JAMI2019　チュートリアル3

主催：一般社団法人PHR協会

テーマ：「健康づくりに貢献するPHR」の流通・活用戦略の課題とその対応

令和元年6月

（一社）PHR協会理事　森口修逸

本チュートリアル専用ページ　http://www.m-p-o.co.jp/phrj/2019tutorial/

（一社）PHR協会のご紹介　http://www.phrj.org

本講演の主旨

1. 国民の健康維持や疾病治療の向上へ
   - 利用者（PHR本人）の同意を得てPHRを収集・利用、
   - さらに、多くの人のPHRを活用して健康管理や医療を改革し実践
2. 2013年：OECDプライバシーガイドライン（ OECD一GL）は30年ぶりに改訂
   - OECD加盟外諸国も含む、プライバシー保護のマネジメントプログラム構築
3. OECD一GLから、
   - 2017年5月全面施行：改正個人情報保護法「**適正かつ効果的な活用を積極的に推進することにより、活力ある経済社会及び豊かな国民生活の実現に資する**」
   - 2018年5月：次世代医療基盤法により匿名加工医療情報の、さらなる利活用へ
   - 2018年5月全面施行：EUのGDPRでは、PbD／PIAによる「設計時からのデフォルトでのプライバシー保護」を要求
4. PHRのような個人健康情報を活用した新たな社会・技術システム
   - プライバシー保護と利用者の合意獲得の観点から、PbD及びPIAの思想が有用
   - 客観的指標による規制緩和不足で、何十年も「技術的には十分」から進めなかった
5. トータルPHRの技術的仕組みを論じ、PbD・PIA思想の活用による客観的指標の提案

EUのGDPR（**G**eneral **D**ata **P**rotection **R**egulation)
PbD（Privacy by Design)
PIA（Privacy Impact Assessment)

1.健康づくりPHRと
トータルPHRの技術的仕組み
（試案）

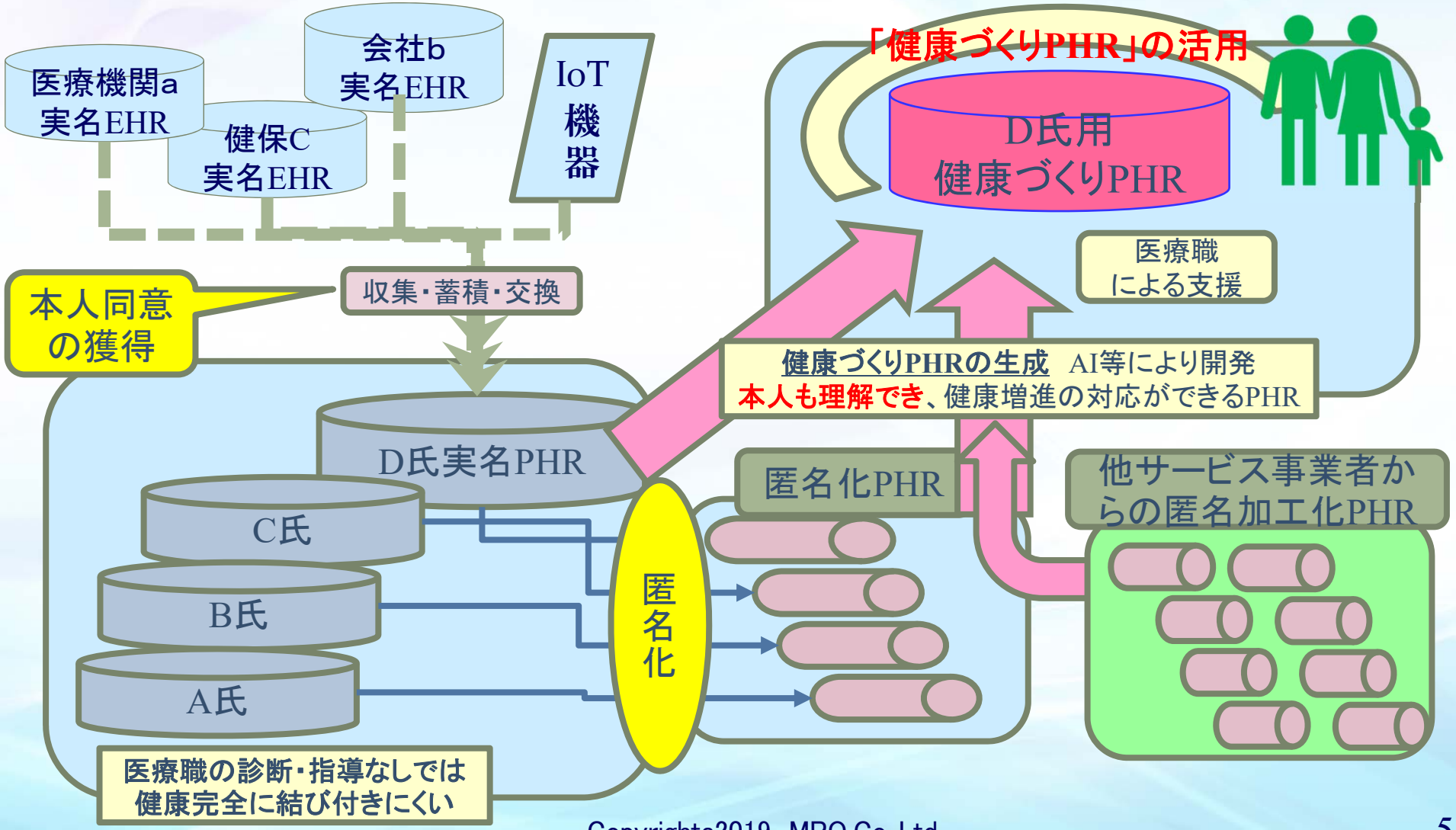
どのように、
個別のPHRを生成し
全人生にわたるトータルPHRへ
蓄積するのか？

健康づくりPHR

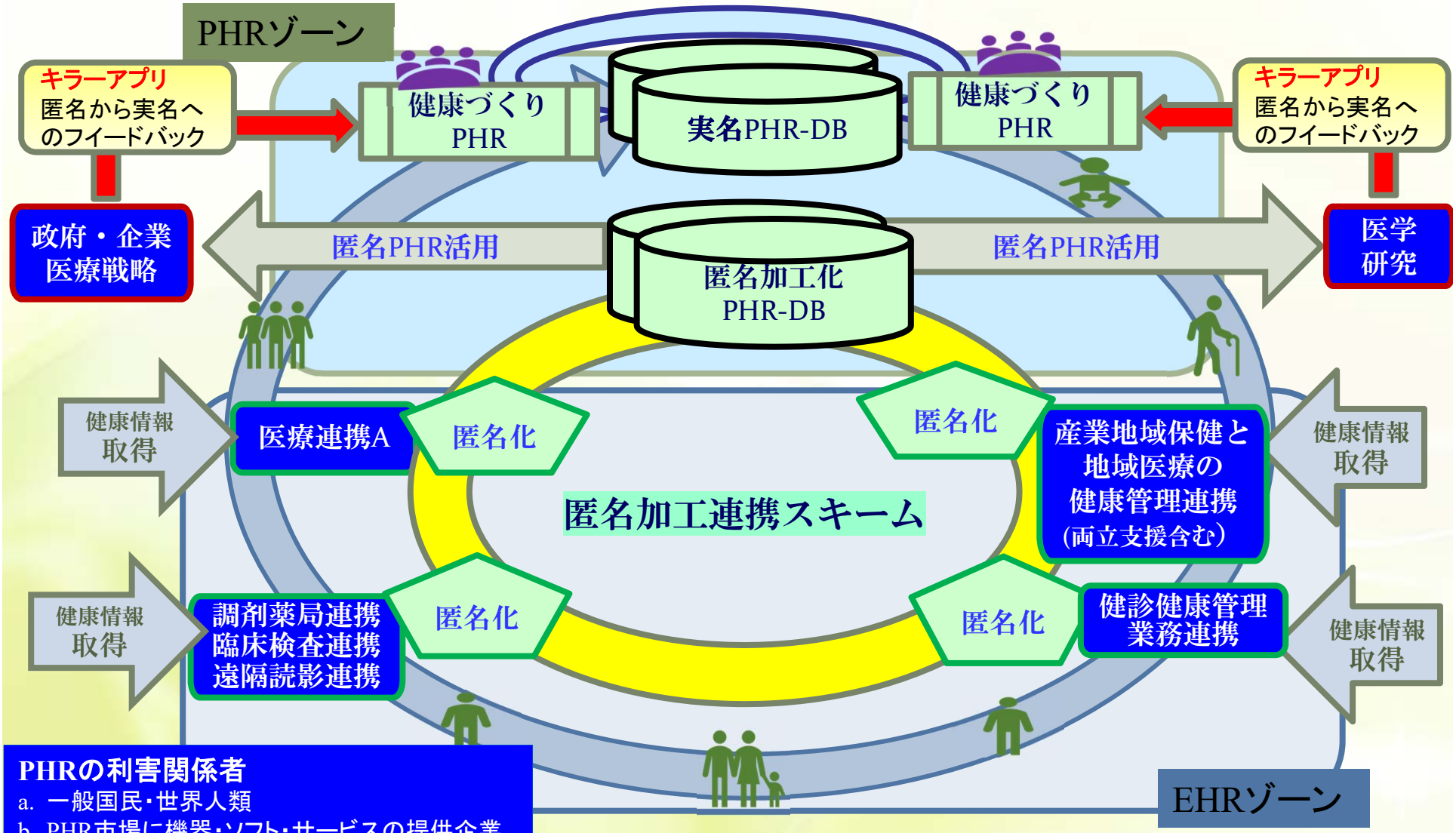
1. 実名PHRや匿名化PHRはEHRとして蓄積されているものを個人別に並べ替えただけで、検査結果や読影・読図所見・診断結果などが、個人の行動変容を直接惹起するには至らず、医師・保健師などの専門家の助けが必要。
2. PHRサービス事業：
   - 個人の特性・自己実現ニーズに対応し、より効果的な行動変容への導きかた・健康増進手法・治療方法・介護施設や介護手法の提案ツールやサービスの提供を行うビジネスが期待できる。
3. 健康づくりPHR ：
   - PHRサービスためのツール。PHRの本質は個人健康情報の本人がその中身を理解して管理し活用するためにある。プロの医師や医療職だけではなく、一般人が理解できる「健康づくりPHR」が必要で、これこそ「PHRのキラーアプリ」となることが期待され開発が急務
   - 健康づくりPHRは医療情報分野における重要な国際戦略商品となりうる。
     我が国は健診大国であり世界に先駆ける、高齢化社会大国である。キラーアプリの基礎データは諸国に比してはるかに充実しており、健康づくりPHRの基礎データ収集・データベース化・AI等によるデータ分析と健康増進策、その成果の分析力は、国際的に優位
4. 現状は、個人健康情報の利活用にブレーキがかかりやすく、市場への投入が遅れている。

実名PHRと匿名化PHRからの健康づくりPHRの生成と活用

PHRを有効に活用するには、実名PHRと匿名化PHR（匿名加工化PHR）の存在が必須であり、さらに、これらが逐次的（リアルタイム）に蓄積できる技術的な検討が望まれる。



保有組織から見たPHRの全体像
―実名・匿名化連携スキーム―

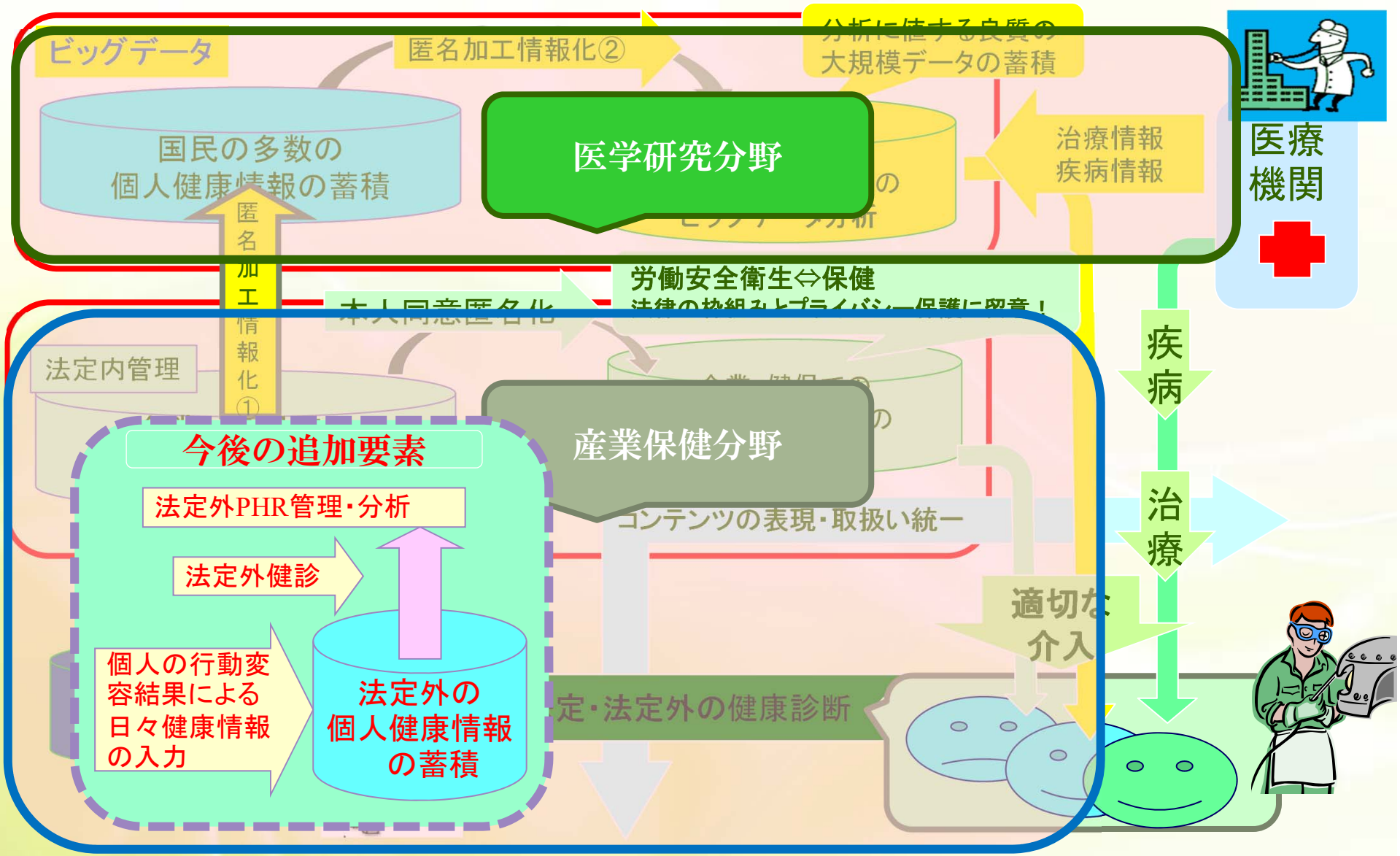


PHRの利害関係者

a. 一般国民・世界人類
b. PHR市場に機器・ソフト・サービスの提供企業
c. 他機関と連携のため実名PHRを活用する機関
d. 他機関から匿名化PHRを提供を受ける機関
e. 認定匿名加工医療情報作成事業者

［GDPRでの仮名化］公共の利益における保管目的、科学的若しくは歴史的研究の目的又は統計目的のために<u>さらなる取扱い</u>

個人健康情報の蓄積とビッグデータ分析



注：PHR：Personal Health Record

厚生労働省が進めているPHR(2020年目標)

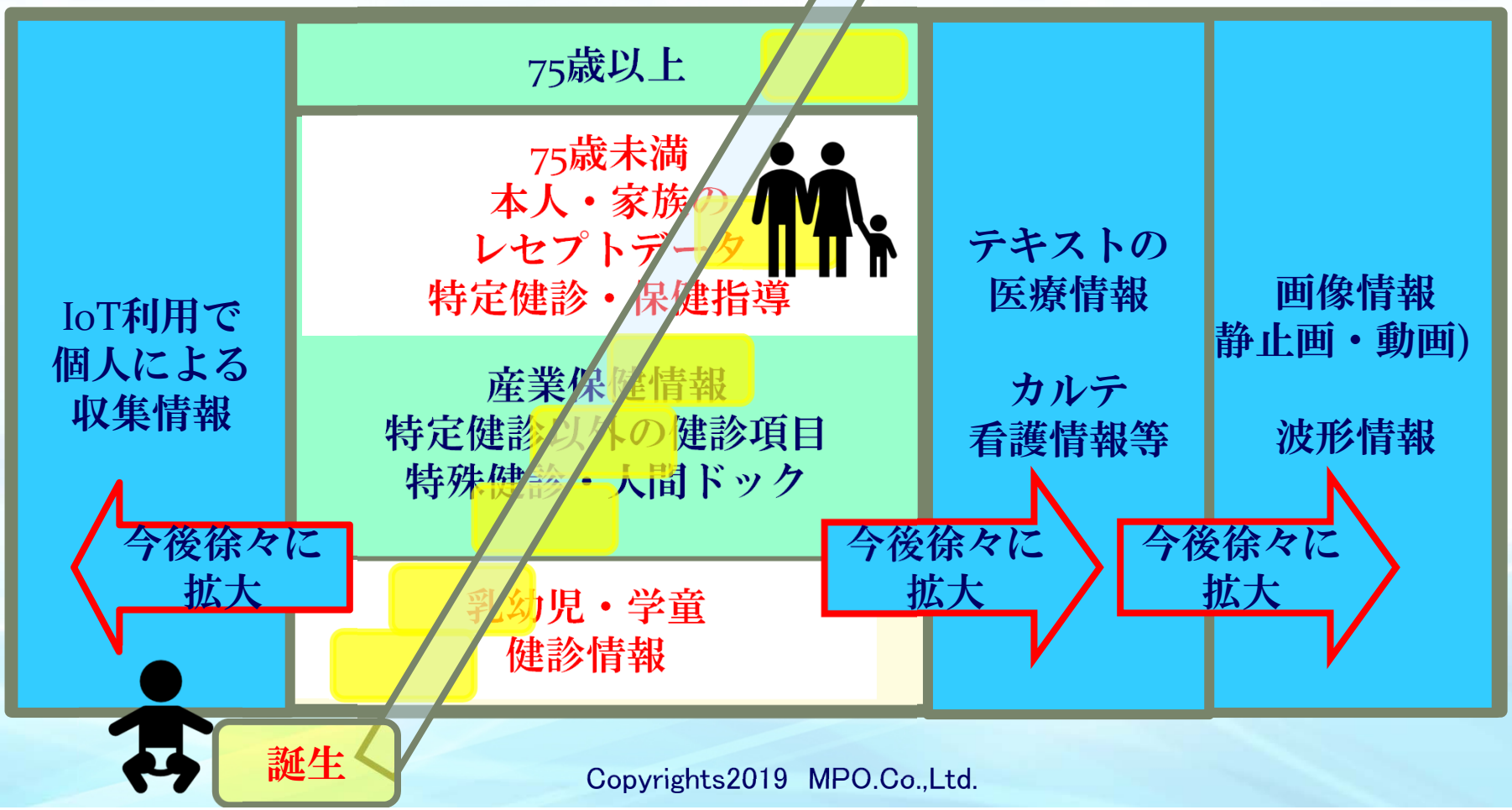
白地の部分は国が管理

緑地の部分はScope外

今後徐々に拡大

死亡

入学➡卒業➡入社➡結婚➡異動➡転職➡退職➡介護　によりデータ発生元が変化



トータルPHRの技術的仕組み（試案）

1. PHR協会は、PHRの実用化により「個人の健康・医療・介護データなどを総合的に管理し、経時的に参照することにより、個人の健康増進や疾病の予防・管理・治療などを通して、個人の健康増進を図る」ことを目指している。

   A) 実名・匿名化のPHRがそのまま連携・蓄積することが望まれる。

   B) EU―GDPRの要求事項のPortability原則にも該当。

2. 現状のPHR的実証実験は特定範囲の患者・住民・従業員の健康情報を蓄積

   A) 特定範囲の機関・組織の連携により、「その範囲の医療の効率化」

   B) 個人健康情報DB化により「特定医学研究の有効性検証」のレベル

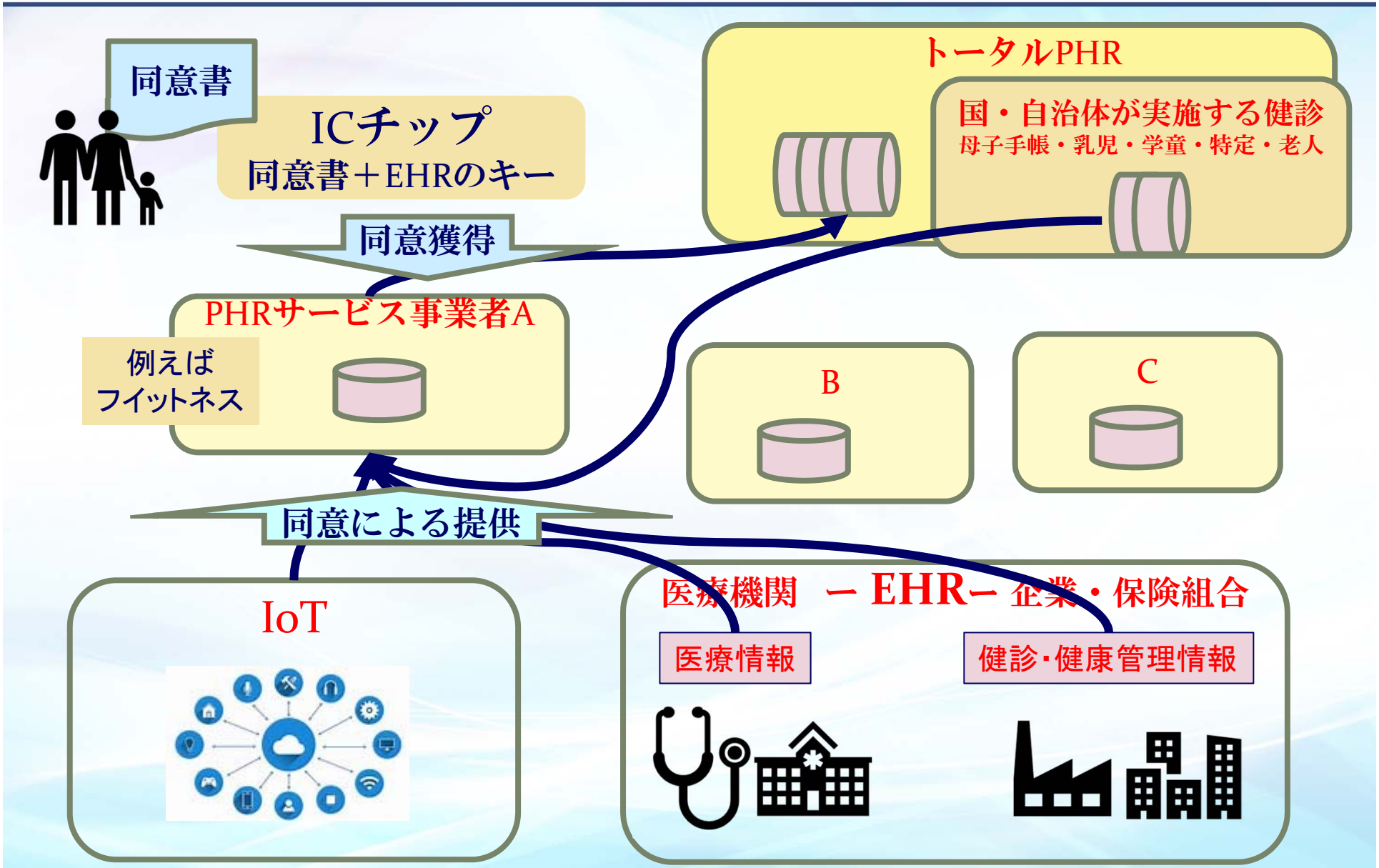
3. PHR化と本人同意を獲得した組織が、PHR活用権を有する（技術的・社会的）仕組の構築が喫緊の課題

   参考資料P14参照

   A) 個人健康情報を、逐次的（発生順）に蓄積、必要に応じて匿名化

   B) このデータベース活用の本人同意を獲得（又は「法的に許可」される）

PHR―EHR連携図（討論用）



2.法的/社会的動向
―特に匿名化とプライバシ評価―

準備された
技術と法制度は十分か？
その活用をためらわせるもの

2-1.　匿名加工情報について

匿名加工情報を企画し利用するのは誰か？

4種類の「匿名加工情報」用語

匿名加工

1. 個人情報保護法下

a. 個人情報保護法:「匿名加工情報」は個人情報保護委員会が認定

b. (行政・独法)個人情報保護法:「非識別加工情報」も同義。運用が異なる

2. 次世代医療基盤法下(匿名加工医療情報)

① 認定事業者を内閣官房医療戦略室が認定 (個人情報保護委員会ではない)

a. 基本方針等では「主務大臣(経産・厚労・文科)が認める」とある。

b. 認定事業者申請中。

② 次世代医療基盤法の基本方針:「4 法第8条第1項及び法第28 条 (3)」

a. 医療情報等及び匿名加工医療情報の適正な取扱いに関して
主務大臣(厚労、文科、経産)、個人情報保護委員会
及び総務大臣(大学法人等の担当?)は相互に緊密に連絡・協力(法第 38 条)

b. 主務大臣の権限
認定匿名加工医療情報作成事業者、及び認定医療情報等取扱受託事業者 へ
a. 立入検査等(法第 35 条)、 b. 是正命令(法第 37 条)
認定の取消等必要な措置を講ずる。(法第 38条)

3. 医学研究倫理指針下

経緯から見て、各組織の倫理委員会が認める、、、
→ これまでの匿名化と実質変わらない?

次世代医療基盤法における事業者種別と取扱情報・安全管理義務

匿名加工

➢安全管理義務

①医療情報取扱事業者

医療情報

➢安全管理義務
➢再識別禁止義務

②認定匿名加工医療情報作成事業者

➢安全管理義務
➢再識別禁止義務
➢認定医療情報等取扱受託事業者に限り、匿名加工医療情報の取扱いの全部又は一部を委託可能。

認定医療情報等取扱受託事業者

匿名加工医療情報

➢(若干の)安全管理義務
➢再識別禁止義務

③匿名加工医療情報取扱事業者

4種類の匿名加工情報

匿名加工

	本人の再度の同意なくして提供可能な匿名化［依拠する規範］	匿名加工の企画決定者	匿名加工情報の加工レベルの認定及び、オプトアウトの届け出先	要配慮個人情報の取得時の利用目的の取扱い等
個人情報保護法	匿名加工情報 ［個人情報保護ガイドライン（匿名加工情報編）］ 識別行為の禁止義務	個人データを保有する事業者自身	個人情報保護委員会	・要配慮個人情報の取得時の利用目的への「明示的」同意は必要 ・匿名加工化及びそれ以降の提供（提供後の利用目的）への同意は、オプトアウトで可
独法個人情報保護法	非識別加工情報 ［独法個人情報保護ガイドライン(非識別加工情報編)］ 識別行為の禁止義務なし	・独法への提案者（開示された保有個人情報から提案） ・個人情報を保有する独法自身	個人情報保護委員会	
次世代医療基盤法	匿名加工医療情報 ［次世代医療基盤法・ガイドライン］	①医療情報取扱事業者 ②認定匿名加工医療情報作成事業者 ③匿名加工医療情報取扱事業者	内閣官房 健康医療政策室	
医学研究倫理指針	匿名加工情報 ［医学研究倫理指針及びガイダンス］	・医学研究を行うことを倫理委員会に認められた団体・個人 ・科研費等を獲得した個人・団体	各大学病院等の倫理委員会	

注：英訳　仮名化：psudonymous
匿名化：anonymous

匿名加工情報と非識別加工情報の比較

匿名加工

非識別加工情報	匿名加工情報
行政・独法改正個人情報保護法	改正個人情報保護法
照合禁止義務がない	照合禁止義務がある
→　個人情報	→　非個人情報
個人情報ファイル簿への 掲載が必須。	開示の必要性なし

「個人情報保護法の逐条解説」よりまとめ
(第5版）　宇賀克也

2-2. ISO/IEC29134による
プライバシー影響評価（PIA）の役割

PIAを活用しPHR利用者本人等に
共感を得るための活動

ISO/IEC29134(PIA)の位置づけ

PHRの実用化を図るうえで、PbD／PIAの理解に、極めて広い分野の理解が必要

☆ 我が国の個人情報保護法関連	個人情報保護法、次世代医療基盤法 個人情報保護４ガイドライン、 労働安全衛生法、 医学研究の倫理指針/ガイダンス
☆ GDPRと関連理念及びISO等	GDPR 特に、25条・35条・40条 PbDの理念、 ISO/IEC29134 （PIA） ISO/IEC29100(フレームワーク)
☆ わが国の保健医療分野における個人情報保護関連の規範	医療・介護ガイダンス等、 保健医療分野の個人情報保護規範 安全管理ガイドライン（厚労省） ASP/SaaS医療情報ガイドライン(総務省) 医療情報受託管理ガイドライン(経産省)
☆ ISMS及びPマーク等、マネジメントシステムに関連する規範	ISO/IEC27000、27001、27002、 27005（旧 Guide 73） 27017、27018 ISO27799 ISO31000 等、 JISQ15001(本文・付属書A)、

これら規範に関連する用語の定義及び翻訳に関する検討（整合性）が不十分。

個人情報、個人データ、匿名化、PII Principal、機微な個人情報、リスク評価、リスクマネジメント 等々

PIAに至る歴史

OECD	1980 OECD-GL　　2013 OECD-GL改訂
EU	1995 EU指令　　2018/5 GDPR施行 2008 ISO22307 PIA(金融) 2017 ISO/IEC29134 PIA(一般) プライバシー影響評価-GL 2011 ISO29100 個人情報保護フレームワーク
日本	2005 個人情報保護法施行　　2017/5 改正個人情報保護法施行 2016 マイナンバー法施行(PIA実施) 1998 Pマーク制度開始 1999 JISQ15001制定　　2017/12 JISQ15001改正 2003 ISMS認証制度発足　　2013 ISO/IEC27001 ISMS要求事項改正

3. GDPR(General Data Protection Regulation)

EUの個人情報保護規則

GDPRで重要なPbD/PIA

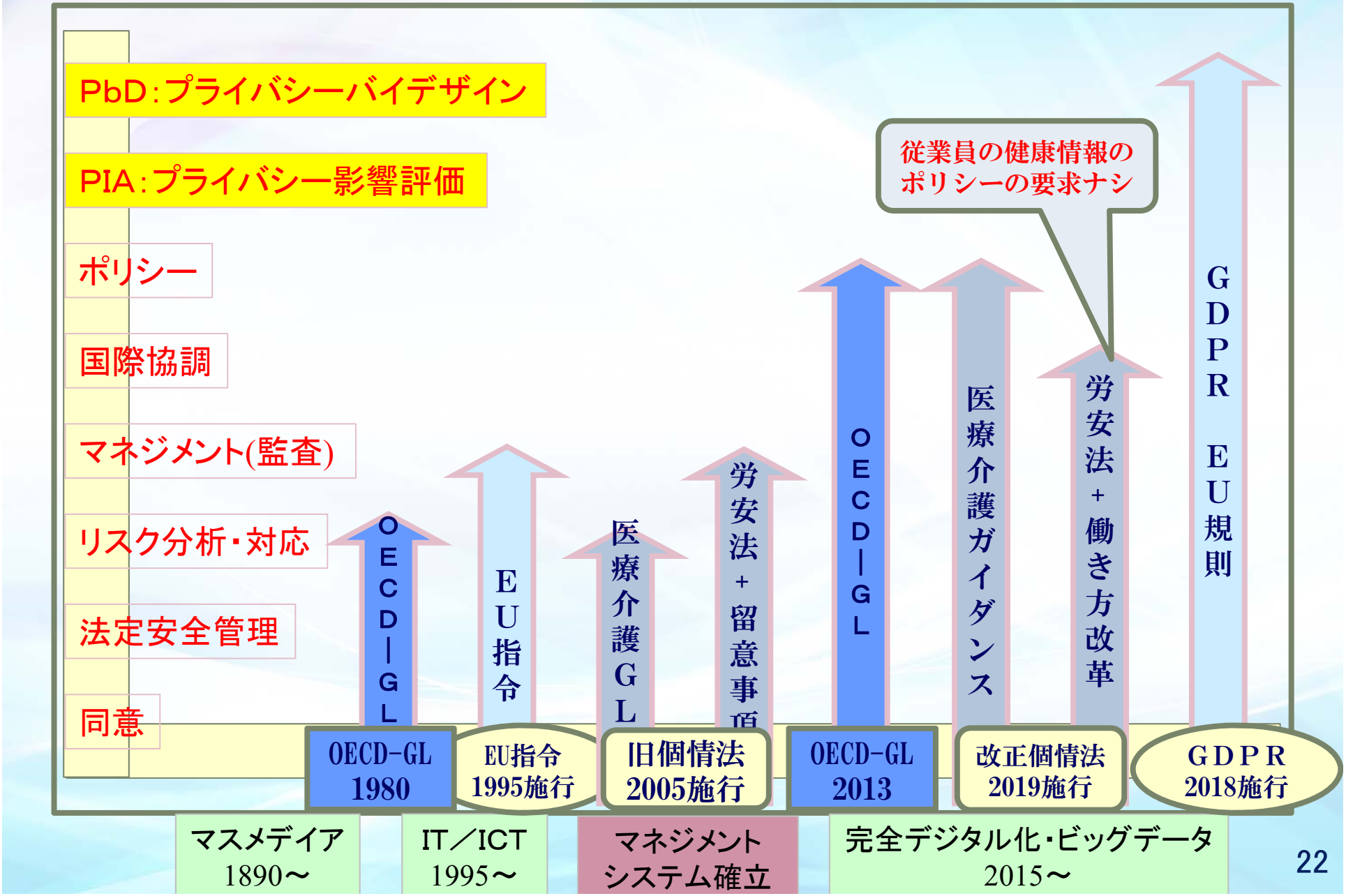
GDPRのプライバシー保護のポイント

1. EU-規則における個人情報の定義・取扱い（第1章～第2章）
   （1）データ主体の権利（第１章・第2章　第12条～22条）
   個人情報の取扱いに関する法制（方針・取得・利用・提供・開示/苦情の受付等）
   （2）第3節（個人データの）訂正及び消去　（EUで特徴的な権利）
   - Right to be forgotten(第17条)　　Right to data portability(第20条)
   - Right to object Automated individual decision-making, including profiling(第21・22条)

   （3）管理者及び処理者　の責任（第4章第 24条）
2. 設計時からの及びデフォルトでのデータ保護(PbD)（第 25条 ）
3. EU域 内に拠点のない 管理者取扱者の代理人（第 27条 ）
4. 個人データ取扱いの安全管理（第2節　第 32条）
5. データ主体への個人データ侵害通知（第 34条）
6. プライバシー影響評価（第3節　第35条）　参照：ISO/IEC 29134 – Privacy Impact Assessment
7. データ保護オフイサーの指名（第4節　第37条）
8. 行動規範（第5節　第 40条 ）　⇒　法制化による規範と認証
   参照：　ISO/IEC29100　Privacy　Framework
9. 研究等における個人情報の取扱い（第9章 第 89条）
   公共の利益における保管目的、科学的若しくは歴史的研究の目的
   又は統計目的の ための取扱いに関する保護措置及び例外

OECD/GDPR/医療介護GS/産業保健(高プロ)指針の比較

概観



3-1.PbDの設計思想

第4節　第 25条 ：設計時からのデフォルトでのデータ保護

GDPR　第25条　PbD　―プライバシー保護の根本思想―

➢ 設計時からのデフォルト(初期設定状態)での個人データ保護

1．最新性・実装コスト・運用範囲・運用状況・運用目的と同様に、
人の生命・自由及び幸福追求の権利に対するリスク発生可能性(likelihood)及びその重大性を考慮する。

2．管理者(controller)は適切な技術的及び制度的設計(仮名化psudomysation等)により、効果的且つ必要な措置で統合的にデータを保護(データ最小化等)し、本EU規則に準拠しデータ本人の権利を保護しなければならない。

デフォルトでの義務

a.**技術的及び制度設計により、** 業務目的に特定して必要な個人データのみ取扱うことを保証。収集された全個人データ、取扱い範囲、保存期間、及びアクセス可能性に適用

b.不特定多数の人物が、PII本人の許可なしに個人データにアクセス不可

3．第42条記載の「EU認証機構」により、本25条規程の要求事項に順守していることを証明できる。

注：PII本人：Personally Indentifiable Information Principal

GDPR　第25条　をMPOが翻訳・まとめ

プライバシー・バイ・デザイン（PbD）

原則1　事後的でなく事前的、救済的でなく予防的であること

- プライバシー上のリスクが発生する前に解決するための救済策を提供する。

原則2　初期設定でプライバシー保護が有効化される事

- 個人データは個人が何もしなくてもそのまま保護される。

原則3　プライバシー保護の仕組みがシステムの構造に組み込まれる

- プライバシー保護の仕組みが構成要素の不可欠な、中心的な機能となる。

原則4　全機能的であること。ゼロサムではなくポジティブサム

- すべての正当な利益及び目標を収める、ポジティブサムアプローチを目指す。

原則5　ライフサイクル全般にわたって保護されること

- すべての データは、データライフサイクル管理のもとに安全に保持され、プロセスの終了時には確実に廃棄される。

原則6　プライバシー保護の仕組みと運用は可視化され透明性が確保されること

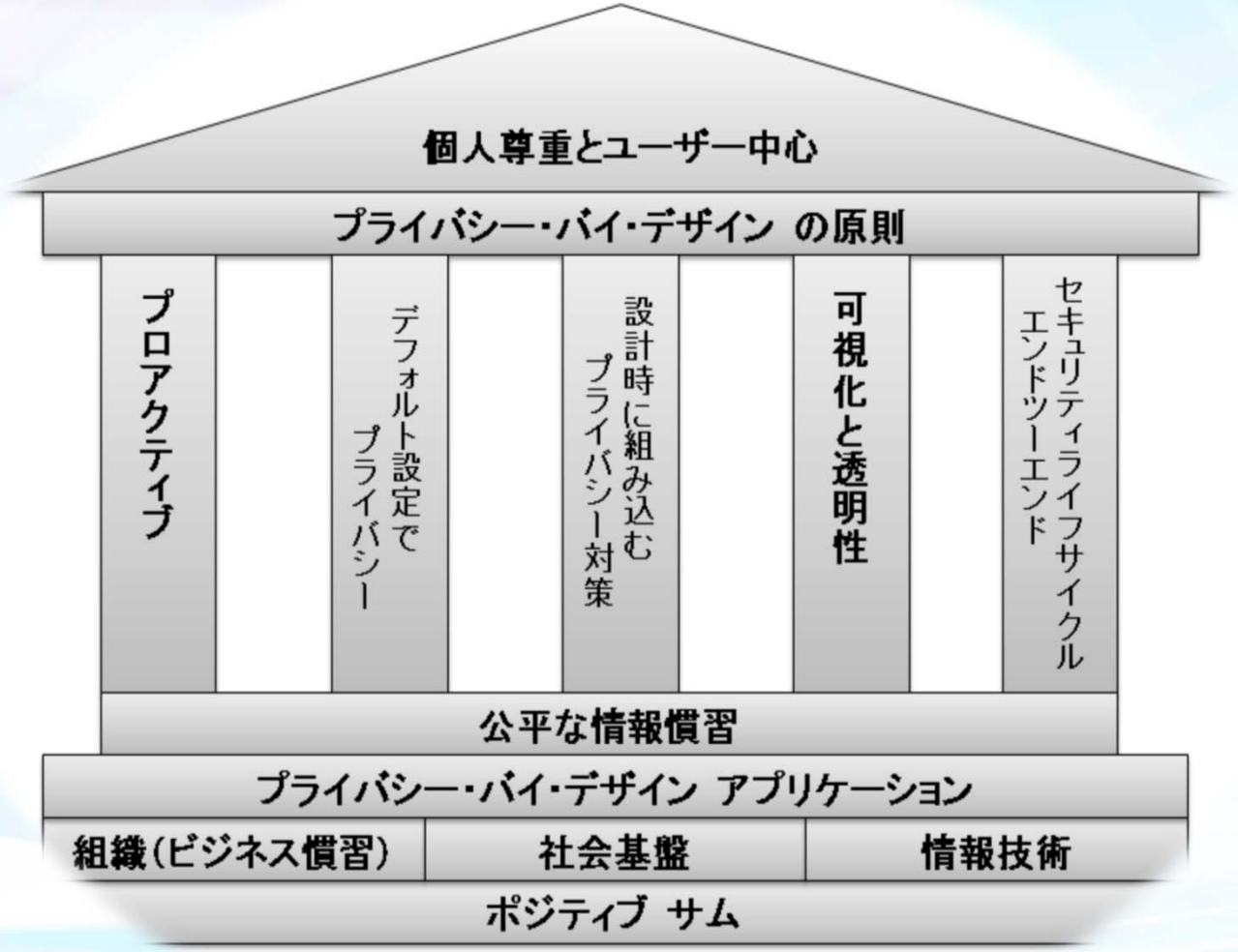
- どのようなビジネス慣行または技術が関係しようとも、システムの構成及び機能は利用者及び　提供者に可視化され、検証できるようにする。

原則7　利用者のプライバシーを最大限に尊重すること

- 設計者及び管理者に対し、プライバシー保護を実現するための強力かつ標準的な手段と適切な通知及び権限付与を簡単に実現できるオプション手段を提供する。

Dr.Ann Cavoukian
オンタリオ州情報・プライバシーコミッショナー

PII本人の権利とPrivacy by Design(PbD)



Privacy by Designのコンセプト

EUで特徴的な権利（第3節 訂正及び消去）

1. 忘れられる権利、削除を求める権利（第17条）

Right to be forgotten

- 本人に関する情報の消去を求める権利を有する。特に、子ども（18歳未満）のときに掲載した情報についてこの権利が認められる。

例、子どものときに安易にSNSに載せた情報のために、就職のときに不利益を被る
容疑者として逮捕されたが無罪判決の場合に、逮捕されたことがGoogleに残る。

2. データ・ポータビリティの権利（第20条）

Right to data portability

- 自己のデータをある事業者から受け取り、別の事業者に移行することができる。

例、あるSNSから他のSNSへのデータ移行が容易。

3. プロファイリングに基づく評価を拒む権利（第22条）

Right to object Automated individual decision-making, including profiling

- 法的影響もしくは重大な影響をあたえる評価で、
①人に関する個人的側面を評価したり、
②その人の労働能力や経済状態、位置、健康、嗜好、信頼性または行動を分析・予想することを意図した、自動処理のみに基づく評価について、例外的を除き、その対象になることを拒む権利を有する。

個人データの取り扱いに関わる個人の保護及び当該データの自由な移動に関する 欧州議会及び理事会の規則
2016年4月14日EU議会可決 2018年5月施行

3－2.プライバシー影響評価(PIA)

第3節　第35条　データ保護影響評価

参照：ISO/IEC 29134/2017- Privacy Impact Assessment

注：GDPRでの記述は「should」(~するべきである)表現であり、
「shall」(～しなければならない)ではない。

PIA（プライバシー影響評価）の意義

PbD達成のために、PIAを実施する

①計画的なプライバシー対策の達成と相対的なコスト削減

・構築する業務システムのプライバシー保護への仕様変更を促す。
・稼働前の対策で、プライバシー問題発覚による停止や、
ビジネスリスク・システム上の対策費用の軽減を図る。

②利害関係者間の信頼構築

③個人情報保護における善管注意義務の達成（Due Diligence）

1. PIA報告書の作成利害関係者の信頼獲得
2. プライバシーや個人情報の取り扱いに関して実施組織・個人など、
利害関係者間で議論する共通の土俵を提供。
3. 組織が個人権利保護への努力姿勢を利害関係者に示すことができる。

➡ PIAは「リスクコミュニケーション」

ISO/IEC29134:2017

PIAの定義

3.7 Privacy Impact Assessment ：PIA

個人特定情報（PII)に関して潜在的プライバシー影響の取り扱いを（実施者が）伝達し・企画するに際して、 組織のより広範なリスクマネジメントの枠組みを組み立てるために、特定し、分析し、評価し、コンサルティングするための、全般的手続き。

overall process of identifying, analyzing, evaluating, consulting communicating and planning the treatment of potential privacy impacts with regard to the proceeding of personally identifiable information, framed within an organization's broader risk management framework.

Note 1 to entry : Adapter from ISO/IEC 29100:2011 2.20

ISO/IEC 29100では、privacy risk assessment と呼称し、
「PIIの処理に関するリスク特定、リスク分析、リスク評価のプロセス全体」とする

ISO/IEC29134

PIA評価の実施：5章～6章（1）

5章. PIA分析の準備

5.1 PIA実施の利益、 5.2 PIA報告の目的、 5.3 PIA実施の責任、 5.4 PIAの規模

6章. PIAの実施手順

6.1 はじめに：

6.2 予備分析：PIAの必要性についてのしきい値の決定

6.3 PIAの準備：

- ・PIAチームの立ち上げと方向付けの決定、
- ・PIA計画の準備と実施のための資源の決定
- ・評価内容の記述
- ・利害関係者との契約

6.4 PIAの実施：

- ・PIIの情報の流れの特定
- ・ユースケースの実施の分析
- ・適切なプライバシー安全対策要件の決定
- ・プライバシーリスクの評価
- ・プライバシーリスクの改善の準備

6.5 PIAのフォローアップ

- ・報告書の準備
- ・発行
- ・プライバシーリスク改善計画の実施
- ・PIAの見直しと監査
- ・プロセスへの変更の反映

参照 ISO/IEC29100 4.5
プライバシー安全対策要件

「6.4.4 PIAの評価」項のNoteは
全体として、PbDを目指す。

「基本的権利」の未実施か、実施が不適切な可能性は
チェック後の改善しかできないということである。
実際、基本的権利を実施しない選択肢は
あってはならない。

PIA評価の実施：PIA報告書　7章

利害関係者（特に、利用者）にPIAで理解させるものは

7章　PIA報告書の要件

- 7.1　はじめに、
- 7.2　レポート構成、
- 7.3　PIAの範囲、
- 7.4　プライバシー要求事項、
- 7.5　リスクアセスメント、
- 7.6　リスク対応計画、
- 7.7　結論と決定、
- 7.8　PIAパブリックサマリー

Likelihood！

6.4.4.1 プライバシーリスクの特定

PbD：「基本的な権利」を実施しなかったり、十分実施しなかったりする可能性があるならば、**チェックされてからしか改善することしかできない。**
実際、これらの基本的権利を実行しない選択肢はあってはならない。

プライバシーリスクの例

- PIIへの無許可の
  - アクセス（機密性の喪失）、修正（完全性の喪失）；
- PIIの
  - 逸失、盗難、または無許可での削除（可用性の喪失）
  - 過度な収集（業務管理の喪失）；
  - 無許可のまたは不適当なリンク；
  - 処理目的の情報が不十分（透明性の不足）；
  - 不必要に長期間の保持
- PII本人の認識または同意なしで
  - 権利に配慮することに関する失敗(例：アクセス権の喪失)；
  - PIIの処理（関連する法律または規制がないのに)；
  - PIIを第三者と共有または異なる目的での利用；

6.4.4.2 プライバシーリスクの分析

下記の各リスクについて特定。
- likelihoodの最も高いリスク源；
- likelihoodが最もありそうな脅威；
- **PII本人のプライバシーに対する最も深刻な影響**
- リスク所有者
- 既存の管理策と対処することで役立つリスク。

システムリスク分析の手順

- 使用する基準の定義：
  プライバシーへの影響を判断するため
- ISO/IEC29134の付属書A
  ＆　組織で別々に定義しても可
- プライバシーリスク分析の成果は
  ➡　PIA報告書で文書化
- 影響度評価は
  ➡　ISMSのリスクマネジメント手法を援用

保健医療分野におけるPIAの実施（案）

1. 脅威の特定
   a. 一般分野の脅威　　ISO/IEC27005 AnnexC
   b. PIAの脅威　　ISO/IEC29134 AnnexB
   c. 保健医療分野の脅威 ISO27799　AnnexA
2. 安全管理措置の特定
   a. ISO/IEC27002　　一般分野の管理策
   b. ISO27799　　保健医療分野特有の管理策
   c. ISO/IEC29134　　プライバシー分野特有の管理策
3. PIIの情報の流れの特定
   ➡ システムリスク分析
4. ユースケースの実施の分析
   ➡ 業務フローリスク分析
5. 適切なプライバシー安全対策要件の決定
6. プライバシーリスクの評価
7. プライバシーリスクの改善の準備

PHRにクラウド無しでは考えられないので、ISO/IEC27017,27018. . .

PIIの性質に基づく影響レベルの例

likelihood

PIIの性質	例	影響レベル
個人特定情報（PII）の本人は、影響されないか、少しばかりの不便に出くわし、それらは全く問題もなく、克服するであろう。 (情報の再入力時間、煩さ、イライラを要した。)。 **公にアクセス可能なPII**	電話帳、アドレス帳、選択リスト　など	1
PII本人は、少し問題はあるが、重要な不便を克服できる。 （追加費用、ビジネスサービスへのアクセス拒否、恐怖、理解不足、ストレス、いささかの身体的疾患　など） 法的なアクセス権を必要とするPII	制限付き公開ファイルまたは 配布リストのメンバー	2
PII本人は、重要な結果に遭遇するかもしれない。その結果、彼らは重大な困難を克服できる可能性はある。 （銀行がブラックリストに掲載している不当支出、物的損害、雇用の損失、逮捕状、健康状態の悪化　など） **許可のない開示がPII本人の評判に影響を与える可能性があるPII**	収入、社会福祉給付、固定資産税、または罰金に関する情報	3
PIIの本人が重大な、もしくは、不可逆的な結果にさえ 遭遇する可能性があり、打ち勝つことができないかもしれない。 (返済不能な借金または働けないなどの、財政的苦痛、長期で、心理学的な、または身体の疾患、死　など)。 無許可の開示、変更、紛失、または破壊がPII本人の存在または健康、自由、および生活に影響を与える可能性があるPII	機関への関与、文章、要員の見直し、健康データ、サービス不能の債務、または PII本人は、刑事事件で被害者になる危険がある	4

注：PII：Personal Identify Information、
PII本人：PII principal

ISO/IEC29134　Annex A　表A.I

likelihoodの測定の仕方

likelihood

支援資産とそれらを活用するためのリスク源の能力

（スキルの利用可能な時間、財源、情報システムとの近接度、やる気、免責感など）。その他に、換言すれば、脅威を実行するために支援資産の特性がどの程度、利用される可能性があるのか？

影響レベル	PIIの性質	例
1）無視	補助資産の特性を悪用して脅威を実行することは表示されない。選択されたリスク源	保護された部屋に保管された紙文書の盗難にバッジリーダーとアクセスコード
2）限定的	支援資産の特性を悪用して脅威を実行することは、選択されたリスクの発生源にとっては困難	バッジリーダーにより、保護された部屋に保管された紙・文書の盗難
3）重要	補助資産の特性を悪用することによって脅威を実行することは、選択されたリスクの発生源	最初に受付でチェックインせずにアクセスしたオフィスに、保管された紙の文書の盗難などの可能性 。
4）最大	補助資産の特性を悪用して脅威を実行することは、選択されたリスクの発生源にとって非常に簡単	ロビーに保管された紙の文書の盗難など。

脅威に最も一致するレベルの値が選択される。この起こりやすさ(likelihood)は、追加の要因を含めることによって修正することができる。インターネットへのアクセス、外国のサイトとのデータ交換、他の情報システムとの相互接続　等

注：起こりやすさ：likelihood

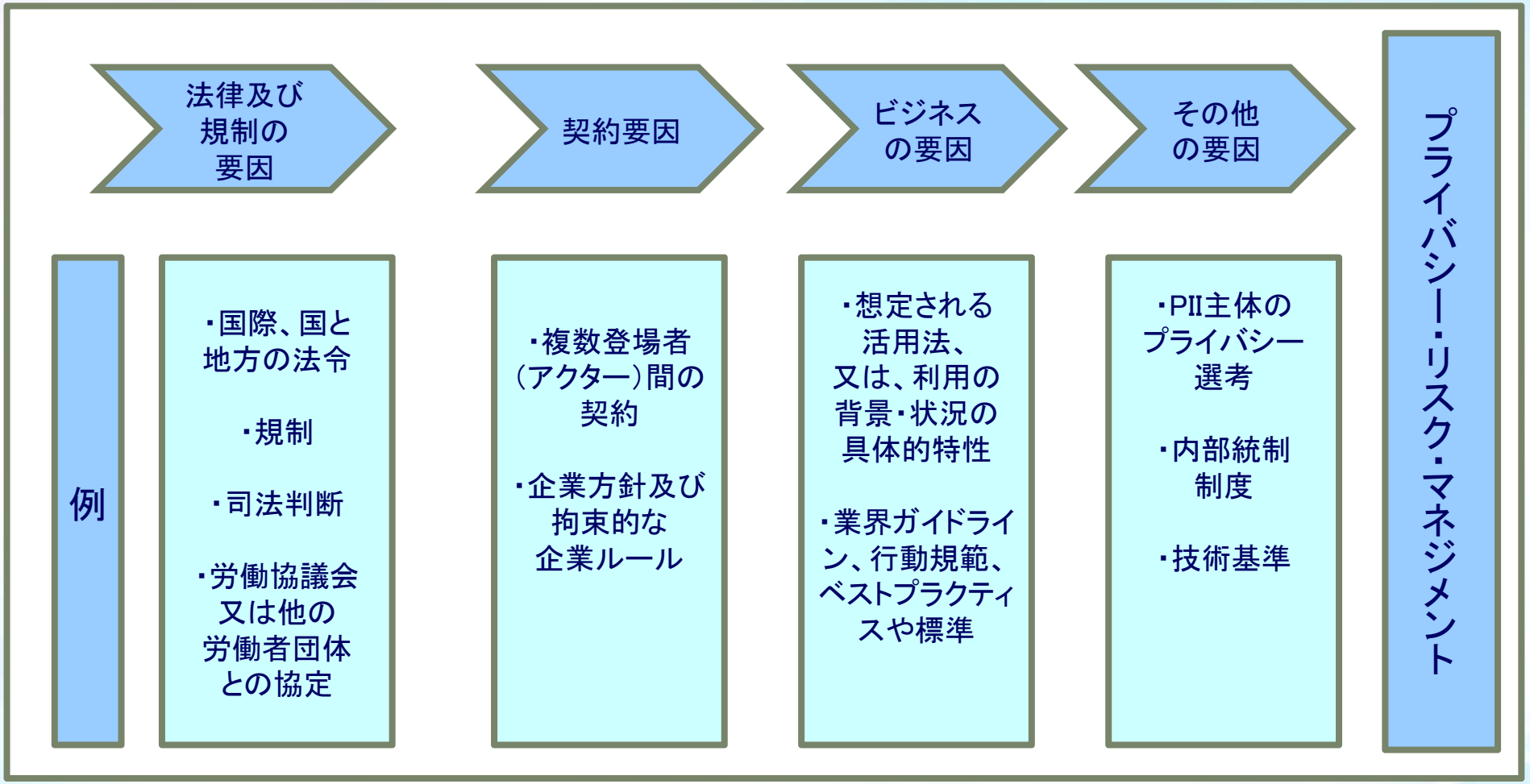
ISO/IEC29134　Annex A　A.3

4-3. 行動規範（第5節　第 40条 ）
⇒　法制化による規制と認証

参照：　ISO/IEC29100　Privacy　Framework

おおむね、ISMSのリスクマネジメント　ISO/IEC27005 を援用

Factors influencing privacy risk management
プライバシーリスクマネジメントに影響を与える要因



(ISO/IEC29134　6.4.3　参照)ではプライバシー評価項目の作成において、
「ISO29100の　4.5　安全対策要件」の記述を参照

ISO/IEC29100:
JISX9250　4.5より

ISO / IEC 29100のプライバシー原則

1. 同意と選択
2. 目的の正当性と仕様
3. コレクションの制限
4. データの最小化
5. 使用、保存および開示の制限
6. 精度と品質
7. 開放性、透明性と予告
8. 個々の参加とアクセス
9. 説明責任
10. 情報セキュリティー
11. プライバシーコンプライアンス

ISO/IEC29100：2011　5.1
（JISX9250：2017）より

PHRの早期立ち上げを目指して

1. PHRの収集・蓄積とその活用が個人の健康管理・疾病管理に極めて有意義であることは大方の一致するところであるが、その革新性ゆえに、システムの有用性とともにプライバシー保護の有効性評価について、十分な議論がなされないまま、長い年月が流れている。
2. 個人健康情報をふんだんに駆使した革新的システムの早期立ち上げには、プライバシー対策のもっともらしさ：Likelihoodの評価に客観性が得にくいゆえに、国民のコンセンサス獲得に多くの年月を要するし、実際、かかってきた。
3. EUのGDPRでは、PbDの達成のために、プライバシーフレームワークに適合したPIA（Privacy Impact Assessment)を行い、国や第三者機関にその適切性を評価されたシステム開発と運用が求められている。
4. 革新的なPHRシステムの総合システムも、PbDの思想にのっとり、事前にPIAを行い、その方針に基づいた開発と保守・運用を行うことは当然望まれる。
5. ISO/IEC29134に適合したリスク分析を援用し、近年発展を遂げている統計学による客観的評価値（例えば、Likelihood）を一つの前提とした民意の獲得が、普及促進の一つの解決策と考えられる。
6. 近年、国からもPHRの創設による健康管理が「データヘルス改革」などにより、推進されつつあるが、それら国の施策も念頭に置きつつ、実績面や将来性を含み、引き続き議論を進める。

ご清聴ありがとうございました

URL: www.m-p-o.co.jp
Email: info@m-p-o.co.jp
TEL&FAX: 045-517-3246