次期県立学校ネットワークシステム

調達仕様書(案)

目次

1. 業務名　次期県立学校ネットワークシステム環境整備業務

2. 業務概要

2.1　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、試験、移行・切替、研修の各業務が対象となる。スケジュールは「2.2 スケジュール」を確認すること。

【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環境において、運用管理（運用統制・連絡調整)、保守・運用受付（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。

2.2　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。

(1) 設計・構築・移行期間

契約締結日から令和 8 年 9 月 30 日まで

(2) 総合運用管理業務

令和 8 年 10 月 1 日から令和 13 年 9 月 30 日まで

設計・構築・移行期間	契約締結日 ～ 令和 8 年 9 月 30 日
総合運用開始日（本稼働）	令和 8 年 10 月 1 日
運用保守期間	令和 8 年 10 月 1 日 ～令和 13 年 9 月 30 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とする。

スケジュール（予定）

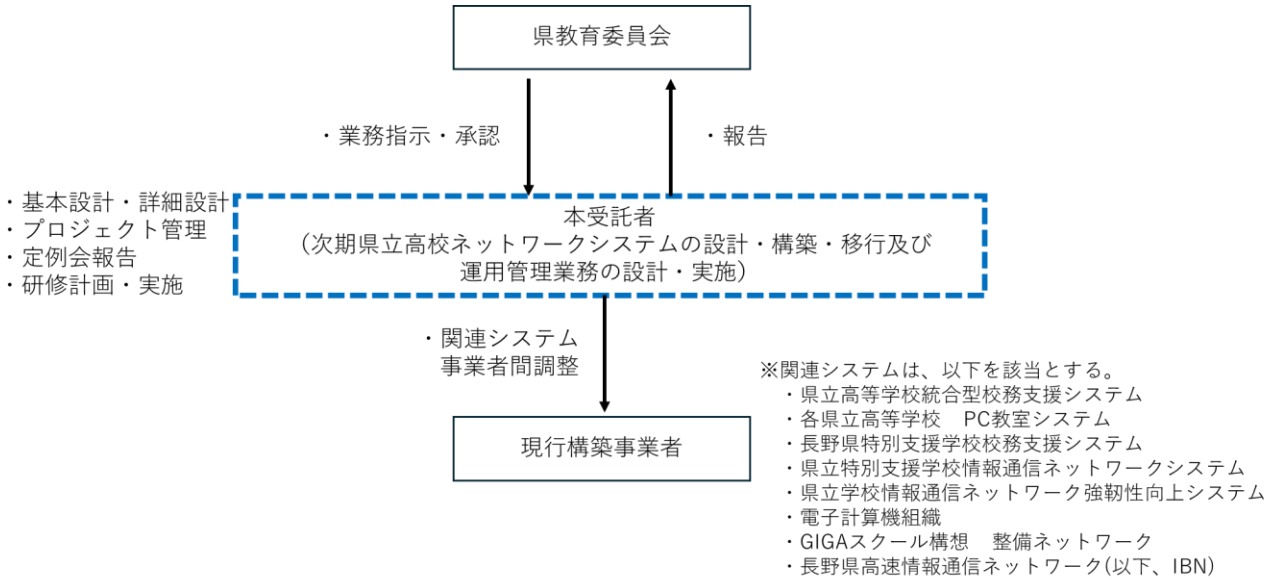
	令和７年５月	６月	７月	８月
公告	★公告	★参加申込提出		
企画提案書			★企画提案書提出期限 ★プレゼン審査	
契約			★事業者決定	★契約

3. 業務委託内容

3.1 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】



県教育委員会は、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。

また、本業務の関連システムである県立高等学校統合型校務支援システム、各県立高等学校　PC 教室システム、県立特別支援学校情報通信ネットワークシステム、長野県特別支援学校校務支援システム、県立学校情報通信ネットワーク強靭性向上システム、電子計算機組織、長野県高速情報通信ネットワーク(以下、IBN)を構築している現行事業者と、システム利用に影響が生じないよう、綿密に事業者間で調整を実施すること。

3.2　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委員会に提出すること。

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県教育委員会の事前レビューを実施し、県教育委員会と協議の上決定すること。

(ア)全体システム構成

(イ)全体スケジュール（構築・移行）

(ウ)体制図

(エ)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）

(オ)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システムを十分に把握した上で実施し、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、クラウド側やサーバ処理を原則とし、クライアント側での処理を過大なものとしないこと。

(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教育委員会に提出すること。

具体的な記載内容には、県教育委員会で事前にレビューを実施し、県教育委員会と協議の上決定すること。

3.3　移行・切替業務

(1)　ネットワーク移行

「7.1 ネットワーク移行計画」に基づき、「移行計画書」を作成し、県教育委員会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、学校向け説明会などにより、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

「7.1 ネットワーク移行計画」に基づき、現行の教員ネットワークに保存されているデータを移行すること

3.4　周辺環境の調達支援・設計・設定指示業務

(1)　本業務の実施にあたり、既存システムへの影響範囲について事前に調査を行い、必要に応じて既存システム業者への設定変更の指示を行うこと。なお、設定変更に係る作業は、現行構築業者と十分に連携を図りながら実施すること。

3.5　　運用管理業務

(1)　運用設計

「8.運用管理要件」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、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、県教育委員会および「3.1 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。

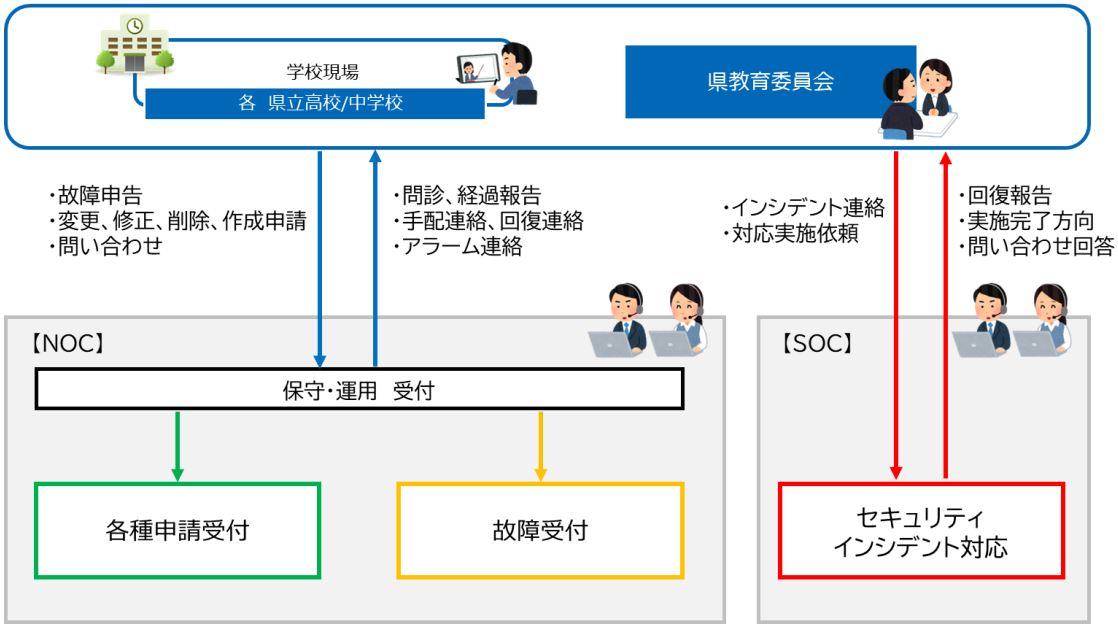
(2)　保守設計

「8.運用管理要件」および「9.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設定変更、障害対応等の管理を行うこと。

主な業務内容は、保守・運用受付（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「3.1 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。

保守・運用においては、円滑にシステム利用が行われるよう学校向けの説明や研修などを実施すること。



3.6　SLA 要件

(1) 県教育委員会と協議の上、サービスレベルを作成すること。

(2) サービスレベルは保守運用手引書にて定義すること。

(3) SLA の更新は、県教育委員会と協議の上、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	平日の 9:00～17:00 の時間帯においては、機能障害の通知受付後２時間以内に復旧のための作業を開始することができる体制を整え、遅くとも翌営業日までに復旧すること。
稼働率および稼働時間	稼働率は 99.9%を目標とすること。 稼働時間は 原則として 365 日 24 時間稼働とする。
大規模災害時	大規模災害時はこの限りではない。県教育委員会と協議の上、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、対策について県教育委員会へ報告すること。

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。

3.7　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、県教育委員会の指示に従い撤去、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委員会に報告すること。なお、これらに係る費用は受託者の負担とする。

3.8　体制要件

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。

3.9　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。

3.10　納品物

本業務の工程毎の納品物を以下に示す。

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、県教育委員会が定める期限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、県教育委員会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. プロジェクト計画書	1 部	・プロジェクト計画書	契約締結後２週間以内
3. プロジェクト管理に係る図書	1 部	・課題管理表 ・議事録/打ち合わせ資料	随時
4. 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
5. 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	
6. 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	構築完了時まで

【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	運用開始時期まで
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	四半期ごと
4. セキュリティ検知状況報告	1 部	・セキュリティ検知の有無および有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	四半期ごと
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

4. 前提条件

4.1　サイジングのための要件

対象拠点は、県立高校・中学８３校(８５拠点)、データセンター、IBN センター、総合教育センター、長野県教育委員会事務局を対象とする。対象校は、別紙１を参照

また、本業務の生徒数および教員数について、下記のとおりとする。なお、セキュリティ対策端末台数は、別紙２を参照

なお、県立高等学校の再編について考慮すること（小諸高校と小諸商業高校が統合し、令和８年度に新校が開校予定であることから、施工にあたっては、県と協議の上、本調達が新校開校の妨げにならないよう考慮すること)。

令和９年度下期以降、県立特別支援学校（18 校、教員数約 1,800 人）等が追加で、本NWを利用する可能性があるため、県立特別支援学校等が利用することが可能な拡張性を有していること。

【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
県立学校	高等学校 （分校含む）	83 校 (85 拠点)	約 42,000 人	4,700 人
	その他教育機関	1 拠点	－	上記に含む
	小計	86 拠点	約 42,000 人	4,700 人
合計		86 拠点	約 42,000 人	4,700 人

4.2 提供するサービスに関する要件

本業務にて運用保守を行う対象となるクラウドサービスおよびデータセンターに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

※本ライセンスにて校務用端末および生徒用端末、PC 教室端末、図書館端末への 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）　デバイス管理機能

（５） 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
（６） セキュア WEB ゲートウェイのライセンス
（７） 教員用端末の端末セキュリティ対策(Endpoint Protection Platform)
（８） 学習用端末（各校 PC 教室）セキュリティ対策の提供
（９） GIGA スクール端末の Web フィルタリング機能の提供
（１０）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
（１１）サーバー用ウィルス管理
（１２）DNS サービス
（１３）統合監視・ログ管理サービス
（１４）図書館システム

4.3 ネットワークに係る要件

4.3.1 WAN 回線に係る要件

本業務では、既存の閉域網回線(IBN)、SINET を経由したインターネット接続および GIGA ネットワーク用インターネット回線を利用して、クラウドサービスおよびデータセンターに接続を行うこと。

4.3.2 校内 LAN に係る要件

本業務では、これまで教員ネットワーク、教育ネットワーク、GIGA ネットワークに分割されていたネットワークを、教員ネットワーク、GIGA ネットワークに統合を行うこと。

本項の詳細については、「6.10 インターネット接続サービス」に示す。

4.3.3 データセンター(ハウジング)に係る要件

本業務では、セキュリティ、構築後の拡張性、災害等発生時等の可用性を考慮したうえで、データセンターにサーバー等センター機器を設置し、システムを構築すること。

データセンターと IBN センター間は１Gbps 以上で接続することとし、その費用は本事業に含めること。

また、構築期間と運用期間（５年間）の利用料を本事業に含めること。

4.4　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、「長野県教育情報セキュリティポリシー」や、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発生しないよう、設計、構築すること。

セキュリティ対策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うこと。

教育ネットワーク ICT 環境において導入するクラウドサービスおよびデータセンターにて提供するサービスについては、一般的なクラウド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」に対応し、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。

その際に多要素の認証を行うこと。

(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)　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

(ア) 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。

（イ）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。

(7)　クラウドサービスの運用管理

サービスの一時停止等、クラウド利用者に影響がある場合、情報提供を行うこと。

(8)　クラウド事業者従業員の人的セキュリティ対策

（ア）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ィポリシーおよび保守運用管理規程等を遵守すること。

（イ）IDおよびパスワードその他の個人認証に必要な情報及び媒体について、適切に管理すること。

(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。 また、アカウント情報が不用意に残置されないようにすること。

(10)　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

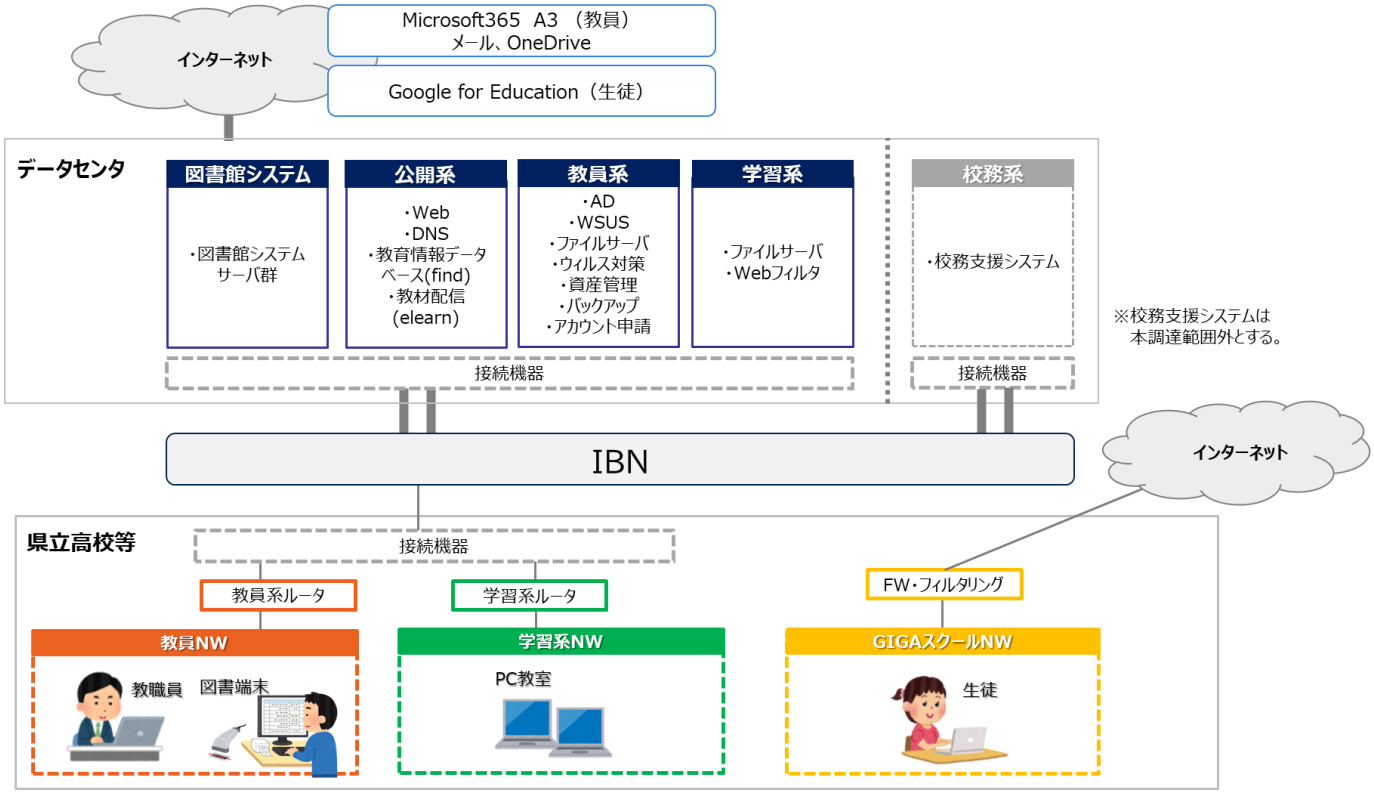
校務系 ICT 環境において導入するクラウドサービスが複数ある場合、受託者はそれぞれのクラウドサービスおよび事業者が上記要件を満たしていることを、担保すること。

5. 全体基本設計

5.1 現行ネットワーク環境

5.1.1 現行構成

現行の県立高等学校情報通信ネットワーク全体構成図を、以下に示す。



現行の県立高等学校情報通信ネットワークは、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。

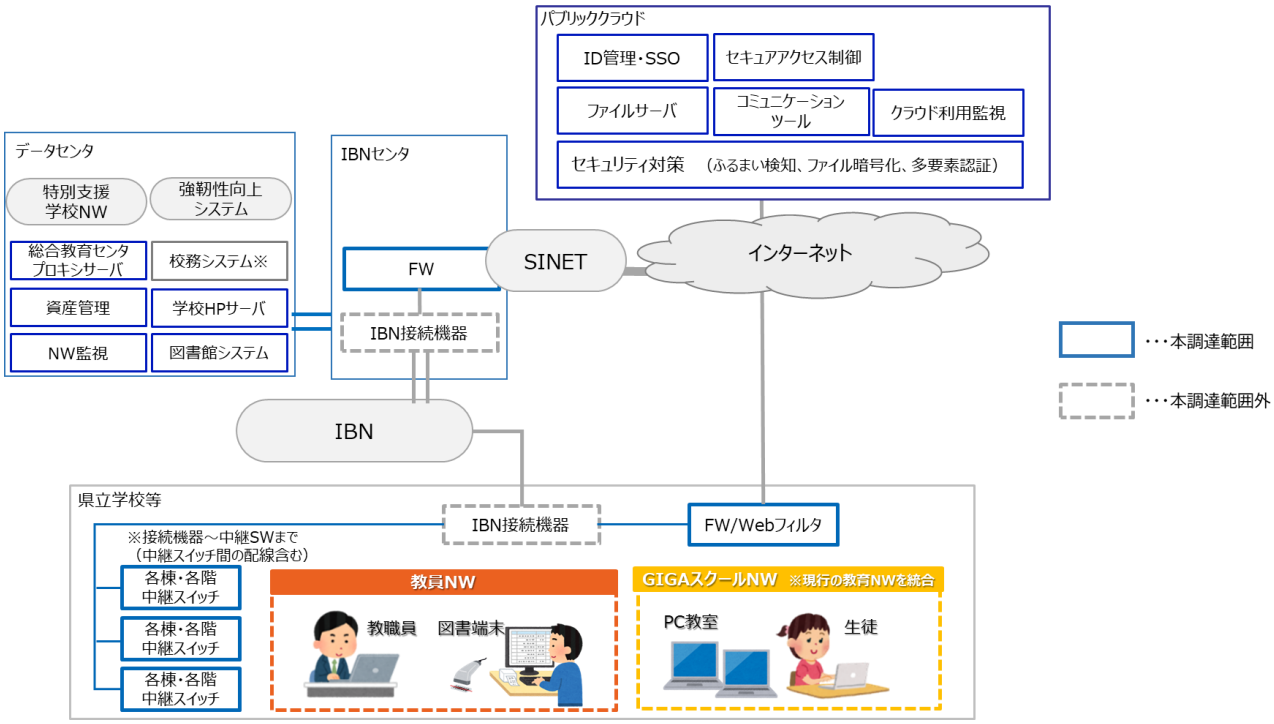
分類	概要
データセンター	教員ネットワーク、教育ネットワークに係るサーバー、ネットワーク機器で構成しサービスを提供している
データセンター設置機器	教員ネットワーク、教育ネットワークに係るサーバー、ネットワーク機器で構成しサービスを提供している
ホームページサービス	県立学校、県立特別支援学校、総合教育センターのホームページを作成する機能の提供
回線	県立学校とデータセンターに接続するための閉域網回線、保守ベンダが運用監視に用いる閉域網回線から構成される
県立学校設置機器	データセンターと県立学校間のネットワーク接続制御を行うルータおよびUTMを提供
外部DNSシステム	nagano-c.ed.jpの権威DNSの提供
教育情報データベースシステム（find）	教育情報図書・ビデオ情報のデータベース、および総合教育センターの研修案内を行うための機能を有するシステムの提供
教材配信システム（elearn）	NetCommonsによるe-ラーニングの提供
内部DNSシステム	高等学校・特別支援学校ネットワーク向けの内部キャッシュDNSの提供
クラウドサービス認証システム	ActiveDirectoryとEntraIDとのID連携機能の提供
ADシステム	教員ネットワーク、教育ネットワークのID管理機能の提供
WSUSシステム	教員ネットワーク、教育ネットワーク接続端末へWindowsUpdateコンテンツ提供
ウィルス対策管理システム	教員ネットワーク、教育ネットワーク内端末のウィルス対策管理、定義ファイル配信機能を有するシステムの提供
コンテンツフィルタリングシステム	教員ネットワーク、教育ネットワーク内端末のWebフィルタの提供
ファイルサーバーシステム	教員ネットワーク、教育ネットワークのファイルサーバー提供
資産管理システム	教員ネットワーク、教育ネットワーク内教員端末の資産管理・USBデバイス管理、ファイル暗号化の機能を有するシステムの提供
アカウント情報申請システム	教員ネットワーク、教育ネットワーク内アカウント等の申請、ファイルサーバーフォルダのアクセス権管理の機能を有するシステムの提供
ネットワークマネジメントシステム	県立高等学校情報通信ネットワークシステムの監視機能を有するシステムの提供
バックアップ管理システム	県立高等学校情報通信ネットワークシステム各サーバーのバックアップの管理機能を有するシステムの提供
高校図書館システム	高等学校図書館の蔵書、貸出管理の機能を有するシステムの提供

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。

5.2　教育ネットワーク環境の全体構成イメージと基本要件

5.2.1　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。



※校務支援システムについて、現在データセンターに設置しているが、更改を検討しているため、本調達においても校務支援システムのクラウド移行も見据えた提案とすること。

(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

・学校ホームページ

・図書館システム

（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

ID 管理　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（主に出張先）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

・教員端末および GIGA スクール端末のインターネット接続用ファイアウォール（Web フィルタリング含む）

・スイッチ等のネットワーク機器（実現する構成に応じ最適な機器を導入すること。）

・教員 NW の中継スイッチ（各校の各階を集約するスイッチ）

※各校の主な台数は別紙３を参照

・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）

「5.2.2 （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。

5.2.2 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

(ア)提案する構成に応じ、学校から各サービスに接続できる構成とすること。 原則、各学校に整備された既設回線を活用することとする。各校、長野県高速情報通信 NW（L2 閉域網）の回線 100M×1 本が敷設されている。また、GIGA 用の回線としてベストエフォートの光回線が松本深志高校のみ 3 回線、生徒 400 人以上の学校は２回線、それ以下は１回線敷設されている。

(2) グローバルＩＰアドレスの提供

(ア)総合教育センターの現行システムに対し、必要数、固定グローバル IP アドレスの割り当てを行うこと。

5.2.3 基本要件

県立高等学校情報通信ネットワーク（以下高校ネットワーク）環境全体のネットワーク利用に関わる要件を以下に示す。 なお、以下に記載する県立学校とは長野県立高等学校及び県立中学校とし、県立特別支援学校は含まない。

なお、各機能の個別要件については、「6.個別基本設計」を参照のこと。

(1) 通信要件

（ア）県立学校教員ネットワークで校務用端末を利用する場合

・ 県立学校教員ネットワークで校務用端末を利用する際は、各学校の既設 IBN 回線を利用して、データセンター内の各システム及び関連システム、MS365 や GoogleWorkspace 及び県立学校ホームページ、インターネットに通信できること。

・ 本業務で整備する機能を利用し校務用端末にセキュリティ対策を行うこと。

・ 図書館システムの司書用端末も校務用端末と同様とする。

（イ） 県立学校 GIGA ネットワーク及び校外で校務用端末を利用する場合

・ 県立学校 GIGA ネットワークまたは校外で校務用端末を利用する際は、各学校の GIGA ネットワーク用既設インターネット回線または利用場所におけるインターネット回線を利用して、MS365 やGoogleWorkspace 等クラウドサービス、インターネットに通信できること。

・ 本業務で整備する機能を利用し校務用端末にセキュリティ対策を行うため、通信を行う際には、全ての通信を終端し監視するなどの仕組を用い対策を行うこと。

・ 図書館システムの司書用端末は、GIGA ネットワーク及び校外での利用は行わない。

（ウ）県立学校 GIGA ネットワークで図書館システム貸出用端末を利用する場合

・ 県立学校 GIGA ネットワークで図書館システムの貸出用端末（主に生徒が利用）を利用する際は、各学校の既設 IBN 回線を利用してデータセンター内の図書館システムに通信できること。また、GIGA ネットワーク用既設インターネット回線を利用して、インターネットに通信できること。

・貸出用端末におけるセキュリティ対策は、本業務で整備する GIGA ネットワーク指導者用端末に対するセキュリティ機能と同様に端末ウィルス対策ソフト、GIGA ネットワーク用 Web フィルタリングとする。詳細は個別基本設計の図書館システムを参照のこと。

・貸出用端末は県立学校教員ネットワーク及び校外での利用は行わない。

（エ）県立学校 GIGA ネットワークで指導者用端末及び生徒用端末を利用する場合

・ 県立学校 GIGA ネットワークで指導者用端末及び生徒用端末を利用する際は、各学校の GIGA ネットワーク用既設インターネット回線を利用して、インターネットに通信できること。

・指導者用端末におけるセキュリティ対策は、端末ウィルス対策ソフトとする。生徒用端末については、GIGA ネットワーク用 Web フィルタリングとする。

・生徒用端末については、個々の端末にアプリケーションの追加、設定変更が生じないようにすること。

（オ）長野県総合教育センターで職員端末、研修用端末を利用する場合

・長野県総合教育センター構内で職員端末、研修用端末を利用する際は、既設 IBN 回線を利用して、MS365 や GoogleWorkspace 及び県立学校ホームページ等 SaaS サービス、プロキシ経由でインターネットに通信できること。プロキシサーバーは環境を整備すること。なお、データセンター内の各システム、関連システムには通信しない。

・長野県総合教育センターの職員端末は構内の ActiveDirectory にドメイン参加しているが、当該環境を継続利用する。

・セキュリティ対策は、既存長野県総合教育センター電子計算機組織の機能を利用し、県立高校情報通信ネットワークで提供していたインターネット境界防御（Firewall）は、本業務で整備する機能により引き続き提供すること。

（カ）長野県教育委員会事務局で校務用端末及び管理用端末を利用する場合

・ 長野県教育委員会事務局で校務用端末及び管理用端末を利用する際は、既設 IBN 回線を利用して、データセンター内の各システム及び関連システム、MS365 や GoogleWorkspace、インターネットに通信できること。

・ 本業務で整備する機能を利用し校務用端末及び管理用端末にセキュリティ対策を行うこと。

(2) データ保護要件

具体的には、以下の基本機能を実装すること。

（ア） 校務用端末及び MS365 上（sharepoint、OneDrive）に保存されたファイルは分類（ラベリング)、保護できること。また、その分類の確認も容易にできること。

（イ） 機密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） 機密情報の分類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。

（エ） 新規ファイルは機密情報の分類として作成されることを基本とし、機密情報に分類された情報であっても、承認者の承認を得たうえで、分類変更が可能であること。

5.2.4　高校ネットワークの機能一覧

本業務で整備する高校ネットワーク環境の全機能一覧を以下に記載する。

なお、本一覧に記載する以外にセキュリティ強化及び利便性向上に資する機能の追加提案を妨げるものではない。また、機能の組み合わせにより記載の機能を代替できる場合は、その内容を明示し提案すること。

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	高校ネットワークにおける校務用端末の認証、認可、アクセス制御、レポート及び監視機能を提供する。また、認証情報は本業務で構築する各システム・機能以外にも連携可能なこと。
	2	エンドポイントセキュリティ・EDR	校務用端末に対するエンドポイントセキュリティ対策として、EPP(Endpoint Protection Platform)およびEDR（Endpoint Detection and Response）機能を提供する。
	3	ウィルス対策	校務用端末以外の端末に対し端末のウィルス対策機能を提供する。対象端末は高校GIGAネットワークに接続する指導者用端末、図書館貸出用端末、普通科パソコン教室端末とする。
	4	パッチ・ソフトウェア配信	校務用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。
	5	端末管理・MDM ・資産管理	校務用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。 また外部記憶媒体制御機能を有し、端末毎もしくはグループ毎に許可・禁止する記憶媒体を個別に制御できること。
	6	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。
	7	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 Loss Prevention）機能を提供する。
	8	アカウント申請システム	高校ネットワークにおけるアカウント情報の申請・承認機能及び認証基盤へのアカウント登録機能を提供する。
ネットワークサービス	9	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。
	10	IPS	校務用端末とインターネット間の通信を監視し、不正な通信の遮断を行うセキュリティ機能を提供する。
	11	DNS	校務用端末に対し高校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内部DNS機能と、高校ホームページ等の長野県教育委員会が保有するドメインの権威DNSとして外部DNS機能を提供する。
	12	統合監視（NMS）	高校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。
	13	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。 なお、生徒向けのフィルタリングは端末にアプリのインストールや個別の設定が不要であることが望ましい。

	14	インターネットファイアウォール	データセンター内に設置し、既設インターネット回線と高校ネットワーク間のルーティング、通信フィルタリング、アクセスログの記録等のファイアウォール機能を提供する。
業務サービス	15	メール	現在利用している教職員の個人メール、学校代表メール等の機関メールの機能を継続して提供する。
	16	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。
	17	教員向けポータル Web サイト	教員への周知情報や情報へのリンク等、高校ネットワークを利用する教員間での情報共有機能を有するポータル Web サイトを提供する。 なお、本業務では全学校共通のポータルサイトを構築し、情報の更新等の運用は業務に含まない。また、学校単位等の利用者を限定したポータルサイトの構築、運用についても含まないものとする。
	18	ホームページ	既存の県立学校（特別支援学校を含む）及び総合教育センターのホームページ、長野県視聴覚ライブラリーを高校ネットワークの内部及び外部に対して公開する機能を提供する。既存コンテンツを移行し、更新のためのアクセス制限ができる機能を有すること。また、SSL 証明書による暗号化通信に対応すること。
	19	教育情報データベース	長野県総合教育センターがインターネットに公開している教育・図書・視聴覚データベースシステムを継続して提供する。SSL 証明書による暗号化通信に対応すること。
学校設置機器	20	学校設置ファイアウォール	学校の既存回線（IBN、GIGA ネットワーク用インターネット回線）に接続し、回線を利用した通信機能を提供する。また、ルーティング、ファイアウォール、ポートフィルタリング機能、DHCP サーバー等を提供する

	21	校内 LAN	学校内に設置されている中継スイッチハブについて、ネットワークの整理統合、機器更新をおこなう。中継スイッチハブ間の配線も Cat6A にて新規に敷設すること。なお中継スイッチハブ間の光配線は既設利用可能とするが光トランシーバは更新すること。ループ検出・通知機能を有すること。またループ検出機能は該当ポートを自動的に閉塞し、校内ネットワーク全体に影響が波及しない機能を有すること。なお、GIGA ネットワークを構成する、無線アクセスポイント及び PoE スイッチは更新の対象外とするが、継続して利用できるよう接続すること。また、現在教育ネットワークに接続しているパソコン教室を GIGA ネットワークに接続するために必要となる環境を提供すること。 その他、中継スイッチは以下の要件を満たすこと ・10/100/1000Base-T を 28 ポート以上有すること ・SFP コンボスロットを 4 スロット以上 ・スイッチングファブリックが 56Gbps 以上 ・ファンレスであること ・動作温度範囲が-5℃～50℃以上であること ・19 インチラックマウントに搭載可能であること ・寸法 440（W）×140（D）×44（H）mm 以下 ・トラフィックセグメンテーション機能を有すること ・イベントログ機能を有しており、最大 60 日間のログが保存できること ・タグ VLAN/ポートベース VLAN に対応していること

6. 個別要件

6.1　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用端末（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 等に対応したクラウド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。

6.1.1　機能要件

(1) 教員ネットワークにおける教職員のアカウント情報および、校務用端末情報の管理を行うことができること。

(2) 教員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。
(7) IP や過去の行動履歴などをもとに、疑わしいと判断されたログインやユーザーが検出された場合に、追加認証の要求やアクセスブロックを自動的に行なう機能を有すること。
(8) 今後、他サービスを導入する際、EntraID と連携した認証が可能な場合は、シングルサインオンによる認証を想定しているため、必要な対応を行うこと。

6.2 EDR

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。

6.2.1 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、通信遮断、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) 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。
(9) 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。
(10) 検索した結果を CSV・Excel 形式ファイルにて出力できること。
(11) 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。
(12) 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。

6.3 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。

6.3.1 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。

6.4 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。

6.4.1 機能要件

(1) 校務用端末(Windows)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) 校務用端末(Windows)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 端末 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) 遠隔で端末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 端末 ごとに異なるポリシーを適用できること。
(8) 遠隔で端末のローカルデータを削除できること。
(9) 校務用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クラウドアクセスを許可する設定ができること。

6.5 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。

6.5.1 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及び随時指定するクラウドサービスに対して、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） 特定の条件においてメールでの通知が可能であること。
（イ） クラウドサービスの利用制限が可能であること。

(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、アクセス権の取り消しができること。

（ウ） ラベルによる重要性分類が示されていない重要情報（要定義）を含む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アクセス権の取り消しができること。

(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、該当サイトとの通信を遮断し、原因となるファイルを隔離またはダウンロードをブロックできること。

(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。

6.6 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。

6.6.1 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) ローカル環境のデバイス内や SharePoint 内の Office ファイル(Word、Excel、PowerPoint)、PDF 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。

6.7 SWG

SWG(Secure Web Gateway)とは、教職員が教員ネットワークからインターネット接続し、クラウドサービス等利用をする際に、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。

6.7.1 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)80 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。

(キ)WEB フィルタリングはクラウド型にすること。

(ク)WEB フィルタリングに障害が発生した際は、サービスが復旧するまでの間あらかじめ設定したサイトへ通信が行えること。

(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) 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 ID、アプリケーション）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) インターネットセキュリティ（DNS セキュリティ）

DNS 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するセキュリティ機能を提供できること。

(6) インターネットセキュリティ（プロキシ）

(ア)Entra ID と連携して Web 閲覧時に SAML 認証ができること。

(イ)HTTPS 通信をオンプレミスのリソースを使用することなくクラウド上のリソースで復号及びセキュリティ検査ができること。

(ウ)個別設定をせずとも、SSE を通過する MS365 宛の通信向けのセキュリティ検査を一括でバイパスする機能を有すること。

(エ)プロキシ(SWG)より固定ＩＰの要件があるインターネットへのアクセス時に、Web 閲覧送信元として契約者専用のユニークなグローバル IP アドレスをクラウド上にて提供できること。提供必要な IP アドレス数については別途協議とする。

(7) インターネットセキュリティ（Firewall）

Firewall ポリシーを一括で管理するためにクラウド型の Firewall 機能を有すること。

(8) インターネットセキュリティ(CASB)

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

(イ)可視化したクラウドアプリケーションのリスク値を確認出来ること。

(ウ)MS365 及び Google Workspace へのアクセスにおいて当組織が契約するテナントへのみアクセス許可し、他組織が契約するテナントへのアクセスについてはブロックできること。
また、契約期間中に新たなサービスの県立学校での利用が決定した場合には、対応できる拡張性を有すること。

6.8　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。

6.8.1　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情報やソフト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、キーワードを指定する際は、空白を挟むことで複数のキーワードおよび数値の範囲を指定して検索が可能であること。

(ウ) 検索条件ごとに表示項目の順序・表示非表示を定義・保存ができ、呼び出せること。

(エ) 検索の際には、本ソフトウェアから削除されたクライアントコンピューターも、検索対象として指定できること。

(オ) BitLocker および他サードパーティ製品により、ハードディスクを暗号化した際に生成される回復キーを収集し、管理できること。収集した BitLocker の回復キー情報は CSV 形式でエクスポートできること。また、これらの暗号化状態をハードウェア一覧で確認でき、暗号化状態が変更された時はドライブログとして記録できること。

(カ) 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。

(キ) クライアントコンピューターがソフトウェアの配布を受ける際、すでに同一のセグ

メント内のクライアントコンピューターに配布されたソフトウェアがキャッシュとして残っていた場合、そのクライアントコンピューター（以下キャッシュ端末と呼ぶ）からソフトウェアを配布できること。

（ク）キャッシュ端末からソフトウェアをダウンロードする際、通信帯域を制限できること。またキャッシュ端末に同時に接続できる端末数を制限し、キャッシュ端末の負荷を抑えられること。４GB 以上のサイズのソフトウェアをキャッシュ配布できること。

（ケ）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。

（コ）セグメント内で最後に電源を切るクライアントコンピューターに対して、セグメント内で電源が入っているプリンターなどネットワーク機器情報をポップアップで通知する機能を有すること。

(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）クライアントコンピューターからサーバー上の共有ファイルや、クライアントコンピューターもしくは組織外のコンピューターから、クライアントコンピューター上に作成された共有フォルダ(ファイルサーバー)へのアクセスおよびファイル操作(作成、コピー、ファイル名変更、移動、上書き、削除)をログとして記録する機能を有すること。また、操作したファイルのフルパスを、フォルダオプション設定を変更することなく、ログとして表示すること。

（ウ）Microsoft 365 / Office Online 上でファイルをローカルに作成した時の、ファイル名やファイルパスをログとして記録する機能を有すること。

（エ）最前面に表示されている Web ブラウザ上で、ユーザーがマウスやキーボードを操作していた時間を集計し記録できること。

（オ）クライアントコンピューター上でアプリケーションソフトウェアから印刷が実行された際に、その印刷されたドキュメント名、１回の印刷枚数、ファイルパスを記録する機能を有すること。

（カ）指定した範囲の IP アドレス以外に対する TCP 通信をログとして記録する機能を有すること。なお、http プロトコル以外の通信を行った場合、およびブラウザ以外のアプリケーションが外部と通信を行ったログも記録すること。

（キ）収集されたファイル操作ログから、一つのファイルに対して、どのような操作（コピー・ファイル名変更、新規作成、削除など）が行われたかを抽出して表示する機能を有すること。また、Microsoft Office 製品については、名前を付けて保存（別ファイル名保存）ログを取得し、表示できること。

（ク）収集したログを一定期間ごとに自動でバックアップする機能を有すること。

（ケ）バックアップされたログについても、リストアすることなくサーバー上に保存されている直近のログと同様に管理コンソール上で検索、閲覧が行えること。

（コ）端末側で保存するログデータは改変されないように難読化されていること。

(3) レポート機能

（ア）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。

（イ）ユーザーや部署ごとの Web ページやアプリケーションを使用した業務時間の把握として、URL やファイルパス、タイトルを指定することで、特定の Web ページやアプリケーションにおいて、ウィンドウの最前面でユーザーがマウスやキーボードを操作していた時間を集計し、ユーザーごとや部署ごとにグラフでレポート出力できること。

（ウ）営業日と業務時間を設定することで、残業時間をユーザー単位で表示名別、部署別、ログイン名別、および端末機単位で端末機名別、コンピューター名別、部署別に、上位からグラフおよび一覧表で表示できること。

(4) 制限・制御・アラート管理

（ア）事前定義されたルールに反した操作が行われた際、その操作を行った利用者のクライアントコンピューターのデスクトップ上にリアルタイムで、ポップアップ形式による通知ができること。

（イ）ルールに反した操作をしたクライアントコンピューターの利用者に注意を促すため、メッセージの内容はルール違反の操作ごとに設定できること。

（ウ）収集したログに基づいて、事前定義されたルールに反した際にその操作ログはアラートログとして、ログ閲覧画面および検索画面にて、アラート項目の優先順位に応じて 3 段階以上に色分けして表示できること。

（エ）各クライアントコンピューターに対して、指定したアプリケーション起動、Windows ストア アプリ起動、指定アプリケーションの名前変更、インストールの実行、Windows システム構成変更、レジストリ変更、Windows ストアの実行、Windows スト

アアプリの自動更新などを禁止できること。

（オ） 起動禁止を除外できる時間設定が、特定のアプリケーションごとに可能である機能を有すること。

（カ） 実行ファイル名が変更された場合も検出できるよう、アプリケーション内部に保存されているハッシュ値やバージョンリソースなどを判定条件として、禁止対照のアプリケーションを指定できること。

（キ） アラート項目ごとにメールでの通知先の設定ができ、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。

（ク） 通知先の設定では、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。

（ケ） クライアントコンピューターに対し管理者権限(Admin 権限)を持つユーザーでのログインを出来ないように抑止する機能を有すること。

（コ） 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) デバイス管理

（ア） USB デバイスをシリアルナンバーごとに管理する機能を有すること。保有 USB デバイスはシステムで台帳管理し、一覧で表示できること。なお、台帳への登録は USB デバイスをクライアントコンピューターもしくは管理者のクライアントコンピューターに挿入した際、利用した USB デバイスのシリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること。

（イ） USB デバイスの一覧を元に、指定した USB デバイスに対して使用許可／不許可および書き込み禁止の、使用制限を設定できること。使用許可／不許可の設定は、ネットワーク全体および指定した部署のみ利用可など柔軟な設定が行えること。

（ウ） 使用制限の設定の際は、ユーザー単位、Active Directory 上のセキュリティグループ単位、クライアントコンピューター単位、およびユーザーとクライアントコンピューターの組み合わせ単位、または、Active Directory 上のセキュリティグループとクライアントコンピューターの組み合わせ単位で設定できること。

（エ） USB メモリがクライアントコンピューターに装着された日時を利用して、所定期間以上使用実績のない USB メモリを、紛失の可能性があると自動判定し、最後の使用者または管理者に対して、USB メモリの所在確認（クライアントコンピューターへの装着）を促す通知を行う機能を有すること。

（オ）USBデバイスが端末に装着された日時とログオンユーザー名とを利用し、USBデバイスを現在所持している可能性が高いユーザーを自動的に特定して表示する機能を有すること。

（カ）USBメモリの最終使用時に、どのようなファイルが保存されていたかを一覧表示（ファイルパス/ファイル作成日時/ファイル更新日時/ファイルサイズ）できること。またUSB管理画面上のファイル一覧から、そのファイルにどのような操作（コピー・ファイル名変更・新規作成・削除など）が行われたかを表示する機能を有すること。

（キ）USBデバイス内ファイルの日時情報を比較し、システム外で作成・編集された外部ファイルの持ち込みを自動判定し、そのUSBデバイスを使用禁止にする機能を有すること。

(6) 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）管理機は、クライアントコンピューター1台もしくは複数台の画面を静止画で同時に確認することができ、その静止画は順次更新できること。

（ウ）管理機から複数のクライアントコンピューターを同時に画面に表示させ、切り替えてリモート操作できること。

（エ）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。

（オ）リモート操作を受けるクライアントコンピューターの画面を、管理者画面で拡大・縮小、全画面表示を行うことができること。

（カ）パスワード入力など、セキュリティの観点からクライアントコンピューターに表示したくない遠隔操作を行う場合は、クライアントコンピューターに対して操作画面を隠しながら遠隔操作を行うことがWindows8以降でも可能であること。操作画面を隠しながらの遠隔操作中は、操作側の画面に隠しながら操作中である旨を通知すること。

（キ）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。

（ク）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。

（ケ）遠隔操作によってクライアントコンピューターのメンテナンスをする際に、遠隔操

作を実行するクライアントコンピューターで行われた操作内容に応じて遠隔操作中の通信量を自動でコントロールする機能を有すること。

（コ）資産管理ソフトがインストールされていない端末は、教育クラウド基盤に接続させないこと。なお、学校外などインターネット環境から接続する場合も、リモート操作やワイプができること。

（サ）特定及び複数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キー及びマウス操作をリモートで行える機能を有すること。操作時はクライアントコンピューターの操作をロックできること。操作する対象となる複数のクライアントコンピューターのウインドウ画面をセンタリング、左上もしくは代表画面にそろえる機能を有すること。また，複数クライアントコンピューターの一斉操作と単体操作を切り替えて利用できること。

6.9　DNS サービス

6.9.1 外部 DNS 機能要件

- Web サービスをインターネットに公開するため外部 DNS サーバーを構築すること。
- Microsoft 社の Office 365 および Google 社の G suite のメールサービスが利用できるよう DNS を設定すること。
- 長野県教育委員会事務局が所有するインターネットドメインの権威 DNS サーバーとして構築し、インターネット及びネットワーク内部からの名前解決に応答すること。
- 現在運用中の外部 DNS サーバーのデータを引き継ぎ、名前解決に支障がでないよう構成をおこなうこと。
- 移行および、維持管理を行い、その際かかる費用を含めること。

6.9.2 内部 DNS 機能要件

- インターネットへは公開しないサービス用に内部 DNS サーバーを構築すること。
- 本ネットワークシステムに接続するパソコン等ネットワーク機器に対し DNS キャッシュサーバーの機能を提供すること。
- プライマリサーバー 1 台と、セカンダリサーバー 1 台以上で構成を行うこと。
- 現在運用中の内部 DNS サーバーのデータを引き継ぎ、名前解決に支障がでないよう構成を行うこと。

6.10　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。

6.10.1　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) GIGA スクール端末の Web フィルタリング機能

（ア）アクセスしようとしている Web サイトをカテゴリーに分類し、カテゴリーごとにアクセスの禁止・許可を制御できること。また、特定のサイトのブロック、許可が可能であること。

（イ）本要件はクラウドサービスでの実現も可とする。

(3)ネットワーク接続機能

(ア)教員 NW については、長野県高速情報通信ネットワーク(IBN)を利用し、データセンター内システムへ接続できるようにすること。

また、SINET を経由したインターネット接続も可能とすること。

(イ)GIGANW については、各学校より直接インターネットへ接続する構成とすること。

6.11　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。

6.11.1 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)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)メールの誤送信を防止するための対策について講じること。その内容については、提案に含めること。

6.12　ファイルストレージ（学校共有ファイルサーバー）

6.12.1 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用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領域に対して、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 以上の領域を確保すること。

6.12.2 非機能要件

当該領域のバックアップを取得すること。バックアップは別領域に保存すること。3ヵ月前までのデータのバックアップを取得しておくこと。

6.13　個人領域ファイルストレージ

6.13.1 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 以上の領域を確保すること。

（オ）別事業で調達する校務用端末のデスクトップのデータおよびマイドキュメントのデータをクラウドサービスと同期ができること。

（カ）利用者の個人ファイルの置き場として構成すること。

（キ）原則、利用者本人だけがアクセスでき、招待することで他利用者に共有できること。共有は編集可能か、閲覧のみかを利用者が設定できること。

（ク）組織外のユーザとはファイル共有できないよう構成すること。

6.13.2 非機能要件

個人領域ストレージについては、1か月前までのデータを復旧できるよう、構築すること。

6.14　学校等ホームページ

各県立高校にて現行利用しているホームページを、継続的に利用ができるように移行を行うこと。また、長野県総合教育センターにて現行利用している教育情報データベースシステム（find)についても、移行を行うこと。なお、ホームページサーバーはクラウドではなくデータセンター内で提供されることを想定している。

6.15　ポータルサイト

6.15.1 システム機能要件

(1) ポータルサイト(SharePoint Online)

（ア）ポータルサイトはWebベースで以下の機能を補修し、リアルタイムで確認できること。

- 教育委員会からのお知らせ（教育委員会から教職員へのお知らせ）
- 掲示板（教職員から他校の教職員への周知事項）
- 在校時間管理
- 電子申請
- 文書管理システム
- ファイルサーバー
- その他

（イ）ポータルサイトは教職員が利用するものであり、生徒に関してはアクセスできないよう構成すること。

（ウ）教育委員会からのお知らせ・掲示板は以下の機能を有すること。

- 教育委員会からのお知らせは、教育委員会のみが投稿することができ、教職員は閲覧権限のみとする。
- 掲示板は教職員が投稿することができ、自分の投稿だけ編集権限を持つこと。

また、新規登録した後でも編集できること。

・お知らせ、掲示板には、件名、本文の他に PDF や Office 文書等のファイルを添付できること。

・お知らせ、掲示板は下書き機能があり、指定した投稿日に合わせて公開できること。

・お知らせ、掲示板は公開期間を指定することができ、公開期間を超えた記事は自動的に非公開となること。

・サイトの容量肥大を防止するため、お知らせや掲示板で一定期間を超えた記事は自動的に削除すること。保持期間は指定できること。

・新着記事は強調表示されること。

（エ）在校時間管理は以下の機能を有すること。

・ポータルサイト上の出退勤ボタンをクリックすることで、教職員ごとに勤務時間が記録されること。

・出退勤ボタンを押し忘れたときには、教職員が実績を追記できること。但し、出退勤ボタンによる打刻は修正できないこと。

・勤務時間（定時）を学校ごとに定義することができ、それを超える勤務時間は残業時間として自動集計されること。

・教職員の残業時間が閾値を超えた場合、承認者に対してアラート通知されること。

・1 ヶ月分の出退勤情報は承認者がいつでも確認することができること。

・出退勤情報は CSV ファイルでエクスポートできること。（週次、月次、年次）

・未記入がある場合には、強調表示されること。

・1 ヶ月分の記録が完了したら、教職員は承認者へ申請を行い、承認者が内容を確認の上、承認処理ができること。

・休憩、休暇申請の機能を有すること。

・有給休暇や休憩時間は、承認者による承認後、合計の残数から差し引いて運用されること。

・休暇の種別を選択できること。

・翌年には、休暇残日数が更新できる機能を有すること。

・県のフレックスタイム制等、発注者と協議し令和８年 10 月時点の勤務制度に合わせてたアプリケーションとすること。

（オ）電子申請（文書管理）は以下の機能を有すること。

・申請フォーマットは単一とし、決裁番号、件名、本文、起案区分、添付ファイル、起案者/承認者が含まれること。

・学校ごとに起案者は主任以上、承認者は校長、教頭、事務長が設定されること。

・決裁番号は自動的に発番されること。

・申請した場合、承認者へメール通知されること。

・承認者が承認・否認した場合、申請者へメール通知されること。

・過去に申請した履歴が学校ごとに閲覧できること。

（カ）ファイルサーバについては以下の機能を有すること。

- 教育委員会と各学校とのファイルのやり取りで一つ、学校毎に一つ、フォルダを用意すること。
- 教職員は所属する学校のフォルダだけアクセスできるよう構成すること。
- 学校毎のフォルダ配下に、校長・教頭・事務局長用のフォルダと一般職員用フォルダの二つを作成すること。その配下は教職員が自由にフォルダを作成できること。
- 校長・教頭・事務局長用のフォルダに一般職員はアクセスできないこと。
- 学校毎に保存できる容量を制限できること。
- 学校担当者に対して、自学校に限定した管理権限を付与できること。
- ファイルサーバに保存された文書に自動的に秘密度ラベルが付与される機能を有すること。
- 組織外のユーザとはファイル共有できないよう構成すること。

（キ）その他

・その他、教職員の働き方改革に資する機能、アプリケーションを複数構築すること。

(2) チャット・チーム・Web 会議

- 生徒と教職員で異なる制御ができること。
- チャット、ファイル共有、Web 会議が一つのツールで提供されること。
- チームの新規作成は申請制とし、承認フローを経て作成されるよう構成すること。
- 学校ごとの教職員チームを作成し、異動・退職の際はアクセス権限設定を動的に行うこと
- チームの機能制限や期限等運用管理は、本県と協議の上、決定すること。
- 1 時間以上の Web 会議を連続して行えること。
- 全教職員が主催者となり Web 会議やライブ配信を開催できること。
- Web 会議内容を録画・録音し、クラウド上又は端末に保存できること。
- 会議参加者にファイルを容易に共有できること。
- 自組織に外部のゲストユーザを招待し、Web 会議上で安全にファイルの共有やコミュニケーションが取れる機能を有すること。
- Web 会議の予定は、スケジュールと連携すること。

6.16　図書館システム

6.16.1 システム機能要件

- 現在利用している高校図書館システムの機能を継承するシステムであること。（現在利用しているシステムソフトウェア：富士通（株）LB@SCHOOL）

・ システムソフトウェアの機能に追加し、(10) その他に記載の機能及び(11)情報交換用 Web ポータルサイト記載の機能を現在利用しているため、継承すること。
・ 書誌データ、所蔵データ、利用者データ、利用統計データ、貸出統計データ、貸出履歴（読書記録）データについて移行をおこなうこと。
・ ソフトウェアにはＴＲＣが提供するＭＡＲＣを利用できること。
・ 学校内において GIGA スクール端末を利用した蔵書検索が行えること。

（１） 全般、共通事項

(ア)地域の学校図書資源の共有化をサポートするシステムであること。
(イ)各学校でのシステム運用負荷を考慮し、プログラムおよび各種データはシステムサーバーで一元管理し、各学校にはサーバーが不必要であること。
(ウ)システムは、先生用と生徒用の２つインターフェースを持ち、先生用機能はＩＤ／パスワードによる利用制限がされていること。
(エ)オペレータ ID／パスワードによるセキュリティー管理ができること。また、オペレータ ID 毎に業務メニューの設定ができること。
(オ)貸出／返却／予約や、利用者登録／検索等、意図的に利用者情報を参照する機能を使用時、自動的にアクセス記録の保存ができること。
(カ)以下のアクセス情報が保存できること。
(アクセス日／時刻、アクセス館／IP アドレス／オペレータ ID、アクセスした業務、アクセスされた利用者番号)
(キ)多言語(UTF-8)を扱えるシステムであること。
(ク)処理選択・コード値選択等がマウスおよびファンクションキーで操作できること。キーボード操作も可能で各入力項目間の移動も TAB キー・矢印キーで可能であること(矢印キーは上下矢印による移動も可能であること)。
(ケ)複数ウィンドウ処理ができること(例：複数業務の起動を行い資料登録途中に入力を中断し、貸出処理を行い、その後中断していた資料登録を継続可能)。
(コ)システムの障害時、機能追加時におけるプログラムの入れ替えはサーバーのみで対応可能でありクライアント毎の入れ替えは不要であること。
(サ)図書館システムは、200 台規模の図書館運用を想定したシステムであること。
(シ)図書館業務メニューから、他関連 Web サイト(県立図書館等)を表示できること。また、Web サイトのリンクは任意に設定できること。
(ス)学校司書向けの「おしらせ・イベント情報」表示ができること。「おしらせ・イベント情報」は任意、かつ、複数の設定、表示が可能であること。

（２） 窓口業務ー先生用_貸出・返却・督促

(ア)利用者コードと資料コードのバーコード走査のみで処理が可能なこと。
(イ)バーコード走査により、「貸出確定」「貸出画面／返却画面切替」ができること。
(ウ)利用者カードを忘れた利用者の場合、貸出画面内で利用者検索し利用者特定～貸出処理が可能なこと。
(エ)利用者に対するコメント（忘れ物、落し物、その他の案内等）通知ができること。
(オ)資料についてのコメント（付録あり、汚れあり等）通知ができること。
(カ)貸出画面上で利用者の現在貸出中・予約中資料一覧を表示できること。(10 件以上／画面)
(キ)貸出延期処理時、貸出統計にカウント する／しない が設定で選択できること。
(ク)その日 1 日の学校毎の貸出冊数、貸出人数の概数を画面に表示できること。
(ケ)貸出画面から紛失処理ができ、督促の対象から外すことができること。

(コ)貸出・返却の作業終了後、画面を切り替えることなく次の貸出･返却の処理を実行できること
(サ)貸出累計回数の管理ができること。また年度毎の貸出回数も確認できること。
(シ)無効(不明・紛失)となっている資料の返却を行うと、設定により、自動的に無効を解除することもできること。
(ス)ネットワーク障害等でサーバへの接続が出来ない場合でも、オフラインで貸出・返却を行えること。
(セ)返却予定日の範囲指定により、未返却者、未返却資料一覧の印刷ができること。

（3）　窓口業務ー利用者管理
(ア)利用者氏名(カナ、日本語、全半角の混在が可能)、利用者コード、クラス、利用者資格、E-mail アドレスからの検索ができること。
(イ)登録利用者の一覧出力では、管理者権限による出力制御ができること。
(ウ)利用者の詳細情報が表示できること。氏名、最終利用日、予約順位、予約待ち順位、貸出資料一覧、予約資料一覧等が確認できること。また、印刷もできること。
(エ)新規利用者の登録、既存利用者の登録情報の修正、登録利用者の削除、利用者カード紛失時等の再交付処理ができること。
(オ)利用者氏名・ヨミを全半角混在で登録できること。
(カ)新規登録時、検索で未登録確認後、登録画面に検索条件を複写できること。
(キ)有効期限や最終利用日等の条件に該当する利用者を抽出し、無効区分、利用者資格区分等の情報を一括で更新できること。
(ク)任意の無効日付、無効区分を指定し、一括してデータ削除できること。あくまで任意処理であり、年度末等に自動で削除されないこと。

（4）　窓口業務ー資料検索・予約
(ア)書名・著者名・出版者・任意定義項目・分類・ISBN・資料コード・内容項目・タグ名等で資料検索できること。書名・著者名・任意定義項目は、全半角混在で検索ができること。
(イ)各種の可変長マークデータから漏れなく検索ができること。(マークデータの全てを検索対象可能とする)
(ウ)自校で修正・入力した書誌データと各マークデータをまとめて検索できること。
(エ)AND、OR、NOT を使用し、項目間の複合高速検索ができること。
(オ)項目により、前方一致、完全一致および中間一致(分かち項目)、後方一致で認識し、検索ができること。
(カ)うろ覚えのキーワードを過去に登録された文字の中から探し出し、入力する手助けができること。
(キ)検索結果は、利用可能／貸出中／貸出不可能／除籍／相互貸借資料／未所蔵により色を分けて分かりやすく表示できること。
(ク)印刷のほか、CSV ファイルで保存やエクセルファイルで保存も可能なこと。
(ケ)対象館を全校、自校限定、または、任意に複数校指定して検索でき、検索結果も、本が今、どの学校のどこでどのような状態になっているかを一目瞭然に表示できること。
(コ)ひらがなとカタカナ、全角と半角のどちらで入力しても検索でき、検索結果は変わらないこと。同様に大文字、小文字（例「や」と「ゃ」、「Ａ」と「ａ」等）どちらで入力しても検索できること。さらに、音が同じもの（例「バ」と「ヴァ」、「を」と「お」、「は」と「わ」、「じ」と「ぢ」等）も、どちらで入力しても検索できること。また、規則を任意設定できること。
(サ)検索結果一覧として表示する項目の任意設定ができること。

(シ)検索結果より、その資料が配架地図上のどこにあるのか表示できること。
(ス)国立国会図書館が保有する書誌情報と横断検索が可能なこと
(セ)TRC-TOOLi-S サイトとの横断検索が可能なこと
(ソ)館毎かつ利用者資格毎に予約冊数の設定ができること。
(タ)予約本の現在の状態(予約中、予約棚)の管理ができること。
(チ)任意に予約取消ができること。
(ツ)バーコードの走査だけで、予約確保の取消しが可能なこと。

（５）　生徒画面、校内検索
(ア)生徒用のインターフェースは、グラフィカルでわかりやすいものであること。
(イ)書名・著者名・出版者・任意定義項目・分類・ISBN・資料コード・内容項目等で資料検索できること。書名・著者名・任意定義項目は、全半角混在で検索ができること。
(ウ)ひらがなとカタカナ、全角と半角のどちらで入力しても検索でき、検索結果は変わらないこと。同様に大文字、小文字（例「や」と「ゃ」、「Ａ」と「ａ」等）どちらで入力しても検索できること。さらに、音が同じもの（例「バ」と「ヴァ」、「を」と「お」、「は」と「わ」、「じ」と「ぢ」等）も、どちらで入力しても検索できること。
(エ)検索結果より、その資料が配架地図上のどこにあるのか表示できること。
(オ)詳細画面から予約申込ができること。
(カ)一定時間経過後、自動的にトップ画面に戻れること。
(キ)検索項目を特定せず、検索語のみの入力で検索できること。
(ク)複数の単語を空白区切りで入力し、単語同士の AND 条件で検索できること。
(ケ)検索結果一覧の印刷ができること。
(コ)自校の蔵書の他に本システムで管理された他校の蔵書情報を検索できること。
(サ)設定により、書名、著者名、出版者、任意定義項目、分類、ＩＳＢＮ、資料コード、内容項目等で資料検索することができること。またＡＮＤ、ＯＲ、ＮＯＴを使用し、項目間の複合検索が行えること。
(シ)学校内のネットワークに接続したパソコンから学校図書館の蔵書検索が出来ること。
(ス)Chrome や Safari などのブラウザからの検索に対応できること。
(セ)学校内であれば接続台数に制限がないこと
(ソ)先生・司書用の機能とは別に、生徒自身で貸出・返却・資料検索ができること。
(タ)貸出・返却の作業終了後、画面を切り替えることなく次の貸出･返却の処理を実行できること。
(チ)バーコードリーダの走査により、「貸出確定」「貸出画面／返却画面切替」ができること。
(ツ)利用者情報が表示されている状態で一定時間が過ぎると画面が利用者確定前の画面に戻ること。

（６）　資料管理業務
(ア)各種可変長マークデータは完全に取り込むことができること。(完全可変長項目数対応)
(イ)複本のデータ管理ができること。
(ウ)書名・著者名等にて入力した漢字項目から自動的にヨミ振り分かちができること。
(エ)書名などカナ漢字ペアで管理されている項目に関しては、漢字入力した通りに自動でヨミ振りできること。
(オ)複数行にまたがったデータを漏れなく入力することができること。

(カ)TRC の TOOLi-S とシームレスな連携ができること。
(キ)標準書誌データ以外に学校独自のローカル書誌データの蓄積ができること。
(ク)蔵書データ登録時に各学校独自のデータを入力できること。
(ケ)各種情報を可変長にて登録し、検索できること。
(コ)雑誌の JAN コードを読み取って受入ができること。
(サ)館コードにより学校毎の管理ができること。
(シ)ISBN コードのある本の蔵書登録については、ISBN コードと既に貼付したバーコードの 2 つを読み取るだけで、書誌データと自動的に連携し所蔵登録できること。
(ス)資料の除籍・復籍処理が連続でできること。
(セ)蔵書点検前処理等の事前処理無しで蔵書点検が開始できること。
(ソ)オンライン、オフラインの両方で蔵書点検ができること。
(タ)蔵書点検の結果、不明資料一覧を印刷できること。
(チ)学校毎に蔵書点検ができること。
(ツ)図書室を開館しながら蔵書点検を実施できる機能を有すること

（7）　相互貸借
(ア)利用者からのリクエストに応じて、他校への相互貸借資料の借受依頼ができること。
※【前提条件】資料コードの重複が無いこと
(イ)どこの学校からどの資料を借りているか画面で表示可能であること。また、借受校へ返却済か等の状態も表示可能であること。
(ウ)各学校の業務端末から、他の学校へ相互貸借のためのリクエストを行うことができること。
(エ)相互貸借のリクエストが自校に来ている場合、業務端末の起動時にメッセージが表示され知らせる機能があること。
(オ)学校間で相互貸借連携機能（依頼・受諾/拒否・貸出・返却）ができること。
(カ)依頼状態はリアルタイムに検索・確認ができること。
(キ)相互貸借で貸し出された本は、貸出校とは別の学校へ、又貸しを行えること。
(ク)他校の所蔵を検索し、相互貸借依頼をかける事ができること。
(ケ)依頼を受けた学校は、許可/保留/拒否の回答とコメントの返信ができること。

（8）　学校図書専用業務
(ア)全学校を対象に、利用者・資料の管理、帳票出力が可能なセンターモードに対応できること。
(イ)学校毎にクラス単位での進級/卒業処理が一括で行えること。
(ウ)クラス更新後、クラス毎に出席番号を設定できること。
(エ)CSV 形式のデータの取り込みによる利用者データの一括登録ができること。
(オ)利用者データを CSV 形式に出力できること。
(カ)卒業生に資料の貸出中利用者がいる場合は、その利用者は削除出来ないようになっていること。

（9）　帳票
(ア)統計資料は Excel と連係し画面で確認でき、必要に応じてプリンタに印刷指示できること。また、Excel で 2 次加工(グラフ作成等)や保存することができること。
(イ)利用者・所蔵情報等、任意の条件によって抽出する機能があり、結果が CSV 形式など加工可能なデータとして保存・印刷ができること。CSV ファイルは項目見出しつきで出力されること。
(ウ)帳票印刷形式に成形された Excel データとして出力できること。

No	帳票一覧
1	新着資料一覧表
2	無効資料一覧表
3	未利用資料一覧表
4	図書原簿
5	所蔵一覧
6	図書一覧
7	雑誌タイトル一覧表
8	貸出資料一覧表
9	督促状
10	返却督促一覧
11	予約図書連絡票
12	予約資料一覧表
13	予約在架資料一覧表
14	予約解除資料一覧表
15	利用者資格別資料区分別利用統計
16	統計分類別所属別貸出統計
17	統計分類別利用者資格別利用統計
18	統計分類別貸出実績表
19	クラス・資料区分別貸出統計
20	クラス・統計分類別貸出統計
21	統計分類別貸出統計
22	学年・クラス別貸出日報
23	学年・クラス別貸出月報
24	学年・クラス別貸出年報
25	多読者一覧表
26	利用者毎貸出実績

27	資料毎貸出実績
28	個人読書傾向表
29	日別利用統計
30	月別利用統計
31	学校別貸出統計
32	ベストリーダ
33	ベストリクエスト
34	分類別蔵書統計表
35	分類別蔵書統計表(ﾘｱﾙﾀｲﾑ)
36	所蔵場所別統計分類別蔵書集計表
37	予算区分別資料区分別蔵書統計
38	蔵書総括表
39	表彰状
40	相互貸借実績統計表
41	三段背ラベル（キハラ）
42	一段背ラベル（埼玉福祉会）
43	利用者カード
44	利用者カードクラス別
45	利用者／資料コード
46	利用者台帳
47	エラーリスト／不明一覧
48	相互貸借貸出表

（１０）　その他

(ア) システムの機能アップ等のモジュール提供や連絡は適時提供を行うこと。

(イ) なお、バージョンアップに関しては、媒体ではなく、ネットワーク経由にて、全ての学校にてタイムラグなく行なえること。

(ウ)検索画面で請求記号の表示ができること。

(エ)所蔵データに対して、費目コード、支払日（予算執行日)、登録番号の入力が可能なこと。

(オ)資料コードをコクヨ「ＬＢＰ－Ａ６９６　ＬＢＰ用ラベルシート」にバーコード印

刷ができること。又、資料コードの指定方法は個別指定及び範囲指定ができること。
(カ)資料コードを指定することにより当該図書の埼玉福祉会仕様の図書背ラベル印刷ができること。又、資料コードの指定方法は個別指定及び範囲指定ができること。
(キ)利用者コードをコクヨ「ＬＢＰ－Ａ６９６　ＬＢＰ用ラベルシート」にバーコード印刷ができること。又、利用者コードの指定方法は個別指定及び範囲指定ができること。
(ク)随時、資料データをテキスト形式に抽出ができること。

(ケ)長野県様式に準じた、物品購入内訳書が作成できること。また、支払履歴は本単位に図書館システムにて確認ができること。
(コ)貸出統計に関しては、明細をテキスト出力ができること。
(サ)長野県高等学校図書館協議会システム委員会（以下 SLA システム委員会）の仕様に基づく、入力補助リストの印刷が可能なこと。
(シ)SLA システム委員会の仕様に基づく、督促状の印刷が可能なこと。
(ス)図書館にて作成した典拠語及び類似語データを図書館システムに反映させる事ができること。なお、典拠語及び類似語データは EXCEL にて簡易的に作成したデータとする。
(セ)所蔵情報に関しては、随時業務にて、特定の条件にて一括更新をおこなうことができること。

（１１）　情報交換等 Web ポータルサイト
(ア)図書館司書同士の情報交換の為の掲示板及び SLA システム委員会からの情報発信のための Web ポータルサイトを提供すること。なお、現存の Web ポータルサイト上のデータは、新 Web ポータルサイト上へも移行を行う事。
(イ)Web ポータルサイトを起点として、各種機能が利用できること。また、Web ポータルサイトからシングルサインオンで図書館システムが起動できること。
(ウ)Web ポータルサイトのトップ画面では、各機能の未読情報がひと目で確認できるように表示されること。
(エ)掲示に対する回答コメント等の情報交換は、リアルタイムで表示・反映されること。
(オ)回覧された内容に対する回答については複数の選択肢を用意することができ、選択肢毎の集計が得られること。

6.16.2 クライアント機能要件

（１）　システム構築要件
(ア)図書館用クライアントパソコンとしてノートパソコン１台、デスクトップパソコン（19.5 インチ以上の液晶ディスプレイを含む）１台を高校図書館システム導入対象校に設置すること。
(イ)屋代附属中学校、及び諏訪清陵附属中学校に対し、デスクトップパソコン（19.5 インチ以上の液晶ディスプレイを含む）1 台を設置すること。
(ウ)ノートパソコンは司書が利用するため各学校の教員ネットワーク、デスクトップパソコンは生徒が主に利用するため GIGA スクールネットワークに接続する。それぞれのパソコンが図書館システムを利用できるよう、校内ネットワークの調整を行うこと。
(エ)ノートパソコンは学校教員が利用する校務用端末と同一の設定とし、その上で図書館システムを利用するための設定等を行うこと。
(オ)図書館用クライアントパソコンの周辺装置として、各パソコンにバーコードリーダ１基、導入対象校毎にプリンター１台とクライアント用 SW-HUB（教員ネットワーク

接続用）　１台を設置する。

(カ)プリンターは教員ネットワークに接続することを基本とするが、学校の要望により GIGA スクールネットワークに接続した図書館用クライアントパソコンから印刷可能となるよう USB ケーブルの接続及び設定を行うこと。なお、パソコンとプリンターの距離が、2m以上となるような環境の場合は別途協議とする。

7.　構築および移行要件

7.1 機能要件

(1) 全ての県立学校の既存保守事業者と連携し県教育委員会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) システム移行にあたり、スケジュール、影響範囲、移行手順等を記載した移行計画書を作成し、長野県教育員会事務局の承認を得ること。

(4) 令和 8 年 9 月 30 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。

(5) 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。

(6) 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、県教育委員会の承認を得ること。

(7) 本期間中に、既存の教育ネットワークや教員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教員ネットワークとして利用できるようにすること。原則としてネットワークに接続されている既設パソコンの設定変更が発生する場合は、長野県教育委員会事務局と協議を行い、変更作業が最小限となるよう構成すること。想定される作業は受託事業者の負担により実施すること。

(8) 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 SharePoint へのデータ移行

(イ)学校ホームページコンテンツ

(9) 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、県教育委員会所管の全校共有等）は受託者にて移行すること。

(10)　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。）

(11)　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。

(12)　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協議の上、教職員の役割とすることも可とする。

(13)　図書館システムについて、各学校向けに現行システムとの変更点についての説明会を必要に応じ１回以上実施すること。

(14)　現在、教員用ネットワークと教育用ネットワーク、GIGA 用ネットワークが分離されているが、教員用ネットワークと GIGA 用ネットワークの 2 系統にすること。それに必要な要件定義、設計、構築、移行等の作業を見込むこと

(15)　中継スイッチハブ間のＬＡＮ配線は新規に敷設すること。

(16)　工事や導入にあたり、梱包に用いられていた段ボール等は持ち帰ること。

(17)　リース終了後の撤去費用を含むこと。なお撤去次期については、本ネットワークシステムの次期更新スケジュールに合わせ調整すること。

(18)　機器設置にあたっては、現行機器が稼働しているため、業務停止の影響がないように、現行システム導入業者と調整・連携し行うこと。移行に伴い必要となる、現行システム導入業者の費用も受託者にて見込むこと

(19)　現在、県立高等学校情報通信ネットワークから長野県内部事務システムへの接続には、内部事務接続ゲートウェイ装置を経由している。本調達では機器更新を行わず、県立学校情報通信ネットワーク強靭性向上システム機器により内部事務接続ゲートウェイ装置の機能を実現するため、必要となる設定変更を本調達にて実施すること。必要となる費用は以下に記載する保守運用事業者に見積もりを依頼すること。

県立学校情報通信ネットワーク強靭性向上システム保守運用事業者
東日本電信電話株式会社　長野支店

8.　運用・保守管理要件

(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保守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委員会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。

8.1　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) 県教育委員会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委員会に報告・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。

8.2 運用・保守体制について

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保守業務を実施すること。運用保守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)　運用受付（NOC）業務

（ア）　運用及びその管理は、平日 9 時から 17 時までとすること。
（重大な影響を及ぼす障害が発生した場合、また発生が予見される場合は、当該障害の復旧もしくは対応処置を行うこと。）

（イ）　運用業務として、変更、修正作成申請や問い合わせ対応を行う各種申請受付を実施すること。

(2)　保守受付（NOC）業務

（ア）　納入機器について常に良好に動作するように保守を行うこと。保守のための受付手段を平日 8 時 30 分から 21 時の時間帯を確保すること。

（イ）　平日の 9 時から 17 時の時間帯においては、機能障害の通知受付後 2 時間以内に復旧のための作業を開始することができる体制を整え、遅くとも翌営業日までに対応すること。

（ウ）　NMS により、本ネットワークシステムの正常性を 24 時間監視し、平日 9 時から 17 時に NMS で障害を検知した場合には県教育委員会に通知するとともに、必要な保守作業を開始すること。平日 9 時から 17 時以外の時間帯においては、翌平日に同様の対応を速やかにおこなうこと。

(2)　セキュリティオペレーションセンター（SOC）業務

（ア）　24 時間 365 日での有人対応を実現し、セキュリティアラートの監視を行うこと

（イ）　セキュリティアラート発生時には長野県教育情報セキュリティポリシーに則り報告するとともにログの分析を行い、脅威の有無を判定すること。また、分析の結果、脅威を有すると判断した場合、事前に定義された判定基準をもとに、脅威の重大度を判定すること。

（ウ）日常的な問い合わせ、確認依頼、及びインシデント対応に関連する質問については、SOC が責任をもって受付・回答を行うこと。また、運用状況、アラート発生件数、対応内容、改善提案などを定期的（例：月次、四半期毎）に発注者へ報告し、発注者はその内容を確認できるようにすること。

（エ） セキュリティアラートの分析により重大なセキュリティインシデントと判断された場合、即時に 24 時間 365 日の体制で初動対応を実施する。これには、被害拡大防止措置・初期状況把握・初動報告が含まれる。

（カ） 重大インシデントにおいては、SOC が中心となり、迅速かつ総合的な対応支援を実施すること。

（キ） 重大なセキュリティインシデント発生時、SOC は事前に定めた緊急通知ルールに従い、関係者（発注者および関連部署・外部パートナー等）への迅速な通知を実施すること。通知方法、連絡先、連絡タイムラインは事前に合意された運用マニュアルに基づくこと。

8.3 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

8.4 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。

8.5 システム運用管理業務

(1) アカウント運用管理（随時作業）

（ア） EntarID の管理

（イ） ユーザーカウント、グループアカウント、ライセンス管理を行うこと

（ウ） 日々の新規アカウント作成、アカウント削除を行うこと

(2)ネットワーク運用管理

（ア） IP アドレス管理、ネットワークアドレス体系管理、学校内固定アドレス管理（払出・変更・廃止）を行うこと

（イ） ネットワーク変更対応、ネットワーク機器の設定変更対応を行うこと

(設置対象場所：各学校、IBN センター、データセンター)

（ウ） ネットワーク監視・障害対応を行うこと

(3) サーバー運用管理

（ア） バックアップジョブの監視を行うこと

（イ） 図書館システムの定期ジョブの監視、ソフトウェアセキュリティパッチ対応を行うこと

（ウ） 資産管理システム設定変更を行うこと

(4) プリンタ等管理

（ア） プリンタ等の IP アドレス管理および通信管理を行うこと

(5) 図書館システム管理

（ア） 図書館システムに関する高校からの相談対応を行うこと

（イ） 図書館システムに関する Q&A 及び設定変更対応を行うこと

（ウ） 運用管理上の軽微な図書館システムの改修を行うこと

(6) Microsoft365 管理運用 （教職員及び学生）

（ア） Microsoft 365 割り当て管理を行うこと

(Microsoft 365 A5 ライセンスの付与・回収、ライセンス数のモニタリングと調整)

（イ） グループポリシー・セキュリティ設定管理を行うこと

（ウ） Office アプリケーションの展開と更新を行うこと

(365Apps（Office 及び Teams 等）未展開者への展開も含む)

（エ） 利用者（教職員・学生）からの問い合わせを行うこと

(7) 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、県教育委員会に報告して必要な対応を行うこと

(8) アクセス権管理

（ア） 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

(9) 年次作業 （教職員及び学生）

（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

(10) 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） SSL 証明書の管理・更新を行うこと

(11) 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、県教育委員会の承認を得た上で設定変更作業を行うこと

(12) バックアップ管理

（エ） 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、県教育委員会と協議の上決めること

(13) その他

（ア） 定期人事異動のアカウントユーザ登録対応
（新設・移動・廃止）

（イ） システム定期点検

（ウ） 学校統廃合時のセンターシステム対応

（エ） 県教育委員会事務局からのシステム運用に関する問い合わせ対応

（オ） 運用・監視状況の書面による定期報告

8.6 報告

(1) 稼働状況報告

ネットワークの稼働状況について、3 か月に 1 度レポート を提出し、報告を行うこと。

(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、報告を行うこと。

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、報告を行うこと。

(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、即座に県教育委員会まで知らせること。 その際に必要であればレポートの提出と報告を命じる。

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委員会へ報告すること。
(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、県教育委員会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委員会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、「3.7 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。