データ連携基盤に求められる互換性・安全性・プライバシーに関する事項について

- スーパーシティ等において、「**データ連携基盤**」は、自治体や事業者、個人等が有する**様々なデータを収集・整理・提供**することにより、**先端的サービスの提供を行う**ために必要不可欠な**中核的な基盤**。
- データ連携基盤の整備・運用に当たっては、
  ① 様々な**データやサービスが相互に連携**し、**相乗効果を創出**するために「**相互運用性の確保**」が重要であるとともに、
  ② データの**安全な管理・運用**を行うために「**セキュリティ対策**」を実施することや、
  ③ **個人情報を含むデータ**を取り扱う場合には「**プライバシー対策**」に万全を期すことが求められる。
- 今後、データ連携基盤を活用した取組が安全かつ円滑に進められるよう、**これらの観点に関する既存の知見**を、「スーパーシティ等における**データ連携基盤に求められる互換性・安全性・プライバシーに関する事項**」として整理。

スーパーシティ構想の全体像

（※）API :Application Programming Interface :
異なるソフト同士でデータや指令をやりとりするときの接続仕様

データ連携基盤に求められる事項

① 相互運用性の確保

- 様々なデータやサービスが相互に連携するための機能の実装
  （ブローカー、オープンAPIの実装　等）
- データの相互利用性に関するルールへの適合
  （データカタログサイトの公開、標準的なデータモデルの参照　等）

② セキュリティ対策

- システム面でのセキュリティ対策
  （暗号化、不正アクセスの検知・遮断、アクセスログ等の証跡管理　等）
- ガバナンス面でのセキュリティ対策
  （セキュリティ計画・規程の策定、責任体制の明確化、要員の確保 等）

③ プライバシー対策

- 個人情報保護法令に基づく適切な措置
  （本人同意の取得、個人情報の適切な管理、第三者提供ルール　等）
- 個人情報保護法令に加えて求められる事項
  （プライバシー影響評価（PIA）の実施、データ分散方式の採用　等）

データ連携基盤に求められる具体的事項（概要）

➢ これまでのスーパーシティやスマートシティ等に関する**ガイドライン等**※で示されている**データ連携基盤に求められる事項**について、**①相互運用性の確保（互換性）**、**②セキュリティ対策（安全性）**、**③プライバシー対策**の観点から**整理して提示。**

※ スマートシティリファレンスアーキテクチャ（内閣府科学技術・イノベーション推進事務局）、政府相互運用性フレームワーク（デジタル庁）、データ連携基盤技術報告書（内閣府地方創生推進事務局）、スマートシティセキュリティガイドライン（総務省）、サイバーセキュリティ経営ガイドライン（経済産業省） 等

① 相互運用性の確保

1．データ仲介（ブローカー）

➢ 複数のデータを仲介し、サービス提供者等へデータを提供するために必要となる機能要件

2．オープンAPI

➢ サービス提供者やデータ提供者等との相互接続を行うために必要となる機能要件

3．データカタログサイト

➢ 多様なサービス提供者等がデータや利用規約等を閲覧・利用できる環境の整備

4．データモデル

➢ 政府相互運用性フレームワーク（GIF）等の標準的なデータモデルの参照

② セキュリティ対策

1．システム要件

＜技術機能面＞

➢ データの暗号化や不正アクセス防止等に関する機能要件

＜管理機能面＞

➢ 脆弱性の適切な管理・対策の実施や証跡管理等の機能要件

2．ガバナンス要件

＜計画整備面＞

➢ 情報セキュリティ基本方針やセキュリティ対策基準、データ取扱基準等の策定

＜実施体制面＞

➢ 持続的かつ適切にセキュリティ対策を講じることができる体制の整備

＜委託先・連携先の管理面＞

➢ データ連携基盤に接続するサービス提供者やデータ提供者のセキュリティ対策状況の確認・管理

③ プライバシー対策

1．個人情報保護法令の確実な遵守

➢ 利用目的の特定、本人の同意の取得、個人情報の安全管理、第三者提供の制限 等

2．法令遵守に加えて求められる事項

＜運用ルールの整備＞

➢ 関係者間の責任明確化や法令遵守の徹底
➢ 第三者提供先の制限
➢ プライバシー保護対象範囲の拡大 等

＜透明性の確保＞

➢ 住民による問い合わせや相談等の窓口整備
➢ 個人情報が扱われる仕組みの公表
➢ パーソナルデータの公開範囲の指定機能 等

＜データの管理方法＞

➢ データ分散方式によるプライバシーインパクト軽減
➢ データ蓄積時のセキュリティ対策の徹底 等

＜プライバシー影響評価（PIA）＞

➢ 個人情報を取り扱う場合に想定されるリスクの事前評価と、適切な対策の検討・実施

①相互運用性の確保（互換性）において求められる事項

- 様々なデータやサービスが相互に連携し、相乗効果を創出するために**「相互運用性の確保」**が重要。
- このため、**ブローカーやオープンAPIといった相互連携に必要な機能の実装**や、**データカタログサイトの公開や標準的なデータモデルの採用等のルールへの適合**することが求められる。

■相互運用性の確保に関する主な求められる事項

必要となる観点	求められる事項
1．データ仲介機能（ブローカー）	データ連携基盤に接続される様々な**データを仲介**し、適切にサービスへデータを送信できる機能を有すること
	パーソナルデータを取り扱う場合、個人が蓄積された自身の**パーソナルデータ（氏名、住所、位置情報等）の所在や同意状況を把握できる機能**を有すること
2．接続方式（オープンAPI）	**多様なサービスやデータ等との接続**を可能にするオープンなAPIを有すること また、アクセス制限や認証管理等を機能を有すること
3．データカタログサイト	情報の見つけやすさを向上させるため、**以下のデータを公開**すること ＜最低限公開すべきメタデータ＞ ・APIエンドポイントまたは静的データの配布URL ・APIまたはデータの利用条件（例：利用規約、利用方法、契約の要否、利用制限、データ形式、データモデル解説）
4．データモデル	デジタル庁が推進する**「自治体標準オープンデータセット」**や**政府相互運用性フレームワーク（GIF）**に記載のある**「地域サービスデータモデル」**における**「地域サービス・データモデル」**等を参照し、**データモデルの標準化を図ること**

②セキュリティ対策（安全性）において求められる事項

- 国内外からのサイバー攻撃リスク等から、データを安全に管理・運用するために**「セキュリティ対策」**が重要。
- このため、**データの暗号化や、不正アクセスの検知・遮断等といったシステム要件**と、**継続的に適切なセキュリティ対策を講じるための計画や実施体制の整備等のガバナンス要件**が求められる。

■セキュリティ対策に関する主な求められる事項

必要となる観点	求められる事項
１．システム要件	データ提供事業者・サービス提供者等の**認証と適切なアクセス制御**を実施すること
	データ連携基盤が行う通信や流通するデータに対して、適切な**暗号化対策**を行うこと
	日々進化するサイバー攻撃等の脅威に対して、これらの**検知・遮断**を行うセキュリティ対策を講ずること
	脆弱性に関する情報収集、**脆弱性を克服するためのプログラムの適用**等の必要な対策を継続的に講ずること
	障害発生時、可能な限り停止することなく稼働し続けるため、**定期的なバックアップや冗長化**を行うこと
	証跡確保のためのログを取得すること（サーバー等に対するアクセスログや操作ログ等）
２．ガバナンス要件	以下の**計画を策定**し、継続的に安全性の確保を行うこと。 ・情報セキュリティ基本方針（情報セキュリティに関する基本的な事項を示す取組方針） ・セキュリティ対策基準（基本方針に基づいて、具体的な遵守事項や判断基準等を定める基準） ・データ取扱基準（セキュリティ・プライバシー等の観点からデータ種別ごとに取扱方法を定めた基準） ・インシデント対応手順（インシデント発生時の対応フローや連絡体制を定めた運用規定） ・事業継続計画（障害等から迅速に復旧するための対応手順、判断基準、役割分担を定めた計画）
	平時及び非常時の**責任体制**及び関係者の**役割分担**を明確にしていること
	サイバーセキュリティに関する計画の策定、実施、評価及びその**改善を継続して行うための仕組み**（第三者認証の取得又は外部監査）を構築すること
	サービス提供者やデータ提供者等のデータ連携基盤に接続する者に対し、アクセス制御や認証機能等の**「スマートシティセキュリティガイドライン」で要求される事項の遵守**を要求すること

③プライバシー対策において求められる事項

- 住民が安心して個人情報を提供し、サービスによる便益を享受するために**「プライバシー対策」**が重要。
- このため、**本人の同意取得**等を含む**個人情報保護法令の確実な遵守**に加え、**法令遵守に加えて**運用ルールの整備、透明性の確保、**プライバシー影響評価（PIA）の実施などの対策を行う**ことが求められる。

■プライバシー対策に関する主な求められる事項

必要となる観点	求められる事項
1．個人情報保護法令の確実な遵守	利用目的の特定、本人の同意の取得、個人情報の安全管理、第三者提供の制限等に関する**個人情報保護法令を確実に遵守**すること
2．法令に加えて要求する事項	データ連携基盤整備事業の実施主体は、データ連携基盤の利用規約等を通じて、**ステークホルダー間の責任分界点を明確化**し、**法令順守を徹底**させること
	個人情報の取扱いを委託する者や**第三者提供先**については、**一定の資格**（プライバシーマーク又はJISQ15001に準じる取扱いをすることが確認されること等）**を有する者に限定**すること
	個人情報より広義なパーソナルデータ（※）をプライバシー保護の対象とすること ※個人情報に加え、個人情報との境界が曖昧なものを含み、個人の属性情報、移動・行動・購買履歴、ウェアラブル機器等から収集されたデータあるいは加工された情報等個人と関係性が見出される広範囲のデータ（個人情報保護法令にて定める個人情報・個人関連情報・仮名加工情報を指し、匿名加工情報は含まれない）
	個人や事業者からの問い合わせ、開示請求、苦情・相談等を受け付ける**窓口の整備**や、住民による訂正の求め、第三者提供停止の求め、利用停止・消去の求めに対応する体制を整備すること
	個人情報が扱われる仕組みやデータ利用者の制限等の**ルールを公表**すること（プライバシーポリシー、利用規約 等）
	自身の**パーソナルデータの公開範囲を指定**するための機能を有すること
	プライバシーインパクトが懸念されるデータについては、原則として、**データ分散方式**とすること また、データの蓄積が必要な場合は、個人情報の保護に万全を期する他、セキュリティ対策を十分に行うこと
	パーソナルデータを扱う前に、**プライバシー影響評価（PIA）**を実施し、個人情報の漏洩等の想定されるリスクの**事前の評価と、適切な対策**の検討を行うこと

（参考）求められる事項一覧

① 相互運用性の確保（互換性）1. データ仲介（ブローカー）

小項目		求められる事項	重要
共通（機能要件）	1	ビルディングブロック方式を採用していること	○
	2	データ提供者からデータを受け付け、必要なサービスへデータを送信できること ※デジタル庁が推奨し、一般社団法人データ社会推進協議会（DSA）において導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	3	データ参照の要求を受け付け、外部サービスが保持するデータを返却可能なこと ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	○
	4	データ利活用の利便性を考慮し、「データ連携基盤技術報告書（内閣府：令和３年３月）」に示されるAPI標準仕様案に沿ったAPI（REST等）を提供可能なこと ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	○
	5	サービス呼び出しの要求を受け付け、外部サービスの処理を実行し、結果を返却可能なこと ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	6	外部サービスへの接続時、接続先サービスのインターフェースに合わせたデータ変換が可能なこと	
	7	データ利用者に対してデータの所在を秘匿することができること ※非パーソナル：推奨、パーソナル：重要 ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	8	データ提供者からデータを受け付け、データストア機能に蓄積可能なこと ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	9	データ参照の要求を受け付け、データストア機能に蓄積されたデータを返却可能なこと ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	10	データ送信時、リアルタイムにデータの分析・変換・加工処理等が可能なこと	
	11	多種多様のアセットからのデータ収集を想定し、標準APIに限らず様々な接続方式（MQTT等）に対応可能なこと	
	12	定期的に他システムを巡回し、データを取得できること	
	13	重要なデータに対しては、リアルタイムデータ等で欠損したデータを補完し、データ品質の向上を行うこと	
共通（非機能要件）	14	利用状況に応じた柔軟なリソース拡張が行えること（スケールアップ・スケールアウト等）	○
	15	保守及びサポート体制を整備すること	○
	16	データ連携基盤事業の実施主体が運用管理を行うためのUIがあること	
	17	データ連携基盤事業の実施主体の保守作業の効率化のため、構築・運用・利用に関する情報が入手可能であること	
	18	５分野以上の先端的サービス間のデータ連携ができること	
	19	２段以上のデータ仲介ができること ※接続する他都市のブローカーを経由して他都市の先端的サービスへアクセスを想定	

① 相互運用性の確保（互換性）1. データ仲介（ブローカー）

小項目	求められる事項		重要
パーソナル（機能要件）	20	【パーソナルデータを取り扱う場合】 個人が、蓄積された自身のパーソナルデータ（氏名、住所、位置情報、購買履歴等）の所在及び共有状況を把握できること 例）パーソナルデータを仲介する際に、データセット種別単位で、データの蓄積先や共有先情報を管理し、本人の開示請求時に所在及び共有状況を開示できること。 ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	○
	21	【パーソナルデータを取り扱う場合】 サービス上で複数のパーソナルデータのデータセットが取り扱われる場合、個人がサービス提携組織（アプリ）による蓄積・共有に対する自身の同意状態を、「データセット種別」の認可粒度で管理できること 例）個人がアプリ上で、パーソナルデータの蓄積・共有の同意を行った結果について、「データセット種別」でブローカーが管理を行い、蓄積・共有の同意状況に応じた処理を実施することができること。 ※データセットとは、例えば心電図データ、購買データの一式等、データをまとめたものを指す ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	○
	22	【パーソナルデータを取り扱う場合】 個人が、蓄積された自身のパーソナルデータの内容をデータ実体単位で確認できること 例）パーソナルデータを仲介する際に、データ実体単位で、データの蓄積先や共有先情報を管理し、本人の開示請求時に所在及び共有状況を開示できること ※データ実体とは、例えば特定の健診日の心電図データ、購買データ等、特定のデータの中身のことを指す ※No20ではデータセット種別の単位で蓄積先や共有先の情報を管理することを要求しているのに対し、No22ではデータ実体単位で管理することを要求している。 ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	
	23	【パーソナルデータを取り扱う場合】 個人が、「サービス提携組織（アプリ）による共有」に対する自身の同意状態を「データ実体」の認可粒度で管理できること 例）個人がアプリ上で、パーソナルデータの蓄積・共有の同意を行った結果について、「データ実体単位」でブローカーが管理を行い、蓄積・共有の同意状況に応じた処理を実施することができること。 ※データ実体とは、例えば特定の健診日の心電図データ、購買データ等、特定のデータの中身のことを指す ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているブローカーを採用する場合は、本要件を満たす	

① 相互運用性の確保（互換性）2. オープンAPI

小項目	求められる事項		重要
共通	24	データ連携基盤で活用するAPIは、可能な限り、狭義のオープンAPI（※）とすること ※狭義のオープンAPIとは、誰でもアクセス可能なAPI、一定の規約や契約が必要なものの誰でもアクセス可能なAPIを指す。なお、広義のオープンAPIとは、参加資格要件等が定められたコンソーシアム等のメンバーのみがアクセス可能なAPI、相手方との相互契約や合意に基づいてアクセス可能となるAPIを含むものを指す	○
	25	APIは、原則として、設計様式としてREST、データ形式としてJSONを利用すること	○
	26	API利用規約は、原則として、「データ連携基盤技術報告書（内閣府：令和３年３月）」API利用規約テンプレート（※）に基づいて作成されたものとすること ※別紙「API利用規約テンプレート」を参照	○
	27	APIは、原則として、「データ連携基盤技術報告書（内閣府：令和３年３月）」の「表 3-3-1 API標準仕様案」に基づき実装すること	○
API管理	28	APIゲートウェイで管理するAPIを登録・参照・変更・削除できること ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているAPIゲートウェイを採用する場合は、本要件を満たす	○
	29	アクセス可能なAPIやデータを制限できるほか、単位時間あたりのAPI実行回数を制限できること ※デジタル庁が推奨し、DSAにおいて導入支援等を行っているAPIゲートウェイを採用する場合は、本要件を満たす	
認証系API	30	「ユーザ管理」（※）に保存された資格情報（ユーザID・パスワード、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 ※「ユーザ管理」とはデータ連携基盤の管理するユーザを一元的に管理する機能を指す	○
	31	「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元に、データ連携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 ※「ユーザ管理」とはデータ連携基盤の管理するユーザを一元的に管理する機能を指す	○
	32	アカウント管理に保存された資格情報（ID・パスワード、生体情報等）を用いて、検証及びアクセストークンの払い出し・失効を行えること	○
	33	他のデータ連携基盤と連携し、他のデータ連携基盤の利用者の認証情報を元に、利用者からの認証要求に対応できること	
	34	【パーソナルデータを取り扱う場合】 パーソナルデータを利用・提供する場合など高いセキュリティが求められる認証に対して、多要素認証（デバイス認証・生体認証、マイナンバーカード等の組み合わせ等）により、セキュアに本人を特定できること	○
	35	【パーソナルデータを取り扱う場合】 利用者を特定のIDに関連付け、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	○
	36	【パーソナルデータを取り扱う場合】 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	○

① 相互運用性の確保（互換性）2. オープンAPI

小項目	求められる事項		重要
認証系API	37	【パーソナルデータを取り扱う場合】 認証されたユーザに関して、あらかじめ通知された目的を達成するために必要な属性を取得できること	
	38	【パーソナルデータを取り扱う場合】 データ連携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	
サービス系API	39	データ連携基盤と連携しているサービスが保持するAPIを、データ連携基盤上のAPIとして公開する機能を提供すること	
	40	データ連携基盤と連携する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	○
データ管理系API	41	データ連携基盤のデータマネジメントと連携し、データのライフサイクル（登録、参照、変更、削除）を管理するためのAPIを提供できること	○
	42	データ連携基盤が保管するデータに変更が生じた際に、リアルタイムに変更内容を通知先に送信するためのAPIを提供できること また、通知内容（条件や通知先等）のライフサイクル（登録、参照、変更、削除）を管理するためのAPIについても提供できること	
	43	分散するデータに対し、その所在のライフサイクル（登録、参照、変更、削除）を管理するためのAPIを提供できること	○
	44	【要配慮個人情報を取り扱う場合】 サービス提供事業者等へ要配慮個人情報を提供する際には、サービスの特性や利用者の要望に応じるために、データ提供先を限定する機能に加えて、データ提供期間を限定する機能を提供すること	○
	45	【パーソナルデータを取り扱う場合】 パーソナルデータの提供時には、データの提供履歴が保存されること	○
	46	データ連携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すること これにより、他のデータ連携基盤と連携し、利用者に他のデータ連携基盤のデータを提供できること 例）Entity IDの中に都市情報をインプットし、どの都市の情報か区別できるようにする　等	
	47	トレーサビリティによるデータ品質向上のため、データ連携基盤と他システムの双方で連携したデータの交換履歴を記録できること	
アセットマネジメント（共通）	48	外部からアクセスするためのネットワークインタフェースをデータ連携基盤として具備すること 補足）スマートシティアセットと連携するためのネットワークは、解決する課題や、接続する機器の仕様により特性（通信距離、通信速度、消費電力等）が異なることを踏まえて、適切なネットワークインターフェースを具備すること	○
	49	データ連携基盤、他システムの双方の取り決めにより、データの利用権限を判断し、データのアクセス範囲を制御できること	○
	50	汎用的な片方向通信プロトコル（HTTP/HTTPS）によるデータアクセスが可能であること	
	51	汎用的な双方向通信プロトコル（MQTT、WebSocket等）によるスマートシティアセットのデータアクセスや、スマートシティアセットへのアクチュエーションが可能であること	
	52	データを記述するために用いる用語や語彙を統一することで、分野を超えたデータの理解を得るため、語彙レポジトリを作成すること	

① 相互運用性の確保（互換性）2. オープンAPI

小項目	求められる事項		重要
アセットマネジメント（システム管理）	53	【他システムと接続する場合】 データ連携基盤と連携する他システムの連携情報ライフサイクル（登録、参照、変更、削除）を管理できること 補足）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	○
	54	【他システムと接続する場合】 登録済の他システムに対して、他システムとの接続状態（稼働状況、機器情報等）を管理、公開できること	
アセットマネジメント（デバイス管理）	55	【デバイス（※）と接続する場合】 デバイス（※）情報（デバイスID、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 ※デバイスとは、IoTセンサやカメラ、モバイルデバイス及び車載コンピュータ等のデータの生成元となる機器を指す	○
	56	【デバイス（※）と接続する場合】 登録済のデバイス（※）に対して、デバイスの状態（稼働状況、機器情報等）を管理、公開できること ※デバイスとは、IoTセンサやカメラ、モバイルデバイス及び車載コンピュータ等のデータの生成元となる機器を指す	
	57	【デバイス（※）と接続する場合】 接続されているデバイス（※）の再起動やデバイスの動作変更等、デバイスの制御を行うためのコマンドを送信できること ※デバイスとは、IoTセンサやカメラ、モバイルデバイス及び車載コンピュータ等のデータの生成元となる機器を指す	○
	58	【デバイス（※）と接続する場合】 接続されているデバイス（※）の死活状況の監視またはデバイスから送信される障害のイベントの監視ができること ※デバイスとは、IoTセンサやカメラ、モバイルデバイス及び車載コンピュータ等のデータの生成元となる機器を指す	○
	59	【デバイス（※）と接続する場合】 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 ※デバイスとは、IoTセンサやカメラ、モバイルデバイス及び車載コンピュータ等のデータの生成元となる機器を指す	○

① 相互運用性の確保（互換性）3. データカタログサイト

小項目	求められる事項		重要
開発者ポータル・データカタログサイト	60	情報の見つけやすさを向上させ、公開されている様々なAPIへの接続をより容易とするために、APIに関するメタデータやデベロッパーサイト（開発者サイト）の情報を取りまとめ、カタログサイトの実装を行うこと	○
	61	カタログサイトにおいて、最低限以下のデータの公開をすること ＜最低限公開すべきメタデータ＞ ・APIエンドポイントまたは静的データの配布URL ・APIまたはデータの利用条件（例：利用規約、利用方法、契約の要否、利用制限、データ形式、データモデル解説）	○
	62	開発ポータルサイト内のカタログ機能に保管されたメタデータ（データカタログ）の登録・取得・検索処理を実行できること	
	63	各エリアのデベロッパーサイトの構築において、連携を前提とした規格や品質の均一化が図られていること	
	64	区域データの提供に関して、不当に差別的な取扱いをする条件その他の不当な条件を付していないこと	○

① 相互運用性の確保（互換性）4. データモデル

小項目	求められる事項		重要
データモデル	65	相互に利用可能なデータ流通のため、デジタル庁が提供する「自治体標準オープンデータセット」や政府相互運用性フレームワーク（GIF）における「地域サービス・データモデル」等を参照し、データモデルの標準化を図ること	○

② セキュリティ対策（安全性）1. システム要件

小項目	求められる事項		重要
システム要件（技術機能）	66	データ連携基盤に対し、権限設定を実施し、管理すること 例）管理者権限の割り当ての最小化アカウントや役割、権限等を整理した一覧表を作成・メンテナンスする等	
	67	データ連携基盤に対し、アクセス制御を実装、運用すること 例）IPアドレス制限、プロトコル・ポート制限等	
	68	データ連携基盤に対し、認証機能を実装すること 例）パスワード、ICカード、クライアント証明書、生体認証、多要素認証等	
	69	データ連携基盤が行う通信（データ連携基盤内の通信及びデータ連携基盤外との通信）及びデータ連携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 例）「CRYPTREC暗号リスト（電子政府推奨暗号リスト）」等で定義された十分な強度の暗号アルゴリズムを採用する等	○
	70	データ連携基盤のAPIにおけるセキュリティ（機密性・完全性・可用性・真正性）を確保すること 例） ・データ提供事業者及びサービス提供者を認証し、アクセス制御を実施する機能を実装する ・TLSを用いた認証や通信の暗号化を行う ・API 利用者ごとにアクセスする時間や回数、取得するデータに制限を設ける ・クロスドメインの通信を許可する際は、ドメインを超えたデータリソースへのデータ連携を制御する CORS（Cross Origin Resource Sharing）を設定する ・APIを通じてデータ連携を行う場合は、APIキーやアクセストークンを使用したOAUTH2.0、OpenIDによる認証などを行う　等	○
	71	日々進化するサイバー攻撃等の脅威に対して、これらの検知及び監視を行うサイバーセキュリティ対策を講ずること 例） ・IDSやIPS、ファイヤーウォールを設置し、通信の監視や検知、不正なアクセス（不正なIPアドレスやポート番号を持つパケット等からの通信・アクセス）を遮断すること、遮断する機能を提供すること ・WAFを設置し、アプリケーションレベルでの不正なコマンドを検知・遮断すること ・SOCによる監視やCSIRTが収集した脅威に関する情報を踏まえたリスクアセスメントを実施し、サイバーセキュリティ対策を講じること　等	○

② セキュリティ対策（安全性）1. システム要件

小項目	求められる事項		重要
システム要件（管理機能）	72	データ連携基盤に対し、脆弱性診断等を実施することで、企画・設計・開発工程における脆弱性を排除すること	○
	73	データ連携基盤に用いるソフトウェア及びハードウェアの脆弱性が顕在化しないよう、当該脆弱性に関する情報収集、当該脆弱性を克服するためのプログラム（いわゆるセキュリティパッチ）の適用等の必要な対策を継続的に講ずること	○
	74	データ連携基盤の運用管理端末へのセキュリティ対策を実施すること 例）ウイルス対策ソフトやOSの脆弱性への対応等	○
	75	データ連携基盤整備事業の実施主体が、サプライチェーン全体の脆弱性を適切に把握し、必要な対応をするため、サービス事業者やデータ提供者等の脆弱性への対応状況を「スマートシティセキュリティガイドライン（第2.0版）（総務省：令和３年６月）」で示すセキュリティチェックシート等で確認すること 例） ・脆弱性診断等を実施することで、サービスを提供するために使用するハードウェアやソフトウェアの脆弱性を把握すること ・脆弱性が発見された場合に直ちにセキュリティパッチなどをリリースできるサポート体制が整っていること　等	○
	76	データ連携基盤を介してデータを仲介・流通する場合及びデータ連携基盤の実施主体が重要なデータを取得する場合は、証跡確保のためのログを取得すること また、取得したログは、証拠保全のために一定期間保存されること （推奨）その他、事後的にインシデントが発覚し、調査するというケースを想定し、ログについても定期的にバックアップを取得すること 補足）サーバー等に対するアクセスログや操作ログ、IDSやIPS等における検知ログ、ファイアウォールにおける通信ログ等を取得する 例）データのアクセスログやシステムログ等を取得し保管することで、住民やデータ提供元からデータの利用状況に関する問い合わせ等があった際に、開示等ができる仕組みを用意する	○
	77	データの原本性保証（作成の段階からその内容が改ざんされてないことを保証すること）が必要と思われる重要データに対しては、デジタル電子署名、電子透かし、ストアドブロージャ等の方法でデータの原本性を確保すること	
	78	複数リージョン選択等により、障害発生時等におけるデータ連携基盤の可用性を確保すること	○
	79	定期的にバックアップを取得し、データ連携基盤の可用性を確保すること（地理的に別の場所にあるデータセンタ等に保管することを推奨）	○

② セキュリティ対策（安全性）2. ガバナンス要件

小項目	求められる事項		重要
セキュリティポリシー	80	対象事業を円滑かつ確実に実施するために必要な事項を定めた運用規程等において、サイバーセキュリティに関する事項を定めていること	○
	81	法令やガイドライン等との整合性を確認し、情報セキュリティ基本方針（目的や対象範囲等の基本的な事項や、セキュリティ担保のための取組方針が記載されるもの）及びセキュリティ対策基準（情報セキュリティ基本方針で定められた事項を実施するために、具体的な遵守事項等の判断基準等を定めるポリシー）を策定すること	○
	82	データ取扱基準を策定し、取り扱うデータをセキュリティやプライバシーの観点を踏まえてオープンデータ、個人情報、秘密情報等に分類するとともに、取り扱うデータの利用目的、内容、取得方法の他、データの所有に関する考え方や利用権限について提供元や利用者との関係性を示すこと	○
	83	策定したデータ取扱基準を契約・規約に反映すること	○
体制整備	84	サイバーセキュリティに関するリスクを経営リスクの一つとして位置付けており、国家戦略特別区域データ連携基盤整備事業に関わる、平時及び非常時の責任体制及び関係者の役割分担を明確にしていること	○
	85	データ連携基盤の構築・運用体制（委託先含む）の中に、サイバーセキュリティの確保に関する運用を的確に行うに足りる知識及び技能を有する者として、情報処理安全確保支援士（※）又はこれと同等以上の知識及び技能を有すると認められる者を配置し、その者による一定の関与が行われること ※情報処理安全確保支援士とは、情報処理の促進に関する法律第15条の登録を受けた情報処理安全確保支援士を指す	○
	86	サイバーセキュリティに関する計画の策定、実施、評価及びその改善を継続して行うことにより、継続的なサイバーセキュリティの水準の向上につながる仕組みを構築し、その有効化を図るため、次のいずれかを実施していること ・サイバーセキュリティの確保のための管理体制について、合理的かつ客観的な基準による公正な第三者認証を取得し、維持していること ・定期的に、サイバーセキュリティに関する外部監査等（当該監査を受けられないやむを得ない事情がある場合であって、独立性及び公平性を担保し、外部監査に準じた措置として組織内において講じているものを含む。）を実施するとともに、当該外部監査等の結果に基づき、サイバーセキュリティ対策の改善を行っていること	○
インシデント対応	87	サイバーセキュリティに関するインシデント（対象事業において収集及び整理をしている区域データの漏えい、滅失又は毀損の発生）に対し、サイバーセキュリティを維持するための責任、権限及び能力を備えた当該インシデントに対応する要員を配置し、対応方針を含む運用規程等を定めていること	○
	88	インシデント対応手順を策定し、インシデント対応に関与する関係主体やそれぞれの責任範囲の明確化、連絡体制や連絡先などの整備、対応における判断基準やインシデント対応フローを明確にすること （セキュリティインシデントの内容や被害状況について速やかに把握し、整理して報告できるようにするための手順やフォーマットを整備することを推奨）	○
	89	インシデント発生時にマルチステークホルダー間でのコミュニケーションが円滑に行われるように、各ステークホルダーのインシデント対応に係る窓口を整備し、ステークホルダー間で共有すること	○
	90	定期的にセキュリティインシデント対応訓練・演習を実施すること	○
事業継続計画	91	不正アクセス等のサイバー攻撃による障害等から迅速に復旧するための方法を含む適切な事業継続計画（障害やセキュリティ事故等が発生した際にどの機能を優先して保護するかといった判断基準や、スマートシティ事業継続のための役割分担、対応手順などを明確にした計画）を策定していること	○

② セキュリティ対策（安全性）2. ガバナンス要件

小項目	求められる事項		重要
リスク管理	92	リスクアセスメントを実施し、守るべき情報資産や機能（サービス）を特定し、それらの情報資産や機能に対して発生する可能性のある脅威とその発生確率、発生した場合の影響度を評価すること	○
	93	継続的なリスクアセスメントの実施とセキュリティに関するポリシーの見直しを実施すること	○
	94	セキュリティ対策への適切な投資を継続的にすること	○
	95	IaaS/PaaS/SaaS等のクラウドサービスにおいて、クラウドサービスの利用者(データ連携基盤提供事業)と提供事業者間の責任分界点を明確にすること	○
	96	適切なデータフローを設計し、システム全体としてセキュリティ・バイ・デザインに基づいたデータ保護を行うこと	○
	97	データ連携基盤上で取り扱うデータの種類を理解した上で、クラウドの設置場所及び設置環境において適用される関連法令や裁判管轄等を確認し、要求事項に対応できているかを確認すること	○
	98	サイバー攻撃に対するリスク分析を実施し、対象事業におけるリスクを認識した上で、対象事業の実施主体に加え、運営業務の外部委託先も含め、当該リスクに応じた技術的及び組織的なサイバーセキュリティ対策を実施すること	○
委託先管理	99	データ連携基盤のシステム構築・運用保守事業者に係る調達仕様書に、セキュリティポリシーを遵守するためのセキュリティ要件を設けること 例） ・調達仕様書に、提供する情報の目的外利用の禁止、情報セキュリティ管理体制の構築、情報セキュリティインシデントへの対処方法に関する事項を設ける ・調達仕様書に、データ連携基盤の運用に関する委託を実施する場合は、脆弱性対応のためのパッチ適用やソフトウェアアップデートなどの追加で必要となるセキュリティ対策に関する事項を設ける　等	○
	100	委託先や提携先の評価基準を策定し、外部委託先のセキュリティ管理体制やセキュリティに関する第三者認証の取得有無等、外部委託を実施する際に求めるべき内容や選定条件を明確にすること	○
	101	データ連携基盤の利用に関する規約等で責任範囲を明確化すること また、システムの責任分界点については、当該事業におけるシステム構成図を基に設定し、データの責任分界点については、データフロー図やデータ取扱基準で示されている取り扱うデータを基に、規約等の中で明確に記載されていること	○
	102	委託先のセキュリティ管理対策を評価すること（セキュリティチェックシートへの回答を求める又はISO/IEC 27001等のセキュリティに関する基準に適合していることの第三者認証の取得状況による評価を確認すること）	○
連携先管理	103	サービス提供事業者に対し、アクセス制御や認証機能等の「スマートシティセキュリティガイドライン（第2.0版）（総務省：令和３年６月）」で要求される事項の遵守を要求すること	○
	104	アセット等のデータ提供者に対し、認証機能や脆弱性情報の把握と対策等の「スマートシティセキュリティガイドライン（第2.0版）（総務省：令和３年６月）」に要求される事項の遵守を要求すること	○

③ プライバシー対策 1. 個人情報保護法令の確実な遵守

小項目	求められる事項		重要
個人情報保護法令の遵守	105	個人情報保護法令を確実に遵守すること ＜遵守事項の例＞　※以下の例に限定するものではない。 ・取り扱う個人情報の利用目的をできる限り特定し、その目的の範囲内で取り扱うこと（第17条第1項、第18条） ・利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合には、本人の同意を取得すること（第18条） ・個人情報の利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなった時は、当該個人データを遅滞なく消去するよう努めること（第22条） ・個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うこと（第25条） ・原則としてあらかじめ本人の同意を得ないで、個人データを第三者に提供しないこと（第27条、第28条） ・全ての保有個人データの利用目的を本人の知り得る状態に置くこと（第32条） ・本人による、訂正の求め、利用停止・消去の求めや、開示請求、苦情対応に対応する体制を整えること（第33条、第34条、第35条、第37条、第40条）	○

③ プライバシー対策 2. 法令遵守に加えて求められる事項

小項目	求められる事項		重要
個人情報保護法令に加えて、要求する事項	106	データ連携基盤整備事業の実施主体は、データ連携基盤を通じて提供されるデータの内容・適法性について一次的な責任を負うため、データ連携基盤に係るマルチステークホルダー間のデータの内容・適法性に関する責任分界点や、データ提供者やデータ利用者に対する個人情報保護法令等をはじめとした法令遵守に関する事項をデータ連携基盤の利用に関する規約等で明確にすること	○
	107	個人データの取扱いの全部又は一部を委託する場合は、個人情報保護法令に従い委託先に対する必要かつ適切な監督を行うことに加え、一定の資格（プライバシーマーク又はJISQ15001に準じる取扱いをすることが確認されること等）を有する事業者を委託先として選定すること また、再委託は原則禁止とし、再委託する場合であっても一定の資格（プライバシーマーク又はJISQ15001に準じる取扱いをすることが確認されること等）を有する事業者に限定すること（※ただし、適切な匿名化（匿名加工情報、統計情報等）を行った上でデータ連携基盤が個人データを提供する場合には、資格を要しないことも許容される）	○
	108	データ連携基盤を通じて、データ利用者へ個人情報の提供を行う場合には、個人情報保護法令に従い必要な場合にはあらかじめ本人の同意を取得することに加え、一定の資格（プライバシーマーク又はJISQ15001に準じる取り扱いをすることが確認されること等）を有する者等に限定して個人情報の提供を行うよう、データ連携基盤の利用に関する規約等に定めるなど必要な対応を行うこと また、データ連携基盤から個人情報の提供を受けたデータ利用者が再提供を行う場合にも、個人情報保護法令に従い必要な場合にはあらかじめ同意を取得することに加え、一定の資格（プライバシーマーク又はJISQ15001に準じる取り扱いをすることが確認されること等）を有する者に限定して再提供が行われるよう、データ連携基盤の利用に関する規約等に定めるなど必要な対応が行うこと	○
	109	個人情報よりも広義なパーソナルデータ（※）をプライバシー保護の対象とした上で、データ連携基盤のセキュリティポリシーやプライバシーポリシー等を策定すること ※個人情報に加え、個人情報との境界が曖昧なものを含み、個人の属性情報、移動・行動・購買履歴、ウェアラブル機器等から収集されたデータあるいは加工された情報等個人と関係性が見出される広範囲のデータ（個人情報保護法令にて定める個人情報・個人関連情報・仮名加工情報を指し、匿名加工情報は含まれない）	○
	110	万が一、個人情報が流出した場合に備えて、事後対応プロセス等に関する運用を明確にすること 補足）個人情報保護法令で定める、個人情報が流出した場合の個人情報保護委員会への報告や、本人への通知に加え、円滑に事後対応が行われるよう、データ連携基盤整備の実施主体の責任範囲や対応プロセス等を明確に定めること	○
	111	データ連携基盤整備の実施主体は、個人情報等の取扱いに関する透明性を確保するため、以下の体制を整備すること ・個人や事業者からの問い合わせ、開示請求、苦情・相談等を受け付けるための窓口を設け、それらがあった場合の対応プロセスを定めること ・本人による、訂正、第三者提供停止、利用停止・消去の求め等に広く対応する体制を整備すること	○
	112	データ連携基盤整備事業の実施主体は、個人情報保護法令に従い利用目的等を通知・公表等することに加え、個人情報が扱われる仕組みやデータ利用者の制限等のルールを公表すること 例）プライバシーポリシー、利用規約の公表、データフロー図 等	○

③ プライバシー対策 2. 法令遵守に加えて求められる事項

小項目	求められる事項		重要
個人情報保護法令に加えて、要求する事項	113	データ連携基盤整備事業の実施主体はパーソナルデータを取り扱う場合において、データ主体の判断で、個人のパーソナルデータの公開範囲を指定するための機能として、オプトイン/オプトアウトを管理できるほか、そのためにわかりやすいUI/UXを提供すること	○
	114	不要なパーソナルデータの取得・蓄積を避けるため、サービスの提供に当たって必要最小限のパーソナルデータを十分に吟味した上で、データを収集すること	○
	115	プライバシー情報等のプライバシーインパクトが懸念されるデータについては、原則として、データ分散方式とすること データの蓄積が必要な場合は、データの暗号化や不正アクセスの防止等、本認定基準に掲げるセキュリティ及びプライバシーに関する要求事項へ対応を行い、個人情報保護に万全を期すること	○
	116	データ連携基盤整備の実施主体自身が、パーソナルデータを取り扱う場合のリスク等を事前に評価するプライバシー影響評価（PIA）を実施すること	○