

民間利活用作業班報告書

令和3年4月

健康・医療・介護情報利活用検討会
健診等情報利活用ワーキンググループ
民間利活用作業班

目次

はじめに.....	1
1. 検討の経過.....	2
2. 民間 PHR サービス利用者へのアンケート調査結果等	4
3. マイナポータル API 接続との関係	7
4. 今後の検討課題.....	8
5. より高いサービス水準を目指すサービスガイドライン.....	9
民間利活用作業班構成員名簿	10
別紙1 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	
別紙2 参考資料集	

はじめに

近年、民間事業者によって、健康診断結果をはじめとする、体重、血圧、血糖値等の情報（いわゆる Personal Health Record。以下「PHR」という。）を用いて、個人の健康維持や生活改善の支援をはじめとした多種多様なサービスが提供されている。我が国の PHR に関する取組としては、平成 29 年 6 月にマイナポータルを通じた予防接種歴の提供が開始されており、その後も乳幼児検診結果、特定健診結果、レセプトの薬剤情報等を順次提供することを通じて、国民の予防、健康づくりの推進等が期待されている。

上記を踏まえ、「健康・医療・介護情報利活用検討会 健診等情報利活用ワーキンググループ」において、PHR の利活用に関して、目指すべき姿として、(STEP1) 国民・患者が自らの保健医療情報を適切に管理・取得できるインフラの整備、(STEP2) 保健医療情報を適切かつ効果的に活用できる環境の整備、(STEP3) 質の高い保健医療を実現するための保健医療情報の活用（研究開発等の推進）が示された。

このうち STEP2 において、安心・安全に民間 PHR サービス等を活用できるルールの整備が求められ、具体的な課題として、①（マイナポータル API 連携に求める基準の整備を含む）適切なルールの整備、②（マイナポータル API 連携に係るものを含む）ルールの要件を満たしていることを証明するための仕組み及び③サービスの技術革新のスピードに対応できる見直しの体制が示された。

本民間利活用作業班では、7 回の議論を行い、国民による安全・安心な民間 PHR サービスの利活用の促進に向け、PHR 事業者として遵守すべき情報の管理・利活用に係るルールとして、「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」（以下「基本的指針」という。）を策定した（別紙 1）。また、基本的指針の策定における考え方及び解説については、Q&A としてとりまとめた。さらに、基本的指針のとりまとめの議論において指摘した、PHR 事業者間において検討すべき事項等については、民間利活用作業班の報告書としてとりまとめた。

1. 検討の経過

1. 1. 第1回（令和2年2月15日開催）

国民の健康づくりに向けた PHR の推進に関する検討会 民間利活用作業班（第1回）

議事：（1）PHR に関する検討の進め方等について

（2）民間 PHR 事業者の現状について

民間利活用作業班の検討のスケジュール等の検討の進め方等について議論。

1. 2. 第2回（令和2年2月19日開催）

国民の健康づくりに向けた PHR の推進に関する検討会 民間利活用作業班（第2回）

議事：（1）民間 PHR サービスに関する論点について

民間 PHR サービスのユースケース、検討事項の整理等の今後の論点等について議論。

1. 3. 第3回（令和2年4月22日メール審議開催）

健診等情報利活用ワーキンググループ 民間利活用作業班（第3回）

議事：（1）民間 PHR サービスに係る基本的な考え方について

民間 PHR サービスに係る基本的な考え方として、民間 PHR 事業者に求められる事項、今後の取組等について議論。

1. 4. 第4回（令和2年10月29日開催）

健診等情報利活用ワーキンググループ 民間利活用作業班（第4回）

議事：（1）自身の保健医療情報を活用できる仕組みの拡大について

（2）本作業班における検討の進め方

（3）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

（4）PHR サービス利用者へのアンケート調査方針

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等について議論。

1. 5. 第5回（令和2年12月2日開催）

健診等情報利活用ワーキンググループ 民間利活用作業班（第5回）

議事：（1）今後の民間利活用作業班の進め方と検討スケジュールについて

（2）健診等情報に関する PHR サービスを活用している健康保険組合等に対するヒアリングの中間報告

（3）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について第4回の意見を踏まえた考え方、基本的指針骨子案等について議論。

1. 6. 第6回（令和3年2月3日開催）

健診等情報利活用ワーキンググループ 民間利活用作業班（第6回）

議事：（1）PHR サービス利用者へのアンケート調査結果等

（2）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（案）
について

PHR サービス利用者へのアンケート結果の報告及び民間 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（案）等について議論。

1. 7. 第7回（令和3年3月25日開催）

健診等情報利活用ワーキンググループ 民間利活用作業班（第7回）

議事：（1）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（案）
について

（2）民間利活用作業班報告書（案）について

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及び民間利活用作業班報告書のとりまとめについて議論。

2. 民間 PHR サービス利用者へのアンケート調査結果等

2. 1. 民間 PHR サービス利用者へのアンケート調査

民間 PHR サービスが適切な形で普及展開されるための課題を明らかにし、民間利活用作業班における議論に資するものとするべく、サービス利用実態及び安全性等についてサービスを選ぶ際のポイントや留意点を明らかにすることを目的に、個人を対象としたアンケート調査（以下「本体調査」という。）を実施した。以下がその結果サマリである。結果の詳細については別紙 2（33～62 ページ）を参照。

【結果サマリ（本体調査・PHR 利用状況）】

利用割合	・ PHR 現利用率は、高いもので 14 % 程度（スクリーニング前の母集団を対象とした概算） ・ 現利用者の利用しているアプリは、「お薬手帳」・「コロナ」・「フィットネス」が多い
PHR 認知度	・ 66.7 % が PHR の名称について「全く知らない」と回答 ・ PHR の名称の認知度は、現利用者・過去利用者の方が高い
利用実態	・ 利用目的として、健康増進・疾病予防、各種手帳等の電子化が多い ・ 勤務先や通学先などから利用するように指示や推薦からという回答はそれほど多くない ・ 体重や血圧、運動、睡眠等の日々のライフログ情報を比較的多く利用している
利用にかかる要因	・ 利用継続要因は、アプリケーション自体のユーザビリティ、利用による健康意識・安心感の実感 ・ 利用離脱要因は、データ登録やアプリ同士の連携コスト、個人情報への漏えいやセキュリティに対する不安
連携ニーズ	・ データ連携に関して 15 % 前後のユーザーが「全て連携してもいい」、50 % 前後のユーザーが「全て連携したくない」 ・ 連携意向が高い項目「医療機関」相手、「健診結果・薬情報・受診・アレルギー」データ ・ 連携意向が低い項目「勤務先・第三者企業・保険者」相手、「経済状況・家族情報・介護」データ、「商品開発・マーケティング」目的

【結果サマリ（本体調査・「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」（案）項目関連）】

情報セキュリティ対策	・ 利用するサービスのセキュリティに対する意識には、ばらつきがある ・ 個人情報の漏えいに対する不安がある人は、利用したことのある人の約半数 ・ セキュリティより利便性をより重視するのは約 2 割、利便性よりもセキュリティをより重視するのは約 3 割 ・ 未利用者は、利用したことがある人よりも、利便性よりセキュリティを重視
個人情報の取扱い	・ 個別に同意をしている割合は、2 割強 ・ 同意内容を理解している割合及び同意の適用範囲やデータ共有相手について分からず不安を感じている割合は、4 人に 1 人 ・ 全てのデータに対する包括的な同意で構わないとする人は約 7 % ・ データの範囲・種類ごとに個別に同意を判断したい及び、全く新しいことに関してはその都度確認して同意をしたいを合わせると、約 9 割が包括的な同意ではなく、データの範囲や種類ごとの同意を望んでいる ・ サービス終了時のデータは、全て消去したい人と、何らから継続して残したい人が半々である
相互運用性の確保	・ リーベス乗り換え時に希望するデータ移行方法は、「事業者にしてもらう」、「自分で行う」が半々 ・ 一方、希望するデータ保存方法については、クラウドを利用することを望む人が約 3 割
その他	・ 判定スコアやプロファイリング結果を信頼するのは、約 3 割

上記の本体調査に加えて、健診等情報を取扱う PHR 事業者の協力を得て、アンケート調査（以下「追加調査」という。）を実施した。本体調査の「オンライン診療・診療予約」「健康診断・医療費」「診療管理」「疾病管理」「お薬手帳」「出産・育児」のアプリ利用者及びそれ以外の PHR サービス利用者と、追加調査における健診等情報を取扱う PHR サービス利用者のデータを元に比較を実施した。以下がその結果サマリである。結果の詳細については別紙 2（26～32 ページ）を参照。

【結果サマリ（追加調査）】

リテラシー	健診等情報を取扱う PHR サービス利用者は、その他の PHR サービス利用者と比べて、PHR に関する説明を医療従事者等から受けており、個人情報の利用先についての理解も高い傾向
ID 連携	健診等情報を取扱う PHR サービス利用者は、その他の PHR サービス利用者と比べて、マイナンバーを含む ID 連携に前向きな傾向
効果実感	- 健診等情報を取扱う PHR サービス利用者は、予防効果、利便性及び金銭的ベネフィット感において、効果を実感している傾向がある - 意識の変容や心理的安全に関しては本調査と追加調査では傾向が異なった

2. 2. 健診等情報に関する PHR サービスを提供している健康保険組合等に対するヒアリング調査

保険者（国保・健保）には、PHR サービスを活用して被保険者等の健康増進を図るものがある。民間利活用作業班における議論に資するものとするべく、被保険者等に向けた PHR サービスの活用の現状と課題を把握するための保険者を対象とするヒアリング調査（ヒアリング調査）を実施した。以下がヒアリング調査から得られた示唆（各団体から得た意見概要）である（別紙 2（63～68 ページ）にも記載）。

【ヒアリング調査から得られた示唆（各団体から得た意見概要）】

		ヒアリング結果
1. サードス全休について	・ サードス内容	（サービス内容・利用状況） - 保健事業の一環として毎月の医療費通知、歴年健診データ（5 年分）を確認できる。 - 健診情報を閲覧できる。 - 端末への健診情報のダウンロードはできない。 （第三者提供） - 健診データ・レセプトデータの第三者提供は許可していない。被保険者へのメリットがなければ提供する意義がない。 - ドッグデータ利用への需要はあり、第三者提供によりサードス費用は下がる。しかし、組織の総意により、PHR に集まった情報は第三者提供しておらず、今後もそのつもりはない。 - 第三者提供はしていない。 - 組織の保有するデータを民間 PHR 事業者に預託しているが、第三者提供ができないため、本人が直接入力する方式に切り替えたい。
	・ 運用状況	- 閲覧機能を必ずしも活用できず、動機付けが課題である。健診データを閲覧するのは、健康に関心が高い層（高年齢）である。 - 閲覧やキャンペーンにポイントを付与している。利用者属性は、ポイント収集を好む層である。 - 健診結果の受け取りまでに要する時間を考えると、WEB 上にログインし健診結果を確認するユーザーは少ない。 - 過去の健診結果閲覧はウェブ上でも閲覧は可能であるが、必要な際は健診機関へ問い合わせをして取得することを想定しているユーザーが多い。
	・ 利用による効果（評価）	- アプリによる健康効果を今後検証する予定である。 - 通院をする者にとっては、健診結果を持ち歩かなくてよいのはメリットである。

		ヒアリング結果
2. リービス導入の経緯	・ サービス導入	・ 広報誌、WEB等により、サービス導入の周知をしている。 ・ 口コミによる利用者拡大が見込まれるため、住民へ直接アプリの登録方法をレクチャーするなど、地道に周知している。 ・ ハガキにて周知をしている。
3. 事業者選定について	・ 事業者選定基準 ・ 適切な評価、選択に必要な課題	(選定基準) ・ スピード感があり自主的な提案ができる信頼感のある事業者を選定。 ・ 当該領域に実績のある事業者を選定。 ・ データの二次利用をしないかと、金額の妥当性の観点から事業者を選定。 ・ 応募事業者のサービス内容には大差なく、予算面が決め手となった。 (第三者認定等の仕組み) ・ 第三者認定の仕組みがあると、選定・評価の指標となるためありがたい。 ・ 信用調査のように、民間PHR事業者のランキングがあるとよい。事業者の強みが見える化されているとありがたい。 ・ 基準はある方がよい。特にセキュリティ等は自分達で判断が難しいため、お墨付きがあると良い。 (事業者の継続性) ・ 契約は1年契約で、半年前までに契約破棄しない限りは契約が続く。 ・ 民間PHR事業者から継続的にサービス提供されることは重要である。 ・ 本人の健診等情報の元データが本人のスマホにあるのなら、PHR事業者のサービスが終了しても問題ない。 ・ 複数のPHR事業者に必要な情報を提供することで、1つの事業者が終了してもリービス全体としては継続できるようなっている。
4. 事業者評価について	・ リービス・事業者評価	・ 自団体においてPHRリービスに対する評価基準は特に定めていない。 ・ 毎年監査を実施し、サービスの棚卸や機能改善の要望への対応を確認している。ただ評価基準までは定めていない。

		ヒアリング結果
5. セキュリティ・個人情報・本人同意について	・ セキュリティ	・ 自団体においてプライバシーマークの取得又はセキュリティ基準の設定等を行っている。 ・ 健診データを外部にアップロードをするのにあたり、特別に独自の個人情報規定を設けて対応している。 ・ 個人情報保護法等関係法令および「国保における個人情報の適切な取り扱いのためのガイドライン」や厚労省の事務連絡文書において示されている基準等を最低ラインとして設定した。 ・ 市町村説明の際は、事業者の対策が適切か厚労省にも確認いただき、理解を得た。 ・ 200数十項目のセキュリティに関する質問について、ヒアリングを実施することに加え、自団体のIT専門家による現地監査を行っている。 ・ 他部署の情報セキュリティ専門家を審査委員に入れて、安全性を確認した。
	・ 個人情報の取扱い	(個人情報の取扱いに関する基本的なルール) ・ 一般的に個人情報の取書は民間PHR事業者と締結している。 ・ 利用目的はより詳細に記載するのが好ましいが、多数の被保険者対象に総意を得るのは難しい。 ・ 健診情報の閲覧には、なりすまし防止と本人同意取得のため、健診閲覧コード（事業者から圧着しに付いて送付）の inputs を必須としている。 (サービス提供終了時・本人解約時のデータ取り扱い規定) ・ 資格喪失後は利用ができない。被保険者から健康データを引き継ぎたいとの要望は今までない。 ・ これまで申し出はないが、本人請求があれば情報の削除などに対応することになっている。退職後も基幹システムの情報は保持している。 ・ サービス終了時は事業者がデータを廃棄する。
	・ 本人同意	・ 特定健診データについて、事業者間のデータ連携は、本人同意が得られれば適宜の特定健診データを引き継いで運用できることにメリットがある。 ・ 委託先のPHR事業者へのデータ提供については、自団体の事業内でのデータ活用と位置付け、本人同意は取得している。本人からの削除依頼に備え、『個人情報削除依頼書』を準備し、健康情報の削除依頼に対応している。（地方公共団体） ・ アプリ登録時に条件を提示しているが、個人のPHR登録時の利用規約については、細かい部分は把握していない。

		ヒアリング結果
6. 安全性・有効性について	・ 安全性・有効性に関する取組	・ 生活習慣病リスクチェックの妥当性は、提供する会社の信頼度、医師等の監修があるかどうかで判断している。 ・ サービス開発に医療系大学が関わっているため、安全性・有効性は担保されていると考えている。 ・ 事業者の知見を活用している。 ・ 安全性・有効性の判断は明示されるとよいが、明確な線引きは難しい。企業努力による部分もある。
7. マイナポータルについて	・ マイナポータルとの連携	(活用の在り方（現在の活用状況、今後の活用プラン）) ・ 既に独自に健康情報と閲覧させる仕組みを構築しているため、マイナポータルとの連携によるメリットのイメージがまだついていない。 ・ 上手く連携しながら、スマホ世代を健康管理に取り入れていきたい。 ・ 現状のサービス拡大も考えているが、マイナポータルも利用できるようになるため、独自のサービスが必要かを判断していきたい。 (活用時の課題) ・ 効果的な保健指導のためには前の健診情報が必要であるが、必ず本人同意を求めるとなると機動性が低下するのではないか。 ・ マイナポータルで連携されたデータが誰のものかをきちんと定着することが必要ではないか。 ・ 普及のためには、リービス提供者にとって魅力的なデータがあることが重要。そのためにデータセットやデータ形式を開放しておく必要がある。 ・ セキュリティを担保することで懸念や不安をどれだけ払拭できるのか。他の情報も連動してくることで不安が増大する可能性がある。

3. マイナポータル API 接続との関係

「はじめに」に記載したとおり、基本的指針はマイナポータル API 連携に際して PIIR 事業者を求める基準でもある。

PIIR 事業者は、基本的指針の遵守状況についてチェックシートの確認事項に沿って確認した結果を自らのホームページ等で公表し、基本的指針の遵守を明らかにした上で、「マイナポータル API 利用規約」（令和 2 年内閣府大臣官房番号制度担当室）に従って、マイナポータルとの API 連携の利用手続きを行い、サービスを提供することとなる。また、基本的指針の見直し時には、一定の期間内に基本的指針を満たすような必要な対応を行うとともに、遵守の状況について自らのホームページに公表した上で、内閣府大臣官房番号制度担当室に、見直し後の基本的指針を遵守したことの報告を行うこととなる。

4. 今後の検討課題

基本的指針の策定においては、その範囲を超えた事項も含めて PHR サービスの発展に向けて引き続き検討すべき事項についての意見も、構成員から多く示された。具体的には、以下に記載する事項が挙げられるが、これに限らず、今後の技術の進歩及び PHR サービスの利用拡大の中で発生する課題等について、更なる検討が望まれる。

<基本的指針の基本的事項に係る留意事項>

- ・いわゆるライフログ等の利活用に際して留意すべき事項

<個人情報適切な取扱いに係る留意事項>

- ・医師又は薬剤師等の氏名等を第三者提供する場合の取扱い

<健診等情報の保存及び管理並びに相互運用性の確保に係る留意事項>

- ・同じデータの項目であっても、健診等において取得されたものと本人が入力したものとは、計測方法及びデータ改変の可能性等の観点で違いが生じ得るため、区別した管理の在り方
- ・データの保存及び管理における、利用者による改ざん防止対策
- ・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対応コスト等の観点を考慮した事業者間での連携の拡大
- ・より効率的なデータ管理及びポータビリティの仕組みの構築を検討した上での、情報種別毎の名称及び単位等の統一並びに通信規格及び交換形式に係る標準化

<要件遵守の担保方法に係る留意事項>

- ・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

<その他>

- ・生活習慣病改善等に向けた PHR サービスを提供する場合の医療従事者等と連携したサービスの提供
- ・上記観点も踏まえて、最新の利用可能な技術及び知見等に基づき、より高い水準を目指すサービスガイドライン（5. に記載）を策定して取り組むなど、先進的かつ高度な取組の推進

5. より高いサービス水準を目指すサービスガイドライン

国民による安全・安心な民間 PHR サービスの利活用の促進に向け、PHR 事業者として遵守すべき情報の管理・利活用に係るルールとして、基本的指針をとりまとめたところであるが、「4. 今後の検討課題」に記載したとおり、引き続き検討が必要な課題がある。

基本的指針については、個人情報保護法等の法令又はガイドラインの改正、その運用状況及び PHR サービス又はセキュリティ技術等の拡大等の状況の変化を踏まえて、必要に応じて検討及び見直しを行うこととするが、例えば、「4. 今後の検討課題」で示したライフログ等の情報は基本的指針の対象としていないこと、また、通信規格や交換形式等に係る標準化については民間主導での調整がおこなわれることが望ましいことなどから、基本的指針を補完するものとして別途、より高い水準の PHR サービスの提供のための民間事業者ガイドラインの策定が望まれる。

このガイドラインの検討については、PHR 事業者間において、最新の利用可能な技術や知見に基づき、より先進的・高度な取組を推進する観点で検討されていくことが期待される。その際、論点に応じて、有識者を交えた議論をすることが重要である。（例えば、生活習慣病改善等に向けた PHR サービスの提供を議論する場合には、医療従事者等と連携するなど。）また、このガイドラインの策定主体や、ガイドライン遵守の認定主体として、PHR 事業者による団体が設立されることにより、ガイドラインの効率的な検討や、利用者の利便性向上に資することが期待される。

なお、基本的指針の遵守状況、民間事業者によるガイドラインの検討状況等によっては、国において、PHR 事業者及び有識者の意見を踏まえつつ、このガイドラインの策定を行うことも考慮すべきである。

健康・医療・介護情報利活用検討会
健診等情報利活用ワーキンググループ
民間利活用作業班
構成員名簿

(構成員(五十音順))

い わ み た く 石見 拓	京都大学 環境安全保健機構 健康科学センター 教授
う さ み しんじ 宇佐美 伸治	公益社団法人 日本歯科医師会 常務理事
う り ゆ う かずひさ 瓜生 和久	独立行政法人 情報処理推進機構 セキュリティセンター長
お ち あ い たかふみ 落合 孝文	渥美坂井法律事務所・外国法共同事業 弁護士
か づ ま ひろゆき 鹿妻 洋之	一般社団法人 保健医療福祉情報システム工業会 保健福祉システム部会 健康支援システム委員会 委員長
きたおか ゆうき 北岡 有喜	独立行政法人 国立病院機構京都医療センター 医療情報部 部長
きたむら りょうた 北村 亮太	健康長寿産業連合会
ながしま きみゆき 長島 公之	公益社団法人 日本医師会 常任理事
なかやま たけお 中山 健夫	京都大学大学院 医学研究科 社会健康医学系専攻 健康情報学分野 教授
みつぎ もとひろ 光城 元博	一般社団法人 電子情報技術産業協会 ヘルスケア IT 研究会 副主査
みやた ひろあき 宮田 裕章	慶應義塾大学 医学部医療政策・管理学教室 教授
もろおか あゆみ 諸岡 歩	公益社団法人 日本栄養士会 理事
主査 やまもと りゅういち 山本 隆一	一般財団法人 医療情報システム開発センター 理事長
わたなべ だいき 渡邊 大記	公益社団法人 日本薬剤師会 常務理事

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

令和 3 年 4 月

(総務省、厚生労働省、経済産業省)

目次

はじめに.....	1
1. 本指針の基本的事項.....	1
1. 1. 本指針の対象とする情報の定義	1
1. 2. 本指針の対象事業者	1
1. 3. 本指針に記載のない事項の取扱い	1
2. 情報セキュリティ対策.....	3
2. 1. 安全管理措置	3
2. 2. 第三者認証の取得	9
3. 個人情報の適切な取扱い.....	11
3. 1. 情報の公表	11
3. 1. 1. 利用目的の特定.....	11
3. 1. 2. 利用目的の明示等.....	11
3. 2. 同意取得	12
3. 3. 消去及び撤回	14
3. 4. その他	15
3. 4. 1. 健診等情報に含まれる利用者以外の個人情報の取扱い	15
3. 4. 2. 匿名加工情報に関する留意事項.....	15
4. 健診等情報の保存及び管理並びに相互運用性の確保	16
4. 1. 健診等情報の保存及び管理	16
4. 2. 相互運用性の確保	16
5. 要件遵守の担保.....	17
5. 1. 本指針の規定する要件を遵守していることの確認.....	17
6. 本指針の見直し.....	18
用語集.....	19
別紙 本指針に係るチェックシート	

はじめに

本指針は、安全、安心な民間 PHR（Personal Health Record）サービスの利活用の促進に向けて、健診等情報を取り扱う事業者による PHR の適正な利活用が効率的かつ効果的に実施されることを目的として、PIIR サービスを提供する事業者が遵守すべき事項を示すものである。

本指針では、要配慮個人情報である健診等情報を取り扱うこととなるサービスを提供する民間事業者が法規制により遵守を求められている事項に加えて、適正な PIIR の利活用を促進するために遵守することが必要と考えられる事項を含めて提示している。

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

本指針が対象として想定する PHR サービスにおいて活用される情報としては、個人が自らの健康管理に利用可能な「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）上の要配慮個人情報で、次に掲げるもの（以下「健診等情報」という。）とする。

- ・個人がマイナポータル API 等を活用して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、予防接種歴、乳幼児健診、特定健診、薬剤情報等が挙げられる。

※「個人がマイナポータル API 等を活用して入手可能な健康診断等の情報」は、健康保険組合等から入手する場合又は個人が自らアプリ等に入力する場合も含む。

1. 2. 本指針の対象事業者

健診等情報を取り扱う PIIR サービスを提供する民間事業者（以下「PIIR 事業者」という。）

※専ら個人が自ら日々計測するバイタル又は健康情報等ののみを取り扱う事業者は、対象事業者としては含めない。

※個人の健康管理ではなく、専ら研究開発の推進等を目的として利用される健診等情報又は匿名加工情報ののみを取り扱う事業者は、対象事業者としては含めない。

1. 3. 本指針に記載のない事項の取扱い

本指針は、個人情報保護法を踏まえ、「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）」（平成 28 年個人情報保護委員会告示第 6 号）並びにマイナポータル API 連携に際して遵守が求められる「マイナポータル API 利用規約」（令和 2 年内閣府大臣官房番号制度担当室）、「マイナポータル自己情報取得 API 利用ガイドライン」（令和元年内閣府大臣官房番号制度担当室）及び「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」（独立行政法人情報処理推進機構セキュリティセンター）の「4 共通して実施すべき対策」を基礎とし、PIIR 事業者が行う健診等情報の適正な取扱いの確保に関する活動を支援するために、具体的な遵守すべき事項を示すものである。

なお、本指針は、個人情報保護法上の主な要求事項を記載しており、本指針に記載のない事項及び関係条文については、上記法令等に加え、「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（平成 28 年個人情報保護委員会告示第 7 号）、「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）」（平成 28 年個人情報保護委員会告示第 8 号）、「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」（平成 28 年個人情報保護委員会告示第 9 号）、「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）及び「「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関する Q&A」（平成 29 年個人情報保護委員会）の最新版をそれぞれ参照されたい。

また、患者等の指示に基づいて医療機関等から医療情報を受領する事業者は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（令和 2 年 8 月総務省、経済産業省）の遵守が求められる。

2. 情報セキュリティ対策

2. 1. 安全管理措置

(1) 法規制に基づく遵守すべき事項

PIHR 事業者は、健診等情報を取り扱うに当たって、その漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置を講じなければならない。

具体的に講じるべき対策の内容に関しては、下記(2)に掲げる対策の例を参照し、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、事業規模及び性質、個人データの取扱状況(取り扱う個人データの性質及び量を含む。)並びに、個人データを記録した媒体の性質等に起因するリスクに応じて必要かつ適切な対策を講じなければならない。

(2) 本指針に基づく遵守すべき事項

以下では、PIHR 事業者が情報セキュリティを確保する上で実施すべき対策について示す。各項目においては、実施すべきリスクマネジメント施策を記載し、その下に当該施策を実現する上での具体的な対策のポイントを示し、更に、分かりやすさの観点から、必要に応じて、より細かな手法例を追加している。

PIHR 事業者において具体的な対策を講じる上では、このうち、対策のポイントの部分を参照し、当該部分に規定される内容又はそれと同等程度以上の対策を講じることが求められる。

(凡例)

■ 対策

- 対策のポイント
- ・ 対策の例

① 情報セキュリティに対する組織的な取り組み

■ 情報セキュリティに関する経営者の意図が従業員に明確に示されている

- 経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持つこと。
- 情報セキュリティポリシーを定期的に見直しすること。

■ 情報セキュリティ対策に関わる責任者と担当者を明示する

- 責任者として情報セキュリティ及び経営を理解する立場の人を任命すること。
- 責任者は、各セキュリティ対策について(社内外を含め)、責任者及び担当者それぞれの役割を具体化し、役割を徹底すること。

■ 管理すべき重要な情報資産を区分する

- 管理すべき健診等情報を他の情報資産と区分すること。
- 情報資産の管理者を定めること。
- 重要度に応じた情報資産の取扱指針を定めること。
- 健診等情報を取り扱う人の範囲を定めること。

■ 個人情報の取扱状況を確認する手段を整備する

- 例えば次のような項目をあらかじめ明確化しておくことにより、個人情報の取扱状況を把握可能としておく。

(例)

- ・ 個人情報データベース等の種類、名称及び個人データの項目
- ・ 責任者、取扱部署
- ・ 利用目的
- ・ アクセス権を有する者 等

■ 健診等情報については、入手、作成、利用、保管、交換、提供、消去及び廃棄における取扱手順を定める

- 各プロセスにおける作業手順を明確化し、決められた担当者が、手順に基づいて作業を行っていること。
- 健診等情報に対して、漏洩及び不正利用を防ぐ保護対策を行っていること。

(例)

- ・ 健診等情報を取り扱う人に対してのみ、アクセス可能とすること。
- ・ 健診等情報の取扱い履歴を残しておくこと。
- ・ 健診等情報を確実に消去又は廃棄すること。 等

■ 外部の組織と情報をやり取りする際に、情報の取扱いに関する注意事項について合意を取る

- 契約書及び委託（再委託等を含む。以下同じ）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ること。

(例)

- ・ システム開発を委託する際の本番データ取扱い時の際の情報管理、例えば管理体制、受託情報の取扱い、受け渡し、返却及び廃棄等について、注意事項を含めること。
- ・ 関係者のみにデータの取扱いを制限すること。
- ・ 外部の組織との間で情報を授受する場合、情報受渡書を以ておこなうこと。
- ・ 契約に基づく作業に遂行することによって新たに発生する情報（例：新たに作製された統計化又は加工された情報等）の取扱いを含めること。 等

■ 個人データの取扱いを委託する場合は委託先での安全管理措置を確保する

- 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、監督を行うこと。

■ 取扱状況を把握するとともに、安全管理措置の見直しを行う

- 個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施すること。
- 外部の主体による監査活動と合わせて、監査を実施すること。

- 従業者（派遣を含む。）に対し、セキュリティに関して就業上何をしなければいけないかを明示する
 - 従業者を採用する際に、守秘義務契約又は誓約書を交わしていること。
 - 秘密保持に関する事項を就業規則等に盛り込むなど、従業者が順守すべき事項を明確にしていること。
 - 違反した従業員に対する懲戒手続きが整備されていること。
 - 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等、具体的に企業機密に接する際に、退職後の機密保持義務も含む誓約書を取ることを。
- 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習得の機会を与える
 - ポリシー及び関連規程を従業員に理解させること。
 - 実践するために必要な教育を定期的に行っていること。

② 物理的セキュリティ

- 健診等情報を保管したり、扱ったりする場所の入退管理及び施錠管理を行う
 - 健診等情報を保管したり、扱ったりする区域を定めていること。
 - 健診等情報を保管している部屋（事務室）又はフロアーへの侵入を防止するための対策を行っていること。
 - 健診等情報を保管している部屋（事務室）又はフロアーに入ることができる人を制限し、人退の記録を取得していること。
- 重要なコンピュータ及び配線は地震等の自然災害又はケーブルの引っ掛けなどの人的災害による重大な被害が起こらないように配置又は設置する
 - 重要なコンピュータは許可された人だけが入ることができる安全な場所に設置すること。
 - 電源及び通信ケーブルなどは、従業員が容易に接触できないようにすること。
 - 重要なシステムについて、地震等による転倒防止、水濡れ防止及び停電時の代替電源の確保等を行っていること。
- 重要な書類、モバイル PC 及び記憶媒体等について、整理整頓を行うと共に、盗難防止対策、紛失対策及び確実な廃棄を行う

（健診等情報を記載した書類について）

- 不要になった場合、シュレッダー又は焼却等により確実に処分すること。
- 健診等情報を記載した書類を保管するキャビネットには、施錠管理を行うこと。
- 健診等情報が存在する机上、書庫及び会議室等は整理整頓を行うこと。
- 郵便物、FAX 及び印刷物等の放置は禁止。重要な書類の裏面を再利用しないこと。

（モバイル PC 及び記憶媒体等について）

- クラウド上のデータを含め、保存した情報が不要になった場合、消去ソフトを用いるなど、確実に処分していること。
- モバイル PC 及び記憶媒体については、盗難防止対策及び紛失対策を行うこと。
- 許可なく私有 PC を会社に持ち込んだり、私有 PC で業務を行ったりしないこと。

③ 情報システム及び通信ネットワークの運用管理

■ 情報システムの運用に関して運用ルールを策定する

- システム運用におけるセキュリティ要求事項を明確にしていること。
 - 情報システムの運用手順書（マニュアル）を整備していること。
 - システムの運用状況を点検していること。
 - システムにおいて実施した操作、障害及びセキュリティ関連イベントについてログ（記録）を取得していること。
- （ログを取得する項目例）
- ・ 個人情報データベース等の利用又は出力の状況
 - ・ 個人データが記載又は記録された書類及び媒体等の持ち運び等の状況
 - ・ 個人情報データベース等の削除又は廃棄の状況（委託した場合の消去又は廃棄を証明する記録を含む。）
 - ・ 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）
- 設備（具体例）の使用状況を記録していること。
 - 取得したログ（記録）については、定期的なレビューを行い、不正なアクセス等がないことを確認すること。

■ ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う

- ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行っていること。
- ウイルス対策ソフトが持っている機能（ファイアウォール機能、スパムメール対策機能及び有害サイト対策機能）を活用すること。
- 各サーバ及びクライアント PC について、定期的なウイルス検査を行っていること。
- 組織で許可されていないソフトウェアのインストール及びサービスの利用の禁止又は使用制限を行っていること。
- PHR サービスの利用者に対して、適切なセキュリティ対策を利用端末に行うように啓発すること。

■ 導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う

- 脆弱性の解消（修正プログラムの適用及び Windows update 等）を行っていること。
- 脆弱性情報及び脅威に関する情報の入手方法を確認し、定期的に収集すること。
- 情報システム導入の際に、不要なサービスの停止等、セキュリティを考慮した設定を実施するなどの対策が施されているかを確認すること。
- Web サイトの公開にあたっては、不正アクセス又は改ざんなどを受けないような設定又は対策を行い、脆弱性の解消を行うこと。

➤ Web ブラウザ及び電子メールソフトのセキュリティ設定を行うこと。

■ 通信ネットワークを流れる重要なデータに対して、暗号化等の保護策を実施する

- TLS (version1.2 以上) 等を用いて通信データを暗号化すること。
- 外部のネットワークから内部のネットワーク又は情報システムにアクセスする場合には、VPN 等を用いて暗号化した通信路を使用していること。
- 電子メールをやり取りする際に、健診等情報については暗号化するなど保護策を講じること。

■ モバイル PC、USB メモリなどの記憶媒体又はデータを外部に持ち出す場合、盗難、紛失等に備えて、適切なパスワード設定又は暗号化等の対策を実施する

- モバイル PC 又は USB メモリ等の使用や外部持ち出しについて、規程を定めていること。
- 外部でモバイル PC 又は USB メモリ等を使用する場合の紛失や盗難対策を講じていること。
- モバイル PC 又は USB メモリ等を外部に持ち出す、若しくはクラウド上のストレージを取り扱う際は、その使用者の認証 (ID 及びパスワード設定並びに USB キー、IC カード認証又はバイオメトリクス認証等) を行うこと。
- 保存されているデータを、重要度に応じて HDD 暗号化又は BIOS パスワード設定等の技術的対策を実施すること。
- モバイル PC 又は USB メモリ等を持ち出す場合の持出者並びに持出及び返却の管理を実施すること。
- 盗難又は紛失時に情報漏えいの脅威にさらされた情報が何かを正確に把握するため、持ち出し情報の一覧及び内容の管理を行うこと。

■ 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。

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

■ 情報 (データ) 及び情報システムへのアクセスを制限するために、システム管理者の ID の管理 (パスワード等認証情報の管理等) を行う

- システム管理者毎に ID 及びパスワード等を割当て、当該 ID 及びパスワード等による識別及び認証を確実にすること。
- システム管理者 ID の登録及び削除に関する規程を整備すること。
- パスワードによる認証を採用する場合、その定期的な見直しを求めること。(ただし、2 要素認証を採用している場合等を除く。) また、容易に類推できないパスワードとし、極端に短い文字列を使用しない (英数、記号を混在させた 8 文字以上の文字列とすることが望ましい) ようシステム管理者に求めること。

- 離席する際は、パスワード等で保護されたスクリーンセーバーでパソコンを保護すること。
- 不要になったシステム管理者の ID を削除すること。

■ 健診等情報に対するアクセス権限の設定を行う

- 健診等情報に対するアクセス管理方針を定め、システム管理者毎にアクセス可能な情報、情報システム、業務アプリケーション及びサービス等を設定すること。
- 職務の変更又は異動に際して、システム管理者のアクセス権限を見直すこと。

■ インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング及び IPS サービス等）を行う

（外部から内部への不正アクセス対策）

- 外部から内部のシステムにアクセスする際、確実な認証を実施すること。
- 保護すべき健診等情報のデータベースは、サービス利用者が利用する機能（閲覧等）及び保守点検時のリモート管理機能を除き、外部接続しているネットワークから物理的に遮断する又はセグメント分割することによりアクセスできないようにすること。

（内部から外部への不正アクセス対策）

- 不正なプログラムをダウンロードさせるおそれのあるサイトへのアクセスを遮断するような仕組み（フィルタリングソフトの導入等）を行っていること。

■ 無線 LAN のセキュリティ対策（WPA2 の導入等）を行う

- 無線 LAN において健診等情報の通信を行う場合は、暗号化通信（WPA2 等）の設定を行うこと。
- 無線 LAN の使用を許可する端末（MAC 認証等）及びその使用者の認証を行うこと。

■ ソフトウェアの選定及び購入、情報システムの開発及び保守並びにサービス利用に際して、情報セキュリティを前提とした管理を行う

- 情報システムの設計時に安全性を確保し、継続的に見直すこと（情報システムの脆弱性を突いた攻撃への対策を講ずることを含む。）。
- ソフトウェア及びクラウド等の他者が提供するサービスの導入及び変更に関する手順を整備し、本指針のセキュリティ対策の遵守を確認すること。
- システム開発において、レビューを実施し、その記録を残していること。
- 外部委託によるソフトウェア開発を行う場合、使用許諾及び知的財産等について取り決めていること。
- 開発又は保守を外部委託する場合に、セキュリティ管理の実施状況を把握できること。

⑤ 情報セキュリティ上の事故対応

■ 情報システムに障害が発生した場合、業務を再開するための対応手順を整理する

- 情報システムに障害が発生した場合に、最低限運用に必要な時間及び許容停止時間を明確にしておくこと。
- 障害対策の仕組みが組織として効果的に機能するよう、よく検討していること。
- システムの切り離し（即応処理）、必要なサービスを提供できるような機能（縮退機能）、情報の回復及び情報システムの復旧に必要となる機能等が、障害時に円滑に機能するよう確認しておくこと。
- 日常のシステム運用の中で、バックアップデータ及び運用の記録等を確保しておくこと。
- 障害発生時に必要な対応として、障害発生時の報告要領（電話連絡先の認知等）、障害対策の責任者と対応体制、システム切替え及び復旧手順並びに障害発生時の業務実施要領等の準備を整えておくこと。

（例）

- ・ 大容量データの復元には時間を要するため、復元に要する時間の事前見積りの実施
- 関係者への障害対応要領の周知、必要なスキルに関する教育及び訓練等の実施を行っていること。

■ 情報セキュリティに関連する事件又は事故等（ウイルス感染、情報漏えい等）の緊急時の対応手順を整理する

- ウイルス感染又は情報漏えい等の発生時の組織内の関係者への報告、緊急処置の適用基準及び実行手順、被害状況の把握、原因の把握、対策の実施、被害者ほか影響を受ける可能性のある本人への連絡、外部への周知方法、個人情報保護委員会への報告、通常システムへの復旧手順並びに業務再開手順等を整えておくこと。

（例）

- ・ ウイルス感染の場合、ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、コンピュータの検査を実施し、ワクチンソフトのベンダの Web サイト等の情報を基に、検出されたウイルスの駆除方法等を試すことが必要となる。
- 情報漏えいの場合、事実を確認したら速やかに責任者に報告し、対応体制を取ること、対応についての判断を行うため 5W1H の観点で調査し情報を整理すること、対策本部で対応方針を決定すること及び被害の拡大防止と復旧のための措置を行うことが必要となる。また、漏えいした個人情報の本人及び取引先等への通知、個人情報保護委員会及び監督官庁等への報告並びにホームページ又はマスコミ等による公表についても検討する必要がある。

2. 2. 第三者認証の取得

（1）本指針に基づく遵守すべき事項

PHR 事業者は、リスクマネジメントシステムを構築するに際して、本指針の対策例に加えて、

標準規格（ISO 又は JIS）等に準拠した対策の追加及び第三者認証（ISMS 又はプライバシーマーク等）を取得することで、客観的に安全管理措置を担保するよう努めなければならない。

ただし、マイナポータル API 経由で健診等情報を入手する PHR 事業者においては、第三者認証を取得しなければならない。

3. 個人情報の適切な取扱い

3. 1. 情報の公表

3. 1. 1. 利用目的の特定

(1) 法規制に基づく遵守すべき事項

① 利用目的の特定

PHR 事業者は、健診等情報を取り扱うに当たっては、その利用目的をできる限り特定しなければならない。また、PHR 事業者は、上記によって特定した利用目的の達成に必要な範囲を超えて、健診等情報を取り扱ってはならず、仮に当該範囲を超える利用目的のために健診等情報を取扱う場合は、後述するとおり、あらかじめ本人の同意を得なければならない。

また、利用目的を単に抽象的又は一般的に特定するのではなく、個人情報に PHR 事業者において、最終的にどのような事業の用に供されるのか、どのような目的で個人情報を利用されるのか、本人にとって一般的かつ合理的に想定できる程度に具体的に特定するように努めなければならない。

② 利用目的の変更

PHR 事業者は、健診等情報を取得する当初に公表又は通知していた利用目的を変更する場合について、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。この場合は、変更された利用目的を本人に通知するか、又は公表しなければならない。

なお、この「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」に関しては、変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲となることが必要であり、それを超える範囲で変更する場合は、後述するとおり、改めての本人の同意取得が必要となる。

3. 1. 2. 利用目的の明示等

(1) 法規制に基づく遵守すべき事項

① 利用目的の明示

PHR 事業者は、例えば契約書のような書面等への記載又はユーザー入力画面等への打ち込みなどにより、直接本人から健診等情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示しなければならない。

この場合、本人に対して、その利用目的を明確に示すことが必要であり、事業の性質及び健診等情報の取扱状況に応じて、内容が本人に認識される合理的かつ適切な方法による必要がある。

② 保有する健診等情報等の本人への開示

PHR 事業者は、本人からの請求があった場合、保有する当該本人に係る健診等情報（保有個人データ）を開示しなければならない。

具体的な開示の手続きに関しては各 PHR 事業者において定めることが必要であるが、例えば同一の本人から、複雑な対応を要する同一内容について繰り返し開示の請求があり、事実

上問合せ窓口が占有されることによって他の問合せ対応業務が立ち行かなくなるなど、業務上著しい支障を及ぼすおそれがある場合等には、開示をしないことが認められている。

(2) 本指針に基づく遵守すべき事項

① サービス利用規約及びプライバシーポリシー等の公表

PIIR 事業者は、利用者及び第三者が当該 PIIR 事業者の取組について評価できるよう、プライバシーポリシー及びサービス利用規約をホームページに掲載するなどにより公表しなければならない。その際、サービス利用規約の概要版を必要に応じて作成するとともに、ホームページのアクセスしやすい場所に掲載するなど分かりやすく公表しなければならない。

3. 2. 同意取得

(1) 法規制に基づく遵守すべき事項

① 健診等情報取得に係る事前の同意取得

本指針の対象となる健診等情報は個人情報保護法上の要配慮個人情報に該当するため、その取得に際しては、あらかじめ、本人からの同意取得が必要であり、オプトアウト手続きによる取得は認められていない。

また、当初の利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合は、改めて本人の同意を得なければならない。また、下記②に記載する事業の承継後に、承継前の当初の利用目的の達成に必要な範囲を超えて、健診等情報を取り扱う場合にも、改めて本人の同意を得なければならない。

② 第三者提供に係る事前の同意取得

要配慮個人情報の第三者提供には、個人情報保護法に基づき同意が不要となる場合を除き、原則として、あらかじめ、本人の同意が必要であり、またオプトアウト手続きによる健診等情報の第三者提供は認められていない。

また、同意の取得に当たっては、事業の規模及び性質並びに個人データの取扱状況（取り扱う個人データの性質及び量を含む。）等に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示さなければならない。

ただし、要配慮個人情報であっても、事業者が、委託、事業承継又は共同利用により当該情報を提供する場合は、第三者提供に該当せず、例えば以下の場合に関しては、あらかじめ本人の同意を得る必要はない。

なお、要配慮個人情報を第三者提供の方法により取得する場合、上記①に従って、提供元が本人から必要な同意（要配慮個人情報の取得及び第三者提供に関する同意）を取得していることが前提となるため、提供を受けた PIIR 事業者が、改めて本人から要配慮個人情報の取得に関する同意を得る必要はないが、当該提供者について、その法人名、住所及び当該提供者が提供された健診等情報を取得した経緯等を確認しなければならない。

(健診等情報の第三者提供に係る同意取得が不要な場合の例)

【個人情報保護法に列挙される例外に該当する場合】

■ 法令に基づく場合

- 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
- 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
- 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。

【第三者提供に該当しない場合の例】

- 委託：保険者が被保険者に対して PHR アプリを保険者のサービスの一環として提供する際に PHR アプリの管理運営会社に個人データを提供する。
- 事業承継：PHR 事業を別の企業に譲渡し、譲渡先企業に個人データを提供する。
- 共同利用（※）：PHR サービスを行っている企業が、例えば同グループに属する企業等と共に総合的な健康サービスを提供するために、取得時の利用目的の範囲内で個人データを共同利用する。

（※）ただし、上記のうち共同利用に関しては、あらかじめ、次に掲げる事項を本人に通知又は本人が容易に知り得る状態に置いておくことが必要である。

- 共同利用をする旨
- 共同して利用される個人データの項目
- 共同して利用する者の範囲
- 利用する者の利用目的
- 当該個人データの管理について責任を有する者の氏名又は名称

③ 外国における第三者への提供

PHR 事業者は、外国にある第三者と連携して我が国内でサービスを提供する場合等に、当該外国にある第三者に健診等情報を提供する際には、原則として、あらかじめ本人から、外国にある第三者への個人データの提供を認める旨の同意を得なければならない。

（２）本指針に基づく遵守すべき事項

① 健診等情報取得に係る同意取得時の利用目的の通知

PHR 事業者は、健診等情報の取得に際しては、利用目的をできる限り特定し、利用目的及びその範囲等について、例えば、本指針に関する Q&A に示されているような方法により、サービス利用規約の概要を提示するなど、分かりやすく通知した上で、本人の同意を得なければならない。

なお、健診等情報以外の個人情報も取り扱う場合には、当該情報についての利用目的の範囲内であることを確認すること。

② 第三者提供に係る同意取得

PHR 事業者は、健診等情報の第三者提供に際しては、提供先、その利用目的（必要に応じてその概要を提示する）及び提供される個人情報の内容等を特定し、分かりやすく通知した

上で、本人の同意を得なければならない。また、同意があった場合でも、本人の不利益が生じないよう配慮しなければならない。

③ 利用者による同意状況の確認

過去の同意内容を確認又は見直すことを希望する利用者が一定程度発生することも想定される。PIR 事業者は、そうした利用者のため、過去の同意状況を利用者が確認できる方策を確保しなければならない。

3. 3. 消去及び撤回

(1) 法規制に基づく遵守すべき事項

① 利用停止等請求を受けた場合の対応

PIR 事業者は、本人から、当該本人が識別される保有個人データが、本人の同意なく健診等情報が取得された、目的外利用がされている又は偽りその他不正の手段により取得された、という理由によって、当該保有個人データの利用の停止又は消去（以下「利用停止等」という。）の請求を受けた場合であって、その請求に理由があることが判明したときは、原則として、遅滞なく、利用停止等の措置を行わなければならない。

② 利用停止等請求への対応の例外

PIR 事業者は、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わる措置をとるときは、当該代替措置によることもできる。

(2) 本指針に基づく遵守すべき事項

① 同意の撤回

PIR 事業者は、健診等情報の取得時及び第三者提供時の当該同意の撤回について、同意する際と同程度の容易さで行えるよう、工夫しなければならない。

具体的には、本人が同意の撤回を希望した場合、同意撤回のための情報及び受付窓口が Web サイトの深層にありアクセスしにくいのは望ましくないため、同意の設定変更を容易にできる機能を提供するなど、工夫に努めなければならない。

② 健診等情報の消去

PIR 事業者は、事業終了等により健診等情報の利用の必要がなくなった場合又は本人の求めがあった場合には、当該事業者が管理している健診等情報（管理を委託している場合を含む。）を消去しなければならない。ただし、多額の費用を要する場合その他の消去を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わる措置をとるときは、当該代替措置によることもできる。

③ 長期間利用がない場合の措置

利用者によるアクセスがなく、長期間利用されない健診等情報について、本人が認知しないままに、当該情報が削除されることは望ましくないため、一定の期間、利用がない場合に

消去等の措置を講じる旨（消去を行う時期等を含む。）を利用者に通知又は公表しなければならない。

3. 4. その他

3. 4. 1. 健診等情報に含まれる利用者以外の個人情報の取扱い

（1）法規制に基づく遵守すべき事項

医師又は薬剤師等の氏名等は、要配慮個人情報には該当しないものの、医師又は薬剤師等の個人情報に該当することに留意し、利用目的の特定、同意の取得等に関して、個人情報保護法に基づき適切に取り扱わなければならない。

3. 4. 2. 匿名加工情報に関する留意事項

（1）法規制に基づく遵守すべき事項

PHR 事業者は、匿名加工情報を作成するときは、個人情報保護委員会規則で定める基準に従い当該個人情報を加工し、匿名加工情報の作成に用いた個人情報から削除した記述等及び加工方法の安全管理のための措置を講じ、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。

また、当該匿名加工情報を第三者に提供するときは、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。

4. 健診等情報の保存及び管理並びに相互運用性の確保

4. 1. 健診等情報の保存及び管理

(1) 法規制に基づく遵守すべき事項

① 正確性の確保

PHR 事業者は、個人情報データベース等への個人情報の入力時の照合及び確認の手續の整備、誤り等を発見した場合の訂正等の手續の整備、並びに記録事項の更新及び保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければならない。

② 第三者提供の記録

PHR 事業者は、健診等情報を第三者に提供したときは、原則として、提供した年月日及び提供先等に関する記録を作成し、一定期間保存しなければならない。また、第三者提供を受けた PHR 事業者は、原則として、提供を受けた年月日及び提供元等に関する記録を作成し、一定期間保存しなければならない。

4. 2. 相互運用性の確保

(1) 本指針に基づく遵守すべき事項

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。

その際、健診等情報のフォーマット等に関しては、マイナポータル API から出力される項目及びフォーマットを基本とし、また、互換性の高い汎用的なデータファイル（例えば、HL7CDA 等）とすることで、利用者が取り扱うことができるようにしなければならない。

② サービス終了時の措置

PHR 事業者がサービスを終了する場合、利用者への健診等情報のエクスポート及び他の 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しなければならない。

③ データ連携先事業者の適切性の確認

PHR 事業者間で健診等情報を利用者を介さず直接的にデータ連携する場合、データ連携先事業者が本指針に規定する対策を行っていることを、当該データ連携先事業者のホームページ等での公表内容又は第三者認証の取得状況等により確認しなければならない。

5. 要件遵守の担保

5. 1. 本指針の規定する要件を遵守していることの確認

(1) 本指針に基づく遵守すべき事項

① 自主的な確認及びその結果の公表

PIIR 事業者は、本指針の別紙チェックシートの確認事項に従って各要件を満たしているかどうかを定期的に確認し、結果を自社のホームページ等で公表しなければならない。ホームページに掲載する際は、本指針 3. 1. 2. (2) ①の「サービス利用規約及びプライバシーポリシー等の公表」における公表と同じページ等に、その結果を掲示するとともに、当該結果の概要を理解しやすいように分かりやすい表現にて記載するよう努めなければならない。

6. 本指針の見直し

PHR サービスを含め、社会における個人情報の利活用のあり方及び保護に関する考え方は、社会情勢及び個人の意識の変化等に対応して変化して行くものと考えられ、関連する法令等も、当該変化に対応して改正等が行われることが見込まれる。

そこで、本指針に関しても、個人情報保護法等の法令又はガイドラインの改正、本指針の運用状況及び PHR サービス又はセキュリティ技術等の拡大等の状況の変化を踏まえて、必要に応じて検討及び見直しを行うものとする。

用語集

アルファベット順・50 音順

BIOS	パソコンなどの主基板等に格納されたコンピュータプログラムの一種で、起動時の OS の読み込み並びに接続された装置及び機器に対する基本的な入出力制御等を行うもの。
HL7CDA	Health Level Seven Clinical Document Architecture の略語。患者診療情報を患者あるいは患者家族等に CD 等の電子媒体で提供するための規格。
IPS	Intrusion Prevention System の略語。サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して攻撃を未然に防ぐシステム。
ISMS	Information Security Management System の略語。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。
ISO	スイスのジュネーブに本部を置く非政府機関 International Organization for Standardization（国際標準化機構）の略語。ISO の主な活動は国際的に通用する規格を制定することであり、ISO が制定した規格（ISO 規格）を指して用いられることも多い。
JIS	Japanese Industrial Standards の略語。我が国の産業標準化の促進を目的とする産業標準化法（昭和 24 年法律第 185 号）に基づき制定される任意の国家規格。
LAN	Local Area Network の略語。主として同一組織内で用いられる情報通信ネットワーク。
MAC アドレス	Media Access Control（メディア・アクセス・コントロール）アドレス。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して MAC アドレスを管理しているため、原則同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。
TLS	Transport Layer Security の略語。インターネットなどのネットワークでデータを暗号化して送受信するプロトコル（通信手順）の一つ。データを送受信する一対の機器間で通信を暗号化し、中継装置などネットワーク上の他の機器による成りすましやデータの盗み見、改竄などを防ぐことができる。SSL の後継規格。
PHR	Personal Health Record の略語。一般的には、生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）である。電子記録として本人等が正確に把握し、自身の健康増進等に活用することが期待される。本指針の対象となる情報については、1. 1. に規定。

PHR サービス	利用者が、予防又は健康づくり等に活用すること並びに医療及び介護現場で役立てること等を目的として、PHR を保存及び管理並びにリコメンド等を行うサービス。
VPN	仮想私設網、Virtual Private Network の略語。不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のこと。
WPA2	Wi-Fi Protected Access 2 の略語。無線 LAN (Wi-Fi) 上で通信を暗号化して保護するための技術規格の一つで、WPA の後継。また、通信機器などが同規格に準拠していることを認定する認証制度。業界団体の Wi-Fi Alliance が運用している。
開示	(本人等からの) 開示請求に基づいて、当該請求の対象となっている保有個人情報、当該請求者に対して閲覧させ、又は写しを交付すること。 特に個人情報保護法第 28 条第 2 項に基づく場合は、書面の交付による方法(開示の請求を行った者が同意した方法があるときは、当該方法)による。
経営者	企業を経営する人。雇用関係からは使用者に同じ。所有と経営との分離していない企業にあっては、資本家・企業家などと同義。
公表	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って、広く一般に知らせること。不特定多数の人々を知ることができるように発表すること。
個人情報データベース等	個人情報を含む情報の集合物であって、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などであり、個人情報保護法に規定されている。
個人データ	個人情報データベース等を構成する個人情報。
従業員	雇われて、ある業務に従事している人。企業と労働・就労契約を結んで雇用されている人。
従業者	事業所に所属して働いている全ての人のこと。
情報資産	情報そのものと、情報を収集したり処理したり保管したりするための装置。
脆弱性	脅威によって悪用される可能性がある欠陥や仕様上の問題。
責任者	代表者によって事業者の内部の者から指名された者であって、責任及び権限を持つ人。
通知	事業の性質及び個人情報の取扱い状況に応じ、内容が認識される合理的かつ適切な方法により、直接知らしめること。開示とは異なり、必ずしも本人等からの請求に基づかない。
プライバシーマーク制度	日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度のこと。
マイナポータル	内閣府大臣官房番号制度担当室が運営する Web システムであり、やりとり履歴、利用者の情報、お知らせの表示や子育てワンストップサービス等の各種情報提供、電子申請等のサービスを提供するもの。

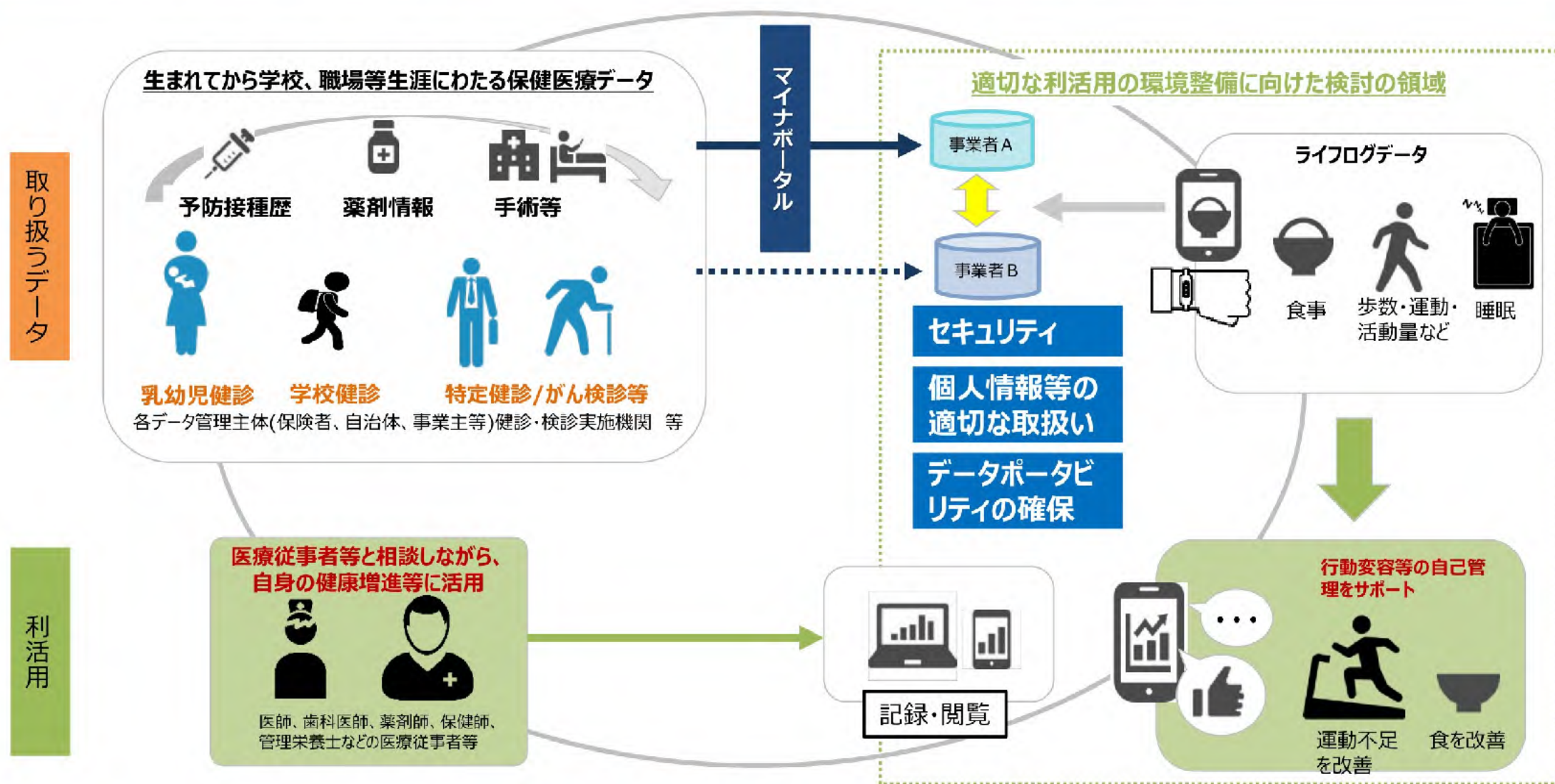
マイナポータル API	民間や行政機関等の組織が提供する外部サービスからの電子申請をマイナポータルで受け付けたり、システム利用者の同意のもと、行政機関から入手した自らの個人情報を外部サービスに提供することを可能にするもの。マイナポータル利用規約別表に掲げられる、マイナポータルが提供する API であり、外部の Web システム等が利用するもの。
無害化	プログラムにとって特別な意味を持つ可能性のある文字や文字列を検知して、一定の規則に従って別の表記に置き換えること。
ファイル無害化	ファイルの構造を分析及び分解し、一定の規則に従ってマルウェア（コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称。）の可能性のある部分を取り除いて、安全なファイルに再構築すること。
明示	事業の性質及び個人情報の取扱状況等に応じ、内容が認識される合理的かつ適切な方法によって、明確に示すこと。相手方が内容を理解できるよう、分かりやすく示すことが必要。
無線 LAN	無線でデータの送受信を行なう LAN のこと。
要配慮個人情報	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個人情報保護法施行令で定める記述等が含まれる個人情報をいう。施行令では、(1)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、(2)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（次号において「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（同号において「健康診断等」という。）の結果、(3)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などが規定されている。

参考資料集

PHR（Personal Health Record）サービス の利活用に向けた国の検討経緯について

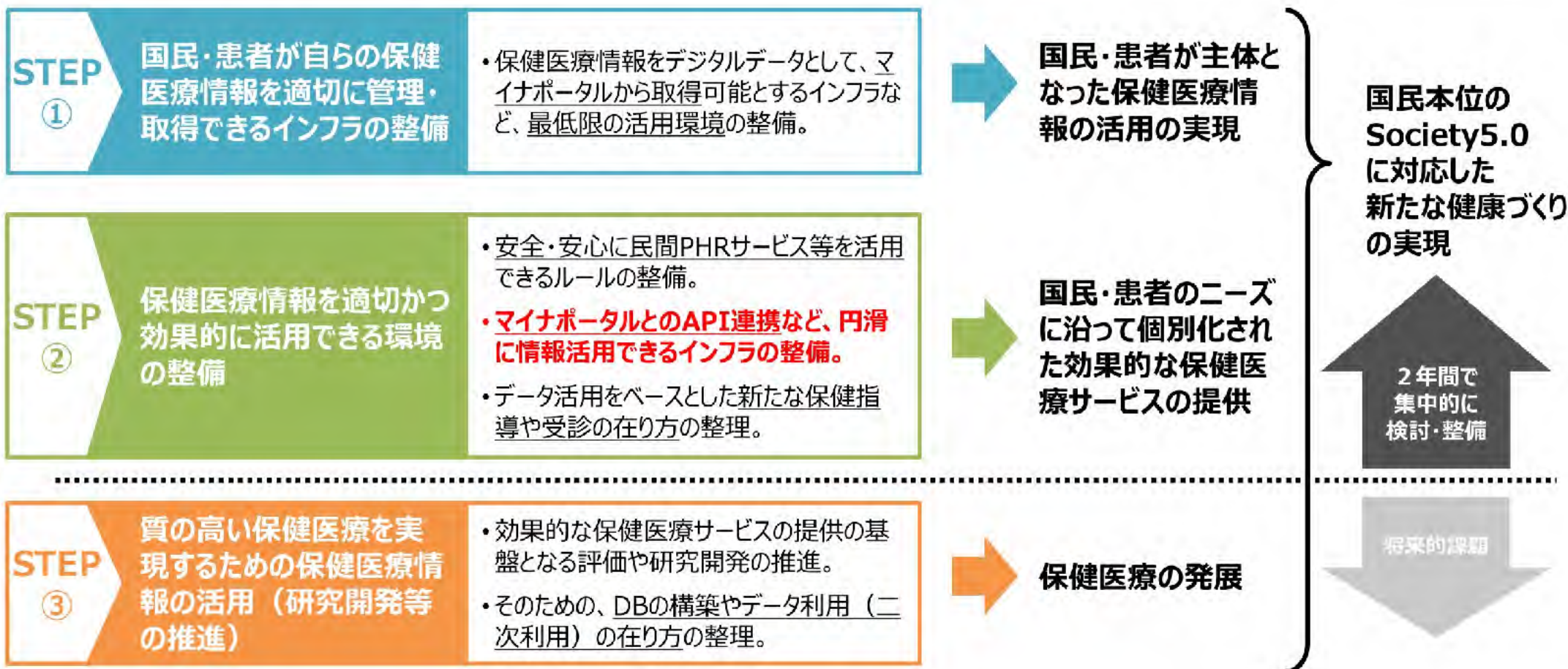
PHR（Personal Health Record）の利活用

- 生まれてから学校、職場等生涯にわたる個人の健康データをマイナポータル等を通じ本人自身が予防・健康づくり等への活用や同サービスの普及展開を図る。



健康・予防・重症化予防に健康データを活用

- 今後、保健医療分野では、予防・健康増進の重要性が高まるとともに、個別化されたより効果的な介入等への期待が高まっている。
- そのためには、保健医療情報の適切かつ効果的に活用できる環境を整備することが必要。具体的には、
 - ① 国民・患者が自らの保健医療情報を**適切に管理・取得**できるインフラの整備
 - ② 保健医療情報を**適切かつ効果的に活用**できる環境の整備
 - ③ **質の高い保健医療を実現**するための保健医療情報の活用（研究開発等の推進）
 を目指し、取組を進めていくことが必要。



- 国民が効果的に保健医療情報を活用できる環境を整備するためには、公的に最低限の利用環境を整備するとともに、民間PHR事業者の活力を用いることが必要不可欠。
 - 個人が取得した保健医療情報を自身で適切に管理できるようにする。
⇒ 相互運用性、情報流出・二次利用対策など
 - 個人のニーズに応じて、保健医療情報を安全・安心かつ効果的に利活用できるようにする。
⇒ 民間サービスとの連携、医療機関等への提示など
 - 将来的に、保健医療の発展（サービスの質の向上）に向けて、適切に研究開発等へ活用できるようにする。

実現に向けて以下の整備が必要

安全・安心に民間PHRサービス等を活用できるルールの整備

- 国民が安心して民間PHRサービスを活用するには、事業者が遵守すべき情報の管理・利活用に係る基準（情報セキュリティ、利用目的、同意取得、相互運用性など）を整理することが必要。

マイナポータルとのAPI連携

- 個人が、データファイルをダウンロードして、事業者にデータファイルを提供する等の手間等をなくすために、API連携が必要。

(課題)

- ✓ (マイナポータルAPI連携に求める基準の整理を含む) 適切なルールの整備。
- ✓ (マイナポータルAPI連携に係るものを含む) ルールの要件を満たしていることを証明するための仕組み。
- ✓ サービスの技術革新のスピードに対応できる見直しの体制。

(参考) データヘルス集中改革プラン等の工程の具体化 (案)

第6回健康・医療・介護情報活用検討会、
第5回医療等情報活用WG及び第3回健診等情報活用WG
(令和2年12月9日) 資料3を抜粋

ACTION 1 : 全国で医療情報を確認できる仕組みの拡大

患者や全国の医療機関等で医療情報を確認できる仕組みについて、対象となる情報（薬剤情報に加えて、手術・移植や透析等の情報）を拡大し、令和4年夏を目途に運用開始

ACTION 2 : 電子処方箋の仕組みの構築

重複投薬の回避にも資する電子処方箋の仕組みについて、オンライン資格確認等システムを基盤とする運用に関する要件整理及び関係者間の調整を実施した上で、整理結果に基づく必要な法制上の対応とともに、医療機関等のシステム改修を行い令和4年夏を目途に運用開始

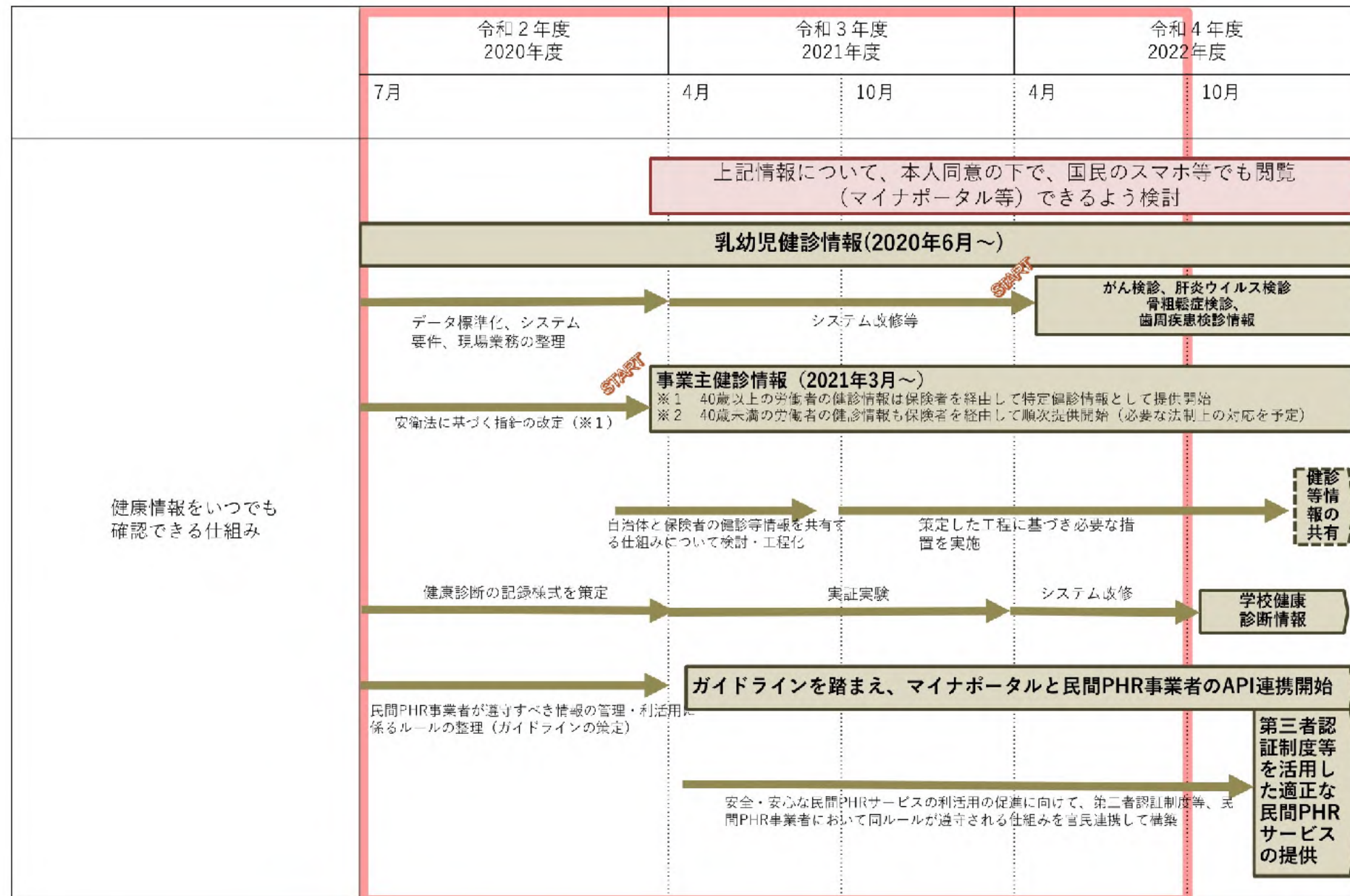
ACTION 3 : 自身の保健医療情報を活用できる仕組みの拡大

PCやスマートフォン等を通じて国民・患者が自身の保健医療情報を閲覧・活用できる仕組みについて、健診・検診データの標準化に速やかに取り組むとともに、対象となる健診等を拡大するため、令和3年に必要な法制上の対応を行い、令和4年度早期から順次拡大し、運用



(参考) データヘルス集中改革プラン等の工程の具体化 (案)

第6回健康・医療・介護情報利活用検討会、
第5回医療等情報利活用WG及び第3回健診等情報利活用WG
(令和2年12月9日) 資料3を抜粋



PHR利活用に向けた国の基本的指針の概要及び参考資料

基本的指針のポイント

- 本指針は、国民・患者本人が取得した健診等情報を、自身のニーズから民間PHR（Personal Health Record）サービスを用いて、予防・健康づくりに活用すること等を想定して、PHRサービスを行う民間PHR事業者における当該情報の取り扱いについて整理した。
- 健診等情報の機微性等を鑑み、個人情報保護法等に定められた対応に加え、丁寧な同意、情報セキュリティ対策、申出に応じた消去、自己点検と結果の公表等の必要な対応を民間PHR事業者を求めるものである。
- これにより、業界の健全な発展や、個人による安全・安心なPHRサービスの利活用の促進を目指す。

● 指針の位置づけ

0	基本的考え	・健診等情報を取り扱うサービスを提供する民間PHR事業者が法規制に加えて、適正なPHRの利活用を促進するために遵守することが必要と考えられる事項を含めて提示
1	指針の対象	・対象情報：個人が自らの健康管理に利用可能な要配慮個人情報（「健診等情報」と定義（健診等情報の具体例として、予防接種歴、乳幼児健診、特定健診、薬剤情報等） ・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

● 民間PHR事業者による健診等情報の取扱いに関する要件（制度上の要求事項に上乗せする主な事項）

2	情報セキュリティ対策	・リスクマネジメントシステムを構築する上で第三者認証（ISMS又はプライバシーマーク等）を取得することに努める。ただし、マイナポータルAPI経由で健診等情報を入手する事業者においては、第三者認証を取得すべき 等
3	個人情報の適切な取扱い	・プライバシーポリシーやサービス利用規約を分かりやすく作成し、ホームページに掲載するなど義務化 ・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、分かりやすく通知した上での同意の徹底 ・本人同意があった場合でも、本人の不利益が生じないように配慮 ・同意撤回が容易に行える環境の整備 ・健診等情報の利用がなくなったり本人の求めがあった場合、健診等情報を消去又は本人の権利利益を保護するため必要な代替措置を行う 等
4	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、民間PHR事業者から利用者へのエクスポート機能及び利用者から民間PHR事業者へのインポート機能について備えるべき 等
5	その他（要件遵守の担保方法など）	・対象事業者は、自己チェックシート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ホームページ等で公表すべき 等

本指針の要件に係るチェックシート（案）

事業者	1. 事業者の名称	2. 事業者の代表者	3. 事業者の所在地
1. 事業者の名称	2. 事業者の代表者	3. 事業者の所在地	4. 事業者の事業内容
5. 事業者の代表者	6. 事業者の代表者	7. 事業者の代表者	8. 事業者の代表者
9. 事業者の代表者	10. 事業者の代表者	11. 事業者の代表者	12. 事業者の代表者
13. 事業者の代表者	14. 事業者の代表者	15. 事業者の代表者	16. 事業者の代表者
17. 事業者の代表者	18. 事業者の代表者	19. 事業者の代表者	20. 事業者の代表者
21. 事業者の代表者	22. 事業者の代表者	23. 事業者の代表者	24. 事業者の代表者
25. 事業者の代表者	26. 事業者の代表者	27. 事業者の代表者	28. 事業者の代表者
29. 事業者の代表者	30. 事業者の代表者	31. 事業者の代表者	32. 事業者の代表者
33. 事業者の代表者	34. 事業者の代表者	35. 事業者の代表者	36. 事業者の代表者
37. 事業者の代表者	38. 事業者の代表者	39. 事業者の代表者	40. 事業者の代表者
41. 事業者の代表者	42. 事業者の代表者	43. 事業者の代表者	44. 事業者の代表者
45. 事業者の代表者	46. 事業者の代表者	47. 事業者の代表者	48. 事業者の代表者
49. 事業者の代表者	50. 事業者の代表者	51. 事業者の代表者	52. 事業者の代表者
53. 事業者の代表者	54. 事業者の代表者	55. 事業者の代表者	56. 事業者の代表者
57. 事業者の代表者	58. 事業者の代表者	59. 事業者の代表者	60. 事業者の代表者
61. 事業者の代表者	62. 事業者の代表者	63. 事業者の代表者	64. 事業者の代表者
65. 事業者の代表者	66. 事業者の代表者	67. 事業者の代表者	68. 事業者の代表者
69. 事業者の代表者	70. 事業者の代表者	71. 事業者の代表者	72. 事業者の代表者
73. 事業者の代表者	74. 事業者の代表者	75. 事業者の代表者	76. 事業者の代表者
77. 事業者の代表者	78. 事業者の代表者	79. 事業者の代表者	80. 事業者の代表者
81. 事業者の代表者	82. 事業者の代表者	83. 事業者の代表者	84. 事業者の代表者
85. 事業者の代表者	86. 事業者の代表者	87. 事業者の代表者	88. 事業者の代表者
89. 事業者の代表者	90. 事業者の代表者	91. 事業者の代表者	92. 事業者の代表者
93. 事業者の代表者	94. 事業者の代表者	95. 事業者の代表者	96. 事業者の代表者
97. 事業者の代表者	98. 事業者の代表者	99. 事業者の代表者	100. 事業者の代表者

※一部抜粋。要件毎にチェック項目を記載

1 対象情報及び対象事業者

● 対象情報：

個人が自らの健康管理に利用可能な「個人情報の保護に関する法律」上の要配慮個人情報で、次に掲げるもの（以下「健診等情報」という。）とする。

- ・個人がマイナポータルAPI等を活用して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、予防接種歴、乳幼児健診、特定健診、薬剤情報等が挙げられる。

※「個人がマイナポータルAPI等を活用して入手可能な健康診断等の情報」は、健康保険組合等から入手する場合又は個人が自らアプリ等に入力する場合も含む。

● 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（以下「PHR事業者」という。）

※専ら個人が自ら日々計測するバイタル又は健康情報等のみを取り扱う事業者は、対象事業者としては含めない。

※個人の健康管理ではなく、専ら研究開発の推進等を目的として利用される健診等情報又は匿名加工情報のみを取り扱う事業者は、対象事業者としては含めない。

(参考) 国内におけるPHRサービス

●PHR (Personal Health Record)

一般的には、生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）である。電子記録として本人等が正確に把握し、自身の健康増進等に活用することが期待される。

●PHRサービス

利用者が、予防又は健康づくり等に活用すること並びに医療及び介護現場で役立てること等を目的として、PHRを保存及び管理並びにリコmend等を行うサービス。

(様々な民間PHRサービスの例)



個人が健康改善目的で利用

- ・食事の写真を撮影するとアプリ上で栄養の推計値の表示やスコア化が行われるとともに、不足している栄養素が紹介や対応するメニューを提示する等の食事管理・食事改善を目的としたアプリサービス
- ・ウェアラブルデバイス等から収集した日々の体重、歩数、睡眠等を用いて、日々の運動の記録・改善を目的としたアプリサービス 等

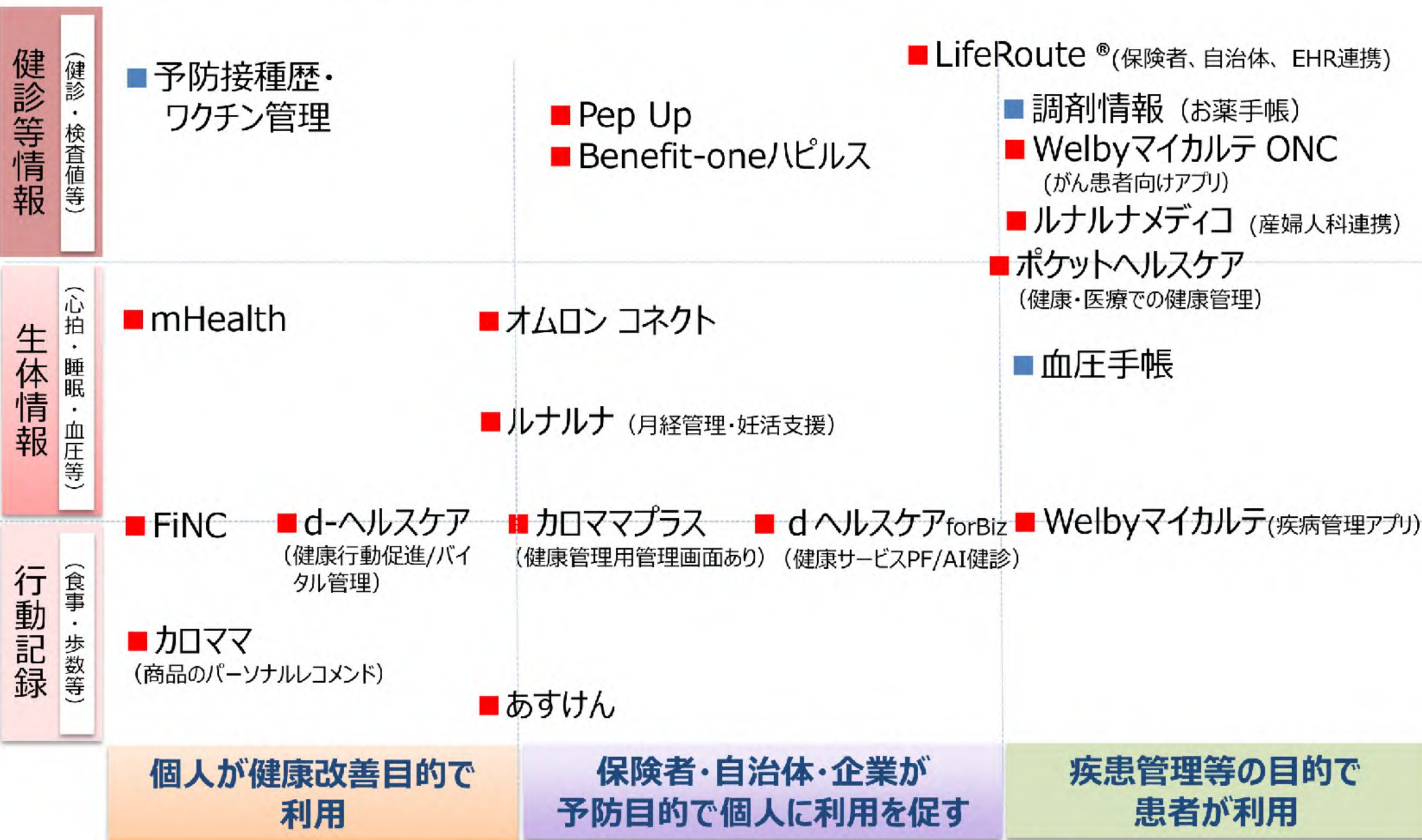
保険者・自治体・企業が予防目的で個人に利用を促す

- ・特定健診データ等をもとにした保健指導・運動プログラムの提供と、企業の健康経営・福利厚生・その他サービスとの組合せとして、保険者・自治体等が被保険者・住民等に対して提供するアプリサービス
- ・電子母子健康手帳や健診・予防接種データ共有など母子への健康支援を目的に提供するアプリサービス 等

疾患管理等の目的で患者が利用

- ・患者自身が、日々の血圧データを記録し、患者自身が閲覧するほか、外来時に医師に掲示するアプリサービス
- ・医師が、生活習慣病患者に対して、外来の合間の健康管理を目的として日常生活の健康データを用いたアプリの利用を促し、外来時に当該利用状況を提示してもらうほか、患者が選択した医療機関がリアルタイムで閲覧できるアプリサービス 等

(参考) 国内における主なPHRサービスの分布 (イメージ)

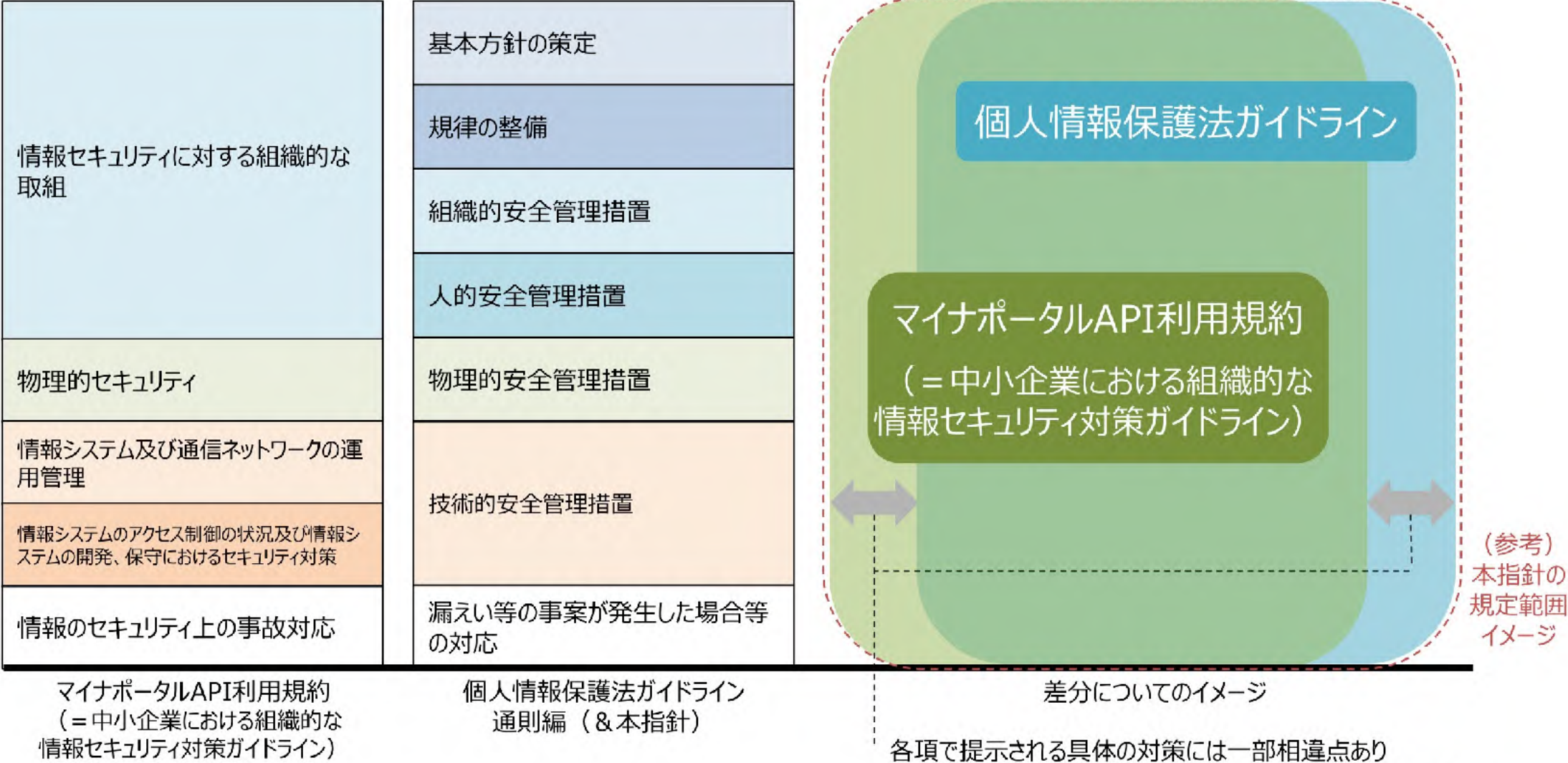


※ ■ は、個別情報を用いたサービスの総称、■ は、民間事業者等が提供する主な個別サービス名

※ 経済産業省において、ヒアリング等をもとに、PHRサービスのイメージとして主な事業者の主なサービスを区分掲載。掲載している区分以外に対象情報として取得している場合や、上記にあげられるサービス以外にも多数存在。

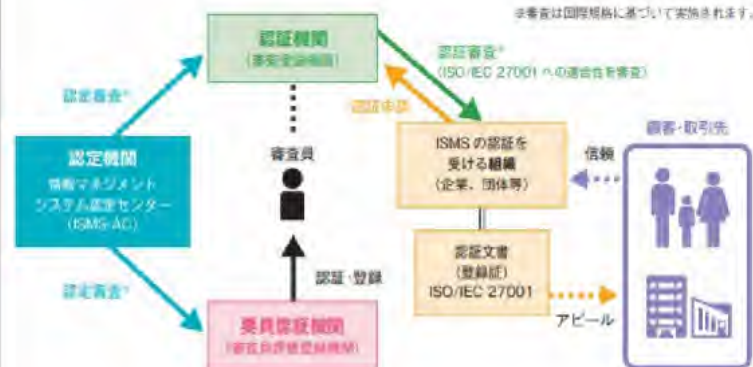
2 情報セキュリティ対策の具体的な対策項目イメージ

概念図



2 Information Security Management System (ISMS) 認証制度 (適合性評価制度)

- ISMSは情報セキュリティ管理を評価する国際的な認証制度であり、個人情報にとどまらない全情報資産の取扱いに関する技術的対策、従業員の教育・訓練、組織体制の整備等を審査し認証している

認証制度名	Information Security Management System (ISMS) 認証制度(適合性評価制度)			
制度設立の背景	■ 経済産業省「情報セキュリティ管理に関する国際的なスタンダードの導入及び情報処理サービス業情報 システム安全対策実施事業所 認定制度の改革について」(2000年7月公表)を受け、財団法人日本情報処理開発協会(現JIPDEC)が、国際規格に基づく物理的・人的対策などを組織全体の包括的な仕組みである ISMSをベースとした制度の創設に着手(2001年度にパイロット運用、2002年度～本格運用に移行) ➢ 認定機関としての独立性をより明確にし、公平な認定活動を推進するため、JIPDECから独立し、認定業務を行う「一般社団法人情報マネジメントシステム認定センター(ISMS-AC)」を法人化(2018年4月)			
認定主体	一般社団法人情報マネジメントシステム認定センター(略称:ISMS-AC)	対象事業者/業界	情報資産を保有する事業者(部門・事業単位も可)	
制度の仕組み(要件等含む)	■ 認定機関であるISMS-ACから認定を受けた認証機関(「ISMSクラウドセキュリティ認証機関」として2020年11月時点で全13機関)へ事業者が認証申請をし、当認証機関が適合性評価を行い認証を付与 ■ 情報のセキュリティの3要素であるCIA(「機密性(Confidentiality)」、「完全性(Integrity)」、「可用性(Availability)」を保護するための要件を規定)が担保されているかを審査 ■ 組織がISMSを確立し、実施し、維持し、継続的に改善するための要求事項を定めた「JIS Q 27001:2014 (情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項)」*2に基づき審査を実施 概念図 			

*1 Pマーク認証と異なり、個人情報だけでなく全情報資産が対象
*2 国際規格であるISO/IEC 27001に基づくJIS規格

2 プライバシーマーク認証（Pマーク認証）

- プライバシーマーク制度は、個人情報マネジメントシステムの要件に従い、個人情報保護マネジメントシステム（PMS）を運用する事業者に対しマークを付与することで、一定の情報管理水準を承認する制度である

認証制度名	プライバシーマーク制度			
制度設立の背景	■ 「行政機関が保有する電子計算機処理に係る個人情報の保護に関する法律」への準拠や、インターネット普及・情報技術発展に伴う個人情報保護の必要性の高まりなどを踏まえ、日本情報処理開発協会（現：日本情報経済社会推進協会）が通商産業省（現：経済産業省）の指導を受けて、プライバシーマーク制度を創設（平成10年～制度運用開始） ➢ 民間事業者を対象とする「個人情報の保護に関する法律」が制定・公布（平成15年5月）されたことに伴い、事業者による法律への適合性、自主的な高い保護レベルでの個人情報管理システムを確立・運用していることのアピール方法として普及が加速			
認定主体	一般社団法人日本情報経済社会推進協会（JIPDEC）	対象事業者/業界	一定条件を満たす国内に活動拠点を持つ事業者*1（但し、医療法人・学校法人等については一部例外）	
制度の仕組み（要件等含む）	■ JIPDECが付与機関となり、事業者からのプライバシーマーク付与の申請に対する審査などを実施 ■ 付与機関から審査機関として指定を受けた団体が、事業者からのプライバシーマーク付与適格性審査申請の受付、申請内容の審査・調査等業務を実施 ■ 申請を希望する事業者は、「JIS Q 15001:2017 個人情報保護マネジメントシステム－要求事項」の要件に従い、個人情報保護マネジメントシステム（PMS）を構築・運用 ➢ 内部規定を作成し、必要な組織体制・セキュリティ対策を構築し、PMSを運用 ■ 事業者は、PMSの実施記録などを取り纏め、審査機関に提出し、審査機関による文書審査・現地審査をクリアすると、プライバシーマーク付与認定として確定し、マークの付与を受けることが可能 概念図 <pre>graph TD; A[個人情報取扱事業者] -- 申請 --> B[付与機関 JIPDEC]; B -- 審査・認定 --> C[プライバシーマーク付与認定指定機関]; C -- 申請 --> A; A -- 審査・認定 --> C;</pre>			

*1 JIS Q 15001「個人情報保護マネジメントシステム－要求事項」に基づいた個人情報保護マネジメントシステム（PMS）を定め運用していること、規定の欠格事項に該当しないことなど、必要な条件を満たしていることが前提となる

2 保健・医療・福祉分野におけるプライバシーマーク認証（MEDIS-DC Pマーク認証）

- Pマーク認証の中でも保健・医療・福祉分野においては「保健医療福祉分野のプライバシーマーク認定」があり、MEDIS-DCが唯一の指定（認証審査）機関として機能し、別途認定指針が制定されている

認証制度名	保健医療福祉分野のプライバシーマーク制度	
対象事業者・業界	■ 保健・医療に関連する事業等が対象 ➢ 原則として、業種の如何を問わず医療機関で取り扱う診療録、検査依頼伝票、検査結果報告書、レセプト等が、取り扱う個人情報の5割以上を占める事業者が対象 例) 病院(大学病院を含む)、診療所(一般・歯科診療所)、健診機関、医学・薬学系教育機関及び研究所等、調剤薬局、検査センター等、健康保険組合、審査支払機関(国保連合会、支払基金)、介護施設・居宅介護サービス事業者、その他保健・医療・福祉分野に関連する事業者	
認定主体	一般社団法人医療情報システム開発センター (Medical Information System Development Center: MEDIS-DC)	
制度の仕組み (要件等含む)	■ 関連規格及びガイドラインに基づく体制を構築し、適格性審査申請チェック表や申請書、マネジメントレビュー、実施計画書などの必要書類をMEDIS-DCの窓口へ申請 ➢ JIS Q 15001「個人情報保護マネジメントシステム要求事項」及び「保健医療福祉分野のプライバシーマーク認定指針 第4版」に準拠したマネジメントシステム(以下、「MS」という。)を構築し、MSに基づき個人情報の適切な取扱いを実施または実施可能な体制が整備されていることが条件 ■ 書類審査及び現地審査を経て、合格と判定されると、合格証の付与、Pマーク使用契約を締結	Medis 概念図 保健医療福祉分野の事業者に対する審査は、業界団体の加入の有無や地域に関係なくMEDIS-DCのみが実施

2 個人情報保護法で事業者の義務とされている事項

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)

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)

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。

■ 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。

2 プライバシーポリシー等の分かりやすい公表

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をホームページ上に掲載。

Fitbit プライバシーポリシー

有効日: 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力だと考えます。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広告サービス](#)
- ・ [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、場合によっては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 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）

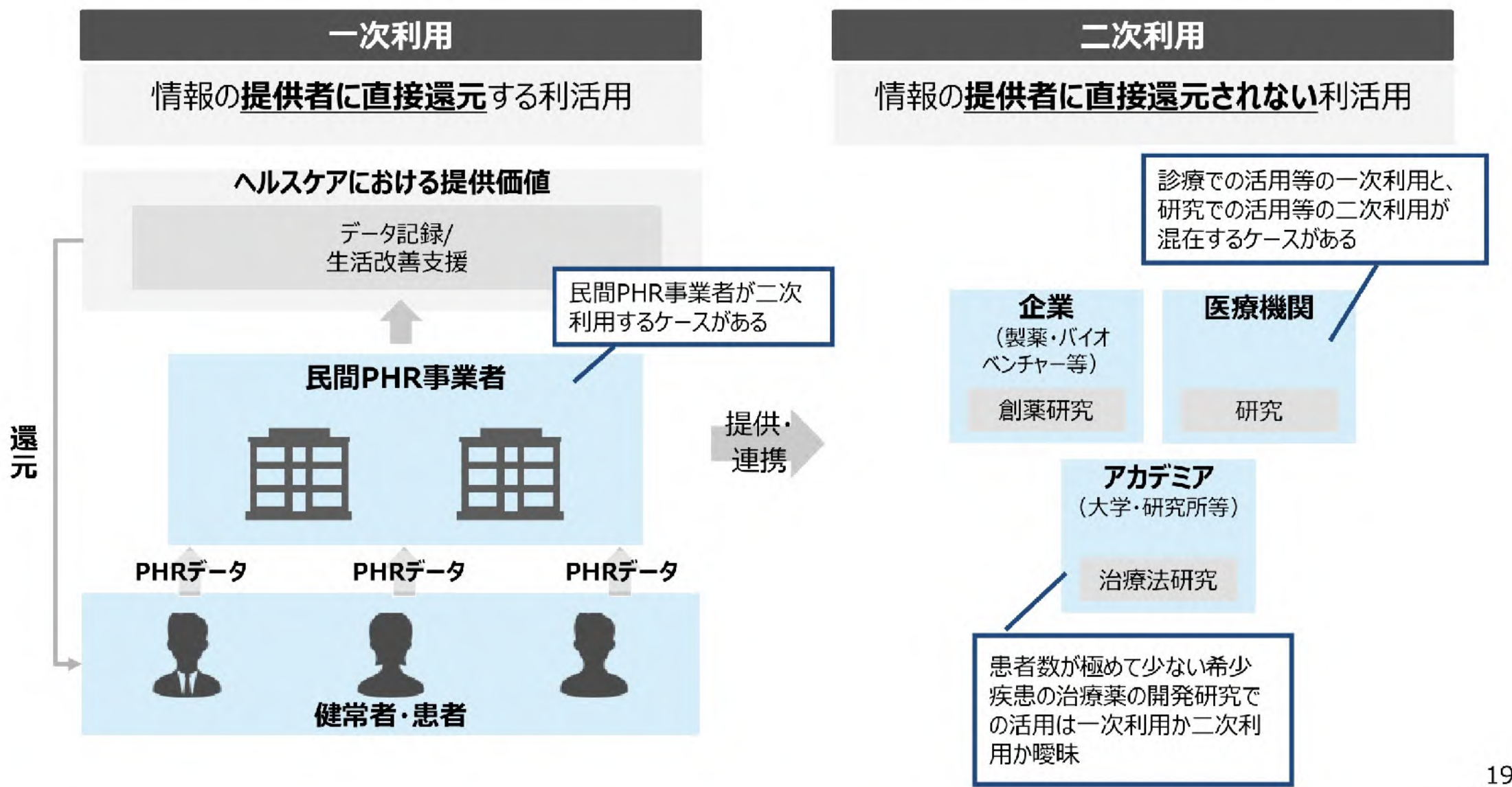


2018 CDPランク（気候変動）

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

3 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。



一次利用として医療機関に自身の情報を掲載する場合に、同意を取得している事例

SoftBank 10:31 100%

医師に見せる

ルナルナデータ番号発行

個人情報の取り扱いについて

施設情報 | 診療内容 | アクセス

広尾レディース

婦人科

診療時間

月	10:00~13:00, 14:30~19:00
火	10:00~13:00, 14:30~19:00
水	10:00~13:00, 14:30~19:00
木	10:00~13:00, 14:30~19:00
金	10:00~13:00, 14:30~19:00
土	10:00~14:00
日	—
祝	—

SoftBank 10:32 100%

医師に見せる

医師に見せるデータの確認

医師に見せるデータの確認

ルナルナアプリでビルモードをご利用中の方は「ビル(OC/LEP)服用中」にチェックをいれてください。

☒ ビル(OC/LEP)服用中

「基礎体温」、「生理日」は必須項目となります。
医師が適切な診察を行うために、なるべくすべての項目にチェックを入れておくことをおすすめします。

☒ 生理日	☒ 基礎体温
☒ 腹痛	☒ 不正出血
☒ SEX日	☒ おりもの

本人確認情報の入力(必須)

問診データの本人確認のため、生年月日を入力してください。

1978 12 06

ルナルナデータ番号を発行

SoftBank 10:32 100%

医師に見せる

ルナルナデータ番号

ルナルナデータ番号

ルナルナデータ番号の発行が完了しました。

受診時に、先生へルナルナ メディコの利用と、下記番号をお伝えください。

● ● ● ● ● ●

※開示するデータの変更や管理は「データ番号一覧」から行ってください。

※データ番号は、データを開示する婦人科ごとに発行が必要です。

※複数の婦人科を受診する際は、データ番号の伝達間違いにご注意ください。

ルナルナ メディコホーム

(出典：エムティーアイ)

研究参加の同意



まずはアプリストアから「ルナルナ」をダウンロード

※ 研究参加にはルナルナIDのログインが必要です

※ 「ルナルナ 体温ノート」「ルナルナ ベビー」からもご参加いただけます

1 「お知らせ」をタップ

2 「お知らせ記事」をタップ

3 こちらのボタンから参加！



同意の撤回の方法



同意を撤回し
研究へデータを提供しない

(出典：エムティーアイ)

3 健診等情報を第三者提供する場合（例1：提供先毎に同意取得する例）

ステップ1

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、分かりにくいと感ずる可能性がある。

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製薬会社の創業に関する研究 ⓘ

...

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)

健診等情報を第三者提供する場合（例2：利用目的毎に同意取得する例）

ステップ1

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。「」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。

第三者提供先（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	

※同意ボタンや を押すと表示される第三者提供先は、現時点の内容を表示しており、今後変更となる可能性があります。

拒否 許可

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 匿名加工情報の取扱いの要求事項

匿名加工情報を取り扱う事業者は、当該情報の適切な加工の他、当該情報の作成時及び第三者への提供時に公表を行う必要がある。

求められる要件

匿名加工情報 を <u>作成</u> する場合	■ 適正な加工 ■ 削除した情報や加工方法に関する情報の漏洩を防止するための安全管理措置の整備 ■ 匿名加工情報に含まれる情報の項目の公表 ■ 他の情報との照合による本人の特定禁止 ■ 苦情の処理等の対応（努力義務） （個人情報保護法第36条）
匿名加工情報 を <u>第三者提供</u> する場合	■ 匿名加工情報に含まれる情報の項目と提供方法の公表 ■ 提供先に対する匿名加工情報であることの明示 （第36条）
匿名加工情報 を <u>受領</u> する場合	■ 他の情報との照合による本人の特定禁止 ■ 加工方法の取得禁止 ■ 苦情の処理等の対応（努力義務） （第38条・39条）

匿名加工情報は、一定のルール(※)の下で、本人同意を得ることなく、事業者間におけるデータ取引やデータ連携等の利活用を促進することを目的に規定。そのため、匿名加工情報としての規律(適正加工、識別行為禁止等)が適用されるものの、第三者提供に本人の同意は不要(※)で、その代わりに、公表・明示義務を適用

※但し、匿名化情報の作成元において、特定の個人を容易に照合できる場合は個人情報扱いとなるため、個人情報としての安全管理措置や第三者提供についての本人の同意やオプトアウト手続が必要

3 医師・薬剤師名の取扱い事例

医師・薬剤師等の個人情報について、PHR事業者において何等か利用する目的があれば、当該目的を公表しておけば本人の同意なく取扱い可



画像出所：日薬が提供する電子お薬手帳（アプリ）

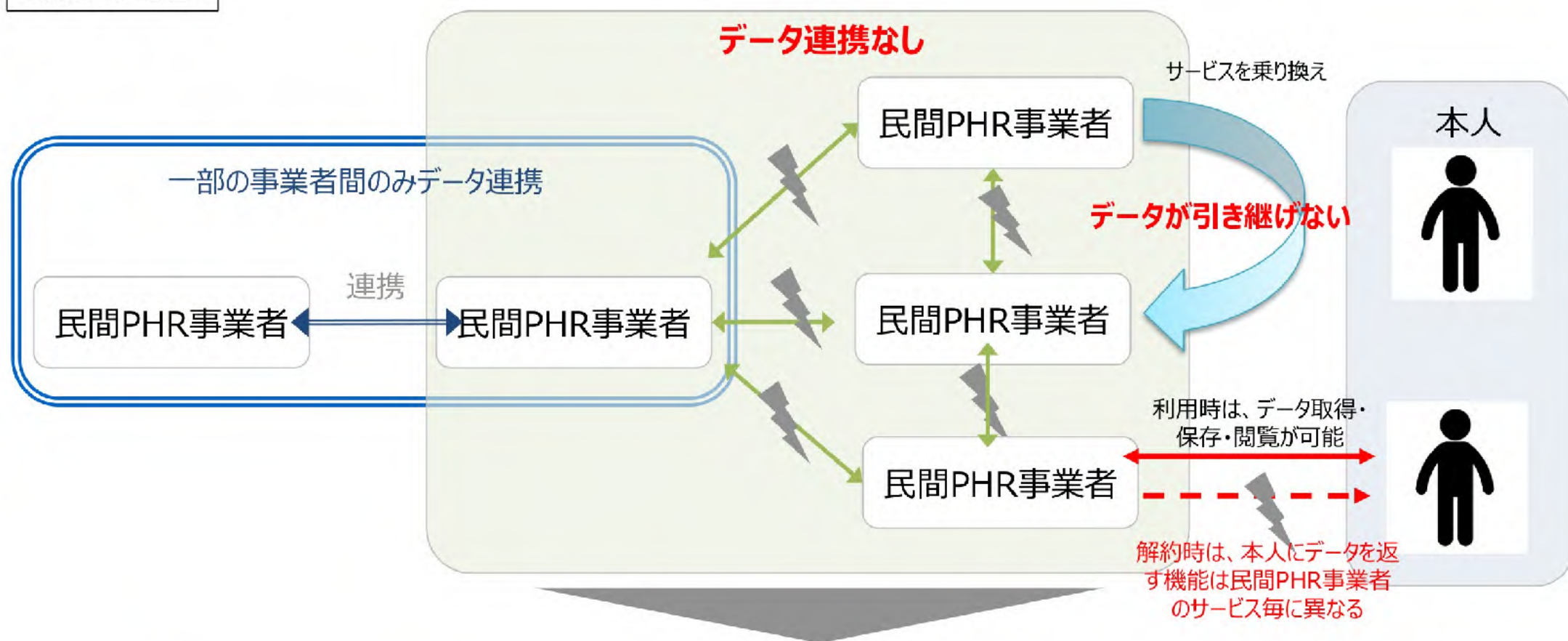
PHRサービス利用者本人以外の個人情報

- PHR事業者が、そのサービス利用者等から、健診等情報を含む各種情報を入力した場合、当該情報の中に、検査や診察を担当した医師の氏名等、本人以外の個人情報に含まれる可能性がある
- 仮にPHR事業者において、あらかじめ、**医師等の個人情報の利用目的を公表していれば、その利用目的の範囲内で、当該医師等に係る個人情報を取得することが可能**（第十八条第一項）
- 一方で、医師等の個人情報の利用目的をあらかじめ公表していないときは、医師本人への通知又は公表が必要（同条同項）
- また、PHR事業者において、医師等の個人情報を利用する必要がなくなったとき（利用目的が達成され当該目的との関係では当該個人データを保有する合理的な理由が存在しなくなった場合や、利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等）は、**遅滞なく消去するよう努めなければならない**。（第十九条）

（参考）PHRサービス利用者
本人の要配慮個人情報

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

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

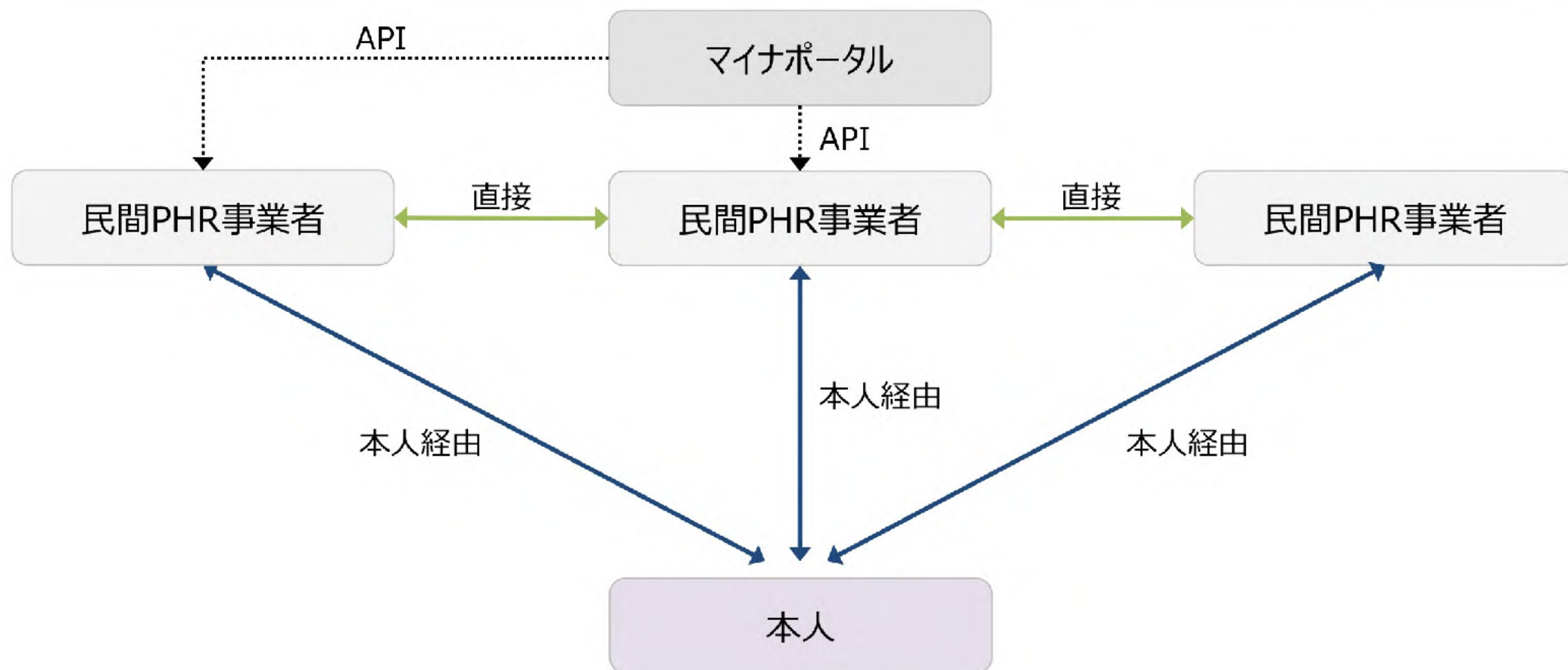
- 本人へのデータのエクスポート
 - 本人からのデータインポート
- ※マイナポータルから出力されるフォーマット等と同様



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



本指針に係るチェックシート項目例

別紙

本指針に係るチェックシート

点検日 【 】 前回点検日【 】
 点検担当者 【 】 前回点検担当者【 】 ※公表時は役職名でも可

※ 業務委託先の遵守状況も含めた点検を行うこと

※ 求められる事項を満たしているか、同等以上の対応を行っている場合にチェックを付けること

1. 基本的事項

項目番号	内容	チェック
1	本指針の対象とする情報の定義	
1-1	個人が自らの健康管理に利用可能な「個人情報の保護に関する法律」(平成15年法律第57号。以下「個人情報保護法」という。)上の要配慮個人情報で、次に掲げるもの(以下「健診等情報」という。)ですか ・個人がマイナポータルAPI等を活用して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	
2	本指針の対象事業者	
2-1	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(以下「PHR事業者」という。)ですか	

2. 情報セキュリティ対策

2. 1. 安全管理措置

(1) 法規制に基づく遵守すべき事項

項目番号	内容	チェック
1	個人情報保護法に基づく適切な取扱い	
1-1	健診等情報を取り扱うに当たって、その漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置を講じていますか ※ 具体的には(2)の対策の実施有無を確認	

(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

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が従業員に明確に示されている	
1-1	経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持っていますか	
1-2	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	

今後の検討課題

<基本的指針の基本的事項に係る留意事項>

- ・いわゆるライフログ等の利活用に際して留意すべき事項

<個人情報の適切な取扱いに係る留意事項>

- ・医師又は薬剤師等の氏名等を第三者提供する場合の取扱い

<健診等情報の保存及び管理並びに相互運用性の確保に係る留意事項>

- ・同じデータの項目であっても、健診等において取得されたものと本人が入力したものとでは、計測方法及びデータ改変の可能性等の観点で違いが生じ得るため、区別した管理の在り方
- ・データの保存及び管理における、利用者による改ざん防止対策
- ・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対応コスト等の観点を考慮した事業者間での連携の拡大
- ・より効率的なデータ管理及びポータビリティの仕組みの構築を検討した上での、情報種別毎の名称及び単位等の統一並びに通信規格及び交換形式に係る標準化

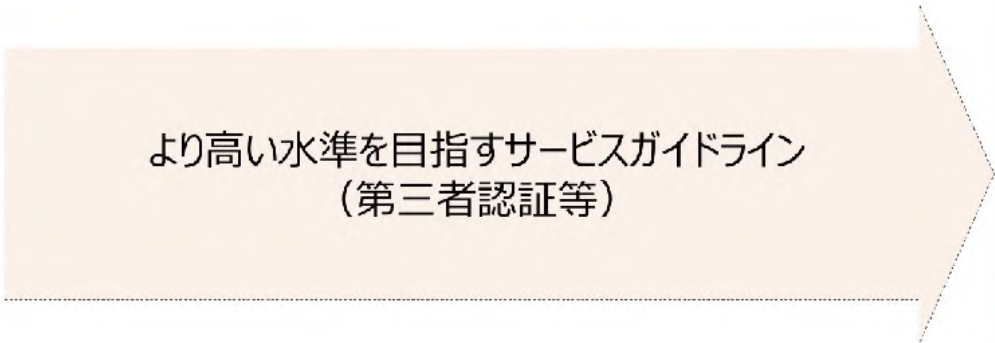
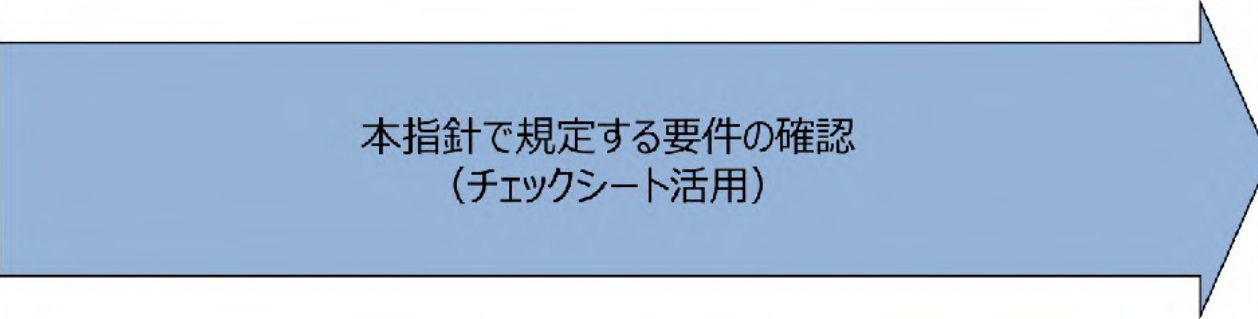
<要件遵守の担保方法に係る留意事項>

- ・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

<その他>

- ・生活習慣病改善等に向けたPHRサービスを提供する場合の医療従事者等と連携したサービスの提供
- ・上記観点も踏まえて、最新の利用可能な技術及び知見等に基づき、より高い水準を目指すサービスガイドラインを策定して取り組むなど、先進的かつ高度な取組の推進

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P H R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）	▲ 20年度	▲ 基本的指針策定  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

民間 P H R サービス利用者へのアンケート調査結果等

I 民間P H Rサービス利用者へのアンケート調査結果

1. 民間P H Rサービスの調査概要と解析結果サマリ
 - (1) 民間P H Rサービスのアンケート実施概要
 - (2) 回答者属性
2. P H R利用状況
 - (1) P H R利用割合
 - (2) P H Rの認知度
 - (3) 利用実態
 - (4) 利用継続要因・離脱要因
 - (5) 連携へのニーズ
 - (6) 調査結果サマリ
3. 「民間P H R事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連
 - (1) 情報セキュリティ対策
 - (2) 個人情報の取扱い
 - (3) 保存・管理、相互運用性の確保
 - (4) その他(判定スコアやプロファイリング結果の信頼性・妥当性)
 - (5) 調査結果サマリ

参考：健診等情報を取扱うP H Rサービス利用者の特徴

II 健診等情報に関するP H Rサービスを提供している 健康保険組合等に対するヒアリング調査結果

I 民間P H Rサービス利用者へのアンケート調査結果

1.民間P H Rサービスの調査概要と解析結果サマリ

1. 民間P H Rサービスの調査概要と解析結果サマリ

(1) 民間P H Rサービスのアンケート実施概要

- 民間P H Rサービスの適切な形での普及展開に向けて、**サービス利用実態及び安全性等についてサービスを選ぶ際のポイントや留意点を明らかにすること**を目的に、個人を対象としたアンケートを実施しました。

【実施概要】

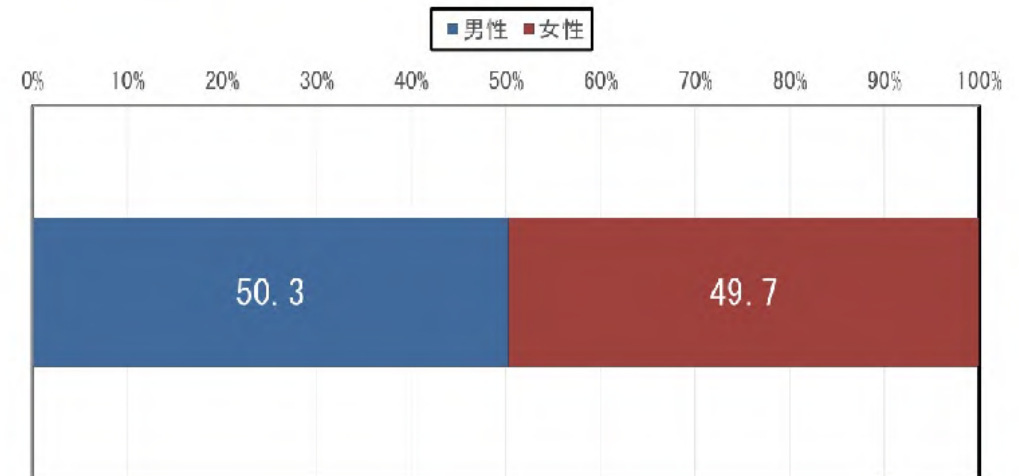
項目	内容
アンケート回答者数	・1,623名
アンケート対象者	・「民間P H Rサービス」の現利用者（867名）、過去利用者（離脱）者（203名）、未利用者（553名） ※スクリーニングによりサンプルバランスを取る（性別・年代・利用有無）
実施方法	・W E Bアンケート調査（W E Bモニターを対象に、電子メールで調査依頼、W E B上で回答）
実施期間	・令和2年12月上旬
調査項目	①属性と利用状況（全員） ・ 年代・性別 ・ P H Rの認知度 ・ 健康意識・健康行動 ・ P H Rによるメリット ・ P H Rの利用経験 ⇒ 現利用者/過去利用者/未利用者を仕分け ②P H R利用者・利用経験者の利用実態・利用促進要因（現利用者・過去利用者のみ） ・ 利用実態(利用種類、目的、利用機能、情報、共有、デバイス、頻度、金額、経緯、継続理由) ・ 利用促進要因（利用による効果） ③P H R過去利用者・未利用者の利用にあたっての懸念点（過去利用者・未利用者のみ） ・ 利用にあたっての懸念点（有効性・安全性、データ連携、個人情報、セキュリティ、同意、サービス終了時への扱い、サービス乗り換え、使い勝手、サービスへの説明に関する意識） ・ 利用していない理由（過去利用者・未利用者のみ） ④今後のP H Rへのニーズ（全員） ・ 欲しい機能、セキュリティと利便性のバランス、連携ID、サービス乗り換え ・ 目的×データ範囲×連携したい相手、同意なく利用されたくない相手 ・ 望ましい同意の在り方 ・ サービスへの希望・不安

1. 民間PHRサービスの調査概要と解析結果サマリ

(2) 回答者属性 (性別・平均年齢・年代別人数)

【回答者性別】

	実数	%
全体	1,623	100.0
男性	816	50.3
女性	807	49.7



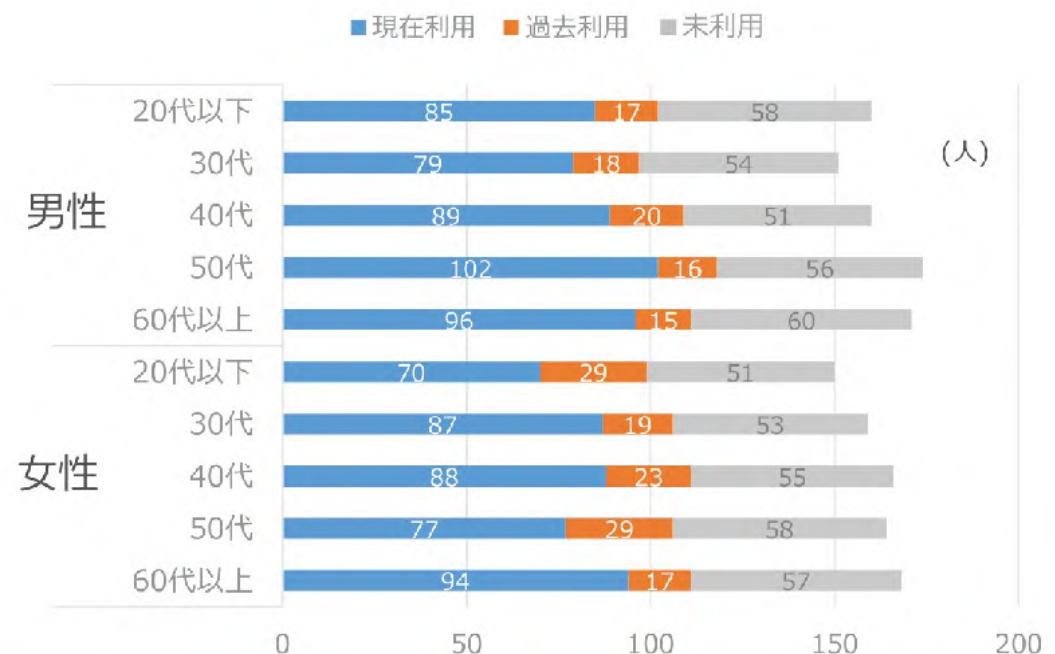
【回答者平均年齢】

全体 (人数)	平均 (歳)	最年長 (歳)	最年少 (歳)
1,623	45.5	70.0	15.0

【回答者年代別】

■ 有効回答数

		現利用者	過去利用者	未利用者	合計
男性	20代以下	85	17	58	160
	30代	79	18	54	151
	40代	89	20	51	160
	50代	102	16	56	174
	60代以上	96	15	60	171
女性	20代以下	70	29	51	150
	30代	87	19	53	159
	40代	88	23	55	166
	50代	77	29	58	164
	60代以上	94	17	57	168
		867	203	553	1,623



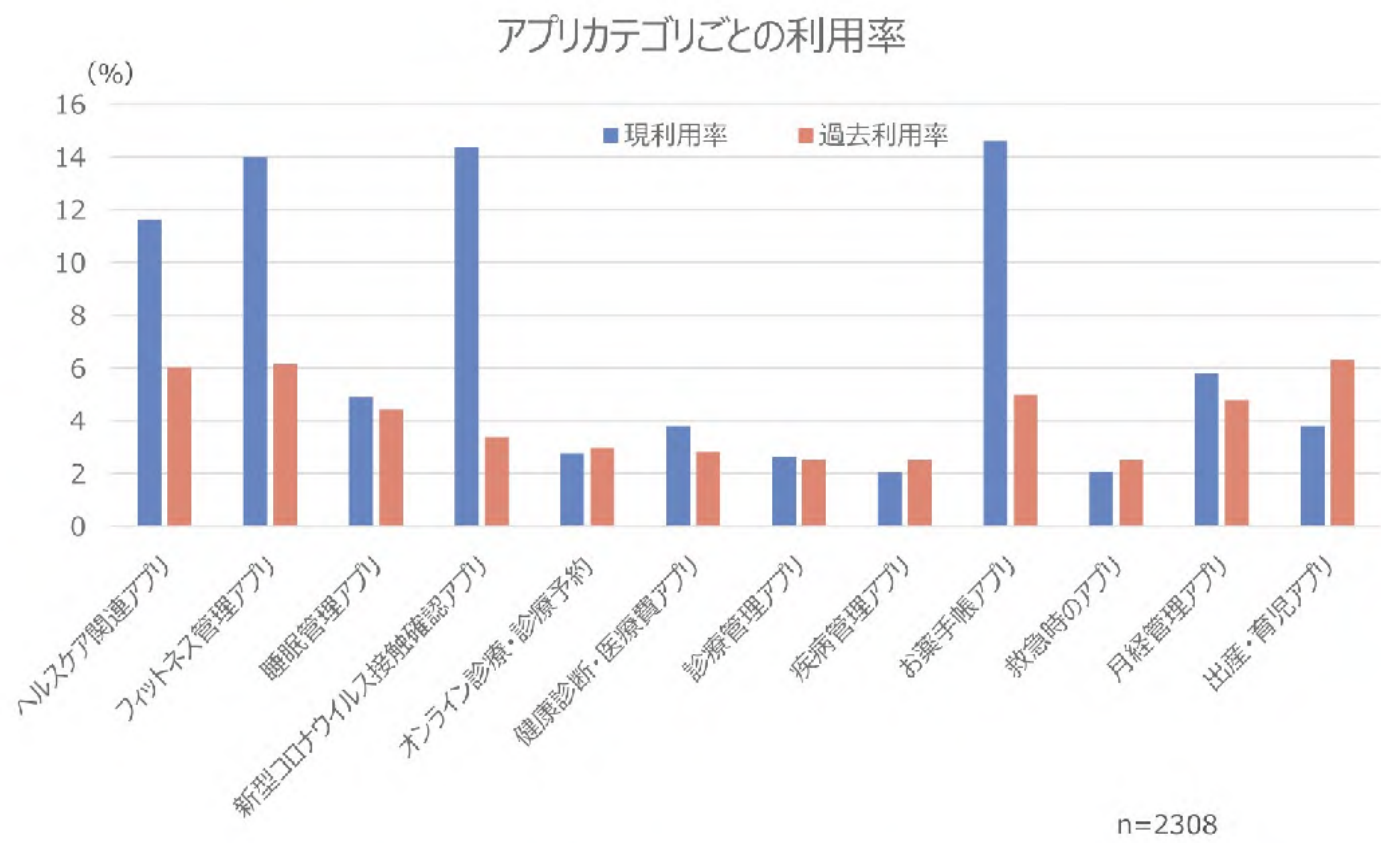
I 民間P H Rサービス利用者へのアンケート調査結果

2. P H R 利用状況

2. P H R 利用状況

(1) P H R 利用割合

- スクリーニング前の母集団を対象とした P H R **現利用率は、高いもので 1 4 % 程度**
- 現利用者の利用しているアプリは、「お薬手帳」・「コロナ接触確認」・「フィットネス」が多い



スクリーニング前の母集団時の属性

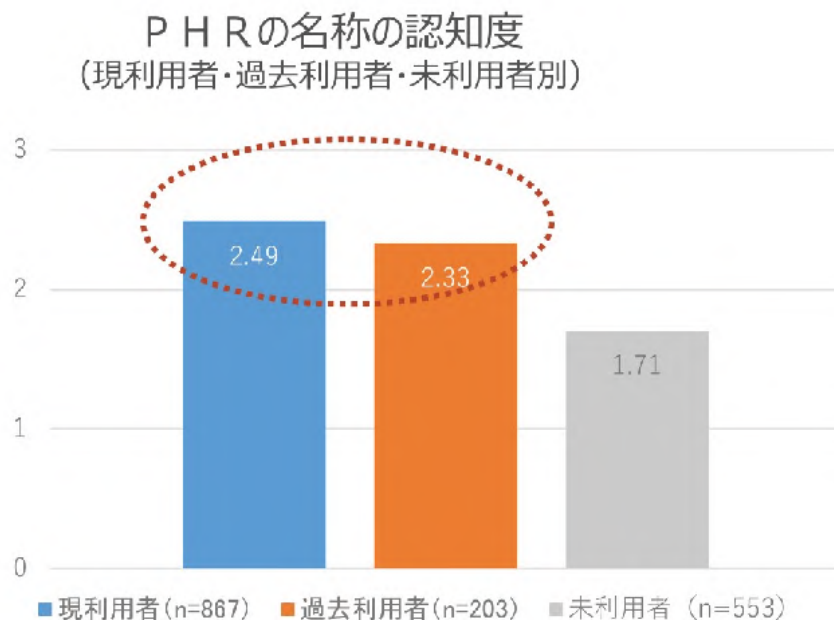
		全体
全体	実数	2,308
男性	実数	1,198
20代以下	実数	240
30代	実数	208
40代	実数	243
50代	実数	259
60代以上	実数	248
女性	実数	1,110
20代以下	実数	159
30代	実数	184
40代	実数	243
50代	実数	248
60代以上	実数	276

※本アンケートにおけるアプリカテゴリは、現存するサービスをベースに便宜的に分類したものであり、P H R サービスを網羅的に分類したものではない。

2. P H R利用状況

(2) P H Rの認知度

- 66.7%がP H Rの名称について「全く知らない」と回答
- P H Rの名称の認知度は、現利用者・過去利用者の方が高い

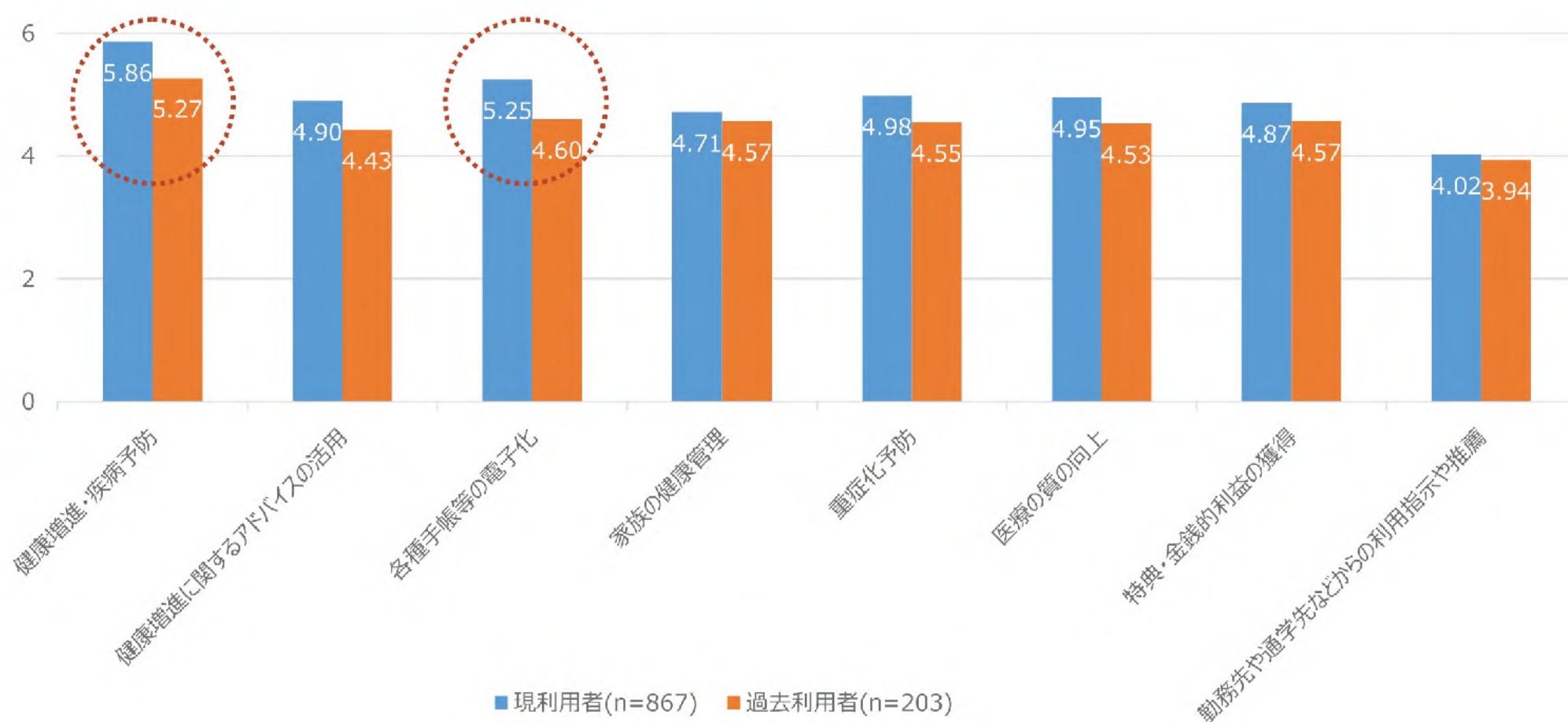


※選択肢「1. 全く知らない」～「9. よく知っている」の平均値を比較

2. P H R 利用状況

(3) 利用実態 ①目的

- 利用目的として、健康増進・疾病予防、各種手帳等の電子化が多い
- 勤務先や通学先などから利用するように指示や推薦からという回答はそれほど多くない

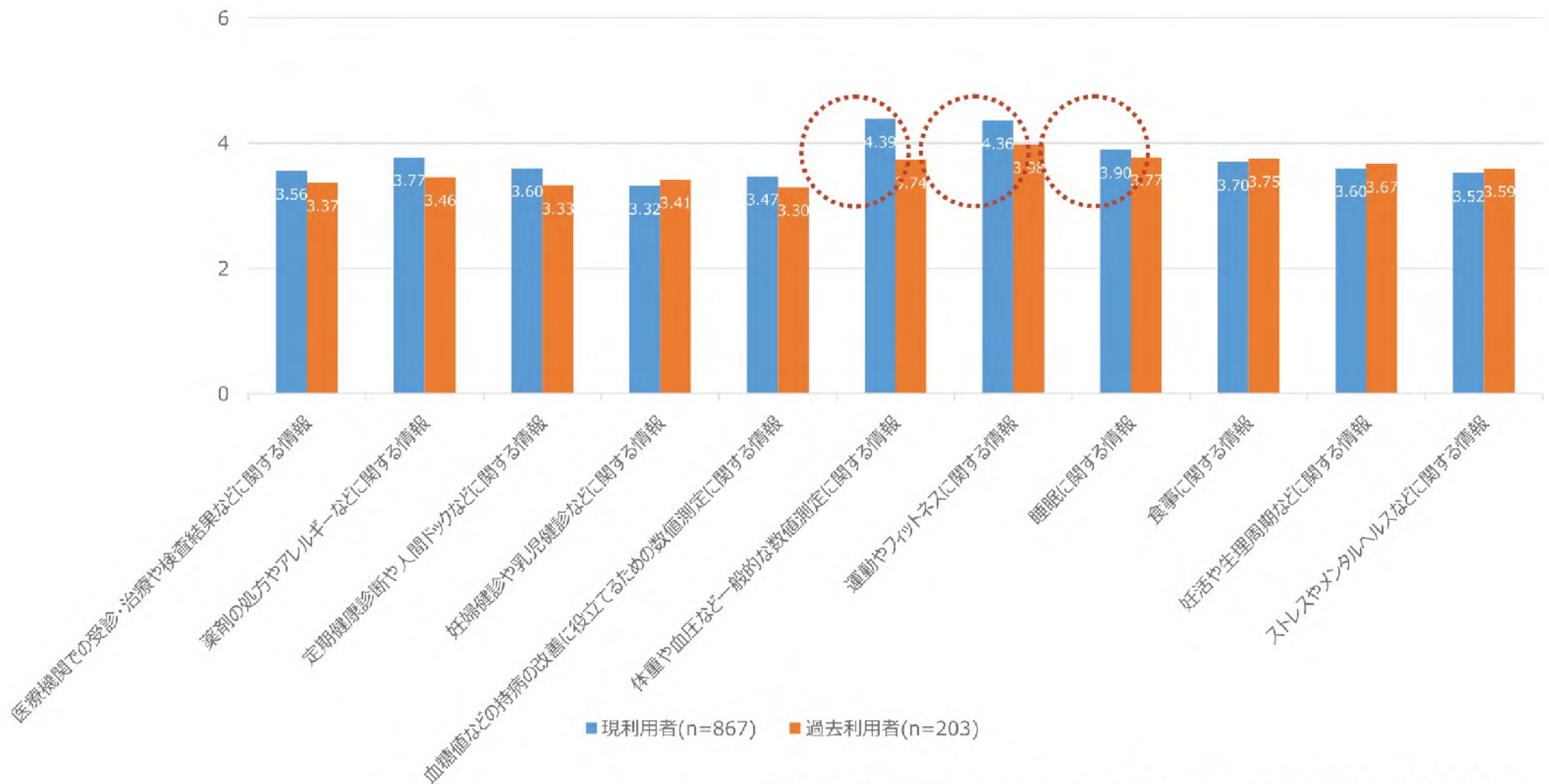


※選択肢「1. 全くあてはまらない」～「9. とてもあてはまる」の平均値を比較

2. PHR利用状況

(3) 利用実態 ②情報

- 体重や血圧、運動、睡眠等の日々のライフログ情報を比較的多く利用している



※選択肢「1. 全くあてはまらない」～「9. とてもあてはまる」の平均値を比較

2. P H R利用状況

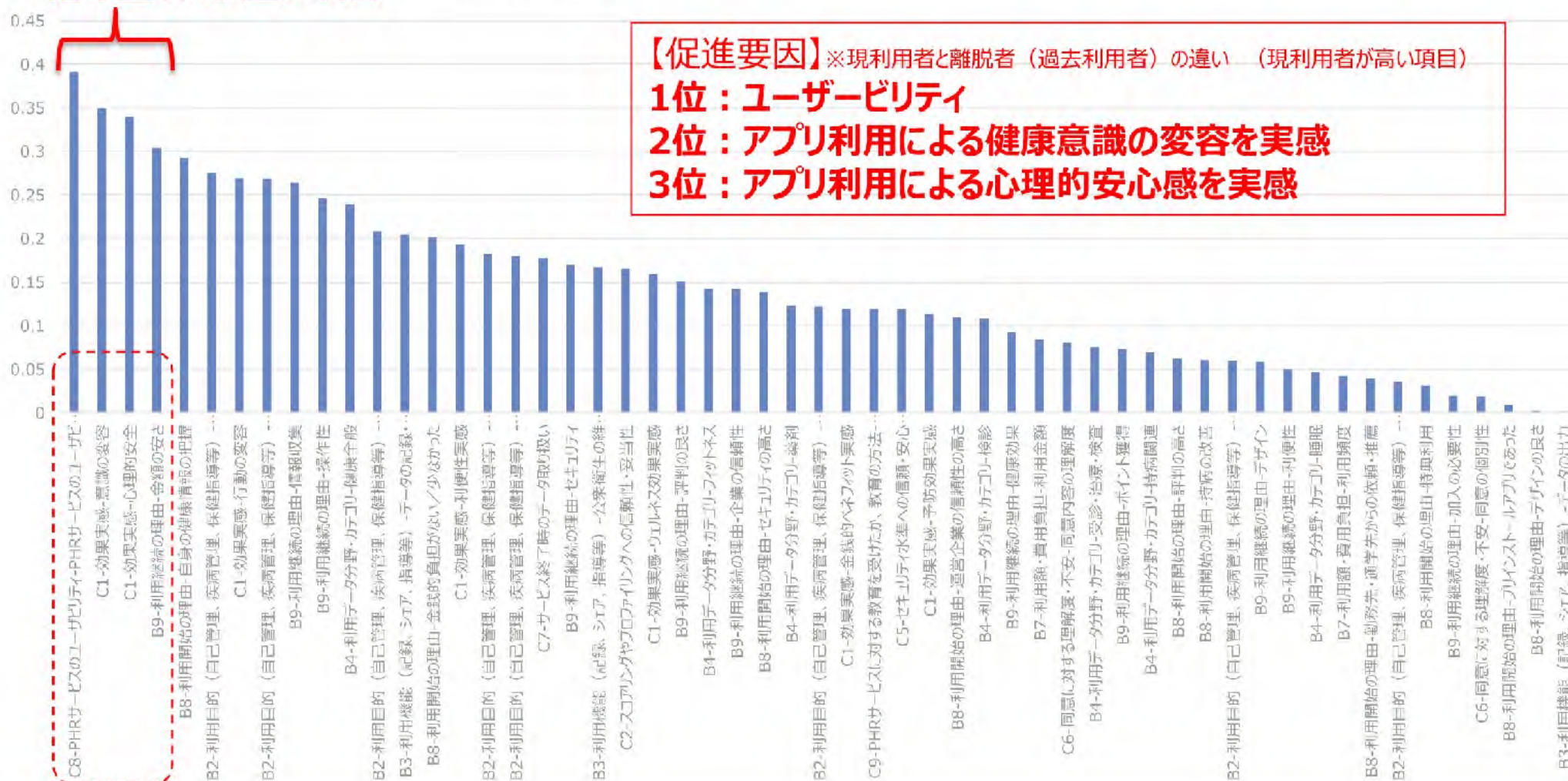
(4) 利用継続要因 (現利用者-過去利用者の差分 (効果量 d) 降順)

- 現利用者と離脱者 (過去利用者) を比較した結果、**P H Rサービスの利用者は、アプリケーション自体のユーザビリティを高く評価し、また利用による健康意識・安心感を実感している**

現利用者-過去利用者の差分 (効果量 d) 降順 ※ > 0 の項目

効果量：2群間の平均値の差を標準偏差で割って標準化したもので、平均値がどれだけ離れているかを評価する指標。0.2以上あれば小さいが効果がある、0.5以上で中程度の効果 と解釈* Cohen(1969)

効果量0.3以上の項目

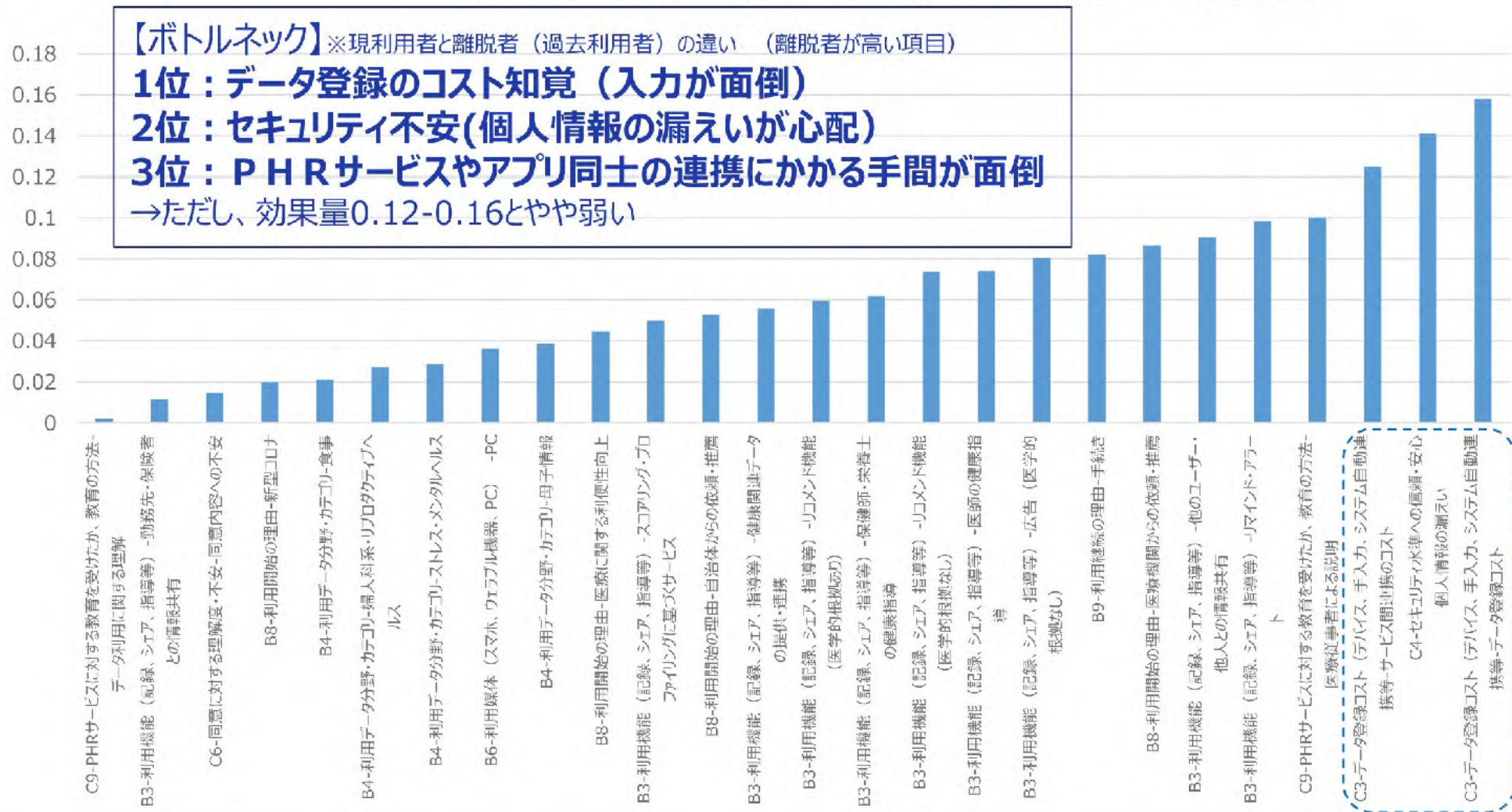


2. P H R 利用状況

(4) 利用離脱要因 (現利用者-過去利用者の差分 (効果量 d) 降順)

- 一方で、離脱者はデータ登録やアプリ同士の連携をコストと考えており、また個人情報の漏えいやセキュリティに対する不安も高い

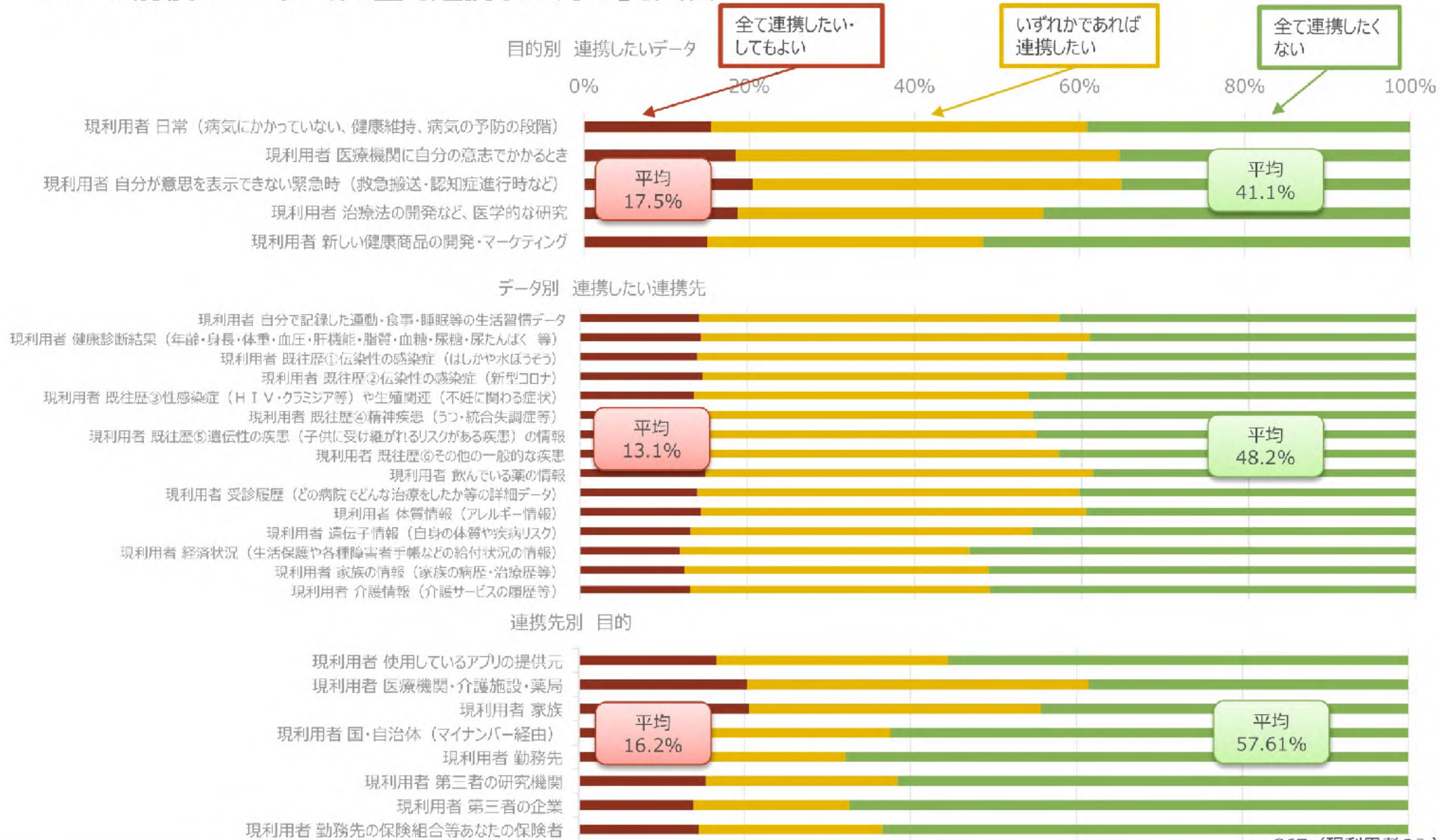
現利用者-過去利用者の差分 (効果量 d) 降順 ※ < 0 の項目



2. P H R 利用状況

(5) 連携へのニーズ 連携したいデータ・相手・目的

- データ別、連携先別、目的別の連携意向をみると、15%前後のユーザーが「全て連携してもいい」、50%前後のユーザーが「全て連携したくない」と回答



n=867（現利用者のみ）

（５）連携へのニーズ 連携したいデータ・相手・目的

- 連携意向が高かったのは「医療機関」相手、「健診結果・薬情報・受診・アレルギー」データ
 - 連携意向が低かったのは「勤務先・第三者企業・保険者」相手、「経済状況・家族情報・介護」データ、「商品開発・マーケティング」目的
- ※「いずれか連携したい」と回答したユーザーの分析結果

高

「データの内容」×「連携相手」×「目的」別に連携したいと答えた割合

低

高

低

目的	データ	連携相手	目的	データ	連携相手
現利用者 日常（病気がかかっていない、健康維持、病気の予防の段階）	26.07%	20.65%	8.54%	8.30%	6.57%
現利用者 医療機関に自分の意志でかかるとき	17.53%	22.41%	11.65%	11.42%	9.57%
現利用者 自分が意思を表示できない緊急時（救急搬送・認知症進行時など）	15.46%	20.65%	11.42%	11.30%	9.00%
現利用者 治療法の開発など、医学的な研究	13.15%	14.88%	6.00%	6.92%	4.73%
現利用者 新しい健康商品の開発・マーケティング	13.26%	11.53%	4.61%	4.96%	4.04%

目的	データ	連携相手	目的	データ	連携相手
現利用者 日常（病気がかかっていない、健康維持、病気の予防の段階）	15.57%	24.45%	16.15%	4.73%	3.34%
現利用者 健康診断結果（年齢・身長・体重・血圧・肝機能・脂質・血糖・尿糖・尿たんぱく 等）	12.92%	31.49%	17.42%	6.34%	4.61%
現利用者 既往歴①伝染性の感染症（はしかや水ぼうそう）	10.38%	29.76%	16.49%	6.23%	3.00%
現利用者 既往歴②伝染性の感染症（新型コロナウイルス）	9.92%	28.84%	16.03%	6.34%	3.81%
現利用者 既往歴③性感染症（H I V・クラミジア等）や生殖関連（不妊に関わる症状）	9.34%	25.84%	14.07%	5.42%	2.19%
現利用者 既往歴④精神疾患（うつ・統合失調症等）	9.23%	27.22%	14.53%	6.46%	5.19%
現利用者 既往歴⑤遺伝性の疾患（子供に受け継がれるリスクがある疾患）の情報	9.11%	26.07%	14.53%	5.54%	6.00%
現利用者 既往歴⑥その他の一般的な疾患	10.27%	28.72%	15.22%	5.31%	6.46%
現利用者 飲んでいる薬の情報	10.61%	32.41%	16.49%	5.65%	6.23%
現利用者 受診履歴（どの病院でどんな治療をしたか等の詳細データ）	10.61%	32.18%	16.26%	5.19%	6.23%
現利用者 体質情報（アレルギー情報）	10.50%	31.60%	17.19%	5.19%	6.34%
現利用者 遺伝子情報（自身の体質や疾病リスク）	9.80%	25.37%	14.76%	4.61%	5.77%
現利用者 経済状況（生活保護や各種障害者手帳などの給付状況の情報）	7.15%	18.11%	12.92%	5.19%	3.00%
現利用者 家族の情報（家族の病歴・治療歴等）	7.50%	18.69%	14.88%	4.27%	3.00%
現利用者 介護情報（介護サービスの履歴等）	7.73%	19.72%	14.07%	5.31%	4.73%

n=867 (現利用者のみ)

2. P H R 利用状況

(6) 調査結果サマリ

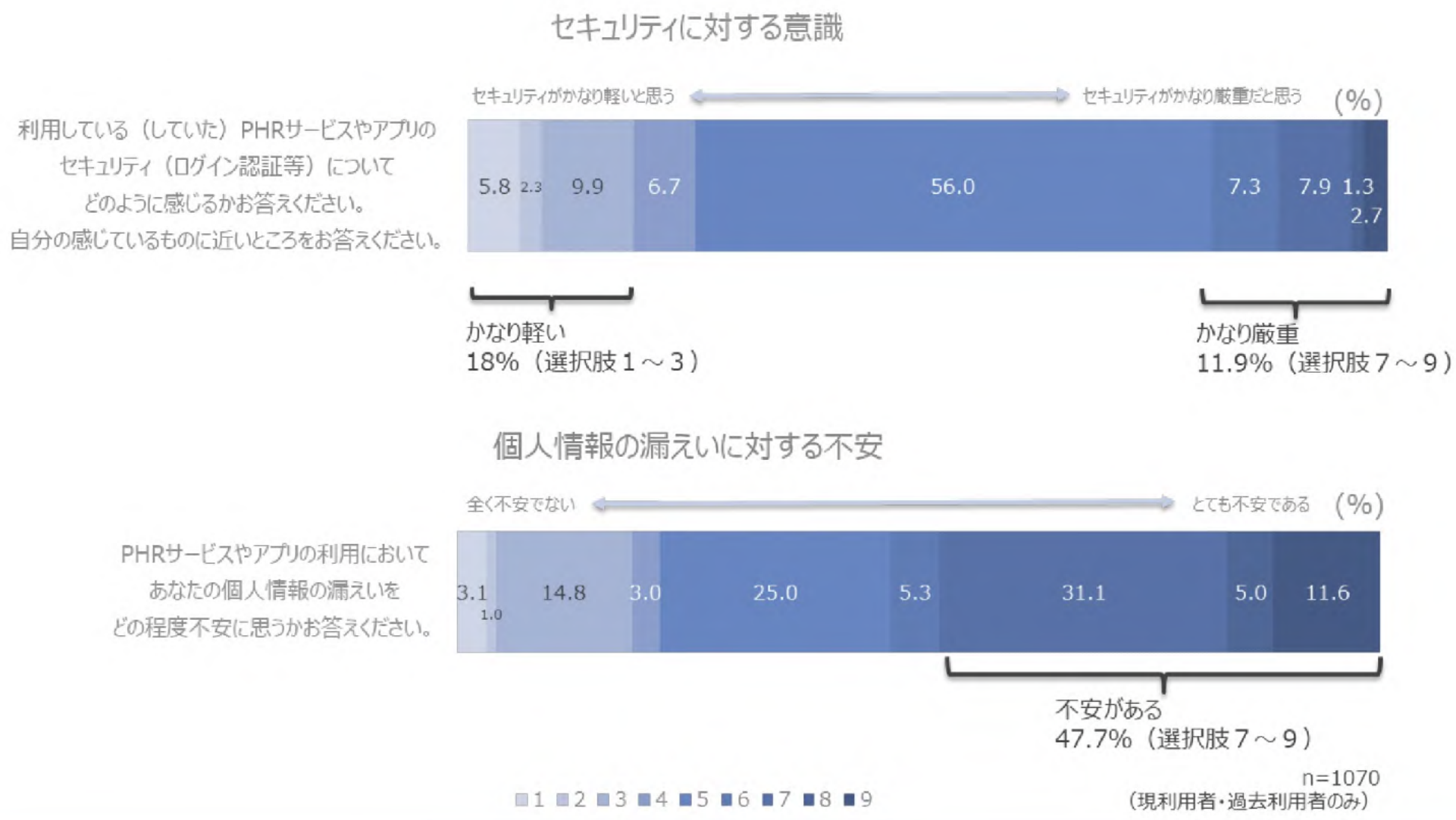
利用割合	・ P H R 現利用率は、高いもので 1 4 % 程度（スクリーニング前の母集団を対象とした概算） ・ 現利用者の利用しているアプリは、「お薬手帳」・「コロナ」・「フィットネス」が多い
P H R 認知度	・ 6 6 . 7 % が P H R の名称について「全く知らない」と回答 ・ P H R の名称の認知度は、現利用者・過去利用者の方が高い
利用実態	・ 利用目的として、健康増進・疾病予防、各種手帳等の電子化が多い ・ 勤務先や通学先などから利用するように指示や推薦からという回答はそれほど多くない ・ 体重や血圧、運動、睡眠等の日々のライフログ情報を比較的多く利用している
利用にかかる要因	・ 利用継続要因は、アプリケーション自体のユーザビリティ、利用による健康意識・安心感の実感 ・ 利用離脱要因は、データ登録やアプリ同士の連携コスト、個人情報の漏えいやセキュリティに対する不安
連携ニーズ	・ データ連携に関して 1 5 % 前後のユーザーが「全て連携してもいい」、5 0 % 前後のユーザーが「全て連携したくない」 ・ 連携意向が高い項目「医療機関」相手、「健診結果・薬情報・受診・アレルギー」データ ・ 連携意向が低い項目「勤務先・第三者企業・保険者」相手、「経済状況・家族情報・介護」データ、「商品開発・マーケティング」目的

I 民間P H Rサービス利用者へのアンケート調査結果

3. 「民間P H R事業者による健診等情報の取扱いに関する基本的指針」（案） 項目関連

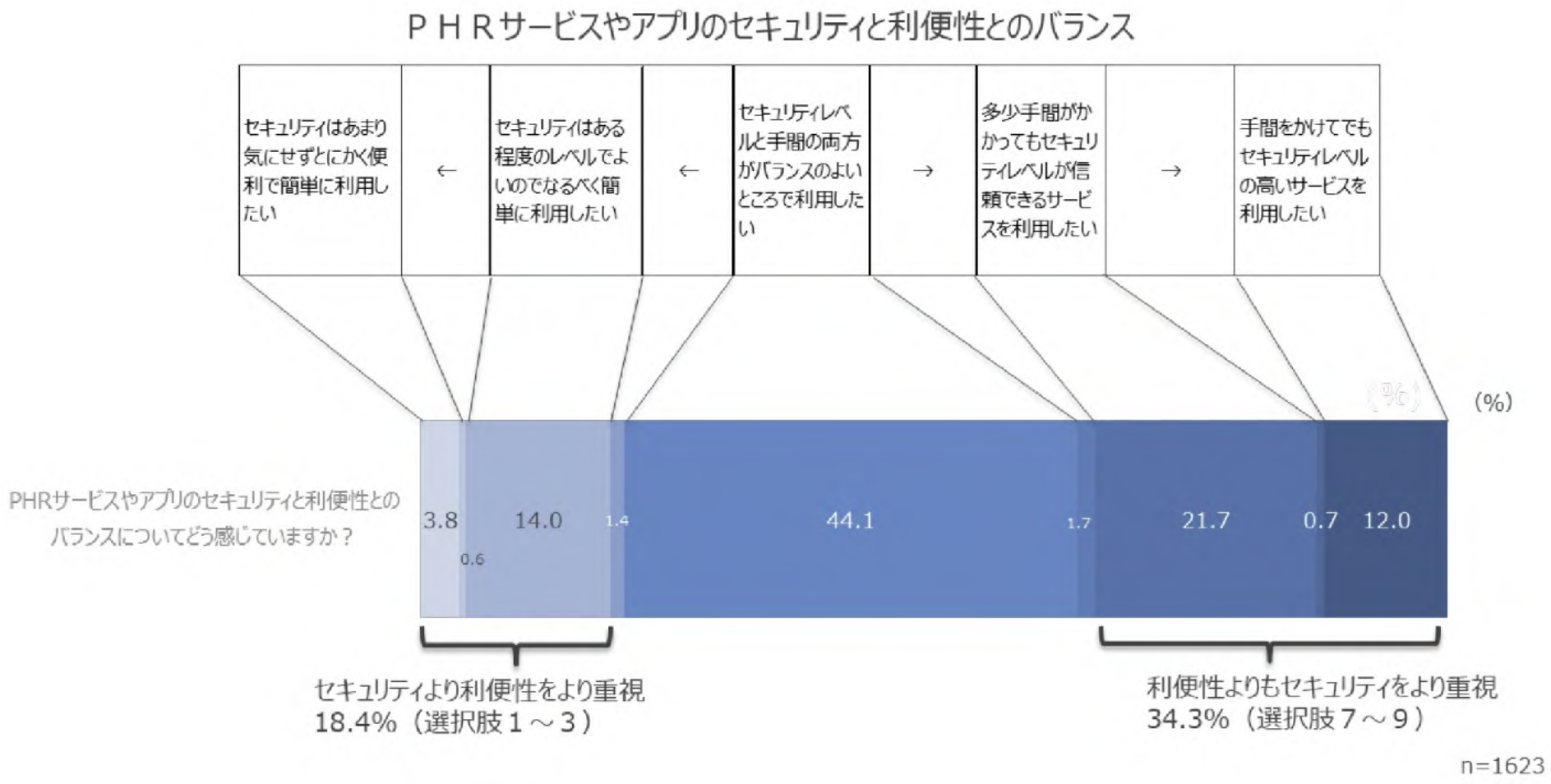
3. 「民間PHR事業者による健診等情報の取扱いに関する基本的指針」（案）項目関連 （1）情報セキュリティ対策 ①セキュリティや個人情報に関する意識

- 利用するサービスのセキュリティに対する意識にはばらつきがある
- 個人情報の漏えいに対する不安がある人は、利用したことのある人の約半数



3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」（案） 項目関連
（1） 情報セキュリティ対策 ②利便性とセキュリティのバランス

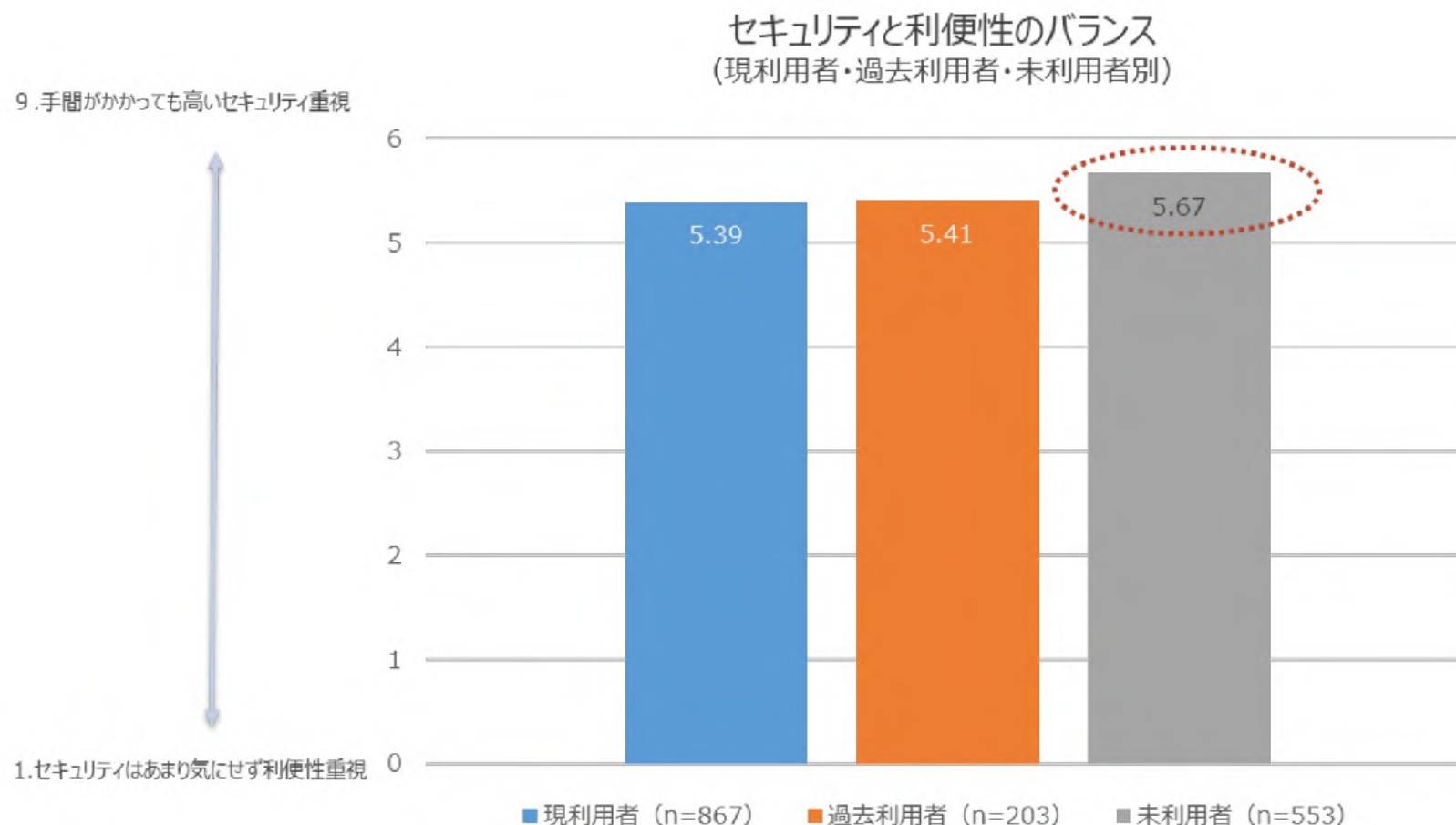
➤ セキュリティより利便性をより重視するのは約 2 割、利便性よりもセキュリティをより重視するのは約 3 割



3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連

(1) 情報セキュリティ対策 ②利便性とセキュリティのバランス (現利用者・過去利用者・未利用者の比較)

- 未利用者は、利用したことがある人よりも、利便性よりセキュリティを重視

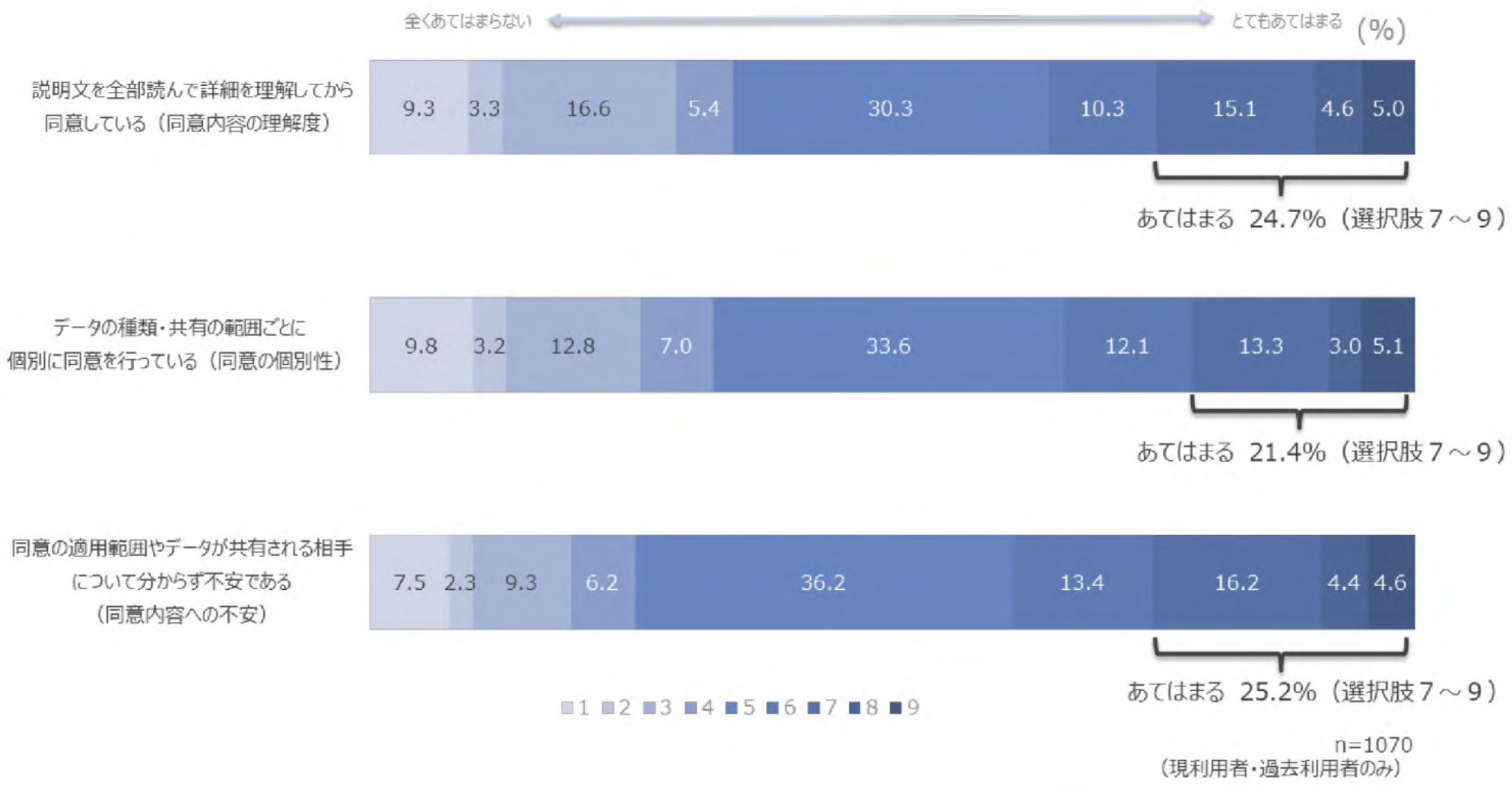


※選択肢「1.セキュリティはあまり気にせず利便性重視」～「9.手間がかかっても高いセキュリティ重視」の平均値を比較

3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連 (2) 個人情報の取扱い ①同意の理解度

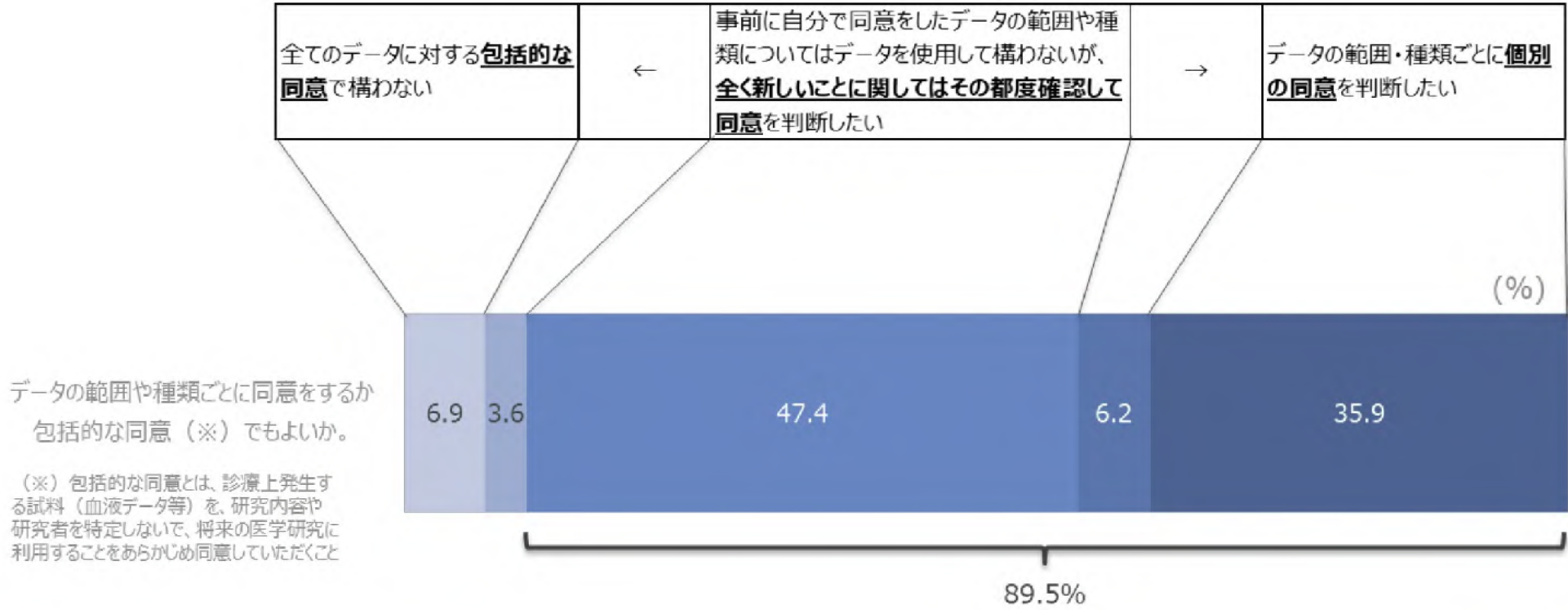
- 個別に同意をしている割合は、2 割強
- 同意内容を理解している割合及び同意の適用範囲やデータ共有相手について分からず不安を感じている割合は、4 人に 1 人

同意内容の理解度・個別性・不安



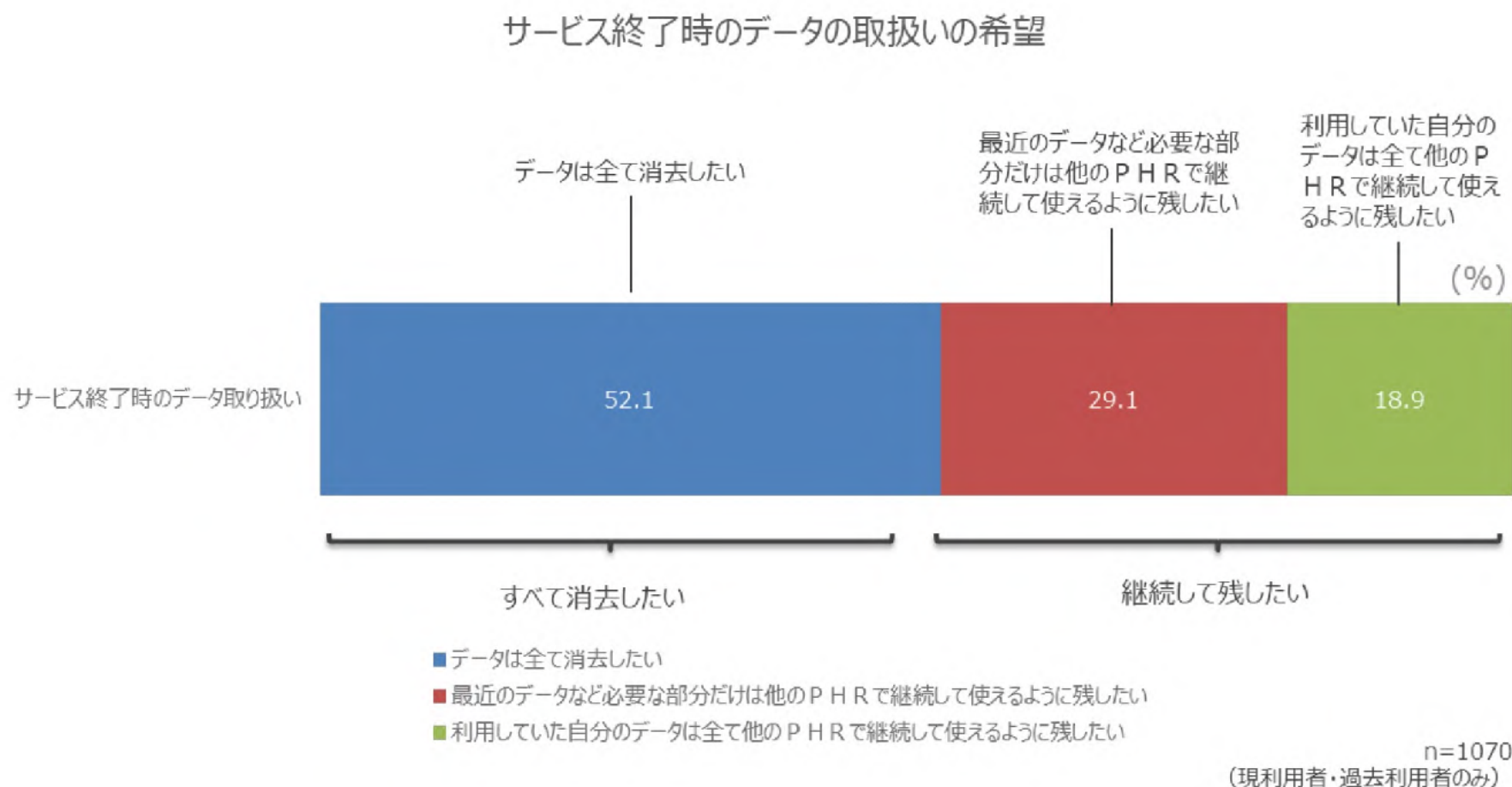
3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」（案） 項目関連
（2）個人情報の取扱い ②包括的同意の在り方

- 全てのデータに対する包括的な同意で構わないとする人は約 7 %
- データの範囲・種類ごとに個別に同意を判断したい及び、全く新しいことに関してはその都度確認して同意をしたいを合わせると、約 9 割が包括的な同意ではなく、データの範囲や種類ごとの同意を望んでいる



3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連 (2) 個人情報の取扱い ③サービス終了時のデータの扱い

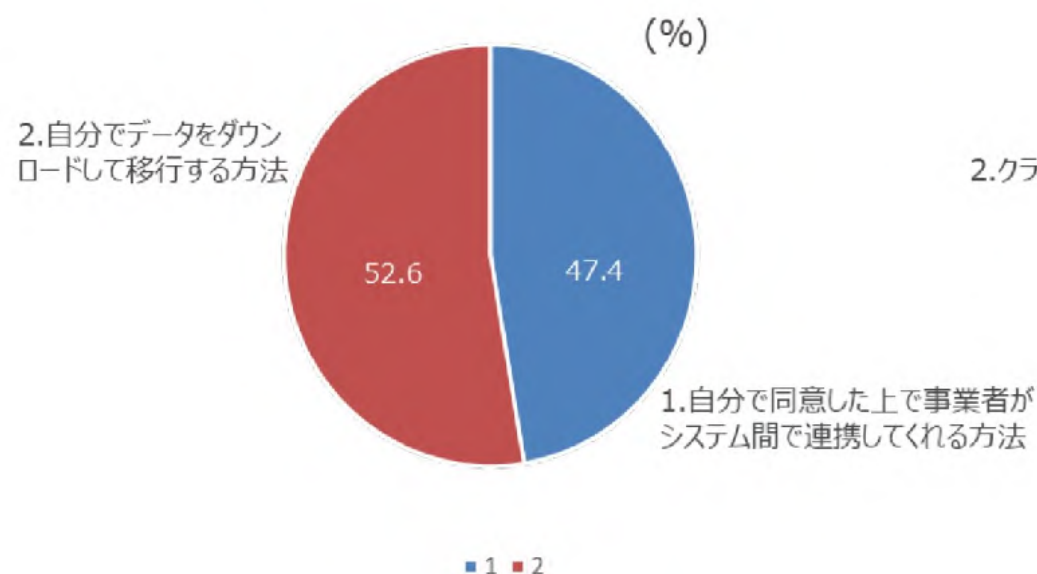
- サービス終了時のデータは、全て消去したい人と、何らか継続して残したい人が半々である



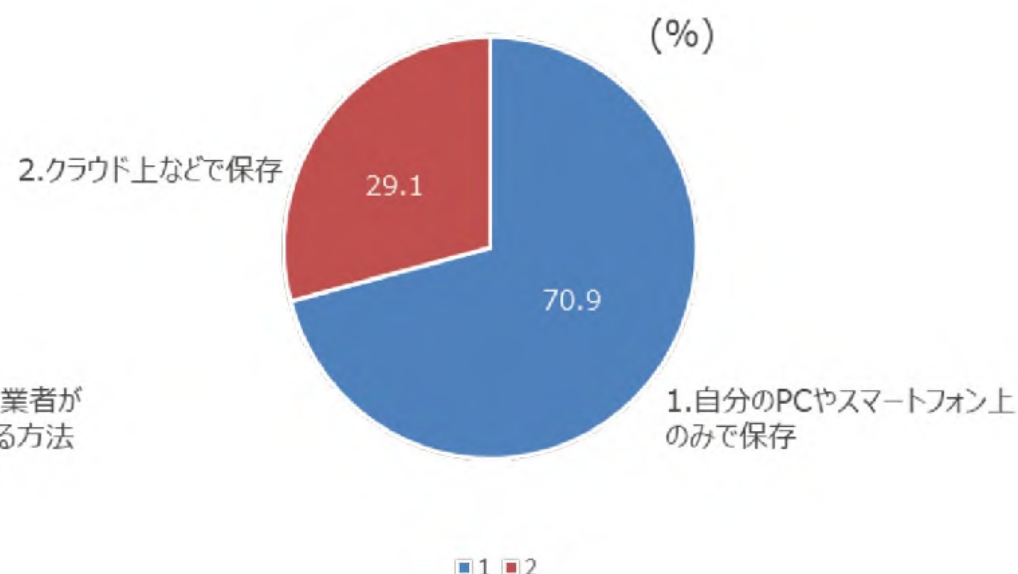
3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連 (3) 保存・管理、相互運用性の確保 ①ポータビリティ、サービス乗り換え

- サービス乗り換え時に希望するデータ移行方法は、「事業者にしてもらう」、「自分で行う」が半々
- 一方、希望するデータ保存方法については、クラウドを利用することを望む人が約 3 割

サービス乗り換え時のデータ移行方法



ダウンロードした場合のデータ保存方法



n=1623

3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連 (4) その他 ①判定スコアやプロファイリング結果の信頼性・妥当性

➤ 判定スコアやプロファイリング結果を信頼するのは、約 3 割

スコアリングやプロファイリングへの信頼性・妥当性



n=1070
(現利用者・過去利用者のみ)

3. 「民間 P H R 事業者による健診等情報の取扱いに関する基本的指針」(案) 項目関連 (5) 調査結果サマリ

情報セキュリティ対策

- ・ 利用するサービスのセキュリティに対する意識にはばらつきがある
- ・ 個人情報の漏えいに対する不安がある人は、利用したことのある人の約半数
- ・ セキュリティより利便性をより重視するのは約 2 割、利便性よりもセキュリティをより重視するのは約 3 割
- ・ 未利用者は、利用したことがある人よりも、利便性よりセキュリティを重視

個人情報の取扱い

- ・ 個別に同意をしている割合は、2 割強
- ・ 同意内容を理解している割合及び同意の適用範囲やデータ共有相手について分からず不安を感じている割合は、4 人に 1 人
- ・ 全てのデータに対する包括的な同意で構わないとする人は約 7 %
- ・ データの範囲・種類ごとに個別に同意を判断したい及び、全く新しいことに関してはその都度確認して同意をしたいを合わせると、約 9 割が包括的な同意ではなく、データの範囲や種類ごとの同意を望んでいる
- ・ サービス終了時のデータは、全て消去したい人と、何らか継続して残したい人が半々である

相互運用性の確保

- ・ サービス乗り換え時に希望するデータ移行方法は、「事業者にしてもらう」、「自分で行う」が半々
- ・ 一方、希望するデータ保存方法については、クラウドを利用することを望む人が約 3 割

その他

- ・ 判定スコアやプロファイリング結果を信頼するのは、約 3 割

I 民間P H Rサービス利用者へのアンケート調査結果

参考：健診等情報を取扱うP H Rサービス利用者の特徴

本調査に加え、健診等情報を取扱うP H R事業者の協力を得て1,774人分の追加アンケート調査を実施。

本調査の「オンライン診療・診療予約」「健康診断・医療費」「診療管理」「疾病管理」「お薬手帳」「出産・育児」利用者及びそれ以外のP H R利用者と、当該追加アンケート調査における健診等情報を取扱うP H Rサービス利用者のデータを比較した。

参考：健診等情報を取扱うPHRサービス利用者の特徴

実施概要

- 前述に示したアンケートでは、健診等情報の利用者の発現が少ないと想定されたため、健診等情報を取扱うPHRサービス利用者に対する追加アンケートを実施し、健診等情報を取扱うPHRサービス利用者の実態を把握した

【追加調査 実施概要】

項目	内容
アンケート対象	・健診等情報を取扱うPHRサービス（※1）（10事業者）利用者 （昨年度事業者アンケートから、「健診等情報を用い、かつ個人向けにサービスを提供する事業者」を抽出）
実施方法	・WEBアンケート調査（上記PHR事業者から自社利用者に案内、WEB上で回答）
実施期間	・令和2年12月下旬
調査項目	＜本体アンケートの項目から以下を抜粋（※2）（一部新規追加）＞ ・ 基本属性 ・ 属性（年代・性別） ・ 【新規追加】現在、利用しているパーソナルヘルスレコード（PHR）サービスやアプリ ・ 利用促進要因（利用による効果） ・ 利用にあたっての懸念点（有効性・安全性、データ連携、個人情報、セキュリティ、同意、サービス終了時への扱い、サービス乗り換え、使い勝手、サービスへの説明に関する意識） ・ 全員 ・ 欲しい機能、セキュリティと利便性のトレードオフ、連携ID、サービス乗り換え ・ 場面×データ範囲×連携したい相手、同意なく利用されたくない相手 ・ 望ましい同意の在り方

（※1）本作業班で議論されている「健診等情報」の定義に該当する情報を取り扱っているサービスを抽出したものであるが、これらは「健診等情報」の範囲と厳密に一致するものではない。

（※2）項目は以下の方針のもと抜粋

- ・ 健診等情報を取扱うPHRサービス利用者が、どのような利用に対して懸念点があるかを把握し、ルール作りに資することを目的に項目を選択する。
- ・ 情報の種類にかかわらず、国民全体の傾向として把握することを目的にした項目については、対象から外す。

なお、以降の解析にあたっては、下記①②③の利用者の回答を比較しており、①及び③を「健診等情報を取扱うPHRサービス（※1）利用者」とした。

①本調査における健診等PHRサービス利用者（n=440）：本調査における現利用者のうち、「オンライン診療・診療予約アプリ」「健康診断・医療費アプリ」「診療管理アプリ」「疾病管理アプリ」「お薬手帳アプリ」「出産・育児アプリ」を選択した回答者

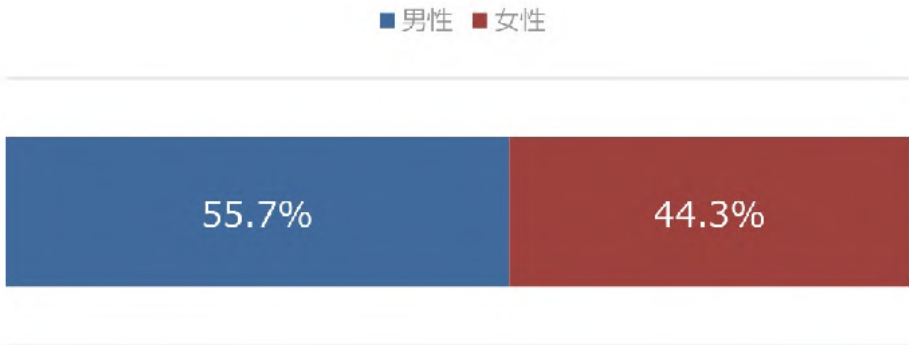
②本調査におけるその他PHRサービス利用者（n=427）：本調査における現利用者のうち、①の回答者以外

③追加調査における健診等PHRサービス利用者（n=1774）：追加調査の回答者

参考：健診等情報を取扱うPHRサービス利用者の特徴
追加調査 回答者属性

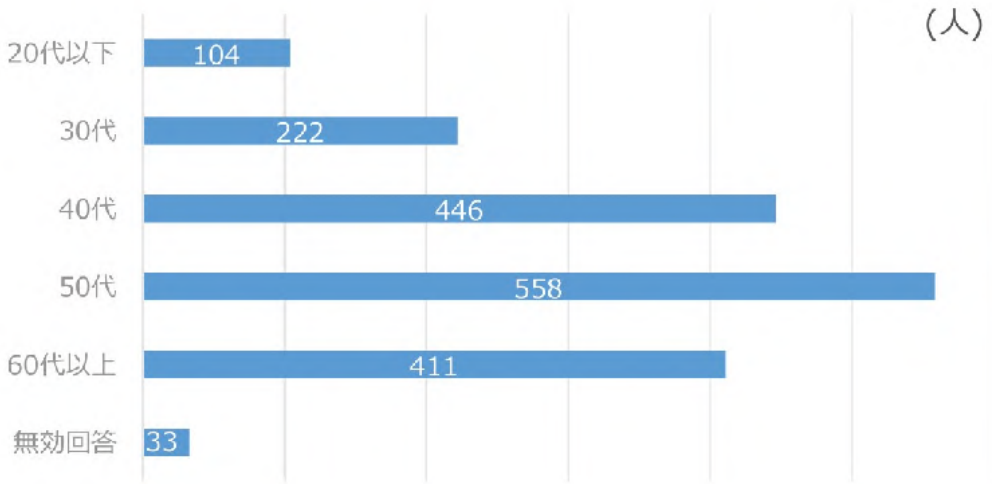
【回答者性別】

性別	人数	%
全体	1,774	100.0
男性	988	55.7
女性	786	44.3



【回答者年代別】

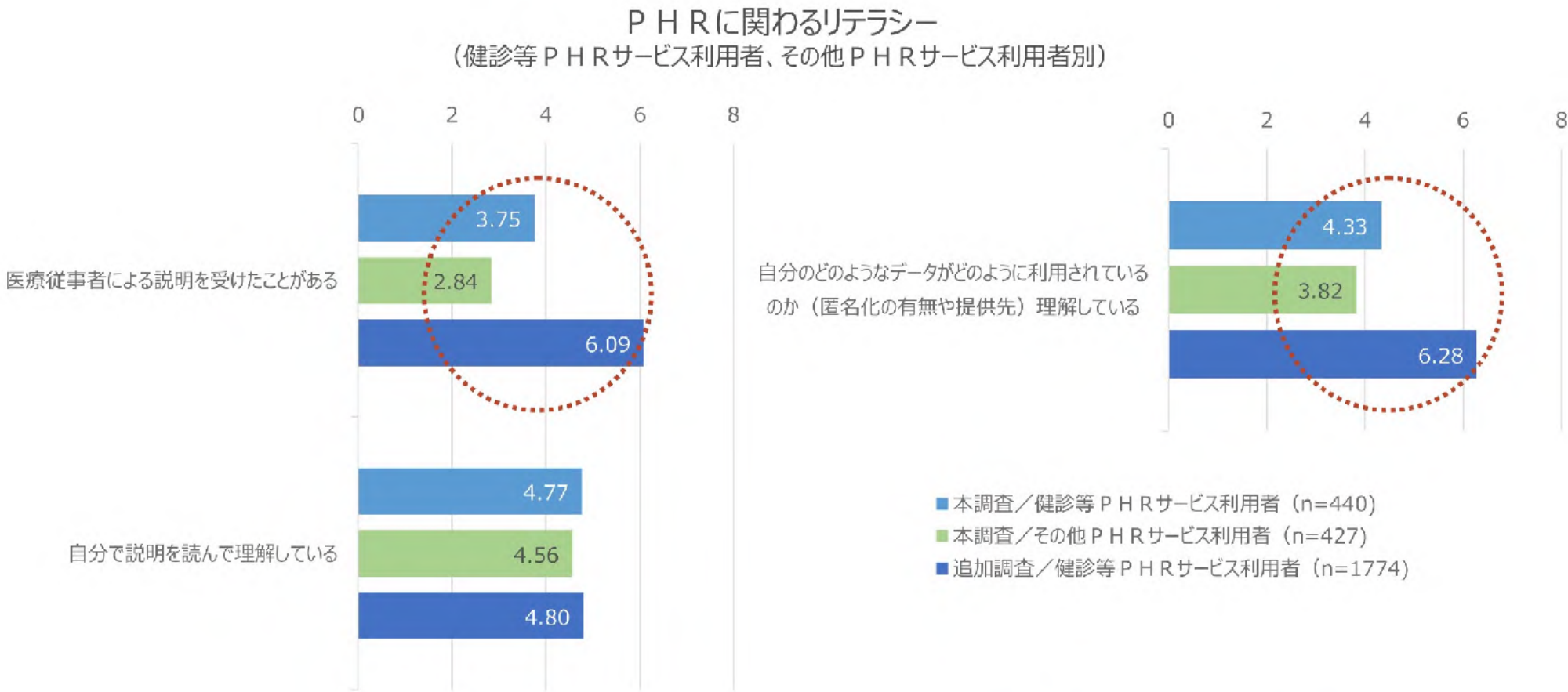
年代	人数	%
20代以下	104	6%
30代	222	13%
40代	446	25%
50代	558	31%
60代以上	411	23%
無効回答	33	2%
	1,774	100%



参考：健診等情報を取扱う P H R サービス利用者の特徴

P H R に関わるリテラシー

- 健診等情報を取扱う P H R サービス利用者は、その他の P H R サービス利用者と比べて、P H R に関わる説明を医療従事者等から受けており、個人情報の利用先についての理解も高い傾向

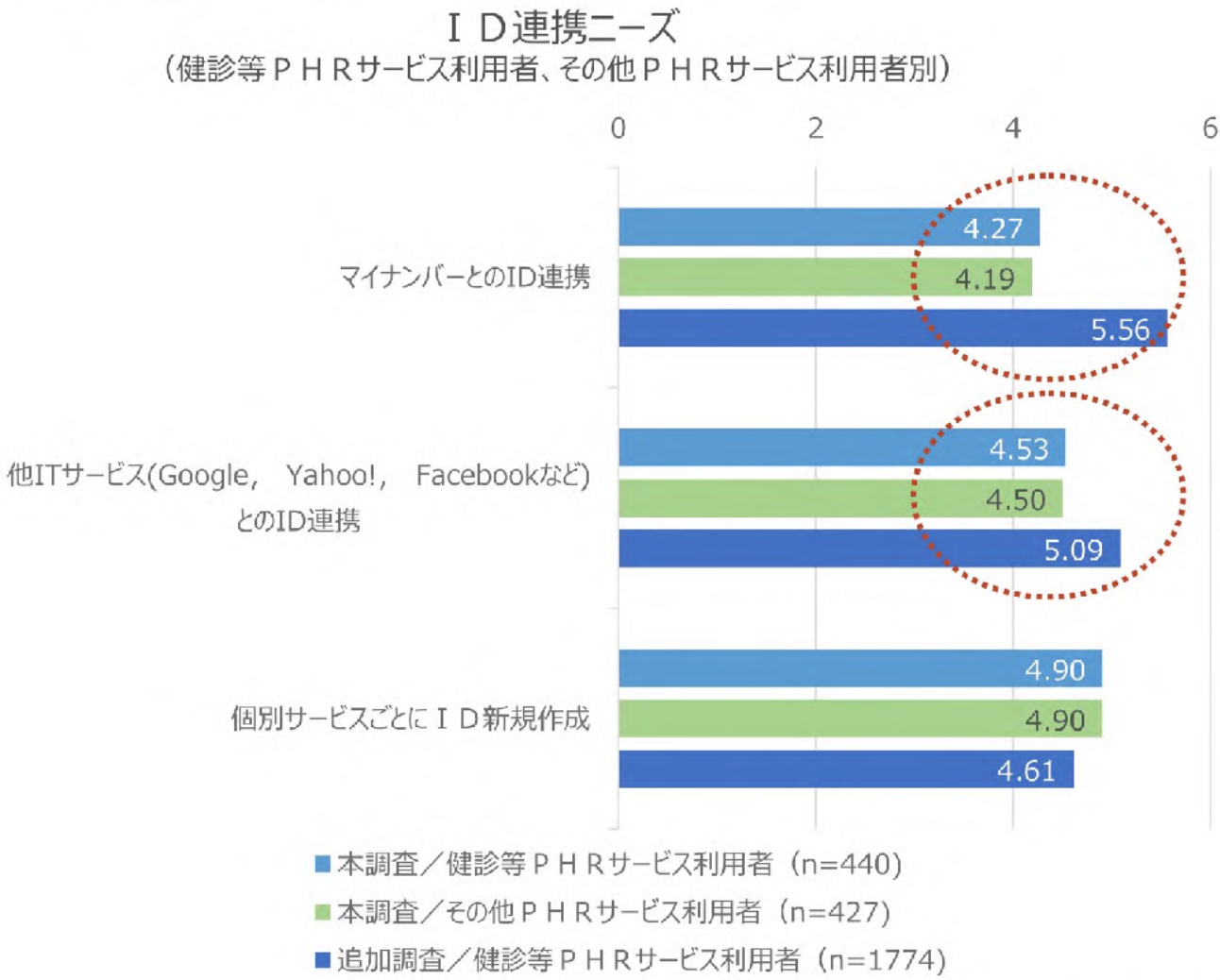


※選択肢「1.全くあてはまらない」～「9.とてもあてはまる」の平均値を比較

参考：健診等情報を取扱うP H Rサービス利用者の特徴

I D連携ニーズ

- 健診等情報を取扱うP H Rサービス利用者は、その他のP H Rサービス利用者と比べて、マイナンバーを含むID連携に前向きな傾向

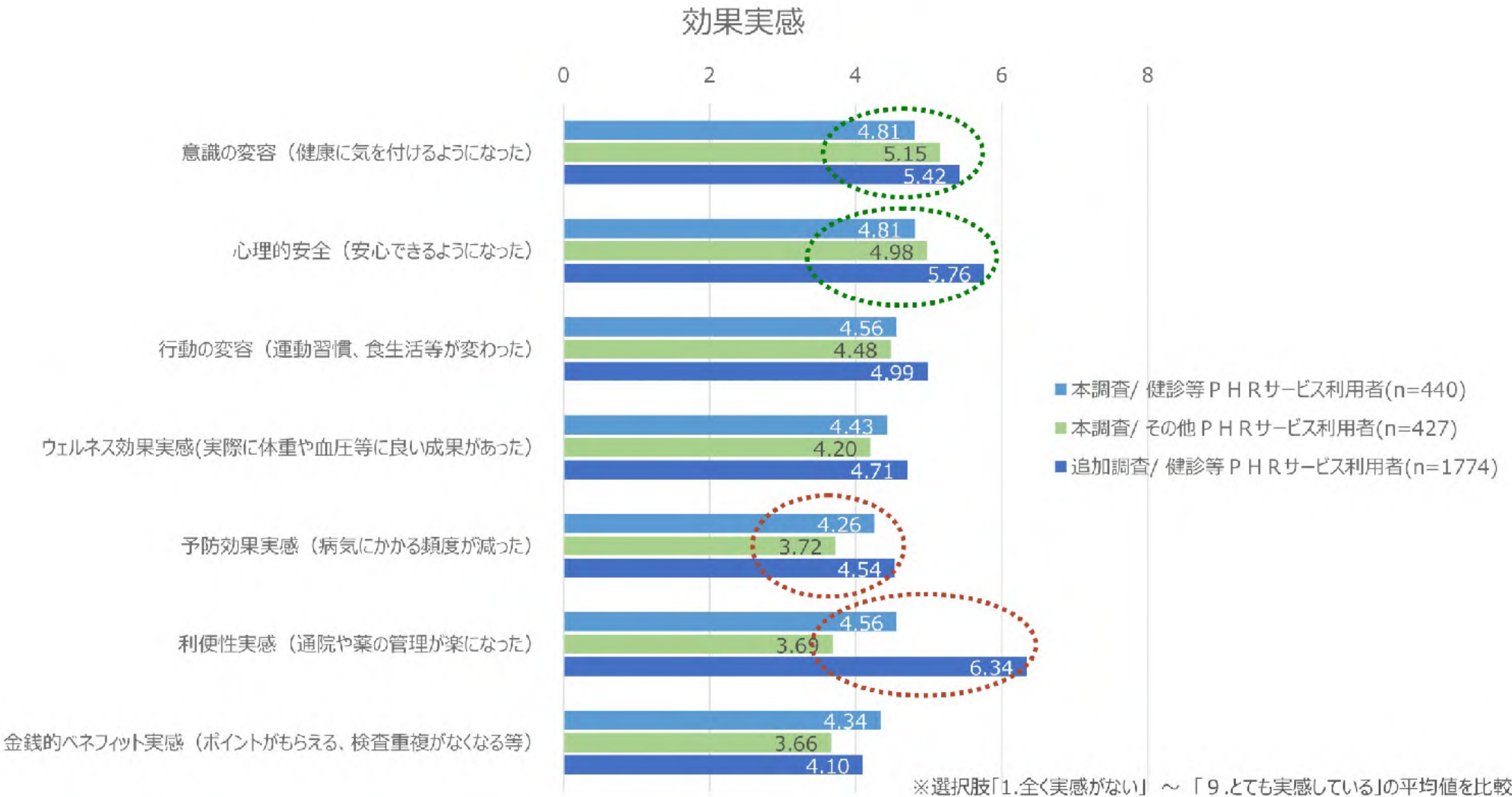


※選択肢「1.全く利用したくない」～「9.とても利用したい」の平均値を比較

参考：健診等情報を取扱う P H R サービス利用者の特徴

効果実感

- 健診等情報を取扱う P H R サービス利用者は、予防効果及び利便性において、効果を実感している傾向がある
- 意識の変容や心理的安全に関しては本調査と追加調査では傾向が異なった



参考：健診等情報を取扱うPHRサービス利用者の特徴
調査結果サマリ

リテラシー	健診等情報を取扱うPHRサービス利用者は、その他のPHRサービス利用者と比べて、PHRに関わる説明を医療従事者等から受けており、個人情報の利用先についての理解も高い傾向
ID連携	健診等情報を取扱うPHRサービス利用者は、その他のPHRサービス利用者と比べて、マイナンバーを含むID連携に前向きな傾向
効果実感	- 健診等情報を取扱うPHRサービス利用者は、予防効果、利便性及び金銭的ベネフィット感において、効果を実感している傾向がある - 意識の変容や心理的安全に関しては本調査と追加調査では傾向が異なった

Ⅱ 健診等情報に関するP H Rサービスを提供している 健康保険組合等に対するヒアリング調査結果

ヒアリング調査概要

【目的】

- ・ 保険者（国保・健保）には、P H R サービスを活用して被保険者等の健康増進を図るものがある。
- ・ そこで、保険者の被保険者等に対するP H R サービスの活用の現状と課題を把握することにより、**国や業界による民間P H R 事業者による健診等情報の取扱いに関するルールづくりに向けた検討に資する情報を取得することを目指す。**
- ・ 本調査では、上記検討における以下の論点において、利用者にとっての利用阻害となる事項を把握する。（同時に利用実態や利用促進につながる要素も抽出する）

【対象】

- ・ 単一健保
 - ・ 総合健保
 - ・ 自治体
- 計 6 団体

【時期】

令和2年 1 1 月下旬
～令和 3 年 1 月上旬

【調査項目構成】

1. サービス全体について
 - サービス内容
 - 運用状況
 - 利用による効果
2. サービス導入の経緯
3. 事業者選定について
4. 事業者評価について
5. セキュリティ・個人情報の取扱い・本人同意について
6. 安全性・有効性について
7. マイナポータルについて

ヒアリング結果から得られた示唆

➤ 各団体から得た意見の概要を以下にまとめた。

		ヒアリング結果
1. サービス全体について	・ サービス内容	(サービス内容・利用状況) ・ 保健事業の一環として毎月の医療費通知、歴年健診データ（5年分）を確認できる。 ・ 健診情報を閲覧できる。 ・ 端末への健診情報のダウンロードはできない。 (第三者提供) ・ <u>健診データ・レセプトデータの第三者提供は許可していない</u>。被保険者へのメリットがなければ提供する意義がない。 ・ ビッグデータ利用への需要はあり、第三者提供によりサービス費用は下がる。しかし、組織の総意により、<u>P H Rに集まった情報は第三者提供しておらず、今後もそのつもりはない</u>。 ・ <u>第三者提供はしていない</u>。 ・ 組織の保有するデータを民間 P H R 事業者に預託しているが、<u>第三者提供ができないため、本人が直接入力する方式に切り替えたい</u>。
	・ 運用状況	・ 閲覧機能を必ずしも活用できておらず、動機付けが課題である。健診データを閲覧するのは、健康に関心が高い層（高年層）である。 ・ 閲覧やキャンペーンにポイントを付与している。利用者属性は、ポイント収集を好む層である。 ・ 健診結果の受け取りまでに要する時間を考えると、W E B 上にログインし健診結果を確認するユーザーは少ない。 ・ 過去の健診結果閲覧はウェブ上でも閲覧は可能であるが、必要な際は健診機関へ問い合わせをして取得することを想定しているユーザーが多い。
	・ 利用による効果（評価）	・ アプリによる健康効果を今後検証する予定である。 ・ 通院をする者にとっては、健診結果を持ち歩かなくてよいのはメリットである。

ヒアリング結果から得られた示唆

		ヒアリング結果
2. サービス導入の経緯	サービス導入	- 広報誌、WEB等により、サービス導入の周知をしている。 - 口コミによる利用者拡大が見込まれるため、住民へ直接アプリの登録方法をレクチャーするなど、地道に周知している。 - ハガキにて周知をしている。
3. 事業者選定について	- 事業者選定基準 - 適切な評価、選択に必要な課題	(選定基準) - スピード感があり自主的な提案ができる<u>信頼感のある事業者</u>を選定。 - 当該領域に<u>実績のある事業者</u>を選定。 <u>データの二次利用をしないこと</u>、<u>金額の妥当性</u>の観点から事業者を選定。 - 応募事業者のサービス内容には大差なく、<u>予算面</u>が決め手となった。 (第三者認定等の仕組み) - 第三者認定の仕組みがあると、<u>選定・評価の指標</u>となるためありがたい。 - 信用調査のように、<u>民間P H R事業者のランキング</u>があるとよい。事業者の強みが見える化されているとありがたい。 <u>基準はある方がよい</u>。特に<u>セキュリティ等は自分達で判断が難しいため、お墨付きがあると良い</u>。 (事業者の継続性) - 契約は1年契約で、半年前までに契約破棄しない限りは契約が続く。 <u>民間P H R事業者から継続的にサービス提供されることは重要</u>である。 - 本人の健診等情報の元データが本人のスマホにあるのなら、P H R事業者のサービスが終了しても問題ない。 - 複数のP H R事業者に必要な情報を提供することで、1つの事業者が終了してもサービス全体としては継続できるようにしている。
4. 事業者評価について	サービス・事業者評価	- 自団体においてP H Rサービスに対する評価基準は特に定めていない。 <u>毎年監査を実施</u>し、サービスの棚卸や機能改善の要望への対応を確認している。ただ<u>評価基準までは定めていない</u>。

ヒアリング結果から得られた示唆

		ヒアリング結果
5. セキュリティ・個人情報の取扱い・本人同意について	・ セキュリティ	・ <u>自団体においてプライバシーマークの取得又はセキュリティ基準の設定等を行っている。</u> ・ <u>健診データを外部にアップロードをするのにあたり、特別に独自の個人情報規定を設けて対応している。</u> ・ <u>個人情報保護法等関係法令および「国保における個人情報の適切な取り扱いのためのガイダンス」や厚労省の事務連絡文書において示されている基準等を最低ラインとして設定した。</u> ・ <u>市町村説明の際は、事業者の対策が適切か厚労省にも確認いただき、理解を得た。</u> ・ <u>200数十項目のセキュリティに関する質問について、ヒアリングを実施することに加え、自団体のIT専門家による現地監査を行っている。</u> ・ <u>他部署の情報セキュリティ専門家を審査委員に入れて、安全性を確認した。</u>
	・ 個人情報の取扱い	(個人情報の取り扱いに関する基本的なルール) ・ <u>一般的な個人情報の覚書を民間PHR事業者と締結している。</u> ・ <u>利用目的はより詳細に記載するのが好ましいが、多数の被保険者対象に総意を得るのは難しい。</u> ・ <u>健診情報の閲覧には、なりすまし防止と本人同意取得のため、健診閲覧コード（事業者から圧着はがきにて送付）の入力を必須としている。</u> (サービス提供終了時・本人解約時のデータ取り扱い規定) ・ <u>資格喪失後は利用ができない。被保険者から健康データを引き継ぎたいとの要望は今までない。</u> ・ <u>これまで申し出はないが、本人請求があれば情報の削除などに対応することになっている。退職後も基幹システムの情報は保持している。</u> ・ <u>サービス終了時は事業者がデータを廃棄する。</u>
	・ 本人同意	・ <u>特定健診データについて、事業者間のデータ連携は、本人同意が得られれば過去の特定健診データを引き継いで運用できることにメリットがある。</u> ・ <u>委託先のPHR事業者へのデータ提供については、自団体の事業内でのデータ活用と位置付け、本人同意は取得していない。本人からの削除依頼に備え、『個人情報削除依頼書』を準備し、健康情報の削除依頼に対応している。(地方公共団体)</u> ・ <u>アプリ登録時に条件を提示しているが、個人のPHR登録時の利用規約については、細かい部分は把握していない。</u>

ヒアリング結果から得られた示唆

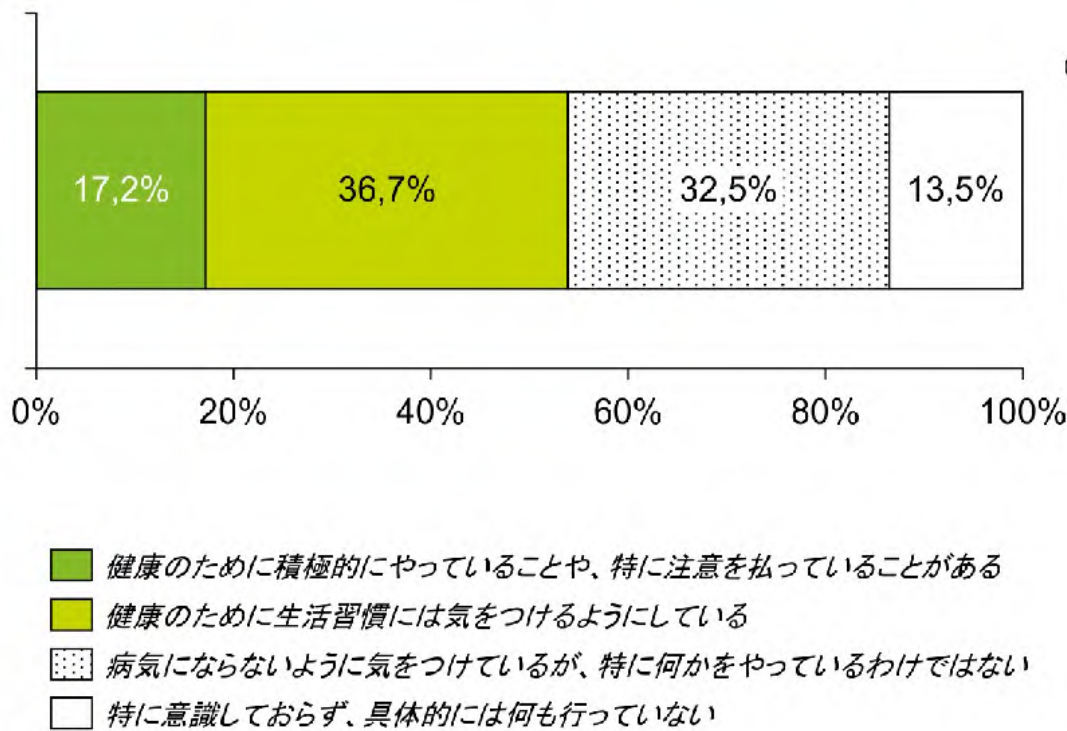
		ヒアリング結果
6. 安全性・有効性について	安全性・有効性に関する取組	- 生活習慣病リスクチェックの妥当性は、<u>提供する会社の信頼度、医師等の監修があるかどうかで判断している。</u> <u>サービス開発に医療系大学が関わっているため、安全性・有効性は担保されていると考えている。</u> - 事業者の知見を活用している。 <u>安全性・有効性の判断は明示がされるとよいが、明確な線引きは難しい。企業努力による部分もある。</u>
7. マイナポータルについて	マイナポータルとの連携	(活用の在り方（現在の活用状況、今後の活用プラン）) <u>既に独自に健康情報を閲覧させる仕組みをもっているため、マイナポータルとの連携によるメリットのイメージがまだついていない。</u> - 上手く連携しながら、スマホ世代を健康管理に取り入れていきたい。 - 現状のサービス拡大も考えているが、<u>マイナポータルも利用できるようになるため、独自のサービスが必要かを判断していきたい。</u> (活用時の課題) - 効果的な保健指導のためには前の健診情報が必要であるが、<u>必ず本人同意を求めるとなると機動性が低下するのではないか。</u> <u>マイナポータルで連携されたデータが誰のものをきちんと定義することが必要ではないか。</u> - 普及のためには、サービス提供者にとって魅力的なデータあることが重要。<u>そのためにデータセットやデータ形式を開放しておく必要がある。</u> - セキュリティを担保することで懸念や不安をどれだけ払拭できるのか。<u>他の情報も連動してくることで不安が増大する可能性がある。</u>

(参考)日本におけるPHR利活用の市場概況

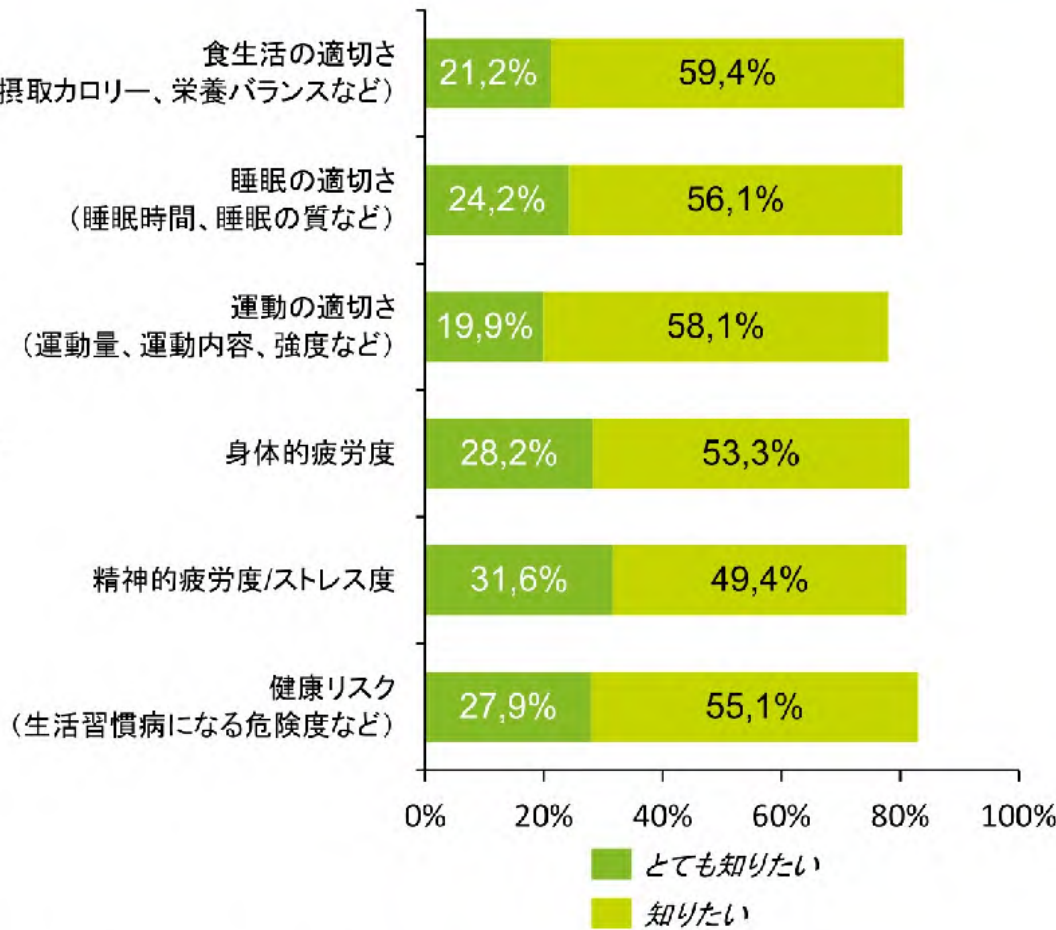
回答者のうち半数以上の人健康に気を付け生活をしていると回答しており、 およそ8割以上の人健康に関する自分自身の情報について知りたいと考えている

● 消費者における健康への関心

健康に気を付けるよう意識しているか (n=5,000)



健康に関して知りたい自分自身の情報 (n=30,000)

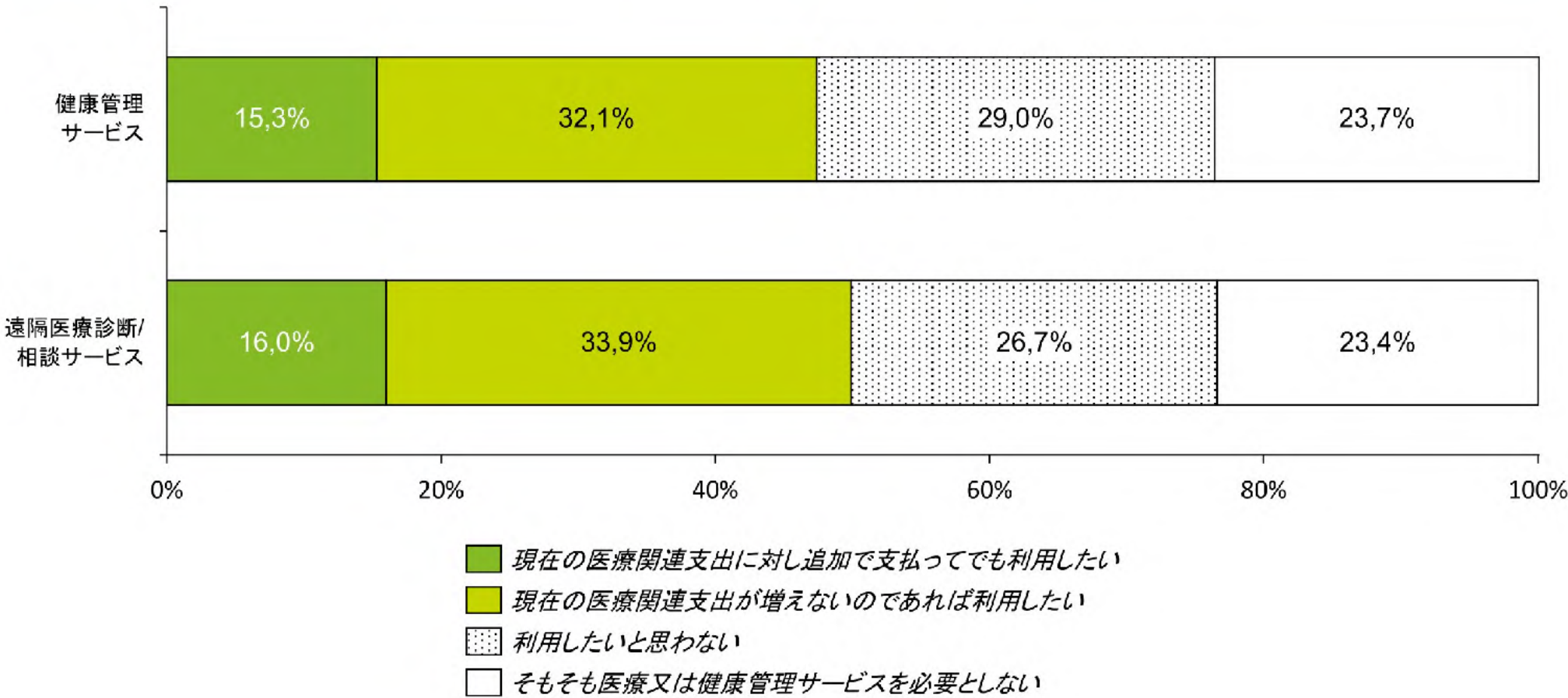


出所: 厚生労働省「健康意識に関する調査」(2014年8月) 及び三菱UFJリサーチコンサルティング「健康関連サービス動向の整理」(2017年9月)をもとに作成

消費者の半数程度に健康関連サービスの利用意向があり、利用意向のある人の3分の1の程度が、現在の支払額に追加しても良いと考えている

● 医療ICTサービスに対する利用意向

医療ICTサービスの段階別利用意向（n=1,000）

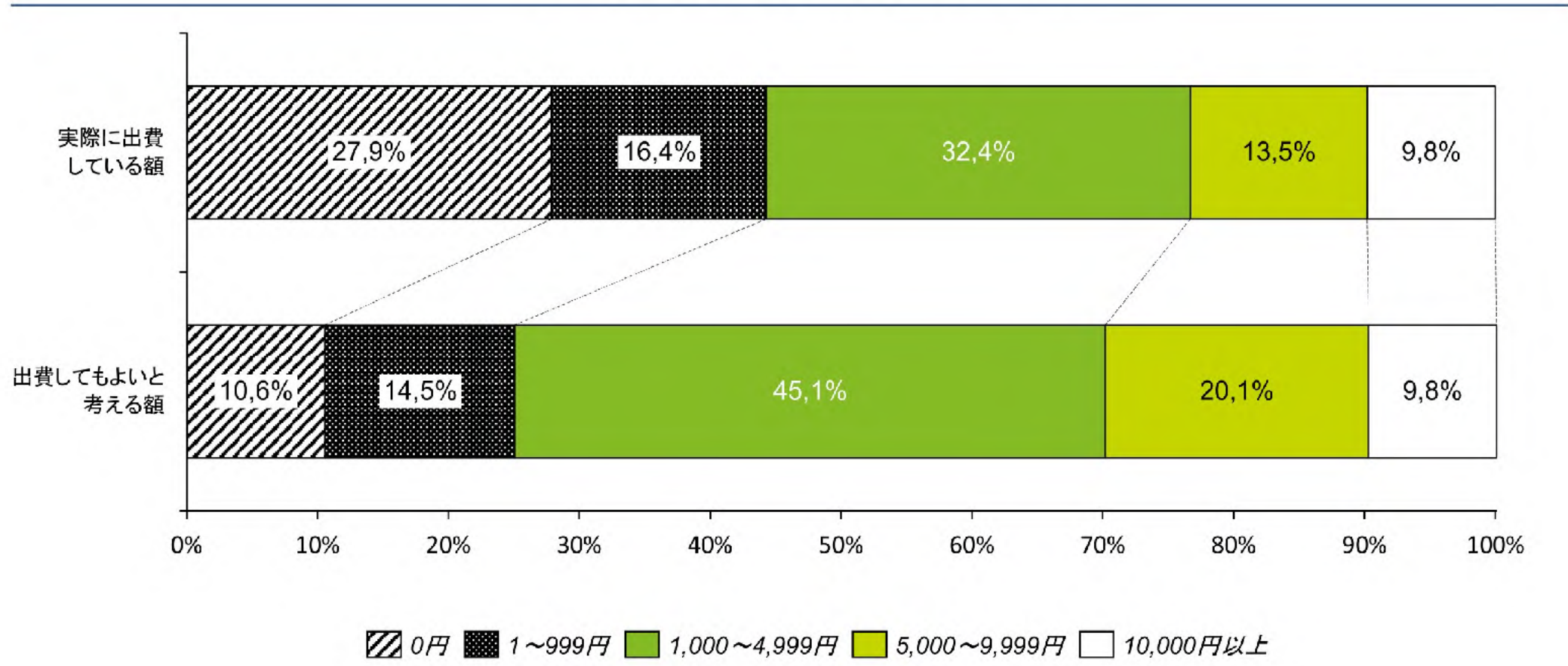


出所:総務省「平成28年版情報通信白書」をもとに作成

健康関連サービスに対する実際の出費額よりも、支払い意思額は高い事がうかがえる

● 健康関連サービスに対する支払い意思額

健康関連サービスへの支払い意思額 (n=5,000)



出所: 厚生労働省「健康意識に関する調査」(2014年8月)をもとに作成

(参考) 米国及び英国におけるPHR利用環境

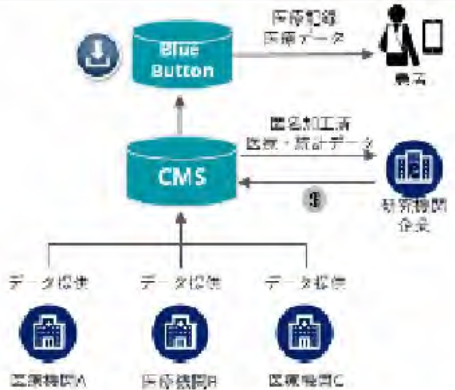
国民皆保険ではない米国においては、各州の医療情報連携をとり、民間の医療保険等で収集される医療情報を統括データベースで管理・利活用する方針を採用

● 米国における医療・保健制度及び情報管理体制の背景



情報集約・活用の体制

- メディケア及びメディケイドのレセプトデータを含む研究目的利用に開かれたデータベースを運営する連邦政府機関には、CMS(メディケア & メディケイドサービスセンター)の他、NIH(国立保健研究所)、CDC(疾病管理センター)、FDA、VHA(退役軍人病院庁)等がある
 - CMSには、メディケア及びメディケイドのレセプト情報、統計、研究データ等が保存されており、産官学の研究目的利用に広く活用されている
- 個人は、自身の医療情報をBlue Buttonのファイルからダウンロードすることができる



医療保険制度概要

- 米国には国民皆保険制度がなく、企業や個人が加入する民間の医療保険で医療費を賄うことを前提としている
 - 民間医療保険に加入できない、又は保険料負担を賄えない低所得者等向けの公的医療支援制度として、メディケアとメディケイドがある
 - ・ メディケアは、公的な医療保険プログラム (medical insurance program) であり、保健福祉省の内部部局であるCMS (Medicare & Medicaid Service Center: メディケア & メディケイドサービスセンター) がデータ保持およびデータベースの運営
 - ・ メディケイドは、低所得世帯を対象とする医療費支援プログラム (medical assistance program) として州政府が運営

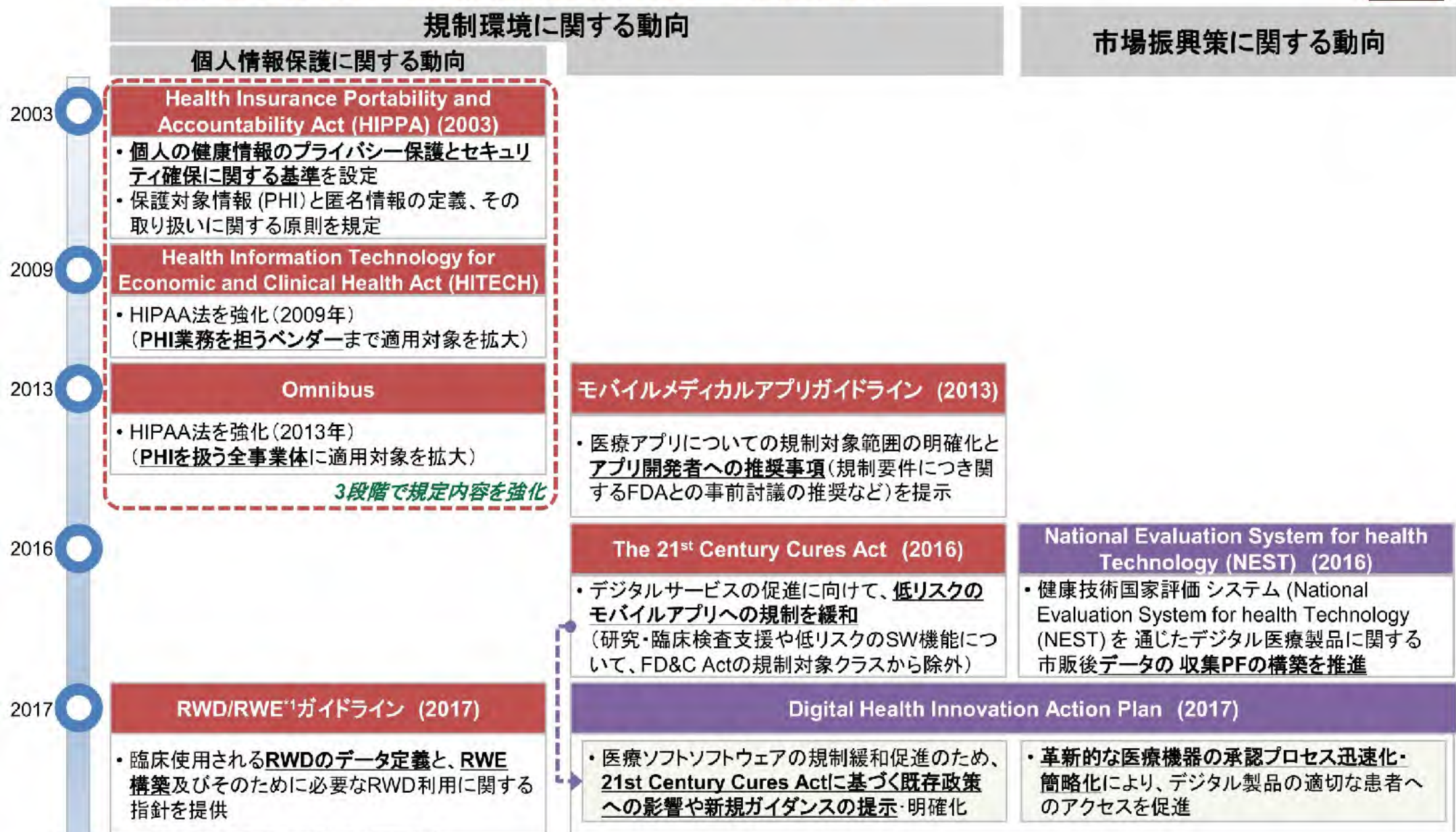
制度の名称	メディケア (Medicare)	メディケイド (Medicaid)
制度の性格	補足的医療保険	医療支援プログラム
保険料の徴収	賦課方式 + 税方式	税方式
財源	パート A: 社会保障税 パート B: 保険料 + 一般財源 パート C/D: 保険料	州政府の特別会計に対して連邦政府が補助金を交付
加入義務	任意	任意
監督機関	CMS (メディケア&メディケイドサービスセンター)	
運営機関	CMS	州政府
支払者	病院保険信託基金 補足的医療保険支払基金	民間保険会社
支払方式	償還払い	償還払い
受益者	65 歳以上高齢者、身体障害者、慢性腎不全患者等	低所得者
受益者数 (人口比)	56.8 百万人 (2016) (14%) ²	66.6 百万人 (2018) (19%) ³

出所: 厚生労働省「諸外国における健康・医療・介護分野のデータベースの現状調査」(平成30年度)、各種公開情報をもとに作成

米国：個人情報情報の取扱いに関しては、HIPPAが広範に参照されるシンプルな体系 そこにPHR関連のガイドラインを整備し、また、関連促進策に多額の予算を充当



● 米国におけるPHRサービス市場形成に向けたルール形成の流れ



*1 Real World Data, Real World Evidenceの略

HIPAAでは、患者情報保護の国家基準である「Privacy Rule」と、電子的に保持等される保健情報の安全確保に関する国家基準である「Security Rule」を規定

● HIPAA (Health Insurance Portability and Accountability Act)



- 概要**
- データ保持者又はそのビジネスアソシエートに保持、送付される**全ての「個人が特定可能な保健情報」に適用される。**これらの情報を「保護対象保健情報: protected health information (PHI)」とする
 - 患者の医療データを使用する原則として、匿名化された情報であるか、個人が特定可能なデータである場合にはプライバシールールの範囲内か、データ提供者が文書で許可した範囲に限定される
 - 匿名化された保健情報(de-identified health information)の使用又は開示には制限はない

構成

HIPAA項目

- I. HIPAA Health Insurance Reform
- II. HIPAA Administrative Simplification
- III. HIPAA Tax Related Health Provisions
- IV. Application and Enforcement of Group Health Plan Requirements
- V. Revenue Offsets

プライバシールール
45CFR Part 160
45CFR Part 164 Subparts A, E

- 個人が特定可能な保健情報を適切に保護することを規定
- 保護対象保健情報の使用・開示・管理に関する要求事項を規定

セキュリティルール
45CFR Part 160
45CFR Part 164 Subparts A, C

- データ保持者が電子化された個人情報適切に管理し、安全上の脅威から個人情報を保護し、関係従業員がコンプライアンスを遵守することを規定

出所: 保健福祉省HP(<https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.10HIPAATitleInformation.aspx>)をもとに作成

米国では、Blue Button 2.0という政府主導のPHRプログラムがあり、患者によるデータアクセスおよび管理能力の拡大を目的に推進されている

● Blue Button 概要

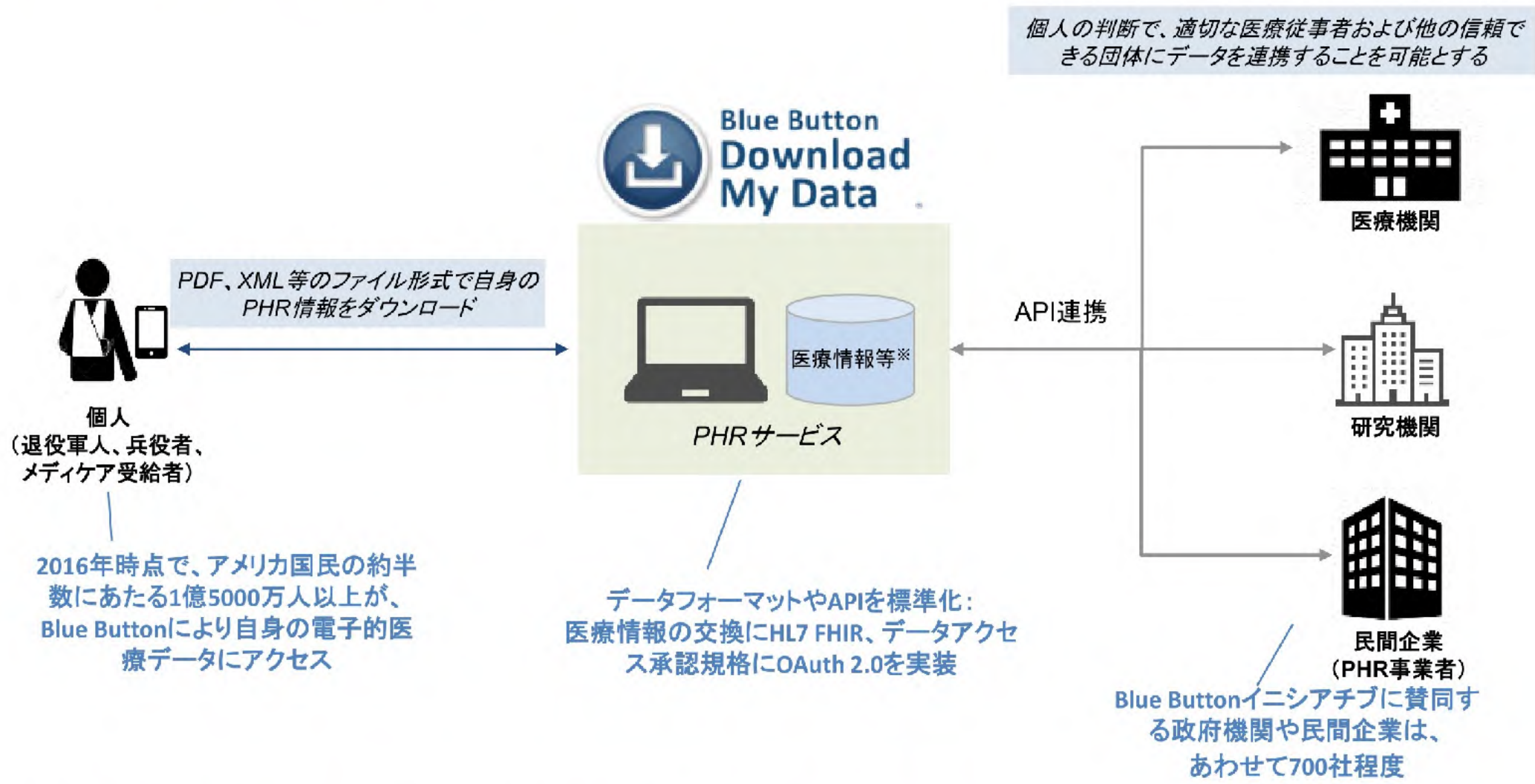


サービス名	Blue Button (米国)
概要	■ メディケア・メディケイドを運営するCMS (Centers for Medicare & Medicaid Services) がサービスを提供
サービスの概要	背景 ■ 2009年12月米国防総省がTRICAREオンラインポータルで患者の健康情報への安全なオンラインアクセスを提供 ■ それを受けて、2010年1月がヘルスケアITの相互利用性向上の作業グループを米マール財団が主催して開始 ✓ 民間企業、非営利財団、連邦政府からの多くの代表が参加し盛んな議論が行われ、“Blue Button Initiative”としてまとめる ■ 米国防総省が2010年にポータルのブランド名を“Blue Button”に変更 ✓ 国防総省が中心となって、健康記録情報を追加や機能強化 ✓ 健康記録のダウンロードだけでなく、APIアクセスを可能に ■ 利用者也賛同機関も毎年増加の大成功 ✓ 2016年時点で、アメリカ国民の約半数にあたる1億5000万人以上が、Blue Buttonにより少なくとも一つ以上の自身の電子的医療データにアクセス ✓ Blue Buttonイニシアチブに賛同する政府機関や民間企業は、あわせて700社程度 ■ 上記を受け、2018年にCMSがUI/UXやデータ相互運用性、セキュリティ/プライバシー対策などの機能を強化した2.0版を開発 情報共有の仕組み ■ 個人が、自分に関するPHR (医療・健康関係のデータ) をダウンロード可能 ✓ 個人の判断で、適切な医療従事者、介護者、および他の信頼できる個人または団体にデータ*を渡すことができ、それらのサービスでの連携を可能にする *: メディケア受給者のパートA、B、Dの4年分データ (処方薬、プライマリケアの治療内容、治療コストなど) ✓ 官民連携プロジェクトであり、多数の健康保険および米国内の病院等の個人の健康記録を保持する機関が参加しており、それらが保持するPHRを簡単に取得できる ■ 構造化データフォーマットやAPIを標準化 ✓ 医療情報の交換にHL7 FHIR、データアクセス承認規格にOAuth 2.0を実装

Blue Buttonを中核として、個人はもちろん医療機関及び民間事業者が医療情報に簡便にアクセス、またデータ活用可能とする仕組みを展開



Blue Button サービス概要図



※: 加入している健康保険、病歴、処方医薬品名、調剤データ、医療処置、バイタルサイン、検査歴等
出所: 各種公開情報を基に作成

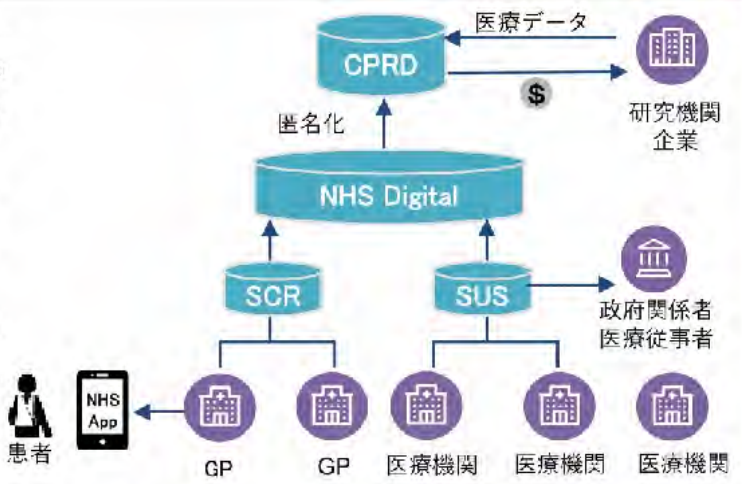
国民皆保険サービスを提供する英国においては、一次診療のデータおよび二次診療のデータを統括データベースで管理・利活用する方針である

● 英国における医療・保健制度及び情報管理体制の背景



情報集約・活用の体制

- 2008 年にNational Health Service (NHS)の主導により、GP が自身の患者の情報を登録して、夜間や緊急時に他の医師や看護師がアクセスすることができるプラットフォーム「Summary Care Record (SCR)」が導入された
- 2018 年、SCR の範囲は、長期的な健康状態、関連する病歴及びケアに関する情報も含むように強化され、EHR からPHR へ進化した。研究目的での提供を可能にするデータベース「Clinical Practice Research Datalink (CPRD)」が構築された
- 二次診療情報はSecondary Uses Service (SUS)に保管され、アクセス者の職位などによってデータの匿名性がidentifiable (識別可能), anonymized (匿名化), pseudonymised (仮名化)の3段階で異なる



医療保険制度概要

- NHS(National Health Service)と呼ばれる国民皆保健サービスを政府が提供しており、イングランド、スコットランド、ウェールズ、北アイルランドに分割され運営されている。国民は、いずれかの診療所を選択し、かかりつけ医(GP: General Practitioner)を登録することになっており、原則として、登録したGP のプライマリケアを受けることとなる。NHS は、GP から構成されるCCG(Clinical Commissioning Group)により運営されている。原則として自己負担は一切ない。すべて税財源で賄っている
- イングランドにおける医療提供者はNHSイングランド(NHS England, 以下NHS)であり、医療機関は、一次診療(primary care)の実施機関としてNHSと契約したGP診療所(GP Practices)等と、入院、救急、精神科治療、コミュニティサービス等の二次診療(secondary care)の実施機関としてNHSと契約した病院等に分けられる

制度の名称	NHS (National Health Service)
制度の性格	保健サービス
保険料の徴収	税方式
財源	一般財源
加入義務	強制
監督機関	Care Quality Commission, NHS Improvement
運営機関	NHS England
支払者	NHS England CCGs (Clinical Commissioning Groups)
支払方式	第三者払い方式
受益者	全居住者
2016 年の受益者数(人口比)	54.3 百万人 (100%)

出所: 厚生労働省「諸外国における健康・医療・介護分野のデータベースの現状調査」(平成30年度)、各種公開情報をもとに作成

英国では2019年にDigital Healthデベロッパー向けガイダンスが公開 サービス機能に応じてデータ品質の担保をデベロッパーへ要求している

● 英国におけるDigital Health Technologiesに関するガイダンス



組織	National Institute for Health and Care Excellence (NICE) 英国国立医療技術評価機構	NICE National Institute for Health and Care Excellence
概要	■ 英国の医療品質向上を目的とした英国政府機関管轄下の特別医療機構として1999年に設立 ■ 主に①NHS(英国国民保健サービス)が用いる医療技術②各疾患に対して行われる治療法の中で、適切な治療手順の判断③公的機関に向けた健康づくりと防疫に関する情報提供といった業務を行っている ■ 2019年3月にはNHS主導の下、NICEがDigital Health Technologies(DHT)に関するEvidence Standards Frameworkを公開	
DHT Evidence Standards Framework	【Evidence Standards Framework for DHT】 要求されるエビデンスはDHTの機能に応じて階層化されている。DHTは4つのTierに分類されており、PHRプラットフォームから自己管理アプリ、診断デバイス等も広く含む。Tier特性に応じてデータ品質に関するエビデンスが求められている ■ Tier1 ➢ PHRプラットフォーム等のシステムサービス ■ Tier2 ➢ 医療従事者とのコミュニケーションツールやフィットネスウェアラブルデバイス等 ■ Tier3a ➢ 禁煙、睡眠改善等の習慣改善や自己管理ツール(医療従事者との情報共有含む) ■ Tier3b(一部Medical Deviceも含む) ➢ 遠隔モニタリングデバイスや診断デバイス、医療判断に影響を与える計算ツール等 機能別に分類されたDHTの階層エビデンス The diagram illustrates the Evidence Standards Framework for Digital Health Technologies (DHT), categorized into four tiers based on functionality and evidence requirements: Evidence tier 1: Includes a box for 'Self-management' (Self-management: DHTs with no measurable patient outcomes that provide services to the health and social care system). Evidence tier 2: Includes three boxes: 'Monitor' (Monitor: Provides information, resources or advice to the patient, practice or clinician, focused on monitoring a condition or general health and fitness), 'Data collection' (Data collection: Collects personal health information using IT tools, new devices and long-term/continuous data), and 'Connectivity' (Connectivity: Allows clinicians to access patient data, records or information). Evidence tier 3a: Includes two boxes: 'Promote/alter behaviour' (Promote/alter behaviour: Address public health issues, smoking, eating, health, sleeping and exercise) and 'Self-management' (Self-management: Allows people to self-manage a specified condition. May include behaviour change programmes). Evidence tier 3b: Includes four boxes: 'Treat' (Treat: Provides treatment, therapy, diagnosis), 'Active monitoring' (Active monitoring: Monitor patient condition using wearable or implanted device and/or sensors data about a specified condition), 'Calculate' (Calculate: A calculation that supports or informs treatment, diagnosis or care), and 'Diagnose' (Diagnose: Diagnose a specified condition, disease or symptom).	

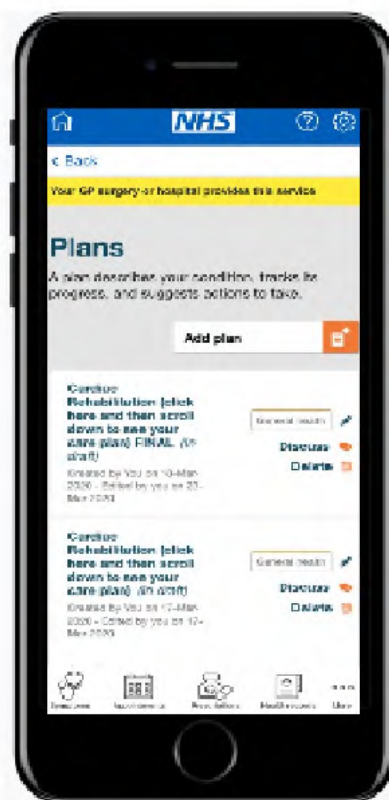
*1 NICE, "EVIDENCE STANDARDS FRAMEWORK FOR DIGITAL HEALTH TECHNOLOGIES", March 2019

NHSアプリを通じて、患者は自身の医療記録を閲覧できるだけでなく、医療データを第三者に提供して利用することが可能

● NHS Appを通じた患者本人によるデータアクセス・管理



- ✓ 氏名、NHS番号、生年月日、メールアドレス等の情報を記入し、ログイン



- ✓ 診察予約管理
- ✓ 処方箋の再発行依頼
- ✓ GP医療記録の閲覧
- ✓ 臓器提供の意思登録
- ✓ NHS111を通じて医師等に連絡



- ✓ GP登録情報をNHSが認定する第三者アプリ*と共有