第1章

基本的な使い方からハードウェアの故障状態の作成まで

Web

エミュレータQEMUの概要とLinuxの起動，テストのための改造

辻 邦彦，小林 哲之，若槻 俊宏

さまざまなCPUアーキテクチャをエミュレートできるオープン・ソース・ソフトウェアQEMUを使ってLinuxの起動までを行う．また，エミュレータの利点として，改造の簡単さがある．これにより，ハードウェアの故障状態を作成して，エラー処理ルーチンが正常に作動するかどうかをテストすることができる．これは実機では難しい，エミュレータならではの利点だ．その方法についても解説する．（編集部）

第1部：基本編

1 QEMUとは？

QEMU[注1]は，さまざまなマシン（コンピュータ）の仮想化とエミュレーションを実現する，オープン・ソース・ソフトウェアです．Quick EMUlatorの略で，筆者はそのまま「キューイーエムユー」か，「キューエム」と発音しています．1台のパソコンの上で，仮想化して複数のパソコンを動作させたり，ARM社のRealView開発ボードのようにアーキテクチャが全く異なるマシンをエミュレートすることができます．

QEMUは2003年，Fabrice Bellard氏のTiny C Compilerプロジェクトから派生する形で開発が開始されました[注2]．もともとは，x86 Linux用のアプリケーション（バイナリ・ファイル）を，PowerPCなどの非x86 Linux上でそのまま実行できるようにするツールで，当時の目標は非x86アーキテクチャ上でWineプロジェクト[注3]を動作させることだったようです．

その後，コミュニティ・ベースで活発に開発が進められ，現在では14のアーキテクチャをサポートする汎用のプラットホームに成長し，2011年12月1日には待望のバージョン1.0がリリースされました．QEMU全体のライセンスはGNU GPL version 2ですが，個別のソース・ファイルはGPL，LGPL，修正BSDL（MITライセンス）などが混在しています．

QEMUはさまざまな目的に利用できますが，本稿では組み込みソフトウェア開発への応用を中心に解説します．また，QEMUは多様なホスト・マシン上で，さまざまなターゲット・マシンをエミュレートできますが，本稿では一般的なx86パソコン上で，ARMアーキテクチャのエミュレーションを解説します．

Column 1 「エミュレータ」という言葉について

組み込みの世界で「エミュレータ」というと，ICE（In-Circuit Emulator）に代表されるような，ハードウェアに別のハードウェアのふりをさせる技術（多くはリアルタイム性が重要になるため，専用のハードウェアが必要）を指すことが多いのですが，本稿では「別のシステムのふりをするシステム（ソフトウェアかハードウェアかは問わない）」という広い意味で使用しています．

エミュレーションは仮想化技術の一部で，QEMUの（準）仮想化機能は，一つの実マシン（例えばパソコン）を仮想化して，複数あるように見せかけることができます．これは，同じく仮想化ソフトウェアであるXen（http://xen.org/）や，Linux KernelのKVM（Kernel-based Virtual Machine）にも利用されている興味深い技術ですが，本稿では扱いません．

注1：http://wiki.qemu.org/
注2：[Tinycc-devel] [announce] QEMU x86 emulator version 0.1, http://lists.gnu.org/archive/html/tinycc-devel/2003-03/msg00084.html
注3：オープン・ソースのWindows API実装で，Microsoft Windowsのアプリケーションをx86 Linuxなどの上で動作させることができる．http://www.winehq.org/