高専情報環境に係る
情報セキュリティ対策業務 一式

令和２年１１月

独立行政法人 国立高等専門学校機構

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

(1) 調達の目的

本調達は，Microsoft Azure の高専機構テナント内に構築されている対象システムを安全に利用するために必要となる情報セキュリティ対策や監視等に係る業務である。本調達では，情報セキュリティ対策の必要性とともに，対象システムを安全に利用する上で，必要となる情報セキュリティ要件を求めるものである。

(2) 情報セキュリティ対策の必要性

独立行政法人は，政府機関等と同様に，政府統一基準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，取り扱う情報システム及び情報に対する適切な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・確保が不可欠である。

(3) 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。

- ・データベース「KOREDA」 (Kosen Open REsource Database)
- ・CBTシステム(学生用)
- ・CBTシステム(作問用)
- ・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

３．請負期間

令和３年４月１日～令和４年３月３１日

４．情報セキュリティに関する要件

4.1　調達するシステムの構成

(1) システムの構成

① 情報セキュリティ対策を講じるための機器やサービス類については，今後対象システムが増減した場合に柔軟に対応できるシステムであること。

② 調達するシステムを Azure 上で運用する場合でも，機構で契約しているサブスクリプションではなく，落札者が別途契約したサブスクリプションにて運用すること。

4.2　対象システムの構成管理

(1) 対象システムに係る台帳等の整備

① 対象システムに対して，セキュリティ要件に係る事項について，システム台帳に整備すること。

② 対象システムを新規構築又は更改する際には，システム台帳のセキュリティ要件に係る内容を記録又は記載し，当該内容について機構担当者へ報告すること。

(2) 対象システム関連文書の整備

① 対象システムの情報セキュリティ対策を実施するために必要となる文書として，以下

を網羅した情報システム関連文書を整備すること。

- 対象システムを構成するサーバ装置及び端末関連情報
- 対象システムを構成する通信回線及び通信回線装置関連情報
- 対象システム構成要素ごとの情報セキュリティ水準の維持に関する手順
- 情報セキュリティインシデントを認知した際の対処手順

4.3 対象システムの監視

(1)対象システムの安定的な稼働及びセキュリティインシデント（予兆も含む）に対する迅速な対応を可能とするため，下記の監視を行うこと。

- 稼働監視
- 障害監視
- リソース監視
- 情報セキュリティ監視

(2)対象システムの監視サービス提供時間は 24 時間体制とする。

(3)対象システムの監視は，対象システムが正常稼動していることを常時監視するとともに，障害発生時には発生事象の検知と記録を行い，速やかに機構担当者へ連絡をすること。また，連絡を行う際には，可能な限り，事象の発生原因及び推奨対策を助言やサポートをすること。

(4)情報セキュリティ対策を講じるための機器やサービス類として，対象システムに対する不正検知やマルウェア検知などの情報セキュリティ侵害を監視・検知するために必要となるサービスや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は，本情報セキュリティ対策業務の調達に含めるものとする。また，セキュリティセンサー等の詳細設定及びシグネチャの設定についても，適切に構築及び設定を行うこと。

(5)対象システムにおいてサービス不能攻撃への対策を実施するため，対象システムまたは通信経路における通信の監視を行うこと。ただし，インターネットを経由した対象システム及びWAFと対象システムとの通信は，HTTPS通信とする。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，攻撃元からの通信を遮断する又は，対象システムをネットワークから遮断する，通信回線の通信量を制限するなどの手段を検討し，対応を行うこと。

(6)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。必要な対応作業を受注者側で行う場合は加点する。

(7)監視状況の結果は，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。また，作成した監視報告書は，翌月初旬を目途に機構担当者へ提出すること。監視報告会は3か月に一度行うこととする。ただし，緊急の報告が必要となった場合

は，その都度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）や人的リソース等は，受注者にて準備するものとする。

(10)納入するシステムが情報セキュリティインシデントを起こした場合，速やかに具体的な報告を機構に行うこと。また，速やかに再発防止策を策定し機構へ提出すること。

4.4 対象システムの対策

(1) 対象システムの運用開始後に，新たに確認された対象システムの脆弱性を排除するため，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 等を参照し，構築時及び定期的に脆弱性診断を実施すること。

(2) 対象システムに対する脆弱性については，以下の既知の脆弱性を排除すること。それ以外の脆弱性を排除する場合は加点する。

- SQL インジェクション脆弱性
- OS コマンドインジェクション脆弱性
- ディレクトリトラバーサル脆弱性
- セッション管理の脆弱性
- クロスサイトスクリプティング脆弱性
- クロスサイトリクエストフォージェリ脆弱性
- クリックジャッキング脆弱性
- HTTP ヘッダインジェクション脆弱性
- バッファオーバーフロー及び整数オーバーフロー脆弱性

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。

(3) 対象システムに対する情報セキュリティ対策を講じるための機器やサービス類を本業務に含めること。ただしゲートウェイ型の機器やサービス類は次の性能を満たすこと。なお，本情報セキュリティ対策業務に関しては，機器やサービス類の利用率等の稼働状況及びトラフック情報について集計すること。また，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。

- スループット: 100Mbps以上
- セッション数: 25万以上

4.5 ログの分析

(1) 対象システムにおいて情報セキュリティ対策を講じるための機器やサービス類が取得・保管しているログを定期的に点検又は分析する機能や仕組み設け，分析結果等の閲覧などにより，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可能なこ

と。

4.6　脆弱性診断

(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等，脆弱性診断や脆弱性情報の収集等により脆弱性に対する対応状況を，構築時及び契約期間中に1回以上実施すること。

※　実際の対象となるIPアドレスやWebアプリケーションに関する情報は，受注者へ別途，個別に共有するものとする。

(2) 認知した脆弱性の結果は，機構担当者へ報告を行うこと。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，脆弱性の改修に際して，必要な助言やサポートを行うこと。

4.7　脆弱性対応

(1) 脆弱性に対する対策が講じられていない状態が確認された場合並びに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に実施可能な対応を検討し，根本対応を実施するまでの暫定対処を講じること。

4.8　バックアップ・アーカイブ

(1) 情報セキュリティ対策を講じるための機器やサービス類について，次に相当する要件を満たすこと。

- 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。
- 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。
- 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なことを確認すること。
- 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なことを確認すること。
- 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か月以上とする。

(2) 情報セキュリティ対策を講じるための機器やサービス類について，トラフィック・攻撃検知・アラートなどのログを，1年以上アーカイブできること。

5．その他

5.1　第三者委託

受注者は，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。

5.2　情報セキュリティを確保するための体制の整備

受注者は，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。

5.3　機密保持

受注者は，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。

・取り扱う情報は情報セキュリティ業務のみに使用し，他の目的には使用しないこと。
・取り扱う情報は情報セキュリティ業務を行うもの以外には秘密とすること。
・取り扱う情報は情報セキュリティ業務を行う場所から持ち出さないこと。
・取り扱う情報は機構の許可なく複製しないこと。
・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。

- 機構から取得した時点で，既に公知であるもの
- 機構から取得後，請負者の責によらず公知となったもの
- 法令等に基づき開示されるもの
- 機構から秘密でないと指定されたもの
- 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

5.4　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。

5.5　情報セキュリティマネジメントシステム等の認証について

受注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若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。

また，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イバシーマーク（JISQ15001）使用許諾の認証を受けていること。

5.6　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。

5.7　請負期間終了後のデータの取り扱いについて

受注者は，本契約の請負期間が終了した場合，速やかに設定を解除しサーバ及び通信機器内のデータを消去する事，その際データ消去証明書を発行し後日高専機構へ提出すること。

5.8　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，応札時に管理体制図を機構に提示すること。

(2) 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。

(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。

- 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
- 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
- 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
- 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
- 各種認証取得に関する資料
- 我が国政府機関における類似のシステム構築・運用実績