西宮市住民基本台帳ネットワークシステムの運用管理に関する要綱

西宮市住基ネット管理委員会の設置及び住民基本台帳ネットワークシステムの運用管理に関する要綱（平成１４年１１月５日）の全部を改正する。

目　次

第１章　総則

（目的）

第１条　この要綱は、西宮市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。）のセキュリティを確保するとともに、適切な運用及び維持管理を図り、もって個人情報の保護を図ることを目的とする。

（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　コミュニケーションサーバ（以下「ＣＳ」という。）、都道府県サーバ、機構サーバ、認証業務連携サーバ、業務端末機、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、プログラム等により構成され、市町村長（地方自治法（昭和２２年法律第６７号）第２８１条に規定する特別区の区長を含む。以下同じ。）が本人確認情報（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６第１項に規定する本人確認情報をいう。以下同じ。）を都道府県知事に通知し、都道府県知事が本人確認情報を地方公共団体情報システム機構（以下「機構」という。以下同じ。）に通知し、市町村の区域を越えた住民基本台帳

に関する事務を処理し、並びに市町村長、都道府県知事及び機構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をいう。

（２）ＣＳ　転入通知（法第９条第１項の規定による通知をいう。）、住民票の写しの交付の特例（法第１２条の４の規定による本人等の請求に係る住民票の写しの交付の特例をいう。）、戸籍の附票記載事項通知（法第１９条第１項の規定による通知をいう。）及び転入届の特例（法第２４条の２の規定による個人番号カード（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号。以下「番号利用法」という。）第２条第７項に規定する個人番号カードをいう。）の交付を受けている者等に関する転入届の特例をいう。）のために必要な情報を市町村長間で通知し、都道府県知事に本人確認情報の通知及び転出確定通知（住民基本台帳法施行令（昭和４２年政令第２９２号）第１３条第３項の規定による通知をいう。以下同じ。）を行い、並びに機構に個人番号とすべき番号の生成（番号利用法第８条第１項の規定による個人番号とすべき番号の生成をいう。）のために必要な情報を通知し、機構から個人番号とすべき番号の通知（行政手続における特定の個人を識別するための番号の利用等に関する法律施行令（平成２６年政令第１５５号）第９条の規定による通知をいう。）を受け、行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令（平成２６年総務省令第８５号。以下「番号利用法総務省令」という。）第３５条第２号及び第７に掲げる事務に係る情報を機構との間で通知し、及び認証業務（電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成１４年法律第１５３号。以下「公的個人認証法」という。）第２条第３項に規定する認証業務をいう。以下同じ。）の実施のために必要な情報を機構との間で通知するために市町村長が使用する電子計算機をいう。

（３）都道府県サーバ　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、並びに機構に本人確認情報の通知を行うために都道府県知事が使用する電子計算機をいう。

（４）機構サーバ　都道府県知事から本人確認情報の通知を受け、本人確認情報の記録、保存及び提供を行い、並びに市町村長から個人番号とすべき番号の生成のために必要な情報を受け、及び市町村長に個人番号とすべき番号を通知するために機構が使用する電子計算機をいう。

（５）認証業務連携サーバ　機構が電子証明書（公的個人認証法第３条第１項に規定する署名用電子証明書及び公的個人認証法第２２条第１項に規定す

る利用者証明用電子証明書をいう。）の発行を受けている者に係る機構保存本人確認情報（法第３０条の９に規定する機構保存本人確認情報をいう。）のうち個人番号以外のものを利用するための機構が使用する電子計算機をいう。

（６）プログラム　電子計算機を機能させて住基ネットを作動させるための命令を組み合わせたものをいう。

（７）情報資産　住基ネットに係る全ての情報並びにハードウエア、ソフトウエア、ネットワーク及び磁気ディスクをいう。

（８）ファイアウォール　ネットワークにおいて、不正侵入を防御する電子計算機をいう。

（９）ドキュメント　住基ネットの設計、プログラムの作成及び運用に関する記録及び文書をいう。

（１０）照合情報認証　静脈等の情報に不可逆演算を施して登録された情報（照合情報）と認証時に読み取られる情報を照合することにより認証する方法をいう。

（１１）照合ＩＤ　操作者を識別するためのＩＤをいう。

（１２）操作者ＩＤ　操作権限を識別するためのＩＤをいう。

第２章　セキュリティ組織

（セキュリティ統括責任者）

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、セキュリティ統括責任者を置く。

２　セキュリティ統括責任者は、市民部長をもって充てる。

３　セキュリティ統括責任者は、本人確認情報の安全確保措置、本人確認情報に関する秘密及び本人確認情報の電子計算機処理に関する秘密の保持義務、本人確認情報の業務外利用及び提供の禁止その他この要綱に定めるセキュリティの確保、適切な運用を図るための事項について指導し、遵守させなければならない。

（システム管理者）

第４条　住基ネットに係るシステムの適切な維持、保全、管理及び運用を実施するため、システム管理者を置く。

２　システム管理者は、デジタル推進課長をもって充てる。

３　システム管理者が不在又は事故等で欠けたときに対応するため、あらかじめ所属の職員の中からシステム管理補助者を指名しておくものとする。

４　前項の規定により指名を受けた職員は、システム管理者が不在又は事故等で欠けたときにその職務を代理する。

（本人確認情報管理責任者）

第５条　住基ネットに係る本人確認情報のセキュリティ対策を実施するため、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、市民課担当課長をもって充てる。

３　本人確認情報管理責任者が不在又は事故等で欠けたときに対応するため、あらかじめ所属の職員の中から本人確認情報管理補助者を指名しておくものとする。

４　前項の規定により指名を受けた職員は、本人確認情報管理責任者が不在又は事故等で欠けたときにその職務を代理する。

（セキュリティ責任者）

第６条　住基ネットの業務端末機を使用する部署において、セキュリティ対策を実施するため、セキュリティ責任者を置く。

２　セキュリティ責任者は、デジタル推進課長、市民課長、市民課担当課長、各支所長、アクタ西宮ステーション所長並びに住民基本台帳法別表第二及び別表第四に規定する事務の担当課長をもって充て、セキュリティ責任者となる同法別表第二及び別表第四に規定する事務の担当課長は別に定める。

３　セキュリティ責任者が不在又は事故等で欠けたときに対応するため、あらかじめ所属の職員の中から補助者を指名しておくものとする。

４　前項の規定により指名を受けた職員は、セキュリティ責任者が不在又は事故等で欠けたときにその職務を代理する。

（住基ネットセキュリティ会議）

第７条　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。

２ セキュリティ会議は、セキュリティ統括責任者のほか、次に掲げる者をもって組織する。

（１）市民課長

（２）市民課担当課長

（３）デジタル推進課長

（４）その他セキュリティ統括責任者が審議に必要と認めた者

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。

（１）住基ネットのセキュリティ対策の決定及び見直しに関すること。
（２）前号の遵守状況の確認に関すること。
（３）緊急時対応計画の策定及び緊急時の対応に関すること。
（４）その他住基ネットのセキュリティに係る重要事項に関すること。
４　議長は、前項の決定を行うにあたり、特に個人情報の保護に重要な影響を及ぼすと認める場合は、西宮市個人情報保護条例（平成１５年西宮市条例第２４号）第４８条第１項に規定する個人情報保護審議会の意見を聴くものとする。
５　議長は、第３項の規定による決定を行ったときは、関係部署に対し周知を行い、その推進に努めなければならない。
６　住基ネットセキュリティ会議の庶務は、市民課において処理する。

（監査）
第８条　セキュリティ統括責任者は、住基ネットのセキュリティを確保するために、必要に応じて監査を受けなければならない。
２　前項の規定により監査を行った者は、監査報告書を作成し、必要に応じて問題点の指摘及び改善の勧告を行うものとする。
３　セキュリティ統括責任者は、監査報告書の結果により必要がある場合は、システム管理者又は本人確認情報管理責任者に命じて、改善計画を作成しなければならない。

（教育・研修）
第９条　セキュリティ統括責任者は、住基ネットに携わる部署の職員に対し、住基ネットのセキュリティ対策並びにＣＳ等及び業務端末機その他操作に関する教育・研修を行う。
２　セキュリティ統括責任者は、前項の教育・研修を行うために、対象者、内容、実施時期等を盛り込んだ教育・研修計画を作成する。
３　本人確認情報管理責任者は、前項の教育・研修計画をもとに、住基ネットの本人確認情報の重要性を認識させ、プライバシー保護に関する意識の高揚を図るために関係職員に対し、計画的に教育・研修を実施するものとする。
４　前項の規定は、システム管理者がシステムに従事する職員の教育・研修について準用する。

第３章　入退室管理

（入退室の管理）
第１０条　住基ネットの管理及び運用が行われる室及び場所の入退室管理者及び

セキュリティ区分は、次のとおりとし、当該区分に基づき、入退室管理を行う。

室及び場所	入退室管理者	セキュリティ区分
住基ネットの本人確認情報、セキュリティ情報等の保管室	システム管理者	レベル２
ＣＳ及びネットワーク機器の設置室		
業務端末機の設置室	業務端末機を設置する部署のセキュリティ責任者	レベル１

２　セキュリティ区分に応じた管理内容は、次のとおりとする。

区　分	管　　理　　内　　容
レベル２	① システム管理者（第４条第３項の規定によるシステム管理補助者を含む。以下この項において同じ。）が入退室の資格を許可する人数は必要最小限とし、事前に許可を得ている者のみが入退室できる。 ②入退室は、その都度、ＩＤ及び照合情報認証により確認を行う。 ③鍵並びにＩＤ及び照合情報認証の管理は、システム管理者が行い、システム管理者から事前に許可を得ている者のみに鍵を貸与する。 ④鍵の受渡し並びにＩＤ及び照合情報認証による入退室についての記録を行い、当該記録を３年間保存する。 ⑤入退室者の識別を行うために、入退室者には名札等の着用を義務付ける。 ⑥システムエンジニアその他関係者が、住基ネットのシステム及び機器（電気通信関係装置を含む。）の保守､入替作業等のために入退室を行う場合は、職員の承認を必要とする。
レベル１	① 業務端末機を設置する部署のセキュリティ責任者（第６条第３項の規定による補助者を含む。以下この項において同じ。）が入退室の資格を許可する人数は必要最小限とし、事前に許可を得ている者のみが入退室できる。 ②業務端末機を設置する部署のセキュリティ責任者は目視により入退室者の監視を行う。 ② 入退室についての日付及び時間の記録を行い、当該記録を３年間保存する。

	④入退室者の識別を行うために、入退室者には名札の着用を義務付ける。 ⑤システム管理者は、セキュリティ責任者が所管する業務端末機の保守、入替作業等に従事させるため所属職員（住基ネットに係る委託業者を含む。）を派遣する場合は、事前にセキュリティ責任者に連絡をするものとする。

3　第１項の規定による入退室管理者は、前項に定める管理を行うほか、住基ネットのセキュリティを確保するために必要な措置を講じなければならない。

第４章　アクセス管理

（アクセスの管理）

第１１条　次に掲げる住基ネットの構成機器について、アクセス管理を行う。

（１）ＣＳ及びシステム管理用の業務端末機（以下「ＣＳ等」という。）

（２）業務端末機

（３）ファイアウォール

2　前項第１号及び第２号のアクセス管理は、パスワード及び照合情報認証により、第３号のアクセス管理はパスワードにより、操作者の正当な権限を確認し、並びに操作履歴及び通信履歴を記録することにより行うものとする。

（アクセス管理責任者）

第１２条　前条のアクセス管理を行う機器の管理者は、次のとおりとする。

機器	管理者				
	オペレーティングシステム		照合ＩＤ及び操作者ＩＤ	操作履歴	通信履歴
	ユーザＩＤ	パスワード			
ＣＳ等	システム管理者	同左	同左	同左	同左
業務端末機	システム管理者	業務端末機を設置する部署のセキュリティ責任者	同左	同左	システム管理者
ファイアウォール	システム管理者	同左	－	－	システム管理者

2　アクセス管理責任者は、デジタル推進課長をもって充てる。

（オペレーティングシステムの管理）

第１３条　システム管理者は、前条に規定するアクセス管理を実施するほか、ＣＳ等のオペレーティングシステムについて、次に掲げるセキュリティ対策を実施しなければならない。

（１）ユーザＩＤに付与する権限については、業務上必要最低限のものとすること。

（２）操作者が業務に利用するユーザＩＤについて、業務以外の操作及び設定変更を行うことができないように制限すること。

（３）ユーザＩＤ及びその権限について、定期に又は随時に見直しを行い、不要なユーザＩＤについては速やかに削除すること。

２　セキュリティ責任者は、定期に又は随時に、ログオンの履歴を確認し、不正なアクセスがないか検査しなければならない。

３　システム管理者は、ユーザＩＤ管理簿を作成し、これを３年間保存するものとする。

（パスワードの管理）

第１４条　システム管理者は、当該システム管理者が所管するＣＳ等のオペレーティングシステム及びファイアウォールのパスワードに関し、業務端末機を設置する部署のセキュリティ責任者は、当該セキュリティ責任者が所管する業務端末機のパスワードに関し、次に掲げる事項を実施しなければならない。

（１）初期設定されているパスワードについては、速やかに変更すること。

（２）パスワードについては、規則性のあるもの又は推測可能なものは使用しないこと。

（３）パスワードの有効期間は、ＣＳ等のオペレーティングシステムにあっては９０日間、ファイアウォールにあっては１８０日間とし、必ず有効期間内に更新すること。

（４）パスワードは、英大文字、英小文字、数字及び記号が混在の最低８桁以上で設定すること。

２　システム管理者は、前項に規定するファイアウォールを除く全てのパスワードについて、連続で３回間違えた場合にはロックアウト（無効）になるよう設定するものとする。

３　何人も、パスワードを他者に漏らし、若しくは他者が知り得る状態においてはならない。

（操作者の管理）

第１５条　ＣＳ等に係る操作者はシステム管理者が、業務端末機に係る操作者は所属のセキュリティ責任者が管理する。操作者の管理は、操作者の照合ＩＤ、照合情報及び操作者ＩＤを管理するものとする。

２　システム管理者（第４条第３項の規定によるシステム管理補助者を含む。以下第８項まで同じ。）は、運用処理が必要と認められる者をＣＳ等の操作者とし、その操作者に対し、照合ＩＤの付与、照合情報の登録、適切な操作権限の付与及び操作者ＩＤの付与をすることができる。

３　セキュリティ責任者（第６条第３項の規定による補助者を含む。以下第９項まで同じ。）は、業務処理が必要と認められる者を業務端末機の操作者とすることができる。

４　市民課のセキュリティ責任者は、各部署のセキュリティ責任者及び操作者に対し、照合ＩＤの付与、照合情報の登録、適切な操作権限の付与及び操作者ＩＤの付与をすることができる。

５　セキュリティ責任者は所属の操作者に対し、照合ＩＤの付与、照合情報の登録、適切な操作権限の付与及び操作者ＩＤの付与をすることができる。

６　第４項及び前項の操作権限ごとの操作者について、セキュリティ責任者と本人確認情報管理責任者が協議の上、決定する。

７　システム管理者は、第２項の照合情報の登録の際に、セキュリティ責任者は、第４項及び第５項の照合情報の登録の際に、照合情報を登録する者が適正に照合情報を登録するように管理する。

８　システム管理者は、ＣＳ等に係る操作者について、人事異動等により運用処理が必要でなくなった場合は、速やかに照合ＩＤ、照合情報及び操作者ＩＤの削除をしなければならない。

９　市民課のセキュリティ責任者は、各部署のセキュリティ責任者について、各部署のセキュリティ責任者は、所属の操作者について、人事異動等により業務処理が必要でなくなった場合は、速やかに照合ＩＤ、照合情報及び操作者ＩＤの削除を、業務に変更が生じた場合は、速やかに適切な操作権限及び操作者ＩＤの追加又は削除をしなければならない。ただし、市民課のセキュリティ責任者は、各部署の操作者について削除及び変更をすることができる。

１０　システム管理者は、ＣＳ等の操作者名簿及び照合ＩＤ並びに操作権限の管理簿を、セキュリティ責任者は、業務端末機の操作者名簿及び照合ＩＤ並びに操作権限の管理簿を作成し、これを７年間保管しなければならない。

１１　システム管理者及び第２項の規定による操作者以外の者は、ＣＳ等の操作をすることはできない。

１２　本人確認情報管理責任者、セキュリティ責任者及び第３項の規定による操作者以外の者は、業務端末機の操作をすることはできない。
１３　ＣＳ等の操作者及び業務端末機の操作者は、次に掲げる事項を誠実に実施及び遵守しなければならない。
（１）ＣＳ等又は業務端末機を業務上必要な処理以外に使用しないこと。
（２）照合ＩＤ、照合情報及び操作者ＩＤを業務上必要な処理以外に使用しないこと。
１４　操作者の管理状況、照合ＩＤ及び操作者ＩＤの利用状況その他必要な事項について、システム管理者は、ＣＳ等に関して、本人確認情報管理責任者は、業務端末機に関して、検査を定期に又は随時に行うものとする。
１５　前項の場合において、システム管理者が不在又は事故等で欠けたため、当該検査ができないときはシステム管理補助者が、本人確認情報管理責任者が不在又は事故等で欠けたため、当該検査ができないときは本人確認情報管理補助者が、それぞれ代行する。
１６　操作者は第１４項の検査があった場合は、協力する義務を負う。
１７　システム管理者はＣＳ等の操作履歴を、業務端末機を設置する部署のセキュリティ責任者は業務端末機の操作履歴を、定期に又は随時に確認し、適切に運用されているか検査しなければならない。
１８　前項の操作履歴の保管期間は７年間とする。

（操作履歴等の記録の管理）
第１６条　システム管理者は、ＣＳに記録された操作履歴及びファイアウォールに記録された通信履歴について、７年前までさかのぼって解析できるよう保管しなければならない。

（業務端末機の利用時間）
第１７条　業務端末機の利用時間は、原則として、西宮市の休日を定める条例（平成２年西宮市条例第２２号）第２条第１項に規定する市の休日を除く日の午前９時から午後５時３０分まで（セキュリティ責任者が必要と認める場合は、午後7時３０分まで）とする。ただし、アクタ西宮ステーションにおいては、西宮市の休日を定める条例第２条第１項第１号及び第２号に規定する市の休日の午前９時から午後４時まで利用できるものとする。

第５章　本人確認情報管理

（本人確認情報の管理）

第１８条　セキュリティ統括責任者、本人確認情報管理責任者、システム管理者、セキュリティ責任者､ＣＳ等の操作者及び業務端末機の操作者は、法に定められた業務の遂行にのみ本人確認情報を利用し、提供するものとし、これ以外に本人確認情報を利用し、提供してはならない。

２　システム管理者は、本人確認情報の漏洩、滅失及び毀損の防止その他本人確認情報の適切な管理を行うために必要な措置を講じなければならない。

３　システム管理者は、前項の規定に基づく措置状況を定期に又は随時に把握しておかなければならない。

４　システム管理者は、本人確認情報に障害が生じ、若しくは生じる恐れが判明したときは、直ちにセキュリティ統括責任者の承認を得て、当該ＣＳ等若しくは業務端末機をネットワークから切り離さなければならない。ただし、緊急やむを得ない場合は、当該承認を得ずに切り離すことができる。

５　システム管理者は、前項本文の規定によりネットワークから切り離したときは、セキュリティ統括責任者及び本人確認情報管理責任者に、前項ただし書の規定によりネットワークから切り離したときは、セキュリティ統括責任者及び本人確認情報管理責任者に直ちに報告しなければならない。

６　前項の規定による連絡を受けた本人確認情報管理責任者は、セキュリティ責任者にその旨を連絡するとともに、セキュリティ責任者から業務端末機の操作者にその旨を伝達するものとする。

７　前項の規定による連絡を受けた業務端末機を設置する部署のセキュリティ責任者は、システム管理者又は本人確認情報管理責任者の指示があるまでは、業務端末機の全部又は一部の使用を停止しなければならない。

（本人確認情報送信の停止）

第１９条　セキュリティ統括責任者は、機構、国の機関等、都道府県知事その他の都道府県の執行機関、市町村長その他の市町村の執行機関又は機構において、本人確認情報若しくは異動等情報が適切に管理又は運用されていないと認める場合は、本人確認情報の送信を停止するものとする。この場合において、セキュリティ統括責任者は、当該本人確認情報若しくは異動等情報の適切な管理のための措置の実施状況について報告を求め、当該本人確認情報若しくは異動等情報の適切な管理のための措置の実施について要請を行うことができる。

（住民基本台帳カード及び個人番号カードの管理）

第２０条　セキュリティ責任者は、返納された住民基本台帳カード（行政手続における特定の個人を識別するための番号の利用等に関する法律の施行に伴う関係法律の整備

等に関する法律（平成２５年法律第２８号）第１９条の規定による改正前の住民基本台帳法（昭和４２年法律第８１号）第３０条の４４第１項に規定する住民基本台帳カードをいう。以下同じ。）及び個人番号カードの管理について、次に掲げる事項を実施しなければならない。

（１）返納された住民基本台帳カード及び個人番号カードは、できるだけ速やかに廃棄すること。

（２）返納された住民基本台帳カード及び個人番号カードを廃棄するまでの間は、紛失及び盗難を防止するため、廃棄する住民基本台帳カード及び個人番号カードを施錠のできる書庫等に保管すること。

（３）廃棄する住民基本台帳カード及び個人番号カードは、焼却、溶解、裁断等により券面印刷の内容が判読できないようにするとともに、ＩＣチップ内の情報の読み出しやＩＣチップのハードウエア構造分析等の脅威を防ぐため、ＩＣチップを物理的に破壊すること。

（秘密保持）

第２１条　セキュリティ統括責任者、本人確認情報管理責任者、システム管理者、セキュリティ責任者、ＣＳ等の操作者、業務端末機の操作者及び住基ネットを利用する事務に従事する職員（正規職員以外の者を含む。次条において同じ。）は、本人確認情報のみならず、住基ネットのセキュリティに係る技術情報、パスワード、具体的な運用方法、マニュアルその他電子計算機処理に関する秘密を漏らしてはならない。

２　前項の規定は、住基ネットを利用する事務に従事しなくなった職員について準用する。

（安全確保）

第２２条　セキュリティ統括責任者、本人確認情報管理責任者、システム管理者、セキュリティ責任者、ＣＳ等の操作者、業務端末機の操作者及び住基ネットを利用する事務に従事する職員は、本人確認情報の漏洩、滅失、毀損及び保護に細心の注意を払わなければならない。

（業務端末機の操作）

第２３条　ＣＳ等及び業務端末機の操作者は、本人確認情報を検索し、抽出し、表示し、保存し、又は印刷（帳票への出力及びその他ハードコピー（業務端末機に表示された画面を紙に印刷したものをいう。以下同じ。）を含む。以下「本人確認情報の検索等」という。）し、操作を終了したときは、速やかに、当

該ＣＳ等及び業務端末機を初期画面に戻すよう努めるものとする。

2　ＣＳ等及び業務端末機の操作者は、業務上必要のない本人確認情報の検索、抽出の操作を行ってはならない。

3　ＣＳ等及び業務端末機の操作者は、長時間にわたり本人確認情報をディスプレイに表示したままの状態で放置してはならない。

4　ＣＳ等及び業務端末機の操作者は、離席する際は業務アプリケーションをログオフ又は終了させなければならない。

5　ＣＳ等及び業務端末機の操作者は、本人確認情報が表示された画面のコピーを必要以上に取ってはならない。

6　ＣＳ等及び業務端末機の操作者は、大量のデータ出力に際しては、事前に本人確認情報管理責任者の承認を得なければならない。

7　業務端末機の操作者は、業務端末機のディスプレイが窓口に来庁している住民から見えないように努めるものとする。

8　業務端末機の操作者は、窓口での本人確認情報の入力、出力に際して、住民票コード及び個人番号を口に出さないように努めるものとする。この場合に、口頭以外の方法により住民票コード及び個人番号を示す場合、その内容が他の住民に触れることのないように努めるものとする。

（帳票等の管理）

第２４条　ＣＳ等及び業務端末機の操作者は、業務上必要のない場合は、本人確認情報を印刷してはならない。

2　システム管理者及び業務端末機を設置する部署のセキュリティ責任者は、帳票管理簿を作成し、出力する帳票の名称、出力する周期及び使用目的を記録した帳票管理簿を作成し、これを３年間保存するものとする。

3　システム管理者及び業務端末機を設置する部署のセキュリティ責任者は、出力した帳票を施錠できる保管庫等に保管するものとし、申請に基づき出力した帳票は申請書を保管することで、届出に基づき出力した帳票は届出書を保管することで、管理するものとする。

4　システム管理者及び業務端末機を設置する部署のセキュリティ責任者は、本人確認情報を帳票によって出力した場合の処理は、次に掲げるところにより実施するものとする。

（１）帳票を出力した際は、出力装置上に放置せず、速やかに回収し、保管しない帳票については使用後速やかに廃棄すること。

（２）帳票を一定期間保管する場合は、システム管理者又はセキュリティ責任者が指定した施錠できる保管庫等に、一般廃棄ごみに混入しないよう区分して

保存した後、廃棄すること。この場合、帳票保管簿を作成し、これを３年間保存するものとする。

（３）廃棄は、裁断、焼却又は溶解により行うこと。

第６章　情報資産管理

（情報資産の管理等）

第２５条　住基ネットの情報資産の管理を行うため、情報資産管理責任者を置く。

２　業務端末機に関する情報資産管理責任者は、業務端末機を設置する部署のセキュリティ責任者をもって充て、本人確認情報及び当該本人確認情報が記録されたサーバに係る帳票に関する情報資産管理責任者は、本人確認情報を検索して利用し当該本人確認情報が記録されたサーバに係る帳票を利用する部署のセキュリティ責任者をもって充て、これら以外に関する情報資産管理責任者は、システム管理者をもって充てる。

３　システム管理者、本人確認情報管理責任者及びセキュリティ責任者は、それぞれが所管する情報資産の管理について、緊急やむを得ない場合には、それぞれの管理補助者に行わせることができる。

４　システム管理者は、住基ネットの情報資産の構成を明確化するほか、情報資産の障害、保守及び性能に関して管理を行わなければならない。

５　システム管理者は、情報資産管理簿を作成し、情報資産の導入、移設及び廃棄等の異動処理に伴う変更履歴を記録するとともに、当該記録を３年間保存するものとする。

（ハードウエアの管理）

第２６条　システム管理者は、住基ネットのハードウエアの障害に備え、当該住基ネットのハードウエアに障害が発生したときの対応手順を整備しなければならない。

２　システム管理者は、ＣＳ等の操作者及び業務端末機の操作者に対し、住基ネットのハードウエアの障害防止策及び住基ネットのハードウエアに障害が発生したときの対応手順を周知徹底しなければならない。

３　システム管理者は、住基ネットのハードウエアに障害が発生しないよう防止対策を講じるとともに、定期に又は随時に、当該防止対策が適正に実施されているか検査しなければならない。

４　システム管理者は、住基ネットのハードウエアの保守対象機器を明確にし、当該保守対象機器について、継続して使用でき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、住基ネットのハードウエアの保守時期及び保守内容について、当該住基ネットのハードウエアの機能及び使用頻度等を勘案し、決定するものとする。
6　システム管理者は、住基ネットのハードウエアの保守作業を実施するときは、本人確認情報の抹消及び漏洩等が発生しないように防止策を講じなければならない。
7　システム管理者は、住基ネットのハードウエアの保守作業を委託するときは、委託先にデータの保護に係る責務を課することを契約条項に入れるとともに、廃棄作業実施状況の報告を求め、指示どおり実施されたか確認するものとする。
8　システム管理者は、住基ネットのハードウエアの利用状況を定期的に分析し、その分析結果に基づき、当該住基ネットのハードウエアの適正な配置を図るものとする。
9　業務端末機を設置する部署のセキュリティ責任者は、住基ネットのハードウエアの障害に備え、緊急時連絡体制表を整備しておかなければならない。
１０　住基ネットのハードウエアに障害若しくは不正行為が発生したときは、緊急時対応計画書に基づいて対応するものとする。

（ソフトウエアの管理）
第２７条　システム管理者は、住基ネットのソフトウエアにバグを発見したとき、住基ネットのソフトウエアがコンピュータウイルスに感染し、若しくは感染している恐れが判明したとき又は不正アクセスにより当該住基ネットのソフトウエアが書き換えられ、若しくは書き換えられた恐れが判明したことにより、当該住基ネットのソフトウエアに障害が生じ、若しくは生じる恐れが判明したときは、直ちにセキュリティ統括責任者の承認を得て、当該ＣＳ等若しくは業務端末機をネットワークから切り離さなければならない。ただし、緊急やむを得ない場合は、当該承認を得ずに切り離すことができる。
2　システム管理者は、前項本文の規定によりネットワークから切り離したときは、セキュリティ統括責任者及び本人確認情報管理責任者に、前項ただし書の規定によりネットワークから切り離したときは、セキュリティ統括責任者及び本人確認情報管理責任者に直ちに報告しなければならない。
3　システム管理者は、住基ネットのソフトウエアに障害が発生したとき又は住基ネットのソフトウエアがコンピュータウイルスに感染したときその他不測の事態に備えて、定期に又は随時に、住基ネットのソフトウエアのバックアップを行わなければならない。
4　システム管理者は、業務内容及び処理形態に応じて、住基ネットのソフトウ

エアに係るバックアップの範囲及び記録する磁気ディスク並びにその保管方法を定めるものとする。

5　システム管理者は、バックアップした住基ネットのソフトウエアと運用中の住基ネットのソフトウエアとの整合性及び同期性に配慮しなければならない。

6　システム管理者は、住基ネットのソフトウエアのバックアップ及びリカバリ方法について、住基ネットのシステムを変更する都度見直しを行うものとする。

7　システム管理者は、住基ネットのソフトウエアのバージョン管理について、兵庫県又は機構の指示に従い実施するものとし、許可なくバージョンアップを行ってはならない。

8　システム管理者は、ＣＳ等及び業務端末機にインストールされているソフトウエアについて、定期に又は随時に確認を行い、その結果を記録しなければならない。

9　システム管理者は、住基ネットのシステムを変更したときは、住基ネットのセキュリティの設定を見直すものとする。

１０　システム管理者は、住基ネットで使用するソフトウエア（機構一括調達ソフト、業務アプリケーションその他機構が指示するソフトウエアを除く。）について、その性能管理を行うものとする。

１１　何人も、住基ネットの運用及び管理に必要なソフトウエア以外のソフトウエアをＣＳ等及び業務端末機に導入してはならない。

１２　第２項の規定による連絡を受けた本人確認情報管理責任者は、セキュリティ責任者にその旨を連絡するとともに、セキュリティ責任者から業務端末機の操作者にその旨を伝達するものとする。

１３　前項の規定による連絡を受けた業務端末機を設置する部署のセキュリティ責任者は、システム管理者又は本人確認情報管理責任者の指示があるまでは、業務端末機の全部又は一部の使用を停止しなければならない。

１４　業務端末機の操作者は、操作の過程において、当該業務端末機のソフトウエアにバグを発見したとき、当該業務端末機がコンピュータウイルスに感染したと認められるとき又は不正アクセスを発見したときは、直ちにセキュリティ責任者にその内容及び状況を報告しなければならない。

１５　前項の規定による報告を受けたセキュリティ責任者は、システム管理者にその内容及び状況を報告しなければならない。

１６　住基ネットのソフトウエアに障害若しくは不正行為が発生したときは、ＣＳ等及び業務端末機の全部又は一部の使用を停止させるとともに、緊急時対応計画書に基づいて対応するものとする。

（ネットワークの管理）

第２８条　システム管理者は、ネットワークの障害発生の検出、当該ネットワークに障害が発生したときの対処、当該ネットワークの障害を復旧するまでのフォローアップ、当該ネットワークの障害直後の対応（二次障害の防止、障害範囲拡大の防止及び障害の切分け）、当該ネットワークに障害が発生したときの運転対応（代替運転及び縮退運転）、状況に応じた復旧作業、当該ネットワークに障害が発生した原因の調査及び当該ネットワークの障害を改修した後の対応について、必要な措置を講じなければならない。

２　システム管理者は、ネットワークの障害予測及び定期診断並びにログの調査及び解析等を行うとともに、住基ネットの継続性及び安定性の確保に努めるものとする。

３　システム管理者は、住基ネットの円滑な運用を確保するため、住基ネットのハードウエア資源の利用状況、回線トラフィック状況等を勘案して、適宜資源の配分について見直しを行うものとする。

４　システム管理者は、ネットワークの保守等のために、ネットワークを停止するときは、事前に、セキュリティ統括責任者、本人確認情報管理責任者、兵庫県及び機構に報告するものとする。ただし、ネットワークの保守等を緊急に行う必要がある場合又は災害若しくは停電等によりネットワークの利用に影響がある場合等において、セキュリティ統括責任者、本人確認情報管理責任者、兵庫県及び機構に通知する時間がないと判断したときは、当該通知をせずにネットワークを停止することができる。

５　システム管理者は、前項ただし書の規定によりネットワークを停止したときは、セキュリティ統括責任者、本人確認情報管理責任者、兵庫県及び機構に直ちに報告しなければならない。

６　システム管理者は、ネットワークの性能情報並びに統計資料の収集及び蓄積に努め、当該蓄積した性能情報により解析を行い、その解析結果に基づき、パフォーマンス上のボトルネックを検出し、ボトルネックがあるときは、その改善措置を講じるものとする。

７　システム管理者は、ネットワークの拡張又は縮小を行う場合は、その計画立案を行い、住基ネットの運用への影響を最小限にとどめるよう実施するものとする。

８　システム管理者は、ネットワークの性能維持について必要があると認めるときは、その内容等をセキュリティ統括責任者、本人確認情報管理責任者、セキュリティ責任者、ＣＳ等の操作者及び業務端末機の操作者に周知するものとする。

９　住基ネットのネットワークに障害が発生したときは、緊急時対応計画書に基づいて対応するものとする。
１０　何人も、ＣＳ等並びに業務端末機を住基ネット以外のネットワークに接続してはならない。

（ドキュメントの管理）
第２９条　システム管理者及びセキュリティ責任者は、住基ネットに係る基本設計書、オペレーション手順書、コード定義書その他のドキュメントについて、施錠可能な場所に保管し、更新、複写、貸与及び廃棄等についてのドキュメント管理簿を作成し、記録するとともに、当該記録を３年間保存するものとする。
２　システム管理者及びセキュリティ責任者は、ドキュメントの廃棄時は裁断又は溶解を行わなければならない。
３　システム管理者は、委託事業者にドキュメントを貸与する場合は、貸出しについて適正に管理し、契約書等で取扱いに関する事項を決定するものとする。

（磁気ディスクの管理）
第３０条　システム管理者は、磁気ディスクを施錠可能な保管庫に収納し、適時、適切に管理されていることの確認及び記録を行わなければならない。
２　システム管理者は、磁気ディスク管理簿を作成し、使用、複写、受け渡し、消去及び廃棄の記録を行うとともに、当該記録を３年間保存するものとする。
３　システム管理者は、住基ネットに係る機器を廃棄しようとするときは、当該機器の磁気ディスクに記録されている情報を廃棄する過程において第三者に入手されることを防ぐため、磁気ディスクの物理的破壊、専用ソフトによる磁気ディスクに記録された情報の消去その他必要な措置を講じなければならない。
４　システム管理者は、住基ネットに係る機器の廃棄又は修理を委託するときは、委託先にデータの保護に係る責務を課することを契約条項に入れるとともに、廃棄又は修理が指示どおり実施されたか確認するものとする。

（耐タンパー装置の管理）
第３１条　システム管理者は、耐タンパー装置用セットアップディスク及び耐タンパー装置用パスワードを施錠のできる保管庫で管理しなければならない。
２　システム管理者は、耐タンパー装置を廃棄するときは、必ず当該耐タンパー装置内の情報が消去されているかを確認するとともに、確実に廃棄されたかどうかを確認するものとする。
３　前条第４項の規定は、システム管理者が耐タンパー装置の廃棄を委託すると

きについて準用する。

（オペレーション計画）

第３２条　システム管理者は、本人確認情報管理責任者と協議のうえ、次に掲げる事項を実施するものとする。

（１）要員計画の策定、実施及びその見直しに関すること。

（２）運用計画の策定、実施及びその見直しに関すること。

（３）バックアップ処理計画の策定、実施及びその見直しに関すること。

第７章　委託管理

（委託管理）

第３３条　システム管理者及び本人確認情報管理責任者は、住基ネットに係る業務について外部委託をしようとするときは、西宮市個人情報保護条例施行規則（平成１６年西宮市規則第９２号。以下「規則」という。）第４条第１項の規定に基づき、個人情報の保護について必要な措置を講じなければならない。

（委託契約書の内容）

第３４条　外部委託に係る契約書は、規則第４条第２項及び第３項に掲げる事項を明記しなければならない。

（受託者の管理状況の調査）

第３５条　システム管理者及び本人確認情報管理責任者は、必要に応じて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を行い、本人確認情報保護のため必要な措置を講じることができる。

第８章　危機管理

（緊急時対応計画）

第３６条　セキュリティ統括責任者は、住基ネットを構成するハードウエア、ソフトウエア及びネットワーク等の障害により住民サービスが停止するとき又は不正行為により本人確認情報に脅威を及ぼす恐れがあるときに備え、住基ネットセキュリティ会議の検討を経て、緊急時対応計画を定めなければならない。

２　セキュリティ統括責任者は、前項の計画により、被害を未然に防ぎ、又は被害の拡大を防止し、早急に復旧を図るために、セキュリティ統括責任者に適切な措置を講じるよう指示するものとする。

第９章　雑則

（委任）

第３７条　この要綱に定めるもののほか､ハードウエアの管理、ソフトウエアの管理、ネットワークの管理等情報資産の管理について必要な事項は、システム管理者が別に定める。

２　この要綱に定めるもののほか、住基ネットの運用について必要な事項は、本人確認情報管理責任者が別に定める。

３　前章に定めるもののほか、緊急時の対応について必要な事項は、システム管理者及び本人確認情報管理責任者が別に定める。

４　この要綱に定めるもののほか、住基ネットセキュリティ会議において検討すべき重要な事項について緊急に対応する必要のある場合は、セキュリティ統括責任者が措置を講じるものとする。

５　セキュリティ統括責任者は、前項の規定により措置を講じた場合は、次の住基ネットセキュリティ会議において、当該措置の内容について報告しなければならない。

付　則

この要綱は、平成１８年２月３日から実施する。

付　則

この要綱は、平成１８年４月１日から実施する。

付　則

この要綱は、平成１９年４月１日から実施する。

付　則

この要綱は、平成２０年４月１日から実施する。

付　則

この要綱は、平成２１年４月１日から実施する。

付　則

この要綱は、平成２２年４月１日から実施する。

付　則

この要綱は、平成２２年７月５日から実施する。

付　則

この要綱は、平成２４年４月１日から実施する。

付　則

この要綱は、平成２４年７月９日から実施する。

付　則

この要綱は、平成２６年４月１日から実施する。

付　則

この要綱は、平成２６年６月１日から実施する。

付　則

この要綱は、平成２７年４月１日から実施する。

付　則

この要綱は、平成２７年１０月５日から実施する。

付　則

この要綱は、平成２８年１月１日から実施する。

付　則

この要綱は、平成２８年４月１日から実施する。

付　則

この要綱は、平成２９年４月１日から実施する。

付　則

この要綱は、平成２９年７月１８日から実施する。

付　則

この要綱は、平成３０年３月１日から実施する。

付　則

この要綱は、令和２年４月１日から実施する。

付　則

この要綱は、令和３年４月１日から実施する。