

住民基本台帳ネットワークシステムにおける個人情報の保護

< 3.外部からの侵入と内部の不正利用の防止 >

外部からの侵入の防止

専用回線の利用、ファイアウォール・IDS（侵入検知装置）の設置により、不正侵入を防止します。

通信を行う際には、データを暗号化します。また、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により、通信相手のなりすましを防止します。

万が一の場合は、「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

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）のシステム操作者に守秘義務を課し、刑罰を加重します。

（通常は1年以下の懲役または3万円以下の罰金 2年以下の懲役または100万円以下の罰金）

また、委託業者が秘密を漏らした場合も、同じ刑罰が科せられます。

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）において、操作者用ICカードやパスワードによる厳格な確認を行い、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ます。また、システム操作者ごとに住基ネットが保有するデータへ接続できる範囲を限定します。

コンピュータの使用記録を保存し、定期的な監査を行うことにより、いつ、だれが、コンピュータを使用したのか、追跡調査ができるようにします。

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ます。