

京都市職員共済組合細則第1号

京都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細則について

京都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細則を次のよう定める。

平成28年9月30日

京都市職員共済組合
理事長 岡田 憲和

京都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細則

(目的)

第1条 この細則は、京都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28年10月1日制定）第23条の規定に基づき、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及びそれに付随するネットワーク機器の適切な管理に関し必要な細目を定めることを目的とする。

(立入り管理)

第2条 システム操作者は、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。）を運用している区画において作業を行う際に、住基ネット及びネットワーク機器について次の各号に掲げる項目を確認しなければならない。

- (1) 機器等の紛失がないこと。
- (2) 電源がオフになっていること。
- (3) 保守作業で一時的に使用した磁気媒体が、機器に挿入されたままの状態になっていないこと。
- (4) ネットワーク機器に、不正な通信ケーブルが接続されていないこと。
- (5) 保守作業で一時的に使用した磁気媒体及びドキュメントが、権限のない者によってアクセス可能な場所に放置されていないこと。

2 システム操作者は、前項の結果について、次の各号に掲げる項目を記載した別紙様式第1号による立入り管理簿に記録しなければならない。

- (1) 日付

- (2) システム開始時分
- (3) システム終了時分
- (4) 開始者氏名
- (5) 終了者氏名
- (6) 確認内容
- (7) 特記事項

3 住基ネットシステム管理者は、前項の立入り管理簿の内容を10日に1度確認しなければならない。

(ユーザID及びパスワード管理)

第3条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第2号によるユーザID管理簿を作成し、ユーザIDの登録及び削除を行う際に必要な項目を記録しなければならない。

- (1) ユーザID
- (2) 登録年月日
- (3) ユーザ名
- (4) 使用開始年月日
- (5) 使用終了年月日
- (6) 削除年月日
- (7) 特記事項

2 住基ネットシステム管理者は、ユーザIDを配付する際に、次の各号に掲げる事項を行わなければならない。

- (1) システム操作者ごとにユーザIDを配付すること。
- (2) システム操作者の異動があった場合には、配付したユーザIDを直ちに削除すること。
- (3) 本人確認情報を利用できる端末のユーザIDは、本人確認情報を利用できる端末にアクセス制限ツールを適用した後に配付すること。
- (4) 初期パスワードを初回ログオン時に必ず変更するようシステム操作者に指示すること。

3 住基ネットシステム管理者は、OSのパスワード管理機能を使用し、これを管理する際、次の各号に掲げる事項を行わなければならない。

- (1) パスワードの有効期間を90日に設定すること。
- (2) パスワードの最低桁数を8桁以上に設定すること。
- (3) パスワードの複雑性を要求するよう設定すること。
- (4) 3回のパスワード入力失敗により、ロックアウトするよう設定すること。
- (5) 初回ログオン時に初期パスワードの変更が必要となるよう設定すること。
- (6) 本人確認情報を利用できる端末のパスワードが漏えいしたおそれがある場合は、パスワードを速やかに変更するようシステム操作者に指示すること。

4 システム操作者は、パスワードを設定する際に、次の各号に掲げる事項を行わなければならない。

- (1) システム操作者が設定すること。
- (2) 90日毎に変更すること。
- (3) 8桁以上とすること。
- (4) 大文字、小文字、英数字及び記号を混在させること。
- (5) 推測されやすい単語、単純な文字列を使用しないこと。
- (6) パスワードのメモを端末又は机中にはり付けていないこと。
- (7) パスワードは、システム操作者が責任をもって管理すること。

5 住基ネットシステム管理者は、実施状況を確認する際に、次の各号に掲げる事項を10日に1度確認しなければならない。

- (1) ユーザID管理簿と現況が一致しており、登録者以外にユーザIDが配付されていないこと。
- (2) 不要となったユーザIDが存在していないこと。
- (3) OSのパスワード管理機能の設定内容が変更されていないこと。
- (4) パスワードのメモを端末又は机上に貼り付けていないこと。

(照合情報の管理)

第4条 住基ネットシステム管理者は、別紙様式第3号による照合情報管理簿を作成し、次の各号に掲げる職員に関する必要な項目を記録しなければならない。

- (1) 住基ネットシステム管理者に関する項目
 - ア 氏名
 - イ 管理開始年月日
 - ウ 管理終了年月日

(2) 拠点管理者に関する項目

- ア 氏名
- イ 照合 I D
- ウ 管理開始年月日
- エ 確認印
- オ 管理終了年月日
- カ 確認印

(3) システム操作者に関する項目

- ア 氏名
- イ 照合 I D
- ウ 委譲開始年月日
- エ 確認印
- オ 委譲終了年月日
- カ 確認印
- キ 有効期限
- ク 操作権限

2 拠点管理者は、職員が新規に住基ネットの操作を実施する必要がある場合、次の各号に掲げる項目を記載した別紙様式第 16 号により住基ネットシステム管理者へ申請し、その承認を受けて、該当する職員に照合 I D を付与し、照合情報を登録しなければならない。

- (1) 照合 I D
- (2) 所属
- (3) 登録者名
- (4) 委譲開始年月日
- (5) 有効期限
- (6) 操作権限
- (7) 操作権限が必要な理由

3 拠点管理者は、システム操作者が操作権限を必要とする業務から外れた場合、次の各号に掲げる項目を記載した別紙様式第 17 号により住基ネットシステム管理者へ申請し、その承認を受けて、該当する職員の照合 I D 及び照合情報を削除しな

ればならない。

- (1) 所属
- (2) 登録者名
- (3) 委譲終了年月日
- (4) 操作権限返却理由

4 拠点管理者は、照合情報登録操作時に、次の各号に掲げる項目に留意しなければならない。

- (1) 登録時には、本人であることの確認を確実に行うこと。
- (2) 照合情報の登録が適正に行われていることを確認すること。
- (3) 登録を実施する拠点管理者及び登録する職員以外から登録の操作をみられないようにすること。
- (4) 有効期限は業務から外れるまでか、外れる時期が確定していない場合は1年後の日付を登録すること。有効期限が切れた場合には、システム操作者がさらに業務から外れるまでか、外れる時期が確定していない場合は1年後の日付を登録すること。その際、申請は不要とする。

5 拠点管理者は、職員へ委譲する操作権限を、実施する業務の変更等に対応して追加・返却しなければならない。また、その場合、住基ネットシステム管理者へ申請し、その承認を受けなければならない。

6 拠点管理者は、操作権限追加・返却をもって照合情報の追加又は削除を実施する際、システム操作者以外の職員から追加又は削除の操作を見られないようにしなければならない。

7 住基ネットシステム管理者は、照合ID及び操作権限の設定状況について、照合情報管理簿により次の各号に掲げる事項を月に1回確認しなければならない。また、照合ID及び操作権限委譲に変更があった場合は、その都度、照合ID及び操作権限の設定状況について、照合情報管理簿により次の各号に掲げる事項を確認しなければならない。

- (1) 拠点管理者から申請された内容のとおり、照合ID及び操作権限が設定されていること。
- (2) 照合情報管理簿に必要な項目（システム操作者の氏名及び所属、委譲年月日等）が記録されていること。

8 照合情報認証を行って業務アプリケーションの操作を実施するシステム操作者は、自身が使用しないときは確実にログオフを行い、他の職員が操作することがないように配慮しなければならない。

(アクセス管理)

第5条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第4号によるアクセス管理簿を作成し、操作ログの確認を行う際に、必要な項目を記録しなければならない。

- (1) 操作ログの期間
- (2) 操作ログの保管場所
- (3) 操作ログの保管年月日
- (4) 保管者名
- (5) 特記事項

2 住基ネットシステム管理者は、10日に1度取得したログの中に不正アクセスの可能性がないか次の各号に掲げる事項を確認しなければならない。

- (1) 不在（休暇を取得している等を含む。）となっているシステム操作者の操作履歴
- (2) 存在しない端末ID及び操作者IDの操作履歴
- (3) 1箇月前、1年前などと比較し、急激に増加しているユーザIDの操作履歴
- (4) 通常と比較して多い本人確認情報の検索

3 住基ネットシステム管理者は、前項の確認により不正アクセスの可能性のあるログを発見した場合は、システム操作者へのヒアリングを実施するとともに、業務記録簿を調査しなければならない。

4 住基ネットシステム管理者は、前項の調査を行った結果、不正アクセスの可能性があると判断した場合は、住基ネットセキュリティ統括責任者、本人確認情報管理責任者及び住基ネットセキュリティ管理者へ報告し、別に定める緊急時対応計画書にしたがって行動しなければならない。

5 住基ネットシステム管理者は、確認した第2項の結果を本人確認情報管理責任者へ報告するものとし、当該操作ログは、7年間、保管庫に保管しなければならない。

6 住基ネットシステム管理者は、前項の実施状況を10日に1度確認しなければならない。

(本人確認情報の管理)

第6条 住基ネットシステム管理者は、本人確認情報を取り扱う際に、次の各号に掲げる事項を確認しなければならない。

- (1) 来庁者及び業務に関わりのない他の職員にディスプレイ画面を見られることがないように設置されていること。
- (2) ディスプレイに斜視防止フィルタが設置されていること。
- (3) スクリーンセーバの起動までの時間が5分以内に設定されていること。
- (4) スクリーンセーバの解除にパスワードの入力が要求されるよう設定されていること。
- (5) 本人確認情報をメモに書き込んだり、本人確認情報を利用できる端末にテキスト文書で保存していないこと。

2 システム操作者は、本人確認情報の検索又は抽出を行う際に、次の各号に掲げる事項を確認しなければならない。

- (1) 業務上必要のない検索をしないこと。
- (2) 事前に検索又は抽出条件を明確にすること。
- (3) 検索又は抽出の結果によって、ディスプレイ上に表示された本人確認情報について、画面のハードコピーを取らないこと。

3 システム操作者は、離席する際に業務アプリケーションを終了させなければならない。

4 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第5号による帳票出力申請簿を作成し、大量に本人確認情報の帳票を出力する際に、システム操作者に必要な項目を記録させなければならない。

- (1) 帳票出力日
- (2) 操作者名
- (3) 帳票名
- (4) 出力理由
- (5) 住基ネットシステム管理者確認印

5 システム操作者は、出力装置を設置する際に、次の各号に掲げる事項を行わなければならない。

- (1) 来庁者及び業務に関わりのない他の職員に出力された帳票を見られないよう設

置すること。

(2) 帳票を出力した際に、出力装置上に放置せず速やかに回収すること。

(3) システム操作者は、出力装置を適時確認し、帳票が放置されている場合は以下の措置を行うこと。

ア 出力したシステム操作者を特定して注意すること。

イ 1時間放置された帳票は廃棄すること。

6 住基ネットシステム管理者は、次の各号に掲げる項目を記録及び管理するための別紙様式第6号による本人確認情報管理簿を作成し、システム操作者に記録させ、これを管理しなければならない。

(1) 出力年月日

(2) 検索対象者

(3) 出力したシステム操作者名

(4) 使用目的

(5) 出力の有無

(6) 廃棄者名

(7) 廃棄年月日

(8) 特記事項

7 住基ネットシステム管理者は、出力された帳票を廃棄する際に、システム操作者に次の各号に掲げる事項を行わせなければならない。

(1) 事前に、住基ネットシステム管理者の了承を得てから廃棄すること。

(2) 帳票の内容が読み出せないよう焼却、裁断又は溶解により廃棄すること

(3) 廃棄状況を本人確認情報管理簿に記録し、住基ネットシステム管理者へ報告すること。

8 住基ネットシステム管理者は、実施状況の確認をする際に、次の各号に掲げる事項を月に1度確認しなければならない。

(1) 本人確認情報管理簿に必要な項目が記録されていること。

(2) 本人確認情報管理簿と現況が一致しており、かつ紛失がないこと。

(3) 出力装置が、来庁者及び業務に関わりのない他の職員に出力された帳票を見られないよう設置されていること。

(4) 出力した帳票が放置されていないこと。

(5) 廃棄状況の記録が残っていること。

(ソフトウェアの管理)

第7条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第7号によるプログラム管理簿及び別紙様式第8号によるソフトウェア管理簿を作成し、機器ごとに起動するプログラム、インストールするソフトウェアについてシステム操作者に必要な項目を記録させなければならない。

(1) プログラムに関する項目

- ア プログラム名
- イ 使用理由
- ウ スタートアップの種類（自動又は手動）
- エ ログオンアカウント
- オ システム操作者名
- カ 特記事項

(2) ソフトウェアに関する項目

- ア ソフトウェア名
- イ バージョン番号
- ウ メーカー名
- エ システム操作者名
- オ 使用理由
- カ 使用開始日
- キ 使用終了日
- ク 保守業者の連絡先
- ケ 特記事項

2 住基ネットシステム管理者及びシステム操作者は、プログラム及びソフトウェアに際し、次の各号に掲げる事項を行わなければならない。

(1) 住基ネットシステム管理者は、本人確認情報を利用できる端末について、プログラム管理簿及びソフトウェア管理簿に登録されていないプログラムの起動、ソフトウェアのインストールを制限すること。

(2) 住基ネットシステム管理者は、プログラム管理簿及びソフトウェア管理簿に登録されたプログラム並びにソフトウェアの脆弱性情報について調査し、脆弱性が

発見された場合は、修正プログラムを適用するよう必要な措置を行うこと。

(3) システム操作者は、プログラム管理簿及びソフトウェア管理簿に登録されていないプログラム並びにソフトウェアを許可なく機器に追加しないこと。

(4) システム操作者は、原則として、本人確認情報を利用できる端末にワープロ、表計算ソフトウェアをインストールしないこと。

3 システム操作者は、プログラム管理簿及びソフトウェア管理簿に登録されていないプログラム並びにソフトウェアを例外的に機器に追加する必要がある場合は、次の各号に掲げる項目を記録するための別紙様式第9号によるプログラム及びソフトウェア追加申請書に記載し、住基ネットシステム管理者に提出しなければならない。

(1) プログラム及びソフトウェア名

(2) 追加理由

(3) 業務内容

(4) 使用開始日

(5) 使用終了日

(6) システム操作者名

4 住基ネットシステム管理者は、前項の申請内容が適正かつ、妥当であるか、又はセキュリティ上問題ないか確認し、了承する。

5 システム操作者は、前項において住基ネットシステム管理者が了承した場合は、プログラム及びソフトウェアを追加し、住基ネットシステム管理者へ報告する。

6 住基ネットシステム管理者は、実施状況を確認する際に、次の各号に掲げる事項を月に1度確認しなければならない。

(1) プログラム管理簿及びソフトウェア管理簿と現況は一致していること。

(2) 不要なソフトウェアがインストールされていないこと。

(3) 追加したプログラム及びソフトウェアについて、プログラム及びソフトウェア追加申請書が提出され、了承が得られていること。

(機器接続の管理)

第8条 システム操作者は、本人確認情報が利用できる機器を追加する際に、次の各号に掲げる事項を記録するための別紙様式第10号による住民基本台帳ネットワーク機器追加申請書に記載し、住基ネットシステム管理者に提出しなければならない。

(1) 申請者の氏名

- (2) 接続機器
- (3) 接続方法（接続場所，必要なネットワークを含む。次項において同じ。）
- (4) 接続理由
- (5) 接続希望年月日
- (6) システム操作者名

2 住基ネットシステム管理者は，前項の申請の内容が適正であり，かつ接続理由は妥当であるか，接続方法について十分なセキュリティ対策が行われているか確認し了承する。

3 システム操作者は，前項において住基ネットシステム管理者が了承した場合は，追加する機器の設置及び設定作業を行い，住基ネットシステム管理者へ報告する。

4 住基ネットシステム管理者は，実施状況の確認をする際に，次の各号に掲げる事項を月に1度確認しなければならない。

- (1) 事前に住民基本台帳ネットワーク機器追加申請書が提出され，了承が得られていること。
- (2) 追加した機器のセキュリティ対策は，継続して行われていること。
- (3) 追加した機器は，機器構成図に記載された場所に設置されていること。

(運用保守)

第9条 住基ネットシステム管理者は，保守対象機器と保守内容について，次の各号に掲げる事項を定めるものとする。

- (1) 保守対象機器の名称
- (2) 保守対象機器の管理責任者の氏名
- (3) 点検項目及び点検方法
- (4) 保守を行う者（以下「保守委託先」という。）の会社名，所属部署，氏名及び連絡先
- (5) 特記事項

2 住基ネットシステム管理者は，保守を行う必要が発生した場合には，次の各号に掲げる事項を確認しなければならない。

- (1) システム操作者は，障害対応のため，緊急に保守を行う場合は住基ネットシステム管理者に報告し，承認を得ること。
- (2) 保守委託先が，保守対象機器を外部へ持ち出す必要がある場合は，システム操

作者は、情報漏えい対策及び保険の適用を確認して住基ネットシステム管理者に報告し、承認を得ること。

(3) 保守作業において、一時的に機器を接続する場合は、機器接続の手続きに従うこと。

(4) 保守作業を行う場合は、システム操作者が立ち会い、これを監視すること。

3 保守委託先は、保守作業が終了した際に、次の各号に掲げる事項を作業報告書に記載し、住基ネットシステム管理者に提出しなければならない。

(1) 保守対象機器の名称

(2) 点検項目及び点検方法

(3) 点検結果

(4) 保守委託先の会社名、所属部署、氏名及び連絡先

(5) 立会ったシステム操作者の氏名

(6) 作業開始年月日時分

(7) 作業終了年月日時分

(8) 特記事項

4 住基ネットシステム管理者は、前項の作業報告書について、保管庫に7年間保管するものとする。

5 住基ネットシステム管理者は、実施状況の確認をする際に、次の各号に掲げる事項を年に1度確認しなければならない。

(1) 保守対象機器は、契約書に定められた内容で保守が実施されていること。

(2) 作業報告書の内容が適切であること。

(3) 作業報告書は、保管庫に7年間保管されていること。

(ラック等の鍵の管理)

第10条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第11号による鍵管理簿を作成し、ラック等（書庫及び保管庫をいう。以下この条において同じ。）の鍵の貸出、返却を行う際に、システム操作者に必要な項目を記録させなければならない。

(1) ラック等の名称

(2) 鍵番号

(3) 使用者の氏名

- (4) 使用理由
- (5) 貸出日時
- (6) 返却日時
- (7) 特記事項

2 システム操作者は、鍵の貸出及び返却の際に、次の各号に掲げる事項を行わなければならない。

- (1) 鍵管理簿へ必要事項を記載し、住基ネットシステム管理者の了承を得ること。
- (2) 鍵の盗難及び紛失時には、直ちに住基ネットシステム管理者へ報告すること。
- (3) 鍵の又貸しを行わないこと。
- (4) 鍵を返却する際は、鍵管理簿に必要事項を記録して住基ネットシステム管理者へ報告すること。

3 住基ネットシステム管理者は、実施状況の確認をする際に、次の各号に掲げる事項を月に1度確認しなければならない。

- (1) ラック等の鍵はすべて揃っていること。
- (2) 鍵管理簿に必要事項が記録されていること。
- (3) ラック等は、使用されていない状態において施錠が確実に行われていること。

(磁気媒体の管理)

第11条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第12号による磁気媒体管理簿を作成し、磁気媒体の作成、入手、保管又は廃棄を行う際に、システム操作者に必要な項目を記録させなければならない。

- (1) 作成又は入手に関する項目
 - ア ラベル名
 - イ 磁気媒体の数量及び種類
 - ウ 作成又は入手年月日
 - エ 作成者又は入手者
 - オ 使用理由及び内容
 - カ 住基ネットシステム管理者の承認印
- (2) 保管に関する項目
 - ア 保管場所
 - イ 保管年月日

(3) 廃棄に関する項目

- ア 廃棄年月日
- イ 廃棄者
- ウ 廃棄理由
- エ 廃棄方法
- オ 住基ネットシステム管理者の承認印

2 住基ネットシステム管理者は、システム操作者に磁気媒体を保管する際に、次の各号に掲げる事項を行わせなければならない。

- (1) 本人確認情報等の重要なデータが格納されている磁気媒体には、他の磁気媒体と判別できるようラベル名を付けること。
- (2) ラベル名は、記号のみとする等、最小限の項目を表記すること。
- (3) 磁気媒体は、保管庫に施錠保管し、権限のない者がアクセスできないようにすること。
- (4) 磁気媒体管理簿についても保管庫に施錠保管すること。

3 住基ネットシステム管理者は、システム操作者に磁気媒体を廃棄する際に、次の各号に掲げる事項を行わせなければならない。

- (1) システム管理者の承認を得てから廃棄すること。
- (2) 専用ソフトウェアによるフォーマット又は物理的粉砕により廃棄すること。また、電子計算機に内蔵されている固定ハードディスクの場合においても、専用ソフトウェアによるフォーマット又は物理的粉砕により廃棄すること。
- (3) 廃棄後、磁気媒体管理簿に記録して住基ネットシステム管理者に報告すること。
- (4) 磁気媒体を住基ネット以外の業務で再使用する場合には、磁気媒体に記録されたすべての内容を専用ソフトウェアにより消去すること。

4 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第13号による磁気媒体利用管理簿を作成し、磁気媒体を利用する際に、システム操作者に必要な項目を記録させなければならない。

- (1) ラベル名
- (2) 利用者
- (3) 利用内容（読取又は複写）
- (4) 利用理由

- (5) 利用日時
- (6) 返却予定日
- (7) 利用場所
- (8) 住基ネットシステム管理者の承認印
- (9) データ漏えい防止のための暗号化対策実施の有無
- (10) 返却日時
- (11) 住基ネットシステム管理者の確認印

5 システム操作者は、磁気媒体を利用する際に、次の各号に掲げる事項を行わなければならない。

- (1) 磁気媒体利用管理簿に必要な項目を記載して住基ネットシステム管理者の承認を得ること。
- (2) 利用中は、保管場所と同等の安全を確保し、権限のない者がアクセス可能な場所に放置しないこと。
- (3) 磁気媒体の盗難又は紛失時には、直ちに住基ネットシステム管理者へ報告すること。
- (4) 磁気媒体を返却する際は、磁気媒体利用管理簿に必要な事項を記載して住基ネットシステム管理者へ報告すること。

6 住基ネットシステム管理者は、実施状況の確認をする際に、次の各号に掲げる事項を月に1度確認し、記録しなければならない。

- (1) ラベル名がはり付けられていること。
- (2) 磁気媒体が、権限のない者によってアクセス可能な場所に放置されていないこと。
- (3) 磁気媒体管理簿に必要な項目（作成者、数量及び種類並びに廃棄時の記録を含む。）が記録されていること。
- (4) 磁気媒体管理簿と現況が一致し、かつ紛失がないこと。
- (5) 廃棄状況の記録が残っていること。
- (6) 磁気媒体利用管理簿に必要な項目（利用者、利用日時及び返却日時を含む。）が記録されていること。

（ドキュメントの管理）

第12条 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別

紙様式第14号によるドキュメント管理簿を作成し、ドキュメントの作成、入手、保管又は廃棄を行う際に、システム操作者に必要な項目を記録させなければならない。

(1) 作成又は入手に関する項目

- ア ドキュメント名
- イ 作成又は入手年月日
- ウ 作成又は入手者
- エ 内容（使用、複写等）
- オ 版数及び更新日時
- カ 住基ネットシステム管理者の承認印
- キ 使用の際の注意事項

(2) 保管に関する項目

- ア 保管場所
- イ 保管年月日

(3) 廃棄に関する項目

- ア 廃棄年月日
- イ 廃棄者
- ウ 廃棄理由
- エ 廃棄方法
- オ 住基ネットシステム管理者の承認印

2 住基ネットシステム管理者は、システム操作者にドキュメントを保管する際に、次の各号に掲げる事項を行わせなければならない。

(1) ドキュメントを保管庫に施錠保管し、権限のない者がアクセスできないようにすること。

(2) ドキュメント管理簿についても保管庫に施錠保管すること。

3 住基ネットシステム管理者は、ドキュメントを廃棄する際に、システム管理者に次の各号に掲げる事項を行わせなければならない。

(1) 事前に、住基ネットシステム管理者の承認を得てから廃棄すること。

(2) ドキュメントの内容を読み出せないよう焼却、裁断又は溶解により廃棄すること。

(3) 廃棄後、ドキュメント管理簿に記録して住基ネットシステム管理者に報告すること。

4 住基ネットシステム管理者は、次の各号に掲げる項目を記録するための別紙様式第15号によるドキュメント利用管理簿を作成し、ドキュメントを利用する際に、システム操作者に必要な項目を記録させなければならない。

- (1) ドキュメント名
- (2) 利用者
- (3) 利用内容（読取又は複写）
- (4) 利用理由
- (5) 利用日時
- (6) 返却予定日
- (7) 利用場所
- (8) 住基ネットシステム管理者の承認印
- (9) 返却日時
- (10) 住基ネットシステム管理者の確認印

5 システム操作者は、ドキュメントを利用する際に、次の各号に掲げる事項を行わなければならない。

- (1) ドキュメント利用管理簿に必要な項目を記載して住基ネットシステム管理者の承認を得ること。
- (2) 利用中は、保管場所と同等の安全を確保し、権限のない者がアクセス可能な場所に放置しないこと。
- (3) 原則として、設計書の重要なドキュメントの複写は行わないこと。
- (4) ドキュメントの盗難又は紛失時には、直ちに住基ネットシステム管理者へ報告すること。
- (5) ドキュメントを返却する際は、ドキュメント利用管理簿に必要な事項を記載して住基ネットシステム管理者へ報告すること。

6 住基ネットシステム管理者は、実施状況の確認をする際に、次の各号に掲げる事項を月に1度確認し、記録しなければならない。

- (1) ドキュメントが、権限のない者によってアクセス可能な場所に放置されていないこと。

- (2) ドキュメント管理簿に必要な項目（ドキュメント名，作成年月日及び作成者を含む。）が記録されていること。
- (3) ドキュメント管理簿と現況が一致し，かつ紛失がないこと。
- (4) ドキュメント利用管理簿に必要な項目（利用者，利用日時及び返却日時を含む。）が記録されていること。
- (5) 廃棄状況の記録が残っていること。

附 則

（施行期日）

この規程細則は，平成28年10月1日から施行する。

（行財政局人事部厚生課）