サセボ・個体差調査（第2群）　室温変動の影響（横国大）

2008.07.29

CMOSの消費電力は，静的消費電力と動的消費電力に分けることができる（図1）．

・静的消費電力：トランジスタが動作しなくても定常的に流れるリーク電流によって発生する．リーク電流は接合温度と正の相関があり，温度が上昇するとリーク電流も増加する．
・動的消費電力：トランジスタが動作したときに発生する貫通電流および充放電流からなる．

サイドチャネル攻撃で利用するのは，もっぱら動的消費電力の変動であるが，データ測定の際には静的消費電力についても確認しておくべきと考え，第2群50枚の測定データを分析した．

図2に，ボード1枚（G51）の波形データの電圧平均値を縦軸に，測定時刻を横軸にしてプロットした．室温変動（空調の動作）により20分～25分程のサイクルで数mVの変動が見られる．

図3は，50枚全部について，平均電圧の様子を測定日ごとに分けて表示したものである．電圧平均値はボードごとに異なるが，各日のラインに合わせてある．赤色が図2のデータである．

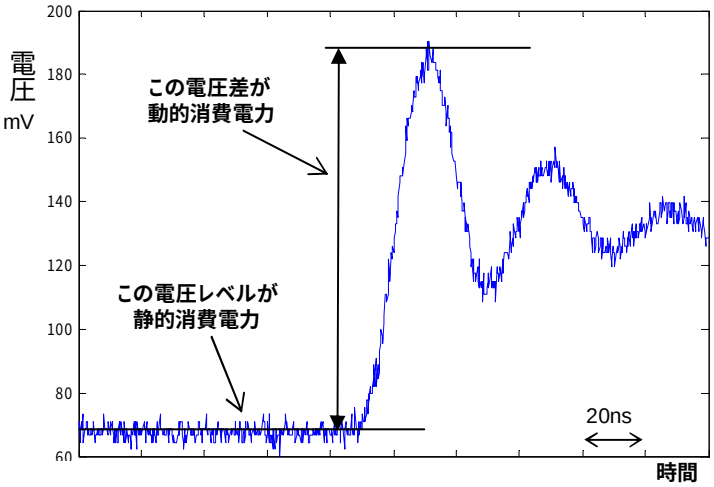

図1：AES動作時の電圧変動の例

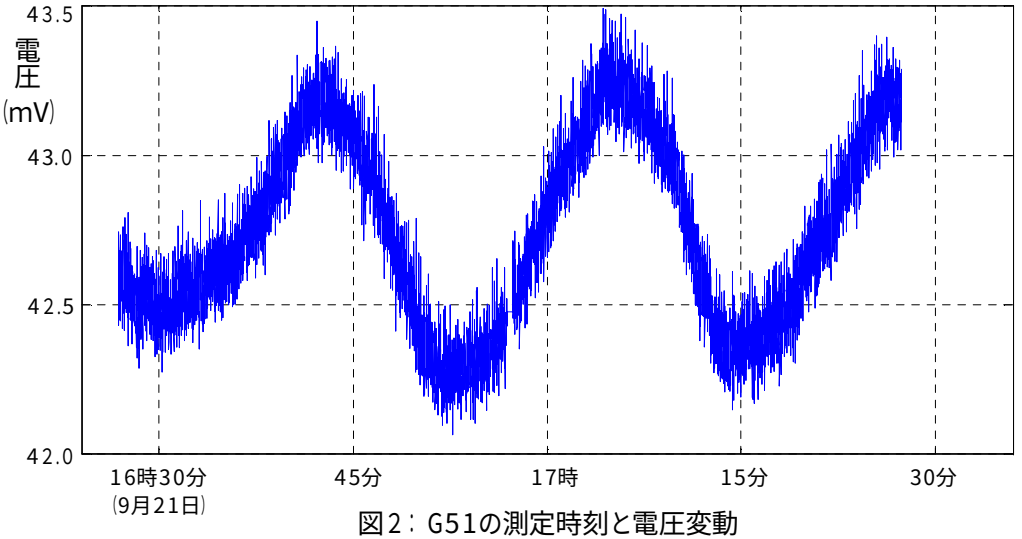

図2：G51の測定時刻と電圧変動

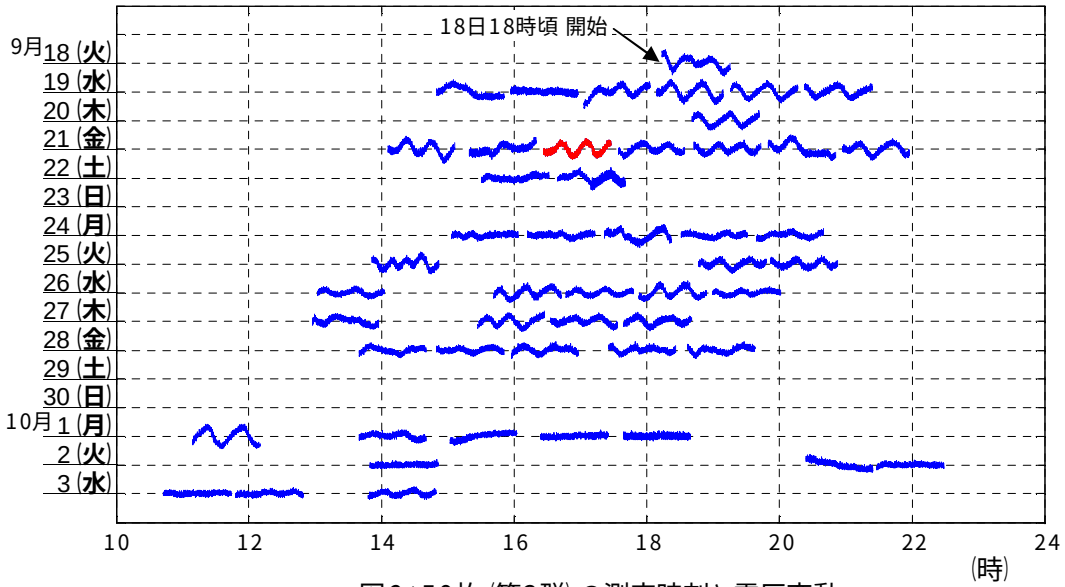

図3：50枚（第2群）の測定時刻と電圧変動