資料1-2

JIPDEC

第３回スーパーシティ／スマートシティにおけるデータ連携等に関する検討会　資料

PIA（プライバシー影響評価）について

2020年12月17日

委員　坂下哲也

（（一財）日本情報経済社会推進協会　常務理事）

はじめに

資料1-2

JIPDEC

- スマートシティ／スーパーシティでは、都市の中の様々なパーソナルデータを利用します。
- 一方で、パーソナルデータの利用は、より繊細・高度なサービスを提供できる反面、漏洩などによる事故が起きると、取り返しがつかない影響（精神的・財産的な影響など）が出る場合もあります。
- そこで、**パーソナルデータを利用する前に、「取得⇒利用⇒保管⇒廃棄」のプロセスのリスクを分析し、システム等の構築前に対策を準備する手法として、PIA（プライバシー影響評価）という手法**が生まれました。
- PIAについては、国際標準（ISO/IEC 29134　）が2017年に成立し、2021年1月に日本産業規格（**JISX9251**）として発行される予定です。
- 本日は、PIAとは何かという御説明をし、スマートシティ／スーパーシティに取り組まれる方々の参考になればと考えています。

PIAについて

環境影響評価

資料1-2

JIPDEC

■ 環境影響評価（環境アセスメント）

- 環境に大きな影響を及ぼすおそれのある事業を実施する事業者が、その事業の実施に伴って生ずる環境への**影響について事前に調査・予測・評価**するとともに環境保全措置の検討を行い、**住民や行政機関などの意見も踏まえた上で、事業実施の際に環境の保全への適正な配慮を行う**ための仕組み。
  - 実際に、受け取った意見をもとに事業計画を調整、変更することも多い。
- 環境影響評価法に定められ、①自然の良好な状態の維持ができるか、②人と自然のふれあいが維持できるか、③環境への負荷はどれくらいかについて、調査・予測・評価をしなくてはならない。

■ 事例（下北風力発電事業）

- 現状を分析。（どのような影響があるかを予測。）
- どのような措置を行うか。
- それによる効果を予測。

これからやろうとしていることに、どのようなリスク（回りへの迷惑等）があり、それを回避するために何をし、その効果があるのだという事を宣言。

特性	工事の内容		①工事期間 工事開始時期：平成30年4月（予定） 試運転開始時期：平成32年10月（予定） 運転開始時期：平成33年10月（予定） ②工事工程 道路工事：約23ヶ月 造成・基礎工事：約22ヶ月 据付工事：約14ヶ月 試運転：約8ヶ月 ※12月～3月までは冬季休工の予定であり、上記月数には含まない。
地域特性・予測評価結果・環境保全措置	大気質	1．現況	平成25年度末現在で青森県内に設置されている一般環境大気測定局は15局、自動車排出ガス測定局は4局あり、対象事業実施区域及びその周囲には一般環境大気測定局である2局（むつ市（苫生小学校）、六ヶ所村（尾駮小学校））が存在する。 測定局の測定項目と環境基準達成状況は、二酸化硫黄、二酸化窒素、浮遊粒子状物質は、測定を行っている測定局では環境基準を満足している。一方、光化学オキシダントは、両測定局で測定を行っており、ともに環境基準を達成していない。 大気環境中のダイオキシン類について、平成25 年度の調査結果は、対象事業実施区域及びその周囲では、むつ合同庁舎局において測定を行っており、環境基準（1年平均値が0.6pg-TEQ/Q/m3 以下）を達成している。 なお、対象事業実施区域及びその周囲では、一酸化炭素、微小粒子状物質及び有害大気汚染物質の測定は実施されていない。
		2．環境保全措置	・規制速度の遵守、急発進、急加速の禁止及びアイドリングストップ等のエコドライブ（環境負荷の軽減に配慮した運転）を実施する。 ・工事工程の調整等により、工事用資材等の搬出入に伴う車両台数のピーク時台数を低減するよう努める。 ・工事用資材等の搬出入に用いる関係車両の出場時には、必要に応じ、散水、タイヤ洗浄等を行う。 ・工事用資材等の搬出入に用いる関係車両は、適正な積載量により運搬するものとし、必要に応じシート被覆等の飛散防止対策を講じる。 ・定期的に会議等を行い、環境保全措置を工事関係者に周知徹底する。 ・環境監視として、関係車両の台数を管理簿に記録する。
		3．予測・評価	工事用資材等の搬出入に伴う窒素酸化物による寄与率は0.2～0.8%程度、降下ばいじん量は全ての地点で1t/km2/月を下回った。 事業実施に際しては、規制速度の遵守等について、工事関係者に周知徹底するとともに、工区間の調整を行いながら、ピーク時台数の低減及び平準化などの環境保全措置を講じ、できる限りの影響の低減に努める。 以上のことから、工事用資材等の搬出入に伴う窒素酸化物及び粉じん等の影響は実行可能な範囲内で影響の低減が図られているものと評価する。

（出典：環境影響評価準備書の審査書、2015年12月）

プライバシー影響評価（以下、「PIA」）

資料1-2

JIPDEC

■ 定義

- 個人のプライバシー等の権利権益を**侵害する可能性、それによる影響**を予測し、その**リスクを分析**した上で、そのようなリスクを**軽減する措置を講じていることを確認**する行為。

■ 実施対象

- 個人識別可能情報（以下，PIIという。）を処理するプロセス，プログラム，ソフトウェア、モジュール，デバイス又はその他の取組み。

必要最低限の個人情報を取得し、考えられるリスクを最大まで軽減する運用とセキュリティ対策が施されるのであれば、「秘密」（プライバシー）は守られるという考え方

具体的に評価する観点

資料1-2

JIPDEC

■ PIAは利用者の立場に立って考えるものである。

項目	説明		
プライバシー影響度	利用する情報のプライバシー性	基本情報、趣味趣向、取引履歴、利用履歴、財産情報、センシティブ情報、特定個人が識別できる画像等、身体・容姿に関する情報、位置情報など	**「使われたい」、「使われたくない」と利用者が感じる度合い**
	利用目的のプライバシー影響度	顧客管理などの必要な業務、サービス提供、技術開発、マーケティング（自社・他社）、情報販売など	
	利用時の加工状態におけるプライバシー影響度	生データ、統計、匿名加工、仮名、プロファイルなど	
利用者の予測可能性	データの取得時のプロセスを踏まえ、定められた目的で利用されることを**利用者が予測できるか**。		
利用者の受益	利用者がデータを利用されることによって、メリットを感じる度合い、又はそれを**認識・実感する機会があるか**。		
オプトアウト手段の提供の有無	オプトアウト手段の提供の有無（オプトアウト手段の認識度・簡便さ）、提供を**拒否した場合の不利益**の程度など。		
利用者への説明	**提供する説明によって、利用者が理解できるか**。		

【参考】プライバシーリスク特定の観点

資料1-2

JIPDEC

- 前提：利用者の基本的権利が守られているか。
- その上で、以下を確認する。
  - PIIへの認可されていないアクセスがあるか。（**機密性の喪失**）
  - PIIへの認可されていない変更がなされるか。（**完全性の喪失**）
  - PIIの紛失・盗難、又は認可されていない持ち出しがあるか。（**可用性の喪失**）
  - PIIが目的の達成に必要以上の取得をしていないか。
  - PIIの認められていない・不適切な紐づけがされていないか。
  - 利用者の権利（開示請求など）への考慮が欠如していないか。
  - 利用者の認識又は同意無しにPIIを処理することはないか。
  - 利用者の同意無しに、目的を変更することはないか。
  - 不必要に長期にPIIを保有することはないか。

対象となるパーソナルデータの範囲

資料1-2

JIPDEC

- ISO29134では、個人情報を**「個人識別可能情報」**（注１）として広くとらえている。
- 必要最低限の個人情報を取得するのがPIAの原則であるが、**プライバシーリスクを分析するには広い範囲でとらえる方が有効**だという考え方によるものである。

	個人情報の定義
個人情報の保護に関する法律	第二条　この法律において**「個人情報」とは、生存する個人に関する情報**であって、次の各号のいずれかに該当するものをいう。 一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。） 二　個人識別符号が含まれるもの
ISO 29134	**・その情報に関連するPII主体を識別するために利用され得る情報** **・PII主体に直接もしくは間接的にひも（紐）付られるか可能性がある情報** ・PII主体が識別可能か否かを判断するには、その個人を識別するために、そのデータを保有するプライバシー利害関係者又は他の者が合理的に利用することができる全ての手段を考慮するのがよい。（注2）

（注1）PII（Personally Identifiable Information）個人識別可能情報
（注2）JIS X 9250(ISO/IEC 29100）「情報技術–セキュリティ技術– プライバシーフレームワーク（プライバシー保護の枠組み及び原則）Information technology-Security techniques-Privacy framework」を使用。

PIAの歴史

制度上のPIA（１）

資料1-2

JIPDEC

- 1998年　オンタリオ州（カナダ）
  - 政府・行政が構築する新規の情報システムプロジェクトの認可において、PIAの実施報告が必須。
- 1999年　カナダ
  - 州政府がプロジェクトの予算認可の条件としてPIAの実施が義務付け。
- 1999年　アルバータ州（カナダ）
  - 健康情報公開法の中で、公共機関の健康医療分野におけるシステム開発にはPIAの実施を義務付け。
- その他
  - オーストラリア
    - 行政機関のPIA報告は公開が義務付け。
  - アメリカ
    - 電子政府法によってPIA実施が義務付け。（208条）
      - 行政管理予算局（OMB、Office of Management and Budget）長官によるチェックが義務付けられており、同長官は、PIA報告書を精査し、予算執行の認否を行う。

制度上のPIA（２）

資料1-2

JIPDEC

- **日本では番号法**（行政手続における特定の個人を識別するための番号の利用等に関する法律）において、特定個人情報保護評価としてPIAの手法を導入。
- **EUでは、GDPR**（一般データ保護規則）において、特定の場合において、DPIAの実施を義務付け。

例	説明
特定個人情報保護評価	①対象人数（本人数）は何人か、②特定個人情報を取り扱う職員・外部委託先の人数は500人以上か、③過去一年以内に、特定個人情報の漏えい等に関する重大事故を発生させたかによって、基礎・重点・全項目評価を選択して実施する。（参考：https://www.ppc.go.jp/files/pdf/260114siryo3-6.pdf）
GDPR（一般データ保護規則）	・第35条において、**DPIA（Data Protection Impact Assessment）**として規定。 ・以下のケースの場合に実施する事が求められている。 – （a）**プロファイリングを含む自動化された処理**に基づいて自然人に関する個人的側面を体系的かつ広範囲に**評価**され、当該評価に基づいて決定がなされ、その決定が自然人に関して法的効果を発生させまたは類似の重大な影響を与える場合 – （b）第 9 条第 1 項で定める**特別なカテゴリーのデータ**、または第 10 条13 で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合。 – (c)**一般の人々がアクセスできる場所において大規模な体系的監視を行う場合。**

PIA実施の段階

PIAの手順例

資料1-2

JIPDEC

■ 実施手順は事業者が作成する。以下に標準的な実施手順をまとめる。

- 評価書作成の後に評価会議（経営、第三者など）を開催し評価を得ることや、評価書を公開し意見収集するなどの手段を採る事が多い。
  - PIIの扱う事業体は様々なので、それに応じたPIAを行ってリスクを見極め、それをカバーする実装を進めるもの。
  - PIAはそれを可能とする柔軟性のある仕組みであり、ユースケースは多用なので、それにうまく適応できるもの。

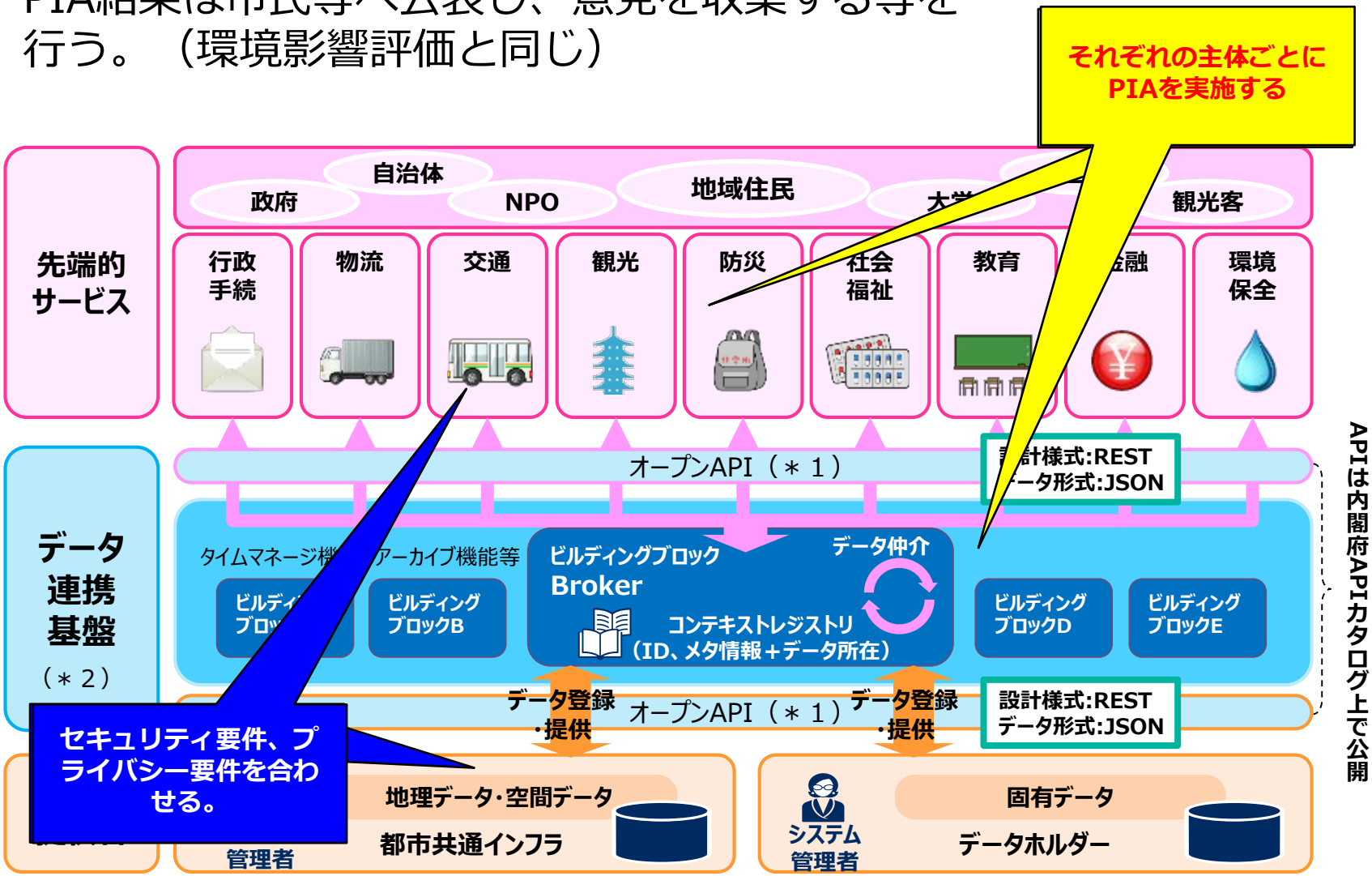
	評価計画を作成する			PIAを実施する			結果をまとめる	
	必要性の検討	実行チームの編成	実施計画の作成	資料収集	データフロー分析	リスク要因の分析	改善計画作成	評価書作成
評価手順	閾値評価	チームの人選など	計画作成	・内部・外部ポリシーなどの収集 ・システム関連資料収集	・PII取り扱い業務の分析 ・フロー作成 ・システム構成図作成	・評価項目作成 ・リスク要因の洗い出し ・影響度の算定 ・改善策（案）の整理	・改善計画作成	・影響評価書作成
成果物	閾値評価書	運営計画書	実施計画書	資料目録	・取り扱い業務一覧 ・データフロー図 ・システム構成図	・影響評価項目 ・リスク分析表 ・改善策一覧	・改善計画書	・PIA評価書

現在

資料1-2

JIPDEC

- 各主体ごとにPIAを実施する。（先端的サービス、データ連携基盤）
- PIA結果は市民等へ公表し、意見を収集する等を行う。（環境影響評価と同じ）

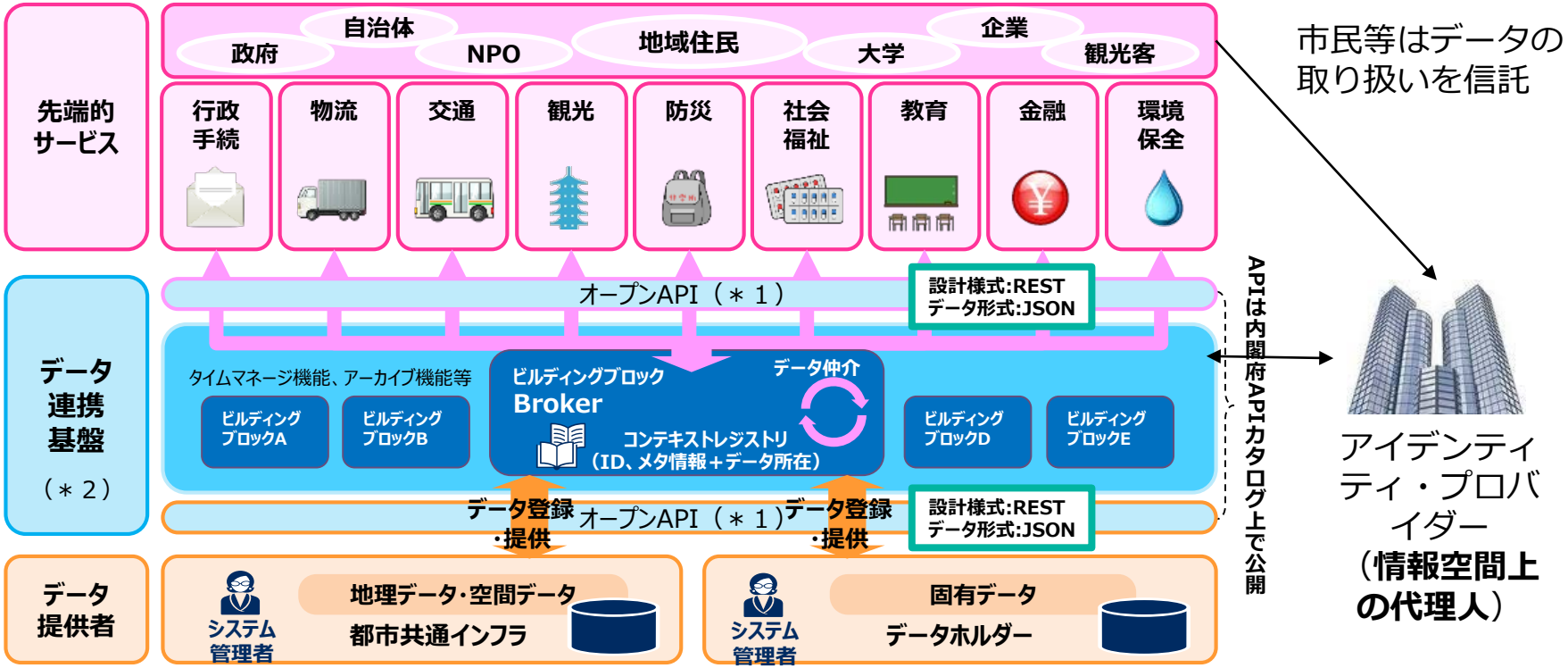


（＊1）API :Application Programming Interface

（＊2）データ分散方式を推奨。必要に応じてデータ蓄積も許容。

将来

- **多様なデータが、様々な目的で利用されるようになると、透明性を高めても個人は把握できなくなる。**
- スーパーシティでは、市民から**“自身のデータがきちんと扱われていることを見ている”アイデンティティ・プロバイダー（情報空間上の代理に）へ『信託』**し、データ利用により利便性を享受するようになるのではないか。



（＊１）API :Application Programming Interface

（＊２）データ分散方式を推奨。必要に応じてデータ蓄積も許容。

参考文献

- 日本規格協会『ISO/IEC 29134:2017　情報技術－セキュリティ技術－プライバシー影響評価の指針 Information technology -- Security techniques -- Guidelines for privacy impact assessment』
  - https://webdesk.jsa.or.jp/books/W11M0010/
- JIPDEC　「プライバシー影響評価（Privacy Impact Assessment）～ISO/IEC29134:2017 の JIS 化について～」
  - https://www.jipdec.or.jp/archives/publications/J0005163_2
- シンヨンジン著、瀬戸洋一・JIPDEC（監訳）『情報化社会の個人情報保護と影響評価』(勁草書房、2012)
- 瀬戸洋一（編）『ISO29134対応　プライバシー影響評価実施マニュアル』（日科技連、2020）