平成 31 年 1 月 31 日
（2019 年）

西宮市情報システム課

「J-Storage」におけるＰＩＡの実施について

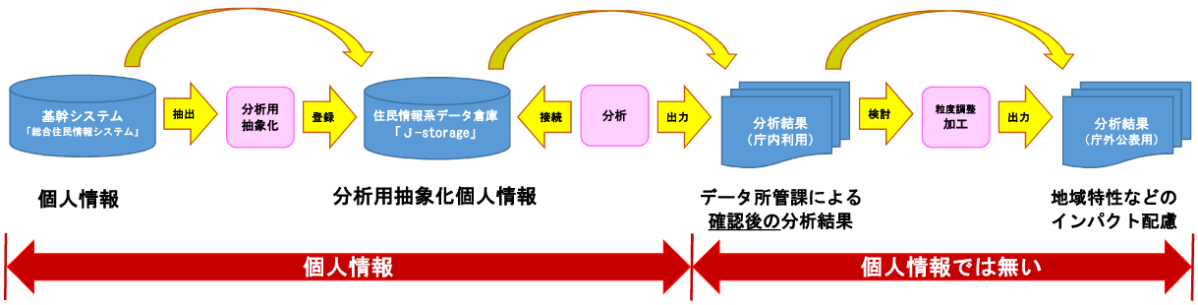
１．「J-Storage」整備の背景

近年、データに基づいた政策立案、いわゆるＥＢＰＭが注目を集めており、市行政においてもその実施が求められている。そこで、庁内におけるデータ分析を推進するため、主に、市の基幹システムに登録された住民情報に**抽象化加工**を施し、**多種のデータ**を、**保存年限を設定することなく**、**予め累積**しておく、庁内共通の分析用基盤として**住民情報系データ倉庫「J-storage」を整備**することとした。

２．「J-Storage」内のデータの性質

「J-storage」に累積するデータでは、マイナンバーや氏名・住所など、**ひと目で個人が特定できる情報を削除**する（抽象化加工の詳細は後述）。一方で市行政の分析においては、同一人のデータのマッチングや、世帯での名寄せが不可欠であることから、**宛名リンク番号や世帯番号を不可逆変換して保有**する。不可逆変換する理由は、分析の過程で得られた情報から、元データ（基幹システムの住民情報）を辿れる可能性を低減するためである。

マッチングのためのキーとなる番号を有していることや、データの組み合わせで個人を特定できる可能性が高いことから、「J-storage」に累積するデータは個人情報として取り扱う必要があるが、既存の西宮市個人情報保護条例の枠組みに当てはめた場合、**収集・加工・保存年限の制限がある**ため分析用基盤としての利用は困難である。そこで、西宮市個人情報保護条例において、新たに**「分析用抽象化個人情報」**として規定することで、**個人情報保護に配慮しつつ、データの利活用を図る**こととした（予定）。



分析結果については、データ所管課により**個人が特定できない**ことを確認した後に**庁内利用**を可能とするが、**地域特性などの配慮を要する情報**が含まれている可能性があることから、**庁外公開**する場合には必要に応じて更に**粒度を調整**するための加工を追加することとする。

３.「J-Storage」のＰＩＡ

「J-storage」は**庁内利用に限定**し、直接データベースにアクセスできるのは**情報システム課に限定**するものの、データ量が多く、機微なデータも含むことから、その取扱には慎重を期す必要がある。

そこで、他市（姫路市）の事例も参考に、これまでの本市におけるＩＳＭＳおよびマイナンバーにおける特定個人情報保護評価のノウハウも活かして、「J-storage」のＰＩＡ（Privacy Impact Assessment：プライバシー影響評価）を実施することとした。ＰＩＡの実施に際しては、マイナンバー制度導入時に作成し、本市において実績のある**「特定個人情報保護評価（全項目）ガイドライン」を準用する**こととした。

なお、特定個人情報保護評価では、しきい値評価の結果に基づいて「しきい値評価のみ」、「重点項目評価」、「全項目評価」の３つのタイプに分けられるが、対象人数が３０万人以上は「全項目評価」の対象であることから、**「J-storage」のＰＩＡは「全項目評価」相当で実施する**こととした。

４.「特定個人情報保護評価（全項目）ガイドライン」

本市では、マイナンバー制度に合わせて導入された**「特定個人情報保護評価」**を、庁内で統一的な基準で実施し、かつ客観的な評価が可能となるよう、平成１７年度から認証継続している**ＩＳＭＳのリスク評価手法**を取り入れた「特定個人情報保護評価（全項目）ガイドライン」（以下、「ガイドライン」という）により運用している。

特定個人情報を守るべき情報資産と捉え、リスク評価シートを作成し、残留リスクの値が許容範囲内に低減するまで脆弱性対策を実施し、これらの対策を評価書に記載している。

５．「J-storage」におけるガイドラインの準用

「J-storage」には、特定個人情報（マイナンバーを含む）を格納しないことから、ガイドラインの**特定個人情報に特化した記述については適用しない**こととするとともに、評価書内の「特定個人情報」という用語は「個人情報」に置き換える。

※詳細は『「J-Storage」における「特定個人情報保護評価書作成ガイドライン」の準用』を参照

６．「J-Storage」内の分析用抽象化個人情報

「J-Storage」に登録する分析用抽象化個人情報は、総合住民情報システムに分類される基幹システムの内、**税務情報を除く全データを対象**とし、**過去分のデータ**も可能な限り登録する。また、登録項目は、将来におけるデータ分析の有用性を確保するため、総務省が作成し、一般財団法人全国地域情報化推進協会（APPLIC）が維持管理する**中間標準レイアウト仕様**のデータ一覧に従う。

■「J-Storage」に格納する個人情報ファイルには、以下の加工を施した情報を、共通部分として先頭に付加して格納するものとする

項目名	項目説明	分析用抽象化の手法
1）個人リンク番号	宛名データベース上の人を統一的に管理する番号	宛名リンク番号をハッシュ関数で不可逆変換した文字列（SHA-256 を使用）
2）世帯リンク番号	住基世帯を管理する番号	世帯番号をハッシュ関数で不可逆変換した文字列（SHA-256 を使用）
3）生年月	宛名データベース上の生年月	生年月日から日を削除かつデータの時点で 90 歳以上をトップコーディング（90 歳に）
4）性別	宛名データベース上の性別（1:男、2:女）	加工なし
5）地域コード	宛名データベース上の町コード　※H30.4 時点 438 町	加工なし

■「J-Storage」には以下の情報を格納してはならない

1）氏名	カナ、漢字とも、姓のみ、名のみも格納不可
2）住所	「町」より下の地番号（住所から得られる位置情報を含む）
3）年月日	年月日がセットになったものは不可（日を除けば格納可）
4）電話番号・ＦＡＸ番号等	電話番号、ＦＡＸ番号を含む個人への連絡先のすべて
5）個人識別符号	生体情報、業務固有ナンバー（識別番号、被保険者番号、基礎年金番号など）
6）情報を連結する符号	マイナンバー、宛名リンク番号、世帯番号など
7）口座番号	口座種別、口座番号、口座名義人の格納不可

※項目としては存在する場合もあるが、データは格納しない
※５）６）において、「宛名リンク番号」「世帯番号」については、それぞれ「個人リンク番号」「世帯リンク番号」に加工することで共通部分として格納可能

■単体データごとに、登録前に以下のチェックを行い、特異な情報に配慮する

１）「住基ファイル」または「住登外ファイル」において、**世帯員数が７人以上の世帯の全レコードを除外**するとともに、他の情報においても同一人のレコードを除外

２）「住基ファイル」または「住登外ファイル」において、**同一地域コード内の世帯数が９以下の場合は隣接する地域に統合**するとともに、他の情報においても同一人のレコードは隣接地域に統合

３）特異なデータの残存について、年１回、元データの所管課の確認を受け、必要に応じて個別の加工を追加

■データのマッチング

１）世帯で名寄せする場合は、**「世帯リンク番号」と「地域コード」**のセットでマッチング

２）複数ファイルを個人で名寄せする場合は、**「個人リンク番号」と「生年月」**のセットでマッチング

※ハッシュ化した「個人リンク番号」や「世帯リンク番号」は、低い確率で同じ値になる可能性がある（ハッシュの衝突）ことから他の項目とセットでマッチングする

■分析結果を庁内利用する前に、個人が特定できないように以下の加工およびチェックを行う

１）データ分析によって得られた値（統計値、集計値など）が**「2」以下**となるものは情報システム課において**「3」に置換**しなければならない

２）データ分析課は、一旦、分析結果が出た際には、分析に用いたデータの全てのデータ所管課に、**結果に個人が特定できる情報が含まれていない旨の承諾**を得なければならない

３）複数データを組み合わせたことにより、いずれかのデータ所管課が、分析結果において**個人が特定できる**と判断した場合は、データ分析課は適切な抽象化ルールの追加を検討し、情報システム課において**追加の抽象化工程**を実施しなければならない

４）データ分析課は、結果を**庁内利用する前**に、分析に用いたデータの全てのデータ所管課に、分析結果および利用用途を報告し、**承認を得なければならない**

■分析結果を庁外への公表する前に、インパクトを考慮して以下の加工およびチェックを行う

1）分析結果を**庁外へ公表**する場合においては、個人が特定できないことはもとより、**地域の特性が明らかになることのインパクトにも考慮**して、地域の範囲を町単位から小学校区、中学校区、支所単位などに拡大したり、数値を平均値と比較して上か下かといった表現に編集したりすることにより、公表の目的を果たせる範囲で、**粒度を粗くする加工**を施さなければならない

2）分析結果を**庁外へ公表**する場合においては、公表前に、分析に用いたデータの全てのデータ所管課に、公表用の分析結果および公表先を報告し、**承認を得なければならない**

※詳細は『個人情報保護評価書（全項目評価書)』を参照

７．ＰＩＡの結果

国の個人情報保護委員会では**特定個人情報保護評価の目的**等を次のように位置づけている。

「情報の漏えいや不正利用等により個人のプライバシー等の権利利益が侵害されると、拡散した情報を全て消去・修正することが困難であるなど、その回復は容易ではないことから、個人のプライバシー等の権利利益の保護のためには、事後的な対応でなく、事前に特定個人情報ファイルの取扱いに伴う特定個人情報の漏えいその他の事態を発生させるリスクを分析し、このようなリスクを軽減するための措置を講ずることが必要となります。特定個人情報保護評価は、このような事前対応の要請に応える手段あり、特定個人情報ファイルを保有する前の段階で適切な保護措置を検討するための制度です。

また、番号制度の導入に対する懸念を払拭する観点からは、特定個人情報ファイルを取り扱う者が、入手する特定個人情報の種類、使用目的・方法、安全管理措置等について国民・住民に分かりやすい説明を行い、その透明性を高めることが求められます。特定個人情報保護評価は、評価実施機関が、評価書において、どのような事務でどのような目的のために特定個人情報ファイルを取り扱うのか、個人のプライバシー等の権利利益の保護のためにどのような措置を講じているのかを具体的に説明することにより、国民・住民の信頼を確保することを目的としています。」

出典：個人情報保護委員会サイト https://www.ppc.go.jp/mynumber/pia2(kaisogo)/

特定個人情報保護評価に準じた「J-Storage」のＰＩＡでは、今後、結果について市民からの意見聴取を行うと共に、個人情報情報保護審議会の承認を得て、評価書を市ホームページ上で公表する手続きを取ることになるが、それにより**特定個人情報保護評価と同等の目的を達成**することができる。

加えて、本市独自のリスク評価も含めたことで、リスク値が許容範囲内に低減できていることを確認していることから、客観的に**十分な脆弱性対策が実施できている**と言うことができる。

以上