令和３年12月８日	資料２
第６回匿名介護情報等の提供に関する専門委員会	

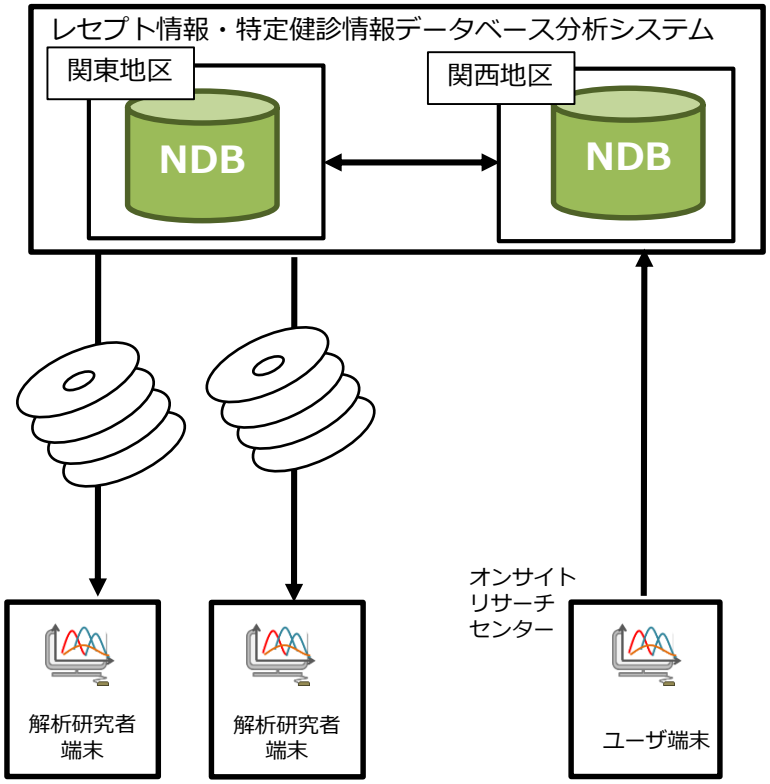
医療・介護データ等の解析基盤（HIC）開発の進捗

令和３年12月８日

厚生労働省保険局医療介護連携政策課
厚生労働省老健局老人保健課

医療・介護データ等の解析基盤（HIC）の開発

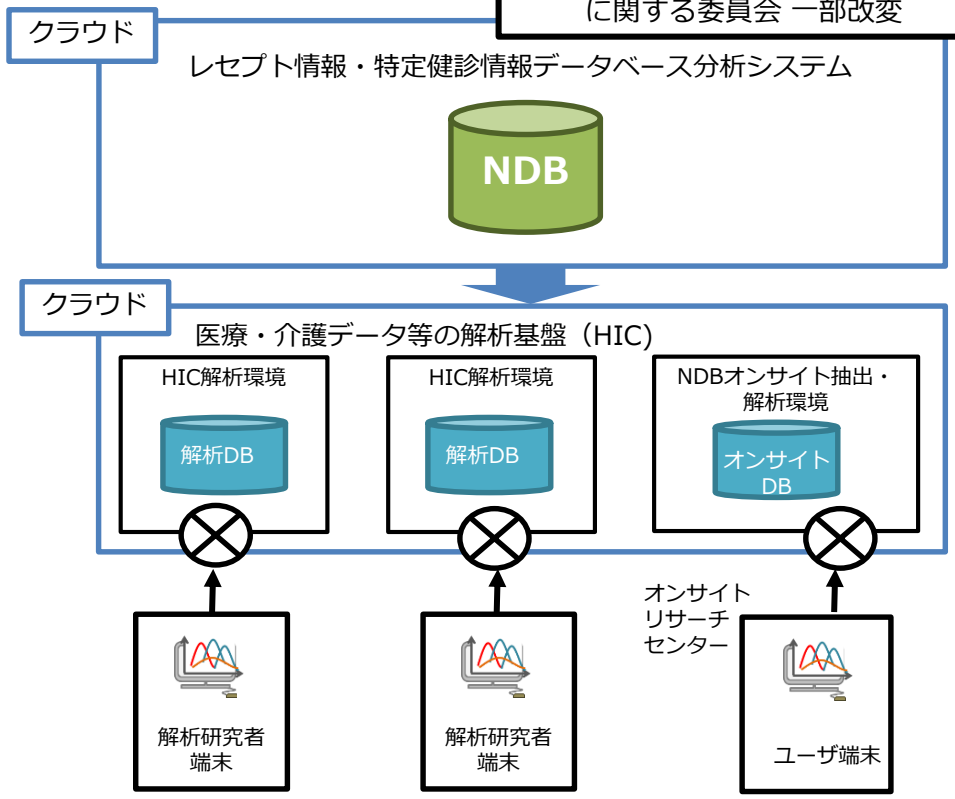
第3回 匿名医療・介護情報等の提供に関する委員会 一部改変



<現行イメージ>

○データ抽出等の作業増大への対応に、システム処理を行う機器の増設が必要となる。

○災害等によりシステム障害が発生した場合、システムが復旧するまで作業が滞る。



<リプレース後イメージ>

○クラウド化に伴い、データ量や処理量に合わせて最適な処理能力の増減を行うことができる。

○複数拠点でシステム（国内のみ）が稼働しているため、被害のないサーバーを利用し、迅速な対応が可能となる。

（※）HIC：Healthcare Intelligence Cloud

HICの機能（予定）

	想定されるユーザ像
【ポータル機能】 NDB・介護DB等の提供申出、利用及び終了に至る一連の手続きを電子化されたポータルサイトにて行う。同時に、データベース研究をしたことのない研究者等に向けて、教育・啓発のためのコンテンツの形成や各種マスターの共有等を行う。	全ての研究者
【探索的利用環境】 データベース研究をしたことはあるが、NDB・介護DB等を利用したことがない研究者等がダミーデータを用いて探索・試行的に分析するための環境を提供する。 （今後、ダミーデータの仕様について検討。）	NDB・介護DB等を利用したことのない研究者
【HIC解析環境】 専門委員会の審査にて承諾された提供申出ごとに、利用者に対して解析環境を提供する。（今後、安全管理措置を含め、HIC解析環境の利用に関するガイドラインについて検討。）	専門委員会で提供申出が承認された研究者

解析環境の環境要件（AWS）

- CPU/メモリ/ストレージ等のハードウェア要件は、データ量や研究目的に応じて選択制とする
- OSはWindows Server 2019 または Ubuntu 20.04 LTSを選択
- データベースはPostgreSQLを準備
- 統計解析等のためにSPSS、Stata、R、Python等を準備

今後のスケジュールと解析環境の試行的利用（案）

	2022年度	2023年度	2024年度
ポータル機能	調査研究・設計・開発		運用開始 順次、機能やコンテンツを拡充
探索的利用環境	データの仕様検討		運用開始
HIC解析環境	試行的利用 HICガイドライン検討・作成		本格利用

※2023年度中の開始可能となったタイミングで順次開始

【解析環境の試行的利用】

- 一部のNDB・介護DBの提供申出に対して、匿名医療情報等の提供に関する専門委員会及び匿名介護情報等の提供に関する専門委員会にて個別審査を実施した上で、HIC解析環境の試行的利用を開始してはどうか。
- 試行的利用においては、匿名レセプト情報・匿名特定健診情報等情報の提供に関するガイドライン（以下、「NDBガイドライン」という。）及び匿名介護情報等の提供に関するガイドライン（以下、「介護DBガイドライン」という。）について、インターネット接続に関する部分を除いて、基本的に準用することとしてはどうか。（NDBガイドライン及び介護DBガイドラインの改正）
- その上で、NDBガイドライン及び介護DBガイドラインはHIC解析環境の実情に合っていないとの指摘もあることから、試行的利用者からの意見を踏まえて、本格利用に向けて、新しくHIC解析環境の利用に関するガイドラインを作成することを検討してはどうか。

（参考）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

第6　提供申出に対する審査
4　審査基準
（4）匿名レセプト情報等の利用場所、保管場所及び管理方法
以下の①から③の措置が取扱者の利用形態を勘案した上で、適切に措置されていること。
① 基本的な事項
ⅰ）匿名レセプト情報等の利用場所・保管場所は国内又はオンサイトリサーチセンターであること。
ⅱ）匿名レセプト情報等を複写した情報システムの利用場所、保管場所及び管理方法は、あらかじめ申し出られた施錠可能な物理的なスペースに限定されており、原則として持ち出されないこと。
またオンサイトリサーチセンターを利用する場合は、匿名レセプト情報等を格納した情報システムの利用場所、保管場所及び管理方法は、オンサイトリサーチセンター内とし、本ガイドライン、利用規約及び運用管理規定を遵守すること。また、オンサイトリサーチセンターから中間生成物又は 最終生成物 を含めたデータの持ち出しを行う場合には、本ガイドラインに準じた匿名レセプト情報等の利用、保管、管理を行うこと。
ⅲ）匿名レセプト情報等を複写した情報システムは、インターネット等の外部ネットワークに接続しないこと。
ⅳ）提供された匿名レセプト情報等は、あらかじめ申し出られた取扱者のみが利用することとし、その他の者へ譲渡、貸与又は他の情報との交換等を行わないこと。
ⅴ）提供する匿名レセプト情報等については全体として個人情報に準じた取扱いを徹底する観点から、匿名レセプト情報等の利用、保管及び管理について、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 令和3 年 1 月）の「6 医療 情報システムの基本的な安全管理」等に定められた措置に準じた措置として、以下②及び③に規定する当該ガイドライン中に示された、情報の安全管理と同等の措置が講じられていること。なお、提供申出者は、ここに規定されている事項以外についても上記ガイドラインの趣旨を十分に理解した上で適切なセキュリティ対策を 講ずる よう努めることが望ましい。
② 匿名レセプト情報等の利用に限らず提供申出者が一般的に具備しておくことが望ましい条件
ⅰ）個人情報保護方針の策定・公開
a）個人情報保護に関する方針を策定し、公開していること。
b）個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。
c）提供される 匿名 レセプト情報等についても当該方針に従った対応を行うこと。
ⅱ）情報セキュリティマネジメントシステム（ISMS ）の実践（必ずしも ISMS 適合性評価制度における認証の取得を求めるものではない。）
a）情報システムで扱う情報をすべてリストアップしていること。
b）リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。
c）このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。
d）リストアップした情報に対してリスク分析を実施していること。
e）この分析の結果得られた脅威に対して、この「（ 匿名 レセプト情報等の利用場所、保管場所及び管理方法」に示す対策を行っていること。
ⅲ）組織的安全管理対策（体制、運用管理規程）の実施
a） 情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定を行うこと。ただし所属機関が小規模な場合において役割が自明の場合は、明確な規程を定めなくとも良い。
b） 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
c） 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
d） 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。
ⅳ）人的安全対策の措置
a）提供申出者は、個人情報の安全管理に関する施策が適 切に実施されるよう措置するとともに、その実施状況を監督するために、以下の措置をとること。
・法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用契約時に併せて守秘・非開示契約を締結すること等により安全管理を行うこと。
・定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。
・従業者の退職後の個人情報保護規程を定めること。
b）提供申出者が組織の事務、運用等を外部の事業者に委託する場合には、当該事業者の内部における適切な個人情報保護が行われるようにするために以下の措置を行うこと。
・受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。
・保守作業等の情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果の確認を行うこと。
・清掃等の直接情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
・委託事業者が再委託を行うか否かを明確にし、再 委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。
c）プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が個人情報にアクセスする場合には、罰則のある就業規則等
で裏づけられた守秘契約等の秘密保持の対策を行うこと。
ⅴ）情報の破棄の手順等の設定
a）個人情報保護方針の中で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。
b情報 処理機器自体を破棄する場合、必ず専門的な知識を有する者が行うこととし、機器に残存した読み出し可能な情報がないことを確認すること。
c情報の破棄を委託する場合には、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 令和3 年 1 月）の「6．6人的安全対策 2. 事務取扱 受託 業者の監督及び守秘義務契約」に準じた対策を行うこと。さらに、委託する提供申出者等は確実に情報の破棄が行われたことを確認すること。

（参考）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

③匿名レセプト情報等の利用に際し講じなければならない安全管理措置
ⅰ）組織的安全管理措置
a）利用者及び 取扱者の権限、責務及び業務を明確にすること。
b） 運用管理規程等において次の内容を定めること。
・理念（基本方針及び管理目的の表明）
・匿名レセプト情報等の適正管理に係る基本方針
・契約書・マニュアル等の文書の管理
・匿名レセプト情報等に係る管理簿の整備
・匿名レセプト情報等の漏洩、紛失又は毀損時の対応
・その他リスクに対する予防、発生時の対応
・機器を用いる場合は機器の管理
・記録媒体の管理（保管及び授受等）の方法
・監査
・苦情・質問の受付窓口
・その他提供申出者が対応を行っていると申し出た事項
c）オンサイトリサーチセンターを利用する場合は、厚生労働省およびオンサイトリサーチセンターにて定められた運用管理規程等を遵守すること。
ⅱ）人的安全管理措置
a) 取扱者は以下のいずれにも該当しないことを確認すること。
・法、健康保険法 大正 11 年法律第 70 号 、介護保険法 平成9年法律第 123 号 、統計法 昭和 22 年法律第 18 号 、個人情報の保護に関する法律、行政機関の保有する個人情報の保護に関する法律又は独立行政法人等の保有する個人情報の保護に関する法律又はこれらの法律 平成 15 年法律第 59 号 に基づく命 令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から起算して5年を経過しないこと
・暴力団員による不当な行為の防止等に関する法律（平成3年法律第 77 号）第2条第6号に規定する暴力団員 又は 暴力団員でなくなった日から5年を経過しない者
・その他、匿名レセプト情報等を利用して不適切な行為をしたことがある等で取扱者になることが不適切であると厚生労働大臣が認めた者
b）提供申出 者 （匿名レセプト情報等の提供を受けた場合にあっては利用者 は取扱者に対し、匿名レセプト情報等を取り扱う上で必要な教育及び訓練を行うこと。
ⅲ）物理的安全管理措置
a）匿名レセプト情報等が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
b）匿名レセプト情報等が参照可能な区画を明示し、取扱者以外の者の無断立ち入りを防ぐ対策を 講ずる こと。また、匿名レセプト情報等を参照できる端末が設置されている区画は、運用管理規程に基づき、許可された者以外立ち入ることが出来ないよう、施錠等の対策を 講ずる こと。ただし、本対策項目と同等レベルの他の取りうる手段がある場合にはこの限りではない。
c）匿名レセプト情報等を物理的に保存している区画への入退管理を実施すること。例えば、以下の措置を実施すること。
・入退者には名札等の着用を義務付け、台帳等に氏名等を記入することにより入退の事実を記録すること 。
・入退者の記録を定期的にチェックし、その妥当性を確認すること。
・入退管理記録は、利用終了後少なくとも1年は保管すること。
d）情報システム等の匿名レセプト情報等が存在する機器に盗難防止用チェーンを設置すること。
e）窃 視防止の対策を実施すること。
f）オンサイトリサーチセンターを利用する場合には、入退室管理を含めオンサイトリサーチセンターによって定められた運用管理規程に従い、匿名レセプト情報等を利用すること。
g）匿名レセプト情報等の消去にあたっては、専用ソフトウェア等を用い、復元不可能な形で行うこと。

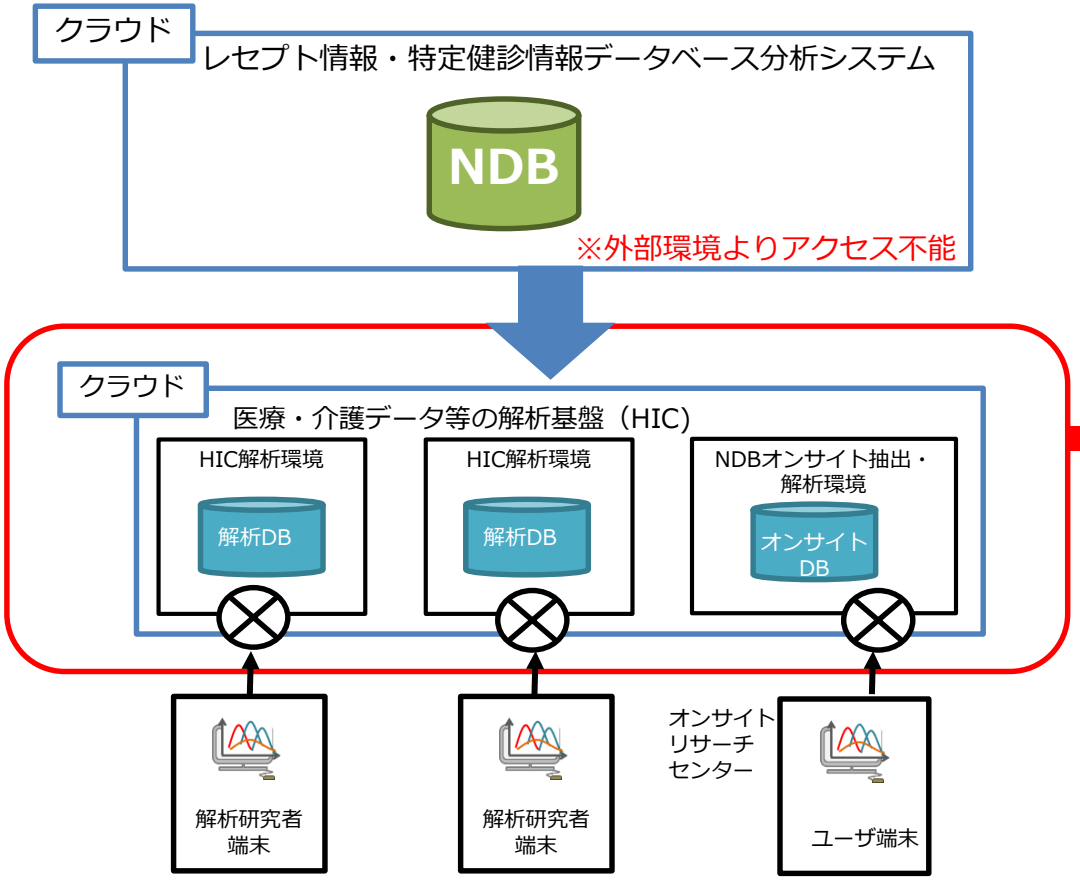
（参考）匿名レセプト情報・匿名特定健診等情報の提供に関するガイドライン

ⅳ）技術的安全管理措置
a）匿名レセプト情報等を利用する情報システムへのアクセスにおける取扱者の識別と認証を行うこと。
b）上記ａ）の取扱者の識別・認証に用いる手段として、セキュリティ強度を考慮し、IC カード等のセキュ リティ・デバイス＋パスワード、IC カード＋バイオメトリクス 指紋、静脈、虹彩のような取扱者の生体的特徴を利用した生体計測 やユーザ ID・パスワード＋バイオメトリクスといった2つの独立した要素を用いて行う方式二要素認証 を採用することを求める。この場合は、必ずしもパスワードの定期的な変更は必要ない。ただし、何らかの事情で上記の実装が困難な場合は、ユーザID とパスワードを組み合わせた認証を行うこと。その場合は、以下の事項に留意すること。
・パスワードは定期的に変更し（最長でも2ヶ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた8文字以上の文字列が望ましい。なお、下記の要件を含め、適切に設定された 13 文字以上のパスワードを用いる場合は定期的な変更は求めない。
・類推しやすいパスワードを使用しないこと。
・匿名レセプト情報等が複写された情報システムが複数の者によって利用される場合にあっては、当該システム内のパスワードファイルでパスワードは必ず暗号化 不可逆変換が望ましい。）され、適切な手法で管理及び運用が行われること。利用者識別に IC カード等他の手段を併用した場合は、システムに応じたパスワードの運用方法を運用管理規程にて定めること。
・取扱者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、取扱者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載 本人確認を行った書類等のコピーを添付）し、本人以外が知りえない方法で再登録を実施すること。
・システム管理者であっても、取扱 者のパスワードを推定できる手段を防止すること。（ 設定ファイルにパスワードが記載される等があってはなら ない。）
c)取扱者が匿名レセプト情報等を利用する情報システムの端末から、長時間離席する際に、あらかじめ認められた取扱者以外の者が利用する恐れがある場合には、クリアスクリーン等の防止策を 講ずること。
d)匿名レセプト情報等を利用する情報システムへのアクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも取扱者のログイン時刻、アクセス時間並びにログイン中に操作した取扱者が特定できるようにすること。
e)匿名レセプト情報等を利用する情報システムはアクセス記録機能を備えたものであること。仮に当該機能がない場合には、業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。
なお、記録等は利用終了後少なくとも１年は保管すること。
f)匿名レセプト情報等を利用する情報システムにアクセスログへのアクセス制限を行い、アクセスログの不当な削除、改ざん及び追加等を防止する対策を 講ずること。
g）上記ｆ）のアクセスの記録に用いる時刻情報は信頼できるものであること。
h）原則として、匿名レセプト情報等を利用する情報システムには適切に管理されていないメディアを接続しないこと。ただし、システム構築時に、やむをえず適切に管理されていないメディアを使用する場合には、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持を行うこと。
i）匿名レセプト情報等の保存・利用に際しては、インターネット等の外部ネットワークに接続した情報システムを使用しないこと。
j）匿名レセプト情報等の利用終了後には、情報システム内に記録された匿名レセプト情報等及び中間生成物を消去することに加え、消去後に当該機器を外部ネットワークに接続する際には、あらかじめコンピューターウイルス等の有害ソフトウェアが無いか検索し、ファイアウォールを導入するなどの安全対策に十分配意すること。
ⅴ）情報及び情報機器の持ち出しについて
提供された匿名レセプト情報等の利用、管理及び保管は、事前に申し出た場所でのみ行うこととし、外部への持ち出しは行わないこと。
ただし、外部委託や共同研究の場合など、やむをえず、あらかじめ申し出た取扱者の間で最小限の範囲で中間生成物等の受け渡しを行う場合には、提供申出者が以下の措置を講じており、匿名レセプト情報等の受け渡しに準用していること。
a）組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
b）運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
c）情報を格納した媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程等に定めること。
d）あらかじめ運用管理規程等で定めた匿名レセプト情報等の盗難、紛失時の対応を取扱者に周知徹底するとともに、当該対応について教育を行うこと。
e）取扱者は、匿名レセプト情報等が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。
f）匿名レセプト情報等の持ち出しに利用する情報機器の起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避け、定期的にパスワードを変更する等の措置を行うこと。
g）盗難、置き忘れ等に対応する措置として、匿名レセプト情報等を暗号化したり、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
h）匿名レセプト情報等が保存された情報機器を他の外部媒体と接続する場合には、情報漏えい、改ざん等の対象にならないようにコンピューターウイルス対策ソフトの導入等の対策を施すこと。
i）匿名レセプト情報等の持ち出しについて、取扱者が個人保有の情報機器（パソコン等）を使用する場合であっても、上記のf）、g）、h）と同様の要件を遵守させること。
j）オンサイトリサーチセンターからの情報の持ち出しについて
オンサイトリサーチセンターからの中間生成物又は最終生成物を含めた情報を持ち出す際には、事前に任意の様式で厚生労働省へ報告することとし、厚生労働省は、当該研究の持ち出し予定情報とあらかじめ承諾された形式が整合的であるか確認することとする。また、必要に応じて専門委員会の委員が確認を行うこととする。
ただし、中間生成物又は最終生成物を持ち出す場合には、事前に申し出た場所でのみ行うこととし、外部への持ち出しは行わないこと。
なお、外部委託や共同研究の場合など、やむをえず、あらかじめ申し出た取扱者の間で最小限の範囲で中間生成物等の受け渡しを行う場合には、提供申出者が上記a）～i）の措置を講じており、匿名レセプト情報等の受け渡しに準用していること。
ⅵ）その他の安全管理措置
a）匿名レセプト情報等の取扱いに関する研究及び業務を外部委託するときは、当該委託を受けた者が講ずる匿名レセプト情報等の安全管理のために必要かつ適切な措置について必要な確認を行うこと。
b）外部委託を行う提供申出者は、外部委託先に対する必要かつ適切な監督を行うこと。
c）取扱者以外の者が匿名レセプト情報等を取り扱うことを禁止すること。

（参考）NDBとHICのセキュリティ要件

第3回 匿名医療・介護情報等の提供に関する委員会 一部改変

○ 医療・介護データ等の解析基盤における情報セキュリティ対策は、情報に対する不正アクセスや情報漏洩及び改ざんを防止するため、気密性、完全性及び可用性の観点から下記の要件を満たすように実施する。
○ 下記要件は、政府機関等の情報セキュリティ対策のための統一基準群等に基づいている。
○ 厚生労働省が準備するHICの具体的なセキュリティ要件はP.９,10の通り。



- 不正プログラム対策
- ファイアウォール機能
- 主体認証機能
- アクセス制御
- ログの保管、分析、管理
- 時刻同期機能
- 利用状況の監視
- 不正行為の監視
- 不正通信の遮断
- 脆弱性対策
- 保存情報(ストレージ)の暗号化
- 通信経路の分離(侵害の防止)
- 無害化処理
- プライバシー保護
- システムの構成管理

（参考）HICのセキュリティ要件１

情報セキュリティ対策	対策に係る要件
不正プログラム対策	不正プログラム（ウイルス、ワーム、ボット等）による脅威に備えるため、感染を防止する機能を備えること。
	設定情報、ウイルスチェックパターンファイルの更新状況、未知のウイルス検知に関する稼働状況及びウイルス被害状況を確認できる環境を整備する設計とすること。
	ウイルス対策に係るポリシー（定時スキャンの設定等）、パターンファイル更新方法等が一括して設定可能な設計とすること。
	未知のウイルスへの対策が可能な仕組みを導入することが望ましい。その際には、検知可能なファイル種別が多数あることに留意すること。
	トラフィックのペイロードをスキャンし不正プログラム（マルウェア）マルウェアによる不正通信（コマンドアンドコントロール通信）、およびゼロデイ攻撃や脆弱性の検知を行い、リアルタイムに検知・遮断する仕組みを提供することが望ましい。
ファイアウォール機能	本システム内ネットワーク、及びインターネット境界におけるネットワーク通信のフィルタリングを実現するためのファイアウォール機能を提供すること。
主体認証機能	認証管理システムを導入し、主体認証を行うこと。なお、本機能はクラウドサービスの認証サービスとは別に用意し、クラウドサービスの認証サービスと連携した管理ができること。
	正当な利用者のみにサービスを提供するため、2つ以上の主体認証方式(多要素主体認証方式)を導入すること。
アクセス制御	アクセス制御を実施し、不正アクセス等の技術的な脅威に対し、ソフトウェアへのログイン制御を行い、本システムの機密性、完全性及び可用性を確保可能な設計とすること。
	海外からのアクセスを遮断できること。
ログの保管、分析、管理	クラウド環境及びソフトウェア等で取得したログを保管し、必要に応じて参照が可能な設計とすること。保管期間について受託者は、厚生労働省と協議を行い決定される期間とする。
	不正行為の発生原因の特定に利用するために、ログの分析が可能な設計とすること。
時刻同期機能	本システム内の仮想サーバ及びクラウドサービスに対して統一的な時刻を提供し、本システム内で生成されるログに記録されるタイムスタンプが、統一された時刻に基づいたものとすること。
利用状況の監視	外部からクラウド上のサービスやリソースの運用管理が可能な監視ツールを備えること。
	監視ツールから、特定の操作を実施した際のレスポンスタイムを基準に、利用者ポータルのサービス正常性を監視すること。
	監視ツールを用いてイベント監視を行うこと。
	システム利用状況を定期的に確認し、一定期間利用していないユーザの通知、アカウント停止、削除等の処理の自動化ができること。

医療・介護データ等の解析基盤の開発及び
レセプト情報・特定健診等情報データベースシステムの更改等一式要件定義書より抜粋

（参考）HICのセキュリティ要件２

第3回 匿名医療・介護情報等の提供に関する委員会 資料

情報セキュリティ対策	対策に係る要件
不正行為の監視	データの不正利用等侵害に迅速に対処するため、インターネット回線とクラウド基盤の接続点の通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。なお、その際に、ゼロトラストセキュリティモデル（NIST SP800-27など）を考慮することが望ましい。ただし、ゼロトラストセキュリティモデルで示す機能全てを導入することを求めるものではない。
	不自然なアクセス（システム管理者や利用者等内部からのアクセスや標的型攻撃等）に関して、ふるまいの検知を自動的に行うこと。
不正通信の遮断	不正通信を検知し、脅威インテリジェンス情報に基づいて、不正アクセス先の宛先や端末を、即時に自動遮断する仕組みを備えること。なお脅威インテリジェンスはIPやURL両方を保有すること。
脆弱性対策	構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。
	脆弱性対策を行うとしたクラウド環境及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。
	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を行う方法（手順等）を備えること。
保存情報(ストレージ)の暗号化	本システムで利用するストーレージにおいて、保存情報(ストレージ)の暗号化を実現するための機能を提供すること。
	暗号化に使用する暗号アルゴリズムについては、「電子政府推奨暗号リスト」を参照し決定すること。
通信の暗号化	利用者端末とクラウドサービス間は、TLS等で暗号化された通信を用いること。
	解析用データを利用者端末からクラウドサービスにアップロード/ダウンロードする際には、TLS等で暗号化された通信を用いること。
	システム運用保守業務担当端末とクラウドサービス間は、TLS等で暗号化された通信を用いること。
通信経路の分離 (侵害の防止)	他利用者に払い出された解析環境へアクセスできないよう、通信回線上で分離すること。
無害化処理	解析用データを利用者端末から外部に持ち出す必要がある場合に備え、データファイルのスキャンによるウイルス・マルウェア対策機能を備えること。
プライバシー保護	情報システムにアクセスする利用者のアクセス履歴、入力情報等を当該利用者が意図しない形で第三者に送信されないようにすること。
システムの構成管理	情報セキュリティインシデントの発生要因を減らすとともに、情報セキュリティインシデントの発生時には迅速に対処するため、構築時の情報システムの構成（ハードウェア、ソフトウェア及びサービス構成に関する詳細情報）が記載された文書を提出するとともに文書どおりの構成とし、加えて情報システムに関する運用開始後の最新の構成情報及び稼働状況の管理を行う方法又は機能を備えること。