KOREDA を核とした情報システムに対する
情報セキュリティ対策構築支援業務　一式

仕　様　書

平成 30 年 12 月

独立行政法人　国立高等専門学校機構

１．　件名

KOREDA を核とした情報システムに対する情報セキュリティ対策構築支援業務　一式

２．　調達の背景および目的

独立行政法人国立高等専門学校機構（以下「機構」という）においては、KOREDA(Kosen Open REsource DAtabase)を中心とした学生統合情報システムを開発中である。学生統合情報システムは、国立高等専門学校(以下「高専」という)における教育活動の基盤となるものであり、統合されたデータベース及び付随するシステム群から構成されている。当該データベース及びシステム群を運用するにあたり，必要となる情報セキュリティ対策や監視等について検討し、実際の稼働に向けた要件定義及び調達支援などを求めるものである。

３．　請負期間

契約締結日～平成 31 年 3 月 25 日

４．　業務の内容

4.1. 業務の概要

機構における学生統合情報システムの構成及び情報セキュリティ対策、運用状況等を調査し、学生統合情報システムに内在する情報セキュリティ上のリスクの有無や課題について、安全性を確保するために必要な推奨対策に関する情報をとりまとめ、学生統合情報システムにおける情報セキュリティ対策システムを調達するための支援を行うこと。

4.2. 業務の対象

学生統合情報システムのうち、平成 31 年 10 月に運用開始予定の次の各システムとする。ただし関係するネットワーク環境を含む。

・統合データベースシステム(KOREDA)
・入試・教務システム
・時間割作成システム
・Web シラバスシステム
・CBT システム
・教材共有システム
・ルーブリック集計システム
・学生ポートフォリオ
・証明書発行システム
・出席管理システム
・学校ポートレイトシステム

なお、学生統合情報システムの全体概要は、参考資料として図 1 および図 2 に示す。全てのシステムはクラウドプラットフォーム上に構築される。

4.3. 業務の詳細

調達する業務は以下のとおり。

4.3.1. 現状調査

業務対象に関するネットワーク構成及びシステム構成を調査し、現状把握することが可能と

なるネットワーク構成図、システム設定情報（設定シート等）を作成すること。現状調査に際しては、既存ドキュメントの確認及び精査も行うこと。ただし、既存情報はほぼ存在していないことを前提に、現地での実施調査（統合データベースシステム(KOREDA)・ルーブリック集計システムについては鹿児島、それ以外のシステムは東京都内）及び担当者へのヒアリング等（遠隔についてはSKYPE 等利用）を行うこと。また、対象のシステムに関する情報セキュリティ対策の施策状況及び運用状況について次の現状調査を行うこと。

（ア）ネットワーク構成及びシステム構成の調査、既存ドキュメント（設計書、運用手順書等）の精査、レビュー
（イ）情報セキュリティ関連ドキュメント（ポリシー、規定、手順書など）の調査、確認
（ウ）既存情報の調査（実地調査、実機調査、担当者ヒアリング等）
（エ）現状調査を踏まえて、ネットワーク構成図、システム構成情報等の作成

4.3.2. リスクアセスメント

現状調査の結果を踏まえて、対象のシステムに対する情報セキュリティに関する次のリスクアセスメント業務を実施すること。

（ア）対象システムに関する情報資産の洗い出し（システム、データ、アカウント等）
（イ）対象システムに関連した情報セキュリティ関連ドキュメントの精査
（ウ）システム管理責任者、担当者等に対する対面によるヒアリング
（エ）情報セキュリティの対策状況を分析・評価
（オ）情報セキュリティ対策における懸念事項と推奨対策の取りまとめ（情報資産、懸念事項、推奨対策、推進計画、優先順位明確化 等）
（カ）リスクアセスメント報告書の作成
（キ）報告会の実施

なお、リスクアセスメントにおいては、次の点について評価する。

- 情報セキュリティに関連した既存の規定類や関連ドキュメントの確認、精査、担当者へのヒアリング、対策状況の分析等を行い、リスクアセスメントに反映させること。
- リスクアセスメントの分析には、セキュリティ上の懸念事項だけではなく、リスクレベル、必要対策（必須対策、推奨対策等）を報告書に分かりやすく取りまとめること。
- 国内外で活用されている下記情報セキュリティガイドライン等の要素を複数取り入れ、客観的かつ網羅的な観点で対策状況を評価すること。
  - The CIS Critical Security Controls for Effective Cyber Defense（CSC 20）
  - JIS Q 27001（ISMS, Information Security Management System）
  - 政府機関の情報セキュリティ対策のための統一基準（NISC）
  - サイバーセキュリティ経営ガイドライン（経済産業省）
  - NIST Cyber Security Framework（NIST CSF）
  - Strategies to Mitigate Targeted Cyber Intrusions（ DEFENCE SIGNALS DIRECTORATE）
  - 地方公共団体における情報セキュリティポリシーに関するガイドライン（総務省）

  情報セキュリティ確保のための対策を NIST の Cyber Security Framework に準じた 5 分野(特定・防御・検知・対応・復旧)、22 項目(カテゴリ)以上からなる網羅的な観点で評価し、当機構における対策状況を可視化して、分かりやすく整理

すること。

- 対策状況の評価には、数値又は段階的な評価基準があること。
- 対策分野の評価は、技術的、組織的、物理的、人的要因を考慮した分析を行うこと。

4.3.3. 対象システム間連携における要件確認およびFIT&GAP分析

リスクアセスメントの結果を踏まえて、次のように対象システム間連携における要件の整理及びFIT&GAPを行うこと。

(ア) 新規のシステム(4．2で提示したシステム以外)を連携させた際のシステム要件の整理・確認
(イ) システム要件とリスクアセスメントの結果によるFIT&GAP分析の実施
(ウ) FIT&GAPの結果取りまとめ(必要業務及び要件等の抽出)
(エ) 報告書作成

4.3.4. 情報セキュリティ対策の調達仕様書の作成支援

学生統合情報システムの情報セキュリティ対策に関する調達仕様書の作成を支援すること。ただし、当機構とともにレビューを行い、レビュー結果を踏まえた修正作業を含むこと。

(ア) 調達仕様書(原案)の作成
(イ) レビュー及び修正作業

4.3.5. 納入成果物

現状調査結果報告書(主な報告事項は下記参照)を電子データ(WORD、EXCEL、POWERPOINT 等)の形式で納品すると共に、その報告会を実施すること。また、現状調査結果報告書の具体の内容については当機構担当者と協議の上で決定すること。

- 現状調査結果報告書
- ネットワーク構成図
- システム構成図(システム設定情報、設定シート等)
- リスクアセスメント報告書
- FIT＆GAP分析報告書
- 調達仕様書原案

なお、成果物の著作権(著作権法第27条及び第28条に定める権利を含む)は、業務終了後に当機構に移転すること。また、成果物について著作者人格権を行使しないこと。

５．　その他

5.1. 業務の実施体制

(ア) プロジェクトの実施体制(問合せ窓口、担当者、補助者)を明示し、整備すること。
(イ) 学生統合情報システムの担当者や開発者などにヒアリングが必要となる場合は、対象となるシステムを事前に明示すること。また、ヒアリングに必要となる実施項目や対応を希望する担当者や開発者など、想定される所要時間等を明示すること。ヒアリング対象の担当者や開発者などの日程調整等は当機構担当者と行うこと。
(ウ) ISO/IEC 27001(ISMS, Information Security Management System)を取得していること。
(エ) 本業務を担当する請負者の体制が下記条件を満たしている場合加点する。

- 情報システムに対するリスクアセスメント業務の経験が過去 3 年以内に 10 回以上あること。
- 本業務を実施するにあたり、2 年以内に CSIRT 運営のアドバイザリ業務、又は CSIRT 構築業務もしくはリスク評価業務の経験があること。
- 情報セキュリティ及びサイバーセキュリティの情勢や技術動向について、十分な知識と経験を有していること。
- 中央省庁または公共団体等における CISO（最高情報セキュリティ責任者）または CISO に準ずる経験がある者をプロジェクト体制に含めること。
- 本業務の責任者及び担当者は、下記資格のいずれかを有していること。
  - CISSP（Certified Information Systems Security Professional）
  - CISA（Certified Information Systems Auditor、公認情報システム監査人）
  - CISM（Certified Information Security Manager、公認情報セキュリティマネージャー）
  - システム監査技術者試験（IPA）
  - 情報処理安全確保支援士（IPA）

5.2. 実施計画

（ア）当機構と協議し、作業内容と作業スケジュール等を記載した業務実施計画を作成すること。

（イ）業務を円滑かつ効果的に実施するため、定期的に進捗状況、課題状況等の報告などを当機構に行うこと。

5.3. 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。

5.4. 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、契約上知り得た情報を、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。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

5.5. 提案内容のプレゼンテーション評価

（ア）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。

（イ）プレゼンテーションにより、当機構における業務の実施に有効な提案について加点する。

参考資料

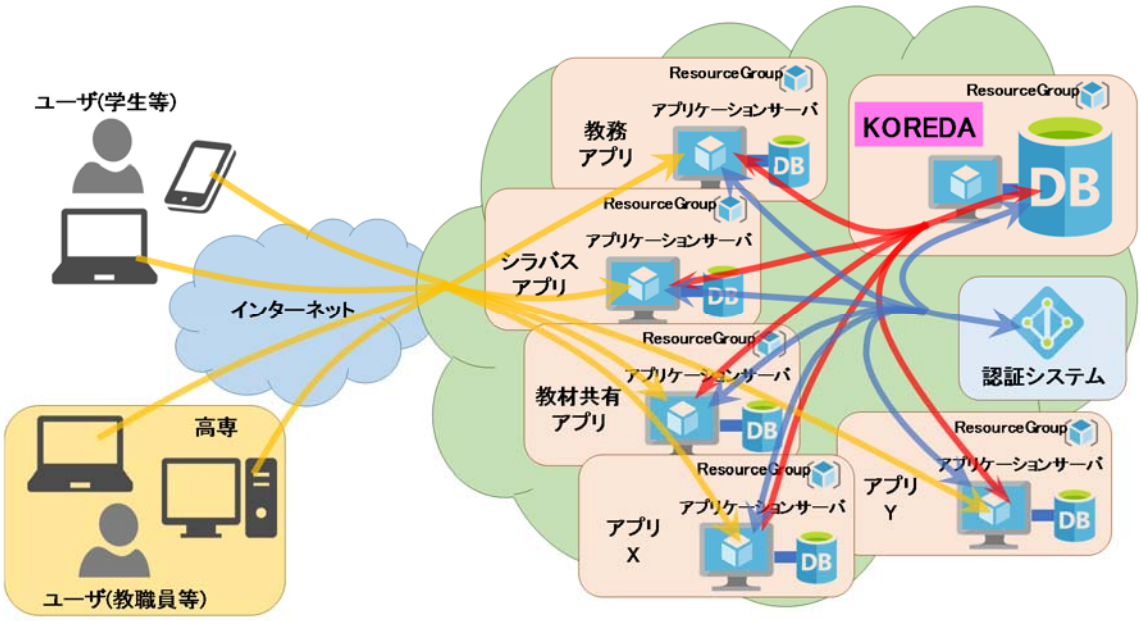

図 1 学生情報統合システムの運用イメージ

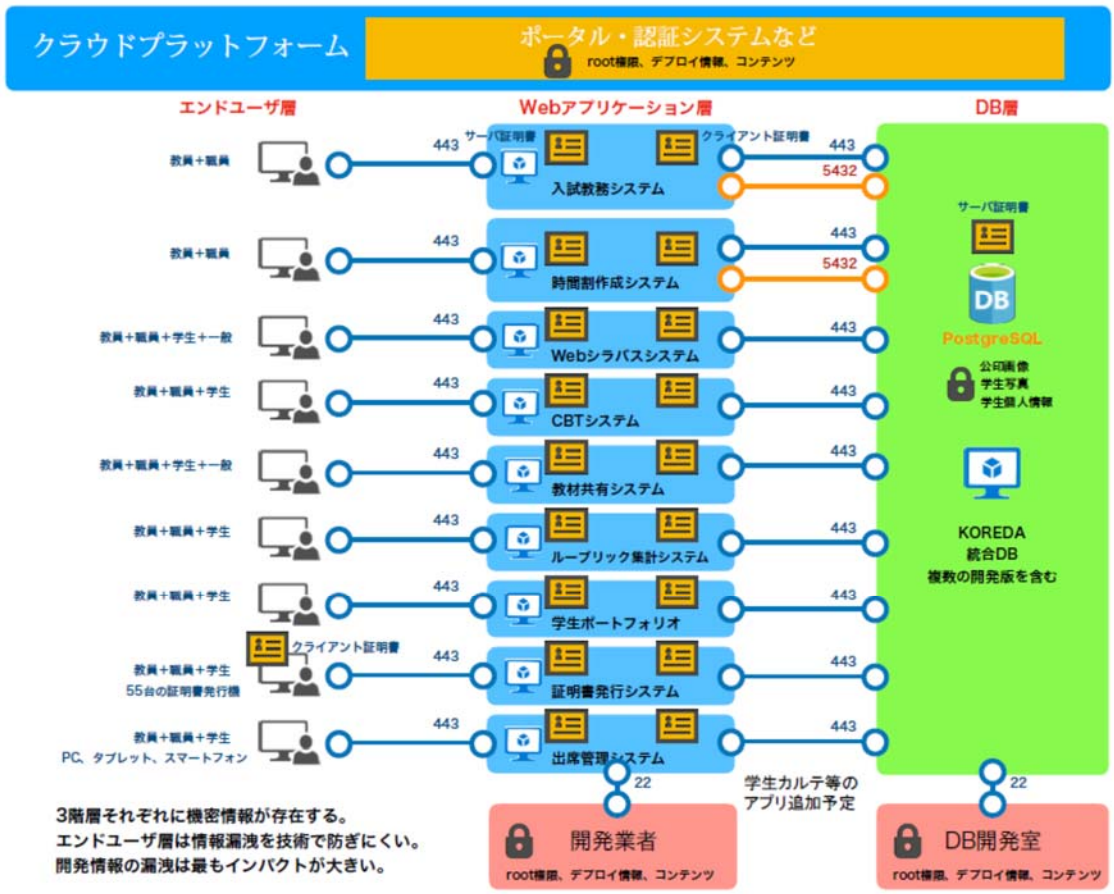

図 2 学生情報統合システムのシステム間連携イメージ