統合型 ID 管理システム

構築及び運用支援業務

仕様書

令和５年４月

札幌市教育委員会生涯学習部

目次

１　システム調達の概要

⑴　背景及び目的

令和４年３月、文部科学省は「教育情報セキュリティポリシーに関するガイドライン（以下、「ガイドライン」という。）」を改訂し、学校ならではの特徴を考慮した情報セキュリティを確立するための対策基準が示された。

また、GIGA スクール構想により、市立学校ではアプリケーション等のシステムを数多く利用することになり、入学・卒業・転校のたびにシステム用アカウント（以下、「ID」という。）情報等のメンテナンスが必要になるため、これが学校においては大きな業務負担となっている。

本業務は、上記の背景を踏まえ、教職員、児童・生徒の ID を統合管理するための統合型 ID 管理システムを構築・運用し、ID の運用管理業務の効率化及び ID の削除漏れ等の人的なミスを防ぎセキュリティレベルを向上させることを目的とする。

なお、今回設置する統合型 ID 管理システムについては、札幌市学校用ネットワークセンターに一元管理する。

⑵　業務名

統合型 ID 管理システム構築及び運用支援業務

⑶　契約期間

契約締結日から令和６年３月 31 日まで

（うち、構築業務：契約締結日から令和６年２月 29 日まで

運用支援：令和６年３月１日から令和６年３月 31 日まで）

⑷　業務の概要

本業務においては、当該サービスを提供するために、新たに仮想基盤を構築する。本業務の範囲には、統合型 ID 管理システムの構築及び当該サービスの提供を含む。また、サービス提供に必要となるサーバ等機器の調達・提供、機器の設置、設定作業、LAN 配線工事、既存システムへの ID 連携作業、運用保守サポートも本業務に含む。

ただし、電源工事及び既設の基幹Ｌ３スイッチの設定は別途本市が委託する事業者が実施する。その他ネットワーク設定等については本業務に含むが、データセンターの運用管理者と調整の上、作業範囲を明確にし、データセンターの運用管理者が実施する分についてはその限りではない。

なお、サーバ機器等を運用する施設（札幌市学校用ネットワークセンター）は、本市が提供するため、指定する施設のラック内に受託者が用意したサーバ機器等をラッキングすること。

⑸　システムの概要

本業務で構築する統合型 ID 管理システムは本市で運用している校務支援システム（児童生徒情報）から出力されたデータ及び CSV で取り込んだデータを集約し、一括管理を行うシステムとする。また、下記の表に示す対象システムとの ID 連携が可能な形式でのデータを出力し、連携先のシステムにて新規 ID の登録及び不要となった ID の削除を可能とするデータ連携を行う。この際、教育系アプリの一部は外字に対応していないため、その場合は常用漢字への変換を行う。

また、今後も ID 連携が必要なシステムの追加が想定されることから、システムの追加に対し、柔軟に対応できるような機能設計が求められる。

なお、インターネットブラウジングが必要の際は、教育系ネットワークから行うこととし、統合型 ID 管理システムが稼働する仮想基盤からは必要最小限のインターネットアクセスを行うこと。

統合型 ID 管理システムから ID 連携する対象システム一覧

No.	システム名	システム概要
1	Microsoft365	Microsoft 社の SaaS 型のクラウドサービスである。
2	OneDrive	Microsoft 社の SaaS 型のクラウドサービスである。
3	Google Workspace for education	Google 社の教育機関向けの SaaS 型のクラウドサービスである。
4	まなびポケット	教育機関向けの SaaS 型のクラウドサービスである。
5	Adobe Creative Cloud Express	Adobe 社の SaaS 型のクラウドサービスである。
6	Active Directory	Microsoft 社のオンプレミスサービスである。

⑹　利用拠点数及びユーザ数（令和４年５月１日現在）

ア　利用拠点数

319 拠点（内、教育委員会１拠点）

イ　利用ユーザ数

児童生徒　　140,413 人

教職員　　9,692 人

※　登録人数は、増減を考慮し、15%増のアカウント数で問題なく動作する仕様・ライセンスを用意し、上記範囲内において、追加でライセンス費用等が発生しないこと。

※　330 程度の同時接続での運用設計に耐えられること。

ウ　利用ドメイン数

Google Workspace for education では小中学校で１つのドメインを利用している。また、高等学校では高等学校ごとのドメインを利用している。利用しているドメイン数を考慮すること。

(7)　スケジュール

	令和5年度										令和６年度～
	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	
契約予定	★										
要件定義	→	→									
基本設計			→	→							
詳細設計				→	→						
試験設計				→	→						
運用設計						→	→				
構築					→	→	→	→			
各種テスト						→	→	→	→		
既存ネットワークとの接続							→	→			
各学校、運用保守事業者への研修									→		
既存データの移行作業								→	→		

ID 更新作業										→	
本番運用										→	

※　上記スケジュールについては、業務の目安を示しているものであるため、委託者と協議の上、ID 更新作業及び本番運用の開始に遅れがない範囲内での調整を可能とする。

２　基本方針

⑴　安定稼働

導入するサーバ機器等のハードウェアやソフトウェアについて、システムを稼働させるために必要な環境構築及び設定を行うとともに、本市のネットワークセキュリティに配慮した配置とすること。

⑵　安全性の確保

本機能で取り扱う情報は、極めて重要度が高いため、情報漏えいや改ざん、紛失（破棄）などが発生しないように十分に配慮されていること。

⑶　システム利用性

入力画面・参照画面などは、ユーザビリティを考慮して設計（分かりやすい情報表示、入力ガイダンス表示など）すること。

また、平常時やピーク時においてもサービスレベルを保持できる仮想基盤としてサイジングすること。

⑷　システム環境

ア　本システムは、本市が別途契約するネットワーク保守・運用事業者が管理する。

イ　受託者は本システムの運用支援を行う。

ウ　本システムは、校務用端末の Web ブラウザ上で動作するものとする。

⑸　システム利用形態

ア　システムの利用者である市立学校の教員および本市の担当職員は、本市が整備する校務用端末を利用するものとする。

イ　本システムは、Web ベースのシステムとし、クライアント側に特殊なミドルウェアやソフトウェアをインストールする必要なく、本システムの機能が実行可能であるものとする。

⑹　システム利用場所

ア　利用場所は、市立学校及び本市教育委員会の執務室とする。なお、将来的な学校新規開設等に伴い利用場所が増減することがあるため、これに備えた機能設計を行うこと。

イ　システム保守は、札幌市学校用ネットワークセンター内で実施する。

⑺　システム利用端末条件

本システムは、市立学校の教員および本市の担当職員が日常業務で使用する校務用端末（クライアント端末）を使用する。

⑻　データベース要件

本システムの情報については、本市専用のサーバ内に構築し、他の業務システムと独立して運用すること。

⑼　本市が提供するもの

ア　サーバラック　１台

(ｱ) EIA 規格 19 型

(ｲ) 幅×高さ×奥行：800×2,000×1,000 ㎜程度

(ｳ) EIA パネル：40U

(ｴ) 耐震荷重：300kg 程度

(ｵ) 電圧・電流：200Ｖ・30Ａ

イ　ウイルス対策ソフト

ウイルスバスターコーポレートエディション Plus

３　サーバ等の要件

⑴　仮想化基盤サーバの構成要件

ア　統合型 ID 管理システムを稼働させるための仮想化基盤サーバを構築すること。

イ　CPU、メモリ、ディスク容量は、統合型 ID 管理システムを安定して稼働させるために十分なリソースをサイジングすること。

ウ　仮想化基盤サーバを既存ネットワークへ接続する必要があるため、既存ネットワークとの接続に必要なネットワークスイッチ、ネットワークモジュールを本調達の範囲で用意すること。

なお、本市で使用しているネットワークモジュールは 10GBase-T 規格対応品であるため、対応した製品を用意すること。また、既存ネットワークとの接続を冗

長化すること。

エ　仮想化基盤サーバ上で稼働する統合型 ID 管理システムをバックアップする仕組みを導入すること。仮想化基盤サーバで利用するディスクとは別なディスクへバックアップする仕組みとすること。

オ　令和 11 年 2 月末までのオンサイト保守（平日 9 時-17 時）であること。

⑵　バックアップおよびログの要件

ア　仮想化基盤サーバ上に構築する統合型 ID 管理システムのバックアップは定期的にバックアップすること。

イ　サーバ OS のバックアップは週１回行うこととし、バックアップデータの保持期間を１か月とする。

ウ　ID データなどのデータバックアップは毎日行うこととし、バックアップデータの保持期間を１か月とする。

エ　システムログ、操作ログは６か月の保持期間とする。

⑶　セキュリティの要件

ア　個人情報となる ID 情報を扱うシステムのため通信の暗号化を行うこと。設計・開発工程で ID 連携先の対象システムの運用保守業者と暗号化通信の方式を調整すること。但し通信暗号化ができない場合はこの限りではない。

イ　統合型 ID 管理システムのシステム管理者向けの Web GUI を HTTPS で通信暗号化すること。

ウ　統合型 ID 管理システムの利用者向けの Web GUI を HTTPS で通信暗号化すること。

エ　ID 連携先が Active Directory もしくは LDAP 通信の場合、LDAPS で通信暗号化すること。

オ　ID 連携先が Unix/Linux サーバの場合、SSH で通信暗号化すること。

カ　本システムで保有するデータは暗号化すること。

キ　仮想化基盤サーバ上に構築する統合型 ID 管理システムのサーバについてウイルス対策ソフトウェアを導入すること。Windows サーバ用のライセンスについては２-⑼－イに記載したウイルス対策ソフトを使用することができるが、当該製品以外の製品が必要な場合は受託者で用意すること。ウイルス対策ソフトウェアの管理サーバについては、オンプレミス、クラウドを問わない。

ク　バックアップデータについてはセキュリティ対策を講じること。

⑷　ID 管理サーバの構成要件

ア　仮想化基盤サーバ上に構築すること。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　ID 管理サーバ用のソフトウェアを構築時点の最新バージョンでインストールすること。

キ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

⑸　ID 管理 DB サーバ（メタディレクトリ）

ア　仮想化基盤サーバ上に構築すること。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　ID 管理 DB サーバ（メタディレクトリ）用のソフトウェアを構築時点の最新バージョンでインストールすること。

キ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

⑹　ID 管理 Web サーバ

ア　仮想化基盤サーバ上に構築すること。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　ID 管理 Web サーバ用のソフトウェアを構築時点の最新バージョンでインストールすること。

キ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

(7) Microsoft Azure Active Directory 連携用サーバ

ア　仮想化基盤サーバ上に AzureAD 連携用サーバを構築すること。ただし、構成上連携用サーバが必要ない場合はこの限りではない。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　Microsoft Azure Active Directory 連携用ソフトウェアを構築時点の最新バージョンでインストールすること。

キ　源泉 AD からユーザ情報及びグループ情報を取得し、Azure Active Directory へ同期ができるように設定すること。

ク　同期項目及び同期間隔については、本市と協議の上設定すること。

ケ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

(8) Google Workspace 連携用サーバ

ア　仮想化基盤サーバ上に Google Workspace 連携用サーバを構築すること。ただし、構成上連携用サーバが必要ない場合はこの限りではない。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　Google Workspace 連携用ソフトウェアを構築時点の最新バージョンでインストールすること。

キ　源泉 LDAP からユーザ情報及びグループ情報を取得し、Google Workspace へ同

期ができるように設定すること。

ク　同期項目及び同期間隔については、本市と協議の上設定すること。

ケ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

⑼ Adobe Creative Cloud 連携用サーバ

ア　仮想化基盤サーバ上に Adobe Creative Cloud 連携用サーバを構築すること。ただし、構成上連携用サーバが必要ない場合はこの限りではない。

イ　CPU、メモリ、ディスク容量は利用者数に応じて適切に構成すること。

ウ　OS をインストールし、構築時点の最新パッチを適用すること。

エ　OS やソフトウェアのライセンスが必要な場合は、本調達の範囲で用意すること。

オ　仮想化基盤サーバとの互換性を担保するために必要なソフトウェアを導入すること。

カ　Adobe Creative Cloud 連携用ソフトウェアを構築時点の最新バージョンでインストールすること。

キ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

⑽ 無停電電源装置

ア　機器設置先の商用電源が停電となった場合でも、調達する機器を稼働させることができるように無停電電源装置を導入すること。

イ　200V30A ブレーカから無停電電源装置へ電源の入力ができること。コンセント形状は L6-30 とする。

ウ　無停電電源装置に搭載されているバッテリの期待寿命が 5 年以上であること。

エ　ネットワークカードを搭載しており、ネットワーク経由で状態監視が出来ること。

オ　無停電電源装置は給電を継続したままでインバータモジュールの交換、バッテリ交換等のメンテナンス作業が実施出来ること。

カ　商用電源が停電後、調達する機器をシャットダウンできる仕組みを構成すること。

キ　令和 11 年 2 月末までのオンサイト保守（平日 9 時-17 時）であること。

⑾ 保守環境

ア　機能試験を実施することができるリソースを有する保守環境を用意すること。

イ　令和 11 年 2 月末まで利用可能なライセンスを提供すること。なお、オープンソースを利用する場合は、その限りではない。

4　機能要件

⑴　統合型 ID 管理ソフトウェアが有する機能要件

ア　本システムの構成上必要な連携を行う機能を有すること。

イ　本システムは連携先の追加を行う可能性があるため、別途の業務により、追加を行えるような柔軟性のある構築とすること。

⑵　Web ブラウザの要件

ア　Microsoft Edge から本システムの Web GUI を利用できること。

イ　Google Chrome から本システムの Web GUI を利用できること。

ウ　上記ア及びイの導入時のバージョンについては担当課と協議すること。

⑶　アクセス権の要件

統合型 ID 管理システムへのアクセスについて、以下の利用者グループ及びアクセス権を設定すること。

ア　システム管理者グループ

（対象者）・・・システム運用管理者（教育委員会）、保守運用事業者

（権限）・・・・システムに関わるすべての操作に対して権限を設定する

イ　学校管理者権限グループ

（対象者）・・・システム利用者（各学校の職員）

（権限）・・・・各学校の登録内容の修正権限等

⑷　システムの機能（基本）

ア　Web GUI にて本システムへログインし利用できること。

イ　一定時間処理が発生しない場合に、ログイン情報を解除し、再度ログインさせる機能を設けること。

ウ　CSV ファイル形式にて一括で追加・更新・停止の処理ができること。

エ　CSV ファイル形式で取り込む際に、源泉データのエラーチェックが実行でき、エラーが発生した場合は取り込み処理が中断されること。

オ　エラーチェックの内容を確認できること。

カ　CSV ファイル形式で取り込んだデータを連携システムに反映するタイミングを以下から選択できること。

(ｱ) ID 管理 DB への取り込みのみで連携先へ反映しない。

(ｲ) ID 管理 DB への取り込み後に連携先へ即時反映する。

(ｳ) ID 管理 DB への取り込み後に指定の時間にて連携先へ反映する。

キ　CSV ファイルの取り込みや連携先へのデータの反映等の処理については、ネットワーク負荷等を考慮し、主に夜間等に実施されるよう担当課と協議すること。

ク　追加・更新・停止の処理状況を確認できること。

ケ　CSV ファイル形式で一括処理した履歴が確認できること。

コ　上記クの履歴を、以下の検索条件で検索できること。

(ｱ) 処理日（期間指定）

(ｲ) 一括処理名

(ｳ) 処理結果（全て、正常、警告、エラー、キャンセル）

サ　CSV ファイル形式で出力したファイルがダウンロードできること。

シ　校務支援システムで更新した ID 情報を、統合型 ID 管理システムへ取り込めること。取り込み頻度は日次以上で人の手を介さず自動で行うこと。

なお、校務支援システムの ID 情報は校務ネットワーク上の所定の場所に csv 形式で出力されるものとする。(取り込み情報の例：氏名、ふりがな、年、組、出席番号、GoogleID 等　その他連携項目は本市、及び校務支援システムの改修事業者と協議のうえで決定すること。)

ス　上記シの他に手動でのデータの取り込みも可能であること。

セ　連携先のシステムの一部は、本市校務支援システムで使用する外字（札幌市ｍｊ明朝フォント）に対応していないため、常用漢字に変換する機能を有すること。なお、文字コードの変換表は本市が提供する。

ソ　変換前の登録者名情報、自動変換された登録者名情報、学校が修正した登録者名情報がそれぞれ容易に確認可能であること。また、テキストデータ等の一覧でも確認できること。

また、ユーザの操作画面では、自動変換を行った文字に色を付ける等、文字の変換が行われたことについて、ユーザが認識できるようにすること。

タ　本市が提供する外字ファイルが更新された際に、フォントファイルを更新する

ための機能を設計すること。

チ　学年・組・出席番号の情報については、読み込んだ情報と学校が修正した情報が容易に確認可能であること。また、テキストデータ等の一覧でも確認できること。

ツ　GoogleID 等の１-(5)の表　統合型 ID 管理システムから ID 連携する対象システム一覧に記載のシステムと連携するために必要なデータの読み込み、出力ができること。また、今後 ID 連携する対象のシステムが増加した際に対応できるような構成とすること。

テ　連携した ID の削除については、自動削除の有無を連携システムごとに設定できること。

ト　連携した ID の削除については、誤操作を回避するような工夫をすること。

⑸　学校管理者の機能

ア　学校管理者はシステム等の運用に秀でているものであるとは限らないため、データの修正等の運用は誰にでも容易なシステムであること。

イ　ヘルプ機能で操作方法がわかるようにすること。

ウ　操作ボタンの大きさや配置を考慮する、マウスポインタや色、画像などに変化をつけてクリックが可能な領域であることを明示的に表現する等ユーザの使いやすさに配慮すること。

エ　入力時にエラーが発生した場合、エラーメッセージに加えて、エラー箇所が特定できるように画像や色、カーソルなどに変化をつけて明示的に表示すること。

オ　統合型 ID 管理システムが処理に失敗した場合は、学校管理者に統合型 ID 管理システム上で原因等を通知すること。なお、通知する内容は本市と協議の上、決定すること。

カ　ログイン後、学校管理者の権限により利用可能なメニューのみを表示し、学校管理者に利用権限の無いデータへのアクセスが出来ないよう制限できること。

キ　連携先システムのアカウントに対するパスワードリセットができること。

⑹　システム管理者の機能

ア　学校管理者が使用できるすべての機能が使用可能であること。

イ　学校管理者のパスワード変更ができること。

ウ　学校管理者のアクセス権の停止ができること。

エ　学校管理者の停止処理時に削除期限日を設定できること。

オ　Web GUI から停止した学校管理者情報が検索できること。

カ　上記オにおいて、ユーザ ID で検索できること。

キ　上記オで検索した学校管理者を復帰できること。

ク　学校管理者情報のアクセス権を停止解除した場合は、停止前のパスワードで利用できること。

５　性能要件

⑴　オンライン処理性能

応答時間に係る要件は以下のとおりとする。なお、ここで定める応答時間は、サーバがクライアント端末からのリクエスト要求を受けて応答結果を返すまでに要するサーバ内の処理時間（以下、「サーバ処理時間」という。）とし、クライアント端末の処理性能やネットワークの伝送性能等は対象外とする。

ただし、全体のレスポンスタイムを考慮し、クライアント端末の処理性能やネットワークの伝送性能に過剰な負荷がかかることを避けた設計とし、性能テストの際には、サーバ処理時間だけでなく、全体のレスポンスタイムを計測したテストを行うこと。

No.	対象	条件	性能目標値	遵守率
1	画面から操作処理	検索系処理	5 秒以内	90%
2		参照系処理	3 秒以内	90%
3		登録・更新系処理	3 秒以内	90%

⑵　バッチ処理性能

バッチ処理に係る時間は、システムの運用時間（オンラインサービス提供時間、バックアップ時間等）や他システムとの連携等を考慮し、運用に影響を与えない時間で完了できること。

６　設計・開発に係る要件

⑴　設計・開発実施計画書等の作成

ア　本業務の実施に先立ち、本業務に係る作業内容、作業体制、スケジュール（WBS を含む）、成果物等を定めた設計・開発実施計画書を作成し、本市の承認を受けること。

イ　設計・開発実施計画書とあわせて、コミュニケーション管理、進捗管理、品質管理、リスク管理、課題管理、変更管理、セキュリティ管理等の管理要領を定めたプロジェクト管理要領を作成し、本市の承認を受けること。

⑵　要件定義

本書に示す要件を踏まえて、受託者が提案するソフトウェア等の提供する機能を元に、本業務にて提供するシステムの要件定義を行うこと。

⑶　設計

ア　本市が承認した要件定義書の機能要件及び非機能要件を満たすための基本設計及び詳細設計を行い、成果物について本市の承認を受けること。

イ　要件定義書の非機能要件等に基づき、必要なハードウェアの仕様（性能、容量、台数等）、ソフトウェアの仕様（OS やミドルウェア等の製品、エディション、数量等）を整理し、本市の確認を受けること。

ウ　上記イにて整理したハードウェア、ソフトウェアに基づき、インフラ基盤構築に必要な環境設計、パラメータ設計等を行い、成果物について本市の承認を受けること。

エ　本システムの次期更改までの間に計画的に発生する運用・保守の作業内容、その想定される時期等を取りまとめた運用・保守計画書を作成し、本市の承認を受けること。

オ　本市が承認した運用・保守計画書に基づき、運用設計及び保守設計を行い、定常的な作業内容、その想定スケジュール、障害発生時における作業内容等を取りまとめた運用・保守手順書を作成し、本市の承認を受けること。

カ　テスト工程における実施内容、開始条件・終了条件、テストの実施体制、スケジュール、テスト環境、テストデータの利用方針等を定めた全体テスト計画書を作成し、本市の承認を受けること。

キ　本システムは連携先、連携元システム事業者及び運用・保守事業者との調整を経て設計を行うこと。

⑷　環境構築・テスト

ア　設計工程の成果物及び全体テスト計画書に基づき、ソフトウェアの設定、インフラ基盤の環境構築、テストを行うこと。

イ　全体テスト計画書に基づき、テスト工程の実施計画書、仕様書を作成し、本市

の承認を受けること。

ウ　テスト工程の実施計画書に基づき、テストの実施状況を本市に報告すること。

エ　テスト工程の実施結果について、実施結果報告書を作成し、本市の承認を受けること。

オ　個人情報が含まれる情報は、原則、テストデータとして使用しないこと。

カ　テストの内容は以下の内容を含むこと。なお、保守環境については以下の a, b, c について実施すること。

ａ　単体テスト

(a) 単体テストの計画

単体テストに必要なテストケース作成やテスト環境構築、テスト実施を計画すること。また、詳細設計の成果物から単体テストに必要なテストケースを洗い出し、単体テスト仕様書として取りまとめること。

(b) 単体テストの実施

要件どおりに動作するか検証すること。

ａ(a)の計画に基づいたテスト環境を構築し、単体テスト仕様書に基づいてテストを実施し、テスト結果を記録すること。テスト結果に対して品質管理に基づく評価を行い、問題がある場合は本市と協議のうえで是正処置を取ること。

ｂ　結合テスト

(a) 結合テストの計画

結合テストに必要なテストケース作成やテスト環境構築、テスト実施を計画すること。また、基本設計の成果物から結合テストに必要なテストケースを洗い出し、結合テスト仕様書として取りまとめること。

(b) 結合テストの実施

要件どおりに動作するか検証すること。

b(a)の計画に基づいたテスト環境を構築し、結合テスト仕様書に基づいてテストを実施し、テスト結果を記録すること。テスト結果に対して品質管理に基づく評価を行い、問題がある場合は本市と協議のうえで是正処置を取ること。

ｃ　総合テスト

システム全体が要件どおりに作動するかを検証する。

(a) 総合テストの計画

総合テストに必要なテストケース作成やテスト環境構築、テスト実施を計画する。要件分析・基本設計の成果物からシステムテストに必要なテストケースを洗い出し、総合テスト仕様書として取りまとめること。

(b) 総合テストの実施

総合テスト仕様書に基づいてテストを実施し、テスト結果を記録すること。テスト結果に対して品質管理に基づく評価を行い、問題がある場合は本市と協議のうえで是正処置を取ること。

d　受入テストの支援作業

受入テストは委託者側で実施するものであるが、受託者は、本市と協力して受入テストをスムーズに実施できるように必要な支援を行うこと。

(a) 受入テストの計画

受入テストにおいて、委託者と調整の上、テスト実施の計画を策定し、受入テスト計画書として取りまとめること。また、システム全体が機能要件、非機能要件を実現できているかを本市が検証するのに必要なテストケースを要件分析、基本設計、開発の各プロセスの成果物から洗い出し、受入テスト仕様書として委託者と協議上、取りまとめること。

(b) 受入テストの実施支援

受入テスト仕様書に基づいたテストの実施を支援し、テスト結果を記録すること。また、テストの実施状況や結果は本市に報告すること。

⑸　移行

ア　校務支援システム（児童生徒情報）及びActive Directory（教職員情報）のデータについては、担当課と協議・調整のうえで、データ移行に関わる実施方針、実施方法、移行対象データ、スケジュール及び移行手順・仕様等を整理したデータ移行計画書を作成し、実施すること。

イ　移行後のデータについて入念な点検作業を行い、移行業務完了報告書を担当課へ提出すること。

ウ　本システムの利用終了時に、次期システム構築業者からデータ移行に必要なシステム情報（データベース構造等の技術構造を除く）の開示等を求められた際に

は、必要な協力を行うこと。また、本業務で構築する統合型 ID 管理システムの稼働が終了し、次期システムへのデータ移行する際には、必要となる各種データの抽出作業についても本業務に含めること。

⑹ 引継ぎ

本市の学校ネットワークを保守・運用する事業者に、必要な設計・開発内容、成果物等の引継ぎを行うこと。引継ぎに際し必要となる事項については、予め上記事業者の担当者と協議の上、決定すること。

7 運用支援に係る要件

⑴ システム稼働時間

原則 24 時間 365 日とする。ただし、法定電源点検、本市が指定するシステム停止日を除き除く。なお、システムのメンテナンス等、計画的な停止を必要とする場合は、予め担当課と協議の上、最大１日程度の停止を可能とする。

⑵ 基本運用体制

統合型 ID 管理システムの本番運用開始後から契約終了までの期間、平日の９時から 17 時の時間において、担当課の職員及び本市の学校ネットワークを保守・運用する事業者からの電話での問い合わせ対応が可能な運用体制を用意すること。

なお、問い合わせに対する一次回答は原則当日、15 時以降の問い合わせに関しては本市の翌開庁日以内に実施すること。

⑶ 運用開始直後の運用体制

初回の年度更新時は、利用者が操作に不慣れなため、多くの問い合わせが発生することが想定される。この想定に対して、適切な対策及び体制を整えること。

⑷ トラブル対応

ア　業務の継続及び早期復旧を図るため、担当課及び本市の学校ネットワークを保守・運用する事業者から障害発生の連絡があった際には、受託者が窓口となり一元的に原因を分析し、統合型 ID 管理システム自体、連携先・連携元システム、またはサーバ・ネットワーク等機器の障害のいずれであるかの切り分けを行うこと。

イ　切り分けの結果、統合型 ID 管理システム自体に起因する障害であった場合、下記ウのとおり、受託者が障害復旧に向けた対応をとること。また、障害の原因が連携先・連携元システムやサーバ・ネットワーク等機器に起因する障害であった

場合、受託者が委託者とサーバ・ネットワーク機器等の保守業者に連絡し、協力して障害の解決にあたること。連携先・連携元システムに原因がある場合、必要な連絡は委託者内で行う。

ウ　システムに障害等が発生した場合、委託者と協議の上、受託者は速やかに障害復旧に必要な対応を行い、原因・処理結果について速やかに委託者に報告すること。また、業務の継続のため、必要に応じて最新の各バックアップデータへの復元作業を実施すること。

エ　受託者は必要に応じてシステムの各マスタの変更作業を行うこと。

オ　業務処理が異常終了した場合の再処理手順を定め、発生時に速やかに再処理を行えるとともに、再処理時の実行手順誤りによるデータ破壊等を防止するよう体制及び手順を確立すること。

カ　障害等発生等によりデータの破損があった場合はバックアップからの復旧を実施すること。

キ　システムの操作等について、想定されるFAQを提供すること。

⑸　ソフトウェア等のアップデート

ア　運用保守の契約期間内において、導入されているOSのパッチについて、半年ごとに最新版にアップデートを行うこと。

イ　運用保守の契約期間内において、導入されているソフトウェア等について、メーカーのサポート期間終了等に対応するためのアップデートを行うこと。

ウ　上記ア、イの他に、緊急を要する脆弱性等が確認された場合は、担当課と協議の上、迅速に対処すること。

エ　アップデートを行う際には、影響度合い等について、担当課と協議の上決定すること。

⑹　監視体制

統合型ID管理システムの監視はネットワーク保守・運用事業者が実施するため、既存の監視ソフトウェア（Zabbix）が使用可能であり、保守・運用に必要な設定を行うこと。また、保守運用事業者が監視業務を行えるように調整連携を行うこと。

⑺　研修

ア　システム導入後に混乱なくスムーズに操作できるよう、学校管理者向け及びシステム管理者向けマニュアルを作成の上、システム構築後なるべく早期に学校管

理者及びシステム管理者に導入前研修を実施すること。

イ　研修はオンライン形式で実施することすること。また、後日になって、学校管理者が研修の内容を振り返ることができるように、Youtube の限定公開等を用いて、アーカイブを用意すること。

ウ　研修の実施前に、研修の内容、スケジュール体制等を定めた研修計画書を作成し、本市の承認を受けること。

⑻　接続先システムの仕様変更に係る対応

運用開始後に、既存の接続先のシステムの仕様変更等により、障害が発生した場合の改修は運用の範囲内で対応すること。

ただし、上記の仕様変更等により、導入したソフトウェア等では、連携そのものが技術的に不可能となった場合は、代替の解決方法とそれに実施する場合の見積を提出すること。

８　本業務の実施体制

⑴　全体の体制

札幌市教育委員会生涯学習部総務課が本業務の担当課となり、本市側の統括責任者及び実施責任者を配置し、本市の関係部門や関連事業者との連携を行う想定であるが、本業務の受託者においても、本業務の円滑な推進のため、主体的に関係部門、関係事業者との連携を図ること。

ア　本市が契約する保守事業者と緊密な連携をとり、常に相互に最新の情報を共有すること。

イ　他の事業者や関係部門からの求めに応じて、資料の提示やヒアリング対応、質問に対する回答や指摘事項に対して協力すること。

ウ　本書に記載のない細部事項、業務上の問題点等については、本市側の統括責任者及び実施責任者と協議し、合意の上実施すること。

⑵　受託者の実施体制

受託事業者は、本業務を効率良く実施できるよう、以下に示すプロジェクト体制を整備すること。

ア　本業務の全体を統括する責任者として、統括責任者を配置すること。

イ　本業務の実務の責任者として、実施責任者（プロジェクトマネージャー）を配

置すること。

ウ　業務別のチームを必要に応じて整備し、それぞれのチームにチームリーダーを配置すること。

エ　本業務に携わる本市や他事業者等、全ての者を含む体制図を明示し、実施計画書に記載すること。

オ　担当者の交代、担当者の増員及び減員がある場合は、体制図を更新するとともに、速やかに本市に報告すること。

⑶　作業場所

ア　本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受託者の責任において用意すること。

イ　定期的に開催する会議については、本市の会議室を用意する。

ウ　会議は原則対面で実施することとするが、受託者側の一部の参加者向けに電話会議や Web 会議等を併用することも可とする。ただし、少なくとも受託者から１名は本市側の参加場所に同席し、電話会議や Web 会議等に必要な環境の持ち込み及びセットアップを行うこと。

エ　本番環境及び保守環境を用いた構築、テストや移行等を行う際は、本市にて作業場所を用意するため、作業日時や作業人数等を本市とあらかじめ協議し、必要最小限の作業時間、作業環境となるよう計画すること。

オ　作業場所に立ち入る際には、あらかじめ委託者に日時等を伝え、許可を得た上で、本市の指示に従い立ち入ること。

カ　受託者の作業従事者は、作業場所へ立ち入る際、常に身分証明書を上半身の見やすい位置に着用するものとする。

⑷　作業の管理に関する要領

受託者は、本業務の実施に先立ち、コミュニケーション管理、進捗管理、品質管理、リスク管理、課題管理、変更管理、セキュリティ管理等の管理要領を定めたプロジェクト管理要領を作成し、当該要領に基づき、本業務に係るプロジェクト管理を適切に行うこと。

９　成果物の範囲、納品期日等

⑴　成果物

本業務における成果物は以下表のとおりとする。また、本市との協議により必要と判断された成果物が生じた際には、別途提出すること。

なお、受託者が提案する開発手法やパッケージソフトウェアの利用により、成果物の作成が不要なものがある場合は、事前に本市と協議の上、納品物を対象外とすることについて本市の承認を受けること。

No.	成果物名	内容	納品期日・補足
1	実施計画書	本業務に係る作業内容、作業体制、スケジュール（WBS を含む）、成果物等を定めた文書。	契約締結日から 2 週間以内
2	プロジェクト管理要領	本業務を適切に関するためのコミュニケーション管理、進捗管理、品質管理、リスク管理、課題管理、変更管理、セキュリティ管理等の管理要領を定めた文書。	契約締結日から 2 週間以内
3	プロジェクト管理要領に基づく管理資料、報告資料	プロジェクト管理要領に基づく進捗報告書、品質報告書、課題管理台帳、リスク管理台帳等の各種管理資料及び報告資料。	随時（原則毎週）
4	要件定義書	受託者が提案する仮想化ソフトウェアを踏まえて、本業務に係る機能及び非機能要件を詳細化した文書。	プロジェクト計画書に定める期日
5	基本設計書	機能設計、システム方式設計、情報セキュリティ設計等の設計内容を記載した文書。	プロジェクト計画書に定める期日
6	詳細設計書	仮想化ソフトウェアの導入・設定、基盤の導入・構築（OS、ミドルウェア等の導入を含む）、必要な詳細仕様、パラメータ等を定めた文書。	プロジェクト計画書に定める期日
7	工程完了報告書	要件定義、基本設計、詳細設計の各工程の完了を本市が判定・承認するための報告書。（各テスト工程については、各テスト工程の実施結果報告書で代替とする。）	プロジェクト計画書に定める期日
8	全体テスト計画書	各テスト工程の定義、実施内容、開始条件・終了条件、テストの実施体制、スケジュール、テスト環境、テストデータの利用方針等を定めた文書。	プロジェクト計画書に定める期日
9	単体テスト実施計画書	テストの対象範囲、開始条件・終了条件、合否判定基準、テスト環境、スケジュール、テスト方法、テストデータの利用方針等を定めた文書。	プロジェクト計画書に定める期日
10	単体テスト仕様書	テストのテストシナリオ、テストケース、確認・検証事項、テスト結果の予測、テスト結果として求めるエビデンス等を定めた文書。	プロジェクト計画書に定める期日
11	単体テスト実施結果報告書	テスト仕様書に基づくテスト結果と、結合テスト実施計画書で定めた終了条件及び合否判定基準に基づく分析結果をまとめた文書。	プロジェクト計画書に定める期日
12	結合テスト実施計画書	テストの対象範囲、開始条件・終了条件、合否判定基準、テスト環境、スケジュール、テスト方法、テ	プロジェクト計画書に定める期日

		ストデータの利用方針等を定めた文書。	
13	結合テスト仕様書	テストのテストシナリオ、テストケース、確認・検証事項、テスト結果の予測、テスト結果として求めるエビデンス等を定めた文書。	プロジェクト計画書に定める期日
14	結合テスト実施結果報告書	テスト仕様書に基づくテスト結果と、結合テスト実施計画書で定めた終了条件及び合否判定基準に基づく分析結果をまとめた文書。	プロジェクト計画書に定める期日
15	総合テスト実施計画書	テストの対象範囲、開始条件・終了条件、合否判定基準、テスト環境、スケジュール、テスト方法、テストデータの利用方針等を定めた文書。	プロジェクト計画書に定める期日
16	総合テスト仕様書	テストのテストシナリオ、テストケース、確認・検証事項、テスト結果の予測、テスト結果として求めるエビデンス等を定めた文書。	プロジェクト計画書に定める期日
17	総合テスト実施結果報告書	テスト仕様書に基づくテスト結果と、結合テスト実施計画書で定めた終了条件及び合否判定基準に基づく分析結果をまとめた文書。	プロジェクト計画書に定める期日
18	受入テスト実施計画書（案）	テストの対象範囲、開始条件・終了条件、合否判定基準、テスト環境、スケジュール、テスト方法、テストデータの利用方針等を定めた文書。	プロジェクト計画書に定める期日
19	受入テスト仕様書（案）	テストのテストシナリオ、テストケース、確認・検証事項、テスト結果の予測、テスト結果として求めるエビデンス等を定めた文書。	プロジェクト計画書に定める期日
20	移行計画書	移行の対象範囲、スケジュール、作業概要、実施方針、移行環境・ツール、実施体制・役割分担等を定めた文書。	プロジェクト計画書に定める期日
21	学校管理者向けマニュアル	一般利用者向けの本システムの操作手順、説明等を記載した文書。	プロジェクト計画書に定める期日
22	システム管理者向けマニュアル	本市職員のシステム管理者向けの本システムの操作手順、説明等を記載した文書。機能分類別にシステム管理者が異なる場合は、分割して作成すること。	プロジェクト計画書に定める期日
23	研修計画書	学校管理者に対し、導入前に操作方法等を伝達する研修の内容、スケジュール、体制等について定めた文書。	プロジェクト計画書に定める期日
24	運用・保守引継ぎ書	本市の学校ネットワークの運用・保守事業者が仮想基盤を運用・保守するにあたり、必要となる引継ぎ事項をまとめること。	プロジェクト計画書に定める期日
25	各種会議の配布資料	受託者が主催する会議体における配布資料一式。	会議開催当日中 ※会議時は紙資料で参加者分配布し、別途電子ファイルをメールで納品すること
26	議事録	受託者が主催する会議体における決定事項、アクションアイテム及び検討内容等を記録した文書。	会議開催から 3 営業日以内 ※電子ファイルをメー

			ルで納品すること

⑵ 納品方法

ア　成果物は、全て日本語で作成すること。ただし、日本国内おいても、英字で表記されることが一般的な文言については、英字で記載しても構わないものとする。

イ　情報処理に関する用語の表記については、日本工業規格（JIS）の規定を参考にすること。

ウ　成果物は紙媒体及び電磁的記録媒体により作成し、別途要件として部数を示す場合を除き、原則紙媒体として１部、電磁的記録媒体として１部を納品すること。

エ　電磁的記録媒体による納品について、Microsoft Word 2019、Microsoft Excel 2019、Microsoft Power Point 2019 で読み込み可能なファイル形式で作成し、SSD の媒体に格納して納品すること。ただし、本市が他の形式による提出を求める場合は、協議の上、これに応じること。

オ　納品後、本市において改変が可能となるよう、図表等の元データも併せて納品すること。

カ　成果物の作成に当たって、特別なツールを使用する場合は、本市の承認を得ること。

キ　成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

ク　電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処すること。

⑶ 知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受託者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て本市に帰属するものとする。

イ　本市は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、

改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、受託者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下、「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により本市がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

ウ　納品される成果物に第三者が権利を有する著作物（以下、「既存著作物等」という。）が含まれる場合には、本市が特に使用を提示した場合を除き、受託者は当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続きを行うこと。この場合、受託者は、当該既存著作物等について事前に本市の承認を得ることとし、本市は、既存著作物等について当該許諾条件の範囲で使用するものとする。

エ　受託者は本市に対し、一切の著作者人格権を行使しないものとし、また、第三者をとおして行使させないものとする。

オ　本業務に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら本市の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、本市は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講ずる。

⑷　契約不適合責任

ア　受託者は、本業務について契約の内容の不適合に対する責任を負うものとする。本市が不適合を知ってから、１年以内に事業者に通知した場合、その不適合が本市の指示によって生じた場合を除き（ただし、受託者がその指示が不適当であることを知りながら、又は過失により知らずに告げなかったときはこの限りでない。）、受託者の責任及び負担において速やかに修正等を行い、指定された日時までに再度納品するものとする。なお、修正方法等については事前に本市の承認を得てから着手するとともに、修正結果等についても本市の承認を受けること。

イ　本市は、前項の場合において、不適合の修正等に代えて、当該不適合により通常生ずべき損害に対する賠償の請求を行うことができるものとする。また、不適合を修正してもなお生じる損害に対しても同様とする。

⑸ 検収

ア　受託者は、成果物等について、納品期日までに本市に内容の説明を実施して検収を受けること。

イ　検収の結果、成果物等に不備又は誤り等が見つかった場合には、受託者は直ちに必要な修正、改修、交換等を行い、変更点について本市に説明を行った上で、指定した日時までに再度納品すること。

10　情報セキュリティ対策及び個人情報保護要件

本業務の履行に当たっては、「個人情報の保護に関する法律」、「札幌市個人情報の保護に関する法律施行条例」、「札幌市教育情報セキュリティポリシー」、「札幌市情報セキュリティ技術対策基準」及び別紙１「個人情報取扱安全管理基準」を遵守し、また、個人情報保護のため、別紙２「個人情報取扱安全管理基準申出書」を提出し、その内容について業務履行開始前までに担当課の評価を受けること。

なお、「札幌市教育情報セキュリティポリシー」及び「札幌市情報セキュリティ技術対策基準」は外部に非公開の内容であることから、詳細については別途契約業者に対して本市から情報を提供するものとする。

⑴ 個人情報保護

本業務の履行にあたり、本システムで取扱う個人情報については、その保護の観点から作業種別に関わらず、個人情報の紛失、漏えい及び改ざんなどが発生しないように十分に留意し、セキュリティ対策について万全の対応を図るとともに、「個人情報の保護に関する法律」、「札幌市個人情報の保護に関する法律施行条例」及び「札幌市教育情報セキュリティポリシー」に従い、個人情報を適切に扱うものとする。

また、本市が提示した資料やデータなどは、本業務以外の目的で使用してはならない。さらに、これらの資料やデータなどは、機密保持可能な特定の作業場所で管理し、作業場所、作業者を報告するとともに、作業終了後までに本市に返却すること。

11　その他

⑴ 機密保持

受託者は、本業務の実施過程で知り得た機密情報、札幌市が開示した情報、他の

担当業者が開示した情報、その他営業機密情報（受託者が作成した情報を含む。）について、本業務の目的以外に使用、または第三者に開示もしくは漏えい、流出、棄損、紛失等をしてはならないものとし、そのための必要な措置を講じることとする。業務において実存する個人データを使用する場合は、予め本市の承認を得ること。また、使用目的を達した場合には、直ちに当該のデータを削除すること。

なお、テストを含む開発段階で使用した開発用機能に、システムへのアクセスに用いる情報（ID やパスワード等）を設定した場合は、開発又は試験の終了後に、これらを確実に除去し、運用後の不正アクセスが発生しないようにすること。

⑵ 監査・調査

本契約の適正な履行を確保するため、必要と認められる場合は、本市およびその委託を受けた第三者による、事業者の所管する施設などに対する定期または、随時の立ち入り調査などに誠実に協力すること。

⑶ 再委託の制限

受託者は、本業務の適正な履行を確保するために必要な範囲内において、本市の承認を得た上で、業務の一部を第三者に再委託することができるものとする。ただし、本業務のうち総合的な企画及び判断並びにプロジェクト管理を第三者に委託してはならない。

受託者は、業務の一部を第三者に再委託したときは、再委託先に自身に求められる情報セキュリティ水準と同等の水準を確保させるとともに、再委託先が実施する情報セキュリティ対策及びその実施状況を本市に報告すること。

⑷ その他

ア　委託内容に関する不明な事項については、担当課と協議すること。

イ　この仕様書に定めのない事項については、担当課との協議合意によるものとする。また受託後、本仕様の変更が必要になった場合には、本市及び受託者と協議合意の上、対応するものとする。

ウ　システムの構築、保守作業はリモート不可のため、現地対応すること。

エ　その他、ユーザの利便性・運用上で有効な機能があれば、提案をすること。

【別紙１】

個人情報取扱安全管理基準

１　個人情報の取扱いに関する基本方針、規程及び取扱手順の策定

個人情報の適正な取扱いの確保について基本方針を策定していること。

また、以下の内容を記載した個人情報の保護に関する規程及び個人情報の取扱手順等が定められていること。

(1) 組織的安全管理措置

(2) 人的安全管理措置

(3) 物理的安全管理措置

(4) 技術的安全管理措置

※　上記(1)～(4)の具体的内容については、個人情報保護委員会ホームページ（https://www.ppc.go.jp）に掲載されている「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」の「４－３－１」の「安全管理措置（法第６６条）」を御確認ください。

２　個人情報の取扱いに関する総括保護管理者及び保護管理者の設置

個人情報の取扱いに関する総括保護管理者及び保護管理者が定められており、基本方針、規程及び個人情報の取扱手順等に明記されていること。

３　従業者の指定、教育及び監督

(1) 個人情報の秘密保持に関する事項が就業規則等に明記されていること。

(2) 個人情報を取り扱う従業者を指定すること。

(3) 個人情報の取扱い、情報システムの運用・管理・セキュリティ対策及びサイバーセキュリティの研修計画を策定し、従業者に対し毎年１回以上研修等を実施していること。また、個人情報を取り扱う従業者は、必ず１回以上研修等を受講している者としていること。

(4) 総括保護管理者及び保護管理者は、従業者に対して必要かつ適切な監督を行うこと。

4　管理区域の設定及び安全管理措置の実施

(1) 個人情報を取り扱う管理区域を明確にし、当該区域に壁又は間仕切り等を設置すること。

【管理区域の例】

・　サーバ等の重要な情報システムを管理する区域

・　個人情報を保管する区域

・　その他個人情報を取り扱う事務を実施する区域

(2) (1)で設定した管理区域について入室する権限を有する従業者を定めること。

また、入室に当たっては、用件の確認、入退室の記録、部外者についての識別化及び部外者が入室する場合は、管理者の立会い等の措置を講ずること。さらに、入退室の記録を保管していること。

(3) (1)で設定した管理区域について入室に係る認証機能を設定し、パスワード等の管理に関する定めの整備及びパスワード等の読取防止等を行うために必要な措置を講ずること。

(4) 外部からの不正な侵入に備え、施錠装置、警報措置及び監視装置の設置等の措置を講ずること。

(5) 管理区域では、許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずること。

5　セキュリティ強化のための管理策

情報資産の盗難、紛失、持出し、複写・複製、目的外の使用及び第三者への提供を防止するため以下の対策を実施していること。

(1) 個人情報の取扱いに使用する電子計算機等は、他のコンピュータと接続しない単独による設置又は当該業務に必要な機器のみと接続していること。また、インターネット及び当該業務を実施する施設外に接続するイントラネット等の他のネットワークに接続していないこと。ただし、本市の許可を得た場合はこの限りでない。

(2) 個人情報の取扱いにおいてサーバを使用している場合は、当該業務を実施する施設内に設置していること。また、サーバへのアクセス権限を有する従業者を定めること。さらに、部外者のアクセスは必要最小限とし、管理者の立会い等の措置を講ずること。ただし、本市の許可を得た場合はこの限りでない。

(3) 個人情報の取扱いにおいて使用する電子計算機等は、アクセス権等を設定し、使用できる従業者を限定すること。また、アクセスログやログイン実績等から従業者の利用状況を記録し、保管していること。

(4) 記録機能を有する機器の電子計算機等への接続制限について必要な措置を講ずること。

(5) 本市が貸与する文書、電子媒体及び業務にて作成した電子データを取り扱う従業者を定めること。

(6) 業務にて作成した電子データを保存するときは、暗号化又はパスワードにより秘匿すること。また、保存した電子データにアクセスできる従業者を限定するとともにアクセスログ等から従業者の利用状況を記録し、契約期間終了後、１年以上保管していること。

(7) 本市が貸与する文書及び電子媒体は、施錠できる耐火金庫及び耐火キャビネット等にて保管すること。また、書類の持ち出し記録等を作成していること。

(8) 個人情報の取扱いにおいて使用する電子計算機は、従業者が正当なアクセス権を有する者であることをユーザ ID、パスワード、磁気・IC カード又は生体情報等のいずれかにより識別し、認証していること。

(9) 個人情報の取扱いにおいて使用する電子計算機は、セキュリティ対策ソフトウェア等（ウィルス対策ソフトウェア等）を導入していること。

(10) 業務にて作成した電子データを削除した場合は、削除した記録を作成していること。また、削除したことについて証明書等により確認できる措置を講ずること。

(11) 個人情報の取扱いにおいて使用する電子計算機等を廃棄する場合は、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用すること。

(12) 本市の許可なく第三者に委託しないこと。

6　事件・事故における報告連絡体制

(1) 従業者が取扱規程等に違反している事実又は兆候を把握した場合の管理者への報告連絡体制を整備していること。

(2) 情報の漏えい、滅失又は毀損等事案の発生又は兆候を把握した場合の従業者から管理者等への報告連絡体制を整備していること。

(3) 情報の漏えい、滅失又は毀損等事案が発生した際の本市及び関連団体への報告連絡体制を整備していること。併せて、事実関係の調査、原因の究明及び再発防止策の検討並びに決定等に係る体制及び手順等を整備していること。

7　情報資産の搬送及び持ち運ぶ際の保護体制

本市が貸与する文書、電子媒体及び左記書類等に基づき作成される電子データを持ち運ぶ場合は、施錠した搬送容器を使用すること。また、暗号化、パスワードによる保護、追跡可能な移送手段等により、破損、紛失、盗難等のないよう十分に配慮していること。

8　関係法令の遵守

個人情報の保護に係る関係法令を遵守するために、必要な体制を備えていること。

9　定期監査の実施

個人情報の管理の状況について、定期に、及び必要に応じ、随時に点検、内部監査及び外部監査を実施すること。

１０　個人情報取扱状況報告書の提出

本市の求めに応じ、又は当該業務契約に基づき、各月の期間ごとの役務完了の書面提出時において、本市が指定する様式にて個人情報取扱状況報告書を提出すること。

１１　情報セキュリティマネジメントシステム（以下「ISMS」という。）又はプライバシーマーク等の規格認証

ISMS（国際標準規格 ISO/IEC27001:2013、日本工業規格 JISQ27001:2014)、プライバシーマーク（日本工業規格 JISQ15001:2006）等の規格認証を受けていること。

【別紙２】

個人情報取扱安全管理基準適合申出書

年　　月　　日

（申請者）

貴市の個人情報取扱安全管理基準について下記のとおり適合していることを申し出ます。

記

●個人情報取扱安全管理基準及び確認事項

※　本申出書において各種資料のご提出をお願いしております。資料が提出できない場合は、実地の監査、調査等の際などに当該書類の内容を確認いたします。

１　個人情報の取扱いに関する基本方針、規程及び取扱手順の策定

貴社の策定した個人情報の取扱いに関する基本方針、規程及び取扱手順等をご記入ください。併せて、当該規程をご提出ください。

２　個人情報の取扱いに関する総括保護管理者及び保護管理者の設置

個人情報の取扱いに関する総括保護管理者及び保護管理者を記載した書類をご提出ください。上記１により提出した基本方針等に記載がある場合は提出不要です。なお、付箋等で該当箇所をご教示願います。

３　従業者の指定、教育及び監督

(1) 当該業務に従事する従業者を「従業者名簿」にてご提出ください。

(2) 従業者の秘密保持に関する事項が明記されている書類をご提出ください。

(3) 従業者を対象とした研修実施報告書等をご提出ください。

4　管理区域の設定及び安全管理措置の実施

設定した管理区域の詳細についてご記入ください。□欄は管理区域に当該装置を設置している場合、■とチェックしてください。また、個人情報を黒塗りにした各管理区域の入退室記録を提出してください。

・管理区域の名称……

入退室の認証方法……

入退室記録の保存期間……

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器……

・管理区域の名称……

入退室の認証方法……

入退室記録の保存期間……

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器……

・管理区域の名称……

入退室の認証方法……

入退室記録の保存期間……

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器……

・管理区域の名称……

入退室の認証方法

入退室記録の保存期間

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器

5　セキュリティ強化のための管理策

セキュリティ強化の詳細についてご記入ください。貴社のセキュリティが各項目の内容に合致している場合は、□欄を■とチェックしてください。

(1) 個人情報の取扱いに使用する電子計算機のセキュリティについて

□　他のネットワークと接続していない。

□　従業者にアクセス権限を設定している。

　　従業者の利用記録の保存期間（　　）

□　記録機能を有する機器の接続制御を実施している。

　　接続制御の方法（　　）

□　従業者の認証方法（　　）

□　セキュリティ対策ソフトウェア等を導入している。

※個人情報を黒塗りにした従業者の利用記録を提出してください。

(2) 文書、電子媒体の取扱いについて

□　取り扱うことができる従業者を定めている。

□　文書、電子媒体の持ち出しを記録している。

　　当該記録の保存期間（　　）

□　文書、電子媒体等について施錠できる耐火金庫等に保管している。

※個人情報を黒塗りにした文書、電子媒体の持ち出し記録を提出してください。

(3) 業務にて作成した電子データの取扱いについて

□　取り扱うことができる従業者を定めている。

□　電子データを保存する時は、暗号化又はパスワードを設定している。

□　電子データの利用状況について記録している。

□　作成した電子データの削除記録を作成している。

※個人情報を黒塗りにした電子データの利用状況の記録及び削除記録を提出してください。

6　事件・事故における報告連絡体制

個人情報取扱安全管理基準の「６　事件・事故における報告連絡体制」(1)から(3)までの内容を満たしていることが分かる書類を提出してください。上記１にて提出した基本方針等に記載がある場合は提出不要です。なお、付箋等で該当箇所をご教示願います。

7　情報資産の搬送及び持ち運ぶ際の保護体制

情報資産を搬送及び持ち運ぶ際の保護体制についてご記入ください。貴社の保護体制が各項目の内容に合致している場合は、□欄を■とチェックしてください。なお、その他の対策を実施している場合は、対策をご記入ください。

□　情報資産を持ち運ぶ場合は、施錠した搬送容器を使用している。

□　上記以外の盗難及び紛失対策を実施している。

※対策を以下にご記入ください。

8　関係法令の遵守

個人情報の保護に係る関係法令を遵守するための体制及び取組等をご記入ください。

9　定期監査の実施

貴社の内部監査及び外部監査の実施状況についてご記入ください。各監査の実施状況が各項目の内容に合致している場合は、□欄を■とチェックしてください。また、各監査の実施状況が分かる書類をご提出ください。なお、外部監査は情報セキュリティマネジメントシステム等の認証を受ける際の審査を外部監査として取り扱っても問題ございません。その場合は、各種申請の認証通知を監査の実施状況の書類といたします。

□　内部監査を実施している。

□　外部監査を実施している。

１０　情報セキュリティマネジメントシステム（以下「ＩＳＭＳ」という。）、プライバシーマーク等の認証等、貴社が取得しているセキュリティ関連の認証についてご記入ください。

また、認証を受けたことが分かる書類をご提出願います。

取得しているセキュリティ関連の認証（ＩＳＭＳ・プライバシーマーク等）

名称……

認証年月日……　最終更新年月日……

名称……

認証年月日……　最終更新年月日……

名称……

認証年月日……　最終更新年月日……