県立学校等情報ネットワークシステム推進事業
仕様書

令和６年４月

目次

1. 業務名

県立学校等情報ネットワーク推進事業

2. 事業概要

1.1　背景と目的

福井県教育庁（以下、「県教育庁」という。）が管轄する県立高校約40校のICT 環境は、主に教職員が校務で利用する「校務系ネットワーク」と、教員・生徒が授業等で利用する「学習系ネットワーク」およびGIGAスクール構想で整備した「タブレット系ネットワーク」が存在している。

このうち、校務系ネットワークについては令和６年度に基盤機器の更新期限を迎える予定であるが、次の更新にあたっては、「教員の業務効率化」と「セキュリティ対策」の両立および「教員の働き方改革」を目的に、クラウド時代に合ったセキュリティを実現するため校務系システムおよびネットワーク環境の全面ゼロトラスト化を計画している。

また、別事業となるが同時期に、持ち運び可能な「校務端末」の整備や、各校内に設置する「校内ネットワーク機器」の集約を予定しており、既存資産を十分活用したうえでICT環境全体を最適化することが求められる。

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、全県立校において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、新たな校務系ICT 環境の構築移行、および移行後の「教育ネットワーク」全体の総合運用管理業務を委託するものである。

1.2　用語の定義

本事業における用語の定義を、以下に示す。

用語	定義
校務系ネットワーク	成績処理などの校務にあたり、教職員が校務端末を利用するためのネットワーク。職員室や準備室等に設置される校務端末が接続し、個人情報など機密性の高い情報をと扱うネットワーク。
学習系ネットワーク	タブレット系ネットワークができる前に教材配信や課題提出などで、教員および生徒が利用するためのコンピュータ教室やCIA教室が接続されているネットワーク。一部の学校では研究用の校内サーバー等も運用されている。
タブレット系ネットワーク	文部科学省「GIGAスクール構想の実現」で構築された全

	県立学校の高速大容量の学習系校内ネットワーク。普通教室、特別教室からタブレット等を用いた学習系授業の際に無線アクセスポイントを経由して接続されるネットワーク。(タブレット系ネットワークは学校からのローカルブレークアウトにより、直接インターネットへ接続している。)
ゼロトラスト化	社内外のネットワークやデバイスのすべてに脅威が潜んでいることを前提にしたセキュリティの考え方。ゼロトラストセキュリティは、企業の情報・システム・ネットワークなどにアクセスするものを単体では信用せず、すべてのデバイスや通信を利用の都度「許可制」にすることでセキュリティを強化する仕組みを実現する。
ICT 環境	県立学校でICT を活用した校務や授業を行うために必要なシステム、基盤、回線、校内ネットワーク機器、端末、総合運用管理などの全般。
校内ネットワーク機器	県立学校の端末と回線を接続するルータ、スイッチ、無線アクセスポイントなどの機器。県立学校の各校内に設置している。
ローカルブレークアウト	クラウドやインターネット向け通信をデータセンター経由とせず、各校、各拠点から直接アクセスする機能。データセンター経由と比較しアクセス集中によるボトルネックの影響を受けにくい。
教育ネットワーク	校務系、学習系、タブレット系を統合した移行後のネットワークのこと。

1.3　調達構築範囲

調達・構築範囲は、構築移行業務と運用管理業務に分かれる。

【構築移行業務】

プロジェクト管理、基本設計・詳細設計・構築、検証・試験、移行・切替、研修の各業務が対象となる。スケジュールの詳細は『1.5スケジュール』を確認すること。

【総合運用管理業務】

構築移行業務にて構築した教育ネットワークのICT環境において、統括運用管理（運用統制・連絡調整）、県立高校サポートセンター（NOC）、セキュリティオペレーションセ

ンター（SOC）の各業務が対象となる。学習系ネットワークの一部の運用管理を担っている事業者と連携・協力して実施すること。

1.4　サービス提供期間

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から令和７年3月31日まで 総合運用管理業務令和７年4月1日から令和12年3月31日まで(60か月)

（地方自治法第234条の3の規定に基づく長期継続契約）

1.5　スケジュール

事業スケジュールは次のとおりを予定しているが、提案事業者の提案内容により両者協議のうえ変更できるものとする。

（1）設計・構築期間

契約締結日から令和７年３月 31 日まで

（2）移行・プレリリース

令和６年１０月１日から令和７年３月３１日まで

（3）総合運用管理業務（福井県教育クラウドサービス提供期間）

令和７年４月１日から令和 12 年３月 31 日まで

設計・構築期間	契約締結日 ～ 令和６年９月３０日
移行期間	令和６年 １０月 １日 ～令和７年 ３月３１日
プレリリース期間	令和６年 １０月 １日 ～令和７年 ３月３１日
総合運用開始日（本稼働）	令和７年 ４月１日
運用保守期間	令和７年 ４月 １日 ～令和 12 年 ３月 31 日

プロポーザルおよび契約のマイルストーンは以下のとおり。プレリリースした機能については、構築移行期間中であっても、極力本稼働時と同等の不具合対応を行うこと。

事業スケジュール（予定）

	令和６年４月	令和６年５月	令和６年６月
事業公告	▲公告 ▲入札参加申請		
入札		▲企画提案提出	▲プロポーザル
事業者決定 契約			▲事業者決定 ▲契約

1.6　「業務効率化」「セキュリティ対策」「働き方改革」の基本的な考え方

県立学校における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みであり、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、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、現行環境では、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、場所や時間の制約等をできる限り受けずにICT を活用できるような環境を実現するため、校長や教諭など「教員の業務効率化」と「セキュリティ対策」「教員の働き方改革」を県教育環境で実現するための基本的な考え方を、以下のとおり定める。

(1) 外部クラウドサービスの利用

教員が校務で利用するサービス・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、使いやすいものを安定的に提供することに加え、将来の拡張性にも柔軟に対応できるよう、県独自で機器やシステムを保有せず、外部のクラウドサービスを利用する。

(2) ICT 環境の集約化・既存ストックの活用

移行後の教育ネットワークについて、できる限り現在の学校環境の物理的なネットワーク資産（ルーター、AP、スイッチなど）や流用可能な端末、およびソフトウェア資産などの既存ストック（従来事業導入リソース）を有効活用しつつ、事業全体のコストダウンおよび使いやすいものを提供する。

(3) どこでも安全に校務ができるICT 環境の整備

教員が持ち運びできる端末を活用して、各県立学校の職員室内のみならず、職員室外、出張先や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、校外で教材を作成したり、教員が端末を持ち帰って自宅から校務用のシステムにアクセスしたりするような使い方が想定される。

この場合、アクセス制御の徹底による端末１台での運用や、県教育庁のセキュリティポリシーに基づく端末の持ち出しを可能とするため、リスクベース認証、ふるまい検知、マルウェア対策、暗号化、SSO などの「アクセス制御による対策」を講じたICT環境を構築する。

(4) 業務効率化とセキュリティの両面を支える総合運用管理

十分なセキュリティ対策のもと整備されたクラウドサービスを教員が存分に活用するとともに、複雑な操作や運用手続きから解放され、校務と教育に真に必要な業務に時間を割くことができるような総合運用管理体制を構築する。

具体的には、学校で独自のルールを決めて外部記憶装置を運用していたり、機微ではないデータを格納するサーバーを運用するなどの差異のある運用の統一化や、教員の実情に応じたサポート体制の確立、サイバー攻撃の検出や対応などを行い、これら業務全体を定期的に改善する。

1.7 その他のセキュリティの基本的な考え方

(1) 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6年1月版)」に準拠したシステムおよびサービスを提供すること。

(2) 設定するパブリッククラウドサービス(SaaS)は、日本国内に設置されていること。

(3) 選定するクラウドサービス(SaaS)は、第三者機関による認証(ISO/IEC27001,27017/ISMAP)を取得済みのものであること。

(4) 受託者は情報セキュリティを確保できる体制を整備し、情報漏えい等のセキュリティ被害への対策が十分に講じられた作業環境において、本調達に係る作業を実施すること。

(5) 受託者の責に起因する情報セキュリティインシデントが発生するなど、万一の事故があった場合は、速やかに県教育庁に報告し、損害に対する賠償等の責任を負うこと。

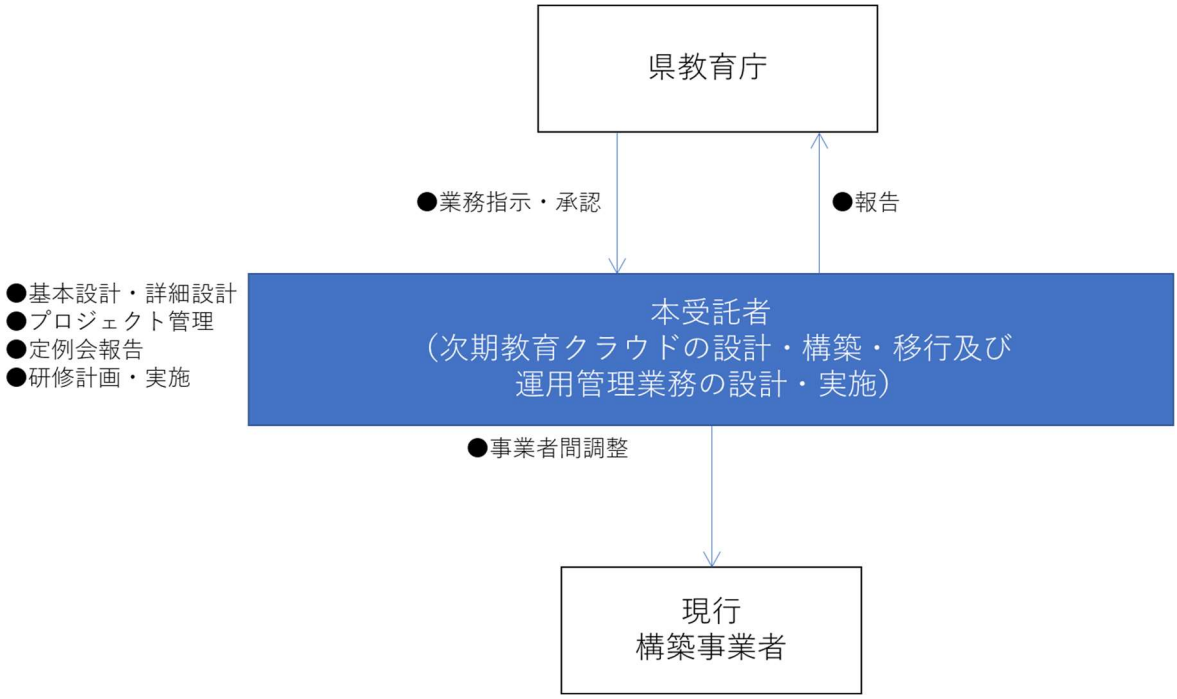
(6) 受託者は、事業の遂行を通じて知り得た情報を漏らしてはならない。またその職を退いた後も同様とする。

3. 業務委託内容

2.1　事業者間役割分担

本業務における事業者間役割分担の基本方針を以下に示す。

【構築移行工程における事業者間役割分担】



・県教育庁は、本業務の受託者に対して、本業務に係る業務指示を行い、求めに応じて実施業務や成果物等に関する承認を行い、成果・結果等に関する報告を受ける。

2.2　プロジェクト管理業務

(1)　プロジェクト立ち上げ時に以下の書類を県教育庁と協議のうえ作成、提出すること。また、これらの書類の記載事項を変更する場合、県教育庁と協議の後、変更後の書類および変更点を記した文書を提出すること。

(ア) 業務工程表
(イ) 構築体制図/連絡図
(ウ) 業務実施責任者/従事者名簿
(エ) 資格要件を満たすことを証する書類

(2)　システムの開発を行う場合、以下の事項を含むプロジェクト方針書を県教育庁と協議のうえ作成、提出すること。協議に際し、県教育庁と受託者双方で決定事項、検討事項、リスク要因を明確にし、現時点で不明点がないようにすること。プロジェクト方針書について概ねの合意ができた時点で基本設計に着手すること。以下を提出書類とすること。

(ア)前提条件と制約条件

(イ)仕様等を決定・変更する場合の合意の手順、報告の頻度

(ウ)県教育庁と受託者の役割と責任分担

(エ)仕様管理計画

(オ)進捗管理計画

(カ)課題管理計画

2.3　設計・構築業務

(1)　基本設計

受託者は、本仕様書の記載内容および要件定義を踏まえた上で、システム構築に係る基本方針を定めた基本設計書を作成し、別途定める期限までに県教育庁に提出すること。

基本設計書には、最低限、次の内容を盛り込むこととし、具体的な記載内容については事前レビューを実施し、教育庁と協議の上決定すること。

(ア)全体システム構成

(イ)物理設計（機器・ソフトウェア一覧、ホスト名/命名規則一覧、接続設計等）

(ウ)論理設計（ネットワーク設計、アプリケーション設計、セキュリティ設計等）

なお、設計にあたっては既存のネットワーク状況を十分に把握した上で実施し、また構築後の運用管理について、特に考慮したものとすること。

またクライアント側での処理を過大なものとせず、基本的にはクラウド側で処理を行うことを原則とする。

(2)　詳細設計

受託者は、本仕様書の記載内容、要件定義および基本設計を踏まえた上で、各システムや設定値を定めた詳細設計書を作成し、別途定める期限までに県に提出すること。

具体的な記載内容については、事前にレビューを実施し、県教育庁と協議の上決定すること。

2.4　プレリリース業務

構築期間内に本事業で構築したサービスを特定の学校を選定して、導入サービスの確認を行うこと。

2.5　検証・テスト業務

新たに導入する全ての機能等のテストを行うこと。
そのうえで、端末、校内ネットワーク機器や回線を含めた新たな教育ネットワークの ICT 環境の全体的な総合テスト（結合試験）を、構築の関連事業者やパソコン教室の整備事業者、ネットワークの管理事業者などの各関連事業者と連携のうえ実施すること。

さらに、新たな校務系 ICT 環境の総合的な機能検証および全体の運用検証を目的とした、県教育庁・各学校ユーザーおよび本受託者の操作による運用テスト（受入試験）を実施すること。

各テストの実施にあたっては、計画策定、テスト仕様策定、テスト実施、テスト結果の報告作成を行うこと。

また、テストにあたっては、必要に応じて複数の学校に訪問し、学校からの新たな校務系 ICT 環境への接続および利用確認のための実地検証を実施すること。

2.6　移行・切替業務

（1） ネットワーク移行

「6.1. ネットワーク移行計画」に基づき、プレリリース、本稼働それぞれで「移行・切替計画書」を作成し、県教育庁の承認のうえ移行および切替を実施すること。

実施にあたり、移行および切替に関する事前検証、テスト、リハーサルなどにより、確実な移行および切替を行うために必要な対策を採用するとともに、学校現場の授業や学習環境、教職員の校務にできる限り影響を及ぼさないよう配慮すること。

（2） データ移行

「6.1. ネットワーク移行計画」に基づき、現行の校務系ネットワークに保存されているデータを移行すること。

2.7　研修業務

（1） 研修を行う場合、以下の事項を含む研修計画書を県教育庁と協議のうえ作成、提出すること。

（ア） スケジュール

（イ） 県教育庁と受託者との役割分担、体制

（ウ） 対象者（一般利用者、システム管理者等）

（エ） 研修内容

・導入時研修（システム管理者向け）

端末利用研修　基本編(Microsoft365 基本機能)

・導入時研修（一般教職員向け）

端末利用研修　基本編(Microsoft365 基本機能)

・年次研修（校務系環境における新機能説明など）

端末利用研修　基本編(Microsoft365 基本機能)

（オ） 研修で使用する環境やデータの準備

（カ） 研修用マニュアル（操作マニュアル等）の作成

2.8　周辺環境の調達支援・設計・設定指示業務

（1） 本業務における既存機器への影響範囲の調査および移行による既存業者への設定変更を指示する旨を記載すること。また、設定変更に伴う費用については、本事業に含めること。

＜記載例＞

項番	既存機器	想定される設定変更内容	変更作業実施者	想定時期
1	校内ネットワーク機器（基幹スイッチ）	教育ネットワークへの接続に伴う設定変更	現行運用保守事業者	令和〇年〇月

（2） 構築期間中に新規調達となるシステム・機器がある場合は必要に応じて各事業者に設定を指示する旨を記載すること。

＜記載例＞

項番	機器	実施内容	想定時期
1	教育ネットワークに接続する端末 〇〇〇台	・調達支援 ・設定指示書の提示	令和〇年〇月

2.9　総合運用管理業務

（1） 運用設計

「7.統合運用管理設計」に基づき、構築した教育ネットワークにおけるシステム、基盤、ネットワーク、校内ネットワーク機器、端末、セキュリティサービスの運用設計を行うこと。

設計にあたっては、県教育庁および『2.1.事業者間役割分担』に記載する現行事業者と連携・協力して実施すること。

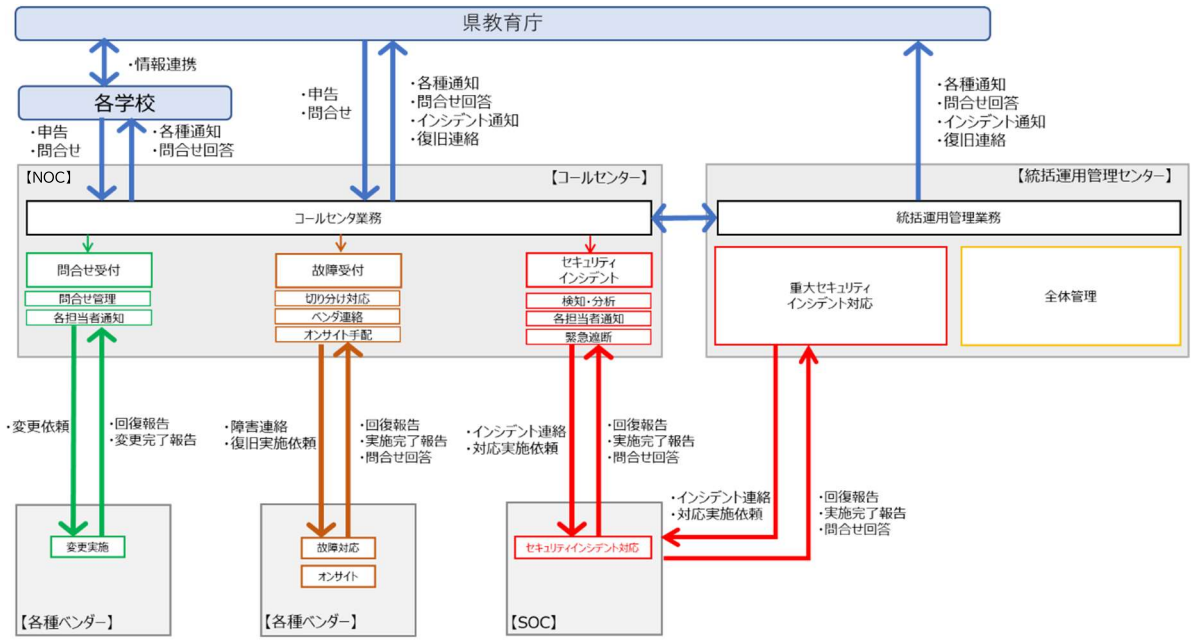
（2） 総合運用設計

「7.総合運用管理設計」および「8.障害検知時の復旧対応」に基づき、県立学校の ICT 環境における業務の分析、企画、業務改善、機能追加、設定変更、障害対応等の総合的な管理を行うこと。

主な業務内容は、統括運用管理（運用統制・連絡調整）、県立高校サポートセンター（NOC）、セキュリティオペレーションセンター（SOC）である。

業務にあたっては、県および『2.1.事業者間役割分担』に記載する関連事業者と密接に連携、協調して実施すること。

【総合運用管理業務における基本体制】



2.10　SLA要件

（1） 県教育庁と協議の上、サービスレベルを作成すること。
（2） サービスレベルは運用保守・監視実施計画書にて定義すること。
（3） SLA の更新は、県教育庁と協議の上、承諾した場合に実施する。
現在、想定している継続性は以下のとおりである。

対象	内容
RTO（目標復旧時間） 平常業務停止時	業務停止を伴う障害が発生した際には、県教育庁と協議した時間以内でのネットワーク復旧を目標とすること。
稼働率	稼働率は 99.9%を目標とすること。
大規模災害時	大規模災害時はこの限りではない。県教育庁と協議の上、可能な限り速やかに対応すること。

上記サービスレベルの基準値を達成できなかった場合、速やかに達成できなかった原因分析と改善に向けた対応、対策について受託者の負担において実施すること。サービスレベルの基準値の達成状況によらず、サービスの停止時においては、各種クラウドサービス（SaaS、IaaS とも）を提供する事業者が定める条項に基づき、受託者が減額される相当額について、対象月の支払金額を減額する。

また、Microsoft365 等のクラウドサービス部分に対する SLA は各提供事業者の基準に従うものとし、上記 SLA 要件の対象外とする。

2.11　業務完了時のデータ消去要件

本業務委託契約期間終了後、本業務で構築した構成・環境について、県教育庁の指示に従い撤去、データの消去を行うこと。

本撤去およびデータの消去に当たってはクラウド上のリソースの消去など適切な処理を実施した上で、実施結果を書面にて県教育庁に報告すること。なお、これらに係る費用は受託者の負担とする。

2.12　　次期事業者へのデータ引継ぎ要件

本業務の委託契約期間終了に伴う更新にあたり、データの移行は、本受託者が主体的に実施する。本業務の受託者は県教育庁または次期事業者からの依頼に基づき、移行対象データの抽出を行うこと。

抽出データは原則編集を行わず、本受託者がコンバート等を行うものとする。

2.13　体制要件

(1) 本受託者は、スケジュールを遵守し、本システムの品質が守れるよう十分な体制を整えること。
(2) 本受託者は、本業務に取り組む体制を明らかにし、契約締結後 7 日以内に県教育庁および各契約学校設置者等に報告すること。

2.14　プロジェクト管理

(1) プロジェクト管理
(ア) 本システムの導入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。
(イ) 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。
(ウ) 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。
(エ) プロジェクト計画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。
(オ) プロジェクト管理にあたってはPMP（Project Management Professional）もしくはプロジェクトマネージャー試験（PM）資格取得者を体制に含めること。

（2）マイクロソフト社サポート契約の活用

本事業における各種設計構築においては、マイクロソフト社の各種プロダクトを利用している。契約期間中は、県教育庁でマイクロソフト社ユニファイドサポートを契約し、構築や運用の際に、問合せ等の支援が受けられるよう体制を整える。受託者は本サポート契約を活用し遅延なく事業を進めること。

2.15　納品物

本業務の工程毎の納品物を以下に示す。いずれの納品物も県教育庁が様式およびファイル形式指定した場合は、当該様式およびファイル形式で提出すること。

また、機能改修や設定変更が生じた場合、構築工程の納品物に準じて必要な書類を作成および更新し、県教育庁が定める期限（特に定めのない場合は毎年度末）までに納品すること。

なお、会議体等で使用したドキュメントなど、下記の納品一覧に記載のないドキュメントについても、県教育庁の求めに応じて参考資料として提出すること。

【納品物一覧】（システム構築関連）

納品物	数量	内容	提出時期
1.　本システムを構成するシステム	1 式	本仕様書の機能要件を満たすもの	納入期限まで
2.　構築体制に係る図書	1 部	・業務工程表 ・構築体制図/連絡図 ・業務実施責任者/従事者名簿 ・資格要件を満たすことを証する書類	契約締結後速やかに 契約締結後２週間以内
3.　プロジェクト計画書	1 部	・プロジェクト計画書	
4.　開発管理に係る図書	1 部	・課題管理表 ・議事録/打ち合わせ資料	随時
5.　設計に係る図書	1 部	・基本設計書 ・詳細設計書 ・移行計画書	随時
6.　マニュアル関係	1 部	・操作マニュアル（利用者用） ・運用マニュアル（管理者用） ・研修テキスト	
7.　完成図書	1 部	・全体システム構成図 ・試験成績書 ・作業施工図面/配線系統図	納入期限まで

【納品物一覧】（システム運用関連）

納品物	数量	内容	提出時期
1. 運用体制に係る文書	1 部	・運用体制図/連絡図/緊急時対応計画 ・資格要件を満たすことを証する書類	随時
2. マニュアル関係	1 部	・運用マニュアル	
3. 月次運用報告書	1 部	・運用状況報告書 ※構成管理、性能管理、障害管理、サービスレベル測定結果を含む	月初
4. セキュリティ検知状況報告【月次】	1 部	・セキュリティ検知の有無およびアリの場合はその内容と対応 ※場合によっては次回の対応方針の報告を含む	月初
5. 緊急セキュリティ報告【随時】	1 部	・緊急セキュリティの内容と対応の報告	随時

3. 前提条件

3.1 サイジングのための要件

移行後の教育ネットワークにおけるICT 環境のサイジングに必要な要件を以下に示す。

【本業務の学校数利用者数について】

分類	区分	学校数	生徒数	教員数（本務者＋兼務者）
県立学校	高等学校（分校含む）	30 校	18,000 人	1,800 人
	特別支援学校	13 校	1,000 人	1,000 人
	その他教育機関	4 拠点	－	250 人
	小計	47 拠点	19,000 人	3,050 人
校務支援参加校	中学校	74 校	22,000 人	2,200 人
	小学校	191 校	43,000 人	3,500 人
	小計	265 校	65,000 人	5,700 人
県立学校＋校務支援参加校 合計		312 拠点	84,000 人	8,750 人

【県立学校一覧】

	学校名	電話番号	住所
1	藤島高等学校	0776-24-5171	福井市文京２丁目８－３０
2	高志高等学校・高志中学校	0776-24-5175	福井市御幸２丁目２５－８
3	羽水高等学校	0776-36-1678	福井市羽水１丁目３０２
4	足羽高等学校	0776-38-2225	福井市杉谷町４４
5	三国高等学校	0776-81-3255	坂井市三国町緑ケ丘２丁目１－３
6	金津高等学校	0776-73-1255	あわら市市姫４丁目５－１
7	丸岡高等学校	0776-66-0160	坂井市丸岡町篠岡２３－１１－１
8	丸岡高等学校 定時制	0776-66-0324	坂井市丸岡町内田１３－６
9	大野高等学校（全日、定時）	0779-66-3411	大野市新庄１０－２８
10	勝山高等学校	0779-88-0200	勝山市昭和町２丁目３－１
11	鯖江高等学校（全日、定時）	0778-51-0001	鯖江市舟津町２－５－４２
12	鯖江高等学校丹南キャンパス	0778-62-2112	鯖江市熊田町 10－7
13	丹生高等学校	0778-34-0027	丹生郡越前町内郡４１－１８－１
14	武生高等学校（全日、定時）	0778-22-0690	越前市八幡１丁目２５－１５
15	武生東高等学校	0778-22-2253	越前市北町８９－１０
16	敦賀高等学校（全日、定時）	0770-25-1521	敦賀市松葉町２－１
17	美方高等学校	0770-45-0793	三方上中郡若狭町気山 114－1－1
18	若狭高等学校（全日、定時）	0770-52-0007	小浜市千種１丁目６－１３
19	若狭高等学校 海洋キャンパス	0770-52-1950	小浜市堀屋敷２－５－２
20	若狭東高等学校	0770-56-0400	小浜市金屋４８－２
21	福井農林高等学校	0776-54-5187	福井市新保町４９－１
22	坂井高等学校	0776-66-0268	坂井市坂井町宮領５７－５
23	科学技術高等学校	0776-36-1856	福井市下江守町２８
24	奥越明成高等学校	0779-66-4610	大野市友江９－１０
25	敦賀工業高等学校	0770-25-1533	敦賀市山泉１３－１
26	福井商業高等学校	0776-24-5180	福井市乾徳４丁目８－１９
27	武生商工高等学校 商業キャンパス	0778-22-2630	越前市家久町２４
28	武生商工高等学校 工業キャンパス	0778-22-2730	越前市文京１丁目 14－16
29	道守高等学校	0776-36-1184	福井市若杉町３５－２１
30	盲学校	0776-54-5280	福井市原目町３９－８
31	ろう学校	0776-24-5190	福井市幾久町２－２２

32	福井特別支援学校	0776-24-5194	福井市光陽３丁目２－３３
33	福井南特別支援学校	0776-36-7631	福井市南居町８２
34	福井東特別支援学校	0776-53-6575	福井市四ッ井２丁目８－１
35	福井東特別支援学校 月見分教室	0776-35-7626	福井市月見２－４－１
36	福井東特別支援学校 五領分教室	0776-61-8518	吉田郡永平寺町松岡下合月２３－３
37	奥越特別支援学校	0779-88-0050	勝山市昭和町３丁目１－６９
38	嶺北特別支援学校	0776-67-0100	坂井市丸岡町熊堂３－３６
39	清水特別支援学校	0776-98-3650	福井市島寺町６８－３３－３
40	南越特別支援学校	0778-27-6600	越前市上大坪町３５－１－１
41	嶺南東特別支援学校	0770-45-1255	三方郡美浜町気山１０６
42	嶺南西特別支援学校	0770-52-7716	小浜市羽賀６７－４９－１
43	県教育庁	0776-20-0564	福井市大手３丁目１７－１
44	嶺南教育事務所	0770-56-1309	小浜市遠敷２丁目２０５
45	教育総合研究所	0776-58-2150	坂井市春江町江留上緑８－１
46	特別支援教育センター	0776-53-6574	福井市四ッ井２丁目８－１

ただし令和７年４月１日以降、武生商工高校（商業キャンパス）は武生商工高校（工業キャンパス）と統合する予定で、その場合は４５拠点となる。

3.2　環境に関する要件

本業務にて運用保守を行う対象となるSaaS型環境として提供される機能については、当該機能の受託者の責任においてバージョンアップや修正プログラムの適用等について適切な対策を講じることとして、検証環境に関する要件については特に言及しない。

現時点で想定する対象機能およびサービスは以下のとおり。

（１）Microsoft A5ライセンスの調達　数量3050ライセンス（５年）
　※本ライセンスにて校務端末へのMicrosoft 365 Apps(Office 365）の提供を行う
（２）各県立高校の学校ホームページの構築移行および運用保守
（３）教職員用メールおよび学校代表メール・グループメールサービスの提供
（４）メール上長承認機能サービスの提供
（５）脱PPAP対応の導入
（６）Intune等デバイス管理機能
（７）Azure Information Protection等セキュリティ分類やラベル付けできる機能の提供
（８）セキュアWEBゲートウェイのライセンス（校務用＋学習用）
（９）教員用端末の端末セキュリティ対策(Endpoint Protection Platform)
（１０）学習用端末（各校コンピュータ教室・CAI教室用）セキュリティ対策の提供
（１１）学習用端末（各校コンピュータ教室・CAI教室用）のWEBフィルタリング機能の

提供
（１２）学校校務系および学習系インターネット回線
（１２）校務用端末のエンドポイントのセキュリティ監視を行い管理するサービスの提供
（１３）サーバー用ウイルス管理
（１４）DNS サービス
（１５）時刻同期サービス
（１６）統合監視・ログ管理サービス

3.3　別事業で導入される校務端末に関する要件

※　本事業では別事業で導入される校務端末の初年度のキッティング（Autopilot）設定を最大で 3050 アカウント分含んでおり端末の仕様は以下を想定している。

(1)　Microsoft 365 Apps(Office 365）がプリインストールされている。
(2)　出荷状態のWindows11/10 に対するアカウントの紐づけなどの各種初期設定をクラウドの機能を使って実施ができる。
(3)　UEFI の設定（例えば組み込みデバイスの無効化）をクラウドの機能を使って実施できる。

3.4　ネットワーク帯域にかかる要件

3.4.1　WAN回線に係る要件

本業務では、「校務系ネットワーク回線（インターネット回線）」を提供してクラウドサービスに接続が行うこと。ただし、移行後の教育ネットワークや各県立学校のネットワーク環境、システムの配置場所や通信特性を加味したうえ設計を行うこと。

現行校務系ネットワーク仕様については、「4.1　現行ネットワーク環境」を参照のこと

3.5　セキュリティに関する要件

セキュリティ対策については、「福井県情報セキュリティポリシー基本方針」や、県教育庁が定める「福井県情報セキュリティ対策基準」、および文部科学省が作成する「教育情報セキュリティポリシーに関するガイドライン」を踏まえるとともに、セキュリティ侵害が一切発生しないよう、設計、構築すること。

セキュリティ対策施策適用状況の定期的な見直しおよびセキュリティホールなどへの対処を行い、改善計画書の作成および報告を行う事。

教育ネットワークICT 環境において導入するSaaS 型クラウドサービスおよびIaaS 型ク

ラウドサービスについては、一般的なSaaSサービスの情報セキュリティ対策として、『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）第1編　第3章　教育現場におけるクラウドの活用について』に含まれる下記要件を満たすこと。

(1) 利用者認証

利用者がクラウドサービスにログインする時の認証機能を提供すること。

その際に必要に応じて多要素の認証を行う事。

(2) アクセス制御

アクセスする権限のない者がクラウドサービスにアクセスできないように、クラウド上の情報資産毎に制限できること。

(3) クラウドに保管するデータの暗号化

クラウドサービスへのデータの保管に際し、情報漏えい等に備えて、暗号化等の保護措置を講じること。

(4) クラウドサービスを提供する情報システムに対する外部からの悪意のある脅威の侵入を想定した技術的セキュリティ対策

(ア) クラウドサービスを監視し、セキュリティ侵害を検知すること。

(イ) クラウドサービスのインターネット接続境界において、クラウド利用者以外による不正な通信・侵入を防ぐ措置を講じること。

(5) クラウドサービスを提供する情報システムの物理的セキュリティ対策

（ア） クラウドサービスのサーバー等ハードウェアについて、情報システムの安定的な運用のために適切に管理すること。

（イ） クラウド事業者側の管理区域（サーバー等を設置）について、情報資産の分類に応じて管理し、入室できる者は許可された者のみに制限すること。

(6) 校務支援システムのクラウドサービスを提供する情報システムの運用管理

(ア) 校務支援システムのデータバックアップについて、必要に応じて定期的に実施すること。

(イ) クラウドサービスにおける情報セキュリティの確保や監査に必要なログを取得し、１年間以上保存すること。

(7) クラウドサービスを提供する情報システムのマルウェア対策

(ウ) クラウドサービスを構成するサーバーおよび運用管理端末等について、マルウェア対策を講じること。

(エ) クラウドサービス内に侵入した攻撃を検知して対処するために、通信をチェックする等の対策を講じること。

(8) クラウド事業者従業員の人的セキュリティ対策

クラウドサービスに関わるクラウド事業者従業員は、クラウド事業者の情報セキュリティポリシーおよび保守運用管理規程等を遵守すること。

（9） データの廃棄等について

サービス利用終了時等において、クラウド利用者のデータが不用意に残置されないよう、適切に破棄すること。

（10） クラウドサービスの将来の方向性について

本事業の導入当初をプライベートクラウドで提案した場合は、5年のサービス期間内にパブリッククラウドへリフトする（AzureやAWS、GCP等)提案し、構築移行を行うこと。

（11） クラウドサービスのセキュリティ認証等について

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、又は以下に示す認証制度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。）
また、その認証に基づいて、「教育情報セキュリティポリシーに関するガイドライン1.9.3 パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」の内容を含む情報セキュリティポリシーおよび保守運用管理規程等を規定していること。

<認証制度の例>

ア　ISO/IEC 27002(情報セキュリティマネジメントシステム)
イ　ISO/IEC 27014(情報セキュリティガバナンス)
ウ　ISO/IEC 27017(クラウドサービスの情報セキュリティ)
エ　ISO/IEC 27018（クラウドサービスにおける個人情報の取扱い）
上記アからエに示す規格と同等のもの

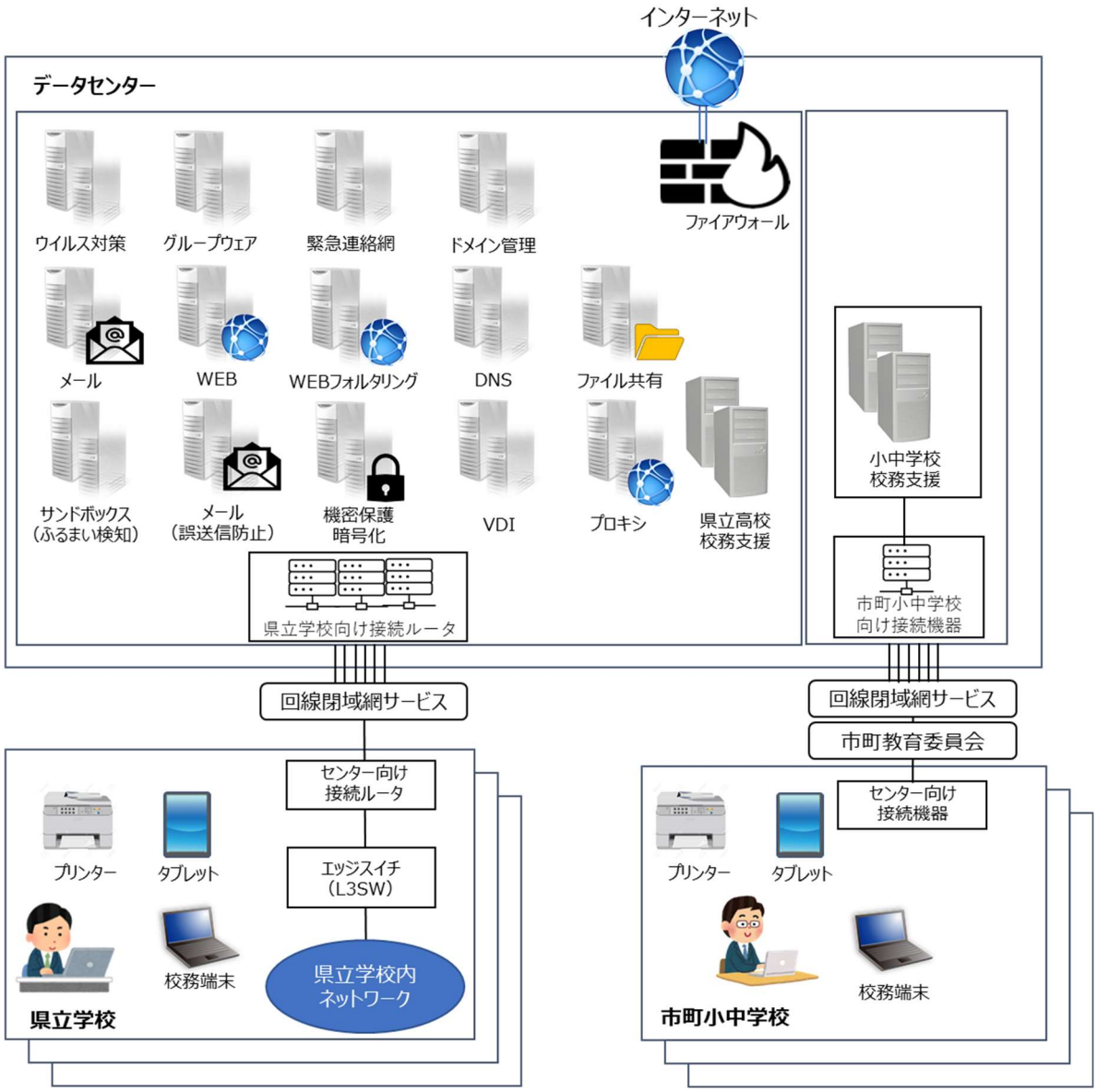
校務系ICT 環境において導入するクラウドサービスが複数ある場合、受託者はそれぞれのクラウドサービスおよび事業者が上記要件を満たしていることを、担保すること。

4.　全体基本設計

4.1　現行ネットワーク環境

4.1.1　現行教育クラウド ネットワーク環境

現行の福井県教育クラウドサービスのネットワーク全体構成図を以下に示す。



現行の福井県教育クラウドは、データセンターに設置するシステムおよび県立学校とデータセンターを結ぶ閉域網回線、校内のネットワーク機器等で構成されている。

本全体構成図上で示されている、ネットワークおよび代表的なシステムの概要を以下に示す。

分類	概要
データセンター	校務系ネットワークに係るサーバー、ネットワーク機器で構成しクラウドサービスを提供している
データセンター 設置機器	校務系ネットワークに係るサーバー、ネットワーク機器で構成しクラウドサービスを提供している。Active Directory によるユーザー認証基盤や、インターネットメール、県立学校向けグループウェア、県立学校向け校務支援システム、インターネット接続サービス関係サービス、セキュリティ対策を導入している
学校ホームページサービス	県立学校の情報公開を促進するため、更新が容易で効果的なホームページを作成する機能を有したWEBサービスを提供
県立学校向け 校務支援システム	校務における業務負担を軽減することを目的とし、教務系（成績処理、出欠管理、時数管理等）・保健系（健康診断票、保健室来室管理等）、学籍系（指導要録等）、学校事務系など統合した機能を有するシステムの提供
市町小中学校向け 校務支援システム	校務における業務負担を軽減することを目的とし、教務系（成績処理、出欠管理、時数管理等）・保健系（健康診断票、保健室来室管理等）、学籍系（指導要録等）、学校事務系など統合した機能を有するシステムの提供
ファイル暗号化	教職員が作成したファイル自体を暗号化し、保存場所を意識することなく自動暗号化されるシステムの提供
リモート接続サービス	セキュリティ対策を実施しながら学校外部から校務系ネットワークへの接続を可能とし、教職員の校外活動を支援する機能の提供
緊急連絡網サービス	保護者、生徒と学校間および教職員と学校間の連絡事項について、迅速かつ正確に伝達するためのメール連絡機能を提供
回線	データセンターからインターネットに接続するための高速インターネット回線、県立学校とデータセンターのに接続するための閉域網回線から構成される
県立学校	データセンターと県立学校間のネットワーク接続制御を

設置機器	行うVPNルータおよび学校内ネットワークを制御するエッジスイッチ（L3スイッチ）を提供

現行の県立学校のネットワークは、各県立学校に整備された閉域網回線を介して利用するデータセンターに構築された教育クラウド基盤、校内のネットワーク機器等で構成されている。

本全体構成図上で示されている、ネットワークおよび代表的なシステムの概要を以下に示す。

現行システムの概要

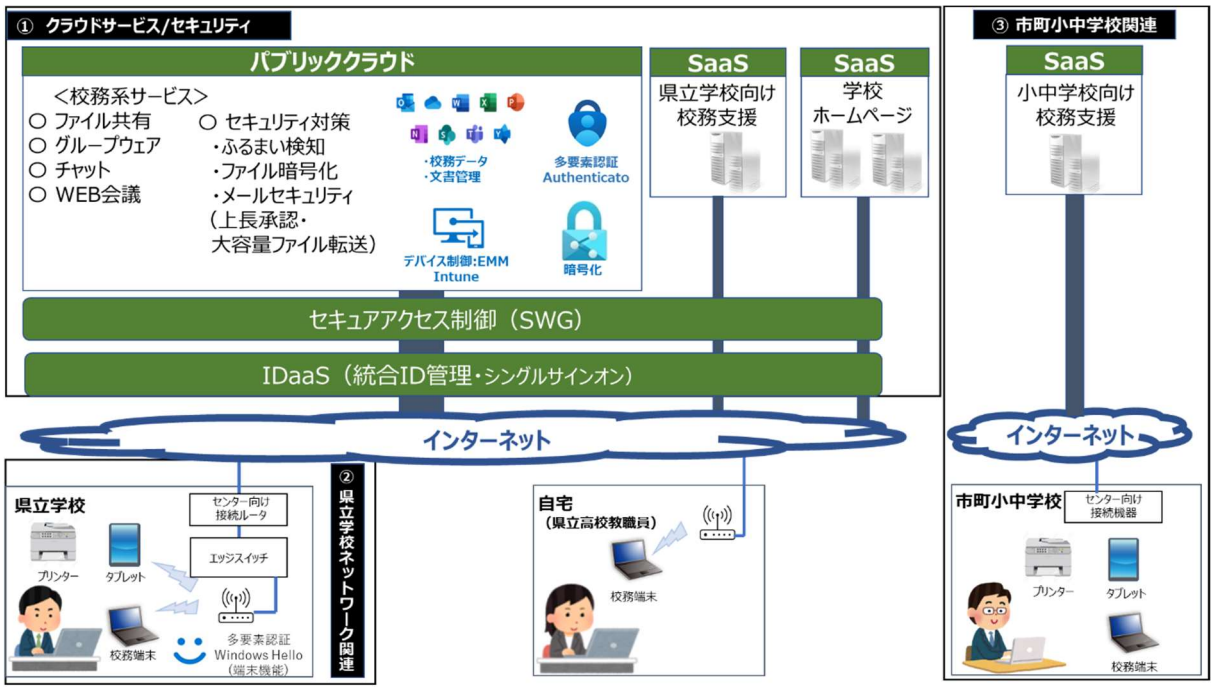
分類	概要
データセンター設置機器 （メールシステム関係）	メール送信時の誤操作防止のため、添付ファイルを自動的に暗号化し送信ができること誤送信防止システム ・メールを送信する時には設定した上長が承認・非承認を行うことができるワークフローの仕組みを実装 ・送信されるメールに添付ファイルがある場合、添付ファイルを暗号化（Zip化）し、パスワードメールを自動送信する ・ファイルアップロード時に自動でウイルスチェックを行い，ウイルスが感染したファイルの送信を防ぐ
データセンター設置機器 （セキュリティ関係）	（ア）Active Directory によるユーザー認証基盤 （イ）サンドボックス機能 ・メールおよびWEBアクセス通知への振る舞い検知し検査結果に基づき、外部との通信を遮断する機能を有する ・OSは複数のバージョンを提供 ・C&Cサーバーへの通信を監視し、通信を検知 外部から入ってくるファイルをサンドボックス上で実行しセキュリティの問題がないかどうかを確認 ・マルウェア解析が実施できること。また、Adobe ReaderやMicrosoft Office 等の脆弱性を突いた攻撃を検知できる機能を有する （ウ）ウイルス対策 教職員およびCAI教室の生徒端末に対し、データセンター側で一元的にシステム化を行いウイルス対策および管理を実施 ・ ウイルススキャン機能

	ドキュメントおよびシステムは、日本語に対応 スケジュールによりフルスキャンが可能 ・ 通知機能 ウイルス感染時はリアルタイムに感染した端末に通知 管理端末で感染端末の状況把握が可能 ・ 更新機能 ウイルスの定義ファイルを毎日自動で端末に配信 エンジンの更新に関しては、管理サーバー側でアップデート時期を調整可能、パターンファイルは最新バージョンを使用
インターネット通信関係	（ア）ファイアウォール システムを外部の攻撃から守るためにファイアウォールを設置し適切なセキュリティ対策および管理を行う （イ）Webフィルタ 教職員用端末に加え、県立学校全校CAI教室等による利用端末において、不適切なWEBサイトや情報を閲覧することのないように、すべてのインターネットへのWebアクセスは、Webフィルタを経由し、有害なサイトにアクセスしないように機能を提供
回線 データセンター　―　県立学校間	データセンターと県立学校間を接続する回線サービス （閉域網）
回線 インターネット接続回線	データセンターからのインターネット接続回線を提供 プロバイダとの接続回線は、冗長化した 1 Gbps 以上の帯域確保された回線を利用
県立学校 設置機器	データセンターと県立学校間のネットワーク接続の制御を行うVPNルータおよび学校内ネットワークを制御するエッジスイッチ（レイヤー 3 スイッチ）を提供 LAN 教室、CAD・高度情報教室、CAI教室等、情報教育をはじめとした各教科の学習を効果的に行うために整備した端末やタブレット、NAS 等が設置されている

4.2　教育ネットワーク環境の全体構成イメージと基本要件

4.2.1　全体構成イメージ

教育ネットワーク環境の全体構成イメージを以下に示す。



(1)　事業範囲

①　クラウド／セキュリティ関連

（ア）学校業務サービス

・Microsoft365 を利用した SaaS 提供

ファイル共有／チャット／WEB 会議／アプリケーション（Excel・Word 等）

インターネットメール　緊急時の連絡用サービス

・基盤、ネットワークサービス

学校ホームページ　　県立学校校務支援システム

（イ）アクセス認証モデル対応

・アクセス認証を実現するためのセキュリティ対策システム

統合 ID 管理　　シングルサインオン　セキュア WEB ゲートウェイ　資産管理

多要素認証　　ファイル暗号化　　ふるまい検知　等

校外からのアクセスについてのセキュリティ対策等

②　県立学校ネットワーク

・インターネット回線（小中学校校務支援システムに関わる仕様については

「4.2.2. 県立学校ネットワーク接続構成」を参照のこと。

・インターネット接続用ファイアウォール

・エッジスイッチ（構成に応じ最適なスイッチを設置すること。）

・校務端末設定（導入初期・年度異動時）

・無線環境整備（校務端末が学校ネットワークに接続するために必要となる設定）

・グローバルアドレス提供

必要なグローバル IP 提供校へのサービスおよびセキュリティ対策（構築・設定）

「4.2.2　（2）グローバルＩＰアドレスの提供」を参照

・必要なプロキシサーバーまたはサービス（全学校に対応すること）

また、利用するサービスに応じセッション数の枯渇等が発生しないようにすること。

③　市町校務支援関連

市町校務支援の費用は本県で負担する「校務支援システム基盤整備費用」と「各市町が負担する校務支援サービス利用料」で構成される。

（ア）　校務支援システム基盤整備費用

本基盤整備費用については以下の「システム利用校およびユーザー数概要」を参考に令和 7 年 4 月 1 日からの 5 年間の費用として本事業の費用に含み提案すること。

（イ）各市町が負担する校務支援サービス利用料

小中学校校務支援システムのサービス利用料は本事業に含まず市町教育委員会と直接契約するものとするが、令和 7 年 4 月 1 日からの 5 年間のサービス利用料についても本県が指定する様式にて別途費用提示すること。

なお、福井市については令和 6 年 6 月時点では対象外とする

表４．２．１　【システム利用校およびユーザー数概要】（予定）

区分		小学校	中学校	合計	教職員数	児童生徒数
福井	福井市	53	27	80	1,548	19,871
高志・奥越	永平寺町	7	3	10	145	1,342
	大野市	9	5	14	205	2,109
	勝山市	9	3	12	170	1,468
坂井	あわら市	10	2	12	170	1,818
	坂井市	19	5	24	549	7,331
鯖丹	鯖江市	12	3	15	407	6,013
	越前町	8	4	12	173	1,515
南越	越前市	17	8	25	496	6,261
	池田町	1	1	2	23	114
	南越前町	4	1	5	79	717
嶺南	敦賀市	13	6	19	375	5,055
	小浜市	9	2	11	208	2,202
	美浜町	3	1	4	63	570
	高浜町	5	2	6	87	709

	おおい町	4	2	6	85	682
	若狭町	9	2	11	150	1,125
合　　計		191	192	77	268	4,933

※児童・生徒数、学校数、学級数は令和 4 年 5 月 1 日現在

4.2.2　県立学校ネットワーク接続構成

(1) ネットワーク接続機能

・インターネットの接続は学校から直接インターネットに接続できる構成とすること。

・校務系業務に支障のないように回線数は下記の要件に準じること。

大中規模校　　：　2 回線

小規模校　　：　1 回線

大中規模対象校

1	藤島高等学校
2	高志高等学校･高志中学校
3	羽水高等学校
4	足羽高等学校
5	三国高等学校
6	金津高等学校
7	丸岡高等学校　全日制
8	大野高等学校（全日、定時）
9	勝山高等学校
10	鯖江高等学校（全日、定時）
11	鯖江高等学校（丹南キャンパス）
12	丹生高等学校
13	武生高等学校（全日、定時）
14	武生東高等学校
15	敦賀高等学校（全日、定時）
16	美方高等学校
17	若狭高等学校（全日、定時）
18	若狭東高等学校
19	福井農林高等学校
20	坂井高等学校
21	科学技術高等学校
22	奥越明成高等学校
23	敦賀工業高等学校
24	福井商業高等学校
25	武生商工（工業キャンパス）
26	武生商工（商業キャンパス）
27	嶺北特別支援学校

小規模対象校

1	丸岡高等学校　定時制
2	若狭高等学校（海洋キャンパス）
3	道守高等学校
4	盲学校
5	ろう学校
6	福井特別支援学校
7	福井南特別支援学校
8	福井東特別支援学校
9	福井東特別支援学校　月見分教室
10	福井東特別支援学校　五領分教室
11	奥越特別支援学校
12	清水特別支援学校
13	南越特別支援学校
14	嶺南東特別支援学校
15	嶺南西特別支援学校
16	県教育庁
17	嶺南教育事務所
18	教育総合研究所
19	特別支援教育センター

(2) グローバルＩＰアドレスの提供

(ア) 県立学校によっては固定グローバル IP アドレスが必要な拠点がある。本ネットワークとは物理的もしくは論理的に隔離した環境で、現行利用中のサービス維持条件にそってグローバル IP アドレスの割り当てを行うこと。

割当てている IP アドレス数は以下。

・科学技術高等学校（16）　　・高志高等学校　（ 8）
・坂井高等学校　　（16）　　・武生商工高校　（16）
・福井商業高等学校（16）　　・教育総合研究所（32）

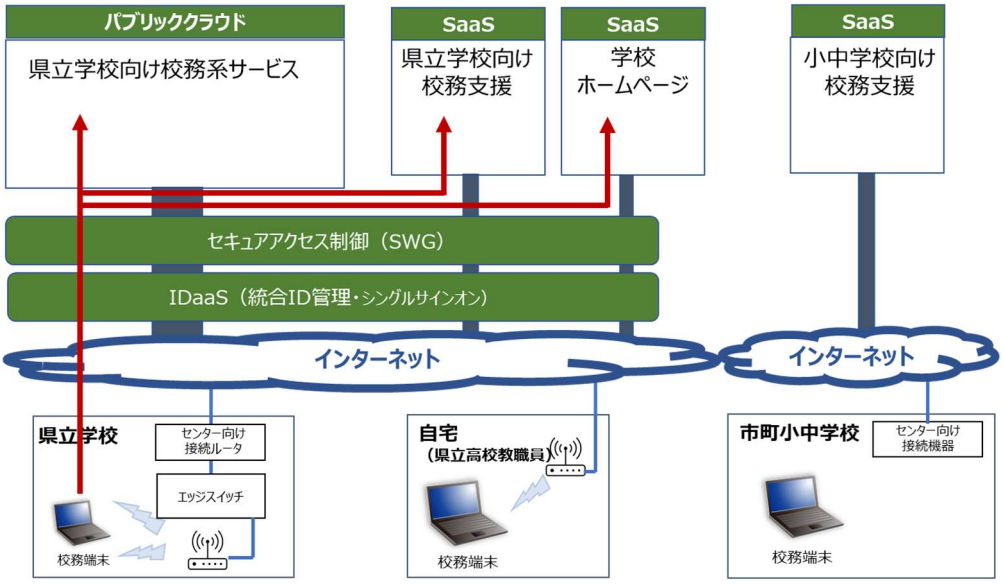
4.2.3　基本要件

教育ネットワーク環境全体の基本要件を以下に示す。

各機能の詳細（個別要件）については、『5.個別基本設計』を参照のこと。

（1） 通信に関する基本要件

（ア）県立学校で校務端末を利用する場合

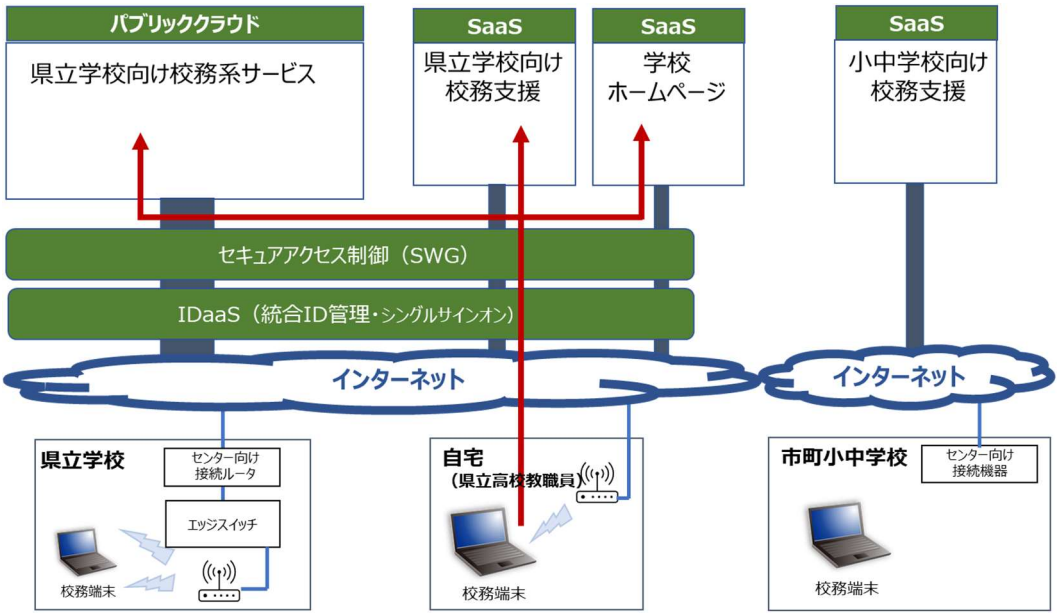


・ 県立学校で校務端末を利用する場合、原則の各学校に準備した回線（IPoE 回線）を利用して、県立学校向け校務系サービス、SaaS 型校務支援システム、学校代表 Web システムに通信できること。

・ 上記に加え、一般のインターネットサイトへアクセス可能であること。

・ 原則教育クラウド基盤経由でセキュリティ対策を施すこと。

（イ）自宅等の校外で校務端末を利用する場合

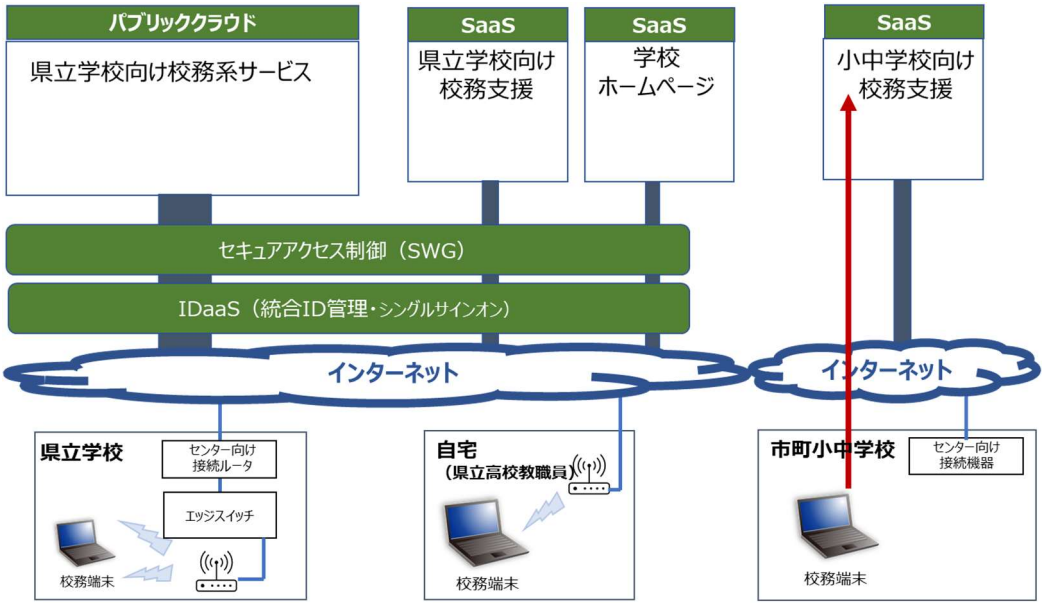


・ 教職員の自宅等校外で校務端末を利用する場合、自宅のインターネット回線等を利用して、教育クラウド基盤経由で県立学校向け校務系サービス、SaaS 型校務支援システムなどの必要なサービス等と通信ができること

・ 上記に加え、一般のインターネットサイトへアクセス可能であること。

・ 原則教育クラウド基盤経由でセキュリティ対策を施すこと。

（ウ）小中学校で校務端末を利用し校務支援システムを利用する場合



・ 小中学校向け校務支援システムを利用する場合はする場合、福井県下小中学校で校務端末を利用し通信できること。

・ 小中学校以外からの通信については利用できないようセキュリティ対策を施すこと。

(2) 校務端末に関する基本要件

（ア）端末に保存されたデータは完全に暗号化されていること。

（イ）端末から外部媒体へのデータコピーを制御すること。(USB メモリ、DVD-R 等)

（ウ）端末に対して常に最新のソフトウェア・パッチを自動配信可能なこと。

（エ）端末上のウイルス感染に加え、不審な挙動やログ情報も検知し、迅速な対応の支援(自動での対応実施含む)ができること。

（オ）端末の一元管理（リモート制御、アプリ配布、利用制限、監視、端末情報収集等）ができること。

（カ）校務端末については、各県立学校からの通信先に対して、原則教育クラウド基盤経由でセキュリティ対策を施したうえで通信を可能とする。

（キ）2024 年度および 2025 年度に別事業で調達する予定の校務端末に初期キッティングを実施すること。初期キッティングは Windows Autopilot を想定すること。ただし特別支援学校の端末については、既存端末の利用を想定しており（950 台）既存端末を含めてキッティングを行うこと。なお、既存端末の回収および端末キッティング後の配布については本事業に含まないこととする。

(3) データのやり取りに関する基本要件

具体的には、以下の基本機能を実装すること。

（ア）校務端末に保存されたファイルは重要情報を分類（ラベリング）できること。また、その分類の確認も容易にできること。

（イ）重要情報に分類されたデータがアクセス権のないユーザーに誤って送付された場合でも、暗号化対策により復号できない（中身が見えない）設定が施されていること。

（ウ）重要情報の分類（ラベリング）についてログの記録と監査が行えること。また、ファイル操作（印刷、コピー、名前変更、クラウドへのアップロード等）についても同様にログの記録と監査が行えることが望ましい。問題がある操作は、ログへの記録等を行う。

（エ）重要情報に分類（ラベリング）された情報であっても、承認者の承認を得たうえで、ラベル制御を行い対象ユーザーに提供できること。

4.2.4 教育ネットワーク環境の全機能一覧

教育ネットワーク環境の全機能一覧を以下に示す。

ただし、各機能が、他の機能を用いて実現可能である場合や、他の複数の機能の組合せや連携において実現可能であり、かつその旨を明確に示された場合、当該要件は充足されていると見做す。

【設計・調達・実装・運用保守の全てを担うもの】

分類	No	機能名称	機能概要と役割
基盤サービス（認証、セキュリティ等）	1	ユーザー認証・IAM	教育ネットワークにおける校務端末（Windows）のログイン認証を行う機能である。また、校内、校外のアクセス元を問わず、Microsoft365 などの校務系システムやサービスにシングルサインオン可能な仕組みを提供する。 福井県共通で利用するActive Directoryによる教職員用認証情報の基盤を構築する。
	2	エンドポイント	校務端末に対するエンドポイントセキュリティ対

		セキュリティ・EDR	策として、EPP(Endpoint Protection Platform)およびEDR（Endpoint Detection and Response）機能を提供する。
	3	パッチ・ソフトウェア配信	校務端末に対して更新プログラムやソフトウェア配信機能を提供する。
	4	端末管理・MDM	校務端末のハードウェア・ソフトウェアの管理機能を提供する。
	5	CASB	特定のクラウドサービスに対する詳細なセキュリティ対策としてのCASB（Cloud Access Security Broker）機能を提供する。
	6	情報漏洩対策・DLP	情報の取扱いを管理し、校務情報等重要情報が意図せず外部に漏えいすることを防止するDLP（Data LossPrevention）機能を提供する。
ネットワークサービス	7	SWG	Web サービスに対するセキュリティゲートウエイ機能を提供する。
	8	DNS サービス	校務端末に対し教育ネットワークに関連する各種ドメインの名前解決機能を提供するとともに、外部向けDNSゾーン情報等の管理を行う。
	9	統合監視・ログ管理サービス	教育ネットワーク全体の死活監視・リソース監視・性能監視等の統合的な監視機能を提供する。
	10	インターネット接続サービス	インターネット（SaaSサービス含む）との接続や、インターネット外部から校務端末を守るファイアウォール機能を提供する。
	11	Webフィルタリング	教員および生徒向けのwebフィルタリングサービスを提供する。
業務サービス	12	校務系メール	現在の校務系ネットワーク環境で利用している教職員の個人メール、学校代表メール、業務用メールそれぞれの機能を提供する。また、県内教職員のグループに対してメールを一括送付する機能を提供する。
	13	オンライン会議	教職員内および外部と実施できるオンラインによる会議機能を提供する。
	14	チャット	教職員内および外部と情報交換できるチャット機能を提供する。
	15	ファイルストレージ	クラウドを利用して、校内の教職員間でファイルを共有する機能を提供する。校内の承認者および

			指定した教職員アカウントのみアクセス可能な領域を定義できること。
	16	教職員向けポータルWebサイト	教職員への情報共有や校内での情報共有、メンバー申請により限られた教員間での情報共有機能を有するWeb サイトを提供する。
	17	統合型校務支援システム	生徒情報の管理や成績処理等を行うシステムを提供する。

【設計・調達・実装・運用保守の全てを担うもの】

学校設置機器	1	学校設置ファイアウォール	教育ネットワークの既存機器を改修しインターネットへ接続できる環境を提供する。 また、教育ネットワークとのルーティング、ファイアウォール、IP・TCP／UDPポートフィルタリング機能等を提供する
	2	エッジスイッチ	教育ネットワークの既存機器を改修し、教育ネットワークを収容する
	3	DHCP サーバー	教育ネットワークの既存機器を改修し、校務端末に動的にIPアドレスを払い出すDHCPサーバー機能を提供する
	4	無線アクセスポイント	教育ネットワークの既存機器を改修し、校務端末にセキュアな無線ネットワーク環境を提供する。

5. 個別基本設計

5.1 ユーザー認証・IAM

ユーザー認証・IAMとは教育ネットワークにおける校務端末（Windows）のログイン認証を行う機能をさす。また、校内、校外のアクセス元を問わず、Microsoft365 などの SAML 認証、OpenID Connect、OAuth 等に対応した校務系サービスにシングルサインオン可能な仕組みを提供する。

5.1.1 機能要件

(1) 教育ネットワークにおける教職員のアカウント情報および、校務端末情報の管理を行うことができること。
(2) 教育ネットワークにおける教職員のアカウント認証が可能であること。なお、端末ログイン認証については、対象 OS を Windows とする。
(3) 主要な機能をブラウザで管理できること。また、特殊な機能の設定や一括処理をする際には PowerShell や API を使ったプログラム等からの管理ができること。
(4) 登録されたメールアドレスやスマートフォンへのコード送信、顔認証、指紋認証等を組み合わせ、本サービスでの認証時に追加での本人確認を行うことでセキュリティ強化ができること。
(5) 認証情報（パスワード等）を、ユーザー自身が変更することができる。
(6) 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レポートとして確認できること。

5.2 EPP・EDR

EPP・EDR とは、校務系端末をウイルス等の脅威から防御するとともに、端末の挙動を常時記録・分析することによりウイルスやランサムウェア等の脅威発生を検出し、迅速かつ詳細に調査・復旧等の対応を行う機能をさす。

5.2.1 機能要件

(1) 既知の攻撃のみならず、未知の攻撃にもリアルタイムに対応すること。
(2) クラウド上にある最新のセキュリティ情報を参照して、ウイルスの検索が可能なこと。
(3) システム動作の監視と制限を行い、不正にシステムが変更されるのを検知できること。
(4) 収集したログファイルを元に、マルウェアの詳細情報（オブジェクト情報、マル

ウェアが生成したプロセス情報、マルウェアの通信先情報など）を可視化する機能を有すること。

(5) 攻撃を検知した場合には、原因、不正振舞の分析、感染した端末の特定、影響範囲把握できること。

(6) 端末がネットワークに接続していない期間のログは、ネットワーク再接続時に収集可能であること。

(7) 正規アプリケーションを阻害する事象（過検知）が発生した場合、検知機能を適用しないファイル・ディレクトリ等を指定し、過検知を回避する機能を有すること。

(8) 管理画面およびマニュアルが日本語に対応していること。

(9) ウイルス感染の疑いのある端末を論理的にネットワークから隔離することができること。

(10) 不正な暗号化や変更から文書を保護するなどのランサムウェア対策機能を有していること。

(11) 検索した結果を CSV・Excel 形式ファイルにて出力できること。

(12) 隔離された端末の脅威分析などを完了し、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。

(13) これらの機能は、原則として Windows を対象として提供されること。

5.3 パッチ・ソフトウェア配信

パッチ・ソフトウェア配信とは、教育ネットワークを利用する教職員の校務用端末に対して、OS や各種アプリケーションの更新プログラムやソフトウェア配信等を行い、端末を最適な状況で利用するための管理を行う機能をさす。

5.3.1 機能要件

(1) Microsoft 製ソフトウェアの更新プログラムの管理や配布に対応できること。

(2) 資産管理システムと連携する等、効率的な配信が可能であること。

(3) 必要に応じて配信するパッチを指定し、配信可能であること。

(4) セキュリティを保ち、Windows 機器に対してソフトウェアの配信を行えること。

(5) 更新プログラム配信対象のグループ分けや配信条件の詳細な指定を行えること。

5.4　端末管理・MDM

端末管理・MDM とは、教育ネットワークを利用する教職員の校務用端末の不正利用や情報漏洩を防ぐため、端末のハードウェア・ソフトウェア情報管理を行う機能をさす。

5.4.1　機能要件

(1) 校務端末(Windows、iOS)について、各デバイスの設定を強制する機能を有すること。
(2) 校務端末(Windows、iOS)について、リモートワイプにてデバイスを初期化できること。
(3) MDM に登録できるデバイスを事前に設定し、制限する機能を有すること。
(4) ポリシーに基づき、登録されている PC のアクセス制御ができること。
(5) Bit Locker 回復キーの管理ができること。
(6) 遠隔で PC の再起動ができること。
(7) 制御ポリシーは管理対象クライアント PC ごとに異なるポリシーを適用できること。
(8) 遠隔で PC のローカルデータを削除できること。
(9) 管理端末の利用情報を取得できること。
(10) Wi-Fi プロファイルの配布ができること。
(11) MDM にデバイスを登録することで、登録済みデバイスのみアクセスを許可する設定ができること。

5.5　クラウドアクセス制御

教職員による特定のクラウドサービス利用に関して、利用内容の可視化を行うと共に、データ内容やアプリケーションの操作内容の制御等を詳細レベルで行うこと。

5.5.1　機能要件

(1) 利用状況の可視化と分析
　(ア) 機能の対象とする教育クラウド基盤で稼働するサービスに対して、教職員の利用を検出・可視化できること。
　(イ) 教育クラウド基盤で稼働するサービスの安全性についてリスクを評価・分析できること。
(2) 制御（コントロール）
　(ア) メールの送受信や、クラウドアプリケーションのサービス自体には影響を与えない状態で、クラウドサービスと API ベースでの連携が可能であること。

(3) データセキュリティ※情報漏洩対策・DLP との連携機能

（ア） 本機能の対象とする教育クラウド基盤で稼働するサービスに対して、取り扱うファイル等の情報に付与されたラベルや含まれる重要性分類の判別が可能であること。

（イ） 教育ネットワークにおける認証を経た利用者の各権限およびファイル等情報に付与されたラベルや、含まれる重要性分類を識別し、削除や隔離ができること。

（ウ） ラベルによる重要性分類が示されていないファイル等情報のアップロードが教育クラウド基盤で稼働するサービスに対して行われた場合、アップロードの遮断やアラート検出など、必要な対応の定義が可能であること。

（エ） 許可されていないファイル等情報の削除や隔離ができること。

(4) 脅威の検出・防御

（ア） 教育クラウド基盤で稼働するサービス内やファイルなどに潜むマルウェアなどの脅威を検知できること。

（イ） マルウェアなどの脅威を検知した場合に、通信を遮断し、原因となるファイルを隔離できること。

(5) ポリシー管理

（ア） 本機能における各種制御について、ポリシーとして定義し適用することが可能であること。

5.6 情報漏洩対策・DLP

情報漏洩対策・DLP(Data Loss Prevention)とは、教育ネットワーク内のシステム、サービスおよび端末内に保存されている校務系情報や個人情報などの重要情報が含まれた特定のデータに対して、過失や意図的な外部へのデータ漏洩を防ぐために各種制御を行う機能をさす。また、特定のデータに対する操作を制御・記録することでインシデント発生時の経路等を追跡できる機能である。

5.6.1 機能要件

(1) ラベル付与

(ア) 機密性に応じたラベル付けができること。

(イ) ラベル付けに応じて閲覧可能なユーザーや端末を制限できること。

(ウ) Office ファイル(Word、Excel、PowerPoint)にラベル付けができること。

(2) 情報漏洩対策

暗号化された状態で格納されたファイルが教育ネットワークの外部に流出した場合、認証を経ない利用者による内容参照や操作が行えないこと。

(3) データ追跡

(イ)ラベリングされたデータ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。

(ウ)ラベリングの操作をログにて、追跡できること。

5.7 SWG

SWG(Secure Web Gateway)とは、不審な URL や IP アドレスへのアクセスをブロックする機能、マルウェアの感染や侵入を検知しブロックする機能、暗号化されたトラフィックの脅威をチェックする機能、通信を可視化する機能など、Web サービスへのアクセスに対してゲートウェイとして機能し、セキュリティ対策を目的とする機能である。これらの機能により、インターネットのトラフィックを分析して、悪意あるファイル・アプリケーションのブロックや Web サイトへのアクセス防止を行い、マルウェアなどの脅威から端末を保護する。

新環境では SaaS 型のシステムを想定しており、教職員が利用する端末の利用場所を問わず、インターネットへのアクセスを制御できるものとする。

5.7.1 機能要件

(1) Web フィルタリング機能

(ア)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。

(イ)Web トラフィックはクラウド上のプロキシ経由とし、URL チェックなどのアクセス制御、URL 単位の詳細な制御ができること。

(ウ)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）の設定ができること。

(エ)20 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すること。

(オ)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。

(カ)フィルタリングのパターンについては、複数作成できることとし、グループごとに適用できること。

(2) マルウェア対策機能

(ア)Web 経由での検知、および検知後に通信をブロックできること。

(イ)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対策ができること。

(3) SSL 復号機能

SSL で暗号化されたトラフィックについても復号を行い、上記(1)から(2)に掲げる機能により脅威の検知・対策ができること。

(4) DNS セキュリティ

DNS の名前解決の仕組みを利用して、ウェブ通信だけでなくすべてのポートとプロ

トコルについて脅威の有無を判定し、危険なドメインへの通信を阻止できることとする。

(5)通信可視化

(ア)ウェブアクセスの履歴（検出時間、ドメイン、クライアント IP、URL、宛先 IP、カテゴリ、脅威名、内部クライアント IP、端末名、クライアントリクエスト ID、アプリケーション、リスク、サブロケーション、MAC アドレス等）を可視化して、利用者の行動や不明な点を検出し、アクティビティの詳細を確認することができること。ウェブアクセスも履歴については、個人毎に確認ができることとする。また、ウェブアクセスの履歴の保管期間は 30 日間以上とすること。

5.8 資産管理システム

資産管理システムとは、情報資産管理と端末セキュリティ対策を単一のシステムで一元的に管理できる機能をさす。

5.8.1 機能要件

(1) 情報資産管理

(ア)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に関するインストール状況等を、資産情報として自動的に収集でき、一覧で表示できること。

(イ)収集した資産情報を検索できること。検索条件には、インベントリ情報や OS のバージョン、空き容量、死活監視状態など複数項目を指定した AND,OR,NOT 検索が可能であること。

(ウ)指定したクライアントコンピューターに対して、複数の任意のプログラムを配布し、自動的にプログラムの実行および解除を行う機能を有すること。また任意指定端末や、検索した資産情報リストをグループとして登録でき、そのグループに対してソフトウェア配布やファイル配布等の各種操作が可能なこと。

(エ)IP アドレスの管理台帳と、資産情報（不許可端末検知情報も含む）を照合し、競合や不正使用、使用期限切れの表示を行えること。また表示方法は、一覧表示およびマップ表示を行えること。

(2) ログ取得

(ア)クライアントコンピューターに対して行われた操作、ログオン・ログオフの日時、実行されたソフトウェアについての起動時刻・操作時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、Web へのアクセス・書き込み・アップロード、クリップボード（テキスト・画像）、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報、接続した通信デバイス、および外部との通信状況等を記録する機能を有すること。

(イ)端末がネットワークに接続していない期間のログは、ネットワーク再接続時に収

集可能であること。

(3) レポート機能

収集されたログを集計、グラフ化し、レポートデータとして閲覧できること。

(4) 制限・制御・アラート管理

(ア) アラート項目ごとにメールでの配信先の設定ができ、アラートの発生時には、設定された通知先にメールを自動送信できること。また、配信先の設定では、複数のメールアドレスをまとめたグループを使用することができること。

(イ) あらかじめ登録されていないクライアントコンピューターが接続された場合、該当のクライアントコンピューター情報を取得し、一覧表示できること。また、接続されたことを管理機のデスクトップにポップアップ表示および、メールで通知できること。

(5) リモート操作

(ア) 特定のクライアントコンピューターに対して、ネットワーク経由で、リモート操作が行える機能を有すること。なお、管理機操作の際のログオンパスワードは、変更できること。

(イ) リモート操作されているクライアントコンピューターのデスクトップに、操作中であることを通知するポップアップを表示する設定ができること。

(ウ) リモート操作時に、操作機側とクライアントコンピューター間でファイルの転送ができる機能を有すること。

(エ) リモート操作時に、操作機側とクライアントコンピューター間でテキストデータやビットマップ形式の画像データをコピー＆ペーストし、共有できる機能を有すること。

5.9 DNSサービス

DNS(Domain Name Service)サービスとは、以下に示す「内部 DNS サービス」および「外部 DNS サービス」からなる。

内部 DNS サービスは、校務端末から教育ネットワーク内のリソースに接続する際に名前解決を行うためのものである。

外部 DNS サービスは、校務系メールで利用しているドメインに関する MX レコード等の正引き情報やメールサーバーの逆引きゾーン情報の管理を行うためのものである。

5.9.1 機能要件

(1) 内部 DNS サービス

各種システムの利用について、校務端末からの名前解決を可能とすること。

(2) 外部 DNS サービス

(ア)校務系メールの送受信に必要な A レコード、MX レコード、PTR レコード、TXT レコード等の管理機能を提供できること。

(イ)送信元アドレスを詐称するなりすましメール対策として、SPF(Sender Policy Framework)、DKIM(Domain Keys Identified Mail)、DMARC(Domain-based Message Authentication、Reporting and Conformance)等の送信ドメイン認証の仕組みを実装すること。

5.10　インターネット接続サービス

インターネット接続サービスとは、各県立学校やプラベートクラウド基盤とインターネットとの境界上で包括的なセキュリティ対策を行うための「ファイアウォール機能」および「インターネット回線」をさす。

ファイアウォール機能は、各県立学校や教育クラウド基盤で稼働する各システムをインターネット上の脅威から保護する役割と、各システムからインターネットへの通信を最小限に限定するための役割を持つ。

なお、県立学校に設置済みであるシステムについては、受託者が各県立学校に確認をすることとする。

5.10.1　機能要件

(1)ファイアウォール機能

(ア)イントラネットからインターネットへの通信については、通信可否 (許可/遮断)の制御が可能であること。

(イ)イントラネット間の通信について通信可否(許可/遮断)の制御が可能であること。

※通信可否の制御にあたってはステートフルインスペクション等を用い、通信前後を把握した上で通過可否判定を行えること。

(ウ)トラフィック方向ごとに異なるセキュリティポリシーが実装可能であること。

(エ)IP アドレスごとに詳細なポリシーが定義できること。

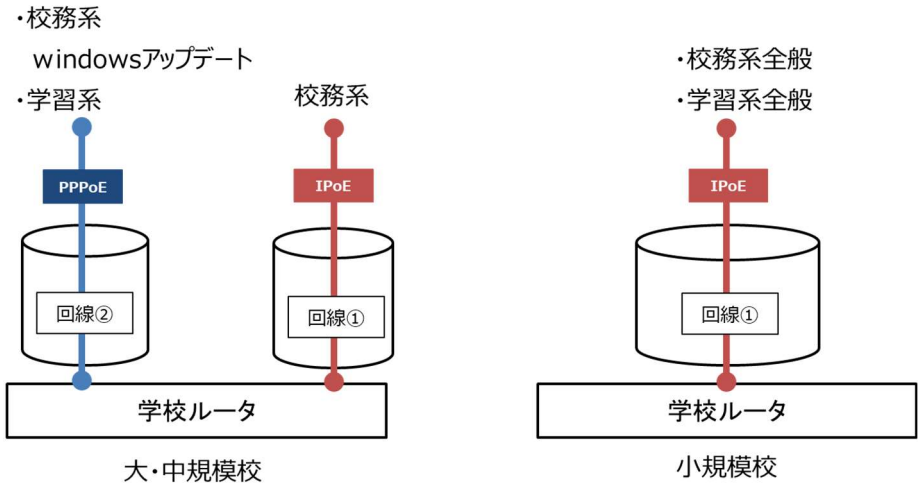
(オ)DoS 攻撃防御機能を有すること。

(2)ネットワーク接続機能

(ア)各拠点との通信においては、通信経路は暗号化されること。

(イ)校務系の通信については IPoE 通信とする

(ウ)IPoE は固定 IP とすること



区分	回線区分	回線用途
大中規模校	回線①	校務系通信
	回線②	学習系通信 校務系パソコンの Windows アップデート通信
小規模校	回線①	校務系通信、学習系通信

5.11　校務系メールについて

各教職員に Microsoft ライセンスが付与され、Microsoft 365 Exchange Online を利用できることとする。利用者は校務用端末機から Microsoft Outlook アプリまたはブラウザから Microsoft365 にアクセスしメール機能を利用でき、校務用端末機へのログイン情報と連携できること。

5.11.1　機能要件

(ア) 学校代表メールや業務メールなどについて、「共有メールボックス機能」や「配布グループ」で指定したアカウントで閲覧できること。

(イ) メールボックスに追加表示したいアカウントのメール環境において一定の操作を行うことで、学校代表メールや業務用メールを自身の環境に追加表示できる仕様とすること。

(ウ) 新環境において、各メールのドメインは現行から変更することを想定しており、ドメインの取得・管理に必要な手続きや費用については受託者の負担とすること。

(エ) メールフィルタリング機能を備えていること

(オ) アドレス帳から全県立学校の教職員を検索できること。

(1) 誤送信防止

(ア)外部に添付メールを送信するときは受託者のみが設定した上長が承認・非承認を行うことができるワークフローの仕組みが実装されていること。

(イ)PPAP 問題を解決するために添付ファイルダウンロード方式を採用すること。

5.12 オンライン会議

新環境ではSaaS 型のシステムを想定しており、Microsoft ライセンスを有効活用し、教育アカウントと連携することで、機能制限なくオンライン会議を実施できる環境を提供する。

5.12.1 機能要件

（ア）音声や映像、画面共有などのリアルタイムコミュニケーション機能が図れるWEB 会議機能を提供すること。

（イ）教職員間、外部と WEB 会議が可能なこと

（ウ）メールにより会議参加者を招待できること

5.13 チャット

校務端末でチャットができる環境を提供すること。

5.13.1 機能要件

（ア）教職員間でメッセージの送受信できること。

（イ）任意の利用者を設定し複数人への同報ができること。

（ウ）送受信した過去のメッセージを確認できること。

（エ）１対１のチャットだけでなく、グループごとにチームを作成できること。

（オ）チャット内にファイルや画像を送信できること。

（カ）１人または複数のユーザーとチャットするときに、自身の画面を共有することができること。

5.14 ファイルストレージ（学校共有ファイルサーバー）

5.14.1 機能要件

（ア）クラウド上に用意されたファイルサーバーを利用すること。

（イ）別事業で調達する校務端末に対してエクスプローラーと同期ができること。

（ウ）フォルダ・ファイル単位にアクセス不可、閲覧、編集可能などのアクセス権が設定できること。
（エ）各県立学校別に割り当てられた保存境域に対して、教職員がアクセス可能であること。
（オ）各学校別に一般・システム管理者・校長・教頭の４つの領域を確保して領域ごとにアクセス権を付与して構築すること。
（カ）各学校に１TB の領域を確保すること。

5.15　個人領域ファイルストレージ

5.15.1　機能要件

（ア）クラウド上に用意されたファイルサーバーを利用すること。
（イ）エクスプローラーで表示ができること。
（ウ）一定期間のバックアップ機能を備えていること。
（エ）教職員１人あたり５０GB の領域を確保すること。

5.16　教職員向けポータルサイト

5.16.1　機能要件

（ア）ポータルはwebベースで問い合わせや各種申請状況を教育庁および各学校情報担当者間でリアルタイムに確認できること。過去の問い合わせや障害対応のやり取りも検索により確認できること。

5.17　データ分析機能

校務データおよび学習データの連携による最適な学びの実現といったICT を活用した教育に関する最新の動向を踏まえデータを分析し、ダッシュボード機能の整備方針を提案すること。

5.18　グループウェア

グループウェアについては、以下の機能を備えること。
(1) スケジュール機能
教職員同士のスケジュールを共有することができること。

(2) 施設予約機能

（ア）会議室などの設備予約する機能を有しており、設備ごとに予約できるユーザーを制限できること。

（イ）予約対象物、開始日時、終了日時、繰り返し条件を指定し、施設・備品の予約登録・削除ができること。また、個数を指定した予約ができること。

(3) 在校管理機能

（ア）各学校の教職員が在校時間（勤務時間）の登録・修正と出力が簡易にできること。

（イ）在校時間記録機能を有すること。

（ウ）承認者が各教職員の入力状態を確認できること。

(4) 休暇申請

（ア）休暇や病休などの種別を選択できること。

（イ）承認者を選択することができること。

（ウ）在校管理システムと連携して個人の休暇簿などに出力できること。

(5) 出張申請機能

（ア）教職員の出張に関して、承認者を選択して申請ができること。

（イ）月ごとに CSV などでエクスポートできること。

(6) 電子申請

（ア）申請、承認機能を有すること。

（イ）ファイルを添付することが可能であること。

5.19 学校ホームページ

県立学校の情報公開を促進するため、更新が容易で効果的なホームページを作成する機能を有したサービスを提供すること。

なお、新たにリニューアルする場合は県が指示するドメインを利用すること。

5.20 緊急連絡網サービス

保護者、生徒と学校間および教職員と学校間の連絡事項について、迅速かつ正確に伝達するための連絡機能またはサービスを提供すること。

5.21　県立学校校務支援システム

県立学校校務支援システムに関わる仕様については「別添 1_県立学校校務支援システム」を参照のこと。

5.22　小中学校校務支援システム

小中学校校務支援システムに関わる仕様については「別添２_小中学校校務支援システム」を参照のこと。

6.　　移行・切替計画

6.1　ネットワーク移行計画

(1) 全ての県立学校の既存保守事業者と連携し県教育庁ならびに教職員の負担が最小となる移行方法を提案し実施すること。
(2) 移行作業に必要な情報収集のため、県立学校の現地確認を実施すること。
(3) 令和７年３月31日までの間に、すべての対象教育機関の移行作業を完了すること。
(4) 各県立学校における現地での移行作業は、校務に支障がない期間／時間帯に実施するよう県立学校と調整すること。業務に支障をきたさないようにすること。
(5) 県立学校と日程調整をした上で、移行作業までにシステム移行実施計画書を作成し、県教育庁の承認を得ること。
(6) 移行完了の翌営業日は、現地にて利用者からの問い合わせに遅滞なく対応できるよう、各教育機関で個別に立会いを行うこと。
(7) 本期間中に、既存の「校務系ネットワーク」や「学習系ネットワーク」に関するネットワーク・機器等についての設定変更も併せて行い、校内では職員室や準備室等に整備している有線ネットワークを継続して現行「校務系ネットワーク」として利用することを可能とし、また職員室・普通教室等における無線AP に対して新たな校務系の無線ネットワークを追加し、新「教育ネットワーク」として利用することを可能とすること。
(8) 主として校務系システムに関して必要なデータ移行を実施すること。以下の項目のデータを移行する。
　(ア)必要なファイルストレージのデータ移行
　(イ)学校ホームページコンテンツ
　(ウ)小中学校校務支援データ
　(エ)県立高校校務支援データ

(9) 基本的には受託者にて現在のシステムで使用されているデータのうち、必要な全て

のデータ移行を行うものとするが、データの安全性や移行の確実性が担保されるなど、合理的な理由がある場合は県教育庁、県立学校教職員にて移行作業を代行する企画提案も可とする。その場合は、理由と具体的な役割分担、手順、想定作業負荷、通信経路、既存システムの設定変更依頼内容等を示すこと。

（10）教職員個人のデータは受託者にて環境や手順を整備したうえで、教職員自身の作業で移行することも可とする。ただし、ファイルの共有のデータ（学校共有、県 教育庁所管の全校共有等）は受託者にて移行すること。

（11）ファイルの移行にあたっては、受託者からの指示に基づいて県立学校側で移行データの整理を行うことも可とする。（例：不要ファイルを削除し、ファイル数や総容量を制限まで削減する、長すぎるファイル名のものは事前に短縮する等。）

（12）学校ホームページコンテンツの移行にあたっては、互換性等の問題で移行できないデータが発生する可能性が想定される。その場合は、設計工程で代替策を整理したうえで、対応すること。

（13）学校ホームページコンテンツの移行にあたっては、教職員が作成したコンテンツ内に埋め込まれたリンクの修正は教職員の役割とすることも可とする。

7. 総合運用管理要件

（1）本調達範囲で構築したシステムを安定的に利用するための運用管理業務を実施すること。

（2）全ての県立学校の現行の保守事業者と連携し県教育庁ならびに教職員の負担が最小となる

保守サービスを提供すること。

7.1 運用管理業務対象機器等

（1）本調達で導入するすべての機器、サービス、システムについて、運用管理業務対象範囲とする。

（2）県教育庁と受託者は定例会を3か月に1回開催すること。定例会の内容については、業務報告および現状の課題などについて県教育庁に報告・協議すること。

（3）緊急性が高い事案や懸念事項がある場合は臨時の定例会を開催すること。

7.2　運用体制について

本調達で構築したネットワークを安定的に利用するために運用管理業務を実施すること。運用管理を実施するために以下の役割を受け持つ体制を配置すること。

(1) 統括運用管理責任者

本業務全体の統括管理を行う全体的な業務責任者

(ア) 全体運用について把握するとともに全体管理を実施すること

(イ) 通常運用管理業務の技術的支援を行うとともに障害発生時の復旧対応を実施すること。

(ウ) 重大なセキュリティ事案が発生した場合に原因調査等の対応を実施すること。

(2) コールセンター業務

(ア) 電話受付は平日 9 時 00 分から 18 時 00 分とする。

(イ) 利用者からのシステムに関する故障連絡や各システムの問い合わせについて一時窓口としての業務を行うこと。連絡を受けた場合は、関係者への連絡等適切な対応をとること。

(ウ) 人員配置については令和 4 年度のコール実績を参考にすること。

問い合わせ内容	R4年度												
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	小計
作業連絡	4	2	1	4	4	1	2	-	1	2	2	5	**28**
アカウントに関する問合せ（グループメンバ・ファイルサーバに関するものも含む）	36	14	5	3	9	7	3	-	3	2	2	32	**116**
校務支援に関する問合せ	164	78	138	116	66	67	55	28	48	31	54	138	**983**
緊急連絡サービスに関する問合せ	-	-	1	-	-	-	-	-	1	1	-	-	**3**
ホームページ・CMSに関する問合せ	5	5	4	6	4	5	2	3	1	2	4	2	**43**
メールに関する問合せ	8	7	6	2	-	3	1	3	-	-	3	4	**37**
Proxy設定に関する問合せ	-	-	-	2	1	4	2	3	2	1	1	3	**19**
端末（PC、プリンタ等）に関する問合せ	10	4	11	5	10	4	6	2	4	4	7	12	**79**
在校時間管理に関する問合せ	-	-	-	1	-	-	-	-	1	-	-	-	**2**
セキュリティインシデント	-	-	-	-	-	-	-	-	-	-	-	-	**0**
その他	19	8	5	8	5	2	4	3	2	7	9	8	**80**

設定作業内容	R4年度												
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	小計
アカウント登録/変更申請	70	25	12	3	13	14	6	6	4	5	4	6	**168**
グループメンバ変更申請	37	6	4	6	8	3	2	6	6	5	3	4	**90**
メール承認者変更申請	2	5	1	-	2	-	-	1	1	-	1	-	**13**
組織メールアカウント登録/廃止申請	-	2	-	-	-	-	-	-	-	1	-	2	**5**
端末接続申請	7	-	2	2	3	5	2	1	4	6	2	5	**39**
パスワード変更申請	15	6	-	-	1	2	1	-	1	-	1	1	**28**
外字申請	-	-	-	-	-	-	-	-	-	-	-	1	**1**
システム担当者変更申請	5	-	-	-	-	-	-	-	-	-	-	1	**6**
プロキシ例外設定申請	-	-	-	-	-	-	-	-	-	-	-	-	**0**
その他	1	-	2	1	1	-	-	-	-	-	-	1	**6**

(3) セキュリティオペレーションセンター（SOC）業務

(ア) セキュリティアナリストは 24 時間常駐し対応可能であること。

(イ) 24 時間 365 日で日本語でのメール・電話での問い合わせが可能なこと。

(ウ) インシデントと想定される事象特定した場合は、速やかに通知が可能なこと。

(エ) 対象製品から送信されたログ、データ、不審イベントを監視し脅威インテリジェンス、攻撃手法等と関連付けてインシデントと想定される事象の特定が可能なこと。

(4) AI チャットボット

・24 時間 365 日教職員の問い合わせに対応すること。

7.3 ネットワーク機器運用管理業務

(1) システムを構成するネットワーク機器のコンフィグ等の設定情報を管理すること。

(2) ネットワーク機器のコンフィグ等の設定情報を管理し、ネットワーク機器の障害時は、即座に交換機器への設定ができるようにしておくこと。

(3) ネットワーク機器のログを管理すること。

(4) ネットワーク機器の障害時には、即座に交換機器への設定を行うこと。

(5) ネットワーク機器の認証 Id およびパスワードを管理すること。

(6) ネットワーク機器の死活監視を実施すること。ネットワークの監視項目は以下とすること。

(ア) 死活監視

(イ) トラフィック監視

(ウ) アラート通知メールを受信できること。特に緊急度の高いアラートについては２４時間３６５日の体制を用意して受信すること。

7.4 通信回線管理

学校の通信回線について回線側に障害が生じている場合は、回線事業者に連絡して復旧依頼を行うこととする。

7.5 システム運用管理業務

(1) アカウント運用管理

(ア) ユーザーカウント、グループアカウント、ライセンス管理

(イ) 日々の新規アカウント作成、アカウント削除

(2) 端末管理

(ア) ユーザー登録・削除を実施すること

(イ) デバイスグループ管理

(ウ) Autopilot 管理
(エ) コンプライアンスポリシー管理
(オ) アプリケーション配布・設定管理
(カ) 端末への証明書配布
(キ) プロファイル管理

(3) ストレージ管理
(ア) 各システムにおける使用状況の管理を行うこと
(イ) クォータ管理を行うこと
(ウ) 空き容量が不足し、利用に影響が出る場合は、県教育庁に報告して必要な対応を行うこと。

(4) アクセス権管理
各システムのアクセス権の追加・変更・削除等の管理を行うこと

(5) 年次作業
(ア) 人事異動、組織変更に伴うアカウント作成・削除
(イ) ファイルサーバーのアクセス権の追加、変更、削除の管理を行うこと。
(ウ) MDM 管理を行うこと

(6) 学校ホームページコンテンツ
(ア) 各学校およびその他利用期間ごとにアカウントを発行すること。またアカウントおよびドメインを管理すること。
(イ) 各学校に割り当てた容量の管理を行い、各学校におけるホームページ運用に影響が生じると判断した場合に、速やかに県教育庁に報告すること。
(ウ) OS の不具合を含めて保守対応を行うこと。
(エ) SSL 証明書の管理・更新を行うこと。
(オ) 合格発表等のイベントへの対応支援を行うこと。

(7) 教職員向けポータルサイト
(ア) 県教育庁からのポータルサイトのメニュー追加や登録、更新、削除などに対して柔軟に対応すること。また、関係者各位と連携をとり情報共有を図ること。

(8) SWG
(ア) URL フィルタリング機能の設定および例外設定の管理を行うこと。
(イ) 学校から設定変更依頼があった場合は、県教育庁の承認を得た上で設定変更作業を行うこと。

(9) バックアップ管理
(ア) 対象システムのバックアップを行うこと。
(イ) バックアップの間隔および世代管理に関して、県教育庁と協議の上決めること。

7.5　報告

(1) 稼働状況報告

ネットワークと校務支援システムの稼働状況について、3 か月に 1 度レポートを提出し、報告を行う事。

(2) セキュリティ検知状況報告

3 か月に 1 度レポートを提出し、報告を行う事。

ただし、提出を要しない月についても緊急セキュリティ通報等の特段の状況があった場合はレポートを提出し、報告を行う事。

(3) 緊急セキュリティ通報

インシデントの発生などがあった場合は、即座に教育政策課まで知らせること。

その際に必要であればレポートの提出と報告を命じる。

8. 活用支援要件

8.1 対象

対象は県立学校等および校務支援参加校とする。

8.2 研修

教職員向けにシステムの利用および校務支援システムの研修を行う事。
また、過去の研修をアーカイブとして利用できること。
研修実施回数については 2/年程度とすること。
（参加人数は各最大で 3050 人程度）

8.3 活用支援

システムを活用するための支援を実施すること。
必要に応じて、現地訪問を視野に入れた研修を行う事。
研修を実施した場合は、アーカイブとして利用できるようにする事。

9.　障害検知時の復旧対応

9.1　障害監視システム運用

ネットワーク機器およびサーバー機器等については、死活監視や性能監視を実施すること。監視対象機器監視項目は以下とする。

(1) 死活監視
(2) プロセス・サービス監視
(3) ジョブ監視
(4) トラフィック監視
(5) サーバー機器の負荷監視（CPU・メモリ等）
(6) サーバー機器のエラー等のアラートなどのログ監視

9.2　障害時の復旧対応

(1) 障害発生時には、システムの緊急停止、ログの取得および保全等の初期対応を適切に行うこと。緊急停止する際には県教育庁へ報告すること。
(2) 本調達において導入する機器の障害発生時における原因切り分け、障害復旧作業については、現地駆け付けを含め本業務の受託者が実施すること。
(3) 障害の原因切り分けのために学校での現地確認が必要な場合は、学校と調整を実施して現地へ駆けつけを実施すること。
(4) システムの障害を検知した場合には、県教育庁が指定するシステム管理者に対してメール等で通知が届くなど、迅速に対応できる仕組みを構築できること。
(5) 障害が発生した場合は、障害対応記録を県教育庁が指定するシステム管理者へ報告し、障害内容に応じて、事後対策を実施すること。また、サービス復旧時間については、「2.10　SLA 要件」を参照すること。
(6) 必要に応じて、バックアップからリストアを行うこと。