ICSCoE TLP: WHITE

データ利活用型スマートシティにおける セキュアなデータマネジメント

スマートシティにおけるプライバシーリスクの考え方について

2022 年 7 月

独立行政法人　情報処理推進機構

産業サイバーセキュリティセンター

中核人材育成プログラム 第 5 期受講者

スマートシティプロジェクト

第 1 章　はじめに 2
1.1　本書の目的 2
1.2　想定読者 3
1.3　著作権及びその他すべての知的所有権 3
1.4　免責事項 3
1.5　注意事項 4

第 2 章　スマートシティについて 5
2.1　これからのスマートシティとは 5
2.2　スマートシティにおけるマルチステークホルダーについて 7
2.3　用語一覧 7
2.4　本書におけるスマートシティについて 9

第 3 章　プライバシーについて 10
3.1　プライバシーと企業が認識すべきプライバシーリスクとは 10
3.2　パーソナルデータとデータマネジメントについて 10
3.3　プライバシーリスクがスマートシティの障害となった過去事例 11
3.4　プライバシーフレームワークと本書の位置付けについて 11

第 4 章　スマートシティにおけるセキュアなデータマネジメントについて 13
4.1　スマートシティにおけるプライバシーリスクとは 13
4.2　スマートシティデータアーキテクチャ 14
4.3　スマートシティで取り組むべきリスク管理 14
4.3.1　データ保護のポリシー、プロセス、手順 16
4.3.2　アイデンティティ管理、認証、アクセス制御 17
4.3.3　データセキュリティ 20
4.3.4　メンテナンス 22
4.3.5　保護技術 23
4.4　プライバシー残存リスクとリスクの許容について 26

第 5 章　総括 27
5.1　本書のまとめ 27
5.2　本書の課題と制約 27
5.2.1　用語の定義について 27
5.2.2　各組織での活用 28
5.3　謝辞 28
参照文献　29
作成者　30

第1章　　はじめに

1.1 本書の目的

近年、Society 5.0 の実現の場としてスマートシティへの取り組みが政府主導で盛んになってきています[1]。Society 5.0 とは、「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）」であると内閣府により定義されています[2]。それは IoT や AI といった ICT 技術進歩によって膨大かつ様々なデータが収集・解析されることで都市の持つ課題解決を図り、新しい価値を生むデータ利活用が進む未来の街の姿です。

多種多様なデータとして官民が保有するオープンデータが注目されており、高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議「オープンデータ基本指針[1]」によれば、オープンデータとは「機械判読に適した形で、二次利用可能なルールの下で公開されたデータ」を指します。様々なデータがオープンデータとして広く公開されることで、新しいサービスによる価値の提供、社会の利便性向上や経済の活性化などにつながることが期待されるため、国や自治体などの公共機関を中心に世界中で取組が進められています。今後は個人のパーソナルデータもそのデータの一つとして活発に取り扱われることが予想されます。そのような世の中ではサービスにより受ける価値だけに目を向けるのではなく、パーソナルデータが適切に取り扱われ、保護されているかという観点でサイバーセキュリティを考えることも重要です。

本書では米国立標準研究所[3]（以降、本書では NIST）が 2020 年に発行した「PRIVACY FRAMEWORK ver1.0 [2]」（以降、本書ではプライバシーフレームワーク）を参照し、スマートシティにおけるサイバーセキュリティの領域とプライバシー保護の領域が重なる部分（図１）について記載しています。プライバシー保護の観点でサイバーセキュリティが実施するべきポイントを知ることでスマートシティにおけるプライバシーについて理解するきっかけとなることを目的としています。

---

[1] 例えば、< https://www8.cao.go.jp/cstp/stmain/r4_smartcity.html>など

[2] 内閣府　「Society 5.0 とは」< https://www8.cao.go.jp/cstp/society5_0/>

[3] National Institute of Standards and Technology, NIST. アメリカ合衆国の国立の計量標準研究所。サイバーセキュリティやプライバシーなどに関する文書を発行している。

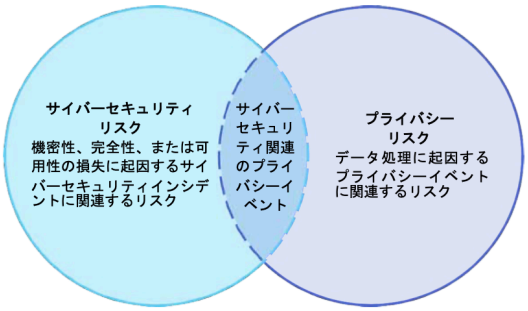

図 1-1 サイバーセキュリティとプライバシーの関係(出典:PRIVACY FRAMEWORK ver1.0)

1.2 想定読者

以下のような方を読者として想定しています。

『スマートシティへの取り組みをこれから開始する企業(サービス提供者・データ提供者)の担当者であり、プライバシーに関するサイバーセキュリティの理解を深めたい方』

スマートシティにおけるサーバーセキュリティの領域についての理解を深めるためには総務省が 2021 年 6 月に発行した「スマートシティセキュリティガイドライン(第 2.0 版)」[3]」を参照することを推奨します。本書ではセキュリティガイドラインで多く触れられていないプライバシーに関するサイバーセキュリティについて記載しています。

1.3 著作権及びその他すべての知的所有権

「データ利活用型スマートシティにおけるセキュアなデータマネジメント(以下、「本作品」)」に関する著作権及びその他すべての知的所有権は、「情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 5 期生プロジェクト「データ利活用型スマートシティにおけるセキュアなデータマネジメントについて(以下、「本プロジェクト」)」に帰属します。

1.4 免責事項

本プロジェクトは、本作品について品質的にも法律的にも何らの保証もしません。また、本プロジェクトは、本作品の使用に起因して生じるすべての直接的、間接的、付随的又は結果的損害、利益の損失等に関し、法的原因の如何を問わず何らの責任も負いません。

1.5 注意事項

本作品の内容は本プロジェクトの見解に基づいております。
独立行政法人情報処理推進機構（IPA）および作成者の所属企業の見解を反映するものではありません。

第2章　　スマートシティについて

2.1 これからのスマートシティとは

内閣府から 2020 年 3 月に「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［4]」（以降、本書ではスマートシティリファレンスアーキテクチャ）が発行されスマートシティを実現するための構成要素と構成要素間の関係性について記載されています。その中でスマートシティは「都市の抱える諸課題に対して、ICT 等の新技術を活用しつつ、マネジメント（計画、整備、管理・運営等）が行われ、全体最適化が図られる持続可能な都市または地区」と定義されています。

これまで日本国内ではスマートグリッドのようなエネルギーの効率活用といった取り組みを単一都市内で行う「個別分野特化型」が多かったですが、近年では政府の活発な取り組みもあって IoT、AI、ビッグデータ等の ICT の発展の恩恵を受けつつ都市管理の複数分野にまたがった「分野横断型」の開発に拡大しています[4]。

スマートシティに限らずデータ利活用が注目されていますが、取り扱われるデータが個別分野という限られたサービスの中だけで処理されるのであれば生み出される価値には限界があります。様々な分野間で実施されるサービスが横断的にデータを活用することで価値を最大化させる事ができるようになるという考えから分野横断型のスマートシティが注目されているのです。

また、スマートシティにおいてはオープンデータが注目されておりその中にパーソナルデータも含まれる事が予想されることについては触れましたが、こうしたデータを安全に、透明性を持って横断的なデータのやりとりを行うためにはそのためのデータ連携基盤が必要となります。スマートシティにおいてデータ連携基盤となるのが都市 OS です。

要約するとこれからのスマートシティとは都市 OS と呼ばれるデータ連携基盤が整備された中で分野横断的にデータをやりとりし、データの持つ価値を最大化することで都市の課題解決や新たな価値を生むサービスにより豊かさを作り出す未来の街の姿と言えます。

---

[4] 例えば、国土交通省「スマートシティの実現に向けて【中間とりまとめ】」<https://www.mlit.go.jp/common/001249775.pdf>

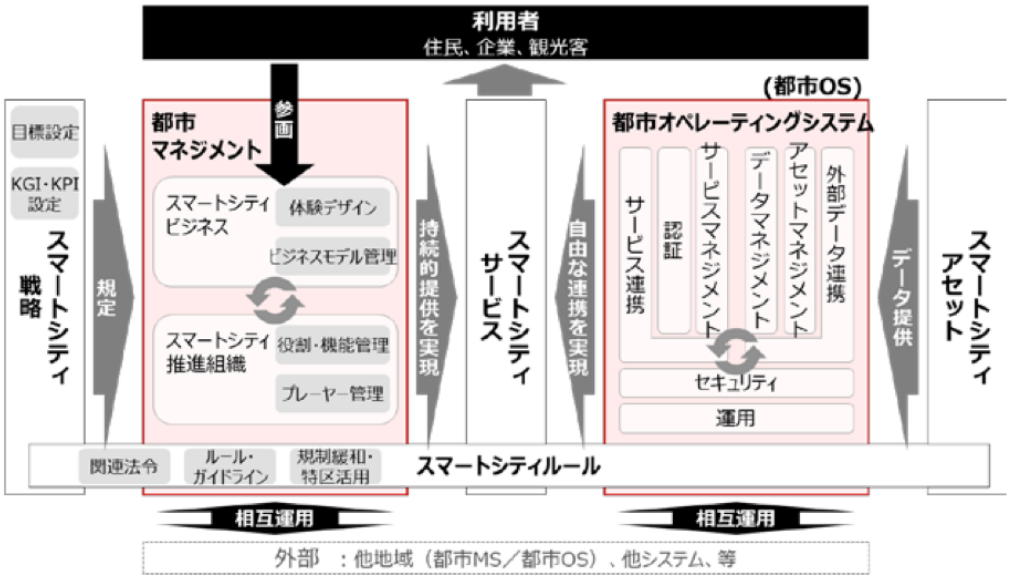

図 2-1 スマートシティリファレンスアーキテクチャ全体像[5]

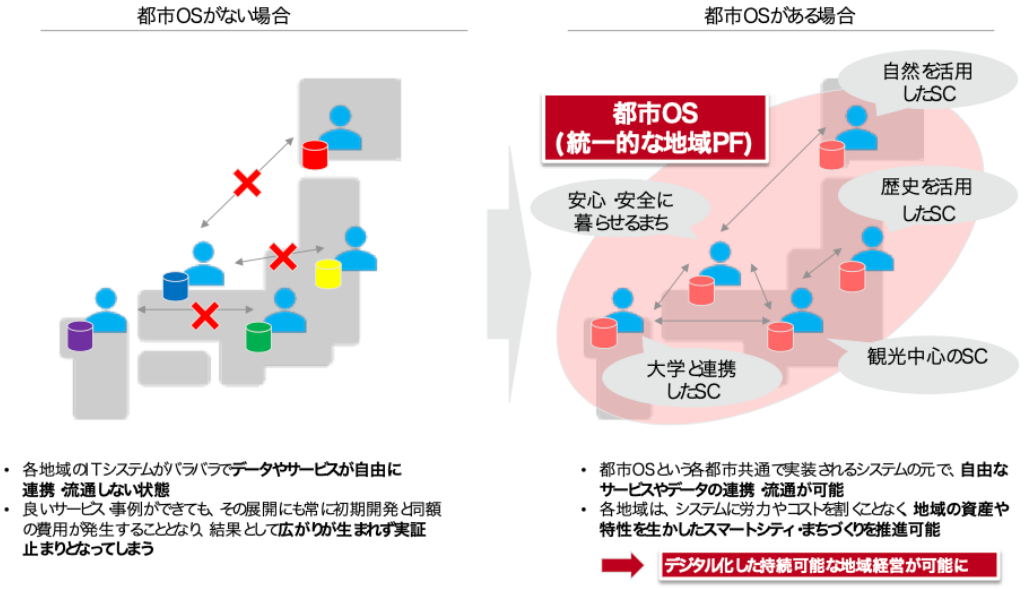

図 2-2 都市 OS で実現するスマートシティ社会（都市 OS が果たす役割）[5]

[5] 出典：内閣府, “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. [4]

2.2 スマートシティにおけるマルチステークホルダーについて

スマートシティではその推進に多様な主体が関わり、セキュリティとプライバシーまたその２つの重なる領域について考える際には登場人物を整理する必要があります。本書では「スマートシティリファレンスアーキテクチャ［4]」を前提とし、リファレンスアーキテクチャで使用されている関係主体に関する用語については同一の意味を持って使用します。

用語	意味・解説
サービス利用者（受益者）	スマートシティサービスの提供の対象として､その提供ニーズを有する主体のこと。なお､提供されるサービスによってはサービス利用者がデータを提供することもある。
サービス提供者	（サービス利用者に対して）スマートシティサービスを提供する主体。
推進主体	スマートシティ全体の推進・運営に関して責任・決定権・主導権を持つ主体｡本書においては地域協議会や地方公共団体などが推進主体に該当し、当推進主体から業務委託を受けるベンダ等は含まない。
投資家・データ等提供者	（時に対価を目的として)スマートシティやスマートシティサービスの開発・運営に必要となるリソースを提供する主体。
都市 OS ベンダ	「推進主体」からの業務委託等を受け、都市 OS の構築・運用を実施する事業者を指す。
IoT 機器ベンダ	「データ提供事業者」や「サービス提供者」に対して IoT 機器を提供する事業者を指す。
セキュリティサービス事業者	「推進主体」からの業務委託を受け、スマートシティの全体または一部のセキュリティ監視等のセキュリティに関するサービスを実施する事業者を指す。

2.3 用語一覧

本節では、スマートシティのセキュリティとプライバシーを考える上で必要な用語を説明する。

用語	意味・解説
個人プライバシーポリシー	個人が自己の指向に従ってパーソナルデータの取り扱い方法を設定したもの。（単にポリシーと記載されている場合は個人プラ

	イバシーポリシーと企業プライバシーポリシーの両方の意を含むものとしています）
企業プライバシーポリシー	規制・法律・法律・リスク・業務上の要件から設定したプライバシーリスクを管理するためのもの。（単にポリシーと記載されている場合は個人プライバシーポリシーと企業プライバシーポリシーの両方の意を含むものとしています）
API	Application Programming Interface：アプリケーション・プログラミング・インターフェース ソフトウェアやプログラム、Web サービスの間をつなぐインターフェース
OAuth	認可を行うためのプロトコル。 2012 年に制定された OAuth2.0 が最新。
OpenID Connect	認証を行うためのプロトコル。 2014 年に OAuth の拡張仕様として制定された
アーキテクチャ	建築学における建築の様式・工法・構造のこと。転じて、基本設計や共通仕様、設計思想などを指す。
オープンデータ	国、地方公共団体および事業者が保有する官民データのうち、国民誰もがインターネット等を通じて容易に利用（加工、編集、再配布等）できるよう公開されたデータ。
オプトイン	加入や参加、許諾、承認などの意思を相手方に示すこと。スマートシティの文脈においては、個人情報の収集や利用などを承諾する手続きを指すことが多い。（⇔オプトアウト）
可用性	許可された者が必要なときにいつでも情報にアクセスできるようにすること。
完全性	保有する情報が正確であり、完全である状態を保持すること。
機密性	許可された者だけが情報にアクセスできるようにすること。
都市 OS	スマートシティの基礎プラットフォーム。API を用いデータや認証等のやり取りを行うことで、スマートシティ間でサービスやデータが相互接続し、流通の効率化を図ることが出来る。
認可	特定の利用者や特定の条件を満たす状況下でデータへのアクセス権限やシステムの操作権限を与える（権限外の利用を拒否する）こと。
認証	システムを利用しようとする者が誰なのかを調べ、事前に登録した利用者本人であることを確かめる手続き。

2.4 本書におけるスマートシティについて

「スマートシティリファレンスアーキテクチャ［4]」では、データ蓄積方式とデータ分散方式が紹介されていますが、本書においてはデータ分散方式のスマートシティを主に紹介しています。都市 OS はデータを蓄積せずに、他システム（データ提供者）の持つデータが都市 OS により管理されるものをデータ分散方式のスマートシティとしています。ここでいう管理とはデータの所在を記したデータカタログやデータへのアクセスコントロールを行うデータ仲介といった機能です。

分散されたデータを都市 OS によりつなげることで一つのビッグデータとし、いつでもデータへのアクセス・分析が可能となることで課題解決につながるサービスを生み出すことのできるスマートシティが主流となると本書では考えています。

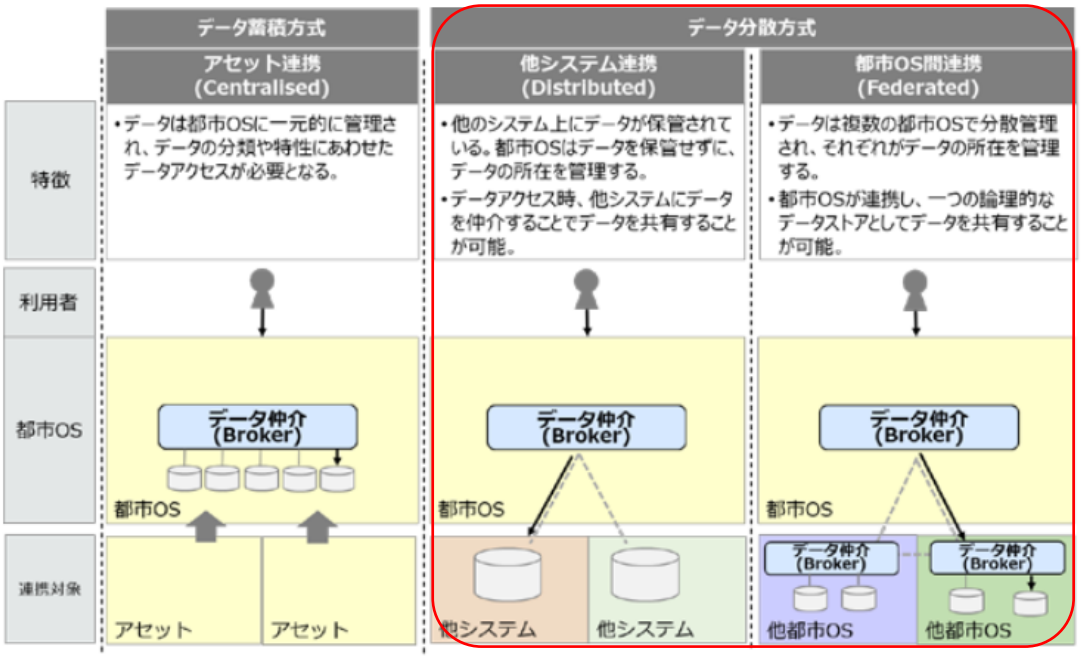

図 2-3　都市 OS の連携方法によるデータ仲介例[6]

[6] 出典：内閣府, “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. [4]

第3章　　プライバシーについて

3.1 プライバシーと企業が認識すべきプライバシーリスクとは

プライバシーついての考え方は社会や時代とともに変化することもあり、明確に定められた定義がありません。総務省・経済産業省が発行する「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 [5]」では次のように書かれています。

プライバシーは従来、「私生活をみだりに公開されない法的保証ないし権利」や「放っておいてもらう権利」として考えられていたものが、情報通信技術が発展し、情報プライバシーという概念が生まれてからは、個人の権利を尊重することの必要性の理解が浸透してきたことも相まって「自己情報のコントロール」などに発展していった。

本書でもプライバシーを「自己情報のコントロール」として定義していますが、時代とともに捉え方が変化するものであることがプライバシーを考えることを困難なものにしており、プライバシーの問題が何かが見えづらくなっていると言えます。しかし、2 章で記述した通りデータ利活用型スマートシティにおいて取り扱うオープンデータには(3.2 で述べる)パーソナルデータも含まれることから、プライバシーを考えずにデータ提供者・サービス提供者がビジネスを進める事ができません。企業が保有するパーソナルデータを処理する中で問題が発生した際にプライバシーリスクが発生する可能性があることを企業は認識する必要があります。

3.2 パーソナルデータとデータマネジメントについて

総務省・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 [5]」によれば、パーソナルデータとは「個人情報保護法の個人情報だけではなく、個人に関連するあらゆる情報」を指します。一般的なサイバーセキュリティにおいて CIA（C:機密性、I：完全性、A：可用性）が語られますが、スマートシティではパーソナルデータを自組織外へ提供することから機密性の考え方でデータを漏洩させないという考え方では不足があります。機密性だけでなく自組織の手から離れたデータが個人の意図しない取り扱いをされないようにデータを適切にコントロールするという考え方が重要となります。パーソナルデータの指す個人が設定した取り扱いのポリシーに基づいてコントロールするということを本書では「データマネジメント」として説明します。

3.3 プライバシーリスクがスマートシティの障害となった過去事例

海外でもスマートシティの取り組みは進められていますが、プライバシーリスクが顕在化した事例があります。Google の子会社である Sidewalk Labs が 2017 年にカナダのトロントで推進したスマートシティの取り組みは非常に注目を集めました [6]が、2020 年にはプロジェクトの撤退が発表されました。撤退の理由はいくつかありましたがその一つとして挙げられたのがプライバシーリスクです [7]。Sidewalk Labs がプロジェクトを進めていく途中で、スマートシティで収集されるデータは必要以上の過剰なものであるという市民団体からの反発と、市民がプライバシーを決定する権利を与えられていないという主張がありました。Sidewalk Labs はその主張に対して当スマートシティにおけるプライバシーポリシーやデータ利活用により市民が得られる利益について説明を行いましたが市民の反発を抑える事ができず撤退という結果につながりました。

この過去事例からもプライバシーに関するポリシーを設定する権利を有するのはスマートシティに参加する市民であるという認識を企業が持つことと、街づくりの初期段階からスマートシティに関わるステークホルダーの間で合意形成を行うことが重要である事がわかります。

3.4 プライバシーフレームワークと本書の位置付けについて

組織がプライバシーリスクを管理する際に有効なのがプライバシーフレームワーク [2]です。プライバシーフレームワークは「コア」「プロファイル」「ティア」の 3 つの要素で構成され、コアはプライバシーリスク管理の機能について主要なカテゴリーとサブカテゴリーに分割しています。(表 3-1)

コアで定義された機能である「特定（Identify-P)」「統治（Govern-P)」「制御（Control-P)」「防御（Protect-P)」はデータ処理に起因するプライバシーリスク管理に利用でき、その中でも「防御（Protect-P)」は特にサイバーセキュリティ関連のプライバシーイベントに関連するリスクの管理に重点をおいているとしています。4 章では「防御（Protect-P)」の機能のカテゴリとマートシティにおける管理策をマッピングさせています。

ただし、組織が実施すべき管理策は「防御（Protect-P)」だけではないことに注意してください。また、プライバシーフレームワークは機能の全てを実施することを求めてはおらず、組織に必要な機能やカテゴリー同士を組み合わせた管理策を選択するためのものとして作成されています。

表 3-1 プライバシーフレームワーク機能一覧[7]

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID-P	（特定）Identify-P	ID.IM-P	棚卸しとマッピング
		ID.BE-P	ビジネス環境
		ID.RA-P	リスク評価
		ID.DE-P	データ処理エコシステムのリスク管理
GV-P	（統治）Govern-P	GV.PO-P	ガバナンスポリシー、プロセス、手順
		GV.RM-P	リスク管理戦略
		GV.AT-P	意識向上とトレーニング
		GV.MT-P	監視と確認
CT-P	（制御）Control-P	CT.PO-P	データ処理のポリシー、プロセス、手順
		CT.DM-P	データ処理管理
		CT.DP-P	処理の分離
CM-P	（通知）Communicate-P	CM.PO-P	コミュニケーションポリシー、プロセス、手順
		CM.AW-P	データ処理の認識
PR-P	（防御）Protect-P	PR.PO-P	データ保護のポリシー、プロセス、手順
		PR.AC-P	アイデンティティ管理、認証、アクセス制御
		PR.DS-P	データセキュリティ
		PR.MA-P	メンテナンス
		PR.PT-P	保護技術
DE	（検知）Detect	DE.AE	異常とイベント
		DE.CM	セキュリティの継続監視
		DE.DP	検出プロセス
RS	（対応）Response	RS.RP	対応計画
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	緩和
		RS.IM	改善
RC	（復旧）Recover	RC.RP	復旧計画
		RC.IM	改善
		RC.CO	コミュニケーション

[7] 出典：米国立標準技術研究所（NIST），“The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,” 2020.

第4章　　スマートシティにおけるセキュアなデータマネジメントについて

4.1 スマートシティにおけるプライバシーリスクとは

プライバシーが時代とともに変化するものであることからプライバシーリスクを捉えることが難しくしている一因となっていますが、具体化できなければ理解を深めることができません。ここでは一例としてパーソナルデータの取り扱いの中で設定されるポリシーの内、公開範囲についてデータマネジメントが適切に行われなかった際に顕在化するリスクについて取り上げてみます。

例えば A さんが自分の趣味についての情報を、所属するとあるコミュニティ内のみに限定し公開しているとします。それはパーソナルデータを公開する代わりに個人にターゲットされた有益な情報を受け取ることのできるサービスを利用するためです。しかし、企業のデータマネジメントの中で問題のあるデータ処理を行ってしまいコミュニティ外の人間に知られてしまった場合、自己情報のコントロールが出来ない状態となりプライバシーリスクが顕在化されたと考えることが出来ます。

このことから機密性に基づきデータを外に出さないことだけではなく、パーソナルデータが指す個人の設定した取り扱いの範囲内でデータマネジメントすることが組織のプライバシーリスク管理において重要であると考えることが出来ます。

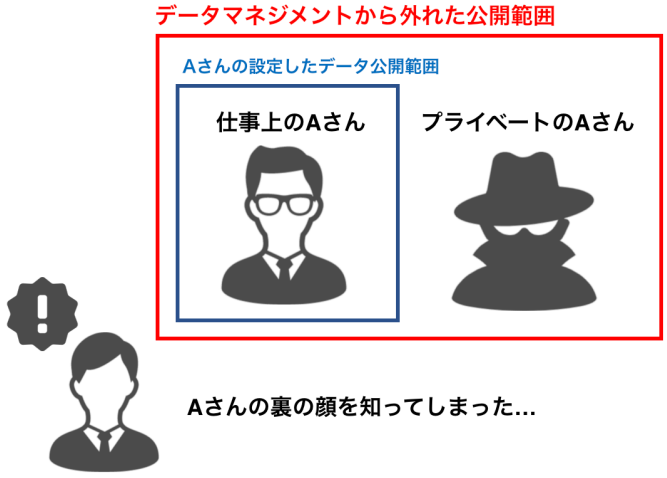

図 4-1　データ公開範囲がコントロール出来ない際に起きうるプライバシーリスク

4.2 スマートシティデータアーキテクチャ

プライバシーリスクは企業がパーソナルデータの処理で問題を起こした際に顕在化します。そのため企業がプライバシーリスク管理を行う際にはデータアーキテクチャ（プライバシーフレームワーク [2]ではデータマップと表現されている。）を用いてステークホルダー間でデータの所在と処理について共通認識を持つことが有効になります。データアーキテクチャとはデータの所在が理解でき、データ処理機能と個人とシステム、サービス間のデータの流れを示すものです。図 6 はデータ分散方式のスマートシティにおけるデータアーキテクチャの一例となります。

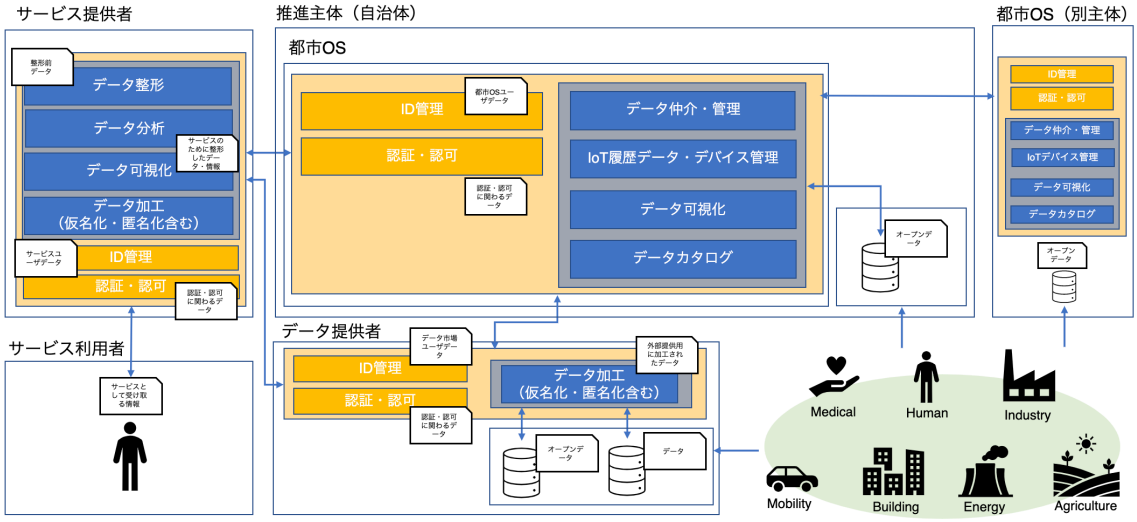

図 4-2 データ分散方式スマートシティにおけるデータアーキテクチャ

4.3 スマートシティで取り組むべきリスク管理

本項ではプライバシーフレームワーク [2]のコアで示された「防御（Protect-P）」機能のカテゴリーがスマートシティにおけるプライバシーリスク管理において果たす役割について説明しています（表 4-1）。各カテゴリーの説明には別の機能のカテゴリーの内容と組み合わせたものも含まれます。

表 4-1　プライバシーフレームワーク「防御（Protect-P）」機能カテゴリー一覧　（出典：米国立標準技術研究所（NIST），“The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,” 2020.）

PROTECT-P（PR-P）：開発と実装	データ保護のポリシー、プロセス、手順（PR.PO-P）：セキュリティやプライバシーに関するポリシー（	PR.PO-P1：情報技術のベースライン構成の作成や維持にあたっては、セキュリティ原則（最小権限の原則など）を組み込みます。
適切なデータ処理の保護。	データ処理エコシステムにおける目的、範囲、役割と責任、管理責任など）、プロセス、手順を維持し、データ保護の管理のために利用します。	PR.PO-P2：構成変更管理プロセスを確立し、導入します。
		PR.PO-P3：情報のバックアップを実行、維持、検査します。
		PR.PO-P4：組織の資産の物理的な運用環境に関するポリシーと規制を満たします。
		PR.PO-P5：保護プロセスを改善します。
		PR.PO-P6：保護テクノロジーの有効性を共有します。
		PR.PO-P7：対応計画（インシデントレスポンスとビジネス継続性）と復旧計画（インシデント復旧と災害復旧）を確立、導入、管理します。
		PR.PO-P8：対応計画と復旧計画をテストします。
		PR.PO-P9：人事の管理手法に、プライバシー手順を含めます（プロビジョニング解除、人事スクリーニングなど）。
		PR.PO-P10：脆弱性管理計画を作成、実装します。
	アイデンティティ管理、認証、アクセス制御（PR.AC-P）：データや端末へのアクセスを、承認された個人、プロセス、端末に限定し、不正アクセスのリスク評価と整合した状態で管理します。	PR.AC-P1：IDと資格情報は、承認された個人、プロセス、端末に対して発行、管理、検証、失効、監査します。
		PR.AC-P2：データや端末への物理的なアクセスを管理します。
		PR.AC-P3：リモートアクセスを管理します。
		PR.AC-P4：アクセス許可と権限の管理に、最小限の特権と職務分掌の原則を取り入れます。
		PR.AC-P5：ネットワークの完全性を保護します（ネットワークの分離、セグメント化など）。
		PR.AC-P6：個人と端末は、クレデンシャル認証に基づいて検証され、トランザクションのリスク（個人のセキュリティリスク、プライバシーリスク、その他の組織的なリスクなど）に対応します。
	データセキュリティ（PR.DS-P）：データを	PR.DS-P1：保存データを保護します。
		PR.DS-P2：転送中のデータを保護します。
	組織のリスク戦略に沿って管理し、個人のプライバシー保護や、データの機密性、完全性、可用性の維持を実現します。	PR.DS-P3：システム/製品/サービスや関連データについて、削除、転送、廃棄中も、正式に管理します。
		PR.DS-P4：可用性を維持するための十分な容量を維持します。
		PR.DS-P5：データ漏洩に対する保護を実装します。
		PR.DS-P6：完全性チェックメカニズムを利用して、ソフトウェア、ファームウェア、情報の完全性を検証します。
		PR.DS-P7：開発環境とテスト環境を、本番環境と分離します。
		PR.DS-P8：完全性チェックメカニズムを利用して、ハードウェアの完全性を検証します。
	メンテナンス（PR.MA-P）：ポリシー、プロセス、手順に沿って、システムのメンテナンスと修理を行います。	PR.MA-P1：承認され管理されたツールを用いて、組織の資産の保守と修復を実行し、対応履歴を記録します。
		PR.MA-P2：不正アクセスを防止する方法で、組織の資産のリモート保守を承認、記録して行います。
	保護技術（PR.PT-P）：関連するポリシー、プロセス、手順、契約に基づき技術的なセキュリティソリューションを管理し、システム/製品/サービスや関連データのセキュリティと復元性を確保します。	PR.PT-P1：リムーバブルメディアを保護し、使用にあたってはポリシーに基づく制限を行います。
		PR.PT-P2：基本的な機能のみを提供するようシステムを構成することで、最小限の機能の原則を組み込みます。
		PR.PT-P3：通信と制御ネットワークを保護します。
		PR.PT-P4：通常時と悪条件下での回復性の要件を満たすため、メカニズム（フェイルセーフ、ロードバランシング、ホットスワップなど）を実装します。

4.3.1　データ保護のポリシー、プロセス、手順

【主な対象者：サービス提供者、データ提供者、推進主体】

データを取り扱うにあたって、プライバシーに関するポリシーを明確にしているかを確認する必要があります。

（関連するカテゴリー：CT.PO-P、PR.PO-P）

ポリシーの一例としては下記のようなものがあります。

・データの種別

・データの取得方法

・データの管理方法

・データの公開範囲（第三者提供を含む）

・データの利用目的

これらのポリシーを明確にし、サービス利用者に認識を持ってもらうための手段と責任を持つことが重要です。企業はポリシーのテンプレートを作成し、個人が自己の指向に従ってポリシーテンプレートから自己の情報に関する取り扱い方法や設定を選択できるように準備する必要があります。企業がデータマネジメントを行うためには、個人プライバシーポリシーを設定する事から始まります。また、企業プライバシーポリシーとテンプレートは参加するスマートシティの定めるポリシーと乖離がないことも確認してください。

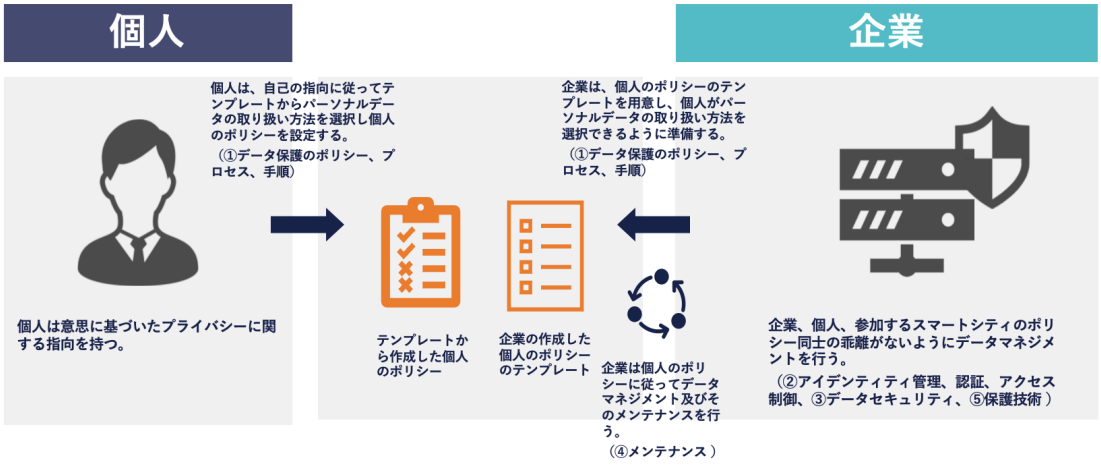

図 3 パーソナルデータ取り扱いポリシー設定に関する個人と企業の関係

3章で紹介した通り、Google のスマートシティに関する取り組みが失敗に終わった原因の1つに市民と都市、企業間でパーソナルデータの取り扱いに関するポリシーの合意形成が取れないままにサービスを進めようとしたことにあります。市民とスマートシティの推進主体が定めたデータ保護方針を元に自組織（サービス提供者、データ提供者）が方針

に沿ったデータマネジメントをおこなっているかを確認してください。

例えばソフトバンクはデータ利活用を進めるためにユーザ自身のプライバシーの理解を促すためプライバシーセンターを立ち上げるという取り組みを行なっています。そこではパーソナルデータの利用状態の確認や利用範囲の変更を個人ができる仕組みを提供しています。これは個人がサービスに登録した時点で得られる同意を永続的に取り扱うのではなく、常に変化するポリシーに対応するための体制をとっているという事です。

図 4-4 ソフトバンクによるパーソナルデータ取り扱いポリシー設定への取り組み事例[8]

4.3.2 アイデンティティ管理、認証、アクセス制御

【主な対象者：推進主体、サービス提供者、データ提供者】

パーソナルデータの取り扱い方針の一つとしてあげられるデータの公開範囲のコントロールのために認証・認可によるアクセス制御が適切に設定されているかを確認する必要があります。

（関連するカテゴリー：PR.AC-P）

分散方式スマートシティでは様々な場所にあるデータが都市 OS によりつながることでデータ市場を作り出すという考え方があります。データ市場ではカタログに記載されたデータについて都市 OS を通したデータのやりとりを行う場合と API によりデータのやりとりを行う場合の２通りの流通経路が考えられます。どちらの場合でもデータへのアクセスは、許可された組織、個人に限定されているかを確認してください。

---

8 <https://www.softbank.jp/privacy/>

4.3.2-1 都市 OS を通したデータのやりとりを行う場合

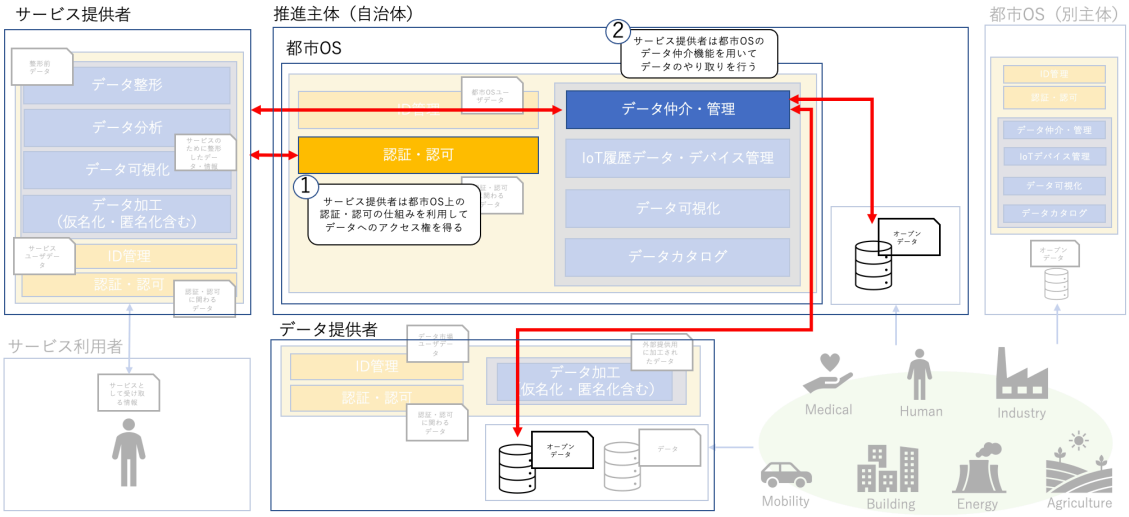

図 4-5 都市 OS を通したデータのやりとり

スマートシティにおいて推進主体やデータ提供者の持つオープンデータは都市 OS によってデータの所在管理が行われデータ仲介機能によって提供されます。一部のデータは申請者のみが利用できるようになっている場合がありますが、その際は都市 OS が提供する認証・認可の仕組みを利用することが出来ます。データ連携基盤上でポリシーを基とした公開範囲の設定が行われているか確認してください。

4.3.2-2　API を用いたデータのやりとりを行う場合

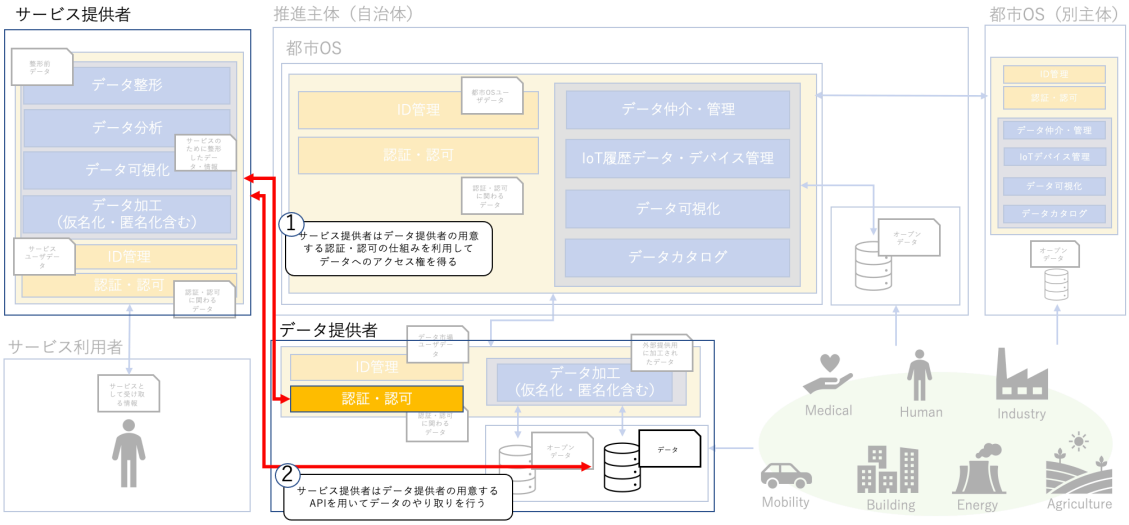

図 4-6 API を用いたデータのやりとり

データ提供者とデータ利用者が直接 API によるやりとりを行う場合にはデータ提供事業者が用意する API で認証認可によるアクセス制御を考える必要があります。API はデータ利活用の促進に役立ちますが、外部から API エンドポイントがアクセスできることから近年サイバー攻撃者の標的になっている領域です。WEB アプリケーションのセキュリティについてのドキュメントを発行している OWASP[9]が 2019 年に API Security Top 10 を発表しており、API のセキュリティについて理解を深めるために役に立ちます。以下ではその中から認証認可に関わる内容を抜粋して紹介しています。

・認証を通過したユーザが全てのレコードにアクセスできるようになっていないか
・脆弱な認証を使用していないか（API キーのような ID のみの認証）
・データの過剰な公開がされていないか
・不要な認証情報を削除せずに残していないか

また、データアーキテクチャ上ではサービス提供者やデータ提供者は ID 管理や認証認可仕組みを企業内に持つという提示を行っていますが、必要に応じてソーシャルログインを用いた認証認可の仕組みを導入することもできます。これは認証認可に必要な ID 情報を自組織内に保持しないということです。ID 情報がサービスに必要でない場合には、それを保持しない事が組織のプライバシーリスクを低減させることに役立ちます。

[9] Open Web Application Security Project の略称。

4.3.3　データセキュリティ

【主な対象者：サービス提供者、データ提供者】

パーソナルデータの管理は個人のプライバシーを保護するために、データの機密性、完全性、可用性を維持出来ているかを確認してください。

（関連するカテゴリー：PR.DS-P）

データセキュリティの領域について必要な管理策を確認するためには総務省から発行されているスマートシティセキュリティガイドライン参照することを推奨します。スマートシティセキュリティガイドラインでは「ガバナンス」「サービス」「都市 OS」「アセット」の４つのカテゴリに分類されており、それぞれのカテゴリにおけるセキュリティの考え方、対策について整理されています。表１に機密性、完全性、可用性それぞれを確保するためのセキュリティ対策について示します。

表 4-2：機密性、完全性、可用性確保のためのセキュリティ対策一覧
出典：スマートシティセキュリティガイドライン（第２版）を参考に筆者作成

機密性･完全性･可用性の分類	セキュリティの考え方と対策	カテゴリ
機密性	組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取決める	ガバナンス　都市 OS
	情報を適切な強度の方式で暗号化して保管する	サービス　都市 OS
	IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する	サービス　都市　OS アセット
	情報を送受信する際に、情報そのものを暗号化して送受信する	サービス　都市 OS
	送受信する情報データ、保管データする情報の暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する	サービス　都市 OS
	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する	サービス　都市 OS
	IoT 機器やソフトウェアが正規品であることを定期的（起動時等）に確認する	ガバナンス　サービス　都市　OS　アセット

	データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する	ガバナンス
可用性	サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース（例:ヒト、モト、システム）を確保する	サービス 都市 OS アセット
	IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う	サービス 都市 OS アセット
	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する	アセット
完全性	IoT 機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する	サービス 都市 OS アセット
	送受信・保管する情報に完全性チェックメカニズムを使用する	ガバナンス サービス 都市 OS アセット
	ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する	都市 OS アセット
	計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する	ガバナンス アセット

4.3.4　メンテナンス

【主な対象者：データ提供者、推進主体】

個人が設定したポリシーに従ってデータマネジメントが行われているかを確認してください。

（関連するカテゴリー：CT.PO-P、CT .DM-P、C M.PO-P、PR .MA-P）

個人のプライバシーに対する指向は日々変化します。また、社会動向、技術動向の変化によっても個人のプライバシーに対する指向が変わる可能性があります。さらに、法規制により個人のプライバシーの取り扱いが変化する可能性もあります。

そのため、4.3.1 で明確にした個人ポリシーテンプレートもそれらの変化に適応させて行く必要があります。すなわち、個人のプライバシー指向を満たせるように、企業は個人ポリシーテンプレートのメンテナンスを行い、プライバシー管理システムの更新を行っていく必要があります。

4.3.5　保護技術

【主な対象者：サービス提供者、データ提供者、推進主体】

技術的なセキュリティ及びプライバシー対策は定められたポリシーと一致するように管理されているかを確認してください。

（関連するカテゴリー：CT.DP-P、PR .PT-P）

参加する都市が形成するプライバシーのポリシーや個人プライバシーポリシー、企業プライバシーポリシーによってはプライバシーリスク管理のために、①～④のカテゴリーで示されたものだけでなく追加の対策が必要な場合もあります。

以下にプライバシー保護技術の一例を紹介します。あくまでも一例でありポリシーと一致したデータマネジメントを行うためには紹介した以外の技術も検討した上で選択する必要があります。

保護技術	技術内容
デジタル署名	送信されたデータが送信者のデータであるかを証明するための技術であり、公開鍵暗号を応用した技術。 実現方式は DSA や RSA などが存在する。
ブロックチェーン	複数技術（P2P ネットワーク、電子署名、ハッシュ関数など）を組み合わせた技術、一般的な中央集権型ではなく分散型のシステムであり、高いセキュリティを担保できる技術。
秘密計算	データを秘匿化したまま計算ができる技術。秘密分散方式、準同型暗号方式、ハードウェアによる実装などの方式がある。
差分プライバシー/ 局所差分プライバシー	分析データから個人データを再識別が困難になるように、データにノイズを追加して処理する技術。生の個人データを収集したあとでノイズを追加する場合を差分プライバシー、個別の個人データにノイズを追加してから収集する場合を局所差分プライバシーと呼ぶ。
仮名化、匿名化	パーソナルデータに対してマスキングなどを実施し、個人特定が不可能となるように加工する技術であり、特定の個人のデータから個人情報を除き、その情報に別の識別情報を付与する技術。
連合学習	自組織内のデータだけでなく他組織のデータも利用して AI の精度向上を図りたい場合に、データそのもののやりとりはせずに組織毎で学習したモデルやパラメータのみを共有し統合する技術。

＜差分プライバシー/局所差分プライバシー：Apple の事例[10]＞

スマートフォンでメールやチャットを利用する際、メッセージの変換を行うときに、予測変換候補が提案される場合がある。

どのような予測変換候補を提案すればよいかを検討するために、スマートフォンのメーカーは、ユーザーの用語の利用頻度や利用される文脈などの情報を収集・把握したい。しかし、それらの情報はユーザーのメッセージというプライベートな情報であるため、ユーザーのプライバシーを侵害してしまう可能性が高く、安易に情報を収集できない。

一方、予測変換候補の提案を検討するに当たり、ユーザー個別のメッセージは特に必要なく、統計的な情報を得られれば十分である。

そこで、差分プライバシーと呼ばれる手法により、ユーザーの情報にノイズを追加して収集することで、収集したデータからの個別のユーザー、もしくは個別のユーザーの情報の識別を防いでいる。統計的に十分なデータ量があれば、個別のユーザー、もしくは個別のユーザーの情報を識別できない状態のまま、十分なデータ量を集めて、スマートフォンメーカーが行いたい予測変換候補の提案を検討することができる。

＜連合学習：Google の事例[11]＞

差分プライバシーの例で述べたとおり、スマートフォンのメーカーは、ユーザーの用語の利用頻度や利用される文脈などの情報を収集・把握したい。

Google では、適切な予測変換候補の提示用の機械学習（機械学習モデル）について、連合学習[12]と呼ばれる手法により、ユーザーのメッセージというプライベートな情報をスマートフォンから出さずに、機械学習モデルの改善を行っている。具体的には、スマートフォンはクラウド上に存在する機械学習モデルをダウンロードする。ダウンロードしてきた、スマートフォン上の機械学習モデルにユーザーのメッセージなどデータから学習させ、機械学習モデルを改善させる。スマートフォン上の機械学習モデルの改善点を要約したデータを作成し、そのデータをクラウド上に送信して共有する。クラウド上の機械学習モデルはその共有されたデータをもとに更新される。クラウド上の機械学習モデルは他のユーザーの更新によりすぐに平均化される。すべての訓練データ（今回の場合はユーザーのメッセージなど）はスマートフォン上に残るため、ユーザーのプライバシーは確保される。

＜秘密計算（準同型暗号方式）：エストニア情報通信技術協会の事例[13]＞

---

[10] ＜https://www.apple.com/jp/privacy/control/＞

[11] ＜https://support.google.com/gboard/answer/9334583?hl=ja＞

[12] フェデレーション ラーニングやフェデレーテッド ラーニングと呼ばれる場合もある

[13] NRI デジタル コラム「データ活用を促進する秘密計算技術！その事例と活用 5 類型」＜https://www.nri-digital.jp/tech/20210825-5528/＞より

エストニアは IT 先進国として知られている。そのエストニアで、IT 系を専攻する大学生の落第率の高さが問題となっている。落第率の高さの理由として「好調な IT 業界による過剰なアルバイト採用が学生の落第を招いている」という仮説が立てられ、エストニア情報通信技術協会（ITL）が調査に乗り出した。

学生のアルバイト量と落第率の相関は、教育科学省が保持する学生データと、税務・関税局が保持する労働者・納税データを掛け合わせれば簡単に割り出すことができる。しかし、個人情報保護の観点からそれぞれのデータを共有することは許されなかった。

ITL はこの問題に対し、秘密計算という手法を採用した。学生データと労働者・納税データを暗号化したまま掛け合わせることで、学生個々人のプライバシーを保護しつつ、学生のアルバイト量と落第率の相関を分析することができた。

＜仮名化・匿名化：神戸市の事例[14]＞

兵庫県　神戸市ではオープンデータの蓄積とそれを有効活用した住民サービスの向上に取り組んでいる。データ利活用の取り組みにおいては生データの方が分析する際には優れているが、個人が特定されないように匿名化をおこなったデータを用いて分析した場合に精度の差がどの程度出るかの実証実験が神戸市と企業の共同で行われた。

住民基本台帳に基づく統計情報のサンプルデータに対して k-匿名化やその他の処理をおこなったデータを用いて分析をかけたところ、傾向把握のような結果を求める場合には十分な精度であることを確認したとされている。

＜ブロックチェーン：加賀市の事例[15]＞

ブロックチェーンとその関連技術は耐改ざん性と透明性の担保に活用できるとして注目されている。加賀市は 2018 年に「ブロックチェーン都市宣言」をするなどブロックチェーンをはじめとした技術を用いた利便性が高く安全なデジタル社会の実現を目指している。ブロックチェーンとその関連技術を用いたプライバシーへの取り組みは未だ実証実験の域を出ないものが多い段階ではあるが、加賀市は取り組みの一環として企業と共同で市の政策に関する電子投票（インターネット投票）の実現に向けて検討をおこなっている。

---

[14]日立ソリューションズ　ニュースリリース「神戸市、オープンデータ推進に向けた匿名化の実証実験を実施」
<https://www.hitachisolutions.co.jp/company/press/news/2021/0316.html>より

[15] 石川県加賀市、xID、LayerX、市の制作に関する電子投票実現に向けた連携協定を締結
<https://prtimes.jp/main/html/rd/p/000000026.000037505.html>より

4.4 プライバシー残存リスクとリスクの許容について

4.3 節ではプライバシーフレームワーク [2]を用いたプライバシーリスク管理策について記載しましたが、データ利活用型スマートシティにおいて組織がデータを保持または処理する限りデータを取り扱う事で発生するプライバシーリスクがゼロになることはありません。例えばリスク管理策として仮名化したデータを扱ったとしても、データの連結によりプライバシーリスクが発生する可能性があることを認識する必要があります。

そこで企業はプライバシー影響評価（PIA）によりプライバシーリスクを認識することが必要です。スマートシティ参画によって得られる利益とプライバシーリスクが自社に与える影響を比較し、自組織がリスクを許容できるレベルまで低減させるように管理策を実施する事が求められます。

欧州では GDPR（General Data Protection Regulation）がデータ保護規則として定められており、パーソナルデータの取り扱いについて詳細に定められています。GDPR の特徴の１つとして、規則に違反した際の多額の制裁金が企業に課せられるという点があります。そのことからもパーソナルデータを取り扱う海外企業は企業規模を問わずプライバシー影響評価（PIA）をした上で、許容できるレベルまで低減するためにリスク管理策を実施しています。日本国内でもプライバシーリスクに起因する顧客のサービスの離脱による収益低下、企業のブランド低下、データマネジメントが適切に行われず流出した場合の対応費等をプライバシー影響評価（PIA）により認識し、許容できるレベルまで管理策を施す事がデータ利活用型スマートシティへの参画に際しては重要になります。

また、ここまで繰り返しプライバシーは時代や社会とともに変化すると触れてきましたがプライバシー影響評価も一度実施すればいいものではありません。それはスマートシティという都市で定期的なガバナンスの見直しがあることと同様に定期的な影響評価の見直しが必要となります。

第5章　　総括

5.1 本書のまとめ

Society 5.0 の実現の場としてデータ利活用型スマートシティの取り組みが社会的に進むとともに、企業はスマートシティに参画して様々なデータの利活用による新たなサービスを創出し、都市に参画するステークホルダーの多くが利益を享受することができるようになります。しかし、企業は同時にパーソナルデータを取り扱うことで発生するプライバシーリスクを認識し管理しなければならないという課題を負うことになりますが、次のような理由から課題解決の難しさがあります。

・発展を続けるスマートシティのあり方を捉えることが難しい
・プライバシーが社会や時代とともに変化することから、プライバシーリスク及びその管理策を捉えることが難しい
・スマートシティ、プライバシー両方に精通した人材確保が難しい

“スマートシティ”と“プライバシー”それぞれの理解を助けるガイドラインやドキュメントは多く発行されています。本書ではそれらの内容を、フレームワークを参考にして整理しており“スマートシティのプライバシー”についての課題・事例・管理策を俯瞰的に捉えることができるようになっています。本書が、これからスマートシティへの参加をはじめる企業の担当者の助けになれば幸いです。

5.2 本書の課題と制約

5.2.1　用語の定義について

本書では「データマネジメント」という言葉にパーソナルデータを適切に取り扱うことでプライバシーリスクを管理することであるという定義付けをしていますが、一般的な定義とは異なることに注意する必要があります。

まず、データマネジメントに関する知識を体系立ててまとめている DAMA-DMBOK [8] では次のように書かれています。

データマネジメントとは、データとインフォメーションという資産の価値を提供し、管理し、守り、高めるために、それらのライフサイクルを通して計画、方針、スケジュール、手順などを開発、実施、監督することである。

本書内では「データマネジメント」という言葉に、上記の定義に加えプライバシーリスク管理に必要な機能・カテゴリも含めて実施されるものという意味を持たせています。

5.2.2　各組織での活用

プライバシーが時代や社会とともに変化すること、またスマートシティのあり方は一様ではなくデータアーキテクチャが変化することから本書で取り上げた内容が将来のスマートシティ全てに適用できるものではないことに注意してください。状況に応じて適切に読替をしてください。また技術的な詳細にも踏み込んでいないため更に興味のある方は参照文献をご覧ください。

5.3 謝辞

本書の作成にあたり、独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラム講師の門林 雄基先生、並びに情報処理推進機構 中山 顕様には、本書の元となるプロジェクトのメンター・講師として、ご指導・ご助言、ご支援を賜りました。改めて御礼申し上げます。

参照文献

[1] 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議,“オープンデータ基本指針（令和３年６月 15 日改正 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）,”2021.

[2] 米国立標準技術研究所（NIST）,“The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,”2020.

[3] 総務省,“スマートシティセキュリティガイドライン（第 2.0 版）,”2021.

[4] 内閣府,“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.

[5] 経済産業省・総務省,“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,”2022.

[6] 日本総合研究所,“海外のデータ活用型スマートシティの現状（概要）,”2018.

[7] KDDI 総合研究所,“調査レポート R&A「Google が描く未来都市はなぜ実現できなかったのか？～Sidewalk Labs のスマートシティ取り組みからの教訓～」,”2022.

[8] DAMA International, DAMA-DMBOK DATA MANAGEMENT BODY OF KNOWLEDGE, 2018.

作成者

本書は、独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラムにおける卒業プロジェクト「データ利活用型スマートシティにおけるセキュアなデータマネジメント」の成果物として作成されました。

＜作成者＞
（◎はリーダー、〇はサブリーダー）
◎中尾 辰弥
〇鈴木 真徳
赤木 駿一
川口 翔太郎
杉浦 良祐
中村 誠