凡例：
必須：本業務のサービスを実現する上で必須の機能要件
拡張性要件：本市が今後スマートシティの各サービスを連携推進していく上で、将来的に必要となる要件。プラットフォームとしての拡張性を担保すること。

機能区分L1	機能区分L2	機能名		機能要件	要件区分
サービス連携	共通サービス	CMS機能	HPコンテンツ登録・更新・削除機	・管理者にて各種情報コンテンツを登録・更新・削除できる機能を備えていること	必須
			プレビュー機能	・ブラウザ同様に、ホームページの現在の状態を閲覧出来ること。 ・また、ディレクトリに沿って任意のページを参照する事も出来ること。 ・ページの新規作成・更新・削除・非公開作業を開始出来ること	必須
			コンテンツ複製機能	・管理者でコンテンツをコピーできること	必須
			コンテンツ公開・非公開機能	・管理者でコンテンツの状態を公開・非公開に出来ること。	必須
			HPコンテンツ表示機能	・登録した記事が表示できること ・カテゴリーの階層で表示できること ・第二階層のカテゴリーのサマリーページの表示ができること ・新着情報の表示ができること ・記事ランキング表示ができること ・よく閲覧される記事のタグ表示ができること	必須
			テンプレート管理機能	・複数のテンプレートを用意し、登録するHPコンテンツに応じて選択ができること	必須
			カテゴリ・タグ管理機能	・タグ登録・更新・削除ができること ・カテゴリ登録・更新・削除ができること	必須
			ID管理機能	・管理者向けのWeb画面を提供し、ID・パスワードにてログイン・ログアウトする機能を提供すること	必須
			アクセス制御機能	・アセット（ユーザー、組織など）ごとに権限を設定することができること ・権限を割り当てるロールを設定することができること	必須
			多言語翻訳機能	・無料翻訳サービス等と連携し、すべてのページで英語・中国語(簡体字)・韓国語に対応した外国語翻訳ができること。	必須
			音声読み上げ	・記事の音声読み上げができること。	必須
			検索エンジン機能	・サイト内をキーワード検索することができる機能を設け、利用者が求める的確な検索結果が表示されるようにすること。	必須
			問い合わせ機能	・利用者が問い合わせフォームから送信した質問、要望等に対して、担当課に内容が通知される機能を提供すること	必須
			ワークフロー機能	・記事作成者、承認者等に応じた権限管理機能を提供すること。	必須
			バナー管理機能	・バナー広告の登録・管理ができること ・登録したバナーを表示できること	必須
			コメント投稿・削除機能	・Webサイト上で、利用者等がコンテンツに関するコメントを投稿・削除できる機能を備えていること	必須
			コメント監視・通知機能	・利用者のコメントを監視する機能を備えていること ・違反コメントについて、利用者等が通知・報告できる機能を備えていること	必須
			マルチデバイス表示機能	・レスポンシブルWebデザイン等を採用し、パソコンやスマートフォンでのWebブラウザに対して適切な画面表示にて表示が可能であること	必須
			お知らせ機能	・重要なお知らせ等を利用者に通知する機能を備えていること	必須
		ログイン機能	ID登録・管理機能	・利用者IDを取得する機能を有すること。 ・ID登録時において利用者の情報を取得できること。 取得する情報としては以下とする。 -年齢 -性別 -住所 -職業 -婚姻の有無 -子どもの有無 -興味がある情報（くらし、あそび、教育、文化、手続き、市政、防災の各分野） -よく行く周辺地域 -市外居住者の属性 ・パスワード忘れの際の再発行機能を有すること。	必須
			ソーシャルログイン連携機能	・ソーシャルIDを用いた利用者ログインが可能であること。 ・ログインに用いるソーシャルIDは、複数ID（Google、Facebook、LINE、Yahooなど）が利用できること。	必須
		レコメンド機能	コンテンツ提供機能	・CMS機能と連携し個人の嗜好性、行動履歴等に基づき、表示コンテンツ・表示順位をWebサイト上で最適化表示できること	必須
			レコメンド設定機能	・管理画面においてレコメンドの設定情報を管理できること	必須
		データ分析機能		・本サイト上のPV数、アクセス状況等を確認できる機能を提供すること。	必須
	API管理	APIライフサイクル管理機能		・デジタルシティ基盤の API のライフサイクル（登録、参照、変更、削除）を管理できること	必須
		APIゲートウェイ機能		・デジタルシティ基盤のAPI の使用量制限やネットワーク速度制限、複数 API の集約等を実行できる機能を有すること	必須
	他都市OS間連携	認証連携機能		・将来的に他の都市 OS と連携し、他の都市 OS 利用者の認証情報を基に、利用者からの認証要求に対応できること。	拡張性要件
認証	認証・認可	認証機能		・「ユーザ管理」に保存された資格情報（ユーザ ID・パスワードや、生体情報等）を用いてユーザの真正性を証明し、アカウントを特定できること。	必須
		認可機能		・「ユーザ管理」と連携し、アカウントに紐づくロールやポリシーを基に、デジタルシティ基盤 の各種機能や管理するデータの利用範囲を許可・制限できること。	必須
		個人認証機能		・将来的にマイナンバーカードによって電子的に利用者の本人確認を行うことが、外部認証機関等との連携により実現できる機能を有すること	拡張性要件
		シングルサインオン機能		・将来的にデジタルシティ基盤と連携する複数のサービスに対する認証を一元的に管理し、シングルサインオンを実現できること。 利用者が一度だけ認証することで、デジタルシティ基盤 と連携する本市スマートシティサービスそれぞれ個別に認証する必要がなくなり、ワンストップサービスの実現につながることが望ましい	拡張性要件
	ユーザ管理	アカウント管理機能		・利用者を特定の ID に関連づけ、認証情報（パスワード）や属性情報（姓名、組織等）の管理と、ID のライフサイクル（登録、参照、変更、削除）を管理できること。	必須
		ロール管理機能		・利用者が所属するグループ（利用者、管理者等）を定義するロールを管理できること。	必須
		ポリシー管理機能		・アカウントやロール別に、デジタルシティ基盤 にアクセスする範囲や権限を定義する制御ポリシーを管理できること。	必須
サービスマネージメント	サービス管理	サービスライフサイクル管理機能		・デジタルシティ基盤と連携する本市で提供する今後のスマートシティサービスのライフサイクル（登録、参照、変更、削除）を管理できること。 ・デジタルシティ基盤が管理するサービスの一覧は、「サービス連携」と連携し、利用者に公開されることが望ましい。	拡張性要件
		サブスクリプション管理		・利用者が利用できるスマートシティサービスに対して、サブスクリプションの状態（利用の開始終了、利用権限の設定変更）を管理できること	拡張性要件
	サービス履歴管理	利用履歴管理		・利用者の同意のもと、利用者によるデジタルシティ基盤やスマートシティサービスの利用履歴の蓄積・公開する機能を提供すること。	必須
データマネジメント	データ仲介	データ蓄積		・デジタルシティ基盤 が管理するデータに対し、「データ管理」と連携しデータを処理（登録・参照・更新・削除）できること。	必須
		データ分散		・他都市 OS や他システムに分散するデータに対し、データを仲介（登録・参照・更新・削除）できること。	必須
	データ管理	データストア		・特性（多様性、頻度、量）が異なる様々なデータに対し、地域が解決する課題に必要なデータを、適切に蓄積・活用できること。 データの分類として、パーソナルデータやリアルタイムデータ等がある。リアルタイムデータ等の連続したデータを時系列で確認できるよう履歴を管理できることが望ましい。	必須
		ユニークID管理		・デジタルシティ基盤が管理するデータそれぞれにユニークな ID を管理し、地域をまたいだ様々なデータの中から一つのデータを特定可能とする仕組みを提供できること	必須
アセットマネジメント	デバイス管理	デバイスライフサイクル登録		・デバイス情報（デバイス ID や、固有の MAC アドレス等）のライフサイクル（登録、参照、変更、削除）を管理できること	拡張性要件
		デバイス認証		・事前に登録されたデバイスのみアクセスを許可することができること。	拡張性要件
	システム管理	システムライフサイクル登録		・デジタルシティ基盤 と連携する他システムの連携情報のライフサイクル（登録、参照、変更、削除）を管理できること。他システムには認証が必要な場合も多く、認証方式やその資格情報についても管理できることが望ましい	必須
外部データ連携	データ処理	データ変換		・外部から取得したデータをデジタルシティ基盤 が扱える形式に変換できること。変換対象は、語彙や、形式、項目等が存在するが、取り扱うデータにより変換対象が異なる。	必須
		データ受付（キューイング）		・デジタルシティ基盤にデータを蓄積するため、データアクセス（登録・参照）を受け付けること。	必須
	データ伝送	プロトコル変換		・地域に展開するスマートシティアセットや他システムと接続するため、一般的な通信プロトコルからデジタルシティ基盤が対応する通信プロトコルに変換できること。	必須
セキュリティ		認証		・デジタルシティ基盤に接続する利用者、スマートシティサービス、他都市 OS、他システム、IoT デバイス等に対して正しい接続相手であるかを検証し、アクセス権限を与える機能を提供すること。	必須
		暗号化		・デジタルシティ基盤 が行う通信（デジタルシティ基盤 内の通信及び基盤 外との通信）及び、デジタルシティ基盤 が管理するデータに対して、それぞれの秘匿性に応じ適切なセキュリティ暗号化を行うこと。	必須
		不正アクセス防止		・デジタルシティ基盤が許可されていない通信（不正な IP アドレスやポート番号を持つパケット等）をブロックする機能を提供すること。ファイアウォール機能とも呼ぶ。	必須
		不正アクセス検知／遮断機能		・不正アクセス防止機能では対応できない、DoS 攻撃やアプリケーション層の脆弱性を突く攻撃等を検知し、遮断する機能を提供すること。	必須