瀬戸内市教育ネットワーク環境構築・運用保守業務仕様書

瀬戸内市教育委員会

令和８年５月

瀬戸内市教育ネットワーク環境構築・運用保守業務　仕様書

目次

1 業務概要

1.1 業務件名

瀬戸内市教育ネットワーク環境構築・運用保守業務（以下「本業務」という。）

1.2 業務背景・目的

文部科学省は、GIGAスクール構想の進展に伴うクラウドサービスの本格活用や、児童生徒の学び方・教職員の働き方の変化等を踏まえ、「教育情報セキュリティポリシーに関するガイドライン」を令和7年3月に改訂した。あわせて、校務DXの推進に当たっては、従来の閉域網・オンプレミスを前提とした境界防御に依存するのではなく、いわゆるゼロトラストの考え方に基づき、強固なアクセス制御等により情報セキュリティを確保した上で、クラウド活用を前提としたシステム構成へ移行していく方向性が示されている。

瀬戸内市教育委員会（以下「教育委員会」という。）においても、これらの国の方針を踏まえ、新しい校務の在り方として、「学校における働き方改革」「教育活動の高度化」「教育現場のレジリエンス確保」の観点から、校務系システム等のクラウド化を進めるとともに、必要なセキュリティ対策（適切な認証・アクセス制御、端末管理、ログ管理等）を講じた上で、極力オンプレミス設備に依存しない、新たな教育情報ネットワーク環境の実現を目指している。

本業務は、以上を総合的に考慮したうえで、計画的な調達及び構築を進め、ICTを活用した校務を一層推進できる環境を整備することを目的として、新たな教育ICT環境の構築・移行、セキュリティポリシー運用準備業務及び運用保守業務を委託するものである。

1.3 業務内容

本業務は、現行システム基盤のサポート終了及び更改時期の到来を踏まえ、文部科学省が令和 7 年 3 月に取りまとめた「次世代校務 DX ガイドブック」及び同月改訂の「教育情報セキュリティポリシーに関するガイドライン」に基づき、次世代校務 DX の実現に向けた教育 ICT 環境の整備を進めるものである。具体的には、「校務系・学習系ネットワークの統合」及び「校務支援システムのクラウド化」を柱として、クラウド上での校務実施を前提としたロケーションフリーな業務環境の整備を図る。

また、校務 DX に不可欠であるクラウドシステムの利活用に当たっては、いわゆるゼロトラストの考え方を踏まえた「強固なアクセス制御」により、適切な認証・アクセス権限管理、端末管理、通信の暗号化、監視・ログ管理等のセキュリティ対策を講じ、ネットワーク環境の整備と併せて学校現場における安全管理措置を確保する。

将来的には、本業務により整備する基盤を活用し、データ連携基盤（ダッシュボード）の創出を見据えて、学校が保有する様々なデータを統合・可視化するとともに、校務系・学習系システムを円滑に接続させることにより、学校経営、学習指導及び教育政策の高度化に活用する。

委託業務内容については、環境構築業務、セキュリティポリシー運用準備業務及び運用保守業務に区分する。

【環境構築業務】

(1) 納入

システム（またはサービス）の調達

(2) 設計・構築

プロジェクト計画、システム設計（基本詳細）運用設計

(3) 設定

システム（またはサービス）および関連するネットワークの設定、各種テスト

(4) データ移行

【セキュリティポリシー運用準備業務】

構築した環境では、校務データ等の機密性が非常に高いデータを取り扱うこととなるため、国が定めるセキュリティポリシーに沿って利用する責任がある。本構築環境で利用を開始する前に、本市の教育情報セキュリティポリシー策定（改訂）支援を実施し、利用者の運用ルールや運用手順および研修を実施支援すること。

また、構築環境のセキュリティ遵守性を評価するために、稼働前に外部監査を受け、合格した環境で利用を開始すること。

※スケジュールの詳細は、『2.3 スケジュール』を確認すること。

【運用保守業務】

環境構築業務にて構築した教育 ICT 環境の運用・維持業務及びセキュリティ対応業務が対象となる。

2 本調達の要件

2.1 調達範囲

本業務で導入するライセンス・ネットワーク機器については、別紙1及び別紙2のとおり。

2.2 履行期間

(1) 教育ネットワーク環境構築業務

契約締結日から令和8年12月31日まで

(2) セキュリティポリシー運用準備業務

契約締結日から令和8年12月31日まで

(3) 運用保守業務

令和9年1月1日から令和9年3月31日まで

なお、上記期間中の業務が適正に履行されている場合においては、瀬戸内市及び受注者の合意により、契約開始日より最長5年間、継続して委託契約を締結できるものとする。

※（1）～（3）についてはそれぞれ契約を行うこととする。

2.3 スケジュール

本業務の実施スケジュール及び関連する業務スケジュール案を下記に示す。

令和 9 年 1 月から新教育ネットワーク環境で学習系システム及び校務系システムを既存の指導用端末で使用するため、令和 8 年 12 月 28 日までに新教育ネットワーク環境の構築を行い、既存の指導用端末を校務系端末として使用できる状態とすること。

なお、本スケジュールは一例であるため、上記要件を満たした上で最適な提案を行うこと。

作業内容	令和８年度						
	７月	８月	９月	10 月	11 月	12 月	R9.１月～3 月
契約	◆						
要件整理・設計	◆						
環境構築	◆	◆	◆	◆	◆	◆	
教育情報セキュリティポリシー策定支援	◆	◆	◆	◆	◆	◆	
検証・テスト				◆	◆	◆	
外部監査						◆	
研修						◆	
データ移行(※)						◆	
完了						◆	
本稼働							運用保守

※データ移行作業は本業務対象外です。

2.4 成果物

本市で想定している納入成果物は以下に示す。

なお、部数については、紙媒体で1部、電子媒体で1部とし、履行期間終了日までに教育委員会に提出し、確認を受けること。

また、電子媒体での納品物についてPDF形式およびMicrosoft Office（Word、ExcelまたはPowerPoint）のOpenXML形式とすること。

NO.	納入成果物	概要
1	プロジェクト計画書	本調達システムの構築計画が記載された文書
2	進捗報告資料	教育委員会との進捗会議にて使用する進捗報告資料
3	進捗会議議事録	進捗会議の議事録
4	システム全体概要書	基本設計資料
5	システム機能仕様書	詳細設計資料、設定パラメータ資料
6	テスト仕様書	結合テスト、システムテスト仕様書兼結果報告書
7	移行手順書	データ移行手順書
8	各種マニュアル	管理者マニュアル 利用者マニュアル システム運用簡易マニュアル

9	運用・保守マニュアル	業務フロー、保守対象内容
10	運用・保守作業報告書 サービス約款	定例会で報告される運用保守作業報告書、サービス約款
11	セキュリティポリシー等の策定支援	教育情報セキュリティポリシー（改訂版）…基本方針/対策基準 教育情報セキュリティポリシー実施手順（改訂版） 教育情報セキュリティポリシー運用要領（新規作成）
12	外部監査報告書	「地方公共団体における情報セキュリティ監査に関するガイドライン（令和7年3月改定）」に定める外部監査を受けた報告書　※別途契約予定
13	サービス仕様書	導入する各種サービスのサービス仕様書
14	各機能を利用するためのライセンスまたはクラウドサービス	システムのライセンス、クラウドサービス

2.5 ドキュメントの権利の帰属

(1) 本業務で作成したプログラム、およびドキュメントの著作権は、当市に帰属する。

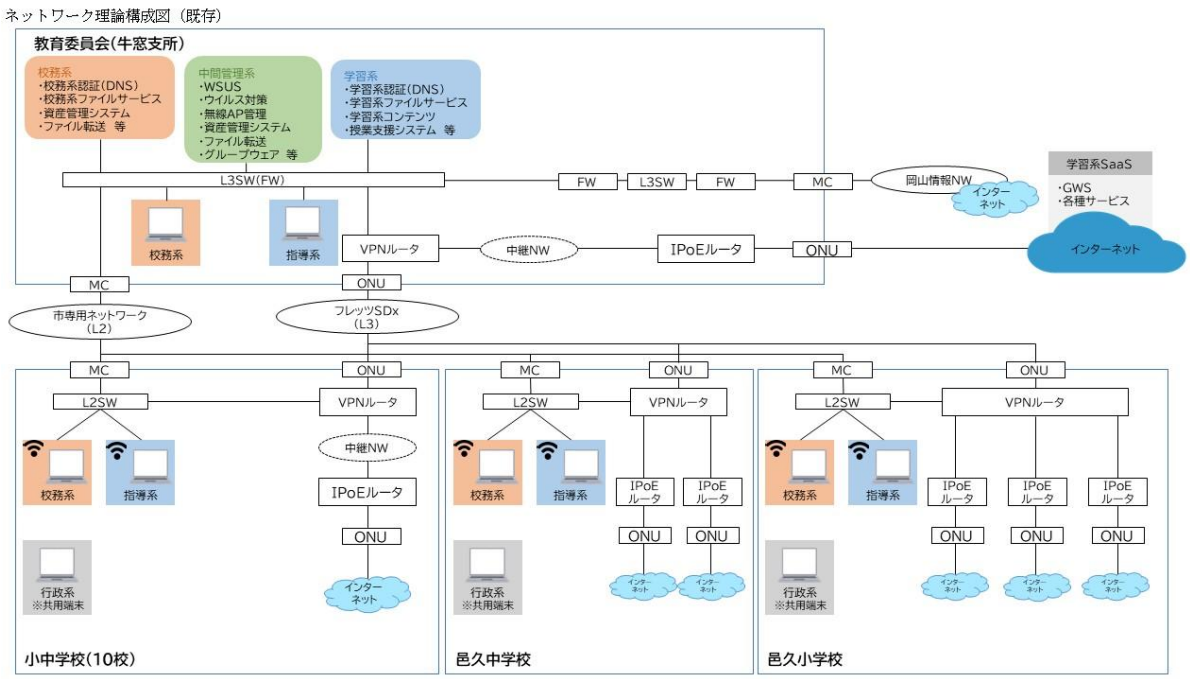
(2) 本業務より前に受注者、および第三者が保有していた著作権は、当市に帰属しない。

(3) その他、本業務で得られた成果物の取り扱い等に関する事項は、協議の上決定する。

3 全体基本設計

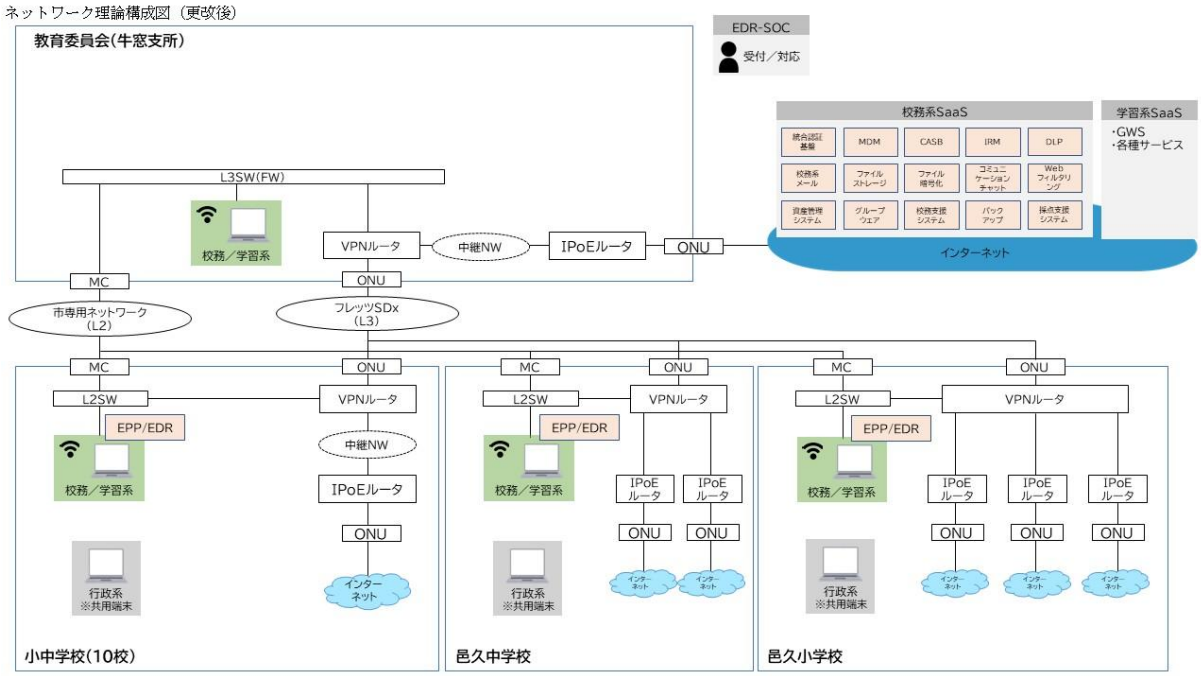
3.1 現行教育ネットワーク全体構成

現行のネットワーク構成を以下に示す。



3.2 新教育ネットワーク全体構成

新教育ネットワーク構成例を以下に示す。



3.3 ネットワークの基本仕様

本書で示す、新たな校務系 ICT 環境の各種要件に基づき方式設計・詳細設計を行うこと。ネットワーク方式、ネットワーク構成、パラメータ・設定等を設計し、方式設計書・詳細設計書等を作成すること。各学校におけるゼロトラストネットワークは、学習系ネットワークを利用しローカルブレイクアウト方式でインターネットに接続して実現する。ネットワークに関する設定等は教育委員会と協議のうえ、学習系環境及び校務系環境（校内の教職員がシステムに同時アクセスできる等）に影響のないように設計・構築・運用すること。

3.4 システム基本仕様

ICT 活用を前提とした教育活動の実現や、教育 DX の推進に向け、ガイドラインや提言に基づき、校務系と学習系のネットワークの統合を図り、アクセス場所（校内外）を問わず、安全に校務基盤等の利用ができるよう、統合型認証基盤を利用したゼロトラスト環境を構築する。具体的には、校外で教材を作成したり、教職員が端末を持ち帰って自宅から校務系システムにアクセスしたりするような使い方が想定される。この場合、アクセス制御の徹底による端末 1 台での運用や、教育委員会のセキュリティポリシーに基づく端末の持ち出しを可能とするため、ふるまい検知、マルウェア対策、暗号化、シングルサインオンなどの「アクセス制御による対策」を講じた ICT 環境を構築する。

3.5 サイジングのための要件

新たな教育 ICT 環境のサイジングに必要な要件を以下に示す。

＜教職員数＞

(1) 教職員数

小学校/中学校/教育委員会　360 名

＜実施場所＞

(1)　小学校

No	学校名	住所
1	牛窓東小学校	瀬戸内市牛窓町牛窓 4433 番地 10
2	牛窓西小学校	瀬戸内市牛窓町鹿忍 2166 番地
3	牛窓北小学校	瀬戸内市牛窓町長浜 3677 番地
4	邑久小学校	瀬戸内市邑久町山田庄 610 番地
5	今城小学校	瀬戸内市邑久町大富 25 番地
6	裳掛小学校	瀬戸内市邑久町虫明 2 番地
7	美和小学校	瀬戸内市長船町東須恵 1666 番地
8	国府小学校	瀬戸内市長船町福里 853 番地
9	行幸小学校	瀬戸内市長船町服部 163 番地

(2)　中学校

No	学校名	住所
1	牛窓中学校	瀬戸内市牛窓町牛窓 6446 番地
2	邑久中学校	瀬戸内市邑久町山手 2 番地
3	長船中学校	瀬戸内市長船町牛文 1010 番地

(3)　その他

No	施設名	住所
1	瀬戸内市教育委員会	瀬戸内市牛窓町牛窓 4911 番地

4 個別基本仕様

新教育ネットワークの整備にあたっては、「教職員の業務効率化」と「セキュリティ対策」の両立を目的として、アクセス制御モデルでの校務系システムとして統合認証基盤の機能を活用して構築することとする。

新教育ネットワークの利用に必要となる、カスタムドメイン及びグローバル DNS サービスは本業務で取得すること。なお、本 DNS サービス取得に必要な設定情報・費用・ライセンス等の契約時に必要な作業については、本業務に含めること。

提案するクラウドサービスは、情報セキュリティ管理・運用の基準となる、ISO/IEC 27001（または ISO/IEC 27017）（※） によるクラウドサービス分野における ISMS 認証取得、ISMAP（政府情報システムのためのセキュリティ評価制度）クラウドサービスリストへの登録、日本セキュリティ監査協会のクラウド情報セキュリティ監査による認定、SOC2 報告書（Service Organization Control Report）の取得のいずれかにより、サービスの信頼

性が確認できること。また、該当する証明書を提出すること。

ただし、クラウド無線管理システムについては、取り扱う情報の内容から上記の信頼性確認・該当する証明書の提出は不要とする。

※オンプレ版の認証は認められない。

4.1 セキュリティ（ゼロトラスト）

4.1.1 IDaaS（Identity as a Service）

「統合認証基盤」の機能により以下のことを実現すること。

(1) アカウント管理

・校務系端末の教職員のアカウント情報及び、各種システムへの権限設定に必要なセキュリティグループを作成する。また、教職員アカウントについては管理職ユーザーと一般教職員ユーザーを区別して管理し、管理職ユーザーのみアクセスすることができるようなデータ領域や暗号化の権限設定等が可能とすること。

・人事異動等の発生時に、発注者によるアカウントの随時追加、削除、編集等が可能であること。

(2) 認証管理

校務系端末、教職員のユーザー認証について、統合認証基盤の機能を活用した多要素認証の実現を提案すること。

(3) SSO（シングルサインオン）機能

校務系端末のシングルサインオンの認証連携については本業務で調達する校務支援システムと採点支援システムを対象としてＳＡＭＬ認証連携を実施すること。

対象ユーザーは教職員/教育委員会のすべてのユーザーが対象である。また、対象デバイスは既に調達を実施し、運用している教職員のデバイスとする。なお、必要な設定情報・費用については、本業務に含めること。

(4) アクセス制御機能

教職員の利用する校務のクラウド環境へのアクセス(接続)について、デバイス管理システムと連携し、対象デバイス以外（個人所有端末を含む）から接続できないよう制御を実施すること。

(5) リスクベース認証

本機能については事業者の任意の提案とする。提案する場合、アカウント ID に関するリスクの検出・管理・脅威からの保護を実施することとし、リスクが高い場合追加の認証が要求されること。

4.1.2 EMM（Enterprise Mobility Management）

「デバイス管理システム」の機能により以下のことを実現すること。

(1) Windows 端末のデバイス管理

教職員の利用する校務のクラウド環境のアクセス(接続)、校務系端末のアクセス（接続）で端末管理ができるようデバイス登録を実施すること。デバイスの登録については、個人所有端末及び Windows 以外のデバイスからの登録ができないようにするなど、セキュリティ対策を実施すること。

(2) 校務系端末の OS の管理（パッチ配信管理）

校務系端末について OS の管理（パッチ配信管理）方法について提案を行うこと。

(3) アプリケーション（ソフト）の配信

校務系端末で利用するアプリケーション（ソフト）の配信方法について提案を行うこと。

(4) セキュリティポリシーの適用

校務系端末でのセキュリティとして、「ファイアウォール、ドライブ暗号化機能」の設定を実施すること。

(5) リモートデバイスの操作

遠隔操作により、デバイスを出荷時の設定にリセットし、既定の設定に復元、削除できること。

4.1.3 EPP/EDR (Endpoint Protection Platform/Endpoint Detection and Response)

「エンドポイントセキュリティソリューション」の機能により以下のことを実現すること。

(1) 脅威検知

・既知のマルウェア情報が登録されたシグネチャベースでの検知を行うこと。校務系端末に配布するシグネチャはインターネット上のサイトより取得し、配信は１日１回行うなど管理を行えること。

・リアルタイム（ファイル操作や実行時）スキャンや一括スキャンを実施すること。

・脅威の検出は、機械学習などの先進的な技術を用いて、ファイルや端末の悪意ある挙動（振る舞い）に基づき検出を行うこと。

(2) 脅威対応

・脅威検知後の対応（通知、実行のブロック、通信遮断、ファイル除去、調査・分析、復旧等）について定義を行えること。

・脅威を検出した際に、被害拡大を防止するため、当該端末の通信を論理的に遮断し、隔離できることし、隔離された端末の問題が解消した後、元の通信状態に戻すことができること。

・脅威の検出結果や端末の状態を可視化するダッシュボード機能を有すること。

4.1.4 CASB (Cloud Access Security Broker)

「クラウド監視」について事業者は以下のことを実現するよう提案すること。

(1) シャドーIT の可視化

・クラウドサービスの利用状況を把握し承認していないシャドーIT の検出を行えること。

(2) 脅威検知

・「CASB」の機能を活用した脅威検知の実現について提案を行うこと。

4.1.5 IRM (Information Rights Management)

「機密データの管理・保護」の機能により以下のことを実現するよう提案すること。

(1) ファイル暗号化について

・「機密データの管理・保護」の機能を活用し、校務環境におけるファイルの暗号化について提案を行うこと。

・ファイルの暗号化については自動での付与機能も含めて、どのような活用が可能か提案を行うこと。なお、ファイル暗号化対象の拡張子で運用が異なる場合、利用方法等について提案すること。

4.1.6 DLP (Data Loss Prevention)

「データ損失」の機能について事業者は以下のことを実現するよう提案すること。

(1) データ損失防止について

・暗号化されたファイルについて、クラウドストレージのデータ損失防止対策の提案を行うこと。

(2) メール送信対策について

・暗号化されたファイルをメールで送付する場合の対策について提案を行うこと。

4.1.7 Webアクセス制御（フィルタリング）

マルウェアへの感染につながりうるセキュリティリスクの高い Web ページへの接続やコンテンツフィルタリングを利用したアクセス不要な Web ページへのアクセス防止を実施すること。

(1) URL フィルタリング

・ギャンブルや犯罪に関する Web サイトなど、職務上閲覧することが不適切なインターネット上の Web サイトをカテゴリから選択してアクセスを禁止すること。

(2) Web アクセスセキュリティ

・既知の悪意のある外部サーバーへの Web アクセスをブロックすること。

(3) 外部攻撃対策

・安全性が確認されている Web サイトへのみアクセスを許可し未登録サイトへのアクセスをブロックすることが可能なデータベースを搭載していること。

・脅威情報への通信が発生した際に、管理者にメール通知が可能なこと。
・脅威情報サイトへアクセスしたクライアント端末をインターネットから隔離し、管理者へメール通知が可能なこと。

(4)SSL 復号機能
・SSL（HTTPS）通信を解析・制御可能であること。
・別途ソフトウェアをインストールせずとも、同一の管理画面上でユーザーのインターネット利用状況の詳細可視化・分析が可能なこと。

(5) ログの保存期間
・WEB フィルタリングを経由した Web アクセス履歴を 1 年間記録できること。

4.2 ネットワーク

4.2.1 校外ネットワーク（ローカルブレイクアウト/センター集約）

現行学習系ネットワークはローカルブレイクアウトを実施して、教育委員会・各学校からインターネットに接続している。ネットワークの設定変更を行い、新「教育系ネットワーク」として利用できるようにすること。ネットワークに関する設定等は教育委員会と協議のうえ、学習系環境に影響のないように設計・構築・運用すること。

4.2.2 学校内ネットワーク（職員室/教室）

・既存の「校務系ネットワーク」、「中間管理系ネットワーク」や「学習系ネットワーク」に関するネットワーク・機器等を新「教育系ネットワーク」として利用できるように設定変更も併せて行うこと。
・収納ボックス等に設置している L2 スイッチを設定変更して、中間管理系ネットワークから新「教育系ネットワーク」として利用可能とすること。
・職員室や準備室等に整備している既存の有線 LAN ケーブルを使用して、校務系ネットワークで利用している学校プリンター等を設定変更して新「教育系ネットワーク」として利用可能とすること。
・現行学習系ネットワークの DNS は教育委員会のサーバー内から提供されている。本業務の環境切替に伴い、DNS サーバーの移行を実施し、既存学校拠点にあるローカルブレイクアウト用ルーターでの DNS の利用へ切替えること。

なお、ローカルブレイクアウト用ルーター及び DNS 設定作業に関して、教育系ネットワークの運用保守業者と協議し、作業費用を含むこと。
上記の教育系ネットワークの保守業者は以下である。
NTT 西日本株式会社　岡山支店
(連絡先) ビジネス営業部エンタープライズビジネス営業部門
〒700-0821 岡山市北区中山下二丁目 1 番 90 号
電話：086-801-5722

4.2.3 無線管理システム

職員室・普通教室等における現存無線アクセスポイント（フルノシステムズ社）を設定変更して、校務系を新「教育系ネットワーク」として利用可能とすること。

また、無線アクセスポイントの管理は、既存オンプレミス無線管理システム（フルノシステムズ社）から本業務で調達するクラウド無線管理システムへ変更すること。

その際、無線 LAN アクセスポイントのネットワーク管理、死活管理の可視化、バージョンアップ等の管理をできるように設定変更を行うこと。

4.3 クラウド・システム

4.3.1 グループウェア

教育委員会では令和２年９月１日から現在に至るまで、グループウェア（ミライム）を利用している。今後はクラウド版のミライムを導入する。システム構築を行い、クラウド版のミライムが利用できるようにすること。なお、現在使用しているミライムのデータ移行作業は今回の業務対象外とする。クラウド版のミライムの構築に当たって必要な設定情報・費用については、本業務に含めることとし、教育委員会と十分に協議し、作業を行うこと。

4.3.2 校務支援システム

教育委員会では令和２年９月１日から現在に至るまで、校務支援システム（スズキ教育）を利用している。今後はクラウド版のスズキ教育ソフト社製「スズキ校務 evanix」の校務支援システムを導入する。システム構築を行い、次項に定める機能・帳票を利用できるようにすること。なお、現在使用している「スズキ校務シリーズ」のデータ移行作業は今回の業務対象外とする。「スズキ校務 evanix」の構築に当たって必要な設定情報・費用については、本業務に含めることとし、教育委員会と十分に協議し、作業を行うこと。

(1) システム化対象機能

・校務支援システムは、以下の機能を導入すること。

項番	機能名	項番	機能名
1	名簿情報管理	7	調査書作成
2	出欠席情報管理	8	体力テスト処理
3	小学校成績処理	9	保健管理
4	中学校成績処理	10	週案簿・時数管理
5	通知表作成	11	学校経営支援機能
6	指導要録作成	12	データ連携用API機能

(2) 必要帳票一覧

・校務支援システムは、以下の帳票を導入すること。

・帳票導入に向けた要件定義は教育委員会と協議の上、決定することとし、短時間でも効率的に進められるよう支援を行うこと。

項番	機能名	備考
1	各種名簿	学校ごとに様式編集機能を有すること、もしくは有する予定
2	出席簿	教育委員会指定の出欠記号に合わせること
3	通知表	学校ごとに様式編集機能を有すること
4	小学校児童指導要録	通常学級 1 様式・特別支援学級用 2 様式
5	中学校生徒指導要録	通常学級 1 様式・特別支援学級用 2 様式
6	健康診断票	
7	検診結果通知文書	学校ごとに様式編集機能を有すること、もしくは有する予定
8	調査書	岡山県調査書の様式、運用に対応していること
9	保健日誌	
10	学校日誌	

(3) システム構築要件

・システムの構築を行うこと。

・各クライアント端末にシステムへの接続に必要な設定を行うこと

・教育委員会で管理する統合認証基盤を使ってシステムにシングルサインオンできるように設定を行うこと。

・提供するリストをもとに教職員のアカウント情報を統合認証基盤に登録すること。

4.3.3 採点システム

受注者は、各学校で実施するテストにおいて、生徒が手書きで解答用紙に記入したもの（解答用紙は教職員が独自に作成したものなどを含む。「解答用紙」は生徒が解答を記入する前の用紙のことを指すものとし、解答を記載したものは「答案」という。以下、同様とする。）を、教職員がスキャナーで画像データ又はＰＤＦデータ化し、採点システムにそのデータを登録することで、パソコン画面で、答案の採点及び得点集計ができるシステムを提案すること。

また、導入する学校は、『3.5＜実施場所＞』に記載のある中学校３校のみ導入をする。

・ブラウザを用いた Web 方式であり、ソフトウェアのインストールが不要であること。

・学校ごとに URL 発行を行い、第三者がアクセスできないよう IP 制限を行うこと。

・IP 制限を掛けた拠点以外からは、個人情報・成績情報が第三者の目に触れないよう、それらが一切表示されず、採点のみに機能制限を行った別 URL を発行すること。

・コールセンターを開設し、平日午前９時から午後６時まで（ただし、土曜日及び日曜日・祝日・年末年始・お盆期間を除く）対応すること。

・保存されるデータは全て暗号化して保存を行うこと。

4.3.4 校務系メール（メール）

「メールセキュリティ対策」の機能により以下のことを実現すること。

(1) 校務系メール

・校務系メールとは、教職員が業務上必要であると教育委員会により認められた場合に利用できる校務系のメール機能とする。

・カスタムドメイン利用、DNS のセキュリティ機能（SPF、DKIM、DMARC 等)関連、MX レコード等の必要な設定作業を実施すること。

・本メールの利用は校務系端末からメールソフトアプリによる利用とし、校務系端末へのログイン情報と連携し、自動認証機能によりアカウント・パスワードを入力せずとも自身のメールボックスを利用できるものとする。

・アドレス帳については全小中学校の教職員の情報を検索・利用できることとする。

(2) メールセキュリティ

・受信したメールの添付ファイルや URL を解析、隔離できること。

・メール利用ユーザーに対して、スパム対策、マルウェア対策、フィッシング対策の保護をすること。

・マルウェアの疑いがあるメールを検疫し、スパム対策ポリシーを使用してフィッシング疑いが高いメールを処理できること。

・添付ファイルをサンドボックスによるスキャンを実施する設定を可能とすること。

4.3.5 ファイルのストレージ

ファイルストレージとは、教職員の個人作成データの保存領域、校内で共有するデータの保存領域の機能とする。「クラウドストレージ」の機能により以下のことを実現すること。

(1) 個人用保存領域

・個人用のクラウドストレージ保存を可能にすることとし、校務系端末からであればどのネットワークからでもアクセス可能とすること。

・個人用の保存領域を指定可能なこと。

(2) 学校保存領域

・クラウドストレージを利用することとし、学校ごとにファイルストレージサイトを構築すること。

・学校ごとで作成されたサイトごとにアクセス権限設定を実施すること。

・サイト内でのドキュメントフォルダに対して、校内の指定されたアカウントのみアクセス可能となるよう設定をすること。

・本サイトへのアクセス権限については、『4.1.1.IDaaS（認証）』と連携し、教職員の人事異動に伴い自動的にアクセス権の付与・削除が行えるように実施すること。

(3) 共有保存領域

・クラウドストレージを利用することとし、教育委員会と各学校全体で利用可能なファイルストレージを 1 サイト構築すること。

・作成されたサイトごとにアクセス権限設定を実施すること。

・サイト内でのドキュメントフォルダに対して、指定されたアカウントのみアクセス可能となるよう設定をすること。
・本サイトへのアクセス権限については、『4.1.1.IDaaS（認証）』と連携し、教職員の人事異動に伴い自動的にアクセス権の付与・削除が行えるように実施すること。

4.3.6 コミュニケーションチャット

「コミュニケーションチャット」の機能により以下のことを実現すること。

(1) チャットグループ

・学校で利用するチャットグループの利用環境（権限・機能）について設計・設定を実施すること。
・チャットグループの作成は教職員ではできないこととする。

(2) チャット機能

・チャット機能が利用できる範囲など設計・設定を実施すること。
・チーム所有者がメッセージの削除を可能とすること。

(3) Web 会議

・Web 会議については、外部機関との会議も含めて利用できるよう設計・設定を実施すること。

(4) チームの作成

・学校ごとにチームを作成することとする。

4.3.7 クラウドバックアップ

校務のクラウド環境のアクセス(接続)、校務系端末のアクセス（接続）に保存しているデータをクラウドネイティブな SaaS 環境にバックアップできるよう提案すること。

別調達で導入した校務系端末を活用し、新教育 ICT ネットワークが利用できるよう以下の設定を実施すること。

(1)バックアップの対象範囲

・校務系メール、ファイルのストレージ、コミュニケーションチャット

(2)データ保持

・世代管理を行うこと。
・バックアップ容量、バックアップ手法について提案すること。

(3)復元

・メール、フォルダ、ファイル、ユーザー、グループ単位など個別に復元できること。
・バックアップ時にデータスキャンすることで、マルウェアに感染したファイルが正常なデータと一緒に復元されることを防止できること。

・復元方法について提案すること。

(4)その他
・メーカーにて日本語によるサポートが提供されること。
・バックアップ失敗時にメールによる通知機能を有すること。

4.3.8 資産管理システム

ハードウェアやソフトウェアなどの IT に関連する資産、PC 操作ログ、デバイス制御、アプリケーション配布、リモート操作などの以下の機能を提供する。

(1) IT 資産
・各クライアントコンピューターに関する各種ハードウェア情報を、資産情報として自動的に収集できること。

(2) ログ取得
・クライアントコンピューターに対して行われた操作、ログオン・ログオフの日時、ファイル操作、Web へのアクセスおよび書き込み・アップロード・ダウンロード、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報等をログとして記録する機能を有すること。
・収集したログをクラウド上で 1 年以上保管できること。

(3) デバイス管理
・USB デバイスをクライアントコンピューターもしくは管理者のクライアントコンピューターに挿入した際、利用した USB デバイスのシリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること。

(4) リモート操作
・特定のクライアントコンピューターに対して、インターネット経由で、リモート操作が行える機能を有すること。

(5) 外部記憶媒体制御
・校務系端末での外部記憶媒体（USB デバイス等）を接続した利用を禁止する設定を実施すること。
・教育委員会が許可した USB デバイスについては利用できるよう設定を実施すること。

5 セキュリティポリシー策定支援要件

本構築においては、セキュリティ遵守が特に重要であることから、セキュリティ要件として個別で記載をする。

(1) 本サービスを提供する施設等は、国内に所在地を置き、必要なセキュリティ及び災害対策等の措置がとられていること。

(2) 情報漏えい及び不法侵入等の対策が施されており、常に最新の状態を保持すること。
(3) 児童・生徒・教職員などの情報をクラウド環境にアップロードするため、文部科学省「教育情報セキュリティポリシー関するガイドライン（令和 7 年 3 月）」および「瀬戸内市情報セキュリティポリシー」の内容を踏まえた「瀬戸内市教育情報セキュリティポリシー」（基本方針/対策基準）、実施手順および実施手順に基づいた運用要領を教育委員会と協議の上策定支援し、9.研修において説明を行うこと。瀬戸内市教育情報セキュリティポリシー」（基本方針/対策基準）、実施手順および実施手順に基づいた運用要領については、契約後別途示す、瀬戸内市情報セキュリティポリシー（基本方針/対策基準）、実施手順及び実施手順に基づいた運用要領と内容の整合性、記述レベルを合わせること。
(4) (3) の策定後、本稼働までに「地方公共団体における情報セキュリティ監査に関するガイドライン（令和 7 年 3 月改定）」に定める外部監査を受け、策定した教育情報セキュリティポリシー（基本方針/対策基準）、実施手順および実施手順に基づいた運用要領が適切であるとの評価を得られるようにすること。
(5) 環境構築及び運用保守において、セキュリティに関する役割の範囲と責任分界点を提示し、教育委員会と協議・合意すること。

6 移行要件

端末移行等は令和 8 年 12 月 1 日から令和 8 年 12 月 25 日までとし、学校行事やイベントに合わせて行うこと。移行する学校の順番及び既存、新規システムの停止期間については、教育委員会と協議の上決定すること。

6.1 端末移行

(1) 端末のデータ移行

・端末内のデータの移行は各自教職員が実施することとし、必要に応じて移行手順書を作成すること。

(2) 端末の回収

・各学校の学習系ネットワークで使用している指導用端末を校務系端末として利活用するため、各学校に整備済の端末を回収して再設定を行うこと。また、端末の回収は令和 8 年 12 月 1 日以降とすること。

既存端末情報：NEC VersaPro タイプ VS PC-V1U46S4GM　340 台

(3) 端末のマスターイメージの作成

・マスターイメージを作成すること。
・本件の 2 台の端末をマスター専用端末として使用し、必要なドライバのインストール及びソフトウェアのインストール等を実施すること。
・OS 及びソフトウェアを最新の状態にアップデートすること。
・本業務で構成上必要な場合、以下のアプリケーションをインストールすること
　ｉ.デスクトップ版 Office（新規購入）

ⅱ.一太郎 Pro 6（既存 30 本流用）

・再設定する端末にインストールするソフトについては、教育委員会が指定するソフトを教育委員会と協議の上受注者にて設定し、各学校の新「教育系ネットワーク」で動作するよう納品を行うこと。

・詳細な設定要件は教育委員会と協議の上決定すること。

・各学校の新「教育系ネットワーク」での動作確認等については、教育委員会及び教育系ネットワーク保守業者と協議を十分に行い、納品を行うこととし、費用が発生する場合は、本業務の費用に含めること。

(4) クローニング作業

・クローニングは、必要なアプリケーションの導入、Wi-Fi など、端末利用に必要となる情報を教育委員会及び既存端末保守事業者と協議の上実施すること。

・デバイス管理システムへの登録とともに、統合認証基盤にも各デバイスを自動登録させること。

・プリンターのドライバインストール及びネットワーク設定を行うスクリプトファイルを作成し納品すること。

・各拠点に応じた環境設定（プリンタ設定、その他運用上必要な設定）を行い、構築後に教職員がすぐに利用できること。

(5) 校務系端末の搬入・設置作業

・令和 8 年 12 月 25 日までに各学校に端末を搬入・設置を行い教職員が使用できるようにすること。

・各学校のネットワーク設定に合わせて必要な端末設定作業を各学校で実施すること。

・既存の校務系端末、再設定前の指導用端末からのデータの移行は実施しないこととする。

(6) イメージファイル及び設定手順書の提出

・設定後のマスターイメージを入れたブート用 USB メモリ 1 式を納品すること。その際の USB メモリは受注者で用意すること。

教職員の端末登録作業について端末利用手順書を作成し提出すること。

6.2 データ移行

次のデータ移行作業は今回の業務対象外とする。

・グループウェア及び校務支援システムのデータ移行

・校務ファイルサーバーデータ移行

・NAS データ移行

7 検証テスト

7.1 システムテスト

新たに導入する全ての機能等のテストを行うこと。そのうえで、校務系端末、校内ネットワ

ーク機器や回線を含めた新たな校務系 ICT 環境の全体的な総合テスト（結合試験）を、各関連事業者と連携のうえ実施すること。

7.2 テスト計画書の作成

各テストの実施にあたっては、計画策定、テスト仕様策定、テスト実施、テスト結果の報告作成を行うこと。また、テストにあたっては、必要に応じて学校に訪問し、学校からの新たな校務系 ICT 環境への接続及び利用確認のための実地検証を実施すること。

実施するテストについて、テスト方針、実施内容及び実施理由、評価方法、実施者テスト工程開始までにテスト計画書として提出し、承認を得ること。

8 研修

受講者分類	研修対象者	研修内容
運用管理者	教育委員会担当者	・クラウドサービスの運用管理業務について ・異常時の対応方法、対応フロー
学校運用管理者	学校管理職	・データアクセス権限設定方法 ・各種承認フローの利用方法
一般職員	学校の教職員	・新しく構築した全体像 ・校務系データと学習系データの取り扱いやフォルダ間のデータ移動等のシステム利用方法
クラウドシステム利用者	クラウドシステム利用者	・セキュリティポリシーおよび実施手順に沿った研修

上記研修会は例示であることに留意し、必要と思われる研修会について、効率的かつ効果的に実施できるよう。内容や実施時期等を具体的に提案すること。

ただし、最終的な研修会の内容や実施時期等については、教育委員会と協議の上、決定すること。

9 運用保守仕様

9.1 運用・保守総括業務

受注者は本調達において、新教育システム構築後のシステムを安定的に稼動させ、その機能が 5 年間十分に発揮できるよう、常に良好な状態を維持するとともに、障害に対する予防保全および障害発生時の早期復旧が行えるよう全体の統括を行うこととし、その運用・保守状況を定例会（1 回/月）にて報告を実施すること。

9.2 障害対応業務

ゼロトラスト環境における障害対応業務において以下のことを実現すること。

(1) ゼロトラスト環境故障受付

・24 時間 365 日：メール・電話による受付を実施すること。

※専用サイト等での受付も可能とするが、別途教育委員会との協議の上決定することとする。

(2) 障害切り分けと対応

・平日 9:00～17:00：受付された障害について切り分けを実施するとともに必要に応じてオンサイト保守対応を実施すること。

・オンサイトでの保守対応が必要な場合は教育委員会・運用保守業者にエスカレーションすること。

(3) ヘルプデスク

・平日 9:00～17:00：教育委員会及び、各学校の代表者からの問い合わせに対する受付・回答を実施すること。

※専用サイト等での受付も可能とするが、別途教育委員会との協議の上決定することとする。

9.3 ＳＯＣ業務

ゼロトラスト環境における「セキュリティオペレーション業務」において以下のことを実現すること。

(1) EDR 監視分析

EDR を常時監視し、危険度の高いアラート発生時には、端末の通信を遮断し、ネットワークから隔離対応を実施すること。また、隔離後、端末の分析を行い、その後の対応について報告・実施すること。

・監視・アラート通知（24 時間 365 日対応）

管理ポータルから監視を実施し、アラート検知時に教育委員会へ通知を実施

・ネットワーク遮断（24 時間 365 日対応）

危険度の高いアラートを検知した場合、該当 PC 端末を論理的に NW から遮断を実施

・アラート分析・報告・対処（平日 9-17 時対応）

危険度の高いアラートについて分析を実施、対処完了後該当 PC 端末の遮断の解除を実施

(2) DLP ログ調査（平日 9-17 時対応）

EDR で検知したインシデントに関して、教育委員会の要請により DLP（機密データの管理・保護）でのログ追跡調査を実施すること。

(3) 端末操作ログ調査（平日 9-17 時対応）

EDR で検知したインシデントに関して、教育委員会の要請により資産管理システムでの端末操作ログの追跡調査を実施すること。

9.4 運用代行業務

新教育システム環境における運用代行業務において以下のことを提案すること。

・校務のクラウド環境のアクセス(接続)、校務系端末のアクセス（接続） における運用代行業務の提案

・Web アクセス制御（フィルタリング）における運用代行業務の提案

・資産管理システムにおける運用代行業務の提案

・クラウドバックアップソフトにおける運用代行業務の提案

10 プロジェクト体制

受注者は、本書に基づき、本システムの構築における具体的な体制、スケジュール、プロジェクト管理方針、プロジェクト管理方法等を含んだプロジェクト計画書を作成、提示すること。

また、プロジェクトの業務の一部を別法人等に再委託する場合は、事前に体制図を示し、当市担当者の承諾を得ること。

また、プロジェクトの体制だけでなく情報セキュリティ遵守体制を示し、本市教育情報セキュリティ責任者の承諾を得ること。

10.1 会議体

受注者は、定期報告の会議体として、月２回程度の定例報告会を開催することする。また、キックオフ会議、各工程の判定会議、移行・稼働判定会議など定例報告会以外の会議が必要な場合は、適宜必要な会議を開催すること。なお会議体の実施方法については、教育委員会担当者と協議のうえ決定すること。

各会議の開催にあたっては、進捗報告書、課題管理表、変更管理票、スケジュール、会議録、その他必要と思われる報告資料等を準備すること。

10.2 プロジェクト管理

本業務遂行にあたっては、下記の業務を実施すること。

項目	要件
進捗管理	プロジェクト計画策定時に定義したスケジュールに基づく進捗管理を実施すること。 受注者は、実施スケジュールと状況の差を把握し、進捗の自己評価を実施し、定例報告会において教育委員会に報告すること。 進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正の計画を策定すること。
品質管理	プロジェクト計画策定時に定義した品質管理方針に基づく品質管理を実施すること。 受注者は、品質基準と状況の差を把握し、品質の自己評価を実施し教育委員会に報告すること。 品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定すること。
課題・リスク管理	プロジェクト計画時に抽出したリスクを管理し、リスクが顕在化した場合は課題として管理すること。 課題発生時には、速やかに対応策を明らかにし、教育委員会と協議のうえ、対応方法を確定し、課題が解決するまで継続的に管理すること。

変更管理	仕様確定後に仕様変更の必要が生じた場合には、受注者は、その影響範囲及び対応に必要な工数等を識別したうえで、教育委員会と協議のうえ、対応方針を確定すること。

11 契約不適合責任

別途、本業務に関する契約書にて提示する。

12 機密保護・個人情報保護

(1) 本業務を遂行する上で知り得た情報、資料、秘密、個人情報等については、その機密を保持するものとし、第三者に漏らしてはならない。また契約終了後も同様とする。

(2) 本業務遂行のために当市が提供した資料、データは業務以外での目的で使用しない。

(3) 本業務の遂行に当たっては以下に掲げる法令等を遵守すること。

1. 国等で定められた法・ガイドライン

・個人情報の保護に関する法律（平成 15 年法律第 57 号）

・不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

・特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（平成26年特定個人情報保護委員会告示第６号）

2. 当市が定める条例・セキュリティポリシー

・瀬戸内市　情報セキュリティポリシー

・瀬戸内市　教育情報セキュリティポリシー

・瀬戸内市　個人情報保護法施行条例（令和 5 年条例第 6 号）

その他、ここに記載しない事項については、別途、本業務に関する契約書にて提示する。

(4) 本業務遂行に当たり、本市の定める「委託事業者向け情報セキュリティ対策チェックシート」及び経済産業省の「クラウドサービスレベルのチェックリスト」を提出し、本市教育情報セキュリティ責任者の承諾を得ること。

13 協議

(1) 導入にあたり疑義が生じた場合、または仕様書や本契約書関連書面に定められていない事項等が発生した場合は、本市と協議を行い、指示を受けること。

(2) 本業務の実施状況について、他団体に情報提供を行う場合は、事前に本市に対して連絡を行い、許可を得ること。