請負についての入札公告

国立大学法人大阪大学において、次のとおり一般競争入札に付します。

１．調達内容

（１） 件名　　大阪大学総合情報通信システム(ODINS) 休日等におけるセキュリティ対応業務

（２） 履行期間　　令和５年４月１日～令和６年３月３１日

（３） 履行場所　　国立大学法人大阪大学（吹田キャンパス）または大阪大学総合情報通信システム（以下、「ODINS」という）への通信制御が可能な場所

（４） 入札方法

落札決定に当たっては、入札書に記載された金額に当該金額の１０パーセントに相当する額を加算した金額（当該金額に１円未満の端数があるときは、その端数金額を切り捨てるものとする。）をもって落札価格とするので、入札者は、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、見積もった契約金額の 110 分 の 100 に相当する金額を入札書に記載すること。

２．競争参加資格

（１）国立大学法人大阪大学契約規則第７条及び第８条の規定に該当しない者であること。

（２）国の競争参加資格（全省庁統一資格）又は、国立大学法人大阪大学の競争参加資格のいずれかにおいて、令和５年度に近畿地域の「役務の提供等」の A、B、C 又は D の等級に格付けされている者であること。

（３）本調達に係る請負業務の要求要件は次に示すとおりである。

1. アラートを受けてから１時間以内にインシデントのハンドリングに着手すること。
2. 攻撃・感染の痕跡の詳細分析や高度な調査（デジタルフォレンジック、ネットワークログ解析、パケット解析等）を行い、原因・侵入手法を特定することができる体制を有すること。
3. インシデントの通知は、アラートが発生してから、原則として 4 時間以内とすること。
4. 国内大学に対してセキュリティオペレーション（マルウェア等に起因する不正な通信や脆弱性を狙った攻撃等の監視、分析、遮断業務等）を運用した実績を有すること。

（４）従事する技術者の要求要件は次に示すとおりである。

1. 業務要員のうち、1 名以上は情報処理安全確保支援士相当の資格を有すること。
2. 業務要員のうち、1 名以上は Linux のシステム運用に携わる職務経験を 3 年以上有すること。
3. 全ての業務要員は IP ネットワークシステムに携わる職務経験を 3 年以上有すること。
4. CISSP 資格を有するセキュリティ技術者を実施体制に組み込み、体制の中から業務要員のリーダー1 名を選定すること。

３．競争執行の場所等

（１）契約条項を示す場所、国立大学法人大阪大学競争入札加入者心得の交付場所並びに問合せ先

〒５６７－００４７　茨木市美穂ヶ丘５－１
国立大学法人大阪大学情報推進部情報企画課会計係
電話　０６－６８７９－８９８０

（２）国立大学法人大阪大学競争入札加入者心得の交付方法

本公告の日から上記３（１）の交付場所にて交付する。

（３）競争参加資格を証明する書類（上記２）及び入札書の受領期限並びに提出場所

令和５年３月２３日　１７時１５分（郵便により提出する場合には受領期限までに必着のこと。）
国立大学法人大阪大学情報推進部情報企画課会計係

（４）開札の日時及び場所
令和５年３月２４日　１３時３０分
大阪大学サイバーメディアセンター 吹田本館１階ミーティングルーム

４．その他
（１）入札保証金及び契約保証金　免除
ただし、落札者が契約の締結をしないときは、違約金として落札金額の１００分の５に相当する金額を大阪大学に支払わなければならない。
（２）入札の無効
本公告に示した競争参加資格のない者の提出した入札書、入札者に求められる義務を履行しなかった者の提出した入札書、その他国立大学法人大阪大学契約規則第２２条第１項各号に掲げる入札書は無効とする。
（３）競争参加資格の確認のための書類　別紙１により作成する。
（４）契約書作成の要否　要
（５）落札者の決定方法
本公告に示した役務を履行できると契約権限者が判断した入札者であって、国立大学法人大阪大学契約規則第１４条の規定に基づいて作成された予定価格の制限の範囲内で最低価格をもって有効な入札を行った入札者を落札者とする。
ただし、落札者となるべき者の入札価格によっては、その者により契約の内容に適合した履行がな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は、予定価格の制限の範囲内の価格をもって入札した他の者のうち最低の価格をもって入札した者を落札者とする。
（６）郵便（配達の記録が残るものに限る。）により提出する場合は、二重封書とし、表封書に「３月２４日開札［大阪大学総合情報通信システム(ODINS) 休日等におけるセキュリティ対応業務］の入札書在中」と朱書きし、中封書の封皮には氏名（法人の場合はその名称又は商号）を記載して、入札書の受領期限までに送付すること。
（７）上記３（４）の開札に立ち会わない競争加入者等については、再度入札を辞退したものとみなす。
（８）契約書の作成
競争入札を執行し、契約の相手方が決定したときは、契約の相手方として決定した日から７日以内（契約の相手方が遠隔地にある等特別の事情があるときは、指定の期日まで）に契約書の取り交わしをするものとする。
（９）その他
電信等による入札は認めない。
詳細は、「国立大学法人大阪大学競争入札加入者心得」による。

令和５年３月９日

国立大学法人大阪大学　理事　中谷　和彦（公印省略）

別紙１

競争参加資格の確認のための書類

（１） 令和５年度の資格審査結果通知書（全省庁統一資格）又は
国立大学法人大阪大学の競争参加資格の写し ・・・１部

（２） 技術者の略歴書（様式任意） ・・・１部

（３） 技術者が入札公告２の（３）4. 及び（４）に示す実績を有することを客観的に証明する書類（様式任意） ・・・１部
ただし、当該実績が本学におけるものである場合には、「技術者の実績」を証明する書類は省略できるものとする。

（注）上記提出書類のほか、補足資料の提出を求める場合がある。

仕様書

大阪大学総合情報通信システム(ODINS)
休日等におけるセキュリティ対応業務

大阪大学

I. 概要

1. 背景と目的

本学の教育・研究活動及び管理運営業務における情報セキュリティリスクの低減を実現し、情報セキュリティ対策の強化及び情報セキュリティインシデント（以下、「インシデント」という。）発生時の被害最小化を図るため、本学では OU-CSIRT（Osaka University Computer Security Incident Response Team）を設置している。

OU-CSIRT 構成員は、インシデントに対し迅速かつ適切な対応をとるため、インシデントに対する分析、通信遮断/解除の判断、改善に向けた対応等を行っている。しかし、インシデントは 24 時間 365 日発生し得るため、OU-CSIRT 構成員のみで常時対応することが難しい状況となっている。

本調達は、本学が 24 時間 365 日体制でインシデントに対応する体制を構築するために実施する。

2. 調達物品名及び構成内訳

2.1. 業務名称

大阪大学総合情報通信システム(ODINS)休日等におけるセキュリティ対応業務

1 式

2.2. 業務場所

国立大学法人大阪大学（吹田キャンパス）または大阪大学総合情報通信システム（以下、「ODINS」という）への通信制御が可能な場所

2.3. 業務期間

令和 5 年 4 月 1 日～令和 6 年 3 月 31 日

2.4. 契約条項

国立大学法人大阪大学が定めた製造請負契約基準によるものとする。

2.5. 請負代金の支払い

請負完了後、当該月の翌々月末までに支払うものとする。

3. 業務要件の概要

3.1. 本調達に係る請負業務の要求要件（以下「業務要件」という。）は「II. 業務内容に関する要件」に示すとおりである。

3.2. 業務要件は全て必須の要求要件である。

4. 情報セキュリティ

4.1. 作業に伴い情報セキュリティインシデントが発生した場合は、本学へ報告し、本学担当者と協議のうえ対応を行うこと。
4.2. II.業務内容に関する要件 項番 1.1.5 及び 1.5.3 に違反してセキュリティ対策を行わなかった結果、本学のシステム又はサービスに影響が発生した場合は、受注者の責任を問い、本学から受注者に損害賠償を請求できるものとする。
4.3. 本学が開示した情報及び本作業の履行上知り得た一切の事項については、いかなる場合にも、本学が開示することを認めていない第三者に開示又は漏えいしてはならないものとし、そのために必要な措置を講ずること。本学が提供した情報を第三者に開示する必要がある場合には、事前に本学と協議し、了承を得ること。
4.4. 作業に関するデータや資料は、本学の許可なしに業務場所から外部に持ち出し及び外部からアクセス可能な状態にしてはならない。

5. その他

5.1. その他留意事項
5.1.1. 本仕様に疑義が生じた場合には、本学担当者と協議するものとする。
5.1.2. データの保護について厳重に注意し、利用者データ及び業務データが流出することが無い様に徹底管理すること。なお、本学に所属する学生、職員、教員等の個人情報に関係する ID やパスワード、氏名等を取り扱う場合の作業は、本学内（または、通信制御が可能な場所）で行いデータの持ち出しは受注者及び受注者が作業を委託する業者を含め一切行わないこと。
5.1.3. 受注者(または、作業の一部を委託する業者)は、国内大学に対してセキュリティオペレーション（マルウェア等に起因する不正な通信や脆弱性を狙った攻撃等の監視、分析、遮断業務等）を運用した実績を有することとする。
5.1.4. 業務場所が本学でない場合、生体認証、IC カード認証等の複数の認証方式によりセキュリティを確保されており、パンデミックや停電、大規模災害時でも事業継続が行えるよう対策が講じられていることとする。

II. 業務内容に関する要件

1. 運用

本業務の対象となるインシデントは、学外機関から本学に対するインシデント疑いの連絡（以下、「アラート」という。）があったもの、及び学外機関が提供するサービスポータル上のログ（以下、「ポータルログ」という。）からインシデントであると判断されたものとする。ポータルログには、本学内と本学外間の通信ログが保存されている。ポータルサイトへのアクセス環境に関しては本学にて準備し受注者に提供するものとする。ただし、ポータルサイトへアクセスするための手段は受注者が用意すること。

また、インシデントの通知対象となる本学の IP アドレスは、133.1.0.0/16、192.50.0.0/21 及び 100.64.0.0/10 とする。

1.1. 業務内容

1.1.1. アラートを受けてから 1 時間以内にインシデントのハンドリングに着手すること。

1.1.2. 受信したアラートについて内容を確認し、本学が提示するインシデント対応ポリシー（以下、「ポリシー」という。）を踏まえ、対処すべき事項（通信遮断処理、設定変更等の実施内容）を検討すること。

1.1.3. アラート内容が、複数あるサイバー攻撃情報のうち代表した 1 つの内容であった場合、その他のサイバー攻撃情報については、ポータルログ等にてアラート発信元が指定する条件（シグネチャ ID や対象日時等）を元に調査すること。調査した結果、該当するサイバー攻撃情報を見つけた場合はポリシーに従い対応すること。

1.1.4. 攻撃・感染の痕跡の詳細分析や高度な調査（デジタルフォレンジック、ネットワークログ解析、パケット解析等）を行い、原因・侵入手法を特定することができる体制を有すること。

1.1.5. インシデント発生を認めた場合、発生場所、発生事象、その影響範囲と共に、通信遮断や隔離の可否及び再発防止の対策事項等について、本学が指定する者に原則として電話またはメールで通知すること。通知方法や通知内容等の詳細についてはポリシーによるものとする。

1.1.6. ODINS 保守請負業者へインシデント対応状況を共有すること。また、ODINS 保守請負業者に対し、内容の確認等が必要となる事案が発生した場合は、受注者が対応を行うこと。

1.1.7. インシデントの通知は、アラートが発生してから、原則として 4 時間以内とすること。

1.1.8. ポリシーに規定されていないインシデントが発生した際は、その旨を本学に電話またはメールで通知し、本学と協議して対処するものとする。また、必要に応じてポリシーのアップデートを行うこと。

1.2. 業務対象時間

1.2.1. 業務対象時間について、平日は 17:15～翌日の 8:30、休日は 8:30～翌日の 8:30 とする。

1.2.2. インシデント対応中の業務が、業務対象時間を超過する場合、本学から指示がない限り、継続して作業すること。ただし、業務対象外時間が 2 時間経過してもインシデント対応が完了しない場合は、本学担当者に引き継ぐものとする。

1.2.3. 本学における休日は、土・日・祝休日、別途本学が指定する休日とし、それ以外を平日とする。本学の平日が受注者側の社内における休日であっても平日として取り扱うこと。

1.3. 業務要員

1.3.1. CISSP 資格を有するセキュリティ技術者を実施体制に組み込み、体制の中から業務要員のリーダー（1 名）を選定すること。
1.3.2. 業務要員のうち、1 名以上は情報処理安全確保支援士相当の資格を有すること。
1.3.3. 業務要員のうち、1 名以上は Linux のシステム運用に携わる職務経験を 3 年以上有すること。
1.3.4. 業務要員は IP ネットワークシステムに携わる職務経験を 3 年以上有すること。
1.3.5. 主たる要員に変更が生じた場合には、本学へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること。

1.4. 受付・報告対応

1.4.1. 本業務の対象となるインシデントに関する本学からの各種依頼に対して、電話及びメールによる受付窓口を準備し、依頼事項に対する支援を実施すること。
1.4.2. 本学からのインシデント対応策推奨手順についての質問や技術的な質問に対して、電話またはメールにて回答を行うこと。
1.4.3. 専任の担当者を設置し、本学の環境を踏まえた支援や質問回答を行うことが望ましい。なお、専任担当者は、本学の専属である必要はなく、本学の環境を理解した応対ができればよい。
1.4.4. ポリシーで規定した作業が完了したインシデントの対応状況、ポリシーのアップデート状況、及び本学からの各種依頼への対応状況等を、月次業務報告書で毎月報告すること。インシデントの対応状況を報告する際は、少なくともインシデント毎にアラートの受信日時、アラートを受けてからインシデントのハンドリングに着手した日時、及びポリシーに従い通知した日時を報告内容に含めること。なお、インシデントの対応状況については、当該インシデントに関連する脅威や脆弱性情報も併せて報告すること。
1.4.5. 受注者は業務期間満了後、業務完了報告書を情報推進部情報基盤課に提出するものとする。

1.5. その他

1.5.1. 本学との契約終了時（途中解約等も含む）には、インシデント履歴やログデータ、レポート等の全ての情報を削除すること。
1.5.2. 本学担当者との電話またはメールでのやり取り、及び提出書類において使用する言語は日本語とすること。
1.5.3. 本学のシステムを操作するオペレーション端末は、脆弱性のないセキュアな端末で実施すること。なお、パッチ管理、アンチウィルス、ID 管理、ログ管理のセキュリティ対策は必須とする。

1.5.4. その他業務上不明な事項が生じた場合は、本学担当者と随時打ち合わせまたは本学担当者と協議の上決定すること。

以　上