Ｃ言語ＳＭ差分ファイル自動生成による高級言語レベルパッチ作成システム*

久保田　賢治†
日本電気通信システム株式会社†

はじめに

アプリケーションソフトウェア開発においてソースコードレベルでのパッチファイル生成を支援するツール『パッチ支援システム』を開発しました。

本稿では、パッチ支援システムの機能や特徴について紹介します。

１．パッチ支援システムとは

パッチとは、問題のあったターゲットメモリの修正を部分的に行うことをいいます。従来、パッチを実現するためには、修正箇所のメモリイメージを持ったパッチファイルを生成し、それをターゲットにダウンロードすることで実現していました。しかし、パッチファイルを生成するためには高級言語の知識だけでなく、アセンブリ言語、機械語の知識やターゲットマシンのメモリ構造の把握等、専門的な知識が必要であることが一般的でした。

本システムでは、パッチファイルを高級言語（Ｃ言語）から自動で生成することができるため、パッチファイル生成のための専門的な知識がなくても簡単に生成することが可能です。

２．パッチファイルの生成方法

パッチ支援システムは、大きく分けて 2 つの機能に分かれます。1 つは、問題のあった修正前のソースコードとそれを修正したソースコードを入力して差分となる関数や外部変数を差分 OM（パッチ OM）として抽出する「SM 分割」、もう 1 つは、その差分 OM をリンクしてパッチファイル（パッチ LM）を生成する「パッチリンカ」です。

この 2 つの機能を使用してパッチファイルを生成する一連の流れを図１に示します。

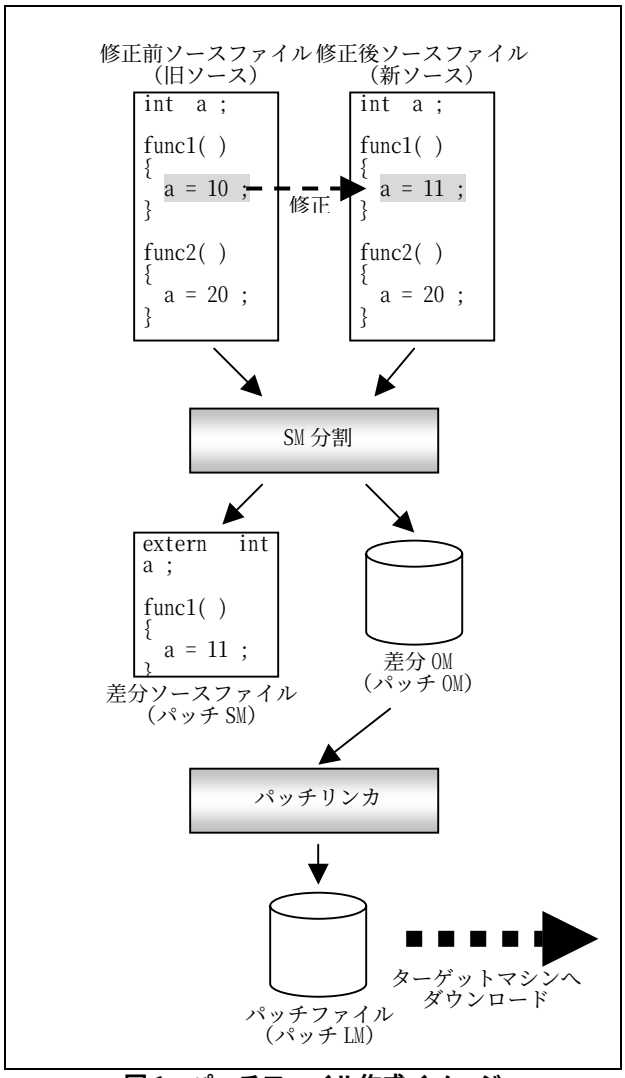

図 1．パッチファイル作成イメージ

パッチファイルを割り付けるためには、パッチエリアという専用のエリアを予め用意する必要があります。

*High-level language level patch making system by C language SM difference file automatic operation generation
†Kenji Kubota:NEC Communication Systemes,Ltd.

３．ＳＭ差分ファイル作成

３．１　プリプロセッサ展開

入力された新旧ソースファイルのプリプロセッサ展開を行います。

３．２　構文解析

構文解析は、プリプロセッサ展開したソースファイルを１行毎に行います。更に、１トークン(※)毎に分解し、その中から定義/参照している全シンボルについて管理を行います。

※トークンとは、Ｃ言語の予約語や演算子、区切り文字、関数/変数シンボルです。

３．３　差分チェック

構文解析の結果をもとに差分のチェックを行います。差分の対象単位は１関数/1 変数です。

３．４　パッチＳＭの作成

差分が発生した関数/変数毎のパッチＳＭを作成します。また、インクルードしているヘッダファイル中で定義している関数/変数に差分がある場合もパッチソースファイルの作成を行います。

尚、作成したパッチソースファイルのマクロ定義等は全て展開済みとします。

３．５　最適化対応

ソースファイルで差分が発生してもコンパイラの最適化によりそれぞれのパッチ OM の raw データに差分がない場合は、パッチＳＭの作成は行いません。

４．いろいろなパッチファイル

通常のパッチファイルは、修正（変更）のあった関数や外部変数、あるいは新規追加になった関数や外部変数なのですが、パッチリンカはそれ以外にもいろいろなパッチファイルを生成します。

４．１　ジャンプパッチ LM

修正後の関数が修正前の関数より大きくなった場合、修正後の関数をパッチエリアに割り付け、修正前の関数が割り付いている箇所にはジャンプコードを割り付けます。ジャンプコードのジャンプ先は修正後の関数の先頭アドレスとなります。

このジャンプコードのパッチファイルを「ジャンプパッチ LM」と呼びます。

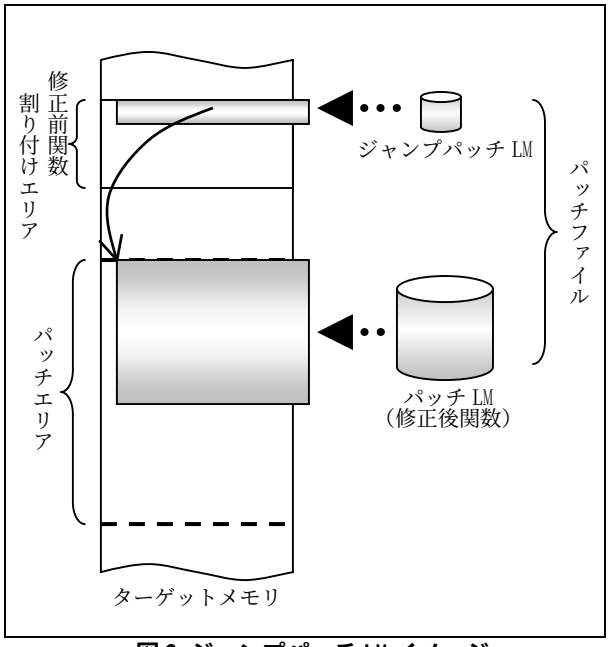

図 2 ジャンプパッチ LM イメージ

４．２　ライブラリパッチ LM

パッチファイルは既存のシステムコールを呼び出すことができるだけでなく、新たな（今までに呼び出していない）システムコール（またはライブラリ関数）を呼び出すことも可能です。パッチリンクの際に、新たなシステムコールが入ったライブラリ・アーカイブファイルを指定することで、そのシステムコールのみが組み込まれたパッチファイル「ライブラリパッチ LM」を生成します。

５．問題点

本システムでは前述の通り、関数に対するパッチファイルについてはいろいろな種類があり、実現不可能なパッチファイルは特にありません。しかし、外部変数に対するパッチについてはいくつかの問題点が残ります。

特に大きな問題が、変数サイズが大きくなる変数へのパッチファイル生成ができないことです。クロスリファレンス機能を設けることで実現は可能ですが、回避案があることと、必要性と改造規模の兼ね合いからこの機能は現在実装していません。