次期教育情報システム詳細設計・

開発・運用保守業務委託仕様書

令和7年5月

佐賀県教育委員会事務局
教育DX推進グループ

目次

第1章 総論

1.1 本業務の背景

本県では、教職員の業務効率化および負担軽減を目的として、平成 24 年度より校務支援システムを導入しており、現在は平成 30 年に整備した「教育情報システム」が稼働している。

しかしながら、学習系と校務系のネットワークが分離されているため、データの連携や利活用が進まず、生徒への適切な指導や評価などに十分活かされていないのが現状である。

また、校務用パソコンは学校内など固定された場所でしか使用できず、柔軟に校務を処理できないなど、ICT 活用を前提とした教育活動や GIGA スクール時代の教育 DX の流れに十分対応しきれていないという課題がある。

文部科学省では、GIGA スクール構想を踏まえ、令和 6 年 1 月に「教育情報セキュリティポリシーに関するガイドライン」（以下「ガイドライン」という。）を改訂し、クラウドサービスの利活用を前提とした目指すべき構成を明確化した。

また、「GIGA スクール構想の下での校務の情報化の在り方に関する専門家会議」においては、「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」（以下「提言」という。）が取りまとめられている。

こうした背景を踏まえ、本県においても、上記ガイドラインや提言に基づき、統合型認証基盤を活用したゼロトラストアーキテクチャを取り入れた業務環境を構築し、校務系と学習系のネットワークを統合することで、校内外を問わず安全に校務・学習システムを利用できるようにし、円滑な教育活動の実現を目指すものである。

さらに、本県では Society5.0 時代を見据え、目指す学びの姿として「誰もがいつでもどこでも誰とでも自分らしく学ぶことができる子ども主体の学び」を掲げ、その実現に向けて「教育 DX プロジェクト」を推進している。

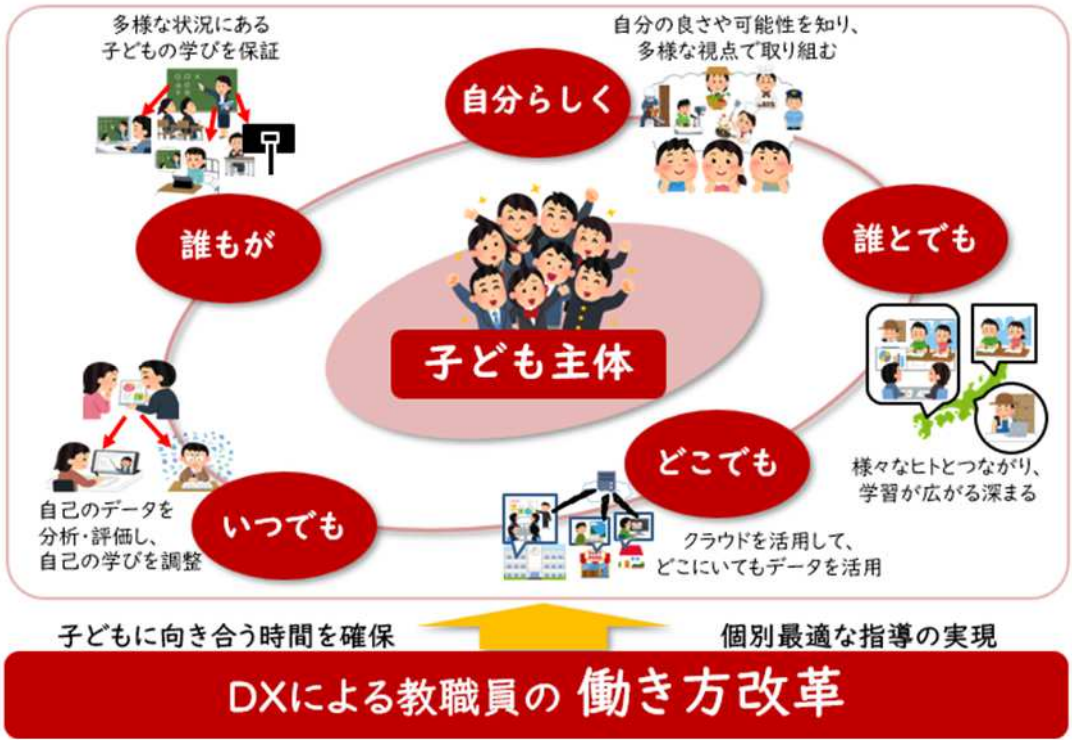


図 佐賀県の教育DXプロジェクト

次期システムは、この将来像のとおり特に【子ども主体の学び】【教職員の働き方改革】を具現化するうえで大きな役割を担うものと、本県は位置づけている。

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」公表について（令和 7 年 3 月時点）

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

1.2 本業務の目的

本業務は、令和8年度に利用期限を迎える教育情報システムおよび周辺インフラ（ネットワーク、セキュリティ等）の更新に向けた詳細設計・開発構築と、その後5年間にわたる運用保守業務を委託するものである。

あわせて、本県が掲げる教育ビジョンである「子どもの主体的な学び」および「教職員の働き方改革」の実現を目指す。

本事業を実現するにあたり、構築・運用保守費用の最小限化を前提としつつ、確実かつ円滑に推進できる事業者を選定するため、総合評価一般競争入札方式を採用し、広く事業者を募集したうえで総合的に評価し、決定するものとする。

1.3 用語の定義

用語の定義について「表1-3-1用語の定義」に示す。

No	用語	意味
(1)	佐賀県教育ネットワーク	佐賀県内の県立学校46校他を結ぶWANおよび県立学校内のLAN並びに教育情報システム、インターネット回線等を含めたネットワークの全体の総称。
(2)	校内LAN	佐賀県内の県立学校46校において、各学校の校務に用いる情報端末及び教職員や生徒が利用する学習指導・学習活動のための情報端末等が接続、もしくは今後接続が予定されているネットワークであり、情報通信技術を効果的に活用した学校教育と学校運営を実現する学校情報化の基盤。
(3)	公共ネットワーク	本庁、佐賀県立学校、現地機関、警察庁舎、市町および消防本部(局)を結ぶワイド・エリア・ネットワーク。
(4)	校務系ネットワーク	県立学校教職員ならびに県教委職員が利用し、主にドキュメント重要性分類Ⅰ～Ⅱを取り扱うネットワーク。
(5)	事務系ネットワーク	県立学校教職員ならびに県教委職員、市町教委職員、市町立学校教職員が利用し、主にドキュメント重要性分類Ⅱ～Ⅲを取り扱うネットワーク。
(6)	公開系ネットワーク	県立学校教職員ならびに県教委職員、市町教委職員、市町立学校教職員が利用し、主にドキュメント重要性分類Ⅳを取り扱うネットワーク。
(7)	学習系ネットワーク	県立学校教職員ならびに県立学校生徒が利用し、主にドキュメント重要性分類Ⅲ～Ⅳを取り扱うネットワーク。
(8)	公衆無線LANネットワーク	学校無線アクセスポイントで災害等の非常時に公開するネットワーク。
(9)	LGWAN系ネットワーク	県立学校の管理職(校長・教頭等)、事務職員及び県教委職員(本庁)が行政事務で利用するネットワーク
(10)	管理系ネットワーク	機器の運用管理・監視等で使用するネットワーク。
(11)	校務系端末	県立学校の教職員が事務処理や校務で利用している端末。 ※県調達及び学校調達は問わない
(12)	学習系端末	県立学校の教職員及び学習者が学習において利用している物理端末。 ※県調達及び学校調達は問わない
(13)	教育情報システム(SEI-Net)	佐賀県立学校の教職員および生徒が利用するシステム。 市町立学校においても一部利用している。 校務管理、学習管理および教材管理等の機能を主体として複数の機能を有した総合システム。

（14）	次期教育情報システム （次期システム）	本業務で詳細設計、構築、運用を行う佐賀県立学校の教職員および生徒が利用するシステム。 市町立学校、市町教育委員会は事務系システムと学校HP（学校CMS）を一部利用する予定。 校務管理、学習管理および教材管理等の機能を主体として複数の機能を有した総合システム。 本仕様書では以下「次期システム」と標記する。
（15）	校務支援システム	生徒の学籍情報や成績情報などを取り扱う校務業務を支援するシステム。
（16）	事務システム	文書決裁、文書管理、事務連絡等で使用される教職員向けのシステム
（17）	学校CMS	各学校の行事や周知、合格発表などを掲載するホームページ。
（18）	ポータルサイト	教職員、県立学校生徒、生徒保護者に提供し、各システムのリンクや行事予定等を提供するWebサイト。
（19）	ダッシュボード	県立学校教職員、県立学校生徒/保護者、県教委に提供し、学習者情報などを集約ならびに視覚化するWebサイト。
（20）	教職員マネジメントシステム	教職員の服務情報や出退勤情報を取り扱う教職員課管轄システムの総称。
（21）	知事部局システム	佐賀県の知事部局が運用管理を行うシステムの総称。
（22）	レベルⅠデータ	現行システムの定義かつ主に生徒関連データ。
（23）	レベル2データ	現行システムの定義かつ主に教職員の事務関連データ
（24）	レベル3データ	現行システムの定義かつ主に一般データ、学習データ。
（25）	ドキュメント重要性分類Ⅰ	セキュリティ侵害が教職員又は生徒の生命、財産、プライバシー等へ重大な影響を及ぼす分類のドキュメント。
（26）	ドキュメント重要性分類Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす分類のドキュメント。
（27）	ドキュメント重要性分類Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼす(Ⅱ以上を除く）分類のドキュメント。
（28）	ドキュメント重要性分類Ⅳ	セキュリティ侵害が発生しても学校事務及び教育活動の実施に影響をほとんど及ぼさない分類のドキュメント。
（29）	パブリッククラウド	仮想マシンやCMSを構築する基盤を、インターネットを通じて提供されるサービス。
（30）	ゼロトラストネットワーク	全てのアクセスを信頼せず、認証と検証を徹底するセキュリティモデル。
（31）	SASE（SSE）	ネットワークとセキュリティを統合し、クラウドベースで提供するアーキテクチャ。

（32）	SaaS	インターネット経由で利用可能なソフトウェアサービス。
（33）	県庁	佐賀県庁を指す。
（34）	市町	佐賀県内にある20団体の市町に対する総称
（35）	県教委	佐賀県教育委員会を指す。
（36）	市町教委	市町の教育委員会を指す。
（37）	教育センター	教員の研修や教育支援を行う専門機関（組織としては佐賀県教育委員会に含む）。 教材開発や教育相談も実施する。
（38）	データセンタ	運用監視やサーバなどを配備している場所。

第2章 現行業務及びシステムの状況

2.1 現行システムの状況

2.1.1 現行教育情報システムの概要

現在稼働している教育情報システムは、教職員が利用するシステムとして平成 30 年度に構築し、令和2年度より本運用を開始したものである。同システムは、教職員にそれぞれ固有の ID を付与し、ブラウザからログオンして使用するウェブシステムであり、校務系機能や学習系機能を中心に複数の機能を統合したシステムとして、佐賀県教育ネットワーク上のデータセンタに配置されている。

また、同システムは県立学校のほか、市町立学校や教育委員会等でも利用しており、県立学校においては各校に整備されている校内 LAN を介してアクセスしている。

一方、市町立学校の場合は、公共ネットワーク接続またはインターネット接続のいずれかを利用してシステムにアクセスしている。ただし、市町によっては同システムの利用状況に差異があり、独自に校務支援システムを整備している場合もある。

教職員は、生徒に係る校務を教育情報システムの校務機能で処理しており、生徒の出席状況や時数管理などの日々の業務、成績表（通知表、指導要録等）の学期ごとの業務、考査や入学・卒業、進級、クラス替えなどの年度ごとの業務を行っている。その他、学校ホームページの作成・公開・管理やスクールニュース（保護者向け緊急情報配信）、学校行事の管理、教育委員会や学校間での文書送受信など、生徒に直接関わらない事務的業務も同システムで実施している。

さらに、教育委員会の他所属システム（保健、服務、出退勤等）や知事部局のシステム（旅費等）、その他外部システム（教職員向けシステム等）についても、教育情報システムを経由して利用している。

県立学校の教職員には、校務系端末に加えて学習系端末も割り当てられており、教職員は校務系機能を利用する際とは別に付与された固有のIDを使用して学習端末にログインし、学習系機能を活用している。

2.1.2 現行教育情報システムの構成

教育情報システムの各サーバはデータセンタの仮想基盤上に構成されている。

教育情報システムのシステム概要図は以下のとおりである。

この構成において、ハードウェア、ソフトウェア、ネットワーク、データ配置、システムインフラ等をすべて運用している。

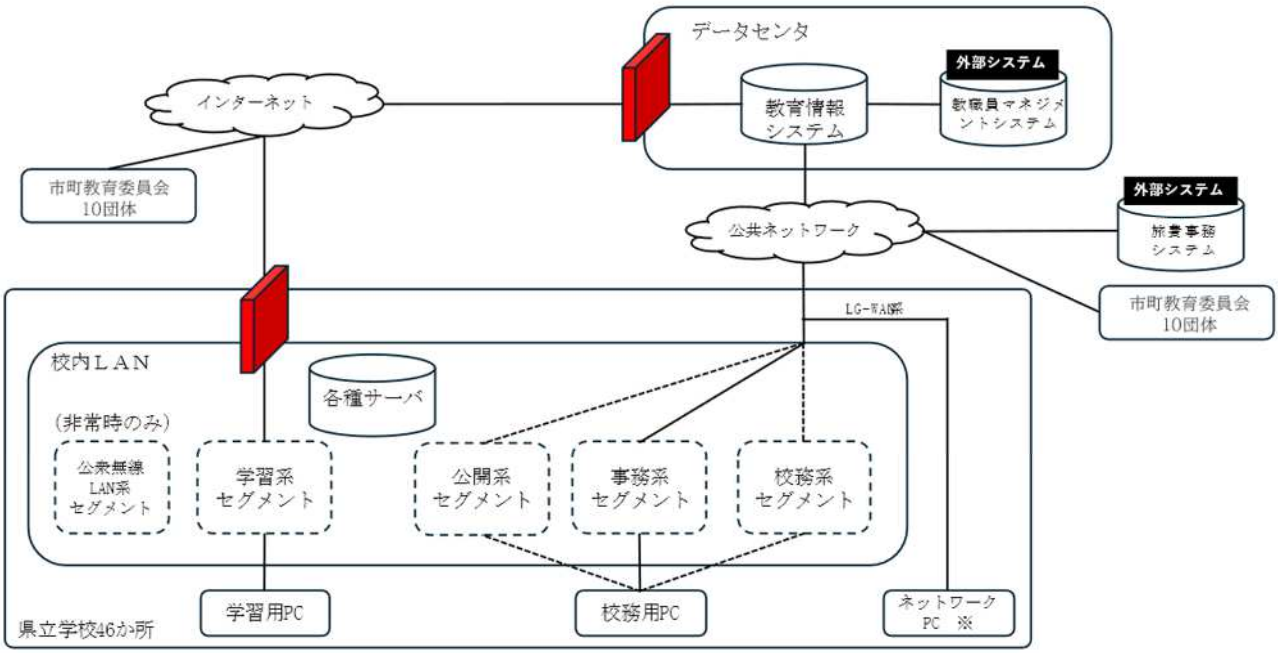


図　佐賀県教育ネットワーク等全体図（概略）

また、教育委員会、学校現場における機器故障対応やセキュリティ対応等の運用保守稼働を集約し最小限となるように構成している。

なお、詳細の把握に現行の設計資料等の必要な資料については、別途詳細資料等を閲覧する機会を設ける。

2.1.3 現行システムの利用状況

教育情報システムは、県内全ての県立学校及び市町立学校での利用実績がある。

システム機能別の利用状況は下記に示すとおりである。

なお、県立学校には、特別支援学校及び通信制学校も含んでいる。

(1) 校務系機能の利用状況

校務系機能は、県立学校や一部の市町立学校の教員が利用している。また、校務系端末から仮想デスクトップ（VDI）を用いて機能を利用しており、同時接続数は約2,000となっている。

なお、市町立学校の校務系機能の利用は、情報セキュリティの観点から公共ネットワークを経由してシステムに接続できる学校にのみ機能を提供している。

(2) 事務系機能の利用状況

事務系機能は、県立学校と市町立学校の教職員が利用しており、利用可能者数は約9,000人である。

また、県立学校と公共ネットワークに接続された市町立学校は校務系端末からブラウザ経由で事務系機能を利用しているが、公共ネットワークに接続していない市町については、インターネットから仮想デスクトップ（VDI）を用いて機能を利用している。

なお、事務系機能の利用に係る仮想デスクトップ（VDI）の同時接続数は約500となっている。

(3) 公開系機能の利用状況

公開系機能は、県立学校の教職員が利用しており、公開の利用可能者数は約2,800人であり、校務系端末から仮想デスクトップ（VDI）を用いて機能を利用している。

なお、公開系機能の利用に係る仮想デスクトップ（VDI）の同時接続数は約500となっている。

(4) 学習系機能の利用状況

学習系機能は県立学校の教員及び生徒が利用しており、利用可能者数は生徒約20,000人、教員約2,800人であり、教職員及び生徒が使用する学習系端末や電子黒板を用いて利用される。

(5) 利用対象者

現行システムにおける利用対象者は、市町立学校の教職員ならびに市町教委職員、県立学校の教職員、県教委職員、県立学校の生徒である。

2.2 次期システムにおいて特に解決を要する現状の課題

教育委員会が現在捉えている解決を要する現状の課題を以下に記載する。

なお、受託者は以下課題も意識し本委託業務に取り組むこと。

方針	区分	課題	現状 ※一部の学校のみの場合あり
【子ども主体の学び（協働的な学び）】	端末	学校間の端末持ち歩き（生徒・教職員）	生徒が他県立学校のネットワークで学習系端末を利用できない。 教職員が兼務校のネットワークで校務系端末を利用できない。
	アカウント	IDの一元管理（学習系・校務系）や認証の強化・効率化	学習系と校務系でIDが異なる。他にも各ソフト別にIDがある。
	ネットワーク	ネットワークの遅延	クラウドサービス利用時にネットワークの遅延が発生
【教職員の	ソフト	先生間の校務・授業等の予定の見える化	ホワイトボードや管理職のみ把握

働き方改革】		文書管理機能の強化（ワークフロー、供覧機能等）によるペーパーレス化の推進	紙中心の供覧・決裁
		校務系による保護者との連携（出席・アンケート取得）	電話または学習系で受付
		校務系による生徒との連携（お知らせ、成績、学習状況等）	紙や学習系でお知らせ
		各機能の業務上の効果及び利用方法・手順が理解されていない	文書による周知マニュアル等の統一的な保管場所は無い
	その他	事務室職員の事務系・校務系における校務業務支援	実施できない
【その他】	運用保守	各学校単位のサーバの廃止（ファイルサーバ、AD 等）	各学校のサーバ室で稼働中
		端末の年度更新作業の効率化	2週間～1カ月程度引き取って更新作業
		市町立学校や県立学校に提供する機能の再定義	各機能の利用にムラがある
		人事異動処理の効率化・高速化	1～2週間端末更新に時間を要する場合あり
		クラウドアプリ等のシステムの追加作業の簡素化	追加時に作業費用を要す場合が多い

なお、これらの課題を含め、基本設計等で顕在化した個別課題を含め、全体課題表及び基本設計からの申し送り表として作成している。資料については、別途詳細資料等を閲覧する機会を設ける。

第3章 本業務の概要

3.1 件名

次期教育情報システム詳細設計・開発・運用保守業務委託契約

3.2 契約方法

総合評価一般競争入札

3.3 履行期間

履行期間は契約締結日～令和 14 年 3 月 31 日とする。

詳細な工程は下表のとおり。

No.	委託内容
1	システム詳細設計業務 -インフラシステム（NW、セキュリティ、クラウド基盤）設計 -校務支援システム設計 -事務系システム設計 -学習公開系システム設計 -セキュリティポリシー改定対応
2	システム開発業務 -開発環境構築 -テスト環境構築 -プログラミング対応 -単体テスト -結合テスト -システムテスト -受け入れテスト
3	環境構築業務: -サーバ構築 -ネットワーク構築 -データベース構築 -ミドルウェア構築 -セキュリティ設定 -端末設定
4	環境移行業務: -移行計画策定 -データ移行 -システム移行リハーサル

	-移行後テスト稼働 -システム移行本番（並行稼働期間あり）
5	システム操作研修: -研修資料作成 -研修実施 -質疑応答対応 -研修効果測定
6	ライセンス調達: -開発用ライセンス調達 -本番用ライセンス調達
7	運用保守業務: -システム監視対応 -セキュリティインシデント対応 -運用操作問い合わせ対応 -システム障害対応 -脆弱性・セキュリティパッチ適用対応

3.4 本業務の範囲

本業務の範囲は以下のとおりとする。

(ア) 本業務に係るプロジェクトの推進及び全体管理（進捗管理、課題管理等を含む）
(イ) 各種打合せおよび検討事項への実施・進行・助言・提案
(ウ) 統合認証基盤およびセキュリティサービスの設計・導入
(エ) パブリッククラウド型の校務支援・事務アプリケーションの設計・導入
(オ) ポータルサイト、ダッシュボードの設計・導入
(カ) ネットワーク環境の設計および構築
(キ) 県立学校の回線調達および環境の設計・導入
(ク) 校務系端末・学習系端末等の設計・設定
(ケ) 次期システム構築後の各種動作試験
(コ) 現行システムから次期システムへの移行計画および移行作業
(サ) セキュリティポリシーを含む各種運用ルールの策定に係るアドバイス
(シ) 各種マニュアルの作成
(ス) システム利用者および運用保守管理者への研修
(セ) 運用保守業務
(ソ) 運用終了後に必要となるデータ移行・消去、システム等の廃棄に係る業務

その他、本県がゼロトラスト環境を構築する上で、提案事項があれば提示すること。

なお、次期システムの各機能の詳細要件を、「第4章次期システムの詳細要件」に記述し、各工程における業務の詳細を「第5章委託業務詳細」に記述する。

3.4.1 資料開示の制限事項

本業務は、ゼロトラストネットワークに関する高度なセキュリティ要求を満たすため、詳細な設計仕様や技術的要件については、本県と秘密保持契約書を締結した事業者のみに開示するものとする。

これは、セキュリティ上の観点からの情報保護を目的としているため、事業者は開札後に速やかにデータを廃棄することとする。

なお、本県のセキュリティポリシーについては、受託事業者のみに開示する。

3.5 本業務の方針

校務DXを取り入れた教育活動の実現、ならびに文部科学省ガイドラインや提言に基づき、佐賀県が進める教育DXプロジェクト及び文部科学省が示す校務DXの方向性から、県では次期システムのコンセプトを以下のとおり設定し、これを目指す要件定義や基本的な構成の設計を行ってきた。

本業務では、以下を実際に構築し、運用する。

(1) 次世代の校務 DX

①校務系ネットワークと学習系ネットワークの統合による教職員端末の1台化

現行では、教員は校務系端末と学習系端末の2台の端末を持ち、用途によって使い分けている状況であるため、校務系と学習系のネットワーク統合を図り、教職員端末の1台化を実現する。

②校務支援システム及び周辺システムのクラウド化

現行では、一部のシステムは学校内のサーバで稼働しており、生徒の学ぶ場所や教職員の働く場所が制限されているため、校務支援システムや周辺システムのクラウド化を実現し、場所の制限を解消する。

③教職員のテレワーク

現行では、教職員向けのテレワーク環境は整備されておらず、働く場所は学校内に制限されているため、テレワーク環境を整備し、教職員の柔軟で多様な働き方を実現する。

④ダッシュボード機能による学習・指導の支援

現行は、校務データや学習データを可視化・分析するツールがなく、データの整理に時間を要し、また、成績情報等を有効活用できていないため、各データの可視化ツールである“ダッシュボード機能”を実装し、データ整理の省力化と、生徒や保護者、教員が各データを活用できる環境を整備する。

⑤ゼロトラストによるセキュリティ対策

現行は、境界型セキュリティが導入されており、利便性の低下や業務の硬直化等を発生させているため、ゼロトラスト型セキュリティを導入し、セキュリティを強化と利便性の両立を図る。

(2) その他次期システムで導入・連携する機能

次期システムにおいて導入・連携を検討する機能等について、以下に示す。

・校務データと学習データの連携機能
・ダッシュボードシステム（教育委員会、教職員、生徒）
・コミュニケーションツール（Teams、Zoom、SNS等）
・デジタル採点システム
・ポータルサイト（教育委員会、教職員、事務室、生徒（eポータル）、保護者）

・オンライン授業配信システム
・教育情報サイト、学習コンテンツ（MEXCBT、学習ドリル）

また、各学校において利用している外部システムは今後も利用できるようにすること、今後接続予定のシステムは随時運用保守の範囲内で接続後利用できること。

(3) 現行機能及び外部システムとの連携

前提として、現行の教育情報システムの校務・事務・学習等の各機能、関連のツール・ソフト等は引き続きこれまでと同等に利用できること。

また、教育委員会の他所属のシステム（保健、服務及び出退勤等）や知事部局のシステム（旅費等）やその他外部システム（感染症管理等）も次期システムを経由して利用できること。

(4) 現行機能の拡充と課題解決

2.2 次期システムにおいて特に解決を要する現状の課題で前述したとおり、基本設計等で顕在化した個別課題を含め、現行の機能における機能拡充の要望や改善の要望を課題としてまとめているため、次期システム構築にあたって改善を図ること。また改善内容については本県へ説明ならびに協議の上で実施すること。資料については、別途詳細資料等を閲覧する機会を設ける。

(5) 運用状況の見える化・セキュリティ障害検知自動化による運用・保守対応の精度向上

次期システムの構成においても、それぞれのシステムで警報があった際、運用保守ベンダにて警報などを取りまとめた上、事象・対処方法等の情報を迅速に教育委員会に報告するような仕組み・体制となるよう運用・保守業務のあり方を設計する。

また、端末・システム・ネットワーク等の状況を見える化、セキュリティ障害や侵害に対して、検知・対象の端末の切り離し等を一定程度自動化、運用・保守対応の対応精度や障害後の分析・報告速度の向上を図る。

そして、システム運用において、教職員への運用負荷の軽減、保守において、システム故障時の早期復旧による学校業務への影響の軽減を実施する。

3.6 実施スケジュール

現行システムの利用期限は令和9年3月末となっており、令和9年4月から次期システムの運用を開始する必要があるため、以下の要件を設ける。

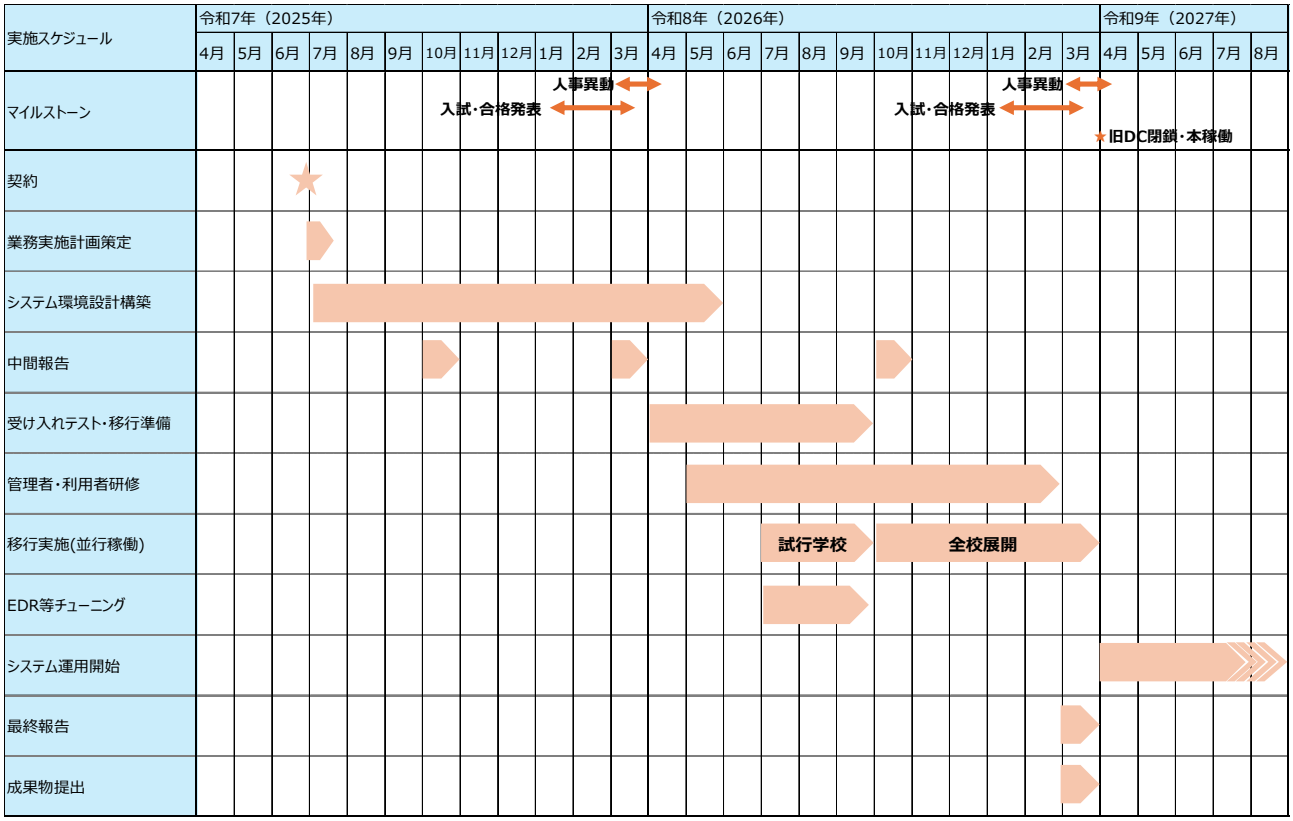
①令和8年9月末までに次期システム環境の構築を行い、移行が開始できる状態とすること。
ただし、令和8年7月頃から一部の県立学校において次期システム環境の試験運用を行うことに留意すること。

②令和8年10月より次期システムへ移行を開始し、令和9年3月末には移行が完了できること。

③令和9年4月より現行システムと切り離し、知事部局等の他システムを含めて、すべて次期システムによる利用開始ができること。

なお、本県で想定しているスケジュールは下図のとおりであるが、あくまでも例示であるため、上記要件を満たせる最適な提案を行うこと。

＜想定している実施スケジュール（例示）＞

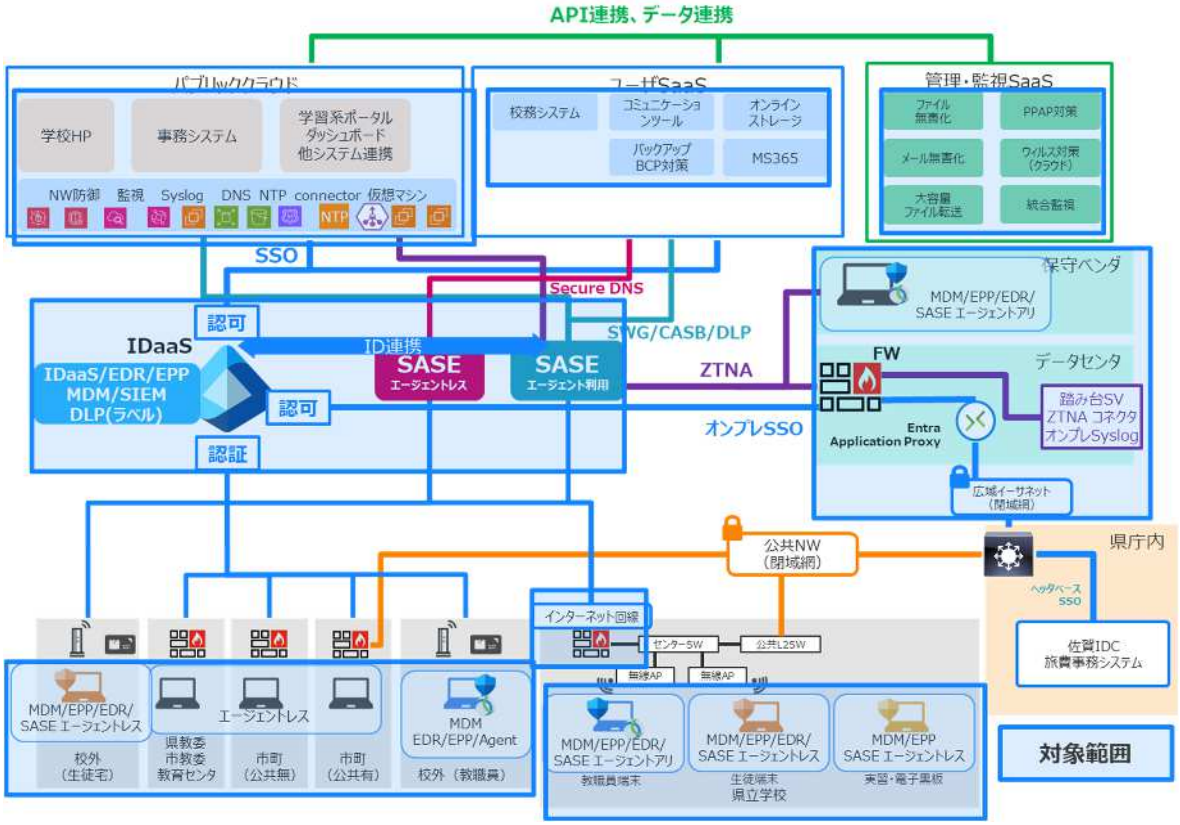


※各ステークホルダへの移行に伴う説明や、設計のヒヤリング、機能確認などについては、順次必要に応じて計画と実施を行うこと。

3.7 次期教育情報システム構成

3.7.1 全体構成

本調達業務で導入するシステムの全体構成イメージを下図に示す。



システムの全体構成イメージに示した対象範囲の全て（ハードウェア、ソフトウェア、ネットワーク、データ配置、システムインフラ）を今回の業務の対象範囲としている。

ただし、市町など県管轄ではない端末のエージェントレスについては端末の設定変更は実施せず、アカウントの適用やクラウド側での設定対応を前提とする。

なお、詳細は外部設計書を確認すること。

更に、全体構成図については以下の点に留意すること。

①上記で示した対象範囲については主に機器導入が必要な意図として記載しており、運用開始後は県立学校の無線AP、各種スイッチやネットワークも含めて運用や保守の対象とすること。

②公共NW（ネットワーク）については、知事部局の回線のため保守の必要はないが、運用事業者からの運用状況（障害発生、点検等による不通等）の情報収集と県への情報提供を適切に実施すること。

③既存システム環境のうち、引き続き活用する機器がある場合は、既存事業者と主体的に協議を行い調整すること。

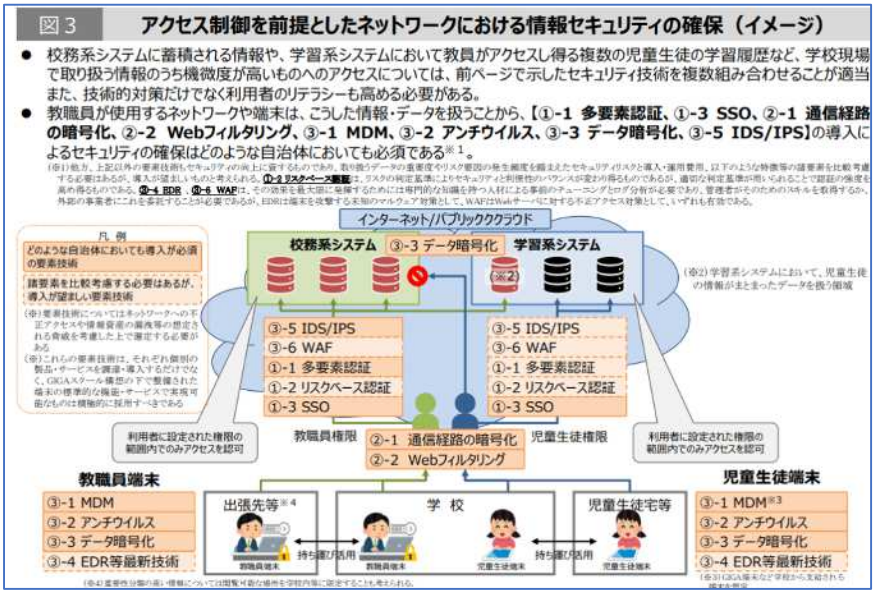
④教育DX推進グループ内やヘルプデスク受託事業者に設置・保管されている校務系端末や学習系端末について、次期システム接続に係る設定変更等の必要な対応を行うこと。

第4章 次期システムの詳細要件

4.1 詳細設計・構築要件

委託対象として構築する次期教育情報システムは、教職員および生徒が利用するものであり、各端末環境・ネットワークシステム環境・アプリケーション環境について、文部科学省が示すネットワーク構成イメージ（下図参照）に沿ったゼロトラスト環境を構築すること。これは、セキュリティの強化や校務DXの推進による教職員の業務負担軽減、ならびに生徒の主体的な学びを支援するためである。

また、環境構築後には、運用保守に向けて各種運用ルールの策定について主体的に支援を行うこと。



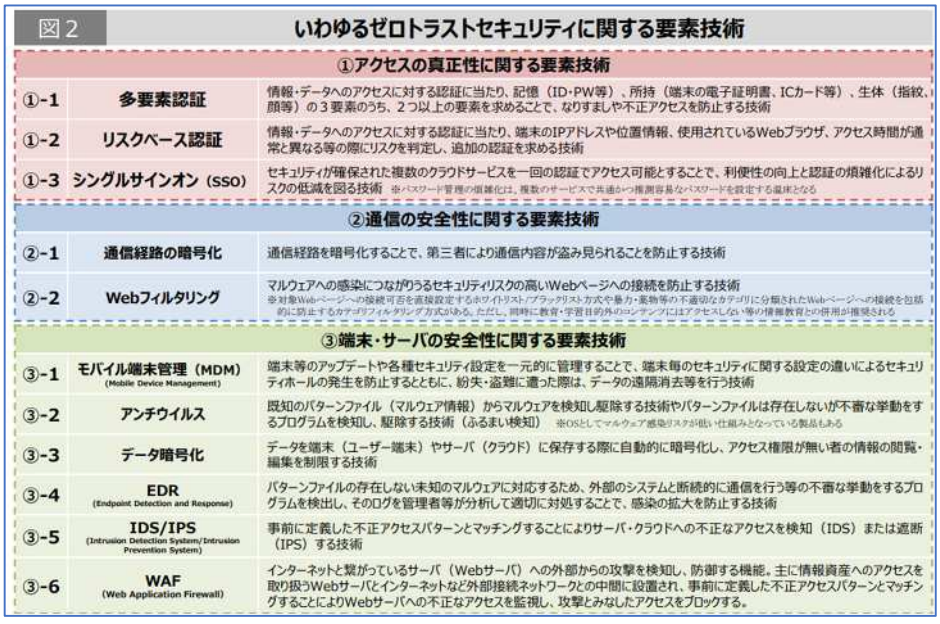


図２ いわゆるゼロトラストセキュリティに関する要素技術

①アクセスの真正性に関する要素技術		
①-1	多要素認証	情報・データへのアクセスに対する認証に当たり、記憶（ID・PW等）、所持（端末の電子証明書、ICカード等）、生体（指紋、顔等）の３要素のうち、２つ以上の要素を求めることで、なりすましや不正アクセスを防止する技術
①-2	リスクベース認証	情報・データへのアクセスに対する認証に当たり、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、追加の認証を求める技術
①-3	シングルサインオン（SSO）	セキュリティが確保された複数のクラウドサービスを一回の認証でアクセス可能とすることで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術 ※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②-1	通信経路の暗号化	通信経路を暗号化することで、第三者により通信内容が盗み見られることを防止する技術
②-2	Webフィルタリング	マルウェアへの感染につながりうるセキュリティリスクの高いWebページへの接続を防止する技術 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある。ただし、同時に教育・学習目的外のコンテンツにはアクセスしない等の情報教育との併用が推奨される
③端末・サーバの安全性に関する要素技術		
③-1	モバイル端末管理（MDM）（Mobile Device Management）	端末等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止するとともに、紛失・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	アンチウイルス	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術（ふるまい検知） ※OSとしてマルウェア感染リスクが低い仕組みとなっている製品もある
③-3	データ暗号化	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術
③-4	EDR（Endpoint Detection and Response）	パターンファイルの存在しない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、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
③-5	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サーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
③-6	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。主に情報資産へのアクセスを取り扱うWebサーバとインターネットなど外部接続ネットワークとの中間に設置され、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Webサーバへの不正なアクセスを監視し、攻撃とみなしたアクセスをブロックする。

図：文部科学省が示すゼロトラストネットワークの構成イメージ

「GIGAスクール構想の下での校務DXについて～教職員の働きやすさと教育活動の一層の高度化を目指して～」

URL：https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf

4.2 インフラシステム要件

4.2.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、本県と秘密保持契約を締結した事業者のみに開示するものとする。

また、必要となるライセンスやリソースについては、【別紙】インフラシステム仕様書を参照すること。

4.2.2 基幹プラットフォーム

次期システムの基幹プラットフォームは、Microsoft 365（以下「M365」という）およびISMAPに登録されたパブリッククラウドを採用するものとする。

ゼロトラスト環境の構築にあたっては、M365 Education A5（以下「M365 A5」という）のライセンスを調達し、そこに含まれる諸機能を主として構築すること。

また、システム環境の基盤構築については、パブリッククラウド基盤を調達し、必要なセキュリティ対策を講じたうえで実施すること。

4.2.3 パブリッククラウド基盤

次期システムとして、SaaSを利用しないシステムについては、パブリッククラウド基盤を調達し、その上に仮想マシンを構築するものとする。

(ア) マルチリージョン構成を採用し、大規模災害にも備えた環境を構築すること。

(イ) データは、日本国内のデータセンタおよび日本国内の法律が適用される環境に保管すること。

(ウ) 基盤上に構築するインスタンスについては、データのバックアップ対策を実施し、データ損傷やランサムウェア感染が生じた場合でも復旧可能な仕組みを実装すること。

(エ) 基盤上に構築するインスタンスには、アンチウイルス等のマルウェア対策を実装すること。

(オ) 保管するデータには暗号化を施すこと。

(カ) WAFやIDS/IPSなどを用いて、外部からの攻撃に対する防御策を講じること。

(キ) Web利用においては、急激な負荷増加にも耐えられるようオートスケール機能を実装すること。

(ク) インスタンスへの運用管理接続については、VPN接続等でファイアウォールに穴を開けることなく、SSEアーキテクチャのZTNA技術や完全閉域回線を利用すること。

(ケ) 管理コンソールへのアクセスについても統合認証基盤と連携し、適切な認証・認可を行ったうえで接続できる機能を実装すること。

4.2.4 統合認証基盤

次期システムでは、M365およびその他のクラウドサービス、校務支援システム、事務系システム、学習系プラットフォームを含む認証基盤として、M365のMicrosoft Entra ID機能を活用し、認証管理を一元化する。ただし、県立学校生徒の私物デバイスを活用する想定はないが、この前提を踏まえつつ、学校の運用実態に応じた認証管理手法（パスワードリセットの方法を含む）を県と協議のうえ実施すること。

(ア) ID管理および各システムへの認証基盤として必要な機能を備えること。

(イ) 人事異動などが発生した場合、知事部局システムまたは教育委員会事務局の人事管理システムから連携されるアカウント情報を用いて、アカウントの随時追加・削除・編集が可能な機能を備えること。

(ウ) 発注者が業務利用する各連携可能なシステムおよびサービスに対して、シングルサインオンまたはユーザ情報の連携が行えること。

(エ) 管理者（発注者が指定する本県教育委員会所属職員および一部の教職員を指す。以下同じ。）が許可を与えた端末および利用者のみ、サービスを利用できるよう制御できること。

(オ) パスワードを忘れた際に、利用者側でパスワードリセットを行えること。

(カ) 保護者については、外部ユーザ招待機能を用いて、保護者自身のメールアドレスで利用できること。

4.2.5 多要素認証

Microsoft Entra IDを認証基盤として活用するにあたり、対応可能な多要素認証方式を導入する。

認証基盤は、県立学校教職員・県立学校生徒、県教委職員、市町教委職員、市町立学校教職員が利用するため、それぞれのユースケースに応じた要件を満たすこと。

なお、学習系端末では生体認証機能を具備していないため多要素認証を実現するための適切な機器の運用保守期間中の提供を本提案に含めること。

(ア) 顔認証や指紋認証などの生体認証を中心に、知的認証、物理認証（トークン等）、地理情報などから少なくとも2種類以上を組み合わせた多要素認証、生体情報を使用できる環境ではFIDO2アライアンスに基づいたパスキー運用が可能であること。

※ユースケースに応じた適切な機器の運用保守期間中の提供を含む

※パスキーについては端末等の利用状況も踏まえ本調達の中で運用可否を検討の上方針決定する

(イ) 県立学校においてはテレワークでの利用も想定しているため、利用場所を問わず認証できること。

(ウ) 個人スマートフォンや教職員及び生徒の私物デバイスを用いた認証を制限できること。

※ただし、通信制学校等で本県が認めた場合に限り、私物デバイスでの認証を許可する。

4.2.6 シングルサインオン（SSO）

Microsoft Entra IDを認証基盤として活用するにあたり、以下のシステム等に対してシングルサインオンを実施すること。また、これらのシステムについてはEntra IDとのSAML認証が可能であることを前提とする。

(ア) M365の利用サービス（Exchange、Teams、SharePoint、OneDrive等）

(イ) 統合型校務支援システム（株式会社ベネッセコーポレーション「ベネッセ校務クラウド」）

(ウ) 教職員向け事務系システム

(エ) デジタル採点システム

(オ) オンライン授業配信システム（Microsoft Teams）

(カ) ポータルサイト、ダッシュボード

なお、記載システム以外に次期システム専用の運用管理に必要なシステムを導入する場合は、シングルサインオン機能を実装、もしくは不正アクセスに対する対策を施すこと。

加えて、校務・事務・学習等に必要なシステム・アプリ等が県教委及び学校に採用された際、シングルサインオン機能の活用が可能な場合は、運用・保守の範囲内の対応として実装・活用することを前提とする。

4.2.7 通信経路の暗号化

県立学校端末よりWebサービスやクラウドサービスを利用する際の通信を暗号化すること。

4.2.8 Web 保護

フィルタリングサービス利用して、悪質なWebコンテンツや教育利用で好ましくないサイトへのアクセス制限が可能なように設定すること。

各種設定に関しては、既存の設定を踏襲した上で設計を実施すること。

4.2.9 クラウドサービス制御、情報流出制御

次期システムを利用するにあたり、不必要なクラウドサービスの利用を制限・可視化し、ドキュメントの重要性分類に従って機微情報の流出を防止すること。

(ア) 本県が認めたクラウドサービスへのみファイルのアップロードを許可できること。

(イ) クラウドサービスの利用状況を可視化し、シャドーITへの対策を可能にすること。

(ウ) BitLocker機能により、県立学校教職員の校務系端末のドライブを暗号化すること。

(エ) クラウドストレージに保存するデータは、すべて自動的に暗号化されること。

(オ) ゼロトラスト環境で認証を経た利用者が暗号化されたファイルを参照する場合、当該利用者の権限に基づきファイルの参照・更新を行えること。なお、更新後に保存するときは再度暗号化を行うこと。

(カ) 機微情報についてはMicrosoft A5の機能を用いて外部へ持ち出しできないよう制限や警告を行うこと。ただし、本県が認めた共有方法で持ち出した場合は、当該行為をレポートとして記録し、運用保守業者から各学校へ通知できること。

(キ) 暗号化された状態で格納されたファイルがネットワーク外部へ流出した場合、認証を経ない利用者が内容を参照・操作できないこと。

(ク) 暗号化されたファイルは、アクセス権を持つ利用者のみが閲覧可能であること。

(ケ) 教職員が作成するファイルには、デフォルトで機密度の高いラベルが付与されること。

(コ) 生徒向けに作成したファイルは、作成者がラベルを変更したうえで共有できること。

(サ) 機密度の高いラベルは、システム管理者および権限保有者、およびファイル作成者のみが変更可能であること。

4.2.10 アンチウイルス

校務系端末ならびに学習系端末に対してウイルス及びマルウェア感染対策を実施すること。

パブリッククラウド上のサーバに対しても同様に感染対策を実施すること。

4.2.11 感染後の検知・対応

昨今のサイバー攻撃では、アンチウイルス製品のシグネチャパターンによる検知・駆除が困難なケースが多いため、EDR機能を活用し、端末感染後の検知および対策を実施すること。

また、ログ分析に基づき、可能な限り早期且つ自動的に端末のネットワークを隔離・遮断し、復旧を行える機能も実装すること。

※インシデントのレベルによって、自動隔離・遮断等を実施することを想定する。

4.2.12 ログの相関分析

アンチウイルス、EDR、MDM、認証情報などのログを集約し、セキュリティインシデントに対応できる機能を実装すること。

4.2.13 端末統制・保護

ゼロトラスト環境下で使用する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ため、MDMを導入する。

(ア) 既存で利用中のWindows端末を管理・制御できること。

(イ) プリンタドライバ等の一斉配布やWindows Update等の一斉管理が可能であること。
その際、配布の時間帯等を発注者が任意に指定できるとともに、ネットワーク等の負荷分散を図る機能を備えること。

(ウ) 管理者が許可していない端末からのログイン等を制御できること。

(エ) 端末紛失時に、遠隔操作にて当該端末のロックやデータ消去等ができること。

(オ) BluetoothやUSBの外部記憶媒体等への接続を制御できること。

(カ) 他セキュリティ製品と連携を行い、端末ロックなどインシデント対応が可能であること。

(キ) 管理端末情報（ハードウェア情報、接続デバイス情報、ソフトウェア情報、ログイン状態など）の可視化や資産管理のために全端末のレポーティングが出来ること。

4.2.14 クラウド・オンプレファイルサーバ

既存環境ではオンプレミスのシステムでファイルを共有しているが、今後はゼロトラストモデルによるアクセス制御を構築するため、以下の要件に基づき、校内外から利用できるクラウドファイルサーバを設計・構築すること。

(ア) ストレージサービスは、M365 の SharePoint Online / OneDrive for Business を利用すること。

(イ) 全体で860TB以上の容量を備えるとともに、県立学校教職員用の個人割り当て容量は1人当たり50GB以上、県立学校生徒は15GB以上とすること。

(ウ) M365 と連携し、ユーザおよびグループ単位でフォルダへのアクセス権限を制御できること。
※フォルダ構成およびアクセス権限等については、発注者との協議により決定する。

(エ) 情報資産の分類に応じて、ファイル暗号化やアクセス権などの制御が可能な仕組みを有すること。

(オ) バージョン履歴機能および削除ファイルの復元機能を有すること。復元可能な期間は、削除操作から概ね90 日以上とすること。

(カ) 校外からクラウド上の校内情報資産にアクセスすることになるため、セキュリティ面について十分に配慮すること。

(キ) 各学校で利用中のオンプレミスサーバ（現行システムのデータセンタ上にあるファイルサーバおよび学校ファイルサーバ）ならびに現行の SharePoint Online に格納されているデータをクラウドストレージへ移行する作業は、受託事業者が実施すること。
また、データ移行については、効率的な実施時期および手法等を提案し、移行中に発生したトラブルに対して速やかに対応すること。
ただし、現行の OneDrive for Business、メール領域に格納されているデータは、各校において移行を行う。

(ク) クラウドへの格納時に、不正なプログラム等を無害化できる対策を実装すること。
(ケ) 校内業務で利用する機器に対応するため、公共NWで接続されたデータセンタ等へオンプレミスのファイルサーバを設置し、機器からのデータを格納できる仕組みを作ること。
(コ) オンプレミスのファイルサーバについては、100GB程度の容量を確保すること。

4.2.15 メールアプリケーション

メールアプリケーションについては、現行システムで利用しており広く普及しているOutlookを継続利用とする。

また、現在は教職員テナント、生徒テナントが分離しているため、移行と合わせてテナント統合を実施すること。

(ア) 教職員が使用するメールについては、Microsoft Exchange Onlineを活用し、外部との送受信可能なメールを使用できるようにすること。
(イ) 生徒が使用するメールについては、Microsoft Exchange Onlineを活用し、同一テナント上のアカウントとのみメール送受信が使用できるようにすること。
(ウ) 現行のメールアドレスを引継ぎできること。
(エ) 過去のメールデータについては、移行後もメール保持期間を過ぎるまで現行システムのメールが確認できるよう方法を提案すること。
(オ) スパム対策、マルウェア対策、フィッシング対策を実装すること。
(カ) 外部から受信するメールのリンク無害化や添付ファイルの自動分離などメール無害化を実装すること。

4.2.16 PPAP 対策・大容量ファイルメール送受信

教職員が外部とのメール送受信時に、メールの添付送信ならびに、Outlookメール添付ファイル上限を超えた資料の送受信も発生するため、PPAP対策を導入する。

(ア) Outlookメールへファイルを添付した際に、自動的に共有リンク化できるようにすること。
(イ) 大容量ファイルについては、専用の送信方法を用いて、共有リンクを生成できるようにすること。
(ウ) 外部より受け取るファイルについては、格納先を提供してファイルを受信できるようにすること。

4.2.17 DNS

学校のホームページ等で外部DNSを利用するが受託事業者はシステムのクラウド化に合わせて当該サーバの設定要件、変更要件を明確にすること。

4.2.18 コミュニケーションツール

チャット及びオンライン会議のコミュニケーションツールとして、Microsoft Teamsを活用し、その環境を構築すること。

現行システムのTeamsにおけるチーム構成は棚卸しを行い、チーム構成は踏襲を行う。

Teams以外に各学校でZoom、Google、YouTubeを利用しているが、継続して利用ができること。

4.2.19 学校拠点設備（ネットワーク）

次期システムでは、各県立学校よりローカルブレイクアウトによる接続ならびに、パブリックサービスを主軸に利

用する構成となるため、インターネット回線の帯域不足が発生することが懸念される。

そのため、インターネット回線や使用機器については以下の要件を満たす最適な構成を構築すること。

(ア) 文科省が推奨している帯域を可能な限り満たす構成を提案すること

参考となる回線種別、回線本数については【別紙】履行対象一覧を参照すること。

ただし、複線化を行う学校については必要帯域が分散されることから回線本数で按分してもよい。

学校規模ごとの当面の推奨帯域

児童生徒数	推奨帯域（Download）	児童生徒数	推奨帯域（Download）
12 人	22 Mbps	525 人	511 Mbps
30 人	54 Mbps	560 人	525 Mbps
60 人	108 Mbps	595 人	538 Mbps
90 人	161 Mbps	630 人	553 Mbps
120 人	216 Mbps	665 人	566 Mbps
150 人	270 Mbps	700 人	580 Mbps
180 人	323 Mbps	735 人	594 Mbps
210 人	377 Mbps	770 人	607 Mbps
245 人	395 Mbps	805 人	621 Mbps
280 人	408 Mbps	840 人	633 Mbps
315 人	422 Mbps	875 人	647 Mbps
350 人	437 Mbps	910 人	660 Mbps
385 人	453 Mbps	945 人	673 Mbps
420 人	468 Mbps	980 人	686 Mbps
455 人	482 Mbps	1,015 人	698 Mbps
490 人	496 Mbps	1,050 人	711 Mbps

図：文部科学省が示すゼロトラストネットワークの構成イメージ

「GIGAスクール構想の実現　学校のネットワーク改善ガイドブック(令和6年4月)」

https://www.mext.go.jp/content/20240509-mxt_jogai01-000035663_001.pdf

(イ) 原則は10Gbps回線のシングル構成で対応すること。

(ウ) 10Gbps回線の提供エリア外は原則1Gbps回線で複線化による帯域確保を行うこと。

(エ) 複線化を利用する際は、SD-WANもしくは、FQDNやアプリケーションによって振り分けができる機能を実装すること

(オ) 複線化を利用する際は、可能な限り異キャリア、異エリア局ルート、異変電所ルート、衛星通信等の分散を行うこと。

(カ) 10Gbps回線が導入できる学校は、10Gbps回線を利用すること。

なお、本調達契約後に10Gbps回線が導入できることが判明した場合、運用保守の範囲内で対応すること。

(キ) 県立学校はゼロトラスト化されるため、FW機能を具備しているルータを用いること。

(ク) 本県で許可していない端末のネットワーク接続を制限するための不正接続防止装置を継続利用すること。

(ケ) 実装後は効果検証（推奨帯域の達成状況、負荷検証結果、満足度検証結果等）を行い県に報告すること。なお、効果検証の内容や方法については、県と協議の上、決定すること。

4.2.20 データセンタ設備（運用保守・監視用）

次期システムでは、パブリックサービスを主軸に各県立学校よりローカルブレイクアウトにより接続して利用する構成となるため、データセンタへ主要設備の配置は行わない想定だが、以下の用途に限り使用を認める。

なお、閉域接続に限り、学校側のネットワークとの接続を許可するが、必要なセキュリティ対策は実装すること。

また、庁内システムへのアクセスについてはセキュリティと責任分界点の観点から、データセンタを中継させること。

ただし、公共NWを用いた閉域接続かつ運用保守に影響が無ければ必ずしもデータセンタの利用は問わない。

(ア) クラウド監視に対応していないネットワーク機器などの運用保守や監視

(イ) 受託事業者の運用保守業務

(ウ) 本県の庁内システムへアクセスする際の通信経路

4.2.21 公共ネットワーク設備

次期システムでは、各県立学校がゼロトラストモデル、公共ネットワークで接続される庁内ネットワークはαモデルとなるため、以下の通信用途での利用は禁止とする。

(ア) 県立学校内の端末より、公共ネットワークを利用した庁内システムへの直接接続

(イ) 県立学校内のネットワーク機器より、公共ネットワークを利用した庁内システムへの直接接続

なお、知事部局にて調達している行政端末については、この限りではない。

4.2.22 監視設備

次期システムでは、パブリッククラウドが主軸となるが、各サービスの監視も受託事業者で実施すること。

(ア) パブリッククラウド上の仮想マシン、ロードバランサ、データベース、WAF、DNSなど

(イ) Webサービス等の外形監視

(ウ) 校内LAN設備（ルータ、既存ネットワークスイッチ）

なお、無線アクセスポイントは現行で使用している専用の監視システムと併用とする

4.3 校務系システム要件

4.3.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、入札参加資格の確認後、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.3.2 校務支援システム

本県が指定する統合型校務支援システム（株式会社ベネッセコーポレーション「ベネッセ校務クラウド」）を利用すること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

なお、システム利用者は県立学校に限定する。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) アカウント情報に基づき、適切なシステム利用権限を付与すること。

(ウ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(エ) 教職員からのシステム利用に係る問い合わせは、受託事業者の問い合わせサービスを介さず、校務支援システムメーカで実施すること。
ただし、受付時間外における問い合わせやシステム障害に関してはこの限りではない。

(オ) 利用機能については、【別紙】校務系システム仕様書を参照とする。
なお、現行利用の校務支援システム機能ならびに帳票をベースに、基本設計段階でFit&Gap資料等を作成している。この資料と次期校務支援システムの設計構想を基に各学校にヒヤリングし、要望があった機能・帳票については、県と対応方法を協議の上、原則カスタマイズ対応を実施すること。

(カ) 当該システムはパッケージ製品のため、機能拡張（UI改善、外部連携機能の拡充等）の予定を明確化の上、本稼働（令和9年4月）までに拡張する予定の機能は、原則対応すること。

(キ) 利用者は県教育委員会・県立学校教職員・県立学校生徒・保護者とする。

4.3.3 ダッシュボード機能

ダッシュボード機能は、本県の画面イメージに合わせたシステムを設計構築すること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(ウ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

(エ) 校務支援システム、学習システム等の連携については、連携によるセキュリティホールが発生しないよう対策を行うこと。

(オ) 利用者は県教育委員会・県立学校教職員・県立学校生徒・保護者とする。

4.3.4 ポータルサイト機能

ポータルサイト機能は、本県の画面イメージに合わせたシステムを設計構築すること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(ウ) 県教育委員会・県立学校教職員・市町立学校教職員・県立学校生徒・保護者などの利用者に合わせたポータルサイトを提供すること。

(エ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

(オ) 教職員はポータルサイトから校務支援システム、事務系システム、学習系・公開系システム等の各システムへ遷移し利用する。

(カ) 県立学校生徒・保護者はポータルサイトから校務支援システム、学習系・公開系システム等の各システムへ遷移し利用する。

4.4 事務系システム要件

4.4.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、入札参加資格の確認後、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.4.2 事務システム

事務系システムについては、本県の利用実態に合わせたシステムを設計構築すること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

なお、事務システムは、県立学校教職員、市町立学校教職員にて利用権限、提供機能が異なることから、適切な利用ができるようシステムを構築すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) アカウント情報に基づき、適切なシステム利用権限を付与すること。

(ウ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(エ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

(オ) 利用機能については、【別紙】事務系システム仕様書を参照とする。

4.5 学習系・公開系システム要件

4.5.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.5.2 学習系システム

学習系システムについては、本県の利用実態に合わせたシステムを設計構築すること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

なお、学習系システムは、県立学校教職員、市町立学校教職員により利用権限や提供機能が異なることから、適切な利用ができるようシステムを構築すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) アカウント情報に基づき、適切なシステム利用権限を付与すること。

(ウ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(エ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

(オ) 利用機能については、【別紙】学習系・公開系システム仕様書を参照とする。

4.5.3 デジタル採点システム

本県が別途調達を行い県立中学校及び県立高校に導入するデジタル採点システム（株式会社シンプルエデュケーション「百問繚乱」）と統合認証基盤を接続し、利用可能なようにすること。

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(ウ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

4.5.4 オンライン授業配信システム

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

(ア) 統合認証基盤とSAML連携し、システムアクセス時には認証基盤を用いたアクセスを行うこと。

(イ) ユーザ情報については、統合認証基盤の情報を用いた運用管理を行うこと。

(ウ) 教職員からのシステム利用に係る問い合わせは、受託事業者にて一次受付体制を構築すること。

4.5.5 学校ホームページ

システム利用時には以下の機能を具備し、適切なセキュリティ対策を実施すること。

(ア) 県立学校、市町立学校のホームページ機能を提供すること。

(イ) 県域で統一した操作方法で学校HPの作成を行うことを可能とすること。

(ウ) データ資源、HP作成、メンテナンス機能は現行踏襲のまま次期システムへ移行すること。

(エ) コンテンツとして動画の埋め込みを可能とすること。

(オ) ウェブアクセシビリティ対応の導入すること。

(カ) 多言語対応を可能とすること。

4.6 校務系・学習系端末要件

4.6.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.6.2 校務系端末

校務系端末については、本県の利用実態に合わせた端末のキッティング要件の定義・設計を行うこと。校務系端末には以下の機能を具備し、適切なセキュリティ対策を実施すること。

なお、次期教育情報システムでは校務系端末と学習系端末を1台に統合することから、統合後も現行の校務用・学習用の利用を踏襲しながら、校務系端末として適切な重要情報資産の範囲（I～Ⅳ）で利用できるように端末の設定と変更を行うこと。

(ア) MDMによる端末統制、紛失後のデータ消去

(イ) アンチウイルスによるマルウェア侵入防止

(ウ) EDRによる感染後の検知対応

(エ) データ暗号化、秘密度ラベルによる情報流出対策

(オ) 多要素認証（生体認証を含む）

(カ) SASEによる通信の保護

4.6.3 学習系端末

学習系端末については、本県の利用実態に合わせた端末のキッティング要件の定義・設計を行うこと。学習系端末には以下の機能を具備し、適切なセキュリティ対策を実施すること。

なお、次期教育情報システムでは生徒・教職員が利用する学習系端末において、重要情報資産分類Ⅲにあた

る個人情報などを扱うことも想定されるため、現行の利用を踏襲しながら、適切な重要情報資産の範囲（主にⅢ～Ⅳ）で利用ができるように端末の設定と変更を行うこと。
更に次期システム下においても、これまでと同様に各種アプリ・インストールソフトなどが利用できることを前提とする。

(ア) MDMによる端末統制、紛失後のデータ消去
(イ) アンチウイルスによるマルウェア侵入防止
(ウ) EDRによる感染後の検知対応
(エ) データ暗号化、秘密度ラベルによる情報流出対策
(オ) 多要素認証（生体認証を含む）

4.6.4 その他 ICT 機器

全体構成のイメージ図に示されている通り、校務系・学習系端末以外にも、電子黒板用、学校購入端末（学習・校務等）、県教委購入端末（特別用途）、県教委用、市町教委用等、多くのICT機器が利用されている。
次期システムを構築する上で、関係するICT機器は全て抽出の上、キッティングの変更など、適切に設計を行い、漏れなく対応すること。

なお、県教育委員会及び県立学校で管理しているものは、キッティングの対応を受託事業者が主体的に実施すること。県で管理しているもの以外は、設計の変更を提案・支援することとし、作業完了まで、進捗を管理・フォローすること。

4.7 運用保守要件

4.7.1 前提条件

機能要件に記載の一部セキュリティ製品名については、「3.4.1資料開示の制限事項」に従い、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.7.2 要求サービスレベル仕様

基盤（DC 側、クラウド側、SaaS 側）、ソフトウェアに関するサービスレベルを下表に示す。

項目		内容	ソフトウェア	基盤	校内 LAN
可用性	稼働時間	サービス提供時間	24 時間 365 日		平日 5:00～22:30 ※1
	稼働率	稼働率(%)＝稼働時間÷稼働すべき時間※稼働率の計算において分母は年間の稼働時間とする	99.9%以上 ※提供サービス単位で集計する。	99.9%以上 ※クラウド、SaaS、回線は提供事業者の基準に準ずる	99.5%以上 （1 校あたり 99.0%以上） ※回線は提供事業者の基準に準ずる

	計画停止(メンテナンス)	メンテナンスについては２週間前までに佐賀県に計画提出※２	100%	
障害対応	障害対応時間	障害復旧対応する時間帯	24 時間 365 日	平日 9:00～17:00 ※県立学校 FW 及びセンターSWは 平日 7:00～22:00
	障害報告時間	障害を認知してから佐賀県へ1時間以内に通知	95%以上	
	復旧時間(暫定)※３	佐賀県へ障害通知後 4 時間以内に暫定復旧を実施	95%以上	
利便性	応答時間	処理の実行指示を与えてから最初の応答(画面表示)が得られるまでの時間	平均 3 秒以内	―
	ターンアラウンドタイム	処理の実行指示を与えてから 全ての実行結果が得られるまでの時間(上段:ファイル出力、 下段:画面出力)	60 秒以内 平均 5 秒以内	―

※1県立学校からの要望により校内 LAN 稼働時間を延長すること

※2事前承認済みのメンテナンス作業や冗長化している設備の方系の運用時間は除く

※3緊急時は除く

※4校内 LAN についてはハードに起因する障害は除く

セキュリティサービスに関するサービスレベルは以下の通りとする。

<table>
<tr><th colspan="2">項目</th><th>内容</th><th>ソフトウェア</th><th>基盤</th><th>校内 LAN</th><th>端末</th></tr>
<tr><td rowspan="5">セキュリティサービス</td><td>DC 側マルウェア検知</td><td>シグネイチャ(パターンファイル)の更新間隔</td><td>―</td><td colspan="2">ベンダリリースから1日以内</td><td>―</td></tr>
<tr><td>DC 側振る舞い検知</td><td>シグネイチャ(パターンファイル)の更新間隔</td><td>―</td><td colspan="2">ベンダリリースから30 分以内</td><td>―</td></tr>
<tr><td>EPP マルウェア検知・駆除</td><td>シグネイチャ(パターンファイル)の更新間隔</td><td>―</td><td>―</td><td>―</td><td>ベンダリリースから1日以内</td></tr>
<tr><td rowspan="2">インシデント通知</td><td>レベル 3 インシデントを検知した場合の通知時間</td><td>―</td><td colspan="3">30 分以内※</td></tr>
<tr><td>レベル 2 インシデントを検知した場合の通知時間</td><td>―</td><td colspan="3">60 分以内※
メール通知</td></tr>
</table>

※インシデント検知によるシステムからのセキュリティ事業者・運用事業者へ通知後からとする

4.7.3 サービス停止の定義

サービス停止の定義を下表に示す。

なお、本定義に当てはまらない事象が発生した際は、都度サービス提供主体者と協議の上、停止判定を行うものとする。

基盤（クラウド基盤含む）・ソフトウェア

項目	説明	停止判定
全システムの停止	全システムが利用できない状態。	停止とする
基盤（DC 側、パブリッククラウド側）システム単体の停止	基盤システム単体が利用できず、一部サービスが利用できない状態	停止とする ※1 ※片系障害等サービスが利用できる場合は停止としない
サブシステム(ユーザ SaaS)の単体の停止	サブシステム単体が利用できず、一部サービスが利用できない状態	停止とする

サブシステム(ユーザ SaaS)の機能不具合	サブシステム自体は稼働しているが、 一部機能に不具合がある状態	停止としない
サブシステム（ユーザ SaaS）処理遅延	サブシステムは稼働しているが、処理時間がシステム性能の目標値を大きく満たさない状態	停止とする ※停止の範囲は都度協議
ソフトウェアの停止	ソフトウェアが利用できない状態	停止とする
ソフトウェアの機能不具合	ソフトウェア自体は稼働しているが、 一部機能に不具合がある状態	停止としない
ソフトウェア処理遅延	ソフトウェアは稼働しているが、処理時間がシステム性能の目標値を大きく満たさない状態	停止とする ※停止の範囲は都度協議
その他システムの停止	学校独自で使用しているソフトウェアが使用できない場合	停止としない

校内 LAN

項目	説明	停止判定
学校全体の停止	校内 LAN が利用できない状態	停止とする
棟全体の停止	一部の棟で校内 LAN が利用できない状態	停止とする ※棟集約 SW 含む棟集約 SW 配下機器が全断の場合
特定のフロアの停止	棟全体は稼働しているが、一部のフロアで校内 LAN が利用できない状態	停止としない
特定の部屋の停止	棟全体は稼働しているが、一部の部屋が利用できない状態	停止としない
インターネット回線の停止	インターネット回線障害で、ネットワークが利用不可の状態	停止とする ※回線が冗長化されている拠点において、片系障害の場合は停止としない ※天災地変等による停止については SLA 集計から除く
公共NW回線の停止	公共NW側障害で公共 NW が利用不可の場合	停止としない ※バックアップ用途のため ※インターネット回線及び公共 NW 回線が同時に停止した際は、停止判定とする。 ※天災地変等による停止については SLA 集計から除く

セキュリティ関連

項目	説明	停止判定
セキュリティ機能が停止	セキュリティ機能が停止し、セキュリティインシデントの検知や対応ができない状態	停止とする
一部のセキュリティ機能が停止	一部のセキュリティ機能は停止しているが、システム全体としてセキュリティレベルが低下していない状態 ※詳細は運用基本設計書に明記	停止としない
セキュリティ機能の機能不具合	セキュリティ機能は稼働しているが、一部機能に不具合がある状態	停止としない
特定の端末でセキュリティ機能が停止	特定の端末でセキュリティ機能が停止している状態	停止としない ※個別対応とする

4.7.4 セキュリティインシデントの定義

セキュリティインシデントレベルを下表に示す。

インシデントレベル	内容	対応
レベル 3 (High)	サイバー攻撃が成功している可能性が高く、早期対応が必要と判断したイベント　(マルウェア感染、C&C 通信が発生しているなど)	・端末の NW 即時切り離し ・利用者へのヒヤリング ・端末の調査（ウイルスチェック） ・端末の回収/調査/リモートワイプ ・同一拠点にて複数の端末でマルウェアの感染が疑われる場合は、対象拠点全体の NW 切り離し
	端末の紛失（教職員）	・端末の所在調査 ・リモートワイプ
レベル 2 (Medium)	サイバー攻撃が成功する可能性があり、攻撃対象の状況確認もしくは追跡調査が必要と判断したイベント。また、端末が一時的にマルウェアに感染した疑いがあるが、即時に駆除され追跡調査が必要と判断したイベント。 (マルウェア感染の疑い、ブルートフォース（総当たり）攻撃、直近で更改された脆弱性攻撃)	・端末の NW 切り離し ・利用者へのヒヤリング ・端末の調査（ウイルスチェック） ・端末調査及び利用者へのヒヤリングにて問題ないと判断された場合、端末のNW切り戻し
	端末の紛失（生徒）	・端末の所在調査 ・リモートワイプ
レベル 1 (Low)	直接サイバー攻撃の被害は発生しておらず、セキュリティインシデントが発生する可能性は低いが、経過観察が必要と判断したイベント(ポート	月次報告書にて件数の報告

	スキャンや脆弱性探索など)	
レベル 0 (Info)	直接サイバー攻撃の被害は発生していないが、今後の攻撃に繋がる可能性も低いイベント (過剰検知、数年以上前の脆弱性攻撃など)	月次報告書にて件数の報告

4.7.5 運用保守対象

運用・保守の対象は、以下の機器/サービス群とする。具体的な製品名は基本設計書を参照すること。

システム区分	説明	提供システム・サービス名
基盤設備(DC 側)	DC 内に整備したネットワーク設備。インターネット回線に加え、DC 間接続回線や県庁ネットワーク向け閉域回線も含む	・ファイアウォール ・管理サーバ ・クラウド接続コネクタサーバ ・インターネット回線 ・閉域ネットワーク回線
基盤設備(クラウド側)	パブリッククラウド上に構築された各システムのサーバ稼働環境を提供している基盤設備及びネットワーク設備	・事務系サーバ基盤 ・公開系サーバ基盤 ・管理系サーバ基盤 ・ロードバランサ ・NTP ・DNS(内部・外部) ・シングルサインオン
ソフトウェア(クラウド側)	パブリッククラウド上に構築された基盤上で稼働するソフトウェア	・事務システム ・事務ポータル ・文書管理システム ・学習ポータル ・学校 CMS
サブシステム(ユーザ SaaS)	ユーザが直接利用する SaaS 型のシステム	・校務システム ・ファイルサーバ
サブシステム(管理・監視系 SaaS)	管理系のシステムを提供している SaaS 型のシステム	・メールシステム機能:外部メール、原本メール、PPAP 対策、大容量メール対応、ファイル無害化、メール無害化、誤送信対策、スパムメール対策 ・監視システム:死活監視、リソース監視、サービス稼働監視、インシデント監視 ・ログ分析 ・バックアップ(サーバ) ・ウイルス対策
セキュリティ機能(DC・クラウド設備)	DC 及びクラウド上に構築されたサーバを対象とした	・アカウント管理基盤(ユーザ認証・多要素認証) ・アンチウイルス

	セキュリティ機能。サーバ内のデータ保護や通信保護を行う	・DDoS 防御 ・Web アプリケーションファイアウォール ・不正ログイン防止 ・通信保護 ・脆弱性監視
セキュリティ機能（端末）	本システム利用時に用いる端末（県教委端末や生徒端末等）を対象としたセキュリティ機能。通信保護やユーザ認証、端末の統合管理や遠隔からの制御を行う	・多要素認証（指紋認証デバイス） ・端末統合管理：隔離、初期化、アップデート管理、デバイス制御、資産管理 ・アンチウイルス ・情報漏洩対策（DLP） ・通信保護 ・URL フィルター ・脆弱性監視
校内 LAN 設備	県立学校に整備しているサーバやネットワーク設備及びインターネット回線	・ファイアウォール ・DHCP サーバ ・不正接続防止装置 ・インターネット回線
その他システム	県が独自で導入しているシステムやアプリケーション。本システムの調達・運用保守範囲外	・旅費管理システム、マネジメントシステム等

4.7.6 運用保守時のカスタマイズ（修正・改善）対応

正式稼働開始後の5年間で運用問い合わせ内容によって設定のチューニング作業やアプリケーション機能の変更、脆弱性に対するバージョンアップ作業、システムから出力される帳票レイアウトの変更など、一定のカスタマイズが発生するため、ファンクションポイントとして運用費用に含めた提示を行うこと。

ファンクションポイントについては以下の内容で想定しているが、運用フェーズで本件のシステムが滞りなく運用できるよう受託事業者にて精査を行うこと。

(ア) 機能改善のうち、制度変更や要望等の利用者起因によるカスタマイズや改修作業については、作業にかかる工数をファンクションポイントの範囲内とすること。

(イ) 利用者からの依頼や要望にて運用責任者側で稼働する必要がある場合については、作業にかかる工数をファンクションポイントの範囲内とすること。

(ウ) インフラストラクチャー、アプリケーションを総合して320FP/年（1FP＝1人日）とすること。なお、利用せず残ったFPは翌年度以降へ繰り越しできることを原則とする。

(エ) 令和9年4月の運用開始後、問い合わせが多く発生することが想定されるため設計構築チームを3か月程度維持する、もしくは相応の対応が出来るようにFP値を上積みすること。

(オ) 修正改善業務の発生例としては下記のようなものを想定しているが、運用保守の範疇外の対応となるも

のをFP消費の対象とする。（詳細な対象は基本設計書を参照すること。）

- 年次切替に伴うシステムの修正
- 学校の制度や書式の改正等に伴うシステムの修正や端末・アカウント設定の変更
- 受託期間中に生じるPC端末環境の変化（OSのバージョンアップ、Webブラウザのバージョンアップ等）に伴い生じるシステムの修正
- 利用者からの要望等による機能改善に伴うシステム修正改善

(カ) 修正改善業務については、県が必要に応じて、次期システムの各箇所の修正・改善に利用できるものとする。

(キ) 修正改善作業実施にあたっては、本番環境に影響を与えない検証環境や資機材で正常動作の確認をおこない、他の機能の動作に影響を与えないことを確実に確認のうえ、県の承認を得たのちに、本番環境にインストールすること。

(ク) 障害対応や不具合切り分けや現地調査等は運用保守範疇となるため、ファンクションポイントの対象外とすること。

4.8 非機能要件

4.8.1 前提条件

非機能要件に記載の一部セキュリティ製品名については、「3.4.1 資料開示の制限事項」に従い、本県と秘密保持契約を締結した事業者のみに開示するものとする。

4.8.2 信頼性要件

操作端末や管理用端末での操作ミス等によるシステム障害が発生しないよう対策を講じること。

(ア) 複数の操作端末からの同時更新等により、データの整合性が失われたり、処理が停止したりしない対策を講じること。

(イ) 各サーバは、システムで求められる運用を考慮し、重要なものについては、負荷分散構成、クラスタ構成等により、信頼性を確保すること。

(ウ) バックアップスケジュールを定義し、バックアップ装置を用いてシステムの設定情報やデータ等のバックアップを実施すること。また、バックアップから迅速なデータ回復ができること。

(エ) 定義されているサービスレベルに従って品質・性能を確保すること。

4.8.3 セキュリティ要件

次期システムは「佐賀県情報セキュリティポリシー」ならびに「文部科学省が公表するガイドライン」に準拠するよう構築し、不正アクセス・コンピュータウィルス等への適切なセキュリティ対策を講じて安全性・信頼性を確保すること。

詳細な次期システムのセキュリティ要件については、【別紙】セキュリティに関する仕様書を参照とする。

なお、情報セキュリティポリシーは、受託事業者のみに開示する。

4.8.4 可用性要件

(1) センター拠点（データセンタ）

(ア) 仮想化技術ならびに高可用性機能を利用した24 時間365 日利用可能なシステム/ネットワーク構成を基本とすること。

(イ) センター内の機器は冗長構成とし、障害時および、メンテナンス時にサービスが停止しない構成とすること。なお、冗長化しない箇所がある場合には、明確に箇所と理由を示すこと。

(ウ) インターフェース障害、ネットワーク機器単体障害等の単一障害によって、長時間の通信断が発生しないよう考慮すること。なお、二重障害は考慮しないものとする。

(エ) 信頼性の高い製品、技術を採用すること。また、市場における標準的技術、標準的製品を採用すること。

(2) 各県立学校および、その他出先拠点

(ア) 24 時間365 日利用可能なシステム/ネットワーク構成を基本とすること。

(イ) 導入機器は基本的にシングル構成とするが、定められたサービスレベル（SLA）を厳守するべき保守用品および保守員の配置をすること。

(ウ) 信頼性の高い製品、技術を採用すること。また、市場における標準的技術、標準的製品を採用すること。

4.8.5 拡張性要件

(ア) 将来の利用学校増加や利用者増加に向けてスケールアウトを前提として、機器等の拡張が可能なシステム構成とすること。

(イ) 県の組織改正、制度変更、将来導入されるシステムとの連携に柔軟かつ低コストで対応できるように考慮すること。

(ウ) 技術の進展に柔軟かつ低コストで対応できるよう、広く利用されている国際的な標準に基づく技術を採用すること。

第5章 委託業務詳細

5.1 前提条件

機能要件に記載する一部の各セキュリティ製品名については、「3.4.1資料開示の制限事項」のとおり、本県と秘密保持契約書を締結した事業者のみに開示するものとする。

5.1.1 システム詳細設計

本県より提示する、県立学校や教育委員会等、利用者へのヒヤリングやアンケートで得られた要望や意見及び基本設計書を参考にシステムの詳細設計を行う。

また、追加で各県立学校、各市町教育委員会、県教育委員会等へのヒヤリング等が必要な事項については、本県との協議の上で実施を行う。

ヒヤリング事項の事例は以下のとおり。

・県立学校へ学校調達で設置している端末有無、端末用途の確認

・県立学校へEDR等チューニングに向けた、学校で利用しているソフトウェア情報の確認

・各市町教育委員会へ移行作業日等の確認

・県立学校へベネッセ校務クラウドの要件確定に伴うヒヤリング

※県立中学校・高校、特別支援学校、通信制など学校種別からピックアップしたヒヤリングを想定

なお、文科省ガイドラインは令和7年3月時点が最新であるが、ガイドラインの改定や国の動向の変化などについても注視し、要件が変更となるような改定が発生した場合は、本県と協議のうえで変更を実施する。

設計に求める要件項目の以下に示す。

詳細な要件項目については、【別紙】システム構築仕様書を参照とする。

また、基本設計フェーズにて発生した申し送り事項、佐賀県課題一覧についても詳細設計フェーズにて対応を行うこと。

① **ネットワーク設計**
現行システムで運用しているネットワークよりゼロトラストネットワークへ移行するため、全体、クラウド、拠点のそれぞれでネットワークの詳細設計を実施すること。

② **パブリッククラウド設計**
パブリッククラウドで実装する、コンピューティング、冗長化、セキュリティの詳細設計を実施すること。

③ **ネットワークセキュリティ設計**
ゼロトラストネットワーク化するにあたり、SWG、CASB、DLPといったセキュリティ製品を利用するための詳細設計を実施すること。

④ **デバイスセキュリティ設計**
ゼロトラストネットワーク化するにあたり、MDM、EPP、EDRといったセキュリティ製品を利用するための詳細設計を実施すること。

⑤ **オンラインストレージ・コミュニケーション設計**
オンラインストレージとコミュニケーションツール製品を利用するための詳細設計を実施すること。

⑥ **認証基盤設計**

統合認証基盤を利用するため、各クラウドサービス等の接続も含めた認証認可の詳細設計を実施すること。

⑦ **校務支援システム設計**

校務支援システムはSaaS製品を利用するが、認証認可やデータ連携、帳票一覧、項目定義など必要な詳細設計を実施すること。

⑧ **事務系システム設計**

本県より提示する画面イメージなどの基本設計書を参考に、事務系機能における詳細設計を実施する。なお、基本設計業務において下記項目を実施している。

- 概念モデル（ER図）設計
- 画面一覧、画面遷移図、画面レイアウト、画面項目定義書、帳票設計
- 帳票一覧、帳票レイアウト、帳票項目定義書
- テーブル一覧、テーブル定義書

⑨ **学習系システム設計**

学習系システムはSaaS製品を利用するが、認証認可やデータ連携など必要な詳細設計を実施すること。

⑩ **校務系端末・学習系端末等設計**

上記①～⑨の利用を前提に、校務系端末・学習系端末、他関係端末等が次期システムを利用するために必要な詳細設計を実施すること。

5.1.2 システム開発・環境構築

設計工程の成果物をもとにプログラミング、機器設定、SaaS設定、単体試験を行う。

環境構築において校務系端末、学習系端末（県立学校生徒に配布している端末、実習や図書室等の学校内で利用する端末）へのエージェントやセキュリティソフトの配布・インストール、端末統制や保護に必要な設定作業についても実施すること。

なお、環境構築で用いるライセンス等については受託事業者が調達の上で実施すること。

5.1.3 各種システム動作試験

システム開発・環境構築の成果物を使用し、設計通りの動作を行うか、すべての処理において確認する。

次期システムはゼロトラストアーキテクチャに基づく環境であるため、以下の要素も取り入れながらセキュリティを担保する試験を実施すること。

また、試行期間・展開期間で出てきた課題や要望については、解決・改善を実施しなければならない。なお、対応方法については、都度県に報告し協議すること。本稼働期間前にでた課題や要望についてはFPの利用は原則認めない。

なお、あくまでも例示であるため、上記要件を満たせる最適な提案を行うこと。

① **アクセス制御の検証**

ユーザ、デバイス、アプリケーションが適切な認証および認可を経てアクセスされているかを確認する。特に、最小権限の原則が正しく適用されていることを検証し、不要な権限付与がないかをチェックする。

② セキュリティポリシーの適用状況確認

ネットワーク全体にわたるセキュリティポリシーが一貫して適用されているかを確認する。また、異常なアクセスや振る舞いが発生した際に、ポリシーに基づいた自動対応が適切に行われるかを試験する。

③ 動的なアクセス制御の検証

利用者のコンテキスト（デバイスの状態、位置情報、振る舞い）に基づいてリアルタイムでアクセスが制限されるか、または認可が適切に変更されるかを試験する。

④ 脅威検知および応答のテスト

不審なアクセスや異常なトラフィックを検知し、リアルタイムにアラートを発し、適切な対応が自動または手動で行われるかを確認する。

⑤ システム全体の可視性と監視機能の確認

ネットワーク内の全てのトラフィック、デバイス、ユーザの動作が監視され、異常が即座に識別される仕組みが機能しているかをテストする。

⑥ データの保護と暗号化

重要データが正しく分類され、移動中および保存中に適切な暗号化が施されているか、データの漏洩が防止されているかを確認する。

なお、重要データは本県の実業務で利用されているデータ形式を本県と協議の上で受託事業者にてデータを作成し網羅的に実施すること。

5.1.4 システム移行

次期システムへの移行は、本番環境との並行稼働期間が発生すること、ネットワーク方式が大きく変わることから、3段階による移行を実施する。

なお、あくまでも例示であるため、安全かつ教職員の負荷が少ない最適な移行提案を行うこと。

①受入環境試験

受託事業者者は、本番環境と隔離された発注者のみが利用できる本番データ相当を投入した受入環境を整備し、併せて移行計画書を提示すること。

また、当該受入環境においては、受託事業者と発注者が合同で業務確認および打鍵確認を行い、移行計画書を含む試行展開判定会議にて承認を得るものとする。

なお、この確認作業においては、移行のみならず、移行後の運用を含む業務フロー全体の確認ならびに本番利用を想定した負荷試験も実施すること。

②移行リハーサル

モデル校として県立学校から2～3校、市町教育委員会・市町立学校及び県教育委員会からも選定し、インフラ環境を含めた移行リハーサルを実施する。

この移行リハーサルにて、実環境を用いた移行に係る流れ、システム動作、手順の妥当性を確認する。

なお、可能な限り知事部局システムも含めて接続試験を実施する必要があるが、接続されるシステム側の状況に応じて本県と協議のうえで実施を行う。

移行に問題ないことを確認し、発注者による本番展開判定会議にて承認を行う。

③本番移行（並行稼働）

全県立学校、全市町教育委員会、全市町立学校、県教育委員会の移行を行う。

移行時には県立学校教職員、市町立学校教職員、各市町教育委員会職員、県教育委員会職員の負担を最大限減らし、システム利用影響が少ない日時で実施すること。

移行作業は一斉移行による影響を極小化するため、順次移行することを前提とする。

ただし、校務支援システムや事務システムなどで順次移行することでデータの不整合等が発生する恐れがあるシステムについては、本県へ懸案事項を提示し協議の上で一斉移行を行う。

順次移行としては、学校単位でのネットワーク構成変更やサーバの切り離しなど、学校単位で実施できる移行を想定している。

また、PPAP対策やSASE導入などシステム単位で時期を調整できるものも順次導入を行い移行していくこと。

校務支援システムなど新たに生徒や保護者へ提供するシステムについては本県とスケジュールを調整の上、リリース時期を調整すること。

5.1.5 システム操作研修

利用職員に対して、次期システムにおける操作研修を行うこと。

研修時には、各種操作マニュアルを作成して納品する。また、研修マニュアル以外にフォローアップ研修に備えた動画も作成し、提供すること。

(ア) 受託事業者は、本番環境とは別に、研修者が操作感や打鍵を実施できる導入研修環境を構築し、操作研修は当該導入研修環境を用いて行うこと。

(イ) 校務支援システムおよび事務システムに関する研修は、集合型研修または学校施設での個別研修、オンライン開催によるWeb研修とし、研修会場は受託事業者が準備すること。

(ウ) 運用研修は、本県の運用管理者およびヘルプデスク委託事業者を対象に実施すること。

(エ) 研修スケジュールは本県と協議のうえで決定し、教職員の業務スケジュールを考慮したうえで受託事業者が作成するものとする。なお、本県から教職員へのスケジュール周知を行う。

(オ) 本実施体制に含まれる構成メンバーについては、所有する資格や実績を含めて具体的に示すこと。

(カ) 操作マニュアルや研修用テキスト（トレーニング資料）、運用開始に向けたシステム管理者向け操作マニュアルや運用手順書等を作成し、十分な教育訓練を実施すること。

※県担当者、学校担当者等のシステム管理者が概要を掴むための、システムの全体概要、作業手順をまとめた説明書（概要版）も作成すること。

※県担当、教職員、生徒、保護者等の利用者が概要を掴むための全体概要や作業の概要書も作成すること。

※新規採用時・異動時、年度初め等のよくある質問に対するQ&AをまとめたFAQ資料も作成すること。

(キ) 次期システムを導入する際は、各学校のサービス利用開始までに校務系、事務系の業務が遂行できるよう提供される機能や操作説明を教職員へ行うこと。

なお、教職員への情報展開に必要な資料や情報提供を行う仕組みを提供すること。

5.1.6 システム運用保守

次期システムを正常に稼働させるために、24時間365日の運用保守体制を構築し、運用開始後5年間の運用保守業務を実施すること。

年度毎にSLAの状況を確認し、SLA未達成が発生した場合、受託者は速やかに原因分析報告書および再発防止策を提出し、県と協議の上、受託者の負担で改善を実施すること。

なお、試行期間、展開期間も運用保守体制を構築し運用開始後と同様に対応すること。

体制として、運用部門の責任者、担当者について都道府県規模、校務システム、教育ネットワークにおける5年以上の運用実績を保有する者を配置することを原則とする。

また、次期システムの機能改善・改修については、県側の担当者が人事異動等で担当入れ替わりが多く、システムへの知識・理解が乏しい人材が運用保守の担当となることもあるため、事業者は、この点を意識し、運用保守を受託する者として、県の要望（画面や帳票）に対する対応時は、その他影響箇所、類似箇所を確認し、常に要望を受けた箇所以外も、広く提案する姿勢で改善・改修に対して臨むこと。

更に、次期システムの改善提案については、課題管理や問題管理の情報をヘルプデスクや次期システム関係者等から常に収集・分析し、主体的に改善の提案をすること。

なお、システム毎に運用内容が異なるため、詳細は【別紙】運用保守仕様書（SLA定義資料）に示す。

校内LANについて、各県立学校から県庁のサーバ室の公共NWへ接続していることから、公共NWの状況（停止・障害・不具合等）に関する情報の収集と周知を主体的に行い、校内LANの適切な運用に資すること。

システムの管理所属（教育DX推進グループ）の管理用端末（校務系・学習系）と関連のネットワーク機器及び機器までの施工した配線についても運用保守の範囲に含めることとし、管理用端末から各県立学校と同様に次期システム等にアクセスできるように機器の更改ならびに設定し運用保守すること。

なお、管理所属の移設時等は、FP等によりネットワークの移設の対応をすることを含む。

5.1.7 システム廃棄

現行システム上のデータを次期システムで利用可能にするためのデータ出力に係る作業を現行事業者へ依頼する。また依頼に伴う費用は本調達費用の範囲に含むこと。

次期システムの運用終了時には、当該システムそのものを機器も含め安全に廃棄すること（不要なデータの安全な廃棄を含む）とし、詳細は県と協議のうえ決定するものとする。

なお、現行システムの廃棄については現行教育情報システムの受託事業者にて行う。

5.1.8 セキュリティポリシー

本県教育委員会事務局にて現在運用しているセキュリティポリシーは、ゼロトラストアーキテクチャを取り入れたシステムに移行する際に、用途変更やデータ利活用に伴い運用ルールの変更が必要となる。

そのため、受託事業者よりセキュリティポリシーの改版案を提示すること。

なお、詳細な次期システムのセキュリティ要件については、【別紙】セキュリティに関する仕様書を参照とする。

(ア) セキュリティポリシー及び運用ルール等の現行資料を提供するため、文科省より発表されている「教育情報セキュリティポリシーに関するガイドライン」との差分を精査すること。

(イ) セキュリティポリシー及び運用ルール等の現行資料を提供するため、文科省より発表されている「教育データの利活用に係る留意事項」に係る対応を精査すること。

(ウ) 精査内容を本県へ報告し、改定方針の合意形成を行うこと。
(エ) 合意した改定方針に従い、セキュリティポリシー等の改定案を提示すること。
(オ) 本対応は、本県と改定スケジュールの合意を取りながら実施すること。
(カ) セキュリティガイドラインの改定状況によっては、インフラやアプリケーションの基本設計への影響も確認すること。

第6章 本業務の遂行に関する要件

6.1 プロジェクト管理

6.1.1 プロジェクト管理方法

PMBOK（ProjectManagementBodyofKnowledge）等、世界的に標準手法として認知されているプロジェクト管理方法を用いること。

6.1.2 プロジェクト基礎データの収集方法

プロジェクトの進捗・品質を担保するために必要な基礎データを明確にし、その取得方法や報告方法について県と合意のうえ収集すること。県に対する報告は収集した基礎データをもとに行うこと。

6.2 プロジェクト体制及び要因に関する要件

6.2.1 委託事業者の要件

本業務の受託事業者は以下の要件を全て満たすこと。

(1)本業務を受託するにあたっては、以下の資格を持つ技術者等を擁する事業者であること。

・メガクラウド（Azure、AWS、GCP等）に関連する資格

・シスコシステムズが認定するCCNPまたは独立行政法人情報処理推進機構が認定するネットワークスペシャリストまたは同等以上の資格

・情報処理推進機構が認定する情報処理安全確保支援士または同等以上の資格

・プロジェクトマネジメント協会が認定するPMPまたは独立行政法人情報処理推進機構が認定するプロジェクトマネージャーまたは同等以上の資格

(2)都道府県規模の校務支援システムや教育ネットワークの設計又は構築をした実績があること。

(3)本業務を実施する組織・部門において、ISMS、ISO/IEC27001、JISQ27001のいずれかに関する情報セキュリティに係る規格を競争入札参加資格確認申請書提出時点で取得していること。

(4)アプリケーションを構築または提供する組織・部門においては、ISMS、ISO/IEC27001、JISQ27001のいずれかの情報セキュリティに係る規格及び、ISO/IEC27017、ISMAPのいずれかのクラウド環境における情報セキュリティに係る規格を競争入札参加資格確認申請書提出時点で取得していること。

なお、構築・提供する組織・部門については、再委託先も可とする。

6.2.2 プロジェクト体制

本業務に遂行に関するプロジェクト実施体制を敷くこと。

外部組織や協力会社等が存在する場合は、その関係や役割、作業分担、責任範囲、指揮系統を明確にすること。

プロジェクト開始後は早期にステークホルダを洗い出し、連絡体制（窓口担当者連絡先まで）を確定すること。

本業務はセキュリティ製品やパブリッククラウド基盤、SaaS製品を組み合わせて使用することを想定しているため、セキュリティ観点で脆弱なシステムとならないよう第三者の視点で設計や構築の妥当性を監査もしくは支援する事業者を体制に含めること。

・第三者事業者は、ISMS、ISO/IEC27001、JISQ27001のいずれかに関する情報セキュリティに係る規格

を取得していること。

・第三者事業者は国・地方自治体、他県教育委員会へのゼロトラストアーキテクチャに係る製品の導入、コンサルティング業務の実績があること。

・第三者事業者を導入製品のメーカとする場合、俯瞰的な判断が困難になる恐れがあることから、必ず製品メーカ以外の事業者も体制に含めること。

・また、次期システムでは、IDaaS(統合認証基盤)、クラウドストレージ、各種アプリ等、マイクロソフト製品を幅広く活用することから、マイクロソフト製品に長けたアドバイザーなどを体制に含め、導入時の設計・設定などが即時提案できる体制とすること。

・また、現行機の運用期限があり、次期システムは本稼働の時期を遅れることはできない中、本事業は様々な分野（インフラ・ネットワーク・アプリ・端末等）が関係するため、各チームのスケジュールを統制し、PJ全体のスケジュールにまとめ、進捗状況の管理、遅延の報告、対策の検討・適用などを適切に支援・遂行するPMOを割り当てること。遅延リスク・是正策の報告、協議はPMO及びプロジェクトマネージャーが県に対して責任をもって行うこととする。

・運用保守期間においては、運用保守の窓口に技術問合せが可能な窓口担当者を1名以上設置し、県からの技術的な問合せや設定の確認等について随時回答と対応すること。（県からの技術確認、設定変更依頼に時間をかけないこと。）

・また、インフラ・ネットワーク、アプリ、ヘルプデスクそれぞれに窓口となる担当者、もしくは統括担当者を設置し、月例の報告会では、各者から技術的な観点も含めて、報告を行い、報告会の場でディスカッションできる様にすること（県からの質問に報告会の場で的確に回答及び改善提案ができる人員で臨むこと。）。

6.2.3 要員計画

本業務を遂行するために、プロジェクトマネージャーを1人割り当てること。

なお、本業務の遂行において主導的役割を担う要員（プロジェクトマネージャー）については、本業務に専任とすること。

また、プロジェクト要員を計画し、要員の情報(プロフィール情報、スキル情報、参画期間、経験情報)を明確にすること。

要員に変更がある場合は定例会等で情報共有をすること。

6.2.4 組織管理・コミュニケーション管理・課題管理方法

本業務におけるプロジェクト体制や連絡体制、組織間・組織内のコミュニケーション管理方法について事前に県の承認を得ること。

また、プロジェクトの実施にあたり、フェーズ毎に課題管理・変更管理を実施することとし、課題の完了や要件や機能の変更は都度県の承認を得ること。

6.3 打合せ・報告に関する要件

受託事業者は、本事業のスケジュール等に十分配慮し、県との打合せ・報告等を主体的に行うこと。

受託事業者は、本業務の実施にあたり、県と行う打合せや報告等に関する議事録を作成し、県にその都度提出して内容の確認を得るものとする。

6.4 成果報告

次のとおり本事業の進捗及び成果を取りまとめて報告を行うこと。実施時期の詳細については、県と協議のうえ決定する。

(1)中間報告

業務の進捗について3.6実施スケジュールに示す期間を目途に中間報告を行うこと。

なお、中間成果物に関しては、各フェーズの完了時に提出を行うこと。内容は県担当者と協議し、承認を得たものを提出すること。

(2)最終報告

業務の結果について取りまとめ令和9年3月を目途に完了報告を行うこと。

なお、本稼働前の最終報告として、次期システムの効果検証（コンセプトに対する実現状況、国の当面のKPIに対する達成状況、DXチェックリスト達成状況、学校・生徒・保護者の満足度検証結果等）結果をまとめた報告書を提出すること。内容は県担当者と協議し、承認を得たものを提出すること。

6.5 本委託業務の納品物

6.5.1 納品物の内容

以下に記すものについては、県が示す期限までに納品すること。

フェーズ	成果物	内容
設計	機能構造図	システム全体機能関連図、個別システム単位の機能関連図
	画面一覧	画面一覧 ※スクラッチ及びユーザ画面をカスタマイズしたアプリケーションシステム
	帳票一覧	帳票一覧 ※帳票を用いるアプリケーションシステム
	バッチ一覧	バッチ一覧
	基本設計書	ベネッセ校務クラウドに係る基本設計書
	詳細設計書（画面）	画面設計書システム全体機能概要書 個別システム単位の機能概要書 プログラムの処理内容を詳細に定義した設計書 画面入出力項目のチェック・編集を定義した設計書 画面遷移図
	詳細設計書（帳票）	帳票レイアウト帳票出力項目の編集を定義した設計書プログラムの処理内容を詳細に定義した設計書

	詳細設計書（バッチ）	ジョブ関連図ジョブスケジュール一覧プログラムの処理内容を詳細に定義した設計書
	詳細設計書 （パラメータ定義シート）	各システムの設定パラメータを詳細に定義した設計書 システム環境構築に関する各種定義情報をまとめたもの
	システム構成図	システムの構成図(構成内容含む)
	アドレス一覧	各システムで設定しているアドレスおよび VLAN などを記載した一覧表
	機器・ライセンス一覧	各システムで使用する機器名、ホスト名、シリアル番号、ライセンス名及び数量を記載した一覧表 期限ありライセンスの場合は、更新年月も記述を行うこと
構築・ 試験	テスト計画書	単体テストのテスト方式、作業手順を定義した計画書結合テストのテスト方式、作業手順を定義した計画書総合テストのテスト方式、作業手順を定義した計画書運用テストのテスト方式、作業手順を定義した計画書
	単体テストチェックリスト	単体テストのチェックリスト、およびテスト結果
	単体テスト結果報告書	単体テストの実施結果、評価をまとめた報告書 (単体テスト全体)
	結合・総合テストシナリオ	結合テストのテストシナリオ総合テストのテストシナリオ
	結合・総合テスト結果報告書	総合テストの実施結果、評価をまとめた報告書 運用テストの実施結果、評価をまとめた報告書 システムテストの実施結果、評価をまとめたもの なお、本稼働前の最終報告書として、次期システムの効果検証（当面の KPI 達成状況、DX チェックリスト達成状況、学校・生徒・保護者の満足度検証結果等）結果をまとめた報告書を提出すること。
	ネットワーク改善結果報告書	ネットワーク改善実装後の効果検証（推奨帯域の達成状況、負荷検証結果、学校満足度検証結果等）結果をまとめた報告書（効果検証の内容や方法については、県と別途協議の上、決定すること。）

	市町向け構築依頼事項	各市町から次期システムを利用する際に、ネットワーク観点ならびに端末観点で市町のシステム業者にて変更する内容の説明資料
	県教委向け構築依頼事項	県教委から次期システムを利用する際に、ネットワーク観点ならびに端末観点で県のシステム業者にて変更する内容の説明資料
移行	システム移行計画書	移行体制観点、スケジュール観点、ネットワーク観点、システム観点、データ観点で移行テストのテスト方式、移行作業内容、作業手順などを具体的に定義した計画書
	システム移行遷移図	システム移行中の構成遷移を示した図
	データ移行仕様設計書	次期システムへの移行要件や移行プログラムの処理内容を定義した設計書
	システム移行実施報告書	移行テストの実施結果、評価をまとめた報告書本番移行の実施結果をまとめた報告書
研修	教育研修計画書	教育研修の計画書
	教育研修実施報告書	教育研修の実施結果をまとめた報告書
	集合研修録画動画	集合研修用に録画した説明動画
	システム管理者向け操作マニュアル	システム管理者向けの運用手順書と操作マニュアル
	端末導入事業者向けマニュアル	端末導入の別事業者がキッティングを行う際に、次期システム向けのセキュリティソフトインストールやアカウント連携等の実施手順を記載した導入マニュアル
	利用者向け操作マニュアル	利用者向けの操作マニュアルと研修テキスト
運用	運用作業計画書	運用業務を遂行するための体制や連絡先、コミュニケーションやインシデント対応、運用作業時のルールならびに計画内容をまとめた計画書
	実績報告書	システムの運用実績をまとめた報告書 ※インフラ、ネットワーク、システム、アプリ、端末等の稼働状況についても報告すること。
	問題対応結果報告	システムの障害対応実績をまとめた報告書

	課題管理の報告	システムの課題管理状況をまとめた報告書
	今後の改善提案	システムの課題に対する改善事項をまとめた報告書 ※教職員や生徒の利用上の課題なども日々の問い合わせから集約し、課題管理への追加・改善の提案としてまとめておくこと。
	運用フロー	システムやネットワーク、SaaS などの障害、運用保守内の設定変更作業に対する佐賀県、受託事業者側の対応のフローをまとめたドキュメント ※各関係機能・機器（サーバ、ネットワーク、Saas、IDaaS、システム、アプリ、端末、その他制御系機能も含む）の設定・パラメータ等の運用上より確認・利用するパラメータもドキュメント内にまとめておくこと。 ※日々の運用作業・保守作業により変更が発生した場合は、常時ドキュメントを最新化しておくこと。
	セキュリティレポート報告	セキュリティ監視で検知したイベントについてまとめた報告書
	運用手順書	システムの運用手順をまとめた手順書。日々の運用作業改善の結果を反映して最新の状態にしておくこと。
保守	保守作業計画書	保守業務を遂行するための体制や連絡先、コミュニケーションや保守対応時のルールならびに計画内容をまとめた計画書
	実績報告書	システムの保守実績をまとめた報告書
	問題対応結果報告	システムの保守対応内容をまとめた報告書
	課題管理の報告	システムの保守管理状況をまとめた報告書
	今後の改善提案	システムの保守に対する改善事項をまとめた報告書
	保守手順書	システムの保守手順をまとめた手順書。日々の保守作業改善の結果を反映して最新の状態にしておくこと
廃棄	廃棄計画書	次期システム運用終了後に廃棄作業を遂行するための体制や連絡先、コミュニケーションや作業時のルールならびに計画内容（廃棄物品、廃棄作業等）をまとめた計画書
	廃棄報告書	運用終了後の次期システムの廃棄作業実績をまとめた報

		告書
	データ消去証明書	運用終了後の次期システムの廃棄物のデータ消去を証明する書類
その他	各種会議・打合せ議事録	定例会、分科会などの打ち合わせ内容を記した資料・議事録
	佐賀県セキュリティポリシー改定案	佐賀県セキュリティポリシーの改版を案としてまとめたもの

6.5.2 形式等

書類（紙媒体）は、A4 判縦長横書き両面を原則とし、日本語表記のものを 1 部提出すること。

書類（電子媒体）は、CD-R 又は、DVD-R により 1 部提出すること（ファイルフォーマットは、MicrosoftOffice、MicrosoftProject、MicrosoftVisio に対応できるデータ形式）。

6.5.3 納品場所

県が指定する場所に納品すること。

第7章 提案書作成要領

7.1 提案書に関する要求事項

提案書に関する要求事項は、次のとおりとする。

7.1.1 提案書の記述に対する要求事項

提案書の内容は、本仕様書で示す事項の全てを満たすことを求めているので、全ての事項に対応した記述をすること。また、記述内容に不備がないよう留意すること。

本仕様書で示す提案事項は、本事業の目標達成に寄与するべく、より優れた提案を求めているものであり、提案内容の性能、技術、ノウハウ、工程等について明確に記述するとともに、具体的根拠を明確に示すこと。

本仕様書に記載されている内容を、提案書に記載しなかった場合でも、仕様書の全ての事項は実施されなければならない。

提案書に記載された提案内容については、受託後、より良い内容となるように県と協議し、提案内容の詳細化やブラッシュアップを実施すること。

7.1.2 提案書の形式

提案書の様式は A4 判用紙に縦書き又は横書きとし、製本すること。ただし、図表等の表現の都合上、用紙の方向や用紙サイズ、記述方向等を一部変更することは差し支えない。

また、提案書の根拠資料については、提案書の末尾にまとめること。

なお、提出部数等は以下のとおりとする。

・紙媒体7部

・紙ベースと同一内容の電子データ（CD-R 又は DVD-R）1枚

（電子データは word、Excel、PowerPoint で作成されたものとする）

7.2 提案書の構成及び記載事項

提案書の記述は、以下の項目の順番と内容に沿った構成とし、「項番」を記載のうえ作成すること。提案に当たっては、本仕様書に示す要件等を踏まえたうえで、根拠を明示し、具体的に記述すること。

(1) 入札参加者の実績に関する提案（仕様書第6章関連）

入札参加者が有する校務支援システム等の設計や構築実績について説明すること。

(2) プロジェクト体制や要員の資格・実績に関する提案（仕様書第6章関連）

本業務の実施体制や要員が有する資格や実績について説明すること。

(3) プロジェクト遂行に関する提案（仕様書第6章関連）

本業務のプロジェクト管理におけるリスクを抽出し、そのリスクに対する方策について具体的に記述し、説明すること。

(4) 次期システムに関する提案（仕様書第3章関連）

次期システム全体構成について対象範囲に沿って提案すること。

また、合わせて、次期システムのコンセプトや次世代の校務デジタル化の実現及び、現状の課題とその解決方法について説明すること。

なお、構築した場合のライフサイクルコストを含めた構築費（イニシャル）・運用保守費（ランニング5年）の見積書の内訳を提出すること。

(5) 次期システムに関する提案（仕様書第4章関連）

①次期システムの機能要件に関する提案

要求（必須）事項については、どのように実現するのかの具体的な方策を記述すること。

提案事項については、何を実現させるのかについて、その手法と共に記述すること。

・インフラシステム（制御・認証・認可等に関する基盤等）

・ネットワーク（県立学校の環境、回線）

・アプリケーション（校務（ダッシュボードを含む）・事務系・学習系・公開系）

・校務系・学習系端末等の ICT 機器

②次期システムの非機能要件に関する提案

信頼性、セキュリティ、可用性、拡張性のそれぞれについて、どのように担保できるのかについて具体的に記述すること。

③次期システムのサービス要件に関する提案

県が示すサービスレベルを確保するために、どのような方策を行うのかについて校内 LAN 運用保守及びヘルプデスクの体制を含め、具体的に記述すること。

また、サービスレベルをさらに高める工夫について提案があれば記述すること。

(6) 委託業務の各工程に関する提案（仕様書第5章関連）

①各工程に関する提案（作業内容、スケジュール）

次期教育情報システムのインフラシステム、ネットワーク、アプリケーション、校務系・学習系端末等の各分野において、各工程（以下ア～ク）を適切に遂行するための作業内容やスケジュールを詳細に記述し提案すること。

ア.システム詳細設計

イ.システム開発・環境構築

ウ.システム動作試験

エ.システム移行

オ.システム操作研修

カ.システム運用保守

キ.運用期間終了後のシステム廃棄

ク.セキュリティポリシー改定

②各工程に関する提案（取組手法・実施方法等）

各工程を主体的且つ効率的・効果的に実施していくための詳細な取組み手法、実施方法、体制等を提案すること。

特に、システムの詳細設計、動作試験、移行、操作研修、試行・展開、セキュリティポリシーの改訂等はステークホルダが多いため、実現性を考慮して、効率的な実施に向けて具体的な考えや工夫を記述すること。

(7) 県内 IT 産業への貢献に関する提案（その他）

県内の IT 技術や情報産業への具体的な貢献内容及び実現方法を提案すること。

7.3 プレゼンテーションについて

提案書の内容について入札参加者によるプレゼンテーションを行うこととし、内容を審査する。

プレゼンテーションは提案書の内容に関する説明や補足を主な目的として実施するものであるため、提出された提案書等を用いて行うものとするが、別途、説明資料（PowerPoint 等）を作成し、説明に用いることは差し支えない。

プレゼンテーションの開催方法は対面形式を想定しており、日時等の詳細は別途通知する。

なお、プレゼンテーションは本業務の遂行において主導的役割を担う予定の者（プロジェクトマネージャー、プロジェクトリーダー等）が行うこととする。

プレゼンテーション（30分）、質疑応答（20分）を想定している。

第8章 その他

8.1 Microsoft ライセンスの共同調達

8.1.1 共同調達範囲

本業務で調達するMicrosoftライセンスに併せて、各市町向けMicrosoftライセンスの共同調達（圏域包括契約）を実施する。

8.1.2 ライセンス契約方法

共同調達においては、各市町が教育委員会で利用するライセンスについて、本県を基本契約とし、受託事業者が各市町と圏域包括契約を締結する。

また、契約に必要となる手続きや費用の算出、説明資料の作成等は受託事業者が行い、本県へ説明したうえで各市町と契約を締結すること。

8.1.3 ライセンス費用算出

本県より共同調達に参加する市町名および必要ライセンス数を入札事業者へ別途提示するため、本委託業務におけるライセンス費用は、共同調達を前提として算出すること。

8.2 業務の再委託

本委託業務を再委託することは認めない。ただし、委託業務の一部についてあらかじめ県から書面による承諾を得た場合は、この限りではない。

8.3 知的財産権の帰属等

知的財産等については、委託契約書による。

8.4 機密保持

(1)受託事業者は、本業務に係る作業を実施するに当たり、県から取得した資料（電子媒体、文書、図面等の形態を問わない。）を含め契約上知り得た情報を、第三者に開示又は本業務に係る作業以外の目的で利用しないものとする。ただし、次のいずれかに該当する情報は、除くものとする。

・取得した時点で、既に公知であるもの

・取得後、受託事業者の責によらず公知となったもの

・法令等に基づき開示されるもの

・佐賀県から秘密でないと指定されたもの

・第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に県と協議の上、承認を得たもの

(2)受託事業者は、県の許可なく、取り扱う情報を指定された場所から持ち出し、或いは複製しないものとする。

(3)受託事業者は、本業務に係る作業に関与した受託事業者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。

(4)受託事業者は、本業務に係る検収後、受託事業者の事業所内部に保有されている本業務に係る佐賀県に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により、速やかに抹消すると共に、県から貸与されたものについては、検収後1週間以内に県に返却するものとする。

8.5 情報セキュリティに関する受託事業者の責任

8.5.1 情報セキュリティポリシーの遵守

受託事業者は、別添の「佐賀県情報セキュリティ基本方針」及び「佐賀県情報セキュリティ対策基準」を遵守すること。

なお、個人情報の扱いについては、契約書別記「個人情報取扱特記事項」を遵守すること。

8.5.2 情報セキュリティを確保するための体制の整備

受託事業者は、佐賀県のセキュリティポリシーに従い、受託事業者組織全体のセキュリティを確保すると共に、発注者から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

8.5.3 脆弱性の管理

IPAの「安全なウェブサイトの作り方」等を参考にセキュアコーディングを実施すること

ソフトウェア等の納品物は新規作成、改修に関わらず、納品前に、アプリケーションおよびプラットフォームの脆弱性診断を行い、問題を解消した上で納品すること。脆弱性診断についても、その結果を報告すること。

ソフトウェア等の納品物はライフサイクルの全期間に渡り脆弱性の監視を行い、新たな脆弱性が確認された際には、県と相談の上、速やかに対応を行うこと。

8.6 履行内容の不適合に係る担保責任

検収後1年間において、納入成果物に仕様書等に適合しないがあることが判明した場合には、受託事業者の責任及び負担において、県が相当と認める期日までに補修を完了するものとする。

8.7 法令等の遵守

(1)受託事業者は、民法（明治29年法律第89号）、刑法（明治40年法律第45号）、著作権法、不正アクセス行為の禁止等に関する法律（平成11年法律第128号）等の関係法規を遵守すること。

(2)受託事業者は、個人情報の保護に関する法律（平成15年法律第57号）及び受託事業者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を適正に取り扱うこと。

8.8 応札条件

本調達における入札説明書に示す「入札参加者の資格に関する事項」を参照すること。

なお、県内の IT 人材育成の観点から、本調達の実施にあたって、受託事業者は下記のいずれかであることが望ましい。

・県内 IT 企業

・県内 IT 企業を含めた共同企業体

・県内 IT 企業を再委託先とする企業

※県内 IT 企業：県内に本店を有する者、県内に支店等を有し、県内支店等に勤務する従業員比率が50%以上の者、又は県内支店等に勤務する従業員が50人以上（うち SE 数が30人以上）の者

8.9 その他

(1)本委託業務を履行するために必要な備品、消耗品等は受託事業者で負担することとし、受託者の保管場所で適切に保管及び管理すること。

(2)本仕様書等に定めがない事項又は疑義のある事項については、県と協議を行い、業務を遂行すること。

(3)本委託業務によって生じる成果品は、県に帰属する。

(4)契約変更を必要とするときや業務の実施方法、その他本仕様書に記載のない事項については県と別途協議すること。

(5)本委託業務の全部若しくは一部を解除し又は契約期間が終了した場合は、受託事業者は当該業務を県が継続して遂行できるよう必要な措置を講じるとともに、引き継ぐ事業者への移行を積極的に支援（情報提供や作業支援を含む）すること。その際、保存されたデータを別のシステムに移行する必要が発生する際は、サーバ上に保存されたデータについて、汎用性のあるデータ形式に変換して提供するとともに、サーバ等記憶媒体上のデータが復元できないよう抹消し、その結果を県に書面で報告すること。また、システムそのもの廃棄も適切に実施すること。なお、実施方法等の詳細については、県と協議するものとする。

(6)地震、台風、洪水、嵐等の自然災害発生時における本業務の実施については、県と協議を行うこと。