別紙２

高専情報環境に係る
情報セキュリティ対策業務 一式

仕様書

令和５年１２月

独立行政法人 国立高等専門学校機構

目次

１．調達件名

高専情報環境に係る情報セキュリティ対策業務　一式

２．調達の目的等

2.1　調達の目的

本調達は、独立行政法人　国立高等専門学校機構（以下、「機構」という。）テナントのMicrosoft Azure（以下、「Azure」という。） 上で運用されている情報システムを安全に利用するために、通信の監視や不正アクセスの遮断、脆弱性診断といった情報セキュリティ対策に関する業務を委託するものである。

2.2　情報セキュリティ対策の必要性

機構は、政府機関等と同様に、「政府機関等のサイバーセキュリティ対策のための統一基準（以下、「統一基準」という。）」に基づく情報セキュリティ監査(助言型のマネジメント監査及びペネトレーションテスト)の対象法人であることから、統一基準に準拠した情報セキュリティ対策への対応ならびに安全な環境の維持・確保を義務付けられている。

本調達の対象システムは、機密性の高い情報を取り扱っており、同時に、場所を問わずアクセスできる利便性を確保しているため、相応の情報セキュリティ対策が求められる。

３．請負期間

令和６年４月１日～令和７年３月３１日

４．対象システム

本書記載の要件における対象システムは以下のものとする。

4.1 対象システムの監視	・CBTシステム(学生用) ・CBTシステム(作問用) ・教材共有システム(令和6年4月1日～6月30日)
4.2　対象システムにおける脆弱性の診断	・CBTシステム(学生用) ・CBTシステム(作問用) ・統合データベースシステム『UDB』（Unified DataBase)(プラットフォーム診断のみ) ・データベース修正用システム(プラットフォーム診断のみ)

なお、対象システムのネットワーク構成図等、詳細情報を示す資料については、情報セキュリティ上の理由から、希望者のみに配布する。希望者は別途、高専機構本部財務課契約係まで、資料を希望する旨、連絡すること。

５．受注条件

(1) 請負者は、一般社団法人情報マネジメントシステム認定センター、公益財団法人日本適合性認定協会、もしくはその他認定機関により認定された審査登録機関によるISO/IEC27001又はJIS Q 27001の認証を受けていること。

(2) 請負者は、一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク（JISQ15001）使用許諾の認証を受けていること。

(3) 情報処理推進機構（IPA）が公開している情報セキュリティサービス基準適合サービスリスト（最新版）「脆弱性診断サービス」分野に登録されていること。

(4) 脆弱性診断に対する知見を有することを証明するため、過去３年以内に本件と同様の

調達実績が50件以上、公的機関における調査実績が過去３年以内に10件以上あること。

(5) 作業従事者は２名以上とし、以下条件を満たすこと。
① 情報セキュリティ診断に関する業務経験を３年以上有すること。
② 以下いずれかの資格を保有していること。
・ 情報システムセキュリティプロフェッショナル認定資格（CISSP）
・ 公認情報システム監査人（CISA）
・ 公認情報セキュリティマネージャ（CISM）
・ 公認情報セキュリティ監査人
・ GPEN GIAC Penetration Tester
・ GWAPT GIAC Web Application Penetration Tester
・ OSCP Offensive Security Certified Professional

６．業務内容

6.1 対象システムの監視

(1) 対象システムの情報セキュリティ監視を行うこと。

(2) 監視サービス提供時間は２４時間体制とする。

(3) 対象システムに対するサービス不能攻撃への対策のため、対象システムや、その通信経路における通信の監視を行うこと。また、サービス不能攻撃と判断される攻撃を検知した場合には、攻撃元からの通信の遮断、対象システムのネットワークからの遮断、通信回線の通信量の制限を例とする、適切な方法で即時の対応を行うこと。

(4) 対象システムにおける、以下の脆弱性を検出し、脆弱性への攻撃を排除すること。
① SQL インジェクション脆弱性
② OS コマンドインジェクション脆弱性
③ クロスサイトスクリプティング脆弱性
④ HTTP ヘッダインジェクション脆弱性
⑤ ディレクトリトラバーサル脆弱性
⑥ セッション管理の脆弱性

上記項目以外にも、システムへ影響を及ぼしかねない脆弱性を検出・認知した場合には、機構担当者へ速やかに報告を行うこと。

(5) 対象システムの安定稼働や利用者または対象システムの要保護情報に対する重大侵害行為を検知した場合には、直ちに機構担当者へ連絡を行い、必要かつ推奨する対応について助言やサポートを行うこと。

(6) 監視状況の結果について、月毎に取りまとめ及び状況分析を行い、監視報告書を作成し、翌月初旬を目途に機構担当者へ提出すること。監視報告書には、監視実施記録及び状況分析、セキュリティ懸念や推奨対策を記載すること。

(7) 監視報告書の内容を報告する監視報告会を、３か月に一度行うこと。ただし、緊急の報告が必要となった場合は、別途、それに関する報告会を行うものとする。

(8) 対象システムに係る監視項目、監視方式、監視体制や連絡フロー等の詳細は、機構担当者と協議した上で決定すること。

(9) 監視に係るファシリティ（設備や機器、電力等）や人的リソースについては、請負者の負担とする。

6.2 対象システムにおける脆弱性の診断

(1) 対象システムで利用するOSやソフトウェアにおいて、新たに確認された脆弱性や未対応の脆弱性が残存していないかの確認を、年１回以上のWebアプリケーション診断と、年１回以上のプラットフォーム診断（以下、「脆弱性診断」という。）により行うこと。なお、診断に必要な対象システムの詳細情報は、契約後に共有する。
また、「統合データベースシステム『UDB』」、「データベース修正用システム」については、Webアプリケーション診断の対象から除外し、プラットフォーム診断のみを行う。

(2) 脆弱性診断は、独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」や 、OWASP(Open Web Application Security Project)Top10 を参照した上で実施すること。

(3) 脆弱性診断の結果は、機構担当者へ報告すること。報告には脆弱性、緊急度、リスク、推奨対策、参考情報等を含むこと。また、脆弱性への対応をシステム改修によって行う必要がある場合、助言やサポートを行うこと。
なお、脆弱性診断の結果、項6.1の(4)に示す項目以外にもシステムへ影響を及ぼしかねない脆弱性を検出・認知した場合には、併せて報告・助言・サポートを行うこと。

6.3 診断結果への対応

(1) 脆弱性診断により対象システムに脆弱性が確認された場合や、対象システムで利用するOSやソフトウェアに関連する脆弱性情報を入手した場合には、対象システムへの影響を考慮した上で、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による脆弱性に対する対応を通知し、必要な助言やサポートを行うこと。

(2) 確認された脆弱性に対して、何らかの要因により、直ちに対象システム側で根本対応が実施できない場合は、リスクを最小化するための暫定的な対応方法を検討し、機構に提案すること。

6.4 対象システムに関する脆弱性情報の提供

対象システムで使用されているOSやソフトウェア等の脆弱性情報を週１回以上の頻度で調査し、入手した場合は機構に報告すること。

7．使用機器やサービス等に係る要件

対象システムの監視や脆弱性の検出等において、機器やサービス類を利用する場合、以下の要件を満たすこと。

7.1 費用負担

利用に関する費用は、請負者が負担すること。

7.2 クラウド上での利用について

クラウド上で機器やサービス類を利用する場合、以下の要件を満たすこと。

① 機器やサービス類をAzure上で運用する場合、機構で契約しているテナント上ではなく、請負者がテナントを別途契約して行うこと。

② 機器やサービスを運用するクラウドサービスの準拠法は日本の法律であること。また、管轄裁判所を日本国内の裁判所とすること。

7.3 機器の構築・設定

(1) セキュリティセンサー（IPS/IDS、WAF等）、エージェントソフトウェア等の機器やサービス等を利用する場合、詳細設定及びシグネチャの設定については、請負者の責任において、適切に構築及び設定を行うこと。

(2) 機器やサービスと対象システムの間でインターネットを経由した通信を行う場合、https等の暗号化された通信であること。

(3) ゲートウェイ型のものを使用する場合は、利用率等の稼働状況及びトラフィック情報について集計すること。また、次の性能を満たすこと。

① スループット: 100Mbps以上
② セッション数: 25万以上

なお、通信量の増加等により、機器やサービス類の性能が不足するもしくは不足が予測される場合は、速やかに機構担当者に相談すること。

7.4 ログの取得

(1) トラフィック・攻撃検知・アラートなどのログを取得・保管すること。

(2) 悪意ある第三者等からの不正侵入、不正操作等の有無を迅速に確認できるようにするため、ログを定期的に点検・分析すること。

(3) 取得したログは、１年以上アーカイブできること。

(4) 機構担当者が求めた場合、指定された範囲のログを提供すること。

7.5 バックアップ

バックアップについて、次に示す要件を満たすこと。

① バックアップを定期的に取得すること。バックアップ間隔は２週間以内、バックアップの保存期間は３か月以上であること。
② バックアップが正常に取得できていることを定期的に点検すること。
③ 保存期間を過ぎたバックアップは適切な方法で消去、抹消又は廃棄すること。自動的な世代管理を設定している場合は、保存期間を過ぎたバックアップ情報が削除されていることを定期的に確認すること。
④ 機器やサービス類を冗長構成にしている場合には、サービスを提供する機器やサービス類を、代替機器やサービス類に切り替えることが可能であること。
⑤ 取得したバックアップ情報から機器やサービス類の運用状態を復元することが可能であること。

８．その他

8.1 第三者委託

請負者は、本業務を自ら履行するものとし、本業務の全部を第三者に委託、又は請け負わせてはならない。ただし、機構に書面によって外部委託の詳細を提出し、許可された場合はこの限りではない。なお、第三者委託を許可された場合であっても請負者は契約による責任を免れることはできない。

8.2 体制整備

(1) 本業務に対する履行体制を整備し、応札時に機構に提示すること。体制は、責任者を明確に示したものであること。また、今後、対象システムが増減した場合に、柔軟に対応できる体制であること。なお、契約後、体制が変更になった場合は、速やかに機構へ報告を行うこと。

(2) 請負者は、情報セキュリティの確保を目的とした体制を整備し応札時に機構に提示すること。報告する体制には、情報セキュリティの確保に関する責任者を含めること。また、体制が変更になった場合は速やかに機構へ報告を行うこと。また、情報セキュリティ侵害発生時には、機構の情報セキュリティ監査を受け入れること。

(3) 請負者は、本業務における情報セキュリティ対策が適切に履行されていることを、ひと月ごとに書面にて機構に提出すること。また、情報セキュリティ対策が不十分だったことが判明した場合、請負者の責において、適切な対策を講ずること。

8.3 機密保持

請負者は、業務を実施するに当たり、機構から取得した資料(電子媒体、文書、図面等の形態を問わない)を含め、取り扱う情報を第三者に開示又は本調達の業務以外の目的で利用しないものとする。

また、取り扱う情報について、以下のことに留意すること。

① 取り扱う情報は情報セキュリティ対策業務のみに使用し、他の目的には使用しないこと。
② 取り扱う情報は情報セキュリティ対策業務を行うもの以外には秘密とすること。
③ 取り扱う情報は情報セキュリティ対策業務を行う場所から持ち出さないこと。
④ 取り扱う情報は機構の許可なく複製しないこと。
⑤ 取り扱う情報については、請負期間終了時に廃棄もしくは抹消を確実に行うこと。機器やサービス等を利用した場合は、機器・サービスごとにデータ消去証明書を機構に提出すること。
⑥ 機密保持契約については、請負期間終了後も同様の扱いとすること。

ただし、次のいずれかに該当する情報は除く。

① 機構から取得した時点で、既に公知であるもの
② 機構から取得後、請負者の責によらず公知となったもの
③ 法令等に基づき開示されるもの
④ 機構から秘密でないと指定されたもの
⑤ 第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に機構に協議の上、承認を得たもの

8.4 サプライチェーンリスクマネジメントについて

① 受注者は、サプライチェーンリスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築すること。また、応札時に情報セキュリティの確保を目的とした体制を整備し、機構に提示すること。報告する体制には、以下の情報

を含めること。
●管理体制図
●請負者の資本関係・役員等の情報
●事業の実施場所
●事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報

② 上記の体制が変更になった場合は速やかに機構へ報告を行うこと。
また、情報セキュリティ侵害発生時には、機構の情報セキュリティ監査を受け入れること。

③ 受注者は、本業務における情報セキュリティ対策が継続して適切に履行されているかどうか、報告書に記載すること。また、情報セキュリティ対策が不十分だったことが判明した場合、受注者の責において、適切な対策を講ずること。

④ 受注者は、業務完了後、本件に係る情報を返却または抹消し、そのことを機構に書面で報告すること。

⑤ システムの開発工程において、機構の意図しない変更が行われていないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

⑥ システムに機構の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入検査等、機構と請負者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

⑦ 請負者は、情報セキュリティインシデントが起こった際の対応手順を、応札時に機構に提示すること。

⑧ 情報セキュリティインシデントが発生した際には、ただちに機構に報告すること。

⑨ 受注者は、機構がサプライチェーンリスクに係る情報セキュリティインシデントを認知した場合又はその疑いが生じた場合に、必要に応じて業務内容、作業プロセス又は成果物を立ち入り検査等で機構が確認することを了承すること。

8.5　契約の履行について

本調達の履行について疑義が生じたとき、又は本調達に伴い機構と交わす契約書に定めない事項については、機構及び請負者の双方で協議の上決定すること。
それにより追加業務等が発生する場合は、高専機構本部財務課契約係を通して発注するので、請負者はそれ以外の者からの発注や依頼を受け付けないこと。

8.6　損害発生時の対応について

請負者の故意又は過失により損害が発生した場合は、請負者の責により原状復帰すること。