業務委託仕様書

1. 業務名

大阪市情報セキュリティ監査補助業務（脆弱性診断等）

2. 本業務の内容

本業務は、本市が情報セキュリティ監査を実施するに当たり、監査対象システムに対するプラットフォーム脆弱性診断（以下「脆弱性診断」という。）による技術的セキュリティ評価の実施、評価結果の資料作成、助言等を行う監査支援業務を委託するものである。

なお、情報セキュリティ管理体制等のＩＣＴ全般統制の観点からの点検や、情報セキュリティ監査報告書の作成は本市が行う。

2.1. 業務項目

（１） 業務計画書作成

受注者は、次の事項を含む業務計画書を本市と協議の上で作成すること。

① 記載内容

ア．業務体制、管理者及び作業従事者の所属、氏名及び経歴の一覧表

イ．本業務に係る管理者（業務責任者）及び作業従事者に関する役割及び氏名を含む体制図

ウ．全体スケジュール

エ．脆弱性診断の実施項目

オ．脆弱性診断の分析・評価方法

カ．脆弱性診断を実施するために本市から情報提供が必要な事項

② 期限

契約締結日からおおむね１週間以内に提出すること。

（２） 業務事前説明会

受注者は本市担当者及び対象システムを所管する部署（以下「被監査部署」という。）に対して、脆弱性診断の実施に関する説明会（２時間程度、日時・場所は本市にて指定する。）を実施し、事前に本市の了解を得ること。また、議事録を作成すること。

（３） 脆弱性診断事前調整

受注者は脆弱性診断の具体的な日程については、本市担当者と事前に調整すること。

なお、被監査部署との調整は本市担当者が行う。

（４） 脆弱性診断実施

受注者は（１）及び（３）に基づき、インターネットを経由して診断対象の情報システムにアクセスし、脆弱性の有無を調査する。

（５） 資料整理・診断結果報告書作成

成果物は次のとおりとし、書面（Ａ４版縦両面印刷を基本とし、必要に応じてＡ３版三つ折りも可。Ａ３版三つ折りの場合、両面印刷は不可とする。）２部を提出すること。

なお、成果物の作成に当たっては、情報システムに係る高度な知識を持たない者でも理解しやすいよう、平易な表現を用いること。

ア．業務体制、管理者及び作業従事者の所属、氏名、経歴及び資格内容の一覧表

イ．本業務に係る管理者（業務責任者）及び作業従事者に関する役割及び氏名を含む体制図

ウ．全体スケジュール

エ．脆弱性診断の実施内容及び結果

オ．脆弱性診断の結果に対する分析・評価の観点、評価及び改善提案

カ．作業実績工数

（６） 診断結果報告会

脆弱性診断の結果について報告会を行うこと。また、議事録を作成すること。

2.2. 脆弱性診断の内容

本契約において想定している脆弱性診断は、情報システムやその基盤となるＯＳやミドルウェア、ファイアウォール等について、最新のセキュリティパッチが適用されているか、各種のセキュリティ設定項目が適切な状態に定められ、運用されているか、不要な通信ポートが開いていないかなどを診断し、脆弱性を含む項目を洗い出し、改善に向けた提案を行うことである。

脆弱性診断として実際に検査する項目は、契約後に指定する診断対象の情報システムにおいて確保すべきセキュリティレベルに鑑みて、本市と協議し、決定すること。なお、運用中のシステムを診断対象とするため、ＤｏＳ攻撃等、システムに対して意図的に負荷を掛けるような試験は行わない。

診断結果については、ＣＶＳＳ（共通脆弱性評価システム）、ＩＰＡの暗号設定ガイドライン等に基づき評価するものとする。

2.3. 診断対象

（１）本市が所管する情報システムのうち、本市管理施設の外部からＩＰ通信が可能な情報システムを本市が１つ選定し、契約締結後に指示する。脆弱性診断の対象とするＩＰアドレス数は対象システムで１個とする。

（２）（１）のＩＰアドレスは、脆弱性診断の対象とする情報システムの各ホストに付与され、診断の対象として選定したものとする。ただし、診断の対象は、各種サーバ、端末、通信回線装置を想定している。

3. 業務期間及びスケジュール

3.1. 契約期間

契約締結日から５か月程度（予定）

3.2. スケジュール（予定）

契約締結後１週間以内	業務計画書提出
契約締結後２か月以内	脆弱性診断実施、診断結果報告書提出

以後、契約期間満了まで	監査報告書作成に必要な事項について本市からの問合せへの対応等

なお、詳細な日程については打合せで決定する。

4. 実施体制

業務体制として、本業務に係る管理者（業務責任者）を１名必ず配置すること。

業務責任者は、以下のいずれかの資格を有していること。

- 情報処理安全確保支援士又は情報セキュリティスペシャリスト
- 公認情報セキュリティ主任監査人
- 公認情報セキュリティ監査人
- 公認情報セキュリティマネージャー（ＣＩＳＭ）
- 公認情報システムセキュリティ専門家（ＣＩＳＳＰ）
- ネットワーク情報セキュリティマネージャー（ＮＩＳＭ）

5. 実施上の留意事項

（１）本業務委託に必要な機器、ソフトウェア、作業者等の一切は受注者が準備すること。

（２）脆弱性診断の準備、実行に関する作業は全て、受注者の管理の下で行うこと。ただし、診断対象の情報システムの関係者以外に実施できない事項については、発注者から当該情報システム関係者に依頼するので、協議の上、依頼する作業の内容及び時刻等の必要事項を書面で提出すること。

（３）診断対象の情報システム及びその情報システムと接続されている全ての情報システムに対して、稼働状況に影響を与えないよう配慮し、業務計画書に示すこと。

（４）業務に必要な回線費、交通費等は受注者の負担とする。

（５）作業の実施中にシステムに障害を発生させた場合は、速やかに本市に連絡するとともに速やかに現状に復する支援を行うこと。

（６）受注者は業務の執行に当たり、故意又は過失により本市又は第三者に損害を与えた場合は、損害賠償の責任を負うものとする。また、業務終了後に本市又は第三者に損害を与えたことが発覚した場合も同様とする。

6. 再委託について

（１）業務委託契約書第 16 条第１項に規定する「主たる部分」とは、「2.１．　業務項目」に記載の業務をいい、受注者はこれを再委託することはできない。

（２）受注者は、コピー、ワープロ、印刷、製本、トレース、資料整理などの簡易な業務の再委託に当たっては、本市の承諾を必要としない。

（３）受注者は、第１号及び第２号に規定する業務以外の再委託に当たっては、書面により本市の承諾を得なければならない。

（４）受注者は、業務を再委託に付する場合、書面により再委託の相手方との契約関係を明確にしておくとともに、再委託の相手方に対して適切な指導、管理の下に業務を実施しなければならない。

なお、再委託の相手方は、大阪市競争入札参加停止措置要綱に基づく停止措置期間中の者、又は大阪市契約関係暴力団排除措置要綱に基づく入札等除外措置を受けている者であってはならない。

7. その他

（1）作業に当たっては、発注者と十分に打合せを行った上、実施すること。
（2）情報システムの取扱には特に留意すること。
（3）業務委託内容及び実施にかかる環境に疑義が生じた場合は、速やかに発注者の指示を仰ぐこと。
（4）受注者は、本市情報システムに関する内容を漏らしてはならない。また、納入後も同じとする。
（5）発注者による成果物の検査が終了した時点で、業務により生成されたデータ並びに複製品等は、受注者の責任で廃棄し、その内容が漏れることのないようにすること。
（6）大阪市契約関係暴力団排除措置要綱を遵守すること。なお、詳細については別添「特記仕様書」を参照のこと。

8. 別添資料

（1）特記仕様書