

リバースエンジニアリングからみえるもの

組込みソフトウェア解析（その2）

植木正雄

ChipWorksでは、組込みソフトウェア解析業務を特許侵害を突き止める目的に限って受託している。メモリに格納されているソフトウェアの抽出、分析作業は違法行為として解釈されやすい。リバースエンジニアリングを正業として展開する当社にとってはソフトウェアのリバースエンジニアリング解析能力を特許侵害調査目的に限定使用することで合法性を確保している。

特許侵害調査としての組込みソフトウェア解析では、当該システムの特典機能を制御しているアルゴリズムについて特許請求項目との関係を、リバースエンジニアリング技術を活用して調査する。侵害調査方法は大きく、①当該ソフトウェアそのものの解析による立証、②システム動作試験に基づく機能解析による立証の2通りある。

一つ目のソフトウェア解析の場合、ソースコードが入手できれば解析は容易になる。システム内のメモリから抽出せずに別の方法でオリジナルを入手できるのであればそれにこしたことはない。しかし、特許侵害調査では、初めから与えられることはまずない。この場合、当該メモリからバイナリ形式で格納されている解析対象プログラムを抽出する必要がある。抽出されたオブジェクトコードはそのままでは解釈不可能なため、これを逆アセンブルや逆コンパイルして、読解可能なアセンブリ言語や高級プログラミング言語で記述されたソースコードに変換する。そのプログラム・フローを分析して、特許技術が侵害されているか否かを解釈することとなる（図1）。

しかし、このソフトウェア解析は、実際には解析に必要な多くの条件が揃わないと実現が難しい。まず、当該システムで使用されているアーキテクチャが一般に普及しているプラットフォームであることが望ましい。そうではない場合には、当該プロセッサの開発ツールが利用できる環境が必要となる。さらに、ソースコードのファイルが大きく複雑であることが多い上に、変換後のソースコードが元のソースコードの完全な再現には至らないため、解析対象となるプログラム部分を探し出すことが困難な場合が多い。このように技術的な制約が多いこと

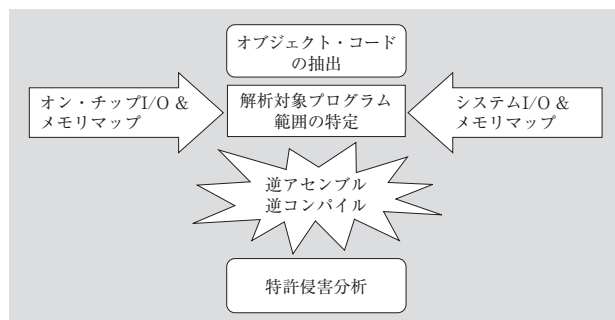


図1 組込みソフトウェア解析手順

から、ソフトウェア解析が成功する可能性は限定的である。それでも、公知のプラットフォームが使用されている、抽出、分析するプログラムサイズが比較的小さければ、この方法は正攻法として大きな威力を発揮する。

二つ目のシステム動作試験に基づく機能解析は、上述のソフトウェア解析が多くの制約ゆえに実施不可能な場合に行う代替策といえる。しかし、実際にはこの方法を取らざるを得ないケースのほうが多い。機能解析では100%侵害を立証することは難しいが、実践的かつ有力な手段として広く活用されている。

一例として、ファームウェアの更新のためのアルゴリズムがある。これはコンピュータ制御された多くの装置に共通の機能として広く採用されている。不揮発性メモリがメモリコントローラの外部にある場合、ファームウェア更新時にデータバス上の信号動作をモニタすることで、特許で開示されたアルゴリズムが当該デバイスで使用されているか否かを示すことができる。機能解析結果に基づく証拠資料で交渉を進めておき、訴訟に発展したときにディスカバリ（米国訴訟の場合）でソースコードの開示を求めることも可能になる。



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