校務系クラウド構築業務

仕様書

令和 7 年 10 月

丹波市教育委員会

目 次

1. 概要

1.1. 背景と目的

丹波市（以下「本市」という。）では、令和 2 年度に GIGA スクール構想の実現に向け、市内の小中学校に 1 人 1 台端末、無線 LAN ネットワークの整備、クラウド型学習支援システムの導入等、学習活動に ICT を活用できる環境を整備してきた。一方で、教職員が校務に利用する ICT 環境については、学習環境とは完全に分離するとともに、各種システムの自前サーバーでの運用を行い、校務用端末も職員室に固定している。これらの仕組みは、従来の境界防御型のセキュリティ対策を踏まえたものであるが、このことにより、1 人 1 台端末の整備とクラウド活用を核とする GIGA スクール時代の教育 DX や働き方改革の流れに適合しなくなっている。

こうした中、文部科学省は、「教育情報セキュリティポリシーに関するガイドライン」の令和 3 年 5 月の改訂により、クラウドサービスの利活用を前提としたネットワーク構成を目指す方向性を示した。さらに、令和 5 年 3 月には、文部科学省の「GIGA スクール構想の下での校務の情報化の在り方に関する専門家会議」が取りまとめた、「GIGA スクール構想の下での校務 DX について」を公表し、校務系・学習系ネットワークの統合、主要なシステムのクラウド化、それらを安全安心な形で実装するためのセキュリティの確保等の必要性が示された。ここでは、次世代校務 DX を通じて、汎用クラウドツールの活用による教職員等の負担軽減・コミュニケーションの迅速化等に加え、ロケーションフリーでの校務実施や、校務系データと学習系データの円滑な連携を通じたきめ細かな学習指導等を可能とすることが求められている。

本業務は、以上のことを総合的に考慮したうえで計画的な調達、構築を進め、市内の全小中学校において ICT を活用した校務をより一層推進できる環境を整備することを目的に、新たなネットワーク環境への移行を行うものである。

1.2. 業務概要

本業務は、構築移行業務と保守運用業務に分かれる。

【構築移行業務】
プロジェクト管理、設計・構築、検証・テスト、クラウド環境への移行・切り替え、研修の各業務が対象となる。具体的な業務内容は『4.1.構築移行業務』を参照すること。

【保守運用業務】
構築移行業務にて構築した校務系クラウド環境について、安定的に運用を行うための問い合わせ対応、障害対応、セキュリティ脆弱性対応、脅威の検知・分析・対応等を行うものである。具体的な業務内容は『4.2. 保守運用業務』を参照すること。

1.3. 委託期間

本業務の委託期間を以下に示す。

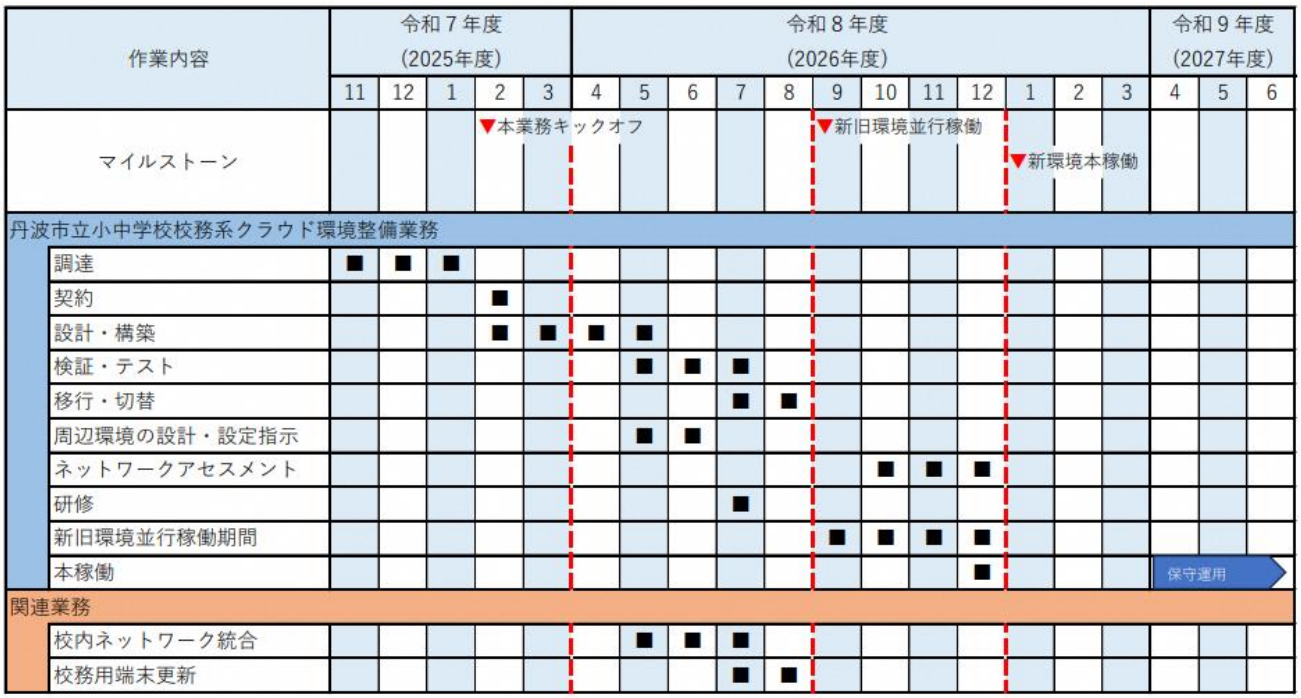
【構築移行業務】 契約締結日の翌日から令和9年3月31日まで

【保守運用業務】 令和9年4月1日から令和14年3月31日までの 60 ヶ月間

1.4. スケジュール

本業務の実施スケジュール、及び関連する業務のスケジュール案を以下に示す。

本業務と並行して、校内ネットワークの統合作業や、校務用端末の更新等を予定している。本業務受注者は、これら関連業務を推進する事業者とも密接に連携しながら、次期ネットワーク環境への移行をマネージメントすること。なお、本スケジュール案は一例であるため、現行ネットワークからの円滑な移行や、次期ネットワークに対する教職員の習熟期間を考慮した最適なスケジュールを提案すること。



2. 現行ネットワークについて

2.1. ネットワーク環境

現行ネットワークの主な構成要素を以下に示す。

2.1.1. 丹波市地域イントラネット

- 各学校は、ダークファイバーによりリング状に構築された丹波市地域イントラネットに接続し、教育委員会で集約してインターネットに接続している。
- 各学校と丹波市地域イントラネットは1Gbpsで接続している。
- 教育委員会が設置されている山南支所と丹波市地域イントラネットは1Gbps回線を2本束ねたリンクアグリゲーション（LAG）構成で接続している。
- インターネット回線については、1Gbpsのベストエフォート光回線を3本使用している。
- 各学校から直接インターネットにアクセスするローカルブレイクアウトは行っていない。

2.1.2. 校内ネットワーク

- 学校内のネットワークは、校務系ネットワークと学習系ネットワークの2層に分離している。
- 校務系ネットワークと学習系ネットワークは、令和8年度中に学習系ネットワークに一本化する予定で、ネットワークの設定変更が必要な場合は、既存のネットワーク等保守業者で行う予定である。
- 職員室や教室に設置されている学習系ネットワーク接続用の無線LANアクセスポイントについては、株式会社フルノシステムズの Acera 1150w を導入しており、教育委員会に設置している無線ネットワーク管理サーバーにインストールした無線ネットワーク管理システム(UNIFAS)にて集中管理している。
- 無線LANの認証については、MACアドレス認証方式を採用している。

2.2. サーバー

2.2.1. センターサーバー

令和 3 年度に教育育員会に構築したセンターサーバーの機器は以下の構成となっており、最長で令和 10 年度まで使用する予定である。

項　目	台数	備　考
校務系 AD サーバー(正)	1	DHCP サーバー機能含む
学習系 AD サーバー(正)	1	DHCP サーバー機能含む
総合管理サーバー	1	vCenter サーバー
仮想基盤サーバー	4	
ストレージ機器	1	Nimble HF20
バックアップサーバー	1	Arcserve UDP 8220 Appliance(24TB)
ファイアウォール(正副)	2	FortiGate 201F　令和 6 年度更新
ルーター	3	令和 3 年度 2 台更新、令和 6 年度追加
標的型サイバー攻撃対策機器	1	Deep Discovery Inspector、令和 5 年度更新
無線ネットワーク管理サーバー	1	UNIFAS　令和7年度更新

2.2.2. 仮想マシン

センターサーバー内の仮想マシンは、主に以下のものが稼働している。

項　目	備　考
校務系 AD サーバー(副)	DHCP サーバー機能含む
学習系 AD サーバー(副)	DHCP サーバー機能含む
校務系プロキシサーバー	i-FILTER
学習系プロキシサーバー	i-FILTER　令和 7 年度廃止予定
校務系プリントサーバー	
学習系プリントサーバー	
校務系 WSUS サーバー	
学習系 WSUS サーバー	

校務系グループウェアサーバー	サイボウズ ガルーン
校務系メールサーバー	
校務系スパム対策サーバー	Barracuda Email Security Gateway
校務系資産管理サーバー	SKYSEA ClientView
校務系教材サーバー	IIS Web サーバー 英語教材等配信
学習系教材サーバー	IIS Web サーバー 英語教材等配信
校務系ウイルス対策サーバー	Apex One
学習系ウイルス対策サーバー	Apex One 令和 7 年度廃止予定
セキュリティ統合管理サーバー	Apex Central 令和 5 年度構築
校務支援システム	Te-Comp@ss 令和 3 年度仮想サーバー移設
CMS	NetCrew 令和 5 年度仮想サーバー移設

2.2.3. ファイルサーバー

校務系のファイルサーバーについては、センターサーバーのストレージに各校 300GB 程度の共有フォルダーを作成し、校長・教頭・教諭・事務・養護・栄養の職種によって、文書分類表に基づきアクセス権を制御している。

令和7年9月現在の使用容量等は以下のとおりである。

- 使用容量 6.5 TB
- ファイル数 663 万個
- フォルダー数 135 万個

2.2.4. CMS

- 仮想マシン上に構築された小中学校ホームページ管理システム（CMS）については、令和10年度にクラウド化する予定である。
- Active Directoryとの同期はしていない。

2.3. 端末

2.3.1. 校務用端末

- 校務用端末については、15インチのWindows端末を使用している。
- SKYSEA Client View をインストールし、トラブル時に教育委員会からのリモート操作によるサポートを行っている。
- Microsoft Office については、Microsoft 365 Apps for Enterprise（旧名：Office365 ProPlus）をインストールし、毎年ライセンス更新を行っている。
- 端末はADサーバーにより管理を行っており、Microsoft Intuneは使用していない。
- エンドポイントセキュリティについては、Trend Micro Apex Oneをインストールして集中管理を行い、標的型サイバー攻撃対策機器（Deep Discovery Inspector）と連携させている。
- Webフィルタリングについては、i-FILTER及びi-FILTER@Cloudを使用している。

2.3.2. 学習用端末

- 学習用端末については、Chromebook端末を使用している。
- Google GIGAライセンスを適用し、Google Workspace管理コンソールを用いて管理している。
- Webフィルタリングについては、i-FILTER@Cloudを使用している。
- 図書システム用のWindowsノートパソコンが15台稼働しており、今後全校に導入予定である。

2.4. 学習環境

- クラウドの学習環境として、Google Workspace、ロイロノート・スクール及びWinBird授業支援 for Chromeを使用している。
- 学習用のMicrosoft Officeについては、Microsoft 5XS0001 O365ProPlusEdu ShrdSvr ALNG SubsVL MVL PerUsrのライセンス特典である Student Use Benefit を利用している。
- ドリル教材については、ラインズ株式会社のラインズeライブラリアドバンスを使用している。
- 学習e-ポータルについては、まなびポケットを採用しているが、MEXCBTとの接続にのみ使用している状況である。

2.5. アカウント

現在運用している主なアカウントは以下のとおりである。

アカウント	使用者	登録	採番方法等
校務用 AD	教職員	手作業	
校務支援システム	教職員、児童生徒	AD 連携、手作業	教職員のみ AD 連携
サイボウズガルーン	教職員	手作業	
メールアドレス	教職員	手作業	
児童生徒用 AD	教職員、児童生徒	手作業	
Google Workspace	教職員、児童生徒	手作業	
Microsoft365	教職員、児童生徒	Google Workspace と同期	SSO
ラインズ e ライブラリアドバンス	教職員、児童生徒	手作業	SSO
丹波市電子図書館	教職員、児童生徒	手作業	SSO 不可
まなびポケット	教職員、児童生徒	手作業	SSO
MEXCBT	教職員、児童生徒	まなびポケットと同期	
各種デジタル教科書	教職員	手作業	一部 SSO あり
CANVA	教職員、児童生徒	Google Workspace と同期	
FigJam	教職員、児童生徒	Google Workspace と同期	
ロイロノート・スクール	教職員、児童生徒	手作業	SSO
WinBird 授業支援 for Chrome	教職員、児童生徒	Google Workspace と同期	SSO

2.6. 保守

- センターサーバー関連は、「株式会社システムリサーチ」が保守を行っている。
- 丹波市イントラネットは、「株式会社鳥取県情報センター」が保守を行っている。
- 無線LANは、「NTT西日本株式会社」が保守を行っている。
- 標的型サイバー攻撃対策機器（Deep Discovery Inspector）は、「NTT西日本株式会社」が保守を行っている。
- CMSは、「福泉株式会社」が保守を行っている。
- 校務支援システムは、「株式会社さくらケーシーエス」が保守を行っている。
- 機器の保守は、学校教育課教育情報管理係にて、正職員3名と会計年度任用職員1名の体制としており、サーバーの保守以外は職員にて対応している。

3. 次期ネットワークについて

本項では本市が考える次期ネットワークの基本的な考え方を示す。本内容をもとに、具体的な次期ネットワークを提案すること。

3.1. 次期ネットワークの基本方針

本市における ICT の活用推進は、校務の効率化や学校の組織力向上のために重要な取組であり、これまでも環境整備に努めてきた。しかし、現行の校務系ネットワークは、校務用端末の校内持ち運びや遠隔利用に対応できていない。また、学習系ネットワークと分離されているため、データ共用や連携が困難であることから、データ受け渡しの負担が増大しているといった課題がある。

また、不正アクセス防止等の十分な情報セキュリティ対策を講じることは、学校における安全安心な ICT 活用のために必要不可欠であるが、現行ネットワークでは、整備当時のセキュリティの考え方である「ネットワーク分離による対策」に基づいているため、「アクセス制御による対策」と比べ業務効率や利便性等が犠牲になっている。具体的には、個人情報を取り扱う職員室、教材を共有する教室等でデータの取扱いに応じてネットワークを分離し、複数の端末を使い分けるような運用を余儀なくされている。

こうした ICT 環境の制約やそれに伴う校務負担の増大が、生徒に関わる時間確保の障壁となっている。本業務では、教員が場所や時間の制約等をできる限り受けずに ICT を活用できる環境を実現するため、「教員の業務効率化」と「セキュリティ強化」を両立するための基本的な考え方を、以下のとおり定める。

① 汎用的なクラウドサービスの活用

教員が校務で利用するサービスや機能を、できる限り低コストで、セキュリティを確保しつつ、使いやすいものが安定的に提供され、かつ将来の機能・性能拡張等にも柔軟に対応できるものにしたい。そのために、本市のサーバー上に構築された校務に係るアカウント管理、グループウェア、ファイルサーバー等の機能について、Microsoft365 を中心とする汎用的なクラウド環境に移行し、ゼロトラストの考え方に基づいたアクセス制御の仕組みを導入する。

② どこでも安全に校務ができる ICT 環境の整備

本市では、令和 9 年度に校務支援システムの更新を予定している。次期校務支援システムは、文部科学省が提唱する「次世代の校務支援システム」を採用することを見据え、ロケーションフリーでの校務実施や、校務系と学習系データの円滑な連携を可能としたい。

本業務においては、次期校務支援システムへの更新後に、教員が端末を持ち運びし、職員室のみならず、出張先、自宅等の校外からも職員室内と同様、安全に校務ができる環境を整備する。具体的には、校外での教材作成や、自宅から校務用のシステムにアクセスするような使い方が想定される。

③ アカウント管理と保守体制のスリム化

本市では、アカウント管理の負担軽減とトラブル対応の迅速化を課題としている。多様なシステムごとに個別のアカウント管理が必要な現状を改善するため、統合 ID 管理ツールの導入等による、運用管理業務の効率化と自動化を目指す。

また、現行ネットワークは複数の事業者によって構築・運用されているため、トラブル発生時の対応に時間や手間がかかることが課題となっている。特に複雑なトラブルでは、事業者間の連携や調整に多くの労力を要している。今後、職員の異動など運用体制の変化も見据え、運用管理ドキュメントの整備や後進の育成とともに、事業者間のコミュニケーションをより緊密にし、運用保守にかかる本市職員の負担が軽減されることを強く望んでいる。

3.2. 次期ネットワークの全体構成イメージ

次期ネットワークの全体構成イメージを以下に示す。これらのイメージは、国が示すアクセス制御を前提としたネットワークを本市の ICT 環境に置き換えた概念図であり、図中に示す各セキュリティ要素技術等の必要性を十分に考慮したうえで、本市にとって費用対効果の高い構成を提案すること。

なお、令和 8 年度から 9 年度にかけて校務支援システム、令和 9 年度から 10 年度にかけて CMS をそれぞれクラウド化する予定である。その上で、現在教育委員会に設置しているオンプレミスのサーバー機器を、最小限の構成で令和 10 年度に更新する。

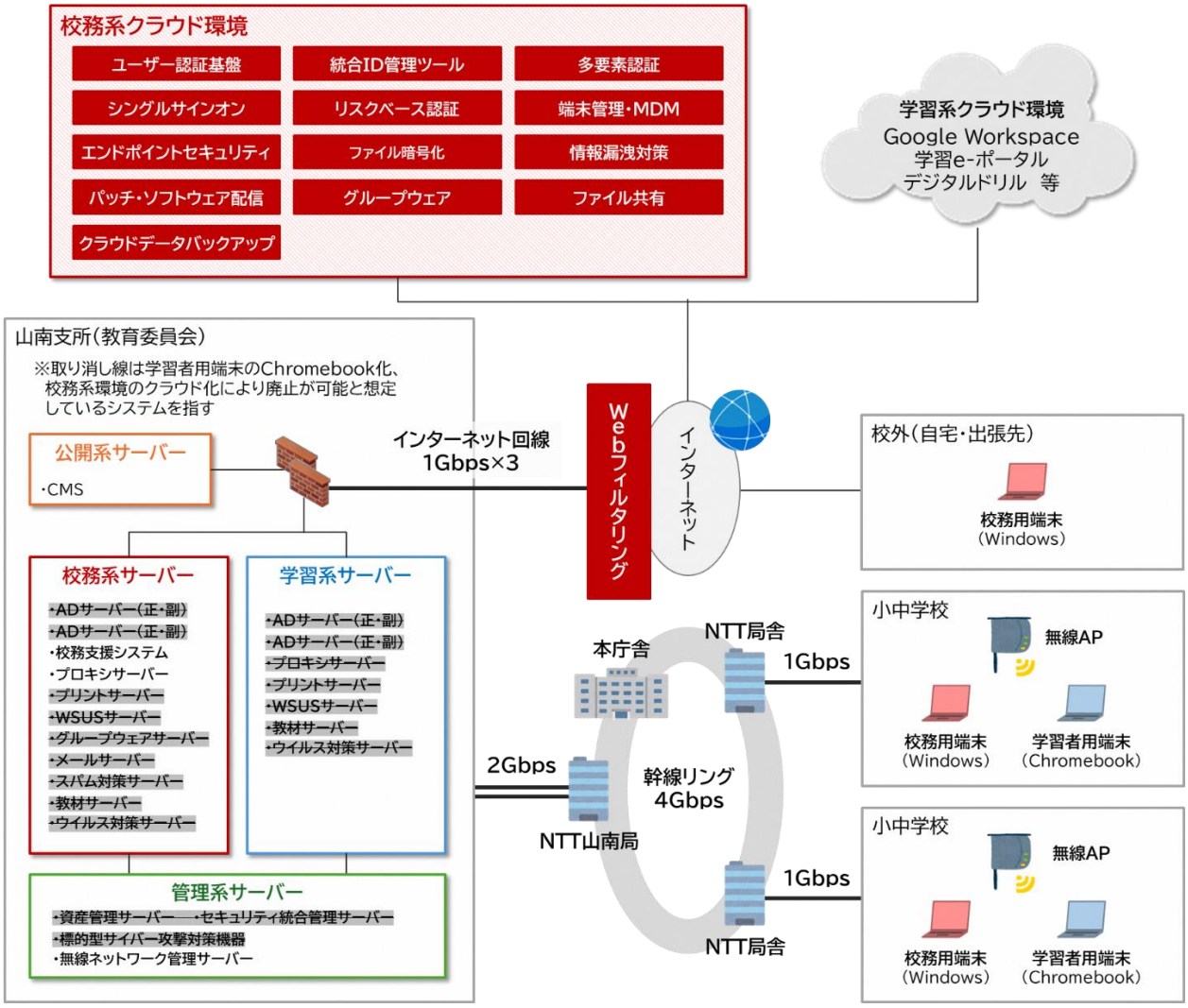


図 3-1 次期ネットワークの全体構成イメージ

4. 業務委託内容

4.1. 構築移行業務

4.1.1. プロジェクト管理業務

(1) プロジェクト計画書の策定

本書に基づき、本システムの構築における具体的な体制、スケジュール、プロジェクト管理方針、プロジェクト管理方法等を含んだプロジェクト計画書を作成すること。

(2) プロジェクト管理

項目	要件
進捗管理	プロジェクト計画策定時に定義したスケジュールに基づく進捗管理を実施すること。 受注者は、実施スケジュールと状況の差を把握し、進捗の自己評価を実施し、定例報告会において本市に報告すること。 進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正の計画を策定すること。
品質管理	プロジェクト計画策定時に定義した品質管理方針に基づく品質管理を実施すること。 受注者は、品質基準と状況の差を把握し、品質の自己評価を実施し本市に報告すること。 品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定すること。
課題・リスク管理	プロジェクト計画時に抽出したリスクを管理し、リスクが顕在化した場合は課題として管理すること。 課題発生時には、速やかに対応策を明らかにし、本市と協議のうえ、対応方法を確定し、課題が解決するまで継続的に管理すること。
変更管理	仕様確定後に仕様変更の必要が生じた場合には、受注者は、その影響範囲及び対応に必要な工数等を識別したうえで、本市と協議のうえ、対応方針を確定すること。

(3) 会議体

本市関係者に対し、作業の進捗状況、工程等の報告を行うための定例会議を1箇月に2回程度主催すること。本稼働後、トラブルなく稼働していると判断できた以降は 1 箇月に1回程度とする。なお、定例会議の終了後 5 開庁日以内に議事録を作成し、電子データで本市担当者に提出し審査・承認を受けること。

(4) プロジェクト体制

業務実施にあたり受注者は本業務を確実に履行できる体制を整備し、プロジェクトに必要なスキルを持った要員を配置すること。なお、プロジェクト発足時からの要員変更にあたっては、必ず本市の了承を得るとともに、変更後の要員のスキルが前任者と同等以上であることを担保すること。

4.1.2. 設計・構築業務

次期ネットワークについて、基本設計、詳細設計、移行設計を行い本市と各種設計書のレビューにて承認を得ること。また、本市の設計レビューにて承認された内容にもとづき、提供するサービスやシステムの構築作業を行うこと。

4.1.3. 検証・テスト業務

(1) テスト方法

受注者は、各種テスト計画書等に基づいて、単体テスト、結合テスト、総合テスト、連携対象システムとの連携テストを主体的に実施すること。また、総合テストおいて発生した障害は、必要に応じて本市へ報告を行った後、復旧作業及び原因の解明、対策を行うこと。また、性能面での問題が発生した場合には、チューニングを施すこと。

各テスト実施時には、テスト実施前にテスト計画書を作成し、具体的な内容を本市と協議すること。また、各テスト終了時には、テスト結果報告書を作成し、本市に提出すること。

(2) テストデータ

各テストで使用するテストデータに関しては、受注者においてテストデータを準備すること。なお、総合テスト以降のテスト工程において、実データが必要な場合には、別途本市と協議すること。受注者の開発環境における実データによるテスト実施は認めない。

4.1.4. 移行・切替業務

現行ネットワーク環境から移行が必要なデータを以下に示す。現行ネットワーク環境からのデータ抽出については受注者自身が行うこととし、各システムへのログインに必要な情報は本市から提供する。

なお、システム運用・各業務への影響を最小限に止めるために、極力各業務の繁忙期を避け、業務に対する影響を抑制するように調整すること。また本市に事前に計画を説明し承認を得ること。

なお、ここに記載されていない他のシステムについても、本市と協議のうえ必要なデータは次期ネットワークに移行すること。

No.	機能名称	移行データ
1	ファイル共有	・校務系ファイルサーバー内のファイル、フォルダー等

4.1.5. 周辺環境の設計・設定指示業務

次期ネットワークへの移行に伴い、既存のセンターサーバーや校内ネットワークに設定変更が必要になることが想定される。また、本業務と並行して、別途、校務系と学習系を一体化した教職員用タブレット端末（約 560 台）の更新を予定している。教職員用タブレット端末の導入にあたっては、マスタ作成とキッティング指示書の作成を行うこと。なお、キッティング作業は、別途教職員用タブレット端末導入業者にて実施するため、本業務の範囲外とする。

本業務受注者は、以下の役割分担に則り、これら周辺環境の設定変更や作業を行う事業者と協議の上、設定指示書の作成や設定作業の支援を行うこと。

○:主担当　△:支援

No.	作業内容	本市	受注者	設定変更 実施者
1	既存機器情報、最新設計と書類の提示	○		△
2	既存環境調査(書類、必要に応じて現地)	△	○	△
3	影響範囲の洗い出し		○	△
4	保守業者等への設定指示書の作成		○	
5	既存機器の再設定(設定変更)		△	○
6	設定変更後の動作確認		△	○
7	設計図書類の改版(変更内容の反映)		△	○
8	設定変更後の既存機器の保守			○
9	1～8 の進捗管理・総合テスト		○	

4.1.6. ネットワークアセスメント業務

ネットワークアセスメントとして、以下の各調査を実施すること。実施場所は山南支所(教育委員会)及び市内 1 校とし、対象校については別途本市より指定する。

なお、本調査は、端末一斉利用時における通信遅延や通信断の原因及び改善方法を特定することを一つの目的としている。そのため、実際に複数台の端末が一斉利用される時間帯に調査を行うか、受注者にて端末を一斉操作するなどし、ピーク時のネットワーク状態を調査すること。

(1) 実施計画策定

(ア) ネットワークアセスメントの実施内容、実施方法等を記載したネットワークアセスメント調査計画書を作成し、本市に提示のうえ承認を得ること。

(イ) 本市関係者(教育委員会担当者、学校関係者、現行ネットワーク事業者等)にヒアリングを行い、現状の課題、調査項目詳細、必要資料等を整理すること。

(ウ) 文部科学省が発行する「GIGA スクール構想の実現　学校のネットワーク改善ガイドブック(令和 7 年 6 月)」に記載の内容にもとづき、調査項目や測定方法を検討すること。

(2) ネットワークアセスメント実施

(ア) 机上調査

既存の完成図書(論理構成図、物理構成図、機器スペック等)等を参照し、ネットワークの構成や設定について物理的・論理的に不具合となり得る箇所の有無を特定すること。

(イ) スループット調査

校内ネットワークの入口の帯域を複数回測定し、学校全体の実効帯域を調査すること。また、教室からも複数回測定し、教室からの実効帯域を調査すること。調査結果をもとに、文部科学省が示す推奨帯域との比較を行うこと。

(ウ) レイテンシ調査

学校内の機器間の応答時間や、利用しているインターネット上のソフトウェアサービス間の応答時間（レイテンシ）の測定を行うこと。調査結果をもとに、応答時間が遅くなっている区間（ボトルネック）を特定すること。

(エ) トラフィック調査

ネットワーク機器の処理性能に対して、トラフィック（通信データの量）がどの程度流れているかを調査すること。調査結果をもとに、通信が正常に処理できない区間（ボトルネック）を特定すること。

(オ) セッション調査

山南支所のインターネット接続ポイントにおいて、ファイアウォールやルーター機器等のセッション上限数を調査すること。調査結果をもとに、活用率の高い主要なアプリケーションごとに、同時端末接続数の上限目安を算出すること。

(カ) CPU・メモリ調査

山南支所のインターネット接続ポイントで稼働するファイアウォール等の機器や、校内の主要なネットワーク機器の CPU・メモリ使用率を調査すること。調査結果をもとに、通信が正常に処理できない区間（ボトルネック）を特定すること。

(キ) 無線 LAN 調査

無線アクセスポイントの電波状況を調査すること。具体的には、校内の複数地点において電波強度、電波干渉、チャネルの設定状態を確認し、問題の有無を確認すること。報告資料については、本市より提供する各校の図面に無線アクセスポイントの設置場所を記録し、視覚的に問題の有無が把握しやすいように表現すること。

(3) 調査結果報告

ネットワークアセスメントの実施結果をもとにネットワークアセスメント調査報告書を取りまとめ、本市に問題の有無や改善策の提言を行うこと。改善策はできる限り複数案を示し、それぞれの案についてのメリット・デメリット、概算費用も合わせて提示すること。

4.1.7. 初期サポート

(1) 教職員からの直接連絡窓口（ヘルプデスク）の開設

(ア) 新旧環境の並行稼働期間及び本稼働直後において、教職員からの直接連絡を受ける体制を確立し、本業務で導入する各サービスの操作方法や仕様等に関する問い合わせに対応すること。

(イ) 窓口の開設時間は平日 9 時 00 分から 17 時 00 分までを必須とする。

(ウ) 教職員からの問い合わせ手段は問い合わせフォーム、電話及び電子メールを必須とし、チャットボットやオンサイトサポートなど、その他に効果的な手段があれば提案すること。

(エ) 問い合わせが集中する時間帯（夕方を想定）には、電話回線や人員を増員するなどし、教職員を待たせない工夫を行うこと。

(2) FAQ の作成・掲載

(ア) 窓口宛に問い合わせがあった内容を FAQ として取りまとめ、週 1 回以上はグループウェアの掲示板等に掲載すること。

(イ) FAQ はサービス別や問い合わせ内容別に分類し、検索性を高める工夫を行うこと。

(ウ) 教職員からのフィードバックを受け、必要に応じて FAQ の内容を改善すること。

(3) 運用保守

(ア) 初期サポート期間において、4.2 保守運用業務に記載の内容を対応すること。なお、初期サポート期間は令和8年9月1日～令和9年3月 31 日までとする。

4.1.8. 研修業務

本システムを利用する教職員、システムの維持管理を行う本市システム担当者に対して、運用開始日までに研修を実施すること。

(1) 研修対象者・研修方法

研修対象者、研修方法は以下のとおりとする。

研修対象者	対象者数	研修方法
本市システム管理者	3 名	対面
教職員	約 550 名	動画配信

(2) 共通事項

(ア) 受注者は研修で使用するシナリオを作成し、事前に本市の承認を得ること。

(イ) 研修には本システムに精通した研修講師及び補助員を配置すること。

(ウ) 研修用 PC、ネットワーク環境及びプロジェクター等の投影資材は本市が用意する。

(3) 教職員向け研修

(ア) 本業務で提供する各サービスの基本的な操作方法を動画形式に纏めて提供すること。教職員が特定の機能やサービス単位で閲覧できるように分割し、体系的に整理すること。

(イ) 動画は教職員が任意のタイミングで閲覧でき、閲覧回数に上限を設けないこと。

(ウ) 動画は教職員用タブレット端末のブラウザや、メディアプレーヤー等のアプリケーションを用いて閲覧できること。

(エ) 動画には字幕表示を付けること。

(4) システム管理者向け研修

(ア) 次期ネットワークの基本構成や運用管理手順について、具体的な操作例や画面を用いて説明すること。

(イ) システム管理者としての役割や、クラウド環境で求められる障害発生時の初動対応、日常的な運用・保守業務のポイントを整理し、チェックリスト等を活用して説明すること。

4.2. 保守運用業務

システムの安定運用のため、以下に示す内容を実施すること。また、その他必要とされる作業があれば提案すること。

4.2.1. 対応時間

保守対応時間は下表の通りとする。本サービス条件はすべての保守（ハードウェア保守、ソフトウェア保守、障害対応）に適用する。ただし、本市が必要と判断した場合は下表の時間以外でも対応すること。

条件項目	内容
問い合わせ受付時間帯	平日 9 時 00 分～17 時 00 分
障害受付時間帯	
障害対応時間帯（※）	
セキュリティ監視・分析・隔離復旧等	24 時間 365 日

（※）17 時 00 分以前に着手した場合は、17 時 00 分以降も継続して復旧対応を行うこと。

4.2.2. 保守運用業務要件

(1) 問い合わせ対応

ア 運用に関する主に技術的な質問等について、電話、電子メール等での問い合わせに対応すること。なお、問い合わせは本市システム担当者から行うものとする。

イ 問い合わせ内容は、作業実績や保守運用上の課題と合わせて保守月次報告書に記録し、保守・運用定例会にて本市に報告を行うこと。

(2) 障害対応

ア 障害を検知、認識した場合は、直ちに障害原因の調査に着手し、情報収集、障害切り分け、ログの解析、復旧処理等の対応を行うとともに影響範囲、復旧目途やその手法等を本市に報告すること。

イ 障害の切り分けにおいて、他のシステム関連業者に障害が起因する場合には、必要に応じて当該業者と連携のうえ、対応すること。

ウ 障害対応にあたっては、仮復旧等の一時的な対処と本格復旧作業に分けて行うなどし、可能な限り学校の ICT 環境の機能維持を優先すること。

エ 障害対応において、設計担当者の支援を受けられるようにすること。特に障害の根本対応の検討については、設計者も参画させ、必要に応じて設計から見直すこと。

オ 障害対応の完了後に、障害の原因、影響、対応経過、根本対応等を記載した障害対応報告書を提出すること。

(3) 構成管理ドキュメントの最新化

ア 安定的な ICT 環境の運用管理のため、設計書、作業手順書、マニュアル等の運用資料を整備・更新し最新の状態に保つこと。

イ 資料については、更新履歴を併記して版数管理を行うこと。

ウ 資料の管理ルールを作成し、これに従い運用すること。

(4) クラウドサービス稼働状況等の点検・報告

ア　本業務で導入する各クラウドサービスの稼働状況を監視すること。

イ　クラウドサービスで障害が発生した際、管理画面からその事案内容及びクラウドサービス事業者の対応状況・改善状況が確認できること。

(5) セキュリティ脆弱性対応

ア　教職員用タブレット端末等にインストールするアプリがある場合、新たに発見された脆弱性については、ベンダー等からの情報収集を継続的に行い、必要な対応策を速やかに適用すること。

イ　重大な脆弱性が発見された場合は、影響範囲の調査およびリスク評価を実施し、対応方針を本市に報告するとともに、遅滞なく更新プログラムの適用を行うこと。

ウ　脆弱性対応の履歴および対応状況を記録し、要請があった場合は本市へ報告できるようにすること。

(6) セキュリティ監視・分析・隔離復旧等

ア　『5.8. エンドポイントセキュリティ』から収集されるデータを 24 時間 365 日体制で監視し、セキュリティインシデント発生時は、被害拡大の防止を最優先として対処を行うこと。

イ　不審な挙動を検知した際に、管理者の判断や操作を介さずに、プロセス停止などの自動対処を行えること。なお、SOC サービス等との連携による実現も可とする。

ウ　インシデント対応および復旧作業の内容を記録し、事後に本市へ報告すること。

(7) 保守・運用定例会の開催

ア　前月までの問い合わせ対応実績や作業実績、課題等を取りまとめた保守月次報告書を作成し、保守・運用定例会にて本市に報告を行うこと。

イ　保守・運用定例会の開催頻度については、月1回程度とし、開催方法等については、受注者より本市に提案し了承を得ること。なお、保守・運用定例会を開催しない月においても、毎月 10 日までに「保守月次報告書」を電子メールにて提出すること。

(8) 年次更新作業

ア　教職員の新規採用、異動、休職、退職の際には、アカウント情報の編集及びアクセス権限付与等の作業を行うこと。

イ　本業務で導入する校務系の各サービス及び Google Workspace は受注者にて作業を実施すること。その他の既存サービス・システムについては、受注者より CSV ファイルを提供し、本市にて各既存サービス・システムへ投入する。

ウ　年度更新作業の手順書をもとに作業を行うこと。作業終了後は実施結果を記録し、本市に報告すること。

エ　年度更新作業に伴い発生した不具合や課題については、速やかに本市に報告し、必要な対応を行うこと。

5. 機能要件

5.1. ユーザー認証基盤

5.1.1. 機能概要

ユーザー認証基盤とは、校内ネットワーク上(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ーの ID 及び認証情報を一元管理し、認証を行う機能を指す。また、ユーザーの利便性を高めるシングルサインオン機能のベースとなる。

5.1.2. 現行ネットワーク環境

現行ネットワーク環境では、ユーザー認証基盤として Microsoft の Active Directory(以下「AD」という。)を利用している。学校内のネットワークは、校務系ネットワークと学習系ネットワークの 2 層に分離されており、校務系ネットワークには校務用 AD を設置し、教職員の ID および認証情報を登録している。また、校務系ネットワークに属する各サーバーおよび端末は、校務系ドメイン(tamba.edu.local)に参加して運用している。

なお、学習用に Web 版 Office を使用しているため、Microsoft365 のテナントには、初期ドメイン(tambaedu.onmicrosoft.com)以外に Google Workspace のドメイン(g.tamba.ed.jp)を追加し、Google Workspace のアカウントを登録している。そのため、OneDrive に学習データが一部保存されていることにも留意されたい。また、ユーザー認証については、Entra ID ではなく Google Workspace 側で認証を行うように設定している。

5.1.3. 次期ネットワーク環境

次期ネットワーク環境ではクラウドサービスを利用することから、SAML 認証、OpenID Connect、OAuth 等に対応したユーザー認証基盤が必要となる。さらに、後述するリスクベース認証、ファイル暗号化(IRM)、および情報漏洩対策(DLP)機能の実現を踏まえ、Microsoft 365 A5 の利用を想定している。

また、センターサーバーの仮想基盤上で稼働している校務支援システムは、現在校務系 AD と ID 連携しているが、令和 9 年度の校務支援システムのクラウド化を機にこの連携を解除し、校務系 AD を廃止する予定である。そのため、令和 8 年度に更新する教職員用タブレット端末については、EntraID と Intune により管理し、校務系 AD ドメインには参加しない。

加えて、本市が導入を予定している次期校務系クラウド(Microsoft 365)と、既存の学習系クラウド(Google Workspace)とのアカウントについても、双方のアカウントを一元的に管理、連携できることが望ましい。

5.1.4. 機能要件

(1) アカウント管理・認証機能

- 次期校務系ネットワークにおける教職員アカウント、教職員用タブレット端末およびサーバー情報の一元的な管理が行えること。
- 本業務で導入するクラウドサービスの認証情報を一元的に管理できること。
- 年度替わり等に伴う異動情報の反映がわかりやすく、容易に行えること。

(2) 認証用IDの統一機能

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

(3) 連携機能

- 『5.2 統合ID管理ツール』、『5.3 多要素認証』、『5.4 シングルサインオン』との連携が取れること。
- 必要に応じて、『5.9 ファイル暗号化（IRM）』、『5.10 情報漏洩対策（DLP）』、『5.13 ファイル共有』等の機能と連携が取れること。

(4) ユーザー制御、端末制御ポリシー管理機能

- 教職員用タブレット端末に対して、ネットワークドライブの自動割り当て、プリンタ設定の適用などの各種設定をスクリプト等により配布・適用できること。

(5) 既存オンプレミス環境とのID連携

- 次期校務系ネットワークのMicrosoft 365環境と、既存のオンプレミス環境に構築された校務系AD環境とのID連携は現状では不要と考えているが、ID管理の効率化やセキュリティ強化のために必要と考えられる場合には、提案も可とする。
- オンプレミス環境にEntra Connectサーバー等の構築が必要な場合は、その構成を提案すること。

(6) 学習系ネットワーク環境とのID連携

- 次期校務系ネットワークのMicrosoft 365環境と、学習系ネットワークのGoogle Workspace環境とのID連携が可能であること。
- シングルサインオン（SSO）による認証連携（SAML2.0等）に対応していること。
- SCIMを利用したIDプロビジョニング（ID情報同期）に対応していることが望ましい。

(7) カスタムドメイン

- 現在使用している初期ドメイン（tambaedu.onmicrosoft.com）については、カスタムドメイン（m.tamba.ed.jp等）への変更または新規作成を行うこと。

5.1.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.2. 統合 ID 管理ツール

5.2.1. 機能概要

統合 ID 管理ツールとは、組織内のアカウント情報を一元的に管理し、複数のシステムやクラウドサービスにまたがる ID 情報を統合的に運用できる仕組みを指す。教職員の異動や児童生徒の入学、進級、卒業、転校などのイベントに応じて、アカウントの作成・変更・削除を一元化し、効率的な ID ライフサイクル管理を実現する。

5.2.2. 現行ネットワーク環境

現行ネットワーク環境では統合 ID 管理ツールを導入していないため、手作業にて Active Directory、グループウェア、授業支援システムなどのアカウントの作成・変更・削除を行っている。

5.2.3. 次期ネットワーク環境

次期ネットワーク環境では、Microsoft 365 アカウントと Google Workspace アカウントの統合的な管理に加え、各種システムおよびクラウドサービスにおける煩雑な ID 管理の効率化と情報セキュリティの向上を目的として、統合 ID 管理ツールの導入を想定している。

5.2.4. 機能要件

(1) IDライフサイクル管理

- アカウントの作成・変更・削除などのIDライフサイクルを一元的に管理できること。
- 教職員の異動や、児童生徒の入学、進級、卒業、転校等の情報をもとにID管理が行えること。

(2) 各種システムとの連携

- CSV出力、取込による各種システムとの連携が可能であること。
- Microsoft 365（Microsoft Entra ID）、Google Workspace に対応していること。

(3) セキュリティ・監査

- アクセス制御、パスワードポリシー設定、二要素認証など、適切な認証・認可機能を有すること。
- 操作ログ、監査証跡の記録・保管が可能であること。

(4) 操作性・将来性

- Webブラウザ上で操作可能なGUIを備えていること。
- 将来的な拡張性を考慮した設計とし、連携先アプリケーションが増えた場合でも、サービス利用料が変動しないこと。（例：新たなクラウドサービス追加時の対応）

5.2.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す教育委員会のシステム管理者とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末のうち、教育委員会にて使用する端末のみとする。

5.3. 多要素認証

5.3.1. 機能概要

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。教育情報資産のアクセス制御として、その重要度に応じてパスワード以外に生体認証や物理認証等の複数の要素を利用して厳格に本人認証を行う必要がある。

5.3.2. 現行ネットワーク環境

現行ネットワーク環境では、教職員が教職員用タブレット端末にログインする際、多要素認証は行っていない。

5.3.3. 次期ネットワーク環境

次期ネットワーク環境では、端末ログイン時やクラウド利用時等のタイミングで、多要素によるユーザー認証ができる仕組みを構築すること。認証要素としては、端末や USB トークン等を用いたデバイス認証、顔や虹彩等を用いた認証等が考えられる。

5.3.4. 機能要件

(1) 多要素認証機能

- 教職員用タブレット端末へのログインや各種クラウドサービス利用時に、認証の3要素（知識情報、所持情報、生体情報）のうち、2要素以上を同時に用いた認証が可能であること。
- 認証要素としては以下が考えられる。
  - ID、パスワード、PIN コード（知識情報）
  - USB トークンなどのセキュリティキー（所持情報）
  - 顔、指紋、虹彩等による認証（生体情報）
- ICカードやセキュリティキー等の物理的な媒体が必要となる場合は、その媒体の費用についても見積もりに含めること。
- 端末に顔認証対応カメラ等の機器が必要な場合は、その旨を提案書に記載すること。

(2) 画面ロック機能

- 利用者が一定時間端末の操作を行わなかった場合、自動的に画面ロックを実行できること。
- 利用者が画面ロックを行わずに離席した際に、自動で画面ロックが行われる機能を有することが望ましい。
- 管理者がロックまでの待機時間をポリシー設定可能であること。
- ロック解除時にも多要素認証が再実行できること。

5.3.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.4. シングルサインオン

5.4.1. 機能概要

シングルサインオンとは、ユーザーが一度の認証で複数のシステムやクラウドサービスへ継続的にアクセス可能とする仕組みであり、利便性の向上と認証管理の一元化を目的とした機能を指す。

5.4.2. 現行ネットワーク環境

現行ネットワーク環境では、『2.5. アカウント』に示す一部アカウントに対してシングルサインオンを行っている。

5.4.3. 次期ネットワーク環境

次期ネットワーク環境では、校務系クラウド環境の Microsoft 365 と、学習系クラウド環境の Google Workspace とのシングルサインオンによる連携およびアカウント同期を想定している。

5.4.4. 機能要件

(1) シングルサインオン機能

- 利用者は1回の認証で、許可された複数の業務システムにアクセスできるシングルサインオン（SSO）機能を利用できること。
- 認証情報は安全に管理され、ID・パスワードの再入力や多重ログインを不要とする仕組みであること。

(2) Microsoft 365およびGoogle Workspaceとの連携

- Microsoft 365およびGoogle Workspaceとのシングルサインオンによる連携およびアカウント同期が可能であること。
- 『5.2 統合ID管理ツール』の機能で要件を満たせる場合は、その利用を前提とした構成を採用してもよいものとする。
- Entra IDを活用し、シングルサインオン対象サービスの一元管理およびアクセス制御（条件付きアクセス等）が行えること。

5.4.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.5. リスクベース認証

5.5.1. 機能概要

リスクベース認証とは、ユーザーのアクセス行動パターン（IP アドレス、端末、場所、時間帯など）を分析し、通常と異なるアクセスが検出された場合に、追加の認証を要求する機能を指す。これにより、なりすましや不正アクセスのリスクを軽減する。

5.5.2. 現行ネットワーク環境

現行ネットワーク環境では、教職員用タブレット端末は職員室からの利用に限定されているため、リスクベース認証は未導入である。

5.5.3. 次期ネットワーク環境

次期ネットワーク環境では、クラウドサービスの利用に伴い、教職員が自宅や出張先から端末を利用する機会も想定されることから、アクセス元に応じたセキュリティ制御が必要であり、リスクベース認証を導入する。

5.5.4. 機能要件

(1) 追加認証

- アクセス行動パターン（IPアドレス、端末、場所、時間帯等）を分析し、通常と異なるアクセスが検出された場合に、追加の認証を要求できること。

(2) レポート

- リスクが高いログインの履歴や、ユーザーの資格情報の漏洩リスクの履歴をダッシュボード等で確認できること。

5.5.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.6. Web フィルタリング

5.6.1. 機能概要

Web フィルタリングとは、校内および校外からインターネットにアクセスする際、特定のコンテンツや Web サイトへのアクセスを制限する機能を指す。これにより、校務上または教育上の観点から不適切とされる Web サイトの閲覧を防止し、安全で健全なインターネット利用環境を実現する。

5.6.2. 現行ネットワーク環境

現行ネットワーク環境では、プロキシサーバーにインストールされた i-FILTER を用いて校務用端末の Web フィルタリングを行っている。教職員用タブレット端末の利用は職員室内に限定されており、学校外からの利用は行っていない。

なお、教職員は学習系の Chromebook 端末も使用しているため、校務用端末で Chrome を使用した際にエージェントがインストールされている場合がある。

5.6.3. 次期ネットワーク環境

次期ネットワーク環境では、校内外を問わず教職員用タブレット端末からインターネットにアクセス可能な運用とすることから、現在利用している i-FILTER@Cloud を継続利用する予定である。ただし、i-FILTER@Cloud にアンチウイルスやサンドボックス等の追加オプションが必要と考えられる場合は提案に含めること。なお、校務支援システムや CMS 等の内部システムについては、本業務の実施後も従来通り学校内からのみの利用に限定する。

5.6.4. 機能要件

(1) Webフィルタリング機能

- 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。
- 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）の設定が可能であること。
- 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。
- 端末の設置場所や利用環境（校内・校外）にかかわらず、常に適切なフィルタリングが適用されること。

(2) SSL復号機能

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

(3) レポート機能

- アクセスしたウェブサイトのURLや時刻の履歴等を記録し、可視化できること。

5.6.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.7. 端末管理・MDM

5.7.1. 機能概要

端末管理・MDMとは、校務用端末およびセンターサーバーの資産管理、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。

5.7.2. 現行ネットワーク環境

現行ネットワーク環境では、SKYSEA Client View（オンプレミス版）にて校務用端末の管理を行っている。

5.7.3. 次期ネットワーク環境

次期ネットワーク環境では、校内外問わずインターネットへアクセスする運用となるため、SaaS型の資産管理システムを採用し、リモートロックやリモートワイプといった遠隔操作機能を備えることが求められる。
Micrsoft365 A5の機能で代用することも可能であるが、不十分である場合には別途サービスを提案すること。

5.7.4. 機能要件

(1) 資産管理機能
- 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。
- ネットワーク機器やプリンタなどの周辺機器についても、構成情報を取得・管理できることが望ましい。

(2) 配信機能
- 対象端末へのプログラム配信等が行えること。

(3) 操作ログ確認
- 対象端末の稼働状況、ファイル操作の確認が行えること。

(4) リモート操作機能
- 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。
- 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（例えば教育委員会内）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。
- 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。

(5) リモートロック・リモートワイプ機能
- 端末の盗難や紛失を想定し、リモートロック・リモートワイプ機能等のMDM機能を備えていること。

5.7.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。

・ 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.8. エンドポイントセキュリティ

5.8.1. 機能概要

エンドポイントセキュリティとは、校務用端末やセンターサーバー等のエンドポイントに対して、マルウェア感染や不正アクセスの防止、脅威の検知・対応を行うセキュリティ対策機能の総称を指す。代表的な機能として、ファイルのスキャンやパターンマッチングによる検出を行う EPP（Endpoint Protection Platform）と、端末上の不審な挙動を検知・記録・分析し、迅速な対処を可能にする EDR（Endpoint Detection and Response）がある。

5.8.2. 現行ネットワーク環境

現行ネットワーク環境では、校務用端末を対象に、Trend Micro Apex One を用いて、EPP によるセキュリティ対策を実施している。なお、標的型サイバー攻撃対策機器（Deep Discovery Inspector）と連携させており、標的型サイバー攻撃対策機器で危険性の高い通信が発見された場合は、Trend Micro Apex Central を通して対象端末の通信を停止している。

5.8.3. 次期ネットワーク環境

次期ネットワーク環境では、校内外からインターネットへアクセスする運用となるため、EPP に加えて EDR 機能を備えた SaaS 型サービスの導入を想定している。ただし、信頼するアプリケーションのみを起動可能とするホワイトリスト型製品を導入し、EDR が不要と判断できる場合には、EDR の導入を行わない選択も可能とする。

5.8.4. 機能要件

(1) EPP機能

・ エンドポイント上で動作するマルウェア対策ソフトとして、以下のような脅威に対してリアルタイムでの検知・ブロック・隔離が可能であること。
  - 既知のマルウェアの実行ファイル、スクリプト、マクロの実行
  - 電子メールに添付された不正ファイルや Web 経由で配布される不正ファイルのダウンロード・実行

・ マルウェアや不正ファイル等を検知した際、管理者へ自動通知可能であること。

(2) EDR機能

・ 以下のようなエンドポイント上の不審な挙動を検知・記録・分析し、マルウェアや内部不正などの脅威に対応できること。
  - 不審なプロセスの起動や、スクリプト・マクロによる不正なコード実行
  - セキュリティ製品の無効化や、システム設定の改変を試みる行為
  - 外部との異常な通信
  - ランサムウェアの兆候となる、大量のファイル暗号化・削除などの異常なファイル操作

・ 不審な挙動を検知した際に、管理者へ自動通知可能であること。

・ 不審な挙動を検知した際に、管理者の判断や操作を介さずに、プロセス停止などの自動対処を行えることが望ましい。なお、SOCサービス等との連携による実現も可とする。

5.8.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.9. ファイル暗号化（IRM）

5.9.1. 機能概要

ファイル暗号化（IRM）とは、次期ネットワークで教職員が取り扱うデータやファイルに対して、機密度に応じたラベル付けと暗号化により保護を行う機能を指す。

5.9.2. 現行ネットワーク環境

現行ネットワーク環境では、ファイル暗号化の仕組みは導入しておらず、ネットワークを校務系、学習系に分離することで各ネットワーク間のファイル移動を制限している。

5.9.3. 次期ネットワーク環境

次期ネットワーク環境では、SaaS 型のサービスを想定しており、取り扱う情報の機密度に応じたラベル等を付与することで、ファイルの暗号化、復号の制御や記録、追跡等の機能を提供する。

5.9.4. 機能要件

(1) 重要性分類に関するラベル定義・付与

- 次期ネットワークにおいて取り扱う情報に対して、「重要性分類」を表すラベルを付与することが可能であること。重要性分類については、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（令和7年3月）」における情報資産の分類等に基づき定義ができること。
- 利用者がファイルを保存する際、重要性分類を表すラベルを当該ファイルに付与可能であること。
- ラベルの付与に対応するファイル形式や、制限事項等について提案書で示すこと。参考までに、教職員が業務で取り扱う主なファイル形式を以下に示す。
  - Microsoft Office ファイル（Word/Excel/PowerPoint で取り扱うファイル）
  - 上記以外の Microsoft Office ファイル（Visio 等で取り扱うファイル）
  - Adobe Portable Document Format （PDF）
  - イメージファイル（GIF、JPEG、PNG、TIFF、BMP）
  - 動画ファイル（MP4、avi、mov、wmv 等）
  - テキスト（TXT/CSV/XML）
- 特定のフォルダーにデータを保存することで、既定のラベルを当該ファイルに付与可能であること。

(2) ファイル暗号化

- 次期ネットワークにおける認証を経た利用者が、暗号化が行われた状態のファイルを参照した場合、当該利用者の権限に基づきファイルの操作（参照／更新）が行えること。なお、操作が完了し再び保存を行う場合は改めて暗号化が行われること。
- 暗号化された状態で格納されたファイルが次期ネットワークの外部に流出した場合、認証を経ていな

い利用者による内容参照等の操作が行えないこと。

- ファイル暗号化時は規定値ラベルやポリシー設定を用いて、自動での暗号化が可能であること。

(3) 情報漏洩対策(操作制御)

- 次期ネットワークにおける認証を経た利用者の各権限に対して、ファイルに付与された重要性分類等に基づくラベル情報をもとに、当該ファイルに対して以下の操作制御が行えること。
  - ファイル操作(参照／更新)の可／不可制御
  - ファイル印刷の可／不可制御
  - 外部への電子メール添付送信の可／不可制御
  - オンライン会議へのファイル添付の可／不可制御
- 上記以外においても、以下の操作に関する制御が可能な場合は、具体的な実現方法等について提案すること。
  - 端末の外部機器(USB、Bluetooth 機器等)へのファイル書出しの可／不可制御
  - 認可されたクラウドサービスへのファイル格納の可／不可制御
  - 認可されないクラウドサービスへのファイル格納の可／不可制御

(4) ポリシー管理

- 次期ネットワークにおいて定義する重要性分類及び重要性分類に応じて行う操作制御について、効率的な定義と適用等管理を可能とするためのポリシー管理を可能とすること。

(5) データ追跡

- ラベリングされたデータを外部に送信した際や、持ち出しされたりした際に、検知・アラート通知ができること。検知・アラートは即時実行されること。
- ラベリングの操作をログにて、追跡できること。

5.9.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.10. 情報漏洩対策 (DLP)

5.10.1. 機能概要

情報漏洩対策(DLP)とは、校務系業務で扱われるデータやファイルの内容に重要情報が含まれているかを判定し、過失または意図的な外部漏洩を防止するために各種制御を行う機能を指す。

5.10.2. 現行ネットワーク環境

現行ネットワーク環境では、「情報漏洩対策(DLP)」の仕組みは導入していない。

5.10.3. 次期ネットワーク環境

次期ネットワーク環境では、SaaS 型のサービスを想定しており、校務系業務で扱われるデータやファイルの内容に重要情報が含まれる場合に、アラートでの警告や操作のブロックなどの機能を提供する。

5.10.4. 機能要件

(1) 重要情報の検出

- 教職員が扱う個人情報や成績情報など、事前に設定した機密情報を自動で検出できること。
- 検出対象は、Exchange Online、SharePoint Online、OneDrive上のデータとする。

(2) ユーザー通知・対応

- ポリシー違反操作（例：外部への機密情報送信）を検出した際、ユーザーに警告やブロック通知を表示できること。
- 電子メール通知によって管理者や担当者へのアラートを送信できること。

5.10.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.11. パッチ・ソフトウェア配信

5.11.1. 機能概要

パッチ・ソフトウェア配信とは、教職員用タブレット端末に対して、OS や Office ソフトウェアの更新プログラム、セキュリティパッチの配信を行うための機能を指す。

5.11.2. 現行ネットワーク環境

現行ネットワーク環境では、センターサーバーの仮想基盤上で校務系 WSUS サーバーを運用しており、プロキシサーバーを経由してインターネットから更新プログラムを取得し、校務用端末へ配信している。

5.11.3. 次期ネットワーク環境

次期ネットワーク環境においては、校務用端末における WSUS サーバーの廃止を前提に、SaaS 型によるパッチおよびソフトウェア配布への移行を検討している。

5.11.4. 機能要件

(1) パッチ配信

- 校務用端末に対して、OSの機能更新プログラム、品質更新プログラム、Office製品のアップデートプログラム等の配信及び管理が行えること。
- 更新プログラム配信対象のグループ分けや配信条件の指定を行えること。

(2) ソフトウェア配信

- セキュリティを保ったうえで、教職員用タブレット端末に対してソフトウェアの配信が行えること。

(3) ネットワーク負荷軽減

- 更新プログラムやソフトウェアの配信に伴うネットワークトラフィックが、イントラネットやインターネット回線に過度な負荷を与えないよう、帯域制御、配信スケジュール設定、ピアツーピア配信の活用等による最適化を図ること。

5.11.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.12. グループウェア

5.12.1. 機能概要

グループウェアとは、組織内の情報共有やコミュニケーション支援を目的として、電子メール、スケジュール・予定表、チャット・メッセージ、オンライン会議・通話、掲示板、ポータルサイト、ドキュメント管理などの機能を統合的に提供する機能を指す。

5.12.2. 現行ネットワーク環境

現行ネットワーク環境では、サイボウズ社の Garoon（オンプレミス版）のグループウェア機能を活用した情報共有およびコミュニケーション支援を行っている。

5.12.3. 次期ネットワーク環境

次期ネットワーク環境では、クラウドサービスの利便性や保守性の向上、他システムとの連携性を考慮し、Microsoft 365 の Exchange Online、Teams、SharePoint Online サービスの導入を想定している。

5.12.4. 機能要件

(1) 電子メール機能

- Outlookを用いて、組織内外との送受信が可能な電子メール機能を提供すること。
- 迷惑メール対策や添付ファイルの制限、自動返信などの基本機能を備えていること。
- 現在の電子メールはサイボウズガルーンサーバー内に蓄積しているが、過去の電子メール閲覧用として当該サーバーを当面の間稼働することも可能であるため、電子メールデータの移行は不要である。

(2) スケジュール・予定表機能

- 利用者または各校の行事予定をカレンダー形式で管理できること。
- 他者との会議調整や予定の共有が可能であること。

(3) チャット・メッセージ機能

- 利用者同士で1対1またはグループによるテキストチャットが可能であること。
- メッセージにはファイル添付やリアクション等が利用できること。

(4) オンライン会議・通話機能

- 利用者同士で音声・ビデオ通話やオンライン会議が実施できること。
- 会議の予約、画面共有、録画などの基本機能を備えていること。

(5) 掲示板機能

- お知らせや業務マニュアルなどの掲示・情報発信が可能であること。

(6) ポータルサイト機能

- 情報共有のためのポータルサイトを学校ごとに作成すること。なお、このポータルサイトは教職員用タブレット端末のブラウザのトップページとして設定することを想定している。
- ポータルサイトには、文書が保存されたフォルダーへのリンク、最近使ったドキュメントの表示、教育委員会及び学校からのお知らせを表示する掲示板、電子メールの新着通知、リンク集等を掲載すること。
- ポータルサイトごとにデザインやナビゲーション、レイアウトをカスタマイズ可能であること。
- 各校におけるポータルサイト管理者による基本的な編集・更新が可能であること。
- 教育委員会職員が横断的に管理できる管理者権限を持てること。
- 各校におけるポータルサイト管理者による基本的な編集・更新が可能であること。
- HTML 等の専門知識を要さずにポータルサイトを作成・編集できること。

(7) ドキュメント管理機能

- 文書ファイルをアップロード・共有・バージョン管理できること。
- アクセス権限を利用者・グループ単位で設定できること。

5.12.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.13. ファイル共有

5.13.1. 機能概要

ファイル共有とは、文書や資料をクラウド上に保存し、他の利用者と安全に共有・共同編集できる機能を指す。個人用の保存領域に加え、グループでの共有フォルダーを活用することで、業務に応じた柔軟な情報共有が可能となる。

5.13.2. 現行ネットワーク環境

現行ネットワーク環境では、『2.2.3 ファイルサーバー』に記載の内容に基づき、ファイル共有等の機能を提供している。

5.13.3. 次期ネットワーク環境

次期ネットワーク環境では、クラウドサービスの利便性や保守性の向上、他システムとの連携性を考慮し、Microsoft 365 の OneDrive や SharePoint Online を想定している。

5.13.4. 機能要件

(1) アクセス制御機能

- ユーザー認証基盤に設定されたアカウント情報を利用し、個人、グループ、職制等によってアクセス権限を付与できること。

- 校務系のデータへのアクセスには、多要素認証が用いられること。
- 校務系のデータには、機密性の観点からユーザー認証だけではなく、端末認証を行うなど、承認された端末以外からのアクセスができないことが望ましい。

(2) ファイルストレージ機能

- 学校ごとに専用のオンラインストレージ領域を持ち、文書やファイルを保存できること。
- ファイルやフォルダーを他の利用者と共有できること。
- 閲覧・編集等の権限を制御したうえで、複数人による同時編集が可能であること。

(3) バージョン管理・復元機能

- ファイルの変更履歴（バージョン）が自動で保存され、任意の時点に復元できること。
- 誤削除や誤操作に備えたごみ箱機能を備えていること。

(4) 端末との同期

- 教職員用タブレット端末において、エクスプローラでの参照、同期が行えること。

5.13.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す全教職員とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末とする。

5.14. クラウドデータバックアップ

5.14.1. 機能概要

クラウドデータバックアップとは、Microsoft 365 の電子メール・コミュニケーション・ファイル共有等の各種サービス（Exchange Online、Teams、SharePoint Online、OneDrive）に保存されたデータを、人的ミスや内部・外部のセキュリティ脅威から保護することを目的として、クラウド環境またはオンプレミス環境にバックアップを取得する仕組みを指す。

5.14.2. 現行ネットワーク環境

現行ネットワーク環境では、センターサーバーの各サーバー及びストレージ内に蓄積されているデータを、オンプレミス環境に設置された Arcserve UDP Appliance によりバックアップ取得・保管している。

5.14.3. 次期ネットワーク環境

次期ネットワーク環境では、教職員等の誤操作によるデータの削除や、サービス障害及びランサムウェア等のサイバー攻撃への対策として、Microsoft 365 上に保存されたデータを別のクラウド環境またはオンプレミス環境へ年に数回バックアップする仕組みの導入を検討している。

5.14.4. 機能要件

(1) バックアップ対象データ

Microsoft 365 A5の訴訟ホールド機能を用いることで、バックアップの代替が可能と考えられるデータについては、任意要件とする。

- Exchange Online の電子メール・予定表・連絡先（任意要件）

- Teams のチャット履歴・添付ファイル・チーム設定情報（任意要件）
- SharePoint Online のサイトデータ・コンテンツ（必須要件）
- OneDrive に保存されたデータおよびメタデータ（必須要件）

(2) バックアップ

- 取得したバックアップの複数世代保持が可能であること。
- バックアップ取得時にMicrosoft 365の各種機能が停止しないこと。
- クラウド環境へのバックアップの場合、あらかじめ容量が決まっている定量定額課金方式であること。
- オンプレミス環境へのバックアップを行う場合、NAS 等の機器が必要であれば提案に含めること。

(3) リストア

- 過去の任意時点の状態へ復元が可能であること。
- アイテム単位(ファイル単位／フォルダ単位等)での個別リストアが可能であること。
- リストアの追加費用がかからないことが望ましい。

5.14.5. 利用者・利用端末

- 本機能の利用者は、『7.1.1.利用者情報』に示す教育委員会のシステム管理者とする。
- 本機能の利用端末は、『7.1.2.端末情報』に示す教職員用タブレット端末のうち、教育委員会にて使用する端末のみとする。

6. 共通非機能要件

次期ネットワーク環境の各機能に共通で求める非機能要件を以下に示す。

(1) 信頼性・可用性

ア　システムは 24 時間 365 日稼働し、定期・非定期メンテナンス等の計画停止を除き、常に利用可能な状態を維持すること。

イ　システムの稼働率は 99.9%以上であることが望ましい。

(2) 拡張性

ア　SaaS 上に配置するシステムについては、アクセスするユーザー数やパフォーマンス状況に応じて、動的にリソースが調整されるオートスケールに対応していることが望ましい。

イ　管理者自らが容易にアカウント管理や権限設定ができること。

ウ　カスタマイズを伴わずに機能追加・修正が可能な設計であること。

(3) 性能

ア　教職員がストレスなく各機能を利用できる性能を確保すること。

イ　繁忙期や始業時刻等のアクセス集中時にも、校務や教材作成等に支障のないレスポンスを保証すること。

ウ　各種端末から、主要なブラウザを用いて快適に利用できること。

(4) セキュリティ

ア　次期ネットワークの構築に際してサーバー等の機器を設置する場合は、特段の理由等がない限り構築時点における最新の OS を利用し、最新のセキュリティパッチを適用すること。

イ　次期ネットワークの構築・運用に際しては、以下の各資料の内容を十分に理解したうえで、万全の対策を講じること。

(ア)　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（令和 7 年 3 月改訂版）」

(イ)　丹波市教育委員会情報セキュリティ対策基準

ウ　個人情報保護法等の法令を遵守し、物理的・技術的・人的セキュリティ対策を徹底すること。

エ　本市ネットワーク内外からの不正な接続及び侵入、情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。

オ　通信および保存データの暗号化（SSL/TLS 等）を実施すること。

カ　ウイルス対策ソフトウェアをサーバー・端末に常駐させること。

キ　サービスの利用記録や例外事象のログを蓄積し、不正検知・原因特定に活用できること。

(5) バックアップ

ア　バックアップデータは安全なデータセンターで管理し、災害時にも迅速な復旧が可能であること。なお、オンプレミス環境に NAS 等を設置してバックアップを取得する提案も可とする。

イ　業務データのみならず、設定情報やログ等も含めてバックアップ対象とすることが望ましい。

ウ　バックアップの取得状況や復旧手順を記録すること。

エ　データの保存期間や世代管理について、要件に応じて設定できること。

(6) 運用・保守性

ア　サービスの運用・保守作業が容易であり、管理者マニュアルや操作手順書を整備・最新化すること。

イ　サービスのバージョンアップや機能追加時にも、既存データや設定が維持されること。

ウ　サービス提供終了時には、蓄積データを汎用的な形式でエクスポートできることが望ましい。

エ　問い合わせや障害発生時のサポート体制が整備されていること。

7. 前提条件

7.1. サイジングのための要件

次期ネットワーク環境のサイジングに必要な本市の端末、利用者等の情報を以下に示す。

7.1.1. 利用者情報

次期ネットワーク環境の利用者情報を以下に示す。

No	分　類	利用者数	
1	児童生徒数	約 4,500 名	
2	小中学校教職員	約 540 名	約 550 名
3	教育委員会職員	約 10 名	

7.1.2. 端末情報

次期ネットワーク環境の利用者情報を以下に示す。

教職員用タブレット端末は、令和 8 年度に本業務とは別途で調達を予定している。また、学習用端末は、令和 7 年度に Chromebook 端末への更新が完了した。

No	分　類	台　数	概　要
1	教職員用タブレット端末	約 560 台	Windows 端末
2	学習用端末	4461 台	Chromebook 端末
		666 台	Chromebook 端末予備機
		約 25 台	Windows端末（図書システム用）

7.1.3. 施設情報

丹波市地域イントラネット内の各施設の情報を以下に示す。

各施設のネットワーク環境については『2.1.1 丹波市地域イントラネット』に示す通り。なお、令和 8 年 4 月に丹波市立吉見小学校と丹波市立三輪小学校の統合を予定している。

No	拠点名	住所	備考
1	丹波市役所	氷上町成松字甲賀1	
2	山南支所（教育委員会）	山南町谷川 1110	
3	崇広小学校	柏原町柏原 683	
4	新井小学校	柏原町大新屋 698-2	
5	上久下小学校	山南町青田 156	
6	久下小学校	山南町谷川 2276	
7	小川小学校	山南町井原 427-1	
8	和田小学校	山南町和田 1	
9	南小学校	氷上町佐野 530	
10	中央小学校	氷上町成松 186-1	
11	西小学校	氷上町上新庄 524	
12	北小学校	氷上町絹山 608	
13	東小学校	氷上町石生 585	
14	青垣小学校	青垣町佐治 282-3	
15	竹山小学校	市島町中竹田 1703-1	
16	吉見小学校	市島町上田 222-1	令和 8 年 4 月に市島小学校に統合
17	三輪小学校	市島町酒梨 205	令和 8 年 4 月に市島小学校に統合
18	春日部小学校	春日町多利 1774	
19	大路小学校	春日町下三井庄 1080	
20	進修小学校	春日町国領 1011-1	
21	黒井小学校	春日町黒井 2205	
22	船城小学校	春日町朝日 90	
23	柏原中学校	柏原町南多田 1226	
24	山南中学校	山南町谷川 1348	
25	氷上中学校	氷上町成松 103	
26	青垣中学校	青垣町小倉 365-1	
27	市島中学校	市島町上垣 2002	
28	春日中学校	春日町野村 2476	

7.2. 本市保有ライセンスの活用要件

現在、本市が保有しているソフトウェアライセンス、または利用しているクラウドサービスを下表に示す。

本業務においては、これらのソフトウェアのライセンスを継続利用する提案も可とする。ただし、現行契約の満了日は下表のとおりであるため、次期ネットワークの検証及び構築期間や、本稼働開始後の保守運用期間において必要となる費用（ライセンス更新、サポート更新）はすべて本業務に含めて提案すること。

メーカー	対象ソフトウェアまたはサービス	保有数量	型名	契約期間
デジタルアーツ	i-FILTER Ver.10 アカデミック版	2,000 式	IHPA-KS02000	2026 年 4 月 ～2027 年 3 月
デジタルアーツ	i-FILTER@Cloud GIGA スクール版	（児童生徒分） 4,460 式 （教職員分） 554 式	型名不明	2025 年 7 月 ～2026 年 6 月
Sky	SKYSEA Client View (GL) Light Edition サーバーライセンス	1 式	SKYSEA000GLT13AHK1	2026 年 4 月 ～2027 年 3 月
Sky	SKYSEA Client View (GL) Light Edition クライアントライセンス	600 式	SKYSEA000GLT13GHK1	2026 年 4 月 ～2027 年 3 月
トレンドマイクロ	更新 教育委員会とりまとめ用 Trend Micro エデュケーションパック	28 式	OTOCMMJAYLIUPN3702Z	2025 年 11 月 ～2026 年 10 月
Barracuda	Barracuda Email Security Gateway アプライアンス	12 式	BSFIV300A-V	2026 年 4 月 ～2027 年 3 月

7.3. Microsoft365 ライセンスの調達要件

次期ネットワークの検証及び構築期間や、本稼働開始後の保守運用期間において必要となる Microsoft365 のライセンスは、本業務の見積金額に含めて提案すること。

なお、Microsoft365 のライセンスについて、令和9年度以降の価格が確約できない場合は、毎年 5%とすること。

7.4. クラウドサービス選定に係る要件

本業務で導入するクラウドサービスについては、ISMAP（政府情報システムのためのセキュリティ評価制度）に認定されているか、以下に示す認証制度のいずれかを取得していること。（サービス稼働開始までに認定・取得する見込みであれば問題ない。）

【認証制度】

(1) ISO/IEC 27001(情報セキュリティ全般)

(2) ISO/IEC 27017（クラウドサービスの情報セキュリティ）

(3) ISO/IEC 27018(クラウドサービスにおける個人情報の取扱い)

8. 成果物一覧

本業務における成果物は、下記のとおりとする。

本業務の委託期間中における成果物の文書管理は受注者側で確実に行い、システム構成変更等による資料の改訂時には速やかに納品すること。

なお、成果物の内容については、本市および第三者が見て理解できる内容となっているかを1つ1つ検品するものとする。

【成果物一覧(構築移行工程)】

No	成果物	成果物の内容	提出期限
1	プロジェクト計画書	プロジェクトを遂行する上での作業概要、体制、スケジュール(WBS)、会議体、進捗管理方法、体制図等	契約締結後10 日以内
2	サービス・機器一覧表	納入するサービスや機器の一覧表	
3	課題管理表	発生した課題内容と対処内容、対応期限、進捗ステータス等	進捗報告会まで
4	進捗報告書等	進捗報告書や中間報告書等	
5	議事録	プロジェクトにおける会議を開催した際の会議内容を記録した議事録	会議後 5 開庁日以内
6	システム構成図	システム全体の物理/論理構成図など	設計工程完了まで
7	基本設計書	次期ネットワーク環境に関する基本設計書	
8	詳細設計書	納入するサービスや機器のパラメータシート	
9	テスト計画書、テスト仕様書兼結果報告書	各種テストに関する実施計画(手順、環境、スケジュール等)、テストの実施結果(テスト消化件数、不具合件数、不具合対応状況)	テスト開始までテスト終了後
10	移行・切替計画書	移行・切替に関する計画(スケジュール、対象データ、データ凍結日、リハーサル回数等)	移行・切替開始まで 移行・切替終了後
11	設定指示書・手順書	関連業務を推進する事業者に対して、次期ネットワークへの移行に必要となるパラメーターや、具体的な手順等を示した指示書	
12	移行・切替結果報告書	移行・切替の結果報告(移行後の検証結果等)	
13	ネットワークアセスメント調査計画書	ネットワークアセスメントの実施体制、スケジュール、調査内容等を記載した計画書	アセスメント実施前まで
14	ネットワークアセスメント調査報告書	調査結果をもとに、現行ネットワーク全体の問題点や改善策を記載した報告書	アセスメント実施後
15	操作マニュアル(利用者向け)	納入するサービスやソフトウェアの利用者向けマニュアル	構築移行工程完了まで
16	保守運用マニュアル	システム管理者の運用や障害時の対応手順などを記したマニュアル	
17	サービスレベル計画書	納入するサービスについてのサービスレベルを規定したもの	

【成果物一覧（保守運用工程）】

No	成果物	成果物の内容	提出期限
1	保守運用業務実施計画書	保守運用業務を実施する上での概要、作業要素、体制、連絡網、スケジュール、会議体、進捗管理方法、体制図等	保守運用開始まで
2	障害対応報告書	発生した障害の内容及び影響範囲、障害への対応結果等	障害対応時
3	作業実施計画書	脆弱性対応や年次更新など、事前計画を伴う作業のタイムスケジュール、連絡体制、業務影響、作業手順等を記載した計画書	作業実施の約2週間前まで
4	作業実施報告書	前月分の障害対応や問合せ対応の状況、定期点検等の作業内容及び作業結果、課題とその解決策、SLA状況の報告、進捗報告等	月次報告時
5	問合せ管理台帳、FAQ	教職員からの問合せ内容、その回答内容。よくある質問とその回答。	
6	ライセンス数報告書	各種サービスやソフトウェアについての月末時点でのライセンス総数、利用数、余剰数をまとめたもの	
7	課題管理表	発生した課題内容と対処内容、対応期限、進捗ステータス	
8	議事録	プロジェクトにおける会議を開催した際の会議内容議事録	会議後5開庁日以内
9	年次報告書、中間報告書	月次報告書の総括、現状分析結果報告、年度中間時点での作業報告の総括	年次報告時 中間報告時
10	年間業務計画書	翌年度分の運用業務の作業内容、実施時期等	
11	各種マニュアル（運用業務、トラブル対応等）	運用設計に基づく保守運用業務、トラブル対応に必要なマニュアル・手順類の不備・不足の更新分	
12	業務完了報告書	業務完了として実施した業務全体の総括	業務完了時
13	引継ドキュメント	次期の事業者への業務引継ぎ文書	
14	移行データ	次期の事業者への移行データ引継ぎ	

これらの成果物は、本業務満了まで活用するため、システム構成や運用、保守の手順変更等で修正した場合は、速やかに改訂版を納品すること。

特に、「操作マニュアル」やシステム運用管理手順を記述した「運用マニュアル」、および「システム障害対応手順書」（システム復旧手順を含む）や保守サービスの説明を記載した「保守マニュアル」は、常に最新の状態となるように確実に修正を行うこと。

なお、これらのマニュアルや運用手順書については、コンピュータの操作に長けていない教職員にもわかりやすい内容で作成すること。

9. 検査

受注者から本業務に係る完了報告を受領した場合に、本業務が完了したかどうか検査を実施する。検査が合格したあと、受注者は本市に対して請求を行うこと。検査が不合格である場合、本市から受注者に対して連絡を

行うため、速やかに対処すること。なお、業務の完了が 3 月末となる場合、1 月下旬に中間検査を行う場合がある。

10. 再委託

（ア） 受託者は、本業務の全部もしくは一部を第三者に委託又は請け負わせてはならない。ただし、予め書面により本市と協議し承認を得た場合はこの限りではない。

（イ） 上記により本市が承認した場合には、承認を得た第三者も受託者としての義務を負うものとし、受託者は当該第三者にこの義務を遵守させるために必要な措置を執らなければならない。
なお、その後に承認を得た第三者についても同様とする。

（ウ） 上記により本市が承認した場合でも、受託者は本市に対し、承認を得た第三者の行為について全責任を負うものとする。

11. 契約不適合責任

検査完了後に本システムの品質又は数量等に関して、契約の内容に適合しないもの（以下「契約不適合」という。）が認められた場合、別途契約書に定める期間や内容に準じて是正措置を行うこと。

12. 知的財産権等

（ア） 本業務の成果物の所有権、著作権等の権利は、本市に帰属するものとする。ただし、受託者はあらかじめ本市及び構築業者の承諾を得た場合には、業務の成果物を基に翻案して、二次的著作物を作成し、譲渡、貸与等をすることができる。

（イ） 本業務の成果物に、受託者が従前から保有する知的財産権（著作権、ノウハウ、アイデア、技術、情報等を含む。）が含まれていた場合は、権利は受託者に留保されるが、本市は、業務の成果物を利用するために必要な範囲において、これを利用できるものとする。

（ウ） 受託者は、本市に対し、著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

（エ） 本業務の成果物に、受託者以外の第三者が保有する知的財産権が含まれる場合は、上記の定めによらないものとするが、本市が、業務の成果物を利用するために必要な範囲において、これを利用できるよう本受託者の責任において必要な処置を講じること。

13. 秘密保護

受託者は、個人情報保護条例及び丹波市教育委員会情報セキュリティ対策基準を遵守すること。

（ア） いかなる場合においても、本市から秘密とされた事項及び本件に関して知り得た業務に関わる事項並びに付随する事項を第三者に漏らしてはならない。

（イ） 本規定は、本件終了後にも有効に存続する。

（ウ） 遵守状況を確認するため、必要に応じて物理的セキュリティ、組織的・人的セキュリティ、情報システムセキュリティについて監査を実施する。

14. その他

（ア）導入にあたり疑義が生じた場合、又は仕様書や提案書で定められていない事項等が発生した場合は本市と協議を行い、指示を受けること。

（イ）本業務の実施状況について、他団体に情報提供を行う場合は、事前に本市に対して連絡を行い、許可を得ること。