電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（住民基本台帳ネットワークシステムセキュリティ基準）

住民基本台帳ネットワークシステムの稼働に伴い、市町村長が住民票の記載等を行った際の電気通信回線を通じた通知の方法、本人確認情報の記録及び保存の方法等についてセキュリティの確保に必要な技術的基準を定めるものとする（総務省告示）。

１．体制、規程等の整備

- システムの企画、開発及び運用に関する責任体制を確立し、規程等を整備
- 操作及びセキュリティ対策についての教育及び研修に関する計画を策定し、実施体制を確立
- 職員を支援し、誤操作等の発生を防止するための問い合わせ窓口を設置
- 住民基本台帳ネットワークシステムの**監査の体制を確立し、システム改善を実施**
- 本人確認情報の漏えいのおそれがある場合に住民基本台帳ネットワークシステムの運営を停止するなど、**緊急時対応計画を作成**　　等

２．住民基本台帳ネットワークシステムの環境及び設備

- 壁、窓、ドア等を堅牢なものとするなど建物等への侵入を防止
- 火災の防止、地震対策等に必要な設備を整備
- **専用回線の利用**により不正侵入を防止
- 予備回線の設置により通信の途絶を防止　　等

３．住民基本台帳ネットワークシステムの管理

- 入退室管理カード等により重要機能室への入室資格を確認
- 電子計算機、端末機等に関し、職員ごとに、必要なアクセス権限を限定
- 指定情報処理機関が管理する**ファイアウォールをネットワーク上の必要な部分に設置**
- 通信についての**通信相手相互の認証**を行い、通信相手のなりすましを防止
- **交換するデータの暗号化**により盗聴・改ざんを防止
- 認証及び暗号化に必要な秘密鍵を厳重に保管し、秘密鍵の漏えい、改ざんを防止
- 端末機の取扱いに際し、操作者識別カード及びパスワードにより権限外のシステム利用を防止
- 不正の監視、早期発見のために**操作履歴を保持し、定期的な監査を実施**
- 目的外のデータベース構築を防止するため、本人確認情報の提供を求める際の照会条件を限定
- 指定情報処理機関にネットワーク監視装置を設置し、障害発生時に迅速に対応
- コンピュータウイルス等が混入されていないかどうかを常時監視し、早期検出、除去を実施
- **侵入検出装置（ＩＤＳ）により不審な通信パターンを解析**し、不正侵入を防止
- 守秘義務がない者が本人確認情報を取り扱うことのないよう再委託を制限　　等

４．既設ネットワークとの接続

- 住民基本台帳ネットワークと既設ネットワークと接続する場合の専用回線の利用、ファイアウォールの設置
- 既設ネットワークと外部ネットワークを接続する場合のファイアウォールの設置

等

５．住民基本台帳ネットワークシステムの運用

- 運用時間、業務開始手続き等に関する運用計画を策定
- 転出確定通知の方法
- 本人確認情報の通知及び記録の方法
- 地方公共団体、指定情報処理機関及び本人確認情報の受領者は、保存期間経過後、本人確認情報を確実に消去
- 本人確認情報の受領者による本人確認情報の適切な管理
- 指定認証機関は、異動等情報を確実に消去するなど異動等情報に対する適切な管理

等