

## 2 「住民基本台帳ネットワークシステム」の概要

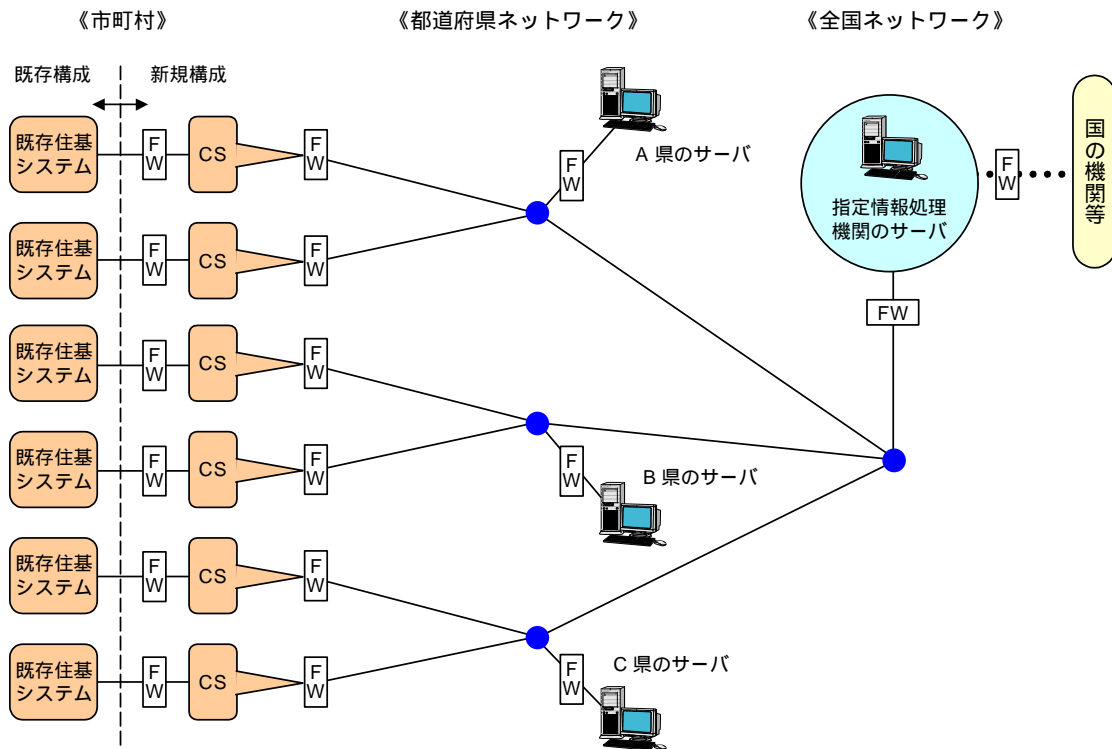
### 1 概要

住基ネットワークシステムの構築にあたり、人為的な不正行為、障害及び災害時にあっても、行政サービスが滞ることのないように、ネットワーク、サーバ、住民基本台帳カードのそれぞれの構成要素に、高い信頼性と安全性を備えたシステムを実現しています。

### 住基ネットワークシステムの構成要素

ネットワーク  
CS  
都道府県サーバ  
全国サーバ  
住民基本台帳カード

### ネットワークの概要図



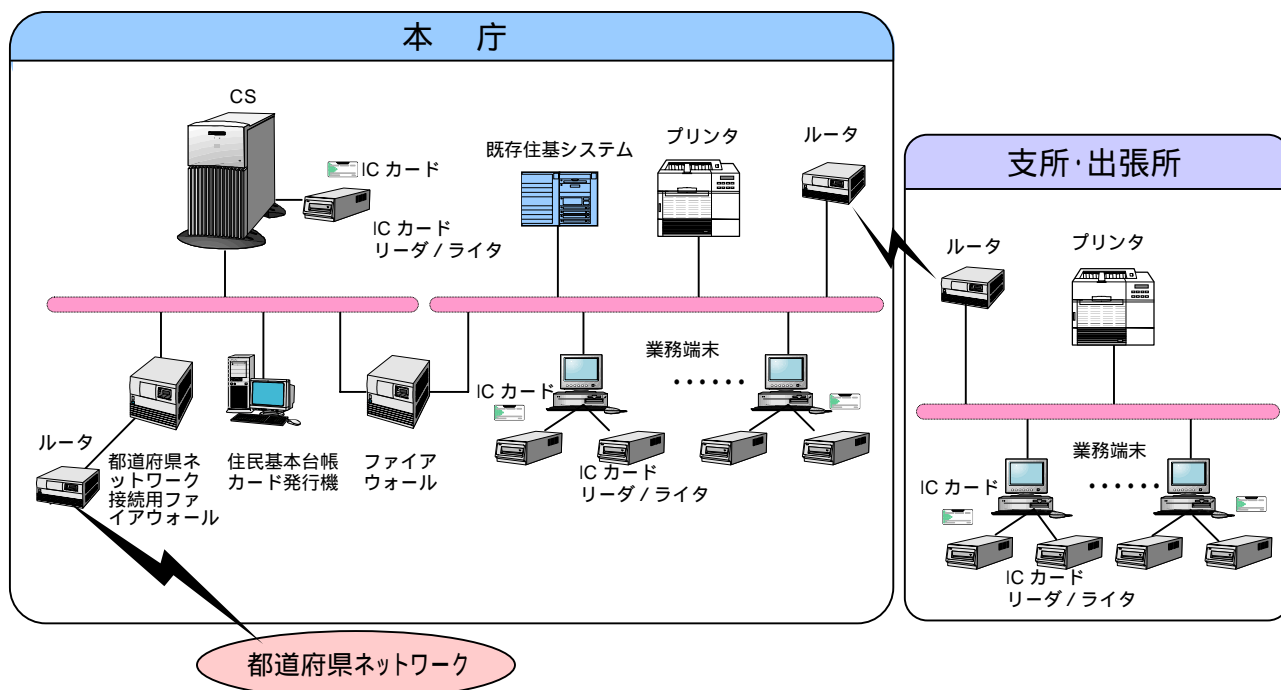
### ネットワークの信頼性確保

ネットワークは専用回線を利用して構築しています。また、ネットワーク障害による業務停止の可能性をできる限り排除するため、市町村(一部を除く)、都道府県及び指定情報処理機関のネットワーク機器及び専用回線について二重化を行っています。

## 2 市町村システムの特徴

市町村システムは、全国3,000を超える全市町村で整備され、住基ネットワークシステムに係る事務に利用されます。特徴としては、高セキュリティシステム、メンテナンス性重視の高い信頼性、既存住基システムとの親和性の高いシステム、操作性・運用性を追求したシステム、などが挙げられます。

### 市町村システムの概要図



### 市町村システムの機器構成と概要

番号	機器名	機器概要
	CS	本人確認情報を記録し、既存住基システム、都道府県サーバ、他市町村CSとデータ交換を行うためのサーバ。外部からのこじあけ等に対して防御性に優れた耐タンパー装置を内蔵。耐タンパー装置は通信時の相互認証及びデータの暗号化に必要な情報を保管管理
	業務端末	CSを利用した業務処理を行い、ICカードリーダー/ライターを接続する端末
	ICカードリーダー/ライター	住民基本台帳カード及び操作者用ICカードの読み書き用機器
	住民基本台帳カード発行機	住民基本台帳カードを発行する機器
	都道府県ネットワーク接続用ファイアウォール	都道府県ネットワークに対する不正アクセスを防止する住基ネットワークシステム専用の機器

## 高セキュリティシステム

市町村システムで管理されるデータの安全保護対策、不正アクセスの防止策には、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊及び盗難、端末の不正利用及びなりすまし等を防止します。具体的な対策は次のとおりです。

- ・ 操作者用 IC カード\* による認証とシステムへのログイン認証
  - ・ 操作者単位にデータの「読み取り」「書き込み」「実行」等のアクセス権限を設定
  - ・ ネットワーク上を流れるすべての通信データの暗号化を実施
- など

## メンテナンス性重視の高い信頼性

運用後の市町村システムの安定稼働を目指します。

### (1) ハードウェア対策

- ・ ハードディスクを RAID システム\* により冗長化
  - ・ 無停電電源装置(UPS)\* により、瞬断及び停電時の影響を排除
  - ・ CS 本体のクラスタ構成\* による二重化、あるいはリカバリサーバ\* の設置により、継続運用を実現
- など

### (2) ソフトウェア対策

- ・ 本人確認情報整合機能によりデータの信頼性を確保
  - ・ 指定情報処理機関からファイルデリバリー機能\* によりソフトウェア資源を配信して、メンテナンス性を向上
- など

## 「既存住基システム」との親和性の高いシステム

既存住基システムと CS との連携方法は、各市町村の取り扱う情報量を考慮し、“回線接続方式”と“媒体交換方式”のいずれかが選択できます。さらに“回線接続方式”はメッセージ転送方式\*かファイル転送方式\*かを選択できます。

- (1) 既存住基システムのさまざまな導入形態に対応した最適な CS の設置形態を実現します。
- (2) 連携する頻度、データ量を踏まえて既存住基システムのハード・ソフト環境に合わせた連携方式を実現します。

## 操作性・運用性を追求したシステム

実際に業務に携わる職員の視点から、住民基本台帳事務としての一連の手続きとシステム操作手順を整理し、わかりやすく操作性のよい画面構成、画面展開を実現します。

### 操作者用 IC カード

住基ネットワークシステムの業務アプリケーションを起動するとき、操作者が本人であるかどうかを認証・識別できる IC カードをいう。

### RAID システム

Redundant Array of Inexpensive Disks の略。低コストのハードディスクを複数台並べ、これにデータを分散して記録し、アクセスを分散させることにより、高速、大容量で信頼性の高いディスク装置を実現するための技術のこと。

### 無停電電源装置 (UPS)

Uninterruptible Power Supply の略。バックアップ用の電池を内部に持ち、停電時でもシステムをそのまま稼働できるようにする装置のこと。

システムを数分間稼働できる程度の容量の電池をもち、この間にシステムを安全にシャットダウンする。

### クラスタ構成

障害対策のために、あたかも一つのサーバに見えるように構成された複数のサーバを指す。

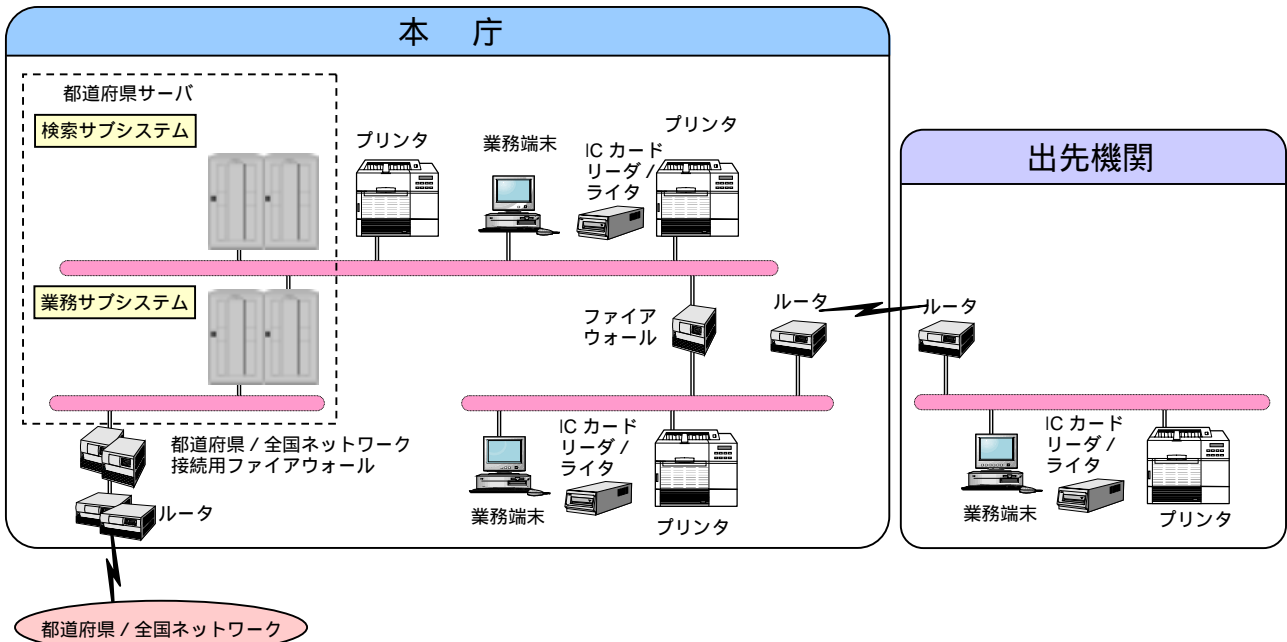
### リカバリサーバ

1 台のサーバがダウンしても、自動あるいは手動により処理内容を引継ぐもう一台のサーバのこと。

### 3 都道府県システムの特徴

都道府県システムは、都道府県内の住民の本人確認情報を記録・保存するとともに、市町村システムと指定情報処理機関システムとを結ぶ重要な中継機能を持ちます。特徴としては、高セキュリティシステム、高信頼性システム、システム利用者支援、などが挙げられます。

#### 都道府県システムの概要図



#### 都道府県システムの機器構成と概要

番号	機器名	機器概要
	都道府県サーバ	都道府県内の市町村住民の本人確認情報を管理するサーバ。サーバはフォルトトレラント構成*またはクラスタ構成を採用し、磁気ディスクのミラーリング*等により高信頼性システムを実現。検索サブシステムと業務サブシステムで構成
	業務端末	都道府県サーバの業務処理を行う装置。本人確認をはじめとした都道府県における各種業務の操作を実施
	ICカードリーダ/ライタ	住民基本台帳カード及び操作者用ICカードの読み書き用機器
	都道府県/全国ネットワーク接続用ファイアウォール	都道府県/全国ネットワーク上からの不正侵入を防止する住基ネットワークシステム専用の機器

#### ファイルデリバリ機能

遠隔地のサーバや端末に対して、プログラムや設定データなどのファイルをネットワークを通じて配信する機能のこと。

#### メッセージ転送方式

コンピュータ間でネットワークを介して通信を行うときに、メッセージと呼ばれるあらかじめ決められた制御文をやりとりすることにより処理を行う方式のこと。

#### ファイル転送方式

コンピュータ間でネットワークを介してデータの受け渡しを行うときに、ファイルというまとまったデータ単位で送信する方式のこと。

#### フォルトトレラント構成

システムの一部が故障しても、全体には影響を与えずに処理が続けられ、その間に故障部分を修理・交換してシステムが復旧される構成をいう。

#### ミラーリング

2台のハードディスクに対して全く同じデータを書き込み、一方のディスクに障害が発生してもデータに損害を与えないための機構のこと。

## 高セキュリティシステム

全国サーバ及びCSとの通信に際しては、最新の認証技術や暗号化技術を採用し、データの盗聴、改ざん、破壊、盗難及び端末操作者のなりすまし等の不正利用を防止できるので、セキュリティ面でより安全なシステムです。

## 高信頼性システム

都道府県サーバは、フォルトトレラント構成またはクラスタ構成を採用し、磁気ディスクのミラーリング等により高信頼性システムを実現します。

## システム利用者支援

GUI(Graphical User Interface)\*を用いたわかりやすく操作性のよい画面構成、画面展開を実現しています。

---

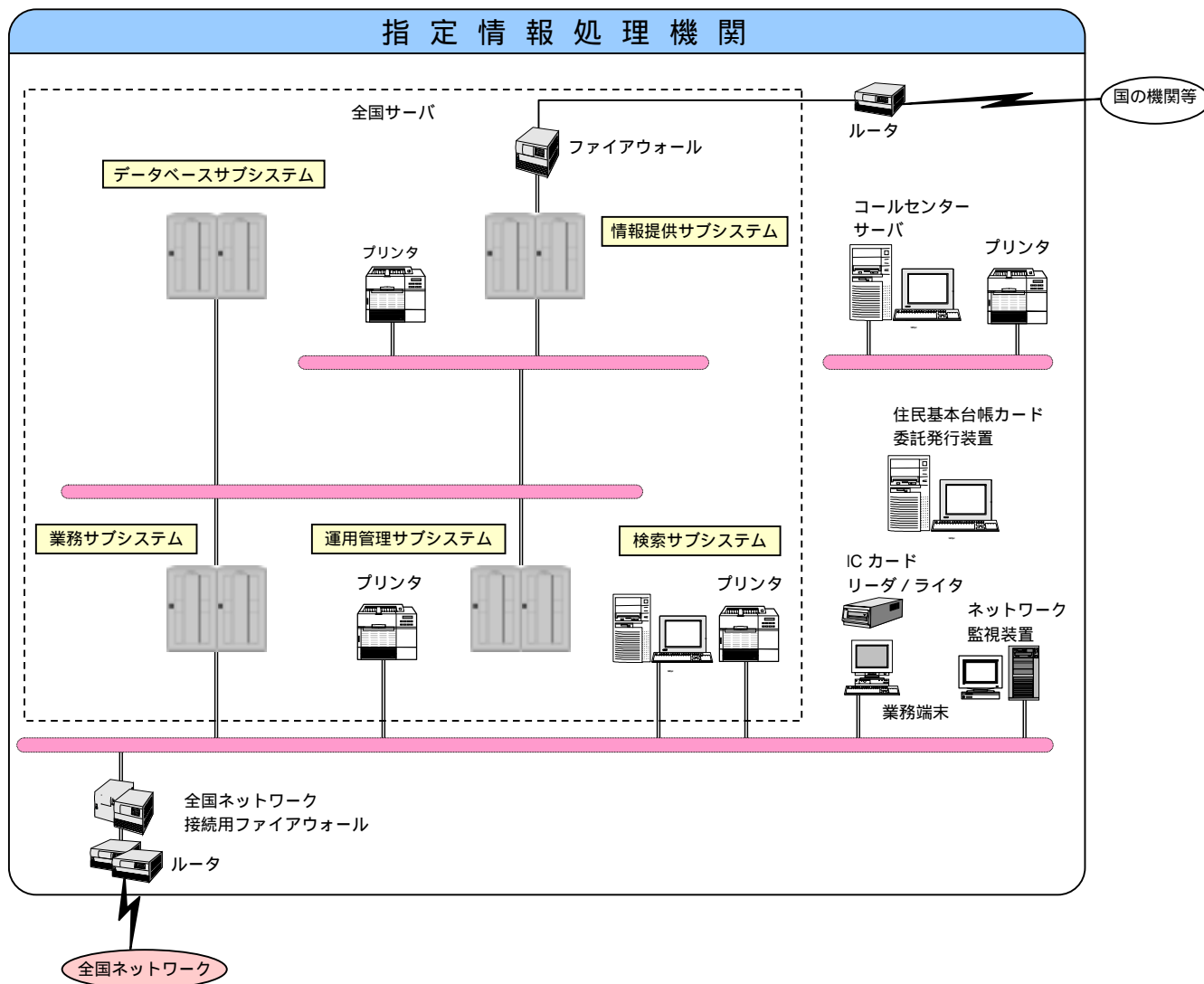
### GUI

Graphical User Interface の略。ビットマップディスプレイによる図形表示等、視覚的な要素を多用して、コンピュータの操作性やユーザに対する情報伝達を向上させたインターフェース。

## 4 指定情報処理機関システムの特徴

システムは、全国民の本人確認情報を管理するため、何よりも個人情報の適切な保護措置を最優先課題に構築しています。特徴としては、高セキュリティシステム、高信頼性システム、システム利用者支援、などが挙げられます。

### ● システムの概要図



## システムの機器の構成と概要

番号	機器名	機器概要
	全国サーバ	全国民の本人確認情報を記録、保存するサーバ。高信頼性システムを実現するクラスター構成。データベースサブシステム、情報提供サブシステム、業務サブシステム、運用管理サブシステム及び検索サブシステムで構成
	ネットワーク監視装置	住基ネットワークシステムのネットワーク機器の監視やサーバの稼働状況の把握を行う装置
	業務端末	指定情報処理機関の業務を行う端末装置。本端末装置では、住民基本台帳カードによる本人確認を実施
	ICカードリーダー/ライター	住民基本台帳カード及び操作者用ICカードの読み書き用機器
	コールセンターサーバ	コールセンター担当部門に寄せられる問合せ情報を管理するサーバ
	住民基本台帳カード委託発行装置	市町村からの委託を受け住民基本台帳カードを発行する装置。なお、住民基本台帳カード発行サーバには機密情報を安全に保管管理するための耐タンパー装置を内蔵
	全国ネットワーク接続用ファイアウォール	全国ネットワークへ接続する場合に、指定情報処理機関への不正アクセスを防止する住基ネットワークシステム専用の機器

## 高セキュリティシステム

最新の認証技術や暗号化技術を採用しており、データの盗聴、改ざん、破壊及び盗難、端末操作者のなりすまし等の不正行為を防止します。

## 高信頼性システム

全国サーバをはじめとするシステム構成ハードウェア及びネットワークの二重化によりサービスの連続性を維持し、障害が起りにくいシステムとなっています。

## システム利用者支援

### (1) 遠隔監視の実現

ネットワークシステム全体の効率的運営を確保するため、ネットワーク全体を常時監視する機能があります。

### (2) コールセンター機能の提供

市町村及び都道府県の業務運用担当者やシステム管理者からの技術面または運用面の問合せを、一元的に受付けて対応するコールセンター機能を提供します。

### (3) 操作性・運用性の追求

GUI (Graphical User Interface) を用いたわかりやすく操作性のよい画面構成、画面展開を実現します。

## 5 住民基本台帳カードの特徴

住基ネットワークシステムの住民基本台帳カードは、本人確認を確実にを行うための重要な構成要素であることから、高いセキュリティ機能を持つ IC カードを採用しています。

### 住民基本台帳カードの概要

#### (1) 住民基本台帳カードの交付

住民の申請により、住民の住所地の市町村長が住民基本台帳カードを交付します。(携帯が義務づけられることはありません。)

#### (2) カード内に記録する情報

- ・住民票コード
- ・パスワード
- ・公開鍵暗号方式\*に対応したカード固有の鍵情報

#### (3) カードの表面に記載する事項(予定)

- ・Aバージョン(氏名、有効期限、交付地市町村名)
  - ・Bバージョン(氏名、有効期限、交付地市町村名、住所、生年月日、性別、写真)
- A、Bのいずれを選ぶかは、住民が申請時に選択します。

#### (4) カードの有効期間

有効期間は10年間です。有効期間が満了後も、希望する住民には、再交付されます。

#### (5) 市町村の独自サービス

市町村の独自サービスの範囲は条例で定める目的に限定されるので、市町村が許可したアプリケーション以外のアプリケーションを搭載できないシステムになっています。また、住基ネットワークシステムサービス以外にどのような市町村独自サービスを受けるとかは住民が選択します。

#### (6) カードのセキュリティ対策

なりすまし、偽造、改ざん等に対し、安全性・信頼性の高い各種セキュリティ対策が講じられています。

住基ネットワークシステムサービス利用エリア、市町村独自サービスエリアは、それぞれ独立しています。したがって、住基ネットワークシステムから市町村独自サービスエリアの情報へアクセスすることはできませんし、住民票コードは、市町村独自サービスエリアでは使用されません。

#### (7) 点字エンボス加工

視覚障害者等でも住民基本台帳カードが使用できるように、住民の希望により表面に点字エンボス加工ができます。

(注) 以上は、今後公布される政省令により、変更が生じる可能性があります。

#### 公開鍵暗号方式

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異なる鍵を使用する暗号方式のこと。一方の鍵を秘密にしておいて、他方の鍵を公開することができる。「非対称暗号方式」とも呼ばれる。



# 住民基本台帳カードのデザイン・イメージ例

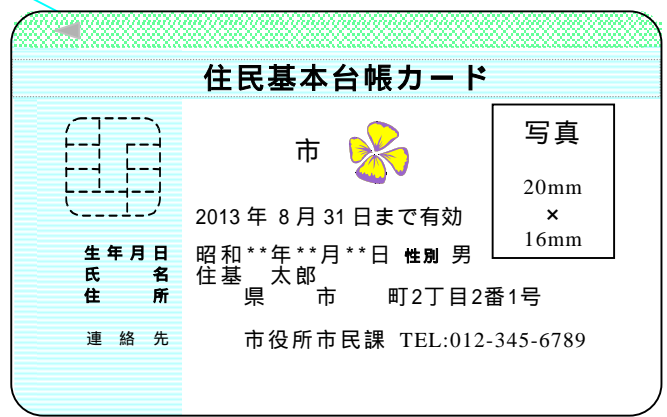
表面デザインイメージ例

目視角度により色が変化する特殊インク(プレ印刷)

A



B



内部アプリケーション等イメージ

