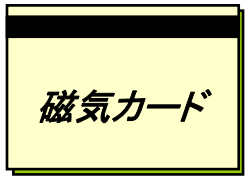
資料　２

住基カードのセキュリティについて

住基カード（ICカード）の特徴等について

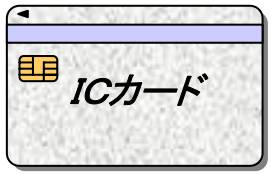
磁気カードとICカードとの比較



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

住基カード（ICカード）の特徴

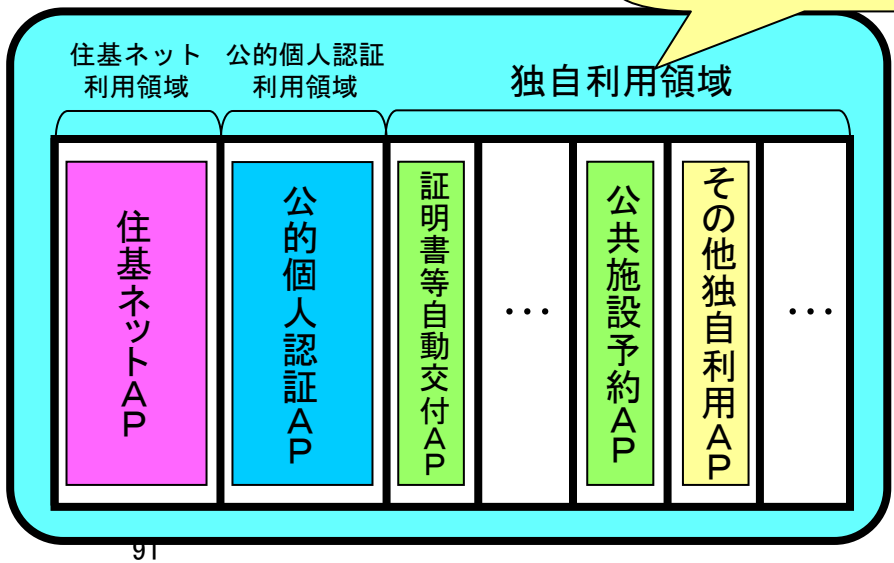
１枚のカードを複数目的に利用
多目的利用（マルチアプリケーション）

主としてキーデバイスの役割（※）
（データベースにアクセスするための認証・暗号化機能）

※データキャリーとしての活用も可能
（データベースとしての情報蓄積機能）

【住基カード（ICカード）のイメージ】

条例により市町村が提供するサービスに利用することが可能な領域。

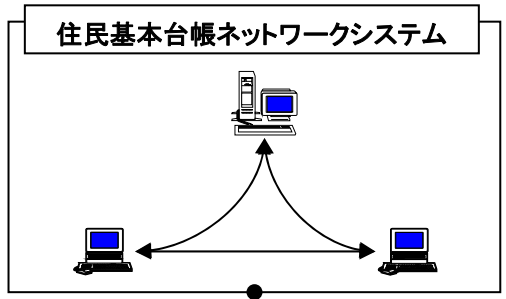


住基カードとその他のICカードの特徴について

住基カードICとその他のICカードとの比較

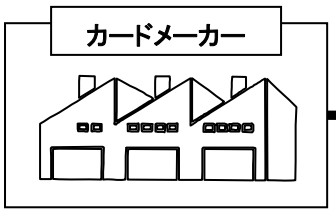
分　類		概要	我が国における実用化動向
接触型		• ISO/IEC 7816準拠	• クレジットカード仕様（EMV仕様） • 全銀協ICキャッシュカード
非接触型 （近接型）	タイプA	• ISO/IEC 14443準拠	• NTT ICテレカ
	タイプB	• ISO/IEC 14443準拠	• 住民基本台帳カード • IC旅券 • 運転免許証ICカード • 国家公務員身分証ICカード
	FeliCa	• ソニーが開発	• JR東日本Suica • 電子マネーEdy

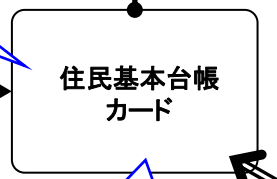
住民基本台帳カードのセキュリティ対策



相互認証：暗号ｱﾙｺﾞﾘｽﾞ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
（総務省告示案第2.2 (2)）

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
（総務省告示案第2.3）



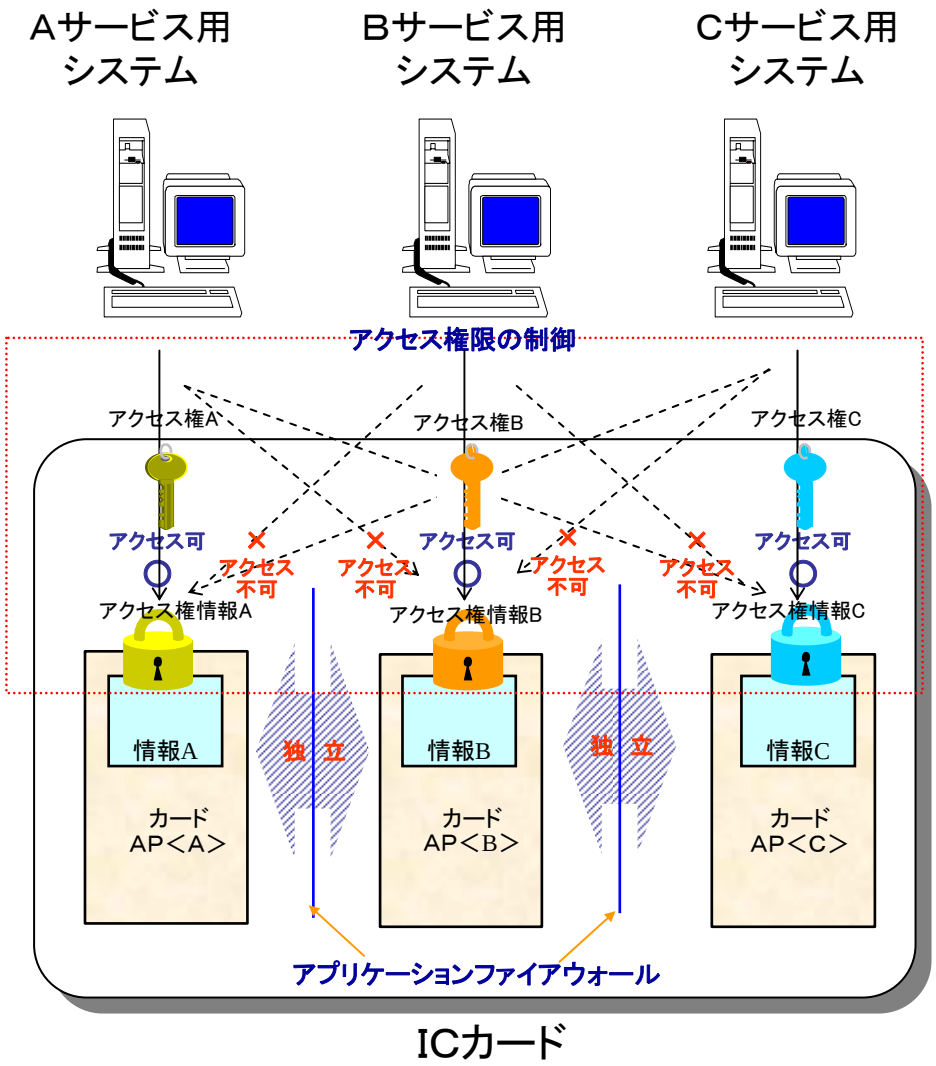


暗証番号
：利用者の暗証番号をカードに送信／照合することによりカードと利用者の結びつきを確認
（総務省告示案第2.2 (1)、第3.1 (2) エ）

輸送鍵：正しいカード発行者のみが解くことが出来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
（総務省告示案第2.2 (2)、第3.1 (1)）

・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
（総務省告示案第2.2 (3)、第3.1 (2) イ）
・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
（総務省告示案第2.2 (5)、第4.2）
・耐タンパー性：物理的/論理的攻撃に対するICﾁｯﾌﾟによる防御対策
（総務省告示案第2.2 (4)）

アクセス権限の制御及び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。

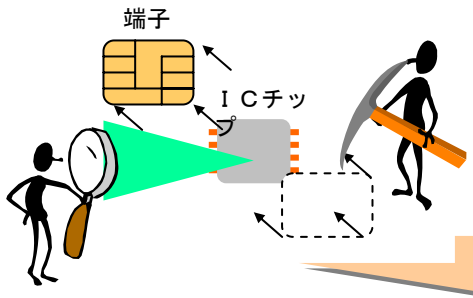
アプリケーションファイアウォール

- 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。

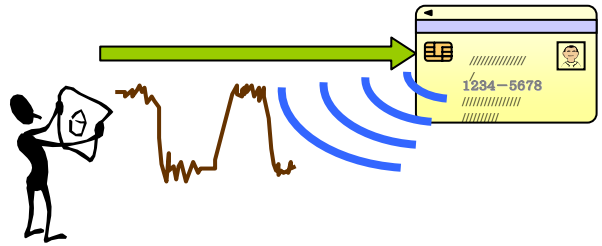
耐タンパー性の概要（１）

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。

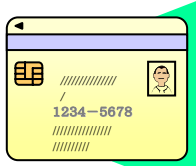
①チップ解析（物理的攻撃）



②信号統計解析（論理的攻撃）



これらの攻撃からは、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。

耐タンパー性の概要（２）

■物理的解析方法と対策（例）