

教育委員会における統合認証基盤設計構築委託

仕様書

1 目的・概要

本委託は、校務系・学習系ネットワークの統合により求められる強固なアクセス制御を実現するため、Microsoft Entra ID を中核とする統合認証基盤 (IDaaS) を設計・構築し、ID およびアクセス権限を一元的に管理可能な環境を整備することを目的とする。

また、これまで ID 管理に用いてこなかった人事データから IDaaS へ登録するために必要な、データ項目の整理・マッピング、データ整形ルールの策定、取込方式の確立および取込検証を実施し、ID ライフサイクル管理の整理・効率化を図る。

さらに、既存 ID 管理システム及び関連システムとの ID 連携に関する検証を行う。

加えて、保有する Microsoft A3 ライセンスで利用可能なセキュリティ機能の有効性及び検証を行い、令和 10 年度の本格運用に向け、利用者影響を最小化した円滑な移行を実現する。

2 委託期間

契約締結日から令和 9 年 3 月 31 日まで

3 履行条件

(1) 履行場所

川崎市総合教育センター（〒213-0001 川崎市高津区溝口 6-9-3）

(2) 委託時の注意

稼働中のシステムに影響を与えることが無いように行うこと。影響が出る場合、書面にて必ず事前に本市へ届け出て了承を得ること。

(3) プロジェクト計画

落札者は、契約締結後 2 週間以内に本業務の基本計画（プロジェクト計画書（実施体制図、スケジュール等））を作成し、本市の合意を得ること。また、基本計画の内容に変更があるときは書面による報告を行い、本市の承認を得ること。実施体制図には以下を記載すること。

a 総括責任者、業務従事者の氏名及び連絡先等

b 一元的窓口となる担当者 1 名

(4) 業務の報告等

打ち合わせ等を行った場合は、議事録を作成の上、速やかに本市担当職員に報告・提出をすること。

4 調達物

(1) 検証用 ID 管理システム

6 (1) の仕様を満たすシステムを調達すること。

※クラウドサービス利用料及びライセンス料を含めること。

期間：令和 9 年 1 月～3 月

(2) 「LDAPManager」用サーバ

ア. 6 (1) の仕様を満たすサーバを調達すること。

※既存の ID 管理システムはエクスジェン・ネットワークス株式会社の「LDAPManager」であり、既存システムへの影響を考え、検証用サーバを用意すること。

- イ. 借入物件の搬入、設定作業、LAN 配線に係る費用を含めること。
- ウ. 借入物件の搬入、据付及び撤去の際に、機器などの損壊が生じた場合、落札者の責任においてこれを補填すること。

(3) 拠点用ファイアウォール

- 6 (6)の仕様を満たすシステムを調達すること。

5 業務範囲

- (1) 検証用 ID 管理システムの調達・導入
- (2) 検証用 ID 管理システムからの連携システムへのアカウント等のプロビジョニング
- (3) 統合認証基盤 (Microsoft Entra ID) の構築
- (4) Microsoft365 を利用したセキュリティ等の構築
- (5) 既存検証端末の設定変更
- (6) 既存ネットワークの設定変更
- (7) 人事データの整形
- (8) 検証用 ID 管理システムへのデータ投入
- (9) 随時・月次・年次更新を含むアカウント管理フローのリハーサル含むテスト
- (10) 運用保守事業者への引継ぎを想定したドキュメント作成
- (11) リスク分析と残存リスクを未然に防ぐ仕組み・サービスを調達する為の仕様書案策定
- (12) 教職員の市内異動時の端末学校間移動についての検討
- (13) 行政系 Microsoft 365 と教育系 Microsoft 365 のテナント共有検証

6 業務内容

(1) 検証用 ID 管理システムの調達・導入

- ア. 検証用 ID 管理システムはクラウド SaaS 型の仕組みを採用すること。サービスは国内リージョンにて稼働していること。8,500 ユーザーライセンスが期間中利用できる環境を構築すること。期間は令和9年1月から令和9年3月までを想定すること。
- イ. 既存の「LDAPManager」と自動連携し、ID 管理ができる仕組みであること。
- ウ. 管理者にて承認された ID が自動的に作成される仕組みを構築すること。
- エ. 検証環境として新規で「LDAPManager」をオンプレで構築すること。主に ID 登録に関するワークフロー機能の実装を想定しているため、各学校からの ID 登録申請を受け付けることができること。ID ワークフローにて承認されたユーザーは、検証用 ID 管理システムに自動的に登録されること。設置場所は、3 (1) 内にあるサーバ室を予定しており、設置に係るすべての費用を含めること。
- オ. 「LDAPManager」用サーバは以下の要件を満たすものを調達すること。

● 「LDAPManager」用サーバ

- LDAP・LDAPManager・ID ワークフローサーバを構築し、ID ワークフローによる ID 申請・承認から検証用 ID 管理システムへの反映まで検証を実施すること。

装置名	数量	仕様（同等とすること）
LDAPManeger 用サーバ	1	(1) CPU : Xeon 6507P プロセッサ(3.50GHz、 8 コア、48MB)以上 (2) メモリ : 128GB 以上を有すること (3) OS : Windows Server 2025 (4) 内部記憶装置 : 480GB×4 本 (SSD、RAID5+Hotspare) (5) ネットワーク機能 : LAN(1000BASE-T/100BASE-TX)×2 (6) 外形寸法 : W435 [483 (突起部含む)] mm×D770 [844 (突起部含む)] mm×H43mm 程度 (7) その他 ア キーボード・マウスを添付すること イ サーバ管理ソフトウェアが添付されていること ウ KVM ケーブル 1.8m×1 エ ラックマウントタイプであること

(2) 検証用 ID 管理システムからの連携システムへのアカウント等のプロビジョニング

連携対象システムは、Microsoft365、GoogleWorkSpace、ActiveDirectory (AD)、L-Gate (学習 e-ポータル)、C4th (小中学校校務支援システム)、スコーレ(市立高校校務支援システム)等を想定している。

連携方法は、API による連携を想定しているが、連携先システムの仕様等により、ファイル連携等も想定している。

なお、連携先システムにおいては本番利用中であることから、データ連携に際しては影響等を確認の上対応すること。

(3) 検証終了後の ID 管理システムについて

令和 9 年 4 月 1 日以降においては、本サービスの継続的な利用を可能とするため、システム環境、サービス利用に係る契約および設定（サービス利用料の支払先を含む）その他関連する必要な環境一式を引き継ぐものとする。なお、検証で使用したアカウントについては、引継ぎの前に一部を残して削除するものとする。

(4) 統合認証基盤及び Microsoft 365 の構築

既に稼働している Entra ID 及び Microsoft A3 ライセンスを利用して Microsoft 365 に対し以下の項目について検証環境を協議の上、設定すること。

ア. Microsoft 365 管理センター

ライセンス/アカウント/グループ管理、組織の設定

イ. Entra ID

アカウント/グループ管理、SAML 連携、条件付きアクセス

ウ. Intune

MDM (モバイルデバイス管理)

エ. Microsoft Defender

Defender 関連のアラート、監査ログ

オ. Microsoft Purview

秘密度ラベル、データ損失防止 (DLP)

カ. SharePoint 管理センター

ファイルの復元、ユーザー誤操作の修正

キ. Exchange 管理センター

メッセージ追跡、メールルール

アドレス帳の作成 (階層型を想定、対象部署は本庁側を含む最大で 15,000 人程度を想定)

ク. Power Platform

業務アプリの作成、フローの管理

ケ. Teams 管理センター

通話/会議/チャットなどの制御、チームの管理

コ. 検証用市立高校用 Microsoft 365 テナントとの連携検証

本案件内で構築する Microsoft 365 は小中学校用テナントに加え、市立高校を想定した検証テナントも構築し、ID 登録・ライセンス付与等に関する連携を検証すること。市立高校は、教職員 ID に加え、生徒 ID も登録・ライセンス付与がなされる点に留意すること。

(5) 既存検証端末の設定変更

川崎市総合教育センターにおいて既存校務端末を設定変更し、動作確認を行うこと。検証用端末の台数は最大で 100 台程度を想定すること。なお、現在本市に整備されている校務端末は以下の機種であり、検証端末は事前に本市の了承を得ること。

	機種	型番
1	LIFEBOOK A5511/G	FMVA86007
2	LIFEBOOK A5511/H	FMVA9200D
3	LIFEBOOK A5512/K	FMVA9600D
4	LIFEBOOK A5513/M	FMVA0B00D
5	LIFEBOOK A5513/N	FMVA0D001
6	LIFEBOOK A5513/R	FMVA0F003
7	dynabook X83/LY	A6X1LYL7411A
8	dynabook X83/LA	A6X1LAL7C12A

端末は EntraID への join にするか、検証用オンプレミス AD (以下「オンプレ AD」と言う。)への join にするか協議の上決定する事、なおオンプレ AD への Join になった場合は、オンプレ AD の調達並びに設定に加え、EntraID と連携設定を実施し動作を確認すること。

※ 1 1 月末までにオンプレ AD の利用有無について決定する。

なお、既設端末への設定変更については導入業者である以下の業者と連携し実施することと

し、必要な費用は本調達に含めること。

●校務端末導入業者

株式会社ウチダシステムズ 電話番号：045-444-2581 ※担当者は別途本市より連絡

(6) 既存ネットワークの設定変更

校務系ネットワークから Microsoft365 へのアクセスを可能にする為に必要なネットワーク機器設定変更を実施すること。なお、既存ネットワークへの設定変更が発生する場合は導入業者である以下の業者と連携し実施すること、必要な費用は本調達に含めること。

閉域ネットワークからインターネットへ直接接続する構成となることから、必要なセキュリティ対策としてUTM（統合脅威管理）機能を有する機器を導入すること。

なお、川崎市立学校において、Fortinet 社製機器が採用されていることを踏まえ、運用の親和性及び管理性の確保から、Fortinet 社製品の採用を優先的に検討すること。

●拠点用ファイアウォール

装置名	数量	仕様（同等とすること）
拠点用ファイアウォール	1	(1) ポート： WAN ポート×2 RJ45 ポート×6 RJ45 FortiLink ポート×2 USB ポート×1 RJ45 管理コンソールポート×1 (2) サイズ：[高さ] 40.5× [幅] 216× [奥行] 160mm (3) ファイアウォールスループット：15Mpps (4) SSL インバクシヨンスループット：1.4Gbps (5) IPSec VPN スループット：7.1Gbps (6) NGFW スループット：1.5Gbps (7) 脅威保護スループット：1.3Gbps (8) 動作環境条件：周囲温度 0～40℃ 周囲湿度 10～90% (9) 最大消費電力：12.8W 以下 (10) その他 ア UTM（統合脅威管理）機能を有すること

●ネットワーク構築業者

富士通 Japan 株式会社 電話番号：044-331-1111

エフサステクノロジーズ株式会社 電話番号：090-6796-1884

株式会社内田洋行 電話番号：03-5634-6402

※担当者は別途本市より連絡

(7) 検証用 ID 管理システムへのデータ投入

人事給与システム等教職員人事データを加工し、ID 管理システムへ投入すること。取り込み方法については可能な限り自動的に取り込みが行える仕組みを協議の上構築・検証・実装すること。なお、令和 9 年の年度切替時対応を本業務で行うこと。

(8) 随時・月次・年次更新を含むアカウント管理フローのリハーサル含むテスト

随時・月次・年次更新を含む教職員アカウントの新規・変更・削除フローのテストを実施すること。年次更新については実際に年度末を想定したテストを実施すること。

(9) 運用保守事業者への引継ぎを想定したドキュメント作成

(1) ～ (6) の業務について今後の運用保守業者に引き継ぐことを想定したドキュメント・手順書を次年度以降の SOC (Security Operations Center) 導入も視野にしていることから、作成すること。

(10) リスク分析と残存リスクを未然に防ぐ仕組み・サービスを調達する為の仕様書案策定

本案件での検証環境構築（ネットワーク・クラウド環境・端末）にてリスク分析を実施し、残存リスクを洗い出すこと。また、事前に危険性を事前に回避するための仕組みやサービス（障害が起きてから動くのではなく、障害が起これないように事前に動く運用）を提言し、その運用委託サービス調達仕様案を作成すること。

(11) 教職員の市内異動時の端末学校間移動についての検討

将来的に強固なアクセス制御環境を構築した上、ロケーションフリー、テレワーク等の拡大も視野にしていることから、端末管理も場所から人へ変更を検討している。

そのため、既存の資産管理システム及び Entra ID 等での資産管理を利用して、教職員の市内異動時の端末学校間移動について検討を行うこと。既存資産管理システムについては下記業者に問い合わせること。

●資産管理システム業者

株式会社内田洋行 電話番号：03-5634-6402 ※担当者は別途本市より連絡

●既存資産管理システム

株式会社内田洋行製 ASSETBASE

(12) 行政系 Microsoft 365 と教育系 Microsoft 365 のテナント共有検証

教育系 Microsoft 365 テナントへ行政系 Microsoft 365 内のユーザー招待を行う予定でいる。本作業の支援を行うこと。

7 成果物

次の成果物について契約期間内に提出し、承認を得ること。

項目	書類
(1) 検証用 ID 管理システムの調達・導入	検証結果報告書
(2) 検証用 ID 管理システムからの連携システムへのアカウント等のプロビジョニング	検証結果報告書
(3) Entra ID 及び Microsoft365 の構築	検証結果報告書
(4) 既存検証端末及び既存ネットワークの設定変更	検証結果報告書
(5) 検証用 ID 管理システムへのデータ投入	人事データ加工に関する情報資料
(6) 随時・月次・年次更新を含むアカウント管理フローのリハーサル含むテスト	検証結果報告書
(7) 運用保守事業者への引継ぎを想定したドキュメント作成	6 に関する運用保守事業者への引継ぎを想定したドキュメント資料
(8) リスク分析と残存リスクを未然に防ぐ仕組み・サービスを調達する為の仕様書案策定	リスク分析と残存リスクを未然に防ぐ仕組み・サービスを調達する為の仕様書案
(9) 教職員の市内異動時の端末学校間移動についての検討	検証結果報告書
(10) 行政側 Microsoft365 と教育側 Microsoft365 のテナント共有	検証結果報告書
(12) 業務完了報告書	業務完了報告書

調整が必要な内容は別途本市と協議の上、調整を行うこと。

8 守秘義務等情報セキュリティーポリシー

- (1) 本仕様書に基づく全ての作業において、市及び学校が提供した業務上の情報を第三者に開示、又は漏えいしないこと。また、そのために必要な措置を講ずること。
- (2) 市及び学校が提供する資料は、原則として貸出しによるものとし、委託完了時には返却すること。また、当該資料の複写及び第三者への提供はしないこと。
- (3) 市及び学校が提供した情報を第三者に開示することが必要である場合は、事前に担当職員と協議の上、承認を得ること。

※上記以外の業務委託の管理要件、情報セキュリティーポリシーについては別紙「川崎市学校情報セキュリティー対策基準」を遵守すること。