弁護士　水町 雅子

2022.2

個人情報保護評価の意義と実践

～顔認証、医療情報、行政情報へのPIA / DPIA実例を通しての分析～

PRIVACY IMPACT ASSESSMENT / DATA PROTECTION IMPACT ASSESSMENT

AGENDA

1. プライバシー影響評価とは何か
2. プライバシー影響評価PIAに向けた取り組み
3. PIAの具体例
    - A) NEC顔認証に対するPIAの例
    - B) 姫路市による行政情報分析に対するPIAの例
    - C) 民間の医療系サービスに対するPIAの例
4. どのように実施すればよいのか
5. 第三者点検（専門家意見）のポイント
6. 参考

I. プライバシー影響評価とは何か

プライバシー影響評価とは

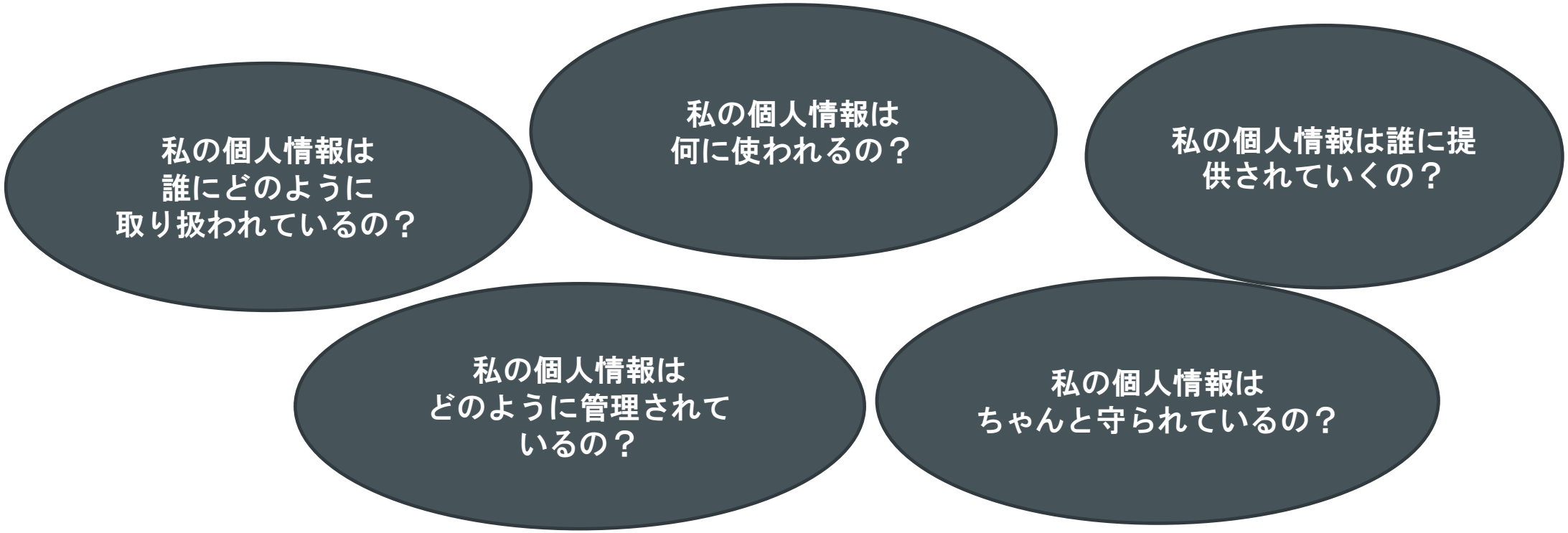
◆ Privacy Impact Assessment （PIA）

- 個人情報を取り扱う制度・事務・ビジネス・ITシステム等を開始する前に、プライバシーに対して与える影響を検討するための仕組み
- 個人情報を取り扱うとプライバシーに対して悪影響が生じるおそれ。その悪影響を緩和・軽減するための方策を検討する
- イギリス、アメリカ、香港、オーストラリア、ニュージーランド、カナダ、韓国その他の国で実施されている
- 行政機関、医療機関、民間企業などさまざまなアクターが実施
- 英米法系の国で主に実施されてきたが、国際的トレンドPrivacy by Design（PbD）の実践手法としての注目度も高く、**GDPR**でも実装された。GDPR上ではPIAではなく**DPIA**（**D**ata **P**rotection **I**mpact **A**ssessment、データ保護影響評価）と呼ばれる。

プライバシー影響評価の意義（ユーザ・消費者・市民にとって）

◆ 個人から見た意義

- 今まではブラックボックスだった個人情報の取扱いを透明化
- プライバシー・ポリシーのあるべき姿をイメージ



プライバシー影響評価の意義（実施側にとって）

◆ 評価実施側から見た意義

- プライバシー保護を体系的に理解・説明できるようになる
  - ✓ 個人情報といっても、漏えいさえしなければいいというものではない

- 個人情報を取り扱う必要性をユーザ・消費者に理解してもらえる
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、具体的に説明できる

- 個人情報を取り扱うに当たって注意すべき点がわかる
  - ✓ 従業員の意識の向上
  - ✓ 研修といった座学だと当事者意識が生まれないことも
  - ✓ 「自分が行っている業務」における注意点を具体的に検討する

- 個人情報を適切に取り扱うことをユーザ・消費者にアピールできる
  - ✓ 取扱いの適正性を具体的にアピール
  - ✓ 「炎上」する前に
  - ✓ 「危ない」VS「必要だ」の原理主義的論争に陥らず、詳細な評価書を基に、問題点を具体的にユーザと討論できる

プライバシー影響評価の意義（実施側にとって）

◆ 評価実施側から見た意義

コミュニケーション手段としての側面も強い	
従業員	個人情報・プライバシーの重要性 業務上の注意点
顧客	信頼の獲得
ITシステムベンダー	個人情報・プライバシーの重要性 要求仕様

プライバシー影響評価でわかること

実施側が宣言すること

- **個人情報**を取り扱う**必要**があるので取り扱います
- 個人情報を**このように**取り扱います
- 個人情報を**適切に取り扱うために各種リスク対策を事前に講じます**

評価書からわかること

- どんなふうに個人情報を取り扱うの？
- どんなリスク対策を講じるの？
- プライバシー保護についてどのように取り組んでいるの？

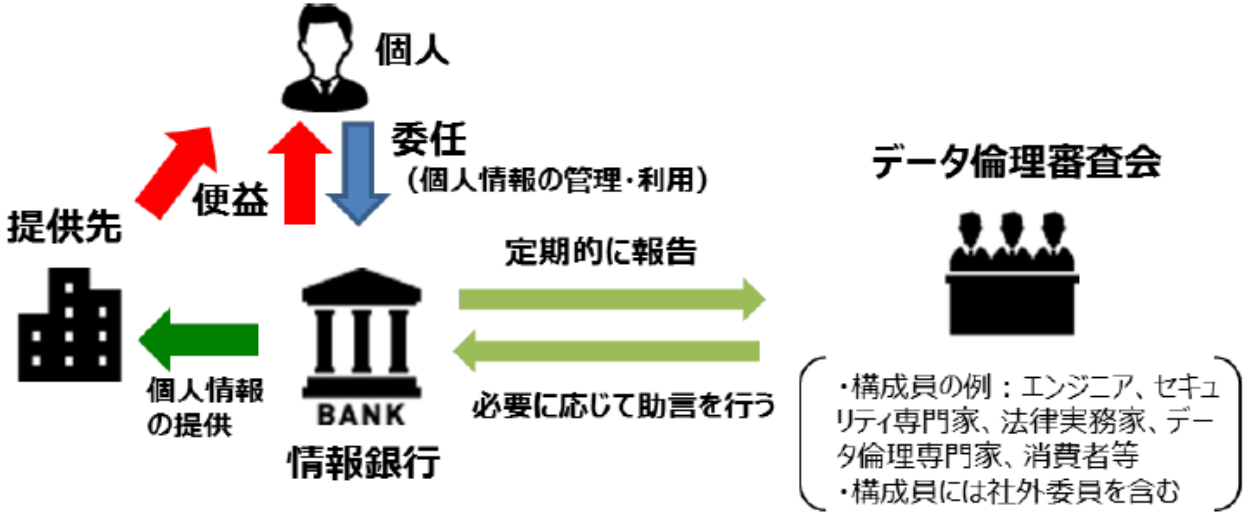
2.　プライバシー影響評価PIAに向けた取り組み

諮問体制（データ倫理審査会）に関する事項

情報信託機能の認定に係る指針ver2.　総務省　経済産業省

■ データ倫理審査会における審議の考え方
- 情報銀行は、個人の代理として、個人が安心して自らに関する情報を預けられる存在であることが期待される。このため、利用者たる個人の視点に立ち、適切な運営が確保される必要がある。
- このため、データ倫理審査会は、情報銀行の事業内容が個人の利益に反していないかという観点から審議を行う。

（例）・個人によるコントローラビリティを確保するための機能が誤解のないUIで提供されているか
・個人の同意している提供先の条件について、個人の予測できる範囲内で解釈されて運用されているか
・個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか
・個人にとって高いリスクを発生させる恐れがある場合には、GDPRで義務づけられているDPIA（データ保護影響評価）を参考にすることも考えられる



●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
- ・個人と情報銀行の間の契約の内容
- ・情報銀行の委任した個人情報の利用目的
- ・個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（ＵＩ）
- ・提供先第三者の選定方法
- ・委任を受けた個人情報の提供の判断

●運営方法
- ・構成員及び（必要な範囲の）議事録は公開する
- ・必要に応じ情報銀行に調査・報告を求めることができる

「情報銀行」認定制度 データ倫理審査会 運用ガイドライン （TPDMS-1140）にて実装

https://www.tpdms.jp/file/TPDMS-1140.pdf

２．民間の自主的取組の推進

○ 具体的には、ＰＩＡ（Privacy Impact Assessment、個人情報保護評価）の取組、個人データの取扱いに関する責任者の設置、企業の自主的な取組を推奨する仕組みなどについて、その取組を促進していくことが考えられる。

（２）ＰＩＡの推奨

○ ＰＩＡについては、特に、大量の個人データを扱う事業者にとっては、こ のプロセスを通じた事前評価を行うことで、個人データの管理や従業員への 教育効果等も含め、事業者自身にとって、効率的かつ効果的に必要十分な取組を進めるための有用な手段である。

○ 中間整理の意見募集でも、ＰＩＡなどについて、漏えい時の緩和措置とし て働くようにすべき、ＰＩＡを努力義務化し、一定の場合は義務化を検討す べきなどの意見もあった。

○ 他方、ＰＩＡについては、自社の基準に基づいて自主的に実施する事業者 が増加してきているとともに、民間において、国際規格（ＩＳＯ/ＩＥＣ ２ ９１３４：２０１７）のＪＩＳ化が進められている中、現時点において、評 価の項目や手法等を規定して義務化することは、かえってこうした自主的な 取組を阻害するおそれもあるため、このような民間の動向を踏まえつつ、民間の自主的な取組を促すことが望ましいと考えられる。

個人情報保護法 いわゆる３年ごと見直し 制度改正大綱

令和元年12月13日 個人情報保護委員会

一般データ保護規則（GDPR）

https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

Section 3 Data protection impact assessment and prior consultation
第３節　データ保護影響評価及び事前協議

Article 35 Data protection impact assessment
第 35 条　データ保護影響評価

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

1. 取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない。類似の高度のリスクを示す一連の類似する取扱業務は、単一の評価の対象とすることができる。

データ保護影響評価（DPIA）及び取扱いが2016/679規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン

https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf

（特定個人情報保護評価）

第二十八条　行政機関の長等は、特定個人情報ファイル（専ら当該行政機関の長等の職員又は職員であった者の人事、給与又は福利厚生に関する事項を記録するものその他の個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）を保有しようとするときは、当該特定個人情報ファイルを保有する前に、個人情報保護委員会規則で定めるところにより、次に掲げる事項を評価した結果を記載した書面（以下この条において「評価書」という。）を公示し、広く国民の意見を求めるものとする。当該特定個人情報ファイルについて、個人情報保護委員会規則で定める重要な変更を加えようとするときも、同様とする。

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（マイナンバー法）

特定個人情報保護評価に関する規則

https://www.ppc.go.jp/files/pdf/PIA_kisoku.pdf

3.　PIAの具体例

A)　NEC顔認証に対するPIAの例

顔認証を利用した顔パス イベント入場に関する

個人情報リスク評価 DPIA・PIA

(Data Protection/Privacy Impact Assessment)

初版　2021年3月

弁護士　水町雅子
作成協力者　日本電気株式会社デジタル・ガバメント推進本部部長　岩田　孝一

このPIAに用いた「顔認証を利用した顔パス イベント入場プロジェクト」は、

個人情報保護に関する民間の自主的取組に資するために、

実案件を模して定義した「ダミープロジェクト」であり、

実在の人物・団体・事件などには一切関係ありません。

Agenda

1　顔パス入場とは

1.1　顔パス入場の概要

①申込時

利用者

・Webから申込み
・氏名、生年月日、住所、電話番号、メールアドレス、パスワードを入力する
・**「顔パス入場」を利用したい場合に限り**、顔写真データの登録の同意を行い、顔写真データをアップロードする
・いったん登録した後に、顔写真登録の取消も可能

②入場時

顔パス利用者

※顔パス入場者以外は、通常ゲートから通常通り入場

・顔パス入場者は、顔パス入場ゲートのカメラで撮影した顔写真データをアップロードして識別･認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む
・ゲートのカメラで顔写真を撮影
・認証できた場合は、入場ゲートが自動的に開く
・認証できなかった場合は、通常ゲートから通常通り入場するか、係員に問い合わせる

1.2　顔パス入場の仕組み

①申込時

①-1　利用者が登録した画像中から顔を検出

①-2　顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出

①-3　利用者が登録した顔写真データを削除、特徴量をイベント管理システムに登録

②入場時

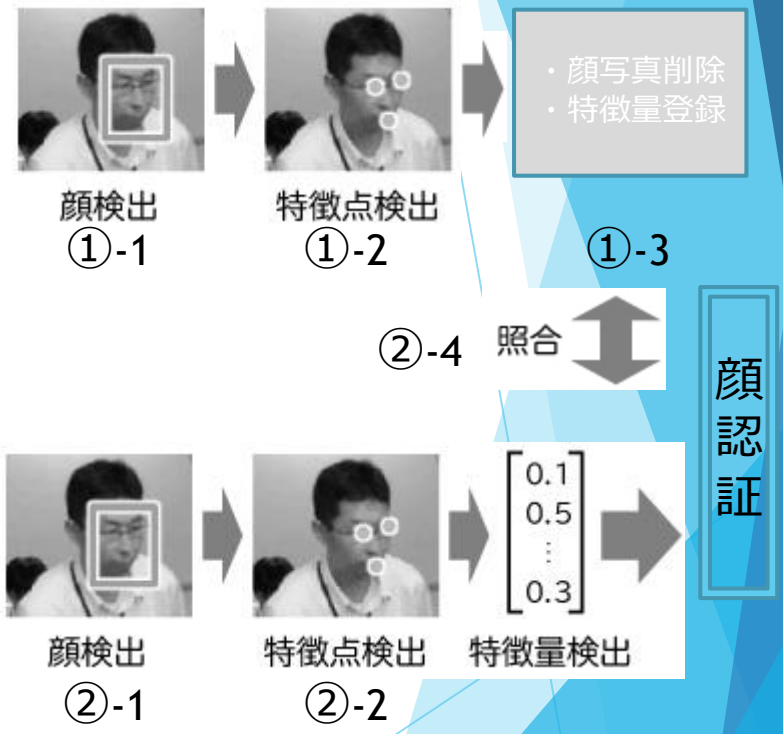
②-1　顔パス入場ゲートのカメラで撮影された画像中から顔を検出

②-2　顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した特徴量を抽出

②-3　撮影された顔写真データを削除

②-4　ゲートのカメラで撮影された画像の特徴量データ（②-2）と、利用者が登録した画像の特徴量データ（①-2）とで顔識別･顔認証を実施し、認証できた場合はゲートを開放

②-5　ゲートのカメラで撮影された画像の特徴量データ（②-2）を削除



2　本評価について

2.1　本評価の目的

顔認証のメリットと懸念

■ 顔認証により、来場者は手ぶら（チケットレス）で、そして入場待ち時間が短縮する等、スムーズにイベントに参加することができます。また、不正入場の防止や接触レスなどの利点もあります。
他方で、重要な個人情報である顔画像が万一悪用されたり流出してしまえば、プライバシーに与える影響は非常に大きく、また様々な場所での監視につながる懸念や、顔認証の精度の問題等もあります。

個人情報やプライバシー権の保護が大前提

■ 顔認証の活用といった比較的新しい取組みはイノベーションに欠かせないものではありますが、個人情報やプライバシー権の保護がまずもって大前提であり、プライバシーに与える悪影響を防止・軽減する対策を事前に十分講じた上で、適法・適正に技術が活用されていくことが重要です。

顔認証に対するプライバシー影響評価

■ 個人情報・プライバシー権保護のための手法として、海外で普及する「DPIA*」「PIA**」というスキームがあります。ビジネスを開始する前に、そのビジネスが個人情報・プライバシーに対してどのような悪影響を与える可能性があり、その悪影響を防止・軽減するためにどのような対策を講じるかを検討するスキームです。

■ 本評価では、「DPIA」「PIA」スキーム（以下、単に「PIA」といいます。）を用いて、顔認証を利用したイベント入場におけるプライバシーへの影響及びそれを防止等する措置を検討します。

*DPIA：GDPR（一般データ保護規則）に規定されたデータ保護影響評価（Data Protection Impact Assessment）
**PIA：英・米・カナダその他の様々な国で実施されているプライバシー影響評価（Privacy Impact Assessment）

2.2　本評価の対象

- 個人情報保護委員会「個人情報保護に関する民間の自主的取組の在り方」に関する調査の一環として、顔認証サービスを展開する日本電気株式会社（以下、「NEC」といいます。）及びJIPDEC（一般財団法人日本情報経済社会推進協会）協力の下、顔認証を利用したイベント入場に関してDPIA・PIAスキームを用いた本評価を実施しました。
- 本評価は、弁護士水町雅子が、NECから資料提供やヒアリングを受けながら実施し、上記個人情報保護委員会「PIA検討会」に提出したものです。なお、NECは、本評価書に記載された内容に偽りがないことを事前に確認しています。
- 本評価は、「NEC顔認証機能を利用した顔パスイベント入場」（以下「顔パス入場」といいます。）をその範囲・対象としています。NECは様々な場面（出入国管理、企業の入退室管理、顔認証決済等）で利用できる顔認証サービスを提供していますが、今回は顔認証を利用したイベント入場を対象に、本評価を実施します。なお、顔認証入場に際する個人情報・プライバシー保護全般を目的としており、実際に稼働しているイベント入場に対する評価ではなく、NEC顔認証技術を元にイベント入場管理を行うことを想定した評価になります。そのため、本評価中に登場するX社・Y社はあくまで仮定の企業になります。

3　顔パス入場の個人情報保護のポイント（対策まとめ）

顔写真データは、大変重要な個人情報です。また、顔認証が悪用等されると、なりすましや監視等につながる懸念もあります。顔認証技術を利用・提供する企業にはこれらのリスクその他のプライバシー権侵害や不正行為を防止するため、様々な対策を応じる必要があります。NECでは本評価記載の通りの措置を講じており、その主なポイントは以下の通りです。

主なポイント

① **顔写真データ自体はすぐに削除**

・顔写真データを利用者が登録後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。

・来場時にゲートで撮影した顔写真データも、速やかに特徴量抽出を行い、撮影データを削除します。

*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

② **希望者だけが、顔パス入場**

・顔パス入場希望者以外は、通常ゲートから通常通り入場できます。

③ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**

・ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。

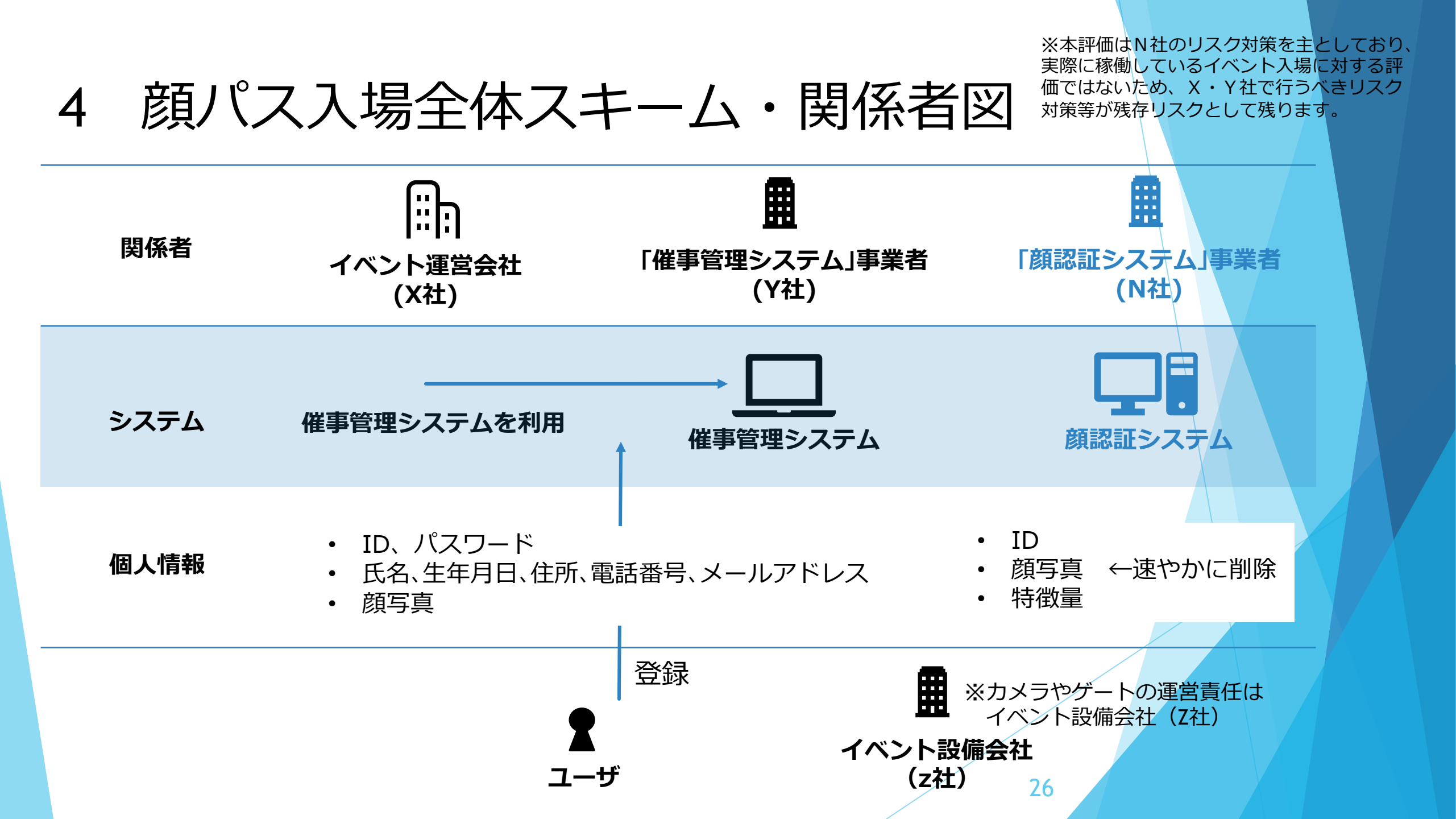
・但し、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しています。

④ **セキュリティ**

・様々なセキュリティ対策を履践しています。NECではPマーク付与認定及びISMS認証を取得しています。

4　顔パス入場全体スキーム・関係者図

※本評価はＮ社のリスク対策を主としており、実際に稼働しているイベント入場に対する評価ではないため、Ｘ・Ｙ社で行うべきリスク対策等が残存リスクとして残ります。



5　リスク対策

個人情報・プライバシーへの影響とその対策

5.1　なりすまして別人が入場することはないのか

激戦を勝ち抜いてチケットを獲得しました。
別人が私になりすまして勝手に入場し、私が入場できなくなることはないのでしょうか。

高精度の認証技術

- 骨格の似た親兄弟でも違いを検知し、双子についても違いを判別します。
- NECの生体認証は、約70の国と地域1000システム以上の導入実績があります。なかでも顔認証は入出国管理や国民IDなど国家レベルでのセキュリティのほか、企業での入退管理や端末ログイン、決済など、様々な用途で使われています。
- NECの顔認証技術は、米国国立標準技術研究所（NIST）主催のベンチマークでNo.1の評価を5回獲得しています。米国国立標準技術研究所(NIST)が実施した最新の顔認証技術のベンチマークテスト(FRVT2018)において、1,200万人分の静止画の認証エラー率0.5%という、第1位の性能評価を獲得しました。なお、NISTのベンチマークテストは数千万人規模の大規模静止画データにおける認証精度と処理速度を評価するもので、使われる評価画像は、登録用画像として1200万人分の静止画像が登録され、照合画像としては未登録人物33万人分、登録人物15万人分が利用されるというものです。
  https://jpn.nec.com/biometrics/face/index.html
- 今後も、精度の維持・向上に努めていくことが求められます。

不正対策も

- 顔認証システムでは、「いつ・だれが入退したか」というデータをログとして正確に残せます。そのため、万一不正が起こっても、究明が可能です。
- 万一不正が起こった場合は、通常ゲートの会場係員が、催事管理システムからお客様のチケット情報を確認したり、どのような人物がお客様のチケットを用いて入場したかどうかを確認します。

5.2　誤認証・誤認識で入場できないことはないのか

激戦を勝ち抜いてチケットを獲得しました。
それなのに、顔認証システムが私を認識してくれなくて、入場できなくなることはないのでしょうか。

マスクやサングラス、横向きでも認証が可能

- NECの顔認証は、マスクやサングラスなどを装着した場合でも、事前に登録した画像データと照合し、本人かどうかを高精度で識別できます。人工知能（AI）の手法の一つである深層学習に、本人と似ている他人との違いを強調する独自の工夫を取り入れ、精度を高めることができました。マスクやサングラスを装着していたり、顔を横に向けていたりしても、正面で撮影した画像をもとに高精度で認証することができます。

入場前であれば顔写真データの差替も可能

- 昔の顔写真で申し込んでしまった場合や、申込後に顔を負傷した場合等であっても、入場前であれば、申込ページにログインいただいたうえで、顔写真データを差し替えることができます。

通常ゲートから入場可能

- 万一、認証エラーになった場合は、通常ゲートから通常の方法で入場できます。
- お客様が当日チケットをお持ちでなかったとしても、Web画面からお客様自身で催事管理システムにログインし、ご自身のチケット情報をご確認いただけますし、会場係員も催事管理システムにログインし、確認することができます。

5.3　入場するために顔画像を登録しなければならないのか

某イベントに参加したいです。
でも、そのために顔画像を登録したり顔認証をするのは嫌です。

希望者だけ、顔画像による顔パス。通常ゲートからチケット提示でも入場できます

- 顔認証による顔パス入場は、あくまで希望者だけが対象。
- 顔パス入場以外に、通常ゲートからチケットを提示し、通常の方法で入場することができます。顔パス入場か通常入場かは自由に選択可能です。通常入場を選択した場合にも来場者に不利益はありません（もっとも、通常入場の際は、入場待ちリスク、係員との接触リスク等はあり）

取消可能

- 一度顔パス入場を申し込んだ方でも、顔パス入場する前までであれば取消が可能。
- 取消を希望された場合は、顔写真､特徴量その他の個人情報を速やかに削除します（但し、問合せ対応のためIDだけは取消済のIDとして記録し保持しておく）。

残存リスク

- 取消時については、NECだけでなく、X社・Y社においても確実に削除されることを確認する必要があります。

5.4　顔画像や特徴量等の個人情報は誰がどこで保管するのか

私の顔画像や特徴量、氏名などの個人情報は誰がどこで保管するのですか？

NECでは顔写真、特徴量、IDのみ保持

- NECでは、顔写真データ、顔写真データから抽出した特徴量、IDのみを保持します。このうち、顔写真データは下記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
- また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。
- NECにおけるこれらの情報の管理方法・リスク対策については、5.6「漏えい対策は」を参照ください。

顔写真、氏名、住所等はX社・Y社

- ID・パスワード、氏名、生年月日、住所、電話番号、メールアドレス、顔写真といった、申込時に登録等していただいた情報は、イベント運営会社X社の責任で保管されます。
- 責任主体はイベント運営会社X社ですが、保管場所はイベント運営会社X社が利用する、Y社催事管理システムになります。Y社催事管理システムの提供・運営・保守等、X社から委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。
- X社・Y社では上記の通り、特徴量はいっさい保持せず、NECから顔認証OKかNGかの情報が提供されるだけです。
- 4「顔パス入場全体スキーム・関係者図」もあわせてご覧ください。

残存リスク

- 催事管理システムでの管理方法・リスク対策については、催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.5　顔認証・顔画像が不正利用されないのか

顔画像を不正コピー等されて、違う目的に利用されることはないのですか？

顔パス入場にのみ利用します

- 顔認証・顔画像は、顔パス入場にのみ利用します。
- NECは委託を受けて顔認証機能を提供する立場であり、登録された顔画像とゲートで撮影された顔画像が一致するか否かを判断する目的以外に個人情報を利用することは、リーガル的にもできません。NECでは顔画像・特徴量の不正を防止するため、社内で権限を与えられた者以外はアクセスできないよう制御し（アクセス制御、入退館・入退室制限等）、アクセス者には守秘義務を課しています。また、顔画像・特徴量を保持する顔認証システムでは逐一ログを取得し、不正コピー・不正持出し・不正提供等を監視します。
- なお、特徴量はNECでのみ保持し、委託業務終了後に廃棄します。

残存リスク

- イベント運営会社X社がどのように個人情報を利用・管理するかどうかは、X社が通知・公表等する利用目的を確認する必要があります。
- 催事管理システム事業者Y社は、一般にX社から委託を受けて催事管理システムで入場申込・入場管理等の機能を提供する立場であり、委託の範囲を超えて個人情報を利用することはリーガル的にもできません。但し、Y社における個人情報の管理方法は、Y社に確認する必要があります。

5.6　漏えい対策は

顔画像や特徴量が漏えいしたら大変ではないですか？

対策

- NECでは、クラウドサービス等を行う上で重要とされるISO/IEC20000(JIS Q 20000:2007)、ISO9001(JISQ9001)、ISO/IEC27017、ISO/IEC27018、ISMS(ISO/IEC 27001/ JIS Q 27001)、プライバシーマーク(JIS Q 15001)、SOC1/SOC2、事業継続マネジメントシステム(ISO/IEC22301)等の認定・認証を取得しています。
- 開発プロセスの各フェーズで、セキュリティの観点から実施すべき事項をセキュリティタスクとして定義し、それらのタスクを ガイドラインに沿って実行することで配備されるソフトウェアは、適切なソースコード診断、脆弱性診断を経て実装されます。
- 不正プログラムの混入やその攻撃による各種の脅威（情報漏洩や可用性低下など）に対抗するために、ウイルス対策ソフトの導入、安全なプログラム設定、不要プロセスの削除等をセキュリティポリシーに纏め、同ポリシーに準拠した設計・構築及び運用体制を確立しています。
- 物理サーバのハードウェア障害時には別物理サーバ にて仮想サーバの自動再起動を行うなど、ハードウェアの故障等によるサービス停止リスクに対抗するための各種設計に基づいて、構成・運用をしています。
- システムの事故（ハードウェア 障害など）に対しては 、適切なモニタリングを行うことでそれを検出し 、可及的速やかに障害からの復旧を行います。
- 広域災害などサービスを継続できなくなる事態に備えて、遠隔地に退避したアプリケーションとデータを復旧することのできる環境で提供しています。
- インターネットに接している IPアドレスに関しては、脆弱性を定期的にスキャニングしています。

5.6　漏えい対策は

顔画像や特徴量が漏えいしたら大変ではないですか？

対策
■ 故障等によりストレージデバイスを交換する場合には、データ流出を防止するための廃棄プロセスが定義されており、それに従った廃棄（NSA（米国家安全保障局）推奨方式や DoD（米国防総省）準拠方式等の消去方式）を徹底しています。 ■ 盗聴による影響を軽減するために専用線接続サービスやVPN（公衆網内に構成するプライベートネットワーク）を採用し、さらにIDS（不正侵入検知システム）を利用することで不審なアクセスの試みを検知しています。 ■ システムメモリ上、またはハードウェア上に何らかの原因で残存するデータの処理に関して適切な管理を行うために、論理的なデータの取り扱い、物理的なデータが記録されている媒体の取り扱いに関して適切な運用規定を設け、運用管理を徹底し、運用内容は第三者機関によって定期的に監査され、必要に応じて改善を実施しています。 ■ ID アクセス管理機能で、リソースへのアクセスを安全にコントロールすることができ、運用担当者の特権 IDの利用に対して有効な統制を実施し、組織内で要求されるアクセス制御を確実に実施しています。
残存リスク
■ イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社がどのように個人情報を管理するかどうかは、それぞれの事業者に確認する必要があります。

5.7　もし特徴量が漏えいしたらどうなるのか

NECでは、顔写真データはすぐ削除し、特徴量とIDのみ保持するということはわかりました。
IDと特徴量が漏えいした場合、特徴量から私の顔がわかるのですか？
また漏えいした特徴量を悪用して、不正なりすましが起きませんか？

特徴量から顔画像の復元は困難です

- 現在の技術では、特徴量データから、顔画像データを復元することは困難です。特徴量データは、顔画像データ（元の生体情報）から不可逆的な方式で変換しています。また特徴量は顔の一部分の特徴のみ抽出するため、特徴量では把握できていない顔の部分が存在します。
- 特徴量データは、日本の個人情報保護法では「個人識別符号」に該当する情報です。氏名や顔画像データなどと紐づけて管理されていなくても、特徴量データ単体で個人識別符号に該当し、明確に個人情報であると定義されています。個人情報保護法に従って、NECでは厳格な管理を実施しています。
- 生体情報は、パスワードなどと異なり、他人に盗み見られたり、わすれてしまうリスクがありません。他方で、その人しか持たず簡単に変更できないという生体情報のメリットは、漏えいしてしまった場合に深刻な問題となります。「一生変わらない」という生体情報のメリットは、「一生変えられない」というデメリットにもなり得ます。そのため、生体認証技術を使う際の生体情報の管理には、厳重なセキュリティ対策が求められます。

5.8　知らない間に顔画像が撮影されないのか

知らない間に顔画像を撮影したり、顔認証したりしないですか？

知らない間に顔認証することはありません

- **顔パス入場ゲートでのみ**顔認証を行います。顔パス入場ゲートは通常ゲートと異なる**外観**になっており、顔認証を実施することを立看板で**周知**しています。
- なお、顔パス入場ゲートで顔画像を撮影した場合であっても、**事前に顔写真を登録していない場合は**顔認証エラーとなります。そして顔パス入場ゲートで撮影された顔画像・特徴量データは速やかに削除されます。
- 顔パス入場ゲート以外では、顔認証を実施しません。

残存リスク

- ゲートカメラの運営はイベント設備会社Z社に委ねられています。ゲートカメラで常時撮影しているか、人がカメラ前に立った時だけ撮影しているのかは、Z社に確認する必要があります。

5.9　顔画像や特徴量を他人に提供することはないのか

顔画像や特徴量を他人に提供することはないですか？

第三者提供は行いません

- NECでは、個人情報保護法に反して、顔画像や特徴量を第三者提供することはありません。NECでは顔認証システムの保守運用等に関して必要な範囲内で委託を行う可能性がありますが、その場合も、個人情報保護法及び同ガイドラインに則って委託先を監督します。
- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社においても、法律に反した第三者提供を行えば、個人情報保護法違反になります。
- なお、個人情報保護法で認められている外部提供として、例えばイベント会場内で犯罪が発生した場合で、警察から令状に基づき来場者情報の提供を求められた場合等は、氏名・顔画像等を警察に提供することがあり得ます。

残存リスク

- イベント運営会社X社、催事管理システム事業者Y社及びイベント設備会社Z社が、個人情報保護法を遵守した上で共同利用等を行う可能性も考えられなくありませんので、それぞれに確認する必要があります。

5.10　顔写真・特徴量を確実に削除するのか

顔画像や特徴量は確実に削除してもらえるのですか？
私が自分で削除依頼をしないといけないのですか？

顔写真データはすぐに削除します

- （申込時）顔パス入場を希望するユーザは顔写真データを登録します。その後、速やかに顔認証システムでは「特徴量抽出*」を行います。特徴量抽出後は、速やかに登録された顔写真データ自体を削除します。
- （来場時）ゲートで顔写真を撮影し、特徴量抽出*を行った上で、上記申込時に登録された特徴量と比較して顔認証を行います。顔認証システムでは、ゲートで撮影した顔写真データも速やかに特徴量抽出*を行い、速やかに撮影データを削除します。
  顔認証の実施後は、特徴量も速やかに削除します。
- スキーム詳細は前記スライド1.2をご参照ください。

*特徴量抽出：まず、画像中から顔を検出した後、顔のなかから目や鼻、口端、顔の輪郭、配置の特徴などの特徴的な点を数値化した顔特徴量を抽出します。顔識別・顔認証は、この特徴量を用いて実施します。

- 削除に当たって申込者の方で特に必要な手続・操作等は一切なく、顔認証システム側で**自動的に削除**します。

残存リスク

- 催事管理システム側でも顔写真データを保持するので、同システムでの削除については催事管理システム事業者Yに確認する必要があります。
- ゲートカメラのデータ自体については、イベント設備会社Z社に確認する必要があります。

5.11　監視につながらないのか

カメラで様々な情報を撮影し、様々な場所の撮影データ等とつなげれば、
人の行動履歴等がつぶさにわかるのではないでしょうか。

監視社会につながらないのでしょうか。

最小限のデータしか取得しないように措置を講じています

■ **NECが提供する顔認証機能では、氏名・住所等の情報は保持しません**
・NECでは、ID・顔写真データ、顔写真データから抽出した特徴量のみを保持します。このうち、顔写真データは上記の通り特徴量抽出後速やかに削除するため、ID及び特徴量のみ保存しています。
・また、NEC顔認証機能で生成した特徴量は、X社・Y社に提供することはありません。NEC顔認証機能内で削除するまで保存されますが、**X社・Y社には**、認証OKか認証NGかの情報をNECから返すだけで、**特徴量自**体は**提供しません**。
・なお、Y社の催事管理システムでは、申込者情報として氏名・住所・電話番号・メールアドレス・ID等の情報を保存しており、Y社は委託の範囲内でこれらの個人情報にアクセスすることができます。またX社もこれらの個人情報にアクセスすることができます。

本件顔パス入場にしか使いません

■ 本件で得た顔写真データ及び特徴量は、本件顔パス入場にしか使いません。

残存リスク

■ X社・Y社で、本件顔パス入場以外に利用したり、申込者が本件顔パス入場のために提供した個人情報以外と結合したりするリスクがありますので、X社・Y社にに確認する必要があります。
■ ゲートカメラ自体のプライバシーリスク対策については、イベント設備会社Z社に確認する必要があります。

5.12　その他のリスク対策（個人情報の取得に関して）

上記のほか、個人情報の取得に際して次の措置を講じています。

個人情報を過剰取得しないか
■ 5.11「監視につながらないのか」参照
不正確な個人情報を取得しないか
■ 本人から直接顔写真データ等の提供を受けた上で、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。 ■ 本人が顔写真データ等を登録する際は、確認・修正画面から、登録内容を確認し、誤りを修正等することができます。
取得の際に個人情報が漏えい・紛失等しないか
■ 本人が顔写真データ等を登録する際は、Web画面から氏名、生年月日、住所、電話番号、メールアドレス、希望パスワード等の入力・確認を行うと申込者IDが付番され、電子メールで通知されたURLにアクセスすることで登録完了します。登録完了後は、申込者IDとパスワードでWeb画面にアクセスし、登録内容の修正・削除を行うことができます。 ■ Web画面、「催事管理システム」、「顔認証システム」といった各間の通信は、HTTPSで通信し、通信暗号化とサーバー認証を行っています。
取得の際に不正が起きないか
■ 本人の同意に基づき本人から直接顔写真データ等の登録を受ける方法を取っており、本人の知らない間にデータを取得することはありません。また、登録された顔写真データだけでは顔認証が行えず、顔パス入場ゲートで実際に来場した人の顔写真を撮影して顔認証を行います。 ■ また5.11「監視につながらないのか」の通り、顔パス入場の目的達成に必要な最小限の範囲内でのみ個人情報を取得します。

5.13　その他のリスク対策（個人情報の利用・提供に関して）

上記のほか、個人情報の利用・提供に際して次の措置を講じています。

個人情報を無関係の者に利用されないか
■ NECが提供する顔認証機能にアクセスできるのは、NECで正当な手続を経て権限を付与された社員・委託先のみです。NEC社員や委託先であっても誰でも閲覧できるわけではなく、業務上必要な範囲内で、正当な社内手続に沿ってアクセス権限を認められた範囲にのみアクセスできます。 ■ 5.11「監視につながらないのか」の通り、X社・Y社には、認証OKか認証NGかの情報をNECから返すだけで、特徴量自体は提供しません。
本件関係者が個人情報を私的利用・私的複製・悪用等しないか
■ →5.5「顔認証・顔画像が不正利用されないのか」、5.6「漏えい対策は」参照。
個人情報が不正提供されないか
■ →5.9「顔画像や特徴量を他人に提供することはないのか」参照。
目的外利用・過剰紐づけされないか
■ →5.5「顔認証・顔画像が不正利用されないのか」、5.11「監視につながらないのか」参照。

5.14　その他のリスク対策（個人情報の安全管理措置に関して）

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- NECはJIS Q15001等に沿って個人情報保護マネジメントシステムを確立するために、「個人情報保護マネジメントシステムガイドライン」群を定めて、遵守しています。
- 事務取扱責任者を定め、各事務取扱責任者の責任範囲を規定します。事務取扱責任者は、事務取扱担当者を明確にし、各事務取扱担当者の役割と個人情報の取扱範囲を規定します。
- 事務取扱責任者は、個人情報の取扱状況を確認するために、個人情報ファイルの利用・出力状況の記録、書類・媒体等の持ち運びの記録、個人情報ファイルの削除・廃棄記録、削除・廃棄を委託した場合の確証、情報システムの利用状況の記録（ログイン実績、アクセスログ等）を記録します。
- 事務取扱責任者は、個人情報ファイルの取扱状況を確認する手段として、各個人情報ファイルの名称、種類、利用目的、取扱部署、責任者、アクセス権を有する者、削除・廃棄の方法を記録します。
- 事務取扱責任者は、管理区域において個人情報の情報漏えいを防止するために、情報システム機器等を設置するマシン室を「管理区域」として特定、入退場の履歴を記録（システムログ）、持ち込む機器を限定し、許可した機器以外の持ち込みを禁止、生体認証とその他個人認証（専用入室ICカード、社員証等）により、許可された者だけが入室できるように制限することを行います。
- 事務取扱責任者は、管理区域及び取扱区域において、個人情報が記録された情報機器及び電子媒体等は、紛失又は窃盗による情報漏えい等を防止するため、情報機器、電子媒体および書類等は、キャビネットや書庫等に施錠し保管、デスクトップ端末等においてキャビネットや書庫等に施錠保管が困難な機器は、セキュリティーワイヤー等で移動や持ち出しができないよう固定することを行います。

5.14　その他のリスク対策（個人情報の安全管理措置に関して）

上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- 事務取扱責任者は、管理区域又は取扱区域から、もしくは管理区域又は取扱区域へ、個人情報が記録された情報機器、電子媒体および書類等を持ち運ぶ際には、情報機器、電子媒体や書類等を持ち運ぶ際の記録、情報機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等が生じないよう運搬担当者が安全な処置を講ずることを確認、機器、電子媒体や書類等を持ち運ぶ際に、紛失や盗難等に備え、追跡ができるよう持ち運びの履歴を記録（運搬担当者、運搬物等）、個人情報が記録された機器・電子媒体等は、データの暗号化又はパスワードにより保護等を行ったことを確認、書類等を持ち運ぶ際には処置（封筒への封緘、目隠しシールの貼付等) を行います。
- 事務取扱責任者は、個人情報の情報漏えいを防止するために、事務取扱担当者の役割や責任に応じて、データベース、フォルダ、ファイル等のアクセス可能領域を限定的に設定していることを確認、情報システムにアクセス可能な機器は、ＩＰアドレス等による端末接続制限により使用可能な機器を限定していることを確認、情報システムにアクセス可能な事務取扱担当者を、認証ＩＤ等により限定していることを確認、ＩＤ・パスワード及び専用ＩＣカード等の共同利用を禁止し、事務取扱担当者の個々に付与していることを確認、なりすましを防ぐため、多要素認証を適用していることを確認することなど、情報システム及び特定個人情報ファイルへのアクセス制御、アクセス者の識別・認証等に関するの対策を講じます。

5.15　その他のリスク対策（個人情報の管理に関して）

上記のほか、個人情報の管理に際して次の措置を講じています。

委託先の不正が起こらないか
■ 利用目的の達成に必要な限度において、個人情報を扱う事務を第三者に委託する場合、当該委託において取り扱う個人情報の安全管理措置が講じられるよう、委託先の適切な選定、委託先の安全管理措置を遵守させるために必要な契約の締結、委託先における特定個人情報の取扱状況の把握など適切な監督を行います。
個人情報が誤って消去等されないか
■ 保存期間内は定期的にデータバックアップを実施し、複数個所に保管します。利用目的の達成等により個人情報の保存の必要がなくなった場合で、法令により必要な一定期間の保存期間を経過した場合には、速やかに当該個人情報を削除または廃棄します。
不要な個人情報がいつまでも保管されないか、古い個人情報を誤って利用しないか
■ 5.10「顔画像・特徴量を確実に削除するのか」参照。

5.16　その他のリスク対策（全般に関して）

上記のほか、次の措置を講じています。

点検・監査等
■ NECではPマーク及びISMS認証を取得しています。 ■ システム監査を年１回実施します。 ■ NECでは、個人情報保護管理者のほか、個人情報保護監査責任者を指定し、監査計画及び監査の実施を行います。
従業者教育
■ NECでは、少なくとも年1回定期的に、かつ必要に応じて適宜、従業者への教育・啓発を行っています。
開示・訂正・利用停止請求
■ 個人情報保護法に則って、X社にご請求いただくことになります。
問合せ対応
■ NECでは、ユーザの方等からのお問合せに真摯に対応いたします。下記、お問い合わせ窓口までお問い合わせください。 https://jpn.nec.com/site/privacy/index.html
残存リスク
■ スライド5.12～5.16は全てNECにおけるリスク対策を記載しています。X社・Y社におけるリスク対策についてはX社・Y社に確認する必要があります。

5.17　個人情報保護法への適合性（抜粋）

取得フェーズ

- 適正取得（個人情報保護法17条）
  - 申込者・利用者が本件顔パス入場を理解した上で申し込んだり利用できるように、下記の通り利用目的の通知等を行っています。利用者に理解していただいた上でセキュリティを確保した方法で個人情報を取得しており、適正取得しています。
  - 仮に要配慮個人情報が映り込んだ場合でも、個人情報保護法17条2項に従った取得です。

利用フェーズ

- 利用目的の特定・公表等（個人情報保護法15条・18条）
  - 本件顔パス入場は、NEC・X社・Y社ともに、事前に特定・公表している利用目的の範囲内です。
  - NEC・X社・Y社ともに、プライバシーポリシー等で利用目的を公表していますが、さらに加えて、顔パス入場申込サイトや顔パス入場ゲートでも、利用目的の通知を行います。
- 目的内利用（個人情報保護法16条）
  - 本件は、事前に特定・公表している利用目的の範囲内の利用です。
  - 加えてNEC・Y社においては、委託の範囲内の利用です。

提供フェーズ

- 第三者提供（個人情報保護法23条）
  - 個人情報保護法23条に反した個人データの第三者提供は行いません。

6　総括

6.1　まとめ

- 本評価において、以下の項目について検討し、プライバシー等への影響を確認しました。

  - スキーム（1.1,1.2,2.1,2.2,4,5.4参照）
  - 個人情報の取扱い（7.1参照）
  - 個人情報利活用の効果（2.1参照）
  - 個人情報保護のポイント（3参照）
  - なりすまし対策（5.1参照）
  - 誤認証・誤認識対策（5.2参照）
  - 顔画像提供の任意性（5.3参照）
  - 個人情報不正利用リスク対策（5.5参照）
  - 個人情報の漏えいリスク対策（5.6,5.7参照）
  - 個人情報不適正取得リスク対策（5.8参照）
  - 個人情報不正提供リスク対策（5.9参照）
  - 個人情報未消去リスク対策（5.10参照）
  - プライバシー権侵害・監視リスク対策（5.11参照）
  - 個人情報の取得リスク対策全般（5.12参照）
  - 個人情報の利用リスク対策全般（5.13参照）
  - 個人情報の提供リスク対策全般（5.13参照）
  - 個人情報の管理リスク対策全般（5.14,5.15参照）
  - 個人情報のその他のリスク対策（5.16参照）
  - 個人情報保護法への適合性（5.17参照）

- 評価実施手続

  - 本評価は世界各国のPrivacy Impact Assessment (PIA)や日本の法制等を参考にして、弁護士水町雅子が評価項目を決定しています。
  - NECから資料提供やヒアリングを受けながら弁護士水町雅子が実施しました。

6.2　水町雅子のコメント

最後に、弁護士水町雅子の意見を次のとおり、述べます。

- 顔認証技術は、より豊かで便利な社会を実現する期待・可能性を有する一方で、プライバシー権侵害の危険性も同時にはらみます。具体的に誰がどのような管理方法で、またどのようなセキュリティ対策を講じて顔写真データや特徴量を保持するのか、顔写真データや特徴量データを具体的にどのように利用し、どのような利用目的で利用するのか、外部提供は発生するのか等々、個人情報・プライバシー等への影響とその対策についての明瞭・透明かつ具体的な説明がなされることが大変重要であると考えます。プライバシー等の人々の権利利益に対する影響を様々な角度から事前に検討し、十分な対策を予め講じておくことは、個人情報やプライバシー権の保護をまずもっての大前提とした上で、適法・適正に新しい技術を活用していくために大きな意義があると考えます。
- 本件顔パス入場は、本人の明示的な同意に基づき、希望者のみが利用し、また目的が限定されていて、顔写真データや特徴量も顔パス入場のためだけに利用するスキームであり、他の顔認証技術の活用手法と比べても、比較的社会的受容性も高いと考えられます。
- 顔認証技術を世界的にも展開しているNECが、「個人情報・プライバシー等保護」と「顔認証技術の活用」を両立させ、このようなPIAを実施することは大変意義深いことであり、顔認証以外の様々な分野における新技術の活用・導入にとっても、PIAの手法は有用であると考えます。今回、本評価に登場するX社・Y社は仮の企業でしたが、実際に顔認証技術を利用する企業においても広く、このPIAを参考にして、個人情報・プライバシー等保護を徹底するための施策・運用等を行っていっていただければ、非常に良いと思います。
- 顔認証技術は海外動向・海外規制、正答率、人権への影響等、様々な観点から、現在も変動している環境下にあります。今後も、様々な観点からのチェックを行い、社会に受け入れてもらえる適正な方法での活用を行っていっていただければと思います。

7　参考

7.1　パーソナルリファレンスアーキテクチャ
「顔認証機能を利用した催事等入場管理パーソナルデータリファレンスアーキテクチャ」

7.2　本評価書と特定個人情報保護評価書との対照関係

7.3　参考URL

7.1　パーソナルリファレンスアーキテクチャ「顔認証機能を利用した催事等入場管理パーソナルデータリファレンスアーキテクチャ」

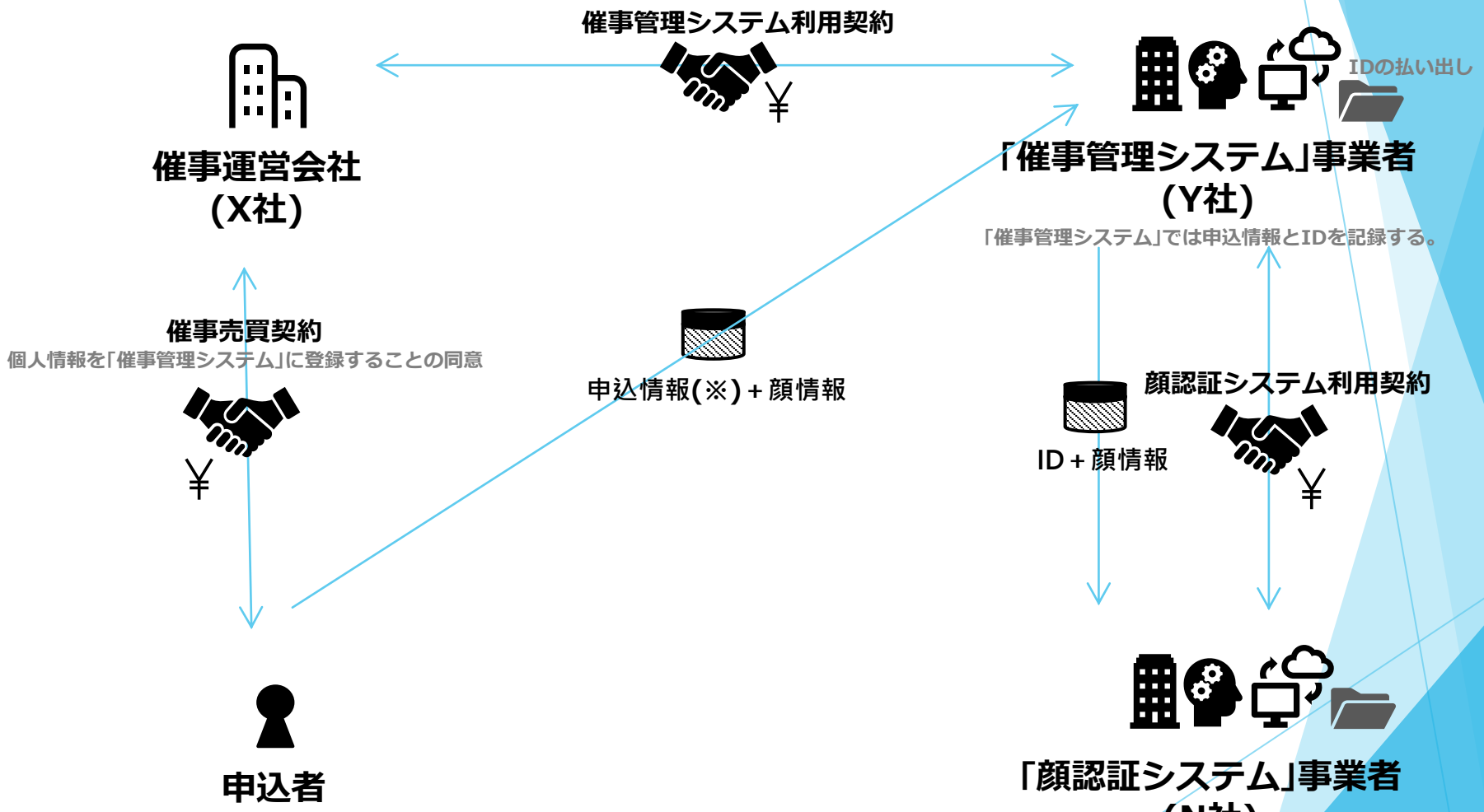
次ページ以降ご参照

1. ステークホルダリスト

名称	概要	ISO/IEC 29100での分類
申込者(エンドユーザ)	Webでイベント申込時に申込情報を提供する。	PII principal (データ主体)
催事運営会社(X社)	申込者から提供された申込情報を蓄積管理する。申込情報を管理蓄積するシステム運用と管理は、催事管理システム事業者(Y社)へ委託する。 個人情報保護法上の個人情報取扱事業者に該当。	Data controller (データ管理者)
「催事管理システム」事業者(Y社)	催事運営会社(X社)から申込情報の管理を受託し、X社に催事管理システムをクラウドサービスで提供する。 個人情報保護法上の委託先に該当。 また、催事管理システムが提供する機能のうち、顔認証情報を管理蓄積するシステム運用と管理は、顔認システム事業者(N社)へ委託する。	Data processor (データ処理者)
「顔認証システム」事業者(N社)	催事管理システム事業者(Y社)から顔認証情報の管理を受託し、Y社に顔認証システムをクラウドサービスで提供する。 個人情報保護法上の委託先(再委託先)に該当。	Data processor (データ処理者)
催事設備会社	催事会場に、催事管理システムと連動するカメラやフラッパーゲート等といったハードウェア設備を設置する。	非該当 (PII扱わない)

2. ビジネス関係

関与する個人、事業者間のビジネス関係(契約など)を明確化する

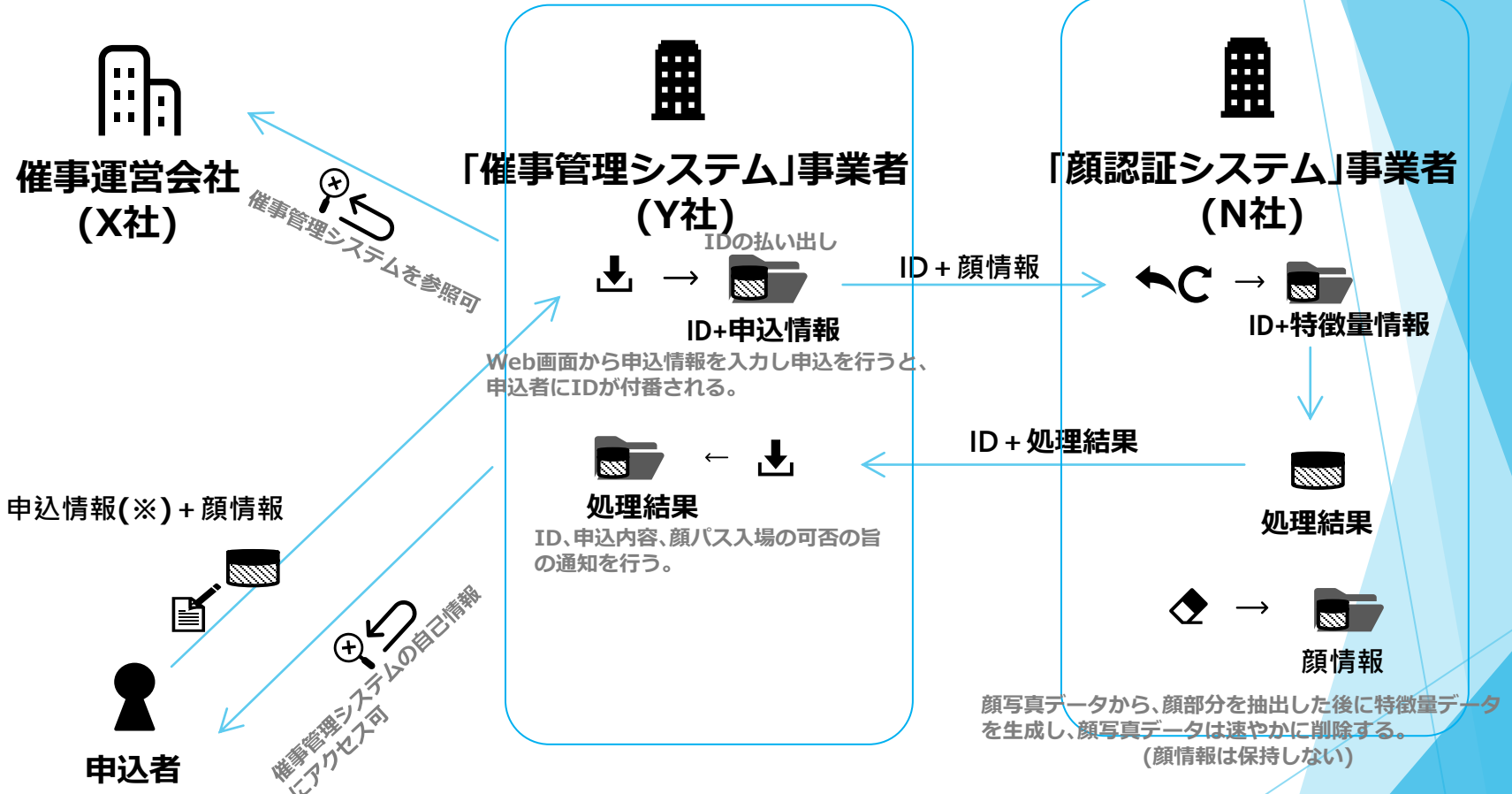


※:氏名、生年月日、住所、電話番号、メールアドレス、パスワード

3. データリソースマップ

パーソナルデータを含むデータセットがどこに存在するのかを明確にする

申込時(顔登録)

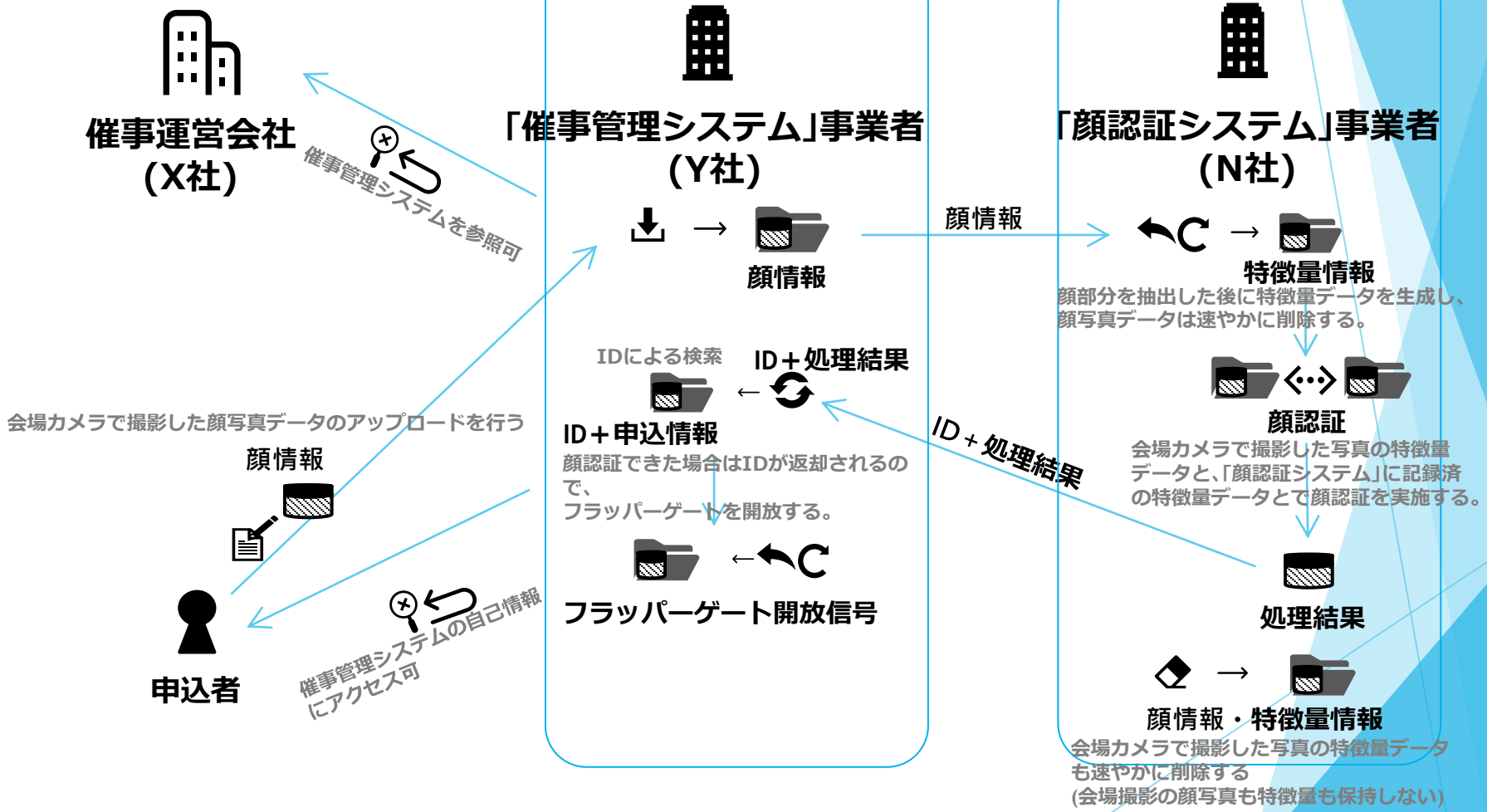


※:氏名、生年月日、住所、電話番号、メールアドレス、パスワード

3. データリソースマップ

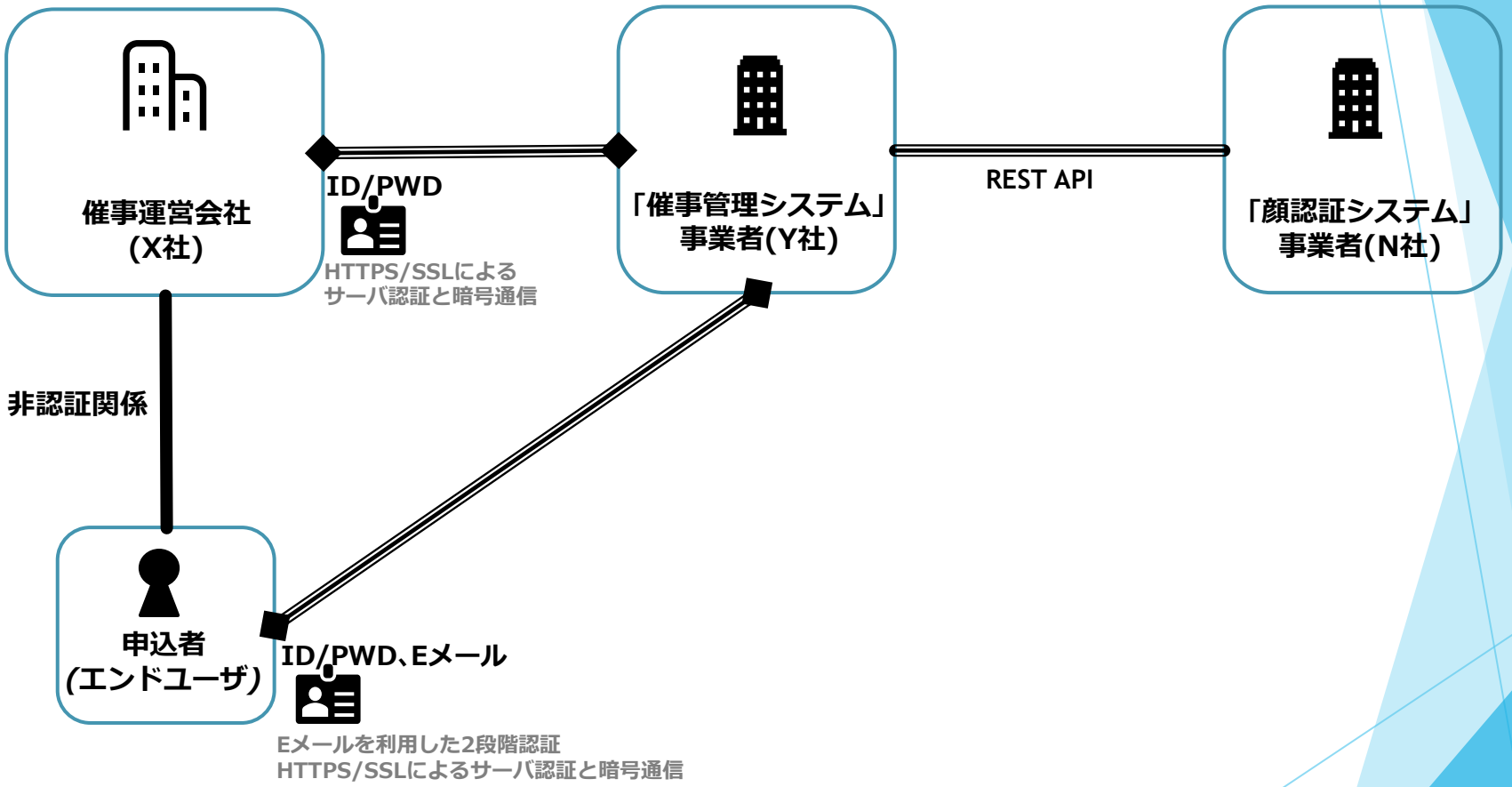
パーソナルデータを含むデータセットがどこに存在するのかを明確にする

入場時(顔認証)

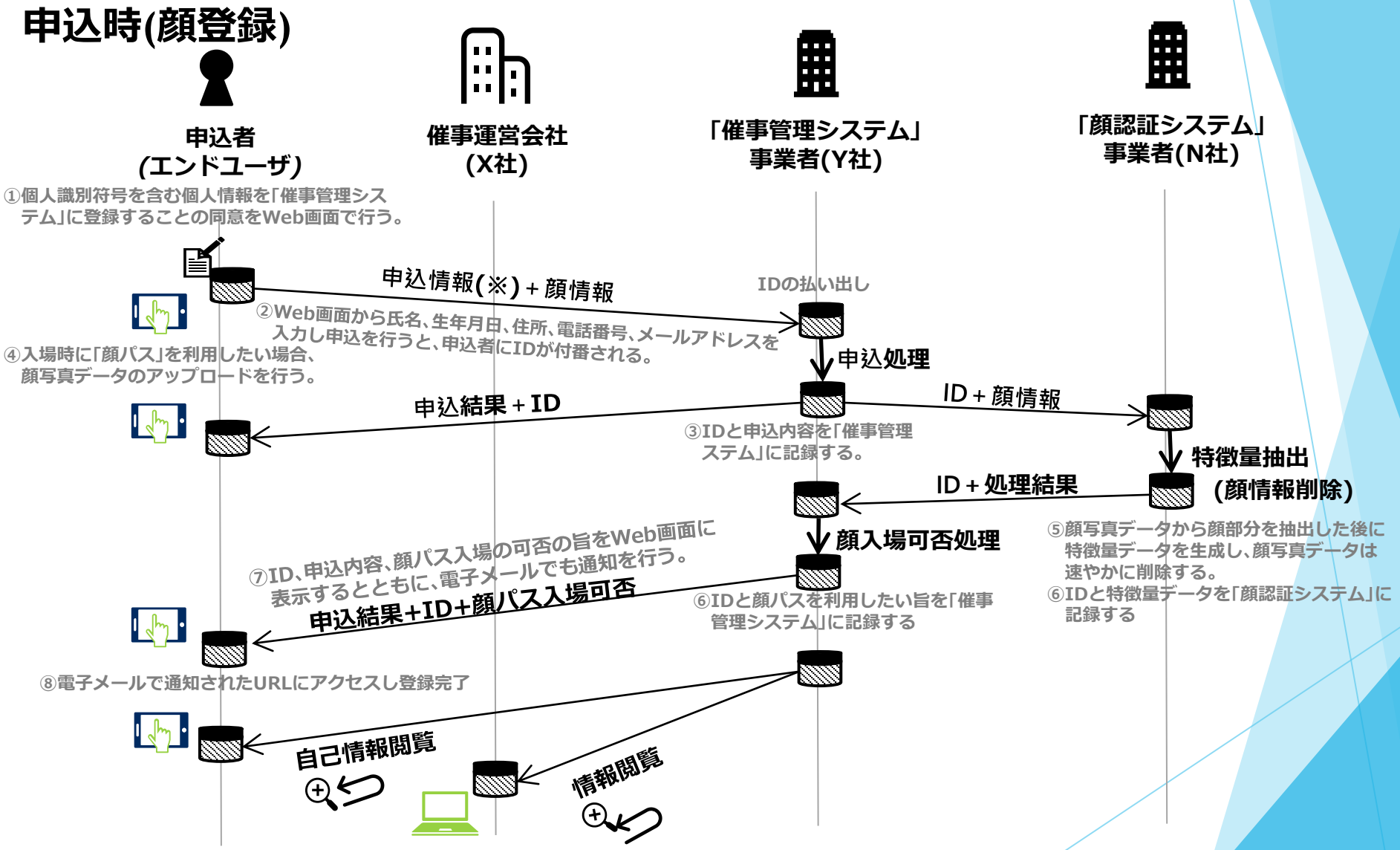


4. トラストリソースマップ

関係者間の認証・認可の関係を明確にする

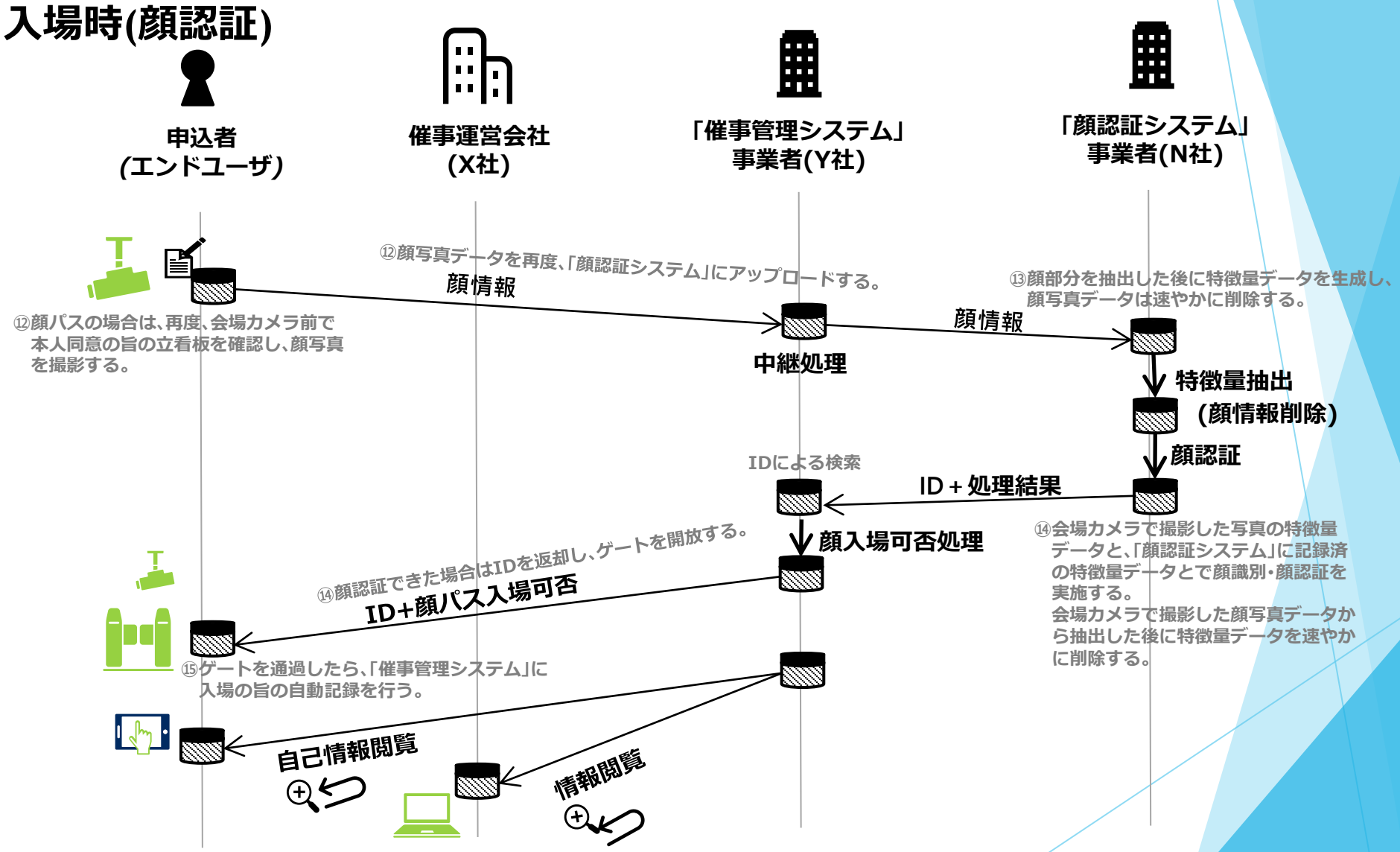


5. データフローシーケンス



※:氏名、生年月日、住所、電話番号、メールアドレス、パスワード

5. データフローシーケンス



5. データフローシーケンス

No.	場面	機能要件	入力	記録	出力
1	申込	個人識別符号を含む個人情報を「催事管理システム」に登録することの同意をWeb画面で行う。同意した場合のみ申込者登録へ進む。	本人同意		
2	申込	Web画面から氏名、生年月日、住所、電話番号、メールアドレス、希望パスワードを入力し申込を行うと、申込者にIDが付番される。	申込者の個人情報		ID
3	申込	IDと申込内容を「催事管理システム」に記録する。		申込者の個人情報とID	
4	申込	入場時に「顔パス」を利用したい場合は、顔写真データを「催事管理システム」に登録することの同意をWeb画面で行う。同意した場合のみ顔写真データのアップロードへ進む。	本人同意		
5	申込	Web画面からIDと顔写真データのアップロードを行うと、顔部分を抽出した後に特徴量データを生成し、顔写真データは速やかに削除する。	顔写真		特徴量
6	申込	IDと特徴量データを「顔認証システム」に記録するとともに、IDと顔パスを利用したい旨を「催事管理システム」に記録する。		特徴量とID、顔パス可否	
7	申込	ID、申込内容、顔パス入場の可否の旨をWeb画面に表示するとともに、電子メールでも通知を行う。			電子メール
8	申込	電子メールで通知されたURLにアクセスすることで登録完了となる。	確認	確認完了	
9	取消	Web画面から、申込時のIDとパスワード、生年月日を入力し、「申込取消」のメールを要求する。	ID、生年月日		電子メール
10	取消	「催事管理システム」から「申込取消」の電子メールが通知されるので、電子メールで通知されたURLにアクセスすることで取消を行う。	確認	取消完了	
11	取消	取消が行われた場合には「顔認証システム」から「特徴量データ」を速やかに削除し、「催事管理システム」からは、「(顔パスを含む)申込内容」を速やかに削除する。問合せ対応のためIDだけは取消済のIDとして記録し保持しておく。		申込者の個人情報、特徴量、顔パスの情報を削除	

5. データフローシーケンス

No.	場面	機能要件	入力	記録	出力
12	(顔)入場	顔パスの場合は、再度、会場カメラ前で本人同意の旨の立看板を確認し、顔写真を撮影し顔写真データを再度、「顔認証システム」にアップロードして識別・認証することの同意を行う。同意された場合のみウォークスルー用のゲートに進む。	本人同意		
13	(顔)入場	会場カメラで撮影した顔写真データのアップロードを行うと、顔部分を抽出した後に特徴量データを生成し、顔写真データは速やかに削除する。	顔写真		特徴量
14	(顔)入場	会場カメラで撮影した写真の特徴量データと、「顔認証システム」に記録済の特徴量データとで顔識別・顔認証を実施し、認証できた場合はIDを返却し、ゲートを開放する。会場カメラで撮影した顔写真データから抽出した後に特徴量データを速やかに削除する。	特徴量		認証結果、ID
15	(顔)入場	ゲートを通過したら、「催事管理システム」に入場の旨の自動記録を行う。	ID	入場済	
16	(顔以外)入場	顔パスを行わない場合、もしくは顔認証で結果がエラーになった場合は、申込時に送付された電子メールもしくはWeb画面からIDを提示し、あわせて、顔写真付の身分証明書を提示することで、会場職員が「催事管理システム」を検索して確認を行い、会場職員がゲートの開放を行う。	ID		申込者の個人情報とID
17	(顔以外)入場	入場者がゲートを通過したら、会場職員がゲートを閉め、会場職員が「催事管理システム」を操作して入場の旨の記録を行う。	ID	入場済	

6．法制関係図

	申込者(エンドユーザ)	催事運営会社(X社)	「催事管理システム」事業者(Y社)	「顔認証システム」事業者(N社)
申込者(エンドユーザ)	NA	売買契約等 個人情報に関する同意 個人情報保護法	個人情報保護法	個人情報保護法
催事運営会社(X社)	売買契約等 個人情報に関する同意 個人情報保護法	NA	委託契約 個人情報保護法	必要かつ適切な監督 個人情報保護法
「催事管理システム」事業者(Y社)	個人情報保護法	委託契約 個人情報保護法	NA	委託契約 個人情報保護法
「顔認証システム」事業者(N社)	個人情報保護法	必要かつ適切な監督 個人情報保護法	委託契約 個人情報保護法	NA

7.2　本評価書と特定個人情報保護評価書との対照関係

- 別添ご参照
  https://www.miyauchi-law.com/f/210812necpia_taishou.pdf

B)　姫路市による行政情報分析に対するPIAの例

総務省実証事業における姫路市行政情報分析基盤

個人情報リスク評価PIA++
（Privacy Impact/Risk Assessment)

初版　平成30年3月
改訂　平成30年5月

１　本評価の範囲・対象

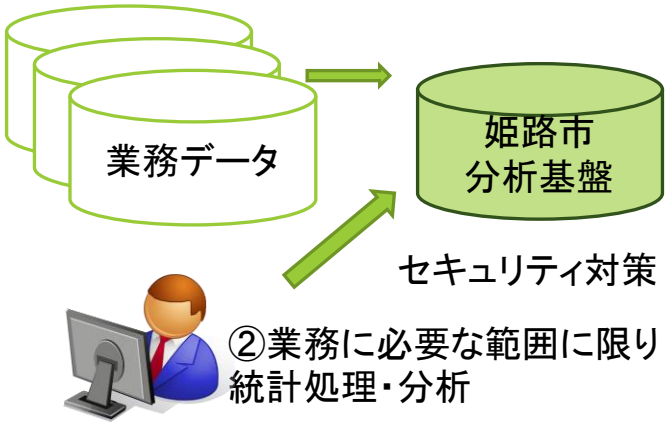
姫路市行政情報分析基盤

- 本評価は、「姫路市行政情報分析基盤」（以下「分析基盤」といいます。）をその範囲・対象としています。
- 分析基盤とは、市役所の持つ業務データを活用して、エビデンスに基づくより良い政策立案（EBPM）を行うために、姫路市が開発・運用するデータ分析基盤システムを指します。総務省が平成２９年度に実施した「地域におけるビッグデータ利活用の推進に関する実証」事業としても採用されています。
- 総務省実証事業では子育てデータの分析を行っていますが、このほかにも市の事業として、住基データ、特定健診データ、業務ログの分析を行っており、将来的にはこれらの分野にとどまらず、市役所の持つ業務データを部局横断的に利活用できる政策支援機能としての運用を目指しています。平成２８年より構築を開始しています。そのうち、総務省実証事業の期間は、平成２９年１０月から平成３０年３月３１日までです。
- 本評価は、弁護士水町雅子が、姫路市及び株式会社エーティーエルシステムズ（姫路市受託事業者、以下「ATL」といいます。）から資料提供やヒアリングを受けながら実施したものです。姫路市及びATLは本評価書に記載された内容に偽りがないことを事前に確認しています。

２　姫路市分析基盤は、どのようなものか

自治体の持つ業務データをもとに分野横断的な分析を行い、より良い行政・政策を目指す仕組み

業務データには個人情報が多く含まれます。
プライバシー権侵害や不正行為を防止するため、本評価記載の通りの厳格な措置を講じます。



主なポイント

① 子育て、住民基本台帳等の業務データ（個人情報）から、**氏名等を削除**して、**誰の個人情報か一見してわからない状態に加工**（抽象化）します

② **市役所職員が**自身の**業務に必要な範囲に限り**、①の情報を元に、市の現状などを**統計処理**します。市職員が閲覧できるのは統計情報のみで、①情報は閲覧することはできません。

③ 分析結果を元に政策立案、課題解決、住民サービス向上等を検討して、**より良い行政**を目指します

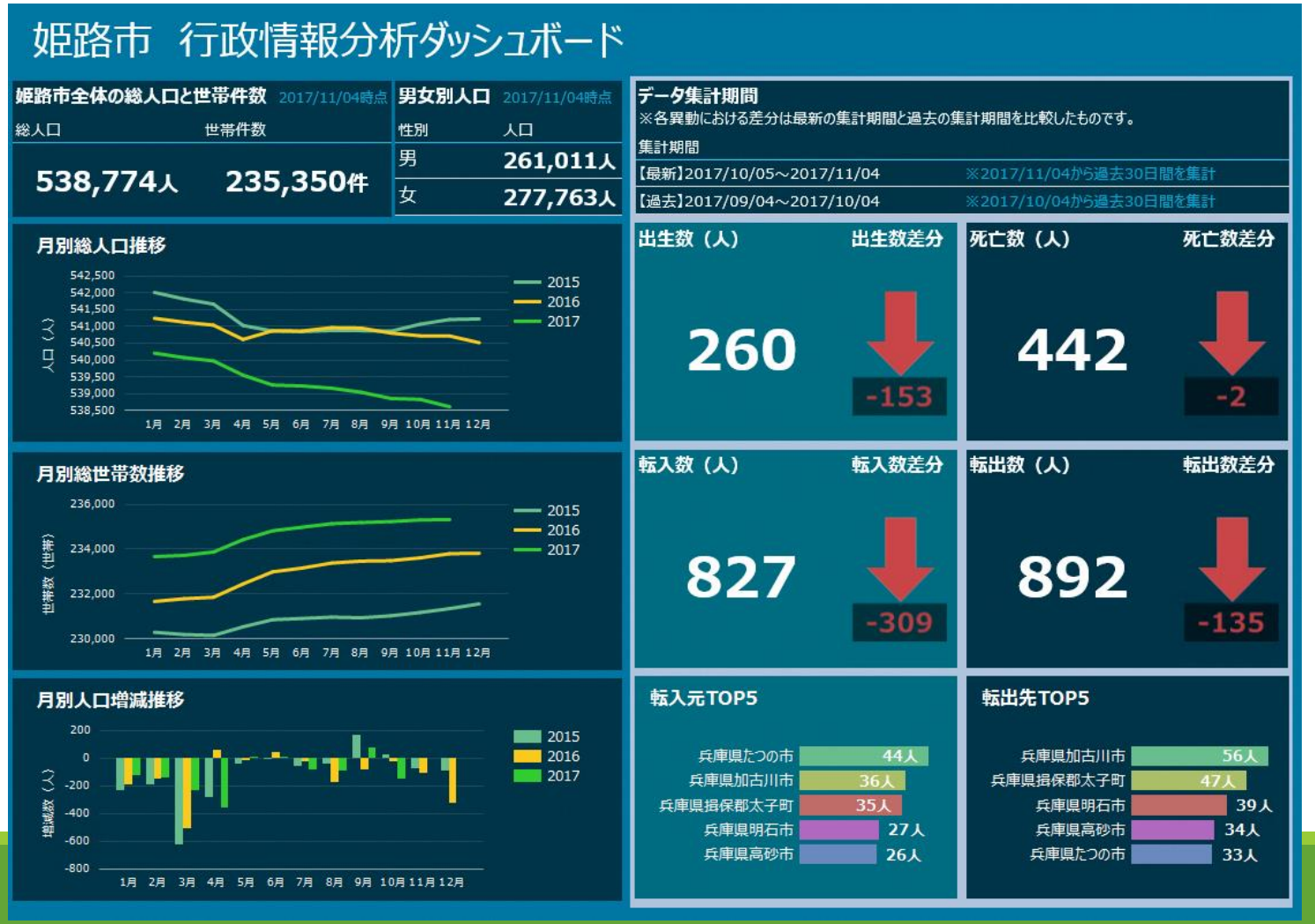
④ 分析・統計作成作業は、地方公務員法上、守秘義務を負う市職員が行います。守秘義務違反等には刑罰や懲戒処分を科せます。

⑤ 姫路市分析基盤は、インターネットと切り離された環境にあり、姫路市が厳重に管理している端末から操作します。セキュリティ対策を厳重に講じています。

２　姫路市分析基盤は、どのようなものか

分析画面のイメージ

- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 住民基本台帳データを分析し図示等することで、人口推移、出生数推移、転出入状況、経年変化等をとらえ、将来予測も可能となります。
- 正確な情報を精緻に分析することで、市の今後の政策検討の基礎データとし、より良い行政政策を検討・実行していきます。
- 右の数値等はダミーです。



２　姫路市分析基盤は、どのようなものか

分析画面のイメージ

- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 子ども子育てデータを分析し表形式で集計等することで、施設、認定区分、地域、定員等の観点から、現状を把握します。
- 正確な情報を精緻に分析することで、市の今後の政策検討の基礎データとし、より良い行政政策を検討・実行していきます。
- 右の数値等はダミーです。

姫路市　教育・保育施設利用状況【概要】

◆施設分類

分類	定員				利用児童数				定員充足率			
	1号	2号	3号	計	1号	2号	3号	計	1号	2号	3号	計
こども園	2,298	3,166	1,577	7,041	2,820	0	1,758	4,578	122.7%	0.0%	111.5%	65.0%
公立幼稚園	1,435	0	0	1,435	1,923	31	1,311	3,265	134.0%	+∞	+∞	* 227.5%
保育園	404	923	633	1,960	1,490	0	980	2,470	368.8%	0.0%	154.8%	* 126.0%
保育所	0	3,450	1,994	5,444	3,332	74	2,233	5,639	+∞	2.1%	112.0%	* 103.6%
合計	4,137	7,539	4,204	15,880	9,565	105	6,282	15,952	231.2%	1.4%	149.4%	100.5%

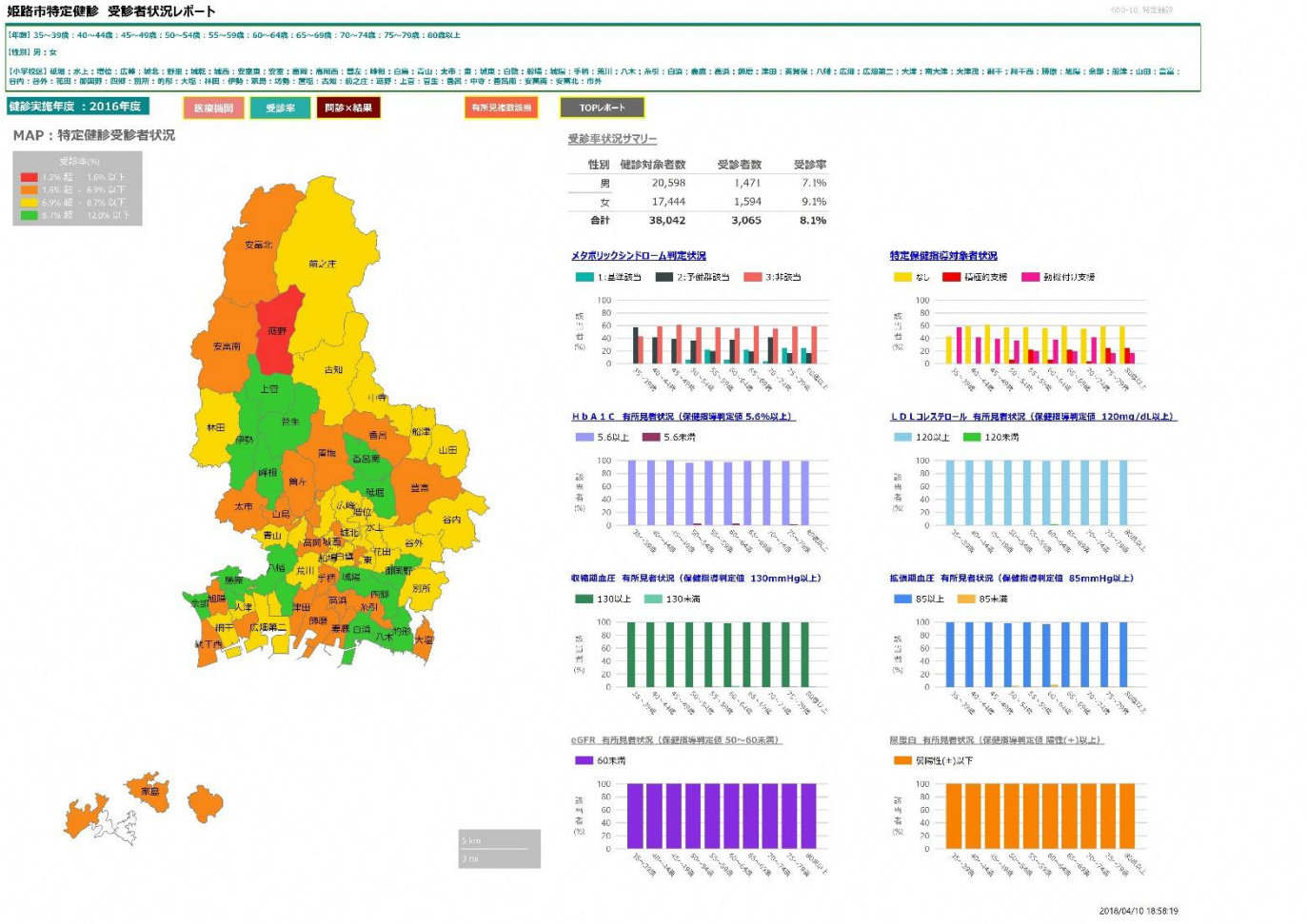
◆地域ブロック別

地域ブロック	定員				利用児童数				定員充足率			
	1号	2号	3号	計	1号	2号	3号	計	1号	2号	3号	計
安富	0	105	35	140	48	11	41	100	+∞	10.5%	117.1%	71.4%
家島	70	0	0	70	147	0	103	250	210.0%	NaN (非数値)	+∞	* 357.1%
広畑	274	870	412	1,556	914	0	543	1,457	333.6%	0.0%	131.8%	93.6%
香寺	215	222	133	570	264	0	196	460	122.8%	0.0%	147.4%	80.7%
飾磨	513	948	510	1,971	1,158	0	712	1,870	225.7%	0.0%	139.6%	94.9%
西部	280	712	368	1,360	705	0	472	1,177	251.8%	0.0%	128.3%	86.5%
中部第一	315	670	415	1,400	973	31	645	1,649	308.9%	4.6%	155.4%	* 117.8%
中部第二	733	951	641	2,325	1,617	0	1,009	2,626	220.6%	0.0%	157.4%	* 112.9%
東部	290	718	347	1,355	977	52	700	1,729	336.9%	7.2%	201.7%	* 127.6%
灘	338	574	342	1,254	652	11	441	1,104	192.9%	1.9%	128.9%	88.0%
北部	616	805	419	1,840	1,053	0	654	1,707	170.9%	0.0%	156.1%	92.8%
夢前	130	154	86	370	236	0	186	422	181.5%	0.0%	216.3%	* 114.1%
網干	363	810	496	1,669	821	0	580	1,401	226.2%	0.0%	116.9%	83.9%
合計	4,137	7,539	4,204	15,880	9,565	105	6,282	15,952	231.2%	1.4%	149.4%	100.5%

２　姫路市分析基盤は、どのようなものか

分析画面のイメージ

- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 特定健診データを分析し地図情報と重ねる等することで、地域ごとの受診率などをわかりやすく図示できます。
- 現状を分析することで、特定健診の受診率向上、ひいては住民の健康状況の向上をめざします。
- 右の数値等はダミーです。



２　姫路市分析基盤は、どのようなものか

分析画面のイメージ

- 分析基盤は、姫路市職員のみ操作できます。分析基盤を通じて作成した統計結果は会議資料や市ホームページ等で利用することがあります。
- 市役所、支所などの利用データを分析することで、窓口の利用状況等がわかり、市役所サービスにおける住民の利便性向上や効率化などをめざします。
- 右の数値等はダミーのため、偏りがありますが現実の数値等ではありません。

施設分類	施設名	日		火		水		木		金		土		合計
		合計		合計		合計		合計		合計		合計		
市役所本庁舎	姫路市役所本庁舎	4	1.37%	247	84.88%	11	3.78%	6	2.06%	21	7.22%	2	0.69%	291
地域事務所	夢前事務所		0.00%	22	100.00%		0.00%		0.00%		0.00%		0.00%	22
支所・出張所	船津市役所		0.00%	71	100.00%		0.00%		0.00%		0.00%		0.00%	71
	豊栄出張所		0.00%	24	100.00%		0.00%		0.00%		0.00%		0.00%	24
	西出張所		0.00%	16	100.00%		0.00%		0.00%		0.00%		0.00%	16
	林田出張所		0.00%	21	100.00%		0.00%		0.00%		0.00%		0.00%	21
サービスセンター	坊勢サービスセンター		0.00%	21	100.00%		0.00%		0.00%		0.00%		0.00%	21
合計		**4**	**0.86%**	**422**	**90.56%**	**11**	**2.36%**	**6**	**1.29%**	**21**	**4.51%**	**2**	**0.43%**	**466**

３　期待される効果

■ 人口減少・少子高齢化が進展する中で、限られた「ヒト・モノ・カネ」を「情報」により、これまで以上に効果的かつ計画的に活用することより、効率的な行政運営と住民のQOL向上を目指します。

■ 前例や職員の経験・勘などに依存しない、第三者による検証が可能で透明性の高いエビデンスベースの政策立案を推進します。

■ 行政データの有効活用を通して、より良い行政・住民サービスの向上を図ります。

３　期待される効果

正確な課題認識、将来予測

- 現状を正確に把握し、過去の状況と比較することで、自治体の持つ課題を正確に認識できます。
  - 例えば、待機児童問題では、どこにどのような待機児童がいてどの地域にどのような保育施設ができればよいのか、今の保育園児が小学生になった際に小学校や学童保育の過不足などの問題はないのか等、自治体の現状と課題を正確に把握することが必要です。
  - 住基データの分析でいえば、最近の転出入の状況を数値で正確に分析することで、どのような世帯が転出しているのか、人口増のためにはどのような施策が必要かなどを分析することも可能です。
  - そのほかにも、市の業務データを分析することで、例えばバス路線が住民ニーズに合致しているか、支所等出先窓口の設置場所が適切か、道路整備の不十分な場所がないか、高齢単身世帯・子育て世帯が多い地域はどこか等、様々な現状・課題を把握することができます。
  - これらはあくまで例に過ぎず、様々な施策において、現状を数値として正確に分析することで、自治体の解決すべき課題を的確に認識することができます。

３　期待される効果

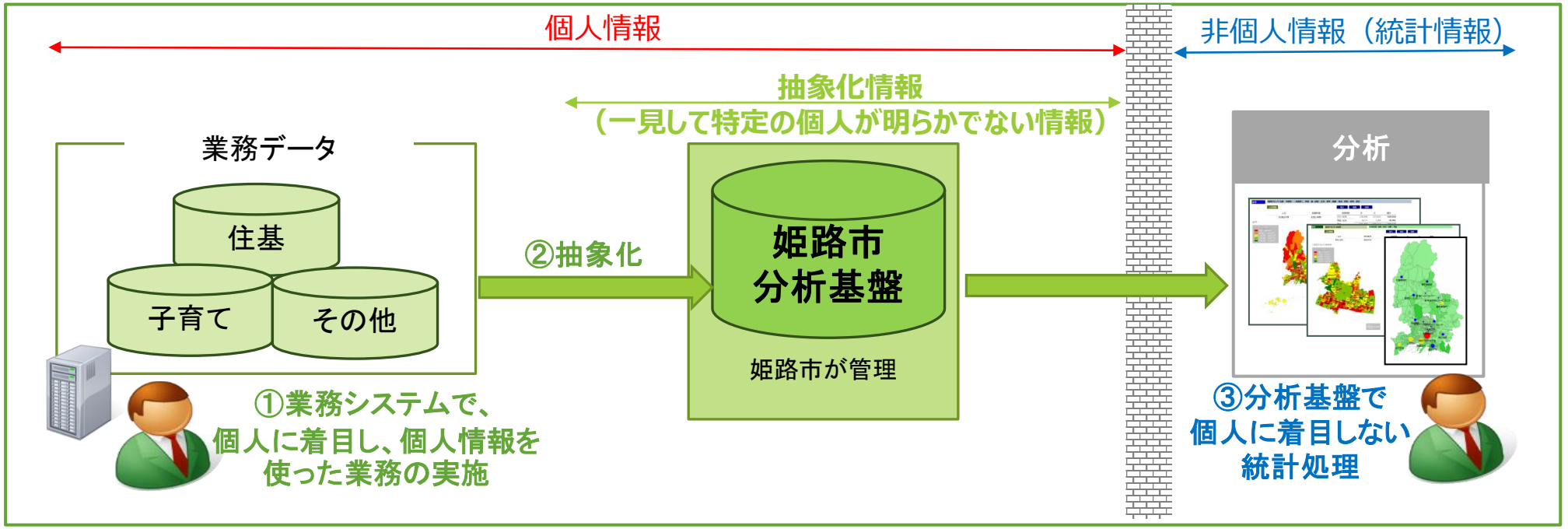
業務改善・効率化

- 分析作業等時間の大幅カット
  - 自治体では、現状分析や計画立案等の業務を行っていますが、職員が個別にデータを集めて表計算ソフト等で分析するのでは、作業に相当の時間を要します。分析基盤を用いると、これまで行ってきた作業時間を大幅にカットすることができました。
  - 例えば、小学校区別年齢別児童数の分析作業に、これまでは56時間を要していましたが、分析基盤では10分以内で実施できます。

- これまでは行えていなかった分析も可能に
  - 例えば、これまでは地域ブロック別0～5歳児の定住率・異動状況や出生児数の校区別地域ブロック別の分析は行えていませんでしたが、分析基盤では10分以内で分析できます。異動状況も可視化されたため、何歳児がどの地域に引っ越す傾向があるかなどを把握することが可能となりました。

- 業務効率化・質の向上
  - 資料作成時間を圧倒的に短縮することができ、かつ、より多くの情報をアウトプット出来るようになりました。
  - 問合せを受けてから回答までのスピードを早くすることができました。
  - 地図情報と重ねて図示できるため、視覚的な説明が可能となり、関係者へのわかりやすい説明が可能になりました。
  - 業務の定型化も促進でき、担当者の能力に依存しないため人事異動に伴う引継ぎも容易となるのではないかと期待されます。

４　姫路市分析基盤の全体像

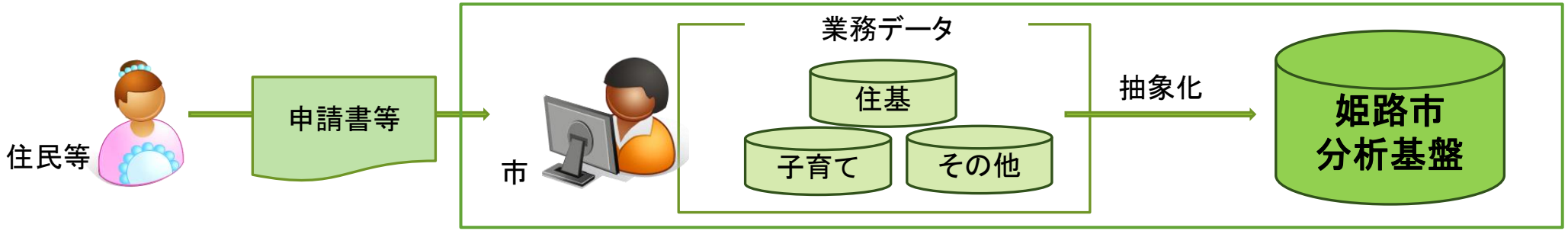


① 市では、行政サービス・業務を実施するために、住基情報、子育て情報その他の業務データ（個人情報を含む）を収集・利用・保管等しています。市職員は原則として自分の担当業務に必要な個人情報のみを取り扱っています。

② 業務データから氏名等を削除して、一見して誰の情報かわからないデータに加工します（抽象化）。抽象化した情報を分析基盤に取り込みます。分析基盤上のデータを、職員等は直接閲覧・ダウンロード・印刷等することはできません。

③ 市職員は分析基盤を利用して、統計処理を行います。統計情報は非個人情報であり、個人に着目しない統計処理のみを行います。

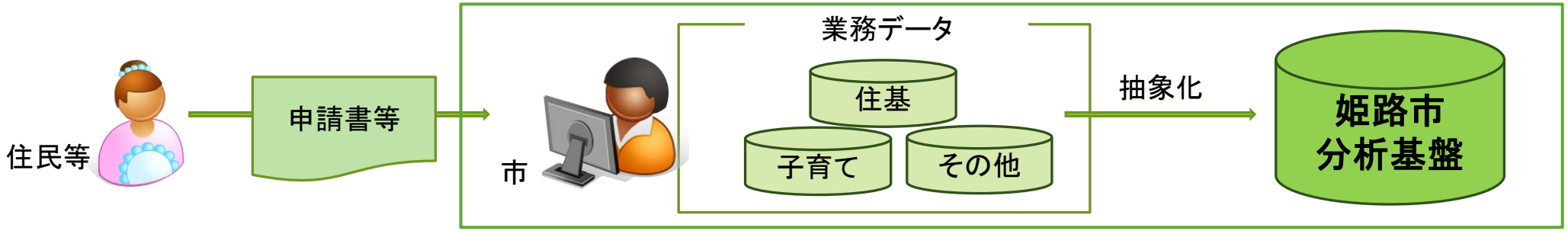
５　姫路市分析基盤で個人情報をどう取り扱うか



◆ **誰の個人情報**：　姫路市の住民・過去住民であった方（約78万5千人）、姫路市職員（約3800人）

- 分析基盤では個人に着目した分析を行わず、あくまで統計処理・統計的把握が目的のため、市の持つ業務データから氏名を削除、住所の番地以下を削除、生年月日は月齢・学年を計算したうえで日を削除、番号・ID等は業務システムで用いているものとは異なるものとし、元の業務データと突き合わせできないよう不可逆変換した情報を保持しています。
- 今後、住基・子育て・特定健診・業務ログという現状のデータ範囲以外に分析基盤を展開していく場合も、既に市で行政サービス・業務を実施するために保有している個人情報から、氏名等を削除して、一見して特定の個人がわからないよう抽象化した上で、分析に利用していきます。
- 氏名等を削除して抽象化しているため、一見して誰の情報かはわからないようになっていますが、氏名が記録されていなくても、どの保育所に入所しているか、抽象化された住所等から、誰の情報かがわかる場合もあります。そこで、市では抽象化していても個人情報として、個人情報保護条例を遵守して、厳格に取り扱います。

５　姫路市分析基盤で個人情報をどう取り扱うか



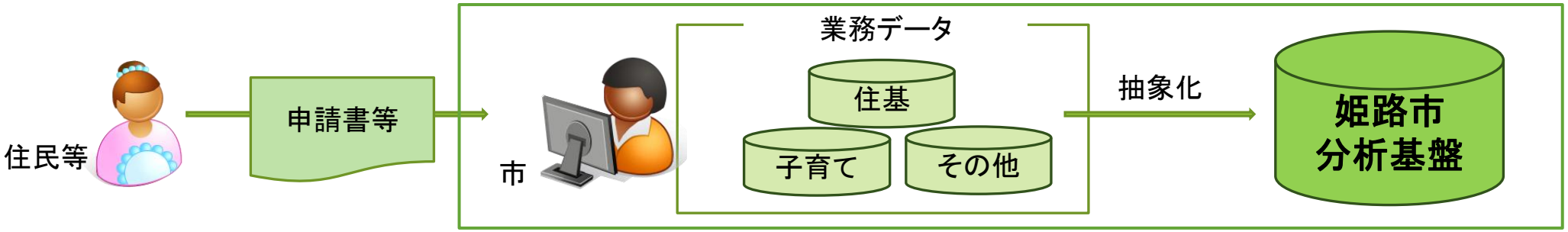
◆ どんな個人情報：

- 子育て：　児童名簿（児童生年月、在園施設、保護者情報、保育料、認定区分（保育の必要性・必要量判定）等）、住民基本台帳情報（住所等）を取り扱います。これらに、非個人情報である保育所情報（所在地、定員等）、認可外施設情報（種類、定員等）を組み合わせて分析しています。
- 住基：　住民基本台帳情報（現住所、前住所、学区等）を取り扱います。
- 特定健診：　年齢、性別、住所、身長、体重、喫煙・飲酒の有無、検査結果等の情報を取り扱います。
- 業務ログ：　端末番号、帳票番号、処理内容等の情報を取り扱います。

◆ 利用主体：

- 市職員のみ
- 子育て：　こども政策課（数名）　　特定健診：　国民健康保険課特定健診担当（数名）、保健所健康課（数名）
- 業務データ：　住民窓口センター（数名）　　住基：　上記利用課すべて、企画政策推進室（数名）、地方創生推進室（数名）

５　姫路市分析基盤で個人情報をどう取り扱うか



◆ 利用目的：

- 統計処理を実施し、現状分析・将来予測を行い、より良い行政サービス・業務をめざします。

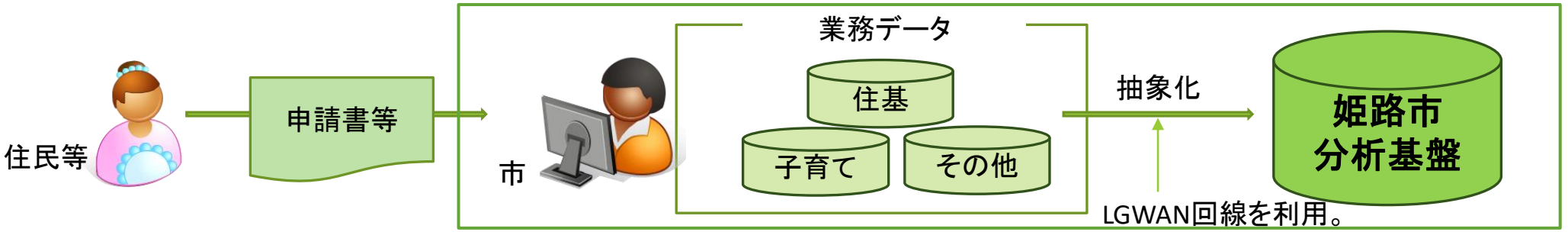
◆ 個人情報の取得経路：

- 姫路市の持つ業務データからシステムを介して、分析基盤に必要な前ページの情報を入手
- 定期的に最新の情報を入手します（統計・分析活用のニーズに応じて、情報ごとに更新頻度を決定）

◆ 個人情報の抽象化：

- 住基情報、子育て情報その他の業務データは分析基盤上にいったん到達するも、その場で抽象化され、保存されません。
  保存される情報は、次の通り業務データを抽象化した情報です。
  - ✓ 番号関連（世帯番号も同様）→不可逆変換
  - ✓ 氏名関連　→全て削除
  - ✓ 生年月日　→年齢算出後、日を削除し、生年月・学年月情報として保持
  - ✓ 住所関連　→番地以下を削除
  - ✓ 続柄　→一部削除

５　姫路市分析基盤で個人情報をどう取り扱うか



◆ 個人情報の取得経路

- 姫路市の持つ業務データからシステムを介して、分析基盤に必要な前ページの情報を入手
- 定期的に最新の情報を入手します（統計・分析活用のニーズに応じて、情報ごとに更新頻度を決定）
  → 「１２　その他のリスク対策（個人情報の取得に関して）　不正確な個人情報を取得しないか」ご参照

◆ 個人情報の保管

- 分析基盤で扱う情報は、①業務データ（生の個人情報）②抽象化情報（個人情報）③統計情報の３種です。
- ①業務データは、前記の通り、分析基盤では保存されず、基幹系業務システム等で保存します。
- ②抽象化情報は、 破棄せずに保存します。不要な情報は破棄すべきですが、分析基盤の目的からして、経年変化を把握することが必要であるためです。詳細は、「１５その他のリスク対策（個人情報の管理に関して）」の「不要な個人情報がいつまでも保管されないか、古い個人情報を誤って利用しないか」を参照してください。
- ③統計情報は、必要に応じ破棄します。

６　情報を分析することで、住民等に不利益処分等がなされることはないか

分析基盤では、様々な情報を突合して分析しますが、これによって住民の方等に不利益処分等がなされることはありません。

住民の方等に不利益な処分等は行わない

- 分析基盤による分析の結果を用いて、直接、個々の住民の方等を対象とした事務処理等を市が行うことはありません。例えば、万一、子育て政策の状況分析を行った結果、特定地域の保育所が過多であると判断されても、それを元に、将来的な適正配置を検討することはあっても、保育所の退所をお願いするようなことはありません。
- また、万一、保育料の滞納があった場合に、分析基盤を通して督促等をさせていただくことはありません。分析基盤はあくまで現状分析及び将来予測のための統計分析を行うシステムであり、保育料の収納管理等は、通常業務の中で通常手続を経て行います。
- 住民の方等を対象とした事務処理は、分析基盤とは別の業務システムを利用し、また法律・条例に従って実施します。

プライバシー権が侵害されないように

- →　次ページ参照

7　個人情報を不正にのぞき見・外部提供等されないか

分析基盤では、住民の方等の個人情報を保持しますが、個人情報が不正にのぞき見られたり、外部提供されたりしないように次の措置を講じています。

業務上必要な分析を行うために必要なデータのみ

- 分析基盤上のデータは、氏名等を削除して抽象化することで、データからは誰の情報かが一見してわからないようになっています。
- 分析基盤を利用できるのは市職員のみです。かつ、市職員であっても誰でも利用できるわけではなく、業務上必要な範囲内で、市の手続に沿ってアクセス権限を認められた範囲にのみアクセスできます。
- 分析基盤上のデータを市職員が直接閲覧することはできず、ダウンロード等もできません。分析ツールで統計処理（集計処理）された状態でしか閲覧できません。
- 市職員は、分析基盤利用課（担当課）・データ保有課・システム管理課とで事前に妥当性をチェックし作成されたレポート様式に沿った統計処理、レポート作成を行います。したがって、個人的興味から、不正な分析を行うことは、システムの機能上、できません。また市職員が実施した分析内容はログとして保存し、所属長等が、「いつ」「誰が」「どのような条件で」分析したかを、ログを確認することでチェックでき、これによっても不正を防止します。
- 複数の部署が持つデータを突合して分析することもありますが、業務上必要な統計処理のみ行い、そのために必要な情報以外は突合・利用できないようにシステム上制御しています。
- データは暗号化されているので、万一、分析基盤のデータを持ち去られてもそれだけでは閲覧することはできません。

外部提供は行いません

- 分析基盤は市職員が利用するのみで、分析基盤で保持する情報を外部提供することは原則としてありません。市以外に分析基盤で保持する情報を提供することは原則としてありません。例外としては、警察の捜査に提供する等の場合のみです。
- 分析基盤を用いて作成された統計情報は、公表等する場合もありますが、統計情報ですので、特定の個人がわからない状態に加工されています。

守秘義務等違反には罰則も

- 市職員は法律上守秘義務等を負い、違反した場合は2年以下の懲役又は100万円以下の罰金等に科せられます（姫路市個人情報保護条例58～62条、地方公務員法60条2号）。市によって懲戒処分がなされる可能性もあります。

８　個人情報が漏えいしないか

分析基盤では、住民の方等の個人情報を保持しますが、個人情報の漏えいを防止するために次の措置を講じています。

技術面

- 総務省実証事業において分析基盤はLGWAN–ASPというインターネットから遮断された環境にあります。総務省実証事業以外の分析基盤は姫路市独自環境（オンプレミス環境）にあり、インターネットから遮断されLGWAN系からも分離された基幹系（個人番号利用事務系）ネットワーク環境です。よって、インターネット経由等での不正アクセスやコンピュータウィルス感染、SPAM メール等の脅威から守られています。
- 通信経路における盗聴対策として、データはHTTPSにより暗号化された状態で通信経路上を伝送されます。
- 利用者認証は事前に許可された市職員のみアクセスできるよう、認証カードとパスワードによる2要素認証を行います。

システム設計・運用面

- 業務データを分析基盤に取り込む際は閉域ネットワーク内で許可された職員が行います。作業記録はログとして取得します。通信は暗号化されます。分析基盤に入力された業務データは即時に抽象化データに変換され、元データは破棄され漏えいの危険性を最小限にします。抽象化データはDBに保持されますが、通常利用する分析基盤APからデータの変更等を行う機能を実装していないため、通常の運用作業でデータの改ざんや漏えいは発生ません。DBサーバに対する直接のアタックについては技術面での対策にて対応します。

法制度面

- 既述の通り、市職員は法律上守秘義務等を負い、違反した場合は2年以下の懲役又は100万円以下の罰金等に科せられます（姫路市個人情報保護条例58～62条、地方公務員法60条2号）。市によって懲戒処分がなされる可能性もあります。

９　統計情報のための適切な加工がなされるか

分析基盤では統計情報を作成しますが、加工が不十分であると、そこから特定の個人が識別されることがありえます。
市では、それを防止するために次の措置を講じています。

適切な加工処理

- 分析基盤では氏名等を削除した抽象化情報のみを保持します。不十分な加工状態のデータを取り込むことがないよう、また氏名等を完全に削除し、番号・ID等を完全に不可逆変換できるように、システム側で、加工処理を自動実行しながら、分析基盤に取り込みます。
- 既述の通り、市職員は抽象化された個人情報自体は閲覧できず、ダウンロード等もできません。分析ツールで統計処理（集計処理）された状態でしか閲覧できません。
- 統計情報であっても、少数データから特定の個人が識別されないよう、統計処理の結果、該当人数が少数となった場合は、画面表示上、「〇名」とは表示させずに、「*」で表示します。

不適切な行為を監視

- 統計情報であっても、万一、違法な意思をもった市職員がいて、特定の個人を追跡する等の目的で、他の業務データと照合したり調査する等の不正行為を行った場合には、可能性は低いものの、特定の個人が識別できることも考えられます。こういった違法行為やその他の違法行為を防ぐためにも、市では、分析基盤で職員がどのようなことを行っているかログを取得し、不適切な行為が行われないよう監視します。

10　なぜ分析基盤を設けるのか

既存の業務システムでデータ分析をするのではなく、今回、分析基盤を設けたのは、次の理由からです。

これまでとの差異

- これまでも市では業務上必要な分析・統計処理を行ってきました。しかしこれまでは、個別業務ごとに、個々にデータを他課から受領し、内部手続を行い、表計算ソフトや個別システムなどで分析・統計処理を行ってきました。そのため、分析・統計処理に至るまでのプロセスに多くの時間を要し、スピーディーで効率的な分析・統計処理が行えないという課題がありました。また、個別業務ごとの分析・統計処理だと、システム面での保護措置レベルにバラツキが生じるなど、情報セキュリティ上の懸念がありました。
- そこで今回、分析基盤を設けることで、データに十分な抽象化加工を行った上で、必要なデータを安全・迅速に受領でき、かつ不適切な行為が行えないようシステム面での保護措置を施した環境を整備しました。
- また、個人情報保護条例への適合性やプライバシー権保護上の措置などを、総務省が設置した有識者会議、そして市が依頼した個人情報を専門とする弁護士等と協議し、個人情報保護条例適合性等の検討を行っています。これにより、個別業務ごとに個々に内部手続や条例適合性検討を行うのではなく、市として統一的かつより高度な個人情報保護・プライバシー権保護を企図しました。

費用対効果

- 分析基盤には一定の費用が必要となりますが、個別業務ごとに、個々にデータを他課から受領し、内部手続を行い、表計算ソフトや個別システムなどで分析・統計処理を行うよりも、スピーディーで効率的な分析・統計処理を行うことができます。削減できる作業時間数やリスク、EBPMの推進による行政経営の最適化を踏まえると、費用対効果上も適切であると考えています。

11　なぜ本人から同意を得ないのか

分析基盤では、個人情報保護条例に基づき、ご本人からの同意を得ることなく、統計処理を行います。その理由は次の通りです。

現状分析・将来予測のために網羅的データが必要

- 市が正確に現状分析・将来予測を行うためには、市の状況を取り巻くデータを網羅的に分析する必要があります。データに偏りがあると、偏った分析しか行えず、現状を的確に分析することが困難となる恐れがあります。
- ご本人から同意を得た場合のみ統計処理を行うとすると、一部の方のデータのみ統計処理することとなる可能性があり、データに偏りが生じることも考えられます。
- 市が正確に現状分析・将来予測を行うことは、住民ニーズや現実の課題に即した的確な行政運営を行ったり住民サービスを向上させるために必要なもので、公益性が認められると考えられます。正確な現状分析・将来予測を行うために、個人情報保護条例上認められている、本人同意以外の方法を採用しています。
- ご本人から同意を得ずに統計処理を行いますが、プライバシー権等を侵害することがないよう、この評価書に記載した厳格な措置を講じます。

個人情報保護条例を遵守

- 個人情報保護条例上認められている方法を採用しています。
- なお分析基盤は、総務省の実証事業として採用されていることもあり、総務省が設置した有識者会議、そして市が依頼した個人情報を専門とする弁護士が個人情報保護条例適合性等の検討を行っています。

12　その他のリスク対策
（個人情報の取得に関して）

分析基盤では上記のほか、個人情報の取得に際して次の措置を講じています。

個人情報を過剰取得しないか

- 統計・分析に不必要な個人情報を取得することがないよう、各統計・分析に必要なデータのみを分析基盤に取り込むように設計します。担当者だけで分析基盤に取り込むデータを決めることはできません。システム所管課とデータ保有課と分析基盤利用課（担当課）とで相互チェックします。

不正確な個人情報を取得しないか

- 地方公共団体が行政サービスや業務を実施する上で利用している業務データを用います。業務データから氏名等を削除する等して一定の加工を加えますが、その際、誤った加工を加えないよう設計の上テストを行っています。
- 業務データの性質ごとに、最新の情報も追加して分析基盤に取り込むことで、正確な統計・分析を行います。例えば住民基本台帳データ・業務ログデータは、日々異動が生じているため、現在は週1回のサイクルで分析基盤に取り込んでいます。特定健診データは年１回、子育てデータは年2回です。

取得の際に個人情報が漏えい・紛失等しないか

- 既述の通り、業務データを分析基盤に取り込む際は、インターネットと完全に切り離された環境を用います。電子媒体等を用いると紛失リスク等もありえるため、業務システムから閉域ネットワーク経由で取り込みます。

取得の際に不正が起きないか

- 業務データを分析基盤に取り込む際は、システム上で実行するため、不正な意図をもって不正データを分析基盤に取り込むことはシステム仕様上できません。また業務データ自体の取得については、姫路市個人情報保護条例8条１項に基づき、事務の目的達成に必要な範囲内でのみ個人情報を収集しています。

13　その他のリスク対策
（個人情報の利用・提供に関して）

分析基盤では上記のほか、個人情報の利用・提供に際して次の措置を講じています。

個人情報を無関係の者に利用されないか

- 分析基盤にアクセスできるのは市職員のみです。かつ、市職員であっても誰でも閲覧できるわけではなく、業務上必要な範囲内で、市の手続に沿ってアクセス権限を認められた範囲にのみアクセスできます。
- アクセス権限の設定は、庁内手続に沿って行います。

本件関係者が個人情報を私的利用・私的複製・悪用等しないか

- →「7個人情報を不正にのぞき見・外部提供等されないか」参照。

個人情報が不正提供されないか

- →「7個人情報を不正にのぞき見・外部提供等されないか」参照。

目的外利用・過剰紐づけされないか

- 業務上必要な統計のためにしか利用できず、そのために必要な情報しか紐づけできないよう、様々な措置を講じています。事前に作成するレポート様式に従ってしか利用できません。
  →「7個人情報を不正にのぞき見・外部提供等されないか」参照。

14　その他のリスク対策
（個人情報の安全管理措置に関して）

分析基盤では上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程

- 全庁的な安全管理体制を整備の上、全庁的にセキュリティポリシー、データ保護管理規程等を整備し職員に周知しています。事故発生手順も作成し職員に周知しています。
- 安全管理体制としては、副市長を「最高情報セキュリティ責任者（CISO）」とし、総務局長を「統括情報セキュリティ責任者」、各所属及び出先機関の長を「情報セキュリティ責任者」に定めています。また、情報セキュリティ事故に関する統一的な窓口として「情報セキュリティ事務局」を設置し、統括情報セキュリティ責任者を委員長とした「姫路市情報セキュリティ委員会」を定期的に開催することで、本市の情報セキュリティに関する重要事項を審議しています。

物理的対策

- 総務省実証事業分については、LGWANというセキュアなネットワークを介したLGWAN-ASPを利用しています。LGWAN-ASPは、地方公共団体情報システム機構が定める基本規程等を遵守し、登録審査に合格したものであり、物理的対策等についても、「総合行政ネットワークASP登録及び接続資格審査要領」等の要求を満たしたものになります。参考→https://www.j-lis.go.jp/data/open/cnt/3/164/1/G-1-1-10_AspShinsaYoryo_20150701.pdf
- 総務省実証事業分以外については、姫路市独自環境（オンプレミス環境）です。入退室管理、人による監視等を行っています。

技術的対策

- →「8個人情報が漏えいしないか」参照

15　その他のリスク対策
（個人情報の管理に関して）

分析基盤では上記のほか、個人情報の管理に際して次の措置を講じています。

委託先の不正が起こらないか

- 分析基盤の管理等を外部事業者に委託します。委託先では必要最小限の者（5～6名程度）にしかデータにアクセスさせないようにします。委託先へのデータ授受は、閉域ネットワークを通して行います。
- 外部事業者とは守秘義務、条例遵守等を定めた契約を締結します。委託先には体制図及び個人単位の誓約書を提出させ、本番データは庁外に持ち出せないようにしています。
- 再委託は、契約で事前承認が要求されます。またインフラ部分（LGWAN-ASPホスティングサービス）以外の再委託は行いません。LGWAN-ASPホスティングサービスは、地方公共団体情報システム機構が定める基本規程等を遵守し、登録審査に合格したものです。

個人情報が誤って消去等されないか

- 定期的にバックアップを取得しています。

不要な個人情報がいつまでも保管されないか、古い個人情報を誤って利用しないか

- 正確な分析・将来予測を行うためには、蓄積されたデータを元に過去からの推移、経年変化の分析が必要です。
- この点、地方公共団体が行政サービス・業務実施に利用している業務データ自体を蓄積していき、分析に活用しようとすると、氏名等も含まれる個人情報であり、また分析に不要な情報まで保存され続けてしまう恐れがあります。また、業務データは公文書管理等の趣旨から、保存年限が市の規則上決まっており、その点からも蓄積が困難です。
- それに対し、分析基盤では、分析に必要な情報のみを保存し、かつ氏名等も削除した情報であり、保存年限も市の文書規則とは異なることから、蓄積データの推移・経年変化・将来予測を行うことに適していると考えられます。

16　その他のリスク対策
（全般に関して）

分析基盤では上記のほか、次の措置を講じています。

点検・監査等

■ システム監査を年1回実施します。

従業者教育

■ 市では、従業者への教育・啓発を行います。委託先であるATLはISMSを取得しており、規定に基づいた情報セキュリティ社員教育を定期的に実施しています。

開示・訂正・利用停止請求

■ 市にて個人情報保護条例に従って、開示・訂正・利用停止請求への対応を行います。請求者本人であることを確認できる書類（運転免許証など）を持参のうえ、市政情報センターにお越しください。
http://www.city.himeji.lg.jp/s30/2212077/_9328/_9344.html

問合せ対応

■ 市では、住民の方等からのお問合せに真摯に対応いたします。
■ 個人情報については姫路市市政情報センターに、システムについては姫路市総務局情報政策室にお問合せください。

17　個人情報保護条例への適合性

- 姫路市個人情報保護条例では、利用規制として9条がありますが、分析基盤はこれに適合しています。条例解釈としては①統計、②目的外利用の2構成が考えられます。本実証ではより丁寧な手続として、まずは②目的外利用を採用しましたが、今後分析基盤が本格展開する際は、①統計で構成することも検討しています。
- ①統計について
  - 最終的な利用形態が特定の個人を識別しない形の場合、統計的にデータを把握しようとする場合は、目的内利用／目的外利用の区別の対象外と考えることも可能であると考えられます。
  - 個人情報保護法制の要を成す、（ア）行政機関や地方公共団体にとっても基本法たる個人情報保護法、（イ）地方公共団体の個人情報保護条例が一般に参考にしている行政機関個人情報保護法、（ウ）統計法の解釈を踏まえ、個人情報保護条例においても上記解釈が可能であると考えられます。
  - まず個人情報保護法を見てみると、統計目的での個人情報の「内部利用（作成）」は、その他の個人情報の利用とは異なり、個人情報保護法16条の規制対象「外」であり、目的外利用とはなりません。なお、統計情報よりも個人情報に近い、匿名加工情報の「内部利用（作成）」であっても、個人情報保護法16条の規制対象「外」であり、目的外利用とはなりません。
  - 次に行政機関個人情報保護法では、統計の公益性の高さ等から、個人情報保護法では一括しては認められていない、統計目的での個人情報の「外部提供」を認めています。個人情報保護法と行政機関個人情報保護法では、利用規制や提供規制等の規定が異なるため、一概にはいえないものの、統計の公益性の高さ等を踏まえると、行政機関個人情報保護法において明文の規定がない統計目的での内部での保有個人情報の「内部利用」についても、個人情報保護法と同様に、目的外利用の対象外という解釈も取りえなくないものと考えられます。
  - 統計法では、一定の統計にかかる個人情報が、行政機関個人情報保護法の適用除外であることが明文化されています（統計法52条1項）。これは、最終的な利用形態、管理規制、統計の元となる個人情報の目的外利用規制、守秘義務・罰則等があることによる。分析基盤でも最終的な利用形態は個人識別性のない形であり、また統計情報の元情報である個人情報自体には、個人情報保護条例上、管理規制、目的外利用規制、守秘義務・罰則等が課せられ、統計法と同様に考えられます。
- ②目的外利用について
  - また、条例上認められる目的外利用という解釈も考えられます。
  - 分析基盤では、児童名簿等の業務データを利用しますが、この個人情報の利用目的と分析基盤における目的は異なるものと考えられます。しかし姫路市個人情報保護条例では目的外利用を一定の範囲で認めており、分析基盤における目的外利用は、姫路市個人情報保護条例9条1項4号「実施機関がその所掌する事務の遂行に必要な限度で目的外利用をする場合であって、当該個人情報を利用することについて相当な理由のあるとき」に該当すると考えられます。

18　まとめ

- 本評価において、以下の項目について検討し、プライバシー等への影響を確認しました。
  - スキーム（1・2・4参照）
  - 個人情報利活用の効果（3参照）
  - 個人情報の取扱い（4・5参照）
  - 不利益処分等の対策（6参照）
  - 不正利用・不正提供リスク対策（7・13参照）
  - 個人情報の漏えいリスク対策（8・14参照）
  - 統計情報におけるリスク対策（9参照）
  - 現状との差異・費用対効果（10参照）
  - 同意（11参照）
  - 個人情報の取得リスク対策（12参照）
  - 個人情報の利用リスク対策（13参照）
  - 個人情報の提供リスク対策（13参照）
  - 個人情報の安全管理リスク対策（14参照）
  - 個人情報の管理リスク対策（15参照）
  - 個人情報のその他のリスク対策（16参照）
  - 個人情報保護条例への適合性（17参照）
- 評価実施手続
  - 本評価は世界各国のPrivacy Impact Assessment （PIA)等を参考にして、弁護士水町雅子が評価項目を決定しています。
  - 姫路市及び姫路市受託事業者ATLから資料提供やヒアリングを受けながら弁護士水町雅子が実施した上で、総務省が設置した有識者会議及びAPPLIC（一般財団法人全国地域情報化推進協会）のご意見を伺っております。
  - なお、本評価における「個人情報」の定義は、姫路市個人情報保護条例に従っています。

19　第三者コメント（総務省有識者会議）

本件は、総務省が平成29年度に実施した「地域におけるビッグデータ利活用の推進に関する実証」事業としても採用されていることから、同事業として総務省が設置した有識者会議のご意見を頂戴しました。

- 頂戴した主なご意見・コメントは次の通りです。

  - 自治体の具体的な政策を知らしめ、住民の目で評価するという個人情報リスク評価PIA^{++}の仕組みは大変有意義であり、他の地方公共団体にとっても参考になるのではないか。
  - どのようなリスクやプライバシーインパクトがあるのかを炙り出し、当該リスク・インパクトと比較する総合判断を行う仕組みである。法律を積極的に解釈してデータを利用する際に個人情報リスク評価PIA^{++}を実施すると有意義だろう。目的外利用の際の相当の理由などの判断も、個人情報リスク評価PIA^{++}を通してできるのではないか。
  - 住民のみならず、議会、個人情報保護審議会、自治体内部の他部署・上席などに説明するための資料としても有意義である。個人情報リスク評価PIA^{++}を実施することがデータ利活用としてより良い取組であり、ぜひ他の地方公共団体にも展開してほしい。特に踏み込んだデータ利活用をする際に個人情報リスク評価PIA^{++}を実施すると良いだろう。
  - 行政透明化、行政ミスの防止、住民福祉の向上になるなど、個人情報リスク評価PIA^{++}の効果は大きい。
  - 行政に広範な裁量がある部分を積極的に住民に公開していくことで、行政裁量が狭まり、より良い行政・透明で開かれた行政の実現につながると考える。

１９　第三者コメント（総務省有識者会議）

本件は、総務省が平成２９年度に実施した「地域におけるビッグデータ利活用の推進に関する実証」事業としても採用されていることから、同事業として総務省が設置した有識者会議のご意見を頂戴しました。

- 頂戴した主なご意見・コメントは次の通りです。

  - 個人情報リスク評価PIA^{++}は第三者がお墨付きを与えるものではなく、リスクがゼロになるものでもない。リスクの度合いと効果の重要性、リスクに対して適切な対策が講じられているか等を測っているものである点を十分に強調した方が良い。個人情報リスク評価PIA^{++}は、「リスクが少しでも残っていたらやめましょう」ではなく「リスクがあっても効果が高い、対策が適切に講じられている」などの点を評価するものであり、リスクがゼロではないとことを説明していくべきである。

  - 「全庁的な安全管理体制」とあるが、もっと具体的に記述すべきである
    （→水町注：ご意見を踏まえ、評価書を修正しました）

  - セキュリティ面の記述に際しては、公開することが逆にセキュリティリスクにならないかを確認する必要がある
    （→水町注：ご意見を踏まえ、確認しました）

20　第三者コメント（APPLIC）

本評価では、より良いプライバシー保護・データ活用の両立のため、地域情報化に精通されているAPPLIC（一般財団法人全国地域情報化推進協会）のご意見を頂戴しました。

- APPLIC（一般財団法人全国地域情報化推進協会）の意見は次の通りです。
  - EBPMは国・地方公共団体において重要な課題である。また、少子高齢社会及び待機児童等の問題から、子育て政策も国・地方公共団体において喫緊の課題となっている。このように本実証では多くの地域が共通的に抱える課題・分野において、課題解決のための一つの手法が示されたと評価している。
  - 特に、取り扱うデータが個人情報であることから、個人情報の保護は絶対的に必要である。地方公共団体が保有するデータを部局・分野横断的に活用する事例であるが、個人情報保護とデータ利活用を両立していると考える。他の地方公共団体への横展開も期待される。
  - 今回の分析基盤では利用者（職員）は直接住民のデータにアクセスすることはできず、アプリケーションとして出力されるのは統計情報だけである。その点でプライバシーインパクトは非常に低い。しかしながら、統計情報を作成するためにシステムとしては住民の個人情報を解析しており、個人情報を取り扱っているということからPIA（プライバシー影響評価、個人情報リスク評価+）を実施している。このように積極的にPIAを実施し、住民に対する影響を十分把握しながらシステム開発を進める姿勢は高く評価できる。特に今回のように法定事務ではない分野での個人情報利用に際しては住民理解を十分に得る観点からもPIAの実施が強く推奨されるべきと考える。

20　第三者コメント（APPLIC）

- 利用される個人情報については基幹システム由来のデータであるが、取得段階で抽象化と称する処理を施しており、不要なプライバシーインパクトを与えない、統計化のために必要な情報とする、いわゆるData Minimizationの配慮がなされている点も評価できる。データの多角的利用による住民サービス向上やEBPMに基づく合理的な行政サービスが求められる中、データの利活用シーンは多彩となる。そこではサービス実施に必要最低限なデータのみ利用するというData Minimizationのポリシーを遵守することが極めて重要となる。
- セキュリティ対策については職員がアクセスできる情報が統計情報であるにも関わらず、利用者認証、端末認証、作業ログの取得など十分な安全対策が取られていると評価できる。
- しかし、制度的に明確な保有期間のある業務データに比べ、分析用に蓄積されるデータについては保管期間についての明確な基準はなく、合理的な判断理由もない。分析の観点からは永続的に保管されることが望ましく、一方で長期的な保管はプライバシーインパクトの増大につながる。分析基盤の継続的な利用に際しては、今後の課題として、長期的なデータ保持に関する評価が望まれる。
- 今回の分析基盤はインターネット系から遮断された環境を前提としている。職員利用を想定したシステムとして妥当なアーキテクチャであり、それによって安全性を高め、プライバシーインパクトを低減させている。しかし、今後の発展性としては、例えばオープンガバメント、集合知の観点で民間との協働の場をネットワーク上に構築するなどを考えると、統計結果をインターネット系からも参照できるようにするといった取り組みも考えられる。今後の発展テーマであるが、インターネット系から完全分離ではない環境の場合の評価の方向性検討もいずれ必要となるのではないか。

２１　水町雅子のコメント

最後に、弁護士水町雅子の意見を次のとおり、述べます。

- 弁護士水町雅子の意見は次の通りです。
  - 個人情報の保護、プライバシー権の保護は当然ながら大変重要であり、公権力として住民等の情報を取り扱っている以上、極めて高い意識・努力が市には要請される。もっとも、個人情報はただ厳重にサーバや書庫にしまっておけばよいというものではなく、地方公共団体として求められる質の高い行政サービス・業務実施・住民サービス向上のために、必要な利活用を、保護と同時に行っていく必要がある。官民データ活用推進基本法も平成２８年に成立しており、保護と利活用の両立は、今後とも各地方公共団体において共通する重要課題となると考える。
  - 本件は、地方情報化として先進的な取り組みを行っている姫路市の事例であり　住民等に求められる行政サービス、説明責任の向上という目的を達成するために、大変良い取り組みであると考える。同時に、これまで姫路市で培ってきた個人情報保護、システム上の保護の措置・経験を十分に取り入れ、保護と利活用の両立を実現していると考える。
  - 時代に即した行政サービスを行い、国民意識・技術トレンド等を十分踏まえた個人情報保護を行うために、今後も継続的に本件のチェック・監査・より良い改善を図っていってほしいと考える。

C)　民間の医療系サービスに対するPIAの例

国立研究開発法人日本医療研究開発機構より受託した、
パーソナル・ヘルス・レコード（PHR）利活用研究事業「RIBS」に関する

個人情報リスク評価PIA++
（Privacy Impact/Risk Assessment)

2018/1　暫定評価版（今後の改定がありうる）

弁護士　水町雅子

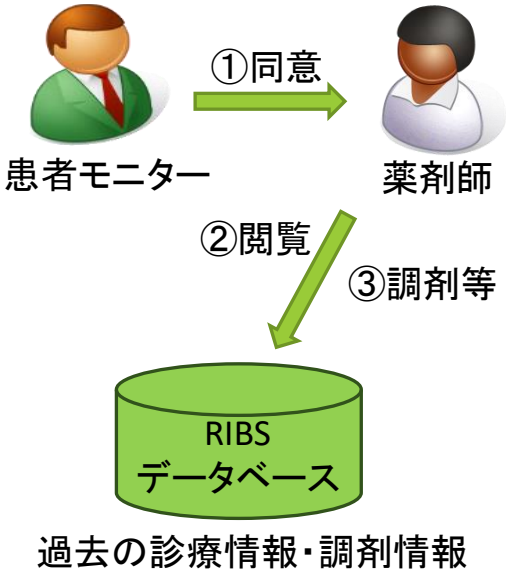
１　本評価の範囲・対象

RIBS

- 本評価は 「RIBS実証事業」 をその範囲・対象としています。
- RIBSとは、医療情報総研が提供する、Receipt Information Browsing Systemの略です。
- 医療情報総研が国立研究開発法人日本医療研究開発機構（AMED）より受託した、パーソナル・ヘルス・レコード（PHR）利活用研究事業「PHRにおける本人による同意や、同意に基づくデータ管理のあり方に関する調査研究」として、RIBSの実証事業が行われました。
- 実証事業の準備・実施期間は、平成２８年１０月１日から平成２９年３月３１日までです。今後、実証事業にとどまらない、本格的な運用を目指しています。
- 本評価は、弁護士水町雅子が、医療情報総研から資料提供やヒアリングを受けながら作成したものです。医療情報総研は本評価書に記載された内容に偽りがないことを表明し保証します。

２　RIBSとは、どのようなサービスか

患者モニターの都度の承認（同意）を前提に、
過去の診療情報・調剤情報を薬剤師が閲覧することで、
より良い診療・調剤を行うことを目指した仕組みです。



① 『**診療情報提供カード**』を**患者が薬剤師に提示**

② **薬剤師が**『診療情報提供カード』にて、**診療情報・調剤情報を閲覧**
- → 薬剤師が閲覧する情報は、その薬局・病院に限らず、患者モニターが過去2年間に受診等した診療情報・調剤情報全般になります。
- → 『診療情報提供カード』自体には**アクセスキーのみが記録**されており、診療情報は記録されていません。薬剤師は、このアクセスキーにより データベースにアクセスし、患者モニターの過去2年分の診療情報を閲覧します。

③ **より適切な調剤、服薬指導**を目指します
- → 過去の診療情報を把握することで、より適切な調剤・服薬指導を図ります。

2　RIBSとは、どのようなサービスか

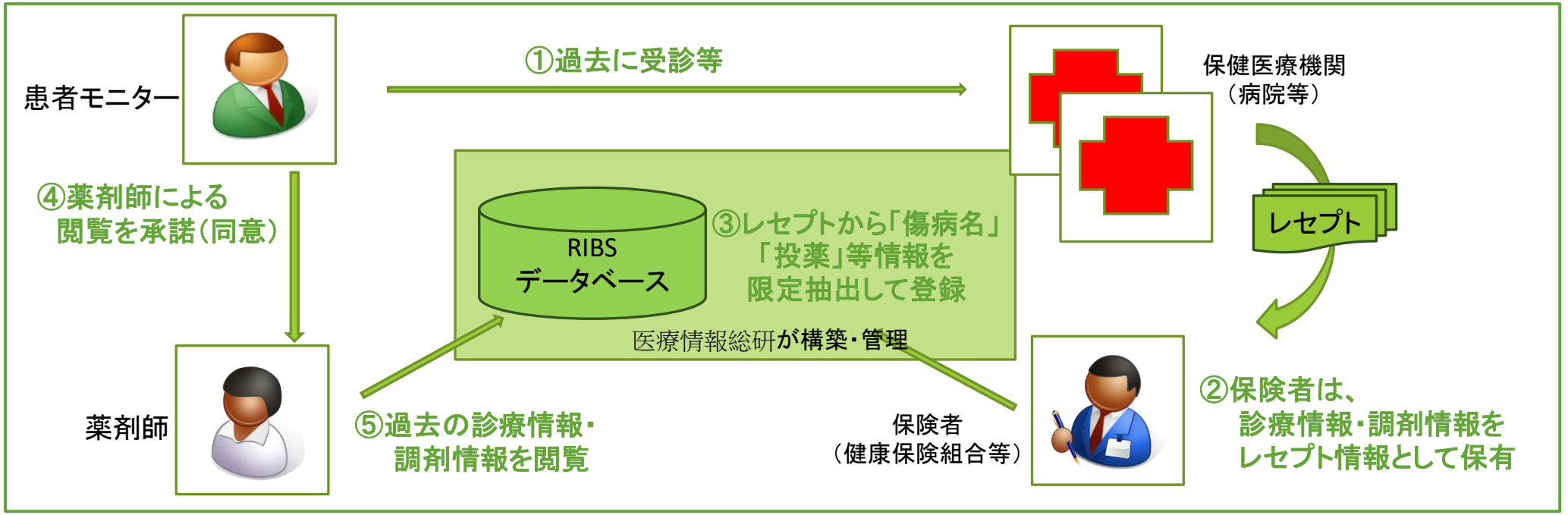
同意

- 患者モニターが『診療情報提供カード』を提示することが、過去の診療情報・調剤情報を薬剤師が閲覧することへの**同意**になります。
- 診療情報を薬剤師に閲覧させるかどうかは、**その都度決めることができます**。
  今回は閲覧させるが、次回は閲覧させないといった選択も可能です。
- 患者モニターになることを同意した場合でも、診療情報提供カードを提示しない
  （＝「診療情報を開示しない」という意思表示をする）ことができます。

診療情報・調剤情報

- 薬剤師が閲覧できる情報は次の項目のみです。
  - 過去に行われた「傷病名」「投薬」「注射」「処置」「手術」「検査」「画像診断」等
  - 詳細は8ページをご参照ください。

3　RIBSの全体像



① 病気やけがで保険医療機関（病院、薬局等）にかかると、個人は、窓口で保険証（被保険者証）を見せて、治療に掛かった費用の一部を支払います。保険医療機関は、残りの医療費について、保険証を交付している保険者（健康保険組合等）に1ヶ月分の診療行為をまとめた**レセプト**で請求します
② **保険者**のもとには、**診療情報・調剤情報**がレセプト情報として保有されています。
③ レセプト情報から「傷病名」「投薬」「注射」「処置」「手術」「検査」「画像診断」等情報を**限定抽出**し、医療情報総研がRIBSデータベースに登録します。
④ 患者モニターから都度、**同意**を得た場合に限り、
⑤ 薬剤師が**過去の診療情報・調剤情報を閲覧**して、より適切な調剤、服薬指導を目指します。

4　期待される効果

患者・被保険者の安全確保

- 医療事故／副作用の発生防止：病名の閲覧が可能になることにより、特定の既往歴がある患者に対する禁忌薬の投薬防止が可能に。相互作用のある薬剤が処方・調剤されることを防止。

より質の高い医療

- 初回訪問患者に関する豊富な医療情報に接し、患者の既往歴の他、受診行動の特性を知ることで、服薬指導や対話の充実が期待。
- 現状では、初診患者の治療方針策定については、患者への問診・検査に頼っているが、RIBSにより診療情報・調剤情報を閲覧できる者を薬剤師だけではなく医師に拡大すれば、傷病名や手術歴等の事実情報を簡便・正確・網羅的に入手できるようになるため、医師による治療方針策定プロセスが合理化され、より質の高い医療が期待
- 緊急時、イレギュラー発生時等、患者への問診が困難な場合にも、より適切な治療が可能に

4　期待される効果

患者利便の向上

- おくすり手帳を忘れても、過去に処方・調剤された薬剤名が明らかに
- 問診票記入にかかる手間が削減。 過去の既往歴を問診で聞かれても、どこまでの範囲の病気を答えればよいのか、何が今の症状に関係する病気なのかわからず、回答に支障が生じる場合も。RIBSにより傷病名や手術歴等が簡便・正確・網羅的にわかれば、患者の問診負担の軽減も期待。

医療費の適正化

- 重複投与の防止により残薬の発生を抑制
- 過去の投薬履歴を閲覧することで、患者に対してジェネリック医薬品に関する適切な説明／推奨が可能に
- 重複検査の抑制も期待

５　RIBSで個人情報をどう取り扱うか

■　誰の個人情報：本実証事業に参加することを事前に同意いただいた患者モニター

- レセプトには医師等の個人情報も記載されていますが、本実証事業では、患者モニター以外の個人情報を削除したデータのみ取り扱います。
- RIBSにアクセスする薬剤師の個人情報も取り扱います。
- 実証事業のため、個人情報の本人数は300人未満です。

■　どんな個人情報：

- RIBSデータベース中の患者モニターの個人情報項目は、診療開始日、傷病名、注射、処置、手術、検査、画像診断、投薬情報（医薬品コード、医薬品名称、1日量、単位、投与日数）、医科/DPC/調剤、入院/入院外等の区別、RIBS-IDです。患者モニターが保有する診療情報提供カードには、氏名、記号番号、RIBS-ID、保険者情報が記載されています。以下「本件個人情報」といいます。
- RIBSにアクセスする薬剤師の個人情報としては、氏名 、調剤薬局名、アクセスログ等を取り扱います。

５　RIBSで個人情報をどう取り扱うか

■ 情報の取得
- 保険者（健康保険組合等）が保有しているレセプト情報のうち、本実証事業への参加を同意いただいた方の個人情報のみを抽出し、さらにそこから本件個人情報を抽出します。
- RIBSデータベースに登録します

■ 情報の利用
- RIBSデータベースにアクセスするのは薬剤師で、同データベースを構築・管理するのは医療情報総研です。

５　RIBSで個人情報をどう取り扱うか

■　情報の利用

- RIBSでは、①認証済みの情報端末、②薬剤師の認証カード+パスワード、③患者の診療情報提供カードの3つが揃ってはじめて情報の閲覧が可能になります。
- ①本実証事業に参加する薬局の中でも、事前に認証済の情報端末でしかRIBSにアクセスできません。②本実証事業に参加する薬局の中でも、事前に登録された認証カードを持つ薬剤師しかRIBSにアクセスできません。③本実証事業に参加する薬局でも、あらゆる方の個人情報を閲覧できるわけではなく、診療情報提供カードを患者が提示した場合に限り、その診療情報提供カードを元に、その患者の個人情報しか閲覧することはできません。
- 個人情報を閲覧することしかできず、印刷したり、情報端末にダウンロードしたり保管することは、システムの仕様上できません。

５　RIBSで個人情報をどう取り扱うか

■ 情報の管理
- RIBSデータベースでは、個人毎に付与されるIDで情報を管理しており、個人名・生年月日等のデータは登録されていません。さらに、データベースと端末との通信は暗号化されています。

■ 情報の廃棄
- 本実証事業期間終了後に、一切の情報を復元不可能な方法で削除します

６　個人情報が漏えいしないか

RIBSでは、患者モニターの過去の「傷病名」「投薬」「注射」「処置」「手術」「検査」「画像診断」という重要な個人情報を取り扱うため、個人情報の漏えいを防止するために次の措置を講じています。

技術面

- FW（ファイアウォール）で不正アクセス、ポートスキャン等を防ぎます。
- WAF（Web Application Firewall）でSQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクションに代表される脆弱性からWebアプリケーションを守ります。
- IPS / IDS（Intrusion Prevention System / Intrusion Detection System）でWebサーバの脆弱性を狙う攻撃、OSの脆弱性を狙う攻撃、Dos攻撃、SYNフラッド攻撃等の不正アクセスを防ぎ、ウィルス検知を行います。
- 事前に許可されたクライアント（クライアント証明書）だけがRIBSにアクセスできます。
- 事前に許可された薬剤師だけがRIBSにアクセスできるよう、認証カードとパスワードによる2要素認証を行います。
- レセプト情報からRIBSデータベースに登録するデータを限定抽出する際は、インターネットと完全に切り離された環境で行います。
- データは、暗号化された状態で通信経路上を伝送されます。

運用面

- カード紛失時は、該当するRIBS-IDに紐づくデータをデータベースから削除した後、RIBS-ID・カードの新規発行を行います。
- RIBSデータベースにデータを登録する際は、記録媒体経由で取り込みます。記録媒体は、鍵のかかる保管庫にて保管し、データベースへの取り込み後は、速やかに保険者に返却しました。

法制度面

- 薬剤師は法律上守秘義務を負い、違反した場合は6月以下の懲役又は10万円以下の罰金に科せられます（刑法134条1項）。医道審議会による行政処分の可能性もあります。

7　同意取得が適切に行われるか

本実証事業では、個人情報の提供に先立ち、事前に患者から同意を得る仕組みとなっています。

患者モニターが言われるがまま診療情報提供カードを提示して、RIBSの仕組みを理解できないままに自身の病歴等を閲覧されてしまうことがあってはなりません。真の同意を適切に得られるよう、RIBSでは次の措置を講じています。

- 診療情報提供カードを配布するのは、本実証事業への参加に同意した方に限ります。なお、これらの方には、本実証事業の仕組みについて、事前に書面でご説明しています。
- このカードを提示することで自身の病歴等を薬剤師が閲覧することがわかるよう、カードの裏面にその旨を記載し、カードの券面に「診療情報提供カード」と大きく表示しています。
- カードを提示しないことによる不利益はありません。カードを提示しなくても、これまで通り調剤等を受けることができます。
- カードを提示するかどうかは、受診の都度、自由に決定できます。本実証事業への参加に同意した方であっても、受診ごとに、診療情報提供カードを提示してもしなくても構わず、自由に決定できます。
- 薬剤師は「診療情報提供カード」の提示を受けた場合でも、すぐにRIBSにアクセスせず、患者に「過去の病歴等を閲覧します」と伝えてからRIBSにアクセスします。

８　別人の病歴等と間違われないか
他人に自分の病歴等を見られないか

RIBSは、過去の病歴等を把握することでより適切な調剤・服薬指導を目指す仕組みですが、仮に閲覧する情報が間違ってしまうと、不適切な調剤・服薬指導がなされるおそれがあります。また、他人に自分の病歴等を見られてしまうようなことがあってはなりません。そこでRIBSでは患者ご本人の病歴等が正しく閲覧されるよう、次の措置を講じています。

データ登録時の正確性確保

- 保険者が保有するレセプトデータから情報を抽出してRIBSデータベースに登録することで、不正確な個人情報を入手することを防止します。
- レセプトデータをRIBSデータベースに登録する際、複数の保険医療機関のレセプトが同一人を指しているか、同姓同名等の誤認を防止するために、医療保険の資格情報（加入者番号、資格取得年月日、資格喪失年月日、氏名等）を元に正確に名寄せします。

アクセス時の正確性確保

- 診療情報提供カードを利用できるのは、原則として本人のみです。例外としては患者モニターの家族がいますが、後述します。
- 診療情報提供カードの表面に、氏名と保険証の記号番号を記載します。
- 薬剤師は、患者から診療情報提供カードの提示を受けた時は、同カードの氏名と処方箋の氏名の一致を確認します。不一致の場合は、RIBSにアクセスしません。
- 診療情報提供カードの表面に、RIBS-IDとQRコードを記載し、ご本人の情報に正しくアクセスできるよう確保します。

他人に見られないか

- 患者モニターの家族に限って、本人以外でも診療情報提供カードを利用できます。家族が患者モニター名の診療情報提供カードと処方箋を持参した場合は、現に看護に当たっている家族の場合に限り、薬剤師がRIBSにアクセスできます。また、本人・家族に対して、病名や処置内容を知らせることはしないよう、参加薬局と契約しています（本人であっても病名等が伏せられている可能性などもあるため、平成 17年3月31日保発第0331007号「診療報酬明細書等の被保険者への開示について」に沿って、本人に対しても、保険医療機関等の同意なく病名や処置内容は知らせないようにしています）。
- 診療情報提供カードを紛失した場合には、診療情報提供カードを盗んだ者、拾った者等が家族になりすますと、診療情報を推測される可能性があります。この点を周知するため、患者モニターへの文書でその旨を特記しています。

９　目的外利用・過剰紐づけされないか

本人の過去の病歴等をその他の情報と突合したりして、本人のさまざまな情報を入手してしまうと、本実証事業の目的を越えて個人情報が収集・利用等されてしまいます。RIBSでは本実証事業の目的以外に本件個人情報が取り扱われないように、次の措置を講じています。

- 本件で個人情報を取り扱うのは、保険者、薬局、医療情報総研の３者です。それぞれが個人情報保護法に服し、個人情報の目的外利用は、個人情報保護法に基づき原則禁止とされています（同法16条）。例外は、法律の定める場合のみです。保険者、薬局、医療情報総研の３者は、契約上も秘密保持義務を負うとともに、情報管理責任者を設置しています。
- 実証事業の目的外に本件個人情報を利用しません。
- 保険者は公法人として自らの保有するレセプト情報等を、個人情報保護法及び厚生労働省等の公表するガイドラインを遵守して取り扱います。
- 医療情報総研は民間事業者ですが、医療情報総研においてもレセプトデータやRIBSデータベースを取り扱うことから、契約で、医療情報総研の秘密保持義務、秘密情報管理基準、秘密情報の取扱いについては事前許諾のない再委託の禁止、立入調査、報告義務等を原則として定めています。医療情報総研は公法人たる保険者から委託を受けた者として、本件個人情報を個人情報保護法及び厚生労働省等の公表するガイドラインを遵守して取り扱います。実証事業の目的外に本件個人情報を利用しません。
- 薬剤師は、刑法上守秘義務を負う法主体として、本件個人情報を個人情報保護法及び厚生労働省等の公表するガイドラインを遵守して取り扱います。実証事業の目的外に本件個人情報を利用しません。また、薬剤師はRIBSデータベースによって情報を閲覧できるだけにとどまり、ダウンロードしたり印刷することが、システム仕様上できません。
- RIBSデータベースは他のシステムと自動連携等することはありません。
- 無権限の外部者については、漏えい対策を行い（→6参照）、そもそも無権限の外部者が本件個人情報を入手することができないよう、対策を行っています。

10　その他のリスク対策
（個人情報の取得に関して）

RIBSでは上記のほか、個人情報の取得に際して次の措置を講じています。

個人情報を過剰取得しないか

■ レセプトデータをそのままRIBSデータベースに登録するのではなく、患者に対し過去に行われた「傷病名」「投薬」「注射」「処置」「手術」「検査」「画像診断」の情報を抽出登録することで、不要な個人情報を入手することを防止します。

不正確な個人情報を取得しないか

■ 保険者が保有するレセプトデータから情報を抽出してRIBSデータベースに登録することで、不正確な個人情報を入手することを防止します。レセプトデータをRIBSデータベースに登録する際、複数の保険医療機関のレセプトが同一人を指しているか、同姓同名等の誤認を防止するために、医療保険の資格情報（加入者番号、資格取得年月日、資格喪失年月日、氏名等）を元に正確に名寄せします。

取得の際に個人情報が漏えい・紛失等しないか

■ RIBSデータベースの元情報となるレセプトデータは、最新のウイルスパターンファイルにてウイルスチェックを行い問題がないことを確認後、暗号化を施したうえで、光ディスク（DVD-R）に記録します。そのうえで、搬送用のジュラルミンケースに収納、施錠し、保険者（健康保険組合等）から医療情報総研に手渡しされます。手渡しが完了した際、医療情報総研は保険者に対し受領書を渡します。レセプトデータを復号化する為のパスワードは、別ルートで提供されます。医療情報総研は復号したレセプトデータから情報を抽出の上、専用線にてRIBSデータベースに登録します。

取得の際に不正が起きないか

■ 医療情報総研が保険者よりレセプトデータを入手してRIBSデータベースに登録することになります。その際の不正等を防止するため、保険者と医療情報総研間の契約で、秘密保持義務、秘密情報管理基準、秘密情報の取扱いについては事前許諾のない再委託の禁止、立入調査、報告義務等を原則として定めています。

11　その他のリスク対策
（個人情報の利用に関して）

RIBSでは上記のほか、個人情報の利用に際して次の措置を講じています。

個人情報を無関係の者に利用されないか

- ①認証済みの情報端末、②薬剤師の認証カード+パスワード、③患者の診療情報提供カードの3つが揃ってはじめて情報の閲覧が可能になります。薬剤師であっても①情報端末の持ち出しは禁止し、②認証カードは実証終了時にすべて返却します。実証段階ではなく本稼働後は、退職時に返却させる予定です。

本件関係者が個人情報を私的利用・私的複製・悪用等しないか

- 薬局では個人情報を閲覧することしかできず、印刷したり、情報端末にダウンロードしたり保管することは、システムの仕様上できません。さらに薬剤師には刑法上の守秘義務も課せられています。
- 医療情報総研が保険者よりレセプトデータを取得し、RIBSデータベースの情報を管理することになります。その際の不正等を防止するため、保険者と医療情報総研間の契約で、秘密保持義務、秘密情報管理基準、秘密情報の取扱いについては事前許諾のない再委託の禁止、立入調査、報告義務等を原則として定めています。医療情報総研では個人情報保護に関する責任者を設置したうえで、個人情報にアクセスする必要最小限度の担当者を定め、保険者に通知します。医療情報総研では操作記録を保存します。
- 保険者は公法人として自らの保有するレセプト情報等を、個人情報保護法及び厚生労働省等の公表するガイドラインを遵守して取り扱います。

12　その他のリスク対策
（個人情報の提供に関して）

RIBSでは上記のほか、個人情報の提供に際して次の措置を講じています。

個人情報が不正提供されないか

- 保険者、薬局、医療情報総研以外への個人情報の提供は原則として認められていません。
- 操作記録を保存しています。
- なお、レセプトデータには患者自身も知らない情報が含まれていることから、「本人の生命、身体、財産その他の権利利益を害するおそれ」がないかどうか、主治医の判断を確認してから開示がなされることとされています（厚生労働省保発第0331007号「診療報酬明細書等の被保険者への開示について」）。RIBSデータベースはレセプトデータを抽出した情報を登録していることから、RIBSデータベース情報を患者モニターへ開示することもこれと同様に考えられます。そこで本実証事業では、RIBSデータベースを閲覧するのはあくまで薬剤師であって、薬剤師が患者モニターに対しデータを見せたり、内容を明らかにすることはしないようにしています。

13　その他のリスク対策
（個人情報の安全管理措置に関して）

RIBSでは上記のほか、個人情報の安全管理措置に関して次の措置を講じています。

安全管理体制／規程
■ 保険者、薬局、医療情報総研の3者は、契約上も秘密保持義務を負うとともに、情報管理責任者を設置しています。 ■ 医療情報総研は安全管理規程を整備し従業者に対し周知しています。保険者、薬局は「健康保険組合等 における 個人情報の適切な取扱いのためのガイダンス」「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に従い、安全管理規程等について検討しています。
物理的対策
■ 有人による監視や入退館（室）装置による管理をしている建物の中で、更に生体認証による入退室管理を行っている部屋に設置したサーバ内に原則として保管します。また、サーバ室の入退室については、システム管理者が許可した者に限定しており、サーバへのアクセスはIDとパスワード等による認証が必要となります。
技術的対策
■ 6参照

14　その他のリスク対策
（個人情報の管理に関して）

RIBSでは上記のほか、個人情報の管理に際して次の措置を講じています。

委託先の不正が起こらないか
■　RIBSは委託先（保険者、医療情報総研、薬局以外の者）には原則として取り扱わせません。
個人情報が誤って消去等されないか
■　定期的にバックアップを取得しています。
不要な個人情報がいつまでも保管されないか
■　医療情報総研では復元不可能な方法で個人情報を消去します。
古い個人情報を誤って利用しないか
■　本実証事業の間、入手可能なレセプトデータをRIBSデータベースに登録していきます。

15　その他のリスク対策
（全般に関して）

RIBSでは上記のほか、次の措置を講じています。

点検・監査等
■　医療情報総研ではPマークを取得し、さらに本評価を実施しています。
従業者教育
■　保険者、医療情報総研、薬局では、従業者への教育・啓発を行います。
開示・訂正・利用停止請求
■　保険者にて個人情報保護法に従って対応がなされます。
問合せ対応
■　医療情報総研にて対応します。問合せ先は、患者モニターが保有する診療情報提供カードに記載されています。

16　まとめ

- 本評価において、以下の項目について検討し、プライバシーへの影響を確認しました。
  - スキーム（1から3参照）
  - 個人情報利活用の効果（4参照）
  - 個人情報の取扱い（5参照）
  - 個人情報の漏えいリスク対策（6・13参照）
  - 同意取得におけるリスク対策（7参照）
  - なりすまし・取り違えリスク対策（8参照）
  - プロファイリングリスク対策（9参照）
  - 個人情報の取得リスク対策（10参照）
  - 個人情報の利用リスク対策（11参照）
  - 個人情報の提供リスク対策（12参照）
  - 個人情報の安全管理リスク対策（13参照）
  - 個人情報の管理リスク対策（14参照）
  - 個人情報のその他のリスク対策（15参照）

- 評価実施手続
  - 実証事業の準備・実施期間は、平成28年10月1日から平成29年3月31日までです。
  - 本評価は、弁護士水町雅子が、医療情報総研（MHI）から資料提供やヒアリングを受けながら、平成29年に作成したものです。
  - 本評価では、日本版Privacy Impact Assessment（PIA)である「特定個人情報保護評価」の全項目評価書と同レベルの厚い評価を行っています。対照関係及び補足事項は別紙の通りです。
  - また本評価は、「特定個人情報保護評価」のみならず、諸外国のPrivacy Impact Assessment（PIA)を参考にして、評価項目を決定しています。

17　有識者（第三者）のコメント

本評価では、より良いプライバシー保護の実現のため、弁護士宮内宏氏のご意見を頂戴しました。

- 弁護士宮内宏氏の意見は次の通りです。
  - 暗号化等のセキュリティ対策については、今後も定期的に見直し、安全性を維持してほしい。
  - 本件におけるプライバシー保護のためには、薬剤師のプロ意識が重要であろう。薬剤師への信頼が担保されて、成り立つ仕組みであると考える。薬剤師のより一層のプロ意識を醸成するようにしてほしい。

１８　水町雅子のコメント

最後に、弁護士水町雅子の意見を次のとおり、述べます。

- 弁護士水町雅子の意見は次の通りです。
  - RIBSは、公法人たる保険者が保有する個人情報を、刑法上の守秘義務を負う薬剤師が閲覧する仕組みである。保険者、薬剤師ともに法的責任は重く、法制度面では十分プライバシー保護が担保されていると考えられる。RIBSを構築・運用する医療情報総研は民間事業者であるが、公法人たる保険者の個人情報をこれまでも取り扱ってきており、実績がある。医療情報総研における一層の従業者教育・従業者監督が重要である。
  - RIBSは、医療の質のより一層の向上、患者の利便性の向上、そして療養担当者による療養に資する仕組みであり、個人情報を利活用することの効果は公益・個益ともに大きいと考えられる。実証事業で得られた成果を踏まえ、RIBSがより一層の効果を発揮するよう、改良改善を行っていき、本稼働後も、より効果を発揮するためにはどのような改良改善が考えられるかという視点を常に持ち続けることが重要であると考える。
  - RIBSにおけるセキュリティ対策をより一層強化し、タブレット・サーバ・伝送路等すべての対象に対して、最新の脅威にも耐えられる対策を常に講じていくことが極めて重要である。
  - 診療情報提供カードを紛失した際の対応や、家族が持参した際の対応を、より確固たる迅速なものにしていくよう、努めていくべきである。

4.　どのように実施すればよいのか

プライバシー影響評価を実施するには

- **諸外国で行われている**Privacy Impact Assessment （PIA）や Data Protection Impact Assessment（DPIA）**を参考にする**
- ISO/JIS**を参考にする**
- **日本で行われている特定個人情報保護評価を参考にする**
- **日本で行われている**PIA**を参考にする**
- **お勧めは、** ISO/JIS**を参考にしながら、特定個人情報保護評価をカスタマイズする**
  - なぜならば、特定個人情報保護評価はわかりにくいという欠点はあるものの、諸外国で行われているものを参考に日本法上規定された仕組みだから
  - ISO/JISを参考にする必要あり。
    しかしこれだけ見れば誰でも簡単に評価できるというものではない。

特定個人情報保護評価をカスタマイズしよう

考え方

- 特定個人情報保護評価が義務付けられるのは、マイナンバーに関する特定個人情報ファイルを保有する官（行政機関、地方公共団体等）がメイン
- それ以外は、あくまで任意実施であり、特定個人情報保護評価を参考にするのみ
- 特定個人情報保護評価をベースに適宜カスタマイズできる
- 特定個人情報保護評価の枠組みを使い、ユーザ・消費者にわかりやすいものを実施していくのがお勧め

特定個人情報保護評価の問題点とその解決策

- 特定個人情報保護評価書は難解
  - ✓ そのまま用いなくてもよい。趣旨を用いてベースに使う。
- 字が多い
  - ✓ パワーポイントなどに変更し、図を多用しよう。
- 何が書いてあるかわかりづらい
  - ✓ 「この欄に書くべきこと」をより明確化する
  - ✓ どんなリスクがあってどんな対策をするのかをよりわかりやすく記載する
  - ✓ ユーザ・消費者目線に立って記載する

特定個人情報保護評価の仕組み

◆ **中心は、評価書**

- 「プライバシーポリシー」「わが社の取組」「わが社のCSRの取組」をイメージ

◆ **評価書をブラッシュアップしていく仕組み**

- 一般意見、専門家意見によって得られた意見をもとにブラッシュアップ
- 一般意見を聴く、専門家意見を聴くは必ずしも実施しなくてよい
- もっとも、海外では一般意見を聴くことは重要視されている（消費者団体との意見交換など）。事前に意見を聴かなくても、評価書を公表することで、ユーザ等からの反応が考えられる。その反応・意見によって、評価書をブラッシュアップ。
- 再評価・評価書の修正によって、継続的にブラッシュアップ

5.　評価のポイント

評価書に何を書くか、何を評価するか

１　サービスの全体像をわかりやすく平易に説明しよう

- ユーザ・消費者に向けての説明をイメージ
- どのようなサービスなのか、何を行うのか

２　個人情報がどう関係してくるかを説明しよう

- そのサービスで個人情報がなぜ必要なのか
- 個人情報を誰がどのように利用するのか
- 個人情報を外部提供するのか、誰に提供するのか
- 個人情報をいつまで保管するのか、いつどう廃棄するのか
- ユーザ個人にメリットはあるのか

３　個人情報の不正に対する不安を払拭するべく、対策をわかりやすく説明しよう

- 悪用しないのか、ＤＭや勧誘電話は来ないのか、外部売却しないのか、漏えいしないのか、無関係な他人に教えないのか、従業員教育はどうなっているのか　などなど

１．サービスの全体像をわかりやすく平易に説明しよう

- サービス・業務の全体像をわかりやすく平易に説明しよう
  - ✓ 市民・消費者に向けての説明をイメージ
  - ✓ 市民・消費者は、企業内部の者とは違い、どのようなサービスなのか、業務なのかが全く分からない場合も多い。企業内部にとっては当然のことであっても、外部から見たらわからない。
  - ✓ たとえるなら、この業務に新しく加わった従業員（新人・異動者）に説明するように、全体像をわかりやすく説明する。
- さらに、サービス・業務の全体像の中での個人情報の流れを追記しよう
- できれば図にするとよい。難しいようであれば平易な文章で。

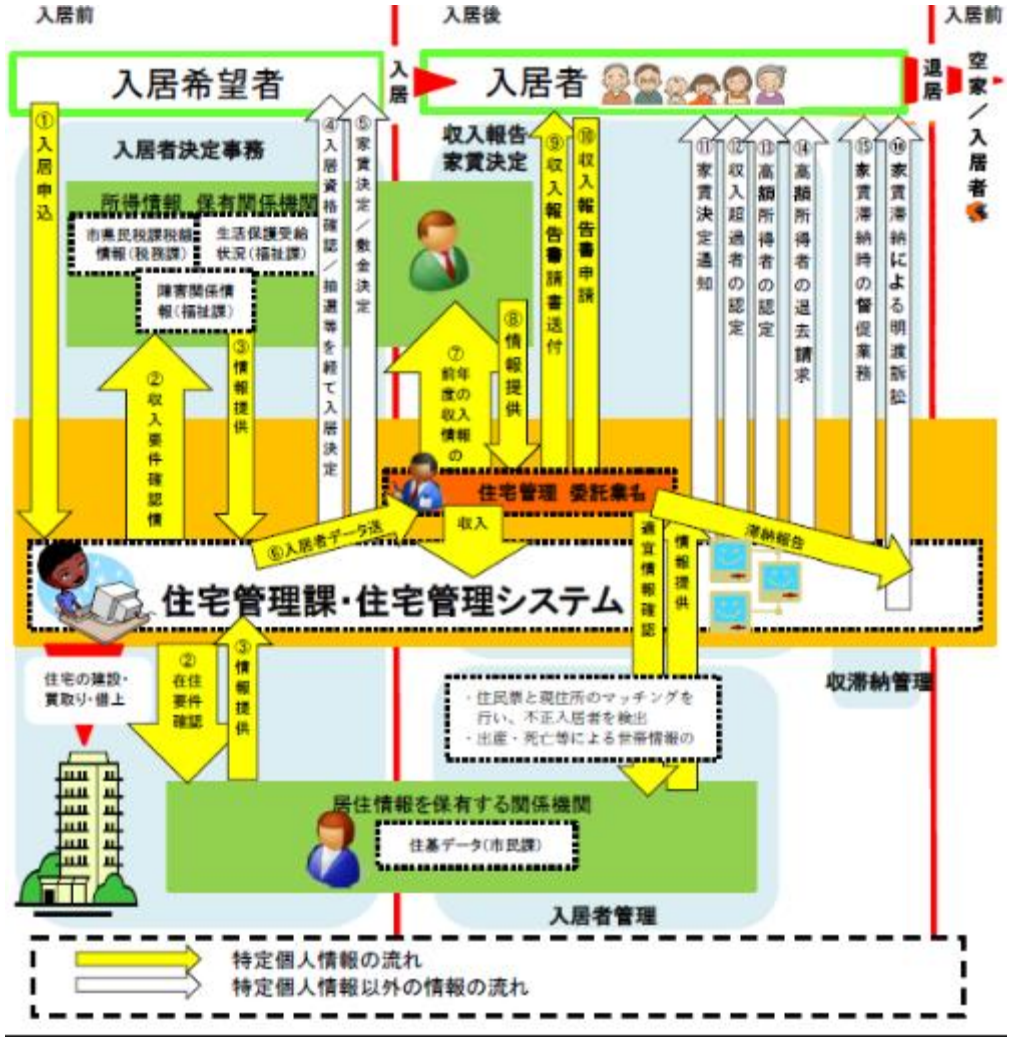
（参考）特定個人情報保護評価書だと・・・重点項目評価書Ⅰ１②・全項目評価書Ⅰ１②別添１に

１．サービスの全体像をわかりやすく平易に説明しよう（例）

- 文章の例（イメージ）
  - 目的：乳幼児医療費助成：経済的負担を心配しなくてもお子さんが病気などを治療できるよう、〇才未満のお子さん*1の医療費等*2のうち保護者等が負担しなければならない分を、市で助成します。
  - 概要：当市では、出生届を受け取ったら、保護者等に申請を促します。保護者等の申請を受け付けたら、助成対象外*1に当たらないか当市で確認し、医療証を発行します。保護者等は病院の窓口等で医療証・健康保険証を提示の上、診療等を受けます。そうすると保険外等の、対象外となる医療費等*2を除き、保護者等は自己負担がなくなります。当市では、病院等から請求を受け、病院等へ対象額を支払います*3。
  - *1～3：例外や、審査・支払機関等の点は、注記するとわかりやすくなる可能性。注記とせず、本文に書いてもよいが、正確に記載しようとして例外の解説が多すぎると、わかりにくくなるので、留意する。

1．どういう業務か説明しよう（例）

- 絵の例（イメージ）



２．個人情報がどう関係してくるかを説明しよう

- サービスや業務の中で個人情報がどうかかわるのか、平易に説明しよう
  - ユーザ・消費者からすれば、誰の個人情報が何のために誰にどのように使われるかわからない。
  - 企業内部にとっては当然のことであっても、外部から見たらわからない。
- サービスや業務の中で個人情報がどう取り扱うのか、平易に説明しよう
  - 不透明だと不安が生じる。具体的に説明することで、納得が得られやすい。
  - 個人情報を誰が何のためにどのように利用するのか
  - 個人情報を外部提供するのか、誰に何のために提供するのか
  - 個人情報をいつまで保管するのか、いつどう廃棄するのか
- ユーザ個人にメリットはあるのか
  - 自分の個人情報を企業の利益のためだけに利用されているという思いも
  - ユーザ個人にどのようなメリットがあるのか、個人情報の利用だけではなく、サービス全体のメリットも含め、説明できるとよい

（参考）特定個人情報保護評価書だと・・・重点項目評価書Ⅱ２③④３⑤・全項目評価書Ⅱ２③④３⑧に記載

２．個人情報がどう関係してくるかを説明しよう（例）

- 例（イメージ）
  - 誰の個人情報：当市在住の〇才未満のお子さん、保護者、過去の対象者*1
    - *1　〇才以上になったお子さんと保護者の個人情報についても、過去△年分の情報を保存しています。
  - どんな個人情報：
    - ＩＤ、氏名・住所・性別・生年月日、連絡先、その他住民票関係情報、医療保険関係情報、児童福祉・子育て関係情報・生活保護・社会福祉関係情報、障害者福祉関係情報
  - どう使用するのか：
    - 医療証関係
      - 出生届を受け取ったら、保護者等の住所宛に乳幼児医療費助成について申請を促す連絡をする
      - 申請を受け付けたら、助成対象外*1に当たらないか〇、△、□情報を元に当市で確認し、医療証を発行する
      - 〇〇の時に、医療証を再発行する
      - 〇〇の時に、医療証を更新する
      - 転出届を受け取ったら、・・・

2．個人情報がどう関係してくるかを説明しよう（ポイント）

- 企業の外のユーザがわかるように
- 具体的に説明する
  - 取得：　どこからいつどのような個人情報を取得するのか
  - 利用：　いつ誰が何のためにどのように利用するのか
  - 委託：　委託先に取り扱わさせるのか
  - 提供：　いつ誰に何のために提供するのか
  - 保管：　どのようにいつまで保管するのか
  - 消去：　いつどのように消去するのか
- 個人情報を取り扱う必要性、合理性を納得してもらえるように説明する
- 不合理なこと、あやしいことはやっていないということの説明にもなる
- ユーザの不信感が解消されるように

３．個人情報の不正対策をわかりやすく説明しよう

１．想定されるリスクを挙げよう

- ユーザの不安を中心に考えるとよい
  自分が一ユーザの立場だったら何を不安に思うか。自分の家族だったら何を不安に思うかなど。
- 個人情報が悪用されないか、ＤＭや勧誘電話が来ないか、外部売却されないのか、漏えいされないのか、無関係な他人に教えないか、従業員教育はきちんとなされているか　などなど
- 個人情報の不正リスク、プライバシーリスクを網羅的に考えるとさらに良い　（追って説明）

２．今行われているリスク対策を確認しよう

- 今行われているリスク対策はどのようなものか
- 外部の人が見て、リスクが防止できると納得してもらえるレベルの対策になっているか考えよう

３．リスク対策を改善しよう

- より納得してもらえるリスク対策に、不正を防止できるリスク対策へとレベルアップしていこう

４．リスク対策を説明し、ユーザの納得を得よう

３．個人情報の不正対策をわかりやすく説明しよう

実はそこまで技術的、難しいものではなく、常識に沿って考えるべきもの

■ 想定されるリスク

- ✓ 例）個人情報が悪用されないか、ＤＭや勧誘電話が来ないか、外部売却されないのか、漏えいされないのか、無関係な他人に教えないか、従業員教育はきちんとなされているか　などなど
- ✓ ユーザは何が不安なのか、自分だったら何を不安に思うか
- ✓ 代表的な不安、社会的マイノリティの不安
- ✓ 漠然とした不安をブレイクダウンして考える

■ リスク対策

- ✓ 例）ダブルチェック、アクセス制御、施錠、外部提供制限　などなど
- ✓ 対策自体をプライバシー影響評価で新しく編み出すわけではない
- ✓ 対策は目新しくなくてもよい、きわめて高度な対策が要求されるわけではない
- ✓ リスクを防止・軽減できると合理的に説明できるか、ユーザの不安が解消されるか

3．個人情報の不正対策をわかりやすく説明しよう

■ 入手の際に想定されるリスクの例

- 過剰入手（目的外）
  - どんなリスクか：　不要な個人情報まで取得してしまう
  - 対策：　取得事項を必要な個人情報に限定するなど
（個人情報を取得する画面・システムの制御、ダブルチェック、様式作成）
- だまし討ち入手（不適切な方法）
  - どんなリスクか：　個人情報が取得されているとユーザから見てわからないようなだまし討ちのような方法で取得してしまう、不適切な方法で取得してしまう
  - 対策：　個人情報を取得する際にその旨を明示、利用目的・利用方法なども合わせて明示するなど
- 安全でない入手方法（漏えい・紛失）
  - どんなリスクか：　入手時に漏えい、紛失等してしまう
  - 対策：　専用線、暗号化、パスワード、封緘、簡易書留
- 取違え（不正確）
  - どんなリスクか：　別人、別情報と取り違えてしまう、内容が間違っている
  - 対策：　本人確認、正確性確保

3．個人情報の不正対策をわかりやすく説明しよう

■ 利用の際に想定されるリスクの例

- 過剰集約（目的を超えた紐づけ）
  - どんなリスクか：　サービスや業務に必要のない個人情報をどんどん集約されてしまう
    （プロファイリング、個人像が勝手に作り上げられる）
  - 対策：　個人情報の紐づけ・集約を限定するなど
    （個人情報の管理をサービスごとに分ける、複数サービスで集約する範囲を限定する）
- 無関係な者による利用（権限のない者による使用）
  - どんなリスクか：　担当者以外の者（元担当者、元従業員、たまたま訪問した人、サイバー攻撃者など）が勝手に利用
  - 対策：　アクセス権限の管理徹底、セキュリティ対策の充実など
- 興味本位の利用（事務外使用）
  - どんなリスクか：　業務担当者が業務のためにではなく興味本位など個人的な理由で勝手に利用
  - 対策：　研修の充実など
- 不正コピー、不正持ち出し
  - どんなリスクか：　個人情報を不正にコピーされたり、外部に持ち出されてしまう
  - 対策：　ルールの明確化、媒体吐出制限など

３．個人情報の不正対策をわかりやすく説明しよう

■ 提供の際に想定されるリスクの例

- 無関係な者への提供・売却（不正）
  - どんなリスクか：　サービスや業務上必要のない相手に他人の個人情報を提供してしまう
  - 対策：　外部提供ルールの明確化、ログの取得・分析・監視、従業員監督・教育
- 不適切な提供方法
  - どんなリスクか：　提供時に漏えい、紛失等してしまう
  - 対策：　専用線、暗号化、パスワード、封緘、簡易書留
- 間違い
  - どんなリスクか：　提供先や提供する個人情報を間違えてしまう
  - 対策：　ダブルチェック、システム化など

3．個人情報の不正対策をわかりやすく説明しよう

■ 委託の際に想定されるリスクの例

- 委託先の杜撰
  - どんなリスクか：　委託先が杜撰に個人情報を取り扱ってしまう
  - 対策：　情報保護管理体制の確認、アクセス者の限定、委託契約、提供ルール、消去ルール
基本的には自社と同様の監督が重要。選定・委託契約・報告徴収。
- 再委託先以降の杜撰
  - どんなリスクか：　再委託先以降が杜撰に個人情報を取り扱ってしまう
  - 対策：　再委託以降の許諾制など
- 不透明
  - どんなリスクか：　ユーザそして委託元にとって個人情報の取扱い実態がわかりづらい
  - 対策：　見える化、報告義務など

３．個人情報の不正対策をわかりやすく説明しよう

■ 保管・消去の際に想定されるリスクの例

- 漏えい等
  - どんなリスクか：　個人情報が漏えいしたり無くなったり欠けたり改ざんされたりしてしまう
  - 対策：　安全管理措置（組織的、人的、物理的、技術的）
- 古くて不正確
  - どんなリスクか：　個人情報が古くなり不正確なまま保有され続けてしまう
  - 対策：　現況確認
  - ※　古いまま保管しつづける必要がある場合等はあてはまらないリスク（例、過去の確定申告書）
- 未消去・未廃棄
  - どんなリスクか：　個人情報が不必要なまま消去されず保管され続けてしまう、不十分な廃棄をされてしまう
  - 対策：　保存期間の設定、確実な廃棄など

6.　第三者点検（専門家意見）のポイント

第三者点検の趣旨

外部者のチェック

- PIAは自己評価である。評価というと日本では第三者評価のイメージが根強い。そこで、日本では、自己評価又は第三者評価したPIAにさらに別の者による点検を入れている。
- 自己評価だからといっておざなりな評価であったり、評価実施機関にとって都合の良い評価であったりしては決してならない
- 自己評価であるのは、自らプライバシー・リスクを想定し、対策を講じることを目的としたものであって、安易な評価を量産するためではない
- そこで、外部者が点検することで、適切に評価が実施されることを担保する

専門的知見の獲得

- プライバシー・リスクを想定しその対策を検討するが、プライバシーの考え方、対策の考え方等において、専門家の観点を入れることで、より適切なプライバシー保護を目指す

方法

- データ倫理審査会

第三者点検の５つの観点

広く意見を述べることができるものの、
主な意見の観点は
５点に大別される

１．取扱実態のわかりやすさ

ポイント

- **一般人**の視点で、**「私の個人情報がどのようになぜ取り扱われるのか」**が**わかりやすく**示されているか
- 第三者点検は実地監査ではない。実際の事務状況を逐一確認し、評価書に記載された通りの実態となるかどうかを監査することは、求められていない。評価書を読んで、論理的矛盾がないか確認するなどする。
- 実地監査を行っても良い。

点検の観点

- **個人情報の流れ**（全体的な流れのほか、どこからどのように入手して、どのように誰が使用し、誰に委託され、誰に提供・移転され、どのように保管・消去されるか）が理解できるよう説明されているか
  - この点は、一般の意見聴取プロセスで重点的に点検される。しかし一般の意見聴取は義務付けられず、また任意に実施しても、現実の実務を踏まえると、あまり意見が提出されないこともあるため、第三者点検においても点検する。
- 個人情報の取扱いの説明に誤りがないか、確認してもよい。例えば、事務を遂行するのに、評価書に記載されている対象者の範囲では狭すぎる場合等は、誤りでないか評価実施機関に確認する。

2．適切な取扱いか

ポイント

- **「個人情報をそのように取り扱う理由などを合理的に説明できているか」**

点検の観点

- まず、評価書に記載したような取扱いをする必要性が、合理的に説明できているか
  - 例えば、その範囲の個人情報を取り扱う必要があるか、その個人情報の項目を取り扱う必要があるか
  - 説明を読んで、一般人の視点に立って納得できる程度に合理的か
- 個人情報の取扱いがプライバシー等へ与える影響度合いはどの程度か
  - 必要性が低かったり影響が大きい場合は、代替策があれば代替策を立て、代替策がない場合は取扱いをやめるか、リスク対策を厚く講じるべき

□ 但し、プライバシーへの影響が大きい場合でも、取扱いをやめたり、代替策を立てることが困難なときも

- 取扱い中止・変更が必須とされるわけではない←プライバシー以外の権利保護のために必要な場合も
- そのような場合は、リスク対策を厚くする等、個人情報を取り扱う必要性とプライバシーに与える影響とを比較考量し、適切な取扱いを図っていく。

3．想定リスクの妥当性

- 第三者点検の中心部分の一つ

ポイント

- 当該事務で自分の個人情報を取り扱われることで、何を**脅威**に感じるか
- 評価書を見て、既に挙げられているもの（**典型リスク**）以外にリスクはないのか検討

点検の観点

- 脅威の例
  - 住民税：正確な情報か（→税額が誤ったりしないか）、みだりに他人に自分の収入を知られないか、みだりに他人の自分の勤務先を知られないか
- 典型リスクも含め、リスク高低を検討するとさらに良い
  - プライバシーへの影響・リスクが大きいものは、リスク対策の適切性の観点から十分なチェックを行う
- 評価実施機関は日々遂行している事務のことなので、プライバシー・リスクを見落とすことも
  - 専門家でない一般人の視点で、自分の個人情報が取り扱われることで何が不安なのか、脅威なのか
  - さらに専門家の視点から、想定されるリスクが他にないのか、リスクの高低はどの程度か

4．リスク対策の適切性

- 第三者点検の中心部分の一つ
- **合理的説明**ができているか
  - 評価書を見て、リスクへの対策として合理的な説明となっているかを確認
  - 最低限、日本語としてリスクと対策がかみ合い、かつその対策によってリスクを防止できることを、一般人が納得できること

  × 個人情報を過剰に入手してしまうリスクに対し、「個人情報を暗号化する」等といった対策

  ← リスクと対策がかみ合っていない。個人情報を暗号化しても、不必要な個人情報を入手しないようにはならない

  × 漏えい・紛失リスクに対し、「安全性が担保されているシステムを使用する」といった記載

  ← なぜそのシステムが安全性を担保されているといえるのかが明らかではない。またトートロジーに陥ったリスク対策も見られる。
- **リスクレベルに応じた対策**か
  - 評価書を見て、リスクレベルに応じた対策となっているかを確認
    - プライバシーへの影響・リスクが大きいものについては、十分な対策がとられているか
    - リスク対策が現在の水準と合致しているか確認することも考えられる
    - 特に、専門的知見を要する観点！
- リスク対策として良い点があれば、その旨を意見するのもよい
  - 批判は当然重要だが、良い点があれば認めることも、評価実施側のモチベーションにつながったり、他の評価実施機関の手本になる等、良い効果が期待

５．手続の適切性

- しきい値判断
  - PIAの実施要否・実施レベルなどを「しきい値評価」によって振り分け判断している場合、判断結果に謝りがないか
  - しきい値判断項目の事実認定に誤りがないか
    - 例えば、対象者数や取扱者数などに基づいてしきい値判断している場合、根拠数値のカウント方法を確認する
- 評価書の非公表箇所は妥当か
  - 評価書に求められる透明性を重視し、真に公表することでリスクがある場合のみ、また公表することでリスクがある部分に限って、非公表とすべき。記載のレベルを抽象化しても、評価の趣旨を体現でき、かつ記載のレベルを抽象化すれば公表できるのであれば、そのように評価書を改めることも検討すべき。記載のうちの一部のみを非公表とすれば足りるのであれば、当該一部のみを墨塗りするなどの措置をとるべき。
- 一般の意見聴取手続の適切性
  - 聴取期間が適切か、形式的に手続を経ただけではないか、得られた意見のうち評価書に反映すべき点を反映しているか、得られた意見のうち評価実施機関の考え方を回答すべきものに回答しているか等
- しきい値判断結果以外は、一般は確認できない点なので、第三者点検での確認が重要

評価書様式ほか

- 個人情報保護委員会Webサイト
  - 評価書記載例
  - http://www.ppc.go.jp/files/pdf/12zenkoumokuyouryo.pdf
  - 重点項目評価書様式（記載要領付）
  - http://www.ppc.go.jp/files/pdf/20160101_youshiki3kisaiyouryou.pdf
  - 全項目評価書様式（記載要領付）
  - http://www.ppc.go.jp/files/pdf/20160101_youshiki4kisaiyouryou.pdf
  - 特定個人情報保護評価の概要
  - http://www.ppc.go.jp/files/pdf/20160101hyoukasyousai.pdf
  - 既に公表済の特定個人情報保護評価書の検索サイト
  - http://www.ppc.go.jp/mynumber/

参考

- 『特定個人情報保護評価のための番号法解説～プライバシー影響評価（PIA)のすべて』
  - 第一法規、２０１５年１１月刊行
  - http://goo.gl/yoWZ1U

- 水町によるPIAの実践例
  - 民間サービス→　http://www.miyauchi-law.com/f/180327PIA.pdf　の9ページ目以降
  - 自治体サービス→　http://www.miyauchi-law.com/f/180628PIAhimeji.pdf

- 作った人が明かすマイナンバー　プライバシー保護の勘所（Itpro)
  - 実はカンタン、「プライバシー影響評価」
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/052100005/?ST=security&P=1
  - 脱・行政文書、間違いのコピペ丸投げ
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600008/
  - どうなっている？あなたの街のマイナンバー
  - http://itpro.nikkeibp.co.jp/atcl/column/15/052100128/080600006/?ST=management&P=1