２　本人確認情報の保護措置について

（１）制度面

ア　保有情報の制限

・都道府県や指定情報処理機関が保有する情報は、本人確認情報（氏名、住所、生年月日、性別、住民票コード及びこれらの変更情報）に限定（住民基本台帳法第 30 条の 5）

イ　利用の制限

・本人確認情報の提供先、利用目的を明確に規定（住民基本台帳法第 30 条の 7 及び 8（別表第一～別表第五）、住民基本台帳法に基づく本人確認情報の利用及び提供に関する条例第 2 条及び第 3 条（別表第一及び別表第二））

ウ　秘密の保持

・秘密の漏えいは刑罰（二年以下の懲役又は百万円以下の罰金）をもって禁止（住民基本台帳法第 42 条）。

（２）技術面（「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」（平成 14 年総務省告示第 334 号））

ア　不正侵入の防止

・専用回線によるネットワークや通信データの暗号化等による外部からの不正侵入の防止

イ　不正利用の防止

・操作者用ＩＣカードとパスワードによる厳重な使用確認やアクセス記録保存等による不正利用の防止

（３）運用面（千葉県住民基本台帳ネットワークシステムセキュリティ対策規程）　※アンダーラインは平成 25 年 1 月に改定した事項

ア　組織・管理体制

・県システムにおけるセキュリティ対策を適正かつ円滑に実施するため、セキュリティ対策会議（会長：総務部長）を設置（第 7 条）

イ　機器等の管理

・必要と認める者以外の者を重要機能室に入室させない（第 8 条）

・端末機は、当該端末機が設置された所属の長が管理し、端末機の画面が操作者以外の者から容易に見えないように、端末機の設置場所に配慮しなければならない（第 10 条）

ウ　操作者の指定

・本人確認情報の利用業務を行う所属長は、端末機を操作し、本人確認情報を取り扱う者（以下「操作者」という。）をあらかじめ指定（指定された者以外は端末機を操作させない）（第 11 条）

エ　監査

・県システムに係る運用管理について、定期的に監査を行うものとする（第 19 条）

オ　研修

・県システムの利用に関し必要な知識を関係職員に習得させるため、住民基本台帳ネットワークシステム、端末機の操作セキュリティ対策について研修を行うものとする（第 20 条）

カ　障害等発生時の対応

・緊急時対応計画書を作成し、ネットワークの障害時や不正アクセスによる本人確認情報の漏えい等のおそれがある場合にとるべき必要な措置を定めている（第 22 条）

≪参考≫　研修、監査の実施について

１　研修の実施

（１）条例による利用拡大に伴う端末利用者向け

・回数等：平成 25 年 1 月 30 日～　合計 11 回

・参加者：413 名

（２）住基ネット端末操作実地研修

・回数等：平成 25 年 3 月 4 日～　26 回

・参加者：290 名

（３）人事異動により新たに住基ネットを利用することとなった者への研修

・回数等：平成 25 年 4 月 11 日～　8 回

・参加者：167 名

２　セルフチェックの実施

・時期：平成 25 年 5 月

・対象：住基ネットを利用している者（474 名）

３　監査の実施

・時期（予定）：平成 26 年 1 月～

・対象：端末機設置所属及び当該端末機を利用している所属

・内容：操作ログと各所属で保管している申請書類等との突合、
　　各種様式の作成状況の確認　等