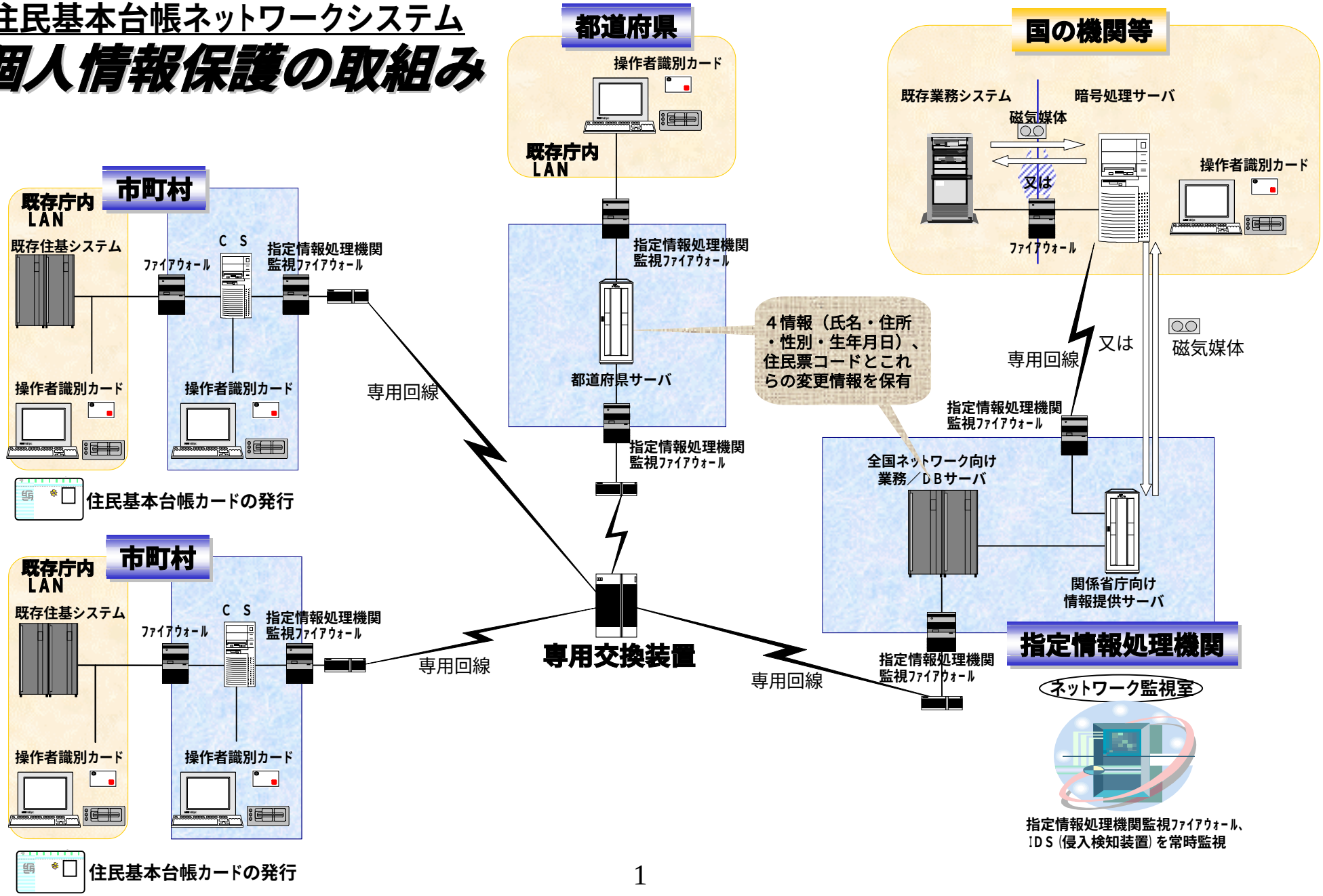
# 住民基本台帳ネットワークシステム
# 個人情報保護の取組み



住民基本台帳ネットワークシステム

# 個人情報保護の基本的考え方

## 保有情報の限定

◎　都道府県･指定情報処理機関が保有する情報は、本人確認情報、すなわち、4情報（氏名･住所･性別･生年月日）、住民票コードとこれらの変更情報に法律で限定。

※　変更情報は異動事由（「転入」、「出生」、「職権記載等」、「転出」、「死亡」、「職権消除等」、「転居」、「職権修正等」、「住民票コードの記載の変更請求」、「住民票コードの職権記載等」のいずれか）、異動年月日と異動前の本人確認情報であり、国外転出者等を除き過去5年間分を保存し、保存期間経過後確実に消去。

◎　住民票の写しの広域交付、転入転出手続の特例等の際には、市町村から市町村へ続柄、戸籍の表示等の情報も送信されるが、市町村のコミュニケーションサーバ（ＣＳ）はすべて全国ネットワーク又は都道府県ネットワークのいずれかの専用交換装置に直接接続され、任意の二つのＣＳ間で直通の通信を行うので、当該通信が都道府県サーバ・指定情報処理機関サーバを通過することも、そこに保有されることもない。

また、専用交換装置は、通過する情報を保存しない仕様となっている。

## 情報提供の限定

◎　情報提供を受ける行政機関や利用事務を法律で具体的に限定。**⇒２６４事務＋公的個人認証サービス事務**

※　都道府県・市町村が情報提供を受ける場合は、法律のほか条例により利用事務を追加できるが、国の機関等が情報提供を受ける場合は、法律以外による利用事務の追加はできない。

◎　情報提供を受ける行政機関や利用事務を変更する法律案を検討する場合、地方公共団体の意見を十分に踏まえ、第三者機関である住民基本台帳ネットワークシステム調査委員会の審議を経て行う。

◎　情報提供の方法としては、行政機関が申請・届出を行った者、年金受給者等についての情報が正確であるかどうかの照合を行う場合に、都道府県・指定情報処理機関から本人確認情報を提供。
　したがって、市町村の全住民の本人確認情報を行政機関に提供するような情報提供形態は全く想定されない。

◎　行政機関が提供を受けた本人確認情報を法律で限定された利用事務以外に利用するは一切禁止。

## 責任体制の確立

◎　市町村はＣＳ（市町村の住民の本人確認情報を保存）の管理責任を負い、都道府県は都道府県サーバ（都道府県の住民の本人確認情報を保存）と都道府県ネットワークの管理責任を負い、指定情報処理機関は指定情報処理機関サーバ（全住民の本人確認情報を保存）と全国ネットワークの管理責任を負う。
　総務省は、制度を所管する立場から、また、指定情報処理機関に対して監督を行う立場から責任を負う。

◎　指定情報処理機関は国の機関等に本人確認情報の提供を行う際には、あらかじめ国の機関等が行う個人情報保護措置等を定めた協定書を取り交わす。また、指定情報処理機関は、本人確認情報の保護を図るため必要がある場合には、国の機関等に対し、報告要求、情報提供停止等を行うことができる。

◎　市町村は、当該住民の本人確認情報の保護を図るため必要がある場合には、都道府県に対し、都道府県を経由して指定情報処理機関に対し、あるいは、都道府県・指定情報処理機関を経由して国の機関等に対し、報告要求等を行うことができる。
　都道府県は、当該住民の本人確認情報の保護を図るため必要がある場合には、指定情報処理機関に対し、あるいは、指定情報処理機関を経由して国の機関等に対し、報告要求等を行うことができる。

◎　都道府県に本人確認情報保護審議会を、指定情報処理機関に本人確認情報保護委員会を設置。
　総務省に住民基本台帳ネットワークシステム緊急対策本部や第三者機関である住民基本台帳ネットワークシステム調査委員会を設置。

## 住民票コードの利用の限定

◎　住民票コードは無作為の番号で、住民の申請によりいつでも変更できる。

◎　民間部門が住民票コードを利用することは禁止されている。特に、民間部門が契約に際し住民票コードの告知を要求したり、住民票コードの記録されたデータベースで他に提供されることが予定されているものを構成した場合、都道府県知事は中止勧告や中止命令を行うことができる。都道府県知事の中止命令に違反した者は、１年以下の懲役又は５０万円以下の罰金が科せられる。

◎　行政機関が住民票コードを利用する場合も、目的外利用の禁止、告知要求制限等の規定により利用が制限。
　したがって、指定情報処理機関と国の機関等との間は住民票コードを利用して本人確認情報の提供を行うことができるが、国の機関等と他の国の機関等との間で住民票コードを利用してデータマッチングをすることはできない。

◎　都道府県と制度を所管する総務省は連携して、住民票コードの民間部門での利用や行政機関での違法な利用がなされないよう、周知徹底、調査等を実施。
　このような取組みにより、住民票コードが、米国のSocial Security Numberのように、事実上官民問わず利用される「共通番号」となることを防止。

住民基本台帳ネットワークシステム

# 外部からの侵入防止対策

## 住基ネットの閉域性

◎　コミュニケーションサーバ（ＣＳ）、都道府県サーバ及び指定情報処理機関サーバ間の通信は、全て専用回線及び専用交換装置で構成されたネットワークを介して行う。また、指定情報処理機関サーバと国の機関等サーバとの間は、専用回線又は磁気媒体でデータ交換を行う。

したがって、これらのサーバ以外との通信を行うことはできない。

## 通信相手の相互認証・暗号通信

◎　暗号技術評価委員会（ＣＲＹＰＴＲＥＣ）において安全性が確認されている公開鍵方式により、通信を行うごとに意図した通信相手に接続されたことを相互に認証する。また、この公開鍵方式における秘密鍵は、指定情報処理機関で耐タンパー装置に封入設定後、当該耐タンパー装置を地方公共団体及び国の機関等に配送するため、第三者（地方公共団体及び国の機関等を含む）が内容を読み出したり、変更することはできない。

したがって、仮に他のサーバをネットワーク接続できたとしても、通信を行うことはできない。

◎　通信相手の相互認証の過程で、その都度耐タンパー装置内で、ＣＲＹＰＴＲＥＣにおいて暗号強度が認知されている暗号方式の一つにより、通信の都度共通暗号鍵を設定し、これをさらに公開鍵方式における公開鍵で暗号化した上で通信相手に輸送する。通信を行う二つのサーバはその共通暗号鍵により暗号化してデータの送信を行い、通信が終わればその共通暗号鍵は廃棄される。

住基ネットにおけるデータ送受信は短時間であり、その都度共通暗号鍵が変わるため、盗聴による恒常的な暗号鍵の解読は不可能。

## 通信プロトコルの制限

◎　住基ネットの通信プロトコルはＴＣＰ／IPを基盤としているが、独自の住基ネットアプリケーションによる通信を行っており、ＳＭＴＰ（電子メール転送プロトコル）、ＨＴＴＰ（WWWデータ転送プロトコル）、ＦＴＰ（ファイル転送プロトコル）、Telnet（仮想端末プロトコル）等のインターネットで用いられる汎用的なプロトコルを使用していない。

　また、すべてのＣＳのネットワーク側、すべての都道府県サーバのネットワーク側と端末機側（端末機側については、都道府県サーバと既存庁内ＬＡＮを接続しない団体を除く）、指定情報処理機関サーバの全方向及び国の機関等サーバ（指定情報処理機関とネットワーク接続しない国の機関等サーバを除く）のネットワーク側に指定情報処理機関監視ファイアウォールを設置して、インターネットで用いられるプロトコルの通過を遮断。

　したがって、ＣＳ、都道府県サーバ、指定情報処理機関サーバ及び国の機関等サーバに対し、ネットワーク側から、住基ネットアプリケーション以外の通信を使用してアクセスすることはできない。また、万一サーバがコンピュータウィルスに感染しても、これを媒介感染しうる通信を行っていないので、他のサーバに感染する可能性はない。

## コンピュータウィルス・セキュリティホール対応

◎　指定情報処理機関において、コンピュータウィルスの発生情報を常時入手し定期的に（危険度が高いものについては随時）、パターンファイルを全団体に配付。また、ＯＳ（Windows、UNIX等）のセキュリティホール発生情報を入手し、危険度が高いものは、システムの影響度を確認した上で全団体にセキュリティホール情報及び対応方法を通知。その他のものは、サービスパック単位でシステムの動作確認を行った上で全団体にサービスパックの適用を通知。

## 不正な通信の遮断と監視

指定情報処理機関監視ファイアウォール、ＩＤＳ

◎　指定情報処理機関監視ファイアウォールは、ラックに厳重に格納・施錠されており、指定情報処理機関のネットワーク監視室から運用管理規程に基づき、ネットワーク側への不正な通信がないか、あるいは、ネットワーク側からの

不正な通信がないか、２４時間常時監視を行っている。万一不正アクセスの前兆を検出した場合、緊急時対応計画等に基づき必要な連絡、対策（関係サーバの一時切り離し等を含む）等を実施。

ネットワーク内にＩＤＳ（侵入検知装置）を設置し、運用管理規程に基づき、指定情報処理機関のネットワーク監視室から常時監視を行うほか、定期的にログの解析を行っている。万一指定情報処理機関監視ファイアウォールを通過した不正アクセスを検出した場合、緊急時対応計画等に基づき必要な連絡、対策等を実施。

**指定情報処理機関サーバ**

◎　指定情報処理機関監視ファイアウォールによって、全方向からの不正な通信を遮断。

**都道府県サーバ**

◎　指定情報処理機関監視ファイアウォールによって、全方向からの不正な通信を遮断。

端末機を設置するため都道府県サーバと既存庁内ＬＡＮを接続する場合、都道府県が厳格に管理するファイアウォールと指定情報処理機関監視ファイアウォール（都道府県サーバと既存庁内ＬＡＮを接続しない団体を除く）によって、端末機側からの不正な通信を遮断。既存庁内ＬＡＮがさらに外部ネットワークと接続する一部の団体は、さらに都道府県管理のファイアウォールを設置し外部からの不正な通信を遮断。

**コミュニケーションサーバ（ＣＳ）**

◎　指定情報処理機関監視ファイアウォールによって、全方向からの不正な通信を遮断。

既存住基システムと接続し、端末機を設置するためＣＳと既存庁内ＬＡＮを接続する場合、市町村が厳格に管理するファイアウォールによって、既存住基システム・端末機側からの不正な通信を遮断。既存庁内ＬＡＮがさらに外部ネットワークと接続する一部の団体は、さらに市町村管理のファイアウォールを設置し外部からの不正な通信を遮断。

**国の機関等サーバ**

◎　指定情報処理機関監視ファイアウォールによって、全方向からの不正な通信を遮断（ネットワーク接続を行わず媒体交換を行うところもある）。

端末機を設置するため、国の機関等サーバと既存庁内ＬＡＮを接続する場合、国の機関等が厳格に管理するファイアウォールによって、端末機側からの不正な通信を遮断。既存庁内ＬＡＮがさらに外部ネットワークと接続する場合（現時点では存在しない）は、さらに国の機関等管理のファイアウォールを設置し外部からの不正な通信を遮断。

住民基本台帳ネットワークシステム

# 内部の不正利用防止対策

## 刑罰の重科

◎　住民基本台帳法により、市町村、都道府県、指定情報処理機関及び国の機関等の担当職員に守秘義務を課し、違反した場合の刑罰を加重する（通常は1年以下の懲役又は3万円以下の罰金　→　2年以下の懲役又は１００万円以下の罰金）。委託業者が秘密を漏らした場合も同じ刑罰が科せられる。

　また、住基ネットを運用する通信事業者は、電気通信事業法により、さらに重い刑罰が科される（3年以下の懲役又は１００万円以下の罰金）。

◎　行政機関個人情報保護法において、国の機関等の担当職員が正当な理由がなく個人情報を提供した場合（2年以下の懲役又は１００万円以下の罰金）、不正な利益を図る目的で個人情報の提供又は盗用を行ったり、職務の用以外の用に供する目的で職権を濫用した個人の秘密を収集した場合（1年以下の懲役又は５０万円以下の罰金）は刑罰が科される予定。

## 照会条件の限定

◎　即時提供（端末機から照会条件を入力し、都道府県サーバ又は指定情報処理機関サーバから即時に本人確認情報の提供を受ける方式）の場合、「住民票コード」、「氏名＋住所」又は「氏名＋生年月日」を端末機に入力しないと本人確認情報の提供を受けられない。「氏名＋住所」又は「氏名＋生年月日」を入力する場合は前方一致検索が可能であるが、該当者が５０人を超えるときは本人確認情報の提供を受けられない。

※　前方一致検索は、少なくとも「氏名の先頭一文字＋住所全部」、「氏名全部＋住所の都道府県・市町村名を除いた先頭一文字」、「氏名の先頭一文字＋生年月日全部」の入力が必要。

◎　一括提供（本人確認情報照会対象者の情報をファイル化して都道府県サーバ又は指定情報処理機関サーバに照会し、これらのサーバから照会結果ファイルを受け取る方式）の場合も同様で、照会元から送られてきた「住民票コード」、「氏名＋住所」、「氏名＋生年月日」等のファイルに、都道府県サーバ又は指定情報処理機関サーバにおいて、本人確認情報を追記して照会元にファイルを返送。

## 操作者識別カード認証によるアクセス制御

◎　本人確認情報は、ＣＳ、都道府県サーバ及び指定情報処理機関サーバ内に保存しており、端末機には存在しない。端末機からサーバにアクセスする際には、常に操作者識別カードと端末機との間で相互認証を行って初めて住基ネットアプリケーションが起動する設計であり、アクセス権限のない職員等及び外部からの本人確認情報データベースへアクセスすることはもちろん、住基ネットアプリケーションを起動することもできない。

　なお、操作者識別カードの種別により、システム操作者ごとに住基ネットが保有するデータ等へ接続できる範囲を限定。

## アクセスログの定期的解析と調査

◎　指定情報処理機関は、運用管理規程に基づき、定期的に指定情報処理機関サーバのアクセスログの解析を行う。万一不正使用の兆候を検出した場合は、緊急時対応計画等に基づき必要な連絡、対策等を実施する。

　都道府県においても、同様にアクセスログの解析を行う。

◎　市町村は、都道府県に対し、あるいは、都道府県を経由して指定情報処理機関に対し、住民のアクセスログの解析要請を行うことができる。

　都道府県は、指定情報処理機関に対し、住民のアクセスログの解析要請を行うことができる。

## 住民に対する本人確認情報提供状況の開示

◎　都道府県サーバ及び指定情報処理機関サーバにおいて、本人確認情報提供状況の開示用データ（提供先／検索元、提供年月日、利用目的等）を生成する機能を実装。

　都道府県は、都道府県サーバの開示用データ及び指定情報処理機関から送信される指定情報処理機関サーバの開示用データを保存し、それぞれの個人情報保護条例により住民から請求があった場合その開示を行う（平成１５年１１月より、準備の整った都道府県から順次、実施）。

## 住民票の写しの広域交付における不正防止

◎　住所地市町村において、交付地市町村の特定の操作者識別カードから一定時間に一定数以上の住民票の写しの広域交付要求があった場合は、住民票の写しの広域交付を停止。

## 担当職員に対する啓発活動

◎　毎年、４７都道府県において、セキュリティ研修会を実施。

　また、本人確認情報の提供を受ける国の機関等の担当職員向けの研修会を実施。

住民基本台帳ネットワークシステム

# 地方公共団体に対する支援

## 一次稼働に際しての支援

◎　住基ネットの一次稼働（平成１４年８月５日）に際し、全市町村を対象に既存庁内ＬＡＮ構成の外部ネットワークからの安全性について点検し、このうち安全性が確認できなかった市町村について、外部ネットワークとの切断又はＣＳ－既存庁内ＬＡＮ間の接続規制を要請し、その間に改善のための技術支援を実施。

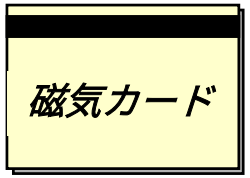
## 二次稼働に際しての支援

◎　全市町村を対象として、セキュリティチェックリストによる点検を要請。また、１０８市町村を選定し、システム運営監査を行い、セキュリティチェックリストの記載内容の検証を実施。

◎　セキュリティチェックリストを回収・分析した結果を踏まえ、４７都道府県を通じて全市町村を対象に技術指導を行い、住基ネットの二次稼働（平成１５年８月２５日）までに改善を図る。

# 住民基本台帳カード

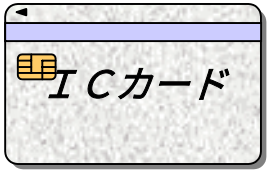
## 磁気カードとICカードとの比較




基本的には
磁気カードはカセットテープと同じ原理。

読み取り装置さえあれば、容易に全ての記録情報が読み取り（書き込み）可能

単に情報を記録する媒体




一方、ＩＣカードは．．．
ＩＣチップで情報記録と情報処理を行なうパーソナルコンピュータ。

暗号化したり、格納される場所に鍵をかけることにより、アクセス権をコントロールする。

情報記録に加え、暗号化や情報保護などの各種情報処理が可能な小さなコンピュータ

## ICカードの利用形態の変遷

| | | |
|---|---|---|
| ICカードの利用環境 | 1枚のカードを1つの目的に利用<br>単目的利用（シングルアプリケーション） | 1枚のカードを複数目的に利用<br>多目的利用（マルチアプリケーション） |
| ICカードの役割 | 主としてデータキャリーの役割<br>（データベースとしての情報蓄積機能） | 主としてキーデバイスの役割<br>（データベースにアクセスするための認証・暗号化機能） |
| ICカードのセキュリティ機能 | ・ｶｰﾄﾞ内保持ﾃﾞｰﾀのｱｸｾｽ管理のみ<br>・暗号機能無し | ・ｶｰﾄﾞ内保持ﾃﾞｰﾀのｱｸｾｽ管理<br>・暗号機能を利用した認証 | ・ｶｰﾄﾞ内保持ﾃﾞｰﾀのｱｸｾｽ管理<br>・さらに強固な暗号の採用や暗号化通信など、より高レベルのセキュリティ機能を実現 |

# 住民基本台帳カード

## カード利用の考え方

1．住民基本台帳カードは、希望する住民に対して、市町村長から交付

2．市町村は、条例の定めにより、カードの独自利用領域を活用した独自サービスの提供が可能

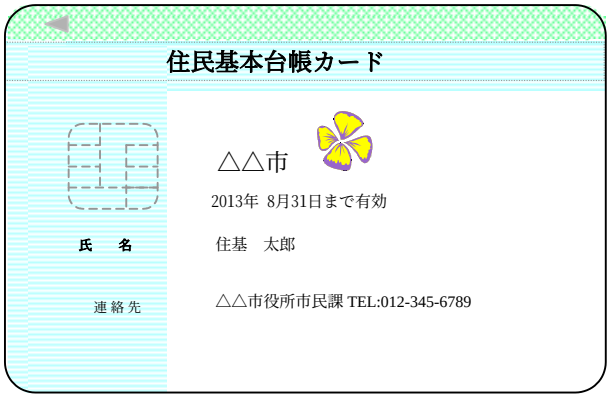
3．カードの独自利用領域を活用した個々のサービス提供は、住民本人の判断により自由に選択

4．住民基本台帳ネットワークシステムでの利用領域、市町村独自利用の各領域はそれぞれ独立

5．独自サービスではアクセスキーとして住民票コードを使用しない等、個人情報保護に配慮

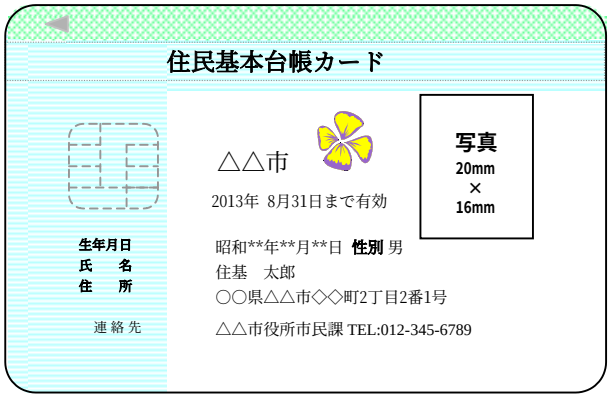
## 券面記載事項

**Aバージョン**




<券面記載事項>
・氏名

**Bバージョン**

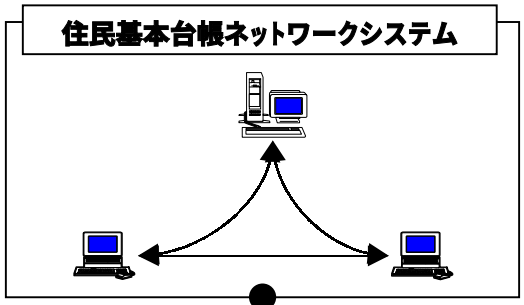



<券面記載事項>
・氏名
・出生の年月日
・男女の別
・住所

**→公的身分証明書として活用**

# 住民基本台帳カード

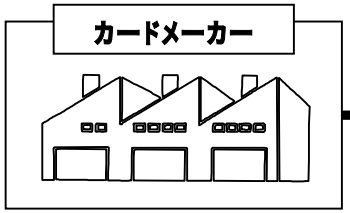
## セキュリティ対策の概要




**ISO15408に基づく評価・認証製品の利用**：ITセキュリティ評価/認証制度に基づくカード調達手続きの実施

**相互認証**：暗号アルゴリズムを利用した認証によりシステムとカードが相互に正当性を確認

**パスワード照合**：利用者のパスワードをカードに送信／照合することによりカードと利用者の結びつきを確認



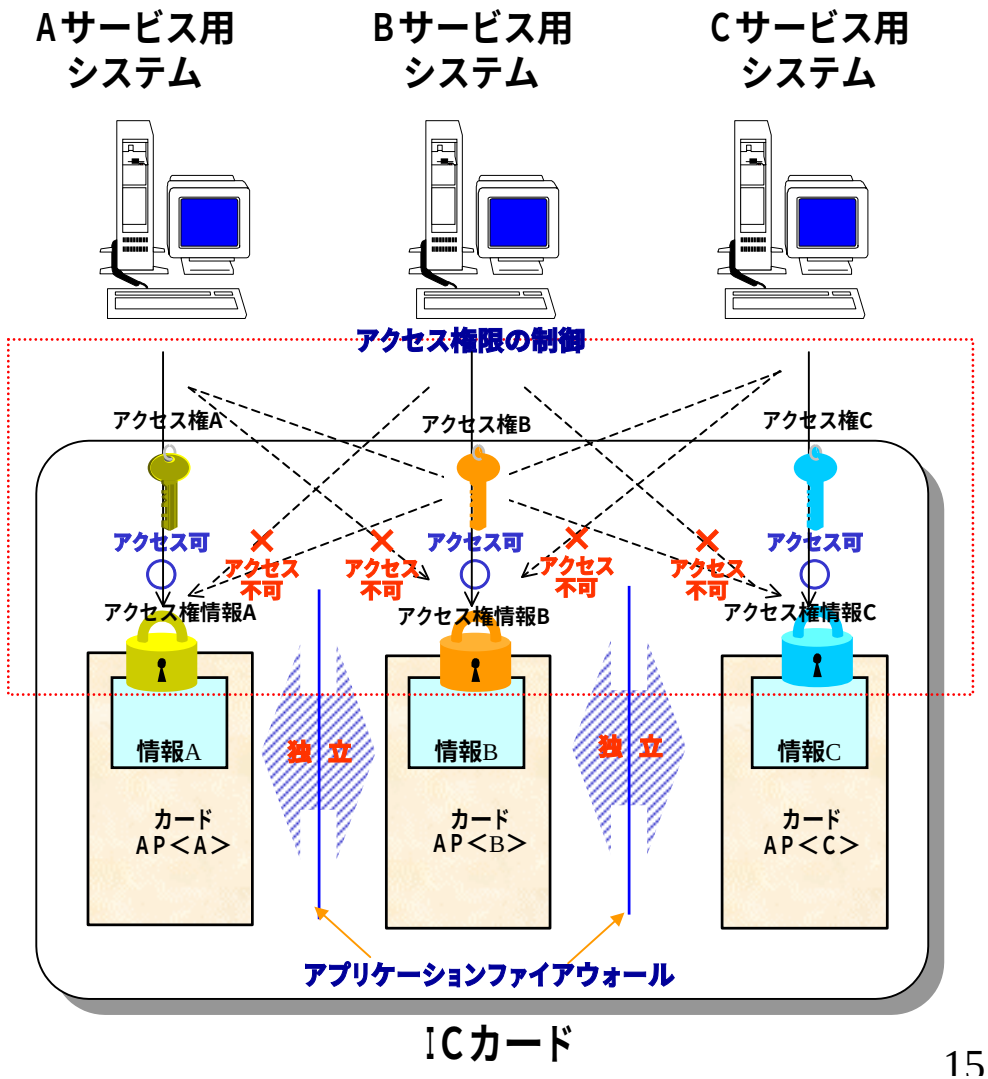

住民基本台帳カード


**輸送鍵**：正しいカード発行者のみが解くことができる鍵をカードに設定し、輸送途中の不正利用からカードを保護

- **アクセス権限の制御**：カード内情報を不正アクセスから保護
- **アプリケーションファイアウォール**：カードアプリケーション間の独立性を確保
- **耐タンパー性**：物理的/論理的攻撃に対するICチップによる防御対策

# 住民基本台帳カード

## アクセス権限の制御とアプリケーションファイアウォール




### アクセス権限の制御

- カード内の各情報毎にアクセス権情報（「認証済みにより読出し可能」等の条件を示すｾｷｭﾘﾃｨ属性）が設定される（図のアクセス権情報A/B/C）。
- アクセス権情報に対し、認証／ﾊﾟｽﾜｰﾄﾞ照合が正しく行われたことにより獲得されるアクセス権（認証／照合結果としてカードに保持されるセキュリティステータス）が、アクセス権情報の条件を満たす場合、情報へのアクセスが可能となる。

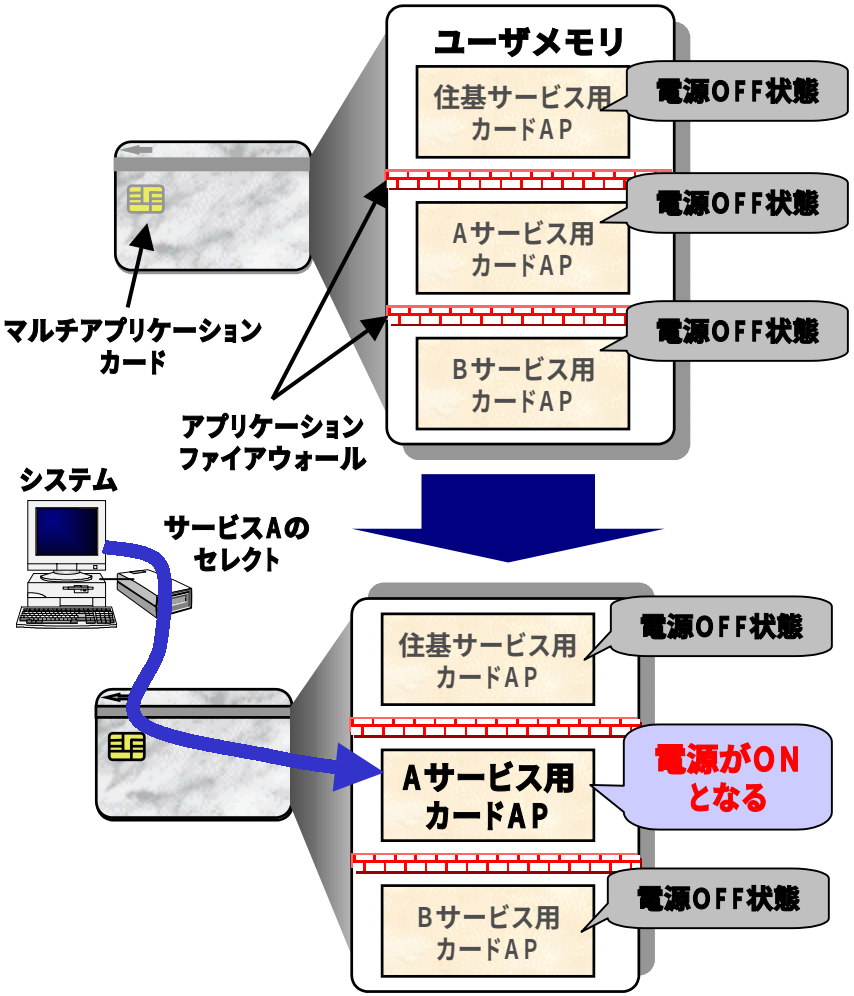
### アプリケーションファイアウォール

- 情報を設定された各カードアプリケーション間は、「アプリケーションファイアウォール」により、カード内でそれぞれ独立している。
  - 属性制御方式：属性情報に従ってメモリへのアクセス許可する方式（属性情報=読み出し専用／読み書き可能／実行可能／アクセス不可などの属性を表す）。
  - ページ管理方式：ページ番号＋論理アドレスでアクセス許可を行う方式（ページ=メモリ上でのAPの論理的配置を表す単位）。
  - 仮想マシン方式：仮想マシンがAPのプログラムを解釈実行する方式（仮想マシン=Java-VMなどにより実現されるアプリケーション実行環境）。

# 住民基本台帳カード

## アプリケーションファイアウォールの仕組み

### 属性制御方式の例




**★カードAP**

セレクトされるまでは、すべてのカードAPが電源ＯＦＦの状態

**★カードマネージャ*によるカードAPのセレクト**

該当カードAPのスイッチを入れ、電源をONする操作に相当
（カードAPを複数同時に電源ONできない）

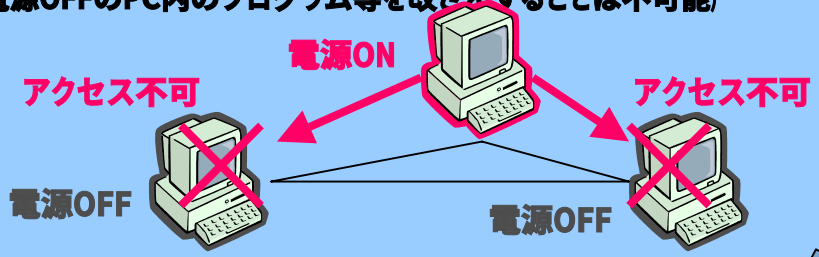
**★アプリケーションファイアウォール機能の実現イメージ**

カードAPをセレクト前は、電源が入っていないので、カードAPに不正にアクセスすることは不可能。
カードＡＰセレクト後も、該当AP以外は電源が入っていないので、不正アクセスは不可能。

*カードマネージャ
カードAPのセレクト等の管理を行うプログラム。
ICチップに焼込まれており、改ざん等は不可能。

**◆不正アクセスのイメージ：**

PCがネットワーク接続されている場合、電源ONのPCから電源OFFのPCにアクセスしても無応答となる。
（電源OFFのPC内のプログラム等を改ざんすることは不可能）



# 住民基本台帳カード

## 耐タンパー性（1）

■ICカードのICチップは、偽造を目的としてカード内の情報を読み出そうとする各種の不正行為に対し、チップ自身が防御する対策を有している。

**ＩＣチップ自身が有する偽造目的の不正防止策を**

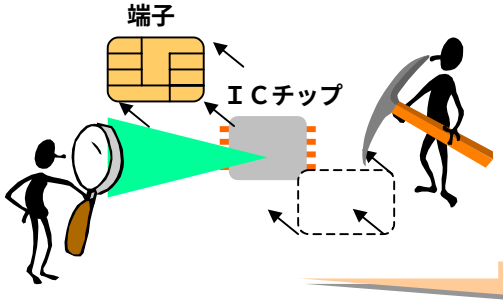
**「耐タンパー性」という。**

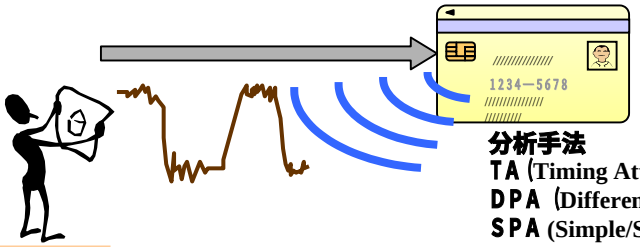
タンパー（tamper）：干渉する;いじくる,いたずらする, 勝手に変えるの意

**主な不正行為**

①ＩＣチップをカードから取り出し、端子をあてる信号検出などの電気的解析あるいは顕微鏡による観察など物理的解析を行ないカード内情報を不正に読み出す。

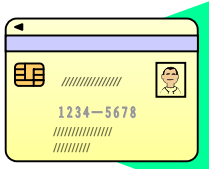
②ＩＣチップの行なう処理によって変化する電力消費量や処理時間等を測定し、統計的に解析することでカード内の情報を推測する。（信号統計解析）




**分析手法**
**ＴＡ（Timing Attack）**
**ＤＰＡ（Differential Power Analysis）**
**ＳＰＡ（Simple/Static Power Analysis）**
**DFA(Differential Fault Analysis)**
**など**

**これら攻撃は以下のような「耐タンパー性」機構により守られる。**



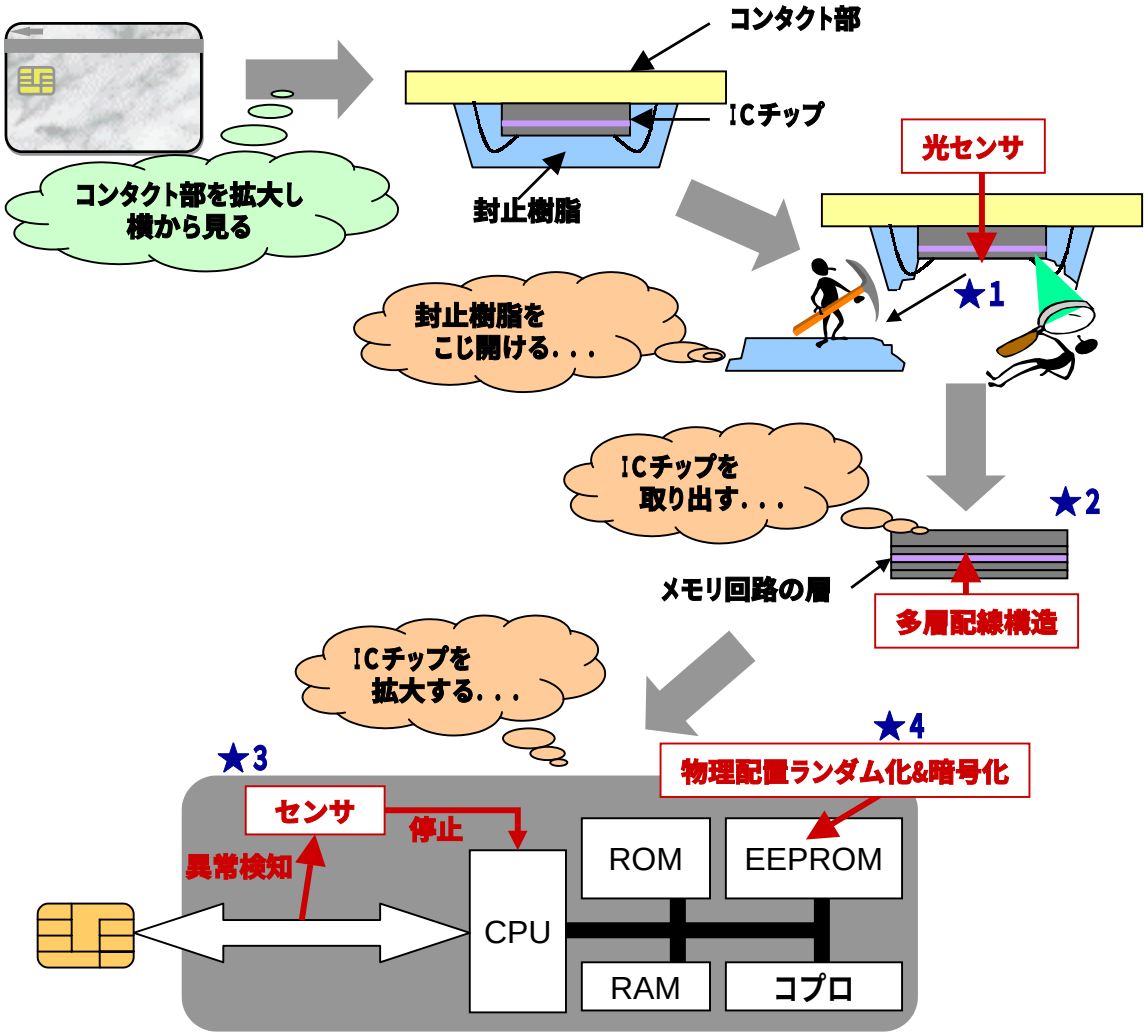

①に対しては…
- チップ取り出し困難なカード構造（こじ開け時は破損する等）の採用
- チップ内の多層化、ダミー回路形成などによる物理的解析の困難化
- 異常検出センサなどによる電気的解析の困難化

②に対しては…
- 回路の冗長な駆動による消費電力、処理時間を攪拌（均一化or不均一化）などによる信号統計解析の困難化。

# 住民基本台帳カード

## 耐タンパー性（2）

### 物理的解析方法と対策（例）




★1：光が当たるとメモリ内容が消去する

★2：多層配線技術により、メモリ回路素子が表面から観察できない。

★3：センサにより電圧異常、クロック異常等を検知すると、動作が停止する。

★4：メモリ素子の物理配置ランダム化&暗号化により、解読不可。