令和3年3月26日	資料1
第3回匿名医療･介護情報等の提供に関する委員会	

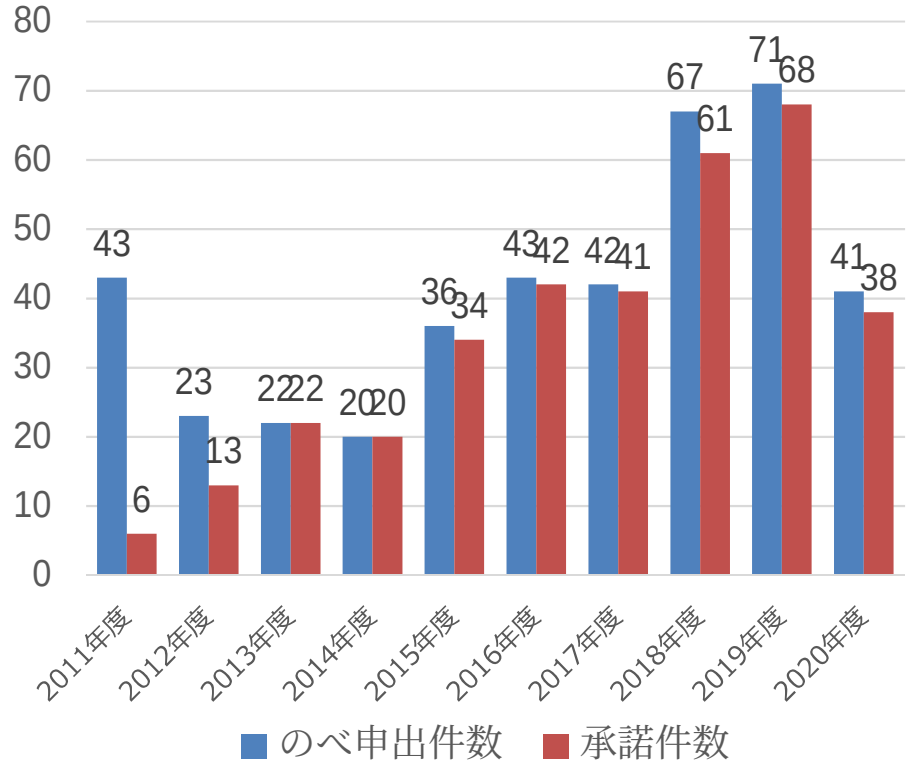
NDBの更改と医療･介護データ等の解析基盤の開発着手

令和３年３月26日

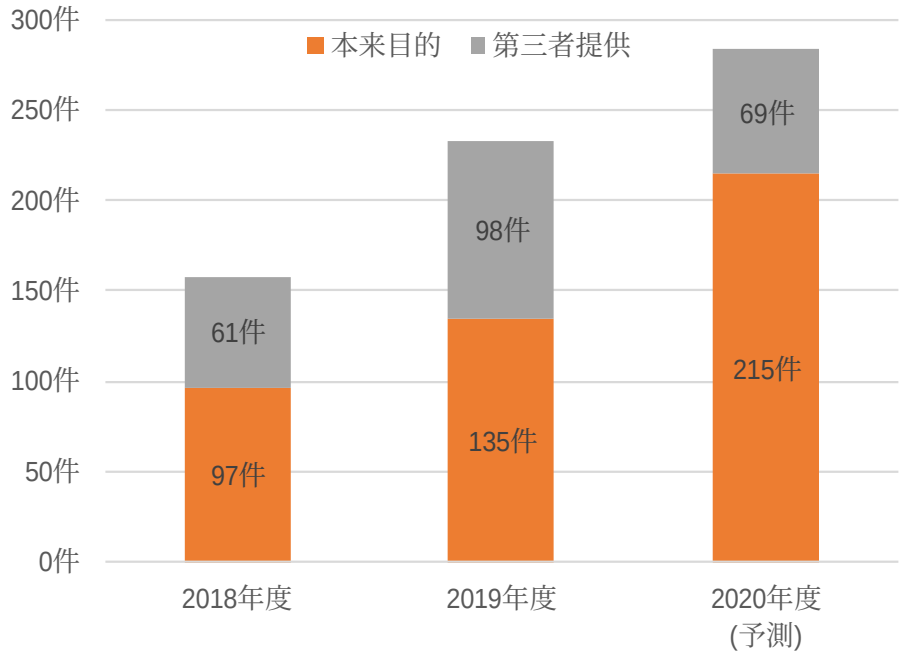
厚生労働省保険局医療介護連携政策課
保険データ企画室

NDB本来目的利用と第三者提供の実績

○ NDBは2009年に稼働開始以降、医療費適正化目的（本来目的）に利用されている。
○ 2011年からは有識者会議の審査を経て、第三者の研究者等への提供が開始された。
○ 2020年10月の法改正により、民間事業者を含めた幅広い主体への提供が可能となった
○ 第三者申出件数は、これまで累計で408件あり、345件承諾されている。申出数は年々増加し、2018年度以降は年間50件を超えている。
○ 加えて、本来目的の抽出作業が直近２年間で２倍以上になっている。



NDB第三者提供申出と承諾件数



NDB抽出作業件数（本来目的／第三者提供）

※　408件の申出に対し、345件を承諾（2020年12月末時点）

NDBの稼働状況

○ 本来目的での利用や第三者提供の増加に伴い、提供までの期間が長期化している。
○ 特に2019～2020年度にかけ本来目的の抽出作業が急増している。
○ 現行のNDBサーバは2014年にリリース（関東）し、2017年にはサーバ増強（関西）を行ったが、老朽化やスペック上の制限等から案件増加に対応できないことが課題となっている。

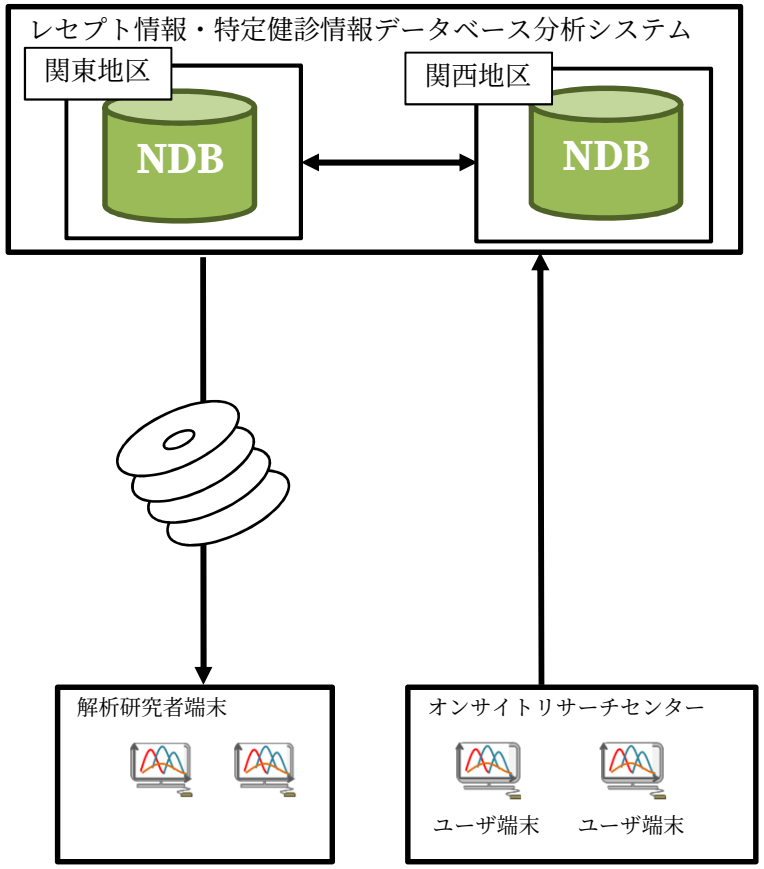
提供申出が承諾された日からNDBデータが提供されるまでに要した平均日数
（サンプリングデータセットを除く）

	提供済み	未提供	取り下げ	平均所要日数	平均所要日数(未提供込み)
2017年度	41	1	1	170.5	192.9
2018年度	49	1	3	281.2	292.0
2019年度	41	16	0	203.1	271.4

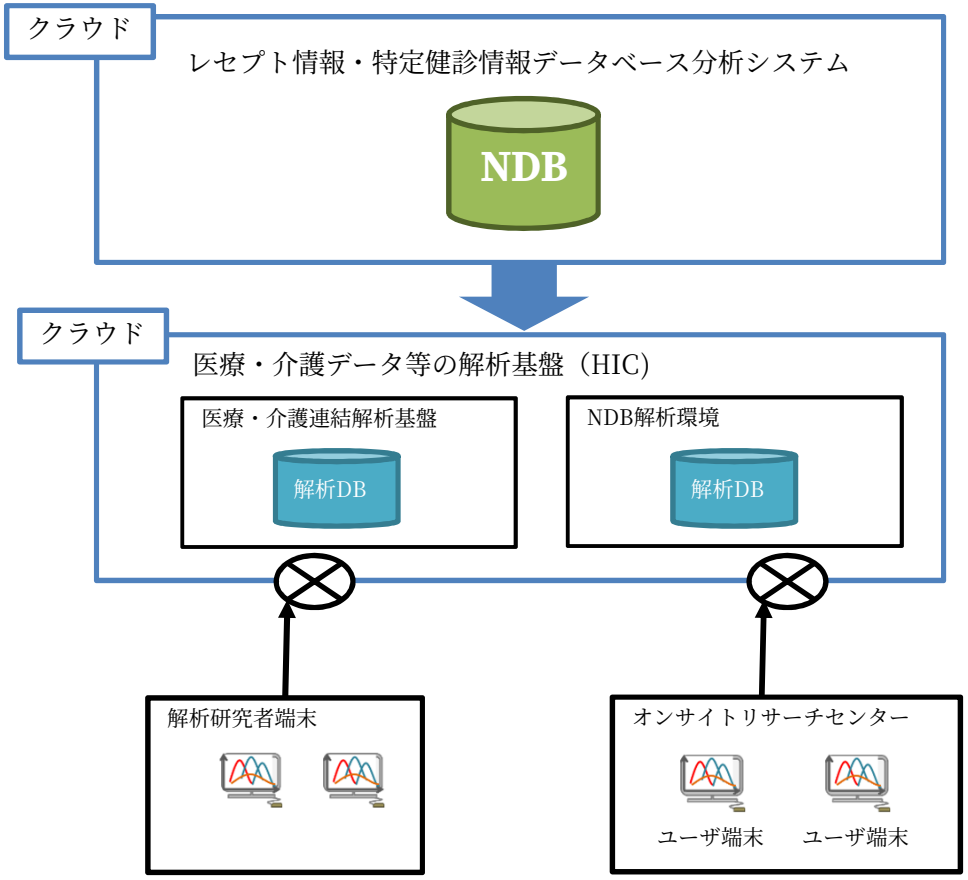
※平均所要日数(未提供込み)は、未提供の提供申出が2021年3月19日（専門委員会開催日）に全て提供された場合

NDBの更改とHICの開発開始

○ 2021年3月から2022年3月にかけて、NDBの更改および医療・介護データ等の解析基盤（HIC）の開発を行う。
○ 国のクラウドバイデフォルトに則り、フルクラウド環境で構築する。
○ 医療介護連携政策課が工程管理支援事業者を直接調達し、データヘルス改革推進本部・内閣官房情報通信技術（ＩＴ）総合戦略室と連携しつつリリースを目指す。



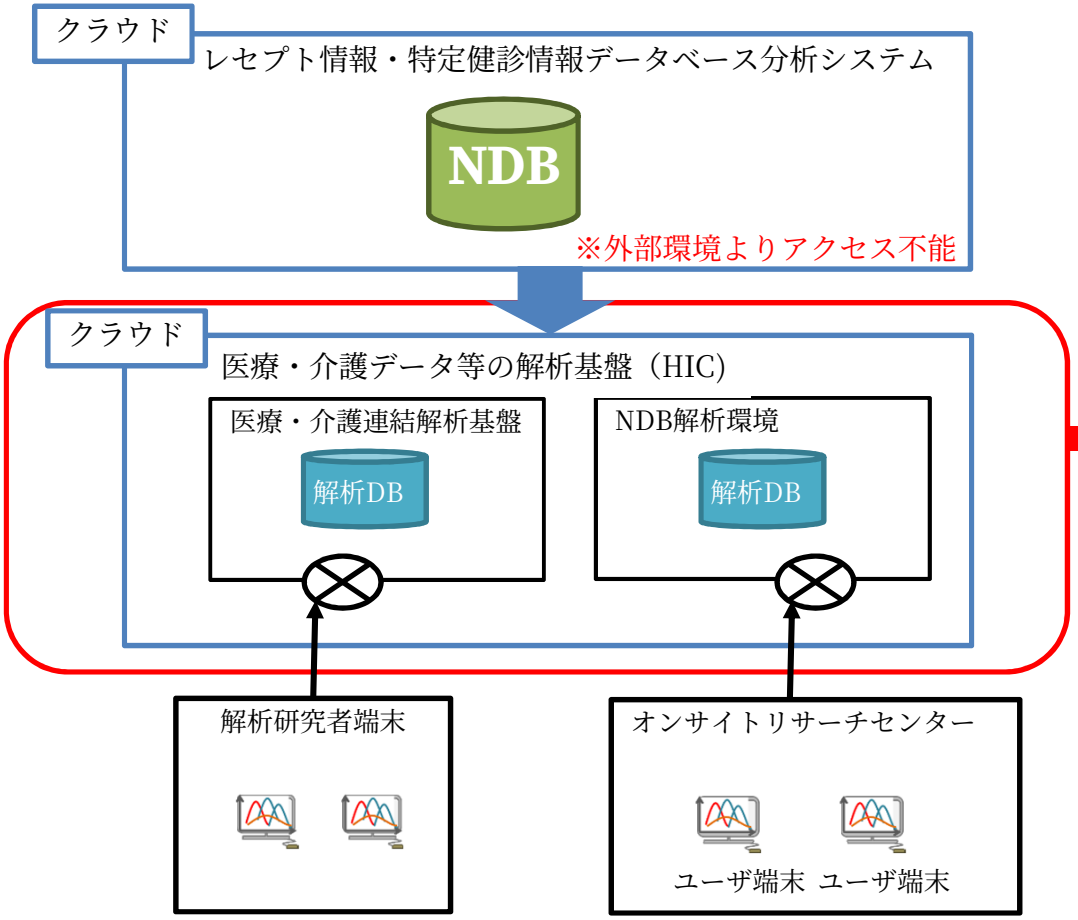
＜現行イメージ＞



＜リプレース後イメージ＞

NDBとHICのセキュリティ要件

○ 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。



- 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

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

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。