組み込み機器は要注意！アルゴリズムだけじゃ安全じゃない!?

研究最先端！

マイコンの消費電力解析による暗号解読

前編

実験！解読の原理

堀 洋平，片下 敏宏

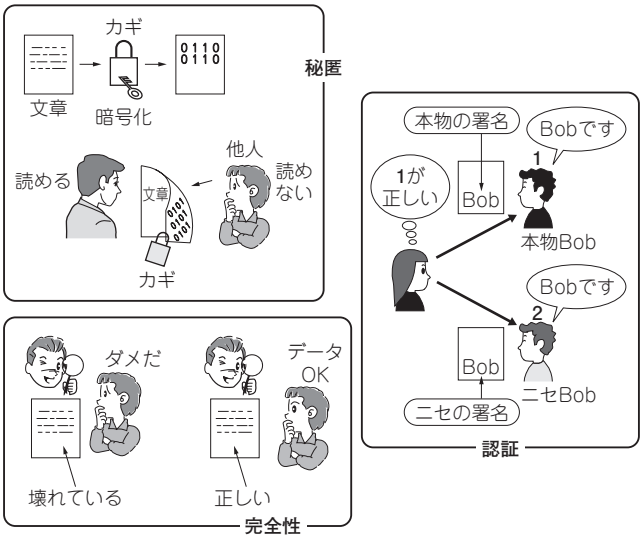

図1　暗号技術の主な用途

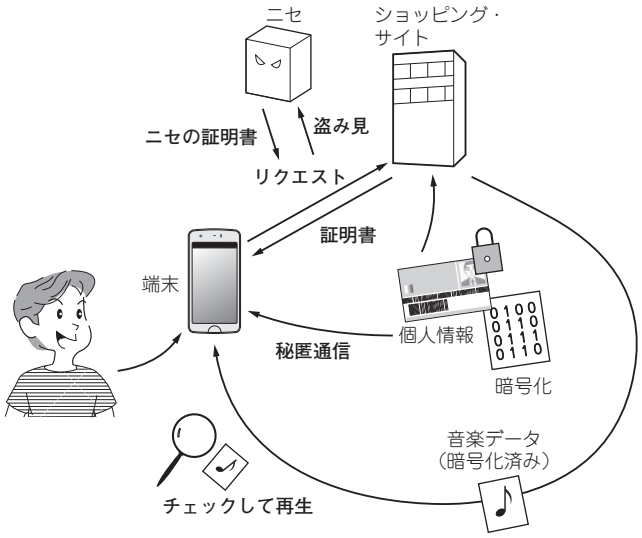

図2　暗号技術は身近に使われている！

近年のマイクロプロセッサでは，機器の認証や情報の保護などの目的で，暗号技術を利用することがあります．

暗号には理論的な評価がなされた安全なアルゴリズムを用いますが，実はそれだけでは十分ではありません．

単純な暗号プログラムでは，マイクロプロセッサの消費電力や電磁波から暗号が解読されてしまう恐れがあります．物理現象からの情報漏えいにも注意しないといけなくなってきています．

そこで本稿では，一般的なマイクロプロセッサの消費電力や電磁波から情報が漏れてしまう原理や，暗号が解析される例を説明し，対策方針を紹介します．

ますます高まる！暗号技術の必要性

● 身近にすでに使われている！暗号技術

マイクロプロセッサが高性能になり，用途が拡大するとともに，**図1**のようなさまざまな用途で暗号技術が利用されています．

- 秘匿：情報を他人に知られないようにする
- 完全性：情報の改ざんや破損の検出
- 認証／否認防止：機器の認証　など

例えば，スマートフォンで音楽データを購入する場合，ショッピング・サイトを認証し，個人情報の通信が暗号化され，購入したデータが破損していないか確認します（**図2**）．暗号技術は身近ですでに使われるようになっています．

● どれだけ当たり前になってきたか…パソコン用CPUには暗号演算専用ハードが！

セキュリティを保つために，より高速な処理が求められるようになり，暗号専用の演算器を搭載したマイクロプロセッサも登場しています．普段私たちが利用しているコンピュータにも暗号機能（例：インテル社AES-NI命令）が追加されるようになっています．