

スマートロックシステム機能要件一覧
※施設予約システム側で対応できる場合は、省略可能

機能分類体系			玄海町想定要件
大項目	中項目	小項目	
■ 基本要件			
基本事項	サービス提供環境	機器環境	利用者の操作機器環境（PC、スマートフォン）及び管理者側（管理システム・ドライバー）の操作機器環境として、指定する機器環境に対応すること。 利用者側の機器環境 ・対応デバイス：スマートフォン ・対応OS、バージョン：Android11以降、iOS12.5.4以降 ・対応ブラウザとそのバージョン：Chrome55.0.283以降、Safari10以降 管理者側の利用環境 ・対応デバイス：PC ・対応OS、バージョン：Windows11 21H2以降 ・対応ブラウザ、バージョン：Microsoft Edge 94以降
		ネットワーク環境	サービスを提供するネットワーク環境及び通信経路の暗号化について指定する要件に対応すること。 提案する内容が要件と異なる場合は、その理由やネットワークセキュリティ面で問題ないことを示すこと。 開錠装置設置環境：インターネット 管理システム環境：インターネット インターネット上の通信経路においては暗号化を行うこと。
		データ管理	・利用者が登録するデータは、デバイス内には保有せず、サービス提供クラウド環境（データセンター内）でデータを保有すること。 ・情報資産は日本国内に保管されること。
			・バックアップ環境：指定した場合を除き全て日本国内であること。 ・サイクル（間隔）：週次 ・保有世代数（保有期間）：4世代（4週間分）以上が望ましい
		サービス提供時間	指定する時間帯でサービスが利用可能とすること。 メンテナンス時間を除き24時間365日利用できること。
	ライセンス・ユーザ数等	利用者側ユーザ数	利用者側アカウントライセンスが必要となる場合は、指定する要件に対応すること。
		管理者側ユーザ数	管理者側アカウントライセンスが必要となる場合は、指定する要件に対応すること。
	デザイン・操作性	デザイン・操作性	表示画面上の項目配置や色使い等、誰もが利用しやすいユニバーサルなデザインであること。また、利用者およびサービスを提供する管理者双方にとって、わかりやすい操作性が確保されていること。
		アクセシビリティ	アクセシビリティに配慮したデザインであること。
		視覚障害者支援	視覚障害を持つユーザーの操作を補助するように配慮することが望ましい。
		多言語対応	指定する言語に対応すること。
	情報セキュリティ	認証資格	適切に情報資産の管理運用を行うため次のいずれ又はここに掲げるもの相当する認証制度・評価制度に対応すること。 ・政府情報システムのためのセキュリティ評価制度（ISMAP） ・ISO27001 ISMS情報セキュリティマネジメントシステム ・ISO27017 ISMSクラウドセキュリティ認証 ・プライバシーマーク
		データセンター	・データセンターは Tier3 または4相当であり、建築基準法（昭和 25 年法律第 201 号）の新耐震基準に適合していること。 ・データセンターの物理的所在地を日本国内とし、情報資産について、合意を得ない限り日本国外への持ち出しを行わないこと。

		個人情報・情報セキュリティの遵守	遵守する法令および条例等は次のとおりとする。 ・個人情報保護法 ・玄海町個人情報保護法施行条例 ・玄海町情報セキュリティポリシー
		システムログ	エラー情報の把握やUI/UXの改善に必要なログ情報を取得すること。
		アクセス・操作ログ	管理システムのアクセスログ・操作ログを取得すること。
		不正プログラム対策	システム（サービス）の稼働環境及び開発・テスト環境においては、コンピュータウィルス等不正プログラムの侵入や外部からの不正アクセスが起きないよう対策を講じるとともに、それら対策で用いるソフトウェアは常に最新の状態に保つこと。
			システム（サービス）の稼働環境及び開発・テスト環境で用いるOSやソフトウェアは、不正プログラム対策に係るパッチやバージョンアップなど適宜実施できる環境を準備すること。
		その他セキュリティ対策	システム運用・監視体制の確保やインシデント対応の実施手順や訓練等が計画的・継続的に実施されていること
	サービス終了時・契約満了時等の対応	保有データの提供	サービス開始後に利用者が入力した情報及び当町が登録した情報のうち、当町の情報管理権限を有する情報（当町が提供を希望する情報）については、契約終了時に全て抽出し当町に提供可能とすること。
		保有データの消去等	データ消去後に、当該データを保存していた記憶装置の物理的破壊を行うとともに、そのエビデンスを提出すること。
		オプトアウト対応	利用者からの申し出により、当該利用者に関する情報を全部または一部削除できること。
	利用規約等	利用規約への同意	サービスの初回利用時やサービスに重要な変更を行った際には、利用者に利用規約の内容を提示し、確認（同意）をとることができること。
		自動取得情報への同意	機器の個体番号やGPS位置情報等、利用者がサービスを利用した場合に自動的に取得する場合は、情報を明示するとともに、それら情報取得について同意を得ることができること。（利用規約の確認に含む場合は不要）
	問い合わせ機能	－	管理者側の問い合わせ方法は次のいずれかの方法とする。 ・サービス内の問い合わせフォームから行えること ・問い合わせ先のメールアドレスを記載すること ・ヘルプデスクを設置すること
資格管理	統計機能	－	集計するデータは次のとおりとする。 利用登録者数、登録団体数、アクティブ利用者数、機能ごとの利用数 など
	関係法規制への対応	－	サービスの稼働、運用・提供に係る関係法規制を遵守するとともに、常に最新動向を把握し、適宜必要な見直し・改善を実施すること。
	利用者側アカウント管理	管理情報	利用者登録に必要な情報は次のとおりとする。 個人利用者の場合：氏名、住所、生年月日、電話番号、メールアドレス、認定されている固定減免の情報 など 団体利用者の場合：団体名、代表者および連絡担当者それぞれの氏名、住所、生年月日、電話番号、メールアドレス、認定されている固定減免の情報 など
		アカウント登録・設定	利用者アカウントIDは、任意の文字列を指定できること。
		アカウント認証方法	ID、パスワードで認証できること。
			その他、マイナンバーカードの公的個人認証サービスを用いた本人認証やログインが実施できることが望ましい。
			利用者がパスワードを失念した場合、利用者自らがパスワードの再設定やパスワードの確認ができること。
		アカウント情報の修正・停止（廃止）	利用者自身がシステム上でアカウント情報の修正・停止（廃止）を行えること。 管理者が利用者のアカウント情報を確認・停止（廃止）、削除ができること。
	管理者側アカウント管理	管理情報	管理者側利用者登録に必要な情報は次のとおりとする。 ・氏名、所属名、メールアドレスなど
		アカウント登録・設定	・システム管理者が、管理者側アカウントを発行することができること。 ※システム管理者等の依頼による委託者等の作業も含む

		アカウント認証方法	管理者アカウントの認証方法（再認証も含む）について、指定する要件に対応すること。 ・ID、パスワードで認証できること。 ・IPアドレス制限や多要素認証等が設定できること。
		アクセス制御	・管理者及び利用者アカウント毎に、使用可能な機能や権限の制御が出来ること。
		アカウント情報の修正・廃止	システム管理者が管理者側利用者アカウント情報を確認・停止（廃止）、削除ができること。
		不正ログイン対策	システム管理者のアカウントについて、同一IDでの同時ログイン操作の制御など不正ログインを防止する対策を講じること。
■機能要件			
前提条件	予約システムとの連携	－	施設予約システムと鍵情報の連携ができること。
鍵情報設定・制御等	鍵情報（暗証番号等）の発行・設定	鍵情報（暗証番号等）の発行	施設予約システムの利用者側画面からの予約に対して、鍵情報（暗証番号等）を自動発行できること。 自動発行される鍵情報（暗証番号等）は、発行毎に異なる番号や予約情報を使いまわしができないQRコード等の設定されること。 施設窓口での予約において、施設予約システムの管理者側画面から職員の操作による鍵情報（暗証番号等）の発行（再発行含む）ができること。
		鍵情報（暗証番号等）の有効期限	鍵情報（暗証番号等）の有効期間を任意に設定できること。
		鍵情報（暗証番号等）の確認	発行した鍵情報（暗証番号等）が、管理システム上で容易に確認できること。
		鍵情報（暗証番号等）の発行数	施設利用者毎に異なる鍵情報（暗証番号等）を、指定する人数分以上を常時発行できること。
	解錠・施錠機能	利用者への通知機能	施設予約システムを通じて鍵情報（暗証番号等）を利用者へ通知することができること。なお、施設予約システムとの連携の要件に対応すること。 施設予約システムの通知機能とAPI連携し、鍵情報（暗証番号等）の通知ができること。
		鍵情報	事前に発行した鍵情報（暗証番号やQRコード等）を利用し、容易に解錠及び施錠が可能であること。 鍵情報は、暗証番号以外に、マイナンバーカードや生体認証情報等を利用した解錠及び施錠に対応すること。
		オートロック	オートロック機能など退出時の施錠忘れを防止する機能があること。
		マスターキー	施設管理者等が解錠するにあたり、マスターキーとなる鍵情報（暗証番号等）を設定することができること。
	異常時への対応	－	災害時、通信環境が正常動作していない状態であっても、管理システムで事前に発行した非常用暗証番号を利用し、開錠できること。
		－	－
施設管理者向け機能	管理システム	複数錠の管理	複数の設置個所をまとめて一括管理できるグルーピング機能を有すること。
		遠隔管理	遠隔操作により施錠及び解錠ができること。
		メンテナンス情報	電池式の場合に遠隔でも電池残量を確認できることが望ましい。
			電池式の場合に電池交換時期を施設管理者に通知できること。
		履歴確認	解錠・施錠履歴を履歴を確認できること。