サセボ・個体差調査（第2群）　データ分析の経過報告（横国大）

2007.10.11

個体差調査・第2群で測定した50枚分のAES11の波形データに対して，CPAを実施した．図1に結果のグラフを示す．

図1のグラフからは，ボードにより差異があるとは言えず，どのボードでもほぼ同じ結果が得られている．

第2群では，シャント用抵抗のバラツキの影響を排除するために，同一の抵抗を差し替えて測定した．その結果，電圧波形は50枚のどのボードでもほぼ同一の形状になった（図2）．また，中間データのハミング距離との相関係数もボードによらず，ほぼ同一の値になった（図4）．

なお，第1群と同様に標準搭載のシャント抵抗で測定した場合には，図3のように第2群の50枚も4グループに分かれる．

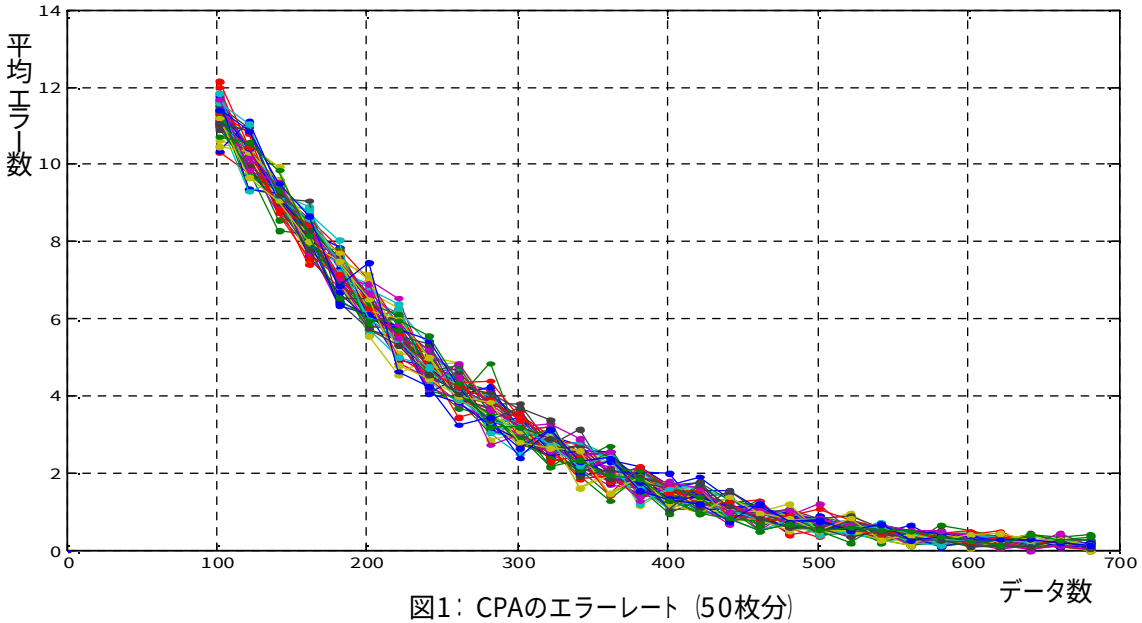

図1：CPAのエラーレート（50枚分）

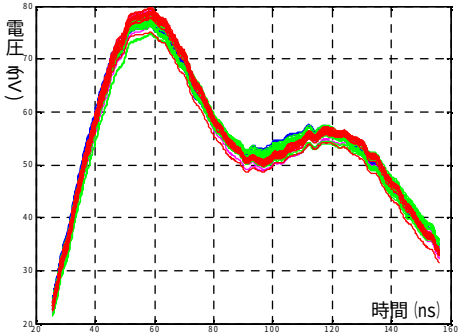

図2：AES動作時の電圧波形の移動平均（50枚分）

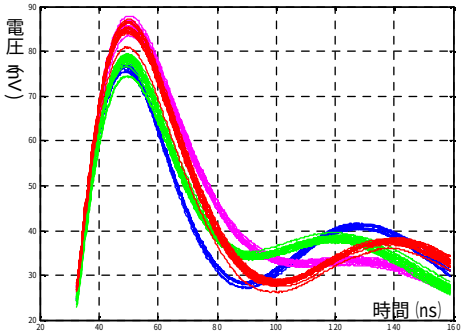

図3：AES動作時の電圧波形の移動平均（50枚分）

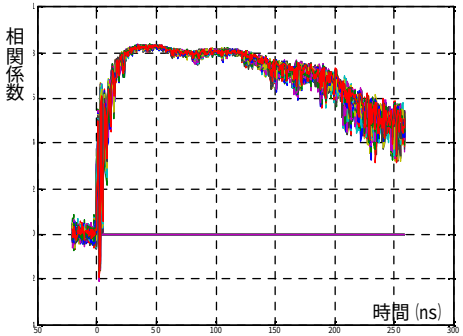

図4：ハミング距離との相関係数（50枚分）