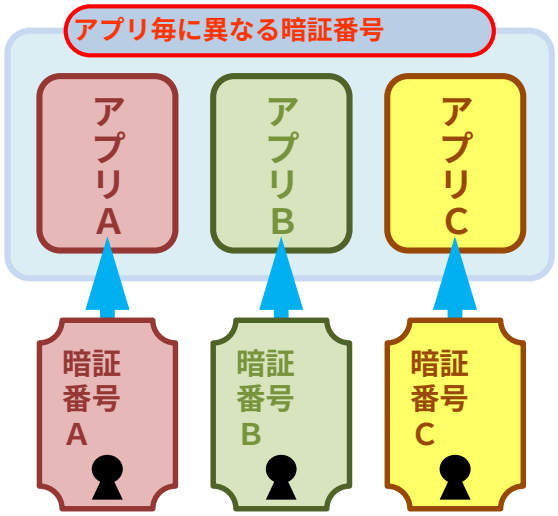
マイナンバーカードのセキュリティー（ICチップ）

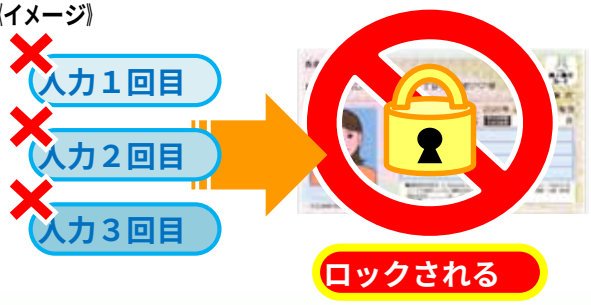
暗証番号

■ アプリケーション毎に異なる暗証番号を設定し情報を保護



■ 暗証番号の入力を一定回数以上間違うとカードがロックされる

《イメージ》



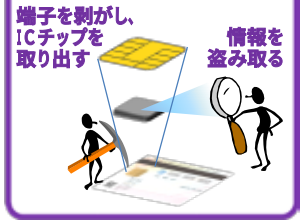
耐タンパー性

■ ＩＣチップは偽造を目的とした不正行為に対する **耐タンパー性** を有する

※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

偽造目的の主な不正行為

① ICチップを取り出し、電気的または物理的に情報を不正に読み出す



② ICチップの電力消費量や処理時間等を測定・解析し、情報を推測

個人番号カードのＩＣチップは、①と②の両方に対抗できる

①に対して

- 光が当たるとメモリ内容消去
- メモリ回路素子が表面から観察できない
- 電圧異常、クロック異常等の検知で動作停止
- 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

②に対して

消費電力、処理時間をかくはんすることで、読み取った信号の統計的な解析を困難にする

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を設定

■ アプリケーション開発者も、アクセス権が条件を満たさないとアクセスできない

■ 情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、それぞれ独立して相互にアクセス出来ない

ＩＳＯ/ＩＥＣ１５４０８認証

■ セキュリティ機能評価の国際標準の認証を取得

●ＩＳＯ/ＩＥＣ１５４０８認証とは

- コンピュータシステムや製品のセキュリティ機能の評価を行うための基準であるＣＣ（Common Criteria）の国際標準
- スマートカードが必要とするセキュリティの要件を記述
- スマートカードの製品調達者は、ＣＣに基づき、Protection Profile（利用者のセキュリティ要件を記述した要件仕様書）を作成
- 評価機関が課程を評価し、認証機関が認証