

(別紙)久留米市学校 ICT 環境 現行環境概要

1. 目的

本資料は、本市における現行の ICT 環境の構成および課題を整理し、次期環境検討に向けて広く情報提供を求めめるための基礎資料として提示するものである。

2. 久留米市立小・中・特別支援学校 ICT 環境全体概要

(1) 対象規模(令和 8 年 6 月時点)

学校数:約 60 校(小学校 42 校・中学校 17 校・特別支援学校 1 校)

児童生徒数:約 26,000 人

教職員数:約 2,400 人

(2) 利用端末

校務用端末:Windows 端末(教職員のみ)

学習用端末:Chromebook(特別支援学校は iPad)

(3) 現行校務系環境の概要

ア. 構成の特徴

- ◆ クラウド中心の構成(図書システム等一部インストール型ソフトウェアあり)
※校務系 Microsoft、学習系 Google
- ◆ ゼロトラスト型セキュリティを採用(ロケーションフリーの実現)
- ◆ 教職員端末の 1 台化(Windows 端末・WiFi 対応・生体認証)

本環境は、クラウドサービスと端末・認証基盤を組み合わせたゼロトラスト型構成として整備しており、認証・端末管理・セキュリティを統合的に運用している。

イ. 校内ネットワーク環境

- ◆ Wi-Fi(校務用端末・学習用端末・印刷機器を接続)
※有線 LAN は廃止
- ◆ インターネット・ローカルブレイクアウト
- ◆ アクセスポイント未設置教室等はホームルーター、モバイルルーターを活用

ウ. 認証・アクセス制御

- ◆ 多要素認証
Intune に登録した校務用端末+3 要素(生体認証・PIN・校内 AP)のうち 2 要素を必須とする。
- ◆ 校務用端末は校務系・学習系両環境にアクセス可
- ◆ 学習用端末は学習系環境のみアクセス可
- ◆ シングルサインオン(SSO)もしくは代理入力によるシームレスな認証・アクセスを実現

エ. システム構成

本市では、Microsoft A5 を基盤としたクラウドサービスを活用し、認証・端末管理・セキュリティ対策を統合的に実装したゼロトラスト環境を構築している。

また、利用者・端末・アクセス状況に応じた動的なアクセス制御を実現し、多層防御の考え方に基づくセキュリティ対策を講じている。

(ア) 機能

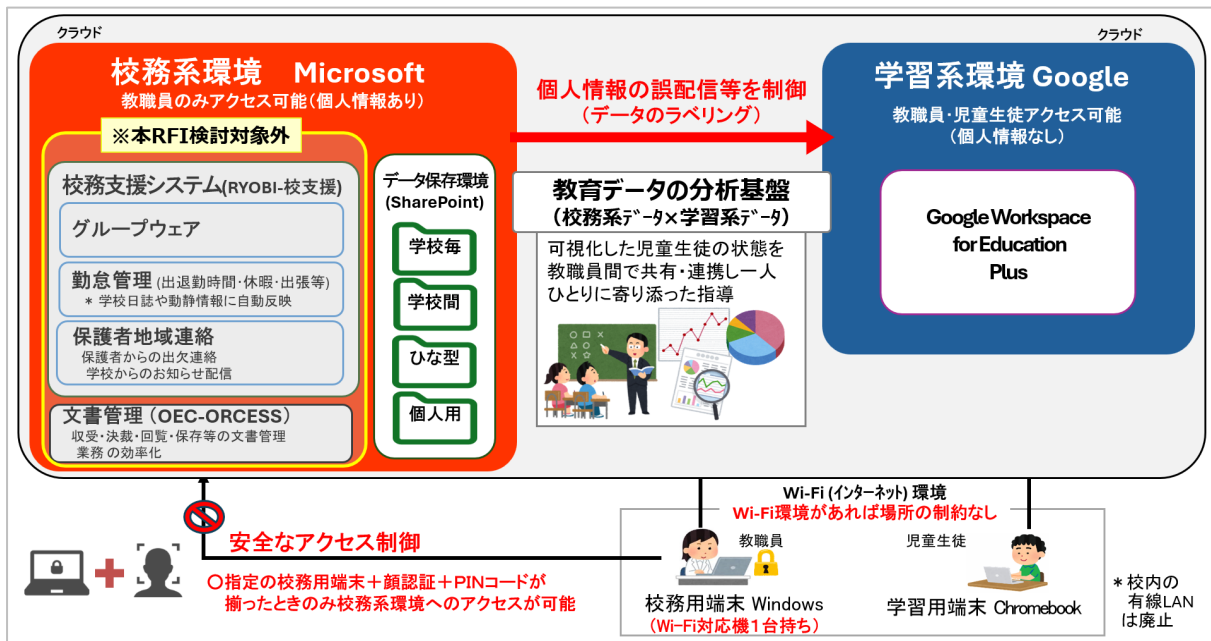
カテゴリ	機能
校務支援システム	校務支援システム・グループウェア・勤怠管理・保護者地域連絡
文書管理システム	文書管理・外部共有メール
多要素認証システム	多要素認証
教育データ分析基盤	ダッシュボード
ネットワーク環境 アクセス認証型 (ゼロトラスト)整備	統合 ID 認証/SSO:IDaaS
	リモートアクセス:SDP
ネットワーク環境 アクセス認証型(ゼロトラ スト)	デバイス制御:EMM
	端末セキュリティ:EDR
	クラウド監視・管理:CASB
	コンテンツ保護:IRM
資産管理システム	Windows Update 制御
	端末操作ログ管理
	リモートアクセス・外部記憶媒体書き出し制限・ソフトウェア配布
データ保存環境	クラウド共有フォルダ・個人フォルダ

(イ) 調達ライセンス・端末数

導入ライセンス	調達ライセンス数
Microsoft365 A5(データ保存環境含む)	2,200
Google Workspace Education Plus	25,300
資産管理システム	2,200
SOC サービス	2,200
SSO マネージャ	2,200
校務支援システム	62 校分
文書管理システム	2,200
Windows 端末(別調達)	2,391 台

※校務支援システム、文書管理システムは、本 RFI の検討対象外であり、参考情報として記載している。

(ウ) 学校 ICT 環境全体構成図 (RFI 対象範囲の整理)

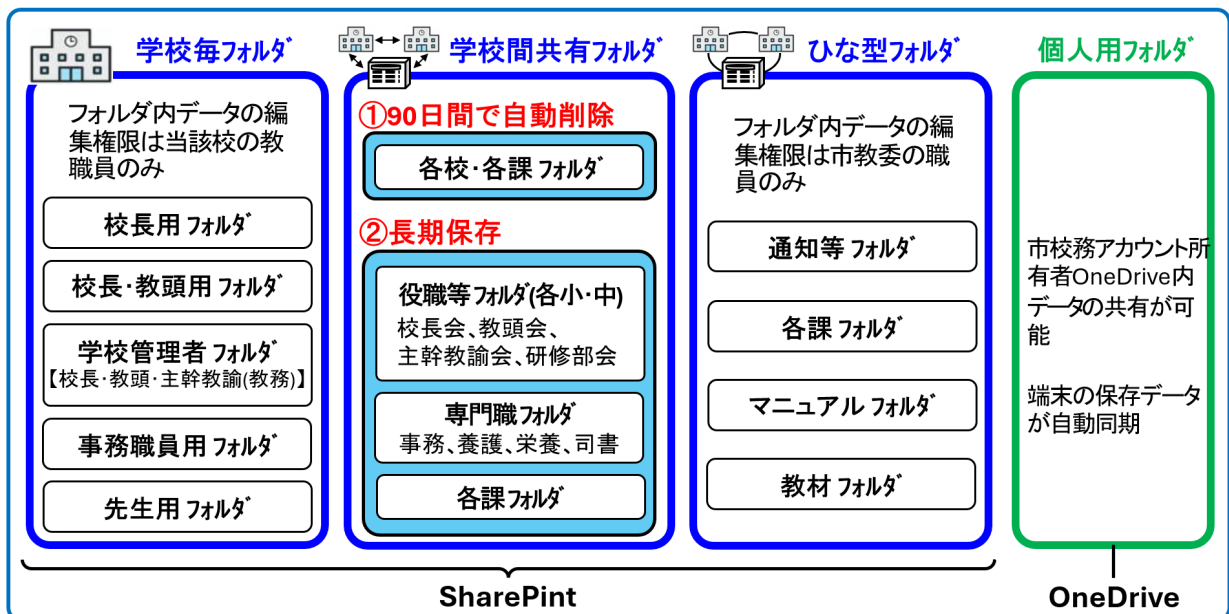


※業務アプリケーション(校務支援システム、文書管理システム)は、本 RFI の検討対象外

(エ) データ保存環境

データ保存環境は Microsoft SharePoint および OneDrive を利用しており、共有データは SharePoint の共有フォルダで管理し、用途ごとにアクセス権限および保存期間を設定している。

端末内個人データは OneDrive に保存し、自動的に同期される構成としている。



オ. 運用

本市の校務系 ICT 環境における運用は、ヘルプデスク、環境監視、オンサイト対応、ICT 支援および各システム運用により構成され、関係事業者が連携して実施している。主な運用内容は以下のとおりである。

(ア) ヘルプデスク運用

- ◆ 教職員からの問い合わせ対応、操作支援、障害受付
- ◆ 障害発生時の一次切り分けおよび関係事業者への対応依頼
- ◆ 問い合わせ内容および対応履歴の管理
- ◆ 月次報告の作成および報告会の実施

(イ) 環境監視・セキュリティ運用

- ◆ EDR 等を活用したセキュリティ監視（アラート監視）
- ◆ 不審な挙動検知時の自動調査・封じ込め対応
- ◆ 脅威の簡易分析および除去対応
- ◆ 監視結果および対応状況のレポートニング

(ウ) アカウント・端末・システム運用

- ◆ アカウントの作成、変更、削除、権限管理
- ◆ 端末管理（設定管理、アップデート制御、ソフトウェア配布）
- ◆ 各種システム設定変更、運用管理
- ◆ ログ管理および資産管理
- ◆ 高リスクアラート発生時の対応、端末隔離等のセキュリティ対応

カ. ゼロトラスト対応状況

文部科学省が示すゼロトラストの要素技術に対する本市の対応状況は以下のとおりである。

※文部科学省「教育情報セキュリティポリシーハンドブック(令和 7 年 3 月)」より

① アクセスの真正性に関する要素技術

要素技術	内容	対応状況
多要素認証	ID/パスワード＋生体・IC カード等	Microsoft Entra ID (Azure AD) 多要素認証(MFA)
リスクベース認証	IP・場所・時間などに応じた追加認証	条件付きアクセス(Conditional Access)／リスクベースポリシー
シングルサインオン	一度のログインで複数サービス利用	SSO (Entra ID)

② 端末・サーバ・通信の安全性に関する要素技術

要素技術	内容	対応状況
通信の暗号化	通信内容の盗聴防止	TLS/SSL (Microsoft 365 標準)
Web フィルタリング	危険サイトのアクセス制御	Microsoft Defender for Endpoint
MDM	端末の一元管理・遠隔制御	Microsoft Intune
アンチウイルス	マルウェア検知・駆除	Microsoft Defender Antivirus / Defender for Endpoint (EDR)
データ暗号化	情報内容を読めない状態にする、アクセス制限	BitLocker/Information Protection (秘密度ラベル)
不正アクセス検知・遮断	IDS/IPS/EDR など	Defender for Endpoint, Entra Application Proxy Connector

3. 現行環境の主な成果

- ◆ ロケーションフリーの実現
- ◆ 教職員の働き方改革の推進
- ◆ 各種 ICT 環境の統合による運用効率化及び経費削減
- ◆ データ連携基盤の整備
- ◆ 校務 DX の推進
- ◆ レジリエンス対応(自然災害・感染症・端末故障など)