資料３－２

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

医療・介護データ等解析基盤（HIC）の現状と取り組みについて

厚生労働省
保険局医療介護連携政策課
Ministry of Health, Labour and Welfare of Japan

NDBデータ提供の抜本的見直し（概要）

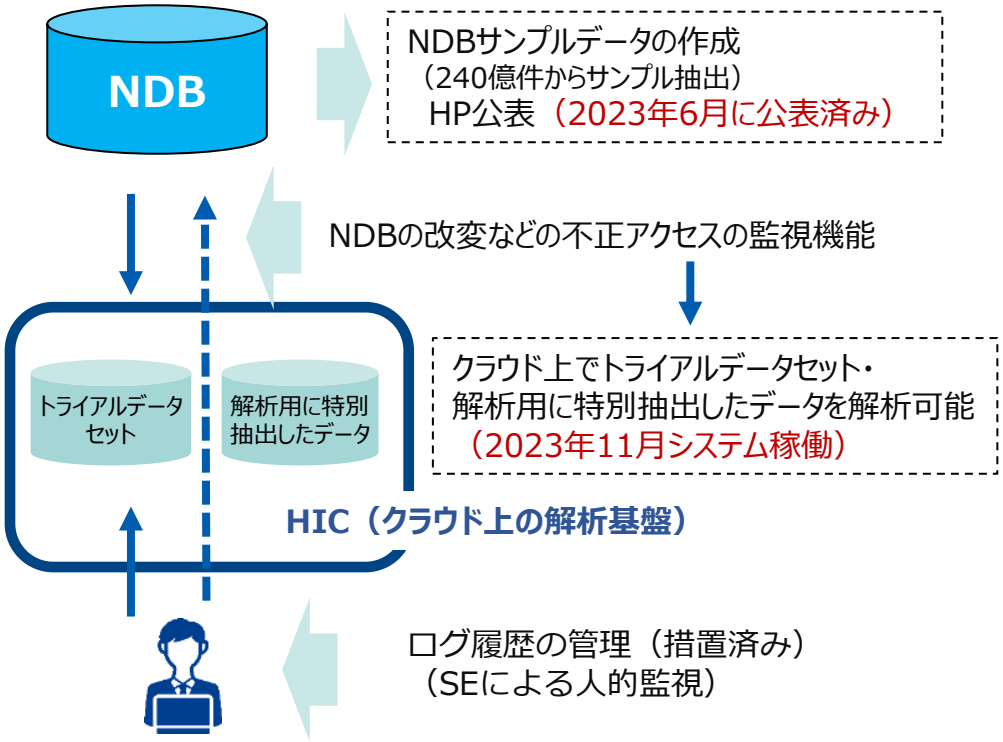
令和５年６月29日
第165回社会保障審議会医療保険部会
資料２
更新

○ **直ちに、サンプルデータの作成、トライアルデータセットの作成、不正アクセス監視機能の実装に取り組み、**
- **2023年6月、NDBサンプルデータを厚労省HPに公表**
- **2023年秋、リモートアクセスでトライアルデータセット・解析用に特別抽出したデータを解析可能**

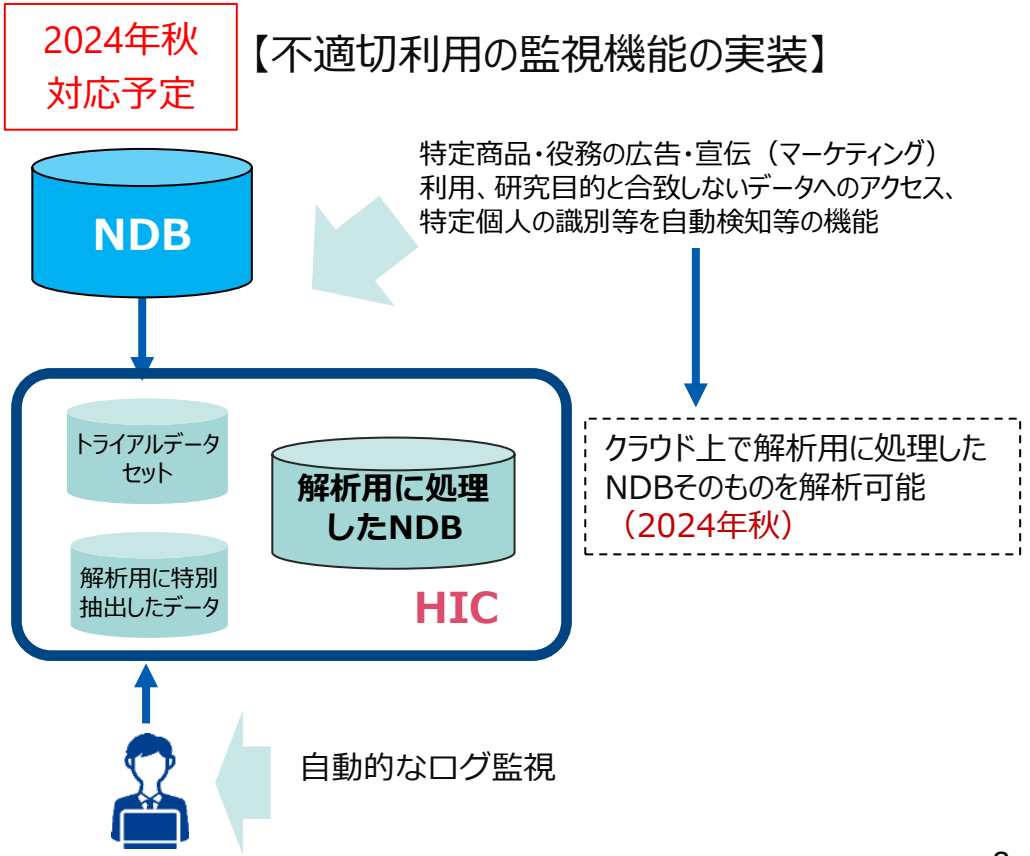
○ **さらに、不適切利用等の監視機能やポータルサイトの機能拡充を開発・実装の上、**
- **2024年秋、リモートアクセスの解析データを拡大**
- **申請からデータ提供まで平均390日の現状に対し、申請〆切を毎月設定し、申請から原則７日で処理**

※申請が月5件程度であることを踏まえ、当面月1回を設定するが、今後申請件数が増えれば複数回設定する

対応済 【不正アクセスの監視機能の実装】

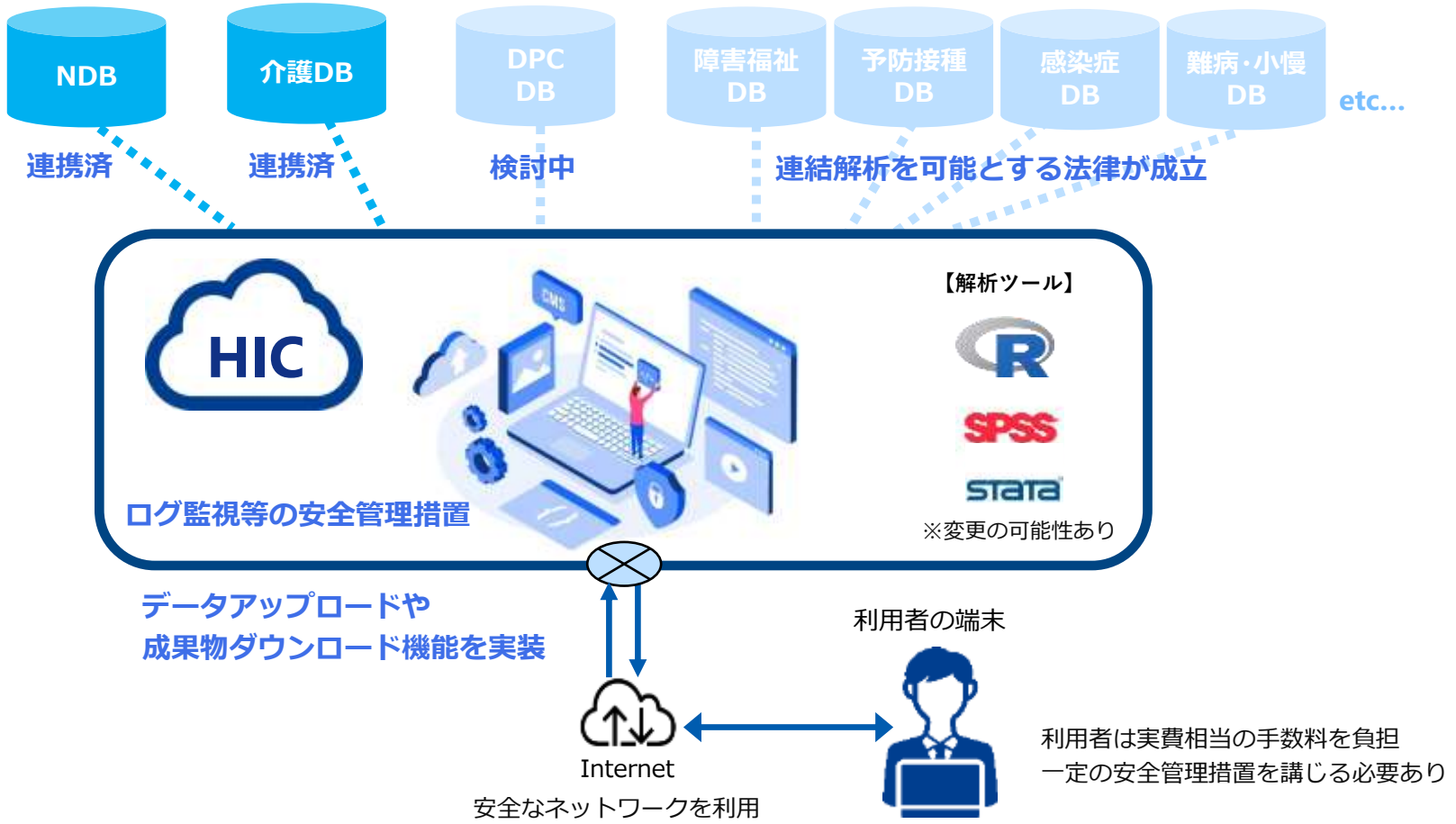


2024年秋対応予定 【不適切利用の監視機能の実装】



医療・介護データ等解析基盤（HIC）

- 医療・介護データ等解析基盤（HIC）は、クラウド上に構築されたプラットフォーム（2023年秋に稼働予定）
- 研究者は、リモートアクセスで安全な環境に接続し、公的DBを解析することが可能。
- 解析ツールや持ち込むデータ・マスタ（容量制限あり）のアップロード、成果物をダウンロードする機能を実装。

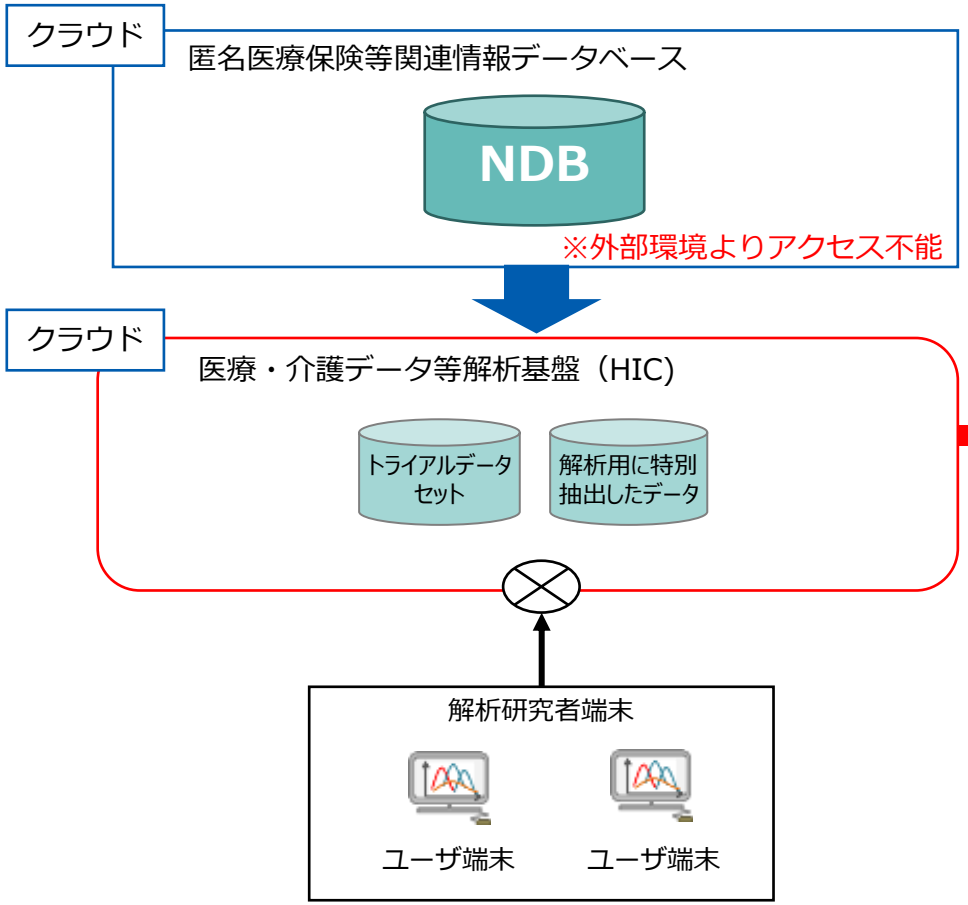


NDBとHICのセキュリティ要件

システム要件

令和３年３月19日
第３回匿名医療情報等の提供に関する専門委員会
資料１改変

○ 医療・介護データ等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、機密性、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。



- 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。

（参考）HICのセキュリティ要件２

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。

HICの安全管理措置

利用者に求める要件

令和５年９月２０日
第１３回匿名医療・介護情報等の提供に関する委員会
資料１
改変

- 安全管理措置については、組織的、人的、物理的、技術的、その他の安全管理措置について、NDBガイドラインを踏まえて設定する。
- オンプレミス環境を前提としたNDBと異なりクラウド上の解析環境であることから、物理的・技術的な安全管理措置については、他の同様の環境であるC-CATや米国VRDCの安全管理措置等を参考に設定する。

C-CAT; Center for Cancer Genomics and Advanced Therapeutics, 本邦がんゲノム情報センター
VRDC; Virtual Research Data Center, Medicareの取扱業者のためのガイドライン

物理的・技術的な安全管理措置

- NDB特別抽出に倣いつつ、HICではログイン可能な者を制限できる点を鑑みて、特別抽出のように取扱者以外の立入制限・入退管理までは求めず、事前に申し出た、職員等に立入が制限された特定の区画において利用できることとする。（サンプリングデータセット・集計表と同様）
- HICの安全管理措置の概要は下記（特にHIC固有の事項は赤字）

利用端末取扱区画の特定	・事前に申し出た、特定された区画（国内に限る）でのみ使用すること ・職員証を持つ者等に入室が制限された特定された区画でのみ使用すること ・利用可能な区画は施錠すること　など
盗難・覗き見防止	・利用端末は施錠された研究室内で保管すること ・利用者が利用端末から離席する際にはログオフ又はパスワード付きクリアスクリーン等の防止策を講ずること ・HICを利用中の画面の撮影、録画、スクリーンショットの取得を禁止すること ・利用端末のデータを追跡・遠隔からの命令等により消去する機能を設けること　など
利用者の認証	・パスワードの規則を遵守すること。類推しやすいパスワードは使用しないこと ・一定回数の入力ミスでHICアカウントがロックされること　など
不正ソフトウェア対策	・OS等のセキュリティ対策のアップグレードを行い、マルウェア対策ソフトウェアをインストールすること　など
ネットワーク対策	・公衆無線LANへの接続を行わないこと、無線LANの不正アクセス対策　など

（参考）利用者が遵守する主な安全管理措置の比較

令和５年９月２０日
第１３回匿名医療・介護情報等の提供に関する委員会
資料１

	HICガイドライン	NDBガイドライン（特別抽出の場合）
組織的措置	運営管理規定を整備	運営管理規定を整備
人的措置	法令・契約違反者等は利用不可	法令・契約違反者等は利用不可
入退室管理	利用場所の施錠 職員等以外の入室禁止	利用場所の施錠 入退室のチェック、取扱者以外の入室禁止
盗難・覗き見防止	クリアスクリーン等による覗き見防止 スクリーンショットやスマートフォン等での撮影禁止 利用端末を追跡・遠隔からの命令等により消去する機能	クリアスクリーン等による覗き見防止 スクリーンショットやスマートフォン等での撮影禁止 窃盗防止用チェーン等設置による盗難防止
認証・識別	パスワードの規則遵守 二重認証	パスワードの規則遵守 二重認証
不正ソフトウェア対策	セキュリティ対策のアップグレード 不正なログオン等が認められれば、サービスの利用停止	セキュリティ対策のアップグレード
ネットワーク対策	公衆無線LANに接続しないこと 無線LANの不正アクセス対策 その他、ネットワークの規定	外部ネットワークに接続しないこと
消去	ー （運用保守業者が削除）	復元不可能な手段で廃棄すること
ログ管理	ー （運用保守業者が管理）	アクセスログの確認・管理

情報の持ち込み及び持ち出しについて

令和５年９月２０日
第１３回匿名医療･介護情報等の提供に関する委員会
資料１

オンサイトリサーチセンターと同様、研究に必要なマスターやSQL等の持ち込みを許可する。

HICの利用に関するガイドライン	（参考）NDBの利用に関するガイドライン
第６の１　HIC解析環境への情報の持ち込み 一部のデータ（マスターやSQL等）は、厚生労働省の確認後に、HIC解析環境に持ち込むことが可能である。 ・持ち込みが許可されているデータについては、各医療・介護データ等のガイドラインを参照すること。 ・ウイルスチェック等、不正なソフトウェア等の混入を防ぐ対策を十分行うこと。 ・厚生労働省の指定の窓口に、持ち込みたい情報について申し出ること。厚生労働省はデータを確認の上、HIC解析環境にアップロードする。	（該当する記載無し）

生成物は、各医療・介護データ等の基準に従い、厚生労働省の確認を経てHICからダウンロード可能である。

HICの利用に関するガイドライン	（参考）NDBの利用に関するガイドライン
第６の２　HIC解析環境からの生成物の取り出し 個票を含まない生成物（SQLを含む）は、厚生労働省の確認後に、利用者がダウンロード可能である。 ・厚生労働省の指定の窓口に、持ち出したい情報について申し出ること。厚生労働省はデータに個票が含まれていないこと、及び該当する医療・介護データ等の公表物の基準を満たしていることを確認の上、持ち出しを許可する。 ・持ち出し後のデータをさらに加工した生成物を用いて公表を行う場合、再度公表物確認が必要になる場合があるため、利用した医療・介護データ等の提供に関するガイドラインに従うこと。	利用者は、NDBデータによる研究成果を、提供申出書に記載した公表時期、方法に基づき公表すること。公表前に、公表予定の研究成果を厚生労働省へ報告し、確認・承認を求めること（以下「公表物確認」という。）。公表物確認を厚生労働省に依頼する前に、利用者自ら当該研究の成果とあらかじめ承諾された公表形式が整合的か点検すること。厚生労働省は、個人情報保護の観点から２の「研究の成果の公表にあたっての留意点」の公表形式の基準を満たしているかを確認（必要に応じて専門委員会の委員が確認を行う）し、承認する。 オンサイトリサーチセンター利用形態ⅰ（成果物のみ持ち出す場合）又はHIC利用の場合は、オンサイトリサーチセンター又はHIC上での公表物確認終了後に、HICからの成果物の持ち出しが可能となる。

HIC利用終了後の措置等

令和５年９月２０日
第１３回匿名医療・介護情報等の提供に関する委員会
資料１

利用者からHIC利用終了書を受領した後、厚生労働省が解析環境を破棄する。

HICの利用に関するガイドライン	（参考）NDBの利用に関するガイドライン
第７の１　HIC利用の終了 利用者は、HIC利用を終了したときは、遅滞なく、利用終了書を厚生労働省に提出しなければならない。厚生労働省は、利用者より利用終了書を受領後、利用停止に係る作業を行い、生成物を含む解析環境を破棄する。利用終了書提出以降は、利用者はHICの利用等はできないものとする。	利用者は、高確法に基づき、NDBデータの利用を終了したときは、遅滞なく、提供を受けたNDBデータ、中間生成物及び最終生成物を消去しなければならない。CD-R又はDVDでNDBデータの提供を受けた場合は、利用終了時に媒体を厚生労働省へ返却すること。 そして、利用場所ごとのデータ措置兼管理状況報告書に消去を実施した証明書を添付した上で、厚生労働省に提出すること。データ措置兼管理状況報告書は、利用場所毎に提出するものであり、変更届出による利用場所の廃止時も提出するものとする。 HICでデータの提供を受けた場合は、HICガイドラインに従うこと。

（参考）他の医療・介護データ等との連結解析に向けて

令和５年９月２０日
第１３回匿名医療･介護情報等の提供に関する委員会
資料１
更新

EBPMや研究利用の基盤として、NDBの利便性・価値向上を図っていくため、

NDBと他の医療・介護データ等との連結解析を順次進めていく。

識別子はID4，ID5

区分	DB名	主なデータ	NDBとの連結の意義・必要性	連結の検討状況等
公的	介護DB	・介護レセプト ・要介護認定情報	要介護者の治療前後の医療・介護サービスの利用状況の把握・分析に資する。	令和２年10月開始
	DPCDB	・DPCデータ （診療情報、請求情報）	急性期病院の入院患者の状態の把握が可能となり、急性期医療の治療実態の分析に資する。	令和４年４月開始
	障害福祉DB	・給付費等明細書情報 ・障害支援区分認定情報	障害者の治療前後の医療・障害福祉サービスの利用状況の把握・分析に資する。	**連結解析を可能とする法案が成立。施行に向けて検討中。**
	予防接種DB	・予防接種記録 ・副反応疑い報告	予防接種の有無を比較した、ワクチンの有効性・安全性に関する調査・分析に資する。	**連結解析を可能とする法案が成立。施行に向けて検討中。**
	感染症DB	・発生届情報	感染症の治療実態と予後の把握・分析に資する。	**連結解析を可能とする法案が成立。令和６年４月施行予定。**
	難病DB	・臨床調査個人票	網羅的・経時的な治療情報を得ることが可能となり、より詳細な治療実態の把握・分析に資する。	**連結解析を可能とする法案が成立。連結に向けて検討中。**
	小慢DB	・医療意見書		
	全国がん登録DB	・届出対象情報 ・死亡情報	各種がんの各ステージ分類毎による治療実態と予後の把握・分析に資する。	引き続き検討中
民間	次世代DB	・医療機関の診療情報	医療情報と連結・分析を可能にすることにより医療分野の研究開発を促進する。	**連結解析を可能とする法案が成立。令和６年５月までに施行予定。**