

2018/3 弁護士 水町 雅子

個人情報リスク評価PIA⁺⁺

～プライバシー影響評価（PIA）の積極的活用～



1. 個人情報リスク評価PIA⁺⁺ / プライバシー影響評価 とは何か

個人情報リスク評価PIA⁺⁺／プライバシー影響評価とは

- 個人情報を活用するビジネスや仕組みに有用な取り組み
- 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

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

私の個人情報は
誰にどのように
取り扱われているの？

私の個人情報は
何に使われるの？

私の個人情報は誰に提
供されていくの？

私の個人情報は
どのように管理されて
いるの？

私の個人情報は
ちゃんと守られているの？

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）

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？



2. 実施例

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

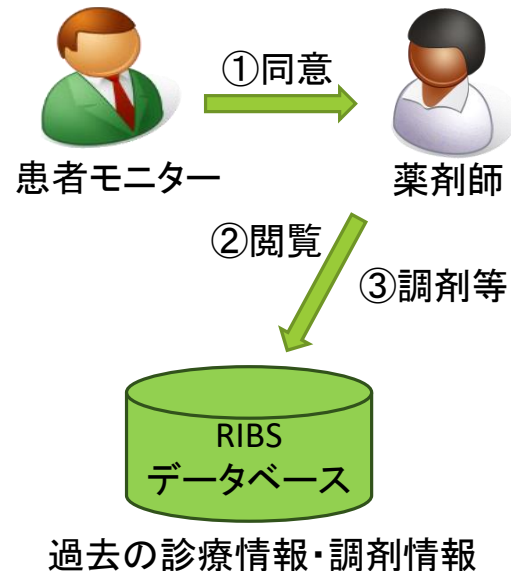
1 本評価の範囲・対象

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

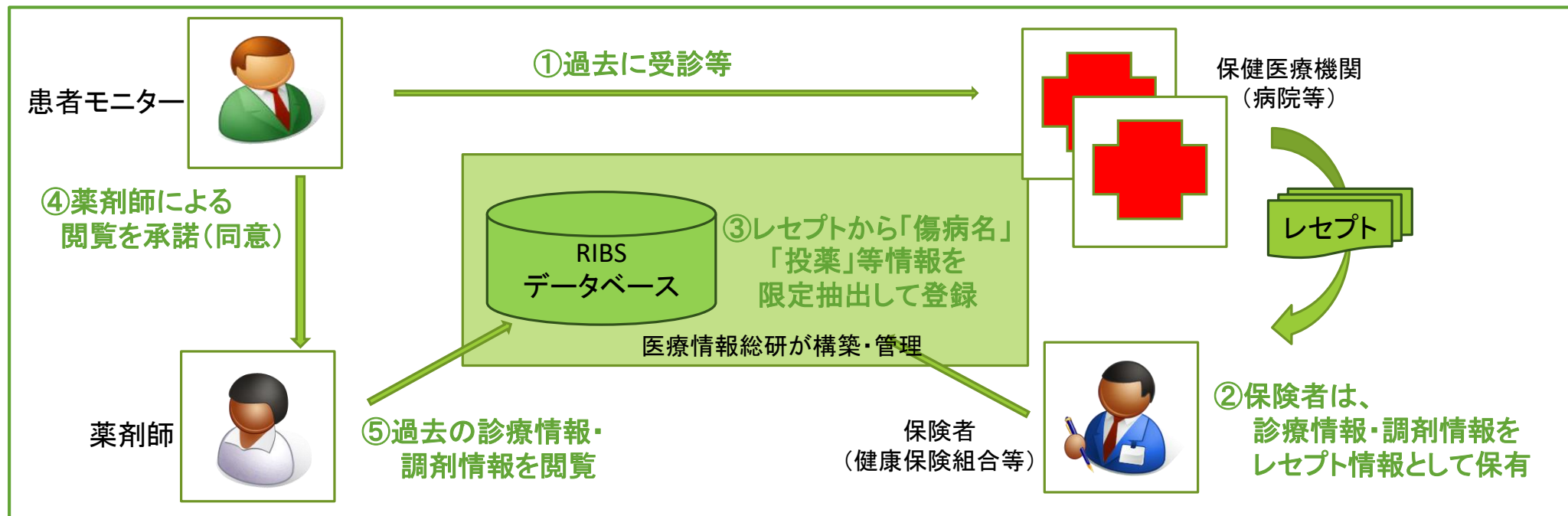


- 患者モニターが『診療情報提供カード』を提示することが、過去の診療情報・調剤情報を薬剤師が閲覧することへの同意になります。
- 診療情報を薬剤師に閲覧させるかどうかは、その都度決めることができます。今回は閲覧させるが、次回は閲覧させないといった選択も可能です。
- 患者モニターになることを同意した場合でも、診療情報提供カードを提示しない（＝「診療情報を開示しない」という意思表示をする）ことができます。

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によって、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

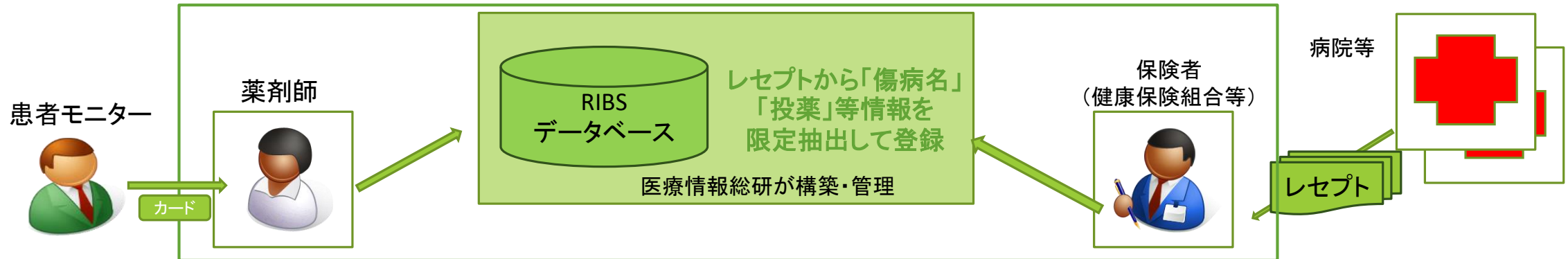
患者利便の向上

- 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

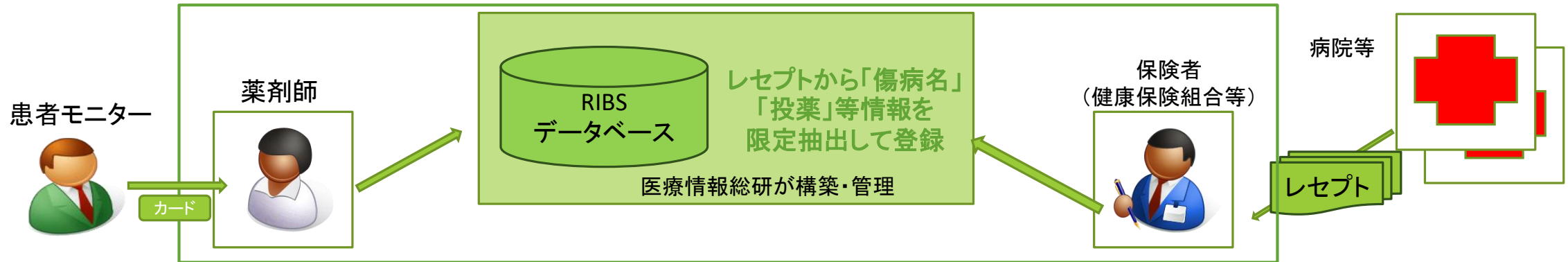
- 重複投与の防止により残薬の発生を抑制
- 過去の投薬履歴を閲覧することで、患者に対してジェネリック医薬品に関する適切な説明／推奨が可能に
- 重複検査の抑制も期待

5 RIBSで個人情報はどう取り扱うか



- 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で個人情報はどう扱うか



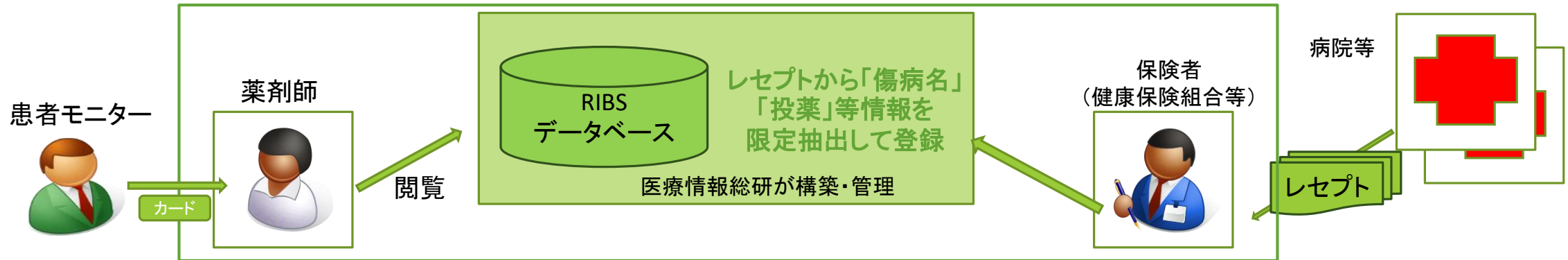
■ 情報の取得

- 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。

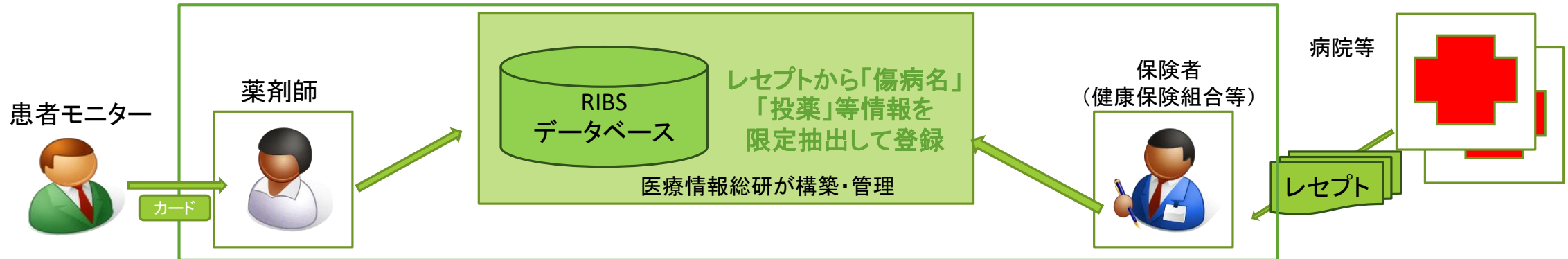
5 RIBSで個人情報はどう扱うか



■ 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で個人情報はどう扱うか



■ 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

氏名 ケンコウ タロウ

記号 234 番号

RIBS- 1234567

ID

利用可能期間 平成29年1月21日～平成29年3月17日

保険者番号 1234567

保険者名称 XXX健康保険組合

保険者所在地

連絡先

実証用



- 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ぬか 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力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取り扱いされないように、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承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承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

(個人情報管理に関して)

RIBSでは上記のほか、個人情報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する。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、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ます。
- 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。



3. 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）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
- ◆ お勧めは、**特定個人情報保護評価をカスタマイズする**

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

評価書案を作る

一般意見を
聴く

専門家意見を
聴く

確定版評価
書を公表

◆ 中心は、評価書

- ・ 「プライバシーポリシー」「わが社の取り組み」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



4. 評価書のポイント

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）官の評価書だと・・・重点項目評価書Ⅰ1②・全項目評価書Ⅰ1②別添1に

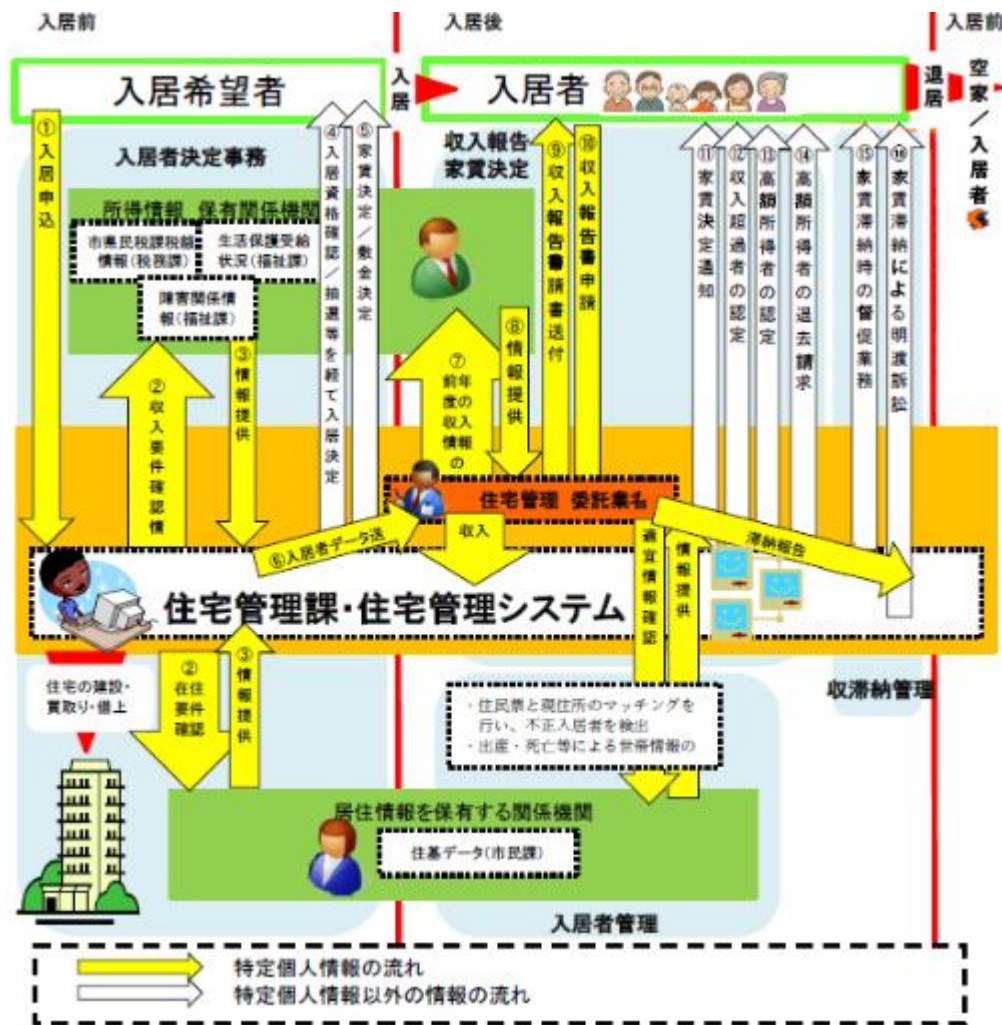
1. サービスの全体像をわかりやすく平易に説明しよう（例）

■ 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. 個人情報は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はどう取り扱うのか、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) 官の評価書だと・・・重点項目評価書Ⅱ 2③④3⑤・全項目評価書Ⅱ 2③④3⑧に記載

2. 個人情報は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. 個人情報は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
- 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
- 取違い（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な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： 外部提供ルールの特化、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： 個人情報に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： 個人情報に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： 個人情報に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

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/12zenkoumokuuyouryo.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>

■ 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>

