セキュリティ基本方針書

セキュリティ基本方針書については、住民基本台帳ネットワークシステム推進協議会（平成１２年９月２５日）において決定した。

指定情報処理機関が定める本人確認情報管理規程、都道府県及び市町村が個々に定める各種の規程・規則を制定・策定する際の根拠となるのみならず、住基ネットの設計・開発・運用に係るセキュリティ対策を実現する際の判断基準となるものである。

基本理念では、住基ネットにおけるセキュリティ対策を構する際の理念を掲げた。

住民基本台帳ネットワークシステムセキュリティ基本方針書
－本人確認情報の安全確保措置－

平成１２年９月２５日住民基本台帳ネットワークシステム推進協議会決定

基本理念

１．（安全性・信頼性の確保）

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。）では、全住民の大切な個人情報である本人確認情報が取り扱われる。基本法である住民基本台帳法に則るとともに、内外の個人情報保護制度、保護技術等の動向を踏まえ、制度、技術及び運用の各面にわたる総合的な安全確保措置を講ずることにより、住基ネットの安全性・信頼性を確保するものとする。また、必要に応じ安全確保措置の見直しを行う。

２．（相互連携・協力と責務の遂行）

住基ネットは、各都道府県、各市町村、都道府県の委任を受けた指定情報処理機関が役割分担の下に共同して整備・管理するネットワークシステムである。したがって、各都道府県、各市町村及び指定情報処理機関は、相互に密接な連携・協力関係を構築・維持し、住基ネットの統一性及び均質性等を保持するとともに、住基ネットの安定的かつ効率的な稼動により住民サービスの向上を図り、それぞれの責務を果たすものとする。

基本方針

１.機密性の確保

常に高い機密を保つためのセキュリティ対策を講ずる。

２.正確性の確保

常に最新かつ正確な状態を保つためのセキュリティ対策を講ずる。

３.住民サービスの継続

住民サービスの継続を確保するために必要なセキュリティ対策を講ずる。

４.本人確認情報の保護措置

住民基本台帳法に基づき、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。）の特性を踏まえた本人確認情報の保護措置を講ずる。

５.本人確認情報保護の優先

住基ネットの運営上、本人確認情報の保護が確保できないと思われる場合には、本人確認情報の保護を住民サービスの継続より優先する。

６.情報資産の適正な管理

外部からの不正な接続及び侵入等を防ぎセキュリティを確保するため、住基ネットを構成する全ての情報（データを含む。）、ソフトウェア、ハードウェア（ネットワークを構成する機器を除く。）、ネットワーク及び記録媒体（以下「情報資産」という。）を適正に管理する。

７.権限の適正な管理

住基ネット関係者は、職務に応じて適正な権限を付与される。付与された権限は不正に使用しない。また、不正に使用されないよう厳重に管理する。

８.各整備管理主体の連携・協力

住基ネットのセキュリティを維持及び遂行するために、都道府県、市町村及び指定情報処理機関等は相互に密接な連携・協力関係を構築・維持する。

９.秘密保持義務

住基ネット関係者及び住基ネット関係者であった者は、知り得た秘密の保持を義務とする。

１０．総合的なセキュリティ対策

住基ネットに対する危険・脅威を的確に把握し、制度面、技術面及び運用面から抑止、予防、検出及び回復について措置を講ずる。