5 個人情報保護のための施策

1 制度（法令）、技術、運用の３つの側面

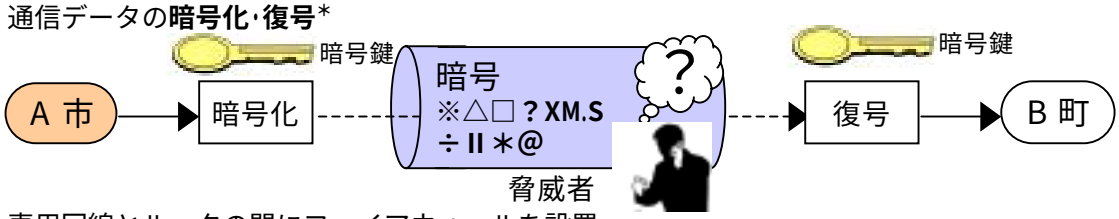
住基ネットワークシステムは、住民の大切な個人情報を取り扱うことから、個人情報の保護を最も重要な課題としています。このため、個人情報保護に関する**国際基準**（**OECD8原則***）を踏まえたうえで、制度（法令）、技術、運用の3つの側面から個人情報を保護する対策を講じています。

制度面からの対策

(1)磁気ディスクに記録する情報を「本人確認情報」に限定しています。
※本人確認情報＝①氏名、②生年月日、③性別、④住所、⑤住民票コード、⑥付随情報
(2)本人確認情報の提供先、利用目的を住民基本台帳法で明確に規定しています。
(3)民間における住民票コードの利用を法令で禁止しています。
(4)「安全確保措置」、「秘密保持(罰則付)」を義務付けています。
(5)技術面及び運用面の対策を「セキュリティ基準」（総務省告示）に規定しています。

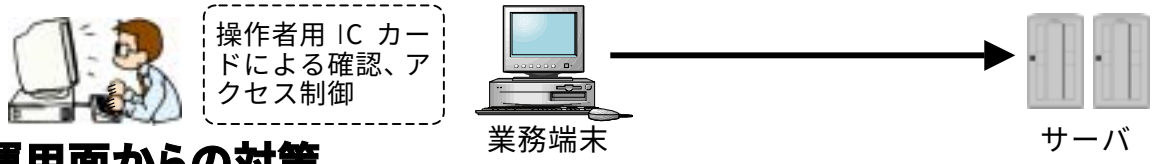
技術面からの対策

(1)外部ネットワークからの不正侵入、情報の漏えいを防止します。
・安全性の高い専用回線でネットワークを構築
・通信データの**暗号化・復号***



・専用回線とルータの間にファイアウォールを設置
・通信相手となるコンピュータとの相互認証
・電磁波漏えいを防止する機器を採用
・全国センターに「侵入検出装置（IDS）」を設置

(2)システム操作者の目的外利用を防ぎます。
・操作者用 IC カードやパスワード等による厳重な確認
・住基ネットワークシステムに蓄積されているデータへの接続制限
・不審な業務パターンの常時監視
・データ通信の履歴管理及び操作者の履歴管理
・ログ（使用記録）取得及び定期的な監査



運用面からの対策

運用管理を徹底し、情報の漏えいを防ぎます。
・「本人確認情報管理規程」の制定による厳重な安全確保措置
・地方公共団体における、体制、規程等の整備に係るセキュリティ対策に関する指針を作成
・指定情報処理機関に本人確認情報保護委員会を設置、都道府県に審議会を設置
・本人確認情報の漏えいのおそれがある場合の緊急時対応計画の作成
・安全・正確性の確保措置の地方公共団体職員及び本人確認情報の受領者への研修

●国際基準・OECD8 原則
1980 年 9 月、OECD（経済開発協力機構）は、「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告」を採択した。8 原則とは、①収集制限、②データ内容、③目的明確、④利用制限、⑤安全保護、⑥公開、⑦個人参加、⑧責任のそれぞれの原則をいう。

●暗号化・復号
データが第三者の不正行為により漏えい、盗聴されないようにすることを暗号化という。情報の受け手が暗号化された情報を元に戻すことを復号という。

●侵入検出装置（IDS）
「Intrusion Detection System」の略で、センサー部と管理装置で構成され、不審な通信パターンの検出を行う。

2 制度面（法令）による個人情報保護対策

平成１１年８月に公布された「住民基本台帳法の一部を改正する法律」では、①記録する個人情報の限定、②「本人確認情報」の利用及び提供制限、③本人確認情報の保護措置について、明確に規定しています。

記録する個人情報の限定

●本人確認情報の記録

都道府県、指定情報処理機関は通知される本人確認情報を磁気ディスクに記録することとしています。

本人確認情報
（
・氏名・生年月日・性別・住所・住民票コード
・付随情報
）

本人確認情報の利用及び提供の制限

●本人確認情報の利用及び提供の制限

本人確認情報を提供できる国の行政機関等及び利用できる事務処理の内容を法律で規定しています。

国の行政機関等
法律の根拠がない目的外の利用禁止

●提供状況の報告

指定情報処理機関は、本人確認情報の提供状況について、本人確認情報の提供先、提供年月、提供件数及び提供方法を少なくとも年１回報告書を作成し、公表しなければなりません。

指定情報処理機関
年次報告書

●住民票コードの利用制限等

市町村長等以外の者は、第三者に対し、住民票コードの告知を求めてはなりません。また、市町村長等以外の者は、業として、住民票コードの記録されたデータベースであって他に提供される予定のものを構成してはなりません。

民 間
住民票コードの
利用禁止

本人確認情報の保護措置

●役職員等の秘密保持義務等

指定情報処理機関の役員及び職員並びに都道府県及び市町村の職員は、本人確認情報処理等に関して知り得た秘密を漏らしてはなりません。また、秘密保持義務規定に違反した者に対しては、通常より重い罰則が課されます。

守秘義務

職 員

システム管理者

システム担当者

●本人確認情報の安全確保

指定情報処理機関、都道府県知事及び市町村長は、本人確認情報の漏えい、減失、き損の防止及びその他の本人確認情報の適切な管理のために必要な措置を講じなければなりません。

セキュリティ基準（総務省告示）の策定

●セキュリティ基準（総務省告示）の策定

住民基本台帳法令に基づき総務大臣が定める基準（「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」（平成１４年総務省告示第３３４号））により、市町村、都道府県、指定情報処理機関及び本人確認情報の提供を受けた行政機関に技術面及び運用面で十分な個人情報保護対策を義務づけています。

3 技術面によるトータルセキュリティ対策

個人情報の漏えい、改ざん、破壊、なりすまし等、住基ネットワークシステム上で考えられるあらゆる脅威に対して、システム、ネットワーク及び住民基本台帳カードそれぞれについて技術面によるトータルセキュリティを実現しています。

A システムのセキュリティ対策

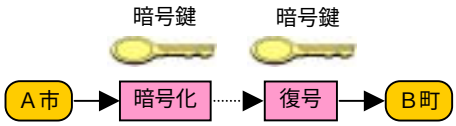
- 操作者用 IC カード認証

操作者用 IC カード

- ログイン認証
- アクセス制御
- 不審な業務パターンの常時監視
- ログ取得と監査
- 耐タンパー装置による秘密鍵の秘匿
- コンピュータウィルス対策
- 電磁波漏えい盗聴の防止

B ネットワークのセキュリティ対策

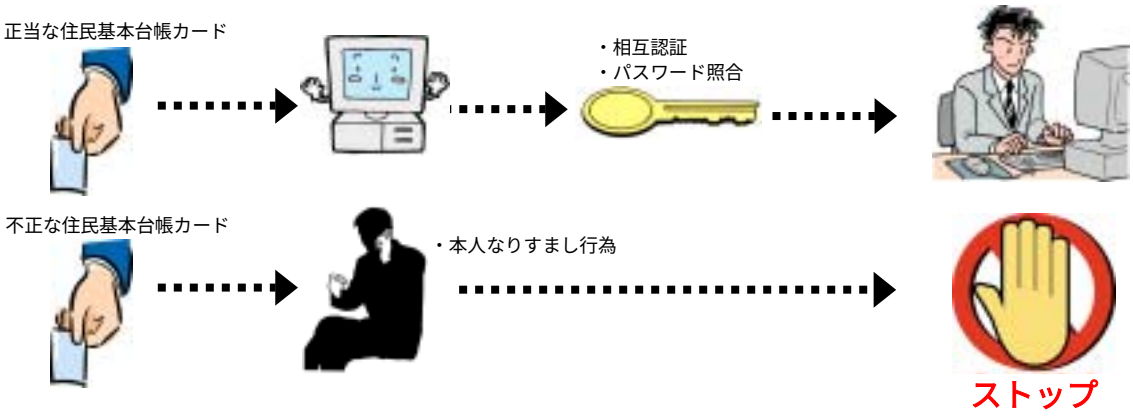
- 通信相手相互認証
- 通信の暗号化



- 電子記録媒体の暗号化
- ログ取得と監査
- ネットワークの物理的・論理的隔離
- ネットワーク機器の不正アクセス対策
- 不審な通信パターンの監視

C 住民基本台帳カードのセキュリティ対策

- パスワード設定によるカード有効化
- **パスワード照合・カードロック機能***
- **相互認証***機能
- カードの一時停止措置
- セキュアＩＣカード発行方式
- 輸送鍵の設定
- 強制アクセス制御機能
- **耐タンパー機構***



●パスワード照合･カードロック機能
住民基本台帳カードの利用にあたり、住民本人しか知り得ないパスワードで本人かどうか照合する。また、規定回数以上の照合に失敗すればカードは自動的に利用できなくなる機能がある。

●相互認証
カード利用時にシステム間の「公開鍵暗号方式」による相互の認証を行うこと。

●耐タンパー機構 (IC カード)
IC カードに埋め込まれたチップをこじ開け、偽造や改ざんを企てる者がいても、容易に不正行為ができないようにした仕組みをいう。

A システムのセキュリティ対策

市町村、都道府県及び指定情報処理機関におけるシステムセキュリティ対策としては、次のような個人情報の保護対策を講じています。

重要情報への不正アクセス防止

脅威者

端末の不正利用・不正操作防止

●操作者用 IC カード認証

システム利用の際には、必ず操作者用 IC カードを使用した認証（公開鍵暗号方式利用）を行い、権限外のシステム利用・操作を防止します。

操作者

操作者用
IC カード

●ログイン認証

システム起動の際には、必ず操作者によりログイン名とパスワードによるログイン認証を行うことで、権限外のシステム利用を防止します。

●アクセス制御

システムの重要な情報（データーベース、ファイル）へのアクセス制御を行います。セキュリティホールとなる不要なプロセスはシステム上から削除します。

●不審な業務パターンの常時監視

通常の業務パターンからかけ離れた端末操作の有無を常時監視し、異常があればその都度、システム管理者に報告するとともに、情報の送信を抑止します。

●ログ取得と監査

不正の監視、早期発見のために各種アクセスログを取得保存し、定期的に監査します。

●電磁波漏えい盗聴の防止

電磁波漏えい対策の規格を具備した機器を採用し、ディスプレイ画面からの漏えい電磁波を屋外から探知するなどのハイテク盗聴を防止します。

暗号鍵（秘密鍵）の不正対策

●耐タンパー装置*による秘匿

認証、暗号化に使用する鍵は、耐タンパー性の高い専用装置に秘匿し、暗号鍵（秘密鍵）の漏えい、改ざんを防止します。

暗号鍵

コンピュータウィルス対策

●ウィルスチェックプログラム

ウィルスチェックプログラムを常時起動させ、万が一コンピュータウィルスが混入した場合でも早期検出・除去を行います。

コンピューター
ウィルス

●耐タンパー装置

全国サーバ、都道府県サーバ、CS などに搭載して、セキュリティ上で重要な情報がハード構成から漏えいしないようにした装置のこと。

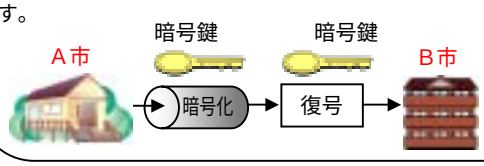
B ネットワークのセキュリティ対策

ネットワークはすべて専用回線による閉じたネットワーク構成となっています。また、ネットワークへの接続個所にはファイアウォールを設置し、不正行為や不正侵入ができないようにアクセス制御を行います。

ネットワーク上の通信への不正対策

●通信の暗号化

ネットワーク上の通信データは暗号化することで、盗聴・改ざんを防止します。暗号化は、**共通鍵暗号方式***で行い、暗号鍵（共通鍵）の交換は公開鍵暗号方式で行います。また、暗号鍵（共通鍵）は通信ごとに変更します。



●電子記録媒体の暗号化

電子記録媒体でデータの受け渡しをする場合も、格納するデータを暗号化します。

●通信相手相互認証

通信を行う際には、必ずお互いに通信相手の正当性を認証（公開鍵暗号方式利用）してから通信することにより通信相手のなりすましを防止します。

●ログ取得と監査

不正の監視、早期発見のために各種アクセスログを取得保存し、定期的に監査します。

ネットワークへの不正アクセス・不正侵入対策

●ネットワークの物理的・論理的隔離

専用回線の利用により第三者からの接続を隔離し、不正アクセス・不正侵入を防止します。また、ネットワークの接続個所にはファイアウォールを設置し、不正行為・不正侵入を防止します。

●ネットワーク機器での不正アクセス対策

ルータ等のネットワーク機器に対しては、適切なアクセス制御とセキュリティホールに対する対策を行います。

●不審な通信パターンの監視

全国センターに、「侵入検出装置（IDS）」を導入し、全国センター内や外部との不審な通信パターンを監視・解析します。

●共通鍵暗号方式
暗号文を作るときの暗号化と、暗号文を解読するときの復号に同じ鍵を使う暗号方式のこと。秘密鍵暗号方式とも呼ばれる。

C 住民基本台帳カードのセキュリティ対策

住民基本台帳カードの交付に際して、住民の本人確認の正確性を確保するため、カード交付通知を住民本人に郵送し、住所地市町村窓口でカード交付通知書と引き換えに住民基本台帳カードが交付されます。また、住民基本台帳カードには本人固有のパスワードが設定され、利用するたびにパスワードの照合作業を行い、なりすまし行為などの不正を防止できるように構成されています。

カードのなりすまし対策

●相互認証機能

カード利用時には、必ずシステム間の相互認証(公開鍵暗号方式利用)を行い、カードのなりすまし、偽造、改ざんを防止します。

●パスワード照合・カードロック機能

カード利用時には、必ずパスワード照合を行うことにより住民のなりすましを防止します。また、規定回数以上の照合失敗により、カードを自動的にロック状態にします。

●カードの一時停止措置

カード盗難・紛失時には、住民の届出によりカード交付管理システム上一時停止措置をとることにより、不正利用を防止します。

カード偽造･改ざん対策

●耐タンパー機構

チップのこじ開け等の攻撃があってもメモリ内の情報が読み出せないようにします。

●強制アクセス制御機能

利用権限のない者のカードに対する不正アクセスを防止します。

カード交付時のセキュリティ対策

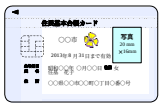
●セキュア IC カード交付方式

偽造などが容易にできないよう耐タンパー装置を利用した安全なカード交付を実現します。

未交付カードの盗難による不正利用対策

●輸送鍵の設定

未交付カードは、輸送鍵を解除しないとカード発行できないようにします。



●パスワード設定によるカード有効化

住民によりパスワードを設定していない未交付カードは利用できないようにします。

4 運用面による個人情報保護対策

指定情報処理機関においては「**本人確認情報管理規程***」に基づいて厳重な安全確保措置を図り、また、地方公共団体における体制、規程等の整備に係るセキュリティ対策に関する指針を**住基ネットワークシステム推進協議会***において作成しています。指定情報処理機関には「本人確認情報保護委員会」の設置、都道府県には本人確認情報の保護に関する審議会の設置が義務づけられています。万が一の際には、緊急時対応計画によりネットワークの運営を停止するなど、個人情報の保護を最優先した運営を行います。さらに、地方公共団体職員及び本人確認情報の提供を受ける行政機関の職員への研修を行います。

本人確認情報管理規程

●入退室管理規則
指定情報処理機関は、本人確認情報の電子計算機処理等を行う施設における入退室管理のため必要な事項を定めることになっています。

●本人確認情報取扱規則
指定情報処理機関は、本人確認情報の電子計算機処理等を行うにあたり、遵守しなければならない事項を定めることになっています。

セキュリティ対策に関する指針

●体制の整備
各地方公共団体は、住基ネットワークシステムの運営に係る責任体制、監査体制を確立するとともに、職員に対する教育・研修を行うこととしています。

●規程の整備
各地方公共団体は、セキュリティ組織規程、入退室管理規程、委託管理規程等住基ネットワークシステムの運営にあたり必要な規程を定めることとしています。

本人確認情報保護委員会、審議会

●本人確認情報保護委員会の設置
指定情報処理機関に設置する本人確認情報保護委員会は、本人確認情報の保護に関する事項を調査審議し、これに関し必要と認める意見を指定情報処理機関の代表者に述べることができます。

本人確認情報保護委員会

●都道府県の審議会の設置
都道府県に設置する審議会は、本人確認情報の保護に関する事項を調査審議し、これらの事項に関して都道府県知事に建議することができます。

都道府県の審議会

●本人確認情報管理規程
住民基本台帳法第30条の18の規定により、指定情報処理機関は、本人確認情報処理事務の実施にあたり、「本人確認情報管理規程」を定めて、総務大臣の認可を受けなければならないとされている。

● 住基ネットワークシステム推進協議会
指定情報処理機関の運営や住基ネットワークシステムの構築･運営について決定する機関であり、都道府県により構成されている。

緊急時対応計画

●指定情報処理機関における緊急時対応計画

指定情報処理機関は、本人確認情報の漏えいのおそれがある場合の行動計画を前もって定めることとされ、住基ネットの運営よりも本人確認情報の保護を最優先することとしています。

●地方公共団体における緊急時対応計画

各地方公共団体も、緊急時対応計画を定めることとしていますが、計画書の例を住基ネットワークシステム推進協議会において決定しております。

教育･研修

●地方公共団体における教育・研修

住基ネットワークシステムの稼働を前に、全国４７都道府県において担当者研修会を行うなど、セキュリティ対策等についての教育･研修を行うこととしています。

●本人確認情報の提供を受ける行政機関における教育・研修

本人確認情報の提供を受ける行政機関においてもセキュリティ対策等について教育･研修を行うこととし、指定情報処理機関が協力することとしています。