武蔵村山市校内通信ネットワーク環境等

更新業務仕様書

令和５年１２月

教育部教育総務課

1　件名

武蔵村山市校内通信ネットワーク環境等更新業務

2　業務目的

本業務は、武蔵村山市（以下「市」という。）の小・中学校に勤務する教職員が使用する校務支援システム（以下「システム」という。）を新たな機能が搭載されたシステムに更新し、これに対応した校内通信ネットワーク環境を構築するとともに、教職員の働き方改革をさらに推進し、教職員が児童・生徒一人一人と向き合う時間を創出することにより、教育活動の質の向上に資することを目的とする。

3　本業務の構築方針

次に掲げる方針を考慮した提案を実施すること。

⑴　ネットワーク構成

教職員の働き方改革の実現の観点から、校務用、指導用に分けられた２台の端末を１台に集約し、かつ、無線化することにより業務効率化及び負担軽減を図る。また、校内に限らず、出張先や自宅等でもロケーションフリーで校務系・学習系データへ接続可能な環境を整備し、教職員一人一人の事情に合わせた柔軟かつ安全な働き方を実現できる環境とする。

⑵　セキュリティ環境

文部科学省公開の「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～（令和５年３月８日）」に示されている「アクセス制御を前提としたネットワークにおける情報セキュリティの確保（イメージ）」を踏まえたセキュリティ環境を構築する。

⑶　システムの構築

ア　教職員の負担軽減の実現

教務系（成績管理、出欠管理、時数管理等）、保健系（健康診断情報、保健室来室履歴情報等）、学籍系（指導要録等）などの機能が統合されたシステムを活用し、教職員の業務効率化及び負担軽減を図る。

イ　信頼性・安定性の確保

システムの信頼性が保たれるよう、十分な実績や体制を備え障害発生が少ないこと。

また、障害が発生した際にも運用停止が極力発生しないこと。

ウ　業務継続性の実現

災害時等においても継続して業務を遂行できるよう、クラウド環境を活用した冗長等の対策が講じられていること。

エ　拡張性・経済性

市内小・中学校の統廃合や学習指導要領の改訂にも柔軟に対応できる拡張性があること。

また、それらの対応が発生した際には、費用が安価に抑えられるよう経済性及び拡張性に優れていること。

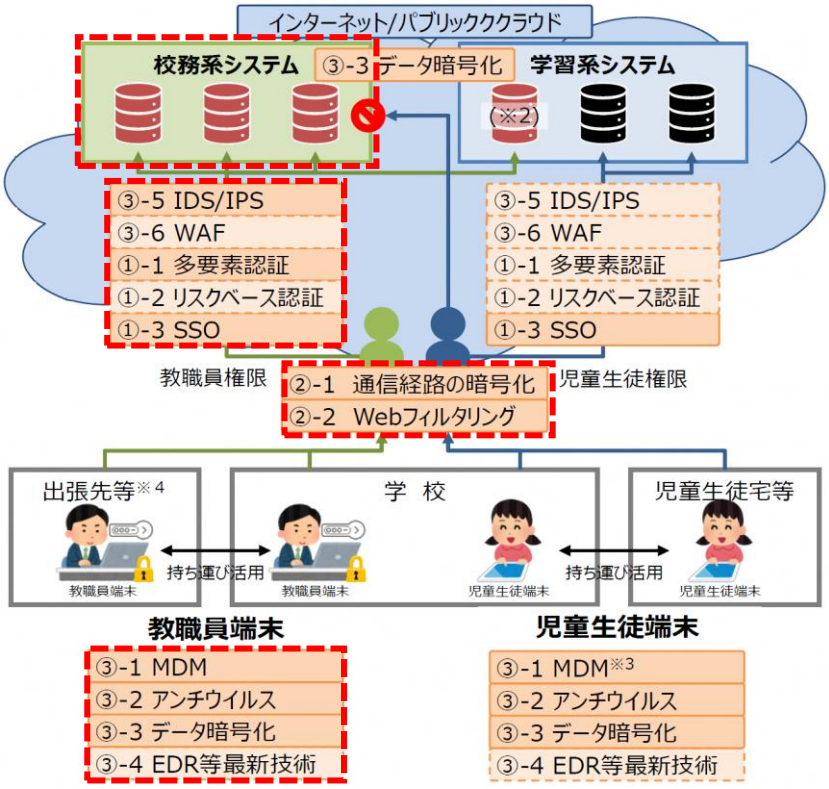
オ　情報セキュリティの確保

学校のみならず、出張先や自宅等に整備されたインターネット回線からシステムに接続可能とすることに伴い、悪意ある第三者からの不正アクセスを防止する仕組みとして多要素認証等を導入し、文部科学省公開の「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～」（令和５年３月８日）」に示されている「アクセス制御を前提としたネットワークにおける情報セキュリティの確保（イメージ）」を踏まえた対策を行うこと。

※　想定するネットワーク構成と調達範囲（赤点線部分）を以下に示す。

※　　濃いオレンジの部分は必須の要素技術。

※　　薄いオレンジの部分は導入が望ましい要素技術。



※　文部科学省公開の「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～」（令和５年３月８日）」から抜粋。

4　本事業の要件及び契約期間

⑴　校内ネットワーク等構築要件

【別紙１】校内ネットワーク等構築要求要件を満たすこと。

ア　構築期間

契約締結日の翌日から令和６年８月３１日まで

イ　納入期限

令和６年８月３１日

⑵　セキュリティ環境提供要件

【別紙２】セキュリティ環境要求要件を満たすこと。

提供期間

令和６年９月１日から令和１１年８月３１日まで

⑶　システム提供要件

【別紙３】システム要求要件を満たすこと。

提供期間

令和６年９月１日から令和１１年８月３１日まで

⑷　運用保守提供要件

【別紙４】運用保守要求要件を満たすこと。

提供期間

令和６年９月１日から令和１１年８月３１日まで

※　⑴～⑷の提供期間終了後、市が要望した場合、別途有償にて継続利用が可能であること。

５　納入場所

⑴　ネットワーク構築及び機器等の導入　　教育委員会、武蔵村山市内小・中学校１３校

⑵　セキュリティ環境構築　　教育委員会、武蔵村山市内小・中学校１４校

⑶　システム構築　　教育委員会、武蔵村山市内小・中学校１４校

※　納品場所は下記のとおり。

No.	名　称	住　所
1	武蔵村山市立第一小学校	東京都武蔵村山市本町 1-1-11
2	武蔵村山市立第二小学校	東京都武蔵村山市三ツ木 2-12-2
3	武蔵村山市立第三小学校	東京都武蔵村山市中藤 1-36-1
4	武蔵村山市立第八小学校	東京都武蔵村山市三ツ藤 2-50-1
5	武蔵村山市立第九小学校	東京都武蔵村山市学園 1-85-1
6	武蔵村山市立第十小学校	東京都武蔵村山市残堀 5-100-1
7	武蔵村山市立雷塚小学校	東京都武蔵村山市学園 4-6-1
8	武蔵村山市立小中一貫校村山学園第四小学校	東京都武蔵村山市緑が丘 1460
9	武蔵村山市立小中一貫校村山学園第二中学校	
10	武蔵村山市立小中一貫校大南学園第七小学校	東京都武蔵村山市大南 2-78-1
11	武蔵村山市立小中一貫校大南学園第四中学校	東京都武蔵村山市大南 2-79-1
12	武蔵村山市立第一中学校	東京都武蔵村山市本町 2-76-1
13	武蔵村山市立第三中学校	東京都武蔵村山市神明 4-117-1
14	武蔵村山市立第五中学校	東京都武蔵村山市残堀 5-55
15	武蔵村山市教育委員会	東京都武蔵村山市本町 1-1-1

6　成果物

受託者は、下表に示す成果物を作成し、市が指定する場所に納品すること。

なお、成果物の納入期限は、市と受託者が双方協議の上、決定するものとする。

【成果物一覧】

No.	成 果 物	数　量	備考
1	プロジェクト設計書	電磁的記録媒体２部、製本２部	
2	基本設計書	電磁的記録媒体２部、製本２部	
3	詳細設計書	電磁的記録媒体２部、製本２部	
4	試験成績書	電磁的記録媒体２部、製本２部	
5	プロジェクト管理資料	電磁的記録媒体２部、製本２部	WBS、議事録、課題管理表等
6	利用者マニュアル	電磁的記録媒体２部、製本２部	
7	運用仕様書	電磁的記録媒体２部、製本２部	
8	構築完了報告書	電磁的記録媒体２部、製本２部	納品一覧を含む

7　再委託の制限

本契約期間中に、機器調達を除く業務に関して、原則、再委託を行ってはならない。再委託が必要な場合、あらかじめ市の承認を受けること。（この場合、再委託の受注者は本仕様書の規定を遵守する義務を負うものとする）

8　秘密の保持

受託者は、業務の履行に際して知り得た情報を第三者に漏らしてはならない。このことは、履行期間終了後も同様とし、そのために必要な措置を講ずること。

9　個人情報の保護

この契約による業務を処理するための個人情報の取扱いについては、別記「個人情報等の取扱いに関する特記仕様書」を遵守しなければならない。

10　瑕疵担保責任

本業務の検査完了後、瑕疵が発見された場合、受注者は無償で補修・追完を行うものとする。

11　情報セキュリティポリシーを踏まえた業務の履行

武蔵村山市情報セキュリティポリシーの要旨を踏まえ、以下の事項を遵守すること。

⑴　複写及び複製の禁止

受託者は、この契約に基づく業務を処理するため、市が貸与する原票、資料、その他貸与品等及びこれらに含まれる情報（以下「市からの貸与品」という。）を、市の承諾なくして

複写及び複製をしてはならない。

⑵　作業場所以外への持出禁止

受託者は、市からの貸与品（複写及び複製したものを含む。）について、市が認める場所以外へ持ち出してはならない。

12　環境により良い自動車の利用

本契約の履行に当たって自動車を使用し、又は利用する場合は、都民の健康と安全を確保する環境に関する条例（平成 12 年東京都条例第 215 号）の規定に基づき、次の事項を遵守すること。

⑴　ディーゼル車規制に適合する自動車であること。

⑵　自動車から排出される窒素酸化物及び粒子状物質の特定地域における総量の削減等に関する特別措置法（平成 4 年法律第 70 号）の対策地域内で登録可能な自動車利用に努めること。

なお、適合の確認のために、当該自動車の自動車検査証（車検証）、粒子状物質減少装置装着証明書等の提示又は写の提出を求められた場合には、速やかに提示し、又は提出すること。

13　検査

⑴　受託者は、本業務の完了後、速やかに市に業務完了報告書及び成果品を提出し、市の検査を受けるものとする。

⑵　受託者は、原則として、あらかじめ指定された日時及び場所において、市の職員が行う検査に立ち会わなければならない。

⑶　受託者は、検査に立ち会わなかったときは、検査の結果について異議を申し立てることができない。

14　その他

その他本仕様書に記載のない事項、又はその他疑義が生じた場合は、市、受託者で協議の上、決定すること。

【別紙 1】校内ネットワーク等構築要求要件

1　基本条件

⑴　ネットワーク構成

ア　文部科学省の「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４年３月）に示されている、アクセス制御による対策を講じた構成とすること。

イ　各種サーバ（システムサーバを除く）の構築場所については、クラウド利用を基本とすること。

ウ　システムサーバの構築場所については、クラウド又はデータセンター利用とする。

エ　データ等の所在地は日本国内とし、日本の法律、条例が適用される環境であること。

オ　教職員用端末からクラウド又はデータセンターへの接続については、GIGA スクール構想で整備した無線 AP の利用を想定した構成とすること。

また、出張先や自宅等に整備されたインターネット回線からも接続可能な構成とすること。

※　原則として、市内小・中学校のインターネット回線は、既設回線である NTT 東日本フレッツ回線を使用する提案とすること。ただし、インターネット回線に接続する機器は 10Gbps に対応可能な機器とすること。（LAN ケーブルを含む。）

⑵　ネットワーク機器の構築

上記、ネットワーク構成を踏まえ、以下の要件を満たす機器を構築すること。

ア　インターネット接続用ルータ

⑺　フレッツ光クロスに IPoE 方式で接続できること。

⑴　有線 LAN インタフェース（10GBASE-T/1000BASE-T/100BASE-TX/10BASE-T）を 4 ポート有すること。

⑼　4Gbps 相当の IPsec 転送性能があること。

⑽　調達台数は、14 台とし、同一メーカ及び同一機種とすること。

⑾　契約期間中、24 時間 365 日のオンサイト保守を提供すること。

イ　L3 スイッチ

⑺　既存ネットワーク（学習系ネットワーク）とのネットワーク分離を可能とする機能を具備していること。

⑴　ループ検知及びポート閉塞機能を有し、syslog による通知が可能であること。

⑼　有線 LAN インタフェースとして、10GBASE-T ポートを 2 ポート以上、PoE+（IEEE 802.3at）に対応した 1000BASE-T ポートを 20 ポート以上有すること。

⑽　調達台数は、13 台（教育委員会分を除く）とし、同一メーカ及び同一機種とすること。

⑾　契約期間中、24 時間 365 日のオンサイト保守を提供すること。

⑿　教職員用端末からパソコン教室のサーバ等へのアクセスを可能とすること。

⑶　教職員用端末のセッティング及び複合機接続支援

ア　教職員用端末のセッティング

市が別途、調達する教職員用端末（500 台）について、OS 及び以下のソフトウェアをインストールし、教職員用端末として利用可能な状態で各学校に配備すること。

また、適切なバージョンにバージョンアップし、最新のセキュリティパッチを適用すること。

㈠　Microsoft365 関連（詳細は、要件定義にて調整）

㈡　その他のソフトウェア関連

㈢　プリンタ及び複合機関連のドライバ

※　別途、調達する複合機も含め利用できること。

※　別途、調達する教職員用端末の想定する仕様は次のとおり。

項　目	想定する仕様
台数	500 台
OS	Windows11 Pro 64bit
ディスプレイ	13 インチ以上
CPU	core i5-1135G7 以上
メモリ	16GB 以上
ストレージ	SSD 128GB 以上
重量	1.4kg 以内
製品種別	2in1 パソコン（ディスプレイとキーボードが分離しないタイプ）
タッチパネル対応	対応
顔認証機能	対応

イ　複合機接続支援

市が別途、調達する複合機の導入に伴い、ネットワークに接続するための技術支援（ネットワーク設定の指示等）を行うこと。

※　別途、調達予定の複合機の想定する仕様は次のとおり。

項　目	想定する仕様
台数	各校 1 台　計 14 台
契約方式	機器本体代、インク、メンテナンスボックス等の消耗品(用紙を除く)及び保守サービス料含む、規定枚数までカラー印刷が可能な基本使用料(月額)方式。
機能	コピー、プリント、スキャン、自動紙送り装置及び FAX 機能搭載。
プリント方式	インクジェット方式
印刷スピード	100 枚/分
耐久枚数	1,200 万ページ以上

ネットワーク	有線及び無線対応
参考機種	LX-10050M（EPSON 社製）

⑷ セキュリティ環境の構築

「【別紙 2】セキュリティ環境要求要件」に示す、セキュリティ環境を構築すること。

⑸ システム環境の構築

「【別紙 3】システム要求要件」に示す、システム環境を構築すること。

⑹ 運用保守環境の構築

「【別紙 4】運用保守要求要件」に示す、運用保守環境を構築すること。

⑺ 共通要件

ア 本事業で導入する機器（教職員用端末含む）の設置場所及び台数は、市の指示どおりに配備すること。

イ 本事業で導入する機器（教職員用端末含む）の動作確認及び通信確認を行うこと。

ウ 各学校の既存機器の利用に支障が出ないようにネットワークを構成し、かつ、既存機器との連携が可能となるように考慮したものを構築すること。ただし、既存機器の設計変更が生じる場合、既存機器に関する設計及び作業は範囲外とするが、技術支援は行うこと。

エ 納入品は全て新品であること。

オ 教職員用端末のデータ移行については、移行作業は原則として利用者による移行とするが、移行方法や手順等の支援を行うこと。

カ 構築期間中に必要となる月額費用（クラウド等のサービス利用料、ライセンス費用等）は、初期費用に全て含めること。

⑻ プロジェクト管理

ア プロジェクト計画書の策定

受託者は、本仕様書に基づき、本業務の構築における具体的な体制、スケジュール、プロジェクト管理方針、プロジェクト管理方法等を含んだプロジェクト計画書を作成すること。

イ プロジェクト管理

受託者は、以下に基づきプロジェクトを管理すること。

No.	管理項目	管理内容
1	進捗管理	プロジェクト計画策定時に定義したスケジュールに基づく進捗管理を実施すること。受託者は、実施スケジュールと状況の差を把握し、進捗の自己評価を実施し、定期的な会議において市に報告すること。進捗及び進捗管理に是正の必要がある場合は、その原因及び対応策を明らかにし、速やかに是正した計画を策定すること。
2	課題・リスク管理	プロジェクト計画時に抽出したリスクを管理し、リ

		スクが顕在化した場合は課題として管理すること。課題発生時には、速やかに対応策を明らかにし、市と協議の上、対応方法を確定し、課題が解決するまで継続的に管理すること。
3	品質管理	プロジェクト計画策定時に定義した品質管理方針に基づく品質管理を実施すること。品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正した計画を策定すること。

【別紙２】セキュリティ環境要求要件

1　基本条件

以下に掲げる各事項に基づき、最適なセキュリティ環境を提案すること。

⑴　マルウェア等への対策

ゼロトラストネットワーク化に伴い、マルウェアの侵入を防ぐことは無論、侵入をいかに早く検知し、被害拡散を防止するとともに迅速に復旧するかが重要となる。また、テレワーク環境の実装に伴い、学校外での端末利用時に一層の注意を払う必要が生じる。以上の点から、エンドポイントセキュリティについて、EPP（エンドポイント保護）と EDR（エンドポイントにおける検出と対応）の二層に分けて提案すること。ただし、提案ソリューションが EPP と EDR の両方の機能を十分に有している場合は、当該単一ソリューションのみを提案しても差し支えない。

⑵　EPP（エンドポイント保護）

EPP に無償のソフト（Microsoft　Defender など）を用いても差し支えないが、一元管理ができるよう留意すること。具体的には、以下の要件を満たすこと。

ア　EPP 対策ソフトにおけるリアルタイム保護の状態やシグネチャのバージョン、スキャン実行日時など、各端末における Microsoft Defender 等の稼働状態を管理コンソールで確認できる機能を有すること。

イ　EPP 対策ソフトにおける脅威検出、シグネチャ更新、スキャン実行などの主要なイベント／ログを管理コンソールで確認できる機能を有すること。

ウ　EPP 対策ソフトのシグネチャのアップデート命令配布及びスキャン命令配布が管理コンソールから実行できる機能を有すること。

エ　EPP 対策ソフトの検出除外設定を配布する機能を有すること。

⑶　EDR（エンドポイントにおける検出と対応）

ア　EDR の目的は、感染後の迅速な隔離、状況把握、対応一元化、ログ収集、他端末／ネットワークへの被害拡散防止等である為、SOC 等のサービスを経由することなく ZDP エンジン、スタティック分析エンジン、サンドボックスエンジン、HIPS エンジン、機械学習エンジン等の５つ以上のエンジンを用い、マルウェアの検知、検知ファイルの隔離及びマルウェアを検知した教職員用端末をネットワークから自動的に遮断を行う機能を有すること。

イ　脆弱性攻撃の防御、マルウェア特有の振る舞いの検知や、仮想環境でのプログラム実行による検知（サンドボックス）などの機能を組み合わせて有しており、未知のマルウェアやゼロデイ攻撃などに対しても、パターンファイルのみに依存しない多層的なマルウェア検知が可能であること。

ウ　改竄されたレジストリや設定ファイルを復旧する機能を有すること。

エ　収集したログの分析が可能であること。

オ　検知ログを Syslog にて転送できること。その際、情報の分析や操作を容易にするため

の標準形式であるCEFフォーマットを選択できること。

カ　検知ファイルと本ソフトウェアで収集した操作ログを紐づけて、マルウェアの侵入経路を調査し、他端末へのマルウェアの存在確認及びネットワーク遮断が行えること。

　また、調査結果及び確認結果はレポートとして出力できること。

キ　ネットワークから遮断した端末及び隔離した検知ファイルは、マルウェア駆除など安全が確認できた後、管理機能から復旧できること。

ク　EDRの判断により遮断設定を行った脅威については、他の端末も含め、ネットワーク全体として以後自動的にブロックできること。

ケ　EDRが収集したログは、ファイル名、ドメイン、IPアドレスなどから複数の条件を選んで検索できること。

コ　ソフトウェアの開発・保守サポートはすべて日本国内で行われていること。また、検出された検体の調査を行う場合、日本国外に持ち出すことなく、日本国内で調査が行われること。

サ　端末がマルウェアに感染した際に、当該端末のWebへの通信を遮断しつつ、管理コンソールからリモート操作による復旧作業が継続できる仕組みを有すること。

⑷　MDM

ア　教職員用端末を紛失した際などに、インターネットを経由して遠隔で画面をロックし操作の制御を行うことや、あらかじめ登録した教職員用端末上の指定フォルダの削除を行う機能を有すること。また、GPSやWi-Fi、IPアドレス、携帯電話基地局からの取得情報を用いて、教職員用端末の位置情報をインターネット経由で確認できること。

イ　端末紛失等に備え、全体管理者はリモートロック（ログイン不可設定）が行えること。

ウ　端末紛失等に備え、全体管理者はリモートワイプ（消去と初期化）が行えること。

エ　インターネットを経由して、教職員用端末の制御状態（画面ロック）を解除できること。さらに、オフラインであっても、管理者が発行した解除コードを、制御中の教職員用端末上で入力することで、制御状態を解除できること。

オ　業務に無関係な私的利用を抑止する方法があること。(操作ログや閲覧画面情報を確保する等の方法を想定)

⑸　遠隔操作

ア　特定の教職員用端末に対して、ネットワーク経由で、リモート操作が行える機能を有すること。

　また、リモート操作されている教職員用端末のデスクトップに、操作中であることを通知するポップアップを表示する設定が可能であること。

イ　パスワード入力など、セキュリティの観点から教職員用端末に表示したくない遠隔操作を行う場合は、教職員用端末に対して操作画面を隠しながら遠隔操作を行えること。

ウ　円滑な操作を行うため、リモート操作時には、通信帯域を制限できること。

　また、リモート操作で画面を受信する際に画質を落とす等、通信データ量を抑制できること。

⑹　資産管理

ア　端末台帳管理を目的に、教職員用端末に関する各種ハードウェア情報を、資産情報として自動的に収集できること。

イ　人事異動者が過去に保有していた端末情報の管理にも備え、検索の際には、本ソフトウェアから削除された教職員用端末も、検索対象として指定できること。

ウ　IP アドレスの管理台帳と、資産情報を照合し、競合や不正使用、使用期限切れの表示を行えること。

　また、表示方法は利便性を考慮し一覧表示及びマップ表示を行えること。

エ　教職員用端末上のソフトウェアに関するインストール状況を収集する機能を有すること。

オ　指定した教職員用端末及び検索グループに対して、複数の任意のプログラムを配布し、自動的にプログラムの実行及び解除を行う機能を有すること。

　また、ソフトウェアの配布日時と対象端末を設定し、配布したソフトウェアの配布状況及び実行状況の確認ができること。

カ　セキュリティパッチを適用する際に帯域負荷がかかると想定される場合は、段階的に適用する仕組みを構築すること。

⑺　ログ管理

以下の機能は、管理コンソール内ですべて処理が可能であること。

ア　ログの閲覧

イ　任意の複数カテゴリを選択した上で、選択したすべてのカテゴリのログを時系列に並べた閲覧

ウ　教職員用端末に対して行われた操作、ログオン・ログオフの日時、実行されたソフトウェアについての起動時刻・操作時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、Web へのアクセス・書き込み・アップロード、クリップボード(テキスト・画像)、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報、接続した通信デバイス及び外部との通信状況等の記録

エ　特殊な Web サイト(通常であれば利用されない)閲覧を確認するため、ネットワーク全体でのアクセスが少ない URL に対するアクセスの自動判定

オ　有事の際のログ検索時に、収集した教職員用端末の全てのログの複数条件による検索

カ　特定の操作をする端末を即時に検索でき、任意のログに対するマーキング。また、検索時に表示された教職員用端末のグループ化及び登録

キ　複合機等利用時の情報漏洩や、過剰利用に備え、教職員用端末上でアプリケーションソフトウェアから印刷が実行された際に、その印刷されたドキュメント名、１回の印刷枚数、ファイルパスを記録

ク　Microsoft 365 上でファイルをローカルに作成した際、ファイル名やファイルパスをログとして記録

ケ　管理コンソール上からマルウェア感染時のマルウェアの挙動監視及び追跡

⑻　アラート管理

ア　事前定義されたルールに沿ってポリシーの適用が可能なこと。ポリシーに反した操作が行われた際、その操作を行った利用者の教職員用端末のデスクトップ上にリアルタイムで、ポップアップ形式による通知ができること。

イ　教職員用端末の操作画面を管理端末で表示し、アラート発生端末の操作画面を拡大して強調することで、ネットワーク管理者の作業負担を軽減する機能を有すること。

ウ　アラート発生時における端末操作画面を、マウスカーソルの位置が強調された形式で表示し、不正操作及び誤操作発生時に早期の問題把握ができる機能を有すること。

エ　個人情報を扱うアプリケーションなど、指定したアプリケーションの起動中は、印刷やクリップボードへのコピー、Print Screen キー、アプリケーションによる画面キャプチャーなどの特定の操作を検知及び禁止できること。ただし、指定したアプリケーションの起動中に印刷を禁止している場合も、指定した複合機等にのみ印刷可能と設定できること。

オ　複合機等の利用に伴い、印刷枚数（１回当たり）、印刷ドキュメント名（キーワード）、印刷ファイルパスに対して、事前定義されたルールに従い、自動的にメール等で通知する機能を有すること。

カ　利用者以外の閲覧対策として、教職員用端末で指定したソフトウェアが起動されている状態及びタイトルに特定の文字を含むウィンドウが表示されている状態で一定時間マウスやキーボードによる操作が無い場合に、ログオフ忘れとして検知できること。

キ　私物パソコン等の持込対策を講じること。

⑼　デバイス管理

ア　USB デバイスをシリアルナンバーごとに管理する機能を有すること。保有 USB デバイスはシステムで台帳管理し、一覧で表示できること。なお、台帳への登録は USB デバイスを教職員用端末に接続した際に自動収集できることが望ましい。

イ　USB デバイスを教職員用端末又は管理者の端末に挿入した際に、利用した USB デバイスのシリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること。

ウ　USB デバイスの紛失に備え、管理台帳に登録されている USB メモリについて、その所在をシステムにおいて確認できること。USB メモリの所在は、各 USB メモリの利用者又は管理者が USB メモリを教職員用端末に挿入することでその所在を一括管理でき、管理台帳に反映できること。調査する期間は任意で設定でき、期間を超過しても所在が確認できていない USB メモリや利用者を表示できること。

エ　USB メモリが教職員用端末に装着された日時を利用して、所定期間以上使用実績のない USB メモリを、紛失の可能性があると自動判定し、最後の使用者又は管理者に対して、USB メモリの所在確認（教職員用端末への装着）を促す通知を行う機能を有すること。

⑽　データ暗号化

ア　教職員用端末の紛失・盗難を想定し、BitLocker 及び他サードパーティ製品によるドライブ暗号化を図ること。

なお、運用の観点から暗号化の回復キーの一元管理ができること。

また、セキュリティの観点からドライブの暗号化状態が変更された時はドライブログとして記録できること。

イ　マルウェア感染時にデータの情報漏洩が発生した場合に備え、ファイル単位で暗号化されており、外部ユーザーが読み取れない仕組みを有すること。

ウ　任意のフォルダを自動暗号化フォルダとして設定し、自動暗号化フォルダにファイルやフォルダをコピー・保存することで自動的に暗号化できること。また、指定したWebサイトにファイルをアップロードする際、自動暗号化フォルダに格納されている暗号化されたファイルのみがアップロードされる設定ができること。

エ　事前定義されたWebサイトに限り、暗号化されていないファイルをアップロードする設定ができること。なお、アップロードできるファイルは指定フォルダに格納されているなどの設定ができること。また、アップロードされたことの記録ができること。

オ　暗号化形式は、復号ツールを使用して復号する形式又は復号ツールが不要なパスワード付きzipファイルを作成する形式から選択できること。

カ　暗号化されたファイルは、特定の端末でのみ復号可能とする設定ができること。

キ　暗号化する際、パスワード入力の失敗回数の上限及び復号可能な期間を設定できること。

⑾　統合認証基盤

ア　シングルサインオン（以下「SSO」という。）により、統合認証基盤への認証を通じて、システム及び学習e-ポータルや汎用クラウドツール等にも追加の認証を行うことなくアクセスできるものとすること。

イ　多要素認証によりSSOが可能なこと。

ウ　教職員の名簿情報に対して一意のIDを付与し管理できること。

エ　認証は多要素認証により実現すること。なお、認証方式については、ユーザーIDとパスワードによる認証に加え、生体認証（顔認証）とすること。

オ　教職員用端末からのみ接続できること。

⑿　ゼロトラスト基盤

ア　IDS/IPS、WAF又はアプリケーションレベルの制御、WEBフィルタリング、アンチウイルス、マルウェア対策、ランサムウェア対策、CASB、サンドボックス機能を有すること。

イ　教職員用端末からゼロトラスト基盤までの経路はIPsec又はSSL-VPNにより暗号化されること。なお、httpsによる暗号化は暗号化対策として認めない。

ウ　複数のサイトで構成され、信頼性の高いゼロトラスト基盤であること。

エ　SSL通信を復号化して検査する機能を有すること。

オ　統合認証基盤とSAML認証等により連携可能なこと。

⒀　Microsoft365要件

ア　Microsoft365 A3以上を導入すること。

イ　ユーザアカウントは、構築するネットワーク環境全体で一意となること。

ウ　ユーザアカウントごとにパスワード管理及びアクセス権管理を行うこと。

エ　教育委員会及び市内小・中学校の教職員にユーザアカウントを付与し、個人用フォル

ダを作成するとともに、適切なアクセス制御を行うこと。

オ　ユーザアカウントの所属及び権限・属性等と連動したグループ用の共有フォルダを作成するとともに、適切なアクセス制御を行うこと。

カ　Microsoft365 の環境構築は、以下の範囲とする。

㈠　メール環境は、現行のメールアドレスを変更することなく利用が可能であり、過去のメールも閲覧可能なことを要件とし、市にとって最適な提案を行うこと。

㈡　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 を採用し、その環境を構築すること。

㈢　組織毎のファイル共有は、組織内のみでの閲覧となる設定を行うため、Sharepoint による環境実装を行うこと。

㈣　共有ファイル以外のファイルは、個人データの管理が行えるよう OneDrive での運用設計を行うこと。

キ　教職員用端末のみをアクセス可能とする条件付きアクセス(多要素認証)の設計のため、条件付きアクセスポリシーの設定及びポリシーの割り当てを実施すること。

ク　端末認証を目的として Microsoft Intune の基本・詳細設計を実施すること。

ケ　Entra ID と以下のサービスとの SSO 連携設定検証作業を実施すること。

㈠　校務支援システム

㈡　学習系 SaaS システム

コ　構築の範囲を対象とした Entra ID に関するユーザーマニュアルを作成すること。

【別紙３】システム要求要件

1　基本条件

⑴　パッケージ要件

ア　導入実績

提案するシステムの実績として、複数の自治体に導入実績があり、500 校以上の学校へクラウド型又はデータセンター型の導入実績を有すること。

イ　稼働実績

提案するシステムは、3 年以上の稼働実績を持ち、学校の校務（出席簿、通知表、指導要録は必須）の情報化を実現し、現在も継続して利用されている製品であること。

ウ　APPLIC 準拠

一般財団法人全国地域情報化推進協会（APPLIC）の準拠登録製品一覧に掲載されている製品であること。

また、APPLIC においてオレンジマークを取得している製品であること。

エ　バージョンアップ

定期的に無償でバージョンアップ（機能改訂若しくは拡張）を図るシステムであること。この際、必要事項（改修内容、適用スケジュール等）を主体的に提案又は説明を行い、市の承諾を得てから実施すること。

また、通知表、指導要録について、国や都の制度又は法令等の改正による変更の必要性が生じた場合は、市の要望に従い無償対応内容を提示すること。

⑵　基本要件

ア　導入するシステムはパブリッククラウドを活用したクラウド型又はデータセンターに構築されたシステムとする。

イ　災害時等においても継続して業務を遂行できるよう、冗長化対策が講じられていること。

なお、単なる機器の冗長構成ではなく、サイト冗長等により冗長化された信頼性の高いシステムであることが望ましい。サイト冗長以外の提案とする場合は、高い信頼性であることを示すこと。

ウ　各校で利用中のインターネット回線から接続し利用できること。

エ　DDoS 攻撃等の防御対策が施されており、WAF（WAAP であれば更に望ましい）による WEB アプリケーションレベルのセキュリティ対策が施されていること。

オ　Microsoft Excel（Microsoft Office）で作成された名簿データや成績データなどを活用できる仕組みを持つこと。

カ　契約期間中は、利用可能であること。ただし、受託者の責めに帰す事由に　より、やむを得ず別のパッケージシステムを利用しなければならないときは、本業務の範囲内で実施し、新たな費用は発生しないこと。なお、別のパッケージへの切替を行う場合は、必要事項（改修内容、適用スケジュール等）を主体的に提案し、市の承諾を得てから実施する

こと。

キ　システムに関わる全ての情報（成績情報、教職員情報、児童・生徒情報等）の運用管理において、効率的に行えるよう工夫されたシステム構成であること。

ク　在校生及び卒業生の情報（法定保存期間が定められた帳票）を管理できること。

ケ　モダンブラウザ（Microsoft Edge 等）を利用した WEB アプリケーションとして利用できるシステムであること。また、特別なソフトウェアをインストールすることなく利用可能なこと。

コ　データは、汎用的なフォーマット（Microsoft Excel、CSV 等）で取り込みや出力が可能であり、既存データの利用や他のアプリケーションとの連携利用が可能なこと。

サ　機密性の高い個人情報等のデータがサーバで一括管理される仕組みを有すること。
　また、教職員用端末にはデータが残らない仕組みとすること。

シ　市の要望に応じて、帳票類・メニュー項目等のカスタマイズに対応可能な構造を有すること。

ス　帳票類は、原則として編集できないように保護された PDF ファイルで印刷が可能であり用紙サイズを問わないこと。

セ　成績データベースは、小学校及び中学校で別々のデータ管理が可能な仕組みとすること。

ソ　運用時において不足する外字が発生した場合は、無償で対応すること。

⑶　利用者数の規模

利用者は各小・中学校の教職員及び教育委員会の職員であり、参考に児童・生徒数も示す。

以下に示す教職員数及び児童・生徒数は令和５年５月１日時点のものであり、年度によって変動するため増減に対して柔軟に対応できること。

No.	学 校 名	利 用 者	児童生徒（参考）
1	第一小学校	28	369
2	第二小学校	18	373
3	第三小学校	19	381
4	第八小学校	35	686
5	第九小学校	27	263
6	第十小学校	24	437
7	雷塚小学校	24	282
8	村山学園第四小学校	22	349
9	村山学園第二中学校	31	192
10	大南学園第七小学校	37	620

11	大南学園第四中学校	21	316
12	第一中学校	32	585
13	第三中学校	25	336
14	第五中学校	31	575
15	教育委員会	4	―
合　計		378	5,764

⑷　機能要件

システムに係る提案対象は以下のとおりとする。

ア　機能要件（必須）

提案するシステムは、以下の機能を有すること。

(ｱ)　学籍管理

学校、教職員、児童・生徒 、転出入情報の管理

(ｲ)　出欠管理

児童・生徒の出欠情報の管理（保護者連絡との連携を含む）

(ｳ)　成績管理

通知表、指導要録、調査書、テスト情報の管理

(ｴ)　予定管理

週案、時数情報の管理

(ｵ)　保護者連絡

欠席連絡（システムとの連携を含む）、アンケート、通知文等の配信

(ｶ)　服務管理

勤怠管理、休暇管理

(ｷ)　保健管理

健康診断情報、保健室来室履歴情報の管理

(ｸ)　ユーザ管理

ユーザ情報、アクセス権限の管理

イ　機能要件（任意）

提案するシステムは、以下の機能を有することが望ましい。

(ｱ)　グループウェア

文書共有、連絡機能、掲示板、行事計画、会議室・備品予約、アンケート

(ｲ)　その他校務支援機能

統計・分析

ウ　非機能要件

提案するシステムは、以下の内容を満たすこと。

(ｱ)　可用性

a　原則として 24 時間 365 日稼働すること。

b　メンテナンス、バックアップ等でサービスの停止が必要な場合は、市と事前に協議を行うこと。

c　バックアップ環境や災害対策環境が、データの同期やバックアップへの切換の仕組みを含め、提供されること。

⑷　性能・拡張性

オンラインレスポンスタイムは、業務に影響ない範囲にとどめること。

⑸　セキュリティ

a　利用者のログイン･ログアウトや､重要なデータに対する操作を証跡として記録し、不正なアクセスに対する分析・調査が行えるようにすること。市の求めに応じ、証跡を提供可能とすること。

b　統合認証基盤と共に多要素認証の仕組みを実現すること。

c　多要素認証以外に有効なセキュリティ対策があれば提案すること。

d　学校内外において、主に利用が想定されている機器以外からのアクセスが可能である場合は、セキュリティ対策と併せて明示すること。

⑹　データ移行

本サービスの契約終了等により次期サービスへのデータ移行の必要性が生じた際には､次期サービスを稼働させるために必要な情報資産及びそれらのデータ､ファイルレイアウト等の仕様について、市が提出を求めた場合は速やかに無償提供すること。

また、提供する情報資産への市からの問合せに対応すること。

なお､データ移行の際の形式や実施方法等については､国の動向を踏まえたものとするよう努めること。

⑸　帳票

ア　東京都で規定・統一された帳票類（調査書、成績一覧表、学校職員の出勤簿、週休日の変更命令簿、超過勤務命令簿、旅行命令簿兼旅費請求内訳書等）は、標準で搭載されていること。また､そのレイアウトが変更された際にも市が変更を求めた場合は無償で修正し、利用時期に遅延なく提供が可能なこと。

イ　指導要録や調査書について､国や都の制度又は法令等の改正があった場合､対応できる仕組みがあること。

ウ　通知表レイアウトについては､各小･中学校で採用されているレイアウトに対応し、入力蓄積された成績データベースから必要な情報のみを抽出した PDF ファイルによる通知表が作成可能なこと。

2　調達・導入

⑴　システムの導入

ア　既存システムに蓄積されたデータを可能な限り引き継ぎ、令和６年９月１日から本格稼働が可能なこと。

また、年度途中での切替えとなることを留意した移行方法を提案すること。

イ　導入に係るスケジュールを作成し、市の承認を得ること。また、各作業の実施前に必

要となる打合せを行い、市の承認を得た上で実施すること。

ウ　システムを稼働するために必要な設計作業、構築、運用準備作業などの全ての作業を実施すること。

⑵　各種テスト

必要に応じて各テストを行うこと。パッケージ製品に関する製品テストはメーカの責任で行うこと。

⑶　履行場所

ア　本件業務の実施にあたっては、市が指定する設置場所又は受託者が管理するセキュリティ区画内にて作業を行うこと。

イ　クラウド又はデータセンターでの作業及びリモート作業（サーバやシステムの設定作業を想定）に当たっては、クラウド又はデータセンターが指定する所定の手続きを経て実施すること。

【別紙４】運用保守要求要件

1　基本要件

契約期間中、以下の役務を提供する運用保守の一元窓口を設けること。

⑴　ヘルプデスク

ア　受付対象者は、教育委員会、各学校の情報システム担当者（緊急時は各教職員からも受付）及び事前に調整した関連事業者窓口とする。

イ　対応時間は、原則、平日の午前８時から午後５時までとする。

ただし、国民の祝日に関する法律（昭和２３年法律第１７８号）に定める休日（以下「休日」という。）及び１２月２９日から１月３日までの間は除く。

ウ　受付方法は、電話又はメールとする。

エ　本業務で整備したセキュリティ環境（MDM、資産管理、デバイス管理等）、システム及び機器等の仕様確認、操作方法確認、調査依頼等に関する問合せを受け付け、対応すること。 なお、本運用保守業務で使用する端末については、受託者が用意すること。

オ　迅速な対応をすることができるように、リモート保守が可能な体制を保有すること。

⑵　故障受付

ア　本業務で整備したシステム及び機器等に障害や故障が発生した場合の受付及び保守ベンダーの手配を行うこと。

また、ネットワーク全体での障害切分けを実施し、障害箇所を絞り込むこと。

なお、回線の不具合及びGIGAスクール構想で整備した児童・生徒用タブレットの故障受付等、本業務の提案範囲外の部分については、関連事業者と事前調整した内容に基づき保守事業者等に取次ぎを行うこと。

イ　本業務で整備した機器等で機器故障と判断した機器については、ハードウェア保守ベンダーを手配し、復旧までの保守ベンダーコントロール並びに状況報告を実施すること。

ウ　本業務で整備したシステム及び機器等のアプリケーションに起因するトラブルが発生した場合には、無償にて対応すること。

エ　システム等の障害発生時には、学校訪問対応や関連事業者へのエスカレーションなど適切な対応を実施すること。

オ　不具合が長期化した場合や重要問題発生時に、ログ調査を実施し、解析結果を報告すること。なお、解決に至らない場合は、必要に応じて現地対応を行うこと。

⑶　アプリケーションのアップデート

ア　アプリケーションのアップデートは、クラウド環境にて無償で実施すること。

イ　アップデート作業に伴い、対応の中断が発生する場合は、原則実施予定日の３週間前までに、市に連絡の上、実施の了解を得ること。ただし、セキュリティインシデント発生等に伴い、緊急対策としてアップデートを実施する場合はこの限りでない。

⑷　バックアップ

ア　本業務で整備したシステム等で扱うデータは、災害及び障害に備えてデータのバック

アップを実施すること。

イ　データのバックアップはクラウド環境で実施すること。

ウ　バックアップデータの世代管理は、1 世代以上とすること。

⑸　ネットワーク監視

ア　ネットワーク機器死活監視による機器障害及び回線障害の検知並びに通知を行うこと。

イ　法定停電の際は、監視抑止を行い、復電後に各機器の状態確認を行うこと。

⑹　セキュリティ

ア　サーバ等機器のウイルス対策については、適切な措置を講じること。

イ　セキュリティインシデントが発生した際には、危険度判定から緊急対応の要否を判断し、関係者に通知するとともに隔離等の対処並びに教職員用端末の回復等について支援すること。

⑺　設定変更

ア　本業務で整備したシステム及び機器等について、暫定対策、セキュリティ対策の見直し等が必要になった場合に設定変更を実施すること。

イ　本業務で整備したシステム及び機器等の利用者の管理を行うこと。利用者の新規登録･変更等の処理は、年度移行時だけでなく、随時実施すること。

⑻　資料更新

設定や運用方法の変更時に、設計図書や運用図書の更新を行い、最新版の提供及び管理を行うこと。

⑼　月次報告

運用対応内容、重要イベントの報告等、定義した内容に基づいて報告書を作成し、月次で報告すること。

⑽　教職員教育・研修

ア　学校の要望に応じた活用支援サポートに対応するための体制があり、必要に応じて年１回以上の訪問サポート対応が可能であること。

イ　年度移行時には、システム等の繰り上げ処理、名簿データ等の取り込み作業において学校での作業を補助できる体制があること。

ウ　本業務で整備したシステム及び機器等の機能を網羅したガイドブック等を提供すること。

エ　訪問サポートの実施にあたっては、児童・生徒が下校した後の時間とするなど、通常業務への影響の回避に配慮すること。

オ　ウイルス感染や端末紛失等、日常起こり得るインシデントを想定した対応マニュアルを作成の上、インシデント訓練を年１回以上実施すること。

個人情報等の取扱いに関する特記仕様書

（法令等の遵守）

第１条　受注者（以下「乙」という。）は、発注者（以下「甲」という。）との間で締結する本契約の履行に当たっては、個人情報の保護に関する法律（平成１５年法律第５７号。以下本特記仕様書において「法」という。）、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号。以下「番号法」という。）、個人情報の保護に関する法律についてのガイドライン（行政機関等編）（以下「個人情報保護法ガイドライン」という。）、特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）（以下「特定個人情報ガイドライン」という。）、武蔵村山市情報セキュリティポリシーその他関係法令等（以下これらを「法令等」という。）を遵守しなければならない。

（定義）

第２条　本特記仕様書で使用する用語は、法及び番号法で使用する用語の例による。

（秘密保持）

第３条　乙は、法令に特別の定めがある場合を除き、本契約の履行に際して知り得た個人情報及び特定個人情報（以下「個人情報等」という。）を第三者に漏らしてはならない。本契約終了後も同様とする。

２　乙は、本契約の履行に携わる乙の従業者（以下単に「従業者」という。）に、個人情報等の秘密保持に係る誓約書を提出させなければならない。

（安全管理措置）

第４条　乙は、本契約の範囲内において、個人情報等の取扱いについて甲が採るべき措置と同等の安全管理措置（個人情報保護法ガイドライン及び特定個人情報ガイドラインで求められる安全管理措置をいう。）を講じる義務を負う。

（従業者の明確化）

第５条　乙は、従業者のうちから、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）に規定する総括保護管理者、保護管理者、保護担当者（特定個人情報については、特定個人情報ガイドラインに規定する総括責任者、保護責任者、事務取扱担当者）及び監査責任者に相当する者（以下「総括保護管理者等」という。）を指名し、個人情報等の安全管理体制の確保及び維持に努めなければならない。

２　乙は、本契約の締結後、速やかに総括保護管理者等を指名し、総括保護管理者等の氏名、役職等及び個人情報等の安全管理体制について甲に書面で届出を行い、承認を得なければならない。総括保護管理者等又は個人情報等の安全管理体制を変更する場合も同様とする。

（監督・教育）

第６条　乙は、本特記仕様書及び法令等が遵守されるよう従業者を監督しなければならない。

２　乙は、従業者に対して、個人情報等の保護、情報セキュリティに対する意識の向上、その他法令等で定められた安全管理措置に関する教育及び研修を実施しなければならない。

（作業場所）

第７条　乙は、あらかじめ個人情報等を取り扱う事務を行う作業場所（特定個人情報を取り扱う事務については、特定個人情報ガイドラインに規定する取扱区域及び管理区域をいう。以下同じ。）を定め、本契約締結後、速やかに甲に書面で届出を行い、承諾を得なければならない。作業場所を変更する場合も同様とする。

２　乙は、甲の事業所内に作業場所を設置するときは、当該事業所に出入りする全ての従業者に乙が発行する身分証を携帯させなければならない。

（持出しの禁止）

第８条　乙は、本契約において取り扱う個人情報等を作業場所以外の場所に持ち出してはならない。ただし、持出しの理由、方法、場所、持ち出す個人情報等の範囲その他甲の指定する事項について、書面によりあらかじめ甲に申し出て承諾を得た場合は、施錠可能な容器に入れる等の盗難防止措置（電磁的記録媒体で持出しを行う場合は、暗号化等の安全管理措置を含む。）を講じる場合に限り、持ち出すことができる。

（目的外利用等の禁止）

第９条　乙は、法令に特別の定めがある場合を除き、本契約に係る個人情報等を利用目的以外の目的のために利用し、又は第三者に提供（以下「目的外利用等」という。）してはならない。

２　乙は、個人情報等の目的外利用等を行うときは、あらかじめ甲の承諾を得なければならない。ただし、やむを得ない理由により事前に承諾を得ることができない場合は、目的外利用等の後、直ちに報告を行うこととする。

（複製等の制限）

第１０条　乙は、甲の指示又は承諾を受けた場合を除き、甲から提供又は貸与を受けた個人情報等が記録された資料を複写し、又は複製してはならない。

（管理）

第１１条　乙は、本契約に係る個人情報等の管理に当たっては、次に掲げる措置を講じなければならない。

⑴　利用目的、収集から廃棄までの手続を明記し従業者に周知する等、違法な利用や漏えい等の事故発生を防ぐ措置

⑵　施錠可能な書庫等で保管し、個人情報等を保有する端末のワイヤーロックを行う等、盗難を防止する措置

⑶　個人情報等の保管場所への入退室及び機器の持込みを管理する措置
⑷　個人情報等を電子データで保管する場合には、次に掲げる措置
ア　電子データにアクセスできる者及びアクセスできる個人情報ファイル又は特定個人情報ファイルの限定、アクセスログの分析等
イ　電子データを保管する端末への機器接続制限
ウ　２段階以上のアクセス認証
エ　セキュリティソフト、ファイアウォール等による外部からの不正アクセス、サイバー攻撃等の防止
オ　電子データを保管する端末をインターネットから独立させる等の手段によるデータの漏えい防止

（受渡し）
第１２条　本契約の履行に必要な個人情報等の受渡しは、甲が指定した日時及び場所において行うものとし、乙は、個人情報等の受渡しを受けたときは、甲に対して受領証を提出しなければならない。

（返却又は消去等）
第１３条　乙は、本契約が終了したとき又は甲の求めがあったときは、直ちに個人情報等を甲に返却するものとする。ただし、甲から指示があったときは、文書に記録されたものについては溶解等の方法により、電磁的記録媒体に記録されたものについては物理的若しくは磁気的な破壊、ソフトウェアによるデータ消去等の復元不可能な方法により消去し、又は廃棄することができる。
２　乙は、前項ただし書の規定により個人情報等を消去し、又は廃棄するときは、甲乙協議により期限を定めた上で、乙の責任により行うものとし、個人情報等の消去又は廃棄が完了したときは、その完了した事実を証する書類を甲に提出しなければならない。

（再委託の制限）
第１４条　乙は、本契約に係る業務の一部を再委託（再委託の相手方が行う再々委託以降の委託を含む。以下同じ。）してはならない。ただし、再委託先の名称、再委託の理由、再委託する業務の内容、再委託先において取り扱う個人情報等、再委託先における安全管理措置、再委託先に対する管理・監督の方法その他甲が指定する事項を明らかにした上で書面により甲の承諾を得た場合は、この限りでない。
２　前項ただし書の規定により再委託を行う場合は、乙は、本契約に係る契約書に定める事項及び法令等を遵守するよう再委託先の管理・監督を行わなければならない。
３　第３条から前条までの規定は、再委託を行う場合について準用する。

（情報漏えい等が発生した場合の措置及び責任）
第１５条　乙は、本契約に関し個人情報等の漏えい、滅失、毀損等の事故が発生したときは、直

ちに必要な調査を行い、当該事故の内容、発生場所、発生状況、事故に係る個人情報等の内容及び件数その他甲が指定する事項について、書面で甲に報告するとともに、影響を最小限に抑える方策及び再発防止策を講じ、書面により速やかに甲に報告しなければならない。この場合において、甲は、これらの報告の内容について、個人情報保護委員会に報告し、及び公表することができる。

２　乙は、乙の責めに帰すべき事由により発生した個人情報等の漏えい等の事故により甲又は第三者に損害を与えたときは、その損害を賠償しなければならない。

３　前２項の規定は、本契約終了後に発覚した事故に対しても適用する。

（契約内容の遵守に関する報告等）

第１６条　乙は、本特記仕様書の遵守状況について、定期に書面で甲に報告しなければならない。

２　乙は、個人情報等の取扱状況、再委託先の監督状況、安全管理体制等に関して甲からの求めがあったときは、書面により直ちに甲に報告しなければならない。

（必要があると認めるときの実地調査又は監査）

第１７条　甲又は甲が指定した者は、乙（第１４条第１項ただし書の規定に基づき、本契約に係る業務の一部を再委託する場合の再委託先を含む。以下本条において同じ。）の業務に支障を生じさせない範囲において、随時に乙の施設への立入り、必要な書類の閲覧･複写、乙の従業者への聴取等、本特記仕様書に基づき適切な措置が講じられているかを確認し、及び検証するための調査又は監査を実施することができる。この場合において、乙は、合理的事由のある場合を除き、甲又は甲が指定した者が行う調査又は監査に協力しなければならない。

２　甲は、前項の調査又は監査の目的を達成するために必要な範囲において、乙に対して情報の提供を求め、又は改善のための指示を行うことができる。

（法令等に違反した場合の契約解除及び賠償）

第１８条　甲は、乙が法令等の規定又は本特記仕様書に定める義務に違反したときは、本契約を解除することができる。

２　乙は、前項の規定により契約を解除されたときは、損害金として甲に対して契約金額（単価契約であって仕様書等の記載により予定数量が明らかな場合は、契約金額に予定数量を乗じて得た額）の１０分の１に相当する額を支払わなければならない。ただし、契約の解除により甲に生じた実際の損害額が当該１０分の１に相当する額を超える場合は、実際の損害額に相当する額を賠償するものとする。

（管轄の合意）

第１９条　本特記仕様書に規定された事項に関連して生じた甲乙間の紛争については、甲の所在地を管轄する裁判所又は東京地方裁判所を第一審の専属的合意管轄裁判所とする。