住基ネット利用に関するセキュリティ対策

１　平時における住基ネットのセキュリティ対策

○個人情報の漏えい等の不正な情報操作の防止、住基ネットへの信頼性・安全性の確保のため、外部から隔離された専用の通信回線の使用、他機関への通信の暗号化

○外部攻撃からネットワークを守る役割を果たす、ファイアウォール等の設置

○業務端末、ドキュメント等の施錠可能なキャビネットへの保管

○住基ネットの利用時における利用課の届出および記録

○住基ネット初任者の理解と意識を高める「研修」の実施

住基ネット初任者の職員に対して「住基ネット初任者研修」を実施し、H25 年度からは、研修終了後に理解度確認テストを行い、８割以上の正答者のみに操作者権限を付与している。

H27 年度からは、初任者研修とは別に全操作者を対象とした「住基ネット担当者研修会」を実施し、セキュリティ確保に努めている。

○住基ネット操作履歴（業務アクセスログ）の確認

操作履歴を記録し、毎月市町村課職員において不正な利用がないかを確認している。

２　住基ネット利用時におけるセキュリティ対策

○支援教育課は市町村課に、操作者の照合ＩＤ登録を申請する。

○市町村課において、上記申請のあった者に対し、初任者研修を実施する。また、研修後理解度確認テストで８割以上の正答者について、照合 ID の登録し、操作者権限を付与する。

○支援教育課は市町村課に、利用事務や件数を記載した申請書をあらかじめ市町村課に提出する。

○照合 ID を登録した支援教育課職員が市町村課に来課、市町村課業務端末利用記録簿に必要事項を記入、市町村課は、記録簿をもとに本人確認を行う。

○市町村課職員立合いのもと、支援教育課職員が、（１）で登録した照合ＩＤを使用し、即時提供・一括提供を実施する。

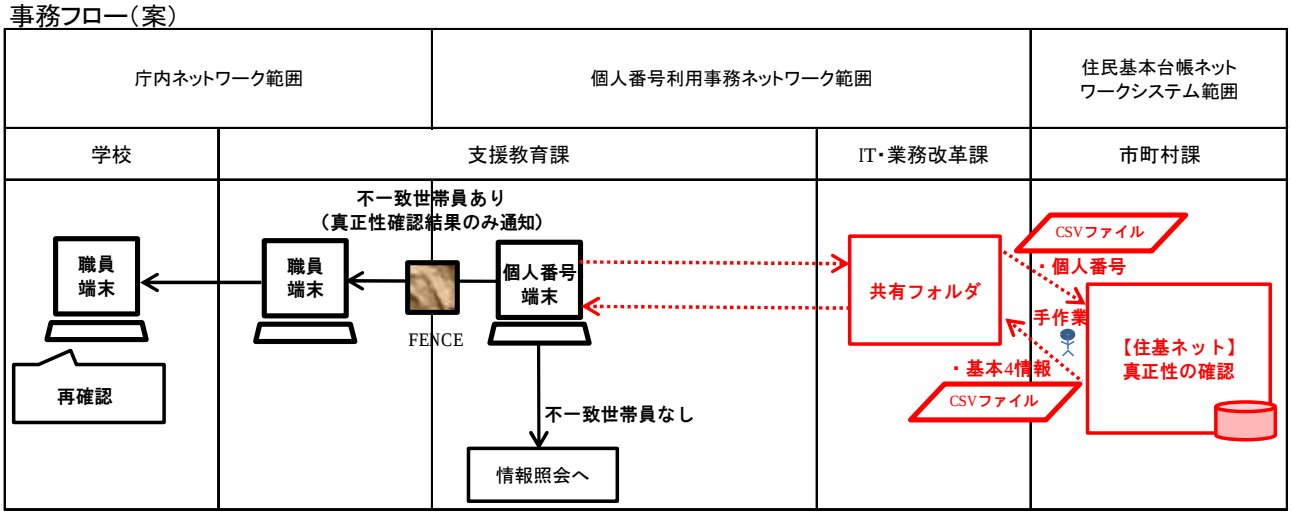
○個人番号の入った CSV ファイルのやりとりについては、住基ネット利用登録を行っている支援教育課職員が手作業で行い、電子記録媒体で外部に持ち出さず、専用線を用いた共有フォルダを介して行う。

３　住基ネット利用後におけるセキュリティ対策

○住基ネットを使用して得た基本４情報は個人番号端末から持ち出さず、真正性確認結果のみを庁内ネットワークで学校へ通知する。個人番号端末は庁内ネットワークとは遮断されており、個人番号端末から庁内ネットワークへ真正性確認結果を持ち出す際には、FENCE（ファイル送受信システム）を経由する。

○個人番号端末へのログインについては静脈認証が必要であり、就学奨励費事務担当者のみを登録している。FENCE（ファイル送受信システム）を経由しての庁内ネットワーク範囲とのデータやり取りは、PC 管理責任者の許可の元、事前に登録している課長補佐級職員（2 名）どちらかの承認をもって行う。

事務フロー（案）


庁内ネットワーク範囲
個人番号利用事務ネットワーク範囲
住民基本台帳ネットワークシステム範囲
学校
支援教育課
IT・業務改革課
市町村課
不一致世帯員あり
（真正性確認結果のみ通知）
職員端末
職員端末
個人番号端末
FENCE
再確認
不一致世帯員なし
情報照会へ
共有フォルダ
CSVファイル
・個人番号
手作業
・基本4情報
CSVファイル
【住基ネット】
真正性の確認