

令和7年度

情報セキュリティ外部監査および情報セキュリティ研修業務委託

入札仕様書

【一般競争入札総合評価落札方式】

- 1 調達件名
- 2 業務委託期間（予定）
- 3 入札にあたっての注意点
- 4 業務の対象と内容
- 5 適用基準および資料閲覧
- 6 監査人の要件
- 7 業務成果物と納入方法
- 8 成果物の帰属
- 9 委託業務の留意事項
- 10 その他

令和7年4月

学校法人 自治医科大学

1 調達件名

令和7年度情報セキュリティ外部監査および情報セキュリティ研修業務委託

2 業務委託期間（予定）

契約開始日 ～ 令和8年3月31日

3 入札にあたっての注意点

入札にあたっては、本紙（以下「仕様書」という）および別紙「令和7年度情報セキュリティ外部監査および情報セキュリティ研修業務委託総合評価基準書」（以下「総合評価基準書」という）に記載されている内容や、下記の注意点をよく確認すること。

3-1 落札者の選定方法

一般競争入札総合評価落札方式によって行う。

※詳細は、総合評価基準書「2 総合評価の方法」を参照すること。

3-2 入札時の提出書類

別紙「入札書郵送方法」に従って下記の提出書類を郵送すること。

【提出書類】

- 入札書
- 技術評価表
- 技術提案書（技術評価表の項番ごとに提案内容を記載すること）
- 監査人の要件を証するものの写し（医科大学における情報セキュリティ監査業務実績含む）※6 監査人の要件を参照
- 見積書
- 入札参加表明書
- 一般競争入札参加資格確認通知書（写）

4 業務の対象と内容

自治医科大学（以下「本学」という）情報セキュリティポリシーに則り、下記のとおり、情報セキュリティ外部監査および情報セキュリティ研修業務（以下「本業務」という）を行うものとする。

4-1 準備業務

下記4-2～4-6の業務を円滑に実施するために、以下の準備をすること。

- (1) 本学の情報システムの管理運用および本業務に係る要望等を把握するためのヒアリングを実施する。
- (2) 業務実施計画書を作成し、本学の承認を得る。

4-2 ペネトレーションテスト

以下の仕様等を満たす脆弱性診断サービスを提供すること。

- (1) 令和7年11月頃を実施予定とする。
- (2) 本学が指定するサーバ(対象数 15IP アドレス)に対して脆弱性診断を行うこと。
- (3) インターネット経由でのリモート診断とし、ツールによる診断および検査者の手作業による診断を併用して実施すること。
- (4) テストは平日8時30分～17時15分の時間帯で実施すること。
- (5) 診断結果報告書は、ツールによる診断結果と検査者の手作業による診断結果の分析を含めて取りまとめること。
- (6) 診断結果報告書は、診断結果に対する具体的な対応方法も記載すること。

4-3 標的型攻撃メール対応訓練

以下の仕様等を満たす標的型攻撃メール対応訓練を実施すること。

- (1) 令和7年9月上旬を実施予定とする。
- (2) 訓練回数、対象
 - ・ 第1回…個人アドレス(教員・事務職員:約7,250/学生:約1,410)
 - ・ 第2回…所属アドレス(約1,000)
- (3) 訓練計画を策定すること。
- (4) 訓練実施の準備として、訓練メール案を作成し、メール配信サーバ等のシステムを設定すること。
- (5) 訓練メールの仕様を次に示す。
 - ・ 訓練メールの内容については、①教員・事務職員用、②学生用、③所属アドレス用と分別し、3種類を提案すること。
 - ・ 数種類のテンプレートから選択でき、本学の要望に沿ってカスタマイズできること。
 - ・ 開封検知方式を添付ファイルやURLリンク等から選択できること。
 - ・ 開封結果をシステム側で検知できること。
- (6) 訓練メール配信サーバは、自社内に構築し、クラウドサービス等外部サーバは利用しないこと。
- (7) 訓練メールを送信するドメインおよびメール送信プログラムを準備すること。
- (8) 訓練メールを送信するサーバのグローバルIPアドレスは1つに固定すること。
- (9) 開封者に対するコンテンツ表示のため、Webサーバを自社内に準備すること。
- (10) 訓練メールは本学が指定する日時に配信し、開封検査は配信日時の1週間後まで実施すること。
- (11) 開封時コンテンツを用いたアンケートの実施と集計を行い、集計結果の分析と分析結果に基づいた改善提案を行うこと。
- (12) 開封結果の簡易報告を検査期間中毎日(休日を除く)行うこと。
- (13) 訓練結果報告書は、結果の評価・分析および対策等の提言を含めて取りまとめること。

4-4 情報セキュリティ研修

以下の仕様等を満たす情報セキュリティ研修を実施すること。

- (1) 標的型攻撃メール対応訓練終了後 2 週間以内に実施する。
- (2) 研修概要：教育研究機関及び医療機関向け情報セキュリティ教育を e-Learning により実施する
- (3) 対象：教職員（教員、医師、事務職員）、医療従事者（看護師、技師）、学生
- (4) 開催方法、時間：再生時間約 30 分間のビデオオンデマンド視聴及び学習問題への回答
- (5) 次に掲げる事項をテーマとして取り入れること。
 - ・ 4－3 標的型攻撃メール対応訓練 の結果
 - ・ 本学が事例提供するセキュリティ事故事例
 - ・ 他の大学・医療機関で発生したセキュリティ事故事例
 - ・ 生成 AI を含む約款型サービス利用における注意点（本学が作成した生成 AI 等の約款型サービス利用における注意点に関する資料へセキュリティ監査人の視点を盛り込む）
 - ・ 実機を用いたサイバー攻撃のデモンストレーション（実演および解説）
- (6) 生成 AI 等の約款型サービス利用における注意点に関する動画の作成にあたり、2 回のオンラインによる打合せ実施を想定すること。
- (7) 動画は、聴覚障害者等に配慮し、字幕を入れること。
- (8) 本学の e-Learning システムを使用してビデオオンデマンド配信を行う。
- (9) ビデオは電子ファイルで提供すること。ファイル形式（拡張子）は「.mp4」とする。
- (10) 学習問題は情報セキュリティ研修の内容に基づく設問および解説とし、出題形式は多肢選択とする。問題数は 15 問程度とするが、詳細は本学と協議の上、決定する。解説は選択肢毎とする（正解・不正解の理由を説明する）こと。
- (11) 教材一式のファイル形式（拡張子）は「.pptx」とする。

4 - 5 監査結果報告

- (1) 監査結果報告書は令和 7 年 12 月 19 日金曜日までに提出すること。
- (2) 監査結果報告書は、詳細版と要約版の 2 種類作成すること。
- (3) 監査結果報告書要約版の構成及び内容は本学の承認を得ること。
- (4) 監査人は本学情報セキュリティ委員会（令和 8 年 1 月 web 会議にて開催予定）に出席し、監査結果報告書要約版を用いて監査結果報告を行うこと。

5 適用基準および資料閲覧

本業務は、以下に示す基準に則り行うものとする。なお、(1) (2) のうち、外部公開をしていない資料は、受託者の要求に応じて閲覧を認める。

- (1) 必須とする基準
 - ア. 自治医科大学情報システム運用基本方針
 - イ. 自治医科大学情報システム運用基本規程
- (2) 参考とする基準
 - ア. 自治医科大学情報倫理規程

- イ. 自治医科大学情報セキュリティ対策基準
- ウ. 自治医科大学学内情報ネットワーク利用規程
- エ. 地方公共団体における情報セキュリティ監査に関するガイドライン（総務省）
- オ. 上記のほか業務委託期間において情報セキュリティに関し有用な基準等で、本学と協議して採用するもの

6 監査人の要件

受託者は、以下に示す要件を全て満たすこと。

- (1) 情報セキュリティサービス基準適合サービスリスト（うち、セキュリティ監査サービスに係る部分および脆弱性診断サービスに係る部分）に登録されていること。
- (2) ISMS（ISO/IEC27001）認証又はプライバシーマーク認証を取得していること。
- (3) 監査責任者、監査人、監査補助者、アドバイザー等の数名で構成される監査チームを編成すること。
- (4) 監査チームには、情報セキュリティ監査に必要な知識および経験（教育研究機関および医療機関における情報セキュリティ監査の実績）をもち、次のA群およびB群に掲げる資格のうち、いずれかの資格を有する者が各群それぞれ1人以上含まれていること。なお、同一の者がA、Bそれぞれの群に属する資格を有していても良い。

【A群】

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、CISA（公認情報システム監査人）、公認システム監査人、ISMS 主任審査員、ISMS 審査員、システム監査技術者

【B群】

情報処理安全確保支援士、CEH（認定ホワイトハッカー）、CISSP（セキュリティプロフェッショナル認定資格）、CISM（公認情報セキュリティマネージャー）

- (5) 監査チームの構成員が、監査対象となる情報資産の管理および当該情報資産に関する情報システムの企画、開発、運用、保守等に関わっていないこと。
- (6) 医科系大学において、過去2年以内に情報セキュリティ監査業務（ペネトレーションテスト、標的型攻撃メール対応訓練、e-Learningによる情報セキュリティ研修等）の実績を有していること。

7 業務成果物と納入方法

以下の業務成果物をそれぞれの納入方法に従って、必要数を提出すること。

項番	業務成果物名	納入方法	
		(紙媒体)	(電子媒体)
1	業務実施計画書	1 部	1 部
2	ペネトレーションテスト診断結果報告書	1 部	
3	標的型攻撃メール対応訓練結果報告書	1 部	
4	情報セキュリティ研修ビデオ(拡張子.mp4)	—	
5	情報セキュリティ研修教材一式(拡張子.pptx)	—	
6	監査結果報告書	1 部	

8 成果物の帰属

成果物およびこれに付随する資料は、全て本学に帰属するものとし、本学の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物およびこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、本学は、本業務の目的の範囲内で自由に利用できるものとする。

9 委託業務の留意事項

業務の実施に当たっては、以下の事項に留意すること。

(1) 資料の提供等

本業務の実施に当たり、必要な資料およびデータの提供は本学が妥当と判断する範囲内で提供する。

なお、受託者は、本学から提供された資料は適切に保管し、特に個人情報に係るものおよび情報システムのセキュリティに係るものの保管は厳格に行うものとする。また、契約終了後は、本業務に当たり収集した一切の資料を速やかに本学に返還し、又は破棄するものとする。

本学が作成した生成 AI 等の約款型サービス利用における注意点に関する資料を複製すること及び本委託業務以外に使用することは固く禁止する。

(2) 技術的検証

技術的検証については、対象情報システムおよび本学の学内ネットワークの運用に対し、支障および損害を与えないように実施するものとする。

(3) 再委託

受託者が、本業務の実施に当たり、他の業者に再委託することを禁止する。

(4) 秘密保持等

受託者は本業務の実施に当たり、知り得た情報および成果品の内容を正当な理由なく他に開示し又は自らの利益のために利用してはならない。これは、契約終了後又は契約解除後においても同様とする。

(5) 議事録等の作成

受託者は、本業務の実施に当たり、本学と行う会議、打ち合わせ等に関する議事録を作成し、本学にその都度提出して内容の承認を得るものとする。

(6) 関係法令の遵守

受託者は業務の実施に当たり、関係法令等を遵守し業務を円滑に進めなければならない。

(7) 報告等

受託者は作業スケジュールに十分配慮し、本学と密接に連絡を取り業務の進捗状況を報告するものとする。

10 その他

本業務の実施に当たり、本仕様書に記載のない事項については本学と協議の上、決定するものとする。

以上