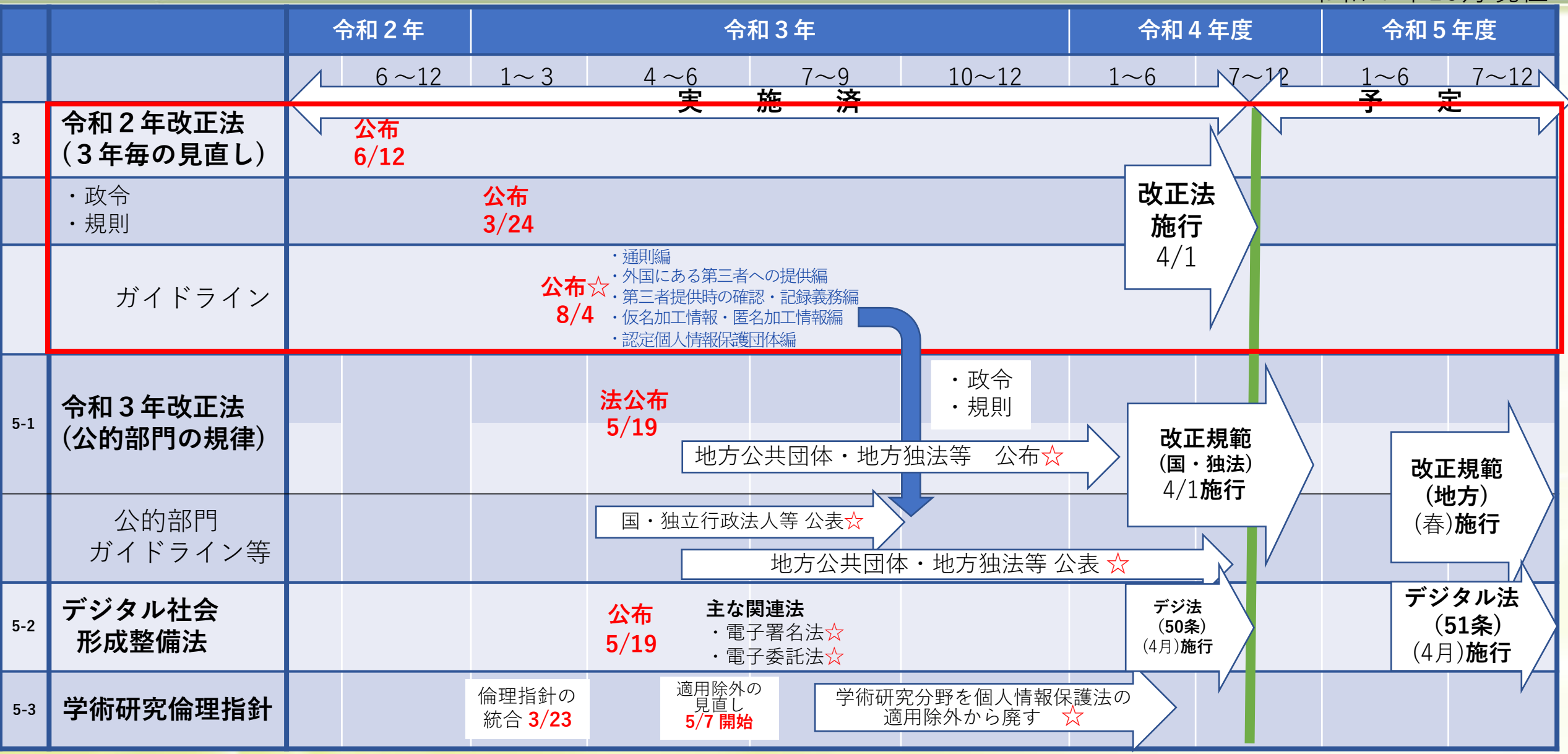
PHR連携による保健医療介護連携の実現への提案
個人情報保護と情報ネットワークの機能

令和４年11月17日

一般社団法人PHR協会
理事　森口修逸

1．改正個人情報保護法の施行ロードマップ

令和４年10月現在



人情報保護委員会：関係資料令和3年5月7日　などからMPOが編集　**赤太字**は☆規範の施行日

2. 改定個人情報保護法の公布とインパクト

個人情報保護法は、2005年に全面施行され、2017年の大改正を経て、

a. 自身の個人情報に対する意識の高まり、
b. 技術革新を踏まえた保護と利活用のバランス、
c. 越境データの流通増大に伴う新たなリスクへの対応等

の観点から**2020年6月に定例の改定を公布、2022年4月に施行**

1	**個人の権利の在り方**	
	◎ 保有個人**データ開示のデジタル化推進**：やがて、データポータビリテイへの対応 ➡ 本人が、開示方法を指示できる、電磁的記録の提供を含む（改正法２８条１項） ◎ **第三者提供記録の開示**の義務化 ➡ 保有状況に問題なくとも、いつでも、開示請求が可能（改正法２８条５項）	
2	事業者の守るべき責務の在り方	漏洩時の本人通知、不正利用の禁止 （改正法２２条２項）
3	事業者における自主的な取組の推進	保有個人情報等の公表事項の追加(改正法２７条)
4	**データ利活用に関する施策の在り方**	**仮名加工情報の新設(改正法３５条)、第三者提供の制限等(改正法２６条)**
5	ペナルティの在り方	法人への重科の導入 最大１億円！ （改正法４２条）
6	法の域外適用及び越境移転の在り方	域外適用の範囲拡大とデータ提供制限の強化(改正法２４条)

3. 令和2年改正法の全体像（1）

個人の 権利

1. 利用停止・消去等の請求権

法違反に加え以下の場合　①利用する必要消失、②重大な漏えい等の発生、③本人の権利又は正当な利益が害された

2. 保有個人データの開示方法　紙・電磁的記録の提供手段選択を含め本人が指定可能

3. 第三者提供記録の開示　本人が開示請求可能

4. 短期保存データの開示等対象化

6ヶ月以内に消去する短期保存データも「保有個人デー タ」に　含めることとし、開示・利用停止等の対象

5. オプトアウト規定の強化　オプトアウト の対象外 の明確化

①要配慮個人情報、②不正取得された個人データ、③オプトアウト規定により提供された個人データ

事業者 の責務

6. 漏えい等報告・本人通知の義務化

漏えい等で、個人の権利利益を害するおそれの場合（※）に、委員会への報告及び本人への通知を義務化

（※）a.個人データの性質や漏えい等の態様に着目、b.要配慮個人情報や財産的被害に至るおそれのある情報の漏えい等

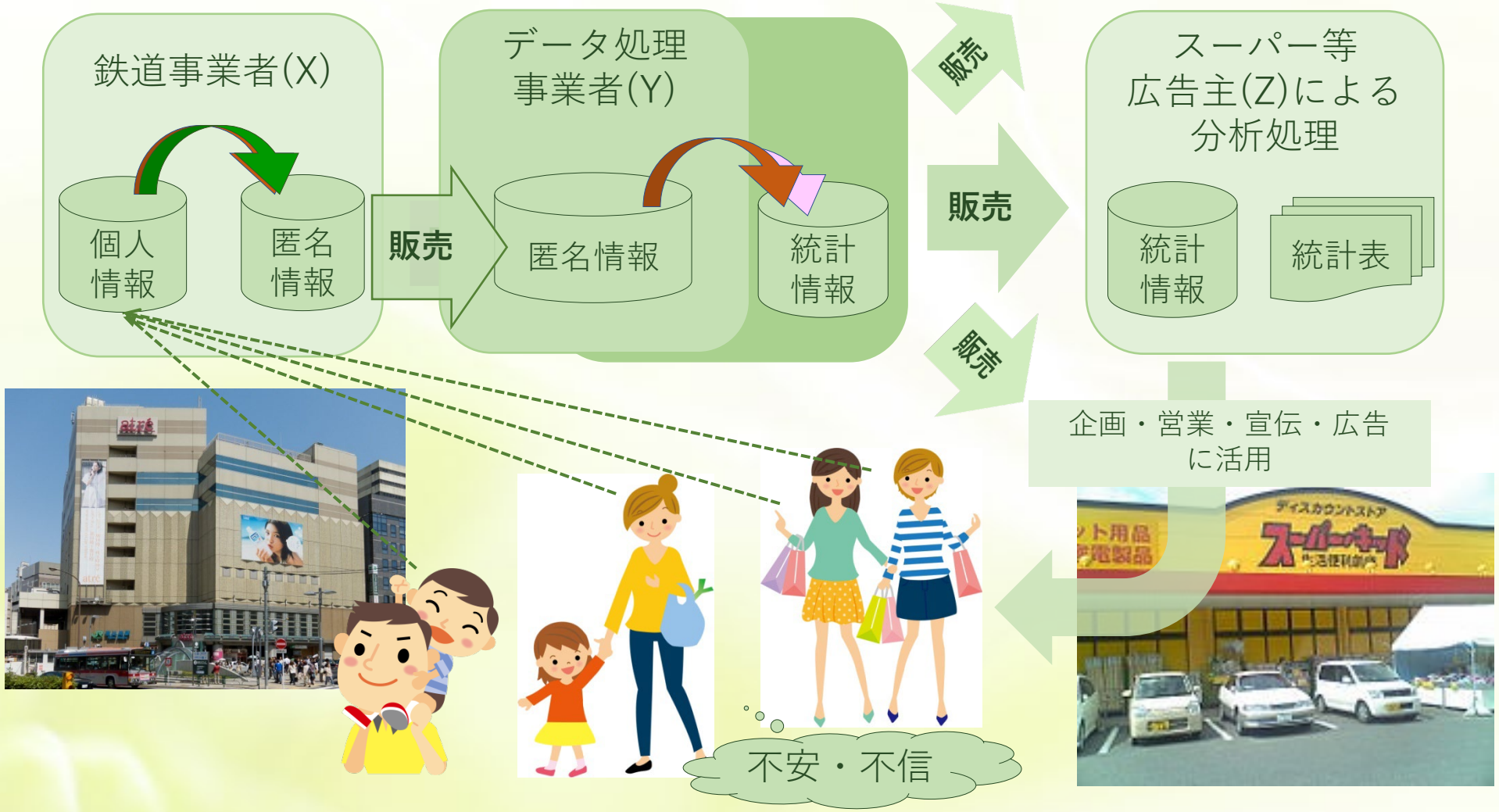
c.不正アクセス による漏えい等（件数の多寡は問わない）、d.安全管理 措置について懸念される一定数以上の大規模漏えい等

7. 「不適正な方法による利用」の禁止

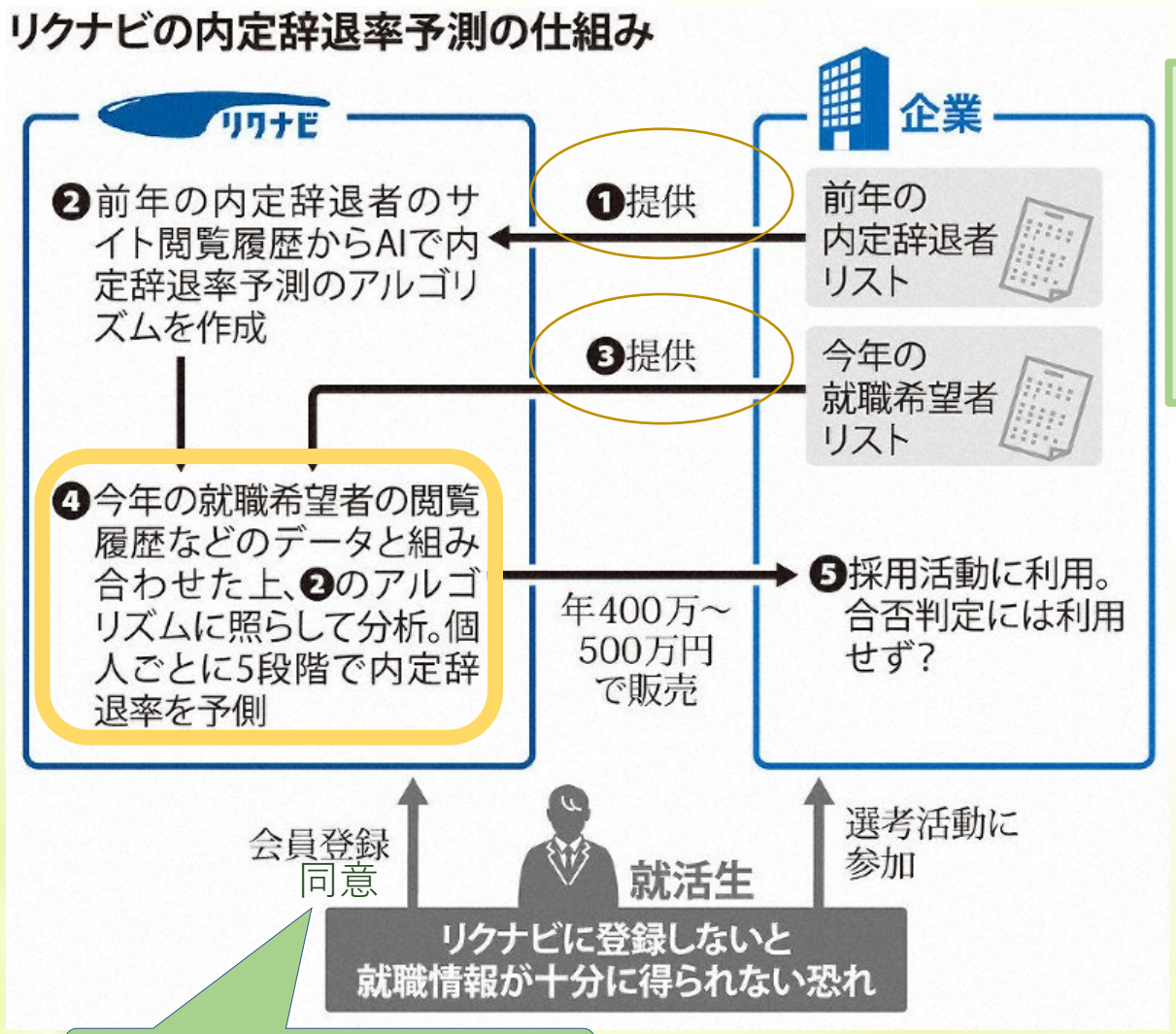
違法又は不当な行為を助長する等　した個人情報の 利用禁止を明確化

3－1. Privacy 2 :個人由来情報を匿名化後、提供し利活用

事業者Xがカード情報から収集した電車の乗降履歴の個人情報を匿名情報に加工後、
事業者Yに情報を提供の事案。事業者は乗客に事前の説明や許可が不要と考えた。



3 - 2. Privacy 3 :同意獲得と「プロファイリング」



真の利用目的の理解は？

ーリクナビ事件の重大性ー

1. どのような「同意」が必要か？
   ➡ 同意の要素・同意の形骸化
2. 個人情報の「提供」にご注意
3. 提供された(情報を買った労務担当）側に問題はないか？

サイト閲覧履歴などのデータを人工知能（ＡＩ）で分析し、個人の志向や能力、信用度を点数化。

プロファイリング

毎日新聞:2019年9月19日

4. 令和2年改正法の全体像（２）

事業者 による 自主的 取組 み

1. 認定個人情報保護団体制度の充実　企業の特定分野（部門）対象の団体を認定可

2. 保有個人データに関する公表事項の追加　保有個人データに関する公表事項の充実

データ 利活用 に関する施策

3. 仮名加工情報の創設

氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する 等を条件に、開示・利用停止請求への対応等の義務を緩和

4. 公益目的に係る例外規定の運用の明確化

利用目的や第三者提供の制限の例外とされる公益目的（生命・身体 の保護、公衆衛生の向上等）について、明確化

5. 個人関連情報　「提供元では個人データに該当しないものの、提供先において個人デ ータとなることが想定される情報」の第三者提供について、本人同意が得られていること等の確認を義務付け

①要配慮個人情報、②不正取得された個人データ、③オプトアウト規定により提供された個人データ

法の域外適用・越境移転

6. 域外適用の範囲の拡大

日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則 によって担保された報告徴収・命令の対象とする

7. 越境移転に係る情報提供の充実

外国所在の第三者への個人データの提供時に、移転先事業者での個人情報の取扱いに関する本人への情報提供の充実等を要求

ペナル ティ

8. ペナルティの引上げ

委員会による命令違反・委員会に対する虚偽報告等の法定刑を引上げ、法人に対する罰金の上限額を引き上げ

4 - 8. 仮名加工情報の検討のポイント（未だに検討中）

1．「仮名化情報の創設」に至る経緯から始まり、　　GDPRからの法制化の意図が記述されている。
　特に、保健医療分野からみた、仮名化の利用方法などに不明の点は多いが、これまでよりは、分かりやすくなってきた。
今後、仮名化について、医療介護のガイダンスなどでどのような具体的な議論ができるか？今のところ不明。
途中経過であるが、第159回個人情報保護委員会（令和２年11月27日）「令和２年11月27日」

2．改正法に関連する政令・規則等の整備に向けた論点について（仮名加工情報）-個人情報保護委員会-（ppc.go.jp）
にも、検討の経過が見えてきた。
①「氏名等を削除した「仮名加工情報」を創設
②内部分析に限定する 等を条件に、
③開示・利用停止請求への対応等の義務を緩和する」ことを前提に、考えられている。
④産業保健分野の扱いとしては、とても都合が良い考え。
　　ただし、学会等、外部への発表には、要注意で、産業保健分野関係者の十分な検討が必要。
要は、以下の事項の検討が必要
① 仮名加工情報を　**作成するための加工基準**
② 仮名加工情報に係る　**削除情報等の安全管理措置の基準**

未だに議論が行われれていない

仮名加工情報の用途がいまいち不明　医療分野では？

次ページ参照

3．氏名や住所等を含まず、氏名等に代わるものとして企業が個人ごとに割り当てているIDと管理されている情報のみが仮名化情報（仮称）ならば、
①　我が国の場合　：個人からの開示請求等に対して、企業が対応しなければならない個人情報の範囲は非常に限定的になる。
②　GDPRにおいて：仮名化情報は安全管理措置の1つとなっているが、 開示請求等に関しては、
　　a．仮名化を自ら行った企業の対応範囲を限定する内容になっていない
　　b．仮名化情報の提供先が、本人からの開示請求等に対応するために（のみ？）機能。

「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」
(P２１以降)

4 - 9.仮名加工情報に係る削除情報等の安全管理措置の基準

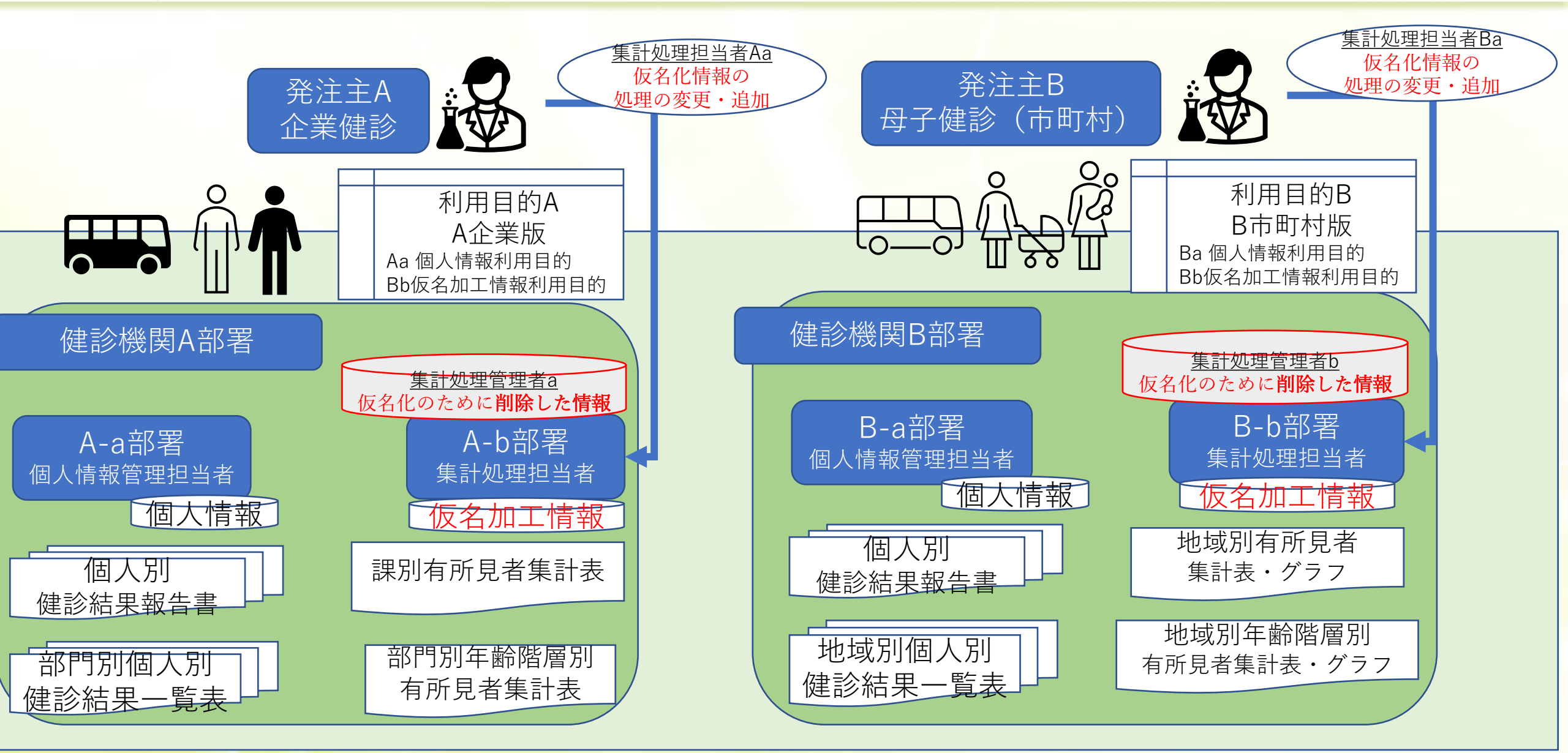
講じなければならない措置の具体例（イメージ）　注：本稿はパブコメ前の情報

- ✓ 削除情報等を取り扱う者の権限及び責任を明確に定めること
- ✓ 削除情報等の取扱いに関する規程類を整備し、当該規程類に従って削除情報等を適 切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を 図るために必要な措置を講ずること
- ✓ 削除情報等を取り扱う正当な権限を有しない者による削除情報等の取扱いを防止

講じなければならない措置	具体例
削除情報等を取り扱う者の権限及び責任の明確化	•削除情報等の安全管理措置を講ずるための組織体制の整備
(ア)削除情報等の取扱いに関する規程類の整備、 (イ)当該規程類に従った適切な取扱い、 (ウ)削除情報等の取扱状況の評価及びその結果の改善を図るための措置の実施	• 削除情報等の取扱いに係る規程等の整備とこれに従った運用・従業員の教育・削除情報等の取扱状況を確認する手段の整備・削除情報等の取扱状況の把握、安全管理措置の評価、見直 し及び改善
正当な権限を有しない者による削除情報等の取扱いを防止に必要・適切な措置	•削除情報等を取り扱う権限を有しない者による閲覧等の防止 • 機器、電子媒体等の盗難等の防止 • 電子媒体等を持ち運ぶ場合の漏えい等の防止 • 削除情報等の削除並びに機器、電子媒体等の廃棄 • 削除情報等へのアクセス制御 • 削除情報等へのアクセス者の識別と認証 • 外部からの不正アクセス等の防止 • 情報システムの使用に伴う削除情報等の漏えい等の防止

4-10. 健診機関の仮名化処理の事例

（委託元から仮名加工情報の処理も含めて受注）



4-11-1.産業保健分野における仮名加工情報活用（論文による整理１）

「**仮名加工情報**」**の提供**に関して、
- a．**委託、事業継承、共同利用の場合**は提供先の事業者と一体として取り扱うことに合理性があり**第三者には該当しない。**
- b．**委託の場合**　：　**契約した業務以外に仮名加工情報を取り扱ってはならない**
- c．共同利用の場合：　利用の目的や範囲等についてあらかじめ公表しているときに限定

「産業保健分野」において：

a．個人情報を仮名加工情報とすれば、
⇒　**利用目的の 変更を公表した上で、事業所内で分析に活用することができる**

b．学会等での公表や外部への提供では**本人同意とともに、事業所への届け出**が必要。

対策案 a．外部への持ち出しの機会が多いにもかかわらず持ち出しに関するルールが未整備な事業場
⇒　産業医が主体的に事業者との間で**持ち出しに関するルール化を提案**することが望ましい。

対策案 b．仮名加工情報や統計情報等の非個人情報を公表する場合
⇒　**当該個人を識別可能な個人情報に復元されないような取扱（匿名加工情報化等）が必要**

対策案 c．**仮名化のために削除した情報の安全管理措置**や**衛生委員会での審議**　等
⇒　手続きを取り決めておくことが望まれる。

ガイドラインの（通則編）及び（事務局レポート
仮名加工情報・匿名加工情報　制度編）

4-11-2.産業保健分野におけるプロファイリング（論文による整理２）

利用目的の特定：「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ことが望ましい」

事例：「事業活動」や 「お客様のサービスの向上」等の表現では利用目的は特定できていない　場合
①閲覧履歴や 購買履歴を分析して趣味・嗜好に応じた商品・サービスを広告することや
行動履歴を分析した 結果をスコア化して第三者に提供することなどを**具体的に表現**する
②本人の行動・関心等に関する情報の**プロファイリング**が行われることについて
本人が予 想できる程度に特定する

産業保健分野において：

個人の健康情報が 本人の健康管理だけでなく、例えば**企業の経営や科学技術の振興のために利用される場合**

対応策
・案１：集団の統計情報として利用するか、同じ事業者内での利用であれば
仮名加工 情報とした上で利用
・案２：あらかじめ問診票への記載や窓口での掲示など合理的な 方法で本人同意を得る

ガイドラインの（通則編）及び（事務局レポート
仮名加工情報・匿名加工情報　事例編）による解釈

4-11-3. デジタル化以前に産業医側が推進すべきこと

1. 事業主による個人健康情報の取扱いを禁止（働き方改革法）
   - ➡ 産業保健職以外が個人健康情報を触れられない**技術的仕組み**の確立

2. 「産業医の個人情報保護基本方針」の宣言
   - ➡ 産業保健職以外が個人健康情報を触れられない**組織的仕組み**の確立

3. 個人情報保護法に基づく「同意の獲得」
   - ➡ 労働安全衛生法以外の法律も関わる業務(両立支援等)は、本人同意を得て、産業医が積極的に実践する

4. 「PHRベースの両立支援ネットワーク」の実現
   - ➡ 個人健康情報を本人が管理による、本人と事業主・主治医・産業医の間の「**PHR Subject Engagement**」(PHR本人の関与)が有効。
     必要な健康管理項目と、本人等に提供するタイミング・手続き等の研究が必要

5. 個人健康情報の管理に影響を与える 人口の高齢化と労働力の流動化

企業活動の変化

1. 企業構造の変化
（製造業 ⇒ サービス産業）

- 大規模事業所から分散・小規模事業所化

2. 企業活動の国際化を契機に個人健康情報の国際化

- 労働者・その家族の海外勤務・永住化による流出
- 海外企業の日本への進出

国民生活の変化

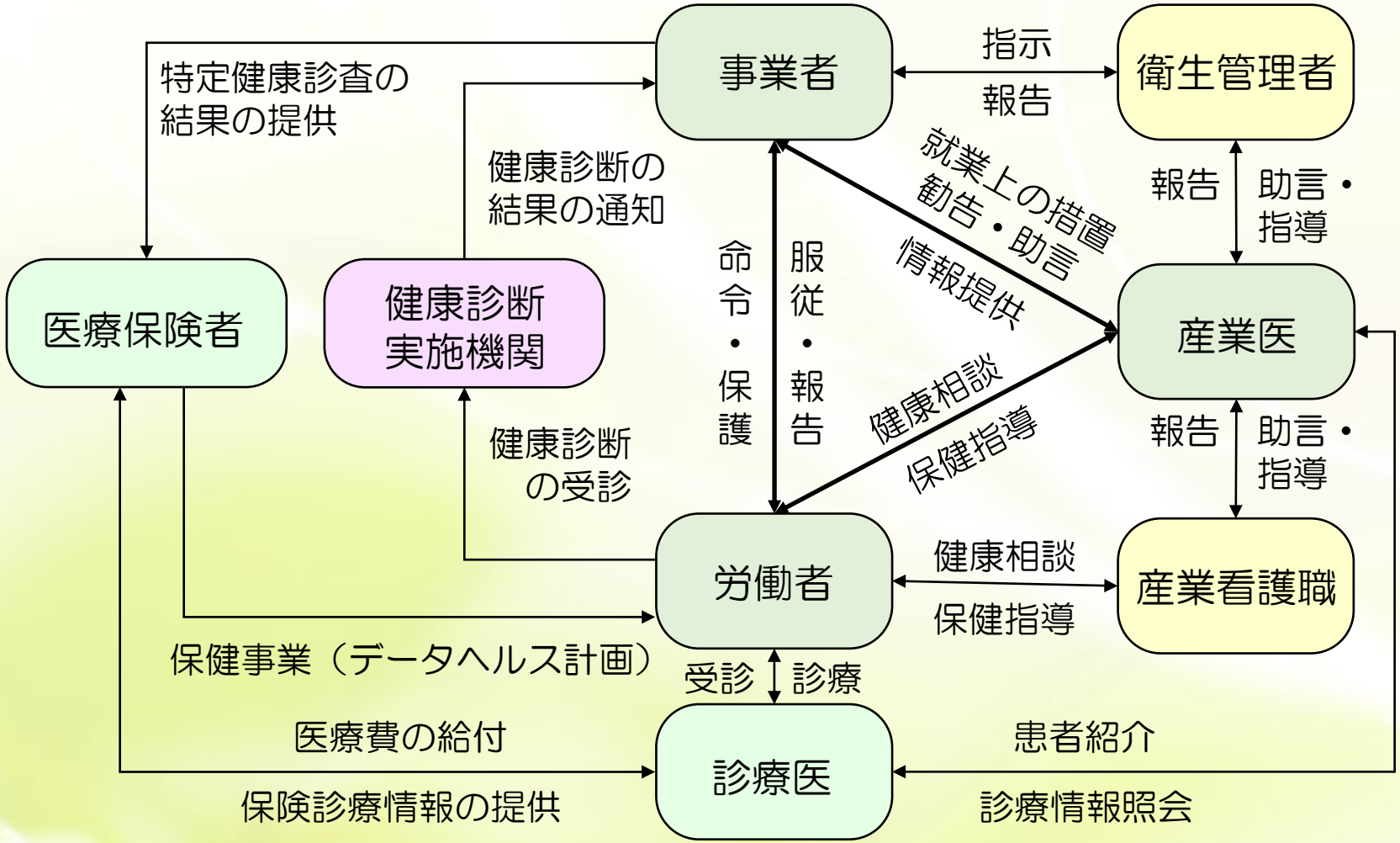
3. 終身雇用制度の崩壊がもたらす労働形態の多様化

- 転属・転職と共稼ぎ・派遣・パート等

4. 高齢者の住居・生活環境の変貌
（同居、別居、老人ホーム・・・）

- 高齢化・超高齢化社会：定年退職後期間増大
- 転居：子育てから、単身赴任、国内・海外への転勤・転職
- 単身者の増大：結婚高齢化・離婚・長寿に起因

6. 産業保健における健康情報の取り扱い

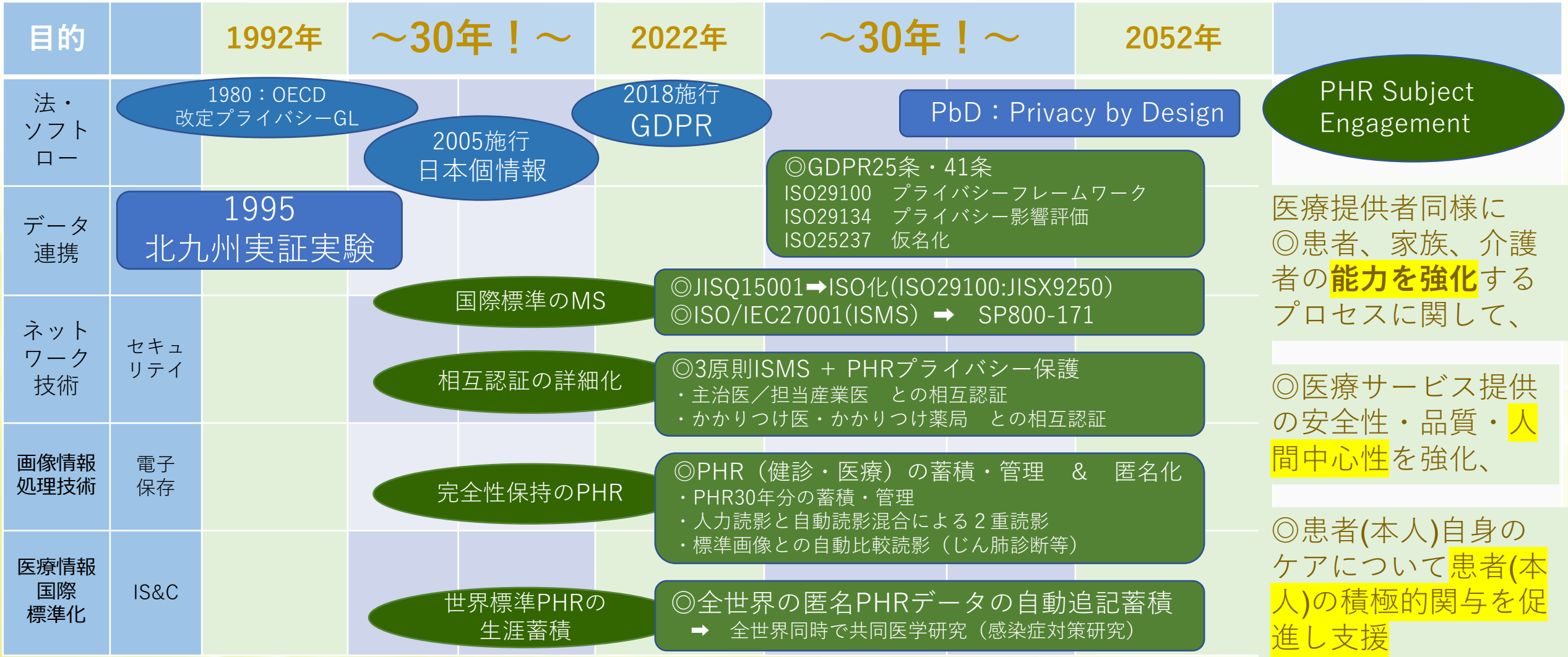


7. PHRによる国民の健康管理における
事業主・の役割の変質と本人の関与への促進

	現在　⇒	PHR化後	⇐　労働者本人	産業医⇒事業者
事業者 衛生管理者	健康管理への命令・保護	⇐受診勧奨結果の報告	服従・報告	
健診機関	健診結果の通知⇒本人へ	健診結果書き込み・通知⇒	健診受診	
	健診結果の通知⇒**事業主へ**			
医療保険者	保健事業 （データヘルス事業）	医療費報告⇒	保険費支払 （給与天引き）	
診療医	診療　カルテ開示	治療　医療情報⇒	受診	
産業医 産業看護師	保健指導	⇐　健康相談情報 保健指導情報　⇒	健康相談	就業上の措置・勧告・助言

	現在　⇒	PHR化後	⇐　労働者本人	産業医⇒診療医
産業医 産業看護師	患者紹介　⇒	⇐　治療　医療情報 保健指導情報　⇒ ⇐　健康相談情報	⇐　健康相談	⇐診療情報照会　⇒

8. PHRの未来への期待



8-1.医療・健診・介護分野におけるリスクの特定

1. 個人情報保護に関するリスク
   - a.不適切な取得、　同意の獲得なし
   - b.　利用、　利用目的にない利用
   - c.　提供、　同意のない提供、法律外の提供
   - d.　開示、　開示の却下、誤った開示
   - e.　苦情処理、受付ミス、受付への対応ミス

2. 個人データに関する情報セキュリテイに関するリスク
   - a.正確性のリスク、
     - ● 誤入力、誤配送　等
   - b.個人データの安全管理のリスク（ネット上も含む）
     - ① 機密性　盗難、窃視、不正なコピー
     - ② 完全性　改ざん、
     - ③ 可用性　破損、逸失、ネット停止

3. BYODのリスク
4. クラウドによるリスク

5. 電子保存3原則のリスク（真正性・見読性・保存性）
   - a.自社内システムの安全管理・電子保存のリスク
   - b.クラウド活用の際の安全管理・電子保存のリスク

8-2.プライバシー・リスクの追加

(1) 個人情報の情報セキュリテイ

a. 不適切な取扱い(情報の**機密性、完全性及び可用性の喪失**)

b. 不適切な、**取得・利用・提供・開示**等

に伴うリスクを特定するために、個人情報保護リスクアセスメントシートに記入

(2) これらのリスク所有者(管理責任者:各部所属長)を特定。

◎**プライバシー・リスクの追加**(ISO／IEC29134　プライバシー影響評価より)

- 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)

(過剰収集) 過度な収集(業務管理の喪失)

(無許可リンク) 無許可のまたは不適当なリンク

(利用目的通知不足) 処理目的の情報が不十分(透明性の不足)

(保管期間過剰) 不必要に長期間の保持

- PII本人の認識または同意なしで

(開示権不足) 権利に配慮することに関する失敗(例:アクセス権の喪失);

(法的無権限処理) PIIの処理(関連する法律または規制がないのに);

(同意不足利用・共有) PIIを第三者と共有または異なる目的での利用;

注:PII:Privasy　Identify Information

9. PHR 活用のための分権的･分散台帳ネットワーク

1. 多種・多機関間(労働者・事業者・医療機関・産業医　等)の連携が　必要な業務には、**分権的な分散台帳方式のネットワーク**が、機密性・完全性の確保に**有効**
   A) 多機関がＣ／Ｓのような主従の関係でなく、P2Pでの連携が可能
   B) 文書情報（医用画像・波形情報なども含む）の発生元、発生時刻、発行責任者が明確で、（適切なレベルで）コミット
   C) 文書の中味の改ざん防止が（適切なレベルで）コミットされている。
2. 個人情報保護の観点

   取得時の同意獲得・適切な利用・提供が行われ、本人の要求に応じてデジタル化を含む適切な方法で開示（ポータビリテイ性への要求）されること
3. 「**PHRの本人による管理**」のために
   A) 自身に関わる情報が流通する文書の状況（どこまで届いたか？）
   B) 中身の確認（改竄されていないこと）の確実性

   の手段をPHRの本人に与える。当該PHRが、**一般個人に分かり易い表現であることが必要**。

10. Engagement（関与）ツールとしての　PHR！

ー PHR Subject Engagementー
PHR本人による健康への関与

注：**Patient Engagement**　WHO(**The World Health Organization**)記事から

医療提供者同様に患者、家族、介護者の能力を強化するプロセスに関して、医療サービス提供の安全性、品質、人間中心性を強化し、患者自身のケアについて患者の積極的関与を促進し支援する。

注：OECD Privacy Guidelineより
Data Subject ➡ PHR subject

11. WHO has explained that

PE encompasses six essential elements:

1. **Design and development** *of patient-centered processes and systems*
2. **Patients' access** *to their own electronic health records (EHRs)*
3. *PE in* **policy development（政策立案）**
4. **Collection of information（情報収集）** *about patient experiences and care outcomes*
5. *Healthcare* **education and training（教育・訓練）**
6. **Educating and empowering people** to recognize their health（**国民の健康の維持増進への認識強化**）needs and seek healthcare in a timely manner

The Personal Health Record (PHR), a smartphone application, can contribute in enhancing all six elements of PE and education/training for medical professionals.

However, **we should establish the standard and interoperability of PHR data,**

- **including transfer protocol (e.g., HL7 FHIR),**
- **standard code of data items, and**
- **minimum data set in each clinical use case**
- **according to the standard clinical guideline**
- **before the PHR is diffused.**

11-1. PHR化のメリット(1)　Nature 論文より

患者自身が生涯にわたる院外も含めた**広範な健康記録を参照できることを望む**（医療現場においても）

PHRの創設

1. 電子健康記録データベースの確立（独立会社が管理する院外も含めた生涯の電子データ＝PHR）
2. **継続的な健康データが患者の医療への関与を高め、**コンプライアンスと治療成果を長期的に改善

PHRの目的

1　患者自身によるデータ管理とデータの使用方法の決定
- データの所有権を英国政府から患者に移す
- レガシーシステムの大規模なリエンジニアリング

2　患者が自身の治療の積極的なエージェントになるように動機付け

➡　**Patient Engagement**

3　システムへの多くのデータの提供により、可能な限り、最良の治療を提供

➡　**患者中心の治療となる**

Blockchain vehicles for efficient Medical Record management」
uraag A. Vazirani　@Medical Sciences Division, University of Oxford　他

11 - 2. PHR化のメリット（2）Nature 論文より

現状の課題

患者にとって：

本人が、うろ覚えで医療専門家に、自分の病歴を何度も繰り返し説明する必要がある

➡ 間違い伝達の元

医師にとって：

オフラインシステムでは検査結果や画像は前回のものしか参照できない。

課題の解決策

1. 全体システムをブロックチェーンで次第次第にリアルタイム化
2. 相互運用性問題の解決

➡ 包括的(comprihensive)に本人データを医師に提供

PHRデータ基盤の確立

データの所有権を個人に維持しつつ、要配慮データのプライバシーやセキュリティを損なうことなく、PHRを管理

システムのリエンジニアリング

1. ＥＵ－GDPRなどの法的制限に留意患者は自分のデータの消去を要求
2. ブロックチェーンの使用で、過去データの記録が常にチェーン上に存在

「Blockchain vehicles for efficient Medical Record management」
huraag A. Vazirani　@Medical Sciences Division, University of Oxford　他

ご清聴ありがとうございました

株式会社エム・ピー・オー

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

附1. GDPRの法律としてのポイント

第1章　第3条　地理的範囲、　第4条　定義
第2章　基本原則
　第6条 適法な取り扱い
　第7条 同意の条件（GL）
　第9条 特別な種類の個人データの取扱い

EUにおける個人情報の定義等

第3章 データ主体の権利（第12条～22条）
　第1節　透明性及び手順（GL）
　第12条 データ主体の権利行使のための透明性のある情報（GL）、通知及び手続
　第2節　情報及び個人データへのアクセス
　第13条 データ主体から個人データを収集する場合に提供される情報

わが国と同等の法制

　第3節 訂正及び消去
　第17条 消去の権利（忘れ られ る権利）
　Right to erasure ('right to be forgotten')
　第20条 データポータビリティー の権利
　Right to data portability（GL）
　第4節 異議を唱える権利及び個人に対する自動化された意思決定
　第22条 プロファイ リング を含む自動化された個人意思決定（GL）
　Automated individual decision-making, including profiling

EUの特徴的な法制

第4章 管理者及び処理者
　第 24条 管理者の責任（GL）
　第 25条 設計時からの及びデフォルトでのデータ保護(PbD)

PbDの法制化

　第 27条 EU域 内に拠点のない 管理者又は、取扱者の代理人
　第2節 個人データの保護
　第 32条 取扱いの保護
　第 34条 データ主体への個人データ侵害通知
　第3節 個人情報影響評価と予備コンサルテーション
　第35条　個人情報影響評価（GL）
　注：ISO/IEC 29134 - Privacy Impact Assessment

PIAの規格化

　第4節　データ保護オフイサー
　第37条　データ保護オフイサーの指名
　第5節 行動規範及び認証（第40条～43条）
　第 40条 行動規範
　注：ISO/IEC 29100 Prvacy Framework

規範と認証の法制化

第9章 特定の取扱いの状況と関係する条項
　第 88条 職場における取扱い
　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
　注：ISO/IEC25237-Pseudonymization

研究における個人情報の取扱い

(GL)あり

附4-12-1. 個人関連情報

［注A］個人関連情報データベース 等を構成するものに限る。以下この章及び第 6 章におい て同じ。

法第三十一条（第一項）　個人関連情報取扱事業者は、第三者が個人関連情報［**注A**］を個人データとして取得することが想定されるときは、第 27 条第 1 項各号に掲げる場合を除くほか、次に掲げる事項について、 あらかじめ個人情報保護委員会規則で定めるところにより確認するこ とをしないで、当該個人関連情報を当該第三者に提供してはならな い。［(1)・(2)略］

3-7-3-1 **個人データとして取得することを認める**旨の**本人の同意を得られている**こと

規則第 26 条（第 1 項）
1 法第 31 条第 1 項の規定による　同項第 1 号に掲げる事項の確認を行う 方法は、
個人関連情報の提供を受ける第三者から申告を受ける方法その他の適切な方法とする。

3-7-3-2 外国にある第三者への提供にあっては、必要な情報が当該本人 に提供されていること

規則第 26 条（第 3 項）
2 前項の規定により個人関連情報取扱事業者 が**個人関連情報**を提供する場合について準用する。
この場合におい て、同条第 3 項中「講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供し」とあるのは、「講じ」と読み 替えるものとする。

3-7-1-2個人関連情報取扱事業者：個人関連情報データベース 等を事業の用に供している者であって、第二条第五項各号に　体系的に構成したものとして政令で定めるものをいう。

3-7-3 本人の同意等の確認の方法（通則編）

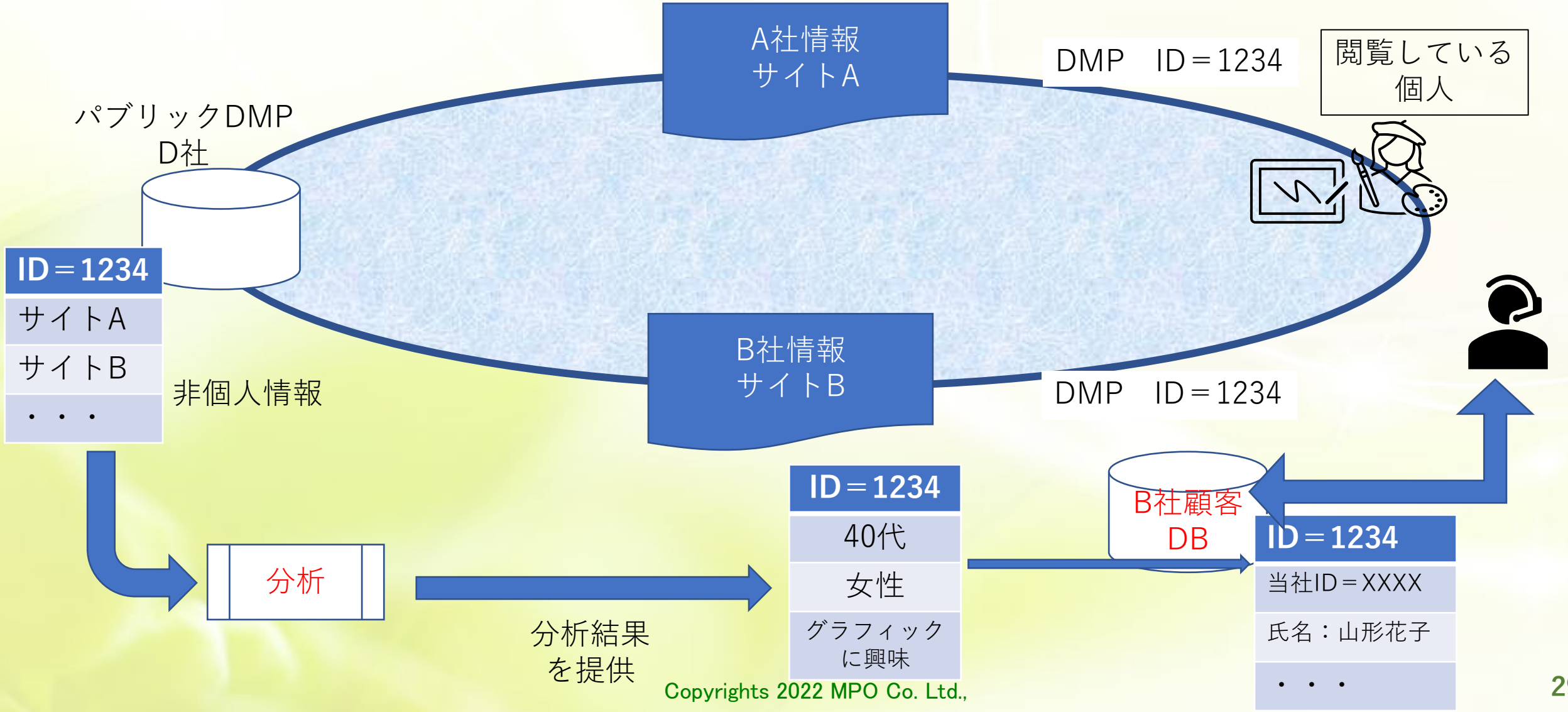
附4-12-2.個人関連情報

個人関連情報：法第 31条（第 1項）2

個人関連情報に該当する事例		➢ 事例 1）**Cookie 等**の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴 ➢ 事例 2）メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等 ➢ 事例 3）ある個人の商品購買履歴・サービス利用履歴 ➢ 事例 4）ある個人の位置情報 ➢ 事例 5）ある個人の興味・関心を示す情報
個人関連情報ではないもの	個人情報等	氏名、生年月日その他 の記述等により特定の個人を識別することができるもの
	仮名加工情報 法第 2 条(第 9 項)	**規則第 18 条の 7（第 1 号）：** 当該個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除
		規則第 18 条の 7（第 2 号）： 当該個人情報に含まれる個人識別符号の全部を削除
	匿名加工情報 法第 2 条(第 11 項)	**法第 1 項 第 1 号に該当する個人情報** 当該個人情報に含まれる記述等の一部を削 除
		法第 1 項 第 2 号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除する （この措置を講じた上で、まだなお法第 2 条第 1 項第 1 号に該当する個人情報であった場合には、同号に該当する個人情報としての加工を行う必要がある。）
	非個人情報等 （統計情報等）	特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではないため、個人関連情報にも該当しない。

附4-12-3. 個人関連情報提供のための同意獲得とは

パブリックDMP（データ・マネジメント・プラットフォーム）による閲覧履歴の分析結果の第三者提供による同意獲得「閲覧している個人」：の同意獲得が（法的に）可能



附4-13-1. 「Metadataとは何か？」

メタデータは、地上電話、携帯電話、デスクトップコンピューター、ラップトップなどのテクノロジーを使用して、通信デバイスと通信サービスプロバイダーによって生成された情報である。

タブレットまたはその他のコンピューティングデバイス。これらは本質的に他の情報に関する情報であり、この場合は、私たちのコミュニケーションに関連している。

メタデータまたはトラフィックデータの一部は、通信技術やオンラインサービスを使用するときに私たちが残すデジタルクラムである。メタデータには、通信の時間と期間、特定のデバイス、アドレス、または連絡先の番号を明らかにする情報が含まれる。

どの種類の通信サービスをどの地理的場所で使用するか。また、私たちが使用するほぼすべてのデバイスには一意の識別番号があるため、通信とインターネットアクティビティは比較的簡単にリンクおよび追跡でき、最終的には関係する個人にまでさかのぼることができる。このメタデータはすべて

アレイビジネスの目的で、通信会社やインターネットサービスプロバイダーなど、さまざまな期間にわたって通信サービスプロバイダーによって収集および保持される。ただし、次のような重要な質問が生じてくる。この情報のすべてに誰がアクセスでき、どのような目的でアクセスできるのか？

この情報を明らかにすることができるために、答えは特に重要である。

A Primer on Metadata: Separating Fact from Fiction
Ann Cavoukian, Ph.D.

附4-13-2. 「生活の、とある一日」

あるブロガーが最近強調したように、2人の個人が互いに通信するために使用するデバイスによって作成されたメタデータは、多くのことを明らかにする可能性がある。–

彼らの動静に関する情報関係、

彼らが住んでいる場所、

彼らが働いている場所、

そして彼らが寝る時間、

彼らが目を覚ます時間、

そして彼らが家を出るときさえ。

スノーデン氏

たとえば、このメタデータにアクセスできる人は、デバイスが毎晩同じ場所を共有している場合、2人が密接な関係を共有していると安全に想定する。カップルの場所は、たとえば、デバイスの三角測量によって明らかにすることができる。

関連する携帯電話タワーに関する信号強度。デバイスの1つが移動することを知っている

平日の午前9時頃に別の場所に移動し、午後5時頃までそこに留まる。通常の夜間の場所に戻る前に、個人の職場だけでなく、通ったルートや使用した交通手段も明らかにすることができる。

A Primer on Metadata: Separating Fact from Fiction
Ann Cavoukian, Ph.D.

附4-13-3. 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こと

- 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破棄される。

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

附15-1. 「ISMSの実践」が要求されているガイドライン

厚生労働省関連の下記ガイドラインで明示的に要求されている。

マネジメントシステムにより組織的・物理的・技術的な対策を行うとともに、職員、及び利害関係者にその意識を徹底する教育・監査が必要

1 医療情報システムの安全管理に関するガイドライン

医療情報システムの安全管理に関するガイドライン 第5.1版

2. 医学研究の倫理指針

人を対象とする生命科学・医学系研究に関する 倫理指針

3. NDB（National DataBase）ガイドライン

（匿名レセプト情報・匿名特定健診等情報の提供に 関するガイドライン）

匿名レセプト情報・匿名特定健診等情報の提供に関するホームページ...

附15-2. 「ISMSの実践」の意味

1 個人情報保護法の**実践を確実にするためには**、単に、経営者・管理者にその知識があるだけでは不可。

2 マネジメントシステムにより組織的・物理的・技術的な対策を行うとともに、特に、職員、及び利害関係者にその意識を徹底する教育・監査が必要

3 保健医療分野及び医学研究の関連分野では、医療情報の安全管理GL、医学研究の倫理指針等に、「ISMSの実践」がうたわれている。（注：ISMS：Information Security Management System: ISO/IEC 27001）

① 医療機関における医療情報システムの運用及び、医学研究所における研究分野では、その徹底が不十分。

② 一方、健診機関では、主に、企業・自治体等からの委託として業務を行うところから、比較的、プライバシーマーク（JISQ15001に基づく個人情報保護マネジメントシステム）が行われている。

③ 産業保健分野では、OHSAS（Occupational Health and Safety Assessment Seriesの略称で、労働安全衛生マネジメントシステムに対する規格。正式にはOHSAS 18001と呼ばれる。

④ マネジメントシステムの実践は、他の医療分野・医学研究分野より有効と考えられる。

4 今後の国際化に向けてISO29100（プライバシーフレームワーク）の適用が必要。

5 データサイエンスを正しく、有効に実践するために、マネジメントシステムが重要な働きを果たす。