

リバースエンジニアリングからみえるもの

リバースエンジニアリングの守備範囲（その2）

植木正雄

時代はいまやシステムLSI。携帯電話などデジタル民生機器には最先端の高機能システムLSIが搭載されている。これらの最新デバイスを一般市場で入手するには、最終製品を購入する以外、手立てはない。一般の物流ルートに乗ることは稀であるからだ。チップワークスでは、最終製品を購入すると、まずその分解調査を行う。筐体、基板などを写真撮影し、使用されているデバイスや電子部品を記録する。必要に応じてプリント基板を分析し、デバイス間接続の配線図を作成する（図1）。

システム解析では、心臓部であるシステムLSIとメモリデバイスを中心とした実装基板上の信号の入出力を電氣的に計測、分析して、システム全体の動きを探る。もちろん、システムLSIそのものの内部回路をすべて解析できれば、全体の動作を完全に解明できる。しかし、フル回路解析には極めて多額の費用がかかるため、その実施は難しい場合が多い。数千万円から数億円になり得るからだ。代替手段として、システム解析が有効となる。

システム解析の対象はデジタル民生機器に限らない。電子機器であれば、民生用以外にもあらゆる分野で対応が可能だ。解析対象によって解析の難易度もまったく異なってくる。最近、チップワークスが実施したシステム解析の実例を2点紹介しよう。一つはデジタルカメラ、もう一つはゲーム機である。デジタルカメラの解析プロジェクトでは、自動焦点機能がどのような制御技術で実現されているかを確認する目的であった。同一モデルのカメラを複数、分解し、筐体の一部から実装基板を露出させた形で正常に機能する実験用カメラを製作する。そして実装基板にインターフェースとロジックアナライザを接続して、テストプログラムで動作させる環境を用意する。その上で、カメラの自動焦点制御の動作タイミングを測定し、所望の機能がどのように実現されているかを調査した。図2は解析時の様子を示したものである。

ゲーム機の解析例では、動画データのビデオメモリへの読み書きがどのように制御されているかを調査した。所期の目的を達成するには半導体メモリに組み込まれて

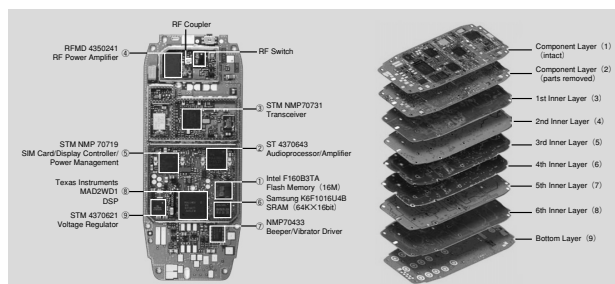


図1 携帯電話の分解調査例（Nokia製携帯電話で使用されているデバイス間の配線レイアウトを調査し、配線図を作成）

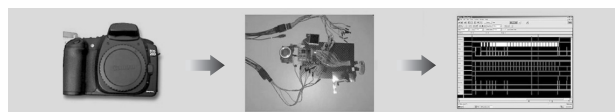


図2 デジタルカメラ・システム解析例（カメラの自動焦点制御の動作タイミングを測定している様子）

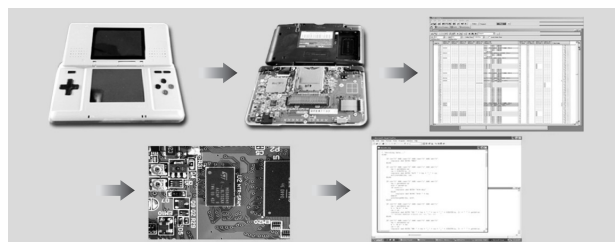


図3 ゲーム機解析例（動画データがビデオメモリにどのように読み書きされているかを調査したときの様子）

いるOSをリバースエンジニア解析するのが最善であったが、これには多額の費用がかかる。それを避けるべく、実機上でのアプリ動作時の信号の入出力を分析した上で、新たに製作したテストプログラムを走らせてビデオメモリへのアクセス動作を究明した（図3）。このように、システム解析は工夫次第で色々な場面でコスト効果的な解析を提供することが可能だ。



CHIPWORKS

植木正雄 / チップワークス代表取締役社長

同社 URL <http://www.chipworks.co.jp/>

お問合せ先 info@chipworks.co.jp