

個人情報保護に関する社内整備と データ利活用のポイント

弁護士 水町雅子

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

◆ 東京大学教養学部関連社会科学卒業

◆ 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

◆ 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、東京都都政改革アドバイザリー会議委員や、地方公共団体の情報公開・個人情報保護審査会委員等を務める。

マイナンバー・個人情報に関する著書・論文・講演・TV出演・新聞取材等多数。『1冊でわかる！個人情報保護法』（労務行政、2017年）

金融法務事情No.2046「改正個人情報保護法と金融機関の実務対応」、労政時報3915号「実務に役立つ法律講座（23）個人情報」

NBLNo.947「ライフログにおける法的問題」等多数



AGENDA

時代背景

- ・ 個人情報保護法の背景
- ・ 各種問題事例から見る個人情報保護への対応
 - ・ 他社で発生したトラブル事例から学ぶ

ルール

- ・ 個人情報保護法のルール
 - ・ 既存データをどのようにしたら利活用できるか
 - ・ 個人データを提供できる場合はどのような場合か
 - ・ 具体例・ルールの意味とともにルールを概観する

対象

- ・ 個人情報 / 要配慮個人情報 / プライバシー権とは何か
 - ・ 個人情報、個人データ、保有個人データ、要配慮個人情報、プライバシー権の共通点と相違点を理解する
 - ・ 技術的な定義よりも、様々な観点から様々なデータが保護されていることを理解する

利活用の 仕組み

- ・ 匿名加工情報とは、非識別加工情報とは
 - － どのような仕組みか
 - － 個人情報と比較してどのような利点があるのか
 - － 匿名加工情報と非識別加工情報の関係性・相違点
- ・ 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

PIA

- ・ 個人情報リスク評価PIA++概要
 - ・ どのようなものか、具体例



個人情報保護法・ データ利活用の背景

個人情報の保護と利活用、時代の背景を感じる

大量データ社会に伴う データ活用と個人情報保護の流れ

データ活用

技術発展・大量データ化により、
データ活用と個人情報保護の流れ
が双方とも急速に強まる

- 技術トレンド：AI、RPA、IoT、ロボット、ブロックチェーン等々
- データ活用：オープンデータ/非識別加工情報、機械学習の促進（著作権法改正、AI）、官民データ活用推進基本法
- 医療×ICT：EHR、PHR、次世代医療基盤法（医療ビッグデータ法）、医療等ID、全国保健医療ネットワーク
- 法律×ICT：裁判手続等のIT化、Online Dispute Resolution
- 役所×ICT：デジタルガバメント、EBPM、デジタルファースト法

個人情報保護

- マイナンバー法・個人情報保護法改正によるレギュレーション強化
- 海外法令の動向（GDPR、カリフォルニア州消費者プライバシー法（CCPA）等）では制裁金も高額
- サイバー攻撃を踏まえたセキュリティ意識の高まり
- 個人情報保護への国民意識の高まり
- 特殊詐欺電話、アポ電強盗等への警戒

個人情報保護をめぐる国の動向

個人情報保護法の経緯

- 平成15年に制定（平成17年全面施行）
- 平成27年に改正（平成29年5月30日に全面施行）
 - 個人情報大規模漏えい事件や国民感情の高まりを踏まえ、**規制強化**
 - ・ 要配慮個人情報というカテゴリを新設し、原則本人同意を要求
 - ・ 外国への個人データ提供を規制
 - ・ 個人データ授受のトレーサビリティ確保のための記録・確認義務新設
 - ・ 小規模事業者に対しても個人情報保護法を適用に
 - ・ 新たな罰則規定の新設
 - データ利活用を促進**するための仕組みも
 - ・ 匿名加工情報というカテゴリを新設し、簡易な手続での利活用・提供を可能に

外国法令の動向

- GDPR（General Data Protection Regulation：一般データ保護規則）
 - ・ 2016年4月に制定、2018年5月25日に施行
 - ・ 原則（適法性・公正性・透明性、目的の限定、データ最小化、正確性、保存制限、完全性・機密性、アカウントビリティ）
 - ・ 本人の権利保障
 - ・ 制裁金 2000万ユーロ以下又は世界全体における売上総額の4%以下
- ・ 米国カリフォルニア州消費者プライバシー法、ロシア改正個人データに関するロシア連邦法、中国サイバーセキュリティ法、豪プライバシー改正法、韓国改正個人情報保護法等

個人情報保護をめぐる国の動向

個人情報保護法は、現在、国で見直し議論中

- 平成27年個人情報保護法改正法では、情報通信技術の進展が著しいこと等から、施行後**3年ごと**の見直し規定が設けられた。
- 内閣府外局の**個人情報保護委員会**では、令和2年（平成29年施行から3年）に向けて、現在、個人情報保護法の検討を行っている。平成31年4月25日に「個人情報保護法いわゆる3年ごと見直しに係る検討の**中間整理**」を公表。

個人情報保護法委員会の中間整理上の主な検討事項

- **データ利活用**（匿名加工情報の周知、仮名化の検討、相談体制充実）
- デジタル化社会でも、個人情報をどのように使われるか本人が予測できるよう、情報提供のあり方の工夫
- **名簿屋対策**（失効徹底、情報入手先の開示、届出変更）
- 個人情報相談のAIチャットボット導入
- 個人情報**漏えい報告**（義務付け、軽微事案の届出不要措置等）
- **開示請求**（本人関与の保障、事業者側の適切な対応、電子開示）
- **利用停止請求**（消費者側からの根強い要望、実務上の論点）
- 認定個人情報保護団体活性化
- ターゲティング広告（クッキーを個人識別符号とする等）
- **外国事業者**への報告徴収・立入検査・命令
- PIA

公取による検討

米グーグルやアマゾンといった「**デジタル・プラットフォーム**」と呼ばれる企業による**個人情報の取扱い**について、**公正取引委員会**が独占禁止法違反に当たる不当なケース案を公表

<https://cyberlawissues.hatenablog.com/entry/2019/11/15/153754>

個人情報保護への国民意識

安心があってこそそのデータ利活用・個人情報への国民意識を重視

- 個人情報に対する不安感
- 詐欺・アポ電強盗や迷惑電話の端緒にも メールや郵送、電話などで詐欺・強盗・迷惑勧誘等も
- ダークウェブでは、ID/PWD、クレジットカード番号等もやりとり
- 便利なデジタル化時代の反面、自分の個人情報が誰にどのように渡るのか、何に使われるかがわかりづらい
- 個人情報漏えいのベネッセ事件では、損害賠償について下級審で判断分かれる

国に
寄せられた
国民からの
苦情・意見

- 提供関連：本人同意のない個人データの第三者提供への苦情、名簿の売買禁止を求める意見、名簿を購入した事業者に名簿の入手先の開示義務付けを求める意見、事業者が家族等への提供に応じない不満
 - 利用関連：個人情報の目的外利用に関する不満、事業者が個人情報を取得・利用する際に本人関与を求める意見
 - 安全管理関連：漏えいへの不満、ずさんな取扱いへの不満、漏えい報告義務化を求める意見、罰則強化の意見
 - 開示等：事業者が保有している情報を知る方法に関する質問、自分の個人情報を削除してほしいとの相談、勧誘拒否の相談
 - SNSにおけるリスクに関する意見
- 出典：個人情報保護委員会「個人情報保護法いわゆる3年ごとに見直しに係る検討の中間整理」

ベネッセ
事件

- 東京高裁令和元年6月28日
 - 一人当たり2000円の損害賠償を命じる
 - 氏名や住所、電話番号などの個人情報は思想信条や性的指向と比べると「みだりに開示されたくないとの性質が強いとは言えない」と指摘。その上で「漏洩の不快感、不安感が抽象的だったとしても、精神的苦痛は避けられない」
出典：日本経済新聞2019/6/28
- 東京地判平成30年6月20日
 - 損害賠償認めず
 - 氏名や住所などの情報が「思想信条や性的指向などの情報に比べ、他者にみだりに開示されたくない私的領域の情報という性格は低い」と判断
出典：日本経済新聞2018/6/20 8

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
- ◆ PC、スマホ、カード、ゲーム機などを利用すると、その履歴が残るとともに、通信

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
商品を購入したか

どの実店舗で
どんな商品
を購入したか

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

データ活用政策の加速化

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、さらに**官民双方で連携**していく方向へも**新法・法改正が毎年のように**行われている現状

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（民） ・ 匿名加工情報の導入 データ活用を促進するための仕組み
平成28年	官民データ活用推進基本法 （官・民） データ活用を促進するための法律 ・ 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・民） ・ 非識別加工情報の導入 官データを民間提供するための仕組み
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 医療データ活用を促進するための仕組み
平成30年	生産性向上特別措置法・産業競争力強化法等の一部を改正する法律（民） ・ 公的データ提供要請制度 （産業における競争力強化や社会課題解決に向けた利活用を促進するため、一定のデータの安全管理（セキュリティ）の確認を受けた上で、国の機関、独立行政法人等の保有するデータの提供を要請できる手続） 官データを民間提供するための仕組み
平成31年	デジタル手続法＝デジタルファースト法（官・民） ・ 行政手続のデジタル化、 デジタルガバメント 利便性向上・データ化へ移行

データ活用政策の加速化

法改正の予定は、今後も続く見込み

令和	元年	公正取引委員会によるデジタル・プラットフォーマー規制（案）（民）
令和	2 年	個人情報保護法改正予定（民） 公正取引委員会がCookie規制を検討中（民）
令和	3 年	地方公共団体のデータを民間が入手しやすくなる法律の制定検討中（官・民）

データ保護と活用の両立



- **個人情報保護 VS データ活用 ではダメ**
 - プライバシー権保護を軽視しては、**国民・消費者の理解**は得られない
 - かといって、個人情報保護は、個人情報を金庫にしまっておいて何にも使わないことを意味するものでもない
 - 個人情報保護法でも、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」が目的
- 国も「DFFT（**Data Free Flow with Trust**）」を掲げる
- データ保護・個人情報保護・プライバシー権保護が前提での、データ活用
- 個人情報保護とデータ活用の**両立**！



各種問題事例から見る 個人情報保護への対応

問題事例から、個人情報の取扱いのポイントを考える

個人情報に関する問題事例

従業員等が有名人の来店情報等をSNSに書き込んでしまった

- 有名ホテル、銀行、不動産等
- ネットで拡散されさらに批判が高まる
- 公式Webサイトで謝罪等の対応も

芸能人〇〇が来店
△と一緒にあったよ^^

芸能人〇〇に接客
かわいかった！

従業員等がSNS等に不適切な書き込み等をしまった

- 社外秘資料が写りこんだ写真を投稿
- 従業員等の家族がSNSに投稿
- 勤務時間中に社用パソコンから不適切な書き込み

個人情報に関する問題事例

タクシーが有名人のドライブレコーダー映像をTV局に提供

- 有名人が逮捕される直前の映像
- タクシー会社のグループ企業代表取締役社長が謝罪し、国土交通省も遺憾の意を表明した上で、映像の適切な管理の徹底について関係団体宛てに通知を発出

従業員等が個人情報を悪用

- 自治体職員が個人情報を不正閲覧しストーカー行為を行う
- 退職した従業員・委託先等が顧客名簿を売却

個人情報に関する問題事例

個人情報が漏えい

- 標的型攻撃等を受けて個人情報が漏えい Ex,日本年金機構
- 従業員等が個人情報の入ったパソコン・鞆等を置き忘れたり紛失する

パーソナルデータの取扱いについて国民の理解を得られなかった例

- 大阪駅での監視カメラ映像の解析（NICT）
- Suica
- リクナビ
- Yahoo!スコア などなど

個人情報をめぐる制裁

刑罰

行政制裁等

民事制裁

レピュテー
ションリスク

プライバシー
マーク

刑罰（個人情報をめぐる制裁）

個人情報保護法に基づく刑罰

◆ 不正提供・盗用

- ・ 業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したとき（個人情報保護法 8 3 条）

◆ 命令違反

- ・ 個人情報保護委員会による命令に違反したとき（個人情報保護法 8 4 条）

◆ 検査妨害等

- ・ 個人情報保護委員会等に報告若しくは資料の提出をせず、若しくは虚偽の報告をし、若しくは虚偽の資料を提出し、又は当該職員の質問に対して答弁をせず、若しくは虚偽の答弁をし、若しくは検査を拒み、妨げ、若しくは忌避したとき（個人情報保護法 8 5 条 1 号）

※個人情報の取得元や保有者等が地方公共団体や国立病院、独立行政法人等、行政機関の場合、個人情報保護条例や独立行政法人等個人情報保護法、行政機関個人情報保護法等に定められた刑罰が科される可能性がある

※また不正競争防止法や刑法等、個人情報保護法制とは別法で罰せられる可能性もある

刑罰（個人情報をめぐる制裁）

- ◆ 漏えいだけでは刑罰は科されないのが原則
 - ・ 漏えい等といっても、書類を電車やタクシーに置き忘れた、USBメモリを紛失した、メールを誤送信した場合でも、漏えい等に当たる可能性あり
 - ・ 刑罰は最終手段なので、謙抑性を有する
 - ・ もっとも、刑罰の話であって、行政制裁、民事制裁、消費者感情悪化等は別の話
- ◆ 漏えいで刑罰が科される場合
 - ・ 不正提供、盗用：例えばベネッセ事件のように関係者が個人情報を売却したなど
 - ・ 命令違反：個人情報保護委員会から改善命令を受けたのに従わないなど
 - ・ 検査妨害等：個人情報保護委員会による立入検査を妨害するなど
- ◆ 通常業務を行っていれば上記行為はありえないはず
- ◆ 対策
 - ・ 盗用等の不正行為が行われないような従業員教育・監督
 - ・ 退職者であっても刑罰の対象（退職したら個人情報にアクセスできないことを担保する技術的対策や運用ルール、誓約等の措置）

行政制裁等（個人情報をめぐる制裁）

個人情報保護法に基づく行政制裁等（広義を含む）

- ◆ 助言・指導（個人情報保護法 4 1 条）
- ◆ 勧告（個人情報保護法 4 2 条 1 項）
- ◆ 命令（個人情報保護法 4 2 条 2 ・ 3 項）
- ◆ 厳密な意味での行政制裁ではないが、立入検査・報告徴収（個人情報保護法 4 0 条 1 項）
- ◆ 過料
 - ・ 個人データの提供をする際に取得の経緯等を偽った場合（個人情報保護法 8 8 条 1 号）

※個人情報の取得元や保有者等が地方公共団体や国立病院、独立行政法人等、行政機関の場合、個人情報保護条例や独立行政法人等個人情報保護法、行政機関個人情報保護法等に定められた行政制裁等がなされる可能性がある

※このほか、事業所管官庁による行政制裁等がなされる可能性もあり（金融庁、厚生労働省など）

行政制裁等（個人情報をめぐる制裁）

- ◆ 不適切事案のレベル感によって、行政制裁等のレベルも変わってくる可能性
 - ・ 1 件のメール誤送信、1 枚の名刺を社内で紛失したという場合
 - ・ 大量の個人情報を漏えいしたり、従業員が悪用したという場合
 - ・ 個人情報の内容、量、態様、影響度合い、講じていた安全管理措置（個人情報保護法 20 条）の内容など
 - ・ 漏えいに限らず、不適切事案全般に対して行政制裁等
 - ・ 重い行政制裁は、事業廃止命令や業務停止命令、業務改善命令等（発出された事例あり）
 - ・ なお、不適切な行為がなくても、報告徴収・立入検査等がなされる可能性はある
- ◆ 対策
 - ・ 個人情報保護法上の義務を再確認
 - ・ 不適切な行為を防止するよう体制・規程・従業員監督・委託先監督その他の運用を徹底
 - ・ インシデント発生後は速やかに被害を最小限に抑える方策を取り、真摯に対応する

民事制裁（個人情報をめぐる制裁）

個人情報保護法に基づく民事制裁（広義を含む）

- ◆ 民事訴訟による損害賠償請求等
- ◆ 和解
- ◆ 自主的なお詫び
- ◆ 契約解除・入札禁止 などなど

民事制裁（個人情報をめぐる制裁）

要配慮個人情報（信条・犯罪）の流出

- ◆ 公安テロ情報流出被害国家賠償請求事件 東京地判平成26年1月15日判タ1420号268頁
- ◆ 結論：500万円の損害賠償を認める（1人のみ200万円）。なお、このほか1割の弁護士費用も賠償すべきとされている。
- ◆ 事案：インターネット上に公安情報と思われるデータが流出。国籍，出生地，氏名，性別，生年月日（年齢），現住所，勤務先及び使用車両、旅券番号、在留資格，本国住所，在留期間、我が国における住所歴及び通学・勤務先歴，「身体特徴」として，身長，体格，髪，ひげ，眼鏡の有無等，「家族交友関係」として，訴外人1名以外の者につき，その家族の氏名，生年月日，勤務先及び住所が記載され，また，一部の者については，「免許関係」として，保有する免許の種別，取得年月日及び免許番号，「犯罪情報」として，検挙年月日，罪名，検挙署及び処分結果が記載されているほか，「容疑」，「対応状況及び方針」，「所属団体」，「地位・役職・役割等」，「モスクへの立ち入り状況」，「立ち寄り徘徊先」，「行動パターン概要」という項目についての記載欄も設けられ，このうち「容疑」と「対応状況及び方針」については全員につき記載がされ，一部の者についてはその余の項目の記載もされた上で，顔写真が添付されたデータなどが含まれていた。特定のイスラム教徒との交友関係等が具体的かつ詳細に記載された書面もあった。
- ◆ 第三者が見れば，原告らがテロリスト若しくはその支援者であるか，又は少なくとも警察からその疑いをかけられているとの印象を抱くことは避け難い。
- ◆ 20を超える国と地域の1万台以上のパソコンにダウンロードされた

民事制裁（個人情報をめぐる制裁）

エステ顧客情報の流出

- ◆ 東京地判平成19年 2月 8日判タ 1262号270頁
- ◆ 結論：3万円の損害賠償を認める（1万7000円の場合も）。なお、このほか弁護士費用も賠償すべきとされている。
- ◆ 事案：エステサロンの顧客情報が流出
- ◆ 氏名，住所，電話番号及びメールアドレス，職業，年齢，性別，関心を有していたコース名，回答の内容等やそれらの情報が蔵置された電子ファイル名，被告が原告らを識別するために付した番号が流出？

地方公共団体 住民情報の流出

- ◆ 大阪高裁平成13年12月25日
- ◆ 結論：1万円の損害賠償を認める。なお、このほか弁護士費用も賠償すべきとされている。
- ◆ 事案：地方公共団体の再々委託先従業員が住民基本台帳のデータを不正にコピーしてこれを名簿販売業者に販売する等して、インターネット上でその購入を勧誘する広告が掲載された

個人情報漏えいに伴う民事裁判例の事例は意外と少ない

民事制裁等（個人情報をめぐる制裁）

- ◆ 不適切事案のレベル感によって、損害賠償額も変わってくる可能性
 - ・ 前述の損害賠償額は1人当たりなので、漏えい人数が多いと積算で高額になる
- ◆ 損害賠償以外にも多額の費用を要する可能性あり
 - ・ 事実調査・原因究明や再発防止策の検討・実装、会見等の実施、自主的なお詫び等
 - ・ ベネッセでは、2014年に260億円の特別損失を計上し、顧客への補償に200億円、おわび文書の発送や事件の調査、セキュリティ対策などに60億円を充てる旨の報道がなされている

https://www.nikkei.com/article/DGXLASGD3IHIG_R30CI4A7EA2000/
- ◆ 対策
 - ・ 不適切な行為を防止するよう体制・規程・従業者監督・委託先監督その他の運用を徹底
 - ・ 技術的対策も十分に行う
 - ・ インシデント発生後は速やかに被害を最小限に抑える方策を取り、真摯に対応する
 - ・ 保険加入等も検討？

レピュテーションリスク等

レピュテーションリスク等（広義を含む）

- ◆ 報道での批判
- ◆ SNS・電話等による批判
- ◆ 謝罪
 - ・ ASKA氏乗車のタクシー事案では、代表取締役社長名での謝罪
<https://news.livedoor.com/article/detail/12352797/>
- ◆ サービス変更
 - ・ Yahoo!スコア <https://www.itmedia.co.jp/news/articles/1909/09/news075.html>
- ◆ サービス廃止
 - ・ リクナビDMPフォロ https://job.rikunabi.com/2021/contents/article/edit~dmp_follow~index/u/?original=1
- ◆ 事業撤退
- ◆ 顧客減少
 - ・ ベネッセの通信講座「進研ゼミ」の会員数は、2012年4月まで400万人程度で推移していたが、個人情報漏えい事案後、2015年4月には271万人に、2016年4月には243万人まで減少したとも報道されている <https://business.nikkei.com/atcl/report/15/110879/051100341/?P=1>
- ◆ 消費者感情の悪化などなど

レピュテーションリスク等

- ◆ 個人情報保護法制上の義務を適正に履行する
- ◆ 個人情報保護法上仮に適法であったとしても、個人の感情から見て不適当な行為を厳に慎み、個人情報保護／プライバシー権保護を第一に考慮して事業を実施することが重要
 - ・ 個人情報保護法制は技巧的な部分も多い
 - ・ 細かい技術的な法規制を暗記したりこねくり回す必要はない
 - ・ 例えば、無理に「委託」構成、「共同利用」構成をとっても、違法・不適當
 - ・ 本人の立場に立って見たときに、素朴な感情として違和感・不快感を感じないか
 - ・ 消費者目線・相手方目線を忘れない
 - ・ 従業者も悪気なく個人情報保護の観点から不適切な行為を行うこともあるので、企業としてチェック・確認を徹底する
- ◆ 個人情報への国民意識の高まりを常に意識する
 - ・ 時代とともに国民意識も変化する
(以前は電話帳ハローページで個人自宅電話番号が公開されていたなど)
 - ・ 個人情報保護の相談を受ける当職でも、年々、国民意識の高まりを感じる。昔は、個人情報を使って何が悪いのかという開き直りや、氏名を消せば個人情報には当たらないという誤解、気にしすぎ・誰もあなたの情報なんて欲しくないという思い込みもあった。
 - ・ 国民意識の高まりと同時に、近年は当職としても、個人情報を取り扱う企業における意識向上も強く感じる。

自社特性に応じたメリハリのある対応

◆ まず何よりも、以下を踏まえる

自社の業種

社会からの信頼

持っている個人情報

◆ 絶対に守るべきところを従業員・委託先に徹底

- ◆ 個人情報保護の議論は細かい点も多いので、細かい点から先に入ってしまうと、絶対に守るべきところが従業員・委託先に伝わらないことも。

◆ パーソナルデータの利活用を行う場合は事前に入念な検討を→利用態様によって大きく異なる

- ◆ 匿名加工情報や非識別加工情報の仕組みを使う場合は、加工方法の十分性が鍵
- ◆ プライバシーポリシーなどの記載が適切・十分か
- ◆ 法律上どのような構成が可能か



個人情報保護法のルール

個人情報取扱のルール

入手時のルール

◆ 利用目的の特定（15条1項）	何に使うかを明らかにします
◆ 利用目的の変更制限（15条2項）	利用目的はむやみには変更できません
◆ 利用目的の通知等（18条）	何に使うか本人がわかるようにします
◆ 適正取得（17条1項）	不正に取得してはいけません
◆ 要配慮個人情報の取得制限（17条2項）	取得できる場合に制限があります
◆ 取得時の確認・記録義務（26条）	適正な取得であることを確認し記録します

利用時のルール

◆ 目的外利用の制限（16条）	利用目的を超えた利用は制限されます
-----------------	-------------------

提供時のルール

◆ 提供の制限（23条・24条）	提供できる場合に制限があります
◆ 提供時の記録義務（25条）	提供の記録をとり保存します

個人情報取り扱いのルール

管理時のルール

◆ 安全管理措置（20条）	安全に管理します
◆ 従業者の監督（21条）	従業者を監督します
◆ 委託先の監督（22条）	委託先を監督します
◆ 正確性確保の努力義務（19条）	個人データの正確性確保に努めます
◆ 消去の努力義務（19条）	個人データの遅滞ない消去に努めます

本人からのアクセスの保障

◆ 開示・訂正・利用停止請求（28～34条）	本人から請求があって法律の要件を満たせば開示・訂正・利用停止します
◆ 保有個人データに関する事項の公表等（27条）	本人がアクセスできるように公表等します
◆ 苦情処理の努力義務（35条）	苦情処理に努めます

※このほかに、匿名加工情報のルールもあります（36～39条）

個人情報の取扱いの主なチェック方法

やりたいことを明確化・分類してから、個人情報保護法上適法かを考える



◆どんなデータを使うか、登場人物はだれか

- プライバシー性の高いデータではないか
- 個人情報保護法だけでなく、個人情報保護条例などが適用になるか

総論

◆どこからだれのどのようなデータを取得するのか

- 適正な取得といえるか、要配慮個人情報の場合 17IIを満たすか

取得

◆社内でだれがどんな目的でどのように使うのか

- 利用目的はプライバシーポリシー等上のものと合致するか
- 不正行為をどのように防止するか
- 取得データを減らせないか、保有データを減らせないか、関与者を減らせないか
- 管理方法は安全か

利用・
管理

個人情報情報の取扱いの主なチェック方法

◆委託するか

- 委託契約で不適切な行為を防止しているか
- 委託先を監督する方法は適切か、不正行為をどのように防止するか
- 適切な委託先を選んでいるか

委託

◆外部提供するか、する場合だれに何のためにどのようなデータを渡すのか

- その相手にその目的でそのデータを渡すことは、社会的に受容性があるか
- 個人情報保護法 2 3 を満たすか
- 安全な授受方法か
- 渡すデータを減らせないか、関与者を減らせないか
- 提供相手による不正行為をどのように防止するか（契約、運用等）

提供

◆データの廃棄は？

◆その他

廃棄等

個人情報取得に当たって



個人情報を
勝手に取られないか
怖いかも・・・

個人情報はきちんとした形で
取得しますよ



□ 不正の手段で取得しない

- ○ 相手に説明してから取得する
- × だまし討ちで取得する
- 個人情報保護法第17条第1項

個人情報取得に当たって



個人情報を
勝手に取られないか
怖いかも・・・

要配慮個人情報は
必ず本人の同意を得た上で
取得しますよ



□ 要配慮個人情報は、原則として、本人の同意を得る

- ※改正個人情報保護法施行後（法第17条第2項）
- 要配慮個人情報とは、病歴など（法第2条第3項）
- 同意を得ない取得とは、例えばオプトアウト（個人情報保護法第23条第2項）
- 同意がなくても取得できる場合もある（前述）

個人情報取得に当たって



個人情報を
何のために聞かれているのか
何に使われるのかわからない
怖いかも・・・

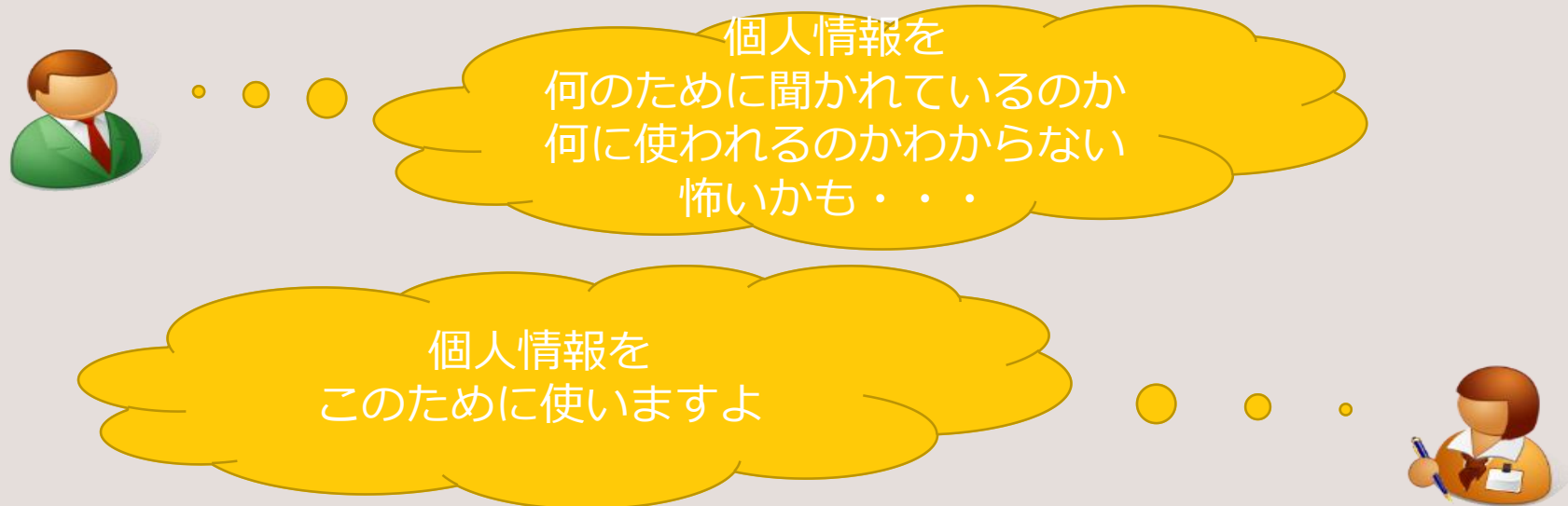
個人情報を
このために使いますよ



□ 何に使うか（利用目的）をまず特定する

- 例えば、商品や案内の送付、マーケティング、人事管理など
- 個人情報保護法第15条第1項

個人情報取得するに当たって



□ 何に使うか（利用目的）が相手にわかるようにする

- 例えば、書面に記載して渡す、Webサイトで公表するなど
- 本人から直接取得する場合は、あらかじめ、本人に示す
- それ以外は、あらかじめ公表するか、取得後速やかに通知するか、取得後速やかに公表する
- 利用目的が明らか、本人・第三者の権利利益を害する恐れがある場合などは、通知・公表等不要（個人情報保護法第18条第4項各号）
- 個人情報保護法第18条

利用目的の考え方

- 個人情報保護法という、本人同意を取得しなければならない規制との誤解もあるが、個人情報保護法の規律の要は「**利用目的**」
- 情報は、その内容や性質によって、一概に悪い、良いと決められるものではない

内容

- どのような内容かに着目する。例えば、名刺1枚とカルテ情報が同様の取扱いでよいのか。
- 要配慮個人情報、センシティブ情報、機微情報の議論につながる。
- しかし、病歴（要配慮個人情報）であっても、医療に必要であれば私たちは開示するし、医療従事者の間の共有や、医学研究者による活用も許容。ブログやSNSなどで病状を公開する人も。

文脈

- どのような文脈で個人情報が取り扱われるかに着目する。例えば、治療なのか、興味本位なのか。
- 利用目的の議論につながる。
- 名刺情報であっても、挨拶なのか、必要な情報の送付のためなのか、不要な勧誘電話のためなのか。
- 江沢民事件

検索性

- 利活用の程度、被害のおそれの程度に着目する。
- 個人データ、個人情報データベース等、マイナンバーの議論につながる。

利用目的の意義



個人情報を
何のために聞かれているのか
何に使われるのかわからない
怖いかも・・・

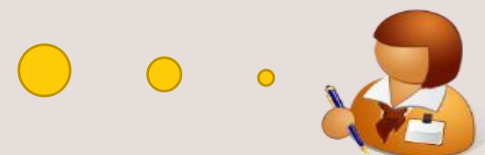
個人情報を
このために使いますよ



- ・「私の個人情報を何に使うのだろうか」
 - ・「こんなつもりで使われるとは思わなかった」
 - ・「こんなつもりで提供したわけではなかった」
- といった、誤解をなくす。本人がわかるようにする。

個人情報を利用するに当たって

約束した範囲外には、
ご本人の同意があるか、
法令で認められた場合以外、
個人情報を使いませんよ



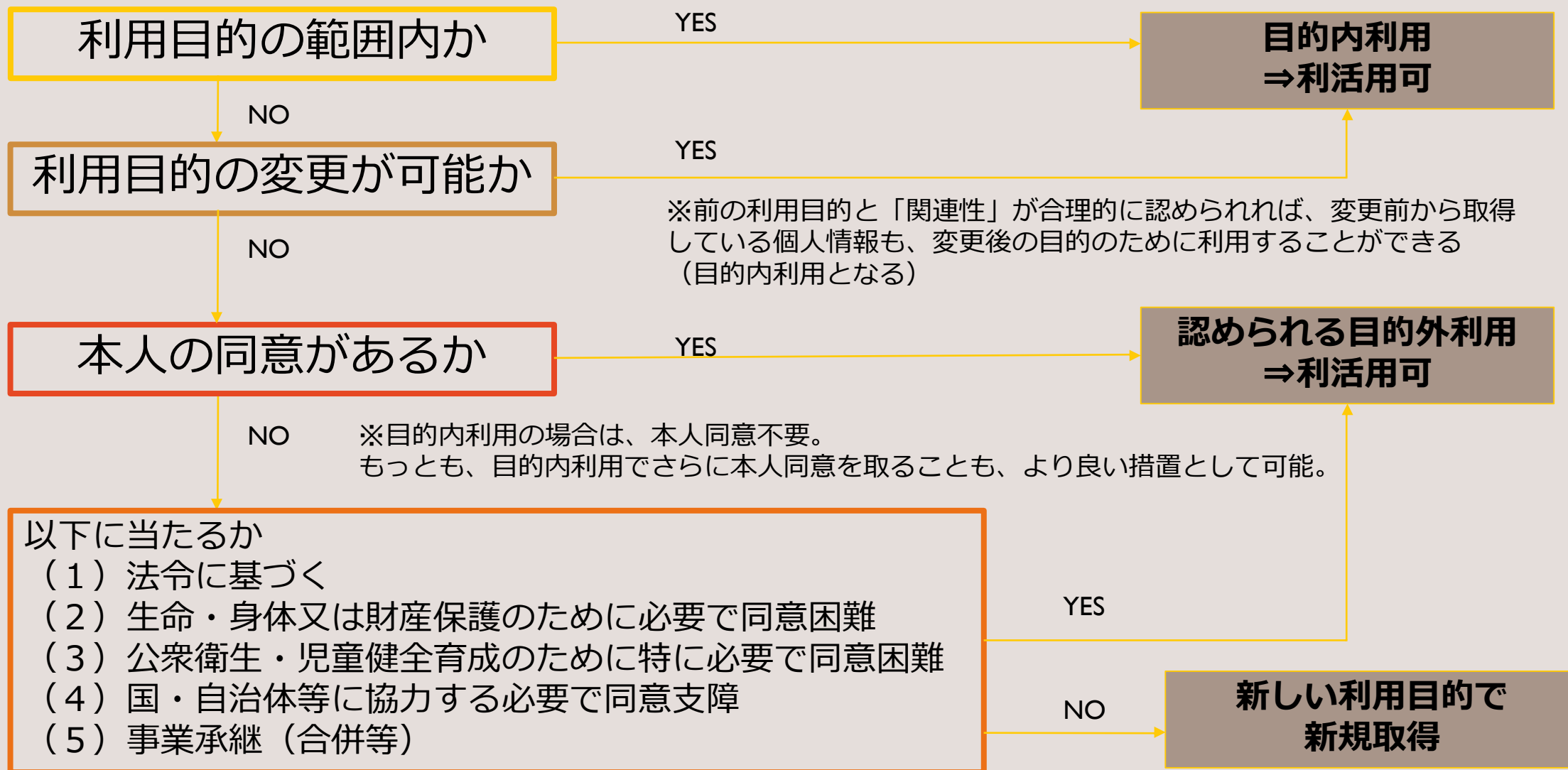
□ 本人の同意なく、利用目的の範囲を超えて、個人情報を取り扱わない

- ○ 誰が利用者と、連絡先はどこか、既往歴は何かを、〇〇サービスの実施のために把握・管理する
- × 新しい事業を始めたので、取得していた個人情報を使って、宣伝の電話をかける、手紙を送る
 - →もともと、利用目的として、これを特定すれば、利用可
 - →本人の同意をとれば、利用目的として特定していなくても、利用可
- ○ 急病のため、把握していた病歴・連絡先を利用する
 - →利用目的として特定していなくても、生命・身体・財産の保護のために必要があつて、同意を得ることが困難な場合は、利用目的の範囲外でも取り扱える
- 個人情報保護法第16条第1項・第3項

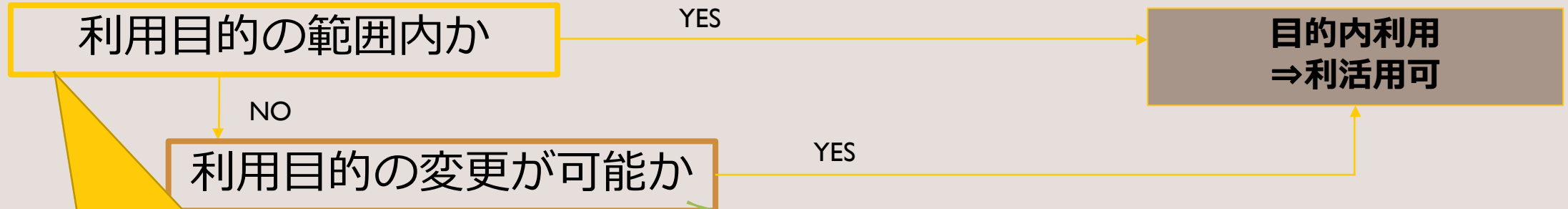
利用目的に基づく規律

利用目的を 特定する (15条1項)	やるべきこと	• 本人が自分の個人情報を知られるかわかるようにする • 何のために使うのか、本人がわかるレベルで特定する
利用目的を 公表等する (18条1・2項)	やるべきこと	• 本人が自分の個人情報を知られるかわかるようにする • Web公表、ポスター掲示、本人に書面交付等
利用目的の 範囲内で取り扱う (16条)	やるべきこと	• あらかじめ決めた利用目的の範囲内で取り扱う 例外) 同意、法令、生命・身体・財産の保護、公衆衛生の向上又は児童の健全な育成の推進、国・自治体・受託者への協力の必要 例外) 第三者提供規制は、利用目的の範囲内か問わない

個人情報利用の検討フロー



目的内利用の解説



- ◆ 法律上、「利用目的の特定」「通知又は公表」義務がある。
- ◆ 通常は、プライバシー・ポリシーなどで公表しているので、プライバシー・ポリシー等に記載している利用目的を確認する。
- ◆ 今、行いたい利用が、既存の利用目的に含まれるかを検討する。

- ◆ 先の通り既存の利用目的を確認する。
- ◆ 既存の利用目的と今、行いたい利用の目的との間に「関連性」が合理的に認められるかを検討する。
- ◆ 改正法で、利用目的変更の範囲が拡大されたものの、厳しい判断に変わりはないので、変更できる場合は限定される
- ◆ 利用目的の変更ができれば、変更前から取得している個人情報も、変更後の目的のために利用することができる（目的内利用となる）

目的内利用の解説：利用目的の変更

- 一度利用目的を特定しても、その後、別の目的のために利用する必要性が生じる場合も
- 再度利用目的を特定しなおして、個人情報を取得しなおすのは、事業者にとっても本人にとっても負担になる場合も



- そこで個人情報保護法では利用目的の変更を認めている
- もっとも無制約に変更できてしまえば、利用目的の意味がなくなる

改正前

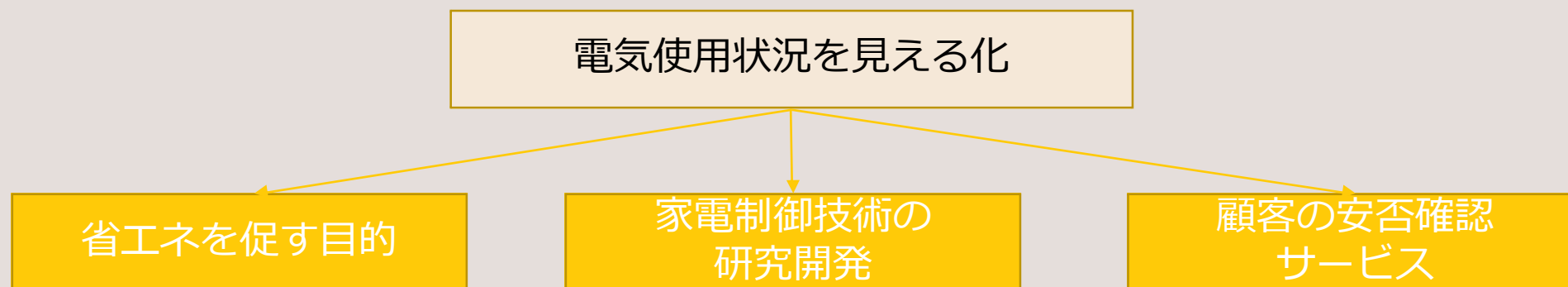
個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない（15条2項）。

改正後

個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない（15条2項）。

目的内利用の解説：利用目的の変更例

- 電力会社が、顧客に省エネを促す目的で、家庭内の機器ごとの電気使用状況を収集して、その使用量等を分析して顧客に提示をしていた場合、あるいは、同じ情報を用いて家電制御技術の研究開発とか、その顧客の安否確認のサービスを行うということができる
 - 山口国務大臣発言 第189回国会 内閣委員会 第4号（平成27年5月8日（金曜日））



目的外利用の解説

本人の同意があるか

YES

認められる目的外利用
⇒利活用可

NO

※目的内利用の場合は、本人同意不要。
もっとも、目的内利用でさらに本人同意を取ることも、より良い措置として可能。

以下に当たるか

- (1) 法令に基づく
- (2) 生命・身体又は財産保護のために必要で同意困難
- (3) 公衆衛生・児童健全育成のために特に必要で同意困難
- (4) 国・自治体等に協力する必要で同意支障
- (5) 事業承継（合併等）

YES

NO

新しい利用目的で
新規取得

- ◆ 目的内利用の場合は、本人同意不要
- ◆ 本人が真に同意しているかがポイント
- ◆ 書面（契約書、同意書等）でサインしてもらう必要はない、Webで同意ボタンクリックでもよい
- ◆ 口頭同意でもよいが、記録に残せる形が望ましい
- ◆ 明示の同意／ 黙示の同意という概念もある

- ◆ 目的外利用でも、個人情報保護法 16 条 2 項に定める場合は、本人同意なく利用可能。
- ◆ 提供規制とほぼパラレルなので、詳細は提供規制をご参照。

個人情報の利用例

例1) 自社のPC製品の顧客に新PC・付属品案内のDMを送付できるか

→通常は可能なようにプライバシーポリシーが作成されている

- 利用目的をプライバシーポリシーなどで確認
 - OKな利用目的例「商品・サービス・キャンペーン情報の提供・DM発送」
- DM発送とまで具体的に記載されていなくても、その利用目的を読んで、一般人が「これならDMも来るな」とわかればOK
- 目的内利用として個人情報保護法上適法（&本人提供は第三者提供に当たらない）

例2) 企業Webサイトでの行動履歴・購買履歴を分析できるか

→プライバシーポリシーに記載されている利用目的に依る

- 統計的把握でなく個人情報のまま〇〇さんがこういう行動をしていてこういうときにこういう商品を買っているなどの分析をすることも可能な場合がある。利用目的による。新商品開発？サービス改良？
- プライバシーポリシーなどで確認
 - 利用目的例「商品やサービスの開発・改善」←個人情報のままでOK・当然安全管理措置等が必要
 - 利用目的例「商品開発のための統計データの作成・集計」←統計のみOK
- 統計的把握なら、上記構成によらずとも、利用目的に明記していなくてもOK
- もっとも、Cookie規制等が強化される可能性もあり、最新動向に常に留意しないと違法となる恐れも

個人情報利用例

例3) 複数会社のWebサイト間で行動履歴・購買履歴を分析し潜在顧客にアプローチできるか

→情報の内容、分析の詳細、アプローチの方法等にもよって、大きく異なる

- このような個人情報利用について、社会的許容性や本人の予測可能性はあるか
- 複数会社間での情報授受について、法的根拠はあるか
 - 共同利用（複数会社が親子会社等の場合、共同キャンペーンの場合等）
 - 同意（本人へわかりやすく説明して、適切な同意を取れるか）
 - オプトアウト（本人へ拒否方法をわかりやすく説明して、通知また公表、届出を行う）
- 利用目的をプライバシーポリシーなどで確認
 - 例「Aサイト、Bサイト、Cサイトと共同で商品・サービス・キャンペーン情報の提供・DM発送」はどうか？
 - GDPR対応の企業サイトだと、かなり詳細に記載している例もある
- Cookie規制等の最新動向に常に留意
- 本人へのアプローチは拒否反応も強い
 - 特に、直接のメール、郵便、SMSなどは、拒否反応も強い

個人情報利用例

例 4) 自社の通販サイトでどのような顧客が購入しているか、AIに学習させられるか

- 例 2 と同じ

例 5) 自社従業員の勤務状況をIoT製品でチェックできるか

→ 態様による

- 利用目的は何か
 - 「雇用管理」「勤怠管理」の場合、タイムカード的な利用は可能であろう
 - A処理に○秒かけている、B処理は平均的従業員より処理が遅い、集中しておらずPCを打っていないなどと管理することは、違法性を帯びる可能性もある
- 仮に、利用目的として十分に特定されていたとしても、労働者の人権侵害に当たる可能性がある

個人情報を提供するに当たって



個人情報を
勝手に提供されないか
怖いかも・・・

個人情報は
法律上認められた範囲でしか提
供しません



□ 個人情報を提供できる場合

□ 後述

□ 改正法で、提供記録、外国への規制等

個人データを提供できる場合

ルール 第三者に個人データを提供できる場合は、法律上限定されている（23条）。

ポイント① 対象は「個人情報」ではなく「個人データ」

ポイント② 本人同意を得なくても、提供できることが法律上認められている

提供できる場合

① 本人の**同意**がある場合（法23条1項柱書）

- 書面でなくてもよい
- Webサイトでチェックボックスにチェックしてもらうなどの方法も可
- 口頭でもよいが、重要度によって、原則として記録が残せる形が良い

② **法令**に基づく場合（法23条1項1号）

例）令状に基づき裁判所に提出

③ 人の**生命、身体**又は**財産の保護**のために**必要**がある場合であって、本人の**同意を得ることが困難**であるとき（法23条1項2号）

例）災害時、意識不明時、重度の認知症の高齢者の状況を家族等に説明する等

個人データを提供できる場合

提供できる場合

④ 公衆衛生の向上 又は 児童 の健全な 育成 の 推進 のために 特に必要 がある場合であって、本人の 同意を得ることが困難 であるとき（法23条1項3号）	例）健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供、児童虐待の情報提供
⑤ 国 の機関若しくは 地方公共団体 又はその委託を受けた者が法令の定める事務を遂行することに対して 協力 する必要がある場合であって、本人の 同意を得ることにより 当該事務の遂行に 支障 を及ぼすおそれがあるとき（法23条1項4号）	例）統計法に定める一般統計調査に協力する
⑥ オプトアウト （法23条2項）	例）一定事項を通知等要。本人に求められれば提供を止める
⑦ 委託 （法23条5項1号）	例）データ入力業者への委託、印刷業務の委託
⑧ 事業の承継 （法23条5項2号）	例）合併先の会社
⑨ 共同利用 （法23条5項3号）	例）一定事項を通知等必要。病院と訪問看護ステーション

個人情報提供例

例 1) 委託先に個人情報を提供できるか（本人同意はない場合）

→本人の同意なくできる

- 委託に必要な個人情報であれば、本人同意なく提供可能
 - 委託に名を借りただけの不適切な提供は不可

例 2) 委託先から個人情報を収集できるか（本人同意はない場合）

→本人の同意なくできる

- 個人情報の収集を委託することは可能
- 例えば、マイナンバーの収集委託、顧客の住所変更事務委託などが可能
- もっとも、委託先が不適切な収集をしている場合は、委託元の責任を問われうる

個人情報提供例

例3) 自社の賃借人情報を他社に渡せるか（本人同意はない場合）

→本人の同意なくできる

- 不動産売買契約に付随して、不動産の売主から買主に対して、当該不動産の管理に必要な範囲で当該不動産の賃借人の個人データを提供することは、本人同意がなくてもできる（事業承継に当たる）
- 個人情報保護委員会Q&A Q2-10-2

例4) 自社の顧客情報を他社に売却できるか（本人同意がある場合）

→ケースバイケースだが、難しい場合が多い

- 本人同意があっても、常識的に見て本人が同意するとは思えないような場合は、本当に真の同意があるのかどうか疑われうる
- 本人への説明、本人が同意する意思、同意取得方法が十二分に適切である必要

個人情報提供例

例 5) 自社が委託を受けて保持している個人情報を他社に渡せるか（委託先指示による場合）

→できる場合が多い

- 委託先が個人情報提供を指示した場合は、できる場合が多い
- もっとも、委託先からその相手への提供行為が違法かどうかはわからないので、委託先に保証してもらうべき

例 6) 自社が委託を受けて保持している個人情報を他社に売却できるか

→できない

- 委託を受けて保持している情報は、あくまで委託元のもの。自社（委託先）が好き勝手にできるわけではない。時々、自分のところで持っているデータは自分のものであり自由にできると勘違いしている企業があるので、注意すべき。自社が委託元で外部に委託する場合、外部委託先がそのような勘違いをしていないかも十二分にチェック・監督し、委託契約で縛るなど必要な措置を取らなければならない
- もっとも、委託先指示による場合などで、そのことが立証できる場合など、あらゆる場合に不可能なわけではないかもしれない

個人情報管理に当たって



職員・委託先が個人情報を
きちんと取り扱ってくれるのか
怖いかも・・・

従業者・委託先の監督をしますよ



- 従業者の監督
 - 個人情報保護法第21条
- 委託先の監督
 - 個人情報保護法第22条
- 正確性の確保（努力義務）
 - 個人情報保護法第19条

個人情報をめぐる本人救済



自分でできることはあるの？

開示・訂正・利用停止に対応します
個人情報保護委員会があります



- 開示・訂正・利用停止
 - 求めに応じる手続、利用目的等を公表したり、遅滞なく回答する（個人情報保護法第24条第1項）
- 個人情報保護委員会
- 認定個人情報保護団体（苦情処理・情報提供など）
 - http://www.ppc.go.jp/files/pdf/personal_ninteidantai.pdf
- 訴訟も

具体例で考える個人情報保護法のルール

自社で保有する顧客情報（個人データ）の例

- 顧客から氏名・住所・病歴などの情報を取得して、管理しています。システム保管。
- 契約や顧客への必要な連絡に利用します。
- そのほかの利用はできるのでしょうか。

入手時 ルール	利用目的の特定（15条1項）	「契約の履行」「商品案内・情報提供」「商品開発」等と利用目的を決める
	利用目的の通知等（18条）	利用目的をWeb等で公表。さらに契約申込時等に書面で示す
	適正取得（17条1項）	だまして入手するなどはダメ
	要配慮個人情報の取得制限（17条2項）	本人から正当に取得していれば、本人の同意ありと考えられる
	取得時の確認・記録義務（26条）	第三者から取得するわけではないので、不要
利用時 ルール	目的外利用の制限（16条）	利用目的の範囲内なら可。利用目的の範囲外でも、裁判所から令状で求められた場合等に顧客情報を検索するなどの目的外利用は適法。

具体例で考える個人情報保護法のルール

自社で保有する顧客情報（個人データ）の例

- 顧客から氏名・住所・病歴などの情報を取得して、管理しています。システム保管。
- 契約や顧客への必要な連絡に利用します。
- そのほかの利用はできるのでしょうか。

提供時 ルール	提供の制限（23条・24条）	データ入力や管理をシステム会社等に委託できる。国外の委託先の場合は、契約書精査等が重要。 令状に基づき裁判所・警察などにも提供できる。週刊誌の問い合わせ対応などは、本人同意なければダメなのが基本。
	提供時の記録義務（25条）	誰にいつ提供したか等を記録する。
管理時 ルール	正確性確保の努力義務（19条）	内容に不正確がないよう努力する。
	消去の努力義務（19条）	不要な情報は速やかに消去するようにする。契約終了時にすぐに消去しなければならないというものではない。
本人 アクセス	開示・訂正・利用停止請求（28～34条） 保有個人データに関する事項の公表等（27条）	本人から見せてくれと言われれば、基本的には開示要。法律の定める要件を満たす場合は、開示しなくてよい場合も。訂正は、データが事実でなく利用目的達成に必要な範囲内で訂正する。利用停止は一定の不正があった場合のみ。

具体例で考える個人情報保護法のルール

応募者から履歴書等を取得して、人事部で管理する例（個人データ）

- 採用応募者から履歴書などの情報を取得して、採用選考に利用します。個人ごとに綴って保管。
- 不採用になった方の履歴書なども返却しません。
- 採用者は、入社後も引き続き、履歴書などの情報を人事管理に利用します。

入手時 ルール	利用目的の特定（15条1項）	「採用・人事管理」等と利用目的を決める
	利用目的の通知等（18条）	採用フォームなどに利用目的を示して、情報取得前に本人に利用目的を明示する。又は利用目的が明らかであり通知等は不要とも解釈可能か（18条4項4号）。
	適正取得（17条1項）	だまして入手するなどはダメ
	要配慮個人情報の取得制限（17条2項）	本人から正当に取得していれば、本人の同意ありと考えられる
	取得時の確認・記録義務（26条）	第三者から取得するわけではないので、不要
利用時 ルール	目的外利用の制限（16条）	「採用・人事管理」等の利用目的以外の利用（例、DMの送付）は制限されるが、 災害・急な重病時に家族に連絡するための目的外利用等 は法律上適法。

具体例で考える個人情報保護法のルール

応募者から履歴書等を取得して、人事部で管理する例（個人データ）

- 採用応募者から履歴書などの情報を取得して、採用選考に利用。個人ごとに綴って保管。
- 不採用になった方の履歴書なども返却しない。
- 採用者は、入社後も引き続き、履歴書などの情報を人事管理に利用。

提供時 ルール	提供の制限（23条・24条）	データ入力や管理をシステム会社等に委託できる。国外の委託先の場合は、契約書精査等が重要。 令状に基づき裁判所・警察などにも提供できる。週刊誌の問い合わせ対応などは、本人同意なければダメなのが基本。
	提供時の記録義務（25条）	誰にいつ提供したか等を記録する。
管理時 ルール	正確性確保の努力義務（19条）	内容に不正確がないよう努力する。
	消去の努力義務（19条）	不採用者の情報は速やかに消去するようにする。
本人 アクセス	開示・訂正・利用停止請求（28～34条） 保有個人データに関する事項の公表等（27条）	本人から見せてくれと言われれば、基本的には開示要。法律の定める要件を満たす場合は、開示しなくてよい場合も。訂正は、データが事実でなく利用目的達成に必要な範囲内で訂正する。利用停止は一定の不正があった場合のみ。

具体例で考える個人情報保護法のルール

お客様からのご意見を取得する例（個人データではない）

- お客さまから苦情などのご意見が郵送されてきた。
- 郵便物の書類のままの状態に対応した後は、「〇月苦情〇件。苦情概要△。」などと、個人が特定できない形にして記録して、書類の実物自体はシュレッダー廃棄。 →個人データではない

入手時 ルール	利用目的の特定（15条1項）	「苦情処理、サービス向上」等と利用目的を決める
	利用目的の通知等（18条）	利用目的が明らかであり通知等は不要とも解釈可能（18条4項4号）。
	適正取得（17条1項）	本人が郵送してきたので特に問題とならない
	要配慮個人情報の取得制限（17条2項）	要配慮個人情報に当たらない
	取得時の確認・記録義務（26条）	—（非個人データには義務付けされない）
利用時 ルール	目的外利用の制限（16条）	「苦情処理、サービス向上」等の利用目的以外の利用（例、DMの送付）は制限される。

具体例で考える個人情報保護法のルール

お客様からのご意見を取得する例（個人データではない）

- お客さまから苦情などのご意見が郵送されてきた。
- 郵便物の書類のままの状態に対応した後は、「〇月苦情〇件。苦情概要△。」などと、個人が特定できない形にして記録して、書類の実物自体はシュレッダー廃棄。 →個人データではない

提供時 ルール	提供の制限（２３条・２４条）
	提供時の記録義務（２５条）
管理時 ルール	安全管理措置（２０条）
	従業者・委託先の監督（２１・２２条）
	正確性確保の努力義務（１９条）
	消去の努力義務（１９条）
本人 アクセス	開示・訂正・利用停止請求（２８～３４条） 保有個人データに関する事項の公表等（２７条）

—（非個人データには義務付けされない）
※もっとも**プライバシー**に配慮

個人情報管理に当たって



個人情報が
漏えいしたり改変されたりしないか
怖いかも・・・

個人情報は
安全管理しますよ



□ 安全管理措置

□ 後述

安全管理措置（一般）

基本方針	プライバシー・ポリシー等を整備すると望ましい。
規律の整備	取扱規程の作成、取扱方法の周知等
組織的安全管理措置	
組織体制の整備	責任者・担当者等を決定等
個人データの取扱いに係る規律に従った運用	ログ等
取扱状況を確認する手段の整備	台帳等
漏えい等の事案に対応する体制の整備	連絡体制の決定等
取扱状況の把握及び安全管理措置の見直し	点検、監査等
人的安全管理措置	
従業員の教育	研修、守秘義務
従業員の監督	（法21条）

<https://www.ppc.go.jp/files/pdf/guidelines01.pdf>

物理的安全管理措置

区域の管理	間仕切り、入退室管理等
機器及び電子媒体等の盗難等の防止	施錠、セキュリティワイヤー等
電子媒体等を持ち運ぶ場合の漏えい等の防止	パスワード、封緘等
削除、廃棄	復元不可能な方法で

技術的安全管理措置

アクセス制御	権限管理等
アクセス者の識別と認証	ID/PWD、カード等
外部からの不正アクセス等の防止	FW、セキュリティ対策ソフト等
情報システムの使用に伴う漏えい等の防止	パスワード等

社内規程・運用とチェックポイント

項目	チェックの観点
取得	
・ 取得方法は適切か	本人に不意打ちを与えないか、漏えい等起きないか
・ 要配慮個人情報を取得するか	要配慮個人情報の規制を遵守しているか（法17条2項）
・ 利用目的は十分か	利用目的に不足はないか（目的外利用での処理は多いのか）、公表・通知されているか
利用	
・ 目的外利用する場合の判断権者は誰か	社内的に定型的な目的外利用は何か、例外的な目的外利用は慎重に要検討
提供	
・ 外部提供する場合の判断権者は誰か	社内的に定型的な外部提供は何か、例外的な外部提供は慎重に要検討、トラブルも多い
・ 提供方法は適切か	漏えいや誤提供は起きないか
・ 外国提供はあるか	契約書は適正か

社内規程・運用とチェックポイント

項目	チェックの観点
管理	
・ 従業者監督は十分か	ミスはありうるのを前提に、重要なものには丁寧な監督を
・ 従業員教育は十分か	他社のトラブル事例の共有なども有用
・ 委託先監督は十分か	委託先で取り扱う個人情報、取り扱う者、処理内容、定期報告、随時報告、連絡体制、契約書、委託先の責任
・ 安全管理措置	組織的（規程上の体制が実態に合っているか、記録・台帳の整備・点検状況、点検・監督状況） 人的（上述＝監督・教育） 物理的（場所、移動、施錠、パスワード、廃棄） 技術（セキュリティ対策）
その他	
・ 開示／訂正／利用停止請求対応	請求権は法的権利、対応は法的義務。 手続を定める。手数料徴収可。



個人情報とは何か

(1) 個人情報とプライバシー権

個人情報とプライバシー権の比較

「個人情報」「個人データ」「保有個人データ」「要配慮個人情報」という種類がある。さらには、「匿名加工情報」「非識別加工情報」「匿名加工医療情報」という種類も。でも、そもそも「個人情報」と「プライバシー」って違うの？ 同じなの？



種類	特徴	規制
個人情報 例) 名刺、企業の役員情報、公開情報	■ 意外と範囲が広い ■ 内容の重要性・秘匿性は問わない	■ 規制は比較的弱め ■ 「個人情報」より「個人データ」「保有個人データ」に規制を強化
要配慮個人情報 例) カルテ情報、検査結果	■ 意外と範囲が狭い ■ 金融の場合は、さらに「機微情報」概念が加わる	■ オプトアウトしていなければ、通常の個人情報と基本的には差異なし
プライバシー権 例) 購買歴、政治思想、不倫	■ 「個人情報」とは違う ■ 一般的な「個人情報」のイメージは、実は「プライバシー」	■ 個人情報保護法（行政による指導等）ではなく、民法（裁判による解決）

制裁の比較

種類	制裁
個人情報保護法違反 例) 不適正取得、第三者提供規制違反、 目的外利用規制違反	■ 行政（個人情報保護委員会）による助言・指導・勧告・命令 ■ 基本的には行政指導、命令違反に対して罰則 ■ 一定の悪質行為には、命令を経ずに罰則（直罰） ■ 個人情報保護法に基づく直接的な賠償責任はない ■ 要配慮個人情報も個人情報も個人データも保有個人データも、個人情報保護法に違反していれば、同様
プライバシー権侵害 例) ネットに他人の私生活上の問題を書き 込む、特定商品の購買者情報を売却	■ 基本的に罰則はない（脅迫罪等を構成する場合は別） ■ 謝罪広告や賠償責任を負う（裁判、和解）



- ✓ 個人情報保護法対応：「個人情報」「個人データ」「保有個人データ」の範囲を正しく理解することが重要。個人情報保護法違反は行政による指導がメイン（罰則もある）。
- ✓ プライバシー権保護：個人情報保護法だけを遵守すればよいというものではなく、一般に不法行為を行えば、裁判で敗訴する可能性（賠償責任を負う）



個人情報とは何か

(2) 個人情報の定義

個人情報定義

定義

「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう（2条1項・2項）。

- ① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
- ② 個人識別符号が含まれるもの
※個人識別符号とは、指紋、掌紋、パスポート番号、健康保険証番号等、特定の個人を識別することができるもの

生きている人の情報

誰の情報かわかるもの

POINT

- 個人情報保護法の細かい論点に入り込むと、本質が見えにくくなる傾向も。
- 定義について細かい点を抑えるのは後回しにして、
まずは①生きている人の情報、②誰の情報かわかるものという2つの要件を満たせば個人情報であると理解しよう。

個人情報定義：生存者

個人情報であるためには、**生存者の情報**であることが必要

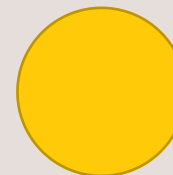
- 民間企業等の法人の情報は、個人情報に当たらない
 - もっとも、法人の役員や従業員の情報は、生存している者の情報であり、個人情報に当たる。

「株式会社はろうの平成28年売上高は、〇円」



個人情報に該当しない
∵ 生きている人の情報ではない

「株式会社はろうの代表取締役社長は、情報太郎である」



個人情報に該当する
∵ 生きている人の情報である

- Cf. プライバシー情報と個人情報は異なる。重要情報・秘密情報でなくても、個人情報に該当する。
- 死者の情報は、原則として個人情報に当たらない
 - もっとも、それが生存者の情報にも該当するような情報、例えば「故情報太郎氏の財産は100億円であり、相続人である情報花子氏が単独で相続する」ことは、個人情報に該当する。

個人情報定義：特定の個人を識別できる

- 誰の情報かわからなければ個人情報には該当しない。
 - したがって、「東京都民の平均年収は〇百万円である」といった情報は、個人情報に該当しない。
- 一方で、誰の情報かわかれば個人情報に該当するため、「氏名が記載されていなければ個人情報に当たらない」という理解は、誤りである。
 - 「うちの会社の社長は四国出身だ」「今の東の関脇は...」「今の阪神の監督は...」「昭和最後の内閣総理大臣は...」
 - 氏名が含まれていなくても、顔写真や指紋があれば、一般に誰の情報かがわかるといえ、個人情報に該当する。
 - また、ユーザIDとだけ結びついている購買履歴であったり、特定のブラウザ情報とだけ結びついているWeb閲覧履歴であったり、匿名のブログに記載された内容であっても、ものによっては、誰の情報かがわかる場合があるので、その場合は個人情報に該当する。いわゆる「特定」。
 - 氏名が記載されていなくても、誰の情報かわかる場合は意外と多い。

誰のことかわかった



個人情報定義：特定の個人を識別できる

- さらに、誰の情報かは、その情報単体でわからなくてもよい。
 - 例えば、表1には仮名とだけ結びついているデータがあり、表2には仮名と実名の結びつきのデータがあったとして、表1と表2を困難なく組み合わせることができれば（→容易照合性）、個人情報に該当する。

仮名	乗降履歴		仮名	実名
A1	2016年6月20日7時32分 千葉駅		A1	情報太郎
	2016年6月20日8時38分 市ヶ谷駅			
	2016年6月20日19時55分 市ヶ谷駅			
	2016年6月20日21時3分 千葉駅			
B2	2016年6月20日8時35分 新宿御苑前駅		B2	難波舞
	2016年6月20日8時58分 四ツ谷駅			
	2016年6月20日18時3分 四ツ谷駅			
	2016年6月20日18時25分 銀座駅			
	2016年6月20日23時35分 銀座駅			
	2016年6月20日23時53分 新宿御苑前駅			

キーワード

容易照合性

個人情報定義の改正

改正前

「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう（旧2条1項）

改正後

※実質的改正箇所は下線部参照

「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。（2条1項・2項）

①当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

②個人識別符号が含まれるもの

POINT

- 最初の（ ）の追加については、記述等は、文書だけに限定されず、幅広い一切の事項をいうという改正で、これまでの明確化
- 2条1項2号の「個人識別符号」は、次のスライドにて詳解

個人識別符号

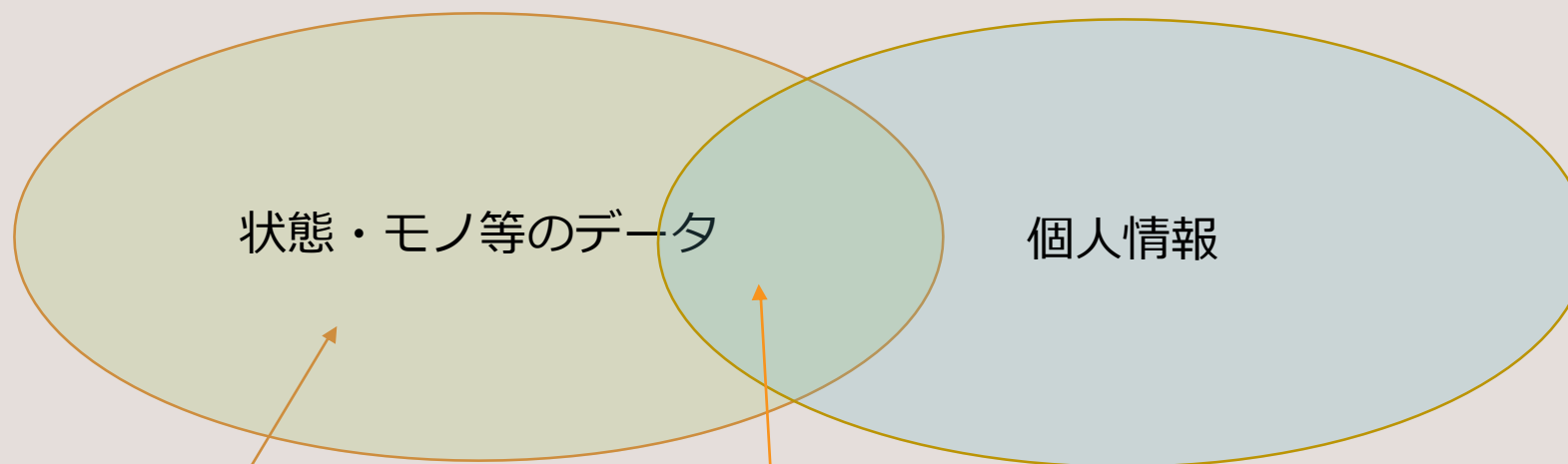
個人識別符号

身体特徴系符号（法2条2項1号符号）	番号系符号（法2条2項2号符号）
イ) ゲノムデータ ロ) 容貌 ハ) 虹彩 ニ) 声 ホ) 歩行の態様 ヘ) 静脈 ト) 指紋又は掌紋 ※これらの組み合わせも含む ※ガイドライン通則編9~11ページ 本人を<u>認証</u>することができるようにしたもの	イ) パスポート番号等 ロ) 基礎年金番号 ハ) 免許証番号 ニ) 住民票コード ホ) 個人番号（マイナンバー） ヘ) 保険証等の記号、番号及び保険者番号等 ト) 雇用保険証番号

※旧法でも個人情報として扱ってきたもの
実務上も、「容易照合性」等その他から、個人情報として取り扱ってきたものと思われる

様々なデータが蓄積される時代

- ◆ IoT時代には、個人情報以外のデータも大量に発生
- ◆ 状態・モノ等のデータであっても、個人情報に該当するものもあれば、そうでないものもある
- ◆ AIで機械学習させるデータも、個人情報であったりそれ以外の情報であったりする



- 機械ログ、運行・走行情報
- 温度、湿度、センサー情報
- 地形、地図、測量情報
- 施設情報
- 生産過程、工事状況情報
- 等さまざま

- 人に関する情報であれば「個人情報」
- 例) 電力消費量であれば、それが誰の情報かわかれば「個人情報」
- 例) 車両運行情報であれば、乗客や運転手、通行人等、人に関する情報があって、それが誰の情報かわかれば「個人情報」



個人情報とは何か

(3) 個人データ／保有個人データ

個人情報定義が広いからこそ、規制対象が異なる

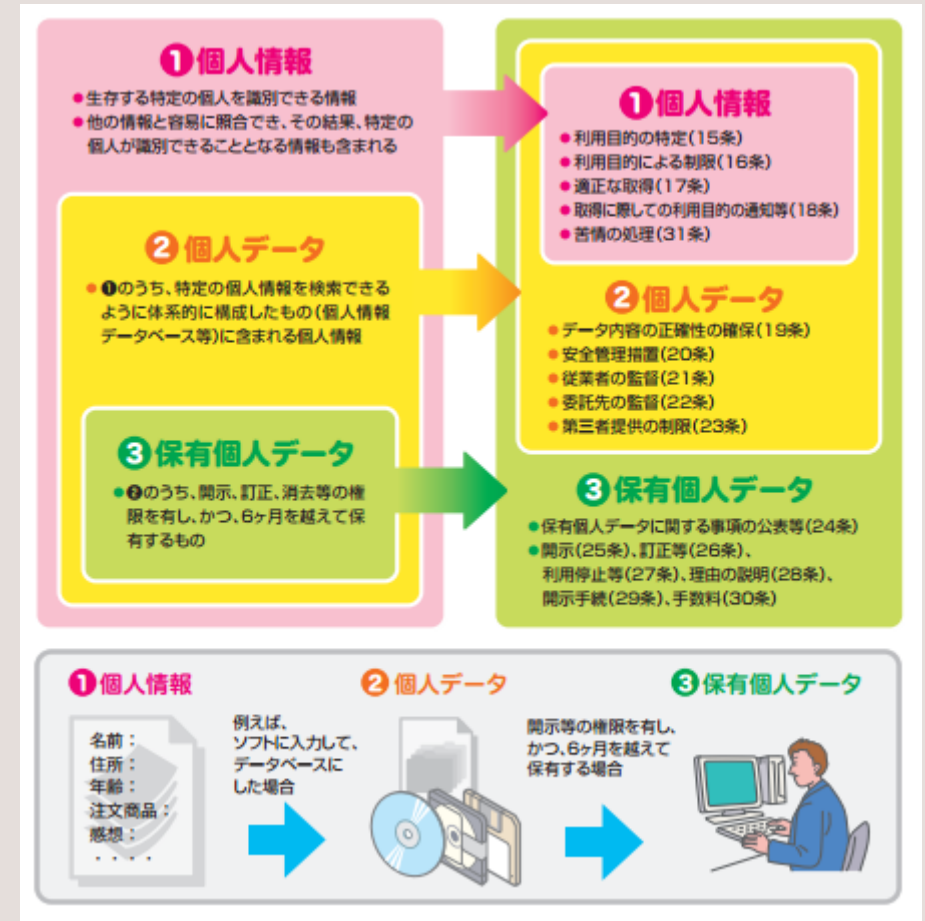
- **個人データ**
 - この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。
- 個人情報データベース等
 - この法律において「個人情報データベース等」とは、個人情報を含む情報の集合体であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。
 - 一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
 - 二 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

POINT



検索性

体系的構成



個人情報定義が広いからこそ、規制対象が異なる

保有個人データ

- この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間（六月）以内に消去することとなるもの以外のものをいう。

POINT ⇒

開示等の権限

6月超え

個人情報 > 個人データ > 保有個人データ





個人情報とは何か

(4) プライバシー権／営業秘密

プライバシー権（判例）

プライバシー権

- ① 私生活上の事実又は私生活上の事実らしく受け取られる恐れ（私生活性）
- ② 一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること、換言すれば一般人の感覚を基準として公開されることによって心理的な負担、不安を覚えるであろうと認められること（非公開の期待）
- ③ 一般の人々に未だ知られていないこと（非公知性）
- ④ （本人との同定可能性）

宴のあと事件(東京地判昭和39年9月28日判時385号12頁)、防衛庁リスト事件(新潟地判平成18年5月11日判時1955号88頁)、石に泳ぐ魚事件一審判決(東京地判平成11年6月22日判タ1014号280頁) 二審判決(東京高判平成13年2月15日判タ1061号289頁)等

POINT

- 個人情報よりも狭い。非公開の期待＋非公知性が求められる。
- 特殊な個人の感受性ではなく一般人の感受性が基準。もっとも、特殊な情報であっても、一般人がその人の立場に立ったならば非公開を欲する場合は、保護対象となる点に十分留意が必要。

営業秘密（不正競争防止法）

営業秘密

- ① 秘密として管理されている（**秘密管理性**）
- ② 生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって（**有用性**）
- ③ 公然と知られていないもの（**非公知性**）

不正競争防止法 2 条 6 項

POINT

- 個人情報以外も含む概念だが、個人情報に当たって、かつ営業秘密に当たるものも多数ある
- 顧客名簿の売却などは、不正競争防止法の罰則で処罰されることもある

具体例で考える個人情報／個人データ／保有個人データ

例	個人情報か	個人データか	保有個人データか
注文書・注文請書・契約書	○	△	△
→担当者名、社長名等でも個人情報 →一枚でただ紙としてあるだけなら、個人情報ではあるが個人データではないが、顧客別にバインダで綴ったりすれば個人データかつ保有個人データ。			
監視カメラの映像	○	×	×
→映りこんでいる人の氏名がわからなくても基本的には個人情報 →通常は特定の個人が検索できるようになっていないので、基本的には個人データではない。			
社員情報・社員家族情報	○	△	△
→外部情報に限らず社員情報であっても個人情報			
社員の健康診断の結果	○	△	△
→要配慮個人情報に該当。 →一枚でただ紙としてあるだけなら、個人情報ではあるが個人データではないが、対象者別にバインダで綴ったり、データ管理すれば個人データかつ保有個人データ。			

※プライバシー権で保護されるかは、内容・文脈等による
 ※営業秘密の場合は、不正競争防止法による保護も及ぶ



個人情報とは何か

(5) 要配慮個人情報

個人情報保護の観点

- 情報は、その内容や性質によって、一概に悪い、良いと決められるものではない

内容

- どのような内容かに着目する。例えば、名刺 1 枚とカルテ情報が同様の取扱いでよいのか。
- **要配慮個人情報**、センシティブ情報、機微情報の議論につながる。
- しかし、病歴（要配慮個人情報）であっても、医療に必要であれば私たちは開示するし、医療従事者の間の共有や、医学研究者による活用も許容。ブログや SNS などで病状を公開する人も。

文脈

- どのような文脈で個人情報が取り扱われるかに着目する。例えば、治療なのか、興味本位なのか。
- **利用目的**の議論につながる。
- 名刺情報であっても、挨拶なのか、必要な情報の送付のためなのか、不要な勧誘電話のためなのか。
- 江沢民事件

検索性

- 利活用の程度、被害のおそれの程度に着目する。
- **個人データ**、個人情報データベース等、**マイナンバー**の議論につながる。

要配慮個人情報

要配慮個人情報

人種	本人の人種（法2条3項）	例）アイヌ
信条	信条（法2条3項）	例）政治的思想
社会的身分	社会的身分（法2条3項）	
障害・健康等	障害（法2条3項、政令2条1号） 身体障害、知的障害、精神障害（発達障害を含む。）その他の規則で定める心身の機能の障害*があること	例）療育手帳を交付され所持している
	病歴（法2条3項）	例）ガンに罹患
	診療等（法2条3項、政令2条3号） 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと	例）インフルエンザのため、2月11日にA病院内科を受診した
	健康診断等の結果（法2条3項、政令2条2号） 本人に対して医師その他医療に関連する職務に従事する者（「医師等」）により行われた疾病の予防及び早期発見のための健康診断その他の検査（「健康診断等」）の結果	例）健康診断の結果、ストレスチェックの結果、特定健康診査の結果

要配慮個人情報

要配慮個人情報

犯罪等	犯罪の経歴（法2条3項）	例）強盗の前科2犯
	刑事事件（法2条3項、政令2条4号） 本人を被疑者又は被告人として、逮捕、搜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと	例）窃盗を被疑事実として逮捕された
	少年事件（法2条3項、政令2条5号） 本人を少年法3条1項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと	例）少年時代に傷害で審判を受けた
犯罪被害	犯罪により害を被った事実（法2条3項）	例）空き巣に入られた

法律による規制

- 原則として本人の同意を得て取得・提供
 - 実務的には、**オプトアウトによる第三者提供・取得の禁止**（23条2項・17条2項）



但し、金融ガイドラインに注意！

要配慮個人情報を取得・提供できる場合

類型	場合	取得	提供
法 2 3 条 1 項類型	同意	○（法 1 7 条 2 項柱書）	○（法 2 3 条 1 項柱書）
	法令に基づく場合	○（法 1 7 条 2 項 1 号）	○（法 2 3 条 1 項 1 号）
	人の生命・身体・財産の保護のために必要で、 同意を得ることが困難	○（法 1 7 条 2 項 2 号）	○（法 2 3 条 1 項 2 号）
	公衆衛生の向上・児童の健全な育成推進のために 特に必要で、同意を得ることが困難	○（法 1 7 条 2 項 3 号）	○（法 2 3 条 1 項 3 号）
	国・自治体・受託者に協力する必要がある、 同意を得ると支障のおそれ	○（法 1 7 条 2 項 4 号）	○（法 2 3 条 1 項 4 号）
	オプトアウト	×（法 1 7 条 2 項になし）	×（法 2 3 条 2 項）
非第三者 （法 2 3 条 5 項類型）	委託	○（法 1 7 条 2 項 6 号・政令 7 条 2 号）	○（法 2 3 条 5 項 1 号）
	事業承継	○（法 1 7 条 2 項 6 号・政令 7 条 2 号）	○（法 2 3 条 5 項 2 号）
	共同利用	○（法 1 7 条 2 項 6 号・政令 7 条 2 号）	○（法 2 3 条 5 項 3 号）
法 1 7 条 2 項類型	公開（by本人・国・自治体・規則）	○（法 1 7 条 2 項 5 号）	—
	本人を目視又は撮影して、外形上明らかな 要配慮個人情報を取得する場合（政令 7 条 1 号）	○（法 1 7 条 2 項 6 号・政令 7 条 1 号）	—

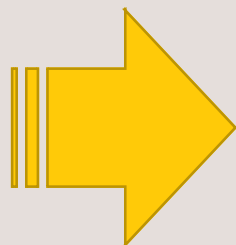
具体例で考える要配慮個人情報

例	個人情報か	個人識別符号か	要配慮個人情報か
履歴書の賞罰欄に記載された前科 →本人の意思で記載しているのであれば、会社は、本人同意に基づき取得できる。	○	×	○
保険証の情報 →法律上は要配慮個人情報ではないが、マル障受給者証などは要配慮個人情報。	○	○	△
ガン治療中の情報 →要配慮個人情報	○	×	○
風邪やものもらいで受診した →特に知られたくない傷病名でなくとも、要配慮個人情報	○	×	○

- 要配慮個人情報に該当しない機微情報の例としては、薬局で自分で購入した薬の情報など（保健医療）

具体例で考える要配慮個人情報

例	個人情報か	個人識別符号か	要配慮個人情報か
健康診断を受けた	○	×	×
→受けた事実だけでは、要配慮個人情報ではない			
健康診断の結果	○	×	○
→健康診断の結果になると、要配慮個人情報			
身長、体重、体温データ	○	×	△
→健康診断、診療等の事業及びそれに関する業務とは関係ない方法により知り得た場合は、要配慮個人情報ではない			



- 要配慮個人情報に該当したとしても、**オプトアウト**していなければ、改正法による影響は基本的には受けない
- 本人から問診票や口頭で聞き取った場合、同意があると考えられる。緊急時に親族から病歴を聞き取ること可（法17条2項1号）

細かい定義よりも、まずは様々なデータ保護があることを理解

◆ このように、定義は細かく技術的事項

個人情報／個人データ／保有個人データ

プライバシー

営業秘密

要配慮個人情報／機微情報

- 個人情報は広い
- 個人データは検索性
- 個人データ等に非該当でも、プライバシー権として保護される！
- 個人情報を盗み出したりすると、不正競争防止法で処罰されることもある
- 要配慮個人情報は意外と狭い。
- 機微情報を忘れないように。

◆ 技術的な定義よりも、まず一番大事なのは、
様々な観点から様々なデータが保護されていることを理解する



匿名加工情報

自社・他者の持つ個人情報等をより容易にビジネス活用できる仕組み

個人情報保護法制の改正

- ◆ 個人情報保護法改正により、規制強化への対応は一定程度完了しているが、**利活用はまだ**対応していないという企業が多い
- ◆ 匿名加工情報と非識別加工情報で、個人（消費者等）を保護しつつ、ビジネスのためにデータを利活用できるように
- ◆ 個人情報よりも制約が少ないので、簡単な手続で利活用や外部提供が可能に

種類	メリット	利活用例
匿名加工情報	個人情報ではないので、目的外利用や外部提供が容易	- 自社で持っている顧客購買履歴を分析 - 他社で持っている顧客属性情報と自社データを組み合わせて分析
非識別加工情報	- 国や自治体からデータを入手できる - 国や自治体の持つ新鮮で正確なデータを入手できる	- 日本に出入国する外国人の情報を分析 - 古物商、風営法許可等の状況を分析 - 国家資格合格者の情報を分析 - 住民データを分析

匿名加工情報

匿名加工情報

概要

- ◆ 個人情報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。

具体的にはどのようなデータか？



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	千代田区麴町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」の段階で、個人情報のまま

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
	千代田区麴町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）

匿名加工情報

・・・個人情報ではない

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
	千代田区麴町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

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

・・・個人情報ではない

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					
千代田区麴町					
千代田区神保町					

必ずしもここまで
丸める必要はない

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

匿名加工情報にかかるルール

規制総論	加工（36条1項）
	■ 規則で定める基準（住所の市町村以下を削除、特殊な情報の削除、ノイズ付加等）・認定個人情報保護団体による自主ルールに従って加工 ■ 要配慮個人情報も匿名加工情報にできる
	安全管理措置（36条2項）
	■ 削除した情報や加工方法に関する情報の漏えいを防止するために安全管理
	公表（36条3・6項・39条）
	■ 情報項目を公表。 匿名加工情報には開示等請求が認められていないため、公表によって、本人が関与
	識別禁止 （36条5項・38条）
提供規制	■ 本人を識別するための行為をしない ■ 自ら匿名加工情報を利活用することは可
	公表（36条4項・37条）
	■ 情報の項目と提供方法を公表 ■ 本人への通知や同意取得は不要
	提供先に明示（36条4項・37条）
	■ 提供先である第三者に、提供情報が匿名加工情報であることを明示



非識別加工情報

国・自治体の持つビッグデータ等をビジネス活用
できる仕組み

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。

非識別加工情報

[*https://www.ppc.go.jp/files/pdf/191202_doukou.pdf](https://www.ppc.go.jp/files/pdf/191202_doukou.pdf)の19P

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（消費者等）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

- ◆ 自分の欲しいデータが非識別加工情報の対象かどうか確認要。
- ◆ 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。
- ◆ 自治体が豊富なデータを保有するが、現段階では、5団体*以外、条例化されていないと思われる。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。

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

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）



加工

非識別加工情報

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

民（企業等）

パターン①自社で匿名加工情報を作成



匿名加工情報

加工



パターン②他社から匿名加工情報を入手

匿名加工情報

他社



※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

非識別加工情報入手の流れ

手続	概要
1) データの調査	入手したいデータがあるかe-Gov等で調べる
2) 国への提案	提案書を作成し国に提出する
3) 国での審査	提案書が審査される
4) 国との契約	適当と認められると契約できる
5) データの入手	契約に基づきデータを手に入る
6) データの利活用	法規制等に従ってデータを利活用する





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

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？

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++の実施例

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

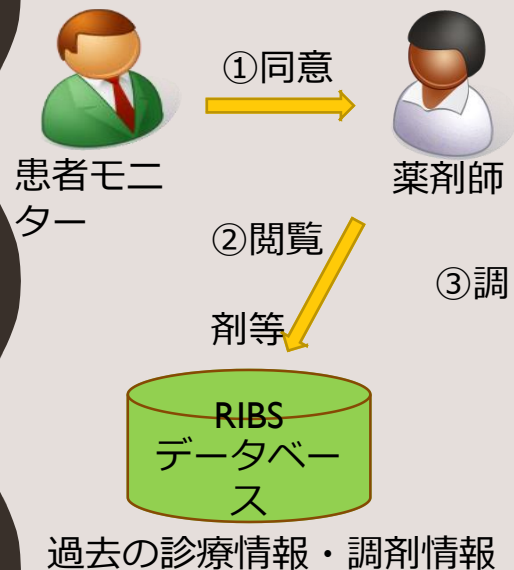
1 本評価の範囲・対象

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、**R**eceipt **I**nformation **B**rowsing **S**ystem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

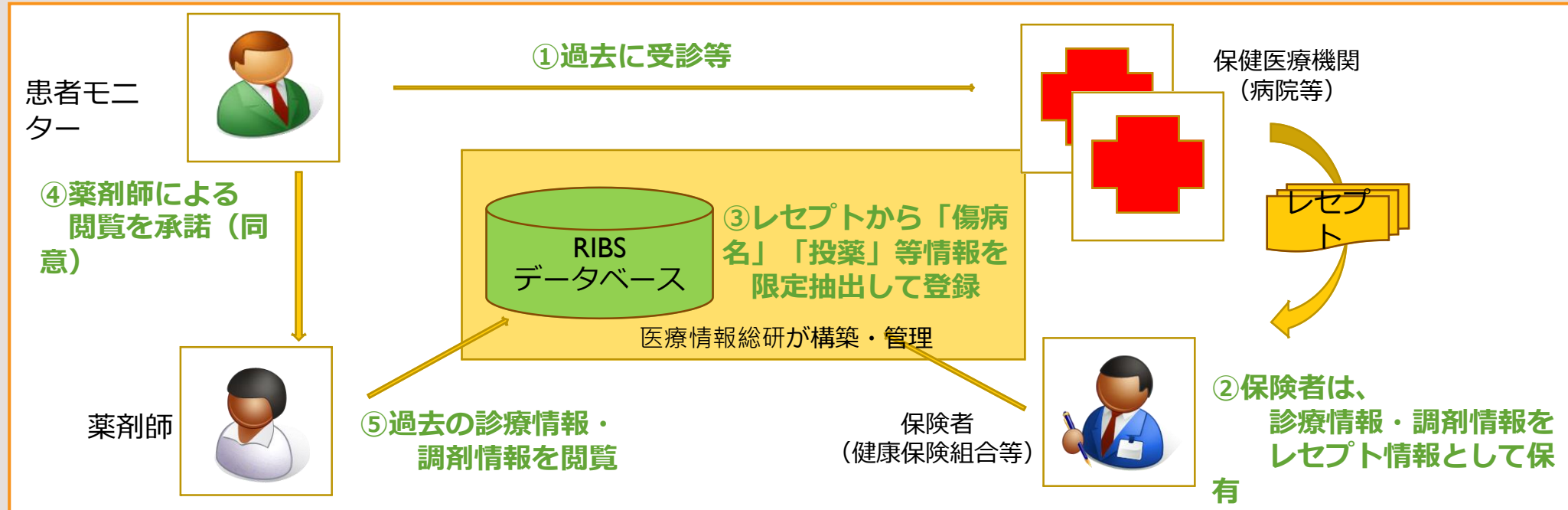


- 患者モニターが『診療情報提供カード』を提示することが、過去の診療情報・調剤情報を薬剤師が閲覧することへの同意になります。
- 診療情報を薬剤師に閲覧させるかどうかは、その都度決めることができます。
今回は閲覧させるが、次回は閲覧させないといった選択も可能です。
- 患者モニターになることを同意した場合でも、診療情報提供カードを提示しない（＝「診療情報を開示しない」という意思表示をする）ことができます。

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

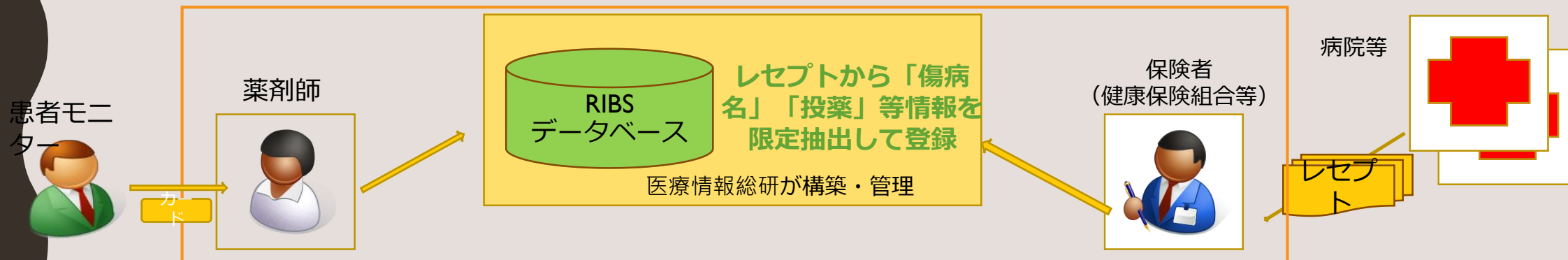
患者利便の向上

- 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

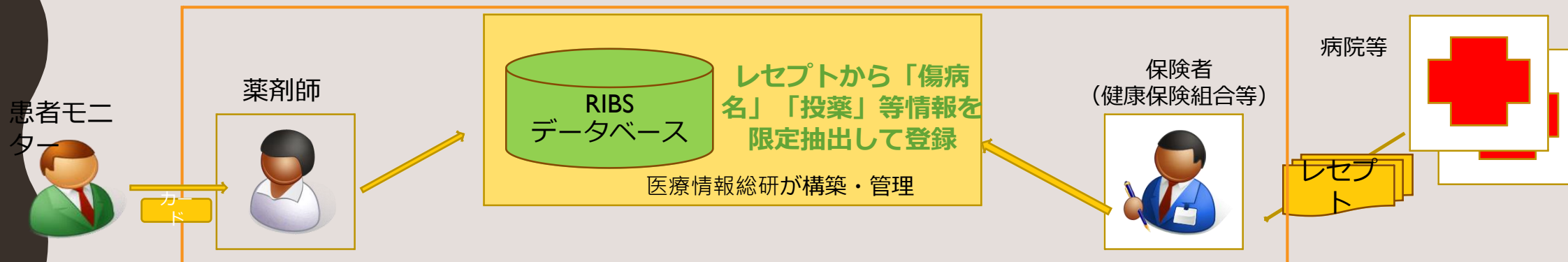
- 重複投与の防止により残薬の発生を抑制
- 過去の投薬履歴を閲覧することで、患者に対してジェネリック医薬品に関する適切な説明／推奨が可能に
- 重複検査の抑制も期待

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



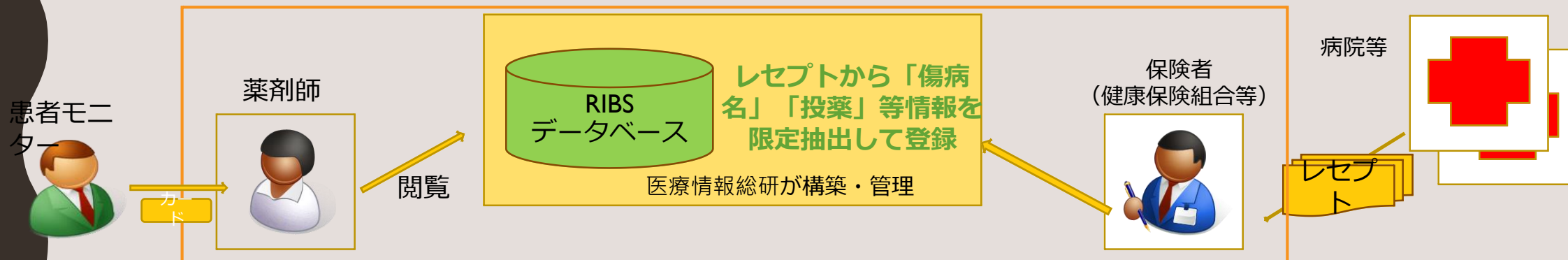
■ 情報の取得

- ・ 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。

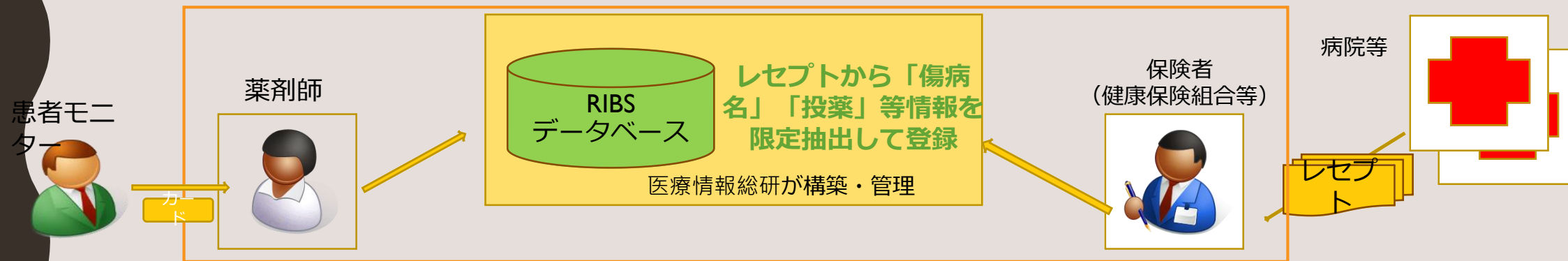
5 RIBSで個人情報はどう扱うか



■ 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）。

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ぬか

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

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ありますが、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。

他人に見られぬか

- 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に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。

1 1 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つが揃って初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。

1 2 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。

1 3 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

1 4 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。

1 5 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）
- ・ 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~~ プライバシーリングリスク対策（9 参

照） ・ 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、評価項目を決定しています。

1 7 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。

1 8 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。

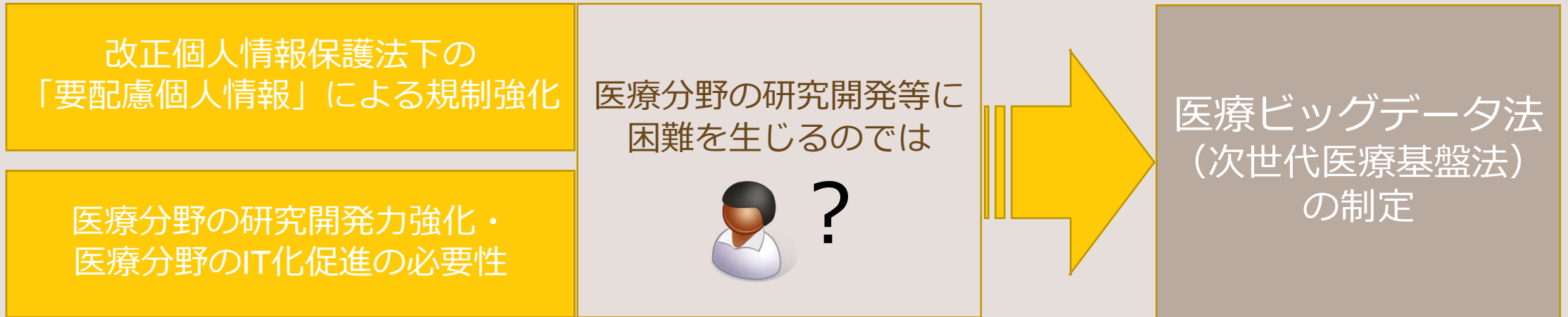
- RIBSは、公法人たる保険者が保有する個人情報、刑法上の守秘義務を負う薬剤師が閲覧する仕組みである。保険者、薬剤師ともに法的責任は重く、法制度面では十分プライバシー保護が担保されていると考えられる。RIBSを構築・運用する医療情報総研は民間事業者であるが、公法人たる保険者の個人情報をこれまでも取り扱ってきており、実績がある。医療情報総研における一層の従業者教育・従業者監督が重要である。
- RIBSは、医療の質のより一層の向上、患者の利便性の向上、そして療養担当者による療養に資する仕組みであり、個人情報を活用することの効果は公益・個益ともに大きいと考えられる。実証事業で得られた成果を踏まえ、RIBS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。



医療ビッグデータ法 (次世代医療基盤法)

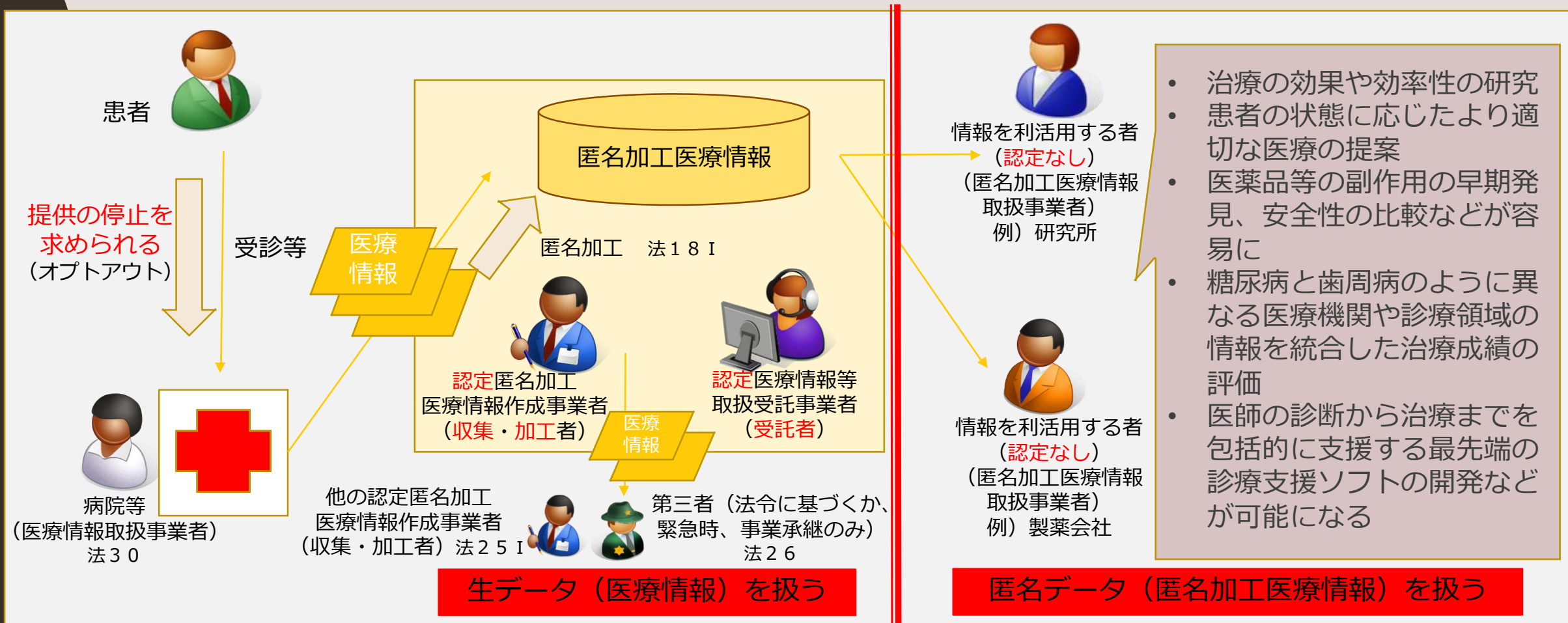
医療データを本人保護及び安全を確保しつつ
より容易に入手できる仕組み

医療ビッグデータ法の制定



- 改正個人情報保護法により、医療情報の多くが「**要配慮個人情報**」となり、規制が強化
 - ✓ 医療分野の研究開発等に困難を生じるという危惧
 - ✓ もっとも、改正個人情報保護法による変化は、オプトアウトの禁止のみ。学術研究の適用除外もある。
- 一方で、医療分野の研究開発力強化、医療分野のIT化促進の必要性
- そこで、改正個人情報保護法の**匿名加工情報とは異なる規律**として、医療ビッグデータ法（次世代医療基盤法）により、**匿名加工医療情報**をより容易に取得できるように改正。
 - ✓ もっとも、個人の不安払しょくのため、**大臣認定制度**を設け、**認定事業者については規制の大幅強化**し、かつ個人がこれに参加しないことを選択できる仕組み（**オプトアウト**）を設けた

匿名加工医療情報の全体イメージ



現状の課題と新法のポイント

現状の課題

- 現在、**全国規模**で利活用が可能な**標準化**されたデジタルデータは**レセプト**データが基本。診療行為の実施結果（**アウトカム**＝**検査結果**、**服薬情報**等）に関する標準化されたデジタルデータの利活用は、世界的にも重要な課題
- 医療サービス提供者や保険者等（一次ホルダー）に関しては、レセプトや特定健診等のデータを収集する仕組みが整備されつつあるが、**個別目的に基づいてシステムが構築**され**情報が分散**。そのため、人の**一生涯を通じた統合的**な健康管理や、**地域差**や**医療保険制度の違い**を踏まえた医療費等の分析が困難
- 研究機関や民間事業者等（二次ホルダー）を含めると、実際の情報流通経路は複雑・多岐。個人は、どこでどのように情報が扱われるのか**不安**が払拭できず、サービス提供者・事業者（一次・二次ホルダー）は、同意取得や匿名化を含めたデータ処理やシステム構築・運用のコストが負担

新法の背景

- 改正個人情報保護法により、ビッグデータ利活用のための「**匿名加工情報**」という規律が新設
- しかし医療情報は通常のデータとは異なる配慮が必要（**個益・公益のための研究等の必要性**、**データの機微性**）

新法のポイント

- 医療ビッグデータ法（次世代医療基盤法）により「**匿名加工医療情報**」を新設
- 研究等に必要なデータを**より容易に統合的に取得**できるように
- 一方で、**データの機微性等から**、**厳しい規律**に（**大臣認定制度**、**認定事業者への規制**の大幅**強化**、個人がこの制度に参加しないことを選択できる仕組み（**オプトアウト**）の導入）

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ある場合は不可（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ある場合は不可（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人情報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） ■ 公布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）	
	主務大臣による命令の可能性（37条5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）

認定事業者等の義務の比較

※利活用者は、 個人情報法の義務 に注意 ※8条3項2号「 提供能力 」で利活用者との契約基準等をチェックされる	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）	△※
従業員の監督	○（21条）	○（29条、21条）	×
従業員等の秘密保持義務	○（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）	×



その他データ関連政策

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

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、自分で住所をコピー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ー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イケないんだよ。

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・自治体を持つデータ（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。



オープンデータ

名称	概要
オープンデータ • http://www.soumu.go.jp/menu_seisaku/ictseisaku/ictriyou/opendata/opendata01.html • http://www.data.go.jp/	■ 非識別加工情報と同様に、国・自治体等が保有する公共データ等をビジネスで活用できるようにする仕組み。 ■ オープンデータも非識別加工情報も、原則として対象範囲に限定はないものの、オープンデータは、概して法令に基づく制度ではないため、人に対するデータというよりは、気象情報、地盤情報、運行情報、駅・バス停の位置情報、農水産物の栽培情報・検査情報・農薬情報、観光情報、公的施設情報などの、物・状態に対するデータがメインとも考えられる。非識別加工情報は、法令に基づく制度のため、個人情報保護のための手当てが法令上整理されており、物・状態に対するデータも対象ではあるが、それよりもさらに人に関するデータを入手しやすい。 ■ オープンデータの場合は、「人が読む」という利用形態に適したデータではなく、機械判読に適したデータでなければならない。非識別加工情報も、書面ではなく電子データで入手はできるものの、必ずしも機械での自動処理が容易な形式で提供されるものではない。 ■ 各行政機関・自治体等がどのようなデータを持っているかという「データカタログ」から入手したいデータを検索し、Webサイトから直接ダウンロードするなどの方法によってデータを取得できる。



まとめ・参考

まとめ

個人情報の保護

- 個人情報に関して絶対に守るべきポイントを押さえ、従業者・委託先に徹底する
 - ・ 自社の業種、社会からの信頼、持っている個人情報、トラブル事例を参考に
- 何を保護すべきか
 - ・ 個人情報、個人データ、保有個人データ、要配慮個人情報、プライバシー権、営業秘密などの様々な概念
 - ・ 技術的な定義よりも、**様々な観点から様々なデータが保護されている**ことをまず理解する
- 個人情報保護法のルール
 - ・ 取得、利用、提供、管理、本人からのアクセスというフェーズごとに考える
 - ・ 利用目的と第三者提供がポイント
 - ・ 同意がなければ、絶対に使えないというような法律ではない
 - ・ 全体的なルールを把握してから、細かい点を書籍やガイドライン、Q&Aで確認しよう

まとめ

個人情報の利活用

- **個人情報**というと、個人情報保護が大変というイメージも
 - 意外と思ひ込みであったりする。個人情報保護法もそこまで厳しい法律ではない。
- もっとも、個人情報を利活用すると、本人（個人、消費者等）に悪影響や被害が生じる恐れがあり、企業としては利活用を躊躇することも
 - そこで、いわゆる「ビッグデータ等」の利活用政策として、「**匿名加工情報**」「**非識別加工情報**」が法制化された
 - 個人情報よりも簡単な手続で利活用や外部提供ができる
 - 匿名加工情報は民間データ、非識別加工情報は官データ
 - 匿名加工情報/非識別加工情報でなくても、**個人情報のまま**でも目的内利用/目的外利用規制を満たせば**利活用が可能な場合もそれなりに広い（不適切な取り扱いを行わないよう注意）**
- 医療に関しては、**医療ビッグデータ法（次世代医療基盤法）**が整備された
- その他、データ利活用を容易化するための政策が今後も展開される見込み
 - 本人（個人、消費者等）保護とデータ利活用の両立のための政策・実践が行われている
 - グレーゾーン解消制度や個人情報リスク評価も活用できる

参考（書籍）

◆ 個人情報



「行政ビッグデータの取得・活用マニュアル」

（日本法令、2018年）

「1冊でわかる！改正早わかりシリーズ 個人情報保護法」

（労務行政、2017年）

◆ マイナンバー入門

要点



「Q&A番号法」（有斐閣、2014年）

「マイナンバーから病歴・犯罪歴がわかってしまうの？」「国が情報を一元管理していいの？」という疑問から、番号法の解釈要点まで、番号制度のポイントを1問1答形式で解説。上中級者向けにも。

簡単



「担当者の不安解消! マイナンバーの実務入門」（労務行政、2016年）

非法律家の実務担当者向けにかなり平易にマイナンバーを解説。

詳細



「逐条解説マイナンバー法」（商事法務、2017年）

制度・法律を網羅的に解説。500ページ超えの重厚解説書。

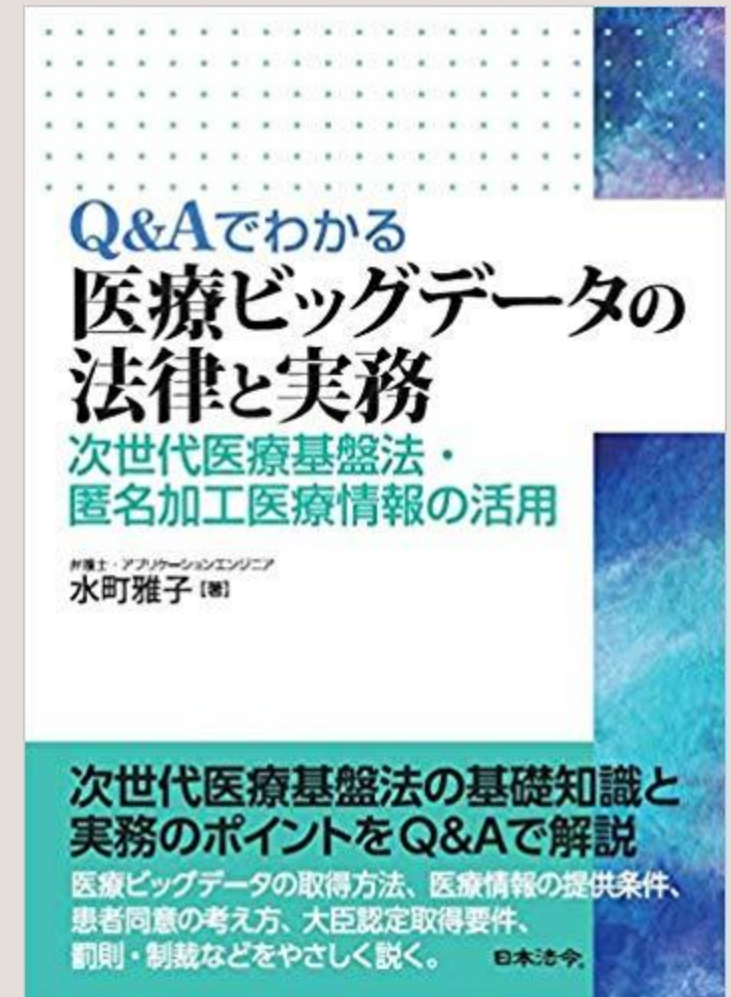
参考 (WEB)

◆ I Tをめぐる法律問題について考えるブログ

<https://cyberlawissues.hatenablog.com/>

◆ 各種参考資料を事務所Webにて公表中

- 個人情報保護に関する社内整備と 関連規程の見直し
<http://www.miyauchi-law.com/f/170313piikaiseigaiyou.pdf>
- 安全管理措置の比較
http://www.miyauchi-law.com/f/170906anzenkanrisochi_comparison.pdf
- 個人データの取得/提供時の記録様式
<http://www.miyauchi-law.com/f/teikyoutoukiroku.pdf>
- 医療ビッグデータ法の詳細概要
<http://d.hatena.ne.jp/cyberlawissues/20170816/1502870156>
- 個人情報リスク評価PIA++
<http://d.hatena.ne.jp/cyberlawissues/20180628/1530155730>



THANK YOU

個人情報、マイナンバー、PIA++、IT/ICT、規程策定、医療ビッグデータ法
（次世代医療基盤法）のご相談、大臣認定申請支援、国との交渉、
企業法務全般、条例策定支援その他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