東大阪市教育ICT環境更新・運用保守業務委託事業仕様書

令和７年５月
東大阪市教育委員会事務局
施設整備室

目次

１　件名

東大阪市教育ICT環境更新・運用保守業務委託事業

２　目的

本市学校園等に整備しているネットワーク機器等は、老朽化が進み、サポート終了を迎えようとしている。また、文部科学省では、令和６年１月に「教育情報セキュリティポリシーに関するガイドライン（以下、「ガイドライン」という。）」を改訂し、クラウドサービスの利活用を前提とした目指すべき構成を明確化し、教育機関における情報セキュリティの強化を図り、安全で信頼性の高いICT環境の実現を推奨している。

東大阪市教育ICT環境更新・運用保守業務委託事業（以下、「本事業」という。）は、ネットワーク機器等を更新し、校務系と学習系のネットワークの統合を図る中でネットワーク環境にかかるボトルネックを解消したうえで、文部科学省が示す学校規模別の推奨帯域を満たすとともに、ガイドラインに則り、統合型認証基盤を利用したゼロトラスト環境を構築し、アクセス場所（校内外）を問わず、安全な校務を可能とすることで、円滑な教育活動の実現を目指すものである。

本事業を実現するにあたり、構築・運用保守費用の最小限化を前提に、民間事業者の持つ高度かつ広範な専門知識、技術や経験等を活用し、確実かつ円滑に本事業を進めていくことのできる事業者を選定するため、公募型プロポーザル方式により事業者を広く募集し、総合的な評価をもって決定するものとする。

３　事業概要

市立小学校・中学校・高等学校においては、校務系ネットワークを廃止し、学習系ネットワークに統合し、幼稚園・こども園、東大阪医療センター院内学級、教育センター及び東大阪市役所本庁舎（以下、「本庁舎」という。）においては、ネットワーク機器及び教育サーバ群等を更新する。また、ゼロトラストセキュリティに対応し、ロケーションフリーかつシームレスに利用できる環境を構築する。

４　対象拠点・人数等

（１）　対象拠点

【別紙１】のとおり。

（２）　人数等

【別紙２】のとおり。

５　更新及び運用保守業務期間

（１）　教育ICT環境更新業務期間

契約締結の日から令和８年３月31日

（２）　教育ICT環境運用保守業務期間

令和８年４月１日から令和13年３月31日

6　成果物

①　導入スケジュール

②　作業計画書

③　完成図書

④　ネットワークの構成図（論理、物理）

⑤　ネットワーク機器の設定情報（設定変更した既設ネットワーク機器も含む）

⑥　ルーティングポリシーとその設定が記されたネットワーク図

⑦　VLAN構成図

⑧　各学校内配線図

⑨　機器性能試験成績書（ケーブル試験含む）

⑩　作業内容確認用写真（作業前、作業中、作業後）

⑪　管理者向けソフトウェア・ハードウェア・クラウド等操作マニュアル

⑫　学校向けソフトウェア・ハードウェア・クラウド等操作マニュアル

⑬　学校ごとに機器や材料の数量、型番、メーカー名、シリアルNO、無線機器のMACアドレス等が確認できる内訳明細のある設計書等の積算書類

⑭　運用保守連絡体制図

⑮　説明会・研修計画

⑯　説明会・研修動画

⑰　課題管理表、議事録及び付随資料

7　事業体制

（1）　本市側の体制

本事業の遂行にあたっては、本市は教育委員会施設整備室を事務局とし、関係部署担当者及び学校園関係者との情報共有を密にしながら円滑な推進を図る。

（2）　受託者側の体制

①　新教育ICT環境を整備及び運用する上で、受託者が行う業務・支援の実施に必要な人員を配置し、体制表にて提示すること。

②　各種対応のスピードと質を確保するため、契約日時点において、大阪府内に保守拠点（本社・支社または営業所）を１箇所以上確保すること。

③　新教育 ICT 環境の運用状況について定期的な報告を行うとともに、システムの維持・向上を図るために、継続的な運用改善を行うことができる体制とすること。

④　事業構成員には、本市と同等以上の規模の自治体において、環境構築整備、運用支援業務等の経験を有する者を含むこと。

⑤ 本事業に従事する要員は、必要な知識・技術に精通し実務経験を有していること。

8　現行教育ICT環境

①　本市の現行教育ICT環境は、【別紙３（図１－１）】のとおりである。

②　本市の回線について、J:COM東大阪局を中継する地域イントラネット網を構築している。全小中

高等学校、教育センター及び東大阪医療センター院内学級からJ:COM東大阪局の間については、８拠点で10Gbpsの回線を共有するベストエフォート型閉域網を構築している。また、幼稚園・こども園から本庁舎の間は、OPTAGE for Business ブロードバンドタイプ（最大200Mbps)を利用している。

③　全小中高等学校の教職員、教育センター内及び東大阪医療センター院内学級用端末は、各拠点内を抜けて地域イントラネット網から本庁舎に接続、ファイアウォール等でのセキュリティ対策を実施後、インターネットサービスプロバイダーであるJ:COM経由でインターネットに接続している。なお、名前解決は、本庁舎サーバ室の業務用仮想サーバ（FUJITSU PRIMEQUEST 3400S）内の仮想ゲストとして構築したDNSサーバが行っている。

④　全小中高等学校の児童生徒用端末は、各拠点内を抜けて地域イントラネット網からインターネットサービスプロバイダーであるJ:COM経由でインターネットに接続している。ただし、校内のL2スイッチが1Gbps対応のため、前述の10Gbpsの回線を活かしきれていない。

名前解決は、J:COM東大阪局に設置しているDNSサーバ（Soliton D3-SX15-A-GIGA2-H2）が行っている。

⑤　幼稚園・こども園内の端末については、各拠点内から本庁舎に接続、ファイアウォール等でのセキュリティ対策を実施後、インターネットサービスプロバイダーであるJ:COM経由でインターネットに接続している。

⑥　体育館で防災及び授業用として接続可能なWi-Fi用の回線も敷設している。

⑦　小中学校現場には、教職員の他に会計年度任用職員等が勤務している。学校現場の会計年度任用職員等は、機微な情報へアクセスできないなど制限された環境で共有端末を使用している。また、学校現場の会計年度任用職員等の中でも、スクールソーシャルワーカー（約30名）、学校司書（約30名）、母国語学級統括指導者及び人権教育推進支援員（約10名）に対しては、MS365 A1ライセンス（ICT支援員（19名）のみ、MS365 A3ライセンス）を付与している。

⑧　教育委員会においては、特定の職員のみ端末を使用している。その中でも施設整備室職員（ICTアドバイザー（５名）含む計11名）のみが、サーバへ直接アクセスできるなど各種サービスの管理者としての権限を持っている。

（１）　小学校内ICT環境について

ア　校務外部系ネットワーク及び防災用フリーWi-Fi（【別紙３（図１－２）】参照）

①　校務外部系ネットワークは、PC教室を起点として、教職員用端末が利用するネットワークとPC教室用のネットワークを１つのセグメントで構築している。LANケーブルは全てCat5eで敷設している。教職員は、二要素認証（LOCK STAR-SGate）により校務内部系ファイルサーバ及び統合型校務支援システム（両備システムズ RYOBI-校支援）に接続している。

②　IEEE802.11ac対応のアクセスポイント（AeroHive AH-AP130-AC-W）は職員室、保健室及び事務室内の他に２～４クラスに１つの割合で、普通教室前の廊下に、一部の学校の特別教室等前にも設置している。ただし、校長室では有線LANである。本庁舎側を通る経路とは別に体育館に導入した防災用Wi-Fiを経由する経路を新設しており、データ量の多さが予想される特定の通信(NHK for School等)に利用(オフロード)している。体育館に導入した防災用フリーWi-Fiについては、令和６年10月より授業等で教職員及び児童用端末から接続できるようになっている。

③　教職員用端末はWindowsタブレット（Windows10 Enterprise 2016 LTSB及び2019 LTSC）を導入している。また、動画編集用iPad１台及び教職員用iPad1台も校務外部系ネットワークに参加している。

④　普通教室等に大型提示装置（以下、「電子黒板等」という）及び実物投影機（以下、「書画カメラ」という）を導入しており、教職員用端末の画面を電子黒板等に無線投影装置を使って無線接続している。なお、新教育ICT環境下でも引き続き使用する。

⑤　職員室に複合機（KONICA MINOLTA 650iSeriesPCL）及び各校独自に導入したプリンター等を設置している。なお、新教育ICT環境下でも引き続き使用する。

⑥　職員室に勤怠管理用タイムレコーダを設置している。なお、新教育ICT環境下でも引き続き使用する。

⑦　図書室に図書館用蔵書管理システム用端末（Windows10 Enterprise 2016 LTSB）を導入している。なお、新教育ICT環境下でも引き続き使用する。

⑧　PC教室にカラーインクジェットプリンタ（EPSON PX-M711TH5）を１台導入しているが、学校によっては職員室等の別室に移動し使用している。なお、新教育ICT環境下でも引き続き使用する。

⑨　PC教室にNAS（I-Oデータ HDL2-X4/ST5）を導入し、教職員用端末、動画編集用iPad及び教職員用iPadが接続しており、動画や写真等を保存している。

イ　学習系ネットワーク（【別紙３（図１－３）】参照）

①　学習系ネットワークは、PC教室を起点として、令和３年度にGIGAスクール構想の実現に向けて構築した児童用端末が利用するネットワークである。LANケーブルは全てCat6Aで敷設している。

②　IEEE802.11ax対応のアクセスポイント（Cisco Meraki MR-36）は普通教室、特別教室、特別支援教室、少人数教室及び留守家庭教室内に設置している。

③　児童用端末はiPad第７世代Wi-Fiモデルを導入し、アクセスポイント（Cisco Meraki MR-36、体育館防災用フリーWi-Fi）にのみ接続できるよう設定している。令和８年度から児童用端末はChromebookWi-Fiモデルに変更する予定である。

④　アクセスポイント（Cisco Meraki MR-36）からPoEスイッチングハブ（Cisco Meraki MS120-24P）を経由して接続しているファイアウォール（Palo Alto Networks PA-850）は、ファイアウォールとしての機能は停止しており、学習系ネットワークのデフォルトゲートウェイ及びDHCPサーバとしてのみ機能している。なお、DHCPサーバの機能を使用し、児童用端末はiPad第７世代のMACアドレスに対して固定のIPアドレスを割り振っている。

⑤　普通教室等に電子黒板等と書画カメラを導入しており、児童用端末の画面をApple TVを使用して電子黒板等に投影している。前述のとおりChromebookに変更した場合、Apple TVを使用した電子黒板等への投影ができなくなるため、電子黒板等を新教育ICT環境下のネットワークに参加させ、無線投影する予定である。

（２）　中学校内ICT環境について

ア　校務外部系ネットワーク及び防災用フリーWi-Fi（【別紙３（図１－４）】参照）

①　（１）ア①と同じ。

② IEEE802.11ac対応のアクセスポイント（AeroHive AH-AP130-AC-W）は基本的に職員室、保健室及び事務室内に設置している。一部の学校で職員室、保健室及び事務室以外の教室前の廊下に設置している。また、IEEE802.11n/a/b/g対応のアクセスポイント（フルノシステムズ ACERA850F）は普通教室及び少人数教室内に設置している。校長室は有線LANである。体育館に導入した防災用フリーWi-Fiについては、令和６年10月より授業等で教職員及び生徒用端末から接続できるようになっている。

③ 教職員用端末はWindowsタブレット（Windows10 Enterprise 2016 LTSB及び2019 LTSC）を導入している。また、動画編集用iPad１台も校務外部系ネットワークに参加している。

④ 普通教室等に電子黒板等及び書画カメラを導入しており、教職員用端末の画面を電子黒板等に無線接続している。なお、新教育ICT環境下でも引き続き使用する。

⑤ （1）ア⑤と同じ。

⑥ （1）ア⑥と同じ。

⑦ 図書室に図書館用蔵書管理システム用端末（Windows10 Enterprise 2019 LTSC）を導入している。なお、新教育ICT環境下でも引き続き使用する。

⑧ カラーインクジェットプリンタ（EPSON PX-M711TH5）をPC教室に１台、職員室に１台導入している。新教育ICT環境下でも引き続き使用する。

⑨ PC教室にNAS（I-Oデータ HDL2-X4/ST5）を導入し、教職員用端末及び動画編集用iPadが接続しており、動画や写真等を保存している。

⑩ PC教室の端末は新教育ICT環境下でも引き続き使用する。（９．５.16参照）

イ 学習系ネットワーク（【別紙３（図１－５）】参照）

（1）イと同じ。

※ 「児童」を「生徒」と読み替えること。

※ 中学校は留守家庭教室なし。

（３） 高等学校内ICT環境について

ア 校務外部系ネットワーク及び防災用フリーWi-Fi（【別紙３（図１－６）】参照）

① 校務外部系ネットワークは、３階第１PC教室横の倉庫を起点として、職員室等、普通教室、第１PC教室、第２PC教室、第３PC教室及びCALL教室用のネットワークが敷設されている。LANケーブルは基本的にCat5e（一部はCat6）で敷設している。

② IEEE802.11ac対応のアクセスポイント（AeroHive AH-AP130-AC-W）は職員室、各教科準備室、普通教室前廊下に概ね２教室に１つの割合でアクセスポイントが設置されている。第１、第２、第３PC教室及びCALL教室は全て有線のネットワークで構成されている。なお、第１、第２、第３PC教室及びCALL教室のネットワーク更新は本事業の対象外である。体育館に導入した防災用フリーWi-Fiについては、令和６年10月より授業等で教職員及び生徒用端末から接続できるようになっている。

③ 教職員用端末はWindowsタブレット（Windows10 Enterprise 2019 LTSC）を導入している。

④ （1）ア⑥と同じ。

⑤ 職員室に設置しているプリンター等は新教育ICT環境下でも引き続き使用する。

⑥ （2）ア⑧と同じ。

イ　学習系ネットワーク（【別紙３（図１－７）】参照）

① （1)イ①と同じ。

② （1)イ②と同じ。

③ 生徒用端末はChromebookを導入し、アクセスポイント（Cisco Meraki MR-36）にのみ接続できるよう設定している。将来的に生徒用端末はBYODになる予定。

④（1）イ④と同じ。

（4） 幼稚園・こども園内ICT環境について

校務外部系ネットワーク（【別紙３（図１－８）】参照）

① 校務外部系ネットワークは、職員室を起点として、教職員用端末が利用するネットワークを構築している。LANケーブルは全てCat5で敷設している。教職員は、二要素認証（LOCK STAR-SGate）により校務内部系ファイルサーバに接続している。

② 職員室でのみ有線LAN接続で教職員用端末を使用できる。

③ 教職員用端末はWindowsタブレット（Windows10 Professional）を導入している。

④ （3)ア⑤と同じ。

⑤ （1)ア⑥と同じ。

（5） 東大阪医療センター院内学級内ICT環境について

校務外部系ネットワーク（【別紙３（図１－９）】参照）

① 校務外部系ネットワークは、３階会議室を起点として、院内学級用端末が利用するネットワークを構築している。LANケーブルは全てCat5eで敷設している。

② IEEE802.11ac対応のアクセスポイント（AeroHive AH-AP130-AC-W）は５階教室内に導入している。

③ 院内学級用端末はiPad第７世代Wi-Fiモデルを導入している。令和８年度から院内学級用端末はChromebookWi-Fiモデルに変更する予定である。

（6） 教育センター内ICT環境について

校務外部系ネットワーク及び防災用フリーWi-Fi（【別紙３（図１－10）】参照）

① 校務外部系ネットワークは、２階サーバ室を起点として、職員用端末が利用するネットワークと研修室用端末が利用するネットワークを異なるセグメントで構築している。LANケーブルは全てCat5eで敷設している。職員は、二要素認証（LOCK STAR-SGate）により校務内部系ファイルサーバに接続している。

② IEEE802.11ac対応のアクセスポイント（AeroHive AH-AP130-AC-W）は研修所員室及び相談所員室内の他に２～４執務室に１つの割合で、執務室前の廊下に設置している。体育館に導入した防災用フリーWi-Fiについては、令和６年度10月より職員用及び研修用端末から接続できるようになっている。

③ 職員用端末はWindowsタブレット（Windows10 Enterprise 2016 LTSB及び2019 LTSC）を、研修用端末はWindowsタブレット（Windows10 Professional 、Windows10 Enterprise 2016 LTSB及び2019 LTSC）、iPad第７世代及びChromebookを導入している。

④ サーバ室に勤怠管理用タイムレコーダを設置している。なお、新教育ICT環境下でも引き続き使用する。

⑤　研修所員室等に設置しているプリンター等は新教育ICT環境下でも引き続き使用する。

⑥　サーバ室にNAS（I-Oデータ HDL2-X4/ST5）を導入し、職員用及び研修用端末が接続している。

（7）　本庁舎内ICT環境について

教育サーバ群（【別紙３（図１－11）】参照）

①　教育サーバ群は、【別紙５】のとおり仮想サーバ、業務用仮想サーバ（FUJITSU PRIMEQUEST 3400S）、統合ストレージ（FUJITSU ETERNUS NR1000 F2650）、ファイアウォール（Fortinet FortiGate-301E）、ADサーバ（FUJITSU PRIMERGY RX1330 M3、業務用仮想サーバ内の仮想ゲスト）、不正端末遮断センサー（PFU iNetSec SF 510センサー）等で構成されている。

②　仮想サーバは、業務用仮想サーバ（FUJITSU PRIMEQUEST 3400S）と管理用仮想サーバ（FUJITSU PRIMERGY RX2530 M4）があり、それぞれ【別紙５】のとおり複数の仮想ゲストで構成されている。

③　統合ストレージ（FUJITSU ETERNUS NR1000 F2650）内では、業務用仮想サーバ（FUJITSU PRIMEQUEST 3400S）のデータストア並びに教職員用端末のみアクセスできる校務外部系ファイルサーバ、校務内部系ファイルサーバ及び個人フォルダの仮想ストレージが稼働している。

④　統合ストレージ（FUJITSU ETERNUS NR1000 F2650）の使用容量は、約20TBである。

⑤　教職員用端末から校務内部系ファイルサーバ及び統合型校務支援システム（両備システムズ RYOBI-校支援）への直接アクセスはファイアウォール（Fortinet FortiGate-301E）にて禁止し、SGateサーバ経由でのみアクセスを許可している。SGateサーバへのログインは、USBキーを利用した二要素認証（LOCK STAR-SGate）が必要である。なお、ファイアウォール（Fortinet FortiGate-301E）は、校務外部系セグメント、校務内部系セグメント、外部接続用セグメント間のアクセス制御を行っている。

⑥　プライベートクラウド型の統合型校務支援システム（両備システムズ RYOBI-校支援）へのアクセスは、【別紙３（図１-11）】を参照。

⑦　パブリッククラウド型出退勤システム（アマノ TimePro-VG）の勤怠データ及びAI型教材（COMPASS Qubena）の児童生徒データを統合型校務支援システム（両備システムズ RYOBI-校支援）へ連携するために、業務用仮想サーバ（FUJITSU PRIMEQUEST 3400S）内にある中継サーバを経由している。教育サーバ群更新後も中継サーバは必要。

⑧　Active Directoryにて、ユーザ、グループ、ファイルへのアクセス権限等を一元管理している。なお、Microsoft EntraIDとは連携していない。

⑨　不正端末遮断センサー（PFU iNetSec SF 510センサー）にて、教育ネットワークへの未許可端末の接続を防止している。

９　本事業の要求仕様

本仕様書及び仕様項目適合確認表（様式第11号）を熟読のうえ、全体の構成について提案すること。なお、「望ましい」と記載された各項目については必須要件ではないが、当該項目を満たさない場合には、積極的に代替案を提示すること。

９．１　基本事項

（１）　事業運営

① 仕様書や企画提案書で定めた基準を満たし確認したことを示す提出状況・要求性能確認書を業務段階ごとに作成し、事前に市に提出して承認を得ること。

② 本事業に関する導入課程の経過、進捗状況について定例会議等を通じて報告すること。また、進捗報告書及び打合せ会議に際しては、議事内容を事前に提示するとともに、毎回受注者が議事録を作成し、会議終了後に速やかに提出すること。

③ サービス提供を進める上で必要な関係部署、関係機関との調整、資料等の作成を行うこと。

④ 本事業に関する構築に際しては、本市が必要と判断した場合、関係するメーカーSE等との質疑（十分なセキュリティ対策が施されているWebシステムを使用してのWeb会議を含む）が可能となるよう配慮すること。

⑤ 設計、構築期間においては、必要に応じて関係者を招集の上で定例会等とは別途の検討会を実施し、スムーズな業務進行を図ること。また、仕様や要件の確認及び確定に関しては、必ず書面により行うこと。

⑥ 課題管理表を作成し、定期的に共有、進捗確認を行うこと。

⑦ 本事業に関する全ての文書は、様式や記載方法及び文書番号の採番ルール等を定め、標準化・統一化を図ること。

⑧ 作業の遅れが生じた場合、原因を調査し、人員の追加や担当者の変更等、体制の見直しを含むリカバリプランを提示し、本市の承認を得たうえで、これを実施すること。

（2） 設定に必要な基礎情報の登録作業

① 新教育ICT環境において必要となる設定情報や登録データについては、本市と協議のうえ決定すること。

② 新教育ICT環境を利用するために必要な利用者の登録を行うこと。また、利用者の所属や役職などに応じた各種権限設定を行うこと。なお、登録に必要な情報は、本市が提供する。必要なデータを作成するにあたっては、本市の求めに応じて作業を支援すること。

③ 構築にあたっては、必要に応じて本市が別途契約しているネットワーク保守業務受託者、通信回線業者等の関係業者とも連携をとり、円滑な構築作業に努めること。

（3） 拠点作業

① 仕様書②におけるネットワークアセスメント調査・分析業務の結果を踏まえて、作業を実施すること。

② 受託者は現地調査・構築に当たり、作業計画書を作成し、本市の承認を受けること。

③ 学校内での作業の具体的な日程調整は受託者が行うこと。調整先は本市が提示する。

④ 基本的な作業は、夏季及び冬季休業期間並びに土曜日、日曜日及び祝日とする。なお、これらでは作業期間が不足する場合や学校の都合により、平日に作業を実施することも可とするが、学校での授業に支障のないよう、また、事故が発生しないように最大限配慮すること。

⑤ 学校内での作業については、可能な作業は事前に実施し、時間短縮に努めること。

⑥ 作業後の正常性確認については、事前に本市と協議した上、作成した試験成績書に基づき確認を行うこと。

⑦ 設計業務に当たり必要となる各種許可申請、届出等がある場合は、受託者の責任において、適切に許可申請、届出を実施すること。

⑧　校舎壁面で点検口等が追加で必要な場合は、アスベストを含有している前提で対応・設置すること。また、配管作業あるいは壁や床の貫通作業が必要な場合は本市の承諾のうえ対応すること。

⑨　作業期間中に学校敷地内において、他の工事や作業等が行われる場合、本市及び学校を通じて、他の工事等の関係者と十分調整を行い、作業を円滑に進めること。

⑩　近隣住民への影響が見込まれる場合は、受託者にて事前に作業内容・影響等について近隣への周知を行うこと。

⑪　作業用車両の駐車場及び資材置き場等は、原則学校敷地内の空きスペースを使用可能とするが、位置を明らかにした上で事前に本市及び学校と協議すること。

⑫　事故、火災等への対応について、受託者はあらかじめ防災マニュアルを作成すること。

⑬　機器の設置に当たり、転倒・転落の防止策やケーブルの抜け防止等を考慮した対応を行うこと。

⑭　アクセスポイント等の整備するネットワーク機器については、児童生徒が容易に触れられないように高所に設置する等の対策を講じること。設置場所については事前に協議し、合意した方針に従い設置すること。

⑮　納入機器の梱包資材については、納入後、受託者が責任をもって処分すること。

⑯　既存のサーバ及びネットワーク機器に影響がないよう設定すること。

⑰　提案に基づく環境と整合をとるため、本市の求めに応じて、既存関係事業者との協議や説明資料の作成などに対応すること。

⑱　本仕様書に無い項目であっても、提案内容において必要となる機器及び各種ライセンス等は 全て見積に含めること。 また、構築期間のライセンス等は構築費用の見積に含めること。

（3）　留意点

①　令和８年３月31日までは、基本的に現行のネットワーク及び教職員用端末を使用することを想定しているが、提案構成を考慮し、部分的ないしは全体的に新ネットワーク及び教職員用端末の使用が望ましい場合は、協議のうえ決定する。

②　前述の８⑦、⑧を考慮、【別紙２】を参考にし、数が増えることも想定し、各拠点のユーザに対する各サービスに必要なライセンス数を調達すること。

③　本事業の全部又は一部を第三者に委託し、又は請け負わせてはならない。ただし、あらかじめ別に定める書面による本市の承諾を得た場合はこの限りでない。

④　業務提案内容の実現に必要な追加費用及び別途費用は、全て受託者の負担とする。

⑤　本仕様書に記載なき事項についても、本事業の目的実現のため必要と推測される場合は、受託者の負担により完全に実施すること。

⑥　教育ネットワーク及び教職員用端末更新に必要な既存機器等の設定作業（データ移行作業含む）は、基本的に受託者が実施することを前提で提案すること。正当な理由で実施できない作業がある場合は、本市が既存関係事業者へ必要な作業費用を支払い、作業を依頼する。

⑦　企画提案書の提案事項を達成する意思が受託者に認められないなど、企画提案書に記載した事項に対する履行状況が特に悪質と認められる場合は、契約を解除し、損害賠償の請求を行うことがある。

９．２　別調達の各機器の仕様等

受託者が環境構築及び運用保守を行う本事業とは別で調達するネットワーク機器及び教育サーバ群機器等並びに教職員用端末の留意点及び各機器の仕様は以下のとおりである。ただし、現時点の想定仕様であり、今後の整備全体概要やコスト面の検討の中で変更が生じた場合は、協議のうえ決定する。

ネットワーク機器等の設置拠点及び想定台数については、【別紙４】、現行の教育サーバ群機器等の情報については、【別紙５】を参照すること。

９．２．１　各機器の共通留意点

① メーカー保証５年以上が付帯していること。
② 原則として受託時点で製品化された最新の製品であること。
③ 納入完了までに機器のファームウェアのバージョンアップ、ソフトウエア等がバージョンアップされる場合は、必要に応じて本事業内でバージョンアップを行うこと。
④ 基本的に365日24時間の稼働が可能な構成とすること。
⑤ 別事業者とリース契約により調達した機器については、契約満了後に無償譲渡を受けることを想定している。

９．２．２　アクセスポイント

① IEEE802.11a/b/g/n/ac/ax以上に準拠すること。
② IEEE802.3atに対応していること。
③ IEEE802.11iに準拠及び認証方式として WPA3、暗号化方式としてAESに対応していること。
④ 2.4GHz帯、5GHz帯及び6GHz帯を同時利用可能なこと。
⑤ アップリンクポートとして、自動検知式の10/100/1000BASE-T（RJ-45）イーサネットを最低限搭載していること。
⑥ 2.4GHz帯と5GHz帯は2×2MIMO、2ストリーム以上に対応していること。また、6GHｚ帯は4×4MIMO、4ストリーム以上に対応していること。
⑦ 周辺のアクセスポイントを検出できる機能を有すること。
⑧ 電源を切断してもログ情報を保持する機能を有すること。
⑨ IEEE802.1xに準拠すること。
⑩ 今回導入するアクセスポイント全台を一括管理できる管理システムはクラウドサービスとして提供されていること。
⑪ 管理システムの障害時でも利用者サービスに影響がなく、利用を継続できるように構成及び設定すること。
⑫ 管理システムとアクセスポイントとの通信は暗号化され、専用VLANで通信すること。
⑬ 管理システムは日本語化されていること。
⑭ SNMPv1/v2c/v3による管理機能を有すること。
⑮ NTPクライアント機能を有すること。
⑯ チャネル管理の自動化により稼働中でも最適なチャネルへの移動が可能であること。
⑰ RF最適化用のスキャン、WIDS/WIPS専用のDual Radioを内蔵することにより、端末への無線LANサービスへの影響を最小化する機能を有すること。

⑱　アクセスポイントを経由して利用したアプリケーションの統計情報を取得できること。
⑲　クライアント単位で利用者利用状況の統計データを表示可能なこと。
⑳　クラウドの信頼性は99.99以上のSLAを提供すること。
㉑　アクセスポイント間あるいは管理マネージャでチャンネルを自動調整できよう設定すること。
㉒　エラーログが取得、確認できるように設定できること。
㉓　防災時利用も想定し00000JAPANなどのSSIDプロファイルを容易に切替及び発出することが可能であること。

９．２．３　PoEスイッチングハブ

①　【別紙４】のコアスイッチ用（集約スイッチ用）及び（教育センター）サーバ室用については、1000BASE-T/2.5GBASE-T/5GBASE-T/10GBASE-Tに対応でき、それら以外は10/100/1000BASE-Tに対応で可とする。
②　IEEE802.1Qに準拠したタグVLAN機能を有していること。
③　IEEE802.3adに準拠したリンクアグリゲーション機能を有していること。
④　RSTPによるループ防止機能を有していること。
⑤　ノンブロッキングを実現できること。
⑥　IEEE802.3at、IEEE802.3afに対応していること。
⑦　１ポートへの最大給電電力が30W以上であること。
⑧　装置全体の給電可能電力が124W以上であること。
⑨　機器に管理IPアドレスを付与し、死活監視を行うこと。
⑩　ポート単位で、同じVLAN内でも他のポートと通信できないように分離可能であること。
⑪　スイッチを経由し利用したアプリケーションの統計情報をグラフィカルに表示可能であること。
⑬　特定のスイッチポートのパケットキャプチャを取得する機能を有すること。
⑭　スイッチの設置箇所、スタックの有無に関わらず、複数のスイッチの複数のポートを一括で設定、管理できること。
⑮　PoEポートから給電されるアクセスポイントに対し、スケジュールを組むことにより指定した時間帯に自動的に給電を停止できる機能を有すること。
⑯　リブートスケジュールが設定できること。
⑰　動作温度は0～45℃、動作湿度は10～90％を保証すること。

９．２．４　L3スイッチ

①　10/100/1000BASE-Tに対応できること。
②　SFP(1G)/SFP+(10G)ポートが４/４以上に対応できること。
③　QSFP+(40G)ポートが２以上であること。
④　ポート数は現行L3スイッチ(Cisco Catalyst3850)のポート数以上であること。
⑤　スイッチ容量は296Gbps以上であること。
⑥　転送レートは180Mbps以上であること。
⑦　MACアドレステーブルが32,000以上であること。
⑧　IEEE802.1Qに準拠したタグ VLAN機能を有していること。

⑨　ポート毎にVLAN設定できること。
⑩　接続速度と通信モードを自動的に設定する機能を有していること。
⑪　ケーブルの種類を自動的に検出する機能を有していること。
⑫　IEEE802.3xに準拠すること。
⑬　EAP透過/BPDU透過機能を有していること。
⑭　パケット転送抑制機能を有していること。
⑮　ストーム抑止機能を有していること。
⑯　ジャンボフレームのサイズは9000bytes以上であること。
⑰　ネットワークループ検出機能を有していること。
⑱　一方向のリンク障害を検出する機能を有していること。
⑲　IEEE802.3ahに準拠していること。
⑳　IEEE802.1agに準拠していること。
㉑　リンクアグリゲーション(LACP対応) 機能を有していること。
㉒　ACL機能を有していること。
㉓　QosのSPQ/WRRを使用できること。
㉔　帯域制限としてLR/CAR/GTSを有してること。
㉕　IEEE802.1x認証、MAC認証、WEB認証の全認証方式をサポートしていること。
㉖　telnet、ssh機能を有していること。
㉗　Syslogを使ったログファイル機能を有していること。
㉘　SNMPエージェント機能（v1/v2c/v3）を有していること。
㉙　標準MIB、Private MIB機能を有していること。
㉚　RMONエージェント機能を有していること。
㉛　IEEE802.3azに準拠していること。
㉜　ネットワーク機器の設定や操作を自動的に実行するための機能（スケジュールタスク）を有していること。
㉝　最大消費電力100W以内であること。
㉞　電源冗長機能を有していること。
㉟　動作温度は0～45℃、動作湿度は10～90％を保証すること。

９．２．５　VPNルータ

①　8×10/100/1000MbpsのLANポート構成であること。
②　転送性能は1Gbps以上であること。
③　IEEE802.1Qに準拠したタグ VLAN機能を有していること。
④　ポート毎にVLAN設定できること。
⑤　行政系LANと通信を行うために複数のルーティングプロトコル（スタティック、RIP、OSPF等）に対応していること。
⑥　リンクアグリゲーション(LACP対応) 機能を有していること。
⑦　行政系ネットワークと教育系ネットワーク間で通信が行われないよう、ACL機能を有していること。

⑧　ループガード機能を有していること。
⑨　ミラーリング機能を有していること。
⑩　IEEE802.1x認証、MAC認証、WEB認証の全認証方式をサポートしていること。
⑪　各園の行政系ネットワークと教育系ネットワークとの通信が論理的に分割して行えるよう、IPsec VPNに対応していること。
⑫　IPv6に対応していること。
⑬　Qos（優先制御）機能を有していること。
⑭　動作温度は0～45℃、動作湿度は10～90％を保証すること。

９．２．６　NAS・NAS用バックアップHDD・NAS用UPS（無停電電源装置）

①　小中学校及び教育センターの総使用容量（約77.2TB）かつ設置拠点内最大使用容量（約1,700GB）を加味し、現行機器同等以上であること。
②　IaaS、パブリッククラウド及びSaaSのクラウドストレージの場合は、ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得していること。

９．２．７　仮想サーバ

①　CPU、メモリ、ストレージ等のリソース要件が新教育ICT環境の運用上、見合った要件であること。
②　高性能ネットワークインターフェイスを備えていること。
③　障害隔離性に優れているなど、十分にセキュリティを強化できていること。
④　ダウンタイムを最小限に抑えるなど、高い水準で可用性及び冗長性を実現できること。
⑤　使用するOS及びソフトウェアが仮想サーバ上で問題なく動作すること。

９．２．８　ストレージ

①　IaaS、パブリッククラウド及びSaaSのクラウドストレージの場合は、ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得していること。
②　オンプレミスのストレージサーバ、またはクラウドストレージ内のフォルダへは、ドラッグ＆ドロップで最大50GBのファイルを移すことが可能であることが望ましい。
③　ユーザ認証基盤に設定されたアクセス権限との連携が取れることが望ましい。
④　ファイルのアップロード時に、自動でウイルスチェックが可能であり、ウイルスを検知した場合は、ファイル所有者への自動通知機能を有すると望ましい。
⑤　レポート機能としてユーザアクティビティ、ユーザの統計情報、フォルダとファイル等を標準で実装していると望ましい。
⑥　オンプレミスのストレージサーバ、またはクラウドストレージへのアクセスログ等の証跡をサービス上に保存し、職員が自身のPCから確認でき、証跡は最大７年間保存可能であることが望ましい。
⑦　フォルダ単位で外部共有を禁止する設定が管理者にて可能であることが望ましい。
⑧　管理者設定では、利用者の権限やテナント全体の設定等が行える設定機能を有することが望ましい。
⑨　アクセス権をもつ複数のフォルダ名/ファイル名/全文検索等、一括してキーワードによる素早いファイル検索が可能であり、検索結果に対して所有者やファイル種類、メタデータ等で絞込が可能であることが望ましい。

⑩　クラウドストレージ提案の場合、導入するクラウドサービスは十分な稼動実績を有し、運用の自動化やサービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われているクラウドサービスであることが望ましい。

⑪　クラウドサービスの契約を終了する場合、クラウドサービス上に保存された発注者のデータについて、クラウドサービス上において復元できないかたちで抹消されることが望ましい。

⑫　クラウドストレージ提案の場合、クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行い、暗号化等に関する技術は、電子政府推奨暗号リストに適合するものが望ましい。

⑬　クラウドストレージ提案の場合、ユーザが自らの意思によりクラウドサービス上で取り扱う情報を確実に削除できることが望ましい。

⑭　クラウドストレージ提案の場合、認証機能のActive Directory又はクラウドサービスにおけるAD機能との連携が可能とし、シングルサインオン（SSO）連携を将来的実現する場合を想定し、SAML2.0による認証が可能なサービスであることが望ましい。

⑮　クラウドストレージ提案の場合、クラウドストレージにファイルを格納した状態で、フォルダ招待及び共有リンクによるファイル共有が可能とし、フォルダ招待においては同一フォルダ内においてもユーザ単位で適切な権限を付与できることが望ましい。

⑯　クラウドストレージ提案の場合、ファイルを暗号化した鍵（DEK）を鍵暗号化（KEK)で管理し、ファイルの転送路に関してもTLSによる暗号化が行われており、鍵暗号化鍵をクラウドサービス上で適切に管理し、第三者による復号を不可とすることが望ましい。

⑰　クラウドストレージ提案の場合、利用ブラウザは、Firefox,Google Chrome,Microsoft Edgeの最新版での利用が可能であることが望ましい。

⑱　クラウドストレージ提案の場合、クラウドサービスの中でバックアップ／レプリケーションがリアルタイムで遠隔地のバックアップサイトに保管され、被災等でメインサイトが使用できなくなった際は、遠隔地のバックアップサイトに切替わり利用継続が可能であることが望ましい。

⑲　メインサイト、バックアップサイトは可用性の観点より複数社のクラウドサービス基盤を利用していることが望ましい。

⑳　クラウドストレージ提案の場合、クラウドストレージにファイルを配置した状態で組織内外の送信者・受信者が双方向で大容量ファイル交換が可能であることが望ましい。

㉑　クラウドストレージ提案の場合、クラウドストレージ上でファイルの共有リンクを発行し、メール・グループチャットに記載することでファイル共有が可能であることが望ましい。

㉒　クラウドストレージ提案の場合、共有リンクを発行する際に、表示のみ又は表示及びダウンロードの選択が可能であることが望ましい。

㉓　クラウドストレージ提案の場合、共有リンクを誰でも参照できるもので発行した場合はパスワードの付与やリンク期限等の設定が可能であることが望ましい。

㉔　クラウドストレージ提案の場合、共有リンクについては発行後の無効化をユーザ自身で行えることが望ましい。ただし、無効化後に最有効化した際にURLが変更となることは問題ない。

㉕　クラウドストレージ提案の場合、クラウドストレージ上のフォルダに対して関係者を招待し、アクセス権を限定したファイル共有が可能な機能を有することが望ましい。

㉖　クラウドストレージ提案の場合、フォルダに対して関係者を招待した際に、指定したフォルダへアクセスするためのURLが記載されたメール通知が可能であることが望ましい。

㉗　クラウドストレージ提案の場合、クラウドストレージのアカウントを有していないユーザにファイルのアップロードを要求することが可能であることが望ましい。

㉘　クラウドストレージ提案の場合、クラウドサービス上に招待した外部関係者を含む受信者の操作内容が確認可能であることが望ましい。

㉙　クラウドストレージ提案の場合、組織内及び外部関係者のアカウントを、管理者が権限の変更及び削除等の操作ができることが望ましい。

㉚　クラウドストレージ提案の場合、エクスプローラからアクセスできることが望ましい。

９．２．９　ファイアウォール

前述の８(７)⑤と同様に校務外部系セグメント、校務内部系セグメント、外部接続用セグメント間のアクセス制御を行う役割を想定をしている。

９．２．10　教職員用端末

（１）　仕様・スペック

教職員用端末に求める仕様・スペックについて以下に示す。ただし、現時点の想定仕様であり、今後の整備全体概要やコスト面の検討の中で変更が生じた場合は、協議のうえ決定する。

①	形状	ノート型PC
②	OS	Windows 11 Pro 64ビット
③	CPU	インテル® Core™ i5プロセッサー13世代以上（AMDの場合は上記と同等以上のCPU性能とする）
④	メモリ	16GB以上
⑤	ストレージ	SSD/256GB以上
⑥	ディスプレイ	13.3型以上 液晶画面 タッチパネル対応
⑦	光学ドライブ	不要
⑧	無線	IEEE802.11a/b/g/n/ac/axに準拠していること
⑨	バッテリー	連続使用10時間以上
⑩	キーボード	JIS標準配列
⑪	インターフェース	USB-Cx2以上 USB-Ax2以上 HDMI RJ45 LAN

（２）　台数

①　2,939台（【別紙６】参照）

②　全て同一の機種・型番であること。

（３）　端末に付随する機器

下記について④を除く端末台数分を想定しておくこと。

・　マウス
・　ACアダプター
・　タッチパネル対応のペン（サードパーティ製可）
・　OAタップ

※　端末設置に足らない場合のみ

（４） 初期設定等の環境構築

後述の９．７または、それ以外の教職員用端末を調達する事業者の作業を想定している。

（５） 端末の修理保証

賃貸借契約を予定しているが、一括購入契約に変更する場合も見込み、以下の仕様に対応できること。

① 調達時に５年間分の端末補償がつくこと。なお、端末補償を含む端末保守の開始時期については、本市と協議のうえ決定する。

② 教職員用端末は原則として５年の利用を想定していることから、追加費用なしで修理（現地修理またはセンドバック）が可能となるよう、修理できる保証とすること。

③ 持ち運び時の落下による故障や不注意による液体こぼし、落雷・停電による破損又は損傷についても、追加費用なしで修理できる保証とすること。また、マウス及びACアダプターについても保証すること。

（６） バッテリー交換

① 全台バッテリー交換（作業含む）に関する費用を含めること。なお、バッテリー蓄電容量60％を切る端末から順次交換すること。

② バッテリー交換については、教職員等の業務に支障が出ない極めて軽微な対応で可能なものであることが望ましい。

９．３ 法令・ガイドライン

本仕様書によるほか、下記の関連法令等に準拠して行うこと。

（１） 順守すべき法令等

① 東大阪市情報セキュリティポリシー

② 東大阪市立学校園情報セキュリティポリシー

③ 東大阪市財務規則

④ 東大阪市個人情報保護条例

⑤ その他の関連法令

（２） 参考にすべきガイドライン等

① 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６年１月版）

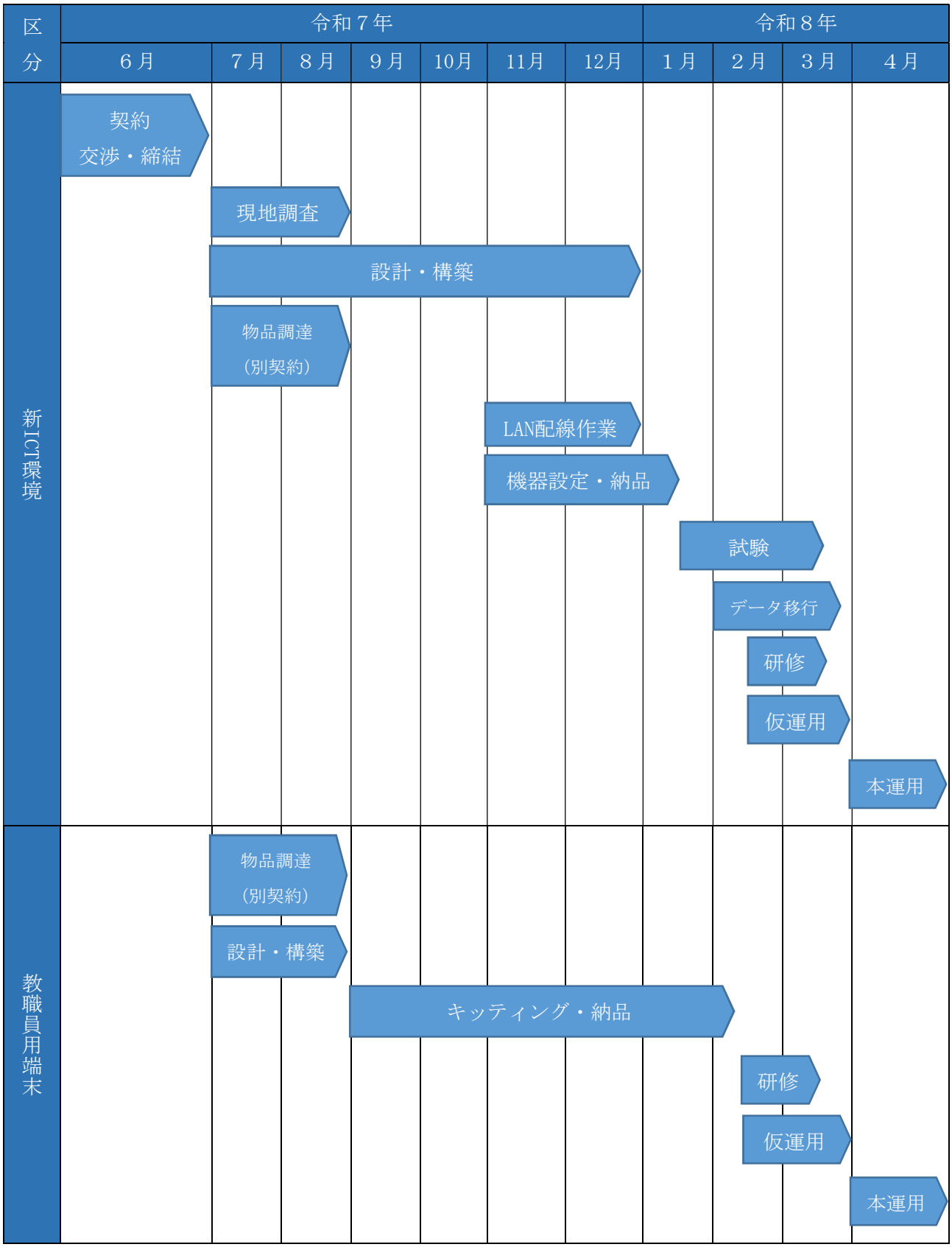
② 教育分野におけるクラウドを中心としたICT環境構築のための調達ガイドブック（令和元年８月追補版）

③ 電気通信設備工事共通仕様書（令和２年３月版）

④ 総務省のIPA（情報処理推進機構）のセキュリティ対策のWebサイト

９．４ スケジュール

本市が想定するスケジュールは、以下のとおりである。その他必要なイベント、イベント毎の時期変更等があれば、対象拠点の運営に配慮し、想定する１日あたりの作業工数を示すとともに、作業候補となる時期を明確にし導入スケジュールを提案すること。なお、各拠点の具体的な作業日は、契約後に各拠点との調整を経て決定する。



９．５　整備・構築作業範囲

①　ネットワーク機器及び教育サーバ群機器等の環境構築（９．６参照）

②　教職員用端末の環境構築（９．７参照）

③　校務のロケーションフリー環境整備（９．８参照）
④　アクセス制御を中心としたゼロトラストセキュリティ対応（９．９参照）
⑤　Microsoft 365 A3(EES)ライセンスの調達及び更新（９.10参照）
⑥　データ移行作業（９.11参照）
⑦　本運用前運用保守（９.12参照）
⑧　運用保守（９.13参照）

９．６　ネットワーク機器及び教育サーバ群機器等の環境構築

以下の各項目の仕様を踏まえ、提案すること。

①　新教育ICT環境における小中高等学校の校内LANは、物理的に校務外部系ネットワークを廃止し、学習系ネットワークに統合する。つまり、教職員等の端末使用も考慮し、継続して児童生徒１人１台の端末を活用し、遠隔教育や動画等を活用した授業スタイルに対応でき、かつ、各校の全児童生徒数以上（最大1,000人）の端末が同時利用中であっても、１学級40人の複数の教室で動画授業等がスムーズに行える通信環境が求められる。前述の10Gbpsの回線を活かすために新たに整備する10Gbps対応のL2スイッチを起点とした通信環境を整備する。学習系ネットワークが整備されていない教室、職員室等にネットワーク機器等を整備し、残りの拠点内LANに関しても、ネットワーク機器を更新し安定した通信環境を構築すること。本庁舎及び幼稚園・こども園以外の各拠点の教職員等及び児童生徒用端末は、各拠点内を抜けて地域イントラネット網からインターネットサービスプロバイダーであるJ:COM経由でインターネットに接続すること。（【別紙３（図２－１、図２－２，図２－３、図２－４、図２－５）】参照）

②　IaaS、パブリッククラウド及びSaaSのクラウドサービスを提案する場合、以下の内容に留意すること。

・　現行のプライベートクラウド型統合型校務支援システム（両備システムズ RYOBI-校支援）及びその他既存の環境と整合が取れるよう、付随するサービス、セキュリティ対策等についても併せて提案すること。
・　IaaS及びパブリッククラウドへの接続回線は提案する構成の中に含めること。また、接続回線費用は、本事業の費用に含めること。なお、既存回線及び提案回線も含めて、協議のうえ、決定する。
・　従量課金型ではなく、毎月定額払いであること。
・　IaaS上に配置するシステムに合わせて、必要なリソース（CPU、メモリ、ディスク等）を十分に配分することができること。また、リソースの枯渇が予見された場合には容易に拡張ができること。（大規模なシステム改修等を除き、拡張に伴う費用は原則保守対応に含むこと。）
・　データセンターは国内に置かれていること。
・　データセンターはUPS装置を備え、冗長構成であること。
・　国内法が適応されること。

９．６．１　L2スイッチ調達

本事業で調達することから、以下の各項目の仕様を踏まえ、提案すること。

①　1000BASE-T/2.5GBASE-T/5GBASE-T/10GBASE-Tに対応できること。
②　SFP+(10G)以上に対応できること。

③　ポート数は現行L2スイッチ（Cisco Catalyst2960-8）のポート数以上であること。
④　スイッチ容量は160Gbps以上であること。
⑤　転送レートは119Mpps以上であること。
⑥　MACアドレステーブルが8,000以上であること。
⑦　IEEE802.1Qに準拠したタグVLAN機能を有していること。
⑧　ポート毎にVLAN設定できること。
⑨　接続速度と通信モードを自動的に設定する機能を有していること。
⑩　ケーブルの種類を自動的に検出する機能を有していること。
⑪　IEEE802.3xに準拠すること。
⑫　EAP透過/BPDU透過機能を有していること。
⑬　パケット転送抑制機能を有していること。
⑭　ストーム抑止機能を有していること。
⑮　ジャンボフレームのサイズは9000bytes以上であること。
⑯　ネットワークループ検出機能を有していること。
⑰　一方向のリンク障害を検出する機能を有していること。
⑱　IEEE802.3ahに準拠していること。
⑲　IEEE802.1agに準拠していること。
⑳　リンクアグリゲーション(LACP対応）機能を有していること。
㉑　ACL機能を有していること。
㉒　IEEE802.1x認証、MAC認証、WEB認証の全認証方式をサポートしていること。
㉓　telnet、ssh機能を有していること。
㉔　ブラウザを使ったWEBコンソール機能を有していること。
㉕　Syslogを使ったログファイル機能を有していること。
㉖　SNMPエージェント機能（v1/v2c/v3）を有していること。
㉗　標準MIB、Private MIB機能を有していること。
㉘　RMONエージェント機能を有していること。
㉙　IEEE802.3azに準拠していること。
㉚　ネットワーク機器の設定や操作を自動的に実行するための機能（スケジュールタスク）を有していること。
㉛　最大消費電力100W以内であること。
㉜　電源冗長機能を有していること。
㉝　動作温度は0～45℃、動作湿度は10～90％を保証すること。

９．６．２　LAN配線作業

以下の各項目の仕様を踏まえ、増設機器（【別紙４】参照）環境まわりの配線を既存のレイアウトにしたがって実施することとするが、最終的には本市と協議のうえ決定し、遅延のない快適な通信を行えるようにすること。

（１）　ケーブル仕様

①　新設する全ての配線は、原則Cat6A に対応したケーブルを敷設すること。なお、幼稚園・こ

ども園のVPNルータとアクセスポイントの間についてはCat5eでも可とする。

② 教育センター内の大研修室（１－１、１－２）においては、Cat5eからCat6Aに敷設替えすること。

③ Cat6A配線については、Cat6A対応のケーブル及びコネクタを使用し作成すること。

④ 全ての配線の敷設後の試験は校正証明書付きの機器で行うこと。

（２） 配線箇所

① 【別紙３（図３）】で各教室内の天井面又は壁面まで配線を実施すること。なお、指定箇所までのケーブルルートについては原則、新設敷設ケーブルルートとすること。

② 敷設ケーブルの両端に、接続先等をラベリングすること。

③ シールド付きケーブル（STP）を利用する場合は、LAN配線それ自体から接地（アース）を十分に行うなど、特性に応じた適切な対応を行うことが望ましい。

④ 事前に現地調査を行うこと。現地調査の結果、必要な場合は以下の内容も実施すること。

・ 配線を行う際、既設のモール管等の相乗りはせず、実施すること。

・ 配線を行う際、区画や壁の貫通作業がある場合は対応すること。

・ 天井内隠ぺい、二重床及びピット内配線は、ころがし配線とするが、露出する場合はスチール管やPF管、モール等で保護すること。

・ 点検口が追加で必要な場合は設置すること。

９．６．３ 電源敷設等作業

（１） 本庁舎サーバ室

① 100V 20A、100V 30A、200V 20A及び200V 30Aの空き回路をそれぞれ複数回路準備しているが、計６回路の範囲内でサーバ等を設置すること。なお、利用する回路については、本市と協議のうえ決定する。

② 本庁舎サーバ室内のサーバラックに別調達のサーバ等を収納する台数に限りがあるため、新規にサーバラックが必要となる場合は、ラック、部品（ねじや棚板等）を受託者にて用意のうえ、設置にかかる工事等及び分電盤からラック設置場所までの電源配線作業の費用を負担し実施すること。

（２） 本庁舎サーバ室以外の拠点

① PoEスイッチングハブを設置する際に電源敷設作業が必要な場合は電源敷設作業を行うこと。

② 電源盤等の増設や改修が必要な場合は別途本市と協議すること。必要な場合は電源タップも受託者にて準備すること。

９．６．４ 機器設定設置作業

① 本事業の提案に応じて発生する新たなVLAN設定については、本市と協議のうえ受託者にて基本実施すること。できない設定がある場合は、その理由を本市に説明すること。

② 必要とあらば新たにIPアドレス体系を構築すること。

③ 小中高等学校においては、校内の通信（現行の学習系無線LANとの電波干渉等）を考慮し設計を実施すること。

④ 設計した内容は文書化し、本市に承認を得ること。

⑤ 設計した内容に従って、機器を設定及び設置し、動作確認を行うこと。なお、教育センターの

作業を最優先にすること。

⑥　各拠点の既設機器等との区分が明確となるよう、ラベル表示等を行うこと。

⑦　アクセスポイント設定設置について、以下の内容を留意すること。

・　アクセスポイント設定時のセキュリティ対策については総務省、IPA（情報処理推進機構）のセキュリティ対策Webサイトを参考とすること。

・　設置場所は、事前に協議し、合意した方針に従い、壁面上部や天井部など、児童生徒の手が届かない場所にするなど配慮すること。

・　設置に際しては、事前に設置可能場所を確認し決定するなど、適切に行うこと。

・　設置に当たり、機器の転倒・転落の防止策やケーブルの抜け防止等を考慮した対応を行うこと。

・　小中高等学校においては、設置後の接続先は既設のHUB-BOX収容のPoEスイッチングハブ（Cisco MS120-24P）を想定している。

・　増設するアクセスポイントのSSIDは、各拠点での想定される運用及び学習系の既設アクセスポイント（Cisco Meraki MR-36）のSSIDを考慮し、本市と協議のうえ作成すること。

・　アクセスポイントを各拠点内に設置する際に想定される無線干渉について、必要とあらば学習系の既設アクセスポイント（Cisco Meraki MR-36）の周波数帯域幅（チャネル幅）等を再設計すること。

・　学習系の既設アクセスポイント（Cisco Meraki MR-36）のフリーWi-Fiを発砲できるよう設定すること。設定する拠点対象については協議のうえ決定する。

⑧　増設するPoEスイッチングハブは HUBボックスを設置し、その中に収容すること。

⑨　小中高等学校においては、学習系のPoEスイッチングハブのうちコアスイッチ（集約スイッチ）（Cisco SystemsMS120-24P）を別調達する1000BASE-T/2.5GBASE-T/5GBASE-T/10GBASE-Tに対応のPoEスイッチングハブに交換し設置・設定すること。交換後取り外したPoEスイッチング（Cisco SystemsMS120-24P）を現在職員室に設置しているPoEスイッチングハブ（Panasonic GS-ASW8TPoE(PN25087B5)と交換し設置・設定すること。構築期間中に実施できない場合は、令和８年４月以降、運用保守開始後、早急に実施すること。

⑩　各拠点に整備している行政系ネットワークを継続利用できるように、小中高等学校のL2スイッチ、幼稚園・こども園のVPNルータ等の更新対象機器の設定を行うこと。

９．６．５　仮想サーバ環境構築作業

以下の各項目の仕様を踏まえ、提案すること。

①　【別紙５】を参考にし、本庁舎サーバ室にパブリッククラウド型出退勤システム（アマノTimePro-VG）の勤怠データ及びAI型教材（COMPASS Qubena）の児童生徒データをプライベートクラウド型統合型校務支援システム（両備システムズ RYOBI-校支援）へ受け渡すための中継サーバは最低限設置することを考慮したうえで構築すること。

②　仮想化ハイパーバイザーのバージョンについて、本事業の契約期間とサポート終了期限に留意すること。

９．６．６　ストレージ・フォルダ環境構築作業

以下の各項目の仕様を踏まえ、提案すること。

① バックアップについて、別のリージョンに製品等を設けるなど、運用上切れ目のない万全な対策を講じるよう構築すること。
② 特定の目的に応じて、関係者のみアクセス可能な共有フォルダ環境を構築すること。フォルダの詳細については、協議のうえ決定し、設定すること。
③ 他拠点の教職員等とデータの受け渡しを行う際、一時的に経由する受渡用フォルダ環境を構築すること。フォルダの詳細については、協議のうえ決定し、設定すること。
④ 新教育ICT環境には、各拠点管理のフォルダを作成するとともに、アクセス制御を行うこと。
⑤ 各教職員等は所属する拠点のフォルダのみにアクセスできるよう権限設定を行うこと。また、職種や職責による権限設定を行うこと。（例）校長フォルダ、事務職員フォルダ等）
⑥ 複数校勤務職員については、原則として、勤務校全てにおいてそれぞれの立場でアクセスが可能とすること。ただし、勤務形態の状況により条件が異なるため、複数校勤務職員の権限設定については協議のうえ決定する。

９．６．７　ファイアウォール設定作業

提案する新ICT環境において、前述の８(７)⑤と同様に校務外部系セグメント、校務内部系セグメント、外部接続用セグメント間のアクセス制御を行う必要がある場合は、設定すること。必要な役割でない場合は、代替の提案を行うこと。

９．６．８　Active Directory等による一元管理環境構築作業

前述の８(７)⑧のとおり、Active Directoryにて、ユーザ、グループ、ファイルへのアクセス権限等を一元管理している。新ICT環境におけるActive Directory、Microsoft EntraID等での一元管理環境を提案し構築すること。

９．６．９　不正端末遮断環境構築作業

前述の８(７)⑨のとおり、不正端末遮断センサー（PFU iNetSec SF 510センサー）にて、教育ネットワークへの未許可端末の接続を防止している。新ICT環境において、教育ネットワークへの未許可端末の接続を防止できる環境を提案し構築すること。

９．６．10　試験

① 事前に試験計画書を作成し、本市に承認を得ること。
②【別紙１】の各拠点において、いずれも本仕様を満たしていることを確認し、結果を書面で市に報告すること。
③ 敷設・設置作業完了後、作業対象の各拠点の各部屋等において無線の通信状況が良好であるかを測定機器等を用いて測定・確認し、試験成績書を提出すること。
④ アクセスポイントを設置した各拠点の各部屋内の2.4GHz及び５GHz帯の電波強度を計り(アクセスポイントの管理マネージャなどを利用して電波強度を測定することも可とする)、測定結果を書面にて提出すること。測定箇所、測定手法、報告書面の提案を求める。なお、拠点内LANを構築後、通信状況の確認のため、各施設内の６か所程度の本市が指定する教室のサイトサーベイ調査を受託者の負担で実施すること。
⑤ 運用開始後、上記の測定結果を満たさないことが判明した場合、受託者の責任において設置場所の変更を行うこと。それにかかる費用は受託者の負担とする。
⑥ 長さ、ワイヤーマップ、挿入損失（減衰)、近端漏話（NEXT)、DCループ抵抗及び反射減衰量

（リターン・ロス）等の規格に適合しているかどうかの合否判定とその結果のレポートが提出可能な機器を利用すること。またフロア配線盤から通信アウトレットまでのリンク性能は、要求されるクラスにおけるJIS X 5150（構内情報配線システム）のパーマネントリンクの性能を満足するものとする。

９．６．11　その他

（１）　児童生徒用端末設定

別調達予定の次期児童生徒用端末（Chromebook）33,448台を新教育ICT環境に参加させること。詳細については、協議のうえ決定する。

（２）　既設の電子黒板等の設定

①　既設の電子黒板等を小中学校内LAN更新後のネットワークに参加させ、別調達の児童生徒用端末（Chromebook）からの無線投影ができるよう設定すること。また、各校で教室間で移動することも考慮し、設定すること。

②　布施小学校のみネットワーク参加ができない大型提示装置を11台設置しているため、無線投影に必要な機器をネットワーク参加ができない大型提示装置台数分整備すること。（【別紙４】参照）

③　学校園等において、電子黒板等を運用保守契約期間内に更新した場合も、調達した電子黒板等に対して上記設定を行うこと。

（３）　中学校PC教室用教職員及び生徒用端末の継続利用

中学校PC教室用教職員（25台のWindowsPC（Windows10 Enterprise 2019 LTSC））及び生徒用端末（1150台のWindowsタブレット（Windows10 Enterprise 2019 LTSC））を継続利用することから、以下の仕様を踏まえつつ、提案すること。なお、端末保守、環境復元（future瞬快　V3　Basic Grade）及びエンドポイントセキュリティ（AppGuard）のラインセンスについては、本市にて別途費用で調達する。

①　【別紙４】のとおり、中学校PC教室に増設するアクセスポイントに中学校PC教室用教職員及び生徒用端末を接続する設定をすること。

②　インターネット利用の際は、本庁舎に設定しているURLフィルタリング機能を有するファイアウォール（PA-3260）を経由すること。

（４）　アクセスポイント移設

孔舎衙小学校の１号館解体工事に伴う別号館教室へのアクセスポイントの移設・設定及び一部撤去を行うこと。なお、移設の際に配線工事が伴う。（参考図書の【孔舎衙小学校_LAN配線図】参照。）

９．７　教職員用端末の環境構築

教職員用端末を調達する事業者と協力し、教職員用端末の初期設定等の環境構築を実施すること。ただし、初期設定等の役割分担については、関係者での協議のうえ、決定する。以下の各項目の仕様を踏まえ、提案すること。

①　協議のうえ決定したIP アドレス及びコンピュータ名等のネットワーク設定を設定しドメイン参加させること。

②　本市指定の各種アプリ等のショートカットアイコンをデスクトップに設置すること。

③　以下の各ソフトウェアをインストール、環境設定及びライセンス認証を行い、端末の利用期

間中は継続的に利用できること。なお、ライセンスについは、受託者負担のもと調達すること。また、本事業で整備する教職員端末で動作可能であることを事前に確認すること。

- 一太郎Pro 5
  指定の小中学校教職員用端末580台分
- JUST PDF 最新版
  全台分
- Fuji Xerox DocuWorks
  小中高等学校教頭用端末80台分
- xSync Classroom
  小学校用教職員端末等全台分
- 写真編集及び作成制作ソフト
  中学校用教職員端末全台
  ※　現在は、エルモ株式会社のデイジーピックス
- LoiloScope 2
  幼稚園・こども園教職員用端末全台分
- Sound it! 8 Basic
  幼稚園・こども園教職員用端末全台分
- 広島教科書販売の事例で学ぶNetモラル クラウド版（ASP型）
  小中高等学校75校分（義務教育学校は１校として算出）
- Let's Try! 1 及び Let's Try! 2（文部科学省が提供する小学校3年生及び4年生向けの英語教材）
  小中学校用教職員端末等全台分及び教育委員会用端末１台
- Dream（大阪府公立小学校英語学習6カ年プログラムの一環として提供されている教材）
  小学校用教職員端末等全台分及び教育委員会用端末１台

④　本市と協議のうえ、無料ソフトウェアをイントールすること。また、図書室用端末にインストールするWin書庫のデータも現行図書室用端末から移行すること。

⑤　現行教職員端末にインストールされているソフトウェア（デジタル教科書等）については、事前に協議の上、初期設定の際のインストール作業に含めることが望ましい。

⑥　ユーザが自由にソフトウェア等をインストールできないよう制御できること。

⑦　Windows及びOffice等ソフトウェアのライセンス認証を行うこと。

⑧　ソフトウェアはすべて最新のセキュリティパッチの適応を行うこと。

⑨　外字対応について、昨今の国・他自治体の動向、受託者の見解を踏まえ提案すること。ただし、提案内容をもとに本市と協議のうえ、最終的に本市が提供する外字ファイルを適用する場合は、設定すること。

⑩　その他当初設定が必要な項目が生じた場合には、別途協議のうえ設定作業を行うこと。

⑪　ドライバー等のインストール設定及び環境設定を行うこと。

⑫　本市と協議のうえ、提案構成に必要な設定を行い、納品前に動作確認すること。

⑬　導入機器等には、導入年月日・管理番号のラベルシールを貼付すること。

⑭　無線LAN接続設定を行うこと。

⑮　各拠点に設置している既設プリンタから印刷が行えるよう設定すること。

⑯　小中学校に設置している複合機（KONICA MINOLTA 650iSeriesPCL）から教職員用端末へのスキャンデータの送信方法を提案すること。

⑰　各拠点に設置している電子黒板等に投影できるよう設定すること。

⑱　端末を設置すること。設置に際しては既設OAタップより電源を確保する。必要に応じてOAタップを新たに設置すること。

９．８　校務のロケーションフリー環境整備

東大阪市立学校園情報セキュリティポリシーにて、学校園長の許可を得た場合のみ、教職員用端末の持ち出しを認めていることから、持ち出した際に学校園勤務と同様の環境を構築し、持ち出しの運用に合わせた柔軟な制御方法を必要とする。

セキュリティを担保した校務のロケーションフリーを実現できる機器構成 、認証手法、その他の制御方法等について、以下の仕様を満たすよう提案すること。

①　本事業で整備する教職員用端末は勤務校以外の本市の別拠点及び拠点外でもWi-Fiに接続することができること。なお、持ち出せる端末を限定する提案も可とする。

②　勤務校以外の本市の別拠点及び拠点外のWi-Fi接続により、学校内で利用可能な校務支援システム、各サービス及びファイルへのアクセスができること。

③　ユーザの権限に応じて、どのシステムにアクセスをさせるのか制御が行えること。

④　９．９．２（ユーザ認証基盤）とSAML認証が行えること。

⑤　学校園長より許可（承認）を受けた者のみが持ち出しによる外部からの接続が可能となるよう仕組みを有することが望ましい。

⑥　拠点外から利用する場合においても、原則として拠点内と同等のセキュリティや端末の操作方法が維持できること。ただし、拠点外から利用する際の初期設定作業や、セキュリティ確保のための作業の発生はこの限りではない。

⑦　持ち出し利用時における拠点外に存在するネットワークハードディスクへの書き込み、USBメモリ等外部記憶装置への書き込み、Bluetooth でのデータ転送、印刷機器からの出力等のデータ持ち出しができない仕組みを有すること。

⑧　端末にエージェントをインストールすることで、IPsec及びSSL-VPNの両方のVPN接続方式に対応し、すべてのIP通信の可視化と制御が可能であること。また、接続されたネットワーク環境に応じて適切なVPN接続方式が自動選択されること。

⑨　80/443ポートを利用したWebアプリケーション以外の動作を保証するため、各サービス及びファイルへのアクセスに対してもVPN方式を利用できること。

９．９　アクセス制御を中心としたゼロトラストセキュリティ対応

【別紙３（図２－１）】の新教育ICT環境において、提案するネットワーク機器等及びサーバ等や校務のロケーションフリー環境整備を進めていく上で、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６年１月版）に則ったゼロトラストセキュリティ対策ソリューションの導入が必要である。

以下の各項目の仕様を踏まえ、最適な構成を提案すること。なお、校務のロケーションフリー環境

における端末利用時においても同じ基準のセキュリティを満たすこと。

９．９．１　多要素認証の整備

多要素認証とは、認証の３要素である「知識情報」、「所持情報」、「生体情報」のうち、２つ以上を組み合わせて認証する機能を指す。

端末へのログイン時や各種システムやアプリケーション利用時など適切なタイミングで、パスワード以外の顔認証の要素に基づき接続でき、セキュリティ強化できるような仕組みを以下の各項目も考慮し提案すること。

① ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているサービスを利用すること。

② 顔認証の仕組みを導入することで、ID／パスワード等の情報が漏洩した場合でも不正アクセスを防ぐことができる仕組みであること。

③ 常時認証機能を有していること。

④ 顔認証の要素の登録は、本市と協議のうえ、受託者にて極力実施すること。

⑤ 会計年度任用職員等のような複数人で１台の端末を利用することに対応していること。

⑥ 複数の教職員用端末でも再登録なしに顔認証できる仕組みを有すること。

⑦ 登録・削除等の認証データの管理を一元的に行えること。

⑧ 認証要素に基づき、以下の各種システムやアプリケーションにアクセスできる、もしくは令和８年４月の本運用までにアクセスできていると望ましい。なお、各種システムやアプリケーションへのアクセス方法として、シングルサインオン(SSO)も考えられるが、提案構成をもとに教職員の業務効率を上げる仕組みを協議のうえ決定する。

- Microsoft 365
- Google Workspace
- 統合型校務支援システム（両備システムズ RYOBI-校支援）
- 保護者等連絡管理システム（両備システムズ RYOBI-校支援 SmartSchoolWeb）
- 出退勤システム（アマノ TimePro-VG）
- デジタル採点システム（大日本印刷 リアテンダント）
- 学習支援プラットフォーム（COMPASS Qubenaマネージャー）
- 授業支援ツール（ロイロ ロイロノート・スクール）
  ※　令和８年度４月以降に別授業支援ツールに変更する可能性あり。
- その他アプリケーション

９．９．２　ユーザ認証基盤の整備

ユーザ認証基盤とは、ネットワーク上（クラウドサービスを含む）のリソースに対するアクセス権限を管理するとともに、アクセスしようとするユーザのID及び認証情報を一元管理し、認証を行う機能を指す。

以下の各項目の仕様を踏まえ、教職員の利便性にも考慮したシングルサインオン(SSO)も含め提案すること。

① ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているサービスを利用すること。

② 教職員のアカウント情報を管理できること（児童生徒のアカウント情報も管理できると望ましい）。

③ 教職員用端末情報を管理できること（児童生徒用端末情報を管理できると望ましい）。

④ ID管理機能、認証機能、シングルサインオン機能、Windowsサインイン認証機能、証明書管理機能、セキュアブラウザ機能を統合的に提供できることが望ましい。

⑤ 本業務で導入するクラウドサービス及びIaaS及びパブリッククラウド上のサービス（以下、「クラウドサービス等」という）の認証情報の一元管理ができることが望ましい。

⑥ 以下の各種システム及びアプリケーションの認証情報を極力管理・連携できることが望ましい。ただし、システム間の連携情報内容によっては、現行の連携を採用することも念頭に置き、協議のうえ、連携構成を決定する。また、システム及びアプリケーションが変更・追加された場合、別途費用がかからず、同様に管理・連携できることが望ましい。なお、国の標準化システムの動向が生じる変更等にも可能な範囲で柔軟に対応すること。

ア 教職員用

（ア） Microsoft 365

（イ） Google Workspace

（ウ） 統合型校務支援システム（両備システムズ RYOBI-校支援）

※ (エ)、(オ)と連携

（エ） 保護者等連絡管理システム（両備システムズ RYOBI-校支援 SmartSchoolWeb）

※ (ウ)と連携

（オ） 出退勤システム（アマノ TimePro-VG）

※ (ウ)と連携

（カ） デジタル採点システム（大日本印刷 リアテンダント）

※ (ア)でSSO

（キ） 学習支援プラットフォーム（COMPASS Qubenaマネージャー）

（ク） 授業支援ツール（ロイロ ロイロノート・スクール）

※ 令和８年度４月以降に別授業支援ツールに変更する可能性あり。

（ケ） デジタル教科書ビューア①（Lentrance Lentrance）

（コ） デジタル教科書ビューア②（光村図書 まなビューア）

（サ） デジタル教科書ビューア③（BPS 超教科書）

（シ） デジタル教科書ビューア④（みらいスクール みらいスクール）

イ 児童生徒用

（ア） Microsoft 365

（イ） Google Workspace

（ウ） ひがしおおさか電子図書館

（エ） AI型教材ドリル（COMPASS Qubena）

※ (ア)でSSO

（オ） 授業支援ツール（ロイロノート・スクール）

※ (ア)でSSO

（カ） 児童生徒用連絡ツール（両備システムズ RYOBI-校支援 学習帳）

※ ア(ウ)と連携

⑦ 本サービスと拠点外装置（ルータ等）との連携によりWi-Fi/VPNのRADIUS認証サービスを提供することが望ましい。

⑧ 年度替わりなどの異動情報の反映がわかりやすく容易であること。

⑨ クラウドサービス等のアクセス制御に、認証基盤のID情報が利用できることが望ましい。

⑩ ９．９．１との連携が取れることが望ましい。

⑪ 必要に応じて、提案した場合のクラウドストレージ、コンテンツ保護等と連携が取れることが望ましい。

⑫ ⑥の各種システム及びアプリケーションに対してシングルサインオン(SSO)でアクセスできることが望ましい。ただし、提案する多要素認証によるアクセス方法も考慮し、協議のうえ、アクセス方法を決定する。

⑬ 各種システム及びアプリケーション代理入力方式によるシングルサインオンが可能であると望ましい。

⑭ 代理入力方式によるシングルサインオンでは、フォームベース認証、基本認証、アプリケーションの認証に対応することが望ましい。

⑮ SAML連携及び代理入力によるシングルサインオンはSaaSやオンプレミス環境を問わず対応できること。

⑯ 認証後に取り扱う情報資産の重要度、教職員の利用場所や状況（各拠点ネットワーク内部か外部か、就業日又は時間等）に応じて、多要素認証の要否、生体情報か所持情報かの選択、など柔軟な運用ができるリスクベース認証機能を有することが望ましい。

９．９．３ エンドポイントセキュリティの整備

エンドポイントセキュリティとは、ネットワークに接続された端末やサーバをマルウェア等の脅威から防御するとともに、端末の挙動を常時記録・分析することによって、ウィルスやランサムウェアなどの脅威発生を検出し、迅速かつ詳細に調査・復旧等を行う機能を指す。

以下の各項目の仕様を踏まえ、提案すること。

① ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているサービスを利用すること。

② 端末内の他のアプリケーションと競合しない仕組みを準備すること。

③ 単一エージェントでEPP/NGEPP/EDRの全ての機能を同時に利用できること。

④ 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が行えること。

⑤ 登録済みのシグネチャでは検知できないような、未知のマルウェアも検知できること。

⑥ ファイルレスのマルウェアを防御する機能を有すること。

⑦ ランサムウェアを防御する機能を有すること。

⑧ 耐タンパー性（例としてEDRSilencerなどのツールへの耐性）を持ち攻撃者がエージェ/センサーを無効化する攻撃に対応できると望ましい。

⑨ インターネット上のサイトから端末に配布するシグネチャを取得し、調達予定の端末に対して可能な限り負担を与えない仕組みで配信及び適用が行えること。

⑩　リアルタイムスキャンやスケジュールスキャンが行えること。
⑪　端末の動作ログ（ネットワーク接続ログ、コマンド操作ログ、プロセス実行ログなどの各種ログ）を常時取得・監視して分析し、脅威を検出できること。
⑫　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）に基づき検出が行えること。
⑬　端末の動作ログについて、一定期間分を保管可能であること。
⑭　イベントログをメールで通知できること。
⑮　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）について定義が行えること。
⑯　脅威を検出した際に、脅威が発生した教職員用端末、侵入経路、被害の状況などを分析・特定できること。また、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。
⑰　脅威を検知した場合には、その根本原因、感染した端末の全台の特定、影響範囲の関係、時系列での不正なふるまいの状況を管理コンソールで把握できること。
⑱　利用者側に表示されるポップアップやエージェントの管理画面などの言語は日本語であること。
⑲　EDR製品の管理コンソールとの通信は許可されている状態で隔離された端末の脅威分析などが完了し、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。
⑳　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。
㉑　マルウェアを受けた被害範囲の特定が可能であること。
㉒　マルウェアを検知したファイルの情報、収集した検体の情報、復旧したファイルの情報等をログで記録し、後述のセキュリティオペレーションセンター（SOC）に連携できること。
㉓　エンドポイントセキュリティとSOCは同一メーカーが提供であると望ましい。
㉔　エージェントが収集した情報を任意のキーワードで検索できること。また、検索条件に合致する端末、プロセス及びファイルなどが特定できること。
㉕　検索した結果をCSVにて出力できること。また日本語データの出力にも対応していること。
㉖　脆弱性のあるアプリケーションを検知する機能を有すること。
㉗　グループごとに任意のポリシー（ブロック設定、自動更新等）が適用できること。
㉘　クライアントOSだけではなく、サーバOSにも対応していること。

９．９．４　統合セキュリティ対策

統合セキュリティ対策とは、拠点内外から新教育ICT環境下のネットワークを安全かつ快適に利用するため、ネットワークやセキュリティに関する様々なサービスを提供する機能を指す。各機能に対して、ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているクラウドサービスを利用し、以下の各項目の仕様を踏まえ、提案すること。

（１）　SSE（Security Service Edge）

①　どのようなアプリケーションが存在していても対応出来るようにするため、リモートアクセスにはZTNA（Zero Trust Network Access）機能とVPN機能双方をクラウド型で備えていること。

② SSE機能とアプリケーションが存在する拠点の間はIPsec接続を行い、以下の何れかの方式でSSEより拠点内のルーティング情報を認識できるようにすること。

- Static Routing
- BGP

③ 端末健全性確認機能(ポスチャー)によるアクセスブロック時にユーザへ理由を提示できること。

④ VPN接続時に端末健全性確認機能(ポスチャー)を行い、以下の観点を用いて脆弱な端末からの接続を制限できることが望ましい。

- 古いOSやブラウザの利用状況
- アンチマルウェア製品の利用状況
- クライアントファイアウォールの利用状況
- ディスク暗号化状況
- 特定ファイルの存在状況
- 特定レジストリの存在状況(Windowsのみ)
- 証明書

⑤ 利用者が利用時に意識して操作することなく、宛先に応じてZTNAとVPNaaSを自動的に判断して切り替えが可能であること。

⑥ 内部リソースへのアクセスに際して、CIDR Block(例:192.168.1.0/24)やIPアドレスレンジ(例:192.168.0.0-192.168.0.10)で指定してポリシーを書けること。

⑦ 内部リソースへのアクセスに際して、ポート番号をレンジ(例:TCP/1024-6500)で指定してポリシーを書けること。

⑧ VPN接続のプロファイルを複数作成できること。

⑨ DNSセキュリティですべての全ポートとプロトコルについて脅威の有無を判定し、フィルタリングポリシーのブラックリストで設定されたドメインへの通信を阻止すること。

⑩ EntraIDと連携してSAML認証できること。

⑪ 他認証基盤と連携してSAML認証できること。

⑫ Web通信において全ての宛先をチェックするフルプロキシ機能を提供すること（除外設定した宛先を除く)。

⑬ 透過型プロキシ及び明示的プロキシに対応すること。

⑭ ファイルタイプによってダウンロード可否の制御ができること。

⑮ ファイルのダウンロード時にアンチウイルスやファイルのレピュテーションチェックができること。また、マルウェアの可能性のあるファイルが発見された場合、クラウド上のサンドボックスでの検証にファイルを受け渡して動作検証が可能なこと。

⑯ ファイアウォールポリシーを一括で管理するためにクラウド型のファイアウォール機能を有すること。

⑰ IPアドレス、ポート番号、プロトコル、アプリケーションによる通信制御が可能なL7ファイアウォール機能を有すること。

⑱ クラウドアプリケーションの利用状況を可視化できること(Shadow ITの可視化)。

⑲　可視化したクラウドアプリケーションのリスク値を確認できること。

⑳　情報漏洩対策として、内部から外部へ送られる通信を監視し、組織にとって重要な情報が外部へ送られたことを検知すると、それをブロックする機能を有すること。

㉑　重要情報を定義するためにキーワードリストや正規表現で独自の検出ルールを作成できること。

㉒　特定の利用者に対して、アクセス制御を除外できること。

㉓　クラウドアプリケーションへの通信経路に異常があった場合、以下の観点からどこに問題があるのかを示唆する機能を有すること。また、通信経路問題の把握をSSEを通らない端末においても可視化できること。

・　端末のCPUやメモリの使用率
・　端末のWi-Fi接続状況
・　端末とSSE間の通信状況
・　SSEと外部SaaS間の通信状況

㉔　複数のIPsecトンネルに対応すること。

㉕　管理ポータルアクセス時にユーザを認証する機能を有すること。

㉖　インターネットアクセスやリモートアクセス時のユーザー認証においてIdPとSAML連携し多要素認証を行う機能を有すること。

㉗　リソース消費やアプリケーション競合を回避する観点から、インターネットアクセス、リモートアクセス、DEMに利用するエージェントが単一のソフトウェアに統合されていること。

㉘　エージェントを自動更新する機能を実装していること。

㉙　エージェントはユーザが容易にサービス停止できないこと。

㉚　エージェントはWindowsログイン前から自動的にSSE基盤に対してVPN接続する機能を有すること。

㉛　日本語のWebGUIを提供すること。

㉜　保守窓口の日本の電話番号がWeb公開されていること。

㉝　30日分の通信ログを保管できること。外部ストレージ、或いはログサーバと連携することで、30日以上保管できること。

㉞　レポート機能や分析機能を有すること。

㉟　ログのSIEM連携機能を有すること。

㊱　稼働率は実績ベースで99.999%以上であること。

㊲　サービス基盤は24時間365日利用可能であること、計画停止の際には事前通知があること。

㊳　サービスにおける障害時及びメンテナンス時には他データセンター（ロケーション）に自動的に切り替わることで継続利用できること。

㊴　国内に2か所以上のデータセンターを有すること。

（２）　IDS/IPS機能

①　VPN通信に対してIPS機能を適用して内部への攻撃を防げること。

②　端末が信頼出来るネットワークの内部にいるかを監視し、設定に応じてVPN接続を自動的に接続・切断する機能を有すること。

（３） 通信経路の暗号化

① 利用場所に関わらず、端末が常時VPN接続を行う構成がとれること。

② セキュアなリモートアクセスであるZTNA機能を有すること。

③ ZTNA接続時に端末健全性確認機能(ポスチャー)を行い、以下の観点を用いて脆弱な端末からの接続を制限できること。

- 古いOSの利用状況
- アンチマルウェア製品の利用状況
- クライアントファイアウォールの利用状況
- ディスク暗号化状況
- システムパスワードの複雑性

④ ZTNA通信に対してIPS機能を適用して内部への攻撃を防げること。

⑤ リバースプロキシ型のクラウド型リモートアクセス機能により、HTTP/HTTPSをアクセスに使用するWebアプリケーションについては端末にエージェントをインストールせずとも外部から利用できるClientless ZTNA機能を有すること。

⑥ Clientless ZTNAでは、特殊なアプリを使用せず普段使用しているブラウザ(Microsoft Edge、Google Chrome等)でリモートアクセスができること。

⑦ Clientless ZTNAでは、特殊なアプリを使用せず普段使用しているブラウザ(Microsoft Edge、Google Chrome等)でRDPやSSH接続を内部アプリに対してできること。

⑧ Clientless ZTNAではSAML認証を使用できること。

⑨ Clientless ZTNAでは接続時の端末健全性確認機能(ポスチャー)により、使用するブラウザの種類によって端末の接続を制限できること。

⑩ IPsec接続された複数の拠点間でSSE機能を介して通信ができること。

⑪ 拠点間通信時にファイアウォール機能を利用できること。

（４） ウェブフィルタリング機能

① URLやカテゴリ、ドメイン名、アプリケーション、宛先リストなどの情報をもとに、ウェブサイトのアクセス可否を制御できること。

② フィルタリングのポリシー（カテゴリ、ホワイトリスト、ブラックリスト、警告用ページ等）の設定が拠点ごとで可能であること。

③ URLフィルタリングにて、レスポンスに対して危険性のあるコードが含まれていないかを確認し、危険性があればアクセスを遮断する機能を有すること。

④ 100以上のカテゴリ制御に対応し、カテゴリ内の情報を随時更新できること。

⑤ 閲覧禁止URLに該当するアクセスを適切にフィルタリングできること。

⑥ フィルタリングによる結果について履歴を取得できること。

⑦ サービスの操作はWeb管理画面で提供され、日本語の表記が行えること。

（５） SSL復号機能

SSLで暗号化されたトラフィックを復号化し、詳細なウェブフィルタリングの制御が行えること。

（６） ファイアウォール機能

① クラウドサービス上でファイアウォール機能を提供する場合も、校内外の利用場所に関わら

ず端末を保護できること。

② レイヤー3、レイヤー4の情報にもとづき通信の監視や制御が行えること。

③ 全てのTCP/UDPポートの通信をアプリケーション識別及びセキュリティポリシーを適用できること。

（7） ログ機能

ア ログ取得

① ログ取得対象端末の電源オン/オフ及びサスペンドの記録が可能であること。

② OSログオン/ログオフ操作の記録が可能であること。

③ OSログオン中に実際に操作した時間の記録が可能であること。

④ アプリケーションの起動と終了の記録が可能であること。

⑤ アプリケーション稼働中に実際にそのアプリケーションを操作した時間の記録が可能であることが望ましい。

⑥ サービスやスタートアップなど、バックグラウンドで起動したアプリケーションの記録が可能であること。

⑦ ファイル操作の記録が可能であること。アプリケーションの種別やバージョンに依存せずに記録可能であること。

⑧ 印刷（プリンター名、ファイル名、ファイルパス、ページ数、印刷アプリケーション名）の記録が可能であること。

⑨ インターネット操作の記録が可能であること。ブラウザの種別やバージョンに依存せず、http及びhttpsの記録が可能であること。

⑩ FTPの記録が可能であると望ましい。

⑪ リモート接続元端末のホスト名及びIPアドレスの記録が可能であること。

⑫ ファイル操作において、ファイル操作の「移動」が記録可能であること。また、ファイル/フォルダのアクセス監査（成功、失敗）が記録可能であること。

イ ログ管理

① 特定の端末を指定して優先的にログを回収できること。

② 各管理者の権限に応じて、ログの閲覧範囲（部門単位）を設定できると望ましい。

③ インターネットアクセス及び内部アクセスについてのログはすべて30日以上保存されること（ログの種類毎に保存期間を設定でき、ログによっては半年以上保存できると望ましい）。

（8） ファイル暗号化

① ファイルを暗号化して保護できること。

② ファイルに秘密度ラベルを適用できること。なお、自動で秘密度ラベルを付けることができると望ましい。

③ 暗号化されたファイルへのアクセスを制御できること。

④ ファイル情報の機密性を視覚的に示すことができると望ましい。

⑤ ファイルを外部に送信されたり、持ち出されたりした際に、検知・アラート通知ができること。

⑥　ファイルの暗号化や暗号化解除のワークフロー機能を有し、管理できること。

⑦　ファイルの暗号化や暗号化解除の操作をログから追跡できること。

⑧　ファイルの最終利用場所の特定ができることが望ましい。

⑨　ファイルに付与された権限にもとづき、当該ファイルに対して以下のような制御が行えることが望ましい。

- ファイル操作（参照／更新）の制御
- ファイル印刷の制御
- 外部へのメール添付送信の制御
- 外付けストレージ（USBメモリ、外付けHDD、スマートフォン等）へのファイル書き出し制御
- 認可されたクラウドサービスへのファイル格納の制御
- 認可されていないクラウドサービスへのファイル格納の制御

⑩　暗号化されたファイルの使用状況を監査し、レポートを生成できると望ましい。

⑪　調達予定の端末において負荷が少なくファイル暗号化機能を利用できること。

（9）　メールセキュリティ対策

Microsoft Exchange Onlineを利用したメールセキュリティ対策に関しては、必須ではないが導入できると望ましい。

また、ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているサービスを利用すること。

①　標的型攻撃メール、ランサムウェアに対して、従来のパターン検索のみならず機械学習AI検索やサンドボックスなど異なる技術を用いて脅威を検知できると望ましい。

②　送信元のIPアドレスを確認やメールに電子署名を付与し送信者の真正性が判断できると望ましい。

③　②の対処が失敗したメールに対して、受信や隔離、拒否の制御ができると望ましい。

④　メール付帯情報（メールヘッダーなど）のなりすましメール検査ができると望ましい。

⑤　ヒューリスティック（経験則）による、スパムメール対策ができると望ましい。

⑥　メール送信元のIPアドレスを評価し、スパムメール対策ができると望ましい。

⑦　パスワードで保護されている圧縮ファイル、ドキュメントファイルに対してもウイルス検索ができると望ましい。

⑧　誤検知の少ない多層チェックを実施し、ユーザによる隔離チェックが柔軟に行えると望ましい。

⑨　ログやレポートを活用し、システムセキュリティ分析、強化及び脅威の軽減ができると望ましい。

⑩　添付ファイルは静的解析によるファイル検査を実施し、既知の脅威を検知・駆除できると望ましい。

⑪　Webレピュテーションによるフィッシングなどの不正URL対策を実施し、URLが評価されない場合は本文URLを書き換え、アクセス先を安全なサーバに変更できると望ましい。

⑫　⑩による検査及び⑪による評価後、不審な判定とされた添付ファイルや、システムが評価できないURLからダウンロードできるファイルがあった場合、サンドボックスによる動的解析を実施し、未知の脅威を検知・駆除できると望ましい。

⑬　隔離されたメッセージを管理コンソールにて確認後、手動で削除または配信できると望ましい。

⑭　隔離された自身のメッセージをユーザコンソールで表示または管理ができると望ましい。

⑮　送信メールをスキャンし、個人情報漏えいのリスクがあるメールを隔離・通知できると望ましい。

９．９．５　端末管理・MDM

端末管理・MDMとは、教職員用端末の物理的資産管理、ライセンス管理、ソフトウェアバージョン管理、プログラム配信、リモートコントロール等を行う機能を指す。

各機能に対して、ISMAPまたは、ISO/IEC27017（クラウドサービスセキュリティ）の認証を取得しているサービスを利用し、契約期間中は、常に最新バージョンが利用できること。

以下の各項目の仕様を踏まえ、提案すること。

（１）　資産管理機能

①　対象端末のハードウェア構成、ソフトウェアのバーション・ライセンス管理ができること。

②　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。

③　資産情報の検索の際は、インベントリ情報やWindows OSのバージョン、ビルド番号、サービスパックなどから、同時に複数項目、複数キーワード及び数値の範囲を指定して検索が可能であること。

④　収集したハードウェア及びソフトウェア情報を、一覧で表示でき、収集した情報をAND,OR,NOTを指定として検索可能であること。また、検索条件を保存する機能を有すること。

⑤　最新のセキュリティパッチを更新していない端末の一覧の取得が可能であること。

⑥　BitLockerの設定情報（暗号化の方法/保護の状態/回復キー）を確認できると望ましい。

⑦　端末における操作ログについては、５年間以上保存できること。

（２）　配信機能

①　対象端末へのアプリケーション、ファイル（Windows Update（累積パッチ、Feature Update）等）等配信が行えること。

②　アプリケーション・ファイル配信が簡便にできる仕組みを準備すること。

③　配信時のダウンロード時の帯域制限が設定でき、ダウンロード期間・時間帯、実行期間・時間帯が指定できると望ましい。

（３）　外部記憶媒体の使用制限機能

①　USBデバイスをシリアルナンバーごとに管理する機能を有すること。

② 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と望ましい。

③ 収集した情報をもとに、指定したUSBデバイスを使用許可/不許可を設定できること。

（4） セキュリティアップデート機能

① OSやアプリケーションのアップデートが行われているか管理できること。

② OSやアプリケーションのアップデートを強制できること。

（5） リモートワイプ機能

端末の盗難や紛失を想定し、リモートワイプ機能を備えていること。

（6） リモート操作機能

① 保守運用の効率化のため、対象端末に対して以下のようなリモート操作機能を持つこと。

- 管理側端末に対象端末の画面が表示できること
- 対象端末のマウス操作やキーボード入力ができること

② 同時に5台以上のリモート操作が可能であること。

③ リモート操作機能は、セキュリティホールとなる可能性が高いため、特定のネットワークの特定の端末からのみ行えるように制限できることが望ましい。

④ リモート操作機能の利用には、対象者の承認が必要なことが望ましい。

9.10 Microsoft 365 A3(EES)ライセンスの調達及び更新

① Microsoft Enrollment for Education Solutions(EES)にて、Microsoft365 A3 Original Edu Sub Per Userを3,000ライセンス（令和８年３月１日～令和13年３月３１日）を本市を担当する日本マイクロソフト株式会社の営業担当と連携し購入すること。

② 令和８年３月１日以降も切れ目なく引き続きマイクロソフトライセンスに付随するサービスを利用できるよう令和８年２月28日までにライセンス更新作業を実施すること。

9.11 データ移行作業

以下の各項目の仕様を踏まえ、本市、本市の既存関係事業者及び受託者側の作業者を明確にし、提案すること。なお、できる限り受託者側での作業完了が望ましい。ただし、具体的な移行データ内容、方法、ボリューム、実施時期等については、協議のうえ決定する。なお、本市が既存関係事業者へ必要な作業費用を支払い、作業を依頼する。

① 本庁舎の既存ファイルサーバ並びに小中学校及び教育センターのNASから新教育ICT環境におけるファイル保存エリアにデータ移行作業を行えること。

② AD（Active Directory）サーバ内の情報を新環境に移行すること。

9.12 本運用前運用保守

以下の各項目の仕様を踏まえ、最適な提案をすること。研修に関しては、内容、時期、回数、対象者、実施場所等について本市と協議のうえ決定する。

（1） 展開支援

① 本事業で発生する各拠点への展開作業に関する進捗管理及び展開に伴う支援を行うこと。

② 展開にあたって本市から本事業に関する情報の提供依頼があった場合は提供すること。

（2） ヘルプデスク

① 仮運用中に想定される各拠点からの問い合わせに対応すること。
② ヘルプデスクの体制案について提示すること。
③ ヘルプデスクの受付時間は、土曜、日曜、国民の祝日に関する法律「昭和23年法律第178号」に規定する休日、受託者側が定める夏期休業期間及び12月29日から翌年の１月３日までの日を除く平日の午前８時30分から午後５時を基本とし、電話にて受付対応すること。
④ 電話受付対応時間外についても、メールでの問合せであれば、24時間365日受け付けること。ただし、時間外に受け付けた問い合わせの対応については、翌営業日以降とする。
⑤ 必要に応じて、リモート操作による支援、問題解決等の対応ができると望ましい。

（３） マニュアル作成
① 研修会等で必要となる研修資料・手引き・手順書等は、すべての研修会において受託者にて用意すること。なお、操作マニュアル等については、PDF等の電子ファイルで提供すること。
② システム管理者向けには、詳細を記したものの他に、経常的に使用するものを作成すること。
③ 学校の教職員等の本市関係者向けには、初心者でも初見で理解できるような平易な内容のものと、詳細を記したものを作成すること。
④ マニュアルについては、変更事項が生じた際には、随時更新すること。

（４） 拠点内LAN引き渡し研修
① 本事業で整備したLAN設備・電気設備の維持管理について、システム管理者に説明を行うこと。その際通常稼働時における運用方法と保守体制、不具合・故障発生時における学校業務に影響する範囲の予測と対応方法、機器の仕様・設定等について具体的なマニュアル等の資料を基に分かりやすく説明すること。
② 本事業で整備したLAN設備・電気設備、端末の維持管理について、各学校へ簡易な説明を行うこと。その際、教職員等が直接触れる機器の仕様・使い方等について、具体的なマニュアル等の資料を基に分かりやすく説明すること。

（５） 端末導入研修
① 端末導入時には、教職員等に向けた導入研修を実施すること。
② 研修の方式、回数については提案すること。ただし、最低中学校区ごとに１回程度は実施すること（現地研修であると望ましい）。また、十分なセキュリティ対策が施されているWebシステムを使用しての実施などの提案も可とする。
③ 研修内容については、現行環境との違い、端末保管やログイン方法などの認証・運用ルールの変更点、新機能、ファイルサーバの操作の考え方、セキュリティの考え方、保守サービス等の内容等を踏まえて提案すること。

（６） 教育情報セキュリティポリシー改訂支援等業務
① 国（個人情報保護委員会含む。）の方針等を基に、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６年１月版）に準拠し、本市が実施すべき具体的な施策について指導・助言のうえ、本事業で整備するセキュリティ対応を考慮した東大阪市立学校園情報セキュリティポリシー改訂の支援を行うこと。
② 東大阪市立学校園情報セキュリティポリシー改訂案を本市に提供できると望ましい。

９.13　運用保守

ディープラーニングの基盤技術により生成AIが発展し、今後もICTの加速度的な技術進化が見込まれることから、本市の教育ICT環境の在り方も技術進化に対応していく必要がある。受託者には、時代の流れに柔軟に対応できる運用保守及び伴走支援を強く求めるものである。

上記を前提とし、以下の各項目の仕様を踏まえ、本事業で整備する教職員用端末、拠点内のLAN回線、ネットワーク機器及びサーバ等並びに既存のLAN回線及びネットワーク機器等の管理や修理対応、ソフトウェアの不具合への対応並びにアカウント管理及び年次更新作業等の運用全般について支援するなど一元的に運用保守を行う最適な提案をすること。

９.13.１　ヘルプデスク

① 電話受付対応時間外についても、メールでの問合せであれば、24時間365日受け付けること。ただし、時間外に受け付けた問い合わせの対応については、翌営業日以降とする。

② 各拠点内に設置するネットワーク機器及び教職員用端末のトラブルから運用支援まで、各拠点の関係者からの問い合わせに対応すること（本市専用のヘルプデスクであると望ましい）。なお、ネットワーク不具合、教職員用端末等の月件数は、100件程度である。

③ 本事業範囲以外の問い合わせについては、本市が提示する関係部署、ヘルプデスク等の連絡先に案内すること。

④ 教職員用端末に差し込むUSBデバイスにかかる申請に対する設定対応ができると望ましい。

⑤ 児童生徒用端末、電子黒板等の問い合わせについて、設置するヘルプデスクで受け付け、本市契約の各保守業者へエスカレーションする対応ができると望ましい。

⑥ ヘルプデスクの体制案について提示すること。

⑦ ヘルプデスクの受付時間は、土曜、日曜、国民の祝日に関する法律「昭和23年法律第178号」に規定する休日、受託者側が定める夏期休業期間及び12月29日から翌年の１月３日までの日を除く平日の午前８時30分から午後５時を基本とし、電話にて受付対応すること。

⑧ 必要に応じて、リモート操作による支援、問題解決等の対応ができると望ましい。

９.13.２　機器及びソフトウェア等保守

（１） 受付対応時間

原則平日の午前８時30分から午後５時とする。日曜日、土曜日、国民の祝日に関する法律「昭和23年法律第178号」に規定する休日、受託者側が定める夏期休業期間及び12月29日から翌年の１月３日までの日は除く。ただし、ネットワーク障害等緊急を要する場合については、この限りではない。

（２） 運用保守の全体統括者の設置

運用保守の全体統括者を設置し、運用状況について、本市に定期的な報告を行うとともに、システムの維持・向上を図るために、継続的な運用改善の提案を行い、本市の承認を得た改善策を推進すること。

（３） 障害対応

① 機器及びソフトウェア等のトラブル事案の受付、事象の切り分け、解決策の提案などに対応すること。

② 障害時の問い合わせや調査依頼に対応すること。また、電話での解決やリモートでの調査が

困難な場合や切り分けが難しい場合には要員訪問し、調査・対応にあたること。原則として、１営業日以内に現地へ訪問して対応すること。

③　修理に時間が掛かる場合は、代替機器を用意し、業務等の学校運営に支障がでないようにすること。

④　故障時の対応として先出センドバック方式を含め、学校運営への影響を最小限にすること。

⑤　障害原因がLANケーブルの劣化等であった場合、新設既設かかわらず、各拠点のネットワーク環境に応じたLANケーブルを用意し、敷設すること。

⑥　整備後に整備対象校より通信状況が悪い箇所があり、当該利用者から申告があった場合は調査を行い、調査の結果、受託者側の整備・保守に原因がある場合は、改修計画の立案とその説明、改修を行うこと。改修については受託者の負担とする。

⑦　必要に応じて、本市が別途契約している保守業者、通信回線業者及びその他の関係業者と連携をとり、機器の円滑な運用、保全、復旧に努めること。

（４）　障害報告

①　障害報告を必要とする障害対象については、協議のうえ決定する。

②　障害発生時のエスカレーションルールに沿って、本市へ速やかに一次報告（復旧までの目標時間、原因等の報告）し、本市と協議のうえ障害対応にあたり、復旧までの目標時間を超える場合は、本市へ迅速に相談し、協議して本市の指示に従うことを想定している。

（５）　機器の交換

①　故障や不具合により修理対応・交換が必要と判断する場合には、予備機をキッティング、導入年月日・管理番号のラベルシールを貼付し、各拠点へ持参し交換対応を行うこと。

②　ネットワーク機器等の予備機については、想定する運用保守で必要な台数を受託者にて準備し、保管すること。

③　前述の９．２．10で示した2,939台（【別紙６】参照）には、端末故障等による交換のための予備端末台数は含んでいないため、故障等の際に遅延なく端末を利用できるように想定する運用保守で必要な台数の予備端末を受託者にて準備し、保管すること。

④　修理保証の対象機器については、故障機を修理後に予備機として保管すること。

（６）　既設機器の運用保守

対象機器は以下のとおりである。

機器名	数量（台）	設置場所
アクセスポイント（Cisco Meraki MR-36）	2489（予備30台含む）	小中高等学校
PoEスイッチングハブ（Cisco Meraki MS120-24P）	373（予備10台含む）	小中高等学校
L3スイッチ（Cisco Catalyst 9300）	2	J:COM東大阪局
ファイアウォール（Palo Alto Networks PA-5260）	2	J:COM東大阪局
DNSサーバ（Soliton D3-SX15-A-GIGA2-H2）	2	J:COM東大阪局

上記機器は、本市の費用負担のもと、令和９年度中に別機器に更新する可能性がある。更新した際、当該機器についても引き続き本事業の契約内で運用保守（各機器の調達及びライセンス費用は除く）すること。

9.13.3　定期点検等

（1）　定期点検

整備したサーバ等については、定期的に点検（ハードウェアの点検、ソフトウェアのメンテナンス、パフォーマンス監視等）を実施すること 。

（2）　計画停電時の電源管理

利用期間中に建物管理上の計画的停電等が発生した場合には、日時や影響等について本市と協議のうえ、受託者にて適切に対応すること。

（3）　ライセンス更新

保守対象のハードウェア及びソフトウェアのライセンスを切れ目なく更新すること。

9.13.4　ネットワーク運用管理

① 構成情報については、以下の内容について電子データで常に最新の情報を管理し、本市から依頼があった場合は、データとして提示できること。

・ ネットワーク機器：機種名、シリアル、導入年月日、設置場所、メーカー、設定情報、IPアドレス

・ ネットワーク系統図：論理図面、物理図面、施工図面での管理を行うこと。

② ネットワーク図面及び機器情報においては、常に最新データとして管理できるように定期的な監査及び更新作業を行うこと。

③ ネットワーク機器のコンフィグ設定情報に関しては、最新の情報で管理を行うこと。

④ ネットワークを監視すること。

⑤ 教育系ネットワークに限らず、環境の変化又は、トラブル対応等で現在稼動しているネットワーク機器に多少の設定情報の変更が生じた時は、対応すること。

⑥ 障害時は、9.13.2（3）、（4）、（5）に準じ、対応すること。

⑦ 計画停電時は、9.13.3（2）に準じ、対応すること。

⑧ ネットワーク機器のライセンスについては、9.14.3（3）に準じ、対応すること。

9.13.5　サーバ運用管理

① 構成情報については、メーカー、機種名、シリアル、OS、導入年月日、設置場所、IPアドレスについて電子データで常に最新の情報を管理し、本市から依頼があった場合はデータとして提示できること。

② サーバの監視を行うこと。

③ 障害時は、9.13.2（3）、（4）、（5）に準じ、対応すること。

④ サーバのバックアップの確認及びバックアップ媒体の管理を実施すること。

⑤ 計画停電時は、9.13.3（2）に準じ、対応すること。

⑥ サーバ内のライセンスについては、9.13.3（3）に準じ、対応すること。

9.13.6　教職員用端末運用管理

① 構成情報については、メーカー、機種名、シリアル、OS、導入年月日、利用者名について電子データで常に最新の情報を管理し、本市から依頼があった場合は、データとして提示できること。

② 不正にインストールされたソフトを発見した場合やアンチウィルスソフト等においてウィルス

が発見された場合は、本市に対して報告すること。

③　障害時は、９.13.２（３）、（４）、（５）に準じ、対応すること。

④　OS及びアプリケーションを含めたイメージバックアップを保持し、保存しておくこと。

⑤　端末にインストールしているソフトウェア等のライセンスについては、９.13.３（３）に準じ、対応すること。

９.13.７　セキュリティ運用管理

（１）　ウィルス対策の管理

①　パターンファイルについては、常に最新のものが使用されているか確認を行うこと。

②　ウィルスの感染情報については、定期的に報告を行うこと。

（２）　セキュリティパッチの管理

①　教職員用端末のセキュリティパッチについては、９．９．３のサービスを利用し、最新のパッチ適用を行うこと。

②　サーバ及びネットワーク機器のセキュリティパッチ実施状況についても、本市と協議のうえ管理を行うこと。

③　最新のセキュリティパッチ情報については、迅速に本市に対して報告ができ、その対応についても迅速に対処すること。

④　最新のパッチ適用の際には、事前に検証を行うこと。

（３）　セキュリティログの管理

本市のシステム等で記録されているセキュリティログのバックアップ及び保管を行うこと。また、本市から過去のセキュリティログ分析の依頼があった場合は、過去のデータを分析して報告を行うこと。

（４）　ソフトウェアのバージョンアップ・Windowsアップデート

①　最新のソフトウェアのバージョンアップの際には、事前に検証すること。

②　定期実施のWindowsアップデートは、通常の学校業務に影響がないように実施できる仕組みを構築し、行うこと。なお、緊急性の高いアップデート等は協議のうえ、即時行うこと。

（５）　Webフィルタリングの管理

Webフィルタリングサービスについて、本市から依頼があった場合にサイトの閲覧可否の設定作業を行うこと。

（６）　セキュリティ支援

最新のセキュリティ情報を入手し本市に情報提供を行うこと。

（７）　ウィルス感染時対応

①　ウィルス感染の疑いが発覚した際には、セキュリティオペレーションセンター（SOC）と連携のうえ至急該当端末を取り除き、ウィルスが当該学校園及び他の学校園等の端末に感染していないか確認すること。

②　ウィルス感染時は、セキュリティオペレーションセンター（SOC）と連携のうえ原因を突き止めるとともに、原因がセキュリティホールやソフトウェアの脆弱性にある場合は、至急でセキュリティパッチやソフトウェアのバージョンアップ等の対応を行うこと。

9.13.8　バックアップ運用管理

①　サーバのバックアップの確認及びバックアップ媒体の管理を実施すること。

②　サーバに問題が発生した場合は、バックアップ媒体より迅速に復旧処置を行うこと。

9.13.9　セキュリティオペレーションセンター（SOC）

①　９．９．３において不正な挙動を検知した際に、その内容を専門的見地から分析し、必要に応じてネットワークから遮断する等の対応を行うこと。

②　９．９．３から通知されるセキュリティアラートをリアルタイムに監視し、脅威に対する一次解析、リスク判断、解決方法の提示などを行うとともに、常駐のヘルプデスクと密接に連携しながら復旧まで行い問題の解決にあたること。

③　セキュリティリスクの状態を可視化し、対策の検討及び対応を行うこと。

④　監視は、サイバー攻撃を受けた時の攻撃手法の分析やトラブル対応が実施できる専門性を有する者が24時間常時体制で運用すること。

⑤　必要に応じて、監視環境のソフトウェアや設定パラメーター等を見直すこと。

⑥　セキュリティ関連の運用データを分析し、検知、防御の精度にかかる閾値や設定の変更を行うこと。変更を行う場合は原則、事前に変更理由、変更内容を本市へ通知すること。

⑦　インシデント検知時の解析回数に上限を設けないこと。

9.13.10　教職員等アカウントの管理作業

①　新教育ICT環境においても教職員等には１人ずつUUIDを付与する。導入当初、その後の採用、異動、退職等に伴うID管理及び更新作業について、受託者の運用保守にて対応することが望ましい。

②　ユーザーID忘れやパスワード再発行、ロック解除など学校現場で即時回復が必要な事象については、ヘルプデスクでの電話対応時間内であれば保守拠点から即時対応できる環境・体制を構築することが望ましい。

9.13.11　年度更新作業

（１）　教職員等アカウント異動

①　人事異動や新規採用等によるアカウントや権限の変更作業を実施すること。

②　人事異動情報等は教育委員会から提示するが、新年度は４月１日から確実に運用可能となることが必要であるため、対応方針を示し、年度末の教職員等アカウント異動はきわめて短い期間で正確な更新作業を実施できること。

（２）　教職員用端末移設

①　年度更新時の学校間等での端末移設・設定を実施すること。詳細な移設対象校や移設対象端末数については、各年度の状況に応じて協議により決定する。なお、毎年度、回収は50台程度、配備は50台程度である。

②　移設先の電子黒板、プリンター等の機器を利用できるよう設定すること。

③　毎年度各小中学校のクラス編成に伴う市内学校間で移設する電子黒板等を小中学校内LAN更新後のネットワークに参加させ、無線投影できるよう設定すること。

（３）　小中学校電子黒板等移設

①　本市の指示する学校間の移設を実施できると望ましい。なお、毎年度移設する電子黒板等は４台程度である。

② 65型電子黒板等については全ての付属品、ケーブル類が揃っているか事前に確認すること。また、各機器の配線やケーブルの収納状況、インシュロック等による固定などは解除せずにそのまま移設できると望ましい。

③ 移設後の小中学校の教職員用端末に投影するための設定を反映させ、教職員立会いのもと動作確認できると望ましい。

④ 学校間の運搬時には2t以上の運搬専用トラックを使用し、車両移動時にはトラック庫内で動くことがないように固定して運搬できると望ましい。

9.13.12 インストール作業

① 学校園にて新規でプリンタ等購入した際の教職員端末へのプリンタドライバのインストール作業を実施できることが望ましい。

② 本市の指示によりソフトウェア及び機器ドライバのインストール・アンインストール作業を実施できることが望ましい。

9.13.13 小学校電子黒板一式保守業務

① 小学校に設置している65型電子黒板（CBS-LCE65H5CL）（766台）、書画カメラ（みエルモんL-12iD）（728台）をはじめとした付随する周辺機器（電子黒板や周辺機器を更新した場合も含む）についても安定稼働するよう保守できると望ましい。

③ 上記①含まれないが、小学校電子黒板等一式が安定稼働するため必要な場合は対応できるとことが望ましい。

9.13.14 教育情報セキュリティポリシー改訂支援等業務

① 将来的に文部科学省が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改訂した際に、本市が実施すべき具体的な施策について指導・助言して、東大阪市立学校園情報セキュリティポリシー改訂の支援を行うこと。

② 東大阪市立学校園情報セキュリティポリシー改訂案を提供できると望ましい。

③ 文部科学省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（令和６年１月版）、総務省の地方公共団体における情報セキュリティポリシーに関するガイドライン(令和５年３月版)及び改訂版の東大阪市立学校園情報セキュリティポリシーに基づいた学校向けの研修動画を作成すること。なお、各セキュリティポリシーの改訂が生じた際は、学校向けの研修動画を再作成すること。研修動画の内容については、本市と協議のうえ決定する。

④ 本市がセキュリティ監査を実施する場合には、監査員に協力すること。

9.13.15 研修・説明会・マニュアル作成

以下の各項目の仕様を踏まえ、最適な提案をすること。契約期間中の研修に関しては、内容、時期、回数、対象者、実施場所等について本市と協議のうえで決定する。なお、研修方法は十分なセキュリティ対策が施されているWebシステムを使用しての実施などの提案も可とする。また、オンデマンドに対応していること。

（1） フォローアップ研修

① 新任教職員等向けの研修内容、方式、回数については提案すること。

② 業務での活用促進を目指し、年数回程度のステップアップ研修を実施できると望ましい。

（2） セキュリティ研修

ネットワーク統合やクラウド化を進めるにあたっては、教職員のセキュリティ意識向上は必須の検討課題であることから、セキュリティ意識醸成や新教育ICT環境におけるセキュリティの考え方の理解促進を目的に定期的に研修を実施すること。オンライン実施も可とする。

（3） 年度更新作業説明会

年度更新に伴う学校にて発生する作業の概要、その他留意点等について説明会を行うこと。

（4） マニュアル作成

９.12(3)と同じ。

９.13.16　業務マニュアルの整備保守

各種運用管理についての業務運用マニュアルに関して、環境の変化に合わせて整備を行い、常に最新の状態を保つこと。また、業務運用マニュアルや運用管理手法を記したドキュメント等については一覧にし、電子フォルダが常に整理された状態を保つこと。詳細については、本市と協議しながら、下記については少なくとも整備すること。

① 日常の監視及びオペレーション作業
② クライアント端末・運用管理に関する作業
③ 年次更新（人事異動時）の作業
④ ネットワークやサーバ等の簡易な設定作業
⑤ 障害対応（障害時の連絡先、切り分け基準等）作業
⑥ 各拠点の端末、セグメント、特殊設定等、各拠点の端末・ネットワーク環境に関する資料

９.13.17　定期報告

① 新教育ICT環境の利用状況、保守対応状況、ヘルプデスク対応状況等を定期的（月１回程度）に報告すること。なお、実施方法及び頻度については運用状況を踏まえて別途協議により決定する。
② 月末時点での各ライセンス数を報告すること。
③ 運用保守課題等の報告を行い、必要に応じてルールの見直しや設定変更等の対応により運用管理業務の品質向上に努めること。

９.13.18　支援対応

① 各拠点向けのFAQ作成し、随時更新すること。
② 整備した機器及びソフトウェア等の運用に関する質疑に対応すること。また、定期的及び経常的支援を提案すること。
③ その他本事業の整備内容についての問い合わせには、可能な限り柔軟に対応すること。

９.13.19　引継ぎ

本事業の運用保守期間が終了を迎えるに当たって、次期ICT環境構築契約事業者から導入による情報の開示や作業の協力を求められた場合、受注者は可能な限りその要請に応じること。ただし、打合せやデータ移行等にかかる諸作業の費用は本事業に含めること。なお、次期契約事業者への引継ぎは、本市が間に入り行うものとし受託者と次期契約事業者のみでやりとりは行わないこと。ただし、本市が承認したやりとりについては、その限りではない。

９.13.20　データ消去

９．２．１⑤のとおり、リース契約により調達した機器については、契約満了後に無償譲渡を受ける

ことを想定しており、当該機器のデータ削除は本市にて実施する予定である。提案するIaaS、パブリッククラウド及びSaaSのクラウドサービスのデータ消去については、受託者側の責任で実施すること。完全なデータ消去後、本市に作業報告書及びデータ消去証明書を提出すること。

10　その他

（1）　権利義務の譲渡等の禁止

受託者は、本業務にかかる契約により生ずる権利または義務を第三者に譲渡し、もしくは承継させ、またはその権利を担保の目的に供することができない。ただし、あらかじめ本市の承認を得た場合は、この限りではない。

（2）　著作権

本事業の履行過程で本事業のため新たに生じた著作物にかかる著作権は、本市及び受託者の共有のものとする。ただし、ソフトウェア等既存の著作物にかかる著作権は除く。

（3）　契約不適合責任

本事業の納品完了後、本契約の内容に適合しないものがあるときは、受託者は無償で補修・追完を行うものとする。この場合において受託者の責任は、発注者が契約不適合を知った日から１年以内に請求があった場合に限る。

（4）　紛争等

本仕様書に基づく作業に関し、第三者との間に著作権にかかる権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら本市の責めに帰す場合を除き、受託事業者の責任、負担において一切を処理すること。この場合、本市はかかる紛争等の事実を知ったときは、受託事業者に通知し、必要な範囲で訴訟上の防衛を責任者にゆだねる等の協力措置を講じるものとする。

（5）　守秘事項等

本事業の履行にあたって本市より提供する各種情報や知り得た秘密については、本事業においてのみ使用することとし、これらを第三者に漏らしてはならない。本規定は、本契約が終了し、または解除された後においてもまた同様とする。

（6）　損害賠償

受託者の責に帰すべき理由により、本市又は第三者に損害を与えた場合には、受託者がその損害を賠償すること。

（7）　調査等

本市は、必要があると認めるときは、受託者に対して委託業務の処理状況について調査し、または報告を求めることができる。この場合において、受託者はこれに従わなければならない。

（8）　協議

本仕様書に定めのない事項またはこの仕様書について疑義の生じた事項については、本市と受託者とが協議して定めるものとする。