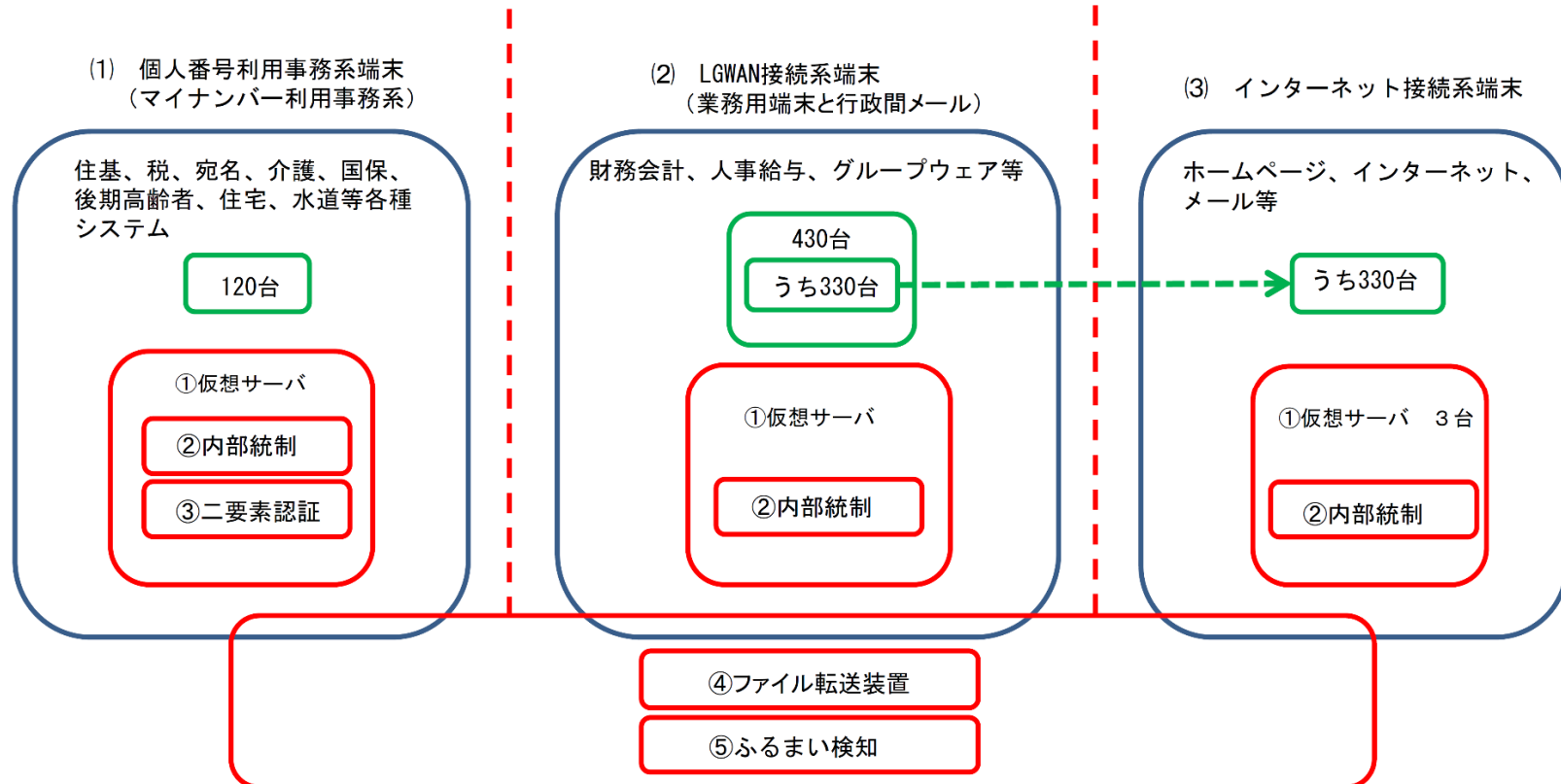


情報セキュリティ強化対策機器

- 総務省から示されたネットワーク強靱性向上モデルに準じ、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つのネットワークに分離。
- 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。

[強靱性向上モデル]



情報セキュリティ強化対策機器

	品 名	説 明	数 量
①	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
②	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。	一式
③	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。	一式
④	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、無害化処理機能も備えたファイル受け渡し装置。	一式
⑤	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
⑥	その他機器設置設定等	導入機器・システムの設置・設定動作検証。サーバ機器のネットワーク情報設定。	一式