

延岡市コワーキングスペースにおけるスマート利用サービス構築委託事業仕様書

第1章 基本事項

1. 業務名

コワーキングスペースにおけるスマート利用サービス構築委託事業

2. 目的

本事業は、延岡市コワーキングスペースにおけるオンライン予約及び使用料決済とスマートロックとを連携させたシステムを導入することで、利用者の利便性向上と、新たに土日祝日の営業に繋げ、利用拡大を図ることを目的とする。

3. 業務内容

ア、施設予約システムの導入

イ、オンライン決済システムの導入

ウ、スマートロックシステムの導入

エ、ア～ウの相互連携、運用保守

4. 契約

契約締結日から 2026 年 3 月 16 日まで

5. 稼働時期・スケジュール

9 月下旬～10 月初旬	契約
10 月初旬～12 月初旬	システム構築
12 月初旬(構築後)～12 月末	運用テスト
	市・コワーキングスペース管理スタッフへの説明等
1 月～3 月 16 日	試験的稼働、調整

6. 成果物

以下の成果物を提出すること

(1) 契約時

業務実施計画書（作業項目・作業内容・役割分担等の記載のあるもの。工程表、業務実施体制及び連絡網等を含む）

(2) システム導入

① システム

ア オンライン予約決済システム

イ スマートロック(4台：入口、ミーティングルーム1～3)

台数、設置場所については上記を想定しているが、受託者と協議の上決定するものとする。

② 随時提出図書

現時点では、下記に示す図書を想定している。詳細は受託者との協議による。

本システム受託者は、随時、書類を提出し、市の承認を得るものとする。

ア 作業工程の計画

イ 会議、打ち合わせの議事録、資料等

③ 導入作業開始時提出図書

現時点では、下記に示す図書を想定している。詳細は受託者との協議による。

本システム受託者は、随時、書類を提出し、市の承認を得るものとする。

ア. プロジェクト計画書

イ. 設定情報

④ 業務完了時

ア. 業務完了報告書

イ. システム操作マニュアル(管理者用)

ウ. システム操作マニュアル(利用者用)

7. その他

- ・業務の実施にあたっては、万全の体制によるものとし、遂行に支障のないようにすること。
- ・業務を他に委託し、または請け負わせてはならない。ただし、あらかじめ市が許可した場合は業務の一部を再委託できるものとする。
- ・本業務に必要な手続き、書類の作成等は、受託者が自己の費用負担において、迅速且つ確実に行うこと。また、本業務の実施にあたり疑義等が生じた場合は、速やかに市と協議のうえ、必要な措置を講じるものとする。
- ・2025年度に必要となる運用費、サポート費等は全て含めること。
- ・本仕様書に記載されていない事項については、両者が別途協議の上、実施することとする。

第2章 システム要件

1. 標準機能要件

「仕様書 別紙1：施設予約システム要求機能一覧」、「仕様書 別紙2：スマートロックシステム要求機能一覧」に示す標準機能要件のとおりとする。なお、対応が難しい場合は、カスタマイズ実現方法または代替案を示すこと。

2. 運用保守要件

市職員及び施設管理者からの問い合わせに関して対応が可能なこと。

対応日時は土日祝日 10:00～17:00 とする。

なお、対応が困難な場合は、コワーキングスペースの運営に支障が出ないような代替の対応方法を用意すること。（システム修復・保守に関しては当日に対応することを要件としない。）

3. 運用要件

○利用者がオンライン上でコワーキングスペースと当施設内ミーティングルームの予約や事前の電子決済を行うことができ、当施設へ自動入館できる機能を有するシステムを要件とする。

【予約決済システム】

ア. オンライン上での決済(クレジットカード、QR、バーコード等)が可能で、スマートロックと連携できること。

イ. 現システムとの互換性を保持できること。または同等のシステムであること。

ウ. 暗号化、マルウェア対策等のセキュリティに関する設計を行うこと。

エ. システムは原則 24 時間 365 日使用可能であること。

【スマートロック】

ア. オンライン決済システムとの連携でコワーキングスペースのスマートロック導入扉を解錠できる QR 等を発行できること。

イ. ミーティングルームごとに対応した解錠 QR 等を発行できること。

ウ. 入口については入室後に自動で扉が閉まり、ミーティングルームについては入室後に扉を閉めた際に鍵がかかる仕様とすること。

4. セキュリティ要件

ア. 延岡市の情報セキュリティポリシー基本指針に準拠すること。

イ. 「仕様書別紙 3 個人情報の取り扱いに関する特記事項」を遵守すること。

ウ. 発注者端末（管理者側）では、固定グローバル IP を持っておれば、IP フィルタリングによって職員側機能を施設外の一般のインターネット回線からは利用できないように設定することができること。

エ. 利用者画面については、SSL または TLS 等の暗号化通信を行うこと。