令和7年度校務 NW 更新事業 【長期継続契約】

仕様書

目 次

1. 本仕様書の目的・総則

本仕様書は、藤井寺市教育委員会の『教育ネットワーク構築業務』に求められる仕様を取りまとめて、構築における用品や構築仕様を定義したものである。
本仕様書は市の調達する物件に適用する。なお、本仕様に示す物件の仕様等について主要事項を示したものであり、明記されていない事項であっても、物件が当然備えるべき事項については含まれるものとする。

2. 構築業務の目的および計画

藤井寺市教育委員会では、以下を目的として構築業務をおこなうこととする。
① 既設サーバの老朽化対策
② ネットワーク一元管理と業務継続性対策

本仕様書では、上記についての仕様を定義するものとする。

3. 賃貸借契約

3.1 賃貸借契約

本業務の契約形態は、5 年間の長期継続による賃貸借とし、以下の期間とする。賃貸借期間終了後は、ハードウェア、ソフトウェア、ライセンス等を全て含むシステム一式を市に無償譲渡するものとする。
支払いは、月額によるものとし、支払い手続きは当市財務規則に従うこととする。
第三者賃貸借方式による契約を希望する場合は、別紙「第三者賃貸借方式による貸付能力等証明書」を提出し、自らが貸付能力を有するとともに、第三者をして貸付できる能力を有することを証明すること。
2026 年 7 月 1 日～2031 年 6 月 30 日
保守料（2026 年 7 月～2031 年 6 月）については代理回収とする。

4. 業務期間

4.1　業務期間

4.1.1業務スケジュール

3.1 項賃貸借期間の開始日までに本システムの構築を完了すること。業務スケジュールは以下とするが詳細な日程については市と協議の上決定することとする。

①	公示・業者決定	2025 年 10 月～
②	契約	2025 年 12 月
③	要件定義・基本設計・詳細設計	2026 年 1 月初旬～3 月初旬
④	サーバシステム設定・搬入設置・切り替え	2026 年 3 月中旬～6 月中旬
⑤	ネットワーク設定・搬入設置・切り替え	2026 年 3 月中旬～6 月中旬
⑥	検収、完成処理	2026 年 6 月下旬
⑦	実運用、運用フォロー	2026 年 7 月 1 日～

4.1.2構築作業工期

2026 年 1 月 ～ 2026 年 6 月 30 日（火）

5. 業務概要

5.1　構築作業概要

5.1.1納入場所・作業実施場所

以下に調達用品の納入をおこない、作業を実施するものとする。

①	藤井寺市役所	大阪府藤井寺市岡 1 丁目 1 番 1 号

5.1.2導入機能と必要数量

導入機能および必要数は下表のとおりとする。各機能の詳細仕様については、「6 項　システム仕様」にて後述する。

表 5.1.2 導入機能と新設・移行仕様

項番	サーバ機能	設置場所	数量	構成分類	新設・移行種別
1	ActiveDirectory	本庁	2	仮想サーバ	既存システムからのデータ移行
2	仮想化基盤サーバ	本庁	2 以上	物理サーバ	新設
3	仮想化基盤ストレージ	本庁	1	物理機器	新設
4	バックアップサーバ	本庁	1	物理サーバ	新設
5	WSUSサーバ	本庁	1	仮想サーバ	既存システムからのデータ移行
6	ファイルサーバ	本庁	1	仮想サーバ	既存システムからのデータ移行
7	資産管理システム	本庁	1	仮想サーバ	既存システムからのデータ移行
8	WEB フィルタリングシステム	本庁	1	仮想サーバ	既存システムからのデータ移行
9	監視システム兼 NTP	本庁	1	仮想サーバ	既存システムからのデータ移行
10	無停電電源装置	本庁	必要数	物理機器	新設
11	KVM	本庁	1	物理機器	新設
12	UTM	本庁	2 以上	物理機器	既設機器の更改
13	基幹スイッチ（10G 対応）	本庁	2 以上	物理機器	既設機器の更改
14	インターネット接続用スイッチ	本庁	2 以上	物理機器	既設機器の更改
15	拠点接続用ファイアーウォール	本庁	1	物理機器	既設機器の更改
16	本庁フロアスイッチ	本庁	2 以上	物理機器	既設機器の更改
17	ネットワークログ管理システム	本庁	1	物理機器	既設機器の更改

5.1.3主要工程

表 5.1.3 主要工程

主要工程	数量	単位
現地調査	1	式
全体基本設計・移行設計	1	式
プロジェクト管理・運営	1	式
【本庁】 仮想化基盤サーバの設計、設定、搬入設置、試験 仮想化基盤ストレージの設計、設定、搬入設置、試験 各仮想サーバ機能の設計、設定、移行、試験 バックアップサーバの設計、設定、搬入設置、試験 ネットワーク機器（UTM 含む）の設計、設定、搬入設置、試験 ネットワークログ管理システムの設計、設定、搬入設置、試験 無停電電源装置、KVM の設計、設定、搬入設置、試験 既設システムからの各サーバ機能のデータ移行 旧機器の離線撤去、廃棄	1	式
【各学校】 各拠点の本庁側システム利用の動作試験、調整	10	式
【ベンダ遠隔保守拠点】 遠隔保守環境の設計、設定、試験	1	式
【共通】 システム管理者向け運用マニュアルの作成 システム管理者向け運用教育 完成図書の作成 移行切り替え後の現地運用立ち合い	1	式

6. システム仕様

6.1 サーバシステムの仕様

6.1.1 サーバシステムの全体仕様

① 各サーバシステムは仮想化基盤サーバに搭載とすること。ただし、バックアップシステムについては、バックアップサーバとして別筐体とすること。
② 仮想化基盤サーバは、冗長構成とし、片系サーバの故障時においても、仮想化基盤上の仮想サーバが自動的にもう片系の仮想化基盤で復旧し、システム利用者への影響が最小限となる構成とすること。
③ 各サーバシステムのデータは、仮想化基盤サーバの筐体とは別筐体とした仮想化基盤ストレージに格納し、仮想化基盤ストレージは高い信頼性と筐体内冗長で構成したストレージ装置とすること。
④ 各サーバ・ストレージハードウェアは、国内製品もしくは国内に保守拠点を持つ製品とすること。
⑤ 仮想化基盤サーバは、CPU、メモリ、内蔵ストレージ、ファン、電源装置に対する電圧、温度の障害検知機能があること。また検知した場合は管理者にメール通知する機能を有すること。
⑥ 仮想化基盤サーバは、CPU、メモリ、内蔵ストレージ、ファン、電源装置の事前障害予知機能をハードウェアの機能として有すること。またその内容を管理者にメール通知する機能を有すること。
⑦ 仮想化基盤サーバ、仮想化基盤ストレージは、同一ベンダーであること。
⑧ 導入時の構成において安定して動作する製品およびサーバリソースを選定・確保すること。
⑨ 仮想化基盤サーバは、物理ディスク 1 基の故障時でも業務が停止しない最適な RAID 構成とすること。また、仮想化基盤ストレージは、物理ディスク2基の故障時でも業務が停止しない最適な RAID 構成とすること。
⑩ 各サーバにはウィルス対策ソフトをインストールすること。
⑪ 各サーバのイメージバックアップを取得すること。設定内容については後述の「バックアップシステム構築仕様」で定義する。
⑫ サーバシステムのハードウェア管理用インタフェースを使用すること。監視内容は後述の「監視システムの構築仕様」で定義する。
⑬ 電源供給が 5 分以上停止した場合において、本システム全体が自動的に通常シャットダウンできること。また、シャットダウンまでに必要な給電能力を持つ、UPS を備えていること。
⑭ OS は Windows Server 2025 の調達とする。ただし、周辺ソフトウェアへの対応状況を考慮し、適宜ダウングレードして使用すること。また、ダウングレードした場合は、運用期間のメーカーサポートを得るために、運用期間中にアップデートを行い、メーカーサポートが途切れることがないように対応すること。なお、「監視システム兼 NTP サーバ」は、RedHat Enterprise Linux での構築とし、運用期間中のメーカーサポートを付帯すること。
⑮ Windows Server 2025 の CAL を必要数含めること。ただし、教職員ユーザ数分の Microsoft365 A3 ライセンスを市で所有しており、これを利用することも可とする。

6.1.2 ActiveDirectory の構築仕様

① ActiveDirectory は冗長構成を必須とする。
② ActiveDirectory は、ドメインレベル等、最新のバージョンとし、既存の ActiveDirectory からドメイン名、アカウント情報、グループ情報、コンピュータ情報、グループポリシーを移行すること。なお、バージョン差異により、運用ポリシーや、その他設定に変更が必要な場合、市と十分協議の上決定し、その内容を反映すること。
③ 既存の校務用端末の DNS サーバおよび NTP サーバとすること。

6.1.3WSUS サーバの構築仕様

① 既存の校務用端末（Windows11 端末）に対するパッチデータの管理・適用を行えること。
② 対象の校務用端末（Windows11 端末）は、各学校、および市役所に存在しており、通信負荷等の低減が可能な構成とすること。
③ セキュリティパッチの取得内容設定、承認設定および端末への配信設定は、市と協議の上決定する。
④ WSUS の管理対象数および更新対象プログラムは以下とする。
・管理対象端末数　520 台
・更新対象プログラム　Windows11

6.1.4ファイルサーバの構築仕様

① 現行のファイルサーバのデータを、本サーバに移行させること。
② 移行は、利用停止期間が最小限となる方法とすること。
③ 16TB 以上の実効容量を確保させること。
④ ファイルサーバリソースマネージャー（FSRM）でクォータ設定を有効化すること。クォータ設定はトップフォルダにハードクォータとして設定すること。
⑤ ボリュームシャドウコピー（VSS）機能を有効化すること。スナップショット取得はデータドライブのみを 1 日 2 回（6:00、12:00）取得とし、制限容量は 1.5TB とすること。なお、③の実効容量に含めてもよい。
⑥ 後述の資産管理システムと連携したファイル暗号化機能を継続利用すること。

6.1.5資産管理システムの構築仕様

① 校務用端末 520 台を管理対象とすること。
② 資産管理システムのソフトウェアは、管理運用の統一性および運用スキルの習熟度の観点から、現行システムで運用中の「SKYSEA Client View 藤井寺市版」とする。
③ 資産管理機能を利用し、全端末の IT 資産（ハードウェア、OS バージョン・パッチ、AP バージョン等）の情報収集し全情報の一覧化を可能にすること。また、現行システムのデータを移行すること。
④ デバイス制御機能を利用し、データ読み出し・書き出し可能な外部記憶媒体を制限させること。また、現行システムの制御設定を移行すること。
⑤ 校務用端末の操作ログを全て取得すること。ログの保存期間は 5 年間とする。また、現行システムのログ情報を移行すること。
⑥ ソフトウェアやファイルの一括配布を有効化すること。配布するソフトウェア・ファイルは市の運用の中で随時決定とする。また、配布は、教育委員会にて利用し、各学校、各教職員での利用は想定しない。
⑦ システム管理者から校務用端末へのリモートログインを可能とすること。その際、リモートログインによる状態確認だけでなく、遠隔設定変更内容も各利用者に反映されるようにすること。
⑧ 現行システムで利用している、ファイル暗号化機能を継続利用すること。
⑨ 現行システムで利用している、既存 IntraGuardian2+と連携した不許可端末のネットワーク接続制限機能を継続利用すること。

6.1.6WEB フィルタリングシステムの構築仕様

① 校務用端末 520 台のプロキシサーバとして機能させること。
② 現行のプロキシサーバの設定・アクセスログを引き継ぐこと。また、運用スキルの習熟度の観点からも、WEB フィルタリングシステムのソフトウェアは、現行システムで運用中の「i-FILTER」とする。
③ 現行のプロキシサーバでのパフォーマンス課題を解消するため、割り当て仮想 CPU コア数 8 以上、割り当てメモリ量 32GB 以上とすること。
④ プロキシサーバの代理アクセス機能・キャッシュ機能に加え、悪意のあるサイト等へのアクセスを制御させる WEB フィルタリング機能を有すること。
⑤ WEB フィルタリングは、URL カテゴリによるアクセス制御の他、サイト単位でのアクセス制御を可能とする WEB サービス制御機能を有すること。
⑥ WEB アクセスポリシーは、ActiveDirectory と認証連携し、ActiveDirectory のアカウント名やグループ名単位でのアクセス制御を可能とすること。
⑦ SSL デコード機能を有し、HTTPS の通信についても WEB フィルタリングを可能とすること。SSL デコードに際しては、WEB フィルタリングシステムメーカーの証明書を発行し、校務用端末 520 台にインストールすること。
⑧ ホワイトリスト等の記述により、業務上必要なサイトへのアクセスは優先的に許可すること。
⑨ WEB アクセスログは本サーバ内に 5 年間分保持されていること。また、ログ検索必要時に、WebUI 画面で容易に該当ログ抽出が可能であること。
⑩ WEB アクセスの統計処理等を視覚効果高くレポーティングできる機能を有すること。
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。
⑫ Google Workspace/Microsoft365/Box/AWS/LINE for Business/Dropbox/Slack/Webex/Apple/OpenAI ChatGPT/Microsoft アカウントにおいて、個人アカウント・テナントの利用を制御できる機能を有すること

6.1.7監視システム兼 NTP の構築仕様

① 本案件で導入する全ての機器（仮想化基盤、仮想サーバ、物理サーバ、ファイアーウォール（UTM 含む）、UPS）の一元的な監視をおこなうこと。
② 監視対象毎の監視項目は以下とする。
【全導入機器（仮想サーバ含む）】　機器死活監視（Ping）
【仮想サーバ・物理サーバ】　リソース監視（CPU/RAM/Disk）
【仮想サーバ・物理サーバ】　プロセス監視（主要プロセスのみ）
※プロセス監視の対象プロセスは市と協議の上決定する。
※他システムの監視も行っているため、同様の監視設定を引継ぎ、動作確認を行うこと。
③ 重大（Critical）・重要（Error）なアラート発生時は、システム管理者および保守ベンダにメールでの通知をおこなうこと。
④ 各サーバのハードウェア管理ソフトウェアからは、重大なアラートを直接システム管理者および保守ベンダにメール通知すること。
⑤ 必要に応じてメールリレーサーバを構成すること。
⑥ 監視画面は各監視項目をグラフ表示とし、視覚効果の高いものとすること。
⑦ 監視イベントについては、本サーバ内に 5 年間保管すること。
⑧ 導入する全システムの時刻同期先が最終的に本システムとなるよう構成すること。
⑨ 本システムの時刻同期先は、UTM メーカーサイトもしくは契約プロバイダサイトとする。

6.1.8バックアップシステム構築仕様

① バックアップは、仮想化基盤サーバ、物理サーバ、仮想サーバを含め、イメージバックアップをフルバックアップおよび増分バックアップを取得するポリシーとし、2 世代以上保管とすること。
② ボリューム単位、フォルダ単位およびファイル単位でのバックアップ・復元が可能となるように構成すること。
③ 各ネットワーク機器、仮想化基盤ストレージ、UPS 等の機器の復旧に必要な設定情報についても、バックアッ

プとして保管すること。

6.1.9サーバシステムのハードウェア仕様

仮想化基盤および物理サーバのハードウェア仕様を以下に記す。

表 6.1.8 サーバシステムハードウェア仕様

対象システム	対象機能	仕様
仮想化基盤サーバ	構成台数	2 台以上
	CPU	Intel Xeon 6517P 3.2G 以上 Core 数 16×2CPU 以上/1 台あたり
	Memory	128GB 以上/1 台あたり
	ディスク	SSD SATA 6Gbps 容量 480GB以上、RAID1 構成 RAID キャッシュ 4GB 以上
	電源	二重化電源
	インタフェース	10GbE ポート 2 ポート以上 1GbE ポート 4 ポート以上 32GB FC ポート 2 ポート以上
	保守グレード	24 時間 365 日受付・対応、4 時間駆け付け目標（メーカー保守）
	ハードウェア管理用ポート	1GbE 1 ポート以上
仮想化基盤ストレージ	構成	1 台、仮想化基盤サーバとの接続および、ストレージコントローラは冗長化
	Memory	32GB 以上/コントローラあたり
	ディスク	SSD SAS 12Gbps 以上、合計実効容量 27TiB 以上、 RAID6+HS 構成もしくは同等構成
	電源	二重化電源
	インタフェース	32GB FC ポート 2 ポート以上/コントローラあたり
	保守グレード	24 時間 365 日受付・対応、4 時間駆け付け目標（メーカー保守）
	ハードウェア管理用ポート	1GbE 1 ポート以上/コントローラあたり
バックアップサーバ	CPU	Intel Xeon 6515P 2.3G 以上 Core 数 16 ×1CPU 以上
	Memory	64GB 以上
	ディスク	システム領域として、SSD SATA 6Gbps 容量 960GB 以上、RAID1 構成、RAID キャッシュ 8GB 以上。 バックアップ格納領域として、HDD 7.2k SAS 12Gbps 以上、合計実効容量 36TiB 以上、RAID6+HS 構成、 RAID キャッシュ 8GB 以上。
	電源	二重化電源
	ネットワークインタフェース	1GbE ポート 8 ポート以上
	保守グレード	24 時間 365 日受付・対応、4 時間駆け付け目標（メーカー保守）
	ハードウェア管理用ポート	1GbE 1 ポート以上

6.2　ネットワーク全体の仕様

6.2.1 ネットワーク機器の冗長性

以下機器は冗長構成とし、万一の運用系機器故障時（Port 故障含む）に自動切り替えにより業務への影響が発生しないように構成すること。

①	UTM	HA による冗長構成（HA リンクはハートビート二重構成、セッション管理二重構成とすること）
②	基幹スイッチ	冗長構成（基幹スイッチ間ケーブルは二重構成とすること）
③	UTM～基幹スイッチ	リンクアグリゲーションによる冗長構成とすること
④	基幹スイッチ～サーバ	サーバ Teaming による冗長構成とすること
⑤	UTM～インターネット接続用スイッチ	リンクアグリゲーションによる冗長構成とすること
⑥	基幹スイッチ～拠点接続用ファイアウォール	リンクアグリケーションによる冗長構成とすること

6.2.2 ネットワークの帯域

ネットワークの帯域は以下とする。

①	UTM～基幹スイッチ	1Gbps×複数本のリンクアグリゲーションにより 2Gbps 以上を確保すること
②	基幹スイッチ～仮想基盤	業務通信は 10Gbps 以上とすること
③	上記①②以外の区間	1Gbps 以上を確保すること

6.2.3 ネットワークのセグメント構成

現行セグメント構成を踏襲する。変更することは可能であるが、各拠点から利用されるシステムであるため、変更が必要な場合は、すべての拠点の必要な機器、端末に対して、本設定変更を行う対応を本調達に含めること。

6.2.4 各学校側ネットワーク、他システムとの接続構成

① 各学校との接続は既存閉域網を継続利用し、VPN 環境を構成すること。
　また、各学校の既存ファイアーウォール機器と、拠点接続用ファイアーウォール間を VPN 接続とすること。
② 各学校側の既存ネットワーク機器について、本調達機器との接続にあたり、バージョンアップが必要な場合、既存保守業者にて実施するため、本調達では作業不要とする。ただし、必要な情報提供を行うこと。
③ 既存校務支援システムの境界ファイアーウォールと接続し、現行同様の通信を可能とすること。

6.2.5 ネットワークのセキュリティ

① セキュリティゲートウェイとしてインターネットとの接続および各学校向け回線との接続に UTM を配置する。UTM では必要最小限の通信に限定するとともに、アンチウィルス・侵入防御・アプリケーションコントロール機能を有効化すること。
② 各学校との接続は既存閉域網を継続利用し、VPN 環境を構成する。VPN 設定については現行同様のセキュリティの設定とすること。
③ UTM、拠点接続用ファイアーウォール、基幹スイッチ、本庁フロアスイッチ、インターネット接続用スイッチおよび既存の学校側ネットワーク機器の通信ログを集中管理するログ管理システムを導入し、通信ログをリアルタイムに自動相関解析する機能を導入すること。事前に市と協議した内容で、対象の解析結果やログ内容に閾値の設定とアラート通知の設定を行うこと。また、運用性、機能性を考慮し、これらの機器のメーカーを統一すること。
④ 現行で導入している、不許可端末の接続を防止するアプライアンス機器（IntraGuardian2+）を継続利用し、校務セグメントに対して、不許可となる端末のネットワーク接続を防ぐこと。

6.2.6 ネットワークの一元管理（プロビジョニング管理・構成管理・故障管理）

① 本庁設置となる UTM、基幹スイッチ、本庁フロアスイッチ、インターネット接続用スイッチの設定や運用管理を一元的に実施できるネットワークシステムとし、メーカーを統一すること。設定については、1 つの WebUI にて、上述の機器全ての設定を施せるものとし、運用管理については、全機器の接続状態や運用ステータスが一目で確認できる物理接続構成図が画面上に表示されるものとすること。
② 機器や物理結線に故障が発生した場合、運用ステータスとしてリアルタイムに画面状態を遷移（赤色表示など）させるとともに、システム管理者およびシステム保守ベンダにメール通知させることで迅速に故障対応可能となる環境とすること。また、機器故障による機器取り替え時に於いても、取替機器への個別設定をせずとも、機器の取り替えと入れ替え・承認操作等、容易な操作をおこなうだけで復旧できるネットワークシステムとすること。
③ 各スイッチの物理接続構成（A 機器のどのポートと B 機器のどのポートが接続されているか）のリアルタイムな状況が視覚効果高く一目で確認できるものであること。
④ UTMからの重大なアラートについても、機器から直接システム管理者および保守ベンダにメール通知をおこなうこと。（ハードウェア監視、HA 監視、セキュリティ監視、ネットワークループ監視、ライセンス期限監視）
⑤ 監視画面は各監視項目をグラフ表示とし、視覚効果の高いものとすること。

6.3　ネットワーク機器の仕様

6.3.1UTM の構築仕様

① 最新の安定バージョンの OS を搭載した UTM とすること。
② 本庁内ネットワークのセキュリティゲートウェイとしてルーティング設定、VLAN 設定、セキュリティ設定を施す。
③ HA 構成による冗長構成とし、両機器間の HA 用リンクはハートビート用、セッション維持用それぞれで二重化構成とする（計 4 本の HA リンクを構成）。
④ 「UTM 自身」「基幹スイッチ」「本庁フロアスイッチ」「インターネット接続用スイッチ」のプロビジョニング（設定追加・変更・削除）の一元的集中管理を本機器でおこなうこと。一元的集中管理の構成とすることにより、全スイッチの設定情報は全て UTM が保持することになるので、スイッチでの個別設定を不要となるよう構成すること。
⑤ 管理対象ネットワークの接続構成、構成要素の詳細情報および運用状態を、WebUI 画面上に物理構成図および論理構成図として表示させることで視覚的・直感的に確認できるシステムとすること。また、運用状態はリアルタイムに状態変化を表示させること。
⑥ SSL/SSH インスペクション機能を有効化し、暗号化通信も自動デコードしての検査・制御を行う機能を持つこと。
⑦ ActiveDirectory と連携し、IP アドレス・MAC アドレス・ドメイン等だけでなく、アカウント情報・グループ情報での各種設定・制御も視野に入れた機能を有すること。
⑧ システムログ・アクセスログ等はネットワークログ管理システムにリアルタイム転送すること。
⑨ UTM 機能として、アンチウィルス・IPS 機能を有効化し、インターネット向けの通信ポリシー（HTTP/HTTPS/FTP 等）には、これらの UTM 機能を適用させること。
⑩ 電源は冗長構成とすること。

6.3.2UTM のハードウェア仕様

UTM のハードウェア仕様を以下に記す。

表 6.3.2 UTM ハードウェア仕様

対象機器	対象機能	仕様
UTM	構成台数	2 台（Active-Passive HA 構成）
	IPv4ファイアーウォールスループット（UDP 1518/512/64Byte 時）	79.5/78.5/70Gbps 以上
	NGFW スループット（エンタープライズ混合テストかつログを有効にした状態）	10Gbps 以上
	脅威保護スループット（エンタープライズ混合テストかつログを有効にした状態）	9Gbps 以上
	IPS スループット（エンタープライズ混合テストかつログを有効にした状態）	12Gbps 以上
	ファイアーウォールレイテンシ（UDP 64byte 時）	4.19μs 以下
	同時セッション数（TCP）	最大 7.8M 以上
	新規セッション数（TCP）	毎秒最大 500,000 以上
	1GbE SFP インタフェース	8 ポート以上
	1GbE RJ-45 インタフェース	16 ポート以上
	10GbE SFP+インタフェース	4 ポート以上
	10GbE SFP+超低遅延インタフェ	4 ポート以上

対象機器	対象機能	仕様
	ース	
	1GbE 管理インタフェース	2 ポート以上
	搭載方法	19 インチラックに搭載可能で、1U 以内であること
	電源	冗長電源
	保守グレード	平日 9:00-17:00 先出しセンドバック
	UTM ライセンス	AntiVirus/WebFilter/ApplicationControl/DNS Filter
	各種シグネチャ・エンジン	自社開発であること
	WebUI	日本語対応していること
	スイッチコントローラ機能	最大 72 台まで管理可能なこと
	WebFilter 機能	80 カテゴリ以上のデータベースを持つこと
	IPS のシグネチャ	10,000 以上のシグネチャを有すること。
	IPS の機能	IPS 機能はユーザが個別でシグネチャの設定(カスタムシグネチャ)できる機能を有すること
	遮断機能	2,000 以上のアプリケーションを識別し遮断が可能なこと。

6.3.3基幹スイッチの構築仕様

① 最新の安定バージョンの OS を搭載したスイッチとすること。
② サーバファームセグメントと UTM 間に基幹スイッチを配置すること
③ 10Gbps のインタフェースを保有するものを選定すること。必要に応じて、SFP モジュール等を用意すること。
④ MCLAG を用いた冗長構成を行う。MCLAG を構成するスイッチ間のケーブルは複数本での冗長化を図ること。
⑤ UTM でのプロビジョニング一元的集中管理となるため本スイッチでの個別設定はないこととする。
⑥ システムログ・アクセスログ等はネットワークログ管理システムへのリアルタイム転送とすること。

6.3.4基幹スイッチのハードウェア仕様

基幹スイッチのハードウェア仕様を以下に記す。

表 6.3.4 基幹スイッチハードウェア仕様

対象機器	対象機能	仕様
基幹スイッチ	構成台数	2台(スタック構成) MCLAG に対応していること
	スイッチング容量(双方向)	720Gbps 以上
	スループット(パケット転送能力,双方向)	1,071Mpps 以上
	ネットワークレイテンシ	1μs 以下
	10/25GbE SFP+/SFP28 インタフェース	8 ポート以上
	1/2.5GbE RJ45 インタフェース	32 ポート以上
	1/2.5/5GbE RJ45 インタフェース	16 ポート以上

対象機器	対象機能	仕様
	MAC アドレス登録数	64,000 以上
	ルーティングエントリー	IPv4:330,000 以上
	VLAN 登録数	4,000 以上
	搭載方法	19 インチラックに搭載可能で、1U 以内であること
	電源	冗長化電源
	MTBF（平均故障間隔）	10 年以上
	管理方法	UTM の GUI から集中管理できること
	保守グレード	平日 9:00-17:00 先出しセンドバック

6.3.5本庁フロアスイッチの構築仕様

① 最新の安定バージョンの OS を搭載したスイッチとすること。
② UTM でのプロビジョニング一元的集中管理となるため本スイッチでの個別設定はないこととする。
③ システムログ・アクセスログ等は本庁のネットワークログ管理システムへのリアルタイム転送とすること。
④ 予備機を 1 台以上用意し、故障時に手動付け替え作業を行うことで迅速な切り替えができること。

6.3.6本庁フロアスイッチのハードウェア仕様

本庁フロアスイッチのハードウェア仕様を以下に記す。

表 6.3.6 本庁フロアスイッチハードウェア仕様

対象機器	対象機能	仕様
インターネット接続用スイッチ	構成台数	2 台（内1台は予備機）
	スイッチング容量(双方向)	20Gbps 以上
	スループット（パケット転送能力,双方向）	30Mpps 以上
	ネットワークレイテンシ	4μs 以下
	1GbE RJ-45 インタフェース	8 ポート以上
	1GbE SFP インタフェース	2 ポート以上
	MAC アドレス登録数	8,000 以上
	VLAN 登録数	4,000 以上
	MTBF（平均故障間隔）	10 年以上
	管理方法	UTM の GUI から集中管理できること
	保守グレード	平日 9:00-17:00 センドバック

6.3.7インターネット接続用スイッチの構築仕様

① 最新の安定バージョンの OS を搭載したスイッチとすること。
② UTM からインターネット間に設置するスイッチとすること。

③　UTM でのプロビジョニング一元的集中管理となるため本スイッチでの個別設定はないこととする。
④　システムログ・アクセスログ等はネットワークログ管理システムへのリアルタイム転送とすること。
⑤　予備機を 1 台以上用意し、故障時に手動付け替え作業を行うことで、迅速な切り替えができること。
⑥　既存インターネット回線を収容し、回線利用のための設定を引き継ぐこと。

6.3.8インターネット接続用スイッチのハードウェア仕様

インターネット接続用スイッチのハードウェア仕様を以下に記す。

表 6.3.8 インターネット接続用スイッチハードウェア仕様

対象機器	対象機能	仕様
フロアスイッチ	構成台数	2 台（内 1 台は予備機）
	スイッチング容量(双方向)	128Gbps 以上
	スループット（パケット転送能力，双方向）	190Mpps 以上
	ネットワークレイテンシ	1μs 以下
	1GbE RJ-45 インタフェース	24 ポート以上
	1GbE SFP+ インタフェース	4 ポート以上
	MAC アドレス登録数	32,000 以上
	VLAN 登録数	4,000 以上
	MTBF（平均故障間隔）	10 年以上
	管理方法	UTM の GUI から集中管理できること
	保守グレード	平日 9:00-17:00 先出しセンドバック

6.3.9拠点接続用ファイアーウォールの構築仕様

①　最新の安定バージョンの OS を搭載したファイアーウォールとすること。
②　各拠点の必要最小限の通信ポリシーのみを通過させる設定とすること。
③　既存の閉域網回線を継続利用し、既存の各拠点のファイアーウォールと VPN 接続を行うこと。
④　システムログ・アクセスログ等は本庁のネットワークログ管理システムへのリアルタイム転送とすること。

6.3.10　拠点接続用ファイアーウォールのハードウェア仕様

拠点接続用ファイアーウォールのハードウェア仕様を以下に記す。

表 6.3.10 拠点接続用ファイアーウォールハードウェア仕様

対象機器	対象機能	仕様
拠点接続用ファイアーウォール	構成台数	1 台
	IPv4ファイアーウォールスループット（UDP 1518/512/64Byte 時）	28/39/39Gbps 以上
	NGFW スループット（エンタープライズ混合テストかつログを有効にした状態）	3.1Gbps 以上
	脅威保護スループット（エンタープライズ混合テストかつログを有効にした状態）	2.8Gbps 以上

対象機器	対象機能	仕様
	IPS スループット （エンタープライズ混合テストかつログを有効にした状態）	5.3Gbps 以上
	ファイアーウォールレイテンシ （UDP 64byte 時）	3.17μs 以下
	同時セッション数（TCP）	最大 3,000,000 以上
	新規セッション数（TCP）	毎秒最大 140,000 以上
	1GbE SFP インタフェース	8 ポート以上
	1GbE RJ-45 インタフェース	16 ポート以上
	10GbE SFP+インタフェース	4 ポート以上
	管理インタフェース	1 ポート以上
	搭載方法	19 インチラックに搭載可能で、1U 以内であること
	電源	冗長電源
	保守グレード	平日 9:00-17:00 先出しセンドバック
	WebUI	日本語対応していること
	スイッチコントローラ機能	最大 32 台まで管理可能なこと

6.3.11 ネットワークログ管理システムの構築仕様

① ネットワークログ管理システムでは、「UTM」「基幹スイッチ」「本庁フロアスイッチ」「インターネット接続用スイッチ」「拠点接続用ファイアーウォール」、既存の学校側ネットワーク機器の集中ログ管理（通信解析・アラート発出）をおこなうこと。また、これら機器とメーカーを統一すること。
② 全てのネットワーク通信ログを保有しており、視覚効果の高い管理画面にて、通信ログ・セキュリティログの検索および統計処理（レポーティング含む）を容易に実施できるようにすること。
③ システムログ・アクセスログ・セキュリティログの保存期間は 5 年間とする。
④ ネットワークログ管理システムを配置し、一元的なログ管理を実施可能とさせること。そのため、UTM の WEB フィルタリング機能をモニタモードで有効化させること（実際の WEB フィルタリングは WEB フィルタリングシステムで実施する）。
⑤ アプリケーション、送信元、送信先、Web サイト、セキュリティの脅威、管理情報の変更、システムイベントのサマリを表示可能なこと。
⑥ 多発するログにより、ログへの深刻度が薄れることを防止する目的も兼ね、SNMP サーバやメールサーバの稼働環境下であれば、ファイアーウォールから収集した同一パターンのログが x 分以内に y 件発生したら管理者にアラートメールを送信，SNMP trap 送信といったイベントを自動的にキックできること。
⑦ ログ収集サーバ側で、リアルタイムイベントのログ分析の結果、事前定義した特定条件に合致するものは「イベント」として処理できること。
⑧ シンプルで直感的な検索機能を使って、ネットワークのアクティビティやトレンドを検索し、レポートを作成可能なこと。
⑨ カスタマイズ可能な PDF テンプレートでレポート表示可能なこと。

6.3.12　ネットワークログ管理システムのハードウェア仕様

ネットワークログ管理システムのハードウェア仕様を以下に記す。

表 6.3.12 ネットワークログ管理システムのハードウェア仕様

対象機器	対象機能	仕様
ネットワークログ管理システム	構成台数	1台
	ストレージ容量	4TB×2 本、合計 8TB 以上
	ストレージ構成	RAID0/1 に対応していること
	搭載方法	19 インチラックに搭載可能で、1U 以下であること
	ログ処理量	1 日当たり最大 100GB 以上であること
	分析時のログ処理持続レート	1 秒あたり最大 2,000 以上であること
	連携可能なネットワークデバイス数	最大 180 以上であること
	保守グレード	平日 9:00-17:00 先出しセンドバック

6.3.13　ベンダ保守拠点の構築仕様

① 既存の閉域網回線に 1 拠点分追加し、ベンダ保守拠点として機能させること。
② セキュリティゲートウェイ機器として、ファイアーウォールを設置し、遠隔保守運用に必要な通信（HTTP/HTTPS/TELNET/SSH/ICMP/RDS/SNMP 等）のみの通信許可設定とすること。
③ セキュリティゲートウェイ機器のシステムログ・通信ログ・セキュリティログは、ネットワークログ管理システムへのリアルタイム転送とすること。
④ セキュリティゲートウェイ機器の時刻同期は、本庁に新規構築する NTP サーバを時刻同期先とすること。
⑤ 画面転送機能を持つリモートアクセスソフトウェアによって、遠隔保守運用を行う場合、①～④の限りではない。必要なリモートアクセスソフトウェアは本調達に含めること。
⑥ 保守運用端末は受注業者にて保守運用に必要な台数を調達すること。
⑦ 保守運用端末にはアンチウィルスソフトを調達・導入し、最新のウィルス定義ファイルに随時更新とする。
⑧ 保守運用端末の WindowsUpdate は随時最新版に更新すること。
⑨ 保守運用端末に構成するソフトウェアは、運用管理に必要な必要最小限のソフトウェアのみとすること。ただし、ベンダ保守拠点での利用に際し、必要なセキュリティを確保するために導入が必要なものはこの限りではない。

6.4　その他機器の仕様

6.4.1UPS の構築仕様

① 本業務で本庁に導入する機器すべての電源供給元となるシステムとする。
② 別系統の電源を複数台の UPS に分散し、冗長化電源を保有する機器についてはそれぞれに分散収容すること。
③ 電源供給停止時には、本業務で本庁に導入する機器全体が正常に停止するよう、順次、自動的に停止処理を行う設定とすること。
④ 仮想化基盤サーバ、仮想化基盤ストレージ、バックアップサーバについては UPS への直接収容とし、それ以外のネットワーク機器については、電源タップ経由での収容とすること。
⑤ 重大（Critical）なアラートは、システム管理者に自動メール通知すること。
⑥ 保守グレードは、オンサイト保守 5 年、24 時間/7 日受付・対応をメーカー保守として付帯すること。

6.4.2KVM の構築仕様

① 仮想化基盤サーバ、バックアップサーバの管理コンソールとして収容する。
② LCD は 17 インチ以上とする。
③ 収容ポート数は 8 以上とする。
④ 日本語キーボードであること。
⑤ 保守グレードは、オンサイト保守 5 年をメーカー保守として付帯すること。
⑥ 既存他システムの管理コンソールも収容すること。

7. 導入作業仕様

7.1 作業全体

① 本事業で調達する機器等を設置し、正常に使用できるように、各種ケーブルの接続を行うこと。ただし、予備機は接続の対象外とする。
② 機器間の配線に必要な部材は受注業者にて用意すること。
③ 配線する LAN ケーブルはエンハンスドカテゴリー6 以上の UTP ケーブルであること。ただし、10Gbps 通信のケーブルはエンハンスドカテゴリー6A 以上の UTP ケーブルとする。
④ 配線時にケーブルの両端に豆札を取り付けるなど、接続先が明確になるようにすること。
⑤ 本市の指定する機器へ名称、管理番号、導入日等を記載したテープラベルを貼り付けること。テープラベルの詳細は落札後、本市と協議の上決定する。
⑥ 本業務で調達する機器、ケーブル等の部材類、ソフトウェアはすべて新品であること。
⑦ 作業時間は、原則、平日の午前9時から午後5時までとし、事前に本市と協議の上、作業計画を提出すること。
⑧ 作業スケジュール案を作成し、本市に提示・承諾を得ること。
⑨ 導入製品のハードウェア、ソフトウェアの窓口については、藤井寺市教育委員会とすること。ただし、各製品のファームウェア管理、バージョン管理、ライセンス管理等は、受注業者で実施することとする。

7.2 搬入作業

① 作業は細心の注意を払って実施すること。万が一、建物・設備等に損傷を与えた場合は、受注業者の負担で修理を行うこと。
② 機器の搬入、設置作業にて発生した廃材、導入物品の梱包材は回収、廃棄を行うこと。
③ 導入物品の付属品や書類等の備品はまとめて、本市へ納入すること。

7.3 設置作業

① 導入機器は本市が指定するラックに搭載すること。
② 新旧機器の並行運転期間については、機器重量・消費電力を考慮した搭載計画とすること。搭載重量および搭載スペースが指定のラックで賄えない場合、本市と協議の上、隣接ラックへの搭載も考慮すること。また、並行期間における電源増設が必要な場合は作業内容、計画等を本市と協議のうえ、承認を得て受注業者の責任において増設すること。
③ ラックに直接固定できない機器については、耐震ベルトの使用などにより耐震対策を施すこと。
④ 電源については既設電源を利用すること。調達機器の必要電源容量を予め算出し、増設が必要な場合は既存分電盤や配線経路などの事前調査を行うこと。また電源増設が必要な場合は作業内容、計画等を本市と協議のうえ、承認を得て受注業者の責任において増設すること。

7.4 機器の撤去

① 本市の指定する更新対象となる旧機器の撤去廃棄作業の費用を見込むこと。

表 7.4 撤去機器一覧

機器名称	機種	台数
仮想化基盤サーバ	DL380 G10	2 台
仮想管理サーバ	DL20 G10	1 台
物理サーバ	DL380 G10	1 台
UTM 機器	Fortigate-300E	2 台
FW 機器	Fortigate-100E	1 台
基幹スイッチ	Fortigate-1048E	2 台

機器名称	機種	台数
L3 スイッチ	FortiSwitch-224E	1 台
L2 スイッチ	FortiSwitch-108E	2 台
ログ管理機器	FortiAnalyzer-200F	1 台
UPS 機器	Smart-UPS 1500 RM 2U LCD	3 台
KVM 装置	AP5717J	1 台

② 撤去機器の廃棄完了後に産業廃棄物管理票（マニフェスト）を本市へ提出すること。
③ 撤去対象に内蔵している SSD 及び HDD の記憶媒体についてはデータが復旧不可能な物理破壊を行うこと。
④ 物理破壊作業は、設置拠点から搬出する前に実施すること。作業時間や場所の確保が困難な場合は、発注者の許可を得た上で、引き取りによる作業も可とするが、機器の回収・運搬時はセキュリティに注意し、情報漏洩のないように対策を行うこと。

8. システム移行仕様

8.1　システム移行仕様

現行システムからの移行については、詳細な現状調査を踏まえ計画すること。提示されたシステム移行計画を元に、市と十分に協議の上別途決定することとする。

なお、移行に際しては、現状業務や授業への影響を十分に考慮し、影響を及ぼすもの、あるいは及ぼす可能性のある作業は土休日での実施とする。

また、移行による運用の変更点は、次項「教育仕様」で定義する。

9. 教育仕様

9.1 教育仕様

教育の仕様を以下に示す。

① 市のシステム管理者向けに、以下の「運用手順書」を作成すること。なお、内容については別途市と協議の上決定する。
(ア) ActiveDirectory 運用手順書(ユーザ追加・削除・変更、人事異動時データ変換ツール利用方法等)
(イ) 資産管理システム運用手順書
(ウ) WEB フィルタリングシステム運用手順書
(エ) 監視システム運用手順書
(オ) ネットワーク一元管理運用手順書
(カ) WSUS 運用手順書
(キ) ファイルサーバ運用手順書
(ク) システム停止起動手順書

② 運用手順書を以って、必要に応じて実機を使用した 1 日程度のハンズオン研修をおこなうこと。
③ 現行運用から変更となる点などについて、各運用手順書に明確に記載されていること。また、ハンズオン研修において、変更点の詳細な説明を実施すること。
④ 研修実施後の質疑応答についても速やかに対応すること。

10. 完成物

10.1 完成図書

以下の完成図書を電子データおよび書籍で納品すること。
(ア) 基本設計書
(イ) システム構成図・物理構成図・論理構成図
(ウ) IP アドレス・VLAN 一覧表
(エ) ユーザ名・パスワード一覧表
(オ) ネットワーク機器設定パラメータシート
(カ) ネットワーク機器 Configuration
(キ) サーバ機器設定パラメータシート
(ク) その他機器設定パラメータシート
(ケ) ソフトウェア設定パラメータシート
(コ) ラック搭載図
(サ) フロア配置図
(シ) 電源供給図

以下の完成図書は電子データのみでの納品とすること。
(ス) トレーサビリティ管理表
(セ) 試験結果成績表
(ソ) 作業写真(事前・事後)
(タ) 各種ライセンス証書
(チ) 各機器・アプリケーション取り扱い説明書、マニュアル
(ツ) 各運用手順書
(テ) 人事異動時データ変換ツール
(ト) 機器およびソフトウェア保守サポート一覧表

11.　運用保守仕様

11.1　対応期間

運用保守業務期間は令和 8 年 7 月 1 日から令和 13 年 6 月 30 日とすること。

11.2　受付時間

① 受付は電話もしくはメールで行うものとすること。
② 受付は平日の午前9時から午後5時までとすること。ただし、国民の祝日に関する法律に定める休日および年末年始の休日（12 月 29 日から 1 月 3 日）は除くものとする。
③ メールでの受付時間は、24 時間 365 日受付可能とすること。なお、メールシステムの障害等により受付できない場合は除外とする。

11.3　対応時間

① 対応は電話、リモートもしくはオンサイトで行うものとする。
② 対応は平日の午前9時から午後5時までとすること。ただし、国民の祝日に関する法律に定める休日および年末年始の休日（12 月 29 日から 1 月 3 日）は除くものとする。

11.4　保守対象

① 本調達で納入するすべての機器・ソフトウェアを対象とすること。
なお、フリーソフトについては対象外とする。
② 対象拠点は表 11.4 に示す拠点とすること。
下記に該当する物品は保守対象外とする。
(ア) 本市の責により発生した故障
(イ) 機器メーカーの定める規定外の使用方法により発生した故障
(ウ) 次に定める機器/消耗品
A) 無停電源装置のバッテリ
B) その他メーカーが定期交換部品および消耗品類と定めるもの

表 11.4 保守対象拠点

拠点名	住所	電話番号
教育委員会事務局	大阪府藤井寺市岡 1 丁目 1 番 1 号	072-939-1402

11.5　保守業務内容

① 故障した機器については修理または予備機との交換にて対応すること。
② 交換対応する機器については予備機を利用し、予備機は契約期間中、本市が保管することとする。
③ 故障の連絡を受けたときは、速やかに故障機器の修理に着手すること。1 営業日以内に受付を行い、復旧については協議の上、迅速に行うこと。
④ リモートメンテナンスで保守業務を行う際は、項 6.3.13 に定める保守運用端末を使用すること。なお設定変更が生じる作業を行う際は事前に本市に通達を行うこと。

11.6　操作問い合わせ

本調達で納入する機器・ソフトウェアに対し、操作上の疑義に対しても、受付窓口にて問い合わせ対応をすること。

11.7　脆弱性に関する通知

導入した機器およびソフトウェアに対し、脆弱性の有無を確認するとともに、重大な脆弱性を確認した際は本市に通知すること。

11.8　定期点検・アップデート対応

① 導入した機器およびソフトウェアに対し、定期点検およびアップデートを実施すること。
② 令和9、10、11、12年の 8 月の閉庁期間にて計 4 回実施すること。なお、時期については本市と協議の上変更できるものとする。
③ 点検については下記対応を実施すること。
　(ア) ハードウェア診断ツールによるチェック
　(イ) ディスクアレイ状態の確認
　(ウ) OS のイベントログチェック
　(エ) バックアップ状態の確認
　(オ) 導入システムの正常性確認
　(カ) ネットワーク機器等接続確認
　(キ) ログチェック
④ アップデートについては下記対応を実施すること。
　(ア) UTM、拠点接続用ファイアウォール、基幹スイッチ、本庁フロアスイッチ、インターネット接続用スイッチ、ネットワークログ管理システムのファームウェアアップデート対応
　(イ) サーバ OS のセキュリティパッチ適用
　(ウ) 資産管理ソフトのアップデート
　(エ) バックアップ管理ソフトウェアのアップデート

11.9　監視

項 6.1.7 で定める監視項目に異常が発生した際は、本市に速やかに通達するとともに原因調査を行うこと。
なお、監視システムが機能しているか定期的に確認を行い、機能していない場合は速やかに復旧させること。

11.10 バックアップ監視

導入したサーバのバックアップ監視を行い、バックアップ異常が発生した際は、本市に通達するとともに原因調査を行い復旧すること。また、障害によりバックアップが失敗している場合は、最新のバックアップを取得するようにすること。ただし、バックアップにより業務に支障が出る場合はこの限りではない。

11.11 運用に関する相談

本調達で納入した機器およびソフトウェアの運用に関して、相談窓口を用意すること。
相談の内容は下記を想定するが、この限りではない。
① ネットワーク機器の設定変更に関する相談
② メーカーの仕様変更に伴う設定相談
③ 脆弱性に対する対応相談
④ Active Directory 運用に関する相談
⑤ WSUS 運用に関する相談
⑥ 資産管理システム運用に関する相談
⑦ フィルタリングソフト運用に関する相談

なお、本市で対応が困難な調査や設定変更などの作業が必要となった際は、項 11.12 に準じて対応すること

11.12 上記に該当しない運用支援業務

日々変化するICT環境の変化に対応するため、本調達で納入する機器・ソフトウェアにおいて、突発的に発生する運用上の問題や設定変更に対して本契約の範囲内で対応すること。月1回2時間を上限とする。これを超過する場合は都度協議にて対応を検討すること。

11.13 成果物の納品

運用保守業務により、本市に納品している成果物に変更が生じた場合は、速やかに提出すること。なお、フォーマットは電子データで納品すること。

12. プロジェクト運営仕様

12.1 プロジェクト運営仕様及び受注者の義務

プロジェクトは以下のとおり運営する。

① 構築プロジェクトは、プロジェクトマネージャを立てて体制構築すること。
② プロジェクトメンバー1名以上は、同規模・同内容の自治体案件実績が 1 件以上あること。
③ プロジェクトマネージャ 1 名以上は、プロジェクトマネジメント資格として、PMP と同等以上の資格を保有していること。
④ 本業務の一次請け会社は、ISMS もしくはプライバシーマークを取得していること。
⑤ 工期内については、市との定例会を開催し、進捗管理・課題管理等について報告すること。開催間隔、開催曜日等については別途市と協議の上決定する。
⑥ 本業務の要件定義書および基本設計書を提出し、市の承認を得ること。工期内において、設計内容に変更を生じる場合は、都度市の承認を得て、基本設計書の修正版を提出すること。
⑦ 現地での作業実施前には、作業体制・連絡体制・作業者名・工事車両有無が分かる作業体制表を作成し、市に提出の上承認を受けること。
⑧ 現地での作業実施前には、そのタイムスケジュール・作業内容および業務・授業への影響が明確に分かる作業手順書を作成し、市に提出の上承認を受けること。
⑨ 本庁、各学校における作業時の規則については、市の指定する通り実施することとする。
⑩ 基本設計書内容のとおり機器導入および施工されており、試験成績書での結果に問題がない事を以って検収とする。ただし、市の本運用開始後に発覚する不具合に対するシステムの設定変更等については、瑕疵期間として対応すること。瑕疵期間は 2026/7/1～2027/6/30 とする。
⑪ 労働安全規則に従い、常に安全管理に必要な措置を講じること。
⑫ 防火、防犯、情報セキュリティその他安全に十分注意し、事故が発生し、その原因が受注者の責に帰す場合は、受注者の責任において処理すること。
⑬ 当市及び学校教育活動業務に支障のないよう留意すること。
⑭ 作業にあたっては、当市及び作業場管理者の指示に従うこと。
⑮ 守秘義務を遵守すること。本市仕様書等の閲覧時及び契約履行中に知りえた情報は外部に漏らしてはならない。
⑯ 本賃貸借範囲に使用する機器の特許権、実用新案権等の工業所有権及びプログラム等の著作権その他知的財産権、また、使用許諾契約等については、すべて受注者の責任において処理すること。
⑰ 関係法令を遵守すること。
⑱ 本仕様書に明記されていない細部の事項については、当市の指示に従うこと。ただし、指示がない場合においても、本仕様書の趣旨に鑑み当然必要と考えられるものについては、受注者の責任において対応すること。
⑲ 本仕様書について疑義等が生じた場合は、当市と受注者との間でその都度協議の上解決を図るものとする。

13.　システム構成イメージ

13.1　システム構成イメージ

現行のシステム構成イメージ図を以下に示す。