第14回民間利活用作業班
（令和6年11月28日開催）

資料３

PHR基本的指針の見直しについて
（案）

PHR基本的指針に関する対応について

- 2021年のPHR基本的指針の策定から3年が経過し、時勢の変化や実際の運用を考慮したPHR基本的指針の見直しやマイナポータルAPI連携審査の運用検討の必要性を認識。
- 特に、PHRサービスが主にクラウド環境で提供されていることや、今後マイナポータルAPI連携項目への電子カルテ情報等の追加が見込まれていることを踏まえ、情報セキュリティ対策に係る項目を中心に、PHR基本的指針を見直しておくことが重要。
- なお、PHR基本的指針の見直しについては、見直し前後におけるマイナポータルAPI連携審査上の整合性担保のため、現行指針を活かして見直し案を検討する。

PHR基本的指針の課題

課題❶ 「対象とする情報」及び「対象事業者」の定義

課題❷ 最新の情報セキュリティ対策への対応

課題❸ 無害化処理の要否

課題❹ インポート／エクスポート機能具備の要否

見直しのスケジュール

・第14回民間利活用作業班：論点の提示

・第15回民間利活用作業班：改定案の検討

・第16回民間利活用作業班：改定案の取りまとめ

・上記終了後、パブリックコメントを実施した上で、改定版を公表予定。

課題① 「対象とする情報」及び「対象事業者」の定義

- 現状を踏まえ、「対象とする情報」及び「対象事業者」の定義の記載について、検討する。

1．対象とする情報

補足資料❶ 補足資料❷ 補足資料❸

- 本指針では、**個人情報保護法上の要配慮個人情報で以下に該当する情報、及び予防接種歴を『健診等情報』**と定義。
  - 個人がマイナポータル APIや健康保険組合等から入手可能な健康診断等の情報
  - 医療機関等から個人に提供され、個人が自ら入力する情報
  - 個人が自ら測定又は記録を行うものであって、医療機関等に提供する情報

※健診等情報の具体例として、乳幼児健診、特定健診、薬剤情報等が挙げられる。

【対応方針】

- **「対象とする情報」の定義**は、医療機関等に提供するか否かはデータ取得時点では判断できないことから、**定義解釈を明確化する観点**から**３点目を「医療機関等に提供する『可能性がある』情報」に修正**する。
- 今後、電子カルテ情報（６情報のみ）等がマイナポータルAPI経由で取得可能となった場合、**「健診等情報の具体例」**に**「電子カルテ情報」**を**追記**する。

2．対象事業者

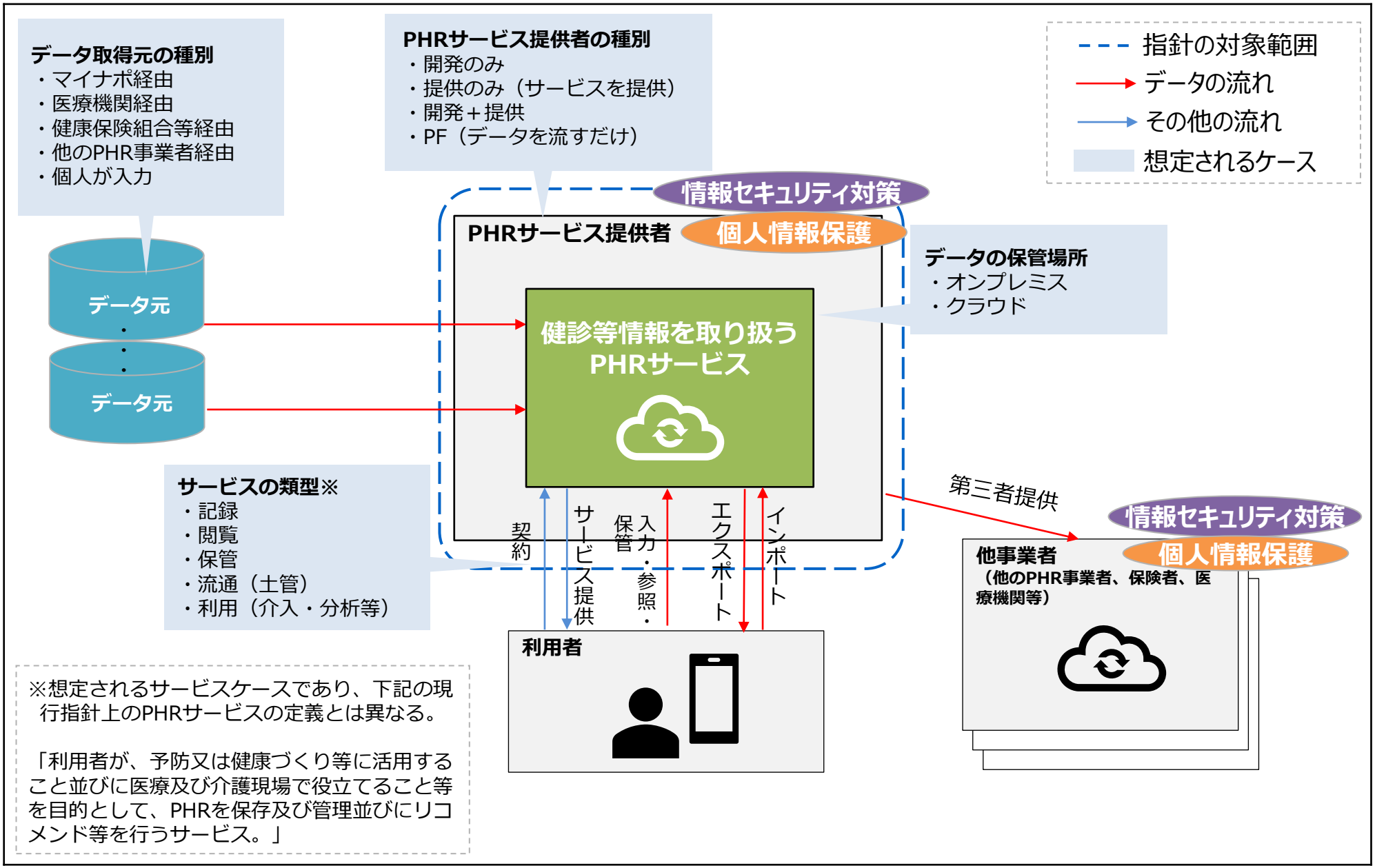
補足資料❹ 補足資料❺

- 本指針では、**「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」**と定義。
- 利用者に対して、**直接的もしくは間接的にPHRサービスを提供する者（PHRサービス提供者）は民間事業者に加え、自治体、健康保険組合、医療機関なども存在。**安心・安全なPHRサービスが利用者に適切に提供されるためには、PHRサービス提供者が基本的指針を遵守した上で、PHRサービスを提供することを求める。

【対応方針】

- 本指針の**対象者は、民間事業者、自治体、健康保険組合、医療機関等を含む、「健診等情報を取り扱うPHRサービスを提供する者（PHRサービス提供者）」**とし、これに伴い、本指針のタイトルを「**PHRサービス提供者**による健診等情報の取扱いに関する基本的指針」に変更する。

補足資料❶ PHR基本的指針の前提：PHRサービス構成



補足資料❷

PHR基本的指針の前提：指針対象となる情報の範囲

PHR

民間ガイドライン※1の対象領域

健診等情報
（要配慮個人情報＋予防接種情報）
（＝現行指針対象）

- 特定健診情報
- 薬剤情報
- 予防接種情報
- 電子カルテ情報
- ・・・

ライフログ

- ウェアラブルデバイス
- スマートフォン
- 環境センサ　　等
  の機器からの取得情報
  ＋
- 個人が手入力した情報

医療機関等から個人に提供され、個人が自ら入力する情報（※2）

ライフログのうち、個人が自ら測定又は記録を行うものであって、医療機関等に提供（提示）する情報（※3）

＜出所＞　※1　民間事業者のPHRサービスに関わるガイドライン（第3版）　PHRサービス事業協会／（一社）PHR普及推進協議会
※2　基本的指針　１．本指針の基本的事項　１．１．本指針の対象とする情報の定義より抜粋
※3　基本的指針　１．本指針の基本的事項　１．２．本指針の対象事業者

補足資料❸

個人情報保護法における要配慮個人情報の定義

個人情報の保護に関する法律　第二条（抜粋）

３　この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

個人情報の保護に関する法律施行令（抜粋）

第二条 法第二条第三項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。

一　身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。

二　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」という。）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」という。）の結果**

三　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**。

要配慮個人情報と指針で対象とする情報との関係性

項目名	マイナポータルAPI連携								今後マイナポAPI連携予定		その他	
	自己情報取得API			医療保険情報取得API								
	予防接種	妊婦健診・乳幼児健診	自治体検診	特定健診	薬剤情報	電子処方箋（処方情報・調剤情報）	医療費通知情報	事業主健診	電子カルテ	診療情報	医療情報（非マイナポ経由、非個人経由）	ライフログ
取扱い	現行指針対象											内容により異なる
	要配慮個人情報											

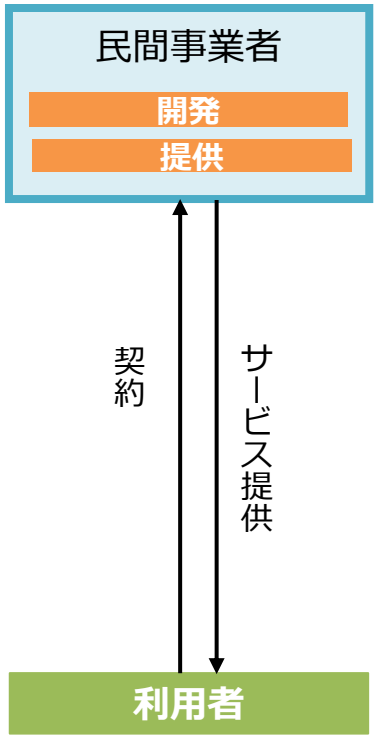
補足資料❹

PHR基本的指針の前提：PHRサービス提供者の類型

※ 現行指針の対象
PHRサービス提供者（**太線囲い**は提供主体）

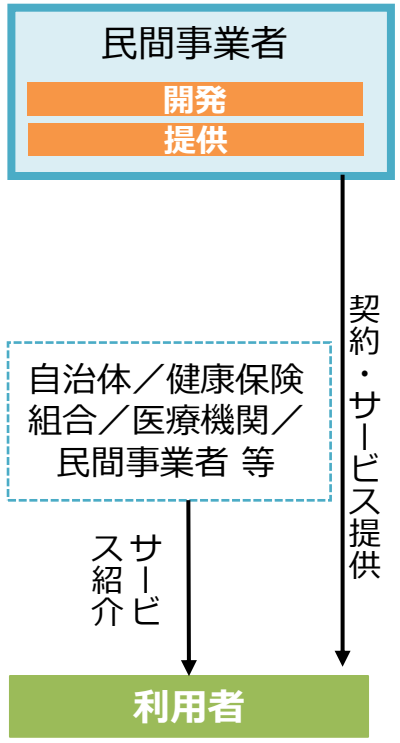
❶ 開発者と提供者が同一 民間事業者による開発・提供

B to C



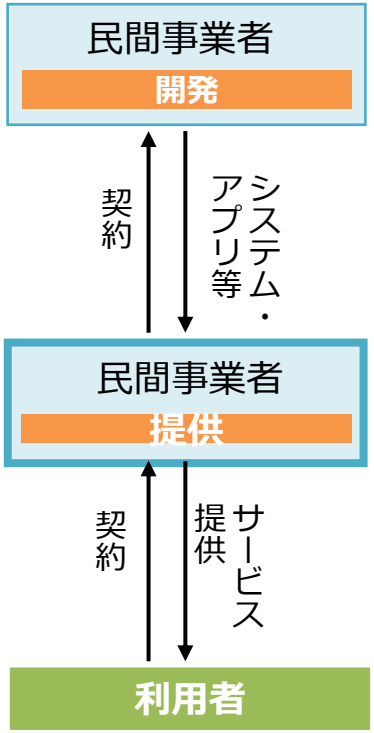
❷ 開発者と提供者が同一 仲介者による紹介

B to G/P/D/B to C



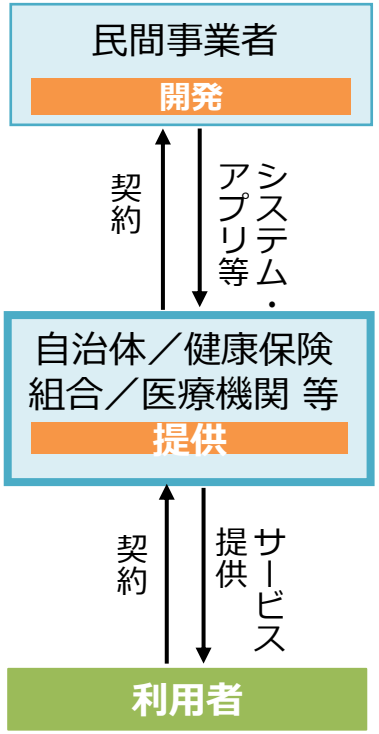
❸ 開発者と提供者が別 民間事業者による提供

B to B to C



❹ 開発者と提供者が別 民間事業者以外による提供

B to G/P/D to C



補足資料⑤ これまでの自治体・健康保険組合の取扱い

（Q&A上の記載）Q１－８　自治体又は健康保険組合は本指針の対象となりますか。

A　本指針は民間 PHR 事業者を対象としており、自治体又は健康保険組合は対象とはしていません。

自治体は、個人情報保護法の適用対象となる他、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）（令和４年１月（令和４年９月一部改正）、個人情報保護委員会）の適用対象となります。

また、健康保険組合又は国民健康保険組合は、個人情報保護法の適用対象である他、「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」（平成29年４月14日（令和４年３月一部改正）個人情報保護委員会、厚生労働省）又は「国民健康保険組合における個人情報の適切な取扱いのためのガイダンス」（平成 29年４月14日（令和４年３月一部改正）個人情報保護委員会、厚生労働省）の適用対象となります。

なお、これらのガイドライン等で規定されていない本指針「４．健診等情報の保存及び管理並びに相互運用性の確保」等については本指針を参考に対応していただくことが望まれます。

（経緯）第７回民間利活用作業班（令和３年３月２５日開催）

本会にて、**PHR基本的指針が民間事業者に対するものであるため自治体・健康保険組合は対象外であると整理した**。一方で、セキュリティや相互運用性の担保については、自治体・健康保険組合としても対象範囲内になり得るため、本指針を参考とするようQ＆Aに記載することとした。

議事録（抜粋）

○【事務局】もともと指針の２ページの対象事業者の定義のところ、１.２.で、**健診等情報を取り扱うＰＨＲサービスを提供する民間のＰＨＲ事業者、これをＰＨＲ事業者とこの指針では定義させていただきまして、健康保険組合ですとか自治体を民間と呼ぶのは我々としては難しいと考えておりますことから、対象となりません**で、健康保険組合のガイダンスなどを遵守してくださいということを書いております。

○【委員】ただ今後、**自治体とか健保組合が主体となってＰＨＲサービスを提供していくことは当然想定されると思う**のですけれども、その場合、相互運用性とか、ここに書かれているセキュリティのこととかはどこを見たらよいのかというか、この指針で共有していただいたほうがよろしいのではないかと思いました。

○【事務局】御指摘ありがとうございます。確かに、健康保険組合とかと調整が済んでいませんので、遵守せよと書くのは書き過ぎなのですけれども、セキュリティですとか相互運用性などについてこの指針の遵守が期待されるとか、それぐらいであれば書くことは可能かと思っています。

課題② 最新の情報セキュリティ対策への対応（最新のGL等への準拠）

- 情報セキュリティ対策については、マイナポータル利用規約が、「中小企業における組織的な情報セキュリティガイドライン」(2008年IPA策定)を引用していたことを受けて、本指針においても、当該ガイドラインをほぼそのまま転記する形で作成している。そのため、最新の情報セキュリティ対策へ対応すべく、記載を見直す必要がある。

【対応方針】

- **関連ガイドライン（中小企業情報セキュリティGL※1、クラウドセキュリティGL※2、NISCハンドブック※3）等を参考に、現行指針に対して項目を追加する。**

最新の情報セキュリティ対策への対応を検討した項目

2.1 安全管理措置

(1)法規制に基づく遵守すべき事項
(2)本指針に基づく遵守すべき事項
① 情報セキュリティに対する組織的な取り組み
② 物理的セキュリティ
③ 情報システム及び通信ネットワークの運用管理
④ 情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策
⑤ 情報セキュリティ上の事故対応
⑥ 外的環境の把握

2.2 第三者認証の取得

(1)法規制に基づく遵守すべき事項

詳細は **資料４** へ

※1 中小企業の情報セキュリティ対策ガイドライン第3.1（IPA） https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
※2 クラウドサービス提供における情報セキュリティ対策ガイドライン第3版（総務省） https://www.soumu.go.jp/main_content/000771515.pdf
※3 インターネットの安心・安全ハンドブック（NISC）https://security-portal.nisc.go.jp/guidance/handbook.html

課題③ 無害化処理の要否

- 外部から受け取るファイルへの無害化処理（現行指針では「サニタイズ処理」に限定）について、過去に本指針の適用範囲を踏まえた議論が行われておらず、また、その必要性を十分に説明できていないことから、見直しを検討する。

（参考）２．１．安全管理措置　（２）　③ 情報システム及び通信ネットワークの運用管理 ＜抜粋＞
■外部から受け取るファイルに対して、無害化を実施する
➢ファイル無害化機器、無害化ソフトウェア又は無害化サービス等を導入し、外部からのファイルを受け取る際に、無害化を実施すること。

【対応方針】

- 未知のマルウエアに対応する必要性から無害化処理が求められているが、**技術的な選択肢は複数あり**、**PHRサービス提供者側が現状に適した技術を選択できる余地を残すべき**ではないか。
- **情報セキュリティ対策全体として必要な対策を規定することを前提に、無害化処理の記載は削除することとする。**

❶経産省の外部サイバーセキュリティ専門家からの意見

- 無害化処理以外にも、**アンチウイルスソフトでのファイルチェックや、機械学習モデルを使ってファイルの中をチェックすることも可能**であり、**無害化処理にこだわる必要はない。**
- まずは、守るべき対象を明確にした上で、必要な対策を検討すべき。その際、**無害化ありきではなく、情報セキュリティ対策全体として、必要な対策について包括的に議論すべき。**

❷事業者からの意見

- **ウイルススキャンでは、未知のウィルスへ対応できるものも含め、手法は様々存在し、技術の選び方の問題**である。一方で、完全に「無害化」することは技術的も費用的にも負担は大きい。
- 無害化は必要な処理であると思うが、なぜ**指針でこの技術だけを取り上げているのかが不明**である。
- **システム同士のやり取りでは、無害化の優先度は低い。**一方で、一般利用者がアップロードする場合は無害化の優先度が高いが、**システムの構成によってセキュリティの対応が異なるため、無害化は一手段に過ぎない。**

課題④ インポート／エクスポート機能具備の要否

- 現行指針では、利用者を介した相互運用性確保のために、「少なくともマイナポータルAPI等を活用して入手可能な自身の健康診断等の情報について、利用者へのエクスポート機能及び利用者からのインポート機能を具備しなければならないこと」としている。当該機能の利用状況やPHRサービス提供者側の負担感を踏まえた上で、当該機能の具備を求めることにつき見直しを検討する。

（参考）４．２．相互運用性の確保　（１）　①利用者を介した相互運用性の確保

健診等情報を取り扱うPHR事業者においては、少なくともマイナポータルAPI等を活用して入手可能な自身の健康診断等の情報について、利用者へのエクスポート機能及び利用者からのインポート機能を具備しなければならない。（後略）

【対応方針】

- **インポート機能（サービス外からのデータ取込み機能）**は、**他者との差異化要素としてPHRサービス提供者側が具備するか判断すべきもの**、**エクスポート機能（サービス外へのデータ出力機能）**は、**自身の情報を様々なサービスで利用可能にするためにPHRサービス提供側が利用者に保証すべきもの**という整理が適当ではないか。
- **このため、指針上は、少なくともマイナポータルAPI等を活用して入手した健診等情報について、PHRサービス提供者に対し、エクスポート機能のみ具備を求めるものとし、インポート機能はPHRサービス提供者側の判断によるもの**とする。なお、インポート及びエクスポート機能の実装方法については、PHRサービス提供者側が判断すべきものと整理する。

事業者からの意見

- これまでの実績として利用者がおらず、メンテナンスコストがかかる。インポートは特にコストが高い。
- 当該機能を利用されたケースは数例しかなく、費用感を踏まえると、割に合わない。
- インポート機能を実装する判断は民間事業者が判断すればよい。
- インポート／エクスポート機能は元々の目的が異なるので、そのため（整理が）あいまいになっているのではないか。