資料３

令和 4 年 1 月 21 日
国立研究開発法人科学技術振興機構

民間競争入札実施事業
「JST セキュリティ監視運用業務」の実施状況について

Ⅰ．事業の概要

国立研究開発法人科学技術振興機構（以下「当機構」という。）のセキュリティ監視運用業務(以下「本業務」という。）については、「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)」に基づき、平成 29 年度から公共サービス改革基本方針に従って民間競争入札を実施している。当該法律の下での事業の運用は、第 2 期目である。

１．委託業務内容

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行うものである。

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等、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。

２．業務委託期間

令和元年 11 月 20 日から令和 5 年 3 月 31 日(約 3 年 4 ヶ月)

３．受託事業者

富士通株式会社

４．実施状況評価期間

令和 2 年 4 月から令和 3 年 12 月までの 21 ヶ月間
※令和元年 11 月から令和 2 年 3 月までは本件監視運用業務のための準備期間のため対象外

５．受託事業者決定の経緯

「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」における民間競争入札

実施要項に基づき、入札参加者（2 者）から提出された提案書について、実施要項に定める評価委員会(令和元年 10 月 17 日開催)において審査した結果、2 者とも評価基準を満たしていた。入札説明会（令和元年 8 月 27 日及び 9 月 12 日の 2 回実施）には、合わせて 5 者の参加があった。

入札価格については、令和元年 11 月 6 日に開札した結果、予定価格の範囲内での応札であり、総合評価を行ったところ、「3. 受託事業者」に記載の者を落札予定者とした。

その後民間競争入札手続に則り、暴力団に係る欠格事項に当たらないことを確認して、令和元年 11 月 20 日付けで契約書を締結した。

Ⅱ. 達成すべき質の達成状況及び評価

民間競争入札実施要項において定めた民間事業者が確保すべきサービスの質の達成状況に対する当機構の評価は、下表のとおりであり、サービスの質は確保されている。

項目	目標値 内容	評価
納品物の納期遵守	目標値：100%納期遵守 納品物の納期遵守率	実施状況評価機関中の納品物納期厳守率は、99.5%である。 前日の監視状況を記した日次報告書の書面提出が遅れたことが 3 回あったが、緊急時の連絡等は別メール等で受けており業務としての問題は何もなかった。 なお、その都度、遅れた理由を確認して、改善方策を講じたことを確認済である。 よって、サービスの質は確保されている。
セキュリティログ受信損失	目標値：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	実施状況評価期間中のセキュリティログの受信損失の割合は、0.00%である。 よって、サービスの質は確保されている。
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	目標値： 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	実施状況評価期間中、当機構担当者からセキュリティインシデント発生の連絡を受けた時刻から、作業完了するまでの時間が 30 分を超えた回数は、0 回である。 よって、サービスの質は確保されている。 なお、実施状況評価期間中に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を受けて通信遮断に至った回数は 0 回である。
サンドボックスが検出したマルウェアの判断時間	目標値：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	実施状況評価期間中のサンドボックスのマルウェア検出ログを受信してから独自の分析を完了するまでの時間が 30 分を超えた回数は、0 回である。 よって、サービスの質は確保されている。

		なお、実施状況評価期間中にサンドボックスにてマルウェアを検出した回数は 307 回である。
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	目標値：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	実施状況評価期間中、危険度 3 のセキュリティインシデントは 1 回のみ発生し、当該 PC の通信遮断等の対応を行うまでの時間は 61 分であったが、以下の通り業務としての問題は何もなかった。 よってサービスの質は確保されている。 当該インシデントについてはマルウェアが検知されたメールを未読の状態で発見し削除したため、61 分かかったことによる被害等の影響は何もなかった。 30 分を超えた原因は、当機構が作成した手順書に従って PC 通信遮断の作業を実施すると約 1 時間かかるものとなっていたためであり、受注者の問題ではなかった。 現在は手順書の改訂を行い、それに基づき試行した結果、目標値である 30 分以内に対応完了できることを確認済である。
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	目標値：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	実施状況評価期間中、危険度 2 のセキュリティインシデント発生時に当機構担当者に連絡するまでの時間が 30 分を超えた回数は 0 回である。また、遮断対応実施の判断が決定してから通信遮断等の対応を行うまでの時間が 30 分を超えた回数は、0 回である。 よって、サービスの質は確保されている。 なお、実施状況評価期間中に危険度 2 のセキュリティインシデントの発生回数は 2 回であり、通信遮断に至った回数は 0 回である。
セキュリティログ保存損失	目標値：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	実施状況評価期間中、6 ヶ月以内のログを損失した期間(日)の割合は、0.00%である。 よって、サービスの質は確保されている。
脆弱性情報に基づくサーバの緊急公開停止	目標値：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	実施状況評価期間中、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が 1 日を超えた回数は 0 回である。 よって、サービスの質は確保されている。

	までの時間	なお、実施状況評価期間中にサーバ停止の緊急公開停止が発生した回数は 0 回である。

Ⅲ．実施経費の状況及び評価

１．今期の実施経費

第 2 期（令和元年 11 月 20 日から令和 5 年 3 月 31 日まで）の契約額

205,000,000 円（税抜　以下の金額もすべて税抜）…①

ただし上記金額には市場化テスト実施前（平成 28 年度）契約にはない以下の仕様が含まれている。

DNS ログの監視対象への追加　10,530,281 円　…②

脆弱性情報に基づくサーバの緊急公開停止　6,694,305 円　…③

また業務開始時の環境整備にかかる初期費用は

3,940,000 円　…④

以上より、業務実施のための経費（①から②③④を減じた額）は下記の通り。

183,835,414 円　…⑤

1 年当たりの金額は、下記の通り

⑤ ÷ 監視実施期間 3 年 ≒ 61,278,471 円（小数点以下切り下げ）…(a)

２．経費削減効果

市場化テスト実施前（平成 28 年 4 月 1 日～平成 29 年 3 月 31 日まで）の契約額

84,700,000 円　…⑥

ただし上記の金額には評価対象となる第 2 期契約にはない以下の仕様が含まれている。

ネットワーク機器の稼働監視・保守・運用　10,130,692 円　…⑦

また業務開始時の環境整備にかかる初期費用は

5,312,436 円　…⑧

以上より、業務実施のための経費（⑥から⑦⑧を減じた額）は下記の通り。

69,256,872 円　… (b)

経費削減効果は下記の通り。

削減額：(b)－(a)＝7,978,401 円　…(c)

削減率：(c)÷(b)≒11.5%（小数点第 2 位切り下げ）

３．評価

市場化テスト前（平成 28 年度）契約金額と比較して、1 年当たり 7,978,401 円（11.5%）削減できた。

Ⅳ．民間事業者からの提案による改善実施事項等

実施期間中に民間事業者から提出された改善提案に基づき、第 2 期において以下を実施した。

１．運用訓練の実施

「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」においてサーバの通信遮断は実施したことがなかったため、訓練としてサーバの通信遮断作業を実施し、民間競争入札実施要項において定めた民間事業者が確保すべきサービスの質を遵守できることを確認した。

２．脆弱性情報の改善

「脆弱性情報の報告」 として提供する脆弱性情報を、これまでの「監視対象機器のみ」から「脆弱性情報に基づくサーバの緊急公開停止の対象ソフトウェア」まで拡大した。

３．その他の業務改善

上記１および２以外に、第２期において以下（１）～（６）に示す業務改善を実施した。

（１）日次報告書、月次報告書への掲載項目の追加、説明文言を見直した。

（２）セキュリティインシデント発生時の当機構への通知内容を見直した。

（３）IP アドレスブラックリスト登録における登録項目（連絡先）を追加した。

（４）セキュリティログの受信経路を見直して短縮した。

（５）何らかの原因によりログが届かなかった場合に迅速に対応できるよう、当機構へのログ再送依頼の手順を見直した。

（６）セキュリティログサーバ障害時の対応時間短縮、作業ミス防止を目的としてセキュリティログサーバ主従切替を自動化した。

Ⅴ． 全体的な評価

達成すべき質については、Ⅱに記載の通り、サービスの質は確保されている。

実施経費については、Ⅲに記載の通り、市場化テスト実施前（平成 28 年度）に比べて経費削減効果がみられた。

Ⅵ. 今後の事業

１． 事業の実施状況

本事業への市場化テスト導入は今期が２期目であるが、事業全体を通した実施状況は以下のとおりである。

① 実施期間中に受託民間事業者が業務改善指示等を受ける、あるいは業務に係る法令違反行為等を行った事案はなかった。

② 当機構には、監事及び外部有識者で構成され、契約の点検・見直し等を行う「契約監視委員会」が設置されており、その枠組みの中で実施状況報告のチェックを受ける体制が整っている。

③ 本事業入札においては二者からの応札があり、競争性は確保されていた。

④ 対象公共サービスの確保されるべき質に係る達成目標について、目標を達成している。

⑤ 経費について、市場化テスト実施前（平成 28 年度）と比較し、1 年当たり 11.5%の経費削減効果があった。

２．次期事業の実施

以上のとおり、本業務については、総合的に判断すると良好な実施結果を得られていることから、次期事業においては「市場化テスト終了プロセス及び新プロセス運用に関する指針」（平成26 年 3 月 19 日官民競争入札等監理委員会決定）に基づき、終了プロセスへ移行した上で、自ら公共サービスの質の維持と経費削減を図っていくこととしたい。

以　上