

教育系ネットワーク・サーバ構築、保守運用業務委託
及び機器賃貸借

仕 様 書

令和 6 年 4 月

山梨市

目 次

1	総括.....	1
1-1	一般事項.....	1
1-2	配線・材料・機器の導入	7
1-3	特記事項.....	10
2	業務仕様	11
2-1	業務目的.....	11
2-2	システム更新	11
2-3	現状調査.....	11
2-4	ネットワーク機器の更新	12
2-5	サーバシステム等の更新	16
2-6	システムのデータ移行.....	26
2-7	Microsoft365 A5.....	26
2-8	システム構築後の総合テスト.....	31
2-9	サーバ室移転	31
2-10	システム切替	31
2-11	端末設定.....	32
2-12	図書館システム端末設定	32
2-13	既存機器の撤去・廃棄.....	32
3	保守運用業務	32
3-1	保守サービスの条件	32
3-2	システム保守支援要員（SE）の派遣.....	34
3-3	保守作業報告	34
3-4	保守期間・保守対応時間	34
3-5	緊急措置対応	34
3-6	保守対象機器	35
3-7	クラウドサービス（Microsoft 365 A5）の監視・保守について	35
3-8	ドキュメント等の管理.....	36
3-9	情報セキュリティ研修の実施.....	37
3-10	最新情報の共有.....	37
3-11	教育情報化推進会議への参加.....	37

別紙 1 対象学校の端末台数

別紙 2 開放系ネットワーク施設と端末台数

1 総括

1-1 一般事項

1-1-1 概要

本書は、「教育系ネットワーク・サーバ構築、保守運用業務委託及び機器賃貸借」に関する仕様を記載したものである。

現在の教育系システムのネットワーク及びサーバは、導入より 5 年以上が経過し、更に再更新を行って利用している。このため、機器の老朽化による故障率が上がり、システムが利用できない時間や頻度の増加が懸念される状況である。

本業務においては、ネットワーク及びサーバシステムの見直しを行い、老朽化したネットワーク機器及びサーバを更新する。これにより故障や古いバージョンによる不具合のリスクが軽減され、ネットワークトラフィックの処理やサーバにおける処理が增強されるため、システムの安定稼働・セキュリティの向上が見込まれる。

また、文部科学省「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。）」の最新版に則り、現状のネットワークを分割する境界防御型によるセキュリティ対策から、リソースに対するアクセス認証や通信の保護をするアクセス制御型によるセキュリティ対策へ変更し、情報セキュリティ対策の強化を行う。

さらに、笛川小学校の無線 LAN システムの更新及び公民館に無線 LAN 環境の整備を行い、更なる教育系ネットワークの利便性の向上を図る。

1-1-2 発注者

名称	山梨市
住所	山梨県山梨市小原西 843

1-1-3 賃貸借開始日と保守運用期間、契約等

機器の賃貸借開始日及び保守期間は次のとおりとする。

- 賃貸借開始日：令和 6 年 10 月 1 日を基本とする。
- 保守運用期間（賃貸借期間）：開始日より 5 年間とする。

賃貸借開始日までに機器を導入し、システムの稼働を行うこと。

賃貸借開始日以前に、ライセンス料やハードウェア保守費等が発生する場合は、そ

の費用も本調達費用に含めること。

支払い方法や契約内容における詳細事項については、構築事業者も含めて協議により決定する。

1-1-4 賃貸借期限後の対応

調達する機器は、賃貸借を1年延長できる内容にて導入すること。またサーバ機器を除く、導入した機器類（NAS、アクセスゲートウェイ、スイッチ、アクセスポイント、ルータ、MC、SFP、ポータブル電源等）及びソフトウェアについては5年間利用後無償譲渡とすること。

1-1-5 履行時間等

原則として、土曜日、日曜日、国民の祝日に関する法律に規定する休日及び年末年始を除く午前8時30分から午後5時15分までとする。前項に規定する時間外であっても、市の要請による場合はその限りではない。

また作業によりサーバ及びネットワーク停止等が想定される場合は、事前に市担当者、学校担当等と十分にスケジュール調整を行うこと。

1-1-6 計画準備

本業務の履行に先立ち、本業務の目的・趣旨を把握した上で、本仕様書に示す業務内容を確認し、諸手続き届及び業務計画書を作成し、発注者が指定する監督員等に提出し、承認を得ること。業務計画書には、スケジュール、作業体制、対応窓口、システム構築内容、セットアップ方法、運用方法、自主検査方法等についても記載を行うこと。

1-1-7 対象施設

- | | | |
|-----|---------------|-------------------|
| (1) | 山梨市役所本庁舎 | 山梨市小原西 843 |
| (2) | 山梨市情報通信センター | 山梨市上神内川 1333 番地 1 |
| (3) | 牧丘支所 | 山梨市牧丘町窪平 350 |
| (4) | 三富支所 | 山梨市三富川浦 262 |
| (5) | 学校給食センター（VPN） | 山梨市正徳寺 1552 |
| (6) | 加納岩小学校 | 山梨市下神内川 123-2 |

(7)	日下部小学校	山梨市小原東 305
(8)	後屋敷小学校	山梨市三ヶ所 877
(9)	日川小学校	山梨市歌田 140-1
(10)	山梨小学校	山梨市落合 1-7
(11)	八幡小学校	山梨市北 1900-1
(12)	岩手小学校	山梨市東 1737-1
(13)	笛川小学校	山梨市牧丘町窪平 1200
(14)	山梨南中学校	山梨市下石森 376
(15)	山梨北中学校	山梨市小原東 359-1
(16)	笛川中学校	山梨市牧丘町窪平 1100
(17)	加納岩公民館	山梨市上神内川 387-1
(18)	日下部公民館	山梨市小原東 577
(19)	後屋敷公民館	山梨市三ヶ所 870-1
(20)	日川公民館	山梨市歌田 596
(21)	山梨公民館	山梨市落合 1-7
(22)	八幡公民館	山梨市市川 1220
(23)	岩手公民館	山梨市東 1734-1
(24)	中牧公民館	山梨市牧丘町西保下 2252
(25)	西保公民館	山梨市牧丘町牧平 36-1
(26)	教育支援センターWith	山梨市上神内川 1348

※No.1～16 は、教育系ネットワーク対象施設、No.17～25 は開放系ネットワーク対象施設、No.26 は独自ネットワーク。

1-1-8 構成

- 1) 仕様書（本書）
- 2) 設計書
- 3) システム構成図
- 4) サーバ室移設概要図

1-1-9 関係法令等

受注者は、委託業務の実施にあたり最高の理論・技術を発揮し、契約書・仕様書・諸法令・条例・規則・関係通知等に準拠して業務を遂行すること。

1-1-10 会社要件

受注者は以下の要件すべてを満たしていること。

また、落札後に市から要求があった場合には、速やかに証明書を提出すること。

- 1) 地方自治体等において小中学校等の教育系ネットワーク(教育委員会ネットワーク)の構築及び保守管理業務の実績を過去 10 年以内に複数件有していること。
- 2) Microsoft 社認定の以下パートナー、または上位パートナー資格を有すること。
 - ・ ゴールドアプリケーションインテグレーション
- 3) ISMS/ISO27001、QMS/ISO9001 又はプライバシーマーク等の個人情報管理の資格を有していること。
- 4) 本社または本店が山梨県内にあり、現地対応できる社員等が本市までに、約 60 分以内に到着できること。

1-1-11 主任技術者

本業務には主任技術者を設置すること。主任技術者は、次のすべての項に該当する者とする。また、落札後に市から要求があった場合には、速やかに証明書を提出すること。

- 1) 3 年以上のプロジェクトマネージャーの実務経験を有する者。
- 2) 本システム構築フェーズにおける進捗会議及び保守運用会議すべてに参加できる者。
- 3) 応札する会社等の正社員（他社からの下請けや出向では無い者）であり、かつ 3 年以上勤務していること

1-1-12 業務範囲

本業務の範囲は、以下のとおりであり、ケーブルの敷設、接続・ハードウェアの導入・設定・調整・試験・運用フォロー・サポート等の全般とする。また、業務実施に伴う関係箇所への連絡・打合せを含むものとする。

- 1) ネットワーク機器の更新（笛川小、公民館無線 LAN システム更新含む）
- 2) サーバシステム等の更新

- 3) データ移行、サーバ室移転、システム切替え
- 4) Microsoft365 A5（別途導入）設定
- 5) 既設機器の撤去、廃棄
- 6) 保守運用業務
- 7) その他発注者より依頼のあった関連業務

1-1-1 3 提出書類

受注者は、本業務に必要な発注者が定める書類を提出すること。なお、承諾された事項を変更しようとするときは、その都度、発注者の承諾を受けること。記載方法の詳細や提出部数については、別途協議とする。

完成図書の概略は以下のとおりである。また着手後に貸与する既存図書の修正も本業務に含むものとする。完成図書は、全て日本語で作成すること。また完成図書は、発注者の指定したファイル様式で作成した電子媒体（CD-R、DVD-R 等）に記録したものも納入すること。

1) 完成図書概要

① 業務計画書

- ・ 業務実施体制
- ・ 導入スケジュール等

② 業務報告書

- ・ 操作運用マニュアル／取扱説明書
- ・ 導入品仕様一覧
- ・ 機器承諾図（機器はメーカー名、品番・型番、仕様、数量等構成がわかるように記載すること）、カタログ
- ・ 導入機器台帳
- ・ 物理ネットワーク構成図
- ・ 論理ネットワーク構成図
- ・ サーバ構成設定資料（パスワード一覧含む）
- ・ サーバ OS 設定資料
- ・ ラックマウント図
- ・ IP アドレス一覧
- ・ ソフトウェア一覧、ライセンス書
- ・ アカウント・パスワード一覧
- ・ 保守体制図

- ・ 付属品・予備品リスト
- ・ 試験結果報告書
- ・ 打合せにて使用した資料、議事録 等

③ 写真関連

- ・ 施工写真（施工前/施工後の写真及びその内容）
- ・ 使用材料、導入機器等

④ その他発注者より指示のあったもの

1-1-1 4 進捗管理

受注者は、随時、発注者に対し作業の進捗状況を報告すること。報告に際しては、原則として関係者を招集しての進捗会議等を開催し、その議事録・課題管理・工程表等をもって進捗報告とする。

1-1-1 5 資料の貸与

本業務の遂行上、調査すべき事項は、受注者が行うものとするが、発注者が所有し、委託業務に利用できる資料は貸与する。この場合、受注者は、借用リストを発注者に提出し、業務完了後、速やかに返却すること。資料等の複写や目的外での使用をしないこと。

1-1-1 6 秘密の保持

受注者は、本業務の遂行によって知り得た秘密・情報を第三者に漏らしてはならない。また入手した情報等は適切に管理を行わなければならない。本項目は、下請負業者にも適用する。

また、本業務にて個人情報を取り扱う必要がある場合は、個人情報保護法に基づき適切な情報管理を行なうこと。

1-1-1 7 仕様変更等の扱い

設計図書等に記載された仕様または本書の内容に変更が必要となった場合は、事前に変更理由書を用意し、発注者と協議、協議簿を作成の上行うものとする。ただし、軽微なものについては発注者・受注者双方、協議、協議簿のみにより行うものとする。

1-1-18 仕様上の疑義

本仕様書記載事項に疑義が生じた場合、発注者と受注者とが協議の上決定する。

1-2 配線・材料・機器の導入

仕様書及び設計書等に基づいた導入工事を行うこと。ただし、仕様書及び設計書等に記載なき事項で疑義が生じたものについては、発注者の指示に従い、工期内に業務を完了するものとする。

1-2-1 共通事項

業務実施にあたっては、関係法令基準を厳守すること。

仕様書及び設計書等に記載がない場合でも、システムを稼働させる上で必要となる配線設備、電源設備（OA タップ含む）、耐震固定などについては、受注者の責任において対応すること。

各機器等搬入にあたっては、既存施設部分、工事目的物の施工済み部分等について、損傷しないよう適切な養生を行うこととし、損害を与えた場合は、受注者の責任において修復すること。

1-2-2 材料

配線機材等は国土交通省大臣官房官庁営繕部監修電気設備工事共通仕様書（最新版）にある JIS、JEC、JEM の基準に該当するものはその適合品とし、それ以外のものは国土交通省大臣官房官庁営繕部監修の建設材料、設備機材等品質性能評価事業設備機材等評価名簿（最新版）による。

また、業務に使用する材料は、仕様書、実施設計図面及び設計書に定める品質及び性能を有する新品とし、見本提出等により材料の色、材質、仕上げの程度についてあらかじめ発注者の検査を受けること。

1-2-3 機器入替・新規設置

機器設置にあたっては、特に以下の事項に留意すること。

- 1) 設計書記載のメーカー、機器、材料を使用すること。記載された機器、材料が廃番となっている場合には、同等以上の機器、材料を使用すること。

- 2) 導入するネットワーク機器、サーバ機器、その他発注者が指示する機器については、別途指示する識別番号などを記載した経年変化しないシール等を添付すること。また、これらの機器に関する情報を発注者の指示する項目（設置場所、識別番号、製品型名及び番号等）、様式に従って提出すること。
- 3) 機器設置場所については、図面で確認するとともに、施工前に各施設の担当者に再確認すること。変更要望が出た場合は、発注者に報告し、その指示に従うこと。
- 4) 導入した機器については、転倒防止、落下防止措置をすること。
- 5) 機器等間のケーブルは、必要に応じて受注者が用意し、接続までを行うこと。ケーブルについては、発注者が指定した色を使用すること。また、敷設するケーブルの両端及びフロア貫通部分等には経年変化のしにくいタグをつけ、接続関係を明示すること。
- 6) 機器設置に伴い、既設のサーバ・ネットワーク機器等の移動・調整が発生する場合は、受注者の責任において対応及びケーブル処理を行うこと。
- 7) UTP ケーブルはカテゴリ 6A を使用すること。既設をそのまま使用する場合はこの限りではないが UTP ケーブルの状態を試験し問題がないことを確認すること。また、既設の UTP ケーブルがエンハンスドカテゴリ 5e でない場合は新たに敷設すること。
- 8) UTP ケーブルでコネクタに不良なものがあれば適宜交換を行い、通信確認を行うこと。
- 9) ハブ等のネットワーク機器については、UTP ケーブルが接続されない空きポートをほこりや不正機器接続から保護するため、モジュラージャックガードを取り付けること。
- 10) 機器設置、接続終了後は、各機器が仕様書記載の機能を満足するよう調整し、問題がないことを確認すること。完成検査受験前には自主検査を実施すること。

1-2-4 業務中の安全管理

受注者は、業務の施工にあたって災害、公害及び、危険防止のため、建築基準法、労働安全衛生法、環境基本法、騒音規制法、振動規制法、大気汚染防止法その他関連法令等に従い、十分な策を講じて業務を進捗すること。

1-2-5 災害防止等

作業の安全対策については、常に作業の安全に留意し、現場管理を十分に行い、災

害防止に努めなければならない。

業務現場における資材等の整理整頓・清掃等を行い、更に火災、盗難予防など業務現場の管理に万全を期すこと。

1-2-6 総合検査

引き渡し前までに、対象となる施設において、構築したシステムの動作確認を行うこと。事前に試験成績表等を作成し、発注者に提示し承認を受けること。原則として総合検査実施時は、担当職員立会いの上、正常稼動確認の印等を受理すること。

1-2-7 取扱説明

受注者は、引渡時に担当者等に対し、十分な取扱説明を行うこと。方法及び回数については、協議の上決定する。取扱説明実施後も電話等による取扱の相談に対し、受け答えのできる環境を用意すること。

1-2-8 引渡

受注者が定められた項目を全て終了し、完成届を提出後、発注者が検査を行う。その結果合格の場合は、発注者が完成検査結果通知書を受注者に提出する。受注者は、これを受けて目的物引渡届を提出することにより、業務の完了及び引渡とする。

1-2-9 保証

引渡後、引渡日から起算して1年以内に生じた不具合、調整不良及び故障等で、受注者の責任とみなされるものについては、受注者が速やかに修正、または設定変更等を行うものとする。その費用は、受注者の負担とする。ただし、受注者の責任以外とみなされた場合は、発注者と協議の上対応を決めること。

1-2-10 発生材及び廃材の処理・不要機器の廃棄

本業務において、引渡を要しない発生材、廃材等の処理は受注者の責任において関係法令に従い行うこと。また、既設機器の撤去及び廃棄は、情報漏洩が発生しないよう対策を施した上で行うこと。ただし、不要機器の使用可能な機器または発注者の指示した機器類は、再使用可能な方法で取り外し、発注者の指示する方法・場所にて保管すること。

1-2-1 1 機器類の仮設置及び移設

本業務の実施期間内に現サーバ室が移転することが予定されている。本業務で設置する機器は市が指定する場所で仮設置し、稼働させること。また、新サーバ室が完成した後は、新サーバ室に仮設置した機器を移設すること。

これらの作業費用も本業務内で実施すること。

1-3 特記事項

1-3-1 システム停止等

本業務を円滑に実施するため、発注者と十分な連絡調整を行うとともに、機器更新（入替）時には通常業務の運用の妨げとならないよう十分配慮すること。

また、本業務遂行によるシステム停止等によりネットワークに影響が出る場合は、発注者と事前に協議を行い、その影響が最小限となるように努めること。原則として、ネットワークを連続して停止する場合は業務時間内（平日）30分以内とする。それを超える場合には、業務時間外等による対応もしくは、代替機器、代替回線等によるネットワークの運転継続措置により対応するものとする。これらに係る一切の経費は受注者の負担とする。

業務完了後の運用開始一定期間は、不測の事態に備え、迅速に対応できる体制を整えること。

1-3-2 情報セキュリティに関する事項

本業務の実施にあたっては、山梨市の教育情報セキュリティポリシーを十分に理解し、業務を遂行すること。また既設ネットワーク機器の設定変更を行う場合は、市担当者と協議の上実施すること。

1-3-3 既設機器の設定変更及び報告

設定変更が必要な既設機器は、必ず事前に発注者の許可を得ること。また発注者の指示に従った設定を行うこと。既設機器との接続は、発注者の了承を得た上で行うこと。

2 業務仕様

2-1 業務目的

本業務は、教育系ネットワークにおけるネットワーク機器、サーバ等の老朽化した機器を新しい機器に入替え、教育系システムの更新と情報セキュリティを向上させることを目的とする。

また、今後のクラウド利用を見据え、情報漏洩や外部からの攻撃、クラウドサービス利用のセキュリティリスクを低減、業務の効率化を行うため、ガイドラインに基づき、ネットワーク分離構成からアクセス制御方式であるゼロトラストセキュリティ構成に移行する。

2-2 システム更新

サーバ及びネットワーク機器類は、新しい機器に更新する。サーバシステムについては仮想基盤上に構築することを前提とし、導入する OS、ミドルウェア、ソフトウェア類は脆弱性対応がされた導入時の最新の安定バージョンとする。

なお、本業務で導入するハードウェア・ソフトウェアに関しては、設計書を参照のこと。

2-2-1 5年間の機器保証及びライセンス利用

特に指定がない場合、ネットワーク機器類、サーバ等のハードウェアに関しては、5年間の機器保証及び保守を含んで調達し、無償交換または、無償修理が可能であること。また今回導入するソフトウェアに関しても、正式稼動（リース開始日）より5年間のライセンス利用を含むこと。構築時より利用料金（ライセンス料金）が始まるものは、正式稼動までの利用料金（ライセンス料金）も含めて調達し、終了期間を統一すること。

2-3 現状調査

本業務は機器の入れ替えだけでなく、ゼロトラストを利用したシステム変更、サーバ室移転と大幅な変更が発生するが、利用者への影響は最小限とする必要がある。ネットワーク構成だけでなく、設定情報、データ・データベース情報、権限等のシステム構成も熟知し、緻密な計画が必要となるため、十分な現状調査と利用状況把握を行

い、調査結果を報告書として提出すること。

2-4 ネットワーク機器の更新

2-4-1 ネットワーク構成

本市の教育系ネットワークは、校務系、校務外部接続系、学習系（GIGA 系）で分離されているが、校務系と校務外部接続系を統合し、山梨県の校務支援システムとの接続には新しく構築するゼロトラストネットワークを経由して接続する構成にする。インターネットとの接続は、現行どおり教育情報セキュリティクラウドを継続利用する。

保守運用業務において、外部から接続が必要な場合には、教育情報セキュリティクラウドとの調整を行うが、必要機器、回線費用は本調達には含めない。

公民館については、開放系（インターネット、メール等）ネットワークが利用できるようにし、基本的にインターネット接続及び指定のファイルサーバのみ利用できるように設定を行う。また、無線 LAN アクセスポイント（以下「無線 AP」という。）を新たに設置し、開放系ネットワークにおいて無線 LAN システムが利用できるようにする。

笛川小においては、現在の無線 AP を、他学校と同様な機器に更新を行い、クラウド上から管理できるシステムへ移行する。

2-4-2 ネットワーク機器

情報センターにファイアウォール、メインレイヤ 3 スイッチを設置し、サーバ等接続のためのレイヤ 3 スイッチを設置する。メインレイヤ 3 スイッチからは本庁、牧丘支所、三富支所を接続する。また、9 学校と 7 出先施設についても接続する。本庁、牧丘支所、三富支所にはレイヤ 2 スイッチを設置する。牧丘支所からは 2 学校、2 出先施設を接続する。三富支所からは 1 出先施設を接続する。施設間の接続は 1Gbps にて行い、学校はスイッチに SFP (Small Form Factor Pluggable ; 光トランシーバ) を使って直接収容し、出先施設はメディアコンバータ（以下、「MC」という。）を使って接続する。

各学校、施設の既設レイヤ 2 スイッチも更新する。更新にあたっては、無線アクセスポイントが接続されているスイッチは、PoE（給電機能）に対応したスイッチを設置する。公民館については無線 AP を導入するため、既設レイヤ 2 スイッチを PoE（給電機能）に対応したスイッチに更新すること。

導入する機器は次の通りである。

1) ネットワーク機器一覧

No.	機器名称
1	アクセスゲートウェイ
2	メインレイヤ 3 スイッチ
3	サーバ用レイヤ 3 スイッチ
5	牧丘支所レイヤ 2 スイッチ
6	三富支所レイヤ 2 スイッチ
7	学校レイヤ 2 スイッチ A : 28pt
8	学校レイヤ 2 スイッチ B : 18pt
9	学校レイヤ 2 スイッチ C : 10pt
10	MC-A 公民館 : 9 台
11	MC-B 公民館 : 9 台
12	SFP モジュール A 支所 : 2 台、学校 11 台
13	SFP モジュール B 支所 : 2 台、学校 11 台
14	無線 AP
15	公民館無線 AP
16	公民館無線用ルータ
17	公民館レイヤ 2 スイッチ

2-4-3 ネットワーク機器仕様

1) アクセスゲートウェイ

仕様	<ul style="list-style-type: none"> ・ FortiGate 400F UTM プロテクション版 5 年パック (AV/IPS/Web フィルタ/スパム+FortiCare)同等以上を付帯 ・FortiGate 400F 平日先出しセンドバック保守 5 年以上付帯 ・ 各ネットワーク間の通信を制御すること ・ ファイアウォールを通過する全ての通信から脅威を排除すること
参考	Fortinet Fortigate 400F

2) メインレイヤ 3 スイッチ

仕様	<ul style="list-style-type: none"> ・ 10/100/1000BASE-T×24、SFP スロット×24、SFP/SFP+スロット×4 付帯 ・ デリバリースタンドアード保守 5 年以上付帯 ・ スタック構成とすること ・ 電源は冗長構成であり、電源ケーブル付帯
参考	AT-x930-28GSTX-N5

3) サーバ用レイヤ 3 スイッチ

仕様	<ul style="list-style-type: none"> ・ 10/100/1000BASE-T×24、SFP/SFP+スロット×4 付帯 ・ デリバリースタンドアード保守 5 年以上付帯 ・ スタック構成とすること ・ 電源は冗長構成であり、電源ケーブル付帯
参考	AT-x530L-28GTX-N5

4) 支所レイヤ 2 スイッチ

詳細	<ul style="list-style-type: none"> ・ 10/100/1000BASE-T×24、SFP/SFP+スロット×4 付帯 ・ デリバリースタンドアード保守 5 年以上付帯 ・ 電源は冗長構成であり、電源ケーブル付帯
参考	AT-x230-28GT-N5

5) 学校レイヤ 2 スイッチ

詳細	<ul style="list-style-type: none"> ・ タイプ A : 10/100/1000BASE-T×24 (PoE-OUT) ・ タイプ B : 10/100/1000BASE-T×16 (PoE-OUT) ・ タイプ C : 10/100/1000BASE-T×8 (PoE-OUT) ・ タイプ A : SFP スロット×4 付帯 ・ タイプ B、C : SFP スロット×2 付帯 ・ デリバリースタンドアード保守 5 年以上付帯
参考	タイプ A : AT-x230-28GP-N5 タイプ B : AT-x230-18GP-N5 タイプ C : AT-x230-10GP-N5

6) MC-A、MC-B

仕様	<ul style="list-style-type: none"> ・ 10/100/1000BASE-T/X MC ・ SMF1 心、2m～25km 伝送距離 ・ 1Gbps 通信対応 ・ イーサポート 10/100/1000bps 対応 ・ 情報センターについてはシャーシを導入
参考	本体：大電 DNS5810WS3E 及び DNS5810WS5E シャーシ：DNHD12E-2P-SNMPⅢ

7) SFP モジュール A、B

詳細	<ul style="list-style-type: none"> ・ 1Gbps 通信対応 ・ 1 芯シングルモードにて通信対応
参考	アライドテレシス AT-SPBD10-13-N5 及び AT-SPBD10-14-N5

8) 無線 AP

仕様	<ul style="list-style-type: none"> ・ Meraki MR46-HW 同等以上 ・ 5 年間ライセンス及びハードウェア保守付帯 ・ 笛川小で利用、クラウド管理可能
参考	Meraki MR46-HW

9) 公民館無線 AP

仕様	<ul style="list-style-type: none"> ・ メールアドレス、SNS アカウント、ID/Password 認証対応 ・ PoE 給電対応 ・ 5 年間ハードウェア保守付帯
参考	バッファロー FS-M1266

10) 公民館無線用ルータ

仕様	<ul style="list-style-type: none"> ・ 業務用ルータ ・ 5 年間先出しセンドバック保守付帯
参考	YAMAHA RTX1220

1 1) .公民館レイヤ 2 スイッチ

仕様	<ul style="list-style-type: none"> ・ PoE 給電対応 ・ 5 年間ハードウェア保守付帯 ・ 公民館の無線通信を集約し、市が別途契約している回線にて通信対応
参考	YAMAHA SWZ2310P-10G

2-5 サーバシステム等の更新

2-5-1 サーバシステム構成

新しいサーバシステムは仮想化基盤システムとして構築する。仮想化基盤の OS を稼働させるための仮想化ホストサーバは 3 台導入するが、1 台のサーバが故障しても、残るホストサーバで全ての仮想 OS を稼働させることができるよう、仮想化基盤を構築すること。また、現状調査に基づき、最適なサイジングを行うこと。

仮想基盤化ストレージは、仮想化基盤のシステムとデータを保管する重要な機器であるため、障害を検出し、かつ万が一の障害時にも継続運転可能な仕組みを構築すること。また、仮想化基盤ストレージの故障に備えて、仮想化基盤の OS のバックアップを定期的に自動取得すること。停電時は、市で用意する UPS からの電源供給が可能な構成とし、電源障害からシステムを保護できるようにすること。

2-5-2 物理サーバ

入替対象となる物理サーバは、次表の通りである。対象のサーバは、基本全て物理サーバとして構築すること。物理サーバは入替前と同等以上のサーバ機能を持ち、ユーザデータを保有する物に関しては、データ移行も行うものとする。また、今後数年間で見込まれるデータ量の増加などを考慮し、物理サーバのリソースは余裕をもって構築すること。

特に記述がない場合、OS が Windows サーバに関しては、ウイルス対策ソフトを導入すること。

No	サーバ名称	接続ネットワーク	備考等
1	仮想化ホストサーバ	管理系	ハイパーバイザー（最新安定版）3 台構成
2	仮想化基盤ストレージ A	管理系	

3	仮想化基盤ストレージ B	管理系	
4	教育系ファイルサーバ用ストレージ	教育系	Windows Server IoT 2022 for Storage
5	教育系バックアップ用ストレージ	教育系	Windows Server IoT 2022 for Storage
6	開放系ファイルサーバ用ストレージ	開放系	Windows Server IoT 2022 for Storage
7.	開放系バックアップ兼仮想バックアップ用ストレージ	管理系 開放系	Windows Server IoT 2022 for Storage

2-5-3 物理サーバ仕様

1) 仮想化ホストサーバ

仕様	<ul style="list-style-type: none"> ・ハイパーバイザーの最新安定版を導入する ・冗長構成とする ・仮想基盤サーバ間で仮想サーバを停止せず移動する <p>※下記で示すのは1台あたりの要件</p> <ul style="list-style-type: none"> ・PRIMERGY RX2530 M6 ラックベースユニット (3.5 インチ HDD/SSD×4) ・Xeon Silver 4310 プロセッサ (2.10GHz、12 コア、18MB)×2 ・CPU 搭載キット(2CPU 目)を含む ・インディペンデントモード設定サービスを含む ・メモリ-128GB(8GB 3200 RDIMM×16) ・RAID 設定サービス(RAID5)を含む ・内蔵 3.5 インチ BC-SATA HDD-1TB(7.2krpm) ×3 ・内蔵 DVD-ROM ユニット(Ultra Slim) ・SAS アレイコントローラカード(PRAID CP500i)(8 ポート/SAS 12Gbps) ・ファイバーチャネルカード(32Gbps) ・ポート拡張オプション(1000BASE-T×4) ・リモートマネジメントコントローラアップグレードを含む ・ライフサイクルマネジメントライセンスを含む ・電源ユニット(900W)[80PLUS Platinum 認証] ×2 ・電源ケーブル(AC100V 対応/1m)(NEMA 5-15P 準拠) ×2 ・ServerView Suite DVD(Tools) & ドキュメントを含む
----	---

	<ul style="list-style-type: none"> ・ラックレールキット(約 850mm) ・SupportDesk パック BIOS/ファームウェアアップデート・定期点検プラス(OS サポートなし)5 年付帯
概要	参考製品 : PRIMERGY RX2530 M6

2) 仮想化基盤ストレージ A

詳細	<ul style="list-style-type: none"> ・仮想化基盤サーバのストレージ領域として使用 <p>※冗長電源構成</p> <ul style="list-style-type: none"> ・ETERNUS DX100 S5 (2.5 インチ用) ・コントローラーモジュール (2CM, 32Gbit/s、FC、2 ポート、DX100 S5 用) ・増設ポート (32Gbit/s、FC、2 ポート→4 ポート、DX100 S5 用) ・マルチモードファイバチャネルケーブル(被覆有/5m) ×3 ・300GB/10krpm 2.5 インチ SAS ディスクドライブ×1 (DX100 S5/DX200 S5 用) ×24 ・AC100V 電源コード(NEMA 5-15P、3m) ・SupportDesk パック Standard(ETERNUS DX100 S5 用)5 年付帯
参考	ETERNUS DX100 S5

3) 仮想化基盤ストレージ B

仕様	<ul style="list-style-type: none"> ・仮想化基盤サーバのストレージ領域として使用 ・TeraStation TS51210RH シリーズ 10GbE 標準搭載 12 ベイ NAS パーシャルポピュレーテッドモデル 4 ドライブ ラックマウントモデル 8TB ・オンサイト保守 HDD 返却不要パック 保守 5 年 TS51210RH シリーズ用付帯
参考	TS51210RH0804

4) 教育系ファイルサーバ用ストレージ

仕様	<ul style="list-style-type: none"> ・ オンサイト保守 HDD 返却不要バック保守年数 5 年以上付帯 ・ 教育系ネットワークに接続 ・ Windows ファイル共有によるファイルサーバとして機能。入替時、現行サーバからデータ移行、アクセス権を引き継ぐ ・ 共有フォルダのパーティションは、Windows システム用とは異なる専用パーティションとする ・ 指定の時間帯にバックアップをとる ・ 利用可能なファイル容量等は発注者、学校担当者と協議を行い、最適な容量等を提案して決定する ・ メディアサーバについても構築すること
参考	WSH5420RN16S2

5) 教育系バックアップ用ストレージ

仕様	<ul style="list-style-type: none"> ・ オンサイト保守 HDD 返却不要バック保守年数 5 年以上付帯 ・ 仮想マシン、ファイルサーバ等のデータをバックアップする
参考	WSH5420RN16S2

6) 開放系ファイルサーバ

仕様	<ul style="list-style-type: none"> ・ オンサイト保守 HDD 返却不要バック保守年数 5 年以上付帯 ・ 開放系から利用する ・ Windows ファイル共有によるファイルサーバとして機能。入替時、現行サーバからデータ移行、アクセス権を引き継ぐ。 ・ 共有フォルダを配置するパーティションは、Windows のシステム用とは異なる専用のパーティションとする ・ 指定の時間帯にバックアップをとる
参考	WSH5420RN16S2

7) 開放系バックアップ兼仮想バックアップ用ストレージ

仕様	<ul style="list-style-type: none"> ・ オンサイト保守 HDD 返却不要バック保守年数 5 年以上付帯 ・ ファイルサーバや仮想マシン等データをバックアップする
参考	WSH5420RN16S2

2-5-4 仮想化基盤上にて稼働するサーバシステム

入替対象となるサーバシステムは、次表の通りである。対象のサーバは全て仮想化基盤上に構築すること。また入替前と同等のサーバ機能を持ち、ユーザデータを保有するシステムに関しては、データ移行を行う。また、今後数年間で見込まれるデータ量の増加などを考慮し、仮想化サーバ上のリソースは余裕をもって構築すること。また、ウイルス対策ソフトを導入すること。

No	サーバ名称	接続ネットワーク	備考等
1.	プロキシサーバ (i-FILTER)	教育系 開放系	Windows Server2022 又は Linux 8.x / 9.x(安定版)
2.	メールセキュリティサーバ (m-FILTER)	開放系	Windows Server2022 又は Linux 8.x(安定版)
3.	内部 Web サーバ	教育系 GIGA 系	Windows Server2022
4.	外部 DNS 兼メールサーバ	教育系 開放系	Linux 8.x / 9.x(安定版)
5.	AD (ActiveDirectory) 兼 DHCP サーバ 1	教育系	Windows Server2022
6.	AD 兼 DHCP サーバ 2	教育系	Windows Server2022
7.	開放系用 AD 兼 DHCP サーバ 1	開放系	Windows Server2022
8.	開放系用 AD 兼 DHCP サーバ 2	開放系	Windows Server2022
9.	アカウント管理兼バック アップサーバ	教育系	Windows Server2022
10.	仮想バックアップサーバ	管理系	Windows Server2022
11.	ゼロトラスト認証サーバ	教育系	Windows Server2022
12.	教育系 WSUS サーバ	教育系	Windows Server2022
13.	開放系 WSUS サーバ	開放系	Windows Server2022
14.	教育系資産管理サーバ	教育系	Windows Server2022
15.	開放系資産管理サーバ	開放系	Windows Server2022
16.	プリントサーバ	教育系	Windows Server2022

17.	グループウェア	開放系	Windows Server2022 desknet's NEO
18.	カロリーメイク	教育系	Windows Server2022
19.	監視サーバ	管理系	Linux 8.x / 9.x(安定版)
20.	仮想化基盤管理サーバ	管理系	専用 OS

2-5-5 仮想化基盤サーバ

1) プロキシサーバ (i-FILTER)

仕様	<ul style="list-style-type: none"> ・ 教育系、公民館のプロキシサーバとして機能する ・ Web ページのキャッシング及び Web ページのフィルタリング（閲覧規制）として機能 ・ i-FILTER の既設設定を引き継ぐ ・ i-FILTER 用の証明書を作成し、各端末に配布する
参考	i-FILTER Ver.10

2) メールセキュリティサーバ (m-FILTER)

仕様	<ul style="list-style-type: none"> ・ 公民館用のメールサーバとして構築する ・ 通過するメールすべてをアーカイブする ・ アーカイブしたメールは保守期間内保持する ・ 添付ファイルはパスワード付き圧縮ファイルにできる ・ スпамメール対策を行う
参考	m-FILTER Ver.5

3) 内部 Web サーバ

仕様	<ul style="list-style-type: none"> ・ 教育系、GIGA 系の Web サーバとして機能する ・ 指導者用デジタル教科書をインストール及び配信する
参考	内部 Web サーバ

4) 外部 DNS 兼メールサーバ

仕様	<ul style="list-style-type: none"> ・教育セキュリティクラウドのセカンダリ DNS 及びメールサーバとして機能する ・NTP サーバとして機能する
参考	外部 DNS ・ メールサーバ

5) AD (ActiveDirectory) 兼 DHCP サーバ 1

詳細	<ul style="list-style-type: none"> ・教育系のドメインコントローラとして機能し、ユーザ管理・コンピュータ管理、ポリシー管理を行う ・クライアントコンピュータのメイン DNS サーバとして機能する ・クライアントコンピュータの DHCP サーバとして機能する ・ファイルサーバの共有資源に関するアクセス制限を設定する ・既存の設定を引き継ぐが、アカウントに関しては端末に紐づいているアカウントを利用者に紐づくアカウントに変更する ・利用者アカウントの詳細については、教育委員会と協議して決定すること。
概要	教育系 ActiveDirectory ・ DNS ・ DHCP サーバ

6) AD 兼 DHCP サーバ 2

仕様	<ul style="list-style-type: none"> ・AD 兼 DHCP サーバ 1 のセカンダリとして動作 ・DNS サーバ ・DHCP サーバ
参考	教育系セカンダリ ActiveDirectory ・ DNS ・ DHCP サーバ

7) 開放系 AD 兼 DHCP サーバ 1

仕様	<ul style="list-style-type: none"> ・開放系（公民館）のドメインコントローラとして機能、ユーザ管理・コンピュータ管理、ポリシー管理を行う ・クライアントコンピュータのメイン DNS サーバとして機能する ・クライアントコンピュータの DHCP サーバとして機能する ・ファイルサーバの共有資源に関するアクセス制限を設定すること ・既存の設定を引き継ぐこと
参考	公民館用 ActiveDirectory ・ DNS ・ DHCP サーバ

8) 開放系 AD 兼 DNS 兼 DHCP サーバ 2

仕様	<ul style="list-style-type: none"> ・ 開放系（公民館）AD 兼 DHCP サーバ 1 のセカンダリとして動作 ・ DNS サーバ ・ DHCP サーバ
参考	公民館用セカンダリ ActiveDirectory ・ DNS ・ DHCP サーバ

9) アカウント管理兼バックアップサーバ

仕様	<ul style="list-style-type: none"> ・ 教育系ファイルサーバをバックアップする ・ Active Directory 管理機能として、ADMS（ID 統合管理ソフトウェア）を導入、教育系サーバの ID 統合管理する ・ ADMS の設定及び運用方法等については、発注者との協議の上決定する。次に設定を実施すること <ul style="list-style-type: none"> ① 導入するファイルサーバ、プロキシサーバと連携する ② 人事異動時に必要なグループ、ユーザ情報を事前登録し、指定した日時に Active Directory に反映させること ③ CSV ファイルによるグループ、ユーザ情報の追加・変更・削除ができる ④ Active Directory への反映時に、アクセス権の猶予期間を設定でき、猶予期間中はファイルサーバ上の異動前、異動後のフォルダの両方にアクセスできる ⑤ 他システムとの ID 連携を考慮し、任意のフォーマットでの CSV ファイルを出力できる
参考	ADMS（アカウント管理） Acronis Cyber Protect Standard Server（バックアップ）

10) 仮想バックアップサーバ

仕様	・ システム障害に備えるため仮想システムのバックアップを定期的に行う
参考	Acronis Cyber Protect Standard Server

1 1) ゼロトラスト認証サーバ

仕様	<ul style="list-style-type: none"> ・ゼロトラストネットワーク（以下、ZTNA という）を構成する <p>※ZTNA は、ユーザが利用する各種システムへのアクセス前にユーザ ID による利用者の認証及び権限の確認、教員端末に対する正常性の検証の確認をアクセス毎に行う。それにより必要最小限の権限を付与し、利用するアプリケーションが内部、クラウド等のどこにあっても、安全かつ容易にシステムを利用できる環境を提供する仕組み</p> <ul style="list-style-type: none"> ・アクセスゲートウェアと連携してゼロトラストネットワーク制御を行う ・アクセス制御の認証は端末ログオン時の情報を利用し、通信ごとに自動で行う ・アカウント管理システムと統合したエンドポイントの管理をする ・アクセス先及びアクセスプロトコルに応じて認証方法（多要素認証、リスクベース認証等）を追加する
概要	FortiGate(FortiOS)、FortiClient

1 2) 教育系 WSUS サーバ

仕様	・教育系クライアントの Windows Update サーバとして動作する
参考	教育系 WindowsUpdate 管理サーバ

1 3) 開放系 WSUS サーバ

仕様	・開放系クライアントの Windows Update サーバとして動作する
参考	開放系 WindowsUpdate 管理サーバ

1 4) 教育系資産管理サーバ

仕様	<ul style="list-style-type: none"> ・教育系ネットワークのサーバ、クライアントの資産情報を管理する ・ログ監視を行う ・ログの保存期間は 2 年間以上 ・運用ルールにより許可されたデバイスのみ使用できるように設定する
----	---

参考	SKYSEA Client View
----	--------------------

1 5) 開放系資産管理サーバ

仕様	<ul style="list-style-type: none"> ・開放系ネットワークのサーバ、クライアントの資産情報を管理する ・ログ監視を行う ・ログの保存期間は2年間以上 ・運用ルールにより許可されたデバイスのみ使用できるように設定する
参考	SKYSEA Client View

1 6) プリントサーバ

仕様	・教育系ネットワーク上の学校配置プリンターを管理する
参考	教育系プリントサーバ

1 7) グループウェアサーバ

仕様	<ul style="list-style-type: none"> ・開放系ネットワークに接続し、公民館用グループウェア、メーラーとして利用できる ・既存のグループウェア（desknet's NEO）の設定、アカウント情報を引き継ぐ ・LGWAN メール及び所定のドメインメールが送受信できるように設定を行う ・公民館サーバ関連のデータをバックアップする
参考	desknet's NEO

1 8) カロリーメイク

詳細	<ul style="list-style-type: none"> ・給食センターにて利用できること ・既存のデータ、環境を引き継ぐ
参考	カロリーメイク 最新センター版

19) 監視サーバ

仕様	<ul style="list-style-type: none"> ・ネットワーク機器及びサーバ機器のシステム監視、リソース監視用として機能する ・ネットワーク管理・アプリケーション監視が機能する ・Zabbixを導入し、既設設定を可能な限り引き継ぐこと ・新規導入機器のリソース・ステータス状態等を監視し、しきい値を超えた場合や障害を検知した場合、通知させること
参考	監視サーバ

20) 仮想化基盤管理サーバ

仕様	<ul style="list-style-type: none"> ・仮想化基盤サーバ及び仮想 OS を管理する ・当サーバの障害に備えて、必要な設定・データ等はバックアップを取得する
参考	仮想化基盤管理サーバ

2-5-6 情報セキュリティ関連ソフト等の導入

教育系システム、開放系システムにおいては、クライアントのウイルス対策ソフト管理機能、Windows Update 管理機能等を導入し、情報セキュリティとして機能するように構築すること。開放系についてはメールのスパム対策の機能を導入すること。

2-6 システムのデータ移行

各サーバシステムの項目において、ファイルサーバについては、既存データを新環境に移行すること。移行に際しては、全てのデータを移行するのではなく、必要なデータのみを移行する方法を発注者と協議して実施すること。

2-7 Microsoft365 A5

Microsoft365 A5 に含まれる様々な機能及びゼロトラストセキュリティの基盤として利用できる認証基盤の設定及び運用管理を行う。

具体的には、多要素認証、リスクベース認証、シングルサインオン、モバイル端末管理、アンチウイルス、データ暗号化アクセス、EDR、SIEM の機能を実現する。

- Microsoft365 テナントは教育委員会と協議して決定すること。
- 管理操作は Web ブラウザ上若しくは PowerShell から設定、情報収集すること。
- アラート機能としてメールの送信等で発呼すること。
- 多要素認証及び SSO（シングルサインオン）機能を適用すること。
- SSO は、基本的に教員端末へのログオン時の認証情報を利用して、その後の Web システム等へのログイン、アクセス制御での認証を行うこと。
- 教職員の利便性向上、負担軽減のため、認証回数は必要最低限になるように SSO を構成すること。
- 利用する教職員用に MS 365 SharePoint を利用して、各種情報共有（FAQ）サイトやファイル等を掲示できる電子掲示版等が機能するポータルサイトを構築すること。

2-7-1 Microsoft Entra ID（旧 Azure ActiveDirectory）

- Microsoft365 A5 に含まれる Active Directory 機能と、本調達で構築する Active Directory との資格情報連携を行い、シングルサインオンで Microsoft365 を利用できるように設定すること。
- 本人確認を厳密に行えるようにすること。
- 条件付きのアクセス制御とすること。
- 不正 ID の異常検出、ID の自動保護、管理者 ID の監視をすること。
- ID 防御機能により、リスクレベルによって自動対処されるようにすること。
- 匿名 IP からのアクセスや、複数回のログイン失敗等不正アクセスの疑いがある事象を検知し、多要素認証を要求する等の自動対処機能を設定すること。
- アカウント漏洩の疑いがある事象を検知し、パスワードリセットを要求すること。
- 管理者ユーザ又は管理者ユーザを乗っ取った第三者が管理者権限を濫用しないよう、管理者権限を有効化する際に他者の承認を求めたり多要素認証を求めたりする等の安全手段を設定すること。
- 生徒情報については、現状の登録を維持すること。

2-7-2 Microsoft Exchange Online

- ・ Microsoft365 A5 に含まれる Exchange Online 機能を利用し、市が指定する、独自ドメインによるメールの送受信を設定すること。
- ・ メール送受信内容をアーカイブし、必要に応じて参照できること。
- ・ アーカイブはサーバ室内にて保存すること。
- ・ 学内だけではなく、学外においてもメールの送受信ができること。

2-7-3 Microsoft Intune

- ・ Microsoft365 A5 に含まれる Microsoft Intune 機能を利用し、端末の資産管理及びモバイルデバイス管理（MDM）をすること。
- ・ モバイルデバイス管理が強制できないデバイス等でも安全に業務データを利用できるように、デバイス上のアプリケーションに対して、データを個人の領域に保存させない、コピー&ペーストを無効化する等の制限を設定すること。
- ・ Windows を使用するデバイスについて、OS のバージョン、パスワードの設定、ロックの設定、脱獄等の状態を監視し、違反した場合アクセスをブロックすること。
- ・ 教育系ネットワークに接続する端末は全て登録し、管理すること。

2-7-4 Windows Defender 及び Advanced Threat Protection

- ・ Microsoft365 A5 に含まれる Windows Defender 機能を利用し、ウイルス対策、除去をすること。
- ・ Microsoft365 A5 に含まれる Windows Defender Advanced Threat Protection 機能を利用し、高度な攻撃からの保護、検出、対応をすること。
- ・ 端末のふるまいを検知して脅威の検出をすること。
- ・ Exploit Guard で脆弱性、マクロ悪用対策、ネットワーク保護をすること。
- ・ Cloud Protection で未知のマルウェア検出が行えるようレプテーションチェックをすること。
- ・ 各端末の脆弱性情報を確認すること。
- ・ 検出した脅威を可能な限りリモートで除去すること。
- ・ 脅威が検出された端末を管理ポータル操作により遠隔でネットワークから隔離すること。
- ・ ふるまい検知機能と標的型メール対策システムは、連動して動作させること。

2-7-5 Microsoft 365 Security Center

- Microsoft365 A5 に含まれる Security Center 機能を利用し、全てのセキュリティ動作を一括して管理できるように統合セキュリティプラットフォームを構成すること。
- アカウント、エンドポイント、メール、アプリ、データ等のアラート全て自動的に相関分析を行い、関連するものを 1 つのインシデントとして提示されるように設定すること。
- インシデントの自動調査及びアカウント、エンドポイント、メール、アプリ、データ等の各レイヤでの自動対処ができるようにすること。

2-7-6 Microsoft Purview Information Protection

- Azure Information Protection 機能を利用し、機微ファイルの保護をすること。
- ファイルに重要性分類ラベル付けと暗号化をすること。
- ファイルに編集、コピー、印刷の不可設定、透かし文字の挿入、有効期限の設定ができるようにすること。
- ラベル付けしたファイルの追跡と閲覧権限のリモート失効ができるようにすること。
- 保護対象のメールやファイルを共有する相手を指定して保護及び暗号化することができ、ファイル毎のパスワードではなく、利用者自身の ID を用いて認証することで復号化すること。
- Outlook、Word、Excel、PowerPoint 等各種 Office で扱うデータや PDF ファイルについて閲覧や編集だけでなく、印刷や部分的なコピー等についても操作を制御すること。
- 組織外のユーザに対しても保護及び暗号化したメール及びファイルを共有できること。
- 指定した保護対象のファイルを追跡管理ができ、誰がいつ、どの IP アドレスで開いたか等の状況を確認すること。
- 指定した保護対象のファイルを共有後であっても共有を取り消し、閲覧等できなくすること。
- 組織で定義したラベルを使用してファイルやメールを分類でき、分類されたファイルやメールは視覚的に分かり易くラベルが表示されること。適切な扱いを促せること。
- メール添付ファイルは、Microsoft365 A5 の DLP ポリシー設定にて、個人情報を含んでいる場合は、ブロック又は上長の承認後、送付されるように設定すること。

2-7-7 クラウドサービスセキュリティ (Microsoft Defender for Cloud Apps)

- API 連携により、統合的に他 SaaS を含めた利用状況の監視をすること。
- ネットワーク機器のログ等から認められていない SaaS 利用やリスクのある SaaS アプリをカタログとのマッチングにより検出すること。
- 大量のデータのアップロード・ダウンロード・削除・変更しているユーザを検出しアラートの上、アカウントを停止できること。
- 対応 SaaS 上に置かれた複数のメールアドレス等の個人情報が含まれたファイルや機密に分類されているファイルを検出し、アラートの上、ファイルを非公開化すること。
- 対応 SaaS 上に置かれた許可されていない個人のメールドメインや競合他社に共有しているファイル、匿名で全員に共有されているファイル、長期間共有されたままになっているファイル等を検出し、アラートの上、ファイルを非公開化すること。
- 管理ユーザが、特定の IP アドレス範囲カテゴリに含まれない IP アドレスから管理操作を行った場合にアラートの上、操作内容を精査すること。
- ランサムウェア検知ポリシーにより、API 連携しているクラウドストレージから特徴的なファイルの拡張子を見つけて、感染ファイルとユーザを検知・把握すること。
- API 連携しているクラウドに特定のラベルが付与されたファイルがアップロードされたことを検出し、非公開化できること。
- API 連携しているクラウドからファイルをダウンロードする際、ファイルに情報保護のための分類ラベルを付与すること。

2-7-8 その他機能

- Microsoft365 クラウドへのアクセスを条件付き（場所、デバイス、利用目的、利用機能）で制御すること。
- 個人用のファイル領域として、OneDrive を利用できるようにすること。
- Microsoft365 A5 に含まれるその他機能（OneNote Class Notebook、Teams、Forms、Photo、Stream、Minecraft、MyAnalytics、Workplace Analytics、PowerBI 等）についても、教育委員会と協議の上利用できるようにすること。

1) 運用要件

- Microsoft365 A5 はクラウドサービスとして提供されているため、日々内容が更新されている。したがって、Microsoft より提供される機能変更内容メール

(Major Change Update Notification) や WEB 上の情報を参照の上、機能アップグレードに追従すること。

- ・ 機能アップグレードや更新についての最新情報を必要に応じて当該利用者に対しアナウンス等を行うこと。
- ・ 機能アップグレード等によりシステム設定等の軽微な変更が必要な場合は対応すること。

2) 教育用ツールとしての活用検討

- ・ Microsoft365 A5 では、Teams や Skype、マイクラフト等、教育用ツールとして利活用可能な機能が提供されている。したがって、それら機能を教育に活かせるよう検討するとともに、研修会等で活用方法を提示する等、教育力の向上を支援すること。

2-8 システム構築後の総合テスト

受注者は、構築したシステムが正常に稼働していること、システムの冗長部が正常に機能していることなどを試験すること。

引渡前には、発注者立ち会いのもとで総合テストを実施し、試験結果に対する承認を得ること。

2-9 サーバ室移転

現行システムのサーバ機器類は、山梨市情報通信センターのサーバ室内にて稼働しているが、令和 6 年度内においてサーバ室を本庁舎内へ移転する予定である。

ただし、サーバ室の完成時期がケーブル類の納入遅延にて具体的に決まっていない。そのため本業務においては、賃貸借開始日前に、一度、山梨市情報通信センター内で仮稼働させ、サーバ室完成後に移転させる。この移転作業についても本業務にて対応すること。

2-10 システム切替

サーバ室移転作業があるため、新旧システムの切替方法については、受注者と協議して実施する予定である。想定では新旧システムの並行稼働は実施せず、全システムの切替を 1 日程度で実施する予定である。但し、ネットワーク機器類においては引越

し前後及び切替前後において設定変更作業があることに留意すること。

2-1-1 端末設定

別途業務等において、教育系で利用する端末を 400 台程度調達する。この端末設定も別途業務（別途契約）として実施する想定である。その際、学校の事務職員においては、行政系システムの財務会計システムが利用できるようにすること。端末設定だけでなく、現在も実施しているレイヤ 3 スイッチ等におけるネットワーク経路も作成すること。

2-1-2 図書館システム端末設定

現在利用している図書館システムを継続して利用できるように、上記端末と同様に設定を行うこと。また現在は 1 台の端末で利用しているが、各学校に 2 台配置し、司書端末と利用者端末に分けて、情報セキュリティに配慮した利用方法に変更すること。

2-1-3 既存機器の撤去・廃棄

既存ネットワーク及びサーバシステムで不要となる機器については、受注者において撤去し、指定の方法で廃棄を行うこと。

継続利用可能な機器については発注者と協議し、発注者が指示する方法にて保管すること。

3 保守運用業務

ネットワーク及びサーバシステム構築後、新しいシステムの保守運用業務を実施すること。保守運用に関しては、次の内容を実施すること。

3-1 保守サービスの条件

3-1-1 ハードウェア保守サービス

- 1) 正常に動作しない場合には、速やかに修理すること。ただし、天災・使用者の故意または過失による場合は除く。
- 2) 修理・交換に長期間を要する場合は、同等スペックの代替機を用意し、現状の復旧を行うこと。

- 3) 故障した部品、機器の修復費用も含むこと。
- 4) サーバ室のネットワーク機器に関しては、必要に応じて機器の調整、機器のクリーニング等を行うこと。
- 5) 対象学校施設における既設の『端末保守』、『プリンタ保守』については、一次切り分け作業までを実施（不良箇所を推定）すること。

3-1-2 システム保守サービス

- 1) サポート専用の受付窓口を設けること。受付時間は下記保守期間・保守対応時間項目を参照のこと。それ以外の時間帯は、メール、FAX 等による対応ができること
- 2) 担当職員より障害の連絡があった場合、もしくは監視装置にて障害を検知した場合には、速やかに電話、メール等で連絡を行い、遠隔または現地にて対応を行う。対応には設定情報の消失に対する復旧作業を含むものとする。
- 3) 故障した部品、機器の修理はオンサイトを原則として対応する。
- 4) 契約時及び設定変更時における機器の設定情報のバックアップを取り保管・管理を行う。
- 5) 各システムを構成する装置、環境設定に基づくソフトウェア中のエラーの特定及び解決を行う。
- 6) メーカーから提供されるセキュリティパッチ等のプログラムを、事前の動作検証を行った上でインストールする。
- 7) 人事異動による機器設定が必要な場合は速やかに対応を行い、ADMS によるサーバでのユーザの設定作業、端末への設定作業、サーバ上での設定作業を含む。運用上必要な作業は全て行うこととする。
- 8) 職員、教員等の増減員による機器設定が必要な場合は速やかに対応を行い、ADMS によるサーバでのユーザの設定作業、端末への設定作業も行う。
- 9) 人事異動等による機器設定変更があった場合、教育委員会及びデジタル戦略推進担当と情報を共有すること。
- 10) 電気設備の定期点検等で停電及びシステムの停止等が想定される場合は、停電前（システム停止前）及び停電復旧後（システム起動後）において、必要に応じて、現地にて対応を行うこと。
- 11) システム構成等に変更があった場合は、系統図等を常に最新の状態に維持管理すること。

3-1-3 運用体制

運用保守を行う者の体制表を作成し、本市の承認を得ること。その際、体制表には次の者をメンバーに加えること。

- 1) プロジェクト責任者
- 2) 主任技術者（プロジェクトマネージャー）
- 3) 情報セキュリティ・品質管理担当者
- 4) プロジェクトリーダー

また上記メンバーの変更を行う場合は、理由書等を提出して本市の承認を得ること。

3-2 システム保守支援要員（SE）の派遣

必要に応じ教育委員会と連携して、サーバ室及び市内の小中学校、出先機関にて対応を行うこと。

3-3 保守作業報告

保守を実施した内容及び前述の作業内容について、月次管理レポート（作業内容、対応状況、課題一覧等）を作成し、毎月報告会を開催し、関係者に説明を行うこと。またシステム変更等があった場合は、最新の情報（システム構成図等）を提示すること。年度末には1年間の資料を図書として提出すること。

原則として本市において作業を行った場合は、迅速に作業報告書を提出すること。

3-4 保守期間・保守対応時間

- ・ 保守期間 令和6年10月1日からの令和11年9月30日とする
- ・ 保守時間 平日8:30～17:30とする

ただし、協議の上緊急を要すると判断された重大な障害、情報セキュリティインシデントの対応は上記に限らず、対応すること。現地にて対応する際は、障害発生から現地到着までの時間は60分以内を目標とする。

3-5 緊急措置対応

本件システムにおいて不正侵入、クラッキング等の重大な情報セキュリティインシデントが認められた場合、速やかにサーバの停止やインターネット切断など必要な緊急措置を行うこと。

3-6 保守対象機器

保守対象機器は、今回導入する機器、別紙の端末、各学校所有のプリンタを対象とする。今回導入したソフトウェア類も対象に含むものとする。また、保守期間の間に施設等の増減があった場合は、その施設等の機器及びソフトウェアについても保守対象とする。

3-7 クラウドサービス（Microsoft 365 A5）の監視・保守について

クラウドサービスの運用に当たり次の業務を行い、定例会等において作業結果報告すること。

3-7-1 サービス健全性の定期的な確認

- ・ 環境が安全な状態に保たれていることを担保するために、以下の確認を定期的に行うこと。実行間隔については、発注者と望ましい間隔を協議の上、決定すること。
- ・ 脆弱性の高低、緊急性の高低等に関する基準値については、発注者と望ましい値を協議の上、決定すること。
- ・ 次に指定する機能名や画面名はセキュリティ管理ツールのアップデートに伴い変更される可能性があることに留意し、同等の目的を実現する機能に適宜読み替えて実施すること。
 - ・ サービス全般の状況確認（Microsoft 365 Defender）
 - ・ Microsoft 365 Defender 管理画面＞セキュリティスコア
 - ・ Microsoft セキュリティスコアの概要からセキュリティスコアがある程度のスコアになっていることを確認すること。
 - ・ ID、アプリ、デバイス、データの各カテゴリに提示されている「おすすめの操作」を確認して、必要な対処を講じること。
 - ・ 端末の健全性の確認（Microsoft Defender for Endpoint）
 - ・ メール通知設定より、新たな脆弱性や脆弱性の悪用が報告された際にセキュリティ担当者又は受注者が指定した者にメールでの通知が行われるように設定をすること。
 - ・ Microsoft 365 Defender 管理画面 ＞ 脆弱性の管理 ＞ ダッシュボードから、露出スコアがある程度の数値以下になっていることを確認すること。
 - ・ Microsoft 365 Defender 管理画面 ＞ 脆弱性の管理 ＞ 推奨事項 から、脆弱性を低下させるための推奨される対処について緊急性の高いものがないか確認すること。

- ・ Microsoft 365 Defender 管理画面 > 脆弱性の管理 > 在庫 から、インストールされているアプリケーションのうち、脆弱性が高く、対処の緊急性が高いものがないか確認すること。
- ・ クライアント管理システムにて、Windows defender と連携して、検知・遮断時にアラート通知及びログを取得すること。
- ・ クライアント管理システムにて、PC の利活用のログをレポート化し、利用者各自の端末利用状況を定期的に可視化すること。

3-7-2 その他運用管理

- ・ 運用管理にあたり、最新の図面、構成図、管理台帳等を整備、リスト化すること。また、運用に関する手順書（パスワード管理、アクセス権、ID 管理、アカウント命名方法等）も整備し、準備されていないものは作成又は作成支援をすること。
- ・ ネットワークに接続する端末（教職員一人一台端末等）は全て Intune へ登録し、管理すること。

3-8 ドキュメント等の管理

- ・ システム更新が発生した場合にはネットワーク図面、システム構成図及び機器等の管理台帳等を修正し、最新の状態を維持・管理すること。
- ・ 各学校の図面（配線図、系統図等）を管理すること。学校でネットワーク構成等の変更があった場合には図面に反映させ、最新の状態を維持・管理すること。毎年最新データであるかを確認し報告すること。
- ・ 最新のドキュメントはファイルサーバ内に共有スペースを作成し、教育委員会等が常に確認できる状態にすること。
- ・ 次の数量等について管理台帳を作成し、学校毎に数量等を確認できるようにすること。
 - ✓ 利用しているライセンス数（職種ごと集計）
 - ✓ アカウント数（利用用途、職種ごと集計）
 - ✓ 端末情報と台数、ソフトウェアの種類・バージョン、利用者情報（職種）、付属品
 - ✓ プリンタ、設置場所、台数
 - ✓ スイッチ・無線 AP 配置図、ラック図
- ・ 管理台帳や図面等は、1 年に最低 1 回は現状確認を行い、定例会等において確認した内容を報告すること。

3-9 情報セキュリティ研修の実施

受注者は毎年、市内の教職員等を対象とした情報セキュリティ研修を毎年（午前、午後の２回）実施すること。情報セキュリティ研修の内容については、担当者と協議を行い、内容を確定させること。本業務内の費用内において実施すること。講師は外部の専門員を利用することも可とする。

3-10 最新情報の共有

報告会等においては、ICT の最新情報や他自治体等の取り組みに関しても、最新情報の提供も行うこと。また報告会や打合せ等においては、ペーパーレス化を図った会議とすること。その際、必要となるハードウェア、ソフトウェアは本業務に含めて調達すること。

3-11 教育情報化推進会議への参加

今後、本市において実施予定である教育情報化推進会議に、必要に応じて参加すること。その際、本市より必要書類、運用ルール等の情報提供や説明依頼があった場合は、これに対応すること。

(別紙 1)

対象学校の端末台数 (1 月現在)

NO	学校名	教師用端末	PC 教室端末
(1)	加納岩小学校	34	—
(2)	日下部小学校	37	—
(3)	後屋敷小学校	25	—
(4)	日川小学校	19	—
(5)	山梨小学校	23	—
(6)	八幡小学校	21	—
(7)	岩手小学校	16	—
(8)	笛川小学校	22	—
(9)	山梨南中学校	38	41
(10)	山梨北中学校	41	41
(11)	笛川中学校	22	38
(12)	給食センター	6	—
(13)	教育委員会	2	—
	合計	301	120

※教職員端末は共有端末 1 台を含む

※中学校は入試用端末 1 台を含む

※PC 教室は中学校のみ

(別紙2)

開放系ネットワーク施設と端末台数

NO	施設名	端末台数
(1)	加納岩公民館	1
(2)	日下部公民館	2
(3)	後屋敷公民館	1
(4)	日川公民館	1
(5)	山梨公民館	1
(6)	八幡公民館	1
(7)	岩手公民館	1
(8)	諏訪公民館(牧丘支所内)	1
(9)	中牧公民館	1
(10)	西保公民館	1
(11)	三富公民館(三富支所内)	1
(12)	生涯学習課	1
	合計	13