資料３－２

住基ネット利用事務の拡大に伴うセキュリティ対策について

県独自利用事務を追加する際には、住民基本台帳ネットワークシステムを利用する事務が増えることから、以下３つの側面から引き続きセキュリティ対策を進めたい。

制度面

- 記録する情報を「本人確認情報」に限定
- 職員の秘密保持義務
- 「本人確認情報」の提供先の制限
- 「本人確認情報」の利用事務を限定

住民基本台帳法で規定

技術面

- 専用回線の利用
- ファイアウォールによる外部からの不正な通信の防止
- 操作者認証に生体認証（静脈認証）を導入　など

運用面

- **職員教育の徹底（セキュリティ対策の周知・徹底）**
  ⇒①新規担当職員（現行事務利用機関）を対象とした研修会を実施（４月）
  ②新規事務利用機関職員に対し、住基ネット利用開始前に研修を実施
- **業務アプリケーション利用上のセキュリティ対策**
  ⇒業務以外での利用禁止、権限のない者による不正な操作防止、出力情報からの情報漏えい防止を徹底
- **物理的なセキュリティ対策**
  ⇒入退室管理による不正アクセス防止、空調設備の確保や災害対策などによる重要機器の物理的保護を実施
- **システム管理に関するセキュリティ対策**
  ⇒磁気ディスクやドキュメント（書類）の適切な管理、ログや操作履歴の徹底管理
- **委託業者の管理**
  契約書による委託業者の秘密保持義務の明確化、委託業務の管理・監視

自己点検、内部監査、外部監査によりチェック