

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を用し、他機関への通信を暗号化している。
- 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を設置している。
- 業務端末、ドキュメント等を施錠可能なキャビネットへ保管している。
- 住基ネットの利用時における利用課の届出および記録を行っている。
- 住基ネット初任者の理解と意識を高める「研修」の実施している。
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）を確認している。
操作履歴を記録し、毎月行政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

- 操作者の登録にあたっては、操作者数について事前に行政課と協議の上、申請することとし、不必要に多くの操作者登録が行われないように努めている。
- 操作者登録にあたっては、初任者研修を実施し、研修後理解度確認テストで8割以上の正答者にのみ、操作者権限を付与することとしている。
- 住基ネットの利用にあたっては、あらかじめ行政課に、利用事務や件数を記載した申請書を提出することとし、利用状況について、把握している。
- 住基ネットの利用時には、行政課業務端末利用記録簿に必要事項を記入させることで、利用の記録を残している。また、記録簿をもとに行政課職員が操作者の本人確認を行っている。
- 一括提供による住基ネット利用時には、行政課職員が立ち会いを実施することで、不適切な操作が行われない体制を確保している。
- 個人番号の入ったCSVファイルのやりとりについては、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（住基ネット連携用フォルダ）を介して行っている。

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附票本人確認情報は、電子記録媒体で外部に持ち出さず、住基ネット連携用フォルダを介して、やりとりを行う。