

仕様書

1 契約方法

賃貸借契約とし、賃貸借料については、毎月均等払いとする。
 賃貸借料金には、機器の設置及び機器を正常な状態で作動させるための設定・保守に係る費用を含むものとする。
 契約期間は令和8年10月1日から令和13年9月30日とする（長期継続契約）。

2 機器構成

番号	項目1	台数	項目2	規格等
1	ノートPC	1	OS	Windows11 Pro 64bit バージョン25H2
			CPU	Intel Corei5 第13世代 または AMD Ryzen5 第5世代 (Zen4) ※1
			メモリ	16GB ※1
			ストレージ	SSD 256GB ※1
			光学ドライブ	搭載の有無を問わない
			ディスプレイ	15.6インチ（解像度 1920×1080ピクセル）以上 カラー液晶方式 ※1
			入力デバイス	マウス（USB接続）：光学またはレーザー式、2ボタン、スクロールホイール付きとすること
				タッチパッド
				日本語キーボード：JIS標準配列（英数、かな）
			USBポート	USB-TypeA（USB2.0または3.0）×2以上 ※1
			HDMIポート	HDMIポートを持つこと
			オーディオ端子	3.5mmオーディオ端子を持つこと
			内蔵カメラ	720p HDカメラ ※1
			LAN	1000BASE-T/100BASE-TX/10BASE-T
			無線LAN	IEEE802.11a/b/g/n/ac/ax規格 ※1 セキュリティ：WPA2エンタープライズ
			重量	2,000グラム以下
リカバリーメディア	ディスクメディアまたはUSBメモリ ※2 ※保守対応等の際に受注者が用意する場合は、納品は不要とする			
保守	5年間オンサイト出張修理			
2	ソフトウェア	1	PDFリーダー	Adobe Acrobat Reader DC 通常版 64bit ※MUI版がプレインストールされている場合はアンインストールすること。
			Microsoft Office	Office LTSC Standard 2024
			ウェブブラウザ	Google Chrome最新版、Microsoft Edge最新版

※1 同等以上の性能を持つものは可とする。

※2 HDD/SSD故障時に再セットアップできること。光学ドライブを搭載しない場合は、USBメモリとすること。

3 納入・運用要件

- (1) 搬入、設置、庁内ネットワークとの接続、通信確認及びアプリケーション動作のための各種設定を行うこと。
- (2) 納入に際して、庁内ネットワークに接続して使用するために必要な設定（セキュリティ等）を情報企画課が実施するので、情報企画課と事前に協議の上作業すること。
- (3) 故障が生じた場合、速やかに正常な状態で作動するよう回復させること。また、保守業務に係る消耗品及び故障箇所修復に係る部品の費用は、受注者の負担とすること。
- (4) 賃貸借期間終了後、機器の引き上げ（搬出・撤去）は受注者が行うこと。また、機器に格納されていたデータは、復元ソフトウェア等を用いても抽出できないよう物理的な手段を用いて完全に消去すること。
- (5) バンドル版のウイルス対策ソフト等がインストールされている場合は、アンインストールを行うこと。
- (6) その他疑義が生じた場合は、発注者（担当者）と相談すること。

4 情報セキュリティ対策要件

No.	対策要件	実施する対策
1	マルウェアの感染防止	マルウェア（ウイルス、ワーム、ボット等）による脅威に備えるため、想定されるマルウェアの感染経路の全てにおいて感染や感染拡大を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。 〔実施主体：市（情報企画課）及び導入業者〕
2	構築時の脆弱性対策	情報システムを構成するソフトウェア及びハードウェアの脆弱性を悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。 〔実施主体：導入業者〕
3	運用時の脆弱性対策	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を行う方法（手順等）を備えること。また、調達機器において、緊急度が高く保守対象の運用に影響を与える可能性が高いと考えられる脆弱性が発生した場合は、発注者と協議の上、機器の稼働に影響が無い範囲で当該脆弱性を解消する支援を行うこと。 〔実施主体：導入業者〕
4	ログの蓄積と管理	情報システムに対する不正行為の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関するログを蓄積し、3年以上保管すること。 〔実施主体：市（情報企画課）〕
5	ログの保護	ログの不正な改ざんや削除を防止するため、ログに関するアクセス制御機能を備えること。 〔実施主体：市（情報企画課）及び導入業者〕
6	時刻の正確性確保	情報セキュリティインシデント発生時の原因追及や不正行為の追跡において、ログの分析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。 〔実施主体：市（情報企画課）及び導入業者〕
7	主体認証	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうちユーザーの認証を行う機能として、生体（顔）＋知識（パスワード）の方式を採用すること。 〔実施主体：市（情報企画課）〕
8	ライフサイクル管理	主体のアクセス権を適切に管理するため、主体が用いるアカウント（識別コード、主体認証情報、権限等）を管理（登録、更新、停止、削除等）するための機能を備えること。 〔実施主体：導入業者〕
9	管理者権限の保護	特権を有する管理者による不正を防止するため、管理者権限を制御する機能又は運用を備えること。 〔実施主体：導入業者〕
10	情報の物理的保護	情報の漏えいを防止するため、PC端末設置場所の入退室管理を徹底する等によって、物理的な手段による情報窃取行為を防止・検知するための機能を備えること。 〔実施主体：市（生涯学習課）〕
11	侵入の物理的対策	物理的な手段によるセキュリティ侵害に対抗するため、情報システムの構成装置（重要情報を扱う装置）については、外部からの侵入対策が講じられた場所に設置すること。 〔実施主体：市（生涯学習課）〕
12	システムの構成管理	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに、文書どおりの構成とすること。 〔実施主体：市（生涯学習課）及び導入業者〕
13	システムの可用性確保	サービスの継続性を確保するため、情報システムの各業務の異常停止時間が目標復旧時間として24時間を超えることのない運用を可能とし、障害時には迅速な復旧を行う方法又は機能を備えること。 〔実施主体：市（生涯学習課）及び導入業者〕
14	調達する機器等に不正プログラム等が組み込まれることへの対策	機器等の調達工程において、本市が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。 〔実施主体：導入業者〕