

# 上市町教育情報化基盤システム更新業務

## 仕 様 書

令和 7 年 6 月

上市町教育委員会

## 目次

第1章 総則	2
1 業務名	2
2 業務目的	2
3 業務方針	2
4 契約方法及び支払方法	2
5 運用開始予定日	2
6 履行期限	3
7 履行場所	3
8 業務内容・業務範囲	3
9 成果品	4
10 特記事項	4
第2章 利用環境等	5
1 児童生徒数及び教職員数	5
2 教職員端末	5
3 無線A P	5
第3章 導入作業	5
1 導入製品	5
2 導入作業	6
第4章 利用者教育	13
1 教職員向け利用教育	13
2 運用管理者向け利用教育	13
第5章 試験	13
第6章 既存ハードウェア機器の撤去	13
第7章 セキュリティ対策	13
1 認証規格等の取得要件	13
2 権限管理等	13
3 情報資産の取扱い	13

## 第1章 総則

### 1 業務名

上市町教育情報化基盤システム更新業務（以下、「本業務」という。）

### 2 業務目的

文部科学省が提唱する「GIGA スクール構想」に基づき、令和2年度に上市町教育情報化基盤システム（以下、「本システム」という。）を構築し、令和7年度中に本システムに導入したソフトウェアやハードウェア機器等の利用ライセンスや保守サポート期間の満了を迎えることから、本システムの更新を行うこととする。

また、文部科学省の「GIGA スクール構想の下での校務DX」や「教育情報セキュリティポリシー」、「令和7年度以降の学校におけるICT環境の整備方針」などで示されている方針に基づき、校務系・学習系ネットワークの統合及び汎用クラウドツールの利用環境の整備を進め、強固なセキュリティ対策や校務環境のクラウド化を取り入れ、次世代の校務DXの実現を目指す。

### 3 業務方針

本業務の実施にあたり、以下の項目に関する事項に留意すること。

- （1）学習系及び校務系ネットワーク分離を必要とせず、認証によるアクセス制御を前提とした、新たな教育情報化基盤システムを実現する。
- （2）教職員の柔軟な働き方のため、教職員端末はGIGA スクール構想下において整備した教育ネットワーク（以下、「GIGA 系ネットワーク」という。）に接続し、学校内だけではなく、自宅や出張先に持ち運んでも安全に利用可能とするロケーションフリーな校務環境を整備する。

### 4 契約方法及び支払方法

#### （1）契約方法

本業務で調達する全ての内容を賃貸借対象物件として、本業務の受注者選定とは別にリース事業者を選定し、賃貸借契約を締結する。このため、本業務の受注者とは業務の履行に必要な条件等を覚書により契約を締結するものとする。

#### （2）支払方法

本業務の調達にかかる全ての費用は、本業務の引き渡し完了後30日以内に、リース事業者から支払われるものとする。ただし、引き渡し完了日までにリース事業者が決定していない場合は、リース事業者との契約締結後30日以内に支払われるものとする。

### 5 運用開始予定日

令和 7 年 11 月 1 日

## 6 履行期限

(1) ソフトウェア、ハードウェア等の調達及び構築

令和 7 年 10 月 31 日まで

(2) 既存ハードウェア機器の撤去

令和 7 年 12 月 26 日まで

(3) 特記事項

①運用開始予定日は業務状況等で若干の変更が生じる可能性があるため、詳細なスケジュールについては協議の上決定し、受注者は柔軟な稼働日設定が行えること。

②運用開始時においては、システムトラブル等に備え、安全かつ確実な運用が行えるよう、十分な支援体制で臨むこと。

## 7 履行場所

履行場所は、以下のとおりとする。

学校名	住所
相ノ木小学校	上市町上荒又 68
上市中央小学校	上市町横法音寺 1
南加積小学校	上市町広野 768
宮川小学校	上市町中江上 2
白萩西部小学校	上市町丸山 43
陽南小学校	上市町柿沢 424-2
上市中学校	上市町稗田 1
上市町教育センター (上市中学校内)	上市町稗田 1
上市町役場 (電算室及び教育委員会事務局)	上市町法音寺 1

## 8 業務内容・業務範囲

主な業務内容及び業務範囲は以下の通りとする。

(1) 主な業務内容

①校務系・学習系ネットワーク統合

②教育情報化基盤システム更新

③校務環境クラウド化

(2) 調達範囲

- ① ソフトウェアおよびハードウェア機器の調達
- ② 調達したソフトウェアおよびハードウェア機器による環境構築作業  
(設計、設定、納入、移行、据付・調整、試験、本番稼動)
- ③ 利用者への教育
- ④ 成果品の提出
- ⑤ 既存ハードウェア機器等の撤去

9 成果品

- (1) 要件定義書
- (2) 基本設計書
- (3) 詳細設計書
- (4) WBS
- (5) 議事録
- (6) 移行計画書
- (7) 作業報告書
- (8) 導入機器・ソフトウェア一覧表
- (9) 写真台帳 (機器設置の施工前・施工中・施工後)
- (10) 運用管理マニュアル
- (11) データ消去証明書

10 特記事項

- (1) 本業務と並行して次の業務（以下、「関連業務」とする。）を調達するため、本業務及び関連業務の双方間で効率的な構築の実施や互いの作業に支障が生じないよう、発注者の指示により、関連業務の受注者と調整のうえで実施すること。

- ① 授業支援システムサービス調達業務（～令和7年9月予定）
- ② 校務支援システムサービス調達業務（～令和7年11月予定）
- ③ 学習者端末 Google Chromebook 導入（～令和7年9月予定）
- ④ 学習者端末フィルタリングソフト導入（～令和7年9月予定）
- ⑤ Microsoft 365 及び Google Workspace for Education ライセンス導入（～令和7年8月予定）
- ⑥ 教職員端末等 Windows11 アップグレード作業（～令和7年10月予定）
- ⑦ 町内小中学校複合機更新業務（～令和7年9月）

※関連業務は現時点での予定も含むため、今後の業務発注状況や構築作業の進捗状況により変更となる可能性がある。

- (2) 本業務における受注者は、G I G Aスクール構想下において同種業務（全部又は一部）の十分な実績があり、技術管理を行える責任者及び実施体制を有すること。
- (3) 発注者は、受注者から本業務の実施のため既存システムの設定情報等に係る資料等の提供の申し出がある場合は、これを貸与する。
- (4) 本仕様書に定めのない事項その他疑義がある場合は、その都度、双方協議のうえ、定めるものとする。

なお、受注者は本仕様書に明記されていない事項であっても、本システムを適切に動作させるために当然備えるべき性能及び機能（構造）等については、完備しているものとする。

## 第2章 利用環境等

発注時点における主な既存利用環境を以下に示す。

- 1 児童生徒数及び教職員数（令和7年4月1日現在）
  - (1) 児童生徒数
    - 1,058人（小学校 678人、中学校 380人）
  - (2) 教職員数
    - 約150人（小学校、中学校、教育支援施設、教育委員会事務局）
- 2 教職員端末
  - (1) 利用台数
    - 約180台（教職員1人1台用、共用、管理用等）
  - (2) 利用機種
    - ①富士通 LIFEBOOK A579/A (Windows10/Windows11)
    - ②富士通 ARROWS TAB Q7311/FE (Windows10)
    - ③富士通 LIFEBOOK A5511/H (Windows10/Windows11)
    - ④DELL Latitude3540 ADL XCT0 (Windows10/Windows11)
    - ⑤Dynabook Y83/LY (Windows10/Windows11)

※「Windows10」で利用している端末は、関連業務にて Windows11 へアップグレードする予定である。
- 3 無線 AP
  - (1) 機種
    - AT-TQ5403-N5（アライドテレシス社）
  - (2) 管理台数
    - 138台

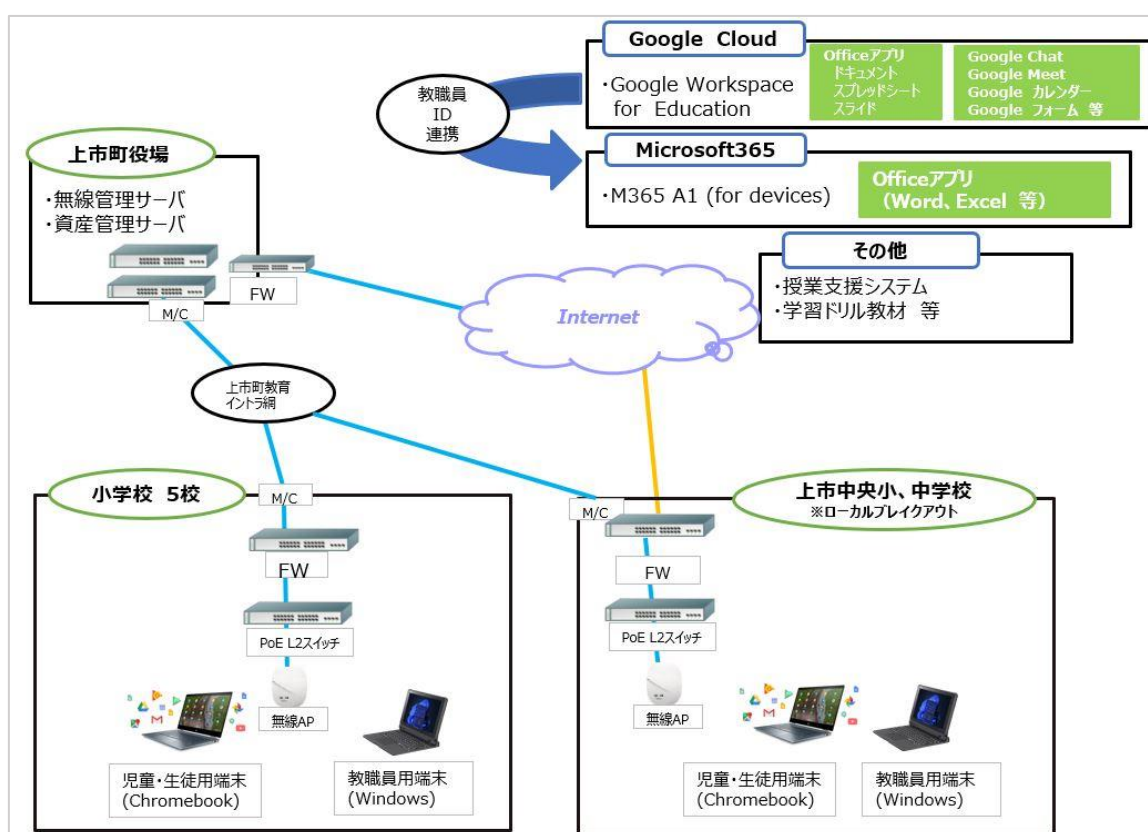
## 第3章 導入作業

- 1 導入製品

- (1) 本業務で導入する製品は、別添1「導入ハードウェア製品及びソフトウェア製品一覧」のとおりとする。
- (2) 導入する製品は全て賃貸借物件の対象とする。
- (3) 調達する製品は5年間利用することを想定していることから導入するハードウェア製品及びソフトウェア製品について、5年間の利用料及び保守料を含むこと。
- (4) 調達する全てのソフトウェアは、原則、導入時の最新バージョンを導入すること。

## 2 導入作業

導入する全体構成のイメージは次の図のとおりである。



### (1) ネットワーク設定

- ①GIGA 系ネットワーク環境を活用し、学習系ネットワーク及び校務系ネットワークを統合してアクセス制御型に沿った構成として有線及び無線で接続できる環境に整備すること。
- ②既存の校務系ネットワークで利用している富山県教育 NOC（以下、「県 NOC」という。）がインターネットサービスの提供を廃止することから、経路設定変更等により対応すること。

なお、県 NOC のインターネットサービスは廃止されるが、県 NOC にある各種システムは継続して利用するため、県 NOC へのアクセス経路は確保すること。

③GIGA 系ネットワーク環境を確認の上、設計し、及び構築すること。

## (2) サーバ構築

### ①基本構成

物理サーバ上に Windows Server OS をインストールし、Hyper-V を利用して 2 台の仮想マシン（ゲスト OS）を構築すること。

＜役割＞

ホスト OS・・・Hyper-V

ゲスト OS 1・・・無線 LAN 管理システム

ゲスト OS 2・・・資産管理システム

### ②資産管理システム

資産管理システムは教職員端末へ新たに導入することから、以下の機能の実現に必要な設定、運用ポリシー等については、発注者と事前に協議の上実施すること。

○教職員端末の資産管理（端末の保有資産情報の自動収集等）

○ログ取得（端末の操作ログ、挙動ログ等の取得）

○EDR 機能（ふるまい検知による未知の脅威の防御）

○外部記憶媒体制御（USB デバイスの利用制限等）

○紛失端末制御（端末紛失時のリモートロック）

### ③無線 LAN 管理システム

無線 LAN 管理システムは既存の管理システムと同等の設定を行うこと。

○無線 AP の個別設定・管理ができるように設定を行うこと

○学校毎にグループを作成し、各グループにて設定・管理ができるように設定を行うこと。

○各学校の各階の図面をインポートし、無線 AP の設置場所がわかるように設定を行うこと。

○設定やファームウェアアップデートのスケジュール配信ができるように設定を行うこと。

## (3) 教職員端末設定

①本業務で調達する新システムの利用にあたり、教職員端末へ以下の設定変更等を行うこと。なお、想定している主な設定は以下のとおりであるが、新システムに必要な設定は明記されていない事項についても設定を行うこと。

○新しいシステム環境に不要となるソフトウェアのアンインストール

○既存ドメイン環境からの降格

○有線 LAN、無線 LAN 環境の接続設定

○Windows 用 Google 認証情報プロバイダ（GCPW）のインストール

○Google Workspace 作業用アカウントでログオン

○新しいシステム環境に必要なソフトウェアのインストール



- プリンタ及び複合機の再設定
- 新しく導入したソフトウェアの設定および動作確認
- データ移行
- BitLocker によるデータ暗号化

- ②上記①の設定は、共用端末や電子黒板等にも同様の設定変更作業を行うこと。
- ③その他学校個別に導入しているソフトウェアや発注者から指示があるものについては、発注者と協議の上導入すること。
- ④既存システムに関わる部分については、発注者と協議の上検証を行うこと。その際、既存保守業者へ確認事項がある場合、必要に応じて発注者より情報開示を行う。また、業者の申し立てがあれば、事前に検証用端末を持ち込んで検証を可とする。
- ⑤既存教職員端末で使用しているプリンタや周辺機器については同様に利用ができるように設定を行う。ただし、OS バージョン依存等により引き続き利用が困難な場合は発注者と協議の上対応方法を検討すること。
- ⑥本業務により調達する管理用端末2台の設定も実施すること。

#### (4) 搬入・設置・調整・廃棄

- ①作業については、学校業務に支障が無いよう配慮すること。  
 なお、ユーザーへの利用者への影響が少なくなるように設定作業は業務時間外や休日に実施することも考慮し作業日の日程を調整すること。
- ②受注者は作業スケジュールを提出し、発注者と協議の上、日程を決定すること。
- ③サーバ機器は発注者の庁舎電算室内既設サーバラックへ設置すること。
- ④エラーや故障等がなく正常に利用可能であることを確認すること。
- ⑤搬入時に出た梱包材などは受注者が責任を持って回収すること。  
 なお、同封されている添付物は発注者へ提供する。但し、発注者にて不要と判断した添付物は受注者にて回収すること。

#### (5) ソフトウェア（クラウドサービス含む）構築

- ①基本概要
  - (ア) 発注者で運用しているドメインによる Google Workspace 環境と密接な運用が実現できる手法により、アカウント管理、アクセス制御管理を実現し、ゼロトラストモデルによる環境を構築すること。
  - (イ) このゼロトラスト環境は、ドメインにおける既存および新規調達された端末を制御するためにモバイルデバイス管理機能を有すること。
  - (ウ) 発注時点で想定する機能要件は以下の通りとする。なお、構築時に以下の機能要件を見直すこともあるため、この場合、発注者と受注者にて協議の上、別に推奨される構成等を設定するものとする。
  - (エ) 本業務で構築する環境に必要な以下の汎用クラウドツールのライセンスは、発注者の関連業務により調達するものを利用すること。

○Google Workspace for Education Plus

○Microsoft 365 A1 for devices

## ②アカウント管理サービスおよび多要素認証によるアクセス制御

### (ア) ユーザー認証

○ユーザーは既存の Google アカウントを使用して認証可能であること。

○ユーザー認証および連携は、Windows11 以降および Chrome OS に対応していること。

○ユーザーID とパスワードは Google Workspace の管理コンソールにて管理可能であること。

### (イ) 多要素認証

○知識情報はパスワード及びPIN コード、所持情報は発注者が所有する教職員用端末、生体情報は顔認証及び指紋認証が設定可能であること。

○発注者が所有・管理する教職員用端末への OS 認証時および Google アカウントへのログイン認証時、Google アカウントのユーザーID に加えて、知識情報・所持情報・生体情報のうち2要素以上を組み合わせた認証が可能となるように設定を行うこと。

○OS 認証時は顔認証または PIN コードにて認証を行えるように設定を行うこと。

## ③アカウント管理サービスによるアクセス制御

### (ア) シングルサインオン(SSO)

○Google を SAML アプリにアクセスするための ID プロバイダ (IdP) として使用し、シングルサインオンを設定することが可能であること。

### (イ) コンテキストウェアアクセス(CAA)

○IP アドレス、デバイス情報、地理情報、時間帯などの属性に基づいて、アプリに対する詳細なアクセス制御セキュリティポリシーが設定可能であること。

○発注者が所有・管理する教職員端末からのアクセス時は、Google Workspace のすべてのコアサービスを利用可能とすること。

○スマートデバイス (iOS、Android に限る) からのアクセス時は、多要素認証が設定されていることを前提として、機微な情報へのアクセスを行わないアプリ (カレンダーやチャットなど) のみ利用可能とし、その他のアプリは利用不可とすること。

## ④ストレージサービス基盤の構成

### (ア) ファイル共有の管理

○Google ドライブ内の重要性・機密性が高い情報資産 (ファイル等) への適切なアクセスレベルおよび保護ルールを設定し、適切なユーザーのみアクセス可能となるように設定すること。

○重要性・機密性が高い情報資産の外部への持ち出し (外部への共有、印刷等)

を適切に制限すること。

○原本を編集されないように、各ユーザーにコピーを共有することが可能であること。

#### (イ) 共有ドライブの管理

○以下の通りファイル管理用の共有ドライブを作成すること。

- ・自治体共通：すべての教職員に対して共有可能とする。
- ・教職員用：対象校に所属するすべての教職員に共有ドライブが表示され共有可能とする。
- ・外部共有用：対象校に所属するすべての教職員に共有ドライブが表示され共有可能とする。
- ・生徒共有用：対象校に所属するすべての教職員に共有ドライブが表示され共有可能とする。
- ・管理職用：対象校に所属するすべての管理職に共有ドライブが表示され利用可能とする。  
ファイル共有は不可とする。
- ・校長用：対象校に所属する校長に共有ドライブが表示され利用可能とする。  
ファイル共有は不可とする。

#### (ウ) Google ドライブの信頼ルール

○個々のユーザー、グループ、組織部門ごとに詳細なアクセスポリシーを適用可能であること。

○教職員用フォルダから生徒用組織部門に属するユーザーへのファイル共有は不可とすること。

#### (エ) ドライブラベルの管理

○外部共有の許可/禁止ラベルを定義することで、機密情報の意図せぬ漏洩を防ぐこと。

○Google ドライブのファイルを URL として添付・共有した場合も、ドライブラベルに応じたファイル参照の制限を行うこと。

#### (オ) データ保護(DLP)

○外部共有用ドライブにファイルが作成またはコピーされた場合に、外部共有禁止のラベルが付与されるように設定すること。

○ファイルを外部ユーザーに共有する際は、学校管理職がラベルを操作することで共有可能にすることが可能であること。

○外部共有禁止ラベルが付与されている場合は、外部組織外へのファイル共有がブロックされるように設定すること。

○ストレージサービスとして Google ドライブを使用すること。

- 重要な情報資産を Google ドライブに保存・運用管理する際には、校務系・学習系ネットワークの統合を踏まえて、情報資産の調査及び棚卸しを行い、情報資産の機密性、完全性、及び可用性を考慮し、被害を受けた場合に想定される影響の大きさに基づいて、それらを分類・仕分けを行うとともに、想定される脅威を整理すること。
- ここで整理する情報資産分類に従い、分類を行った上で、各情報資産のアクセス制御方針に基づいた適切なアクセス制御設定をすること。

#### ④教職員端末のセキュリティ管理

##### (ア) Intune for Education (MDM) 端末管理

- Microsoft 365 A1 for devices ライセンスに付属する Intune for Education を使用し、デバイスのポリシー適用をクラウドで実現すること。
- 構成プロファイル、レジストリ・バッチ配布、更新リングの設定により以下の制御を行うこと。
  - ・タスクバーのニュースの非表示化
  - ・既定のアプリの設定
  - ・BitLocker の有効化 (デバイスの暗号化)
  - ・ストレージセンサーの設定
  - ・エクスプローラーの初期表示および表示対象ドライブ設定
  - ・ユーザプロファイル内の制御対象フォルダのファイル削除
  - ・データ一時保存用フォルダの作成およびファイル削除
  - ・Windows Hello for business 有効化
  - ・初回ログイン時のプライバシー設定の無効化
  - ・Windows Update の設定

##### (イ) Google 認証プロバイダ (GCPW) 認証

発注者が所有・管理する教職員端末に対して Windows 用 Google 認証プロバイダ (GCPW) をインストールし、Google アカウントによる Windows への OS 認証を可能とすること。

##### (ウ) Windows Hello

- 発注者が所有・管理する教職員端末に対して、OS 認証時は顔認証または PIN コード入力にて認証を行えるように設定すること。

##### (エ) 端末の暗号化 (BitLocker)

- 紛失・盗難時の情報漏えい防止のため、Windows 端末の内蔵ストレージを暗号化すること。

##### (オ) ウイルス対策 (ESET PROTECT Advanced)

- Windows 端末にウイルス対策ソフトを導入し、ファイルのアクセス時や実行時にウイルスを検知すること。

○ローカルドライブに個別情報が残らない仕組みを構築することを前提とし、ソフトウェアを導入すること。

(カ) Web フィルタリング (Soliton DNS Guard for Education)

○ローカルブレイクアウトによるネットワーク接続も想定したプロキシ型以外の方式（拡張機能型・DNS 型等のネットワークに依存しない方式）の Web フィルタリングソフトとして、Soliton DNS Guard を導入すること。

(キ) グループポリシー、端末の初期化

○ローカルドライブに個別情報が残らない仕組みを構築すること。

○Intune for Education 端末管理ポリシーにより、以下の通り制御を行うこと。

- ・サインイン時および端末ロック時に、ユーザプロファイル内の対象フォルダ（デスクトップ、ドキュメント、ピクチャ、ビデオ、ミュージック、ダウンロード）のファイルを削除する。
- ・ローカルに自動的にデータ一時保存用フォルダを作成し、対象フォルダへドライブを設定したうえで、ドライブのショートカットをデスクトップに作成する。

(ク) デスクトップ版 Google ドライブ

○デスクトップ版 Google ドライブを導入し、Google ドライブ上のファイルをデスクトップより操作可能とすること。

(ケ) リモートロック

○端末紛失時を想定しリモートロック、端末内データ消去、接続している Wi-Fi 機器等の情報を基に PC の位置情報を表示が可能であること。

(6) 移行作業

- ①学習系及び校務系 Active Directory サーバのアカウント情報を統合し、Google Workspace を認証基盤としたアカウント情報の一元管理へ移行すること。
- ②現在 Microsoft365 にて SSO 環境を構築し利用している別添 2「SSO 利用サービス一覧」のサービスが Google Workspace でも継続し利用できる設定をすること。  
なお、構築時にサービスの増減がある場合等も想定されるため、設定前に発注者と協議すること。
- ③既存の学習系及び校務系ファイルサーバにあるデータを Google Drive の共有ドライブへ移行すること。
- ④学習系及び校務系 IP アドレスとホスト名の管理・運用を行う DNS サービスについては、移行の必要性を調査し、必要であれば移行すること。
- ⑤学習系及び校務系の動的に IP アドレスを割り当てる DHCP サービスについて、移行の必要性を調査し、必要であれば移行すること。
- ⑥既存の校務系ネットワーク経由で利用中の以下のクラウドサービスは IP アドレス制限を行って利用していることから、ネットワーク経路変更等で継続利用できる

よう別途対応を協議すること。

○デジタル採点支援システム「リアテンドント」(大日本印刷(株))

## 第4章 利用者教育

### 1 教職員向け利用教育

本業務で導入した新システムの操作等に関し、教職員向けの利用方法に関する研修会を各校において1回以上開催すること。

なお、実施時期や実施方法、内容等は発注者へ提案し、協議の上行うこととする。

### 2 運用管理者向け利用教育

本業務で導入した新システムの運用管理等に関し、運用管理方法などを記載した手順書作成や説明等を行うこと。

## 第5章 試験

1 導入するシステム等については、初期不良等がないことを確認すること。

2 初期不良が発見された場合は、速やかに発注者と協議の上、対応すること。

## 第6章 既存ハードウェア機器の撤去

1 発注者の指示により本業務後に不要となる既存ハードウェア機器の撤去を行うこと。  
なお、新システムの運用開始後も一定期間継続利用するサーバがあるため、既存サーバのデータ消去及び回収はこのサーバが不要となったタイミングで発注者の指示により実施すること。

2 あらかじめ撤去する機器内のデータ消去を行い、その結果についてデータ消去証明書を発行すること。

## 第7章 セキュリティ対策

### 1 認証規格等の取得要件

①受注者は、ISO/IEC27001 およびプライバシーマーク認証を取得していること。

②クラウドサービスで利用するサーバが、ISO/IEC2701 又は ISO/IEC2701 を取得した事業者により運用されていること。

### 2 権限管理等

アクセス権限のない者がアクセスできないよう制限する機能を有すること。学校を超えたデータ閲覧が生じないように、教員が操作・閲覧等可能な情報の範囲を、当該教員が所属する学校に限定するような適切なアクセス制限を行える環境とすること。

### 3 情報資産の取扱い

- ①パブリッククラウド上で取り扱う保有個人情報については、児童・生徒氏名、学年、組、番号、ユーザーID、メールアドレス、ユーザー名、パスワード等、本システムの利用に必要な最小限の情報に限定すること。
- ②受注者は、本業務の遂行に当たり発注者の所掌する情報資産の保護（データバックアップを含む）について万全を期すものとし、その機密性、可用性及び完全性を維持する上で必要な技術的・物理的・人的セキュリティ対策を行うこと。
- ③受注者は、適切なウイルス対策及びマルウェア対策等を行い、情報の改ざん、毀損及び漏えい等を防止すること。
- ④発注者が受注者において実施している教育内容について報告等を求めた場合は、必要な情報を提供すること。