第１号様式

令和２年１０月７日

公募型見積合わせ公告

国立大学法人大阪大学において、次のとおり公募型見積合わせ方式に付します。

１．調達内容

（１）調達番号　　情推001
（２）調達件名及び数量　　ODINSサーバ監査業務　一式
（３）納入期限　　令和３年１月２９日まで
（４）納入場所　　国立大学法人大阪大学情報推進部情報基盤課

２．見積参加資格

（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）本学と取引実績のある者であること。
（３）その他経理責任者等が認めた者

３．見積書の提出場所等

（１）見積書の提出場所、契約条項を示す場所、国立大学法人大阪大学公募型見積合わせ方式参加者心得の交付場所及び問合せ先
〒567-0047 大阪府茨木市美穂ケ丘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　06-6879-8981

（２）国立大学法人大阪大学公募型見積合わせ方式参加者心得の入手方法
本公告の日から上記３（１）の交付場所にて交付します。また、インターネットにより本学ホームページにアクセスし、参加者心得を出力することもできます。

（３）見積書提出期限
令和2年10月14日（水）17時00分

４．その他

（１）契約保証金　　免除
（２）契約書作成の要否　　要
（３）その他詳細は、国立大学法人大阪大学が定めた「国立大学法人大阪大学公募型見積合わせ方式参加者心得」に定めています。

仕様書

ODINS サーバ監査業務

大阪大学

令和 2 年 9 月

Ⅰ. 概要

1. 背景と目的

大阪大学総合情報通信システム（以下「ODINS」という。）は大阪大学における研究基盤のキャンパスネットワークとして運用されている。一方で技術の急速な進展により、インターネットからの不正アクセスやそれらを試みる行為は後を絶たないのが現状である。不正アクセスへの備えとして各部局が管理するサーバに適切なセキュリティ対策が実施されているかを確認し、脆弱性が発見された場合の解決策を指導することを目的とする。

2. 調達物品名及び構成内訳

2.1. 業務名称

ODINS サーバ監査業務　一式

2.2. 業務場所

国立大学法人大阪大学（吹田キャンパス・豊中キャンパス・箕面キャンパス）
または ODINS への通信が可能な場所

2.3. 成果物提出期限

令和 3 年 1 月 29 日(金)

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。

3.3. 必須の要求要件は本学が必要とする最低限の要求要件を示しており、提案された要件がこれらを満たしていないとの判定がなされた場合には不合格となり、落札決定の対象から除外する。

4. 情報セキュリティ

4.1. 情報セキュリティ及び個人情報保護について保護措置を講ずる体制を整備しており、ISO/IEC27001(JIS Q 27001)「情報セキュリティマネジメントシステム(ISMS)」認証が取得済みであることを証明すること。(業務

を再委託する場合には、受注者の責任において、委託先に適切な保護措置を講ずる体制を整備させること。）

4.2. 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、本学と協議のうえ対応を行うこと。

4.3. 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。

4.4. 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。

4.5. 作業に関するデータや資料は事前に許可した機器や保存先に格納すること。

4.6. データその他本作業の履行上発生した納入成果物については、本学の許可なしに、作業実施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。

II. 業務内容に関する要件

1. 業務内容

1.1. 監査実施計画書の提出

監査開始の 1 週間前までに、少なくとも以下の内容を含めた監査実施計画書を本学に提出すること。

- 監査実施手順の説明
- 監査対象となる脆弱性の説明
- 監査スケジュール
- 監査実施時の留意事項
- 監査実施体制及び監査実施期間中の緊急連絡先
- 監査終了後の問い合わせ先情報

1.2. 脆弱性監査作業

受注者はインターネットからの攻撃を想定し、脆弱性監査ツール（オープンソース等の無償の監査ツールは使用しないこと。）を用いて調査対象サーバの IP アドレスに対して、精度の高い監査と解析を実施すること。

（脆弱性監査の内容）

- ポート開放状況
- 攻撃者がシステムに仕掛けたバックドアやスクリプトの検出
- 破りやすいアカウントやパスワード、サービス、デフォルトのアカウントの

調査

- 各種 OS やソフトウェアに脆弱なバージョンがないか、脆弱なセキュリティ設定はないか等の調査
- 脆弱性が存在することで有名なサービスの使用可否の調査
- ルータ等、ネットワークデバイスの脆弱性の調査

1.3. 成果物の提出

成果物として、次の各資料を本学に提出すること。各資料には、少なくとも以下に列挙した内容を含むこと。

(1) 監査実施計画書

- 1.1 に示した内容

(2) 総括報告書

- 監査概要
- 総合評価と、リスクレベルの分布
- 部局別評価と、部局別リスクレベルの分布

(3) 部局別報告書

- 監査概要
- 当該部局の評価と、リスクレベルの分布
- 監査対象機器（IP アドレス）毎に、検出された脆弱性タイトル、リスクレベル（High、Medium、Low 等）、脆弱性内容、推奨対策案、セキュリティパッチ情報（取得先へのハイパーリンクを埋め込むこと）を記載すること。脆弱性内容については、専門的・技術的な分析結果及びその解説を盛り込み、作成すること。（監査ツールが出力する結果レポートをそのまま報告書として提出することは不可とする）

(4) リスク検出結果一覧表

表形式で、次の内容を記載すること。

- 部局名
- 監査対象 IP アドレス
- 監査対象 IP アドレスに対応するドメイン名（本学が指定したもの）
- 脆弱性タイトル
- リスクレベル
- 脆弱性内容（簡略な記載でも可）
- 対応結果（本項目は監査を受けた者が対処を行った際に入力する項目につき、列の作成のみ行い中身は空欄にしておくこと）
- 備考欄

（成果物作成時の留意点）

- (1)～(4)は日本語で作成すること。
- (1)～(3)は PDF 及び Word2019 等の編集可能な形式、(4)は Excel2019 等の編集可能な形式とすること。

・ 成果物は電子媒体（CD-ROM または DVD-ROM）として 2 部提出すること。
・ (3)は、本学が指定する部局単位（計 45 部局）で作成し、部局毎にフォルダで仕分けすること。
・ (4)は、全体版（検出された全てのリスク）と、部局版（当該部局の対象 IP アドレスに対して検出されたリスク）をそれぞれ作成すること。部局版については、本学が指定する部局単位で作成し、前項と同じフォルダに格納すること。

2. 監査日時

原則として令和 2 年 10 月～12 月の平日 9:00-17:00 とするが、詳細は本学と協議の上、決定するものとする。

3. 監査対象 IP アドレス・監査対象ポート

（監査対象 IP アドレス数）

974 個

（監査対象ポート）

TCP と UDP を対象とする。TCP については全ポート（1-65535）を監査対象とすること。なお、具体的な監査対象 IP アドレスの情報については、契約後に本学から受注者に伝えるものとする。

4. 情報の守秘義務

受注者は、個人情報保護法を考慮し次の項目を遵守すること。これに違反した場合、契約解除等の適切な措置をとるものとする。

(1) 業務遂行上、知り得た個人情報について機密保持等の義務を負うこと。
(2) 業務遂行上、個人情報の複製の必要性がある場合は本学の許可を得ること。
(3) 個人情報の漏洩等の事案が発生した場合は、いつでも本学の事情聴取に応じること。
(4) 業務終了後、本学の許可を得て媒体に複写した個人情報は消去、又は返却すること。

5. その他

(1) 受注者が作成した本件に関する全ての書類の原本及び複本、一部の複写は、本件業務終了後、機密管理の上廃棄すること。
(2) 請負作業中に異常事態が生じたときは本学担当者に報告し、協議の上適切な対応を行うこと。
(3) 作業責任者は、業務の進捗状況について常に把握し、本学担当者から進捗の質問に対してすぐに対応できるようにすること。また、本学担当者が常時契約履行に関する調査を行える体制とすること。

(4) 受注者は提出後、1年間は本学から提出された監査結果に関するメールによる問い合わせに対応する体制をとること。

(5) 受注者はISMS(Information Security Management System)適合性評価制度及び品質マネジメント規格ISO9001の認証を取得していること。

(6) 診断者は次のいずれかの条件を満たすこと。

・情報処理推進機構の「情報セキュリティサービス基準適合サービスリスト」に記載されていること。

・CREST（Council for Registered Ethical Security Testers）認定を取得していること。

(7) 診断主担当者は以下の資格のいずれか一つを保有していること。

1. 公認情報システムセキュリティ専門家（CISSP）
2. Cisco Certified Network Professional Security（CCNP Security）
3. 情報処理安全確保支援士

以上

第２号様式

見　積　書

調達番号：　情推001

調達件名：　ODINSサーバ監査業務　一式

見 積 金 額　　金　　円也

国立大学法人大阪大学が定めた製造請負契約基準を熟知し、仕様書及び公募型見積合わせ方式参加者心得を承諾の上、上記の金額によって見積します。

令和　　年　　月　　日

国立大学法人大阪大学　殿

住　　所
会 社 名
氏　　名　　[印]
電話番号

１ 見積金額は、消費税額及び地方消費税額を除いた金額を記載してください。
２ 見積書の日付は、提出日を記載してください。
３ 本学が見積公告【２．見積参加資格（１）（２）】以外に見積参加資格を示した場合、それを有しているかどうか証明するための書類を見積書に添付してください。

※ 再度見積及び参加者不在の取扱いに係る見積書は、本様式以外のものを使用することができる。

請　負　契　約　書（案）

請負の表示　ODINS サーバ監査業務　一式

請負代金額　　金　　円也（うち消費税額及び地方消費税額　　円）

上記の消費税額は、消費税法第２８条第１項及び第２９条並びに地方税法第７２条の８２及び第７２条の８３の規定に基づき、請負代金額に１１０分の１０を乗じて得た額である。

発注者 国立大学法人大阪大学 理事 中谷 和彦 と 受注者　　との間において上記の請負業務（以下「業務」という。）について、上記の請負代金額で次の条項によって請負契約を結ぶものとする。

第１条　受注者は、別紙の仕様書に基づいて、業務を実施するものとする。
第２条　業務は国立大学法人大阪大学情報推進部情報基盤課で行うものとする。
第３条　受注者は、業務を行う上で知り得た発注者に関する事項を他に漏らし、又は他の目的に使用してはならない。
第４条　受注者は、業務を行う上で知り得た個人情報については、別紙「個人情報取扱の特記事項」を遵守して取り扱うものとする。
第５条　成果物の提出期限は、令和３年１月２９日までとする。
第６条　受注者は、業務の完了後、完了通知書を国立大学法人大阪大学情報推進部情報企画課会計係に送付するものとする。
第７条　請負代金は、１回に支払うものとし、業務の完了確認後、当該月の翌々月末までに支払うものとする。
第８条　契約保証金は免除する。
第９条　受注者は、業務を実施するにあたって、発注者の建物、設備等を損傷しないよう善良な管理者の注意義務を怠ってはならない。
第１０条　受注者は、前条に違反し建物、設備等を損傷した場合は、賠償の責を負うものとする。
第１１条　この契約についての必要な細目は、別冊の国立大学法人大阪大学が定めた製造請負契約基準を準用するものとする。
第１２条　この契約について、発注者と受注者との間に紛争を生じたときは、発注者所在地の所轄裁判所の裁決により、これを解決するものとする。
第１３条　この契約に定めのない事項について、これを定める必要がある場合は、発注者と受注者とが協議して定めるものとする。

上記契約の成立を証するため発注者及び受注者は、次に記名し、印を押すものとする。
この契約書は２通作成し、双方で各１通を所持するものとする。

令和２年　月　日

発注者　吹田市山田丘１番１号
国立大学法人大阪大学　理事　中谷 和彦

受注者

個人情報取扱の特記事項

（基本的事項）

第１　この契約により、発注者から業務を請け負った者（以下「受注者」という。）は、この契約による業務を行う上で、個人情報を取り扱う際には、個人情報の保護の重要性を認識し、個人の権利利益を侵害することのないようにしなければならない。

（秘密保持）

第２　受注者は、この契約による業務に関して知り得た個人情報を他人に知らせ、又は本契約を履行する以外の目的に使用してはならない。

２　受注者は、この契約による業務に従事する者に対し、在職中及び退職後においても、この契約による業務に関して知り得た個人情報を他人に知らせ、又は本契約を履行する以外の目的に使用してはならないこと、その他個人情報の保護に関して必要な事項を周知させなければならない。

３　前２項の規定は、この契約が終了し、又は解除された後においても同様とする。

（保管及び搬送）

第３　受注者は、この契約による業務に係る個人情報の漏えい、改ざん、滅失、毀損その他の事故を防止するため、個人情報の厳重な保管及び搬送に努めなければならない。

（再委託の禁止）

第４　受注者は、発注者の指示又は承諾があるときを除き、この契約による業務に係る個人情報の処理を自ら行うものとし、第三者にその処理を委託してはならない。

（契約目的以外の利用等の禁止）

第５　受注者は、発注者の指示又は承諾があるときを除き、この契約による業務に係る個人情報を当該業務の処理以外の目的に使用し、又は第三者に提供してはならない。

（複写及び複製の禁止）

第６　受注者は、発注者の指示又は承諾があるときを除き、この契約による業務に係る個人情報を複写若しくは複製してはならない。

（事故発生時の報告義務）

第７　受注者は、この特記事項に違反する事態が生じ、又は生じるおそれがあることを知ったときは、速やかに発注者に報告し、その指示に従わねばならない。この契約が終了し、又は解除された後においても同様とする。

（個人情報の返還等）

第８　受注者は、この契約が終了し、又は解除されたときは、この契約による業務に係る個人情報を速やかに発注者に返還し、又は漏えいを来さない方法で確実に処分しなければならない。

（適正な管理）

第９　受注者は、この契約による業務を学外で実施する場合には、個人情報の適正な管理のために必要な措置を講じなければならない。この場合において、発注者の求めに応じ、責任者等の管理体制及び個人情報の管理状況に係る検査に関する事項等についての書面を提出しなければならない。

（違反した場合の措置等）

第 10　発注者は、受注者がこの特記事項に違反していると認めたときは、契約の解除及び損害賠償の請求をすることができるものとする。