

次世代医療基盤法とその展開

NPOデジタル・フォレンジック研究会「法務・監査」・「医療」合同分科会
2018年11月19日

おがたコンサルティング 代表
デジタル・フォレンジック研究会 「医療」分科会メンバー
国立精神・神経医療研究センター 研究PJアドバイザー

公認医療情報システム監査人 医療情報技師

緒方 健

おことわり

- 本スライドのうち、分析や意見にわたる部分は当職の関与する機関、団体の公式見解ではなく、当職の個人的見解です。
- 本稿で解説している内容は内閣官房・個人情報保護委員会・厚生労働省等の政府機関等により公表された資料、報道、文献、裁判例、学会報告及び講演記録をもとにしており、今後変更の可能性があります。

自己紹介

● 緒方 健 おがた けん

おがたコンサルティング 代表

- セキュリティ対策・情報管理に関するコンサルティング、点検・監査（内部監査・第三者認証審査）受託
- (国研) 国立精神・神経医療研究センター
 - 精神保健研究所 研究PJ委嘱アドバイザー
- 電気通信事業関係機関（旧総務省外郭）
 - プライバシーマーク審査部 主任審査員
- その他、医療ベンチャー企業（複数社）
 - 医療関連サービスのセキュリティ支援
 - 医療機器（AI診断支援機器）開発に参画
- 元 ISO審査登録機関 QMS/ISMS主任審査員
- IDF・情報ネットワーク法学会・日本医療情報学会・ISACA東京支部 各会員
- 日本ユーザビリティ医療情報化推進協議会 (JUMP) ゲノムが作る新たな医療推進委員会 委員
- 公認医療情報システム監査人
- 医療情報技師
- 経産省高度情報処理技術者（情報セキュリティアドミニストレータ）
- 情報セキュリティマネジメントシステム (ISMS : ISO/IEC27001) 主任審査員
- プライバシーマーク（個人情報保護マネジメントシステム）主任審査員

法律

医療分野の研究開発に資するための匿名加工医療情報に関する法律
(平成29年法律第28号)

- 通称
 - 次世代医療基盤法
 - 医療ビッグデータ法

目的規定

- 法1条（目的）

この法律は、医療分野の研究開発に資するための匿名加工医療情報に関し、国の責務、基本方針の策定、匿名加工医療情報作成事業を行う者の認定、医療情報等及び匿名加工医療情報の取扱いに関する規制等について定めることにより、健康・医療に関する先端的研究開発及び新産業創出（健康・医療戦略推進法（平成二十六年法律第四十八号）第一条に規定する健康・医療に関する先端的研究開発及び新産業創出をいう。第三条において同じ。）を促進し、もって健康長寿社会（中略）の形成に資することを目的とする。

次世代医療基盤法によって実現できること(例)

政府資料

自らが受けた治療や保健指導の内容や結果を、データとして研究・分析のために提供し、その成果が自らを含む患者・国民全体のメリットとして還元されることへの患者・国民の期待にも応え、ICTの技術革新を利用した治療の効果や効率性等に関する大規模な研究を通じて、患者に最適な医療の提供を実現する。

■ 治療効果や評価等に関する大規模な研究の実現

例1) 最適医療の提供

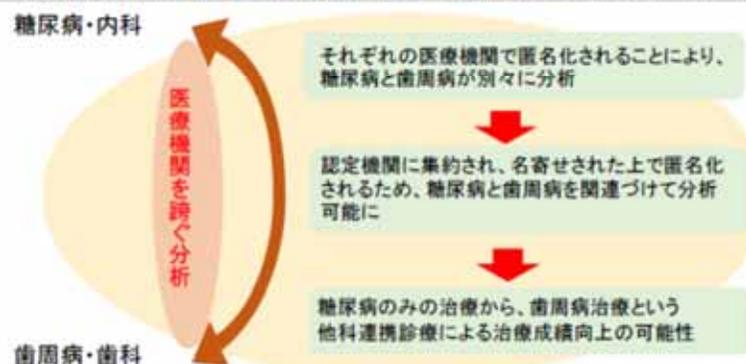
- 大量の実診療データにより治療選択肢の評価等に関する大規模な研究の実施が可能になる。

<例: 狭心症治療>



例2) 異なる医療機関や領域の情報を統合した治療成績の評価

- 糖尿病と歯周病のように、別々の診療科の関連が明らかになり、糖尿病患者に対する歯周病治療が行われることで、健康状態が向上する可能性



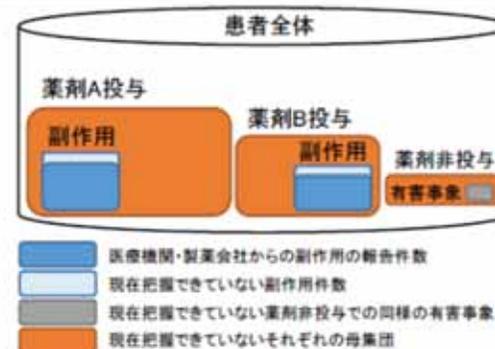
■ 医薬品市販後調査等の高度化、効率化

<医薬品等の安全対策の向上>

- 副作用の発生頻度の把握や比較が可能になり、医薬品等の使用における更なる安全性の向上が可能に

例3) 最先端の診療支援ソフトの開発

- 人工知能(AI)も活用して画像データを分析し、医師の診断から治療までを包括的に支援



「医療情報」

法2条（定義） この法律において「医療情報」とは、特定の個人の病歴その他の当該個人の心身の状態に関する情報であって、当該心身の状態を理由とする当該個人又はその子孫に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号（中略）を除く。）をいう。以下同じ。）であるものが含まれる個人に関する情報のうち、次の各号のいずれかに該当するものをいう。

一 当該情報に含まれる氏名、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（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

二 個人識別符号が含まれるもの

死者は含まれるのか

「医療情報」 / 「政令」

施行令1条 医療分野の研究開発に資するための匿名加工医療情報に関する法律（以下「法」という。）第二条第一項の政令で定める記述等は、次に掲げるものとする。

- 一 特定の個人の**病歴**
- 二 次に掲げる事項のいずれかを内容とする記述等（前号に該当するものを除く。）
 - イ 身体障害、知的障害、精神障害（発達障害を含む。）その他の**主務省令**で定める**心身の機能の障害**があること。
 - ロ 特定の個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（八において「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**（八において「健康診断等」という。）の結果。
- 八 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、特定の個人に対して**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。**

「医療情報」 ／「主務省令で定める心身の機能の障害」

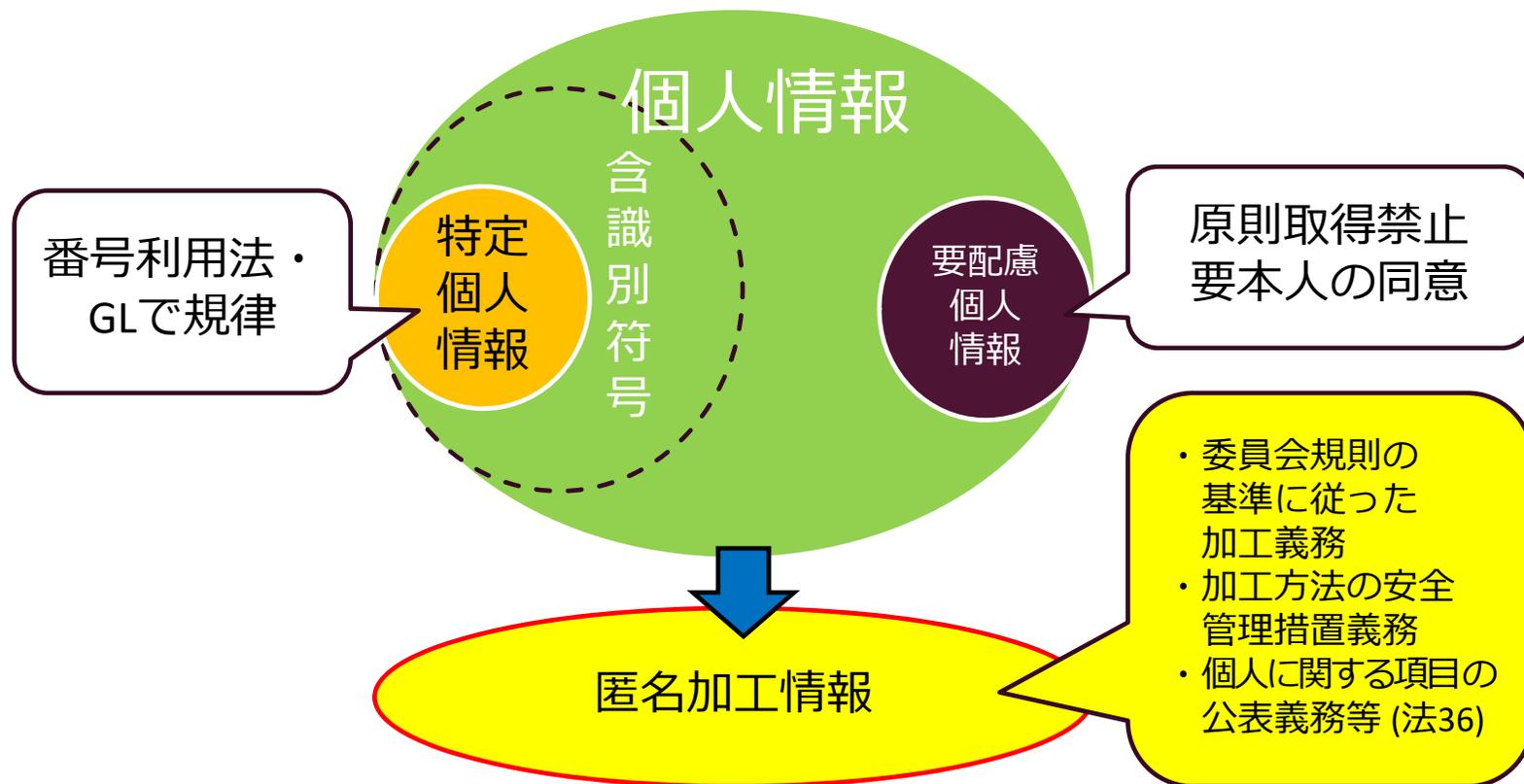
- **施行規則2条**

令（以下「令」という。）第一条第二号イの主務省令で定める心身の機能の障害は、個人情報保護に関する法律施行規則（中略）第五条各号に規定する障害とする。

- 身体障害者福祉法（昭和24年法律第283号）別表に掲げる身体上の障害
- 知的障害者福祉法（昭和35年法律第37号）にいう知的障害
- 精神保健及び精神障害者福祉に関する法律（昭和25年法律第123号）にいう精神障害（発達障害者支援法（平成16年法律第167号）第2条第1項に規定する発達障害を含み、前号に掲げるものを除く。）
- 治療方法が確立していない疾病その他の特殊の疾病であって障害者の日常生活及び社会生活を総合的に支援するための法律（平成17年法律第123号）第4条第1項の政令で定めるものによる障害の程度が同項の厚生労働大臣が定める程度であるもの

- 医療分野の研究開発に資するための
匿名加工医療情報に関する法律

匿名加工情報（個人情報保護法2）



匿名加工情報

特定の個人を識別することができないように個人情報を加工し、当該個人情報を復元できないようにした情報

1. 適切な加工（個人情報法36 、個人情報規則19）
2. 安全管理措置（個人情報法36 、 ）
3. 公表義務（個人情報法36 、 ）
4. 再識別行為の禁止（個人情報法36 、 38）

匿名加工のレベル

(PPCガイドライン匿名加工情報編P4)

- 法において「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、**一般人の判断力又は理解力をもって**生存する具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。匿名加工情報に求められる「特定の個人を識別することができない」という要件は、あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、**一般人及び一般的な事業者の能力、手法等を基準として**当該情報を個人情報取扱事業者又は匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるものである。

適切な加工

- ① 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（置換を含む）すること。
 - 例 氏名は削除。
- ② 個人識別符号の全部を削除すること。
 - 例 顔画像、指紋等。
- ③ 個人情報と他の情報とを連結する符号を削除すること。
 - 例 事業者内で個人情報を分散管理してデータベース等を相互に連結するために割り当てられているID等は削除する。
- ④ **特異な記述等を削除すること。**
 - 例 年齢116歳のように、国内で数名しかいない場合など。
- ⑤ 上記のほか、個人情報とデータベース内の**他の個人情報との差異等の性質を勘案し、適切な措置**を講ずること。

特異な記述等の削除

PPCガイドライン匿名加工情報編3-2-4 (p13) 【想定される加工の事例】

- 事例 1) 症例数の極めて少ない病歴を削除する。
- 事例 2) 年齢が「116歳」という情報を「90歳以上」に置き換える。

個人情報データベース等の性質を踏まえた その他の措置

PPCガイドライン匿名加工情報編3-2-5（p14）【想定される加工の事例】

- 事例 1) 移動履歴を含む個人情報データベース等を加工の対象とする場合において、自宅や職場などの所在が推定できる位置情報（経度・緯度情報）が含まれており、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、推定につながり得る所定範囲の位置情報を削除する。（**項目削除／レコード削除／セル削除**）
- 事例 2) ある小売店の購買履歴を含む個人情報データベース等を加工の対象とする場合において、当該小売店での購入者が極めて限定されている商品の購買履歴が含まれており、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、具体的な商品情報（品番・色）を一般的な商品カテゴリーに置き換える。（**一般化**）
- 事例 3) 小学校の身体検査の情報を含む個人情報データベース等を加工の対象とする場合において、ある児童の身長が 170 cm という他の児童と比べて差異が大きい情報があり、特定の個人の識別又は元の個人情報の復元につながるおそれがある場合に、身長が 150cm 以上の情報について「150 cm以上」という情報に置き換える。（**トップコーディング・ボトムコーディング**）

匿名加工医療情報

法2条3項（定義）

この法律において「匿名加工医療情報」とは、次の各号に掲げる医療情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように医療情報を加工して得られる個人に関する情報であって、当該医療情報を復元することができないようにしたものという。

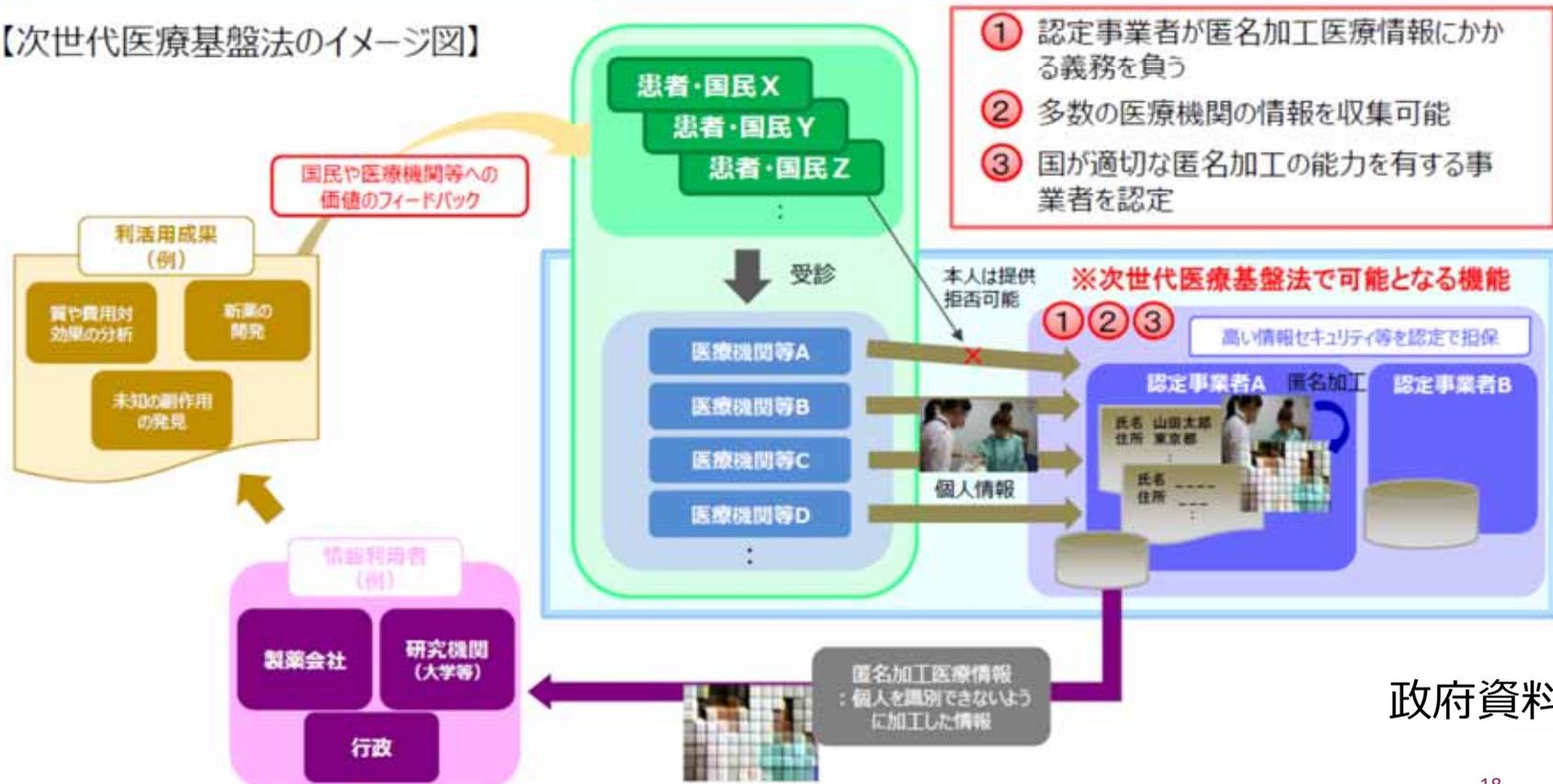
- 当該医療情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
- 当該医療情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

次世代医療基盤法の全体像(匿名加工医療情報の円滑かつ公正な利活用の仕組みの整備)

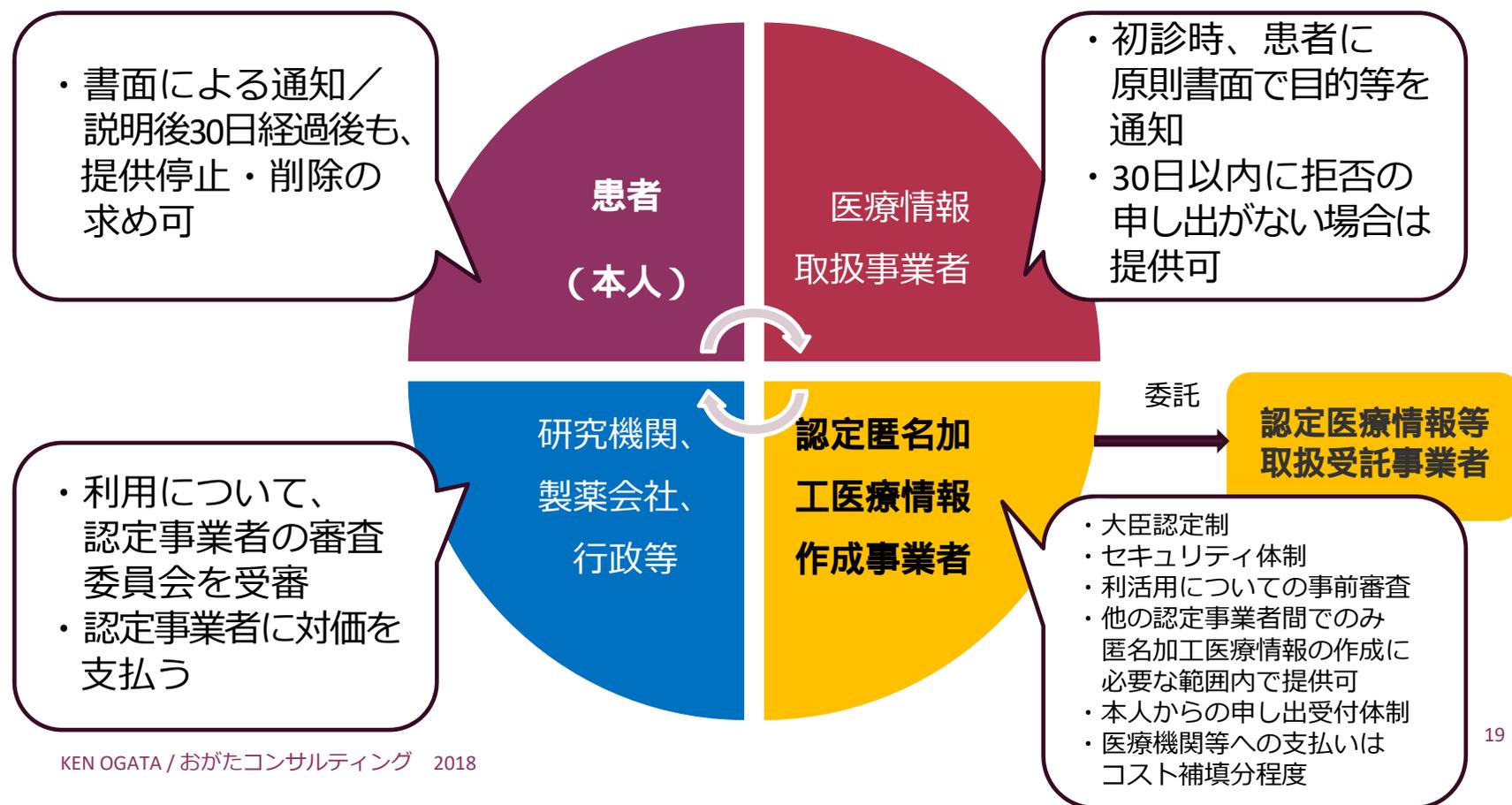
個人の権利利益の保護に配慮しつつ、匿名加工された医療情報を安心して円滑に利活用することが可能な仕組みを整備。

- ① 高い情報セキュリティを確保し、十分な匿名加工技術を有するなどの**一定の基準**を満たし、医療情報の管理や利活用のための匿名化を**適正かつ確実に**行うことができる者を**認定する仕組み**(=認定匿名加工医療情報作成事業者)を設ける。
- ② 医療機関等は、**本人が提供を拒否しない場合**、認定事業者に対し、**医療情報を提供できる**こととする。
認定事業者は、収集情報を匿名加工し、医療分野の研究開発の用に供する。

【次世代医療基盤法のイメージ図】



匿名加工医療情報を巡るサイクル



認定匿名加工医療情報作成事業者

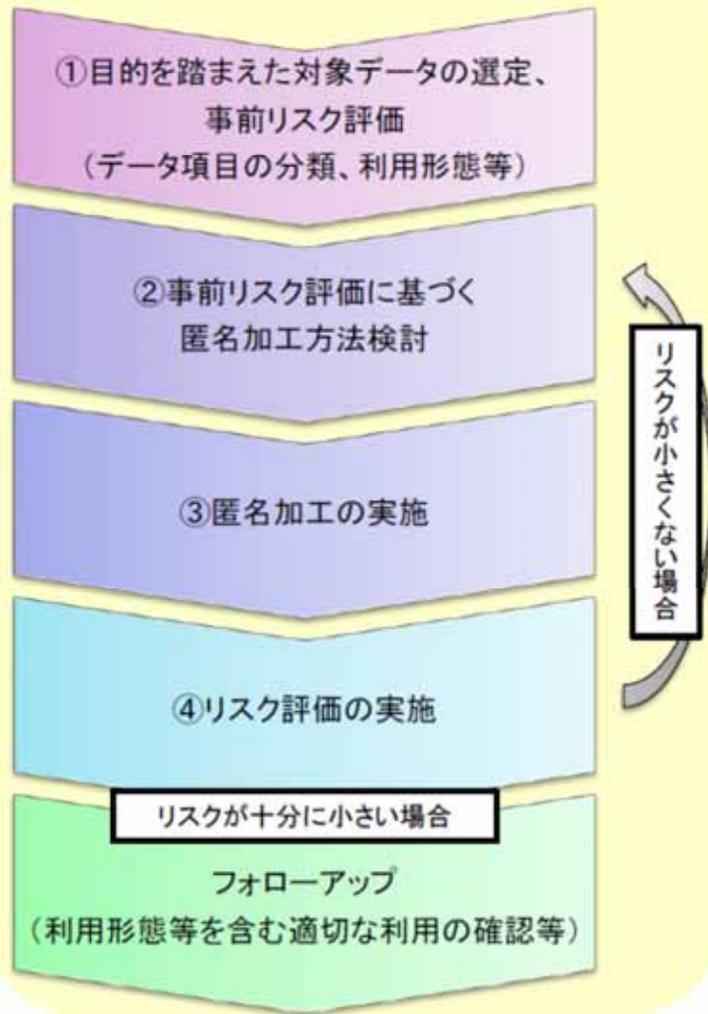
- その名の通り主務大臣の「認定」を受けねばならない
 - 総括管理責任者
 - 匿名加工の専門家
 - 医療情報検索システムその他の匿名加工医療情報作成事業に必要な設備
 - 厚労省標準規格
 - 内部規則、検証（監査・第三者認証）
 - 経理的基礎（財務基盤）、中期事業計画
 - 審査委員会
 - 広報・相談窓口
 - 義務・・・個人情報保護法上の第三者提供時・匿名加工情報作成・取扱時の義務のスキームを踏襲（確認・記録義務、再識別の禁止等）

匿名加工医療情報の作成プロセス

政府資料

○匿名加工医療情報の作成に用いられる医療情報の性質や匿名加工医療情報の利用の用途、形態等を踏まえて適切に匿名加工の程度を調整する。

①作成プロセスのイメージ



②医療情報の分類と具体的な匿名加工方法

- 下表のデータ項目に分類
- 識別子と準識別子については、匿名加工を行うことが必須。
- 静的属性と、半静的属性については、再識別のリスクに応じて匿名加工の要否を検討し、必要な場合は匿名加工を行う。
- 動的属性については、基本的に匿名加工は不要。

分類	定義	分類例	匿名加工の例
識別子	個人に直接紐づく情報	氏名、被保険者番号等	削除、もしくは他の記述等への非可逆な置き換え
準識別子	複数を組み合わせて個人の特定が可能な情報	生年月日、住所、所属組織等	k-匿名性を満たすように一般化、データ項目削除等を実施
静的属性	不変性が高い情報	成人の身長、血液型、アレルギー、日付等	匿名加工の要否を検討し、必要な場合は、トップ・ボトムコーディング、一般化等
半静的属性	一定期間、不変性がある情報	体重、疾病、処置、投薬等	匿名加工の要否を検討し、必要な場合は、トップ・ボトムコーディング、一般化等
動的属性	常に変化する情報	検査値、食事、その他診療に関する情報等	基本的に匿名加工は不要であるが、必要な場合はトップ・ボトムコーディング等

匿名加工のレベル (基盤法ガイドライン匿名加工医療情報編P6)

- 法において「特定の個人を識別することができる」とは、情報単体又は複数の情報を組み合わせて保存されているものから社会通念上そのように判断できるものをいい、**一般人の判断力又は理解力をもって**具体的な人物と情報の間に同一性を認めるに至ることができるかどうかによるものである。匿名加工医療情報に求められる「特定の個人を識別することができない」という要件は、あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、**一般人及び一般的な事業者の能力、手法等を基準として当該情報を医療情報取扱事業者又は匿名加工医療情報取扱事業者が通常の方法により特定できないような状態にすることを求める**ものである。

匿名加工のレベル

- この場合、「一般人又は一般的な事業者」は、一般人及び一般的な医療従事者、一般的な医療機関等を指す。これは、ある特定の疾患や治療法について専門性を有していない一般的な医療従事者（医師、看護師等）を想定するものである。また、判断の基準となる「一般人又は一般的な事業者の能力、手法等」については、例えばスーパーコンピュータのような高度な機能を有する資源や高度なハッキング・スキルを利用する等のあらゆる手法によって特定や復元を試みたとしてもできないというように、技術的側面からすべての可能性を排除することまでを求めるものではない。
- また、「当該医療情報を復元することができないようにしたもの」とは、通常の方法では、匿名加工医療情報から匿名加工医療情報の作成の元となった医療情報に含まれていた特定の個人を識別することとなる記述等又は個人識別符号の内容を特定すること等により、匿名加工医療情報を医療情報に戻すことができない状態にすることをいう。
- これは、あらゆる手法によって復元することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく、少なくとも、一般人及び一般的な事業者（一般的な医療従事者）の能力、手法等を基準として当該情報を医療情報取扱事業者又は匿名加工医療情報取扱事業者が通常の方法により復元できないような状態にすることを求めるものである。

データ消去義務（法19）

- 認定匿名加工医療情報作成事業者は、認定事業に関し管理する医療情報等又は匿名加工医療情報を利用する必要がなくなったときは、遅滞なく、当該医療情報等又は匿名加工医療情報を消去しなければならない。

医療情報取扱事業者

- 医療機関等
 - オプトアウトに必要な通知を行う
 - 本人等からの請求受付窓口
EHR事業者等は含まれるのか?

オプトアウト

- 法30条

医療情報取扱事業者は、認定匿名加工医療情報作成事業者に提供される医療情報について、主務省令で定めるところにより本人又はその遺族（死亡した本人の配偶者（婚姻の届出をしていないが、事実上婚姻関係と同様の事情にあった者を含む。）、子、父母、孫、祖父母及び兄弟姉妹。令6）からの求めがあるときは、当該本人が識別される医療情報の認定匿名加工医療情報作成事業者への提供を停止することとしている場合であって、次に掲げる事項について、主務省令で定めるところにより、あらかじめ、本人に通知するとともに、主務大臣に届け出たときは、当該医療情報を認定匿名加工医療情報作成事業者に提供することができる。

- 法31条

医療情報取扱事業者は、前条第一項の規定による通知を受けた本人又はその遺族から当該本人が識別される医療情報の認定匿名加工医療情報作成事業者への提供を停止するように求めがあったときは、遅滞なく、主務省令で定めるところにより、当該求めがあった旨その他の主務省令で定める事項を記載した書面を当該求めを行った者に交付しなければならない。

オプトアウト

- 法定事項の通知（基盤法ガイドライン医療情報の提供編p4）
 - 医療情報取扱事業者の事業の性質及び医療情報の取扱状況に応じて適切に対応することが求められるが、医療情報取扱事業者が医療機関等である場合には、法施行前から通院している患者を含め、法施行後、最初の受診時に行うことを基本とする。
 - その上で、本人との関係に応じて、その後の受診時にも通知を行うなど、より丁寧な形で通知を行うか否かは、認定匿名加工医療情報作成事業者に対して医療情報の提供を行うこととした医療情報取扱事業者の判断による。
 - なお、法施行前又は本人に対する通知を行う前に医療情報取扱事業者が取得した当該本人の医療情報についても、本人に通知し、当該本人が拒否しない場合には、認定匿名医療情報作成事業者に提供することができる。
- 30日間の熟慮期間経過後提供。その間はいつでも提供拒否可
- 提供後も、識別可能な限りも、提供停止・削除の求め可

患者への通知記載事項（法30）

- 医療分野の研究開発に資するための匿名加工医療情報の作成の用に供するものとして、認定匿名加工医療情報作成事業者に提供すること。
- 認定匿名加工医療情報作成事業者に提供される医療情報の項目 次の分類項目のうち該当する項目を記載する。
 - 診察・検査・治療の内容や結果等に関する情報
 - 健康診断の結果等に関する情報
 - 調剤に関する情報
 - その他
- 認定匿名加工医療情報作成事業者への提供の方法
 - 高度な安全管理措置を講じた手段により、認定匿名加工医療情報作成事業者に対して提供する旨を記載する。
- 本人又はその遺族からの求めに応じて当該本人が識別される医療情報の認定匿名加工医療情報作成事業者への提供を停止すること。
- 本人又はその遺族からの求めを受け付ける方法
 - 受付方法の具体的な事例だけでなく、本人又はその遺族が求めを行う際の連絡先も記載しておくことが 28 必要である。

認定匿名加工医療情報作成事業者のセキュリティ確保の基本的考え方 政府資料

安全面での課題

情報の漏洩

盗み見

情報・システムの改変・破壊

個人の医療情報の悪用
被 誤情報の活用、業務停止

害 認定匿名加工医療情報作成事業者への信頼喪失等

基本的手口(複数の組合せによる)

①騙し・なりすましによる暗証等の入手

②標的型攻撃メール等によるネットワークからの侵入・操作

③ソフトウェアの脆弱性の利用、不正通信ソフトウェア、ハードウェアの製造工程における意図せざる変更

④内部の不正アクセス(盗み見、記録メディアによる情報の持出し)

対応方針

①組織・人的要因の徹底排除

②基幹システムはオープンネットワークから分離

③多層防御・安全策の導入(想定外の手口にも対応)

具体策(「三本の柱」)

①組織・人的要因の徹底排除

- ・教育・運用・管理体制の整備(罰則付守秘義務)
- ・警備員・監視カメラ・入退室管理

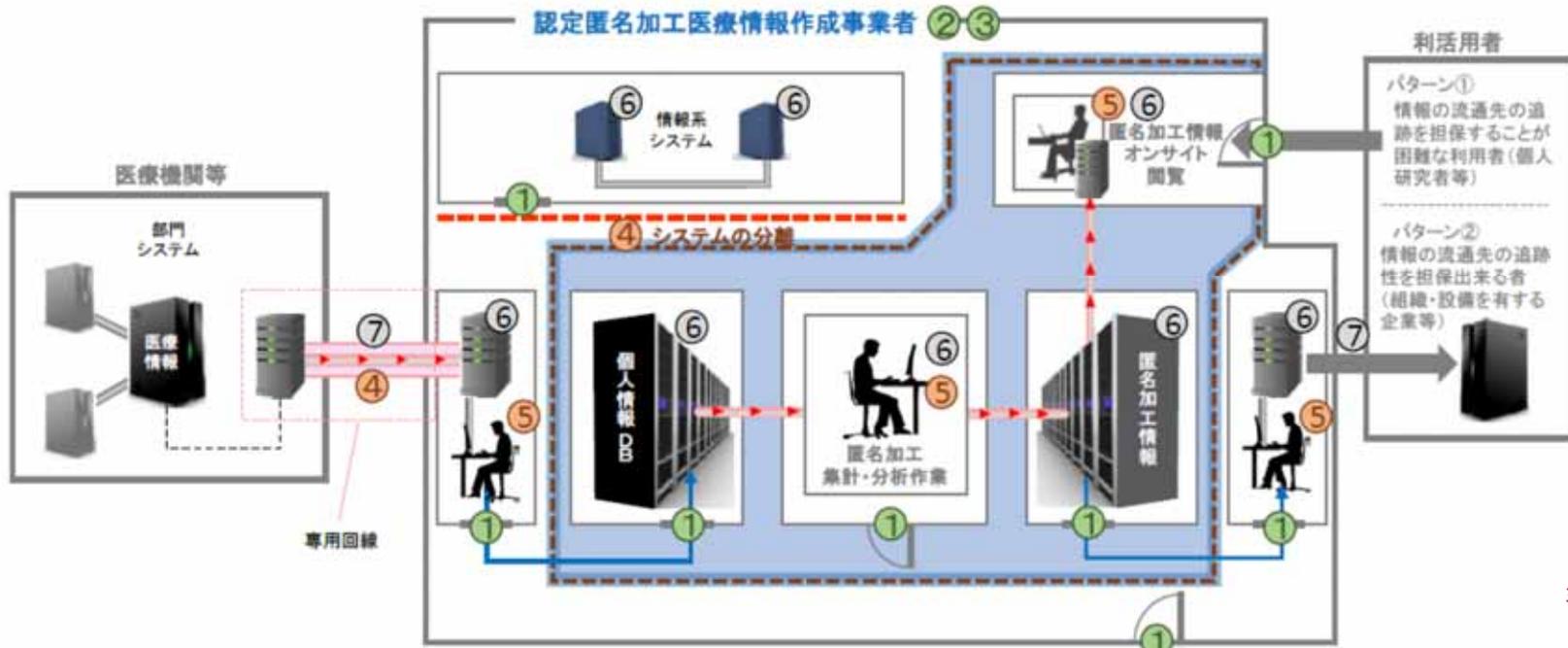
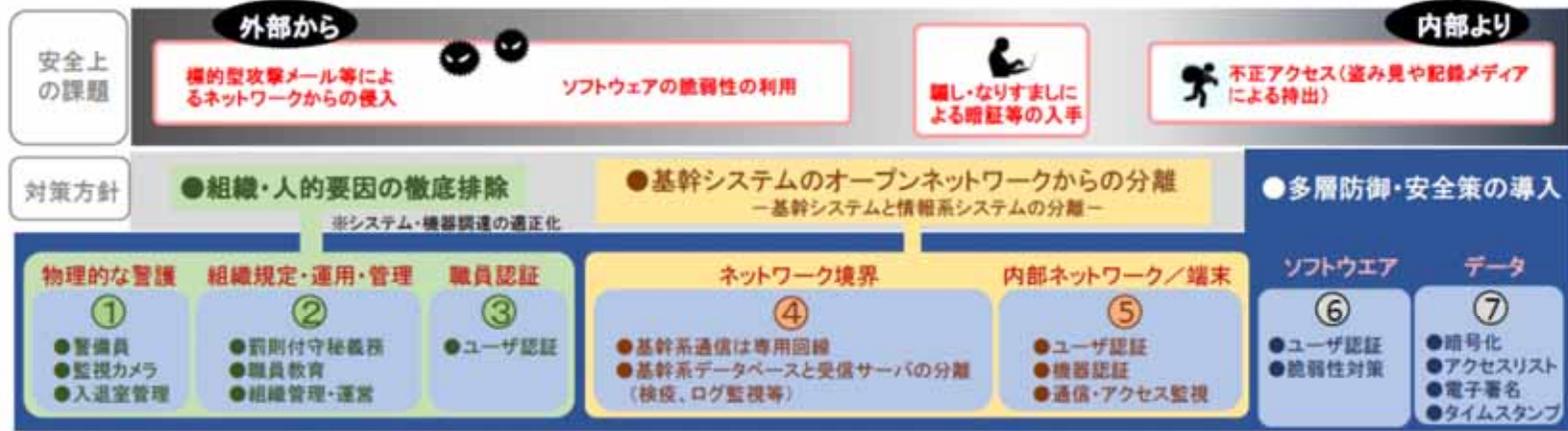
②基幹システムはオープンネットワークから分離

- ・基幹業務系と情報系システムの分離
- ・基幹業務系はインターネット等オープン環境から分離

③多層防御・安全策の導入(想定外の手口にも対応)

- ・基幹業務に係るデータの送受信は、基幹業務データベースと切り離し実施(ファイアーウォール等)
(それぞれ対応状況の異なる医療機関のセキュリティ水準に影響を受けないよう認定事業者の責任においてセキュリティ対策を実施)
- ・アクセスログ/データ操作ログをリアルタイムで監視(予定されない通信、アクセスは直ちに遮断する等)
- ・記録メディアの制限
- ・ソフトウェアの不断のアップデート(脆弱性対応等)
- ・データの暗号化(万が一、悪意ある者がデータ断片を入手しても解読困難)
- ・匿名加工情報利用者側のデータ利用の追跡性(トレーサビリティ)確保
- ・第三者認証を含む継続的なセキュリティ水準の確保や緊急時の対応、監督官庁への連絡体制の確保

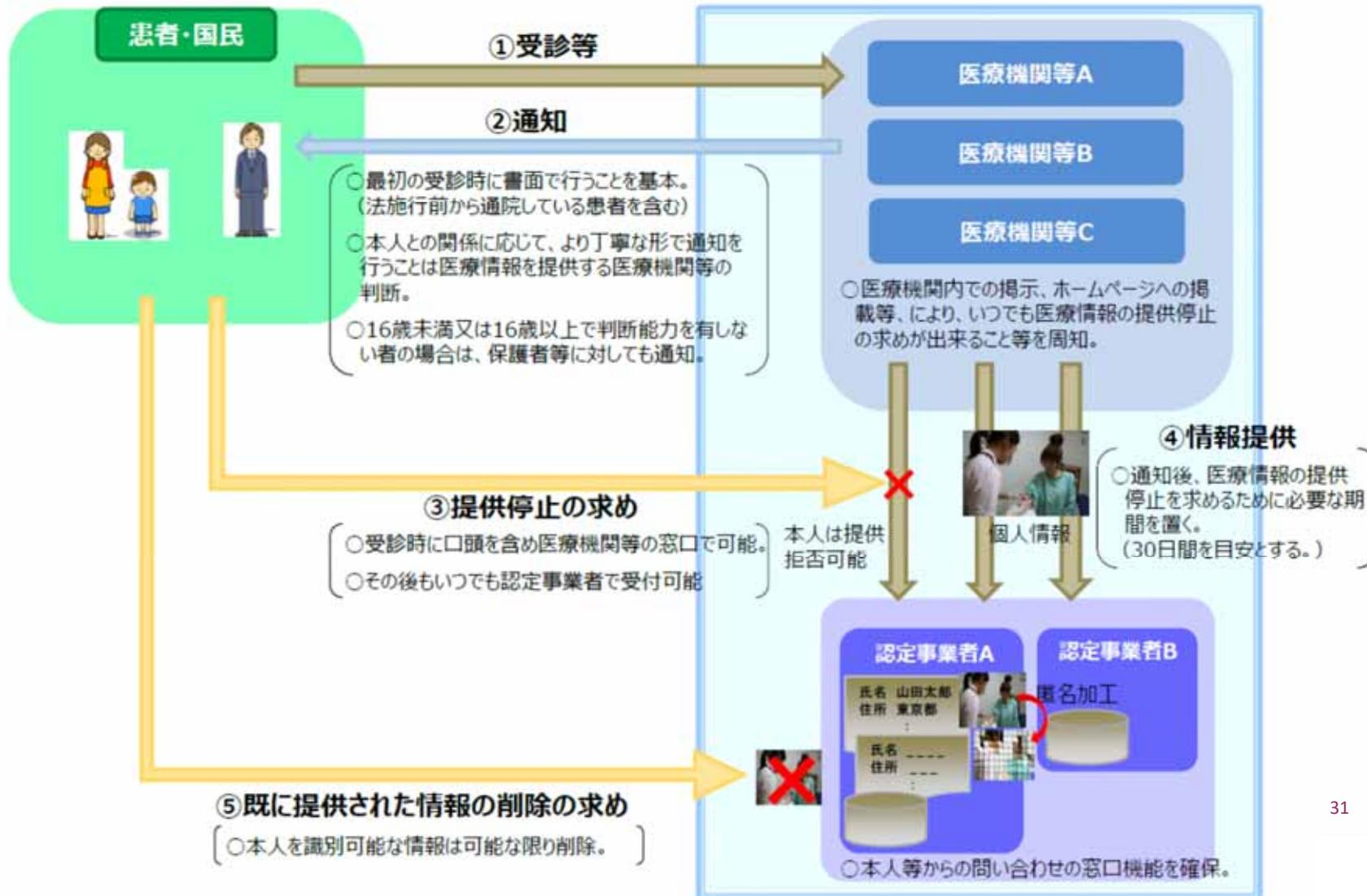
認定匿名加工医療情報作成事業者の具体的セキュリティ対策(詳細版) 政府資料



認定事業者に対する医療情報の提供に係る手続について

政府資料

- 次世代医療基盤法においては、医療機関等は、あらかじめ本人に通知し、本人が提供を拒否しない場合、認定事業者に対して医療情報を提供することができる（医療機関等から認定事業者への医療情報の提供は任意）



罰則（主要なもの）

- 認定匿名加工医療情報作成事業者又は認定医療情報等取扱受託事業者の役員若しくは従業者又はこれらであった者が、正当な理由がないのに、その業務に関して取り扱った個人の秘密に属する事項が記録された医療情報データベース等（中略）を提供したときは、二年以下の懲役若しくは百万円以下の罰金に処し、又はこれを併科する。（法44）
- 認定匿名加工医療情報作成事業者又は認定医療情報等取扱受託事業者の役員若しくは従業者又はこれらであった者が、その業務に関して知り得た医療情報等又は匿名加工医療情報を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、一年以下の懲役若しくは百万円以下の罰金に処し、又はこれを併科する。（法45）
- 認定事業に関して知り得た医療情報等又は匿名加工医療情報の内容をみだりに他人に知らせ、又は不当な目的に利用した者（法46③）は一年以下の懲役若しくは五十万円以下の罰金に処し、又はこれを併科する。
- 法の規定に違反して医療情報等及び匿名加工医療情報を消去しなかった者（法47②）は、五十万円以下の罰金に処する。

利点

- 医学研究において
 - 現在...「人を対象とする医学系研究に関する指針」に依らねばならない
 - 「指針」...最も厳しいルール
- 「匿名加工医療情報」にすることによって、煩わしい個別同意から解放される、と期待

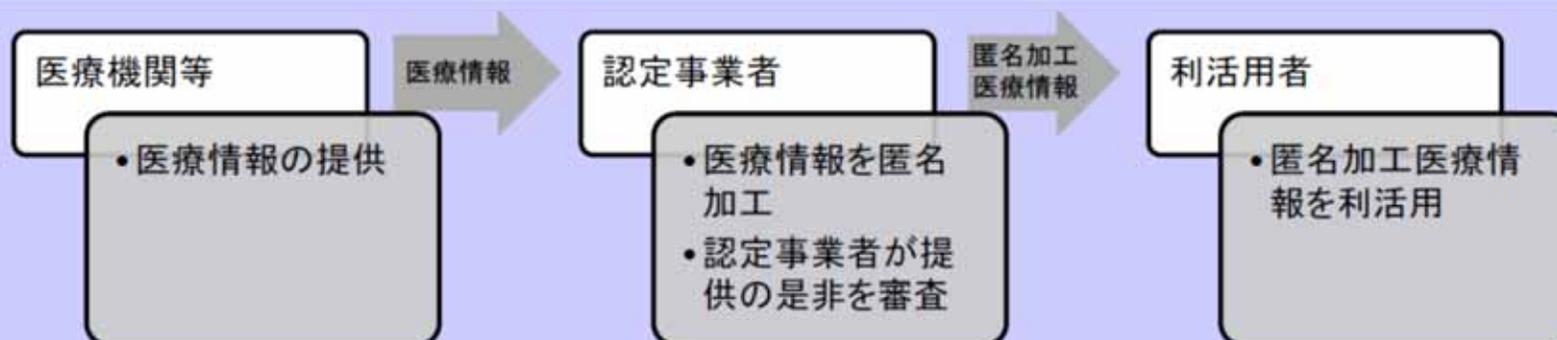
次世代医療基盤法と研究倫理指針との関係について

政府資料

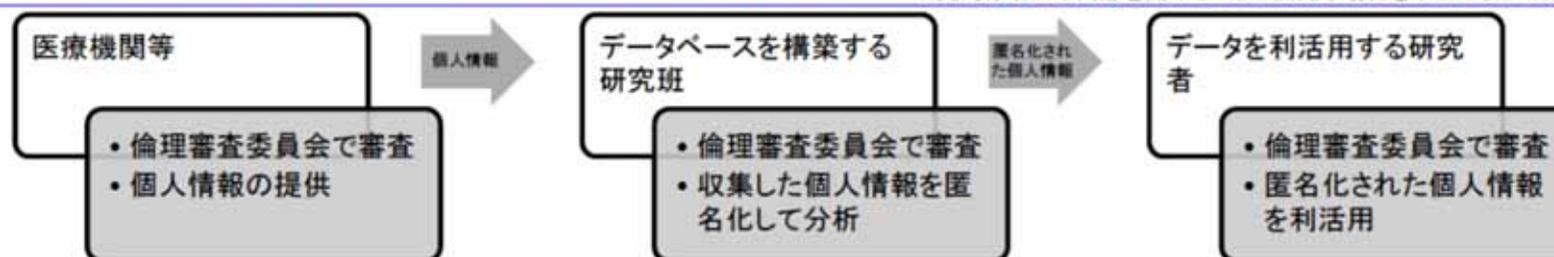
認定事業者による医療情報の取得、加工、匿名加工医療情報の提供の一連のプロセスは、法に基づくもので必要な手続きとされているため、医療機関等が医療情報を提供する際、認定事業者が医療情報を収集する際、認定事業者が匿名加工医療情報を提供する際、及び利活用者が匿名加工医療情報を利活用する際に指針※で求められている倫理審査委員会の承認等の手続きは不要。

※人を対象とする医学系研究に関する倫理指針

次世代医療基盤法



<参考> 学術研究(個人情報保護法第4章は適用除外※) 学術研究の中で倫理審査委員会での審査が必要となる例のうち、研究対象者から同意を受けることが困難な場合を示したものである



※研究目的が営利事業への転用に置かれているなど、学術研究の目的とはみなされない場合には、個人情報保護法第4章の規定が適用される。 34
また、個人情報保護法においては、匿名加工情報を第三者に提供する際に倫理審査委員会で審査することは求められていない。

課題（私見）

- 後ろ向き研究
- 二次、三次以降の利用（情報銀行）
- 第三者認証・監査との関係
- 事故発生時の法的問題
- 「値付け」の問題



ご清聴ありがとうございました