

教育情報基盤システム等構築事業賃貸借
仕様書

太子町教育委員会

令和8年9月

I 総則

1. 件名 教育情報基盤システム等構築事業賃貸借

2. 業務目的

本業務は、太子町教育委員会及び町立小中学校における校務処理環境の安定化及び効率化を図るため、校務用端末の更新、クラウドストレージ及び認証基盤の整備、並びに既存ファイルサーバのクラウド移行を実施するものである。併せて、インターネット利用の安全性を高める仕組みや、端末の不正利用・ウイルス感染等を防止する仕組みを導入することにより、情報セキュリティを強化し、教職員が日常的に安全かつ円滑に校務を遂行できる環境を整備することを目的とする。

3. 適用範囲

本仕様書は、太子町教育委員会が実施する本業務について、業務内容その他必要な事項及び受注者が履行すべき事項を定めるものである。

4. 適用基準

本業務の遂行に当たっては、本仕様書によるほか、関係法令、太子町契約規則その他関係規程等を遵守し、適正に実施しなければならない。

5. 対象区域

対象区域は、太子町内に所在する太子町立小学校、中学校及び太子町教育委員会とする。

学校名	郵便番号	所在地	電話番号
太子町立磯長小学校	583-0991	大阪府南河内郡太子町大字春日 1569 番地	0721-98-0040
太子町立山田小学校	583-0992	大阪府南河内郡太子町大字山田 372 番地	0721-98-0049
太子町立中学校	583-0991	大阪府南河内郡太子町大字春日 1479 番地	0721-98-0043
太子町教育委員会	583-0992	大阪府南河内郡太子町大字山田 88 番地	0721-98-0300

6. 構築期限及び契約期間

(1) 構築期限及び端末等納入期限

令和8年12月31日までとする。

(2) 端末等賃貸借期間

令和9年1月1日から令和13年12月31日までとする。

(3) システム及びサービス提供期間

(2)に定める端末等賃貸借期間と同一の期間とする。

(4) 保守期間

(2)に定める端末等賃貸借期間と同一の期間とする。

(5) その他

本仕様書に基づき調達する端末等の賃貸借物件については、賃貸借期間満了後、太子町教育委員会に無償譲渡するものとする。

7. 賃貸借金額の支払い

支払いは、賃貸借期間を 60 ヶ月で算出した月額賃貸借金額とし、1 ヶ月単位の支払いとする。
受注者は、当該月の翌月上旬に請求し、発注者は請求月末までに支払うこととする。

8. システムの全体像

既設のサーバ機能のうち共有フォルダ（ファイルサーバ）機能及び資産管理システムをクラウド環境へ移行するものとする。

各種サーバ機能については、原則としてサービス利用型とし、SaaS を活用した構成とすること。
また、校務用端末の整備を実施すること。

なお、各校の既存オンプレミスサーバ（校務支援システム）との連携及び運用を考慮したシステム設計を行うこと。

9. 概要

- (1) 受注者は、本業務の実施に当たり、太子町教育委員会の指示に従うこと。
- (2) 受注者は、現在稼働中のシステムに影響を及ぼさないよう、既存環境を十分に調査及び理解した上で作業を実施すること。
- (3) 学校内で実施する作業の日程調整は、受注者が行うものとし、その調整先は教育委員会が別途提示するものとする。
- (4) 学校内での作業においては、事前に実施可能な作業をあらかじめ行うなど、作業時間の短縮及び学校運営への影響の低減に努めること。
- (5) 受注者は、整備する校務用端末について、ネットワーク接続後に正常に稼働することを保証すること。
- (6) 受注者は、構築作業の進捗状況、課題及び対応状況について、適宜太子町教育委員会へ報告すること。
- (7) その他導入する上で別途費用が発生する場合、その費用も入札額に含むこととする。

Ⅱ 調達内容

1. 調達範囲

- (1) 環境構築及び運用に必要なハードウェア、ソフトウェア及び各種サービスの選定、調達、設定、設置並びに動作確認
- (2) クラウド環境及び運用保守環境の構築、クラウドサービスの提供並びに運用保守
- (3) 既存環境から新環境への移行作業
既存端末から新端末へのデータ移行は、太子町教育委員会が実施し、受注者は移行手順書（マニュアル）の作成等、サポートを実施するものとする。
既存ファイルサーバからクラウド環境へのデータ移行は、受注者が実施するものとする。
残置するサーバは、校務支援システムの機能のみとする。
- (4) 導入に伴う各種設計、試験、教育、操作説明及び各種ドキュメントの作成
- (5) その他、本仕様書に明記されていないが、本システム構築及び安定稼働に不可欠な一切の作業を含む。

2. 調達物一覧

調達物は、次のとおりとする。

No.	調達機器及びサービス	備考
1	校務用端末	95 台（内訳は詳細機能要件に記載）
2	Microsoft 365 A3	95 ユーザー分
3	資産管理システム	95 台分
4	SWG	95 台分
5	IDaaS	95 ユーザー分
6	クラウドストレージ	4TB 以上
7	EDR・EPP	95 台分
8	モバイルルーター	1 台（教育委員会用）

3. 提出書類等

導入完了後、成果物として下記の書類を提出すること。

No.	納品物	内容
1	基本設計書	本事業の要件を実現するために実装すべき機能や基礎的な事項についてまとめたもの
2	詳細設計書	基本設計書で定められた内容を実現するための実現方法を具体的に定めたもので、導入システムや機器の設定パラメータ等や設定根拠等について技術的な事項をまとめたもの
3	システム構成図	ネットワーク及びシステムの情報・構成をわかりやすくまとめた図
4	ハードウェア台帳	ハードウェア情報、バックアップ、リカバリ手順書
5	ソフトウェア台帳	ソフトウェア情報
6	ライセンス一式	本システム運用に必要なライセンス証書等
7	各種マニュアル	導入したシステムのマニュアル一式
8	保守連絡先一覧	保守に係る連絡先をまとめたもの

Ⅲ 各種サービスの要件

1. 基本方針

システムの構成及び構築は、原則として SaaS 型サービスを活用して行うものとする。

本調達により導入するハードウェア、ソフトウェア及びクラウドサービスは、校務系情報の機密性、完全性及び可用性を確保できる構成とすること。

教育委員会及び各学校における既存の業務及び運用を十分に考慮し、業務への影響を最小限に抑えた設計及び構築を行うこと。

システムの導入及び移行に当たっては、既存システム及び既存ネットワーク環境との整合性を確保し、安定した運用が可能な構成とすること。

2. 運用要件

教育委員会及び学校職員が専門的な知識を有していなくても、日常的な運用及び管理を行うことができる構成とすること。また、システム運用に係る管理者の負担軽減に配慮した構成とすること。

3. 設計及び構築作業

受注者は、本仕様書に定める要件に基づき、本システムの設計及び構築を実施すること。

なお、設計及び構築作業に必要となるライセンス費用、サービス利用料その他関連費用については、本調達に含むものとする。

4. 詳細機能要件

■校務用端末（国内メーカーであること）

仕様

OS	Windows 11 Pro(64bit)
CPU	Intel Core5 120U 以上
メインメモリ	16GB 以上
表示機能	15.6 型以上
キーボード	テンキー付き日本語キーボード（JIS 配列準拠）
ストレージ	暗号化機能付き 256GB 以上
光学ドライブ	スーパーマルチドライブ内蔵
無線 LAN	IEEE802.11a/b/g/n/ac/ax 準拠（Wi-Fi6E 以上）
添付品	AC アダプタ、電源コード、保証書、光学式有線マウス
ディスプレイ出力	HDMI ポート×1（本体に内蔵）
USB ポート	Type-C×1 以上、Type-A×2 以上
Web カメラ	内蔵（Windows Hello 対応）
サウンド	マイク×1 以上、スピーカー×1 以上（※マイクと共用可）
重量	2.0kg 以下

納品台数

太子町立磯長小学校	34 台(内予備機 3 台)
太子町立山田小学校	24 台(内予備機 3 台)
太子町立中学校	36 台(内予備機 3 台)
太子町教育委員会	1 台

設定要件

- (1) OS の初期設定及び認証基盤への参加設定を実施すること。
- (2) グループウェア、EDR・EPP、資産管理システムその他本調達で導入するソフトウェアについて、利用に必要なすべての設定を実施すること。
- (3) 不要なプリインストールアプリケーションを削除すること。削除対象のアプリケーションについては、太子町教育委員会と協議すること。
- (4) 必要なドライバのインストール等、既存プリンターを継続して利用するために必要な設定を実施すること。
- (5) 校務用 SSID へ接続できるよう設定すること。
- (6) 履行場所において、設置確認及び動作確認を実施すること。
- (7) リース対象物品であることを示す管理ラベルを作成し、当該物品の本体等の見やすい箇所に貼付すること。
- (8) 本調達で導入する各 SaaS について、シングルサインオン（SSO）による認証が利用できるよう設定すること。

■Microsoft365 A3

- (1) Microsoft 365 A3 (Education Faculty Pricing) ライセンスを調達し、提供すること。
- (2) 校務用クラウドサービスの認証基盤として、Microsoft Entra ID 又は同等以上の機能を有するディレクトリサービスを構築すること。
- (3) 利用者の異動又は退職に備え、利用者アカウントの新規作成、変更及び削除に係る運用手順書等を提供すること。
- (4) カスタムドメインの設定、利用者アカウントの作成、グループ設計その他本システムの利用に必要な初期設定を実施すること。
- (5) 初期設定に付随して必要となる各種作業についても、本調達の範囲内で実施すること。
- (6) 校務用メールサービスを利用可能とするため、メール基盤の構築及び設定を実施すること。
- (7) 本調達により導入する端末 95 台に対し、設定及び導入を実施すること。

■資産管理システム

- (1) 情報セキュリティ対策ソフトウェアという観点も踏まえ、ISO27001、ISO/IEC 27017 及び P マークを取得しているメーカーの製品を選択すること。
- (2) クライアント端末のハードウェア情報及びソフトウェア情報を自動収集できること。
- (3) 収集した資産情報について、複数条件による検索及び CSV 形式での出力ができること。
- (4) OS バージョン、空き容量、インストールソフトウェア等の情報を管理できること。
- (5) BitLocker の暗号化状態及び回復キーを管理できること。
- (6) ソフトウェア及び Windows 更新プログラムの配布・適用管理ができること。
- (7) 端末のログオン・ログオフ、電源操作、アプリケーション利用状況を記録できること。
- (8) ファイル操作（作成、削除、コピー等）を記録できること。
- (9) Web アクセス、ダウンロード、アップロードの履歴を記録できること。
- (10) USB メモリ等の外部記憶媒体の利用履歴を記録できること。
- (11) 収集したログを管理画面上で検索・閲覧できること。
- (12) 一定時間キーボードやマウスの操作が行われなかった場合、その状態をログとし記録できること。
- (13) 不適切な操作や管理者が定義したルール違反を検知し、利用者及び管理者へ通知できること。
- (14) 指定したアプリケーションがインストールされていない端末からログインがあった場合、その旨を通知できること。
- (15) 指定したアプリケーションの実行制御ができること。
- (16) 指定した Web サイトへのアクセス制御ができること。
- (17) 長期間未接続の端末やログ未収集端末を検知できること。
- (18) USB デバイス等の接続機器を管理できること。
- (19) デバイスごとに利用許可、読取専用、利用禁止の設定ができること。
- (20) ユーザー単位、端末単位又は組織単位で利用制御ができること。
- (21) シリアル番号やベンダ ID、及びプロダクト ID が取得できず、個体識別が行えない USB デバイスについては、台帳への登録を制限できること。
- (22) インターネット経由で端末のリモート操作ができること。

- (23) リモート操作時にファイル転送ができること。
- (24) 利用者の画面を非表示にした状態で保守作業ができること。

■SWG

- (1) Web フィルタリングソフト、もしくはWeb フィルタリングの機能を提供していること。
- (2) 国内で開発・販売されている製品で、日本語によるサポート対応が可能であること。
- (3) 学校ごとに適切な IT 教育を実施するにあたり、児童生徒・教職員等が利用する IT 端末のブラウザ上に下記の情報教育の表示ができるインフォメーション機能を有すること。
 - (1) 児童生徒向けにはインターネット利用時のマナー等の表示が可能で、必要に応じてマナーテストの実施が可能なこと。
 - (2) 教職員向けには、テスト問題（無償提供）にて、教職員が注目すべき行動規程に対する理解を促進し、教職員等への情報セキュリティ教育を支援する内容が含まれていること。
 - (3) 表示内容は教育委員会、及び各学校担当者が作成、追加も可能であり、任意に変更ができる機能を含んでいること。
 - (4) 同様の内容が高い頻度で表示されないよう、最大 100 問のテストをランダム表示できること。
- (4) YouTube 動画を動画 ID、チャンネル ID、ハンドル名を入力することで簡潔に制御設定が可能なこと。
また、チャンネル ID を登録することでそのチャンネル内の動画 ID を自動取得する機能を有していること。
- (5) 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 DB を搭載していること
- (6) ファイル拡張子のリスク別判定の結果安全性が確認できないファイルを、パターンマッチング型のアンチウイルス・振る舞い検知型のサンドボックスに通すことによって、安全性・効率性をどちらも備えることが可能なこと
- (7) HTTP/HTTPS 以外の通信についても制御可能なこと。
- (8) 各アプリケーションへのアクセスの許可に必要なポート及びプロトコル情報を製品データベース側で配信し、設定に反映することができる機能を備えていること。さらに、管理者がアプリケーションを選択するだけで当該サービスへのアクセス制御設定を自動的に行えること。
- (9) IPS 機能を搭載していること。
- (10) IPS のシグネチャデータベースは、製品側で自動的に更新され、最新の攻撃手法や脆弱性に対応可能であること。
- (11) フィルタリングの DB が 1 営業日に最低 4 回は更新されること。また、出口対策用の DB を有し、以下の内容が含まれていること。
 - (1) メーカー独自に収集した、改ざんが行なわれている脆弱な Web サイトの IP アドレス /URL リスト
 - (2) 上記の IP アドレス /URL リストの情報は「改ざんサイト」カテゴリとして明示的に DB に登録・反映される

- (12) Web サービスを機能ごと・組織ごとに制御する機能を有し、Web サービスごとの「ログイン、書き込み、アップロード」等操作ごとに制御でき、それらの設定は同一の管理画面上のボタン1つで簡潔に実施できること。
- (13) Web サービスにログイン後のページもカテゴリ判定が可能なこと。
- (14) Web サービスが取得している認証を表示し、ISMAP 等の国内認証を含めて取得認証ごとに表示・絞り込み検索・制御が可能なこと。
- (15) 管理者画面の二段階認証を行うことで不正ログイン防止を強化できること。
- (16) Google Workspace/Microsoft365 において、個人アカウント・テナントの利用を制御できること。
- (17) データ送信(POST)規制は、「パスワード解除」「警告のみ」「監視」と併用して設定が可能なこと。
- (18) 指定したドメイン・アカウント以外の生成 AI へのログインを制御することが可能なこと。
- (19) 生成 AI での「質問内容」「回答内容」両方のログを取得できること。
- (20) メーカーが推奨するフィルタリング設定のテンプレートが用意されていること。
- (21) ACL でのフィルタリングルールの設定ができること。
- (22) SSL デコード対象を Web サービスに限定し、ルールパーツで条件設定が可能なこと。
- (23) クラウド製品上で、標準で1年間ログの保存ができること。
- (24) 特定の曜日・日付・時間単位でフィルタリングルールの設定が可能なこと。また、祝祭日設定が可能であり、時間割プリセット機能を有していること。
- (25) 長期休暇やテスト期間等の任意の日時を管理者で指定のうえ、フィルタリングルールの反映が可能なこと。
- (26) ユーザーの Web 利用の時間制限ができること。
- (27) ISO27001 の認証を取得していること。

■IDaaS

- (1) PC またはスマートデバイスのウェブブラウザで利用する SAML2.0 に対応したウェブサービスや業務システムに連携し、「顔認証」、「ワンタイムパスワード認証」、「QR コード認証」、「パスワード認証」、「FIDO 認証 (WebAuthn)」を利用できる認証システムであること。また、これらを組み合わせた多要素認証を利用できること。
- (2) SAML2.0 と連携してシングルサインオンが可能な認証システムであること。
- (3) Windows OS のログオンに、「顔認証」、「ワンタイムパスワード認証」、「QR コード認証」、「パスワード認証」を利用して、また、これらを組み合わせた多要素認証が可能な認証システムであること。
- (4) Windows ログオンは、Active Directory で管理するドメイン端末の他、ワークグループ端末でも利用可能なこと (Active Directory 及びワークグループのユーザー情報をインポートすることで Windows ログオンを実現すること)
- (5) SAML などフェデレーション方式による連携ができない業務システムに対し、システム側を改修することなく、多要素認証を使ったログイン認証が可能で、代行入力方式にてシングルサインオンが利用できる認証システムであること。
- (6) Windows ログオン及び代行入力方式での認証において、ネットワーク途絶等により共通認証基

盤提供サービスを利用できない場合には、クライアント端末単独でログオン認証を代替できるオフライン認証機能を有すること。

(7) PIN/パスワード認証（知識による認証）

ユーザーに設定された PIN またはパスワードによる認証が可能なこと。

(8) 顔認証（存在による認証）

登録された顔情報によって、PC またはスマートデバイスに搭載されたカメラ（もしくは外付けのウェブカメラ）に顔をかざすことで認証が可能なこと。

(9) 1 パターンの登録で、顔の向きや、環境の変化や、メガネや帽子などに影響されにくく、マスク着用時の認証が可能であること。

(10) マスク着用時や暗所・逆光における認証精度の低下を防ぐために、ディープラーニング等を応用した認証機能を有していること。

(11) 顔写真や動画によるなりすましを防止するため、パッシブ方式（追加動作不要で、リアルタイムに顔を撮影したものか否かを判定する方式）による偽造対策が顔認証エンジンにより取られていること。

(12) 複数のカメラが接続または搭載されている場合、カメラの選択が可能であること。

(13) 保守性を鑑み、本システムで採用する認証システムの開発業者と、顔認証ソフトウェア内部で使われている顔認証技術の開発業者は同一であること。

■クラウドストレージ

(1) データセンターは日本国内に所在されていること。

(2) 総ディスク容量として 4TB 以上を提供すること。

(3) 想定されるユーザー数（95 ユーザー＋予備など）を全てカバーできるライセンス体系であること。

(4) オンラインストレージ機能を利用できること。

(5) Web ブラウザで利用可能なこと。

(6) 最大 30GB のファイルを送受信できること。

(7) パスワードの自動生成機能及び自動送信機能が利用できること。

(8) 上長承認機能を利用できること。

(9) 承認者を 2 名以上またはグループ単位で設定できること。

(10) 送信した URL 単位でファイルのダウンロード状況を確認できること。

(11) アップロードしたファイルを複数ユーザで共有できること。

(12) 管理者がアクセス権限を設定できること。

(13) CSV ファイルでユーザの一括登録、変更及び削除が可能であること。

(14) ユーザ単位で、利用可能な機能を制限できること。

(15) データの利用頻度や保存期間に応じて複数の保存領域へ自動または手動で移行・管理できるストレージ階層化機能を有すること

(16) AI 技術を利用したデータ活用機能を有すること。

(17) 通信の内容が https により暗号化されていること。

(18) グローバル IP アドレスによるアクセス制御ができること。

(19) ファイル登録時に自動でウイルスチェックを行うこと。

- (20) サービス利用終了時には、保存データが復元不可能になるよう消去すること。
- (21) 既設ファイルサーバーからクラウド環境へのデータ移行を実施すること。

■EDR・EPP

- (1) 単一のエージェントでエンドポイント防御機能を提供できること。
- (2) プロセスの挙動、レジストリ変更、メモリ操作、権限昇格等の不審な挙動を監視し、シグネチャに依存しないふるまい検知機能を有すること。
- (3) リアルタイム検索機能を有すること。
- (4) 予約検索機能を有すること。
- (5) オンデマンド検索機能を有すること。
- (6) 既知マルウェアを検出・ブロックできる機能を有すること。
- (7) AMSI(Microsoft Antimalware Scan Interface) を利用した防御機能を有すること。
- (8) ファイルレスマルウェアに対応した防御機能を有すること。
- (9) ランサムウェア攻撃を検知し、ロールバックできる機能を有すること。
- (10) ランサムウェアにより暗号化されたファイルを復旧させる際にボリュームシャドウコピーを利用せずに復元できること。
- (11) マスターブートレコードを暗号化するランサムウェア攻撃を検知・ブロックできる機能を有すること。
- (12) リモートからのランサムウェア攻撃に対する防御機能を有すること。
- (13) ブラウザに存在する脆弱性を攻撃して Web ブラウザに感染する MITB (Man-in-the-Browser) 攻撃を防止する機能を有すること。
- (14) ブラウザの Cookie を保護する機能を有すること。
- (15) マルウェア検知時にプロセスの停止やファイルのクリーンアップ機能を有すること。
- (16) 脅威を駆除した後に脅威の侵入経路及びファイルに対する影響範囲（発生日時、アプリケーションなど）などをマッピングして表示する機能を有すること。
- (17) デバイスへの攻撃と思われる検知が確認された場合に、Safe モードの再起動を防止するなどといった形で保護レベルが自動的に高くなる機能を有すること。
- (18) Safe モードで起動しても保護機能を保持し続けること。
- (19) ダウンロードしたファイルを評価するレピュテーション機能を有すること。
- (20) USB メモリや MTP/PTP 接続デバイスといった、外部機器の接続に対して制御する機能を有すること。
- (21) アプリケーションコントロール機能を有すること。
- (22) 情報漏えい対策 (DLP) 機能を有すること。
- (23) 高度な攻撃を受けた場合に自動で防御機能を高める機能を有すること。

■モバイルルーター

用途：教育委員会からの各種 SaaS サービス及び校務支援システムへのアクセス、ファイルのアップロード等。

- (1) 固定 IP アドレスを付与できる製品であること。
- (2) 不正利用防止機能を有すること。

- (3) 無線 LAN 規格は IEEE 802.11 に対応すること。
- (4) 通信規格は 4G LTE に対応すること。
- (5) 月間通信容量は 100GB 以上であること。

■DNS・ドメイン

ドメインの利用料及びゾーン情報を管理する DNS サーバーの利用料を含むこと。

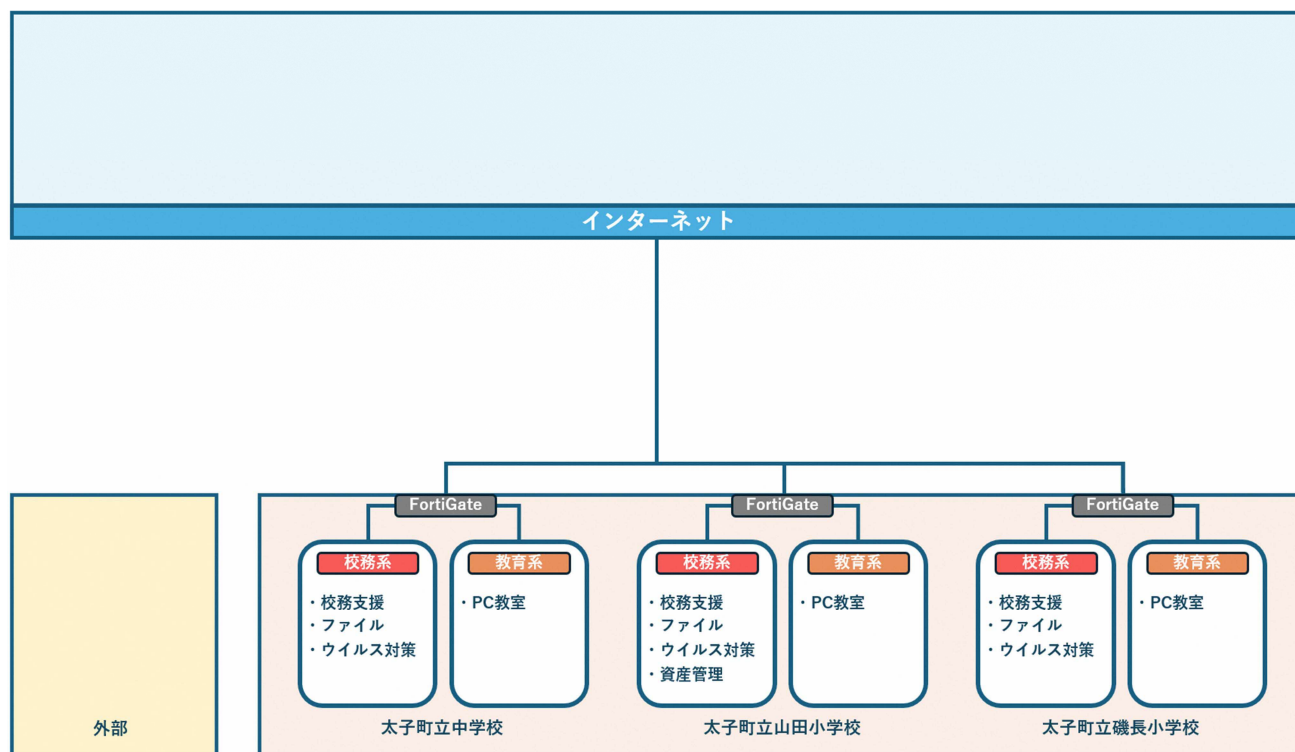
■その他

- (1) 調達した全ての機器及びサービスを適切に利用できるよう、必要な設定を行うこと。
- (2) 本業務に係る全てのサービス及びソフトウェア並びに発注者が指定するソフトウェアについて、調達する全ての端末で利用可能となるよう設定すること。
なお、本業務外で有償ライセンスが必要となるソフトウェアについては、発注者から当該ライセンス及びインストールメディアの提供を受けるものとする。
- (3) 既存プリンターについては、発注者の指示の下、調達する端末で利用できるよう設定を行うこと。
- (4) メールについて、詳細設定やデータ移行等については発注者と別途協議を行うこと。
- (5) その他の詳細な要件については、落札後速やかに発注者と協議の上、決定すること。
- (6) 現在の設定及び構築内容については、発注者が情報提供を行うものとする。設定変更が必要な場合、発注者を通じて現行保守業者との連携を図るものとする。
- (7) 構築作業に発生する廃棄物及び機器製品の梱包材等の回収に係る費用については入札額に含むこととし、適切に処理をおこなうこと。

5. 保守要件

- (1) 保守受付時間は、平日 9 時 00 分から 17 時 00 分までとする。
(土曜日、日曜日、祝日、年末年始及びお盆期間を除く。)
- (2) 賃貸借期間中における障害発生時には、切り分け、障害分析及び障害箇所の特定を実施すること。
- (3) ハードウェア、ソフトウェア及びサービスについて、製品及び技術に関する情報提供を行うこと。
- (4) 納入製品に不具合が生じた場合には、復旧作業を実施すること。
- (5) 落下等により納入機器が破損した場合の修理費用は太子町の負担とする。
- (6) OS の破損、機器交換又は修理後に必要となる OS 及び各種ソフトウェアの再設定、並びにマスターイメージ等を用いた復元作業は、本調達の範囲内で実施すること。
- (7) 各学校において本システムを効果的に活用できるよう、運用に関する相談対応及び有益な情報の提供を行うこと。
- (8) 本調達で導入する SaaS について、年次更新作業、利用者の追加・変更・削除、ライセンス管理並びにシングルサインオン（SSO）の設定変更等、運用に必要な管理作業を実施すること。
- (9) 本調達の対象となる PC、ソフトウェア及び SaaS を保守対象とし、既存ネットワーク機器その他本調達対象外の機器及びシステムは保守対象外とする。

【現状構成図】



【次期構成図】

