資料37

情報公開･個人情報保護審議会　諮問・報告事項

件名	国保情報集約システムにおける生体認証による照合情報の外部提供等について

内容は別紙のとおり

条例の根拠

【諮問】

◇第 12 条第 2 項第 4 号（外部提供）
◇第 17 条第 1 項第 4 号（外部電子計算機との結合）

（担当部課：健康部医療保険年金課）

事業の概要

事業名	国保情報集約システムの操作業務
担当課	医療保険年金課
目　的	国保情報集約システムにおける操作者を確認するため、照合情報を記録する。
対象者	健康部医療保険年金課の職員
事業内容	1　概要 平成３０年４月から、国民健康保険制度改革による都道府県化に伴い、東京都国民健康保険団体連合会（以下「国保連」という。）が運営する国保情報集約システムの運用が開始され、医療保険年金課において国保情報集約システムに係る事務を処理することとなる。このシステムにおいてはマイナンバー（個人番号）を活用する。マイナンバーの利用事務に対しては、総務省の「自治体情報システム強靭性向上モデル」において、強固なセキュリティ対策として「二要素認証」を講じることが推奨されている。 このことにより、区では操作者が正当なアクセス権限を有していることを確認するため、国保情報集約システムへのログイン時にＩＤ及びパスワードのほか、なりすましや偽造が困難な生体認証（静脈認証）を導入することで、情報セキュリティ対策の一層の強化を図り、個人情報等の重要情報の保護及び情報漏えい防止対策をさらに徹底する。 なお、照合情報（対象職員の生体認証情報）は、国民連が管理する国保情報集約システムサーバ群のデータベースに暗号化して格納され、人事異動により医療保険年金課の職員でなくなったときに職員が削除処理を行う。 2　対象者数 医療保険年金課の職員（国保資格係、国保給付係及び庶務係） ３０名（平成２９年度現在）

別紙（外部提供関係）

◇外部提供（第 12 条第 2 項第 4 号関係）・・・諮問事項

件名　国保情報集約システムにおける生体認証による照合情報の外部提供について（情報の追加）

保有課（担当課）	医療保険年金課
登録業務の名称	国保情報集約システムの操作業務
登録業務の目的	なりすまし防止
外部提供の相手方	東京都国民健康保険団体連合会
外部提供を行う理由	国民健康保険制度改革に伴い、平成３０年４月から、国保情報集約システムを利用した事務運用を行う。総務省の「自治体情報システム強靭性向上モデル」では、マイナンバー利用環境において 二要素認証が推奨されおり、区では情報セキュリティ対策の一層の強化を図り、個人情報等の重要情報の保護及び情報漏えい防止対策をさらに徹底するため
外部提供を行う情報項目	資料３７－３(10)職員情報　生体認証による照合情報
外部提供を行う際に使用する記録媒体	電磁的媒体（国保情報集約システム認証サーバ（国保連が運用管理））
外部提供に当たっての区としての情報保護対策	１　主管課において、ユーザの管理を行って提供する個人情報を限定する。
外部提供の相手方としての情報保護対策	１　国保連が定めた関係者（システム運用者等）以外はサーバルームへの入室は行えないようにサーバルームは常時施錠管理する。 ２　サーバルーム入室時の身分確認、サーバルーム内での身分証明書の常時着用、入退室に関する記録保持を遵守し、サーバルームへの入退室管理を適切に行い物理的に不審者の入室や機器破壊から資産を保護する。 ３　ユーザ管理を随時行い、削除するユーザについては生体情報の消去を行う。
外部提供の時期	平成２９年１２月２５日から（次年度以降も同様の外部提供を行う）
緊急時の外部提供における本人通知の状況	＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

別紙（電子計算機の外部結合関係）

◇外部との結合（第 17 条第 1 項第 4 号関係）・・・諮問事項

件名　国保情報集約システムにおける生体認証による照合情報の外部結合（情報の追加）について

保有課（担当課）	医療保険年金課
登録業務の名称	国保情報集約システムの操作業務
結合される情報項目（だれの、どのような項目か）	1　個人の範囲 医療保険年金課の職員 2　記録項目 資料３７－３(10)職員情報　生体認証による照合情報 3　記録するコンピュータ 国保情報集約システム認証サーバ（国保連が運用管理）
結合の相手方	東京都国民健康保険団体連合会
結合する理由	国民健康保険制度改革に伴い、平成３０年４月から、国保情報集約システムを利用した事務運用を行う。総務省の「自治体情報システム強靭性向上モデル」では、マイナンバー利用環境において 二要素認証が推奨されているため。
結合の形態	既存の専用線（ＬＡＮ）
結合の開始時期と期間	平成２９年１２月２５日から（次年度以降も同様の外部提供を行う）
情報保護対策	1　専用線及びＩＰアドレスによる接続端末の制限 2　パスワードによるアクセス制限 3　不正アクセス対策（ファイアーウオール等）マルウエア対策、脆弱化対策等、物理対策（情報窃盗・侵入対策）等のセキュリテイ対策はシステム基盤として実装、実施している。 4　最新のセキュリテイパッチ・ウイルスパターン適用により、通信及びデーターのセキュリテイを確保する。