資料４

前回の意見を踏まえた論点

目次

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

1．対象情報及び対象者

１．対象情報及び対象者①

前回提示した対象情報及び対象者の案

- 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

前回の主な意見

- 例えば、診療所等で測定したHbA1c値を、患者自身がPHRアプリに入力した場合は対象となるのか。
- 調剤情報を取り扱う電子お薬手帳は対象となるのか。

１．対象情報及び対象者②

対象情報及び対象者の考え方（案）

- 対象情報：

個人が自らの健康管理に利用可能な個人情報保護法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
・医療機関で測定された検査値又は調剤記録等の医療機関等から個人に提供される情報
・個人が自ら測定する検査値等で診療録に記録された情報

※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、レセプト記載の薬剤情報並びに医療機関等から個人に提供された検査値及び調剤記録等が挙げられる。
※上記情報を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。

２．　情報セキュリティ対策

２．情報セキュリティ対策①

前回提示した考え方（案）

※制度上の要求事項へ上乗せする事項は★

- 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。（★）

前回の主な意見

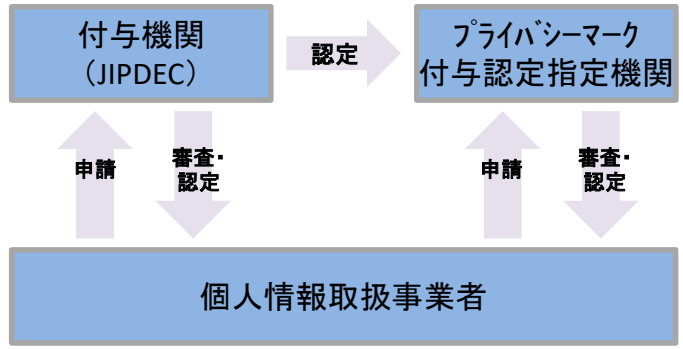
- 第三者認証を取得することに努めるべきと努力義務になっているが、中小企業等が大変ということであれば、PHRに特化して中小企業でも取りやすい第三者認証の取得を義務とすべき。
- 以前のアンケートでISMS、Pマークを取得している事業者は約半数（＊）だったので、義務化をするとやや厳しいという印象。一定件数以上の情報を取り扱う事業者は義務化し、急に超えてしまったら猶予期間内に取得するなどが現実的。

（＊）ISMS、Pマークを取得している事業者はアンケート回答者の６割程度

- 健診等情報を取扱う事業者であり、そこまでの情報を扱うなら、そのくらいの認証は必要ではないか。
- マイナポータルに直接接続する事業者だけであれば、１つの考え方として、ISMS、Pマークの義務付けという考えはあり得る。

2．情報セキュリティ対策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	

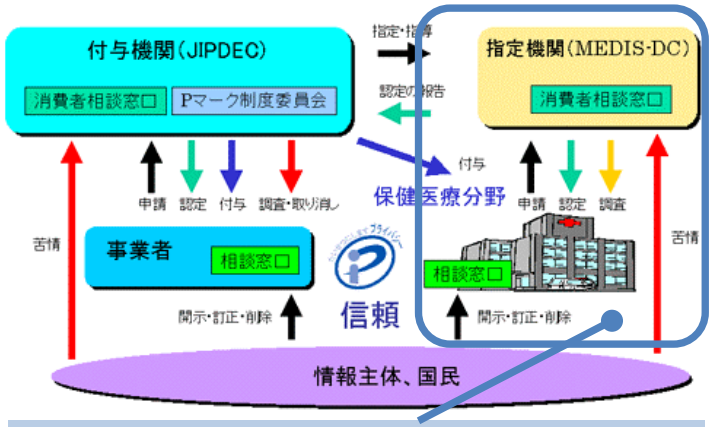
*1　JIS Q 15001「個人情報保護マネジメントシステム－要求事項」に基づいた個人情報保護マネジメントシステム（PMS）を定め運用していること、規定の欠格事項に該当しないことなど、必要な条件を満たしていることが前提となる

2．情報セキュリティ対策③　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

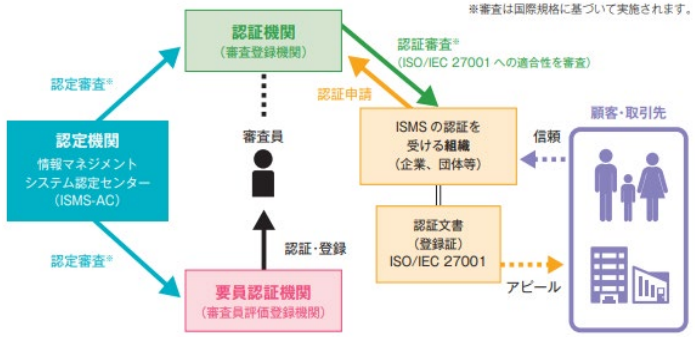
概念図



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．情報セキュリティ対策④ 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．情報セキュリティ対策⑤

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★

- 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又はプライバシーマーク等）を取得することに努めるべき。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。（★）

※患者等の利用者の指示に基づいて医療機関等から健診等情報を受領するPHR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）の遵守が必要となり、当該ガイドラインでは「プライバシーマーク認定又はISMS認証を取得すること」とされている。

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

前回の主な意見

- 匿名加工情報に関する制度上の要求事項を整理すべき。
- 匿名情報の第三者提供は、この指針の外である、今回の検討の外であるという理解で良いかを整理して検討すべき。
- 医師名、薬剤師名が入っている場合、要配慮個人情報ではないがどのように対応すべきか。

3．個人情報の適切な取扱い②　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
匿名加工情報を作成する場合	■ 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）
匿名加工情報を第三者提供する場合	■ 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）
匿名加工情報を受領する場合	■ 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．個人情報の適切な取扱い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手した場合、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を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

3．個人情報の適切な取扱い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★

＜匿名加工情報の取扱い＞

- 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。

＜医師名、薬剤師名の取扱い＞

- 医師・薬剤師の氏名等は、要配慮個人情報には該当しないものの医師・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うこと。
- 医師・薬剤師の氏名等を第三者提供する場合の取扱いについては、業界において関係団体と協議の上で、検討すべき。（★）