

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4年11月



独立行政法人 国立高等専門学校機構

目次

1. 調達件名	3
2. 調達の目的等	3
2.1 調達の目的.....	3
2.2 情報セキュリティ対策の必要性.....	3
3. 請負期間	3
4. 対象システム	3
5. 受注条件	4
6. 業務内容	4
6.1 対象システムの監視.....	4
6.2 対象システムにおける脆弱性の診断.....	5
6.3 診断結果への対応.....	5
6.4 対象システムに関する脆弱性情報の提供.....	6
7. 使用機器やサービス等に係る要件	6
7.1 費用負担.....	6
7.2 クラウド上での利用について.....	6
7.3 機器の構築・設定.....	6
7.4 インシデント発生時の対応.....	7
7.5 ログの取得.....	7
7.6 バックアップ.....	7
8. その他	7
8.1 第三者委託.....	7
8.2 体制整備.....	8
8.3 機密保持.....	8
8.4 技術提案について.....	9
8.5 ワーク・ライフ・バランス等の推進に関する評価.....	9
8.6 サプライチェーンリスクマネジメントについて.....	9
8.7 契約の履行について.....	10
8.8 損害発生時の対応について.....	10

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5年4月1日～令和6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。

- 統合データベースシステム『UDB』（Unified DataBase）
- CBTシステム(学生用)
- CBTシステム(作問用)
- 新CBTシステム検証環境
(ただし、令和5年9月1日～令和5年12月31日まで)
- 教材共有システム
- ルーブリック集計システム
- データベース修正用システム

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。

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。それ以外の脆弱性について検出・攻撃の排除が可能な場合は加点する（**一部加点項目**）。
 - 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

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。

必要な対応作業を請負者側で行う場合は加点する。（**加点項目**）

- (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2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』」と「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 インシデント発生時の対応

機器やサービスが情報セキュリティインシデントを起こした場合、速やかに状況を調査し、機構に報告すること。また、速やかに再発防止策を策定し、資料にまとめて機構へ提出すること。なお、本資料は電子ファイルで作成・提出するものとする。

7.5 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。

7.6 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して指定されたもの
- 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 技術提案について

- (1) 本件業務について、本書の要求をどのように満たすか、あるいはどのように実現するか技術的要件ごと具体的に技術提案を行うこと。また、そのための提案書等資料を提出すること。
- (2) 提出された提案書等に基づき、プレゼンテーションを行うこと。プレゼンテーションの実施については別に指定する。
- (3) プレゼンテーションにより、機構における業務の実施に有効な提案がなされた場合は、評価の際に加点する。（**加点項目**）

8.5 ワーク・ライフ・バランス等の推進に関する評価

女性の職業生活における活躍の推進に関する法律に基づく認定企業（えるぼし認定企業）、次世代育成支援対策推進法に基づく認定企業（くるみん認定企業等）及び、青少年の雇用の促進等に関する法律に基づく認定企業（ユースエール認定企業）については加点するので、認定されていることが確認できる書面の写しを提出すること。

なお、配点は別紙「高専情報環境に係る情報セキュリティ対策業務 加点項目および評価基準」により、複数の認定が該当する場合は、最も配点が高い区分により加点することとする。（**加点項目**）

8.6 サプライチェーンリスクマネジメントについて

- (1) 請負者は、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、応札時に管理体制図を機構に提示すること。
- (2) 請負者は、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。
- (3) 本業務において使用する機器等については予め機構に機器等リストを提出し、機構がサプライチェーンリスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、機構と迅速かつ密接に連携し提案の見直しを図ること。

(4) その他、サプライチェーンリスクに関し、以下の資料を提出し、対策を講じていることを証明した場合は加点する。(加点項目)

- ① 当該システムに関して、想定されるサプライチェーンリスク及びそれに対する軽減策についての説明資料
- ② 想定されるサプライチェーンリスクに鑑み、当該システムで使用される機器を選定した理由に関する説明資料
- ③ 調達機関の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類
- ④ 当該システムに調達機関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、追跡調査等を実施する手順及び体制を示す資料
- ⑤ 各種認証取得に関する資料
- ⑥ 我が国政府機関における類似のシステム構築・運用実績

8.7 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。

8.8 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。