議案第66号　説明資料

情報セキュリティ強化対策用機器

品　　名	説　　明	数量
仮想サーバ	１台のサーバ機器内で複数のWindowsなどのOSを稼働させる装置	５台
内部統制システム	各端末の不正なアクセス監視（外部からの不正アクセス及び内部での個人情報不正閲覧等）や操作記録を行い、個人情報漏えいやウィルス感染の原因究明を目的とする。 デバイス制御（USBメモリ等）を行うことにより、許可されたデバイス以外でデータの持ち出しを不可能とし、個人情報、内部情報の不正流出を防止する。	一式
二要素認証システム	個人番号の情報漏えい防止策として、個人番号利用事務系端末に今までのログインパスワードのほか職員証のICカードにパソコン端末アクセス権限を設定し、パスワードとカードの二つの要素で認証する。	一式
ファイル転送装置	分離されたネットワークから接続可能な場所にファイル受け渡し、セキュリティ要件として必要な上長承認、ログ管理機能も備えたファイル受け渡し装置	一式
ふるまい検知	標的型サイバー攻撃による悪意のあるソフトウェア活動を検知し、感染端末を自動的に遮断	一式
その他機器設置設定等	新規導入機器・システムの設置・設定動作検証。既存システムのネットワーク変更に伴うサーバ機器のネットワーク情報設定	一式

情報セキュリティ強化対策用機器

■現状は、基幹系端末（住基、税、宛名、介護、国保、後期高齢者、住宅、水道等各種システム）と情報系端末（財務会計、人事給与、グループウェア、インターネット等を二分離して運用中。（平成27年度実施済）

■今回は、総務省から示されたネットワーク強靭性向上モデルに準じ、現行の二分離を個人番号利用事務系端末（住基、税、宛名、介護、国保、後期高齢者、住宅、水道等各種システム）とLGWAN接続系端末（財務会計、人事給与、グループウェア等）、インターネット接続系端末（ホームページ、インターネットメール等）の３つのセグメントに分離。

■特定個人番号の情報漏えい防止策として、個人番号利用事務系端末に今までのログインパスワードのほか職員証のICカードにパソコン端末のアクセス権限を設定し、パスワードとカードの二つの要素で認証。

■内部統制システムを導入し、不正なアクセスの監視（外部からの不正アクセス及び内部での個人情報不正閲覧等）、デバイス制御を行う。