

個人情報の保護対策は 利用目的など法律で限定

住民基本台帳ネットワークシステムでは、個人情報の保護を最も重要な課題としています。個人情報保護に係る国際的な基準を十分踏まえたうえで、制度や技術、運用などあらゆる面で次のとおり十分な対策を行っています。

① 都道府県や指定情報処理機関が保有する情報は、法律で情報（氏名、生年月日、性別、住所）と住民票コードの変更情報（本人確認情報）と言いい、本人かどうかの確認）に限定されています。



② 都道府県や指定情報処理機関が情報提供を行う行政機関の範囲や利用目的を法律で具体的に限定。行政機関が、住民から提供された情報を目的以外に利

用することを禁止しています。
③ 住民票の写しの広域交付や転入、転出の手続きの簡素化の

住民票コードは 民間が利用できない番号

① 民間部門が住民票コードを利用することは法律で禁止されています。特に民間部門が住民票コードの記録されたデータベース（整理された情報の集まり）を作成したり、金融機関との契約の際、住民票コードの告知（情報）を要求すると、刑罰（一年以下の懲役または五十万円以下の罰金）を科せられます。

② 行政機関が住民票コードを利用することも法律で具体的に限定しています。

③ 住民票コードは、無作為の番号で住民の申請により、いつでも変更できません。わが国の住民票コードは、市区町村が住民票に記載する番号で、民間が利用できない、限られた行政分野で用いられる限定的な番号です。

外部からの侵入と 内部の不正利用を防止

◆ 外部からの侵入防止
① 専用回線の利用、ファイアウォール・IDS（侵入検知装置）の設置で、不正侵入を防止しています。

② 通信を行うとき、データを暗号化し、通信相手のコンピュータの正当性を確認してから通信を行うことで、通信相手のなりすましを防止しています。

際には市区町村間で、続柄、戸籍の表示なども送信されます。しかし、都道府県や指定情報処理機関のコンピュータに保有されることはなく、通過することはありません。



③ 万が一の場合「緊急時対応計画」に基づき、ネットワークの運営を停止するなど、個人情報の保護を最優先した運営を行います。

◆ 内部の不正利用の防止

① 地方公共団体・指定情報処理機関・本人確認情報の受領者（行政機関）のシステムを操作者に秘密を守る義務を課し、刑罰を加重します（通常は一年以下の懲役または三万円以下の罰金↓二年以下の懲役または百万円以下の罰金）。

委託業者が秘密を漏らした場合も同じ刑罰に処せられます。

② 地方公共団体・指定情報処理機関・本人確認情報の受領者（行政機関）は、操作者の識別

住民基本台帳カードは 個人情報を守る高度機能を

住民基本台帳カードは、高度のセキュリティ機能を備えたICカードを採用することにより、住民ネットワークでの本人確認の利用、公的個人認証サービスでの秘密鍵などの保存カードとしての利用、市区町村の条例に規定する独自サービスでの利用を安全に行うことが次のとおり可能になっています。

① それぞれの利用目的ごとに、正当なカード利用者かどうかの確認を利用者自身が入力するパスワードで行います。

カードやパスワードによる厳格な確認を行います。正当なシステム操作者だけがコンピュータを操作できるようにしています。

③ コンピュータの使用記録を保存し、監査を行うことで、いつ、だが、コンピュータを使用したのか追跡調査が出来るようにしています。

④ 全国で地方公共団体・指定情報処理機関・本人確認情報の受領者（行政機関）のシステム操作者のセキュリティ研修会を実施しています。

⑤ 住民からの請求に応じて、都道府県知事から自己の本人確認情報の提供状況を開示できるように準備しています。

② 利用目的ごとにそれぞれ、カードとシステム間で相互の正当性を確認します。

③ 利用目的ごとの独立性を確保し、個人情報を保護するための措置として、カード内にアプリケーションファイアウォールを設け、利用の制限を行います。

④ カードのチップ部分への物理的・論理的攻撃に対する防御対策を講じます。

詳しくは、役場住民課(☎051-2113)までお問い合わせください。