

青森県立学校統合型校務支援システム環境構築・運用保守業務
企画提案要求仕様書

令和 7 年 4 月

青森県教育委員会

目次

第1章 概要.....	3
1 業務概要.....	3
2 調達範囲.....	5
3 規模要件.....	7
4 セキュリティ基盤.....	7
第2章 仕様.....	8
1 統合型校務支援システム.....	8
2 パブリッククラウド.....	8
3 統合認証基盤.....	9
4 校務データストレージ.....	9
5 バックアップについて.....	9
6 データ暗号化.....	9
7 機微情報のデータ紛失/漏洩防止.....	10
8 クライアントパソコン等のデバイス管理.....	10
9 クライアントパソコン等のセキュリティ対策.....	10
10 ダッシュボード機能等(データ関係基盤)の創出.....	10
11 通信回線及び関連機器.....	10
12 可用性.....	11
13 性能・拡張性.....	11
14 メール環境について.....	11
15 保護者連絡ツールとの連携について.....	11
第3章 構築.....	12
1 設計.....	12
2 試験計画及び試験結果報告.....	12
3 構築試験及び構築作業.....	12
第4章 導入支援.....	13
1 データ移行.....	13
2 研修.....	13
3 操作マニュアル.....	13
第5章 運用保守.....	14
1 運用保守.....	14
2 定例会等.....	15
第6章 拡張性・発展性・将来性に関する提案.....	15

第1章 概要

1 業務概要

(1) 業務名称

青森県立学校統合型校務支援システム環境構築・運用保守業務（以下、「本業務」という。）

(2) 背景と趣旨

(ア) 背景

青森県教育委員会（以下、「県教育委員会」という。）では、県立学校の校務の効率化を目的として、令和2年度から統合型校務支援システムをオンプレミス型として導入し、現在までの運用に至っている。セキュリティ体制についても従前の「教育情報セキュリティポリシーに関するガイドライン（平成29年10月18日）」に基づいた構成となっている。

文部科学省は「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～（令和5年3月8日）」において、次世代の校務 DX の方向性として3つの観点（働き方改革の観点、データ連携の観点、レジリエンスの観点）を掲げ、アクセス制御を前提としたネットワークにおける情報セキュリティの考え方の下、校務支援システムのパブリッククラウド上での運用を推奨している。

そのため、青森県教育委員会では更なる校務の効率化・標準化、システムを活用することによる教育データの利活用など次世代の校務 DX に向けて、「教育情報セキュリティポリシーに関するガイドライン（令和7年3月）」に基づき、文部科学省が推奨するクラウド環境の活用をベースとしたシステム環境を整備し、外部システムとの教育データ連携の促進を図り、教育データ利活用による教育の質の向上を目指すものである。

(イ) 趣旨

青森県立学校において児童生徒、家庭（保護者）、学校が一体となった教育活動の展開による教育の質の向上を目指すことを目的として、教育データやクラウド技術を活用した次世代の教育環境を実現するため、統合型校務支援システムのクラウド環境での構築・運用及び保守業務について企画提案競技により事業者を選定するための手続きに必要な事項を定めるものである。

(3) 業務内容

(ア) 統合型校務支援システム等の導入

統合認証基盤を介して、IaaS 型または SaaS 型のパブリッククラウド（以下、「パブリッククラウド」という。）に接続するクラウドサービスとして提供すること。

県立学校に統一した統合型校務支援システムを導入し、校務事務の負担軽減を図ること。

文部科学省の「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」内にある、「3. 次世代の校務 DX の方向性」の「(4) データ連携基盤（ダッシュボード）の創出」を参考に、各種データを連携し可視化する仕組みを提案すること。

(イ) 校務系ファイルサーバのデータ移行

既存データセンターで運用されている、校務系ファイルサーバの校務データ等、校務に関する重要な情報（機微情報）をパブリッククラウドへ移行する。ファイルは学校単位、県教育委員会単位で管理可能とする。

(ウ) 強固なアクセス制御の実装とデータ暗号化

(ア) で移行した機微情報は、重要な情報資産であり、紛失、漏洩等を防止するため、強固なアクセス制御を実装し不正アクセス等を防止すること。また対象となる機微情報はデータ保護の観点からデータ暗号化できること。

(エ) 校務系システムとインターネット接続の経路

現在、校務系システムは青森県教育ネットワークの校務系（仮想化）環境にあり、その経路は県総合学校教育センターにて校務系（仮想化）と校務外部接続系（インターネット接続）に分離されている。本業務にて校務系システムがパブリッククラウド利用となるため、校務系（仮想化）への経路を廃止すること。

また、学校からのインターネット接続は、別事業にて、学習系回線からのみとする予定である。

(オ) 統合型校務支援システムなどのクラウド利用環境におけるセキュリティ対策の導入

外部記憶媒体の利用制限や統合型校務支援システム環境の利用者を特定するための認証システム、クライアントパソコン等端末のネットワークへの不正接続を防止する機能を提供し、情報の不正持ち出し、不正利用を防止すること。

(カ) SaaS 型パブリッククラウド統合認証基盤と統合型校務支援システム環境等の認証連携

SaaS 型パブリッククラウド統合認証基盤（以下、「統合認証基盤」という。）への認証を通じて、シングルサインオン（SSO: Single Sign On）により、統合型校務支援システムへの追加認証を行うことなくアクセスできること。

(4) 前提条件

(ア) 統合型校務支援システム環境構築及び運用

本業務では、統合型校務支援システム環境を構築し、本稼働後 5 年間の運用保守を行うものとする。

(イ) 情報セキュリティにおける公的認証

情報セキュリティマネジメントシステム「ISO/IEC 27001」を取得していること。

ISMS クラウドセキュリティ認証「ISO/IEC 27017:2015」を取得していること。

政府情報システムのためのセキュリティ評価制度(ISMAP)を取得していること。

(ウ) セキュリティポリシーへの準拠

文部科学省の「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」(令和 5 年 3 月 8 日) 及び「教育情報セキュリティポリシーに関するガイドライン(令和 7 年 3 月)」に準拠したものとする。

(エ) 統合型校務支援システム環境の設置場所について

統合型校務支援システム環境の設置場所はパブリッククラウド上とし、外部からの攻撃者等の脅威から保護し、情報セキュリティリスクを最大限低減すること。

また、大規模災害等の不測の事態を想定し、機微情報のデータバックアップ/データリストアを実現し、統合型校務支援システム環境の BCP/BCM についても考慮すること。

(オ) 統合型校務支援システムの導入

県立学校向けの統合型校務支援システム環境を導入することとし、構築に当たっては、効率的かつ効果的なシステムを導入するため、他の教育委員会に浸透している質の高いシステムを採用することを基本とする。

なお、都道府県及び政令指定都市において、本県同等以上の規模（規模については「3 規模要件」を参照）を対象に、文部科学省が推奨するパブリッククラウド及びゼロトラストセキュリ

ティを利用した、集中管理型運用による全校運用稼働・運用実績を持つ製品であること。また、一般財団法人全国地域情報化推進協会（APPLIC）が規定した「教育情報アプリケーションユニット標準仕様」v2.0 以降の準拠登録・互換接続確認製品（オレンジマーク）であること。

既存の統合型校務支援システム環境で運用されているデータについては、新たに導入される統合型校務支援システム環境へ最新のデータを移行すること、データ移行時は教職員への影響が極力でないこと。

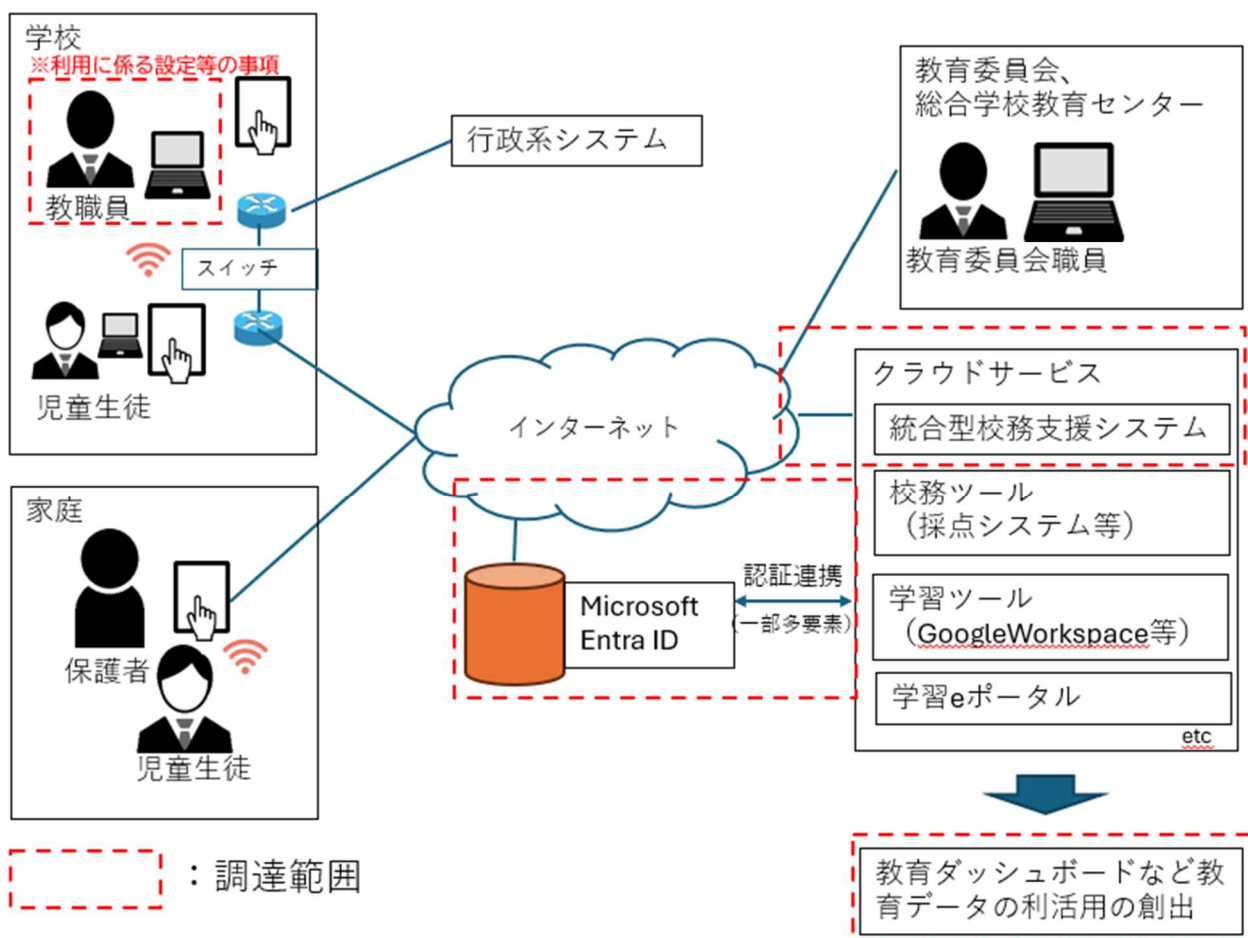
統合型校務支援システム環境の機能及び帳票等について、県教育委員会及び各県立学校が必要又は有効である場合には、県立学校が取りまとめ、試行時及び保守において可能な範囲でカスタマイズを依頼できるものとする。

2 調達範囲

（１）調達範囲については次のとおりとする。（構築に係る環境整備を含む。）

- ・ 統合型校務支援システム
- ・ パブリッククラウド
- ・ 統合認証基盤
- ・ データ暗号化
- ・ 機微情報のデータ紛失/漏洩防止
- ・ 校務データストレージ
- ・ クライアントパソコン等のデバイス管理
- ・ クライアントパソコン等のセキュリティ対策
- ・ 通信回線及び関連機器
- ・ ダッシュボード（データ連携基盤）の創出
- ・ 上記に係る機器賃貸借及び運用保守

(2) 全体構成イメージは下図とする。



- 各種教育データを連携し可視化する教育ダッシュボード等の仕組みを提案に含めること。
- 教職員端末からの利用にあたり、必要となる設定等の内容を含む。
※教職員端末の調達は含めない。
- 学校、教育委員会、家庭からの通信回線は調達範囲に含めない。
※ただし、環境構築、運用・保守に必要な通信回線は含めること。
- その他、上記図中以外で必要となる要件等がある場合は提案に含めること。

3 規模要件

項目	数値
拠点数（県立高等学校 46 校、県立特別支援学校 20 校、県立中学校 1 校） ※令和 9 年度に大湊高等学校と、むつ工業高等学校が統合し、新しい学校となる（大湊高等学校と、むつ工業高等学校は令和 10 年度末で閉校） ※令和 9 年度に浪岡高等学校と、青森西高等学校が統合し、新しい学校となる（浪岡高等学校と、青森西高等学校は令和 10 年度末で閉校）	67 拠点 （令和 9 年度～ 69 拠点） （令和 11 年度～ 65 拠点）
県教育庁、県総合学校教育センター	2 拠点
クライアントパソコン数（教職員）	3,800
統合型校務支援システムのアカウント数（教職員）及び教職員数及び教職員用 Microsoft アカウント数	3,800
児童生徒数及び児童生徒用 Microsoft アカウント数	22,050

※閉校となる学校について、閉校後はそれぞれの統合校で証明書発行等が可能なこと。

4 セキュリティ基盤

今回の調達範囲に対して、文部科学省の「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」(令和 5 年 3 月 8 日) 及び、「教育情報セキュリティポリシーに関するガイドライン(令和 7 年 3 月)」に相当する機能を提供すること。

(1) ゼロトラストセキュリティへの変更

校務処理の効率化のため、物理的な分離方式からゼロトラストセキュリティへ変更する。職員室以外からも安全に校務処理が行えるよう教職員の利便性を考慮し、かつセキュリティを担保し安全に利用できるよう構成する。

県立学校の教職員及び児童生徒は Microsoft365 A3 を利用している。ゼロトラストセキュリティの実現については、Microsoft365 A5 にステップアップし、A5 の機能を積極的に活用して実現するか、A3 をベースにした他の提案で実現すること。

(2) 情報セキュリティ強化

令和 7 年 3 月に改訂された「教育情報セキュリティポリシーに関するガイドライン」(文部科学省) に準じた、アクセス制御による対策を講じたシステム構成とし、重要性分類毎の情報を安全に取り扱うために、情報セキュリティを強化する。

(3) 校務系 AD の一元管理

現在は、教職員の校務用パソコンのアカウント管理には、オンプレミス型で Windows ActiveDirectory (AD) を利用しているが、クラウド型の EntraID での管理に移行する。

(4) 学校毎のファイル共有サービスの管理

現在は、オンプレミス型で各校から利用できるファイルサーバ(各校 500GB) を配置しているが、Microsoft365 で使用できる SharePoint や OneDrive、または他クラウドサービス等で提案すること。

(5) SSO の実装

使用する各種サービスに Microsoft365 アカウントを基本とした SSO を実現すること。

※提案に当たっては、以下の仕様、構築、導入支援、運用保守の各要件に留意すること。

第2章 仕様

1 統合型校務支援システム

- (1) 統合型校務支援システムについては、各県立学校で利用されている既存のクライアントパソコン（約3,800台）で利用できることを前提として、最適なパフォーマンスを実現できるように構成すること。

（クライアントパソコンの主な仕様）

項目	仕様
OS	Windows10、11（令和7年10月からはWindows11のみ）
CPU	Intel Core i3 第8世代以降
メモリ	8GB
Office	Microsoft365 A3

- (2) 別紙1「統合型校務支援システム機能要件」、別紙2「グループウェア機能要件」の機能を有すること。
- (3) 各県立学校で利用する機能や帳票については仕様を統一するものとする。ただし、学校運営の独自性や特色を損なわないよう構築業務委託期間において教育委員会と協議し、本調達費用範囲内でカスタマイズを協議するものとする。
- (4) データ量の増加、将来的な機能拡張に伴うシステム拡張の容易性を担保できるシステムとする。また、学習指導要領等の法の改訂による変更は、契約の範囲内で、原則無償で対応すること。ただし、本仕様書の機能以外のシステム拡張による諸費用は当該受託者と別途協議する。
- (5) 制度改正に伴う指導要録等の様式変更などについて、他都道府県における過去の変更実績と、どのように対応するのか経費負担の有無を含め提案すること。
- (6) グループウェア機能については、統合型校務支援システムと別製品でも構わないが、統合型校務支援システムとユーザ管理を連携する機能を持つこと。
- (7) 教職員が利用するクライアントパソコンは、令和7年度から順次更新し、Windows Helloに対応した機器となる。全てのクライアントパソコンがWindows Helloに対応するのは、令和11年度を予定している。
- (8) 統合型校務支援システムの運用にあたり、生体認証リーダーやバーコードリーダーなど必要となる付帯機器がある場合は含めること。

2 パブリッククラウド

- (1) 日本国内にある、本県から直近のリージョンであること
- (2) 事前に定義した不正アクセスパターンとマッチングすることにより、不正なアクセスを検知（IDS：Intrusion Detection System）及び遮断（IPS：Intrusion Prevention System）する仕組みを導入すること。
- (3) DDoS 対策を講じること。
- (4) 統合型校務支援システム等のシステムに対し、マルウェア対策を講じること。
- (5) 統合型校務支援システムが稼働するVM（Virtual Machine）はディスク暗号を講じること。

- (6) 事前に定義した不正アクセスパターンとマッチングすることにより、統合型校務支援システムの Web アプリケーションの脆弱性対策（WAF：Web Application Firewall）及び不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする対策（WAF）について、必要に応じて提案すること。
- (7) 統合型校務支援システム等のシステムに対して、保守アクセス（リモートメンテナンス）を実施するため、安全な経路による接続ができる機能を講じること。

3 統合認証基盤

- (1) 現在、データセンターで運用されている Active Directory を統合認証基盤（EntraID）に移行し、デバイス管理及びアカウント管理を行うこと。
- (2) 統合型校務支援システムやクラウドツールが統合認証基盤と連携し、SSO が可能であること。
- (3) 統合型校務支援システムへのアクセス制御の仕組みとして、多要素認証の機能を提供すること。多要素認証の手段としては、教職員の私物（スマートフォンなど）を使用せず実現すること。また、教職員のクライアントパソコンが Windows Hello 対応のものに移行していくことを考慮すること。
- (4) リスクベース認証により、校内、校外での条件付きアクセスを講じること。条件付きアクセスは、アクセス条件の組み合わせによりアクセス先の可否を講ずること。
- (5) 県立学校毎にグループ分けし、アカウント管理ができること。
- (6) 保護ポリシーにより適切にデータ保護ができること。

4 校務データストレージ

- (1) 現在、データセンターで運用されているファイルサーバにある校務データ等の機微情報を、クラウド側の共有データストレージに移行すること。
- (2) クラウド側の共有データストレージの階層・構造、アカウント情報やアクセス権については、現在、データセンターで運用されているファイルサーバと同様なレベルで構成され、統合認証基盤で管理すること。
- (3) 各県立学校の管理者に対して、アクセス権限管理等の一部委譲ができること。
- (4) 県立学校 1 校当たり、1 TB 以上の容量を確保すること、ただし現状の運用状況や利用者（教職員）数、今後のデータ容量の増加を想定した容量を計画し、発注者と協議の上で容量を決定すること。また、運用上必要に応じて、容量の拡張が可能であり、拡張時に費用が改めて発生する場合は、発注者と協議すること。

5 バックアップについて

- (1) バックアップは、最低でも日次で取得すること。
- (2) バックアップ手法および範囲は、受注者の提案事項とする。
- (3) バックアップデータのリストアにあたっては、データの完全性を保証すること。

6 データ暗号化

- (1) クラウド利用上、情報漏洩や攻撃者の脅威に対するデータ保護の観点としてデータの暗号化（保存データや転送中データ）を実施すること。データ暗号化の対象は、個人情報や校務データのような機微情報とする。
- (2) データ保護の観点からデータ暗号化を実施するが、利便性も考慮しつつ柔軟なアクセス制御（ア

クセス制御設定の構成等の作成・編集・削除)が可能であること。

- (3) 柔軟なアクセス制御について、発注者と設計・構築・運用中も協議しつつ、教職員の業務への影響を考慮しながら検討・検証・設定すること。
- (4) データストレージ等に暗号化対象のデータ(個人情報や校務データ等)が存在する場合、データ暗号化の対象とすること。

7 機微情報のデータ紛失/漏洩防止

データ紛失/漏洩防止機能(DLP: Data Loss Prevention)により、校務データ等の機微情報を保護し、過剰共有によるリスクを軽減すること。また、誤って又は故意に不適切な共有等で、機微情報を紛失/漏洩することを防ぐこと。

8 クライアントパソコン等のデバイス管理

- (1) クライアントパソコンのハードウェア情報(コンピュータ名、IP アドレス、OS バージョン等)、ソフトウェア情報(アプリケーション情報、Windows 更新プログラム等)を一括収集できること。
- (2) 異常を検知した場合のアラート機能を備えること。
- (3) 情報漏洩等の事故を防ぐため、USB 等の利用制限や不正ソフトウェアのインストールを禁止できること。
- (4) 収集した情報を一覧表示でき、検索条件により抽出できること。
- (5) 許可されていないクライアントパソコン等が接続された場合に検出できること。
- (6) クライアントパソコンに対して、ソフトウェアを配布できること。
- (7) クライアントパソコン等、管理対象のデバイスを紛失や置き忘れた場合でも、リモート操作によりデバイスロック、データ削除や初期化等の対処ができること。

9 クライアントパソコン等のセキュリティ対策

- (1) 現行、オンプレミス方式で EPP (Endpoint Protection Platform) のサーバを構築しているが、EPP をクラウド管理のものに移行することを提案すること。
- (2) パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを分析して適切に対処することで、感染の拡大を防止する機能(EDR: Endpoint Detection and Response)を提供すること。

10 ダッシュボード機能等(データ関係基盤)の創出

学校における教職員の業務効率化や、県教育委員会による学校支援等について、現状運用されている各種データを連携し可視化できる仕組み(ダッシュボード機能等)を提案すること。

11 通信回線及び関連機器

「教育情報セキュリティポリシーに関するガイドライン(令和7年3月)」から、「第1編 総則 第3章 教育現場におけるクラウドの活用について」「(3) 学校現場におけるクラウドサービスの利用」「①IaaS・PaaS 型プライベートクラウドサービスの利用」に準ずること。

1.2 可用性

統合型校務支援システムの構成等について、障害発生時を想定し、予備機への切り替え運用等の対応について提案すること。また、システム停止や故障発生により通信が停止し継続運用ができなくなった場合、速やかに復旧を図ること。復旧のためバックアップデータのリストアが伴う場合も含まれる。

1.3 性能・拡張性

- (1) 通信上のレスポンス低下等、システムの性能面で不測な状態が発生した場合は、県教育委員会に報告の上、原因を究明するとともに、性能低下や性能不足に陥った原因が設計上の不備であった場合については、受注者の費用負担で是正措置を講ずること。
- (2) 学校現場での教育 ICT 化や教育 DX が急速に進んでいくことを考慮した拡張計画を検討し、発注者と協議の上、システム全体の設計を実施すること。
- (3) 統合型校務支援システムの様式変更等が必要となった場合には、随時対応すること。また、法の改定等による様式変更等に対しては、原則無償で対応すること。

1.4 メール環境について

本県で既に導入・運用されているメール環境を新システム導入後も利用できるよう、考慮すること。

1.5 保護者連絡ツールとの連携について

欠席連絡等の保護者連絡ツールがあれば提案すること。また、そのツールと統合型校務支援システムとのデータ連携等があれば提案すること。

第3章 構築

1 設計

- (1) 受注者は、本仕様書及び発注者との協議に基づいて本システムの設計を行うこと。
- (2) システム開発に必要な環境は受注者にて用意すること。

2 試験計画及び試験結果報告

- (1) 単体試験及び総合試験を実施する場合には、受注者は試験計画書を発注者へ提出し、承諾を受けること。
- (2) 単体試験及び総合試験を実施した場合には、受注者は試験結果報告書を発注者へ提出すること。
- (3) 試験計画書及び試験結果報告書を作成する場合には、その内容について、事前に発注者と協議すること。

3 構築試験及び構築作業

- (1) パブリッククラウド、統合認証基盤、統合型校務支援システム

- (ア) 単体試験

パブリッククラウド、統合認証基盤、統合型校務支援システムは、クラウドによるシステム実装であり、事前に単体試験が行えないため、(イ)で各々構築後(2)を実施する前に、試験計画書に基づき、各々でシステムの動作試験を行うこと。

- (イ) 構築作業

設計に基づき各々の構築を実施し、構築後(ア)での記載の通り、試験計画書に基づき、各々でシステムの動作試験を行い、(2)を行った上で移行準備に取り組むこと。

受注者は発注者と協議の上、構築手順書を作成し承認を得ること。

- (2) 総合試験

試験計画書に基づき、(1)構築後、各システムで提供する各種機能・サービスの通信・動作試験や、構成機器の切替試験（冗長構成の切替試験等）の総合的な動作試験を行うこと。

(3) 上記(1)、(2)の試験に係る日程や実施時間帯については、発注者と協議の上、決定すること。

第4章 導入支援

1 データ移行

- (1) 受注者は、事前（設計段階）に統合型支援システムのデータ移行計画書を作成し、発注者と協議の上承認を得ること。
- (2) 受注者は、既存データセンターの仮想化基盤上で運用中の統合型校務支援システムのデータを、パブリッククラウド上で新たに構築した統合型校務支援システムに移行すること
- (3) データ移行は、3（2）総合試験前までに、その時点のデータを移行し各種試験を行い、本業務による本番移行時に差分データを移行すること。
- (4) データ移行後、統合型校務支援システム環境が正常動作していることを確認し、発注者に報告すること。
- (5) 統合型校務支援システム環境が運用開始後、不具合が生じた場合は即時対応し回復させること。
- (6) データ移行で学校現場の教職員に稼働が発生する場合、事前（設計前）に発注者と協議し、必要な移行マニュアルを作成し、発注者の承認を得るとともに、データ移行に関する研修等を行うものとする。また、必要に応じてオンラインによる支援等を実施すること。
- (7) 現行のシステムで使用している外字の移行について提案すること。

2 研修

- (1) 統合型校務支援システムの円滑な導入・稼働を実現するために、各県立学校の管理者、システム管理者、教務担当者、保健管理担当者及び一般教職員を対象とした研修を実施すること。
- (2) 本システムの円滑な導入を実現するため、すべての対象校へシステムの操作に関する研修を実施すること。研修の形態は、複数校以上の対象校をまとめた集合研修での実施も可とする。
- (3) 集合研修の場合は、少なくとも1学校当たり3名程度の教職員に対して行うことを想定する。
- (4) 特別支援学校の学部や障害種別を配慮した、研修計画についての提案を求める。開催場所及び開催時期については、発注者と協議の上、決定することとする。
- (5) 統合型校務支援システムの研修会は、メーカー又は導入するソフトウェアに詳しい指導員が行うこと。
- (6) 研修に必要な道具等は、受注者が準備すること。
- (7) 研修資料については、統合型校務支援システム上で参照できるようにすること。また、内容に変更が生じた場合は、随時、更新及び修正を施すこと。
- (8) 研修終了後、研修内容を発注者へ文書にて報告するとともに、研修資料を電子媒体（Word形式又はExcel形式及びPDF等）で発注者に提出すること。

3 操作マニュアル

- (1) 統合型校務支援システム利用者が、システム操作や業務内容を理解できる分かりやすいマニュアルを作成すること。利用者の立場を十分に考慮すること。
- (2) マニュアルの提供方法として、常に最新の電子マニュアルが参照できるよう、オンラインマニュアルでの提供の仕組みを用意すること。
- (3) システムの改修等によりシステムの仕様とマニュアルに差異が生じた場合、マニュアルを更新して納品すること。

第5章 運用保守

1 運用保守

(1) 運用サービスの提供

- (ア) 受注者は契約期間中、問合せ窓口を開設し、電話又はメール等により県教育委員会、教職員又は県教育委員会設置のヘルプデスクからの問合せに対応すること。
- (イ) 統合型校務支援システム等の操作に関する問合せは、メーカーサポートの範囲とし、標準的な利用方法から外れる場合は、県教育委員会に報告、相談するものとする。
- (ウ) 年度末始の人事異動に伴う、アカウントの登録、変更、削除に係る作業と支援を行うこと。
- (エ) 統合認証基盤等におけるアカウントやセキュリティの運用管理（各種設定変更等）、パブリッククラウドの管理などの運用管理業務を行うこと。統合認証基盤等の設定変更を行う際には、発注者との協議の上でセキュリティ対策や情報漏洩対策を施した上で作業を進めること。
- (オ) 月次で運用サービスの状況を報告すること。

(2) 保守サービスの提供

- (ア) アプリケーション及びシステムサービス等の不具合を検知又は県教育委員会及び教職員より報告を受けた場合、不具合の原因を調査し、メーカー等と連絡・協議を行い、速やかに問題解決及び不具合の復旧を実施すること。故障対応記録を発注者へ報告し、故障内容に応じて発注者承認の上、事後対策を実施すること。
- (イ) 情報セキュリティインシデントを検知又は県教育委員会及び教職員より報告を受けた場合、原因の調査を実施し、メーカー等と連絡・協議を行い、速やかに問題解決及び情報セキュリティインシデントを復旧させること。情報セキュリティインシデント対応記録を発注者へ報告し、情報セキュリティインシデントの内容に応じて発注者承認の上、事後対策を実施すること。
- (ウ) 納入する機器は、運用開始から5年以上のメーカー正規のサポートが受けられること。
- (エ) 部品交換等が必要な場合や故障が発生した場合は、速やかに必要な交換、保守等を行うこと。
- (オ) 保守サービス提供時は、県教育委員会、県総合学校教育センター、県教育委員会設置のヘルプデスク等と連携した対応を行うこと。
- (カ) 既存機器は保守対象外とするが、県教育委員会からの相談があれば原因の一次切り分け等を行い、復旧・改善に向けた支援をすること。
- (キ) 月次で保守サービスの状況を報告すること。

(3) 情報資産の廃棄

- (ア) 機微情報を記録している電磁的記録媒体等が不要となった場合には、電磁的記録媒体等の初期化等、情報を復元できないよう処置した上で廃棄すること。
- (イ) 廃棄を行った場合には、処理を行った日時、担当者及び処理内容を記録し発注者へ報告すること。

(4) 契約満了後の対応

- (ア) 本契約期間満了及び契約解除に伴い、本システムから次期統合型校務支援システムにデータの引継が発生する場合は、指定する時期にシステム内の移行対象となるデータをCSV形式等で抽出し、発注者へ提供すること。
- (イ) 本システムから完全にデータを消去すること。なお消去する時期については発注者と協議の上実施すること。

2 定例会等

- (1) 県教育委員会が運営実施する月 1 回の定例会に参加し、運用保守に関する情報交換を行うこと。
- (2) 県教育委員会から要請がある場合又は県教育委員会との協議が必要な事案が発生した場合には、臨時の会議等を開催すること。

第 6 章 拡張性・発展性・将来性に関する提案

本事業の発展性・将来性を考えて、システムの拡張性・発展性について必要に応じて提案すること。

「参考事項」

- ・ 現在利用している各種サービス等は以下である。
 - ① Microsoft365 A3
 - ② Google Workspace for Education
 - ③ デジタル採点システム「百問繚乱」
- ・ 令和 7 年度に学校内のネットワーク構成を再編する予定である。
- ・ 令和 7 年度に県立高等学校、県立特別学校、県立中学校の入学者選抜に係る、Web 出願サービスを構築する予定である。
- ・ 令和 9 年度でオンプレミスのメールサーバを廃止し、Microsoft365 アカウントで使用しているメールに完全移行する予定である。
- ・ 令和 8 年度に学校徴収金システムを構築する予定である。