資料５

民間ＰＨＲ事業者による健診等情報の取扱いに関する要件について
前回の意見を踏まえた考え方（案）

民間ＰＨＲ事業者による健診等情報の取扱いに関する要件　構成

１．対象情報及び対象者

２．情報セキュリティ対策

３．個人情報の適切な取扱い

４．健診等情報の保存・管理、相互運用性の確保

５．その他（要件遵守の担保方法など）

別紙　本指針の要件に係るチェックシート

1．対象情報及び対象者

1．対象情報及び対象者

前回の論点

- 民間利活用作業班で今回検討を行う民間PHR事業者の主たる対象情報及び対象事業者については以下の通りとする。

  ・対象情報：　マイナポータルの「自己情報取得API」等を活用して取得される情報など、国民自身が自らの健康管理に積極的に活用することを想定して提供されるものを想定＝健診等情報

  ・対象事業者：　健診等情報を取り扱うPHRサービスを提供する民間事業者

前回の主な意見

- 健診等情報を扱う事業者全般を対象とした議論ということでよいか。健診等情報を扱わず、ライフログしか扱わないという事業者は対象外としてよいか。

対象情報及び対象者の考え方（案）

- 対象情報：　マイナポータルAPI等を活用して入手可能な自身の健康診断等の個人情報保護法上の要配慮個人情報となる保健医療情報（以下「健診等情報」という）
  ※　具体例として、予防接種歴、乳幼児健診、特定健診、レセプト記載の薬剤情報等

- 対象者：　健診等情報を取り扱うPHRサービスを提供する民間事業者等

２．　情報セキュリティ対策

2．情報セキュリティ対策①

前回の論点

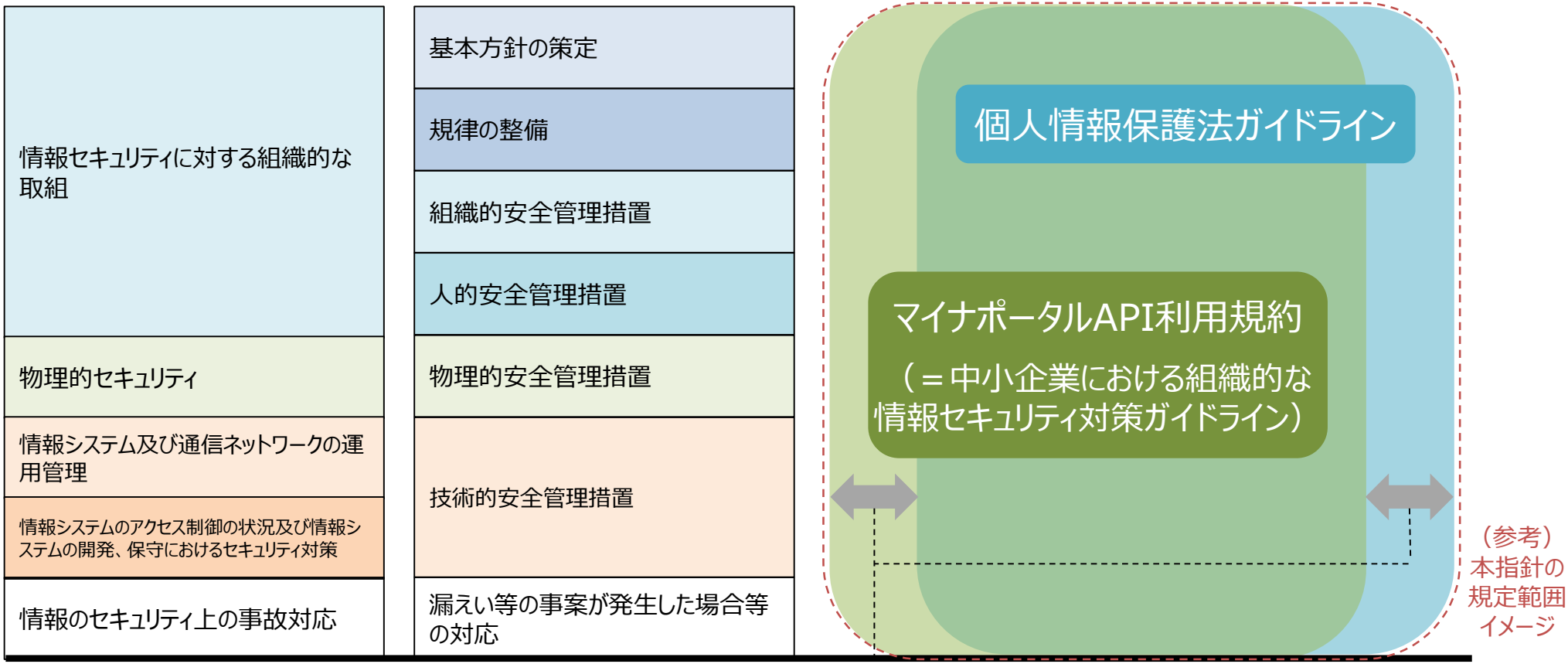
- 健診等情報は、国民が安心して民間PHRサービスを活用するためには、民間PHR事業者が一定の「情報セキュリティ」の水準等を満たすことが求められている。特に、今後、マイナポータルAPIを活用し、民間PHR事業者が取得することが見込まれることから、健診等情報を取り扱う場合においても一定のセキュリティ基準の確認が望ましいのではないか。
- なお、マイナポータルAPIに接続できる事業者については、「マイナポータルAPI利用規約　第3条2項2号と3号」で、機密性の保持や情報セキュリティ要求事項の遵守を求めている。また、「マイナポータルAPI利用条件確認書」の「情報セキュリティに対する組織的な取組状況」や「物理的セキュリティ」などにおいて、IPA（情報処理推進機構）の「中小企業における組織的な情報セキュリティ対策ガイドライン」の確認を求められている。

前回の主な意見

- 「中小企業における組織的な情報セキュリティ対策ガイドライン」の「４共通して実施すべき対策」はそれほど特殊なことが書かれているわけではなく、基本的なセキュリティ基準である。
- マイナポータルAPI利用条件記載のセキュリティ基準に加えて、要配慮情報が含まれる健診等情報を扱う事業者としてのプラスしたセキュリティ基準が必要。

2．情報セキュリティ対策②

差分についての概念図（イメージ）



各項で提示される具体の対策には一部相違点あり

例）中小企業における…ガイドラインは、対象として想定する中小企業の取り扱う情報の種類や保管状況、リスクなどの状況を踏まえて策定されており、通則にはない自然災害や人的災害対策（転倒やケーブルの引っ掛け防止など）を規定する一方、通則では規定されている個人データの取扱状況の把握及び安全管理措置の見直しについて明記されていない　等

2．情報セキュリティ対策③

健診等情報を扱う民間PHR事業者に求められる考え方（案）

※制度上の要求事項へ上乗せする事項は★

- 個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、リスクに応じて、必要かつ適切な安全管理措置を講じなければならず、また、個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組むべき。
- 講ずべき安全管理措置として、基本方針の策定、個人データの取扱いに係る規律の整備、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置、漏えい等の事案が発生した場合等の対応、に相当する内容が挙げられるべき。
- リスクマネジメントシステムを構築する上で、標準規格（ISO及びJIS）等を参考にすることや、それに基づいた第三者認証（ISMS及びプライバシーマーク等）を取得することに努めるべき。（★）

３．個人情報の適切な取扱い

３．個人情報の適切な取扱い①

前回の論点

- 健診等情報の利用目的等については、民間PHR事業者は、利用目的の適切性についても留意し、わかりやすい形で提示した上で適切に同意取得されることが望ましいのではないか。
- 民間PHR事業者が、その他の民間PHR事業者に対して健診等情報を提供・連携する際には、提供先について、利用目的に応じた適切な同意の取得を検討すべきではないか。（例えば、同じ情報であっても、診療所での閲覧や、地域医療連携ネットワークシステムにおける活用など、利用目的に応じた同意）
- マイナポータルAPI経由での健診等情報は、事業の終了や同意の撤回がなされた場合、適切に消去されることが望ましいのではないか。その際、同意の撤回は同意を与えるのと同程度の容易さで行えることが望ましいのではないか。

前回の主な意見

（同意取得に関する前提）
- 民間PHR事業者が第三者に提供してしまった後で、本人が事後的に情報の重要性に気付くということもある。説明の在り方・同意の取り方については十分に議論が必要。
- 同意取得した情報について、民間PHR事業者の利用規約が変更された場合の取扱いについて検討が必要。

(一次・二次利用における同意取得に関して)
- 二次利用においては本人が利用用途について必ずしも完全に理解できないということが出てくる。同意という行為がある以上は十分な説明が大前提。
- 純粋な一次利用と、二次利用の中に公益利用と民間利用があるので、考慮すべきではないか。
- 一次の中にも同意をどのレベルまで求めていくのかが変わってくるのではないか。
- 二次利用・第三者提供については健診等情報以外の情報との整合性も考慮する必要がある。まずは一次利用の同意・説明の仕方について議論すべきではないか。
- 一次利用、二次利用に関して、現在、PHRサービスが綺麗に分かれないと思われる。
- 本作業班の対象情報は「国民自身が自らの健康管理に積極的に活用することを想定して提供されるもの」。自身の情報を活用する仕組みは、第三者提供に当たらない。二次利用は本人の意図でない情報の利活用をPHR事業者が提案する場合であり、これは「国民自身が自らの健康管理に積極的に活用することを想定して提供されるもの」から外れる。
- 個人を識別できる情報と匿名加工した情報を切り分けて議論することが必要。

3．個人情報の適切な取扱い②

個人情報保護法で事業者の義務とされている事項

個人情報保護法上において、利用目的の通知又は公表の義務を明記。利用規約やプライバシーポリシーの掲載義務までは記載なし。

	個人情報の保護に関する法律についてのガイドライン（通則編）
要配慮個人情報に関連する事業者の義務とされている事項（利用目的の特定と通知又は公表に関するもの）	■ 法第18条 第1項 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、 速やかに、**その利用目的を、本人に通知し、又は公表しなければならない。** 「公表」とは、広く一般に自己の意思を知らせること（不特定多数の人々が知ることができるように発表すること）をいい、公表に当たっては、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならない。 「公表に該当する事例」 • 事例1）**自社のホームページのトップページから１回程度の操作で到達できる場所への掲載** • 事例2)自社の店舗や事務所等、顧客が訪れることが想定される場所におけるポスター等の掲示、パンフレット等の備置き・配布 • 事例3)（通信販売の場合）通信販売用のパンフレット・カタログ等への掲載

（参考）個人情報の保護に関する法律についてのガイドライン（通則編）において、「プライバシーポリシー」の掲載は、以下の事例で記載されているのみ。

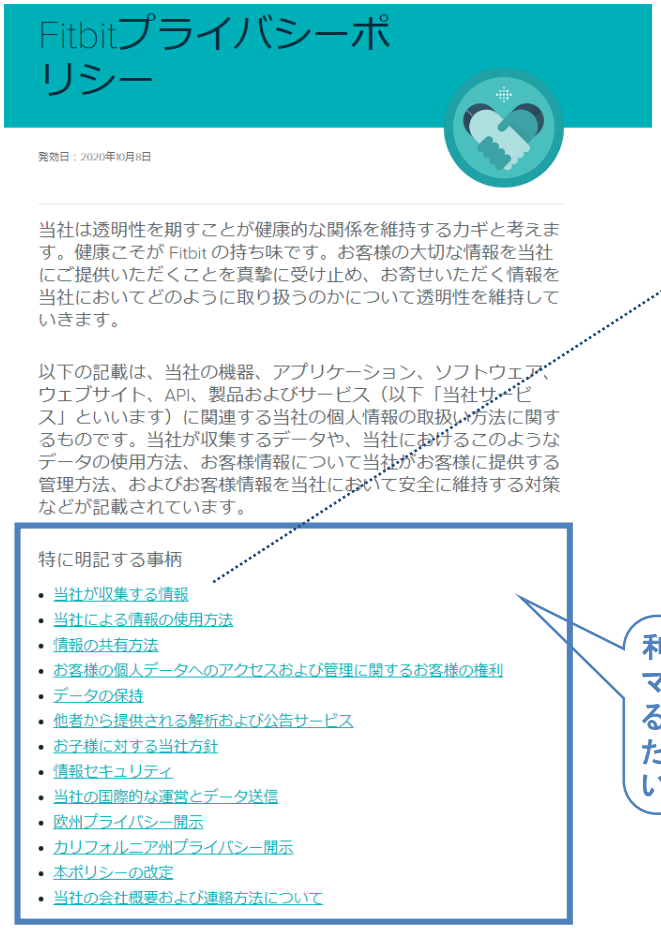
■個人情報の取扱いに関する苦情処理（法第35条関係）
- 個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない
- 個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない

（※1）消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するためには、**「個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）」を策定し、それをホームページへの掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することや、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることも重要**である。

3．個人情報の適切な取扱い③

必要な情報を全体的に提供すると同時に、概要版などをあわせて分かりやすく伝えている事例

プライバシーポリシーとは、事業者が個人情報も含めたプライバシーに関する情報の取扱方針を定めた文書。ホームページ上に掲載。



Fitbitプライバシーポリシー

発効日：2020年10月8日

当社は透明性を期すことが健康的な関係を維持するカギと考えます。健康こそが Fitbit の持ち味です。お客様の大切な情報を当社にご提供いただくことを真摯に受け止め、お寄せいただく情報を当社においてどのように取り扱うのかについて透明性を維持していきます。

以下の記載は、当社の機器、アプリケーション、ソフトウェア、ウェブサイト、API、製品およびサービス（以下「当社サービス」といいます）に関連する当社の個人情報の取扱い方法に関するものです。当社が収集するデータや、当社におけるこのようなデータの使用方法、お客様情報について当社がお客様に提供する管理方法、およびお客様情報を当社において安全に維持する対策などが記載されています。

特に明記する事柄

- 当社が収集する情報
- 当社による情報の使用方法
- 情報の共有方法
- お客様の個人データへのアクセスおよび管理に関するお客様の権利
- データの保持
- 他者から提供される解析および公告サービス
- お子様に対する当社方針
- 情報セキュリティ
- 当社の国際的な運営とデータ送信
- 欧州プライバシー開示
- カリフォルニア州プライバシー開示
- 本ポリシーの改定
- 当社の会社概要および連絡方法について

利用規約項目のサマリーも記載している為、利用者が読みたい項目を選びやすい

出所：Fitbit HP

当社が収集する情報

お客様が当社サービスをご利用いただくと、当社は以下の種類の情報を収集します。

お客様が当社に提供する情報

アカウント情報
当社サービスにおけるアカウントを作成する際には、特定の情報を提供していただくことになります。この情報の内容として、氏名、メールアドレス、パスワード、生年月日、性別、身長、体重等のほか、場合によって携帯電話番号が必要になることがあります。当社のアカウントを作成する際に提供が必要な情報は、これ以外にはありません。なお、任意で、その他の種類の情報、例えば顔写真、経歴、国に関する情報、およびコミュニティ内でのユーザー名等を提供することもできます。

追加情報
また、使い勝手を改善し、本サービスの特定の機能を有効にするために、食品、体重、睡眠、水分、女性の健康状態、アラーム、およびディスカッション掲示板などの追加情報を任意で提供することもでき、これらを本サービスでの友人に送ることもできます。

さらに、お友達のメールアドレスの提供、ソーシャルネットワークのアカウントへのアクセス、またはお客様のモバイル機器の連絡先リストを使用することによって、当社サービス上でお友達とつながったり、まだ入会していないお友達を招待することも可能です。当社ではお客様の連絡先リストは保存されません。お客様の連絡先リストは、お客様がお友達をリストに追加するために使用した後、消去されます。

お客様が当社に連絡する場合やアンケート、コンテスト、販促活動などに参加する場合、当社はお客様が提供する氏名、連絡先、メッセージなどの情報を収集します。

３．個人情報の適切な取扱い④

利用規約における個人情報の公表事例

利用規約とは、PHRサービスを提供する民間PHR事業者が、PHRサービスを利用する際の条件に関して明記された文書であり、任意で公表している。個人情報の取扱いに加えて、PHRサービスの内容、禁止事項等が記載されている。

パーソナルカラダサポート利用規約

パーソナルカラダサポート利用規約（以下「本規約」といいます。）は、ソフトバンク株式会社（以下「当社」といいます。）が提供する本サービス（第１条（定義）に規定します。）を利用する場合に、お客様に適用される条件を定めたものです。本サービスを利用する場合は、本規約の内容を必ず事前にご確認頂き、ご同意の上ご利用ください。本規約にご同意頂くことができない場合は、本サービスを利用することはできません。

第１条（定義） 本規約において使用する用語は、次の各号に掲げる意味として用いるものとします。

(1) 「本サービス」とは、当社が「パーソナルカラダサポート」の名称の下で提供する、お客様の歩数、体重及び睡眠時間等の健康情報の記録及び管理、並びにヘルスケアに関連した特典の提供を受けることができるサービス等の総称をいいます。

第 20 条（情報の利用目的等）

1. 当社は、本情報について、次の各号に定める目的に従って利用するほか、当社プライバシーポリシー（http://www.softbank.jp/corp/group/sbm/privacy/）に従って取扱います。
   (1) お客様からの問い合わせへの対応及び当社のサービスの利用に関する手続きのご案内や情報の提供等のカスタマーサポートのため
   (2) お客様の利便性の向上、品質改善及び有益なサービスの提供を目的として、利用状況の分析、効果測定、その他各種マーケティング調査及び分析を行うため並びに個人が識別できない状態で第三者へ提供するため
   (3) 当社及び第三者のサービス等の案内のため
   (4) 当社が提供する特典の適用の有無を識別するため
   (5) 当社のサービスの不正契約・不正利用（不正 ID 取得）の防止及び発生時に調査等を行うため
   (6) 個人が特定できない範囲で、統計データ等として活用するため
   (7) その他、当社のサービスを提供するために必要な業務のため
2. 当社は、Google Inc.及びその完全子会社に対して、本アプリに含まれる Google Analytics™により、本情報の一部を提供するものとします。
3. Google Inc.及びその完全子会社は、前項に基づき受領した本情報の一部を Google Inc.のプライバシーポリシーに従い利用するものとします。

（出典：パーソナルカラダサポート利用規約）

健康相談ポケットドクターサービス利用規約
（一般ユーザーの方）

第1条（規約の適用）

株式会社オプティム（以下「当社」といいます。）とMRT株式会社（以下「MRT」といいます。）は、この健康相談ポケットドクターサービス利用規約（以下「本規約」といいます。）により予約相談サービス（以下「本サービス」）を提供します。本サービスは、遠隔による医療健康相談を行うことを目的としています。本サービスの利用者（以下「利用者」といいます。）は、自己の責任において本サービスを利用してください。本サービスの利用、相談に対する回答やアドバイスにより何らかの不都合、不利益が発生し、また

第18条（情報の収集と利用）

第19条（保存情報・個人情報の保護）

（出典：健康相談ポケットドクターサービス利用規約）

3．個人情報の適切な取扱い⑤

公表情報等に基づき、第三者が企業の取組みを評価している事例

CDP（Carbon Disclosure Project）による企業評価

■ CDP（Carbon Disclosure Project）とは

- 企業・政府の温室効果ガス排出量削減による森林保護推進を目的とした、国際的な非営利団体で、世界の時価総額50%以上を占める7,000社以上の企業の環境データを保有
- 「気候変動」等に対する取り組みを、開示の透明性、環境問題への認識、リスク低減・機会実現の管理、リーダーシップの観点から評価（最高ランクから順にA、A-、B、B-、C、C-、D、D-の8段階）

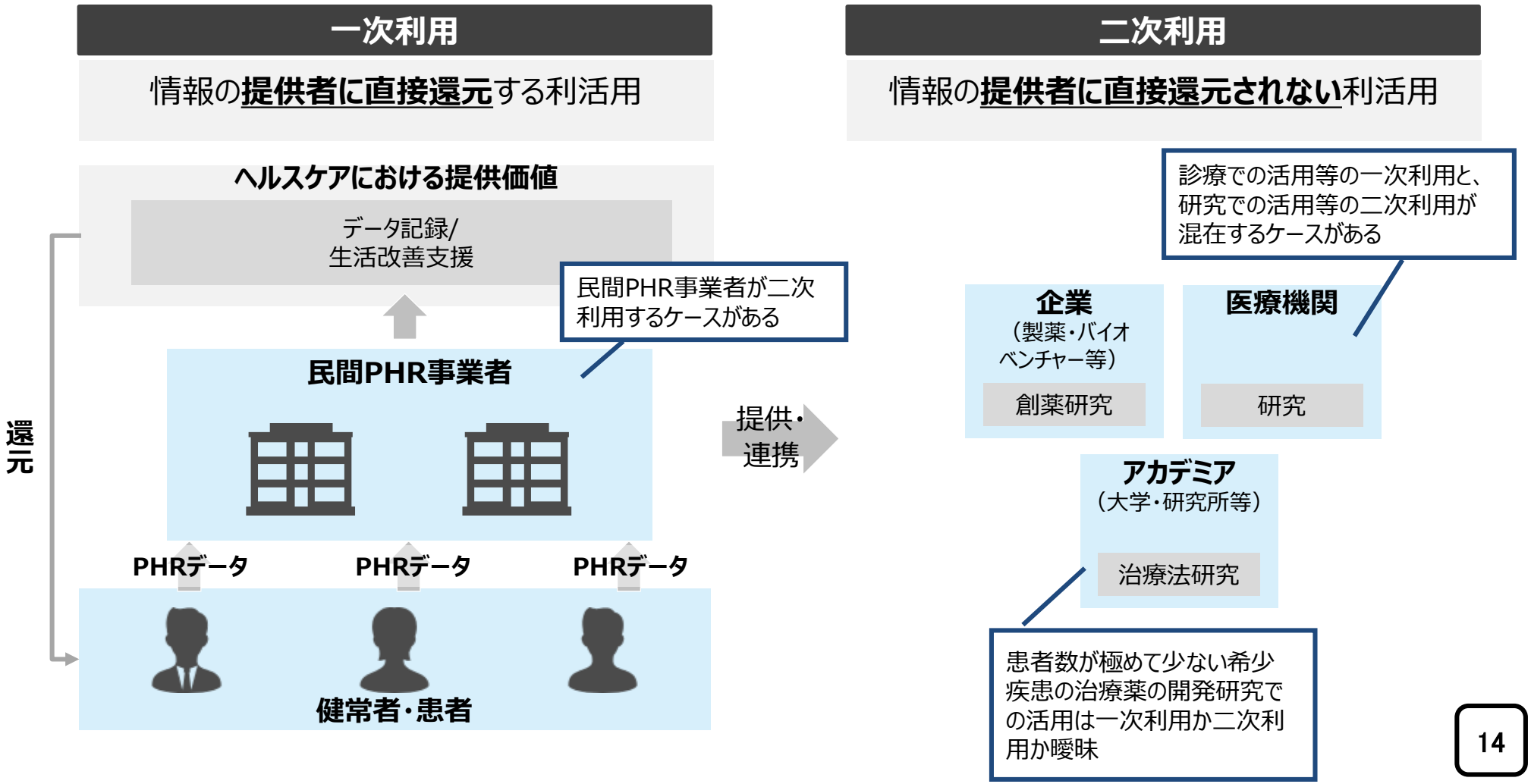
2018 CDPランク（気候変動）

A-ランク企業（例）	Aランク企業（例）
KONICA MINOLTA NTT DATA NOMURA DAIFUKU ASKUL	MARUI GROUP MS&AD INSURANCE GROUP SOMPO ホールディングス 戸田建設 TODA CORPORATION 小野薬品工業株式会社

3．個人情報の適切な取扱い⑥

一次利用と二次利用の考え方

一次利用とは情報の提供者に直接利用結果を還元する方法であり、二次利用とは研究開発用途など情報提供者に直接利用結果を還元しない方法である。なお、現状は二次利用を目的とした第三者提供では、匿名加工しているケースがほとんどであり、この場合は個人情報保護法上の個人情報とならない。



3．個人情報の適切な取扱い⑦

一次利用として医療機関に自身の情報を掲示する場合に、同意を取得している事例

（出典：エムティーアイ）

3．個人情報の適切な取扱い⑧

匿名加工した上で、二次利用として提供しているが、丁寧に本人同意を取得している事例

研究参加の同意

同意の撤回の方法

（出典：エムティーアイ）

3．個人情報の適切な取扱い⑨

＜個情法上の個人情報を第三者提供する場合＞
提供先毎に同意取得する例

ステップ1

以下の事業者があなたの個人情報へのアクセスを求めています。同意しますか？

マイナポータル

要配慮情報を扱う事業者

アプリA

目的	同意
データ取得	
第三者提供	

ステップ2

以下情報を提供します

予防接種歴
特定健診
薬剤情報

ステップ3

例1　提供先毎に同意

企業名等が多数表示されることになる。ユーザーが確認する際、分かりにくいと感じる可能性がある。

提供先一覧	同意
AAに関する研究	
A大学	
B大学	
C大学	
D大学	
…	
Z企業	
BBに関する研究	
A企業	
B企業	
C企業	
D企業	
E企業	
D企業	
C製薬会社の創薬に関する研究	
…	

拒否　許可

内容等の説明を表示

研究内容
AAに関する研究として、…

（※同意ボタンや ⓘ ボタンを押すとポップアップ）

3．個人情報の適切な取扱い⑩

＜個情法上の個人情報を第三者提供する場合＞ 利用目的毎に同意取得する例

ステップ1

以下の事業者があなたの個人情報へのアクセスを求めています。同意しますか？

マイナポータル

要配慮情報を扱う事業者

アプリA

目的	同意
データ取得	
第三者提供	

ステップ2

以下情報を提供します

予防接種歴
特定健診
薬剤情報

ステップ3

例2　利用目的毎に同意

利用目的毎に表示。「i」をクリックすることで詳細（内容、提供先等の説明）を表示、確認できる。

提供先（目的別）	同意
AAに関する研究	
BBに関する研究	
C製薬会社の創薬に関する研究	
：	

内容、提供先等の説明を表示

研究内容
AAに関する研究として、・・・
提供先
A大学
B大学
C大学
・・・

内容、提供先等の説明を表示

研究内容
C製薬会社における創薬に関する研究として、・・・ ・糖尿病に関する創薬研究 ・高血圧疾患病に関する創薬研究 ・・・ ・・・

（※同意ボタンやⓘボタンを押すとポップアップ）

３．個人情報の適切な取扱い⑪

健診等情報を扱う民間PHR事業者に求められる考え方（案）

※制度上の要求事項へ上乗せする事項は★

＜情報の公表＞
- 第三者が評価できるよう、プライバシーポリシーやサービス利用規約をHPに掲載するなどにより、わかりやすく公表するべき。（★）

＜同意取得＞
- 健診等情報の同意取得に当たっては利用目的をできる限り特定し、利用目的や範囲等について、例えばサービス利用規約の要約を提示するなど、わかりやすく通知すべき。（下線部分が★）
- 特に、利用目的に第三者提供を含む場合は、利用目的、提供される個人情報の内容や提供先等を特定し本人の同意を得るべき。（下線部分が★）

＜消去・撤回＞
- 事業終了等により健診等情報の利用が必要なくなった場合又は本人の求めがあった場合、事業者が管理している健診等情報を消去するべき。（下線部分が★）
- 同意の撤回について、本人が容易に行えるようにする工夫を講じるべき。（★）
- 利用者によるアクセスがなく、長期間利用されていない健診等情報の取扱いについては、各事業者において考え方を整理し公表するべき。（★）

＜その他＞
- 第三者提供をする場合等、提供先事業者が本ガイドラインのセキュリティ及び適切な個人情報の取扱いについて同等の対策を行っている事業者であることを上述したＨＰ等での公表内容または第三者認証の取得状況等により確認するよう努めるべき。（★）

４．健診等情報の保存･管理、相互運用性の確保

４．健診等情報の保存・管理、相互運用性の確保①

前回の論点

- 健診等情報については、本人がサービスを乗り換えた場合であっても、自らの健康管理を継続的に活用できるよう、ポータビリティの確保が望ましいのではないか。例えば、本人に対して健診等情報を利用可能な形式でエクスポートでき、その情報について事業者はインポートできる機能を用意することが望ましいのではないか。
- マイナポータルAPI経由による健診等情報の本人へのエクスポートのフォーマット等は、マイナポータルから出力されるフォーマット等と同様とすることが望ましいのではないか。
- 事業者間でマイナポータルAPI経由による健診等情報を移転させる場合には、両事業者ともマイナポータルAPI経由の健診等情報を取り扱うことが許された事業者又は一定の要件遵守が証明された事業者が望ましいのではないか。

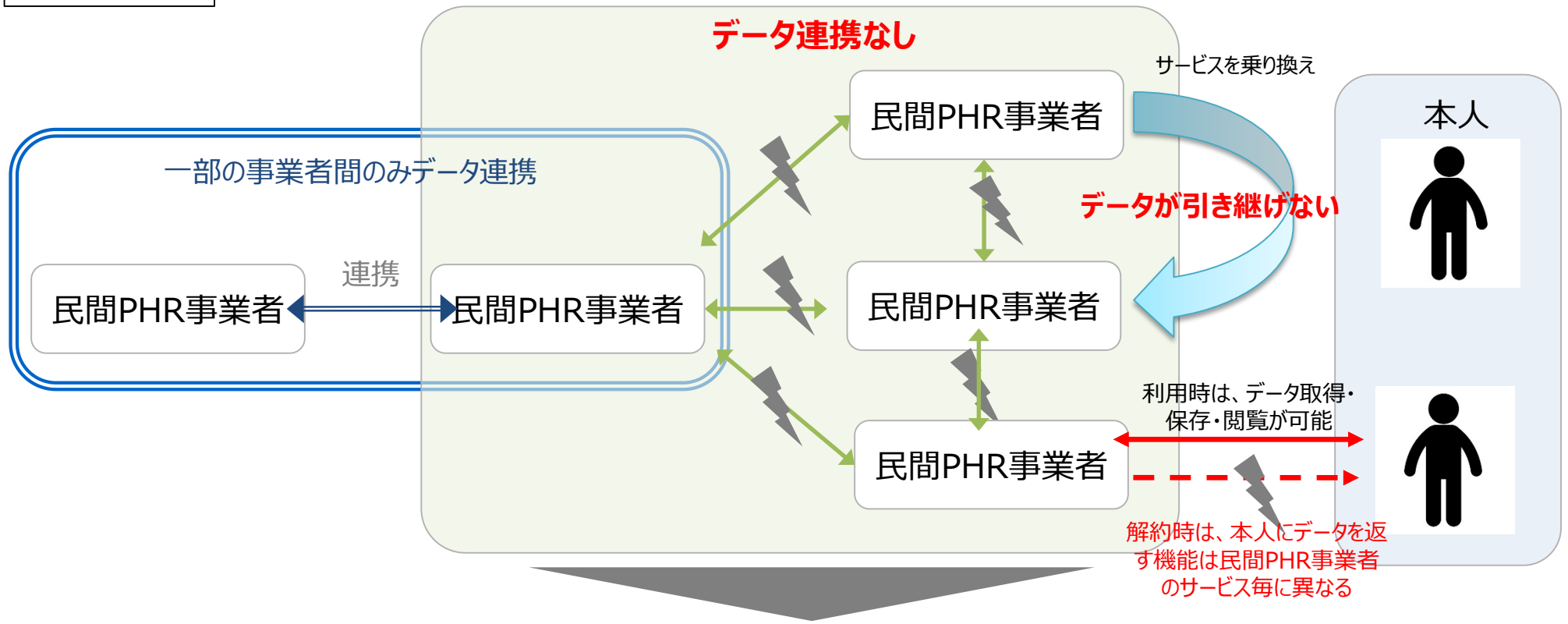
前回の主な意見

- 健診等情報はあくまで本人の情報なので、民間PHR事業者が廃業する場合には、次の事業者に適切に引き継げるようにする必要がある。
- 一方の民間PHR事業者が廃業した場合に、もう一方の民間PHR事業者に健診等情報がスムースに移行できるのが望ましいので、こういうケースを一次利用・二次利用という言い方で整理するのは実態にそぐわなくなってしまう。

４．健診等情報の保存・管理、相互運用性の確保②

現状、事業者間の互換性は技術的な課題やデータフォーマット等の理由により一部の事業者間のみとなっている。

現状のイメージ図



１．事業者間(N対N)において標準的なフォーマット(項目粒度・名称、単位等)やファイル規格/拡張子等が統一されておらず、互換性の確保が困難
２．民間PHR事業者が、①データ取得も含めたサービスの設計、②利用者がサービスの乗換を前提としていない、③明確な枠組み・ルールもない、ことからサービス利用・終了後の本人への提供が困難

４．健診等情報の保存・管理、相互運用性の確保③

健診等情報のポータビリティについての概念図

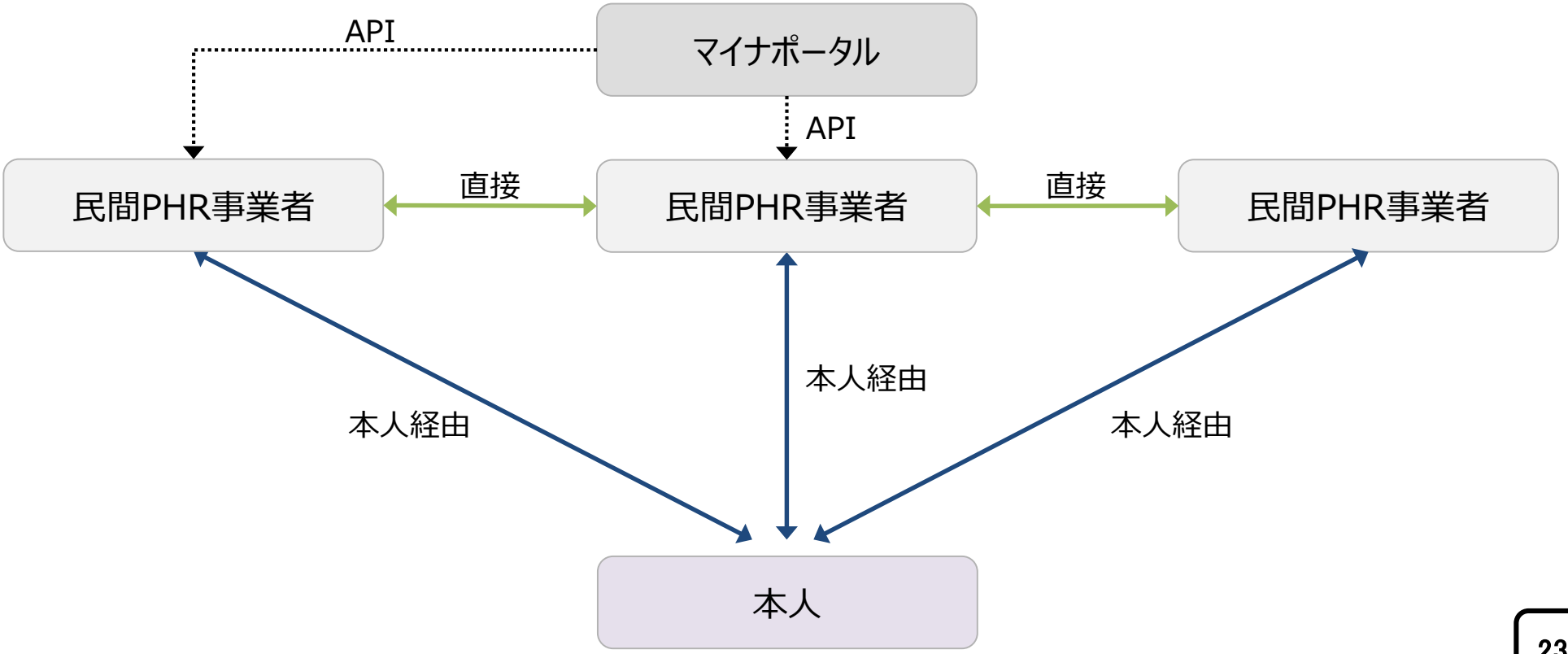
【凡例】 ◀……考え方(案)　マイナポータルAPIを経由したデータ取得

↔ 考え方(案)　**本人を介したデータ※の引継ぎ**
- 本人へのデータのエクスポート
- 本人からのデータインポート

※マイナポから出力されるフォーマット等と同様

↔ 考え方(案)　**個人の同意を前提とした民間PHR事業者間の直接的なデータ連携**

※API連携の通信規格や交換形式は業界による整備が望ましい。データ連携先事業者の一定の要件遵守の確認は必要



４．健診等情報の保存・管理、相互運用性の確保④

健診等情報を扱う民間PHR事業者に求められる考え方（案）

※制度上の要求事項へ上乗せする事項は★

- 健診等情報について、民間PHR事業者から本人へのエクスポート機能及び本人から民間PHR事業者へのインポート機能について備えるべき。（★）
- その場合の健診等情報のフォーマット等は、マイナポータルから出力されるフォーマット等と同様とするなど社会通念上一般的なデータファイルで扱うことができるようにすべき。（★）
- 民間PHR事業者間での健診等情報の直接的なデータ連携については、本人にとっての利便性向上や事業者にとっての対応コスト等も考慮しつつ、事業者間での連携の拡大に努めるべき。（★）

  ※なお、現在民間PHR事業者Aを利用しているユーザーが民間PHR事業者Bに乗り換える場合、データ連携をした上で、民間PHR事業者Aは情報を消去する。
- 民間PHR事業者間でのAPI連携の通信規格や交換形式は業界による標準化に取り組むよう努めるべき。民間PHR事業者間での直接的なデータ連携時には、データ連携先事業者が本指針の要件を満たしていることを確認すべき。（★）
- 健診等情報を取り扱うサービスを事業終了する場合、本人への当該健診等情報のエクスポート及び他の民間PHR事業者への当該健診等情報のエクスポートが実施可能な期間を十分に確保するべき。（★）

５．その他（要件遵守の担保方法など）

５．その他（要件遵守の担保方法など）①

前回の論点

- マイナポータルAPIに接続できる事業者は社会的信用が必要とされ、「マイナポータルAPI利用規約　第3条2項1号」で刑法等の違反がないことを求めている。
- その他、健診等情報の取扱う事業者として、社会的信用として必要とされるものはないか？

前回の主な意見

- 特に意見無し

健診等情報を扱う民間PHR事業者に求められる考え方（案）

※制度上の要求事項へ上乗せする事項は★

- マイナポータルAPIに接続できる事業者は社会的信用が必要とされ、「マイナポータルAPI利用規約　第3条2項1号」にあるとおり、刑法等により罰せられ、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５年を経過しない者がいないこと。
- 上記に加えて、マイナポータルAPIに接続できる事業者は、個人情報保護法の規定により刑に罰せられ、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５年を経過しない者がいないこと。（★）

※本指針、または、マイナポータルAPI利用規約に追加

５．その他（要件遵守の担保方法など）②

前回の論点

- 健診等情報の取り扱う民間PHR事業者に求められる要件を「証明する仕組み」についても、検討が求められている。
- 例えば、民間PHR事業者による業界団体においても、行政や関係団体の協力を得つつ、「証明」を行うことが考えられるが、①現状、業界団体といえるような団体があるのか、②情報セキュリティや個人情報の適切な取扱いなどの「証明」について、どのように行うべきか、等検討が必要ではないか。
- なお、このような「証明」の仕組みの構築には一定期間を要することから、経過措置としてどのような対応が考えられるか、検討が必要ではないか。

前回の主な意見

- 国が基本的なルールをつくり、業界団体が立ち上がるまでの間は、各事業者が自己チェックすることになるが、その場合も、自己チェックの支援や相談に関して第三者機構が行う。業界団体が立ち上がれば、自主的なガイドラインをつくり、その上で第三者的なチェックを行うという、全体的なスキームが必要なのではないか。

５．その他（要件遵守の担保方法など）③

健診等情報を扱う民間PHR事業者に求められる考え方（案）

※制度上の要求事項へ上乗せする事項は★

- 対象事業者は、自己チェックシート（別紙）に沿って本指針の各要件を満たしているかどうかを確認し、点検後のチェックシートを自社のＨＰで公表すべき。（★）
- 国が定める本指針に加えて、民間PHR事業者間での直接的なデータ連携時の通信規格や交換形式の標準化、リコメンドの有効性確保等を業界で検討した上で、より高い水準を目指すサービスガイドラインを作成することが望ましいのではないか。その際、第三者による証明が行われることがより望ましく、具体的な証明方法については業界によって検討されるのが望ましいのではないか。

５．その他（要件遵守の担保方法など）④

本指針に加えて、サービスガイドラインを策定する場合のイメージ（案）

より高い水準を目指すサービスガイドライン

（サービスガイドライン）

※基本的指針で規定する要件よりもより高い水準（事業者間での直接的なデータ連携時の通信規格や交換形式の標準化、リコメンドの有効性確保等）を目指すサービスガイドライン。

より高い水準を目指すサービスガイドライン
（第三者認証等）

民間ＰＨＲ事業者による健診等情報の取扱いに関する基本的指針

（基本的指針）

▲国の指針策定
（20年度中を目途）

本指針で規定する要件の確認
（チェックシート活用）

20年度　　21年度以降

別紙　本ガイドラインの要件に係るチェックシート項目（例）

項目番号		内容	チェック
1		情報セキュリティに関する経営者の意図の明確化	
	1-1	経営者が関与した上で、情報セキュリティポリシーを策定していますか	
	1-2	情報セキュリティポリシーの実現に対して、経営者が責任を持っていますか	
	1-3	情報セキュリティポリシーを定期的に見直していますか	
2		情報セキュリティ対策に関わる責任者と担当者の明確化	
	2-1	責任者として情報セキュリティと経営を理解する立場の人を任命していますか	
	2-2	責任者は、各セキュリティ対策について（社内外を含め）、責任者、担当者それぞれの役割を具体化していますか	
	2-3	責任者は、上記で具体化した役割について、適切に実施するよう徹底させていますか	
3		管理すべき重要な情報資産の区分	
	3-1	サービスに係るリスクの分析を行っていますか	
	3-2	分析により特定されたリスクに対して、必要な対応措置等を講じていますか	
	3-3	管理すべき重要な情報資産を、他の情報資産と分類していますか	
	3-4	資産について、台帳管理等により所在確認等を行う旨を定めていますか	
	3-5	情報資産の管理者を定めていますか	
	3-6	重要度に応じた情報資産の取り扱い指針を定めていますか	
	3-7	重要な情報資産を利用できる人の範囲を定めていますか	
	3-8	PHRサービスを提供する上で管理すべき情報については、独自の区分を設定していますか	
4		重要な情報の、入手、作成、利用、保管、交換、消去、破棄における取り扱い手順の整理	
	4-1	各プロセスにおける取扱いの作業手順を明確化していますか	
	4-2	各プロセスの担当者は、上記手順に基づいて適切に作業を行っていますか	
	4-3	重要な情報に対して、漏洩や不正利用を防ぐ保護対策を行っていますか	
5		外部の組織と情報をやり取りする際の、情報の取り扱いに関する注意事項に関する合意の取得	
	5-1	契約書や委託業務の際に取り交わす書面等に、情報の取扱いに関する注意事項を含めていますか	
6		個人データの取扱いを委託する場合の安全管理措置の確保	
	6-1	自らが講ずべき安全管理措置と同等の措置が講じられるよう、監督を行っていますか	
7		従業者（派遣を含む）への、セキュリティに関する就業上の対応の明確化	
	7-1	従業者を採用する際に、守秘義務契約や契約書を交わしていますか	
	7-2	従業者が遵守すべき事項を明確にしていますか	
	7-3	違反を犯した従業員に対する懲戒手続きが整備されていますか	
	7-4	在職中及び退職後の機密保持義務を明確化するため、プロジェクトへの参加時など、具体的に企業機密に関する際に、退職後の機密保持義務を含む契約書を取っていますか	
8		情報セキュリティに関するルールの周知及び情報セキュリティに関わる知識取得機会の確保	
	8-1	最新のポリシーや関連規程を従業員に理解させていますか	
	8-2	実践するために必要な教育を定期的に行っていますか	

※チェックシートの項目毎にチェックするための、具体的に定めている書類や整えるべき書類について、指針で例示