○仙台市職員共済組合住民基本台帳ネットワークシステム セキュリティ管理規程

平成２１年３月３０日
仙台市職員共済組合規程第２号

（目的）

第１条　この規程は、仙台市職員共済組合（以下「組合」という。）が住民基本台帳ネットワークにより提供を受ける本人確認情報の保護並びにそれに付随するネットワーク機器の適切な管理及び運営に関し必要な事項を定め、本人確認情報の漏えい、滅失及びき損の防止並びにその他本人確認情報の適切な管理を図ることを目的とする。

（定義）

第２条　この規程において、次に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

⑴　本人確認情報　住民基本台帳法（昭和４２年法律第８１号）第３０条の９の規定により組合が提供を受ける同法第３０条の６第１項に規定する本人確認情報（氏名、出生の年月日、男女の別、住所、個人番号、住民票コード及びこれに付随する情報を含む。）をいう。

⑵　記録媒体　磁気媒体及び紙媒体で本人確認情報を記録するすべての媒体をいう。

⑶　ドキュメント　本人確認情報の利用に係るシステムの設計及びプログラム作成並びに運用に関する記録及び文書をいう。

⑷　情報資産　住民基本台帳ネットワークに係るすべての情報並びにソフトウェア、ハードウェア、ネットワーク及び記録媒体をいう。

（住基ネットセキュリティ統括責任者）

第３条　住民基本台帳ネットワークシステム（以下「住基ネット」という。）のセキュリティ対策を総合的に実施するため、住基ネットセキュリティ統括責任者を置く。

２　住基ネットセキュリティ統括責任者は、事務局長をもって充てる。

３　住基ネットセキュリティ統括責任者は、本人確認情報管理責任者、住基ネットシステム管理者及び住基ネットセキュリティ管理者を監理する。

（本人確認情報管理責任者）

第４条　本人確認情報に係る取扱いを適切に管理するため、本人確認情報管理責任者を置く。

２　本人確認情報管理責任者は、事務局次長をもって充てる。

３　本人確認情報管理責任者は、本人確認情報に係る取扱いについて管理し、

本人確認情報を取扱う者（以下「システム操作者」という。）を指名する。
４　本人確認情報管理責任者は、本人確認情報の漏えい、滅失及びき損の防止その他当該本人確認情報の適切な管理を図るための必要な措置を講ずるものとする。
（住基ネットシステム管理者）
第５条　住基ネットの適切な管理を行うため、住基ネットシステム管理者を置く。
２　住基ネットシステム管理者は、総務係長をもって充てる。
３　住基ネットシステム管理者は、本人確認情報に係る管理を行うほか、住民基本台帳ネットワークを運用している部屋の入退室管理、情報資産管理、記録媒体管理、ドキュメント管理、アクセス管理、ユーザＩＤ及びパスワード管理並びに照合情報の管理に関し必要な措置を講ずるものとする。
４　住基ネットシステム管理者は、生体認証時に用いる照合情報の管理を行う拠点管理者（以下「拠点管理者」という。）を２名指名しなければならない。
（住基ネットセキュリティ管理者）
第６条　住基ネットを利用する係においてセキュリティ対策を実施するため、住基ネットセキュリティ管理者を置く。
２　住基ネットセキュリティ管理者は、年金係長をもって充てる。
３　住基ネットセキュリティ管理者は、住民基本台帳ネットワークのセキュリティ対策を職員へ徹底させるとともに、セキュリティに対する脅威が発生した場合は、情報収集を行い、その結果を住基ネットセキュリティ統括責任者に報告しなければならない。
（拠点管理者）
第７条　住基ネットを利用する部署において住基ネットに係る照合情報管理業務の適正な運営を行うため、拠点管理者を置く。
２　拠点管理者は、住基ネットシステム管理者から指名されたシステム操作者をもって充てる。
３　拠点管理者は、システム操作者の照合情報を新規登録、削除及び委託する操作権限の追加並びに委託した操作権限の返却をする場合は、住基ネットシステム管理者へ申請し、承認を受けなければならない。
（住基ネットセキュリティ会議の設置）
第８条　住民基本台帳ネットワークのセキュリティに関する審議を行うため、住基ネットセキュリティ会議を設置する。
２　住基ネットセキュリティ会議は、次に掲げる者をもって組織する。
⑴　住基ネットセキュリティ統括責任者
⑵　本人確認情報管理責任者

⑶　住基ネットシステム管理者
⑷　住基ネットセキュリティ管理者
⑸　拠点管理者
３　住基ネットセキュリティ会議は、次に掲げる事項を審議する。
⑴　住民基本台帳ネットワークのセキュリティ対策の決定及び見直し
⑵　前号のセキュリティ対策の遵守状況の確認
⑶　セキュリティ監査の実施
⑷　教育及び研修の実施
⑸　情報資産の機能が正常に動作しない場合の対応
⑹　住民基本台帳ネットワークの目的外使用、 運営を阻害する行為又は本人確認情報に脅威を及ぼすおそれがある場合の対応
４　住基ネットセキュリティ統括責任者は、住基ネットセキュリティ会議を招集するとともに、議長を務めるものとする。
５　議長は、住基ネットセキュリティ会議において、関係職員及び外部の専門家に出席を求め、意見又は説明を聴くことができる。
６　住基ネットセキュリティ会議の庶務は、 総務係において処理する。
（本人確認情報の取扱者）
第９条　本人確認情報は、システム操作者以外の者に取扱いをさせてはならない。
２　システム操作者は、大量の本人確認情報を取り扱う際、あらかじめ本人確認情報管理責任者の承認を得なければならない。
（本人確認情報の利用制限）
第１０条　本人確認情報を利用する事務は、年金である給付の支給に関するものであって、次に掲げるものに限るものとする。
⑴　給付の請求をすると見込まれる者の生存の事実又は氏名若しくは住所の変更の事実の確認
⑵　給付の請求の受理、その請求に係る事実についての審査又はその請求に対する応答
⑶　給付を受ける権利に係る申出若しくは届出の受理又はその申出若しくは届出に係る事実についての審査
⑷　受給権者又は給付の額の加算の原因となる者の生存の事実又は氏名若しくは住所の変更の事実の確認
（本人確認情報及び記録媒体の管理）
第１１条　本人確認情報は、記録媒体に記録し、次回の年金給付後は、遅滞なく当該本人確認情報を消去及び廃棄しなければならない。
２　本人確認情報管理責任者は、火災その他の災害及び盗難に備えて、システ

ム操作者に記録媒体を所定の場所に保管させ、適切に管理を行わせなければならない。

3　記録媒体を外部に持ち出す場合には、本人確認情報管理責任者及び住基ネットシステム管理者の承諾を得なければならない。また、外部への搬送については、相手方、記録媒体の種類、数量及び当該記録媒体に記録された本人確認情報の件数を記録し、かつ、施錠できる容器を使用し、又は厳重な包装を行うことにより、滅失、き損及び盗難（以下「滅失等」という。）を防止する措置を講じなければならない。

4　記録媒体の本人確認情報の消去及び廃棄については、本人確認情報が第三者に漏えいすることがないよう措置を講じなければならない。

5　記録媒体を廃棄する場合には、破砕その他確実な措置を講ずるとともにその旨記録しなければならない。

6　住基ネットシステム管理者は、記録媒体の障害の有無について、記録しなければならない。

（ドキュメントの管理）

第１２条　ドキュメントは、住基ネットシステム管理者が管理するものとし、所定の場所に保管するとともに、その保管状況を記録しなければならない。

2　ドキュメントを複製し、又は外部に持ち出す場合には、住基ネットシステム管理者の許可を得なければならない。

（入退室の管理）

第１３条　住基ネットシステム管理者は、次に掲げる住基ネットを運用している部屋において、それぞれのセキュリティ区分に応じた入退室管理を行うものとする。

セキュリティ区分	部　　屋
レベル３	記録媒体の保管室
レベル２	サーバの設置室
レベル１	業務端末機（生体認証装置等を含む。）及びネットワーク機器の設置室

2　それぞれのセキュリティ区分に応じた入退室管理の方法は、次のとおりとする。

セキュリティ区分	入退室管理の方法
レベル３	住基ネットセキュリティ統括責任者から許可された者のみ入退室を行う。

レベル２	本人確認情報に係る電算処理を外部に委託した場合の本人確認情報管理責任者が指名する者のみ入退室を行う。
レベル１	住基ネットシステム管理者から許可されたシステム操作者のみ入退室を行う。

３　前項の場合において、住基ネットシステム管理者は、入退室管理を行うため入退室管理簿を作成し、これに入退室の状況を管理しなければならない。

４　住基ネットシステム管理者は、機器の設置又は保守若しくは撤去に係る業者が入退室をする場合には、入退室管理簿に所要の事項を記載させ、識別を行うため、名札を着用させるとともに、システム操作者の立会いをさせなければならない。

（アクセス管理）

第１４条　住基ネットシステム管理者は、住基ネットの操作履歴を確認しなければならない。

２　住基ネットシステム管理者は、住基ネットに係るユーザＩＤをシステム操作者に配付し、不正なアクセスがないよう管理方法を定めるとともに、ユーザＩＤ管理簿を作成し、管理しなければならない。

（システム操作者の照合情報の管理）

第１５条　住基ネットシステム管理者は、照合情報を保管するとともに、これを紛失し、又は盗難されることがないよう管理方法を定め、併せて、照合情報管理簿を作成し、これに利用状況を記録しなければならない。

（システム操作者の責務）

第１６条　システム操作者は、次に掲げることを遵守しなければならない。

⑴　ユーザＩＤ及びパスワードの管理

⑵　照合ＩＤの管理

（操作履歴の記録）

第１７条　住基ネットシステム管理者は、住基ネットの操作履歴について、７年前まで遡って解析できるよう、保管するものとする。

（情報資産管理）

第１８条　住基ネットシステム管理者は、情報資産を保管するとともに、当該資産を紛失し、又は盗難されることがないよう管理方法を定め、併せて、情報資産管理簿を作成し、これを管理しなければならない。

（職員の教育及び研修）

第１９条　住基ネットセキュリティ管理者は、必要と認める職員に対し、住基ネットの操作及びセキュリティ対策について、教育及び研修を実施するものとする。

（事故発生時の対応）

第２０条　システム操作者は、本人確認情報に関する事故、住基ネットの欠陥及び誤作動を発見した場合には、速やかに住基ネットシステム管理者に報告し、住基ネットシステム管理者は、別に定める緊急時対応計画書にしたがって対応しなければならない。

（守秘義務）

第２１条　職員（職員であった者を含む。）は、本人確認情報に関し知り得た情報をみだりに他人に知らせ又は不当な目的に利用してはならない。

（委託）

第２２条　本人確認情報に係る処理を外部に委託する場合には、本人確認情報に関する秘密保持、その他本人確認情報の保護の水準を満たしている者を委託先とし、委託先が講じるべき安全管理措置に関し必要な事項を委託契約書に明記するものとする。

２　前項に規定する委託契約書には、次に掲げる事項を明記するものとする。

⑴　秘密保持義務
⑵　目的外使用の禁止
⑶　複写及び複製の禁止
⑷　第三者提供の禁止
⑸　再委託の禁止
⑹　作業場所
⑺　個人情報の授受の方法及び保管方法
⑻　個人情報の管理責任者
⑼　個人情報の管理状況に関する報告義務
⑽　事故等の発生時における報告義務
⑾　委託処理終了後の個人情報の返還及び消去並びに廃棄
⑿　契約事項に違反した場合の契約解除及び損害賠償
⒀　前各号に掲げるもののほか、個人情報の保護に関し必要な事項

３　住基ネットシステム管理者は、前項の場合において、必要と認められる場合には、記録媒体の授受の手続き、搬送の方法及びその経路並びに保管方法その他本人確認情報の滅失等を防止するための必要な事項につき、契約の相手方と覚書を締結するものとする。

（補則）

第２３条　この規程に定めるもののほか、必要な事項は、理事長が別に定める。

附　則

この規程は、平成２１年４月１日から施行する。

附　則

この規程は、平成２６年５月１６日から施行する。

附　則

この規程は、平成２８年６月１４日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から適用する。

⑴　第２条第１号（「第３０条の７第３項」を「第３０条の９」に、「第３０条の５第１項」を「第３０条の６第１項」に改める部分に限る。）の規定　平成２７年１０月５日

⑵　第２条第１号（「住所」の下に「、個人番号」を加える改正規定に限る。）の規定　平成２８年１月１日

⑶　第５条第２項及び第８条第６項の規定　平成２８年４月１日