第2章

サイドチャネル攻撃のからくりを理解する

―― DESとRSAに対する攻撃と基本的な防御法

佐藤 証

ここでは，正規の経路以外から暗号LSIの内部情報を読み取るサイドチャネル攻撃のしくみを解説する．具体例として，公開かぎ暗号のRSAと共通かぎ暗号のDES（Data Encryption Standard）を取り上げる．暗号アルゴリズムの特徴や回路の実装方法に応じて攻撃のしかたは異なる．攻撃法を理解しておけば，有効な対策を打つ際の手がかりになる．（編集部）

暗号LSIモジュールへの攻撃法にはさまざまな種類がありますが，**図1**に示すように，大きく「破壊攻撃」と「非破壊攻撃」に分類できます．

破壊攻撃は，特別な装置を備えた実験室において，LSIのパッケージを開けて行います．回路パターンを解析して回路図を起こしたり，直接メモリの内容を読み出したり（あるいはメモリに書き込んだり），さらにはLSIの中の配線をつなぎ変えるといった芸当すら可能です．しかし，こうした破壊攻撃は非常に高価な装置と高いスキルが要求されるため，個人レベルでは実行不可能です．

これに対して，非破壊攻撃は内部動作に応じて変化する電流や電圧，電磁波，処理時間などを観測します．対策が施されていない回路は，オシロスコープやパソコンといった簡単な設備で攻撃できます．サイドチャネル攻撃は，この非破壊攻撃に分類されます．

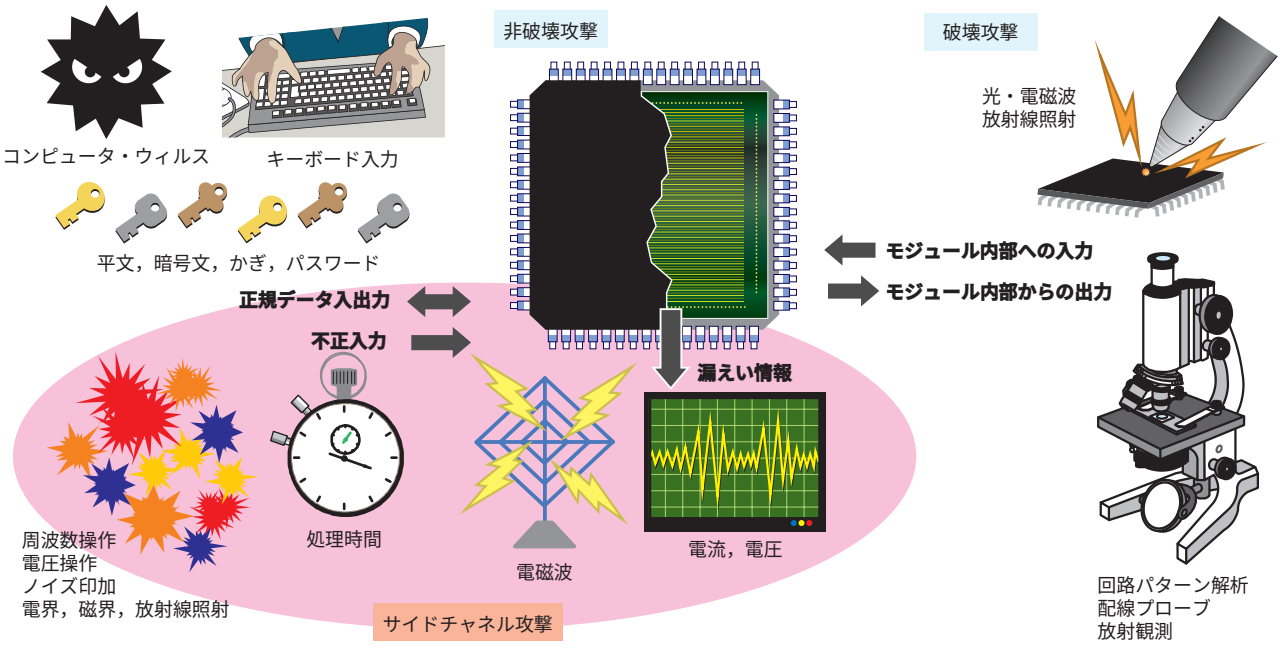

図1　暗号LSIモジュールへのさまざまな攻撃法
サイドチャネル攻撃は非破壊攻撃に分類される．これは，正規の入出力以外のチャネルを通じて観測されたデータをもとに秘密情報を解析する手法である．

● 情報を正規の経路以外から取り出す

サイドチャネルとは，正規の入出力経路ではないことを意味しています．つまり，サイドチャネル攻撃はそうした経路から観測できるあらゆる情報を使って，LSIの内部のデータを読み取ろうとするものです．ただし，キーボードやテンキーの状態を監視して，暗号LSIを始動させるためのパスワードやピンを割り出すというのは範囲外です．あくまでも，LSI内部にある秘密情報を取り出すというのが攻撃の目的です．

また，サイドチャネル攻撃では，正規のデータ入出力にほかの観測情報を組み合わせて解析を行います．このとき，統計処理が行いやすいように入力データのパターンを1ビットずつ変えたり，LSIに与える電圧や動作周波数を変えたり，あるいはスパイク・ノイズを電源へ印加したり，電子ビームを照射することによって計算を誤らせてかぎ情報の漏えいをねらうといった手法もあります．

RSA暗号を作った3人のうちのひとりであるShamirは，米国Intel社のCeleronプロセッサにRSA暗号ソフトウェアを実装し，秘密かぎごとに発生する音が異なることを利用した音響攻撃を示しています[(1)]．この音は，LSIの発熱によって生じます．**図2**に示すように，スプレーによる冷却という不正入力(？)で音のスペクトルが変化するようすがわかります．

サイドチャネル攻撃の研究は，公開かぎ暗号の処理時間が秘密かぎのビット・パターンによって異なることを利用する解析手法[(2)]を，1996年にKocherが提案したのが始まりです．それからまだ10年しかたっていませんが，解析や防御手法の研究はますます活発に行われています．

以下に，その中でもっとも基本的な二つの攻撃法を説明します．一つは単純電力解析(SPA：simple power analysis)，もう一つは差分電力解析(DPA：differential power analysis)です．これらを，RSAとDESの二つの暗号に対して適用する例を挙げます．

1 RSAをSPAで攻撃する

RSAは公開かぎ暗号の代表とも言えるもので，暗号化と復号に異なるかぎを用います．xを元のデータ(平文と言う)，yを暗号文，eとnを暗号化かぎ，dを復号かぎとするとき，暗号化と復号は次のような簡単なべき乗剰余算の式で表されます(a mod bは，aをbで割った余りを意味する)．

暗号化：$y = x^e \bmod n$ ……(1)
復号　：$x = y^d \bmod n$ ……(2)

かぎの作りかたは専門書に譲るとして，まずは簡単な例を示しましょう．平文を$x = 2$，暗号化かぎを$e = 9$，$n = 69$，復号かぎを$d = 49$とします．式(1)から暗号文は29($= 2^9 \bmod 69$)となります．これを式(2)に当てはめると，$x = 2$($= 29^{49} \bmod 69$)となり，平文2と暗号文29の相互変換がべき乗剰余算で確かにできていることがわかります．試しに，暗号文29を暗号化かぎで変換しても$29^9 \bmod 69 = 62$となり，平文(この場合は2)に戻すことはできません．

この暗号化かぎはだれに渡してもよいため，公開かぎ(public key)と呼ばれます．これが公開かぎ暗号の名まえの由来です．また，復号かぎは秘密かぎ(private key)と

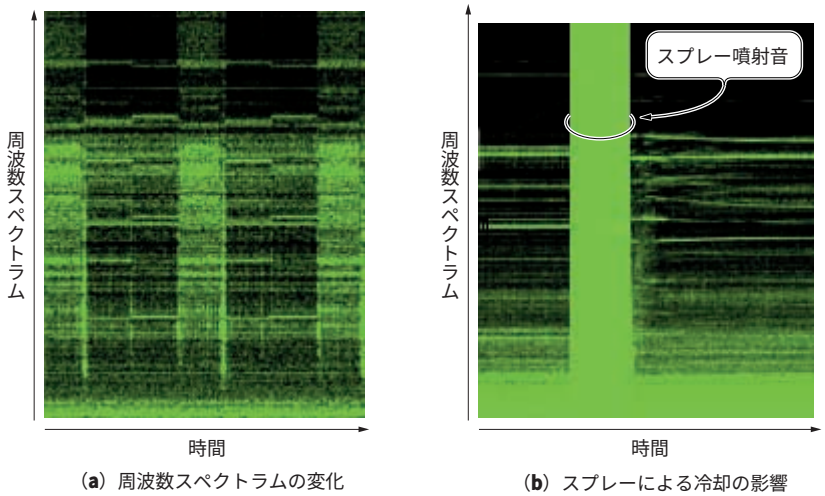

図2
Shamirの音響攻撃による観測波形
図は，RSA暗号ソフトウェアをCeleronプロセッサに実装し，動作中にプロセッサが発生する音の周波数を横軸に，時間を縦軸にとってグラフ化したもの．(a)では演算処理に応じてスペクトラムが変化するようすがわかる．プロセッサの発熱によって音が生じるため，スプレーで冷却すると，(b)のようにスペクトラムが変化する．