

ソフトウェア部品流通の基盤を整えた



第2章

メモリ管理のしくみとプロセッサへの実装



SH-3, Pentium, ARMのメモリ保護機能

IIMP カーネルは、SH-3, Pentium, ARM という、異なる形態の MMU (memory management unit) を持つプロセッサに実装された。ここでは、それぞれのプロセッサにおけるメモリ管理のしくみとメモリ保護機能実装のポイントを解説する。 (編集部)



1 MMU とは

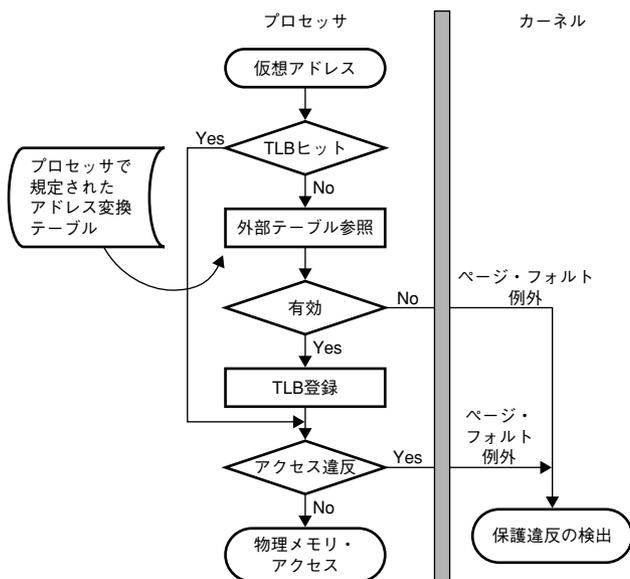
金田一 勉, 原田雅章

MMU (memory management unit ; メモリ管理ユニット) とは、プロセッサが持つメモリ保護のための機能です。MMUではなく MPU (memory protection unit ; メモリ保護ユニット) を持つプロセッサもありますが、MPUについ

ての説明は本稿4節の「ARMへの実装」に譲り、ここではMMUについて解説します。

MMUは、以下のような役割を持っています。

- 1) 仮想アドレスを物理アドレスに変換する情報テーブルを持つ
- 2) プログラムがメモリ領域にアクセスする方法に制約を設ける情報を持つ
- 3) 変換の対象となる仮想アドレスが情報テーブルにない場合やアクセス方法に違反がある場合、例外を発生させる



【図1】 CISCタイプのMMUにおけるプロセッサとカーネルの処理分担概念図

CISCタイプのMMUでは、メモリ保護違反判定はプロセッサによって高速に処理される。ソフトウェアによる最適化の余地はあまりない。カーネルはプロセッサが規定するアドレス変換テーブルを用意して、プロセッサに処理を依頼する。

MMUが持つアドレスの変換情報テーブルを、一般にTLB (translation look-aside buffer) と言います。

アドレスの変換情報テーブルの一つ一つは「エン트리」と呼ばれます。MMUは、いくつかのエントリを持ちます。一つのエントリは、「ページ」と呼ばれる固定長のメモリ領域のアドレスを変換対象としています。

1ページを4Kバイトとすると、例えば、仮想アドレス12345678Hは、上位20ビットのページ番号(12345H)と下位12ビットのオフセット(678H)に分けられます。MMUは、このページ番号(12345H)をTLB内から検索し、一致する変換情報から物理アドレスを取得し、その物理アドレスにオフセット(678H)を加算して実際の物理アドレスに変換します。

また、エントリには、対象となるメモリ領域へのアクセス方法を制約する情報を設定することができます。例えば、

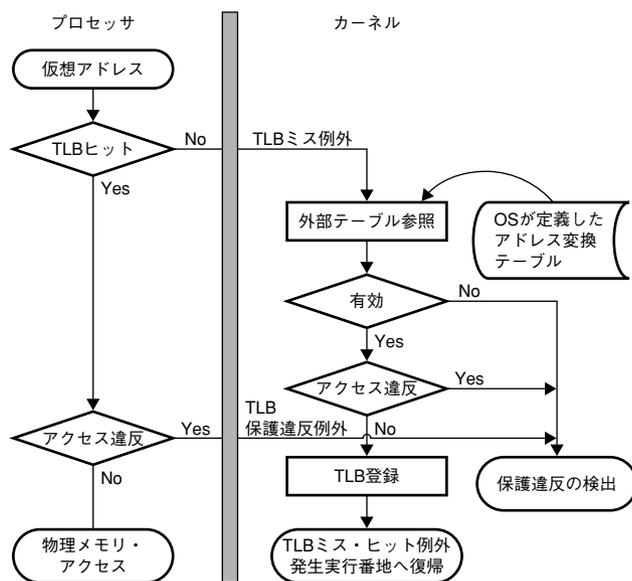
「書き込みを許可しない」, 「特権を持つプログラムはアクセスできるが, 非特権のプログラムはアクセスできない」という情報です。この情報により, メモリ領域へのアクセス保護を実現することができます。

MMUは, CISC (complex instruction set computer ; 複合命令セット・コンピュータ) タイプと RISC (reduced instruction set computer : 縮小命令セット・コンピュータ) タイプに大別できます。

CISCタイプのMMUは, TLB情報テーブルとは別に, アドレス変換テーブルを設定します。ソフトウェアがアクセスする仮想アドレスの情報がTLB情報テーブルにない場合, 自動的にアドレス変換テーブルからTLB情報テーブルに情報がコピーされるので, ソフトウェアでは, それらの情報テーブルの設定だけを行います(図1)。

RISCタイプのMMUには, CISCタイプのアドレス変換テーブルのようなものはなく, TLB情報テーブルの更新はソフトウェアで行います(図2)。

きんだいち・つとむ
(株)エルミックシステム
はらだ・まさあき
エーアイシーエンジニアリング(株)



【図2】RISCタイプのMMUにおけるプロセッサとカーネルの処理分担概念図

メモリ保護違反判定の大部分をソフトウェアで処理しなければならず, TLBの利用方法やOSが定義する外部テーブルの構造でソフトウェアの性能が左右される。逆に言うと, OSの規模に合わせて, 保護情報を設定する外部テーブルの構造を最適化することができる。

2 SH-3への実装

金田一 勉

μ ITRON4.0/PXの保護機能は, 大別して以下の2種類の保護を行います。

- 1) カーネル・オブジェクト保護
- 2) メモリ保護

カーネル・オブジェクト保護の処理はIIMPカーネルの共通部で行うため, プロセッサに依存しません。各プロセッサごとに実装するのは, 主にメモリ保護についての処理です。

メモリ保護機能に関する開発項目は以下のとおりです。

- 1) サービス・コールをソフトウェア割り込みとする
- 2) システムが占めるメモリ領域を管理する
- 3) MMUを初期化・設定し, 不正なメモリへのアクセスを検出できるようにする
- 4) MMUからの例外に対する処理を行う
- 5) ユーザ・ドメイン切り替え時にMMUの情報を切り替

える

- 6) タスク例外処理ルーチンの起動を行う
- 7) アドレスの正当性をチェックする

筆者は, TOPPERS/JSPカーネルに対して, μ ITRONメモリ保護機能仕様(μ ITRON4.0/PX)に準拠した機能をSH-3向けに追加しました。本稿では, このうちのMMUに関連する部分を中心に解説します。

SH-3は, RISCタイプのMMUを持つプロセッサです。RISCプロセッサは, 多くの組み込みシステムに採用されています。

今回の実装は, リアルタイム・システムにおいて, 保護機能を有しながらリアルタイム性を損なわないようにするための一つの方法だと思います。IIMPカーネルをほかのRISCプロセッサに実装する場合に, 本記事の内容が参考になれば幸いです。

●SH-3のMMUのしくみ

前節でも述べたように, MMUはアドレスを変換することを主な目的としています。プログラムがアクセスする仮想アドレスをMMUで物理アドレスに自動的に変換し, 実際のメモリ領域にアクセスします。アドレスの変換の際に, 読み出