群馬県立学校次期ネットワーク環境整備

要件定義書

令和８年８月５日

群馬県教育委員会事務局総務課

目次

第１章 現状 ICT 環境の構成と課題（As-Is）

１-１　現状 ICT 環境の整理

現状のネットワーク構成図を示す。

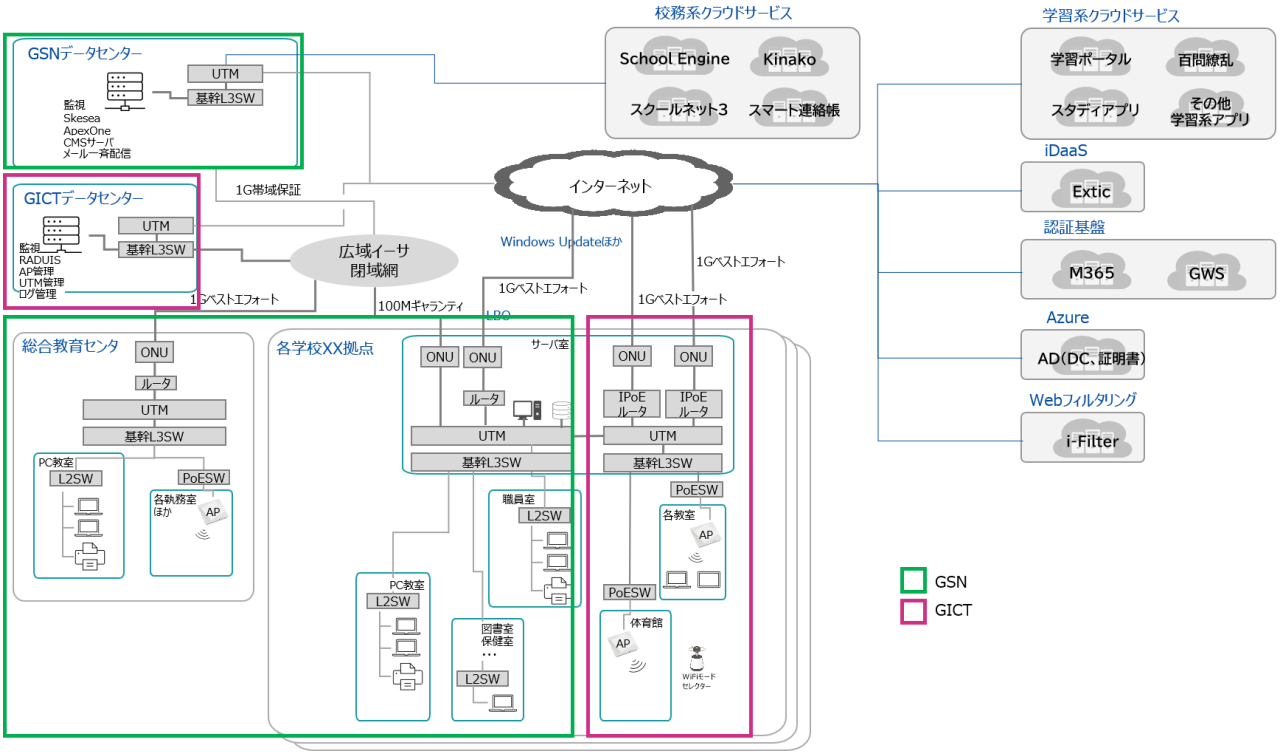


図　1-11　現状ネットワーク構成図

１-１-１ ネットワーク

生徒情報管理システム（校務支援システム）の利用等を目的としたネットワーク GSN（ぐんまスクールネットの略称）及び GIGA スクール構想により整備された GICT（学習系ネットワークの略称）の２系統のネットワークを利用している。なお、各拠点の整備状況は、「別紙 2_学校 NW 機器、LAN 工事一覧」のとおりである。

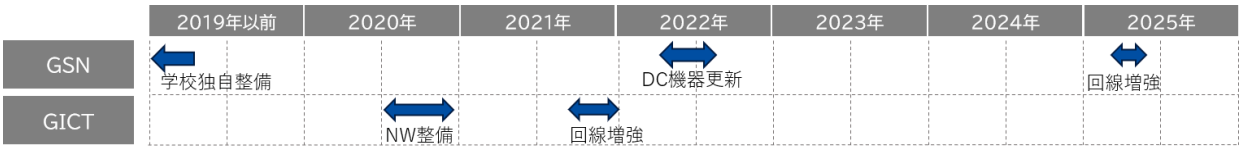


図　1-22　ネットワーク整備年表

(1)GSN

①LAN

平成 12 年頃に整備され、主に職員室、校長室、保健室、事務室、図書室、体育教官室、PC 教室等を対象として有線 LAN 環境が構築された。各学校には L2 スイッチ及び UTM が設置（学校によっては、L3 スイッチも設置）され、校務系セグメント・生徒系セグメントが論理分離されている。校内 LAN は各校毎に修繕を行っているが、データセンターから各校の UTM までは、総合教育センターで運用を行っている。

PC 教室については、児童生徒 1 人 1 台端末の整備により、検定を実施しない普通高校では廃止する

方針となっているが、専門高校等では継続利用を予定している。継続利用する施設については、機器、配線設備の老朽化が進行している状況である。

②WAN

KDDI 広域イーサネット等の閉域網を利用し、各学校とデータセンターを接続するハブ&スポーク型構成である。

インターネット接続はデータセンターに集約されており、特定のクラウドサービス（Microsoft 365 等）への通信のみ 500Mbps の帯域確保回線へ振り分ける等のトラフィック制御を行っている。なお、令和 7 年度、ネットワークボトルネック解消を目的として、各拠点において一部通信においてローカルブレイクアウト（NTT 回線）を使用している。

(2)GICT

①LAN

GIGA スクール構想に基づき、令和 2 年度に全県立学校を対象として一斉整備した学習系ネットワークである。整備にあたっては、各校のサーバ室等を起点として、新たに LAN ケーブルを敷設し、以下の施設に無線 LAN 環境を構築した。

・ 普通教室：全教室に整備済み。
・ 特別教室：約 3 分の 2 の教室に整備済み。
・ 体育館：各校 1 台のアクセスポイント（AP）を整備済み。
・ 職員室：各校の職員室に整備済み。
（ただし、職員室が複数存在する学校では、一部未整備の職員室が存在する。）
・ 会議室：主に第一会議室を対象とし、約 3 分の 1 の学校に整備済み。

なお、アクセスポイントの整備基準は、原則として以下のとおりである。

・ 県立高等学校の普通教室：1 教室につき AP1 台
・ 特別支援学校の普通教室：2 教室につき AP1 台
・ 県立高等学校及び特別支援学校の特別教室：2 教室につき AP1 台

②WAN

各学校から直接インターネットへ接続するローカルブレイクアウト構成を採用している。

回線構成は以下のとおりである。

・ 高等学校：IPoE 方式による 1Gbps（ベストエフォート）のインターネット回線を、学校規模に応じて 1～3 回線導入
・ 特別支援学校：PPPoE 方式による 1Gbps（ベストエフォート）のインターネット回線を導入
また、各学校の学習系ネットワークのインターネット接続ゲートウェイには UTM を設置し、校内 LAN とインターネット間の境界防御を実施している。

1-1-2 データセンター

GSN、GICT それぞれの用途のサーバ群が設置されている。その用途は以下のとおりである。

(1)GSN

表 1-11 GSN データセンター/サーバ群

サーバ	用途
監視（PRTG）	各拠点 UTM の監視及びリモートメンテナンス
IT 資産管理（Skysea）	教職員端末のデバイス管理、アプリ配信
アンチウイルス（ApexOne）	教職員端末のライセンス、定義ファイル配信管理

Web フィルタリング（i-Filter）	GSN 用 Web フィルタリング（オンプレ版）
学校 CMS（NetCommons3）	各学校のホームページ
メール連絡網システム	特別支援学校の保護者向け一斉配信メールサーバ
DNS サーバ	gsn.ed.jp ドメイン

※学校 CMS、メール連絡網システム、DNS サーバは別調達を想定

(2)GICT

表 1-22　GICT データセンター/サーバ群

サーバ	用途
監視（Zabbix）	各拠点 UTM、SW、PoESW、AP の監視及びリモートメンテナンス
RADIUS（ Account@Adapter+ ）	無線 AP ユーザ認証
無線アクセスポイント管理（UNIFAS）	無線アクセスポイント集中管理
UTM 管理（FortiAnalyzer）	UTM 集中管理
ログ管理（Syslog）	ネットワーク機器ログ収集、保管
RedmineSV	問合せ・インシデント管理
コンソール SV	リモートメンテナンス用

1-1-3 ネットワーク監視

GICT を構築した業者の 1-1-2 データセンター内に遠隔監視環境を整備しており、運用保守の範囲で死活監視などを行っている。

(1)GSN

データセンターから各拠点 UTM まで遠隔監視を行っている。

(2)GICT

データセンターから各拠点のアクセスポイントまで遠隔監視を行っている。また、障害時等には、リモートメンテナンスが行える環境が整備されている。

1-1-4 総合教育センター

総合教育センターは、群馬県における研修事業、調査研究事業及び教育活動支援事業の拠点である。また、過去に GSN の集約拠点としての役割を担っていた経緯から、現在はヘルプデスク窓口としての機能を有している。

ICT 環境についてはこれまで独自に整備・運用してきたが、専任の保守事業者を配置していないことから、機器更新や障害対応に課題を抱えており、特にネットワーク機器については老朽化が進行している。

1-1-5 端末

教職員用・児童生徒用端末は、現在の状況は以下のとおりである。

なお、教職員には、GSN 用として Windows 端末、GICT 用として Chromebook 等の 2 台を貸与しており、私用の端末利用も許可している。

表 1-33　端末利用状況

学校	教職員	児童生徒
県立高校	GSN:県貸与 Windows GICT:県貸与 Chromebook 個人端末も可	GICT:個人端末(BYOD) ※全生徒の 20％弱は、県貸与 Chromebook を使用
特別支援学校 (小中学部)	GSN:県貸与 Windows GICT:県貸与 iPad 個人端末も可	GICT:県貸与 iPad
特別支援学校 (高等部)	GSN:県貸与 Windows GICT:県貸与 iPad 個人端末も可	GICT:個人端末(BYOD)
中央中等教育学校	GSN:県貸与 Windows GICT:県貸与 Chromebook 個人端末も可	GICT:県貸与 iPad
夜間中学校	GSN:県貸与 Windows GICT:県貸与 Chromebook	GSN:県貸与 Chromebook
総合教育センター	GSN:県貸与 Windows 研修用:県貸与 Windows、 県貸与 Chromebook、 県貸与 iPad	

1-1-6 セキュリティ

GSN 及び GICT において実装している主なセキュリティ対策は、表 1-4 のとおりである。
GSN では、各学校及びデータセンターに UTM を設置し、ネットワーク境界におけるアクセス制御及び脅威対策を実施している。一方、GICT では各学校に UTM を設置しているが、データセンターでの集約的なセキュリティ対策は実施していない。

また、端末に対するセキュリティ対策については、GSN ではアンチウイルスソフトウェアを導入しているが、GICT では導入していない。通信制御については、両ネットワークとも Web フィルタリングを実装している。

無線 LAN については、GICT において利用者認証によるアクセス制御を実施している。

表 1-44　実装しているセキュリティ

区分	GSN	GICT
境界制御	各学校及びデータセンターに UTM を設置	各学校に UTM を設置
エンドポイント	アンチウイルスソフトウェア導入	なし
通信制御・監視	web フィルタリング	web フィルタリング
アクセス制御	利用なし	無線 LAN におけるユーザ認証

1-1-7 認証基盤

(1)構成要素

現在の認証基盤は、iDaaS として Extic（エクスジェン・ネットワークス）を採用し、Microsoft Entra ID 及び GWS との認証連携を実施している。

Extic を統合認証基盤として利用し、学内システム及びクラウドサービスに対するユーザアカウント管理、プロビジョニング及びシングルサインオン（SSO）を実現している。

主な構成要素は以下のとおりである。

・ iDaaS：Extic
・ 認証基盤：Microsoft Entra ID
・ Web フィルタリングサービス：i-Filter
・ グループウェア基盤：Google Workspace for Education
・ 無線 LAN 認証基盤（無線 LAN 集中管理サーバ、RADIUS サーバ）

(2)運用方法

利用者アカウントの管理については、各学校からアカウント情報の変更申請書を Excel で ICT ヘルプデスクに送付し、その申請情報をもとに Extic で管理している。Extic に登録されたユーザ情報は、プロビジョニング機能により Microsoft Entra ID 及び GWS へ自動連携される。

一方、生徒情報管理システムにおいて利用する組織情報やグループ情報については、Extic との自動連携を行っておらず、Microsoft Entra ID へ別途手動登録を実施している。

また、i-Filter@Cloud については、ユーザ情報を CSV ファイルにより連携している。

(3)認証･連携方式

現行環境における主な認証方式は以下のとおりである。

表 1-55 主な認証方式

システム・サービス	認証方式
生徒情報管理システム（校務支援システム）	Entra ID との OIDC 連携によるシングルサインオン
GWS	Extic 経由のシングルサインオン
Entra ID 利用サービス	Entra ID 認証
i-Filter@Cloud	ユーザ認証（証明書認証併用）
無線 LAN	RADIUS 認証

(4)認証フロー

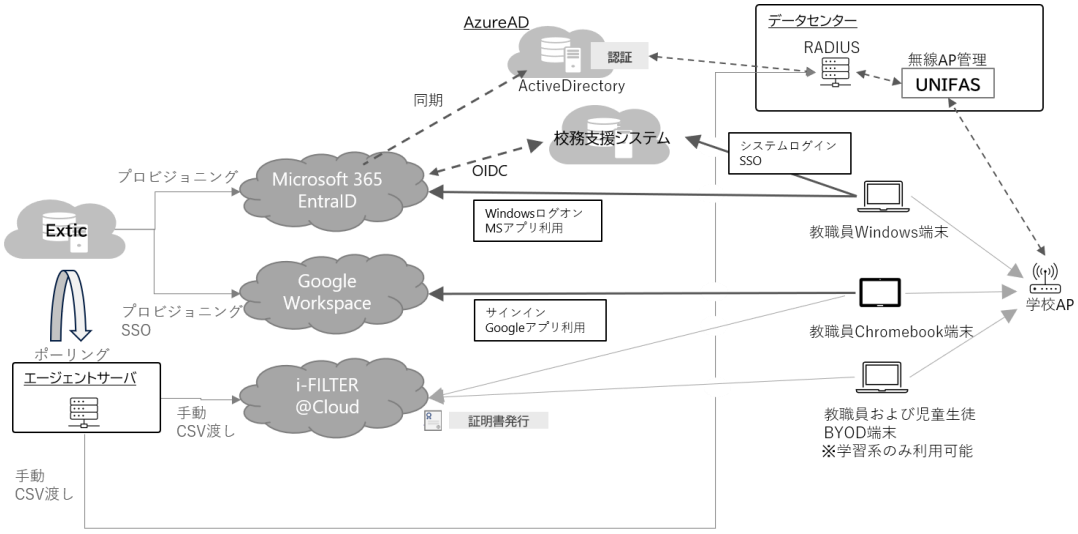


図 1-33 認証フロー図

③生徒情報管理システム(校務支援システム)

教職員が Windows 端末から生徒情報管理システムへアクセスする際は、Microsoft Entra ID との OIDC 連携によりシングルサインオンを実施している。

①Microsoft サービス

教職員 Windows 端末、BYOD 端末及び児童生徒端末において、Microsoft 365 及び関連アプリケー

ション利用時は Microsoft Entra ID による認証を実施している。

② Google サービス

教職員 Windows 端末、Chromebook 端末、BYOD 端末及び児童生徒端末において、Google Workspace へのサインイン認証を実施している。

③ 無線 LAN アクセス（GICT）

利用者が無線 LAN へ接続する際は、無線 LAN コントローラから RADIUS サーバを経由し、Azure 上の認証基盤に対して認証を実施している。GICT のインターネットアクセス時は i-Filter@Cloud による認証を実施している。利用にあたっては、県貸与端末についてはエージェントのインストールを行い、BYOD については事前に端末へのルート証明書の設定が必要となる。

1-1-8 運用・保守

運用・保守は、GSN、GICT それぞれ 2 つの一次受付窓口があり、それぞれの問合せ内容により、エスカレーション先が設けられている。

なお、現在は、GSN は 3 名（職員 2 名、委託事業者 1 名）、GICT は 5 名（職員 1 名、委託事業者 4 名）の体制で運用している。

GSN の年間問合せ件数は約 400 件、GICT の年間問合せ件数は約 450 件（案件単位）となっている。

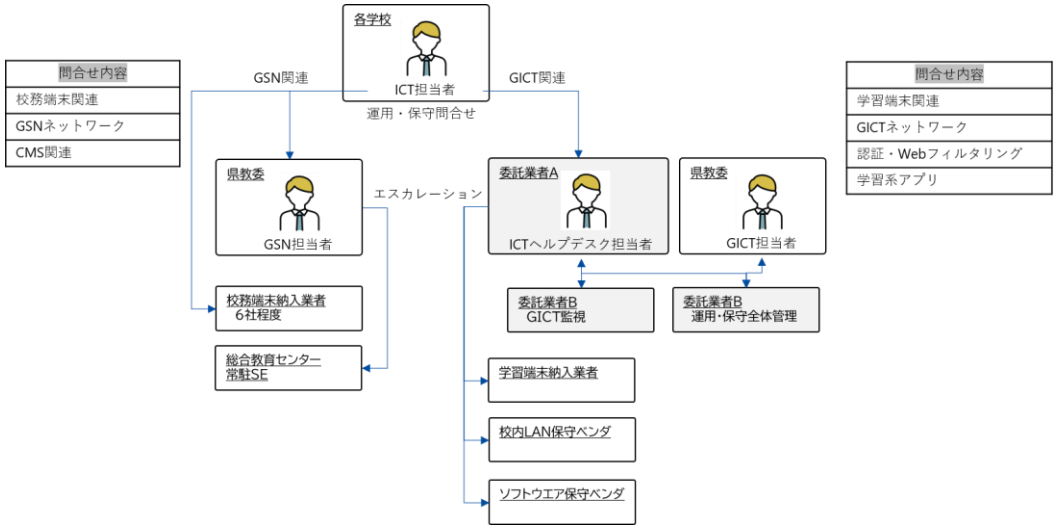


図　1-4　運用・保守フロー図

1-2　現状 ICT 環境の課題と次期環境整備の方向性

1-2-1 現地調査結果

令和 8 年 5 月から 6 月にかけて、学校現場における ICT 環境の実態把握及び次期ネットワーク環境整備に向けた要件整理を目的として、現地調査及びヒアリングを実施した。

主な調査観点は以下のとおりである。

- GSN 及び GICT ネットワーク統合の実現性確認
- Wi-Fi 利用要望の高い職員室、会議室、体育館等における無線 LAN 環境の確認
- GSN 系統の校内 LAN 配線及びネットワーク機器の現状把握
- 学校 ICT 担当者からの課題、要望の把握

現地調査の結果、GSN 及び GICT はサーバ室を起点として物理的に分離されたネットワークとして構築されているものの、校内配線構成等を確認したところ、サーバ室内の基幹スイッチへ集約する形でネットワーク統合を実施できる見込みであることを確認した。

また、GICT 整備時において職員室等へ無線アクセスポイント（AP）が設置されている学校も多く、次期ネットワーク環境において無線 LAN 利用エリアの拡張を実施する際、既設配線を活用できる可能性が高いことを確認した。

一方で、現在の無線 LAN 環境は主に授業利用を想定した設計となっており、職員室、会議室、特別教室等において日常的な業務利用を支えるには十分な収容能力及び通信品質を備えていない状況が見受けられた。

特に体育館については、学年集会や研修会等において学年単位での利用ができる無線 LAN 環境を求める要望が多く、既設の AP1 台構成では対応が困難であることが確認された。

また、GSN は平成 14 年頃から運用されており、その後のネットワーク拡張や改修については学校ごとに実施されてきた経緯がある。このため、県教育委員会において校内 LAN の構成や配線状況を十分に把握できていない状況であった。

たとえば EPS（電気・配線スペース）や各執務室等には、Cat5 ケーブルやサポート期限を迎えているネットワーク機器が多数残置されていることを確認した。また、増設や改修が繰り返された結果、配線の整理が不十分となり、保守性や障害対応性の観点で課題を有する学校も見受けられた。

これらの状況から、次期ネットワーク環境の整備にあたっては、校内 LAN 配線及びネットワーク機器の構成を再整理するとともに、老朽化した配線・機器の計画的な更改を実施する必要がある。

学校 ICT 担当者ヒアリング結果をまとめたものが以下のとおりである。

カテゴリ		大項目	現調結果	課題
ツール	A	ネットワーク統合	✓ GSNおよびGICTが物理的に独立した2系統として運用されていることによる管理コストおよび保守運用負荷が二重に発生	✓ 強固なセキュリティおよびアクセス制御を担保しつつ、ネットワーク統合実現
	B	校務支援システムと周辺システムのクラウド化	✓ 教員間でのICTリテラシー格差による活用状況のバラツキ	✓ 生成AIやチャット利用促進にむけた啓発および教育実施による底上げ
	C	教職員端末の1台化 ロケーションフリーによる校務処理	✓ 職員室外からのアクセスへの不安/懸念が根強い ✓ 私物端末への依存	✓ 場所や端末に依存しない安全なアクセス環境整備 ✓ 教職員の理解・意識向上 ✓ 端末に関するルール統一、運用基準策定
	D	ゼロトラストによるセキュリティ対策	✓ 業者とのデータ受け渡しなどUSBメモリ利用が継続 ✓ 年々増加するデータの管理がNASに集中	✓ クラウドストレージ環境整備（GoogeDrive利用促進）
	E	ダッシュボード整備・データ連携	✓ 複数システムの使い分け、手入力作業が発生することによる負担	✓ ダッシュボードによる情報の一元化・データ連携 ✓ クラウドアプリのSSO連携強化による認証の簡素化および利便性向上
	F	通信帯域最適化・ 無線LAN再配置	✓ GSN(HUB・ケーブル・端末)経年劣化 ✓ 利用集中に起因した速度低下・接続不安定 ✓ 会議室、職員室などのWiFiエリア拡大要望	✓ ネットワーク統合に合わせ機器リプレース ✓ 無線LAN強化(AP増設・コントローラ型へ)
ルール	G	ネットワーク運用ルール	✓ 接続不良・トラブル対応は属人的運用に依存 ✓ ネットワーク制限や認証・データ連携の不便さによる業務効率の低下	✓ 県で統一したトラブル対応の標準化 ✓ ID・認証の統合（一人１アカウント運用の徹底）
マインドセット・スキル	H	セキュリティ教育・操作研修	✓ スキル格差による教職員への運用負担の深刻化 ✓ 問い合わせや業務効率低下など現場の負担が増大	✓ 常駐・巡回型ICT支援員、ヘルプデスク強化 ✓ 動画研修、チャットボット、ナレッジ基盤の活用 ✓ キッティング・設定・導入はアウトソーシング活用

図　1－5　学校 ICT 担当者ヒアリング結果及び課題

1－2－2 次期環境整備の方向性

現状 ICT 環境の分析結果を踏まえ、次期ネットワーク環境整備において解決すべき課題及び目指すべき方向性を以下に整理した。

表　1－6　現状 ICT 環境の解決すべき課題一覧

カテゴリ	課題	方向性
(1)全体構成	➢　複雑化による運用負荷増大及び柔軟	✓　シンプル・安全・低コストの ICT

	性の低下	環境整備を実現する
(2)ネットワーク統合及び校内 LAN 再整備	➢ GSN、GICT ネットワークの分離による業務非効率 ➢ GSN の配線複雑化、老朽化により通信品質の低下 ➢ ネットワーク機の重複配置により運用負荷が増大している	✓ 強固なセキュリティを確保しつつネットワーク統合を実現する ✓ 運用管理の効率化及びコスト最適化を図る ✓ PC 教室再整備
(3)クラウド周辺システムの有効利用	➢ GWS、生成 AI の有益アプリ利活用のバラツキ ➢ 同一利用者が複数システムへ個別認証を行っている	✓ クラウドサービスを活用し利便性向上を図る ✓ SSO などの認証連携強化
(4)端末 1 台化及びロケーションフリー	➢ 教職員端末２台持ちにより業務が非効率 ➢ 校務端末の持ち出しができない ➢ 校内外問わず柔軟な働き方を支援する環境が不足している ➢ 私物端末利用の依存 ➢	✓ 教職員端末 1 台化を実現する（Windows） ✓ 校外からも安全に利用できる認証基盤及びアクセス環境を整備する。 ✓ 教職員の利便性とセキュリティを両立する
(5)ゼロトラストを前提としたセキュリティ対策	➢ USB メモリ利用や NAS 利用継続 ➢ クラウドストレージ利用のセキュリティ対策が不十分のため、機微な情報の格納場所がない	✓ クラウドストレージ利用を推進する ✓ 重要性分類に応じたアクセス制御及び情報保護を実装する ✓ USB メモリについては原則利用不可とするが、限定的利用ができる環境とする
(6)無線 LAN 環境の拡充	➢ 職員室や会議室で快適に利用できる無線 LAN 環境が不足している ➢ 体育館等の大人数利用に対応できていない	✓ 校内全域における業務利用を前提とした無線 LAN 環境を整備する ✓ 体育館等の高密度環境に対応した無線 LAN 設計を行う ✓ 有線 LAN への依存度を低減する
(7)運用保守体制強化	➢ GSN と GICT 問合せ窓口が分離している ➢ 特に無線 LAN 接続不具合による問合せ増による学校 ICT 担当者の負担増 ➢ 障害情報や対応履歴が十分に共有・活用されていない	✓ 統合ヘルプデスクの実現 ✓ ナレッジ管理及び FAQ 活用による自己解決率向上 ✓ AI チャットボット等による問合せ対応効率化
(8)群馬県全体のコミュニケーション強化	➢ 児童生徒が県立学校進学時にアカウントが変わってしまう。 ➢ 市町村立学校、市町村教委とアカウント体系が異なり、コミュニケーションに支障がある。	✓ 児童生徒アカウント活用を見据えた拡張性を確保する ✓ Gunmal（県内共通基盤）の参加

(1)全体構成

現行システムは、データセンター及び既存クラウド基盤に依存した構成となっており、システムの複雑化により運用負荷の増大や柔軟性の低下が課題となっている。また、新たなサービス導入や環境変更に対する柔軟性の低下も懸念される。

次期環境では、クラウドサービスの積極的な活用を前提とし、シンプルかつ拡張性の高い ICT 基盤を目指す。

主な検討事項

- ✓ 利用中システムの SaaS 化を前提とした全体アーキテクチャ
- ✓ SaaS 移行の適否判断及び、移行が困難なシステムの取り扱い（代替案・例外対応）

✓　将来的な拡張性及びベンダロックイン回避を考慮した構成

(2)ネットワーク統合及び校内 LAN 再整備

GSN／GICT の分離構成により、機器構成の重複や運用の複雑化、コストの二重化が発生している。また、GSN は導入から長期間が経過しており、学校独自の増設・改修が繰り返された結果、県教育委員会が校内 LAN の実態を十分に把握できていない状況にある。

次期環境では、ネットワーク統合とあわせて校内 LAN 環境の再整備を実施し、運用品質及び保守性の向上を図る。

なお、県としては、校内 LAN 環境は現行の GICT をベースとして活用し、GSN については可能な限り既設 LAN 配線及び近年導入したネットワーク機器を活用したうえで、ルータ及び基幹スイッチなど上位ネットワークにおいて統合する構成を想定している。ただし、より有効な提案がある場合はこれに限定しない。

主な検討事項

✓　GSN／GICT 統合を前提としたネットワークアーキテクチャ
✓　校内 LAN の標準化及び可視化
✓　老朽化した配線・機器への対応
✓　段階的な移行方式及び移行リスク低減策
✓　運用負荷軽減及びコスト最適化

(3)クラウド周辺システムの有効利用

Google Workspace、生成 AI 等のクラウドサービスを利用できる環境は整備されているものの、教職員間の ICT 利用活用には差があり、十分に活用されていないサービスも存在する。

次期環境では、単なるシステム整備に留まらず、教職員が ICT 活用による効果を実感できる環境づくりを推進する。

主な検討事項

✓　教職員の ICT 活用レベル向上策（体験型研修）
✓　生成 AI 等の新技術活用方策
✓　利用定着に向けた研修・伴走支援

(4)端末 1 台化及びロケーションフリー

現行の複数端末運用により、端末管理の負荷増大及び利便性の低下が課題となっている。また、校外への端末持出しや校内の様々な場所での業務実施を想定した環境整備が十分ではない。

次期環境では教職員端末の 1 台化を実現するとともに、学校内外を問わず安全かつ円滑に利用できる環境の実現を目指す。県としては、既存資産及び利用実態を踏まえ、教職員端末は Windows 前提として検討している。

主な検討事項

✓　教員端末の 1 台化
✓　MDM 等による端末（配布、設定、更新、廃棄）を効率化するための管理基盤
✓　のぞき見防止等を含む情報漏洩対策
✓　校外利用を前提としたアクセス制御

(5)ゼロトラストを前提としたセキュリティ対策

本環境におけるセキュリティ対策については、「教育情報セキュリティポリシーに関するガイドラ

イン（令和 7 年 3 月版)」の準拠を前提とする。

一方で、現状では外部事業者とのデータ受け渡し等における USB メモリ利用や、写真・動画等の大容量データ増加に伴う NAS 利用が拡大しており、情報漏えいリスク及びデータ管理の複雑化が課題となっている。

また、データの重要性に応じた適切な管理区分やアクセス制御の考え方が十分に整理されておらず、教職員がデータ保管場所や共有方法の判断に迷う場面も発生している。

次期環境では、ゼロトラストの考え方に基づき、クラウドサービスを前提としたセキュリティモデルへ移行するとともに、データの重要性に応じた情報管理を実現することを目指す。

主な検討事項

- ✓ クラウドストレージへの段階的移行方針（リフトアップ計画）
- ✓ データの重要性分類に基づく情報管理設計
  （セキュア領域／公開領域の分離、アクセス制御ポリシー データ共有ルール）
- ✓ データ保護対策 （暗号化、DLP、監査ログ、ランサムウェア対策）

(6)無線 LAN 環境の拡充

GIGA スクール構想に基づき、各教室及び体育館等に無線アクセスポイント（AP）整備を実施してきたが、主として授業利用を前提とした構成であり、教職員の日常的な業務利用を十分に考慮したものとはなっていない。

近年は、職員室、会議室、校内共用スペース等における無線 LAN 利用ニーズが増加しており、校内のどこでも業務を行える環境の整備が求められている。

また、体育館における学年集会や研修会等では、多数の端末が同時接続されるため、既存構成では通信品質及び収容能力に課題がある。

さらに、VR ゴーグルや電子黒板、プリンタ等の Wi-Fi 対応機器については、従来利用者認証方式では運用が困難なケースもあり、多様な端末を安全にかつ円滑に接続できる仕組みが求められている。

次期環境では、有線 LAN への依存を低減し、校内全域で安定して利用できる無線 LAN 環境の実現を目指す。

主な検討事項

- ✓ 無線エリア拡張・AP 最適配置
- ✓ スムーズな BYOD 接続の方法
- ✓ 体育館等における高密度環境への対応
- ✓ VR ゴーグル、電子黒板、プリンタ等の非 PC 端末への対応
- ✓ 利用者及び端末種別に応じた認証・アクセス制御

(7)運用保守体制強化

GSN 及び GICT は構築時期や運用事業者が異なることから、問合せ窓口が分散しており、学校現場において適切な問合せ先の判断が困難となるケースが発生している。その結果、障害対応の遅延や学校 ICT 担当者の負担増加につながっている。

また、近年は障害対応だけでなく、Google Workspace や生成 AI 等の活用相談など、ICT 利活用に関する支援ニーズも増加しており、問合せ内容が高度化・多様化している。

さらに、県教育委員会では、蓄積された問合せ履歴や障害対応履歴を活用したチャットボットによる自動応答の取り組みを進めており、今後は適用範囲の拡大やナレッジ活用の高度化を目指している。

次期環境では、利用者視点で分かりやすく、継続的に改善可能な運用保守体制の構築を目指す。

主な検討事項

- ✓ 統合ヘルプデスクの実現
- ✓ 問合せ管理及び対応履歴の一元管理
- ✓ ナレッジ管理及び FAQ 活用
- ✓ チャットボットとの連携及び継続的な学習・改善
- ✓ 学校 ICT 担当者の負担軽減策

(8)群馬県全体のコミュニケーション強化

群馬県では、市町村学校及び一部大学を対象として Google Workspace を基盤とした統合環境「Gunmal」が整備されている。

一方、県立学校は Gunmal への参加が未了であり、アカウント基盤やコミュニケーション基盤が分断されている状況にある。また、児童生徒は高校進学時にアカウント引き継ぎが

次期ネットワーク環境整備においては、県立学校の Gunmal 参加を視野に入れ、県全体で情報共有や連携強化するとともに、児童生徒の小学校から高校までの ID 体系の統合を目指す。

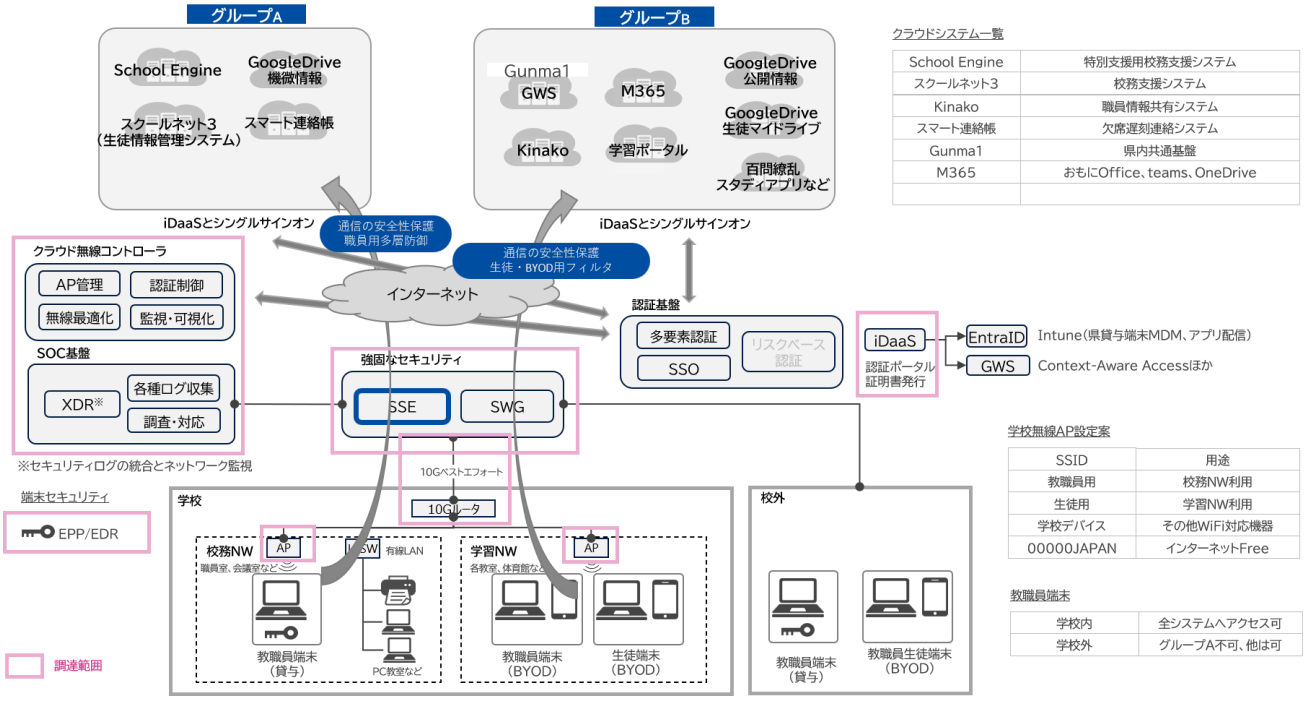
主な検討事項

- ✓ 県立学校の Gunmal 参加方式
- ✓ 既存認証基盤との連携方法
- ✓ 教職員アカウント統合方針
- ✓ 児童生徒アカウント活用方針

第２章 次期ネットワーク環境の全体構想（To-Be）

２-１　次期ネットワーク環境構成イメージ（案）

次期ネットワーク環境整備において、県が求める強固なセキュリティ環境構成イメージ案（図２-1）を示す。文部科学省が推奨してい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（令和 7 年 3 月版）を準拠すれば、提案構成は問わない。



グループ A：機微情報を扱うシステム群
グループ B：グループ A 以外の県立学校が利用するシステム群

図　2-11 強固なセキュリティ環境イメージ

上記構成イメージ（案）における Before-after 一覧は以下のとおりである。

カテゴリ	ICT	現環境（before）	次期環境（after）
端末	教職員校務端末	2 台	1 台（WindowsOS） グループ A、B、Internet アクセス可能※1
	教職員 BYOD	学習利用で可	学習利用で可 グループ B、Internet アクセス可能
	生徒 BYOD	学習利用で可	学習利用で可 グループ B、インターネットアクセス可能
	校務端末管理（MDM）	Skysea	Intune
	校務端末暗号化	Windows Education 標準 BitLocker	Windows Education 標準 BitLocker
	エンドポイントセキュリティ（校務端末）	トレンドマイクロ ApexOne	Windows Defender＋市販 EDR 又は、市販 EPP＋市販 EDR

ネットワーク	教育ネットワーク	GSN と GICT の 2 系統	GICT に統合
	GSN（校務 NW）	境界型（データセンター UTM）	ゼロトラスト
	GICT（学習 NW）	境界型（学校 UTM）	ゼロトラスト
	Wi-Fi	主に学習系（GICT）用途で利用	学習系・校務系問わず利用
		学校端末	学校端末、Wi-Fi 対応機器
		職員室、教室、体育館、会議室	現環境をベースに増設を行う。
	インターネット回線	GSN メイン回線：専用線 GSN サブ回線：1G ベストエフォート型 GICT：1G ベストエフォート型（学校により複数回線）	対象エリアであれば 10G ベストエフォート回線 1 本へ乗り換え 対象外エリアであれば、現回線継続 なお、利用者が少数のエリアは、1G ベストエフォート回線とする。（詳細は別紙 2 のとおり）
	監視	データセンターオンプレ監視	ゼロトラスト SOC、クラウド型 Wi-Fi コントローラ
セキュリティ	Web フィルタリング	i-Filter	ゼロトラスト
認証	iDaaS	Extic	市販 iDaaS（証明書発行ができるもの）※2
	SSO	GWS、生徒情報管理システム	左記に加えて汎用クラウドアプリ全般へ拡大
データほか	ストレージ	GoogleDrive（公開情報）、学校 NAS	GoogleDrive（機微情報、公開情報）へ移行
運用	ロケーションフリー	無	可能

※1　校外ではグループ A にアクセスさせない

※2　後述の Gunmal アカウント統合に向けた構成による

2-2　統合ネットワーク（GSN/GICT）の基本方針

次期ネットワーク環境の整備にあたっては、教職員及び児童生徒が安全かつ快適にデジタルサービスを利用できる環境を実現するとともに、校務 DX の推進及び教育活動の高度化を支える ICT 基盤の構築を目指す。

現行環境では、GSN 及び GICT の分離による運用の複雑化、認証基盤やクラウドサービスの個別最適化、校内 LAN 設備の老朽化、教職員端末の複数台運用など、様々な課題を抱えている。

このため、次期環境では「クラウドファースト」及び「ゼロトラスト」の考え方を基本とし、GSN 及び GICT の統合、教職員端末の 1 台化、校内無線 LAN 環境の拡充、認証基盤の統合並びに運用保守体制の強化を実現する。

また、将来的なサービス追加や利用者増加にも柔軟に対応できる拡張性を確保するとともに、市町村立学校との連携を見据えた Gunmal との親和性を考慮した構成とする。

あわせて、教職員が校内外を問わず同様の操作性で安全に業務を行える環境を整備し、利用者の利便性向上とセキュリティ確保を両立する ICT 基盤を目指す。

2-2-1 基本方針

(1)シンプルかつ持続可能な ICT 基盤の実現

GSN 及び GICT の統合やクラウドサービス活用を推進し、複雑化した現行構成を見直すことで、運用負荷の軽減及びコスト最適化を図る。

(2)ゼロトラストを前提としたセキュリティ強化

ネットワーク境界防御に依存しないセキュリティモデルへ移行し、利用者、端末、アプリケーション及びデータを中心とした多層防御を実現する。

(3)時間や場所にとらわれない校務環境の実現

教職員端末の 1 台化及び無線 LAN 環境の拡充により、校内外を問わず安全かつ柔軟に業務が行える環境を整備する。

(4)クラウドサービスの有効活用による校務 DX 推進

認証基盤やクラウドサービスの統合・連携を推進するとともに、Google Workspace、生成 AI 等の新たなデジタルサービスも活用できる基盤を整備する。

(5)運用負荷の軽減と県域連携の強化

統合ヘルプデスクやナレッジ活用を推進するとともに、Gunma1 との連携を視野に入れた県全体のコミュニケーション基盤強化を図る。

2-3　端末・アカウント統合の基本方針（Gunma1 統合等）

現在、県立学校の GSN アカウントを県単独で使用しているが、次期ネットワークにおいては、市町村立学校（小学校、中学校等）が共通で使用する Gunma1 アカウントの導入により、小中高一貫したアカウント体系の実現を行う。なお、現在の Gunma1 アカウントの構成は以下のとおりである。

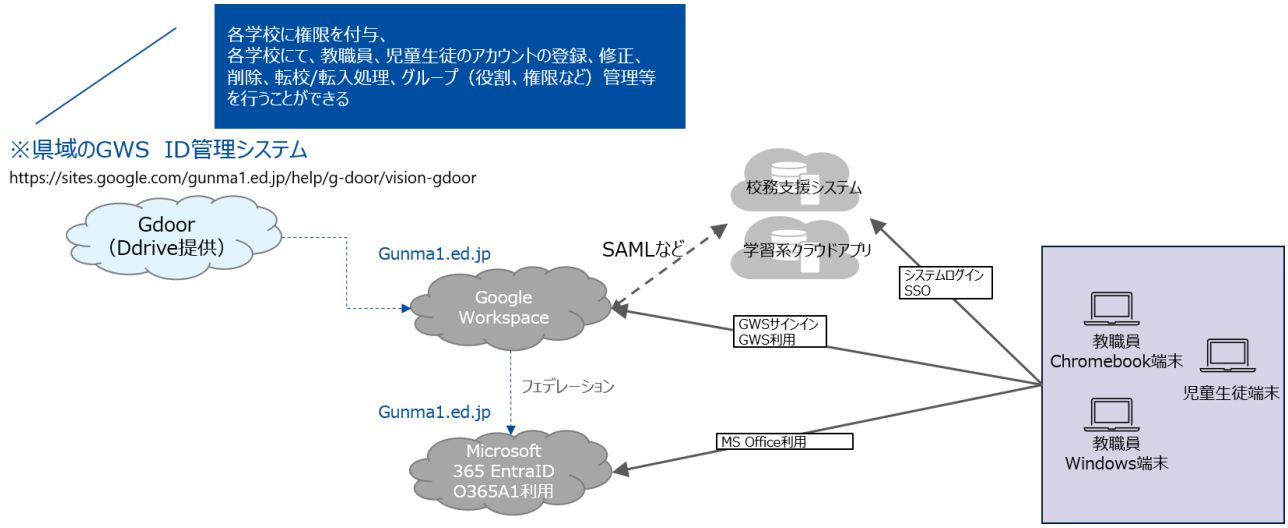


図　2-2　市町村の認証フロー

2-3-1 基本方針

県立学校においては、現在、県独自の GSN アカウント（edu-g.gsn.ed.jp）を利用している。一方、市町村立学校では、県共通アカウントである Gunma1 アカウント（gunma1.ed.jp）を利用している。

次期ネットワークでは、小中高を通じた統一的な認証基盤の実現を目的として、県立学校における Gunma1 アカウントの活用について検討している。

ただし、現時点では以下の課題があると認識している。

- ✓ 県立学校の利用者を Gunmal アカウントへ移行する場合、認証情報の移行、端末再設定、教職員等の運用負荷が大きいこと。
- ✓ Microsoft Entra ID については、市町村立学校と県立学校で利用目的やライセンス体系が異なっていること。
  - ➢ 市町村立学校：主に Web 版 Microsoft 365 を利用
  - ➢ 県立学校：Microsoft 365 A3 ライセンスを利用し、デスクトップアプリ、端末管理、OS 管理等を実施

本 RFI においては、小中高を通じた統一的な認証基盤の実現に向け、アカウント管理方式、認証基盤の構成、移行方式及び運用方式について提案を求めるものとする。

なお、県では現時点における有力な構成案の一つとして、以下の認証基盤構成を想定しているが、その実現可否、実装上の課題及び留意事項に意見を求める。

- ✓ Google Workspace は Gunmal アカウントへ統合する。
- ✓ Microsoft Entra ID は県立学校の既存テナントを継続利用する。
- ✓ iDaaS を中心とした認証連携及びアカウント管理を実施する。

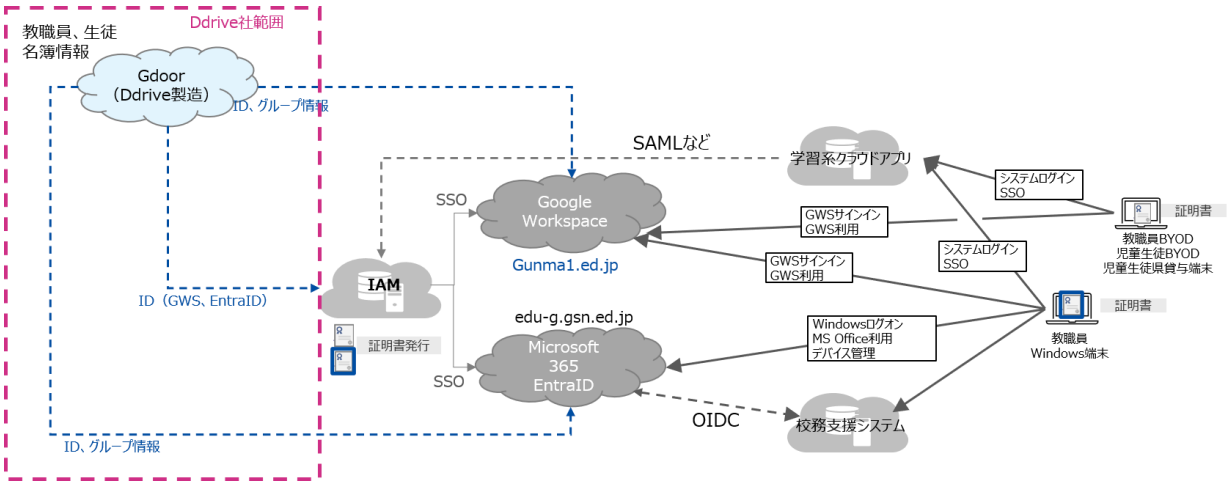


図 2-3 検討中の認証フロー案

また、提案に当たっては、上記構成案に限定するものではない。県が目指す統一的な認証基盤の実現に向けて、より実現性、運用性、拡張性及び費用対効果に優れた構成案がある場合は、その理由及びメリットを含めて併せて提案すること。

第3章 機能・システム要件

3-1 認証基盤要件

本認証基盤については、利便性とセキュリティの両立を前提とし、現行システムよりも教職員による運用負荷軽減を考慮した提案を求める。

3-1-1 多要素認証

知識情報（ID 及びパスワード等）、生体情報（指紋、静脈、顔、声紋等）、物理情報（IC カード、USB トークン、クライアント証明書、トークン型ワンタイムパスワード等）のうち、異なる認証方式

２要素以上を組み合わせた多要素認証が可能であること。ただし、ハードウェアトークン等の紛失リスクが発生するデバイスに関しては、リスク対策を考慮すること。
また、教職員はスマートフォン等の支給を受けていないため、その点も考慮すること。

３-１-２リスクベース認証

端末の IP アドレスや位置情報、使用されている Web ブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、本人であることを確認できること。

３-１-３SSO 連携等

各種クラウドサービスとのシングルサインオンが可能であること。

- ✓ SAML、OpenID Connect 等を用いた SSO 実装
- ✓ 対象クラウドサービスとの接続実績

３-１-４証明書発行

端末認証等に利用する証明書発行機能を下記のとおり有すること。

- ✓ ICT に詳しくない教職員でも実施可能な証明書配布・設定方式（自動配布、ゼロタッチ、MDM 連携等）を備えていること。
- ✓ 県教育委員会（センター側）からの一括配布・管理方式を備えていること。
- ✓ 証明書のライフサイクル管理（更新・失効）の運用が容易なこと。

３-１-５ID 連携（プロビジョニング）

外部サービスとの ID 連携が可能であること。

- ✓ 市町村共通基盤であるの Gunmal へ参加
- ✓ Google WorkSpace、Microsoft Entra ID 等のプロビジョニング
- ✓ ID 同期
- ✓ 複数 ID の基盤併存

３-１-６Wi-Fi 認証

RADIUS 認証機能を有していること。

３-２　ネットワーク・無線 LAN 要件

３-２-１ネットワーク要件

(1)ネットワーク統合

現在、別系統で運用している GSN 及び GICT ネットワークを物理的に統合（論理的に分離）し、両ネットワークからインターネットへの接続を可能とすること。
また、既存システム及び端末への影響を最小限とし、移行期間中においても円滑な運用を継続できる構成を提案すること。

(2)機器更新

- ・ ルータ
- ・ 基幹スイッチ
- ・ PoE スイッチ（L2 スイッチ）
- ・ 無線アクセスポイント

・　UTM　※クラウド FW の設置により省略も可

対象機器の詳細は「別紙 2_学校 NW 機器、LAN 工事一覧」を参照すること。

また、GSN で整備されたネットワーク機器については、現地調査結果を踏まえ、流用・更新・撤去の方針を提案すること。

(3)インターネット回線

10Gbps 提供エリアについては、10Gbps 回線（ベストエフォート）への切替を基本とすること。

10Gbps 未提供エリアについては、既存回線の継続利用を基本とし、最適な回線構成を提案すること。（なお、院内教室や農場については、同時接続数が少ないため 1Gbps 回線（ベストエフォート）とする。）

(4)LAN 配線

GICT 整備により敷設された LAN 配線については、原則として流用すること。

また、GSN 整備時に敷設された LAN 配線についても、現地調査の結果、品質及び性能上問題がない場合は流用を可とする。

一方で、老朽化や性能不足（Cat5 以下等）が確認された配線については、更新が必要な箇所を明確化し、更新内容を提案すること。

(5)有線 LAN 環境の継続利用

校長室、保健室、準備室、PC 教室その他 Wi-Fi 整備対象外のエリアについては、既存の有線 LAN 環境を継続利用することを前提とする。

このため、無線 LAN 環境と既存有線 LAN 環境が混在する構成においても、利用者が支障なくネットワークを利用できること。

また、既存有線 LAN 設備の流用にあたり必要となる接続方式、収容方法及び機器構成について提案すること。

(6)LAN 工事に関する見積について

校内 LAN 工事費用については、本来、各学校の現地調査を実施した上で詳細な工事内容を確定する必要がある。しかしながら、本 RFI では概算費用を把握することを目的としているため、以下の 3 パターンを標準モデルとし、それぞれについて見積を作成すること。

なお、ネットワーク機器の台数等については「別紙 2 学校 NW 機器・工事一覧表」を参照すること。また、LAN 工事に係る図面については、「別紙 3～5_見積算出モデル校」を参照すること。

また、長期間の運用停止とならないようプロジェクト計画を想定すること。そのうえで、プロジェクト管理費、設計費、構築費、施工管理費等の見積を作成すること。

■パターン A：赤城特別支援学校（本校）モデル

GIGA スクール構想に伴い整備された既設 LAN 配線は流用可能であることを前提とする。

見積対象範囲は以下のとおりとする。

・　無線 LAN アクセスポイント（AP）の更新作業
・　既設 PoE スイッチの更新作業
・　既設基幹スイッチの更新作業

■パターン B：太田フレックスモデル

GIGA スクール構想に伴い整備された既設 LAN 配線の流用に加え、一部エリアにおいて新規 LAN 配線

敷設が必要であることを前提とする。

見積対象範囲は、パターン A に加え、以下のとおりとする。

- 職員室への LAN 配線敷設及び AP 新設
- 会議室への LAN 配線敷設及び AP 新設
- 体育館への LAN 配線敷設及び AP 新設
- PoE スイッチの増設作業

■パターン C：前橋工業モデル

見積対象範囲は、パターン B に加え、以下のとおりとする。

- GSN 環境として整備された PC 教室内 L2 スイッチの更新作業
- PC 教室内の既設 LAN 配線の更新作業

３-２-２無線 LAN 要件

(1)対象デバイス

本無線 LAN 環境においては、以下の端末種別の接続を想定する。

- ✓ 教職員用貸与端末（Windows、iPad）
- ✓ 教職員 BYOD 端末（Windows、Chromebook、iPad、MacBook など）
- ✓ 生徒用貸与端末（Chromebook、iPad）
- ✓ 生徒用 BYOD 端末（Windows、Chromebook、iPad、MacBook など）
- ✓ 校務・授業で利用する各種 Wi-Fi 対応機器（電子黒板、プリンタ、VR ゴーグルなど）

(2)SSID 設計

利用者及び用途に応じた複数 SSID を柔軟に設定可能であること。

SSID ごとの認証方式及びアクセス制御が可能であること。

（例）

- ✓ 教職員用 SSID
- ✓ 生徒用 SSID
- ✓ 学校デバイス SSID
- ✓ 00000JAPAN 用 SSID（体育館等避難所 AP のみ、災害時に手動有効化）

(3)認証･アクセス制御

端末認証及びユーザ認証を組み合わせ、安全なアクセス制御が可能であること。

(4)無線 LAN 制御基盤(コントローラ)

クラウドコントローラ型により、無線 AP の一元管理が可能であり、下記機能を有すること。

- ✓ AP 集中管理
- ✓ 電波最適化・ローミング
- ✓ 可用性・冗長化

(5)給電･収容要件

無線アクセスポイントへの給電は PoE+以上を前提とし、 必要な給電容量を確保すること。

(6)性能要件

- ✓ 職員室においては、教職員が日常的に同時接続する環境を想定し、業務に支障のない通信性能を確保できること。また、体育館等の高密度利用を想定し、通信性能を確保できること。（詳細は、「別紙 2_学校 NW 機器、LAN 工事一覧」を参照のこと）
- ✓ 上記を実現するために必要となる無線アクセスポイントの台数、設置場所、性能（無線規格、同時接続性能等）及び電波設計方針を示すこと

3-3　セキュリティ・通信制御要件

3-3-1 通信の暗号化

通信の秘匿性を高めるために通信又は通信経路を暗号化し保護する仕組みを提案すること。

3-3-2 Web フィルタリング

業務上、不適切なサイトやマルウェア感染やフィッシングサイト等危険なサイトへの通信をブロックする Web フィルタリングの機能を提供すること。

また、以下の機能を備えていること。

① カテゴリーベースでの制御が可能なこと。
② ホワイトリスト/ブラックリストによる特定の Web サイトへのアクセスを制御できること。
③ SSL 通信に対しても通信を復号化してチェックできる機能を備えていること。

3-3-3 MDM

端末を一元的に監視・管理する機能を提供すること。端末のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防ぐとともに、紛失・盗難等の際に遠隔でデータ消去を行うなどして情報漏洩を防ぐこと。

なお、iPad については MDM 及び MDM 運用を別途調達しているため、本件は Windows 及び Chromebook の MDM 及び MDM 運用までを調達範囲とする。（なお、Windows 及び Chromebook の台数は、RFI 依頼書のとおりとする。）

BYOD 端末については、MDM 管理は不要とする。

3-3-4 アンチウイルス

コンピュータウイルスやマルウェア感染への対策として、既知のパターンファイル（マルウェア情報）からのマルウェアの検知・駆除する機能を提供すること。

また、パターンファイルが存在しない未知のマルウェアからも端末を保護できること（ふるまい検知）。

3-3-5 EDR

未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、感染した端末の特定や隔離、影響範囲、時系列での不正なふるまいの状況を一元的に把握することが可能な、感染の拡大を防止する機能を提供すること。

また、以下の機能を備えていること。

① シグネチャレスで、未知既知のマルウェア感染を防御する機能を有すること。
② ランサムウェア特有の挙動を検知し、端末を防御する仕組みを有すること。
③ 端末がインターネットにアクセスできない場合、エージェント自身がローカルで悪性判定を行う仕組みを有すること。

3-3-6 SASE 等

端末・通信の安全性に関する要素技術を SASE(Secure Access Service Edge)で提案する場合は、以下の要件も満たすこと。(ここで言う SASE には、SSE も含む)なお、SASE 以外の技術要素を持って解決することを妨げるものではない。

① SAML(Security Assertion Markup Language)認証によるシングルサインオン機能があること。
② 契約者に占有されるリソース及びグローバル IP アドレスにより提供される SASE サービスであること。
③ 外部 SaaS などで送信元 IP によるアクセス制限に対応するために、契約者占有のグローバル IP が割り当てられること。
④ ユーザで SASE のサービスを停止できないように制限が掛けられること。
⑤ 端末にユーザがログインする前に SASE サービスに接続されて、端末が保護されること(なお、初回ログインは除く。)又は、ユーザが認証されるまではインターネット接続が許可されないシステムあること。
⑥ SASE サービスへのユーザの接続及び利用状況により、サービス基盤のリソースがオートスケールする機能を有すること。
⑦ 全ての TCP/UDP ポートの通信をアプリケーション識別及びセキュリティポリシーを適用できること。
⑧ SaaS サービスに対してテナントベースでのアクセス制御機能を有すること。
⑨ SSL 復号化機能を有し、SSL 通信に対しても脆弱性防御、アンチウイルス、マルウェア対策機能を適用できること。
⑩ 多層防御の観点からネットワークベースのアンチウイルス、マルウェア対策機能を保持していても端末のアンチウイルス、マルウェア対策は別途提案すること。

3-3-7 ソーシャルエンジニアリング対策

教室で業務端末を使用することを想定して、盗み見防止の対策を提案すること。

3-3-8 外部サービス

パブリッククラウドサービスを利用する場合の要件を以下に示す。

(1)データセンター要件

データセンターファシリティスタンダード（日本データセンター協会）ティア３，４等に相当する設備を有すること。また、クラウドサービス及び保管データは，日本国内法の適用を受けること。

(2)ネットワーク要件

ア．インターネット接続要件

安定した常時接続回線を確保し、冗長化（複数回線）を満たしていること。

イ．ネットワーク構成要件

2 拠点以上でサービスを提供し、地震等の災害及び単一障害に対して耐性を持っていること。

ウ．セキュリティ要件

すべての通信は TLS 等により暗号化を必須とすること。

(3)クラウドサービス認定要件

重要情報を取り扱う場合は、サービス提供者が ISMS クラウドセキュリティ（ISO/IEC 27017）認証、日本セキュリティ監査協会のクラウド情報セキュリティ監査による認定、SOC2 報告書（Service Organization Control Report）等のクラウドサービスに関わる規格の認定を受けていること。あるいは、同等の対策を実施していること。その考え方、対策について提案すること。

(4)IDS/IPS(Intrusion Detection System/Intrusion Prevention System)

事前に定義した不正アクセスパターンとマッチングすることにより不正なアクセスや攻撃を検知（IDS）又は遮断（IPS）する機能を提供すること。

(5)WAF(Web Application Firewall)

インターネットと繋がっているサーバ（Web サーバ）への外部からの攻撃を検知し、防御する機能を提供すること。

第４章 非機能要件（品質、情報セキュリティ）

４-１　品質要件

４-１-１ 性能

提案するシステム全体として、業務開始時の一斉通信による通信負荷やセキュリティ対策、各種ソフト等により端末の動作遅延等が無いよう考慮して提案すること。

繁忙期や利用者数の増加時においても、著しい性能低下が発生しないシステム構成とすること。

なお、利用者の操作に対するレスポンスについては、一般的な業務利用においてストレスなく利用できる性能を目標とし、主要な処理については概ね 3 秒程度以内で応答すること（※）を目安として提案すること。

またバッチ処理を行う場合は、他システムとの連携を考慮し、運用に影響を与えないよう他システムと調整すること。

※SaaS 等、外部クラウド環境に起因する遅延についてはこの限りではないが、ネットワーク経路（調達範囲内）におけるボトルネックが発生しないよう帯域・セッション数を設計すること。

４-１-２ レスポンスタイム

本システムは、利用者が業務を円滑に実施できるよう、十分なレスポンス性能を確保すること。

レスポンスタイムは利用者数の増加や繁忙期においても著しく低下しないこと。また、想定利用者数における性能根拠を提案書に記載すること。

４-１-３ 拡張性

クラウドサービスでの提供が前提とし、利用者数の増減に柔軟に対応できること。

また、利用者数、通信量、データ量等の増加に伴い性能低下等の課題が発生した場合には、その要因を分析し、改善に向けた対応策を提案できること。

機能の変更・追加及び新規システムとの連携については、原則として追加費用のかからないよう拡張性を確保すること。

以上を踏まえて運用開始後に想定される本システムに係る状況の変化について、対応方針及び具体的な対応方法を提案すること。下記については具体的な対処方法を示すこと。

- ✓　教職員用端末の仕様変更（OS、ブラウザの更新等）
- ✓　他システムとのデータ連携における変更

- ✓ 利用者の増減、利用頻度の増減への対応
- ✓ 処理対象データ量の増減への対応
- ✓ 通信量増加やアクセス集中等による性能変化への対応（必要に応じた回線増強、設定変更、構成見直し等含む）
- ✓ 機能変更、追加時の考え方
- ✓ 拡張時の追加費用を抑制する方策
- ✓ その他想定されることへの対応

4-2　情報セキュリティ対策・ポリシー準拠

4-2-1 準拠すべき規程類

下記の規程やガイドライン等に従うこと。
また、クラウドサービス等の外部サービスを利用する場合は、下記の情報セキュリティ対策を遵守すること。

群馬県情報セキュリティポリシーに示す「クラウドサービス利用規程」を遵守すること。特に、重要情報を取り扱う場合は、提案時にリスクの洗い出しとその対策について確認したサービスを選択すること。また、添付資料の「(様式２）クラウドサービス（重要情報を取り扱う場合）利用申請時確認事項」を用いて本業務の契約前に県の承認を得ること。承認が得られない場合は提案を不採択とするので留意すること。

「地方公共団体における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 月版)」の「第４編　地方公共団体におけるクラウド利用等に関する特則」を参照して開発、運用・保守を行うこと。
独立行政法人情報処理推進機構（IPA）から公開されている「安全なウェブサイトの作り方（改訂第７版)」を参考に、必要なセキュリティ対策を実装すること。
クラウドサービス等におけるデータの廃棄については、総務省から提供されている「地方公共団体における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月版)」の「第４編 地方公共団体におけるクラウド利用等に関する特則（例文・解説)」の「(8.3. 外部サービス（クラウドサービス）の利用（自治体機密性 2 以上の情報を取り扱う場合）(8) クラウドサービスを利用した情報システムの更改・廃棄時の対策③の解説)」に記載されている「除去」もしくは「破壊」を想定している。ただし、今後変更、修正される可能性があり、確定した方法で廃棄できるよう対応すること。

契約終了時のデータの取り扱いについては、群馬県情報セキュリティポリシー、及び、添付資料「ディスク処分の基本方針」の規定に従うこと。また、保守等で交換した電子的記録機器も同様の取り扱いを行うこと。特に、重要情報が保管されている場合はそのことを踏まえて対応すること。

4-2-2 データの廃棄等

本業務で取り扱うデータについては、契約期間中は適切に保管し、漏えい、滅失、毀損等を防止するために必要な措置を講じること。
契約終了時又は県からの指示があった場合は、本業務により取得又は作成したデータについて、県の指示に従い返還又は廃棄を行うこと。

データの廃棄にあたっては、第三者による復元が不可能な方法により実施することとし、電子データについては論理消去又は物理破壊等の適切な措置を講じること。

また、ハードディスク、SSD、USB メモリその他記録媒体を廃棄又は交換する場合についても同様の措置を講じること。

廃棄完了後は、県から求めがあった場合、廃棄方法及び廃棄対象を記載した証跡資料又は廃棄証明書を提出すること。

第５章 プロジェクト・運用保守要件

５-１　移行要件

本システムの移行にあたっては、学校の授業や教職員の現行業務への影響を最小限とすることを前提とし、安全かつ確実な移行を実現するための設計及び計画の提案を求める。

５-１-１ 移行方式・移行設計

- ✓ 現行環境から次期環境への移行方式の提案
  （段階移行、並行稼働、切替方式 等）
- ✓ 業務影響を最小化するための移行設計（無停止又は短時間停止）の実現方法
- ✓ ネットワーク、認証、端末、データそれぞれの移行方針の整理

５-１-２ 並行運用・無停止要件

- ✓ 移行期間中における現行ネットワークと新ネットワークの並行運用方式の提案
- ✓ 並行運用に伴う課題（ルーティング、認証整合性、データ整合性等）及び対策
- ✓ 切替タイミング及びロールバック方法の提示

５-１-３ 作業計画等

- ✓ 作業計画の提示
- ✓ 進捗管理、課題管理、リスク管理及び品質管理の実施方法の提示
- ✓ 想定されるリスク及びその対応策の提示

５-１-４ 作業実施条件

- ✓ 学校運営への影響を考慮した作業計画の提案
  （長期休業期間、夜間・休日作業等の活用）
- ✓ 作業に伴う影響範囲及び事前周知・調整方法

５-１-５ 移行対象及び移行手順

- ✓ 移行対象（ネットワーク機器、端末、アカウント、データ等）の整理
- ✓ 各対象ごとの移行手順及び優先順位の提案
- ✓ 大規模環境を考慮した拠点単位・段階的移行計画

※NAS データ移行作業は教職員を想定

５-２　運用保守要件

５-２-１運用体制

(1)運用統括者

運用の全体統括者を設置すること。全体統括者はシステム運用状況について、発注者に定期的な報告を行うとともに、システムの維持・向上を図るため、継続的な運用改善の提案を行い、発注者の承認を得た改善策を推進させること。

(2)運用要員

学校現場の状況及びネットワーク環境に精通した専任担当者を設けること。また、運用保守業務の実施にあたり、常駐、巡回訪問、リモート対応等を含めた最適な運用体制を提案すること。

５-２-２運用保守設計

県にとって最適な運用保守設計を行い、県と協議の上決定すること。なお、県が想定している運用保守設計範囲は下記のとおりである。

① 障害対応：障害発生時の迅速な復旧手順、代替手段の確保
② 監視体制：24 時間監視、アラート通知、ログ収集・分析
③ セキュリティインシデント対応：検知・報告・復旧のプロセス整備
④ SLA 定義：本環境整備全体でのサービスレベル
⑤ 端末・ソフトウェア保守：OS 及びソフトウェアのセキュリティパッチ適用、OS 及びソフトウェアのバージョンアップ等
⑥ 研修・定例会：教職員向け操作研修、簡易マニュアル提供、定例会における運用状況、問合せ傾向、学校現場の課題及び改善提案の報告
⑦ 問合せ・インシデントの蓄積・展開：FAQ 作成、利用者への公開環境の構築、問合せ対応経過の記録、学校現場の困り感や要望の把握、複数校で共通する課題の整理
⑧ ドキュメント類整備：利用者用マニュアル、管理者用マニュアル
⑨ 運用改善に向けた県へのフィードバック：問合せ、インシデント、要望等の蓄積情報をもとに、学校現場における課題を分析し、県教育委員会の判断を要する事項、追加対応が必要と考えられる事項、設定・運用ルール・周知・研修等の改善が必要な事項を整理し、定例会等で報告すること。

５-２-３障害対応

(ｱ) 障害対応マニュアルを作成の上、障害発生の際には、マニュアルに基づき対応すること。
(ｲ) 障害が発生した場合は、本システムの緊急停止、ログの取得及び保全等の初期対応を適切に行うこと。
(ｳ) 併せて、関係者へ連絡調整を行うとともに、障害箇所の特定、進捗管理を行い、同様な障害が再発しないよう対応すること。また、各種ソフトウェアやデータの復旧作業を行うこと。
(ｴ) 対応終了後は、再発防止策について、遅滞なく文書にて報告すること。また、内容については、対応マニュアルに反映させるとともに、関係者に対しても障害が発生した経緯及び今後の対応について説明を行うこと。
(ｵ) 障害対応については、検知後 1 時間以内に初期対応（影響範囲の特定、関係者への通知、

応急措置等）を開始すること。

(ｶ) 障害対応については、SLA 項目として具体的に提案すること。

(ｷ) 不測の事態に備えて、検証や対策のための環境や体制を整えること。

(ｸ) 現地での対応が必要な場合は、現地に作業員を派遣すること。

(ｹ) 問合せ対応業務の対応経過について、一案件ごとに必要な項目を記録し、全件蓄積・保管すること。また定例会にて報告すること。

(ｺ) クラウド利用である利点を活かしたリモート保守を原則とし、軽微な障害・問合せ等について迅速な対応を実施すること。

(ｻ) クラウド環境のリモートサポート内容として、以下 5-2-5 リモート監視等を実施すること。ただし、セキュリティレベル維持のため、一部の作業については発注者と協議のうえで実施すること。

(ｼ) 流用した既存設備（主に SW、LAN 配線、ハブボックス等）物理的な故障に伴う、交換機器の調達費用及びオンサイト交換作業費用については、都度精算を行い、請求できるものとする。

5-2-4 OS/ソフトウェア保守/アカウント

(ｱ) 端末の OS セキュリティパッチ適用管理を行うこと。

(ｲ) 端末の OS 及びソフトウェアに重大な影響を与える脆弱性が見つかり、かつ、その対応が緊急を要する場合は、協議の上、必要な緊急更新ファイルの適用作業を速やかに実施すること。

(ｳ) 端末の OS 及びソフトウェアのバージョンアップが必要な場合は、県教育委員会と協議の上で実施すること。OS やソフトウェアの購入費用は含めないこととする。

(ｴ) 本システムで提供されるクラウドサービスに OS 及びソフトウェアの脆弱性対応やバージョンアップが含まれていない場合、受託者で実施する費用を運用保守費用に含めること。

(ｵ) 本システムで用いる各種証明書がサポート終了とならないように管理すること。

(ｶ) 本システムで用いる証明書の取得費用及び更新費用は運用保守費用に含めること。

(ｷ) 年度移行に伴い人事異動や組織変更が発生するが、年度更新作業が発生する場合は、作業費用を見込むこと。なお人事異動・組織変更に伴う更新作業については本県からのデータ受領後、短期間（3 日程度を目安）で完了するように実現方法、支援体制等を提案書に記載すること。

(ｸ) システムメンテナンスについて、利用者に影響のあるシステムへのメンテナンスは、可能な限り業務影響がない時間帯で実施すること。

(ｹ) 年度末・年度始めの異動・進学処理において、受託者のヘルプデスクが代行作業を契約内で請け負うスキームを用意すること。

5-2-5 リモート監視等

(ｱ) 受託者はリモート監視を行うこと。リモート監視の実施拠点においては適切なセキュリティ対策が行われていること。

(ｲ) 障害の検知・障害原因の調査を実施し、メーカ等と連絡・協議を行い、速やかに問題解決・障害復旧を実施し、障害対応記録を発注者へ報告すること。また，平日 9:00～17:00（土日祝日、年末年始（12/29～1/3）を除く）おいては，システム障害認知後，６時間以内を目標にサービス復旧を行うこと。

(ｳ) なお、事後対策が必要な場合は、障害内容に応じて発注者承認の上，事後対策を実施すること。

5-3　統合ヘルプデスク要件

5-3-1 統合ヘルプデスクの設置

統合ヘルプデスクを設置すること。原則 ICT すべての問合せの一次窓口となることを想定している。統合ヘルプデスクは、単なる問合せ受付・回答窓口に留まらず、学校現場から寄せられる困り感、要望、運用上の課題を把握し、県教育委員会が必要な改善判断を行えるよう、問合せ内容を記録・整理する役割を担うこと。

特に、複数校で共通して発生している課題、学校 ICT 担当者の負担増につながっている課題、県の判断を要する課題については、県教育委員会へ報告・共有すること。

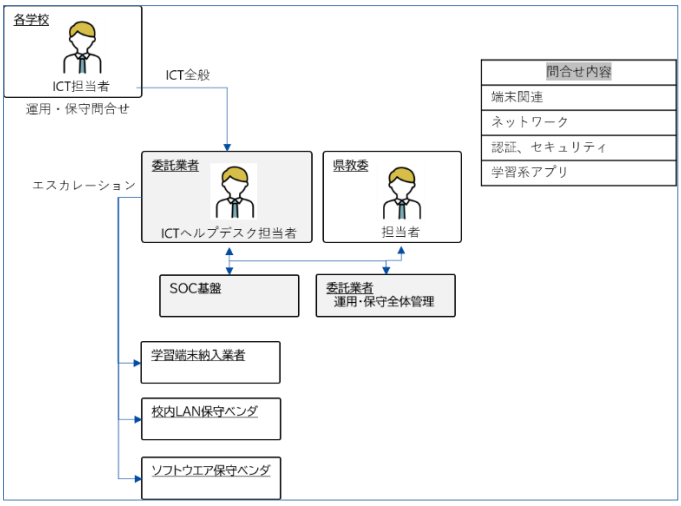


図　3-1　統合ヘルプデスクイメージ

① 平日 9:00～17:00（土日祝日、年末年始（12/29～1/3）を除く）までは、電話又はメール、チャット等で受付対応すること。

② 上記対応時間外について、メール問合せであれば、24 時間 365 日対応すること。ただし、時間外に受け付けた問合せの対応については、翌営業日以降とする。

③ 教職員端末の保守対応を行うこと。（必要に応じて端末メーカとのやり取り含む）

④ 上記以外の問合せで、本契約外に関するものは、可能な限り問合せ先を案内すること。

⑤ BYOD（教職員及び生徒の私物端末）に関するヘルプデスクのサポート範囲は、指定の『ネットワーク接続手順書（マニュアル）』の提供及びマニュアル記載事項の説明に留めるものとする。個別の私物端末の OS 設定、不具合調査、操作代行等はサポート対象外とする。

5-3-2 システム運用時間

(ｱ) 本システムの運用時間については、計画停止を除き、24 時間 365 日常時稼働すること。特に平日 9:00～17:00（土日祝日、年末年始（12/29～1/3）を除く）はユーザに対して原則無停止のサービスとすること。

(ｲ) メンテナンス等でシステム停止が必要な場合は、原則 1 ヶ月前までにその方法、頻度、必要な停止時間を県と協議すること。

(ｳ) 緊急時の対応及びシステム停止については、随時、県と協議すること。

5-3-3 セキュリティインシデント監視

(ｱ) 受託者はクラウド環境及び端末でのインシデント発生の監視を 24 時間行うこと。
(ｲ) セキュリティインシデントの重要性や影響度を加味して、優先度を定義し、連絡体制を整備すること。
(ｳ) 群馬県教育委員会の教育情報セキュリティポリシーに準拠した形で、対応フローを事前に定義すること。
(ｴ) 重大なセキュリティインシデントが発生した場合は、1 時間以内に事前に取り決めたフローに従い、県教育委員会に連絡すること。また、事前の定義したフローに従い、対処を行うこと。

5-3-4 情報セキュリティ管理

(ｱ) 本システムのアクセスログ、システムログ、監査ログ等を収集し、少なくとも半年間は保管すること。また、必要に応じて調査・分析し、インシデントの有無や対応等について報告するなど、適切なセキュリティ対策をとること。
(ｲ) システム障害や事故・事件、セキュリティインシデント等の発生時等には、収集した各種ログデータ等の調査・分析を行い、原因究明等を行うこと

5-3-5 定例会

(ｱ) 毎月 1 回の定期運用・保守報告会を開催し、作業実績、各監視状況等報告、今後の計画、課題等を報告すること。
(ｲ) 会議後は議事録を作成し、 1 週間以内に県に提出し承認を得ること。

5-4 マニュアル・研修要件

5-4-1 マニュアル

本システムの運用及び利用に必要な各種マニュアルを作成し、電子媒体にて提供すること。
マニュアルは利用者の役割に応じて作成し、少なくとも以下を含むこと。

(ｱ) システム管理者向け運用マニュアル
(ｲ) 学校 ICT 担当者向け運用マニュアル
(ｳ) 一般利用者向け操作マニュアル

マニュアルは編集可能な形式及び PDF 形式で提供すること。
記載内容は利用者が理解しやすい表現とし、専門用語を使用する場合は用語説明を付すこと。
また、利用者が必要な情報を容易に参照できるよう、目次、検索機能又はリンク機能等を備えた電子マニュアルとして提供すること。

5-4-2 研修

受託者は、本システムの円滑な導入及び運用開始を目的として研修を実施すること。
研修対象者及び回数、実施方法については提案によるものとするが、少なくとも以下の内容を含めること。

(ｱ) システム管理者向け研修
(ｲ) 学校 ICT 担当者向け研修

（ｳ） 一般利用者向け研修

研修は対面方式、オンライン方式又は両方式の併用を可能とし、研修資料を提供すること。

また、欠席者や後任者への展開を考慮し、研修資料及び研修動画の提供可否について提案すること。

第６章 追加提案事項

６-１　追加提案

本書記載の要件以外にも県教育委員会及び教職員の業務効率化、利便性向上、セキュリティ向上、運用負荷軽減並びにコスト最適化に資する提案があれば積極的に提案すること。

また、本 RFI において明示的に要件化していない事項についても、システムの可用性向上、事業継続性の確保（BCP）、災害対策（DR）、バックアップ、冗長化、サイバー攻撃対策、将来的な拡張性の確保等の観点から有効な提案がある場合は、その実現方法、期待効果、概算費用及び前提条件を含めて提案すること。