参考資料１

鳥取県住民基本台帳ネットワークシステム管理運営要綱

（趣旨）
第1条　この要綱は、鳥取県における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。）の管理及び運営について必要な事項を定めるものとする。

（用語の定義）
第2条　この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
（1）　住基ネット　県内の市町村長、知事及び指定情報処理機関（住民基本台帳法（昭和42年法律第81号。以下「法」という。）第30条の10第1項に規定する指定情報処理機関をいう。以下同じ。）の使用に係るサーバ、業務端末等、電気通信関係装置（ファイアウォールを含む。以下同じ。）、電気通信回線、プログラムにより構成され、市町村長が本人確認情報（法第30条の5第1項に規定する本人確認情報をいう。以下同じ。）を知事に通知し、知事が本人確認情報を指定情報処理機関に通知し、並びに知事及び指定情報処理機関が本人確認情報の記録、保存及び提供を行うためのシステム
（2）　セキュリティ　住基ネットの完全性、機密性及び可用性の確保を図ることを目的とした行為
（3）　サーバ　市町村長から本人確認情報の通知及び転出確定通知を受け、本人確認情報の記録、保存及び提供を行い、指定情報処理機関に本人確認情報の通知を行うための知事の使用にかかる電子計算機
（4）　ファイアウォール　住基ネットにおいて不正な侵入を防御する電子計算機
（5）　業務端末等　県において本人確認情報を検索する際に使用する電子計算機、ICカードリーダライタ及びプリンタ
（6）　共同利用所属　業務端末等を設置しない所属
（7）　操作者用ICカード　サーバ又は業務端末等を動作させる際に操作者を識別するICチップが埋め込まれたカード
（8）　プログラム　サーバ及び業務端末等を機能させて住基ネットを動作させるための処理手順
（9）　管理区域　サーバ及び電気通信関係装置を設置する室
（10）　ドキュメント　住基ネットの設計及び運用に関する記録及び文書

（セキュリティ統括管理者等）
第3条　住基ネットのセキュリティ対策を総合的に実施するため、セキュリティ統括管理者を置く。
2　セキュリティ統括管理者は、企画部参事監（情報技術に関する統括事務を行う者に限る。以下、「IT統括監」という。）をもって充てる。

（システム管理者）
第4条　住基ネットの適切な管理を行うため、システム管理者を置く。
2　システム管理者は、情報政策課長をもって充てる。

（セキュリティ管理者）
第5条　住基ネットを利用する部署においてセキュリティ対策を実施するため、セキュリティ管理者を置く。
2　セキュリティ管理者は、業務端末システムを設置する部署の所属長及び本人確認情報を利用する部署の所属長をもって充てる。

（鳥取県住基ネットセキュリティ会議）
第6条　セキュリティ統括管理者は、鳥取県住基ネットセキュリティ会議（以下「セキュリティ会議」という。）を招集するとともに、議長を務める。
2　セキュリティ会議は、セキュリティ統括管理者、システム管理者、県民室長、自治振興課長をもって組織する。
3　セキュリティ会議は、次に掲げる事項を所掌する。

（1） 市町村及び関係機関からの情報収集及び円滑な連絡調整に関すること。
（2） 住基ネットのシステムに係るセキュリティ対策に関すること。
（3） 重大障害又は重大不正行為が発生した場合の対応に関すること。
（4） その他システムのセキュリティ確保のため必要な事項に関すること。

（個人情報保護審議会等からの意見聴取）
第7条 システム管理者は、特に必要と認められる事項について、鳥取県住民基本台帳法施行条例（平成14年鳥取県条例第42号。以下「条例」とする。）の規定により設置される、個人情報保護審議会の意見を聴くものとする。
2 システム管理者は、必要と認めるときは、関係職員に対して意見又は説明を聴くことができる。

（関係部署に対する指示等）
第8条 システム管理者は、セキュリティ管理者に対しセキュリティ上必要な要請、又は指示をすることができる。

（管理区域の入退室管理）
第9条 管理区域への入退室については、システム管理者が事前に許可した者についてのみ、これを行うことができる。

（改善の要求）
第10条 セキュリティ統括管理者は、管理区域への適切な入退室管理が行われていないと判断される場合、システム管理者から報告を求め、調査を行い、必要な改善を求めることができる。

（アクセス制御）
第11条 システム管理者は、閲覧権限がない職員等がアクセスすることが不可能となるように、システム上制限しなければならない。
2 前項は、操作者用ICカード及びパスワードにより操作者の正当な権限を確認すること並びに操作履歴を記録することにより行うものとする。
3 業務端末等が設置された所属のセキュリティ管理者は、業務端末等使用簿（様式第1号）を備え付け、操作者は業務端末等を使用する都度業務端末等使用簿に使用状況を記載しなければならない。

（操作者用ICカードの発行及び回収）
第12条 システム管理者は、セキュリティ管理者が業務端末等使用者報告書（様式第2号）により指定した職員に操作者用ICカードを貸与するものとし、退職、人事異動等に際しては、回収する。
2 システム管理者は、操作者用ICカードの発行及び回収の都度、操作者用ICカード発行簿（様式第3号）に記載し、発行の際セキュリティ管理者から操作者用ICカード受領書（様式第4号）を徴さなければならない。

（操作者用ICカードの管理）
第13条 セキュリティ管理者は、操作者用ICカードの不正使用及び損傷がないよう管理し、操作者用ICカードを施錠可能な保管庫等に保管しなければならない。
2 操作者用ICカードの貸与を受けた職員は、次に掲げる事項を遵守しなければならない。
（1） 操作者用ICカードを紛失し又は盗難されないよう、責任をもって管理すること。
（2） 操作者用ICカードを他者に貸与し、若しくは職員間で共有を行ってはならないこと。
（3） 操作者用ICカードを目的外に利用してはならないこと。
（4） 操作者用ICカードをカードリーダに常時挿入しないこと。
（5） 操作者用ICカードを紛失し又は盗難された場合は、セキュリティ管理者を通じて、直ちにシステム管理者に報告すること。
3 システム管理者は、操作者用ICカード管理簿（様式第5号）を作成しなければならない。
4 セキュリティ管理者は、所属の職員に貸与された操作者用ICカードについて、適正な利用及び管理が行われるよう必要な措置を講じなければならない。

5　システム管理者は、適正に操作者用ICカードが管理、利用されるよう、セキュリティ管理者及び各操作者に対して指導を行うこととする。
6　操作者用ICカードの紛失又は盗難の届出があった場合は、システム管理者は速やかに失効の手続きをとると共に、セキュリティ管理者に再発防止策の策定等を指示しらなければならない。

（パスワード）
第14条　各操作者は、操作者用ICカードに設定したパスワードの管理について、次に掲げる事項を遵守しなければならない。
（1）　操作者は、パスワードについて、他者への漏えいを防止する手段を講ずるとともに、他者が知り得る状態においてはならないこと。
（2）　パスワードは6文字以上とし、規則性のあるものや、容易に推測可能なものをパスワードに設定してはならないこと。
（3）　操作者は、パスワードについて、半年に1回以上変更を行わなければならないこと。
（4）　操作者は、前号の規定により自ら変更を行う場合を除き、パスワードを変更する必要が生じたときは、セキュリティ管理者を経由してパスワード変更申請書（様式第6号）によりシステム管理者に依頼すること。

（操作者用ICカードの再発行）
第15条　操作者は、操作者用ICカードの紛失、損傷又はその他の事由によりICカードの再発行を受ける必要があるときは、セキュリティ管理者を経由して操作者用ICカード再発行申請書（様式第7号）をシステム管理者に提出しなければならない。
2　システム管理者は、前項の操作者用ICカード再発行申請書の提出を受けたときは、内容を調査し、再発行の必要を認めた場合は再発行する。
3　システム管理者は、再発行の際、セキュリティ管理者から操作者用ICカード受領書（様式第4号）を徴さなければならない。

（操作履歴の記録及び解析）
第16条　システム管理者は、業務端末等の操作履歴について、7年前までさかのぼって解析できるよう、保管するものとする。
2　システム管理者は、年に1回以上前項の操作履歴を解析し、住基ネットの適正な利用を確保しなければならない。

（情報資産の管理）
第17条　住基ネットの情報資産（住基ネットに係るすべての情報並びにソフトウェア、ハードウェア、ネットワーク及び磁気ディスクをいう。以下「情報資産」という。）について、管理責任者を置くものとする。
2　前項の情報資産のうち、住基ネットを利用する部署に設置する業務端末等の情報資産に関する管理責任者はセキュリティ管理者とする。
3　本人確認情報、当該本人確認情報が記録されたサーバに係る帳票のほか、業務端末等を除く住基ネットの情報資産に関する管理責任者はIT統括監とする。

（本人確認情報を取り扱うことができる者）
第18条　本人確認情報は次の者に限り、取り扱うことができる。
（1）　企画部地域づくり支援局情報政策課において、住基ネットに関する事務に従事する職員
（2）　住基ネットを利用する部署において、法別表第3、別表第5及び条例に定める事務に従事する職員
（3）　鳥取県から本人確認情報の管理について委託を受けた事業者のうち、別に指定するもの

（本人確認情報に関する秘密保持義務）
第19条　次の各号に掲げるものは、法第30条の31第1項の秘密保持義務の対象となるものであるので、その取扱いについては留意しなければならない。

（1） 本人確認情報
（2） 住基ネットのセキュリティに関する情報技術
（3） 操作者用ICカードのパスワード
（4） 住基ネットの具体的な運用に関する情報
（5） 運用手引書

（本人確認情報を取扱うに当たっての留意事項）
第20条 本人確認情報を取扱うに当たっては、次の各号について留意すること。
（1） 本人確認情報の検索は、業務上必要な場合に限り行うものであること。
（2） 本人確認情報画面を表示する場合は、業務上必要のない本人確認情報を表示しないこと。
（3） 業務端末システムから離れる際には、スクリーンセーバー機能を活用し、長時間にわたり本人確認情報を表示したままの状態にしないこと。
（4） 表示された本人確認情報が、来庁者から見えない位置に業務端末機を設置すること。
1. 本人確認情報を表示した画面のハードコピーは、業務上必要な場合に限り取得又は出力すること。
2. 本人確認情報の出力は、業務上必要な場合に限り行うこと。
3. 前号により出力した帳票は、適正に管理し、本人確認情報が出力された帳票を廃棄する場合においては、シュレッダー等により裁断する等の措置を講ずること。

（本人確認情報の記録されたサーバにおいて出力される帳票の取扱い）
第21条 システム管理者は、本人確認情報の記録されたサーバにおいて出力される帳票において以下の事項を記録するものとする。
（1） 出力帳票の種類
（2） 出力年月日
（3） 使用目的
（4） 申請者
（5） 数量
2 システム管理者は前項に掲げる帳票を施錠が可能な保管庫に保管し、紛失及び盗難を防止するための措置を講じるものとする。
3 システム管理者は、前項に掲げる帳票を廃棄する場合においては、シュレッダー等により裁断する等の措置を講ずるものとする。

（操作履歴の開示）
第22条 システム管理者は、業務端末等の操作履歴について、本人から請求があった場合、開示できるよう調整するものとする。

（業務の委託）
第23条 システム管理者及びセキュリティ管理者は、外部委託をしようとする場合においては、あらかじめ、委託を受けようとする者における情報の保護に関する管理体制等について確認するものとする。

（外部委託の承認）
第24条 セキュリティ管理者は、外部委託をしようとするときは、委託する事務の内容、理由及び情報の保護に関する事項等について、あらかじめ、システム管理者の承認を受けなければならない。

（委託契約書への記載事項）
第25条 開発又は保守等を外部委託事業者に発注する場合は、外部委託事業者から再委託を受ける事業者も含めて必要に応じて次の条件（再委託事業者が遵守すべき事項を含む）を明記した契約を締結しなければならない。
（1） 再委託の制限に関する事項
（2） 本人確認情報等の保管、返還又は廃棄に関する事項

(3) 本人確認情報等の目的外使用の禁止、複製・複写及び第三者への提供の禁止に関する事項
(4) 本人確認情報等の秘密保持に関する事項
(5) 事故等の報告に関する事項
(6) 県の情報セキュリティの遵守
(7) 業務上知り得た情報の守秘義務
(8) 提供された情報の返還義務
(9) 県による定期的な報告徴収、監査・検査の実施
(10)従業員に対する教育の実施
(11)県の情報セキュリティの遵守のために構築する体制
(12)県の情報セキュリティが遵守されなかった場合の規定(契約解除、損害賠償等)
(13)分類1の情報資産係るデータバックアップのための外部施設等への搬送時における暗号化による盗難、不正コピー等の防止
(14)作業場所の特定

(受託者の管理状況の調査)
第26条 システム管理者及びセキュリティ管理者は、必要に応じ、受託者における当該外部委託に係るセキュリティ対策の実施状況について調査するものとする。

(オペレーション計画)
第27条 システム管理者は、指定情報処理機関、管内市町村及び住基ネットを利用する部署と協議の上、次の各計画を策定するものとする。
(1) システム運用計画
(2) 緊急時対応計画
2 システム管理者は、オペレーションに関する各計画の見直しを必要に応じて行う。また、セキュリティ管理者は、障害が発生する確率を下げるため、オペレーションミスの原因分析、再現防止策の策定など、必要な措置を講じるものとする。

(監査)
第28条 システム管理者は、住基ネットの本人確認情報処理事務等について、年に一回以上内部監査を実施するほか、必要に応じて外部監査を実施するよう努めなければならない。
2 システム管理者は、監査結果をもとに必要な改善措置を講じるものとする。
3 システム管理者は、監査結果及び改善措置について、セキュリティ統括管理者に報告するものとする。

附 則
この要綱は、平成14年8月2日から施行する。
附 則
この要綱は、平成18年3月3日から施行する。
附 則
この要綱は、平成18年4月1日から施行する。
附 則
この要綱は、平成19年8月24日から施行し、第4条、第17条及び第18条の改正は、同年7月5日から適用する。
附 則
この要綱は、平成20年4月1日から施行する。
附 則
この要綱は、平成20年4月23日から施行する。

様式第１号（第 11 条関係）

業務端末等使用簿

日付	開始時間	終了時間	所属名	職名	氏名	利用業務	カード種類	カード番号	チェック

様式第２号（第 12 条関係）

業務端末システム使用者報告書

年　　月　　日

住基ネットシステム管理者　様

セキュリティ管理者
所　属　長　　印

次のとおり業務端末使用者を指定（追加・変更）しました。

係　名	職　名	職員番号	氏　名	利用事務	指定 （追加・削除・継続）	備　　考

注１）　指定欄に、追加、削除、継続のいずれかを記入し、備考欄にその旨記入すること
　　備考欄例　４月１日付け　人事異動。

注２）　提出時点の端末使用者をすべて記入すること

様式第３号（第12条関係）

操作者用ＩＣカード発行簿

発行日	所　属　名	職名	氏名	権限種別	ICｶｰﾄﾞ番号	返納日等	理　由

様式第４号（第12条関係）

操作者用ＩＣカード受領書

権　限　種　別：

操作者用ＩＣカード番号：

パスワード確認：

年　　月　　日

住基ネットシステム管理者　様

上記操作者用ＩＣカードを受領しました。

所属名

職氏名　　印

注１）　操作者用ＩＣカード番号は、カードの表書きの番号を記入すること。
注２）　パスワードについては、確認の結果を良、不良で記入すること。

様式第５号（第13条関係）

操作者用ＩＣカード管理簿

カード種別	カード番号	貸与者			貸与日	ｶｰﾄﾞﾁｪｯｸ日	備　考
		所属	職名	氏名			

様式第６号（第14条関係）

パスワード変更申請書

年　　月　　日

住基ネットシステム管理者　様

セキュリティ管理者
所　属　長　　印

下記職員の操作者用ＩＣカードのパスワード変更を申請します。

記

１　職員の職氏名
　　職　名
　　氏　名

２　パスワードの変更を必要とする理由

３　今回パスワードを変更しようとする操作者用ＩＣカード番号

様式第７号（第15条関係）

操作者用ＩＣカード再発行申請書

年　　月　　日

住基ネットシステム管理者　様

セキュリティ管理者
所　属　長　　印

下記職員の操作者用ＩＣカードの再発行を申請します。

記

１　職員の職氏名
　　職　名
　　氏　名

２　再発行が必要となった理由

３　紛失又は損傷等の操作者用ＩＣカード番号