IFI Policy Recommendation

IFI Policy Recommendation No.20 March 2023

スマートシティデータガバナンスガイドライン

―スマートシティ実装におけるデータ利活用の考え方―

渡部俊也
東京大学未来ビジョン研究センター 教授/データガバナンス研究ユニット

美馬正司
株式会社日立コンサルティング ディレクター

東京大学未来ビジョン研究センター
Institute for Future Initiatives, The University of Tokyo

「スマートシティデータガバナンスガイドライン」取りまとめの狙い

本ガイドラインは、スマートシティにかかわる自治体や事業者に対してスマートシティのデータガバナンスに関する具体的提言として活用していただくことを目的に作成したものである。

スマートシティは IoT、AI 等の新しい技術を活用しつつ、都市や地域の抱える諸課題の解決を行うことを可能とする持続可能な都市や地域であり、Society 5.0 の先行的な実現の場として、昨今、多くの地域で取組が進められている。政府では 2021 年度より、デジタル技術の活用により地方を活性化し持続可能な経済社会を目指す「デジタル田園都市国家構想」を推進しており、今後、各地域におけるスマートシティへの取組はより活性化することが期待される。

一方、スマートシティの取組の中にはデータの利活用が先行することで市民の意識との乖離等が生じてしまい、その展開がとん挫するケースも見られる。テクノロジーの進展によって、スマートシティの可能性が広がっていることは間違いないが、テクノロジーを中心として進めること、あるいはテクノロジーを活かすためのデータ収集等が先行することは、結果的に市民や社会の反発を受ける可能性を有する。

そこで、スマートシティにおいて ICT やデータ活用を先行させるのではなく、「人間中心」の本来の価値を創出できるよう、スマートシティの推進におけるデータガバナンスの考え方を「スマートシティデータガバナンスガイドライン」（以下、本ガイドライン）としてとりまとめることとした。

データガバナンス とは、スマートシティにおけるデータの取扱いに関するルールを定め、これに基づき適切な利活用をコントロールする仕組みであり、それ自体が市民や社会の意識や認識との差異が生じないようにするプロセスを内包することで、適切なスマートシティの推進に貢献する。

本ガイドラインでは、人間（市民）を中心として位置づけ、その権利保護とサービス（便益）の創出等の両立を図るため、スマートシティにおけるデータの取扱いを適切にガバナンスする手順等について解説したものである。

なお本ガイドラインの策定は、未来ビジョン研究センターデータガバナンス研究ユニット https://ifi.u-tokyo.ac.jp/units/data-governance/ が参加する、日立東大ラボのハビタットプロジェクトの活動として行われた。策定に当たっては日立東大ラボ http://www.ht-lab.ducr.u-tokyo.ac.jp/research/ におけるスマートシティの取り組み、特に柏の葉スマートシティの取り組みについては UDCK（柏の葉アーバンデザインセンター）および三井不動産などの関係者から詳しくヒアリングおよび分析を行いガイドライン素案を作成したうえで 2023 年 3 月 20 日に実施された公開ワークショップ「スマートシティとデータガバナンス：ポリシーとガイドライン」において専門家パネル（Dr. Oscar Huerta（Policy Analyst on Urban Development and Governance Policy Analyst on Urban Development and Governance ,OECD）、原山優子（東京大学未来ビジョン研究センター客員研究員、東北大学名誉教授）、佐脇紀代志（内閣官房デジタル田園都市国家構想実現会議事務局審議官）、羽深宏樹（京都大学法学系特任教授）、田丸健三郎（日本マイクロソフト株式会社　業務執行役員 ナショナルテクノロジーオフィサー）、目黒麻生子（経済産業省商務情報政策局国際室　室長）、笹尾知世（東京大学大学院 新領域創成科学研究科ハビタット・イノベーション研究社会連携講座　特任助教））における議論を経て、最終のとりまとめを行ったものである。

目次

1. 本ガイドラインの趣旨

1.1. 背景と目的

社会のいたるところでデジタル化が進展し、メタバース等の仮想空間の開発も進められ、我が国が目指す未来社会 Society 5.0[1]への取組は着実に前進しているように見受けられる。スマートシティは IoT、AI 等の新しい技術を活用しつつ、マネジメント(計画、整備、管理・運営等)の高度化により、都市や地域の抱える諸課題の解決を行い、また新たな価値を創出し続ける、持続可能な都市や地域であり、Society 5.0 の先行的な実現の場として、昨今、多くの地域で取組が進められている。

また、政府では、デジタル技術の活用により、地域の個性を活かしながら、地方を活性化し、持続可能な経済社会を目指す「デジタル田園都市国家構想」を 2021 年度から推進している。デジタル田園都市国家構想推進交付金によって、今後、各地におけるスマートシティへの取組がより活性化することが想定される。

一方、スマートシティの取組の中にはデータの利活用が先行することで市民の意識との乖離等が生じてしまい、その展開がとん挫するケース（トロント等）も見られる。先進的な技術の適用においては、都市や地域を構成する人々や社会全体との意識や認識の間に差異が生じ、これが問題化することが少なくない。テクノロジーの進展によって、スマートシティの可能性が広がっていることは間違いないが、テクノロジーを中心として進めること、あるいはテクノロジーを活かすためのデータ収集等が先行することは、結果的に市民や社会の反発を受ける可能性を有する。

そこで、スマートシティにおいて ICT やデータ活用が先行するのではなく、「人間中心」で本来の価値を創出できるよう、スマートシティの推進におけるデータガバナンスの考え方を「スマートシティデータガバナンスガイドライン」(以下、本ガイドライン）としてとりまとめることとした。データガバナンス[2]とは、スマートシティにおけるデータの取扱いに関するルールを定め、これに基づき適切な利活用をコントロールする仕組みであり、それ自体が市民や社会の意識や認識との差異が生じないようにするプロセスを内包することで、適切なスマートシティの推進に貢献する。

本ガイドラインでは、人間（市民）を中心として位置づけ、その権利保護とサービス（便益）の創出等の両立を図るため、スマートシティにおけるデータの取扱いを適切にガバナンスする手順等について解説する。

1.2. 想定読者

本ガイドラインの想定読者は、地方公共団体やまちづくり推進団体等においてスマートシティに関わる担当者になる。

また、担当者のみならず、首長や責任者等、スマートシティの推進に関わる人、あるいはスマートシティ在住の市民等が読むことも想定する。

---

[1] サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society)。

[2] DAMA Data Management Body of Knowledge V2 (DMBOK2)によると、データガバナンスとは「データ資産の管理に対する権限とコントロール（計画、監視、執行）の実践」と定義される。

2.　スマートシティの考え方

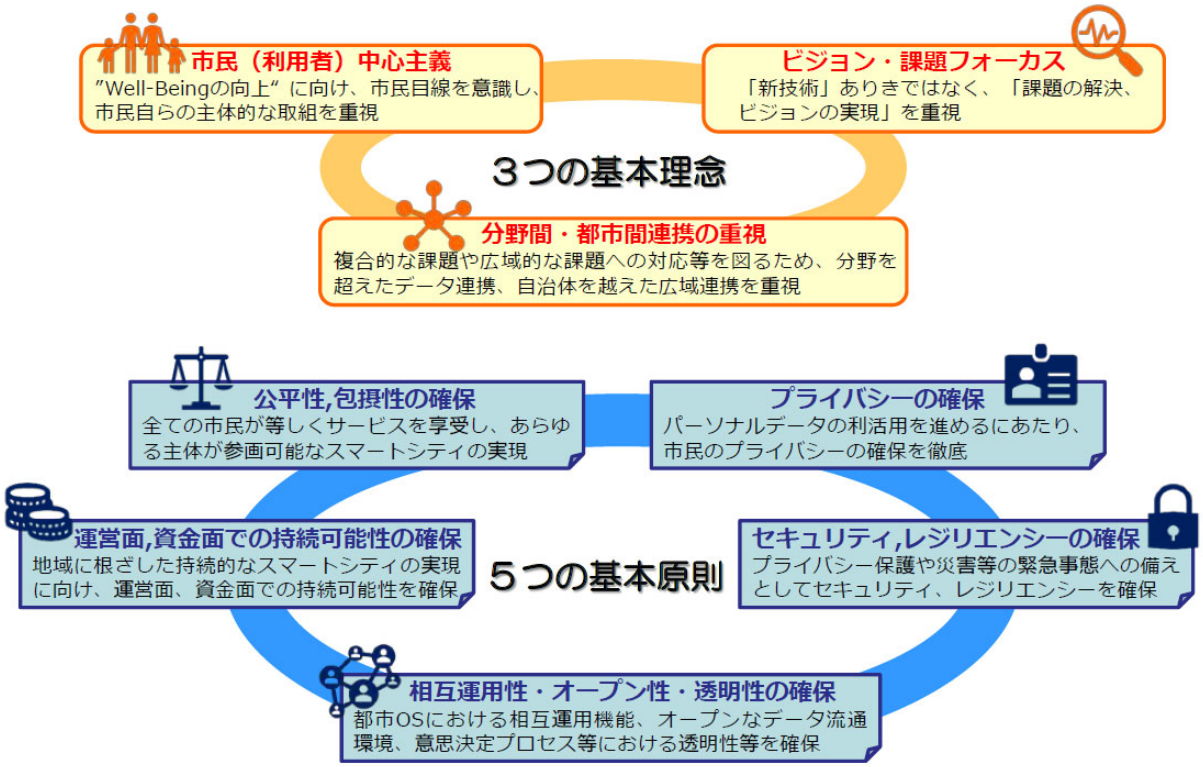
2.1.　スマートシティとは

スマートシティについては、様々な捉え方が存在するが、本ガイドラインでは、内閣府の「スマートシティガイドブック」における定義を参照する。「スマートシティガイドブック」では、スマートシティを以下の 3 つの項目で定義している。

- ICT 等の新技術や官民各種のデータを活用した市民一人一人に寄り添ったサービスの提供や、各種分野におけるマネジメント(計画、整備、管理・運営等)の高度化等により［手段］
- 都市や地域が抱える諸課題の解決を行い、また新たな価値を創出し続ける［動作］
- 持続可能な都市や地域であり、Society 5.0 の先行的な実現の場［状態］

また、上記の 3 つの項目に加えて、3 つの基本理念、5 つの基本原則に基づいてスマートシティを進めることを期待している。特に 5 つの基本原則はデータガバナンスにも大きく関わる考え方であり、スマートシティに取組む地域では、十分に検討し、考慮した推進が求められる。

図 2-1　スマートシティの基本理念と基本原則



出典：内閣府・総務省・経済産業省・国土交通省スマートシティ官民連携プラットフォーム事務局「スマートシティガイドブック」

参照先

スマートシティ - Society 5.0 - 科学技術政策 - 内閣府（cao.go.jp）

2.2. スマートシティの捉え方

内閣府の「スマートシティガイドブック」を見ると、大きな構想や計画、全体像があり、地域横断的な組織体制があるものがスマートシティだと考えられる傾向もあるかも知れないが、広い意味では、ICT 等を活用して市民の便益の向上を図る取組全体をスマートシティとして捉えることができる。

つまり、「スマートシティ」という名を冠していなくても、（パーソナル）データを活用して地域課題を解決するような政策や取組は、ある意味スマートシティに関する取組であり、相応のデータガバナンスが求められる。

もちろん、同ガイドブックの基本理念の最初に記述されているように、「市民（利用者）中心主義」ということがスマートシティの前提として最重要であることは揺らぎがない。本ガイドラインでも、「人間中心」を一番の基盤としてスマートシティのデータガバナンスについて解説する。

> 「人間中心」
> スマートシティの目的はそこで生活する人間の便益の向上であり、ICT やデータの活用が目的化するような取組であってはならない。したがって、市民等の便益を高めることを志向するだけでなく、プライバシーや尊厳を保護することを前提として進められることが不可欠となる。

2.3. スマートシティの推進組織

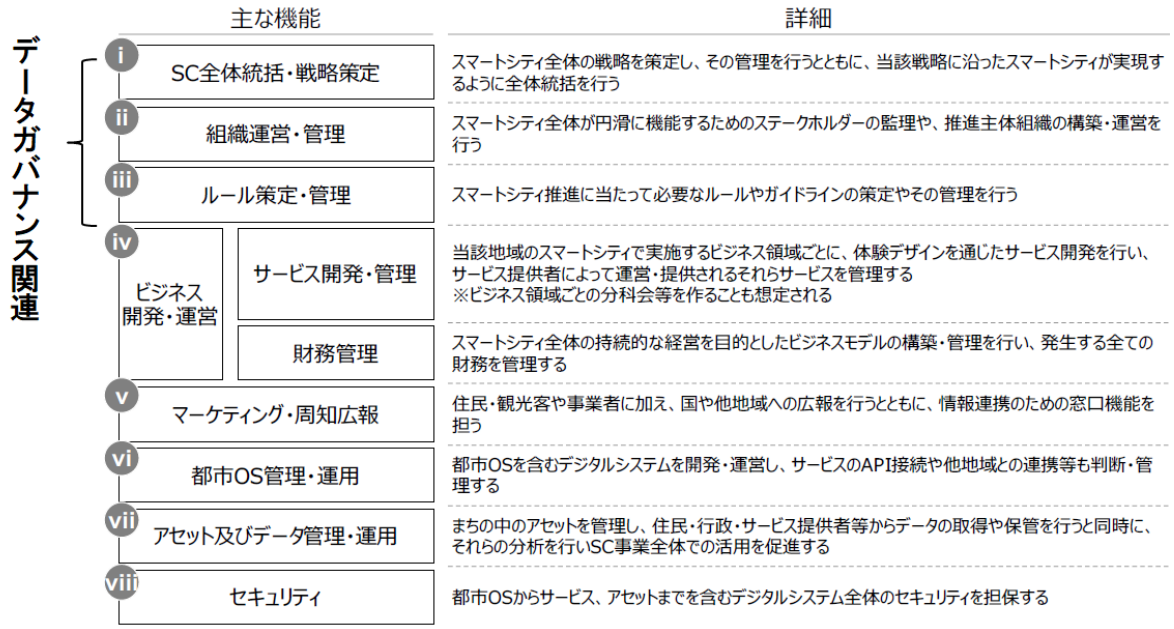
スマートシティの推進においては、多様なステークホルダーが関わり、それぞれの意見を調整し、同じ方向性に向けて推進するための推進組織が必要になる。産、官、学、市民等、多様な主体が関わる形で構成され、中立性を担保するとともに、スマートシティの推進に必要な機能を提供することが求められる。具体的には、スマートシティ戦略の策定やサービスの開発、広報、都市 OS[3]の運用、ステークホルダー間の調整等、機能は多岐に渡り、ルールの策定・管理等のデータガバナンスも機能の一つとなる。本ガイドラインでは、スマートシティ推進組織が中心となり取組むことを前提として、データガバナンスの考え方やプロセスについて記述している。

もちろん、前述したようにスマートシティとは言及しない、地方公共団体のデジタル政策の一つとしての取組等も存在する。実際には、これらもスマートシティの一環として捉えることができ、このような場合には、各政策の推進主体（例えば地方公共団体）がデータガバナンスについても推進することが不可欠となる。

---

[3] スマートシティ実現のために、スマートシティを実現しようとする地域が共通的に活用する機能が集約され、スマートシティで導入する様々な分野のサービスの導入を容易にさせることを実現する IT システムの総称。

図 2-2　スマートシティの推進組織の機能の例



出典：戦略的イノベーション創造プログラム（ＳＩＰ）第２期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業「スマートシティリファレンスアーキテクチャの使い方」に加筆

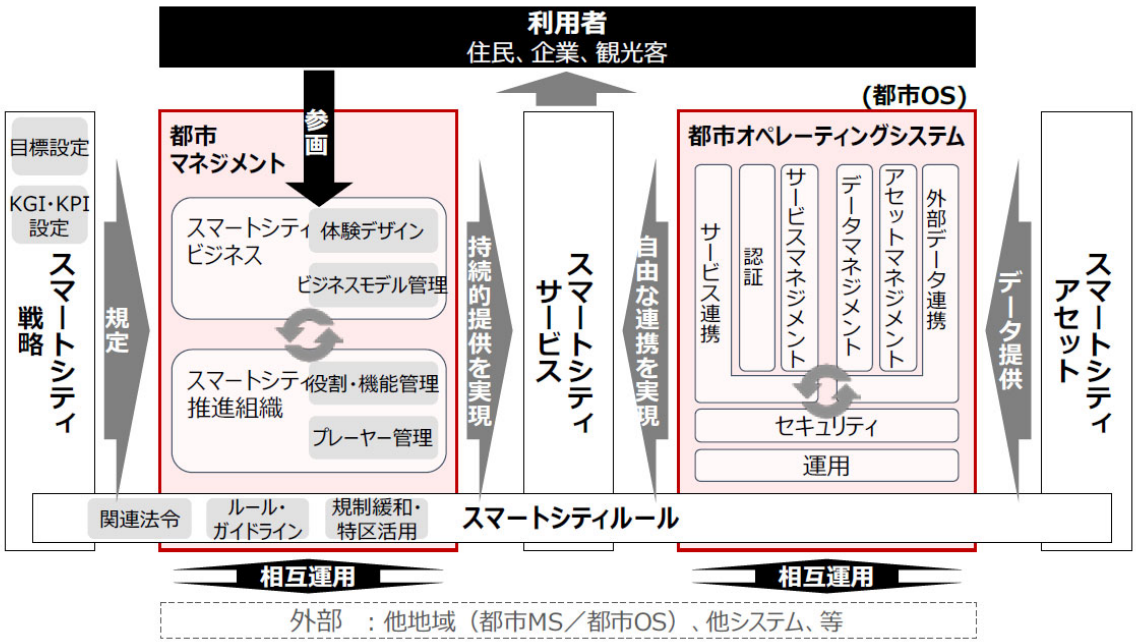
3. データガバナンスの考え方

3.1. サービスが最初

本ガイドラインはデータガバナンスを主題としているが、スマートシティを考える上で中心となるのは、前述したように人間であり、そのサービス（便益）を最初に据えることが不可欠である。内閣府が取りまとめた「スマートシティリファレンスアーキテクチャ　ホワイトペーパー」にもあるように（図 3-1）、（スマートシティ）サービスが人間、つまり利用者である市民、企業、観光客等に提供され、都市のマネジメント（事業、組織等）や都市 OS を含む ICT の基盤がこれを支える形になる。スマートシティのルールはサービス、都市のマネジメントや ICT を更に下支えするものであり、このような関係性、つまりアーキテクチャ[4]（レイヤー構造）を考慮した検討が必要となる。

本ガイドラインではデータガバナンスについて示すものであるが、スマートシティに取組む各地域では、まずはサービス（便益）を起点としてスマートシティを検討し、その内容に基づきデータガバナンスを検討するという流れが必然である。また、このようなスマートシティを構成する要素を明らかにしておくこともデータガバナンスを検討する上で必要であり、データガバナンスを検討する前提として、スマートシティのアーキテクチャ（レイヤー構造）を整理しておくことが望まれる。

図 3-1　スマートシティのアーキテクチャ（レイヤー構造）



出典：戦略的イノベーション創造プログラム（ＳＩＰ）第 2 期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業「スマートシティリファレンスアーキテクチャのつかい方」

参照先

戦略的イノベーション創造プログラム / アーキテクチャ構築及び実証研究の成果公表　科学技術政

---

[4] （一般論として）特定の目的を実現するための、「システムとその外界との関係」及び「システムを構成する要素間の関係性」を記述したもの。

策 - 内閣府 (cao.go.jp)

サービス（便益）は目指すべきスマートシティの目的とも合致するものであり、一義的には「市民一人一人に寄り添ったサービスの提供を通じて Well-Being の向上」に結びつくことが求められる。しかしながら、地域が置かれている状況、社会課題、市民の意識によってもスマートシティで目指す目的は異なると考えられる。なお、内閣府の「スマートシティガイドブック」では、以下に示すようなスマートシティのサービス（便益）が例示されている。

表 3-1　スマートシティのサービス（便益）の例

①安全で質の高い市民生活・都市活動の実現　【社会】
✓　行政手続き、購買、移動、医療、健康、観光などあらゆる都市サービスが効率化されるとともに個々人の属性や嗜好に対応したものとなることで、全ての市民が等しく便利で豊かな生活を享受できる、社会的包摂（インクルージョン）を実現する効果
✓　災害発生時、感染症拡大時などの非常事態においてもデータに基づく即応的な対応が講じられたり、新しい日常におけるリモート・リアルの新しい暮らし・働きの場が提供されたりするなど、安全、安心な生活を享受できる効果 等
②持続的かつ創造的な都市経営・都市経済の実現　【経済】
✓　各種データや新技術を駆使した様々な市民、事業者向けサービスが続々と創出される環境が生まれ、地域経済が活性化する効果
✓　安全、便利で快適な街なか等を市民や来街者が行き交い、消費やサービスの購入等により地域経済が循環するとともに、交流を通じて様々なイノベーションが生まれる効果
✓　企業や行政におけるシステムの効率化等が図られ、生産性の向上につながる効果 等
③環境負荷の低い都市・地域の実現　【環境】
✓　業務活動、日常生活や移動行動などあらゆる場面で、現実のヒトやモノの動きに対応した形でエネルギー・資源利用が最適化され、脱炭素社会の実現につながる効果 等

出典：内閣府・総務省・経済産業省・国土交通省スマートシティ官民連携プラットフォーム事務局「スマートシティガイドブック」

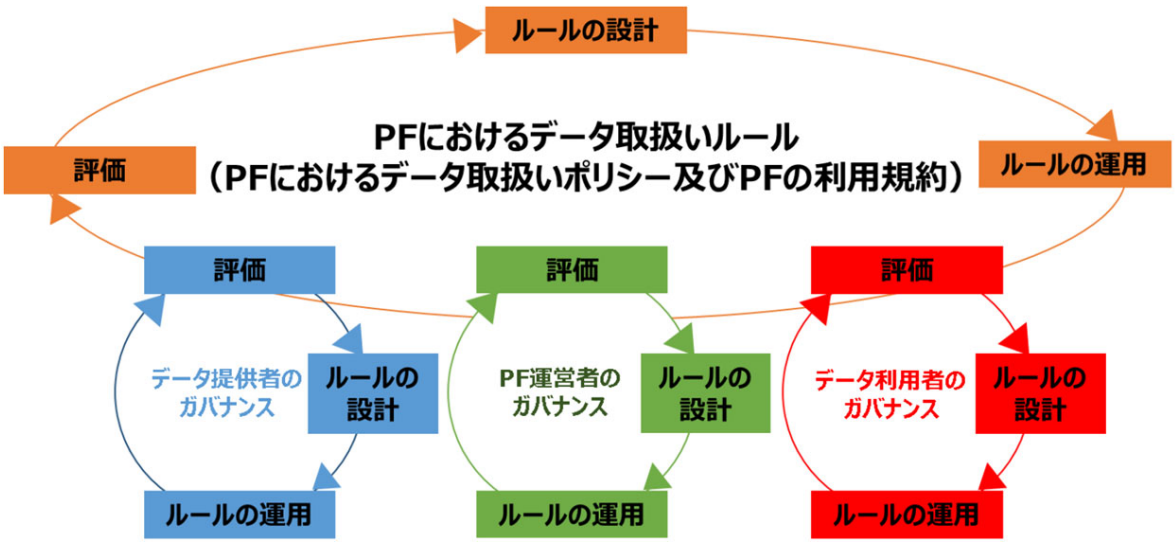
3.2.　データを起点とした捉え方

サービス（便益）を最初に考えることが不可欠ではあるものの、スマートシティの適切な実現、運用を考慮し、個人のプライバシーや尊厳に配慮する上では、データを起点として捉えることが望ましい。人間の体に例えると、サービスとは人間の活動そのものであるが、データの収集、流通、分析、利用という一連の流れ（プロセス）がスマートシティという「体」の血管としての役割を果たしており、その取扱い如何がスマートシティを構成する個人（細胞）のプライバシーや尊厳（機能）を大きく損なう可能性があるためである。繰り返しになるが、データのライフサイクル（情報の処理）がサービスを創生する上で不可欠な要素であり、これを適切にコントロールすることが、結果的に適切なサービス（便益）につながる。

スマートシティでは、市民や地域の便益のために、様々なデータが流通し、利活用される可能性がある。データには提供者と利用者がおり、これを仲介しデータを流通させるプラットフォーマー（プラットフォーム運営者）等も想定される。このようなステークホルダーを通じて、データが適切に取り扱われることがスマートシティでは重要であり、一定のルールが求められる。ルールを定め、これを運用し、その適切性等を評価するという一連のマネジメントサイクルを回すことで、ガバナンスが形成される。

図 3-2 に示すのは、デジタル庁、内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」に示されたプラットフォーム（以下、PF）におけるデータの取扱いルールのイメージであるが、スマートシティのデータガバナンスにおける基本構造もこのような構成になると考えられる。すなわち、スマートシティの PF になる都市 OS や都市のマネジメントに関するルールがあり、その上で、データのライフサイクルに関わる個々のステークホルダーのコントロールを行うためのルールも必要となる。

図 3-2　データを起点としたガバナンス



出典：デジタル庁、内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」

参照先

プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0 (digital.go.jp)

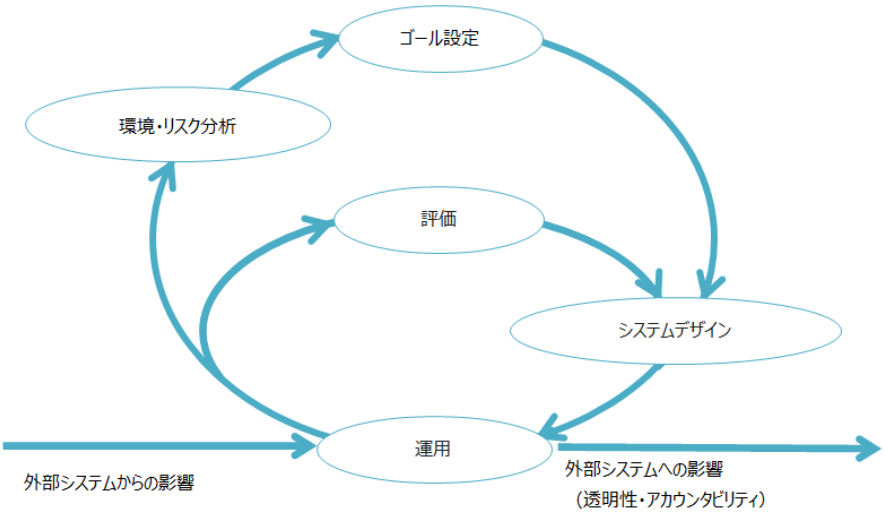
3.3.　アジャイル・ガバナンス

スマートシティで取り組まれるサービス（便益）は交通、健康・医療、防災、教育、環境・エネルギー、観光・地域活性化、インフラ維持管理、物流等、多岐に渡るが、多くは全方位的に進められるのではなく、地域のニーズに即してサービスの選択と集中が行われることが多い。また、そのような取組においても計画どおりに進まないこともあり、事業を見直すことも想定される。スマートシティはまちをより良い環境にするためのトライ・アンド・エラーであり、データガバナンスにおいても同様の考え方が求められる。つまり、最初から完璧なルールを形成するのではなく、スマートシティの取組の中でルールを運用し、評価し、見直すというループを迅速に回す「アジャイル・ガバナンス」が重要になる。

「アジャイル・ガバナンス」とは、経済産業省「GOVERNANCE INNOVATION ver2.0：アジャイル・ガバナンスのデザインと実装に向けて」において示された「政府、企業、個人・コミュニティといった様々なステークホルダーが、自らの置かれた社会的状況を継続的に分析し、目指すゴールを設定した上で、それを実現するためのシステムや法規制、市場、インフラといった様々なガバナンスシステムをデザインし、その結果を対話に基づき継続的に評価し改善していくモデル」である。スマートシティを含むSociety 5.0では、常に変化する環境とゴールを踏まえ、最適な解決策を見直し続けることが必要である。そのためには、ゴールや手段が予め設定されている固定的なガバナンスモデルを適用することは妥当ではない。「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」「改善」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていくガバナンスモデルが必要とされる。

スマートシティのデータガバナンスにおいても、「アジャイル・ガバナンス」の考え方に則り、サービス（便益）起点ではあるものの、当初の計画に固定することなく、ルールの設計、運用、評価というループを常に回していくことが求められる。

図3-3　アジャイル・ガバナンス



出典：経済産業省「GOVERNANCE INNOVATION ver2.0：アジャイル・ガバナンスのデザインと実装に向けて」

参照先

「GOVERNANCE INNOVATION Ver.2: アジャイル・ガバナンスのデザインと実装に向けて」報告書を取りまとめました　（METI/経済産業省）

3.4.　人間中心のガバナンス

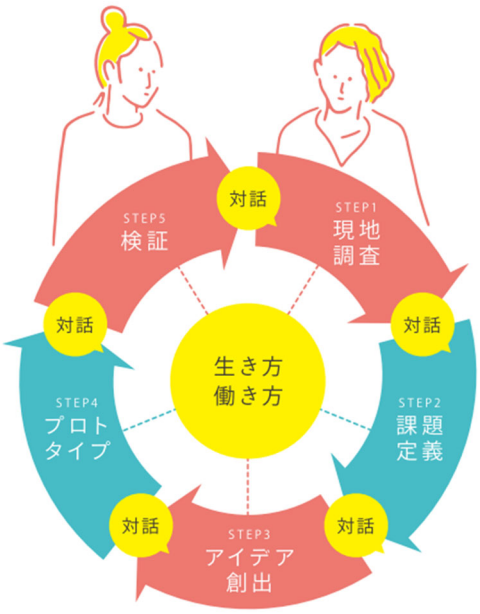
人間中心で考える場合、スマートシティにおけるデータガバナンスの在り方も一様ではない。つまり、地域によって市民等のステークホルダーの価値観は異なり、それに応じて求められるルール等も変化する。例えば、高齢化が進み、外出中に行方不明になったり、ひとり歩き中の事故が起きたりする心配がある地域では、見守りのために路上カメラを設置することが受け入れられるかもしれないが、人口の移動の多い都心ではプライバシーを重視するためにこのような見守りカメラに市民が反対することも考えられる。このようにデータガバナンスの在り方は地域によって異なる。

また、人間中心でデータガバナンスを考えるにあたり、スマートシティで生活する市民等の参画は不可欠であり、実現するサービス（便益）によっては、市民だけでなく、関係団体、事業者等、多様なステークホルダーを巻き込み、地方公共団体等の推進主体が一方的にルールを整備するような形にはなってはいけない。

市民等を巻き込む手法としてリビングラボが挙げられる。リビングラボとは、オープンイノベーションを生活の場で実践するための手法であり、「社会の複雑な課題を住民と企業等の提供者が一緒になって生活環境で実験し、この競争と実装と評価と改善から新しいサービスや商品をうみだす一連の活動」である。実際、大阪市、柏市、鎌倉市、横浜市等、スマートシティに取組む複数の地域でリビングラボの手法は実践されている。スマートシティにおいてもその活用は想定され、リビングラボの中でルール等、データガバナンスについて検討することも想定される。

スマートシティは、都市という物理的に閉じた空間でサービス（便益）を検討するため、全国的な政策等とは異なり、ステークホルダーがフェイス・トゥ・フェイス（感染症予防等への配慮は必要）で集まり、より緊密な議論のもと、推進できるというメリットがある。データガバナンスの検討においてもこのメリットを活かすことが不可欠である。

図 3-4　リビングラボの流れ



出典：経済産業省「リビングラボ導入ガイドブック」

参照先
リビングラボ導入ガイドブック

3.5. トラストの考え方

スマートシティでは、多様なステークホルダーが関わるため、ステークホルダー間のデータ連携を適切に行えるように「トラスト[5]」の考え方を活用することが重要になる。つまり、市民等のステークホルダーが他のすべてのステークホルダーを理解し、その安全性や信頼性等を確認することは不可能である、という視点に立ち、スマートシティの推進組織等がこれを代行すること（スマートシティ全体としての信頼性を担保すること）で、個々のステークホルダーの負荷の軽減を図ることが望まれる。例えば、医療データ等を活用し、民間企業が提供する PHR サービスを用いて市民の健康増進を図ることをスマートシティとして推進する場合、市民が各 PHR サービスの安全性や信頼性等を理解することは難しい。したがって、スマートシティの推進組織等が PHR サービスを評価し、選定するような仕組みで「トラスト」を醸成し、市民が安心して円滑に PHR サービスを利用できるようにすることが想定される。これは医療データの提供元となる地方公共団体や医療機関等との関係性でも必要と考えられ、このようなサービス全体の信頼性を担保するためにルールや技術的な対策も含めた設計が必要となる。

また、「トラスト」は、すべてがオンラインで完結するサイバー空間の中でより重要になってきている概念であるが、スマートシティは地域という物理的な結びつきの上に成り立っていることにも留意が必要である。つまり、サイバー空間だけで設計されたサービスで求められるような高い「トラスト」のレベル（例えば、本人確認が困難であるため電子証明書を用いた多要素認証を行う等）よりも、スマートシティでは実社会における結びつきとの組み合わせを前提に検討することで、より適切で簡易な「トラスト」を創出することも可能と考えられる。例えば、「通いの場」のように、物理的あるいはオンラインにおいてでも対面で集まり、市民が一緒に健康増進活動を行うような場が存在し、前述したような PHR サービスと連携した取組みを行うことで、より強固な「トラスト」が形成される。

データ連携に参加する民間企業が市民からの「トラスト」を獲得するためには、個人情報の取扱いに関する第三者認定を受けることも考えられる。プライバシーマーク[6]は、その代表的なものであり、17,000 を超える数の事業者が取得している。認定の内容は基本的には個人情報保護法遵守のマネジメントシステムであり、小規模な民間企業でも取得することができる。データ連携の中でも取得した情報をさらに提供するようなハブ的な役割を果たすステークホルダーについては、日本 IT 団体連盟の情報銀行認定[7]を受けることも考えられる。情報銀行は、本人から個人情報を預かり、本人に合った提供先に必要な情報を提供する仕組みであり、日本 IT 団体連盟の情報銀行認定は、その仕組みとしての安全性を認証するものである。認定基準は、総務省・経産省の「情報信託機能の認定スキームの在り方に関する検討会」が策定した「情報信託機能の認定に係る指針」に準拠したものとなっている。法人に対する認定のみならず、事業部門に対する認定も可能なため、例えば自治体の都市 OS も認定を取得することができる。

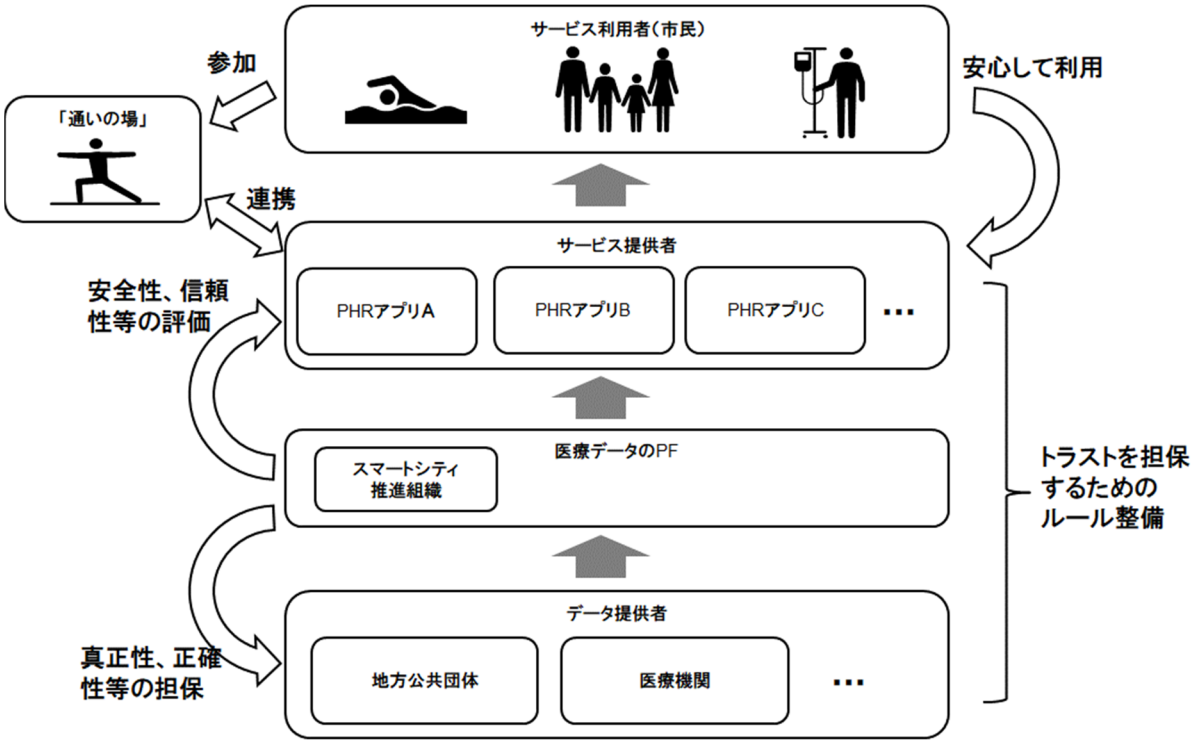
---

5 「信頼」と訳されるが、Society 5.0 を目指す中で、「トラスト」は様々な分野、対象、目的に応じて異なる意味合いを持つ概念であることがデジタル庁「トラストを確保した DX 推進サブワーキンググループ報告書」で確認されている。同ワーキンググループでは、真正性（作成者、発信元又は存在時刻が記載どおりであること）や非改ざん性のオンラインでの確保のみならず、データの真実性（データの内容が正しいこと、虚偽ではないこと等を含む。）の確保、情報の発信者（ソシキ、ヒト、モノ）の確からしさ、長期にわたる経時的トラスト（longitudinal trust）の確保も含まれるべきであるという意見があがっている。

6 https://privacymark.jp/

7 https://tpdms.jp/

図 3-5　トラストのイメージ



3. 6.　DFFT

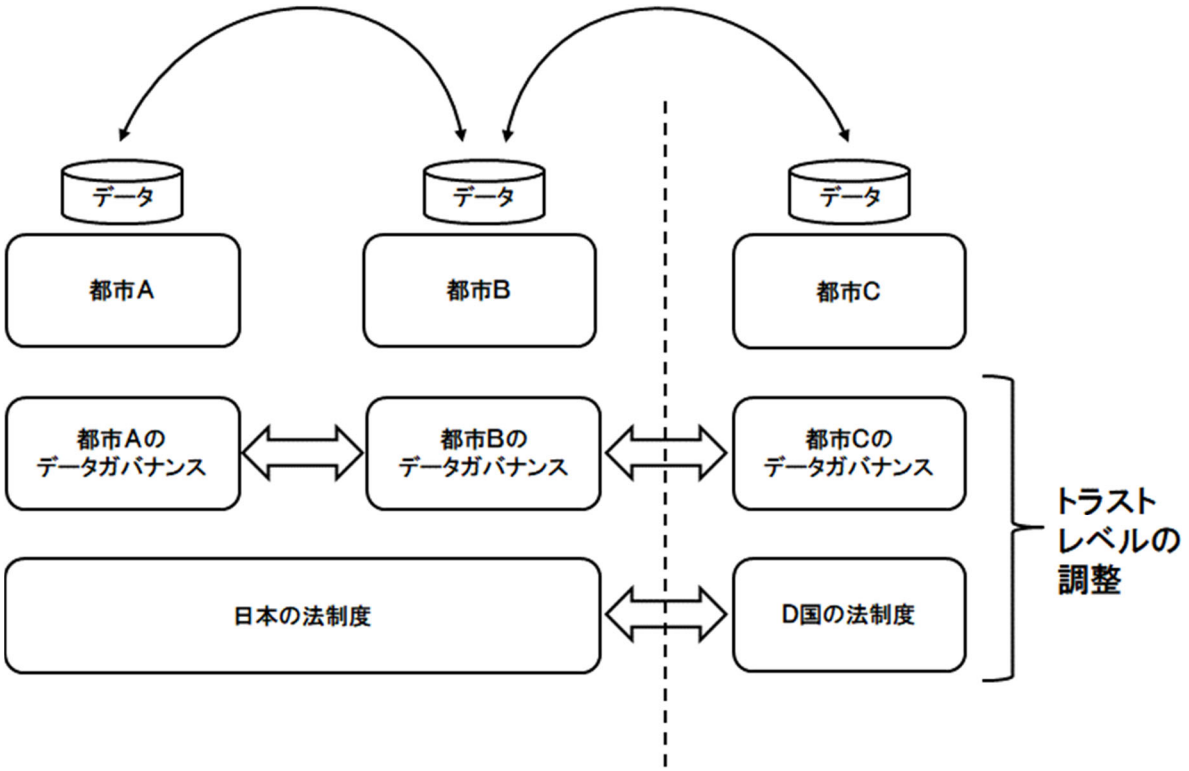
DFFT は Data Free Flow with Trust の略であり、2019 年 1 月に行われた世界経済フォーラム年次総会（ダボス会議）にて「自由で公正かつ安全のための、信頼ある自由なデータ流通（DFFT : Data Free Flow with Trust）」の概念を日本政府が提唱した。

スマートシティにおいても、他の都市とのデータ連携、あるいは外国人等、海外からの観光客や居住者の流入において他の国とのデータ連携が生じる可能性がある。その際、データ連携が円滑にできることを目指したものが DFFT であり、前述したように、ここにおいても「トラスト」がデータ連携の鍵となる。

例えば、国を跨ってパーソナルデータを移転する際、個人の同意を得ることが求められる場合が多いが、加えて移転先において適切な管理が期待できるか等、相応の確認が必要となる。DFFT は、データガバナンスを含むトラストのレベル（法制度を含むルール等のデータガバナンスのレベル）を事前に調整しておくことで、円滑なデータ連携を実現するという考え方になる。

地域や国を跨ったデータ連携は、スマートシティを進める上で必要となることが想定され、特に国を跨ったところにおいては、国レベルでの調整が不可欠であり、国の政策動向等を考慮した対応が求められる。例えば、EU 域内の個人情報について、十分性認定に基づいて移転を受ける個人情報取扱事業者は、個人情報保護委員会「個人情報の保護に関する法律に係る EU 及び英国域内から十分性認定により移転を受けた個人データの取扱い関する補完的ルール」を遵守することが必要となる。

図 3-6　DFFT のイメージ



4.　データガバナンスのプロセス

4. 1.　スマートシティのプロセスとデータガバナンス

内閣府の「スマートシティガイドブック」では、スマートシティの推進プロセスを以下に示す 5 段階で整理している。データガバナンスは、計画（戦略）作成段階から実証・実装段階、定着・発展段階まで継続的に実施されるものである。

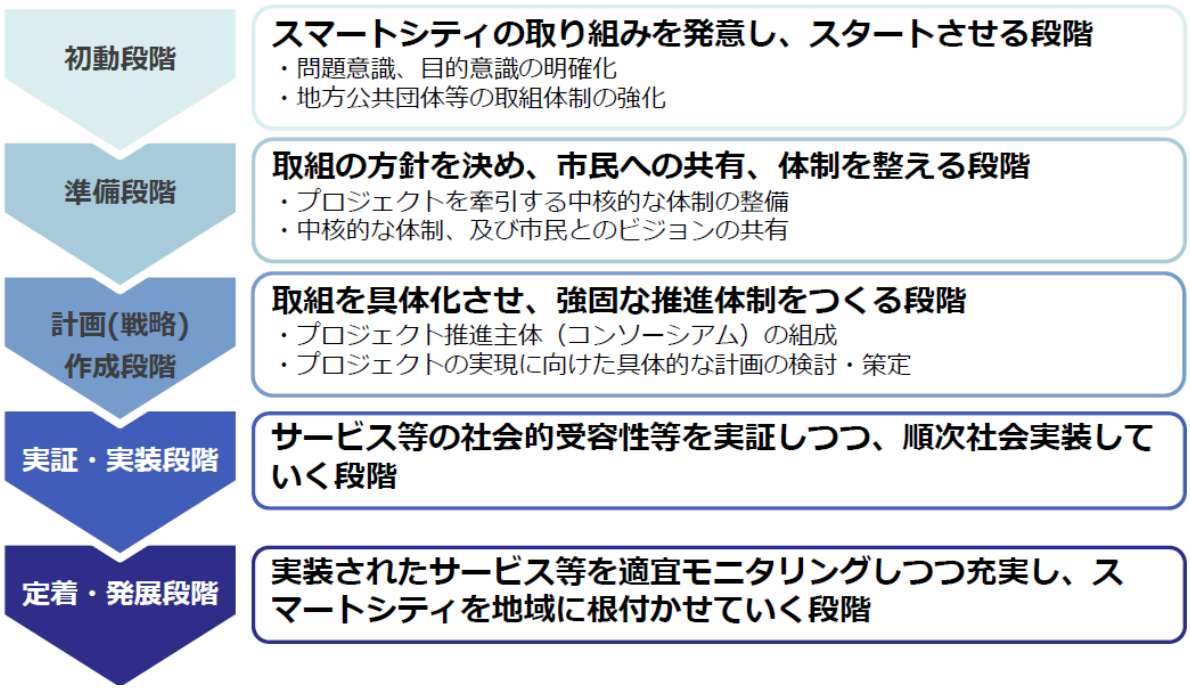
データガバナンスはスマートシティのプロジェクトの企画段階からバイ・デザインで検討されるべきであり、便益（サービス）の内容の具体的な計画の検討と併行して、どのようなルールが必要で、どのようにガバナンスするかということが検討される必要がある。

実証・実装段階では、検討したデータガバナンスの仕組み自体も便益（サービス）と合わせて検証し、そのフィージビリティ等を確認することが不可欠である。

定着・発展段階では、データガバナンスの仕組みと合わせて便益（サービス）が実装されることになるが、便益（サービス）だけでなく、データガバナンスの仕組みも定期的に評価して、改善されなければならない。

スマートシティとしてのプロセスの詳細については、内閣府の「スマートシティガイドブック」を参照すること。

図 4-1　スマートシティの進め方



出典：内閣府・総務省・経済産業省・国土交通省スマートシティ官民連携プラットフォーム事務局「スマートシティガイドブック」

参照先

スマートシティ - Society 5.0 - 科学技術政策 - 内閣府（cao.go.jp）

4.2. データガバナンスのプロセス

データガバナンスに関わる要素を切り出して整理すると、以下のプロセスになる。

まず、市民等の便益（サービス）を起点とした事業概要を整理する。これは前述したスマートシティの推進プロセスの計画（戦略）作成段階に行われるものと同じものであり、データガバナンスのために個別に実施するものではない。

次に事業分野に関係する関係法令等を整理する。個人情報保護法等、分野横断的に関係する法令と各事業分野に関係する法令が存在する。また、ソフトロー[8]と呼ばれる国や業界団体等が整備するガイドライン等も考慮する。

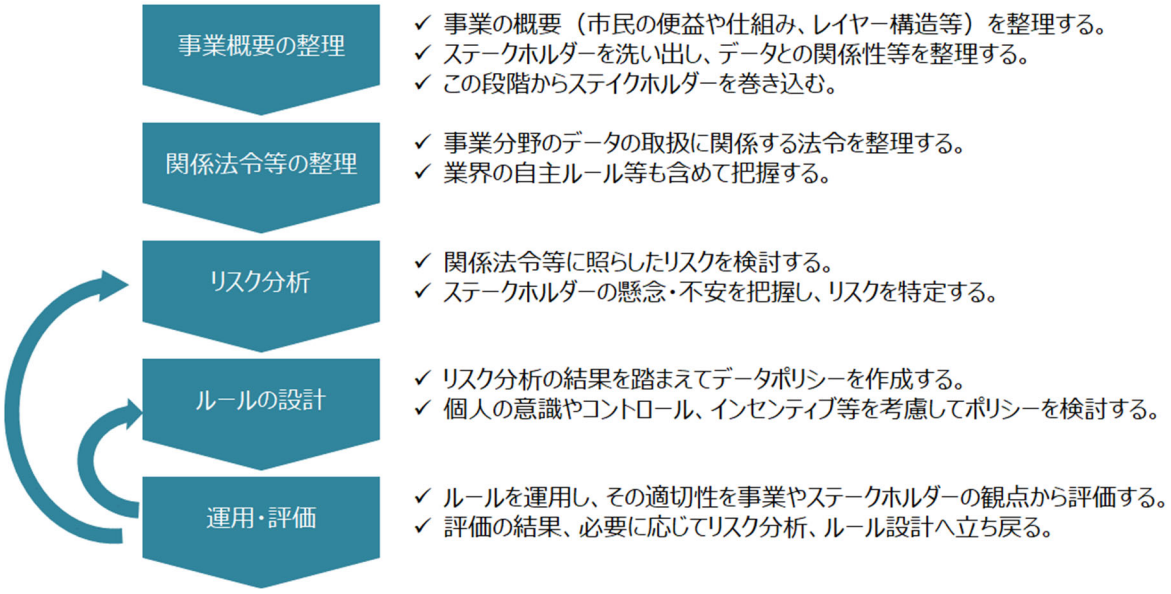
そして、事業概要や関係法令等を踏まえて、リスク分析を行う。リスク分析は関係法令等に照らして検討するだけでなく、多様なステークホルダーの視点も踏まえた検討が不可欠である。

リスク分析の結果を踏まえ、データポリシーの作成等のルールの設計を行う。ただし、リスクの低減は必要ではあるものの、過度なルールによってスマートシティに期待されるサービス（便益）が阻害されないように考慮することも重要である。

最後にルールを実際に運用し、評価するが、前述したスマートシティのプロセスでも述べたように定期的に評価して改善することが不可欠であり、評価の結果、リスク分析やルール設計に立ち戻ることが必要である。

このプロセス自体はスマートシティの推進主体が行う活動になるが、前述したように市民を含めた多様なステークホルダーを巻き込む形で推進することが望ましい。

図 4-2　データガバナンスのプロセス

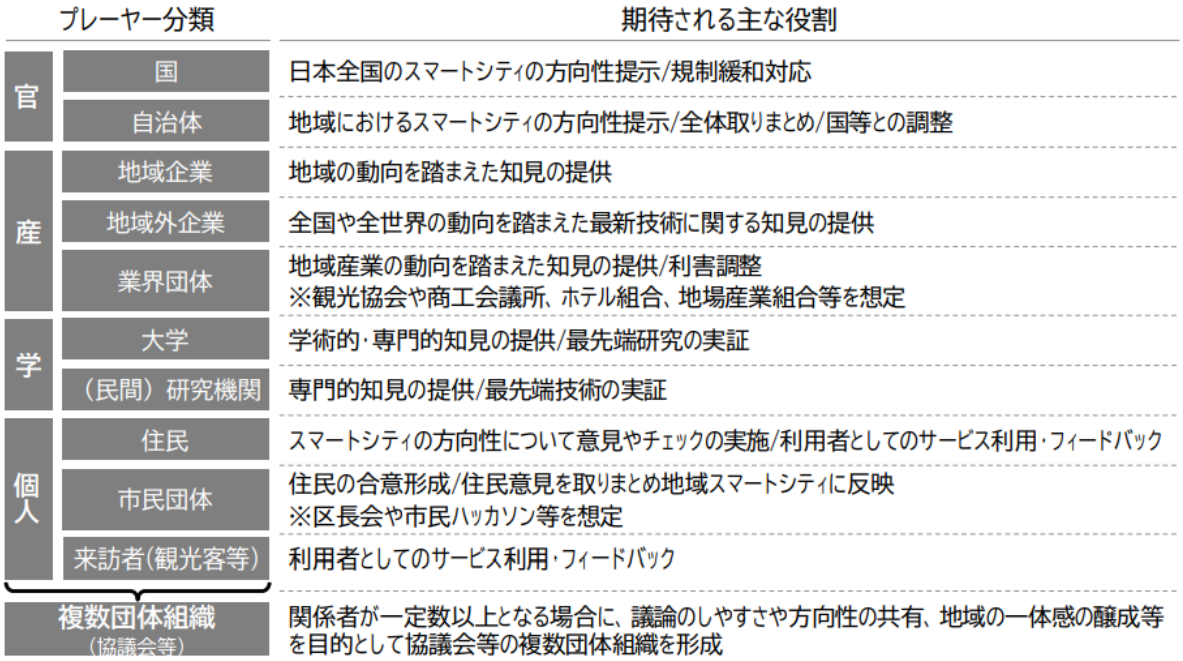


[8] 民間で自主的に定められているガイドラインのほか、行政府が示す法解釈等も含む広い概念。

4.3.　ステークホルダーの巻き込み

スマートシティにおいては、様々なステークホルダーが存在するが、データガバナンスが有効に機能するためには、データガバナンスのプロセス自体に重要なステークホルダーを巻き込むことが不可欠である。一方、すべてのステークホルダーを等しく巻き込むことは現実的ではない。したがって、個別の事業概要の整理においてステークホルダー分析を行うことが想定される。

図 4-3　スマートシティに関するステークホルダー



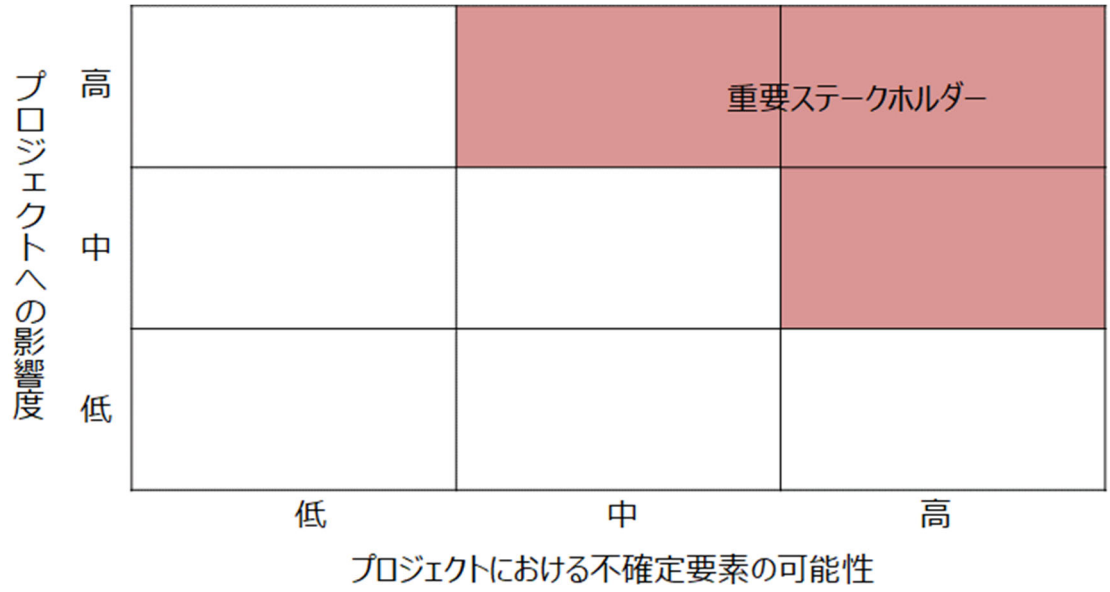
出典：戦略的イノベーション創造プログラム（ＳＩＰ）第２期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業「スマートシティリファレンスアーキテクチャホワイトペーパー」

2020 年 1 月の世界経済フォーラム年次総会（ダボス会議）が、「ステークホルダーがつくる、持続可能で結束した世界」というテーマを掲げたことも注目され、「ステークホルダー資本主義」という言葉も出てきている。「ステークホルダー資本主義」とは、企業活動を通してステークホルダーへの貢献をめざす長期的な企業経営のあり方であるが、このことはスマートシティの取組においても同様と考えられる。つまり、ステークホルダーへの貢献を含めた長期的な視点にたったサービス（便益）創出がスマートシティにおいて求められる。

ステークホルダーについては、事業にサービスの提供や享受、あるいはデータのやり取りで直接的に関わるステークホルダーに目がいきがちであるが、業界団体や競合するサービス等、間接的に関係したり、影響を受けるステークホルダーも考慮することが不可欠である。例えば、市民のヘルスケアに関するプロジェクトを起こす場合、市民とサービスの提供者、あるいはそれに関わる医療・介護事業者だけがステークホルダーと考えられがちであるが、地域の医師会や当該分野でボランティア等として活動する NPO 等もステークホルダーとなる。

ステークホルダーの重要性については、事業への影響度と事業について不確定要素（マイナスの影響）を与える可能性等を考慮し、選定する。不確定要素とは、ステークホルダーの権利や既得権益に影響する可能性や、ステークホルダーが不安に感じる要素等を想定し、評価することになる。

図 4-4　重要なステークホルダーの選定

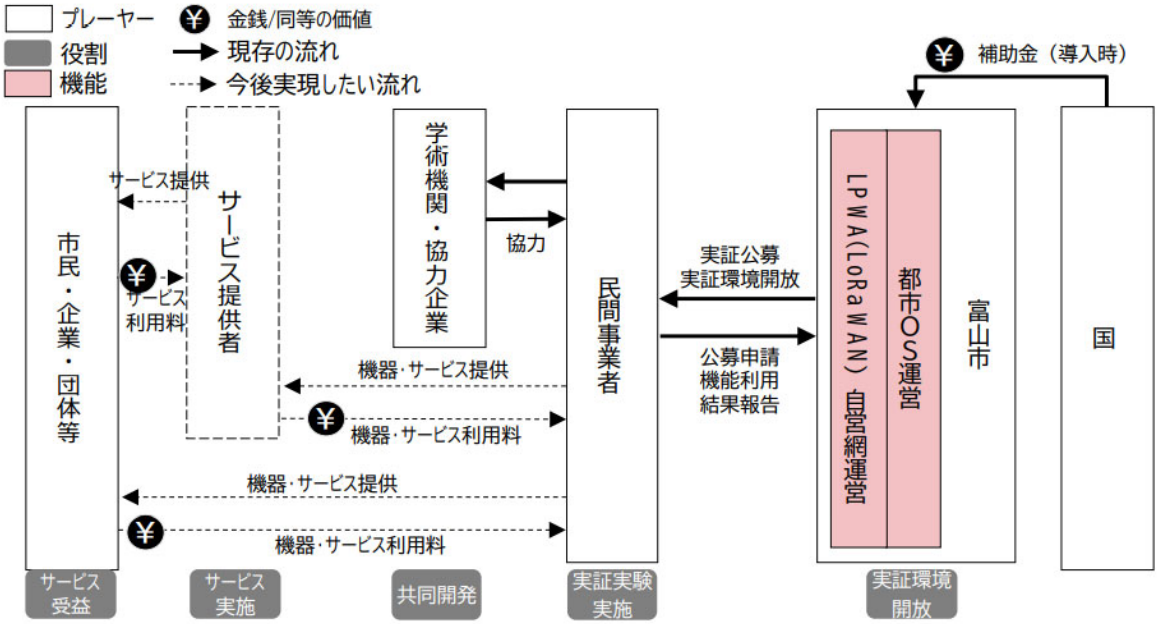


5. データガバナンスプロセスの解説

5.1. 事業概要の整理

まず、事業の概要を整理する。これはスマートシティの計画（戦略）策定と同義であり、整理する項目は目標、取組内容、実施主体、ステークホルダー（関係者）、推進方針、スケジュール（ロードマップ）等が含まれる。この際、最も重要なのは市民や社会等のサービス（便益）であり、これを起点として事業が組み立てられているかどうかである。サービス（便益）を起点としてスマートシティの事業のアーキテクチャ（レイヤー構造）を明らかにする（3.1.参照）とともに、併せて当該事業のステークホルダーを洗い出し、便益やデータ等の関係性を含めてビジネスモデルを整理する。注意が必要なのはアーキテクチャやビジネスモデルには間接的なステークホルダーが必ずしも表現されないことであり、事業概要の整理に当たっては、間接的なステークホルダーも含めて資料として整理することが求められる。

図 5-1　スマートシティのビジネスモデルの例



出典：戦略的イノベーション創造プログラム（ＳＩＰ）第２期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業「スマートシティリファレンスアーキテクチャホワイトペーパー」

この時点、もしくはスマートシティの準備段階においてステークホルダー分析を行い、重要なステークホルダーについては、スマートシティのプロジェクトだけでなく、データガバナンスのプロセスに関しても巻き込みを図ることが望ましい。前述したように、ステークホルダーの重要性については、事業への影響度と事業について不確定要素（マイナスの影響）を与える可能性等から評価し、間接的なステークホルダーが含まれる場合もある。ステークホルダーの関わり方（エンゲージメント）については、その特性等を踏まえて検討する必要がある。一般的にステークホルダーの関わり方に関しては、表 5-1 のように整理される。特に重要度の高いステークホルダーについては、インボルブメント/協働の手法を候補として検討することが望ましい。

表 5-1　ステークホルダーのエンゲージメント手法

形態	手法
情報発信	ステークホルダー個別アナウンス、メディア広報　等
情報収集	アンケート調査、ソーシャルメディア分析、有識者会議　等
双方向	個別交渉、連絡会議　等
インボルブメント/協働	プロジェクト参加、リビングラボ、ステークホルダーとのパートナーシップ、マルチステークホルダープロセス[9]　等

また、多様なステークホルダーを巻き込む際は、貢献できる内容や関心事等が異なるため、最低限の共通事項について合意をしておくことが重要になる。スマートシティの目指すべきサービス（便益）、その実現に向けた大まかな役割分担、協働を行うためのルール（参加の仕方、成果・知的財産等の取扱い等）等については事前に整理し、合意しておくことが望ましい。

[9] 3 者以上のステークホルダーが、対等な立場で参加･議論できる会議を通し、単体もしくは 2 者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセス。

5.2.　関係法令等の整理

データガバナンスを考える上でまず満たすべき要件は法令遵守である。法令に違反するようなスマートシティでは、市民の信頼は得られず、本来の便益を享受することも難しい。デジタル化の進展に伴い様々な分野において法律の見直しも進んでおり、事業分野に精通した有識者等と連携して関係法令等を整理することが望ましい。もちろん個人情報保護法等、データを扱う上で分野横断的に基本となる法律もあり、これらを遵守することも必要不可欠である。内閣府の「スマートシティリファレンスアーキテクチャ　ホワイトペーパー」では、表 5-2 のような関係法令が例示されている。

例えば、柏の葉のスマートシティにおいて進められているフレイル予防 AI の研究開発では、地方公共団体が持つ医療、介護等の情報を活用するために、柏市の個人情報保護条例だけでなく、国の高齢者の医療の確保に関する法律（高確法）、国民健康保険法、介護保険法等を踏まえたデータガバナンスの枠組みが検討されている。なお、地方公共団体の個人情報保護条例については、令和 5 年 4 月施行の個人情報保護法に統合されることになっている。

表 5-2　スマートシティの関係法令

分野	関連法令
交通モビリティ	道路交通法、道路運送法、道路運送車両法、鉄道事業法、航空法　ほか
健康福祉	医療法、介護保険法　ほか
エネルギー	電気事業法　ほか
通信	電波法　ほか
農業	農地法　ほか
行政手続き	デジタル手続法　ほか
まちづくり	都市計画法、道路法、河川法、都市公園法　ほか

出典：戦略的イノベーション創造プログラム（ＳＩＰ）第 2 期ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業「スマートシティリファレンスアーキテクチャホワイトペーパー」

また、関係法令だけでなく、関係府省や業界団体が作成するガイドライン等も考慮することが不可欠である。昨今、技術革新が目覚ましく、これに法律レベルで対応することの難しさから、ソフトローと呼ばれる企業等の自主規制を前提にしたガバナンスの仕組みも併用されることが多い。したがって、事業分野におけるソフトロー等についても調査し、整理しておくことが重要である。

例えば、カメラ画像を用いた事業を検討しているのであれば、経済産業省、総務省がとりまとめている「カメラ画像利活用ガイドブック ver3.0」、交通データでは国土交通省「MaaS 関連データの連携に関するガイドライン Ver.2.0」等が代表的なソフトローとして挙げることができる。また、国だけでなく、一般社団法人 LBMA Japan「位置情報等の「デバイスロケーションデータ」利活用に関するガイドライン」のように民間企業を中心とする自主的なソフトローも存在する。

表 5-3　考慮すべきソフトローの例

利用データ等	ソフトロー
カメラ画像	経済産業省、総務省「カメラ画像利活用ガイドブック ver3.0」
位置情報	一般社団法人 LBMA Japan「位置情報等の「デバイスロケーションデータ」利活用に関するガイドライン」
交通	国土交通省「MaaS 関連データの連携に関するガイドライン Ver.2.0」
健康情報	総務省、厚生労働省、経済産業省「民間 PHR 事業者による健診等情報の 取扱いに関する基本的指針」
医療情報	厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5.2 版」 経済産業省、総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」
スマートフォンアプリ	総務省「スマートフォン　プライバシー　イニシアティブ」

5.3. リスク分析

事業概要や関係法令等の整理を踏まえ、事業の実施にあたり、データのライフサイクルを通じてリスク等が存在しないか検討する。リスクの着眼点としては、デジタル庁、内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」を参考にすると、以下の 6 つが想定される。以降において主要な着眼点について述べる。

表 5-4　スマートシティにおけるリスクの着眼点

着眼点	概要
関係法令等の遵守	関係法令、ソフトロー等を適切に把握し、その内容を遵守しているか。
プライバシー保護	個人に関する情報等を扱う場合、その取扱いにおいて不安や不快感を抱かせないように配慮されているか。
知的財産や秘匿情報の尊重	スマートシティに参加する組織が保有する知的財産や秘匿すべき情報が適切に保護されているか。
セキュリティの確保	情報の漏洩、サービスの改ざん等の問題が生じないように適切に安全管理が行われているか。
適正な運用	スマートシティのサービスが市民等の公平性を損ねたり、被害等を与えたりする危険性がないか。
全体のガバナンスの維持	スマートシティのサービスを構成するステークホルダー全体において、上記の着眼点のリスクを低減する仕組みになっているか。

（1）関係法令等の遵守

スマートシティにおける関係法令等の遵守においては、法律で明文化されているものへの対応は相対的に難しくないが、ソフトローや判例等に依拠する部分については、判断が明確でなく、リスクにつながると考えられ、その多くはプライバシー侵害に関係する。住民の一部からプライバシー侵害を理由として提訴され、敗訴すれば、住民に対する損害賠償（不法行為（民法 709 条）に基づく損害賠償請求）や事業の停止（人格権侵害に基づく差止請求）を命じられることとなる。既存のスマートシティの事業計画を精査し、プライバシー侵害が問題となりやすい事案として、「①顔認識カメラによる撮影」、「②位置情報の利用」、「③教育データの利用」の 3 点について示す。

①顔認識カメラによる撮影

カメラによる人の姿態の撮影と、撮影した情報の利用・公開については、一定の場合に肖像権侵害・プライバシー侵害として損害賠償請求及び差止請求の対象となることが判例法理として確立している。その多くは、警察による防犯カメラとマスメディアによる報道に伴うものである。顔認識カメラによる撮影は、特徴量抽出のために行われるものであり、特徴量は肖像の形状を数値に置き換えたものであるため肖像権侵害の対象にならないとする意見もあるが、一般には顔認識カメラによる撮影が肖像権侵害となることがあり得ると考えられている。

警察による写真撮影に関しては、これまで裁判所によって厳しい基準が示されており、「現に犯罪が行なわれもしくは行なわれたのち間がないと認められる場合であって、しかも証拠保全の必要性および緊急性があり、かつその撮影が一般的に許容される限度をこえない相当な方法をもつて行なわれる

とき」[10]などが適法性の要件として示されている。これは極めて厳格な要件であるが、警察による撮影行為と警察とは別の行政組織としての自治体の事業計画における撮影行為は、区別されるべきである。事業計画における自治体や商店街の撮影行為は、撮影データが警察に提供されるような特段の事情がない限り、民間事業者の撮影行為に近いものとして考えてよいであろう。

民間事業者の防犯カメラに関する裁判例は少ないが、コンビニエンスストアの防犯カメラに関する裁判例が参考になる。代表的なケースである東京地判平成 22 年 9 月 27 日（判タ 1343 号 153 頁）は、コンビニの防犯カメラにおける撮影行為自体が肖像権・プライバシーを侵害するものとして不法行為に当たるかが争われた事案である[11]。本件では、違法性の判断基準を以下のように示している。

> 本件監視カメラは，本件店舗を訪れた客の個別的承諾を得ることなく，商品を選定したり，これを購入する姿を無差別に撮影するものであり，客の上記人格的利益[12]及びプライバシー権が侵害されるおそれを内包するものであるということができる。したがって，本件監視カメラにおいて，本件店舗内の客を撮影し，その撮影に係る画像を報道機関に提供することによりこれを公表等することが不法行為法上違法といえるか否かは，撮影の目的，撮影の必要性，撮影の方法及び撮影された画像の管理方法並びに提供の目的，提供の必要性及び提供の方法等諸般の事情を総合考慮して，上記姿を撮影され撮影に係る画像を公表等されない利益と上記姿を撮影し撮影に係る画像を公表等する利益とを比較衡量して，上記人格的利益及びプライバシー権の侵害が社会生活上受忍限度を超えるものかどうかを基準にして決すべきである。

本判決は、本人の承諾のない撮影と提供の双方が問題になった事案であるが、撮影に限っていえば本判決は、「撮影の目的」、「撮影の必要性」、「撮影の方法」、「撮影された画像の管理方法」を総合的に考慮してプライバシー侵害・肖像権侵害の有無を判断するという方法を採用しており、顔認証カメラによる撮影全般の適法性を判断する際に参考となる裁判例である。

このような総合判断の観点からは、プライバシー侵害・肖像権侵害を防ぐため、以下のことに注意すべきである[13]。

- 利用目的が正当であり、利用目的との関係で撮影の必要性があることが求められる。不適切な例としては、正当な理由なく差別的取扱いを行うために利用することや「地域店舗の事業の用に供する」というような不明確な利用目的でカメラ画像の取得や利用を行うことが挙げられる。
- 撮影方法・手段や利用の方法が相当であることが求められる。不適切な例としては、プライバシーへの影響が過大な撮影方法を用いること（例えば被写体の同意を得ずに、長期に広範囲にわたる追跡を行う等）、必要のない撮影範囲でのデータ取得、必要な期間外でのデータの保管、あえて被写体がカメラで撮影されていると認識できないような方法で撮影した場合（例えば、隠し撮り等）が挙げられる。
- 撮影された画像の管理を適切に行うことが求められる。不適切な例としては、被写体の情報を目

---

[10] 最判昭和 44 年 12 月 24 日　京都府学連事件（判タ 242 号 119 頁、判時 557 号 18 頁）なお、この基準は事例判決であり、警察による写真撮影一般には妥当しないという意見が有力である（最判平成 20 年 4 月 15 日刑集 62 巻 5 号 1398 頁の最高裁判所判例解説）

[11] 同種事件として、名古屋地判平成 16 年 7 月 16 日（判タ 1195 号 191 頁）も参照

[12] 最高裁京都府学連事件（前脚注 10）を引用して、「肖像権」の用語を使わず人格的利益としている。

[13] カメラ画像利活用ガイドブック ver3.0　12 頁を元に作成。

的外に容易に利用できてしまう状態で保管することが挙げられる。

参照先
犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会報告書（案）
カメラ画像利活用ガイドブック ver3.0

②位置情報の利用

位置情報は、所在場所に関する情報のみではなく、わずかな期間の取得で、自宅住所や学校・勤務先などが把握できる情報である。また、教会、政党事務所、病院に通っていること等が分かれば、信条や健康状態などの機微な情報を推認させることにもなる。その一方で、多くのスマホアプリによって取得・利用されている実情がある。

位置情報とプライバシーに関する裁判例としては、「N システム」[14]に関する一連の事件が参考になる。N システムに関する裁判例は複数あるが、最近の裁判例の違法性判断の基準としては以下が示されている。

> (a)取得、保有、利用される情報が個人の思想、信条、品行等に関わるかなどの情報の性質はどのようなものか、(b)取得、保有、利用する目的が正当なものであるか、(c)取得、保有、利用の方法が正当なものであるか、(d)情報の管理方法の厳格さはどの程度か、などを総合して判断すべきである。

上記判決は、情報の性質（上記(a)）について、以下のように評価して、一定の機微性・プライバシー性があることを明らかにしている。

> 車両を用いた移動に関する情報が大量かつ緊密に集積されると，車両の運転者である個人の行動等を一定程度推認する手掛かりとなり得ることは否定できないというべきであり，原告らの主張するような国民の行動に対する監視という問題も生じ得るから，Nシステム等によって得られる情報が，目的や方法のいかんを一切問わず収集の許される情報とはいえないことも明らかである。

これは、断片的な位置情報の「大量かつ緊密」な集積が個人の行動の把握につながることを裁判所が認識していることを示す注目すべき判示である。

また、ここでも先ほどのカメラ撮影と同様の基準が用いられていることに注意すべきである。すなわち、カメラの３つの要素に「(a)取得される情報の性質」を加えた 4 要素での総合判断となっている。このような総合判断の観点からは、プライバシー侵害・肖像権侵害を防ぐため、以下のことに注意すべきである。

- まず、非常時の利用に関するものや防災・減災目的での利用については、「(a)取得される情報の性質」について位置情報が機微なものであることを前提としても、「(b)取得・利用の目的」の正当性において、適法化の可能性が高いものである。これに対して、位置情報を商用目的に利用してコンテンツのレコメンドや行動ターゲティング広告をする場合には、「(b)取得・利用の目的」の正当性が高いとは言えず、「(c)取得・利用の方法」が厳格に審査されることとなるであろう。基本的には対象者の有効な同意を取得しなければプライバシー侵害とされるおそれを払しょくできないであろう。
- 次に、顔認証カメラにより位置情報を捕捉する場合については、「(c)取得・利用の方法」の相当

[14] 正式名称は「自動車ナンバー自動読取装置」。走行中の車両のナンバープレートを撮影して手配車両と自動的に照合するシステムであり、速度違反車両のみを撮影する「オービス」とは異なる。

性が問題となり得る。位置情報を把握するためには、他の方法、例えば指先の静脈を利用した認証によること等も可能であり、そちらの方の権利侵害性が低いからである。事業計画において指先静脈認証等、他の方法でも位置情報が取得できる場合には、「(c)取得・利用の方法」の相当性を欠くものと判断される可能性がある。

- さらに、N システムについて、裁判所が断片的な位置情報であっても「大量かつ緊密に集積」されることにより個人の行動の把握や監視につながると考えていることに留意すべきである。このような裁判所の考え方を前提にすると、同じ位置情報であっても、N システムによって取得される車両の移動情報と、例えばスマートフォンアプリの GPS 位置情報ではその精度が大きく異なることに注意すべきである。N システムの場合、車両による移動は個人の生活における移動全般のうちごく一部であり、家族など本人以外の情報が混入することなどにより精度が低く、その分「行動の監視」につながりにくい。スマートフォンの GPS 位置情報は、(個人の生活における全移動を把握できるものであり、かつ１人１台が原則であるから他人の情報が混入することはなく精度の高い監視が可能となる点で、N システムに比べるとプライバシー侵害のおそれが高いことに注意すべきである。このことから、スマートフォンの GPS 位置情報を取得・利用する場合には、「(b)取得・利用の目的」、「(c)取得・利用の方法」、「(d)取得された情報の管理方法」の総合判断において、各要素を厳格に判断すべきであることになる。
- なお、総合判断の最後の要素である「(d)取得された情報の管理方法」は、安全管理を求めるものであり、事業計画がこれを欠く場合には、位置情報の把握がプライバシー侵害とされる可能性がある。

③教育データの利用

自治体が保有する教育データの利用においては、本ガイドラインが重視する人間中心主義（＝児童生徒中心主義）が最も強く要請される。また、デジタル庁ほかが公表した「教育データ利活用ロードマップの炎上」に見られるように[15]、教育データの「一元管理」については、社会の根強い不安が存在する。したがって、他分野のデータを合わせて一元的に管理することや、長期間のデータを保存して児童生徒を観察すること等については、慎重な検討が必要である。他方で、教育データの利活用については、かねてから教育者などにより「児童生徒の利益」のためのものであるべきことが強調されており、学習塾等の事業者が営利目的で教育データを利用することについては、それが同時に児童生徒にとっても高い有用性を有することが求められる。

前記の取得型プライバシー侵害の判断基準である、「(a)取得される情報の性質」、「(b)取得・利用の目的」、「(c)取得・利用の方法」、「(d)取得された情報の管理方法」の総合判断はここにおいても有効である。そして上記のような教育データの特殊性に配慮した総合判断の観点からは、プライバシー侵害を防ぐため、以下のことに注意すべきである。

- 「(b)取得・利用の目的」においては、児童生徒の利益になることが必須であり、総合判断といえどもこれを欠く事業計画は妥当ではない。
- 「(c)取得・利用の方法」については、「一元管理」への懸念との関係で、他分野のデータとの統合や長期間のデータ保有については、特に慎重な検討が必要である。
- 非行その他の逸脱行動の予防は、学校教育における重要な課題であり、学習履歴や学校における

---

15 DIAMOND online「まだ始まってもいないのに…デジタル庁の『教育データ利活用』が大炎上してしまったワケ」2022 年 1 月 28 日。

生活態度全般の変化を記録・分析することにより、非行の可能性を予測することは、「(b)取得・利用の目的」として合理性の高いものである。しかしながら「(c)取得・利用の方法」との関係では、問題を残している。第一に、得られる予測の精度が低いことによる「誤ったラベリング」の問題がある状況下では、不当な差別・不利益を児童生徒に帰結するものとなるため、実施すべきではない。また、機械学習の成果により予測精度が十分向上したとしても、統計的に非行を行う可能性の高い属性を有する児童生徒がその児童生徒の個人的な信念や考えによって結局非行に至らないことは、可能性としては否定できないのであって、それにもかかわらず、「非行のおそれあり」と判定することは、その生徒の個人としての自律性を否定する結果となる[16]。非行に陥る属性を持ちながらそれを自らの意思で克服する可能性を否定する点において、データによる非行の予測は、「(c)取得・利用の方法」において合理性を欠いており、プライバシー侵害のおそれがあるというべきである。

- なお、総合判断の最後の要素である「(d)取得された情報の管理方法」は、安全管理を求めるものであり、事業計画がこれを欠く場合には、教育データの利用がプライバシー侵害とされる可能性がある。

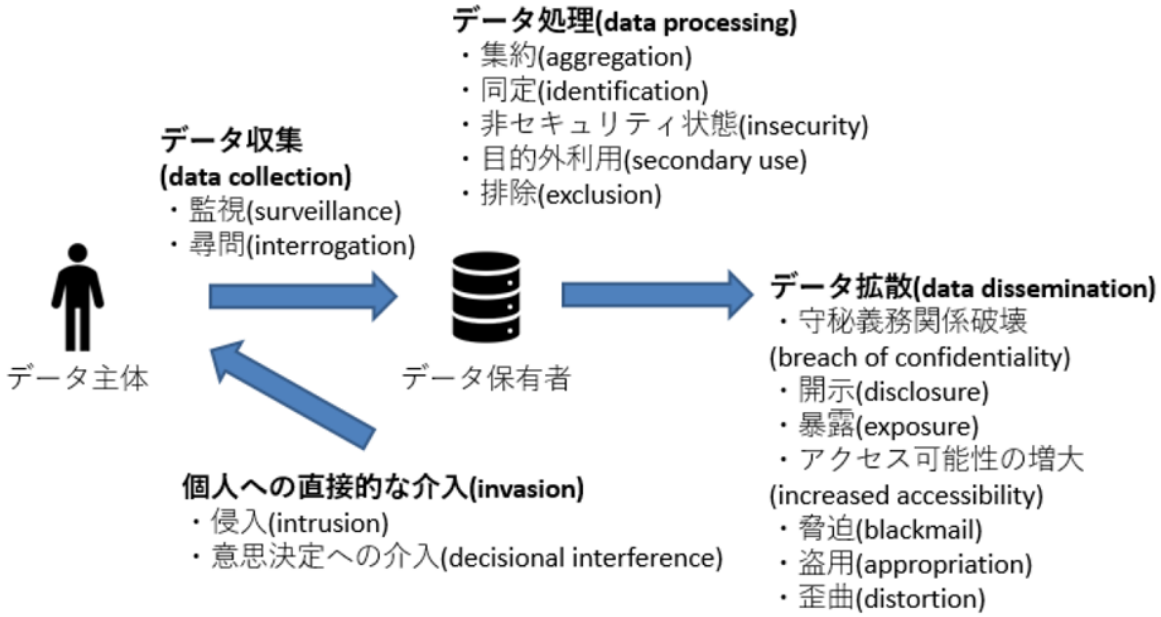
（2）データライフサイクルにおけるプライバシー保護

「関係法令等の遵守」では、ソフトローや判例等に基づくプライバシー侵害のリスクについて述べたが、人間中心でスマートシティを実現する上で市民等、ステークホルダーの視点から幅広くリスクを検討することも不可欠である。例えば、（1）の各場面以外であってもパーソナルデータを扱う場合には、図 5-2 に示すような観点からプライバシー保護に関するリスクを検討することが考えられる。これは米国のプライバシーの研究者であるダニエル・ソルブが整理したもので、データ主体である個人からデータを収集し、処理し、移転（拡散）あるいは個人へのフィードバック（介入）を行うデータライフサイクルにおけるリスクを整理したものであり、リスクを発想する上で参考となる。(詳細は参考資料)

前述したように、「人間中心」でスマートシティを考える場合、データ活用に対する市民の受容性等も地域によって異なる。したがって、地域のスタークホルダーの意識を把握することもリスク分析において求められる。

16 山本龍彦「プライバシーの権利を考える」（信山社 2017）102 頁は、犯罪予測についてではあるが同様の考え方を示している。

図 5-2　プライバシーリスク



出典：経済産業省「DX 時代における企業のプライバシーガバナンスモデルガイドブック ver1.2」

（3）セキュリティの確保

スマートシティにおいては、関係法令等の違反、プライバシー等の権利の侵害だけでなく、情報の漏洩等、セキュリティリスクが高まる可能性があることについても留意が必要である。スマートシティにおいてセキュリティリスクが高まる要因は、多様なステークホルダーにおいてデータ連携が発生することに起因する。

データ連携する場合、そのデータ連携に必要な情報通信ネットワーク全体としてセキュリティを担保するだけでなく、データを出す側と受ける側双方においても十分なセキュリティレベルの確保が求められる。また、データが複数のステークホルダー間で共有されるため、インシデントが起こった際の対応も複雑になる。例えば、どこかの組織からデータの漏洩等が発生した場合、当該組織だけでなく、スマートシティの中でデータ連携している組織にも影響があり、インシデント対応を連携して行うことが求められる。

加えて、スマートシティでは、都市 OS 等、PF となる情報システムを整備する場合も少なくない。これらはデータ連携のハブとなるだけでなく、様々なデータが蓄積される可能性があり、セキュリティ面の問題が発生した場合、被害が大きくなるということにも留意が必要となる。

また、前述したようにデータ自体がスマートシティの血流として組織を跨って連携することを考慮すると、その正確性、真正性が担保されていないことも大きなリスクとなる。データの品質が担保されていないことで AI の開発に失敗したり、スマートシティのサービスが本来の便益を創出できなかったりする可能性も出てくる。

参照先

総務省｜報道資料｜「スマートシティセキュリティガイドライン（第 2.0 版）」（案）に対する意見募集の結果及び「スマートシティセキュリティガイドライン（第 2.0 版）」の公表（soumu.go.jp）

5.4. ルールの設計

リスクを低減するという視点からスマートシティの事業におけるデータポリシー（ルール）を作成する。これにはスマートシティ全体（推進組織）という大きな取組の枠組みでのルールと、個別のサービス（便益）、つまり事業毎に設定するルールの二つのレベルが存在する。

スマートシティ全体のルールは、データを扱う上での基本的な考え方や原則を示すものであり、個別の事業で設定するルールの共通項となる。また、個別の事業のルールを設定するための組織や意思決定プロセス等もこれに規定することになる。

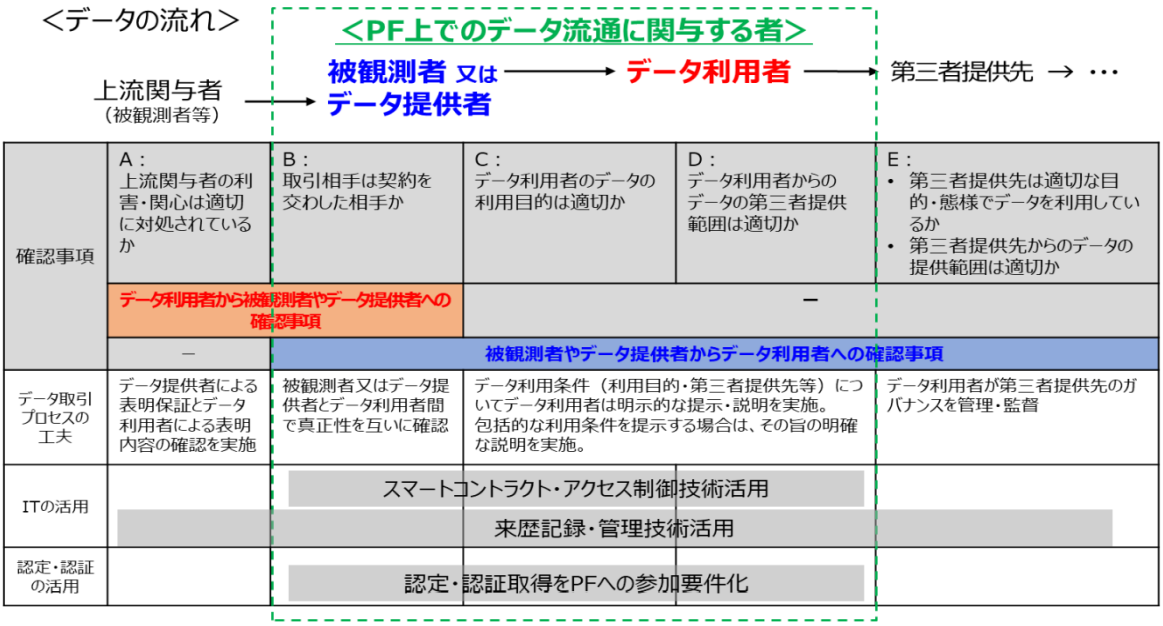
一方、事業単位のルールでは、サービス（便益）の内容やその事業分野の関係法令、地域特性等を踏まえて個別に検討する必要があり、データの扱いはより具体的に規定することになる。

どちらのレベルにといても、以下に示す点を考慮した設計が求められる。

（1）データのコントローラビリティ

スマートシティで取り扱うデータが個人に関するデータ（パーソナルデータ）、あるいは企業や環境等に関するデータ（ノンパーソナルデータ）に限らず、データのコントローラビリティを確保することがデータガバナンスの基本となる。したがって、データ提供者（パーソナルデータの場合は個人）やデータ利用者、あるいは第三者等、データの流通、ライフサイクルを踏まえた上で、それぞれでどのようにしてリスクを低減する対策を行うか、ということがルール設計そのものになる。図 5-3 はデジタル庁、内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」に示された PF におけるコントローラビリティ確保のための確認事項と確認の方法であるが、このような事項を定めることがルール設計となる。なお、パーソナルデータの場合はデータ化された対象である個人が被観測者（すなわち、被観測者＝本人）である。ノンパーソナルデータの場合は被観測者が存在しない場合（例えば気象データ）もあるが、在庫データや工作機器の稼働情報等、組織の活動等がデータ化される場合は当該組織が被観測者となる。

図 5-3　PF におけるコントローラビリティ確保のための確認事項と確認の方法



出典：デジタル庁、内閣府知的財産戦略推進事務局「プラットフォームにおけるデータ取扱いルールの実装ガイダンス ver1.0」

（2）パーソナルデータに関するルール

すべてのデータにおいてコントローラビリティの確保が起点となるものの、特にパーソナルデータに関しては、個人のプライバシーや尊厳を尊重した取扱いが求められ、以下の観点からルールを検討することが重要である。もちろん、5.3(1)記載のとおり、個人情報保護法および民法のプライバシー侵害に関するルールを遵守することが前提となる。

〇十分な通知と周知

パーソナルデータを活用する上では、その利用目的等を個人に知らしめることが必要不可欠である。スマートシティの中には、新たなデータの活用等も含まれ、個人が想起できない場合も少なくない。したがって、個人の認識のレベルを考慮して、できるだけ丁寧で分かり易い通知を行うことが重要である。[17]

例えばカメラ等のセンサーデータの活用、あるいは一度、収集したパーソナルデータの二次利用については、同意を得ることが難しい場合がある。この場合、5.3(1)記載のとおり、「(a)取得される情報の性質」、「(b)取得・利用の目的」、「(c)取得・利用の方法」、「(d)取得された情報の管理方法」の総合判断によって本人の同意なく適法に実施しうることがあるが[18]、その場合においても、できるだけ利用目的を周知できるように工夫することが必要である。例えば、柏の葉のスマートシティにおいては、AI カメラ（画像は即時削除し、年齢や性別、人流等の属性データのみを活用）を導入にするにあたり、掲示物等で通知するだけでなく、ホームページでデータ取扱いのポリシーを発信したり、住民説明会を実施したりして、丁寧な周知を行っている。

〇安全性の担保

スマートシティでは、多様なステークホルダーが事業に関わることが想定される。便益（サービス）の創出のためにステークホルダーの関与が必要であっても、データへのアクセス可能性を広げることは、リスクの拡大にもつながる可能性がある。したがって、パーソナルデータの安全性を確保するため、データへのアクセスを制御するとともに、アクセスできるステークホルダー個々における安全性を担保するようなルール整備が必要となる。なお、個人データの場合には個人情報保護法により原則としてステークホルダーのアクセスには本人の同意が必要である（27 条 1 項）。[19]

〇透明性と自己情報コントロール

スマートシティでは、データの取得が先行して問題化した事例も少なからず存在する。したがって、市民の便益を含めて、データの流れや利活用の仕組み等でできるだけ公開し、その推進プロセス自体

---

17 要配慮個人情報の取得や個人情報の第三者提供を行う場合等においては、個人情報保護法に基づき同意が必須となる。また、肖像権侵害・プライバシー侵害の観点からも同意が求められる場合がある。18 前脚注のとおり、同意が必要な場合が存在する。二次利用においては、同意が困難な場合は匿名加工、非個人情報化等の対応も想定される。

18 前脚注のとおり、同意が必要な場合が存在する。二次利用においては、同意が困難な場合は匿名加工、非個人情報化等の対応も想定される。

19 同意に基づき個人情報の共有、第三者提供等を行う場合、個人情報保護法に基づき、組織的、人的、物理的、技術的な安全管理措置が求められる。また、委託を行う場合においても委託先の安全管理措置を担保することが不可欠である。

の透明性を高めることが重要である。また、市民が自分のデータがどのように使われているかを認識し、必要に応じて、利用の停止やデータの修正等が行えるような自己情報コントロールを実現することも市民の信頼を得るために必要である。

〇最小取得原理

スマートシティで懸念されるのは、個人に関するデータが無作為に取得、統合され、個人のプライバシーが侵害されることである。このような懸念を払しょくするため、不必要なデータの取得や名寄せは行うべきではない。また、データを活用する際にもできるだけプライバシーに配慮した活用方法を検討する必要がある。

例えば、公衆衛生目的として、個人の医療データを用いる場合では、少なくとも個人を特定するようなデータは必要ない場合もある。その場合は、匿名加工を行う等、よりプライバシーに配慮した活用を検討することが望ましい。

（3）セキュリティ等に関するルール

前述したようにスマートシティでは多様なステークホルダーにおいてデータ連携が行われる可能性があり、その場合は適切なセキュリティレベルが確保できるよう、ルールを規定しておくことが求められる。また、スマートシティにおいてトラストを形成し、効率的な運用を図るためにもデータの信頼性等を担保するための取り決めも必要になる。具体的には、以下のような事項についてデータ連携するステークホルダー間でルールを設定することが想定される。

・データ連携する組織において求められる安全管理措置（組織的、人的、物理的、技術的）
・データ連携のログ等の保存等、透明性を担保するための方法、考え方
・データを出す側、受け取る側で正確性や真正性を担保するための方法、考え方

特にスマートシティでは、分野を跨ったデータ連携が行われることが想定され、これによってセキュリティレベルが異なる場合に留意が必要である。例えば、医療情報等を地域の公衆衛生や健康増進に活用しようとした場合、民間のサービス等においても医療機関と同等のセキュリティレベルが求められる。また、都市 OS のような PF については、データが集約されたり、データ連携のハブとなったりする特性から、より強固なセキュリティが求められるということについても配慮してルール設計を行うことが必要である。さらに、スマートシティが本来のサービス（便益）を実現する上で、AI 等の適正な開発の前提になるデータの正確性、真正性の担保も非常に重要であり、そのためのルールも不可欠である。一般社団法人 AI データ活用コンソーシアム「AIDC プラットフォームにおけるデータ提供契約に関する報告書」等を参考として、データの出す側、受け取る側での遵守事項等を定めるとともに、複数の組織を跨ぐことを前提とした来歴管理の方法等も決めておくことが望ましい。

加えて、セキュリティのインシデントが発生した場合の対応等についてもステークホルダー間でルールを定め、合意しておくことが必要である。具体的には以下のような事項についてルール形成を行っておくことが考えられる。

・インシデントが発生した場合に速やかにステークホルダー間で情報共有を行うこと
・インシデントが発生した場合の対応プロセス、情報共有の方法、連絡窓口等
・データ連携等における責任分解点等
・必要に応じて第三者やスマートシティの運営主体等による監査に対応すること

参照先

AIDC プラットフォームにおけるデータ提供契約に関する報告書.pdf (aidata.or.jp)

（4）個益と公益

個益（個人に対する直接的な便益）と公益（地域や社会全体における便益）の関係性も含めたルール設計も必要である。スマートシティの取組は必ずしも個人に対して直接的な便益として返るものばかりではなく、社会という大きな枠組みの中で便益を創出するものもある。したがって、公益のために市民が協力するということも含め、インセンティブ等を含めたルール設計が求められる。

例えば、接触確認アプリ（COCOA）については、自分自身の感染防止という個益に加えて家族やさらには社会全体の感染抑止につながるとする公益効果も期待され、使われているとする研究がある。このように個益と公益が共存する政策においても、必ずしも万人に受け入れられるわけではないことを考慮すると、個益が見えにくく、公益が中心となるスマートシティへの取組は市民等に対してより配慮を行ったルール設計が必要となる。

例えば、公益性を担保するような客観的な仕組み（有識者会議による審査等）、透明性を担保するような情報の公開、公益の可視化等が求められる。

（5）インセンティブ設計

データガバナンスにおいて設計したルールを遵守してもらうためにはインセンティブ設計も重要となる。スマートシティのサービスが各ステークホルダーに与える影響や便益を明らかにすることは重要であるが、その便益を享受するために守るべきルールも合わせて合意してもらうことが不可欠である。例えば、サービス提供者の参加資格を審査し、ルールの運用状況をモニタリングし、ルール違反時にはその審査とペナルティの執行を行えるようにする等の対応が考えられる。また、逆に適切にルールを守りスマートシティの運営に貢献しているステークホルダーを評価し、公表することで、レピュテーションを高める等のインセンティブ設計も有効である。

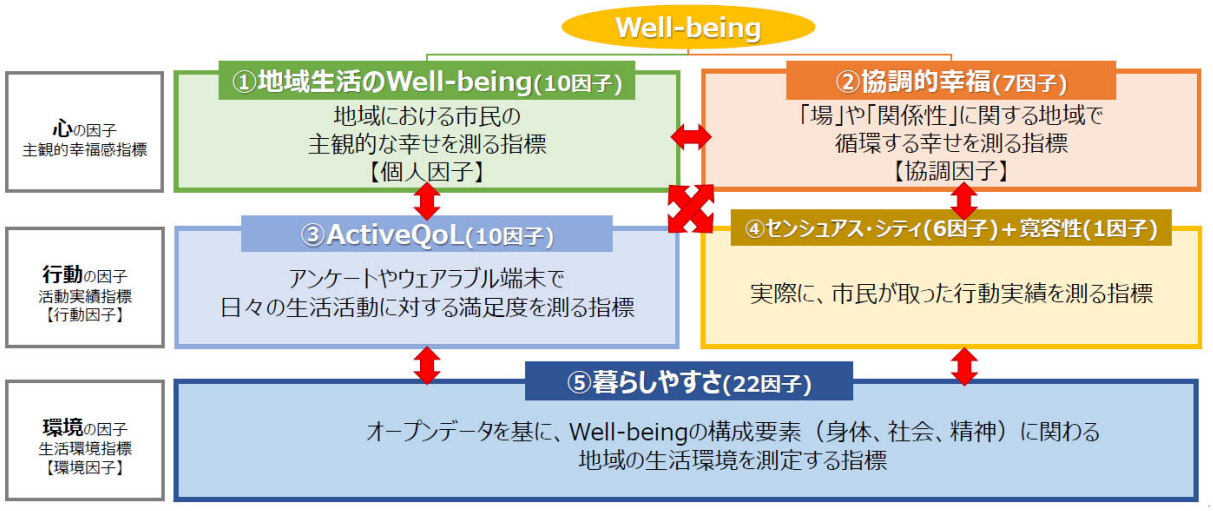
5.5. 運用・評価

設計したルールを実際のスマートシティの中で運用し、適切に機能するか評価する。

重要なのは、スマートシティとしての運用・評価がまず存在し、その中でルールの運用・評価があるということである。

通常、事業の実現に向け、PDCA サイクルを確立していくためには、取組の進捗や効果を評価できる KPI 等を設定することが有効である。スマートシティにおいても、サービス（便益）によって目指すべき地域の姿や定量的な指標等を設定することになり、評価指標を定める上で、一般社団法人スマートシティ・インスティテュート（SCI-Japan）が開発、普及している Liveable Well-Being City 指標等が参考になる。

図 5-4　Liveable Well-Being City 指標の体系



出典：デジタル庁、一般社団法人スマートシティ・インスティテュート「LWC 指標利活用ガイドブック」

参照先

一般社団法人スマートシティ・インスティテュート｜Liveable Well-Being City 指標　ご紹介と活用について（sci-japan.or.jp）

スマートシティのサービス（便益）や目指すべき姿がどのくらい達成されているかという評価を踏まえ、ルールに関しても運用・評価を行う。スマートシティが期待された効果を創出していないのであれば、その原因としてルール等が起因していないか評価する必要がある。また、ルールの運用・評価において KPI 等の評価指標を定めておくことが望ましい。例えば、以下のような指標が想定される。

・市民からの苦情等の件数や内容
・ルールの遵守状況（違反した件数や内容等）
・ルールの運用に必要な労力
・ルールの啓発等の活動（研修の件数等）

評価の結果、ルールが過剰であったり、あるいは適切に遵守されていなかったりするような場合には、ルールの内容や仕組み自体を見直すことが必要になる。また、ルールについては、社会環境の変化に応じて見直しが必要になる場合がある。関係法令等が改正された場合、技術的な進展に伴い仕組

み自体が変わる場合、あるいは市民等の意識が変化した場合等、様々な変動要因も考慮し、運用・評価、ルールの見直しを行うことになる。

参考資料　プライバシーリスクの内容

データ収集	監視	継続的なモニタリングにより、個人に対して不安や居心地が悪い感情を与えてないか
	尋問	個人に圧力をかけて情報を詮索してないか、深く探るような質問で個人が強制を感じ、不安になってないか
データ処理	集約	ある個人の情報の断片を集め、それにより、個人が想像しなかった新しい事実が明らかになることにより、個人の期待を裏切ってないか
	同定	あらゆるデータを個人に結び付けることで、個人にとって害のある情報も結び付けられてしまい、個人に不安、不満を与えてないか
	非セキュリティ	パーソナルデータを不適切に保護し、個人に対して不利益を被るようなことが起こってないか
	目的外利用	個人の同意なしに当初の目的とは違うデータ利用を実施し、個人を裏切るような行為になってないか
	排除	個人のデータの開示・訂正の権利を与えない等、重要な意思決定に対して個人のコントロールが効かないようになっていないか
データ拡散	守秘義務関係破壊	特定の関係における信頼関係により取得した個人のデータを、他社に開示するなどで個人へ裏切りの感情を与えてないか
	開示	個人のデータを第三者へ開示されることで、二次利用先で更なるプライバシー問題が生じていないか
	暴露	生活の諸側面の他者への暴露により、深刻な恥辱を経験し、個人の社会参加能力を妨害することになっていないか。
	アクセス可能性の増大	パーソナルデータへの他者のアクセス可能性を増大させ「開示」のリスクを高めていないか
	脅迫	パーソナルデータの暴露、他者への開示などを条件に、脅迫者と非脅迫者に強力な権力関係を作り出し、支配され、コントロールされる事態になっていないか。
	盗用	他者のアイデンティティやパーソナリティを誰かの目的のために用い、個人が自分自身を社会に対してどのように掲示するのかについてコントロールを失わせ、自由と自己開発へ介入することになっていないか。
	歪曲	個人が他者に知覚され判断される仕方を操作し、虚偽であり、誤解させることで、恥辱やスティグマ、評判上の危害に帰結することはないか。自分自身についての情報をコントロールする能力と、社会にとって自分がどのようにみられるかを限定的にしないすることになっていないか。自己アイデンティティと公共的生活に従事する能力に不可欠な評判や性格を捻じ曲げることになっていないか。社会的関係の恣意的かつ不相応な歪曲が行われる恐れはないか。
個人への直接的な介入	侵入	必要以上の個人へのアプローチ（メールや電話等）により、個人の日常の習慣が妨げられ、居心地が悪く不安な感情を引き起こされてないか
	意思決定への介入	個人の生活において重要な意思決定に対して AI を用いている場合等において、決定方法が不透明で、個人に萎縮効果が働いてないか

出典：経済産業省「DX 時代における企業のプライバシーガバナンスモデルガイドブック ver1.2」