国のIT・データ活用戦略と法律トレンド

～行政ビッグデータ（オープンデータ、非識別加工情報、官デ法）・医療ビッグデータ・デジタルファースト・DPIA等～

弁護士　水町雅子

2019.3

講師略歴

弁護士　　水町雅子　（みずまちまさこ）

http://www.miyauchi-law.com　　メール→osg@miyauchi-law.com

- 東京大学教養学部相関社会科学卒業
- 現、みずほ情報総研入社

ITシステム設計・開発・運用、事業企画等業務に従事

- 東京大学大学院法学政治学研究科法曹養成専攻（法科大学院）修了
- 司法試験合格、法曹資格取得、第二東京弁護士会に弁護士登録
- 内閣官房社会保障改革担当室参事官補佐

マイナンバー制度立案（特にマイナンバー法立法作業、情報保護評価立案）に従事

- 特定個人情報保護委員会（現、個人情報保護委員会）上席政策調査員

マイナンバー制度における個人情報保護業務（特にガイドライン、特定情報保護評価）に従事

- 首相官邸IT総合戦略本部「パーソナルデータに関する検討会」参考人

個人情報保護改正検討

- 宮内・水町IT法律事務所（旧、五番町法律事務所）共同設立、現在にいたる

その他、東京都港区・東京都杉並区・茨木県つくば市の情報公開・個人情報保護審査会委員、
東京都都政改革アドバイザリー会議委員等を務める。

元SE（言語はPHP, Java, Perl, VB等）として、ITと法律の融合を目指す。
IT案件・情報案件（個人情報、医療データ、マイナンバー、不正競争防止法等）を中心に取り扱う。

AGENDA

- データ利活用の背景
  - 様々なデータが蓄積される時代だからこそのデータ利活用政策
- 匿名加工情報／非識別加工情報／オープンデータ
  - どのような仕組みか
  - どのような手続で外部提供できるのか
  - 導入・安定運用に向けた課題は何か
- 医療ビッグデータ法（次世代医療基盤法）
  - 医学研究促進のため、医療データを取得容易に
  - 大臣認定による規律、匿名加工医療情報
- その他データ関連政策
  - オープンデータ、官民データ、マイナンバー、デジタルガバメントほか
- 個人情報保護のためのわかりやすい手法　PIA　／DPIA

データ利活用の背景

データを活用する技術トレンド・政策・法律が百花繚乱

データ活用戦略・トレンド

官民でデータを活用しようという政策・技術トレンドが百花繚乱

官民データ活用推進基本法		医療ビッグデータ法	デジタルファースト法	
マイナンバー法改正		オープンデータ/非識別加工情報（行政ビッグデータ）		
匿名加工情報（個人情報保護法改正、ビッグデータ対応）			デジタルガバメント	
ワンストップ（子育て・相続・引越）			ワンスオンリー	
AI （著作権法改正、機械学習の促進）			ペーパーレス	
全国保健医療情報ネットワーク		医療等ID	EHR	PHR
ブロックチェーン		IoT　クラウド	ドローン	ロボット
マイナンバーカード		キャッシュレス	JPKI	自動運転
EBPM	RPA	Society5.0	DPIA	8K

様々なデータが蓄積される時代

- もはや書面で個人情報を提供するだけではない
- トレンドのAI、ブロックチェーン、RPA、EHR 、PHR、IoT、ロボット等もデータを活用する仕組みともいえる

どんなキーワードでネット検索をしたか	どんなサイトを閲覧したか	どんなアプリをインストール／起動しているか	生活時間帯、ネット活動時間帯
どんなSNSを使用しているか	SNSへのログイン（頻度・時間帯）	SNS内での行動	フォロワー／友人の数・種類
どのサイトでどんな商品を購買したか	どの実店舗でどんな商品を購買したか	どんな課金をしているか	どんなゲームをプレイしているか
家族構成	居住地、勤務地	移動履歴（GPS、交通系ICカード）	カード決済状況
体重、血圧、体温	歩数、ランニング距離	電子おくすり手帳	電子母子手帳

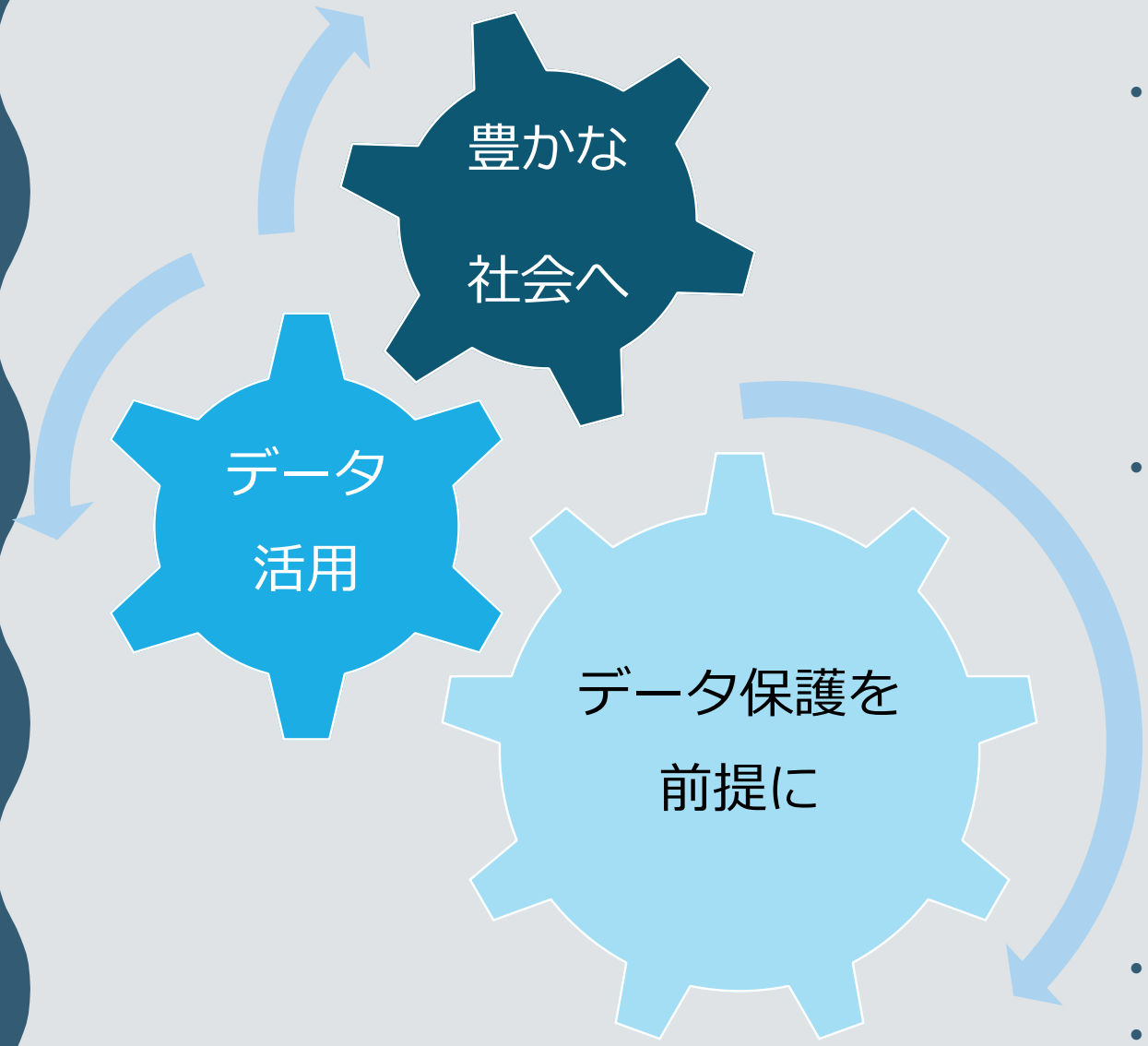
スマホ
パソコン
機器、センサー
クレカ
ポイントカード
ICカード
POS端末
GPS

データ利活用政策の加速化

このデータ利活用の流れは民間だけではなく、行政にも押し寄せている

平成２５年	マイナンバー法（官・民）
平成２７年	個人情報保護法が改正（官・民） • 匿名加工情報の導入
平成２８年	官民データ活用推進基本法（官・民） • 官民データ活用推進計画の策定義務・努力義務
	行政機関個人情報保護法及び独立行政法人等個人情報保護法が改正（官） • 非識別加工情報の導入
平成２９年	次世代医療基盤法（医療ビッグデータ法）（官・民） • 匿名加工医療情報の導入
平成３１年予定	デジタルファースト法案（官・民） • 行政手続のデジタル化

データ保護と活用の両立



- 個人情報保護
  - マイナンバー法によるレギュレーション
  - 個人情報保護法改正によるレギュレーション強化
  - GDPR施行
  - サイバーセキュリティ対策
  - 国民意識の高まり
- 他方で、データ活用
  - 官民データ活用推進基本法、次世代医療基盤法（医療ビッグデータ法）、匿名加工情報（個人情報保護法改正、ビッグデータ対応）、オープンデータ/非識別加工情報（行政ビッグデータ、行政機関個人情報保護法改正・独立行政法人等個人情報保護法改正）、EBPM、機械学習の促進（著作権法改正、AI）、デジタルファースト法、マイナンバー法改正、全国保健医療ネットワーク、EHR、PHR、医療等ID
  - AI、RPA、IoT、ロボット、Society5.0
- データ活用とデータ保護の両立を意識した国の政策
- 国際的トレンド

プライバシーリスクを低減するよう加工した個人情報の利活用

オープンデータ／非識別加工情報／匿名加工情報

官民データ活用推進基本法（H28）

民間も公的機関もデータを活用しよう！
官データと民データを掛け合わせてもいいね
国・自治体で計画を立てて推進します

対象データ	官データ（国データ・独法データ・自治体データ） 例）気象、自動車、免許、許認可、施設情報、税情報
	民間データ 例）企業情報、地図、ドラレコ、混雑率、顧客層
手法	• ネットで行政手続（お役所に行かずにスマホ等から簡単に）10条1項 • 電子契約（契約もIT化）10条2・3項 • オープンデータ／非識別加工情報／匿名加工情報　→**次スライド以降** • AI／IoT／クラウド　16条 • マイナンバーカード／電子証明書　13条 • IT整備・BPR　15条　人材確保・教育　17・18条
効果	• 便利な社会、国民が安全で安心して暮らせる社会及び快適な生活環境の実現 • EBPM、透明で開かれた効率的な行政 • 新事業創出、産業発展、国際競争力の強化、地域活性

非識別加工情報

店舗を新設したい。高収入の大人女性向けの店舗にしたい。
ターゲット層が近くに居住しつつも、類似店舗が少ない地域はどこだろうか。

国・自治体が持っているデータを利活用してはどうだろう。
住所、生年月日、性別、世帯年収、子の有無などが国・自治体に情報としてあるはず。

個人情報だから取得できないのでは。

ビッグデータ等の利活用のために、「非識別加工情報／匿名加工情報」ができたはず。
個人情報ではなく（注）データを丸めて加工した情報を国・自治体から民間が取得できる。

（注）もっとも、法律上、民間にとっては個人情報ではないデータだが、国・自治体にとっては個人情報である。

オープンデータ

子どもができたよ。そこで近所の保育園・子ども関連施設を調べようと思っても、無料の地図アプリに全部表示されているわけではないし、自治体のWebサイトを見ると、住所が載っているだけで、自分で住所をコピペして地図アプリに入れないと、場所もよくわからない。なんてこの国は不親切なんだ。

私が、子育て支援アプリを作るよ。保育園・幼稚園・学校・公園・民営遊び場などの子ども関連施設情報を地図に落とし込んで、かつ保護者の口コミを載せたアプリにしよう。

僕もエンジニアだから、自分で作ろうとも思ったけどね。自治体のWebサイトに載っている住所を自分でコピペしてアプリに情報登録するのは、面倒だよ。子ども関連施設は増減するから、新規／廃止があるたびに自分で修正処理をしないといけないんだよ。

データ利活用のために、「オープンデータ」政策があるはず。
国・自治体が持つデータ（個人情報ではない）を中心として、機械処理できるような形状で公開して、商用利用も可能とする政策だよ。

匿名加工情報

店舗を新設したい。高収入の大人女性向けの店舗にしたい。
ターゲット層が近くに居住しつつも、類似店舗が少ない地域はどこだろうか。

他社が持っているデータを利活用してはどうだろう。
潜在顧客情報、マーケット情報、立地情報など、他社データを基に、分析・検討しよう。

個人情報なのに、他社から取得して問題はないのか。

ビッグデータ等の利活用のために、「非識別加工情報／匿名加工情報」ができたはず。
個人情報ではなくデータを丸めて加工した情報を「匿名加工情報」といって、通常の個人情報よりも容易に入手できる。

個人情報等の種類（例）

生の個人情報

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
水町雅子	千代田区五番町2	1981/10/23	女性	300-400万	既婚	なし
水町雅男	千代田区五番町2	1984/05/03	男性	300-400万	既婚	なし
難波舞	千代田区霞が関3-1	1970/06/18	女性	800-900万	独身	なし
番号太郎	千代田区麹町1-2	1963/09/25	男性	500-600万	既婚	あり
千代田一郎	千代田区神保町2-3-5	1997/10/10	男性	5000万-5500万	独身	あり

抽象化情報

・・　世間的イメージの匿名化は「抽象化情報」の段階。NOT「非識別加工情報」

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
－	千代田区五番町2	1981/10	女性	300-400万	既婚	なし
	千代田区五番町2	1984/05	男性	300-400万	既婚	なし
	千代田区霞が関3	1970/06	女性	800-900万	独身	なし
	千代田区麹町1	1963/09	男性	500-600万	既婚	あり
	千代田区神保町2	1997/10	**男性**	**5000万-5500万**	**独身**	**あり**

削除

番地以下削除

年齢・月齢情報を保持したうえで日の削除

個人情報等の種類（例）

非識別加工情報/匿名加工情報

具体的なデータの状態は、非識別加工情報と匿名加工情報とで変わらない

氏名	住所	生年月日	性別	世帯年収	既婚／独身	子の有無
－	千代田区五番町2	1981/10	女性	300-400万	既婚	なし
	千代田区五番町2	1984/05	男性	300-400万	既婚	なし
	千代田区霞が関3	1970/06	女性	800-900万	独身	なし
	千代田区麹町1	1963/09	男性	500-600万	既婚	あり
	千代田区神保町2	1997/10	男性	3000万超	独身	なし

削除

番地以下削除

年齢・月齢情報を保持したうえで日の削除

上位・下位5%丸め処理

その他特異データの削除、ノイズ付加等

統計情報

住所	年齢構成	性別	世帯年収	既婚／独身	子の有無
千代田区五番町	高め（平均X)	男性55%	平均700万	既婚75%	あり55%
千代田区霞が関					
千代田区麹町					
千代田区神保町					

必ずしもここまで丸める必要はない

参考）個人情報等の種類

分類	説明
生の個人情報	• そのままの状態（生データ）
抽象化情報 （法令上の用語ではない）	• 特定の個人が一見して明らかになる情報の削除 • 明らかに一意の番号の削除 • その他プライバシーに配慮した加工
非識別加工情報	• 特定の個人が一見して明らかになる情報の削除 • 特定の個人が一見して明らかにならなくても、特定の個人を識別しうる情報の完全削除 • 再識別は可 • 官にとっては依然として個人情報、民に渡れば非個人情報
匿名加工情報	• 特定の個人が一見して明らかになる情報の削除 • 特定の個人が一見して明らかにならなくても、特定の個人を識別しうる情報の完全削除 • 非識別加工情報が民間に渡れば匿名加工情報になる • 再識別は禁止 • 非個人情報
統計情報	• 完全に個人情報ではない • 匿名加工情報との境界は曖昧な部分が残る • 非個人情報

似たような政策がいっぱい？

- 非識別加工情報／オープンデータ／匿名加工情報／情報公開制度という、類似政策が４種類展開中
- 実はそれぞれ細かい法制上の違いがあって複雑ではあるが、ポイントを平たくまとめると以下の通り

オープンデータ	機械判読できるデータを取得できる 例）施設情報、道路交通量、公衆無線LANアクセスポイント、NPO法人情報、レストラン情報、バリアフリートイレ、消火栓情報、街路灯情報、税情報、治安情報
非識別加工情報	官の持つデータを取得できる 例）自動車免許情報、二輪車防犯登録情報、古物商情報、税理士情報、出入国情報、雇用保険台帳、高年齢雇用継続給付台帳
匿名加工情報	民の持つデータを容易に取得・提供できる 例）購買動向、医療情報
情報公開請求	公文書を公開して透明な行政に 例）交際費支出状況、公用車運行、施設情報

非識別加工情報

概要

- 官の持つデータを民間が利活用するためのしくみ
- 官が豊富かつ新鮮な大量のデータを保有するのは、公の利益のため。
  官の持つデータ価値を民間に還元する。いわゆる「ビッグデータ等」の利活用のため。
- 提供を受ける民間においては、**誰の情報かわからなくさせる**ことで、個人（住民等）を保護

利点

- 一般に広く公開情報とはなっていない情報を入手できる！
- 行政機関等が業務遂行の目的で保有する個人情報をもとに加工を行うため
  ・情報が悉皆的であり個人の漏れがないこと　　・個人に対する情報の種類や蓄積量が多いこと
  ・行政情報であるため情報が新鮮かつ正確であること

注意点

- 民間の欲しいデータが非識別加工情報の対象となっていない場合も多い（条例未制定自治体も多い）。全国統一フォーマット等でないと、データを入手しても活用できない場合も。
- 自治体からすれば、誰の情報かわからなくさせる加工度合いの保証が困難→国で「作成組織」を検討。立法措置も検討中。総務省「地方公共団体の非識別加工情報の作成・提供に係る効率的な仕組みの在り方に関する検討会」。
- もっとも今後は、「非識別加工情報」か「官民データ」か「オープンデータ」か、名称や形態は別として、官の持つデータ価値を民間に還元する流れが強化される見込み。
- 行政機関個人情報保護法や独立行政法人等個人情報保護法に従った手続（提案書の作成、審査、契約）が必要となる。手数料も必要で無料ではない（自治体からすれば未納時の処理も発生）。

匿名加工情報

匿名加工情報

概要

- 個人情報を匿名加工する
- **誰の情報かわからなくさせる**ことで、個人（消費者等）を保護
- 個人情報ではなくなり、簡単な手続で、内部での利活用や外部提供が可能

注意点

- 個人情報保護法の対象外となるわけではない。
  すなわち、一切のルールが課されないわけではなく、一定のルールに従う必要がある。
  もっとも、そんなに大変なルールではない。
- 法定の加工基準を満たす必要があるが、法定基準が厳格かつ抽象的。
  自分が利活用したいデータが厳格な加工を施せるものか、適したものかを
  十分検討する必要がある。

個人情報と匿名加工情報

自社が保有する顧客情報について、顧客の属性ごとに購買履歴を分析したい場合

種類	個人情報	匿名加工情報
データの**状態**	**易** • 誰の情報かがわかる状態でOK • 生データの状態でよい	**難** • 誰の情報かがわからないように加工することが必要
ルール（目的外利用）	**難** • **利用目的を確認**する • 利用目的に「顧客動向分析」などとあれば、利用目的の**範囲内**で、分析可 • 利用目的の**範囲外**なら、**本人の同意等**、個人情報保護法１６条に定める要件が必要 • 利用目的の**事後変更**もできるが、規制あり（関連性要）	**易** • **利用目的の範囲内でも範囲外でもOK**

個人情報と匿名加工情報

自社が保有する顧客情報について、顧客の属性ごとに購買履歴を分析したい場合

種類	個人情報	匿名加工情報
ルール（安全管理）	**難** • **義務**（個人情報保護法２０条）	**普通** • **加工方法等については義務**（個人情報保護法３６条２項） • **匿名加工情報自体については努力義務**（個人情報保護法３６条６項・３９条）
ルール（開示等）	**難** • 本人から求めがあれば、保有個人データは**原則開示が義務**（個人情報保護法２８条） • 訂正・利用停止請求も	**易** • 開示不要（反対に、誰の情報かわからないので、本人特定ができず、開示できない）

個人情報と匿名加工情報

他社が保有する顧客属性情報と自社が保有するデータを組み合わせて分析したいので、
他社から情報を入手したい場合

種類	個人情報	匿名加工情報
前のスライドのルールに加えて……		
ルール（提供）	**難** • グループ会社等で**共同利用**の要件を満たす場合は、個人情報保護法２３条５項３号で可 • **オプトアウト**（拒否されたらやめる）でも、個人情報保護法２３条２・３項で可能だが、社会的非難を浴びる可能性もある。また要配慮個人情報（健康診断結果、病院受診、病歴、犯罪歴等）はオプトアウト不可 • **本人同意**が必要な場合も多い	**易** • 以下の**簡易な手続で可** • 提供時に情報項目＆提供方法の**公表** • 提供先に対し匿名加工情報であることの**明示**

参考）加工基準

	行政機関個人情報保護法	個人情報保護法
	非識別加工情報	匿名加工情報
加工基準 ⇒同じ	一　個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 二　個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 三　個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）。 四　特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 五　前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。	一　保有個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 二　保有個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 三　保有個人情報と当該保有個人情報に措置を講じて得られる情報とを連結する符号（現に行政機関において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該保有個人情報と当該保有個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。） 四　特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。） 五　前各号に掲げる措置のほか、保有個人情報に含まれる記述等と当該保有個人情報を含む個人情報ファイルを構成する他の保有個人情報に含まれる記述等との差異その他の当該個人情報ファイルの性質を勘案し、その結果を踏まえて適切な措置を講ずること。

非識別加工情報と匿名加工情報

- ✓ 「匿名加工情報」も「非識別加工情報」も、**生の個人情報を加工した状態のデータ**。両方とも、**個人**（消費者・国民等）**を保護しつつ、データ流通を容易化する法制上の仕掛け**である。
- ✓ 「非識別加工情報」は中でも、官の持つデータ民間が利活用するためのしくみ
  - 非識別加工情報は行政機関／独立行政法人等がもっているデータの状態をいい、非識別加工情報が民間の手に渡った瞬間、「匿名加工情報」になる
  - 非識別加工情報の時点で、官内部では識別可能。民では識別禁止。
  - 法制が技術的かつ複雑ではある…

次ページで図表化

非識別加工情報
◆　官の持つデータを民間が利活用するためのしくみ
匿名加工情報
①自分の持つ個人情報を匿名加工情報に加工することで、簡単な手続での利活用ができる ②他社の持つ匿名加工情報を入手することで、簡単な手続での入手ができる ③非識別加工情報は行政機関／独立行政法人等がもっているデータの状態をいい、非識別加工情報が民間の手に渡った瞬間、「匿名加工情報」になる ※民間は非識別加工情報を手に入れるまでは行政機関個人情報保護法／独立行政法人等個人情報保護法に従い、手に入れた瞬間から個人情報保護法に従う

オープンデータと非識別加工情報と匿名加工情報

官（行政機関・独立行政法人等・地方公共団体等）

民（企業等）

パターン①自社で匿名加工情報を作成

加工

わが社

加工

パターン③官から入手
※非識別加工情報は民の手に渡った瞬間、「匿名加工情報」になる

パターン②他社から匿名加工情報を入手

加工

他社

パターン④官からオープンデータを入手
※オープンデータは個人情報ではないものが通例

※その他、他社から生の個人情報を入手し、自社で匿名加工情報化すること等もできるが、割愛

現状の課題（利用者目線・制度論）

- 制度があまり知られていない
  - 利用者が固定されている、多くの国民・企業は知らない状態
  - 類似制度が多数あり、どういう関係にあるのかわかりづらい
  - 国の資料も専門用語が多くわかりづらい
- 実は一般目線から見ると、理解が難しい
  - 「オープンデータ」という語感から、国・自治体がWeb公開しているものがすべて「オープンデータ」という誤解も　→実際は違う！
  - 国・自治体がWeb公開しているデータであっても、自由に利用できるわけではない（転用禁止・商用利用禁止記載がある）
    - 例）介護サービス情報公表　http://www.kaigokensaku.mhlw.go.jp/
      「本ウェブサイトの目的に沿って利用することとし、関係のない営利行為等の対象にする行為については、これを禁止します。」
  - オープンデータとしてWeb公開されているものは、ほぼ自由に利用できることが通例。
    オープンデータをよく知っている人間から見たら違いがわかるが、一般目線では違いがわかりにくい。
  - さらにいえば、転用禁止のWeb公開情報も、情報公開請求すれば転用可？
    制度が複雑で不思議

現状の課題（ニーズをとらえた制度か）

- 民間ニーズにマッチしていない恐れ
  - ほしい情報が入手できない可能性も高い
  - 具体的に民間にどのようなニーズがあり、どのようなデータが有用かを、丁寧にヒアリングする必要あり（国レベルでの対応が望ましい）。データカタログの整備も有用かもしれないが、それよりもキラーコンテンツを１０個ぐらい用意する方がインパクトが大きいのではないか。
  - 複数自治体をまたいでデータがほしいという場合もあり（A市、B市どちらの施設にしようか検討中の場合等）
  - 複数自治体間で比較ができるよう全国統一フォーマットとする、データを利活用しやすい形態で民間に提供する必要性（国レベルでの対応が望ましい）等の必要性
  - 全国統一手続にする等しないと民間からしてみたら入手手続が難しい

現状の課題（将来展望）

- データ利活用の総合ビジョン
  - 似たようなデータ利活用政策が複数展開中。しかも霞が関や自治体での担当省庁・部署がそれぞれ違ったりして、横連携があまりとれていない場合も。似たような政策を複数展開すると、民間にとってわかりにくいし、公務員の作業量の重複・無駄も
  - 非識別加工情報、オープンデータ、官民データ、庁内利活用、情報公開等とのすみ分けを行い、それぞれの利点・活用スキームを明らかにすべき。国や自治体として、どういうデータ利活用政策を打っていくのか、総合ビジョンが必要。昨今の国のデータ利活用政策は場当たり的な散発的な印象も受ける。散発的政策に振り回されず、団体ごとに課題解決に必要な取組みは何か、住民や住登外者の福祉向上のために求められるものは何かという視点に立って、どのような取組みを自団体として進めていくか、総合ビジョンを立てて、計画を立てていく必要性。
  - データ利活用政策自体は時代の方向に合致しており、また公益の実現・より良い行政の実現・住民等の福祉向上のために有用な施策。BUT実態と政策が乖離している印象も受ける。実態に沿った政策へと転換していく必要がある。もっとも、国の政策云々ではなく、データ利活用が自治体にとっても必要なことは事実。

- データ利活用という視点・公共の役割転換という視点
  - 近年、IT化及びそれに伴う大量データ化を受けて、社会、そして行政の在り方も大きく変容。自治体職員としても、これまで通りの業務運営だけではなく、現代の社会に合わせた業務運営が求められる。
  - 今後は、データ利活用と言う視点、公共の役割転換という視点が必要不可欠となってくる。

現状の課題（公務員意識等）

- プライバシー権侵害の恐れ
  - 民間に渡る非識別加工情報が、誰の情報であるかがわからない状態であることを担保する必要
  - 全国の全自治体で、それが担保できるのかという不安
    →国で「作成組織」を認定する等の措置、立法措置検討中

- 自治体側にメリットがないという自治体側の思い
  - 庁内利活用であればメリットが感じやすいのでは？
  - 情報公開制度も自治体側にメリットがないが、制度が安定運用されている。商用利用へのアレルギー、個人情報の不安が原因なのか？
  - プライバシー性の高い情報（例えば、所得額情報や障害情報など）は、いったん、非識別加工情報の対象から外し、法人情報やプライバシー性の低い情報から運用を開始していくことも考えられるのでは

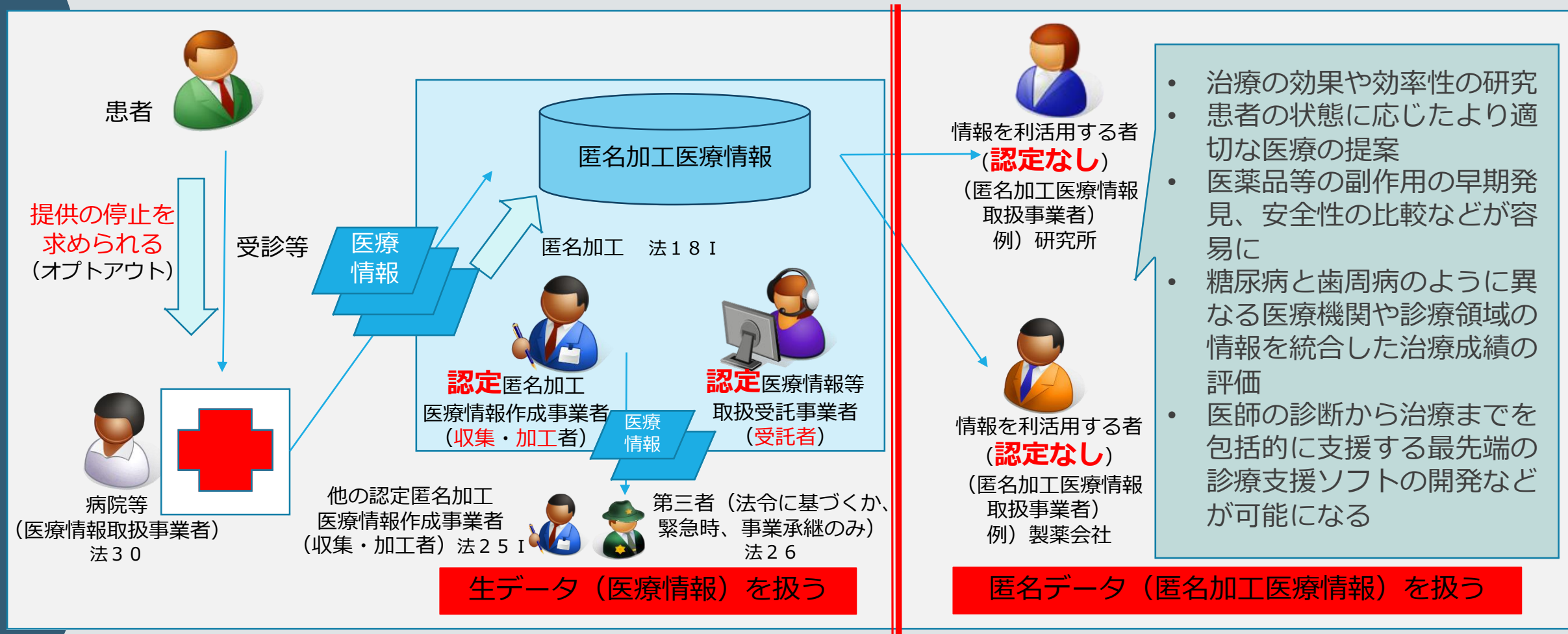
現状の課題（公的機関での運用等）

- 個人情報取扱事務の整備
  - 民間が必要データを調査するのに、国の場合、e-Govに掲載された「個人情報ファイル簿」を見ることになっている
  - 自治体の場合、「個人情報取扱事務登録簿」等がこれに当たるが、更新・精査されていない例も多い
  - データカタログである個人情報取扱事務の整備が必要
- 運用フローの確立
  - 手数料額が作業時間によって異なると、民間が想定するよりも膨大な金額がかかる可能性も。その結果未払いが発生しては、自治体側でその処理が必要に。またデータの加工形態が民間のニーズと異なりすぎるとトラブルになる恐れ。民間と丁寧な話し合いが必要。
- 条例
  - 国提供の条例ひな形では足りない可能性。自条例や自団体での運用に合わせてカスタマイズする必要あり。

医療ビッグデータ法（次世代医療基盤法）

匿名加工医療情報

次世代医療基盤法の全体イメージ



- 治療の効果や効率性の研究
- 患者の状態に応じたより適切な医療の提案
- 医薬品等の副作用の早期発見、安全性の比較などが容易に
- 糖尿病と歯周病のように異なる医療機関や診療領域の情報を統合した治療成績の評価
- 医師の診断から治療までを包括的に支援する最先端の診療支援ソフトの開発などが可能になる

医療ビッグデータ法（次世代医療基盤法）とは

目標・効果	患者の健康状態・QOLの改善	より質の高い医療	医学の発展	新サービスの実現	健康長寿社会の形成
背景	• AIの進化 • IT化の発展 • 医療ITの進展に伴い医療情報が電子データとして大量蓄積可				
懸念・不安	• 医療情報はプライバシー性が高い極めて重要な個人情報 • 個人情報保護が徹底されるのか • 反面、全データに必ず同意が必要とすれば、活用できるデータが少数にとどまり、大規模な研究等は難しく、医療分野の研究開発等が困難になる恐れ				

目標・効果を達成しつつ懸念・不安を解消するために

次世代医療基盤**法**（医療ビッグデータ法）の制定

医療ビッグデータ法（次世代医療基盤法）のポイント

次世代医療基盤法のポイント
① 医療情報をそのままではなく、匿名加工して誰の情報かわからなくした上で研究開発などに役立てる →万一漏えいしたり悪用されても、誰の医療情報かがわからないように厳格に匿名加工 →匿名加工方法は法律で定められていて、これを守らなければならない
② 患者本人は拒否することができる、患者が拒否すれば匿名加工医療情報を外部提供できない →いつでも拒否できることで、患者の権利を保障
③ 大臣認定を受けた事業者しか匿名加工医療情報を作成・提供することはできない →安全・的確に加工等できる能力をもった適切な事業者か大臣認定。認定後もチェック。
④ 大臣認定を受けた事業者から委託を受けた業者が不正行為等をしないよう、外部委託先も大臣認定を受ける必要がある →不適切な事業者へ外部委託されないようにする
⑤ 大臣認定事業者には高い管理基準等が求められ、安全管理体制等を厳格に整備する必要がある →一度大臣認定を取得すればよいというものではなく、問題があれば大臣認定が取り消され、事業が継続できなくなりうる

認定事業者等の義務の比較

※利活用者は、個情法の義務に注意 ※認定事業者側の義務として、利活用者が適切な措置をとるよう契約するよう求められる	認定匿名加工医療情報作成事業者（収集・加工者）	認定医療情報等取扱受託事業者（受託者）	匿名加工医療情報取扱事業者（利活用者）※
大臣認定	○（８条）	○（２９条、８条）	×
帳簿	○（１３条）	○（２９条、１３条）	×
目的外利用の厳格化	○（１７条）	○（２９条、１７条）	×
主務省令基準に従った医療情報の加工	○（１８条１項）	○（２９条、１８条１項）	×
識別禁止	○（１８条２項・３項）	○（２９条、１８条２項）	○（１８条３項）
消去義務（**努力義務ではない**）	○（１９条）	○（２９条、１９条）	×
安全管理措置	**○（２０条）**	**○（２９条、２０条）**	×
従業者の監督	○（２１条）	**○（２９条、２１条）**	×
従業者等の秘密保持義務	○（２２条）	**○（２９条、２２条）**	×
委託先の監督	○（２４条）	**○（２９条、２４条）**	×
第三者提供制限の厳格化	○（２６条）	**○（２９条、２６条）**	×
苦情処理（**努力義務ではない**）	○（２９条）	**○（２９条、２７条）**	×

利活用者（匿名加工医療情報取扱事業者）のやるべきこと
匿名加工医療情報を大臣認定事業者から取得する側

①	**大臣認定や大臣届出等は、不要** **→大臣認定が要求されるのは匿名加工化する認定匿名加工医療情報作成事業者と認定医療情報等取扱受託事業者**
②	医療分野の研究開発に役立てるためであれば、基本的に誰でも、匿名加工医療情報を取得できる。 →製薬会社・保険会社・研究所に限られない！
③	もっとも、大臣認定事業者設置の第三者委員会で審査を受ける必要あり →次世代医療基盤法基本方針に照らして適切な医療分野の研究開発に資するか →匿名加工医療情報の利用内容が、科学的に妥当か →匿名加工医療情報に基づく研究開発結果を一般市民に提供する場合、その公表方法等が、一定の地域や団体に属する者等の本人や子孫以外にも不利益が生じないよう配慮されているか →研究開発にかかる金銭その他の利益収受・管理の方法が妥当か
④	識別禁止 →取得した匿名加工医療情報が誰の情報かわかるように他の情報と照合したり、削除した記述を取得したり、詳しい加工方法を取得したりすることは禁止（次世代医療基盤法１８条３項）

利活用者（匿名加工医療情報取扱事業者）のやるべきこと

匿名加工医療情報を大臣認定事業者から取得する側

⑤　匿名加工医療情報に対する安全管理措置
　→個人情報や特定個人情報よりも少しレベルを下げることも可能か

⑥　大臣認定事業者との取得契約の締結
- 取得する匿名加工医療情報の利用目的・利用態様・利用範囲等の利用条件を明確化する
- 安全管理措置を適切に講じること
- 大臣認定事業者が、匿名加工医療情報の取得側が契約遵守をしていることを確認できること
- 他者に匿名加工医療情報をさらに提供する場合は、
  利用条件を含め事前に大臣認定事業者の許可を得るとともに契約を締結すること
- 利活用条件に反する匿名加工医療情報の取扱いを行った場合は契約違反であり、
  かつ利用停止・公表等の制裁措置の対象になること
- 大臣認定事業者は、提供する際に匿名加工医療情報であることを明示すること

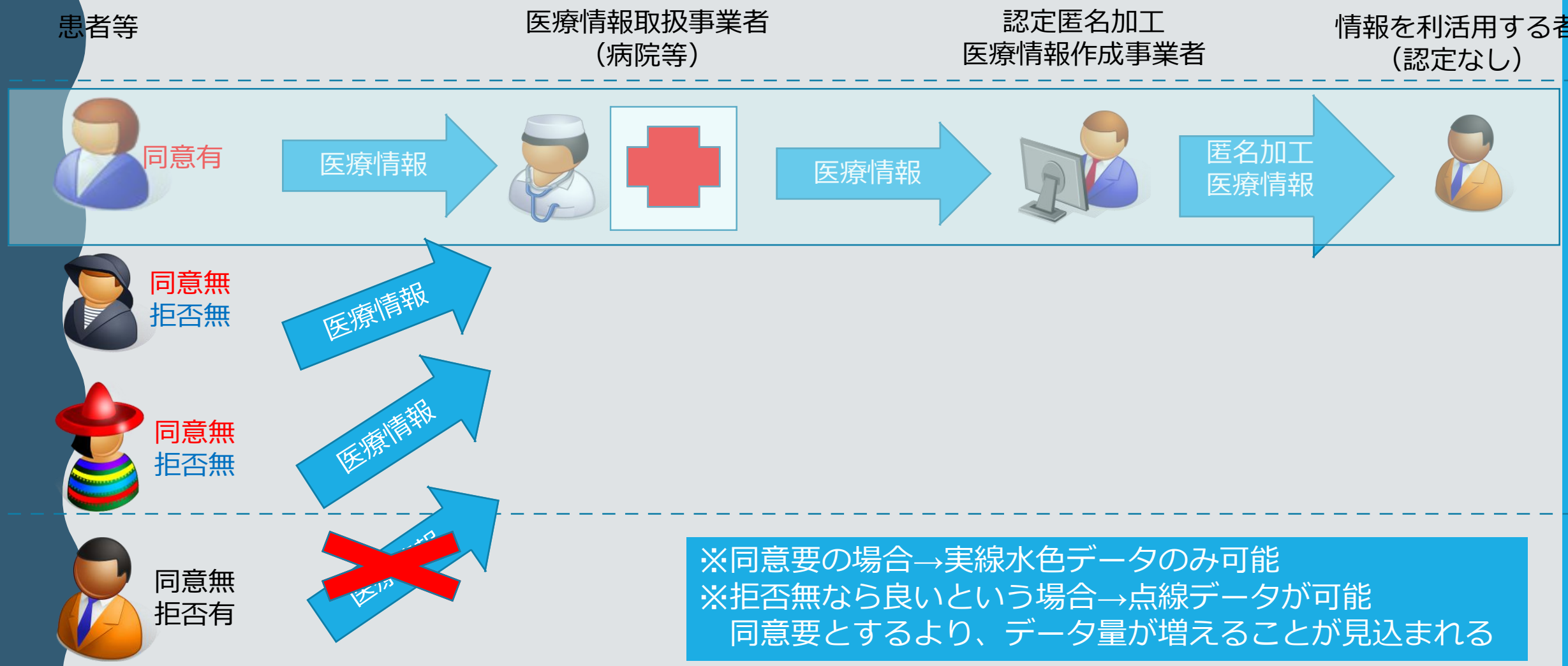
同意と拒否の相違点

次世代医療基盤法では同意は不要で拒否がなければ、医療情報を提供できる。
明確な同意がなくとも明確な拒否がなければ、
匿名加工医療情報を作成して外部提供することができる。

【同意要の場合】	同意を取得	⇒	外部提供	⇒	同意撤回されたら止める
【拒否がなければよい場合】	↑ 不要		外部提供	⇒	拒否されたら止める

※拒否無なら良いという場合、同意取得行為が不要

同意と拒否の相違点



※同意要の場合→実線水色データのみ可能
※拒否無なら良いという場合→点線データが可能
　同意要とするより、データ量が増えることが見込まれる

匿名加工医療情報作成事業者の認定条件

認定条件	■ 申請者が、医療分野の研究開発に資するよう、医療情報を取得・整理・加工して、匿名加工医療情報を適確に作成・提供するに足りる能力を有するものとして主務省令で定める基準に適合していること（８条３項２号）
	■ 医療情報等及び匿名加工医療情報の漏えい、滅失又は毀損の防止その他の当該医療情報等及び匿名加工医療情報の安全管理のために必要かつ適切なものとして主務省令で定める措置が講じられていること（８条３項３号）
	■ 申請者が、医療情報等及び匿名加工医療情報の安全管理のための措置を適確に実施するに足りる能力を有すること（８条３項４号）
	■ 医療ビッグデータ法その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者は不可（８条３項１号イ）
	■ 認定を取り消され、その取消しの日から二年を経過しない者は不可（８条３項１号ロ）
	■ 匿名加工医療情報作成事業を行う役員又は主務省令で定める使用人に、成年被後見人若しくは被保佐人又は外国の法令上これらに相当する者、破産手続開始の決定を受けて復権を得ない者又は外国の法令上これに相当する者、この法律その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者、認定を取り消された場合において、その処分のあった日前三十日以内に当該認定に係る事業を行う役員又は主務省令で定める使用人であった者で、その処分のあった日から二年を経過しないものがいる場合は不可（８条３項１号ハ）
	■ 法人に限る（８条１項）

医療情報等取扱受託事業者の認定条件

認定要	■ 大臣認定を取得した受託者以外には、委託不可（２３条１項）
	■ 再委託以降も、大臣認定を取得した受託者以外不可、かつ委託者の許諾要（２３条２項）
認定条件	■ 医療情報等及び匿名加工医療情報の漏えい、滅失又は毀損の防止その他の当該医療情報等及び匿名加工医療情報の安全管理のために必要かつ適切なものとして主務省令で定める措置が講じられていること（２９条、８条３項３号）
	■ 申請者が、医療情報等及び匿名加工医療情報の安全管理のための措置を適確に実施するに足りる能力を有すること（２９条、８条３項４号）
	■ 医療ビッグデータ法その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者は不可（２９条、８条３項１号イ）
	■ 認定を取り消され、その取消しの日から二年を経過しない者は不可（２９条、８条３項１号ロ）
	■ その事業を行う役員又は主務省令で定める使用人に、成年被後見人若しくは被保佐人又は外国の法令上これらに相当する者、破産手続開始の決定を受けて復権を得ない者又は外国の法令上これに相当する者、この法律その他個人情報の適正な取扱いに関する法律で政令で定めるもの又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者、認定を取り消された場合において、その処分のあった日前三十日以内に当該認定に係る事業を行う役員又は主務省令で定める使用人であった者で、その処分のあった日から二年を経過しないものがいる場合は不可（２９条、８条３項１号ハ）
	■ 法人に限る（２９条、８条１項）

病院等（医療情報取扱事業者）のやるべきこと

提供義務	**医療情報を提供する義務はない**、また自ら匿名加工して個情法に従った外部提供も可能
提供時の義務	提供するなら以下の義務がある
	①　オプトアウト準備（３０条１項） ■ 本人に通知（提供すること、提供データの項目、提供方法、提供を停止する旨、提供停止の求めの受付方法） ■ 主務大臣への届出 ■ 初回のみではなく、一定事項に変更があれば、本人に通知＆主務大臣に届け出る（３０条２項） ■ 主務大臣は届け出られた内容を公表する（３０条３項）
	②　オプトアウトへの対応（３１条） ■ 求めがあれば、遅滞なく書面を交付（３１条１項） ■ 交付した書面の写しを保存（３１条３項） ■ あらかじめ承諾があれば、書面ではなくデータでも可（３１条２項・３項） ■ 提供を停止する（もっとも、**既に提供した情報の削除は法的には義務ではない**）
	③　記録（３２条） ■ 認定匿名医療情報作成事業者へ提供したときは、年月日等を記録し保存
監督	主務大臣による報告徴収・立入検査の可能性（３５条１項）　※内閣総理大臣、文部科学大臣、厚生労働大臣及び経済産業大臣（３９）
	主務大臣による命令の可能性（３７条５項）

加工等の能力があること
（法８条３項２号・規則５条）

データ
（９号）

- **自ら取得できる医療情報（アウトカムを含む）が、認定事業開始時点で年間１００万人以上、事業開始後３年目に年間２００万人以上に達することを基本とする**
  レセプトや健診情報はカウントに含めない。延べ人数ではなく実人数。

難

人
（１・２号）

- 統括管理責任者を設置
- 大規模な医療情報の加工に相当の経験・識見を有する者を確保
  アウトカムを含む大規模な医療情報について、利用用途等に応じた個人識別性のリスク評価により匿名加工の程度を調整するなど、匿名加工に一定の実務経験・知見を有する者
- 匿名加工医療情報を用いた医療の研究開発推進に相当の経験・識見を有する者を確保
  大学、研究機関、企業等において一定の総括的な権限者として、アウトカムを含む大規模な匿名加工医療情報を用いた医療分野の研究開発を５年以上行うなど、利活用者の研究開発ニーズを理解しニーズ開発する専門性を有する者
- 医療情報の取得及び整理に相当の経験・識見を有する者を確保
  医療機関の医療情報部などで一定の権限者としてアウトカムを含む大規模な医療情報を５年以上管理するなど、適切に医療情報を取得し利活用者のニーズに応じて必要な情報を選定抽出することに専門性を有する者。医療機関からの受託経験でも可。

難

加工等の能力があること
（法８条３項２号・規則５条）

提供審査体制
（７号）

匿名加工医療情報の提供の是非の判断に際し、基本方針に照らし、医療分野の研究開発に資するために適切に取り扱われることについて適切に審査できる体制整備が必要　⇒　中立・公正な**委員会**を運営する

- ５名以上男女両性から成る委員会を構成（自然科学の有識者（医学・医療の専門家等）、人文・社会科学の有識者（倫理学・法律学の専門家等）、本人の観点も含めて一般の立場から意見を述べられる者、認定事業者に所属しない者を複数含める）
- 委員会では次の事項を審査

  ①匿名加工医療情報の**利用目的**が、基本方針に照らして適切な医療分野の研究開発に資するか
  ②匿名加工医療情報の利用内容が、**科学的**に妥当か
  ③研究開発結果を一般市民に提供する際は、その公表方法等が、**一定の地域や団体に属する者等の**本人や子孫以外にも**不利益**が生じないよう配慮されたものとなっているか
  ④研究開発にかかる金銭その他の**利益収受・管理の方法が妥当**か
- 委員会**規程**を定める（組織・運営、迅速審査の適用範囲・審査方法等実施手順等について）
- 委員会規程、委員名簿、委員会開催状況及び審査概要（年１回以上）を公表する
- 審査資料は、研究開発終了が報告されるまで保管
- 委員会審査を経て、認定事業者と匿名加工医療情報取扱事業者との間で**契約**で、匿名加工医療情報の利用条件（利用目的、内容等）、安全管理措置、違反時の制裁措置を明記して、匿名加工医療情報を提供する
- 医療情報取扱事業者→認定事業者、認定事業者→匿名加工医療情報取扱事業者への提供は、倫理指針の適用対象ではなく、**倫理審査委員会の承認は不要**

加工等の能力があること
（法８条３項２号・規則５条）

差別的取扱禁止（１１号）	● 特定の匿名加工医療情報取扱事業者に対して不当な差別取扱いをしない ● **利用料**等の匿名加工医療情報の提供条件に付いて、不当な差別的取り扱いをするものでないことを明確に定めている**内部規則等**を申請時に添付する
運営体制（４号）	● 以下の内容を含む内部規則等を定める ①内部管理体制（責任体制、法令等遵守状況の検証方法等、認定受託者を含めた組織体制） ②医療情報の取得（排他的・恣意的契約を締結しない、通知書面の内容・通知方法の確認等） ③匿名加工医療情報の提供（安全管理措置、金銭等の収受・管理方法等） ④内部規則等を全役職員に周知徹底する方法 ● 内部規則等に基づく事業運営の検証がされるなど、法令等遵守の運営確保
広報啓発相談体制（８号）	● 広報・啓発活動を行う体制を整備 ● 匿名加工医療情報作成事業の実施状況について公表 ● 本人、医療情報取扱事業者、匿名加工医療情報取扱事業者からの相談に適切に応じる体制整備
設備（３号）	● 大規模な医療情報を適切に格納、検索、保管できる検索システム ● 大規模な医療情報を円滑・適正に取得できる設備 ● 匿名加工医療情報を円滑・適正に提供できる設備
標準規格（１０号）	● 「保健医療情報分野の標準規格として認めるべき規格について」（平成２２年３月３１日付け医政発０３３１第１号厚生労働省医政局長通知）で医療情報取扱事業者から医療情報の提供を受けられる体制を整備

加工等の能力があること
（法８条３項２号・規則５条）

経理的基礎（５号）	● 匿名加工医療情報作成事業の開始及び継続に必要な資金等を確保可能であること　難 ● 事業の開始・継続に要する資金の総額及び資金調達方法を記載した書類、単年の事業計画書・収支予算書、中期的計画、財務諸表によって審査 ● 匿名加工医療情報作成事業以外を兼業しているときは、匿名加工医療情報作成事業部門における経理区分を明確にして書類を提出する
中期的計画（６号）	以下の事項を含み、基本方針に照らし適切であることが求められる。目標と具体的達成計画も必要。中期的とは５年間を基本とする。 ● 事業運営方針（計画期間を含む） ● 医療情報を提供する医療情報取扱事業者 ● 自ら取得する医療情報の内容・規模 ● 提供する匿名加工医療情報の内容・提供先 ● 匿名加工医療情報作成事業にかかる収支

安全管理措置（法８条３項３・４号・規則６条）

組織的安全管理措置
（１号）

〇基本方針の策定
- ①関連法令・規程等の遵守、②安全管理措置に関する基本的な考え方、③質問及び苦情の対応窓口等

〇権限・責任・業務の明確化
- 情報セキュリティを含む安全管理の業務経験を５年以上有する者等を事業者ごとに配置

〇漏えい時等の体制整備
- 関係法令等に違反している事実又はその兆候を把握した場合の責任者への報告連絡体制の整備
- 事故対応の担当者と責任者の明確化（事故対応には、事実関係の調査及び原因の究明、再発防止策の検討及び策定、事実関係、再発防止策等の報告も含む）
- 緊急時の対応の観点から、高い責任と権限を有する者が、オープンなネットワーク環境から切り離した環境で基幹系システムにアクセスできる取扱環境（シンクライアント方式の活用等）を確保
- 漏えい等の事案発生時の報告窓口の一元化
- 情報のやり取り時（病院等の医療情報取扱事業者から医療情報を受け取る際、匿名加工医療情報を利活用者に提供する際）には、ログの収集をし、収集したログを監視・分析する体制を整備
- 情報システムへの脅威に対する備えや監視・分析に取り組む（CSIRT（Computer Security Incident Response Team）の設置、SOC（Security Operation Center）の整備等）
- 内閣府への報告は義務⇔個人情報保護委員会への報告は努力義務

〇規程策定・運用評価・改善

〇第三者認証等

安全管理措置
（法８条３項３・４号・規則６条）

人的安全管理措置 （２号）	○欠格事由に該当しないことの確認 ・誓約書、確認書等 ○目的外取扱いの防止 ・制度の趣旨・目的を従業者と確認したり、守秘義務を徹底するために就業規則に対応条項を盛り込んだり、誓約書を取得したり、違反行為を行った者に対して懲戒を行う旨を定めるなど ○教育・訓練 ○無権限者による取扱い防止 ・認定事業に関して管理している医療情報等や匿名加工医療情報を取り扱う区域への立入管理・制限 ・認定事業に関して管理している医療情報等や匿名加工医療情報を取り扱う端末のログイン制限 ・就業中に知り得た認定事業に関して管理している医療情報等や匿名加工医療情報について、退職後の取扱いに関するルールの策定 ・認定事業に関して管理している医療情報等や匿名加工医療情報を送信等するに当たっては、２人以上の担当者による相互確認を行う等の措置を講じる

安全管理措置
（法８条３項３・４号・規則６条）

物理的安全管理措置
（３号）

○他の施設設備との区分
・上記で特定した区域を壁で区切ったり、施錠可能な扉等を設ける

難

○立入・機器持込制限、常時監視装置
・入退室管理として、ＩＣカード、指紋認証、静脈認証等による管理システムを設置し、生体認証を含む２以上の認証手法を組み込む
・施設設備の内部をカメラで常時監視置
・機器（カメラ、スマートフォン、携帯電話等）の持込み・持出しの記録（入退室管理簿の整備等）等
・権限を有しない者によるアクセス・閲覧の防止（入退室管理、座席配置の工夫、のぞき込みを防止する措置の実施等）
・基幹系システムを管理する区域と事務を実施する区域とが物理的に離れている等、両区域間の機器を電気通信回線を用いて接続する場合は専用線を用いる
・匿名加工医療情報を利活用者に閲覧させる場合は、閲覧させる区域も上記の区域として指定して安全管理措置を講じるとともに、閲覧に際しては大臣認定事業者等の従業者が立ち会う 。

○端末装置への記録機能の制限
難

・シンクライアント端末を用いて、端末に医療情報を残さず接続終了時にすべて削除する
・作業中はパスワード付きスクリーンセーバー等の起動を徹底
・持ち出し防止のため、ワイヤーでの固定等
・可搬記録媒体への記録機能を有する端末を用いる場合には、CD-R、USBメモリ等の外部記録媒体の接続を制限・管理

○復元不可能な削除・廃棄
・削除・廃棄記録の保存も必要

安全管理措置
（法８条３項３・４号・規則６条）

技術的安全管理措置 （４号）	○不正アクセスの防止 ・認定事業に関して管理している医療情報等や匿名加工医療情報へのアクセス権限付与者及びその者に付与する権限の限定 （例）アクセス権限を必要最小限の者に付与する、付与したアクセス権限自体も読取可能、修正等可能、削除可能などレベル分けして限定する等 ・基幹系システムに導入したアクセス制御機能の有効性の検証（例）ＯＳ・ウェブアプリケーションの脆弱性有無の検証 ・ユーザＩＤ、パスワード、ワンタイムパスワード、ＩＣカード等による識別・認証 （例）ICカードとワンタイムパスワードで識別・認証する （注意）取扱者を個別に識別できるように、ユーザＩＤ等を付与する。共有IDなどは不可。 （注意）ユーザＩＤと全く同じパスワードの禁止、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したＩＤを停止する等の対策を講ずる等 ・基幹系システムを管理する区域、及び認定事業医療情報等を取り扱う事務を実施する区域間は、専用線を用いる ・ウイルス対策ソフトウェアの導入及び当該ソフトウェアの有効性・安定性の確認 （例）パターンファイルや修正ソフトウェアの更新の確認 ・端末及びサーバ等のＯＳ、ミドルウェア（ＤＢＭＳ等）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆるセキュリティパッチ）の適用

安全管理措置（法８条３項３・４号・規則６条）

技術的安全管理措置
（４号）

○動作記録・異常検知・異常制御
- 基幹系システム及び外部との接続のあるシステム（一次受信サーバ及び出口サーバ）の利用状況（ログイン実績、アクセスログ等）の保管及び定期的な監視
- 認定事業医療情報等へのアクセス状況（操作内容も含む。）の監視　難
- 採取したログの改ざん・不正消去防止措置
- 侵入検知システム・侵入防御システム等による基幹系システム及び外部との接続のあるシステム（一次受信サーバ及び出口サーバ）への外部からのアクセス状況の監視
- 機器・装置の異常動作時における対処・制御措置

○使用目的に反する動作をさせる機能の不存在確認
- 電子計算機、端末装置等の調達履歴の管理
- 基幹系システム管理区域、及び認定事業医療情報等事務を実施する区域における通信監視の徹底
- できれば、意図しない変更の不存在を担保できる製造事業者による機器等を用いる

○専用線（仮想専用線も可）
- ＩＰ－ＶＰＮサービス、広域イーサネット、又は政府推奨暗号を用いた暗号化を併用した高度なインターネットＶＰＮ

○医療情報の一次受信サーバは外部送信不可

○匿名加工医療情報の送信サーバは、外部受信不可

○医療情報の受信サーバ、匿名加工医療情報の送信サーバ、医療情報の管理サーバは別サーバにし、一方向通信で専用線を用いる

○暗号化等

安全管理措置
（法８条３項３・４号・規則６条）

その他の措置
（５号）

〇漏えい等の際の被害補償のための措置
〇施設設備の障害発生防止、障害検知・対策のための
　事業継続計画の策定、予備機器設置等
〇医療情報取扱事業者による医療情報の提供方法・安全管理措置が
　適正である旨の確認
〇匿名加工医療情報の利用態様・安全管理措置が適正であることを
　匿名加工医療情報の提供契約において確保

＜契約＞
・提供する匿名加工医療情報の利用目的、利用態様、利用範囲等の利用条件を明確化する
・匿名加工医療情報であることを明示する
・匿名加工医療情報取扱事業者において安全管理措置を適切に講じる
・大臣認定事業者が匿名加工医療情報取扱事業者に対して契約遵守状況を確認すること
・匿名加工医療情報取扱事業者が他の匿名加工医療情報取扱事業者に匿名加工医療情報を提供する場合は、利用条件を含め事前に大臣認定事業者の許可を得るとともに契約を締結すること
・利活用条件に反する匿名加工医療情報の取扱いを行った場合は契約違反であり、かつ利用停止・公表等の制裁措置の対象になること

＜匿名加工医療情報取扱事業者から匿名加工医療情報の提供を受けた他の匿名加工医療情報取扱事業者へ＞
・利用条件等を踏まえて問題ないかどうかの許可を行い契約を締結
・帳簿（次世代医療基盤法１３条）に、すべての提供先（他の匿名加工医療情報取扱事業者も含む）の名称を記載

大臣認定の取消（法１５条）

大臣認定は以下の場合に、取り消されることがある（法１５条１項各号）

・偽りその他不正手段により認定・認可を受けた場合
・認定要件（欠格事由・加工等の能力・安全管理措置）を満たさなくなった場合
・変更認定を不当に受けなかった場合
・次世代医療基盤法に反して医療情報を提供した場合
・大臣命令に違反した場合

認定医療情報等取扱受託者の大臣認定取消について、認定匿名加工医療情報作成事業者との違いは次の通り。

・認定要件に加工等の能力が含まれないことから、これを満たさなくなった場合における取消がない

・医療情報の提供制限について、他の認定匿名加工医療情報作成事業者への提供については、認定医療情報等取扱受託事業者はできない（２９条における２６条１項の読み替え）

・大臣命令を発出できる場合の差異（再委託制限違反が追加、委託制限違反が削除、他の認定匿名加工医療情報作成事業者への提供制限違反が削除、医療情報の取得制限違反の削除）

マイナンバー

マイナンバー制度導入後のロードマップ（案）

H30.7月現在

2015年（H27年）(10月) / 2016年（H28年） / 2017年（H29年） / 2018年（H30年） / 2019年（H31年） / 2020年（H32年） / 2021年..2023年（H33年）（H35年）

マイナンバー

マイナンバーの通知

【１月から順次】
・マイナンバーの利用開始
（社会保障・税・災害対策分野）

▼【11月13日から】
・情報連携の本格運用を順次開始

▼【１月から】
・預貯金口座への付番開始

【2019年通常国会に向けて検討】
・戸籍事務、旅券事務、在外邦人管理業務、証券分野などの公共性の高い業務、罹災証明事務

▼【通常国会】
・マイナンバー法改正案の国会提出

法改正を踏まえたシステム整備等

▼【2023年度】
・戸籍情報の情報連携開始

マイナンバーカード

交付申請受付開始

【１月から】交付開始

▼【９月から】マイキープラットホーム等運用開始
・地方公共団体発行の各種カードの一元化（図書館カード等）
・自治体ポイントの管理

▼【11月から】旧氏併記の開始

▼【2019年度末】
・コンビニ交付サービス導入市町村の人口１億人

【１月から順次】
・公的個人認証・ICチップの民間開放、地方公共団体による独自利用

▼【2018年度末】
・国家公務員身分証一体化（本省分）の原則移行完了

【2019年通常国会に向けて検討】
公的個人認証等の利便性向上に係る必要な法制上の措置
・利用者証明用電子証明書のスマートフォン搭載
・利用者証明用電子証明書のPIN入力不要化

【2019年度中国会に向けて検討】
・海外転出後のマイナンバーカードにおける公的個人認証サービスの継続利用

▼【通常国会】
・関連法案の国会提出

【2020年度からの本格運用に向けて検討】
・医療保険のオンライン資格確認システム整備等

▼【2020年度から】
・健康保険証としての本格運用開始

マイナポータル

マイナポータルの構築

【１月から】
・アカウント開設開始

▼【11月13日から】本格運用開始

▼【７月から】
・子育てワンストップサービスのサービス検索を開始

▼【10月から】
・子育てワンストップサービスの電子申請開始

▼【2018年度から順次】
・就労証明書の電子化、障害児施策へのワンストップサービスの拡充の検討
・介護ワンストップサービスの検討、順次運用開始

▼【2018年度内】
・死亡・相続、引越等の手続のワンストップ化検討

▼【2019年度から】
・API提供開始

▼【2019年度から段階的】
・民間が発行する各種証明書データとの連携

▼【2019年度内】
・法人設立登記後手続のワンストップ化

▼【2020年度内】
・法人設立全手続のワンストップ化

▼【2020年度から順次】
・ライフイベントに伴う企業が行う従業員の社会保険・税手続のワンストップ化

※本ロードマップは「経済財政運営と改革の基本方針2018」、「未来投資戦略2018」、「世界最先端IT国家創造宣言・官民データ活用推進基本計画」等を元に内閣官房において作成。

課題：企業にメリットがない

課題	**マイナンバーの収集・保管だけさせられて、企業には特にメリットがない**
改善方法	マイナンバー導入による企業へのメリットを出していく • 煩雑な行政手続の簡易・迅速化　（eLTAXなど） • 一方的な取扱義務ではなく、企業がマイナンバーの保護を行うことを大前提に利活用できるように • 企業のニーズがもしあれば、金融機関における名寄せや企業における従業者名寄せに利用できるようにしてもよいのでは（特定個人情報の提供制限を厳格に維持すれば悪用のリスクも抑えられるのでは？ただ、従業者管理をグループ会社に一括委託している企業もある。グループ会社への提供は番号法１９条２号で解釈できる？） マイナンバーの保護措置の緩和・軽減も検討要 • マイナンバー＝危険というわけではない • 本人確認が過負荷 →企業（官以外の関係事務実施者）での本人確認はもっと簡素化してよいのでは • 企業は記録の残る書留等でマイナンバーを授受 ⇔ 自治体から特別徴収義務者への通知は「普通郵便」可 企業にだけお金のかかる方法？個人情報保護委員会ガイドラインと総務省の齟齬？ マイナンバー収集負荷軽減のためなら、制度導入直後に特別徴収義務者へ通知すべきだったか

課題：企業にメリットがない

マイナンバーの民間活用例

- **保険金を受け取り忘れない機能**
  - 親が子供に伝えずに生命保険に加入していたような場合、保険金の受け取り忘れがありうる
  - 被保険者が死亡したら、役所に届け出が行くので、役所と保険会社でマイナンバーで連携して、被保険者が死亡したことを保険会社が知って、保険金受取人の最新住所に保険金受取の連絡をしてはどうか

- **預貯金を忘れてしまわない機能**
  - 少額を入れた預貯金口座の存在を忘れ、自分のせっかく貯めたお金を無駄にしてしまうケースがある。また親が子供に伝えずにいた預貯金口座があると、相続できない。相続人が銀行に開示を求めても、口座開設当時の住所がわからないと口座情報を教えてくれなかったりするが、子供が生まれる前の住所など、子供ではわからないこともある。被相続人の財産を確定するのに労力がかかるのは大変。マイナンバーで被相続人財産が確定できれば、相続財産額の争いも減るのではないか。
  - マイナンバーを銀行・証券会社に届け出れば、自分や被相続人の口座情報を教えてくれる制度を作ってはどうか（お知らせが郵送だと銀行側が大変ならマイナポータルの活用も）

デジタル・ガバメント

デジタルファースト、GOVTECH

デジタルファースト法案／デジタル手続法案

２０１９年３月１５日通常国会に法案提出

情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律案

デジタルファースト

- 原則オンライン
- サービスデザイン思考

コネクテッド・ワンストップ

- 一回で手続完了
- 民間ともつながる
- 書式・様式の統一

ワンスオンリー

- 重複の排除

スマホやコンビニで
お役所手続ができるよ

何度も同じ手続を
しないでも良いよ
例）住所変更

デジタル・ガバメント推進方針

すぐ使える 簡単便利な 行政サービス	サービスデザイン思考 サービスを利用する際の利用者の一連の行動に着目し、サービス全体を設計
	UX：ユーザーエクスペリエンス 利用者の心理や行動等を含めた体験全体を最良に
	デジタル化の障壁の分析・改善 書面による提出、対面原則、押印等の障壁は何か
	BCR
	情報発信の多様化 Webサイトへの画一的な情報掲載から、プッシュ型、民間サービスとの融合等も
官民協働 プラットフォーム	オープンデータ　API　規格整備・標準化 マイナンバー　公的個人認証 クラウド　リモートアクセス　テレワーク

平成29年５月30日付け　https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20170530/suisinhosin.pdf

デジタルファースト法案／デジタル手続法案

- 新法ではなくオン化法（行政手続等における情報通信の技術の利用に関する法律）改正。
- 実際上、「デジタルファースト」を実効的に推進していく具体方策の規定はない？
  - 行政手続のオンライン化を原則実施と資料でいっていても、法律上は原則デジタルとは書かれていない？　自治体は努力義務。　結局進まない？
  - 本人確認や手数料納付をオンライン化といっても、「できる」規定？　進まないのでは？
  - 添付書類削減といっても、「できる」規定？　進まないのでは？
- 個別措置は以下の通り
  - 住基法改正
    - 国外転出者の本人確認情報の公証（戸籍の附票の記載事項の追加・記載された本人確認情報の保存・提供）
    - 本人確認情報の長期かつ確実な保存及び公証（住民票等の除票を除票簿として保存・安全確保措置等）
    - 本人確認情報の提供を受けることができる事務の追加（酒類製造免許に関する事務等を追加）
  - マイナンバー法改正
    - 災証明書の交付事務等の個人番号利用事務への追加
    - 社会保障分野の事務の処理のために、情報連携の対象の事務や情報を追加
  - マイナンバーカード／公的個人認証の利用拡大
- 資料
  - 法案　http://www.cas.go.jp/jp/houan/190315/siryou3.pdf
  - 新旧　http://www.cas.go.jp/jp/houan/190315/siryou4.pdf
  - 概要説明　https://www.cas.go.jp/jp/houan/190315/siryou1.pdf
  - 水町　条文解説　https://cyberlawissues.hatenablog.com/entry/2019/04/03/130426

行政デジタル化の課題

- 総論大賛成だが実装困難？
  - 　総論としては素晴らしい、こうあるべき
  - 　総論から実装へ結びつかない。国民のニーズ・窓口現場の対応・窓口処理・バックオフィス処理・公務員のデジタルアレルギー（対面確認・押印なしで良いのかという不安も）を具体的に分析して、実装へと結び付けていかないといけないが、霞が関ではほぼ窓口現場がなく、大上段の総論のみ対応し、実装は窓口現場や自治体に丸投げの危険性。
  - 　全手続にデジタル化義務を課しても、使われない手続もある。利便性が抜本的に上がる手続を選抜すべき。例えば、国民がよく利用する手続（一生で２～３度の手続がスマホでできても、あまりうれしくない）、紙だと面倒くさい手続（現況届など、毎年同じようなことを何度も繰り返し書かされるもの）、官民ともにメリットがでる手続（法人登記、資格確認、住民票などがデジタル可になれば、さまざまな手続が便利になる。インフラ的なものから投資すべきでは）などを重点的に取り組んでは？
  - 霞が関の窓口現場として、国税庁、年金機構、ハローワーク、特許庁がある。国税は既にデジタル化？（eTax, 申告書作成コーナー, KSK）特許庁も既にデジタル化。士業を主なカウンターパートとする窓口は、デジタル化しやすい傾向も
  - 　使いづらいオンライン化だと、利用率低調なうえに、構築・運用コストがもったいない。しかし使いやすくするためには、ユーザエクスペリエンス向上等が必要で、いわゆるお役所仕事ではない民間スキルの投入が必要。ここを徹底できるか。利用率低調については、以前のIT戦略本部でも既に総括したのでは？先祖返り？
  - 　マイナンバーの情報連携も低調な中、ワンスオンリーやワンストップができるのか。役所では、ネットで申請を受けた場合、それを役所で紙に印刷して、ITシステムに入力する処理をしているところも。この現状を打破できる力をもった、強力なマネジメントが必要。総論のみ提示し実装を丸投げするのではなく、実装に向けた力強いサポートこそが必要ではないか。
  - 　霞が関や自治体では、ITスキルがこれまであまり重視されてこなかった。しかし、IT知識なしに、政策立案が困難な時代に（ITが関係しない政策が珍しい時代）。IT人材育成が急務。お役所の省庁間調整スキルだけでは、デジタル・ガバメントは困難。

行政デジタル化の課題

- 抜本的解決が必要？
  - 小売店はリアル店舗からネットショッピングへ。反対にネットショップがリアル店舗出店も。デジタルとリアルの融合が当たり前の時代。銀行でも、窓口からATMへ、オンラインバンキングへの変化が。官に求められるデジタル化とは何か。
  - そもそも、官民の切り分けが、時代にそぐわないのでは？
    通常のBPRよりももっと高次のレベルでの公的業務の刷新が必要ではないか
  - 例）霞が関で単純作業に費やす時間が多く、政策の検討・実装に向けたサポートができにくい（書類の印刷、各署へ届け出る、会議体の日程調整、会議体の議事録作成、会議体の座席セッティング、手続書類作成などロジ業務が多い）
  - 例）自治体業務の多くに民間スキルが活用されている（委託・指定管理者制度等）。かつての市役所窓口のイメージと違い、窓口業務は民間が実際に回している場合も。保育園・高齢者施設・公民館・公園も民間が管理（指定管理者・助成等）。では、自治体の固有の業務、自治体の本業、自治体がやるべきことは何なのか。
  - 過去のIT総合戦略・決定が実行できているかの確認がなされていない？

個人情報リスク評価ＰＩＡ＋＋

個人情報を預かるも、効果が高く、リスク対策も講じていることを対外的にアピールする仕組み

個人情報リスク評価PIA++とは

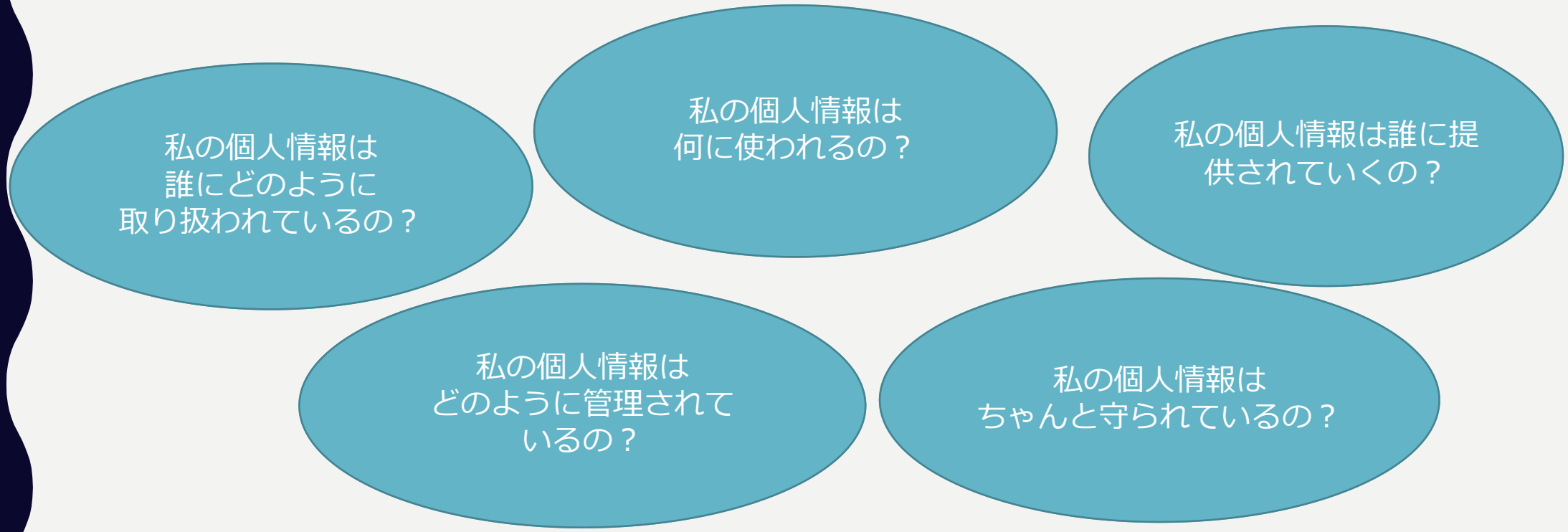
- 個人情報を活用するビジネスや仕組みに有用な取組み
- その仕組みがもたらすメリット、個人情報が必要な理由、個人情報保護対策を体系的に説明できる
- 諸外国でも取り入れられている仕組みで国際的アピール力もある

- 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。透明性のある企業経営・行政運営等に資する。
- 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、韓国その他さまざまな国で実施されているPIA（Privacy Impact Assessment）を参考
- 日本で行われている特定個人情報保護評価を基に、消費者にも企業にも行政にも役立つPIAを目指して水町が再構築したもの（簡易的に個人情報リスク評価PIA++と表記する場合もある）。
- 行政機関、医療機関、民間企業などさまざまなアクターの経営診断等に適用可能

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



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

意義（実施側にとって）

コミュニケーション手段としての側面も強い	
対・従業員	個人情報・プライバシーの重要性 業務上の注意点
対・顧客	信頼の獲得
対・ 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？

PIA / DPIAの実施例（民間サービス）

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

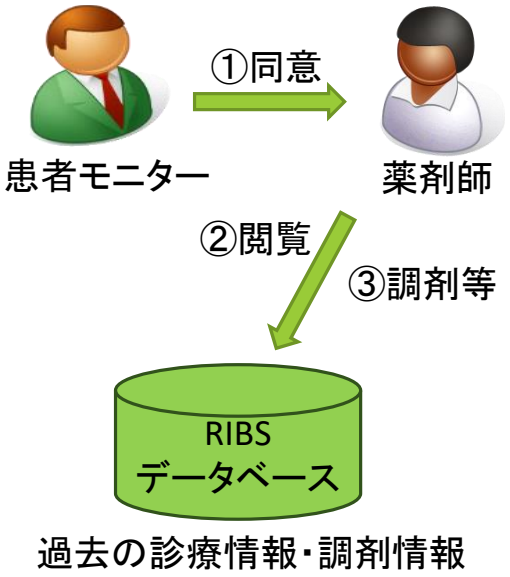
１　本評価の範囲・対象

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。

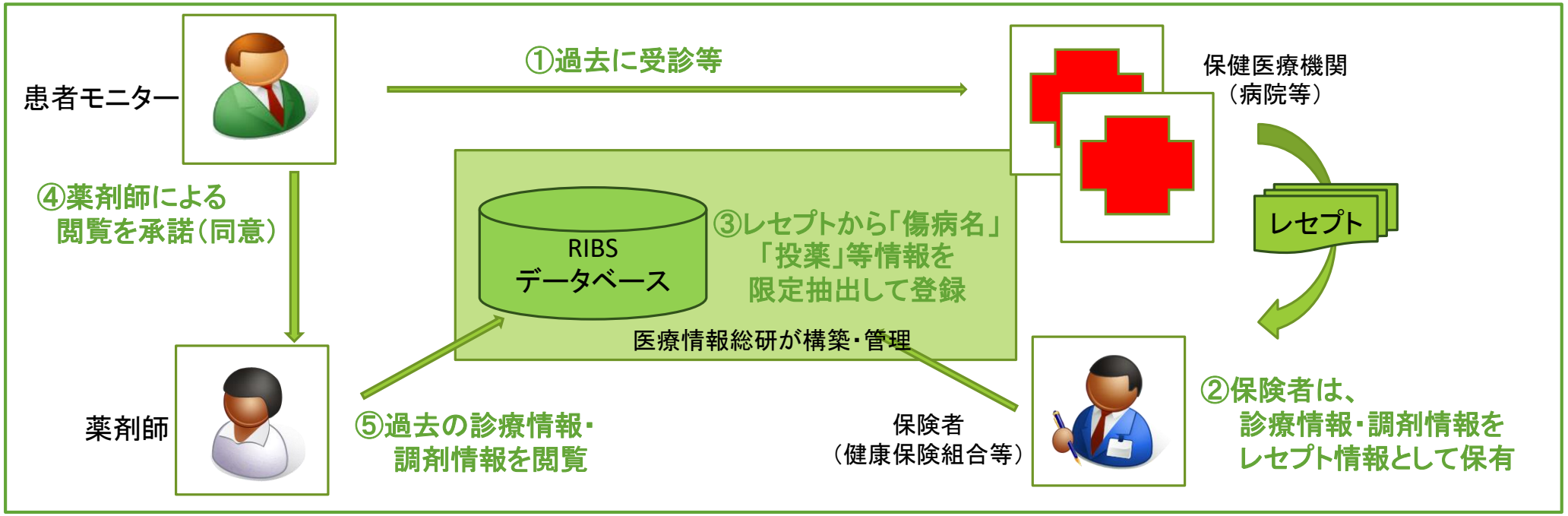
■ 診療情報を薬剤師に閲覧させるかどうかは、**その都度決めることができます**。
今回は閲覧させるが、次回は閲覧させないといった選択も可能です。

■ 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。

PIA / DPIAの実施例（自治体サービス）

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

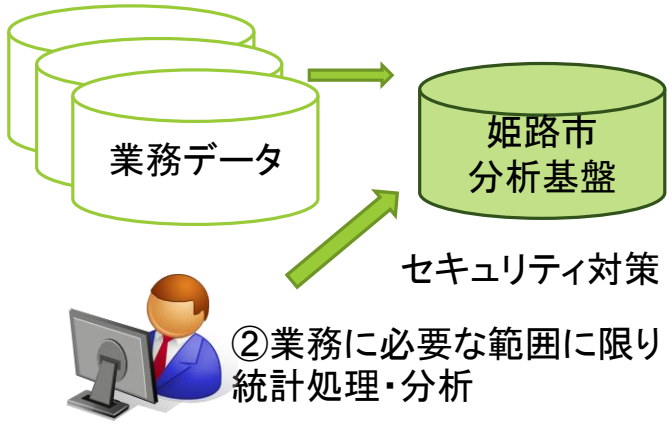
姫路市行政情報分析基盤

- 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

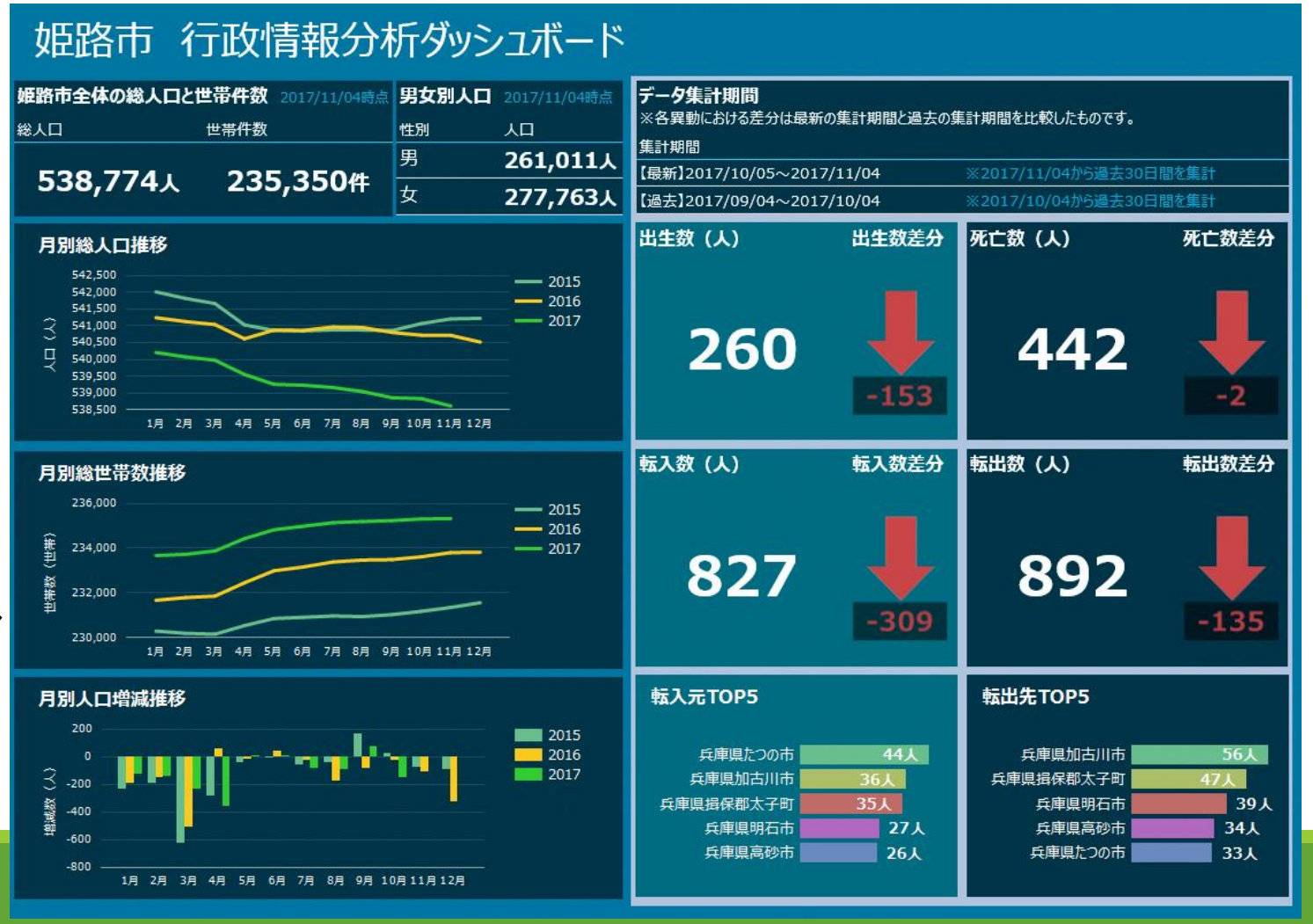
④ 分析・統計作成作業は、地方公務員法上、守秘義務を負う市職員が行います。守秘義務違反等には刑罰や懲戒処分を科せます。

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%

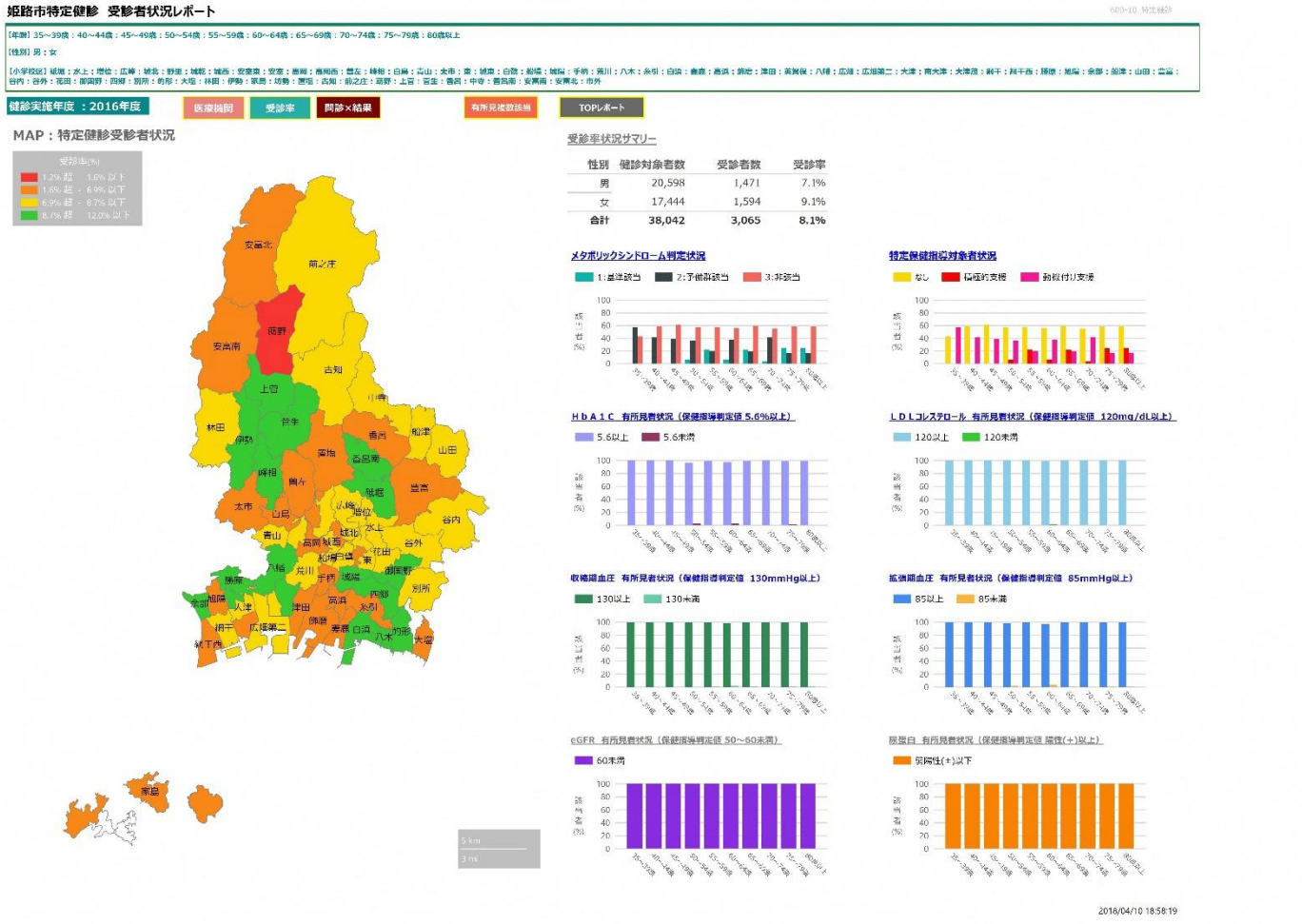
◆地域ブロック別

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	飾西市役所		0.00%	71	100.00%		0.00%		0.00%		0.00%		0.00%	71
	鶴居出張所		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

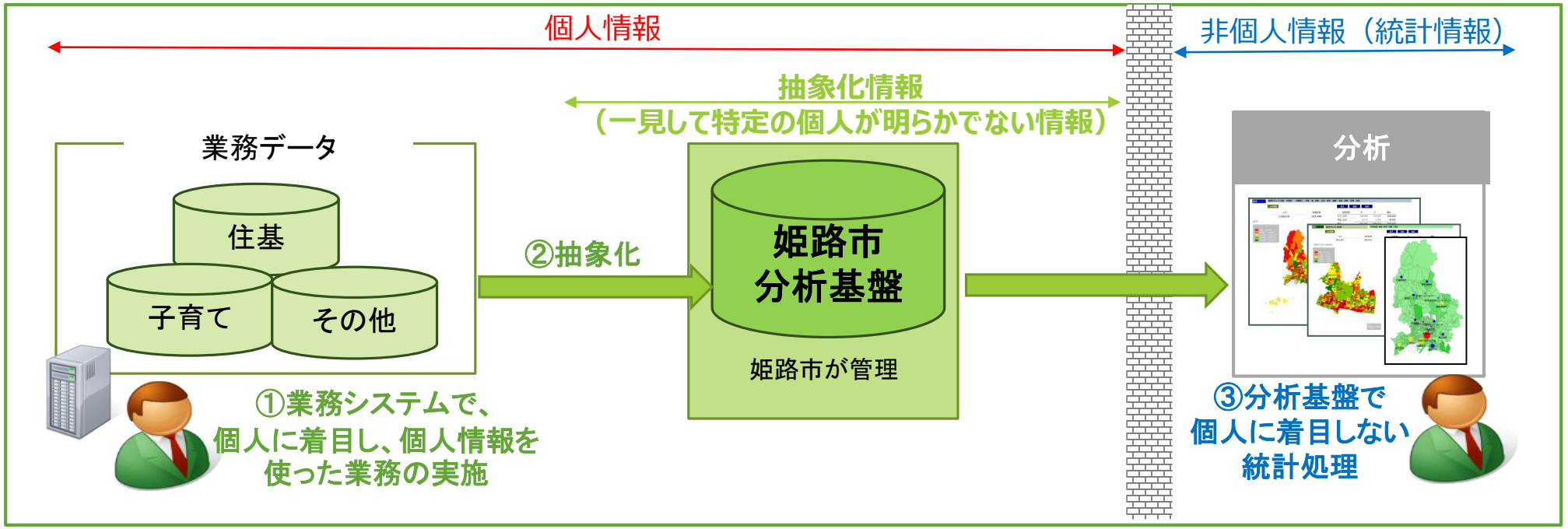
業務改善・効率化

- 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

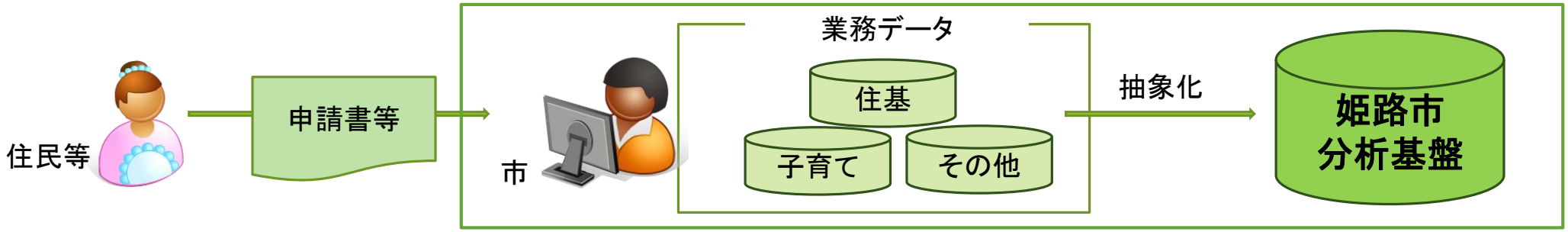


① 市では、行政サービス・業務を実施するために、住基情報、子育て情報その他の業務データ（個人情報を含む）を収集・利用・保管等しています。市職員は原則として自分の担当業務に必要な個人情報のみを取り扱っています。

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。

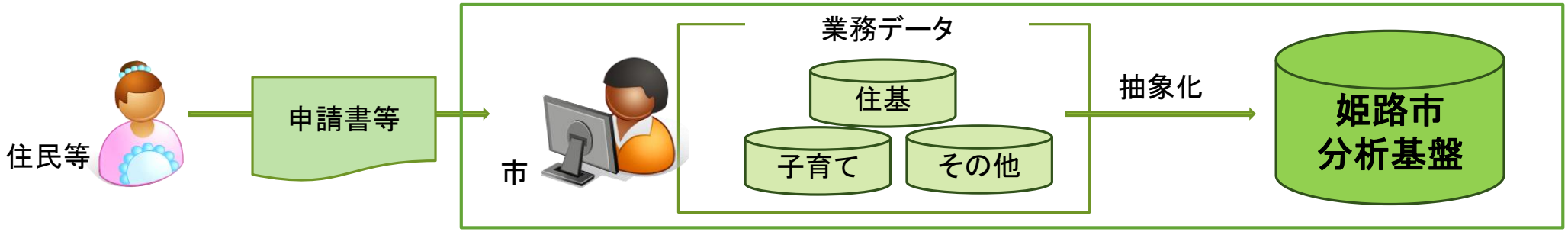
５　姫路市分析基盤で個人情報をどう取り扱うか



◆ **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



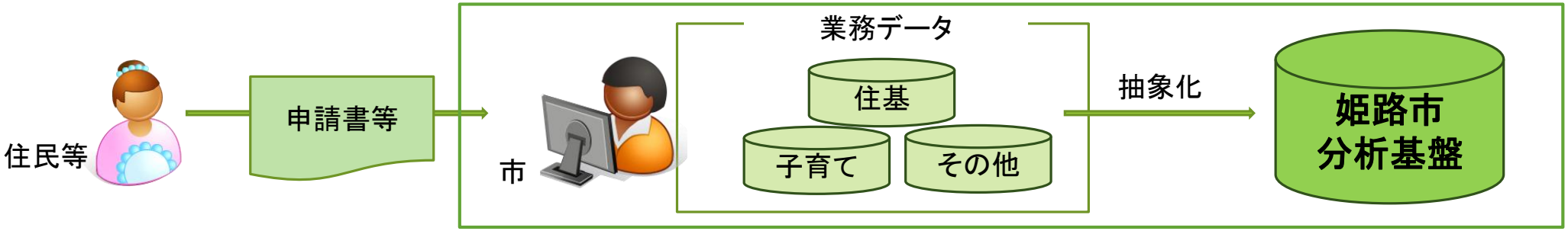
◆ どんな個人情報：

- 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。

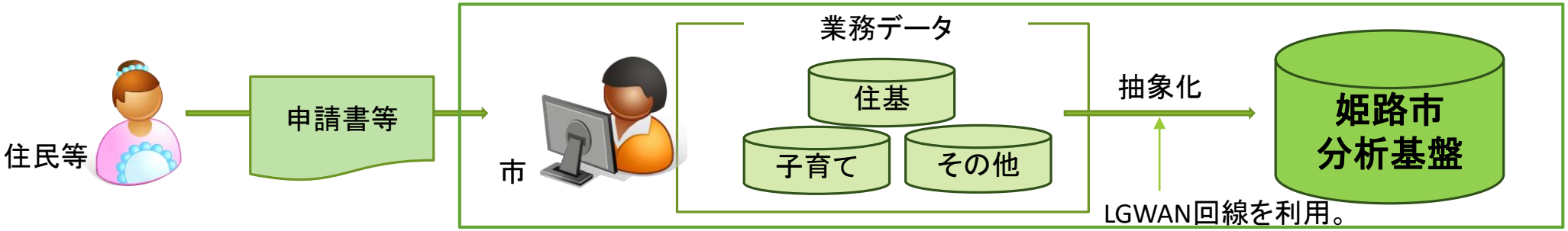
◆ **個人情報の取得経路：**

- 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。

22　参考

- 本評価書は、**総務省「地方公共団体におけるデータ利活用ガイドブックVer. 1.0」**別添資料2（150ページ～165ページ）と同一のものです。参照容易性を考え、PIA評価書のみ、本PDFに切り出したものです。

  総務省「地方公共団体におけるデータ利活用ガイドブックVer. 1.0」
  http://www.soumu.go.jp/main_content/000551807.pdf

- 本評価書と特定個人情報保護評価書との対照関係は、以下をご覧ください。
  http://www.miyauchi-law.com/f/180628PIAtaishou.pdf

- 本評価書は自治体における個人情報取扱いに対するPIAですが、PIAは民間企業においても実施が推奨されるものです。**民間企業における個人情報取扱いに対するPIA**については、以下の実例があります。
  http://www.miyauchi-law.com/f/180327PIA.pdf
  のうちの9～32ページ

参考資料

- 次世代医療基盤法
  - 水町作成資料　http://www.miyauchi-law.com/f/170828iryobigdata.pdf
- マイナンバー課題
  - 水町作成資料　http://www.miyauchi-law.com/f/171115mynumber_kadai.pdf
- オープンデータ
  - 東京都　http://opendata-portal.metro.tokyo.jp/www/index.html
  - 総務省　http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/index.html
- 非識別加工情報
  - 水町作成資料　http://www.miyauchi-law.com/f/170926hishikibetsu.pdf
- PIA
  - 日経XTECH　https://cyberlawissues.hatenablog.com/entry/2018/11/30/111317
- 自治体におけるプライバシーと情報管理～一般的な個人情報保護条例の理解～
  - 水町作成資料　http://www.miyauchi-law.com/f/180123jichitai_hogo.pdf

IT / ICT、情報法、PIAに関するお問い合わせ、ご相談がありましたら、
お気軽にどうぞ

http://www.miyauchi-law.com

宮内・水町IT法律事務所
弁護士　水町　雅子
電話　→　03-5761-4600
メール→　osg@miyauchi-law.com