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

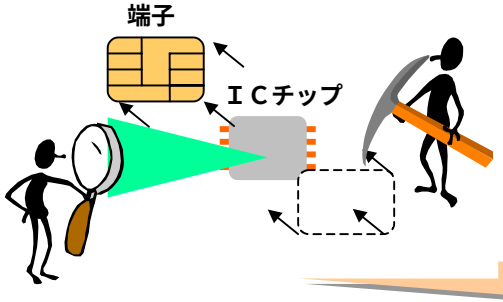
「耐タンパー性」という。

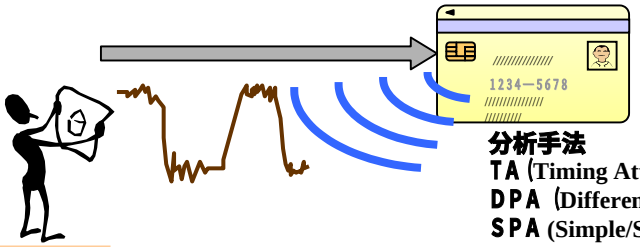
タンパー（tamper）：干渉する;いじくる,いたずらする, 勝手に変えるの意

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。

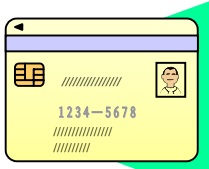
②ＩＣチップの行なう処理によって変化する電力消費量や処理時間等を測定し、統計的に解析することでカード内の情報を推測する。（信号統計解析）





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。



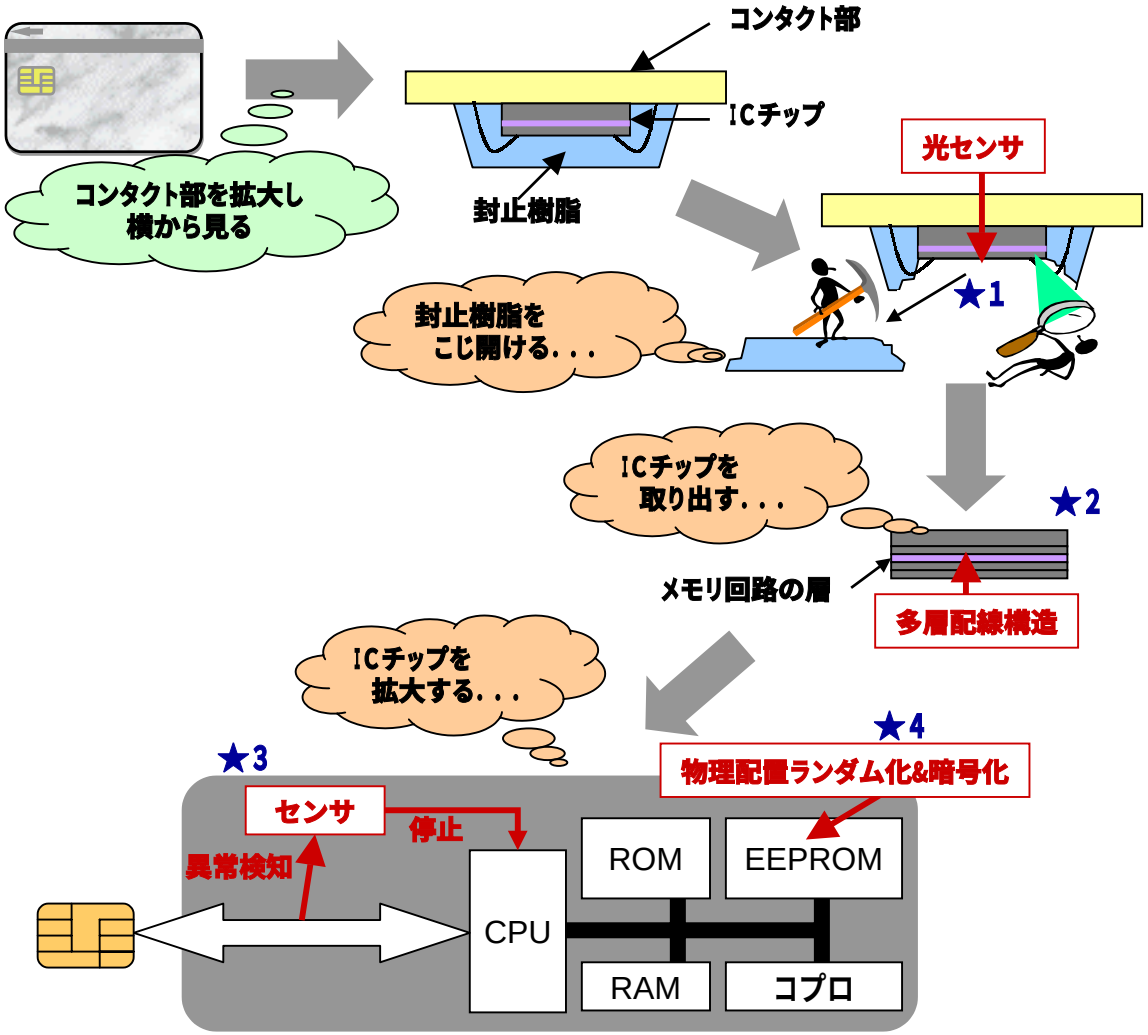
①に対しては…
- チップ取り出し困難なカード構造（こじ開け時は破損する等）の採用
- チップ内の多層化、ダミー回路形成などによる物理的解析の困難化
- 異常検出センサなどによる電気的解析の困難化

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。