（資料３）

住民基本台帳に関する事務に係る特定個人情報保護評価書の点検について

所管課等名　民生局地域支援部窓口サービス課（システム係）

１　事務の説明

住民を対象とする行政を適切に行い、また、住民の正しい権利を保障するため、住民に関する正確な記録が整備されるよう、住民基本台帳の管理等を行います。

２　事務の中で取り扱う特定個人情報ファイル

・住民基本台帳ファイル
・本人確認情報ファイル
・送付先情報ファイル

３　特定個人情報ファイルを利用して行う事務

・個人を単位とする住民票を世帯ごとに編成し、住民基本台帳を作成します。
・転入届、転居届、転出届、世帯変更届等の届出又は職権に基づく住民票の記載、消除又は記載の修正を行います。
・住民基本台帳の正確な記録を確保するための措置を行います。
・転入届に基づき住民票の記載をした際の転出元市町村に対し通知します。
・本人又は同一の世帯に属する者の請求による住民票の写し等を交付します。
（コンビニエンスストアでの申請による住民票の写し等のデータ作成及び証明書交付センターへの送信を含む）
・住民票の記載事項に変更があった際に都道府県知事に対して通知します。
・地方公共団体情報システム機構へ本人確認情報を照会します。
・住民からの請求に基づき住民票コードを変更します。
・個人番号の通知及び個人番号カードの交付を行います。
・個人番号カード等を用いた本人確認を行います。

４　特定個人情報ファイルの取扱いプロセスにおけるリスク対策

この保護評価書の中で最も重要な部分である特定個人情報ファイルの取扱いプロセスにおけるリスク対策について、特定個人情報ファイルの目的外の利用や漏えい、委託先における不適切管理のリスク及びその対策について明らかにしています。

（１）特定個人情報の入手におけるリスク対策

・住民異動届を受付ける際は、厳格な本人確認を行い対象者の情報以外の入手を防止しています。
・住民基本台帳ネットワークシステムから、対象者以外の情報は入手しません。
・住民異動届出書には、住民基本台帳法で届出に必要とされる事項以外は原則届出人に記載させません。
・住民基本台帳法関連法令及び住民基本台帳事務処理要領に基づき適正な事務処理を行い、住民に対しては適切な案内を行い、不適切な情報の入手を防止します。

（２）特定個人情報の使用におけるリスク対策

・特定個人情報の利用事務でないシステムから個人番号にアクセスできないよう制御を行っています。
・住基システムで利用できる端末を限定し、住基システムに登録した端末以外では住基システムが利用できない仕組みになっています。
・住基システムを利用する必要がある職員を限定したうえで、ユーザーIDによる識別並びにパスワード及び生体情報による認証を行います。この際、ユーザーごとに利用可能な機能を制限することで、不正利用ができない仕組みとなっています。
・認証に使用するパスワードは年１回以上、変更する運用を行っています。

（３）特定個人情報ファイルの取扱いの委託におけるリスク対策

①　委託先へのリスク対策

委託契約の中で、特記事項を付記し、特定個人情報の取扱いに関して受託者に対し、以下の内容を義務付けています。

・個人情報の漏えい、滅失、改ざん、き損及びその他の事故を未然に防止

するため必要な措置を講じること。

・委託業務の従事者以外が個人情報を取り扱うことがないよう必要な措置を講じること。

・他の業務で取り扱う個人情報と取り違えが発生しないよう措置を講じること。

・個人情報を外部に持ち出さないこと（委託者の承認を得た場合を除く）。

・従事者に対し、特定個人情報保護に関する教育及び研修を実施すること。

・特定個人情報の内容を第三者に漏らさないこと（委託業務終了後も含む）。

② 再委託先へのリスク対策

・委託業務について、原則再委託を認めていません。

・再委託を行う際は、受託者は事前に委託者に対し、再委託の範囲と再委託先を通知し、委託者の承認を受ける必要があります。

・再委託先に特定個人情報の取り扱いをさせる場合は、再委託先においても、特定個人情報の取扱いに関する特記事項を徹底させるよう受託者に求めます。

（４）特定個人情報の提供・移転におけるリスク対策

・電子記録媒体を使用したファイルの受け渡しは、媒体の受渡記録を残しています。

・ファイルの利用を開始する際は、ファイルの受け渡しの手段を問わず、あらかじめ窓口サービス課に対しデータ利用申請書を提出し、その承認を受けることが必要です。

・LANケーブルを通じファイルを利用する際は、情報システム管理担当課が、当該ファイルの利用について窓口サービス課の承認を受けた事実を確認したうえで、ファイルの利用が開始できるよう制御しています。

（５）特定個人情報の保管・消去におけるリスク対策

① 特定個人情報の保管

特定個人情報を蓄積するストレージ装置を管理区域内にのみ設置することとし、同管理区域に対し以下の制限を実施しています。

a) 管理区域は、地震、津波、火災、落雷等の災害の影響を免れる施設におくものとする。

b) 管理区域およびストレージ装置は、予期せぬ電源断があってもデータ喪失を喪失しないだけの耐性を備えさせる。

c) 管理区域へ入退室できる者を制限し、生体認証を実施する。

d) 管理区域を24時間体制で監視・録画する。

e) 管理区域への記録媒体の持込および記録媒体を隠匿しうる鞄等の持込を制限する。

また、ガバメントクラウドについては、政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っています。

また、事前に許可されていない装置等に関しては、外部に持出できないこととしています。

② 特定個人情報の消去

個人情報及び個人番号を記録した磁気ディスク等を廃棄する際は、必ずデータの消去又は物理的破壊処理をして廃棄をします。なお、特定個人情報を記録した媒体等を処分する場合は、両方の措置をします。

また、ガバメントクラウドにおいては、データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去します。

※ NIST 800-88

米国国立標準技術研究所（NIST）が発行した媒体のデータ抹消処理、廃棄に関するガイドライン

※ ISO/IEC27001

情報セキュリティマネジメントシステム（ISMS）に関する国際規格