○総務省告示第三百三十四号

電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準

第１　用語の定義

１　住民基本台帳ネットワークシステム

コミュニケーションサーバ、都道府県サーバ、指定情報処理機関サーバ、認証業務連携サーバ、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（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５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、委任都道府県知事（法第３０条の１０第３項に規定する委任都道府県知事をいう。以下同じ。）が本　人確認情報を指定情報処理機関（法第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。）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、住民基本台帳カード（法第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。）を発行し、並びに都道府県知事及び指定情報処理機関が本人確認情報の記録、保存及び提供を行い、法第３０条の８第３項若しくは法第３０条の１１第９項の通知があった旨の情報（以下「異動等情報」という。）の提供を行うためのシステム

２　コミュニケーションサーバ

転入通知（法第９条第１項の規定による通知をいう。以下同じ。）、住民票の写しの交付の特例（法第１２条の２の規定による住民票の写しの交付をいう。以下同じ。）及び転入転出の特例（法第２４条の２の規定による住民基本台帳カードの交付を受けている者等に関する届出の特例をいう。以下同じ。）のために必要な情報を市町村長間で通知し、並びに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。以下「令」という。）第１３条第３項の規定による通知をいう。以下同じ。）を行い、住民基本台帳カードを発行するための市町村長の使用に係る電子計算機

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、並びに委任都道府県知事にあっては、指定情報処理機関に本人確認情報の通知を行うための都道府県知事の使用に係る電子計算機

４　指定情報処理機関サーバ

委任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、保存及び提供を行うための指定情報処理機関の使用に係る電子計算機

５　認証業務連携サーバ

都道府県知事が電子証明書（電子署名に係る地方公共団体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３条第１項に規定する電子証明書をいう。以下同じ。）の発行を受けている者に係る異動等情報を利用し、又は都道府県知事若しくは指定情報処理機関が指定認証機関（同法第３４条第１項に規定する指定認証機関をいう。以下同じ。）に対し、電子証明書の発行を受けている者に係る異動等情報の提供を行うための都道府県知事若しくは指定情報処理機関の使用に係る電子計算機

６　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

７　データ

住民基本台帳ネットワークシステムにおいて通知され、記録され、保存され、又は提供される情報

8　プログラム
　電子計算機を機能させて住民基本台帳ネットワークシステムを作動させるための命令を組み合せたもの
9　ファイル
　磁気ディスク（これに準ずる方法により一定の事項を確実に記録しておくことができる物を含む。以下同じ。）に記録されているデータ及びプログラム
10　ドキュメント
　住民基本台帳ネットワークシステムの設計、プログラム作成及び運用に関する記録及び文書
11　電子計算機室
　電子計算機及び電気通信関係装置を設置する室
12　磁気ディスク等保管室
　磁気ディスク及びドキュメントを保管する室
13　重要機能室
　電子計算機室、磁気ディスク等保管室、受電設備、定電圧・定周波電源装置等の設備を設置する室並びに電子計算機室及び磁気ディスク等保管室の空気調和をする空気調和機及びその付属設備を設置する室

第2　体制、規程等の整備
1　体制の整備
(1)　責任体制等の確立
　住民基本台帳ネットワークシステムのセキュリティ（正確性、機密性及び継続性の維持をいう。以下同じ。）を確保するため、住民基本台帳ネットワークシステムの企画、開発及び運用に関する責任体制及び連絡体制を明確にすること。また、防災組織及び防犯組織を整備し、通常時及び非常時の責任体制の確立を図ること。
(2)　連絡調整を行う場の設置
　都道府県知事、市町村長及び指定情報処理機関は、住民基本台帳ネットワークシステムのセキュリティ対策に関し、連絡調整を行う場を設けること。
(3)　監視体制の整備
　都道府県知事、市町村長及び指定情報処理機関は、住民基本台帳ネットワークシステムの運用に関し、異常な状態を早期に発見し、相互に連絡することができるよう体制の整備を図ること。
2　規程等の整備
(1)　規程の整備
　住民基本台帳ネットワークシステムの企画、開発及び運用に関する規程を整備すること。
(2)　住民基本台帳ネットワークシステム設計書等の整備
　住民基本台帳ネットワークシステム設計書、操作手順書、緊急時における作業手順書等を整備すること。
3　人事、教育、研修等
(1)　要員管理
　住民基本台帳ネットワークシステムの運用に必要な職員の配置、交替等の人事管理を適切に行うこと。また、プログラムの作成及び住民基本台帳ネットワークシステムの操作の各事務は、同一の者が行うことのないように配慮すること。
(2)　教育及び研修
ア　住民基本台帳ネットワークシステムを運用する職員に対して、住民基本台帳ネットワークシステムの操作及びセキュリティ対策についての教育及び研修を実施するために、教育及び研修に関する計画を策定し、そ

88

の実施体制を確立すること。

イ　指定情報処理機関は、都道府県知事及び市町村長に対し、教育及び研修に関する技術的な協力を行うこと。

(3) 問い合わせ窓口の設置

職員を支援し、誤操作等の発生を防止するため、操作等に関する問い合わせ窓口を設置すること。

4　住民基本台帳ネットワークシステムの監査

監査の体制を確立し、住民基本台帳ネットワークシステムの企画、開発及び運用の各段階におけるセキュリティ対策の評価を行い、その結果に基づき住民基本台帳ネットワークシステムの改善に努めること。

5　緊急時体制

(1) 作動停止時における事務処理体制

ア　住民基本台帳ネットワークシステムの構成機器、関連設備又はソフトウェアの障害等により住民基本台帳ネットワークシステムの全部又は一部が作動停止した場合の行動計画、住民への周知方法、都道府県知事、市町村長及び指定情報処理機関との連絡方法等について、都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を図り定めること。

イ　実際に問題が発生した場合に適切な対応を図ることができるよう、都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を図り、教育及び研修を行うこと。

(2) データの漏えいのおそれがある場合の事務処理体制

ア　データの漏えいのおそれがある場合の行動計画（住民基本台帳ネットワークシステムの全部又は一部を停止する基準の策定を含む。）、住民への周知方法、都道府県知事、市町村長及び指定情報処理機関との連絡方法等について、都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を図り定めること。

イ　実際に問題が発生した場合に適切な対応を図ることができるよう、都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を図り、教育及び研修を行うこと。

第３　住民基本台帳ネットワークシステムの環境及び設備

1　建物及び重要機能室

(1) 建物等への侵入の防止等

ア　住民基本台帳ネットワークシステムに係る建物及び重要機能室（以下「建物等」という。）の壁、窓、ドア等が容易に破壊されないよう必要な措置を講ずること。

イ　建物等への侵入を検知するための措置を講ずること。

ウ　電力及び電気通信回線の切断等を防止するための措置を講ずること。

エ　重要機能室の外に設置された関連設備に対する不当な接触の防止について、必要な措置を講ずること。

(2) 重要機能室の配置及び構造

ア　重要機能室の配置及び構造については、セキュリティ対策及び保守が容易に行えるよう配慮すること。

イ　重要機能室については、その表示を行わない等、できるだけ所在を明らかにしないようにすること。

ウ　重要機能室に、緊急事態発生の際の連絡設備を設ける等、連絡体制を整備すること。

エ　電子計算機室及び磁気ディスク等保管室は、他の部屋と区別して専用の部屋とすること。専用の部屋を確保できない場合は、電子計算機及び電気通信関係装置を厳重に固定し、磁気ディスク及びドキュメントを専用保管庫により施錠保管すること。

89

オ　電子計算機室及び磁気ディスク等保管室の常時利用する出入口を限定すること等により、侵入の防止を容易に行えるよう配慮すること。

2　障害の防止等

(1) 電気的及び機械的障害の防止等

住民基本台帳ネットワークシステムの構成機器又は関連設備の電気的及び機械的障害の発生を防止し、検知するため、及びこれらの障害が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。

(2) 水又は蒸気による障害の防止等

住民基本台帳ネットワークシステムの構成機器又は関連設備の水又は蒸気による障害の発生を防止するため、これらの障害の発生を検知するため、及び障害が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。

(3) 火災の防止等

建物等からの出火の防止のため、必要な措置を講ずること。また、建物等の火災による住民基本台帳ネットワークシステムの構成機器又は関連設備の損傷を防止するため、火災の発生を検知するため、及び火災が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。

(4) 地震対策

地震による建物等又は住民基本台帳ネットワークシステムの構成機器若しくは関連設備の損傷を防止するため、及び地震が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。

(5) 急激な温湿度変化等に対する措置

空気調和設備は、その容量に配慮し、急激な温湿度変化等に対する措置を講ずること。

(6) 転倒、移動等に対する措置

住民基本台帳ネットワークシステムの構成機器及び関連設備には、転倒、移動等に対する措置を講ずること。

(7) その他の障害の防止等

動物その他による障害を防止するため、これらの障害の発生を検知するため、及び障害が発生した場合の対策を図るため、必要な措置を講ずること。

3　ネットワークの設備及び構造

(1) 専用回線の使用

電気通信回線からのデータの盗取を防止するため、コミュニケーションサーバ、都道府県サーバ及び指定情報処理機関サーバを結ぶ電気通信回線は、専用回線（接続先が固定されており、所定の伝送速度が保証されている回線をいう。以下同じ。）を使用すること。また、国の機関等（法別表第一の上欄に掲げる国の機関又は法人をいう。以下同じ。）に本人確認情報を提供するために都道府県サーバ又は指定情報処理機関サーバと国の機関等の使用に係る電子計算機を結ぶこととした場合又は指定認証機関に異動等情報を提供するために認証業務連携サーバと指定認証機関の使用に係る電子計算機を結ぶこととした場合における電気通信回線は、専用回線を使用すること。

(2) 予備の回線の設置

通信が途絶しないようにするため、コミュニケーションサーバ、都道府県サーバ及び指定情報処理機関サーバを結ぶ電気通信回線には、予備の回線を設けること。

(3) ネットワークの構造

ネットワークは、転入通知、第６の４の(1)及び(2)の通知並びに第６の５の(3)及び(4)の通知が都道府県サーバ及び指定情報処理機関サーバを通

過しない構造とすること。

第４　住民基本台帳ネットワークシステムの管理

１　入退室管理

(1) 入室資格の付与

重要機能室への入室者を限定すること。また、重要機能室に入退室する者に鍵を貸与する際に、その者が入室する権限を有することを確認すること、入退室管理カードによって重要機能室に入退室する者が入室する権限を有することを確認すること等により、入退室の管理を適切に行うこと。

(2) 鍵又は入退室管理カードの管理

ア　重要機能室の出入口の鍵は所定の場所に保管し、その管理は定められた者が行うこと。

イ　入退室管理カードの管理方法を定めること。

(3) 搬出入物品の確認

重要機能室への搬出入物品は、重要機能室に入室する権限を有する職員が内容を確認すること。

(4) 事務室の管理

事務室における住民基本台帳ネットワークシステムの構成機器、関連設備等の盗難、損壊等を防止するため、職員が不在となる時の事務室の施錠等、必要な措置を講ずること。

２　ソフトウェア開発等の管理

(1) セキュリティを高める設計の実施

住民基本台帳ネットワークシステムの開発又は変更を行う際には、住民基本台帳ネットワークシステムのセキュリティを高める設計を行うこと。

(2) 住民基本台帳ネットワークシステムの試験の実施

ア　住民基本台帳ネットワークシステムの開発又は変更を行った場合には、試験を適切に実施すること。

イ　ファイルの安全を確保するため、別途、試験環境を用意し、試験を行うこと。

(3) 住民基本台帳ネットワークシステムの開発等に際してのエラー及び不正行為の防止

ア　住民基本台帳ネットワークシステムの開発又は変更を行う際には、住民基本台帳ネットワークシステムの開発又は変更の計画を策定すること、住民基本台帳ネットワークシステムの開発又は変更の責任者を指定すること、プログラムの作成、変更又は廃止は責任者の承認を得て行うこと等エラー及び不正行為の防止のための手続を明確にすること。

イ　住民基本台帳ネットワークシステムの開発又は変更の各段階で使用するドキュメントの様式を標準化すること。

ウ　住民基本台帳ネットワークシステムの変更に応じてドキュメントを更新し、責任者が確認すること。

３　住民基本台帳ネットワークシステムの管理

(1) アクセス権限の限定

住民基本台帳ネットワークシステムを運用する職員に対して、電子計算機、端末機、電気通信関係装置、電気通信回線、ファイル等に関し、必要なアクセス権限を付与すること。

(2) ファイアウォールによる通信制御

電気通信回線に接続する電子計算機における不正行為又は電子計算機への不正アクセス行為に対して住民基本台帳ネットワークシステムを保護するため、コミュニケーションサーバ、都道府県サーバ及び指定情報処理機関サーバ間等、必要な部分には、指定情報処理機関が管理するファイアウォールを設置し、通信制御を行うこと。

(3) 電気通信関係装置の管理

エラー及び不正行為により電気通信関係装置の不当な運用が行われないようにするため、電気通信関係装置の管理に際しては厳重な確認を行う等、管理権限がある者以外の者による操作を防止するための措置を講ずること。また、通信に際しては、電気通信関係装置相互の認証を行うこと。

(4) 通信相手相互の認証

コミュニケーションサーバ、都道府県サーバ又は指定情報処理機関サーバそれぞれの間の通信については、通信相手相互の認証を行うこと。また、都道府県サーバ又は指定情報処理機関サーバから国の機関等に本人確認情報を提供し、又は認証業務連携サーバから指定認証機関に異動等情報を提供するための通信についても、通信相手相互の認証を行うこと。

(5) データの暗号化

コミュニケーションサーバ、都道府県サーバ又は指定情報処理機関サーバそれぞれの間の通信については、交換するデータの暗号化を実施すること。また、都道府県サーバ又は指定情報処理機関サーバから国の機関等に本人確認情報を提供し、又は認証業務連携サーバから指定認証機関に異動等情報を提供するためのデータの交換についても、データの暗号化を実施すること。

(6) 模擬攻撃の実施

ネットワーク経由の模擬攻撃を適宜実施し、その実施結果に基づき必要な措置を講ずること。

(7) 情報収集等

セキュリティ対策に関する情報を収集し、分析を行い、必要な措置を講ずること。

4 端末機操作の管理

(1) 端末機の管理

端末機（都道府県サーバ又は指定情報処理機関サーバと国の機関等の使用に係る電子計算機を電気通信回線で結ぶこととした場合における当該電子計算機の端末機を含む。以下４において同じ。）の取扱いは、当該端末機の管理を行う責任者の指示又は承認を受けた者が行うこと。

(2) 端末機の操作者の確認

端末機の取扱いに際しては、操作者が正当なアクセス権限を有していることを操作者識別カード及び暗証番号又はこれと同等以上のものと認められる方法により確認すること。

(3) 操作者識別カードの発行及び管理

都道府県、市町村及び指定情報処理機関が相互に密接に連携し、操作者識別カードの発行及び管理を行うこと。

(4) 暗証番号の取扱い

暗証番号の管理方法を定め、操作者は当該管理方法を遵守すること。

(5) ファイルに対する利用制限

端末機の操作者ごとに利用可能なファイルを設定する等、ファイルの利用を制限する方法を定めること。

(6) 操作履歴の記録等

住民基本台帳ネットワークシステムを操作した履歴を磁気ディスクに記録し、法令を遵守していることを監査する等、その利用の正当性について確認すること。

(7) 照会の条件の限定

正当な利用目的以外の目的にデータベースが構成されることを防止するため、本人確認情報の提供を求める際の照会の条件を限定すること。

(8) 強制的に終了する機能

端末機には、複数回のアクセスの失敗に対して、強制的に終了する機能を設けること。

5 電子計算機の管理

(1) 秘密鍵の厳重な管理

コミュニケーションサーバ、都道府県サーバ、指定情報処理機関サーバ及び認証業務連携サーバにおいて、通信相手相互の認証及び送受信するデータの暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。また、指定情報処理機関サーバと国の機関等の使用に係る電子計算機との間で電気通信回線又は磁気ディスクによりデータを交換する場合における国の機関等の使用に係る電子計算機又は指定認証機関の使用に係る電子計算機においても、通信相手相互の認証又はデータの暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。

(2) 他のソフトウェアの作動禁止

コミュニケーションサーバ、都道府県サーバ、指定情報処理機関サーバ及び認証業務連携サーバでは、住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこと。また、指定情報処理機関サーバと国の機関等の使用に係る電子計算機との間で電気通信回線又は磁気ディスクによりデータを交換する場合における国の機関等の使用に係る電子計算機又は指定認証機関の使用に係る電子計算機においても、住民基本台帳ネットワークシステムの管理及び運用に必要なソフトウェア（認証業務（公的個人認証法第２条第２項に規定する認証業務をいう。以下同じ。）に必要なソフトウェアを含む。）以外のソフトウェアを作動させないこと。

6 磁気ディスクの管理

(1) 保管場所

磁気ディスクは、保管庫等を設けることにより、できるだけ常温常湿の場所に保管すること。

(2) 持ち出し及び返却の確認等

ア 磁気ディスクの盗難の防止等のため、その保管位置を指定し、持ち出し及び返却の措置を講ずること。特に、市町村（特別区を含む。以下同じ。）の住民記録システム（電子計算機、端末機、電気通信関係装置、電気通信回線、プログラム等の全部又は一部により構成され、住民基本台帳に関する記録を管理し、及び住民基本台帳に関する事務を処理するためのシステムをいう。以下同じ。）とコミュニケーションサーバとの間において、磁気ディスクによりデータを送付する場合は、データの送付を実施するごとに、保管状況を確認すること。

イ 重要な磁気ディスクは他の磁気ディスクと判別することができるようにすること。

7 構成機器及び関連設備等の管理

(1) 管理方法の明確化

ア 住民基本台帳ネットワークシステムに機器を接続するための手続、方法等を定めるとともに、構成機器、関連設備等の管理方法を明確にすること。

イ 利用するハードウェア、ソフトウェア及び磁気ディスクの種類、数量等を文書等で体系的かつ一元的に記録管理し、現況と一致させること。また、これを関係職員に周知し、管理しているハードウェア、ソフトウェア又は磁気ディスク以外のものを使用しないこと。

(2) 保守の実施

住民基本台帳ネットワークシステムの構成機器及び関連設備の保守を定期に又は随時に、実施すること。また、保守の実施に当たっては、エラー及び不正行為を防止し、データを保護するため、必要な措置を講ずること。

(3) 稼働状況の監視

指定情報処理機関において、構成機器の稼働状況を監視し、必要に応じ、都道府県知事及び市町村長に状況を通知すること。

(4) 不正プログラムの混入防止等

住民基本台帳ネットワークシステムにコンピュータウイルス等の不正プログラムが混入されていないかどうかを監視する措置を講じ、混入されていた場合には駆除する措置を講ずること。また、コンピュータウイルス等の不正プログラムが発見された場合の必要な措置を定め、住民基本台帳ネットワークシステムを運用する職員に周知すること。

8 データ、プログラム、ドキュメント等の管理

(1) データ等の取扱い及び管理

ア データ、プログラム及びドキュメントについては、定められた場所に保管すること、受渡し及び保管に関し必要な事項を記録すること、使用、複写、消去及び廃棄は責任者の承認を得て行うとともにその記録を作成すること等、その取扱い及び管理の方法を明確にすること。

イ プログラムの改ざん、消去等を防止するために、プログラムの登録及び抹消は、責任者の指示又は承認を受けた者が行うこと。

ウ データ、プログラム及びドキュメントを廃棄する場合には、消磁、破砕、溶解等の措置を講ずること。

(2) データの処理

ア データの処理に際しては、データを処理する者の牽制体制について必要な措置を講ずること。

イ データの処理に関する計画を作成すること、臨時のデータの処理については責任者の承認を得て行うこと、データの処理の記録を作成し、必要に応じ計画と突き合わせること等、計画的なデータの処理を実施すること。

ウ 重要なデータの入力に際しては、必要に応じて責任者の承認を得て行うこと。また、責任者の事前承認が困難なオンライン入力データについては、その重要性に応じて、入力後に承認する手続を定めること。

エ データ入力作業のエラーを発見し、確認する機能を設けること。また、エラーデータの修正のための入力手続を定め、適切な処理を行うこと。

オ データ入力用の原票及び媒体の取扱方法を定めること。

カ 大量のデータの出力に際しては、事前に責任者の承認を得ること。

(3) 帳票の管理

ア 未使用の重要な帳票の在庫管理及び廃棄の方法を定めること。また、重要な印字済みの帳票の受渡し及び廃棄の方法を定めること。

イ 事務室の出力装置から出力する場合のデータの漏えいを防止するため、必要な措置を講ずること。

9 障害時等の対応

(1) 障害の早期発見

住民基本台帳ネットワークシステムの障害箇所を発見するための機能を整備すること。

(2) 早期回復のための代替機能等の整備

ア 重要なファイルについては、他の磁気ディスクに複製することとし、必要に応じ、複製された磁気ディスクを当該ファイルを記録した磁気ディスクとは別に保管すること。また、住民基本台帳ネットワークシステムの重要な構成機器及び関連設備について、障害が発生した時に代替することができる機能を整備する等、必要な措置を講ずること。

イ 障害が発生した時に、データ処理等に関する情報を基に速やかに住民基本台帳ネットワークシステムを回復させるための機能を整備すること。

ウ あらかじめ定められた作業手順に従って代替機能等が確実に機能することを、試験により確認すること。

(3) 不正アクセスの早期発見

不正アクセスを早期に発見するための機能を整備すること。

(4) 不正アクセスが判明した場合の対応

都道府県知事、市町村長及び指定情報処理機関は、不正アクセスが判明した場合、相互に連絡調整を行い、被害状況の把握、被害拡大を防止するための措置等必要な措置を講ずること。

10　委託を行う場合等の措置

(1) 委託先事業者等の社会的信用の確認等

住民基本台帳ネットワークシステムの開発、変更、運用、保守等について、委託を行う場合は、委託先事業者等の社会的信用と能力を確認すること。

(2) 委託先事業者等に対する監督

委託先事業者等に対し、この基準と同様のセキュリティ対策を実施させるとともに、適切な監督を行うこと。また、委託先事業者等によるエラー及び不正行為を防止し、データを保護するため、必要な措置を講ずること。

(3) 再委託の制限等

委託業務の一部を第三者に委託する場合の制限、事前申請及び承認に関する事項を委託先事業者等と取り交わすこと。

(4) 委託先事業者等の分担範囲等の明確化

住民基本台帳ネットワークシステムの開発、変更、運用、保守等に複数の委託先事業者等が関わる場合は、分担して行う範囲及び責任の範囲を明確にするとともに、作業上必要な情報交換を行えるような措置を講ずること。

(5) 要員派遣を受ける場合等の措置

要員派遣を受ける場合又は非常勤職員、臨時職員等を雇用する場合には、必要に応じ、秘密保持に関する誓約書を提出させる等の措置を講ずること。

第５　既設ネットワークとの接続

1　既設ネットワークとの接続条件

住民記録システムとの接続、端末機の設置等のため、住民基本台帳ネットワークシステムと既設ネットワークとを接続する場合（都道府県サーバ又は指定情報処理機関サーバと国の機関等の使用に係る電子計算機を電気通信回線で結ぶこととした場合における国の機関等の使用に係る電子計算機と既設ネットワークを接続する場合及び指定認証機関の使用に係る電子計算機と既設ネットワークを接続する場合を含む。）は、既設ネットワークにおいて、次のようなセキュリティ対策を講ずること。

(1) 体制の整備等

ア　既設ネットワークのセキュリティを確保するため、既設ネットワークの開発及び運用に関する責任体制及び連絡調整体制を明確にすること。

イ　既設ネットワークにおいて、個人情報の漏えいのおそれがある場合の事務処理体制を確立すること。

(2) 電気通信回線上の盗取の防止

電気通信回線は専用回線を用い、又はそれに準じた通信データの盗取の防止についての必要な対策を講ずること。

(3) ファイアウォールによる通信制御

既設ネットワークと住民基本台帳ネットワークシステム（都道府県サーバ若しくは指定情報処理機関サーバと国の機関等の使用に係る電子計算機を電気通信回線で結ぶこととした場合における国の機関等の使用に係る電子計算機又は指定認証機関の使用に係る電子計算機。以下(4)アにおいて同じ。）との間にファイアウォールを設置し、住民基本台帳ネットワークシステム上の処理（認証業務に必要な処理を含む。）又は住民記録システム上の処理に係る通信のみが可能となるよう通信制御を行うこと。

(4) 電気通信関係装置の保護等

ア　既設ネットワークと住民基本台帳ネットワークシステムの電気通信関

係装置、電気通信回線等を共有しないこと。

イ　既設ネットワークに係る電気通信関係装置等は、既設ネットワークの管理責任者以外の者による操作を防止するための措置を講ずること。

(5) 機器の接続

既設ネットワークの管理責任者は、ネットワークに機器を接続するための手続、方法等を定め、接続状況を適切に管理すること。

(6) 外部との接続

ア　既設ネットワークの管理責任者は、既設ネットワークを外部ネットワークに接続するための手続、方法等を定め、接続及び運用に関する業務を総括的に管理すること。

イ　既設ネットワークと外部のネットワークを接続する場合は、既設ネットワークと外部のネットワークとの間にファイアウォールを設置し、厳重な通信制御を行うこと。

2 既設ネットワークとの接続状況についての連絡調整

(1) 都道府県知事、市町村長及び指定情報処理機関の連絡調整

都道府県知事、市町村長及び指定情報処理機関は、既設ネットワークとの接続状況について相互に連絡調整を行うこと。また、都道府県知事、市町村長及び指定情報処理機関は、それぞれの既設ネットワークにおいて個人情報の漏えいのおそれがある場合は、相互に連絡調整を行うこと。

(2) 都道府県知事等と国の機関等の連絡調整

都道府県知事（委任都道府県知事にあっては、指定情報処理機関。以下(2)及び(3)において同じ。）及び都道府県サーバ又は指定情報処理機関サーバと国の機関等の使用に係る電子計算機を電気通信回線で結ぶこととした場合における国の機関等は、既設ネットワークとの接続状況について相互に連絡調整を行うこと。また、都道府県知事及び国の機関等は、それぞれの既設ネットワークにおいて個人情報の漏えいのおそれがある場合は、相互に連絡調整を行うこと。

(3) 都道府県知事等と指定認証機関の連絡調整

都道府県知事及び指定認証機関は、既設ネットワークとの接続状況について相互に連絡調整を行うこと。また、都道府県知事及び指定認証機関は、それぞれの既設ネットワークにおいて個人情報の漏えいのおそれがある場合は、相互に連絡調整を行うこと。

3　認証業務に係る受付窓口端末の設置

(1) 住民基本台帳ネットワークシステムと認証業務に係る受付窓口端末（認証業務及びこれに附帯する業務の実施に関する技術的基準（平成１５年総務省告示第７０６号）第１条第１号に規定する受付窓口端末をいう。以下同じ。）を接続する場合には、当該受付窓口端末は、第５の１(3)に基づき設置するファイアウォールを介して住民基本台帳ネットワークシステムと接続する既設ネットワーク上に設置すること。

(2) 市町村長は、認証業務及びこれに附帯する業務の実施に関する技術的基準第３条に規定する方法で端末機から受付窓口端末に対しデータの送付を行うに際し、電気通信回線を通じてデータの送付を行う場合は、当該端末機は、(1)の既設ネットワークに設置すること。

第６　住民基本台帳ネットワークシステムの運用

1　運用計画

(1) 処理の種類等の決定

都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を図り、住民基本台帳ネットワークシステムにおける即時処理、日々処理等処理の種類及びその内容について定めること。

(2) 運用計画

都道府県知事、市町村長及び指定情報処理機関は、相互に密接な連携を

図り、住民基本台帳ネットワークシステムの運用時間、業務開始手続等についての計画を定めること。

2　転入通知

市町村長は、他の市町村から当該市町村の区域内に住所を変更した者につき住民票の記載をしたときは、遅滞なく、コミュニケーションサーバを介してその旨を当該他の市町村の市町村長に通知すること。

3　転出確定通知

(1) 転入通知を受けた市町村長は、速やかに、コミュニケーションサーバを介して転出確定通知を都道府県知事に通知すること。

(2) 転出確定通知を受けた都道府県知事は、その旨を都道府県サーバに保存されている本人確認情報に付記すること。

4　住民票の写しの交付の特例

(1) 住民票の写しの交付の特例に係る請求があった旨の通知

請求書により、住民票の写しの交付の特例に係る請求があった場合には、請求を受けた市町村長（(2)及び(3)において「交付地市町村長」という。）は、住民基本台帳カード又は住民基本台帳法施行規則（平成１１年自治省令第３５号）第５条第２項に規定する書類により本人確認を行い、令第１５条の２第１項に規定する事項をコミュニケーションサーバに入力し、これを請求をした者が記録されている住民基本台帳を備える市町村の市町村長（(2)において「住所地市町村長」という。）に通知すること。

(2) 住民票の写しの情報の通知

(1)の通知を受けた住所地市町村長は、請求内容を必要に応じて審査し、令第１５条の２第２項に規定する事項を住民記録システムから電気通信回線又は磁気ディスクを介して（住民記録システムを有しない市町村にあっては、手入力により）コミュニケーションサーバに入力し、これを交付地市町村長に通知すること。

(3) 住民票の写しの交付

(2)の通知を受けた交付地市町村長は、コミュニケーションサーバの端末機画面等により請求書内容の審査を行い、プリンタから打ち出した書類を認証して交付すること。

(4) 請求書の保存

審査した請求書の保存に当たっては、その保存方法について定めること。

5　転入転出の特例

(1) 付記転出届又は世帯員に関する付記転出届の受理及び審査

付記転出届（法第２４条の２第１項に規定する付記転出届をいう。(1)及び(3)において同じ。）の受理に際しては、コミュニケーションサーバの端末機から検索する等により住民基本台帳カードの保有の確認を行うこと。また、付記転出届又は世帯員に関する付記転出届（法第２４条の２第２項に規定する世帯員に関する付記転出届をいう。）の内容の審査は、必要に応じ、住民記録システムの端末機画面又は住民票に記録されている事項を記載した書類と照合して行うこと。

(2) 転出証明書情報の登録

住民票の異動処理に基づき、令第２４条の４に規定する事項（(4)及び(5)において「転出証明書情報」という。）を住民記録システムから電気通信回線又は磁気ディスクを介して（住民記録システムを有しない市町村にあっては、手入力により）コミュニケーションサーバに入力すること。

(3) 最初の転入届を受けた旨の通知

最初の転入届（法第２４条の２第１項に規定する最初の転入届をいう。(5)において同じ。）を受けた市町村長（(4)において「転入地市町村長」という。）は、その旨をコミュニケーションサーバを介して付記転出届を受けた市町村長（(4)及び(5)において「転出地市町村長」という。）に通知すること。

97

(4) 転出証明書情報の通知
(3)の通知を受けた転出地市町村長は、(2)の転出証明書情報を転入地市町村長に通知すること。
(5) 最初の転入届又は最初の世帯員に関する転入届の受理及び審査
最初の転入届の受理に際しては、住民基本台帳カードを回収すること。また、最初の転入届又は最初の世帯員に関する転入届（法第２４条の２第２項に規定する最初の世帯員に関する転入届をいう。）の内容の審査は、転出地市町村長から通知された転出証明書情報に係る端末機画面又はプリンタ等から打ち出された書類を転入届と照合して行うこと。
(6) 届出書の保存
届出書の保存に当たっては、その保存方法について定めること。

6　本人確認情報の通知及び記録
(1) 市町村長から都道府県知事への通知
市町村長が住民票の記載、消除又は法第７条第１号から第３号まで、第７号及び第１３号に掲げる事項（同条第７号に掲げる事項については、住所とする。）の全部若しくは一部についての記載の修正を行った場合は、翌運用日の業務開始までに、住民記録システムから電気通信回線又は磁気ディスクを介して（住民記録システムを有しない市町村にあっては、本人確認情報の手入力により）、本人確認情報をコミュニケーションサーバに記録し、都道府県知事に電気通信回線を通じて送信すること。
(2) 都道府県知事における本人確認情報の記録
都道府県知事は、市町村長から本人確認情報の通知を受けた場合は、都道府県サーバに本人確認情報を記録すること。この場合において、通知された本人確認情報に基づいて磁気ディスクに当該本人確認情報が確実に記録されたことを更新件数リスト等により確認すること。
(3) 委任都道府県知事から指定情報処理機関への通知
市町村長から本人確認情報の通知を受け、都道府県サーバに本人確認情報を記録した委任都道府県知事は、速やかに、当該本人確認情報を指定情報処理機関に電気通信回線を通じて送信すること。
(4) 指定情報処理機関における本人確認情報の記録
指定情報処理機関は、委任都道府県知事から本人確認情報の通知を受けた場合、指定情報処理機関サーバに本人確認情報を記録すること。この場合において、通知された本人確認情報に基づいて磁気ディスクに当該本人確認情報が確実に記録されたことを更新件数リスト等により確認すること。

7　本人確認情報の消去
(1) 市町村長における本人確認情報の消去
市町村長は、コミュニケーションサーバにおける本人確認情報について、当該本人確認情報に係る者に係る新たな本人確認情報が記録された日から起算して５年を経過する日までの期間（住民票の消除が行われたことにより記録された本人確認情報にあっては、当該本人確認情報が記録された日から起算して５年を経過する日までの期間）経過後遅滞なく、当該本人確認情報を確実に消去すること。
(2) 都道府県知事又は指定情報処理機関における本人確認情報の消去
都道府県知事又は指定情報処理機関は、都道府県サーバ又は指定情報処理機関サーバにおける本人確認情報について、令第３０条の６又は令第３０条の１１に規定する期間経過後遅滞なく、当該本人確認情報を確実に消去すること。

8　本人確認情報等の提供等
(1) 国の機関等に対する本人確認情報の提供
ア　都道府県知事（委任都道府県知事にあっては、指定情報処理機関）は、国の機関等に対し、本人確認情報の提供を行う場合は、あらかじめ、本人確認情報の提供の具体的方法、本人確認情報の漏えい、滅失及びき

損の防止その他の本人確認情報の適切な管理のための措置等について、国の機関等と協議して定めること。

イ　国の機関等は、本人確認情報の提供を受けるに際しては、職員に対し住民基本台帳ネットワークシステムの操作及びセキュリティ対策についての教育及び研修を実施すること、磁気ディスクにより本人確認情報を送付する場合において盗難等の防止のための措置を講ずること、本人確認情報を取り扱う者を限定すること、大量の本人確認情報を取り扱う際には責任者の承認を得ること、本人確認情報の取扱い等について委託を行う場合は第４の10と同様の措置を講ずること、本人確認情報の保存を行う必要がある期間経過後遅滞なく、当該本人確認情報を確実に消去すること等、本人確認情報の適切な管理のための措置を講ずること。

ウ　都道府県知事（委任都道府県知事にあっては、指定情報処理機関）は、必要に応じ、国の機関等に対し、提供を行った本人確認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。また、委任都道府県知事は、必要に応じ、指定情報処理機関を経由して、国の機関等に対し、指定情報処理機関が提供を行った当該都道府県の住民に係る本人確認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。

エ　市町村長は、必要に応じ、都道府県知事（指定情報処理機関が本人確認情報の提供を行った場合は、都道府県知事及び指定情報処理機関）を経由して、国の機関等に対し、都道府県知事又は指定情報処理機関が提供を行った当該市町村の住民に係る本人確認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。

(2) 区域内の市町村の執行機関等に対する本人確認情報の提供

ア　都道府県知事又は指定情報処理機関は、必要に応じ、区域内の市町村の執行機関等（当該都道府県の区域内の市町村の執行機関、他の都道府県の執行機関又は他の都道府県の区域内の市町村の執行機関をいう。以下同じ。）に対し、提供を行った本人確認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。また、委任都道府県知事は、必要に応じ、指定情報処理機関を経由して、区域内の市町村の執行機関等に対し、指定情報処理機関が提供を行った当該都道府県の住民に係る本人確認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。

イ　市町村長は、必要に応じ、都道府県知事（指定情報処理機関が本人確認情報の提供を行った場合は、都道府県知事及び指定情報処理機関）を経由して、区域内の市町村の執行機関等に対し、都道府県知事又は指定情報処理機関が提供を行った当該市町村の住民に係る本人確認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。

(3) 市町村長が行う他の市町村の執行機関への本人確認情報の提供

市町村長は、必要に応じ、他の市町村の執行機関に対し、提供を行った本人確認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。

(4) 都道府県知事の本人確認情報の利用等

ア　都道府県知事は、必要に応じ、当該都道府県の執行機関（都道府県知事を除く。）に対し、提供を行った本人確認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。

イ　市町村長は、必要に応じ、都道府県知事に対し、都道府県知事が利用した当該市町村の住民に係る本人確認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。また、市町村長は、必要に応じ、都道府県知事を経由して、当該都道府県の執行機関（都道府県知事を除く。）に対し、都道府県知事が提供を行った当該市町村の住民に係る本人確認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。

(5) 都道府県知事の本人確認情報の提供又は利用の状況に係る情報の保存

ア　都道府県知事は、自己に係る本人確認情報の提供又は利用の状況に関する情報の開示請求に適切に対応するため、国の機関等、区域内の市町村の執行機関等若しくは当該都道府県の執行機関（都道府県知事を除く。）に対し本人確認情報の提供を行った場合又は本人確認情報を利用した場合は、個人ごとの本人確認情報の提供又は利用の状況に係る情報を必要な期間保存すること。

イ　委任都道府県知事は、自己に係る本人確認情報の提供の状況に関する情報の開示請求に適切に対応するため、指定情報処理機関に対し、指定情報処理機関が国の機関等又は区域内の市町村の執行機関等に対し本人確認情報の提供を行った場合における個人ごとの本人確認情報の提供の状況について報告を求め、当該提供の状況に係る情報を保存すること。この場合において、指定情報処理機関は、委任都道府県知事に対し、住民基本台帳ネットワークシステムを通じて、当該提供の状況に係る情報の通知を行うことができること。

ウ　都道府県知事は、ア及びイの情報について、保存を行う必要がある期間経過後遅滞なく、確実に消去すること。

(6) 指定認証機関に対する異動等情報の提供

ア　都道府県知事又は指定情報処理機関は、指定認証機関に対し、異動等情報の提供を行う場合は、あらかじめ、異動等情報の提供の具体的方法、異動等情報の漏えい、滅失及びき損の防止その他の異動等情報の適切な管理のための措置等について、指定認証機関と協議して定めること。

イ　指定認証機関は、異動等情報の提供を受けるに際しては、職員に対しセキュリティ対策についての教育及び研修を実施すること、異動等情報を取り扱う者を限定すること、異動等情報の取扱い等について委託を行う場合は第４の10と同様の措置を講ずること、異動等情報を確実に消去すること等、異動等情報の適切な管理のための措置を講ずること。

ウ　都道府県知事又は指定情報処理機関は、必要に応じ、指定認証機関に対し、提供を行った当該都道府県の住民に係る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。

　また、委任都道府県知事は、必要に応じ、指定情報処理機関を経由して、指定認証機関に対し、指定情報処理機関が提供を行った当該都道府県の住民に係る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。

エ　市町村長は、必要に応じ、都道府県知事（指定情報処理機関が異動等情報の提供を行った場合は、都道府県知事及び指定情報処理機関）を経由して、指定認証機関に対し、都道府県知事又は指定情報処理機関が提供を行った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。