

## 健診等情報を取り扱う民間PHR事業者に求められる要件についての論点整理

---

# 1. 検討の対象

# 検討の対象とする民間PHR事業者及び対象情報

- 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

## **2. 健診等情報を取り扱う民間 P H R 事業者の要件についての論点**

## 2 - 1 情報セキュリティ対策

# 情報セキュリティ対策

- 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と。
- なお、マイナポータルAPIに接続できる事業者については、「マイナポータル自己情報取得 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、「マイナポータル自己情報取得 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。

区分	項目
情報セキュリティ	マイナポータルAPI経由で取得した健診等情報は、本人同意を得た期間に限り保持し、及び本人同意を得た目的に限り利用し、並びにその機密性を維持すること。
	「マイナポータル自己情報取得 API利用規約」において別途内閣府大臣官房番号制度担当室が定められている情報セキュリティ要求事項(「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」など)を遵守すること。

## **2 - 2 個人情報**の適切な取扱い

# 適切な利用目的、同意の取得、撤回方法、データ消去

- 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。

## (例) 連携先の同意と撤回

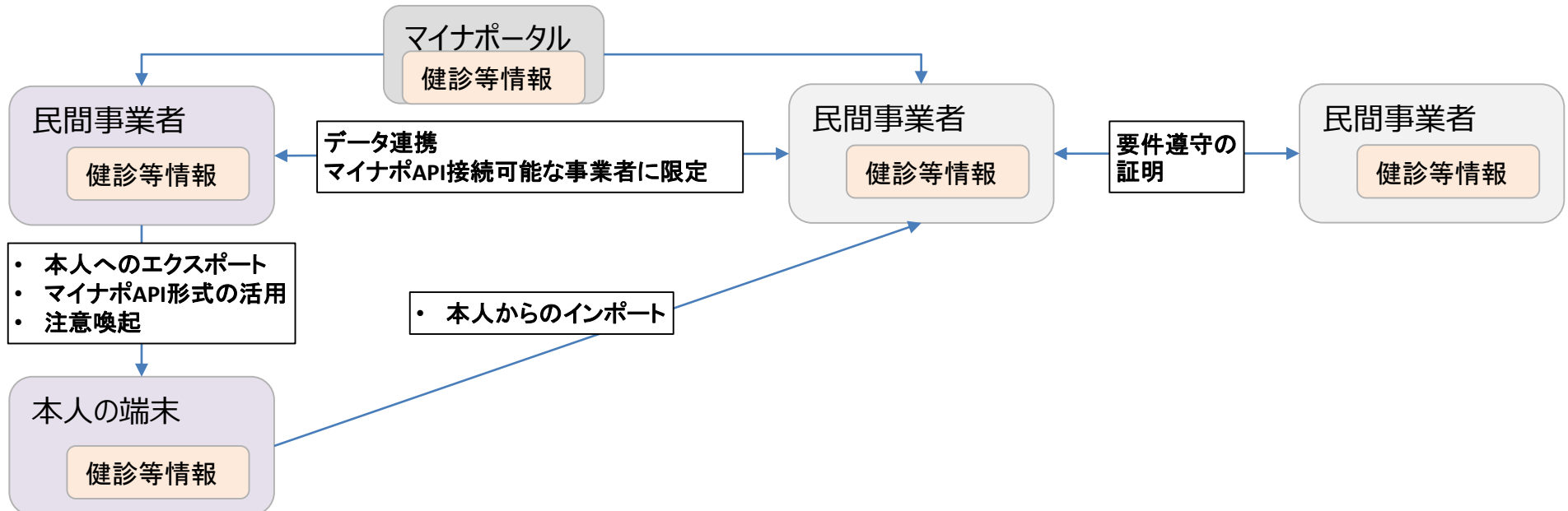
連携先	同意
XXフィットネス ⓘ	<input checked="" type="checkbox"/>
XX栄養管理アプリ ⓘ	<input type="checkbox"/>
XX生活習慣病 重症化予防アプリ ⓘ	<input checked="" type="checkbox"/>
:	



## **2 – 3 健診等情報の保存・管理、相互運用性の確保**

# 健診等情報の保存・管理、相互運用性の確保

- 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。



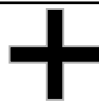
## **2 - 4 その他（要件遵守の担保方法など）**

# PHR事業者求められる適切な事業運営・体制

- 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、「マイナポータル自己情報取得 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？

## マイナポータルAPI経由で情報連携するための適格性【必須ルール】

区分	項目
社会的信用	役員若しくは担当部署責任者において、過去5年間に、下記の法令等に基づく刑事罰の執行等がないこと
	・ 行政手続における特定の個人を識別するための番号の利用等に関する法律
	・ 暴力団員による不当な行為の防止等に関する法律若しくはこれらに相当する外国の法令
	・ 刑法若しくは暴力行為等処罰に関する法律



## そのほかの社会的信用（例）

区分	項目例
社会的信用	・「個人情報の保護に関する法律」違反がないこと ・個人情報の安全管理に関する信用度（第三者認証や、流出等事故がない旨の実績、目的外利用や不当利用等を行わない誓約及び行っていないことに対する実績やその情報の公開 等）

# 要件遵守の担保方法など

- 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。

## (例)要件を満たしていることの証明方法

- ・ 自己チェックによる証明
- ・ (業界団体を含む)第三者による証明