資料２－１

改正次世代医療基盤法における Visiting環境の考え方

（正式名称：医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律）

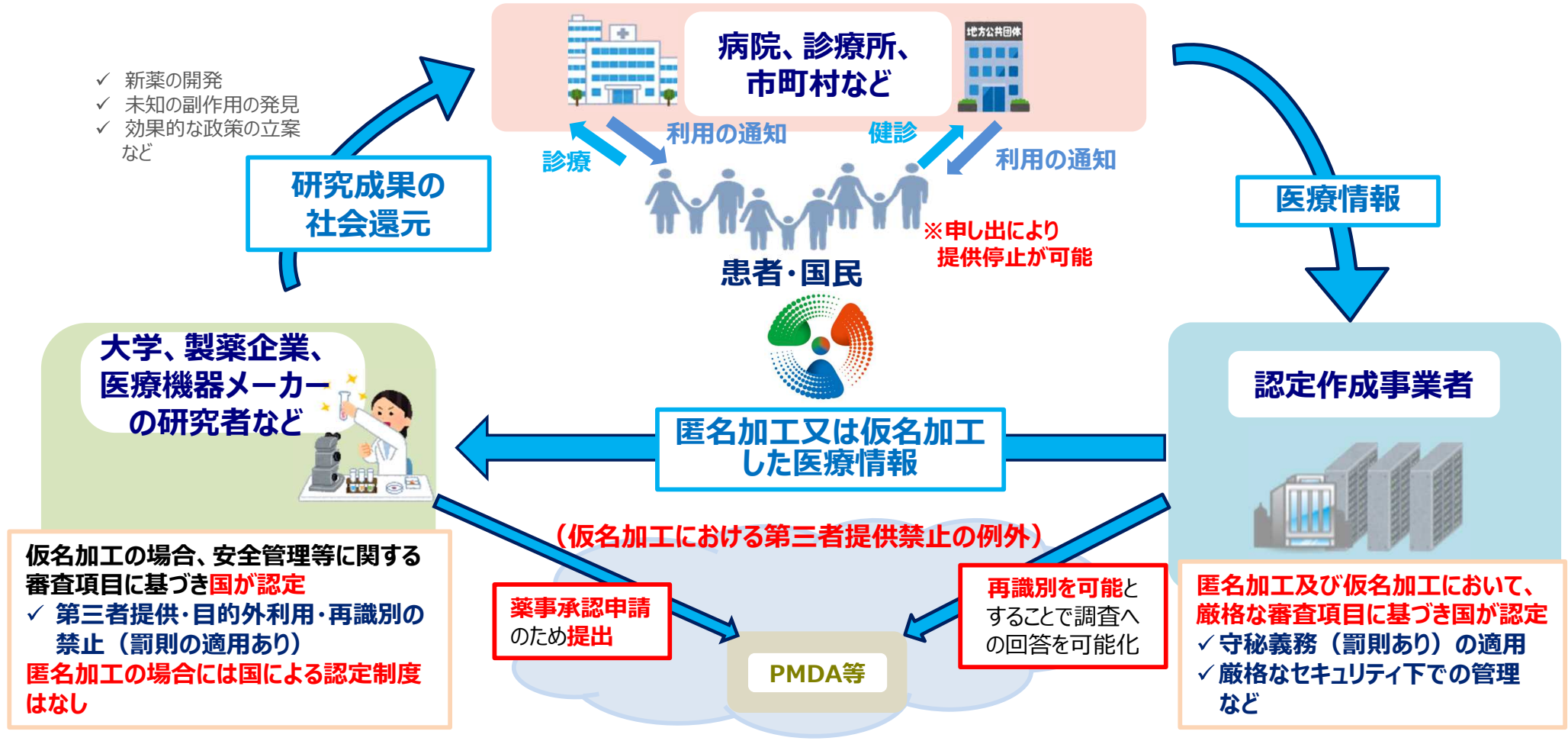
次世代医療基盤法

令和６年３月

内閣府 健康・医療戦略推進事務局

改正次世代医療基盤法に基づく仮名加工医療情報の利活用に係る仕組みの創設

- 改正次世代医療基盤法で、**新たに「仮名加工医療情報」の作成・提供を可能とする仕組みを創設。**その際、個人情報の保護の観点から、**仮名加工医療情報の提供は国が認定した利活用者に限定**。
  ※「匿名加工医療情報」については、改正前と同様、利活用者の認定は不要
- 仮名加工医療情報では、匿名加工医療情報とは異なり、医療データの削除、改変が不要であるなどの違いがあることから、以下が可能となり、制度の有用性が向上。
  ①**希少な症例**についてのデータ提供
  ②同一対象群に関する**継続的・発展的なデータ提供**
  ③**薬事目的利用の前提**であるデータの真正性を確保するための**元データに立ち返った検証**
- 現在、令和６年５月までの改正法施行に向けて、次世代医療基盤法ガイドライン案（新GL）等の調整を行っているところ。次頁以降の内容は、政府内で調整中のものであり変更がありうる。

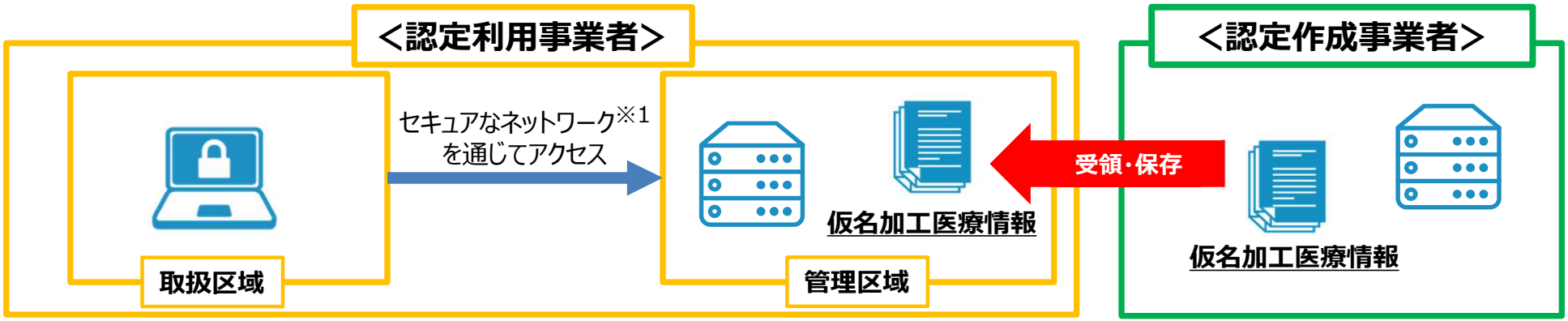


認定利用事業者の安全管理措置に関する基本的な考え方（1）

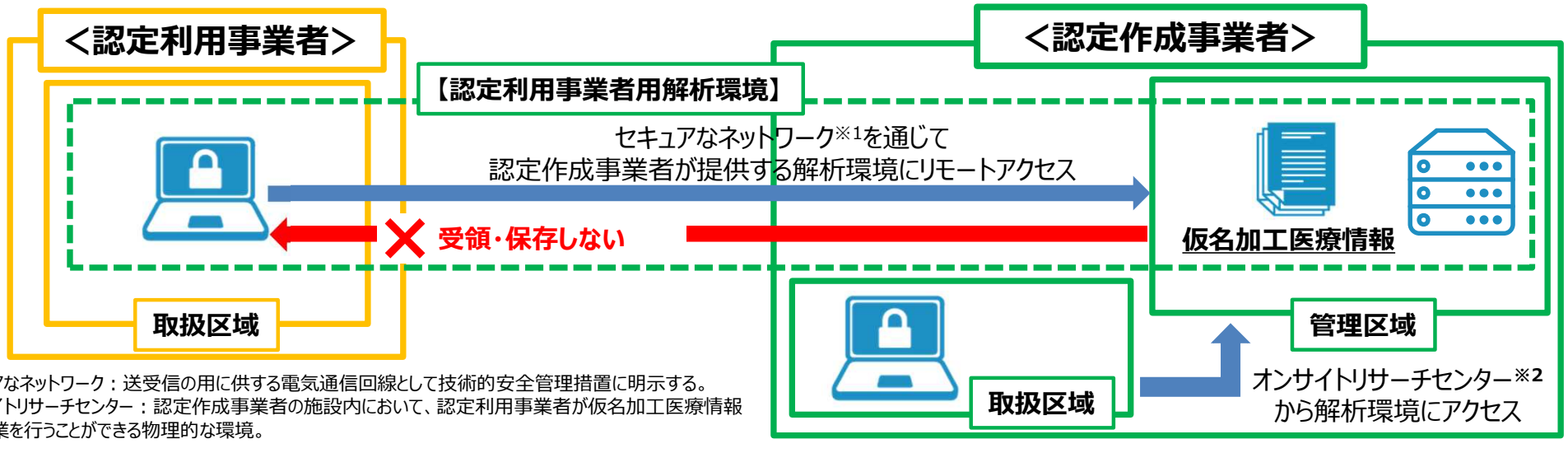
○「**Ⅰ型認定**」「**Ⅱ型認定**」及び「**管理区域**」「**取扱区域**」

- 確実な安全管理措置の確保と仮名加工医療情報の利活用促進の両立の観点から、利用事業者が自らの整備した環境下に仮名加工医療情報を保存することが可能な**Ⅰ型認定**に加え、認定作成事業者等が整備したVisiting環境での利用に限定し、当該環境を前提とした安全管理措置の要件を定める**Ⅱ型認定**の２種類を設ける（新GLⅣ-5-1-1-2参照）。
- また、提供仮名加工医療情報※を取り扱う施設設備として、仮名加工医療情報を保存する機器が設置される**管理区域**と、提供仮名加工医療情報の操作・解析等を行う**取扱区域**を特定し、安全管理のために必要かつ適切な措置を講じることを求める（新GLⅣ-14-3-1-1参照）。　※認定作成事業者から認定利用事業者に提供された仮名加工医療情報

【Ⅰ型認定】仮名加工医療情報を認定利用事業者の管理区域に保存する



【Ⅱ型認定】認定利用事業者は仮名加工医療情報を保存せず、Visiting環境限定で利用



※1 セキュアなネットワーク：送受信の用に供する電気通信回線として技術的安全管理措置に明示する。
※2 オンサイトリサーチセンター：認定作成事業者の施設内において、認定利用事業者が仮名加工医療情報を用いた作業を行うことができる物理的な環境。

認定利用事業者の安全管理措置に関する基本的な考え方 (2)

- 認定利用事業者は、自らの仮名加工医療情報の利用環境に応じて、**管理・取扱区域における仮名加工医療情報の取扱いに関するリスクの分析を行い、その結果に応じて講じるべき具体的な措置を検討・実施**する必要あり。それぞれの区域において生じ得る脅威及びそれによるリスクに対応するための措置としては、例えば、以下が考えられる※（新GL14-3-1参照）。

※ もっとも、各認定利用事業者において自らの利用環境に応じた個別のリスク分析及び当該分析に応じた措置の検討が必要であり、下記の全ての「具体的な手段」の実施を必ずしも必須とするものではなく、また、これらの手段のみにより安全管理措置が十分であることを示すものでもない。

※ とりわけ、取扱区域においては、認定利用事業者の業務内容や研究開発の目的・内容、取扱者の利用環境等によって、適切な安全管理措置の組合せは多様であると考えられる。

	（Ⅰ型認定の場合）管理区域	取扱区域
生じ得る脅威の例	• 取扱者以外の者による当該区域への無断立入り及び機器の持出し並びに仮名加工医療情報の閲覧・操作 • 取扱者自身による不正利用（例えば、機器の無断持ち出しや画面撮影等） 等	• 取扱者以外の者による仮名加工医療情報の閲覧・操作 • 取扱者自身による不正利用（例えば、画面撮影等） 等
当該脅威によるリスクに対応するために**講ずべき措置**及び**具体的な手段の例**	① **（物理的措置(2)）施設設備への立入り及び機器の持込みの管理及び制限**（新GLⅣ-14-3-2参照） • 生体を含む２要素以上の手法による認証を含む入退室の管理 • 機器を収納したラックに対する施錠・固定等による不正・不要なアクセスの防止 • 可搬記録媒体、スマートフォン等の機器の持込みの管理・制限 • 監視カメラ等による常時監視 ② **（物理的措置(3)）機器の紛失・盗難又は不正な持出しの防止等**（新GLⅣ-14-3-3参照） • 手荷物の検査、入退室管理簿の整備、ワイヤによる機器の固定等による機器等の持出しの管理・制限 • 間仕切りの設置・座席配置の工夫、のぞき見対策のシートの貼付、パスワードスクリーンセイバーの設定、画面撮影の禁止等による窃視の防止 ③ **（技術的措置(3)）電子計算機・端末装置の動作の記録及び操作の検知・制御**（ログを保存し、改ざん・不正な消去を防止する措置を講じること等）（新GLⅣ-14-4-3参照）	① **（物理的措置(3)）機器の紛失・盗難又は不正な持出しの防止等**（新GLⅣ-14-3-3参照） • 間仕切りの設置・座席配置の工夫、のぞき見対策のシートの貼付、パスワードスクリーンセイバーの設定、画面撮影の禁止等による窃視の防止 • 監視カメラの設置、端末装置等の操作時のPC内蔵カメラの利用、責任者又はその指名する者による監視その他の適切な手段による取扱区域の監視 ② **（技術的措置(3)）電子計算機・端末装置の動作の記録及び操作の検知・制御**（ログを保存し、改ざん・不正な消去を防止する措置を講じること等）（新GLⅣ-14-4-3参照） ※ Ⅱ型認定の場合には、認定利用事業者自らがこれらの措置を実施する必要は必ずしもなく、**認定作成事業者がビジティング環境の整備の一環として講じる安全管理措置との組合せにより、必要十分な安全管理措置を総合的に整備**することが必要

※ 詳細については、参考資料参照

認定作成事業者に係る関連規律等のポイント

② 認定作成事業者による認定利用事業者に対する仮名加工医療情報の審査・提供・監督等のあり方

（法第40条において準用する第９条第３項第3号及び第4号並びに第21条関係）

(1) 仮名加工医療情報の提供の際の認定作成事業者による審査に関して、**認定作成事業者の設置した審査委員会による倫理的・科学的観点からの審査等の規律を設ける（匿名加工医療情報の提供の際も同様）**。

(2) 認定作成事業者が認定利用事業者に対して仮名加工医療情報を提供する際の提供の方法や、提供後の認定作成事業者による監督については、認定作成事業者における安全管理措置の一環として、両者において取り決めるべき事項やVisiting環境の整備等についての考え方を示し、**認定利用事業者に対する仮名加工医療情報の提供・利用の際に適正な取扱いが確保されること**を求める（詳細は、補足資料６～８ページ参照）。

③ 認定作成事業者におけるクラウド利用に係る考え方の整理（（法第40条において準用する）第９条第３項第3号及び第4号並びに第21条関係）

- ✓ 従前実施していた新規・変更の認定に際しての現地確認等に係る考え方を改めて整理し、現地確認又はそれに代わる書面により物理セキュリティも含めた管理体制の十分性が確認可能であること等、必要な要件を満たしている場合にはクラウドサービスを利用することも許容されることを明確化する。
- ✓ なお、上記の考え方については、認定利用事業者においても同様とする。

認定利用事業者に対する仮名加工医療情報の提供のあり方

5ページ②（２）補足資料

- 認定利用事業者における複数種類の認定制度も踏まえ、**認定作成事業者が認定利用事業者に対して仮名加工医療情報を提供する際の取決め事項や提供の方法について、概要以下のとおり規律を定める**（新GLⅡ-25-4-1-1参照）。

  - ✓ 現行法においては、認定作成事業者に対して、その安全管理措置の一環として、**匿名加工医療情報取扱事業者との間の契約において、「匿名加工医療情報取扱事業者による当該匿名加工医療情報の利用の態様及びこれに係る安全管理のための措置」を適正に講じること**が求められており（規則第6条第5号二）、また、現行GLにおいては、適正な取扱いの確保のために必要な認定作成事業者と匿名加工医療情報取扱事業者との間で取り決めるべき事項に関する考え方等が示されている。
  - ✓ そこで、仮名加工医療情報に関しても、現行法における上記の規律を踏まえ、主務省令において、**認定作成事業者における安全管理措置の一環として、認定利用事業者に対する仮名加工医療情報の提供の際に適正な取扱いが確保されること**を求める。
  - ✓ また、新GLにおいて、認定作成事業者における安全管理措置の具体的な内容として、仮名加工医療情報の提供に際しては、認定利用事業者がⅠ型認定・Ⅱ型認定のいずれの認定を取得するかも踏まえた上で、**認定作成事業者と認定利用事業者との間で少なくとも以下の事項を取り決める必要がある**との考え方を示す。
    - ① 少なくとも以下の事項を含む仮名加工医療情報の利用条件及びそれに応じた安全管理措置
      - **利用目的**
      - **利用範囲**（例えば、仮名加工医療情報を取り扱う者、仮名加工医療情報を取り扱う場所等）
      - **利用内容**（例えば、提供する仮名加工医療情報の内容等）
      - **提供方法**（例えば、電気通信による方法、可搬記録媒体を用いる方法、Visiting環境（オンサイト環境、リモートアクセス環境等。）による方法等）
      - **利用形態**（例えば、 認定利用事業者独自の解析ツール・データの持込みや、成果物（中間成果物を含む。）の持出しに関する事項等）
      - **利用期間及び利用終了時の措置**（例えば、仮名加工医療情報の消去、廃棄等）
    - ② 認定作成事業者による、認定利用事業者に対する、仮名加工医療情報の利用条件及びそれに応じた安全管理措置の遵守状況に関する**定期的な監督**（次々頁参照）
    - ③ 他の認定利用事業者との**共同利用及びそれに応じた安全管理措置に関する、認定作成事業者の承諾及び契約等の締結**
    - ④ 上記の各事項に違反する仮名加工医療情報の取扱いが生じた場合の措置と制裁（例えば、利用の停止、氏名又は名称の公表等）

認定利用事業者に対する仮名加工医療情報の提供のあり方（続き）

5ページ②（２）補足資料

✓ さらに、現行GLにおいては、認定匿名加工医療情報作成事業者は、その安全管理措置の一環として、匿名加工医療情報取扱事業者への匿名加工医療情報の提供の際には、**①電気通信により送信する場合には専用線等（IP-VPNサービスに用いられる仮想専用線その他のこれと同等の安全性が確保されると認められるものを含む。）を用いる必要があること**、**②データの機密性、完全性及び真正性を確保する必要があること**等の考え方が示されている。

✓ そこで、仮名加工医療情報の提供に際しても、上記の現行GLと同等の基本的な考え方を示した上で、当該考え方に対応した具体例として、Ⅰ型認定・Ⅱ型認定の区別も念頭に置きつつ、認定作成事業者において満たすべき要件に関して以下のような一定の事例や留意点を明らかにする（新GLⅡ-25-4-1-2参照）。

① **電気通信による提供**：認定作成事業者が認定利用事業者に仮名加工医療情報を提供する、又は、認定作成事業者が管理する仮名加工医療情報に認定利用事業者がアクセスするために使用する回線は、**専用線等**（IP-VPNサービスに用いられる仮想専用線その他のこれと同等の安全性が確保されると認められるものを含む。）を用いること

② **電気通信によらない方法（可搬記録媒体等）での提供**：認定作成事業者が認定利用事業者に仮名加工医療情報を提供する際に、電気通信によらない方法で移送するときは、セキュリティサービス等を用いることにより、配達の記録を保存するとともに、配達状況の追跡可能性（トレーサビリティ）を確保すること

③ **サーバ構成**：認定作成事業者は医療情報を取り扱う領域と仮名加工医療情報を取り扱う領域とを区分すること。また、認定作成事業者において、認定利用事業者が解析サーバにアクセスするためのVDI接続基盤を構築する場合、認定利用事業者が認証された解析サーバ内の領域のみにアクセスできる構成を構築すること

④ **Visiting環境（オンサイト環境、リモートアクセス環境等）を構築する場合の技術的な安全管理の要件**：

- **利用事業者の認証方法**：リモートアクセス環境の利用時には、生体を含む二要素認証を必須とすること
- **ログの保存：**アクセスログ・操作ログを保存する機能を備えること
- **暗号化**：認定作成事業者は、解析サーバ内に保存されたデータ、解析サーバーから認定利用事業者が利用する端末への伝送中のデータを暗号化すること
- **設定**：認定作成事業者の許可のないデータのダウンロード・アップロードや、スクリーンショット・印刷を禁止する設定を行うこと

認定作成事業者による認定利用事業者に対する監督のあり方

5ページ②（２）補足資料

- 認定作成事業者における認定利用事業者に対する監督については、**個情法における委託元による委託先に対する監督の規律を踏まえ**、省令及びGLにおいて概要以下の規律を設ける（新GLⅡ-25-4-2参照）。

省令事項		認定作成事業者が、提供した仮名加工医療情報について適切な取扱いが行われるよう、認定利用事業者に対して必要かつ適切な監督を行う体制を備えていることを、認定作成事業者における安全管理措置の一環として規定。
GLの記載事項	両者間の取決め	• 認定作成事業者は、認定利用事業者との間で、認定作成事業者による認定利用事業者に対する仮名加工医療情報の利用条件及びそれに応じた安全管理措置の遵守状況に関する**定期的な監督**（例えば、**必要に応じて仮名加工医療情報を取り扱う場所に赴く又はこれに代わる合理的な方法での監督**、名簿の管理、利用終了時の措置等）について取決めを行うこととする。
	監督義務の履行	• 認定作成事業者は、上記の取決めに基づき、認定利用事業者に対して、**適切な方法により、定期的な監査を実施する必要があり、また、そのための体制を整備することが必要**となる。 • **定期的な立入検査・実地検査までを求める趣旨ではないが、**必要に応じて行えるように取り決めておくことが望ましい。 • 認定利用事業者において仮名加工医療情報の取扱者に変更・追加があった場合には、認定利用事業者より報告を受けることにより、**認定作成事業者が取扱者の適格性の確認と名簿の管理を行う**。 • **仮名加工医療情報及び成果物（中間成果物を含む。）の利用終了時**は、例えば以下のような形で、利用終了が確実に行われたことを認定作成事業者が確認する。 　• 【**Ⅰ型認定**の認定利用事業者の場合】認定作成事業者は、認定利用事業者における消去の状況を管理・確認し、その記録を保管すること 　• 【**Ⅱ型認定**の認定利用事業者の場合】認定作成事業者は、認定利用事業者によるVisiting環境上の当該データおよびスクリプトの消去の状況を管理・確認し、又は、認定作成事業者の権限と責任により当該データおよびスクリプトを消去し、その記録を保管すること。 • さらに、Ⅱ型認定を取得する認定利用事業者に対しては、例えば、**認定利用事業者のアクセスログ等の利用状況を監視**し、想定されない利用（例：外部記憶媒体の接続、データの利用量やアクセス頻度が異常な水準となったこと等）が生じた場合の検知・制御体制を整備し運用すことが必要となる。 • また、認定作成事業者は、**認定利用事業者からの要望（独自データと仮名加工医療情報を合わせた解析、独自の解析ツールの使用、成果物の持出しなど）**について確認の上、可否や方法の回答を行い、必要な対応を行う。

参 考 資 料

認定利用事業者の安全管理措置に関する基準（組織的安全管理措置 (1)）

(1) 仮名加工医療情報の安全管理に係る基本方針（新GLⅣ-14-1-1参照）

✓次に掲げる事項を含め、**仮名加工医療情報の安全管理に関する基本的な考え方を明らかにした基本方針**を策定する必要がある。
- 仮名加工医療情報を利用する一連の過程で生じ得るリスクを分析し、その結果に応じ、仮名加工医療情報の安全管理のために必要かつ適切な措置を講ずる方針
- 適用される法、個人情報保護法その他の関係法令及び内部規則等の遵守を徹底する方針

✓策定にあたっては、データのライフサイクル全般に亘って適切にリスク管理を行うというデータマネジメントの観点を勘案することが望ましい。

(2) 安全管理責任者（新GLⅣ-14-1-2参照）

✓ 「仮名加工医療情報の安全管理に関する相当の経験及び識見を有する責任者」（安全管理責任者）を設置し、以下の事項を明らかにする必要がある。
- **認定利用事業者内の組織体制における権限及び責任**
- 安全管理責任者が業務を全うすることが可能であること（以下に該当する場合にはその内容を記載する必要あり）
  - 安全管理責任者の勤務形態が出向又は派遣である場合にあっては、当該認定利用事業者と出向元又は派遣元との間の契約等により、安全管理責任者の権限及び責任について取り決めていること
  - 安全管理責任者が認定利用事業者以外の法人又は個人で兼業する場合（非常勤又は臨時的な業務に就く場合を除く。）にあっては、当該兼業の内容（兼業先となる法人の名称を含む。）
- 安全管理責任者に係る契約関係
  - 安全管理責任者が認定利用事業者のためにその指揮命令又は監督を受けてその業務に従事する契約関係（例えば、雇用、出向、派遣等）にあることを明らかにする必要がある
- **安全管理責任者の実務経験及び専門性**
  - **個人情報保護を含む情報セキュリティに係る実務経験を有するなど、必要な専門性を有すること**をいう
  - 申請書類においては、上記を満たしていることが分かる具体的な経歴、業績、資格等を明らかにする必要がある

※安全管理責任者が業務に従事し得ない場合の代位者を指定することが必要（**Ⅱ型認定の場合には任意**）

認定利用事業者の安全管理措置に関する基準（組織的安全管理措置 (2)）

(3) 取扱者の権限及び責務並びに業務（新GLⅣ-14-1-3参照）

✓ 認定利用事業者における取扱者の権限及び責務並びに業務を明らかにした上で、当該権限及び責務を自覚して誠実かつ適正に職務を遂行する者を採用し又は選任することが可能となるよう、**必要かつ適切な取扱者の範囲及び当該取扱者の採用又は選任に関する方針**を明らかにする必要がある。

✓ また、当該方針に基づいて、取扱者の範囲は、名簿等（電磁的記録による場合も含む。）により適切に管理する必要がある。

- 取扱者の名簿等については、認定作成事業者による認定利用事業者に対する監督の一環として、認定作成事業者に対して定期的に報告する必要がある。

(4) 漏えい等事態に際しての事務処理体制（新GLⅣ-14-1-4参照）

✓ 次に掲げる事項を始めとする、漏えい等事態に際しての事務処理体制を明らかにする必要がある。

- 漏えい等事態に対応するための組織体制（例えば、責任者及び担当者の定め等）
- 組織的に漏えい等事態を速やかに把握するとともに、**主務府省に対する報告を実施するための体制及び方針**（例えば、担当者から責任者への連絡、認定作成事業者への連絡等）
- 漏えい等事態に関して、**原因究明のための調査**を実施し、その結果に基づき、当該漏えい等事態に伴う被害を最小化するための対策を実施する方針
- 漏えい等事態に関する事実関係の調査を実施した結果に基づき、**類似事案の再発を防止するための対策**を実施する方針

(5) 安全管理措置に関する規程の策定・実施・評価・改善（新GLⅣ-14-1-5参照）

✓ 仮名加工医療情報の安全管理に係る実効性を担保するために、自ら恒常的にリスク分析を実施し、その結果に応じて必要かつ適切な措置を講ずる観点から、**安全管理措置に関する規程に係るPDCAサイクルを実現すること**が求められる。

✓ そこで、申請書類においては、Ⅰ型認定とⅡ型認定のいずれの認定を取得する予定なのかも踏まえ、次に掲げる事項を含む安全管理措置に関する規程の策定・実施・評価・改善に関する方針を明らかにする必要がある。

- 仮名加工医療情報の利用に係るリスク分析を実施した結果
- 当該結果に応じ、仮名加工医療情報の安全管理のために**必要かつ適切な措置を講ずるため策定する規程**の概要
- 当該規程の運用を把握して分析するための**評価を定期的及び必要時に行う方針**（例えば、対象、方法、頻度、体制等）
- 当該評価の結果に基づき、**必要に応じ、当該規程の運用を改善する方針**（例えば、手順、頻度、体制等）

認定利用事業者の安全管理措置に関する基準（人的安全管理措置）

(1) 取扱者等が欠格事由等に該当しないことの確認（新GLⅣ-14-2-1参照）

✓ 申請書類において、以下の事項について誓約する必要がある。

- 申請者の特定役員又は特定使用人が暴力団員等に該当しないこと
- 申請者の取扱者が、欠格事由（法第44条において準用する第９条第３項第１号ハ）及び暴力団員等のいずれにも該当しないこと
- 申請者が、暴力団員等がその事業活動を支配する者又は暴力団員等をその業務に従事させ、若しくは当該業務の補助者として使用するおそれのある者でないこと

(2) 仮名加工医療情報の適切な取扱いの確保（新GLⅣ-14-2-2参照）

✓ 取扱者を始めとする認定事業従事者について、責務を自覚して誠実かつ公正に職務を遂行する者を採用・選任し、また、内部規則等の遵守を徹底させる観点から、次に掲げる措置を講じることを求める。

- 内部規則等に違反する行為をした認定事業従事者に対する懲戒その他の制裁
  - 申請書類においては、内部規則等に違反する行為が、認定利用事業者の就業規則等で規定される懲戒等の制裁の事由に含まれることを明らかにする必要がある。
- **認定事業従事者に対する内部規則等の内容に関する周知（認定利用事業者に対する、書面又は電磁的方法等による取扱者の誓約書の提出を含む。）**

(3) 取扱者に対する教育及び訓練（新GLⅣ-14-2-3参照）

✓ 申請書類においては、認定事業従事者に対する定期的な研修（eラーニングシステムを用いて行われるものを含む。）を始めとする教育及び訓練について、対象者、内容、方法、頻度等に関する計画を記載する必要がある。

✓ また、教育及び訓練に係る年月日、内容、方法等に関する記録を作成するとともに、当該記録をその作成日から３年間保存する必要がある。

認定利用事業者の安全管理措置に関する基準（物理的安全管理措置 (1)）

(1) 施設設備の特定（新GLⅣ-14-3-1参照）

✓ 仮名加工医療情報に係る**管理区域（当該情報が保存された機器等が置かれた区域を含む当該機器等を管理する区域）**及び**取扱区域（当該情報の操作、解析等を実施する区域）**を特定することを求める（必ずしも専用の区域を設ける必要はない）。

✓ また、管理区域・取扱区域のそれぞれにについて、認定利用事業者自らの利用環境を踏まえた仮名加工医療情報の取扱いに関する**リスクの分析を行い、その結果に応じて講じるべき安全管理措置の具体的な手段を検討し、実施すること**を求める。

✓ なお、Ⅱ型認定の場合には、認定利用事業者の管理する環境下には取扱区域のみが存在することになる。また、その場合には、認定作成事業者がVisiting環境の整備の一環として講じる安全管理措置との組合せにより、必要十分な安全管理措置を総合的に整備することが必要であり、また、それで足りる。

(2) 施設設備への立入り及び機器の持込みの管理及び制限（新GLⅣ-14-3-2参照）

✓【Ⅰ型認定の場合のみ】仮名加工医療情報の安全管理を全うするために、**管理区域について次に掲げる措置**を講じることを求める。

- 管理区域に対する**立入りを管理及び制限する措置**（例えば、次に掲げる事項）
  - 生体を含む２要素以上の手法（例えば、顔、指紋、静脈、ICカード等）による認証を組み込んだ入退室の管理
  - 監視カメラによる入退室に関する常時の監視
  - 仮名加工医療情報を取り扱う機器を収納したラックに対する不正なアクセス（不要なアクセスを含む。）の防止（例えば、施錠、固定等）
- 管理区域外の**機器の管理区域への持込みを管理及び制限する措置**（例えば、手荷物の検査、入退室管理簿の整備等）
- 管理区域を常時監視するための**カメラその他の装置を備え付ける措置**（例えば、次に掲げる事項）
  - 管理区域を監視するためのカメラを設置する箇所
  - 端末装置を操作する取扱者の手元を鮮明に記録しないような監視カメラの映像に関するフレームレート
  - 監視カメラの映像を保存する方法及び期間
  - 主務府省又は認定作成事業者による監督のための監視カメラの映像の閲覧に関する手続

認定利用事業者の安全管理措置に関する基準（物理的安全管理措置 (2)）

(3) 機器の紛失若しくは盗難又は不正な持出しの防止等（新GLⅣ-14-3-3参照）

✓ 仮名加工医療情報の取扱いに係る機器の紛失又は盗難を防止するとともに、当該機器又は仮名加工医療情報の不正な持出しを防止するため、管理区域及び取扱区域の区別にも応じて、次に掲げる措置を講じることを求める。

- 【Ⅰ型認定の場合のみ】管理区域内の**機器の持出しを管理及び制限する措置**
  - 例えば、手荷物の検査、入退室管理簿の整備、ワイヤによる機器の固定等
- 【Ⅰ型認定・Ⅱ型認定共通】管理・取扱区域における端末装置によって取り扱われる**仮名加工医療情報が盗み見られるリスクを低減するための措置**
  - 例えば、間仕切りの設置・座席配置の工夫、のぞき見対策のシートの貼付、パスワードスクリーンセイバーの設定、スクリーンショット・画面撮影の禁止、取扱者以外の者の取扱区域に対する立入りの限定
  - なお、取扱区域については、取扱者以外の者の立入りを禁止する必要は必ずしもないが、職員証のある者や研究室の鍵を貸与された者のみの立入りを認めるなど、不特定多数の者が取扱区域に立ち入ることのないよう適切な制限が設けられた環境とする必要がある。
- 【Ⅰ型認定・Ⅱ型認定共通】取扱区域における端末装置について、**取扱者以外の者による端末装置の操作や仮名加工医療情報の閲覧を制限するための措置**（例えば、次に掲げる事項）
  - 監視カメラの設置、端末装置等の操作時のPC内蔵カメラの利用、研究開発責任者若しくは安全管理責任者又はその指名する者による監視その他の適切な手段による取扱区域の監視
  - 上記の監視記録の保存及び記録の改ざん防止のための措置
  - 主務府省又は認定作成事業者による監督のための監視記録の確認に関する手続

(4) 分析成果物の外部への持出し（新GLⅣ-14-3-4参照）

✓ 仮名加工医療情報を利用して行った分析の結果から得られた成果物（中間成果物を含む。）を外部に持ち出す場合には、仮名加工医療情報の漏えい等事態や仮名加工医療情報の第三者提供に該当することのないよう留意する必要がある。

- この点、**仮名加工医療情報から作成された統計情報や、仮名加工医療情報を機械学習の学習用データセットとして用いて生成した学習済みパラメータ（重み係数）**については、特定の個人との対応関係が排斥される限度で「個人に関する情報」に該当しないため、成果物として管理・取扱区域の外部に持ち出し第三者に提供することが可能。

✓ 成果物の外部への持出しを行う場合には、仮名加工医療情報を提供した認定作成事業者による監督の下で、当該認定作成事業者との事前の取決めに従い、適切な措置を講じる必要がある。

- 例えば、認定作成事業者による成果物の事前確認及び持出しの許可が考えられるが、必ずしもこのような対応を必須とするものではなく、**成果物の内容・性質・規模や持出し後の用途（組織内での利用か一般への公表が想定されるか等）に応じて適切に事前の取決めを行い、当該取決めに基づく措置を実施**すれば足りる。

認定利用事業者の安全管理措置に関する基準（物理的安全管理措置 (3)）

(5) 復元不可能な手段での消去又は廃棄（新GLⅣ-14-3-5参照）

【Ⅰ型認定の場合】

✓仮名加工医療情報の保有については、認定事業を実施するために必要な範囲で最小限度とすることが求められることから、仮名加工医療情報の提供に当たっては当該情報の利用の態様に十分配慮して必要な保有期間を取り決める必要がある。

✓そして、当該保有期間の終了後には、漏えい等事態が生じないよう、次に掲げる措置を講じることを求める。

- **復元不可能な手段による仮名加工医療情報の消去又は当該情報が記録された機器の廃棄**（例えば、専用のツール又はコマンドの実行、暗号技術検討会及び関連委員会（CRYPTREC）によって安全性が確認された暗号アルゴリズムを用いた暗号化消去（Ｐ）、物理的な破壊等）
- 上記の消去又は廃棄に関する記録の作成及び保存並びに認定作成事業者への報告

【Ⅱ型認定の場合】

✓認定利用事業者は、認定作成事業者が管理するVisiting環境においてのみ仮名加工医療情報を取り扱うこととなることから、予め認定作成事業者により定められたポリシーに則り、適切な利用期間を設定するとともに、**当該期間経過後には、認定作成事業者の監督の下で、利用を終了するための適切な措置を実施すること**を求める。

認定利用事業者の安全管理措置に関する基準（技術的安全管理措置 (1)）

(1) 仮名加工医療情報を処理できる者の限定（新GLⅣ-14-4-1参照）

【Ⅰ型認定の場合】仮名加工医療情報を取り扱う施設設備に不特定多数人がアクセスする環境では、漏えい等事態を生じるおそれがあるため、取扱者の認証等を適切に行うために、認定事業管理情報等を取り扱う機器について**必要最小限のアクセス権限を付与するとともに、アクセス権限の付与を受けた取扱者を識別し、かつ、認証した上で、必要最小限の操作を認可するよう設定し、かつ、管理する措置**を講じることを求める。その際の具体的な手段としては、例えば以下が考えられるが、**最新の技術動向を踏まえた合理的な水準を確保できるよう、適切な認証等を実現する**必要がある。

- アクセス権限の付与及びパスワードの利用に関するポリシーの設定
- アクセス権限の付与を受ける取扱者の限定及び取扱者の識別のためのユーザIDの付与
- 生体を含む２要素以上の手法（例えば、顔、指紋、静脈、ICカード、パスワード等）による個々の取扱者の認証
- 個々の取扱者に係る一定の回数を超える認証の失敗に際してのユーザIDの効力の停止
- 個々の取扱者に認可される操作の限定

【Ⅱ型認定の場合】認定作成事業者より付与された認証情報を、定められたポリシーに則り、適切に管理及び利用することを求める。

(2) 不正アクセス行為の防止（新GLⅣ-14-4-2参照）

【Ⅰ型認定の場合】仮名加工医療情報を取り扱う施設設備についてサイバー攻撃等の不正アクセス行為に対して脆弱性を抱える環境では、漏えい等事態を生じるおそれがあるため、**①仮名加工医療情報を取り扱う機器のネットワークにおける不正なアクセス（不要なアクセスを含む。）を制御する措置**、及び、**②仮名加工医療情報を取り扱う機器における脆弱性に対応する措置**を講じることを求める。②の具体的な手段としては、例えば、以下の事項を実施することが考えられるが、**最新の技術動向を踏まえた合理的な水準を確保できるよう、適切な措置を講ずる必要がある**。

- オペレーティングシステム（OS）、ミドルウェア（DBMS）、アプリケーション等のソフトウェア及びファームウェアについて、サポート期限等を定期的に把握した上で、その影響を評価した結果に基づき、必要かつ適切なバージョンアップを実施する等の対策
- これらのソフトウェア及びファームウェアについて、脆弱性の有無を定期的に確認した上で、その影響を評価した結果に基づき、必要かつ適切なセキュリティパッチを適用する等の対策
- ウイルス対策ソフトウェアの利用及びそのパターンファイルの定期的な更新
- 不要なソフトウェアの動作（起動を含む。）の停止
- 組織として許可されないソフトウェアの導入の防止

【Ⅱ型認定の場合】認定作成事業者から利用を許可又は貸与された機器を、認定作成事業者との事前の取決めに基づき定められたポリシーに則り、適切に利用することを求める。

認定利用事業者の安全管理措置に関する基準（技術的安全管理措置 (2)）

(3) 電子計算機及び端末装置の動作の記録並びに操作の検知及び制御（新GLⅣ-14-4-3参照）

【Ⅰ型認定の場合】仮名加工医療情報を取り扱う電子計算機及び端末装置を始めとする機器については、動作（アクセスを含む。）の履歴（ログ）の記録が、不正アクセスの検知、漏えい等事態に関する原因の究明等に資する重要な情報となることから、これらの機器の動作の履歴については、**ログを２年以上保存し、ログの改ざん又は不正な消去を防止した上で、基幹系システム及び端末装置の動作の履歴に関するログの収集、監視及び分析を定期的に実施すること**が求められる。そこで、申請書類においては、次に掲げる事項を明らかにする必要がある。

- ログを保存する措置
- ログの改ざん又は不正な消去を防止する措置
- ログの収集、監視及び分析を定期的に実施する措置
- 通常想定されない操作を検知し、それに応じて操作を制御する措置

【Ⅱ型認定の場合】認定作成事業者から利用を許可又は貸与された機器を、認定作成事業者との事前の取決めに基づき定められたポリシーに則り、適切に利用することを求める。

(4) 電気通信回線との接続に伴う漏えい等の防止（新GLⅣ-14-4-4参照）

【Ⅰ型認定の場合】仮名加工医療情報の送受信や移送に際しては、**データの機密性、完全性及び真正性を確保する必要があること**から、以下の措置を講じることを求める。

- 電気通信による方法で仮名加工医療情報を送受信する場合（認定利用事業者内で物理的に離れた区域に送受信する場合を含む。）には、専用線等※を用いて安全性が確保された手段によること。
  ※ 専用線を用いる方法のほか、例えば、**仮想的に他のネットワーク環境と分割されたLAN、暗号化を併用したIP-VPNサービス若しくは広域イーサネットに用いられる仮想専用線又は政府推奨暗号を用いた暗号化を併用した高度なインターネットVPNに用いられる仮想専用線等であって、専用線と同等の安全性が確保されると認められるもの**を用いる方法が考えられるが、最新の技術動向を踏まえた合理的な水準を確保できるよう、適切な方法による必要がある。
- 仮名加工医療情報を取り扱う機器について、データの機密性、完全性及び真正性が確保されるよう適切な構成とすること（例えば、以下のような措置を講ずることが考えられるが、最新の技術動向を踏まえた合理的な水準を確保する必要がある）。
  - 認定作成事業者からの受信専用の「一次受信サーバ」と、仮名加工医療情報の保存、操作及び解析等の用に供する「解析サーバ」とを置き、両者の間は専用線等で接続するなど、**オープンなネットワーク環境へのアクセスを必要最小限にとどめ、不正又は不要なアクセスを制御する措置**
- 仮名加工医療情報に係る**データ及びストレージ等を適切に暗号化すること**。
- ソフトウェア等の更新を適切に実施すること。

【Ⅱ型認定の場合】認定作成事業者との事前の取決めに基づき定められたポリシーに則り、仮名加工医療情報の送受信又は移送を適切に行い、かつ、認定作成事業者から利用を許可又は貸与された機器を適切に利用することを求める。

認定利用事業者の安全管理措置に関する基準（その他の措置）

(1) 共同利用の場合における安全管理の確保（新GLIV-14-5-1参照）

✓ 認定利用事業者間での仮名加工医療情報の共同利用は、仮名加工医療情報の第三者提供禁止の原則の例外として特別に認められるものであることを踏まえ、**共同利用を行う場合は、共同利用に係る安全管理に関する責任の所在を明確にした上で、必要かつ適切な措置を講じる必要**がある。

✓ その一環として、共同利用を実施する全ての認定利用事業者及び当該共同利用に係る仮名加工医療情報の提供を行った認定作成事業者の間で、以下の事項を取り決める必要がある。

① 共同して利用する**事業者の範囲**及び利用する**仮名加工医療情報の項目**
② 共同利用者のうち、仮名加工医療情報の管理について責任を有する認定利用事業者（「**責任事業者**」）**の名称**
③ 各共同利用者における仮名加工医療情報の**取扱責任者、問合せ担当者及び連絡先**
④ 共同利用する仮名加工医療情報の取扱いに関する事項
⑤ 共同利用する仮名加工医療情報の取扱いに関する取決めが遵守されなかった場合の措置
⑥ 共同利用する仮名加工医療情報に関する漏えい等事態その他の事件・事故が発生した場合の報告・連絡に関する事項
⑦ 共同利用を**終了する際の手続**

※ 共同利用に係る安全管理に関する責任の所在について主務府省があらかじめ把握しておく観点から、認定申請の際には、**共同利用の予定の有無及び共同利用を実施する場合の責任事業者の名称を明らかにし、主務府省に届け出る必要がある**こととするが（共同利用者の追加・変更に伴い責任事業者が変更となる場合には変更の届出が必要となる。）、それ以外の事項については、事前の認定・届出事項ではなく、認定作成事業者の監督の下で適切に実施する必要がある。