直ちに対応の必要はない |

すべてのログとは、東京本部設置機器については以下のすべてである。

- IPS 機能付きファイアウォール#1 と IPS 機能付きファイアウォール#2 が出力する検知した IPS イベントのログ
- IPS 機能付きファイアウォール#1 と IPS 機能付きファイアウォール#2 が出力する通過した、又は遮断した通信のログ
- IPS 機能付きファイアウォール#2 が出力するアンチウイルス機能、URL フィルタ機能、サンドボックス機能が検知したイベントのログ
- WAF が出力する Web サーバへの接続ログ及び遮断した通信のログ
- アンチウイルスソフトウェア管理サーバが出力する検知したマルウェアのログ
- 認証サーバが出力する認証の成否等に関するログ
- DNS サーバが出力する DNS 問い合わせの内容に関するログ

日本科学未来館設置機器については次である。

- IPS 機能付きファイアウォールが出力する検知した IPS イベントのログ
- IPS 機能付きファイアウォールが出力する通過した、又は遮断した通信のログ
- IPS 機能付きファイアウォールが出力するアンチウイルス機能、URL フィルタ機能、サンドボックス機能が検知したイベントのログ
- アンチウイルスソフトウェア管理サーバが出力する検知したマルウェアのログ
- 認証サーバが出力する認証の成否等に関するログ
- DNS サーバが出力する DNS 問い合わせの内容に関するログ

いずれでもすべてのログを監視の対象とすること。部分的としてはならない。これらのログを少なくとも次の観点ではリアルタイムに分析し、危険度に応じた対応を行うこと。

- 各ファイアウォールが出力するログの中に、悪意があるホストとの通信がないか
- 各ファイアウォールや IPS 機能が出力するログに、攻撃キャンペーン（攻撃者が侵入・潜伏しようする一連の活動）との関連性が高いものがないか
- 各ファイアウォールや IPS 機能が出力するログで、特定の通信先に関するものが急増していないか

- サンドボックス機能がマルウェアと判定したファイルがないか(「2(3)ア② サンドボックスが検出したマルウェアの分析」)
- アンチウイルスソフトウェア、URL フィルタ、サンドボックス機能などが検出しているファイルの中に、攻撃キャンペーンで使用しているものがないか
- 認証サーバに対する認証要求が急増していないか。特権アカウントの認証失敗が多数ないか
- DNS サーバに対する悪意があるホストの名前解決要求や、DNS トンネリングのようなプロトコルの正常な振る舞いを装った通信が発生していないか

請負者はログを世界中から収集した最新の脆弱性情報、マルウェア情報、悪意のある通信先情報、攻撃者情報、攻撃手法情報と統合し、相関的な分析を行うこと。それにより、機器単一のログを調査するだけではわからない侵入、マルウェアへの感染、改ざん、情報の流出等の攻撃を検出すること。分析に用いるルールを随時更新し、可能な限りゼロデイ攻撃と標的型攻撃も検出すること。ログの上では遮断できている攻撃やマルウェアであっても、それが遮断できなかった攻撃等が 2 次的に引き起こした可能性も考慮すること。

危険度0～3までの全ての事象に関して JST に報告すること。報告には以下の内容を含めること。なお、トラフィックログなど接続・遮断に関する情報のみ記録されるものについては JST と協議の上で事象毎の報告内容を定めること。

- 検出日時
- 検出対象
- 分析結果
- 推奨する対処方法

危険度 3 又は危険度 2 のログを検出した場合は、「2(3)ア③ セキュリティインシデントへの対応」を行うこと。

② サンドボックスが検出したマルウェアの分析

サンドボックス機能がファイルを評価した結果は、専用の Web サイトでその詳細を確認できる。サンドボックス機能が出力したログにファイルをマルウェアと判定するものがあり、かつアンチウイルスソフトにより駆除が行われていない場合は、請負者はその Web サイトを用いて、本当にマルウェアであるかどうかをログ受信後原則 30 分以内に独自に判定すること。それが難しい場合は中間報告を実施すること。なお、そのサイトではファイル自体のダウンロードも可能であるため、必要であれば

ダウンロードを実施してよい。ただし、そのファイルを請負者の外に送ることは禁ずる。Web サイトの URL とログインに必要な情報は、受注後に開示する。

サンドボックス機能の判定の通りマルウェアであると判断した場合は、危険度 3 として「2(3)ア③セキュリティインシデントへの対応」を行うこと。マルウェアではないと判断したファイルが JST ドメインの公開サーバ上で見つかっている場合、ファイアウォールのメーカーに判定変更を要求する手続を実施すること。この手続の対象とする JST のドメインと、手続の詳細は開示資料に記す。

③ セキュリティインシデントへの対応

請負者はセキュリティインシデント発生時には、被害の拡大防止を最優先とすること。

危険度 3 の事態発生時には、請負者は JST 担当者の判断を仰ぐことなく、30 分以内に問題の PC 等又はサーバの通信を遮断する措置をとること。これは基本的には PC の場合はアンチウイルスソフトウェア管理サーバで該当 PC のネットワークからの隔離を、公開サーバの場合は負荷分散装置で対象サーバの分散先からの除外とファイアウォールでの通信遮断を行うこととする。これらの手順は開示資料に記す。対応実施後は速やかに JST 担当者に連絡し、検出したログの内容、日時、攻撃の種類、確認できている被害、被害 IP アドレスと加害 IP アドレス、推奨する対応等を明確に説明すること。

危険度 2 のインシデントの場合は、その検出後 30 分以内に JST 担当者に連絡し、遮断対応の要否を確認すること。遮断実施の判断になった場合は、その後 30 分以内に前述のものと同様の遮断対応を完了すること。

なお、JST 担当者が独自に危険度 3 又は 2 の発生を検知し請負者に申告することがある。請負者はそれを受け、JST 担当者が提示する情報を基に 30 分以内に前述の遮断対応を完了すること。さらに、JST 担当者と協調して攻撃の詳細を調査し、被害の拡大防止のために推奨する対応等を助言すること。

これらの対応は月に 2 回を想定している。

④ 特に重要なインシデント発生時の現場対応

JST 担当者は、特に重要なセキュリティインシデント発生時には請負者に JST 内でのサポートを要請する。請負者はそれに応じ適切なスキルを持った人員 2 名程度を手配して「1(2)エ 業務実施場所」に記載の場所でインシデントの調査、被害拡大防止、証拠保全等のサポート業務に従事させること。1 回あたりの期間は全員の合計で 64 時間とする。このサポート業務の開始は平日の日中とするが、状況により夜間及び休日におよぶ可能性がある。

この対応は 1 年に 2 回を想定している。

⑤ IP アドレスブラックリストの登録

請負者は様々な情報源から独自に収集した最新の IP アドレス評価情報を基に、各平日に 1 回通信を遮断するべき IP アドレスリストを更新し、そのリストが含む IP アドレスとの通信を遮断するよう JST 担当者が指定する機器に設定を行うこと（ただし、遮断すべき IP アドレスリストに更新が発生しなかった場合は、対象機器への設定は不要）。また、通信遮断設定が行われているがその必要がなくなった IP アドレスについては、精査した上でリストから削除を行うこと。これらの設定手順は開示資料に記す。

請負者は IP アドレスの評価情報を複数の情報源から得て、それらから適切に遮断すべき又は遮断の必要がなくなった IP アドレスのリストを作成すること。JST 担当者から遮断対象の IP アドレス追加の依頼があった場合は、それも遮断対象に含めること。

JST 担当者から IP アドレスの遮断設定削除の依頼があった場合は、その IP アドレスの通信先としての危険度を評価し、十分低いと判断した場合はその対応を行うこと。評価の結果によらず、その判断の根拠を JST 担当者に説明すること。

⑥ 脆弱性情報の報告

請負者は JST 担当者が指定する機器やソフトウェアについて広く脆弱性に関する情報を収集し、注意を要するものがあれば電子メールで遅滞なく報告すること。報告対象は開示資料に記す。

⑦ 脆弱性情報に基づくサーバの緊急公開停止

請負者は収集している脆弱性情報の中に、JST 担当者が指定する Web サイトが該当するものを発見した場合、その影響度を評価すること。評価の結果が情報漏えいや Web サイトの改ざん、利用者の通信内容盗聴などがすぐにでも発生する可能性が高いとなった場合は、JST 担当者の判断を仰ぐことなく速やかに Web サイトを公開停止とする対応を実施すること。その手順は開示資料に記す。対応実施後は JST 担当者に連絡し、脆弱性の内容や停止した Web サイトなどを明確に説明すること。緊急性が高くない場合は、JST 担当者に連絡し、公開停止の要否を確認すること。いずれの場合も、該当の脆弱性情報の公表から 1 日以内にこれらの対応を完了させること。

Web サイトが脆弱性の影響を受けるかどうかの判断には、各サーバのインストール済みソフトウェアバージョン一覧を得る JST が導入している仕組みを使った結果も加味すること。その利用方法は開示資料に記す。

### イ　納品物の作成

請負者は「1(4) 納品・検収要件」に定める通り納品物を納めること。各納品物の内容は次に従うこと。

① 計画書

当該業務スケジュール、体制、連絡窓口、会議体等、セキュリティログ監視及び機器の設定手順等を明確に記すこと。体制では責任者を明確にすること。当該業務において有用な資格等を保持している要員については、それを付記すること。再委託を行っている場合は「1(5)ア 再委託」に定める内容も記載すること。また、作成した計画書、運用手順書、報告書等の作成と更新及び承認等についての文書・記録管理手順と、JST からの貸与品の管理手順も含めること。契約期間中、計画書は適宜修正すること。

② 情報システムセキュリティ管理手順書

請負者の当該業務実施環境について、JST の情報セキュリティポリシーに従い管理手順書を作成すること。作成にあたっては、請負者が希望すれば 2017 年 10 月から契約中の「JST セキュリティ監視運用業務」において、その請負者が納品したものをひな形として貸与する。

③ 日次報告書

当該日のセキュリティ監視に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。

- セキュリティインシデントが発生している場合はその状況
- 各セキュリティ監視機器が出力したログの統計情報(全ログ件数、ファイアウォールのポリシーによって遮断した通信の上位 10 位以内、IPS で検知しているイベントの上位 10 位以内、WAF が検知しているイベントの上位 10 位以内)
- サンドボックス機能がマルウェアと判定したファイルがあった場合は、その解説(「2(3)ア② サンドボックスが検出したマルウェアの分析」で行った対応、独自に行った判定の根拠、メーカーへの判定変更手続を行った場合はその状況を含めること)
- アンチウイルスソフトウェアがマルウェアと判定したファイルがあり、注意事項又は何らかの推奨する対応がある場合は、その内容

- 特筆すべきログがある場合はその解説（ログの意味、注意を要する理由、推奨する対応を含めること）

④ 月次報告書

当該月の当該業務に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。

- 実施した当該業務の内容とかかった工数（「1(3)ア 工数・課題管理」）
- 課題管理表（「1(3)ア 工数・課題管理」）
- サービスレベル報告。「3(1) サービスレベル」に定めるサービスレベルと比較し、実績がどうであったかを報告すること。逸脱している項目については改善計画を立案し、その内容を記すこと
- 当該月の日次報告書の内容をまとめたもの
- 当該月全体でのセキュリティログの統計情報
- 当該月のログの傾向や、請負者が収集している様々な情報を総合して分析した結果から導出した JST 全体のセキュリティレベル評価。それが十分なレベルでないならば、その原因と推奨する対策

⑤ 改善提案書

当該業務のあらゆる面からコスト削減、効率向上、統制とセキュリティ強化等の改善が可能な点を洗い出し、その改善案を提示すること。改善案には実施した場合の効果と、実施にかかる費用の概算も記すこと。

### ウ　その他の業務

① 問い合わせ対応

請負者は納品物及び当該業務に関すること並びに脆弱性、マルウェア、攻撃者及び攻撃手法等のセキュリティに関する JST 担当者からの問い合わせに回答すること。一次回答は 1 営業日以内に行うこと。

問い合わせは 1 年に 40 回程度を想定している。

② ログの調査

請負者は JST 担当者からの依頼に基づき、受信しているセキュリティログの調査を行うこと。回答は 2 営業日以内に行うこと。これは主に指定する宛先への通信が指定する期間に行われていたかどうか、行われていたとしたらいつ、どの送信元からだったのかの調査などである。調査対象となるログは 6 ヶ月前までとする。

この調査依頼は月に 2 回程度の発生を想定している。

③ 停電対応

当該業務の対象機器がある東京本部と日本科学未来館のビルは、例年それぞれ 2 月と 12 月に電気設備法定点検が行われる(実施時期は変わり得る)。これによる停電時に、請負者が持ち込んだ機器に何らかの作業が必要になる可能性がある。その場合は、請負者の負担で適切に対応を行うこと。

④ 月次報告会

請負者は毎月の 6 営業日以降 10 営業日以内又は JST 担当者と同意した日に、前月の月次報告書を説明する会を開催すること。9 月と 3 月に開催の報告会では改善提案書についても説明すること。報告会の質疑応答の内容には議事録を作成し、報告会の 3 営業日後までに JST 担当者に送付すること。

## 3　サービスレベル及びその他の要件

### (1) サービスレベル

当該業務について、運用支援の効率化、品質向上及び円滑化を図るため、下記に示す「表 3 サービスレベル」に対してサービスレベルアグリーメントを締結すること。請負者はこれらの遵守のため、常に各項目を測定、記録し、サービスレベルが適切な範囲に収まっているかを確認すること。下記の目標値は、天災や大規模停電等による障害及び計画停止の場合は除く。

提案時点でこれらの達成が困難であると判明している場合(定期的な保守業務によりログの監視ができない時間帯が存在するなど)は、請負者は困難である項目それぞれについて、提案書に目標値とどの程度の乖離が生じるのかを明確に記すこと。

表 3 サービスレベル

| 項目 | 目標値 | 内容 | 業務の詳細 |
|---|---|---|---|
| セキュリティログ保存損失 | 少なくとも 6 ヶ月分を損失 0% | 保存しているセキュリティログの損失 | 「1(2)キ 当該業務環境・ツール等」 |
| 納品物の納期遵守 | 100%納期遵守 | 納品物の納期遵守率 | 「1(4) 納品・検収要件」 |
| セキュリティログ受信損失 | 0.01%以下 | 請負者による分析が行われずに失ったセキュリティログの時間の割合。月に 5 分以内のログ損失 | 「2(3)ア① セキュリティログの監視」 |
| サンドボックスが検出したマルウェアの確認時間 | 30 分以内 | サンドボックスでのマルウェア検出のログを受信してから独自の分析を完了するまでの時間 | 「2(3)ア② サンドボックスが検出したマルウェアの分析」 |
| 危険度 3 のセキュリティインシデント発生時の初動対応 | 30 分以内 | 危険度 3 のセキュリティインシデント発生時に、その検知から通信遮断対応を完了するまでの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |
| 危険度 2 のセキュリティインシデント発生時の初動対応 | 30 分以内と 30 分以内 | 危険度 2 のセキュリティインシデント発生時に、その検知から JST 担当者に連絡を行うまでの時間及び遮断対応実施の判断からその実施完了までの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |
| JST 担当者からのセキュリティインシデント発生の申告を受けてからの初動対応 | 30 分以内 | JST 担当者からのセキュリティインシデント発生の連絡受付後に、遮断対応を完了するまでの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |

| | | | |
|---|---|---|---|
| 脆弱性情報に基づくサーバの緊急公開停止 | 1 日以内 | 脆弱性情報公表後からサーバの緊急公開停止を実施し JST 担当者に連絡するまで、又は JST 担当者に連絡し指示のあった対応を実施完了するまでの時間 | 「2(3)ア⑦ 脆弱性情報に基づくサーバの緊急公開停止」 |

(2) セキュリティ要件

請負者は以下の情報セキュリティ管理事項を遵守すること。

ア　要求事項

請負者は JST の「情報システムに関する情報セキュリティ対策ガイドライン(委託先用)」に準拠して当該業務を実施すること。同ガイドラインは開示資料として閲覧できる。また、当該業務のセキュリティに責任を持つセキュリティ管理責任者を設定し、その責任と権限を明確化すること。

イ　管理対象

請負者は次のすべてに対しセキュリティ管理を実施すること。

- 当該業務の対象機器及びそれらの設定情報
- 請負者(及び再委託者がある場合は再委託者)の当該業務環境
- 要員
- 設備、場所
- ドキュメント類(手順書、マニュアル等)
- 各種台帳
- 業務データ(ログ、分析結果及び課題管理表など)
- 貸与品

ウ　管理全般

請負者は各管理対象に対し、重要性・情報の区分に応じた管理方法を定めること。請負者内部のセキュリティ管理で用いている監視・連絡体制図を JST に提示し、管理が十分遂行できることを証明すること。管理状態の定期的な点検又は監査を実施し、

JST に報告すること。当該業務の要員に対してはセキュリティに関する教育等を実施し、その状況を管理台帳に記録すること。

### エ　セキュリティ管理内容

請負者は JST の情報セキュリティポリシー等に準じて業務を実施すること。特に下記事項を確実に実施すること。それぞれの事項についてその内容をあらかじめ又は変更時に JST に開示し、了承を得ること。

### オ　変更管理

設定変更等の作業は、あらかじめ決めた要員のみが実施すること。変更管理表を作成し、現在の状態及び変更履歴を記録すること。作業は作業者と確認者の複数名体制で行うこと。

### カ　情報受渡し

請負者と JST 担当者間で設定情報等の機密情報を受け渡す時は、第三者が容易に閲覧できないよう、暗号化やパスワード認証を施した情報の受渡し方法をとること。受渡しの際には、最新のパターンファイルを実装したアンチウイルスソフトウェアによるチェックを行うこと。

要員が作業等のため機密情報を外部へ持ち出す際は、セキュリティ管理責任者の承認を得て管理台帳に記録し、暗号化、パスワード設定等のセキュリティ対策を施すこと。管理台帳は JST 担当者からの求めに応じ開示すること。

ログ情報は海外に開示しないこと。海外での調査・分析が必要な場合は、送付する情報やそのタイミングについて JST 担当者へ事前に連絡し、了承を得ること。その場合もデータ暗号化等のセキュリティ対策を施すこと。

### キ　当該業務実施場所

請負者の当該業務を実施する場所は、認証装置により入退室を制限・記録できる機構を有すること。また、請負者以外の他者とは完全に入退室を分離し、物理的に隔離していること。

### ク　使用機器

当該業務に使用する機器は、作業者以外が使用することがないよう、権限の付与、取消しについて管理を行い、他の者の操作を禁止すること。

機器からは外部記憶媒体に書き込みのできる不要なデバイスを取り外すこと。プリンタを設置する場合は必要最小限の台数とし、利用者を制限すること。

当該業務で使用するPCは、以下の事項を遵守すること。

- すべて管理台帳で管理すること
- 他の業務と兼用しないこと。私的利用をしないこと
- 利用開始の前にアンチウイルスソフトウェアによるスキャンを実施すること
- 当該業務に必要のないソフトウェアはインストールしないこと
- OSとインストールしているソフトウェア、アンチウイルスソフトウェアのパターンファイルを最新の状態に保つこと
- 利用中に一定時間操作がなければロックし、その解除に認証を求める設定とすること
- 盗難防止策を施すこと

### ケ　可搬型外部記憶媒体

当該業務に可搬型外部記憶媒体(USBメモリ、DVD等)を利用する場合は、それらの管理台帳を作成し、本業務専用として管理すること。媒体は施錠可能なキャビネットなどに保管すること。利用する際は日時、利用者、媒体を識別する名称等を記録すること。データの書き込み時には暗号化を施し、読み取り時にパスワードを求めるようにすること。当該業務外での利用と外部への持ち出しは厳禁とする。

月に1回は棚卸しを行い、万が一紛失等が発生した場合は速やかにJST担当者に報告すること。

不要になった場合又は契約満了時には内容の読み取りを不可能に処理した上で廃棄すること。

### コ　目的外使用の禁止

請負者が当該業務で使用するあらゆるデータは、本契約の目的以外に使用しないこと。契約終了時には確実に削除すること。

## サ　ID・パスワード管理

当該業務で使用する操作端末ごとに管理者名、使用者名、それらの利用権限、担当作業内容及び ID を管理台帳で管理すること。権限を一人に集中させすぎないように、かつ必要以上の要員に権限を付与しないこと。ID の追加、削除又は権限の変更時にセキュリティ管理責任者が承認するルールを定め、その内容を JST に報告すること。

不要な ID は速やかに削除すること。デフォルトで存在する ID は使用する必要がなければ削除又は無効化すること。それができなければパスワードを適切に設定し、可能であればさらに ID 名を変更すること。

ID は個人ごとに付与し、作業担当者変更（追加、減少を含む）の際には、記録を残すこと。当該業務を担当しなくなった作業担当者の ID は速やかに削除し、同一 ID の引継ぎは行わないこと。複数の使用者による ID 共有は原則禁止するが、システム的に実現が不可能であれば、共有する ID を実際にはだれが利用したのかを記録すること。ID を共有している作業担当者に変更があった場合は、必ずパスワードの変更を行うこと。

ID は半年に 1 回以上棚卸しを行い、結果を報告すること。

当該業務で使用するパスワードは原則 13 文字以上、英小文字、英大文字、数字、記号の複合（4 種類が望ましいが最低限 3 種類）であること。また、複数の使用者により共有している ID については、90 日ごとにパスワードを変更すること。パスワード更新を強制的に行う仕組みがなければ、更新期間の管理を管理台帳で行うこと。

当該業務で使用するパスワードを操作端末に記憶させないこと。他システム、他サービスで使用している ID とパスワードの組合せは使わないこと。

## シ　情報管理

当該業務に関するドキュメントや媒体等は、管理台帳により管理し、施錠可能なロッカー等に保管すること。

## ス　業務データ管理

当該業務に関するデータは国内に保持すること。

## セ　守秘義務

請負者は当該業務の内容及び当該業務に関連して開示を受けた、又は知り得た相手方の技術的若しくは事業運営にかかる一切の情報(以下「機密情報」という)につき最

大限の注意を払い秘密を保持すること。事前に JST の書面による承諾を得ることなく、本業務の目的外で使用又は第三者に開示・漏えいしてはならない。

なお、請負者は自社の従業員のうち本業務に従事する従業員にのみ機密情報を開示するものとし、本業務に関与しない従業員には、いかなる手段においても一切機密情報を開示し又は使用させてはならない。また、本件の実施完了後は、本件に関する情報を返却又は確実に破棄すること。

本業務の提供により知り得たすべての事項については、契約期間中はもとより、契約終了後においても外部に漏らさず、機密保持のために十分な体制・設備で厳重に管理し、情報漏えいを確実に防止すること。

本業務の提供において知り得た情報が紛失や盗難等による第三者への情報漏えいの発生又はそのおそれがある場合は、速やかに JST 担当者に電話、口頭等による連絡を行うとともに、書面で報告すること。また、直ちに事実調査を行い、漏えいした情報の内容、原因、再発防止策等について記載した書面を JST 担当者へ提出し、事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。なお、請負者以外の者の作業も含め、対処にかかる費用はすべて請負者が負担すること。

請負者の設備や機器に保存しているログ情報は、JST からの要請により削除可能であること。交換や撤去を行う際は、機器に残っているデータはすべて適切に消去すること。

## ソ　サプライチェーンリスク管理

請負者は本件で用いる機器について、その設計・製造・試験・納入・設置構築等の各工程において、意図しない変更や機密情報の窃取等の防止を、一貫した品質保証体制の下で行っている保証を、そのサプライヤーに求めていること。それを説明する書類(体制図、社内基準等)を、可能な範囲で提出すること。さらに、請負者は本件で用いる機器に意図しない変更が行われているなどの不正が見つかった時には、追跡調査や立入検査等により JST と連携して原因を調査し、排除するための手順及び体制を整備していること。それを説明する書類(体制図、社内基準等)を、可能な範囲で提出すること。

また、本件で用いる機器が、その保守等の目的で機器情報を収集する仕組み等を持つ場合、その手段、方式等をすべて明確にし、事前に JST 担当者の承認を得ること。

## タ　監査

JST 担当者は必要に応じ請負者に対し当該業務に関する監査を行う。請負者は監査に協力すること。対応のために多大な工数が必要な場合は、別途調整する。

## 4 開示資料一覧

- 2017 年度下期から契約中の「JST セキュリティ監視運用業務」において、その請負者が報告した業務内容と作業工数（「1(3)ア 工数・課題管理」）
- ネットワーク概要図（「2(1)ア 本案件の目的」）
- セキュリティログ監視機器の機種、ハードウェア構成、設定、監視対象となるログのサンプルとその 1 日当たりのサイズ、ログの取得方法等（「2(1)イ セキュリティログ監視対象」）
- サンドボックスがマルウェアと誤判定したファイルが JST ドメインのサーバ上で見つかった時の対応手順（「2(3)ア② サンドボックスが検出したマルウェアの分析」）
- セキュリティインシデント発生時の緊急通信遮断手順（「2(3)ア③ セキュリティインシデントへの対応」）
- IP アドレスブラックリスト登録手順（「2(3)ア⑤ IP アドレスブラックリストの登録」）
- 脆弱性情報を収集し報告する対象一覧（「2(3)ア⑥ 脆弱性情報の報告」）
- 情報システムに関する情報セキュリティ対策ガイドライン(委託先用)（「3(2)ア 要求事項」）

以上

**別添２**

# JST セキュリティ監視運用業務

# 提案書作成要領（案）

**令和元年 6 月**

国立研究開発法人科学技術振興機構

「JST セキュリティ監視運用業務」において、入札を希望する者は、本提案書作成要領に基づき、以下の内容を記載した提案書を作成し、必要部数を締切日までに国立研究開発法人科学技術振興機構（以下、「当機構」という。）に対して提出しなければならない。

## 1. 提案書の作成

(1)様式

ア　使用言語

日本語とする。

イ　用紙サイズ等

A4 版縦置き、横書きを原則とする。図表については必要に応じて A3 版横又は縦置き、横書きを使用することができる。

ウ　項番設定

項番の付番を以下の基準に従うこと。さらに項目を細分化する必要等から以下の付番以下のレベルが必要となった場合には、適宜追加設定して差し支えない。

図表番号は章内での一連番号とし、あわせて図表題名を付すこと。

| 見出し種類 | 項番表示 |
|---|---|
| 見出し１ | １、２、３、・・・ |
| 見出し２ | （１）、（２）、（３）、・・・ |
| 見出し３ | ア、イ、ウ、・・・ |
| 見出し４ | （ア）、（イ）、（ウ）、・・・ |
| 見出し５ | A、B、C、・・・ |
| 見出し６ | (A)、(B)、(C)、・・・ |
| 見出し７ | a、b、c、・・・ |
| 見出し８ | (a)、(b)、(c)、・・・ |

エ　データ形式

文書類を電子媒体に保存する形式は、Microsoft Word 2010 以上、Excel 2010 以上、PowerPoint 2010 以上又は PDF 形式とする。ただし、当機構が別途形式を定めて提出を求めた場合はこの限りではない。

オ　作成部数等

・提案書及び関連資料　　7 部（正本 1 部、副本 6 部）
・総合評価基準及び対応表　　7 部（正本 1 部、副本 6 部）
・参考見積書　　7 部（正本 1 部、副本 6 部）
・上記文書等を格納した電子媒体　　1 式

ただし、電子媒体は、入札希望者が用意する CD-R 媒体等とする。

(2)提案書の記載方法

ア　提案書の表紙

表題を「JST セキュリティ監視運用業務　提案書」とし、以下を明記すること。

・提案者の住所、名称、代表者名
・社印の押印（正本１部のみでよい）
・連絡担当者の所属、氏名、電話番号、ファクシミリ番号及び電子メールアドレス
・提案書の提出日

イ　提案書の目次構成

・提案書の目次構成は特に定めないが、調達仕様書に示す要件との対応がわかるように構成すること。
・本業務の概要又は概略から書き起こし、順次詳細部分に言及する等、構造的な構成とすること。
・適切な目次を付け、提案書の内容及び構成を端的に表現できるようにすること。

ウ　提案書の記載事項

・調達仕様書に示す要件及び総合評価基準書の別紙「総合評価基準及び対応表」（以下、「総合評価基準及び対応表」という。）に示す評価の観点を理解し、実現方式等について具体的に提案及び記載すること。
・全ての頁に通し頁番号を記入すること。
・提案及び記載の中で関連資料を参照する場合は、資料名だけでなく関連資料の通し頁番号も記載すること。

エ　関連資料

・必要に応じて提出すること。
・全ての頁に通し頁番号を記入すること。

オ　総合評価基準及び対応表

「総合評価基準及び対応表」における評価の観点の内容との対応関係を把握できるようにするため、「総合評価基準及び対応表」の「提案書の該当頁」欄及び「関連資料の該当頁」欄に対して該当する頁番号を記入したものを提出すること。

カ　参考見積書

作業内容を確認するために、参考見積書を作成すること。参考見積書は下記の
一時経費、運用経費、回線経費に分けて作成すること。また単価×工数等を示すこと。

・一時経費：運用環境、体制構築にかかる初期費用
現行の端末にインストールされているウィルス対策ソフトを入れ替える場合は、当該ソフトウェアの購入費と端末へのインストール支援作業の費用も含めること。
・運用経費：個々の作業にかかる費用。調達仕様書の項目（セキュリティ監視業務、納品物の作成、その他）に分けて作成すること。
・回線経費：運用のために接続用回線等にかかる費用

(3)入札時開示資料

入札時に開示する資料は以下のとおり。当該資料はセキュリティにかかる情報が含まれているため、閲覧のみとする。閲覧は入札説明書記載の方法で申し込むこと。

・2017 年度下期から契約中の「JST セキュリティ監視運用業務」において、その請負者が報告した業務内容と作業工数
・ネットワーク概要図
・セキュリティログ監視機器の機種、ハードウェア構成、設定、監視対象となるログのサンプルとその 1 日当たりのサイズ、ログの取得方法等
・サンドボックスがマルウェアと誤判定したファイルが JST ドメインのサーバ上で見つかった時の対応手順
・セキュリティインシデント発生時の緊急通信遮断手順
・IP アドレスブラックリスト登録手順
・脆弱性情報を収集し報告する対象一覧
・情報システムに関する情報セキュリティ対策ガイドライン(委託先用)

(4)留意事項

ア　当機構が特段の技術知識及び特定の製品に関する一切の知識を有することなく、提案書等の審査が可能となるような提案書を作成すること。

イ　提案書の記載内容が、調達仕様書記載内容の単純な引き写しになっている等、入札希望者による具体的な提案に欠けていると当機構がみなす場合、該当項目に関する提案書の記載内容を評価しない場合があるので、留意すること。

## 2. 提案手続

(1)提出期限

入札説明書記載のとおり。

(2)提出場所

〒102-8666
東京都千代田区四番町 5 番地 3　サイエンスプラザ
国立研究開発法人科学技術振興機構

契約部契約業務課

＊持参の場合は契約部契約業務課の窓口にて承りますので直接お越しください。

電話 03-5214-7996　　ＦＡＸ03-5214-8433

(3)提出方法

提出場所へ持参すること。ただし、郵送も可とする。

(4)提出部数

書面 7 部、電子媒体（CD-ROM 等）1 式

(5)その他

ア　応募及び提案に係る経費は、提案者の負担とする。

イ　提出された提案書等は、当該業務の請負者の選定のためにだけ使用する。

ウ　提出された提案書等は、返却しない。

エ　必要に応じて確認及び追加資料の提出を求めることがあるので、提案者はその内容についての説明及び資料提出を行うこと。

別添３

# JST セキュリティ監視運用業務

# 総合評価基準書（案）

令和元年 6 月

国立研究開発法人科学技術振興機構

## 1. はじめに

本書は国立研究開発法人科学技術振興機構（以下、「当機構」という）の「JSTセキュリティ監視運用業務」（以下、「本業務」という）に関する総合評価について定めたものである。

## 2. 評価基準

(1) 評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（総合評価基準書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

| |
|---|
| 価格点と技術点の配分<br>価格点の配分：技術点の配分　＝　1：1 |

| |
|---|
| 総合評価点　＝　価格点（840 点満点）＋ 技術点（840 点満点） |

(2) 合否決定方法

提出された提案書の内容が、別紙「総合評価基準及び対応表」に示す評価項目において必須項目と定められた要求要件を全て満たしている場合に「合格」とし、一つでも欠ける場合は「不合格」とする。

(3) 総合評価点

ア　価格点

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。

| |
|---|
| 価格点　＝　（1－入札価格÷予定価格）×　840 点 |

イ　技術点

技術点の評価は以下のとおりとする。

(ア) 提出された提案書の内容が、別紙「総合評価基準及び対応表」に示す評価項目において必須項目と定められた要求要件を全て満たしており、「合格」したものに、「基礎点」として 210 点与える。

(イ) 「合格」した提案書について、総合評価基準書に基づき、総合評価委員会の委員ごとに加点部分の評価を行う。各委員の評価結果を委員会で確

認し、事実誤認等があれば各委員において訂正する。なお、各委員が行う加点部分の評価は、別紙「総合評価基準及び対応表」に示す評価項目毎に以下の評価基準及び得点に基づき点数化する。確定した各委員の採点結果の平均値（小数点以下切り捨て）を算出し、「加点」とする。

評価基準及び得点

| 評価 | 評価基準 | 得点 |
|---|---|---|
| S | 実績の場合は、A 評価を満たし、かつ、記載された根拠が本業務の効果的・効率的な実施に資すると判断できるものであること。<br>提案の場合は、A 評価を満たし、かつ、その実効性、有効性が優れておりその根拠が客観的に示されていること。 | 配点×１．０ |
| A | 実績の場合は、B 評価を満たし、かつ、それが本業務の効果的・効率的な実施に資する根拠が記載されていること。<br>提案の場合は、B 評価を満たし、かつ、その手順や方法等がより具体的（実効性、有効性等の根拠を含む）であること。 | 配点×０．７ |
| B | 評価の観点に示した内容が記載されている。 | 配点×０．３ |
| C | 評価の観点に示した内容が記載されていない。 | 配点×０ |

(ウ) 「基礎点」と「加点」の合計点を「技術点」とする。

| 技術点　＝　基礎点（210 点）　＋　加点（630 点満点） |
|---|

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 内容 | 頁 | 評価項目番号 | 必須項目 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○× | 加点項目番号 | 加点項目 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 SABC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 発注要件 | 4 | － | － | － | － | － | － | － | － | － | － | － |
| 1(1) 発注内容 | 4 | － | － | － | － | － | － | － | － | － | － | － |
| 1(1)ア 案件名 | 4 | － | － | － | － | － | － | － | － | － | － | － |
| JSTセキュリティ監視運用業務 | | － | － | － | － | － | － | － | － | － | － | － |
| 1(1)イ 発注概要 | 4 | － | － | － | － | － | － | － | － | － | － | － |
| 本件は国立研究開発法人科学技術振興機構の総合的なセキュリティ対策のため、セキュリティ機器やサーバ機器、関連ソフトウェアが生成するログを監視し、セキュリティインシデント発生の際にはその対応を行う業務を調達するものである。 | | 1 | 発注概要について、提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | 2 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(1)ウ 用語定義 | 4 | － | － | － | － | － | － | － | － | － | － | － |
| － | | － | － | － | － | － | － | － | － | － | － | － |
| 1(2) 発注条件 | 5 | － | － | － | － | － | － | － | － | － | － | － |
| 1(2)ア 契約期間 | 5 | － | － | － | － | － | － | － | － | － | － | － |
| 契約期間は契約締結日（令和元年11月29日見込み）から令和5年3月31日までとする。<br>なお、引継ぎ等の準備は令和2年3月31日までとし 、セキュリティ監視業務は令和2 年4月1日から令和5年3月31日まで とする。<br>請負者は契約期間開始から遅滞なく本書で定めるサービスレベルで当該業務ができるよう体制と環境を構築すること。 | | 3 | 業務開始までのスケジュールおよび体制が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 4 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | | | | | | |
| 1(2)イ 選定条件 | 5 | － | － | － | － | － | － | － | － | － | － | － |
| ① 請負者は契約期間中24時間常時複数名によるセキュリティ監視が可能な体制(人員、設備等)があること。監視要員の人数、保有資格、業務経験、交代スケジュールは適切であること。 | | 5 | 仕様書の2.(3)の「ア.セキュリティ監視業務」「イ.納品物の作成」「ウ.その他の業務」の業務毎に以下の(a)～(c)が提案書に具体的に記載されていること。<br>(a) 体制図（人員及びその技術スキル、責任者と責任分担、使用設備、交代スケジュール）<br>(b) 当該業務をサービスとして実施する場合は、そのサービス内容（カタログ等）<br>(c) 業務の一部を再委託する場合は、再委託先についても上記(a)(b)を記載すること。 | | | | － | － | － | － | － | － |
| | | 6 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(2)イ ② 請負者はセキュリティ監視機器又は同等の製品について、そのログを監視する業務の受注実績があること。 | | 7 | 受注実績が提案書に具体的に記載されていること。<br>受注実績には以下の要素が含まれていること。<br>・実施時期<br>・監視を実施した対象の組織の人数（概算値）<br>・監視を実施した対象のネットワークの規模（PCおよびサーバ等の台数）<br>・1ヶ月 当たり監視ログ量（概算値） | | | | 加1 | JSTと同規模以上の組織について、セキュリティログ監視を実施した実績を多く持っていること。 | | | 30 | |
| 1(2)イ ③ 請負者はISO9001に準拠又は同等の品質管理体制を実施していること。同等の品質管理体制とは、品質管理方針、品質管理体制を制定し、文書管理、記録の管理などについて、文書化した手順により実行していること及び内部監査を実施していることを言う。 | | 8 | 認定証の写しが提示されているか、または、同等の品質管理体制を実施していることが提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 1(2)イ ④ 請負者はISO/IEC27001又はJIS Q 27001に準拠した管理若しくは同等の情報セキュリティ管理を実施していること。同等の情報セキュリティ管理を実施しているとは、情報セキュリティ方針、情報セキュリティ管理体制を制定し、リスクアセスメント、リスクアセスメントに基づく管理策、内部監査、教育を実施していることを言う。 | | 9 | 認定証の写しが提示されているか、または、同等のセキュリティ管理実施していることが提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 1(2)イ ⑤ 請負者のセキュリティ監視を行う要員には、セキュリティの専門家を含んでいること。専門家であるとは、下記の資格のいずれかを有することを指す。<br>・情報処理安全確保支援士<br>・CISSP(Certified Information Systems Security Professional)<br>・GIAC(Global Information Assurance Certification) | | 10 | セキュリティ監視を行う要員の認定証の写しが提案書に提示されていること。 | | | | 加2 | 以下のいずれかのセキュリティ資格を有している者がセキュリティ監視要員として多く体制に含まれていること。<br>・情報処理安全確保支援士<br>・CISSP(Certified Information Systems Security Professional)<br>・GIAC(Global Information Assurance Certification) | | | 50 | |
| 1(2)イ ⑥ 請負者の当該業務を請け負う部門には、下記のいずれかの資格を持つ者、または本業務と類似した業務実施経験を3年以上有する者が在籍しており、本業務の実施体制に含んでいること。<br>・PMI(Project Management Institute)認定PMP(Project Management Professional)<br>・情報処理推進機構認定プロジェクトマネージャ<br>・Expert Certificate in IT Service Management (ITIL Expert) | | 11 | セキュリティ監視を行う要員が持つ認定証の写しか、または本業務と類似した業務実施経験を3年以上有する者の所属および作業内容について提案書に提示されていること。 | | | | － | － | － | － | － | － |
| 1(2)イ ⑦ 請負者は常に最新のセキュリティ関連情報を世界中から収集していること。収集した情報を当該業務で活用できる体制を確立していること。 | | 12 | 以下の(a),(b)が提案書に具体的に記載されていること。<br>(a) 情報収集ソース（サイト）や収集頻度、収集量、内容<br>(b) 収集した情報を当該業務で活用するための体制 | | | | 加3 | 本業務のより効果的な実施に資する情報収集を拡大していくための方策を多く提案していること。本業務のより効果的な実施に資すると判断できれば加算する。<br><br>例えば、以下の方策が考えられる。<br>・情報収集するための組織が日本以外の世界各地に存在する。<br>・24時間365日の体制で情報収集している。<br>・業界標準となるサイトや団体と密接に情報交換し、最新の情報を収集している。 | | | 50 | |
| | | 13 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(2)ウ 言語 | 6 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者はJST担当者への連絡を日本語で行うこと。納品物の報告書等も日本語で作成すること。ただし、システム的に生成する日次の報告書等は英語でもよい。その場合であっても、請負者はJST担当者からの求めがあれば、その内容について日本語で解説すること。 | | 14 | 言語について提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 1(2)エ 業務実施場所 | 6 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務はリモート作業とする。請負者が当該業務を行う場所は、原則として請負者の負担で用意すること。ただし、必要に応じJST内での作業はあり得る。JSTのサーバ室へ入室する際には、入退室記録等の手順に従うこと。<br>当該業務対象機器の設置場所は下記の通り。会議等の開催場所は、原則として東京本部とする。<br>[東京本部]<br>〒102-8666 東京都千代田区四番町5-3<br>国立研究開発法人科学技術振興機構 東京本部<br>[日本科学未来館]<br>〒135-0064<br>東京都江東区青海2-3-6 日本科学未来館 | | 15 | 作業実施場所について提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 16 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | | 評価項目 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 必須項目 | | | | 加点項目 | | | | | | |
| 内容 | | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定〇× | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定SABC |
| 1 (2) オ 貸与品<br>JST担当者は請負者に必要に応じ次のものを貸与する。請負者は貸与品の管理責任者を定め、紛失や破損のないよう留意すること。万一、紛失等が発生した場合は、速やかにJST担当者に報告し、指示に従うこと。第三者への貸与は禁ずる。<br>契約満了時又は不要になった場合は速やかに返却すること。電子データはすべて消去すること。<br>・当該業務対象機器の設置場所に入館するためのカード<br>・当該業務対象機器に関する設計書等の資料、設定情報及びログデータのサンプル等<br>・情報セキュリティ規程及び関連規則<br>・情報システムセキュリティ管理手順書 | | 7 | 17 | 貸与品について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| | | | 18 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |
| 1 (2) カ 開示資料<br>本件に関する開示資料は、入札前は所定の手続に沿って申請を行った応札予定者に対し一部をマスクした上で、開札後には秘密保持契約締結後にマスクしていないものを請負者に開示する。資料は「4 開示資料一覧」に列挙している。 | | 7 | 19 | 開示資料について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| 1 (2) キ 当該業務環境・ツール等<br>当該業務に使用する請負者側の環境(監視機器、セキュリティログを収集・分析する機器、請負者とJSTとの間の接続回線・接続機器(請負者側とJST側の両端)、当該業務に使用するソフトウェア及びツール等)は、請負者の負担で用意すること。セキュリティログは少なくとも6ヶ月前にさかのぼって調査が可能なように、JSTにあるものとは別に請負者の環境にも保存すること。なお、「2(2)ウ JST内への機器設置」にあるように、必要であればJST内への機器の設置は可能である。前述のJSTのものとは別にとしているセキュリティログの保存は、その機器で行ってもよい。<br>これらの準備にかかる費用は、月額費用とは分けて初期費用として計上すること。 | | 7 | 20 | 当該業務環境・ツール等について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| | | | 21 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |
| 1 (3) 当該業務条件 | | 8 | — | — | — | — | — | — | — | — | — | — | — |
| 1 (3) ア 工程・課題監理<br>請負者は計画書等に従い確実に当該業務を実施し、その実績を定量的に記録すること。記録を行う作業単位は、工数と実績を評価する上で適切であること。可能であれば、作業件数とその稼働時間の両方を記録すること。請負者はこの記録に基づき、必要であれば要員の増員、配置の変更等を適切に計画すること。<br>当該業務遂行中に発生した課題については課題管理表を作成し、課題の内容、発生日、完了日、対応者、対応結果等を記録すること。業務遂行に支障をきたす重大な課題、懸念等が発生した場合は、速やかにJST担当者に報告すること。<br>なお、2017年10月から契約中の「JSTセキュリティ監視運用業務」において、その請負者が報告した業務内容と作業工数は、開示資料として閲覧できる。 | | 8 | 22 | 工程・課題管理について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| | | | 23 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |
| 1 (3) イ 連絡体制<br>請負者は24時間365日当該業務を実施するための体制を整えること。JST担当者からのインシデント発生の申告、問い合わせ等を受け付ける連絡窓口を設けること。<br>請負者がインシデント発生時等に連絡するJST担当者の連絡先は、受注後に開示する。連絡先は優先度を付けた複数の電話番号とメールアドレスの一覧である。連絡が必要となった場合は、請負者はその一覧に従い連絡を実施すること。電話での場合は、連絡が取れるまで一覧中の電話番号に少なくとも2巡は連絡を試みること。電話での連絡ができたかどうかにかかわらず、一覧中のすべてのメールアドレスに必要な情報を送信すること。 | | 8 | 24 | 連絡体制について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| | | | 25 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |
| 1 (3) ウ 変更への対応<br>すべての当該業務の対象となる機器で、契約期間中に設定の変更、機能の追加あるいは削除、ソフトウェアのバージョン変更、機種の変更、何らかの原因によるログの増大又は機器の追加、撤去を含むネットワーク構成の物理的、論理的な変更等(なお、これらの変更作業は当該業務の範囲内ではない。)があり得る。これらの変更があったとしても、請負者はサービスレベルを落とすことなく継続的に当該業務を遂行すること。それらにより請負者の設備や体制等に増強等が必要となる場合は、JST担当者と協議すること。 | | 8 | 26 | 変更への対応について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| | | | 27 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |
| 1 (4) 納品・検収要件 | | 8 | — | — | — | — | — | — | — | — | — | — | — |
| 1 (4) ア 納品物<br>請負者は下記に定める報告書等を所定の期日までに納品すること。<br>納品形態を電子データとしているものは、基本的には指定する宛先への電子メールでの送付とするが、JST担当者が認めた場合は、請負者が用意したWebサイトへの掲載としてもよい。Webサイトによる納品の場合は、JST担当者以外が閲覧することができないよう、適切な認証、暗号化の仕組みを盛り込むこと。その仕組みの妥当性について、事前にJST担当者の了承を得ること。<br>電子データとして納める電子ファイルは、内容の変更が可能な形式にすること。電子データは納品時点における最新のパターンファイルを実装したアンチウイルスソフトウェアによるチェック実施後に納品すること。 | | 8 | 28 | 納品物について提案書に具体的に記載されていること。 | | | | — | — | — | — | — | — |
| 1 (4) ア ① 受注時、随時納品物<br>・計画書<br>・情報システムセキュリティ管理手順書<br>1 (4) ア ② 日次納品物<br>・日次報告書<br>1 (4) ア ③ 月次納品物<br>・月次報告書<br>1 (4) ア ④ 半期納品物<br>・改善提案書 | | | 29 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | — | — | — | — | — | — |

# 総合評価基準及び対応表（案）

**別添３**

| 仕様書等 | | | | 評価項目 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 必須項目 | | | | | 加点項目 | | | | | | |
| 内容 | | | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定〇× | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定SABC |
| 1(4)イ 納品日 | | | 9 | － | － | － | － | － | － | － | － | － | － | － |
| 1(4)イ | ① 受注時、随時納品物<br>受注日の翌営業日から起算して10営業日以内とする。ただし、契約期間中に変更があった場合は、更新版を随時納め、JST担当者の承認を得ること。 | | | 30 | 納品日について提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 1(4)イ | ② 日次納品物<br>日本時間で当該日の翌日午前中までとする。ただし、請負者が希望すれば、送付は平日のみでも可とする。その場合は、本来休日に送付するべきだった分(金曜、土曜、日曜、祝日の分)は、直後の営業日の午前中に送付すること。 | | | 31 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(4)イ | ③ 月次納品物<br>日本時間で当該月の翌月の10営業日までとする。 | | | | | | | | | | | | | |
| 1(4)イ | ④ 半期納品物<br>9月末と3月末までとする。 | | | | | | | | | | | | | |
| 1(4)ウ 納入場所・担当者 | | | 10 | － | － | － | － | － | － | － | － | － | － | － |
| － | | | | － | － | － | － | － | － | － | － | － | － | － |
| 1(4)エ 検収 | | | 10 | － | － | － | － | － | － | － | － | － | － | － |
| 検収はJST担当者が次のすべてを確認、承認することにより完了とする。<br>①計画した当該業務をすべて実施し、実績報告をしていること。<br>②報告書の形式及び内容が正しいこと。<br>③すべての納品物が指定の媒体、数量、形式となっていること。<br>④すべての納品物の記載内容及び情報が妥当であること。<br>なお、JST担当者が納品物の内容について修正、追加を依頼した場合は、速やかに対応し再納品すること。 | | | | 32 | 検収について提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 33 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | | | | | | |
| 1(5) その他前提条件 | | | 10 | － | － | － | － | － | － | － | － | － | － | － |
| 1(5)ア 再委託 | | | 10 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は本業務のすべてを一括して再委託してはならない。一部を再委託する場合は、原則として、あらかじめ提案書に再委託先に委託する業務の範囲、再委託を行うことの合理性と必要性及び再委託先の履行能力並びに報告徴収、個人情報の管理及びその他運営管理の方法(以下「再委託先等」という。)について記載しなければならない。<br>契約締結後にやむを得ない事情により再委託を行う場合には、請負者は再委託先等を明らかにした上で、事前にJSTの承認を得なければならない。<br>再委託においては、JSTに対して負う義務を適切に履行するため、請負者は再委託先の事業者に対し必要な措置を講じさせるとともに、再委託先から必要な報告を徴収することとする。また、再委託先の事業者が行う業務はすべて請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由は、請負者の責に帰すべき事由とみなして、請負者が責任を負うものとする。 | | | | 34 | 再委託について提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 35 | 当該業務の一部を再委託する場合に、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 36 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(5)イ 要員の準備 | | | 11 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務開始時から円滑に業務を実施するよう、請負者の各要員は当該業務に必要な知識と技術の習得、運用手順書の熟知に努めること。 | | | | 37 | 要員の準備について、提案書に具体的に記載されていること。 | | | | 加4 | 各要員が当該業務に必要となる最新の知識と技術を習得するための方策が多く提案されていること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 30 | |
| | | | | 38 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(5)ウ 要員の交代 | | | 11 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者側の都合により要員交代の必要がある場合は、JSTに対して事前に通知するとともに、充分な業務引継ぎを行い、滞りなく業務を遂行すること。また、計画書に記載している体制を修正すること。 | | | | 39 | 要員の交代について、提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 40 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 1(5)エ 引継ぎ | | | 11 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務の契約満了時、別契約の請負者との間で業務の引継ぎを行う必要がある場合は、本契約の請負者は新規業者が円滑に当該業務を開始できるよう最大限協力すること。JSTは円滑な引継ぎのために現行請負者及び請負者に対して必要な措置を講ずるとともに、適切に引継ぎが行われているかを監督し、その完了を確認する。<br>本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者又はJSTから業務の引継ぎを受けるものとする。引継ぎ期間は本業務開始日前の4ヶ月を想定している。<br>本業務の終了に伴い請負者が変更となる場合には、請負者は当該業務の開始日までに業務内容を明らかにした書類等により、次回請負者に対し引継ぎを行うこと<br>いずれの場合でも、引継ぎに必要となる経費は、現行請負者に発生した経費は現行請負者の負担、JSTに発生した経費はJSTの負担、引継ぎを受ける請負者に発生した経費は引継ぎを受ける請負者の負担とする。<br>当該業務でJSTのために作成した相関分析の分析ルール等は、可能な限り新規業者に引継ぐこと。ただし、請負者が事業継続上特に秘匿したい情報は除外してよい。 | | | | 41 | 引継ぎについて、提案書に具体的に記載されていること。 | | | | 加5 | JSTに引き継ぐ技術情報について、より多く提供可能かが提案されていること。技術情報は、IPアドレスブラックリストや、ログ解析の際に使用した分析ルール（監視項目、分析アルゴリズム、データ抽出のための式など）などを想定している。 | | | 30 | |
| | | | | 42 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | 評価項目 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 必須項目 | | | | 加点項目 | | | | | |
| 内容 | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定〇× | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定SABC |
| 2 当該業務要件 | 12 | － | － | － | － | － | － | － | － | － | － | － |
| (1) 当該業務概要 | 12 | － | － | － | － | － | － | － | － | － | － | － |
| 2(1)ア 本案件の目的 | 13 | － | － | － | － | － | － | － | － | － | － | － |
| JSTのネットワーク環境は、様々なネットワーク機器とセキュリティ機器、サーバ類、端末及びそれらにインストールしたソフトウェアが構成している。当該業務に関するネットワークの概要図は開示資料に含めている。<br>中長期計画においてJSTは「ICTを適切に活用し業務の効率化を推進する」としている。昨今のインターネットを活用した情報発信、情報収集は、業務に多大な効率化の恩恵を与えたが、悪意を持つ者にとってもそれは同様である。そのような者はインターネット上のあらゆるところから任意の時間に攻撃を試みることができ、その手法は様々な者が随時開発、公開している。ひとたび悪意を持つ者にネットワーク環境への侵入を許せば、それはJSTが保有する国民の財産である様々な情報資産を重大な脅威にさらすことになる。そのような場合に備え、同じく中長期計画で「情報システムに対するサイバー攻撃への防御力、攻撃に対する組織的対応能力の強化に取り組む」とも掲げている。本件はJSTネットワーク環境のセキュリティ監視を行い、攻撃等発生時の速やかなインシデント対応が可能なシステムと体制を整え、組織的対応能力の強化を行うものである。 | | 43 | 本案件の目的が提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | 44 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2(1)イ セキュリティログ監視対象 | 14 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者が当該業務でセキュリティログ監視を行う対象とする機器を「表 1 セキュリティログ監視対象(東京本部)」と「表 2 セキュリティログ監視対象(日本科学未来館)」に示す。表に記載の通り、対象機器は大きく東京本部所属のものと日本科学未来館所属のものに分かれている。請負者はそれぞれのログを適切に収集できるよう収集用機器や回線を設計、構築すること。それぞれの機器のログを請負者の環境に送付するための設定作業等は、JST担当者が行う。<br>各機器の機種、ハードウェア構成、設定、監視対象となるログのサンプルとその1日当たりのサイズ、ログの取得方法等は開示資料に記す。<br>なお、使用しているネットワークプロトコルのアドレスファミリーはIPv4のみである。 | | 45 | セキュリティログ監視対象が提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | 46 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2(2) 当該業務環境 | 14 | － | － | － | － | － | － | － | － | － | － | － |
| 2(2)ア 当該業務環境における条件 | 14 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者の当該業務環境は「3(1) サービスレベル」に定めるサービスレベルを保証できる構成とすること。<br>請負者の環境が、JST以外の受注先業務の環境を共有する場合は、JST用の機器とJST以外用の機器は物理的又は論理的に分離し、JSTと他組織との間で請負者を介した通信、情報の移動ができないようにすること。適切にファイアウォールやアンチウイルスゲートウェイなどを設置し、セキュリティを確保すること。なお、セキュリティログ監視に用いる機器がインターネットと通信することは、ソフトウェアやデータのアップデート又は当該業務に直接関連する場合を除いて禁ずる。<br>請負者は自らの当該業務環境の詳細について、事前にJST担当者の承認を得ること。 | | 47 | サービスレベルを保証できる業務環境の構成が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 48 | 仕様書内容を理解し且つ適合していることが提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 2(2)イ 回線 | 14 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は自身の負担で当該業務に用いる環境とJSTを接続する回線を用意すること。回線は東京本部及び日本科学未来館のそれぞれに敷設すること。<br>回線は24時間の監視が可能なもので、当該業務実施に十分な帯域を有すること。「III.Aサービスレベル」に定めるサービスレベルを達成するよう複数回線の敷設、回線切断時の自動切替えの仕組み導入などの方策をとること。なお、サービスレベル及びセキュリティを維持しているのであれば、インターネットVPNを用いてもよい。<br>JSTとの接続回線はJST以外への通信に用いてはならない。やむを得ず他用途と共用する場合は論理的に分離し、JSTとの間で行われるべき通信が他の回線へ漏えいすること及びJST向け回線に不要な通信が入り込むことを防止する対策を施すこと。<br>インターネットVPNを用いる場合は、適切なアクセス制御、認証、暗号化を設定すること。通信には、あらかじめJST担当者が許可した固定IPアドレスを用いること。インターネットVPNとして用いる回線を、VPN確立のためではないインターネット宛ての通信に用いることは禁ずる。<br>請負者は利用する回線について、その種別、サービスレベル/セキュリティの担保に関する施策をあらかじめJST担当者に開示し承認を得ること。 | | 49 | サービスレベルを達成できる回線の構成が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 50 | 提案された回線が仕様書に適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2(2)ウ JST内への機器設置 | 15 | － | － | － | － | － | － | － | － | － | － | － |
| JST内へ請負者の機器を設置する必要がある場合は、その用途を明確にし、JST担当者の承認を得た上で行うこと。機器には所有者を明示すること。JST担当者がその機器にセキュリティ対策が必要と判断した場合は、適切な対策を施し、その内容について承認を得ること。 | | 51 | JST内への機器設置について、提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 52 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2(3) 当該業務内容 | 15 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は次の業務を実施すること。<br>各業務でJST担当者への連絡を実施した場合は、その日時と連絡した内容を記録すること。その記録を月次報告書に記載すること。 | | 53 | 業務連絡について、提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 54 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2(3)ア セキュリティ監視業務 | 15 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は次の業務を実施すること。<br>各業務でJST担当者への連絡を実施した場合は、その日時と連絡した内容を記録すること。その記録を月次報告書に記載すること。 | | 55 | セキュリティ監視業務において、以下の(a)～(c)が提案書に記載されていること。<br>(a) 体制図（人員及びその技術スキル、設備、交代スケジュール）<br>(b) 当該業務をサービスとして実施する場合は、そのサービス内容（カタログ等）<br>(c) 業務の一部を再委託する場合は、再委託先についても上記(a)(b)を記載すること。 | | | | － | － | － | － | － | － |
| | | 56 | セキュリティ監視フローが提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 57 | インシデント対応フローが提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 58 | セキュリティ)監視は全て契約期間中24時間体制で実施することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | 59 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | | | 評価項目 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 評価項目番号 | 必須項目 | | | | 加点項目 | | | | | |
| 内容 | | | | | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○ × | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 S A B C |
| 2 | (3) | ア | ① セキュリティログの監視<br>請負者はセキュリティ監視機器が出力するすべてのログを常に受信し、JSTにとっての危険度が高いものを検出すること。危険度は次のように定義する。<br><br>危険度3 既知のマルウェアが侵入している、公開サーバのコンテンツ等が書き換わっている、又は何らかの情報が漏えいしており緊急対応が必要である<br>危険度2 危険度3の状態であると確認はできていないが、その可能性が高く、早急な確認が必要である<br>危険度1 攻撃が成功した可能性は低いが、経過を観察する必要がある<br>危険度0 問題ない通信とは言い難いが、直ちに対応の必要はない<br><br>すべてのログとは、東京本部設置機器については以下のすべてである。<br>●IPS機能付きファイアウォール#1とIPS機能付きファイアウォール#2が出力する検知したIPSイベントのログ<br>●IPS機能付きファイアウォール#1とIPS機能付きファイアウォール#2が出力する通過した、又は遮断した通信のログ<br>●IPS機能付きファイアウォール#2が出力するアンチウイルス機能、URLフィルタ機能、サンドボックス機能が検知したイベントのログ<br>●WAFが出力するWebサーバへの接続ログ及び遮断した通信のログ<br>●アンチウイルスソフトウェア管理サーバが出力する検知したマルウェアのログ<br>●認証サーバが出力する認証の成否等に関するログ<br>●DNSサーバが出力するDNS問い合わせの内容に関するログ<br><br>日本科学未来館設置機器については次である。<br>●IPS機能付きファイアウォールが出力する検知したIPSイベントのログ<br>●IPS機能付きファイアウォールが出力する通過した、又は遮断した通信のログ<br>●IPS機能付きファイアウォールが出力するアンチウイルス機能、URLフィルタ機能、サンドボックス機能が検知したイベントのログ<br>●アンチウイルスソフトウェア管理サーバが出力する検知したマルウェアのログ<br>●認証サーバが出力する認証の成否等に関するログ<br>●DNSサーバが出力するDNS問い合わせの内容に関するログ<br><br>いずれでもすべてのログを監視の対象とすること。部分的としてはならない。これらのログを少なくとも次の観点ではリアルタイムに分析し、危険度に応じた対応を行うこと。<br>●各ファイアウォールが出力するログの中に、悪意があるホストとの通信がないか<br>●各ファイアウォールやIPS機能が出力するログに、攻撃キャンペーン（攻撃者が侵入・潜伏しようする一連の活動）との関連性が高いものがないか<br>●各ファイアウォールやIPS機能が出力するログで、特定の通信先に関するものが急増していないか<br>●サンドボックス機能がマルウェアと判定したファイルがないか（「2(3)ア② サンドボックスが検出したマルウェアの分析」）<br>●アンチウイルスソフトウェア、URLフィルタ、サンドボックス機能などが検出しているファイルの中に、攻撃キャンペーンで使用しているものがないか<br>●認証サーバに対する認証要求が急増していないか。特権アカウントの認証失敗が多数ないか<br>●DNSサーバに対する悪意があるホストの名前解決要求や、DNSトンネリングのようなプロトコルの正常な振る舞いを装った通信が発生していないか<br><br>請負者はログを世界中から収集した最新の脆弱性情報、マルウェア情報、悪意のある通信先情報、攻撃者情報、攻撃手法情報と統合し、相関的な分析を行うこと。それにより、機器単一のログを調査するだけではわからない侵入、マルウェアへの感染、改ざん、情報の流出等の攻撃を検出すること。分析に用いるルールを随時更新し、可能な限りゼロデイ攻撃と標的型攻撃も検出すること。ログの上では遮断できている攻撃やマルウェアであっても、それが遮断できなかった攻撃等が2次的に引き起こした可能性も考慮すること。<br>危険度0～3までの全ての事象に関してJSTに報告すること。報告には以下の内容を含めること。なお、トラフィックログなど接続・遮断に関する情報のみ記録されるものについてはJSTと協議の上で事象毎の報告内容を定めること。<br><br>・検出日時<br>・検出対象<br>・分析結果<br>・推奨する対処方法<br><br>危険度3又は危険度2のログを検出した場合は、「2(3)ア③ セキュリティインシデントへの対応」を行うこと。 | | | | 60 | セキュリティログの監視業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 61 | セキュリティ監視機器のログや通信内容及び収集した情報を総合し相関的に分析して、ゼロデイ攻撃や標的型攻撃といった未知の攻撃を、検出する方法が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 62 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 内容 | 頁 | 評価項目番号 | 必須項目 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○ × | 加点項目番号 | 加点項目 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 S A B C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 (3) ア ② サンドボックスが検出したマルウェアの分析<br>サンドボックス機能がファイルを評価した結果は、専用のWebサイトでその詳細を確認できる。サンドボックス機能が出力したログにファイルをマルウェアと判定するものがあり、かつアンチウイルスソフトにより駆除が行われていない場合は、請負者はそのWebサイトを用いて、本当にマルウェアであるかどうかをログ受信後原則30分以内に独自に判定すること。それが難しい場合は中間報告を実施すること。なお、そのサイトではファイル自体のダウンロードも可能であるため、必要であればダウンロードを実施してよい。ただし、そのファイルを請負者の外に送ることは禁ずる。<br>WebサイトのURLとログインに必要な情報は、受注後に開示する。<br>サンドボックス機能の判定の通りマルウェアであると判断した場合は、危険度3として「2(3)ア③セキュリティインシデントへの対応」を行うこと。マルウェアではないと判断したファイルがJSTドメインの公開サーバ上で見つかっている場合、ファイアウォールのメーカーに判定変更を要求する手続を実施すること。この手続の対象とするJSTのドメインと、手続の詳細は開示資料に記す。 | | 63 | サンドボックスが検知したマルウェアの分析業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 64 | セキュリティ監視機器のログや通信内容及び収集した情報を総合し相関的に分析して、ゼロデイ攻撃や標的型攻撃といった未知の攻撃を、検出する方法が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 65 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) ア **③ セキュリティインシデントへの対応**<br>請負者はセキュリティインシデント発生時には、被害の拡大防止を最優先とすること。<br>危険度3の事態発生時には、請負者はJST担当者の判断を仰ぐことなく、30分以内に問題のPC等又はサーバの通信を遮断する措置をとること。これは基本的にはPCの場合はアンチウイルスソフトウェア管理サーバで該当PCのネットワークからの隔離を、公開サーバの場合は負荷分散装置で対象サーバの分散先からの除外とファイアウォールでの通信遮断を行うこととする。これらの手順は開示資料に記す。対応実施後は速やかにJST担当者に連絡し、検出したログの内容、日時、攻撃の種類、確認できている被害、被害IPアドレスと加害IPアドレス、推奨する対応等を明確に説明すること。<br>危険度2のインシデントの場合は、その検出後30分以内にJST担当者に連絡し、遮断対応の要否を確認すること。遮断実施の判断になった場合は、その後30分以内に前述のものと同様の遮断対応を完了すること。<br>なお、JST担当者が独自に危険度3又は2の発生を検知し請負者に申告することがある。請負者はそれを受け、JST担当者が提示する情報を基に30分以内に前述の遮断対応を完了すること。さらに、JST担当者と協調して攻撃の詳細を調査し、被害の拡大防止のために推奨する対応等を助言すること。<br>これらの対応は月に2回を想定している。 | | 66 | セキュリティインシデントへの対応業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 67 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) ア **④ 特に重要なインシデント発生時の現場対応**<br>JST担当者は、特に重要なセキュリティインシデント発生時には請負者にJST内でのサポートを要請する。請負者はそれに応じ適切なスキルを持った人員2名程度を手配して「1(2)エ 業務実施場所」に記載の場所でインシデントの調査、被害拡大防止、証拠保全等のサポート業務に従事させること。1回あたりの期間は全員の合計で64時間とする。このサポート業務の開始は平日の日中とするが、状況により夜間及び休日におよぶ可能性がある。<br>この対応は1年に2回を想定している。 | | 68 | 特に重要なインシデント発生時の現場対応業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 69 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) ア **⑤ IPアドレスブラックリストの登録**<br>請負者は様々な情報源から独自に収集した最新のIPアドレス評価情報を基に、各平日に1回通信を遮断するべきIPアドレスリストを更新し、そのリストが含むIPアドレスとの通信を遮断するようJST担当者が指定する機器に設定を行うこと（ただし、遮断すべきIPアドレスリストに更新が発生しなかった場合は、対象機器への設定は不要）。また、通信遮断設定が行われているがその必要がなくなったIPアドレスについては、精査した上でリストからの削除を行うこと。これらの設定手順は開示資料に記す。<br>請負者はIPアドレスの評価情報を複数の情報源から得て、それらから適切に遮断すべき又は遮断の必要がなくなったIPアドレスのリストを作成すること。JST担当者から遮断対象のIPアドレス追加の依頼があった場合は、それも遮断対象に含めること。<br>JST担当者からIPアドレスの遮断設定削除の依頼があった場合は、そのIPアドレスの通信先としての危険度を評価し、十分低いと判断した場合はその対応を行うこと。評価の結果によらず、その判断の根拠をJST担当者に説明すること。 | | 70 | IPアドレスブラックリストの登録業務が提案書に具体的に記載されていること。 | | | | 加6 | 遮断すべきIPアドレスの更新と対象機器への反映は頻度が高いことが望ましいため、IPSで通信拒否する設定の実施頻度を上げるための方策が提案されている場合、加点とする。 | | | 50 | |
| | | 71 | IPアドレスの評価情報について、以下の(a),(b)が提案書に具体的に記載されていること。<br>(a) 情報収集ソースや収集頻度、収集量、内容<br>(b) 情報の評価方法 | | | | － | － | － | － | － | － |
| | | 72 | 仕様書内容を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) ア **⑥ 脆弱性情報の報告**<br>請負者はJST担当者が指定する機器やソフトウェアについて広く脆弱性に関する情報を収集し、注意を要するものがあれば電子メールで遅滞なく報告すること。報告対象は開示資料に記す。 | | 73 | 脆弱性情報の報告業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 74 | 以下の(a),(b)が提案書に具体的に記載されていること。<br>(a) 情報収集ソース（サイト）や収集頻度、収集量、内容<br>(b) 収集した情報を当該業務で活用するための体制 | | | | － | － | － | － | － | － |
| | | 75 | 業務仕様を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) ア **⑦ 脆弱性情報に基づくサーバの緊急公開停止**<br>請負者は収集している脆弱性情報の中に、JST担当者が指定するWebサイトが該当するものを発見した場合、その影響度を評価すること。評価の結果が情報漏えいやWebサイトの改ざん、利用者の通信内容盗聴などがすぐにでも発生する可能性が高いとなった場合は、JST担当者の判断を仰ぐことなく速やかにWebサイトを公開停止とする対応を実施すること。その手順は開示資料に記す。対応実施後はJST担当者に連絡し、脆弱性の内容や停止したWebサイトなどを明確に説明すること。緊急性が高くない場合は、JST担当者に連絡し、公開停止の要否を確認すること。いずれの場合も、該当の脆弱性情報の公表から1日以内にこれらの対応を完了させること。<br>Webサイトが脆弱性の影響を受けるかどうかの判断には、各サーバのインストール済みソフトウェアバージョン一覧を得るJSTが導入している仕組みを使った結果も加味すること。その利用方法は開示資料に記す。 | | 76 | 脆弱性情報に基づくサーバの緊急公開停止業務が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| | | 77 | 業務仕様を理解し且つ適合していると判断できること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | | | 評価項目 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 必須項目 | | | | | 加点項目 | | | | | |
| 内容 | | | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定〇× | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定SABC |
| 2 (3) イ | 納品物の作成 | | 20 | － | － | － | － | － | － | － | － | － | － | － |
| | 請負者は「1(4) 納品・検収要件」に定める通り納品物を納めること。各納品物の内容は次に従うこと。 | | | 78 | 納品物の品目が提案書に具体的に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) イ | ① 計画書<br>当該業務スケジュール、体制、連絡窓口、会議体等、セキュリティログ監視及び機器の設定手順等を明確に記すこと。体制では責任者を明確にすること。当該業務において有用な資格等を保持している要員については、それを付記すること。再委託を行っている場合は「1(5)ア 再委託」に定める内容も記載すること。また、作成した計画書、運用手順書、報告書等の作成と更新及び承認等についての文書・記録管理手順と、JSTからの貸与品の管理手順も含めること。契約期間中、計画書は適宜修正すること。 | | | 79 | 仕様に従い計画書を作成することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 80 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) イ | ② 情報システムセキュリティ管理手順書<br>請負者の当該業務実施環境について、JSTの情報セキュリティポリシーに従い管理手順書を作成すること。作成にあたっては、請負者が希望すれば2017年10月から契約中の「JSTセキュリティ監視運用業務」において、その請負者が納品したものをひな形として貸与する。 | | | 81 | 仕様に従い仕様書情報システムセキュリティ管理手順書を作成することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) イ | ③ 日次報告書<br>当該日のセキュリティ監視に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。<br>・セキュリティインシデントが発生している場合はその状況<br>・各セキュリティ監視機器が出力したログの統計情報(全ログ件数、ファイアウォールのポリシーによって遮断した通信の上位10位以内、IPSで検知しているイベントの上位10位以内、WAFが検知しているイベントの上位10位以内)<br>・サンドボックス機能がマルウェアと判定したファイルがあった場合は、その解説(「2(3)ア② サンドボックスが検出したマルウェアの分析」で行った対応、独自に行った判定の根拠、メーカーへの判定変更手続を行った場合はその状況を含めること)<br>・アンチウイルスソフトウェアがマルウェアと判定したファイルがあり、注意事項又は何らかの推奨する対応がある場合は、その内容<br>・特筆すべきログがある場合はその解説(ログの意味、注意を要する理由、推奨する対応を含めること) | | | 82 | 仕様に従い日次報告書を作成することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 83 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) イ | ④ 月次報告書<br>当該月の当該業務に関する次の情報を含めること。統計情報は、東京本部と日本科学未来館で分けて集計すること。<br>・実施した当該業務の内容とかかった工数（「1(3)ア 工数・課題管理」）<br>・課題管理表（「1(3)ア 工数・課題管理」）<br>・サービスレベル報告。「3(1) サービスレベル」に定めるサービスレベルと比較し、実績がどうであったかを報告すること。逸脱している項目については改善計画を立案し、その内容を記すこと<br>・当該月の日次報告書の内容をまとめたもの<br>・当該月全体でのセキュリティログの統計情報<br>・当該月のログの傾向や、請負者が収集している様々な情報を総合して分析した結果から導出したJST全体のセキュリティレベル評価。それが十分なレベルでないならば、その原因と推奨する対策 | | | 84 | 仕様に従い月次報告書を作成することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| | | | | 85 | 業務仕様を理解し且つ適合していることが提案書から判断できること。 | | | | － | － | － | － | － | － |
| 2 (3) イ | ⑤ 改善提案書<br>当該業務のあらゆる面からコスト削減、効率向上、統制とセキュリティ強化等の改善が可能な点を洗い出し、その改善案を提示すること。改善案には実施した場合の効果と、実施にかかる費用の概算も記すこと。 | | | 86 | 仕様に従い改善提案書を作成することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) ウ | その他の業務 | | 21 | － | － | － | － | － | － | － | － | － | － | － |
| | ① 問い合わせ対応<br>請負者は納品物及び当該業務に関すること並びに脆弱性、マルウェア、攻撃者及び攻撃手法等のセキュリティに関するJST担当者からの問い合わせに回答すること。一次回答は1営業日以内に行うこと。<br>問い合わせは1年に40回程度を想定している。 | | | 87 | 仕様に従い問い合わせ対応を実施することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) ウ | ② ログの調査<br>請負者はJST担当者からの依頼に基づき、受信しているセキュリティログの調査を行うこと。回答は2営業日以内に行うこと。これは主に指定する宛先への通信が指定する期間に行われていたかどうか、行われていたとしたらいつ、どの送信元からだったのかの調査などである。調査対象となるログは6ヶ月前までとする。この調査依頼は月に2回程度の発生を想定している。 | | | 88 | 仕様に従いログの調査を実施することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) ウ | ③ 停電対応<br>当該業務の対象機器がある東京本部と日本科学未来館のビルは、例年それぞれ2月と12月に電気設備法定点検が行われる(実施時期は変わり得る)。これによる停電時に、請負者が持ち込んだ機器に何らかの作業が必要になる可能性がある。その場合は、請負者の負担で適切に対応を行うこと。 | | | 89 | 仕様に従い停電対応を実施することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 2 (3) ウ | ④ 月次報告会<br>請負者は毎月の6営業日以降10営業日以内又はJST担当者と同意した日に、前月の月次報告書を説明する会を開催すること。9月と3月に開催の報告会では改善提案書についても説明すること。報告会の質疑応答の内容には議事録を作成し、報告会の3営業日後までにJST担当者に送付すること。 | | | 90 | 仕様に従い月次報告会を実施することが提案書に記載されていること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 内容 | 頁 | 評価項目 必須項目 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○× | 評価項目 加点項目 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 SABC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 サービスレベル及びその他の要件 | 23 | － | － | － | － | － | － | － | － | － | － | － |
| (1) サービスレベル | 23 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務について、運用支援の効率化、品質向上及び円滑化を図るため、下記に示す「表 3 サービスレベル」に対してサービスレベルアグリーメントを締結すること。請負者はこれらの遵守のため、常に各項目を測定、記録し、サービスレベルが適切な範囲に収まっているかを確認すること。下記の目標値は、天災や大規模停電等による障害及び計画停止の場合は除く。<br>提案時点でこれらの達成が困難であると判明している場合(定期的な保守業務によりログの監視ができない時間帯が存在するなど)は、請負者は困難である項目それぞれについて、提案書に目標値とどの程度の乖離が生じるのかを明確に記すこと。 | | 91 | サービスレベルの各項目毎に<br>・目標値を遵守すること<br>・遵守するための方法<br>が提案書に明確に記載されていること。 | | | | － | － | | | － | － |
| | | 92 | サービスレベルの項目の一つである「セキュリティログ保存損失」の目標達成のための方策が提案されていること。<br>目標値：保存しているセキュリティログの損失を少なくとも6ヶ月分を損失0%に抑えること | | | | 加7 | サービスレベルの項目の一つである「セキュリティログ保存損失」の削減のための方策が多く提案されていること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 10 | |
| | | 93 | サービスレベルの項目の一つである「納品物の納期遵守」のための方策が提案されていること。<br>目標値：納品物の納期遵守率を100%にすること | | | | － | － | － | － | － | － |
| | | 94 | サービスレベルの項目の一つである「セキュリティログ受信損失」の目標達成のための方策が提案されていること。<br>目標値：請負者による分析が行われずに失ったセキュリティログの時間の割合を0.01%（月に5分以内のログ損失）に抑えること。 | | | | 加8 | サービスレベルの項目の一つである「セキュリティログ受信損失」の損失削減のための方策が多く提案されていること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 10 | |
| | | 95 | サービスレベルの項目の一つである「サンドボックスが検出したマルウェアの確認時間」の目標達成のための方策が提案されていること。<br>目標値：サンドボックスでのマルウェア検出のログを受信してから独自の分析を完了するまでの時間を30分以内にすること。 | | | | 加9 | 「サンドボックスが検出したマルウェアの確認時間」の判断時間削減のための方策を提案していること。セキュリティに関する最新の動向や技術をマルウェアの判断方法に随時活かすための方策を多く提案していること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 50 | |
| | | 96 | サービスレベルの項目の一つである「危険度3のセキュリティインシデント発生時の初動対応」の目標達成のための方策が提案されていること。<br>目標値：危険度3のセキュリティインシデント発生時に、その検知から通信遮断対応を完了するまでの時間を30分以内にすること。 | | | | 加10 | サービスレベルの項目の一つである「危険度3のセキュリティインシデント発生時の初動対応」の時間削減のための方策が多く提案されていること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 50 | |
| | | 97 | サービスレベルの項目の一つである「危険度2のセキュリティインシデント発生時の初動対応」の目標達成のための方策が提案されていること。<br>目標値：危険度2のセキュリティインシデント発生時に、その検知からJST担当者に連絡を行うまでの時間を30分以内にすること。および遮断対応実施の判断からその実施完了までの時間を30分以内にすること。 | | | | 加11 | サービスレベルの項目の一つである「危険度2のセキュリティインシデント発生時の初動対応」の時間削減のための方策が多く提案されていること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 50 | |
| | | 98 | サービスレベルの項目の一つである「JST担当者からのセキュリティインシデント発生の申告を受けてからの初動対応」の目標達成のための方策が提案されていること。<br>目標値：JST担当者からのセキュリティインシデント発生の連絡受付後に、遮断対応を完了するまでの時間を30分以内にすること。 | | | | 加12 | セキュリティインシデント発生時に、適切なスキルを持った人員を手配するための方策や請負者が持っているサービス体制に関する工夫を多く提案していること。提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 50 | |
| | | 99 | サービスレベルの項目の一つである「脆弱性情報に基づくサーバの緊急公開停止」の目標達成のための方策が提案されていること。<br>目標値：脆弱性情報公表後からサーバの緊急公開停止を実施しJST担当者に連絡するまで、又はJST担当者に連絡し指示のあった対応を実施完了するまでの時間を1日以内にすること。 | | | | 加13 | セキュリティに関する最新の動向や技術をサーバ停止をする条件に生かし、サーバ停止を速やかに実施する方策を多く提案していること。<br>提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 50 | |
| | | 100 | サービスレベルの測定方法が提案書に具体的に記載され、かつ適切であること。 | | | | | | | | | |
| | | 101 | サービスレベルの実績（達成状況）及び適正な範囲に収まらなかった項目の改善計画を月次報告書の中に記すことと、月次報告会においてJST担当者に報告することが提案書に記載されていること。 | | | | － | － | － | － | － | － |
| 3 (2) セキュリティ要件 | 24 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は、以下の情報セキュリティ管理事項を遵守すること。 | | － | － | － | － | － | － | － | － | － | － | － |
| 3 (2) ア 要求事項 | 24 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者はJSTの「情報システムに関する情報セキュリティ対策ガイドライン(委託先用)」に準拠して当該業務を実施すること。同ガイドラインは開示資料として閲覧できる。また、当該業務のセキュリティに責任を持つセキュリティ管理責任者を設定し、その責任と権限を明確化すること。 | | 102 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) イ 管理対象 | 24 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は次のすべてに対しセキュリティ管理を実施すること。<br>・当該業務の対象機器及びそれらの設定情報<br>・請負者(及び再委託者がある場合は再委託者)の当該業務環境<br>・要員<br>・設備、場所<br>・ドキュメント類(手順書、マニュアル等)<br>・各種台帳<br>・業務データ(ログ、分析結果及び課題管理表など)<br>・貸与品 | | 103 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) ウ 管理全般 | 24 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者は各管理対象に対し、重要性・情報の区分に応じた管理方法を定めること。請負者内部のセキュリティ管理で用いている監視・連絡体制図をJSTに提示し、管理が十分遂行できることを証明すること。管理状態の定期的な点検又は監査を実施し、JSTに報告すること。当該業務の要員に対してはセキュリティに関する教育等を実施し、その状況を管理台帳に記録すること。 | | 104 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) エ セキュリティ管理内容 | 25 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者はJSTの情報セキュリティポリシー等に準じて業務を実施すること。特に下記事項を確実に実施すること。それぞれの事項についてその内容をあらかじめ又は変更時にJSTに開示し、了承を得ること。 | | 105 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | | 評価項目 | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 必須項目 | | | | 加点項目 | | | | | | |
| 内容 | | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定〇× | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定SABC |
| 3(2)オ 変更管理 | | 25 | － | － | － | － | － | － | － | － | － | － | － |
| 設定変更等の作業は、あらかじめ決めた要員のみが実施すること。<br>変更管理表を作成し、現在の状態及び変更履歴を記録すること。<br>作業は作業者と確認者の複数名体制で行うこと。 | | | 106 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3(2)カ 情報受渡し | | 25 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者とJST担当者間で設定情報等の機密情報を受け渡す時は、第三者が容易に閲覧できないよう、暗号化やパスワード認証を施した情報の受渡し方法をとること。受渡しの際には、最新のパターンファイルを実装したアンチウイルスソフトウェアによるチェックを行うこと。<br>要員が作業等のため機密情報を外部へ持ち出す際は、セキュリティ管理責任者の承認を得て管理台帳に記録し、暗号化、パスワード設定等のセキュリティ対策を施すこと。管理台帳はJST担当者からの求めに応じ開示すること。<br>ログ情報は海外に開示しないこと。海外での調査・分析が必要な場合は、送付する情報やそのタイミングについてJST担当者へ事前に連絡し、了承を得ること。その場合もデータ暗号化等のセキュリティ対策を施すこと。 | | | 107 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3(2)キ 当該業務実施場所 | | 25 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者の当該業務を実施する場所は、認証装置により入退室を制限・記録できる機構を有すること。また、請負者以外の他者とは完全に入退室を分離し、物理的に隔離していること。 | | | 108 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3(2)ク 使用機器 | | 26 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務に使用する機器は、作業者以外が使用することがないよう、権限の付与、取消しについて管理を行い、他の者の操作を禁止すること。<br>機器からは外部記憶媒体に書き込みのできる不要なデバイスを取り外すこと。プリンタを設置する場合は必要最小限の台数とし、利用者を制限すること。<br>当該業務で使用するPCは、以下の事項を遵守すること。<br>・すべて管理台帳で管理すること<br>・他の業務と兼用しないこと。私的利用をしないこと<br>・利用開始の前にアンチウイルスソフトウェアによるスキャンを実施すること<br>・当該業務に必要のないソフトウェアはインストールしないこと<br>・OSとインストールしているソフトウェア、アンチウイルスソフトウェアのパターンファイルを最新の状態に保つこと<br>・利用中に一定時間操作がなければロックし、その解除に認証を求める設定とすること<br>・盗難防止策を施すこと | | | 109 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3(2)ケ 可搬型外部記憶媒体 | | 26 | － | － | － | － | － | － | － | － | － | － | － |
| 当該業務に可搬型外部記憶媒体(USBメモリ、DVD等)を利用する場合は、それらの管理台帳を作成し、本業務専用として管理すること。媒体は施錠可能なキャビネットなどに保管すること。利用する際は日時、利用者、媒体を識別する名称等を記録すること。データの書き込み時には暗号化を施し、読み取り時にパスワードを求めるようにすること。当該業務外での利用と外部への持ち出しは厳禁とする。<br>月に1回は棚卸しを行い、万が一紛失等が発生した場合は速やかにJST担当者に報告すること。<br>不要になった場合又は契約満了時には内容の読み取りを不可能に処理した上で廃棄すること。 | | | 110 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3(2)コ 目的外使用の禁止 | | 26 | － | － | － | － | － | － | － | － | － | － | － |
| 請負者が当該業務で使用するあらゆるデータは、本契約の目的以外に使用しないこと。契約終了時には確実に削除すること。 | | | 111 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 | | | | 評価項目 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 必須項目 | | | | | 加点項目 | | | | | | |
| 内容 | | | 頁 | 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○ × | 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 S A B C |
| 3 (2) | サ | ID・パスワード管理 | 27 | － | － | － | － | － | － | － | － | － | － | － |
| | | 当該業務で使用する操作端末ごとに管理者名、使用者名、それらの利用権限、担当作業内容及びIDを管理台帳で管理すること。権限を一人に集中させすぎないように、かつ必要以上の要員に権限を付与しないこと。IDの追加、削除又は権限の変更時にセキュリティ管理責任者が承認するルールを定め、その内容をJSTに報告すること。<br>不要なIDは速やかに削除すること。デフォルトで存在するIDは使用する必要がなければ削除又は無効化すること。それができなければパスワードを適切に設定し、可能であればさらにID名を変更すること。<br>IDは個人ごとに付与し、作業担当者変更（追加、減少を含む）の際には、記録を残すこと。当該業務を担当しなくなった作業担当者のIDは速やかに削除し、同一IDの引継ぎは行わないこと。複数の使用者によるID共有は原則禁止するが、システム的に実現が不可能であれば、共有するIDを実際にはだれが利用したのかを記録すること。IDを共有している作業担当者に変更があった場合は、必ずパスワードの変更を行うこと。<br>IDは半年に1回以上棚卸しを行い、結果を報告すること。<br>当該業務で使用するパスワードは原則13文字以上、英小文字、英大文字、数字、記号の複合（4種類が望ましいが最低限3種類）であること。また、複数の使用者により共有しているIDについては、90日ごとにパスワードを変更すること。パスワード更新を強制的に行う仕組みがなければ、更新期間の管理を管理台帳で行うこと。<br>当該業務で使用するパスワードを操作端末に記憶させないこと。他システム、他サービスで使用しているIDとパスワードの組合せは使わないこと。 | | | 112 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) | シ | 情報管理 | 27 | － | － | － | － | － | － | － | － | － | － | － |
| | | 当該業務に関するドキュメントや媒体等は、管理台帳により管理し、施錠可能なロッカー等に保管すること。 | | | 113 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) | ス | 業務データ管理 | 27 | － | － | － | － | － | － | － | － | － | － | － |
| | | 当該業務に関するデータは国内に保持すること。 | | | 114 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) | セ | 守秘義務 | 27 | － | － | － | － | － | － | － | － | － | － | － |
| | | 請負者は当該業務の内容及び当該業務に関連して開示を受けた、又は知り得た相手方の技術的若しくは事業運営にかかる一切の情報(以下「機密情報」という)につき最大限の注意を払い秘密を保持すること。事前にJSTの書面による承諾を得ることなく、本業務の目的外で使用又は第三者に開示・漏えいしてはならない。<br>なお、請負者は自社の従業員のうち本業務に従事する従業員にのみ機密情報を開示するものとし、本業務に関与しない従業員には、いかなる手段においても一切機密情報を開示し又は使用させてはならない。また、本件の実施完了後は、本件に関する情報を返却又は確実に破棄すること。<br>本業務の提供により知り得たすべての事項については、契約期間中はもとより、契約終了後においても外部に漏らさず、機密保持のために十分な体制・設備で厳重に管理し、情報漏えいを確実に防止すること。<br>本業務の提供において知り得た情報が紛失や盗難等による第三者への情報漏えいの発生又はそのおそれがある場合は、速やかにJST担当者に電話、口頭等による連絡を行うとともに、書面で報告すること。また、直ちに事実調査を行い、漏えいした情報の内容、原因、再発防止策等について記載した書面をJST担当者へ提出し、事態の収拾及び拡大防止の措置を迅速かつ適切に行うこと。なお、請負者以外の者の作業も含め、対処にかかる費用はすべて請負者が負担すること。<br>請負者の設備や機器に保存しているログ情報は、JSTからの要請により削除可能であること。交換や撤去を行う際は、機器に残っているデータはすべて適切に消去すること。 | | | 115 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) | ソ | サプライチェーンリスク管理 | 28 | － | － | － | － | － | － | － | － | － | － | － |
| | | 請負者は本件で用いる機器について、その設計・製造・試験・納入・設置構築等の各工程において、意図しない変更や機密情報の窃取等の防止を、一貫した品質保証体制の下で行っている保証を、そのサプライヤーに求めていること。それを説明する書類(体制図、社内基準等)を、可能な範囲で提出すること。さらに、請負者は本件で用いる機器に意図しない変更が行われているなどの不正が見つかった時には、追跡調査や立入検査等によりJSTと連携して原因を調査し、排除するための手順及び体制を整備していること。それを説明する書類(体制図、社内基準等)を、可能な範囲で提出すること。<br>また、本件で用いる機器が、その保守等の目的で機器情報を収集する仕組み等を持つ場合、その手段、方式等をすべて明確にし、事前にJST担当者の承認を得ること。 | | | 116 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| 3 (2) | タ | 監査 | 28 | － | － | － | － | － | － | － | － | － | － | － |
| | | JST担当者は必要に応じ請負者に対し当該業務に関する監査を行う。請負者は監査に協力すること。対応のために多大な工数が必要な場合は、別途調整する。 | | | 122 | 仕様書内容を理解し且つ適合していることが提案書に具体的に示されていること。 | | | | － | － | － | － | － | － |
| | | | | － | － | － | － | － | － | － | － | － | － | － | － |
| | | 自由提案<br><br>仕様書にはないが、以下の点を考慮した有益な提案をした場合、加点を行う。<br><br>・JSTに特有の事情を勘案し、攻撃を未然に防ぐこと。<br>・JSTで扱っているセキュリティ機器で独自に分析を可能とするシグネチャなどを作成して本業務に生かせること。<br>・セキュリティ監視の品質を落とさず運用コストが下がること。 | | － | － | － | － | － | 加14 | より多くの有益な提案がされていること。提案内容が本業務のより効果的な実施に資すると判断できれば加算する。 | | | 100 | |

# 総合評価基準及び対応表（案）

別添３

| 仕様書等 内容 | 頁 | 評価項目 必須項目 評価項目番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 判定 ○× | 加点項目 加点番号 | 評価の観点 | 提案書の該当頁 | 関連資料の該当頁 | 配点 | 判定 SABC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ワーク・ライフ・バランス等の推進に関する取り組み | | － | － | － | － | － | － | － | － | － | － | － |
| ワーク・ライフ・バランス等の推進に関する取り組みについて、認定内容等により加点する。複数の認定等に該当する場合は、最も配点が高い区分により加点を行う。複数の項目に該当する場合は、最も配点が高い区分により加点を行う。 | | － | － | － | － | － | 加15 | 女性の職業生活における活躍の推進に関する法律（平成27年法律第64号）（女性活躍推進法）に基づく認定（えるぼし認定を受けている場合、段階によって加点する。<br>1段階目（※①）：10点<br>2段階目（※①）：15点<br>3段階目：20点<br>※①　労働時間等の働き方にかかる基準は満たすこと。 | | | 20 | |
| | | － | － | － | － | － | 加16 | 女性の職業生活における活躍の推進に関する法律（平成27年法律第64号）（女性活躍推進法）に基づく行動計画を策定済みの場合、加点する。<br>※女性活躍推進法に基づく一般事業主行動計画の策定義務がない事業主（常時雇用する労働者の数が300人以下のもの）に限る（計画期間が満了していない行動計画を策定している場合のみ）<br>加点：10点 | | | | |
| | | － | － | － | － | － | 加17 | 次世代育成支援対策推進法（平成15年法律第120号）（次世代法）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）を受けている場合、加点する。<br>・くるみん（旧基準）（※①）：15点<br>・くるみん（新基準）（※②）：15点<br>・プラチナくるみん：20点<br>※①　旧くるみん認定マーク（次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29年厚生労働省令31号）による改正前の認定基準又は同附則第2条第3項の規定による経過措置により認定）<br>※②新くるみん認定マーク（次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29年厚生労働省令31号）による改正後の認定基準により認定） | | | | |
| | | － | － | － | － | － | 加18 | 青少年の雇用の促進等に関する法律（昭和45年法律第98号）（若者雇用促進法）に基づく認定を受けている場合、加点する。<br>加点：10点 | | | | |

判定（○×）が全て○のとき「合格」として基礎点　210 点付加　　加点は満点(配点×1．0)の場合　630 点付加

**別添４**

# ＪＳＴセキュリティ監視運用業務
# サービスレベルアグリーメント
# （案）

**令和元年６月**

国立研究開発法人科学技術振興機構

本書は、ＪＳＴセキュリティ監視運用業務として提供されるサービスの品質に対する要求水準を規定するとともに、規定した内容が適正に実現されるための運営ルールを、ＪＳＴと請負者の合意として明文化したものである。

## １．　前提条件

JST セキュリティ監視運用業務調達仕様書（以下、仕様書という）の
１.(2) 発注条件
１.(3) 当該業務条件
１.(4) 納品・検収条件
１.(5) その他前提条件
に示すとおりとする。

## ２．　業務の範囲

仕様書 2.当該業務要件に示すとおりとする。

## ３．　役割と責任の分担

個々の業務に関して、JST と請負者が果たす役割、実施責任の所在は以下表１のとおりとする。

表１．役割と責任の分担

| 仕様書における業務 | 請負者 | JST |
|---|---|---|
| 2.(3).ア セキュリティ監視業務 | | |
| ①セキュリティログの監視 | 監視実施<br>攻撃の成功またはその可能性が高い事象を検出時は JST へ連絡し、その内容、推奨する対応等を説明 | 説明を受けて請負者と対応を協議 |
| ②サンドボックスが検出したマルウェアの分析 | 分析実施<br>マルウェアと判断した場合は JST へ連絡しその内容、推奨する対応等を説明<br>マルウェアでなく且つ JST ドメイン公開サーバ上で見つかった場合は、判定変更手続きを実施 | 説明を受けて請負者と対応を協議 |
| ③セキュリティインシデントへの対応 | 対応実施 | 説明を受けて請負者と対応を協議 |
| ④特に重要なインシデント時の現場対 | 現場対応実施 | 説明を受けて請負者と対応を協議 |

| | | |
|---|---|---|
| 応 | | |
| ⑤IP アドレスブラックリストの登録 | 請負者が持つ情報を基に登録実施<br>依頼を受けて設定を変更 | 設定変更を依頼 |
| ⑥脆弱性情報の報告 | 報告実施 | ― |
| ⑦脆弱性情報に基づくサーバの緊急公開停止 | 対応実施 | 説明を受けて請負者と対応を協議 |
| 2.(3).イ 納品物の作成 | | |
| ①計画書<br>②情報セキュリティ管理手順書 | 作成し提出<br>適宜修正し再度提出 | ― |
| ③日次報告書<br>④月次報告書<br>⑤改善提案書 | 作成し提出 | ― |
| 2.(3).ウ その他の業務 | | |
| ①問い合わせ対応 | 対応実施 | 問い合わせ |
| ②ログの調査 | 調査実施 | 調査を依頼 |
| ③停電対応 | 対応実施 | 対応日を指示し依頼 |
| ④月次報告会 | 開催 | 開催日を指定 |

## ４．　サービスレベル

当該業務が目標とするサービスレベルを表２に示す。

下記の目標値は、天災や大規模停電等による障害及び計画停止の場合は除く。

表２．サービスレベル

| 項　目 | 目標値 | 内　容 | 業務の詳細<br>（調達仕様書の該当箇所） |
|---|---|---|---|
| セキュリティログ保存損失 | 少なくとも6ヶ月分を損失0% | 保存しているセキュリティログの損失 | 「1(2)キ 当該業務環境・ツール等」 |
| 納品物の納期遵守 | 100%納期遵守 | 納品物の納期遵守率 | 「1(4) 納品・検収要件」 |

| | | | |
|---|---|---|---|
| セキュリティログ受信損失 | 0.01%以下 | 請負者による分析が行われずに失ったセキュリティログの時間の割合。月に5分以内のログ損失 | 「2(3)ア① セキュリティログの監視」 |
| サンドボックスが検出したマルウェアの確認時間 | 30分以内 | サンドボックスでのマルウェア検出のログを受信してから独自の分析を完了するまでの時間 | 「2(3)ア② サンドボックスが検出したマルウェアの分析」 |
| 危険度3のセキュリティインシデント発生時の初動対応 | 30分以内 | 危険度3のセキュリティインシデント発生時に、その検知から通信遮断対応を完了するまでの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |
| 危険度2のセキュリティインシデント発生時の初動対応 | 30 分以内と30分以内 | 危険度2のセキュリティインシデント発生時に、その検知からJST担当者に連絡を行うまでの時間及び遮断対応実施の判断からその実施完了までの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |
| JST 担当者からのセキュリティインシデント発生の申告を受けてからの初動対応 | 30分以内 | JST 担当者からのセキュリティインシデント発生の連絡受付後に、遮断対応を完了するまでの時間 | 「2(3)ア③ セキュリティインシデントへの対応」 |
| 脆弱性情報に基づくサーバの緊急公開停止 | 1日以内 | 脆弱性情報公表後からサーバの緊急公開停止を実施しJST担当者に連絡するまで、又はJST担当者に連絡し指示のあった対応を実施完了するまでの時間 | 「2(3)ア⑦ 脆弱性情報に基づくサーバの緊急公開停止」 |

上記に記載の危険度の定義は下記の通り。

| | |
|---|---|
| 危険度3 | マルウェアが侵入している、公開サーバのコンテンツ等が書き換わっている、又は何らかの情報が漏えいしており緊急対応が必要である |
| 危険度2 | 危険度3の状態であると確認はできていないが、その可能性が高く、早急な確認が必要である |
| 危険度1 | 攻撃が成功した可能性は低いが、経過を観察する必要がある |
| 危険度0 | 問題ない通信とは言い難いが、直ちに対応の必要はない |

## 5． 結果対応および運営ルール

（1）請負者は、サービスレベルの遵守のため、常にサービスレベル項目を測定、記録し、サービスレベルが適切な範囲に収まっているかを確認する。

（2）請負者は、月次報告書において、サービスレベルの実績および適正な範囲に収まっていない項目については改善計画を立案しその内容を記す。

（3）請負者は、毎月の 6 営業日以降 10 営業日以内又は JST と同意した日に、前月の月次報告書を説明する会（以下、月次報告会という）を開催し、JST に対して報告する。

（4）JST と請負者は、月次報告会にて改善計画を協議し、サービスレベルが適切な範囲に収まるような方策をすみやかに実施する。

## 6．　サービスレベルアグリーメントの改定

「4.サービスレベル」で設定した項目、目標値、内容については、必要に応じて見直しを実施し改定するものとする。改定の契機は以下のとおりとする。

（1）JST 及び請負者双方の合意事項に明確な変更が生じた場合

（2）JST 及び請負者双方が必要と認めた場合

## 7．　サービスレベルアグリーメントに係る免責事項

以下の場合はサービスレベルアグリーメントの適用外とする。

（1）天災や大規模停電等による障害

（2）計画停止

（3）JST 及び請負者双方の協議の上で計測の除外とした場合